Overview of “Computer Forensics”

Don Mason, Associate Director
National Center for Justice and the Rule of Law
University of Mississippi School of Law

[These materials are based on §§4.3.1-4.3.3 in the National Center for Justice and the Rule of Law publication, Combating Cyber Crime: Essential Tools and Effective Organizational Structures, A Guide for Policy Makers and Managers (2007).]

Copyright © 2010 National Center for Justice and the Rule of Law – All Rights Reserved

§4.3.1. COMPUTER FORENSICS

Forensics is the application of scientific techniques of investigation to the problem of finding, preserving, and exploiting evidence to establish an evidentiary basis for arguing about facts in court.

Computer Forensics is the scientific study and use of processes involved in the identification, preservation, recovery, extraction, examination, interpretation, documentation, and presentation of the contents of computer media (digital evidence) for evidentiary and/or root cause analysis. Usually pre-defined procedures are followed, but flexibility is expected and encouraged because the unusual will be encountered.


Digital forensics is preferred by some when referring to the application of forensics to information stored or transmitted by computers but computer forensics remains in common use.

• Features of Digital Evidence and Computer Forensics Methodology

  • Digital evidence can be duplicated exactly.

  • Computer forensics requires duplication of the original evidence so that a copy can be examined as if it were the original.

  • Computer forensics involves both data recovery and analysis.

  • Even if “deleted,” digital evidence can be recovered from computer media (at least until completely overwritten).

  • Even when attempts have been made to destroy digital evidence, it can remain and be detected.
• Computer forensics is governed by valid laboratory principles.

• **Guiding Principles**
  
  • The rules of evidence apply to digital evidence.
  
  • Actions taken to secure, collect, and analyze digital evidence should not change the evidence in any way (i.e., not affect the integrity of the evidence).
  
  • Persons accessing or conducting examinations of digital evidence should be trained for that purpose.
  
  • All activity relating to the seizure, access, examination, storage, or transfer of digital evidence must be fully documented and that documentation must be preserved and available for review.

§4.3.2. **Basic Model of Computer Forensics**

Computer forensics is typically reactive and after-the-fact – essentially the “post-mortem” examination of media to gather digital evidence from hard drives, disks, etc. The following briefly describes the steps that must be taken.

• **Policy and Procedure Development**
  
  • Effective computer forensics capability requires that policies and procedures be in place to govern the unit’s or task force’s functions and operating parameters.

• **Assessment**
  
  • Forensic examiners should assess digital evidence thoroughly with respect to the scope of the case to determine the course of action to take. This includes review of the search warrant or other legal authorization, consultation with the case investigator (goals and avenues of investigation, search terms, etc.), assessment of the hardware and software anticipated and of the location where they will be found, and planning of steps to acquire the evidence.

• **Acquisition / Preservation**

  • **in general**
    
    • Proper “bag & tag” procedures are employed to protect and preserve the integrity of the computer and/or media.
    
    • Hard drives or other media are duplicated to create bit-stream images – each is a “forensic copy” that preserves everything on the drive or disk.
• At least two copies of the bit-stream forensic image are made.

• A strict chain of custody is established.

- **special cautions due to the nature of computers and digital evidence**

  • Improper shutdown of networked computers may cause loss of evidence, damage to the network system, disruption of a business, and potential civil liability.

  • Collection and transportation of computer evidence must reflect awareness of the susceptibility of the evidence to damage or alteration. Concerns include electro-magnetic fields from static, radio transmitters, speaker magnets etc., and heat, cold, or humidity (e.g., from placement on heated seats or prolonged storage in the trunk of a patrol car).

  • Exposure to shock and vibrations during transport can cause damage or alteration.

  • Evidence such as times, dates, or system information in battery-powered devices may be lost or altered due to the passage of time or prolonged storage if the batteries are allowed to discharge.

- **Authentication**

  • The evidence is proven to be exactly what the suspect left behind, generally through calculation of *hash values* of the original evidence and the forensic copies.

  • The strict chain of custody, with limited personnel access, is maintained.

  • The examiner conducts *validation of tools* (hardware, software, methods, etc.) to ascertain and demonstrate reliability of the tools and the results.

- **Analysis/Examination**

  • Unlike other types of evidence, analysis can be performed on an exact copy of the original.

  • A forensic copy (never the original) is examined in a controlled environment.

  • Time stamping/hash code techniques can be used to prove evidence has not been compromised.

  • A specialist recovers, extracts, and analyzes data in all of the following:
• present/active files (documents, spreadsheets, images, email, etc.)
• all file system types
• archive files (backups)
• deleted files
• “slack” space
• other unallocated space
• swap space
• temporary files (cache, print records, temporary Internet files, etc.)
• encrypted or otherwise hidden files
• compressed or corrupted files
• non-partitioned areas

• The specialist also examines how the computer was being used.

• **Reporting**

  • All steps, actions, and observations are documented.
  
  • All findings and the results of automated processes are reported.
  
  • If necessary, testimony is given.

§4.3.3. **SPECIAL AND EMERGING ACTIVITIES OR PROCESSES**

As computer forensic techniques evolve in response to ever changing technologies and due to expanding knowledge, specialized forensic “models” or processes are emerging to modify or supplement the model set out in §4.3.2.

Variations include:

• **Triage forensics** (“on-site previewing” or “rolling forensics”)
  
  • Uses write blocking hardware and software for on-site previewing, enabling on-site “triage” to find evidence and determine whether an image should be made or the computer seized for off-site examination.
  
  • Useful in knock-and-talk situations or for probation and parole officers to monitor compliance with conditions of release.

• **Hand-held** (or “Mobile,” “Cell phone,” or “Portable Electronic Device”) **forensics**
  
  • Specialized techniques and tools to examine small devices with embedded computers and memory, such as cellular phones, wrist watches, personal digital assistants (PDAs), digital cameras, and hybrid devices.
• Preserves and examines data on solid-state devices.

• **CD and DVD forensics**
  • Preserves and examines data stored on optical devices.

• **Live forensics**
  • Bag and tag procedures for when a running computer is encountered (especially in home and small office networks).
  • Used to acquire or analyze evidence in volatile memory, such as RAM.

• **Network forensics**
  • Captures, records, and analyzes events occurring on a functioning/operating computer network.
  • Useful for intrusion detection, monitoring, etc.
  • Involves examining audit logs; traffic, time, and packet analysis; session reconstruction; and identifying connections.

• **Software forensics**
  • Examination of computer code or text and analysis of data to determine authorship.
  • Examination of questioned *electronic* documents.