WINDOWS FORENSICS

Cheat Sheet

Abstract

Embark on your Windows Forensics journey with this essential cheat sheet. Whether you're a novice investigator or a seasoned pro, these foundational artifacts will guide you through the intricate world of Windows system analysis.

Keval Parmar

Digital Forensics and Incident Response

Table of Contents

1. Introduction

When dealing with digital investigations, particularly in the Windows environment, having a comprehensive understanding of the operating system and its artifacts is crucial. The Windows Forensics Cheat Sheet serves as a concise guide for forensic analysts, incident responders, and security professionals. It provides essential information on where to find critical artifacts, interpret them, and use them effectively during investigations.

The Windows Forensics Cheat Sheet empowers investigators by providing quick access to critical artifacts and guidance on their interpretation. Whether you're analysing a compromised system, responding to a breach, or conducting proactive security assessments, this cheat sheet is an indispensable resource.

For more detailed information and practical examples, refer to the full cheat sheet and explore the open-source tools available for Windows forensic analysis.

What is Incident Response process?

The incident response process follows a cyclical pattern, allowing organizations to detect, respond to, and recover from security incidents. Here are the key phases:

1. **Preparation:**
    - Establish incident response policies, procedures, and a dedicated team.
    - Identify critical assets, define roles, and create communication channels.
2. **Identification:**
    - Detect and confirm security incidents.
    - Gather initial information about the incident's scope and impact.
3. **Containment:**
    - Isolate affected systems to prevent further damage.
    - Preserve evidence while minimizing disruption to business operations.
4. **Eradication:**
    - Remove the root cause of the incident.
    - Patch vulnerabilities, eliminate malware, and address security gaps.
5. **Recovery:**
    - Restore affected systems to normal operation.
    - Validate that the threat has been neutralized.
6. **Lessons Learned:**
    - Conduct a post-incident review.
    - Document findings, update procedures, and enhance security measures.

Remember, the incident response process is iterative. As new information emerges, revisit each phase to adapt and improve your defences.

2. Memory & Triage Acquisition

Memory is a crucial part of forensic investigations. Most of the volatile data resides into the memory.

It contains following items that will be useful in investigating any system.

- **Processes:** information about running processes.
- **Opened files:** details of currently files that are in use.
- **Registry keys and devices:** insights into system configuration.
- **Network connections:** active network sessions.
- **Encryption keys and passwords:** sensitive data temporarily stored.
- **Rootkits and memory-only exploits:** detecting stealthy threats.
- **Configuration settings**: system parameters.

Memory acquisition helps to bypass the disk encryption also.

There are two main things in windows:

- **Hibernation (After Windows 2000)** is a power-saving feature that uses less energy than sleep. When your system hibernates, it saves the content in memory onto the hard drive (inside the "Hiberfil.sys" hidden system file).

- **DRIPS** (**After Windows 8.1**) refer to the Deepest Runtime Idle Platform State. It corresponds to the lowest power state for the System on a Chip (SoC) during Connected Standby or Modem Standby. Understanding DRIPS helps uncover system behaviour during low-power modes.

  DRIPS helps determine the lowest power state of the System on a Chip (SoC) during Connected Standby or Modem Standby. Forensic analysts can assess the energy-saving behaviour of devices during these low-power modes. By understanding **DRIPS**, investigators gain insights into system behaviour during idle periods. It aids in reconstructing events, especially when the system is in a low-power state. **DRIPS** allows the SoC to wake up for specific events (e.g., network activity, input signals). Detecting these triggers can reveal hidden activities or unauthorized access.

  SleepStudy Report:

  It stores last 3 days of records which you can find using this command in CMD–

  powercfg /SLEEPSTUDY

  Look for the DRIPS histogram within the report. It reveals wake-up patterns during low-power sessions. typical low-power sessions have sleep time intervals close to 32 seconds. However, if the histogram shows sleep intervals less than one second (closer to 512 milliseconds), it implies frequent interrupts or hardware components preventing the system from entering DRIPS**.**

How to acquire Memory Image?

- **For live system RAM acquisition**:
  - FTKImager
  - Magnet
  - Dumpit
  - Belkasoft

- **For dead system RAM acquisition:**
  - Hibernation file = %SystemDrive%/hiberfil.sys
  - Page file = %SystemDrive%/pagefile.sys
  - Memory dump = %WinDir%/memory.dmp

How to analyse Memory?

There are many tools out there to analyse the memory, but **Volatility3** provides best utilities to do memory forensics.

Other than that, Memoryze & Volcano are there.

Volatility3: https://www.volatilityfoundation.org/3

Memoryze: https://fireeye.market/apps/211368

Volcano: https://www.volexity.com/company/contact/

How to acquire Disk Image?

First check for the encryption whether drive is encrypted or not. You can use tool called **EDD by magnet** to check.

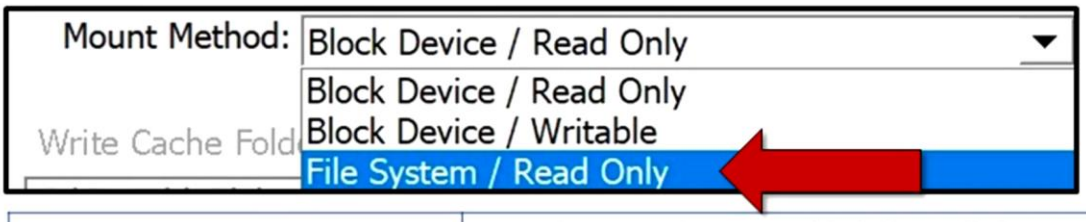
Tools to acquire image:

- FTK Imager
- CyLR (Command Line Tool)
- Arsenal Image Mounter

Mount Types:

Raw/DD, E01, S01, AD1, L01

FTK Imager Mount Method

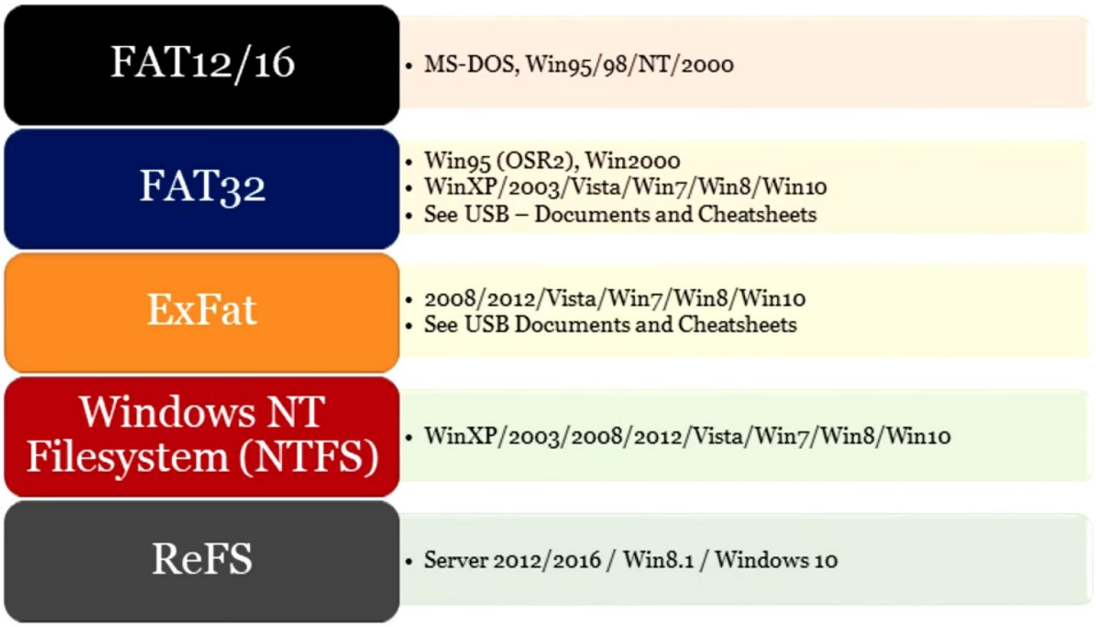


Block Device / Read Only	Treats the mounted image as a block device (disk). Image will be subject to NTFS permissions and Windows file/folder protection.
Block Device / Writable	Mounts image as a writable device, saving any changes in a cache file (no changes made to original image).
Filesystem / Read Only	Creates a virtualized folder structure, circumventing Windows file/folder protection. Shows deleted files. Filesystem starts in [root] folder.

This is logical mounted image which you can see by mounting it. AD1 & L01 images have no drive geometry, so they must be mounted logically.

Physical mounted images cannot be view by windows explorer, can be viewed by windows application that perform Physical Name Querying

3. Windows File System



- **FAT- File Allocation Table**
  - **FAT12/16 –** Used in floppy disk.
  - **FAT32 -** 32 Bit, 4GB file size limit, No security.
  - **ExFAT –** For specially USBs & SD Cards.
- **NTFS – New Technology File System.** 64 Bit, 16 TB (deleted files can be recovered unless that space is not overwritten.)
- **ReFS** – resilient filesystem. It is specially made for file server, but there is no forensics tool made for ReFS File System.

As of now, NTFS (New Technology File System) is the default file system used by Microsoft Windows for storing and retrieving files. It has replaced the older File Allocation Table (FAT) system and offers several advantages, including support for larger file sizes, improved security, and better performance.

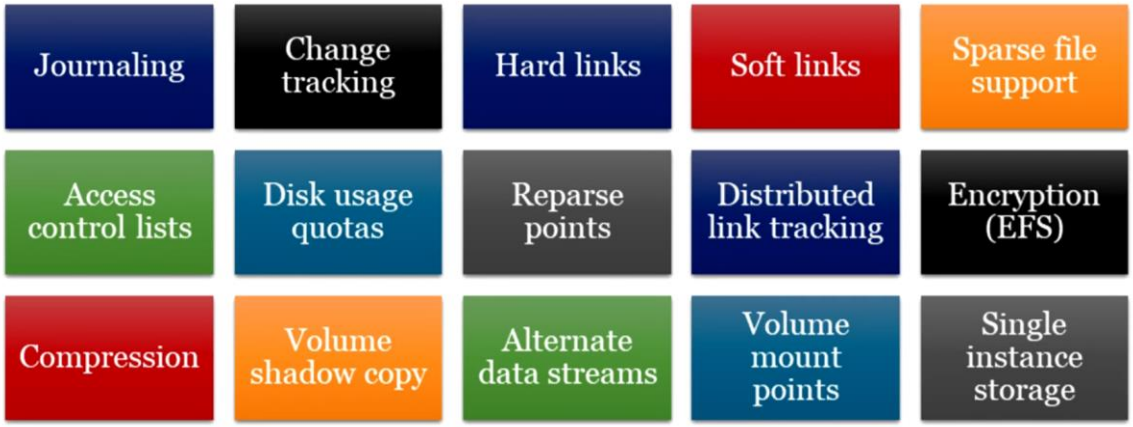
NTFS Cluster:

NTFS Cluster contains two types:

1. **Allocated:**
   a. data block is actively being used by a file.
   b. Data exists on file system not deleted.
2. **Unallocated:**
   a. Data block is not being used by a file.
   b. Data may or may not exist in the block or cluster.
   c. May contain deleted or unused data.

if data is deleted and that space where data was written is not overwritten than it is possible to recover that data. If user had wiped the hard disk than it is not possible to recover the deleted data. One wipe is enough to make it not possible to recover.

Core NTFS Features:



- **Notable NTFS Artifacts**
  - NTFS Time Stamps
  - Alternate data streams Zone.Identifier (from where file came)
  - Volume shadow copy

MFT (master file table):

The Master File Table (MFT) is a very structured database that tracks all the objects to be saved on an NTFS volume. Every object gets a FILE record within the MFT. It has 1024 bytes long records. The first 24 MFT entries are reserved for special use by the NTFS volume. The first 12 entries are used by system files that make NTFS work. These files are all named starting with a $ and are hidden from view unless using specialized tools.

#0 - $MFT: Master File Table. A database that tracks every file in the volume.

#1 - $MFTMirr: A backup copy of the first four records of the MFT.

#2 - $LogFile: Transactional logging file.

#3 - $Volume: Contains volume name, NTFS version number, dirty flag.

#4 - $AttrDef: NTFS attribute definitions.

#5 - . : Root directory of the disk. Tracks the allocation (in-use versus free) of each cluster in the volume.

#6 - $Bitmap: Tracks the allocation (in-use versus free) of each cluster in the volume.

#7 - $Boot: Boot record of the volume.

#8 - $BadClus: Used to mark defective clusters so that NTFS will not attempt to use them.

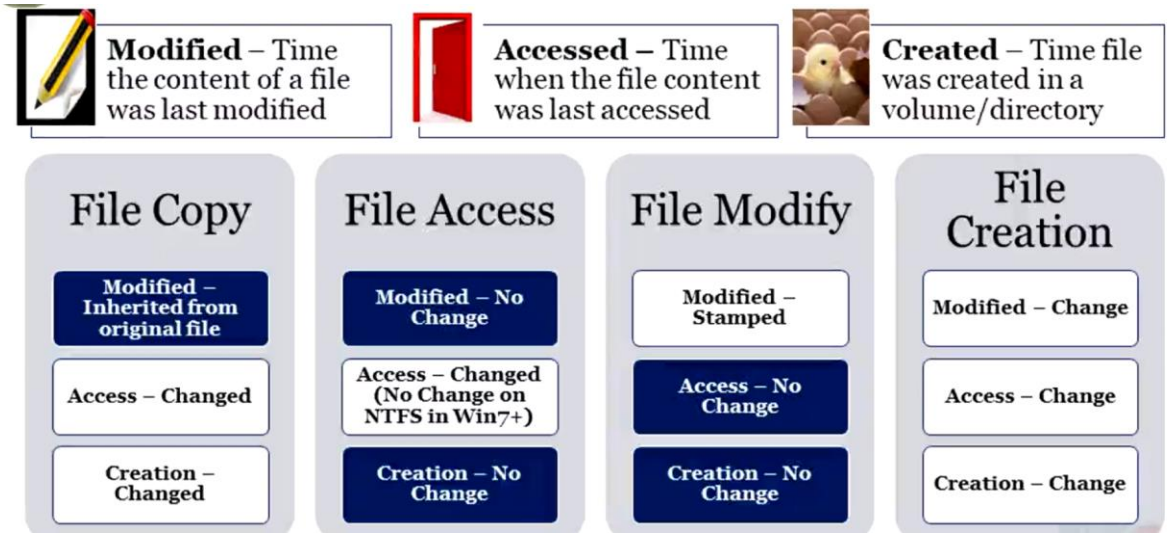
#9 - $Secure: Tracks security information for files within the volume.

#10 - $Upcase: Table of Unicode uppercase characters used to assist sorting filenames.

#11 - $Extend: A directory containing $ObjId, $Quota, $Reparse, $UsnJrnl.

Windows Time Rule:

Time rule will help you that how or when file is created. Is it copied? Is it created? Is it moved? It will answer to all those questions.



Zone.identifiers:

It will tell you that from where file had come.

- NoZone = -1
- MyComputer = 0
- Intranet= 1
- Trusted= 2
- Internet= 3
- Untrusted= 4

Shadow copy:

Shadow Copy, also known as **Volume Snapshot Service (VSS)** or **Volume Shadow Copy Service**, is a technology included in Microsoft Windows. It allows creating backup copies or snapshots of computer files or volumes, even when they are in use. Here's how it works:

1. **Snapshot Creation:**
    - A shadow copy is a snapshot of a volume that duplicates all the data held on that volume at a specific instant in time.
    - Windows periodically crawls the system, looking for file changes made since the last crawl. It records these changes, creating a history of the file/folder.
2. **Use Cases for Shadow Copies:**

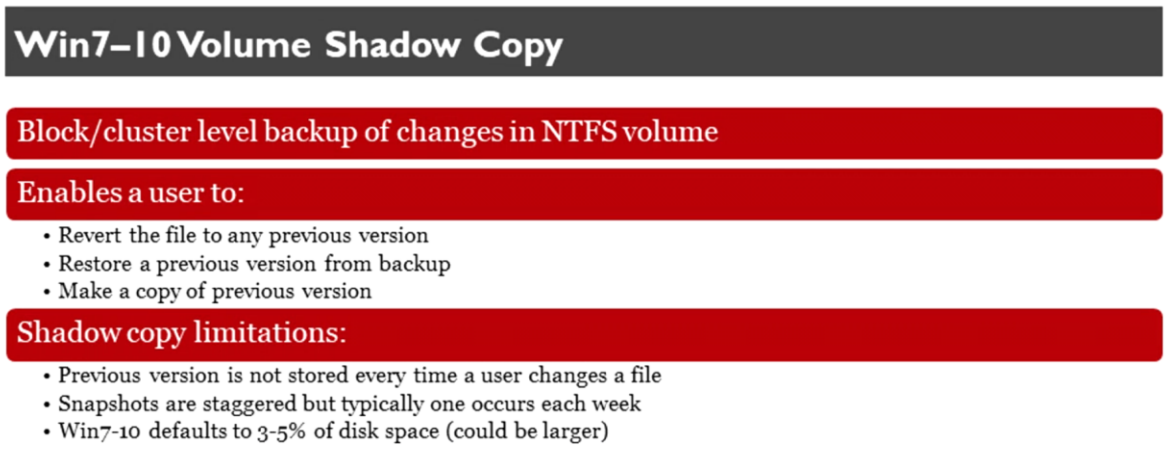
- **Restoring LUNs (LUN Resynchronization and LUN Swapping):** Shadow copies can be used to restore Logical Unit Numbers (LUNs) efficiently.
- **Restoring Individual Files (Shadow Copies for Shared Folders):** Allows retrieving specific files from a snapshot.
- **Data Mining:** Shadow copies aid in data analysis by providing historical views of file changes.

3. **Components of a VSS Solution:**

    - **VSS Service:** Part of the Windows operating system that ensures components can communicate and work together.
    - **VSS Requester:** The software (e.g., backup applications) that requests shadow copy creation.

Examples include Windows Server Backup and System Center Data Protection Manager.

Remember that shadow copies are valuable for data protection and recovery, especially when dealing with live applications and large data sets. They allow you to back up application data without taking applications offline, ensuring consistent backups and efficient restores.



Tools that can parse the volume shadow copy are:

- Magnet Forensics IEF
- VSC-Toolset: http://dfstream.blogspot.com/p/vsc-toolset.html
- Ubuntu SIFT Workstation with libvshadow installed on it: http://digital-forensics.sans.org/community/downloads
- Shadow Explorer

There are several ways to create a new volume shadow copy:

- System Snapshot
- Software Installation
- Manual Snapshot

SSD (Solid State Drive):

A **Solid-State Drive (SSD)** is a semiconductor-based storage device that uses integrated circuit assemblies to store data persistently. Unlike traditional hard disk drives (HDDs), SSDs have no moving parts.

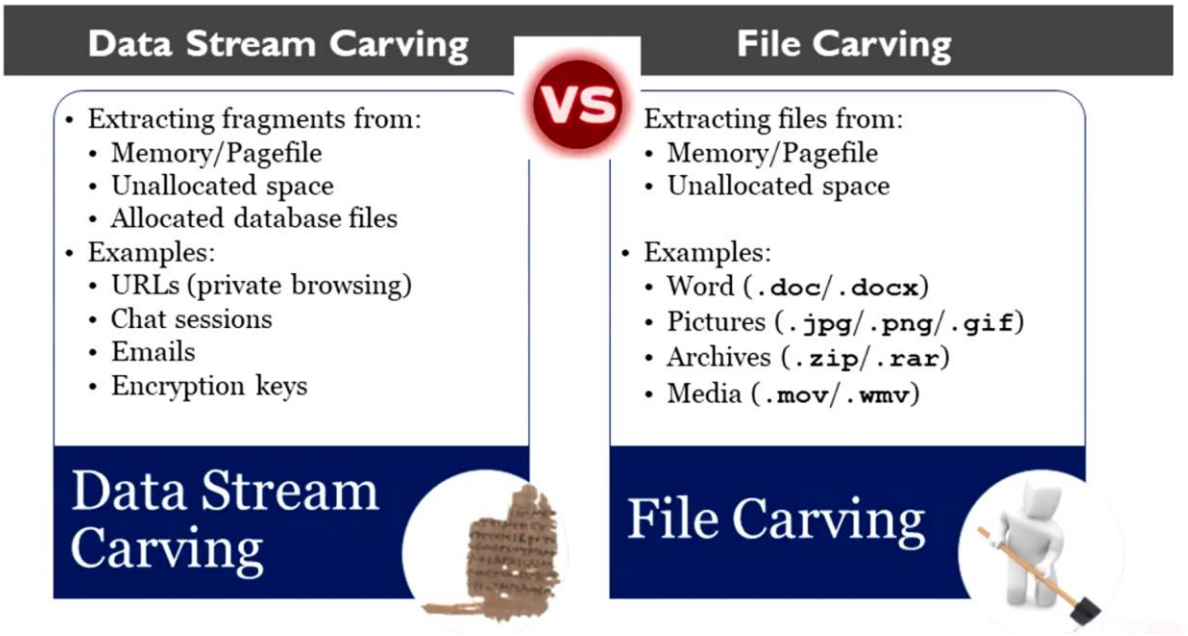
SSD manufacturers use non-volatile flash memory. SSD's do not require batteries. Non-volatility allows flash SSDs to retain memory during a sudden power loss. SSD design is proprietary. Most every detail is proprietary on the format of specifically how data is stored on the SSD.

In SSD reading/writing operation done very quickly and doing same operation to same place again & again will lead to corruption of hard disk. SSDs have limited number of writes and as a result will need two different capabilities that are used to help reduce the overall wear and tear of the SSD:

trim and wear levelling.

- **Wear levelling** means if content is change, store it to new location. Every 5 write cycle data moved to new location. Slack space disappears & you can no longer be sure that the exact physical location of sector.
- **Trim** tells OS that which file has been deleted & have free space in it which can be overwritten.

Data/File Carving:



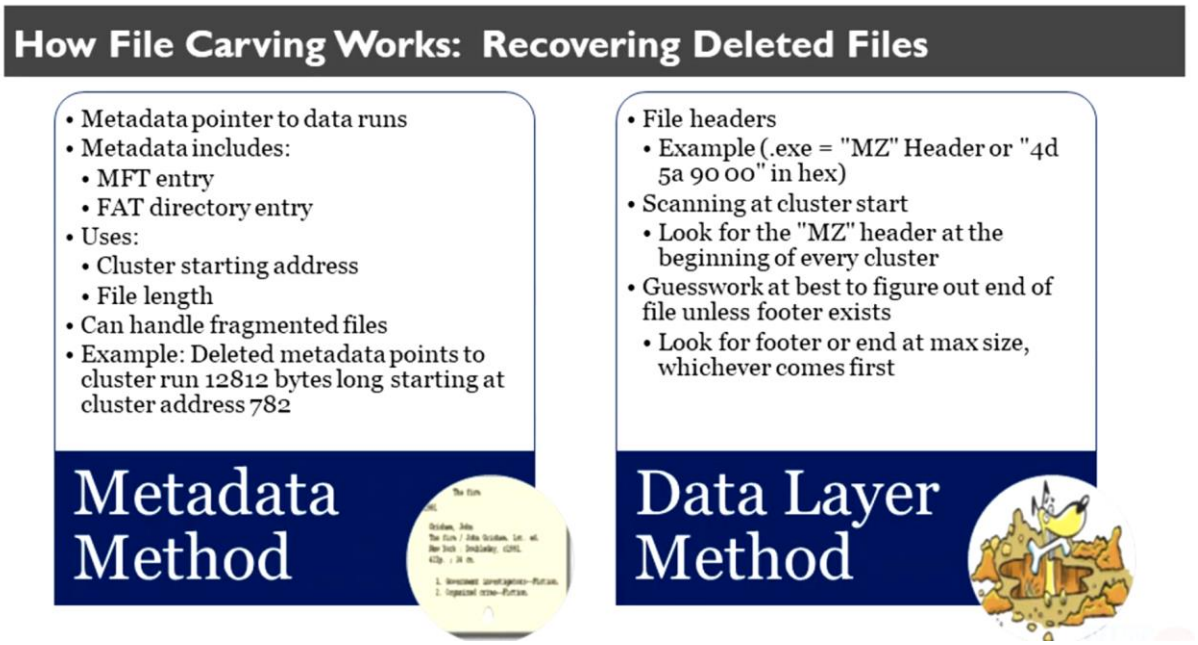
The Internet Evidence Finder (IEF) searches the selected drive, folder (and sub-folders, optionally), or file (memory dumps, pagefile.sys, hiberfil.sys, etc.) for Internet artifacts.

IEF can be downloaded from http://www.magnetforensics.com/

There is a lot of metadata of a file which helps us to identify that where, when and by whom file is created.

You can parse this data using a tool called:

EXIFTool: https://exiftool.org/



4. Windows Registry

The Windows Registry is a crucial component of the Microsoft Windows operating system. It serves as a centralized database that stores a wide range of information, settings, options, and values related to both software and hardware installed on Windows systems.

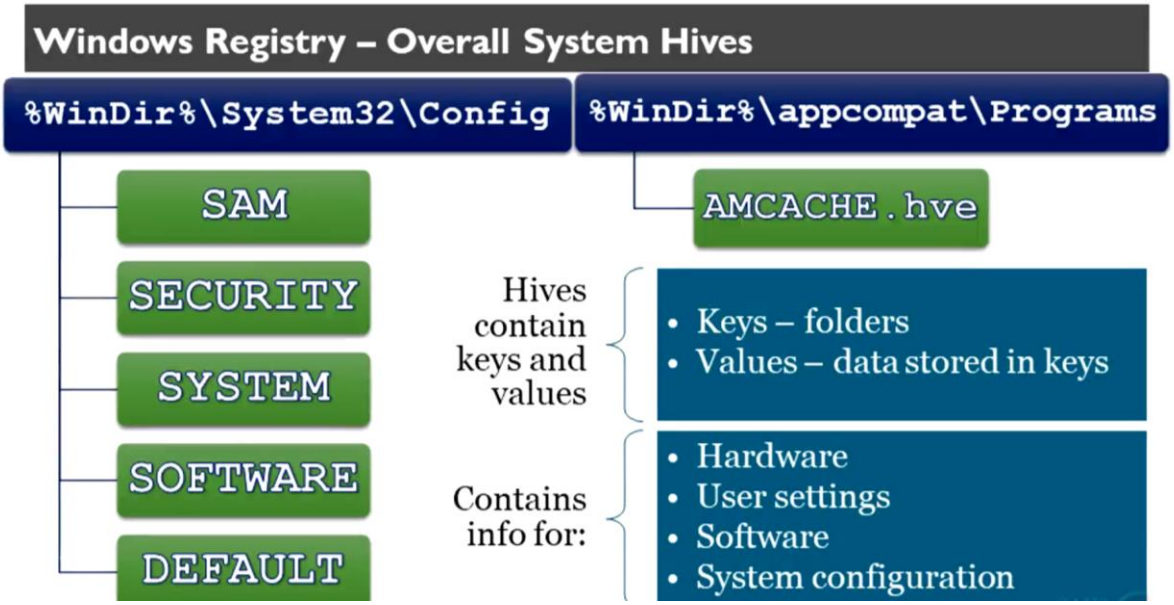
The registry is organized in a hierarchical structure with keys and subkeys. Each program or component installed on your system can create its own subkey within the registry.

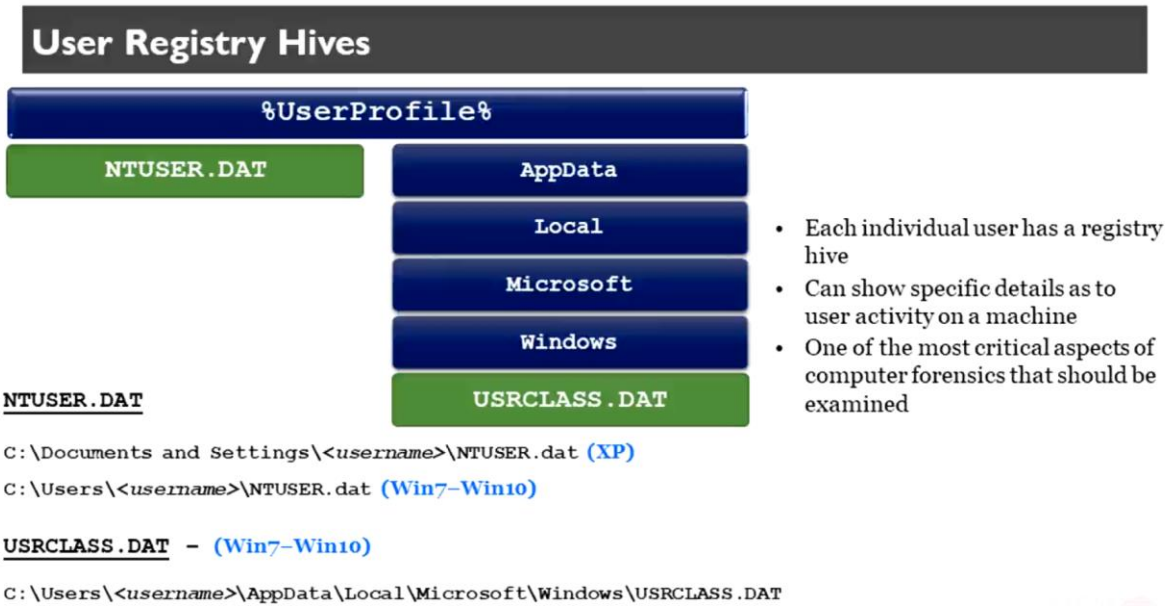
The registry contains information about:

- **System settings:** Such as startup programs, hardware configurations, and user preferences.
- **Application settings:** Including program-specific configurations.
- **Device drivers:** Information needed for hardware components to function properly.
- **User profiles:** User-specific settings and preferences.

Path:

- **Core Path:** System32/Config/RegBack
- **Amcache.hve:** %WinDir%/Appcompact/Programs
- **NTUser.dat:** %username%/
- **UserClass.dat:** %username%/Appdata/Local/Microsoft/Windows/





Difference between NTUSER.DAT & USERCLASS.DAT

NTUSER.DAT:

Contains user specific settings & configurations. All keys related to user.

USERCLASS.DAT:

Stores information about file associations & default settings for the user.

Which folder user has opened or closed. Aid for virtualized registry root for UAC (user account control).

AMCACHE.HVE

AmCache hive is in C:\Windows\AppCompat\Programs\Amcache.hve. Windows creates this hive to save information on programs that were recently run on the system.

Registry Hive	Nickname	File
HKEY_LOCAL_MACHINE\SAM	HKLM\SAM	**SAM**
HKEY_LOCAL_MACHINE\Security	HKLM\Security	**SECURITY**
HKEY_LOCAL_MACHINE\System	HKLM\System	**SYSTEM**
HKEY_LOCAL_MACHINE\Software	HKLM\Software	**SOFTWARE**
HKEY_USER or HKEY_CURRENT_USER	HKCU	**NTUSER.DAT**

Registry file contains log files also which is helpful to identify whether drive is dirty or not. Dirty hive doesn't have every data, when system gets restart it stores data that are in transection logs into registry hive permanently.

LOG1 file has data that is not written to registry, and it has started writing to registry.

LOG2 file have data means that data has been written to registry, and process of writing is completed.

If LOG1 & LOG2 files are not same, it means hive is dirty.

Each key has last written time so that we can see when the last registry has been changed.

There is Win32 API to timestamp the files but there are no Win32 API to timestamp the registry key. Users need to make function to do that.

MRUs are most recent used files. which indicates last changes made to registry.

Registry hives have unallocated space similar to file systems. A deleted key is marked as unallocated.

Recovery of unallocated keys is possible due to lack of anti-forensics tools.

Tools:

Registry acquisition:

- **KAPE–**https://www.kroll.com/en/services/cyber-risk/incident-response-litigation-support/kroll-artifact-parser-extractor-kape
- **Autopsy –** https://www.autopsy.com/download/
- **FTK Imager -** https://www.exterro.com/digital-forensics-software/ftk-imager

Rgistry Parsing:

RegRipper - https://github.com/keydet89/RegRipper3.0

RegEdit – it is windows default software.

Registry Explorer by Eric Zimmerman - https://ericzimmerman.github.io/#!index.md

Registry Forensics:

What is SAM Registry?

This hive lists the local accounts of the system and their equivalent security identifiers.

It is useful to discover username & RID mapped to them.

Last login

Last failed login

Logon count

Password policy

Account Creation Time

When a user logs in using a Microsoft Live ID, which most non-active directory systems will try and force you to do, the login count will not increment in our testing. The LiveID used for the login is stored under the IntemetUserName value. We can check whether password is required for an account or not using 3rd party tool SAMInside.

The empty NT-Hash is always 31D6CFe0d 16ae931 b73c59d7 e0c089c0.

SAMinside can be pointed to any specific SAM and SYSTEM hive files and tell you whether there are passwords set for an account. If you see a <Disabled> entry in the LM- or NT-Password field, then the hash type is currently turned off.

If you see a <Empty> field next to one of the LM- or NT-Password fields, then a password is not needed to log in.

What is a control set?

A control set contains system configuration settings needed to control system boot, such as driver and service information.

ControlSetO0 1 is typically the ControlSet that you just booted into the computer with. This is usually the most up-to-date version of the ControlSet.

Contro1Set002 is the "Last Known Good" version. This version is the one that is considered good when the previous boot occurred in case something drastic happened during the current boot cycle.

Considering we are examining the ControlSet not in an active machine, another way to look at this is that ControlSetO0l would be the last successful boot Of the machine and Contro1Set002 would be the previous "successful boot" before that.

You can identify by REG_DWORD key that which CurruntControlSet is this, if value is set to 1 that means this is the CurruntControlSet001.

NTFS Last Access Time ON/OFF:

Turns last access timestamp ON or OFF. If disabled, the last access timestamp recording in the NTFS file system will not occur.

fsutil behavior set disablelastaccess 0

To determine if last access timestamps are being updated on a system you are examining you can examine the following registry key.

SYSTEM\CurrentControlSet\Control\FileSystem

Locate NtfsDisableLastAccessUpdate ->If set to 0xl, then access time stamps are turned off.

If the last access timestamp is turned off, we will not be able to see when file data was last accessed by the system.

Network Interface:

The key's location is found here in the SYSTEM hive:

SYSTEM\CurrentContro1Set\Services\Tcpip\Parameters\Interfaces

it will allow you to see the TCP/IP information configured, the IP address, the gateway, and other potentially useful information.

If the machine was configured for DHCP, it will contain the DHCP IP address that was assigned, the subnet mask, and the DHCP server's IP address.

Network Location Awareness (NLA) has been built into Win7 and up to aid the user to identify where the computer might be connected to adjusting the firewall appropriately.

This also allows for some very unique forensic information to be obtained through this structure.

"First, let's start with what NLA does. For each network interface the PC is connected to, NLA aggregates the network information available to the PC and generates a globally unique identifier (GUID) to identify each network.

In other words, it creates a network profile for any network it connects to. The Windows Firewall then uses that information to apply rules from the appropriate Windows firewall profile.

This allows you to apply a different set of firewall rules depending on which network you are connected to.

For example, a public network could get a very restrictive set of rules, a home network could get a less restrictive set of rules, and a managed network could get a set of rules determined by an administrator."

With NLA, it will show a list of all the networks the machine has ever connected to via their DNS suffix (for example, sans.org). Identifying intranets and networks that a computer has connected to is incredibly important.

Investigators will find this key useful due to the fact that in some cases, just by examining this key, it might be able to give you the geo-location of where this laptop might have been based on identifying the networks that it attached to and when.

Most info regarding NLA will be stored under the following three places:

HKLM\Software\Microsoft\Windows NT\CurrentVersion\NetworkList

HKLM\Software\Microsoft\Windows\CurrentVersion\HomeGroup

C:\Windows\System32\NetworkList

The network type will be listed as

either 0x47 (hex) for wireless, 0x06 (hex) for wired, or 0xl 7 (hex) for broadband (3g) networks.

The "Category" value specifies what type of network the user chose when selecting the network profile.

Public (0) Private/Home (1) Domain/Work (2).

You can find Geo-location of MAC address/SSID by using,

http://wigle.net/

Client-Side Caching (CSC)

When user is not connected to network, and they want to access network files at that time CSC is useful.

Users need to select offline file access mode so that OS will copy all files into local system, these cached copies named offline flies.

We can see how folder is cached via CSCFlags:

Windows Offline Files caches files in the directory **C: \Windows\ CSC**.

• **CSCFlag = 0**: Default option means that the user must specify which files he would like to be cached.

• **CSCFlag = 16**: For automatic document caching, "All files and programs that users open from the shared folder are automatically available offline" with the "optimize for performance" unchecked.

• **CSCFlag = 32**: For automatic program caching. Same as above, but with "Optimize for performance" checked.

• **CSCFlag = 48:** Caching is disabled.

• **CSCFlag = 2048:** Default Win7-lO setting until user disables the "Simple File Sharing" or uses the "advanced" sharing options. It is also the default setting for "Homegroup."

Type: Type of device or share accessed [2]

• 0 = Disk Drive or Folder

• 1 = Printer

• 2 = Device

• 3 = IPC

• 2147483648 = Admin (Disk, Printer, Device, or IPC)

What is SHIMCACHE?

Application compatibility checking within windows OS. Checks to see if applications to be "Shimmed" to run application on currentOS or via olderOS parameters.

AppCompactCache will track the executable file's last modification date, file path and if it was executed.

Application will be shimmed again if the file content is updated or renamed.

BAM & DAM

Background Activity Moderator

Desktop Activity Moderator

It is for windows 10 only. It provides full path of the execution file and also last execution date.

Registry keys:

System Information:

OS Version:

- SOFTWARE\Microsoft\Windows NT\CurrentVersion

Current Control set:

- HKLM\SYSTEM\CurrentControlSet
- SYSTEM\Select\Current
- SYSTEM\Select\LastKnownGood

Computer Name:

- SYSTEM\CurrentControlSet\Control\ComputerName

Time Zone Information:

- SYSTEM\CurrentControlSet\Control\TimeZoneInformation

Network Interfaces and Past Networks:

- SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces

Autostart Programs (Autoruns):

- 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
    - Ifstart value is set to 0x02, then service will start at boot.

SAM hive and user information:

- SAM\Domains\Account\User

Shutdown Information

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

BAM/DAM (Windows 10):

- SYSTEM\CurrentControlSet\Services\bam\UserSettings\{SID}
- SYSTEM\CurrentControlSet\Services\dam\UserSettings\{SID}

External Devices:

Device identification:

- SYSTEM\CurrentControlSet\Enum\USBSTOR

- SYSTEM\CurrentControlSet\Enum\USB

First/Last Times:

- SYSTEM\CurrentControlSet\Enum\USBSTOR\Ven_Prod_Version\USBSerial#\Properties\{83d a6326-97a6-4088-9453-
  - a19231573b29}\####
  - Oo64=first connection
  - 0066=last connection
  - 0067=last removal

USB device Volume Name:

- SOFTWARE\Microsoft\Windows Portable Devices\Devices
- HKLM\SYSTEM\MountedDevices
- Find Serial # to obtain the Drive Letter of the USB device.
- Find Serial # to obtain the Volume GUID of the USB device.

Program Execution:

Last Command Executed in Run:

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

RecentApps Key – GUI Program Execution:

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Search\RecentApps

GUI Program Execution: UserAssist Key:

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

For XP/VISTA:

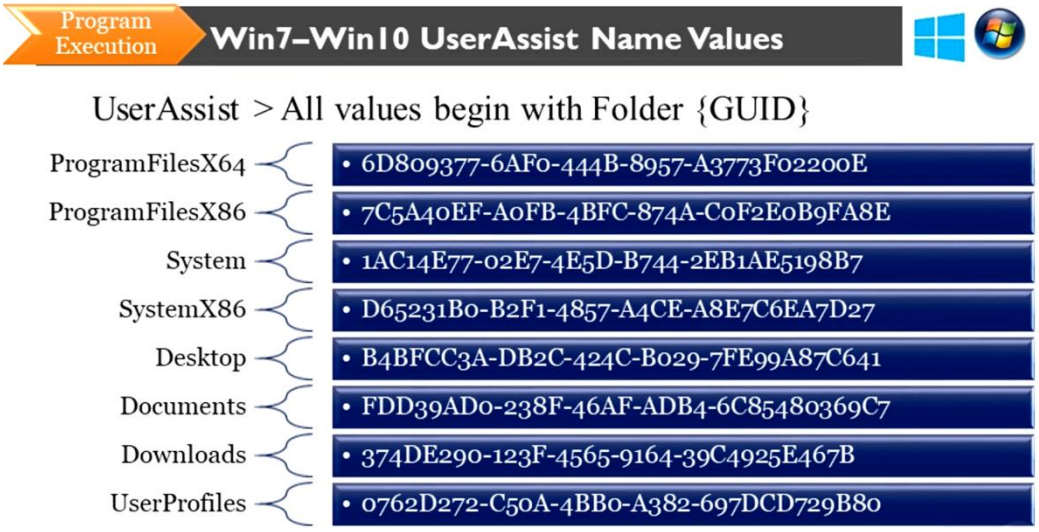
5e6ab780 -> Internet Toolbar

75048700 -> Active Desktop

Win7 +:

CEBFF5CD -> Executable file execution

F4E57C4B -> Shortcut File Execution



Application Compatibility Cache ShimCache:

XP -> SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatibility\AppCompatCache

Server 2003/2008/2012, WIN 7-10:

SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatCache\AppCompatCache

Application Compatibility Cache AmCache:

AmCache.hve\Root\File\{Volume GUID}\######

File/Folder Usage:

Recent Files:

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

Office Recent Files:

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

ShellBags:

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

Open/Save and LastVisited Dialog MRUs:

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

Windows Explorer Address/Search Bars:

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

Network Behaviour:

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList

- \Signatures
  - \Unmanaged (record DefaultGatewayMac, DnsSuffix, FirstNetwork (SSID), ProfileGuid)
  - \Managed

- \Nla
    - \Cache
- Profiles

Most info regarding NLA will be stored under the NetworkList key above, and also:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\HomeGroup
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList**Profiles**\{**GUID**}

Network Types:

- 0x06 = Wired
- 0x17 = Broadband
- 0x47 = Wireless

Category:

- 0 – Public
- 1 – Private
- 2 - Domain/Work

Auditing Registry Through PowerShell:

- Get-ChildItem -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\'
- Get-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\'
- Get-ItemPropertyValue -Path 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\' -name SecurityHealth
- Get-ChildItem -Path 'HKLM:\SYSTEM\CurrentControlSet\Enum\USBSTOR'
- Get-ChildItem -Path 'HKLM:\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_SanDisk&Prod_Cruzer_Blade&Rev_1.00'

Malware Persistence in Registry:

- **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run and RunOnce**
- **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run and RunOnce**
- **HKEY_CLASSES_ROOT\Directory\Background\Shell** – Launches while running any shell or on mouse click option.
- **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects** - BHOs can modify browser behavior, inject advertisements, or steal sensitive information.
- **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services**–Create as a service themselves.
- **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices**-Malware may add entries here to run as a service during user login.
- **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows** and add as AppInit_DLLs
- **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Notify** – Launches itself when windows kernel event occurs, such as user login, user logoff.

- **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shared TaskScheduler** - Malware may add entries under this key to run code when the Windows Explorer starts.
- **HKEY_CURRENT_USER\Control Panel\Desktop\SCRNSAVE.EXE** - Malware can modify this value to set a screensaver executable that contains malicious code.

5. ShellBags Item

ShellBags:

- **What Are Shellbags?**
  - **Shellbags** are a set of registry keys that contain details about a user's viewed folders.
  - These details include information such as:
    - Folder size.
    - Position (where the folder appears on the screen).
    - Icon associated with the folder.
  - Essentially, shellbags track and maintain a history of directory traversal within the registry.

- **Where Are Shellbags Located?**
  - In Windows XP, shellbags are stored within the **NTuser.dat** hive.
  - In Windows 7 and later versions, they reside in the **UserClass.dat** hive under **HKCU (HKEY_CURRENT_USER)** (or **HKCR for Win7+**).
  - The shellbags held in the **BagMRU** (Most Recently Used) follow a structure like that found within Windows Explorer, with numbered folders representing parent/child relationships.
  - Each newly explored folder creates a corresponding shellbag entry.
  - The data within these shellbags is stored in hexadecimal format, making it challenging to interpret directly.

- **Why Analyze Shellbags?**
  - **Folder Access:** Shellbag analysis reveals information about folder access, including desktop items, control panel categories/items, drive letters, directories, and even compressed archives.
  - **Evidence of Activity:** It acts as a historical record, indicating what directory items may have been removed from the system.
  - **Traversal Patterns:** Shellbags provide evidence of directory navigation and traversal, potentially revealing remote access (e.g., RDP or VNC) and interactions with network resources.
  - **Deleted Folders:** Information persists even for deleted folders, serving as a valuable reference for items no longer part of the file system.

- **Shellbags Analysis Tools:**
  - **ShellBags Explorer:** Developed by Eric Zimmerman, this tool allows you to explore shellbag data visually (GUI) or via the command line (CLI).
  - It provides a visual representation of the user's directory structure, enabling recursive sorting, filtering, and manipulation of shellbags.
  - Timestamps (creation, access, interaction) are exposed, allowing the creation of a timeline for investigative purposes.

Recent Documents Shortcut Files(.lnk):

LNK automatically created by windwos in recent folders. If you create a file in folder, it will create two links – file link & parent folder link. If you create a folder in a folder, it will create three links – folder link, parent folder & grandparent folder. When we make same file name in different location It will point to the last file that we have accessed.

Max=149/2 (lnk files) = around 75 last lnk files we can see.

This LNK files will point to:

Target file MAC times

Volume Information (Name, Type, Vol. Serial #)

Fixed, removable, or Network Target

Original Path & Location.

Tool:

LEcmd.exe – LNK Explorer Command line edition by ERIC Zimmerman

First opened time = file creation

Last opened time = file modification

If target modified time > target created = indicates copy of a file.

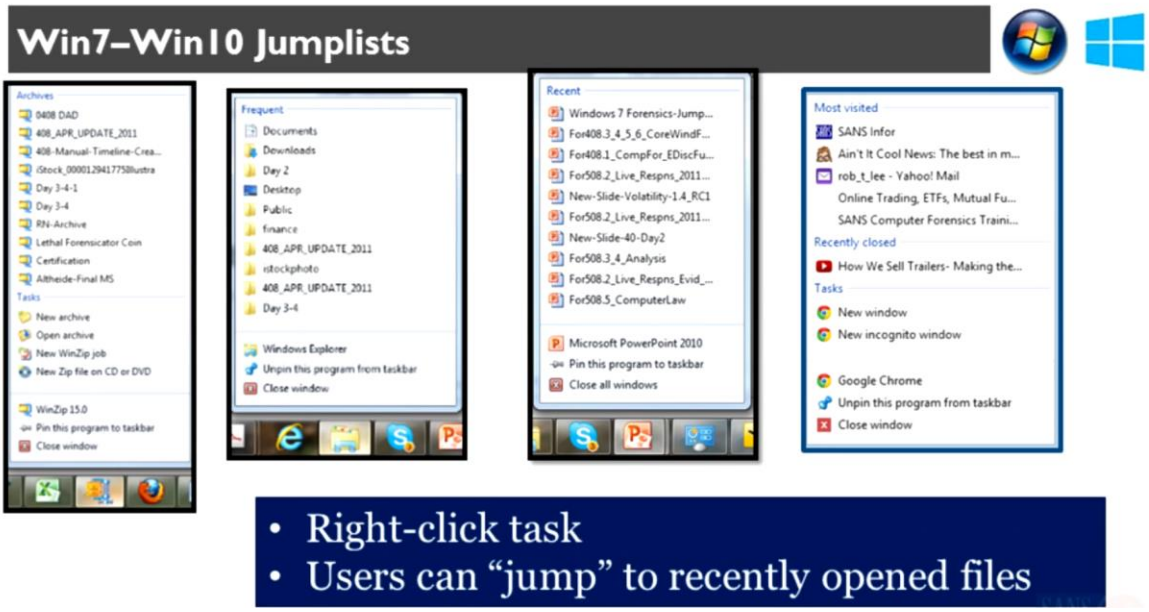
Jumplist:

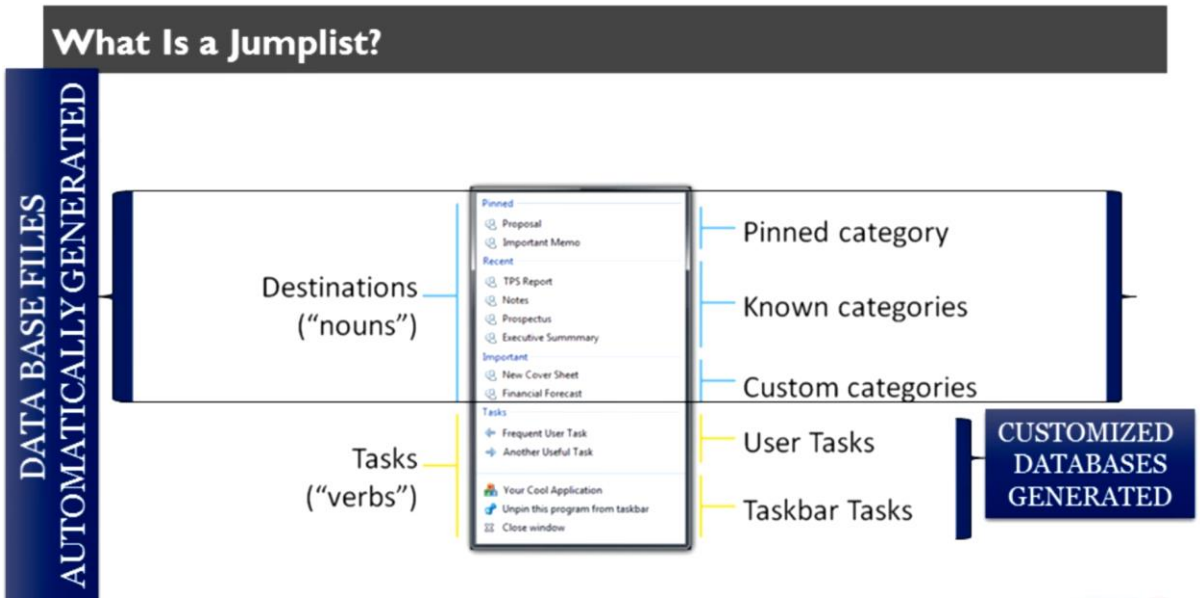
It is a recent file that user have last accessed. There are two types of Jumplists are there.

Automatic jumplist is created automatically when the user opens a file or application.

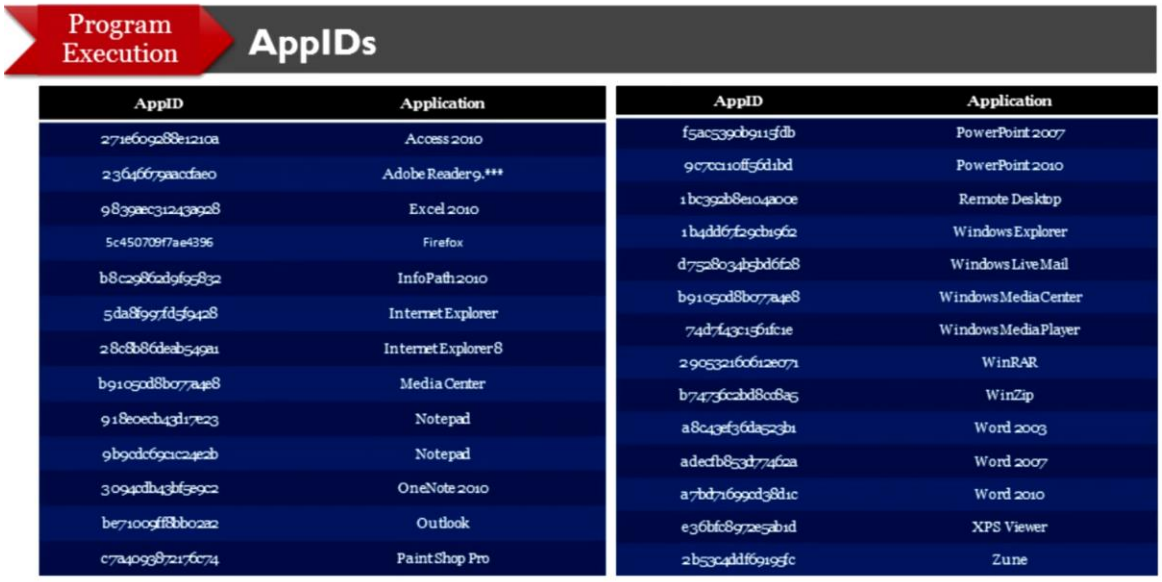
Custom jumplist created when user pins a file or application to Taskbar or start menu.

When user starts any program from start menu entry will be added to the Jumplist.





When you parse a jumplist it will show Application ID rather than name of application this id remains same in every device. Following list contains some of the famous applications and their IDs.



AppID	Application
271e60928e1210a	Access 2010
2364f679aacdae0	Adobe Reader 9.***
9839aec31243a928	Excel 2010
5c450709f7ae4396	Firefox
b8c29862d9f95832	InfoPath 2010
5da8f997fd5f9428	Internet Explorer
28c8b86deab549a1	Internet Explorer 8
b91050d8b077a4e8	Media Center
918e0ecb43d17e23	Notepad
9b9cdc69c1c24e2b	Notepad
3094cdb43bf3e9c2	OneNote 2010
be71009ff8bb02a2	Outlook
c7a4093872176c74	Paint Shop Pro

AppID	Application
f5ac539cb9115fdb	PowerPoint 2007
9c7cc110ff56d1bd	PowerPoint 2010
1bc392b8e104a00e	Remote Desktop
1b4dd67f29cb1962	Windows Explorer
d75280345b5bd6f28	Windows Live Mail
b91050d8b077a4e8	Windows Media Center
74d7f43c151d1c1e	Windows Media Player
2905321606120e071	WinRAR
b74736c2bd8c08a5	WinZip
a8c43ef36da523b1	Word 2003
adecfb853d77462a	Word 2007
a7bd71699cd38d1c	Word 2010
e36bfc8972e5ab1d	XPS Viewer
2b53c4ddf6919f5c	Zune

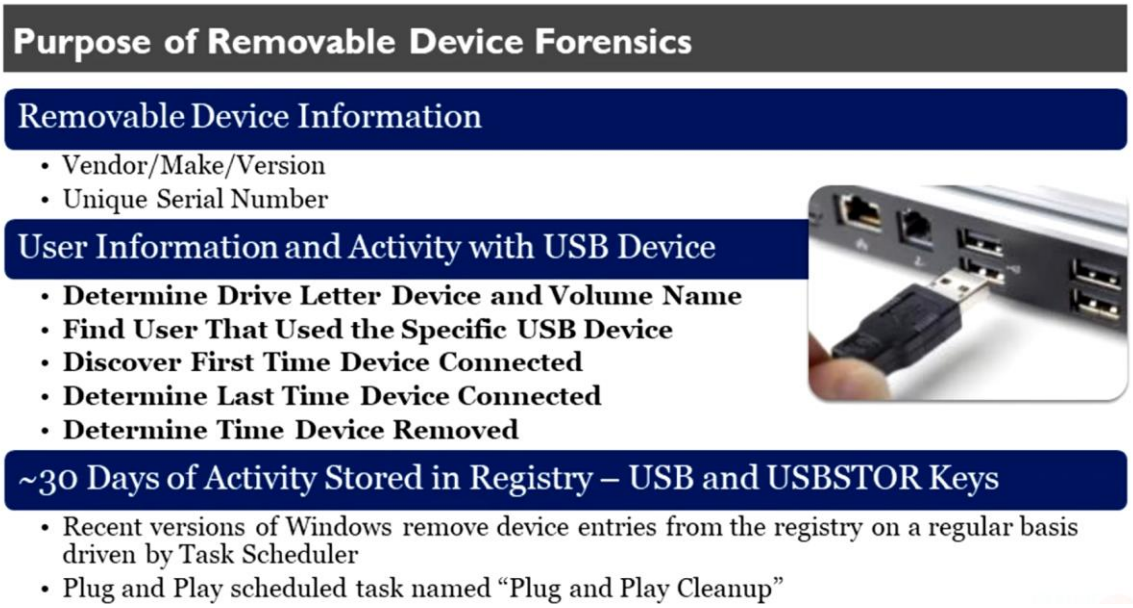
Tool:

JLEcmd.exe

6. USB Forensics

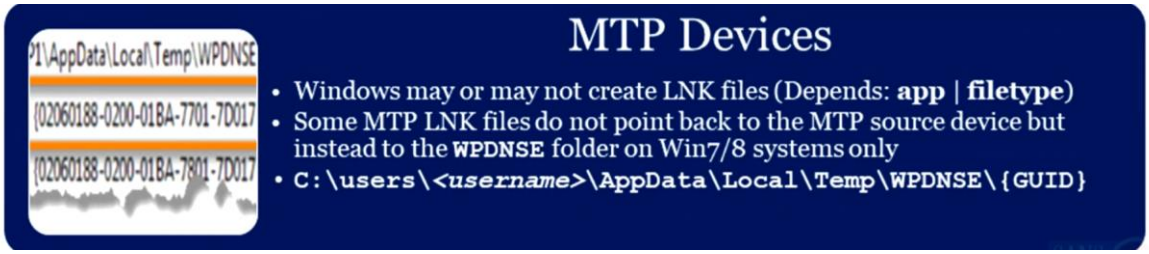
USB forensics plays a crucial role in Windows forensics, and here's why it's important:

- **Valuable Evidence Source:** USB devices are ubiquitous in our digital lives. People use them for data transfer, storage, and communication. As a result, investigating USB artifacts becomes crucial during digital forensic examinations. These artifacts provide valuable evidence about user activities, file transfers, and system interactions. By analysing USB-related data, investigators can gain insights into how external devices were used and their potential involvement in criminal activities or security incidents.
- **Role in White-Collar Crimes:** USBs play a significant role in white-collar crimes. Whether it's corporate espionage, data theft, or unauthorized access to sensitive information, USB devices are often at the center of such activities. Seizing USB devices during forensic investigations allows us to understand their role in potential criminal acts. By examining USB artifacts, we can trace the connections between devices, files accessed, and user behaviour.
- **Artifact Locations and Interpretation:** The Windows operating system maintains a record of USB device history in various locations, including the Windows registry and system files. These artifacts reveal when a USB device was connected, which specific device it was, and whether any data transfers occurred. For instance, the Event Viewer logs USB-related events, providing timestamps for device insertion and removal. Additionally, the registry contains information about the last plugged-in USB storage devices. Properly interpreting these artifacts helps reconstruct timelines and understand the context of USB device usage.



There are 3 protocols to be used:

- Mass storage class
- Picture transfer protocol
- Media transfer protocol.

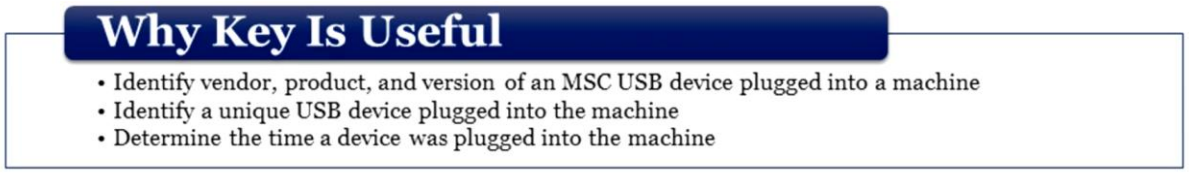


USBSTOR:

PATH: SYSTEM/CurruntControlSet/Enum/USBSTOR

MSC, PTP And MTP USB Enumeration

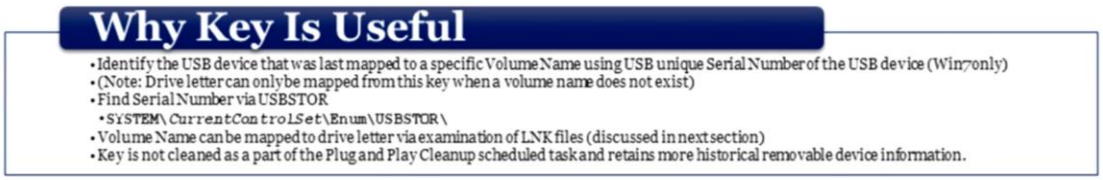
PATH: SYSTEM/CurruntControlSet/Enum/USB



DEVICE WITHOUT A UNIQUE SERIAL NUMBER WILL HAVE AN "&" IN THE 2nd CHARACTER OF SERIAL NUMBER.

Discover Volume Name of USB:

SOFTWARE\Microsoft\Windows Portable Device\Devices



Find User that used USB device:

1. **After discovering volume name look for GUID:**

   SYSTEM\MountedDevice

2. **Using GUID go to NTUSER.DAT and look for MountPoints**

   NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2

First and Last Connected & USB Removal:

SYSTEM\CurrentControlSet\Enum\USBSTOR\Ven_Prod_Version\USB iSerial#\Properties\{GUID}\####

0064 – First Install

0066 - Last Connected

0067 – Last Removal

It will give 64-bit Hex Windows Time which you can parse using – DCode Tool https://www.digital-detective.net/dcode/

PnP log files:

Setupapi.log:

XP -> C:\Windows\setupapi.log

Win7-10 -> C:\Windows\inf\setupapi.dev.log

You can see this log file using any text editor tool.

You can also look into Event Logs to track time of removable devices.

IF EMDMgmt Ket Present -> Discover Volume Serial Number

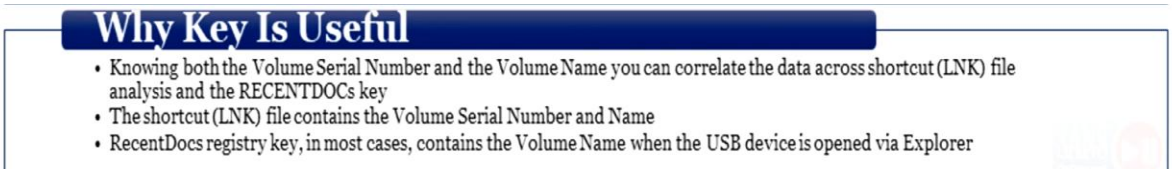
On Win7+ this key may not be populated if the internal drive is an SSD. This is created when a filesystem is initially formatted.

This key is traditionally used for ReadyBoost (**Readyboost** is used to make flash memory as caching database between hard disk and RAM.) but is disabled if the system is an SSD.

ReadyBoost is a Windows program that caches frequently used files. It leverages free space on fast removable devices, such as flash drives, CompactFlash memory cards, and Secure Digital (SD) cards, to augment system memory. The primary goal is to enhance overall performance without requiring users to purchase additional hardware. RAM significantly influences system speed, so ReadyBoost helps by fetching frequently used files from the flash drive instead of relying solely on RAM.

SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt

Use volume name and USB Unique Serial Number to find.



Tool:

There is a tool to automate the USB device forensics.

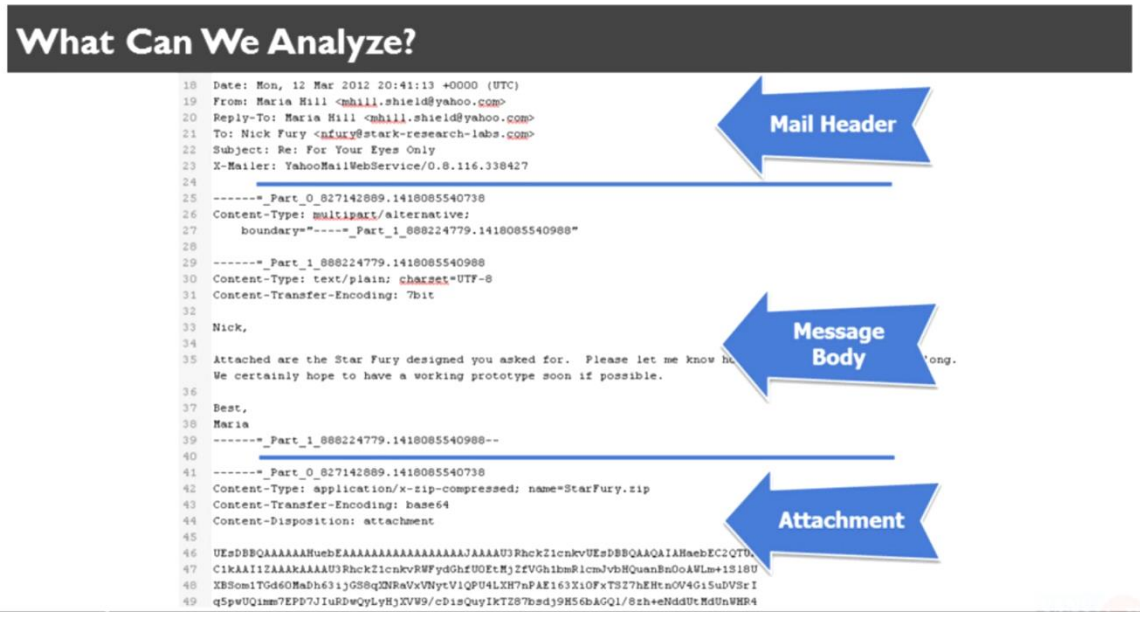
USBDeviceForensics - https://github.com/woanware/usbdeviceforensics

7. E-Mail Forensics

E-mail forensics is a critical field within digital forensics. Email communication is a common vector for cybercrimes such as phishing, fraud, and data breaches. Forensic experts analyse email evidence to trace the origin, identify malicious actors, and understand the attack vectors. In legal cases, emails serve as crucial evidence. Intellectual property theft, harassment, and insider threats can be detected through email forensics. Corporations investigate employee misconduct, policy violations, and unauthorized data sharing. Email trails help reconstruct events, timelines, and interactions. Investigating insider threats, data leaks, or sensitive information exposure relies on analysing email content. Email headers, metadata, and content provide clues for authentication. Determining the authenticity of an email or identifying the sender is crucial. Malicious attachments or links in emails can lead to malware infections. Forensic experts analyse email attachments, URLs, and payloads to understand the attack. Email forensics ensures adherence to privacy and security standards.

What E-Mail Forensics tells us?

- **Who sent the mail?**
- **When was it sent?**
- **Where was it sent from?**
- **Is there relevant content?**



Email Headers

```
X-Received: by 10.107.12.150 with SMTP id 22mr12969805iom.71.1425596919087;
      Thu, 05 Mar 2015 15:08:39 -0800 (PST)
Received-SPF: none (google.com: <redacted> does not designate permitted sender hosts) client-ip=216.82.254.107;
Authentication-Results: mx.google.com; spf=none (google.com: <redacted> does not designate permitted sender hosts)
Return-Path: <redacted> >
Received: from [216.82.254.67] by server-11.bemta-7.messagelabs.com id FD/5E-02764-6F1E8F45; Thu, 05 Mar 2015
23:08:38 +0000
Received: from [99.6.44.118] (helo=<redacted>) by
From: John H <redacted>
To: <redacted>
Subject: Thought you should know
Date: Thu, 5 Mar 2015 15:11:48 -0800
Message-ID: <003501d05788$c2415a20$46c40e60$@earthlink.net>
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="----=_NextPart_000_0036_01D05756.B41F0480"
X-Mailer: Microsoft Outlook 14.0
Thread-Index: AdBXmcGEc8JRPZK/S0KLRGIzUpoAeA==
Content-Language: en-us
X-Originating-IP: 99.6.44.118
```

E-Mail Authentication:

SPF (Sender policy framework):

Validates the sending IP address the originating domain.

DKIM (Domain key identified mail):

Verifies that message content has not changed via digital signature.

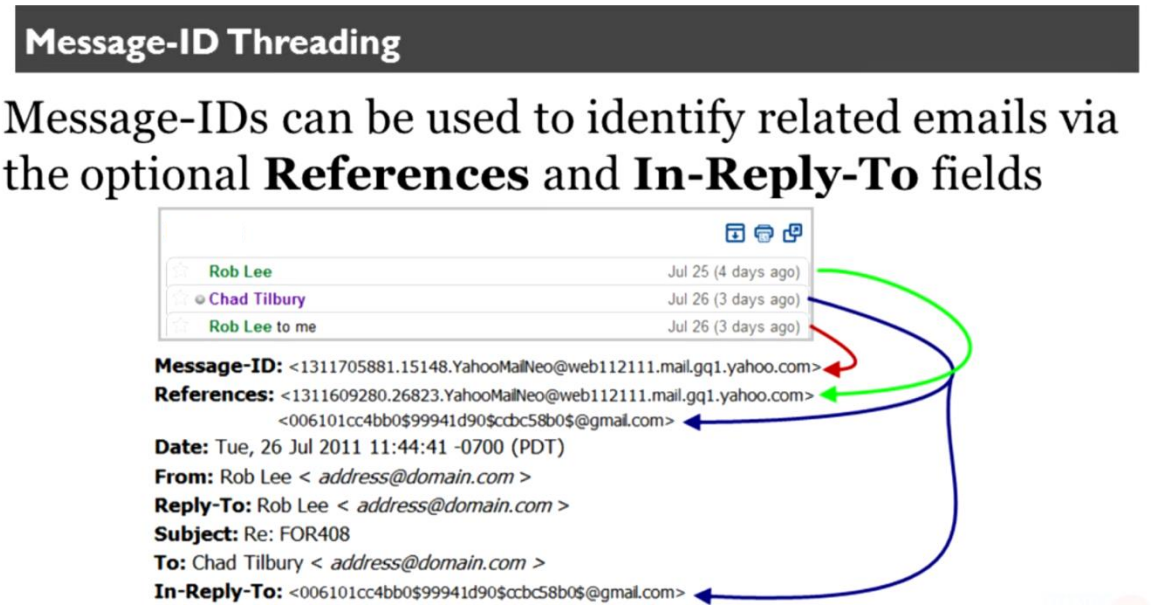
Valid SPF & DKIM increase trust in other parts of the header.

```
Received-SPF: pass (google.com; domain of guccifer20@aol.fr designates 204.29.186.19 as permitted sender) client-ip=204.29.186.19;
Authentication-Results: mx.google.com; dkim=pass header.i=mx.aol.fr; spf=pass (google.com; domain of guccifer20@aol.fr designates
   204.29.186.19 as permitted sender) smtp.mailfrom=guccifer20@aol.fr; dmarc=pass (p=QUARANTINE dis=NONE)
   header.from=aol.fr
```

What is Message-ID?

According to RFC 2822, the standard for email format, each email should have a globally unique identifier called Message-ID. The Message-ID is a critical field in the email header. It comprises a long string of characters that ends with the Fully Qualified Domain Name (FQDN). Message IDs are generated by client programs that send emails, such as Mail User Agents (MUA) or Mail Transfer Agents (MTA).

Message-IDs can be used to identify related E-Mails via the optional References and IN-Reply-To fields.



Messaging Applications Programming Interface:

The Messaging Application Programming Interface (MAPI) is an essential API for Microsoft Windows that enables programs to become email aware. MAPI allows applications to interact with email systems. While designed to be protocol-independent, it is commonly used to communicate with Microsoft Exchange Server. MAPI provides functions for accessing message transports, message stores, and directories.

It significantly increases the properties present in an E-Mail.

- Additional timestamp
  - MAPI-Client-Submit-Time (Local System Time)
  - MAPI-Conversation-Index (times of other messages in thread)
- Additional unique identifiers
  - MAPI-EntryID
- Information on actions taken on message.
  - MAPI-message-Flags
  - Pr_Last_Verb_Executed (read, replied, forwarded, etc.)

Host Based E-Mail Forensics:

host-based email forensics, which involves analysing email evidence directly on the host system.

- E-Mail stored on the local machine.
- Identify all email storage locations.
  - Find via filetype search.
  - Review email client configuration information.
- Potential for password protection.
- Search for deleted email archives.

Microsoft Outlook:

File Extension:

.PST

Path:

%USERPROFILE%\AppData\Local\Microsoft\Outlook (outlook 2010 and earlier)

%USERPROFILE%\Documents\Outlook (Outlook 2013/16)

Registry key:

HKEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\Windows Messaging\Subsystem\Profiles\Outlook

Offline Folder Files:

When you work with Microsoft Outlook, you have the option to operate in offline mode. This is particularly useful when you want to avoid connection charges or when your network connection is slow. With a Microsoft Exchange Server or Microsoft 365 account, you can enable offline mode to work seamlessly without being connected to the network.

Here's how you can switch between working offline and online in Outlook:

- Click on Send / Receive in the ribbon.
- Select Work Offline.
- When you're working offline, the Work Offline option will be highlighted on the ribbon or displayed in the status bar at the bottom of the Outlook window.
- To go back online, click Send / Receive and choose Work Offline again.

You can also adjust how much email data is available when working offline:

Navigate to File > Account Settings > Account Settings.

Select your Exchange or Microsoft 365 account and click Change. Under Offline Settings, adjust the slider to choose the desired amount of time (e.g., all, 12 months, 6 months, 3 months, or 1 month).

Note that Cached Exchange Mode must be turned on for this feature to work. By default, Outlook synchronizes 12 months of email data, but you can customize this setting.

Offline Outlook Data File (.ost):

Most account types, including IMAP, Microsoft 365, Exchange, and Outlook.com, use an Offline Outlook Data File (.ost).

An .ost file stores a synchronized copy of your mailbox information on your local computer. It allows you to work with the contents of an Exchange folder even when you're offline. The next time you connect to the Exchange server, the offline folders are automatically synchronized with the server.

Location of Offline Outlook Data Files:

drive:\Users\user\AppData\Local\Microsoft\Outlook

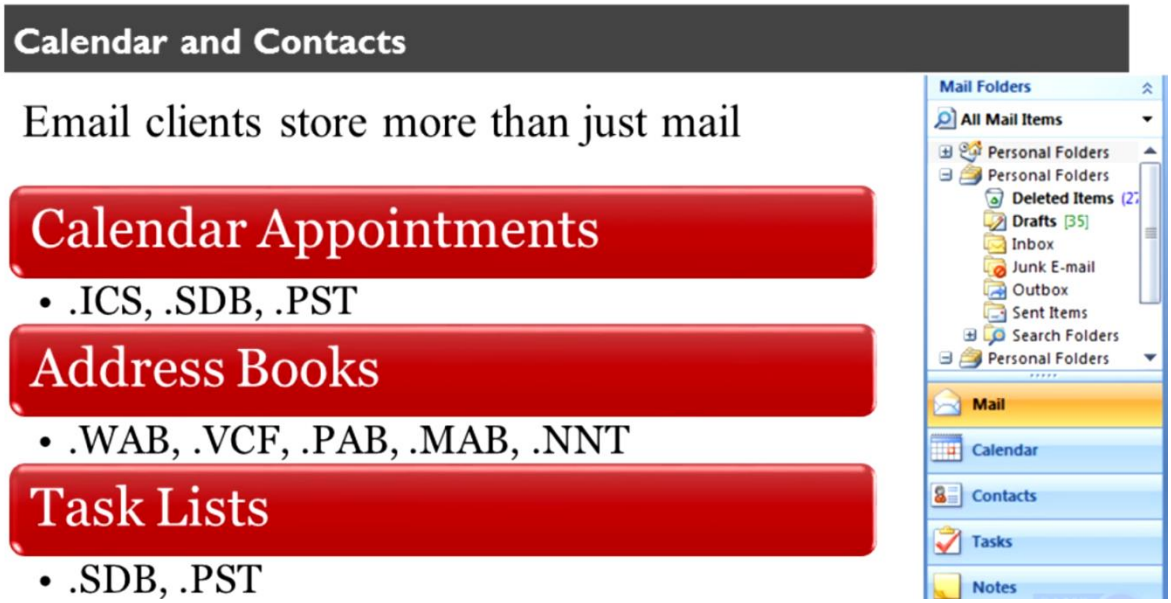
Outlook Attachment Recovery:

Outlook uses a "Secure Temp Folder" to open an attachment. Previewed and opened attachments can be recovered. Prior to Outllook 2007, attachments persisted util disk cleanup. In OutLook2007+ attachments remains only if message or Outlook is closed before the attachment or in the event of application crash.

Path:

%APPDATA%\Local\Microsoft\Windows\Temporary Internet Files\Content.outlook

%APPDATA%\Local\Microsoft\Windows\INetCache\Content.outlook



E-Mail Encryption:

Email encryption ensures that the content of your emails remains confidential and secure during transmission. When you send an encrypted email, only the intended recipient (who possesses the decryption key) can read its contents. Even if intercepted, the email appears as gibberish to unauthorized parties.

Types of Email Encryption:

S/MIME (Secure/Multipurpose Internet Mail Extensions):

- S/MIME provides end-to-end encryption for individual emails. It uses digital certificates to sign and encrypt messages.
- When you send an S/MIME-encrypted email, the recipient's email client decrypts it using their private key. S/MIME requires both the sender and recipient to have valid certificates.

PGP (Pretty Good Privacy):

- PGP is another method for end-to-end email encryption. It uses public-key cryptography.
- With PGP, you generate a key pair (public and private keys). You share your public key with others, and they can use it to encrypt messages to you.
- Only you can decrypt these messages using your private key. PGP is widely used for secure email communication.

E-Mail Server:

An email server, also known as a mail server, is a software program responsible for sending and receiving email messages between mail clients.

It acts as a virtual post office, handling the distribution of incoming mail to local users and sending out outgoing messages.

Most corporate environments employ dedicated mail servers, also can be hosted offsite or cloud.

Because of massive amount of data and business considerations it makes forensics copies difficult to make, you may require specialized tools.

It stores deleted mail for a short time.

Microsoft Exchange:

Microsoft Exchange is an email and collaboration platform that provides business-class features for organizations. It offers both hosted (cloud-based) and on-premises solutions. Key features include email, calendars, contacts, tasks, and more. Exchange might be broken up into multiple storage groups, each with multiple .EDB database. Mail box can be exported in .PST file format.

Extension:

.EDB: stores mail, attachments, contacts, Journal, Notes, Tasks, calendar & address book entries.

.LOG: contain messages not yet written to .EDB

"Recoverable Items" in Exchange

Deletions	Items removed from user's Deleted Items folder; <shift>+<delete> items; Deleted mail from POP or IMAP accounts
Purges	Temp location for hard-deleted items from Deletions folder and items that exceed retention period
Discovery Hold	Deleted items from mailboxes placed on hold
Versions	Copy-on-write changes to items in active mailboxes placed on hold
Audits	Audit log entries for mailboxes with auditing enabled
Calendar Logging	Calendar changes when calendar logging is enabled
Message Tracing	Log showing message details of sent and received mail

- By default, email retained for 14 days and mailboxes for 30 days
- Exchange 2010+ includes indexing and retention of *all* deleted objects

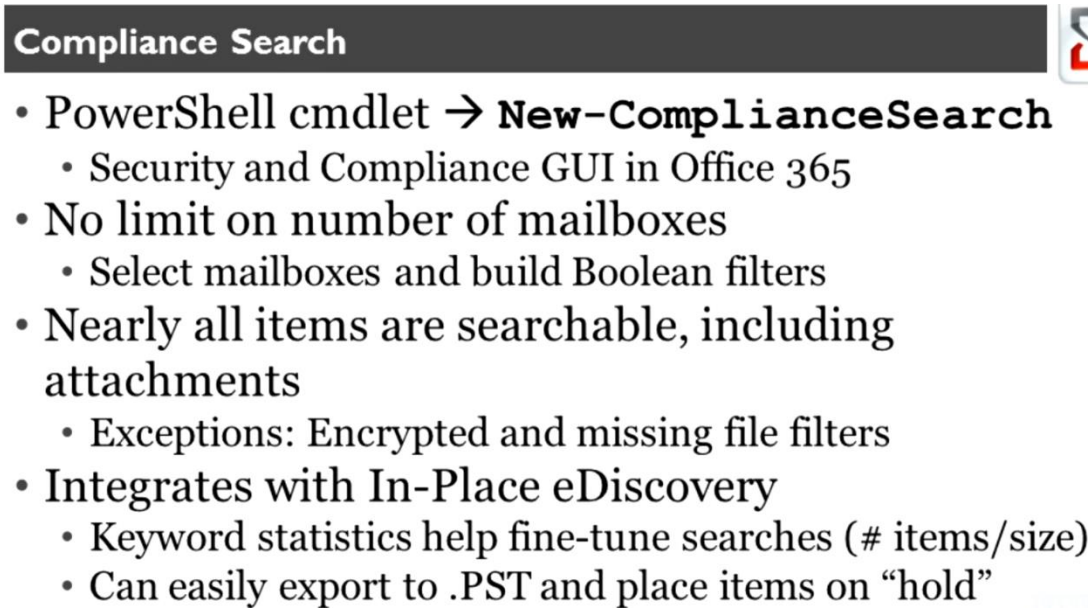
Export mail in exchange:

PowerShell is now the easiest way to export mail:

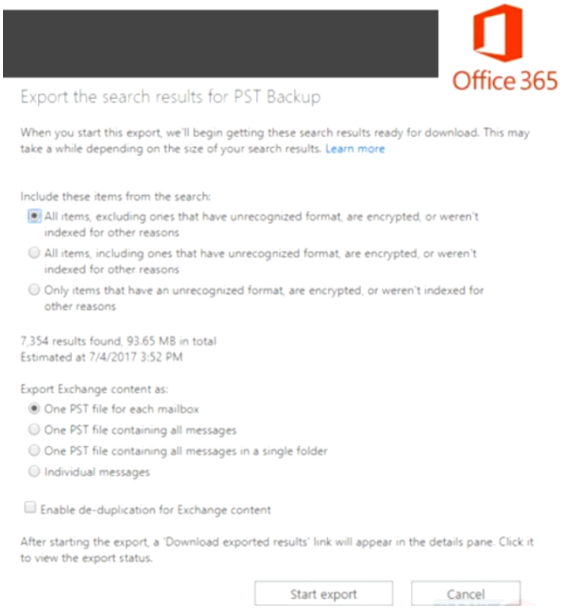
New-MailboxExportRequest -Mailbox usrename -FilePath \\server\folder\roblee.pst

Output can be filtered by nearly every mail component:

New-MailboxExportRequest -Mailbox usrename -ContentFilter { (body -like "*HYDRA*") -and (Received -it "03/02/2012") } -FilePath \\server\folder\roblee.pst



You can also export mails to .pst using office 365.



Unified Audit Logs in Office 365

- Search and export logs
  - Exchange Online
  - SharePoint Online
  - OneDrive for Business
  - Azure AD
- Not enabled by default
  - Need to enable for *each* user
  - Up to 90 days retention
- Much to be desired
  - No default logging for owners
  - Viewed messages only for admin users (MessageBind)
  - No logoff events
  - IP address and client included

Action	Admin	Delegate	Owner
Copy	✓		
Create	✓	✓	✓
FolderBind	✓	✓	
HardDelete	✓	✓	✓
MailboxLogin			✓
MessageBind	✓		
Move	✓	✓	✓
MoveToDeletedItems	✓	✓	✓
SendAs	✓	✓	
SendonBehalf	✓	✓	
SoftDelete	✓	✓	✓
Update	✓	✓	✓

Tools:

F-Response - https://www.f-response.com/

Kernal .OST and .PST file viewer - https://www.nucleustechnologies.com/pst-viewer.html

8. Additional Artifacts

Windows Search Database:

Windows Search plays a crucial role in helping users find files, emails, and other content on their Windows systems. The Windows Search database stores information related to indexed files, directories, and more.

As forensic investigators, understanding this database can provide valuable insights during investigations. Windows Search uses the Extensible Storage Engine (ESE) to store its data.

Interestingly, ESE is the same engine that Microsoft Exchange utilizes for its databases. However, due to the proprietary nature of ESE, limited information is available in the public domain about its structure and forensic analysis.

Path:

C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb

Tools:

Libesedb - https://github.com/libyal/libesedb

ESE Database View - https://www.nirsoft.net/utils/ese_database_view.html

Sanderson ESE DB Extension – https://sqliteforensictoolkit.com/ese-extension/

LostPassword's Search Examiner - https://www.passware.com/products/

ESE NT Utilities – Windows.edb

Windows ships with an ESE recovery tool : **ESENTUTL**

https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh875546(v=ws.11)

ESE NT Utilities – Windows.edb

Windows ships with an ESE recovery tool: **esentutl**

Read headers: **esentutl /mh Windows.edb**

Recover dirty db: **esentutl /r edb /d**

Repair dirty db: **esentutl /p Windows.edb**

```
C:\cases\Windows>esentutl /r edb /d

Extensible Storage Engine Utilities for Microsoft(R) Windows(R)
Version 6.3
Copyright (C) Microsoft Corporation. All Rights Reserved.

Initiating RECOVERY mode...
    Logfile base name: edb
            Log files: <current directory>
        System files: <current directory>
   Database Directory: <current directory>

Performing soft recovery...
                        Restore Status (% complete)

          0    10   20   30   40   50   60   70   80   90  100
          |----|----|----|----|----|----|----|----|----|----|
          ..................................................

Operation completed successfully in 0.437 seconds.
```

Thumbnails:

By default, Windows displays thumbnails for various file types, including images, videos, and documents.

Thumbnails are miniature representations of the actual content, allowing you to quickly identify files without opening them. However, sometimes you might encounter issues where thumbnails don't display correctly or appear as default icons.

It stores thumbnails in thumbs.db. it catalogues pictures in a folder and stores a copy of the thumbnails even if the picture were deleted.

Location:

WinXP: automatically anywhere.

Win7/8/10: automatically created anywhere accessed via a UNC (Universal naming Convention) path

Thumbcache:

Win7/8/10 Thumbcache Path:

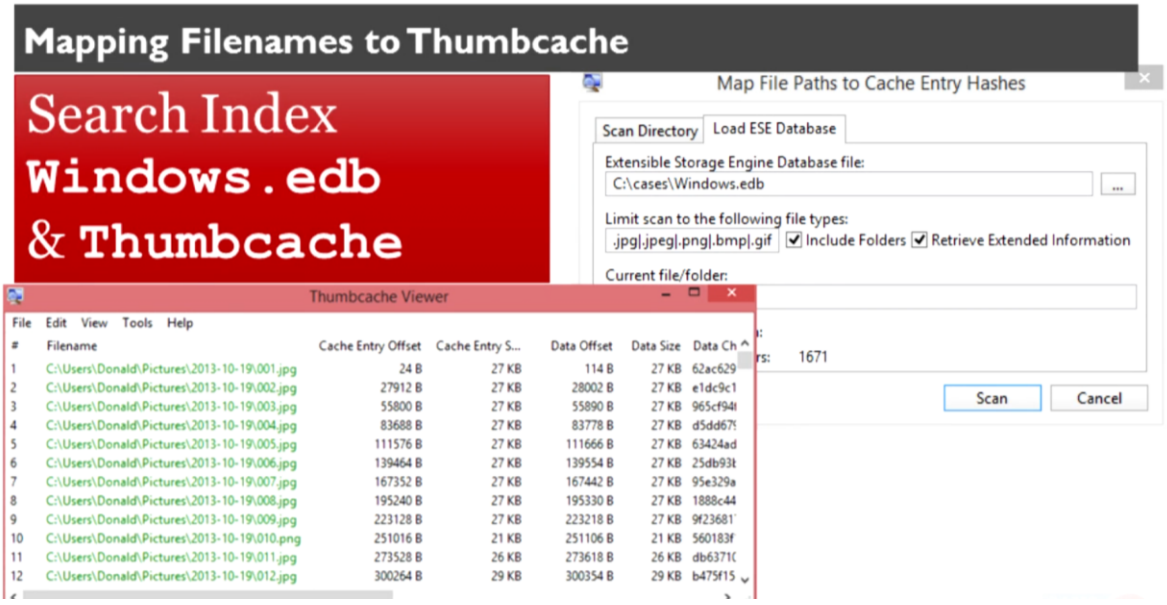
C:\Users\<username>\AppData\Local\Microsoft\Windows\Explorer\

Thumbcache_32.db

Thumbcache_96.db

Thumbcache_256.db

thumbcache_1024.db



It will try to get old name of the file using windows.db

Tools:

ThumbsDBViewer - https://thumbsviewer.github.io/

ThumbCacheViewer - https://thumbcacheviewer.github.io/

Recycle Bin:

The Recycle Bin is a familiar icon you'll find on your Windows desktop. It serves as a temporary storage area for files and folders that you've deleted from your computer.

When you delete something (whether intentionally or accidentally), it doesn't immediately vanish forever. Instead, it goes to the Recycle Bin. Think of it as a safety net – a second chance to recover files before they're permanently removed.

When you delete a file or folder, it's moved to the Recycle Bin. The file still occupies space on your hard drive, but it's no longer visible in its original location.

If you change your mind or realize you deleted something by mistake, you can open the Recycle Bin, find the item, and restore it. However, if you empty the Recycle Bin (either manually or automatically), the files are permanently deleted.

Path:

C:\$Recycle.bin – Vista\Win7\Win8\Win10

Deleted time and original filename contained in separate files for each deleted recovery file.

C:\Recycler – 2000\NT\XP\2003

Win7/8/10 $Recycle.Bin:

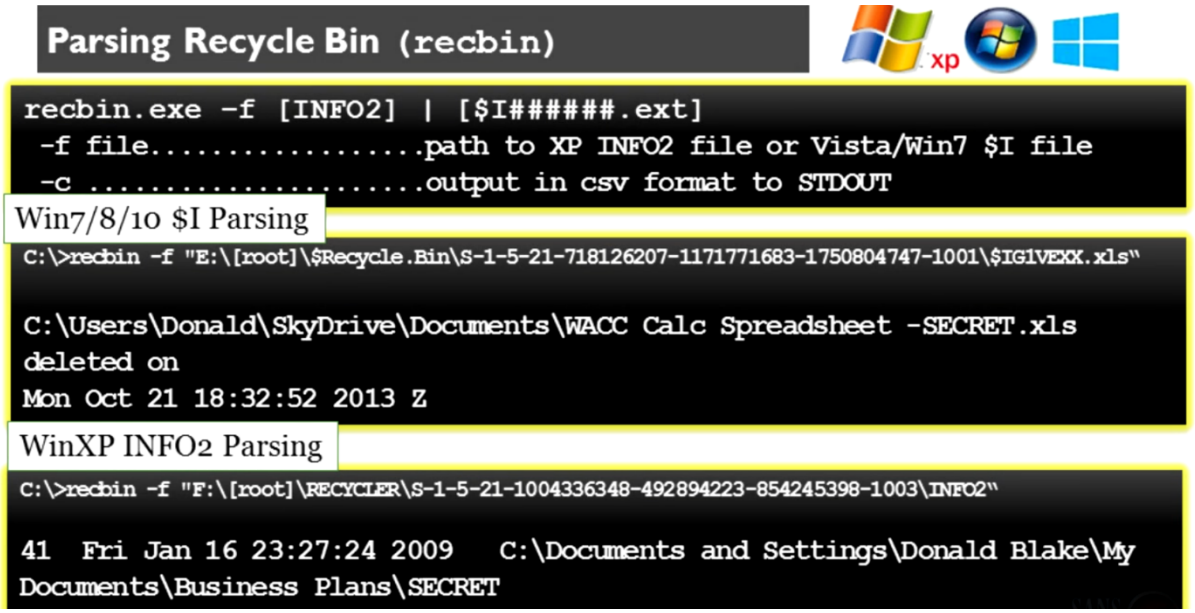
Under $recycle.bin and SID Files preceded by,

$I###### - original path and name, recycled date/time

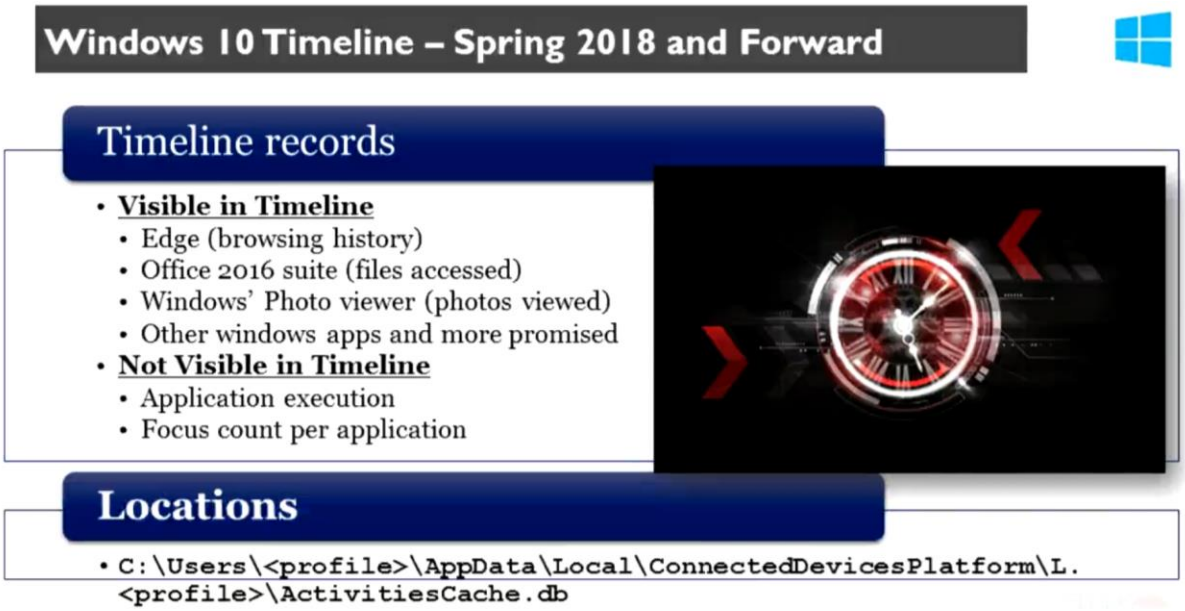
$R###### - contains recovery data.

Tools:

RBCMD: https://github.com/EricZimmerman/RBCmd



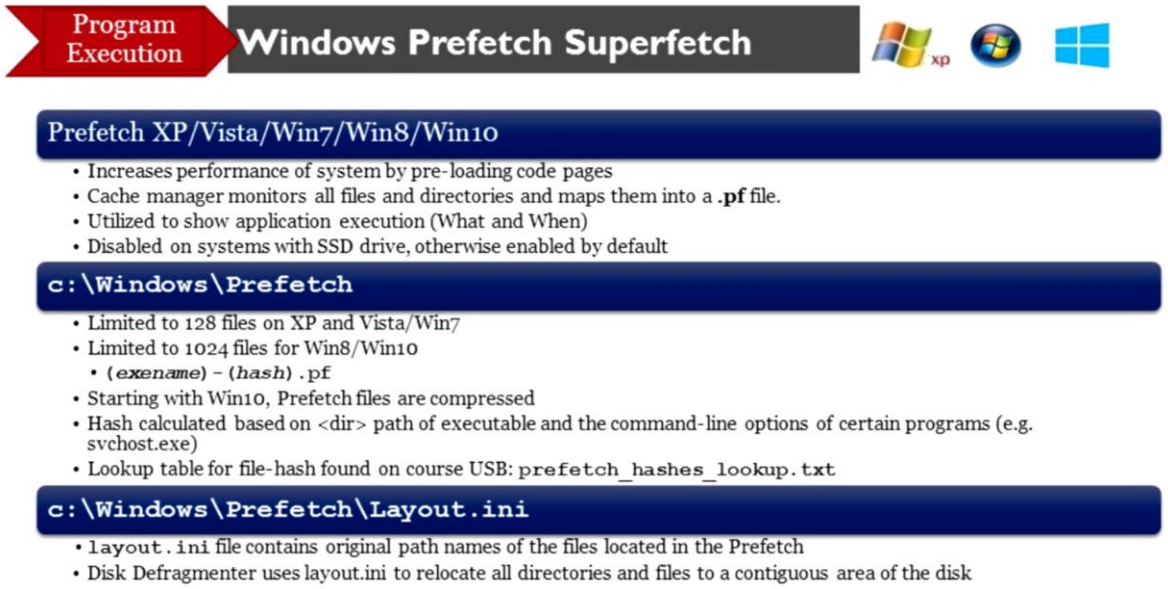
Windows10 timeline:



Tools:

WxTCmd.exe by Eric Zimmerman - https://github.com/EricZimmerman/WxTCmd

Windows Prefetch:



Maybe there will be 10 sec differences between actual run time and prefetch time.

Tools:

PECmd.exe by Eric Zimmerman - https://github.com/EricZimmerman/PECmd

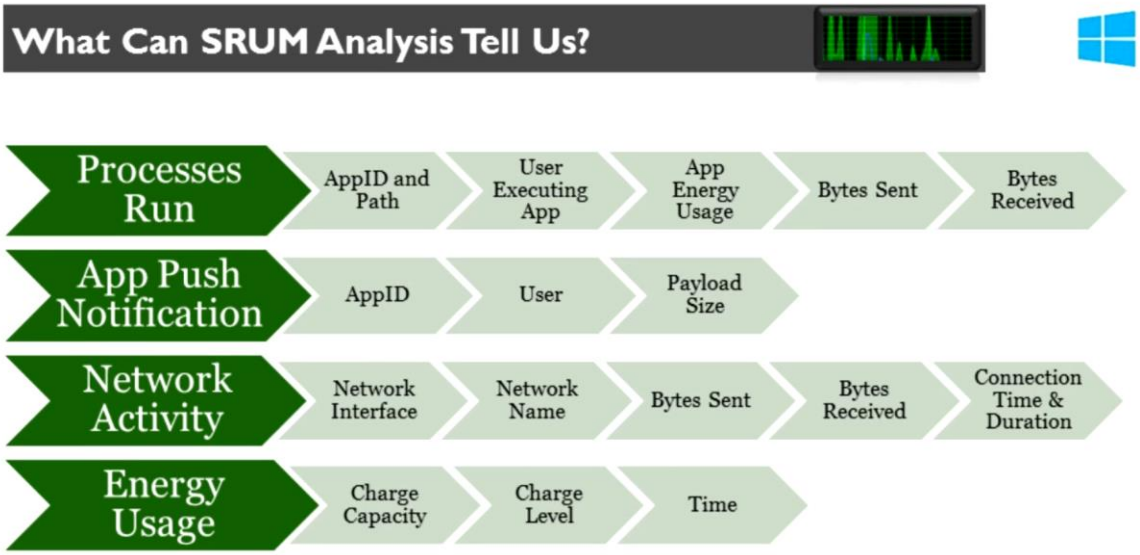
Pf.exe - https://www.nirsoft.net/utils/win_prefetch_view.html

SRUM:

System Resource Usage Monitor (SRUM) is a feature introduced in Windows 8 and later versions. It tracks resource usage by applications and services on a Windows system. SRUM collects data on resource utilization, such as CPU, memory, network, and disk usage. It helps administrators analyse system performance and resource consumption over time.

SRUM records usage data in a database called the SRU (System Resource Utilization) database. The database stores information about processes, network connections, and energy consumption.

It stores 30 to 60 days of historical system performance.



Path:

Registry - SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SRUM\Extensions\

{973F5D5C-1D90-4944-BE8E-24B94231A174}	Windows Network Data Usage Monitor
{97C2CE28-A37B-4920-B1E9-8B76CD341EC5}	Energy Estimation Provider (Windows 10)
{d10ca2fe-6fcf-4f6d-848e-b2e99266fa86}	WPN SRUM Provider
{d10ca2fe-6fcf-4f6d-848e-b2e99266fa89}	Application Resource Usage Provider
{DD6636C4-8929-4683-974E-22C046A43763}	Windows Connectivity Usage Monitor (Windows 8.1, Windows 10)
{fee4e14f-02a9-4550-b5ce-5fa2da202e37}	Energy Usage Provider

C:\Windows\System32\SRU\

Tools:

ESE Database View – https://www.nirsoft.net/utils/ese_database_view.html

Network Usage View - https://www.nirsoft.net/utils/network_usage_view.html

SRUM Dump - https://github.com/MarkBaggett/srum-dump

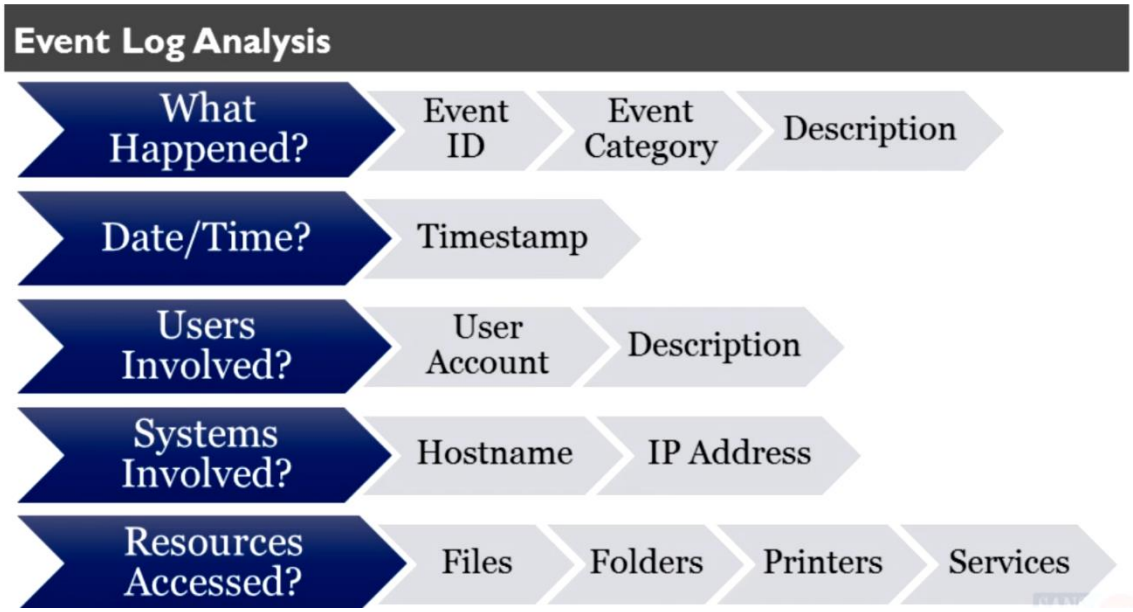
SRUMMonkey - https://github.com/devgc/SrumMonkey

9. Eventlogs:

An event log is a structured file that contains records of various events occurring on a computer system, application, or device. Think of it as a detailed journal that documents actions, errors, and other noteworthy occurrences.

Each entry in an event log typically includes a common set of fields:

- Timestamp: The date and time when the event occurred.
- Event ID: A unique identifier for the specific event type.
- Source: The application or component responsible for the event.
- Description: Details about what happened.
- User: The user account associated with the event (if applicable).



Types of Event Logs

Security	• Records access control and security settings information • Events based on audit and group policies • Example: Failed logon; folder access
System	• Contains events related to Windows services, system components, drivers, resources, etc. • Example: Service stopped; system rebooted
Application	• Software events unrelated to operating system • Example: SQL server fails to access a database
Custom	• Custom Application logs • Examples: Server logs including *Directory Service, DNS Server*, and *File Replication Service*

What Are We Likely to Find? Default Security Logging

	Workstation	Workstation Recommended	Server	Server Recommended
Account Logon		Success/Failure		Success/Failure
Account Mgmt	Success	Success/Failure	Success	Success/Failure
Directory Service				DC Only
Logon Events	Success	Success/Failure	Success	Success/Failure
Object Access				
Policy Change	Success	Success/Failure	Success	Success/Failure
Privilege Use				Success/Failure
Detailed Tracking		Success		Success
System Events	Success/Failure	Success/Failure	Success/Failure	Success/Failure

‡ Windows 7 and above include more granular options, some of which audit by default

Path:

NT\Win2000\XP\Server 2003:

- .evt file type
- %systemroot%\System32\config
- **Filenames:** SecEvent.evt, AppEvent.evt, SysEvent.evt

Vista\ Win7\8\2008\2012\win10\2016:

- .evt file type
- %systemroot%\System32\winevt\logs
- Remote log server
- **Filenames:** security.evtx, Application.evtx, System.evtx, etc.

Events and their IDs:

1. **Logon/ Logoff**

Tracking Account Usage (1)

Scenario

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

Relevant Event IDs

- 4624– Successful Logon
- 4625 – Failed Logon
- 4634 / 4647 – Successful Logoff
- 4672 – Account logon with superuser rights (Administrator)

Investigative Notes

- Event descriptions provide a granular view of logon information
- Windows does not reliably record logoffs (ID 4634) so also look for ID 4647 → user initiated logoff for interactive logons
- Logon events not recorded when backdoors, exploited services, or similar malicious means are used to access a system

Logon Type Codes

Logon Type Code	Explanation
2	Logon via console (that is, using the keyboard)
3	Network logon
4	Batch logon – often used by Scheduled Tasks
5	Windows Service logon
7	Credentials used to lock or unlock screen
8	Network logon sending credentials in cleartext
9	Different credentials used than logged on user – runas command
10	Remote interactive logon (Remote Desktop Protocol)
11	Cached credentials used to logon – system likely offline from DC
12	Cached Remote Interactive (similar to Type 10)
13	Cached unlock (similar to Type 7)

2. RDP:

Tracking Account Usage Remote Desktop Protocol (1)

Scenario

- Track Remote Desktop Protocol logons to target machines

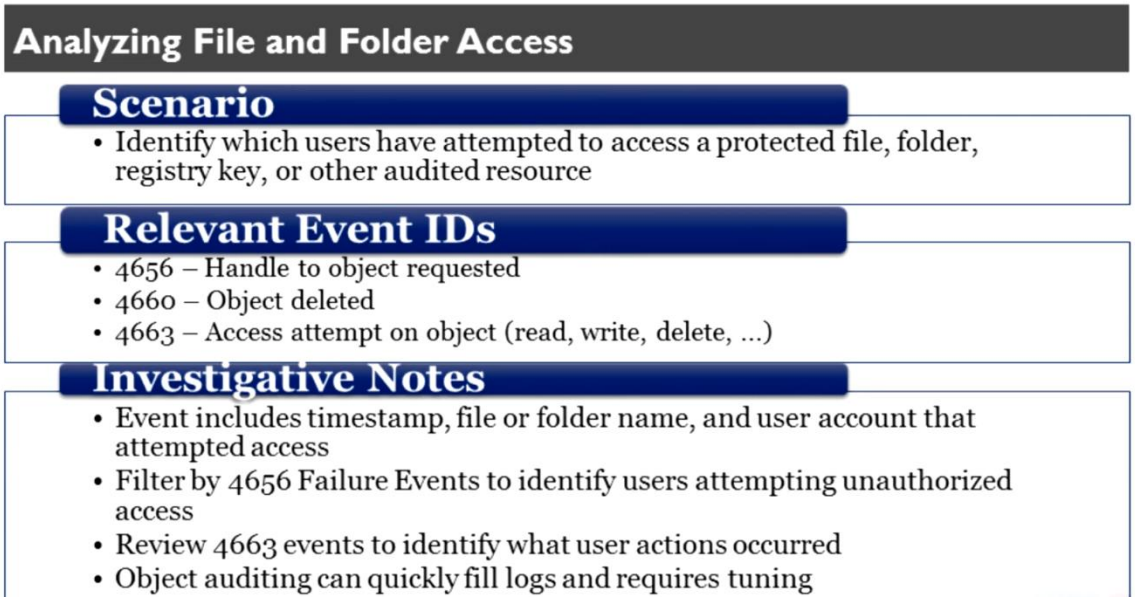
Relevant Event IDs

- 4778 – Session Connected/Reconnected
- 4779 – Session Disconnected

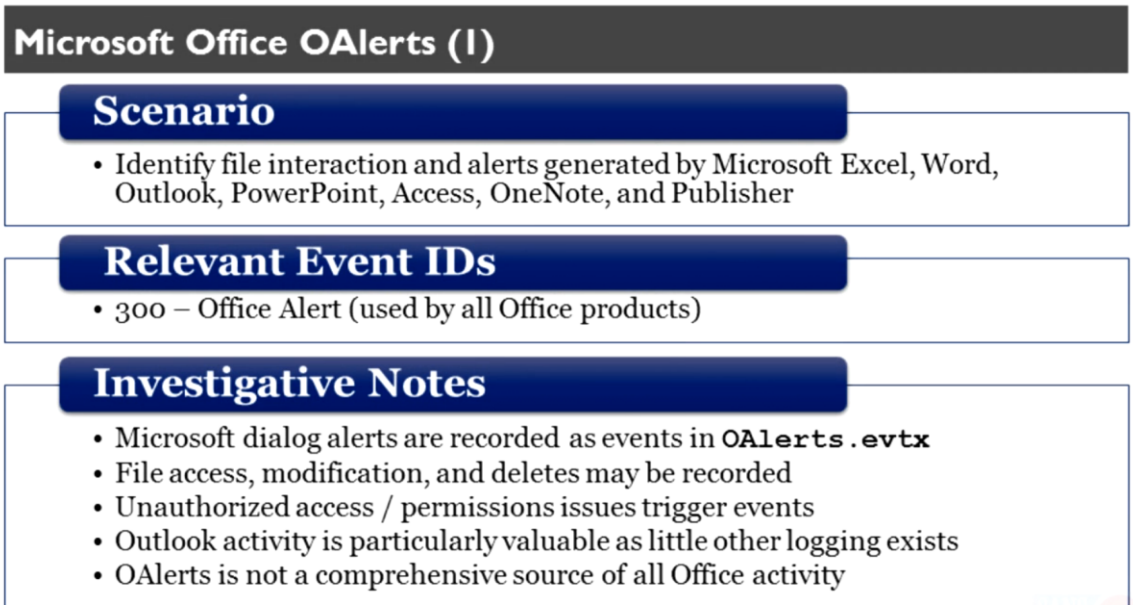
Investigative Notes

- Event log provides hostname and IP address of remote machine making the connection
- On workstations, you will often see current session disconnected (4779) followed by RDP connection (4778)
- These events are also used to track "Fast User Switching" sessions
- The auxiliary logs **`Remote Desktop Services - RDPCoreTS`** and **`TerminalServices-RemoteConnectionManager`** record similar info

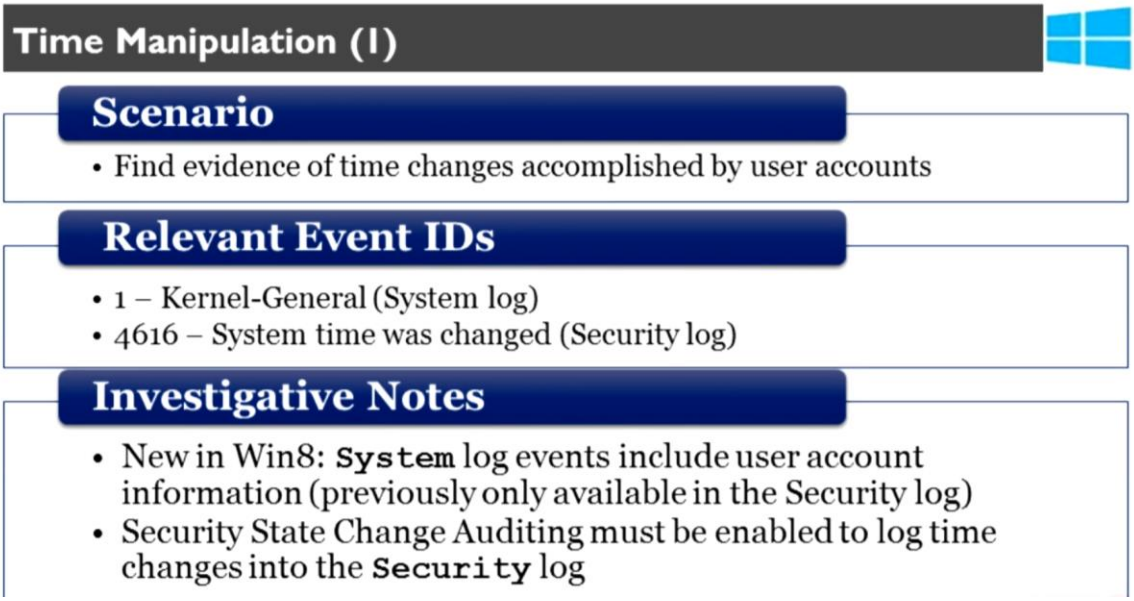
3. **File and Folder Access:**



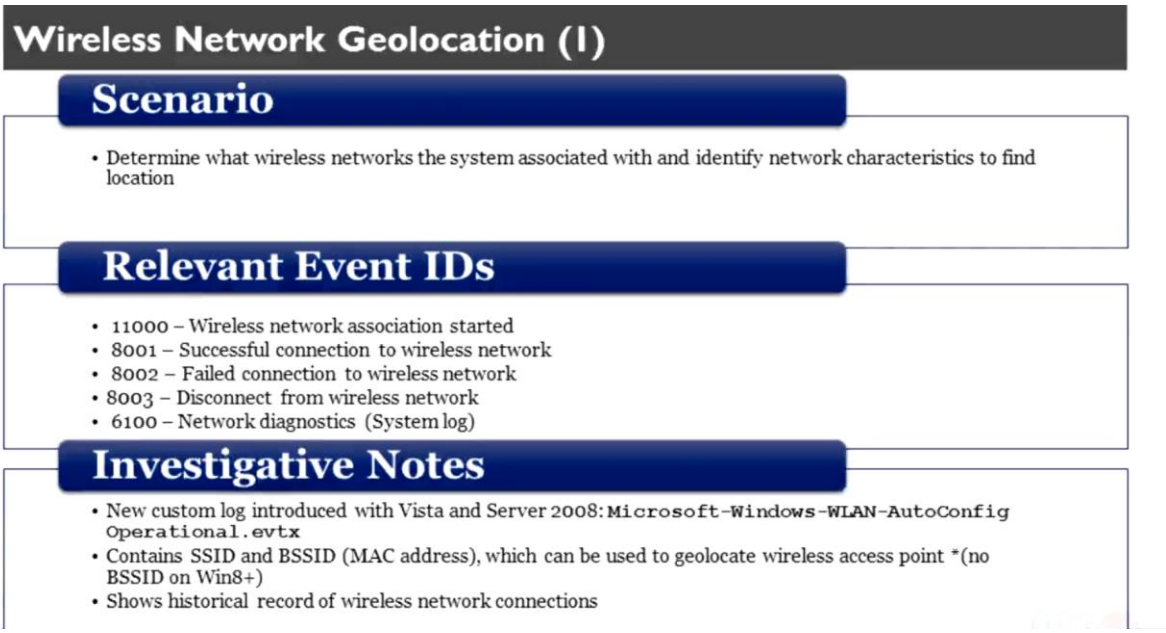
4. **Microsoft office OAlerts:**



5. **Time Manipulation:**



6. **Wireless Network Geolocation:**



Tools:

EventLogExplorer - https://www.eventlogxp.com/

EventLogView - https://www.nirsoft.net/utils/full_event_log_view.html

EvtxECmd - https://www.sans.org/tools/evtxecmd/

10. Internet Browsers

Web browsers are used across various devices (mobile, tablets, desktops) and serve not only for web surfing but also for navigating through the device's file system.

Key artifacts include:

Browsing History: Reveals the user's navigation history.

Cached Files: These can include downloaded images, videos, documents, executables, and scripts.

Cookies: Contain information about user sessions and preferences.

Form Data: Includes search queries, logins, passwords, and other input data.

Bookmarks: Provide insights into the user's interests.

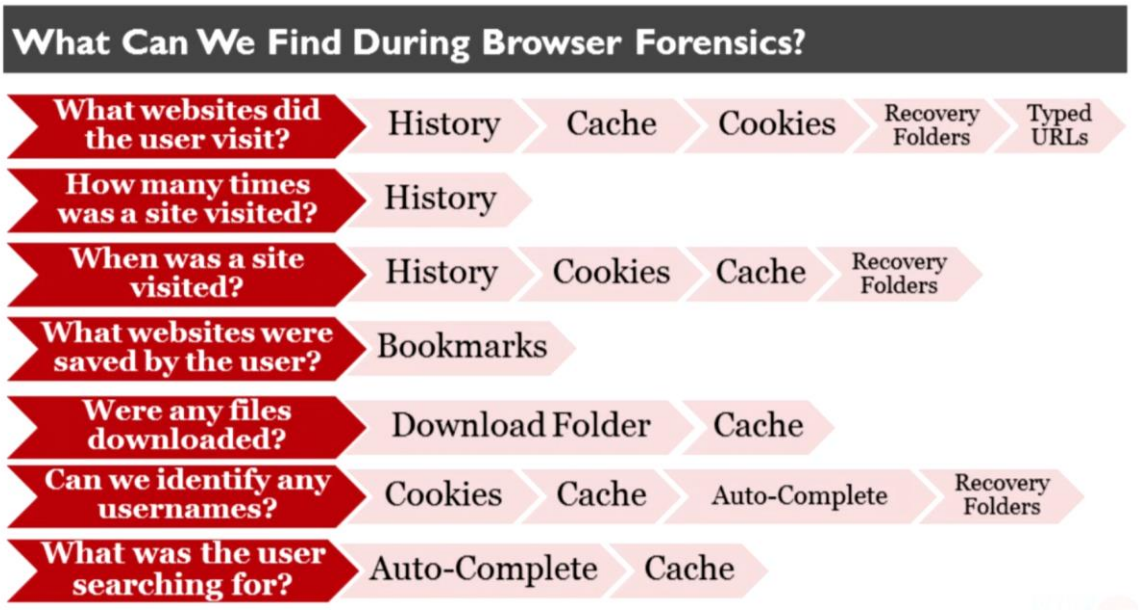
Browser forensics plays a crucial role in incident response, helping investigators understand how attacks on computers or networks originated and identifying the source of compromise.

Popular Web Browsers:

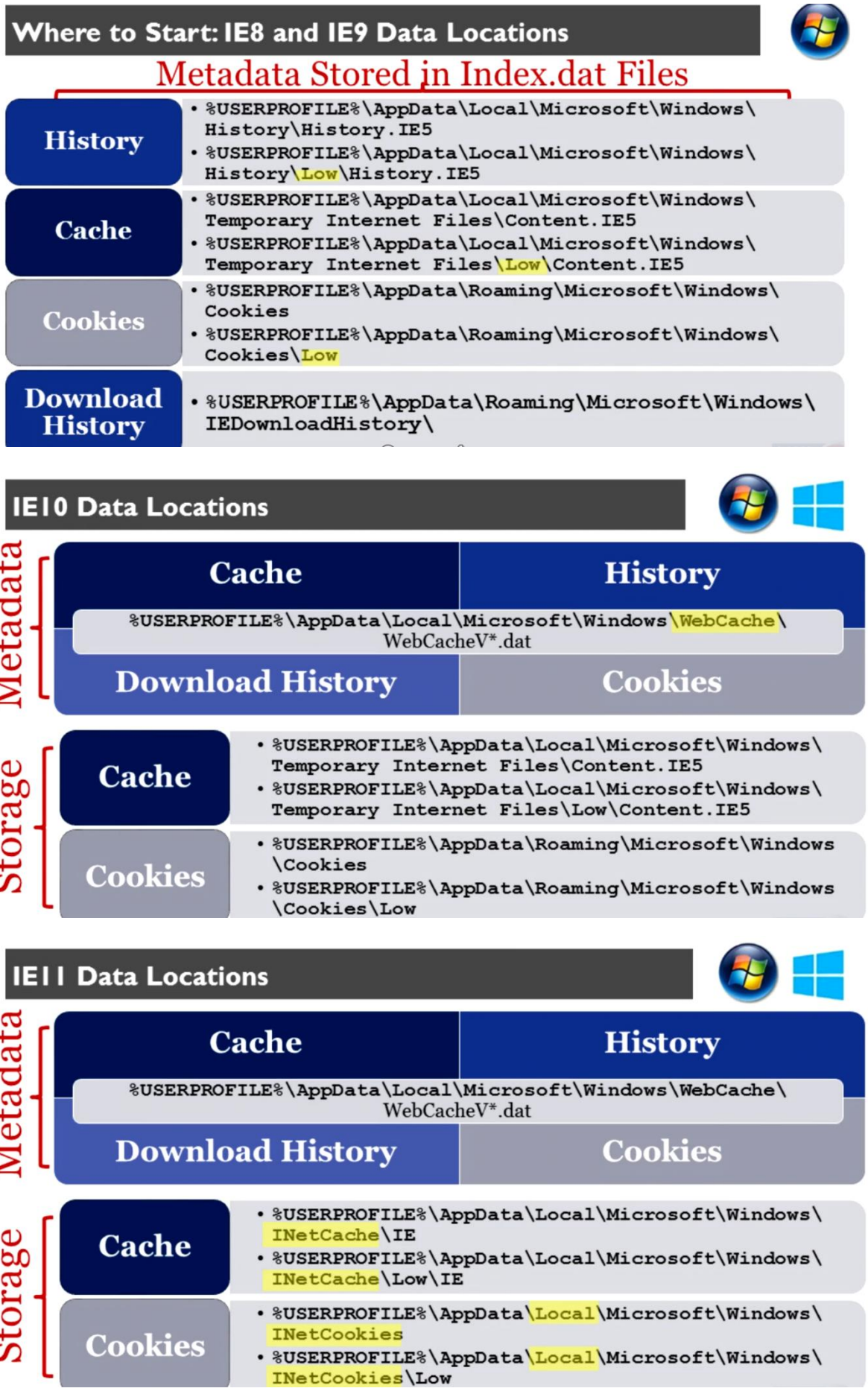
Internet Explorer: A default browser in Windows, now replaced by Microsoft EDGE in Windows 10. EDGE can work in InPrivate mode, preserving user privacy.

Google Chrome: Known for its speed, extensions, and memory consumption. It also offers Incognito mode to prevent permanent storage of history, cookies, and form data.

Mozilla Firefox: commonly known as Firefox, is a free and open-source web browser developed by the Mozilla Foundation and its subsidiary, the Mozilla Corporation.



Internet Explorer



IE10+ Cache Metadata: WebCacheV*.dat

Filename/FileSize	Name and size (in bytes) of cached file on disk
SecureDirectory	Location of file within cache subdirectories
AccessCount	Number of uses of cached content
URL	Origin of cached content

IE Cache Timestamps

Each entry records several timestamps in cache metadata:

- Filesystem timestamps are also available for cached files

Creation Time	• The first time the content was viewed • Creation time of cached file (UTC)
Accessed Time	• The last time the local content was viewed by the user • Stored in UTC time
Modified Time	• The last time content was changed on the web server • Set by the website and stored in UTC time
Expiry Time	• Used by the cache to age out old versions of pages • Set by the website and stored in UTC time

Cookie Metadata:

Metadata remains constant but location changes:

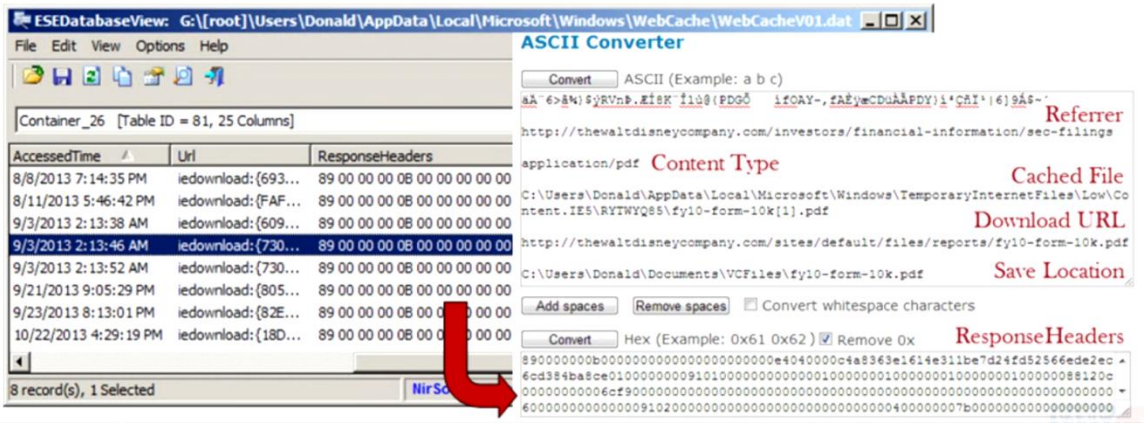
Index.dat (IE4-IE9)

WebCacheV*.dat “Cookies” tables (IE10+)

Filename	Cookie filename on disk
URL	Issuing domain of cookie
AccessCount	How many times cookie has been passed to site
CreationTime	First time cookie saved to system (UTC)
ModifiedTime	Last time website modified cookie (UTC)
AccessedTime	Last time cookie was passed to website (UTC)
ExpiryTime	When cookie will no longer be accepted (UTC)

IE Download History

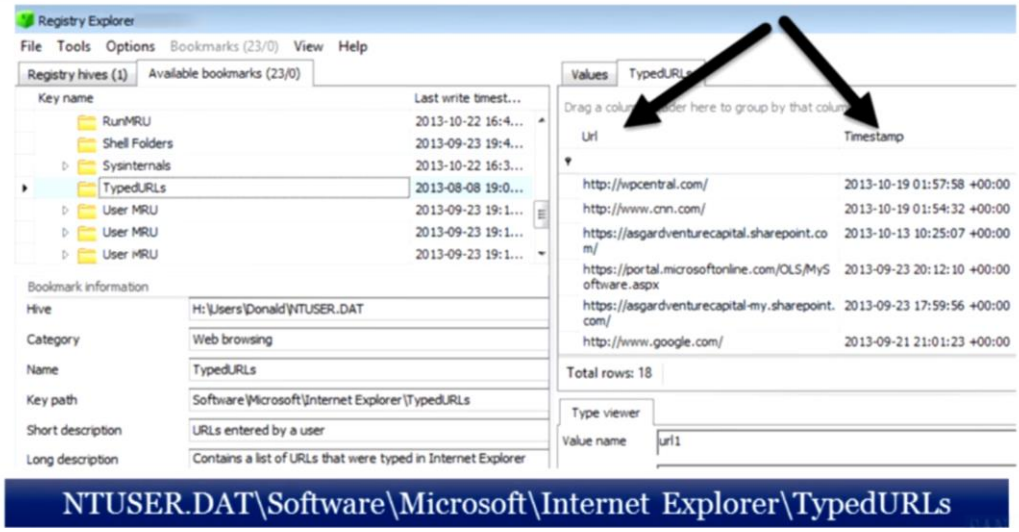
- Download data stored in WebCacheV*.dat in IE10+
  - ResponseHeaders field must be parsed



Hands on Keyboard: IE Auto-Complete

- Address bar history: Typed URLs registry key:
  `NTUSER\Software\Microsoft\InternetExplorer\TypedURLs`
  - Records the last 25 web addresses typed by user (IE9)
  - Increased to the last 50 addresses in IE10+
- IE10+ records last used time of each typed URL:
  `NTUSER\Software\Microsoft\InternetExplorer\TypedURLsTime`
- Also part of Auto-Complete:
  - Browsing history
  - Favorites
  - Form data

TypedURLs

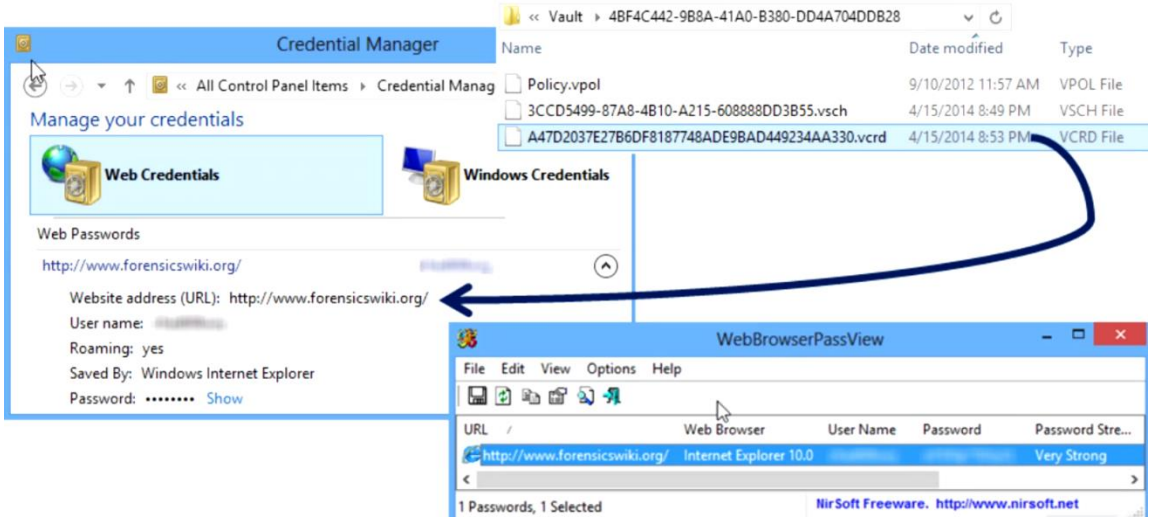


NTUSER.DAT\Software\Microsoft\Internet Explorer\TypedURLs

Auto-Complete Data: Protected Storage/Windows Vault

- Internet Explorer Credential Manager:
  - Auto-complete form data
  - Website usernames and passwords
  - Network, Exchange server, and FTP passwords
  - If it isn't acquired live, requires cracking:
    - NirSoft WebBrowserPassView is a free tool for live acquisitions
    - Commercial tools such as Passcape can crack offline
- IE10 introduced the Windows Vault to store creds:
  - %USERPROFILE%\AppData\Local\Microsoft\Vault\{GUID}
  - Each entry is stored as a single .vcrd file
  - Prior to IE10, "Protected Storage" saved data in the registry

Decrypting .vcrd Files



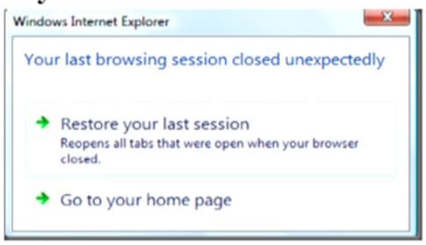
Web Browser Bookmarks: Looking at Saved Locations

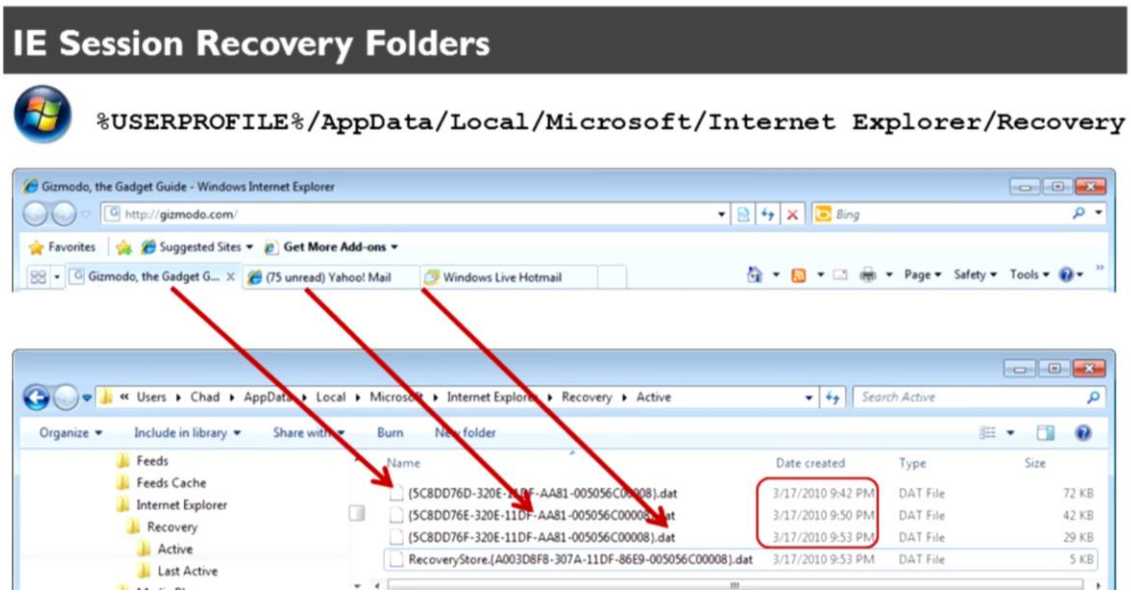
- Bookmarks are not always parsed by forensic tools
  - Provide intent and insight into interests and activities
  - Can determine user account, URL, URL parameters, page title, creation date, and last used date
  - Be careful: Not every bookmark is user-generated
  - A bookmark does not prove the site was visited
- NirSoft **`FavoritesView`** parses IE and Firefox

Browser	Bookmark Location(s)
Internet Explorer	`%USERPROFILE%\Favorites\*.url`
Edge	`Spartan.edb`
Firefox	`places.sqlite, bookmarks-<date>.json (backup)`
Chrome	`Bookmarks, Bookmarks.bak`

IE Session Recovery

- IE8+ saves the current and last browser session:
  - Provides automatic crash recovery and "rollback" feature
  - Enabled by default and deleted when History is cleared*
- Allows us to identify:
  - Tabs open in last session
  - Historical websites viewed in *each* tab
  - Referring websites
  - Time session started/ended:
    - Creation time of .dat files in Active folder = session start
    - Creation time of .dat files in LastActive folder = session end
  - HTML, JavaScript, and XML from the page
  - Other artifacts such as form data



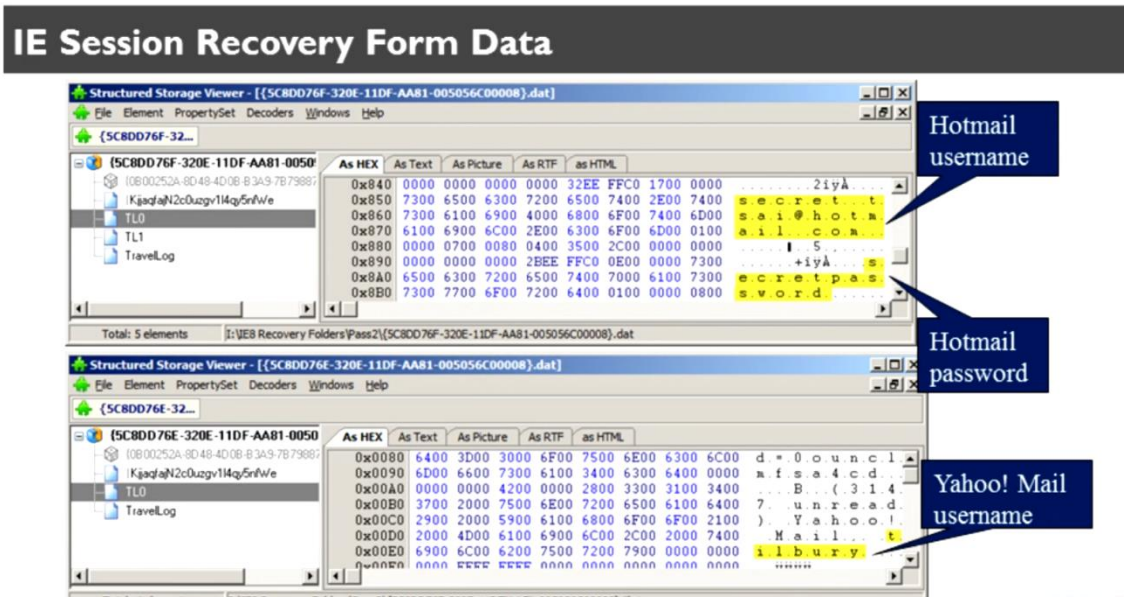


There will be two directories Active & last active.

Tools:

Structured storage viewer - https://www.mitec.cz/ssv.html

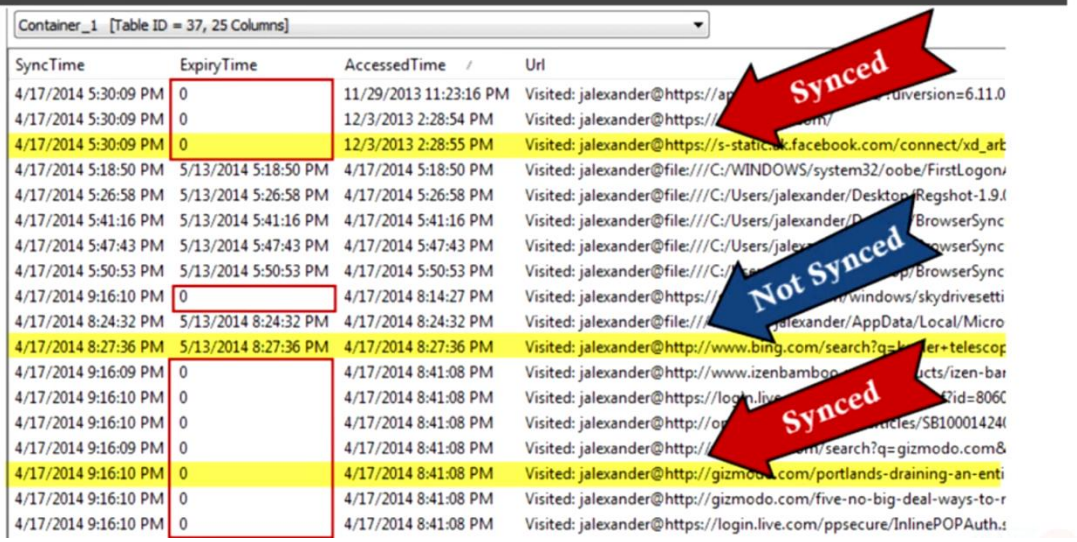
ParseRS - https://github.com/jtmoran/parseRS/tree/master



Can We Differentiate Synced Data?

Artifact	Can we tell if it originated via a sync?
TypedURLs	**Unlikely:** Possibly via TypedURLsTime key
Favorites	**Unlikely:** Possibly via timestamp analysis
Tabs	**Yes:** Parse MachineInfo.dat and Tab .dat files
History	**Yes:** Compare SyncTime and AccessedTime for entry in WebCacheV*.dat. If times differ by more than ± 5 seconds, it likely originated from a different system *
	Alternatively, if ExpiryTime = 0, a history entry was recorded in WebCacheV*.dat due to a sync operation *

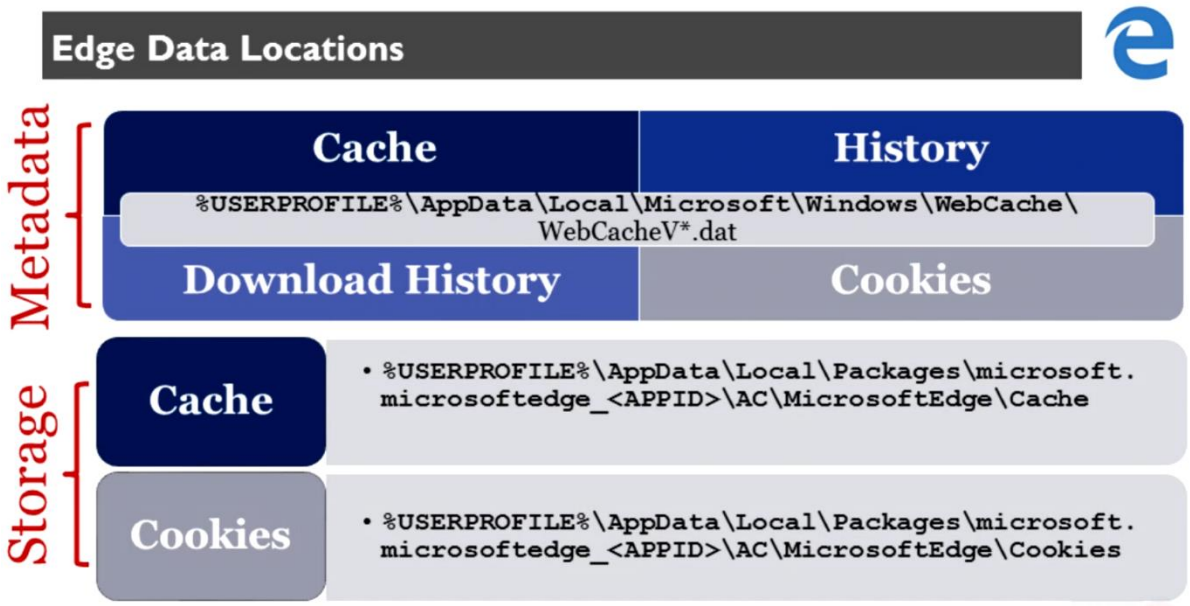
Identifying Synchronized IE History



ExpiryTime = 0 data is synced

ExpiryTime = date data in not synced.

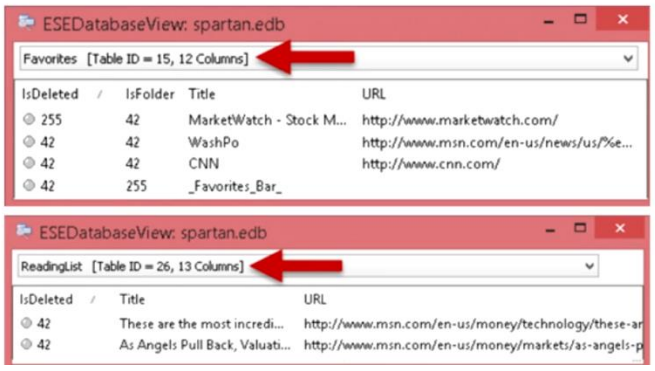
EDGE



Spartan.edb

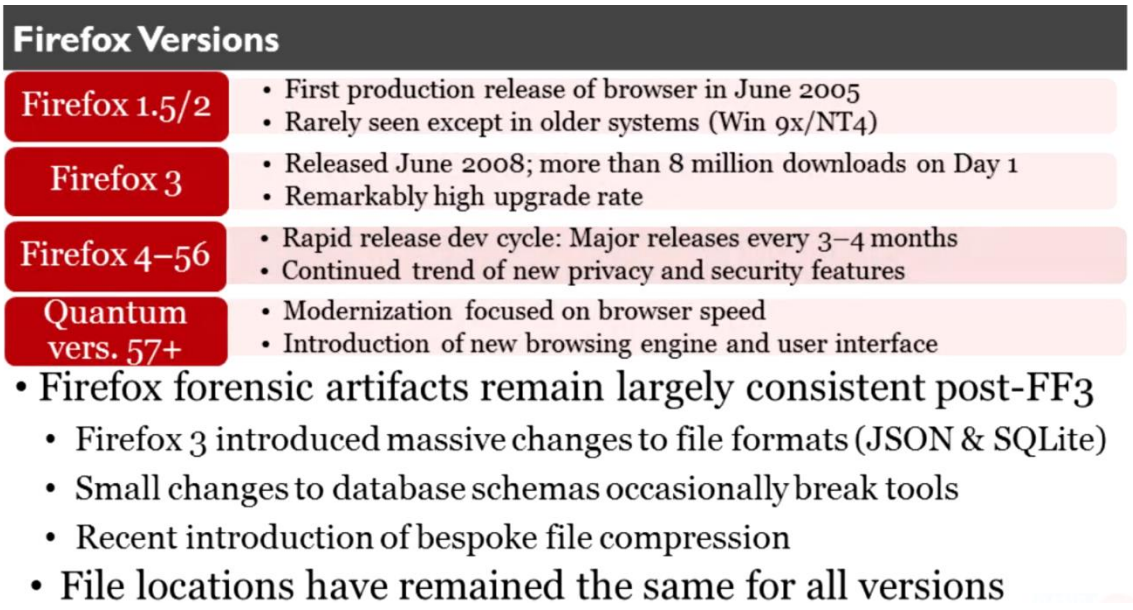
Bookmarks • Reading List • WebNotes • Top Sites • SweptTabs

%LOCALAPPDATA%\Packages\Microsoft.MicrosoftEdge_<APPID>\AC\MicrosoftEdge\User\Default\DataStore\Data\nouser1\120712-0049\DBStore\Spartan.edb



Browser Artifacts	Where to Find Them
Internet History	WebCacheV*.dat Session Recovery {GUID}.dat
Cache Files	WebCacheV*.dat
Cookies/Web Storage	WebCacheV*.dat / DOMStore
Bookmarks	Spartan.edb
Download History	WebCacheV*.dat
TypedURLs	Edge TypedURLS (registry)
Web Passwords	.vcrd files
Web Notes	WebNotes folder / Spartan.edb
Reading List	Spartan.edb

Firefox



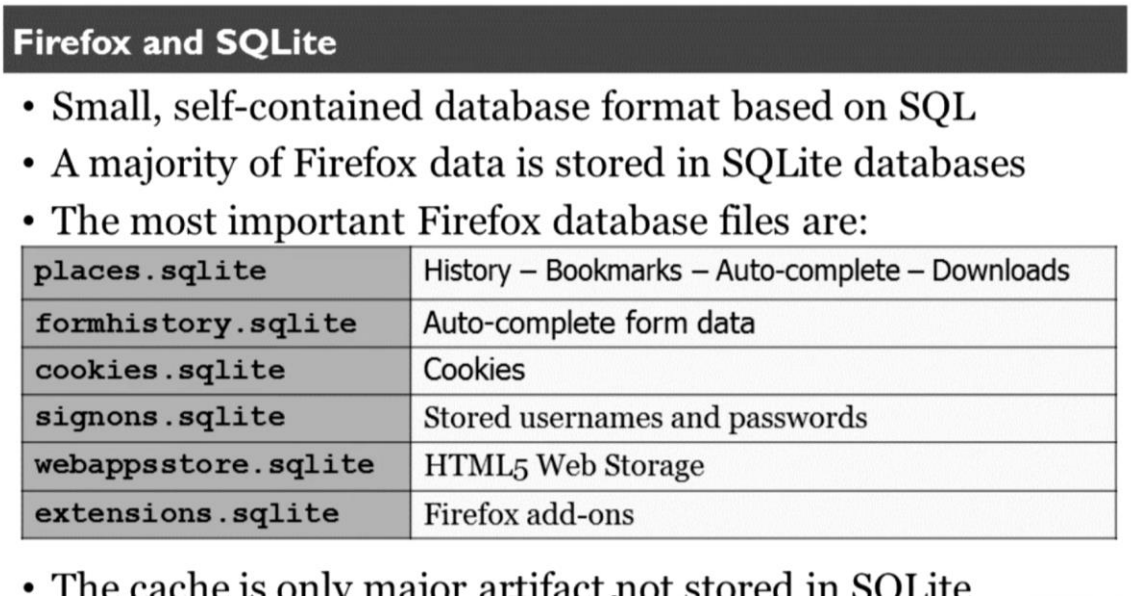
Path:

History-Cookies-Bookmarks-Auto-Complete

%USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profile\<Rnadom text>.default.

Cache:

%USERPROFILE%\AppData\Local\Mozilla\Firefox\Profiles\<random text>.default\Cache



History Artifacts in Firefox: Investigating Sites Visited

Firefox maintains more history info than IE!

Investigative Questions	places.sqlite
What was the complete URL that was visited?	`url`
What was the title of the page visited?	`title`
When was the site first visited?	`visit_date*`
When was the site last visited?	`visit_date*`
How many visits were made to the site?	`visit_count`
Was the URL typed by the user?	`typed`
Was the page retrieved without any user actions?	`hidden`
What page led the user to this one?	`from_visit`
How did the user request the page?	`visit_type`

How Was the Web Page Requested? Visit Types in Firefox

The `visit_type` field gives us specific information about how the entry in `places.sqlite` was requested

Type	Description
1	User followed a link and the page was loaded
2	User typed the URL to get to the page (with or without auto-complete)
3	User followed a bookmark to get to the page
4	Indicates some inner content was loaded such as images and iframes
5	Paged accessed due to a permanent redirect (HTTP 301 status code)
6	Paged accessed due to a temporary redirect (HTTP 302 status code)
7	File indicated by history was downloaded (non-HTML content)
8	User followed a link that loaded a page in a frame

Tool:

NirSoft: MZHistory View - https://www.nirsoft.net/utils/mozilla_history_view.html

NirSoft: MZCache View - https://www.nirsoft.net/utils/mozilla_cache_viewer.html

NirSoft: Mozila Cookies View - https://www.nirsoft.net/utils/mzcv.html

GA Cookie Cruncher – Mari DeGrazia - https://github.com/mdegrazia/Google-Analytic-Cookie-Cruncher

Firefox Cookies: Going Deep into Website Activity

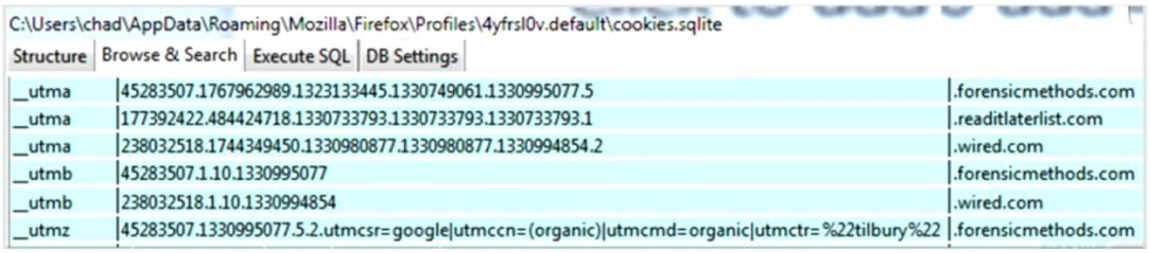
- Provide an additional means to profile Internet activity
- Firefox stores all of a user's cookies in **`cookies.sqlite`**
  - Stored in the profile folder, linking them to a user account

Investigative Questions	cookies.sqlite
What website domain issued the cookie?	`host`
What is the cookie name?	`name`
Was the cookie issued in a secure connection?	`isSecure`
What values/preferences were stored?	`value`
When was the cookie created?	`creationTime`
When was the cookie/site last accessed?	`lastAccessed`

Google Analytics Cookies

Google uses several different cookies to track user activity on participating sites (>50% of all sites on Internet)

__utma	Unique visitors	**__utmv**	Custom values
__utmb	Session tracking	**__utmx**	Website optimization
__utmc	Session status (deprecated)	**__utmz**	Traffic sources



Firefox Download History: Examining What Was Downloaded

Investigative Questions	places.sqlite Table: moz_annos
What was the filename?	`place_id (ref. moz_places)`
Where was the file downloaded from?	`place_id (ref. moz_places)`
Where was the file saved?	`anno_attribute_id 4`
When did the download end?	`anno_attribute_id 5 (endTime)`
How large was the download?	`anno_attribute_id 5 (fileSize)`
Was the download successful?	`anno_attribute_id 5 (state)`

Firefox 26+: places.sqlite Firefox 3–25: downloads.sqlite

- The default download directory is the user's Downloads folder
  - Changes to the default are recorded in the **`prefs.js`** file

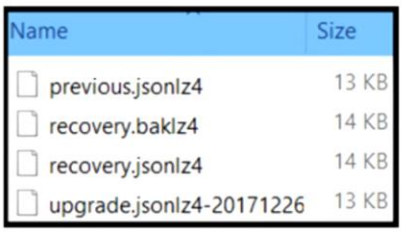
Firefox Auto-Complete: What Was the User Typing?

- Firefox maintains a vast amount of data that a user has typed into web forms:
  - Helps users fill in common web forms without retyping the data
  - Perfect for usage profiling: Providing items and people being searched for, usernames and aliases, email addresses, and so on
  - Form data is not tied to a specific website (only a form name)

Investigative Questions	formhistory.sqlite
What type of form was the data entered into?	`fieldname`
What was the data typed by the user?	`value`
How many times has value been used?	`timesUsed`
When was the data first typed in?	`firstUsed`
When is the last time the data was used?	`lastUsed`

Firefox Session Restore

- Records the following information for open windows/tabs:
  - Tab history
  - Cookies
  - Typed form data
  - Session start, tab last access and close times
- Saved in **`sessionstore.jsonlz4`**
  - JavaScript format (compressed)
  - File deleted when browser is closed
    - Unless user opts to "Show windows and tabs from last time"
    - Possible to find multiple deleted **`sessionstore`** files
- **`sessionstore-backups`** folder contains older sessions



jsonlz4 Compression

- Firefox has recently introduced compressed files
  - Customized version of LZ4 "fast compression"
  - Look for "lz4" tags: `json.lz4` • `json.mozlz4` • `baklz4`
- Used for other files, including bookmark backups
- **`dejsonlz4`** is a free tool to decompress files

```
Select Command Prompt
dejsonlz4.exe -h
Usage: dejsonlz4 [-h] IN_FILE [OUT_FILE]
   -h  Display this help and exit.
Decompress Mozilla bookmarks backup file IN_FILE to OUT_FILE.
If OUT_FILE is '-' or missing, decompress to standard output.
```

Firefox Extensions (2)

- Extensions are applications that can be downloaded by a user to extend the functionality of Firefox:
  - Can give information about how browser was used or where to look for additional browser artifacts

Investigative Questions	extensions.json
What extensions were installed?	`name`
What version of extension?	`version`
Extension information page?	`sourceURI`
When was the extension installed?	`installDate`
When was the extension last updated?	`updateDate`
Was the extension enabled?	`active`

Google Chrome

Win7+: `%USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default`

- Artifacts stored in the following formats:
  - SQLite (a majority of artifacts)
  - JSON
  - SNSS (session restore files)

Investigating Sites Visited: Chrome History Database (2)

Chrome keeps prolific history metadata

Investigative Questions	History (urls/visits)
What was the complete URL that was visited?	`url`
What was the title of the page visited?	`title`
What times was the site visited (historical)?	`visit_time`
When was the site last visited?	`last_visit_time`
How many visits were made to the site?	`visit_count`
Was the URL typed by the user?	`typed_count`
What page led the user to this one?	`from_visit`
How long was the page viewed?	`visit_duration`
How did the user request the page?	`transition`

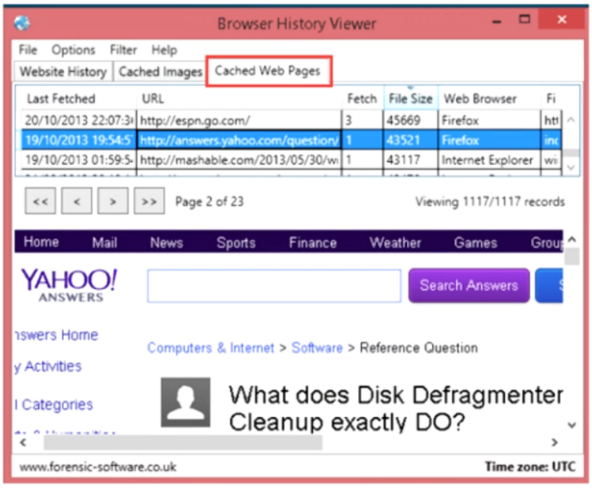
Chrome History Page Transition Types

Page Transition tells us why a URL was visited

	Type	Description
0	Link	User clicked a link
1	Typed	URL typed in address bar (same as IE Typed URLs)
2	Auto_Bookmark	Via a suggestion in the Chrome UI (NOT a user favorite)
3	Auto_Subframe	Content loaded in a non-top level frame (Advertisement)
4	Manual_Subframe	User request to load content in nontop level frame
5	Omnibox Generated	Suggested based on user typing but user did NOT see URL
6	Start_Page	Home page of a tab
7	Form_Submit	User-filled out information in a form and submitted
8	Reload	Page refreshed
9	Keyword	Keyword typed to identify site (that is, "Wired" <TAB>)
10	Keyword Generated	The actual URL generated (and visited) as a result of keyword

Rebuilding Cached Web Pages

- Renders HTML pages and intercepts image requests:
  - If image exists in cache, it is included
  - Available for Chrome, IE10+, and Firefox
- Uses only data available in cache:
  - Does **not** access Internet
- NetAnalysis and IEF can also rebuild pages



http://www.forensic-software.co.uk/FreeTools.aspx

Chrome Cookies

- Located in Cookies database (SQLite format)
- Starting with v33, most cookie values are encrypted
  - Windows DPAPI crypto API used
  - Decryption possible on live system with user logged in

Investigative Questions	Cookies
What website domain issued the cookie?	`host_key`
What is the cookie name?	`name`
What values/preferences were stored?	`value / encrypted_value`
When was the cookie created?	`creation_utc`
When was the cookie/site last accessed?	`last_access_utc`

Chrome Session Recovery – Strings

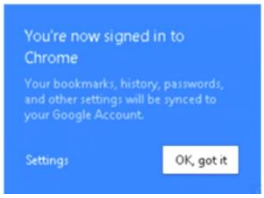
Chrome Synchronization (2)

What Is Synced?

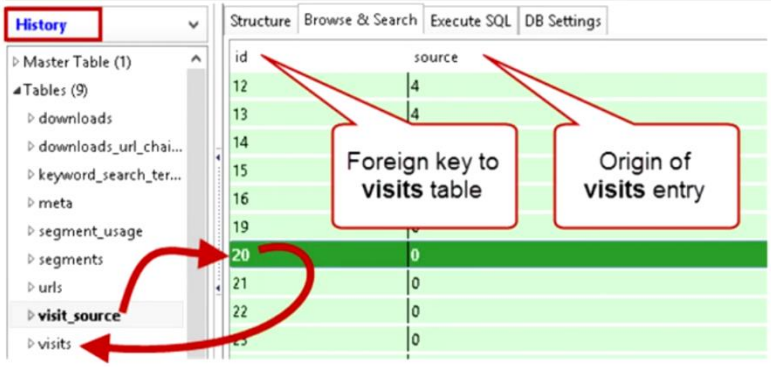
- History
  - `visit_count, typed_count, last_visit_time`
- Bookmarks
- Preferences
- Extensions
- Passwords (encrypted)
- Web Data (auto-complete)
- Top Sites (+thumbnails)
- Tabs

What Is Not Synced?

- Download History
- Cookies
- **`keyword_search_terms`**
- Shortcuts (Omnibox typed)
- Network Action Predictor



Identifying Synced Chrome History



Source	Origin
0	**Synced**
1	User Browsed
2	Extension
3	Firefox Import
4	IE Import
5	Safari Import

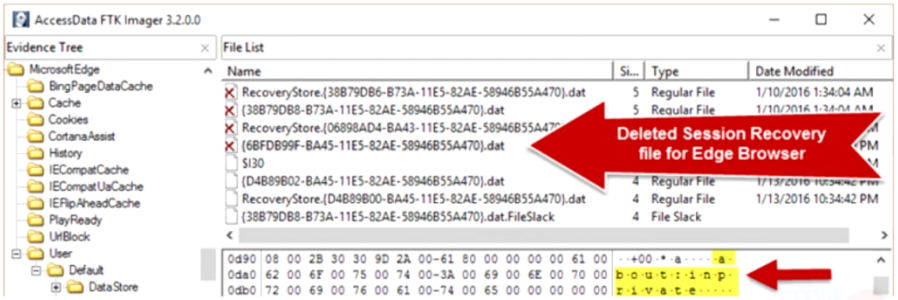
- The **`visit_source`** table identifies synced history entries via the **`source`** field (0 = synced to local)
- Other synced artifacts are more difficult to discern

Tools:

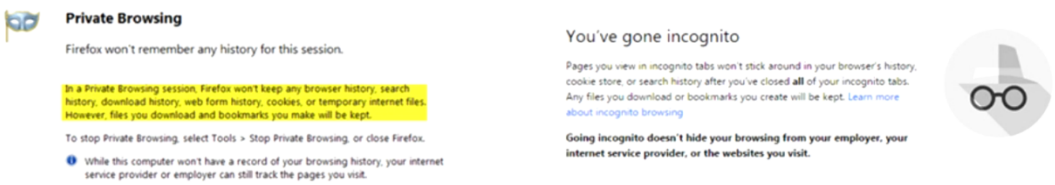
Hindsight Chrome Forensics: https://github.com/obsidianforensics/hindsight

Recovering InPrivate Artifacts

- Some artifacts can be recovered via file undeletion:
  - Cache files
  - Automatic Crash (Session) Recovery files
- Residue from all other artifacts can still be found:
  - Unallocated space/Pagefile.sys
  - Memory



Chrome and Firefox Private Browsing



- Chrome and Firefox have moved private browsing artifacts to memory:
  - SQLite database updates are done only in memory
  - Limited disk-based remnants
- There are still some leaks:
  - If outside viewers are used, IE records local file access!
  - Downloaded files persist in the filesystem (no metadata is kept)
  - Bookmarks are maintained (and identified as added in private mode)

Tor Private Browsing

- The Tor Browser is a modified version of Firefox
  - All browsing activity is via "Private Browsing"
  - Very limited disk-based remnants
- Application execution artifacts can identify usage
  - Prefetch – `TOR.EXE, START TOR BROWSER.EXE`
  - UserAssist – `Start Tor Browser.exe`
- Browser artifacts stored under install folder
  - \Data\Browser folder contains Firefox databases
  - \Data\Tor folder contains preferences and status files
    - "State" text file can show TOR version and last execution time

Identifying Selective Deletes

- New browser privacy options facilitate selective deletions
- Look for gaps in database record identifiers or significant time gaps (such as an entire day missing)
- Deleted data can often be recovered by carving the unallocated space within the database

Tools:

SQLite Deleted Data

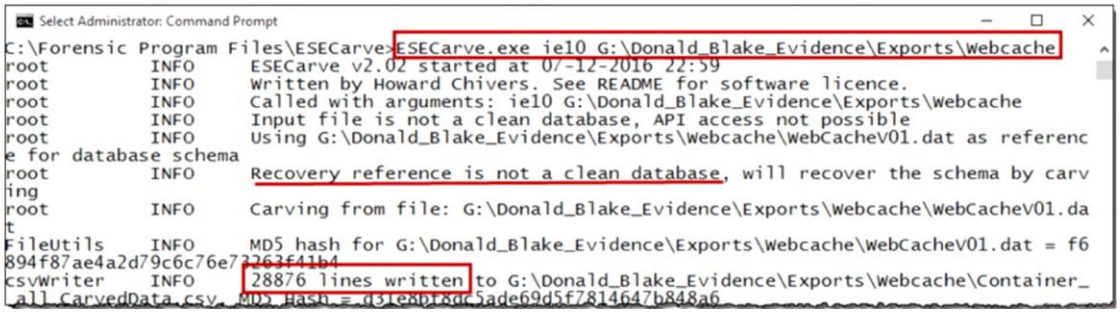
SQLite databases can contain deleted entries and several tools can recover them:

- CCL Group Epilog (commercial)
- Sanderson SQLite Recovery (commercial)
- sqlparse.py by Mari DeGrazia (free)


```
C:\Forensic Program Files\SQLite Parser>sqlparse.py
Usage: Parse deleted records from an SQLite file into a TSV File or text file
Options:
  -h, --help            show this help message and exit
  -f smsmms.db, --file=smsmms.db
                        sqlite database file
  -o output.tsv, --output=output.tsv
                        Uutput to a tsv file. Strips white space, tabs and
                        non-printable characters from data field
  -r, --raw             Optional. Will out put data field in a raw format and
                        text file.
```

Carving ESE Databases

- ESECarve by Howard Chivers:
  - Recovers resident and deleted entries from ESE
  - Can carve from clean (using API) or dirty databases
  - Output in .csv format (-y performs deduplication)



InPrivate Session Recovery

```
C:\Forensic Program Files\parseRS>parseRS.py -d G:\Exports\IERecoveryFiles

RecoveryStore.{2F8A1D83-BCA3-11E6-82E6-58946B55A470}.dat:
    Opened:              12/07/2016 17:32:54 UTC
    Closed:              N/A
    InPrivate Browsing: YES

    Open Tabs:
        {2F8A1D85-BCA3-11E6-82E6-58946B55A470}.dat:
            Page Order:   0, 1, 2, 3
            Current Page: https://search.wikileaks.org/?q=guccifer+2.0
            Page 0:
                URL:      https://www.google.com/?gws_rd=ssl
                Title:    wikipedia - Google Search
            Page 1:
                URL:      https://www.google.com/?gws_rd=ssl
                Title:    q=wikileaks
            Page 2:
                URL:      https://wikileaks.org/
                Title:    WikiLeaks
```

InPrivate Browsing Detected