EnCase® Forensic Concepts

EnCase Forensic

EnCase Forensic (EnCase) provides examiners/investigators with a single tool for conducting large-scale and complex examinations/investigations from beginning to end. It features superior analytics, enhanced e-mail/Internet support, and a powerful scripting engine.

With EnCase you can:

- Acquire data in a forensically sound manner using software with an unparalleled record in courts worldwide
- Investigate and analyze data from multiple platforms—Windows, Linux, AIX, OS X, Solaris, and more—using a single tool
- Find information despite efforts to hide, cloak, or delete
- Easily manage large volumes of computer evidence, viewing all relevant files, including deleted files, file slack, and unallocated space
- Transfer evidence files (files representing data on media to be examined) directly to colleagues, attorneys, or supervisors as necessary
- Review options that allow non-technical individuals to review evidence with ease
- Use reporting options for quick report preparation

Forensically Sound Acquisitions and Examinations

EnCase Forensic produces an exact binary duplicate of the original drive or media, then verifies it by generating MD5 and SHA-1 hash values for related image files and assigning validation values to the data. These checks and balances reveal any inconsistencies with acquired data.

When using EnCase to examine an evidence file, it is important to understand that EnCase is incapable of changing data on the evidence file.

EnCase® Evidence File

The central component of the EnCase® methodology is the evidence file. The evidence file may consist of multiple segments, with the extension documenting the order of the segments. EnCase® v7 has two different formats for the evidence file: the Legacy format (.E01) and the Current format (Ex01). The Legacy format may be read by any version of EnCase. EnCase v7 as well as EnCase version 6.19 read the unencrypted Current evidence file format. Regardless of format, an evidence file can be moved without altering the evidence file verification. If an evidence file is moved and the case file is reopened, EnCase v7 will request the new location of the evidence file.

EnCase® Legacy (E01) Evidence File

The uncompressed evidence file contains three basic components (header, checksum, and data blocks) that work together to provide a secure and self-checking description of the state of a computer disk at the time of analysis. If the evidence file is compressed, the compression and decompression algorithms include validation of the data blocks.

Header

Among other things, the header contains administrative information entered by the examiner during the creation of the evidence file. Elements such as segment size, number of segments, compression (or not), name, notes, and password are stored in the header. The case information cannot be changed without causing the verification process to report an error. There is only one header per evidence file. The header is automatically compressed (regardless if the examiner selects compression as an option for the evidence file creation), and the compression algorithm validates that the header information has not changed.

Cyclical Redundancy Check (CRC)

The Cyclical Redundancy Check (CRC) is a variation of the checksum and works in much the same way. The advantage of the CRC is that it's order-sensitive. The string "1234" and "4321" will produce the same checksum, but not the same CRC. Most hard drives store one CRC for every sector. When a read error is generated from a disk, this usually means that the CRC value of the sector on the disk does not match the value that is recomputed by the drive hardware after the sector is read. If this happens a low-level, disk-read error occurs. The CRC is present after each data block if the evidence file is not compressed.

Evidence File Format

Each file contains an exact, bit-stream image copy of the target media. When a file is created, the user provides information relevant to the investigation, which is stored in the header. Every byte of each data block within the file is verified using a 32-bit CRC (either through the compression algorithm or a CRC value), making it extremely difficult if not impossible to tamper with the evidence once it has been acquired. Note that if compression was activated during the acquisition of media, segregated CRC values will not be stored following the data blocks. The validation will occur through the compression/decompression algorithm.

The default size of a data block is 64 sectors. EnCase will identify the data block by the range of sectors if an error occurs. The odds of two data blocks that contain different data producing the same CRC are roughly one-in-four billion. This allows examiners, investigators, and attorneys to confidently stand by the evidence in court.

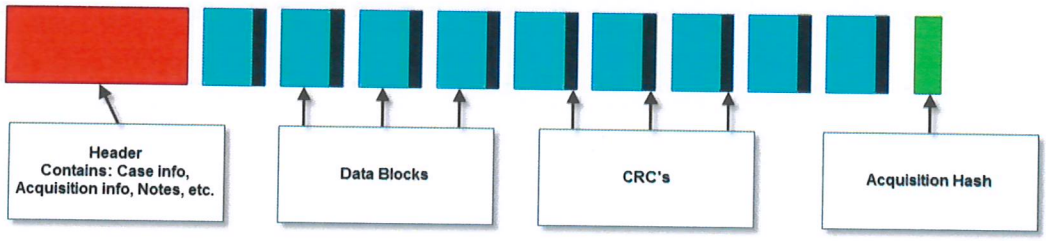

Figure 4-1 Parts of a complete uncompressed EnCase evidence file with one segment

By default EnCase calculates an MD5 hash (Message Digest 5) when it acquires a physical drive or logical volume. This 128-bit hash value, called the "Acquisition Hash," represents a validation of the original media and is written to the end of the last segment of the evidence file. This validation value becomes part of the documentation of the evidence. The MD5 hash value is optional and can be deselected during the acquisition process. Though the MD5 hash value is optional and not mandatory, it is highly recommended that the default selection to generate a hash value be selected to give the examiner the ability to verify that both the imaged media and the evidence file contain the exact same data. Once the evidence file is created, it is marked as a read-only file. Based upon its read-only status and CRCs, data cannot be written to the evidence file after acquisition has completed.

EnCase also provides the ability to calculate an SHA-1 hash (Secure Hash Algorithm) when it acquires a physical drive or logical volume. This 160-bit hash value, called the "Acquisition SHA-1," represents a validation of the original media and is written to the end of the last segment of the evidence file. This validation value becomes part of the documentation of the evidence. Though the SHA-1 hash value is optional and not mandatory, it is recommended that the selection to generate a SHA-1 hash value be selected to give the examiner the ability to verify that both the imaged media and the evidence file contain the exact same data. This is a second level of verification.

The examiner may choose to generate an Acquisition Hash, an Acquisition SHA-1 hash, both values, or neither value. ***The latter is not recommended.***

When an evidence file is added to a case, EnCase automatically verifies the CRC values (by using the values written into the evidence file or the values generated during decompression of the compressed data) and recomputes the hash value(s) for the evidence data within the evidence file. The Acquisition hash value(s), which is stored in the evidence file, and the Verification hash value(s), which is computed when the evidence file is added to a case, should appear in the report immediately confirming that the evidence file has not changed since acquisition.

At any time while using EnCase within the Viewing (Entry) view, highlight a drive/volume, select **Device→Hash** to recompute the hash value of the drive or volume. The verification process can only be successfully completed after both the MD5/SHA-1 acquisition and verification hash values match and no CRC errors are reported.

Compression

Compression technology allows EnCase to store the data from a large disk in a relatively small file. EnCase uses an industry-standard compression algorithm (Zlib) to achieve an average size reduction of 50%. If most of the disk contains text data, the compression ratio may be much higher. However if the majority of the media contains compressed data, such as JPG files, video data, and similar types of files, the compression realized may be minimal. Compressed evidence files take longer to generate due to the additional processing time required to compress the information. Compression ***never*** has any effect on the final evidence and compressed blocks are checked for validity in the same way as uncompressed ones. If a device is acquired with and without compression to two different evidence files, the resulting Acquisition MD5/SHA-1 hash values stored at the end of both evidence files will be the same. The hash computation during acquisition occurs prior to compression of the data. The hash value stored within the evidence file represents a hash of the original media imaged.

EnCase® Evidence .Ex01 and .Lx01 v2

EnCase v7 has a new evidence file (.Ex01) format, which restructured the way data is stored.

The new format allows for encryption and supports a new compression algorithm (bzip2). The improved format includes redundant documentation of administrative data.

The technical specifications of this format may be found on the Guidance Software Customer Portal:

https://support.guidancesoftware.com/forum/downloads.php?do=file&id=1185

Note that accessing this data requires a username and password to access the Customer Portal.

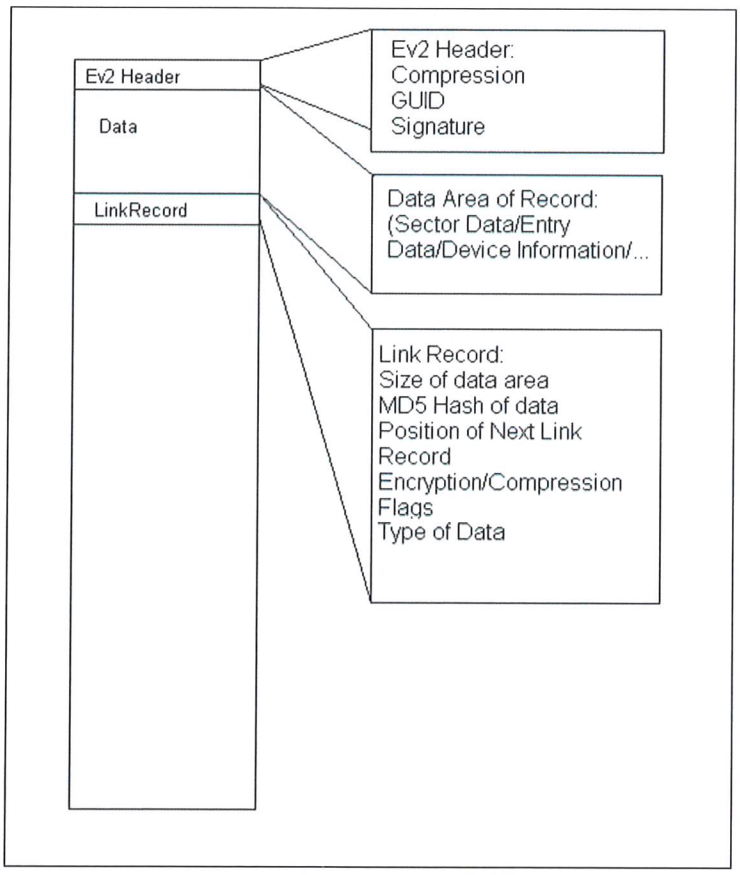

Figure 4-2 New EnCase evidence file format

Case File

The case file is a text file that contains information specific to one case. The case file contains pointers to any number of evidence files or previewed devices, files representing searches and keywords, hash and signature analysis results, etc.

Before media can be previewed or evidence files analyzed, a case file must be created when the user runs EnCase. The case file cannot be simultaneously accessed by more than one examiner at a time.

In EnCase v7, the default location for saving the case files is the User Data folder. It is suggested that the case file be saved into a unique folder structure.

Verifying an Evidence File Automatically

The first time an evidence file is added to a case, EnCase will begin to verify the integrity of the entire disk image in the background. This is usually quite fast for small (thumb drive) evidence files, but can take longer for hard-disk evidence files. The examiner may conduct his examination while the verification occurs.

Case Backup File

The backup file is a manual or auto-saved backup of the open case file. The backup files are saved (by default) within the user folder structure `C:\Users\<Username>\My Documents\EnCase\CaseBackup`. The individual file(s) related to the case that was changed may be located within the CaseRevisionFiles folder. These backed up files have a "number" and an underscore prepended to the filename, and the extension CaseRevision added as the last extension. The root of the CaseBackup folder contains the CaseBackupDatabase.sqlite which houses the administrative information related to the backup. .

EnCase® Configuration Files

Configuration files may be stored in several different folders. These configuration files represent default settings within EnCase that are the default installation settings, specific user settings, or global user settings. In the past, when configuration files were changed, the user had to export the data from the configuration file to ensure it was not lost and import the data within the new configuration file for the newer version of EnCase. Now changes to configuration files are separated from the original configuration file. EnCase integrates these settings in a manner invisible to the user.

Configuration Files Locations

The following location list defines the areas used by EnCase and gives a brief description of which types of files should reside in which location:

- **Program Files, EnCase installation Folder**
  - This folder contains files that are created by the installer and are unmodified by the application.
- **User Data**
  (`C:\Users\<username>\My Documents\EnCase`)
  - This folder is for user-created files that are not necessarily EnCase-version or installation specific, such as CaseBackup files, user created conditions, and files representing created index or raw searches.
- **User Application Data**
  (`C:\Users\<username>\AppData\Roaming\EnCase\EnCase7-1`)
  - This folder is for configuration files and user temp files that pertain to a specific user and installation folder of EnCase, such as viewers.ini and modifications to filetypes.ini.
- **Global Application Data**
  (`C:\ProgramData\EnCase\EnCase7-1`)
  - This folder contains files that are for the configuration of EnCase regardless of the user, such as NAS settings and temporary files (Cache) from evidence processor operations, the noise file for the indexing process, and images used within report templates.
- **Shared Files Folder**
  - This folder can be pointed to a folder where users keep shared files (EnScript modules, searches, conditions, file types, text styles, and keys).

Device or Evidence Cache

The Device or Evidence Cache contains much of the data viewed through the case file. Its primary purpose is to store the results of the EnCase® Evidence Processor, which is responsible for performing processes, including but not limited to, Signature Analysis, Hash Analysis, and Indexing the case. It stores this cache based on a GUID (Globally Unique Identifier) associated with each device and/or evidence file associated with the case. The Device Cache and Evidence Processor will be discussed later.