Advanced Computer Forensics

EnCE EnCase Forensics: The official EnCase Certified Examiner Study Guide

Chapter 6

EnCase Environment

Home Screen

- Initial Screen Where You Can Access:
  - Recent Cases
  - Case Files
    - New Case
    - Open a Case
  - Tools
    - Options
  - Help
    - Help
    - Paths
    - About

Home Screen Within a Case

- Evidence
  - Add Evidence
  - Process Evidence
- Search
  - Search
  - Results
- Browse
  - Evidence
  - Records
- Report
  - Reports
  - Bookmarks
  - Report Templates

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 one evidence file
    - Select the items you want to see with a blue check
    - See the Load Selected Evidence on the toolbar
    - Open

EnCase Layout

- Evidence Layout
  - Tee-Table
    - 3 Windows
      - Tree Pane – Left pane shows evidence
      - Table Pane – Right pane shows items within the evidence selected
      - View Pane – Bottom pane shows the data of the item selected in the Table Pane
  - Tabs
    - Within each window there are tabs
      - These tabs change the view within the particular pane the tab is chosen in
      - Presents selected information in different ways and sometimes even different information regarding the same item
  - Other Views
    - Bookmark, Secure Storage, Records, etc.
      - Work with each to become familiar with what each shows you

Creating a Case

- Before Getting to the Tree-Table View
  - Create a Case
    - Home Screen – New Case
    - Case ->New Case from the toolbar
  - Case Options Dialog Box
    - 4 Sections
      - Templates Area – Default templates and custom options
      - Case Name
      - Case Path
      - Case Information Area

Templates - 1

- .Case Template
  - Stored in Users\<username>\Documents\EnCase\Templates Folder
  - Templates are predefined and ship with EnCase – Users can make custom templates if they choose
  - Templates contain unique information for:
    - Case Information – default values
    - Bookmark Folders and Notes – you can add to these within the case
    - Tag Names – can be altered within the case
    - Report Template – you can manipulate this as well
    - User-Defined Report Styles
  - Creating a Custom Template
    - Create using a template then customize items and then Case drop-down menu on the toolbar and Save as Templatge
    - Choose a name and path – include hash library paths, or bookmark notes to this template

Templates - 2

- Name
  - Descriptive case name (could include case # etc.)
- Full Case Path
  - Takes info. From Base Case Folder Path and Name
- Base Case Folder
  - Default is stored in Documents or My Documents Folder
  - Better location would be on a different drive than your system drive
    - Store evidence and evidence cache with your case file as well
- Primary Evidence Cache
  - Stores metadata about evidence files
    - Each piece of evidence has a GUID and has a folder assigned to it by the GUID which contains a cache of that evidence
    - Evidence Processor also stores data within this folder
    - Increases performance and scalability when you have large evidence sets
    - You can assign this path to the Base Case Folder

Templates - 3

- Secondary Evidence Cache
  - For previously created caches
    - You can store them in this location and EnCase will only read them from this location
    - New Caches will be written to the Primary Evidence Cache
  - Case Info.
    - Examiner
    - Case #
    - Description
      - Custom information in this area may save you time as things like “examiner name” will not change from case to case

File Management - 1

- Extremely Important Skill
  - Case File Organization and Management
    - Best Practice
      - Distinctive Folder Naming Conventions
        - Separate drive or network drive – separate from OS in case there is an issue – Network allows for multiple examiners to have access to the same evidence files
        - Examiners can access the same files at the same time and work on different facets of the same case
      - EnCase encapsulates the image of the device into an evidence file with multiple redundant integrity checks. Cross-contamination of image files is NOT an issue as it was in the past
    - Examiners can open multiple cases ast once and conduct analysis on each concurrently
    - Cases are sometimes started as separate cases and are then found to be related
      - This allows examiners to work on both separately, but together at the same time
    - Multitasking by an examiner – allowing the examiner to work on two totally separate cases concurrently
      - Manually working on one while the other is completing an automated process

File Management - 2

- Case File Organization and Management
  - Best Practice
    - Distinctive Folder Naming Conventions
      - Placed within the “cases folder”
      - EnCase creates Email, Export, Tags and Temp folders
      - You can place Evidence and Evidence Cache in this folder as well. You can place them anywhere you chooses
      - Performance in increased by keeping them all on one system drive
      - Continually save using Ctrl S or the drop down – Save All is a good idea
    - Default backup - \Users\<username>\Documents\EnCase\Cases\Backup – Same drive – should change this to a different drive from your “working” case drive. You can dictate how many backups and how frequently they backup

File Management - 3

- Naming Conventions

[Instructor Selected Image]

Adding Evidence - 1

Add a Local Device

- Blue check the local device (usually drive 0)
- Blue check the drive and select Load Selected Evidence from the Evidence tab or double-click
- You should now be able to preview your drive / evidence
- To Acquire – select your drive in the Table Pane – Click the acquisition icon and drop-down on the Evidence tabs' toolbar / acquire
- From the location Tab – Under Name name the evidence – this is automatically inserted in the filename portion of the path which you can change
- Format Tab – default format is ex01, compression enabled, MD5 hash default, file segment is 2048MB, no password / encryption is enabled – You should review the options for these
- Advanced Tab – Block size is 64 sectors, Error granularity is standard (same size as block or exhaustive=1sector), Use default unless you have a reason. Start and stop sector defining the range of acquisition, threads – reader and worker
- Click cancel and back to your case

Adding Evidence - 2

- Add an Evidence File
  - Navigate to the Evidenced Folder of the case and select
- Add Raw Image
  - Select the Image
- Acquire a SmartPhone
  - Tools ->FastBloc SE
  - Connect the device utilizing USB – EnCase will impose a write block on it and notifies you
  - Open or Create a New Case – Add Evidence then Add Local Device, accept defaults and next
    - A yes in the write blocked column and a green box around it indicate successful write blocking
  - Select the device and click finish
  - Double-click – then select it to preview and then acquire – can also parse and acquire
- Add Crossover Preview
  - Attach to another computer via crossover – still need to write block using FastBlock SE or a hardware write protector
- Once Evidence is Added – Save and Save often – Utilize SAVE ALL!!

Tree Pane Navigation - 1

Device and Icons

- A LIVE device is indicated with a blue triangle in the bottom right corner
- A RED triangle indicates a live device over the network using Enterprise FIM
- An evidence file has what looks like a magnifying glass – or finder icon
- 2 Gold Cylinders with black arrow indicates a RAID device
- Right clicking on a device or folder level you can expand or contract all by selecting it
- Square – Blue Check – Selecting for an action or processing (blue=DO) Selects all child objects as well
- Homeplate – Set Include Folders trigger – Green when selected (green=screen) – All files and folders at that level and below are shown in the table pane
  - Holding CTL will allow you to select multiple Set Include Folders to compare different items side by side
- Dixon box located on the Table tab indicates the number of items you have selected out of the total number of items in the case

Tree Pane Navigation - 2

Split Mode – Tree Pane

- Table
  - No Tree view just Table
- Tree-Table (Default)
  - 3 Sections – Tree Pane, Table Pane, View Pane
- Traeble
  - Only have Table Pane on top and View Pane on bottom – the tree is brought into the name column of the table
- Tree View
  - NO Table – Just the Tree Pane and the View Pane – Tree Pane on the left and View on the right
- Right Side Menu
  - Collection of menu items regarding options for currently selected items (sort of like a right-click)

Table Pane Navigation - 3

Table View

- Sort
  - Can applu up to 6 sorts – usually 3 is the common max
  - Place your cursor in the column then choose the sort option (A to Z icon)
  - Double-click the header – Double-click again will reverse the sort order
  - Multiple column sorts – hold the shift key and double-click the next column to sort by
  - Place your cursor in a second column and utilize the sort order again
  - Remove a sort – double-click the header again
  - Reset all sorts – place cursor in any column and choose remove sort in the sort menu
  - Sort on blue checked by using the unnamed column header above the blue check boxed. Sorts between those selected and those not selected
- Hide
  - Showing and hiding columns – open it using the Table right-side menu -> columns ->show columns
  - Columns hidden or deactivated will not have a check – remove or add to show / hide the columns
  - Reset returns all columns to the EnCase default settings
- Lock
  - Usually the name column – keeps the column where you put it – usually to always be visible (indicated by a dark line to the right of the locked columns)
  - Right side menu – column – unblock – repeat select the column
- Move
  - You can click and drag the column header to a new location – you can replace a locked column – drag a no on on to it
  - Column Names and Descriptions (pages: 271-271) – It is important to know what is column indicates

Gallery View

Tab within the Table Pane

- Gallery
  - View images in the case at any level you determine
  - Use the Set Include Folders button to direct the content of the Table Pane
  - Files are based solely on extension until the case/file has been processed. After that it is a signature analysis that will dictate what constitutes a picture
    - Programs such as Firefox change extensions and other items might be partial downloads etc. These will only be seen after a signature analysis has been completed
    - Users may attempt to alter extensions to hide information
  - Select – bookmark – copy – unerase
  - Right-clicking will allow you to change the thumbnail images – fewer columns or more columns – fewer rows or more rows
  - Corrupt images are cached so as not to “crash” EnCase
    - .art – AOL picture conversions
  - Tools ->Options ->Global Menu

Timeline View

Tab within the Table Pane

- Timeline
  - Review the chronological activity in a graphical manner
  - All dates and times are enabled by default
  - Menu on the Timeline tab toolbar Date and Type where you can enable or diable timestamps
  - Use the green Set Include Folders trigger to select the level of the Table Pane content
  - One interesting view is looking at deleted files only
    - Go to the users folder in the recycle bin and check out the timeline view. This could indicate that someone knew/heard they were going to be investigated
    - Selecting a file within this view will bring the file into the View Pane and the location is highlighted in the tree. Full path is in the GPS at the bottom
    - You can increase or decrease the resolutions – use the plus and minus on the number pad – double click – click higher or lower on the timeline tab toolbar
  - Can specify a date range for the Timeline view
  - No reporting or printing for the Timeline View – take screenshots – They can be included in PPT presentations or put in the final report via HTML or print based
  - Options menu on the Timeline toolbar will allow you to select date ranges and color schemes

Disk View

Must choose AFTER selecting your device

- Select the entry
- Select the device in Table View (do NOT blue check) only highlight
- Device ->Disk View
  - Shows sectors by blocks by default
  - If you would like to see clusters check View Clusters box on the toolbar
    - You won't see sectors outside of the partition because they aren't clusters. Remember clusters are a logical group of sectors
  - Blocks are color coded by their function
    - Blue – Allocated
    - Gray with a raised bump – Unallocated
  - Auto Extents
    - When you select a sector all seekers contained within that program etc. become highlighted by default – you can toggle this on and off on the toolbar
  - Can go to a sector by right-clicking and entering it or right click GoTO
  - Adding and Deleting Partitions
    - Must find the start of the partition – then recover

View Pane Navigation - 1

Multitude of options

- Text View
- Hex View
- Picture View
- Report View
- Doc View
- Transcript View
- File Extents View
- Permissions View
- Decode View
- Field View
- Lock Option
- Dixon Box
- Navigation Data (GPS)

View Pane Navigation - 2

- Text View
  - Content is driven by the selection in the Table Pane
  - Output determined by the Text Style – located on the Text Tab toolbar
    - Usually just leave Wester European Windows and adjust the wrap length settings under Options when needed
- Hex View
  - Shows each byte in hexadecimal notation and Text on the right
    - Pure raw data
    - Select data – bookmark, export, copy/paste, etc. (practice this)
      - View as text, integer, date/time, partition tables, DOS entries, etc.
- Picture View
  - If EnCase detects it is a picture it will try to view it in this view

View Pane Navigation - 3

- Report View
  - Detailed report of the properties of the object selected in the Table Pane
  - See all attributes and properties including permissions
  - Can right-click and export sa a web page or document – Quick detailed information regarding a file
- Doc View
  - Many common document formats (Word, Excel, PDF, etc) can be viewed the way they would look in their native application
    - Printing and bookmarking are available in this view
- Transcript View
  - Suppresses file noise like metadata and formatting
    - Usually text within here is indexed by the indexing engine. Any search hit or bookmark will appear in both the Doc and Transcript views

View Pane Navigation - 4

- File Extents View
  - Details about the cluster runs for a file
- Permissions View
  - Detailed security permissions for a file
    - Owner, SID, read, write, execute, etc.
- Decode View
  - Locate data in Text or Hex – select it then click Decode View tab and select the type you want to apply
    - Decoding a partition table in the MBR – located at sector 0 – Place cursor at offset 446-509 (64 bytes) – select the info then Decode view Windows -> Partition Entry – populates information

View Pane Navigation - 5

- Field View
  - Allows you to display metadata quickly when looking at a file
  - Same fields as in Table view, but displayed in the bottom pane
- Lock Option
  - Locking a view type for the view pane – EnCase will force an item to be viewed with the locked options and not try to view it in a default
    - Toggle – for instance wanting to see all data in hex (even Doc files or images)
- Dixon Box
  - Indicates the number of selected items in relation to the total number of items in the case
    - Clicking the box selects all objects (if non are already selected)
    - Clicking the box deselects currently selected items (if some are selected)
    - Keep an eye on the Dixon box before choosing an action – This could save a lot of time as running actions on all items versus a few can be time consuming
  - Double click the bottom right progress bar to abort a current process if you have too many items selected

View Pane Navigation - 6

- Dixon Box
  - Doesn't show you which files just how many
    - Two quick methods of seeing your selections
    - Green plate the Set Include Trigger at the case level and sort by the nameless column in the Table Pane
    - Double-click the nameless column above the check boxes and the selected files should come to the top
- Navigation Data (GPS)
  - Precise location in the evidence file
    - Real-time information – changes whenever you change data being viewed

Navigation Data (GPS)

[Instructor Selected Image]

Other Views and Tools - 1

- Conditions and Filters
  - Located on the toolbars where applicable
    - Seen on the Results View
    - Will have to open to see the results of your filters or conditions
- EnScript
  - Located on the Application Toolbar
    - Can run it from the drop-down menu or create/edit your own
- Text Styles
  - Located on the toolbars where applicable
    - Remember we can use the Options and Codepage menus as well
- Adjusting Panes
  - Select the vertical and horizontal lines separating the different view panes – click and drag to your viewing preferences
  - Multiple monitor environments can greatly improve the efficiency and effectiveness.
  - You can unlock or detach the view pane to create a customized screen configuration (click the undock located by the lock box in the View Pane)
  - Clicking the red Close icon in the upper right will return the View Pane to the original location

Other Views and Tools - 2

- Other Views
  - More meaningful after having processed a case
    - Records View etc.
- Global Views and Settings
  - File Types View – View Menu on the application toolbar
    - 800 different entries or file types defined in the table
    - Signature, file type and viewers are in one table
    - Allows you to view, delete, modify, or create new file type entries
    - These options are located on the toolbar
    - These are updated frequently by the Guidance Software team, but can't include them all
    - User defined file types are stored in the user's AppData area and not in global settings as updates would overwrite what users have defined
  - What happens when I double click a file
    - EnCase looks to this filetype.ini location – if the file is set for internal viewing EnCase will tell you. If it is set for Windows to handle the viewing it will have Windows as the file viewer. In that case EnCase creates a temporary file in the temporary folder of the case. If it is set for an installed viewer – one you configured then that viewer will be listed as the viewer – EnCase will create a temporary file again
  - External Viewers are Sometimes Necessary
    - Right click the file in Table View and select Open With Submenu – you can add one, select File Viewers, and you will see the Edit File Viewers dialog box – Click New and name the viewer and provide a path – Next time this viewer should be listed as an option

Other Views and Tools - 3

- Tools ->Options
  - Global View – Changes all EnCase
  - Backup locations, Boolean values, auto save, backup frequency and files, Recycle Bin, picture options
  - Date Formats
  - Colors – Default colors for search hits etc. No need to change everything, but if you choose to other color combinations may work better for you
  - NAS – Used in EnCase Enterprise environment – This is your path to your licensing info.
  - Debug Tab – System cache settings that can be adjusted – Usually leave the defaults – Should only be changed by EnCase Technical Support

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.