Intelligent Response

MIR+MCIC User Guide

MIR 2.3 + MCIC 2.3

Please visit our forums at https://forums.mandiant.com/

MIR and MCIC Users Guide

Disclaimer

Table of Contents

List of Figures

List of Examples

Part I. Introduction

Table of Contents

Chapter 1
About this Book

The latest version of this document is available at *https://forums.mandiant.com/topic/official-mir-documentation/*.

1.1. Who Should Use This Book

The MANDIANT Intelligent Response *User Guide* is for incident responders, security professionals, and electronic evidence discovery analysts at all levels of their career. It is also for managers and others who need to understand how MIR and MCIC work and how staff members who use this software can most effectively do their jobs.

To get the maximum benefit from this user guide you should be familiar with basic incident response procedures and digital forensic concepts. You should also have a solid understanding of the various Microsoft Windows operating systems.

This guide provides basic information about the installation and use of MCIC, MIR Console and Agent. For information about the installation and use of the Controller appliance, please consult the *Administration Guide*.

1.2. How This Book is Organized

This guide contains the following...

Part I: Introduction

About This Book
This chapter, containing information about the *User Guide* and ending with MANDIANT product support details and reading recommendations.

Part II: About MANDIANT Intelligent Response

Chapter 2, What is Incident Response?
This chapter discusses the various types of security incident work tasks that incident responders and security professionals will encounter in their use of MANDIANT Intelligent Response.

Chapter 3, Electronic Evidence Discovery
A short discussion of electronic evidence discovery.

Chapter 4, The MANDIANT View of Incident Response
MANDIANT takes a specific approach in responding to incidents and investigations. We share our observations with you.

Chapter 5, What MIR Can Do for You
How our hardware appliances and software security tools help in using the MANDIANT approach to incident response and evidence discovery.

Chapter 6, System Requirements
System requirements for using MIR software.

Chapter 7, Speaking MIR
Incident response, and MIR particularly, has its own vocabulary, concepts, and software components. This chapter will help you come up to speed on MANDIANT's technology, and should be read by anyone who will be involved in the decision to use MANDIANT Intelligent Response, and those who will be using it in their day-to-day work.

Chapter 8, Installing MIR
This chapter contains procedures for installing the various MANDIANT Intelligent Response components.

Part III: MCIC Guide

Chapter 9, MCIC Quick Start
Out of the box, MCIC can perform a simple sweep of your network.

Chapter 10, Concept of Operations
Several important concepts and limitations of the MCIC Console are explained in this chapter.

Chapter 11, MCIC User Interface
MANDIANT Intelligent Response sweeps and basic results analysis can be done through a web browser using the MCIC Console interface. This chapter provides a high-level overview of the user interface, basic interaction with the Console, and customization and configuration information.

Chapter 12, URL Direct Access
Information on how to integrate MIR responses with web-scraping tools.

Chapter 13, Sweeping with MCIC
How to create a sweep, build its script, set its sweep windows, pick IOCs, and run a sweep.

Chapter 14, MCIC Remote Access
Enforce secure HTTPS and a secure user access mode.

Part IV: MIR Guide

Chapter 15, Console Overview
Your main interaction with MANDIANT Intelligent Response will be through an application called the Console. This chapter provides a high-level overview of the application user interface, basic interaction with the Console, and customization and configuration information.

Chapter 16, MIR Quick Start
This chapter runs you through a quick and simple usage example for the MIR Console. By the end of the chapter, you should have enough experience to start usefully exploring the Console's capabilities.

Chapter 17, Working with Audit Items
Most of your investigatory work will be directed to collecting information from Windows computers on your local network, organizing and reducing the content, and finding indicators of compromise that point to a security breach. This chapter covers all these details, with task-specific instruction that will help you develop a workflow that is efficient and productive.

Chapter 18, Using Search on Audit Results
The security breach discovery process will usually involve a lot of data-mining of audit results. MANDIANT Intelligent Response software has a powerful search engine that expedites this process. Naturally, the *Search* chapter explains how to use these tools effectively.

Chapter 19, Collaboration
If you are working with a team of security professionals, you will be interested in the support MANDIANT Intelligent Response provides for collaboration and data-sharing. This chapter discusses multi-user basics, change conflict resolution, and user activity tracking.

Part V: Appendices

Appendix A, Audit Modules and Analysis Commands
Detailed information about the use, parameters, and data returned by the Audit Modules and Analysis Commands.

Appendix B, Searches
A comprehensive listing of search keywords.

Appendix C, Error Messages and Troubleshooting
This appendix provides guidance on identifying and resolving problems you may encounter during your discovery and analysis workflow.

Appendix D, Agent Command-line Reference
MANDIANT Intelligent Response Agents can be installed or run audits from the command line, providing more flexibility than that available through installer-based use. This appendix provides a full description of command line usage, as well as some examples of command line use.

Appendix E, Client Scripts
The sample client script that ships with MANDIANT Intelligent Response is described here.

Appendix F, CEF-Compliant Logging
Instructions on configuring MIR to log to a remote server.

Appendix G, Script Acquisition via HTTPS
How to acquire audit data using the web API.

Appendix H, ArcSight Integration
MIR provides a logging and query interface compatible with Hewlett Packard's *Arcsight* enterprise security management tool.

Appendix I, Entropy, Anomalies, and Entry Point Signatures
There are several advanced techniques used in detecting suspicious file structures and file contents. This appendix discusses their application in your discovery workflow.

Appendix J, Legal Notices and Credits
MANDIANT Intelligent Response makes use of several Open Source and Shared Source technologies. For compliance with their various licensing terms, their full license declarations are included in this appendix.

1.3. How to Get Support

MANDIANT provides product support for its users. Telephone support is available via our support line at *877-9MANDIA* (877-962-6342). Email support is available from `<mirsupport@mandiant.com>`.

Many customers find our community forums to be a valuable resource. Please join us at *https://forums.mandiant.com*.

Before contacting Product Support, please have the following information prepared:

- Your name.
- Your company name.
- Email and telephone contact information.
- Your Controller serial number(s).
- The MTMS version number.
- The Agent version number.
- A detailed description of the problem, including any screenshots, error messages, or issues documents, and a list of steps and conditions that produced the problem.

1.3.1. Finding the Agent Version Number

1. Using Windows Explorer, navigate to the Agent installation directory.
2. Right-click `miragent.exe`, choose **Properties**, and select the **Details** tab.
3. Note the **Product Version** number. This is the value needed by MANDIANT Product Support.

1.3.2. Finding the Controller Serial Number

The Controller serial number is located on the left side of the Controller frame when facing the front of the appliance. If the unit is rack-mounted, you may need to remove the Controller from the rack.

1.4. For Further Reading

For a list of books and articles that MANDIANT staff members and others have written about computer security, incident response, and electronic evidence discovery, visit *http://www.mandiant.com/news_events/books/* and *http://www.mandiant.com/news_events/articles/*.

Part II. About MANDIANT Intelligent Response

Table of Contents

Chapter 2
What is Incident Response?

Incident response is the act of restoring the confidentiality, integrity, and availability of your information systems when they have been compromised by unauthorized activity. These types of incidents include:

- Computer security breaches, caused by viruses, trojan horses, and worms; and through social engineering via email, instant messaging, and phishing.
- Computer intrusions, such as break-ins to web applications or other server-hosted infrastructure.
- Unauthorized use of intellectual property and theft of customer data.
- Internal investigations of employee behavior.

2.1. Types of Security Incidents

2.1.1. Computer Intrusions

Attacks on your computer and network infrastructure can range from seemingly harmless vandalism by curious hacking hobbyists seeking notoriety, to sophisticated, aggressive, wide-scale theft of sensitive information or denial of service that can seriously jeopardize corporate — or even national — security.

Direct Exploit of Vulnerabilities

Direct exploitation of a vulnerability in your information technology infrastructure involves an attacker directly interacting with a computer system or network component (such as a router or switch) to get it to do something unintended. Such attacks include efforts to disrupt computer systems, steal data, or run malicious programs.

Direct exploitation is the grandfather of computer attacks. Original computer crackers from the ’70s, ’80s, and early ’90s practiced this form of compromise, giving rise to modern computer attack methods. Today, direct exploits are far less common in modern corporate and agency environments but do still happen, particularly when new vulnerabilities are announced by vendors or security researchers.

Viruses

A computer virus is usually an executable (`.exe`) file that is loaded and run on a computer without you knowing it. Some viruses are more annoying than they are destructive. Others can rapidly reproduce themselves, compromising system integrity or sensitive data. The most common way to “catch” a virus is through email, instant messaging, or web-browsing. Merely receiving an infected message is enough to infect your computer.

Worms

A worm is similar to a virus. Like viruses, worms can replicate themselves thousands of times. Unlike viruses, worms travel on their own throughout a network, replicating

automatically to more computer systems. A worm typically does this by exploiting vulnerabilities in other computer systems, automatically attacking systems across a network as it replicates itself.

Sophisticated worms can have many of the capabilities of a trojan horse: an attacker could obtain unfettered access to compromised systems, giving them complete control to do whatever they please. The self-replicating nature of worms makes them a particularly dangerous threat to consumer, corporate, and government networks.

Trojan Horses

A trojan horse is a program that installs malicious or damaging files under the guise of doing something desirable. While masquerading as legitimate software, a trojan horse may install a malicious payload that steals your information or changes the way your system behaves. For example, trojan horses are commonly used to set up networks of zombie computers, which are then used by various criminal enterprises to send spam or launch denial of service attacks.

Unlike viruses or worms, a trojan horse relies on you to run an executable file. Modern trojan horses can perform almost any operation: altering or erasing data, downloading and uploading files, installing spyware, logging keystrokes to steal sensitive data, turning off security protections on the victim system, and facilitating remote access to a computer. The list of compromises is nearly limitless.

Phishing

Phishing occurs when a criminal tries to fraudulently get sensitive information via online social engineering. Using email, instant messaging, fraudulent web sites, or a combination of these techniques, an attacker tricks victims into voluntarily providing personal information to them: banking and financial information, account numbers, user names and passwords, or Social Security numbers. Some criminals create web sites that masquerade as legitimate, well-known retail stores, then pose as online customer support representatives who need sensitive data to finish a transaction. Clever criminals impersonate people in need, conning the unwitting into directly transferring cash or other valuables.

Phishing is one of the most common techniques used by criminals planning to steal identities from their victims. It is important that organizations train their employees to be cautious and aware: there are no software solutions to the problem of phishing.

2.1.2. Internal Investigations

Insider abuse or malfeasance is an all-too-common reality in corporate and government environments. High-tech companies and agencies, computer systems and networks are often subjected to employee misbehavior. In your incident responses, you may be investigating instances of poor judgment (misuse of computers or networks to view inappropriate materials in the work environment, for example); or you may be examining outright criminal activity such as theft, embezzlement, or trafficking.

Theft and Misuse of Intellectual Property

Corporate secrets and intellectual properties are extremely valuable and often the heart of a high-tech company. Employees have often been involved in plots to steal these secrets and peddle them to the highest bidder. This class of incident also includes less exotic offenses, such as copyright infringement and plagiarism.

Compromise of Personally Identifiable Information

If an attacker can obtain personally identifiable information for an individual, it becomes trivial to steal the victim's identity and commit a number of crimes. Company insiders are often an excellent source of this data: someone with legitimate access to a customer database can quickly steal thousands — even millions — of records.

Digital Contraband

The Internet provides access to an endless source of media and software content that greatly increases your exposure to significant liability and business disruption. Employee misbehavior can lead to your corporation becoming a host or conduit to unlicensed or illegally copied software, pirated media content, and highly illegal forms of pornography. In all cases, these create situations that can lead to corporate liability or sanctions.

2.2. Combating the Threat

Companies with mature information security programs form *incident response teams*: experts who take action when an incident is suspected. A mature response process addresses every aspect of an incident, from immediate response through reporting findings to an organization's information security program so that new prevention and detection measures can be taken.

Chapter 3
Electronic Evidence Discovery

Electronic evidence discovery (EED) — sometimes called electronic data discovery or electronic document discovery — is any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case.

EED is typically initiated by some form of legal service (such as a subpoena, search warrant, or court order) requiring a corporation or agency to surrender documents that match certain criteria. “Documents” refers not only to paper materials, but to digital artifacts, including email, word processing files, spreadsheets, databases, images, and every other form of digitally-stored information. Inclusion criteria can specify document names, contents, subject matter, dates and times of creation or last access, recipients or other parties to a communication, and storage locations.

An organization that receives a request for EED must respond to the request within time and scope limits set by the courts, or face exposure to court sanctions or other legal action. MANDIANT Intelligent Response helps you meet these requirements.

3.1. What Organizations are Doing about It

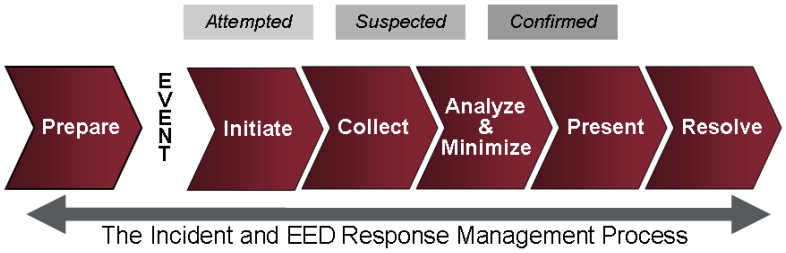
Organizations often employ personnel or contract services to respond to EED requests. Various technologies may be used to aid in the discovery and classification of data, including search technologies, disk imaging programs (software that copies the entire contents of a hard drive), and data review software (software that enables an analyst to review its contents and categorize it based on their observations).

Chapter 4
The MANDIANT View of Incident Response

MANDIANT's incident response philosophy has six major phases:

- Prepare
- Initiate
- Collect
- Analyze and minimize
- Present
- Resolve

Figure 4.1. The MANDIANT IR/EED Process



You will note the process is labeled "The Incident and EED Response Management Process." The reasoning for this is straightforward: when you examine the major aspects of EED and the processes needed to comply with a legal request; they are nearly identical to those needed for a computer security incident. An external event (such as court order) precipitates a response. You must identify information responsive to the request, collect it, analyze it to ensure it is compliant with the legal order, and present it to the requestor.

MANDIANT Intelligent Response focuses on the most labor-intensive part of this continuum for both incident response and EED: collection, analysis and minimization, and presentation.

4.1. Prepare

Preparation involves implementing measures before an incident occurs to ensure that resources for responding have been identified, assets that need to be defended have been inventoried, and potential actions to be taken in various response scenarios have been outlined. Thorough preparation also includes ensuring an incident response team has the tools it needs to do its job.

In an EED context, preparation involves measures taken before legal service is received to ensure the resources for responding have been identified, assets subject to discovery requests are available for review, and potential actions to be taken have been outlined. Preparation also includes ensuring the proper technologies have been staged for conducting EED activities.

4.2. Initiate

Once a security event is detected, usually via an observant employee or a component of your security infrastructure (such as intrusion detection systems or anti-virus software), the response process is kicked off through notification to the Incident Response Team.

For EED, initiation involves notifying a collection team of the legal request, identifying and notifying custodians of the requested data, and forming a collection strategy.

4.3. Collect

In an incident response scenario information must be collected about the suspected breach. This could include records from a detection system, reports from employees, or data from systems suspected to be compromised. This is similar to gathering evidence at a crime scene. In incident response, however, evidence collection often occurs while a breach is ongoing. Because of that, activities are often prioritized around reducing or eliminating risk, versus strict evidence preservation procedures.

Information must be collected in compliance with criteria specified in the warrant, subpoena, or court order for EED situations. This could include any form of digitally-stored information, such as email, word processing documents, or databases. In some circumstances, the criteria may be so broad as to call for collection of the entire contents of a hard drive or other storage media in one or more computer systems. Collections often span many systems, email boxes, or other information repositories.

4.4. Analyze and Minimize

Once data has been collected in response to a computer security incident, it must be sifted to identify the methods used by the attacker and to develop indicators (similar to footprints) that can be used to identify other systems or networks the attacker might have compromised. In most corporate environments quickly identifying the method used to conduct an attack, preventing its continued use, and expelling an attacker from your IT systems are the primary objectives. The volume of data that must be analyzed for even a small incident can be challenging.

When responding to a legal order, the tasks and challenges are similar. The primary difference is the data of interest is described in a legal document versus a matter of investigative insight. Once data has been collected, it must be sifted to identify information responsive to the discovery request. This typically involves a manual review of information by a human being familiar with the discovery request. Some technologies may be used during this phase, including search engines, databases, document mark-up tools, and other data organization and review technologies.

4.5. Present

When the details of a computer intrusion are understood, they need to be communicated in a way that is useful to analysts and investigators. IT organizations need enough technical data to counter the threat. Attorneys need to understand the scope of compromise, the likely source, and information that speaks to liability. Executives need to understand all these aspects and any continued threats to the business.

Presentation of EED results involves packaging information responsive to the request for delivery according to directives in the discovery request, or according to standards of care established by a judicial, legislative, or regulatory body. Legal counsel needs to thoroughly understand the information being provided in the response so that subsequent issues raised during the litigation process can be properly addressed.

4.6. Resolve

When responding to computer security incidents, the vulnerabilities or other circumstances that led to the breach need to be mitigated. Technical defenses need to be adjusted, compromised systems cleaned, and processes modified to bring the incident to a close. Feedback into proactive security activities needs to be provided so that future incidents of a similar type can be prevented or more efficiently resolved.

EED events often involve additional questions or requests for production of more information after an initial collection is finished. Full resolution may call for additional collection or more analysis of previously acquired information.

Chapter 5
What MIR Can Do for You

MANDIANT Intelligent Response is our vision for a technology platform that solves many problems faced by information security professionals. By concentrating on three of the four central phases of incident response — detection, collection, and analysis — we focus on providing tools that increase your ability to monitor systems and scope potential incidents by gathering critical data and analyzing it with powerful tools. With MANDIANT Intelligent Response, you can gather information from distributed locations to a central system and then analyze that information in a collaborative environment. MIR reduces the time needed to acquire incident data, understand its importance, and apply it to resolving an incident.

5.1. Features

MANDIANT Intelligent Response provides features that are of key importance to information security professionals, focusing on the rapid acquisition of the most relevant information associated with a security breach and using advanced search and analysis tools to reduce the time to understand and scope an incident.

MIR's feature set includes:

Centralized Data Acquisition
This allows you to acquire information over a network from any computer system that has a MIR Agent installed. You can acquire:

- Disk contents: files, deleted files, or the contents of an entire disk.
- System and process memory.
- System metadata: file listings, open network ports, system configuration data such as the Windows registry, and running processes.
- Eventlogs.

Data Analysis Tools
These help you review acquired data for indications of compromise. You can:

- Compare data sets to identify differences and similarities, such as suspicious processes and files.
- Create hash sets and compare them to identify changes.
- Timeline events on a system and adjust time skews to normalize different system clocks.

Powerful Search Capabilities
MIR search tools enable you to parse acquired data for specific words or phrases. With minimal effort, you can craft *indicators of compromise* to sweep through thousands of systems for those indicators. A summary report will list suspect systems, "clean" systems,

and systems experiencing communication errors; and report collation tools assist you in sharing that information appropriately.

Team Collaboration Tools

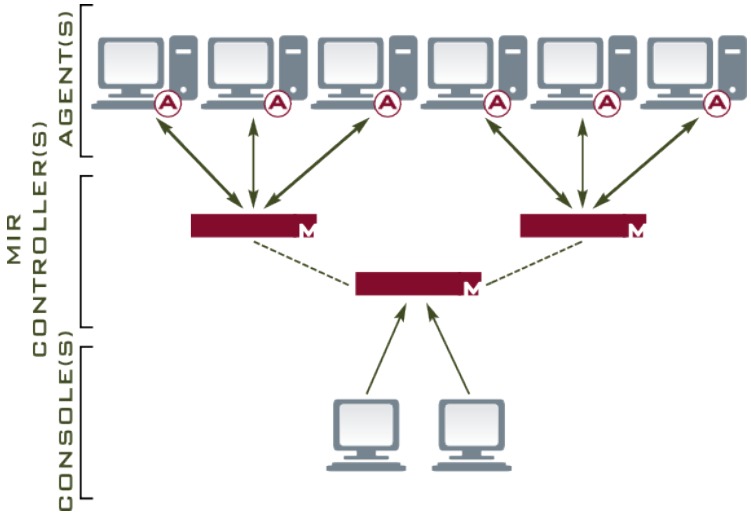
MIR lets you work as a team to acquire, analyze, review, and report on the same set of data simultaneously, allowing legacy serial tasks to be run in parallel and reducing your response times and costs. MIR's use of open format data exports lets you analyze the results of your investigation further, using your own or third-party tools.

5.2. Architecture

MANDIANT Intelligent Response comprises three main components: Controllers, Agents, and Consoles.

Investigators use the Console application to connect to a Controller appliance. In turn, Controllers connect to Agents. Agents are software components installed on end-user computer systems that enable the Controller to gather information about the system. All data is passed through and tracked by the Controller, ensuring all Consoles are accessing the same information.

Figure 5.1. MIR Architecture



The Controller

The Controller appliance is the heart of MANDIANT Intelligent Response: a combination of specialized hardware and MANDIANT Controller software. Analysis of acquired data is conducted by the Controller, enabling investigators to collaborate on the same set of information.

Future versions of the Controller appliance will allow you to cluster multiple units, enabling you to monitor vast numbers of Agents while still providing a unified view of data, analysis, and reports.

The Agent

The Agent is software installed on a computer system that you want to monitor. Agents allow analysts to gather information about any aspect of a system, from hardware inventory to retrieval of memory, registry, and hard drive data.

Consoles

Consoles provide an interface for using the system, displaying acquired data, and conducting analysis on that data. All data is sourced from the Controller, ensuring every Console has access to the same information and preventing Console users from creating divergent records.

There are two Consoles: MCIC, a simple interface for configuring and running sweeps; and MIR, a robust management tool for the creation and maintenance of host configurations, indicators of compromise, and detailed analysis of results.

Chapter 6
System Requirements

The MANDIANT Intelligent Response system is comprised of hardware and software components. The requirements for these components are as follows:

Network Appliance Requirements

- Installed and operational. You may require authorization for some functions. See the *Administration Guide* for additional information.

Console Requirements

- Microsoft Windows 7, Windows Vista, and Windows XP SP2 or higher.
- 1 GB of RAM.
- Microsoft .NET 3.5 SP1 software installed.
- Microsoft Internet Explorer 6 or higher.
- 75 MB of free disk space.
- Administrator-level privileges for installation.

Agent Requirements

- 32 bit versions of Windows 7, Microsoft Vista, Windows 2003 SP2, Windows 2000 SP4, and Windows XP SP2 or higher.
- 64 bit versions of Windows 7, Windows 2008 R2, and Microsoft Windows 2003 SP2.
- 512 MB of RAM.
- 12 MB of free disk space.
- By default, the Controller must be able to initiate TCP connections to the Agent on port `22201`.
- To test Agent Discovery Service, the Agent must be able to initiate TCP connections to the Controller on port `8077`.
- Administrator-level privileges for installation.

On Hosts that do not support memory-related audits, such as Windows Vista 64 bit, an Issue Document will be returned indicating an error occurred and that the Audit could not determine the OS version.

A long-standing bug in the Windows operating system causes any program using the `windows\temp` directory to fail when the directory has reached its 64K space allotment for files or folders.

In such case, the following message is written to the Agent log file (see *Appendix C, Error Messages and Troubleshooting*):

```
WARNING [Discovery CheckForUpdates]- Agent was not able to
create a temporary download folder. Agent will not update.
(13)
```

The solution is to manually remove some or all of the files in the `windows\temp` directory before attempting to install the Agent again.

Chapter 7
Speaking MIR

MANDIANT Intelligent Response has three main components: Agents, Controllers, and Consoles.

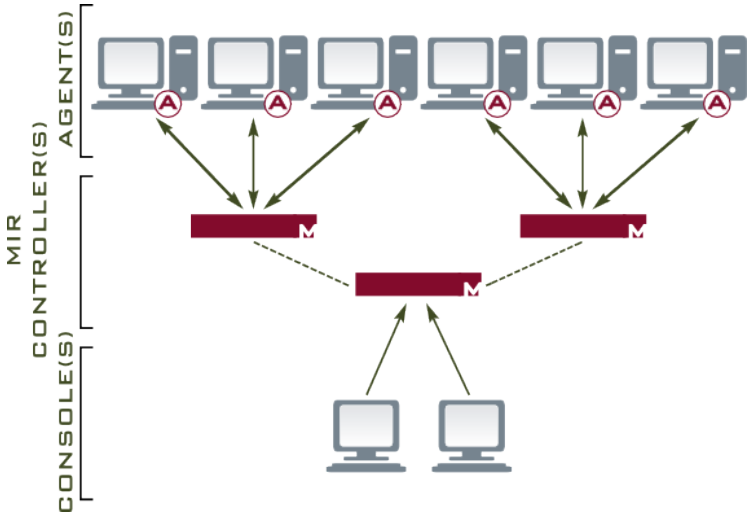
Agents are deployed on systems from which you want to retrieve information. They obtain factual *items* from the system, and forward them to the Controller. Whether responding to a security incident or a legal service, you seek factual evidence: time stamps, files containing specific data, discrepancies between expected data and actual data, and so on. Agents do the work of requesting and finding information: the items they discover are forwarded to the Controller for further processing.

Controllers are proprietary network appliances that house MANDIANT middleware. They comprise a hardware component and a software component, but are normally treated as a single component. They manage and retrieve data from Agents, then index and prepare that information for your use. The Controller acts as the go-between for Agents and Consoles and serves to largely decouple you from the need for a single, fixed workstation — an important benefit when your local network is distributed through a vast space.

Consoles are the main user interface for MIR. They connect to Controller appliances to launch data collection jobs across Agents, view data, and conduct analysis. For ease of use, MIR provides two Console interfaces: a simple UI named MCIC, suitable for configuring network sweeps and performing a first-pass investigation of results through a web browser; and a stand-alone console named MIR, which provides a comprehensive UI for managing hosts and agents, creating indicators of compromise, configuring scripts, jobs, and schedules, and so on.

This chapter describes these components in detail and introduces you to MANDIANT Intelligent Response terminology. It also details the features and capabilities of the Console interface. Note that examples and procedures in later chapters assume familiarity with this material.

Figure 7.1. MIR Architecture



7.1. MIR Terminology

When you are working with MIR you will often encounter specialized terms. These terms refer to actions within the system (such as “conduct an audit”), as well as data resources within the system (such as “an audit from a specific host”). Understanding these terms will make using the product easier. Following is a list of commonly-used terms.

Agent
Software installed or run on a Host, used to collect Items from the system.

Host
In the scope of a local network secured by MANDIANT Intelligent Response, a Host is a Microsoft Windows system on which an Agent has been installed.

Item
A separate piece of an Audit or Analysis data, such as record of port information or a single system information record. Items are not mutable: you cannot change them, because they are created from factual information on a Host. Examples include file sizes, process listings, checksums, directory listings, and other items.

Audit
A collection of items from a Host that has been gathered by an Audit Module. The term Host Audit may be also be used for this collection of information. Audit Modules are run by Agents.

Analysis
An operation to identify and manage differences and similarities between Audit collections, using one or more Analysis Commands, reducing the data to the most relevant elements.

Script
A series of instructions for conducting an Audit, an Analysis, or an initialization of data through the Console. These are called Host Audit Scripts, Analysis Scripts, and Client Scripts, respectively. Scripts are used by Jobs, which provide the Script with a list of objects upon which to act.

Job
A list of objects upon which a Script will act, plus the Script itself.

Resource
Any user-managed, organizational object. Resources are mutable: you can change them, because you created or collated them. Examples include Host Records, Audit Results, Result Sets, Documents, Indicators, Labels, and other objects.

Result Set
Multiple Audit Results and Analysis Results that are part of the same job are packaged in a Result Set. Consider an example where multiple Hosts are being audited simultaneously. The results from each Host would be in an Audit Result. All the Audit Results for the job would in turn be placed in a Result Set.

7.2. The Agent

Agents are installed on systems from which you want to collect items. Agents may be configured to communicate over a network or may run interactively in local mode, writing

acquired items to local storage (such as a hard drive or USB key). When configured for network operation, an Agent can run as a daemon or as a persistent Windows service.

Agents are packaged with multiple Audit Modules. Each module enables the collection of a different type of item. *Appendix A, Audit Modules and Analysis Commands* has a condensed list of modules, followed by details for each of the many Modules (description, data returned, parameters, etc.)

7.3. The Controller

The Controller is a network appliance that manages data acquisition, data organization, and data storage; and provides search functionality and a application interface to this information. Its data analysis capabilities allow you to manipulate data once it has been acquired from a series of Agents, and its multi-user support ensures users connecting to the same Controller can use the same set of Agents, view the same data, and work collaboratively on analysis and reporting.

Analysis is provided through a series of Analysis Commands, which use one or more Controller services to manipulate datasets acquired from Agents. These commands evaluate or transform information so that investigators can minimize datasets down to the most relevant elements. The following Analysis Commands are supported in MIR:

Timeline
: Takes time-based events from multiple Result Documents, potentially of different types (such as a file listing and event logs), and merges them into a single time-ordered view.

Time Skew
: Adjusts timestamps in a Result Document. Useful for comparing Audits between Hosts with differing clock settings.

Document Difference
: Shows the difference between two Result Documents across a common set of fields, hiding information they share. Useful for finding differences between Hosts or changes to a single Host over time.

Document Intersection
: Shows the overlap between two Result Documents across a common set of fields, hiding information that differs. Useful for finding similarities between Hosts.

The Controller also indexes all data returned by Agents and provides a powerful search engine that allows you to create arbitrarily complex terms based on keywords, boolean logic, ranges, and wildcards.

7.3.1. A Note on Agent Management

Before MIR can be used to acquire data, Controllers must obtain network address information for their target Hosts. MIR provides two methods for finding deployed Agents:

Agent Discovery
: The Agent Discovery Service runs on the Controller and allows Agents to periodically report their network address and status to the service. This self-reporting process allows you to easily find all (properly-configured) Agents on your local network without requiring further knowledge.

Manual Specification
In the manual case, you connect to the Controller using a Console and enter network address information finding your deployed Agents. This process requires you to know the target Host's IP addresses.

7.4. Consoles

Consoles provide an interface for using the MIR system in a collaborative environment. Through a Console, you can execute jobs that acquire or analyze data, display acquired data, and write reports. A Console connects to the Controller through the local network and requests data to be rendered to the user interface. All user requests to acquire new data, analyze data, or modify data are sent from the Console to the Controller for fulfillment. Additional features implemented within the software are also available through the Console.

There are two consoles:

MCIC
Runs through a browser and provides a simple UI for basic network sweeping and investigation.

MIR
A stand-alone application that provides a comprehensive UI for configuring, managing, and maintaining the MIR system.

In working with Consoles, there are many terms that have special meaning:

Libraries
Collections of Resources organized by type, as part of the user interface provided by the Console. Libraries help you quickly reference, collate, or modify resources as you develop Scripts and Jobs.

The following Libraries are available through the Console:

Jobs
Contains all Jobs on the system.

Hosts
Contains all Hosts known to the Controller. This includes both manually-configured Hosts and those created through the Agent Discovery Service.

Indicators
Contains all Indicators defined on the system.

Labels
Contains all available Labels, including those provided by the system and those created by users.

Saved Searches
Contains saved searches. As you develop your incident response workflow, you will find that some searches are used frequently: it is useful to save those searches for re-use.

Scripts
Contains all Scripts on the system.

Results Documents
Contains all Audit Results on the system, whether from Host Audit Jobs or Analysis Jobs.

Hosts
In the Console, a Host is also a Resource: a record created by yourself or the Agent Discovery Service, storing information about the network location, hostname, and other information about a particular Microsoft Windows system on which an Agent has been installed.

Indicators
A pattern or patterns of data that indicates a Host may have been compromised. Typical Indicators of Comprise include malware byte signatures and executable file structural flaws.

Labels
The Console provides a method for marking data for future reference. Labels are particularly useful as a Case Note folder: by labeling all items and resources (Hosts, Audit Results, Indicators, etceteras) relevant to the current investigation with the same Label, you can easily find the collected objects later.

Chapter 8
Installing MIR

Installing MIR gets you up and running with MANDIANT Intelligent Response. The material below assumes that your administrator has installed and configured the Controller. Your administrator must also have provided you with a user account, account password, Console and Agent installers, and several installation configuration files.

The following examples cover the simple install case. The *Administration Guide* covers deployment in further detail.

8.1. Installing the Controller

Your MANDIANT Intelligent Response administrator is responsible for installing and configuring the Controller.

8.2. Installing the Agent

Agents are installed or run on Host systems, sending requested items to the Controller or writing it to local storage. You can then access these items using a Console.

There are several ways to deploy Agents; your choice will be determined in part by the type of investigation you are doing and your usual business practices. The following examples demonstrate two ways to install an Agent: first, by using the interactive Windows installer, which results in the Agent being installed in Service Mode; and secondly, manual installation for Portable Use Mode. In Service Mode, the Agent is “permanently” installed and runs as a Windows Service; in Portable Use Mode, the Agent runs from and stores data to a portable media device.

The Agent installer is approximately 6 MB. Once installed, the Agent uses 12 MB of disk space.

Agent Requirements

- 32 bit versions of Windows 7, Microsoft Vista, Windows 2003 SP2, Windows 2000 SP4, and Windows XP SP2 or higher.
- 64 bit versions of Windows 7, Windows 2008 R2, and Microsoft Windows 2003 SP2.
- 512 MB of RAM.
- 12 MB of free disk space.
- By default, the Controller must be able to initiate TCP connections to the Agent on port `22201`.
- To test Agent Discovery Service, the Agent must be able to initiate TCP connections to the Controller on port `8077`.
- Administrator-level privileges for installation.

On Hosts that do not support memory-related audits, such as Windows Vista 64 bit, an Issue Document will be returned indicating an error occurred and that the Audit could not determine the OS version.

A long-standing bug in the Windows operating system causes any program using the `windows\temp` directory to fail when the directory has reached its 64K space allotment for files or folders.

In such case, the following message is written to the Agent log file (see *Appendix C, Error Messages and Troubleshooting*):

```
WARNING [Discovery CheckForUpdates]- Agent was not able to
create a temporary download folder. Agent will not update.
(13)
```

The solution is to manually remove some or all of the files in the `windows\temp` directory before attempting to install the Agent again.

8.2.1. Installing an Agent Using the Windows Installer

The easiest way to install an Agent is with the Windows installer. This method lets you quickly perform a default install, but limits your customization options. By default the Agent is installed as a Windows Service listening on TCP port `22201`.

You must have Admin-level privileges to install the Agent.

1. Create a folder named `MTMS Install` on the Host or on portable media.
2. Copy `AgentSetup.msi`, the Agent installer to the `MTMS Install` folder.
3. Copy `conf.xml` to the `MTMS Install` folder.
4. Start `AgentSetup.msi` and follow the prompts:
   a. In the **Welcome to...** window, click **Next**.
   b. In the **License Agreement** window, select **I Agree** and click **Next**.
   c. In **Select Installation Folder**, accept the default installation destination unless you have reason to install to a different location. Clicking **Disk Cost...** will display the available and required drive space for the installation.

      Click **Next** to continue.
   d. In **Confirm Installation**, click **Next**. A progress bar will advance as the software is installed.
   e. In the **Installation Complete** window, click **Close**.

Note that Agent installation does not require a system restart.

8.2.2. Customizing the Agent Configuration

1. Create a folder named `MIR Install` on the Host or on portable media.
2. Copy `AgentSetup.msi`, the Agent installer, from the MIR software CD to the `MIR Install` folder.
3. Copy `conf.xml`, the default Agent configuration to the `MIR Install` folder.

4. Using any plain text editor (`notepad.exe`) open `conf.xml` and configure your preferences. Closing tags must be used. Most values may be left with their default values; exceptions are noted below.

   <section name="discovery">
   Contains settings for the Agent Discovery Service, which is used to maintain an up-to-date list of Hosts in the Console's Host Library.

   <key name="server">*localhost:8077*</key>
   The Controller's Discovery Service address and port. **This setting must be customized.**

   <key name="error_retries">*3*</key>
   The number of times the Agent will attempt to contact the Controller before taking a time-out.

   <key name="interval">*30*</key>
   The length, in minutes, of an error retry time-out.

   <section name="service">
   Contains settings for the Agent's *Services* entry in the Windows Management Console.

   <key name="service_name">*IntelligentResponseAgent*</key>
   The short-form name of the Agent. This value should not be modified.

   <key name="service_displayname">*Intelligent Response Agent*</key>
   The long-form name of the Agent. This value should not be modified.

   <key name="service_description">*MANDIANT Intelligent Response Agent*</key>
   The description displayed in the Agent Service details. This value should not be modified.

   <key name="audit_issue_filter_level">*info*</key>
   When creating an Audit Issues Document, detailing the operation and success or failure of the Agent Module, include all information at and above this level. `debug`, `info`, `warning` and `error` are acceptable values providing progressively less information (and less network traffic.)

   <key name="hidden">*false*</key>
   On 32-bit Windows XP and Vista hosts, hides the process name from *Task Manager*, hides the installer from *Add/Remove Programs*, and hides the installation folders. When **false**, the user can easily see and kill the Agent process and can un-install the Agent.

   On 64-bit Vista and on Windows 7 hosts, this setting hides the installer from *Add/Remove Programs* and hides the installation folders. The process name is not hidden in the *Task Manager*.

   <key name="hideFromAddAndRemove">*false*</key>
   Hides the installer from *Add/Remove Programs*, making it more difficult for a user to remove the Agent. This setting is applicable only when *hidden* is *false*.

<key name="firewall_exception_mode">*auto*</key>
Determines how the Agent will handle Windows Firewall exceptions. Exceptions will be removed when the Agent is uninstalled or when *MIRAgent.exe* is executed with the `-cleanup` or `-dissolve` options.

`Auto`
Add an exception when starting the MIRAgent process and remove it when stopping.

`ServiceAdd`
Add an exception once only when installing as a service and remove it when uninstalling..

`AlwaysAdd`
Add an exception once.

`NeverAdd`
Do not add an exception.

<section name="web_server">
Configures access to the Agent by Controllers.

<key name="bind_ip_string">*0.0.0.0*</key>
Sets the local address on which the Agent will listen for Controller communications.

<key name="bind_port">*22201*</key>
Sets the port on which the Agent will listen for Controller communications.

<section name="logging">
Contains settings for the Agent log reporting.

<key name="enabled">*true*</key>
Sends Audit and Agent logging information to the Controller. When `false`, logging information will not be available in Consoles, and network traffic will be reduced.

<key name="log_level">*info*</key>
Includes all logging information at and above this level. `debug`, `info`, `warning` and `error` are acceptable values providing progressively less information (and less network traffic)

<key name="maxIndex">*4*</key>
The maximum index number for rolled-over log files. When rolled-over log index numbers are incremented, the oldest log file will be deleted if its index value exceeds the maximum index number.

<key name="minIndex">*0*</key>
The starting index number for rolled-over log files.

<key name="maxFileSize">*250*</key>
The maximum size of a log file before the current log file renamed to `filename.ext.min log rollover index`. When this happens, existing rolled-over log index numbers are incremented.

<key name="filename">*MIRAgent*</key> and <key name="fileext">*log*</key>
Sets the name and extension of the host log file. See for *Appendix C, Error Messages and Troubleshooting* for location and content details.

<section name="credentials">
Contains SSL credentials.

<key name="cacert">-----BEGIN CERTIFICATE-----*certificate data*</key>
The Controller's CA Certificate. This may be downloaded directly from the controller at *https://Controller* URI or Hostname/mircacert.pem and then pasted here. **This setting must be customized.**

<key name="crl">-----BEGIN X509 CRL-----*certificate data*</key>
The Controller's CRL. This may be downloaded directly from the controller at *http://Controller* URI or Hostname/mircacrl.pem and then pasted here. **This setting must be customized.**

Use care when copying SSL credential data. Extraneous characters — including spaces at the end of a line — will create an certificate errors. The installer can not confirm the correctness of the credential data, resulting in a complete installation but an Agent that can not run.

8.2.3. Removing an Agent using the Windows Control Panel

Agents sometimes need to be re-installed to update their `mircacert.pem` and `mircrl.pem` certificates; or need to be removed from a Host. This is easily accomplished using the Windows **Add or Remove Programs** control panel.

1. In **Start** → **Control Panel** → **Add or Remove Programs**, select **MANDIANT Intelligent Response Agent**.
2. Click **Remove** and follow the prompts.

There are a number of alternative installation scenarios: *Portable Use Mode*, which allows you to collect data without connecting to the network, or collect data without installing an Agent on the Host system; various command-line driven installation options that provide more configuration options than permitted through the Windows Installer process; and so on. See the *Administration Guide* for details.

8.3. Installing the Consoles

Consoles are your primary interface to the MANDIANT Intelligent Response system. Consoles communicate with the Controller, which in turn controls the behaviour of Agents. Installing the MIR Consoles (MCIC and MIR) is a straightforward process.

The Console installer is under 10 MB and the Console installed footprint is approximately 60 MB. More details can be found in the *Administration Guide*.

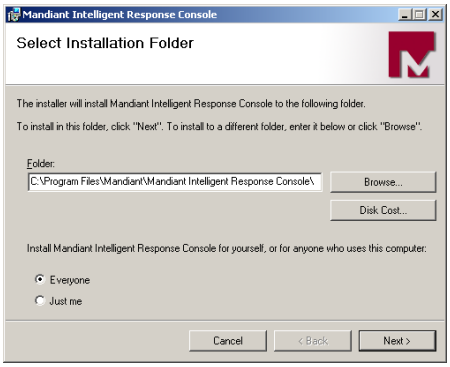
8.3.1. Installing the MIR Console

The Console has the following requirements:

- Microsoft Windows 7, Windows Vista, and Windows XP SP2 or higher.
- 1 GB of RAM.
- Microsoft .NET 3.5 SP1 software installed.
- Microsoft Internet Explorer 6 or higher.
- 75 MB of free disk space.
- Administrator-level privileges for installation.

You may wish to export your custom IOCs before you uninstall the old Console.

1. Copy `ConsoleSetup.msi`, the Console installer, to your workstation.
2. Start `ConsoleSetup.msi` and follow the prompts:
3. In the **Welcome to...** window, click **Next**.
4. In the **License Agreement** window, select **I Agree** and click **Next**.
5. In the **Additional Tasks** window, enable the options you want to use, then click **Next**.
6. In **Select Installation Folder**, accept the default installation destination unless you have reason to install to a different location. Clicking **Disk Cost...** will display the available and required drive space for the installation.
7. Select **Everyone** or **Just me** depending on whether you want all users with access to this workstation to have the ability to use the Console, or want access to be restricted to just your own account.
8. Click **Next** to continue. A progress bar will advance as the software is installed.



9. In the **Installation Complete** window, click **Close**.

8.3.2. Uninstalling the Console

1. In **Start** → **Control Panel** → **Add or Remove Programs**, select **MANDIANT Intelligent Response Console**.

2. Click **Remove** and follow the prompts.

Part III. MCIC GUIDE

Table of Contents

Chapter 9
MCIC Quick Start

If you are eager to begin using MCIC, here is a brief description of how to start a sweep.

We strongly recommend reading *Chapter 10, Concept of Operations* before using MCIC.

1. Browse to MCIC at `https://Controller URI or Hostname/apps/webclient/`.

   Log in with your usual MIR Console credentials.

2. The first time you run MCIC a **System Message** will ask you to confirm that the correct *Deployed Agent Version* has been configured. When you click **OK**, you will be automatically taken to the **Settings** → **Global Settings** page.

3. In **Settings** → **Global Settings**:

   a. Set **Agent Discovery Timestamp Window** to a value suitable for your environment. This will be the same value as the discovery interval value used by MIR Agents.
   This is important!
   If it is too low, Hosts will be missed during the sweep.

   b. Set **Deployed Agent Version** to match that of the Agents deployed in your network.
   This is important!
   The parameters passed to Agents vary dependent on their version; if this value is incorrect, Agents may reject sweep requests.

4. Click **Sweeps** in the left navigation pane. In the main window, click **Create New Sweep**.

   a. Provide a **Sweep Name**.

   b. Leave **IOC Source** as **All IOCs (Default)**.

   c. Click **Build New Script**.

      Ensure **Selected IOCs** includes the IOCs you wish to sweep.

   d. Click **Get Audit Modules**.

      If a “Show Errors” message appears at the top of the **Script Builder** window, expand the error list by clicking the **+** symbol. Review the error messages and take appropriate remedial action.

   e. At the bottom of the **Script Builder** window, provide a **Script Name**. The sweep name is often a good choice.

   f. Click **Generate Script**. Wait a moment, then close the window as prompted.

   g. Set the **End Date**. Do not bother with a start date, as you will run the sweep immediately.

h. Click **Save Sweep**.

After a moment, the **Sweep Status** view will be shown. The Job will start running soon, and will continue to run until your specified **End Date**.

5. Once the Job has reached an acceptable success rate, generate a report of hits by clicking **Generate**.

If you need to end a sweep:

1. Stop the sweep:
   Click **Sweeps** in the left navigation pane. Click **Pause** in the the main window.

2. Stop any running Jobs:
   Click **Sweeps** in the left navigation pane. In the main window, the message “Sweep Job is Currently Running” shows that a Job is running. To stop the Job, click **View Running Job** and then **Cancel** the Job that is shown.

Chapter 10
Concept of Operations

MCIC is a very powerful tool that can make searching your environment for IOCs an easy task. Unfortunately, it also makes it easy to severely affect the performance of the MIR Controller and potentially of Agent Hosts on your network. To help reduce the likelihood of a problem MANDIANT recommends each MCIC user carefully read this section and understand and follow its guidance.

10.1. What is a sweep?

MANDIANT calls the process of searching your environment for a set of IOCs a *sweep*. MANDIANT does not use the term “scan” as it generally implies a network-based function or some other process that is not similar to what we call a sweep.

10.2. What is a Job?

A Job is a unit of sweep work. By default a sweep is broken into work units of 5,000 Hosts each. The default sweep configuration allows a maximum of 100 result sets per sweep. These defaults have been picked to keep the sweep process efficient.

10.3. What do I need to be able to sweep?

To perform a sweep you need a set of IOCs and a group of Hosts that you would like to sweep.

10.4. What should I do before I run a sweep?

Before running a sweep across many Hosts, you should always test the sweep. It is very easy to create an IOC that will return too much data, or not the correct data, causing problems. MANDIANT recommends the following:

- Use the MIR Console to Label a small number of Hosts for testing.
    - Ideally, Label one or two Hosts from each major category of Hosts. For example, two servers, two desktops, and two laptops.
- Create a new sweep and run it against the test Hosts.
- Generate a MCIC report and examine the hits.
- Open the MIR Console and manually inspect the Audit Results documents for each Host in the test Job.
    - This is important, as sometimes extraneous results are returned that the MCIC reporting process removes. The same can be said of issue documents: sometimes a particular audit will generate large lists of issues, especially if audit issue logging is set to info.

      These extraneous results nonetheless create network and machine load, and eliminating them by refining the sweep parameters will improve performance. * When you are

satisfied the sweep is correctly configured, create a new sweep and run it against all Hosts.

10.5. How long will a sweep try to sweep Hosts?

The sweep tries to check all Hosts for the specified IOCs. If a Host is offline or has a problem, the sweep will try it again at the next opportunity. Once all Hosts are successfully swept the sweep will end.

The actual run time that a sweep will need varies. Factors such as the number of IOCs you are looking for, the speed of the Hosts that you are inspecting, and the availability of those Hosts all plays into how long a sweep will take. An important controlling factor is the Sweep Timeout setting, which controls how long a Job will wait for a Host to acquire data before leaving it for the next pass.

Keep in mind that once the sweep process is finished on a Host, it is not checked again during that sweep.

10.6. Can I run more than one sweep at a time?

MANDIANT recommends that you run only one enterprise-wide sweep at a time. If you are targeting smaller numbers of Hosts (numbering in the hundreds), multiple concurrent sweeps are probably OK. The key is to monitor the indexer size and other Controller health indicators, and ensure you do not exceed recommended thresholds.

10.7. What happens to new Hosts that appear on the Controllers after a sweep is started?

MCIC will periodically detect new Hosts and automatically add them to active sweeps.

10.8. How often should I run a new sweep?

For sweeps of large sets of IOCs you should try to start a new sweep at least once a month. Depending on the environment you may be able to run more than once a month. The balance is a trade-off between user impact and the risk of missing an infection.

10.9. How often should I generate IOC Findings reports?

Standard sweeping protocol for MANDIANT is to generate findings no more than once a day. However, during an active incident, MANDIANT consultants generate findings reports on an as-needed basis — sometimes multiple times throughout the day.

10.10. Why do I not reach 100% completion?

The sweep process needs a Host to be online and remain online while MIR is inspecting that Host for IOCs. Many common conditions prevent this:

- Environments that have highly mobile users (wireless, VPN, different sites, etc.)
- User is on vacation.

- User is issued multiple computers and rarely turns them all on.
- User goes home and shuts their computer off.
- The **Settings** → **Global Settings** → **Deployed Agent Version** value does not match the version number of deployed Agents.
- ...and other instances of Host inaccessibility.

10.11. What if the Controller fails?

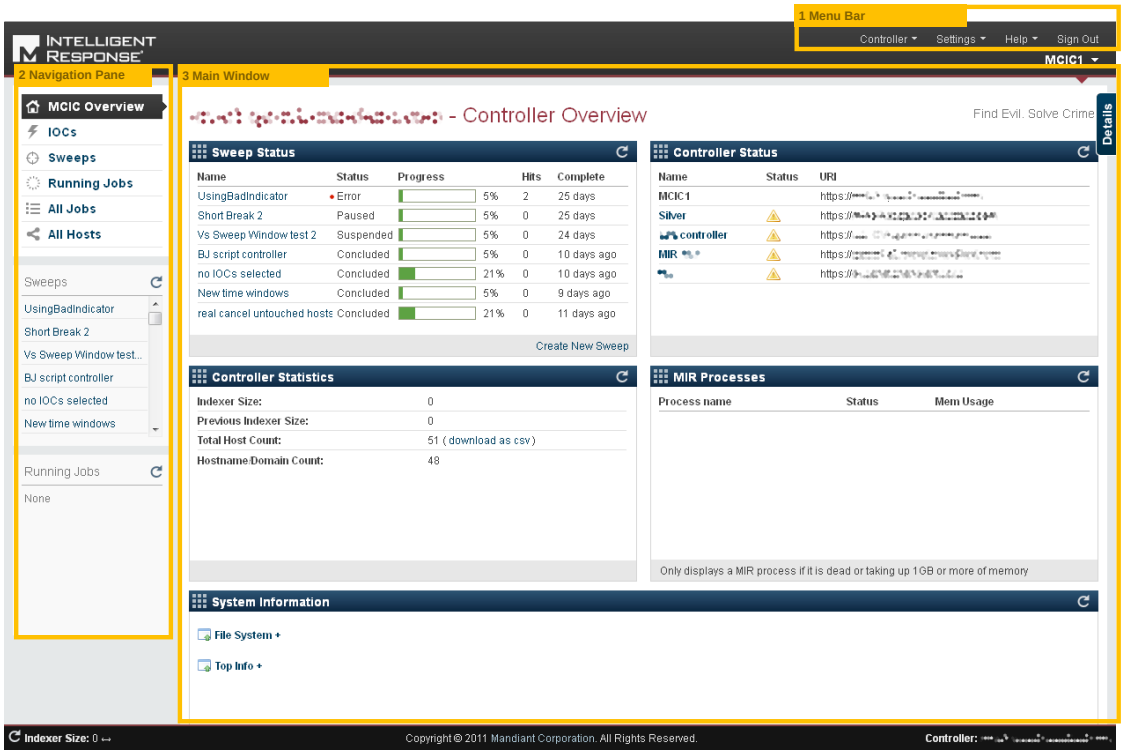
If the MIR Controller is rebooted, powered-cycled, or crashes during a sweep, the system may not correctly record Hosts' sweep states. This may lead to Hosts being considered as "swept" although they were not. It is recommended that after an uncontrolled failure event, that you run the sweep again: some hosts may be re-swept, but this will ensure that all Hits are found.

When the MIR Controller must be rebooted or power-cycled, pause the sweep and cancel all running Jobs before performing the reboot or power cycle. This will ensure that Hosts' sweep states are correctly recorded.

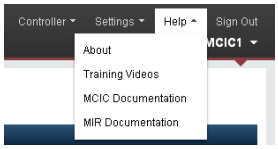
Chapter 11
MCIC User Interface

The MCIC interface has three main areas:

- The menu bar.
- The navigation pane.
- The dashboard pane.



11.1. The Menu Bar



The menu bar provides the following menu items:

Controller

/workspaces/1
A web interface to all MIR documents and information.

Administration
Opens the MIR Controller Administration web interface.

Open Console
Opens the MIR Console, if it is installed.

System Reports
Manages system report packages. (Administrators only.)

Settings

Global Settings
Settings for Sweeps and Audits.

Controllers
Settings for Controller networks.

Help

About
The version number and a brief description of MCIC.

Training Videos, MCIC Documentation, MIR Documentation
Opens your default browser to access MANDIANT's online resources.

Sign Out
Logs you out of the Controller.

11.1.1. System Reports

Controller → **System Reports** provides access to the `MIRSystemEval.sh` Controller Report generation utility. This command is available to Administrators only.

When using this command, you may choose to enable or disable log file collection. Log files greatly increase the size of report files.

There is no limit on report file size or the number of reports you may keep on the Controller, as long as there remains adequate disk space. We suggest deleting reports that are no longer needed, using the **Delete** icon to the right of the report entry.

11.1.2. The Settings Command

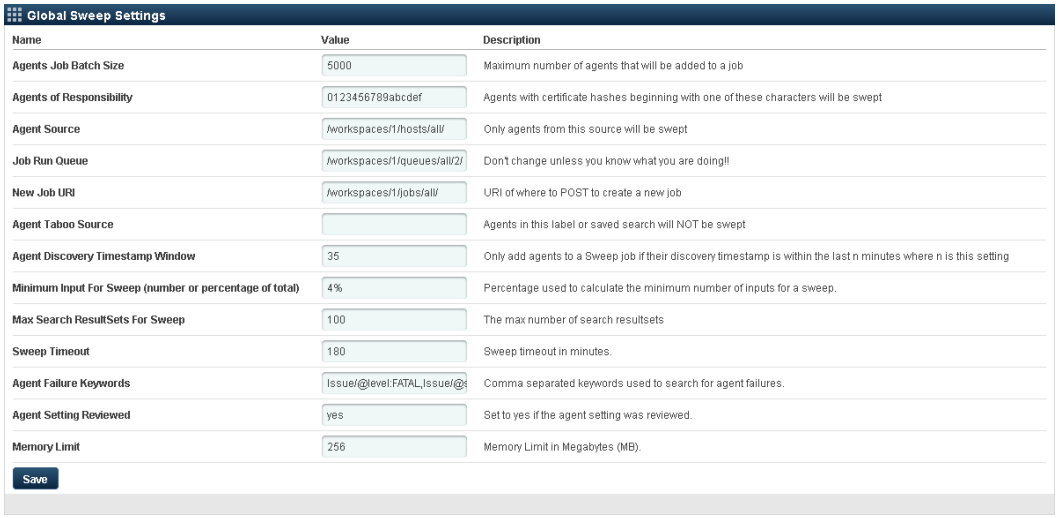
MCIC settings are viewed and changed through the **Settings** menu. Settings affecting the performance of sweeps and audits are accessed through **Global Settings**. Configuration of the MCIC Controller network is accessed through **Controllers**.

11.1.2.1. Global Settings

Agent Discovery Timestamp Window and **Deployed Agent Version** are the most important settings and ***must*** be correctly configured for your installation. See *Chapter 9, MCIC Quick Start*.

All settings except those noted above should be fine at their default settings for most environments. These settings are global: they are applied to all sweeps.

There are three sections: **Global Sweep Settings**, **Deployed Agent Version**, and **Audit Preferences**.



In **Global Sweep Settings** you can set the default configuration for new sweeps. The fields are as follows:

Agents Job Batch Size
: Limits the number of Agents (Hosts) that MCIC will put into a single Job. If a Controller or network has performance issues you may want to lower this number.

Agents of Responsibility
: A list of hexadecimal digits used by Controllers to filter the Agents with which they will communicate. When more than one Controller will sweep Agents, you need a way to decide which Controller will sweep which Agents. Since all Agents have a unique certificate hash, you can use the first letter of that hash to assign the Agent to a specific Controller. By default, includes all sixteen hexadecimal digits.

Agent Source
: The workspace used as the source of Agent discovery data when **All Hosts** is selected as the input for a sweep.

Job Run Queue
: The queue URI into which MCIC will place sweep Jobs. By default it uses the *run now* queue, which runs a Job immediately.

New Job URI
: The URI to POST to create a new job.

Agent Taboo Source
: Agents in this label or saved search will NOT be swept.

Agent Discovery Timestamp Window
: When MCIC creates a new sweep it checks the discovery time of an Agent before it puts the Agent into the sweep. If the difference between the current time and last discovery time is more than *discovery window* minutes, MCIC assumes the Agent is offline and does not add the Agent to the sweep.

Minimum Input For Sweep
: The percentage of Agents that must be online before the sweep is started. This helps prevent starting Jobs that will be largely unsuccessful.

Max Search ResultsSets For Sweep
The maximum number of times the Job will be run, to pick up new and previously-failed Agents, before sweeping is stopped.

Sweep Timeout
The length of time an Agent can be unresponsive before it is dropped from the current pass of the Sweep.

Agent Failure Keywords
Comma-separated keywords used to search for agent failures.

Agent Setting Reviewed
When MCIC is first run, you are asked to check that the Deployed Agent Version is correct. If it is, this value is set to **yes** and the question is not asked again. You may manually set this to **no** if you want the question to be asked again.

Memory Limit
Sets the memory limit for MCIC.

Script Acquisition Duplicate Window
Limits how often a script audit result acquisition can be repeated.

Choose IP Host by Discovery Time
If set to **no**, MCIC fails to create a script acquisition when an IP address mistakenly maps to multiple hosts. If set to **yes**, the newest host is chosen.

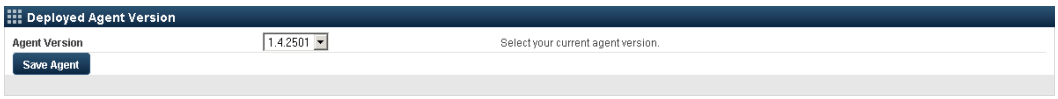
Script Acquisition Display Label
When provided a label name, restricts the display of scripts in the **Script Acquisition** window to those associated with the label. Leave blank to display all scripts.

Log CEF for all acquisitions
Enables CEF-compliant logging of acquisitions.

Log CEF for IOC hits
Enables CEF-compliant logging of IOC hits.

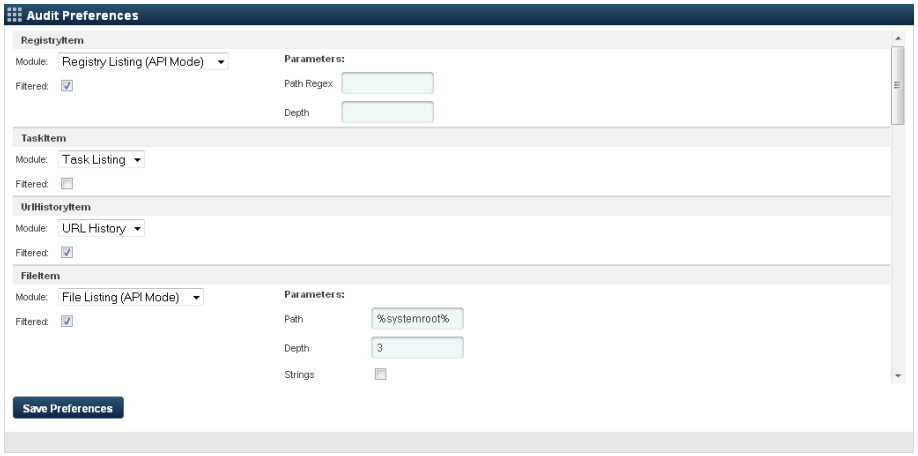
Background IOC hit search frequency
When greater than zero, MCIC automatically searches for IOC hits in all active sweeps every *setting value* minutes.

Index Audit Results
When enabled, all jobs and scripts will be configured to exclude audit results from Controller indexing.



In **Deployed Agent Version** you must pick the Agent version number applicable to your deployment.

Agent Version
Configures the script parameters sent to Agents. This value **must** match the version number of your deployed Agents.

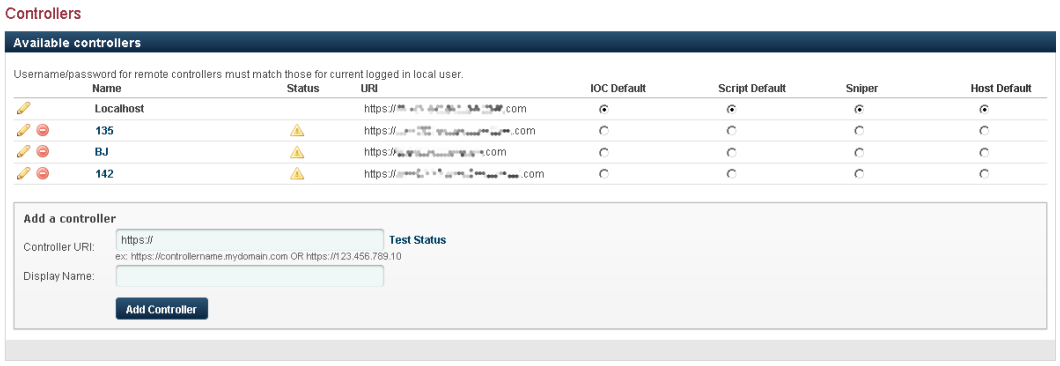


In **Audit Preferences** you can choose what type of audit you would like for each collection category, and define default settings for each. For example, if you would like MCIC to use the *Raw Mode* file listing by default, you can select that in the *FileItem* preferences. You can also set some default Audit Module parameters, such as depth in the *FileItem* audit. See the MIR *User Guide* for details.

Audit Preferences settings are used as a template when a script is built. During the script building process, you will always have a final opportunity to adjust parameters before running a new sweep.

11.1.2.2. Controllers

In multi-controller installations, it is common to use a separate Controllers for various controller tasks. MCIC supports this configuration through the **Controller Settings** window; we recommend using it when possible.



Configuring separate sweeper and sniper Controllers requires Single Discovery setup. See the MIR *Administration Guide* or contact MANDIANT technical support for assistance.

You may configure the following data sources:

IOC Default
: Identifies the Controller that will provide entries for the **IOC Source** selector when configuring a Sweep.

Script Default
Identifies the Controller that will provide entries for the **Script Name** selector when configuring a Sweep.

Sniper
Identifies the Controller that will provide acquisition services for Sweeps. This provides a single, centralized location for all acquired files.

Host Default
Identifies the Controller that will provide Labels and Saved Searches entries for the **Host Source** and **Excluded Hosts** selectors when configuring a Sweep.

You need to have the same credentials on each Controller: MCIC uses the same user name and password for each Controller you wish to access.

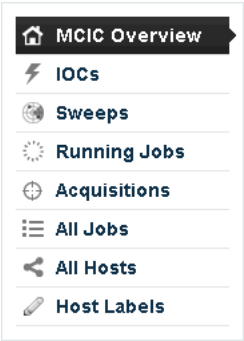
Choosing a new Controller *does not* transfer data to the new Controller. You may temporarily regain access to them by using the **Advanced Params** controls while configuring a Sweep.

11.2. The MCIC Dashboard

The visual appearance and functionality of the main MCIC pane varies depending on content, as selected by the controls in the **Navigation** pane or controls in the dashboard. Many table views provide **Toggle Columns** and **Show X Entries** controls above the table header, allowing you to customize the display of information. As well, many columns can be sorted by ascending or descending values, by clicking the column header. Controls for viewing the **First**, **Previous**, **Next**, and **Last** page are at the bottom right of the list.

11.3. The Navigation Pane

The **Navigation** pane, on the left, provides access to MCIC functionality.



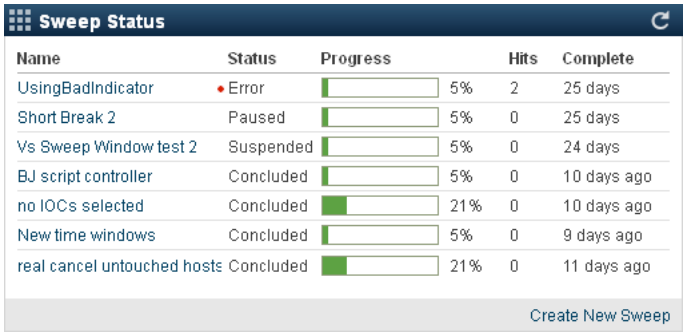
The following sections detail the choices available through the **Navigation** pane:

11.3.1. MCIC Overview

MCIC Overview provides information about the MIR Controller, its indexer, knowledge of Hosts and Jobs, MIR sub-processes, and other system information.

These views are automatically updated every five minutes. To refresh manually, click the **Refresh** button in a section title to fetch the latest Controller information for that section.

11.3.1.1. Sweep Status



The **Sweep Status** overview lists the top current sweeps. The information provided is a summary of the information that is provided on individual sweep pages, which are accessed through the **Sweeps** view in the **Navigation** pane or by clicking the Sweep name.

Information provided in this overview pane includes:

Name
The name of the sweep. Clicking the sweep name will take you to its details page. (Note: the displayed name is truncated at sixteen characters. You may wish to bear this in mind when naming sweeps.)

Status

Error
Attention required. Hover over the status message to see a description of the problem.

Scheduled
The sweep is not currently running, but will be later.

Suspended
The sweep is suspended because of a sweep window exclusion. It will start (subject to host availability) when the exclusion window time period has passed.

Running
Actively sweeping. Hover over the icon to see a description of its current job.

Paused
Sweep paused. Hover over the icon to see a description of its current job (a job can be running if it was started before the sweep was paused.)

Concluded
Sweep is finished and is no longer active.

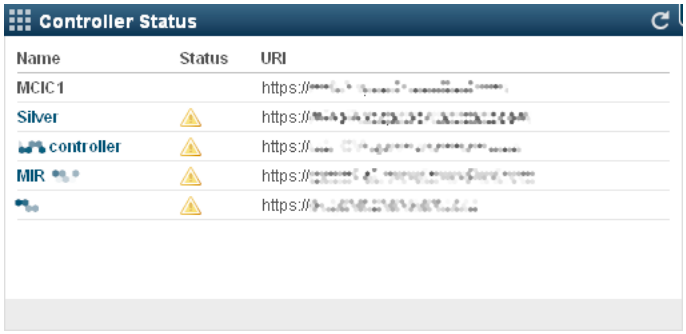
Progress
Shows a progress bar for the sweep. Hover over the bar to see percentages for completed and pending Hosts.

Hits
Shows the number of hits the sweep has reported. Available only if the **IOC Findings Report** on the **Sweeps** page has been generated and refreshed.

Complete
: Shows the time remaining until the sweep configuration expires; or, if the sweep configuration expired, the number of days or hours ago it expired.

At the bottom of the status area is a link titled **Create New Sweep**, which provides a shortcut to **Sweeps** → **Create New Sweep**.

11.3.1.2. Controller Status



The **Controller Status** overview provides a quick view of the status of the Controllers known to MCIC (added through **Settings** → **Controllers**.) It comprises:

Name
: The name of the Controller. Clicking the controller name will take you to its MCIC home page.

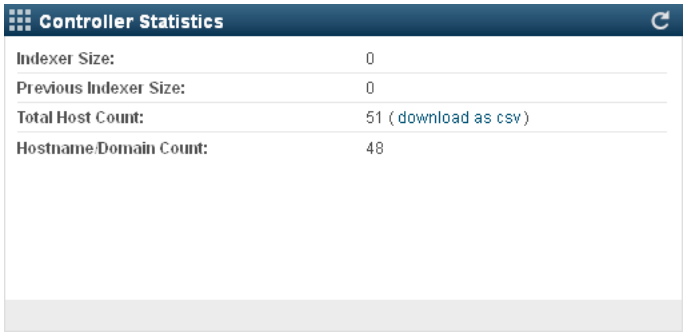
Status
: Shows one of two icons representing the status of the Controller:

Attention required. Hover over the icon to see a description of the problem.

Controller is okay and may be used for creating and running sweeps.

URI
: The address of the controller.

11.3.1.3. Controller Statistics

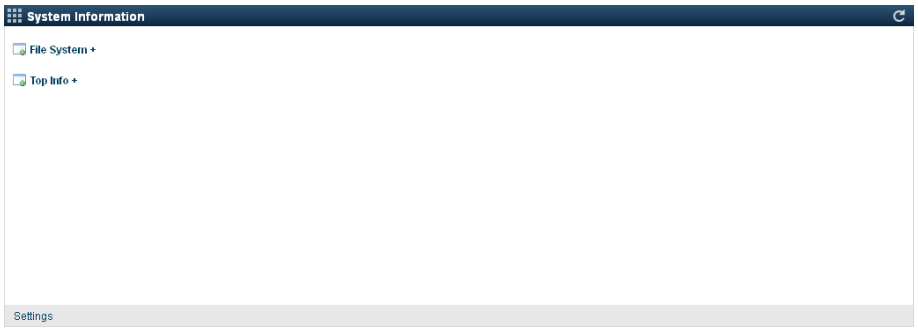


Controller Statistics provides information about the status of the Controller's indexing operations and known Hosts. The stats are automatically updated every few minutes to provide search and filter capability.

11.3.1.4. MIR Processes

The health of a Controller can be affected by runaway processes that are consuming memory, and by dead processes that have not yet been removed from memory. The **MIR Processes** overview monitors these conditions.

11.3.1.5. System Information



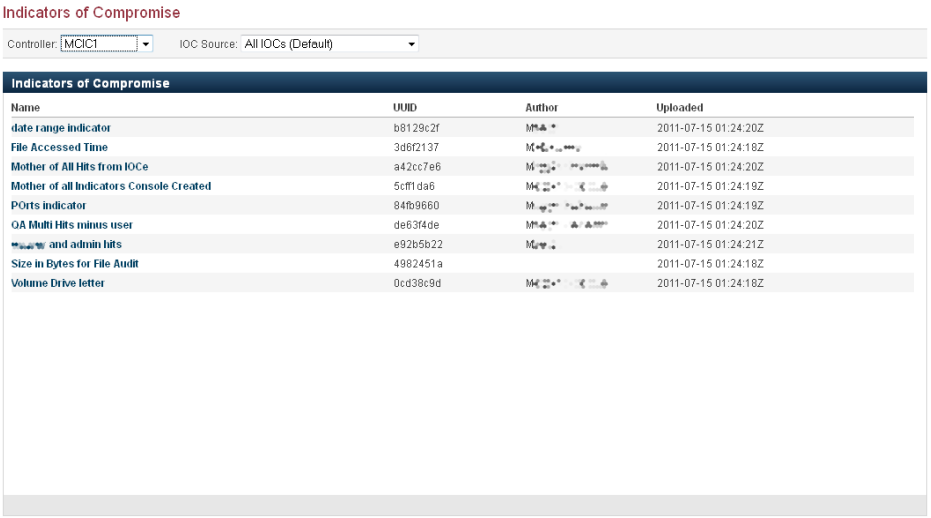
Additional troubleshooting information is available by expanding the entries in **System Information**:

File System
: Shows a list of open files on the MCIC workstation.

Top Info
: Lists the processes that are currently running on the workstation, in order of CPU utilization.

At the bottom of the status area is a link titled **Settings**, which provides a shortcut to **Settings** → **Global Settings**.

11.3.2. IOCs



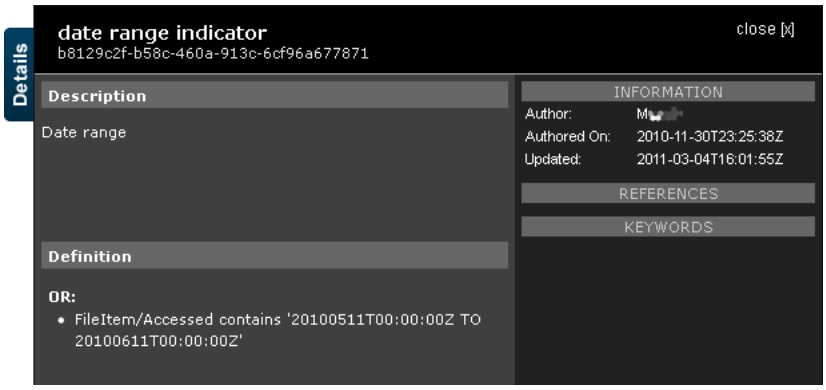
The **IOCs** view shows a list of known **Indicators of Compromise**. Clicking the name of an IOC displays a detailed view of the IOC; click the **Details** button at the left of the view to hide it.

The **Controller** and **IOC Source** selectors, at the top of the table, allow you to override the default Controllers used as sources for scripts and IOCs. You will need the same credentials on each Controller you wish to access.

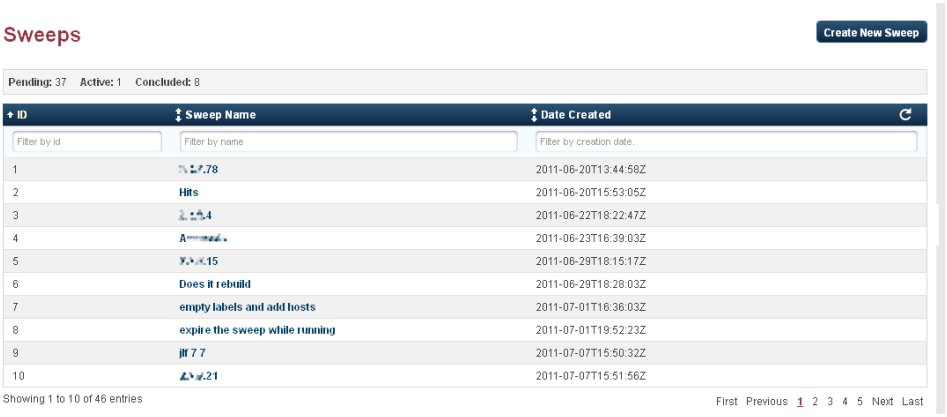
The list of IOCs is retrieved from the Controller's IOC Atom feed whenever MCIC needs to display it. This ensures the list is always up-to-date when you access it.

IOC management is performed using the MIR Console. Using the Console you can add, delete, and view IOCs.

The **Details** view provides a comprehensive overview of the IOC definition, the term that resulted in the IOC detecting a Hit, information about the Hit parameters, scheduling, etcetera. To help with direct investigation, you may click **launch acquisition** at the top of the **Details** pane. If MCIC can determine the correct file path, that information will be provided, otherwise you will need to provide the file path and file name to be acquired. You may choose API or RAW modes of retrieval.



11.3.3. Sweeps



The **Sweeps** view shows the most recent sweeps created in MCIC. Click a column header to sort the table using the column data; or type a term in the **Search** box and click **Filter** to reduce the list. Click the **Refresh** button to fetch the latest Controller information.

Clicking **Create New Sweep** will add a new entry to the Sweeps list. See *Section 13.1, "Creating a Sweep"*, below.

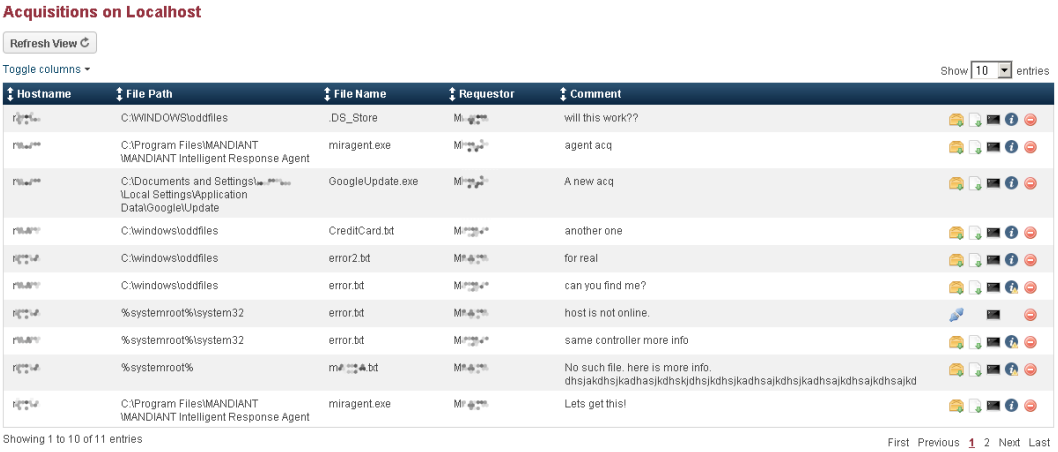
Clicking a sweep name will display its status page. See *Section 11.3.10, "Sweep Details"*, below.

11.3.4. Running Jobs

The **Running Jobs** view shows a listing of all Jobs running on the MIR Controller, including Jobs created by MCIC and Jobs created through the MIR Console. You can sort Jobs by type, author, title, created or modified date. You can filter the list using the case-sensitive Job titles filter box at the top of the list. Click on a Job title to display it using the MIR Console. You can also cancel a running Job by clicking its **Cancel** button in the **Action** column.

Cancelling a Job does not cancel the sweep.

11.3.5. Acquisitions



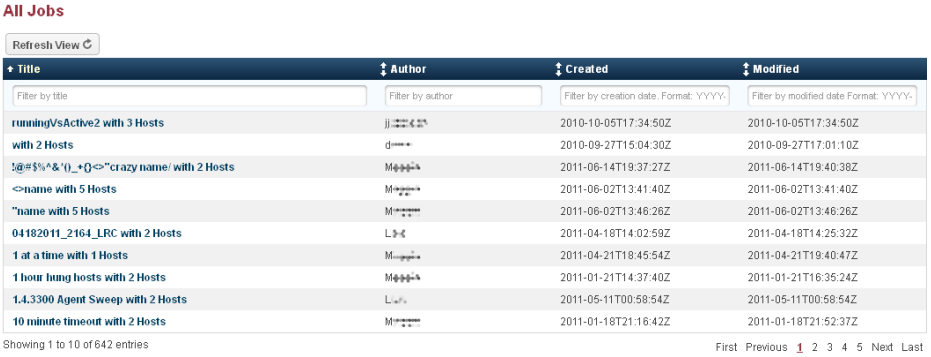
Acquisitions displays a list of files retrieved using **Acquisition** in the **All Hosts** window, or **launch acquisition** in an IOC **Details** pane.

To the right of each file entry are icons to download the package or file, view the messages generated while acquiring the file, view details, or remove the file from Controller storage. The package is password protected against accidental unprotected viewing (password: *Infected*), and contains an audit record and the requested file. In packages and for direct downloads, an underline is appended to the file extension of the acquired file to prevent accidental execution of the potentially infected file.

Acquired script entries are listed similarly. An “M” icon links to the audit result set. Optional columns are provided for **Script URI** and **Results Size** information.

Various types of acquisitions will present differing download and viewing options; specifically, options for downloading everything except the image file (which is often very large) are provided when appropriate.

11.3.6. All Jobs

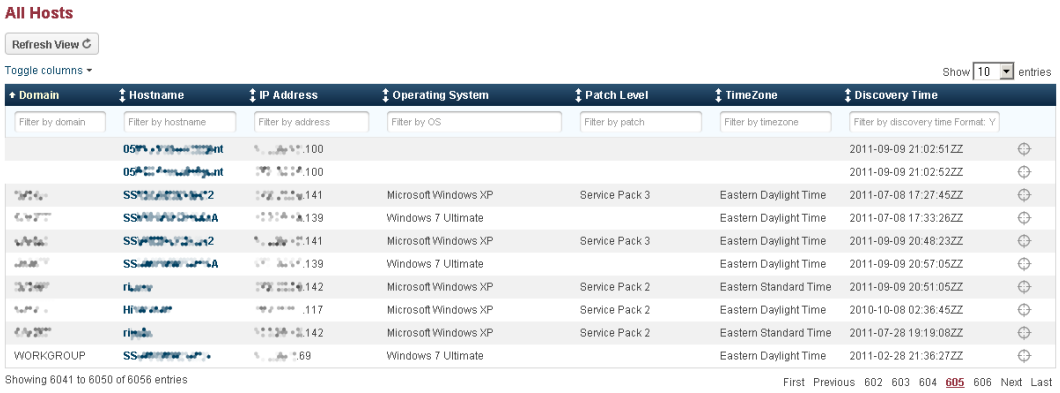


The **All Jobs** view shows a listing of all Jobs on the MIR Controller, including Jobs created by MCIC and Jobs created through the MIR Console. Click a column header to sort the table

using the column data. Type a search term in the **Filter** box to show only matching entries. Click the **Refresh View** button to fetch the latest Controller information.

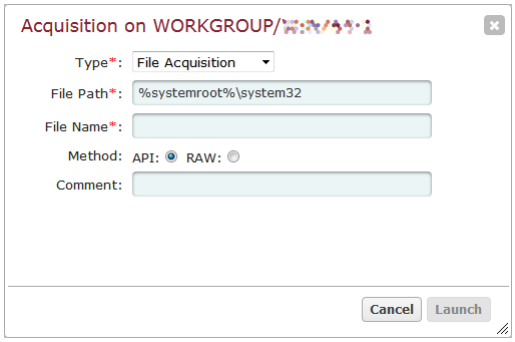
Clicking a Job title will start the MIR Console, showing you details for that Job.

11.3.7. All Hosts



The **All Hosts** view shows a list of known Hosts. Click a column header to sort the table using the column data; or type in a *search* box to filter the list. Click the **Refresh View** button to fetch the latest Controller information.

Clicking a Hostname will start the MIR Console, showing you details for that Host. Click the **Acquisition** icon at the right of the Host row to acquire files from that Host.



The **Acquisitions** form requires you to choose **File Acquisition** or **Script Acquisition**. The former retrieves the specified file from the host, storing it locally; the latter runs a saved host audit script on a single host. See *Section 11.3.5, "Acquisitions"* for details. Note that the script label used in filtering the list is configured in *Section 11.1.2.1, "Global Settings"*.

11.3.8. Host Labels

The **Host Labels** page is used to manage automatic Label rules on the local controller. These rules can be used to assign label names to groups of Hosts based on specific host properties. This enables you to include or exclude Hosts from sweeps automatically.

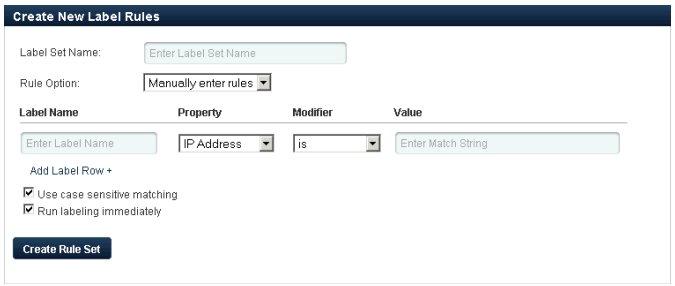
Host Labeling rules may be uploaded as a CSV file, or by manually creating rules using MCIC. It is important to note that rules cannot remove Labels from Hosts.

There are five properties that may be matched using one of several logic operators:

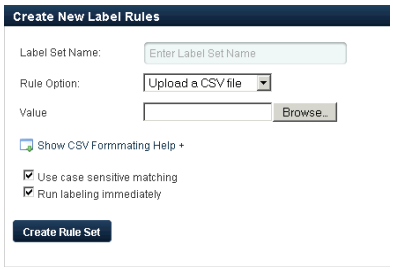
- IP Address
- Hostname
- Domain
- Agent Manager Certificate Hash
- Product (Operating System)

The top part of the **Host Labels** page lists the automatic Labels and provides information regarding their run status.

In **Create New Label Rules**, you may manually create new rules or choose to upload a CSV rules file by providing a **Label Set Name** and then selecting your choice from the **Rule Option** menu. The controls below the menu vary with the selected option.



When choosing **Manually Enter Rules**, a table-style list of controls is displayed. Each row comprises a **Label Name**, a Host **Property** and **Modifier**, and a match value. More rules can be appended by selecting **Add Label Row+**. Before creating the rule set, you may choose to **Use case sensitive matching** and to **Run labeling immediately** after creating the rule set. Finally, **Create Rule Set** will upload the manually-created automatic labeling rule set to the local Controller.

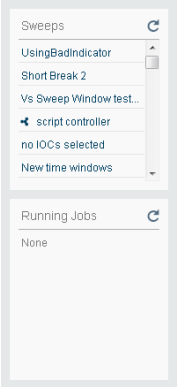


Upload a CSV file requires a path to the file; you can use **Browse** to use the standard file explorer to find the file. As with manual rule creation, you may choose to **Use case sensitive matching** and to **Run labeling immediately** after creating the rule set. **Create Rule Set** will upload the CSV rule set to the local Controller.

See *Section 13.4, "Automatic Host Labeling"* for further details.

11.3.9. Quick Lists

MCIC has two "quick lists" at the bottom of the **Navigation** pane: **Sweeps** and **Running Jobs**. These show sweeps and running Jobs, with the most recently created listed first. The names are clickable and will show the corresponding **Sweep Status** or **Running Job** view. Click the **Refresh** button in a list title to fetch the latest Controller information for that list.



11.3.10. Sweep Details

Clicking a Sweep name in the **Navigation** pane quick list, or in the **Sweeps** view, will open a detailed view of that sweep. The following information is displayed:

11.3.10.1. Sweep Controls

A small set of sweep controls is presented for convenience.

Pause pauses the sweep. The **Sweep Window Status** will change to **Paused**. Click **Activate** to start the sweep again.

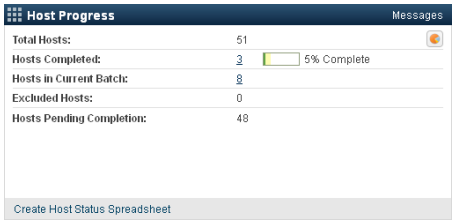
The **Refresh** button will update the information presented in the **Status** panes.

Configure brings up the **Sweep Configuration** window with the Sweep settings displayed. You may change the Sweep parameters to your satisfaction.

Delete deletes the stop the Sweep and remove it from MCIC.

Finally, **View Running Job** displays **Running Job Information** comprising various Job information and Job Stats, plus the option to **Cancel** the Job.

11.3.10.2. Host Progress



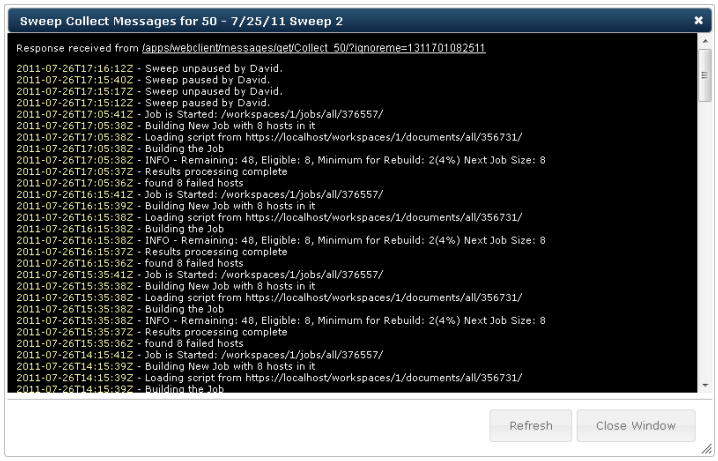
The **Host Progress** pane shows statistics regarding the selected Sweep.

Clicking the **Graph** icon shows a pie chart illustration of the same data.

Clicking the value displayed for **Hosts Completed** or **Hosts in Current Batch** will display a detailed view of corresponding Hosts.

Clicking **Create Host Status Spreadsheet** creates a Microsoft Excel-compatible host-by-host status spreadsheet. Click the **Refresh** button to update the sweep spreadsheet.

Clicking **Messages** displays a live view of Sweep activity: Jobs being built, informational messages about settings, Host counts, Job success and failure, etceteras. It is a good idea to periodically check the messages for each active sweep, to ensure progress is being made and that there are no error messages needing attention. The most recent messages are at the top.



11.3.10.3. IOC Findings Report

The **IOC Findings Reports** area shows the number of hits found in the sweep[1]. Click **Generate Report** to initialize a report. This process can take several minutes; when done, you will be presented with a list containing **Total Hits**, **New Hits**, and **IOC Hit History**.

[1] When **Index Audit Results** is enabled.

Click **Refresh** to run a full IOC search against all agents that have returned and indexed data.

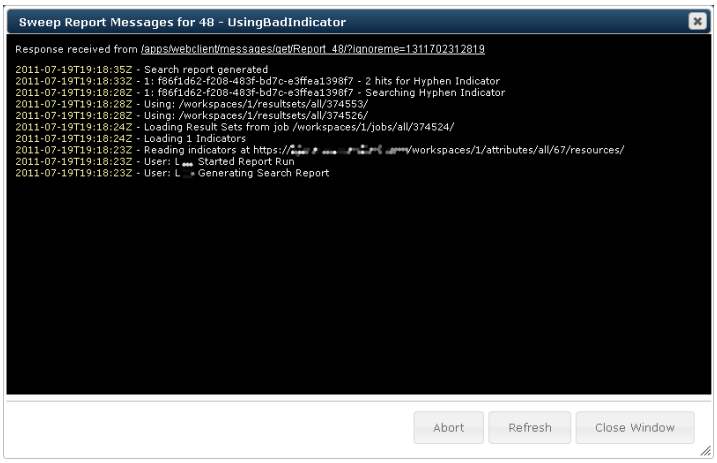
Click **Update** to run a search against the same data, but limited to those IOCs that are new or updated since the sweep was originally created; this helps reduce false positives as you improve your IOCs. (If no IOCs have changed, no report is generated.)

Clicking the **Graph** icon shows a pie chart illustration of the same data.

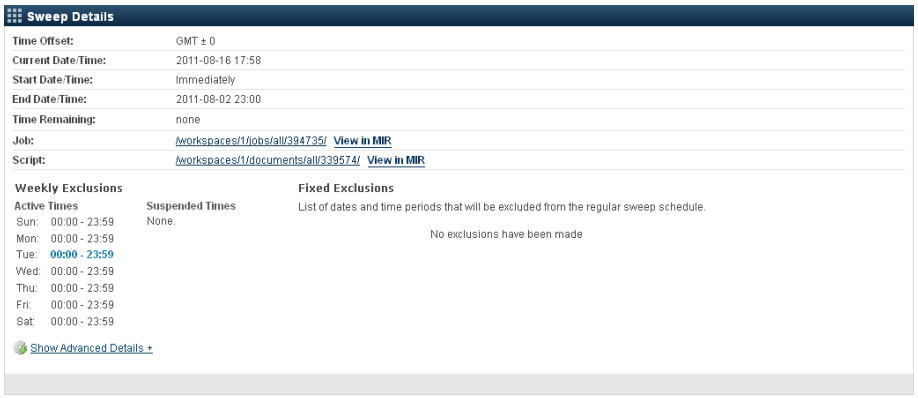
Click the hit count number to view hit details. See *Section 11.3.11, "Hit Details"*, below. Sweeps that are new since the last report was generated are available through **new hits found automatically**

Settings → **Global Sweep Settings** → **Background IOC hit search frequency** controls how often automatically-discovered hits are discovered and logged.

Clicking **Messages** displays a live view of search Report generation: the *ResultSet* names as they are searched, the Indicators being used, the number of hits, any errors encountered, etceteras. It is a good idea to periodically check the messages for each active sweep, to ensure progress is being made and that there are no error messages needing attention. The most recent messages are at the top.



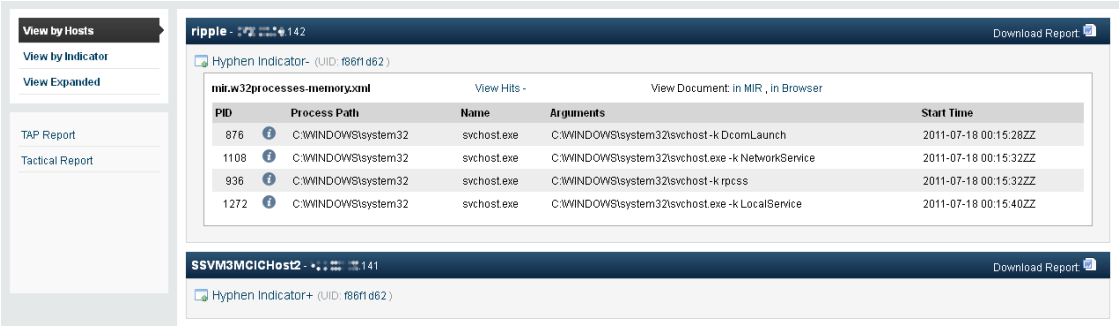
11.3.10.4. Sweep Details



The **Sweep Details** area shows information about the sweep. If a Sweep is running, clicking the **Job** or **Script URI** will display its raw XML data; clicking **View in MIR** to open this data in the MIR Console.

Clicking **Show Advanced Details** displays relevant detailed information about the Sweep. Clicking links will display an RSS feed or raw XML data.

11.3.11. Hit Details



After initializing a report by clicking **Generate Report**, click on the **Total Hits** or an **IOC Hit History** value to see a hits report. A new **Search Hits** window will be opened, listing the hits for that Sweep.

Hovering over the Host name will display Host information.

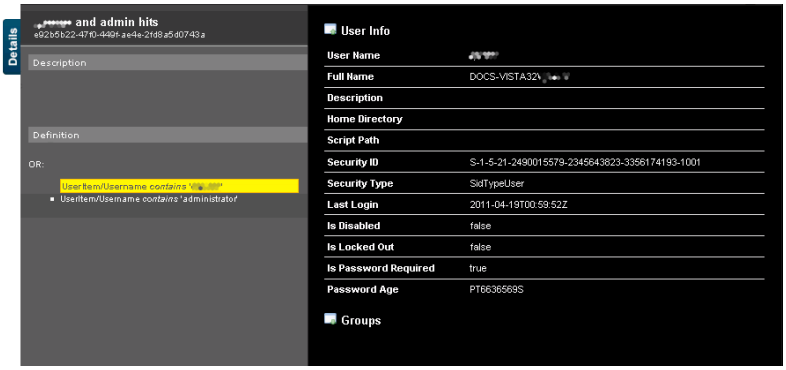
Clicking the Sweep name will expand a list of Audits resulting in Hits. Click **View Hits** to see the items that made a Hit.

In the **Navigation** pane on the left, you can choose the type of view shown on the right. **View by Hosts** groups the hits by their Host, and then by indicator; **View by Indicator** groups them by Indicator, and then by host. **View Expanded** groups by Host and expands the detail view of each hit.

Clicking the Indicator **UID** opens the **Details** pane, showing the definition and other information about the indicator that was used in generating the hits listed below it.

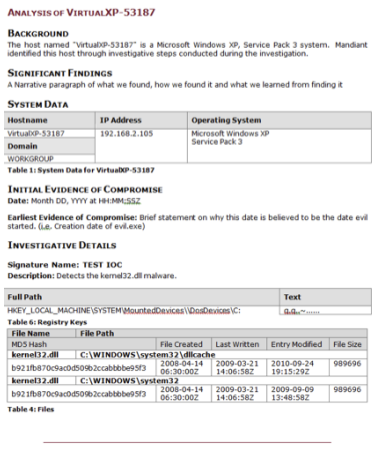
Clicking the Host name opens the MIR Console.

To find out which IOC term was matched to create the Hit, click the Hit's **indicator** button. The **Details** pane will be opened and the corresponding IOC matching term highlighted, with details for that hit listed to the right.



11.3.11.1. IOC Hit Reports

A full report can be generated in Microsoft Word format by clicking **TAP Report** or **Tactical Report** in the **Navigation** pane. An example report is shown below and can be used as a shell to document further details and findings for each Host.



ANALYSIS OF VIRTUALXP-53187

BACKGROUND

The host named "VirtualXP-53187" is a Microsoft Windows XP, Service Pack 3 system. Mandiant identified this host through investigative steps conducted during the investigation.

SIGNIFICANT FINDINGS

A Narrative paragraph of what we found, how we found it and what we learned from finding it

SYSTEM DATA

Hostname	IP Address	Operating System
VirtualXP-53187	192.168.2.105	Microsoft Windows XP Service Pack 3
Domain		
WORKGROUP		

Table 1: System Data for VirtualXP-53187

INITIAL EVIDENCE OF COMPROMISE

Date: Month DD, YYYY at HH:MM:SSZ

Earliest Evidence of Compromise: Brief statement on why this date is believed to be the date evil started. (i.e. Creation date of evil.exe)

INVESTIGATIVE DETAILS

Signature Name: TEST IOC

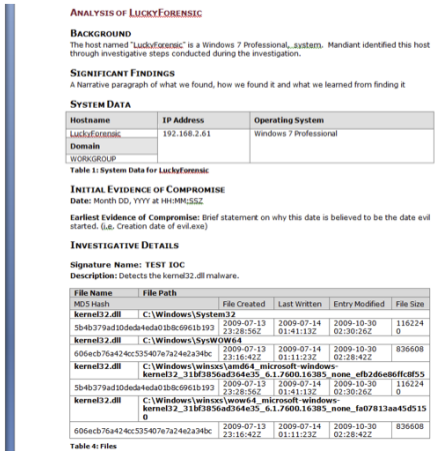
Description: Detects the kernel32.dll malware.

Full Path	Text
HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices\\DosDevices\C:	.....

Table 6: Registry Keys

File Name	File Path				
MD5 Hash		File Created	Last Written	Entry Modified	File Size
kernel32.dll	**C:\WINDOWS\system32\dllcache**				
b921fb870c9ac0d509b2ccabbbbe95f3		2008-04-14 06:30:00Z	2009-03-21 14:06:58Z	2010-09-24 19:15:29Z	989696
kernel32.dll	**C:\WINDOWS\system32**				
b921fb870c9ac0d509b2ccabbbbe95f3		2008-04-14 06:30:00Z	2009-03-21 14:06:58Z	2009-09-09 13:48:58Z	989696

Table 4: Files



ANALYSIS OF LUCKYFORENSIC

BACKGROUND

The host named "LuckyForensic" is a Windows 7 Professional, system. Mandiant identified this host through investigative steps conducted during the investigation.

SIGNIFICANT FINDINGS

A Narrative paragraph of what we found, how we found it and what we learned from finding it

SYSTEM DATA

Hostname	IP Address	Operating System
LuckyForensic	192.168.2.61	Windows 7 Professional
Domain		
WORKGROUP		

Table 1: System Data for LuckyForensic

INITIAL EVIDENCE OF COMPROMISE

Date: Month DD, YYYY at HH:MM:SSZ

Earliest Evidence of Compromise: Brief statement on why this date is believed to be the date evil started. (i.e. Creation date of evil.exe)

INVESTIGATIVE DETAILS

Signature Name: TEST IOC

Description: Detects the kernel32.dll malware.

File Name	File Path				
MD5 Hash		File Created	Last Written	Entry Modified	File Size
kernel32.dll	**C:\Windows\System32**				
5b4b379ad10deda4eda01b8c6961b193		2009-07-13 23:28:56Z	2009-07-14 01:41:13Z	2009-10-30 02:30:26Z	116224 0
kernel32.dll	**C:\Windows\SysWOW64**				
606ecb76a424cc535407e7a24e2a34bc		2009-07-13 23:16:42Z	2009-07-14 01:11:23Z	2009-10-30 02:28:42Z	836608
kernel32.dll	**C:\Windows\winsxs\amd64_microsoft-windows-kernel32_31bf3856ad364e35_6.1.7600.16385_none_efb2d6e86ffc8f55**				
5b4b379ad10deda4eda01b8c6961b193		2009-07-13 23:28:56Z	2009-07-14 01:41:13Z	2009-10-30 02:30:26Z	116224 0
kernel32.dll	**C:\Windows\winsxs\wow64_microsoft-windows-kernel32_31bf3856ad364e35_6.1.7600.16385_none_fa07813aa45d5150**				
606ecb76a424cc535407e7a24e2a34bc		2009-07-13 23:16:42Z	2009-07-14 01:11:23Z	2009-10-30 02:28:42Z	836608

Table 4: Files

Chapter 12
URL Direct Access

MIR supports HTTPS access to various MCIC pages and a limited set of commands.

Menu Items

Access menu items directly by URL by polling:

```
https://controllername/apps/webclient \
  /direct?target=iocs
  /direct?target=sweeps
  /direct?target=runningjobs
  /direct?target=acquisitions
  /direct?target=jobs
  /direct?target=hosts
```

View Acquisition Special Command

To filter the acquisitions list by a specific field, use:

```
https://controllername/apps/webclient
  /direct?target=acquisitions&input=[FIELDNAME]&id=[VALUE]
```

where `[FIELDNAME]` is the name (lowercase and underscored) of the field to filter by and `[VALUE]` is the filter value.

View Sweep Special Command

To go right to the sweep details for a specific sweep, use

```
https://controllername/apps/webclient
  /direct?target=sweeps&input=[SWEEPID]
```

where `[SWEEPID]` is the numeric id of the sweep.

Creating an Acquisition Special Command

To go straight to the acquisition creation menu, use

```
https://controllername/apps/webclient
  /direct?target=hosts&input=[IPADDRESS]&id=[ID]
```

where `[IPADDRESS]` is the ip address of the target host and `[ID]` is the external ID with which to associate this acquisition.

Accessing IOC Hit Details

To access the hit review for a specific IOC hit on a sweep, use

```
/sweep/xmlReport/[SWEEPID]/true/?filter=hit_hash,%3D,[HITHASH]
```

where `[SWEEPID]` is the numeric id of the sweep and `[HITHASH]` is the unique hash value of the hit.

Chapter 13
Sweeping with MCIC

13.1. Creating a Sweep

Before creating a new sweep, you need to have loaded your IOCs. If you do not intend to sweep all Hosts, you need to create and assigned Labels or a Saved Search that identifies those Hosts that will be included (or excluded).

To create a new sweep:

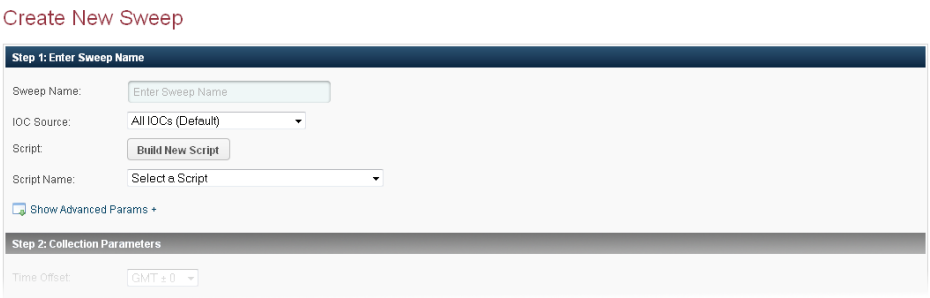
1. Browse to MCIC at *https://Controller* URI\ or\ Hostname/apps/webclient/

   Log in with your usual MIR Console credentials.

2. In the **Navigation** pane, select **Sweeps**, then click **Create New Sweep**

   OR

   In the **MCIC Overview** main window, in the **Sweep Status** pane, click **Create New Sweep**.



3. In **Step 1: Enter Sweep Name**

   - Provide a **Sweep Name**.
   - From **IOC Source** select a set of Indicators of Compromise (these sets are configured in MIR Console with Labels.)
   - Either

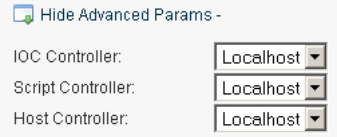
     a. Click **Build New Script**. See *Section 13.2, "Using Build New Script"*, below, for details.

     OR

     b. Choose a script in **Select a Script**. In this case, you will need to manually select the appropriate IOCs in **Step 3: Reporting Parameters**.

   Note that all MIR users can see the name you provide for the sweep and its script.

Advanced Parameters



Clicking **Show Advanced Params** + displays selectors:

- **IOC Controller** selects a Controller from which to source IOCs.
- **Script Controller** selects a Controller from which to source Scripts.
- **Host Controller** selects a Controller from which to source Labels and Saved searches, used to filter Hosts.

Controllers are added through **Settings** → **Controllers**.

4. In **Step 2: Collection Parameters**

- Set the **Time Offset**. The **Current Date/Time** value will be updated, and should match local time.
- The sweep is automatically set to begin immediately after saving. If you wish to delay the sweep start, click **Set Custom Date/Time**.
- Set the sweep **End Date/Time**. The **Sweep Duration** value will be updated to display the time span in days.
- From **Host Source** choose **All Hosts**, a *Console Label*, or a *Saved Search* identifying those Agents that are to be swept.
- From **Excluded Hosts** choose **None**, a *Console Label*, or a *Saved Search* identifying those Agents that are not to be swept

The *Host Source* and *Excluded Hosts* labels and searches lists are processed at the time the sweep is built or rebuilt. This ensures the sweep is using the most up-to-date Controller data.

The results of these queries are added to the sweep's previously-acquired host source and excluded host lists. It is important to understand that hosts are never removed from the sweep's host source or excluded host lists during the life of the sweep.

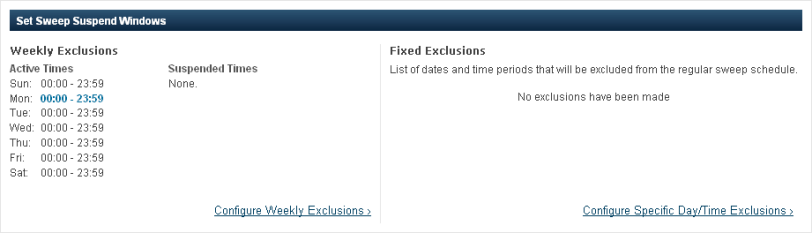
In other words, once included or excluded from a sweep, a host will remain in that state for the remainder of the sweep. To effect an immediate change, the sweep must be reconfigured and rebuilt.

Note that using MIR Console to remove a Label from a Host will not remove it from MCIC.

Sweep Windows

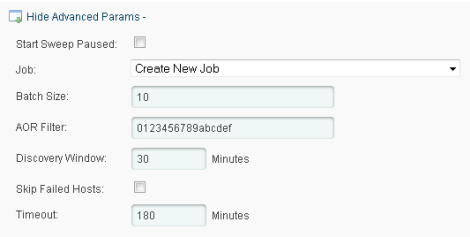
Sweep windows allow you to configure a time schedule for weekly sweep periods, and to insert one-off exclusion times. This flexibility allows you to design your sweep to run during periods Hosts will be online but unused, at minimum inconvenience to Host and network users. Note that under **Active Times**, the current time window is emphasized in bold text.

See *Section 13.1.1, "Configuring Weekly Sweeps"* and *Section 13.1.2, "Configuring One-shot Exclusions"* for details.



Advanced Parameters

Advanced parameters allow you to fine-tune sweep details:



Clicking **Show Advanced Params +** displays more controls:

Start Sweep Paused

If this option is selected when creating a new sweep, the sweep will be created but will not be activated. If it is selected while the sweep is running, the sweep will halt after its current action.

Job

Manually selects the MIR Job that will run by the sweep.

Batch Size

Limits the number of Hosts that MCIC will put into a single Job. A Job is a group of Hosts that are submitted to the MIR Controller to check for IOCs. If a Controller or network has performance issues you may want to lower this number.

AOR Filter

(Agents of Responsibility) A list of hexadecimal digits used by Controllers to filter the Agents with which they will communicate. Since all Agents have a unique certificate hash, you can use the first letter of that hash to assign the Agent to a specific Controller.

Discovery Window
When MCIC creates a new sweep it checks the discovery time of a Host before it puts the Host into the sweep. If the difference between the current time and last discovery time is more than *discoveryWindow* minutes, MCIC assumes the Host is offline and does not add the Host to the sweep.

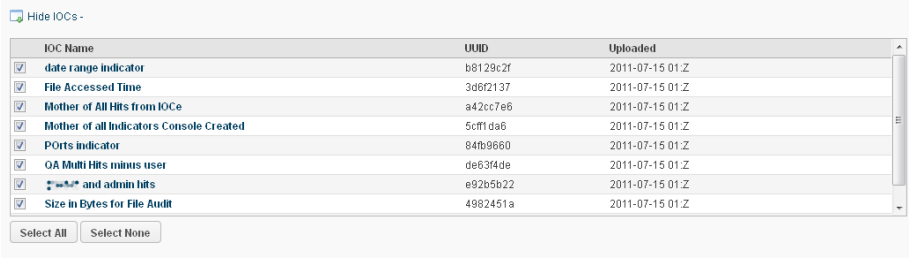
Skip Failed Hosts
When selected, MCIC will skip those Hosts that were assumed hung during the last sweep. When clean, hung Hosts are recycled into the next Sweep.

Timeout
Sweep timeout in minutes. The timer is reset whenever a new Host is acquired. When the timer expires, Hosts remaining in the sweep queue are assumed hung. MCIC will end the sweep and begin the process of building a new job.

Index Audit Results
Controls indexing of audit result documents. Note that IOC Finding Reports are not available when indexing is disabled.

5. In **Step 3: Reporting Parameters**

   - **If** you wish to restrict the IOCs used in the sweep, click **Show IOCs** and select your desired IOCs.



   - Otherwise, the IOCs used to build the script will be automatically and inclusively selected.

6. Click Save Sweep.

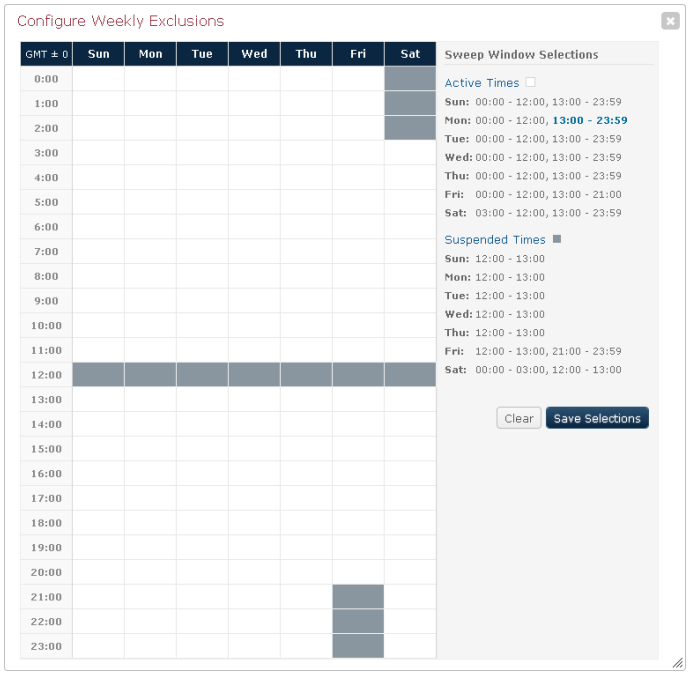
13.1.1. Configuring Weekly Sweeps

A weekly sweep schedule, with valid sweep and no-sweep times may be configured with a one-hour time resolution.

1. Click **Configure Weekly Sweep Selections** to display a weekday/time calendar interface. Grid cells with a white background show a valid sweep time; sweeps are prevented from running during those time cells with a colored background.

2. Click or drag cells to toggle their status. The sweep window time spans listed to the right will be automatically updated.

3. Click **Save Selections** when the weekly schedule has been configured. Click **Clear** or the **Close Window** button to cancel all changes.



13.1.2. Configuring One-shot Exclusions

The weekly schedule may be refined for one-time exclusion events, without affecting the regular schedule. These events will happen on specific dates and times and have a one-hour time resolution.

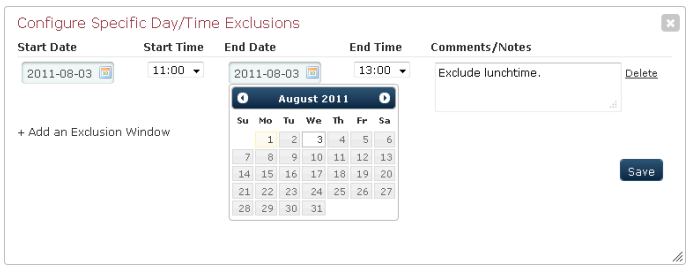
1. Click **Configure Specific Day/Time Exclusions**.

2. Using the calendar and time controls, specify the exclusion **Start Date**, **Start Time**, **End Date**, and **End Time**. During this period the sweep will not be allowed to run.

3. Provide a useful description in **Comments/Notes** so that others will understand why the sweep pattern is interrupted.

4. To add another exclusion period click **Add an Exclusion Window**. To remove an exclusion, click **Delete** to its right.

5. Click **Save** when the weekly schedule has been configured. Click the **Close Window** button to cancel all changes.



13.2. Using Build New Script

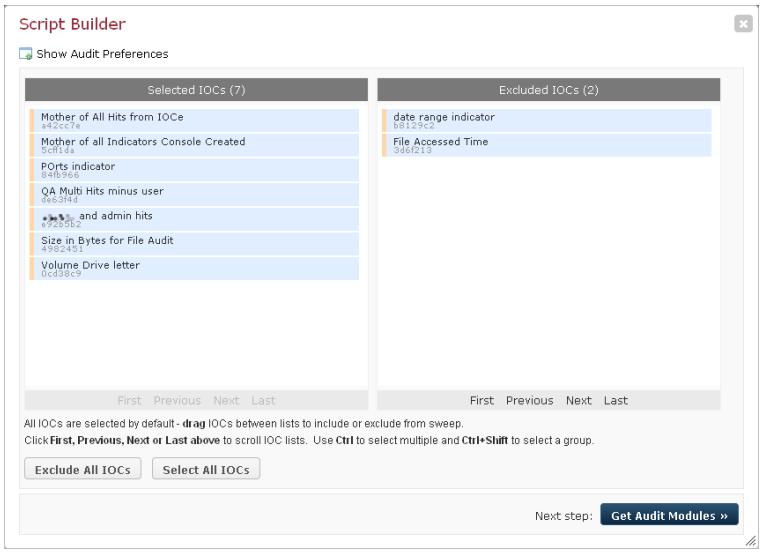
While creating a new sweep, you will have the opportunity to pick an existing script, or to build a new script.

To build a new script:

1. In the **Navigation** pane, select **Sweeps** and then click **Create New Sweep**. On the **Create New Sweep** main page, click **Build New Script**.

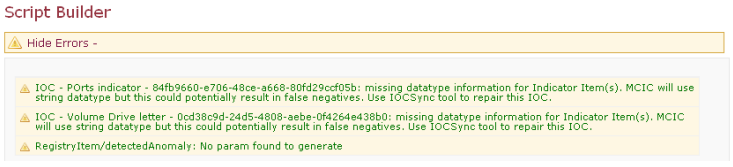
2. Drag and drop IOCs between the **Selected IOCs** and **Excluded IOCs** panes.

   Note that you can click **Show Audit Preferences** to adjust your settings without going through the **Settings** → **Global Settings** menu.



3. Click **Get Audit Modules**. The script builder will analyze the list of **Selected IOCs** and determine which Audit Modules are needed.

   Sometimes Script Builder may be unable to determine the correct Audit Module or parameter. Click **Show Errors** at the top left and use its feedback in troubleshooting.

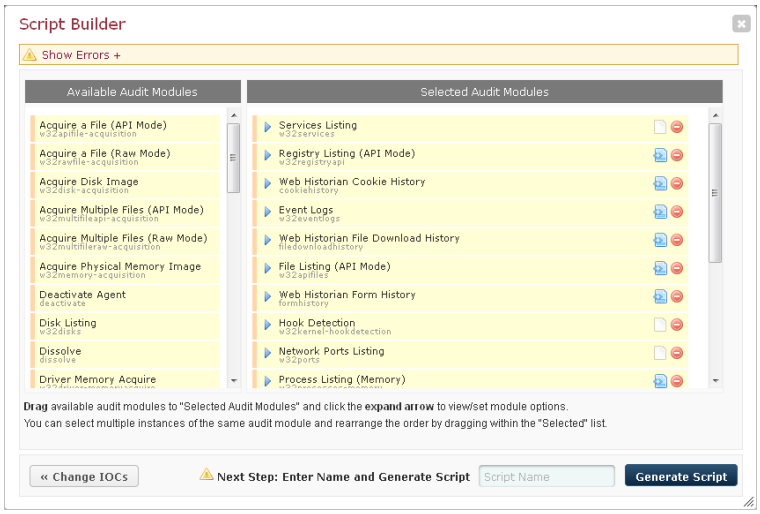


   There are four main causes of errors in Script Builder:

   - A bad IOC containing an invalid term.
   - MCIC cannot determine which Audit Module was suitable for an IOC.

- MCIC cannot determine which Audit parameter was needed to detect a specific part of an IOC.
- An incorrect Agent version was set in **Settings** → **Global Settings**. In any of these cases, you can either choose to ignore the warnings (which may cause you to miss finding an IOC) or manually determine and implement the appropriate fix. MANDIANT encourages users of MCIC to report any Script Builder errors so that we may troubleshoot and fix the issue for future versions of MCIC.

4. Drag and drop Audit Modules between the **Available Audit Modules** and **Selected Audit Modules** panes. This step is required when the script builder has not been able to determine the correct Audit Modules.



5. Click the **Expand** arrow of an Audit Module to adjust its parameters.

   Click the or **Filter** icon of an Audit Module to add or modify its XPath filter settings.

6. Click the **Delete** icon of an Audit Module to remove an Audit Module from the script.
7. Provide a **Script Name**. We suggest using the sweep name.
8. Click **Generate Script**. Remember to also **Save Sweep** in the **New Sweeps** window if you were configuring a new sweep.

13.3. Running Sweeps

Sweeping is the process of searching for data across a network of Hosts. Most of the time sweeps will be run:

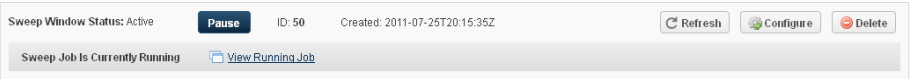
- immediately after creation, by default.
- at the time specified by clicking **Set Custom Date/Time**.
- during the time periods configured by sweep windows.

If you want to run sweeps manually, click the sweep name in any view that shows it (the **MCIC Overview** view provides a **Sweep Status** overview of the top current sweeps; the

Sweeps view lists all sweeps; the **Sweeps** quicklist provides a list of the most-recently viewed sweeps.)

Selecting a sweep will display its details view, described in *Section 11.3.10, "Sweep Details"*. At the top of the view are controls to **Activate** or **Pause** the sweep, to **Configure** its settings as described in *Section 13.1, "Creating a Sweep"*, to **Refresh** the detailed information, and to **Delete** the sweep.

You will most often use these controls while developing a new sweep, by running a limited sweep, checking results, and fine-tuning its configuration. Clicking **View Running Job** displays **Running Job Information** comprising various Job information and Job Stats, plus the option to **Cancel** the Job.



13.4. Automatic Host Labeling

For environments where simple Host properties can determine whether a given Host belongs in a Sweep, automatic Host Labeling can be used to assign a Label to those hosts. The label can serve to determine whether that group of hosts should be swept.

Automatic labeling rules can be generated manually using MCIC or provided using a CSV list.

Automatic host labeling is strictly additive: the rules can only *assign* a Label to a Host. There is no facility to automatically remove a Label from a Host. See *Section 13.4.3, "Updating Automatic Label Rules"* for a manual work-around.

13.4.1. Creating Labeling Rules Manually

MCIC provides a simple rules creation tool. Note that once created, MCIC can not change the rules, and any applied labels will require manual removal through the MIR console.

1. In the **Navigation** pane, select the **Host Labels** view.

2. In **Create New Label Rules**, provide a **Label Set Name**. For **Rule Option**, ensure **Manually enter rules** is selected.

3. In the table below these controls, configure a rule:

   Label Name
   The Label that will be associated with every Host that matches this rule. This name can be up to 32 characters. The comma character cannot be part of a label name.

   Property
   The Host property that will be compared to the rule's match string. You may select one of five properties: **IP Address**, **Hostname**, **Domain**, **AM Cert Hash** [1], and **Product** [2].

[1] Agent Manager Certificate Hash
[2] Operating System

Modifier
The comparison operator for the rule. You may choose **is**, **is not**, **contains**, **not contains**, **regex match**, or **CIDR**.

The **CIDR** modifier is useful only when matching **IP Address** properties.

Value
The match value that will be compared to the selected Host property. This may be a string, Perl regular expression, or CIDR expression. Commas are allowed in the value string.

4. Add additional rows to the table using **Add Label Row**. Note that **Label Name**s may be repeated, allowing one label to identify hosts that match any of several properties.

5. Choose whether the rules will **Use case sensitive matching**. You may also choose to **Run labeling immediately** when the rule set is created.

6. Click **Create Rule Set** to upload the labeling rules to the local controller.

The rule set is sent to the local Controller. When the rule set is run, any host that matches any rule in the set will be assigned the applicable label. These labels and their associated hosts may then be used for controlling which machines take part in a given sweep.

If errors are detected in the rules, error messages will be displayed and the rule set will not be uploaded to the Controller.

13.4.2. Uploading CSV Labeling Rules

Labeling rules can be configured using a four-field CSV table. The four fields correspond to those used in the MCIC manual interface:

Field 1
The Label name. Up to 32 ASCII characters. The comma character can not be used.

Field 2
The Host property. Valid values: **ip**, **hostname**, **domain**, **amcerthash**, **product**. This field is not case sensitive.

Field 3
The modifier. Values: **is**, **isnot**, **contains**, **containsnots**, **regex**, **cidr**. This field is not case sensitive.

Field 4
The value. This may be a string, Perl regular expression, or CIDR expression.

To upload a CSV Labeling Rules file:

1. In the **Navigation** pane, select the **Host Labels** view.

2. In **Create New Label Rules**, provide a **Label Set Name**. For **Rule Option**, ensure **Upload a CSV file** is selected.

3. Use the **Browse** button to find the CSV file using a standard file explorer window.

4. Choose whether the rules will **Use case sensitive matching**. You may also choose to **Run labeling immediately** when the rule set is created.

5. Click **Create Rule Set** to upload the labeling rules to the local controller.

If a fatal error occurs, a message will be displayed and the label set will not be created. If non-fatal errors occur, the label set will be created, and error messages will be displayed.

13.4.3. Updating Automatic Label Rules

Label Sets cannot be changed after creation. Labels cannot be automatically removed from Hosts. To perform a rules update:

1. Export the rule set as a CSV file.

2. Modify the CSV file.

3. Delete the old rule set and the old labels.

4. Upload the new CSV file.

5. Run the labelling rule set.

13.5. Sniping (Acquisitions)

Sniping is the process of acquiring targeted information from a specific Host. The Acquisitions function in MCIC allows you to request files from Hosts, and manages the process of retrieving, storing, and indexing those files without further intervention.

MCIC also supports REST API operations to create, update, and delete both types of acquisition. The target host can be identified directly by its MIR Agent certificate hash, or indirectly by its IP address.

Acquired files are listed in the **Acquisitions** view, selected in the **Navigation** pane. Each row lists an acquisition request, its status, and provides links for downloading or deleting the files. See *Section 11.3.5, "Acquisitions"* for details.

File acquisitions can be initiated in two ways:

13.5.1. From an IOC Hit Report

IOCs are often caused by malware. A common next step in investigating a confirmed IOC hit is to acquire the file for further analysis. To do this:

1. Expand the view of the hit.

2. Click the **I**nformation icon to open the **Details** pane.

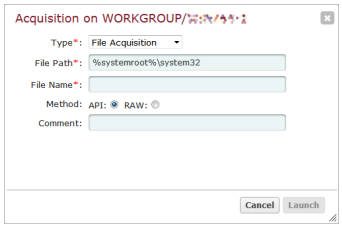
3. Highlight the path and/or name of the file you wish to acquire.

4. Click **launch acquisition**, found near the top of the details view.

5. An **Acquisition** form will be shown. By default, MCIC assumes you wish to capture a **File**. In **Type**, you may select **Script** to run a script on the host and retrieve the audited data.

6. When capturing a **File**:

   a. If you selected a file in the **Details** pane, the **File Path** and **File Name** will be pre-filled with the appropriate data. If you select only the file name, the path will default to `%systemroot%/system32`. If you did not select a file name, you will need to provide both the path and file name. You may use the standard Windows environment variables when describing the path.



   b. Choose the acquisition method: **Raw** or **API**. API is faster and more reliable, but RAW can access files hidden by rootkits.

   c. Optionally, add a comment describing the acquisition. This will be displayed in the Acquisitions view, helping you to locate the file in the future.

   d. Click **Launch**. The file will be acquired when the Host is available. The acquired file will be stored on the Controller that has been designated “Sniper”.

7. When capturing a **Script**:

   a. The **Script Controller** will be filled with your MCIC default. In **Script URI**, select the script to be run on the host. You may provide a comment for inclusion with the retrieved data.

      Only scripts labeled **.favorite** are offered as choices (a different label can be set in **Settings** → **Global Sweep Settings** → **Script Acquisition Display Label**). You may provide text which will be visible in the **External ID** column in the acquisitions list.

   b. Click **Launch**. The script will be run on the host and will generate audit data. The acquired data will be stored on the "Sniper" controller.

13.5.2. From the All Hosts view

To acquire a file not associated with an IOC hit:

1. In the **All Hosts** view, locate the Host that has the file you wish to acquire.

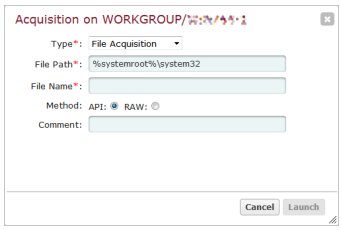
2. Click the **Acquisition** icon to the right of a Host entry.

3. An **Acquisition** form will be shown. By default, MCIC assumes you wish to capture a **File**. In **Type**, you may select **Script** to run a script on the host and retrieve the audited data.

4. When capturing a **File**:

   a. If you selected a file in the **Details** pane, the **File Path** and **File Name** will be pre-filled with the appropriate data. If you select only the file name, the path will default to

`%systemroot%/system32`. If you did not select a file name, you will need to provide both the path and file name. You may use the standard Windows environment variables when describing the path.



b. Choose the acquisition method: **Raw** or **API**. API is faster and more reliable, but RAW can access files hidden by rootkits.

c. Optionally, add a comment describing the acquisition. This will be displayed in the Acquisitions view, helping you to locate the file in the future.

d. Click **Launch**. The file will be acquired when the Host is available. The acquired file will be stored on the Controller that has been designated “Sniper”.

5. When capturing a **Script**:

a. The **Script Controller** will be filled with your MCIC default. In **Script URI**, select the script to be run on the host. You may provide a comment for inclusion with the retrieved data.

Only scripts labeled **.favorite** are offered as choices (a different label can be set in **Settings** → **Global Sweep Settings** → **Script Acquisition Display Label**). You may provide text which will be visible in the **External ID** column in the acquisitions list.

b. Click **Launch**. The script will be run on the host and will generate audit data. The acquired data will be stored on the "Sniper" controller.

Chapter 14
MCIC Remote Access

To simplify secure remote access of MCIC features, MIR includes a controller update that introduces a new “MIR Remote” web service. This service monitors the url

`https://controllername/remote/*`

The MIR web service accepts only requests from MIR users in the RemoteOnly controller group. These users:

- Cannot access any other MIR resources including the Admin UI and whole REST API.
- Must have a password of minimal length (by default 8 characters, but configurable in the Admin UI).
- Cannot access the MCIC UI or any direct MCIC URL.
- Can only access select MCIC functions through the remote service:
- Current version information (`/sys/version/`).
- Create acquisition POST URL (`/acquisitions/create`)

The Remote web service authenticates the user, then relays the request to MCIC. For instance, to get the current MCIC version:

`GET` *`https://controllername/remote/apps/webclient/sys/version`*

Or to create a new acquisition:

`POST` *`https://controllername/remote/apps/webclient/acquisition/create`*

Since the original username and password of the RemoteOnly user are not known by MCIC, all actions done through the remote web service are attributed to “Remote User” in the MCIC UI.

MIR administrators can restrict access to the remote web service through IP Address filtering (in the Admin Console, select **Application** → **ConfigFiles** → **Remote Web Service** → **IP Address Filtering**; see the *Administration Guide* for details.)

Part IV. MIR GUIDE

Table of Contents

Chapter 15
Console Overview

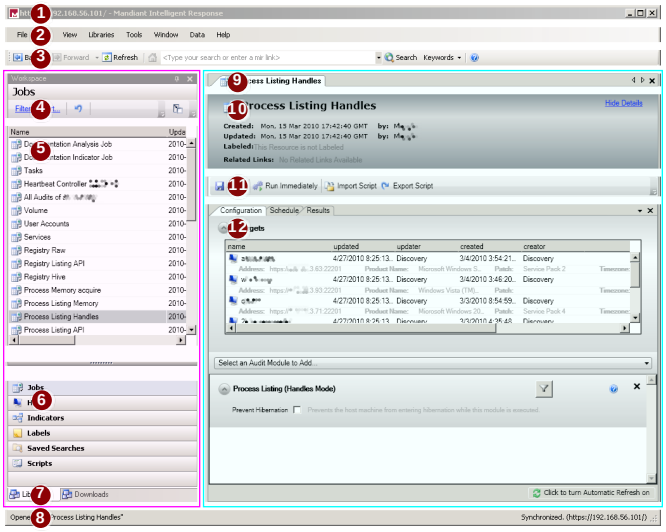
The MIR Console is your main tool for collecting, analyzing, and reporting on data. It provides a familiar Windows work environment with standard controls, such as tabs, menu bars, and buttons. This chapter assumes familiarity with the Windows user interface: the clicking of buttons, the use of the keyboard and mouse together to make multiple selections, the use of tabs to provide more information than can easily fit a single screen, and so on.

Incident response and electronic evidence discovery generate a lot of raw data; fortunately, most of that data can be categorized to make it easier to find, annotate, and link it with other findings. To aid in this, the Console provides a set of “Libraries” containing the main types of data.

The Console window, in its default configuration, comprises two main panes of functionality: on the left, the **Workspace** pane and on the right, various *Viewers* and *Editors*. Either pane contains tabs, tool bars, and other controls suitable to the type of work being performed and the type of data being displayed. The default layout of Console components can be largely customized, and these new layouts saved for re-use.DCP: Idea: a Layouts library in the Workspace.

Console User Interface Components

Showing the Library (left box, tinted pink) and a Viewer (right box, tinted blue).



1. Title Bar
2. Menu Bar
3. Console Tool Bar
4. Library Tool Bar
5. Library Contents List
6. Library Selectors
7. Workspace Tabs
8. Status Bar
9. Viewer/Editor Tabs

10.Summary Details
11.Viewer/Editor Tool Bar
12.Viewer/Editor Display Area

15.1. The Menu Bar

The Console menu bar contains the following commands:

File

Home
Opens the login window. Successful login connects the Console to the Controller. After successful connection, the Console is synchronized and workspace Resources are displayed.

New

Host
Creates a new Host resource, used by Audit Scripts to identify which Agents will be queried, and to associate Audit Results with their data sources.

Host Audit Job
Creates a new Audit Job. Audit jobs combine a list of Hosts to target with a list of configured Agent Modules; when the Audit is done, the modules will return their findings to the Controller.

Analysis Job
Creates a new Analysis Job. These jobs are applied against existing documents, and are used to adjust or compare their contents.

Host Audit Script
Creates a new Audit Script resource, allowing you to apply an Audit to a Host without creating a formal Host Audit Job.

Analysis Script
Creates a new Analysis Script resource, allowing you to apply an adjustment or document comparison without creating a formal Analysis Job.

Label
Creates a new Label. Labels can be “attached” to resources, allowing you to easily collate them.

Save *[name]*
Saves the item or resource.

Save *[name]* as Copy...
Saves the item or resource using a new name.

Rename *[name]*...
Renames the item [1].

[1]Note that the rename dialog window sometimes displays behind the application, resulting in a seemingly unresponsive Console. The dialog appears on the Task bar, where it can be selected.

Connect to Controller
Displays the **Connect to Controller** window. This window is normally used only during the first run of the Console, to set the Controller URI, default user name, and synchronization and **Hosts** Library options. These options may also be set by selecting **Tools** → **Options...**.

Exit
Quits the Console. If you have made changes to Jobs, Indicators, and so on, you will be prompted to save your work.

Edit
Commands in this menu vary dependant on the displayed Item or Resource.

Copy
Copies the selected data or objects. There are multiple copy options under the menu at any given time depending on context.

Copy Link to
Copies the object URI to the highlighted object. There are multiple copy link options under the menu at any given time depending on the context.

Find
Performs a search within views that support it.

Rename
Renames the selected object.

View

Libraries
In the **Workspace** pane, puts the **Libraries** tab on top.

Downloads
In the **Workspace** pane, puts the **Downloads** tab on top.

Toolbars
Toggles the display of various toolbars.

Refresh *[displayed Item or Resource]*
Refreshes the view of the currently active resource.

Show Controller Time/Hide Controller Time
Toggles the display of the controller time, in the lower right of the Console.

Full Screen
Maximizes the Console window.

Libraries
Displays the selected Library in a new *Viewer* Tab.

Some libraries can be accessed only through this menu; these libraries are not listed in the Libraries **Workspace**.

Tools

Label *[displayed Item or Resource]*
Applies a Label to the selected object.

Run Client Script...
Loads a Client Script for execution through the Console.

Manage Labels...
Opens the Label Management window.

Security

Change Password...
Allows you to change your password.

Import Trusted CA Certificate...
Loads a CA certificate.

Options...
Opens the Console configuration window.

Window

New Horizontal Tab Group
Displays all open tabs in separate windows, arranged horizontally.

New Vertical Tab Group
Displays all open tabs in separate windows, arranged vertically.

Close Tab
Closes the current, top-most tab.

Close All Tabs
Closes all open tabs.

Save Layout
Saves the current layout.

Load Layout
Loads the most-recently saved layout.

Restore Default Layout
Restores the default Console layout.

[list of open tabs]
Opens the selected tab.

Data
This menu is available when items or resources are displayed.

Sort data...
Allows you to configure a complex sort based on the contents of two or more columns.

Remove Data Sorts
Removes all complex sorts.

Filter data...
Allows you to reduce the number of data items displayed by filtering the list.

Remove Data Filters
Removes all data filters.

Filter for *[item or resource]*
Creates a data filter based on the selected object.

Search for *[item or resource]*
Searches for items related to the selected object.

Help

User Guide
Opens this *User Guide*.

What is new...
Display the contents of the *Release Notes* file using the Notepad text editor. Click the window close button or select **File** → **Exit** to dismiss the window.

About
Displays a window showing the MANDIANT Intelligent Response Console version number, EULA, and links to the MANDIANT website and product support email. Click **Close** to dismiss the window.

15.2. The Console Tool Bar

The Console tool bar contains the following commands:


Back
Go back in the tab history, to display previously-seen information. This is similar to the navigation controls in a web browser, and is useful when double-clicking a data item has re-used the current tab.


Forward
Go forward in the tab history, to display previously-seen information. This is similar to the navigation controls in a web browser, and is useful when double-clicking a data item has re-used the current tab.


Refresh
Refreshes the view of the currently active resource.


Views
Displays views.


Home
Opens the login window. Successful login connects the Console to the Controller. After successful connection, the Console is synchronized and Library Resources are displayed.


Search
To the left of the search button is a search term entry field. To the right of the search button is the **Keywords** selector, which provides a shortcut for placing search term delimiters in the term entry field.

Help
Opens the Help file.

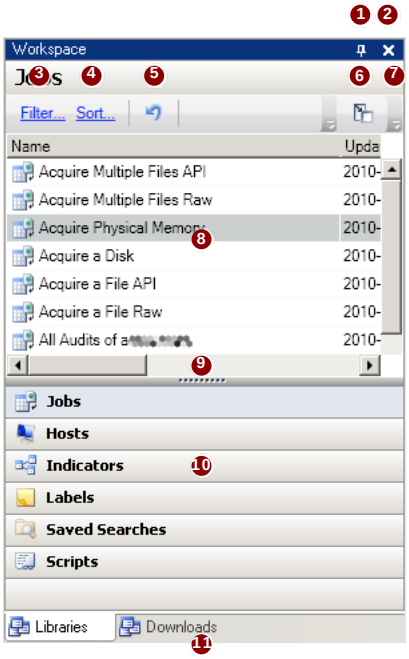
15.3. The Workspace

The **Workspace** pane, by default positioned on the left of the Console window, has tabs titled **Libraries** and **Downloads**. You will work within the **Libraries** tab most often; it provides convenient access to Libraries of resources and documents. You'll use the **Downloads** tab when you want to monitor long-running activities between the Console and the Controller. Both these tabs are discussed in more detail below.

15.3.1. The Libraries Tab

As you perform your investigations you will naturally create and discover a variety of resources, which are automatically filed into various Libraries. When a Library is selected, a list of its contents is displayed. If an item you seek is not readily available in the list you can always open the full library, filter by Label, or search for the item. Having identified a desired resource, you can copy its link address or open it in an *Editor* or *Viewer*.

Library pane User Interface Components



1. Toggle Workspace pane Hiding
2. Close Workspace pane
3. Configure Library Filter
4. Configure Library Sort Order
5. Remove Library Filters
6. Open Library in Viewer
7. Show Hidden Icons (if any)
8. Library Contents List
9. pane Splitter Adjustment
10. Library Selection Buttons

11.Workspace Tabs

The **Libraries** tab selects three-part pane, as shown above:

pane Controls, Library Name, and Tool Bar

To the right of the pane title bar are two control buttons. The **Autohide Toggle** button collapses the **Workspace** pane to a small tab, freeing space for the **Viewer/Editor** pane; toggling it again restores the **Workspace** pane to always-visible. The **Close** button closes the current Workspace; it can be restored by selecting **View** → **Libraries** or **View** → **Activity**.

Below the pane title bar is the name of the open library and its tool bar. When the tool bar is expanded to full width, it shows these controls:

Filter...
Allows you to filter the Library contents by including or excluding entries based on the contents of the columns.

Sort...
Allows you to sort the Library contents by columns, with support for sorting on more than one column.

Reset Filters
Resets filters and sort settings. For most Libraries, this removes filters and sorts; for the Script Libraries, this restores the original filter.

Open Library
Displays the full contents of the Library using the *Viewer* pane.

View Hidden Controls
Displays hidden buttons, if the **Workspace** pane is too narrow to display all of them.

Library Contents

The middle of the pane displays the Library contents.

Double-clicking a quick-select entry opens that resource using an appropriate *Viewer* or *Editor*. Right-clicking allows you to copy the Item or Resource address (usually for inclusion as a link in a document), export the resource as a file to your local storage, or perform other context-appropriate actions.

Clicking a column header sorts the list alphanumerically using the data in that column; clicking a second time will reverse the sort order. Right-clicking a column header allows you to configure the display of columns.

Between the Library contents and the Library selector buttons is a pane splitter that can be dragged to adjust the contents space.

Library Selector Buttons

The bottom of the pane is dedicated to library selectors, plainly labeled.

Users with installations with a high number of Host systems may wish to disable the Hosts Library (*Section 15.3.6, "Configuring the Console"*), to avoid excessively long

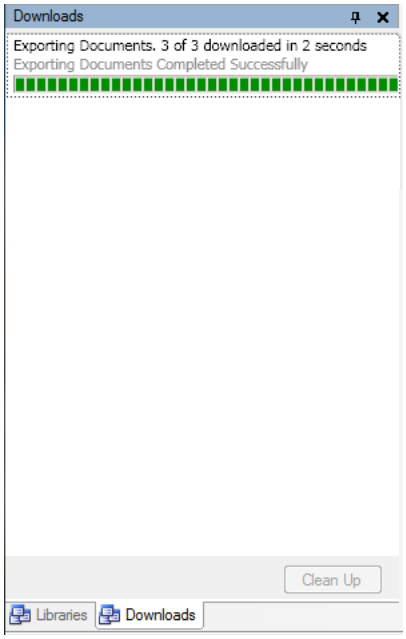
Controller synchronization times. The Host Library will remain available in the **Libraries** menu.

Changed from v1.3.x: the **Audit Results**, **Analysis Results**, and **All Documents** buttons have been removed. Those commands are still available through the Libraries menu.

15.3.1.1. The Downloads Tab

The **Downloads** tab displays long-running activities between the Console and the Controller, such as importing and exporting Audits and the execution of Scripts. Note that it does not display the status of currently running Jobs: that information is available by opening the *Job Editor* for the appropriate Job.

The pane controls and top-right icons are the same as the Libraries pane. The **Clean Up** button removes completed activities from the list.

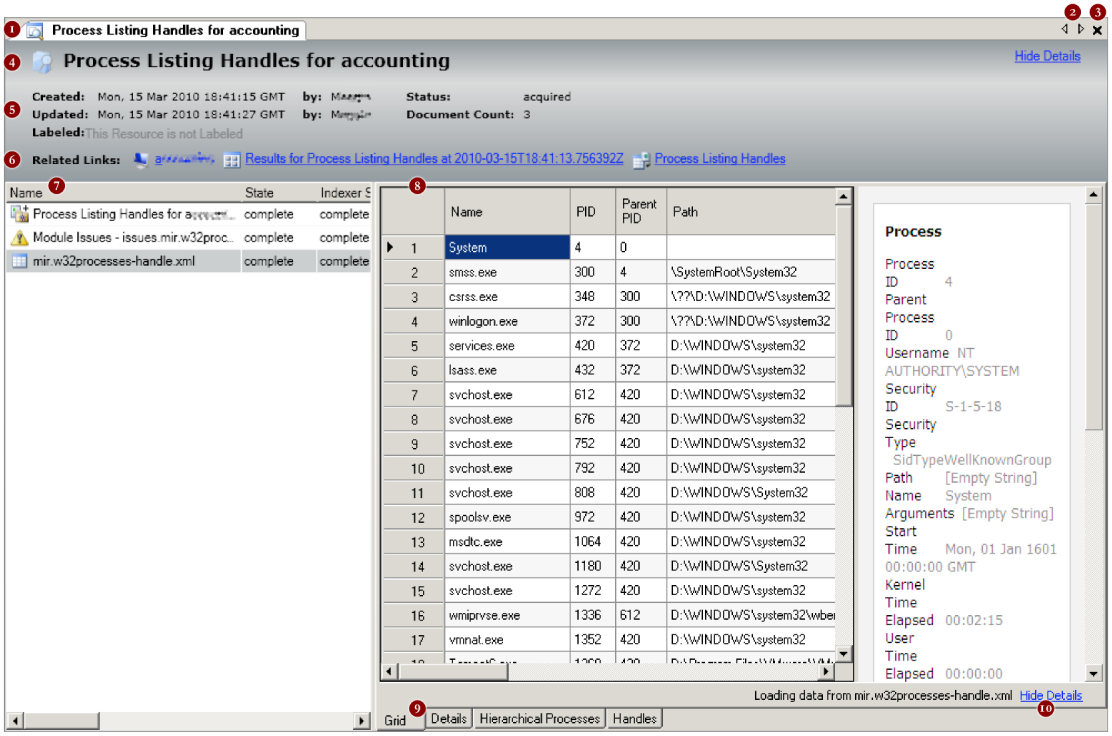


15.3.2. Viewers and Editors

Any resource you open from a Library or list of data objects (e.g. an Audit Result) is displayed in a *Viewer* or *Editor* tab. Each resource has its own custom view which provides more details about the resource and may allow you to edit those details. For example, viewing a Job or Script will show the Job and Script *Editor*, while viewing the results of a Port Listing Audit will display a grid of information, detailing all the data gathered during the Audit.

In a *Viewer*, the view may be "drillable" — that is, double-clicking a row in the viewer will show more detail about the resource or open it. If you wish to open a resource in its own tab, right-click the resource and choose **Open in a New Tab**.

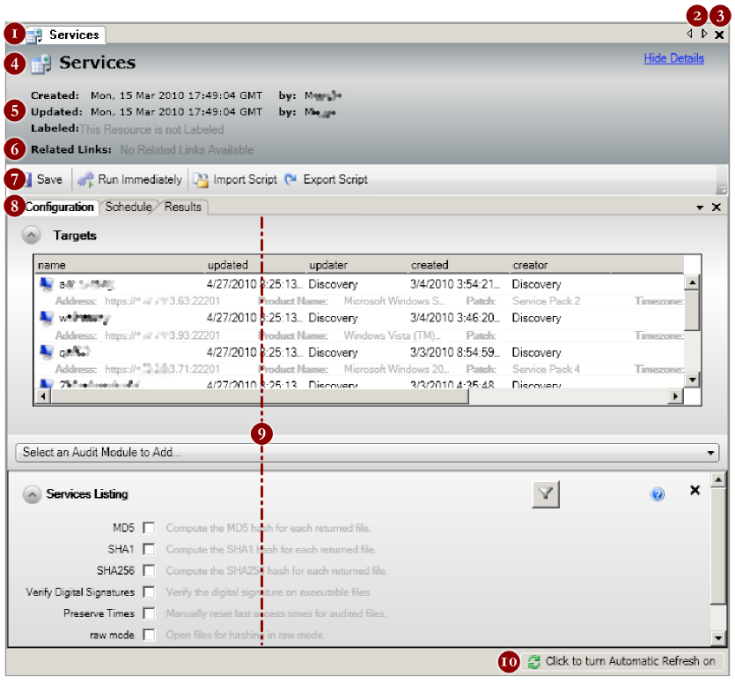
Typical Viewer User Interface Components



1. Viewer/Editor Tab Bar
2. Previous/Next Tab Selector Arrows
3. Closes Tab
4. Document Name
5. Document Details
6. Related Links
7. Document Contents (grid view)
8. Viewer Type Selector
9. Item Details
10. Item Details Toggle

Most views are organized as a set of columns that describe various aspects of the document. Like a spreadsheet, you may sort and filter by clicking a column header.

Typical Editor User Interface Components



1. Viewer/Editor Tab Bar
2. Previous/Next Tab Selector Arrows
3. Closes Tab
4. Resource Name
5. Resource Details
6. Related Links
7. Editor Tool Bar
8. Editor Tab Bar
9. Editor Working Area
10. Controller Automatic Refresh Toggle

15.3.2.1. Navigating Viewer/Editor Tabs

Clicking on a tab makes it the top-most, current tab. As well, you can scroll through tabs or close individual tabs by using the tab bar ◁ ▷ ✕ controls in the upper right hand corner of the Viewer. You can close multiple tabs by right-clicking a tab and selecting **Close**, **Close All**, or **Close All But This**. If the tab is associated with a single resource, you may also choose **Copy Link**, **Rename Resource**, or **Delete Resource**.

15.3.2.2. The Summary Area

The Summary View displays information about an object being viewed in the Document Viewer. It includes the name of the object, when the object was created or changed, and by

whom. It also contains links to the history of the object, and any references used to create it. The Summary View also contains links to historical information about the object being viewed, and the user who created or modified it.

15.3.2.3. Editor Tool Bars

Each editor has its own tool bar, specific to the commands that can be applied to its contents.

The Host Editor Tool Bar

Save
Saves the Host configuration to the Controller.

Create Audit

All Audits
Opens a new Host Audit Job tab for the Host pre-populated with audits.

Custom Audit
Opens a new Host Audit Job tab for the Host.

Run Audit
Runs Audits or Scripts against the Host.

Import Audit
Imports Audit data from a local storage device, typically a portable data storage device. A standard file selection window will be displayed.

The Host Audit Job Tool Bar

Save
Saves the Job to the Controller.

Run Immediately
Runs the Audit.

Import Script, **Export Script**
Imports and Exports a Script to/from a local storage device; this enables you to share Scripts between Audit Jobs and with co-workers. A standard file selection window will be displayed.

The Indicator Job Tool Bar

Run Immediately
Runs the Audit.

Import Script, **Export Script**
Imports and Exports a Script to/from a local storage device; this enables you to share Scripts between Audit Jobs and with co-workers. A standard file selection window will be displayed.

Generate Filters
Adds Audit Modules to the Job, applicable to the Indicators that are being used. The Audit Modules need to be manually configured for the Hosts.

The Analysis Job Tool Bar

Save
Saves the Job to the Controller.

Run Immediately
Runs the Audit.

Import Script, **Export Script**
Imports and Exports a Script to/from a local storage device; this enables you to share Scripts between Audit Jobs and with co-workers. A standard file selection window will be displayed.

The Host Audit Script Tool Bar

Save
Saves the Script to the Controller.

Create Job
Creates a new job, based on the Script.

Import Script, **Export Script**
Imports and Exports a Script to/from a local storage device; this enables you to share Scripts between Audit Jobs and with co-workers. A standard file selection window will be displayed.

The Analysis Script Tool Bar

Save
Saves the Script to the Controller.

Create Job
Creates a new job, based on the Script.

Import From Disk, **Export to Disk**
Imports and Exports a Script to/from a local storage device; this enables you to share Scripts between Audit Jobs and with co-workers. A standard file selection window will be displayed.

Add to Favorites
Applies the **.favorite** Label to the Script.

15.3.3. The Status Bar

The status bar is found at the bottom of the window. On its left, it displays information about the Console's current activity.

On its right, the status bar displays information about its communication with the Controller. If **View** → **Show Controller Time** has been used, the Controller time is also shown.

15.3.4. User Interface Basics

15.3.4.1. Tabs

Sections of the interface may have multiple functions that can be selected by using tabs within that section. For example, the Workspace contains tabs for both **Libraries** and **Downloads** at the bottom of the pane. Each tab displays different information in the Workspace environment. The *Viewer/Editor* side of the Console uses tabs across the top to provide access to different documents; while some Editors include subtabs for different editing functions, and some Viewers include tabs at their bottom edge to select different view formats.

15.3.4.2. Resource Icons

In both the Workspace and Viewer/Editors views, resources are identified by specific icons:

 Job

 Host

 Indicator

 Label

 Case Note

 Saved Search

 Script

 Various Result Documents

15.3.4.3. Basic Navigation

The Console is a standard Windows application that behaves like many familiar office productivity programs you might have used. One of the most important things to remember when using the Console is the paradigm for mouse clicks. Generally, the following rules are followed within the interface:

Clicking a resource selects it
: If you click on a resource in any of the Viewers/Editors that comprise the interface, the resource you clicked on is selected. The selected resource is highlighted, and any detail views for selected resource are updated.

Double-clicking a resource in a Library opens it in a Viewer/Editor
: This double-click action will lead to one of two outcomes:

A. The top-most Viewer/Editor tab will be re-used, displaying information associated with the selected resource. This is the default behavior.

OR

B. A new tab will be created in the Viewer/Editor, in which the information associated with the selected resource will be displayed. This is the alternate behavior.

See *Section 15.3.6, "Configuring the Console"* to change this behavior.

Double-clicking a resource in the Document Viewer opens it in the current tab
In some cases, resources in the Document Viewer are "drillable." That is, there may be a view for resources that provides more information. This new information will replace the current view.

You can return to the previous or next view by using the Back and Forward buttons in the Console tool bar.

Right-clicking a resource displays its context menu
Options for renaming, deleting, exporting, and labeling an object are displayed on the context menu for an item.

Hovering over a resource displays a Summary View
If you position the mouse over a resource and do not move it for a few moments, a Summary View for that resource will be displayed.

Clicking linked information in the Summary View opens a new Document Viewer tab
Clicking on linked information in the Summary View opens that resource or data in a new Document Viewer tab.

In addition to a familiar mouse-click paradigm, the Console provides additional actions when viewing data:

Sorting Data
Clicking on the column will sort the grid or list on that column. Clicking again on the column header reverses the order of the sort.

For complex sorting, right-click a column header and choose **Sort...** or **DataSort...**. A window will be displayed that allows you to specify multiple sort terms.

Some data that appears to be numeric may be represented and stored as a string. As such, it may sort lexically (that is, alphabetically) versus numerically when a column is sorted.

Filtering Data
The Controller generates a *lot* of data. You will sometimes find your Libraries easier to navigate when you filter their contents to restrict your item choices to a particular set of data.

Right-click a column header and choose **Filter...** or **Data** → **Filter...** to create a filter that reduces the number of entries when viewing a list of resources.

Copying individual or multiple cells within a grid or list
As with spreadsheets, you can drag or use **Shift+Click** to select multiple contiguous rows, columns, or cells. You can then copy and paste them into another document.

You can also use the standard **Ctrl+Click** action to select non-contiguous items.

Selecting which columns to display
Right-click a column header and choose **Configure Columns...** to select individual columns for display. Use this, along with column reordering, to avoid side-scrolling to see the fields you want to see.

Changing the display order of columns in a grid or list
Dragging a column header will allow you to reposition the column. You may also right-click a column header and choose **Configure Columns...** to use the column display editor window to arrange the order of columns.

Sizing columns
Dragging a column edge adjusts the width of a column. You can also set widths by right-clicking a column header, choosing **Configure Columns...**, then selecting a column name and setting its pixel width.

15.3.4.4. Keyboard Shortcuts

Ctrl+A	Select All.
Ctrl+C	Copies information to the clipboard.
Ctrl+K	In a Case Note, inserts a link.
Ctrl+L	In a Case Note, formats an unordered list.
Ctrl+M	Tabs forward through a Case Note.
Ctrl+Shift+M	Tabs backward through a Case Note.
Ctrl+N	In a Case Note, formats an ordered list.
Ctrl+P	Opens the Print dialog box.
Ctrl+S	Saves the contents of the active tab.
Ctrl+V	Pastes information from the clipboard.
Ctrl+X	In a Case Note, cuts text or a link, placing a copy into the clipboard.
Alt+F4	Exits MIR.
Ctrl+F4	Closes the active tab in the Document Viewer.
F11	Maximizes the Console to full screen.

15.3.5. Customizing Your Interface

The Console interface can be significantly reorganized according to your preferences. Each view can be closed, auto-hidden, undocked, or moved. These changes are stored locally, so if you work on more than one Console, you can display your interface differently on each one.

The default interface configuration can be easily restored by selecting **Window** → **Restore Default Layout**.

15.3.5.1. Moving Viewer/Editors and Tabs

All tabs can be reorganized or “torn” into separate panes. This is especially useful for side-to-side or top-to-bottom comparisons of different documents. The Workspace can also be reorganized within the Console window or “torn” into a separate window of its own.

Reorganizing panes and Tabs

panes and tabs can be moved into separate frames:

1. Drag the pane title bar or tab title you want to move.

2. Placement icons will appear on the Console window: one near each edge and one in the middle. As you drag over these icons a blue background will show you where the tab will be placed.

   Release on the quadrant you desire. The tab will now appear in its own frame.

3. You can move additional tabs into the new frame by repeatedly “dropping” tabs into the placement quadrant.

You can restore the reorganized tab back to its original location by selecting **Window** → **Restore Default Layout** or by dragging the tab back to its original location.

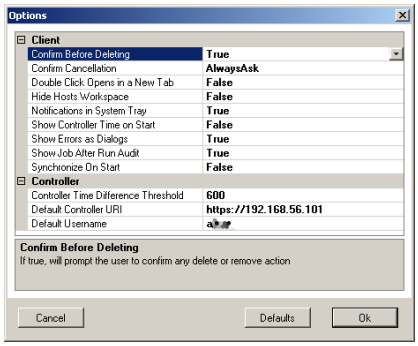
15.3.5.2. Saving, Loading and Restoring Layouts

To save custom layouts, select **Window** → **Save Layout**. To restore, select **Window** → **Load Layout**. Saving a layout preserves tab organization, hidden viewers, and any changes to the display of the Workspace pane. Only one layout may be saved. Restoring the layout loads the last saved layout.

Restoring the default layout overwrites any changes you have made to the appearance of the Console, including reorganized tabs, changes to the Workspace pane, and any closed or hidden viewers. To return the layout to its default state, select **Window** → **Restore Default Layout**.

15.3.6. Configuring the Console

After installation, the first step to using MIR is configuring the Console by choosing **Tools** → **Options**. This opens a window with configurations for the Client.



15.3.6.1. Client Options

The Client section configures the behavior of the Console, your main working environment. The following options are available, with defaults shown *like this*.

Confirm Before Deleting
True: Prompt to confirm any delete or remove action.

False: Delete or remove actions are performed without confirmation.

Confirm Cancellation
AlwaysAsk: Prompt to confirm before cancelling a job.

AlwaysYes: Cancel jobs without confirmation.

Double Click Opens in a New Tab
True: Double-clicking a resource opens a new tab.

False: Resources are opened in the current tab.

The Console must be restarted when this option is changed.

Hide Hosts Library
True: The Hosts Library is opened when the Console is started.

False: The Hosts Library will not be opened when the Console is started; this can improve startup time when the Controller has many Host records.

Notifications in System Tray
True: When activities complete, a pop-up is displayed in the Windows System Tray.

False: No pop-ups are displayed when an activity completes.

Open With Cache Location
Chooses the directory into which temporary files are cached. Used by the **Open With...** command.

Show Controller Time on Start
True: Displays the Controller's time in the Console status bar.

False: The Controller's time is not displayed.

Show Details Popup in Lists
True: When hovering over a list item, display an overlay with details for the item.

False: Do not show details for list items.

Show Errors as Dialogs
True: Errors are displayed in pop-up dialog boxes.

False: Errors are displayed in the Console status bar.

Show Job After Run Audit
True: When you run an Audit manually, a new *Viewer* tab will be opened on the right, showing details about the Job.

False: The audit is run in the background, with no new tab being opened.

Synchronize on Start
True: When started, the Console will attempt to connect to and synchronize with the Controller.

False: Synchronization requires clicking the **Home** button in the Console menubar.

15.3.6.2. Controller Options

The Controller section configures the behavior of the Controller appliance. The following options are available, with defaults shown *like this*.

Controller Time Difference Threshold
600: Sets the acceptable time difference, in seconds, between the local Console and the Controller. Time differences larger than this value will display a warning.

Default Controller URI
[set by administrator]: The Uniform Resource Identifier (URI) of the Controller, a fully qualified hostname or IP address.

Default Username
[no default]: The name used when connecting to the Controller.

The default user name is displayed when connecting, and may be overridden by the user at that time.

Chapter 16
MIR Quick Start

16.1. Using MIR for the First Time

This section provides a hands-on introduction to MANDIANT Intelligent Response by stepping you through an Audit of a single target Host. Before you begin, get the following from your MIR administrator:

- Your MIR user name and password.
- The hostname or IP address of a MIR Controller on the same local network as the Host.

The following examples make these assumptions:

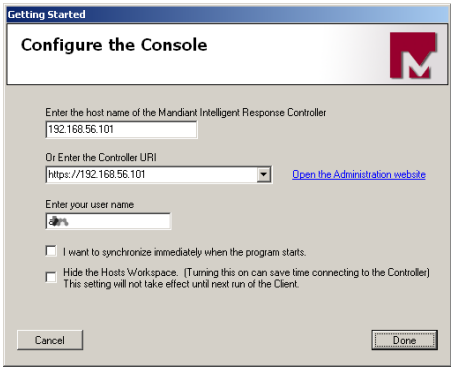
- The Controller has been correctly installed.
- At least one Agent has been installed on the Host or on a removable media device, and the Controller can connect to it over the network per the requirements outlined in the *Administration Guide*.
- The Console has been installed on the workstation, and you can connect to the Controller from your Console over the network.

16.1.1. Connecting to the Controller

16.1.1.1. First-Run Configuration of the Console

To start using the Console:

1. Double-click the Desktop shortcut, **MANDIANT Intelligent Response Console**. If the shortcut is not available, choose **Start** → **Program Files** → **MANDIANT** → **MANDIANT Intelligent Response Console**.
2. If this is the first time the Console has run, a **Connect to Controller** configuration window will be shown:



a. In **Enter the host name...** provide the host name or IP address of the Controller. As you type the **Controller URI** field will show a best-guess URI address which can be corrected as needed.

b. In **Controller URI** provide the `https` address of the Controller.

c. In **Enter your user name** provide your user name. When you connect, you will be asked for your password as well.

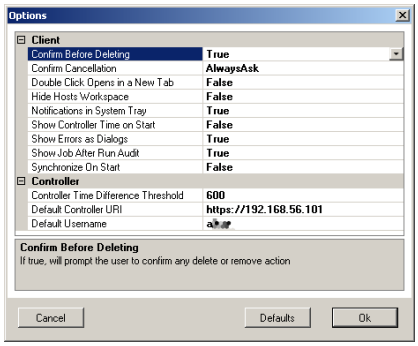
d. Click **Done**.

If the Console has been previously configured, you will not be presented with the **Connect to Controller** window.

16.1.1.2. Configuring the Controller Address

If the Controller address changes, or if there are multiple Controllers in your local network, you may need to configure the Controller address before logging on. If you configured the Controller through the **Connect to Controller** configuration dialog, you can skip this step. Otherwise:

1. Choose **Tools** → **Options**.
2. In Default Controller URI provide the `https://` address of the Controller. Click **Ok** to accept the change.
3. If you are logged into a Controller, you will have to restart the Console. If you are following the *Quick Start* in sequence, you are not yet logged into the Controller and can skip this step.



16.1.1.3. Logging On

If the Console has a valid TDCA and Controller address, you can log into the system:

1. In the tool bar, click **Home**.
2. In the **Enter Credentials** window, provide your user name and password, then click **Ok**.

If the TDCA is not recognized, you will be presented with an alert window. You can continue to log in, but need to be aware that you are operating with reduced security.

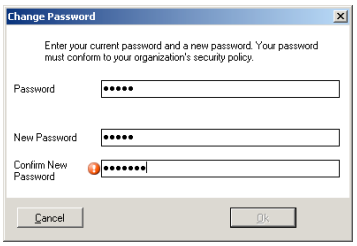
3. The Console status bar will indicate the system is synchronizing. Depending on network traffic and the amount of data to be synchronized, this may take a few seconds.

16.1.1.4. Changing Your Password

If this is your first time logging into the Controller, change your password. You may, of course, change your password at any time.

1. Close all *Viewer/Editor* tabs.
2. Choose **Tools** → **Security** → **Change Password...**.
3. In the **Change Password** window, provide your original password and your new password, then click **Ok**.

   An exclamation mark on a red background will be displayed beside **Confirm New Password** if your new password and confirmation password do not match.



Your Console should now be ready for use. In the next section, you will create a Host Audit and examine the results.

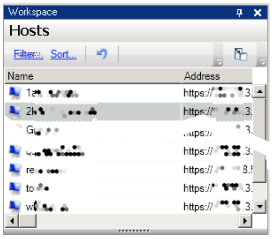
16.1.2. Running an Audit Job

Host Audit Jobs — also called Host Audit Scripts — request Items from deployed Agents, which return those Items to the Controller, where they are categorized and analyzed. There are several methods for running a Job: for this *Quick Start* you will either select an existing Host or create an entry for a new Host, and then create and execute an Audit against that Host.

16.1.2.1. Selecting an Existing Host

If the Controller is already aware of an Agent, the Agents Host resource is found in the Hosts Library:

1. In the **Workspace** pane on the left of the Console, click **Hosts**. The **Hosts** Library will be displayed at the top of the pane. (If the **Hosts** Library button has been hidden, choose **Libraries** → **Hosts**. The **Hosts** Library will be shown in a *Viewer* tab.)



2. Double-click the Host name to display its current IP address, description, and any Audits that have been run against it.

16.1.2.2. Searching for a Host

If you want to find a specific Host based on its IP address, use the search bar at the top of the Console window.

The search will take the form:
`+Host/address:`*`ip_address`*

If you were searching for a Host with an IP address of 10.201.137.40, your search term would look like this:
`+Host/address:10.201.137.40`

Once you enter the search term, click **Search**. The results are displayed in a new tab. Double-clicking the entry will display the Host details.

If searching does not reveal the Host, it is because the Controller has not been successfully contacted by (or the Host is not using) its Agent Discovery Service. The Host Resource will have to be manually configured.

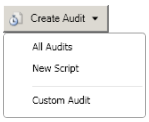
16.1.2.3. Manually Adding a Host

If you can not find an appropriate Host for the *Quick Start*, you will need to add one manually. See *Section 17.1.1, "Manually Adding and Configuring a Host"* for instructions.

16.1.2.4. Configuring a Custom Audit Script

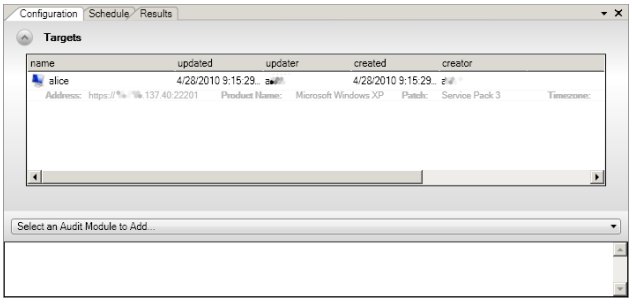
Once you have identified a Host, the next step is to create and configure an Audit. The Audit with its list of Hosts is called a Job.

1. In the **Host Name** tool bar, click **Create Audit** and choose **Custom Audit**.



   A new *Viewer/Editor* tab named **Custom Audit of Host Name** will be created.

2. Select the **Configuration** sub-tab. The **Targets** area will list the Host; below that is a **Select an Audit Module to Add...** selector.



3. From **Select an Audit Module to Add...**, choose the type of Items you wish to collect.

4. Click **Save** (Ctrl+S) in the *Editor* tool bar. Provide a **Name** for the Job and click **Ok**. Note the *Viewer/Editor* tab name changes from **Custom Audit of name** to the new name.

Leave this tab open; you will be using it to run the Job and view the results.

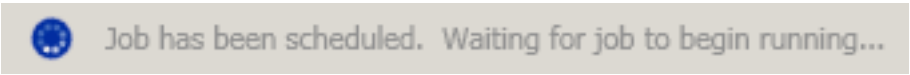
16.1.2.5. Running a Custom Audit Script and Viewing Results

If you wish to run a Job immediately after creating it (see *Section 16.1.2.4, "Configuring a Custom Audit Script"*), you can do so from the *Viewer/Editor* tab:

1. Click **Run Immediately**.

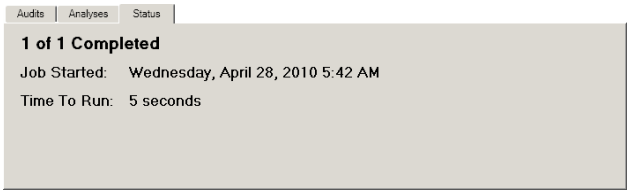
   The Console will send the Job to the Controller, as indicated in the *Editor* status bar. While the Job queues and executes the *Editor* will prevent you from making changes or queuing additional jobs.

   There may a minute delay as the Job waits in the queue; it will be executed the next time the Controller checks for waiting Jobs. During this period the **Schedule** tab will be selected, showing the queued Jobs.

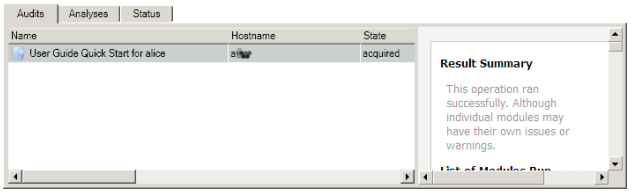
   

   When the Job begins executing the *Viewer/Editor* will switch to the **Results** tab and list each Result Set that has or will be created. The **State** column will be periodically updated as long as the **Click to turn Automatic Refresh Off** button remains active (blue).

   Selecting a Result Set will activate its **Status** sub-tab. The **Status** sub-tab shows the number of Host Audits completed, the time the Job started, and the time that has elapsed.

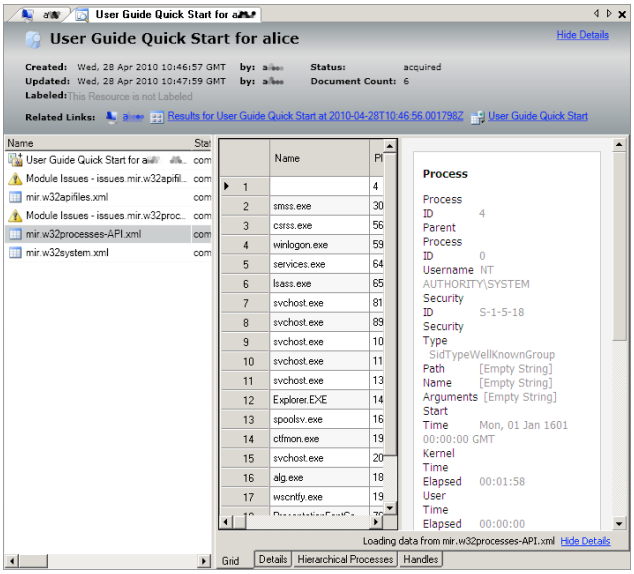
2. When **State** indicates **acquired**, click the **Audits** sub-tab. On the left is a list of each Audit Job. Click an entry to see a summary of the Audit Modules that were run.

3. In the **Audits** sub-tab, double-click Audit Job entry to display a detailed list of its documents. This is like clicking a link on a web page: the *Viewer/Editor* controls are replaced with content from a new "page." As with a web browser, you can use the **Back** button to restore the previous view.

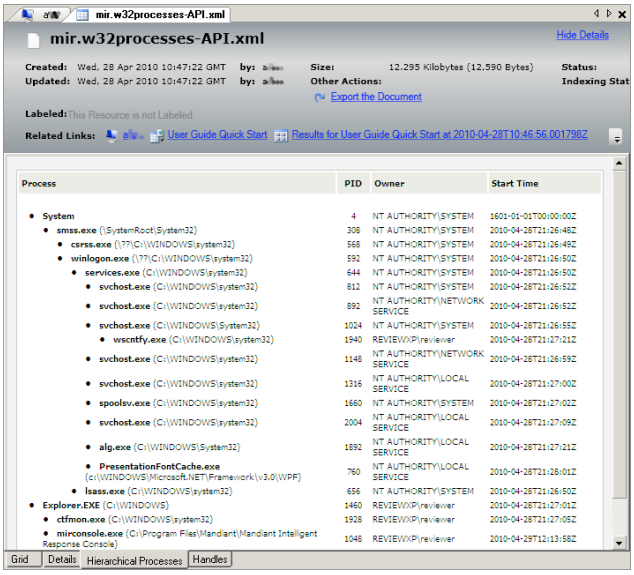
The new page shows a list of documents on the left and, when you click one of the documents, the contents of that document to the right. Double-clicking a document replaces the two-pane view with a full-size view of the document. You can use the **Back** button to restore the two-pane view, and click it again to restore the *Viewer/Editor* page.

4. Clicking a document in the two-pane *Viewer* will give you a Console window looking similar to this:



5. Double-click a document to display its contents. For many documents, a set of tabs at the bottom of the *Viewer* will provide different views of the document.

   For example, opening a `mir.w32processes-API.xml` document and selecting the **Hierarchical Processes** tab will display information similar to this:



16.1.3. Wrapping Up

16.1.3.1. Logging Off

1. Choose **File** → **Exit**.
2. If you made any changes, you will be prompted to save your work. Select **Yes** to save your work, **No** to exit without saving, or **Cancel** to stay logged in.

16.1.4. Uninstalling an Agent

Uninstalling removes the Agent from the Host. It stops and removes the service, stops and removes any active kernel drivers, and removes any Windows firewall exceptions.

If you installed the Agent in Portable Use Mode and ran it from a removable media device, the Agent was not installed onto the Host and does not need to be removed.

16.1.4.1. Removing an Agent using the Windows Control Panel

1. In **Start** → **Control Panel** → **Add or Remove Programs**, select **MANDIANT Intelligent Response Agent**.
2. Click **Remove** and follow the prompts

Chapter 17
Working with Audit Items

When you discover or receive a report about a suspected security breach, the first order of business is to collect information about the event. This is similar to collecting evidence at the scene of a crime. The evidence could be records from a detection system, reports from employees, or data from systems that may have been compromised.

Your investigations may also be in response to legal action, perhaps a search warrant, subpoena, or court order. These investigations might include collection and analysis of any form of digitally stored information: email, word processing documents, databases, and so on.

In some circumstances the type of evidence needed may be so broad that you will need to collect the entire contents of a hard drive or other storage device, on one workstation or many. These collections often span many systems, email accounts, or other information repositories.

MANDIANT Intelligent Response supports you in all cases by providing tools that make collecting, organizing, and analyzing data faster and easier. This chapter describes these features, from launching Audits that collect information from target systems, to running Analysis Commands against those results to narrow the scope of an investigation.

17.1. Creating Host Records

To run an Audit over the network or import locally-collected audit data into a Controller, a Host Resource must exist in the system. Host Resources store information about the host system, including hostname, IP address data, and other details.

HostResources can be created manually or automatically. If you use the Agent Discovery Service installed Agents will periodically register their current IP address and other details with the Controller: you will not have to manually create HostResources or manage their network address information. Refer to *Administration Guide* for further details regarding the Agent Discovery Service.

If Agent Discovery Service has not been configured, you will have to manually create Host Resource before you can run Audits or import locally-collected audit data into the Controller. There are two methods for manual Host Resource creation: through the Console user interface, or by using Client Scripts. The former is preferable when you have only a few Hosts to create; the latter is a better choice for batch creation.

This section describes how to create individual Hosts via the Console. Refer to *Appendix E, Client Scripts* for more information regarding the Client Script interface.

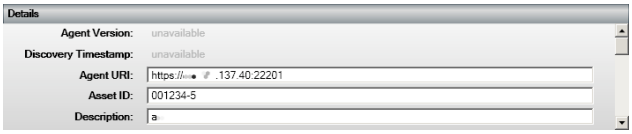
17.1.1. Manually Adding and Configuring a Host

You can add a Host Resource manually if you know the Host's IP address or hostname:

1. Choose **File** → **New Host**. A tab named **New Host** will open in the *Viewer/Editor* pane, where you will create the new Host Resource.

2. In the **Details** area the only *required* information is **Agent URI**. It has the format `ip_address|hostname [https://]:[port]`. By default Agents listen on TCP port `22201`.

   For example, if you are connecting to a Host with an IP address of 10.201.137.40, you would enter `https://10.201.137.40:22201` in **Agent URI**.



   Providing an **Asset ID** or **Description** is optional. You can provide that information at this time if you know it. If not, it can be added later.

3. Click **Save** (CtrlS) in the **New Host** tool bar.

   You will be prompted to enter a name for the Host. You can enter any next you like; a common convention is to enter the actual hostname of the host system, if one exists. The **New Host** tab name will be replaced by the new name.

   Click **Ok** to save this new Resource.

If the **Hosts** Library is visible, you will see the new Host in its list as soon as the Controller sends it to the Console.

17.2. Collecting Audit Items

Agents are responsible for collecting information from Host systems. They can be installed on a Host "permanently" as a network daemon or Windows service, or run from a removable media device without installing anything on the Host.

When you choose to use network-based acquisitions, you develop Scripts, and Jobs using the Console interface. The Console sends these to the Controller, which in turn contacts the appropriate Agents, sends them their instructions, and receives Items back from them. You can then use the Console to further process this data.

When you choose *Portable Use Mode*, the Agent is installed and run from a removable media device. In this case, you execute the Agent from the command line and acquired Items are saved to local storage (the system hard drive, the portable media device, or other storage device). This information can then be imported through the Console, which sends Items to the Controller for further processing.

Details about Agent deployment are in the *Administration Guide*. More information about the Agent and its command-line operation is found in *Appendix D, Agent Command-line Reference*.

The following examples assume Agents have been installed on many Host systems. For network acquisition examples, it is assumed that the Agent is running as either a daemon or a Windows service.

17.2.1. Configuring and Running Jobs

To collect information from an Agent, you must create a Host Audit Job. Host Audit Jobs specify a list of Hosts on which to run the Job, along with a list of Agent Modules to be

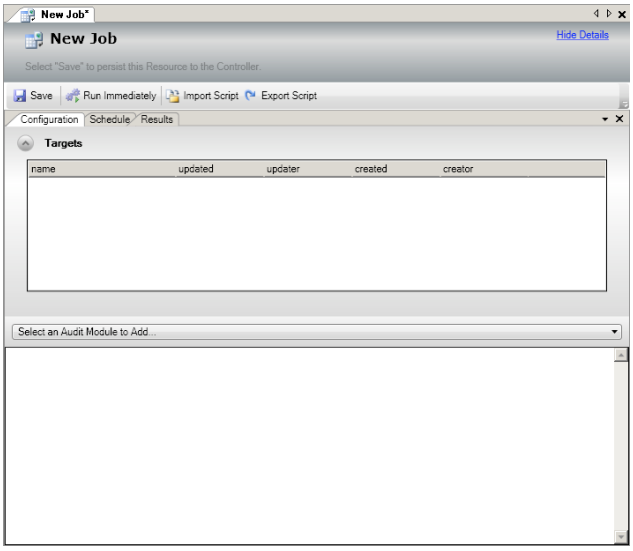
used in performing the Audit. Each Module collects particular Items and may have several parameters that allow you to customize what is retrieved and how it is collected.

Complete details on Agent Modules are available in *Appendix A, Audit Modules and Analysis Commands*.

17.2.1.1. Creating a New Host Audit Job

Jobs combine a list of Hosts with a list of Agent Modules. When a Job is run, the Controller requests the Agent on each Host to send back Items from those Modules. When the Job is finished, you can then search, analyze, and otherwise work with these Items.

1. Choose **File** → **New** → **Host Audit Job**. A tab labelled **New Job** will open in the *Viewer/Editor* pane.



2. Select the **Configuration** tab.

3. Add Host records to the **Targets** box by dragging or pasting Resources from:

   - The **Hosts** Library, adding each Host as an individual entry in **Targets**.

     OR

   - The **Labels** Library, adding a collection of Hosts sharing a common label.

     OR

     The **Saved Searches** Library, adding a collection of Hosts that the Controller will identify using a particular search query.

4. Choose Audit Modules appropriate for the Items you wish to collect from the Hosts by choosing them from the **Select an Audit Module to Add...** selector. Each module you choose will be listed below the selector; if the module has configurable parameters, those settings will be shown, with required parameters outlined with a red box.

5. Configure the modules to collect the Items you seek. Each module has different parameters, far too many to list here. See *Appendix D, Agent Command-line Reference* for details.

6. Some audits will return an immense amount of data. This information is normally indexed, so that it can be included in searches. Choosing **Do not index audit results**, found above the audit module selector, will prevent indexing, and may significantly speed up your controller interactions. See *Appendix B, Searches* in the appendices for details.

7. When you are satisfied that you have added all the Hosts and Modules required for this Host Audit Job, click **Save**. You will be prompted to name the Job. The **New Job** tab name will be replaced by the new name.

The Job can now be found in the Library, ready for use at any time.

It is a good idea to test your new Job before moving on. The next two tasks describe how to run a Job and how to cancel it if the need arises. When the Job has finished its test run, you would naturally check that it collected suitable Items: see *Section 17.2.5, "Viewing Job Results"* later in this chapter for further instructions.

17.2.1.2. Testing a Job

As you build out the Jobs Library, you will often perform Audits by using an existing Job.

1. Open the Job in the *Viewer/Editor*.

2. Confirm that the **Targets** and Audit Module selections are appropriate.

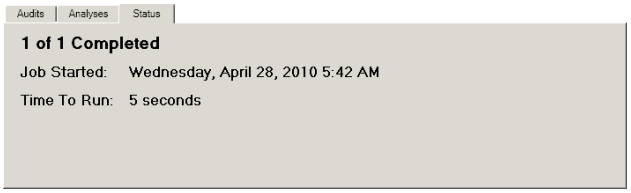
3. Click **Run Immediately**.

   The Console will send the Job to the Controller, as indicated in the *Editor* status bar. While the Job queues and executes the *Editor* will prevent you from making changes or queuing more jobs.

   There may a minute delay as the Job waits in the queue; it will be executed the next time the Controller checks for waiting Jobs. During this period the **Schedule** tab will be selected, showing the queued Jobs.

   When the Job begins executing the *Viewer/Editor* will switch to the **Results** tab and list each Result Set that has or will be created. The **State** column will be periodically updated as long as the **Click to turn Automatic Refresh Off** button remains active (blue).

   Selecting a Result Set will activate its **Status** sub-tab. The **Status** sub-tab shows the number of Host Audits finished, the time the Job started, and the time that has elapsed.

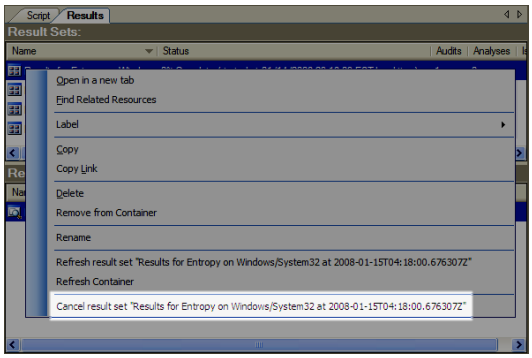


4. When the **State** reports **acquired**, you may select the Job, and then select the **Audits** sub-tab to view the results.

Once the Job has been started by the Controller, it will continue to run unless explicitly canceled. If it is a long-running Job, you can close the Console and come back to it later for Analysis tasks.

17.2.1.3. Canceling a Running Job

1. Open the Job in the *Viewer/Editor*.
2. Select the **Results** sub-tab. Identify the running Job through its **Name** and **Status** entries.
3. Right-click the Job and choose **Cancel result set...**.

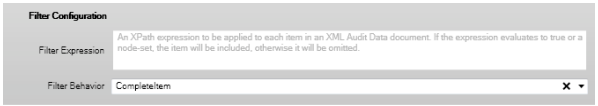


17.2.2. Audit Module Filters

While creating or editing a Host Audit Script or Job, XPath 2.0 filtering can be added to any Module, limiting the Items returned by Agents. While some module configuration options serve a similar purpose — specifying regex filters, for example — XPath filters provide greater flexibility.

17.2.2.1. Applying an XPath Filter to a Script or Job

1. Open the Script or Job. Click the **Configuration** sub-tab to view its Audit Modules.
2. Click the **Agent Filter** button for the Audit Module you wish to filter. The module will expand to show a **Filter Configuration** area.



3. In the **Filter Expression** box, type a valid XPath 2.0 filter. As you type, the icon on the **Agent Filter** button change to a warning symbol when parentheses or brackets are unbalanced. When the XPath structure is valid, the icon reverts back to the filter symbol.

   Filter expressions may reference data using:

   - Column header names, like `SizeInBytes`.

- Keywords, like `/FileItem/Created`. See *Section 18.4.6, "Keywords"* for a list of keywords.
- Environment variables, like %SYSTEMDRIVE%.

Environment variables point to the local location, not the current user location.

4. Using the Filter Behavior selector, choose the filter matching rule:

CompleteItem
When a match is found within a node, return the entire node.

For example, if the filter matches part of a *File* node, the entire *File* node would be returned in the results, including its children.

ExcludeUnmatchedSiblings
When a match is found within a node, return child nodes that fulfill the match, and exclude their non-matching siblings.

For example, if you were matching the name of a *Handle* in a process, only handles with a match would be returned; other handles would be excluded.

ExcludeChildren
When a match is found within a node, return the node but exclude its children.

17.2.2.2. Audit Module Filter Examples

Look for files and directories less than a specific size in a File Audit:

```
//*[SizeInBytes<10000]+
```

Look for only files less than a specific size in a File Audit:

```
//*[(FileAttributes!='Directory') and (SizeInBytes<100000)]
```

For a User Accounts audit, find the username *qauser*:

```
/UserItem[((Username[(lower-case(.) = 'qauser')]))]
```

Look for only a specific file based on a case-insensitive value:

```
//*[contains(lower-case(FullPath), '3dgarro.cur')
or contains(lower-case(FullPath), '3dgmove.cur')
or contains(lower-case(FullPath), '3dgnesw.cur')
or contains(lower-case(FullPath), '3dgno.cur')
or contains(lower-case(FullPath), '3dgns.cur')
or contains(lower-case(FullPath), '3dgnwse.cur')
or contains(lower-case(FullPath), '3dgwe.cur')
or contains(lower-case(FullPath), '3dsmove.cur')
or contains(lower-case(FullPath), '3dsns.cur')]
```

Find Any files with Created, Modified or Accessed dates in the time range 01 SEP 2009 to 11 SEP 2009:

```
/FileItem/Created[year-from-dateTime(.) = 2009 and month-from-dateTime(.) = 09
and (day-from-dateTime(.) > 01 and day-from-dateTime(.) < 11)] |
/FileItem/Modified[year-from-dateTime(.) = 2009 and month-from-dateTime(.) =
 09
and (day-from-dateTime(.) > 01 and day-from-dateTime(.) < 11)] |
/FileItem/Accessed[year-from-dateTime(.) = 2009 and month-from-dateTime(.) =
 09
and (day-from-dateTime(.) > 01 and day-from-dateTime(.) < 11)]
```

17.2.3. Job Scheduling

Jobs have a powerful scheduling feature. Job scheduling is available through the Schedule tab in the *Viewer/Editor*.

Jobs may be scheduled for future execution. MIR Administrators can create *Job Queues* for recurring Jobs, allowing them to be scheduled for execution on a regular basis; you can also schedule a one-shot Job without requiring administration access.

See the *Administration Guide* for more details on defining and using Job Queues.

17.2.3.1. Scheduling Jobs

1. Set up a Job, as described previously.
2. In the *Viewer/Editor*, select the **Schedule** sub-tab. You have two options. Either:

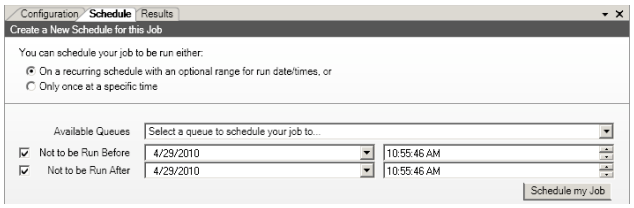
   - For a recurring Job, pick **On a recurring schedule with an optional range for run date/times**.

     This option requires your MIR Administrator to set up at least one Job Queue. Examples of Job Queues might be "every hour on the hour," "every day at noon," or "every time a new host is discovered."

   Assuming queues are available:

   i. In the **Available Queues** selector, choose a pre-defined Job Queue. These include a number of default times ("Every House on the Hour", "Event: On New Host Discovery" and so on) as well as schedules defined by the MIR Administrator.

   ii. If you wish to restrict the time frame in which the Job will run, enable and configure the dates and times in **Not to be Run Before** and/or **Not to be Run After**.



OR

- For a Job that will run only once, select **Only once at a specific time**. This option does not involve your MIR Administrator.

  i. Set **Will be Run Around** to the date and time you want the Job to execute.

3. Click **Schedule my Job** when you are satisfied with its settings. The Job is now queued for future execution.

When Jobs are scheduled they are placed in a queue on the Controller. The Controller checks for due Jobs once every minute. There may be a minor delay between the scheduled time and the time the Job executes.

17.2.4. Audit Item Collection without the Network

In addition to collecting Items from a Host over the network, Agents can collect data locally for later import into a Controller. In this scenario the Agent is typically installed in *Portable Use Mode*, which allows you to take it from system to system using removable media such as a USB flash drive.

17.2.4.1. Collecting Audits in Portable Use Mode

Portable Use Mode configures an Agent's critical files, such as its credentials for communicating with a Controller, so that they can be taken from system to system. Instruction for creating portable Agents is provided in the *Administration Guide*.

You must be familiar with the use of the DOS command line to use a portable Agent.

Assuming the portable device is mounted in the Host system as `E:\` and the Agent is installed in `E:\mir`:

1. On the host system, choose **Start** → **Run**. Then:

   - On Windows 2000, Windows 2003, Windows XP:
     In the **Run** window, type `cmd.exe` and press **Return**.
   - On Windows Vista, Windows 7:
     In the **Start Search** box, type `cmd.exe`. Right-click the `cmd.exe` search result and select **Run as administrator**.

2. Navigate to the drive and directory containing the Agent. For example:
   ```
   cd e:\mir
   ```

3. To see a list of command line options, type the following:

   ```
   miragent -?
   ```

   The command line options are explained in detail in *Appendix D, Agent Command-line Reference*.

   To conduct a portable Audit, you must provide a Script to the Agent so that it knows what Items to collect. The Agent installation includes several sample scripts. In the Job and Audit *Viewer/Editor* s you can export a script; this can be a useful starting point as well.

If you had a Script that performed a *System* Audit, the command for executing that Audit might look like this:

```
miragent -o -script SystemAudit.Batch.xml
```

4. Audit Results are written to the current working directory. The collected Result Set is stored in a directory using the form `.\[audit name]\[hostname]\[date]`. For example, an Audit run on Host *DMERKEL* on *January 13th, 2008* at *9:45am EST*, would be stored in `.\Audits\DMERKEL\20080113144509\`.

   The Result Set directory will contain the following files:

   `Issues.BatchResult.xml`
   Contains errors or other messages that occurred in the Agent while the Audit was executed.

   `BatchResult.xml`
   Contains the configuration passed to the Agent when the Audit was executed. In the Console, hovering over this document will display the version of Agent used to collect the Items in the Audit.

   `mir.module.xml.gz`
   Contains the results returned by the indicated Audit Module.

   `issues.mir.module.xml.gz`
   Contains errors and warnings encountered by the Audit Module while it was executing.

For full details on Portable Use Mode, see the *Administration Guide*.

A portable Agent may also be used for network-based collections. For instance, if you want to avoid a full install of the Agent on a Host system, but still want to collect data over the network, the Agent can be used in Portable Use Mode to avoid having to run the Agent installer. See the *Administration Guide* for more information.

17.2.4.2. Importing Audit Data via the Console

Once Audit Results have been gathered by an Agent in Portable Use Mode, you can import them to the Controller using the Console.

To do this, bring the Audit files (presumably via removable media) to a Console workstation and:

1. Using the **Hosts** Library, open the appropriate Host for these results.

   If an appropriate Host does not exist in the Library, you will need to create a new Host record. See *Section 17.1.1, "Manually Adding and Configuring a Host"* for details.

2. On the *Viewer/Editor* side of the Console, select the appropriate Host tab.

   Click  **Import Audit**. Browse to the portable media device and locate the directory that contains the Result Set for this Host. Select it and click **Ok**.

   The Console expects the Result Set directory name to start with a date-time string in the form of *`YYYYMMDDHmmss`*; e.g., `20080113144509`. You may append an

"extension" to the *YYYYMMDDHmmss* assigned name, e.g., `20080113144509 File API`.

If the directory to be imported is not named with a leading date-time string, the Console will notify you of the error.

3. You can view the import progress using the **Downloads** tab on the left side of the Console.

By default imported Result Sets are named using the hostname and the execution time as recorded by the Agent. The creation and modified times correspond to the time the Result Set was imported. An **.imported** Label is automatically applied to all imported objects. An issues document is created for each module, even if no issues were generated. Also, document links in the `BatchResult.xml` file will not be functional.

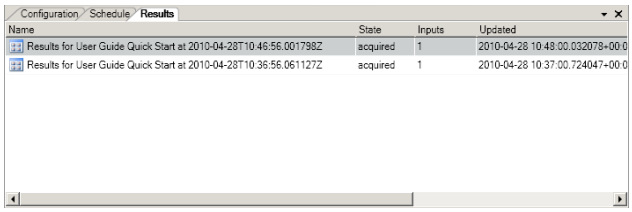
17.2.5. Viewing Job Results

Each time a Job is run, the Items it collects are packaged as a time-stamped Result Set; each set contains Host Audit Results and Analysis Results; both of these contain any Documents containing Items generated by an Audit Module.

Result Sets are listed in the *[job name]* tab, in the upper part of the **Results** sub-tab. Selecting a Result Set displays its contents in the lower part of the viewer, in either the **Audits** Results tab or the **Analyses** Results tab, depending on its type.

Double-clicking a Result Set, Audit Result, or Analysis Result will open a view of that item. You can use the  **Back** button to return the Job *Viewer*.

If you use the Job *Viewer/Editor* to run a Job manually, the display will automatically select the **Results** tab. To view results for other Jobs, open them from the **Jobs** Library and select the tabs manually. The following screenshot shows the results for a typical job.



By default, the following columns are displayed in the Results list:

Name
: The Result Set name. By default, the Result Set is named after the Job that created it. Sorts alphanumerically.

State
: The running state of the Job that created (or will create) the Result Set. Valid values are `Pending`, `Running`, and `Acquired`.

Inputs
: The number Hosts targeted by this Job.

Updated
The last date the Job was updated. Sorts chronologically.

Updater
The MIR username of the user who last edited the Job.

Created
The date and time (according to the Controller) the Job was created.

Creator
The MIR username of the user who created the Job.

Mimetype
The MIME type of the resource.

Href
The URI for this Item or Resource record.

By default, the following columns are displayed in the **Audits** Results and **Analyses** Results lists:

Name
The Result name. This name is automatically derived from the Job name and the hostname for the Agent that supplied the Result. Sorts alphanumerically.

Hostname
The name of the Host from which the Result was obtained.

State
The running state of the Job that created (or will create) the Result. Valid values are `Pending`, `Running`, and `Acquired`.

Errors
The number of errors encountered in running the Job against this Host.

Documents
The number of Documents in this Result.

Host Href
The URI for the Host resource.

ResultSet Href
The URI for the ResultSet resource.

Updated
The last date the Job was updated. Sorts chronologically.

Updater
The MIR username of the user who last edited the Job.

Created
The date and time (according to the Controller) the Job was created.

Creator
The MIR username of the user who created the Job.

Href
The URI for this Item or Resource record.

Mimetype
The MIME type for this item.

17.2.6. Scripts versus Jobs

As previously discussed, Jobs and Scripts are used to specify the what, where, and how of Item collection and analysis. To recap:

Script
A Script is a series of instructions for conducting a Host Audit, an Analysis, or an initialization of Resources through the Console. They are commonly called Host Audit Scripts, Analysis Scripts, or Client Scripts.

Job
A Job is a Host Audit Script or Analysis Script with added information about inputs to the script. Host Audit Jobs provide a list of Hosts/Agents on which the Script will be run, while Analysis Jobs provide a set of input Resources against which to execute the Script.

In short, Jobs contain Scripts, which list actions to take. A Script cannot be executed without a Job, which specifies the inputs to the Script, whether they are Hosts or Documents within the system.

17.2.6.1. Why Use Scripts

In previous sections, the examples focused on direct creation of a Job. When a Job is created directly, a Script is also created. However, when a Script is created in this fashion it is not addressable as a separate object. That is, the only way to manipulate that Script is through the Job that contains it.

On the surface, it may appear that Scripts are superfluous. You can do any collection or analysis task by using Jobs. However, Scripts have two very useful attributes:

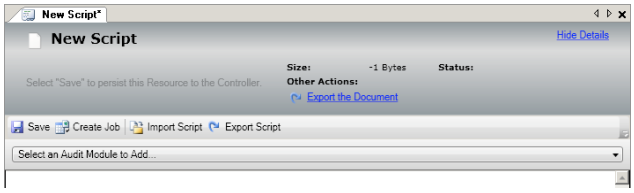
Scripts can be exported and imported
The commands and parameters to collect or analyze Items are useful, and may be deployed on multiple MIR environments.

For example, if two users, each with their own deployment, want to exchange the parameter settings to conduct a specific Host Audit (perhaps an Audit that gathers specific Indicators of Compromise), they can do so with Scripts. The commands to be executed (e.g., Agent Modules or Analysis Commands) and their associated parameters are shared, but not information about any of the inputs to the Scripts (e.g., specific Host information or Documents from within the system).

Scripts can be easily reused
If a series of commands is often used, a Script can be created once and then reliably reused with different sets of inputs. While a Job could serve the same purpose, the Script

is cleaner, acting as a Job "template." When used properly, Scripts are a powerful workflow enhancement tool.

Scripts are developed using a *Viewer/Editor* that is like the one used in the **Configuration** tab in a Job, but lacking the (unnecessary) **Targets** area.



17.2.6.2. Creating and Using Scripts

Creating a Script

1. Choose **File** → **New** → **Host Audit Script** or **Analysis Script**. A tab labeled **New Script** will be opened on the right.

2. Choose Audit Modules or Analysis Commands suitable for the Items you wish to collect or transform. Each module or command you choose will be listed below the selector; if it has configurable parameters, those settings will be shown.

   See *Appendix A, Audit Modules and Analysis Commands* for description and parameter details.

3. Click **Save** to finish. You will be prompted to name the Script. The **New Script** tab name will be replaced by the new name.

Creating a Job from a Script

To create a Job from an existing Script, add Targets to it.

1. Using the **Scripts** Library, open the Script.

2. Click the **Create Job** button in the *Editor* tool bar. A tab labeled **Custom Job from...** will be created.

3. Select the **Configuration** tab and add **Targets** to the Job.

   For Host Audit Jobs, you can drag resources from the **Hosts**, **Labels**, and **Saved Searches** Libraries to the **Targets** area.

   For Analysis Jobs, open the Job or Host that generated the Result Documents you wish to analyze. Select the first (*Left*) document, **Ctrl+C** copy it, then return to the Job and **Ctrl+V** paste it into the **Targets** area. Repeat for the second (*Right*) document.

4. When you are finished designing the Job, click **Save**. You will be prompted to name the Job. The **Custom Job from...** tab name will be replaced by the new name.

Note that if a Script from the Library does not capture all the information you seek, you can add more modules or commands to the Job you are creating.

17.2.6.3. Importing and Exporting Scripts

Scripts can be exported or imported using the *Editor*.

Exporting a Script from the Console

1. Open an existing Script or Job, or create a new Script or Job.
2. Click the **Export Script** button in the *Editor* tool bar.
3. Choose a location in which to save the Script, as well as a filename, and click **Ok**.

If you examine the Script directly, you will see that it is an XML document. Scripts can be manipulated manually if they adhere to the schema for MIR Host Audit and Analysis Scripts [1].

Importing a Script to the Console

1. Open a Script or Job, or create a new Script or Job.
2. Click the **Import Script** button in the *Editor* tool bar.
3. The Script will be loaded into the *Editor*. Click **Save** to save it to the Controller.

Importing a Job to a Portable Agent

Jobs exported from the Console must be modified before they are compatible with Portable Agents. MANDIANT provides a script that automates the conversion process [2]:

1. Export a Job as described in *the section called "Exporting a Script from the Console"*.
2. Open a Windows command prompt and change to the directory where you saved the script (e.g. `cd directory`).
3. To convert a single file:
   - Type the following at the command prompt:
     `clientExportToAgent.bat script.xml`
     The converted script will be named `script.batch.xml`.
4. To convert many files:
   - Type the following at the command prompt:
     `clientExportToAgentScriptMany.bat regex destination path` + The converted scripts will be saved to the destination path, using the *`script.batch.xml`* naming pattern.

[1] You may contact MANDIANT Technical Support for more information regarding data object schema.
[2] Available for download at *https://forums.mandiant.com/topic/jobs-on-the-run-exporting-scripts-from-the-console-to-use-with-portable-agents#post-11*

17.2.6.4. Using Favorite Scripts

Scripts can be marked as *Favorites*, which allows you to easily access them from the context menu of any Host. Using *Favorites*, you can quickly pick a Host or set of Hosts against which to run a Script and launch a Job.

Creating Script Favorites

1. Create a Script using the *Script Editor* (not the *Job Editor*).
2. Save the Script and name it. While still viewing the Script in the *Editor*, click **Add to Favorites** in the tool bar.

Using Favorite Scripts

1. Open a Host tab.
2. Click the **Create Audit** or **Run Audit** button and pick a favorite Script from the menu.

   Create Audit will create a new Host Audit Job populated with the Hosts and the Script.

   Run Audit will immediately run an Audit against the Hosts using the Script.

Sharing Indicators

Indicators may be exported and imported for sharing with other Controllers or MIR installations. As well, while many Indicators can be built using the Editor, there may be circumstances where you need to use more powerful expressions: in these cases, you might wish to export, hand-edit, and import the changed Indicator.

IOC files are the primary method of storing Indicators when they are not on a MIR Controller. They are XML files that adhere to a specific schema specified by the MIR platform. Creating, modifying, and saving these files is a simple procedure.

Exporting Indicators

1. In the **Indicator** Library, select one or more Indicators.
2. Right-click the selected Indicators and choose **Export Selected Indicators...** or **Tools** → **Export Selected Indicators...**. A standard folder selector window will be displayed. Select the destination folder for the exported Indicators.
3. The Indicators will be saved as separate `.ioc` files to the destination folder. These are XML files and may be opened using any common text editor.

Editing Indicators by Hand

IOC files are well-structured, schema-validated XML files. If you wish, you can open these files using a plain text editor or an XML editor, and manipulate the IOC definitions manually. This is an advanced task requiring knowledge of XML conventions.

Importing and Updating Indicators

On occasion MANDIANT may release updates to the default set of Indicators; as well, you may have opportunities to use Indicators from other MIR installations, or bring Indicators forward from a previous version of the Controller. In all cases, you will use the import tool.

Importing a MANDIANT IOC Update or other Indicators

To update your IOCs:

1. Copy the update folder, containing multiple `.ioc` files, to the workstation on which you are running the Console.

2. Choose **Tools** → **Import Indicators...**. A new window will open, titled **Upload IOCs**.

3. Select the first tab, titled **Choose Source**.

4. Click the top button, labeled **I am uploading an IOC update provided by MANDIANT containing multiple .ioc files**. A standard folder selector window will be displayed. Select the update folder you copied to the workstation and click **Ok**.

   When you have selected the update folder, the **Upload IOCs** window will automatically move to the next tab, titled **Configure Target**.

5. Provide your login credentials for the Controller URI (shown in the Console status bar, on the right) and your username and password.

6. Choose how collisions between existing IOC IDs and imported IOC IDs will be handled:

   - If you want the imported IOCs to replace existing ones in all cases, select the first option, **Replace all IOCs with the same ID regardless of modified date**.

     This is the option you will normally choose when performing a MANDIANT-supplied IOC update.

     OR

   - If you want the imported IOCs to replace existing ones only when the imported IOC is newer, select the second option, **Replace all IOCs with the same ID when the imported IOC is newer**.

     OR

   - If you do not want any IOCs to be replaced, select the third option, **Do not replace IOCs with the same ID**.

   You may choose to attach a label to IOCs which could have been replaced but were not (options b and c, above), so that you may easily open them in the Console for closer examination. If this is the case, select **Label IOCs with the same ID which are not replaced** and provide a new or existing label name.

7. In most cases, you should perform a test run of the import to check for IOC collisions. Click **Check for Collisions** to do so. The **Review Collisions** tab will be automatically selected, and after a few moments the list of IOCs will be updated to show which ones collide.

Selecting an IOC will show the modification dates for the importing and existing IOCs.

You may return to the **Configure Target** tab to adjust the collision-handling options, or you may uncheck **Upload** for individual IOCs to prevent them from being part of the update.

8. The new IOCs are now ready to be imported. Click **Upload IOCs** to start the import process. The button will provide upload progress.

9. When the IOCs have been uploaded to the Controller the **Upload Report** tab will be automatically selected. This tab presents detailed information on the upload.

10. You may now choose another update source by returning to the **Choose Source** tab and repeating this process, or close the **Upload IOCs** window to return to the Console.

17.3. Viewing Results

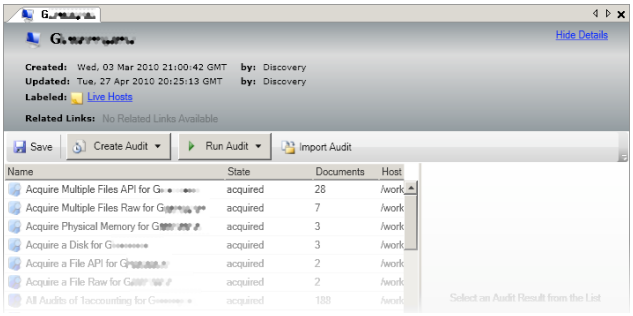
Once Results have been collected, you can use the Console's search, sorting, and filtering tools to further your investigation. Some of these tools provide familiar interfaces similar to many common office productivity applications; others provide far more powerful data-mining capabilities. You can also export Results, so that you can manipulate them directly with your own analysis tools.

17.3.1. Navigating to Your Resources and Items

Audit Results and Analysis Results ultimately contain the information you want. You have several options for navigating to Results, depending on how they are organized:

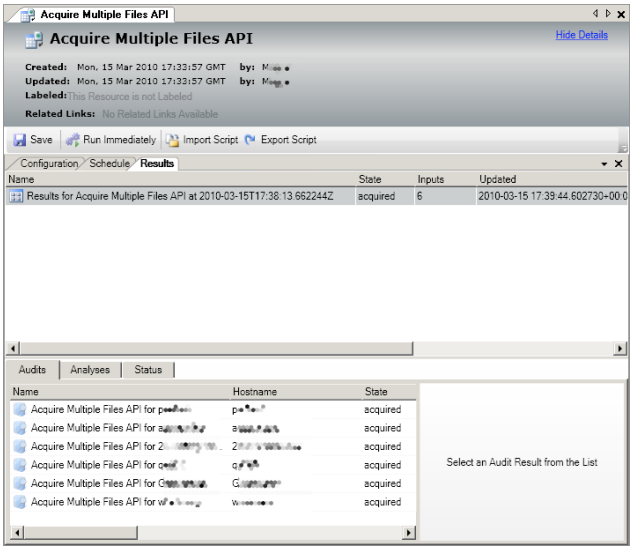
Through the Host Library

Every Host record maintains a list of its associated Audit Results. If you mentally organize your investigation efforts by Host, you will most often use the **Hosts** Library to navigate to the Results you seek. When you open a Host by double-clicking its Library entry, the Console lists all the Result Sets that have been obtained from that Host.



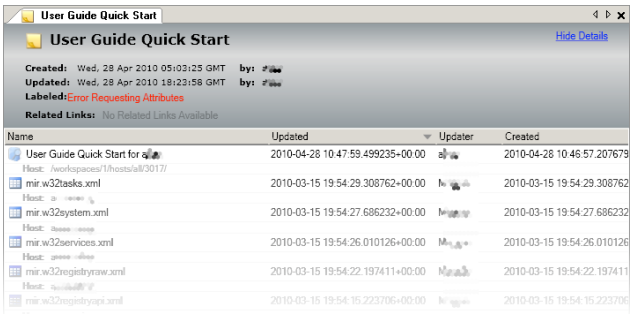
Through the Job Library

Every Job within the system maintains a list of all Result Sets created by that Job. If you tend to think of your investigations through the use of Jobs, you can use the **Jobs** Library to retrieve the Result Set you seek. When you open a Job by double-clicking its Library entry, and select the **Results** sub-tab, the top half of the *Viewer* displays a list of the Result Sets associated with that Job; the bottom half displays the contents of a selected Result Set.



Through Labels

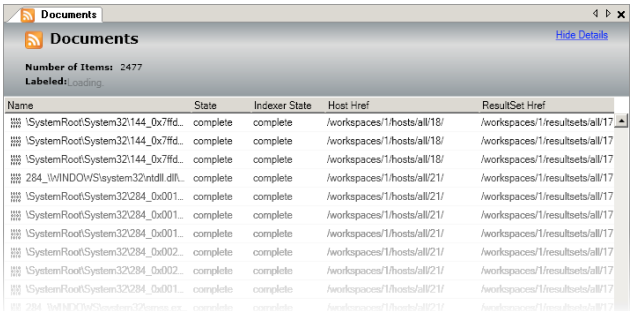
If you apply Labels to Audit Result Sets, you can easily find them again by using the **Labels** Library. When you open a Label by double-clicking its Library entry, a *Viewer* pane will show a list of Results tagged with that Label.



Through Audit and Analysis Results

In all cases, the Audit Result and Analysis Result Libraries — accessed using the **Libraries** menu — list every Result known to the Controller.

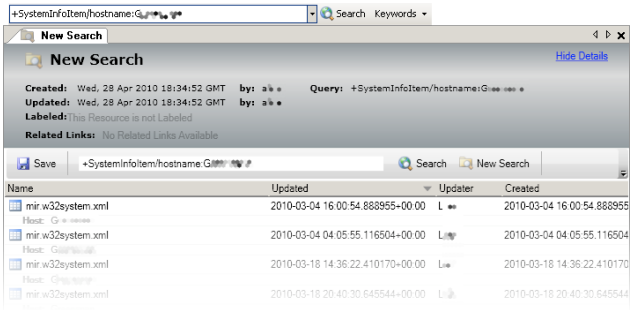
Note, however, that unless you have uniquely named the Results, finding them through these Libraries can be challenging. See *Section 15.3.1, "The Libraries Tab"* for more information.



By Searching

One of the most powerful ways to navigate to Results is with the Search feature. Basic use of the search feature is simple: type a string you wish to find in the **Search** box and click on the **Search** button. A new tab in the *Viewer/Editor* pane will display a list of Documents that match your search request.

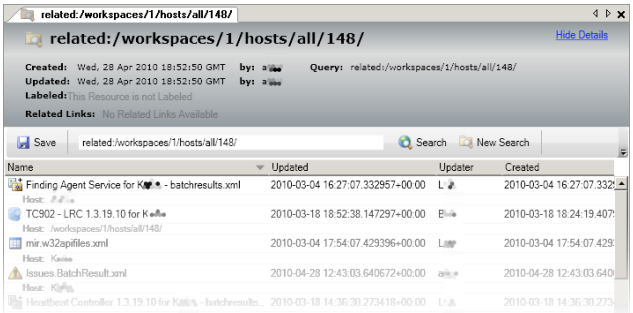
Searches can be far more complex than that, however: logic operators and keyword qualifiers can be used to greatly reduce the list of results, helping you find the results you seek more quickly. For full details on using the Console search features, see *Chapter 18, Using Search on Audit Results*.



By Finding Related Resources

The Controller understands the "relationship" some Resources and Results have with one another. For example, it knows that Hosts are related to a series of Audit Results and Audit Documents, as well as the Jobs that have been run against them and the Items they acquired.

When you have identified a Resource or Result that is associated with the information you seek, you can right-click its entry and select Find* Related Resources* from the context menu. A new tab titled **Related...** will be displayed, listing everything related to that Resource or Result.



17.3.2. Views

When you have navigated to the Results you seek, you will want to view them. The Console provides a number of *Viewers*:

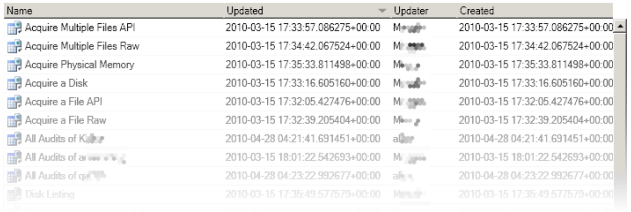
List Views

List views are a common view, providing a simple spreadsheet-like table view of information. Each row of the table represents a single Item or Resource, with each

column entry presenting information about the Item or Resource. You have probably encountered this type of view already; it displays the contents of Libraries, for instance.

The columns displayed in a List view can be customized by right-clicking a column header and selecting the columns that are to be displayed or hid. Rows in the list view can be sorted by the contents of a white column by clicking the column header. The content of columns with a light blue background is not sortable; clicking a blue column header will have no effect.

Lists may be sorted and filtered by choosing **Data** → **Sort List...** and **Data** → **Filter List...**. See *Section 15.3.1, "The Libraries Tab"* for more details about available List views and their associated columns.

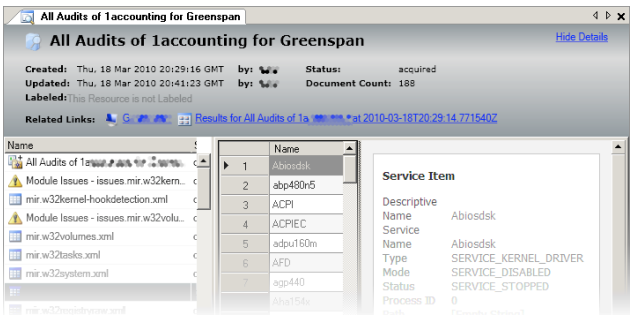


Result Views

Result views display the contents of an Audit or Analysis. This view is relatively complex, comprising three panes of information. At the top of the view is a descriptive overview of the Job that created the data, with clickable links to related resources. The left side of the view displays a list of Documents; when a Document is selected, the right side of the view lists the contents of the Document.

As with List views, columns can be customized and clicking a column header sorts the contents of the table.

See *Appendix A, Audit Modules and Analysis Commands* for full information about the content of Audit Results and Analysis Results views.

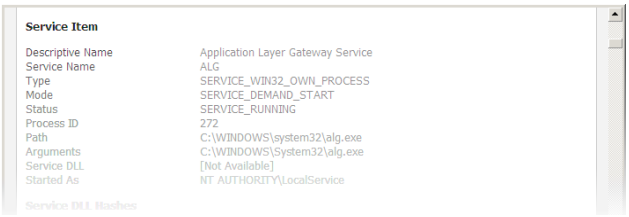


Grid Views

The Console displays most information in the system as a grid, which behaves in a manner similar to common spreadsheet applications. Grids are typically used to display the content of Host Audits and Analyses. Items are displayed in rows, and the column headers describe each entry in the row. The grid can be sorted or filtered on each column or multiple columns by clicking on column headers or choosing **Data** → **Sort...** or **Data** → **Filter...**. See *Section 17.3.3, "Sorting and Filtering"* for more details.

Detail Views

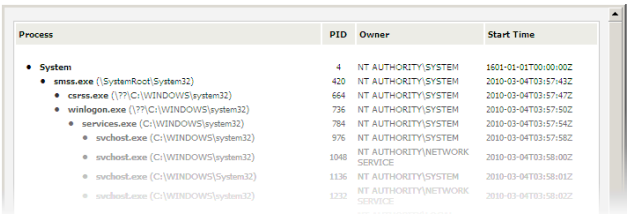
Grid views may have an additional Details view for some Items in an Audit or Analysis. These views expose more information about an Item that may not be possible to display in a common Grid view.



Alternate Views

Some Document selections provide special-purpose views for particular types of information. A *Processes* listing, for instance, can display a hierarchical tree view; a *Ports* listing can display a netstat-style view.

These views are displayed as sub-tab options in the *Viewer*, as optional choices in the **View** → **Views** menu, and through the **Views** button in the main tool bar.



Binary Views

Items which the Console does not natively know how to display are displayed in Binary view. In this view, the left column displays the offset address, the middle columns display hex values for the data, and the right column displays the ASCII representation of the data.

17.3.3. Sorting and Filtering

The Console provides powerful sorting and filtering tools for use in List and Grid views.

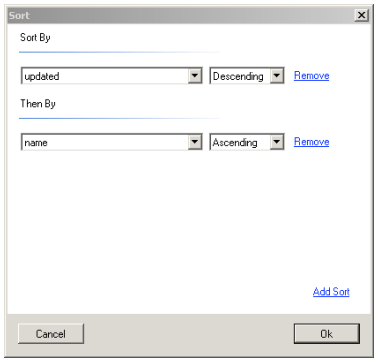
White column headers provide simple sort-order functionality, as described previously: clicking a column header sorts the rows by the values in the column, and clicking it a second time sorts the rows in reverse order. (Blue column headers do not provide sort functionality.)

More advanced sorting and filtering options are available through the **Data** menu, which provides **Sort...** and **Filter...** commands that allow complex expressions. This menu also provides commands for removing sorts and filters, and will display context-appropriate shortcuts for searching and filtering based on the currently-selected item.

17.3.3.1. Sorting

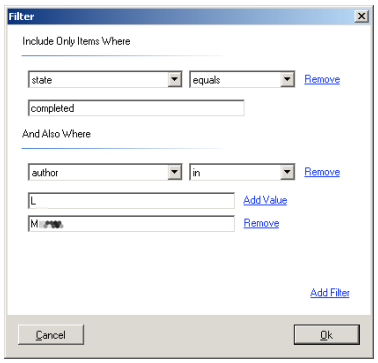
Sorting a List or Grid view is done in a manner common to spreadsheets. As previously mentioned, simple single-column sorts can be made by clicking on column headers. To do a multi-column sort, choose **Data** → **Sort...**. A **Sort** settings window will allow you to set more sort criteria for multiple columns.

For each sort criterion, select a column to sort from the drop-down list and then specify **Ascending** or **Descending** beside it. To add more criteria, click **Add Sort** at the bottom right of the window. To remove a criterion, click the **Remove** link next to that item. To perform the sort, click **Ok**. Subsequently clicking a column header will revert the order to a simple single-column sort.



17.3.3.2. Basic Filtering

Filtering hides row entries in a List or Grid view, reducing the items listed. To specify a filter, select **Data** → **Filter...**. A **Filter** settings window will allow you to set filter criteria based on the values of column entries in each row.



For each filter criterion, select a column against which a comparison will be performed; in the adjacent selector, choose the comparison operation (for example, **equals**, **does not end with**, **is null**, and so on). In the entry box below the column selector, type the value against which the column entry will be compared.

To add more filter criteria, click **Add Filter** at the bottom right of the window. To remove a criterion, click the **Remove** link next to that item. To view the filtered List or Grid view, click **Ok**.

Different filter operators will be displayed depending on the data type of the column selected:equals:: Matches entries that are identical to the specified value.

does not equal
Matches entries that are not identical to the specified column.

greater than
Matches entries that are greater than the specified value. (Numeric and Date/Time columns only.)

greater than or equal
Matches entries that are greater than or equal to the specified value. (Numeric and Date/Time columns only.)

less than
Matches entries that are less than the specified value. (Numeric and Date/Time columns only.)

less than or equal
Matches entries that are less than or equal to the specified value. (Numeric and Date/Time columns only.)

between
Matches entries that are between two specified values, inclusive of the values. (Numeric and Date/Time columns only.)

not between
Matches entries that are not between two specified values, inclusive of the values. (Numeric and Date/Time columns only.)

starts with
Matches entries that start with the specified value. Case sensitive. (String columns only.)

does not start with
Matches entries that do not start with the specified value. Case sensitive. (String columns only.)

ends with
Matches entries that end with the specified value. Case sensitive. (String columns only.)

does not end with
Matches entries that do not end with the specified value. Case sensitive. (String columns only.)

like
Matches entries that match wildcard value. % is the wildcard character for use in filters. For example, `%foo%` would match all values in a column having *foo* as part of the string. (String columns only.)

not like
Matches entries that do not match a wildcard value. % is the wildcard character for use in filters. (String columns only.)

in
Matches entries equal to any one of the specified values. Click **Add Value** to add additional values for comparison. Click **Remove** next to a value to remove it from the filter.

not in
Matches entries that are not equal to any of the specified values. See the *in* operator, above.

is null
Matches null entry values . Note some fields that show `0` (zero) may match *is null*, instead of *equals* with a value of `0` (zero).

is not null
Matches entries that are not null. See the *is null* operator, above.

To remove all filters, select **Data** → **Reset Filter** → **filter description** or right-click a column header and select **Reset Filter**.

Time values may be entered as `YYYY-MM-DDTHH:MM:SSZ` or `MM/DD/YYYY HH:MM:SS XM`.

17.3.4. Viewing Results using External Programs

The **Open with...** command lets you open a MIR resource using an external program. For convenience, several alternative tools have been pre-configured for your use; these include Microsoft Internet Explorer, Firefox, MANDIANT Web Historian, MANDIANT Highlighter, and MANDIANT Redline. You may easily add more tools to the command.

Only those applications known to be compatible with the selected data are listed in **Open with...**. For instance, MANDIANT Redline is available only when viewing Audits; Windows Explorer if there are files that can be viewed; Firefox if the data can be presented as a link to the Controller.

17.3.4.1. Opening a MIR Resource in an External Program

While viewing a list of resources:

1. Right-click the resource you wish to open in an external program.
2. Select **Open with...** and choose an external program.

   The resource will be downloaded to your local disk (`%temp%` by default) [3]. Most resources are downloaded as a single file. Audit Results are an exception: they result in the creation of a sub-directory, as if you were storing an offline Audit. The **Downloads** window will show a progress bar for the download.

   When the transfer has finished, the selected external program will run with the downloaded file or directory as its command line argument.

[3] FireFox is configured to access the resource URL, bypassing the download step. This behavior is not available for other external programs.

Windows maximum path length restrictions may create issues when saving the resource. To avoid this problem, we recommend configuring external programs to use a short root path.

17.3.4.2. Configuring Open With

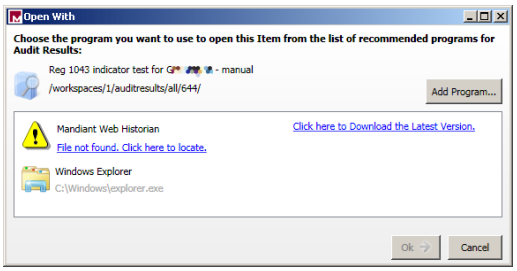
The destination directory for data exported to external programs can be configured:

1. Select **Tools** → **Options...**.
2. In **Open With Cache Location**, set the directory path for the exported files. You may use the standard Windows environment variables (`%temp%`, `%homepath%`, etc.)

17.3.4.3. Adding External Programs to the Open With Menu

While viewing a list of resources:

1. Right-click a resource.
2. Select **Open with** → **Choose Program...**. An **Open With** window will be displayed, with an **Add Program...** button and a list of known programs.



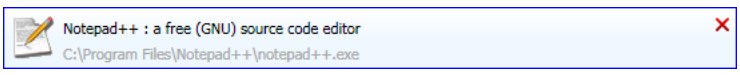
3. Click **Add Program...** to add a new program to the list. A standard file selection window will allow you to navigate to the program. Click **Open** to add the program to the list.

   For MANDIANT tools, a **Click here to Download the Latest Version** link will fetch the software; you can then run its installer and subsequently make use of the application.

17.3.4.4. Removing an External Program from the Open With Menu

While viewing a list of resources:

1. Right-click a resource.
2. Select **Open with** → **Choose Program...**. An **Open With** window will be displayed, with an **Add Program...** button and a list of known programs.
3. Select the program you wish to remove and click the red **X** on the right. The program will be removed without confirmation.



17.3.5. Exporting Data

Audit Results are easily exported so that you can manipulate them with other software, such as image viewers, spreadsheets, or scripts. Audit Documents, acquired files, and disk images can all be exported using the Console.

You can also export Job Scripts, both for use with Portable Use Mode Agents, and so that you can share them with other MIR deployments or users. See *Section 17.2.6, "Scripts versus Jobs"* for more information about sharing Scripts.

To export documents, acquired files, or disk images, select them in a List or Grid view. You can then choose **Tools** → **Export document...** or right-click the entry and choose **Export Document...**.

Host Audit and Host Analysis data is stored as XML. Schemas for these documents have been provided on your documentation CD.

Acquired files are stored in the original format, and disk images are stored as bit-for-bit **dd** (*"convert and copy"*) images.

17.4. Organizing Results

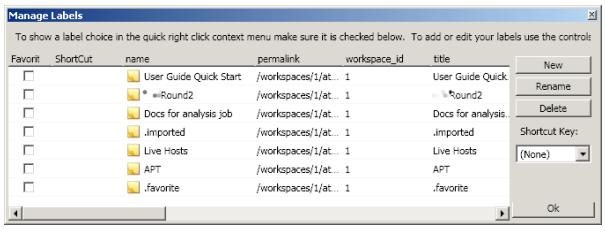
The Console uses Libraries and Labels as the main methods for data organization within the system. Library behavior is discussed in detail in *Section 15.3.1, "The Libraries Tab"*. This section discusses the use of Labels to organize information, which allows you to arbitrarily group Resources and Items according to your personal workflow.

Labels can be applied to anything that can be listed. The application of a Label in no way changes the information it tags; but applying a Label makes it very easy to open a *Viewer* that displays everything that has been given a particular Label. You can also apply multiple Labels to things, which allows you greater flexibility in organizing your work.

17.4.1. Creating and Managing Labels

Labels are created and managed by choosing the **Tools** → **Manage Labels...** command, which opens a **Manage Labels** window. This window is simple and self-explanatory: on the left is a list of Labels and on the right, buttons for managing Labels.

Labels can be created, renamed, and deleted. When a Label is marked as a **Favorite** it will appear at the top the **Tools** → **Label...** menu and item/resource right-click **Label** menu, making it easier to apply the Label. Labels can also be assigned a **Shortcut Key**, allowing you to quickly apply a Label to entries by highlighting them and using the assigned key sequence.



Favorited Labels are saved at the local level: they are not saved to the Controller.

There are two special Labels: *.imported* and *.favorite*. These are used to identify imported audits and to “favorite” bookmarked objects respectively. The “ . ” at the beginning of the Label name indicates their special system-generated status. You cannot create Labels that begin with “ . ”.

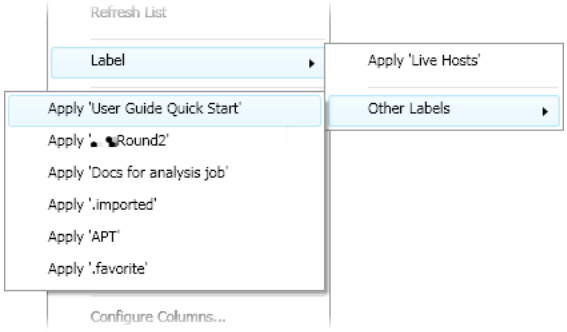
17.4.2. Applying and Removing Labels

Applying and removing Labels is simple: select the entries to be labeled, choose **Tools** → **Label...**, and select a Label to be applied or removed; alternatively, select the entries, right-click, and choose a Label. When a Label is applied, a checkmark will be placed beside its name in the menu; to remove an applied Label, select it again.

The **Labels...** sub-menu lists your favourite Labels only; choose **Labels** → **Other Labels...** to see the remaining Labels.

If you have assigned a shortcut key for a desired Label, simply select the objects to be labeled and use the shortcut to apply or remove the Label.

When it is applicable the **Tools** menu displays several labeling options dependant on the selected objects.



17.4.3. Viewing Labeled Objects

To see which objects have been given a specific Label, open the Labels Library and double-click the Label name. On the right, a *Viewer* will list all objects that have been assigned that Label.

17.5. Analyzing Data

Investigations often involve poring through data to find information that is relevant to the matter at hand. MANDIANT Intelligent Response provides several analysis tools to manipulate data after it has been collected. These analysis features provide you with several tools to minimize information down to a manageable set in quickly and efficiently.

Once you have collected data from Agents, you can review it and perform various actions on it to better understand whether it is relevant to your investigation or incident. The Controller provides a set of Analysis Commands — operations that can be performed on data after it is collected — that allow you to compare and contrast sets of information.

This section describes how to set up and run Analysis Jobs. See *Appendix A, Audit Modules and Analysis Commands* for full details on Analysis Commands, their required parameters, and output.

17.5.1. Setting Up an Analysis

Analyses are run via Analysis Jobs, which are very similar to Host Audit Jobs; they are configured and launched through a Job Editor using a similar user interface.

17.5.1.1. Running a Timeline Analysis

Timeline combines documents into a single time-ordered list.

1. Choose **File** → **New** → **Analysis Job**. A new titled **New Job** will be displayed to the right.
2. In the **Targets** box, drag or paste any number of Documents to be time-lined.
3. Using the **Select an Analysis Command to Add...** selector, choose **Timeline**. A **Timeline** Analysis Command will be inserted below the selector.
4. In the **Timeline** command area, click **Choose a Field...** and select the time field that will be used to place the document items into the time line. The **Document Type** field will be automatically completed when you select the time field.

   Click the **+** button to add an entry for each type of document.
5. Click **Run Immediately**. When the Job is complete, a new document with data listed in time-order will be created and displayed.

17.5.1.2. Running a Time Skew Analysis

Time Skew adds or subtracts a set value from all time values in documents.

1. Choose **File** → **New...** → **Analysis Job**. A new titled **New Job** will be displayed to the right.
2. In the **Targets** box, drag or paste any number of Documents to be corrected.
3. Using the **Select an Analysis Command to Add...** selector, choose **Time Skew**. A **Time Skew** Analysis Command will be inserted below the selector.
4. In the **Time Skew** command area, specify the **Offset** in hours, minutes, and seconds. The format is *hh:mm:ss*.

   For example, `00:00:10` will add 10 seconds to all date/time values contained in the input Documents. To subtract times, specify a negative value. For example, a value of `-10:30:10` will subtract 10 hours, 30 minutes, 10 seconds from those values.
5. Click **Run Immediately**. When the Job is complete, a new document with corrected time values will be created and displayed.

Time Skew creates a new document with the same name as the source document, with a tag at the end showing the skew value.

For example, adding 10 seconds skew to a file originally named `mir.w32rawfiles.08d8a1a8.xml` would create a file named `mir.w32rawfiles.08d8a1a8-PT10S.xml`.

17.5.1.3. Running a Document Difference Analysis

Document Difference compares two documents and lists the differences between them.

1. Choose **File** → **New...** → **Analysis Job**. A new titled **New Job** will be displayed to the right.
2. In the **Targets** box, drag or paste two Documents to be "diffed."

   Unlike other Analyses, the order of the inputs is relevant to *Document Difference*. The first input in the Targets box is "*Left*." The second input in the Targets box is "*Right*." Document Difference will only use the first two inputs. Any others provided in the Targets box will be ignored.
3. Using the **Select an Analysis Command to Add...** selector, choose **Document Difference**. A **Document Difference** command will be inserted below the selector.
4. In the **Document Difference** command area, click **Choose a Field...** and select the field you wish to compare between the two documents.

   If you wish to compare multiple fields, click the **+** button to add more field entries.
5. Click **Run Immediately**.

17.5.1.4. Running a Document Intersection Analysis

Document Intersection compares two documents and lists the fields that are the same.

1. Choose **File** → **New...** → **Analysis Job**. A new titled **New Job** will be displayed to the right.
2. In the **Targets** box, drag or paste two Documents to be "diffed."

   Unlike other Analysis, the order of the inputs is relevant to *Document Difference*. The first input in the Targets box is "*Left*." The second input in the Targets box is "*Right*." Document Difference will only use the first two inputs. Any others provided in the Targets box will be ignored.
3. Using the **Select an Analysis Command to Add...** selector, choose **Document Intersection**. A **Document Intersection** command will be inserted below the selector.
4. In the **Document Intersection** command area, click **Choose a Field...** and select the field you wish to compare between the two documents.

   If you wish to compare multiple fields, click the **+** button to add more field entries.
5. Click **Run Immediately**.

17.5.1.5. Viewing Analysis Results

1. Open the Job. A *Viewer/Editor* tab will be displayed on the right.
2. On the **Results** tab for the completed Job, select a Result Set resource. The results of the Analysis will be listed in the **Analyses** sub-tab.

3. Double-click the Analysis. On the left, a list of **Documents** will be displayed. When you select a document, its contents will be displayed on the right.

   The following documents should be present in your Analysis:

   `Left Difference.xml` or `Left Intersection.xml`
   Contains the differences or commonalities, respectively, between the first document (*Left*) and second document (*Right*).

   In other words, for a Difference Analysis it lists all the things that are in *Left* that are not in *Right*; or for an Intersection Analysis, all the things in *Left* that are also in *Right*.

   `Right Difference.xml` or `Right Intersection.xml`
   Contains the differences or commonalities, respectively, between the second document (*Right*) and first document (*Left*).

   `Analysis Manifest.xml`
   Contains information about the parameters supplied for the Analysis and any resulting errors.

17.5.2. Viewing the Results of an Analysis

Viewing Analysis Results is no different from reviewing the results from a Host Audit. See *Section 17.3, "Viewing Results"* for details on various data viewing capabilities.

Chapter 18
Using Search on Audit Results

As mentioned in *Section 17.3.1, "Navigating to Your Resources and Items"*, search is one of the best tools for finding the information you seek. The Controller's search engine helps you quickly find only the items you need out of all the data in the system. Audits and Analyses are all thoroughly indexed by the Controller, giving you powerful tools to quickly find what you are looking for.

A powerful keyword construction method, unique to MIR's approach to search indexing, gives you the ability to quickly narrow the scope of information you are reviewing by targeting only those key data that are relevant to your interests.

Some types of audits return vast amounts of data that you may never want to search. To help you manage Controller resource demands, global and per-job settings can exclude audit result categories from indexing. See the *Appendix B, Searches* Appendix for details.

The following types of data are searchable:

- All Result Documents.
- All object metadata.

Files acquired using *w32apifiles-acquisition*, *w32disk-acquisition*, *w32driver-memoryacquire*, *w32memory-acquisition*, *w32process-memoryacquire*, and *w32rawfiles-acquisition* are not searchable in this version of MIR. You can export data of these types and use third-party tools to perform detailed searches.

Any query executed on the Controller will cause memory to be used. This is not generally noticeable on queries against small datasets or on queries against filtered or otherwise limited datasets. However, when doing unfiltered and unlimited queries against large datasets (100,000+ documents), excessive memory can be consumed, leading to a non-responsive controller or out-of-memory errors.

18.1. Concepts and Definitions

Before discussing the search engine, common terms need to be defined:

Category
: Data indexed by the Controller's search engine is divided into *categories*. Categories define different data entities within the system. Every resource within the system is a member of at least one category.

  You can limit searches by using category keywords. For example, the following query would look only inside Audit data for *[term]*, ignoring all other categories of data:

  ```
  +category:/audit +[term]
  ```

  Note that searches by category for documents will return only those documents that contain data. Zero-length documents cannot be returned by a category search.

Content

Content is textual information that is indexed by the Controller. The content of a *File Listing* Audit is the listing of file data returned in the Result Document. The content of the *Path* field for an individual file item from that Audit could be similar to:

```
C:\WINDOWS\SYSTEM32\foo.exe
```

Field

The label for a data element is a self-descriptive *field* name.

For example, in a *File Listing* Audit there are multiple fields of information returned, such as *Path*, *SizeinBytes*, and *Accessed*. Searches can be constrained to specific fields. The following example would search for Documents that contain *Process* items with a *userTime* field value of *[term]* :

```
+processItem/userTime:[term]
```

When doing a search with no fields, all indexed items within a document are searched.

Identity

Every Resource in the system has a unique ID called an *identity*. In text, identities look like a path to a document on a file system or web site:

```
/workspace/1/hosts/all/1/
```

Keyword

Special instructions to limit the scope of a search to specific fields, categories, or document types are called *keywords*.

Metadata

Metadata is "data about data." Creation dates/times, names of objects, modification history — all these things are *metadata*.

Search Operators

The logic components of a search query are called *operators*. Boolean logic, range indicators, and groupings are operators that make it possible to construct complex search queries.

Boolean operations applied to Audit Results provide row-level granularity, allowing you to specify a combination of fields and terms identifying a specific row.

For example, a *File Listing* will show a single filename and file size on each row: you can construct a boolean search that seeks a particular filename *and* file size, but you cannot make a search that seeks a particular filename *and* another filename, as the latter would require search to span rows.

For Documents that are not row-oriented, boolean searches apply across the whole document: for instance, searching for a particular filename *and* another filename.

Search Query

The full search definition, constructed of terms, operators, and keywords, is a *query*.

Search Term

Terms are the string components of a search query. Multiple terms can be combined using search operators to form complex queries (see *Section 18.4, "Search Syntax"* for details).

There are two types of terms: *Single Terms* and *Phrases*.

Single Term

A single word such as *test* or *hello*. If multiple single terms are provided, the search will find documents that contain all the terms, in any order.

Phrase

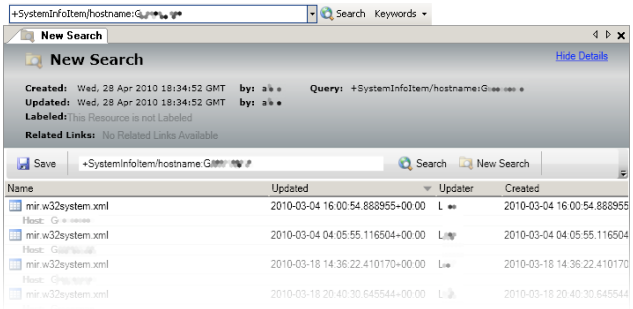
A group of words surrounded by double quotes such as *"hello dolly"*. The search will find documents that contain all the words, in the order specified.

18.2. Using the Search Bar

Search queries can be typed directly into the search box in the Console tool bar:

Search queries must adhere to the formal syntax (see *Section 18.4, "Search Syntax"*) and can be directly typed into the search box, followed by pressing **Return** or clicking the **Search** button. Results will be returned in a *Viewer* tab named **New Search**, with a list of matching documents and the number of "hits" for the query within each document.

Additional searches can be run against the documents listed in the **New Search** tab. Enter the search query in the tab's search box and click **Search** or **New Search**. The former will re-use the tab, while the latter displays results in another tab.



18.3. Saving Searches

Search queries can become quite complex with the introduction of keywords, operators, and multiple terms. As you develop discovery and analysis workflows you will find that some searches are performed frequently. In these cases, you may want to save a search for re-use.

In the **New Search** tab, clicking the **Save** button will prompt for a name for the search query, then save it in the **Saved Searches** Library. Double-clicking a saved search will execute the search and display the results in a new tab.

18.4. Search Syntax

By default, the Controller will search for any terms you enter as a search query. If you type in the words *duck*, *goose*, and *bear*, it will search all the information stored within the system

and return anything that has the words duck, goose, *OR* bear. Note the use of *OR* in this context: by default the search engine tries to find a match for anything you have entered as a search query.

By understanding the syntax of search queries, you can modify this behavior to better match your intentions when conducting a search.

18.4.1. Special Characters

The following characters are treated as special by the search engine:

```
+ - && || ! ( ) { } [ ] ^ " ~ ? : \
```

This means that if you want to search for these characters, you must "escape" them by prepending the backslash "`\+" escape character. For example, to search for "+C:\windows\system32\calc.exe+", which contains a colon and several backslashes that need to be escaped, you would enter: +C\:\\windows\\system32\\calc.exe`

Whitespace is also treated as special and should be escaped if the search term is not contained in quotes. For example, if you were searching for the path "C:\Program Files" you would represent that as:
`C\:\\Program\ Files`
or
`"C\:\\Program Files"`

18.4.2. Case-Sensitivity

Keywords in search strings are case-sensitive, but the search term itself is not. For example, the following search fails to produce results because of the upper-case *N* in the *Name* keyword:
`PortItem/localPort:20155 ProcessItem/Name:MIRAgent`

To ensure proper case when using keywords, use the **Keyword** selector.

18.4.3. Boolean Operators

Boolean operators allow terms to be combined logically. Valid Boolean operators are:

AND
OR
NOT

Boolean operators must be ALL CAPS to be recognized by the search engine.

Remember, per *Note*, search queries across Audit Documents are "by row." Boolean operators in search terms for Audit Documents help create a search that more accurately matches individual rows, not entire Documents. For other forms of documents, boolean search operators span the whole document.

18.4.3.1. Boolean OR

OR is the default conjunction operator. If there is no boolean operator between two terms, the *OR* operator is implicit. *OR* links two terms and finds a matching document if *any* of the

OR'd terms exist in a single row within the document (or in the document itself if it is not an Audit). This is equivalent to a union using sets.

The symbol "||" is an alternative to the word *OR*, for those users who are habituated to programming language operators.

The following three searches are equivalent, returning documents that have rows that contain either the term "lsass.exe" or "notepad.exe":

```
lsass.exe notepad.exe

lsass.exe OR notepad.exe

lsass.exe || notepad.exe
```

18.4.3.2. Boolean AND

AND links two terms and finds a matching document if and only if it contains *all* the terms exist in a single row in the document (or the document itself if it is not an Audit). *AND* is the equivalent to an intersection using sets.

You can use the symbol "&&" or prepend "+" to each individual term instead of using *AND*.

The following three searches are equivalent, returning documents that contain a row that has both the term "notepad.exe" and "69120":

```
notepad.exe AND 69120

notepad.exe && 69120

+notepad.exe +69120
```

18.4.3.3. Boolean NOT

The *NOT* operator *excludes* documents that have rows which contain the term after *NOT* (or the document itself if it is not an Audit). This is equivalent to a difference using sets. Note that *NOT* can only be used in conjunction with other terms. In other words, a search query that contains only a *NOT* term is invalid (e.g. "NOT notepad.exe" will fail to return a useful result).

The symbols "!" and "–" can be used in place of the word *NOT*.

The following three searches are equivalent, returning documents that contain a row that has the term "notepad.exe" but not the term "ed55ad0a7078651857bd8fc0eedd8b07f94594cc" (notepad.exe's sha1 sum):

```
notepad.exe NOT ed55ad0a7078651857bd8fc0eedd8b07f94594cc

notepad.exe !ed55ad0a7078651857bd8fc0eedd8b07f94594cc

notepad.exe -ed55ad0a7078651857bd8fc0eedd8b07f94594cc
```

Note that rows containing "notepad.exe" without a *sha1sum* field match the criteria of "NOT *[sha1 sum]*".

18.4.3.4. Logic Grouping

Parentheses "( )" can be used in a search query to group terms. This is useful in creating complex boolean operations where multiple criteria need to be applied. The following examples illustrate using parentheses for term grouping:

- Find all documents that contain a row (or have content) with either "notepad.exe" without a sha1sum value *OR* "notepad.exe" without a file size:
  ```
  (+notepad.exe !ed55ad0a7078651857bd8fc0eedd8b07f94594cc) OR
  (+notepad.exe !69120)
  ```

- Find all documents that contain a row (or have content) with "notepad.exe" *OR* "lsass.exe" *AND* their respective size in bytes of 69120 or 13312:
  ```
  (lsass.exe OR notepad.exe) AND (69120 OR 13312)

  (lsass.exe AND 13312) OR (notepad AND 69120)

  (lsass.exe 13312) (notepad 69120)

  (Filename: notepad.exe AND SizeInBytes:69120) OR
  (Filename:lsass.exe AND SizeInBytes:13312)
  ```

18.4.4. Range Searches

Range searches allow you to match documents with field values between specified lower and upper bounds. The search can be either inclusive or exclusive of the boundary terms. *Inclusive* ranges are denoted by square brackets "[ ]"; *exclusive* range queries are denoted by curly brackets "{ }". The operator word *TO* is placed between the range terms to indicate that this is a ranged search operation.

Due to software limitations, range searches are restricted to the first 10^{10} bytes (~9.3 Gb). Range seaches larger than this will return a subset of the requested data.

Range searches are typically performed with a Keyword.

Consider the following search:

```
created: [2007010101 TO 2008010101]
```

The first four digits in the search represent the year, the next two the month, the next two the day, and the final two the time based on the 24-hour clock. This *inclusive* search query would find documents that were created *on or after* 1AM, January 1st, 2007, and *before or on* 1AM, January 1st, 2008.

If curly braces had been used, it would be an *exclusive* search, returning items created *after* 1AM, January 1st, 2007, and *before* 1AM, January 1st, 2008:

```
created: {2007010101 TO 2008010101}
```

18.4.4.1. Searching for a Range in Date/Time Fields

Date and time fields can be searched using a range search query. In general, date/time range queries have the format (*inclusive* and *exclusive*, respectively):

```
[YYYYMMDDhh TO YYYYMMDDhh]

{YYYYMMDDhh TO YYYYMMDDhh}
```

The resolution of date/time fields for range searching purposes is to the hour, even if the field has more information (e.g. minutes, seconds).

18.4.4.2. Searching for a Range in Duration Fields

Duration fields can be searched using a range search query. In general, duration range queries have the format (*inclusive* and *exclusive*, respectively):

```
[DDDhhmm TO DDDhhmm]

{DDDhhmm TO DDDhhmm}
```

The resolution of duration fields for range searching purposes is to the minute, even if the field has more information (e.g. minutes, seconds).

18.4.5. Wildcards

You can use an asterisk "*" to represent any unknown characters at the end of a search term. You can use this to search for a wide variety of conditions.

Consider an example where you want to search for Host objects on a given subnet:

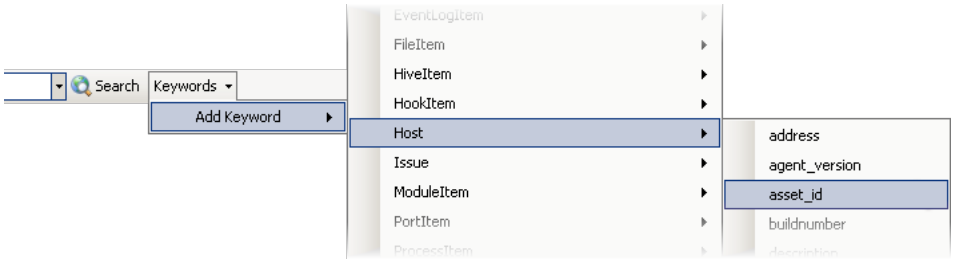
```
+Host/address:172.16.*
```

This search term will find all Hosts within the 172.16 subnet.

18.4.6. Keywords

Keywords provide a method for you to instruct the search engine to narrow the scope of its search to specific types of objects within the system, or specific fields within those objects. The various *Audit Data* returned by each Audit Module (see *Appendix A, Audit Modules and Analysis Commands*) each have a unique identifying keyword. When these keywords are combined, they can be a powerful tool for finding information within the MIR system.

Using these keywords directly can be difficult: the list is long and some keywords may not use an intuitive name. The Console provides a **Keywords** selector to help you in adding keywords to your search queries:



Clicking the **Keywords** selector displays a list that shows an organized list of all keywords currently known to the Controller. The list will expand as incoming Result Documents are prepared for searches, generating more keywords.

Examples that show the utility of keywords:

- Find all Jobs belonging to user *Lois* for a given time period:
  `+category:/db/entity/job +creator:Lois +created:[2008020100 TO 2008021400]`
- Find Audit Results created by user *Lois* for a given time period:
  `+category:/db/entity/resultset +creator:Lois +created:[2008020100 TO 2008020500]`
- Find all *File Listings* containing a file named *evil.exe*:
  `+FileItem/Path:evil.exe`
- Find all Audits of any kind referring to *evil.exe*:
  `+category:/audit +"evil.exe"`
- Find all *File Listings* with executable files that have sections:
  - named *.EVIL* OR *.tls* inside of them

OR

- all *File Listings* matching a series of four different md5 values

OR

- all *File Listings* that have an executable that imported *msevilvcrt.dll* OR *mybackdoor.dll*

OR

- all *Registry Listings* with a specific path

OR

- all Hosts with ports open to "192.168.*" OR "localhost":

```
FileItem/PEInfo/Sections/Section/Name:(
  ".EVIL" OR ".tls") OR
FileItem/Md5sum:(
  "82b24cb70e5944e6e34662205a2a5b78" OR "a2c3ff437616894740b20490334e1238" OR
  "019a82e5b5d213027da92244f03dcfdb" OR "c2c3ff437616894740b20490334e1238") OR
FileItem/PEInfo/ImportedModules/Module/Name:(
  "msevilvcrt.dll" OR "mybackdoor.dll") OR
RegistryItem/Path:(
  "HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\
\Evil" OR
  "HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Evil" OR
  "HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Services\\Evil") OR
PortItem/remoteIP:(192.168.* OR 127.0.0.1)
```

18.4.6.1. Search Keywords

Some keywords, such as "category," allow you to further specify a type of document through additional keywords as specified in the *Value* column of the table below. When you select

those keywords from the Query Builder, both the keyword (e.g., “category”) and the value (e.g., “/audit”) are populated into your search query automatically.

When you use a keyword that does not pre-define additional values (e.g., “FileItem/MD5Sum”), then you will need to provide the value to search for. As new data types are added to subsequent versions of MIR, more keywords will become available.

A list of keywords and the values they require are listed in *Appendix B, Searches*.

Chapter 19
Collaboration

The features discussed throughout this guide are available to multiple simultaneous users: multiple Consoles can be connected to a single Controller. All users will be able to see the same information and interact with the data, allowing an investigative or response team to coordinate their actions by using MANDIANT Intelligent Response.

There are several features that are designed to make collaboration more efficient and prevent users from unknowingly overwriting one another's data, and from making changes to the system that others cannot detect or understand. This chapter outlines these capabilities, allowing you to more effectively leverage MIR in a team environment.

There is no limit to the number of users who can access a single Controller. However, system performance is affected as more users are active on the system. Extensive data collections (grabbing the entire registry from hundreds of systems simultaneously, for example) can affect the experience for other users. If you are working in a multi-user environment and see performance issues, check to see what other users may be doing: heavy network traffic is a likely culprit.

19.1. Multi-User Basics

Users can be added and removed through the Administration Console, a web interface hosted on the Controller used to configure multiple aspects of a MIR deployment (see the *Administration Guide* for details). Once multiple users have been added, they can simultaneously log into the Controller using the Console on different workstations.

19.1.1. Access Controls

This version of MIR has one global workspace in which all users interact. As such, there are no granular access controls for allowing or preventing the reading and writing of data to/from the Controller. Users can be defined as having *User*, *Admin*, *Read Only*, or *Search Only* data access. See the *Administration Guide* for more information regarding access control.

19.1.2. Multi-User Edits and Conflict Resolution

When multiple users are working through a single Controller it is possible, and even likely, that two or more users will try to change the same information at the same time. The Controller detects this situation and provides a warning and conflict resolution options.

Consider a scenario where two users are modifying a Job. Users "Lois" and "Meggin" edit the Job and begin making changes, and Meggin saves her changes first. The changes are written to the Controller. When Lois saves her changes, the following conflict resolution options are presented to her:

Overwrite the saved copy with your copy
: Overwrites the Job on the Controller (here, the version with Meggin's changes in it) with the version currently being edited by you (in this case, Lois).

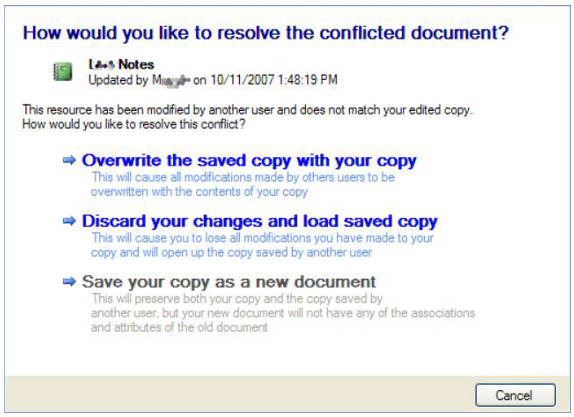
Discard your changes and load saved copy

Discards your changes (here, Lois' changes), and reloads the Job from the Controller into the editor (here, the Job with Meggin's changes).

Save your copy as a new Job

Creates a new Job on the Controller containing only your changes (in this case, Lois' version).

In many circumstances, the appropriate action will be to save a copy of your changes and then manually review the two files so that you can reconcile differences.



Part V. APPENDICES

Table of Contents

Appendix A
Audit Modules and Analysis Commands

Extensive details on the use, parameters, and data returned by Agent *Audit Modules* and *Analysis Commands* follows. By understanding how to use these powerful features, you can greatly enhance your ability to discover, analyze, and present information.

1. Audit Modules

Audit Modules provide several ways to collect information from *Hosts*. The table below provides a brief summary of each module, and is followed by detailed information about each *Module*, including parameters, special considerations, and data returned.

All modules support a parameter called *Prevent Hibernation*. Prevent hibernation attempts to keep a system from going into power saving mode if it is set to *True*. The default is *False* for all modules

Acquire Disk Image , `w32disk-acquisition`
Acquires contents of a disk drive.

Acquire a File (API Mode) , `w32apifile-acquisition`
Acquires contents of files using Windows system calls for file access.

Acquire a File (Raw Mode) , `w32rawfile-acquisition`

Acquires and downloads a specific file using a method that may bypass security or access restrictions and retrieve deleted files

Acquire Multiple Files (API Mode) , `w32multifileapi-acquisition`
Acquires multiple files based on filter criteria (e.g. path, filename) using Windows system calls for file access.

Acquire Multiple Files (Raw Mode) , `w32multifileraw-acquisition`
Acquires multiple files based on filter criteria (e.g. path, filename) using Windows system calls for file access.

Acquire Physical Memory Image , `w32memory-acquisition`
Acquires contents of a target system's memory.

Deactivate Agent , `deactivate`

Deactivates the running agent without uninstalling it. No further audits will be possible until the agent is started again.

Disk Listing , `w32disks`

List of physical devices which may be acquired as a Disk Image

Dissolve , `dissolve`

Dissolves the Agent from the host computer.

Driver Memory Acquire , `w32driver-memoryacquire`

Allows for the acquisition of a driver from live memory or from a memory image.

Drivers by Memory (ModuleList) , `w32drivers-modulelist`
Parses an operating system maintained list of loaded drivers.

Drivers by Signature (DriverList) , `w32drivers-signature`
Scans memory for loaded driver structures.

Event Logs , `w32eventlogs`

Acquire complete listings of the operating system event logs. Enumerates and acquires all logs if none are specified.

File Listing (API Mode) , `w32apifiles`
Gathers a list of files using Windows system calls.

File Listing (Raw Mode) , `w32rawfiles`
Gathers listing of files by directly examining structures on the target system's disks.

Hook Detection , `w32kernel-hookdetection`

Finds the presence of root kits using IRP, System Service Descriptor Table Hooks, and Interrupt Descriptor Table Hooks (IDT)

Host Network ARP Table , `w32network-arp`

Returns information about entries in the IPv4 and IPv6 Address Resolution Protocol (ARP) tables on a host. Each host maintains its own ARP table necessary for basic network traffic routing. Entries in the ARP table describe mappings from IP addresses to physical interface addresses.

Host Network DNS Cache table , `w32network-dns`

Returns DNS records stored in the computer's in-memory DNS cache table, which is maintained by the DNS Client Services windows component (which must be running for the table to be resident). The DNS cache table stores various DNS records that describe recently visited website domains.

Host Network Routing Table , `w32network-route`

Displays the IPv4 and IPv6 routing tables which store information about how a network destination is routed on a given interface.

Inclusion Filter , `regexv2`
Filters an XML Audit Data document **before** all other filters, allowing only qualified data to pass to the standard filter stream.

Network Ports Listing , `w32ports`

Active and listening ports and, where available, the process associated with them.

Persistence , `w32scripting-persistence`

Get details of the persistence locations.

Prefetch , `w32prefetch`

Get details of the prefetch files kept in %SystemRoot%\Prefetch.

Process Listing (API Mode) , `w32processes-API`
Lists running processes as reported by the operating system.

Process Listing (Handles Mode) , `w32processes-handle`
Obtains a list of running processes by using Windows system calls to enumerate handles.

Process Listing (Memory) , `w32processes-memory`

Lists running processes with comprehensive information about imported modules, sections, and other data gathered from advanced memory scanning techniques.

Process Memory Acquire , `w32processes-memoryacquire`

Allows for the acquisition of memory space for a specified process.

RegEx , `regex`
Filters an XML Audit Data document.

Registry Listing (API Mode) , `w32registryapi`

Returns a listing of registry keys using standard API methods

Registry Listing (Raw Mode) , `w32registryraw`

Returns a listing of registry keys using Raw methods which may bypass security and access restrictions.

Registry Hive Listing , `w32hivelist`

Lists registry hives for use in a Registry Listing audit. Includes hives which can only be acquired in Raw mode (such as the SAM hive).

Restart Agent , `restart`

Restarts the agent service.

Services Listing , `w32services`
Gathers a list of configured and running services on the target system.

System Information , `w32system`

General system information such as network devices, registration information, and local time.

System Restore , `w32systemrestore`

Get details associated with each restore point on the system.

Task Listing , `w32tasks`

List of Scheduled tasks (created via the 'at' command or Task Scheduler)

User Accounts , `w32useraccounts`
Retrieves a list of user accounts from the target system.

Volume Listing , `w32volumes`

List volumes which may be mounted by physical disks.

Web Historian Cookie History , `cookiehistory`

Returns a history of Cookies stored on the system

Web Historian File Download History , `filedownloadhistory`

Returns a history of Files downloaded through a browser

Web Historian Form History , `formhistory`

Returns a history of forms edited through a browser. Form history is not collected for internet explorer since it is not stored in an index.dat file; autocomplete/autofill/ intelliforms are stored in registry and need to be extracted completely differently than other internet explorer history data.

Web Historian URL History , `urlhistory`

Returns a history of URLs visited. The options "GetThumbnails" and "GetIndexedPageContent" are only available for Chrome and Chrome Frame browsers.

XPath, `xpath`
Filters an XML Audit Data document.

XPath2, `xpath2v2`
Filters an XML Audit Data document.

1.1. Acquire Disk Image: `w32disk-acquisition`

1.1.1. General Information

Acquires a bit-for-bit copy of a specified drive from the target system. Note that drive images can be extremely large; acquisition time across a network connection is highly dependent on network performance and congestion.

When attempting to acquire USB flash drives set the size so you do not read beyond the “end” of the drive. Doing so will generate end of disk read errors and may cause the USB flash drive to malfunction.

This version of MIR is unable to acquire network mounted shares. If you attempt such an acquisition the Agent will appear to build an image file; however, the read operations are failing and a well formed image will not be returned.

1.1.2. Audit Data

The module returns the requested drive image, if found. Any errors encountered will be reported in an Issues document (see _Error Messages and Troubleshooting_ in the Appendices). The image can be exported from the Controller to your local machine via the Console.

If the target Agent is running in daemon mode ("-d") and bad sectors are encountered, the operating system may present a dialog box to the end user. If the target agent is installed as a service this behavior does not occur. This is an aspect of the Windows operating system, not the MIR Agent.

1.1.3. How to Run `w32disk-acquisition`

In the Job or Script Editor, use the Agent Module chooser to select w32disk-acquisition.

Parameters:

Path (String)
The global path of the symbolic link for the disk or volume to acquire. The trailing back-slash is optional. Example: \\.\

Filename (String)
The name of the file to acquire. Example: PhysicalDrive0

offset (Integer)
Specifies the offset in bytes from the beginning of the disk.

size (Integer)
Specifies the size to acquire in bytes.

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.2. Acquire a File (API Mode): `w32apifile-acquisition`

1.2.1. General Information

Acquires a file from the target system by using Windows system calls to open and read the file. Since it uses standard system calls to read files, the last accessed time for the acquired file will be modified.

Windows 2000, Windows 2003, Windows XP. If you select the Preserve Times option, the module will manually "preserve" the last accessed time by recording it before the file is read, and restoring it to that value after the file is read. Acquire a File (API Mode) cannot be used to acquire a deleted file.

Windows Vista, Windows 7. You must disable Preserve Times. If you need to preserve the file time, choose a Raw Mode file audit module instead.

1.2.2. Audit Data

The module returns the requested file, if found. Any errors encountered will be reported in an Issues document (see _Error Messages and Troubleshooting_ in the Appendices). The file is viewable in the Hex Viewer, and can be exported through the Console to your local machine.

When the file is acquired it is named according to its source path and filename. A unique identifier is also appended to reduce the chance of a naming collision if you export the file.

In cases where the acquired file has an extremely long filename you may have to rename it when it is exported from the Controller, in order to save it to your local drive where the Console is running.

1.2.3. How to Run `w32apifile-acquisition`

In the Job or Script Editor, use the Agent Module chooser to select w32apifile-acquisition.

Parameters:

Path (String)
The absolute path of the directory containing the file to acquire. The trailing back-slash is optional. Example: C:\WINDOWS\

Filename (String)
The name of the file to acquire. Example: notepad.exe

Preserve Times (Boolean)
Manually reset last access times for audited files.

Default: false

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.3. Acquire a File (Raw Mode): `w32rawfile-acquisition`

1.3.1. General Information

Acquires and downloads a specific file using a method that may bypass security or access restrictions and retrieve deleted files

Returns only the first match of a deleted file if INode is not specified.

Acquires a file from the target system, bypassing standard Windows system calls. The File Allocation Table (FAT) or Master File Table (MFT) is read directly off of the disk. The module

directly accesses allocated sectors on the disk for the requested file and assembles it before packing it in an Audit Result. `w32rawfile-acquisition` can be used to acquire deleted files. Since the standard operating system calls are bypassed, file metadata, including last accessed time, is not modified when the file is read.

A file can take multiple clusters of storage space on a disk. If the file is appended to at a later time, then the additional clusters needed may not immediately follow the initial ones. Such a file is called fragmented. If a fragmented file and another file that lie between the original and appended clusters are both deleted, then the acquisition of the fragmented file will appear incorrectly to succeed. A file of the proper size will be acquired, but the contents will be wrong, containing parts of both files.

1.3.2. Audit Data

The module returns the requested file, if found. Any errors encountered will be reported in an Issues document (see _Error Messages and Troubleshooting_ in the Appendices). The file is viewable in the Hex Viewer, and can be exported through the Console to your local machine.

When the file is acquired it is named according to its source path and filename. A unique identifier is also appended to reduce the chance of a naming collision if you export the file.

In cases where the acquired file has an extremely long filename you may have to rename it when it is exported from the Controller, in order to save it to your local drive where the Console is running.

1.3.3. How to Run `w32rawfile-acquisition`

In the Job or Script Editor, use the Agent Module chooser to select w32rawfile-acquisition.

Returns only the first match of a deleted file if INode is not specified.

Parameters:

Path (String)
The absolute path of the directory containing the file to acquire. Example: D:\ C:\WINDOWS\

Filename (String)
The name of the file to acquire. Example: notepad.exe:malware.ads

Inode (Integer)
The Inode of the file to return. Note: if the inode is not specified and deleted is set to true, the first file encountered is returned.

Deleted (Boolean)
Acquire deleted files.

Default: false

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.4. Acquire Multiple Files (API Mode): `w32multifileapi-acquisition`

1.4.1. General Information

Acquires multiple files from the target system by using Windows system calls to open and read the file. Since it uses standard system calls to read files, the last accessed time for the acquired file will be modified. `w32multifileapi-acquisition` cannot be used to acquire a deleted file.

Windows 2000, Windows 2003, Windows XP. If you select the Preserve Times option, the module will manually "preserve" the last accessed time by recording it before the file is read, and restoring it to that value after the file is read.

Windows Vista, Windows 7. You must disable Preserve Times. If you need to preserve the file time, choose a Raw Mode file audit module instead.

1.4.2. Audit Data

The module returns files matching the criteria specified in the parameters supplied to the module. Any errors encountered will be reported in an Issues document (see _Error Messages and Troubleshooting_ in the Appendices). The files are viewable in the Hex Viewer, and can be exported through the Console to your local machine.

When the file is acquired it is named according to its source path and filename. A unique identifier is also appended to reduce the chance of a naming collision if you export the file.

In cases where the acquired file has an extremely long filename you may have to rename it when it is exported from the Controller, in order to save it to your local drive where the Console is running.

1.4.3. How to Run `w32multifileapi-acquisition`

In the Job or Script Editor, use the Agent Module chooser to select w32multifileapi-acquisition.

Parameters:

Path (String)
Path where search starts. The trailing back-slash is optional. Examples: C:\ D:\WINDOWS\

Regex (String)
Specifies the Perl Compatible Regular Expression a file must match to be returned. You must use standard Regular Expression escaping ('\\' matches a single '\', '\.' matches '.') Examples: Match all files in any subdirectory: .* Match .xls files in any subdirectory: .*\.xls Match .xls files in a subdirectory named Temp: .*\\Temp\\.*\.xls

Depth (Integer)
Number of directory levels to include, with -1 representing full depth

Minimum Sizes (Strings)
The minimum file size (in bytes) of a returned file.

Maximum Sizes (Strings)
The maximum file size (in bytes) of a returned file.

Filter MD5 (Strings)
Filter the results based on a specific MD5 hash

Filter SHA1 (Strings)
Filter the results based on a specific SHA1 hash

Filter SHA256 (Strings)
Filter the results based on a specific SHA256 hash

Content Regex (Strings)
Search files for particular content.

AND Operator (Boolean)
A file's content must match all regex parameters.

Default: false

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.5. Acquire Multiple Files (Raw Mode): `w32multifileraw-acquisition`

1.5.1. General Information

Acquires files from the target system based on parameters supplied to the module, bypassing standard Windows system calls. The File Allocation Table (FAT) or Master File Table (MFT) is read directly off of the disk. The Module directly accesses allocated sectors on the disk for the requested file and assembles it before packing it in an Audit Result. `w32multifileraw-acquisition` can be used to acquire deleted files. Since the standard operating system calls are bypassed, file metadata, including last accessed time, is not modified when the file is read.

A file can take multiple clusters of storage space on a disk. If the file is appended to at a later time, then the additional clusters needed may not immediately follow the initial ones. Such a file is called fragmented. If a fragmented file and another file that lie between the original and appended clusters are both deleted, then the acquisition of the fragmented file will appear incorrectly to succeed. A file of the proper size will be acquired, but the contents will be wrong, containing parts of both files.

1.5.2. Audit Data

The module returns files matching the criteria specified in the parameters supplied to the module. Any errors encountered will be reported in an Issues document (see _Error Messages

and Troubleshooting_ in the Appendices). The files are viewable in the Hex Viewer, and can be exported through the Console to your local machine.

When the file is acquired it is named according to its source path and filename. A unique identifier is also appended to reduce the chance of a naming collision if you export the file.

In cases where the acquired file has an extremely long filename you may have to rename it when it is exported from the Controller, in order to save it to your local drive where the Console is running.

1.5.3. How to Run `w32multifileraw-acquisition`

In the Job or Script Editor, use the Agent Module chooser to select w32multifileraw-acquisition.

Parameters:

Path (String)
Path where search starts. The trailing back-slash is optional. Examples: C:\ D:\WINDOWS\

Regex (String)
Specifies the Perl Compatible Regular Expression a file must match to be returned. You must use standard Regular Expression escaping ('\\' matches a single '\', '\.' matches '.') Examples: Match all files in any subdirectory: .* Match .xls files in any subdirectory: .*\.xls Match .xls files in a subdirectory named Temp: .*\\Temp\\.*\.xls

Depth (Integer)
Number of directory levels to include, with -1 representing full depth

Minimum Sizes (Strings)
The minimum file size (in bytes) of a returned file.

Maximum Sizes (Strings)
The maximum file size (in bytes) of a returned file.

Active Files (Boolean)
Enumerate the active files. Active means non-deleted files.

Default: true

Deleted Files (Boolean)
Enumerate the deleted files.

Default: false

Filter MD5 (Strings)
Filter the results based on a specific MD5 hash

Filter SHA1 (Strings)
Filter the results based on a specific SHA1 hash

Filter SHA256 (Strings)
Filter the results based on a specific SHA256 hash

Content Regex (Strings)
Search files for particular content.

AND Operator (Boolean)
A file's content must match all regex parameters.

Default: false

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.6. Acquire Physical Memory Image: `w32memory-acquisition`

1.6.1. General Information

Acquires a copy of system memory from the target system. Note that this may be several gigabytes on some systems. Acquisition may be slow over network connections depending on available bandwidth.

On Hosts that do not support memory-related audits, such as Windows Vista 64 bit, an Issue Document will be returned indicating an error occurred and that the Audit could not determine the OS version.

1.6.2. Audit Data

The module returns the requested memory image. Any errors encountered will be reported in an Issues document (see _Error Messages and Troubleshooting_ in the Appendices). The image can be exported from the Controller to your local machine via the Console.

The Agent makes no attempt to determine the amount of physical memory in a host because the API calls that provide this data may be subverted. If no size (amount of physical memory) is specified, all of memory will be acquired. However, if the user specifies a size greater than the amount of physical memory, an image the specified size will be returned.

1.6.3. How to Run `w32memory-acquisition`

In the Job or Script Editor, use the Agent Module chooser to select w32memory-acquisition.

Parameters:

offset (Integer)
Specifies the offset in bytes from the beginning of physical memory. Note: This will be rounded to the lower page boundary.

size (Integer)
Specifies the size of memory to return. Note: This will be rounded to the next page boundary.

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.7. Disk Listing: `w32disks`

1.7.1. General Information

List of physical devices which may be acquired as a Disk Image

Lists the physical storage devices on the target system. The information provided from this Audit can be used when running `w32disk-acquisition`.

1.7.2. Audit Data

Disk Name
System name for the disk.

Disk Size
Size of the disk in bytes.

1.7.3. How to Run `w32disks`

In the Job or Script Editor, use the Agent Module chooser to select w32disks.

Parameters:

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.7.4. Item Details

Additional data is provided for each disk in the Audit. These may be viewed through the Details Viewer.

PartitionList
This collection contains a list of all partitions contained on the physical drive as well as their size.

1.8. Dissolve and Deactivate Agent

These two modules allow you to stop and disable (`deactivate`) or uninstall (`dissolve`) a running Agent on a target system. Neither module takes any parameters, and only one or the other should be included in an Audit. If both are included the Agent may deactivate or dissolve, but you will be unable to verify which occurred.

If an Agent is deactivated, it will have to be manually re-started on the target system if you wish to use it again. Dissolved Agents must be reinstalled before they can be used.

If a Job has been canceled remotely, its current Audit remains “active” on its Host until it is timed out (twelve hours by default, controlled by the Job’s expiration setting). As long as the

Audit remains in such a state, subsequent requests to dissolve its Agent will not occur. As soon as the Job expires it will execute properly and remove the Agent.

1.8.1. Audit Data

These modules do not return audit data.

1.8.2. How to Run Dissolve or Deactivate Agent

In the Job or Script Editor, use the Agent Module chooser to select dissolve or deactivate.

Parameters:

immediate (Boolean)
Execute the command immediately without waiting for existing audits to finish.

Default: false

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.9. Driver Memory Acquire: `w32driver-memoryacquire`

1.9.1. General Information

Allows for the acquisition of a driver from live memory or from a memory image.

Acquires a copy of the memory in use by a driver on the target system.

On Hosts that do not support memory-related audits, such as Windows Vista 64 bit, an Issue Document will be returned indicating an error occurred and that the Audit could not determine the OS version.

1.9.2. Audit Data

The module returns the requested driver memory image. Any errors encountered will be reported in an Issues document (see _Error Messages and Troubleshooting_ in the Appendices). The image can be exported from the Controller to your local machine via the Console.

1.9.3. How to Run `w32driver-memoryacquire`

In the Job or Script Editor, use the Agent Module chooser to select w32driver-memoryacquire.

Parameters:

driver name (String)
The driver name to acquire.

memory file (String)
The full path and filename of the file that represents the host's physical memory.

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.10. Drivers by Memory (ModuleList): `w32drivers-modulelist`

1.10.1. General Information

Parses operating system maintained lists of loaded and running drivers. Note that the data generated by this module and that generated by Drivers by Signature (DriverList) may be different and that difference is not, in and of itself, an indication of a "hidden" driver.

The module may also be used to parse the contents of a memory dump, such as one produced by a MIR Agent local audit, or another memory dump and analysis tool. It could also be used to analyze the memory file from a virtual machine. The memory file to be analyzed must reside on the same system as the Agent that is running.

The list of identified driver objects is returned, including names, base addresses, size, the path to the executable file on disk that contains the driver code.

1.10.2. Audit Data

ModuleAddress
Address of the driver module in memory.

ModuleInit
Address of the initialization function for the driver.

ModuleBase
Base address for the module object.

ModuleSize
Size of the module in bytes.

On 64 bit systems, Windows returns a value double that of the actual size of the module. On 32 bit systems, the reported size is correctly reported.

ModuleName
Name of the module (e.g. `kdcom.dll`)

ModulePath
Path to the executable file on disk containing the driver.

1.10.3. How to Run `w32drivers-modulelist`

In the Job or Script Editor, use the Agent Module chooser to select w32drivers-modulelist.

Parameters:

memory file (String)
The full path and filename of the file that represents the host's physical memory.

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.10.4. Item Details

Additional Item details are not available in this audit. However, the Details Viewer displays the full contents of a selected row item and translates memory addresses into hexadecimal representation.

1.11. Drivers by Signature (DriverList): `w32drivers-signature`

Scans memory looking for structures matching drivers and reports on them. Note that the data generated by this module and that generated by Drivers by Memory (ModuleList) may be different and that difference is not, in and of itself, an indication of a "hidden" driver.

The module may also be used to parse the contents of a memory dump, such as one produced by a MIR Agent local audit, or another memory dump and analysis tool. It could also be used to analyze the memory file from a virtual machine. The memory file to be analyzed must reside on the same system as the Agent that is running.

The list of detected driver objects is returned, including names, base addresses, size, and the memory addresses of various required function calls within the driver.

Windows 2000, Windows 2003, Windows XP. If you select the Preserve Times option, the module will manually "preserve" the last accessed time by recording it before the file is read, and restoring it to that value after the file is read.

Windows Vista, Windows 7. You must disable Preserve Times. If you need to preserve the file time, choose a Raw Mode file audit module instead.

Windows 7 Pro 32 bit is not recognized by Drivers by Memory. No data will be returned.

1.11.1. Audit Data

Driver Object Address
Address in memory for the driver object.

Image Size
Size of the entire driver image in memory, in bytes.

Image Base
Base address for the driver image in memory.

DriverName
Name of the driver, if available

DriverInit
Address of the driver's initialization function.

DriverStartIo
Address of the driver's DriverStartIo function.

DriverUnload
Address of the driver's DriverUnload function.

Irp
Address of functions handling various IRP_MJ messages, including:IRP_MJ_CREATE, IRP_MJ_CREATE_NAMED_PIPE, IRP_MJ_CLOSE, IRP_MJ_WRITE, IRP_MJ_READ, IRP_MJ_QUERY_INFORMATION, IRP_MJ_SET_INFORMATION, IRP_MJ_QUERY_EA, IRP_MJ_FLUSH_BUFFERS, IRP_MJ_QUERY_VOLUME_INFORMATION, IRP_MJ_SET_VOLUME_INFORMATION, IRP_MJ_DIRECTORY_CONTROL, IRP_MJ_FILE_SYSTEM_CONTROL, IRP_MJ_DEVICE_CONTROL, IRP_MJ_SHUTDOWN, IRP_MJ_LOCK_CONTROL, IRP_MJ_CLEANUP, IRP_MJ_CREATE_MAILSLOT, IRP_MJ_QUERY_SECURITY, IRP_MJ_SET_SECURITY, IRP_MJ_POWER, IRP_MJ_SYSTEM_CONTROL, IRP_MJ_DEVICE_CHANGE, IRP_MJ_QUERY_QUOTA, IRP_MJ_SET_QUOTA, IRP_MJ_PNP

1.11.2. How to Run `w32drivers-signature`

In the Job or Script Editor, use the Agent Module chooser to select w32drivers-signature.

Parameters:

memory file (String)
The full path and filename of the file that represents the host's physical memory.

enumerate imports (Boolean)
Boolean indicating whether or not to enumerate imports of all loaded modules for a given driver.

Default: false

enumerate exports (Boolean)
Boolean indicating whether or not to enumerate exports of all loaded modules for a given driver.

Default: false

strings (Boolean)
Boolean indicating whether or not to parse a specified driver for strings.

Default: false

shortest matched string (Integer)
Minimum Recognized String Length

Preserve Times (Boolean)
Manually reset last access times for audited files.

Default: false

MD5 (Boolean)
Compute the MD5 hash for each returned file.

Default: false

SHA1 (Boolean)
Compute the SHA1 hash for each returned file.

Default: false

SHA256 (Boolean)
Compute the SHA256 hash for each returned file.

Default: false

Verify Digital Signatures (Boolean)
Boolean indicating whether or not to verify if the loaded drivers are digitally signed. This operation can not be performed on a memory image.

Default: false

raw mode (Boolean)
Open files for hashing in raw mode.

Default: false

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.11.3. Item Details

Each line item might also contain a listing of Device Items, which are the object's properties and the object's names used by a driver to communicate with its userland components. These are available through the Details pane.

In some cases this audit may not be able to populate all information about a driver if the section of memory containing it is paged to disk.

1.12. Event Logs: `w32eventlogs`

1.12.1. General Information

Acquire complete listings of the operating system event logs. Enumerates and acquires all logs if none are specified.

Collects an XML-formatted extraction of the Windows Event Logs from the target system. The user specifies which log to collect according to its name (e.g., System, Application, Security). For more details regarding Windows Event Logs, refer to Microsoft operating system and developer documentation.

1.12.2. Audit Data

EID
Numeric event ID.

log
The Event Log in which the event originated.

index
Index number for the entry within its Event Log.

type
Event type. Typically one of the following: Error, Warning, Information, Success Audit, Failure Audit.

categoryNum
Event category number.

GenTime
The time the event was generated by the system.

writeTime
The time the event was written to the Event Log.

reserved
Reserved for future use.

source
The Event source (e.g. `Application Popup` or `HHCTRL`).

machine
The system name of the computer that generated the event.

user
The user associated with the event, if any.

category
Event category string, if specified.

message
Message contained in the event.

To see the contents of any Message field (or any other field that is truncated) hover over it. The contents appear as tip text.

1.12.3. How to Run `w32eventlogs`

In the Job or Script Editor, use the Agent Module chooser to select w32eventlogs.

Parameters:

eventlog (String)
The eventlog(s) in which to parse (e.g. Application System Security)

eventlogfullpath (String)
The full path and filename to the eventlog(s) to parse

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.12.4. Item Details

Additional data may be provided on certain event log entries. Additionally, some applications generate more complex Event Log message structures. These may be viewed through the Details Viewer.

blob
If the event log message contains an unstructured binary blob, the array of bytes id displayed in this collection.

Detected Anomalies
For future use.

unformatted Message
If the content of the message is unformatted, but is otherwise not a binary blob, the content of the strings associated with the message can be viewed through this collection.

1.13. File Listing (API Mode): `w32apifiles`

1.13.1. General Information

May return more information than expected if 'Get Resources' is selected, it is strongly recommended to only use this parameter when targetting a single file.

File Listing (API Mode) uses Windows system calls to generate a file listing. The module also has the ability to generate additional information about the file contents, including secure hash checksums and an assessment of the entropy of file content. For executable files, certain aspects of the file's structure can be assessed and help provide insight into anomalous behaviors. See _Entropy, Anomalies, and Entry Point Signatures_ in the Appendices for additional information. File Listing (API Mode) cannot be used to acquire a deleted file.

Windows 2000, 2003, XP. If you select the Preserve Times option, the module will manually "preserve" the last accessed time by recording it before the file is read, and restoring it to that value after the file is read.

Windows Vista, Windows 7. You must disable Preserve Times. If you need to preserve the file time, choose a Raw Mode file audit module instead.

This version of MIR is unable to list files from network mounted shares. If you attempt such a listing, an error will occur.

1.13.2. Audit Data

DevicePath
The location of the file on the device.

FullPath
The full path on the filesystem to the file.

Drive
Drive letter the file is stored on.

FilePath
Path tot he file minus drive and filename.

FileName
Name of the file, including extension.

FileExtension
Extension for the file.

Size in Bytes
File size in bytes.

Created
Date/time of file creation.

Modified
Date/time of last modification of the file's contents.

Accessed
Date/time of the last access to the file.

Changed
Date/time of the last modification to either the file's content or the file's metadata (e.g. permissions, attributes).

File Attributes
Attributes as reported by the file system, includes:ReadOnly, Hidden, System, Directory, Archive, Device, Normal, Temporary, SparseFile, ReparsePoint, Compressed, Offline, NotContentIndexed, Encrypted.

Username
Name of the user that owns the file (only valid for NTFS filesystems).

SID
Security Identifier of the group associated with the file.

SIDType
The SID type for the SID as reported by the operating system.

Peak Entropy
Number, generally between 0 and 1, indicating the highest amount of entropy for any characteristic of that file. See _Entropy, Anomalies, and Entry Point Signatures_ in the Appendices for more information. Only populated if Analyze Entropy is set in parameters.

Peak Code Entropy
Number, generally between 0 and 1, indicating the highest amount of entropy for the executable code portion of a file. See _Entropy, Anomalies, and Entry Point Signatures_ in the Appendices for more information.

MD5Sum
MD5 hash value across the file's contents. Only populated if proper parameter set in Job.

Sha1Sum
Sha1 hash value across the file's contents. Only populated if proper parameter set in Job.

Sha256Sum
Sha256 hash value across the file's contents. Only populated if proper parameter set in Job.

1.13.3. How to Run `w32apifiles`

In the Job or Script Editor, use the Agent Module chooser to select w32apifiles.

May return more information than expected if 'Get Resources' is selected, it is strongly recommended to only use this parameter when targetting a single file.

Parameters:

Path (String)
Path where search starts. The trailing back-slash is optional. Examples: C:\ D:\WINDOWS\

Regex (String)
Specifies the Perl Compatible Regular Expression a file must match to be returned. You must use standard Regular Expression escaping ('\\' matches a single '\', '\.' matches '.') Examples: Match all files in any subdirectory: .* Match .xls files in any subdirectory: .*\.xls Match .xls files in a subdirectory named Temp: .*\\Temp\\.*\.xls

Depth (Integer)
Number of directory levels to include, with -1 representing full depth

MD5 (Boolean)
Compute the MD5 hash for each returned file.

Default: false

SHA1 (Boolean)
Compute the SHA1 hash for each returned file.

Default: false

SHA256 (Boolean)
Compute the SHA256 hash for each returned file.

Default: false

Preserve Times (Boolean)
Manually reset last access times for audited files.

Default: false

Analyze Entropy (Boolean)
Calculate entropy for executable files. High entropy may indicate a packed executable.

Default: false

Enumerate Imports (Boolean)
Identify modules and functions imported by executable files.

Default: false

Enumerate Exports (Boolean)
Identify modules and functions exported by executable files.

Default: false

Analyze File Anomalies (Boolean)
Detect higher-order anomalies which may indicate malicious files.

Default: false

Scan Entry Point Distance (Integer)
Specifies the number of bytes from the entry point to scan for jumps.

Verify Digital Signatures (Boolean)
Verify the digital signature on executable files

Default: false

Minimum Sizes (Strings)
The minimum file size (in bytes) of a returned file.

Maximum Sizes (Strings)
The maximum file size (in bytes) of a returned file.

Filter MD5 (Strings)
Filter the results based on a specific MD5 hash

Filter SHA1 (Strings)
Filter the results based on a specific SHA1 hash

Filter SHA256 (Strings)
Filter the results based on a specific SHA256 hash

Content Regex (Strings)
Search files for particular content.

AND Operator (Boolean)
A file's content must match all regex parameters.

Default: false

Strings (Boolean)
Boolean indicating whether or not to parse specified files for strings. If strings is enabled, default string length is 4.

Default: false

shortest matched string (Integer)
Minimum Recognized String Length. Default: 4

Include Files (Boolean)
Return file item types.

Default: true

Include Directories (Boolean)
Return directory item types.

Default: true

Get Resources (Boolean)
Return resources stored in a PE file.

Default: false

Get Resource Data (Boolean)
Return all data associated with all resources in a PE file. WARNING: This option can return very large amounts of data even with narrowly-scoped audits. Consider using "Exclude Resource Types" and verifying the size of the results from a single host before running on multiple hosts.

Default: false

Get Version Info (Boolean)
Return version information stored in a PE file.

Default: false

Exclude Resource Types (Strings)
List of resource types to exclude when extracting PE resources.

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.13.4. Item Details

Additional data may be provided on certain file listing items. The following additional information may be viewed through the Details Viewer.

Detected Anomalies
For future use.

INode
First INode allocated for the file.

Not provided in w32apifiles. Use w32rawfiles to obtain INode information.

Streams
Identifies whether the file has any Alternate Data Streams (ADS was provided in NTFS to provide compatibility with older versions of Apple's Hierarchical File System). A file may only have an ADS on an NTFS file system. The job must have the Analyze File option set in Job parameters to detect ADS.

PEInfo
Section that is populated when a file is an executable and one or more file analysis options (Analyze Entropy, Analyze Imports, Analyze Exports, Analyze File) have been set for the Audit. Includes detected executable type information (e.g. `DLL`, `executable`).

PEInfo - Detected Anomalies
A collection that contains information about any anomalies discovered when the file was analyzed. Only present for executable files when the Analyze File option is set in Job parameters. See _Entropy, Anomalies, and Entry Point Signatures_ in the Appendices for more information.

PEInfo - Detected Entry Point Signature
A collection that contains information about any entry point signatures discovered in the file (e.g., packers, compilers). Only present for executable files when the Analyze File option is set in Job parameters. See _Entropy, Anomalies, and Entry Point Signatures_ in the Appendices for more information.

Advanced PEInfo
Information generated when the Scan Entry Point parameter is specified (see below).

Export Information
Lists any functions exported by the executable for other programs to use.

Sections
Detailed information about executable file sections, including section size, entropy value, and other characteristics as described in Microsoft's Portable Executable and Common Object File Format.

Imported Modules
A collection that contains a list of any DLLs and associated function calls imported by the file. Only present for executable files when the Analyze Imports option is set in Job parameters.

Digital Signature
Identifies if the file is signed, whether the signature correctly verifies, and the identity of the signing certificate.

String Information
If string extraction was requested for the file, contains the list of strings of the minimum length requested or longer.

1.14. File Listing (Raw Mode): `w32rawfiles`

1.14.1. General Information

May return more information than expected if 'Get Resources' is selected, it is strongly recommended to only use this parameter when targetting a single file.

`w32rawfiles` reads the File Allocation Table (FAT) or Master File Table (MFT) directly off of the disk of the target system to generate a file listing. Much like `w32apifiles`, this module also has the ability to generate additional information about the file contents, including secure hash checksums and an assessment of the entropy of file content. For executable files, certain aspects of the file's structure can be assessed and help provide insight into anomalous behaviors. See _Entropy, Anomalies, and Entry Point Signatures_ in the Appendices for additional information.

Unlike `w32apifiles`, `w32rawfiles` does not modify any file metadata when it creates file listings or reads file contents because it is bypassing standard operating system calls. Because of this, `w32rawfiles` can also gather information about deleted files.

An infinite loop will be created if the Audit reads the file to which enumeration results are written. Please avoid auditing your results directory when running an Agent from the command line.

This version of MIR is unable to list files from network mounted shares. If you attempt such a listing, an error will occur.

1.14.2. Audit Data

DevicePath
The location of the file on the device.

FullPath
The full path on the filesystem to the file.

Drive
Drive letter the file is stored on.

FilePath
Path tot he file minus drive and filename.

FileName
Name of the file, including extension.

FileExtension
Extension for the file.

Size in Bytes
File size in bytes.

Created
Date/time of file creation.

Modified
Date/time of last modification of the file's contents.

Accessed
Date/time of the last access to the file.

Changed
Date/time of the last modification to either the file's content or the file's metadata (e.g. permissions, attributes).

File Attributes
Attributes as reported by the file system, includes:ReadOnly, Hidden, System, Directory, Archive, Device, Normal, Temporary, SparseFile, ReparsePoint, Compressed, Offline, NotContentIndexed, Encrypted.

Username
Name of the user that owns the file (only valid for NTFS filesystems).

SID
Security Identifier of the group associated with the file.

SIDType
The SID type for the SID as reported by the operating system.

Peak Entropy
Number, generally between 0 and 1, indicating the highest amount of entropy for any characteristic of that file. See _Entropy, Anomalies, and Entry Point Signatures_ in the Appendices for more information. Only populated if Analyze Entropy is set in parameters.

Peak Code Entropy
Number, generally between 0 and 1, indicating the highest amount of entropy for the executable code portion of a file. See _Entropy, Anomalies, and Entry Point Signatures_ in the Appendices for more information.

MD5Sum
MD5 hash value across the file's contents. Only populated if proper parameter set in Job.

Sha1Sum
Sha1 hash value across the file's contents. Only populated if proper parameter set in Job.

Sha256Sum
Sha256 hash value across the file's contents. Only populated if proper parameter set in Job.

1.14.3. How to Run `w32rawfiles`

In the Job or Script Editor, use the Agent Module chooser to select w32rawfiles.

May return more information than expected if 'Get Resources' is selected, it is strongly recommended to only use this parameter when targetting a single file.

Parameters:

Path (String)
Path where search starts. The trailing back-slash is optional. Examples: C:\ D:\WINDOWS\

Regex (String)
Specifies the Perl Compatible Regular Expression a file must match to be returned. You must use standard Regular Expression escaping ('\\' matches a single '\', '\.' matches '.') Examples: Match all files in any subdirectory: .* Match .xls files in any subdirectory: .*\.xls Match .xls files in a subdirectory named Temp: .*\\Temp\\.*\.xls

Depth (Integer)
Number of directory levels to include, with -1 representing full depth

MD5 (Boolean)
Compute the MD5 hash for each returned file.

Default: false

SHA1 (Boolean)
Compute the SHA1 hash for each returned file.

Default: false

SHA256 (Boolean)
Compute the SHA256 hash for each returned file.

Default: false

Analyze Entropy (Boolean)
Calculate entropy for executable files. High entropy may indicate a packed executable.

Default: false

Enumerate Imports (Boolean)
Identify modules and functions imported by executable files.

Default: false

Enumerate Exports (Boolean)
Identify modules and functions exported by executable files.

Default: false

Analyze File Anomalies (Boolean)
Detect higher-order anomalies which may indicate malicious files.

Default: false

Scan Entry Point Distance (Integer)
Specifies the number of bytes from the entry point to scan for jumps.

Verify Digital Signatures (Boolean)
Verify the digital signature on executable files

Default: false

Minimum Sizes (Strings)
The minimum file size (in bytes) of a returned file.

Maximum Sizes (Strings)
The maximum file size (in bytes) of a returned file.

Active Files (Boolean)
Enumerate the active files. Active means non-deleted files.

Default: true

Deleted Files (Boolean)
Enumerate the deleted files.

Default: false

Parse NTFS INDX Buffers (Boolean)
Parse unused space in NTFS INDX buffers to find previous directory entries.

Default: false

Filter MD5 (Strings)
Filter the results based on a specific MD5 hash

Filter SHA1 (Strings)
Filter the results based on a specific SHA1 hash

Filter SHA256 (Strings)
Filter the results based on a specific SHA256 hash

Content Regex (Strings)
Search files for particular content.

AND Operator (Boolean)
A file's content must match all regex parameters.

Default: false

Strings (Boolean)
Boolean indicating whether or not to parse specified files for strings. If strings is enabled, default string length is 4.

Default: false

shortest matched string (Integer)
Minimum Recognized String Length. Default: 4

Include Files (Boolean)
Return file item types.

Default: true

Include Directories (Boolean)
Return directory item types.

Default: true

Get Resources (Boolean)
Return resources stored in a PE file.

Default: false

Get Version Info (Boolean)
Return version information stored in a PE file.

Default: false

Get Resource Data (Boolean)
Return all data associated with all resources in a PE file. WARNING: This option can return very large amounts of data even with narrowly-scoped audits. Consider using "Exclude Resource Types" and verifying the size of the results from a single host before running on multiple hosts.

Default: false

Exclude Resource Types (Strings)
List of resource types to exclude when extracting PE resources.

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.14.4. Item Details

Additional data may be provided on certain file listing items. The following additional information may be viewed through the Details Viewer.

Detected Anomalies
For future use.

INode
First INode allocated for the file.

Not provided in w32apifiles. Use w32rawfiles to obtain INode information.

Streams
Identifies whether the file has any Alternate Data Streams (ADS was provided in NTFS to provide compatibility with older versions of Apple's Hierarchical File System). A file may only have an ADS on an NTFS file system. The job must have the Analyze File option set in Job parameters to detect ADS.

PEInfo
Section that is populated when a file is an executable and one or more file analysis options (Analyze Entropy, Analyze Imports, Analyze Exports, Analyze File) have been set for the Audit. Includes detected executable type information (e.g. `DLL`, `executable`).

PEInfo - Detected Anomalies
A collection that contains information about any anomalies discovered when the file was analyzed. Only present for executable files when the Analyze File option is set in Job parameters. See _Entropy, Anomalies, and Entry Point Signatures_ in the Appendices for more information.

PEInfo - Detected Entry Point Signature
A collection that contains information about any entry point signatures discovered in the file (e.g., packers, compilers). Only present for executable files when the Analyze File option is set in Job parameters. See _Entropy, Anomalies, and Entry Point Signatures_ in the Appendices for more information.

Advanced PEInfo
Information generated when the Scan Entry Point parameter is specified (see below).

Export Information
Lists any functions exported by the executable for other programs to use.

Sections
Detailed information about executable file sections, including section size, entropy value, and other characteristics as described in Microsoft's Portable Executable and Common Object File Format.

Imported Modules
A collection that contains a list of any DLLs and associated function calls imported by the file. Only present for executable files when the Analyze Imports option is set in Job parameters.

Digital Signature
Identifies if the file is signed, whether the signature correctly verifies, and the identity of the signing certificate.

String Information
If string extraction was requested for the file, contains the list of strings of the minimum length requested or longer.

1.15. Hook Detection: `w32kernel-hookdetection`

1.15.1. General Information

Finds the presence of root kits using IRP, System Service Descriptor Table Hooks, and Interrupt Descriptor Table Hooks (IDT)

May find legitmate hooks such as those used by antivirus software.

Detects potential rootkits on target systems by identifying hooks in operating system functions, operating system structures, and loaded device drivers.

On Hosts that do not support memory-related audits, such as Windows Vista 64 bit, an Issue Document will be returned indicating an error occurred and that the Audit could not determine the OS version.

1.15.2. Audit Data

HookDescription
Specifies whether the identified hook is against a Driver or a SystemCall.

HookedFunction
Identifies the function that has been hooked.

HookedModule
Identifies the module (e.g., executable file) that has been hooked.

HookingModule
Identifies the module (e.g., executable file) performing the hooking operation.

HookingAddress
Identifies the address in memory of the hooking code.

1.15.3. How to Run `w32kernel-hookdetection`

In the Job or Script Editor, use the Agent Module chooser to select w32kernel-hookdetection.

May find legitmate hooks such as those used by antivirus software.

Parameters:

idt (Boolean)
Boolean indicating whether or not to verify certain entries in the IDT.

Default: false

ssdt_index (Boolean)
Boolean indicating whether or not to verify the System Service Descriptor Table.

Default: false

ssdt_inline (Boolean)
Boolean indicating whether or not to check System Service Descriptor Table's functions for modifications to their prologues.

Default: false

drivers (Boolean)
Boolean indicating whether or not to check the systems drivers for IRP hooks.

Default: false

memory file (String)
The full path and filename of the file that represents the host's physical memory.

Verify Digital Signatures (Boolean)
Boolean indicating whether or not to verify if the hooked and hooking modules are digitally signed. This operation can not be performed on a memory image.

Default: false

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.16. Host Network ARP Table: `w32network-arp`

Returns information about entries in the IPv4 and IPv6 address resolution protocol (ARP) tables on a host. Each host maintains its own ARP table necessary for basic network traffic routing. Entries in the ARP table describe mappings from IP addresses to physical interface addresses.

1.16.1. Audit Data

Interface
The IPv4 or IPv6 address of the network interface.

PhysicalAddress
The hardware/MAC address of the IP address being mapped/resolved.

IPv6Address
The IPv6 address being mapped/resolved.

IPv4Address
The IPv4 address being mapped/resolved.

CacheType
One of "Dynamic", "Static", "Invalid" or "Other" (IPv4 only).

InterfaceType
One of "IEEE 1394 (Firewire)", "Tunnel Encapsulation", "802.11 Wireless", "ATM", "Software Loopback", "PPP", "Token Ring", "Ethernet" or "Other" (IPv6 only).

State
One of "Unreachable", "Incomplete", "Probe", "Delay", "Stale", "Reachable" or "Permanent" (IPv6 only).

IsRouter
True if the network device is acting as a router (IPv6 only).

LastReachable
The time span that a node assumes a neighbor is reachable after having received a reachability confirmation (IPv6 only).

LastUnreachable
The time span that a node assumes a neighbor is unreachable after not having received a reachability confirmation (IPv6 only).

1.16.2. How to Run `w32network-arp`

In the Job or Script Editor, use the Agent Module chooser to select w32network-arp.

Parameters:

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.17. Host Network DNS Cache table: `w32network-dns`

Returns DNS records stored in the computer's in-memory DNS cache table, which is maintained by the DNS Client Services windows component (which must be running for the table to be resident). The DNS cache table stores various DNS records that describe recently visited website domains.

1.17.1. Audit Data

For all Audits

Host
The domain name common to a set of DNS records.

RecordName
The domain name for this DNS record.

RecordType
The type of DNS record; one of "A", "NS", "MD", "MF", "CNAME", "SOA", "MB", "MG", "MR", "NULL", "WKS", "PTR", "HINFO", "MINFO", "MX", "TEXT", "RP", "AFSDB", "X25", "ISDN", "RT", "NSAP", "NSAPPTR", "SIG", "KEY", "PX", "GPOS", "AAAA", "LOC", "NXT", "EID", "NIMLOC", "SRV", "ATMA", "NAPTR", "KX", "CERT", "A6", "DNAME", "SINK", "OPT", "DS", "RRSIG", "NSEC", "DNSKEY",

"DHCID", "UINFO", "UID", "GID", "UNSPEC", "ADDRS", "TKEY", "TSIG", "IXFR", "AXFR", "MAILB", "MAILA", "ALL", "WINS", "WINSR/NBSTAT".

TimeToLive
The record's time to live value.

Flags
The record's flags; one of "Question", "Answer", "Authority", "Additional".

DataLength
The length in bytes of the RecordData field.

RecordData
A container for DNS data specific to a single DNS record. The data fields that will appear here depend on what type of DNS record was captured, as shown below:

For PTR, NS, CNAME, DNAME, MB, MD, MF, MG and MR records

Host
A PTR host name.

For A records

IPv4Adress
An A record IPv4 address.

For SOA records

PrimaryServerName
The name of the authoritative DNS server for the zone to which the record belongs.

AdministratorName
The name of the responsible party.

SerialNumber
The serial number of the SOA record.

Refresh
The time span before the zone should be refreshed.

Retry
The time span before retrying a failed refresh of the zone.

Expire
The time span after which an unresponsive zone is no longer authoritative.

DefaultTimeToLive
The time which cache resolvers should expire a record.

For MINFO and RP records (mail information)

MailboxName
The fully qualified domain name of the mailbox responsible for the mailing list.

MailboxErrorsName
The fully qualified domain name of the mailbox to receive mailing list error messages.

For MX, AFSDB and RT records (mail exchanger)

MxHost
The fully qualified domain name of the host willing to act as a mail exchange.

Preference
The preference given to this record among others of the same owner.

For HINFO, ISDN, TEXT and X25 records (text record)

String
Descriptive text.

For NULL records

Blob
Null data.

For WKS records (well known service)

Protocol
"TCP" or "UDP"

IPv4Address
The IPv4 address of the service.

Bitmask
The bits of this bitmask correspond to the port number of the specified protocol.

For AAAA records

IPv6Address
The IPv6 address.

For KEY records

Algorithm
One of "RSA/MD5", "Diffie-Hellman", "DSA", "Elliptic Curve".

Protocol
"DNSSEC"

KeyFlags
A set of flags as specified in RFC 3445.

For SIG, RRSIG records

Signer
The name of the authority that signed the signature.

TypeCovered
Either "SIG" or "RRSIG".

Algorithm
One of "RSA/MD5", "Diffie-Hellman", "DSA", "Elliptic Curve".

LabelCount
The number of labels in the original signature RR owner name.

OriginalTimeToLive
The time-to-live value set by the signature.

ExpirationDate
The expiration date of the signature.

DateSigned
The date the signature became valid.

KeyTag
A value that represents the method to choose which public key is used to verify the signature.

For ATMA records (ATM address)

AddressType
The format of the ATM address; either "AESA" or "E164".

ATMAddress
An array of bytes representing the ATM address.

For NXT, NSEC records (next)

NextHost
The name of the next domain.

Type
The record type.

For SRV records (service)

TargetHost
The service target host name.

Priority
The priority of the target host; lower values imply higher priority.

Weight
The weight of the target host.

Port
The port used on the target host for this service.

For NAPTR records (Naming Authority Pointer)

Order
NAPTR processing order.

Preference
Preference value.

Flags
NAPTR flags.

Services
Available services.

RegularExpression
A substitution expression as defined in RFC 2915.

Replacement
NAPTR query name

For OPT records (option)

Blob
A byte array of variable transport level information (see RFC 2671).

For DS records (Delegation Signer)

Algorithm
One of "RSA/MD5", "Diffie-Hellman", "DSA", "Elliptic Curve".

DigestType
Always "SHA-1".

DigestLength
The length in bytes of the message digest.

Digest
The digest in byte array form.

KeyTag
A value that represents the method to choose which public key is used to verify the signature.

For DNSKEY recordS (public key)

Algorithm
One of "RSA/MD5", "Diffie-Hellman", "DSA", "Elliptic Curve".

Protocol
"DNSSEC".

KeyFlags
A set of flags as specified in RFC 3445.

KeyLength
The length of the associated public key.

PublicKey
The public key.

For TKEY records (Transaction key)

KeyName
The name of the key.

Key
The shared-secret key.

KeyLength
The length of the associated key.

CreationDate
The date the key was created.

ExpirationDate
The expiration date of the key.

Error
One of "Bad signature", "Bad key", or "Bad timestamp".

Mode
The scheme used for key agreement; one of "DNS_TKEY_MODE_SERVER_ASSIGN", "DNS_TKEY_MODE_DIFFIE_HELLMAN", "DNS_TKEY_MODE_GSS", "DNS_TKEY_MODE_RESOLVER_ASSIGN".

For TSIG records (Transaction signature)

KeyName
The name of the key.

Algorithm
One of "gss.microsoft.com" or "gss-tsig".

SignatureLength
The length of the signature.

Signature
The message authentication code (MAC) generated by the algorithm.

FudgeTime
The time, in seconds, the creation date might be in error (see MSDN).

OriginalXid
The Xid identifier of the original message.

For WINS records (Windows Internet Name Service)

MappingFlag
The WINS mapping flag that specifies whether the record must be included in zone replication; either "DNS_WINS_FLAG_SCOPE" or "DNS_WINS_FLAG_LOCAL".

WinsServerIPv4Address
The IPv4 address of the WINS server.

LookupTimeout
The time span that a DNS server attempts resolution using WINS lookup.

CacheTimeout
The time span that DNS server using WINS lookup may cache the WINS server's response.

For WINSR records (WINS reverse-lookup)

MappingFlag
he WINS mapping flag that specifies whether the record must be included in zone replication; either "DNS_WINS_FLAG_SCOPE" or "DNS_WINS_FLAG_LOCAL".

Host
The host name of the WINS server.

LookupTimeout
The time span that a DNS server attempts resolution using WINS lookup.

CacheTimeout
The time span that DNS server using WINS lookup may cache the WINS server's response.

For DHCID records (Dynamic Host Configuration Protocol Information)

Blob
A byte array of DHCID client, domain and SHA-256 digest information (see RFC 2671).

1.17.2. How to Run `w32network-dns`

In the Job or Script Editor, use the Agent Module chooser to select w32network-dns.

Parameters:

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.18. Host Network Routing Table: `w32network-route`

Analyses the IPv4 and IPv6 routing tables which store information about how a network destination is routed on a given interface.

1.18.1. Audit Data

IsIPv6
True if this record is an IPv6 record.

Interface
The IPv4 or IPv6 address of the network interface.

Destination
The route destination.

Gateway
The gateway address used in the route.

Netmask
The netmask used in the route.

RouteType
One of "Direct", "Indirect", "Invalid" or "Other" (IPv4 only).

Protocol
One of "Local", "Netmgmt", "ICMP", "EGP", "GGP", "Hello", "RIP", "IS-IS", "ES-IS", "Cisco IGRP", "BBN IGP", "OSPF", "BGP", "Auto Static", "Static", "Static Non DOD", "Unknown" or "Other"

ValidLifetime
The time span of the maximum validity of the route (IPv6 only).

PreferredLifetime
The time span of the preferred validity of the route (IPv6 only).

RouteAge
The time span since the route was added or modified in the routing table.

Metric
The route metric.

IsLoopback
True if the device is a loopback device (IPv6 only).

IsAutoconfigureAddress
True if the device address is autoconfigure (IPv6 only).

IsPublish
True if the route is a published route (IPv6 only).

IsImmortal
True if the route is an immortal route (IPv6 only.

Origin
One of "Manual", "Well-known", "DHCP", "Router Advertisement", or "6 to 4 tunneling" (IPv6 only).

1.18.2. How to Run `w32network-route`

In the Job or Script Editor, use the Agent Module chooser to select w32network-route.

Parameters:

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.19. Inclusion Filter: `regexv2`

Filters an XML Audit Data document **before** all other filters, allowing only qualified data to pass to the standard filter stream.

1.19.1. Audit Data

None.

1.19.2. How to Run `regexv2`

The `regexv2` filter must be added manually to the filter batch script. The following parameters are required:

Parameters:

expression (String)
A regular expression to be applied to each item in an XML Audit Data document. If the expression evaluates to true, the item will be included, otherwise it will be omitted.

type (String)
The type of filter. Acceptable values: Inclusion, Standard.

path (String)
The path to the item being filtered. Used only with Inclusion filters.

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.19.3. Usage Examples

Example A.1. Excluding FileItems

```
<filter>
  <module name="regexv2"/>
  <config type="ParameterListModuleConfig">
    <parameters>
      <param name="type">
        <value type="xsd:string">Inclusion</value>
      </param>
      <param name="path">
        <value type="xsd:string">\FileItem\StringList\string</value>
      </param>
      <param name="expression">
        <value type="xsd:string">ZRandom</value>
      </param>
    </parameters>
  </config>
</filter>
```

The Inclusion filter passes all data *except* those entries in `FileItem\StringList\string` that *do not* match the text `ZRandom`. All other items in the resulting document

are written to the Audit Result document, as there are no standard filters being applied subsequent to the inclusion filter.

Example A.2. Multiple Exclusions

```
<filter>
  <module name="regexv2"/>
  <config type="ParameterListModuleConfig">
    <parameters>
      <param name="type">
        <value type="xsd:string">Inclusion</value>
      </param>
      <param name="path">
        <value type="xsd:string">\FileItem\StringList\string</value>
      </param>
      <param name="expression">
        <value type="xsd:string">ZRandom</value>
      </param>
    </parameters>
  </config>
</filter>
<filter>
  <module name="regexv2"/>
  <config type="ParameterListModuleConfig">
    <parameters>
      <param name="type">
        <value type="xsd:string">Inclusion</value>
      </param>
      <param name="path">
        <value type="xsd:string">\FileItem\PEInfo\ImportedModules\Module
\ImportedFunctions\string</value>
      </param>
      <param name="expression">
        <value type="xsd:string">ZShellResourceManager</value>
      </param>
    </parameters>
  </config>
</filter>
```

As in the previous example, the first filter passes all data, except those in `FileItem\StringList\string` that do not match `ZRandom`. An additional Inclusion filter passes all data, but includes only those `FileItem\PEInfo\ImportedModules\Module\ImportedFunctions\string` named `ZShellResourceManager`. All other items in the resulting document are written to the Audit Result document, as there are no standard filters being applied subsequent to the inclusion filters.

Example A.3. Inclusion and Standard Filtering Combination

```
<filter>
  <module name="regexv2"/>
  <config type="ParameterListModuleConfig">
    <parameters>
      <param name="type">
        <value type="xsd:string">Inclusion</value>
      </param>
      <param name="path">
        <value type="xsd:string">\FileItem\StringList\string</value>
```

```
      </param>
      <param name="expression">
        <value type="xsd:string">ZRandom</value>
      </param>
    </parameters>
  </config>
</filter>
<filter>
  <module name="xpath2v2"/>
  <config type="ParameterListModuleConfig">
    <parameters>
      <param name="expression">
        <value type="xsd:string">/FileItem/PEInfo/ImportedModules/Module[Name
 = 'GDI32.dll']</value>
      </param>
    </parameters>
  </config>
</filter>
```

As in the first example, the data stream is stripped of those `FileItem\StringList\string` that do not match `ZRandom`. A standard filter is then applied that passes only those `/FileItem/PEInfo/ImportedModules/Module` named `GDI32.dll`.

1.20. Network Ports Listing: `w32ports`

1.20.1. General Information

Active and listening ports and, where available, the process associated with them.

Running two ports audits simultaneously may cause both to fail.

Collects a listing of all open network ports, the process they are associated with, port status, and the address and port number it is connected to.

1.20.2. Audit Data

Pid
Process ID for the process using the network port.

Process
Name of the process using the port.

Path
Path to the executable file on disk that spawned the process.

State
Current state for the network port and associated connection (e.g. Listening, Established, TimeWait, Unknown).

LocalIP
Local IP address to which the port is bound.

RemoteIP
Remote IP address to which the port is bound.

LocalPort
Local port number to which the port is bound.

RemotePort
Remote port to which the port is bound.

Protocol
Protocol being used by the port (e.g. TCP, UDP).

1.20.3. How to Run `w32ports`

In the Job or Script Editor, use the Agent Module chooser to select w32ports.

Running two ports audits simultaneously may cause both to fail.

Parameters:

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.21. Persistence: `w32scripting-persistence`

1.21.1. General Information

Get details of the persistence locations.

1.21.2. Audit Data

For each persistence key or startup item, the Audit module attempts to locate an associated file. If a file is not applicable to the key or value name, or it cannot be opened, file information is not recorded in the persistence item (only a *RegistryItem* will be contained in the *PersistenceItem*). If a file was determined from the startup folder, registry information is not recorded in the persistence item (only a *FileItem* will be contained in the *PersistenceItem*).

Services are enumerated from the Service Control Manager (SCM) database using Win32API through the traditional Service Audit module, rather than through the registry. Therefore, *PersistenceItems* written for a service will not include a *RegistryItem*. If the service has an associated binary (and/or DLL), a *PersistenceItem* containing a *FileItem* and a *ServiceItem* will be written for each.

Persistence data is stored as a series of *PersistenceItem* structures in an XML document. The complete schema for a *PersistenceItem* consists of a *RegistryItem*, a *FileItem*, a *ServiceItem*, and several top-level fields which are simply "bubbled up" from the other embedded items (this is done to account for sorting/filtering limitations for nested items in Console). This XML structure is illustrated below[1]:

```
<PersistenceItem>
top level fields for sorting
```

[1] Full Schema is available from MANDIANT Support.

```
    <RegistryItem>registry fields</RegistryItem>
    <FileItem>file fields</FileItem>
    <ServiceItem>service fields</ServiceItem>
</PersistenceItem>
```

One top-level field is not there just for sorting—RegContext. This field helps an investigator identify why the item is being reported as a persistence item when such an inference cannot be made from the Registry path itself. For example, when parsing CLSIDs it is useful to retain the top-level key context to know which persistence mechanism it belongs to (Context handler, browser helper object, etc).

PersistenceType may have a value of *Registry*, *Service*, *ServiceDll*, or *Link*, describing the persistence mechanism used for the related file.

Caveats and Notes

The following keys will not report a *FileItem* due to the nature of the data they contain (persistence is not necessarily gained through execution of a file):

HKLM\Software\Microsoft\Windows NT\CurrentVersion\IniFileMapping
: This key contains various registry *Value Names* that describe an INI autorun mapping strategy that windows uses to parse INI files.

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options*
: Each subkey contains various registry *Value Names* that describe runtime configuration options for the given image/process.

Not all CLSIDs correspond to an entry in the HKCR hive. In such cases, a *FileItem* will not be reported. In the Startup folder, files that are not links or executable will not generate a *FileItem* entry.

Any of the registry walks may encounter cases where a persistence file cannot be parsed from its registry value. This is because the audit module must sanitize the input string stored in the registry value and cannot account for all possible formats. For example, `rundll32` and `regsvr32` have a predictable format which can be reliably parsed. Also, if the string contains a recognizable path such as `System32` or `Program Files`, the audit module may be able to resolve the path. However, there are other cases that will fail the sanitization function and a *FileItem* will not be reported.

Any file that has a LNK extension is assumed to be a Microsoft LNK shortcut file and subsequently parsed to locate the target of the shortcut. If successfully parsed and the target file can be opened, a *FileItem* is reported for the target file (not the LNK file itself). There are a few known limitations with LNK parsing (such as `Recent Places` and `Recycle Bin` shortcuts), but most common cases are handled successfully in our testing.

itemList
: A list of discovered persistence items.

  PersistenceItem
  : A discovered persistence item. Returned data includes the persistence mechanism used; details on how the item was discovered; full file information including checksums, entropy data, and anomalies; and registry details.

1.21.3. How to Run `w32scripting-persistence`

In the Job or Script Editor, use the Agent Module chooser to select w32scripting-persistence.

Parameters:

MD5 (Boolean)
Compute the MD5 hash for each returned file.

Default: false

SHA1 (Boolean)
Compute the SHA1 hash for each returned file.

Default: false

SHA256 (Boolean)
Compute the SHA256 hash for each returned file.

Default: false

Preserve Times (Boolean)
Manually reset last access times for audited files.

Default: false

Analyze Entropy (Boolean)
Calculate entropy for executable files. High entropy may indicate a packed executable.

Default: false

Enumerate Imports (Boolean)
Identify modules and functions imported by executable files.

Default: false

Enumerate Exports (Boolean)
Identify modules and functions exported by executable files.

Default: false

Analyze File Anomalies (Boolean)
Detect higher-order anomalies which may indicate malicious files.

Default: false

Scan Entry Point Distance (Integer)
Specifies the number of bytes from the entry point to scan for jumps.

Verify Digital Signatures (Boolean)
Verify the digital signature on executable files

Default: false

Get Resources (Boolean)
Return resources stored in a PE file.

Default: false

Get Version Info (Boolean)
Return version information stored in a PE file.

Default: false

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.22. Prefetch:`w32prefetch`

Enumerates prefetch files in `%SystemRoot%\Prefetch`. Returns a list of all prefetch files and parses each file for information saved by the Windows prefetcher when the associated binary is run.

Windows prefetching is supported only on Windows XP, Windows Server 2003, and later system. If prefetching has at any time been disabled on the system, prefetch information may not be available.

1.22.1. Audit Data

ApplicationFullPath
Fully qualified path and name of the prefetch file.

CreationTime
The date and time the prefetch file was created.

SizeInBytes
Size of the file in bytes.

PrefetchHash
A 32-bit prefetch hash generated by Windows.

ReportedSizeInBytes
The expected size of the file (as encoded inside the prefetch file).

ApplicationFileName
The name of the executable binary associated with this prefetch file.

LastRun
The date and time the associated application was last run.

TimesExecuted
The number of times the associated application has been run since the creation of the prefetch file.

AccessedFileList
A list of all files accessed by the application, as recorded by the Windows prefetcher.

VolumeList
A list of information about each volume containing files listed in the AccessedFileList. This information is parsed from the prefetch file: it is not from a live volume audit.

1.22.2. How to Run `w32prefetch`

In the Job or Script Editor, use the Agent Module chooser to select w32prefetch.

Parameters:

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.23. Process Listing (API Mode): `w32processes-API`

1.23.1. General Information

Lists running processes as reported by the operating system.

Collects a listing of all processes running on the target system by enumerating all running threads to identify process information.

1.23.2. Audit Data

Pid
Process ID for the process.

ParentPid
Process ID for the parent process of this process.

UserOwner
Name of the user that owns the process. May not be populated in a w32processes-memory audit.

SID
Security Identifier for the UserOwner. May not be populated in a w32processes-memory audit.

SecurityType
SID Type for the UserOwner. May not be populated in a w32processes-memory audit.

Path
Path to the executable on disk that started this process.

Name
Process name.

Arguments
Arguments passed to the process when it was started.

StartTime
Date/time according to the system clock that the process was started in GMT.

Kernel Time Elapsed
Amount of execution time for the process in hours:minutes:seconds.

User Time Elapsed
Time elapsed since process was started, including both execution and idle time in hours:minutes:seconds.

1.23.3. Item Details

Detail View information for individual processes is not used in the `w32processes-API` audit. However, additional information is provided in the Process Listing (Memory) audit.

1.23.4. How to Run `w32processes-API`

In the Job or Script Editor, use the Agent Module chooser to select w32processes-API.

Parameters:

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.24. Process Listing (Handles Mode): `w32processes-handle`

1.24.1. General Information

Collects a listing of all processes running on the target system by tracing all threads back to the process that created them and then eliminating duplicates.

1.24.2. Audit Data

Pid
Process ID for the process.

ParentPid
Process ID for the parent process of this process.

UserOwner
Name of the user that owns the process. May not be populated in a w32processes-memory audit.

SID
Security Identifier for the UserOwner. May not be populated in a w32processes-memory audit.

SecurityType
SID Type for the UserOwner. May not be populated in a w32processes-memory audit.

Path
Path to the executable on disk that started this process.

Name
Process name.

Arguments
Arguments passed to the process when it was started.

StartTime
Date/time according to the system clock that the process was started in GMT.

Kernel Time Elapsed
Amount of execution time for the process in hours:minutes:seconds.

User Time Elapsed
Time elapsed since process was started, including both execution and idle time in hours:minutes:seconds.

1.24.3. How to Run w32processes-handles

In the Job or Script Editor, use the Agent Module chooser to select Process Listing (Handles Mode).

1.24.4. How to Run `w32processes-handle`

In the Job or Script Editor, use the Agent Module chooser to select w32processes-handle.

Parameters:

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.24.5. Item Details

Detail View information for individual processes is not used in the w32processes-handles audit. However, additional information is provided in the Process Listing (Memory) audit.

1.25. Process Listing (Memory): `w32processes-memory`

1.25.1. General Information

Lists running processes with comprehensive information about imported modules, sections, and other data gathered from advanced memory scanning techniques.

May return more information than expected if run against all processes, specifying a PID is recommended.

Collects a listing of all processes running on the target system by directly parsing structures contained in system memory.

On Hosts that do not support memory-related audits, such as Windows Vista 64 bit, an Issue Document will be returned indicating an error occurred and that the Audit could not determine the OS version.

Windows 2000, Windows 2003, Windows XP. If you select the Preserve Times option, the module will manually "preserve" the last accessed time by recording it before the file is read, and restoring it to that value after the file is read.

Windows Vista, Windows 7. You must disable Preserve Times. If you need to preserve the file time, choose a Raw Mode file audit module instead.

1.25.2. Audit Data

Pid
Process ID for the process.

ParentPid
Process ID for the parent process of this process.

UserOwner
Name of the user that owns the process. May not be populated in a w32processes-memory audit.

SID
Security Identifier for the UserOwner. May not be populated in a w32processes-memory audit.

SecurityType
SID Type for the UserOwner. May not be populated in a w32processes-memory audit.

Path
Path to the executable on disk that started this process.

Name
Process name.

Arguments
Arguments passed to the process when it was started.

StartTime
Date/time according to the system clock that the process was started in GMT.

Kernel Time Elapsed
Amount of execution time for the process in hours:minutes:seconds.

User Time Elapsed
Time elapsed since process was started, including both execution and idle time in hours:minutes:seconds.

1.25.3. How to Run `w32processes-memory`

In the Job or Script Editor, use the Agent Module chooser to select w32processes-memory.

May return more information than expected if run against all processes, specifying a PID is recommended.

Parameters:

pid (Integer)
Specifies the Process ID (PID) of the process to analyze.

process name (String)
The first 15 characters of the process name. Cannot be specified in conjunction with PID.

handles (Boolean)
Boolean indicating whether or not to parse the process handles.

Default: false

sections (Boolean)
Boolean indicating whether or not to parse the process memory sections.

Default: false

ports (Boolean)
Boolean indicating whether or not to parse the process for open ports.

Default: false

enumerate imports (Boolean)
Boolean indicating whether or not to enumerate imports of all loaded modules for a given process.

Default: false

enumerate exports (Boolean)
Boolean indicating whether or not to enumerate exports of all loaded modules for a given process.

Default: false

Content Regex (Strings)
Only return processes with particular content.

Preserve Times (Boolean)
Manually reset last access times for audited files.

Default: false

MemD5 (Boolean)
Compute the MD5 hash for each returned file from memory.

Default: false

MD5 (Boolean)
Compute the MD5 hash for each returned file.

Default: false

SHA1 (Boolean)
Compute the SHA1 hash for each returned file.

Default: false

SHA256 (Boolean)
Compute the SHA256 hash for each returned file.

Default: false

Verify Digital Signatures (Boolean)
Boolean indicating whether or not to verify if the loaded modules within the processes address space are digitally signed. This operation can not be performed on a memory image.

Default: false

raw mode (Boolean)
Open files for hashing in raw mode.

Default: false

detect injected dlls (Boolean)
Boolean indicating whether or not to detect injected dlls.

Default: false

strings (Boolean)
Boolean indicating whether or not to parse a specified process for strings. If strings is enabled, default string length is 4.

Default: false

shortest matched string (Integer)
Minimum Recognized String Length. Default: 4

memory file (String)
The full path and filename of the file that represents the host's physical memory.

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.25.4. Item Details

Additional data may be provided on some process items. These may be viewed through the Details Viewer.

Detected Anomalies
For future use.

Handles
The list of open handles for the process and data associated with each handle. Includes the AccessMask for the handle, its name, address, pointer count, and type (e.g., event, file handle, semaphore, mutex).

Memory Sections
The list of distinct memory sections within the process. Identifies mapping status, name (e.g. `kernel32.dll`), flags, region size, and the starting memory offset for that section.

Open Ports
The list of open network ports for the selected process. Includes protocol, state, creation time, local endpoint, and remote endpoint.

Imports
Lists modules and function calls imported by the process.

Exports
Lists function calls exported by the process.

String Information
If string extraction was requested for the process, contains the list of strings of the minimum length requested or longer.

1.26. Process Memory Acquire: `w32processes-memoryacquire`

1.26.1. General Information

Allows for the acquisition of memory space for a specified process.

Acquires a copy of the memory in use by a running process on the target system.

On Hosts that do not support memory-related audits, such as Windows Vista 64 bit, an Issue Document will be returned indicating an error occurred and that the Audit could not determine the OS version.

1.26.2. Audit Data

The module returns the requested memory image. Any errors encountered will be reported in an Issues document (see _Error Messages and Troubleshooting_ in the Appendices). The image can be exported from the Controller to your local machine via the Console.

1.26.3. How to Run `w32processes-memoryacquire`

In the Job or Script Editor, use the Agent Module chooser to select w32processes-memoryacquire.

Parameters:

pid (Integer)
Specifies the Process ID (PID) of the process to analyze.

process name (String)
The first 15 characters of the process name. Cannot be specified in conjunction with PID.

Content Regex (Strings)
Only return processes with particular content.

memory file (String)
The full path and filename of the file that represents the host's physical memory.

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.27. RegEx: `regex`

Filters an XML Audit Data document.

1.27.1. Audit Data

../generated

1.27.2. How to Run `regex`

In the Job or Script Editor, use the Agent Module chooser to select regex.

Parameters:

expression (String)
A regular expression to be applied to each item in an XML Audit Data document. If the expression evaluates to true, the item will be included, otherwise it will be omitted.

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.28. Registry Listing (API Mode): `w32registryapi`

1.28.1. General Information

Returns a listing of registry keys using standard API methods

Returns a list of registry keys and values from the target system. The module uses Windows system APIs to retrieve the data, and is therefore subject to the access restrictions and limitations of the target OS. Refer to Microsoft operating system and developer documentation for more information about the Windows Registry.

1.28.2. Audit Data

Path
Path to the registry key. Includes hive name.

Type
Type of registry key entry (e.g. REG_KEYREG_DWORDREG_SZREG_BINARY).

Modified
Last modified date/time for the key, if known.

NumSubKeys
Number of registry keys subordinate to this key.

NumValues
Number of values stored within this key and all subordinate keys.

ReportedLengthInBytes
Length of the value, provided in the registry key.

Hive
The name of the hive in the path to the registry item.

KeyPath
The portion of the path that contains the parent keys of the registry item.

ValueName
The value name of the registry item.

Username
The name of the Windows user account that owns the registry item.

Text
The text representation of the data stored in the registry item, if applicable.

Value
The binary representation of the data stored in the registry item, if applicable.

detectedAnomaly
Any identified anomalies present during the audit.

1.28.3. How to Run `w32registryapi`

In the Job or Script Editor, use the Agent Module chooser to select w32registryapi.

Parameters:

Path (String)
Top-level Registry key to walk from. Path if specified must include the hive name (such as HKLM).

Path Regex (String)
Specifies the Perl Compatible Regular Expression a key or value name must match to be returned. Examples: Match any key or value in any sub-key of the root: .* Match any key or value named Run in any sub-key: .*\\Run Match any key or value in a sub-key of Services: .*\\Services\\.* (note that backslashes must be escaped).

Value Regex (String)
Return results only for values that contain data matching a Perl Compatible regular expression, such as "svchost(\d\d)?\.exe". Note that REG_SZ values are automatically converted from UTF16 to UTF8 for comparison, all other values are compared "as-is".

Type (String)
Control whether keys and values are returned. Valid values for type are "KeysOnly", "ValuesOnly", or "All". Default is "All".

Depth (Integer)
Specifies the number of levels to recurse in the tree of keys rooted at root_key. Use -1 to recurse the entire tree. Starting depth is not relative to the hive.

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.28.4. Item Details

Additional data may be provided on some registry items. These may be viewed through the Details Viewer.

Value
If the data stored in the registry key is a byte array (versus a text value), the raw byte sequence is displayed (in decimal).

1.29. Registry Listing (Raw Mode): `w32registryraw`

1.29.1. General Information

Returns a listing of registry keys using Raw methods which may bypass security and access restrictions.

Returns a list of registry keys and values from the target system. The module bypasses Windows system APIs to retrieve the data and instead directly accesses the registry hives from the file system by directly reading sectors from the target system's disk. It is therefore not subject to access restrictions, and can read sections of the registry not available to `w32registryapi`.

It should also be noted that the `w32registryraw` module can only read the information in the registry directly on disk. The Windows operating system creates many "virtual linkages" (similar to symlinks or aliases on a file system) that `w32registryraw` cannot see. As such, the raw registry structure may look significantly different than the virtual registry structure. Note that the virtual structure is what most users are familiar with—it is the same structure as presented by tools such as RegEdit.

Refer to Microsoft operating system and developer documentation for more information about the Windows Registry and how physical and virtual registry structures differ.

Since the API and Raw registry structures differ significantly, performing an analysis such as a Diff, will typically not yield useful results. w32registryraw is useful primarily for finding hidden data or information that you could not otherwise access via `w32registryapi`, not for comparisons between API and Raw versions of the audit.

1.29.2. Audit Data

Path
Path to the registry key. Includes hive name.

Type
Type of registry key entry (e.g. REG_KEYREG_DWORDREG_SZREG_BINARY).

Modified
Last modified date/time for the key, if known.

NumSubKeys
Number of registry keys subordinate to this key.

NumValues
Number of values stored within this key and all subordinate keys.

ReportedLengthInBytes
Length of the value, provided in the registry key.

Hive
The name of the hive in the path to the registry item.

KeyPath
The portion of the path that contains the parent keys of the registry item.

ValueName
The value name of the registry item.

Username
The name of the Windows user account that owns the registry item.

Text
The text representation of the data stored in the registry item, if applicable.

Value
The binary representation of the data stored in the registry item, if applicable.

detectedAnomaly
Any identified anomalies present during the audit.

1.29.3. How to Run `w32registryraw`

In the Job or Script Editor, use the Agent Module chooser to select w32registryraw.

Parameters:

Path (String)
Top-level Registry key to walk from. Path if specified must include the hive name (such as HKLM).

Path Regex (String)
Specifies the Perl Compatible Regular Expression a key or value name must match to be returned. Examples: Match any key or value in any sub-key of the root: .* Match any key or value named Run in any sub-key: .*\\Run Match any key or value in a sub-key of Services: .*\\Services\\.* (note that backslashes must be escaped).

Value Regex (String)
Return results only for values that contain data matching a Perl Compatible regular expression, such as "svchost(\d\d)?\.exe". Note that REG_SZ values are automatically converted from UTF16 to UTF8 for comparison, all other values are compared "as-is".

Type (String)
Control whether keys and values are returned. Valid values for type are "KeysOnly", "ValuesOnly", or "All". Default is "All".

Depth (Integer)
Specifies the number of levels to recurse in the tree of keys rooted at root_key. Use -1 to recurse the entire tree. Starting depth is relative to the hive (eg, \HKLM\SOFTWARE).

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.29.4. Item Details

Additional data may be provided on some registry items. These may be viewed through the Details Viewer.

Value
If the data stored in the registry key is a byte array (versus a text value), the raw byte sequence is displayed (in decimal).

1.30. Registry Hive Listing: `w32hivelist`

1.30.1. General Information

Lists registry hives for use in a Registry Listing audit. Includes hives which can only be acquired in Raw mode (such as the SAM hive).

Returns the Hive Name and Hive Key for Windows Registry hives on the target system. Run this Audit before running either the `w32registryapi` or `w32registryraw` Audits to locate the path name to use in either of those Audits.

1.30.2. Audit Data

HiveName
The name of the registry hive (e.g. HKEY_LOCAL_MACHINE\SAM, HKEY_LOCAL_MACHINE_SECURITY, HKEY_LOCAL_MACHINE_SYSTEM)

HiveKey
The path to the file on the target system hard drive containing the registry hive.

1.30.3. How to Run `w32hivelist`

In the Job or Script Editor, use the Agent Module chooser to select w32hivelist.

Parameters:

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.31. Restart Agent

This module lets you restart a deactivated Agent on a target system.

1.31.1. Audit Data

This module does not return audit data.

1.31.2. How to Run Restart Agent

In the Job or Script Editor, use the Agent Module chooser to select deactivate.

Parameters:

immediate (Boolean)
Execute the command immediately without waiting for existing audits to finish.

Default: false

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.32. Services Listing: `w32services`

1.32.1. General Information

Returns a list of installed services from the target system using Windows system APIs.

Windows 2000, Windows 2003, Windows XP. If you select the Preserve Times option, the module will manually "preserve" the last accessed time by recording it before the file is read, and restoring it to that value after the file is read.

Windows Vista, Windows 7. You must disable Preserve Times. If you need to preserve the file time, choose a Raw Mode file audit module instead.

1.32.2. Audit Data

name
Name of the service.

descriptiveName
Human readable name as specified by the service.

mode
Start-up mode for the service (e.g., SERVICE_DEMAND_START, SERVICE_BOOT_START, SERVICE_DISABLED, SERVICE_AUTO_START)

startedAs
User the service was started as.

path
Path to the executable that started the service. Includes any arguments provided during startup.

serviceDLL
Path to the DLL, if any, that controls the service.

status
Current running status of the service (e.g. SERVICE_RUNNING, SERVICE_STOPPED).

PID
Process ID of the running service.

type
Service type (e.g. SERVICE_WIN32_SHARE_PROCESS , SERVICE_KERNEL_DRIVER, SERVICE_WIN32_OWN_PROCESS, SERVICE_FILE_SYSTEM_DRIVER).

1.32.3. How to Run `w32services`

In the Job or Script Editor, use the Agent Module chooser to select w32services.

Parameters:

MD5 (Boolean)
Compute the MD5 hash for each returned file.

Default: false

SHA1 (Boolean)
Compute the SHA1 hash for each returned file.

Default: false

SHA256 (Boolean)
Compute the SHA256 hash for each returned file.

Default: false

Verify Digital Signatures (Boolean)
Verify the digital signature on executable files

Default: false

Preserve Times (Boolean)
Manually reset last access times for audited files.

Default: false

raw mode (Boolean)
Open files for hashing in raw mode.

Default: false

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.32.4. Item Details

Additional data may be provided on some services items. These may be viewed through the Details Viewer.

description
A collection of additional descriptive text supplied by the service that may further describe its function.

1.33. System Information: `w32system`

1.33.1. General Information

General system information such as network devices, registration information, and local time.

Returns a series of information about the target system's configuration, including name, date/time settings, currently logged in user, network interfaces, and operating system version. Uses Windows API calls to obtain all data returned in the Audit.

1.33.2. Audit Data

Available Physical Memory
Currently available memory on the target system.

Bios
BIOS name.

BiosDateString
Date string information provided by the BIOS.

BiosVersion
BIOS version number.

Detected Anomalies
For future use.

Domain
Windows Domain to which the system is currently assigned.

Hostname
Hostname as reported by the target system.

InstallDate
Install date/time for the operating system on the target system.

ItemGenerated
Date/Time the system information was gathered by MIR according to the system clock of the target system where the Agent was installed. Time presented as GMT.

LoggedInUser
User that was logged into the system at the time of the Audit.

MachineName
Machine name, as reported by the target system.

NetworkInfoList
A collection of network information from the target system, including network interfaces, DHCP configuration, and MAC addresses.

OSbitness
The word length of the Host OS: 32-bit or 64-bit.

OsBuild
OS build number.

OsString
OS version string.

PatchLevel
OS patch level.

Primary Network Adapter MAC
MAC of the default network interface.

Processor Identity
Processor identification string.

ProcType
Processor type.

ProductId
Product identifier for the installed operating system.

ProductName
Name of the installed operating system.

Registered Organization
Registered organization for the operating system installed on the target system.

Registered Owner
Registered owner for the operating system installed on the target system.

System Date
Date/time reported by the system at the time of the Audit.

TimeZoneDST
Default timezone for daylight savings time.

TimeZoneStandard
Default timezone for standard time.

Total Physical Memory
Total amount of physical memory installed in the system.

Uptime
Uptime for the system as reported at the time of the Audit.

1.33.3. How to Run `w32system`

In the Job or Script Editor, use the Agent Module chooser to select w32system.

Parameters:

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.33.4. Item Details

Additional details are displayed about each network adapter in the system:

Adapter
The system identifier for the network adapter.

Description
Friendly name for the adapter.

Dhcp Lease Expires
Date/time the current DHCP lease expires for the interface, if any.

Dhcp Lease Obtained
Date/time the current DHCP lease was obtained for the interface, if any.

Dhcp Server List
List of DHCP servers providing addresses to the interface.

IpGateway List
Default gateway information for the interface.

Ip Info List
IP address and netmask settings for the interface.

MacAddress
Mac address for the interface.

1.34. System Restore: `w32systemrestore`

1.34.1. General Information

Get details associated with each restore point on a Windows XP system.

1.34.2. Audit Data

AclChangeSecurityID
Security Identifier associated with this change log entry.

AclChangeUsername
User name associated with this change log entry.

BackupFileName
Name of the backup file used to restore the change log entry

ChangeEvent
General event that caused parent restore point to be created (e.g. 'System Checkpoint' or 'Software Installation').

ChangeLogEntryFlags
Flags for this change log entry.

ChangeLogEntrySequenceNumber
Sequence number for this change log entry.

ChangeLogFileName
Name of the change log file for the restore point.

Created
Date and time parent restore point was created.

DebugInfoProcessId
Debug process ID for the change log entry.

DebugInfoProcessName
Debug process name for the change log entry.

DebugInfoThreadId
Debug thread ID for the change log entry.

DebugInfoTimeStamp
Debug timestamp for the change log entry.

FileAttributes
Attributes for the object described by this change log entry.

NewFileName
File path for a renamed change log entry.

OriginalFileName
File path for the change log entry.

OriginalShortFileName
Short name of the backup file.

OriginalVolumePath
Volume path for the change log entry.

ProcessName
Name of the process that made the change.

RegistryHives
List of hive files contained in parent restore point's registry snapshot.

ReportEntryType
Type of the change log entry.

RestorePointDescription
Description of parent restore point (i.e. why it was created).

RestorePointFullPath
Full path and directory of parent restore point.

RestorePointName
Name of the log file for this entry's parent restore point.

RestorePointType
Type of parent restore point.

1.34.3. How to Run `w32systemrestore`

In the Job or Script Editor, use the Agent Module chooser to select w32systemrestore.

Parameters:

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.35. Task Listing: w32tasks

1.35.1. General Information

List of Scheduled tasks (created via the 'at' command or Task Scheduler)

Returns the list of tasks from the target system that were scheduled with Task Scheduler or the ‘at’ command.

Windows 2000, Windows 2003, Windows XP. If you select the Preserve Times option, the module will manually “preserve” the last accessed time by recording it before the file is read, and restoring it to that value after the file is read.

Windows Vista, Windows 7. You must disable Preserve Times. If you need to preserve the file time, choose a Raw Mode file audit module instead.

1.35.2. Audit Data

AccountName
User account the task will run as.

ApplicationName
Path to the application that will execute as part of the task.

Comment
User supplied comments.

Creator
User that created the task.

ExitCode
Exit code from last execution of task.

Flags
Any flags set when task was scheduled (e.g. TASK_FLAG_DONT_START_IF_ON_BATTERIES, TASK_FLAG_KILL_IF_GOING_ON_BATTERIES).

MaxRunTime
Maximum time the task will be allowed to run.

Most Recent Run Time
Most recent run time of the task.

Name
Task name.

NextRunTime
Next scheduled execution time for the task.

Parameters
Parameters passed to the task at run time.

Priority
Priority set by the user (e.g. NORMAL_PRIORITY_CLASS).

Status
Task execution status (e.g. SCHED_S_TASK_HAS_NOT_RUN).

Working Directory
Working directory for the task when it executes.

1.35.3. How to Run `w32tasks`

In the Job or Script Editor, use the Agent Module chooser to select w32tasks.

Parameters:

MD5 (Boolean)
Compute the MD5 hash for each returned file.

Default: false

SHA1 (Boolean)
Compute the SHA1 hash for each returned file.

Default: false

SHA256 (Boolean)
Compute the SHA256 hash for each returned file.

Default: false

Verify Digital Signatures (Boolean)
Verify the digital signature on executable files

Default: false

Preserve Times (Boolean)
Manually reset last access times for audited files.

Default: false

raw mode (Boolean)
Open files for hashing in raw mode.

Default: false

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.35.4. Item Details

Additional data may be provided on some task items. These may be viewed through the Details Viewer.

TriggerList
List of execution triggers.

WorkItemData
List of data needed to run the task.

1.36. User Accounts: `w32useraccounts`

1.36.1. General Information

1.36.2. Audit Data

User Name
Name of the user.

Full Name
Full name of the user.

Description
Text description of the account, if any.

Home Directory
Home directory for the user on the target system.

Script Path
Script path set for the user.

Security ID
SID for the user.

Security Type
SID Type (typically `SidTypeUser`).

Last Login
Last login date/time for the user according to the target system clock.

Is Disabled
True if the account is disabled.

Is Locked Out
True if the account is locked-out.

Is Password Required
True if the account requires a password to log in.

Password Age
Password age in days, hours, minutes, and seconds. (ddd.hh:mm:ss).

1.36.3. How to Run `w32useraccounts`

In the Job or Script Editor, use the Agent Module chooser to select w32useraccounts.

Parameters:

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.36.4. Item Details

Additional data may be provided on some task items. These may be viewed through the Details Viewer.

Groups
List of groups in which the user is a member.

1.37. Volume Listing: `w32volumes`

1.37.1. General Information

List volumes which may be mounted by physical disks.

1.37.2. Audit Data

VolumeName
System identifier for the volume.

DevicePath
System path to the volume.

DriveLetter
Drive letter assigned to the volume.

VolumeType
Type of volume (e.g. DRIVE_FIXED, DRIVE_REMOVABLE).

Name
User-assigned name for the volume, if any.

Volume Serial Number
Serial number reported by the volume.

FileSystemFlags
Comma separated listing of flags set on the volume (e.g. FILE_CASE_SENSITIVE_SEARCH, FILE_CASE_PRESERVED_NAMES, FILE_UNICODE_ON_DISK, FILE_PERSISTENT_ACLS, FILE_FILE_COMPRESSION, FILE_VOLUME_QUOTAS, FILE_SUPPORTS_SPARSE_FILES, FILE_SUPPORTS_REPARSE_POINTS, FILE_SUPPORTS_OBJECT_IDS, FILE_SUPPORTS_ENCRYPTION, FILE_NAMED_STREAMS).

FileSystemName
Name of file system type for the volume (e.g. NTFS, FAT).

Actual Available Allocation Units
Free allocation units available on the volume.

Total Allocation Units
Total allocation units on the volume.

BytesPerSector
Volume sector size, in bytes.

Sectors Per Allocation Unit
Allocation unit size, in sectors.

CreationTime
Date/time volume was created, as reported by the target system.

IsMounted
Indicates whether or not the volume is currently mounted.

1.37.3. How to Run `w32volumes`

In the Job or Script Editor, use the Agent Module chooser to select w32volumes.

Parameters:

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.38. Web Historian Cookie History: `cookiehistory`

Returns a history of Cookies stored on the system

Cookie history is not available for Safari 4 and Safari 5.

1.38.1. Audit Data

Profile
The name of the user profile folder (Firefox/Chrome) or history folder (Internet Explorer and others) that contained this record.

BrowserName
The name of the browser.

BrowserVersion
The detected browser version.

Username
The Windows account name that created this record.

HostName
The domain name portion of the URL, including sub domains (Firefox/Chrome only).

FileName
The name of the file the cookie was stored in (Internet Explorer only).

FilePath
The full path to the cookie file, including the file name (Internet Explorer only).

CookiePath
The domain path for which the cookie is valid.

CookieName
The name of the cookie variable.

CookieValue
The value of the cookie variable.

IsSecure
Whether or not the cookie must only be transmitted over HTTPS (Firefox/Chrome only).

IsHttpOnly
Indicates the cookie is non-scriptable and should not be revealed to the client application (Firefox/Chrome only).

CreationDate
The date the cookie was created.

ExpirationDate
The date the cookie will expire.

CookieFlags
Attributes of the cookie (Internet Explorer only).

LastAccessedDate
The date the cookie was last accessed.

LastModifiedDate
The date the cookie was last modified.

1.38.2. How to Run `cookiehistory`

In the Job or Script Editor, use the Agent Module chooser to select cookiehistory.

Parameters:

TargetBrowser (String)
The name of the supported browser whose history will be extracted (Firefox, Internet Explorer, Safari, or Chrome).

PathToHistoryFiles (String)
The path to a user profile directory, the base profile directory, or a single history file from supported browser types.

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.39. Web Historian File Download History: `filedownloadhistory`

Returns a history of Files downloaded through a browser

File download history is not available for Safari 4 and Safari 5.

1.39.1. Audit Data

Profile
The name of the user profile folder (Firefox/Chrome) or history folder (Internet Explorer and others) that contained this record.

BrowserName
The name of the browser.

BrowserVersion
The detected browser version.

Username
The Windows account name that created this record.

DownloadType
The type of download operation.

FileName
The name of the file that was downloaded.

SourceURL
The URL from which the file was downloaded

TargetDirectory
The local directory where the file was downloaded to.

TemporaryPath
Temporary directory used for the download, if applicable.

Referrer
The HTTP referrer attribute of the request header, if available.

MimeType
The MIME type of the downloaded file.

FullHttpHeader
The entire HTTP header that caused the download (Internet Explorer only).

LastAccessedDate
The date the file was last accessed.

LastModifiedDate
The date the file was last modified.

BytesDownloaded
The number of bytes that were downloaded.

MaxBytes
The actual size of the file to be downloaded.

CacheFlags
Attributes for Internet Explorer cached files, which are considered downloaded files.

CacheHitCount
How many times this cached file has been used.

LastCheckedDate
The last date the cached file was synchronized.

StartDate
The date the download began (Firefox/Chrome only).

EndDate
The date the download ended (Firefox/Chrome only).

State
The current state of the download operation.

AutoResume
Whether or not auto resume is enabled for this download (Firefox/Chrome only).

1.39.2. How to Run `filedownloadhistory`

In the Job or Script Editor, use the Agent Module chooser to select filedownloadhistory.

Parameters:

TargetBrowser (String)
The name of the supported browser whose history will be extracted (Firefox, Internet Explorer, Safari, or Chrome).

PathToHistoryFiles (String)
The path to a user profile directory, the base profile directory, or a single history file from supported browser types.

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.40. Web Historian Form History: `formhistory`

Returns a history of forms edited through a browser. Form history is not collected for internet explorer since it is not stored in an index.dat file; autocomplete/autofill/intelliforms are stored in registry and need to be extracted completely differently than other internet explorer history data.

Form history can not be retrieved for MSIE 8, MSIE 9, Safari 4, Safari 5.

1.40.1. Audit Data

Profile
The name of the user profile folder (Firefox/Chrome) or history folder (Internet Explorer and others) that contained this record.

BrowserName
The name of the browser.

BrowserVersion
The detected browser version.

Username
The Windows account name that created this record.

FormType
Either 'Normal' for all non-login forms or 'Login' for form records that are login forms.

UsernameFieldName
The name of the user name form field on the web page (Login type forms only).

PasswordFieldName
The name of the password form field on the web page (Login type forms only).

HostName
The base URL (http and domain) where the form is contained.

HttpRealm
The realm that this login information applies to on the server side, as specified in the WWW-Authenticate header specification.

FormSubmitURL
The URL that this form is submitted to (a page on the server).

UsernameFieldValue
The value that was stored in the username field for the login form (Login type forms only).

EncryptedPassword
The value that was stored in the password field for the login form, typically base64-encoded and encrypted (Login type forms only).

EncryptionType
The type of encryption used in the stored password (Login type forms only).

CreationDate
The date the form information was created.

Guid
The GUID of the client-side application that handles encryption/decryption of the password (Login type forms only).

FormFieldName
The name of the form field on the web page (Normal type forms only).

FormFieldValue
The value that was stored in the form field (Normal type forms only).

FirstUsedDate
The date the form was first used (Chrome/Firefox only).

LastUsedDate
The most recent date the form was used (Chrome/Firefox only).

TimesUsed
The number of times the form has been used (Chrome/Firefox only).

1.40.2. How to Run `formhistory`

In the Job or Script Editor, use the Agent Module chooser to select formhistory.

Parameters:

TargetBrowser (String)
The name of the supported browser whose history will be extracted (Firefox, Internet Explorer, Safari, or Chrome).

PathToHistoryFiles (String)
The path to a user profile directory, the base profile directory, or a single history file from supported browser types.

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.41. Web Historian URL History: `urlhistory`

Returns a history of URLs visited. The options "GetThumbnails" and "GetIndexedPageContent" are only available for Chrome and Chrome Frame browsers.

Firefox v4.x and Firefox v5.x are not supported in the Web Historian Audits. No data will be returned from those browser versions.

1.41.1. Audit Data

Profile
The name of the user profile folder (Firefox/Chrome) or history folder (Internet Explorer and others) that contained this record.

BrowserName
The name of the browser.

BrowserVersion
The detected browser version.

Username
The Windows account name that created this record.

URL
The web page visited.

PageTitle
The title of the page visited, as it appeared in the browser title bar.

HostName
The domain name portion of the URL, including sub domains (Firefox/Chrome only).

Hidden
Whether or not the URL record was transparent to the user.

Typed
Whether or not the user physically typed the URL in the record.

LastVisitDate
The date that the URL was visited (in UTC time).

LastVisitDateLocal
The date that the URL was visited (in local time).

VisitFrom
The URL the user was viewing before navigating to the record URL.

VisitType
The type of visit – bookmark, typed, redirect, etc.

VisitCount
The number of times this URL was visited.

Thumbnail
If available, a JPEG thumbnail of the URL as it appeared in the browser (Chrome/Safari only).

FirstBookmarkDate
The date this URL was first bookmarked, if any (Chrome/Firefox only).

IndexedContent
Text content of web pages that were indexed by the browser (Chrome only).

1.41.2. How to Run `urlhistory`

In the Job or Script Editor, use the Agent Module chooser to select urlhistory.

Parameters:

TargetBrowser (String)
The name of the supported browser whose history will be extracted (Firefox, Internet Explorer, Safari, or Chrome).

PathToHistoryFiles (String)
The path to a user profile directory, the base profile directory, or a single history file from supported browser types.

GetThumbnails (Boolean)
Should the audit attempt to retrieve thumbnail images of websites visited

Default: false

GetIndexedPageContent (Boolean)
Should the audit attempt to retrieve indexed page content of websites visited

Default: false

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.42. XPath: `xpath`

Filters an XML Audit Data document.

1.42.1. Audit Data

../generated

1.42.2. How to Run `xpath`

In the Job or Script Editor, use the Agent Module chooser to select xpath.

Parameters:

expression (String)
An XPath expression to be applied to each item in an XML Audit Data document. If the expression evaluates to true or a node-set, the item will be included, otherwise it will be omitted.

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

1.43. XPath: `xpath2v2`

Filters an XML Audit Data document.

1.43.1. Audit Data

../generated

1.43.2. How to Run `xpath2v2`

In the Job or Script Editor, use the Agent Module chooser to select xpath2v2.

Parameters:

expression (String)
An XPath expression to be applied to each item in an XML Audit Data document. If the expression evaluates to true or a node-set, the item will be included, otherwise it will be omitted.

type (String)
The type of filter. Acceptable values: Standard.

Prevent Hibernation (Boolean)
Prevents the host machine from entering hibernation while this module is executed.

Default: false

2. Analysis Commands

Analysis is the transformation and collation of information after it has been collected. *Analysis Commands* accept *Result Documents* as input and perform operations against them, resulting in a new set of modified *Documents*.

MIR provides four *Analysis Commands* for manipulating data on the Controller after it has been collected. The table below provides a brief summary of their use, and is followed by details for each of the *Analysis Commands*, including parameters, special considerations, data returned, and usage instructions.

Timeline
Takes time-based events from multiple *Result Documents*, potentially of different types (such as a file listing and event logs), and merges them into a single time-ordered view.

Time Skew
Adjusts timestamps in an *Result Document*. Useful for comparing *Audits* between *Hosts* with differing clock settings.

Document Difference
Shows the difference between two *Result Documents* across a common set of fields, hiding information they share. Useful for finding differences between *Hosts* or changes to a single *Host* over time.

Document Intersection
Shows the overlap between two *Result Documents* across a common set of fields, hiding information that differs. Useful for finding similarities between *Hosts*.

2.1. Timeline

A *Timeline Analysis* takes multiple *Documents* with date/time fields and merges them to a single, time-ordered grid view. This *Analysis Command* is useful for comparing time-based information from multiple sources. The fields to use for time comparisons is selectable.

2.1.1. Analysis Data

The *Analysis Command* returns a single *Document* with the following information:

Source
The path to the source *Document* for the entry.

Uid
The unique identifier assigned to the entry by the Controller.

Time
The date/time for the entry from the source *Document*.

SourceItemType
The source *Document* type.

SourceField
The name of the field from which the Time entry was extracted.

ItemXML
The original item extracted from the source *Document*.

2.1.2. Usage

Running a Timeline Analysis

Timeline combines documents into a single time-ordered list.

1. Choose File → New → Analysis Job. A new titled New Job will be displayed to the right.
2. In the Targets box, drag or paste any number of *Documents* to be time-lined.
3. Using the Select an Analysis Command to Add... selector, choose Timeline. A Timeline *Analysis Command* will be inserted below the selector.
4. In the Timeline command area, click Choose a Field... and select the time field that will be used to place the document items into the time line. The Document Type field will be automatically completed when you select the time field.

   Click the + button to add an entry for each type of document.
5. Click  Run Immediately. When the *Job* is complete, a new document with data listed in time-order will be created and displayed.

2.2. Time Skew

This *Analysis Command* helps reconcile time differences between *Documents* from different target systems. The *Analysis* results in a new copy of the input *Documents* that have all of their date/times modified by the value specified by the user.

2.2.1. Analysis Data

Multiple *Documents* of any type may be specified as input to the *Analysis Command*. Copies of each *Document* will be generated, with all date/time values in those copies modified by the amount specified by the user for that *Job*. The original input *Documents* are not modified, nor will *Documents* that lack date/time values.

2.2.2. Usage

Running a Time Skew Analysis

Time Skew adds or subtracts a set value from all time values in documents.

1. Choose File → New... → Analysis Job. A new titled New Job will be displayed to the right.
2. In the Targets box, drag or paste any number of *Documents* to be corrected.
3. Using the Select an Analysis Command to Add... selector, choose Time Skew. A Time Skew *Analysis Command* will be inserted below the selector.

4. In the Time Skew command area, specify the Offset in hours, minutes, and seconds. The format is *hh:mm:ss*.

   For example, **`00:00:10`** will add 10 seconds to all date/time values contained in the input *Documents*. To subtract times, specify a negative value. For example, a value of **`-10:30:10`** will subtract 10 hours, 30 minutes, 10 seconds from those values.

5. Click  Run Immediately. When the *Job* is complete, a new document with corrected time values will be created and displayed.

Time Skew creates a new document with the same name as the source document, with a tag at the end indicating the skew value.

For example, adding 10 seconds skew to a file originally named `mir.w32rawfiles.08d8a1a8.xml` would create a file named `mir.w32rawfiles.08d8a1a8-PT10S.xml`.

2.3. Document Difference

Document Difference compares two input *Documents* (*Left* and *Right*) across a set of selected fields to identify all items in *Left* that are not in *Right*, and all items in *Right* that are not in *Left*. This is useful for identifying deltas between two similar sets of information. For example, a *Host*'s process or file listing could be compared to that of a baseline system to find unexpected items.

Note that for this form of difference operation the "order" of records in a *Document* not important. The *Document Difference Analysis Command* looks for any difference at all locations within each input *Document*.

2.3.1. Analysis Data

Document Difference creates two files: `Left Difference.xml` and `Right Difference.xml`. *Left Difference* contains all items in the first ("left") input *Document* that are different from the items in the second ("right") input *Document*. *Right Difference* contains all items in the second input *Document* that are different from those in the first input *Document*.

The fields returned in `Left Difference.xml` will be the source fields from the first input *Document*. For example, if the first input *Document* was a *File Listing*, then file list items (e.g. DevicePath, Path, File Size) will be returned in `Left Difference.xml`. Likewise, `Right Difference.xml` contains fields from the second input *Document*.

2.3.2. Usage

Running a Document Difference Analysis

Document Difference compares two documents and lists the differences between them.

1. Choose File → New... → Analysis Job. A new titled New Job will be displayed to the right.

2. In the Targets box, drag or paste two *Documents* to be "diffed."

Unlike other Analysis, the order of the inputs is relevant to *Document Difference*. The first input in the Targets box is "*Left*." The second input in the Targets box is "*Right*." Document Difference will only use the first two inputs. Any others provided in the Targets box will be disregarded.

3. Using the Select an Analysis Command to Add... selector, choose Document Difference. A Document Difference command will be inserted below the selector.

4. In the Document Difference command area, click Choose a Field... and select the field you wish to compare between the two documents.

   If you wish to compare multiple fields, click the + button to add more field entries.

5. Click  Run Immediately.

2.4. Document Intersection

Document Intersection is the complement to *Document Difference*: it compares two *Documents* (*Left* and *Right*) across a set of selected fields to identify all items that are found in both *Documents*. This is useful for identifying similarities between two sets of information. For example, a *Host*'s process or file listing could be compared to that of a baseline system to find matching items.

Note that for this form of difference operation the "order" of records in a *Document* not important. The *Document Intersection Analysis Command* looks for any similarity at all locations within each input *Document*.

2.4.1. Analysis Data

Document Intersection creates two files: `Left Intersection.xml` and `Right Intersection.xml`. *Left Intersection* contains all items in the first ("left") input *Document* that match items in the second ("right") input *Document*. *Right Intersection* contains all items in the second input *Document* that match items in the first input *Document*.

The fields returned within `Left Intersection.xml` will be the source fields from the first input *Document*. For example, if the first input *Document* was a *File Listing*, then file list \ilitems (e.g. DevicePath, Path, File Size) will be returned in `Left Intersection.xml`. Naturally, `Right Intersection.xml` contains fields from the second input *Document*.

2.4.2. Usage

Running a Document Intersection Analysis

Document Intersection compares two documents and lists the fields that are the same.

1. Choose File → New... → Analysis Job. A new titled New Job will be displayed to the right.

2. In the Targets box, drag or paste two *Documents* to be "diffed."

Unlike other Analysis, the order of the inputs is relevant to *Document Difference*. The first input in the Targets box is "*Left*." The second input in the Targets box

is "*Right*." Document Difference will only use the first two inputs. Any others provided in the Targets box will be disregarded.

3. Using the Select an Analysis Command to Add... selector, choose Document Intersection. A Document Intersection Command will be inserted below the selector.

4. In the Document Intersection command area, click Choose a Field... and select the field you wish to compare between the two documents.

   If you wish to compare multiple fields, click the + button to add more field entries.

5. Click  Run Immediately.

Appendix B
Searches

B.1. Indexing

When the Controller receives an audit result, it categorizes and indexes the document. For some audits this produces a vast amount of information that you may ultimately not need. Several control points allow you to regulate document indexing, on a global and job-specific basis.

Regular expression filters (regex) can be configured to exclude audit result categories, globally and per-job, as follows:

B.1.1. Global Indexing Restrictions

Controller administrators can use the web administration console to configure the **Application** → **ConfigFiles** → **Search Indexer** → **category_exclude_regex** setting.

The regex filter will apply to all audit results, for all jobs. For example, `/audit/(files)|(disks)/.*` will exclude file and disk audits from indexing.

B.1.2. Per-Job Indexing Restrictions

Each job can add an additional exclusionary filter.

MIR Console users creating or modifying a job may select **Do not index audit results**. This adds `/audit` to the list of exclusionary regexes. If no other exclusions apply, this permits indexing of support issues, and excludes all audit result documents.

In the MIR Console, the Jobs Library displays a **skip_indexing_on** column showing any job-specific exclusions. The **Do not index audit results** control also indicates the type of exclusion:

empty	no job-specific exclusions apply
check	`/audit` documents are excluded
grey	a custom regex has been applied

For fine-grained control of the **skip_indexing_on** value the job must be managed using the MIR REST API.

B.1.3. MCIC Indexing Restrictions

MCIC users have access to a global setting, **Index Audit Results**. **Yes** enables indexing; **No** adds `/audit` to the list of exclusionary regexes by default. If no other exclusions apply, this permits indexing of support issues, and excludes all audit result documents.

When creating sweeps, **Advanced Params** → **Index Audit Results** initially mirrors the global setting, and can be used to override the global default.

When audit results indexing is disabled, IOC Finding Reports are also disabled.

When audit result indexing is disabled for an acquisition, no MCIC functionality is affected.

B.1.4. Audit Result Categories

Exclusionary audit result indexing regexes should target the following categories:

/audit/eventlogs/w32	Event Log Audits
/audit/files/w32	Files Audits
/audit/ports/w32	Ports Audits
/audit/processes/w32	Process Audits
/audit/registry/w32	Registry Audits
/audit/services/w32	Services Audits
/audit/system/w32	System Audits
/audit/tasks/w32	Tasks Audits
/audit/volumes/w32	Volume Audits
/audit/disks/w32	Disk Audits
/audit/hivelist/w32	Hive Audits
/audit/drivers-memory/w32	Driver by Signature Audits
/audit/drivers-modulelist/w32	Driver by Memory Audits
/audit/useraccounts/w32	User Account Audits
/audit/kernel-rootkitdetection/w32	Rootkit Hook Audits
/audit/network-arp/w32	Network ARP Audits
/audit/network-dns/w32	Network DNS Audits
/audit/network-route/w32	Network Route Audits
/audit/prefetch/w32	Prefetch Cache Audits
/audit/systemrestore/w32	System Restore Audits
/audit/scripting-persistence/w32	Persistence Audits
/support/issue	Issues
/support/issues	Issues
/support/batchresult	Batch Results
/unknown	Unrecognized

B.2. Search Keywords

As discussed in *Chapter 18, Using Search on Audit Results*, the search system supplies a series of keywords that can be used to refine the scope of a search match. MIR search services make keywords available through the Search Query Builder, which allows you to select from a visual pick list. The search system supplies only keywords in the Search Query Builder that are currently present somewhere in the dataset on your Controller. For example, if a System Information Audit has not yet been collected into your Controller, the keywords for System Information Audits will not appear in the Search Query Builder.

The remainder of this appendix provides a list of keywords that are typically available for your use.

Some keywords, such as “category”, allow you to further specify a type of document through additional keywords as specified in the *Value* column of the table below. When you select those keywords from the Query Builder, both the keyword (e.g., “category”) and the value (e.g., “/audit”) are populated into your search query automatically.

When you use a keyword that does not pre-define additional values (e.g., “FileItem/MD5Sum”), then you will need to provide the value to search for. As new data types are added to subsequent versions of MIR, more keywords will become available.

The **category** keyword takes the following values:

/audit	Audit Data Only
/db	Database Only
/analysis/timeline	Timeline Analyses
/audit/eventlogs	Event Log Audits
/audit/drivers-memory	Memory Drivers Audits
/audit/drivers-modulelist	Module Drivers Audits
/audit/files	File Audits
/audit/processes	Process Audits
/audit/registry	Registry Audits
/audit/ports	Ports Audits
/audit/services	Service Audits
/audit/system	System Audits
/audit/tasks	Task Audits
/audit/volumes	Volume Audits
/audit/hivelist	HiveList Audits
/audit/disks	Disk Audits
/support/issue	Issues
/support/batchresult	BatchResults
/support/script	Scripts
/db/entity/job	Jobs
/db/entity/audittrail	Audit Trail Entries
/db/entity/logentry	Log Entries
/db/entity/searchfolder	Search Folders
/db/entity/host	Host Metadata
/db/entity/resultset	Result Set Metadata
/db/entity/auditresult	Audit Result Metadata
/db/entity/analysisresult	Analysis Result Metadata
/db/entity/queue	Job Scheduling Queue

/db/entity/queuedjob	Job Assigned to Queue
/db/entity/document	Document Metadata

The following keywords require a user-supplied value:

content
created
creator
datetime
DiskItem/@created
DiskItem/@uid
DiskItem/DiskName
DiskItem/DiskSize
DiskItem/PartitionList/Partition/PartitionLength
DiskItem/PartitionList/Partition/PartitionNumber
DiskItem/PartitionList/Partition/PartitionOffset
DiskItem/PartitionList/Partition/PartitionType
Document/content-type
EventLogItem/@created
EventLogItem/@uid
EventLogItem/category
EventLogItem/categoryNum
EventLogItem/EID
EventLogItem/genTime
EventLogItem/index
EventLogItem/log
EventLogItem/machine
EventLogItem/message
EventLogItem/reserved
EventLogItem/source
EventLogItem/type
EventLogItem/unformattedMessage/string
EventLogItem/user
EventLogItem/writeTime
FileItem/@created
FileItem/@uid
FileItem/Accessed
FileItem/Changed
FileItem/Created
FileItem/DevicePath
FileItem/FileAttributes
FileItem/INode
FileItem/Md5sum
FileItem/Modified
FileItem/Path
FileItem/PeakCodeEntropy
FileItem/PeakEntropy
FileItem/PEInfo/BaseAddress
FileItem/PEInfo/DetectedAnomalies/string
FileItem/PEInfo/DetectedEntryPointSignature/Name
FileItem/PEInfo/DetectedEntryPointSignature/Type

FileItem/PEInfo/Exports/ExportedFunctions/string
FileItem/PEInfo/Exports/ExportsTimeStamp
FileItem/PEInfo/Exports/NumberOfFunctions
FileItem/PEInfo/Exports/NumberOfNames
FileItem/PEInfo/ExtraneousBytes
FileItem/PEInfo/ImportedModules/Module/ImportedFunctions/string
FileItem/PEInfo/ImportedModules/Module/Name
FileItem/PEInfo/PEChecksum/PEComputedAPI
FileItem/PEInfo/PEChecksum/PEFileAPI
FileItem/PEInfo/PEChecksum/PEFileRaw
FileItem/PEInfo/PETimeStamp
FileItem/PEInfo/Sections/Section/DetectedCharacteristics
FileItem/PEInfo/Sections/Section/DetectedSignatureKeys/string
FileItem/PEInfo/Sections/Section/Entropy/@AverageValue
FileItem/PEInfo/Sections/Section/Name
FileItem/PEInfo/Sections/Section/SizeInBytes
FileItem/PEInfo/Sections/Section/Type
FileItem/PEInfo/Subsystem
FileItem/PEInfo/Type
FileItem/SecurityID
FileItem/SecurityType
FileItem/Sha1sum
FileItem/Sha256sum
FileItem/SizeInBytes
FileItem/StreamList/Stream/@created
FileItem/StreamList/Stream/@uid
FileItem/StreamList/Stream/Md5sum
FileItem/StreamList/Stream/Name
FileItem/StreamList/Stream/SizeInBytes
FileItem/Username
HiveItem/@created
HiveItem/@uid
HiveItem/Name
HiveItem/Path
Host/address
Host/agent_version
Host/asset_id
Host/description
identity
Issue/@context
Issue/@level
Issue/@number
Issue/@ref
Issue/@summary
job
moduleresults/moduleresult/@type
moduleresults/moduleresult/auditdata/@generator
moduleresults/moduleresult/auditdata/@generatorVersion
moduleresults/moduleresult/auditdata/@href
moduleresults/moduleresult/auditdata/@itemSchemaLocation
moduleresults/moduleresult/config/@type

moduleresults/moduleresult/config/command
moduleresults/moduleresult/config/inputs/input
moduleresults/moduleresult/config/params/field
moduleresults/moduleresult/config/params/input/type
moduleresults/moduleresult/config/params/result/type
name
PortItem/@created
PortItem/@uid
PortItem/localIP
PortItem/localPort
PortItem/path
PortItem/pid
PortItem/process
PortItem/protocol
PortItem/remoteIP
PortItem/remotePort
PortItem/state
ProcessItem/@created
ProcessItem/@uid
ProcessItem/arguments
ProcessItem/kernelTime
ProcessItem/name
ProcessItem/parentpid
ProcessItem/path
ProcessItem/pid
ProcessItem/SecurityID
ProcessItem/SecurityType
ProcessItem/startTime
ProcessItem/Username
ProcessItem/userTime
processor/@name
processor/@type
processor/@version
processor/issues/@generator
processor/issues/@generatorVersion
processor/issues/@href
processor/issues/@itemSchemaLocation
processor/moduledefs/moduledef/@context
processor/moduledefs/moduledef/input/format/@mimetype
processor/moduledefs/moduledef/input/format/name
processor/moduledefs/moduledef/module/@name
processor/moduledefs/moduledef/module/@version
processor/moduledefs/moduledef/output/format/@content-type
processor/moduledefs/moduledef/output/format/@mimetype
processor/moduledefs/moduledef/output/format/@schema
processor/moduledefs/moduledef/output/format/@schema-type
processor/moduledefs/moduledef/output/format/defName
processor/moduledefs/moduledef/output/format/name
processor/moduledefs/moduledef/paramdefs/paramdef/@name
processor/moduledefs/moduledef/paramdefs/paramdef/@repeatable
processor/moduledefs/moduledef/paramdefs/paramdef/@required

processor/moduledefs/moduledef/paramdefs/paramdef/@type
processor/moduledefs/moduledef/paramdefs/paramdef/@usage
queue
RegistryItem/@created
RegistryItem/@uid
RegistryItem/Modified
RegistryItem/NumSubKeys
RegistryItem/NumValues
RegistryItem/Path
RegistryItem/ReportedLengthInBytes
RegistryItem/Text
RegistryItem/Type
related
ServiceItem/@created
ServiceItem/@uid
ServiceItem/description
ServiceItem/descriptiveName
ServiceItem/mode
ServiceItem/name
ServiceItem/path
ServiceItem/pid
ServiceItem/serviceDLL
ServiceItem/startedAs
ServiceItem/status
ServiceItem/type
status
SystemInfoItem/@created
SystemInfoItem/@uid
SystemInfoItem/availphysical
SystemInfoItem/biosInfo/biosDate
SystemInfoItem/biosInfo/biosVersion
SystemInfoItem/buildNumber
SystemInfoItem/date
SystemInfoItem/directory
SystemInfoItem/domain
SystemInfoItem/hostname
SystemInfoItem/installDate
SystemInfoItem/MAC
SystemInfoItem/machine
SystemInfoItem/networkArray/networkInfo/adapter
SystemInfoItem/networkArray/networkInfo/description
SystemInfoItem/networkArray/networkInfo/dhcpLeaseExpires
SystemInfoItem/networkArray/networkInfo/dhcpLeaseObtained
SystemInfoItem/networkArray/networkInfo/dhcpServerArray/dhcpServer
SystemInfoItem/networkArray/networkInfo/ipArray/ipInfo/ipAddress
SystemInfoItem/networkArray/networkInfo/ipArray/ipInfo/subnetMask
SystemInfoItem/networkArray/networkInfo/ipGatewayArray/ipGateway
SystemInfoItem/networkArray/networkInfo/MAC
SystemInfoItem/OS
SystemInfoItem/patchLevel
SystemInfoItem/processor

SystemInfoItem/procType
SystemInfoItem/productID
SystemInfoItem/productName
SystemInfoItem/regOrg
SystemInfoItem/regOwner
SystemInfoItem/timezoneDST
SystemInfoItem/timezoneStandard
SystemInfoItem/totalphysical
SystemInfoItem/uptime
SystemInfoItem/user
TaskItem/@created
TaskItem/@uid
TaskItem/AccountName
TaskItem/ApplicationName
TaskItem/Creator
TaskItem/ExitCode
TaskItem/Flag
TaskItem/MaxRunTime
TaskItem/MostRecentRunTime
TaskItem/Name
TaskItem/NextRunTime
TaskItem/Parameters
TaskItem/Priority
TaskItem/Status
TaskItem/TriggerList/Trigger/TriggerBegin
TaskItem/TriggerList/Trigger/TriggerFrequency
TaskItem/WorkingDirectory
updated
updater
UserItem/@created
UserItem/@uid
UserItem/description
UserItem/disabled
UserItem/fullname
UserItem/grouplist/groupname
UserItem/LastLogin
UserItem/lockedout
UserItem/passwordrequired
UserItem/SecurityID
UserItem/SecurityType
UserItem/Username
UserItem/userpasswordage
VolumeItem/@created
VolumeItem/@uid
VolumeItem/ActualAvailableAllocationUnits
VolumeItem/BytesPerSector
VolumeItem/CreationTime
VolumeItem/DevicePath
VolumeItem/DriveLetter
VolumeItem/FileSystemFlags
VolumeItem/FileSystemName

KeywordValueTitleVolumeItem/IsMounted
VolumeItem/Name
VolumeItem/SectorsPerAllocationUnit
VolumeItem/SerialNumber
VolumeItem/TotalAllocationUnits
VolumeItem/Type
VolumeItem/VolumeName
xmlrecord

Appendix C
Error Messages and Troubleshooting

Enterprise environments can be very complex and enterprise security software is in turn often complex in order to meet some of the challenges posed by those environments. Failures and errors can occur for a variety of reasons. Clearly communicating these issues is an important aspect of enterprise products.

This appendix outlines the error reporting infrastructure contained in MIR, and provides guidance on identifying and resolving problems you may encounter.

C.1. Errors, Issues, and Logs

MIR uses three concepts to report information about anomalies in the operation of the system: error notification, issues documents, and log files.

Error notifications are typically communicated to you via a notification in a user interface, such as the Console or the web-based Administration Console. Issues Documents are generated as part of an audit, and report anomalies, failures, and other problems at each level in the process of collecting information from a MIR Agent. Log files capture information about the operation of a system component and may be useful in diagnosing errors and failures.

C.1.1. Errors

The Console and Administration Console directly report errors encountered during application operation. These errors are typically caused by direct failures, such as Console's inability to contact the Controller due to a network problem, or the failure of an administrative change to take effect due to insufficient user privileges. In these instances the error is reported directly to you via a message in the user interface or a dialog box.

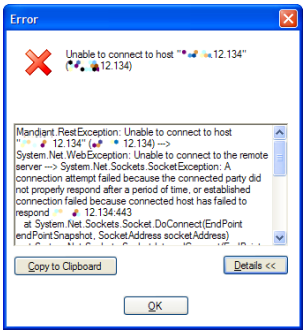
If an error is non-fatal, the Console will ask you to acknowledge the error before continuing. If the error is fatal, you will be asked to acknowledge the error; the Console is then shut down.

C.1.1.1. Console Errors

The Console provides three methods for communicating anomalies: error dialogs, activity status notifications, and warnings.

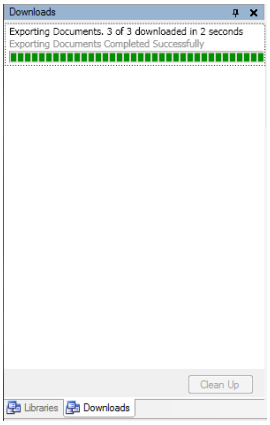
Error Dialogs

An error dialog is displayed when a problem is encountered that requires notification and acknowledgement. A summary of the problem is shown, along with buttons to display further information, copy the error message to the clipboard, and to acknowledge the error (and thus dismiss the dialog). Some errors are fatal and will prevent further operation of the Console until remedied. Examples of issues that will display error dialogs include connection failures and authentication failures.



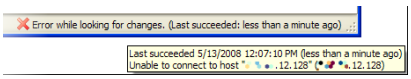
Download Status Notifications

The Console includes a **Downloads** Pane that reports on the status of long running operations, such as data import and export activities. If these activities change to an unexpected state (for example, if a long running import or client script is cancelled by the user) a notification is reported by turning the status bar for that activity red. Status text is also displayed in the status bar at the bottom of the Console window. Hover your mouse pointer over the status bar to see complete message text.



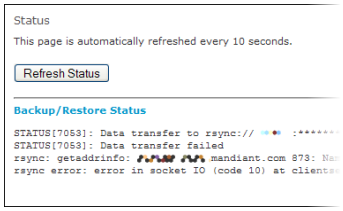
Warnings

Warnings are important information that does not require immediate attention, but may indicate an anomaly or other potential error within the system. Warnings are typically displayed in the Console status bar. For example, if there is an error when the Console is communicating with the Controller, that is communicated to the user as a warning. While it is an error condition, it is not fatal: you can continue to view the Console, but the information may not be completely up-to-date.



C.1.1.2. Administration Console Errors

The Administration Console displays errors, status, progress, and processing messages in the main page frame. When errors are encountered they are generally reported directly from the subsystem that encountered the error.



C.1.2. Issues Documents

Issues Documents are created as part of running a Host Audit, and are included as part of the Audit Results for a given Job. Issues report errors, anomalies, warnings, or informational items that were encountered as a result of attempting to collect the information specified in a Job script. These issues could occur at two levels in the system:

Agent Module
: Issues generated by the auditor. They might include operating system level information (info, warning, or errors) which help to describe why some information may not have been retrieved. Errors at this level are often not fatal and usually do not cause the overall script to fail.

Audit Execution
: Issues at this level are sometimes fatal, indicating that the overall script failed to run. This could be due to a number of reasons: the script failed to parse, the Controller couldn't reach the Agent, there was authentication failure between Controller and Agent, the Agent failed to parse a Job Script, or etceteras.

Items within an issues document have the following format:

```
Level Message Code Context
```

Level
: The severity of the issue item (e.g. INFO, FATAL)

Message
: The verbatim message describing the error. This message may be directly generated by MIR, or it may be generated by the target host operating system and placed directly in the issue item.

Code
: A numeric value that may be useful for MIR Customer Support in diagnosing your issue.

Context
: A string that may or may not be populated in the issue item. When present it helps identify where in the MIR software the issue was encountered.

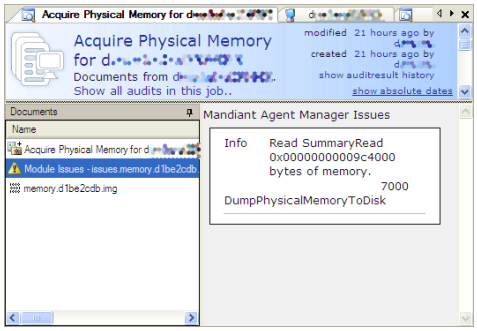
MIR defines two types of documents to capture these events: module issues and batch result issues, as detailed below.

C.1.2.1. Module Issues

Module issues contain a variety of items, often reported by the Host operating system as the MIR Agent collects information. Some fatal errors that interrupt the execution of an Audit Module are reported here; more often you will see informational or non-fatal items

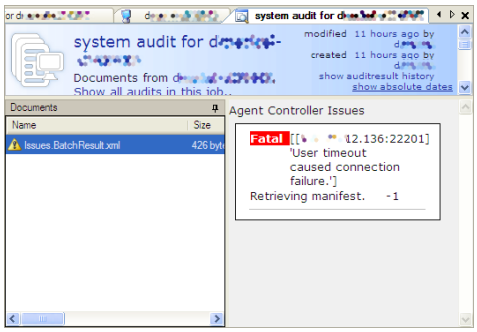
reported as a result of attempting to access a specific piece of information. For example, when retrieving a file listing, errors encountered on individual file listing line-items would be non-fatal, but would be recorded as issues. The file listing action might complete, but the Issues Document for that module would report why you may not have retrieved all of the expected information.

Module issues are displayed as a document in an Audit Result, and are named `Module Issues - [module result document].xml`. The screenshot below illustrates an Issues Document for a *Memory Acquisition* Module. Note the issue reported is a non-fatal informational item.



C.1.2.2. Batch Result Issues

Batch result issues record information that impact the entire Audit Result. Some of these may be informational, but they are more commonly fatal. Batch result issues are displayed as a document in an Audit Result and are named `Issues.BatchResult.xml`. There will only be one batch result issues document per audit result. The figure below illustrates a batch result issues document for an Audit where the Controller could not contact the Agent.



C.1.3. Logs

Every component of MIR creates one or more log files to record activity, errors, or other information that may be useful in auditing or troubleshooting system activities. This section identifies available log files by component and their use. With the exception of Controller activity logs, most logs are primarily used for troubleshooting errors and working with MANDIANT Customer Support.

C.1.3.1. Agent Logs

The Agent log contains informational messages about connections from Controllers, attempts to contact Agent Discovery Service, and other standard operating messages. If errors or other

problems are encountered, they are also written to the log. The log file can be retrieved from the Agent remotely via a *File Acquisition* Audit.

The location of this file varies dependent on the Host OS:

Windows 7 and Windows Vista

```
%SYSTEMDRIVE%\ProgramData\MANDIANT\MANDIANT Intelligent
Response Agent\MIRAgent.log
```

Windows XP and 2K3

```
%SYSTEMDRIVE%\Documents and Settings\All Users\Application Data
\MANDIANT\MANDIANT Intelligent Response Agent\MIRAgent.log
```

Windows 2K

```
%SYSTEMDRIVE%\Documents and Settings\All Users.WINNT
\Application Data\MANDIANT\MANDIANT Intelligent Response Agent
\MIRAgent.log
```

The log file has the following format:

```
Date Time [ThreadID] LogLevel [Context] Message
```

```
05-14-2008 17:27:09 [0x000006c8] INFO    [Win32Service
AgentManagerService HttpdAgentManager Discovery]- The Discovery
Server settings file 'discovery.xml' has been loaded.
05-14-2008 17:27:09 [0x000006c8] INFO    [Win32Service
AgentManagerService HttpdAgentManager Discovery]- The Discovery
service has started.
05-14-2008 17:27:09 [0x00000ad4] INFO    [Discovery]- Starting
Discovery request.
05-14-2008 17:29:30 [0x00000ac0] INFO    [HttpdAgentManager
shttpd]- Connection from 172.16.12.128:56158 on socket 352
05-14-2008 17:29:31 [0x00000ac0] INFO    [HttpdAgentManager]-
Verifying client certificate…
V0
AC71725DBF21E0EE
sha1WithRSAEncryption
/CN=MIR_CA/O=Mandiant/C=US
May 14 09:26:50 2008 GMT
May 12 09:26:50 2018 GMT
/CN=MIRApp/O=Mandiant/C=US
05-14-2008 17:29:31 [0x00000ac0] INFO    [HttpdAgentManager]- …
client certificate verified.
```

C.1.3.2. Controller Logs

The Controller maintains logs for every application service that provides MIR functionality. Logs are directly accessible via the Administration Console or exportable from the system via **syslog-ng**.

Console logs are standard syslog-formatted log files stored in plain text. Log messages are generally of the format:

```
Date Time LogLevel [Context] Message
```

The following table outlines the MIR Controller services and their function:

mir_agent
Logs Discovery data to the audit files.

mir_agent_controller
Controls all interaction with deployed Agents.

mir_agent_dispatcher
Controls dispatch of tasks to subsystems responsible for interacting with deployed Agents.

mir_agent_upgrade_proxy
Controls the Agent over-the-network (Discovery) upgrade process.

mir_analyzer_dispatcher
Dispatches analysis jobs to associated components.

mir_analyzer_service
Conducts analysis tasks.mir_auditManages the system activity audit log.

mir_data
The data management service responsible for organizing and storing information in associated databases and on disk.

mir_discovery_server
The Agent Discovery server.mir_discovery_serviceThe Agent Discovery Service. Registers new Agents and updates their records as information (such as network address) changes.

mir_indexer
Indexes acquired data so it can be made available to mir_searcher.

mir_lcd
Controls the LCD panel on the front of the Controller (deprecated).

mir_mbus
The back-end message bus that transmits messages between MIR Controller components.

mir_pound
Web caching service for the Controller.

mir_restore_web
Performs Controller backup and restore tasks.

mir_scheduler
Schedules and executes tasks within the system.

mir_script_runner
Parses Job Scripts and controls dispatch to either the Analysis engine or Agent management subsystem.

mir_searcher
Controls MIR's search engine.

mir_searcher_dispatcher
Controls dispatch of tasks to subsystems responsible for resolving search requests.

mir_web
The primary web service that Consoles interact with, plus the log files for mir_web_admin, mir_web_files, and mir_web_static.

mir_web_admin
Provides the admin UI interface.

mir_web_files
Provides file transfer services.

mir_web_static
Serves static content for the mir_web service.

mir_discovery_proxy
Proxy server for discovery.

C.1.3.3. Console Logs

The location of Console logs varies dependent on the Host OS:

Windows 7 and Windows Vista

Crash Logs
```
%SYSTEMDRIVE%\Users\[username]\AppData\Local\MANDIANT
Corporation\MANDIANT Intelligent Response\[Console
version]\[\*.log]
```

Error Messages
```
%SYSTEMDRIVE%\Users\[username]\AppData\Roaming
\MANDIANT Corporation\MANDIANT Intelligent Response
\Mirconsole.apperrors.log
```

Log Messages
```
%SYSTEMDRIVE%\Users\[username]\AppData\Roaming\MANDIANT
Corporation\MANDIANT Intelligent Response\Mirconsole.log
```

User Settings
```
%SYSTEMDRIVE%\Users\[username]\AppData\Local
\MANDIANT_Corporation
\mirconsole.exe_StrongName_[hash]\[Console version]
```

Windows XP, Windows 2K3, Windows 2K

Crash Logs
```
%SYSTEMDRIVE%\Documents and Settings\[username]\Local
Settings\Application Data\MANDIANT Corporation\MANDIANT
Intelligent Response\[\*.log]

%SYSTEMDRIVE%\Documents and Settings\All Users\Application
Data\MANDIANT Corporation\MANDIANT Intelligent Response
\[\*.log]
```

Error Messages

```
%SYSTEMDRIVE%\Documents and Settings\[username]\Application
Data\MANDIANT Corporation\MANDIANT Intelligent Response
\Mirconsole.apperrors.log
```

Log Messages

```
%SYSTEMDRIVE%\Documents and Settings\[username]\Application
Data\MANDIANT Corporation\MANDIANT Intelligent Response
\Mirconsole.log
```

User Settings

```
%SYSTEMDRIVE%\Documents and Settings\[username]\Local
Settings\Application Data\MANDIANT_Corporation\user.config
```

Like most other log files in the system, the Console logs follow the format:

```
Date Time LogLevel [Context] Message
```

The Console writes three logs into the directory it was installed into:

`Console.log`
Records general errors, warnings, and information about Console operation. Used for general Console troubleshooting.

`Console.History.log`
Records full details of any exception errors that interrupt Console operation. Used for troubleshooting of a specific exception or error.

`ChangeDetection.log`
Records change notifications received by the Console. Used for troubleshooting collaboration and view update issues.

C.2. System Reports

MCIC provides a robust MIR system evaluation report tool, available to Administrators only, through the command-line interface or through MCIC. This tool queries the controller, compiling a package of configuration, logs, and state information that helps MANDIANT Product Support to identify issues.

Please see the Administration Guide (Appendix *Error Messages and Troubleshooting*) for details.

Appendix D
Agent Command-line Reference

D.1. Commands and Flags for Using the Agent

Commands

```
MIRAgent.exe {[-?] | [-i] | [-u] | [-d] | [-o [basedir]] | -
regencert} [secondary flags]
```

Flags for Conducting Local Audits

```
MIRAgent.exe -o [basedir] [-f] [-script filename] [-encoding
{gzip | aff | none}] [-notimestamp] [-auditissuefilterlevel
{debug | info | warning | error}] [-allowmultiple] [-portable]
[-cleanup]
```

Flags for Starting the Agent in Daemon Mode

```
MIRAgent.exe -d [-bind ip address[:port number]] [-allow
network/mask, …] [-settings filename] [-fw {on | service |
auto | off}] [-allowmultiple] [-certpath path] [-keypath path]
[-capath path] [-crlpath path] [-credspath path] [-memcert]
[-disablediscovery] [-auditissuefilterlevel {debug | info |
warning | error}] [-encoding {gzip | aff | none}] [-portable]
[-cleanup]
```

Flags for Installing the Agent as a Windows Service

```
MIRAgent.exe -i [-start] [-servicename name] [-servicedisplay
displayname] [-settings filename]
```

Flags for Uninstalling the Agent if it was Installed as a Service

```
MIRAgent.exe -u [-servicename name]
```

Flags for Regenerating Agent Credentials

```
MIRAgent.exe -regencert [path] [-regencreds]
```

Flags for Displaying On-screen Help for Agent Commands

```
MIRAgent.exe {-i | -u | -d | -o | -regencert} -?
```

D.1.1. Local Audit Flags

```
MIRAgent.exe -o [basedir] [-f] [-script filename] [-encoding {gzip
| aff | none}] [-notimestamp] [-auditissuefilterlevel {debug |
info | warning | error}] [-allowmultiple] [-portable] [-cleanup]
```

-allowmultiple

Allows multiple Agents to run on the same system. Each Agent must be bound to a different port using the `-bind` notation.

-auditissuefilterlevel debug | info | warning | error

Filter audit issues at the specified level. Default: `info`.

-cleanup
Allows the Agent to clean up any artifacts on the Host system that were created when an Audit was executed. For example, executing a memory Audit installs a driver on the Host machine. Specifying this parameter removes the driver when the Agent has finished executing.

-encoding gzip | aff | none
Sets the compression method for storing or transmitting Audits. Default: `gzip`.

-f
Forces the creation of the directory specified by the `-o` *`basedir`* argument.

-notimestamp
Do not add a timestamp to the output directory tree.

-portable
Installs configuration files in the local application folder, leaving no trace on the Host computer after audit completion.

-o [*basedir*]
Instructs the Agent to Audit the system on which it is installed, and to store the results locally. If *`basedir`* is not specified, the results are stored in the current working directory.

Audit files are stored in `basedir/Audits/machine/date`, where *`machine`* is the name of the system on which the Agent is running, and *`date`* is a date-time stamp in the form YYYMMDDHHMMSS.

-script *filename*
Executes the specified Agent command script file.

D.1.1.1. Examples

`miragent.exe -o -script scriptfile.xml`
Executes an Agent command file and writes the script output to `.\`*`hostname`*`\`*`date`*`.`

`miragent.exe -o c:\temp -script scriptfile.xml`
Executes an Agent command file and *if the C:\temp directory exists,* writes the script output to `C:\temp\hostname\date`.

`miragent.exe -o c:\audits -f -script scriptfile.xml`
Executes an Agent command file and writes the script output to `C:\temp\hostname \date`. If the `C:\audits` directory does not exist, it will be created.

`miragent.exe -o -script scriptfile.xml -encoding none`
Executes an Agent command file and writes the script output to `.\`*`hostname`*`\`*`date`*`.`. The script output is not compressed.

`miragent.exe -o -script scriptfile.xml -cleanup`
Executes an Agent command file and writtes the script output to `.\`*`hostname`*`\`*`date`*`.`. After the Agent has completed its tasks, it removes its artifacts from the system.

D.1.2. Daemon Mode Flags

```
MIRAgent.exe -d [-bind ip address[:port number]] [-allow
network/mask,…] [-settings _filename] [-fw {on | service | auto
| off}] [-allowmultiple] [-certpath path] [-keypath path] [-
capath path] [-crlpath path] [-credspath path] [-memcert] [-
disablediscovery] [-auditissuefilterlevel {debug | info | warning
| error}] [-encoding {gzip | aff | none}] [-portable] [-cleanup]
```

-allow *network/mask,…*
Specifies an IP Allow List using a comma-separated list of network addresses and netmasks in CIDR (Classless Internet Domain Routing) notation. By default the Agent allows connections from all IP addresses. When `-allow` is set, only connections from the specified networks or systems are permitted.

-allowmultiple
Allows multiple Agents to run on the same system. Each Agent must be bound to a different port using the `-bind` notation.

-f
Forces the creation of the directory specified by the `-o basedir` argument.

-bind *ip address[:port number]*
Sets the IP address and TCP port number that the Agent will listen on. By default, the Agent listens on TCP port `22201`.

-capath *path*
Tells the Agent to use the public certificate file located at the specified directory. This overrides any settings file specified and is saved in that settings file. By default the value is `miragentcert.pem.protected` and is found in the current working directory.

-cleanup
Allows the Agent to clean up any artifacts on the Host system that were created when an Audit was executed. For example, executing a memory Audit installs a driver on the Host machine. Specifying this parameter removes the driver when the Agent has finished executing.

-credspath *path*
Tells the Agent to use the credentials file located at the specified directory. This overrides any settings file specified and is saved in that settings file. By default the value is `creds.protected` and is found in the current working directory.

-certpath *path*
Tells the Agent to use the certificate file located at the specified directory. This overrides any settings file specified and is saved in that settings file. By default the value is `cert.protected` and is found in the current working directory.

-crlpath *path*
Tells the Agent to use the CRL (Certificate Revocation List) file located at the specified directory. This overrides any specified settings file and is saved in that settings file. By default the value is `mircrl.pem.protected` and is found in the current working directory.

-d
Instructs the Agent to begin listening in daemon mode. By default the Agent listens on TCP port `22201`. `-d` is often used with `-bind` to set the listening port; and with `-allow` to restrict IP addresses.

-disablediscovery
Disables the Discovery service. When the service is disabled, the Agent will not attempt to contact the Controller.

-encoding gzip | aff | none
Sets the compression method for storing or transmitting Audits. Default: `gzip`.

-fw on | service | auto | off
Automatically configures the Windows firewall to allow connections to the Agent.

- `on` adds a persistent exception for the Agent.
- `service` allows connections only when the Agent is running as a service.
- `auto` allows connections to the Agent while it is running in daemon mode and will remove the exception when the Agent exits.
- `off` prevents the Agent from setting any exceptions itself. You will need to manually set firewall exceptions in this case.

-keypath *path*
Tells the Agent to use the private key file located at the specified directory. This overrides any settings file specified and is saved in that settings file. By default the value is `miragentkey.pem.protected` and is found in the current working directory.

-memcert
Tells the Agent to use a certificate generated in memory only. Each time the Agent is started a new certificate is generated and remains in memory as long as the Agent is active.

-portable
Installs configuration files in the local application folder, leaving no trace on the Host computer after audit completion.

-settings *filename*
Instructs the Agent to use a specific settings file. If *`filename`* does not exist, the Agent stores its current settings in that file. By default, Agents do not store settings.

This flag needs to be used at least once with a default set of flags in order for a settings file to be created.

D.1.2.1. Examples

`miragent.exe -d -bind 127.0.0.1:22222`
Runs the Agent as a daemon listening local connections on port 22222.

`miragent.exe -d -bind 127.0.0.1:22222`
Runs the Agent as a daemon listening to all connections on port 22222.

`miragent.exe -d -encoding gzip`
Runs the Agent as a daemon, using gzip compression on its data files.

`miragent.exe -d -memcert`
Runs the Agent as a daemon, using SSL certificates generated in memory.

`miragent.exe -d -cleanup`
Runs the Agent as a daemon, removing any artifacts when the daemon exits.

D.1.3. Service Mode Flags

MIRAgent.exe -i [-start] [-servicename *name*] [-servicedisplay *displayname*] [-settings *filename*]

MIRAgent.exe -u [-servicename *name*]

-i
Installs the Agent as a Windows service.

-servicename *name*
Used with `-i`, sets the short name of the Agent service when it is installed.

-servicedisplay *displayname*
Used with `-i`, sets the display name of the Agent service when it is installed.

-start
Instructs the Agent to start when it has been previously installed as a service. The `-start` flag is only available with `-i` to both install and start the Agent with one command.

-u
Stops and uninstalls the Agent if it is running as a service.

D.1.3.1. Examples

`miragent.exe -i -servicename MyShortName`
Runs the Agent as a service with the short name *MyShortName*.

`miragent.exe -i -servicename MyShortName -servicedisplay MyDisplayName`
Runs the Agent as a service with the short name *MyShortName* and the display name *MyDisplayName*.

`miragent.exe -i -start`
Runs the Agent as a service and then starts the service.

`miragent.exe -u -servicename MyShortName`
Stops and uninstalls the Agent that has the short name *MyShortName*.

D.1.4. Special Usage

D.1.4.1. Start Agent as a Service Using a Settings File

1. Start the Agent in daemon mode, specifying a new settings file:

```
miragent -d -settings mysettingsfile.xml
```

2. Stop the daemon by tapping **Enter**.
3. Install the Agent as a service and start it, using the new settings file:

```
miragent -i -start -settings mysettingsfile.xml
```

D.1.4.2. Install the Agent onto a Removable Media Device and Execute the Agent on a New Host

1. Install the Agent on a 32-bit or 64-bit host to create a 32-bit or 64-bit portable Agent, respectively:

```
msiexec /quiet /i C:\AgentSetup.msi PORTABLE=True TARGETDIR=C:
\MIRAgent COMMONAPPDATAFOLDER=C:\MIRAgent
```

2. Copy the installation to the removable media device:

```
copy C:\MIRAgent E:\MIRAgent
```

3. Install the removable media device at the target machine and run the Agent:

```
cd e:\MIRAgent miragent -portable -capath mircacert.pem -crlpath
mircrl.pem -fw auto
```

or

```
cd e:\MIRAgent miragent -portable -memcert -settings
service.settings.xml
```

or

```
cd e:\MIRAgent miragent -portable -memcert -capath mircacrt.pem -
crlpath mircrl.pem -fw auto
```

D.1.4.3. Install the Agent and Burn a CD

1. Install the Agent on the device, making sure to select the **Portable Install** option.
2. Burn the installation folder to a CD
3. On the target machine, run the Agent using the following command:

```
miragent -d -memcert -capath mircacert.pem -crlpath mircrl.pem -
fw auto
```

D.1.5. A Note on Default Behaviors

Agent commands have default behaviors as follows:

Interface and Port Binding
The Agent binds to all available network interfaces unless a more specific binding is explicitly specified on the command line or in a settings file. The default port is TCP `22201`.

Firewall Exceptions
Firewall exceptions are set while the Agent is active as a service. The exception is added when an Agent is installed.

Compression
All audits are collected and packaged using gzip unless otherwise specified.

Output Base
Directory audits collected with the `-o` flag are stored in `.\Audits` according to Host name and collection date.

Appendix E
Client Scripts

E.1. Using the Example Scripts

The sample client script shipped with MIR can be used as a template for creating your own Scripts. To do this:

1. Open `C:\Program Files\MANDIANT\MANDIANT Intelligent Response Client\Sample\Example.clientscript` with any text or XML editor.
2. Rename and save the file.
3. Modify the example script as needed, then run it via the Console.

E.2. Running Client Scripts

1. Choose **Tools** → **Run Client Script...** from the Console menu bar.
2. Select the script to run and click **OK**.

   You will be presented with a confirmation dialog that outlines the steps the Script will perform. Click **OK** to continue, or **Cancel** to abort.

Annotated Sample Client Script

```
<?xml version="1.0" encoding="utf-16"?>
<script xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
chaining="implicit">
<commands>
<!-- this name attribute controls the name displayed while it
executes -->
<command xsi:type="ExecuteClientScript"
name="Create and Import Example Data">
<clientScript>
<commands>
<!-- Adds the named host to the library. Specifying the id
attribute stores the result of this command (the host "dawkins")
for later reference by commands such as AddJobInput. The id is
optional. -->
<command xsi:type="AddHost" id="dawkins">
<name>dawkins</name>
<address>https://192.168.1.100:22201</address>
<!-- the result of the containing command is set as input to
this command, which adds it to a different folder-->
<commands>
<command xsi:type="AddLabel">
<label>active</label>
</command>
<command xsi:type="AddLabel">
<label>todo</label>
</command>
```

```
<command xsi:type="AddLabel">
<label>examples</label>
</command>
</commands>
</command>
<!-- Adds the named host to the library -->
<command xsi:type="AddHost" id="feynman">
<name>feynman</name>
<address>192.168.2.129</address>
<!-- the result of the containing command is set as input to
this command, which adds it to a different folder-->
<commands>
<command xsi:type="AddLabel">
<label>examples</label>
</command>
<command xsi:type="AddLabel">
<label>corporate</label>
</command>
</commands>
</command>
<!-- Adds the named host to the library -->
<command xsi:type="AddHost" id="darwin">
<name>darwin</name>
<address>192.168.1.101</address>
<!-- the result of the containing command is set as input to
this command, which adds it to a folder-->
<commands>
<command xsi:type="AddLabel">
<label>examples</label>
</command>
<command xsi:type="AddLabel">
<label>dmz</label>
</command>
</commands>
</command>
<!-- Adds the named host to the library -->
<command xsi:type="AddHost" id="curie">
<name>curie</name>
<address>192.168.1.102</address>
<!-- the result of the containing command is set as input to
this command, which adds it to a folder-->
<commands>
<command xsi:type="AddLabel">
<label>examples</label>
</command>
<command xsi:type="AddLabel">
<label>accounting</label>
</command>
<!-- Only valid inside the commands block of a host, imports
into that host specifically - the user is asserting that the
offline audit belongs to this host -->
<command xsi:type="ImportAuditResult">
<localPath>
Sample\Audits\EXAMPLE\20080101235959\
</localPath>
<commands>
<command xsi:type="AddLabel">
<label>examples</label>
</command>
<command xsi:type="AddLabel">
```

```
<label>.imported</label>
</command>
<command xsi:type="AddLabel">
<label>todo</label>
</command>
</commands>
</command>
</commands>
</command>
<command xsi:type="AddSearch">
<name>Any IP in 192.168.1.0/32</name>
<query>
address:[192.168.1.0 TO 192.168.1.255]
</query>
<commands>
<command xsi:type="AddLabel">
<label>examples</label>
</command>
</commands>
</command>
<command xsi:type="ImportCaseNotes">
<name>Getting Started</name>
<localPath>Sample\Getting Started.entry</localPath>
</command>
<!-- Add a script using a local script file -->
<command xsi:type="ImportAuditScript">
<name>Complete Audit</name>
<localPath>
Sample\AgentScripts\AllAudits.Batch.xml
</localPath>
<commands>
<command xsi:type="AddLabel">
<label>examples</label>
</command>
<command xsi:type="AddLabel">
<label>.imported</label>
</command>
<command xsi:type="AddLabel">
<label>.favorite</label>
</command>
</commands>
</command>
<!-- Add a job using a local script file -->
<command xsi:type="AddAuditJob">
<name>Ports Audit</name>
<schedule>now</schedule>
<scriptLocalPath>
Sample\AgentScripts\PortAudit.Batch.xml
</scriptLocalPath>
<commands>
<!-- Add job inputs using ids for already added hosts -->
<command xsi:type="AddJobInput" idref="feynman"/>
<command xsi:type="AddJobInput" idref="curie"/>
<command xsi:type="AddLabel">
<label>.favorite</label>
</command>
<command xsi:type="AddLabel">
<label>examples</label>
</command>
<!--Queue this job in the Queue with a specified name-->
```

```
<command xsi:type="QueueJob">
<QueueName>Every Day at Noon</QueueName>
</command>
<!--Queue this job in the default Queue (Run Immediately)-->
<command xsi:type="QueueJob"/>
</commands>
</command>
<!-- Add a job using an inline script -->
<command xsi:type="AddAuditJob">
<name>Processes</name>
<schedule>now</schedule>
<script chaining="implicit">
<commands>
<command xsi:type="ExecuteModuleCommand"
id="urn:uuid:e007669c-2c8a-49e5-ae80-11ba8cd37996">
<module name="w32processes-API"/>
</command>
</commands>
</script>
<commands>
<command xsi:type="AddLabel">
<label>.favorite</label>
</command>
<command xsi:type="AddLabel">
<label>examples</label>
</command>
</commands>
</command>
</commands>
</clientScript>
</command>
</commands>
</script>
```

Appendix F
CEF-Compliant Logging

The controller and MCIC work together to provide CEF logging support for:

- Status information for acquisitions.
- IOC hit details for sweeps.

All CEF logging follows the CEF specification as described by ArcSight (*http://www.arcsight.com/collateral/CEFstandards.pdf*).

In addition, users can configure which servers will receive CEF syslog events through the Admin UI in **Appliance** → **Config** → **Logging**. All CEF logging is stored on the local machine logs alongside existing syslog log files.

F.1. Common Log Fields

All CEF logging contains the following fields:

Time
Timestamp of the log entry.

Device Vendor
`MANDIANT`

Device Product
`MIR`

Device Version
The MIR version number.

Device Host Name
Hostname of the MIR controller.

Name
A description of the logged event.

Event Class ID
The same as the Device Host Name.

Custom String 1 Label
`Host Agent Cert Hash`

Custom String 1
The host agent certificate hash (AM Cert Hash) related to the event.

F.2. Logging for acquisitions

MCIC logs acquisition status information for:

- Creation, either successful or unsuccessful
- Update (i.e. of the comment field)
- Status (e.g. when the job is created)
- Delete

MCIC always logs CEF for acquisitions created from the remote service. Logging activity for other acquisitions is controlled by the **Log CEF for all acquisitions** global setting.

The fields logged are:

Device Receipt Time
The time of the acquisition event.

Severity
`0` (informational), 2 (warning) or 4 (error).

Device Action
`Create`, `Update`, `Status`, `Delete`.

For all cases except unsuccessful acquisition creation, MCIC also logs:

External ID
The acquisition index number

Destination IP, Destination Host, Destination Domain
The usual network information

For File Acquisitions:

Filename, File Path
Standard file information.

For Script Acquisitions:

Custom String 1 Label
`Script Name` (the label for the entry)

Custom String 1
The name of the script

When an acquisition fails:

Message
When an acquisition creation request fails, a descriptive error message is logged.

F.3. Logging for IOC hits

Whenever an IOC hit is found by a search report it is logged to CEF. This activity is controlled by the MCIC global setting **Log CEF for IOC hits**. Note that IOC hits logging occurs for both manual and automatic search reports; every hit found during a report is logging. This means

that multiple CEF log events may be triggered for the same IOC hit. Although automatic search reports only search through new result sets, manual reports do not. Therefore, manual search reports will always log all IOC hits in a sweep.

Fields logged:

Device Receipt Time
The time when the IOC hit was found.

Severity
`10` (IOC Hit)

Threat Priority
`10` (IOC Hit)

Device Action
`Sweep IOC Hit Search`

External ID
The sweep ID in MCIC.

Destination IP, Destination Host, Destination Domain
The usual network information

Device Custom String 2 Label
`Hit Hash` (the label for the entry)

Device Custom String 2
The IOC hit hash value for the hit

Device Custom String 3 Label
`Sweep Name` (the label for the entry)

Device Custom String 3
The name of the sweep that discovered the hit.

Device Custom String 4 Label
`IOC Name` (the label for the entry)

Device Custom String 4
The name of the IOC that discovered the hit.

Device Custom String 5 Label
`IOC UUiD` (the label for the entry)

Device Custom String 5
The UUID of the IOC that discovered the hit.

Also IOC hit logs contain built-in event categorization data:

Category Significance
`Compromise`

Category Behavior
`Execute`

Category Technique
`Exploit`

Category Device Group
`IDS`

Category Outcome
`Success`

Category Object
`Host`

Appendix G
Script Acquisition via HTTPS

Acquisitions can be requested directly (i.e. without UI) by calling *https://controllername/apps/webclient/acquisitions/create*

The required and optional POST parameters depend on the desired acquisition:

Acquisition Type
The following parameter must be specified:

type
Either `file` or `script`.

Host Definition
One and only one of these two parameters must be specified:

am_cert_hash
The host certificate hash, used by MIR to uniquely identify a known host.

ip_address
The IP address of the host. See *Section G.1, "Host Disambiguation"* below for more details.

File Parameters
If *type* is set to `file`, the following parameters are required:

file_path
The path to the directory where the file to be acquired is stored.

file_name
The name of the file to be acquired.

Script Parameters
If type is set to `script`, only one of the following parameters is required:

script_uri
The full URI of the script to be used in the acquisition. The URI must point to a controller that is known to the MCIC instance.

script_name
The name of the script to be used in the acquisition. The script must exist on the local controller.

Optional Parameters
Regardless of the value of *type*, the following parameters may be included:

comment
Descriptive comment on the acquisition. This is the only field that may be changed after the acquisition is created.

force
Either 0 or 1, determines whether or not to force creating a duplicate acquisition. See Force Behavior, below.

external_id
This external ID will be stored with the acquisition record for later reference.

G.1. Host Disambiguation

If the user provides an IP address instead of a certificate hash to specify the target host for an acquisition, that IP address may map to zero, one, or more than one host record in MIR.

- If no host matches are found, the acquisition is not created.
- If one host match is found, the acquisition is created.
- If more than one host if found, an MCIC setting defines the behavior as either of the following:
  - Select the most recently discovered host as the target for the acquisition,

    OR

  - Fail to create the acquisition as if no match were found.

By default, MCIC will select the most recently discovered host.

G.2. Force Behavior

When a script acquisition is requested with a configuration (i.e. host and script) identical to an acquisition previously created, the MCIC behavior is determined by the **Script Acquisition Duplicate Window** global setting:

- If the setting is `-1` (negative one), MCIC will always fail to create a duplicate acquisition unless the force parameter is given.
- If the setting is `0` (zero), MCIC will always create duplicate acquisitions without giving a warning.
- If the setting is `>0` (greater than zero), MCIC will only fail to create a duplicate acquisition if the identical acquisition was created within that number of minutes. The default value for this setting is 60 (minutes).

Appendix H
ArcSight Integration

Hewlett-Packard's ArcSight Enterprise Security Manager (ESM) platform can be used as a CEF-compliant MCIC log server. There are three integration options:

- Use URL integration commands which access the MCIC HTTPS site directly.
- Configure Arcsight correlation rules to run a script stored locally on the ESM manager machine, which in turn will communicate with MCIC.
- Create and configure a CounterACT-type FlexConnector using a local ESM script to communicate with MCIC, and piping the results through Smart Connector for use in integration commands and/or correlation rules.

H.1. URL Integration Commands

MIR supports ArcSight HTTPS access to various MCIC pages and a limited set of commands. The following URLs show a sample of the integration commands that are possible using the ArcSight Integration Commands feature. See ArcSight documentation for instructions on creating and configuring URL Integration Commands.

The URLs below use the `${deviceHostName}` variable as the MIR instance hostname, however in practice this may be unnecessary or undesirable if only one MIR hostname is being used in the environment or if the URL command needs to work when initiated against an event that did not originate from a MIR controller.

View acquisitions created from an event

```
https://${deviceHostName}/apps/webclient/direct?
  target=acquisitions&amp;input=external_id&amp;id=${eventId}
```

View all acquisitions on a target host

```
https://${deviceHostName}/apps/webclient/direct?
  target=acquisitions&amp;input=hostname&amp;id=${targetHostName}
```

View details for an acquisition

```
https://${deviceHostName}/apps/webclient/direct?
  target=acquisitions&amp;input=id&amp;id=${deviceExternalId}
```

View details for a sweep

```
https://${deviceHostName}/apps/webclient/direct?
  target=sweeps&amp;input=${externalId}
```

Create acquisition on a target host via MCIC

```
https://${deviceHostName}/apps/webclient/direct?
```

```
  target=hosts&amp;input=${targetAddress}&amp;id=${eventId}
```

View IOC hit details

```
https://${deviceHostName}/apps/webclient/sweep/xmlReport/${externalId}/true/
  ?filter=hit_hash,%3D,${deviceCustomString1}
```

H.2. SmartConnector/FlexConnector

The script acquisition, remote web service, and MCIC API features can be integrated as an ArcSight Flex CounterACT *SmartConnector*, allowing two-way communication between an ArcSight ESM manager/console and MIR.

H.2.1. Installing the MIR Connector

ArcSight provides its own documentation for installing and maintaining SmartConnectors. In addition, MANDIANT has a separate installer for MIR-specific Connector files.

To install a MIR Connector:

1. Obtain the MIR connector installer zip package and unzip it to a local folder on the machine where the connector will be installed.
2. Copy the MIR CA cert file for the specified MIR environment to `mircacert.pem` in the same folder.
3. Edit the `MCICCommand.properties` files with appropriate parameters for the MIR target.
4. Run the SmartConnector install package. Take note of the installation folder used during the installation.
5. When the install is complete, a **SmartConnector Configuration Wizard** window will open.
   - Before continuing with the configuration, run the `install.bat` file in the MIR connector installer package. Provide the path to the SmartConnector install package used earlier.
6. Return to the **SmartConnector Configuration Wizard** window. Using the **Connector** selector, choose **Flex CounterACT**.
7. For **Use the Configuration Wizard for CounterACT Commands**, select **No**.
8. For **Configuration File**, use `MIRFlexConnector`. Capitalization is not important.
9. Proceed through the rest of the configuration, choosing defaults or customizing as appropriate.

H.2.2. Updating the MIR Connector

At any time after the installation, if users need to change the MIR settings, they can:

1. Stop the SmartConnector service.

2. Change the `MCICCommand.properties` file and/or `mircacert.pem`.
3. Re-run `install.bat`.
4. Restart the SmartConnector service

H.2.3. Removing the MIR Connector

The MIR connector must be removed before uninstalling ArcSight's Connector.

To remove a MIR connector:

1. Stop the SmartConnector service.
2. Obtain the MIR connector installer zip package and unzip it to a local folder on the machine where the connector will be installed.
3. Run the `uninstall.bat` file in the MIR connector installer package.

H.2.4. Using the Connector

Once the connector is installed and configured, the commands can be run manually or through correlation, as with any SmartConnector commands. The currently-supported commands and their parameters are:

When used in a MIR single discovery (i.e. multi-controller) environment, MIR connectors must be connected to the *sniper* machine. Pointing the connector to a *sweeper* machine will cause acquisition commands to fail. Furthermore, for script acquisitions only scripts that are local to the sniper machine can be used.

The connector parameters for file name, file path, and script name support spaces as part of the parameter value. Do not enclose values in double quotes.

Create Script Acquisition

- Host IP Address
- Script URI
  Note that the script URI must reference a script on the target controller, not a script on a different controller.
- Script Name

Create File Acquisition (API)

- Host IP Address
- File Name
- File Path

Create File Acquisition (RAW)

- Host IP Address

- File Name
- File Path

Get MIR Version

- No parameters. See *Section H.3.2, "Running a SmartConnector Command"*.

H.3. Common ArcSight Tasks

ArcSight is a complete enterprise security manager platform, with functionality far beyond the scope of this manual. Please consult the ArcSight user guide for detailed information regarding the use of URL integration, connectors, and rules.

There are a few common tasks that we can address:

H.3.1. Configuring a URL Integration Command

URL integration allows an ArcSight console user to connect back to the MCIC UI:

1. In the ArcSight **Navigator** pane, select **Integration Commands** from the dropdown list. The **Navigator** will display the **Commands** tab with a list of **Integration Commands**.
2. Right-click a *Commands* folder and select **New Command**. In the **Inspect/Edit** pane, the **Command Editor** will be displayed.
3. In **Type**, choose **URL** as the integration target type.
4. Provide a **Name** and a **URL** from *Chapter 12, URL Direct Access*. Click **Ok**.
5. Right-click the *Commands* folder again and select **New Configuration**. In the **Inspect/Edit** pane, **Configuration Editor** will be displayed.
6. In **Type**, choose **URL** as the integration configuration type.
7. Again, provide a **Name**, then select the **Commands** tab.
8. Click **Add** and select the previously-created command. Click **Ok**.
9. Click **Ok** at the bottom of the **Inspect/Edit** pane to save the configuration.

Now when you right-click an entry in the **Radar** view, you can select **Integration Commands** → **Your Command**. When you do this, MCIC will be opened to display the content appropriate for that entry.

H.3.2. Running a SmartConnector Command

ArcSight connectors allow ArcSight to command and control other products. This allows ArcSight to, for example, launch MCIC acquisitions based on ArcSight correlation rules. Connector commands can also be run manually from the ArcSight console.

1. In the ArcSight **Navigator** pane, select **Connectors** from the dropdown list. The **Navigator** will display the **Connectors** tab with a list of **Connectors**.

2. Right-click the **Connector** item that corresponds to *install MIR smart connector* and select a command from **Send Command** → **CounterACT**.

3. If the command requires parameters, a **Command Parameters** window will provide an opportunity to configure them. Click **Ok** when complete.

In the **Viewer** pane, a new **Connector Command** tab will be displayed. The bottom pane will display the command output as it is received by the ArcSight console.

H.3.3. Assigning Correlation rules with Connector Integration

When a MIR connector is configured in an ArcSight ESM installation, the connector commands can be configured to run automatically when triggered by correlation rules. The parameters for the connector commands can be filled in by event fields as needed. Correlations rules are configured in the ArcSight Console:

1. In the ArcSight **Navigator** pane, select **Rules** from the dropdown list. The **Navigator** will display the **Rules** tab with a list of **Rules**.

2. Right-click a **Rules** folder and select **New Rule**. In the **Inspect/Edit** pane, the **Rule Editor** will be displayed.

3. In the **Attributes** tab, provide a **Name** for the rule.

4. In the **Conditions** and **Attributes** tabs, configure event rules that will trigger the connector action.

5. In the **Actions** tab, select an action scenario. Click **Add**, then **Execute Connector Command**.

6. A window will be displayed. In the **Connector** dropdown list, select the MIR connector, then select a connector command. Note that MIR actions are prefixed with the label *counteract*.

7. If the selected command requires parameters, provide them as hard-coded strings or ArcSight field variable references.

8. Click **Ok** to close the configuration window.

9. In the **Rule Editor** tab, click **Ok** to save the new rule.

This rule will now run on the ArcSight manager and trigger the MIR connector actions as needed. If the MIR installation is configured to log CEF events back to the ArcSight ESM instance, the results of these connector actions will be logged.

Appendix I
Entropy, Anomalies, and Entry Point Signatures

A common problem facing incident responders is identifying suspicious or outright malicious software on a computer system. The Good Guys use a variety of techniques, from live response (the examination of a system's state while it's running) to temporal analysis (a fancy phrase for "timelining"), and everything in between. All of these techniques are geared towards identifying how the Bad Guys got in, what they left behind, and whether or not they're still lurking about.

Further complicating this equation is the fact that the Bad Guys don't want to be found and they usually know a lot about the techniques the Good Guys use to find them. Enter the world of anti-forensic techniques: a branch of hackery devoted to devising methods to hide things or to foil the analytical techniques used by the Good Guys. It's the modern day equivalent of backtracking across your own footsteps or dropping caltrops on the trail while you're being chased.

Some of the more common techniques in employ today include:

- Deleting indicators of entry to a system once it's compromised, removing log file entries, file modification/access dates, and system processes.
- Obfuscating running malware by changing its name or execution profile such that it appears to be something benign.
- Storing data on disk in a "packed" format. Packing is a technique that obfuscates or encrypts data or software and encapsulates it in a file along with a program to perform decryption/de-obfuscation. For example, a "Packed Executable" is a piece of software that contains an "unpacking" program and a payload. That payload is often malicious software, such as a virus or trojan horse.
- Encrypting data through use of an encryption algorithm and encryption key.

MANDIANT's *File Listing* Modules have the ability to analyze entropy and structure within executable files in order to provide information about potential anomalies which may be indicators of compromise.

I.1. The Entropy of Evil

One of the fundamental properties of encrypted, compressed, or obfuscated (depending on the method of obfuscation) data is that its entropy (or "randomness") tends to be higher than that of structured data, such as user generated documents and computer programs. A measure of entropy isn't a sure-fire method for identifying malware or the Bad Guy's hidden data store. A valid user may have encrypted or, more commonly, compressed information stored on a computer system. However, looking at entropy does provide an excellent filter when you are faced with a multi-gigabyte data reduction problem. Entropy is a measurement that can be used to determine if a stream of data is random.

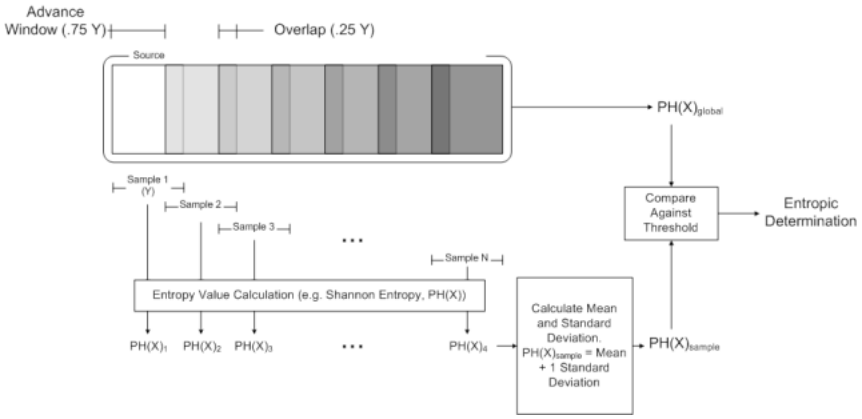
Entropy is a global measurement across a block of data. This means that data could return a low entropy measurement, although small sections might contain very high entropy.

MANDIANT Intelligent Response implements a unique sliding-window method for determining the entropy of a file, which makes it useful when analyzing a large block of data that may have small sections with highly random data, and are therefore potentially interesting to the investigator. Here is how it works:

1. The file is opened and bytes read in to calculate a *Global Entropy* value for the entire file. MIR uses the Shannon Entropy algorithm to calculate entropy for any block of data it analyzes.

2. MIR then divides the file into overlapping *samples* and calculates the entropy across them. For arguments sake, assume a file of size *X* is divided into *n* chunks:

Figure I.1. Entropy Analysis Flow



3. The mean and standard deviation of all entropy values from all samples is calculated. The overall entropy for the input file is derived by taking the mean and adding one standard deviation to it. This value is referred to as the *Sample Source Entropy*.

4. *Sample Source Entropy* and *Global Entropy* are compared to a threshold. This threshold is an empirically derived value between 0 and 1 (we have typically used 0.9). If either entropy value is greater than the threshold, the data block is determined to be entropic, and therefore potentially interesting.

I.2. Other File Anomalies

In addition to entropy, MIR can analyze executable files and determine a number of characteristics about their structure. Some of these characteristics may indicate an increased probability of suspicious software.

PE Structure Anomalies

Executable files ("Portable Executables" or PE Files, per Microsoft's *Portable Execution and Common Object File Specification*) have an expected structure and format. There are a number of anomalies that can occur within a PE that are often (though not always) suspicious indicators. See the table below for more information on PE anomalies that MIR can identify.

Imports Table
: Executable files often use functionality from other files on the system, such as Dynamically Linked Libraries (DLLs). These linkages are referred to as "imports". Excessive numbers of imports or redundant imports are often suspicious.

Section Permissions
: Sections of an executable file have individual permissions that indicate whether they can be read or contain executable code. Various combinations of these permissions in conjunction with other anomalies (such as the entropy measure for a section of a file) are frequently suspicious.

As mentioned above, there are several PE File anomalies that MIR can detect. The following table details these:

section_starts_unaligned
: Some packing tools will place data at a non-aligned offset within a section. This thwarts some forms of analysis and detection while still allowing the Windows operating system to properly load data or code contained in such a section.

checksum_is_zero
: Headers in a Windows Portable Executable contain a checksum for data contained inside them. If the contents have been modified, the checksum must be adjusted or Windows will not load the file. Attackers sometimes zero out this checksum if they modify the contents of an executable file. The file will still load and execute without a mismatched checksum error.

contains_eof_data
: This indicates that data may exist in the file past the End of File marker. This technique is sometimes used by an attacker to avoid casual inspection of their malicious data or payload by tools that only inspect information that comes before the EOF marker.

incorrect_imageSize
: This indicates that information contained in the executable file's header does not cross-check when attempting to calculate the size of the executable. This kind of discrepancy is sometimes an indicator of malicious manipulation.

corrupted_imports
: This indicates that there is no information in the file about imports (that is, linkages to DLLs that are used by the executable file). Highly suspicious, and often a sign of malicious modification of an executable file or extreme corruption.

empty_section_name
: This indicates that sections within the executable file are not properly named. Like other anomalies, this is a common artifact in a maliciously crafted or modified executable file.

non_ascii_section_name
: This indicates that sections within the executable file have names that contain non-ASCII characters — frequently a suspicious property.

overlapping_headers
: This indicates that header information in different sections of the executable file overlap.

oversized_optional_header
: This indicates that an optional header section of the executable file is larger than is standard, an indication of a potentially altered file.

oversized_section
: This indicates that a section of an executable file is larger than specified in associated header information.

invalid_entry_point
: This indicates that the entry point into the executable file is invalid or malformed in some fashion. While it may still execute, it violates standard form for Portable Executables.

I.3. Entry Point Signatures

In addition to the anomalies discussed above, MIR can identify several entry point signatures in executable files: that is, structural patterns that may indicate how an executable file was compiled or how it was packed. The following signatures can be identified by MIR:

I.3.1. Compiler Signatures

Borland Pascal v7.0 for Windows
Borland C for Win32 1994
Borland C for Win32 1995
Borland C for Win32 1999
Borland C
Borland C DLL
Borland Delphi vx.x (Component)
Borland Delphi DLL
Borland Delphi v2.0–v7.0
Borland Delphi v5.0 KOL/MCK
Borland Delphi v5.0 KOL
Borland Delphi v6.0 KOL
Borland Delphi Setup Module
Borland Delphi
Borland Delphi (Component)
Cygwin32
FASM v1.3x
Free Pascal v0.99.10
LCC Win32 v1.x
LCC Win32 DLL
Microsoft Visual C
Microsoft Visual C v2.0
Microsoft Visual C vx.x
Microsoft Visual C v4.x
Microsoft Visual C v4.2
Microsoft Visual C v4.2 DLL
Microsoft Visual C v5.0
Microsoft Visual C v5.0 DLL
Microsoft Visual C v5.0/v6.0 (MFC)
Microsoft Visual C v6.0 SPx
Microsoft Visual C v6.0

Microsoft Visual C v6.0 DLL
Microsoft Visual C v6.0 (Debug Version)
Microsoft Visual C v7.0
Microsoft Visual C v7.0 DLL
Microsoft Visual C# v7.0 / Basic .NET
Microsoft Visual C DLL
Microsoft Visual C
Microsoft Visual Basic v5.0
Microsoft Visual Basic v5.0/v6.0
Microsoft Visual Basic v6.0 DLL
MinGW GCC v2.x
MinGW GCC DLL v2xx
MinGW v3.2.x (Dll_main)
MinGW v3.2.x (Dll_WinMain)
MinGW v3.2.x (main)
MinGW v3.2.x (WinMain)
MinGW v3.2.x (Dll_mainCRTStartup)
MinGW v3.2.x (_mainCRTStartup)
Stranik 1.3 Modula/C/Pascal
WATCOM C/C 32 Run-Time System 1988-1995
WATCOM C/C 32 Run-Time System 1988-1994
WATCOM C/C
WATCOM C/C++ DLL

I.3.2. Packer Signatures

\.BJFnt v1.1b
\.BJFnt v1.2 RC
\.BJFnt v1.3
\.BJFnt v1.3
32Lite v0.03a
AcidCrypt
AcidCrypt
Alloy v1.x.2000
APatch GUI v1.1
ASPack v1.00b
ASPack v1.01b
ASPack v1.02a
ASPack v1.02b
ASPack v1.02b
ASPack v1.03b
ASPack v1.03b
ASPack v1.04b
ASPack v1.05b
ASPack v1.06b
ASPack v1.06b
ASPack v1.06b
ASPack v1.061b
ASPack v1.07b
ASPack v1.07b (DLL)
ASPack v1.07b

ASPack v1.07b
ASPack v1.07b
ASPack v1.08
ASPack v1.08
ASPack v1.08
ASPack v1.08.01
ASPack v1.08.01
ASPack v1.08.01
ASPack v1.08.01
ASPack v1.08.01
ASPack v1.08.01
ASPack v1.08.02
ASPack v1.08.x
ASPack v1.08.03
ASPack v1.08.03
ASPack v1.08.03
ASPack v1.08.04
ASPack v2.xx
ASPack v2.000
ASPack v2.001
ASPack v2.1
ASPack v2.11
ASPack v2.11b
ASPack v2.11c
ASPack v2.11d
ASPack v2.12
ASPack v2.12
ASPack v2.xx
Anticrack Software Protector v1.09 (ACProtect)
Anticrack Software Protector v1.09 (ACProtect)
Anticrack Software Protector v1.09 (ACProtect)
Anticrack Software Protector v1.09 (ACProtect)
ASProtect vx.x
ASProtect vx.x
ASProtect v1.0
ASProtect v1.1
ASProtect v1.1 MTE
ASProtect v1.1 MTEb
ASProtect v1.1 MTEc
ASProtect v1.1 BRS
ASProtect v1.2
ASProtect v1.2x
ASProtect v1.23 RC1
ASProtect v2.1x
ASPR Stripper v2.x unpacked
Blade Joiner v1.5
BopCrypt v1.0
CExe v1.0a
CD-Cops II
CodeCrypt v0.14b
CodeCrypt v0.15b

CodeCrypt v0.16b - v0.163b
CodeCrypt v0.164
Code-Lock vx.x
CodeSafe v2.0
CopyControl v3.03
CreateInstall Stub vx.x
Crunch/PE
Crunch/PE v1.0.x.x
Crunch/PE v2.0.x.x
Crunch/PE v3.0.x.x
Crunch v4.0
CrypKey v5 - v6
CrypWrap vx.x
CICompress v1.0
CipherWall Self-Extrator/Decryptor (GUI) v1.5
CipherWall Self-Extrator/Decryptor (Console) v1.5
DAEMON Protect v0.6.7
DEF v1.0
Ding Boy's PE-lock v0.07
Ding Boy's PE-lock Phantasm v0.8
Ding Boy's PE-lock Phantasm v1.0 / v1.1
Ding Boy's PE-lock Phantasm v1.5b3
DBPE v1.53
DBPE v2.10
DBPE v2.10
DBPE v2.33
DBPE vx.xx
DxPack 1.0
EP v1.0
EP v2.0
ExeBundle v3.0 (standard loader)
ExeBundle v3.0 (small loader)
Exe Shield vx.x
Exe Shield v1.7
Exe Shield v2.7
Exe Shield v2.7b
Exe Shield v2.9
EXE Stealth v1.1
EXE Stealth v2.7
EXE Stealth v2.71
EXE Stealth v2.72
EXE32Pack v1.36
EXE32Pack v1.37
EXE32Pack v1.38
EXE32Pack v1.39
EXE32Pack v1.3x
EXECryptor v1.3.0.45
EXECryptor v1.3.0.45
EXECryptor v1.4.0.1
EXECryptor v1.5.1.x
EXECryptor vx.x.x.x

EXEJoiner v1.0
ExeSmasher vx.x
EZIP v1.0
FSG v1.0
FSG v1.1
FSG v1.2
FSG v1.3
FSG v1.31
FSG v1.33
Feokt FixupPak v1.20
Gleam v1.00
Guardant Stealth aka Novex Dongle
Hasp dongle (Alladin)
Hasp 4 envelope dongle (Alladin)
Hardlock dongle (Alladin)
Inno Setup Module
Inno Setup Module
Inno Setup Module v1.09a
Inno Setup Module v1.2.9
Install Stub 32-bit
JDPack
kryptor 3
kryptor 5
kryptor 6
kryptor 8
kryptor 9
Krypton v0.2
Krypton v0.3
Krypton v0.4
Krypton v0.5
KGCrypt vx.x
LameCrypt v1.0
LTC v1.3
Lockless Intro Pack
LaunchAnywhere v4.0.0.1
Microsoft CAB SFX module
Macromedia Windows Flash Projector/Player v3.0
Macromedia Windows Flash Projector/Player v4.0
Macromedia Windows Flash Projector/Player v5.0
Macromedia Windows Flash Projector/Player v6.0
Neolite v2.0
NeoLite vx.x
NeoLite v1.0
NeoLite v1.0
NeoLite v2.00
NeoLite v2.00
NeoLite v2.0
NFO v1.0
NFO v1.x modified
NoodleCrypt v2.0
Nullsoft Install System v1.xx

Nullsoft Install System v1.xx
Nullsoft Install System v1.98
Nullsoft Install System v2.0b2, v2.0b3
Nullsoft PIMP Install System v1.3x
Nullsoft PIMP Install System v1.x
NX PE Packer v1.0
Obsidium v1.1.1.1
Obsidium v1.0.0.59 Final
Obsidium v1.0.0.61
Obsidium vx.x.x.x
ORiEN v2.11 (DEMO)
Pack Master v1.0 PC
PE Encryptor Alpha preview
PEEncrypt v4.0b (JunkCode)
PE Crypt v1.00/v1.01
PE Crypt v1.02
PE Crypt32 v1.02
PE Crypt32 (Console v1.0, v1.01, v1.02)
PE Intro v1.0
PE Lock NT v2.01
PE Lock NT v2.02c
PE Lock NT v2.03
PE Lock NT v2.04
PE Lock v1.06
PE Pack v0.99
PE Pack v1.0
PE Packer
PE Password v0.2 SMT/SMF
PE Protect v0.9
PC Shrinker v0.20
PC Shrinker v0.29
PC Shrinker v0.45
PC Shrinker v0.71
PC-Guard v3.03d, v3.05d
PC-Guard v4.05d, v4.10d, v4.15d
PC-Guard v5.00d
PE-Crypter Pack Master v1.0
PEBundle v0.2 - v2.0x
PEBundle v2.0b5 - v2.3
PEBundle v2.44
PECompact v0.90 - v0.92
PECompact v0.94
PECompact v0.971 - v0.976
PECompact v0.977
PECompact v0.978
PECompact v0.978.1
PECompact v0.978.2
PECompact v0.98
PECompact v0.99
PECompact v1.00
PECompact v1.10b1

PECompact v1.10b2
PECompact v1.10b3
PECompact v1.10b4
PECompact v1.10b5
PECompact v1.10b6
PECompact v1.10b7
PECompact v1.20 - v1.20.1
PECompact v1.22
PECompact v1.23b3 - v1.24.1
PECompact v1.24.2 - v1.24.3
PECompact v1.25
PECompact v1.26b1 - v1.26b2
PECompact v1.33
PECompact v1.34 - v1.40b1
PECompact v1.40b2 - v1.40b4
PECompact v1.40b5 - v1.40b6
PECompact v1.40 - v1.45
PECompact v1.46
PECompact v1.47 - v1.50
PECompact v1.55
PECompact v1.56
PECompact v1.60 - v1.65
PECompact v1.66
PECompact v1.67
PECompact v1.68 - v1.84
PECompact v1.4x+
PECompact v1.84
PECompact v2.x
PE Diminisher v0.1
PE Diminisher v0.1
PEncrypt v1.0
PEncrypt v3.0
PEncrypt v3.1
PEnguinCrypt v1.0
PENightMare v1.3
PENightMare 2 Beta
PENinja
PENinja modified
PEMangle
PESHiELD v0.1b MTE
PESHiELD v0.2 / v0.2b / v0.2b2
PESHiELD v0.25
PESHiELD v0.251
PEShit
PE Spin v0.b
PEtite v1.2
PEtite v1.3
PEtite v1.4
PEtite v1.4
PEtite v2.0
PEtite v2.1

PEtite v2.2
PEtite vx.x
PEX v0.99
PEX v0.99
PKLITE32 v1.1
PKLITE32 v1.1
PKLITE32 v1.1
Private EXE v2.0a
Private EXE v2.0a
Program Protector XP v1.0
Protection Plus vx.x
RatPacker (Glue) stub
Shrinker v3.2
Shrinker v3.3
Shrinker v3.4
Shrink Wrap v1.4
SecuPack v1.5
SmokesCrypt v1.2
Soft Defender v1.0 - v1.1
SoftSentry v2.11
SoftSentry v3.0
SoftWrap Spalsher v1.0 - v3.0
Special EXE Password Protector v1.0
SPEC b2
SPEC b3
Stealth PE v1.1
Stone's PE Encryptor v1.0
Stone's PE Encryptor v1.13
Stone's PE Encryptor v2.0
SVK-Protector v1.11
SVK-Protector v1.051
SVK-Protector v1.32
Symantec Visual Cafe v3.0
SOFTWrapper for Win9x/NT (Evaluation Version)
TASM / MASM
tElock v1.00
tElock v0.41x
tElock v0.42
tElock v0.51
tElock v0.4x - v0.5x
tElock v0.60
tElock v0.70
tElock v0.71
tElock v0.71b2
tElock v0.71b7
tElock v0.80
tElock v0.7x - v0.84
tElock v0.85f
tElock v0.90
tElock v0.92a
tElock v0.95

tElock v0.96
tElock v0.98
tElock v0.98b1
tElock v0.98b2
tElock v0.99
The Guard Library
Thinstall vx.x
UG2002 Cruncher v0.3b3
UPX v0.51 UPX v0.60 - v0.61
UPX v0.62 UPX v0.70
UPX v0.71 - v0.72
UPX v0.89.6 - v1.02 / v1.05 - v1.24 DLL
UPX v0.80 - v0.84
UPX v0.89.6 - v1.02 / v1.05 - v1.24
UPX v1.03 - v1.04 UPX v0.89.6 - v1.02 / v1.05 - v1.24 (Delphi) stub
UPX v0.89.6 - v1.02 / v1.05 - v1.24 (RAR SFX) stub
UPX v0.89.6 - v1.02 / v1.05 - v1.24 (RAR SFX) stub
UPX v0.81 - v0.84 Modified
UPX v0.89.6 - v1.02 / v1.05 - v1.24 Modified
UPX v1.03 - v1.04 Modified
UPX Alternative stub
UPX Modifier v0.1x
UPX Modified stub
VBOX v4.2 MTE
VBOX v4.3 MTE
VOB ProtectCD 5
VOB ProtectCD
Virogen Crypt v0.75
Winkript v1.0
WinZip 32-bit SFX v6.x module
WinZip 32-bit SFX v8.x module
WinRAR 32-bit SFX Module
Wise Installer Stub
Wise Installer Stub
Wise Installer Stub v1.10.1029.1
WWPack32 v1.00, v1.11, v1.12, v1.20
WWPack32 v1.x
X-PEOR v0.99b
Xtreme-Protector v1.05
Xtreme-Protector v1.06
XCR v0.11
XCR v0.12
XCR v0.13
X-PEOR v0.99b
y0da's Crypter v1.0
y0da's Crypter v1.1
y0da's Crypter v1.2
y0da's Crypter v1.x / Modified
ZCode Win32/PE Protector v1.01
*** Protector v1.1.11 (DDeM->PE Engine v0.9, DDeM>CI v0.9.2)
eXpressor v1.0x / v1.1x

eXpressor v1.2x
eXpressor v1.3x
eXpressor v1.4x
SafeDisk v2.65.010

Appendix J
Legal Notices and Credits

In addition to the open source projects listed below, MANDIANT Intelligent Response contains technologies from the Sleuthkit Project and the public packer database provided by Bobsoft and the PEiD Project. MANDIANT wishes to thank Bobsoft, the PEiD Project team, and Brian Carrier for their excellent work. Learn more about them at:

Sleuthkit
http://www.sleuthkit.org

PEiD Public Packer Database
http://www.peid.info

J.1. Component License Notices

MANDIANT Intelligent Response makes use of several Open Source and Shared Source technologies. The following license declarations are included in compliance with the licenses for those components. Note that these declarations govern MANDIANT's use of these technologies. Your purchase and use of MIR is governed solely by the MIR *End User License Agreement* (EULA) and software purchase agreement, which comply with the notices contained herein.

J.1.1. Be.HexEditor

Project URL. *http://www.gotdotnet.com*

License. This license governs use of the accompanying software ("Software"), and your use of the Software constitutes acceptance of this license. You may use the Software for any commercial or noncommercial purpose, including distributing derivative works. In return, we simply require that you agree:

1. Not to remove any copyright or other notices from the Software.

2. That if you distribute the Software in source code form you do so only under this license (i.e. you must include a complete copy of this license with your distribution), and if you distribute the Software solely in object form you only do so under a license that complies with this license.

3. That the Software comes "as-is", with no warranties. None whatsoever. This means no express, implied or statutory warranty, including without limitation, warranties of merchantability or fitness for a particular purpose or any warranty of title or non-infringement. Also, you must pass this disclaimer on whenever you distribute the Software or derivative works.

4. That no contributor to the Software will be liable for any of those types of damages known as indirect, special, consequential, or incidental related to the Software or this license, to the maximum extent the law permits, no matter what legal theory it is based on. Also, you must pass this limitation of liability on whenever you distribute the Software or derivative works.

5. That if you sue anyone over patents that you think may apply to the Software for a person's use of the Software, your license to the Software ends automatically.

6. That the patent rights, if any, granted in this license only apply to the Software, not to any derivative works you make.

7. That the Software is subject to U.S. export jurisdiction at the time it is licensed to you, and it may be subject to additional export or import laws in other places. You agree to comply with all such laws and regulations that may apply to the Software after delivery of the software to you.

8. That if you are an agency of the U.S. Government, (i) Software provided pursuant to a solicitation issued on or after December 1, 1995, is provided with the commercial license rights set forth in this license, and (ii) Software provided pursuant to a solicitation issued prior to December 1, 1995, is provided with "Restricted Rights" as set forth in FAR, 48 C.F.R. 52.227-14 (June 1987) or DFAR, 48 C.F.R. 252.227-7013 (Oct 1988), as applicable.

9. That your rights under this License end automatically if you breach it in any way.

10. That all rights not expressly granted to you in this license are reserved.

J.1.2. libcurl

Project URL. *http://curl.haxx.se*

License. COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2007, Daniel Stenberg, <<daniel@haxx.se>>.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

J.1.3. libxml2, libxslt, libexslt

Project URL. *http://xmlsoft.org*

License. License (libxml2)Except where otherwise noted in the source code (e.g. the files hash.c, list.c and the trio files, which are covered by a similar licence but with different Copyright notices) all the files are:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of the authors shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from him.

J.1.4. lxml

Project URL. *http://codes.peak.net/lxml*

License. lxml is copyright Infrae and distributed under the BSD license (see doc/licenses/BSD.txt), with the following exceptions:

Some code, such a selftest.py, selftest2.py and src/lxml/_elementpath.py are derived from ElementTree and cElementTree. See doc/licenses/elementtree.txt for the license text.

test.py, the test-runner script, is GPL and copyright Shuttleworth Foundation. See doc/licenses/GPL.txt. It is believed the unchanged inclusion of test.py to run the unit test suite falls under the "aggregation" clause of the GPL and thus does not affect the license of the rest of the package.

The doctest.py module is taken from the Python library and falls under the PSF Python License.

Copyright (c) 2004 Infrae. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of Infrae nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL INFRAE OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;

LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The ElementTree/XML Toys Library

Copyright (c) 1999-2003 by Secret Labs AB

Copyright (c) 1999-2003 by Fredrik Lundh

By obtaining, using, and/or copying this software and/or its associated documentation, you agree that you have read, understood, and will comply with the following terms and conditions:

Permission to use, copy, modify, and distribute this software and its associated documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies, and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Secret Labs AB or the author not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

SECRET LABS AB AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL SECRET LABS AB OR THE AUTHOR BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

J.1.5. log4net, Lucene

Project URLs. *http://logging.apache.org/log4net/*

http://lucene.apache.org

License. Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

   "License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

   "Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

   "Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of

this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the

Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   You must give any other recipients of the Work or Derivative Works a copy of this License; and

   You must cause any modified files to carry prominent notices stating that You changed the files; and

   You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

   You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied,

including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

J.1.6. OpenSSL

Project URL. *http://www.openssl.org*

License. LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact <openssl-core@openssl.org>.

OpenSSL License

Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (*http://www.openssl.org/*)" *

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact <openssl-core@openssl.org>.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (*http://www.openssl.org/*)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (<eay@cryptsoft.com>). This product includes software written by Tim Hudson (<tjh@cryptsoft.com>).

Original SSLeay License

Copyright © 1995-1998 Eric Young (<eay@cryptsoft.com>)

All rights reserved.

This package is an SSL implementation written by Eric Young (<eay@cryptsoft.com>). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (<tjh@cryptsoft.com>).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (<eay@cryptsoft.com>)" The word *cryptographic* can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (<tjh@cryptsoft.com>)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

J.1.7. PyLucene

Project URL. *http://pylucene.osafoundation.org*

License. Copyright (c) 2004 - 2005 Open Source Applications Foundation. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

J.1.8. SQLAlchemy

Project URL. *http://www.sqlalchemy.org*

License. This is the MIT license: *http://www.opensource.org/licenses/mit-license.php*

J.1.9. Twisted

Project URL. *http://twistedmatrix.com*

License.

J.1.10. zlib

Project URL. *http://www.zlib.net*

License. Copyright © 1995-2005 Jean-loup Gailly and Mark Adler This software is provided "as-is", without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly <jloup@gzip.org>

Mark Adler <madler@alumni.caltech.edu>

J.1.11. nginx

Project URL. *http://nginx.org/*

License. Copyright © 2002-2010 Igor Sysoev

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY AUTHOR AND CONTRIBUTORS "AS IS" AND * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

J.1.12. PCRE

Project URL. *http://www.pcre.org/*

License. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the University of Cambridge nor the name of Google Inc. nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

J.1.13. ipaddr

Project URL. *http://code.google.com/p/ipaddr-py/*

License. Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

   "License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

   "Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

   "Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

   "You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   You must give any other recipients of the Work or Derivative Works a copy of this License; and

   You must cause any modified files to carry prominent notices stating that You changed the files; and

   You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

   You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

J.1.14. commons-codec

Project URL. *http://commons.apache.org/codec/*

License. Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

   "License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

   "Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

   "Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

   "You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

   "Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

You must give any other recipients of the Work or Derivative Works a copy of this License; and

You must cause any modified files to carry prominent notices stating that You changed the files; and

You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages

of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

J.1.15. google-gson

Project URL. *http://code.google.com/p/google-gson/*

License. Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

   "License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

   "Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

   "Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

   "You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

   "Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

   "Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   You must give any other recipients of the Work or Derivative Works a copy of this License; and

You must cause any modified files to carry prominent notices stating that You changed the files; and

You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer

failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

MANDIANT CORPORATION
WWW.MANDIANT.COM