# SEARCHING, VIEWING AND BOOKMARKING

Chapter 7
Key Concepts

# SEARCH TYPES

**3 Types**

- Index Searches – Evidence data is indexed when you use the Evidence Processor prior to searching
  - **Searches the index for results**
- Raw Searches – Searches based on non-indexed, raw data
- Tag Searches – Searches based on user-defined tags

# INDEX SEARCH

- **Entries from the Evidence Processor:**
  - **Contain pointers to the occurrences of the specific work on the device.**
    - **Generating an index (used in the Processing Evidence Files)**
    - **Searching the index**
  - **Generating the index – Creates a file associated with devices. It can be time consuming if the evidence is very large, and thus create a fairly large index file.**
  - **Search index – Should be completed early on in the workflow sequence**
    - **Case must contain the device to index**
    - **Right-click evidence processor**
      - Select indexing text
- **Results are almost instantaneous!**

# RAW SEARCH

- Uses Keywords to search selected data
  - Takes a while to get results
    - You can be precise and flexible if you can utilize GREP expressions
    - You will begin to know when to use Index vs RAW with experience
  - EnCase encourages the Index Search method
    - If you need results from PDF, compressed or even Office files later than 2007 you will need indexed searching to even get hits on your searches.

# RAW SEARCH continued

- Allows you to find related files and folders
  - **By name or time**
  - **Go to file button in the evidence folder structure**
    - Permissions tab will tell you who had access to the file
    - You can then add evidence with a bookmark
    - Bookmarking multiple files does NOT allow you to create a note/comment for the bookmark
  - **Search and Results tab**
    - Copy Files
    - Copy Folders
    - Add Results to Hash Library
    - Save Results

# SEARCH RESULTS

- **Columns must be enabled in order to include them in a view:**
  - **General Columns:**
    - **Unique Offset, Description (file, archive), True Path, Full Path, Symbolic Link, Entry Modified**
  - **E-Mail Metadata**
    - **Received (time), Sent (time), Has Attachment**
  - **Internet Metadata**
    - **Action URL, Icon URL, Requesting URL, URL Host, URL Host Name, URL Name**

# CREATING A SEARCH QUERY

- **Keywords**
  - Stored for future use within EnCase
    - Home ->Search ->enter the keyword or words
    - A dynamic list is displayed on the right side
      - Shows the term and the number of occurrences
    - You cType “Tyler”
    - Click ->Play
    - an double-click a query and it will show info. regarding the term
  - The results will display in the Table Pane of the Search View
  - You can review file entries in the transcript and compressed views
  - You can save the results in the Results view
    - Searches ->Save as
    - Searches folder in your under your case folder

# RAW SEARCH KEYWORDS

- Creating
  - Decide what you would like to search
    - All evidence and devices (launch from table tab)
    - Limited set of data ->Entries tab select items (blue check)
      - RAW search selected
  - RAW Search All
    - New RAW Search All

# KEYWORDS

- New Keyword Dialog box
  - Expression – your search string, phrase or GREP expression
  - Name – Label that appears with the keyword in Search Hits View (very useful when using GREP)
  - Case Sensitive – Upper and lowercase letters
  - GREP – used to narrow a search and limit false-positives, or when only portions of a word are known
  - ANSI Latin 1 – default code for Windows OS
  - Unicode – foreign language character sets (Office, Windows 2K and above). You still need to use the ANSI Latin-1 or another appropriate code page in order to get results.
  - Unicode Big-Endian – Non-Intel based data scheme multiple byte numerical values – reverse Endian (most significant first to least significant)

# KEYWORDS – Page 2

- **New Keyword Dialog box**
  - **UTF-8 – Universal Character Set Transformation Format. The most common format that applications encode their Unicode. 8 bit form of Unicode. Offers foreign language support.**
  - **UTF-7 – Special format that encodes Unicode within US-ASCII in a way that all mail systems can accommodate.**
  - **Whole Word – Keyword as a whole word and not within a larger word. Cuts down on false positives.**

# KEYWORD OPTIONS

- **Keyword Search Options**
  - **Search Entry Slack – search the slack areas between the end of the logical data to the end of the physical file for all items searched**
  - **Use Initialized Size – Search only the initialized size of an entry as opposed to the logical or physical. If the initialized size is smaller than the logical size, the space after the initialized size is zeroed out. Searches only data a user would see within a file.**
  - **Undelete entries before searching – Logically "undelete" deleted files prior to searching. Will find keyword fragmented between a starting cluster and an unallocated cluster. Searching for portions of words is also encourages, GREP search.**
  - **Search Only Slack Area of Entries in Hash Library – Used with hash analysis. If the file is identified from the hash library, then it will not be searched. The slack area of these files will be searched. If this option is turned off, EnCase will ignore the hash analysis.**

# ENTERING KEYWORDS

- **Adding a Keyword List**
  - **New RAW Search**
    - Add Keyword List
      - Can be entered by the keyboard or pasted from a text document (one expression per line)
      - You still have the ability to add / remove the code pages associated with the keywords
    - OK – Search begins

# Viewing Results

- **Adding a Keyword List**
  - New RAW Search
    - Add Keyword List
      - Can be entered by the keyboard or pasted from a text document (one expression per line)
      - You still have the ability to add / remove the code pages associated with the keywords
    - Use the Go to file to get to the originating location/file
      - Use Back to return to Search View
  - Keyword searches not initiated from Evidence Processor are stored with the case
  - Keyword searches that are conducted within the Evidence Processor can belong to multiple cases

# Refreshing Search Results

- **RAW allows you to see results as the search finds them.**
  - **Refresh RAW Search Hits icon in the search tab to refresh hits.**
    - **Refresh will turn green when new hits are available**
- **TAG Searches**
  - **Search for instances of a particular tag you have created. (more in later lessons)**
- **Search Summary**
  - **Summary tab**
- **Results to LEF**
  - **Export to a Logical Evidence File (entries and records)**

# CONTINUE THE INVESTIGATION

- Switching Views
  - Doc view to see items as they were such as .html documents
    - Select file then go to originating evidence
- Bookmarking Evidence
  - Search, Results or Evidence Views
    - Can add comments as well
    - Choose your folder to add the evidence to or create a new one.
    - Use back button to return to the results view of your query

# FIND RELATED

- **Allows you to find related files and folders**
  - By name or time
  - Go to file button in the evidence folder structure
    - Permissions tab will tell you who had access to the file
    - You can then add evidence with a bookmark
    - Bookmarking multiple files does NOT allow you to create a note/comment for the bookmark
  - Search and Results tab
    - Copy Files
    - Copy Folders
    - Add Results to Hash Library
    - Save Results

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.