Digital Forensics Artifact knowledge base

Release 20221121

unknown

Nov 21, 2022

CONTENTS

The Digital Forensics Artifacts Repository, is a free, community-sourced, machine-readable knowledge base of digital forensic artifacts that the world can use both as an information source and within other tools.

This knowledge base provides documentation accompanying the machine-readable definitions in the repository.

The source code is available from the project page.

CHAPTER

ONE

FILE SYSTEMS

File system artifacts.

1.1 New Technologies File System (NTFS)

NTFS is a file system that is predominantly used on Windows NT and later derived version.

1.1.1 References

- ForensicsWiki: New Technology File System (NTFS)
- New Technologies File System (NTFS)
- Linux NTFS file system support

CHAPTER

TWO

WEB BROWSER

Web browser artifacts.

2.1 Google Chrome/Chromium disk cache

Google Chrome/Chromium uses disk cache to store resources fetched from the web so that they can be accessed quickly at a latter time if needed.

2.1.1 Cache version 2

On Linux Google Chrome/Chromium 8

```
/home/$USER/.cache/chromium/Cache/
/home/$USER/.cache/google-chrome/Cache/
```

On Linux Google Chrome/Chromium 9 to 51

```
/home/$USER/.cache/chromium/$PROFILE/Cache/
/home/$USER/.cache/google-chrome/$PROFILE/Cache/
```

On Mac OS

```
/Users/$USER/Library/Caches/Google/Chrome/$PROFILE/Cache/
```

Where the $PROFILE contains the name of the profile. The default profile is named "Default".

On Windows XP

```
C:\Documents and Settings\%USERNAME%\Local Settings\Application Data\Google\Chrome\User␣
↪Data\%PROFILE%\Cache\
```

On Windows Vista, 7

```
C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\%PROFILE%\Cache\
```

Where the %PROFILE% contains the name of the profile. The default profile is named "Default".

2.1.2 Media Cache

```
/home/$USER/.cache/chromium/$PROFILE/Media Cache/
/home/$USER/.cache/google-chrome/$PROFILE/Media Cache/
```

2.1.3 Application Cache

```
/home/$USER/.config/chromium/$PROFILE/Application Cache/Cache/
/home/$USER/.config/google-chrome/$PROFILE/Application Cache/Cache/
```

2.1.4 GPUCache

On Linux Google Chrome/Chromium 68

```
/home/$USER/.config/google-chrome/$PROFILE/GPUCache/
/home/$USER/.config/google-chrome/$PROFILE/Storage/ext/$EXTENSION/def/GPUCache/
/home/$USER/.config/google-chrome/ShaderCache/GPUCache/
```

Where the $EXTENSION contains the identifier of the extension such as "nmmhkkegccagdldgiimedpiccmgmieda".

2.1.5 References

- Forensicswiki: Google Chrome
- Example Google Chrome Cache files, by chrome-specimens project

2.1.6 Test versions

2.2 Mozilla Firefox disk cache

Mozilla Firefox uses disk cache to store resources fetched from the web so that they can be accessed quickly at a latter time if needed.

There are 2 known disk cache formats:

- Mozilla Firefox disk cache format version 1
- Mozilla Firefox disk cache format version 2

2.2.1 Firefox 1 to 31

Mozilla Firefox 1 to 31 use the Mozilla Firefox disk cache format version 1.

On Linux Mozilla Firefox 1 to 20

```
/home/$USER/.mozilla/firefox/$PROFILE.default/Cache/
```

On Linux Mozilla Firefox 21 to 31

```
/home/$USER/.cache/mozilla/firefox/$PROFILE.default/Cache/
```

On Mac OS

```
/Users/$USER/Library/Caches/Firefox/Profiles/$PROFILE.default/Cache/
```

On Windows XP

```
C:\Documents and Settings\%USERNAME%\Local Settings\Application Data\Mozilla\Firefox\
↪Profiles\%PROFILE%.default\Cache\
```

On Windows Vista, 7

```
C:\Users\%USERNAME%\AppData\Local\Mozilla\Firefox\Profiles\%PROFILE%.default\Cache\
```

2.2.2 Firefox 32 and later

Mozilla Firefox 32 and later use the Mozilla Firefox disk cache format version 2.

On Linux

```
/home/$USER/.mozilla/firefox/$PROFILE.default/cache2/
```

On Mac OS

```
/Users/$USER/Library/Caches/Firefox/Profiles/$PROFILE.default/cache2/
```

On Windows XP

```
C:\Documents and Settings\%USERNAME%\Local Settings\Application Data\Mozilla\Firefox\
↪Profiles\%PROFILE%.default\cache2\
```

On Windows Vista, 7

```
C:\Users\%USERNAME%\AppData\Local\Mozilla\Firefox\Profiles\%PROFILE%.default\cache2\
```

2.2.3 References

- Forensicswiki: Mozilla Firefox
- Example Mozilla Firefox Cache files, by firefox-specimens project

CHAPTER

THREE

WINDOWS

Windows operating system artifacts.

3.1 Active Desktop

Active Desktop was a feature of Microsoft Internet Explorer 4.0 that added support for HTML content on the desktop, along with other features.

3.1.1 Significance

Malware is known to use Active Desktop settings and components for persitence.

3.1.2 Settings

The Active Desktop settings can be found in the Windows Registry key:

```
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Desktop\General
```

3.1.3 Components

The Active Desktop components can be found in the sub keys of the Windows Registry key:

```
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Desktop\Components
```

3.1.4 References

- Wikipedia: Active Desktop
- Sophos: Troj/DwnLdr-GWV

3.2 Activities Cache Database

Windows activity history keeps track of activity on a device, such as application and services usage, files opened, and websites browsed.

Windows uses the activity history data to provide you with personalized experiences (such as ordering your activities based on duration of use) and relevant suggestions (such as anticipating what your needs might be based on your activity history).

3.2.1 Significance

The Windows activity history can be used to determine system and user activity.

3.2.2 On-disk path

On-disk the Windows activity history is stored in a Activities Cache database. This SQLite database can be found in the following path:

```
C:\Users\%USERNAME%\AppData\Local\ConnectedDevicesPlatform\L.%USERNAME%\ActivitiesCache.
↪db
```

3.2.3 Versions

Windows activity history databases were first observed on Windows 10 1803.

3.2.4 References

- Windows 10 activity history and your privacy
- Salt Forensics: Windows 10 Timeline – Initial Review of Forensic Artefacts
- An examination of Win10 ActivitiesCache.db database

3.3 AMCache

The AMCache is an stores metadata about program installation and execution for Windows Application Compatibility.

The AMCache can be found on Windows 7 and Server 2008 R2 and later in the file:

```
C:\Windows\AppCompat\Programs\Amcache.hve
```

This file uses the Windows NT Registry File (REGF) format.

3.3.1 References

- ForensicsWiki: AMCache
- ForensicsWiki: Windows Application Compatibility
- Windows NT Registry File (REGF) format specification

3.4 Environment variables

3.4.1 References

- Wikipedia: Environment variable - Windows
- Recognized Environment Variables
- Driver Package Isolation - DriverData and ProgramData
- About User Profiles

APPX_PROCESS environment variable

- Beyond good ol' Run key, Part 17
- .NET Framework 4.6 allows side loading of Windows API Set DLL

Windows Registry environment variable expansion

- Expanding Environment Variables

3.5 Windows Event Log

The Windows Event Log is used by Microsoft Windows to store application and system logs. Typical Event Logs are: Application, System, and Security

Entries in Event Log files contain very little human-readable data. EventViewer, which is the Windows native Event Log viewing application, makes Event Log entries human-readable by combining pre-defined message string templates, which are stored in DLLs and EXEs, with variable data stored in the Event Log entry.

The combination of event identifier, its qualifiers and provider is needed to determine the message string template for a specific Event Log entry. Information about Windows Event Log providers can be found in the Windows Registry.

A common misconception is that event identifiers are globally unique, however they are only unique in the context of a specific version of a specific Log provider.

3.5.1 Windows NT4

On Windows NT4 the Event Logs files can be found in:

```
C:\WINNT\System32\config
```

Windows NT4 uses the Windows Event Log (EVT) format.

3.5.2 Windows 2000, XP and 2003

On Windows 2000, XP and 2003 the Event Logs files can be found in:

```
C:\Windows\System32\config
```

Windows 2000, XP and 2003 uses the Windows Event Log (EVT) format.

3.5.3 Windows Vista and later

On Windows Vista and later the Event Logs files can be found in:

```
C:\Windows\System32\winevt\Logs\
```

Windows Vista and later uses the Windows XML Event Log (EVTX) format.

3.5.4 References

- Wikipedia: Event Viewer
- Wikipedia: Log file
- ForensicsWiki: Windows Event Log (EVT)
- ForensicsWiki: Windows XML Event Log (EVTX)
- Windows Event Viewer Log (EVT) format
- Windows XML Event Log (EVTX) format
- EventLog keys
- Sysinternals Sysmon unleashed
- Export corrupts Windows Event Log files

3.6 Jump Lists

Jump Lists are a Windows Taskbar feature that gives the user quick access to recently accessed application files and actions.

Jump Lists were introduced in Windows 7

There are multiple variants of Jump Lists:

- AutomaticDestinations (*.automaticDestinations-ms) files
- CustomDestinations (*.customDestinations-ms) files

- Explorer StartPage2 ProgramsCache Registry values

3.6.1 AutomaticDestinations

The AutomaticDestinations Jump List files are located in the user profile path:

```
C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\*.
↪automaticDestinations-ms
```

3.6.2 CustomDestinations

The CustomDestinations Jump List files are located in the user profile path:

```
C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\*.
↪customDestinations-ms
```

3.6.3 Explorer StartPage2 ProgramsCache

The Explorer StartPage2 ProgramsCache Jump Lists are stored in the Windows Registry:

```
Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2
Value(s): ProgramsCacheSMP, ProgramsCacheTBP
```

3.6.4 References

- ForensicsWiki: Jump Lists
- dtFormats: Jump lists format
- WinReg-KB: Programs Cache values

3.7 Recent file cache

The recent file cache is an stores metadata about program installation and execution for Windows Application Compatibility.

The recent file cache can be found on Windows 7 in the file:

```
C:\Windows\AppCompat\Programs\RecentFileCache.bcf
```

3.7.1 References

- ForensicsWiki: Windows Application Compatibility
- RecentFileCache.bcf format

3.8 Windows Registry files

The Windows Registry is a hierarchical database that stores various settings for the Windows operating system and applications.

3.8.1 Windows 3.1

Windows 3.1 uses the SHCC Windows Registry file format

3.8.2 Windows 9x/Me

On Windows 95, 98 and Me the Windows Registry files can be found in:

```
%SystemRoot%\
```

Windows 95, 98 and Me uses the CREG Windows Registry file format

3.8.3 Windows NT4 and later

On Windows NT4 and later the Windows Registry files can be found in:

```
%SystemRoot%\System32\Config\
%UserProfile%\
%UserProfile%\Local Settings\Application Data\Microsoft\Windows\
%UserProfile%\AppData\Local\Microsoft\Windows\
```

Windows NT4 and later uses the REGF Windows Registry file format

3.8.4 References

- Wikipedia: Windows Registry
- Forensicswiki: Windows Registry
- WinReg-KB: Registry - Files
- The Windows NT Registry File Format
- Windows 9x Registry File (CREG) format specification
- Windows NT Registry File (REGF) format specification
- Windows registry file format specification

3.9 Services and drivers

3.9.1 Significance

Malware can add new services or drivers to gain persistence, or modify existing ones to avoid detection.

For example the ZeroAccess rootkit will make the following changes to the Windows Security Service Center (WSCSVC), Windows Defender (WINDEFEND), and Windows Firewall (MPSSVC) services, among others.

- Set the 'Start' value to 4, indicating that the service should be disabled
- Set the 'DeleteFlag' value to 1, indicating that the service should be removed
- Set the 'ErrorControl' value to 0 and 'Type' value to 32, causing it to fail to be started by the Service Controller without generating error messages

3.9.2 Settings

The services and drivers settings can be found in the Windows Registry key:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services
```

3.9.3 References

- Services and drivers

3.10 System Resource Usage Monitor (SRUM)

System Resource Usage Monitor (SRUM) is used to monitor desktop application programs, services, Windows applications and network connections.

3.10.1 SRUM extensions

3.10.2 Database

The SRUM database is typically stored in:

```
C:\Windows\System32\sru\SRUDB.dat
```

SRUM uses the Extensible Storage Engine (ESE) Database File (EDB) to store its folder data.

3.10.3 References

- System Resource Usage Monitor (SRUM) database
- SRUM forensics, by Yogesh Khatri