EnCase Computer Forensics

Windows Operating System Artifacts

Dates and Times - 1

- You must verify the date and time settings for the evidence.
  - Verify and alter EnCase Time Zone information when necessary
  - Microsoft often stores in both local and GMT (Greenwich Mean Time)
  - Time Zone effects MAC information
    - Modified
    - Accessed
    - Created

Dates and Times - 2

- Adjusting for Time Zone Offsets
    - Determine which Control Set is the current one
        - Mount the system registry
            - This is a compound file so you will need to mount is and View the File Structure from the Entries drop-down
            - System\NTRegistry\Select\Current
                - View as a 32-bit integer
                - This determines which control set is current
        - System Registry Keys
            - Win NT/2000 – C:\Winnt\System32\Config
            - XP/Server 2003-2008/Windows Vist/7
                - C:\Windows\System32\Config

Date and Time - 3

- Navigate to the System Key
  - Navigate to the System Control indicated in the previous step
- Navigate to System\NTRegistry\ControlSetoo?\Control\TimeZone Information
  - Review information located there
  - There are Bias times, Daylight Bias and names etc.

Dates and Times - 4

- ActiveTimeBias – current offset from GMT
- If in a Daylight Savings time zone and ActiveTimeBias = StandardBias then you are in Standard Time
- If the ActiveTimeBias=DaylightBias the computer is set for daylight saving time
- StandardName indicates the time zone setting

- YOU CAN USE ENSCRIPTS TO ACCOMLISH THIS AS WELL
- MUST COMPLETE BEFORE PROCESSING

Date and Time - 5

- Adjusting the Date and Time Zone
  - Evidence tab Entries view
    - Focus at top or Entries Level
    - Highlight the device
    - Modify Time Zone Settings from Device Drop-down menu
    - Select the correct time zone offset based on your earlier analysis of the time zone settings for your device
    - Select OK

Recycle Bin - 1

- User can hold down the Shift key when pressing Delete to bypass the Recycle Bin (few users know this)
- Detail of the Recycle Bin
  - User Deletes File
    - MFT for file is deleted
    - Directory entry or MFT entry made for the file in the Recycle Bin
    - New filename has nothing to do with original file
      - D[original drive letter of file] [index number].[original file extension]
      - D=deleted

Recycle Bin - 2

- INFO2 File
  - When a user views files in the Recycle Bin – stored as a hidden file named INFO2
    - When a user deletes a file an entry is also in the INFO2 file
    - INFO2 – database for deleted files
      - Files Original filename and path (ASCII and Unicode)
      - Date and Time of deletion
      - Index number – link between new filename and INFO2 record
      - Records in the INFO2 database are a fixed length
        - Important because we can bookmark-viewing tool that can decode the fields so you can include it in your report as a sweeping bookmark
        - Must know starting point and record length
        - Utilize the proper wrap length depending on OS (491 chart)
        - Decode tab allows for EnCase to report INFO2 information

Determining the Owner of Files in Recycle Bin - 1

- When a user first deletes a file a folder with their SID is created and whenever they delete a file it resides within that folder
- Mounting the SAM (Security Accounts Manager) – registry file
  - EnCase scans the SAM when loading the evidence files resolving SID to authenticated users
  - Highlight the SID folder in the recycle bin
    - Permissions view – NTFS permissions appear
  - Local logon accounts where the hosts SAM stores the SID

Determining the Owner of Files in Recycle Bin - 2

- SID for a Domain Logon
  - Stored on the Server
  - EnCase cannot resolve these because the SAM is not local
  - You will need to obtain the username for the SID manually in the Secure Storage View after that EnCase will remember the SID and username combination and resolve it for you
  - EnCase EDS module processes the cached domain accounts with Analyze Encrypted Files System (EFS)
    - Get the volume to show in table view ->highlight it->Analyze EFS from the Device drop-down menu
      - The cached info. Will be analyzed and available to the examiner

Files Restored or Deleted from the Recycle Bin

- Emptying the Recycle Bin deletes the files in the FAT or MFT and the INFO2 database.
  - Checking the slack immediately after the 20-byte header you will see much of the INFO2 records in the Recycle Bin prior to it being emptied.
- Restored Files
  - A record is created int eh MFT for the folder where the file was originally locatd
  - Entry for the file in the MFT of the Recycle Bin is marked deleted
  - Entry in INFO2 file – not deleted 1st character 00h – similar to E5h for deleted files

Evidence Processor to Determine Status of Recycle Bin Items

- Restored or Deleted items
  - INFO2 search for string 00 3A 5C
    - Looks for :\preceded by 00h
    - You would then need to analyze the files further to see original paths and MFT entries for filenames, starting clusters, and so forth
- Windows Artifact Parser
  - Launch Evidence Processor
  - Modules at the bottom
  - Recycle Bin Files is one
    - Looking in unallocated clusters will add significant time
  - Run Case Analyzer from the EnSCript menu – provides you with an interface where you can drill down and review various artifacts recovered

Recycle Bin Bypass

- Right Click the Recycle Bin ->Properties
  - Do Not Move Files to the Recycle Bin
  - Represented in the Registry
    - NukeOnDelete registry value to 01h
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVerson\Explorer\BitBucket
  - Once set when a file is deleted
    - Indicated by a lot of deleted files and not much info. In the INFO2 record artifacts
    - Suspect it has been set
    - Verify via Registry

Windows Vista/7 Recycle Bin -1

- $Recycle.Bin
  - $I – Individual index files in the Recycle Bin
    - Full path begins at byte offset 24
    - Time stamp for deletion – immediately precedes the path 64bit Windows time stamp FO 16-23
    - Creation and Deleted time stamps (should match)
    - File size is also important FO 8-11 Dword value
      - Only parent folder is renamed everything else will not be
  - $R – Deleted filename starts with $R
  - Both have a GUID that matches
  - EnCase will show you the data with the filename before it has been deleted.
  - Short Name column will show you the raw filename

Windows Vista/7 Recycle Bin - 2

- Updated Recycle Bin for Win 7
  - Identify files placed in the Recycle Bin from mapped drives

Link Files -1

- .lnk files – Shortcuts
  - Applications, directories, documents or data fles
  - Printers etc
- Changing the Properties of a Shortcut
  - Icon – right click icon ->properties ->shortcut tab
- Forensic Importance
  - Properties, contents, and creation specifics
    - Creation
      - Created by the OS and by applications at install
      - Created by the User with or without their knowledge

Link Files - 2

- Created in the Recent Folder
  - When a user opens a file
    - Users\UserName\AppData\Roaming\Microsoft\Windows\Recent
  - Contain MAC time stamps
    - May indicate a user was aware of a program and intentionally created easy access to it

Link Files - 3

- Content
  - Describes the various attributes of the target file
    - Complete Path
    - Vol. serial number on which the target exists
    - File’s size in bytes
    - MAC time stamps of target
      - Created, last accessed and last written (in that order)
      - FO 28, 36, 44
      - Select all three – starting at FO28 to FO52 - 24 bytes
      - Decode view – Choose dates under view types->Windows Date/Time
      - All three will be shown in their respective order
      - Find a link file wherever they may exist
        - String \x4C\x00\x00\x00\x01\x14\x02

Link File Parser

- Located within the EnCase Evidence Processor
  - Modules
  - Windows Artifact Parser
  - Select this option when running the Evidence Processor
    - This will add time to the process
  - Once the processor completes run Case Analyzer
    - This parses information found and presents it to you in a hierarchical navigation
  - You should parse unallocated space as well as link files may often be stored in swap files etc.
  - Hibernation file holds much info as well. Hiberfil.sys

Windows Folders - 1

- Examiners should be familiar with directory and naming conventions for various Windows OS
  - System File Locations

[Instructor Selected Image]

Windows Folders - 2

- Windows creates a unique folder when a user logs on for the first time.
  - A folder is created that bears the name of the user
  - Created if a user logs on locally or through a domain
- Reparse Points
  - Microsoft's way of maintaining backward compatibility while changing names and locations of folders
- Windows segregates user's configurations, environment and document files into sub-folders under the root user folder.

Windows Folders - 3

- NTUSER.DAT is also created at first log-on
  - It is comprised of the user's registry hive
  - Specific to that user ONLY
  - File Creation date would indicate the first time the user logged on
  - Last Written date – user last logged out / used the computer

Windows Folders - 4

- Recent Folder
  - Provides a user interface that lists documents the user has recently created or modified
  - There is a link file created in order to access this information.
  - C:\Users\%UserName%\AppData\Roaming\Microsoft\Windows\Recent
    - Users are unaware of this link file creation
  - Contains only link files
  - This folder can contain hundreds of link files even though Windows displays only the 15 most recently used.
  - One link file per document – the link file is updated every time it is accessed.

Windows Folders - 5

Desktop Folder

- Usually shortcuts (link files), applications or documents
- Contents of the Desktop come from 3 locations:
    - Registry
    - All Users/Desktop or Public/Desktop
    - User's Desktop Folder

Windows Folders - 6

- My Documents/Documents
  - Purpose of folder
    - Segregated storage of data
- Send To Folder
  - Objects or links that will appear in the Explorer interface
    - Good spot to find attached media (.zip, usb, etc)
- Temp Folder – sub-folder of the Local Settings
  - Users\%UserName%\AppData\Local\Temp
  - Many files can be found here – used by many applications
  - Normally a “hidden” folder

Windows Folders - 7

- Favorites Folder
  - Internet shortcut files for Microsoft Internet Explorer
  - .url files
  - Besides vendor manipulated OS shortcuts and those default to the browser the items here can generally be explained to be placed by the user
  - Multiple favorites with the same time-stamp may indicate malicious software

Windows Folders - 8

- Windows Vista Low Folders
  - Cookies, History and Temporary Internet Files
    - Low folders are created for security
    - Windows places items here so they will have the lowest possible level of integrity and is in a “protective” shell
  - Maneuvering around in the Windows Explorer shell items from opening documents will also make it into this area therefore not everything is located in Low

Windows Folders - 9

- Windows Vista Low Folders
  - Differences can lie in these exceptions:
    - Disabling Internet Explorer 9 protected mode
    - Running IE9 in Administrator mode
    - Turning off the UAC
    - Trusted sites are considered “safe” the protected mode does not apply to those sites
    - Viewing local HTML files

Windows Folders - 10

- Cookies Folder
  - \Users\%UserName%\AppData\Roaming\Microsoft\Windows\Cookies
    - Includes a Low folder as well
  - Pieces of code placed on a users computer to enhance a user's browsing experience
  - .txt file extentions
  - Index.dat file keeps track of them all
    - Pointers to the cookie file and the originating web domain name
    - Dates
      - Could be used to check cookie expiration date with system time
      - CookieView is included in EnCase as a viewer
      - You can open the cookie with the viewer

Windows Folders - 11

- History folder
  - Local folder – because it does NOT follow a user in a domain setting
    - C:\Users\%UserName%\AppData\Local\Microsoft\Windows\History
    - History of Internet Browsing
  - Must parse Internet History in Evidence Processor in order for EnCase to decode them for your viewing
  - Once parsed they are located
    - IE history and web cache – results in the Records tab
    - Case Analyzer can also be used to summarize info.

Windows Folders - 12

- Temporary Internet Files
  - Local Settings – does NOT follow a user on the domain
    - C:\Users\%UserName%\AppData\Local\Microsoft\Windows\Temporary Internet Files
      - Low folders are here as well
    - Stores files downloaded and cached from the Internet
      - Index.dat file

Windows Folders - 13

- Swap File
  - Pagefile – area where information is written when RAM is maxed
  - Should always check this file
  - Registry Key
    - Key:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
    - A setting of ClearPageFileAtShutdown with a value of 1 indicates the page file is to be deleted at shutdown

Windows Folders - 14

- Hibernation File
  - Hiberfil.sys
  - Holds the entire RAM
- Print Spooling
  - Writing the print job to a couple of files so the print job can run in the background
    - Winnt\system32\spool\printers
    - Windows\system32\spool\printers
    - Can be configured by the user
      - Key:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wondows\NT\CurrentVersion\Print\Printers\DefaultSpoolDirectory
      - Could be sen to the server in a networked environment

Windows Folders - 15

- Print Spool
  - 2 files
    - Shadow file .shd extension
      - Username, printer, name of file and print mode
    - Spool file .spl extension
      - Actual print job graphical data
    - Matching 5 digit names
    - Default printing mode is EMF – Microsoft Enhanced Metafile
    - Each page printed will be represented by an EMF file embedded within the spool file in the order they were printed
    - Has it's own unique header
    - Usually located in slack space

DOL Disclaimer and CCBY

This workforce product was funded by a grant awarded by the U.S. Department of Labor’s Employment and Training Administration. The product was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties, or assurances of any kind, express or implied, with respect to such information, including any information on linked sites, and including, but not limited to accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.