

File Download

Open/Save MRU

Description:

In 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 NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU

Interpretation:

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

E-mail Attachments

Description:

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

Location: Outlook

XP %USERPROFILE%\Local Settings\Application Data\Microsoft\Outlook
Win7 %USERPROFILE%\AppData\Local\Microsoft\Outlook

Interpretation:

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

Skype History

• 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 C:\Users\<username>\AppData\Roaming\Skype\<skype-name>

Interpretation:

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

Index.dat/ Places.sqlite

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

Location: Internet Explorer

XP %userprofile%\Local Settings\History\History.IE5
Win7 %userprofile%\AppData\Local\Microsoft\Windows\History\History.IE5
Win7 %userprofile%\AppData\Local\Microsoft\Windows\History\Low\History.IE5

Location: Firefox

IE %userprofile%\Application Data\Mozilla\Firefox\Profiles\<random text>\default\places.sqlite
Win7 %userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\<random text>\default\places.sqlite

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 access via a link.

Downloads.sqlite

Description:

Firefox 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

IE %userprofile%\Application Data\Mozilla\Firefox\Profiles\<random text>\default\downloads.sqlite
Win7 %userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\<random text>\default\downloads.sqlite

Interpretation:

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

Created for FOR408 – Windows Forensics – SANS Digital Forensics and Incident Response faculty created the "Evidence of..." categories to map a specific artifact to the analysis question that it will help to answer. Use this poster as a cheat-sheet to help you remember where you can discover key items to an activity for Microsoft Windows systems for intrusions, intellectual property theft, or common cyber-crimes.

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
• Program Locations for Win7 Userassist
• Program Files64 60809377...
• Program FilesX86 7C54A0EF...
• System 7C14E77...
• SystemX86 D6523180...
• Desktop 04BFC3CA...
• Documents FDD39AD0...
• Downloads 374DE290...
• UserProfiles 0762D272...

Last Visited MRU

Description:

Tracks the specific executable used by an application to open the files documented in the Open/SaveMRU 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\<username>\Desktop folder

Location:

XP NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU
Win7 NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU

Interpretation:

Tracks the application executables used to open files in Open/SaveMRU and the last file path used.

RunMRU Start->Run

Description: Whenever someone does a Start -> Run command, it will log the entry for the command they executed.

Location: NTUSER.DAT HIVE

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

Interpretation:

The order in which the commands are executed is listed in the RunMRU list value. The letters represent the order in which the commands were executed.

Application Compatibility Cache

Description: Windows Application Compatibility Database is used by Windows to identify possible 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\AppCompatCache
Win7 SYSTEM\CurrentControlSet\Control\SessionManager\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 1024 entries
• LastUpdateTime does not exist on Win7 systems

Tool to parse:

MANDIANT'S ShimCacheParser

Win7 Jump Lists

Description:

• The Windows 7 task bar (Jump List) is engineered to allow users to "jump" or access items they frequently or have recently used quickly and easily. This functionality cannot only be recent media files, but recent tasks as well.
• The data stored in the AutomaticDestinations folder will each have a unique file prepended with the AppID of the associated application.

Location:

Win7 C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

Interpretation:

• First time of execution of application.
• Creation Time = First time item added to the AppID file
• Date/Time File of that name was first opened
• 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

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 (evenname)-hash.pf

Location:

Win7/XP C:\Windows\Prefetch

Interpretation:

• Each .pf file will include last time of execution, # of times run, and device and file handles used by the program
• Date/Time File by that name & path was first executed
• Creation Date of .pf file (<10 seconds)
• Date/Time File by that name & path was last executed
• Embedded last execution time of .pf file
• Last Modification Date of .pf file (<10 seconds)

Services Events

Description:

Analysis 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]

Interpretation:

• 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.
Win7 %userprofile%\Local Settings\History\History.IE5
Win7 %userprofile%\AppData\Local\Microsoft\Windows\History\History.IE5
Win7 %userprofile%\AppData\Local\Microsoft\Windows\History\Low\History.IE5
Interpretation:
• Stored in index.dat as: file://C:/directory/filename.ext
• Does not mean file was opened in browser

File Opening / Creation

Open/Save MRU

Description:

In 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 NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU

Interpretation:

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

Last Visited MRU

Description:

Tracks the specific executable used by an application to open the files documented in the Open/SaveMRU 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 NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU

Interpretation:

Tracks the application executables used to open files in Open/SaveMRU and the last file path used.

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 time and location of 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 time and location of 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 time and location of the last folder opened.

Office Recent Files

Description:

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

Location:

XP NTUSER.DAT\Software\Microsoft\Office\VERSION
• 14.0 - Office 2010
• 12.0 - Office 2007
• 11.0 - Office 2003
• 10.0 - Office XP

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.

Shell bags

Description:

• Can track user window viewing preferences to Windows Explorer
• Can be utilized to tell if activity occurred in a folder
• In some cases, you can see the files from a specific folder as well

Location:

XP NTUSER.DAT\Software\Microsoft\Windows\ShellBags
XP NTUSER.DAT\Software\Microsoft\Windows\ShellBagsMRU
XP NTUSER.DAT\Software\Microsoft\Windows\ShellNoRoam\Bags
Win7 USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\ShellBags
Win7 USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\ShellBagsMRU
Win7 NTUSER.DAT\Software\Microsoft\Windows\ShellBags

Interpretation:

Store 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 (Link)

Location:

XP C:\Documents and Settings\<username>\Recent
Win7 C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Recent
Win7 C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

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

Win7 Jump Lists

Description:

• The Windows 7 task bar (Jump List) is engineered to allow users to "jump" or access items they frequently or have recently used quickly and easily. This functionality cannot only be recent media files, but recent tasks as well.
• 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 team.

Location:

Win7 C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

Interpretation:

• Using the Structured Storage Viewer open up one of the AutomaticDestinations 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).

Prefetch

Description:

Increases performance of 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.

Location:

Win7/XP 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

Index.dat 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

XP %userprofile%\Local Settings\History\History.IE5
Win7 %userprofile%\AppData\Local\Microsoft\Windows\History\History.IE5
Win7 %userprofile%\AppData\Local\Microsoft\Windows\History\Low\History.IE5

Interpretation:

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

Deleted File or File Knowledge

XP Search – ACMRU

Description:

You can search for multiple things 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 of 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

Win7 Search – WordWheelQuery

Description:

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

Location: Win7 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

Last Visited MRU

Description: Tracks the specific executable used by an application to open the files documented in the Open/SaveMRU 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 NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU

Interpretation:

Tracks the application executables used to open files in Open/SaveMRU and the last file path used.

Thumbs.db

Description: Hidden file in directory where pictures are on Windows XP machine exist. Catalogs all the pictures and stores a copy of the thumbnail even if the pictures were deleted.

Location:

Each directory where pictures resided that were viewed in thumbnail mode. Many camera's also will auto generate a thumbs.db file when you view the pictures on the camera itself.

Interpretation:

• Thumbnail Picture of Original
• Last Modification Time
• Original Filename

Vista/Win7 Thumbnails

Description: On Vista/Win7 versions of Windows, thumbs.db does not exist. The data now sits under a single directory for each user of the machine located in their application data directory under the home directory.

Location:

C:\Users\<username>\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. Vista/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 thumbnail cache will store the thumbnail copy of the picture based on the thumbnail size in the content of the equivalent database file.

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:\RECYCLE.BIN\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
• Windows XP
• INFO2
• Hidden file in Recycle Bin called INFO2
• Maps filename to the actual name and path it was deleted from

Win7 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 7
• C:\\$RecycleBin
• Deleted Time and Original Filename contained in separate files for each deleted recovery file

Interpretation:

• SID can be mapped to user via Registry Analysis
• Windows 7
• Files Preceded by \$R##### files contain
• Original PATH and name
• Deletion Date/Time
• Files Preceded \$R##### files contain
• Recovery Data

Index.dat 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.

Interpretation:

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

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 off of 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.

VISTA/Win7 Network History

Description:

Identifies networks that the computer has been connected to

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

Location: SOFTWARE HIVE

SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged
SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed
SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Na\Cache

Interpretation:

• Identifying intranets and networks that a computer has connected to is incredibly important
• Not only can you tell the intranet name, you can tell the last time the network was connected to 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

