SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

Windows Forensic Analysis

POSTER

You Can't Protect What You Don't Know About

digital-forensics.sans.org

$25.00
DFPS_FOR500_v4.13_10-22
Poster Created by Rob Lee with support of the SANS DFIR Faculty

SANSForensics   @SANSForensics   dfir.to/DFIRCast   dfir.to/LinkedIn

Windows® Time Rules[1]

$STANDARD_INFORMATION

	File Creation	File Access	File Modification	File Rename	File Copy	Local File Move	Volume File Move *(move via CLI)*	Volume File Move *(cut/paste via Explorer)*	File Deletion
	Modified – Time of File Creation	Modified – No Change	Modified – Time of Data Modification	Modified – No Change	Modified – Inherited from Original	Modified – No Change	Modified – Inherited from Original	Modified – Inherited from Original	Modified – No Change
	Access – Time of File Creation	Access – Time of Access *(No Change on NTFS Volumes > 128 GB)*	Access – Time of Data Modification	Access – No Change	Access – Time of File Copy	Access – No Change	Access – Time of File Move via CLI	Access – Time of Cut/Paste	Access – No Change
	Metadata – Time of File Creation	Metadata – No Change	Metadata – Time of Data Modification	Metadata – Time of File Rename	Metadata – Time of File Copy	Metadata – Time of Local File Move	Metadata – Inherited from Original	Metadata – Inherited from Original	Metadata – No Change
	Creation – Time of File Creation	Creation – No Change	Creation – No Change	Creation – No Change	Creation – Time of File Copy	Creation – No Change	Creation – Time of File Move via CLI	Creation – Inherited from Original	Creation – No Change

$FILENAME

	File Creation	File Access	File Modification	File Rename	File Copy	Local File Move	Volume File Move *(move via CLI)*	Volume File Move *(cut/paste via Explorer)*	File Deletion
	Modified – Time of File Creation	Modified – No Change	Modified – No Change	Modified – No Change	Modified – Time of File Copy	Modified – No Change	Modified – Time of Move via CLI	Modified – Time of Cut/Paste	Modified – No Change
	Access – Time of File Creation	Access – No Change	Access – No Change	Access – No Change	Access – Time of File Copy	Access – No Change	Access – Time of Move via CLI	Access – Time of Cut/Paste	Access – No Change
	Metadata – Time of File Creation	Metadata – No Change	Metadata – No Change	Metadata – No Change	Metadata – Time of File Copy	Metadata – No Change	Metadata – Time of Move via CLI	Metadata – Time of Cut/Paste	Metadata – No Change
	Creation – Time of File Creation	Creation – No Change	Creation – No Change	Creation – No Change	Creation – Time of File Copy	Creation – No Change	Creation – Time of Move via CLI	Creation – Time of Cut/Paste	Creation – No Change

[1] Windows Time Rules based off of testing on Windows 10 Release version 1903

SANS Windows Artifact Analysis: Evidence of...

The "Evidence of..." categories were originally created by SANS Digital Forensics and Incidence Response faculty for the SANS course FOR500: Windows Forensic Analysis. The categories map a specific artifact to the analysis questions that it will help to answer. Use this poster as a cheat-sheet to help you remember where you can discover key Windows artifacts for computer intrusion, intellectual property theft, and other common cyber crime investigations.

Application Execution

Shimcache

Description

Windows Application Compatibility Database is used by Windows to identify possible application compatibility challenges with executables. It tracks the executable file path and binary last modified time.

Location

- **XP: SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatibility**
- **Win7+: SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache**

Interpretation

Any executable present in the file system could be found in this key. Data can be particularly useful to identify the presence of malware on devices where other application execution data is missing (such as Windows servers).

- Full path of executable
- Windows 7+ contains up to 1,024 entries (96 entries in WinXP)
- Post-WinXP no execution time is available
- Executables can be preemptively added to the database prior to execution. The existence of an executable in this key does not prove actual execution.

Task Bar Feature Usage

Description

It tracks how a user has interacted with the taskbar.

Location

Win 10 1903+: NTUSER\Software\Microsoft\Windows\CurrentVersion\Explorer\FeatureUsage

Interpretation

- Only tracks GUI applications
- Does not include timestamps
- AppLaunch tracks data only for pinned applications, showing user knowledge of the application
  - Data persists after an application is unpinned
- AppSwitched tracks a count of application focus, showing user interaction directed at the application
  - Not tied to pinned applications

Amcache.hve

Description

Amcache tracks installed applications, programs executed (or present), drivers loaded, and more. What sets this artifact apart is it also tracks the SHA1 hash for executables and drivers. (Available in Win7+)

Location

Win7/8/10: C:\Windows\AppCompat\Programs\Amcache.hve

Interpretation

- A complete registry hive, with multiple sub-keys
- Full path, file size, file modification time, compilation time, and publisher metadata
- SHA1 hash of executables and drivers
- Amcache should be used as an indication of executable and driver presence on the system, but not to prove actual execution.

Jump Lists

Description

Windows Jump Lists allow user access to frequently or recently used items quickly via the task bar. First introduced in Windows 7, they can identify applications in use and a wealth of metadata about items accessed via those applications.

Location

Win7/8/10: %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

Interpretation

- Each jump list file is named according to an application identifier (AppID). List of Jump List IDs -> **https://dfir.to/EZJumpList**
- Automatic Jump List Creation Time = First time an item added to the jump list. Typically, the first time an object was opened by the application.
- Automatic Jump List Modification Time = Last time item added to the jump list. Typically, the last time the application opened an object.

UserAssist

Description

UserAssist records metadata on GUI-based program executions.

Location

NTUSER.DAT HIVE: NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{GUID}\Count

Interpretation

- GUIDs identify type of execution (Win7+)
  - CEBFF5CD Executable File Execution
  - F4E57C4B Shortcut File Execution
- Values are ROT-13 Encoded
- Application path, last run time, run count, focus time and focus count

Windows 10 Timeline

Description

Win10 Timeline records recently used applications and files in a "timeline" database in a SQLite format.

Location

C:\Users\<profile>\AppData\Local\ConnectedDevicesPlatform\<account-iD>\ActivitiesCache.db

Interpretation

Full path of executed application

- Start time, end time, and duration
- Items opened within application
- URLs visited
- Databases still present even after feature deprecation in late-Win10

BAM/DAM

Description

Windows Background/Desktop Activity Moderator (BAM/DAM) is maintained by the Windows power management sub-system. (Available in Win10+)

Location

- **Win10: SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\{SID}**
- **Win10: SYSTEM\CurrentControlSet\Services\dam\State\UserSettings\{SID}**

Interpretation

Provides full path of file executed and last execution date/time

- Typically up to one week of data available
- "State" key used in Win10 1809+

System Resource Usage Monitor

Description

It records 30 to 60 days of historical system performance including applications run, user accounts responsible, network connections, and bytes sent/received per application per hour.

Location

C:\Windows\System32\SRU\SRUDB.dat

Interpretation

- SRUDB.dat is an Extensible Storage Engine database
- Three tables in SRUDB.dat are particularly important:
  - {973F5D5C-1D90-4944-BE8E-24B94231A174} = Network Data Usage
  - {d10ca2fe-6fcf-4f6d-848e-b2e99266fa89} = Application Resource Usage
  - {DD6636C4-8929-4683-974E-22C046A43763} = Network Connectivity Usage

Prefetch

Description

Prefetch increases performance of a system by pre-loading code pages of commonly used applications. It monitors all files and directories referenced for each application or process and maps them into a .pf file. It provides evidence that an application was executed.

- Limited to 128 files on XP and Win7
- Up to 1024 files on Win8+

Location

- **WinXP/7/8/10: C:\Windows\Prefetch**
  Naming format: (exename)-(hash).pf
- **WinXP/7/8/10: SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters**
  EnablePrefetcher value
  (0 = disabled; 3 = application launch and boot enabled)

Interpretation

- Date/Time file by that name and path was first executed
  - Creation date of .pf file (-10 seconds)
- Date/Time file by that name and path was last executed
  - Last modification date of .pf file (-10 seconds)
- Each .pf file includes embedded data, including the last eight execution times (only one time available pre-Win8), total number of times executed, and device and file handles used by the program.

CapabilityAccessManager

Description

It records application use of the microphone, camera, and other application-specific settings.

Location

- **Win 10 1903+: SOFTWARE\Microsoft\Windows\CurrentVersion\CapabilityAccessManager\ConsentStore**
- **Win 10 1903+: NTUSER\Software\Microsoft\Windows\CurrentVersion\CapabilityAccessManager\ConsentStore**

Interpretation

- LastUsedTimeStart and LastUsedTimeStop track the last session times.
- The NonPackaged key tracks non-Microsoft applications

Commands Executed in the Run Dialog

Description

It is a history of commands typed into the Run dialog box that are stored for each user.

Location

NTUSER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

Interpretation

It is an MRU key, so it has temporal order via the MRUList key.

Last-Visited MRU

Description

It tracks applications in use by the user and the directory location for the last file accessed by the application.

Location

- **XP: NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU**
- **Win7/8/10: NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU**

Interpretation

We get two important pieces of information from this key: applications executed by the user, and the last place in the file system that those applications interacted with. Interesting and hidden directories are often identified via this registry key.

System Information

Operating System Version

Description

Determine the operating system type, version, build number and installation dates for current installation and previous updates.

Location

- **SOFTWARE\Microsoft\Windows NT\CurrentVersion**
- **SYSTEM\Setup\Source OS**

Interpretation

CurrentVersion key stores:

- **ProductName, EditionID—**OS type
- **DisplayVersion, ReleaseId, CurrentBuildNumber—**Version info
- **InstallTime—**Installation time of current build (not original installation)

Source OS keys are created for each historical OS update:

- **ProductName, EditionID—**OS type
- **BuildBranch, ReleaseId, CurrentBuildNumber—**Version info
- **InstallTime—**Installation time of this build version
- **Times present in names of Source OS keys are extraneous:**
  InstallTime = 64-bit FILETIME format (Win10+)
  InstallDate = Unix 32-bit epoch format
  (both times should be equivalent)

Computer Name

Description

Stores the hostname of the system in the ComputerName value

Location

SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName

Interpretation

Hostname can facilitate correlation of log data and other artifacts.

System Boot and Autostart Programs

Description

Lists of programs that will run on system boot or at user login

Location

- **NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run**
- **NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\RunOnce**
- **SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce**
- **SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run**
- **SOFTWARE\Microsoft\Windows\CurrentVersion\Run**
- **SYSTEM\CurrentControlSet\Services**
  If Start value is set to 0x02, then service application will start at boot (0x00 for drivers)

Interpretation

- Useful to find malware and to audit installed software
- This is not an exhaustive list of autorun locations

System Last Shutdown Time

Description

It is the last time the system was shutdown. On Windows XP, the number of shutdowns is also recorded

Location

- **SYSTEM\CurrentControlSet\Control\Windows** (Shutdown Time)
- **SYSTEM\CurrentControlSet\Control\Watchdog\Display** (Shutdown Count – WinXP only)

Interpretation

- Determining last shutdown time can help to detect user behavior and system anomalies
- Windows 64-bit FILETIME format

Deleted Items and File Existence

Thumbs.db

Description

Hidden database file created in directories where images were viewed as thumbnails. It can catalog previous contents of a folder even upon file deletion.

Location

Each folder maintains a separate Thumbs.db file after being viewed in thumbnail view (OS version dependent)

Interpretation

Includes:

- Thumbnail image of original picture
- Last Modification Time (XP Only)
- Original Filename (XP Only)
- Most relevant for XP systems, but Thumbs.db files can be created on more modern OS versions in unusual circumstances such as when folders are viewed via UNC paths.

Windows Search Database

Description

Windows Search indexes more than 900 file types, including email and file metadata, allowing users to search based on keywords.

Location

Hidden System Folder

- **Win XP: C:\Documents and Settings\All Users\Application Data\ Microsoft\Search\Data\Applications\Windows\Windows.edb**
- **Win7+: C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb**
- **Win7+: C:\ProgramData\Microsoft\Search\Data\Applications\Windows\GatherLogs\SystemIndex**

Interpretation

- Database in Extensible Storage Engine format
- Gather logs contain a candidate list for files to be indexed over each 24 hour period
- Extensive file metadata and even partial content can be present

IE|Edge file:///

Description

Internet Explorer History databases have long held information on local and remote (via network s¬hares) file access, giving us an excellent means for determining files accessed on the system, per user. Information can be present even on Win11+ systems missing the Internet Explorer application.

Location

- **IE6-7: %USERPROFILE%\LocalSettings\History\History.IE5**
- **IE8-9: %USERPROFILE%\AppData\Local\Microsoft\Windows\History\History.IE5**
- **IE10-11 and Win10+: %USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat**

Interpretation

- Entries are recorded as: **file:///C:/<directory>/<filename>.<ext>**
- It does not mean the file was opened in a browser

Search – WordWheelQuery

Description

Maintains an ordered list of terms input into the File Explorer search dialog

Location

Win7+: NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery

Interpretation

Keywords are added in Unicode and listed in temporal order in an MRUlist

User Typed Paths

Description

A user can type a path directly into the File Explorer path bar to locate a file instead of navigating the folder structure. Folders accessed in this manner are recorded in the TypedPaths key.

Location

NTUSER\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths

Interpretation

- This indicates a user had knowledge of a particular file system location
- It can expose hidden and commonly accessed locations, including those present on external drives or network shares

Thumbcache

Description

Thumbnails of pictures, documents, and folders exist in a set of databases called the thumbcache. Maintained for each user based on the thumbnail sizes viewed (e.g., small, medium, large, and extra large). It can catalog previous contents of a folder even upon file deletion. Available in Windows Vista+

Location

C:\%USERPROFILE%\AppData\Local\Microsoft\Windows\Explorer

Interpretation

- Database files are named similar to: Thumbcache_256.db
- Each database file represents thumbnails stored as different sizes or to fit different user interface components
- Thumbnail copies of pictures can be extracted and the Thumbnail Cache ID can be cross-referenced within the Windows Search Database to identify filename, path, and additional file metadata.

Recycle Bin

Description

The recycle bin collects items soft-deleted by each user and associated metadata. Only relevant for recycle-bin aware applications.

Location

- **Win XP: C:\Recycler**
- **Win7+: C:\$Recycle.Bin**

Interpretation

- Each user is assigned a SID sub-folder that can be mapped to a user via the Registry
- **XP:** INFO2 database contains deletion times and original filenames
- **Win7+:** Files preceded by $I###### files contain original filename and deletion date/time
- **Win7+:** Files preceded by $R###### files contain original deleted file contents

SANS DFIR CURRICULUM

@SANSForensics   dfir.to/DFIRCast   dfir.to/LinkedIn

OPERATING SYSTEM & DEVICE IN-DEPTH

FOR308
Digital Forensics Essentials

FOR498
Battlefield Forensics & Data Acquisition
GBFA

FOR500
Windows Forensic Analysis
GCFE

FOR518
Mac and iOS Forensic Analysis & Incident Response
GIME

FOR585
Smartphone Forensic Analysis In-Depth
GASF

INCIDENT RESPONSE & THREAT HUNTING

FOR508
Advanced Incident Response, Threat Hunting & Digital Forensics
GCFA

FOR509
Enterprise Cloud Forensics & Incident Response
GCFR

FOR528
Ransomware for Incident Responders

FOR572
Advanced Network Forensics: Threat Hunting, Analysis & Incident Response
GNFA

FOR578
Cyber Threat Intelligence
GCTI

FOR608
Enterprise-Class Incident Response & Threat Hunting

FOR610
REM: Malware Analysis Tools & Techniques
GREM

FOR710
Reverse-Engineering Malware: Advanced Code Analysis

SEC504
Hacker Tools, Techniques & Incident Handling
GCIH

Network Activity/Physical Location

Timezone

Description

It identifies the current system time zone.

Location

SYSTEM Hive: SYSTEM\CurrentControlSet\Control\TimeZoneInformation

Interpretation

- Time activity is incredibly useful for correlation of activity
- Internal log files and date/timestamps will be based on the system time zone information
- You might have other network devices and you will need to correlate information to the time zone information collected here.

Network History

Description

Network History identifies networks that the computer has been connected to.

- Networks could be wireless or wired
- Identify domain name/intranet name
- Identify SSID
- Identify Gateway MAC Address

Location

Win7/8/10 SOFTWARE HIVE:

- **SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged**
- **SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed**
- **SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Cache**

Interpretation

- Identifying intranets and networks that a computer has connected to is incredibly important
- Not only can you determine the intranet name, you can determine the last time the network was connected to it based on the last write time of the key
- This will also list any networks that have been connected to via a VPN
- MAC Address of SSID for Gateway could be physically triangulated

Cookies

Description

Cookies give insight into what websites have been visited and what activities may have taken place there.

Location

Internet Explorer

- **IE6-8: %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Cookies**
- **IE10: %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Cookies**
- **IE11: %USERPROFILE%\AppData\Local\Microsoft\Windows\INetCookies**

Firefox

- **XP: %USERPROFILE%\Application Data\Mozilla\Firefox\Profiles\<random text>.default\cookies.sqlite**
- **Win7/8/10: %USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\cookies.sqlite**

Chrome

- **XP: %USERPROFILE%\Local Settings\ApplicationData\Google\Chrome\User Data\Default\Local Storage**
- **Win7/8/10: %USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\Local Storage**

WLAN Event Log

Description

It determines what wireless networks the system is associated with and identifies network characteristics to find the location.

Relevant Event IDs

- 11000 – Wireless network association started
- 8001 – Successful connection to wireless network
- 8002 – Failed connection to wireless network
- 8003 – Disconnect from wireless network
- 6100 – Network diagnostics (System log)

Location

Microsoft-Windows-WLAN-AutoConfig Operational.evtx

Interpretation

- Shows historical record of wireless network connections
- Contains SSID and BSSID (MAC address), which can be used to geolocate wireless access point *(no BSSID on Win8+)

Browser Search Terms

Description

Records websites visited by date and time. Details stored for each local user account. Records number of times visited (frequency). Also tracks access of local system files. This will also include the website history of search terms in search engines.

Location

Internet Explorer

- **IE6-7: %USERPROFILE%\Local Settings\History\History.IE5**
- **IE8-9: %USERPROFILE%\AppData\Local\Microsoft\Windows\History\History.IE5**
- **IE10-11: %USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat**

Firefox

- **XP: %userprofile%\Application Data\Mozilla\Firefox\Profiles\<randomtext>.default\places.sqlite**
- **Win7/8/10: %userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\places.sqlite**

System Resource Usage Monitor

Description

It records 30 to 60 days of historical system performance including applications run, user accounts responsible, network connections, and bytes sent/received per application per hour.

Location

- **SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SRUM\Extensions**
- **{973F5D5C-1D90-4944-BE8E-24B94231A174} = Windows Network Data Usage Monitor**
- **{DD6636C4-8929-4683-974E-22C046A43763} = Windows Network Connectivity Usage Monitor**
- **SOFTWARE\Microsoft\WlanSvc\Interfaces\**
- **C:\Windows\System32\SRU\**

Interpretation

Use tool such as **srum_dump.exe** to cross correlate the data between the registry keys and the SRUM ESE Database.

File/Folder Opening

Open/Save MRU

Description

In the simplest terms, this key tracks files that have been opened or saved within a Windows shell dialog box. This happens to be a big data set, not only including web browsers like Internet Explorer and Firefox, but also a majority of commonly used applications.

Location

- **XP: NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU**
- **Win7/8/10: NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDlMRU**

Interpretation

- **The "*" key –** This subkey tracks the most recent files of any extension input in an OpenSave dialog
- **.??? (Three letter extension) –** This subkey stores file info from the OpenSave dialog by specific extension

Recent Files

Description

Registry Key that will track the last files and folders opened and is used to populate data in "Recent" menus of the Start menu.

Location

NTUSER.DAT: NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

Interpretation

- **RecentDocs –** Overall key will track the overall order of the last 150 files or folders opened. MRU list will keep track of the temporal order in which each file/folder was opened. The last entry and modification time of this key will be the time and location the last file of a specific extension was opened.
- **.??? –** This subkey stores the last files with a specific extension that were opened. MRU list will keep track of the temporal order in which each file was opened. The last entry and modification time of this key will be the time when and location where the last file of a specific extension was opened.
- **Folder –** This subkey stores the last folders that were opened. MRU list will keep track of the temporal order in which each folder was opened. The last entry and modification time of this key will be the time and location of the last folder opened.

Jump Lists

Description

The Windows 7 task bar (Jump List) is engineered to allow users to "jump" or access items have frequently or recently used quickly and easily. This functionality cannot only include recent media files; it must also include recent tasks. The data stored in the AutomaticDestinations folder will each have a unique file prepended with the AppID of the association application and embedded with LNK files in each stream.

Location

Win7/8/10: C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

Interpretation

- Using the Structured Storage Viewer, open up one of the AutomaticDestination jumplist files.
- Each one of these files is a separate LNK file. They are also stored numerically in order from the earliest one (usually 1) to the most recent (largest integer value).

Shell Bags

Description

It identifies which folders were accessed on the local machine, the network, and/or removable devices. It also shows evidence of previously existing folders after deletion/overwrite and when certain folders were accessed.

Location

Explorer Access:

- **USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags**
- **USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU**

Desktop Access:

- **NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU**
- **NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags**

Interpretation

Stores information about which folders were most recently browsed by the user.

Shortcut (LNK) Files

Description

Shortcut Files are automatically created by Windows with recent items. Opening local and remote data files and documents will generate a shortcut file (.lnk)

Location

- **XP: C:\%USERPROFILE%\Recent**
- **Win7/8/10: C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\**
- **Win7/8/10: C:\%USERPROFILE%\AppData\Roaming\Microsoft\Office\Recent\**

Note these are primary locations of LNK files. They can also be found in other locations.

Interpretation

- Date/Time file of that name was first opened
  - Creation Date of Shortcut (LNK) File
- Date/Time file of that name was last opened
  - Last Modification Date of Shortcut (LNK) File
- LNKTarget File (Internal LNK File Information) Data:
  - Modified, Access, and Creation times of the target file
  - Volume Information (Name, Type, Serial Number)
  - Network Share information
  - Original Location
  - Name of System

Prefetch

Description

It increases performance of a system by pre-loading code pages of commonly used applications. Cache Manager monitors all files and directories referenced for each application or process and maps them into a .pf file. Utilized to know an application was executed on a system.

- Limited to 128 files on XP and Win7
- Limited to 1024 files on Win8-10
- (exename)-(hash).pf

Location

WinXP/7/8/10: C:\Windows\Prefetch

Interpretation

- Can examine each .pf file to look for file handles recently used
- Can examine each .pf file to look for device handles recently used

Last-Visited MRU

Description

Tracks the specific executable used by an application to open the files documented in the OpenSaveMRU key. In addition, each value also tracks the directory location for the last file that was accessed by that application.

Example: Notepad.exe was last run using the `C:\Users\Rob\Desktop` folder

Location

- **XP: NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU**
- **Win7/8/10: NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\ LastVisitedPidlMRU**

Interpretation

Tracks the application executables used to open files in OpenSaveMRU and the last file path used.

IE|Edge file://

Description

A little known fact about the IE History is that the information stored in the history files is not just related to Internet browsing. The history also records local, removable, and remote (via network shares) file access, giving us an excellent means for determining which files and applications were accessed on the system, day by day.

Location

Internet Explorer:

- **IE6-7: %USERPROFILE%\Local Settings\History\ History.IE5**
- **IE8-9: %USERPROFILE%\AppData\Local\Microsoft\Windows\History\History.IE5**
- **IE10-11: %USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat**

Interpretation

- Stored in index.dat as: **file:///C:/directory/filename.ext**
- Does not mean file was opened in browser

Office Recent Files

Description

MS Office programs will track their own Recent Files list to make it easier for users to remember the last file they were editing.

Location

NTUSER.DAT\Software\Microsoft\Office\VERSION

- 14.0 = Office 2010
- 12.0 = Office 2007
- 11.0 = Office 2003
- 10.0 = Office XP

NTUSER.DAT\Software\Microsoft\Office\VERSION\UserMRU\LiveID_####\FileMRU

- 15.0 = Office 365

Interpretation

Similar to the Recent Files, this will track the last files that were opened by each MS Office application. The last entry added, per the MRU, will be the time the last file was opened by a specific MS Office application.

Account Usage

Last Login

Description

Lists the local accounts of the system and their equivalent security identifiers.

Location

- **C:\windows\system32\config\SAM**
- **SAM\Domains\Account\Users**

Interpretation

- Only the last login time will be stored in the registry key

Last Password Change

Description

Lists the last time the password of a specific local user has been changed.

Location

- **C:\windows\system32\config\SAM**
- **SAM\Domains\Account\Users**

Interpretation

- Only the last password change time will be stored in the registry key

RDP Usage

Description

Track Remote Desktop Protocol logons to target machines.

Location Security Log

Win7/8/10:
%SYSTEM ROOT%\System32\winevt\logs\Security.evtx

Interpretation

- Win7/8/10 – Interpretation
  - Event ID 4778 – Session Connected/Reconnected
  - Event ID 4779 – Session Disconnected
- Event log provides hostname and IP address of remote machine making the connection
- On workstations you will often see current console session disconnected (4779) followed by RDP connection (4778)

Services Events

Description

- Analyze logs for suspicious services running at boot time
- Review services started or stopped around the time of a suspected compromise

Location

All Event IDs reference the System Log

7034 – Service crashed unexpectedly

7035 – Service sent a Start/Stop control

7036 – Service started or stopped

7040 – Start type changed (Boot | On Request | Disabled)

7045 – A service was installed on the system (Win2008R2+)

4697 – A service was installed on the system (from Security log)

Interpretation

- All Event IDs except 4697 reference the System Log
- A large amount of malware and worms in the wild utilize Services
- Services started on boot illustrate persistence (desirable in malware)
- Services can crash due to attacks like process injection

Logon Types

Description

Logon Events can give us very specific information regarding the nature of account authorizations on a system if we know where to look and how to decipher the data that we find. In addition to telling us the date, time, username, hostname, and success/failure status of a logon, Logon Events also enables us to determine by exactly what means a logon was attempted.

Location

Win7/8/10:
Event ID 4624

Interpretation

Logon Type	Explanation
2	Logon via console
3	Network Logon
4	Batch Logon
5	Windows Service Logon
7	Credentials used to unlock screen
8	Network logon sending credentials (cleartext)
9	Different credentials used than logged on user
10	Remote interactive logon (RDP)
11	Cached credentials used to logon
12	Cached remote interactive (similar to Type 10)
13	Cached unlock (similar to Type 7)

Authentication Events

Description

Authentication mechanisms

Location

Recorded on system that authenticated credentials

Local Account/Workgroup = on workstation

Domain/Active Directory = on domain controller

Win7/8/10:
`%SYSTEM ROOT%\System32\winevt\logs\Security.evtx`

Interpretation

Event ID Codes (NTLM protocol)

- 4776: Successful/Failed account authentication

Event ID Codes (Kerberos protocol)

- 4768: Ticket Granting Ticket was granted (successful logon)
- 4769: Service Ticket requested (access to server resource)
- 4771: Pre-authentication failed (failed logon)

Success/Fail Logons

Description

Determine which accounts have been used for attempted logons. Track account usage for known compromised accounts.

Location

Win7/8/10:
%system root%\System32\winevt\logs\Security.evtx

Interpretation

- Win7/8/10 – Interpretation
- 4624 – Successful Logon
- 4625 – Failed Logon
- 4634 | 4647 – Successful Logoff
- 4648 – Logon using explicit credentials (Runas)
- 4672 – Account logon with superuser rights (Administrator)
- 4720 – An account was created

External Device/USB Usage

Key Identification

Description

It tracks USB devices plugged into a machine.

Location

- **SYSTEM\CurrentControlSet\Enum\USBSTOR**
- **SYSTEM\CurrentControlSet\Enum\USB**

Interpretation

- Identify vendor, product, and version of a USB device plugged into a machine
- Identify a unique USB device plugged into the machine
- Determine the time a device was plugged into the machine
- Devices that do not have a unique serial number will have an "&" in the second character of the serial number.

First/Last Times

Description

This determines temporal usage of specific USB devices connected to a Windows Machine.

Location *First Time*

Plug and Play Log Files

- **XP: C:\Windows\setupapi.log**
- **Win7/8/10: C:\Windows\inf\setupapi.dev.log**

Interpretation

- Search for Device Serial Number
- Log File times are set to local time zone

Location *First, Last, and Removal Times (Win7/8/10 Only)*

System Hive:
\CurrentControlSet\Enum\USBSTOR\Ven_Prod_Version\USBSerial#\Properties\{83da6326-97a6-4088-9453-a19231573b29}\####

- 0064 = First Install (Win7-10)
- 0066 = Last Connected (Win8-10)
- 0067 = Last Removal (Win8-10)

User

Description

Find User that used the Unique USB Device.

Location

- Look for GUID from **SYSTEM\MountedDevices**
- **NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2**

Interpretation

This GUID will be used next to identify the user that plugged in the device. The last write time of this key also corresponds to the last time the device was plugged into the machine by that user. The number will be referenced in the user's personal mountpoints key in the NTUSER.DAT Hive.

PnP Events

Description

When a Plug and Play driver install is attempted, the service will log an ID 20001 event and provide a Status within the event. It is important to note that this event will trigger for any Plug and Play-capable device, including but not limited to USB, Firewire, and PCMCIA devices.

Location *System Log File*

Win7/8/10: %system root%\System32\winevt\logs\System.evtx

Interpretation

- Event ID: 20001 – Plug and Play driver install attempted
- Event ID 20001
- Timestamp
- Device information
- Device serial number
- Status (0 = no errors)

Volume Serial Number

Description

Discover the Volume Serial Number of the Filesystem Partition on the USB. (NOTE: This is not the USB Unique Serial Number, which is hardcoded into the device firmware.)

Location

- **SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ENDMgmt**
- Use Volume Name and USB Unique Serial Number to:
  - Find last integer number in line
  - Convert Decimal Serial Number into Hex Serial Number

Interpretation

- Knowing both the Volume Serial Number and the Volume Name, you can correlate the data across SHORTCUT File (LNK) analysis and the RECENTDOCs key.
- The Shortcut File (LNK) contains the Volume Serial Number and Name
- RecentDocs Registry Key, in most cases, will contain the volume name when the USB device is opened via Explorer

Drive Letter and Volume Name

Description

Discover the last drive letter of the USB Device when it was plugged into the machine.

Location

- **XP:** Find **ParentIdPrefix** – **SYSTEM\CurrentControlSet\Enum\USBSTOR**
- Using **ParentIdPrefix** Discover Last Mount Point – **SYSTEM\MountedDevices**
- **Win7/8/10: SOFTWARE\Microsoft\Windows Portable Devices\Devices**
- **Win7/8/10: SYSTEM\MountedDevices**
  - Examine Drive Letters looking at Value Data Looking for Serial Number

Interpretation

Identify the USB device that was last mapped to a specific drive letter. This technique will only work for the last drive mapped. It does not contain historical records of every drive letter mapped to a removable drive.

Shortcut (LNK) Files

Description

Shortcut Files are automatically created by Windows with recent items. Opening local and remote data files and documents will generate a shortcut file (.lnk)

Location

- **XP: C:\%USERPROFILE%\Recent**
- **Win7/8/10: C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\**
- **Win7/8/10: C:\%USERPROFILE%\AppData\Roaming\Microsoft\Office\Recent\**

Note these are primary locations of LNK files. They can also be found in other locations.

Interpretation

- Date/Time file of that name was first opened
  - Creation Date of Shortcut (LNK) File
- Date/Time file of that name was last opened
  - Last Modification Date of Shortcut (LNK) File
- LNKTarget File (Internal LNK File Information) Data:
  - Modified, Access, and Creation times of the target file
  - Volume Information (Name, Type, Serial Number)
  - Network Share information
  - Original Location
  - Name of System

Browser Usage

History

Description

It records websites visited by date and time. The details are stored for each local user account and records the number of times visited (frequency). It also tracks access of local system files.

Location

Internet Explorer

- **IE6-7: %USERPROFILE%\Local Settings\History\History.IE5**
- **IE8-9: %USERPROFILE%\AppData\Local\Microsoft\Windows\History\History.IE5**
- **IE10, 11, Edge: %USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat**

Firefox

- **XP: %USERPROFILE%\Application Data\Mozilla\Firefox\Profiles\<random text>.default\places.sqlite**
- **Win7/8/10: %USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<random text>.default\places.sqlite**

Chrome

- **XP: %USERPROFILE%\Local Settings\Application Data\Google\Chrome\User Data\Default\History**
- **Win7/8/10: %USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\History**

Cookies

Description

Cookies give insight into what websites have been visited and what activities may have taken place there.

Location

Internet Explorer

- **IE6-8: %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Cookies**
- **IE10: %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Cookies**
- **IE11: %USERPROFILE%\AppData\Local\Microsoft\Windows\INetCookies**

Firefox

- **XP: %USERPROFILE%\Application Data\Mozilla\Firefox\Profiles\<random text>.default\cookies.sqlite**
- **Win7/8/10: %USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\cookies.sqlite**

Chrome

- **XP: %USERPROFILE%\Local Settings\ApplicationData\Google\Chrome\User Data\Default\Local Storage**
- **Win7/8/10: %USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\Local Storage**

Cache

Description

The cache is where web page components can be stored locally to speed up subsequent visits. It gives the investigator a "snapshot in time" of what a user was looking at online.

- Identifies websites which were visited
- Provides the actual files the user viewed on a given website
- Cached files are tied to a specific local user account
- Timestamps show when the site was first saved and last viewed

Location

Internet Explorer

- **IE8-9: %USERPROFILE%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5**
- **IE10: %USERPROFILE%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5**
- **IE11: %USERPROFILE%\AppData\Local\Microsoft\Windows\INetCache\IE**
- **Edge: %USERPROFILE%\AppData\Local\Packages\microsoft.microsoftedge_<APPID>\AC\MicrosoftEdge\Cache**

Firefox

- **XP: %USERPROFILE%\Local Settings\ApplicationData\Mozilla\Firefox\Profiles\<randomtext>.default\Cache**
- **Win7/8/10: %USERPROFILE%\AppData\Local\Mozilla\Firefox\Profiles\<randomtext>.default\Cache**

Chrome

- **XP: %USERPROFILE%\Local Settings\Application Data\Google\Chrome\User Data\Default\Cache - data_# and f_######**
- **Win7/8/10: %USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\Cache\ - data_# and f_######**

Flash & Super Cookies

Description

Local Stored Objects (LSOs), or Flash Cookies, have become ubiquitous on most systems due to the extremely high penetration of Flash applications across the Internet. They tend to be much more persistent because they do not expire, and there is no built-in mechanism within the browser to remove them. In fact, many sites have begun using LSOs for their tracking mechanisms because they rarely get cleared like traditional cookies.

Location

Win7/8/10: %APPDATA%\Roaming\Macromedia\FlashPlayer\#SharedObjects\<randomprofileid>

Interpretation

- Websites visited
- User account used to visit the site
- When cookie was created and last accessed

Session Restore

Description

Automatic Crash Recovery features built into the browser.

Location

Internet Explorer

- **Win7/8/10: %USERPROFILE%/AppData/Local/Microsoft/Internet Explorer/Recovery**

Firefox

- **Win7/8/10: %USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\sessionstore.js**

Chrome

- **Win7/8/10: %USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\**
  Files = Current Session, Current Tabs, Last Session, Last Tabs

Interpretation

- Historical websites viewed in each tab
- Referring websites
- Time session ended
- Modified time of .dat files in LastActive folder
- Time each tab opened (only when crash occurred)
- Creation time of .dat files in Active folder

Google Analytics Cookies

Description

Google Analytics (GA) has developed an extremely sophisticated methodology for tracking site visits, user activity, and paid search. Since GA is largely free, it has a commanding share of the market, estimated at over 80% of sites using traffic analysis and over 50% of all sites.

__utma – Unique visitors

- Domain Hash
- Visitor ID
- Cookie Creation Time
- Time of 2nd most recent visit
- Time of most recent visit
- Number of visits

__utmb – Session tracking

- Domain hash
- Page views in current session
- Outbound link clicks
- Time current session started

__utmz – Traffic sources

- Domain Hash
- Last Update time
- Number of visits
- Number of different types of visits
- Source used to access site
- Google Adwords campaign name
- Access Method (organic, referral, cpc, email, direct)
- Keyword used to find site (non-SSL only)