Computer Forensic
Evidence Collection and Management

Chapter 11

Extracting Computer and Electronic Evidence

Chapter Objectives

- Learn the functions that occur in a computer forensics lab
- Understand the techniques required to image a hard drive
- Identify a process for deciding what evidence to collect
- Look at the steps required to successfully process latent electronic evidence
- Understand the importance of the chain-of-custody and documentation

Introduction

- The function of a computer forensics lab is to provide technical support in the detection, preservation, recovery, examination, and reporting of electronic and computer-related latent evidence.
- Procedures and techniques must be in place to preview the content of computer hard drives without risk of changing the data, capture an exact copy of the data held on computer hard drives and other media, an automatically produce a printable audit trail to identity the actions taken.
- Capturing an exact copy of the data involves a process known as imaging.
- Having captured the data from the suspect machine in a fashion that enables any information fund to bused as evidence, the next step is to process the image.
- Computer investigators can utilized highly sophisticated tools, many of which are not available for general release.

Forensic Laboratory Functions

- Computer forensic consultant organizations and law enforcement organizations are usually the major players when it comes to operating an electronic evidence laboratory.
- Examiners will be utilizing no evidentiary hardware and software to conduct forensic imaging or analysis of electronic and computer evidence.
- Equipment preparation and maintenance is an important lab operating procedure and equipment must be monitored and documented to ensure proper performance is maintained.
- Documentation for each tool used is an important consideration.
- The main functions that occur in the lab will consist of forensic imaging, forensic analysis, forensic examination, and report generations.

IACIS Guide for Forensic Examinations

- The International Association of Computer Investigative Specialists (IACIS) has established a guide for forensic computer and digital evidence examinations.
- Computer and digital media examinations are different and depend on the specific circumstances of the investigation .
- Cases involving computers and other electronic devices cross multiple disciplines.
- Computer system components, other electronic devices, and digital and electronic media are items of evidence just like any other items of evidence.
- When examining a computer, the system, date, and time should be collected, preferably from the BIOS setup. Depending on the BIOS, other information such as system serial numbers, component serial numbers, hardware component hashes, etc. should be noted.
- Examination of media should be conducted in a forensically sound examination environment.
- Conducting an examination on the original evidence media should be avoided.
- Examination of the media should be completed logically and systematically by starting the search where the data of the evidentiary value is most likely located.

IACIS Guide for Forensic Examinations (Cont.)

- Examples of items to be noted might include:
  - The number and type of partitions for hard drives.
  - The number of sessions for optical disks
  - File system on the media
  - A full directory listing should be made that includes folder structure, filenames, date/time stamps, logical file sizes, etc
  - Installed operating systems
  - User-created files should be examined using native applications, file viewers or hex viewers
  - Operating systems files and applications created files should be examined
  - Installed applications
  - File hash comparisons may be used to exclude or include files for examination
  - Unused and unallocated spaced on each volume should be examined for previously deleted data, deleted folders, slack space data , and intentionally placed data
  - Previously deleted file names of apparent evidentiary value should be noted.
  - Keyword searches may be conducted to identify files or areas of the drive that might contain data of evidentiary value and to narrow the examination scope
  - The system are of the volume should be examined and any irregularities or peculiarities noted.
  - Examination of areas of the media that are not normally accessible
- At the conclusion of the examination process, sufficient notation of any discovered material of an apparent incriminating or exculpatory evidentiary nature should be made.

Managing the Imaging Process

- The chain-of-custody must be maintained o devices received at the lab for examination.
- Receipts must also be completed for any device received and evidence logs maintained.
- Any exceptions between the inventory documentation and the actual evidence must be documented.
- The first step in the imaging process is to document the current condition of the evidence.
- The remaining steps would be conducted based on the standard procedures.
- Basically these include the following:
  - Hardware or software write-blockers would be used to prevent modification of the evidence
  - Forensic images would be captured using hardware and software that is capable of capturing a bit-stream image of the original media
  - Properly prepared media should be used when making forensic copiers to ensure no commingling of data from different cases
  - Forensic images should be archived to media and maintained consistent with the departmental policy and applicable laws.
- Upon completion of the imaging process, the next step involves forensic examination and analysis

Evidence Collection And Archiving

- The examiner should review the documentation that accompanies the evidence to determine the processes necessary to complete the examination and also ascertain legal authority to perform the request.
- Basic guiding principles during evidence collection include the following:
  - Capture as accurate a picture of the system as possible
  - Keep detailed notes.
  - Note the difference between the system clock and the UTC
  - Be prepared to testify outlining all actions taken and at what times.
  - Minimize changes to user and system data as it is being captured.
  - Remove external avenues for change.
  - When confronted with a choice between collection and analysis, conduct collection activities first and analyze later
  - Proceed from the volatile to the less volatile
  - Be methodical
- Procedures should be feasible, repeatable and reproducible.
- Additional types of examinations might need to be conducted on the same device.
- Forensics analysis would be conducted on the second bit-level copy of the evidence, as the analysis will almost certainly later file access times.

Evidence Collection And Archiving (Cont.)

Order of Volatility

- When collecting evidence, proceed from the volatile to the less volatile.
- An example order of volatility for a typical system consists of the following:
  - Registers and cache
  - Routing table, Address Resolution Protocol (ARP) cache, process table, kernel statistics, memory
  - Temporary file systems
  - Disk
  - Remote logging and monitoring data that is relevant to the system in question
  - Physical configuration and network topology
  - Archival media

Things to avoid

- It is also too easy to destroy evidence, however inadvertently. Several “don’ts” include the following:
  - Do not trust the program on the system
  - Do not run program that modify the access time of all files on the system
  - When removing external avenues for change, note that simply disconnecting or filtering from the network may trigger “dead man switches”
  - Do not overlook the possibility of changes introduced via a wireless access.
- Decision-making should be minimized during the collection process.

Evidence Collection And Archiving (Cont.)

Privacy Considerations

- Examiners must respect the privacy rules and guidelines of the organization and legal jurisdiction.
- Do not intrude on people's privacy without strong justification

Legal Considerations

- Computer evidence needs to be admissible, authentic, complete, reliable, and believable.
- There must be nothing about how the evidence was collected and subsequently handled that casts doubt about it authenticity and veracity.
- Techniques and procedures must be objective.
- The methods used to collect evidence should be transparent and reproducible.
- Document all steps and processes used to identify and extract the evidence.

Residual Data

- Proprietary information can be recovered from residual data that remains on hard drives.
- *Residual data* refers to data that is not active on the computer system.
- Delete , format, and Fdisk commands do not remove data from a hard drive.
- During operations, operating system and applications create files in the background that include the followings:
  - Automatic backup files
  - Globally unique identifiers
  - Internet browser files
  - Internet history files
  - Metadata
  - Power savers features
  - Temporary files
  - Temporary Internet files
  - Spooler files
  - Virtual memory and swap files.

Examining the Digital Images

- Examination of a computer must be done thoroughly, carefully, and without changing anything on the compute.
- At the previous stage, simple checks may be performed to determine current status of the data files.
- All data is copied to create the images including data such as:
  - Data that may have been deleted
  - Information hidden outside the normal storage areas
  - Old data that has been partially overwritten
- Often it is hidden data that contain vital evidence to prove or disprove a case.
- The image is an exact replica of the suspect computer hard drive or other media.
- Having captured the data from the suspect machine in a fashion that enables any information found to be used as evidence, the nest step is to process the image.
- Computer investigators can utilize highly sophisticated tools, many of which are not available for general release.
- With the right tools, and entire computer network can be searched for specific words or characters.

Qualifying a Computer for Forensic Recovery

- In practical every computer there is “deleted” data that can be recovered; however, the data recovered is not always relevant to the case.
- It is possible to predict and prioritize the best computers for recovery based on a series of questions, such as:
- Did any person involved use the computer?
- *A file can be divided into several pieces and exits in various location on a hard drive.*
- *If the deleted time was an e-mail a different set of rules apply*
- How long has it been since files were deleted?
- *Because of the way files are left behind as dead space on the hard drive, as space is needed by different programs or Web pages, the file pieces are gradually overwritten.*
- How much has the computer been used since files were deleted.
- Because files are overwritten gradually, the more the computer is used, the more likely new files have overwritten older files erasing your valuable information.
- If the computer is necessary for operation of the business, the specialist can safely and effectively “clone” or image the hard drive to preserve the information.

- Even when there is no one to answer questions, there is still a good possibility of recovering valuable evidence from the right computer, even when the files never exited on the computer.

Forensic Tools

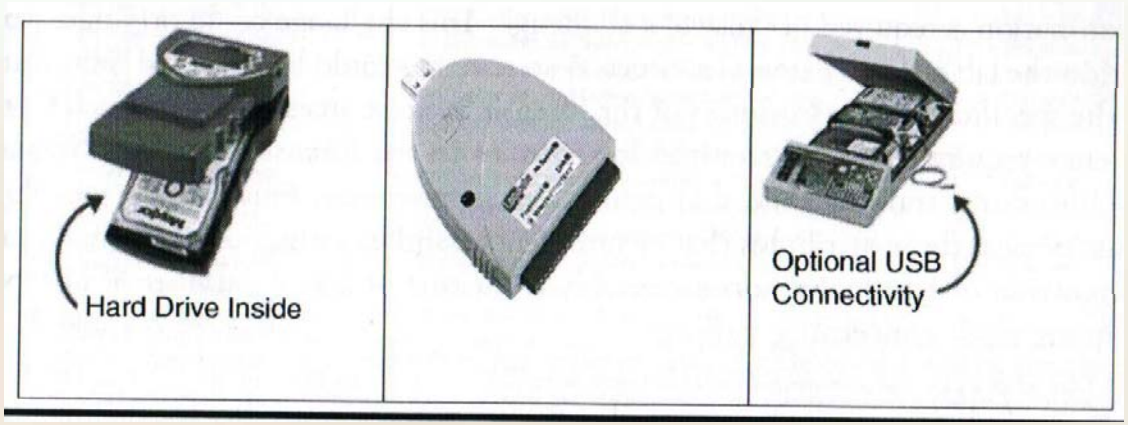
- Tools should include programs need to perform evidence collection and forensics on read-only media. A set of tools should be available for each of the operating system being examined.
- The set of software tools should include the following features:
  - Examine processes
  - Examine system state
  - Make bit-to-bit copiers
  - Generate checksums and signatures
  - Generate core images and examine them
  - Create script to automate evidence collection
- The Coroner's Toolkit (TCT) is a suite of computer security programs. It is intended to assits in a forensic analysis of a UNIX system after a break-in.
- The Ultimate Toolkit includes the following modules:
  - Forensic Toolkit (FTK)
  - Password Recovery Toolkit
  - Registry Viewer
  - FTK Imager
- EnCase Forensic provides investigators with tools to authenticate, search, and recover compute evidence.
- The iLook Investigator forensic is a comprehensive suite of computer forensic tools used to acquire and analyze digital media.

Forensic Tools

- The Sleuth Kit is a collection of UNIX-based command line file and volume system forensic analysis tools.
- The Autopsy Forensic Browser is a graphical interface to the command line digital investigation analysis tools in the Sleuth Kit
- Foremost is a console program to recover files base on their headers, footers and internal data structures.
- dcfldd is an enhanced version of the GNU dd.
- GNU is a set of programs written to provide a free UNIX framework
- SafeBack is used to create mirror-image (bit-stream) backup files of hard disks or make a mirror-image copy of an entire hard disk drive or partitions.
- The MacQusition Boot CD is a forensic acquisition tool used to safely and easily image Mac suspect drives using he suspect's own system.

Disk Drive Examinations

- Two techniques for disk drive examination include the use of a hardware forensic imaging tool or a software forensic product.
- The two techniques employed in the lab setting include the Logicube Forensic MD5 and Access Data Forensic Toolkit
- The primary function of the hardware solution is to produce a drive-to-drive image that is forensically sound.



Disk Drive Examinations

IDE-to-IDE Imaging

- Bit-bit imaging is simple using the hardware device with an integrated drive electronics (IDE) and power cables.
- The first step is that the computer must be opened to revel the internal hard drive.
  - After opening the case, the IDE cable and disk drive power cable must be disconnected from the internal hard disk.
  - Insert a black hard drive into the Imaging device. Connect to the IDE cable in the imaging device.
  - Connect the IDE cable from the imaging device to the internal hard drive
  - Connect the power cable from the imaging device to the internal hard drive
  - Connect the power cable from the imaging deice to some acceptable power source.
- This completes the step for the physical connectivity for an IDE image.
- The next step is to perform the actual imaging process
- Each imaging product will provide different levels of options that can take place during the imaging process.

Disk Drive Examinations

Software Acquisition

- Software acquisition tools create a forensically sound image that makes no changes to the data and information on the suspect hard drive.
- The forensic image must be identical in every way to the original, including file slack and unallocated space.
- Forensic software products can examine hard drive images created by the bit-bit imaging process described in the previous section

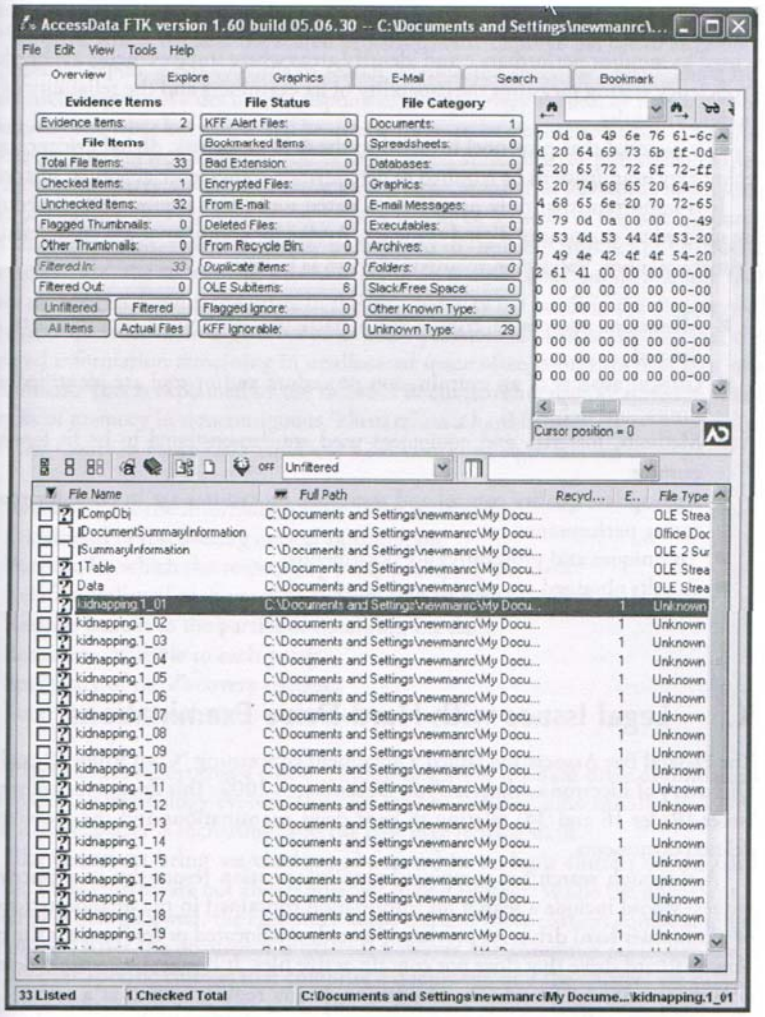


Figure 11.2 AccessData FTK main screen.

Disk Drive Examinations

Software Acquisition

- Software acquisition tools create a forensically sound image that makes no changes to the data and information on the suspect hard drive.
- The forensic image must be identical in every way to the original, including file slack and unallocated space.
- Forensic software products can examine hard drive images created by the bit-bit imaging process described in the previous section

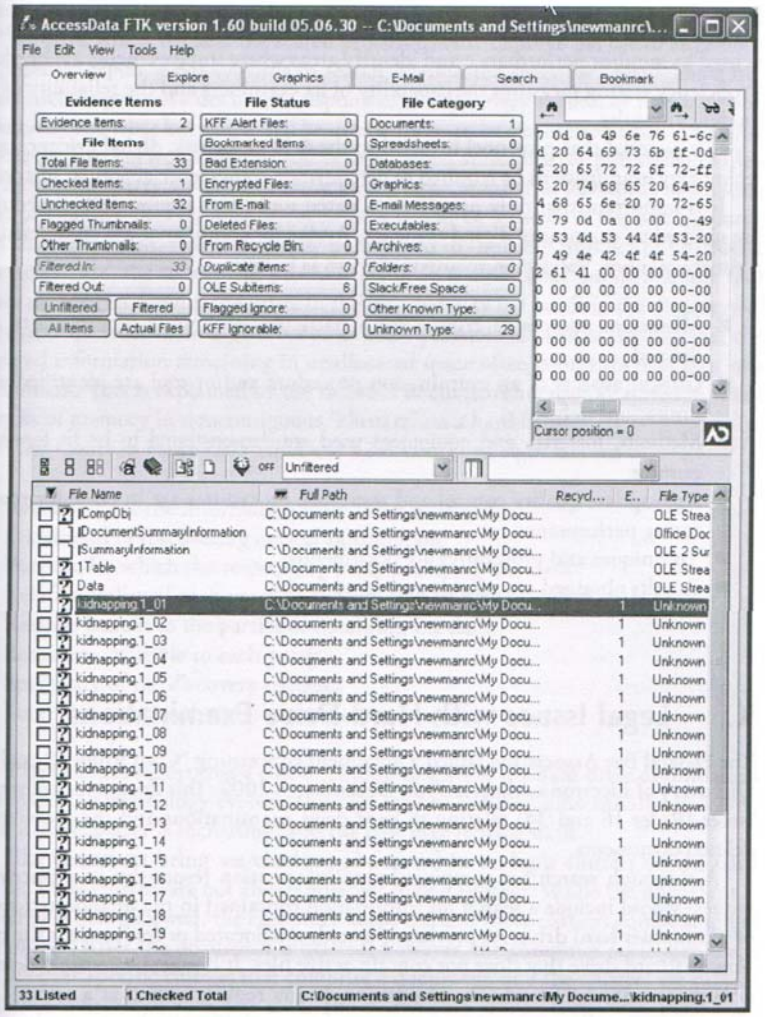


Figure 11.2 AccessData FTK main screen.

Review and Quality Assurance

- The forensic lab should have a written policy establishing the protocols, technical, peer, and administrative review.
- A statement should be provide that related to the specific quality assurance of the forensic lab resources and personnel.
- A number of observations are made concerning staff:
  - An individual must have overall authority and responsibility for the management and quality of the work accomplished in the lab.
  - Examiners must be responsible in a particular case for identifying, retrieving, interpreting, and reporting findings
  - Examiners must have achieved levels of competency for specific equipment and services. They must be able to write reports of factual information in their specific specialist areas and provide factual testimony in legal proceedings.
  - Technical specialist must be able to provide information concerning interpretations of various forensic tests.

Review and Quality Assurance (Cont.)

Proficiency Testing and Validation

- Proficiency testing is an integral part of an effective quality assurance program
- It is used to monitor performance and identify areas where improvements are needed.
- Validation requirements are as follows:
  - Minimum acceptable criteria for a particular technique or procedure are defined.
  - Critical aspects of an examination procedure and/or tool are identified and limitation defined
  - Methods, material, and equipment used are demonstrated to be fit for their purpose
  - Appropriate quality control and assurance procedures are in place for monitoring performance
  - Techniques and procedures are documented
  - Result obtained are reliable and reproducible.

Legal Issues with Hard Drive Examinations

- The Federal Bar Association issued a document concerning “Civil Rules Regarding Discovery of Electronic Materials”. This document addressed issues relating to hard drive examination and the problem of deleted documents.
- A thorough search for computer-based information responsive to a discovery request would include a search for information contained in the unallocated space of a computer hard drive.
- A forensic expert used keyword to search unallocated space for “hits”.
- Determine what keywords will be used is likely to be a contested issue.
- This becomes more probable in view of the fact hat the deleted information remaining is unallocated space often comprises only part of a document.
- The Court in Rowe examined eight factors:
  - Availability of the information from other sources
  - Likelihood of discovering critical information
  - Purpose for which the respond party maintains the data
  - Relative ability of each party to control costs and its incentive to do so
  - Relative benefit to the parties of obtaining the data
  - Resources available to each party
  - Specificity of the discovery requests
  - Total cost associated with the production.

Legal Issues with Hard Drive Examinations (Cont.)

- The document being searched may be stored in multiple clusters on the hard drive. Theses clusters are not always adjacent to one another.
- A search of unallocated space may reveal individual clusters, which may or may not contain portions of a document , and often does not reveal entire documents, much less entire documents that are useful.
- In other cases, however , a forensic examination of a hard drive and unallocated space may lead to the discovery of an important missing piece of evidence. , such as a “smoking gun” document.
- There are numerous legal implications of the various parties' responsibilities concerning preservation of electronic evidence, the need to meet-and-confer early in the case on electronic discovery issues, recovery of deleted electronic materials, management of electronic document production, privilege issues, and post-litigation electronic document return or destruction.
- Failure to abide by the various requirements can result in inadmissibility of the forensic evidence.

Legal Issues with Hard Drive Examinations (Cont.)

Redaction

- The court may request redaction of evidence used in a trial .
- After litigation, data may be reacted prior to returning media to the defendant.
- Redaction means cutting, rearranging, altering, or refining data off a hard drive. Items that may be included in such a request are:
  - E-mails
  - Files
  - Files and slack
  - Files slack only
  - Free space
  - Entire drive
  - Specific identified sectors
- Requests might be made to remove specific e-mails or the entire folder. Once specific e-mails have been identified, usually with a forensic program, an individual e-mail must be deleted.
- Files to be deleted are based upon the analyst's report. Overwriting the file can take considerable time as numerous passes are required –usually seven.
- If free space is to be wiped, files may not have to be overwritten, as deleted files are located in drive free space.

Legal Issues with Hard Drive Examinations (Cont.)

- Specific sectors to be deleted would be identified by the analyst.
- It is necessary to use custom software to overwrite the list of sectors provided.
- Examination documentation should be case specific and contain sufficient details to allow another forensic examiner to perform an independent review of the facts and details.
- The chain-of-custody and investigative journal must be clearly documented.