Chapter 5

EnCase Concepts

Within EnCase

- You can:
  - Acquire forensically sound data
  - Search and find data even though a suspect may have tried to hide it or deleted it
  - Transfer/share case analytics with others
  - Produce and manipulate reports
  - Analyze many different file formats and devices
  - Manage large amounts of data

EnCase Evidence File

- Evidence extension
  - .E01 – legacy (v6)
  - .Ex01 – current (v7)
    - Stores data differently than v6
    - Specs on Guidance Software site
- Forensically Sound
  - MD5 and SHA-1 – physical drive of volume
    - Files as well
    - One or the other, both or none
  - CRC – after every block

EnCase Files - 1

- Header
  - Entered by the investigator
    - Administrative information
    - Segment size
    - Number of segments
    - Compressed or not, name, notes and passwords
    - One header per evidence file
    - Automatically compressed even if the evidence is not

EnCase Files - 2

- CRC
  - Works like MD5 and SHA-1
    - Takes less processing power so it is quicker, but there are many less options before a “collision”
    - Most HDs have a CRC per sector. If they don’t match then there is an error (disk error)
    - CRC is present after each data block in EnCase if not compressed
      - If compressed the validation is within the compression/decompression process

EnCase Files - 3

- Evidence File Format
  - Exact bit-for-bit copy
  - Information entered by the user is in the header
  - Every byte of each data is verified with CRC
    - Default size of data block is 64 sectors
  - MD5 calculated by default
    - Acquisition hash – physical drive or logical vol.
  - Once created the file is marked read-only
  - SHA-1 option – acquisition SHA-1
    - Validation of the original written to the last segment of the evidence file
    - Provides a second level of verification

EnCase

- Automatically
  - Verifies the CRC when evidence is added to a case
  - Re-computes the hash value for the data
  - Acquisition hash values stored in the evidence file and verification hashes which is computed when a file is added to a case
  - Appears in the report
  - Verification at any time
    - Highlight drive or volume – Device->Hash

Ex01 and Lx01 Format

- Reconstructed how data is stored
  - EV2 Header
    - Compression
    - GUID
    - Signature
  - Data
    - Sector / entry / device info
  - Link Record
    - Size of data area
    - Hash value
    - Position of next link record
    - Encryption / Compression flags
    - Type of data
    - CRC

Case File

- Text file with information specific to a case
  - Pointers to evidence files or previewed devices
  - Searches, keywords, hash and signature analysis results
  - Case files created when EnCase is run
  - Cannot be simultaneously accessed by more than one examiner
  - Default location User Data – should create unique case related folders for all of the pertinent files created for a case.

Backup

- Scheduled
- Custom
- On Demand
- C:\Users\<username>\Documents\EnCase\CaseBackup (location- can be customized)
  - BaseBackupDatabse.sqlite
  - Case file, Primary EvidenceCache, Secondary EvidenceCache if used, dates/times/sizes of all files and everything in the case folder except:
    - Export folder
    - Temp folder
    - Evidence files

Configuration Files - 1

- Default installation settings
- Specific user settings
- Global user settings
  - Older version made the user export these
  - New version separates them from the updatable area
  - Saved per user – AppData area for that particular user

Configuration Files - 2

- Location
  - Program Files – EnCase Installation
    - C:\Program Files\EnCase7\Config
      - Created by the installer and are NOT modified
        - Remain the same forever
  - User Data
    - C:\Users|<username>\Documents\EnCase
      - User-created files not EnCase version or install specific
      - Backup user data (CaseBackup files, user keys, user created conditions, filters, templates, index, raw searches)
  - User Application Data
    - C:\Users|<username>\AppData\Roamine\EnCase\EnCase7-1
      - Configuration and user temp files that pertain to a specific user installation folder of EnCase
        - Local.ini, viewers.ini, modification to filetypes.ini

Configuration Files - 3

- Location
  - Global Application Data
    - C:\ProgramData\EnCase
      - Contains the files that are for the configuration of EnCase regardless of user
        - NAS
        - Report Template Images
        - Noise Files (for indexing)
  - Shared Files Folder
    - Pointed to a folder where shared files are kept
      - EnScript modules
      - Searches
      - Conditions
      - File types, text styles and keys

Device/Evidence Cache

- Stares the results of the EnCase Evidence Processor
  - Performs processes
    - Signature analysis
    - Hash analysis
    - Indexing
    - Stores Cache based on GUID
      - GUID associated with each device and/or evidence with the case
      - Default C:\Users\<username>\Documents\EnCase\EvidenceCache\<GUID of device>
      - Created when evidence is added

Evidence Cache Folder

- Contains – results for a device
  - Cache
  - Index
  - Evidence Processor
    - \Users\<username>\Documents\EnCase\Evidence Cache\<Hash> (win7 up)
    - \Documents and Settings\<username>\My Documents\EnCase\Evidence Cache\<Hash>
  - Hashes
    - CRC – 32
    - MD5 – 128
    - SHA-1 - 160

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.