

***Computer Forensics:
Using EnCase[®] for Forensic Investigations***

Allen C. Johnston
Mississippi State University
acj4@msstate.edu

Abstract

Computer forensics refers to the examination of computer and communication devices for the purposes of preserving, identifying, verifying, extracting, and documenting electronic evidence. Often described as a two-stage process (Volonino, 2003), computer forensics involves the analysis of computer hard disks through sophisticated procedures and software tools. The first stage involves the discovery, recovery, preservation and control of electronic data, while the second stage involves the analysis, verification and presentation of electronic evidence (e-evidence) for investigative purposes.

The purpose of this paper is to describe the steps involved in a basic forensic analysis of a crime suspect's computer using a Windows[®] based forensic data acquisition and analysis program. Through the techniques specific to EnCase Forensic Edition Version 4, this paper explains the steps involved in the acquisition, recovery and analysis of latent data. This type of data is also referred to as ambient data and typically exists unbeknownst to most computer users. The tools and techniques described in this case are specially designed to deal with this type of data that is located in unconventional computer storage areas and formats.

Acquisition of Evidence

The first step in this investigative process is to acquire the evidence. The goal is to obtain an exact replica of the data without compromising its integrity; however, because computer systems may contain volatile data in RAM, the acquisition process is a dynamic one. For the purposes of this paper, we will assume that we are only interested in files that are known to have been created and stored on the crime suspect's hard drive. In this scenario it is permissible to shutdown the suspect's computer and boot it with a DOS boot utility. EnCase for DOS allows for a forensically sound acquisition of data without running the risk of altering access dates and time stamps. EnCase for DOS write blocks the suspect's hard drive during acquisition, thus preventing accidental data modifications. The procedure used in this investigation was as follows: (1) the crime suspect's hard drive was connected to the storage computer via IDE ribbon cable; (2) the storage computer was booted with an EnCase boot disk; (3) EnCase for DOS was executed from the DOS prompt; (4) the storage computer's hard disk was unlocked to allow the suspect's hard drive image to be written to it; (5) the suspect's hard drive was acquired and saved to a predetermined location on the storage computer's hard disk.

Evidence Authentication

The second step in this investigative process is to authenticate the evidence. The goal is to verify the integrity of the e-evidence. In other words, this procedure is necessary to prove that the data is exactly the same as the original and that the time and date stamps of the acquired data match that of the original. A cryptographic technique called a hash is used as “a sort of electronic fingerprint for an individual file or even an entire floppy or hard drive.” (kruse, p. 13) The EnCase for DOS utility provides the option of creating an MD5 hash value of the evidence at the time of acquisition. This hash value is of the newly created drive image. For evidentiary purposes, it is critically important that this hash value exists. Without it, there is no proof that the acquired image is an exact match of the original hard drive. During the analysis phase of the investigation, EnCase allows the investigator to create a hash value for any file. Since the hash value is determined by the file’s contents, any change to the file or timestamp results in a mismatch with any future MD5 hash value. Mismatched hash values strongly imply that the file has been modified either intentionally or unintentionally. It is also important to note that a hash value cannot be generated on a partial file; therefore, if a deleted file has been partially overwritten, an MD5 hash value for that incomplete file is not available.

Data Analysis

The third step in this investigative process is analysis of the data. At this point, we are working solely with the acquired image. EnCase allows for the inspection of data located in various places on the hard disk image, such as unallocated space and slack space. Through the use of multiple file viewers, it is possible to quickly search and identify important data at various stages of existence. EnCase clearly identifies a file’s status and provides a mechanism for recovery from deletion. In some instances, the files have been deleted, yet their filename is intact and the starting cluster of the data is still available. These files are easily recovered. Additionally, EnCase can recover remnants of files that have been deleted and partially overwritten. In either case, EnCase provides critical information about the file, such as date created, last accessed and last written, and the full path. As should be expected, the more information the investigator can obtain, the better prepared he or she will be to effectively and efficiently present the findings as e evidence.

Conclusion

This paper presents a simple approach to a computer forensic investigation. These types of investigations are becoming more frequent and touch on many different domains. For example, we now see computer forensic techniques being employed for cases involving drug crimes as well as illegal accounting methods. While there are numerous tools available for this kind of analysis, the circumstances of a particular case will dictate whether or not the EnCase suite of tools can be used affectively. Throughout the investigative process, it is critically important that proper documentation of the entire process of the evidence is maintained. There are numerous requirements to the documentation process that are beyond the scope of this paper, and should be reviewed

carefully prior to any computer forensic investigation. Hopefully, this paper has created an appreciation for a few of the tools available to computer forensic specialists in their ongoing investigative pursuits.

References

Volonino, L. (2003) Electronic Evidence and Computer Forensics. *Communications of the Association for Information Systems*, 12, 27, 457-468.

Warren G. Kruse, Warren G. & Heiser, Jay G., 2003. *Computer Forensics: Incident Response Essentials*, Addison-Wesley.