Digital Forensics: An Introduction

An online course presented by the
American Board of Information Security and Computer Forensics
and the
American Board for Certification in Homeland Security
Introduction to Computer Forensics
Introduction to Computer Forensics

- A basic definition: The collection and analysis of data from computers and other digital devices in the interest of obtaining evidence.
Introduction to Computer Forensics

- Evidence obtained in a computer forensic investigation can be useful in criminal, civil, or corporate investigations, but different legal rules may apply.
Introduction to Computer Forensics

• Why is digital forensics important?
  ▫ According to some estimates, almost 95 percent of criminals leave evidence which could be captured and analyzed through proper computer forensic procedure.
Introduction to Computer Forensics

• Why is digital forensics important?
  ▫ Some criminals are getting smarter; data-hiding techniques such as encryption and steganography can put evidence of criminal activity where traditional search methods cannot find it.
    • Encryption – scrambling data, such as an e-mail message, so that it cannot be read if intercepted in transit.
    • Steganography – hiding a message in a larger file, typically in a photographic image or sound file.
Introduction to Computer Forensics

• Computer forensics is not just about “detective work” – searching for and attempting to discover information.

• Computer Forensics is also concerned with:
  ▫ Handling sensitive data responsibly and confidentially.
  ▫ Taking precautions to not nullify findings by corrupting data.
  ▫ Taking precautions to ensure the integrity of the data.
  ▫ Staying within the law and rules of evidence.
Introduction to Computer Forensics

• Before we get into the specifics of computer forensics, let’s look at steps that are common to all forensic investigations...
Introduction to Computer Forensics
The Forensic Process

Collection  Examination  Analysis  Reporting
Introduction to Computer Forensics

Phase 1: Collection

Identify, isolate, label, record, and collect the data and physical evidence related to the incident being investigated, while establishing and maintaining integrity of the evidence through *chain-of-custody*. 
Introduction to Computer Forensics

Phase 2: Examination

Identify and extract the relevant information from the collected data, using appropriate forensic tools and techniques, while continuing to maintain integrity of the evidence.
Analyze the results of the examination to generate useful answers to the questions presented in the previous phases.

*The case is typically “solved” in this phase.*
Introduction to Computer Forensics

Phase 4: Reporting

Reportin the results of the analysis, including:

- Findings relevant to the case
- Actions that were performed
- Actions left to be performed
- Recommended improvements to procedures and tools
Introduction to Computer Forensics

• What are we investigating?
  ▫ Identity theft
  ▫ Fraud and embezzlement
  ▫ Software piracy and hacking
  ▫ Blackmail and extortion
Introduction to Computer Forensics

• What are we investigating?
  ▫ Child pornography and exploitation
  ▫ Prostitution, infidelity, domestic violence
  ▫ Terrorism and national security
  ▫ Theft of intellectual property and trade secrets
Introduction to Computer Forensics

• What evidence can we recover?
  - Computer Fraud Investigations
    - Accounting software and files
    - Credit card data
    - Financial and asset records
    - Account data from online auctions
    - E-mail, notes, and letters
Introduction to Computer Forensics

• What evidence can we recover?
  ▫ Child Exploitation Investigations
    • Chat logs
    • Photos and digital camera software
    • Internet activity logs
    • Movie files
    • Graphic editing and viewing software
    • User-created directory and file names to classify images
Introduction to Computer Forensics

• What evidence can we recover?
  ▫ Network Intrusion and Hacking Investigations
    • Network usernames
    • Internet protocol (IP) addresses
    • Executable files (including viruses and spyware)
    • Security logs
    • Configuration files
    • Text files and other documents containing sensitive information such as passwords
Introduction to Computer Forensics

- What evidence can we recover?
  - **Identity Theft Investigations**
    - Identification Templates
      (Birth certificates, driver’s licenses, Social Security cards)
    - Electronic images of signatures
    - Credit card numbers
    - Credit card reader/writer/scanner
    - Online trading information
Introduction to Computer Forensics

• What evidence can we recover?
  ▫ Harassment and Stalking Investigations
    • Victim background research
    • Maps to victim locations
    • Photos
    • Diaries
    • Internet activity logs
    • E-mails, notes, and letters
Introduction to Computer Forensics

• What evidence can we recover?
  ▫ Software Piracy Investigations
    • Software serial numbers
    • Software cracking utilities
    • Image files of software licenses
    • Binary files for software installation
    • Chat logs
    • Internet activity logs
Introduction to Computer Forensics

- **Evidence** is something that tends to *establish* or *disprove* a fact.
- Four types of evidence
  - Real
  - Documentary
  - Testimonial
  - Demonstrative
Introduction to Computer Forensics

• **Real evidence** is something you could actually carry into court and show to a jury.
  ▫ This type of evidence is the most powerful.
  ▫ Real evidence typically “speaks for itself.”
Introduction to Computer Forensics

• **Documentary evidence** is any evidence in written form.
  - Database files, server logs, e-mail, etc.
  - Documentary evidence could be faked by a skilled computer user and therefore must be authenticated to be admissible in court.
  - Always produce the original document, not a copy.
Introduction to Computer Forensics

• *Testimonial evidence* is the statement of a witness, under oath, either in court or by deposition.
  ▫ This type of evidence typically supports or validates the other types.
Introduction to Computer Forensics

• *Demonstrative evidence* recreates or explains other evidence.
  ▫ Demonstrative evidence does not “speak for itself” and is used to illustrate and clarify previous points.
  ▫ This type of evidence is most helpful in explaining technical topics to non-technical audiences.
Introduction to Computer Forensics

- Five characteristics of useful evidence
  - Admissible
  - Authentic
  - Complete
  - Reliable
  - Believable
Introduction to Computer Forensics

- Evidence should be...
  - Admissible
    - If the evidence you uncover will not stand up in court, you have wasted your time and possibly allowed a guilty party to go unpunished.
Introduction to Computer Forensics

• Evidence should be...
  ▫ **Authentic**
    • It must be directly related to the incident being investigated.
    • The digital forensic investigation may reveal evidence that is interesting but irrelevant.
Introduction to Computer Forensics

• Evidence should be...
  ▫ Complete
    • The investigator should approach the case with no preconceived notions about someone’s guilt or innocence.
    • Forensic methods should eliminate alternative suspects and explanations until a definite conclusion is reached.
Introduction to Computer Forensics

• Evidence should be...
  ▫ Reliable
    • There should be no question about the truth of the investigator’s conclusions.
    • Reliability comes from using standardized and verified forensic tools and methods.
    • Qualification (by a judge) of an investigator as an expert witness in a case will help to establish credibility and reliability.
Introduction to Computer Forensics

• Evidence should be...
  ▫ **Believable**
    • The investigator must produce results that are clear and easy to understand, even among the most non-technical members of a jury.
    • Have other investigators have used the same forensic techniques and reached similar conclusions?
Introduction to Computer Forensics

• The “Best Evidence” Rule
  ▫ Evidence presented in court should be original and the actual item investigated or examined (and therefore considered “best evidence”).
    • Federal Rules of Evidence consider a printout of computer data to be “original” if it can be read by sight and if it accurately represents the stored data.
    • A proper forensic image can be considered Best evidence if the original evidence has been returned to its owner.
Introduction to Computer Forensics

• The Daubert Test
  ▫ The Case of *Daubert v. Merrill Dow Pharmaceuticals* established new criteria to determine the reliability, relevancy, and admissibility of scientific evidence.
Introduction to Computer Forensics

• The Daubert Test
  ▫ The theory or technique must have been tested, and that test must be replicable.
  ▫ The theory or technique must have been subject to peer review and publication.
  ▫ The error rate associated with the technique must be known.
  ▫ The theory or technique must enjoy general acceptance within the scientific community.
Introduction to Computer Forensics

• Some *common-sense* rules of evidence:
  ▫ Evidence is admissible only if it is relevant.
  ▫ Relevant evidence is admissible unless and until another rule says it is *inadmissible*.
  ▫ The judge presiding over a case can render your evidence admissible or inadmissible.
Introduction to Computer Forensics

- Federal Rules of Evidence
  - These are the most relevant legal rules for a forensic investigator.
  - The rules became Federal law in 1975.
  - These rules pertain to evidence presented in federal courts.
    - State courts may have their own rules of evidence but often use the federal rules as guidelines.
Introduction to Computer Forensics

• Federal Rules of Evidence
  ▫ Forensic investigators should know...
    • Rule 401: Definition of "Relevant Evidence"
      "Relevant evidence" means evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence.
Introduction to Computer Forensics

- **Rule 402: Relevant Evidence Generally Admissible; Irrelevant Evidence Inadmissible**

  All relevant evidence is admissible, except as otherwise provided by the Constitution of the United States, by Act of Congress, by these rules, or by other rules prescribed by the Supreme Court pursuant to statutory authority. Evidence which is not relevant is not admissible.
Introduction to Computer Forensics

- Rule 403: Exclusion of Relevant Evidence on Grounds of Prejudice, Confusion, or Waste of Time

  Although relevant, evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence.
Introduction to Computer Forensics

- **Rule 601: General Rule of Competency**

  Every person is competent to be a witness except as otherwise provided in these rules. However, in civil actions and proceedings, with respect to an element of a claim or defense as to which State law supplies the rule of decision, the competency of a witness shall be determined in accordance with State law.
Introduction to Computer Forensics

- **Rule 702: Testimony by Experts**

  If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case.
Introduction to Computer Forensics

- **Rule 703: Bases of Opinion Testimony by Experts**

  The facts or data in the particular case upon which an expert bases an opinion or inference may be those perceived by or made known to the expert at or before the hearing. If of a type reasonably relied upon by experts in the particular field in forming opinions or inferences upon the subject, the facts or data need not be admissible in evidence in order for the opinion or inference to be admitted.
Introduction to Computer Forensics

- **Rule 703: Bases of Opinion Testimony by Experts**
  
  (continued)

  Facts or data that are otherwise inadmissible shall not be disclosed to the jury by the proponent of the opinion or inference unless the court determines that their probative value in assisting the jury to evaluate the expert's opinion substantially outweighs their prejudicial effect.
Introduction to Computer Forensics

- **Rule 1002: Requirement of Original**
  To prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of Congress.
Introduction to Computer Forensics

- **Rule 1003: Admissibility of Duplicates**
  A duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original.
Introduction to Computer Forensics

- Evidence uncovered in a digital investigation may be direct evidence of a crime or might simply corroborate other evidence.
- The crime or incident being investigated might not necessarily be a computer-based crime.
Introduction to Computer Forensics

• A recent example: Dennis Rader was identified as the “BTK Killer” due to evidence that connected him to an incriminating Microsoft Word document e-mailed to a TV station.
• The evidence that led to Rader’s conviction was actually contained within the “metadata” (data about data) that is created by default in Microsoft Office documents.
Introduction to Computer Forensics

• Who should perform this kind of work?
  ▫ True computer forensics should be performed by forensic experts specifically trained and experienced in investigative methods.
Introduction to Computer Forensics

• Who should perform this kind of work?
  ▫ System administrators and information security professionals should gain enough knowledge to know they don’t have to be forensics experts. They should, however, work to minimize risk to their environment to help in the event of an incident.
## Introduction to Computer Forensics

Request for Computer Forensic Service

National Institute of Justice
www.ojp.usdoj.gov/ni

---

<table>
<thead>
<tr>
<th>Department of Maryland State Police</th>
<th>Computer Forensic Laboratory</th>
</tr>
</thead>
<tbody>
<tr>
<td>7150 C Columbia Gateway Drive, Columbia, Maryland 21046</td>
<td></td>
</tr>
</tbody>
</table>

### REQUEST FOR SERVICE

<table>
<thead>
<tr>
<th>Date Submitted</th>
<th>MSP Complaint Control:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Submitting Agency</td>
<td>Address:</td>
</tr>
<tr>
<td>City:</td>
<td>County:</td>
</tr>
<tr>
<td>Agency Case:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Location Served</th>
<th>Suspects Last Name, First Name, M.I.</th>
<th>Sex</th>
<th>Age</th>
<th>Taxing Number</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Case Title:</th>
<th>Date of Arrest:</th>
<th>Date of Release:</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Crime:</th>
<th>Date of Offense</th>
<th>Date Charges Filed</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Owner of Property:</th>
<th>Name:</th>
<th>Address:</th>
<th>Telephone:</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Type of Service (C)</th>
<th>Search Warrant/Consent/Administrative/Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Computers</td>
<td>Submitted/Government/MCDD/Other</td>
</tr>
</tbody>
</table>

| Has this evidence been previously viewed, assessed, or examined by anyone? | Yes | No |
| Are you aware of any privileged information contained within the evidence being submitted for examination? | Yes | No |
| Are you aware of any other information related to the evidence being submitted? | Yes | No |

<table>
<thead>
<tr>
<th>Urgent Request for Examination:</th>
<th>Date Requested</th>
<th>Period of Request</th>
<th>Telephone where you can be reached</th>
<th>Date Analysis Needed:</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Reason for Request:</th>
<th>(Except for immediate Court dates, all Urgent requests must be accompanied by a written justification.)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>SERVICE REQUESTED: (Requests for field service must be received at least 2 business days prior to service):</th>
</tr>
</thead>
</table>

### INSTRUCTIONS

- Please provide all requested information and make any unusual circumstance in the “Service Requested” area.
- Please attach the Request for Laboratory Examination Claim of Custody Long Form (CL-260) and a copy of your agency instruction: Property Record Form.
- Please attach a Detailed Report of seized evidence, which includes personal data, e-mail addresses, hard drives, screen names, passwords, target websites, accelerators, and a list of any other information relevant to your investigation.

<table>
<thead>
<tr>
<th>LABORATORY USE ONLY:</th>
<th>Date Case Received:</th>
<th>Case Priority:</th>
</tr>
</thead>
<tbody>
<tr>
<td>LBN/CASE #:</td>
<td>Received by:</td>
<td>Priority:</td>
</tr>
</tbody>
</table>
Introduction to Computer Forensics

• In criminal investigations, the rights of all citizens (including criminal suspects) are protected by the U.S. Constitution’s Fourth Amendment and decades of legislation and case law.

• Failure to observe proper “search and seizure” procedure can ruin a criminal investigation, no matter how incriminating the evidence.
Introduction to Computer Forensics

- The search warrant (required by the Fourth Amendment in most cases) should...
  - Clearly state what you are searching for.
  - Clearly state the area in which you are authorized to search.
  - Be signed by a judge.
Introduction to Computer Forensics

The Fourth Amendment:

“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”
Introduction to Computer Forensics

• Does law enforcement always need a search warrant?
  ▫ The “plain view” doctrine says that an officer can seize evidence that is in plain view as long as:
    • The officer is legally present at the site of the evidence.
    • The officer can legally access the evidence.
    • The officer has probable cause to believe that the evidence or contraband is related to a crime.
Introduction to Computer Forensics

• Does law enforcement always need a search warrant?
  ▫ When applying the *plain view* doctrine, keep in mind that the right to *seize* evidence gathered through the plain view exception does not necessarily imply the right to *search* that evidence.
Introduction to Computer Forensics

• Does law enforcement always need a search warrant?
  ▫ If the owner of a computer or other digital evidence gives consent, the device may be seized.
    • Consent should be given in writing.
    • Consent should acknowledge the possibility of future forensic examination by a trained computer forensic examiner or analyst.
Introduction to Computer Forensics

Search Consent Form

Obtains owner’s consent to search for electronic evidence

U.S. Secret Service
www.secretservice.gov
Introduction to Computer Forensics

• Does the Fourth Amendment mean that our digital information is private?
  ▫ To determine whether an individual has a reasonable expectation of privacy in information stored in a computer, it helps to treat the computer like a closed container such as a briefcase or file cabinet. The Fourth Amendment generally prohibits law enforcement from accessing and viewing information stored in a computer without a warrant if it would be prohibited from opening a closed container and examining its contents in the same situation.
Introduction to Computer Forensics

• Other rules governing the collection of evidence
  ▫ The Wiretap Act
    • Omnibus Crime Control and Safe Streets Act of 1968 (18 USC Section 2501)
  ▫ Electronic Communications Privacy Act
    • 18 USC Section 2701
  ▫ USA PATRIOT Act
  ▫ Right to Financial Privacy Act (RFPA)
  ▫ Fair Credit Reporting Act (FCRA)
Introduction to Computer Forensics

- Title 18 U.S.C.
  - Much of the U.S. Federal law involving computer crime can be found in Title 18 of the United States Code.
  - 18 U.S.C. § 1030: Fraud and Related Activity in Connection with Computers
Introduction to Computer Forensics

• 18 U.S.C. § 1030 makes *Denial of Service Attacks* a federal crime.
  ▫ 18 U.S.C. § 1030(a)(5)(A) (transmission of program, information, code, or command, resulting in damage).
Introduction to Computer Forensics

• 18 U.S.C. § 1030 makes *Substitution or Redirection of a Web site* a federal crime.
  ▫ 18 U.S.C. § 1030(a)(5)(A)(i) (transmission of program, information, code, or command, resulting in damage).
Introduction to Computer Forensics

• 18 U.S.C. § 2252B makes certain *Use of a Misleading Domain Name* a federal crime.
  ▫ 18 U.S.C. § 2252B (using misleading domain name with intent to deceive a person into viewing obscene material or with intent to deceive a minor into viewing harmful material).
Introduction to Computer Forensics

  - 18 U.S.C. § 1030(a)(4) (accessing a computer to defraud and obtain something of value).
Introduction to Computer Forensics

  - 18 U.S.C. § 2261A (using any facility of interstate or foreign commerce to engage in a course of conduct that places person in reasonable fear of death or serious bodily injury to person, person's spouse or immediate family).
Introduction to Computer Forensics

• Corporate (or private) investigations are not subject to the same “search and seizure” rules and Fourth Amendment issues.
• These types of investigations often involve misuse or abuse of company assets, falsification of data, discrimination, harassment, and similar matters likely to involve litigation.
Introduction to Computer Forensics

• The Fourth Amendment does not apply to searches conducted by private parties who are not acting as agents of the government.

• The Fourth Amendment ...

"is wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any government official."

Introduction to Computer Forensics

- A major threat to a corporate data network may be workers who violate the company’s security policy, leaving the network vulnerable to attack.
- A skilled digital forensic investigator can often trace and neutralize these threats without the involvement of law enforcement.
  - When the corporate investigation reveals illegal activity, however, police involvement may be called for. Proceed with caution and consult legal counsel if necessary.
Introduction to Computer Forensics

- **Ethical issues:**
  - The digital forensic investigator must maintain absolute *objectivity*.
  - It is not the investigator’s job to determine someone’s guilt or innocence.
Introduction to Computer Forensics

• Ethical issues
  ▫ It *is* the investigator’s responsibility to accurately report the relevant facts of a case.
  ▫ The investigator must maintain strict confidentiality, discussing the results of an investigation on only a “need to know” basis.
Computer Forensic Tools: Hardware
Computer Forensic Tools: Hardware

• The hardware tools needed for a successful forensic analysis can be divided into two categories, *incident response* and *laboratory*.
  
  • Incident response tools would include the hand tools, cabling, identification supplies, and other items necessary to perform an investigation at the scene of an incident.
  
  • Laboratory tools would include the devices and accessories necessary to perform an analysis, under controlled conditions, of evidence retrieved from an incident scene.
Computer Forensic Tools: Hardware

- A modern mobile forensic workstation
  F.R.E.D. L.
  (Forensic Recovery of Intelligence Device - Laptop)
  by Digital Intelligence
  www.DigitalIntelligence.com
Computer Forensic Tools: Hardware

- The UltraKit
  by Digital Intelligence
  www.DigitalIntelligence.com

Includes write-blockers, cables, adapters, and power supplies necessary for obtaining evidence during incident response.
Computer Forensic Tools: Hardware

• An practical item in the digital forensic toolkit is the Faraday cage, a container that isolates wireless devices from radio frequency signals that could compromise data.
  • The Faraday cage can prevent some laptop PCs, mobile phones, and smartphones from being remotely “wiped” of data or otherwise locked down by wireless instructions.
  • In an emergency, a Faraday cage can be improvised by wrapping a wireless device in several layers of aluminum foil.
Computer Forensic Tools: Hardware

- The Wireless StrongHold Bag by Paraben
  www.Paraben.com

  A Faraday cage built into an evidence bag for the safe collection of wireless devices in incident response.
Computer Forensic Tools: Hardware

- Other essential hardware for incident response:
  - Laptop or notebook PC for data acquisition
  - Write-blockers
  - External hard drives
  - USB drives, floppy disks and external floppy drive
  - Portable network hub or network switch
  - Network cables
    - *Straight-through* cable will allow connection to a hub.
    - *Crossover* cable will bypass a hub or switch in a direct PC-to-PC connection.
Computer Forensic Tools: Hardware

• Other essential hardware for incident response:
  ▫ Evidence inventory logs
  ▫ Evidence identification tape, labels, and stickers
  ▫ Evidence bags (paper and antistatic)
  ▫ Crime scene tape
  ▫ Gloves
  ▫ Nonmagnetic hand tools
  ▫ Cameras (photo and video)
Computer Forensic Tools: Hardware

• In the digital forensic laboratory
  ▫ Forensic workstations are customized computer systems that contain the equipment necessary for analysis of suspect computers.
Computer Forensic Tools: Hardware

• In the Digital Forensic Laboratory
  ▫ In addition to standard PC components such as motherboards, hard drives, and memory, forensic workstations may include:
    • Disk duplicators
    • Disk erasers
    • Write-blockers
Computer Forensic Tools: Hardware

- There are three generally accepted methods for duplicating hard drives
  - Dedicated forensic duplication systems
  - System-to-system imaging
  - Imaging on the original system
Computer Forensic Tools: Hardware

• Disk Imaging on a Dedicated Forensic System
  ▫ Platform specifically built and designed to accommodate numerous types of hard drive connections.
  ▫ Specialized bit-level imaging software transfers an exact copy of the contents of the original hard drive (or other data source) to one or more blanks.
  ▫ Typically, an investigator will make more than one copy of the suspect hard drive using this method.
    • If the forensic analysis is correct, the investigation should produce the same results on identical copies of the drive.
Computer Forensic Tools: Hardware

- Tableau Forensic Duplicator
  www.tableau.com

  Provides disk-to-disk and disk-to-file duplication.

  Wipes disks to remove all traces of previous data on lab workstation hard drives.

  Creates cryptographic hashes.
Computer Forensic Tools: Hardware

• System-to-System Disk Imaging
  ▫ This method uses two separate computer systems -- the suspect and a specialized forensics imaging system.
  ▫ Depending on the type of drives and connections available, both systems are booted from CD-ROM, DVD, USB drive, or floppy disk which loads the imaging software.
  ▫ Data is transferred between the computers using serial, parallel, Ethernet, or USB ports.
  ▫ This method can be slow, and is often not suited to on-the-scene incident response.
Computer Forensic Tools: Hardware

• A modern forensic laboratory workstation
  
  F.R.E.D.
  (Forensic Recovery of Intelligence Device)
  by Digital Intelligence

www.DigitalIntelligence.com
Computer Forensic Tools: Hardware

• Disk Imaging on the Original System
  ▫ Uses the original (suspect) computer to perform the disk imaging transfer process.
  ▫ A blank drive matching the original hard drive’s capacity and configuration is added to the system.
  ▫ A forensic boot disk is used to create a bit-level image of the original disk.
  ▫ This method is typically used in on-the-scene incident response when it is impractical to transport a computer to the investigator’s laboratory.
Computer Forensic Tools: Hardware

• To avoid the possibility of data contamination, digital forensic workstations are typically not connected to the Internet or any computer outside of the laboratory’s secure network.
Computer Forensic Tools: Hardware

• *Never* check e-mail, surf the Internet, or perform typical IT duties on a forensic workstation. Viruses and spyware will seriously compromise your investigation!

• Under no circumstances should peer-to-peer file sharing applications be allowed on the same network as the forensic workstation.
Computer Forensic Tools: Hardware

• Evidence on Removable Media
  ▫ Removable media is normally imaged using a dedicated forensics system. This allows multiple images to be stored on a local hard drive. Duplicate copies can be burned from those images. As with any other kind of digital evidence, original source material should be handled as little as possible.
Evidence on Removable Media

- CDs and DVDs are the easiest and safest to handle since they are usually in read-only mode. When dealing with handwritten labels on CDs and DVDs, consider that the disk may be mislabeled and you are actually dealing with a re-writable disk.
- On floppy disks, be sure the write-protect tab is set in the write-protected mode.
Computer Forensic Tools: Software
Computer Forensic Tools: Software

- Software used in digital forensic analysis comes in two varieties:
  - Commercial software
  - Open-source software
- In either case, the software is typically used for copying data from a suspect’s disk drive (or other data source) to an image file, and then analyzing the data without making any changes to the original source.
Computer Forensic Tools: Software

- Advantages of commercial forensic software:
  - Proven admissibility in court (for major brands).
  - Dedicated technical support.
  - Strict quality control for forensic accuracy.
  - Often comes with an easy point-and-click graphical user interface.
  - Better documentation.
  - Greater availability of training and supplemental materials.
Computer Forensic Tools: Software

- Disadvantages of commercial forensic software:
  - High initial cost.
  - Cost of annual licensing / maintenance.
  - Licensing often done through USB keys or “dongles” which can be lost or damaged.
  - Customer may need to be a member of a restricted group of customers (such as law enforcement or academia) to receive best pricing and functionality.
Computer Forensic Tools: Software

• Advantages of open-source forensic software:
  ▫ Lower initial cost
    • Open-source software is often free.
    • It is possible to create your own forensic software from source code, incorporating only the features you need.
  ▫ Fewer (if any) licensing issues.
Computer Forensic Tools: Software

- Disadvantages of open-source forensic software:
  - Little (if any) vendor support on free software.
  - Perceived as less standardized and reliable, therefore less likely to produce admissible results.
  - Often uses command-line interface instead of the point-and-click interface familiar to Windows users.
Computer Forensic Tools: Software

• What does forensic software do?
  ▫ Disk imaging
  ▫ Data recovery
  ▫ Integrity checking
  ▫ Remote access
  ▫ Password recovery
  ▫ Permanent file deletion
  ▫ Searching and sorting
Computer Forensic Tools: Software

• Commercial Forensic Software: EnCase
  ▫ Manufactured and sold by Guidance Software.
  ▫ Market leader, widely recognized and accepted.
  ▫ Key features include:
    • Court-validated Logical Evidence File format.
    • Advanced search options.
    • Internet and email support.
    • Multiple viewers.
    • Instant message analysis.
    • Support for most system files.
    • Multiple acquisition options.

http://www.guidancesoftware.com
Computer Forensic Tools: Software

• Commercial Forensic Software: Forensic Toolkit
  ▫ Manufactured and sold by AccessData.
  ▫ Commonly known as FTK.
  ▫ FTK is known for:
    • Intuitive functionality.
    • E-mail analysis.
    • Customizable data views.
    • Stability.

http://www.accessdata.com
Computer Forensic Tools: Software

• Commercial forensic software: P2 Commander
  ▫ Manufactured and sold by Paraben.
  ▫ Comprehensive digital forensic examination tool that includes these programs:
    • E-mail Examiner
    • Network E-mail Examiner
    • Forensic Sorter
    • Chat Examiner
    • Advanced Registry & System Analyzer
    • Text Searcher

http://www.paraben.com
Computer Forensic Tools: Software

• Commercial forensic software: Device Seizure
  ▫ Manufactured and sold by Paraben.
  ▫ Recovers data from over 2,200 mobile devices, including mobile phones, smartphones, and iPhones.
    • Calls received, dialed, and missed
    • E-mail
    • Text message history
    • Deleted text messages
    • Phonebook

http://www.paraben.com
Computer Forensic Tools: Software

Paraben *Device Seizure*

[Image of Paraben's Device Seizure software interface]

http://www.paraben.com
Computer Forensic Tools: Software

- **Open-source Forensic Software: Helix**
  - Manufactured by e-fense.
  - Linux-based collection of forensic applications with a unique graphical user interface.
  - Can be used on PCs running Windows, Linux, and Mac OS.
  - Originally a free download, authorized copies of Helix are now available by subscription to the e-fense Forum, which provides Helix support and training.
Computer Forensic Tools: Software

Drive imaging in Helix:

http://www.e-fense.com
Computer Forensic Tools: Software

Device

http://www.e-fense.com
Computer Forensic Tools: Software

Volatile data acquisition in Helix:

http://www.e-fense.com

http://www.abchs.com
Computer Forensic Tools: Software

- SleuthKit and Autopsy
  - SleuthKit is a set of Unix-based forensics tools.
  - Autopsy is the graphical front end for SleuthKit.

- Download SleuthKit and Autopsy at www.sleuthkit.org
Computer Forensic Tools: Software

- **dtSearch**
  - The dtSearch product line can instantly search terabytes of text across a desktop, network, Internet or Intranet site.
  - Highlights “hits” in HTML while displaying embedded images.

Available from
dtSearch Corp.
www.dtsearch.com
Computer Forensic Tools: Software

- SMART
  - SMART is another excellent Linux distribution designed for incident response and forensic analysis.
  - When used as a bootable forensic CD, SMART will not automatically mount file systems, activate swap partitions, or otherwise change data on the target computer.
  - SMART Linux is available at www.asrdata.com
Computer Forensic Tools: Software

• Analysis of connected storage devices using SMART:

SMART Linux
www.asrdata.com
Computer Forensic Tools: Software

- Data acquisition using SMART:
  - SMART will create a bit-for-bit copy of the target drive

SMART Linux
www.asrdata.com
Computer Forensic Tools: Software

- Data authentication using SMART:
  - A good forensic program will compute a hash value to assure integrity of the evidence

SMART Linux
www.asrdata.com
Computer Forensic Tools: Software

- **NFI Defraser**
  - Defraser detects and restores complete and partial multimedia files, from places that are typically invisible to the Windows file system (such as unallocated disk space).
  - Developed by the Netherlands Forensic Institute.
  - Download NFI Defraser at defraser.sourceforge.net
Computer Forensic Tools: Software

- **guymager**
  - A Linux-based forensic imaging platform.
  - User-friendly graphical interface, multi-language support.

Disk acquisition in guymager:
Computer Forensic Tools: Software

- **DEFT: Digital Evidence and Forensics Toolkit**
  - DEFT is a Xubuntu Linux-based live CD which includes many popular and useful utilities for computer forensics, incident response, penetration testing, and security analysis.

  - Download DEFT from www.deftlinux.net
Computer Forensic Tools: Software

- **DEFT: Digital Evidence and Forensics Toolkit**

![DEFT Digital Evidence and Forensics Toolkit](image)
Computer Forensic Tools: Software

- **DEFT**: Digital Evidence and Forensics Toolkit

Also available: *DEFT Extra*

DEFT tools in a Windows graphical interface
Computer Forensic Tools: Software

• Standards and Testing
  ▫ How do we know if our forensic software is good?
  ▫ The National Institute of Standards and Technology tests forensic software and hardware through its Computer Forensics Tool Testing Project.
  • Download CFTT test results and thousands of pages of related NIST research at www.cftt.nist.gov
Computer Forensic Tools: Software

• Standards and Testing
  ▫ Whether commercial or open-source, forensic software should meet these criteria:
    • Should be accepted by law enforcement, security professionals, and the legal community.
    • Should be able to export image files to multiple platform formats.
    • Should have efficient storage capabilities.
    • Should be fully functional when launched from portable computing platforms (such as laptops).
Incident Response
Incident Response

- **Incident response** happens BEFORE the forensic analysis begins.
  - Incident response is the response to a computer crime, security policy violation, or similar event.
  - Digital evidence is secured, preserved, and documented in this phase.
  - The incident responder is not necessarily the forensic specialist who will conduct the analysis of the digital evidence.
Incident Response

• In a large corporate setting, the incident responder might be a technician-level employee in security or information technology.
• In a smaller company, the network administrator or security officer might also be the incident responder in addition to performing several other duties.
Incident Response

• In the case of a criminal investigation, a sworn law enforcement officer or “crime lab” technician typically has incident responder responsibilities.

• There is always the possibility that law enforcement personnel will be called in after corporate personnel have done their own incident response. Be prepared to deal with an incident scene that may have been compromised.
Incident Response

The U.S. Department of Justice has published much research about incident response (through its National Institute of Justice programs).

The NIJ’s *Electronic Crime Scene Investigation: A Guide for First Responders* has many helpful guidelines.
Incident Response

- Incident Response – *What’s the rush?*
  - Even a brief delay in the start of an investigation could give a criminal suspect time to erase, hide, or destroy digital evidence.
Incident Response

- Incident response – *What’s the rush?*
  - In the workplace, delayed incident response greatly increases the likelihood of data being altered by another computer user or by background processes like automatic software updates, disk utilities, or data backups.
Incident Response

- National Institute of Justice guidelines for dealing with digital evidence:
  - Actions taken to secure and collect digital evidence should not affect the integrity of that evidence.
  - Persons conducting an examination of digital evidence should be trained for that purpose.
  - Activities relating to the seizure, examination, storage, or transfer of digital evidence should be documented, preserved, and available for review.
Incident Response

- Depending on the availability of investigative personnel, the incident responder may be called upon to:
  - Recognize, identify, seize, and secure all digital evidence at the scene.
  - Document the entire scene and the specific location of the evidence found.
  - Collect, label, and preserve the digital evidence.
  - Package and transport digital evidence in a secure manner.
Incident Response

- Unauthorized seizure can be a criminal offense!
- Before attempting a device seizure, be sure you have a search warrant or are covered by corporate policy or similar authority.
Incident Response

National Institute of Justice

Computer Evidence Worksheet

www.ojp.usdoj.gov/ni/j/
Incident Response

• Guidelines for First Responders
  ▫ Until the incident scene is secured, do nothing that will alter the condition of any electronic device.
    • If the computer is on, LEAVE IT ON.
    • If the computer is off, LEAVE IT OFF.
  ▫ Politely but firmly resist offers of technical help from anyone who is not authorized to assist in the investigation.
Incident Response

• Guidelines for First Responders
  ▫ “Pull the Plug” vs. “Shut Down”
    • Pulling the plug immediately halts processing, but destroys anything in memory and can corrupt files.
    • Shutting down protects files from corruption, but writes entries into the systems activity logs and therefore changes the state of the evidence.
Incident Response

- Guidelines for First Responders
  - “Pull the Plug” vs. “Shut Down”
    - Forensic tools designed specifically for incident response may provide an option for a more reliable capture of digital evidence by keeping a computer’s memory “alive” long enough to be analyzed.
Incident Response

• Guidelines for First Responders
  • Take the appropriate measures to avoid compromising fingerprints, blood, DNA, and other physical evidence left on mice and keyboards.
  • Protect your own health and safety:
    • A crime scene may contain blood or other biohazards.
    • Some electrical and electronic equipment can hold an electrical charge even when unplugged.
    • Lasers in CD/DVD drives and laser printers can cause eye injury.
Incident Response

• Guidelines for First Responders
  • Look for signs of active communications with other computers, such as chat room activity or instant messaging.
  • Look for network hardware such as routers or wireless access points that may point to additional evidence elsewhere on the network.
Incident Response

• **Investigative Questions (General)**
  • When and where was the computer purchased? Was it new or used?
  • Who has access to the computer hardware and software?
  • Where is the removable media stored? (CDs, DVDs, floppy disks, USB drives, backup tapes, etc.)
  • Whose fingerprints might be found on the removable media?
Incident Response

- Investigative Questions (General)
  - How may people use this computer? Who are they?
  - What are their usernames?
  - At what times of the day do the individual users have access to the computer?
  - If more than one person uses this computer, can all the users access every file, folder, and program?
  - What is the level of computer experience or expertise of each user of the computer?
Incident Response

- Investigative Questions (General)
  - How does the computer access the Internet? (Cable, DSL, dial-up, office LAN, etc.)
  - Does the suspect or victim have an e-mail account? What is their e-mail address?
  - Who is the Internet service provider and/or e-mail service provider?
  - Which e-mail client (such as Outlook) does the suspect or victim use?
Incident Response

- **Investigative Questions (General)**
  - Does the suspect or victim use remote access software (such as PC Anywhere or GoToMyPC?)
  - Do any users of the computer use online storage or remote storage?
  - Has any software (such as Evidence Eliminator) been used to “clean” the computer or wipe the hard drive?
  - Does the computer contain encryption software?
  - Is the computer always left on? If it is turned off when not in use, how often does that happen?
Incident Response

• Investigative Questions (Identity Theft & Financial Crime *Victims*)
  • Are you aware of any unusual activity on your bank accounts or credit cards?
  • What accounts have been compromised?
  • Have you given personal information to any person or organization?
  • Do you pay your bills online?
  • Have any bank statements or bills not arrived in regular mail when you expected them?
Incident Response

- Investigative Questions (Identity Theft & Financial Crime *Suspects*)
  - Does the computer contain any software for making financial documents such as checks?
  - Does the computer contain any software for making counterfeit driver’s licenses or other identification?
  - Does the computer contain any software for scanning and manipulating photographs?
  - Has the computer been used to purchase anything online?
Incident Response

• Investigative Questions (Child Exploitation Victims)
  • Has the victim been in any online chat rooms?
  • Did the victim give any information to anyone online indicating their true name, age, and location?
  • Has the victim received any pictures or gifts from the suspect?
  • Who is on the victim’s chat room “buddy lists”?
  • Does the victim use any social networking sites such as Facebook or MySpace?
Incident Response

• Investigative Questions (Child Exploitation Suspects)
  • Has the suspect been in any online chat rooms?
  • What is the suspect’s chat room name or online identity?
  • Who is on the suspect’s chat room “buddy lists”?
  • Does the suspect use any social networking sites such as Facebook or MySpace?
  • Does the suspect use more than one computer? Where are those computers?
Incident Response

• Investigative Questions (Hacking and Intrusions)
  • Who first observed the illegal activity?
  • Are any employees or former employees considered suspects?
  • Who is the network administrator?
  • Is there a diagram of the network available?
  • Are computer and server logs available? Are the logs current?
  • Can the logs be immediately secured to prevent access by suspects?
Incident Response

• Evidence on Storage Devices – What to Look For
  ▫ Internal hard drives
  ▫ External hard drives
  ▫ USB drives (thumb drives)
  ▫ Removable media
    • CD-ROM and CD-RW
    • DVD and DVD+R / DVD-R
    • Floppy disks and Zip disks
    • Memory cards
### Hard Drive Evidence Worksheet

<table>
<thead>
<tr>
<th>Hard Drive #1 Parameter Information</th>
<th>Hard Drive #2 Parameter Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOS Disk</td>
<td>PTABLE</td>
</tr>
<tr>
<td>Capacity</td>
<td>Cylinders</td>
</tr>
<tr>
<td>Ctrl REV</td>
<td></td>
</tr>
<tr>
<td>IDE</td>
<td>50 Pin SCSI</td>
</tr>
<tr>
<td>Jumper</td>
<td>Master</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hard Drive #1 Label Information</th>
<th>Hard Drive #2 Label Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Model</td>
</tr>
<tr>
<td>Not Available</td>
<td>Not Available</td>
</tr>
</tbody>
</table>

**Incident Response**

National Institute of Justice

*Hard Drive Evidence Worksheet*

[www.ojp.usdoj.gov/ni](http://www.ojp.usdoj.gov/ni)
Incident Response

• Evidence on Handheld Devices – What to Look For
  ▫ Mobile phones are the obvious choice, but don’t forget...
    • Personal Digital Assistants
    • iPod and other .mp3 media players
    • Pagers
    • Digital cameras
    • Global Positioning System (GPS) receivers
Incident Response

- Evidence on Peripheral Devices – What to Look For
  - Keyboards and mice
  - Webcams
  - Microphones
  - Memory card readers
  - USB and FireWire hubs
  - Voice over IP (VoIP) devices (Vonage, Magic Jack)
Incident Response

• Evidence from Other Sources – What to Look For
  ▫ Digital cameras
  ▫ Video cameras
  ▫ Digital video recorders (TiVo)
  ▫ Digital audio recorders
  ▫ Video game consoles
  ▫ Fingerprint/thumbprint reader
  ▫ Satellite receiver and access cards
Incident Response

- Evidence from Other Sources – What to Look For
  - Network hubs
  - Network switches
  - Wireless access points
  - Modems (phone / cable / DSL / ISDN)
  - Wireless cards and antennas
Incident Response

• Evidence from Other Sources – What to Look For
  ▫ Network information may available from a network administrator.
  ▫ If this information can be obtained without compromising the suspect PC, it would be helpful to know:
    • IP (Internet protocol) address
    • Domain name server (DNS) information
Incident Response

• Example: Internet Abuse by Employees
  ▫ An employee is surfing inappropriate Web sites, sending malicious e-mails, or “moonlighting” using a company-owned PC during the workday.
Incident Response

- Example: Internet Abuse by Employees
  - You suspect that the employee is using a workplace PC for more serious activity, such as stealing trade secrets or leaking confidential information, via e-mail or blog postings.
Incident Response

• Example: Internet Abuse by Employees
  ▫ Assuming that a corporate security policy is in place warning employees that their computer use can be monitored and recorded, what evidence should you look for?
    • The offending e-mails, including headers
    • E-mail server logs
    • Web server logs
    • Web URL information from browser history, bookmarks/favorites, and cache
Computer Investigations

• The goal of a successful computer forensics investigation is to gather *admissible* evidence of a crime, security policy violation, or similar incident.

• This evidence might be located on a suspect’s computer, peripheral devices, on a network, or some combination of these.
A fundamental concept of digital forensics is to work from a **copy** of the data you’re investigating (whenever possible) instead of the original source.

The ability to make an exact **bit-for-bit** copy of a hard disk or (similar storage device) is a common feature of forensic software packages such as EnCase and Helix.
Computer Investigations

• Why not just copy the files or “back up” the files?
  ▫ For a forensically pure copy of the data, the investigator must use a process that does not write any information to the suspect hard drive.
  ▫ The simple act of booting into Windows will alter the contents of the hard drive.
Computer Investigations

• Why not just copy the files or “back up” the files?
  ▫ Working within Windows, Mac OS, or Linux/Unix operating systems will alter timestamps, logs, and other data, leaving clues that the investigator was there.
  ▫ Simply copying the files from the target computer will not capture data held in “slack space” or other areas not seen by the operating system.
The Association of Chief Police Officers (UK) offers some good advice on digital forensic investigations.
Computer Investigations

• ACPO Principle #1:
  “No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.”
Computer Investigations

- ACPO Principle #2:
  “In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.”
Computer Investigations

- ACPO Principle #3:
  “An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.”
Computer Investigations

• ACPO Principle #4:
  “The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.”
Computer Investigations

• Some basic steps to begin the investigation:
  ▫ Photograph and/or videotape the computer and surrounding area \textit{before} unplugging any cables or power cords.
  ▫ Photograph whatever data is on the monitor.
  ▫ Draw a diagram detailing locations of peripherals and how they are connected to the PC.
  ▫ Look for removable media stored nearby, such as CDs, DVDs, and USB drives.
Computer Investigations

• Some basic steps to begin the investigation:
  ▫ Look for and document connections to networks, servers, and offsite file storage.
  ▫ Look for written notes containing passwords or Web site URLs.
  ▫ Note the presence of computer books, manuals, software packaging, and other items that may give a clue as to how the computer was used.
  ▫ Determine the time of the last access to the PC.
Computer Investigations

• Always think “admissibility” – *document everything*, record all actions, decisions, and results promptly and properly, with the assumption that you may be called upon in court to explain and justify your findings.
Computer Investigations

• What would render your evidence inadmissible?
  ▫ Illegal or inappropriate seizure because of a lack of a proper search warrant or corporate authority.
  ▫ Booting into the computer’s operating system and “poking around” for evidence.
  ▫ Violation of the chain of custody concept, causing doubts about who had access to the evidence at all times.
Computer Investigations

• Chain of Custody
  ▫ Establishes the integrity of the evidence-handling process.
  ▫ Proves continuity of the possession of evidence by means of a written record.
    • The location of evidence should be traceable from its original point of seizure or collection through the analysis phase to the time it is presented in court or returned to its owner.
Computer Investigations

• Chain of Custody
  ▫ Answers the questions:
    • Where has this evidence been?
    • Who has had access to this evidence?
    • What has been done to this evidence?
    • Has this evidence been left unattended?
    • Has this evidence been subject to tampering?
Computer Investigations

• What goes in the chain of custody log?
  • Case number and item number (or tag number).
  • Date, time, and location the item was seized.
  • Who the item was seized from.
  • Who originally collected the evidence.
Computer Investigations

• What goes in the *chain of custody* log?
  • Full name and signature of the person who receives the evidence.
  • Description of the evidence including brand name, model name or number, and serial number.
  • Hash values.
Computer Investigations

• Handling Digital Evidence
  ▫ Each link of the *chain of custody* must ensure that evidence remains unaltered.
  ▫ Use *standardized* and *repeatable* processes and documentation.
  ▫ Whether your investigation takes place in the field or in the lab, your goal is to leave the state of the target (suspect) computer as *undisturbed* as possible.
Computer Investigations

• When handling and processing digital evidence, *documentation* is critical.
  ▫ Evidence log entries should be written in ink, and logs should be kept in bound volumes to ensure pages are not removed.
  ▫ Record all evidence collection procedures in evidence logs at the time the evidence is collected; do not rely on your memory.
Computer Investigations

• Always conduct your investigation with data integrity in mind.
  ▫ You may be called upon to answer these questions about the evidence you have collected:
    • How is the original source being protected?
    • How was it acquired?
    • How was it copied (mirrored)?
    • Did you change the original data in any way? Are you sure?
  ▫ Answering “I don’t know” to any of these questions may get your evidence ruled inadmissible or invalid.
Computer Investigations

• The Investigator’s Report
  ▫ All the important facts and conclusions from the investigation should be documented and clearly presented.
  ▫ What did you learn in the investigation, and what are the next steps to be taken?
    • Discovery methods
    • Personnel involved
    • Exact sequence of events
    • System events
    • Actions taken with documented times
    • Preventative measures resulting from the investigation
    • Recovery steps taken and further recommendations
Computer Investigations

• Analyzing a Completed Investigation
  ▫ With the investigation complete, is it same to resume normal operations?
  ▫ What went well, what needs improvement, and what are the investigator’s next steps?
  ▫ Did our investigation reveal weaknesses in our network security or physical security?
  ▫ Are there regulatory issues? Did we break any laws or rules in this investigation? Will we be fined or penalized?
  ▫ Will more training, tougher standards, or better policy prevent a recurrence of the initial cause of the investigation?
Computer Investigations

• Handling Digital Evidence
  ▫ Digital forensic investigators should work in teams of two, with one person performing analysis and the other handling documentation.
  ▫ One person designated as Evidence Custodian should know the location of evidence at all times and should be the keeper of locks, combinations, and other physical controls.
  ▫ Evidence Custodian records all receipts and transfers; no evidence enters or leaves without documentation.
Computer Investigations

• Handling Digital Evidence
  ▫ When restoring evidence files, always restore to a hard drive or similar media with the same file system as the original drive (NTFS drive restored to NTFS, FAT 32 restored to FAT 32, etc.).
  ▫ Always be prepared to demonstrate, through MD5 or a similar hashing function, that your investigation has not added data to (or removed data from) the original source of evidence.
Forensics Over the Network
Forensics Over the Network

• **Network Forensics**
  ▫ Systematic tracking of incoming and outgoing traffic:
    • To ascertain how an attack was carried out or how an event occurred on a network.

• **Determine the cause of the abnormal traffic.**
  ▫ Internal threat: system malfunction or bug
  ▫ External threat: attackers and hackers
Forensics Over the Network

- Intruders leave clues that can be uncovered with event logging and good audit procedures.
Forensics Over the Network

• **A well-defended network is arranged in layers.**
  ▫ Hide the most valuable data at the innermost part of the network, to deny easy access by attackers.

• **Defense in depth (DiD)**
  ▫ Modes of protection:
    • People
    • Technology
    • Operations
Forensics Over the Network

• A Network Forensic Procedure: Live Acquisition
  ▫ Live acquisitions are especially useful when dealing with active network intrusions or attacks.
Forensics Over the Network

- A Network Forensic Procedure: Live Acquisition
  - Live acquisitions might not follow typical forensics procedures.
  - Data in memory (RAM) and certain temporary files will be lost when a computer is turned off, so it is vital to capture the most “perishable” data first.
Forensics Over the Network

- Create or download a bootable forensic CD.
- Keep a log of all your actions.
- Send the acquired data to a clean network drive.
- Copy the physical memory (RAM).
- Obtain a hash value of all files you recover, to demonstrate that you have not altered their content.
Forensics Over the Network

- Helix is an excellent choice for the bootable forensic CD used over the network.
- Helix operates in two modes:
  - Windows Live (GUI or command line) and bootable Linux.
- The Windows Live GUI version includes a runtime prompt for accessing the command line.
  - The graphical user interface will use more resources than the command line interface.
Forensics Over the Network

- Live Acquisition of Physical Memory Using Helix
  - Output is directed to the investigator’s workstation across the network for analysis.

Helix

www.e-fense.com
Forensics Over the Network

- **Network Forensic Procedure**
  - Always use a standard installation image for systems on a network.
  - Close any way in after an attack.
  - Attempt to retrieve all volatile data.
  - Acquire all compromised drives.
  - Compare files on the forensic image to the original installation image.
Forensics Over the Network

• Packet sniffer
  ▫ Also known as a packet analyzer.
  ▫ Can be either hardware or software that can monitor a network, identify network traffic, and analyze the content.
Forensics Over the Network

- **Wireshark: A Well-known Packet Sniffer**
  - Formerly known as Ethereal, it was renamed due to trademark issues.

Wireshark
www.wireshark.org
Forensics Over the Network

• Sysinternals
  ▫ A collection of free tools for analysis of PCs running Windows.
Forensics Over the Network

- These Sysinternals tools (from the PsTools suite) may be of particular interest to the forensic analyst.
  - **PsPasswd** changes account passwords.
  - **PsSuspend** suspends processes.
  - **PsLoggedOn** shows who’s logged locally.
  - **PsGetSid** displays security identifier (SID).
Where to Learn More
Where to Learn More

• Computer Crime and Intellectual Property Section, U.S. Department of Justice:
  http://www.cybercrime.gov
• Federal Rules of Evidence:
  http://federalevidence.com/rules-of-evidence
• International High Technology Crime Investigation Association:
  http://www.htcia.org/
• Forward Edge II, U.S. Secret Service:
  http://www.forwardedge2.com/
Where to Learn More

- Guidance Software (EnCase): http://www.guidancesoftware.com
- AccessData Corporation (Forensic Toolkit): http://www.accessdata.com
- e-fense (Helix): http://www.e-fense.com
Where to Learn More

- Internet Crimes Against Children Task Force:  
  http://www.icactraining.org/default.htm
- Forensic Focus:  
  http://www.forensicfocus.com/
- Security Distro:  
  http://www.securitydistro.com
- Hackin9 Magazine:  
References

References


