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_v4.9_4-19
Poster Created by Rob Lee with support of the SANS DFIR Faculty

## Windows® Time Rules

### $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 only on NTFS Win7+)* | Access – No Change | 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 |

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.

## File Download

### 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

### Email Attachments

**Description**

The email industry estimates that 80% of email data is stored via attachments. Email standards only allow text. Attachments must be encoded with MIME/base64 format.

**Location**

Outlook
XP:
**%USERPROFILE%\Local Settings\ApplicationData\Microsoft\Outlook**
Win7/8/10:
**%USERPROFILE%\AppData\Local\Microsoft\Outlook**

**Interpretation**

MS Outlook data files found in these locations include OST and PST files. One should also check the OLK and Content.Outlook folder, which might roam depending on the specific version of Outlook used. For more information on where to find the OLK folder this link has a handy chart: **http://www.hancockcomputertech.com/blog/2010/01/06/find-the-microsoft-outlook-temporary-olk-folder**

### Skype History

**Description**

- Skype history keeps a log of chat sessions and files transferred from one machine to another
- This is turned on by default in Skype installations

**Location**

XP:
**C:\Documents and Settings\<username>\Application\Skype\<skype-name>**
Win7/8/10:
**C:\%USERPROFILE%\AppData\Roaming\Skype\<skype-name>**

**Interpretation**

Each entry will have a date/time value and a Skype username associated with the action.

### Browser Artifacts

**Description**

Not directly related to "File Download". Details stored for each local user account. Records number of times visited (frequency).

**Location**

Internet Explorer
- IE8-9:
  **%USERPROFILE%\AppData\Roaming\Microsoft\Windows\IEDownloadHistory\index.dat**
- IE10-11:
  **%USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat**

Firefox
- v3-25:
  **%userprofile%\AppData\Roaming\Mozilla\ Firefox\Profiles\<random text>.default\downloads.sqlite**
- v26+:
  **%userprofile%\AppData\Roaming\Mozilla\ Firefox\Profiles\<random text>.default\places.sqlite Table:moz_annos**

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

**Interpretation**

Many sites in history will list the files that were opened from remote sites and downloaded to the local system. History will record the access to the file on the website that was accessed via a link.

### Downloads

**Description**

Firefox and IE has a built-in download manager application which keeps a history of every file downloaded by the user. This browser artifact can provide excellent information about what sites a user has been visiting and what kinds of files they have been downloading from them.

**Location**

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

Internet Explorer:
- IE8-9:
  **%USERPROFILE%\AppData\Roaming\Microsoft\Windows\ IEDownloadHistory**
- IE10-11:
  **%USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\ WebCacheV*.dat**

**Interpretation**

Downloads will include:
- Filename, Size, and Type
- Download from and Referring Page
- File Save Location
- Application Used to Open File
- Download Start and End Times

### ADS Zone.Identifer

**Description**

Starting with XP SP2 when files are downloaded from the "Internet Zone" via a browser to a NTFS volume, an alternate data stream is added to the file. The alternate data stream is named "Zone.Identifier."

**Interpretation**

Files with an ADS Zone.Identifier and contains ZoneID=3 were downloaded from the Internet
- URLZONE_TRUSTED = ZoneID = 2
- URLZONE_INTERNET = ZoneID = 3
- URLZONE_UNTRUSTED = ZoneID = 4

## Program Execution

### UserAssist

**Description**

GUI-based programs launched from the desktop are tracked in the launcher on a Windows System.

**Location**

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

**Interpretation**

All values are ROT-13 Encoded
- GUID for XP
  - 75048700 Active Desktop
- GUID for Win7/8/10
  - CEBFF5CD Executable File Execution
  - F4E57C4B Shortcut File Execution

### Windows 10 Timeline

**Description**

Win10 records recently used applications and files in a "timeline" accessible via the "WIN+TAB" key. The data is recorded in a SQLite database.

**Location**

**C:\Users\<profile>\AppData\Local\ConnectedDevices Platform\L.<profile>\ActivitiesCache.db**

**Interpretation**

- Application execution
- Focus count per application

### RecentApps

**Description**

GUI Program execution launched on the Win10 system is tracked in the RecentApps key

**Location**

Win10:
**NTUSER.DAT\Software\Microsoft\Windows\Current Version\Search\RecentApps**

**Interpretation**

Each GUID key points to a recent application.
AppID = Name of Application
LastAccessTime = Last execution time in UTC
LaunchCount = Number of times executed

### Shimcache

**Description**

- Windows Application Compatibility Database is used by Windows to identify possible application compatibility challenges with executables.
- Tracks the executables file name, file size, last modified time, and in Windows XP the last update time

**Location**

XP:
**SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatibility**
Win7/8/10:
**SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache**

**Interpretation**

Any executable run on the Windows system could be found in this key. You can use this key to identify systems that specific malware was executed on. In addition, based on the interpretation of the time-based data you might be able to determine the last time of execution or activity on the system.
- Windows XP contains at most 96 entries
  - LastUpdateTime is updated when the files are executed
- Windows 7 contains at most 1,024 entries
  - LastUpdateTime does not exist on Win7 systems

### Jump Lists

**Description**

- The Windows 7 task bar (Jump List) is engineered to allow users to "jump" or access items they 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 associated application.

**Location**

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

**Interpretation**

- First time of execution of application.
  - Creation Time = First time item added to the AppID file.
- Last time of execution of application w/file open.
  - Modification Time = Last time item added to the AppID file.
- List of Jump List IDs -> **http://www.forensicswiki.org/wiki/List_of_Jump_List_IDs**

### Amcache.hve

**Description**

ProgramDataUpdater (a task associated with the Application Experience Service) uses the registry file Amcache.hve to store data during process creation

**Location**

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

**Interpretation**

- Amcache.hve – Keys = **Amcache.hve\Root\File\{Volume GUID}\#######**
- Entry for every executable run, full path information, File's $StandardInfo Last Modification Time, and Disk volume the executable was run from
- First Run Time = Last Modification Time of Key
- SHA1 hash of executable also contained in the key

### System Resource Usage Monitor (SRUM)

**Description**

Records 30 to 60 days of historical system performance. Applications run, user account responsible for each, and application and bytes sent/received per application per hour.

**Location**

**SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SRUM\Extensions {d10ca2fe-6fcf-4f6d-848e-b2e99266fa89} = Application Resource Usage Provider 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.

### BAM/DAM

**Description**

Windows Background Activity Moderator (BAM)

**Location**

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

**Investigative Notes**

Provides full path of the executable file that was run on the system and last execution date/time

### 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:\%USERPROFILE%\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.

### Prefetch

**Description**

- 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
- (exename)-(hash).pf

**Location**

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

**Interpretation**

- Each .pf will include last time of execution, number of times run, and device and file handles used by the program
- 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
  - Embedded last execution time of .pf file
  - Last modification date of .pf file (-10 seconds)
  - Win8-10 will contain last 8 times of execution

## Deleted File or File Knowledge

### XP Search – ACMRU

**Description**

You can search for a wide range of information through the search assistant on a Windows XP machine. The search assistant will remember a user's search terms for filenames, computers, or words that are inside a file. This is an example of where you can find the "Search History" on the Windows system.

**Location**

NTUSER.DAT HIVE
**NTUSER.DAT\Software\Microsoft\Search Assistant\ACMru\####**

**Interpretation**

- Search the Internet – ####=5001
- All or part of a document name – ####=5603
- A word or phrase in a file – ####=5604
- Printers, Computers and People – ####=5647

### Thumbcache

**Description**

Thumbnails of pictures, office documents, and folders exist in a database called the thumbcache. Each user will have their own database based on the thumbnail sizes viewed by the user (small, medium, large, and extra-larger)

**Location**

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

**Interpretation**

- These are created when a user switches a folder to thumbnail mode or views pictures via a slide show. As it were, our thumbs are now stored in separate database files. Win7+ has 4 sizes for thumbnails and the files in the cache folder reflect this:
  - 32 -> small - 96 -> medium
  - 256 -> large - 1024 -> extra large
- The thumbcache will store the thumbnail copy of the picture based on the thumbnail size in the content of the equivalent database file.

### Thumbs.db

**Description**

Hidden file in directory where images on machine exist stored in a smaller thumbnail graphics. thumbs.db catalogs pictures in a folder and stores a copy of the thumbnail even if the pictures were deleted.

**Location**

WinXP/Win8|8.1
Automatically created anywhere with homegroup enabled
Win7/8/10
Automatically created anywhere and accessed via a UNC Path (local or remote)

**Interpretation**

Include:
- Thumbnail Picture of Original Picture
- Document Thumbnail – Even if Deleted
- Last Modification Time (XP Only)
- Original Filename (XP Only)

### 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 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%\LocalSettings\History\History.IE5**
IE8-9
**%USERPROFILE%\AppData\Local\Microsoft\WindowsHistory\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

### Search – WordWheelQuery

**Description**

Keywords searched for from the START menu bar on a Windows 7 machine.

**Location**

Win7/8/10 NTUSER.DAT Hive
**NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery**

**Interpretation**

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

### Win7/8/10 Recycle Bin

**Description**

The recycle bin is a very important location on a Windows file system to understand. It can help you when accomplishing a forensic investigation, as every file that is deleted from a Windows recycle bin aware program is generally first put in the recycle bin.

**Location**

Hidden System Folder
Win7/8/10
- **C:\$Recycle.bin**
- Deleted Time and Original Filename contained in separate files for each deleted recovery file

**Interpretation**

- SID can be mapped to user via Registry Analysis
- Win7/8/10
  - Files Preceded by $I###### files contain
- Original PATH and name
- Deletion Date/Time
  - Files Preceded by $R###### files contain
- Recovery Data

### 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.

**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.

### XP Recycle Bin

**Description**

The recycle bin is a very important location on a Windows file system to understand. It can help you when accomplishing a forensic investigation, as every file that is deleted from a Windows recycle bin aware program is generally first put in the recycle bin.

**Location**

Hidden System Folder
Windows XP
- **C:\RECYCLER" 2000/NT/XP/2003**
- Subfolder is created with user's SID
- Hidden file in directory called "INFO2"
- INFO2 Contains Deleted Time and Original Filename
- Filename in both ASCII and UNICODE

**Interpretation**

- SID can be mapped to user via Registry Analysis
- Maps file name to the actual name and path it was deleted from

# Network Activity/Physical Location

## Timezone

**Description**

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.

## 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**

## Network History

**Description**

- Identify 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

## WLAN Event Log

**Description**

Determine what wireless networks the system associated with and identify network characteristics to find 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 (SRUM)

**Description**

Records 30 to 60 days of historical system performance. Applications run, user account responsible for each, and application 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**

- Which folders were accessed on the local machine, the network, and/or removable devices. Evidence of previously existing folders after deletion/overwrite. 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 automatically created by Windows
  - 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\**
- **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**

- 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
- 11.0 = Office 2003
- 12.0 = Office 2007
- 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**

Track 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**

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**

**Win7/8/10:**
**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**
- **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 automatically created by Windows

- Recent Items
- Open local and remote data files and documents will generate a shortcut file (.lnk)

**Location**

**XP:**

- **%USERPROFILE%\Recent**

**Win7/8/10**

- **%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent**
- **%USERPROFILE%\AppData\Roaming\Microsoft\Office\Recent**

**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**

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.

**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

- IE8-9: **%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Cookies**
- IE10: **%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Cookies**
- IE11: **%USERPROFILE%\AppData\Local\Microsoft\Windows\INetCookies**
- Edge: **%USERPROFILE%\AppData\Local\Packages\microsoft.microsoftedge_<APPID>\AC\MicrosoftEdge\Cookies**

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\Application Data\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
- 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)