SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

Windows Forensic Analysis

POSTER

Master Windows Forensics – You Can't Protect the Unknown

digital-forensics.sans.org

$25.00
DFPS_FOR500_v4.14_12-22
Poster created thanks to the support and contributions of the
SANS DFIR Faculty ©2022 SANS Institute. All Rights Reserved

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

Windows® Time Rules[1]

$Standard_Information Win10 v1903

File Creation	File Access	File Modification	File Rename	File Copy (new file)	Local File Move	Volume File Move (move via CLI)	Volume File Move (cut/paste via Explorer)	File Deletion (shift+delete)
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 if System Volume > 128 GiB)	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

$Standard_Information Win11 v22H2

File Creation	File Access	File Modification	File Rename	File Copy (new file)	Local File Move	Volume File Move (move via CLI)	Volume File Move (cut/paste via Explorer)	File Deletion (shift+delete)
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	Access – Time of Data Modification[2]	Access – Time of Rename[2]	Access – Time of File Copy	Access – Time of Local File Move	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 – Inherited from Original	Metadata – Time of Local File Move	Metadata – Time of File 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 File Move via CLI	Creation – Inherited from Original	Creation – No Change

[1] Windows timestamp updates are notoriously dependent on the operating system version and a very specific combination of actions. These charts illustrate the differences between Windows 10 v1903 and Windows 11 v22H2. Use these rules as heuristics indicating common actions, but always perform testing of specific actions on specific OS versions when working with critical evidence. Reference https://www.khyrenz.com/blog/windows-11-time-rules/ for additional context.

[2] Access times in Windows 11 should be considered approximate as they were sometimes noted to differ by up to a few seconds from the actual time of activity.

SANS Windows Artifact Analysis: Evidence of...

The "Evidence of..." categories were originally created by SANS Digital Forensics and Incident Response faculty for the SANS course FOR500: Windows Forensic Analysis. The categories map specific artifacts to the analysis questions they can help to answer. Use this poster as a cheat sheet to remember and discover important Windows operating system artifacts relevant to investigations into computer intrusions, insider threats, fraud, employee misuse, and other common cybercrimes.

Application Execution

Shimcache

Description

The 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

Task Bar Feature Usage 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

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

%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.

Last Visited MRU

Description

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+: 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.

Commands Executed in the Run Dialog

Description

A history of commands typed into the Run dialog box 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

Windows 10 Timeline

Description

Win10 records recently used applications and files in a "timeline" database in 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

- **SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\{SID}**
- **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 (SRUM)

Description

SRUM 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

Win8+: **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

- **C:\Windows\Prefetch**
  Naming format: (exename)-(hash).pf
- **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

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

UserAssist

Description

UserAssist records metadata on GUI-based program executions.

Location

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

File and 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, including Microsoft Office applications, web browsers, chat clients, and 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 tracking the last files and folders opened. Used to populate data in places like the "Recent" menus present in some Start menus.

Location

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

Interpretation

- **RecentDocs –** Rollup key tracking the overall order of the last 150 files or folders opened. MRU list tracks the temporal order in which each file/folder was opened.
- **.??? –** These subkeys store the last 20 files opened by the user of each extension type. MRU list tracks the temporal order in which each file was opened. The most recently used (MRU) item is associated with the last write time of the key, providing one timestamp of file opening for each file extension type.
- **Folder –** This subkey stores the last 30 folders opened by the user. The most recently used (MRU) item in this key is associated with the last write time of the key, providing the time of opening for that folder.

MS Word Reading Locations

Description

Beginning with Word 2013, the last known position of the user within a Word document is recorded.

Location

NTUSER\Software\Microsoft\Office\<Version>\Word\Reading Locations

Interpretation

- Another source tracking recent documents opened
- The last closed time is also tracked along with the last position within the file
- Together with the last opened date in the Office File MRU key, a last session duration can be determined

Last Visited MRU

Description

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+: **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.

Shortcut (LNK) Files

Description

Shortcut files are automatically created by Windows, tracking files and folders opened by a user.

Location

- XP: **%USERPROFILE%\Recent**
- Win7+: **%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\**
- Win7+: **%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
- LNK Target 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

Office Recent Files

Description

MS Office programs track their own recent files list, to make it easier for users to access previously opened files.

Location

- **NTUSER.DAT\Software\Microsoft\Office\<Version>\<AppName>\File MRU**

- 16.0 = Office 2016/2019/M365	- 12.0 = Office 2007
- 15.0 = Office 2013	- 11.0 = Office 2003
- 14.0 = Office 2010	- 10.0 = Office XP

- **NTUSER.DAT\Software\Microsoft\Office\<Version>\UserMRU\LiveID_####\File MRU**
  - Microsoft 365
- **NTUSER.DAT\Software\Microsoft\Office\<Version>\UserMRU\ADAL_####\File MRU**
  - Microsoft 365 (Azure Active Directory)

Interpretation

- Similar to the Recent Files registry key, this tracks the last files opened by each MS Office application
- Unlike the Recent Files registry key, full path information is recorded along with a last opened time for each entry

Shell Bags

Description

Shell bags identifies which folders were accessed on the local machine, via the network, and on removable devices, per user. It also shows evidence of previously existing folders still present after deletion/overwrite.

Location

Primary Data:

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

Residual Desktop Items and Network Shares:

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

Interpretation

- Massive collection of data on folders accessed by each user
- Folder file system timestamps are archived in addition to first and last interaction times
- "Exotic" items recorded like mobile device info, control panel access, and Zip archive access

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

- **%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations**
- **%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations**

Interpretation

- Each jump list file is named according to an application identifier (AppID). List of Jump List IDs -> https://dfir.to/EZJumpList
- Each Jump List contains a collection of items interacted with (up to ~2000 items per application)
- Each entry is represented as a LNK shell item providing additional data
  - Target Timestamps
  - File Size
  - Local Drive | Removable Media | Network Share Info
  - Entries kept in MRU order including a timestamp for each item

Office Trust Records

Description

Records trust relationships afforded to documents by a user when presented with a security warning. This is stored so the user is only required to grant permission the first time the document is opened.

Location

NTUSER\Software\Microsoft\Office\<Version>\<AppName>\Security\Trusted Documents\TrustRecords

Interpretation

- Can identify documents opened by the user and user interaction in trusting the file
- Records file path, time the document was trusted, and which permissions were granted

Office OAlerts

Description

MS Office programs produce alerts for the user when they attempt actions such as closing a file without saving it first.

Location

OAlerts.evtx

Interpretation

- All Office applications use Event ID 300
- Events include the program name and dialog message, showing some user activity within the application

Internet Explorer file:///

Description

Internet Explorer History databases have long held information on local and remote file access (via network shares), 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

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

Interpretation

- Entries recorded as: **file:///C:/directory/filename.ext**
- Does not mean file was opened in a browser

Deleted Items and File Existence

Thumbs.db

Description

The hidden database file is 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

- **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

Internet Explorer file:///

Description

Internet Explorer History databases have long held information on local and remote (via network shares) 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

This maintains an ordered list of terms put 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. It is 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

%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

Hidden System Folder

- 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 **$I######** contain original filename and deletion date/time
- Win7+: Files preceded by **$R######** 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

Browser Activity

History and Download History

Description
History and Download History records websites visited by date and time.

Location
Firefox
- XP: **%USERPROFILE%\Application Data\Mozilla\Firefox\Profiles\<randomtext>.default\places.sqlite**
- Win7+: **%USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<random text>.default\places.sqlite**

Chrome/Edge
- XP: **%USERPROFILE%\Local Settings\Application Data\Google\Chrome\User Data\<Profile>\History**
- Win7+: **%USERPROFILE%\AppData\Local\Google\Chrome\User Data\<Profile>\History**
- Win7+: **%USERPROFILE%\AppData\Local\Microsoft\Edge\User Data\<Profile>\History**

Interpretation
- Web browser artifacts are stored for each local user account
- Most browsers also record number of times visited (frequency)
- Look for multiple profiles in Chromium browsers, including "Default", and "Profile1", etc.

Media History

Description
Media History tracks media usage (audio and video played) on visited websites (Chromium browsers).

Location
Chrome/Edge
- **%USERPROFILE%\AppData\Local\Google\Chrome\User Data\<Profile>\Media History**
- **%USERPROFILE%\AppData\Local\Microsoft\Edge\User Data\<Profile>\Media History**

Interpretation
- Three primary tables: playbackSession, origin, playback
- Includes URLs, last play time, watch time duration, and last video position
- Not cleared when other history data is cleared

HTML5 Web Storage

Description
HTML5 Web Storage are considered to be "Super Cookies". Each domain can store up to 10MB of text-based data on the local system.

Location
Firefox
- **%USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\webappstore.sqlite**

Chrome/Edge
- **%USERPROFILE%\AppData\Local\Google\Chrome\User Data\<Profile>\Local Storage**
- **%USERPROFILE%\AppData\Local\Microsoft\Edge\User Data\<Profile>\Local Storage**

Interpretation
Chrome uses a LevelDB database, Firefox uses SQLite, and IE/EdgeHTML store data within XML files

HTML5 FileSystem

Description
HTML5 FileSystem implements the HTML5 local storage FileSystem API. It is similar to Web Storage, but designed to store larger binary data.

Location
Chrome/Edge
- **%USERPROFILE%\AppData\Local\Google\Chrome\User Data\<Profile>\File System**
- **%USERPROFILE%\AppData\Local\Microsoft\Edge\User Data\<Profile>\File System**

Interpretation
- A LevelDB database in this folder stores visited URLs and assigned subfolders to locate the data
- Files are stored temporarily ("t" subfolders) or in permanent ("p" subfolders) storage

Auto-Complete Data

Description
Many databases store data that a user has typed into the browser.

Location
Firefox
- **%USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\places.sqlite**
- **%USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\formhistory.sqlite**

Chrome/Edge
- **%USERPROFILE%\AppData\Local\Google\Chrome\User Data\<Profile>\History**
- **%USERPROFILE%\AppData\Local\Microsoft\Edge\User Data\<Profile>\History**
  - keyword_search_terms – items typed into various search engines
- **%USERPROFILE%\AppData\Local\Google\Chrome\User Data\<Profile>\Web Data**
- **%USERPROFILE%\AppData\Local\Microsoft\Edge\User Data\<Profile>\ Web Data**
  - Items typed into web forms
- **%USERPROFILE%\AppData\Local\Google\Chrome\User Data\<Profile>\Shortcuts**
- **%USERPROFILE%\AppData\Local\Microsoft\Edge\User Data\<Profile>\ Shortcuts**
  - Items typed in the Chrome URL address bar (Omnibox)
- **%USERPROFILE%\AppData\Local\Google\Chrome\User Data\<Profile>\Network Action Predictor**
- **%USERPROFILE%\AppData\Local\Microsoft\Edge\User Data\<Profile>\ Network Action Predictor**
  - Records what was typed, letter by letter
- **%USERPROFILE%\AppData\Local\Google\Chrome\User Data\<Profile>\Login Data**
- **%USERPROFILE%\AppData\Local\Microsoft\Edge\User Data\<Profile>\ Login Data**
  - Stores inputted user credentials

Interpretation
- Includes typed-in data, as well as data types
- Connects typed data and knowledge to a user account

Browser Preferences

Description
Configuration data associated with the browser application, including privacy settings and synchronization preferences.

Location
Firefox
- **%USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\prefs.js**

Chrome/Edge
- **%USERPROFILE%\AppData\Local\Google\Chrome\User Data\<Profile>\Preferences**
- **%USERPROFILE%\AppData\Local\Microsoft\Edge\User Data\<Profile>\Preferences**

Interpretation
- Firefox prefs.js shows sync status, last sync time, and artifacts selected to sync
- Chrome uses JSON format
  - per_host_zoom_levels, media-engagement, and site_engagement can help to show user interaction
  - Contains synchronization status, last sync time and artifacts selected to sync
- Edge preferences include account_info, clear_data_on_exit, and sync settings

Cache

Description
The cache is where web page components can be stored locally to speed up subsequent visits.

Location
Firefox
- XP: **%USERPROFILE%\Local Settings\Application Data\Mozilla\Firefox\Profiles\<randomtext>.default\Cache**

Firefox 31-
- Win7+: **%USERPROFILE%\AppData\Local\Mozilla\Firefox\Profiles\<randomtext>.default\Cache**

Firefox 32+
- Win7+: **%USERPROFILE%\AppData\Local\Mozilla\Firefox\Profiles\<randomtext>.default\cache2**

Chrome/Edge
- XP: **%USERPROFILE%\Local Settings\Application Data\Google\Chrome\User Data\<Profile>\Cache - data_# and f_######**
- Win7+: **%USERPROFILE%\AppData\Local\Google\Chrome\User Data\<Profile>\Cache\ - data_# and f_######**
- Win7+: **%USERPROFILE%\AppData\Local\Microsoft\Edge\User Data\<Profile>\Cache\ - data_# and f_######**

Interpretation
- 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
- Similar to all browser artifacts, cached files are tied to a specific local user account
- Timestamps show when the site was first saved and last viewed

Bookmarks

Description
Bookmarks include default items, as well as those the user chose to save for future reference.

Location
Firefox 3+
- **%USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\places.sqlite**
- **%USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\bookmarkbackups\bookmarks-<date>.jsonlz4**

Chrome/Edge
- **%USERPROFILE%\AppData\Local\Google\Chrome\User Data\<Profile>\Bookmarks**
- **%USERPROFILE%\AppData\Local\Microsoft\Edge\User Data\<Profile>\Bookmarks**
- **%USERPROFILE%\AppData\Local\Google\Chrome\User Data\<Profile>\Bookmarks.bak**
- **%USERPROFILE%\AppData\Local\Microsoft\Edge\User Data\<Profile>\Bookmarks.msbak**

Interpretation
- Provides the website of interest and the specific URL that was saved
- Firefox bookmarkbackups folder can contain multiple backup copies of bookmarks in JSON format. Field names match those in places.sqlite
- Chromium Bookmark files are in JSON format
- Note: not all bookmarks are user-generated; it is possible to bookmark a site and never visit it

Stored Credentials

Description
Browser-based credential storage typically uses Windows DPAPI encryption. If the login account is a Microsoft cloud account in Windows 10 or 11, DPAPI uses a 44-character randomly generated password in lieu of the account password.

Location
Firefox
- **%USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\logins.json**

Chrome/Edge
- **%USERPROFILE%\AppData\Local\Google\Chrome\User Data\<Profile>\Login Data**
- **%USERPROFILE%\AppData\Local\Microsoft\Edge\User Data\<Profile>\Login Data**

Interpretation
- Firefox stores the hostname and URL, creation time, last used time, times used, and time of last password change in JSON format.
- Chromium-based browsers use a SQLite database and include the origin URL, action URL, username, date created, and date last used.
- Credential metadata can be available even if actual credentials are encrypted. Actual credentials are easiest to retrieve on a live system with the user account logged in.

Browser Downloads

Description
Modern browsers include built-in download manager applications capable of keeping a history of every file downloaded by the user. This browser artifact can provide excellent information about websites visited and corresponding items downloaded.

Location
Firefox 3-25
- **%USERPROFILE%\AppData\Roaming\Mozilla\ Firefox\Profiles\<random text>.default\downloads.sqlite**

Firefox 26+
- **%USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\places.sqlite**
  - **moz_annos** table

Chrome/Edge
- **%USERPROFILE%\AppData\Local\Google\Chrome\User Data\<Profile>\History**
- **%USERPROFILE%\AppData\Local\Microsoft\Edge\User Data\<Profile>\History**
  - **downloads** and **download_url_chains** tables

Interpretation
Download metadata includes:
- Filename, size, and type
- Source website and referring page
- Download start and end times
- File system save location
- State information including success and failure

Extensions

Description
Browser functionality can be extended through the use of extensions, or browser plugins.

Location
Firefox 4-25
- **%USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\extensions.sqlite**
- **%USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\addons.sqlite**

Firefox 26+
- **%USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\addons.json**
- **%USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\extensions.json**

Chrome/Edge
- **%USERPROFILE%\AppData\Local\Google\Chrome\User Data\<Profile>\Extensions\<GUID>\<version>**
- **%USERPROFILE%\AppData\Local\Microsoft\Edge\User Data\<Profile>\Extensions\<GUID>\<version>**

Interpretation
- The newer Firefox JSON format stores more information than in older versions
  - Extension name, installation source, installation time, last update, and plugin status
- Chrome/Edge extensions each have their own folder on the local system, named with a GUID, containing the code and metadata
  - Creation time of the folder indicates the installation time for the extension. Beware that extensions can be synced across devices affecting the interpretation of this timestamp.
  - A manifest.json file provides plugin details including name, URL, permissions, and version.
  - The preferences file can also include additional extension data

Session Restore

Description
Automatic crash recovery features are built into the browser.

Location
Firefox (older versions)
- Win7+: **%USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\sessionstore.js**

Firefox (newer versions)
- Win7+: **%USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\sessionstore.jsonlz4**
- Win7+: **%USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\sessionstore-backups\**

Chrome/Edge (older versions)
- Win7+: **%USERPROFILE%\AppData\Local\Google\Chrome\User Data\<Profile>**
- Win7+: **%USERPROFILE%\AppData\Local\Microsoft\Edge\User Data\<Profile>**
  - Restore files = Current Session, Current Tabs, Last Session, Last Tabs

Chrome/Edge (newer versions)
- Win7+: **%USERPROFILE%\AppData\Local\Google\Chrome\User Data\<Profile>\Sessions**
- Win7+: **%USERPROFILE%\AppData\Local\Microsoft\Edge\User Data\<Profile>\Sessions**
  - Restore files = Session_<timestamp>, Tabs_<timestamp>

Interpretation
- Historical websites viewed in each tab
- Referring websites
- Time session started or ended
- HTML, JavaScript, XML, and form data from the page
- Other artifacts such as transition type, browser window size and pinned tabs

Cookies

Description
Cookies provide insight into what websites have been visited and what activities might have taken place there.

Location
Firefox
- XP: **%USERPROFILE%\Application Data\Mozilla\Firefox\Profiles\<randomtext>.default\cookies.sqlite**
- Win7+: **%USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\cookies.sqlite**

Chrome/Edge
- XP: **%USERPROFILE%\Local Settings\Application Data\Google\Chrome\User Data\<Profile>\Cookies**
- Win7+: **%USERPROFILE%\AppData\Local\Google\Chrome\User Data\<Profile>\Network\Cookies**
- Win7+: **%USERPROFILE%\AppData\Local\Microsoft\Edge\User Data\<Profile>\Network\Cookies**

System Information

Operating System Version

Description
This determines 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
This 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 & Autostart Programs

Description
System Boot and Autostart Programs are 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

Cloud Storage

OneDrive

Description
OneDrive is installed by default on Windows 8+ systems, although it must be enabled by a user authenticating to their Microsoft Cloud account before use.

Location
Default local file storage:
- **%USERPROFILE%\OneDrive** (Personal)
- **%USERPROFILE%\OneDrive** - <CompanyName> (Business)

File storage folder location info:
- **NTUSER\Software\Microsoft\OneDrive\Accounts\<Personal | Business1>**

File metadata:
- **%USERPROFILE%\AppData\Local\Microsoft\OneDrive\logs\<Personal | Business1>**
  - **SyncDiagnostics.log**
  - SyncEngine "odl" logs
- **%USERPROFILE%\AppData\Local\Microsoft\OneDrive\settings\<Personal | Business1>**
  - **<UserCid>.dat**

Interpretation
- It is critical to check the registry to confirm the local file storage location
- Metadata files only exist if OneDrive is enabled
- SyncDiagnostics.log can sometimes contain file metadata
- Some files are only stored in the cloud and will not be stored locally
- Deleted items are stored in an online recycle bin for up to 30 days (personal) or 93 days (business)
- OneDrive for Business Unified Audit Logs in Microsoft 365 provide 90 days of user activity logging

Google Drive for Desktop

Description
Google Drive for Desktop is the new name for the merged Google Backup and Sync and File Stream applications. It uses a virtual FAT32 volume named "My Drive", which is only accessible to the user when they are logged in.

Location
Local drive letter for the virtual volume and account ID:
- **NTUSER\Software\Google\DriveFS\Share\**

Default local file cache:
- **%USERPROFILE%\AppData\Local\Google\DriveFS\<account identifier>\content_cache**

File metadata:
- **%USERPROFILE%\AppData\Local\Google\DriveFS\<account identifier>\metadata_sqlite_db**

Interpretation
- Assigned drive letter can help tie file and folder access artifacts to Google Drive
- Google Workspace Admin Reports provide 180 days of user activity logging
- metadata_sqlite_db database uses protobuf format for many important fields

Box Drive

Description
Box Drive uses a virtual filesystem, implemented as an NTFS reparse point. Excellent metadata logging is available.

Location
Default reparse point to virtual filesystem:
- **%USERPROFILE%\Box**

Default local file cache:
- **%USERPROFILE%\AppData\Local\Box\Box\cache**

File metadata and configuration data:
- **%USERPROFILE%\AppData\Local\Box\Box\logs**
  - **Box_Streem** logs
- **%USERPROFILE%\AppData\Local\Box\Box\data**
  - **sync.db** & **streemsfs.db** databases – file metadata
  - **metrics.db** – user account info

Interpretation
- Metadata available for both local and cloud-only files, including SHA1 hashes
- A search for the value "logDriveInformation" within the Box_Streem logs can identify the location of the virtual filesystem folder if it is not apparent
- Detailed usage logging available, but may only go back a few weeks

Dropbox

Description
Dropbox can be a challenging application to investigate. Older versions encrypt most metadata using Windows DPAPI, but recent versions tend to have more information available.

Location
Default local file storage:
- **%USERPROFILE%\Dropbox**
- **%USERPROFILE%\Dropbox\.dropbox.cache** (up to 3 days of cached data)

File storage folder location:
- **SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SyncRootManager\Dropbox!<SID>!Personal\UserSyncRoots**

File metadata and configuration data:
- **%USERPROFILE%\AppData\Local\Dropbox\**
  - **nucleus.sqlite3**, **sync_history.db**, and **aggregation.dbx** – usage and file metadata
  - v90-: **filecache.dbx**, **config.dbx** – encrypted with Windows DPAPI
  - **info.json** – app configuration data

Interpretation
- Metadata for local, cloud, and deleted files can all be identified
- Deleted files can exist in both the local and online recycle bins. Online recycle bin retention is 30 days (personal) or 120 days (business)
- Dropbox business "advanced tier" provides detailed logging while consumer Dropbox provides only limited logs via "Events" page

Account Usage

Cloud Account Details

Description
Microsoft Cloud Accounts store account information in the SAM hive, including the email address associated with the account.

Location
SAM\Domains\Account\Users\<RID>\InternetUserName

Interpretation
- InternetUserName value contains the email address tied to the account
- The presence of this value identifies the account as a Microsoft cloud account

Last Login and Password Change

Description
The SAM registry hive maintains a list of local accounts and associated configuration information.

Location
SAM\Domains\Account\Users

Interpretation
- Accounts listed by their relative identifiers (RID)
- Last login time, last password change, login counts, group membership, account creation time and more can be determined

Service Events

Description
Analyze logs for suspicious Windows service creation, persistence, and services started or stopped around the time of a suspected compromise. Service events also record account information.

Location
- Win7+: **%SYSTEM ROOT%\System32\winevt\logs\System.evtx**
- Win10+: **%SYSTEM ROOT%\System32\winevt\logs\Security.evtx**

Interpretation
- Most relevant events are present in 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+)
- Auditing can be enabled in the Security log on Win10+:
  - 4697 – A service was installed on the system (from Security 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

User Accounts

Description
Identify both local and domain accounts with interactive logins to the system.

Location
SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList

Interpretation
- Useful for mapping SID to user account name
- Subkeys are named for user SIDs and contain a ProfileImagePath indicating the user's profile path

Remote Desktop Protocol (RDP) Usage

Description
Track RDP logons and session reconnections to target machines.

Location Security Log
Win7+: %SYSTEM ROOT%\System32\winevt\logs\Security.evtx

Interpretation
- Multiple events can be used to track accounts used for RDP
  - Event ID 4624 – Logon Type 10
  - Event ID 4778 – Session Connected/Reconnected
  - Event ID 4779 – Session Disconnected
- Event log provides hostname and IP address of remote machine making the connection
- Multiple dedicated RDP/Terminal Services logs are also available on modern Windows versions

Successful/Failed Logons

Description
Profile account creation, attempted logons, and account usage.

Location
Win7+: **% SYSTEM ROOT%\System32\winevt\logs\Security.evtx**

Interpretation
- Win7+:
  - 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

Authentication Events

Description
Authentication Events identify where authentication of credentials occurred. They can be particularly useful when tracking local vs. domain account usage.

Location
Win7+: %SYSTEM ROOT%\System32\winevt\logs\Security.evtx

Interpretation
- Recorded on system that authenticated credentials
  - Local Account/Workgroup = on workstation
  - Domain/Active Directory = on domain controller
- 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)

Logon Event Types

Description
Logon Events provide very specific information regarding the nature of account authorizations on a system. In addition to date, time, username, hostname, and success/failure status of a logon, Logon Events also enable us to determine by exactly what means a logon was attempted.

Location
Win7+: %SYSTEM ROOT%\System32\winevt\logs\Security.evtx

Interpretation
Event ID 4624

Logon Type	Explanation
2	Logon via console
3	Network Logon
4	Batch Logon
5	Windows Service Logon
7	Credentials used to unlock screen; RDP session reconnect
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)

Network Activity and Physical Location

Network History

Description
Identify networks to which the computer connected. Available information includes domain name/intranet name, SSID, first and last time connected, and Gateway MAC Address.

Location
- **SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces**
- **SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards**
- **SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged**
- **SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed**
- **SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Cache**
- **SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles**

Interpretation
- Multiple registry keys can be correlated to provide a rich picture of network activity.
  - Interfaces info can be correlated with other keys via DhcpDomain value
  - Signatures and Profiles keys are correlated via the network ProfileGUID value
- Network data includes VPN connections
- MAC Address of SSID for Gateway can assist with device geolocation
- Network Profile NameType values:
  - 6 (0x06) = Wired
  - 23 (0x17) = VPN
  - 71 (0x47) = Wireless
  - 243 (0xF3) = Mobile Broadband

Browser URL Parameters

Description
Information leaked within browser history URL parameters can provide clues to captive portal sign-ins and other similar information sources that can identify connected networks and even approximate physical locations.

Example:
https://maps.google.com/maps?hl=en-US&gl=US&um=1&ie=UTF-8&fb=1&sa=X&geocode=KWv-o9E_nLJBBdixYmN41uvu&daddr=Hyatt+Place+Portland-Old+Port,+433+Fore+St,+Portland,+ME+04101

Location
Multiple – see the history information within the *Browser Usage* section

Timezone

Description
Registry data identifies the current system time zone. Event logs may be able to provide additional historical information.

Location
- **SYSTEM\CurrentControlSet\Control\TimeZoneInformation**
- **%SYSTEM ROOT%\System32\winevt\logs\System.evtx**

Interpretation
- Some log files and artifact timestamps can only be correctly interpreted by knowing the system time zone
- Event ID 6013 in the System.evtx log can provide information on historical time zone settings

WLAN Event Log

Description
Determine historical view of wireless networks associations.

Location
Win7+: **Microsoft-Windows-WLAN-AutoConfig Operational.evtx**

Interpretation
- Provides historical record of wireless network connections
- SSID can be used to correlate and retrieve additional network information from Network History registry keys
- 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)

Network Interfaces

Description
List available network interfaces and their last known configurations.

Location
- **SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces**
- **SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards**

Interpretation
- Interfaces key includes the last known IP address, DHCP and domain information for both physical and virtual network adapters. Subkeys may be present containing historical network data
- NetworkCards key can provide more detail on network availability
- The two keys are mapped via the interface GUID value
- Unlikely to be a complete view of every connected network

System Resource Usage Monitor (SRUM)

Description
SRUM 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
Win8+: **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
- Records data approx. once per hour, in batches

External Device/USB Usage

USB Device Identification

Description
Track USB devices plugged into a machine.

Location
- **SYSTEM\CurrentControlSet\Enum\USBSTOR**
- **SYSTEM\CurrentControlSet\Enum\USB**
- **SYSTEM\CurrentControlSet\Enum\SCSI**
- **SYSTEM\CurrentControlSet\Enum\HID**

Interpretation
- Identify vendor, product, and version of a USB device plugged into a machine
- Determine the first and last times a device was plugged into the machine
- Devices that do not have a unique internal serial number will have an "&" in the second character of the serial number
- The internal serial number provided in these keys may not match the serial number printed on the device
- ParentIdPrefix links USB key to SCSI key
- SCSI\<ParentIdPrefix>\Device Parameters\Partmgr\DiskId matches Partition/Diagnostic log and Windows Portable Devices key
- Different versions of Windows store this data for different amounts of time. Windows 10/11 can store up to one year of data
  - Some older data may be present in **SYSTEM\Setup\Upgrade\PnP\CurrentControlSet\Control\DeviceMigration**
- HID key tracks peripherals connected to the system

Event Logs

Description
Removable device activity can be audited in multiple Windows event logs.

Location
Win7+: **%SYSTEM ROOT%\System32\winevt\logs\System.evtx**

Interpretation
- Event IDs 20001, 20003 – Plug and Play driver install attempted

Location
%SYSTEM ROOT%\System32\winevt\logs\Security.evtx

Interpretation
- 4663 – Attempt to access removable storage object (Security log)
- 4656 – Failure to access removable storage object (Security log)
- 6416 – A new external device was recognized on system (Security log)
- Security log events are dependent on system audit settings

Location *Connection Times*
- Win10+: **%SYSTEM ROOT%\System32\winevt\logs\Microsoft-Windows-Partition/Diagnostic.evtx**

Interpretation
- Event ID 1006 is recorded for each device connect/disconnect

Drive Letter and Volume Name

Description
Discover the last drive letter and volume name of a device when it was plugged into the system.

Location
XP:
- Find **ParentIdPrefix** – **SYSTEM\CurrentControlSet\Enum\USBSTOR**
- Using **ParentIdPrefix** Discover Last Mount Point – **SYSTEM\MountedDevices**

Win7+:
- **SOFTWARE\Microsoft\Windows Portable Devices\Devices**
- **SYSTEM\MountedDevices** Examine available drive letter values looking for a serial number match in value data
- Win7+: **SOFTWARE\Microsoft\Windows Search\VolumeInfoCache**

Interpretation
- Only the last USB device mapped to a specific drive letter can be identified. Historical records not available.

User Information

Description
Identify user accounts tied to a unique USB Device.

Location
- Document device Volume GUID from **SYSTEM\MountedDevices**
- **NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2**

Interpretation
If a Volume GUID match is made within MountPoints2, we can conclude the associated user profile was logged in while that device was present.

Shortcut (LNK) Files

Description
Shortcut files are automatically created by Windows, tracking files and folders opened by a user.

Location
- XP: **%USERPROFILE%\Recent**
- Win7+: **%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\**
- Win7+: **%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
- LNK Target 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

Connection Timestamps

Description
Connection timestamps determine 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+: **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+: **SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_&Prod_\USBSerial#\Properties\{83da6326-97a6-4088-9453-a19231573b29}\####**
- Win7+: **SYSTEM\CurrentControlSet\Enum\SCSI\Ven_Prod_Version\USBSerial#\Properties\{83da6326-97a6-4088-9453-a19231573b29}\####**
  - 0064 = First Install (Win7+)
  - 0066 = Last Connected (Win8+)
  - 0067 = Last Removal (Win8+)

Interpretation
Timestamps are stored in Windows 64-bit FILETIME format

Location *Connection Times*
- Win10+: **%SYSTEM ROOT%\System32\winevt\logs\Microsoft-Windows-Partition/Diagnostic.evtx**

Interpretation
- Event ID 1006 is recorded for each device connect/disconnect
- Log cleared during major OS updates

Volume Serial Number (VSN)

Description
Discover the VSN assigned to the file system partition on the USB. (NOTE: This is not the USB Unique Serial Number, which is hardcoded into the device firmware, nor the serial number on any external labels attached to the device.)

Location
- **SOFTWARE\Microsoft\WindowsNT\CurrentVersion\EMDMgmt**
  - Find a key match using Volume Name and USB Unique Serial Number:
    - Find last integer number in matching line
    - Convert decimal value to hex serial number
  - This key is often missing from modern systems using SSD devices
- **Win10+: %SYSTEM ROOT%\System32\winevt\logs\Microsoft-Windows-Partition/Diagnostic.evtx**
  - Event ID 1006 may include VBR data, which contains the VSN
  - VSN is 4 bytes located at offsets 0x43 (FAT), 0x64 (exFAT), or 0x48 (NTFS) within each VBR
  - Log cleared during major OS updates

Interpretation
The VSN and device Volume Name can help correlate devices to specific files via shell items present in LNK files and registry locations.

SANS DFIR

$25.00
DFPS_FOR500_v4.14_12-22
Poster created thanks to the support and contributions of the SANS DFIR Faculty ©2022 SANS Institute. All Rights Reserved