COMP 5350 / 6350
Digital Forensics

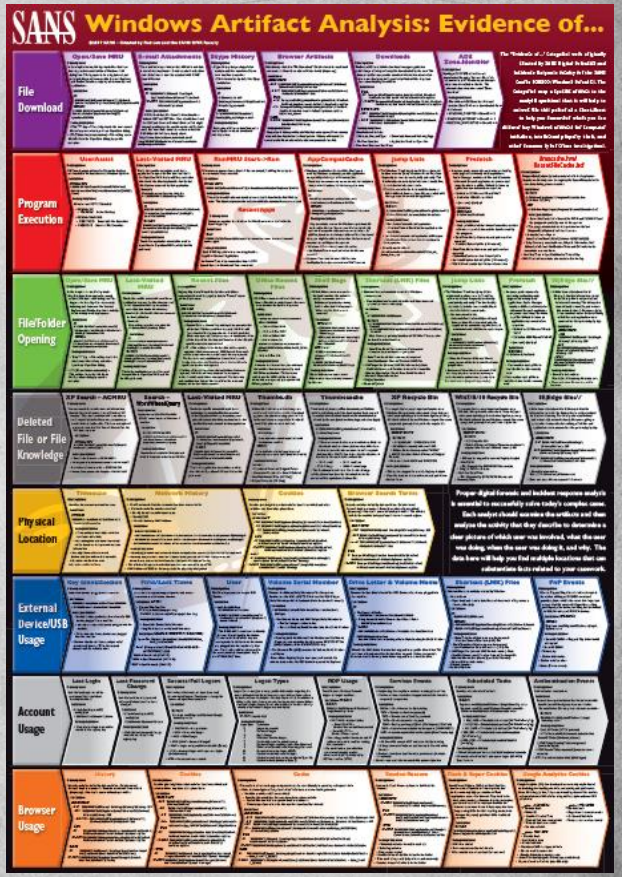
Timeline Analysis

Event Timelines

- By consolidating different digital artifacts collected during a forensics analysis we can generate a list of events based on user, date/time, and source
  - ✓ File Modification
    - Created
    - Accessed
    - Copied
  - ✓ Operating System Modification
    - Registry
    - File System
  - ✓ Event Logs
  - ✓ Application Execution
  - ✓ Device Connections

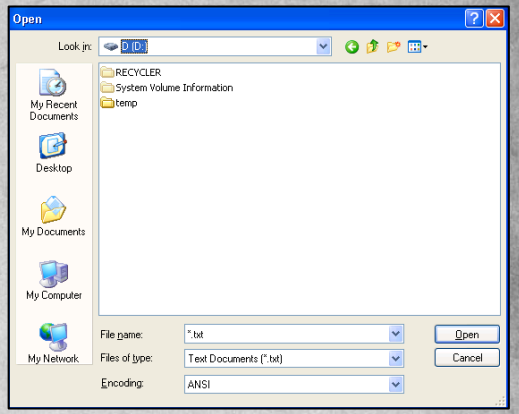
SANS Artifact Analysis

- The SANS institute provides a wide variety of technical training across numerous cybersecurity domains
- SANS has mapped digital artifacts in the Windows OS along with their storage location in the file system
  - ✓ File Download
  - ✓ Program Execution
  - ✓ File Opening / Creation
  - ✓ Deleted File / File Knowledge
  - ✓ Physical Location
  - ✓ USB / Drive Usage
  - ✓ Account Usage
  - ✓ Browser Usage

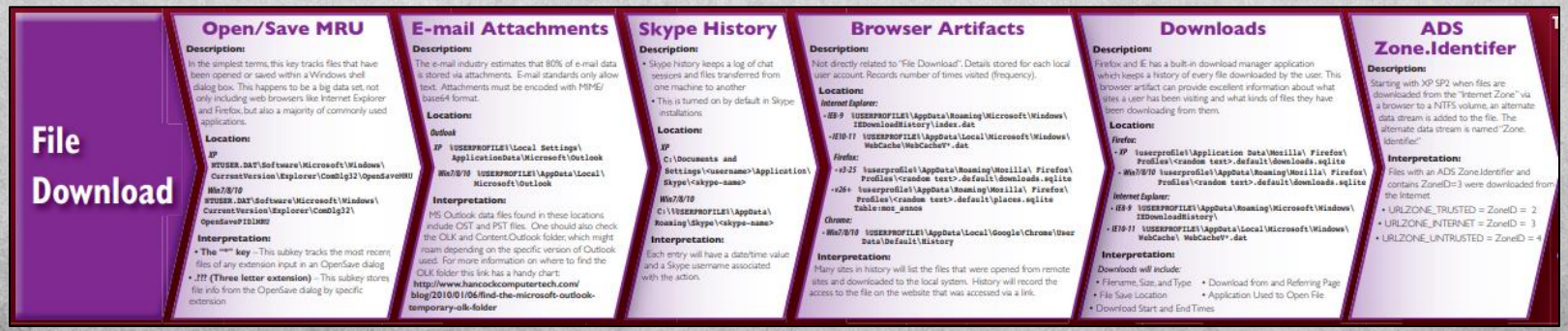


File Download – Open / Save MRU

- Tracks files opened or saved within a Windows shell dialog box
- Includes web browser and application keys
  - ✓ “*” key: Subkey that tracks most recent files of any extension input in an OpenSave dialog
  - ✓ *.???: Subkey stores file info from OpenSave dialog by specific extension

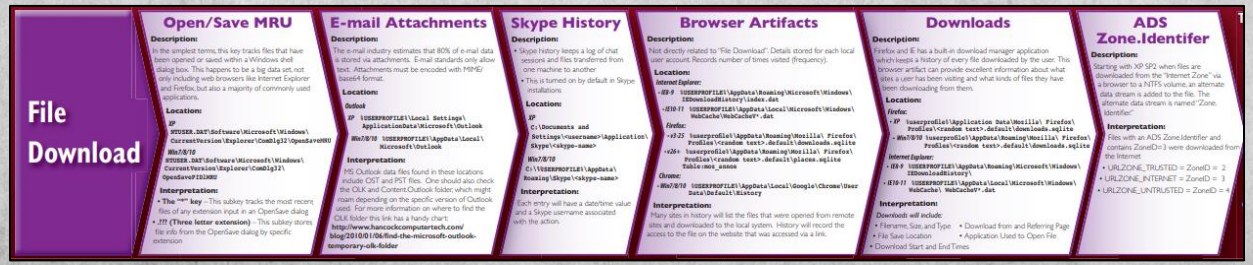


NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDlMRU



File Download – Browser Artifacts

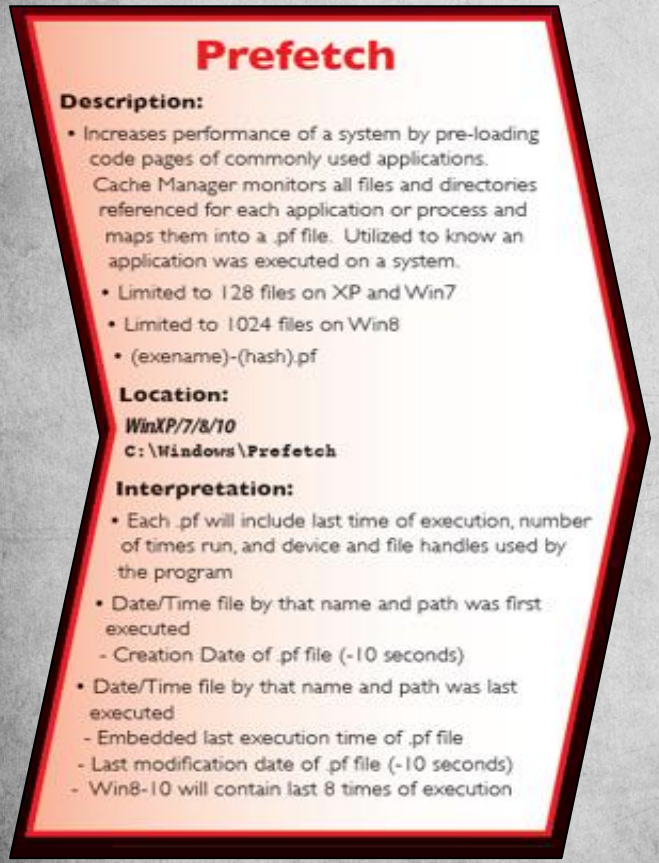
- Not directly related to “File Download” MRU, but is maintained in each user account
- Shows files opened from remote sites and downloaded to local system
- Records file access on the website that was accessed through a link
- Browser History Locations:
  - ✓ IE 10 & 11: %USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat
  - ✓ Chrome: %USERPROFILE%\AppData\Local\Google\Chrome\UserData\Default\History



Program Execution

- There are seven different methods of identifying program execution
  - UserAssist*
  - Last-Visited MRU*
  - RunMRU Start*
  - AppCompatCache
  - Jump Lists
  - Prefetch
  - RecentFileCache

Program Execution – Prefetch



- Increases performance of a system by preloading commonly used applications
- Cache Manager monitors all files and directories for each application and maps them into a .pf file
- Proves application execution on a system
- Each prefetch file includes
  - ✓ Last execution time, number of times run, and program file handles
  - ✓ Date and time path was first executed
  - ✓ Creation Date of .pf file
  - ✓ Date and time file by that name and path was last executed

C:\Windows\Prefetch

File / Folder Opening

- In addition to some file and folder access artifacts that we have introduced in the Ranmore course, other methods include:
  - ✓ Open / Save MRU*
  - ✓ Last-Visted MRU*
  - ✓ Recent Files*
  - ✓ Shell Bags*
  - ✓ Prefetch
  - ✓ Link Files
  - ✓ Jump Lists
  - ✓ IE / Edge Browser Files

File / Folder Opening – Link Files

- Links (LNK) are shortcuts automatically created by Windows for recent items and when opening local and remote data files
- Link files can provide valuable forensics information including:
  - ✓ LNK creation date
  - ✓ When LNK was last opened
  - ✓ LNK modification date
- LNK file data includes:
  - ✓ Target file MAC times
  - ✓ Volume Information
  - ✓ Network Share information
  - ✓ Original Location
  - ✓ System Name

C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent

File / Folder Opening – Jump Lists

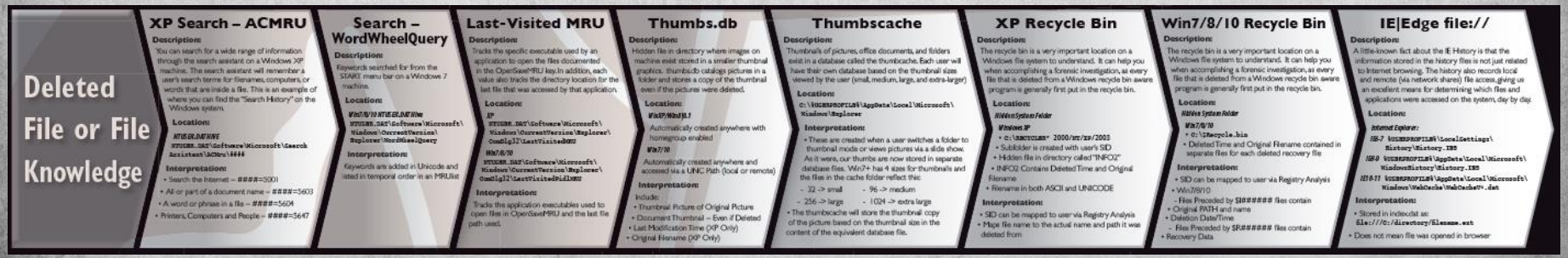
- Jump Lists provide provides access to recently or frequently used items
- Jump lists includes both user files and recent tasks

C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

- Data stored in this directory has unique files prepended with the associated application (AppID) and embedded file LNK
- Each LNK is stored numerically based on order of access, incremented from 1

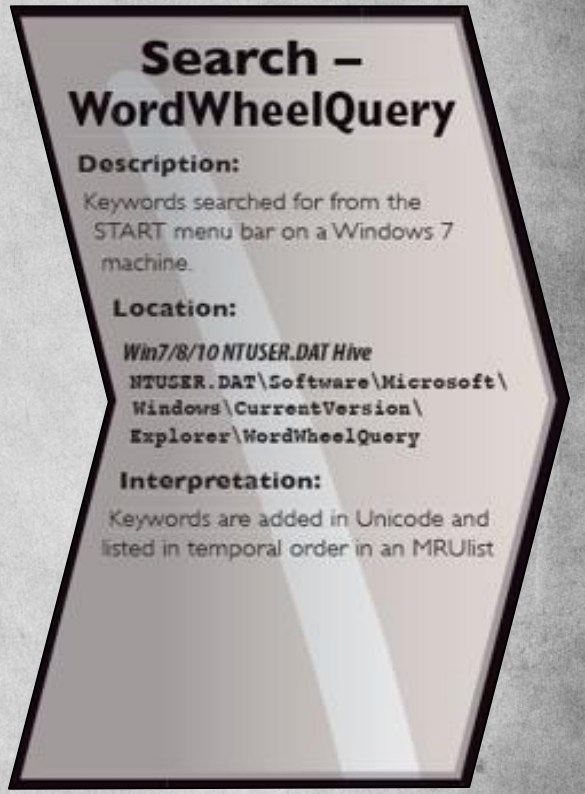
File Knowledge

- The most common forensic artifacts relative to file knowledge:
  - ✓ WordWheelQuery
  - ✓ Last-Visited MRU*
  - ✓ Thumbscache
  - ✓ Recycle Bin*
  - ✓ Browser Files



File Knowledge – WordWheelQuery

- Keywords searched for from the START menu bar on a Windows 7 / 8 / 10
- Keywords are added in Unicode and listed in temporal order in an MRUlist



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

File Knowledge – Browser Files

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

- IE tracks both local and remote file access history, not just internet browsing history
- As a result, IE can provide history of when files and applications were accessed on a system along with timestamps
- IE 10 & 11 Locations

%USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat

Physical Location

- There are four main ways to find forensics artifacts relative to the physical location of the system under investigation
  - ✓ Timezone
  - ✓ Network History
  - ✓ Cookies
  - ✓ Browser Search Terms

Physical Location – Cookies

- Cookies identify viewed websites and track network details including IP, date / time, and time zone
- IE, Firefox, and Chrome and each have specific cookie storage locations
  - ✓ IE 11 Cookies

%USERPROFILE%\AppData\Local\Microsoft\Windows\INetCookies

  - ✓ Firefox Cookies

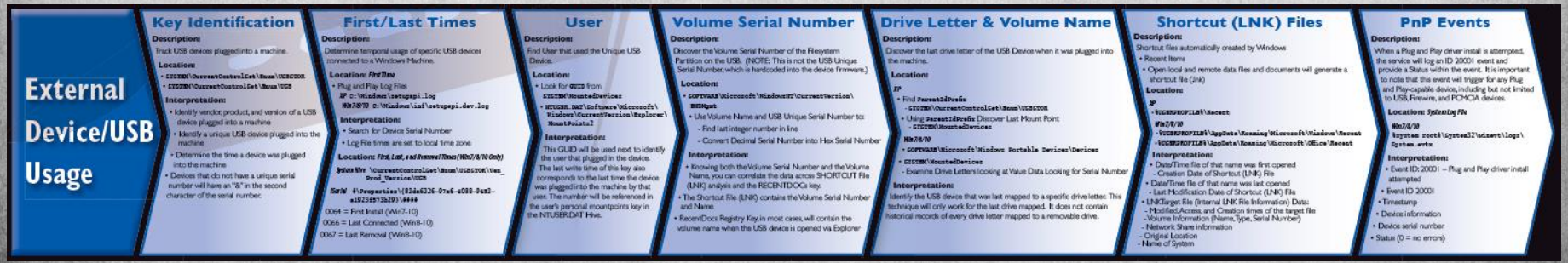
%USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\cookies.sqlite

  - ✓ Chrome Cookies

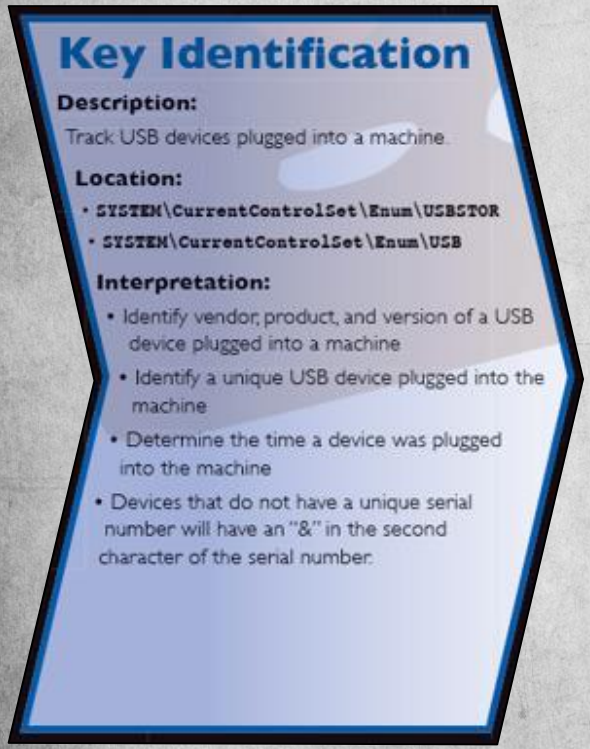
%USERPROFILE%\AppData\Local\Google\Chrome\UserData\Default\Local Storage

External Device / USB Usage

- Windows provides seven artifacts for the forensic analysis of externally connected devices
  - ✓ Key Identification
  - ✓ First / Last Device Connection Times*
  - ✓ User – USB Identification
  - ✓ Device VSN*
  - ✓ Device Drive Letter*
  - ✓ LNK File
  - ✓ PnP Events



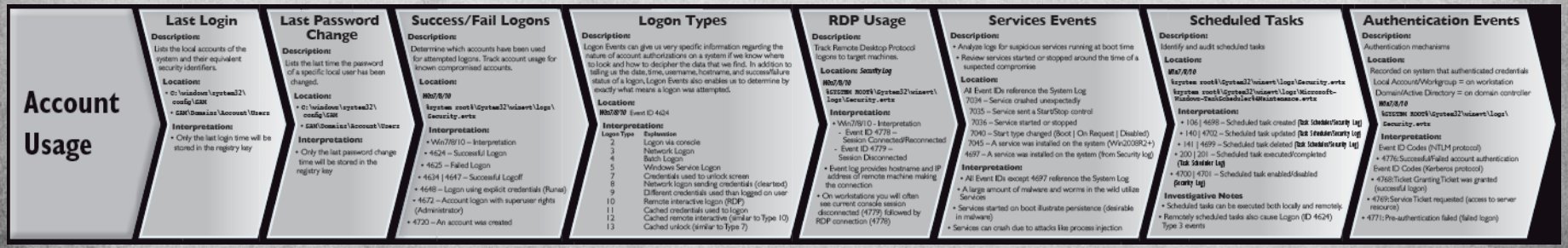
External Device / USB Usage – Key Identification



Track USB devices plugged into a specific system
Identify vendor, product, and version of a USB device plugged into a 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.

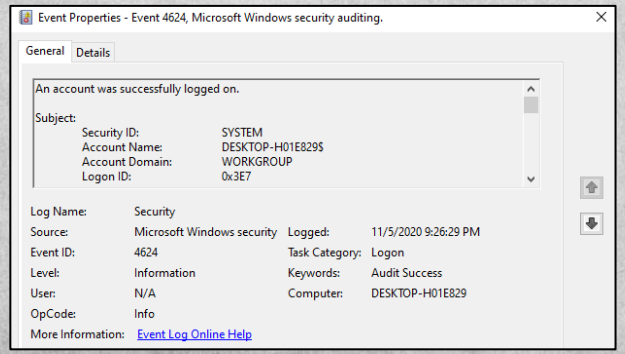
Account Usage

- Windows provides eight artifacts relative to account usage that can be identified through event logs and associated event ID's:
  - ✓ Last Login
  - ✓ Last Password Change
  - ✓ Success / Fail Logons
  - ✓ Logon Types
  - ✓ RDP Usage
  - ✓ Service Events
  - ✓ Scheduled Tasks
  - ✓ Authentication Events



Account Usage – Logons

- Windows event logs provide audit information for successful and unsuccessful logins
- Some of the more common logon related event ID's include:
  - ✓ Successful Logon – 4624
  - ✓ Failed Logon – 4625
  - ✓ Successful Logon – 4634 / 4647
  - ✓ Account Created – 4720



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

%system root%\System32\winevt\logs

Account Usage – RDP Usage

- Remote Desktop Protocol allows remote connection and graphical access to Windows systems
- Event log ID's related to RDP connections:
  - ✓ Session Connected or Reconnected – 4778
  - ✓ Session Disconnected – 4779
- Event logs will contain additional networking information
  - ✓ Remote IP Address
  - ✓ Hostname

%system root%\System32\winevt\logs\Security.evtx

Browser Usage

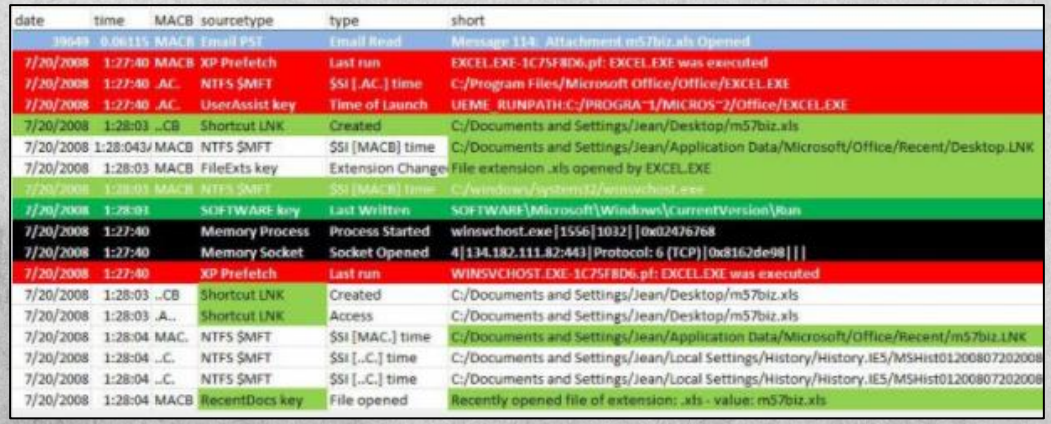
- There are six different artifacts relative to browser account usage:
  - ✓ History
  - ✓ Cookies
  - ✓ Cache
  - ✓ Session Restore
  - ✓ Flash and Super Cookies
  - ✓ Google Analytics Cookies

Timeline Analysis Tools

- With a knowledge of the different artifacts and their associated storage paths within Windows, we can now introduce the types of tools that can assist with providing a chronological listing of events
- Keep in mind that different artifacts are going to format time related information in different ways, so it will be necessary to parse files in different formats
- A few examples of some commercial and open-source log parsing and aggregation tools include:
  - ✓ LogStash
  - ✓ Splunk
  - ✓ Log2Timeline / Plaso
  - ✓ Timesketch

Log2Timeline / Plaso

- Plaso is a Python-based backend engine for Log2Timeline which is used to extract timestamps and aggregate results
- Some capabilities available when using these two tools:
  - ✓ Parsing Engines
  - ✓ Plug-Ins
  - ✓ Tagged Events



date	time	MACB	sourcetype	type	short
39649	0.06115	MACB	Email PST	Email Read	Message 114: Attachment m57biz.xls Opened
7/20/2008	1:27:40	MACB	XP Prefetch	Last run	EXCEL.EXE-1C75F8D6.pf: EXCEL.EXE was executed
7/20/2008	1:27:40	.AC.	NTFS $MFT	$SI [.AC.] time	C:/Program Files/Microsoft Office/Office/EXCEL.EXE
7/20/2008	1:27:40	.AC.	UserAssist key	Time of Launch	UEME_RUNPATH:C:/PROGRA~1/MICROS~2/Office/EXCEL.EXE
7/20/2008	1:28:03	..CB	Shortcut LNK	Created	C:/Documents and Settings/Jean/Desktop/m57biz.xls
7/20/2008	1:28:043/	MACB	NTFS $MFT	$SI [MACB] time	C:/Documents and Settings/Jean/Application Data/Microsoft/Office/Recent/Desktop.LNK
7/20/2008	1:28:03	MACB	FileExts key	Extension Change	File extension .xls opened by EXCEL.EXE
7/20/2008	1:28:03	MACB	NTFS $MFT	$SI [MACB] time	C:/windows/system32/winsvchost.exe
7/20/2008	1:28:03		SOFTWARE key	Last Written	SOFTWARE\Microsoft\Windows\CurrentVersion\Run
7/20/2008	1:27:40		Memory Process	Process Started	winsvchost.exe|1556|1032||0x02476768
7/20/2008	1:27:40		Memory Socket	Socket Opened	4|134.182.111.82:443|Protocol: 6 (TCP)|0x8162de98|||
7/20/2008	1:27:40		XP Prefetch	Last run	WINSVCHOST.EXE-1C75F8D6.pf: EXCEL.EXE was executed
7/20/2008	1:28:03	..CB	Shortcut LNK	Created	C:/Documents and Settings/Jean/Desktop/m57biz.xls
7/20/2008	1:28:03	.A..	Shortcut LNK	Access	C:/Documents and Settings/Jean/Desktop/m57biz.xls
7/20/2008	1:28:04	MAC.	NTFS $MFT	$SI [MAC.] time	C:/Documents and Settings/Jean/Application Data/Microsoft/Office/Recent/m57biz.LNK
7/20/2008	1:28:04	..C.	NTFS $MFT	$SI [..C.] time	C:/Documents and Settings/Jean/Local Settings/History/History.IE5/MSHist012008072020080
7/20/2008	1:28:04	..C.	NTFS $MFT	$SI [..C.] time	C:/Documents and Settings/Jean/Local Settings/History/History.IE5/MSHist012008072020080
7/20/2008	1:28:04	MACB	RecentDocs key	File opened	Recently opened file of extension: .xls - value: m57biz.xls

Log2Timeline Installation

- We will use Log2Timeline to aggregate our Windows artifacts
- Installation:
  - ✓ https://plaso.readthedocs.io/en/latest/sources/user/Ubuntu-Packaged-Release.html
  - ✓ sudo add-apt-repository ppa:gift/stable
  - ✓ sudo apt-get update
  - ✓ sudo apt-get install plaso-tools