Advanced Computer Forensics

EnCE EnCase Forensics: The Official EnCase Certified Examiner Study Guide

Understanding Data

Chapter 7

Understanding, Searching for, and Bookmarking Data

Understanding Data - 2

- Binary Numbers
  - 1 or 0 - on or off (pit, pulse, or magnetic state)
    - Bit 1 or 0
    - Nibble 4 bits
    - Byte 8 bits
    - Word 2 bytes (16 bits)
    - D-word 4 bytes (32 bits)
    - Q-word 8 bytes (64 bits)

Understanding Data - 3

- The following table demonstrates a byte.
  - It can be used to indicate 256 numbers ranging from 0 to 255
  - The least significant bit is the furthest to the right (0)
  - Most significant bit is the furthest to the left (128)
  - Adding up all of the decimal values will give you 255

[Instructor Selected Image]

Understanding Data - 4

The following table demonstrates a byte.

- All Os – add all of the last row
- together and you get O

[Instructor Selected Image]

- All 1s – add all of the last row
- and you get 255

[Instructor Selected Image]

Understanding Data - 5

The following table demonstrates a byte.

- You should be able to create this yourself and be able to give the correct decimal equivalent to a binary number. The following example ends up being 99

[Instructor Selected Image]

Understanding Data - 6

- Hexadecimal

[Instructor Selected Image]

Understanding Data - 7

- Hexadecimal
  - The charts below describe how we can utilize Hex to display a binary number in Hex.

Decimal View [Instructor Selected Image]

Hex View [Instructor Selected Image]

Characters

- ASCII
    - American Standard Code for Information Interchange
        - Represents data that is in text format
        - Maps characters and other keys to binary or hex
        - 7 of the 8 bits are used to create 128 (0-127) characters of letters, numbers and punctuation
        - The 8th bit is used for parity / error checking in ASCII low-bit
    - ASCII (high-bit)
        - Utilizes the 8th bit for an additional 128 characters
        - Complete list at www.cpptutor.com/ascii.htm

ASCII

- Upper and Lowercase are represented as two different codes
    - This will be important to remember when we search
- Numbers are different
    - Numbers as TEXT are represented by one code
    - Numbers as Integers are represented by a different code
        - 8 as text is one code and 8 in an equation or representing an integer will be in a different code
        - Sometimes integers such as IP addresses are stored in humanly readable ASCII text and another program might store it in it's integer form (128.175.24.251 or 80 AF 19 FB – some even FB 19 AF 80)
        - Hex – 54 45 58 54 could represent any of the following
            - Integer – 1,413,830,740
            - IP address – 84.69.88.84 OR 84.88.69.84
            - Text – the word TEXT all uppercase

Unicode

- Worldwide standard for processing
  - The ASCII limit of 256 could not accommodate all characters in all languages
  - Unicode contains the ASCII, all languages even those with pictographs
  - Uses 2 bytes per character instead of one
  - Some programs store the characters in both ASCII and Unicode (A = 41h in ASCII and 4100h in Unicode)
  - *You will always want to search in both formats*

Browsing

- Browsing Evidence
  - Once Selected
    - Screen showing the evidence within the case
  - Viewing Data
    - Double-click the evidence item you would like to view
      - If you have viewed it before it will be read from the Evidence Cache
      - If it’s the first time it will be parsed and the cache will be created taking a little more time.
    - Viewing more than on evidence file
      - Select the items you want to see with a blue check
      - See the Load Selected Evidence on the toolbar
      - Open

Evidence Processor - 1

- Collection of tools that carry out a series of routines necessary for a proper examination of evidence
- Must have carried out the following steps:
  - Ensure EnCase has completed the verification process
    - Check the verification to make sure it completed with zero error and that the acquisition and verification hashes match
  - Account for space
  - Determine the Time Zone settings for various evidence items
    - Adjust EnCase to reflect the Time Zone offsets as needed
      - EnCase will default to the Time Zone of the examiner's workstation otherwise and this could make all evidence off by the difference of the two

Evidence Processor - 2

- Time Zones

  In Windows the information is located at

  - HKLM\System\ControlSet001\Control\TimeZoneInformation\TimeZoneKeyName
  - The Control Set 001 will not always be the active time

  The hive that houses this registry key is located at

  - \Windows\System32\config\SYSTEM
  - These hives are compound files and need to be *mounted* in order to see them in hierarchical format
  - Place your cursor on the parent folder in the tree (config), highlight SYSTEM open the entries menu and select View File Structure – accept the defaults (It takes a few minutes to parse this information)
  - Once the hive turns blue then it is complete – it is now a hyperlink
  - Clicking it will open it in it's own view pane

Evidence Processor - 3

- Time Zones
    - Current Control Set
        - Choose the Select Key and then Current in the table view
        - Seeing a 01 00 00 00 would indicate that ControlSet 001 is the active ControlSet
    - TimeZoneName
        - ControlSet001\Control\TimeZoneInformations\TimeZoneKeyName
        - Check to see if Dynamic Daylight Time disable hasn't been activated
        - 00 00 00 00 means enabled (Daylight Time is enabled)
    - Changing Time Zone in EnCase
        - Entries View – highlight the root so the device is shown in the table view
        - With the device highlighted – Open Device menu on the Evidence toolbar and select Modify Time Zone Settings

Evidence Processor - 4

- You Must
  - Acquire your evidence first
    - Can be run from the Evidence Tab or the Home screen
    - Evidence Tab is more commonly utilized
    - Select the evidence to process and then launch the Evidence Processor from the Evidence Tab Toolbar
  - You can make many selections regarding the processing
    - Items with Red Flags will ONLY run the first time the evidence is processed
    - Items without Red Flags can be run and re-run.
    - Recover Folders – Red Flag
    - File Signature and Protected File Analysis are Locked and will ALWAYS run
    - Hash Analysis – Red Flag (MD5 or SHA-1 or both)

Evidence processor - 5

Evidence Processing Options

  - Expand Compound Files – Run at any time
  - E-mail – Run at any time
  - Internet History – Run at any time (check unallocated as well for a comprehensive search)
  - Searching for Keywords – Run at any time (will increase the processing time exponentially)
  - Text Indexing – Takes considerable time to run, but increases search hit quickness (Here is where you will choose to skip items in a Hash library) – you can also extract personal information
  - File Carver – can search for parts of files based on their file signature and the File Types table. We can glean information from parts of files that may have been deleted
- To save for future use – find the Save Settings and Load Settings in the toolbar
  - May take hours or days to process evidence – (you would want the ability to do other investigations – another machine or a powerful one would help)

Evidence Processor - 6

- Results
    - Records Tab
    - Entries View

Searching for Data - 1

- Make sure you index
  - Indexed Searches
    - Run against indexed items – results instantaneous
  - RAW Searches
    - Utilizing keywords and keyword lists to search for the entire stream of data
    - Can also search within the View Pane
    - Each has its benefits
- Creating Keywords
  - RAW within the Evidence Processor – stored within devices cache files (used for that device)
  - RAW from toolbar – Table tab – all devices –
  - Entries Tab – based on selections in the Tree Pane – from a file (.keyword)

Searching for Data - 2

- Creating Keywords
    - Choose entire device / all evidence OR Select files or locations
        - Raw Search Selected – New Raw Search
        - Create a folder, choose one, or store it in the root
        - Launch the New Keyword dialog box
        - Right-click – Table Pane and New, Containing folder and New
        - Edit New
        - Insert on Keyboard
    - Enter your search string
    - Select the Search Options (review them on p.358 -360)

Searching for Data - 3

- Managing Keywords
    - Within the .keyword file you can
        - Create folders and keyword structure
        - Move folders and words
        - Delete
        - Add
- Adding Sets of Keywords
    - Importing or Adding
    - With all words selected right click and drag to a folder in Tree Pane – once you release you will have the option to Move or Copy them (Copy)
    - Export the whole list by starting at the root – right-click the folder or root and choose Export – browse to where you want to store it and OK
    - Importing – Choose the level – right-click (Import) choose the path OK
    - Adding – Add a list – Choose where to save it – Add list menu options – type or paste into this dialog box -OK

Searching for Data - 4

- GREP Keywords
  - Very Flexible Options and Expressions
    - GREP Syntax on p. 365 and 366
    - Must know these tools and creating expressions well
    - If what you are looking for is a GREP expression like a hyphen then you need to use the backslash in order to tell the machine that you are looking for the item – not using it as an expression - (\-)
    - Keyword Tester within EnCase allows you to test your GREP expression prior to running it. You create a “test” file and then run your expression against it.
- Starting a Search
  - Select words to search for and select the device, location or files you want to search and then OK
  - Entry Slack – between the end of a file and the last byte of the cluster

Searching for Data - 5

- Starting a Search
  - Use Initialized Size – Only the initial size of an entry only in NTFS – data a user would see in a file
  - Undelete Entries Before Searching – EnCase will logically “undelete” the file before searching the data – This will find keywords that may span the starting cluster and the next unallocated cluster. Assumption that the next unallocated space belongs to the file is forced
  - Skip Contents of known files or Search Only Slack Area of Files in Hash Library – Must have done a Hash Analysis previously – if the file exists it is NOT searched – Excludes known files within a search, but the slack area is still searched
  - You may want to utilize the WebMail Parser under the Carve Option in order to gather any webmail that may be on the machine

Viewing Hits / Bookmarking - 1

- Results are under the Search Tab
  - View Search
  - Choose the applicable tab – usually the last used opens by default
  - Right-Click Options
    - Copy – copies data in the table in which the cursor is placed to the clipboard allowing placement somewhere else
    - Save Results – Saves the results of the search to a file
    - Bookmark – Launches the window where you can bookmark the results.
    - Go to File – Launches Entries Viewing Tab within the Search Tab and places focus on the selected file with the path in the Tree to the left
    - Find Related – Finds files related by filename or time

Viewing Hits / Bookmarking - 2

- Bookmarking
  - References to specific files / data
  - Bookmarks can be created in almost any location where data can be found.
    - Can contain notes added by the examiner
    - Can be organized into a hierarchical manner
    - Reflect the layout of the items within your Report
  - Bookmarking is one of the most necessary skills as it is directly reflected within your report
    - You can find evidence all day long, but if you can't report it or display it well your case will suffer.

Bookmarking - 1

- Highlighted Data Bookmarking
    - Referred to as the *sweeping bookmark*
    - Locate your data in the view pane
        - Click and drag to highlight it
        - Place your cursor in it – right-click - Bookmark
        - Can choose Note, Single Item or RAW (Choose RAW for highlighted text)
        - Enter comments and or choose a location in the bookmark tree for the bookmark (maximum length of a comment is 1,000 characters)
    - Folder names act as Headings and Subheadings for your report
        - Create this as you go so that labeling will be more accurate
        - You can also decode the information to show how the user saw the RAW data. In the example in the book that is HTML – you would want to decode so that we can view it as they saw it – bookmark the decoded information.
        - Make sure to choose the Bookmarking data structure of the decoded data
        - Save and Review to make sure it is what you want.

Bookmarking - 2

- Notes Bookmark
  - Notes, comments or any text format you can paste into it
  - Helps enhance information in your report
    - Limit of 1,000 characters
    - Built in formatting tool
    - Right-click where you want to insert the note bookmark – Add note
    - Type or paste in text – formatting pretty straightforward – show in report
    - It will be presented as sort of a footnote within the folder by default, but you can move it by clicking and dragging to the desired location

Bookmarking - 3

- Notable File Bookmark
  - Inserts a bookmark or reference to a file that contains information significant to your case
  - Does NOT bookmark data, but rather information regarding the file
    - Attributes and properties
    - Right-click the file from the Table View – bookmark – Single Item
    - Choose the destination folder, add a comment
- Bookmarking Selected Items
  - Notable File Bookmarks can be created from Selected Items
    - Select with Blue checks
    - Right-click bookmark Selected Items
    - Choose your destination folder – create a notes bookmark or let the folder name indicate the contents
    - Verify your Dixon box prior to bookmarking!!!

Bookmarking - 4

- Other Bookmarks
    - Various routines, threads, or EnScripts might have the option to bookmark – If it is selected it is sent as a Notes bookmark which can be dragged to the folder of choice.
        - Can copy and paste from 3rd-party tools, Internet research or most text daga into the notes bookmark to include in your report
- Log Record Bookmark
    - EnScript runs and parses data from entries. The data is written to a log record
        - No pointer to the data
        - Important when parsing the registry
        - View Log Records
        - We will very often see verification etc. located here – best practices tells us we should – bookmark the log records (place blue checks – right-click – bookmark – table view (name and comments) – choose columns to show

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.

Except where otherwise noted, this work by Central Maine Community College is licensed under the Creative Commons Attribution 4.0 International License.