Malwarebytes
BREACH
REMEDIATION

Malwarebytes Forensic Timeliner
Administrator Guide

Version 1.01

24 January 2017

Malwarebytes

Notices

This document is provided "as-is." The information contained in this document is subject to change without notice and is not warranted to be error-free. If you find any errors, we would appreciate your comments; please report them to us in writing.

Third Party Project Usage

Malwarebytes software is made possible thanks in part to many open source and third party projects. A requirement of many of these projects is that credit is given where credit is due. Information about each third party/open source project used in Malwarebytes software – as well as licenses for each – are available on the following page.

https://www.malwarebytes.com/support/thirdpartynotices/

Sample Code in Documentation

The sample code described herein is provided on an "as is" basis, without warranty of any kind, to the fullest extent permitted by law. Malwarebytes does not warrant or guarantee the individual success developers may have in implementing the sample code on their development platforms. You are solely responsible for testing and maintaining all scripts.

Malwarebytes does not warrant, guarantee or make any representations regarding the use, results of use, accuracy, timeliness or completeness of any data or information relating to the sample code. Malwarebytes disclaims all warranties, express or implied, and in particular, disclaims all warranties of merchantability, fitness for a particular purpose, and warranties related to the code, or any service or software related there to.

CWB22-1001a

Table of Contents

Introduction

Malwarebytes Forensic Timeliner (timeliner.exe, or "*Timeliner*") is a standalone tool, used to generate and display forensic system timelines on Windows systems. It is written in C++ using the Windows API, and is packaged as a single portable Windows executable (EXE) that runs on all modern versions of Windows (XP through Windows 10 clients, 32/64-bit, Servers 2003 (32-bit only) through 2012 (32/64-bit), and has no dependencies other than standard Windows DLLs. *Timeliner* must be run either as SYSTEM or as a local administrator on the machine.

Timeliner is intended to be used to retrospectively discover and display indicators of prior malware infection, notably the malware's source (when was the malware first created/downloaded/encountered, and where did it come from) and the malware's effects (what other files or artifacts did the malware create, delete, or modify). *Timeliner's* data sources are chosen to help answer these specific questions. For example, the browser history data sources might indicate where on the Internet some malware was downloaded from, and the USN Journal data source might indicate what files the malware might have dropped on the system when executed.

What's New

The following changes have been made in this version of *Malwarebytes Forensic Timeliner*:

New Features:

- Support for usage of proxy server for Internet connectivity

Key Features

The following are key features included in *Timeliner*:

- Collect and Export Windows full system historical timeline from many data sources
- Supported log formats include CSV and Event log (CEF)
- Ability to filter/exclude events that may be uninteresting or irrelevant from data sources

System Requirements

Following are minimum requirements for an endpoint on which *Timeliner* may be installed. Please note that these requirements do not include other functionality that the endpoint is responsible for.

- **Operating System:** Windows 10 (32/64-bit), Windows 8.1 (32/64-bit), Windows 8 (32/64-bit), Windows 7 (32/64-bit), Windows Vista (32/64-bit), Windows XP (Service Pack 2 or later, 32-bit only), Windows Server 2012/2012 R2 (32/64-bit), Windows Server 2008/2008 R2 (32/64-bit), Windows Server 2003 (32-bit only).

  PLEASE NOTE: Windows servers using the Server Core Installation process are specifically excluded

- **CPU:** 800 MHz or faster
- **RAM:** 256 MB (512 MB or more recommended)
- **Free Disk Space:** 20 MB
- **Screen Resolution:** 800x600 or higher
- **Active Internet Connection**, for license validation and client updates
- **USB 2.0 Port** (optional, depending on deployment method)

External Access Requirements

If your company's Internet access is controlled by a firewall or other access-limiting device, you must grant access for *Timeliner* to reach Malwarebytes services. Please assure access is available for:

https://*.mwbsys.com	Port 443	outbound

Using Malwarebytes Forensic Timeliner

Timeliner is designed specifically for use by IT staff. It may be deployed to a endpoint by local insertion of a USB drive which contains the program, or by pushing the program out to the endpoint using psexec, Powershell, or any other deployment method which you may currently use.

License Key Status

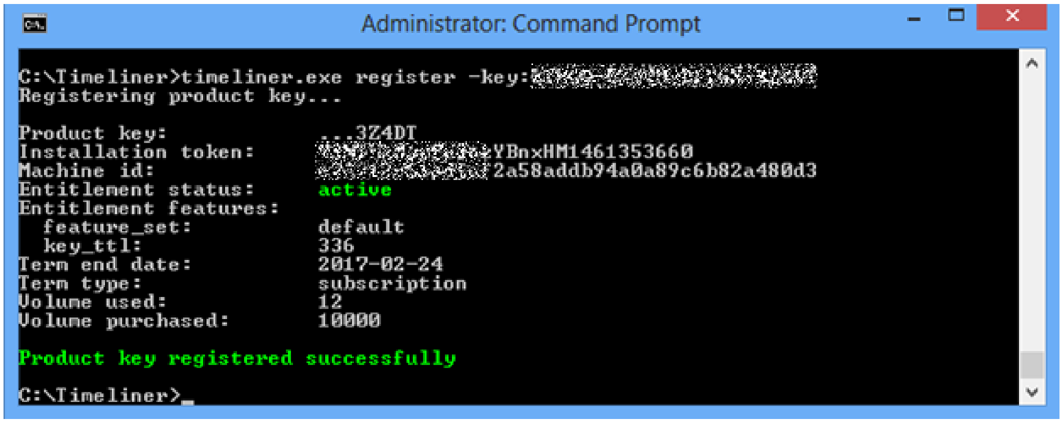
Timeliner uses a license key, which was provided to you upon your purchase of the client. Once registered, the license key is considered active for 14 calendar days – unless a different time interval was specified at time of purchase. Each time the client is used on an endpoint, license status is checked. If your license deactivates (times out), you cannot perform critical operations that the client is intended for. If this occurs, you must re-register the client. This is to prevent unauthorized use of the client. There is no additional cost to re-register the client.

Getting Started

Getting started with *Timeliner* is very simple. Using an endpoint with a live Internet connection, access an elevated Windows command line prompt (run as Administrator) and issue the following commands:

```
timeliner.exe register –key:<prodkey>
```

Please note: You must substitute your license key for **`<prodkey>`** in the above example. The screenshot below shows what you can expect to see for a successful client registration.



```
C:\Timeliner>timeliner.exe register -key:[redacted]
Registering product key...

Product key:              ...3Z4DT
Installation token:       [redacted]YBnxHM1461353660
Machine id:               [redacted]2a58addb94a0a89c6b82a480d3
Entitlement status:       active
Entitlement features:
  feature_set:            default
  key_ttl:                336
Term end date:            2017-02-24
Term type:                subscription
Volume used:              12
Volume purchased:         10000

Product key registered successfully

C:\Timeliner>_
```

Operations

The basic functionality of *Timeliner* is to:

1. Generate a full system historical timeline from the available data sources
2. Search that timeline for particular events by date/time or filename/path
3. Filter out events that may be uninteresting or irrelevant
4. Print out remaining relevant events to a CSV file or send them to an external log system (SIEM, Syslog)

When searching a timeline (Step #2, above), *Timeliner* can be run in one of four basic modes of operation:

1. **[-all]:** outputs a full system timeline,
2. **[-target ...]:** searches for a particular filename or path, or website name or partial path
3. **[-date ...]:** searches for a particular date/time
4. **default:** searches for events today (equivalent to **-date NOW**).

For full details of usage and command line syntax, see the documentation provided by running **timeliner.exe** (the program name with no arguments).

Data Sources

Timeliner utilizes Windows data sources to generate historical timelines for malware incursions and potential incursions. All data sources are subclasses of the **TimelineSource** abstract class. The following is a list of data sources which are added to the timeline, in alphabetical order.

DATA SOURCE	PURPOSE
ADS	An Alternate Data Stream is a Windows feature that is often used for hiding malicious code. It is also used for many legitimate purposes. Only files with alternate data streams are added to the timeline.
AppCompatCache	This is a record of file name, size, last modification and last execution. While a listed file may not have been actually executed, its existence in the cache shows that Windows has interacted with the file.
ChromeBrowserHistory	This provides the Chrome browser history of visited websites.
EventLog	This is a record of user login, logout and system startup events
FirefoxBrowserHistory	This provides the Firefox browser history of visited websites.
IEBrowserHistory	This provides the Internet Explorer browser history of visited websites.
JavaCache	This is a record of all loaded Java applets as recorded by Java's IDX Cache.
Jumplist	Jumplists are lists of recently opened files which are available to an application from the Windows Start Menu.
MFT	The Master File Table contains a record of known file creation times.
MRU	The Most Recently Used List is a chronological record of files which have been opened or accessed.
MUICache	The MUI Cache contains a list of applications which have been executed.
NetworkMap	This is a record of all networked drives which have served as mapped drives for the endpoint.
Prefetch	Prefetch entries aid in speeding up launch of an application. They also contain a record of DLLs used by an application as well as the most recent run time of the application.
RecentFiles	This is a record of shortcuts (*.lnk files) to files recently executed by the user.
RegistryModified	This is an aggregate record of last-modified dates for a variety of registry keys.
Schedule Task	This is a record of tasks which have been scheduled for later or periodic execution.
ShimCache	Used in conjunction with AppCompatCache, this source contains a record of files which have created processes during execution.
USBDrives	This is a record of all USB key attach/detach events
UserAssist	The UserAssist registry key allows determination of how, when and how often programs are launched, on a user-by-user basis.
USN Journal	Uses the Update Sequence Number Journal (change log) to identify all file create, delete, and rename events.
WinShares	This is a record of folders whose read/write access rights have been changed to make the folder available to others.

Notes about individual data sources:

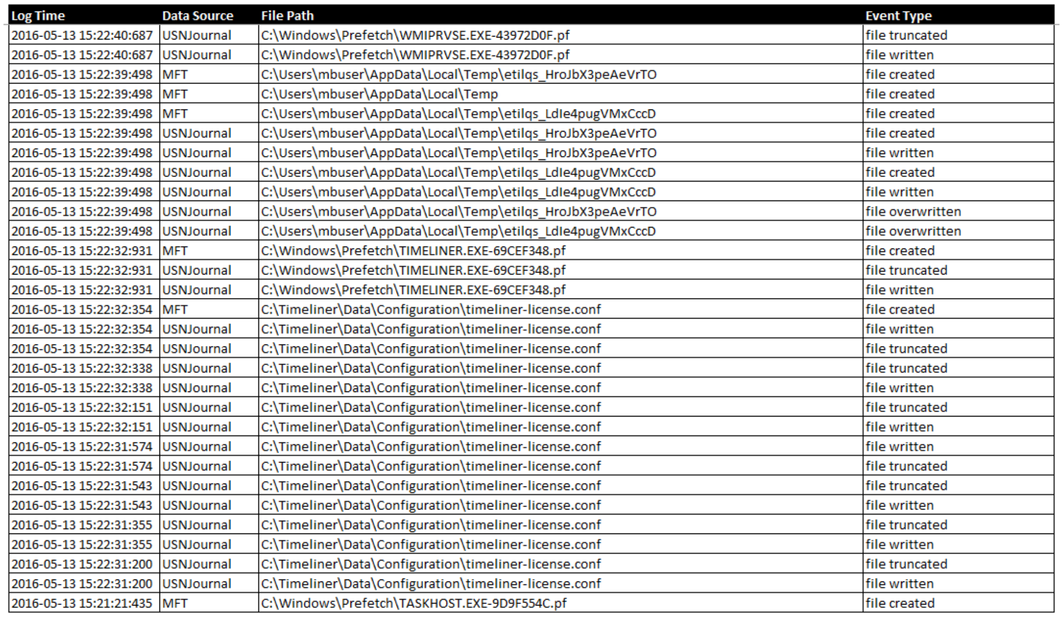
- The **USN Journal** is a circular buffer, and typically contains data for only the last 3-5 days of operation. Based on activity level on the endpoint in question, data may cover more *or* less time.
- The registry data sources (**ShimCache**, **UserAssist**, **MUI**, and **MRU**) are only sometimes present and reliable. They are not complete lists of executed programs. Windows does not maintain a complete list of executed programs.
- **Prefetch** is our most reliable indicator of execution, but it is disabled by default when Windows is installed on a solid-state drive (SSD).

…and some notes about data sources as a whole…

- Because many data sources used by *Timeliner* are ephemeral (notably the **USN Journal**, a circular buffer of unknown size), *Timeliner* should be run as soon as possible after a compromise, but before an anti-malware scan or remediation (which can destroy many indicators used by *Timeliner*).
- Browsers (notably Chrome and Firefox) should be closed during a *Timeliner* run. If left open, their history files will be locked and unavailable to Timeliner.
- In order to retrieve timeline events from all user accounts on the machine, *Timeliner* loads user HKCU registry hives (ntuser.dat) into temporary storage under HKU.
- In order to retrieve timeline events from both x86 and x64 native views of the registry on 64-bit versions of Windows, *Timeliner* disables Wow64 redirection for both the registry and the filesystem. Registry redirection is disabled in individual calls to *RegOpenKeyEx*, while filesystem redirection is disabled explicitly by calls to *Environment::DisableFilesystemRedirection* from *Main*.
- Windows API calls are used to read both the MFT and the USN Journal.
- Timeline events with unknown dates are currently stored at "time 0", or "0000-00-00 00:00:00". These events will appear in timelines constructed using the **"collect -date"** switch, unless **"settings -exclude.timeBefore"** is specified (which it is by default).

Event Logging

When *Timeliner* executes, it produces a log (CSV format) which you may save to a filename of your choice. The screenshot below is a sample from a log produced by *Timeliner.*



Log Time	Data Source	File Path	Event Type
2016-05-13 15:22:40:687	USNJournal	C:\Windows\Prefetch\WMIPRVSE.EXE-43972D0F.pf	file truncated
2016-05-13 15:22:40:687	USNJournal	C:\Windows\Prefetch\WMIPRVSE.EXE-43972D0F.pf	file written
2016-05-13 15:22:39:498	MFT	C:\Users\mbuser\AppData\Local\Temp\etilqs_HroJbX3peAeVrTO	file created
2016-05-13 15:22:39:498	MFT	C:\Users\mbuser\AppData\Local\Temp	file created
2016-05-13 15:22:39:498	MFT	C:\Users\mbuser\AppData\Local\Temp\etilqs_LdIe4pugVMxCccD	file created
2016-05-13 15:22:39:498	USNJournal	C:\Users\mbuser\AppData\Local\Temp\etilqs_HroJbX3peAeVrTO	file created
2016-05-13 15:22:39:498	USNJournal	C:\Users\mbuser\AppData\Local\Temp\etilqs_HroJbX3peAeVrTO	file written
2016-05-13 15:22:39:498	USNJournal	C:\Users\mbuser\AppData\Local\Temp\etilqs_LdIe4pugVMxCccD	file created
2016-05-13 15:22:39:498	USNJournal	C:\Users\mbuser\AppData\Local\Temp\etilqs_LdIe4pugVMxCccD	file written
2016-05-13 15:22:39:498	USNJournal	C:\Users\mbuser\AppData\Local\Temp\etilqs_HroJbX3peAeVrTO	file overwritten
2016-05-13 15:22:39:498	USNJournal	C:\Users\mbuser\AppData\Local\Temp\etilqs_LdIe4pugVMxCccD	file overwritten
2016-05-13 15:22:32:931	MFT	C:\Windows\Prefetch\TIMELINER.EXE-69CEF348.pf	file created
2016-05-13 15:22:32:931	USNJournal	C:\Windows\Prefetch\TIMELINER.EXE-69CEF348.pf	file truncated
2016-05-13 15:22:32:931	USNJournal	C:\Windows\Prefetch\TIMELINER.EXE-69CEF348.pf	file written
2016-05-13 15:22:32:354	MFT	C:\Timeliner\Data\Configuration\timeliner-license.conf	file created
2016-05-13 15:22:32:354	USNJournal	C:\Timeliner\Data\Configuration\timeliner-license.conf	file written
2016-05-13 15:22:32:354	USNJournal	C:\Timeliner\Data\Configuration\timeliner-license.conf	file truncated
2016-05-13 15:22:32:338	USNJournal	C:\Timeliner\Data\Configuration\timeliner-license.conf	file truncated
2016-05-13 15:22:32:338	USNJournal	C:\Timeliner\Data\Configuration\timeliner-license.conf	file written
2016-05-13 15:22:32:151	USNJournal	C:\Timeliner\Data\Configuration\timeliner-license.conf	file truncated
2016-05-13 15:22:32:151	USNJournal	C:\Timeliner\Data\Configuration\timeliner-license.conf	file written
2016-05-13 15:22:31:574	USNJournal	C:\Timeliner\Data\Configuration\timeliner-license.conf	file written
2016-05-13 15:22:31:574	USNJournal	C:\Timeliner\Data\Configuration\timeliner-license.conf	file truncated
2016-05-13 15:22:31:543	USNJournal	C:\Timeliner\Data\Configuration\timeliner-license.conf	file truncated
2016-05-13 15:22:31:543	USNJournal	C:\Timeliner\Data\Configuration\timeliner-license.conf	file written
2016-05-13 15:22:31:355	USNJournal	C:\Timeliner\Data\Configuration\timeliner-license.conf	file truncated
2016-05-13 15:22:31:355	USNJournal	C:\Timeliner\Data\Configuration\timeliner-license.conf	file written
2016-05-13 15:22:31:200	USNJournal	C:\Timeliner\Data\Configuration\timeliner-license.conf	file truncated
2016-05-13 15:22:31:200	USNJournal	C:\Timeliner\Data\Configuration\timeliner-license.conf	file written
2016-05-13 15:21:21:435	MFT	C:\Windows\Prefetch\TASKHOST.EXE-9D9F554C.pf	file created

Event Logging to syslog

Timeliner integrates very easily into a corporate network, allowing simplified deployment to endpoints as well as subsequent forensic analysis. That integration includes event logging using industry-standard methods. We have implemented logging using CEF (Common Event Format), and more specifically, output is tailored to the ArcSight Security Intelligence platform and others which support the CEF format.

Page 7 describes the four settings which control logging to your existing SIEM. While *Timeliner* automatically generates output files which correspond to each program execution, CEF logging is only performed after the feature has been enabled and properly configured.

Command Line Parameters

Timeliner supports a variety of command line parameters, which can be used from a command prompt, batch file or script. When used from a script, additional commands may be required to support the scripting model being used.

Conventions

The command line structure uses modifiers. These are shown as hyphens (-) immediately preceding parameters. Multiple modifiers may be combined with a parameter. When multiple parameters are used, they must be separated by spaces. In addition, the following conventions are used:

- **text without brackets or braces**
  Items you must type as shown
- **<text inside angle brackets>**
  Required information for which you must supply a value
  Example: **timeliner <*parameter_1*>**
- **[text inside square brackets]**
  Optional items
  Example: **timeliner [*parameter_1*]**
- **Grouping of dots (…)**
  A set of specifications
  Example: **timeliner <*parameter _1*> [*parameter_2*] … [*parameter_n*]**
- **{text inside braces}**
  A set of required items; choose one from the list provided
  Example: **timeliner {0 | 1 | 2 | 3}**
- **vertical bar (|)**
  Separator between mutually exclusive items; choose one
  Example: **timeliner <0 | 1 | 2 | 3>**

Command Line Overview

Timeliner commands are specified in the following format:

timeliner { version | register | collect | settings } [*options*]

Following is a list of high-level commands which may be executed. Each command is detailed beginning on the next page.

version	Displays the program version number.
register	Using your license key, this unlocks the features of *Malwarebytes Forensic Timeliner*. This will also show license status.
collect	Defines specifications to be used for data collection, followed by collection itself.
settings	Used to specify universal program settings. These settings are persistent, and are used for program settings which tend to be constants.

In addition, you may type **timeliner** without any additional specifications to see a list of valid commands. This list will span multiple windows if the command line is launched to its default size, so you will achieve best results by stretching the window to show more command line dialog at one time.

Command Line Reference

Commands listed here are listed individually. These are primarily used by a system administrator via script, batch file, GPO update, or Remote Desktop. The admin may configure *Timeliner* to operate as a remote task while the endpoint is not in use. When executed from a script, additional commands may be required to support the scripting model being used.

register

Usage:

timeliner register [-key:<*prodkey*>]

Purpose:

Specifies the unique license key assigned to the partner or customer. This is passed to the licensing server for validation to ensure it is active (non-expired). **A live Internet connection is required.** If the key is valid and the license is active, it will also display status about the license (expiration date, volume purchased, volume used, etc.).

If the key is active, the local installation will operate with this status for 14 calendar days (or the time interval specified in your Malwarebytes license agreement). This "Last Known Good" status is persisted on the USB or wherever the binaries are stored. This allows the USB installation to work as if it were fully registered on offline endpoints or without needing the key.

If **-key** is not specified, license status and the expiration date/time are displayed. **Please note:** If the key is not active, the user may not update threat signature databases, scan for malware, list quarantine contents, or restore files from quarantine.

Parameters:

-key:<*prodkey*>

Specification of <*prodkey*>, the license key assigned to the user.

version

Usage:

timeliner version

Purpose:

Displays the program version number.

Parameters:

none

collect

Usage:

timeliner collect [-all]
[-target:<*string*>]
[-date:<*dateString*>]
[-output:<*fileName*>]
[-excludeTypes:<*eventTypes*>]
[-includeTypes:<*eventTypes*>]

Purpose:

Collects forensic data related to possible malware incursions based on criteria specified by the user here. System data may be specified by inclusion of text strings, date/time, and may be set to include or exclude specified event types. Specifications provided here are often changed, so they are not included in **settings**.

Parameters:

-all

All available system data will be collected.

-target:<*string*>

Text string to be searched for. The string is not case-sensitive. Only data containing this string is collected.

-date:<*dateString*>

The earliest date/time that data will be collected for. The format for <*dateString*> is:

```
yyyy-mm-dd hh:mm:ss.msec
```

If a time is not specified, the beginning of the day is used (0 h, 0 m, 0 s, 0 ms). **Please note** that exclude times (before and after, as specified in **settings**) use this parameter as a reference to the date/times that they represent.

-output:<*fileName*>

Filename which will contain requested data after collection. If a filename is specified, it will override the default filename and save the output file to the program home directory unless a different directory is specified as part of the filename. The default log filename is:

```
forensic-log-<hostname>-<yyyy>-<mm>-<dd>-<hh>-<mm>-<ss>
```

-excludeTypes:<*eventType_1*>[,*eventType_2*,*eventType_n*]

Event types to be excluded from data collection. When multiple event types are listed, they should be separated by commas. You may use **-excludetypes** or **-includetypes** during a single instance of data collection, but not both. Event types which may be specified are:

ads
fileattrchanged
filecreated
filedeleted
fileencrypteddecrypted
fileexecuted
fileexecutedsubsequent
fileoverwritten
filerenamedfrom
filerenamedto
filesecuritychanged
filetruncated
filewritten
† jumplists
networkmap
registrykeymodified
shares
systemstartup
usbatacheddetached
userlogoff
userlogon
websitevisited

Notes: Event types preceded by (†) are not available on Windows XP or Windows Vista.

-includeTypes:<*eventType_1*>[,*eventType_2*,*eventType_n*]

Event types to be included in data collection. When multiple event types are listed, they should be separated by commas. You may use **-excludetypes** or **-includetypes** during a single instance of data collection, but not both. See parameter **-excludetypes** for a list of event types which may be specified.

settings

Usage:

```
timeliner settings [-exclude.browserTIF:true | false]
                   [-exclude.oprphaned:true | false]
                   [-exclude.temporary:true | false]
                   [-exclude.goodDirs:true | false]
                   [-exclude.recycled:true | false]
                   [-log.enabled:true | false]
                   [-log.server:<host>]
                   [-log.port:<port>]
                   [-log.test]
                   [-exclude.export:<filename>]
                   [-exclude.import:<filename>]
                   [-exclude.timeBefore:<time>]
                   [-exclude.timeAfter:<time>]
                   [-exclude.installBefore:<time>]
                   [-proxy.clear]
                   [-proxy.enabled:true|false]
                   [-proxy.server:<host>]
                   [-proxy.port:<port>]
                   [-proxy.user:<user>]
                   [-proxy.password:<password>]
```

Purpose:

This parameter allows a user to define settings that will be used as default specifications for all executions of *Timeliner*. While these settings may be modified at any time, they are typically rather static in nature. Typing **"timeliner settings"** with no additional parameters will display current program settings.

Parameters:

-exclude.browserTIF:true | false

Determines whether browser Temporary Internet Files (TIF) are excluded (true) or included (false). The default value is false. A list of all folders containing Temporary Internet Files can be found in Appendix A.

-exclude.orphaned:true | false

Determines whether orphaned file entries are excluded. Orphaned files sometimes come into existence after they have been deleted, their parent directory entry has been deleted, and the space used by the parent directory entry in the Master File Table has been reallocated. The default value is true.

-exclude.temporary:true | false

Determines whether temporary files and folders are excluded (true) or included (false). The default value is false.

-exclude.goodDirs:true | false

Determines whether activity for *known good* folders is excluded from data collection. These folders are listed as [well-known folders] in Appendix A. The default value is true. **Please note** that when gathering data for specific directories (rather than the default "*all*" directories), you may wish to change the value of this parameter to false.

-exclude.recycled:true | false

Determine whether contents of the Windows Recycle Bin is excluded. The default value is false.

-log.enabled:true | false

Specifies whether program execution is logged to a syslog server. All data utilizes a CEF (Common Event Format) standard. If this parameter is set to *true*, the syslog *host* IP/FQDN and *port* number must also be specified before event logging can take place. The default value is false.

-log.server:<host>

IP address or Fully-Qualified Domain Name (FQDN) of a syslog server which will receive event logs generated by *Timeliner*. A valid *port* number must also be specified before logging can take place.

-log.port:<port>

Valid port number for the syslog server which will receive event logs generated by *Timeliner*. A valid syslog *host* specification must also be specified before logging can take place.

-log.test

Responds with a text message indicating success or failure in communicating

-exclude.export:<filename>

Filename that the exclusion list is exported to, typically to allow editing of the list. Filename must be a valid Windows path/filename. If the filename includes embedded spaces, the entire filename must be surrounded by double quotes (").

-exclude.import:<filename>

Filename that the exclusion list is imported from. Filename must be a valid Windows path/filename. If the filename includes embedded spaces, the entire filename must be surrounded by double quotes (").

-exclude.timeBefore:<time>

Exclude data collection for records written to data sources before the specified time. The default value is 1d (one day). You may specify time increments with letters w (weeks), d (days), h (hours), m (minutes), s (seconds) or l (lower case L, representing milliseconds). **Please note** the following:

- All time increments are relative to the date/time specified in **collect –date**.
- You may combine multiple time specifications (i.e. 1w2d).
- You may collect data for time windows by combining **timeBefore** and **timeAfter**.

-exclude.timeAfter:<time>

Exclude data collection for records written to data sources after the specified time. The default value is 1d (one day). You may specify time increments with letters w (weeks), d (days), h (hours), m (minutes), s (seconds) or l (lower case L, representing milliseconds). **Please note** the following:

- All time increments are relative to the date/time specified in **collect –date**.
- You may combine multiple time specifications (i.e. 1w2d).
- You may collect data for time windows by combining **timeBefore** and **timeAfter**.

-exclude.installBefore:<time>

Exclude data collection for files created before the specified time. The default value is 7d (seven days). You may specify time increments with letters w (weeks), d (days), h (hours), m (minutes), s (seconds) or l (lower case L, representing milliseconds). Please note that time increments are relative to the time that collection begins.

[-proxy.clear]

Clear all existing proxy settings

[-proxy.enabled:true|false]

Specifies whether a proxy server is required to access the licensing server. If this parameter is set to *true*, the proxy server host IP/FQDN and port number must also be specified. If authentication is required for proxy access, the user name and password associated with the user name must also be specified. The default value is false (disabled).

[-proxy.server:<host>]

IP address or Fully-Qualified Domain Name (FQDN) of a proxy server used to access the licensing server. If this parameter is specified, the port must also be specified. If proxy usage is disabled, this parameter is ignored.

[-proxy.port:<port>]

Valid port number for the proxy server used to access the licensing server. If proxy usage is disabled, this parameter is ignored.

[-proxy.user:<user>]

User name when proxy usage is enabled and authentication is required. If a password is required, it must also be specified. If proxy usage is disabled, this parameter is ignored.

[-proxy.password:<password>]

Password for user when proxy usage is enabled. If proxy usage is disabled, this parameter is ignored.

Appendix A: Data Source Exclusions

Default settings for excluded folders used by *Timeliner* are listed below. You can add (exclude from reporting) or remove (include in reporting) an excluded folder at will. To add a new folder to be excluded, simply insert it after a new line in the corresponding folder section. Only one folder may be listed per line, and the allowable wild card is '*'. To remove an excluded folder, you may delete it or put a semicolon in front of the folder entry. To include a subfolder under an excluded folder, you must insert it under the excluded folder and put a '+' in front of the folder entry. Here is an example:

*\Windows\AppCompat\*	Do not report on files in this folder tree
+*\Windows\AppCompat\Programs\*	Report on files in this folder tree

To bring the new settings into effect, please run:

```
timeliner setting -exclude.import:<filename>
```

Where **`<filename>`** is the name of the file which the exclude list was previously exported to. This method provides granularity to allow inspection of the file system.

```
[well-known folders]
    *\.git\*
    *.obj
    *.lck
    *\pagefile.sys
    *\Config.Msi
    *\$Extend\*
    *\System Volume Information\*
    *\Users\sshd_server\*
    *\Users\*\NTUSER.DAT*
    *\Windows\AppCompat\*
    *\Windows\AppReadiness\*
    *\Windows\assembly\*
    *\Windows\Boot\*
    *\Windows\Fonts\*
    *\Windows\IME\*
    *\Windows\inf\*
    *\Windows\Logs\*
    *\Windows\Installer\*
    *\Windows\L2Schemas\*
    *\Windows\Microsoft.NET\*
    *\Windows\Microsoft .NET\*
    *\Windows\PolicyDefinitions\*
    *\Windows\Registration\*
    *\Windows\rescache\*
    *\Windows\ServiceProfiles\*
    *\Windows\Servicing\*
    *\Windows\SoftwareDistribution\*
    *\Windows\System32\catroot\*
    *\Windows\System32\catroot2\*
    *\Windows\System32\config\*
    *\Windows\System32\DriverStore\FileRepository\*
    *\Windows\System32\GWX\*
    *\Windows\System32\LogFiles\*
    *\CCleaner\*
    *\Cisco Systems\*
    *\Cisco\*
    *\Citrix\*
    *\Common Files\Adobe\*
    *\Common Files\Apple\*
    *\Windows\System32\MsDtc\*
    *\Windows\System32\spool\*
    *\Windows\System32\spp\*
    *\Windows\System32\sru\*
    *\Windows\System32\Sysprep\*
    *\Windows\System32\Tasks\Microsoft\*
    *\Windows\System32\wdi\*
    *\Windows\System32\wbem\Performance\*
    *\Windows\System32\wbem\Repository\*
    *\Windows\Winsxs\*
    *\AppData\Local\Packages\Microsoft.*
    *\AppData\LocalLow\Microsoft\*
    *\AppData\Roaming\Microsoft\Windows\Themes\*
    *\ProgramData\Microsoft\*
    +*\ProgramData\Microsoft\Windows\Start Menu\*
    *\Microsoft\Windows\Sqm\*
    *\Microsoft\Windows\Recent\AutomaticDestinations\*
    *\Microsoft\Windows\Recent\CustomDestinations\*
    *\SystemIndex\Indexer\CiFiles\*
    *\3M\*
    *\Acronis\*
    *\Adobe\*
    *\Apple Computer\*
    *\ArcSoft\*
    *\ASUS\*
    *\ATI Technologies\*
    *\AVAST Software\*
    *\Avira\*
    *\Bonjour\*
    *\Box\*
    *\Box Sync\*
    *\Broadcom\*
    *\Carbonite\*
    *\OpenSSH\*
    *\OpenVPN Technologies\*
    *\Panda USB Vaccine\*
    *\QuickTime\*
    *\Realtek\*
    *\Reference Assemblies\*
```

[well-known folders] (continued)

*\Common Files\Java\*
\Common Files\Microsoft Shared
*\Common Files\VMware\*
\COMODO
\CrashPlan
\CyberLink
\Dell
\Dropbox
\EPSON Software
\Fiddler2
\Fitbit Connect
\Foxit Reader
\G Data
\Google
\Hewlett-Packard
\HP
\Intel
\Internet Explorer
\iPod
\iTunes
\Java
\Kaspersky Lab
\LANDesk
\LastPass
\Lenovo
\Logitech
\Malwarebytes Anti-Exploit
\Malwarebytes Anti-Malware
\McAfee
\Microsoft Analysis Services
\Microsoft Games
\Microsoft Office 15
\Microsoft Office
\Microsoft Silverlight
\Microsoft SQL Server Compact Edition
\Microsoft SQL Server
\Microsoft Sync Framework
\Microsoft Synchronization Services
\Microsoft Visual Studio 8
\Mozilla
\Mozilla Firefox
\Mozilla Maintenance Service
\NVIDIA Corporation
*\Reference Assemblies\Microsoft\*
\SAMSUNG
\Sandboxie
\Seagate
\Skype
\Sophos
\Spotify
\Stardock
\Steam
\Symantec
\TAP-Windows
\TeamViewer
\TechSmith
\TextPad 5
\Thunderbird
\TOSHIBA
\Trend Micro
\uTorrent
\USOShared
\USOPrivate
\VideoLAN
\VLC
\VMware
\WebEx
\Webroot
\Western Digital
\WindowsApps
\Windows Defender
\Windows Journal
\Windows Kits
\Windows Mail
\Windows Mail
\Windows Media Player
\Windows Multimedia Platform
\Windows NT
\Windows Photo Viewer
\Windows Portable Devices
\Windows Sidebar
\WindowsPowerShell
\WinRAR
\WinZip
\Wireshark
\Yahoo!

[temporary folders]

*.tmp
*.temp
\Temp

[browserTIF folders]

\Firefox
\Chrome
\Cache
\Temporary Internet Files
\Content.IE5
\History.IE5
\Cookies
\INetCache
\INetCookies
*.sbstore
*.cache
*.pset
*\Windows\System32\IE11WIN10_*

```
[recycle bin folders]
        *\RECYCLER\*
        *\RECYCLED\*
        *\$Recycle.Bin\*
```

Appendix B Mapping Data Sources to Event Types

The following list maps the event types which data may be collected for, and the data sources where this data originated.

Available filtering event types are:

EVENT TYPE	DATA SOURCE
ads	ADS
fileattrchanged	USN Journal
filecreated	MFT USN Journal
filedeleted	USN Journal
fileencrypteddecrypted	USN Journal
fileexecuted	AppCompatCache JavaCache MRU MUICache Prefetch RecentFiles RegistryLoadPoints ShimCache UserAssist WinJob
fileexecutedsubsequent	ShimCache
fileoverwritten	USN Journal
filerenamedfrom	USN Journal
filerenamedto	USN Journal
filesecuritychanged	USN Journal
filetruncated	USN Journal
filewritten	USN Journal
jumplists	JumpListFiles
networkmap	NetworkMap
registrykeymodified	RegistryLoadPoints
shares	WinShares
systemstartup	EventLog
usbattacheddetached	USBDrives
userlogoff	EventLog
userlogon	EventLog
websitevisited	ChromeBrowserHistory FirefoxBrowserHistory IEBrowserHistory