Processing Evidence Files

Evidence Processor

- First task for every case!!
  - After adding the evidence and confirming it has validated with no errors and is browse able.
  - Allows you to run one automated session that collect and analyzes your case data. You can run this unattended freeing you to work on other aspects of the case.
  - Once finished you can begin to analyze and report for your investigation:
  - 2 Categories
    - Preparation
    - Processing
  - You must acquire the evidence you cannot be previewing it
  - Confirm time zone is configured properly

Time Zone

- Determine Time Zone setting on suspect device
    - Location - C:\Windows\System32\Config\system
        - Right-click on the file SYSTEM hive Entries->View File Structure
        - Encase will scan and parse the registry and build a cache file
        - Once the file has been created the file becomes a compound file indicated with a green + sign
        - Double clicking on this file will open the file
        - Browse to the location HKEY_LOCAL_MACHINE\System\ControlSet001\Control\TimeZoneInformation\TimeZoneKeyName (check it out in HEX)
        - Verify Daylight Time disabled is off (HEX 00 00 00 00) Means DST is used

Time Zone continued

- Configuring Time Zone Settings
  - Evidence
  - Right-click the evidence file
  - Right-click on Device in the drop down menu
  - Click Modify time zone settings
    - The Case Time Settings dialog appears
  - Select the appropriate time zone and click OK

Preparing Evidence for Processing

- After adding evidence to the case you must:
  - Acquire the evidence if not already acquired
  - Select the evidence you intend to process
  - Add options in the processor as you continueYou can select additional options on subsequent Evidence Processor runs, however you cannot remove previously run options
  - You can run modules over and over again with different settings each time. The results will all be added to the case
  - You cannot process previously processed and processed evidence together. All evidence processed at one time must use the same settings
  - Right-click the evidence select process
    - Managing Evidence Processor Options opens up

Managing Evidence Processor Options

- Process Options
  - Unprocessed Evidence Files - # in ()
  - Selected Unprocessed Evidence Files - # selected that are not processed and remaining in the case will be in ()
  - Current Item - name of the evidence file ()
  - Options Label - Assign a label for Process for later

Using the Processor Settings Toolbar

- Evidence Toolbar
  - Split Mode - Change the display format of the options pane
  - Edit - Edit the options for a selected task in the window
  - Save - Save the current selection of settings as an Evidence Processor template
  - Load - Load a saved template to run against the current data
  - Use Defaults - Reset options to default settings
  - Dropdown side menu - Allows you to perform actions, such as printing the results and changing the layout of the Evidence Processor panels
    - Functions with a lock cannot be changed or disabled
    - Functions that are red-flagged cannot be run at a later date if not initially selected

Evidence Processor Prioritization

- Prioritization Link
    - Enables you to process a subset of the evidence and begin examining it while it continues to process the remaining evidence
        - Click the Hyperlink
            - Enable Processing Prioritization (checkbox)
            - Documents
            - Pictures
            - Items within certain dates
            - Process only prioritized items

Enabling Evidence Processor Lock/Unlock Mechanisms

- Prevents you from configuring the processor in ways that create inconsistent states of evidence
    - Recover Folders
    - Protected File Analysis
    - Hash Analysis
    - Email
    - Keyword Searches

File Signature Analysis

Thumbnail

Compound Files

Internet Artifacts

Index

Evidence Processing Tasks

- Use the Evidence Processor pane to select tasks
  - If the name is in blue font click on it to configure it
  - If it is in black no configuration is necessary

Evidence Processor Lock/Unlock Mechanisms

- Recover Folders - deleted or corrupt (FAT and NTFS)
- File Signature Analysis - Determine if extension matches header
- Protected File Analysis - Identify encrypted and password-protected files
- Thumbnail Creation - Creates image thumbnails for faster display
- Hash Analysis - Generates MD5 and/or SHA1 hash values for files and compares agains your Hash Library

- Expand Compound Files - Expands compound and compressed files - ZIP, RAR, etc
- Find Email - Extract individual e-mail from archive files - PST, NSF, DBX, EDB etc
- Find Internet Artifacts - Collects internet related artifacts - histories or cached pages (can also check unallocated space
- Search for Keywords - search raw text for keywords
- Index and Metadata - creates an index when you need to search for keywords in compound files.

Evidence Processing Useful Features

- Simultaneous processing of multiple devices
- Convenience of acquiring devices right from the Evidence Processor
- Saving sets of Evidence Processor options as templates to be run with little or no modification at a later date.
- On-screen instructions to guide you through settings
- Automatic processing of the results from any EnScript modules accordion to the current processor settings (Index, Keyword search, etc.)

Tasks – Page 1

- Recover Folders
  - FAT - searches for . .. signatures for deleted folder in the unallocated clusters
    - Rebuilds the files and folders found within
  - NTFS through MFT records for files without parent folders - useful when drives have been reformatted or the MFT has become corrupt
    - Recovered files are placed in gray Recovered Folders virtual folder in the root of the NTFS partition
- File Signature Analysis -
  - Determines whether the extension of a file has been modified and whether it matches the type of file indicated by the header bytes. Not user-configurable always enabled to support other EnCase v7 operations

Tasks– Page 2

- Protected File Analysis
  - Uses Passware Encryption Analyzer (http://www.lostpassword.com/encryption-analyzer.htm) to identify these types of files and information about the application used to protect them
  - You can export the index and known passwords as a dictionary used for decrypting protected files. This feature requires a valid installation of the Passware Kit
- Thumbnail Creation
  - Generates thumbnails for all images and stores them as part of the cache
  - smaller and faster loading - improves the speed that you can work with pictures

Tasks– Page 3

- Hash Analysis
  - Digital fingerprint of a file or data (binary data written in hexadecimal notation)
  - Most Common Uses:
    - Identify when a “chunk” of data changes
    - Verify data has not changed
      - Hash value is equal before and after verification
    - Comparing a hash value agains a library of known good and bad hash value seeking a match
  - Also computes the Entropy value if desired (randomness in a file) helps in near-match analysis

Tasks– Page 4

- Expand Compound Files
  - Expand archive, .zip, .rar, registry etc.
  - Extracts and process them in accordance to processor settings (includes nested or archived files)
- Find E-Mail
  - Select to extract email messages from archives
    - Click - Find Email
    - Email archive types that you want to examine
    - Search for Additional Lost or Deleted Items
      - Formats: PST, NSF, DBX, EDB, AOL, MBOX, EMLX
  - Thread E-Mail
    - can track different threads and communication patterns (senders and receivers)
      - Show conversations and show related messages features

Tasks– Page 5

- Find Internet Artifacts
  - For browser histories and cached pages
  - Also searches within unallocated space
- Search for Keywords
  - Raw search during process
  - Selecting the keyword search in the processor displays the current case keywords
    - RECOMMENDATION - Keyword searching be done outside of the processor so that it will save time

Tasks– Page 6

- Index Text and Metadata
  - Creates a searchable index of data
    - Instantly search terms in a variety of ways
    - Search on the transcript output of a file (Office 2007 and 2010)
    - Takes time - usually thought that the time to create the index is gained back with near instantaneous search times
      - RECOMMENDATION: Always index your case
    - Slack and unallocated space
      - Increases total indexing time, but info could be in the location

File Slack– Page 1

Microsoft OSs allocate disk space for files by clusters

Drive slack

Unused space in a cluster between the end of an active file and the end of the cluster

Includes:

RAM slack and **file slack**

File Slack– Page 2

[Instructor Selected Image]

Unallocated Space– Page 1

- Sectors not associated with an allocated file.
  - Free space of a disk or volume
    - Unwritten to or previously written with no historical attributes currently associated with them
    - They are combined into “unallocated” clusters
      - These are divided into sections and indexed with shared metadata
    - RECOMMENDED: Indexing with East Asian support
      - Prevents meaningless strings from being added to the index

Unallocated Space– Page 2

- Sectors not assigned to any partition scheme are under the Unused Disk Area – EnCase handles these as they do Unallocated Clusters
- Including Slack and Unallocated Clusters
  - Click Index Text
  - Set maximum word length to 64
  - Select Index slack and Unallocated
  - Index only for either known items or all items in the hash select appropriate check boxes
  - Select for East Asian support
  - OK

Personal Information

- Searches document, database, and Internet files for:
    - Credit Card Numbers
    - Phone Numbers
    - Email
    - Social Security Numbers
- Entry Condition – allows you to determine the categories to search. Unselect to search all files on the device.

Modules– Page 1

- These can be added during the processing:
  - Canned from EnCase
  - Create your own
  - Select modules that are relevant to your case
- Do NOT enable Modules by default as it will add unnecessary time to all case processing

Modules– Page 2

- System Info Parser – Report on core system information for Linux and Windows
  - Startup Routine (linux)
  - User Activity (linux)
  - OS
  - Hardware
  - Software
  - Accounts/Users
  - Network Information

Shared / Mapped Drives

USB Devices

Network Shares

Advanced Windows Registry

time zone, hardware – etc.

Other AutoRuns

can see UNC paths device

connectivity history – USB with drive

Modules– Page 3

- IM Parser – Search for IM artifacts – buddy-lists and messages
- File Carver – Search evidence for file fragments
  - Automatically checks file headers for file length – more accurate carved files
  - Search all or selected files, file slack, and/or unallocated for deleted or embedded files by header
  - Over 300 file types supported for carving HTML and webmail by keywords
  - Uses GDI libraries to accurately carve images. The libraries identify the actual length of the file to be carved

Modules– Page 4

- File-Carver
  - GDI includes:
    - .jpeg, .ico, .gif, .png
  - Carving Process
    - Identified by signatures
    - When a file is established by header it tries to find the size
    - If GDI indicates a size then that size is carved
    - If the GDI does not then it utilized the standard method

Modules– Page 5

- File-Carver
  - File Naming – once carved the files are named:
    - <sn> : an incrementing serial number
    - <fn> : name of the entry (filename)
    - <fo> : file offset where the header was found
    - <ps> : physical sector of the file offset
    - <po> : offset from beginning of physical sector corresponding to file offset
    - <ext> : first file extension associated with the found file header bytes

Modules– Page 6

- File-Carver
  - 3 Options in the file carver
    - All, Optimized or Standard
    - Optimized includes

      Compound document files, Outlook personal folder, Audio video interleave, flash video, enhanced metafile graphic and bitmap

Modules– Page 7

- Windows Event Log Parser – locate and parse event logs
    - EVT and EVTX along with corrupt or partial .log files
- Windows Artifact Parser –
    - Link files, recycle bin files, MFT
- Unix Login – search for specific events
- Linux Syslog Parser –
- OSX Artifact Parser – Plist artifacts, log giles, text files
- Snapshot – live preview only – open ports logged on users etc.

Processor– Page 1

- Once finished configuring the Processor Options:
  - OK – Time required to complete depends on evidence size and processing options selected – RAM, disk I/O and processing power
    - You can still browse, examine and bookmark evidence while this runs
- Evidence Processor Performance Scaling
  - Processor is optimized for the hardware and number of cores that the examiner machine has to be more efficient.

Processor– Page 2

- Processing a Live Device
  - You can process a live device
  - All options are available except Index Text
    - Home
    - Add Evidence..Local Device..Add Network Preview or Crossover Preview
      - Select appropriate checkboxes of the devices you want to add then finish
      - In the Evidence tab – click Process Evidence
      - Under process select appropriate checkboxes
      - Review modify options
      - OK

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.