FIREEYE TECHNICAL DOCUMENTATION

# REDLINE

## USER GUIDE

## RELEASE 2.0

Redline User Guide

Release 2.0

Revision 1

**FireEye Contact Information:**

Website: www.fireeye.com

Support Email: redline@fireeye.com

**Phone (US):**

1.408.321.6300

1.877.FIREEYE

# Contents

# About Redline®

Redline lets you analyze a potentially compromised endpoint memory and file structure to find signs of malicious activity. With Redline, you can:

- Collect run processes, files, registry data (Windows only), and memory images (in Windows versions before 10).
- View imported data, including narrowing and filtering results around a given timeframe using Redline's TimeWrinkle™ and TimeCrunch™ features.
- Perform Indicators of Compromise (IOC) analysis (Windows only).
- Use whitelists to filter out known valid data based on MD5 hash values.

For examples of how to use Redline, see Use Cases and Best Practices on page 86.

# Timeline

Timeline in Redline helps identify when a compromise was introduced, which files were touched, and if (and how) the compromise persists.

Timeline provides a list of events sorted by time, which can be an overwhelming number of events. You can use the TimeCrunch and TimeWrinkle features along with filtering by user and/or process to hide activity that is irrelevant to your analysis.

For more information about using Timeline, see Timeline on page 57.

# Indicators of Compromise (IOCs)

IOCs are supported only for Windows endpoints.

Look for specific artifacts, such as files or processes, that may indicate a breach has occurred. You can use standard Indicators of Compromise (IOCs) as an artifact defining method.

For more information about IOCs, see Indicators of Compromise (IOCs) on page 52.

# Whitelists

A whitelist is a list of MD5 hash values known to be valid. Any components with a whitelisted MD5 hash value are known to be standard valid components. Whitelisting allows you to hide a large amount of data in Redline. Redline includes a whitelist by default and you can add additional whitelists. For more information about whitelists, see MD5 Whitelist on page 66.

# Installation

Redline is installed, upgraded, and uninstalled using a standard Windows wizard.

## System Requirements

Redline software can run on the following operating systems:

- Windows 10 (32-bit and 64-bit versions)
- Windows 8.x (32-bit and 64-bit versions)
- Windows 7 (32-bit and 64-bit versions)
- Microsoft Vista (32-bit version)
- Windows XP SP2 (32-bit version)
- Windows Server 2008 R2 (64-bit version)
- Windows Server 2003 R2 (32-bit and 64-bit versions)

For a list of operating systems on which you can run a Redline Collector, see Run Redline Collector on Host Computer on page 19.

Redline requires Microsoft .NET 4 or later. If .NET is not installed, the Redline installer will open a Microsoft .NET installation page in the default browser.

If the screen resolution for the machine on which you are running Redline is less than 1280x1024, Redline may not display as intended.

Redline can be run on a virtual machine (VM); however, the performance suffers. When executing on a VM, Redline experiences higher than expected CPU use when idle. Compared to running Redline on an actual computer, Redline on a VM takes considerably longer to perform intensive operations like creating an analysis session.

## Install

Installing Redline on a potentially compromised computer is a less than optimal practice, because of the following reasons:

- You cannot be certain that your analysis results are not compromised.
- You create the risk of overwriting potential evidence on disk or in memory.

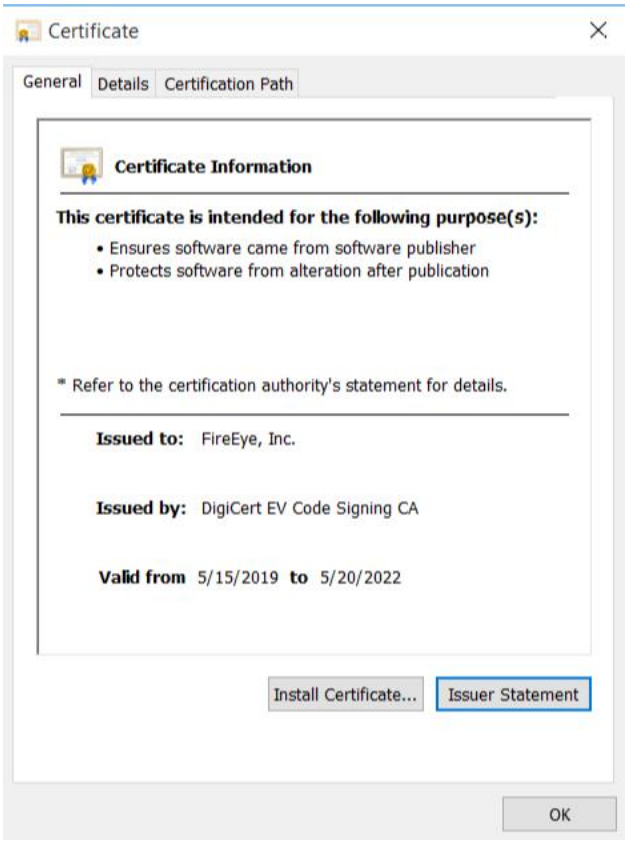
 

- You may tip off the attacker that you are investigating.

A clean environment is required for a Redline installation. Typically, this is a computer known to be secure and free from malware, in an area of the network that prevents it from any exposure to the suspect environment. Often, this computer is fully disconnected from the network. If you suspect the Redline workstation is infected, find a clean environment and run Redline from there.

To install Redline:

1. Download Redline from http://www.fireeye.com/services/freeware.html.
2. Verify the installer image to ensure you are installing a legitimate edition of Redline:
    a. Right-click **Redline.msi** and select **Properties**.
    b. Select the **Digital Signatures** tab.
    c. Verify the list contains **FireEye, Inc.**. Select it and click **Details**.
    d. Click **View Certificate** on the Digital Signature Details window.
    e. Confirm that the certificate was issued by **DigiCert EV Code Signing CA**.



3. Start the installation wizard by opening **Redline.msi**.
4. Click **Next** in the Welcome to the Redline Setup Wizard window.
5. Read the End User License Agreement carefully. To continue installing Redline, select **I Agree** and then click **Next** in the License Agreement window.
6. Choose a different installation folder and restrict user access to the application in the Select Installation Folder window (optional). By default, Redline is installed to **C:\Program Files(x86)\Redline** for **Everyone** to use.
7. Click **Next** in the Confirm Installation window. Redline should take only a few seconds to install.
8. Click **Close** to complete the installation process.

# Upgrade

You can upgrade Redline to a newer version by following the Redline installation instructions, see Install on page 3.

Upgrade does not impact the tags and comments that were added to an analysis session. See Tags and Comments on page 69 for more information.

# Uninstall

Redline is removed using the standard Windows uninstall software functionality. If you open the Redline installer (.msi file) and Redline is already installed, you will be given two options:

- Repair Redline
- Remove Redline

To remove Redline, select **Remove Redline** and click **Finish**.

To repair your current Redline installation, select **Repair Redline** and click **Finish**.

# Redline Collectors

A Redline Collector package contains an executable script to collect data from a potentially compromised endpoint. There are three types of Redline Collectors: Standard Collector, Comprehensive Collector, and IOC Search Collector (Windows only).

To use a Redline Collector:

1. Select the type of Redline Collector. See Select Redline Collector Type below.
2. Configure that Redline Collector. See Configure Standard and Comprehensive Redline Collectors on the next page or Configure IOC Search Redline Collector on page 8.
3. Save the Redline Collector package onto a portable media device.
4. Run the Redline Collector package on the potentially compromised host computer. See Run Redline Collector on Host Computer on page 19.
5. Import the audit (i.e., the data collected by the Redline Collector) into Redline. See Import Data into Redline on page 25.

# Select Redline Collector Type

Redline has three collector types:

- **Standard Collector.** The Standard Collector configures scripts to gather the minimum amount of data to complete an analysis.
- **Comprehensive Collector.** The Comprehensive Collector configures scripts to gather most of the data that Redline collects and analyzes. Use this type of Redline Collector if you intend to do a full analysis or if you have only one opportunity to collect data from a computer.
- **IOC Search Collector (Windows only).** The IOC Search Collector collects data that matches selected Indicators of Compromise (IOCs). Use this Redline Collector type when you are looking only for IOC hits and not any other potential compromises. By default, it filters out any data that does not match an IOC, but you can opt to collect additional data. If you do not use an IOC Search Collector, you can still analyze data collected with IOCs after the data has been imported into Redline to create an analysis session. The effectiveness of the IOC analysis depends on the data available in the analysis session. See Indicators of Compromise (IOCs) on page 52 for more information.

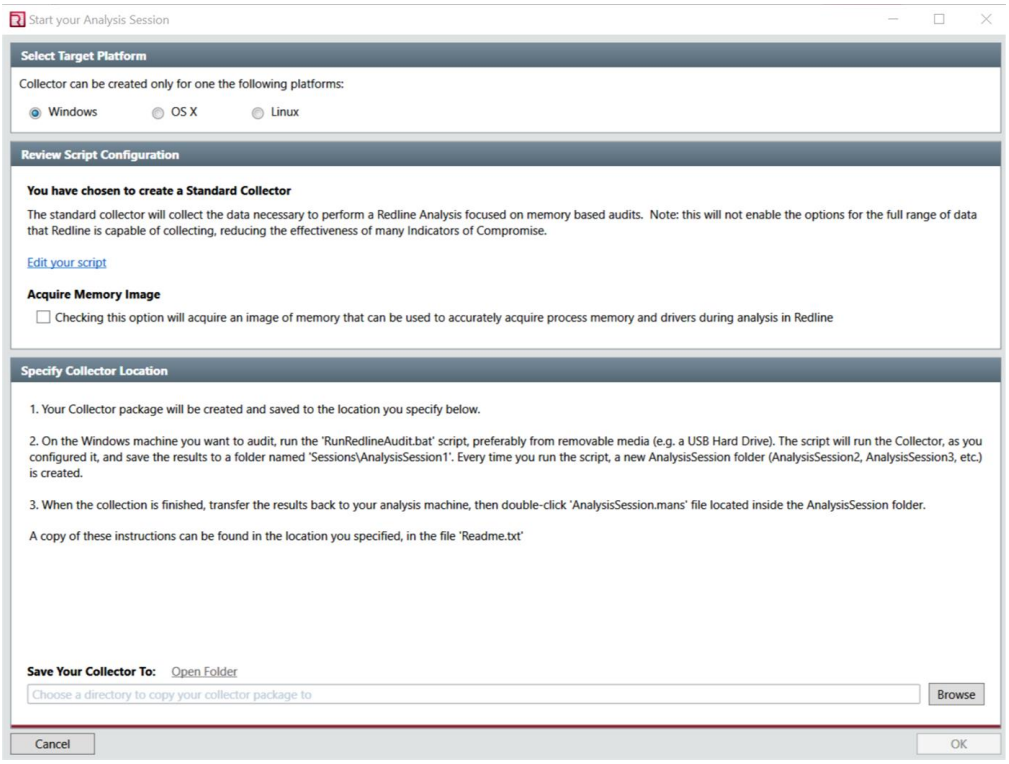
All three Redline Collectors have the option to acquire a memory image (this is only for Windows, and does not include Windows 10 update 1809). This option is required to acquire processes and drivers when analyzing data in Redline. See Driver and Process Acquisition on page 82 for more information.

The Redline Collector script has memory, disk, system, network, and other options preselected. You can modify these options within any collector type. See Edit Redline Script on page 9 for more information.

# Configure Standard and Comprehensive Redline Collectors

To configure either a Standard or Comprehensive Redline Collector:

1. Select **Create a Standard Collector** or **Create a Comprehensive Collector** on the Redline home screen or from the menu.




2. Select the target platform for the collector.
3. Click **Edit your script** to open the View and Edit Your Script window to make changes. See Edit Redline Script on page 9 for more information.

4. Click the option under **Acquire Memory Image** either on the Memory tab of the View Your Script window or under Review Script Configuration (optional). This is only for Windows, and does not include Windows 10 update 1809.

You must select **Acquire Memory Image** to acquire drivers and processes during data analysis in Redline. See Driver and Process Acquisition on page 82 for more information.

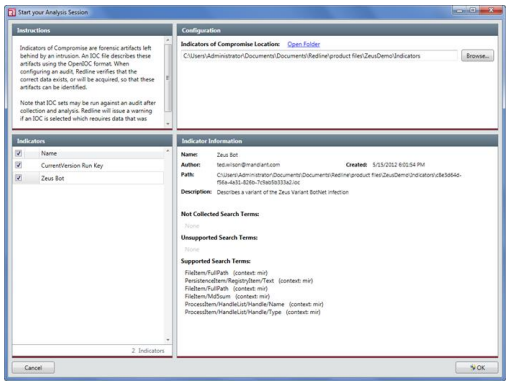
5. Click **Browse** under **Save Your Collector To** on the collector configuration window to specify an empty directory to save the collector.
6. Click **OK** to write the Redline Collector.

# Configure IOC Search Redline Collector

This functionality is supported only for Windows hosts.

To configure an IOC Search Collector:

1. Select **Create an IOC Search Collector** on the Redline home screen or from the menu.
2. Click **Browse** next to **Indicators of Compromise Location**.
3. Select the folder in which the IOC files are located.




4. Click **Open Folder** to view the individual IOCs (optional).

Note which IOCs are in the folder. You will need to select the same IOCs when you import the IOC Search Collector data into Redline. See Import Data into Redline on page 25 for more information.

5. Review the list of indicators. Each IOC can be enabled and disabled selectively using its checkbox. To enable or disable the entire list, select the checkbox at the top of the column. Selecting a column header will sort the list. See Data Analysis with IOCs on page 53 for more information about the indicators.
6. Click **Next** to proceed with configuring the collector.
7. Click **Edit your script** to open the View and Edit Your Script window to make changes. See Edit Redline Script below for more information. Note that unchecking default options may reduce the IOC analysis effectiveness. The following message may appear in red at the bottom of the View and Edit Your Script window: "Script may not gather all the data needed for your IOCs." To enable the options so the script collects the data, click **Click here to fix**.

By default, the script collects only data matching an IOC. Uncheck the filtering options, which are advanced parameters on the Memory tab, to collect additional data. See Memory Options in Script on page 11 for more information.

8. Click the option under **Acquire Memory Image** either on the Memory tab of the View Your Script window or under Review Script Configuration if desired (this is only for Windows and does not include Windows 10 update 1809).

You must select **Acquire Memory Image** to acquire drivers and processes during data analysis in Redline. See Driver and Process Acquisition on page 82 for more information.

9. Click **Browse** under **Save Your Collector To** on the collector configuration window to specify an empty directory to save the collector.
10. Click **OK** to write the IOC Search Collector.

# Edit Redline Script

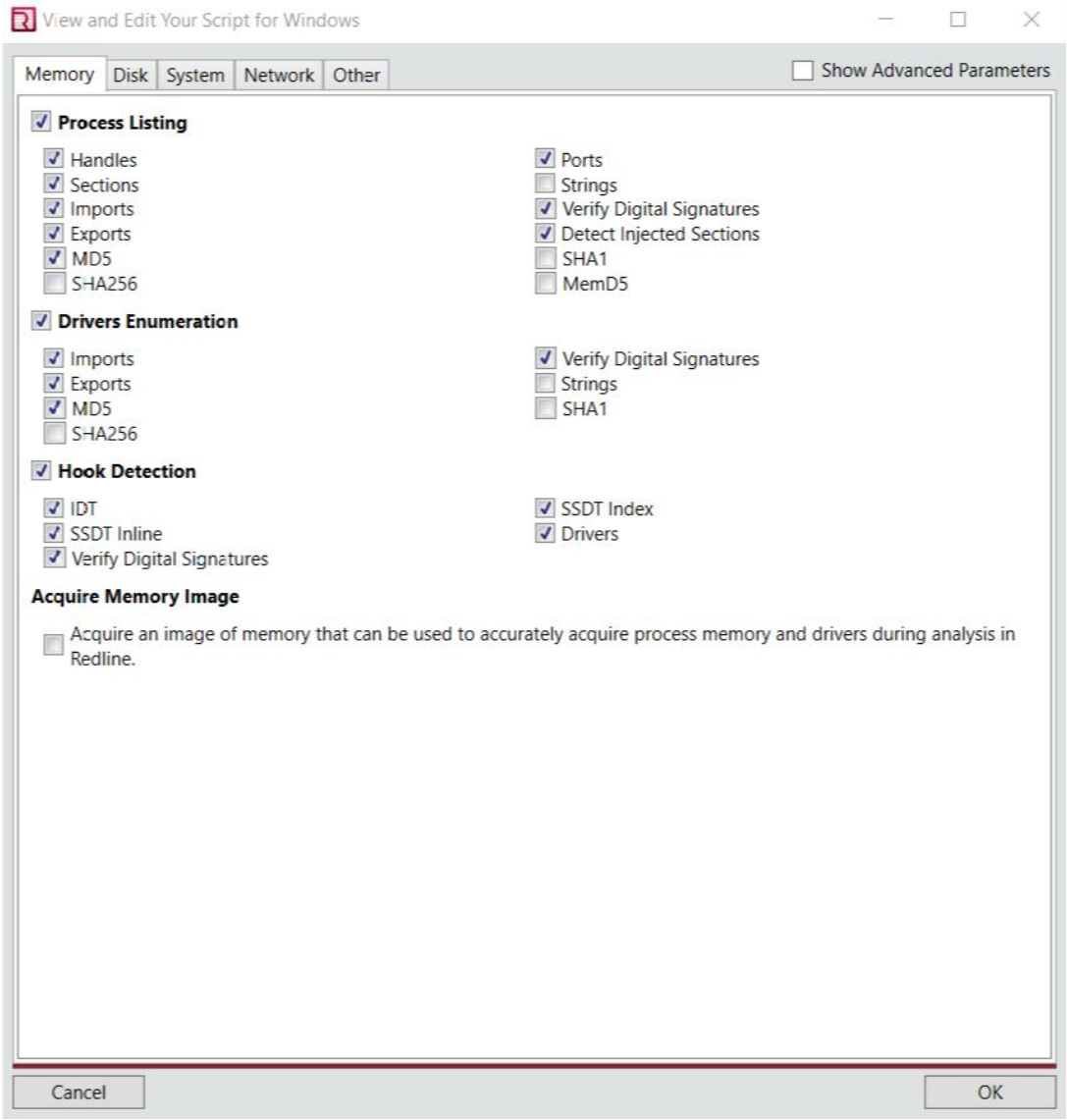
Redline collects data for analysis by using a predefined, configurable script as follows:

- A Redline Collector runs the script to collect disk, memory, system, network, and other data from a potentially comprised endpoint.
- When you open a memory image in Redline, the script is run against it to create an analysis session.

When deciding what data to collect with the script, consider the impact of collecting the following:

- Strings and resource data for files increases the size of the data collected.
- Hashes and digital signatures increase the amount of time it takes the script to run.
- Path and depth for both files and registry could increase both the data size and collection time depending on the drive size.

To edit scripts, click **Edit your script** on the Start Your Analysis Session window when configuring a Redline Collector or analyzing a saved memory file (this is only for Windows versions prior to 10). The View and Edit Your Script window has the following tabs for configuring a script: Memory, Disk, System, Network, and Other. Only the Memory tab is available when configuring a script to analyze a memory image.



View and Edit Your Script window accessed by clicking **Edit your script** on the Start Your Analysis window.

You can check and uncheck options under each tab. By default, only the basic options are shown. To display the advanced options on all tabs, select **Show Advanced Parameters** in the top right corner.

# Memory Options in Script

You can configure the script to collect memory data such as process listings, drivers enumeration (Windows only), and hook detection (Windows versions prior to 10 only).

## Process Listings

Platform support: Windows, OS X, Linux. Script options are supported on Windows only.

The script provides options to collect the following process listings data from memory; the option's impact is noted if relevant:

- Handles
- Memory sections and injected memory sections
- Imports
- Exports
- MD5, SHA256, SHA1, and MemD5 hashes (increase data collection time). You must collect MD5 to use the whitelisting function in Redline. See MD5 Whitelist on page 66 for more information about whitelisting.
- Ports
- Strings (increases data size)
- Digital signature verification (increases data collection time and requires Internet access on the computer on which the Redline Collector is run to ensure accurate data is collected)

To filter what is collected, you can specify the following:

- One process ID (PID) to analyze
- First 15 characters of the name of one process
- Shortest matched string (the default is 8)
- A regular expression to return only matching processes with particular content

These filter options are advanced parameters.

## Drivers

 Platform support: Windows.

The script provides options to collect the following drivers data; the option's impact is noted if relevant:

- Imports
- Exports
- MD5, SHA256, and SHA1 hashes (increase data collection time)
- Digital signature verification (increases data collection time)
- Strings (increases data size)

By default, the shortest matched string is 8 characters. To change the number of characters for the shortest matched string, enter a new number; this option is an advanced parameter.

## Raw File Access

 Platform support: Windows.

By default, the Redline script uses a Windows API to gather information from the host. These system calls are not able to access files locked by the operating system or deleted files, and they have the potential to return false information if malware hooks those calls and modifies the information sent and received.

When using raw file access, the script accesses and parses structures as they exist on the disk and in memory directly, thus avoiding any tampering caused by rootkits. Using raw file access may also allow the script to access information restricted by the operating system's user access controls and deleted files that still exist in the master file table.

Raw access is more powerful than Windows API calls but takes longer to process data. The options to include active raw files and parse the NTFS INDX buffers are applicable only when using raw file access; see Disk Options in Script on the next page for more information.

Using raw file access is an advanced parameter option for process listing and drivers enumeration. In addition to selecting these options in each script, you can set using raw file access as a global default option on the Redline Options window. See Global Default Script Options on page 17 for more information.

## Hook Detection

 Platform support: Windows (versions prior to Windows 10).

For hook detection, the script provides options to collect:

- Interrupt Descriptor Table (IDT)
- System Service Dispatch Table (SSDT) inline and SSDT index
- Drivers
- Digital signatures (increases data collection time)

The script also has the option to acquire a memory image for process and driver acquisition during analysis in Redline. See Process and Driver Acquisitions on page 83 for more information.

## IOC Search Collector Filtering

 Platform support: Windows.

By default, an IOC Search Collector script filters out data that does not match an Indicator of Compromise (IOC). To disable the filter and return more data, uncheck the **Apply Collector Based Filtering** options under Processing Listing, Driver Enumeration, and Hook Detection. These options are advanced parameters only when you are editing a script for an IOC Search Collector.

# Disk Options in Script

 Platform support: Windows, OS X, and Linux

You can configure the script to enumerate and collect both file and disk (Windows and OS X only) data.

The script provides the following file enumeration options; the option's impact is noted if relevant:

- Include active files (Windows only; applicable only if the script is using raw file access. See Memory Options in Script on page 11 for more information)
- Parse NTFS INDX buffers (Windows only; applicable only if the script is using raw file access on Windows. See Memory Options in Script on page 11 for more information)
- Analyze entropy (Windows only)
- Enumerate imports (Windows only)
- Verify digital signatures; this increases data collection time (Windows only)
- Include directories*
- Get resources (Windows only)

- Get resource data; this increases data size (Windows only)
- Get MD5, SHA256, and SHA1 hashes (and also filter based on specific hash values) (increases data collection time)
- Include deleted raw files (Windows only)
- Analyze file anomalies (Windows only)
- Enumerate exports (Windows only)
- Get strings; this increases data size (Windows only)
- Include files*
- Get program executable (PE) version info (Windows only)
- Include Remote Locations (OS X and Linux only)

*You must select either include directories or include files for the script to get results.

By default, the script collects data from the %systemdrive% path on Windows, and from / (root) on OS X and Linux. You can modify this path or specify a regular expression for it. By default, the search depth is 6 levels; the scan entry point distance is 8; and the shortest match string is 8 characters long. You can search for files using regular expressions to match content, and enter resource types for the script to exclude when extracting PE resources (Windows only). These options are all advanced parameters. Depending on the driver size, the path and depth can increase both the data collection time and size.

For disk enumeration for Windows and OS X, the script provides options to collect the following:

- Disks
- Volumes

## System Options in Script

 Platform support: Windows, OS X, and Linux

You can configure the script to collect system and registry information and event logs.

For system information, the script provides options to:

- Obtain machine and operating system (OS) information
- Analyze system restore points (Windows versions prior to 10 only)
- Enumerate the registry hives (Windows only)
- Obtain user accounts (Windows and OS X only)
- Obtain groups (OS X only)
- Obtain the prefetch cache (Windows only)

You can specify the top-level path to start gathering data and the level of depth to go for registry enumeration. You can further limit data gathering by specifying a regular expression and type. These options are advanced parameters. Depending on the driver size, the path and depth can increase both the data collection time and size.

The script enumerates and acquires all logs by default on Windows. You can specify the event logs to parse, including the file name and path, under advanced parameters.

The script can be configured to acquire system logs on OS X.

## Network Options in Script

 Platform support: Windows, OS X, and Linux

You can configure the script to collect network information (all OS) and browser history (Windows and OS X only).

The script provides options to enumerate the ports (all OS) and collect data from the following tables (Windows and OS X only):

- Domain naming system (DNS)
- Address resolution protocol (ARP)
- Routing

For browser history (Windows and OS X only), the script provides options to collect:

- Cookies
- Form history (Chrome and Firefox only)
- Thumbnails (Chrome and Firefox only)
- Quarantine Events (OS X only)
- Files downloaded
- URL history
- Indexed page content (Chrome and Firefox only)

You can also specify a target browser (Windows and OS X) and the path for history files to be parsed (Windows only); both are under advanced parameters.

To enter specific browsers from which to collect data, type the name of each browser on a separate line for the Target Browser option. To have the script collect data from every browser on the host computer, leave the Target Browser option blank.

All browsers store web history in the Windows user profile folder for each user account on the system. You can specify a specific public folder or specific history files from which to collect data by typing the path for the History Files Location option.

## Other Options in Script

 Platform support: Windows, OS X, and Linux

You can configure the script to collect services, tasks, and common memory persistence mechanisms data. These options are only available for Windows and OS X.

For both services and tasks, the script provides options to collect MD5, SHA256, and SHA1 hashes values and verify digital signatures; these options increase data collection time. In the advanced parameters options, you can opt to collect services and tasks using raw file access (Windows only). See Memory Options in Script on page 11 for more information.

For common memory persistence mechanisms, the script provides the following options; the option's impact is noted if relevant:

- Analyze entropy (Windows only)
- Enumerate imports (Windows only)
- Get resources (Windows only)
- Obtain MD5, SHA256, and SHA1 hashes (increase data collection time)
- Analyze file anomalies (Windows only)
- Enumerate exports (Windows only)
- Get program executable (PE) version info (Windows only)
- Verify Digital Signatures (OS X only)

By default the scan entry point distance (Windows only) is set to 8; you can change this under advanced parameters.

Linux pages have a different set of configurable script options, which consist of tasks, kernel modules, login history, and shell history. For tasks, the script provides options to collect MD5, SHA256, and SHA1 hash values.

In the advanced parameters options you can configure the following:

- Kernel Modules
    - Enumerate Aliases
    - Enumerate Dependencies
    - Enumerate Parameters
    - MD5, SHA1, SHA256 (increase data collection time)

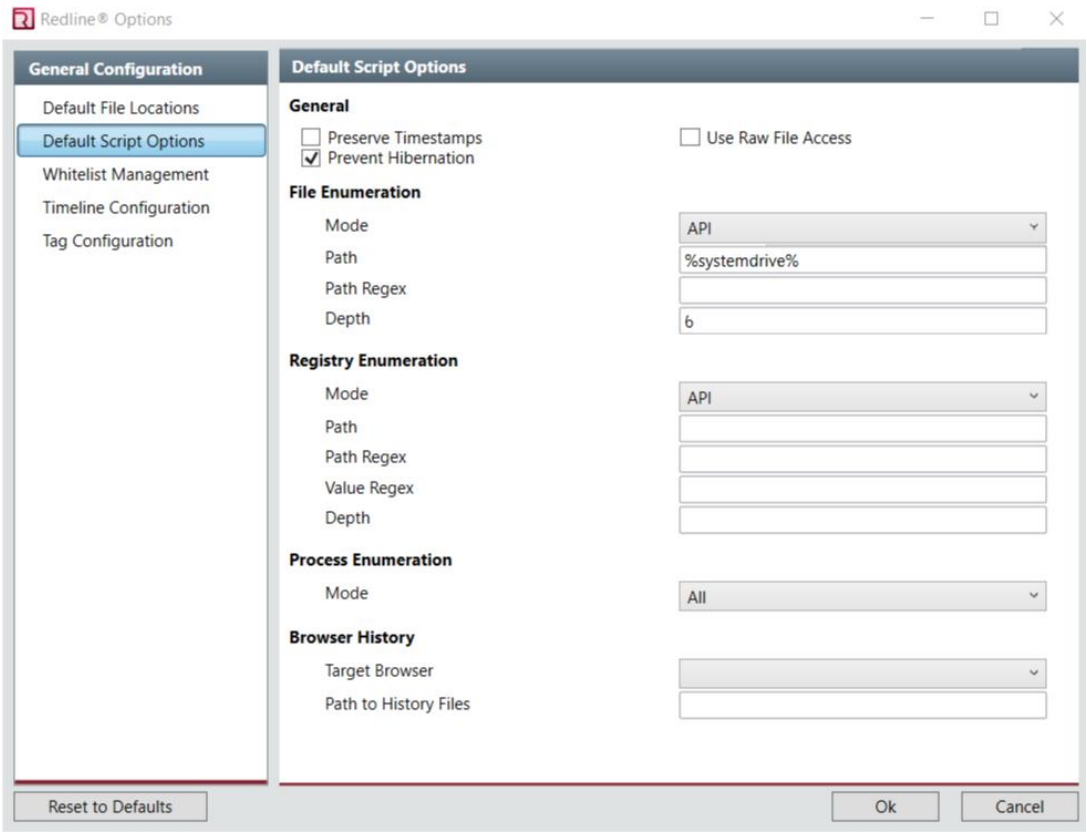
 

- Login History
  - History Path (default/var/run/utmp)
  - Include Failed Logins
  - Include Historical Logins
- Shell History
  - Filter by username(s). Enter one username per line.
  - Filter by shells. Supported shells are bash, zsh, and ksh93. Enter one shell name per line. If no shell name is entered, then all shells are processed.
  - Command regex. Enter one regex per line (must be a Perl-compatible regular expression)

## Global Default Script Options

 Platform support: Windows

Script global default options are set under **Default Script Options** on the Redline Options window, accessed by selecting **Redline Options** under the  menu.




Default Script Options in Redline Options window.

The following scripting options are global defaults (i.e., apply to every script):

- **Preserve Timestamps.** File timestamps are not updated when a file is read.
- **Prevent Hibernation.** The Redline Collector will not allow the host computer to hibernate, which allows the collection to finish in a timely fashion.
- **Use Raw File Access.** The script uses raw file access instead of a Windows API for accessing files. This option can be changed in each script; see Memory Options in Script on page 11 for more information.
- **File Enumeration.** The script can use Windows API or raw file access or both to enumerate the files. You can specify a search path name or regular expressions, and search tree depth.
- **Registry Enumeration.** The script can use Windows API or raw file access or both to enumerate the registry. You can specify a search path root, path name, and both path and value regular expressions, as well as search tree depth.
- **Process Enumeration.** The script can use handles, memory, or Windows API, or all three to enumerate processes.

- **Browser History.** The script can read the cache from Firefox, Microsoft Internet Explorer, Safari, Chrome, or all of these. You can set the path for the script to read history files.

# Run Redline Collector on Host Computer

**Windows**

Redline Collectors support the following versions of Windows:

- Windows 10 (32-bit and 64-bit)
- Windows 8.1, Update 1 (32-bit and 64-bit)
- Windows 8 (32-bit and 64-bit)
- Server 2019 (64-bit)
- Server 2016 (64-bit)
- Sever 2012 R2 (64-bit)
- Server 2012 (32 bit and 64 bit)
- Server 2008 R2 (32-bit and 64-bit)

Redline Collectors support the following versions of OS X:

- Mavericks 10.9 (64-bit)
- Yosemite 10.10 (64-bit)
- El Captain 10.11 (64-bit)
- Sierra 10.12 (64- bit)
- High Sierra 10.13 (64-bit)
- Mojave 10.14 (64-bit)

## Linux

Redline Collectors support the following versions of Linux:

- RHEL versions 6.8, 6.9, 6.10, 7.2, 7.3, 7.4,7.5, 7.6 (64-bit)
- CentOS versions 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6 (64-bit)

**To run a Redline Collector on a Host Computer:**

1. Mount the portable storage device containing the Redline Collector on the host computer.
2. Execute **RunRedlineAudit.bat** from the device. It will save the results to a folder named **Audits**.
3. When the collection is finished, import the audit (i.e., data collected by the Redline Collector) into Redline; see Import Data into Redline on page 25.

To acquire a memory image from the host, the device on which you want to save the image (i.e., the portable storage device) must have at least the equivalent amount of available drive space as the host computer.

- SUSE Enterprise Linux versions 11.4, 12.2, 12.3, 15 (64-bit)
- Ubuntu versions 14.04, 16.04, 18.04 (64-bit)
- Amazon Linux AMI versions 2018.3 (64-bit)

# Run Redline on This Computer

Platform support: Windows

The **Analyze This Computer** option on the menu allows you to configure a Redline Collector, run it, then analyze the data on the same computer.

The **Analyze This Computer** option is offered only for training and demonstration purposes. This is a great way to gain experience using Redline, but it is not recommended for actual investigations.

Always conduct real investigations in Redline installed on a clean and protected computer.

# Running A Redline Collector

## Step 1: Create a Collector on your Computer

1. Select to **Create a Standard Collector** from the **Redline Start** screen.

   You can choose standard or comprehensive. For this example, we will do a standard collection.

2. On the **Select Target Platform** pane, select your target platform: Windows (default), OS X, or Linux

3. On the **Review Script Configuration** pane, click **Edit your script**.

   You can use the default settings or select the **Show Advanced Parameters** checkbox to add advanced parameters. For this example, we will use the default settings.

4. To save your Collector, click the **Browse** button to browse to an empty folder on your computer or create a new empty folder. The folder must be empty.

   This folder is where you will create your Collector. Click the **Ok** button and Redline will create the audit scripts that are used to collect data from the host computer.

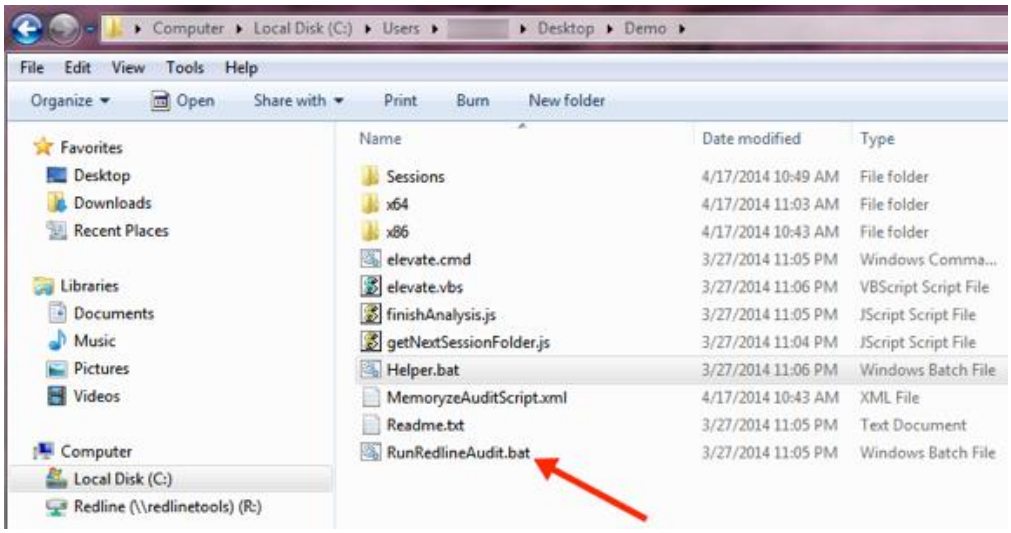
   
   

# Step 2: Run a Collector on a Host Computer

## Windows

1. Move the Collector file to the host computer you wish to collect files from.
2. To execute the Collector, click the **RunRedlineAudit.bat** file. The Collector creates the following folders **Sessions > AnalysisSession1 > Audits** and collects the data under the **Audits** folder.

   Each time the **.bat** runs, Redline will number the **AnalysisSessions** (Analysis Session1, 2, and 3) folders as they are created.




## OS X

1. Move the Collector file to the host computer you wish to collect files from.
2. To execute the Collector, double-click the **RunRedlineAudit** script file in Finder. You will need to know the superuser (sudo) password in order to execute the script.

   The Collector creates the following folders **Sessions > AnalysisSession1 > Audits** and collects the data under the **Audit** folder.

   - Each time the script runs, Redline will number the **AnalysisSession** (Analysis Session1, 2, and 3) folders as they are created.

## Linux

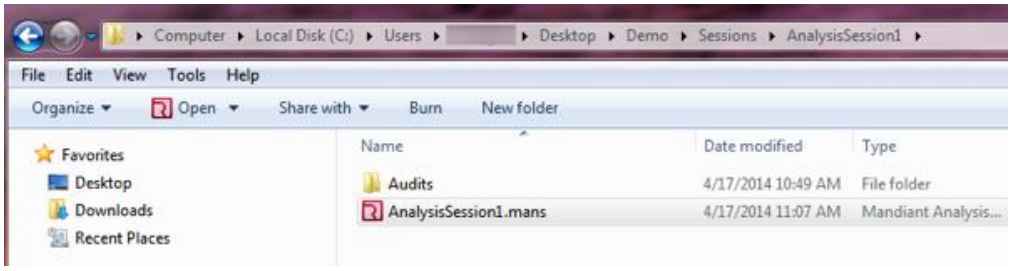
1. Move the Collector file to the host computer you wish to collect files from.
2. To execute the Collector, double-click the **RunRedlineAudit** script file in File Browser or run it in Terminal using the `bash RunRedlineAudit` command. You will need to know the superuser (sudo) password in order to execute the script.

   The Collector creates the following folders **Sessions > AnalysisSession1 > Audits** and collects the data under the **Audit** folder.

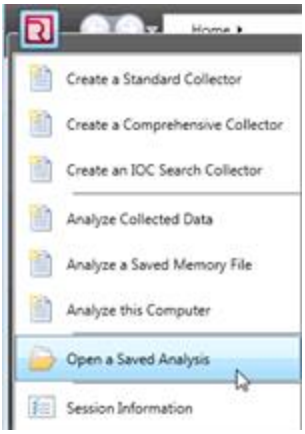
   - Each time the script runs, Redline will number the **AnalysisSession** (Analysis Session1, 2, and 3) folders as they are created.

# Step 3: Import Collector Data on your Computer

1. After the Collector completes the collection, go into the **AnalysisSession** folder and you will see an **Audits** folder and an **AnalysisSession.mans** file.




   Alternatively, you can open the .mans file from the Redline menu. Select **Open a Saved Analysis**.




2. Double-click the .mans file to create your session in Redline. This automatically imports the data into Redline.

You can now begin your investigation.

# Analysis Session Creation

A Redline analysis session contains data collected from one potentially compromised computer along with Redline's analysis of that data.

To create an analysis session, Redline can do the following:

- Import a Redline Collector audit.
- Import an audit from FireEye Endpoint Threat Prevention Platform (HX).
- Open Triage Collections from FireEye Endpoint Threat Prevention Platform (HX).
- Analyze memory images from Mandiant Memoryze™.

Redline can analyze data with Indicators of Compromise (IOCs) when data is initially imported into Redline or any time after the analysis session has been created (Windows only).

# Import Data into Redline

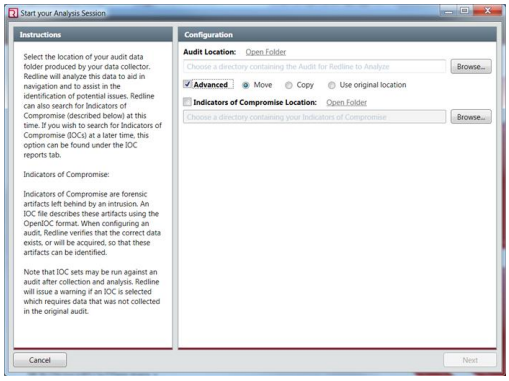
Redline can import audits from any Redline Collector or the FireEye Endpoint Threat Prevention Platform (HX).

To import data:

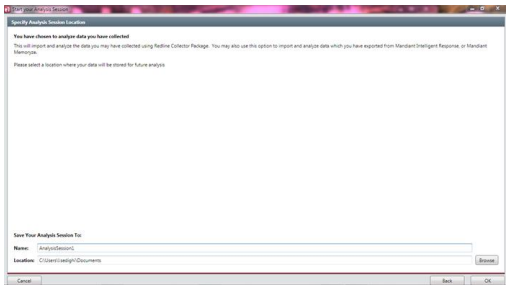
1. Select **Analyze Collected Data** from the  menu.
2. Select the folder containing the audit files by clicking **Browse** under **Audit Location** on the Start Your Analysis window. Once you have selected the folder, click **Open Folder** to view the folder's contents (optional).

   Check the **Advanced** box to view the alternative options for opening your audit. You many choose to move, copy, or use the original locations. Redline will remember your selection and use that as default until you change it.
3. Select the Indicators of Compromise (IOC) files location to compare the audit data against an IOC and create an IOC Report. This is optional and only supported on

Windows. See Data Analysis with IOCs on page 53 for more information.




4. Click **Next**.
5. Under **Save Your Analysis Session To** the **Name** field is the name of the folder where your Analysis Session is stored. This folder is in the **Location** specified.



6. Click **OK** to create the analysis session. If you opted to analyze the data against IOCs (Windows only), Redline creates an IOC Report in the background after creating the analysis session. See IOC Reports on page 55 for more information.

# Analyze Memory

Platform support: Windows versions prior to 10

Several third-party utilities capture a direct image of an operating system's physical memory. Redline can analyze these dd-format memory image files, but the analysis is limited to the data collected in the image, which may not be very extensive.

To ensure that Redline has adequate data to analyze, we recommend that you use a Redline Collector to capture a memory image.

When you analyze a memory image file, the computer on which Redline is installed must have enough available free memory to load the entire memory image.

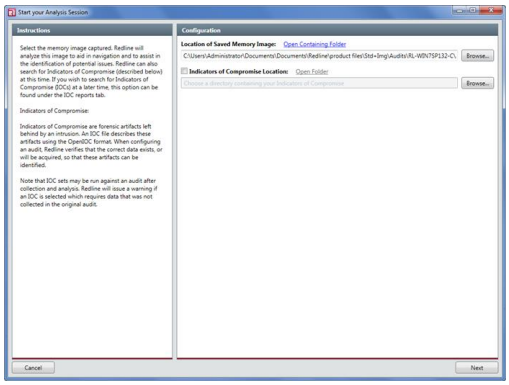
 

Memory analysis ranges from minutes to many hours depending on:

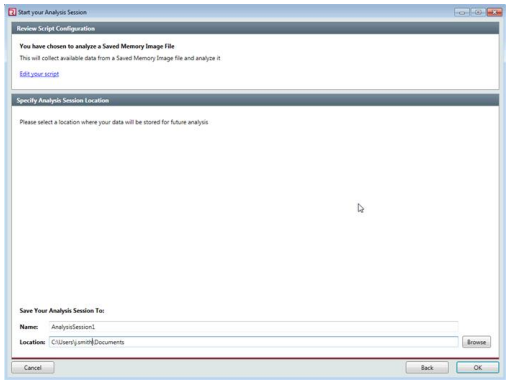
- Size of the captured memory image
- Operating system (OS) captured in the image

To import memory images into Redline to create an analysis session:

1. Copy the image to the computer on which Redline is installed. Do not open the memory image file over a network share.
2. Select **From a Saved Memory File** under Analyze Data on the home screen or **Analyze a Saved Memory File** from the menu.
3. Click **Browse** under **Location of Saved Memory Image**.
4. Select a folder containing Indicator of Compromise (IOC) files to create an IOC Report (optional). See Data Analysis with IOCs on page 53 for more information.

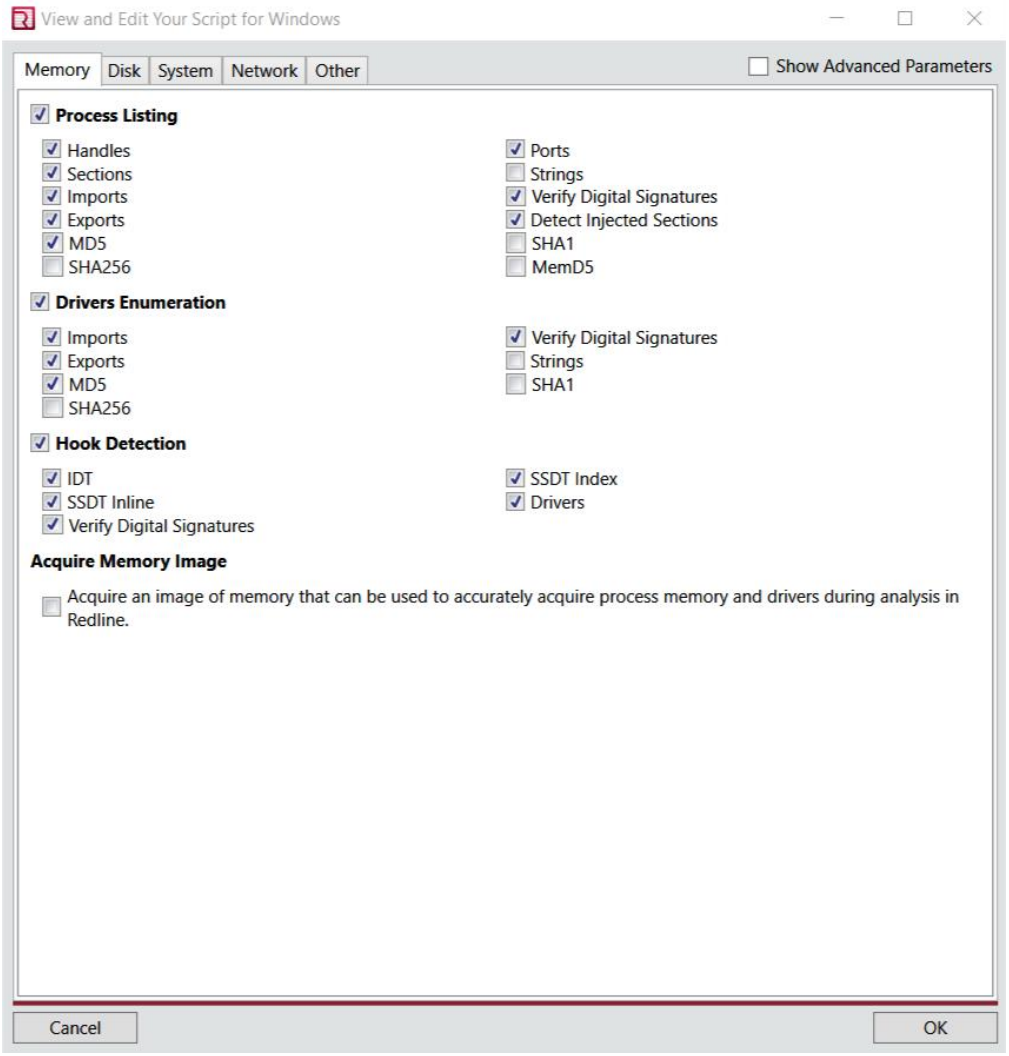



5. Click **Next**.




6. Under **Save Your Analysis Session To** the **Name** field is the name of the folder where your Analysis Session is stored. This folder is the **Location** specified.

7. Click **Edit you script** under Review Script Configuration if you wish to change the default memory script options. See Edit Redline Script on page 9 for more information.




8. Click **OK** on the Start Your Analysis Session Window to create an analysis session.

# Open HX Triage Collection

Redline recognizes FireEye Endpoint Threat Prevention Platform (HX) Triage Collections as analysis sessions.

To open a Triage Collection in Redline, do one of the following:

- Double-click the Triage Collection.
- Select **Open a Saved Analysis** from the home screen or menu and locate and select the Triage Collection.

# Open Saved Analysis Session

Redline analysis sessions are saved continuously.

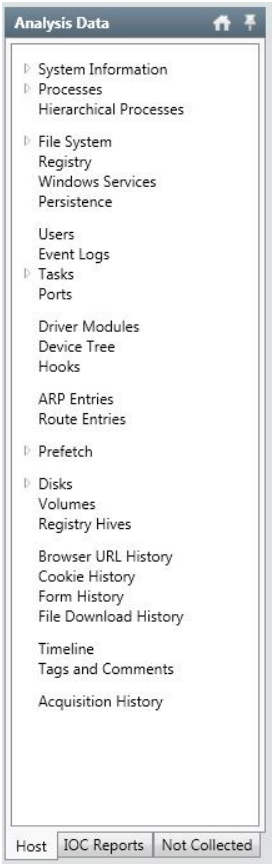
To load a previously saved analysis session, do one of the following:

- Select the analysis session under **Recent Analysis Sessions** on the home screen if listed.
- Select **Open Analysis** on the home screen and locate and select the analysis session.
- Select **Open a Saved Analysis** from the menu and locate and select the analysis session.

# Analysis Data

In an analysis session, Redline automatically groups data by types, such as processes or users, and creates views to help you spot potential areas of compromise. For example, Redline searches the data for executed processes and creates a process view listing, which includes MD5 hash and digital signature information.

The data types available for analysis depend upon the data in the analysis session.

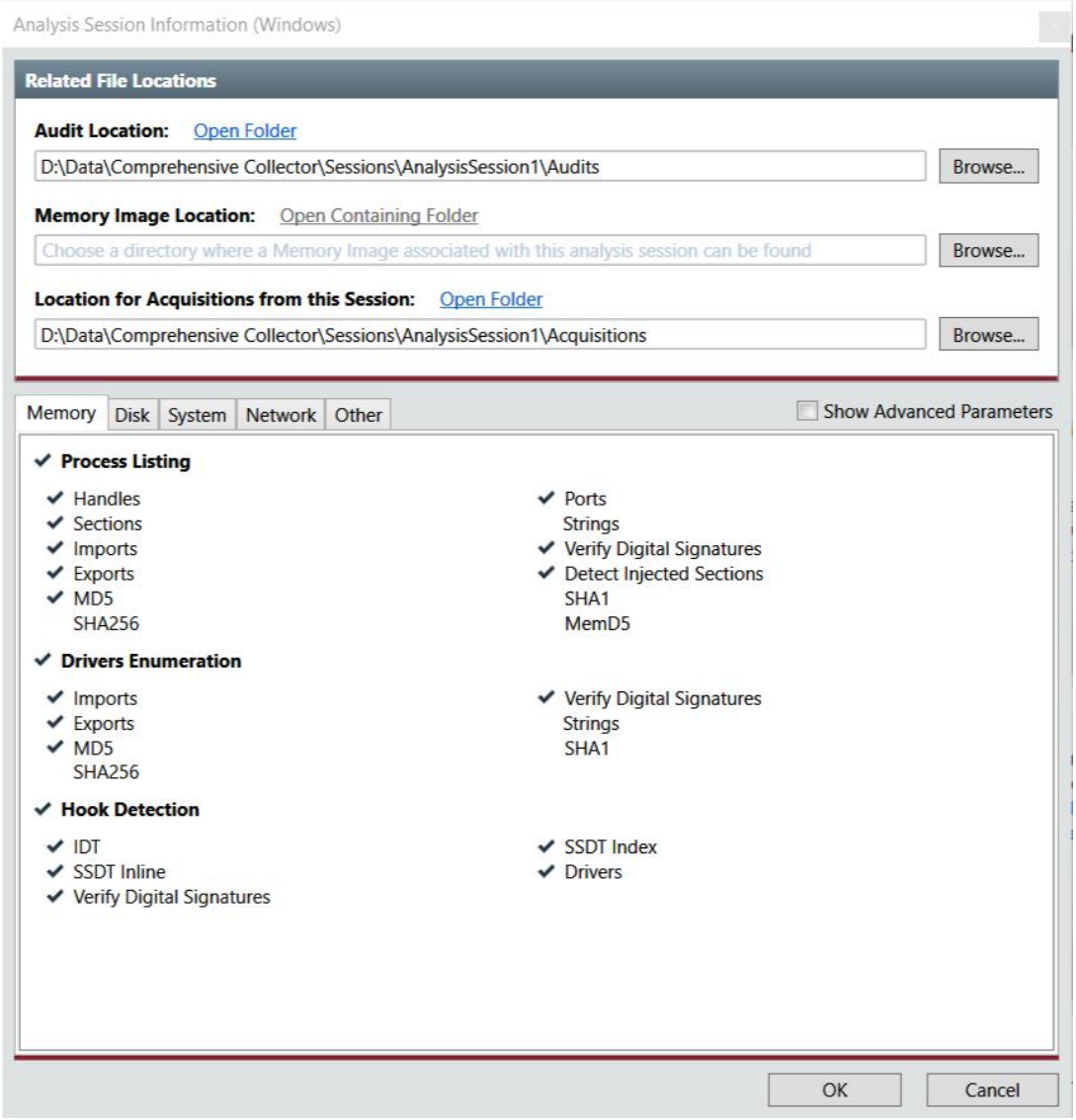



To view a data type, select it on the Analysis Data window's Host tab in an open analysis session. For more information on ways to view data, see Table and Details Views on page 62.

Pictured to the left: Host tab of Analysis Data window for data collected by a Redline Comprehensive Collector on Windows.

# Session Information

To view what data was collected for the analysis session and related file locations, select **Session Information** from the menu to open the Analysis Session Information window. The title of this window also indicates the platform where the data was collected.




Analysis Session Information window.

You can configure the audit and image memory locations and location for acquisitions on the Analysis Session Information window for the current analysis session only. The global default values for acquisitions locations are configured on the Default File Locations on the Redline Options window. See Default Acquisition Locations on page 83 for more information.

# Data Not Collected

Redline displays analysis session data that it cannot parse on the Analysis Data window's **Not Collected** tab.

Analysis failures can be caused by the following:

- Configuration of the Redline Collector script. To view the script options selected, see the Analysis Session Information window. See Session Information on page 30 for more information.
- Configuration of the FireEye Endpoint Threat Prevention Platform (HX) Triage Collection
- Limitations of a third-party memory capture utility
- No data available to collect

# System Information

 Platform support: Windows, OS X, Linux

System information includes machine, BIOS (Windows only), operating system information, and the user account used to collect the data (e.g., run the Redline Collector).

To view system information, select **System Information** on the Analysis Data window's Host tab.

# Network Adapters

 Platform support: Windows, OS X, Linux

Information about network adapters includes the adapter name, dynamic host configuration protocol (DHCP) lease, media access control (MAC) address, internet protocol (IP) information, IP gateways, and DCHP servers.

To view information about network adapters, select **Network Adapters** under **System Information** on the Analysis Data window's Host tab.

# Processes and Their Attributes

 Platform support: Windows, OS X, Linux

Redline displays information about the running processes at the time of data collection, including:

- Process name
- Parent process
- Username
- Path
- Time started and elapsed
- Signature information (Windows and OS X only)

To view information about processes, select **Processes** under the Analysis Data window's Host tab.

To see what running processes started other processes, click **Hierarchical Processes** under **Processes**.

Review all processes listed under iexplore.exe and other browsers; these are usually processes started by the user. Look for processes that are not usually spawned by the parent under which they are listed. Check the arguments for anything that looks out of the ordinary.

## Handles

 Platform support: Windows only

A handle is a connection from a process to an object or resource in a Windows operating system. Operating systems use handles to reference internal objects such as files, registry keys, and other resources. Handle types are defined for each Windows version, but there are common names across most versions.

Reviewing handles can tell you if a process uses the network and if it has any open files (such as log files for sniffers or keystroke loggers) as well as the security context in which the process is running.

To view handles in Redline, select **Handles** under **Processes** on the Analysis Data window's Host tab.

Handles are filtered into the following common handle types: file, directory, processes, registry key, semaphore, mutant, event, and section.

## Memory Sections

 Platform support: Windows

Redline displays the memory sections that comprise each running process.

Examine unsigned memory sections used by few processes. Legitimate dynamic link libraries (DLLs) are typically used by many processes, and system DLLs are usually signed.

To view memory sections, click **Memory Sections** under **Processes** on the Analysis Data window's Host tab.

Redline breaks the memory sections into the following filters:

- **Injected memory**
- **Named sections only**

## Strings

Platform support: Windows

Redline displays information about captured strings. When creating any type of Redline Collector, by default, strings are not captured. To enable string collection, check **Strings** on the **Memory** tab on the View and Edit Your Script window. See Memory Options in Script on page 11 for more information.

To view strings, click **Strings** under **Processes** on the Analysis Data window's Host tab.

## Ports

Platform support: Windows

Malware often initiates outbound connections to command and control (C2) servers or listens on a port for incoming connections. Review ports and connections for unusual or unexpected source or destination ports and addresses, especially from what appears to be system processes.

To view ports, click **Ports** under **Processes** on the Analysis Data window's Host tab.

Redline filters ports by:

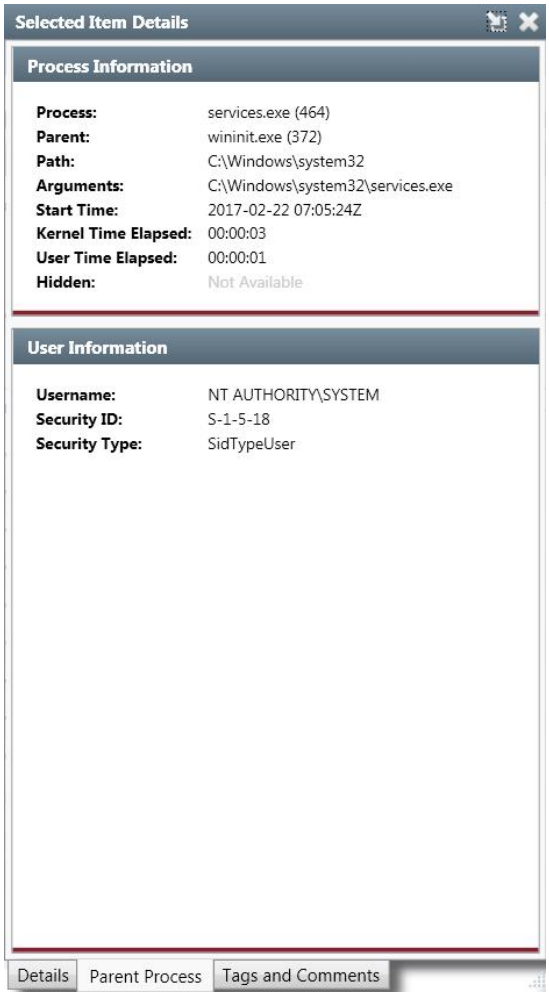
- **Listening ports.** Review listening ports for unknown ports in a listening state and confirm known processes are listening only on ports typical in your environment.
- **Established ports.** Review established ports for outbound connections to IPs in suspicious locations and look for communication on suspicious or nonstandard ports.

Network ports here are only network ports found within process memory space. For information about network ports used by Windows API calls, see **Ports** on the Analysis Data window's Host tab.

# Parent Process Tab

Use the **Parent Process** tab to view process information. The **Parent Process** tab appears at the bottom of the **Selected Item Details** pane.




The **Selected Item Details** pane displays the following information:

- **Process Information**—This area contains information about the process you selected to view. This includes the process name, the parent process name, the path the process uses, the arguments the process uses, the start time, the elapsed kernel time, the elapsed user time, and the state of the process.
- **User Information**—This area contains information about the user of the process. This includes the users name, the security identification number, and the security type.

## Viewing Parent Process Information

1. In the Redline user interface in the **Analyze Data** area, click the appropriate link that points to the session you want to view.

   The **Timeline Configuration** pane appears and the **Alerts** tab is selected..
2. Click the **Fields** button at the bottom of the **Timeline Configuration** pane.
3. Select the **Deselect All** check box at the top of the pane.
4. Select a process agent event.
5. In the process agent events list on the right, select a process agent event instance.
6. Click the **Show Details** link on the bottom of the pane.

   The **Selected Item Details** pane appears.
7. Click the **Parent Process** tab.

   The parent proces information appears in the **Selected Item Details** pane.

# Files and Their Attributes

 Platform support: Windows, OS X, Linux

Redline displays file attributes, such as file metadata, file hashes, timestamps, user information, file path, and digital signatures. For Windows, it also shows specific lists for the following:

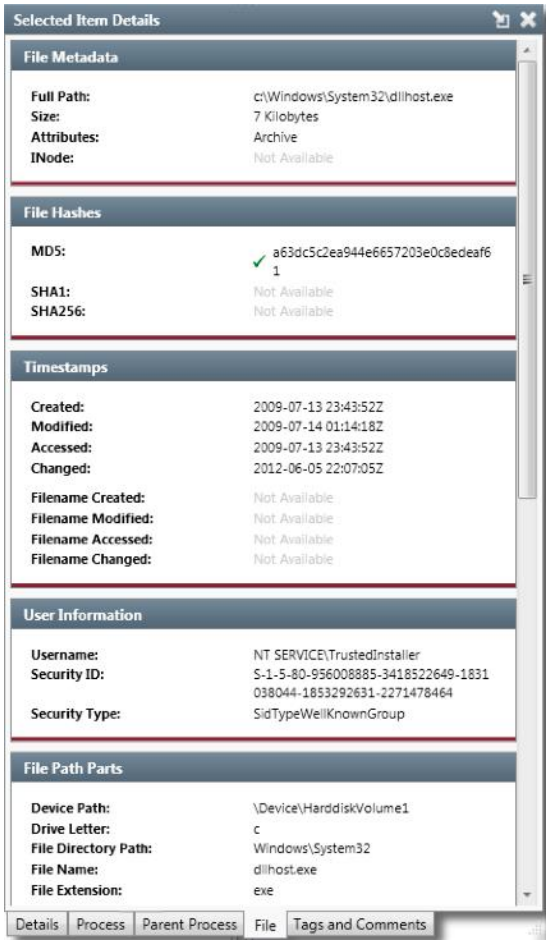
- **Imports**
- **Exports**
- **Strings**
- **Alternate Data Streams**. Attackers often use alternate data streams to hide files from Windows Explorer. However, streams are not necessarily malicious. Windows uses alternate data streams to store legitimate information, such as Zone Identifier information for downloaded files, and to address Windows/Linux compatibility issues.
- **Program Executable (PE) information** as well as version information. Any executable file regardless of its extension has PE header information. Review files that have PE information and an extension that is not typical of an executable (such a .txt).
- **Resource Data**

To view files and their attributes, click **File System** on the Analysis Data window's Host tab.

You can select nodes to limit the display in the table view. On the Directory Tree tab on the Filters window, select the node. The **Apply Selections Recursively** option determines whether subnodes are included automatically (selecting a node selects all its subnodes) or independently (selecting a node does not select all its subnodes). Right-click a tree node to toggle the node and all its subnodes.

# File Details

When you click the **File** tab, the **Selected Item Details** pane displays. You use this pane to view information about the file that was audited.




The **Selected Item Details** pane displays the following information:

- **File Metadata**—Information about the file metadata. This includes the full path, the file size, the attributes, and the iNode (Windows only).

- **File Hashes**—Information about the hashes. This includes the MD5 sum, SHA1 sum, and the SHA256 sum.
- **Timestamps**—Information about the time stamps. This includes the date the file was created, the file was modified, the date the file was accessed, and the date the file was changed. For Windows, it also includes the date the file name was created, the date the file name was modified, the date the file name was accessed, and the date the file name was changed.
- **User Information**—This area contains information about the user of the audits. This includes the users name, the security identification number, and the security type.
- **User Groups (OS X and Linux)**—This area contains the group name the user belongs to, group ID, and group permissions.
- **File Path Parts**—This area contains the names of the parts of the file path that is used for audits. This includes the drive path (Windows only), the drive letter (Windows only), the file directory path, the file name, and the file extension.
- **PEInfo (Windows only)**—This area contains information about the Windows OS executable format and how it is loaded into memory. This includes the PE type, the peak entropy, and the peak code entropy.
- **Advanced PEInfo (Windows only)**—This area contains advanced information about the Windows OS executable format.sub-system type, the base address, the PE time stamp, the number of extraneous bytes, the EP jump code depth, EP jump code op-codes, the PE file raw checksum, the PE file API checksum, and thePE file computed API checksum.
- **Digital Signature (Windows and OS X)**—This area contains information about the certificate. This includes does the signature exist and is it verified. It also includes a description of the signature, the certificate issuer, and the subject of the certificate.
- **Exports Information (Windows only)**—This area contains information about the exports associated with a process. This includes the DLL name, the exports time stamp, the number of functions, and the number of names.

## Viewing File Information

1. In the Redline user interface in the **Analyze Data** area, click the appropriate link that points to the session you want to view.

   The **Timeline Configuration** pane appears and the **Alerts** tab is selected..
2. Click the **Fields** button at the bottom of the **Timeline Configuration** pane.
3. Select the **Deselect All** check box at the top of the pane.
4. Select a process agent event.
5. In the process agent events list on the right, select a process agent event instance.

6. Click the **Show Details** link on the bottom of the pane.

   The **Selected Item Details** pane appears.

7. Click the **File** tab.

   The file details appear in the **Selected Item Details** pane.

# Registry

Platform support: Windows

Redline displays registry information, such as user information and key values, for registry entries.

To view registry information, click **Registry** on the Analysis Data window's Host tab.

You can select nodes to limit the display in the table view. On the Directory Tree tab on the Filters window, select the node. The **Apply Selections Recursively** option determines whether subnodes are included automatically (selecting a node selects all its subnodes) or independently (selecting a node does not select all its subnodes). Right-click a tree node to toggle the node and all its subnodes.

The Registry Modified timestamp is not a definite indication that a specific value was changed. This timestamp indicates a value within the parent key was changed. Redline propagates the registry modified timestamp down to all registry values to facilitate analysis based on time.

# Services

Platform support: Windows, OS X

Redline displays the services known to the host and information about them such as status (e.g., stopped or running) as well as digital signatures and hashes.

To view Windows services, click **Windows Services**(for Windows) or **Services**(for OS X daemons) on the Analysis Data window's Host tab.

Attackers often install backdoors as a service to attain persistence and ensure that the malware restarts when the compromised computer is restarted. Often, an attacker will make a small change to an existing service's name so it will look very similar to what you would expect. For example, the service name would have an "m" instead of "rn" as expected.

For Windows, if you know that a benign service name is supposed to be associated with a specific descriptive name, check the descriptive name of other services with the same or similar service name. Any other descriptive name showing up with that service name is suspect.

# Persistence Mechanisms

 Platform support: Windows, OS X

Redline displays persistence mechanisms discovered on a host along with the associated files, services, and registry entries for each one.

To view persistence mechanisms, click **Persistence** on the Analysis Data window's Host tab.

Review persistence mechanisms to identify how a potential compromise maintains its presence.

# Quarantine Events

 Platform support: OS X

Mac OS X keeps a log of all downloaded files. Files are added to the log even if you are using "private" browsing in Safari or "incognito" in Google Chrome. This log is not cleared even if the browser downloads information gets cleared.

To view a list of downloaded files, click **Quarantine Events** on the Analysis Data window's Host tab. Review downloaded files for potential threats.

# Agent Events

 Platform support: Windows, OS X, Linux

For analysis sessions with an HX Triage Collection or MIR audit data, Redline displays agent events.

To view agent events, click **Agent Events** on the Analysis Data window's Host tab.

Under agent events, Redline also displays the following event types:

- **File write (Windows and OS X).** File write events occur any time a file is written to. These events attempt to group all writes to a single file within 15 seconds into a single event. Additional file write event data includes the MD5 and the first bytes from the lowest offset that was written in the file.
- **Registry key (Windows only).** Registry key events occur whenever a registry key or key value from a preconfigured list of keys commonly used for persistence is modified. Additional registry key event data includes the key value type and the actual value to which the key was changed.
- **IP address change (Windows and OS X).** IP address change events occur whenever the IP address of the host system is changed. Additional IP address change event data includes the date and time generated and the new address.
- **Network connection.** Network connection events occur any time the host computer establishes a network connection. In the case of connectionless protocols (i.e., ICMP), an event is captured any time data is transferred. Additional network connection event data includes generated date and time, PID, process, local and remote IP, local and remote ports, and protocol.
- **Image load (Windows and OS X).** Image load events occur whenever an executable or linked library is loaded into memory. Additional image load events data includes generate date and time, PID, process, full path, and user name. Investigate these events to determine if a specific process or library was started on a host computer.
- **DNS lookup (Windows and OS X).** DNS lookup events occur whenever the host computer makes a DNS request. Additional DNS lookup event data includes generated date and time, host name, PID, and process.
- **Process Events**. A process event occurs when a process starts and again when a process ends. An agent will also generate a process event if it starts while a process is running.
- **Exploit Events (Windows and OS X).** An exploit event occurs when an agent detects a specific malware method like heap spraying. Heap spraying refers to the attempt to insert software into a predetermined location in a vulnerable browser.
- **URL Monitor Events (Windows and OS X).** A URL monitor events occur whenever a URL is accessed.

# Users

Platform support: Windows and OS X

Redline displays different user information details based on the underlying OS. The common user information is your username, your last login date and time, the group name that you belong to, and the home directory.

To view a list of users, click **Users** on the Analysis Data window's Host tab.

If the potentially compromised host belongs to an organization that has conventions for naming users (such as first initial and last name) then check the user names for any that appear to not follow the convention.

# Groups

 Platform support: OS X

This audit returns all the groups present in a Mac OS X host. The following information is returned:

- Group Name
- Full Name
- User List
- Group ID

To view the groups, click **Groups** on the Analysis Data window's Host tab.

# Syslog

 Platform support: OS X

Mac hosts collect numerous amounts of log files containing all sorts of information about processes, applications, connectivity, drivers, etc. This information can be very useful to security professionals in their quest for finding evil.

To view system logs, click **Syslog** on the Analysis Data window's Host tab.

# Tasks and Their Attributes

 Platform support: Windows, OS X, Linux

Redline displays a scheduled tasks list that includes task information, file hashes, digital signatures, application, and schedule information.

To view scheduled tasks, click **Tasks** on the Analysis Data window's Host tab.

Each task may have a list of triggers (Windows and OS X only) or actions (Windows only), which you can view in the details view. Click **Triggers** or **Actions** under Tasks.

# Network Ports

 Platform support: Windows,OS X, Linux

Malware often communicates through network ports, either listening for commands or making outbound connections. Check network port lists for unusual or unexpected port connections.

To view network ports enumerated by the operating system, click **Ports** on the Analysis Data window's Host tab.

Redline filters ports by:

- **Listening ports.** Review unknown ports in a listening state and confirm known processes are listening only on ports typical in your environment.
- **Established ports.** Review established ports for outbound connections to IPs in suspicious locations and look for communication on suspicious or nonstandard ports.

This view lists network ports that were found using OS API calls. For network ports found in process memory space, see **Ports** under **Processes** on the Analysis Data window's Host tab (Windows only).

## Event Logs

 Platform support: Windows

Redline displays an event logs list that includes the application that generated the log, log's message, user, timestamp when log was generated, source, and type.

To view event logs, click **Event Logs** on the Analysis Data window's Host tab.

# Kernel Modules

 Platform support: Linux

This audit shows a list of loaded kernel modules.

To view enumerated kernel modules, click **Kernel Modules** on the Analysis Data window's Host tab.

# Driver Modules

Platform support: Windows

Redline lists driver modules information including the path, name, base, size, and address.

To view driver modules, click **Driver Modules** on the Analysis Data window's Host tab.

# Device Tree

Platform support: Windows

Malware authors sometimes use device driver layering to intercept data. They may place a keylogger, file logger, or other data-stealing routine on top of a system device driver. However, many device driver layers are legitimate routines providing common filtering tasks.

To view devices, click **Device Tree** on the Analysis Data window's Host tab.

In particular, look at:

- **Ntfs.** The System Restore driver is often layered on \Ntfs; other drivers may indicate a file filter driver, which can hide files and directories or filter file content.
- **Kbdclass.** Keylogging malware is often layered on \Kbdclass.

# Hooks

Platform support: Windows (limited support for Windows 10)

Hooks are subroutines injected into the usual system function mechanisms, allowing a third party to monitor and modify data as it moves from source to destination. Rootkits often use hooks in the kernel to implement hiding functions.

To view hooks inserted into the operating system, click **Hooks** on the Analysis Data window's Host tab.

Redline filters hooks as follows:

- **IDT hooks.** The Interrupt Descriptor Table (IDT) is a data structure used to implement an interrupt vector table. The processor uses IDT to determine the correct response to interrupts and exceptions. IDT hooks are usually malicious.
- **SSDT hooks.** The System Service Dispatch Table (SSDT) is an internal dispatch table within Microsoft Windows. Hooking SSDT calls is often used as a technique in both Windows rootkits and antivirus software.
- **IRP hooks.** I/O request packets (IRPs) are kernel mode structures used by Windows Driver Model (WDM) device drivers to communicate with each other and with the operating system.

# DNS Entries

 Platform support: Windows, OS X

Redline displays information from Domain Name System (DNS) records stored in the computer's in-memory DNS cache table, which is maintained by the DNS Client Services Windows component. The information displayed includes the host, record name, time to live, data length, flags, and record type.

To view DNS entries, click **DNS Entries** on the Analysis Data window's Host tab.

# ARP Entries

 Platform support: Windows, OS X

A computer maintains an Address Resolution Protocol (ARP) table for basic network and traffic routing. Redline displays information about entries in the IPv4 and IPv6 ARP tables. The information displayed includes physical, IPv4, and IPv6 addresses, interface type (static or dynamic), cache type, last unreachable and reachable dates, and if it is a router.

To view ARP entries, click **ARP Entries** on the Analysis Data window's Host tab.

# Route Entries

 Platform support: Windows, OS X

Redline displays network routing entries including interface, destination, gateway, protocol, route type (indirect or direct), netmask, preferred and valid lifetimes, and origin. The list also shows if the address is autoconfigured, and if the entry is IPv6, loopback, and published.

To view route entries, click **Route Entries** on the Analysis Data window's Host tab.

# System Restore

 Platform support: Windows (not supported on Windows 10)

Window's system restore monitors critical operating system files and other various application files and provides a simple and immediate recovery to various points in time through the creation of restore points.

Redline displays information about Windows restore points such as change log file name, created date, change event, change log entry type, original file name, restore point name, and file attributes.

To view Windows restore points, click **System Restore** under the Analysis Data window's Host tab.

System restore can sometimes show evidence of a compromise, such as files that were used during a compromise and later deleted.

# Prefetch

 Platform support: Windows

Windows uses prefetch to maintain a reference to recently executed code. This reference is stored in the %SYSTEMROOT%\Prefetch directory.

Redline lists the prefetch cache contents. For each application name, Redline shows the path, last run and created dates and times, prefetch cache, size, and number of times executed.

To view prefetch cache contents, click **Prefetch** on the Analysis Data window's Host tab.

If you suspect that an attacker has deleted files, review the accessed files of any known bad processes to find references to files that were deleted. To view the files accessed by applications in the prefetch cache, click **Accessed Files** under Prefetch.

To view the volume name, type, device path, and other information about volumes referenced in the prefetch cache, click **Prefetch Volumes** under Prefetch.

# Disks

 Platform support: Windows, OS X

Redline lists the disk name and its size for Windows and OS X. Additionally for OS X, Redline lists disk type, connection, and device path.

To view disk information, click **Disks** on the Analysis Data window's Host tab.

For partition number, length, offset, and type, click **Partitions** under Disks.

# Volumes

 Platform support: Windows, OS X

Redline lists the volume name, device path, and file system name for volumes for all supported OSes. All other attributes are OS-dependent.

To view volume information, click **Volume** on the Analysis Data window's Host tab.

# Registry Hives

 Platform support: Windows

Redline displays the hive name and key for host registry hives.

To view registry hives, click **Registry Hives** on the Analysis Data window's Host tab.

# Browser URL History

 Platform support: Windows, OS X

Redline displays information about uniform resource locators (URLs) viewed using Microsoft Internet Explorer, Firefox, Chrome, and Safari, including host name, URL, page title, browser name and version, visit from, visit count, first (Windows only) and last visit dates, and first bookmark date.

To view the URL history, click **Browser URL History** on the Analysis Data window's Host tab.

Redline has the following filters for browser URL history records:

- **All.** Shows all URLs.
- **Redirects.** Shows all URLs for visit types that were a variation of a redirect, which is often used to bounce a user from site to site before finally reaching a malware staging server.
- **Visit from.** Shows all URLs generated after the user first viewed another page, which can be valuable information in determining a sequence of events.
- **Visited once.** Shows only URLs that had exactly one visit; rarely visited sites are an indication of suspicious activity.
- **Visited bookmarked URLs.** Shows only URLs that were visited by the user selecting a URL from the browser's bookmarks. Bookmarks may indicate that the user frequently visits a website and trusts it.
- **Typed URLs.** Shows only URLs that the user visited by typing the address into the browser, which implies that the user was aware of the site.
- **Hidden visits.** Shows all URLs accessed without the user's direct knowledge, including hidden IFrames often used by embedded ad sites which could be potentially infected with malicious obfuscated JavaScript.
- **Forms.** Shows all URLs on which the user entered data.

# Cookie History

 Platform support: Windows, OS X

Cookies are a means for a website to store information on a user's computer for later retrieval. They are most commonly used to track login and session information about a user's visit to a website. You can use cookies as a resource for analyzing certain types of browser-based activity.

Redline lists browser cookies from Microsoft Internet Explorer, Firefox, Chrome, and Safari, including the cookie's name, path, value, and flags; host name; browser version; profile; user name; creation, expiration, last accessed, and last modified dates; file name; and file path.

To view the cookie history, click **Cookie History** on the Analysis Data window's Host tab.

Redline has the following filters for cookie history records:

- **All.** Shows all cookies.
- **Secure cookies.** Shows only cookies that must be sent over HTTPS, which is an uncommon restriction for cookies and may indicate suspicious activity.
- **HTTP only cookies.** Shows only cookies that are hidden to the application.
- **Cookies with flags.** Shows only cookies that have attribute flags set. Applicable only for Internet Explorer (Windows only).

# Form History

 Platform support: Windows, OS X

Whenever a user enters data on a form, such as a login form on a bank website or even a simple text box like the one on the Google search page, a form history entry is recorded.

Redline lists form data entered into Firefox or Chrome, including browser name and version, user name, profile, form field name and value, form type, creation and last used dates, encryption password and type, password, user field name, and number of times used.

To view the form history, click **Form History** on the Analysis Data window's Host tab.

Redline has the following filters for form history records:

- **All.** Shows all forms submitted by a browser.
- **Login.** Shows login type forms.
- **Normal.** Shows all forms except login type forms.

# File Download History

 Platform support: Windows, OS X

Downloaded files are a common mechanism for attackers to use to gain access to a computer. Users are likely to download files with names of interest (such as "birthday wishes"). Many users are aware that .exe files should not be downloaded and run. However, if a file has a ".txt" or another similar indication of a file type in the file name and the user has file extensions turned off in their Windows Explorer, the user may open the file not realizing that the actual extension is .exe and the file is an executable.

Redline lists files downloaded using Microsoft Internet Explorer, Firefox, Chrome, and Safari, including source URL, target directory, browser name and version, bytes downloaded, start and end date, download type (Windows only), file name, user name,

profile, cache flags (Windows only), cache hit count (Windows only), and last accessed checked and modified dates (both Windows only).

To view the file download history, click **File Download History** on the Analysis Data window's Host tab.

Redline has the following filters for file download history records:

- **All.** Shows all files that were both manually or automatically downloaded.
- **Plain text.** Shows downloaded files that have well-known plain text extensions (i.e., .txt, .html, .htm, .xml, .css, and .js).
- **Images.** Shows downloaded image files (i.e., .jpeg, .jpg, .bmp, .gif, .png, .tioff, .ico, and .ani).
- **Media.** Shows downloaded files that have common audio and video format extensions (i.e., .swf, .swa, .mov, .mpeg, .mp3, .mpa, .mp4, .wma, .wav, and .midi).
- **PDFs.** Shows downloaded files that have the portable document form (.pdf) extension.
- **IE leak records (Windows only).** Shows only Internet Explorer LEAK records, which indicate a cached file was in use when cache cleanup was being performed and thus it was not removed from the system.
- **IE redirect records (Windows only).** Shows only Internet Explorer redirect records, which indicate the visit was a result of a redirect operation.
- **Manual downloads.** Shows all manual downloads (i.e., any file such as an installer that was not automatically downloaded as part of viewing the page).
- **Saved to non-standard locations (Windows only).** Shows files that were downloaded to non-standard locations, such as to program file or system directories.
- **Full HTTP header available (Windows only).** Shows files that had the entire HTTP header captured when downloaded.
- **Large than 20 kilobytes.** Shows downloaded files that are larger than 20KB.
- **Incomplete.** Shows any downloads that were not completed for any reason.

# Shell History

Platform support: Linux

Shows command history for the most popular Linux command shells: bash, zsh, and ksh93. This audit assumes default history filename (.bash_history, .zsh_history, .sh_history).

To view the shell history, click **Shell History** on the Analysis Data window's Host tab.

# Login History

 Platform support: Linux

Enumerates user sessions, including currently active, historical, and failed sessions. Note that only interactive sessions are displayed. Non-interactive sessions, like the ones used for SCP or SFTP, are not a part of this audit.

To view the login history, click **Login History** on the Analysis Data window's Host tab.

# Investigation

 IOCs are supported for Windows only

Redline analyzes the data collected from the potentially compromised computer and produces hits against Indicators of Compromise (IOCS).

When reviewing analysis session data in Redline, you can:

- Use table and details views
- Use tags and comments
- Search
- Filter out known good data with a whitelist
- Filter data based on timeline
- Acquire drivers and processes
- Search the web directly for more information
- Export data to a CSV file

# Indicators of Compromise (IOCs)

As part of your investigation, you may want to look for specific artifacts such as files or processes that may indicate a breach. You can use standard Indicators of Compromise (IOCs) as a method of defining those artifacts.

An IOC is an individual characteristic or series of characteristics that, when observed, indicate the presence or execution of specific malware or the use of known attacker methodologies (i.e., attributes of suspicious activity).

## More about IOCs

IOCs are forensic artifacts of an intrusion that have been identified on a host. They comprise logically grouped sets of descriptive terms (called indicator terms) about specific threats.

A simple IOC might look for the signature of specific compromise artifacts. These can be traditional forensic objects, such as MD5 hash values, compile times, file size, name, path locations, registry keys, and so on. More complex IOCs use more advanced forensic

techniques. These IOCs look for data that are harder for attackers to change or artifacts that attackers are more likely to recycle, such as running process components (including process handle names), and imports and exports used by an executable.

Indicators attempting to detect methodology do not focus on specific pieces of forensic evidence. Instead, they focus on the common methods that attackers use. Methodology indicators don't necessarily show a specific instance of a compromise, but they will show the result of tactics repeated by adversaries.

Ultimately, the best IOCs have these properties:

- The IOC identifies only attacker activity.
- The IOC is inexpensive to evaluate — it is typically simple and evaluates information that is less expensive to collect or calculate.
- The IOC is expensive for the attacker to evade. In other words, to evade the IOC the attacker must drastically change tactics, tools, or approach.

IOCs are meant to be shared. They are plain text files, which make them easy to modify and send to others. Mandiant's free editor tool called IOC Editor is available for download at https://www.fireeye.com/services/freeware.html.

For more information about the IOC standard, visit http://openioc.org/.

## Data Analysis with IOCs

Redline can analyze existing data with IOCs. When you select the IOCs that you want to use, Redline reviews the data and provides some preliminary information on the expected results.

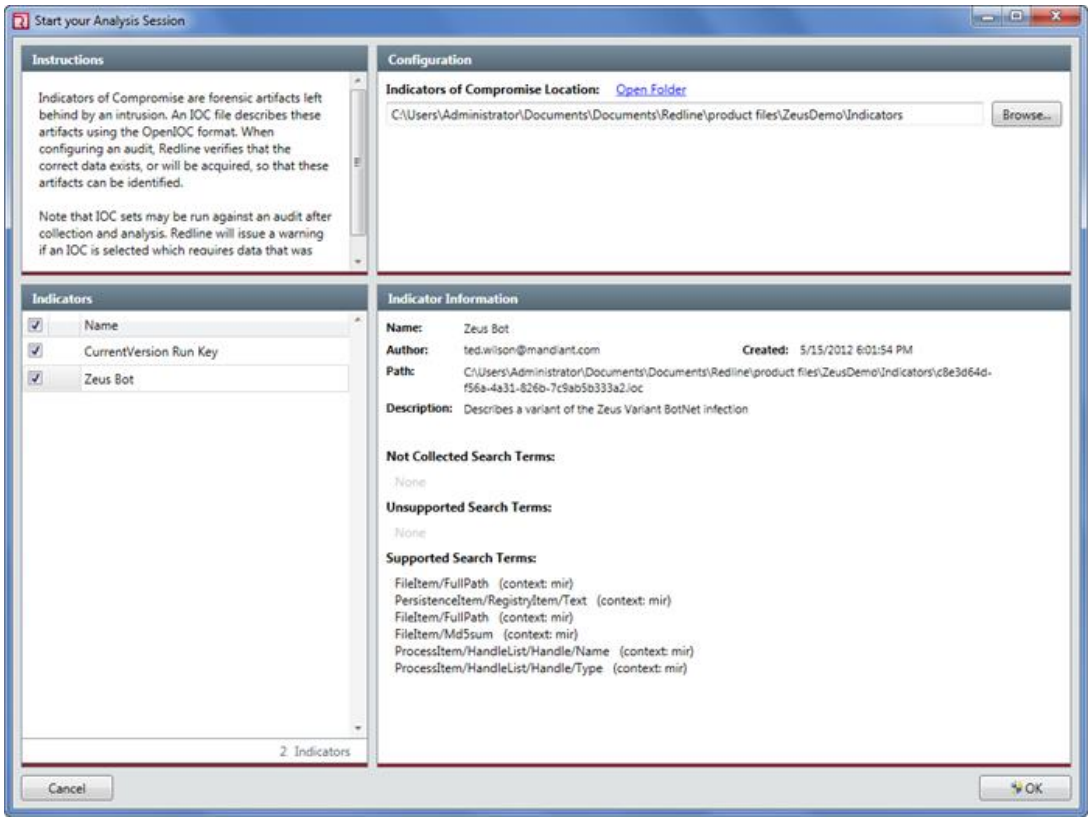
To select IOCs for analysis:

1. Access the IOC configuration window. This window will open when you are configuring an IOC Search Collector (see Configure IOC Search Redline Collector on page 8 for more information); when you open a saved memory file (see Analyze Memory on page 26 for more information); or when you create a new IOC Report (see IOC Reports on page 55 for more information).
2. Click **Browse** next to **Indicators of Compromise Location**.

If you are analyzing existing data collected using an IOC Search Collector, select the same IOCs that you selected when configuring the collector.

3. Select the folder in which the IOC files are located.
4. Click **Open Folder** if you want to view the individual IOCs within the folder (optional).

5. Review the list of indicators. Enable and disable each IOC by checking it. To enable or disable the entire list, select the checkbox at the top of the column. Selecting a column header sorts the list.
6. Select a specific indicator to reveal details about it to the right in the Indicator Information box.




If an IOC is not compatible with Redline, it will be highlighted in the indicators list as follows:

- A warning indicates that Redline will evaluate the IOC, but it may falsely indicate there were no hits (a false negative) due to a lack of collected data or unknown terms.
- An error indicates that Redline cannot evaluate the IOC.

Each indicator shows such detailed information as the name, creation date, description, and information about the search terms as follows:

- Not Collected Search Terms (for analysis of existing data only). Lists terms that Redline cannot hit because the data is missing (e.g., if a Redline Collector was used and the proper options were not enabled in the script).
- Unsupported Search Terms. Lists terms that Redline does not understand. These

search terms will not produce any hits in Redline.

- Supported Search Terms. Lists terms that Redline recognizes and will evaluate.

## IOC Reports

When Redline evaluates data with Indicators of Compromise (IOCs), it creates an IOC Report. Redline can generate an IOC Report when data is imported or any time after an analysis session has been created.

IOC Reports contain the following information:

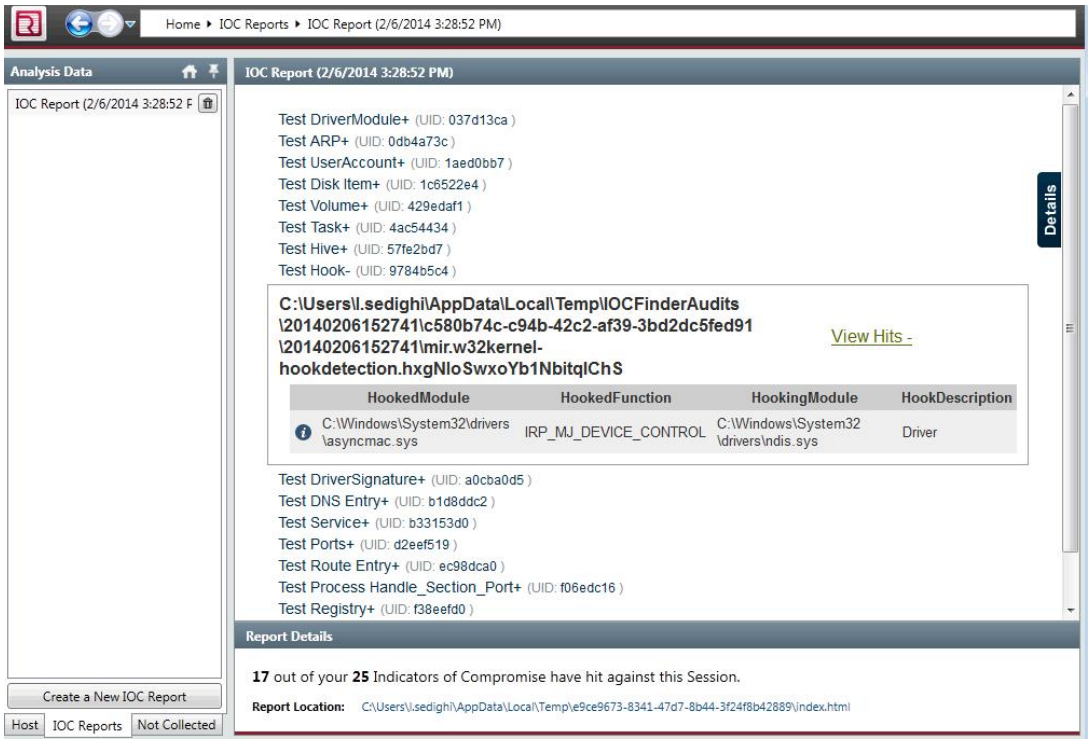
- Details about the IOC, such as definition and author
- Hits associated with each file that corresponds to an IOC
- Detailed information about each hit
- Number of indicators that generated hits
- Location of the IOC Report

To create a new report, click **Create a New IOC Report** on the IOC Reports tab on the Analysis Data window. See Data Analysis with IOCs on page 53 for information on the options in the IOCs configuration window.

When you create the IOC report during your Analysis session, Redline creates an IOC folder at the same level as your .mans file on your computer.

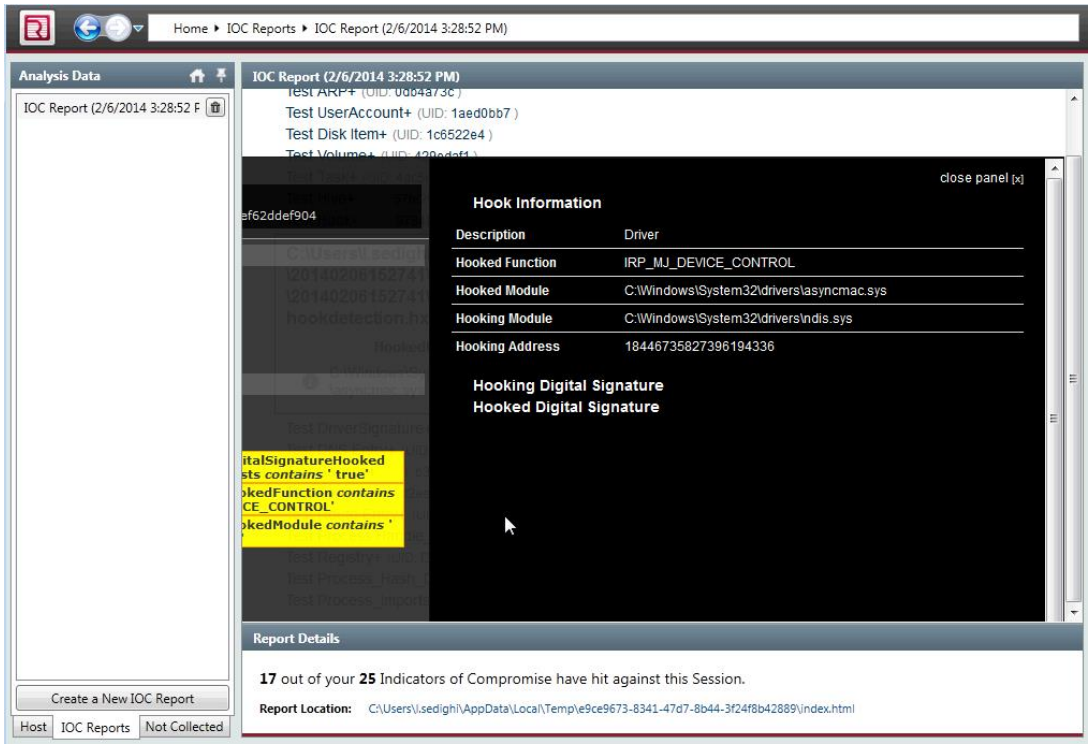
Click the **IOC Reports** tab at the bottom of the Analysis Data window to open IOC Reports. Select an IOC name to display files containing IOC hits. Click the UID to reveal its details.




IOC Report accessed from IOC Reports tab on Analysis Data window

In the IOC file hits, click **View Hits +** to see hits. Select  to display full hit details and, in particular, the IOC terms that were matched by the hit.



Hit details within an IOC Report

Reports are saved as interactive web pages and may be shared by archiving the file folder as a zip file. Click **IOC Report Location** in the Report Details window to open the IOC Report folder.

To remove an IOC Report from the analysis session, click  to the right of the report name in the Analysis Data window.

# Timeline

Timeline is a valuable tool for identifying when a compromise originally occurred, which files were touched, and if (and how) the compromise persists.

Timeline displays events (i.e., all items that have time associated with them) sorted by time. The fidelity of time in Timeline is one second; events that happen within the same second won't necessarily be in the correct sequence order.

With Timeline, you can apply filters to see only events that are associated with specific users and processes. TimeWrinkle and TimeCrunch further filter the list, displaying only those events that happened at or near a specific time of interest, and hiding noisy events that happened at a specific time, respectively.

**Timeline** is an option on the Analysis Data window's Host tab. It displays information using the same views as other options on the Host tab. For more information on views, see Table and Details Views on page 62.

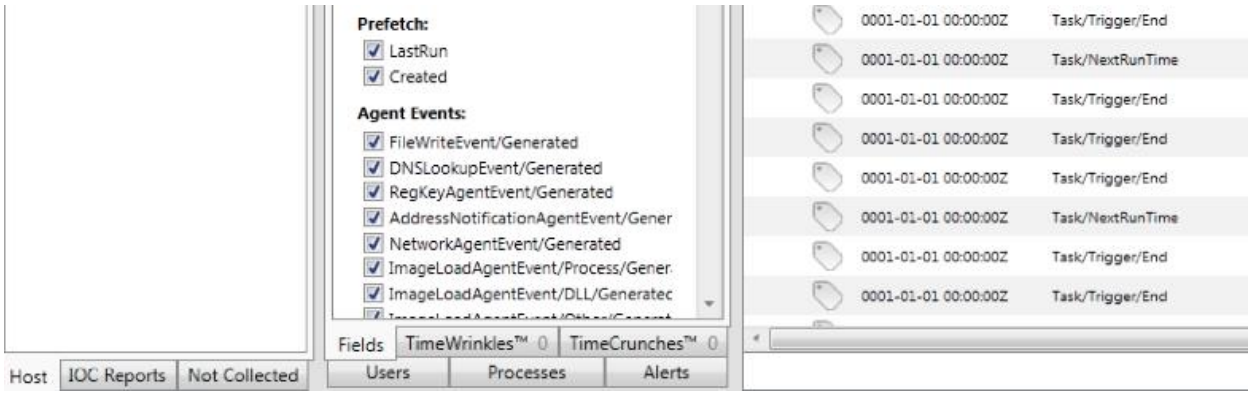
## Timeline Field Filter

Field filters in Timeline are a means of excluding and including entire categories of time-related events from the table view by checking those categories that you care about. For example, you can remove file accessed events, which tend to be very noisy, from the table view so you can focus on other events.

To display only events containing the selected time field, use the options under the **Fields** tab in the Timeline Configuration window. Select any combination of fields.

The fields filter works in conjunction with the user and process filters. For example, if you select **Files Created** on the Fields filter and **Show Only Events Associated** and **JaneDoe** on the Users filter, only files created by JaneDoe are displayed.



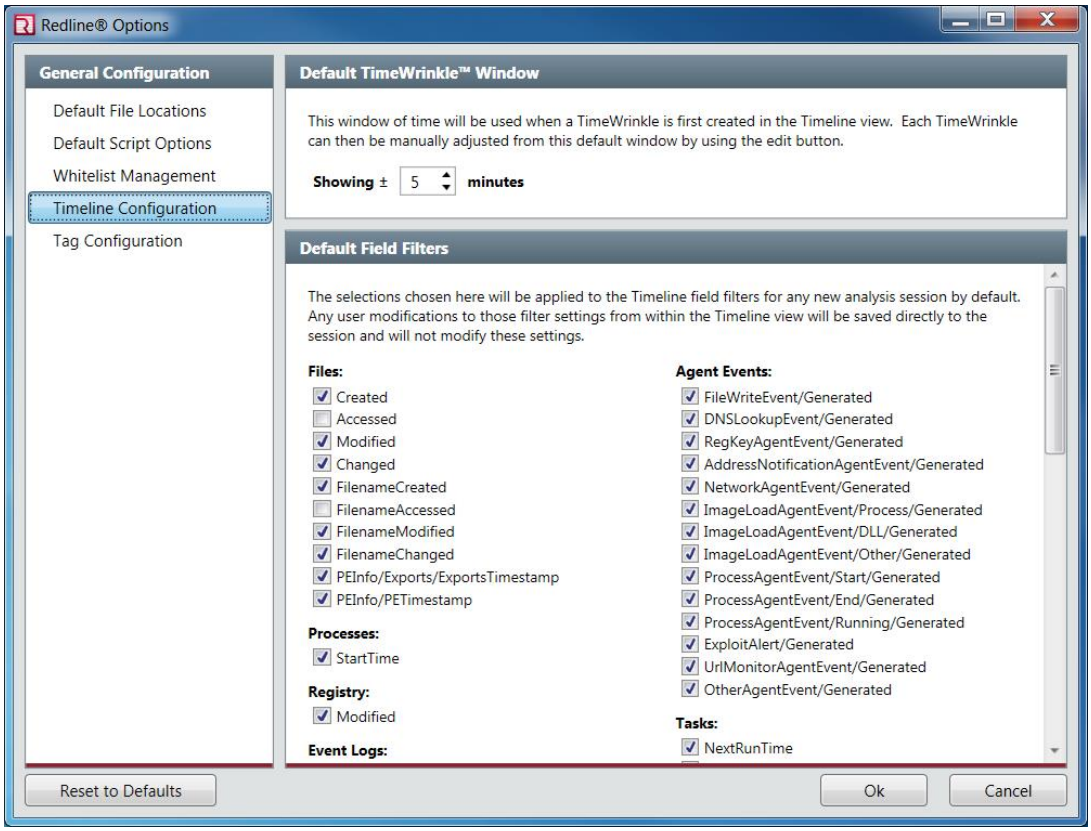

Fields tab on Timeline Configuration window.

Selecting **Show All** displays every event without changing your selections; clearing the checkbox restores the filtered list.

Selecting **Deselect All** clears all fields, resulting in an empty list, and changes the checkbox to Select All. You can select new fields, which automatically clears the Select All checkbox and restores the Deselect All label. Checking **Select All** selects all fields; you can then deselect fields to remove from the list.

If you make any modifications to the field filter settings directly in Timeline view, the updated settings are saved with the analysis session.

The default field filters for all new analysis sessions are set under **Timeline Configuration** in the Redline Options window, which is accessed under the menu.




Timeline Configuration options on Redline Options window.

Any changes you make to the default field filters apply only to new analysis sessions.

## Timeline User Filter

You can opt to display only file, process, registry, event logs, quarantine events, tasks, URL history, file download history, cookie history, and form history events associated with a specific user by using Timeline's user filter. Not all of the listed items are available on each platform.

Set the user filter by doing one of the following:

- Select the **Show Only Events Associated with Selected User** option as well as the user on the **User** tab in the Timeline Configuration window.
- Right-click a specific user-related event on the Timeline table view and select **Show Items Related to User from the Selected Item**. To return to the full listing, clear **Show Only Events Associated with Selected User**.

The user filter works in conjunction with the field filter and process filter.

# Timeline Process Filter

You can opt to display only file, process, registry, event logs, syslog, tasks, URL history, file download history, cookie history, and form history events associated with a specific process by using Timeline's process filter. Not all of the listed items are available on each platform.

Set the process filter by doing one of the following:

- Select the **Show Only Events Associated with Selected Process** option as well as process name on the Process tab in the Timeline Configuration window.
- Right-click a specific process-related event on the Timeline table view and select **Show Items Related to Process from the Selected Item**. To return to the full listing, clear **Show Only Events Associated with Selected Process**.

The process filters works in conjunction with the field filter and user filter.

# TimeWrinkles™

TimeWrinkle provides you the means to filter Timeline view to display only events that occurred in a set of configurable windows of time that match the current fields, users, and process filters.

TimeWrinkle comes in two varieties: custom and item-based.

## Custom TimeWrinkles

If you know the general time when suspicious activity occurred, use a custom TimeWrinkle to restrict the timeline to only events that took place around that time. Click **New Custom TimeWrinkle** on the TimeWrinkle tab in the Timeline Configuration window. You can change the date and time. Click  to save the new TimeWrinkle.


To edit a TimeWrinkle, select the **TimeWrinkle** on the TimeWrinkles tab. Select  and select a new date and time. Click  to save the change. Click  to delete the TimeWrinkle.

## Item-Based TimeWrinkles

If you know something more specific than just the general time when suspicious activity occurred (such file name or MD5 hash), use an item-based TimeWrinkle. Creating an item-

based TimeWrinkle will take a selected item (e.g., file, registry key, or process) and narrow the timeline to events that took place around any of the associated timestamps for that item. Right-click an event in the Timeline table view and click **Add New TimeWrinkle**. A new TimeWrinkle is created around that event using the default amount of time.

To change the default time for TimeWrinkles, set a new time for the **Default TimeWrinkle** option under **Timeline Configuration** on the Redline Options window, which is accessed under the menu. See Timeline Field Filter on page 57 to see the window.

## TimeCrunches™

To reduce data in the Timeline table view, you can trim out a minute's worth of events for a specific field by using a TimeCrunch. A TimeCrunch hides events of the same type that happened within the same minute as the selected event.

The most common example of noisy, irrelevant data is when an antivirus scan updates the files accessed timestamp on a very large number of files in a very short time. When this occurs, the file accessed timestamp will become too noisy to be of investigative use for the window in which the antivirus scan ran. Applying a TimeCrunch excludes a minutes worth of this cluttersome data without losing potentially relevant file accessed timestamps elsewhere in your timeline.

To create a TimeCrunch, do one of the following:

- Right-click an event in the Timeline table view and click **Add New TimeCrunch**. A new TimeCrunch is created that hides all the events of the same type as the one selected during the same minute.
- Click **New Custom TimeCrunch** on the TimeCrunch tab. Select the timestamp and type of event to hide. Click to save the new TimeCrunch.


To edit a TimeCrunch, select **TimeCrunch** on the TimeCrunches tab in the Timeline Configuration window. Select and select a new date and time and event type. Click to save the change. Click to delete the TimeCrunch.

You can create multiple TimeCrunches, hiding several spans of noisy data. You can use also TimeCrunches in conjunction with TimeWrinkles.

# Table and Details Views

Redline has two view types:

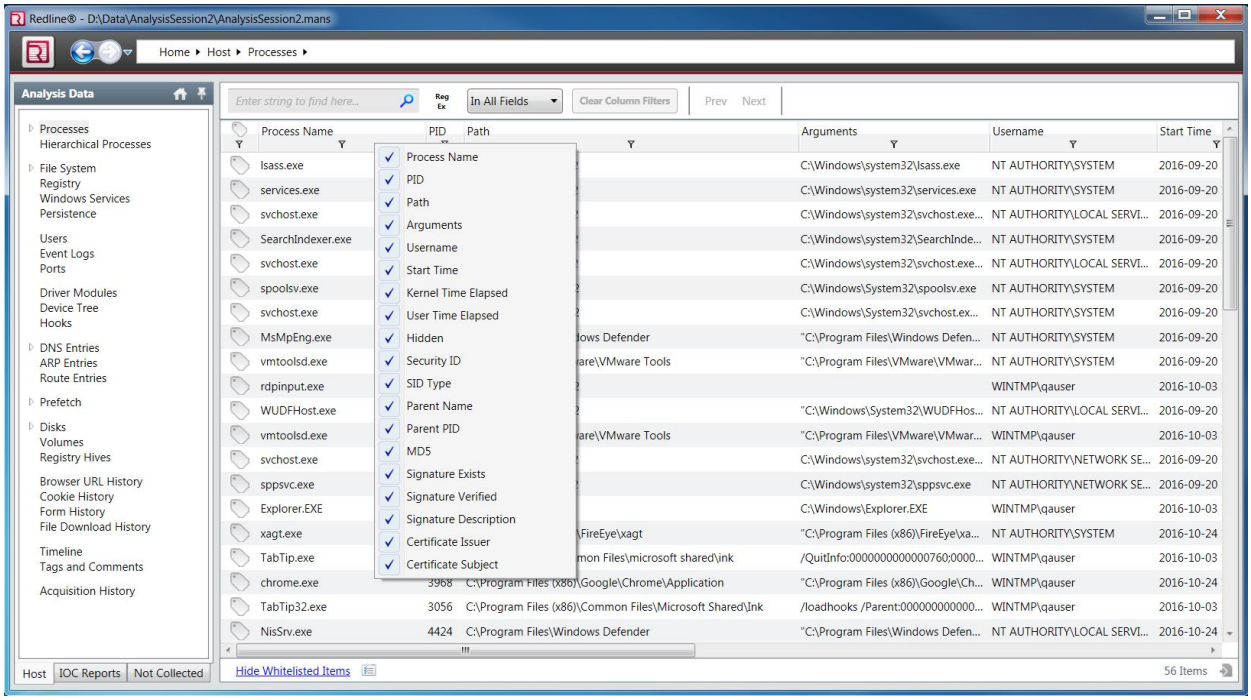
- Table views
- Details views

For areas that have multiple attributes or components, such as processes, tasks, and disks, Redline displays a global list of all sub-items and their related parents. For detailed information about a specific item and its attributes, open its details view.

## Table Views

All data displayed on the Analysis Data window's Host tab, except system information and network adapters, is displayed as a table.

The table view behaves like a typical table. Click the heading to sort the list. Drag and drop columns to arrange the order in which the columns are displayed. Right-click on the table headings to select columns displayed.




Process table view displaying options for columns

Right-click an item in the table view for additional options (such as select all, copy, copy with headers, or tags). See Copy on page 81 and Tags and Comments on page 69 for more information.

# Details Views

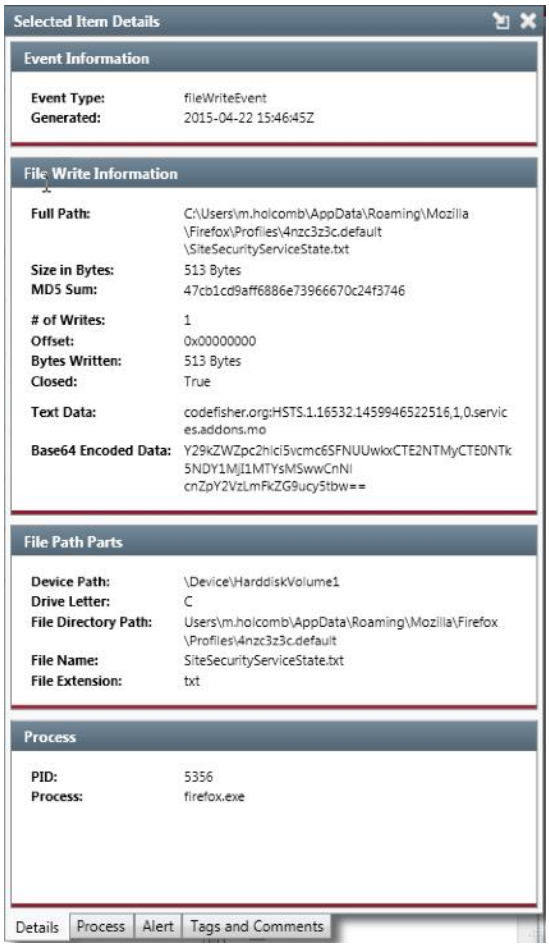
Double-click any row in the table view to open the details view to fill the whole right pane.

To open a separate details pane that can be docked to the right side of the table, click Show Details at the bottom of the table view. This window can also be torn off to become its own window; just click .

Tabs along the bottom of the details view display various categories of information related to the selection. For example, in a process details view, ports are displayed under the **Ports** tab.

# Alerts Details

All alerts that are displayed in the **Timeline Configuration** pane are hyperlinks. You click any alert hyperlink to view a list of event instances. You click the **Details** tab to view information about the event instance.




The **Selected Item Details** pane displays the following information:

- **Event Information**—Information about the alert you selected to view. This includes the event type, and the date and time when the alert was generated.
- **File Write Information**—Information about the results of the file search. This includes the full path, the file size, the MD5 sum, the number of writes, the offset, the number of bytes written, the state of the file, the malicious text that was found, and the Base64 encoded data.
- **File Path Parts**—Information about the parts of the file path that is used in the audit. This includes the drive path, the drive letter, the file directory path, the file name, and the file extension.
- **Process**—Information about the process that triggered the event. This includes the process ID and the process type.

## Viewing Alert Details

1. In the Redline user interface in the **Analyze Data** area, click the appropriate link that points to the session you want to view.

   If there are alerts in the session, the **Timeline Configuration** pane appears and the **Alerts** tab is selected. If there are no alerts in the session, the Start Your Investigation page displays.
2. In the **Timeline Configuration** pane, click on an alert.
3. Click the **Show Details** link on the bottom of the pane.
4. Click the **Details** tab.

   The alert details appear in the **Alert** pane.

# Alerts Details Using the View in HX Button

Use the **View in HX** buttons to view information in real time on an HX Series appliance. To use the **View in HX** buttons, the URL of your HX Series appliance must be included in your .mans file.

The contents of this pane varies. There can be multiple buttons, two for each alert. Each button will expose a different view. The **View in HX** buttons appear in the **Selected Item Details** pane.


In the example shown above, there are four buttons:

- The topmost button—Opens an HX pane that displays alert details about a file write event because the file path contains the suspicious word **meg**.
- The second button down—Opens an HX pane that displays indicator details for the **meg** alert.
- The third button down—Opens an HX pane that displays alert details about a file write event because file path contains the suspicious word **.txt**.
- The fourth button down—Opens an HX pane that displays indicator details for the **.txt** alert.

## Viewing Alerts on the HX Series Appliance

1. In the Redline user interface in the **Analyze Data** area, click the appropriate link that points to the session you want to view.

   The **Timeline Configuration** pane appears and the **Alerts** tab is selected.

2. In the events list on the right, select an event instance that is marked **PRE**.

3. Click the **Show Details** link on the bottom of the pane.

   The **Selected Item Details** pane appears.

4. Click the **Alert** tab.
5. In the **Selected Item Details** pane, click a **View in HX** button.

   The HX appliance page appears with alert or indicator information on it.

**PRE** stands for presence. The presence mark means that the IOC is present, but execution has not been detected yet.

# Find

All table views in Redline have find capability to help you find specific data in the current table view. For example, you have a potentially compromised credit card number. Using Find, you can search the entire list of strings from all processes in memory to locate it.


Find pane located at the top of the table view

To find specific data, type a search term or regular expression in the text box. Click **Reg Ex** if the term entered is a regular expression. Searches are case insensitive; use a regular expression if case is important.

By default, Redline searches all fields within the current table view. To search one particular field, select it from the drop-down list.

To start the search, click . Use **Prev** and **Next** to move through the matched items.

Find is applicable only for items currently displayed in the table view. If items are not displayed because additional filters, such as the tags and comment filter, have been applied, then Find will not locate and display those items. For more information on tags and comments, see Filter by Tags and Comments on page 70.

# MD5 Whitelist

Redline supports filtering out data using a whitelist, which is a list of MD5 hash values known to be valid. When filtering based on a whitelist, Redline does not display any file

with an MD5 hash value in the whitelist.

Redline checks MD5 hash values against whitelists for the following data types:

- Processes
- Memory sections within processes
- File system files
- Alternative data streams within the file system
- Windows services
- Persistence
- Tasks

In addition to supporting MD5 hash values, Redline filters on MemD5 values collected for memory sections. Redline filters based on the MD5 value if both MD5 and MemD5 exist.

Redline includes a whitelist by default, which you can supplement or replace; see Expanding and Replacing Whitelists on the next page for more information.

## Filtering Table View Using Whitelists

In some table views, Redline displays ✓ next to the MD5 value of a specific entry if Redline has found that value in the whitelist. Entries lacking a check mark are not in the whitelist.

By default, when you open a table view displaying MD5 hashes, all data is displayed. You can filter out the whitelist items (i.e., those with a green check mark) by clicking **Hide Whitelist Items** at the bottom of the table view. The link changes to **Include Whitelist Items** to allow you to put the filtered items back into the table view.

When sorting on the MD5 hash column in table views, Redline sorts on the item's whitelisted state instead of the actual value in order to group whitelisted items together. To find an actual MD5 value, use Find; see Find on the previous page for more information.

You can change the default so that the whitelist items are hidden from view when you open the table view. To change the default, check the **Hide Whitelist Items by Default** option under Whitelist Management on the Redline Options windows, which is opened by clicking  at the bottom of the table view. See Expanding and Replacing Whitelists on the next page to see this window.

# Expanding and Replacing Whitelists

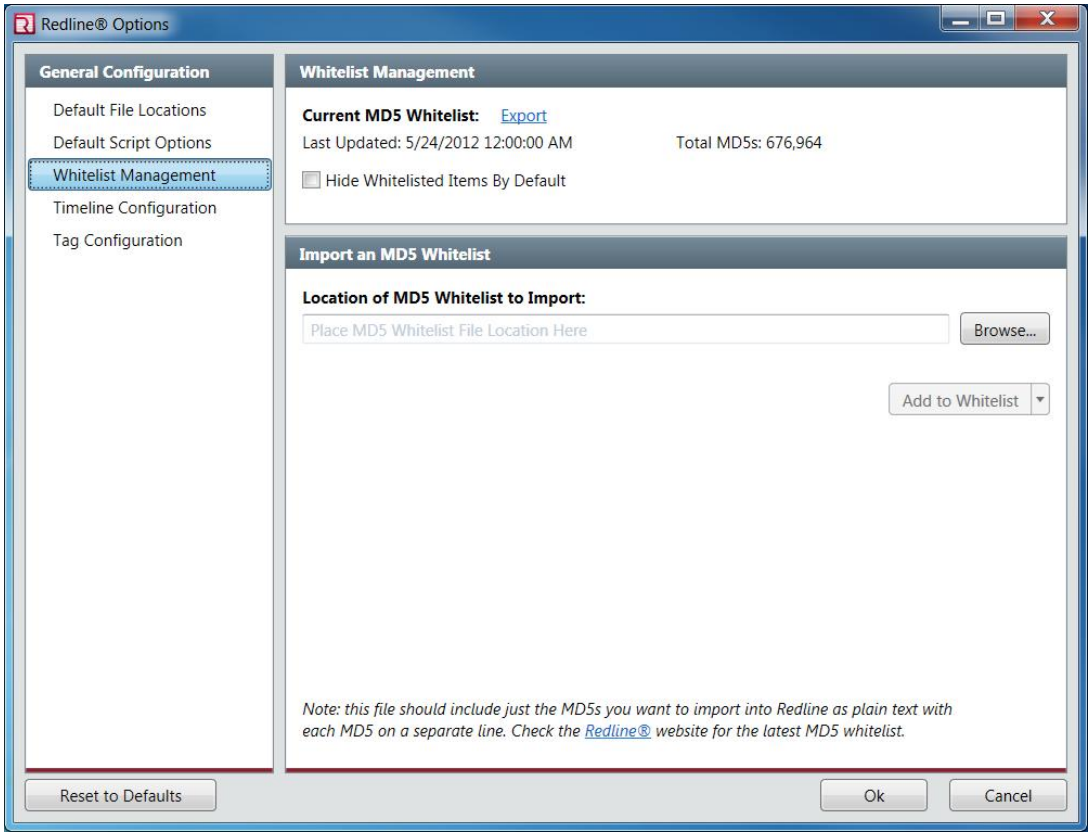
Redline includes a whitelist by default that has extracted MD5 hashes of various operating system components, based on standard, unaltered installations and service pack upgrades. This whitelist contains hashes for Microsoft Windows components, including known good DLLs and executable hashes, from Microsoft Windows Server Update Service and the National Software Reference Library.

Download new, updated whitelists from the website at https://www.fireeye.com/services/freeware/redline.html.

As you discover common, known-good components in your network, you can add them to a new whitelist file. The whitelist must be a plain text file with each MD5 hash value on a separate line.

You can import new whitelists into Redline to supplement the existing whitelist or to replace it.

The whitelist is managed under Whitelist Management on the Redline Options window, which is opened by clicking  at the bottom of the table view.




Whitelist Management options on Redline Options window.

To replace a whitelist or add to the existing whitelist, click **Browse** for the **Location of MD5 Whitelist to Import** option on the Whitelist Management window. Locate the new whitelist file and select it, then select one of the following:

- Select **Add to Whitelist** to merge the new whitelist file with your existing whitelist file. This option is the default choice.
- Select **Replace Whitelist** to remove the existing whitelist file from Redline and use the new whitelist file instead.

Whitelist configuration changes apply to all analysis sessions.

# Tags and Comments

You can tag top-level analysis data item with one of six user configurable tags, and add comments. You can also filter any table view according to specific tags assigned or by whether comments have been added.

Tags and comments are useful for annotating entries as you investigate. You can then return to these entries for further investigation, both in Redline and in other third-party tools, by exporting the table view of specifically tagged items to a CSV file. See CSV File Export on page 82 for more information.

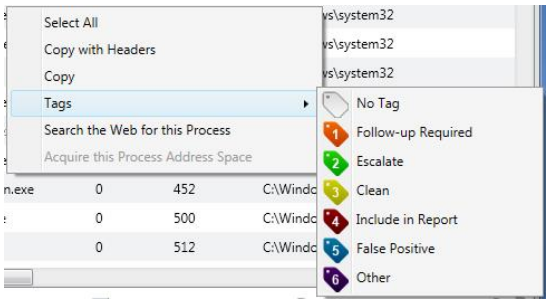
## Add Tags and Comments

You can add tags and comments to all top-level items in the Analysis Data window except system information. You can add tags to hierarchical processes but not filter hierarchical processes by the assigned tag.

Tags and comments that you add to items are stored with the analysis session.

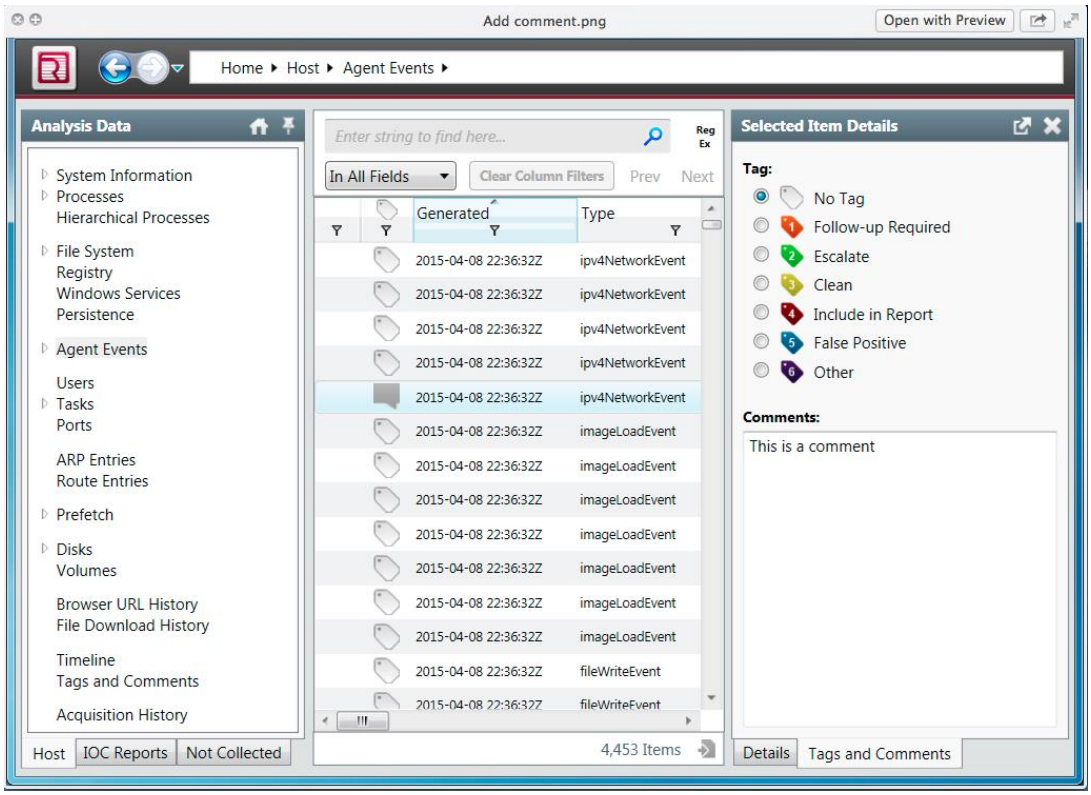
To add a tag and/or comments to a specific item, do one of the following:

- Click  to cycle through the tags.
- Select a single item or use **Ctrl** or **Shift** to select multiple items in the table view. Right-click and select the tag to apply. Only tags can be applied from this menu, not comments.




Right-click menu option for applying tags.

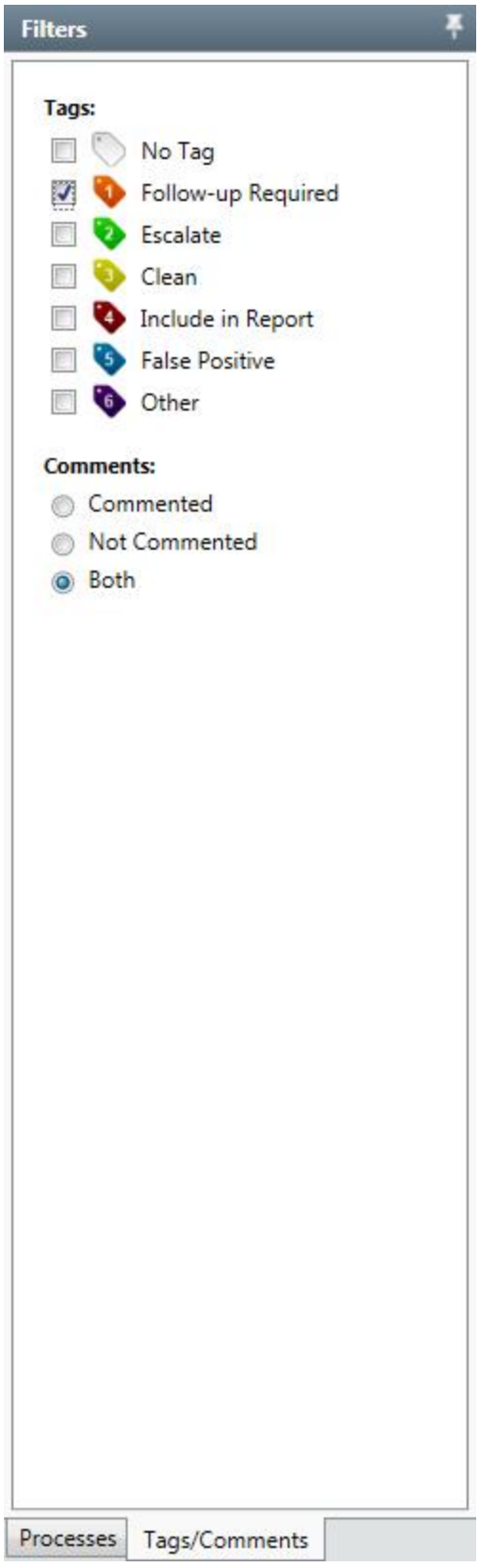
- Open the Tags and Comments window by clicking the **Tags and Comments** tab in an item's details view. This is the only way to add a comment.




Tags and comments are saved with the analysis session. For example, if you mark 10 users with green tags then close the analysis session, those same 10 users will have green tags when you open the analysis session again.

## Filter by Tags and Comments

Once you have tagged items, click **Tags and Comments** on the Analysis Data window's Host tab to view all items with specific tags and/or comments.


Filters
Tags:
No Tag
Follow-up Required
Escalate
Clean
Include in Report
False Positive
Other
Comments:
Commented
Not Commented
Both
Processes
Tags/Comments

In the table view, the  column displays the tag. A gray tag icon means no tag or comment has been applied. For items with tags and/or comments, hover over the tag to view the explanation or comment in a tooltip.

To sort and filter tagged items:

- Click the header in the tags column to sort the table view.
- Select the **Tags/Comments** tab on the Filters window.

Tags/Comments on the Filters Window

To limit the table view to display items with only specific tags, select the tags. To display all items that do not have a tag, select **No Tag**. To limit the table view to display only items with comments or without comments, select **Commented** or **Not Commented**, respectfully.

The tags and comments filters work together as an "and" type filter. For example, to display only items with a green tag that have comments, select the green tag and **Commented**.

## Customize Tags

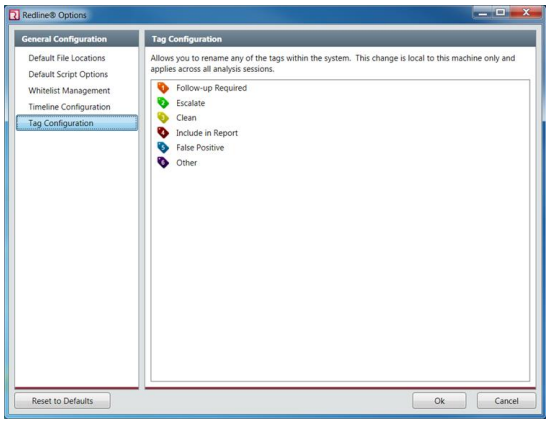
By default, Redline has the following configurable tags:

- Follow up Required (orange)
- Escalate (green)
- Clean (yellow)
- Include in Report (red)
- False Positive (blue)
- Other (purple)

You can rename any of these tags.

Changes to any tags apply to all analysis sessions viewed.

Click **Tag Configuration** on the **Redline Options** window, which is accessed under the  menu.




Tag Configuration options on the Redline Options window.

To change a tag, select it and click . After typing a new name, click to save it.

# Column Filters

Column filters allow you to narrow the items shown in the data grid by selecting and defining the parameters of a column. For example, by applying the filter to the Process Name columns, you can exclude Safe non-.exe files from the data grid in order to focus on suspicious .exe files only.

Redline includes two types of filters:

- Basic Filters below
- Advanced Filters on the next page

By default, no filters are applied.

## Basic Filters

Basic filters allow you to select items from a predetermined set of attributes specific to a column to display in the data grid.

The following table lists all of the columns with basic filters and their selectable attributes.

| Column | Filter Attributes |
|---|---|
| Hooked Signature Exists | • Selected<br>• Not Selected |
| Hooked Signature Verified | • Selected<br>• Not Selected |
| Signature Exists | • Selected<br>• Not Selected |
| Signature Verified | • Selected<br>• Not Selected |
| Injected | • Selected<br>• Not Selected |

| Column | Filter Attributes |
| --- | --- |
| Mapped | • Selected<br>• Not selected |
|  | Tags<br>• No Tag<br>• Follow-up Required<br>• Escalate<br>• Clean<br>• Include in Report<br>• False Positive<br>• Other<br>Comments<br>• Comments<br>• Not Commented |

## Advanced Filters

Advanced filters allow you to extract more granular lists of data by entering values to narrowly define parameters within a column. Multiple advanced filters can be applied to a column. When multiple filters are applied to a column, they function as a logical OR statement. By default, no filters are applied to a column.

Advanced filters can be applied to the following columns:

- Process Name
- PID
- Path
- Arguments
- Username
- Start Time
- Kernel Time
- User Time Elapsed
- Hidden
- Security ID
- SID Type
- Parent Name
- Parent PID
- MD5
- Signature Description
- Certificate Issuer
- Timestamp
- Field
- Summary
- Handle Name
- Handle Type
- Occurrence
- Address
- Object Address
- Count
- Section Name
- Certificate Subject
- Handle Index
- Module Init
- MemD5
- SHA1
- SHA256
- Protection
- Region Start
- Region Size
- Raw Flags
- String
- Created
- State
- Local IP Address
- Remote IP Address
- Remote Port
- Protocol
- Module Base

The following table describes the most common advanced filters among the columns.

| Advanced Filter | Description |
|---|---|
| contains | Includes items in the data grid that contain the entered value. |
| does not contain | Excludes items in the data grid that contain the entered value. |
| equals | Includes items in the data grid that exactly match the entered value. (This filter is case-sensitive.) |
| does not equal | Excludes items in the data grid that exactly match the entered value. (This filter is case-sensitive.) |
| starts with | Includes items in the data grid that start with the entered value. |
| does not start with | Excludes items in the data grid that start with the entered value. |
| ends with | Includes items in the data grid that end with the entered value. |
| does not end with | Excludes items in the data grid that end with the entered value. |
| regex | Includes all items in the data grid returned by your regular expression. |
| empty | Includes the empty Parent PID cell. |
| non-empty | Includes the non-empty Parent PID cell. |

The following table describes the columns with advanced filters that allow you to define ranges.

| Column | Filter | Notes |
|---|---|---|
| Start Time | Date/Time Range<br><br>or<br><br>Time Wrinkle | Date/Time Range allows you to define a range by providing a “from” date and time as well as a “to” date and time. If this filter is active and returns results, click its green >> icon to highlight the item with the earliest timestamp it returns.<br><br>Time Wrinkle allows you to define a range by providing a date and time, as well as start and end points in relation to it. |
| Kernel Time | From/To | Define a time range using the [d.]hh:mm[:ss[.ff]] format. |
| User Time Elapsed | From/To | Define a time range using the [d.]hh:mm[:ss[.ff]] format. |
| Created | Date/Time Range<br><br>or<br><br>Time Wrinkle | Date/Time Range allows you to define a range by providing a “from” date and time as well as a “to” date and time. If this filter is active and returns results, click its green >> icon to highlight the item with the earliest timestamp it returns.<br><br>Time Wrinkle allows you to define a range by providing a date and time, as well as start and end points in relation to it. |
| Size | From/To | Define a range of bytes, kilobytes, megabytes, or gigabytes. Decimals are not allowed. |

## Adding Filters

Filters can be added to any column with the icon in its header.

**To add a basic filter to a column:**

1. Click the icon in the header of the column.

   The filter window appears.

2. Select the item attributes you want the data grid to display.
3. Click Filter at the bottom right of the filter window.

**To add an advanced filter to a column:**

1. Click the icon in the header of the column.

   The filter window appears.

2. Select a parameter from the drop-down menu.

   The items listed in the drop-down menu vary per column.

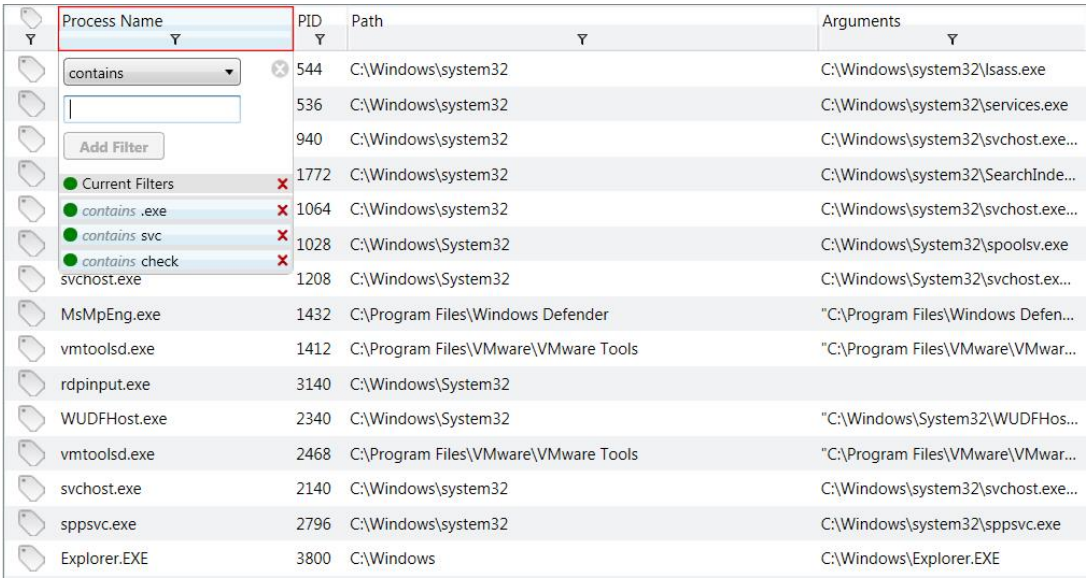
3. Enter the values that define the parameter in the text field below the drop-down menu.
4. Click Add Filter at the bottom of the filter window or press the Enter key to add the filter.

   The new filter appears below the Add Filter button.

5. Repeat steps 1 - 4 to add additional filters.

To close the filter window when you are done adding filters, click the icon.

After a filter is added to a column, that column's header will be outlined in red.




## Turning Advanced Filters Off and On

By default, advanced filters are turned on when they are first added. After filters have been added to a column, you can toggle them off and on. This allows you to quickly compare

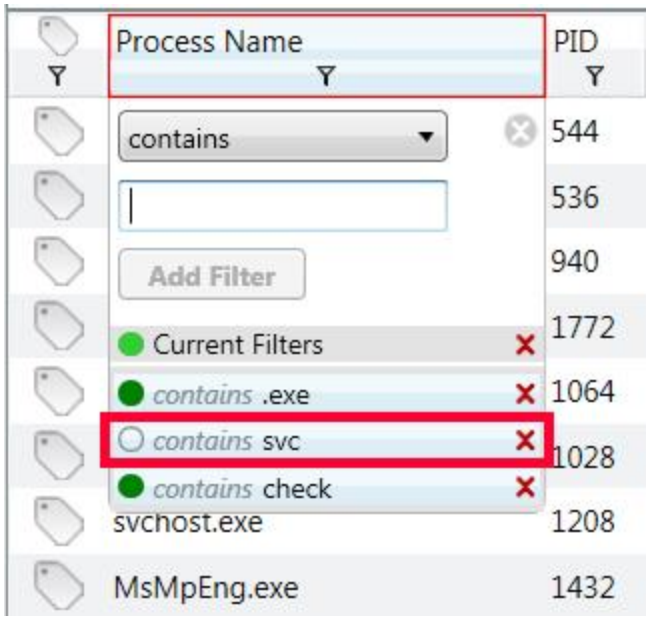
the results of different filter configurations because it is more efficient than adding and removing filters completely.

**To turn an advanced filter off:**

1. Click the icon in the header of the column.

   The filter window appears.

2. Click the icon of the filter you want to turn off.




   The

   turns transparent when the filter is off.

3. Repeat step 2 to turn off additional filters.

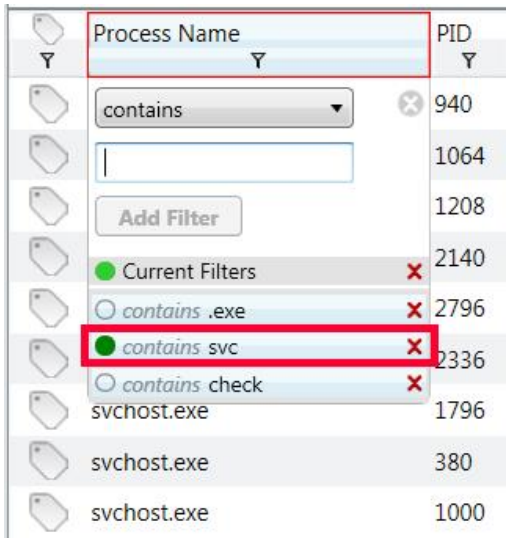
A column's header remains outlined in red whether its filters are on or off.

**To turn an advanced filter on:**

1. Click the icon in the header of the column.

   The filter window appears.

2. Click the ○ icon of the filter you want to turn on.




   The ○ turns green when the filter is on.

3. Repeat step 2 to turn on additional filters.

## Removing Filters

You can remove a basic filter from a column, remove an individual advanced filter from a column, remove all advanced filters from a column, or remove all filters from the data grid completely.

**To remove a basic filter from a column:**

1. Click the ▼ icon in the header of the column.

   The filter window appears.

2. Click None to deselect all of the item attributes.

3. Click Filter at the bottom right of the filter window.

**To remove an individual advanced filter from a column:**

1. Click the ▼ icon in the header of the column.

   The filter window appears.

2. Click the icon of the filter you want to remove.

**To remove all advanced filters from a column:**

1. Click the icon in the header of the column.

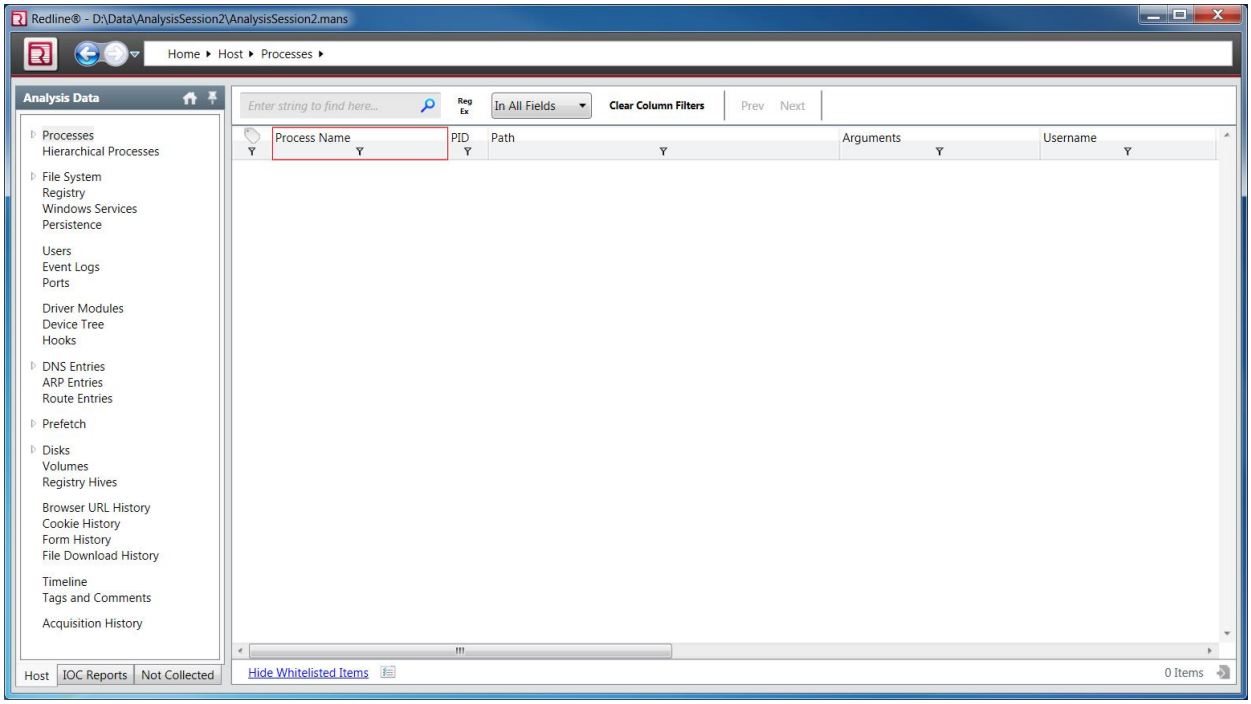
   The filter window appears.

2. Click the icon to the right of Current Filters.

To close the filter window when you are done removing filters, click the icon.

**To remove all filters among all columns in your currently displayed data grid:**

- Click the Clear All Filters button located at the top center of the Redline UI.




When there are no filters left in a column, the column's header is no longer outlined in red.

# Copy

Redline has the option to copy one line or all lines currently displayed in the table view, either with or without the header, in comma separated value (CSV) format.

To copy one item, right-click it in the table view and select either **Copy** or **Copy with Headers**. To copy all the items in a table view, right-click and select **Select All** then right-click again and select **Copy** or **Copy with Headers**.

The Select All function and Copy function are limited to the rows in the table view that have been paged into memory (which is roughly 20K).

# CSV File Export

Redline can export data displayed in a table view directly to a comma separate value (CSV) formatted file. The export will include all possible fields for each audit type regardless of whether the column is hidden from view. The export function is not limited to the rows in memory, like the copy function is.

To export the current table view to CSV, click  on the bottom of the table view.

# Web Search

Redline has the option to search the web for additional information about processes, imports, exports, and strings. Right-click the item in the table view and select the **Search the Web** option. Redline then performs a Google web search for the file name, process name, function name, or string data using your default web browser.

# Driver and Process Acquisition

Platform support: Windows versions prior to 10

If you have a memory image associated with your analysis session, you can use Redline to extract driver and process binaries for in-depth analysis using another tool.

This functionality requires enabling the **Acquire Memory Image** option when configuring a Redline Collector or analyzing a saved memory image to create an analysis session.

## Process and Driver Acquisitions

You can perform a deeper analysis of a suspect process or driver by fetching a copy of it from a live memory capture. Redline does not provide tools for inspecting address spaces or drivers; you will need to use a third-party tool.

To acquire a process address space:

- Right-click the named memory section in the memory sections table view and select **Acquire Process Address Space**.

To acquire a driver, right-click the driver in the driver modules or hooks table view and select one of the following depending on the type of driver: **Acquire Driver**, **Acquire This Hooked Driver**, or **Acquire This Hooking Driver**.

Acquisitions are done as background tasks because they take considerable time to complete. To view running background tasks, select **Background Tasks** under the  menu.

If Redline cannot find a process or driver, it writes a warning in an .xml file. These files are saved in the Default Unsafe Acquisition Staging Location. See Default Acquisition Locations below for more information.

If the memory image does not match the analysis session data, the acquisition may fail or cause unexpected results. This can happen if, in the time between collecting the data and acquiring its memory image, changes happened to the process or driver. You can work around this problem by creating a new analysis session from the memory image to acquire a process or driver.

Redline will fail if it tries to write the process or driver to a file path greater than 260 characters. If you encounter this, configure your acquisition staging directory to have a shorter path length and then retry the acquisition.

## Default Acquisition Locations

As part of process and driver acquisition, Redline provides a way to safely handle these potentially malicious files by doing the following:

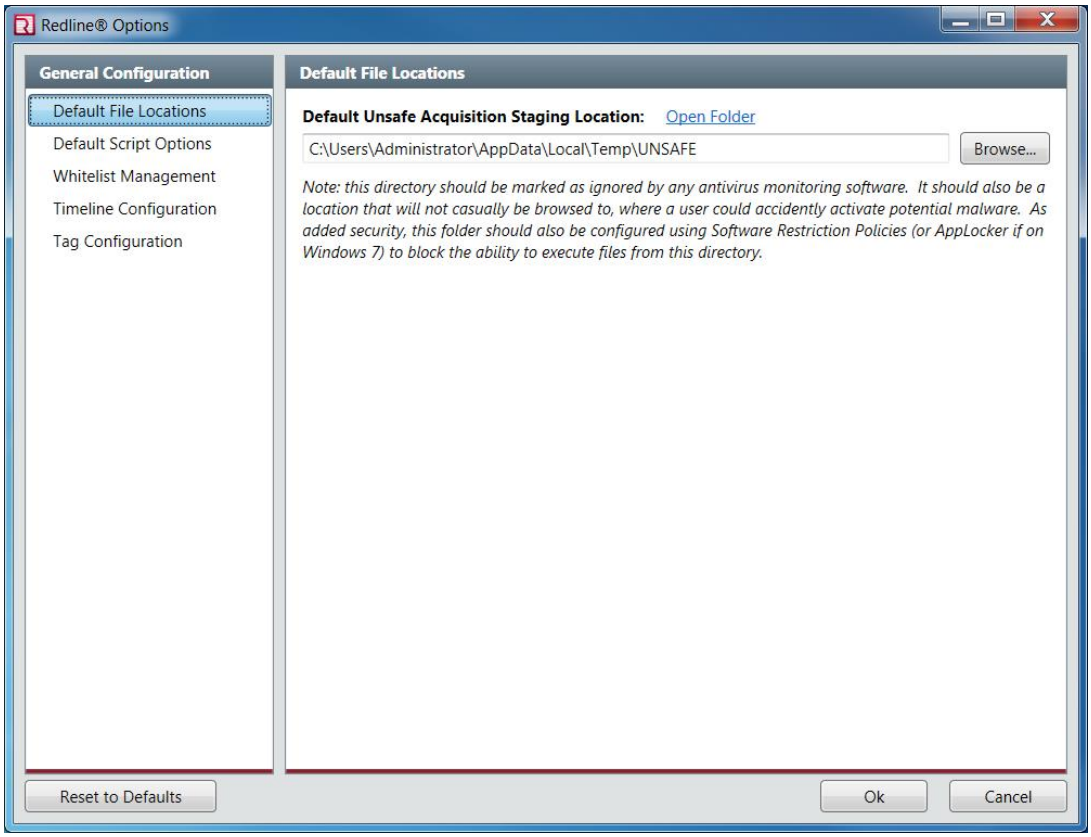
1. Writing the files in an unprotected and unsafe form to an unsafe acquisition staging location.
2. Placing the files collected into a password-protected zip file and writing a text file that contains the password (which is “Safe”).
3. Placing the zip file in the default acquisition location or the location specified.

The unsafe acquisition staging location should be:

- Created in a location that will not be casually browsed to, where a user could accidentally activate potential malware.

- Excluded from any active antivirus protection, to avoid the antivirus cleaning up or deleting any files you wish to analyze.
- Configured in Software Restriction Policies (or App Locker on Windows 7) to block the ability to execute files in this directory.

The unsafe acquisition staging location and the default audit and acquisition locations are set under **Default File Locations** on the Redline Options window, which is accessed under the menu.




Default File Locations options on Redline Options window.

Changes to these Redline options apply only to new analysis sessions. Existing sessions are not affected.

## Acquisitions History

To view the drivers and processes acquired, click **Acquisition History** on the Data Analysis window's Host tab.


Acquisition History window

To view a particular file, click it to open the directory containing the zipped, password-protected acquisition file for that process or driver in Windows Explorer. Accompanying the acquisition is a plain-text Readme file containing the password for the zip file. The password is “Safe” (note the capital S). Files are placed in password-protected zipped files to prevent accidental execution and deletion.

The acquisition folder is displayed at the bottom of the window. Click  to see the folder locations, including the audit location, memory image location, and location for acquisitions for this analysis session. See Session Information on page 30 for more information.

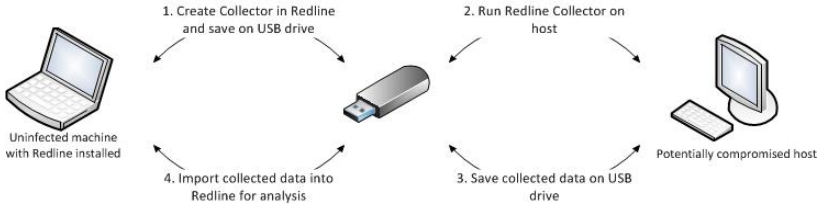
# Use Cases and Best Practices

Investigating a potential compromise on a host is a complex process. The best practices and use cases below are intended to help you get started on your investigation.

## Getting Started with Redline

You suspect an endpoint in your organization is compromised. To investigate:

1. Use Redline to create a Redline Collector.
2. Save the Redline Collector onto a portable storage device.
3. Run the Redline Collector from the portable storage device on the potentially compromised computer to generate an audit (i.e., collect date and save it to a file).
4. Save the audit from the target host back onto the portable storage device.
5. Import the audit into Redline to create an analysis session.
6. Review the data in the analysis session to begin your investigation.




Redline Basic Workflow

If you find a suspicious event, use the TimeWrinkles feature of Timeline to filter all events that occurred around that same time. If you suspect malicious activity by a process or single user, filter the timeline to show events associated with that specific process or user. See Timeline on page 57 for more information.

As you review your data, make use of tagging and commenting to maintain a record of your findings. See Tags and Comments on page 69 for more information.

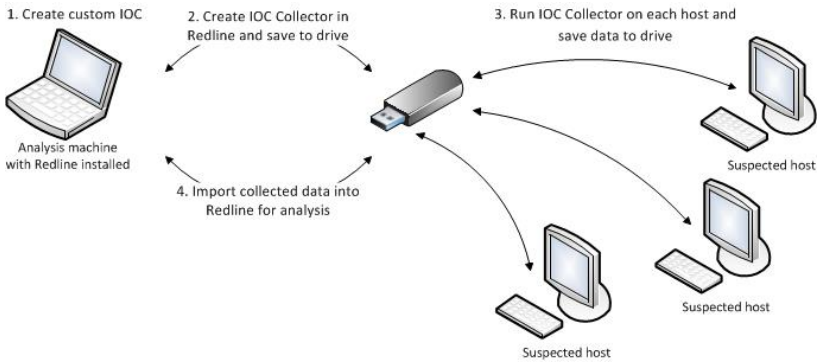
# Using IOCs to Find Known Threats

Platform support: Windows

Evidence suggests that a Windows endpoint in your organization has been compromised. You are able to determine the cause of the compromise and recognize some Indicators of Compromise (IOC) (e.g., specific file names or processes). To help identify if any additional endpoints are compromised, you either find an existing IOC or create a new one..

To help determine if other endpoints are also compromised:

1. Use Redline to create an IOC Search Collector.
2. Save the IOC Search Collector onto a portable storage device.
3. Run the IOC Search Collector from the portable storage device on each potentially compromised endpoint to generate an audit (i.e., collect date and save it to a file).
4. Import each audit into Redline and generate an IOC Report; see IOC Reports on page 55 for more information.
5. Review each IOC Report for any hits.




Redline with IOC analysis workflow

# Reviewing HX Triage Collections

Redline works with FireEye Endpoint Detection (HX) to triage events. Depending on the configuration, HX can automatically perform a Triage Collection on any endpoint involved in an alert.

To investigate a Triage Collection:

1. Download a Triage Collection around an alert in HX and open it in Redline.
2. Follow the initial lead and see what other suspicious evidence you can find.

3. Follow up in HX — depending on your findings, you may decide to contain your host in HX.

For example, you have a HX alert that provides contextual information such as a file name, process ID, or a timestamp of when the event occurred. Use Timeline in Redline to search for the network activity (by IP or DNS name) or host activity (such as a malicious file name) and discover what process was responsible for generating this alert. Use Timeline features like TimeWrinkles and filtering to see what actions the process took: files it created, network connections it generated, or registry keys it modified.

# Reviewing Web History Data

 Platform support: Windows, OS X

If you suspect that an endpoint has been compromised through its web browser, you can use Redline to review web history data stored in Microsoft Internet Explorer, Chrome, Firefox, or Safari.

To collect web history data from a potentially compromised endpoint and analyze it in Redline, you need to:

1. Configure a Redline Standard Collector so the script collects web history data.
    - Click **Edit your script** in the Start Your Analysis window
    - Click the **Network** tab and select **Browser History** then **Cookies**, **Form History**, **File Downloads**, and **URL History**.
    - Click **Show Advanced Parameters** to display options for **Target Browser** and **History Files Location** (Windows only) to collect data from specific directories for a specific browser. See Redline Collectors on page 6 for more information on creating a Collector and editing the script.
2. Run the Collector and import the audit into Redline. See Run Redline Collector on Host Computer on page 19 and Import Data into Redline on page 25 for more information.
3. Click the **Investigate** link under "I am Reviewing Web History Data" on the Start Your Investigation page.
4. Review the web browser URL history as a starting point then move on to cookie history, form history, and file download history recorded as needed. See Analysis Data on page 30 for more information on the data displayed.

To assist in your investigation:

- Sort the data in the table view by modifying the column header for ordering and sizing and right-clicking on a column header to show and hide columns.
- Use Find to locate specific records. See Find on page 66 for more information.
- Use Timeline to see a chronological listing of all web-based events (e.g., URL last browsed to, file download started, etc.) in a single display. You can use this to follow the activities of a user as they occurred on the system. See Timeline on page 57 for more information.
- Use tags and comments to mark your findings as you perform your investigation, making it easier to keep track of what you have seen while moving forward. See Tags and Comments on page 69 for more information. You can then go back and review tagged data in a table view then export it a CSV (comma separated values) file and import it into a reporting solution; see CSV File Export on page 82 for more information.

# Planning Compromise Responses

To be able to respond as effectively as possible to potential compromises of endpoints in your organization, consider a strategy or protocol for "live response" that does the following:

- Automates the collection of a standard data set
- Minimizes reaction time
- Minimizes interaction with the potentially compromised endpoint
- Minimizes changes to the potentially compromised endpoint

Live response results may contribute to administrative actions or legal proceedings, or may affect the business or people's lives. A sound process will help ensure findings are accurate, complete, and defensible.

A streamlined and effective live response process requires coordination. For example, if all you know about the potentially compromised endpoint is just an IP address, you will likely need to determine the host name and its physical location. You must have proper access to the host to be able to run a live response collection, and you must have a place to store collected data.

To create a live response process:

- Define the goal and deliverables
- Define organizational roles and responsibilities
- Design the process to be repeatable and automated as possible
- Design the process to be clear and easy to follow

- Consider all operating systems, not just Microsoft Windows
- Test the tools used in the process
- Document the process
- Train everyone involved

## Data Collection and Handling

Changes to a potentially compromised endpoint are unavoidable when responding to an incident. Understanding and minimizing those changes is important. Some points to consider:

- Treat the potentially compromised endpoint as "hot" — do not interact with it unless you have a plan.
- Consider everything you connect to the suspect endpoint as accessible to the attacker.
- Do not copy or save data to the potentially compromised endpoint unless there is no other option. Use a removable storage device, a network share (which must be considered compromised), or other remote media options.
- Do not perform any analysis on the potentially compromised endpoint. Do not "poke around" or "check one thing" on it.
- Focus on system data (file listings, logs, etc.), not user data.

Data collection is a balancing act between collecting too much and too little. Lean on the side of collecting excess data when you know little about the situation.

Consider the time it takes to collect data and the details of the situation. When time is the most critical component, you will want to modify the data collection routine; when time is not an issue, you might want to collect more data.

Always consider the data to be evidence. Consider using a standard "bag and tag" process that includes creating an evidence tag and initiating a chain of custody. The evidence tag describes the data collected and the chain of custody documents where it has been.

Always maintain positive control over evidence. Keep the data on encrypted file systems and under lock and key when not in your direct possession. Perform analysis on working copies, not the original, to prevent accidental alteration or data loss.

## Live Response Data Review Goals

When reviewing live response data, it is important to have goals to guide your investigation. The recommended goals are:

1. Determine if the endpoint has been compromised.
2. Determine the earliest evidence of compromise.

3. Determine the initial cause or method of intrusion.
4. Determine the scope of the compromise.
5. Assess the data exposure and damage. What did the attacker steal?
6. Document all findings. For more information on documenting, see Reporting below.

## Reporting

Create a report of every live response analysis you perform, regardless of findings. Consider including the following sections in the report:

- Background. How and why the endpoint was suspect (the initial lead information).
- Major Findings. A list of findings, each with one or two sentences of supporting information. Always list the source and date associated with the earliest evidence the endpoint was compromised.
- Evidence Examined. A list of examined evidence.
- Timeline of Events. Events presented as a table that includes the date, time (including time zone), and event.
- Details. For each analysis performed, details and any associated findings.

# Redline Licenses

Redline links to the following libraries:

- SQLite ADO.NET Provider Version 1.0.111.0 Public Domain. No license.
- Exception Reporter Version 2.1.1 LGPL (http://exceptionreporter.codeplex.com/license)
- Log4Net Version 1.2.10 Apache License 2.0 (http://logging.apache.org/log4net/license.html)
- Ookii Dialogs Version 1.0.0 (http://www.ookii.org/software/dialogs/)
- WPF Shell Integration Library Version v2 MICROSOFT PUBLIC LICENSE (Ms-PL) (http://archive.msdn.microsoft.com/WPFShell/Project/License.aspx)
- GeckoFX Version 2.0.0 Mozilla Public License 1.1 (http://www.mozilla.org/MPL/)

# Support

Check for updates to the Redline endpoint security tool at https://www.fireeye.com/services/freeware/redline.html.

Check out the FireEye blog at https://www.fireeye.com/blog.html for security information and insight on today's advanced threats from the leader in advanced threat protection.

E-mail Redline@FireEye.com regarding problems with the Redline endpoint security tool.

# Glossary

## A

**Acquisitions**

A Redline feature that allows users to acquire processes or drivers from a copy of a live memory capture for further analysis in another tool.

**Audit**

Data collected by a Redline Collector from a potentially compromised endpoint.

## E

**Endpoint**

See Host.

**Endpoint Threat Protection Platform (HX)**

A FireEye platform product that helps information security teams detect, respond to, and contain attacks. Among other things, HX can help enterprises use a variety of intelligence sources to find attackers; integrate endpoint coverage with network defenses; reach remote endpoints (no matter what kind of Internet connection they have); triage events more quickly and confidently, by providing endpoint context for network events; and contain endpoints and immediately deny attackers further access through those endpoints.

## F

**False Positive**

A hit on a threat or indicator of compromise (IOC) that is actually a benign condition.

## H

**Hit**

A match on a detection indicator that indicates the presence or execution on a host of a threat with that indicator.

**Host**

A computer system from which a Redline Collector (or other agent) collects data.

**HX**

See Endpoint Threat Protection Platform.

## I

**Indicator of Compromise (IOC)**

An individual characteristic or series of characteristics that, when observed, indicate the presence of specific malware or the execution of attacker methodologies (i.e., attributes of suspicious activity).

**IOC Hit**

When characteristics of an IOC match characteristics observed on a host.

## M

**Memoryze**

Mandiant's free memory analysis tool that helps incident responders find evil in live memory. Using Memoryze, incident responders can acquire the physical memory from a Windows operating system and perform advanced analysis of live memory while the computer is running.

## R

**Redline**

A tool for investigating hosts for signs of malicious activity through memory and file analysis, and subsequently developing a threat assessment profile. It provides several benefits including rapid triage, and guided analysis. Redline users can directly open Mandiant Intelligent Response (MIR) audits and Endpoint Threat Protection Platform (HX) Triage Collections to perform in-depth analysis (including establishing the timeline and scope of an incident).

**Redline Collector**

A package containing an executable script to run on a potentially compromised computer system to generate an audit that is imported into Redline for analysis.

**Regular Expression (Regex)**

Characters, words, or patterns of characters against which Redline can match data. It can be used when configuring a script in a Redline Collector or using Find in an analysis session.

## S

**Script**

Instructions in XML format that tell a Redline Collector what data to collect.

## T

**Triage Collection**

A package of time-sensitive data about the host which has been created by Endpoint Threat Protection Platform (HX).

## W

**Whitelist**

A list of MD5 hash values (and related files) known to be valid. Any components with a whitelisted MD5 hash value are known to be standard valid components.