EnCase Computer Forensics

File Signature Analysis and Hash Analysis

File Signature Analysis - 1

- Compares Headers to Extensions against a database of information.
  - Results
    - Match – header is known and extension matches
      - - if the header does not match any other known extension
    - Alias – header has a match, but the extension is not correct
      - Takes info of the header to determine the file's origin
    - Bad Signature– has a known extension, but the header does not match the header of the extension or any other known header
    - Unknown – can't find a header match or extension match
  - Windows Application Binding
    - Stored
      - Ntuser.dat - \Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts
        - OpenWithList
        - OpenWithProgids

File Signature Analysis - 2

- Hiding Information
  - Changing Extensions
    - Makes a file seem as though it is corrupt
      - Application called to open it does not know how to open a file with such a header.
      - System 32 folder .dll files?
- Linux
  - Does NOT use extensions it uses header information to bind to an application
- MAC
  - Uses a combination for HFS+ (current) HFS
    - Creates a 32bit value – file type code
    - Creates a 32bit value – creator code

File Signature Analysis - 3

- MAC
  - 7 Rules of Precedence for binding
    - User Defined – overrides all
    - Creator Code
    - File Extension
    - Last 4 more complex check it out at apple.com

File Signature Analysis - 4

- Creating a New File Signature
  - Stored
    - FileTypes.ini
    - View File Types
    - Table/Database of extensions, categories, names, headers, footers, viewers and other metadata
  - Any item can be viewed from either the fields or report pane
  - Adding a record/file type
    - New – follow tabs and enter info.
  - Deleting
    - Right click - delete

File Signature Analysis - 5

- Editing a File Signature
  - P. 440-442
    - Multiple extensions associated with a particular header
      - Use the ; and no spaces to separate the extensions
- Conducting a File Signature Analysis
  - Run over all files
  - Run within the Evidence Processor
    - Looks at ever file on the device and compares its header to verify a match
  - Complete 8.1

File Signature Analysis - 6

- Filter
  - Filter -> Entries -> by signature
    - You can use this method to view the signature analysis by EnCase Signature Entry
    - Must view in the Results tab

Hash Analysis - 1

- MD5 and SHA-1
  - Odds of two dissimilar files having the same hash
    - 340 billion billion billion billion
    - If 2 files have the same hash value you can safely say they are in fact the same file bit for bit
    - Hash is completed on the data and not any metadata or file names and extensions
- Hash Sets and Hash Libraries
  - Collection of hash values of common files grouped together
    - Know Programs
    - Hacking Tools
    - Contraband Files

Hash Analysis - 2

- Creating Hash Sets
  - Downloaded and imported from external sources
    - NSLR
    - Police Dept. Files
  - Created by the User
  - Must create a folder to hold the hashes
    - EnCase7 Program Files
      - Hash Libraries
      - 2 Subfolders
        - Hash Library #1 and NSLR
  - Managing Hash Sets
    - Tools ->Manage Hash Library
    - Open ->Hash Library and select NSLR

Hash Analysis - 3

- Managing Hash Sets
  - Open NSLR Set
    - View the contents and structure
  - Creating a New Hash Set
    - New Hash Library -> browse to the folder
      - Once you hit OK the folder is populated with the Hash Library structure
      - Have files that have hashes
        - Blue check files ->Open Entries menu ->Hash\Sig Selected
        - Green back button to Evidence Table – double click evidence item and view the entries again
        - Select the files ->Entries menu ->Add to Hash Library ->Choose the library and metadata associated with it
      - Can select create a new hash set – right click anywhere in the existing hash set table and choose New Hash Set – give it a name and a category then OK
      - Can import legacy hash sets as well

Hash Analysis - 4

- Query a Hash Set
  - Copy file hash -> from within the Hash Manager -> Launch the query and paste in the hash – this will run a query just for that one file
  - Queries only the open database
- Hash Analysis
  - Home Screen – Must apply them to your case
    - Hash Libraries
    - Select up to two Hash Libraries to apply to your case
    - Change Hash Library to select the path
      - Enable with a blue check
      - Select what sets within the libraries or right click within the table and select all items

Hash Analysis - 5

- Hash Analysis
  - Must have already hashed your files in the case
  - Opting not to search in the files content areas of files that were found in hash libraries
    - SAVES TIME!!!
  - With hashing completed and sets add to the case
    - You can view the results of your hash analysis
      - File will show with a positive value in the Hash Set column if found.
  - Filtering Based on Hash Sets
    - Filter ->Find Entries by Hash Category
    - Filter -> Known files so you don’t focus on them

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.