MODULE - 1

Overview of Digital Forensics – Digital Investigations – Professional Conduct – Digital Forensics Investigation – Private Sector High Tech Investigations – Data Recovery Workstations and Software – Conducting an Investigation.

Digital Forensics

Digital forensics is the process of storing, analyzing, retrieving, and preserving electronic data that may be useful in an investigation. It includes data from hard drives in computers, mobile phones, smart appliances, vehicle navigation systems, electronic door locks, and other digital devices. The process's goal of digital forensics is to collect, analyze, and preserve evidence.

Steps of Digital Forensics

Identification

This is the initial stage in which the individuals or devices to be analyzed are identified as likely sources of significant evidence.

Preservation

It focuses on safeguarding relevant electronically stored information (ESI) by capturing and preserving the crime scene, documenting relevant information such as visual images, and how it was obtained.

Analysis

It is a methodical examination of the evidence of the information gathered. This examination produces data objects, including system and user-generated files, and seeks specific answers and points of departure for conclusions.

Documentation

These are tried-and-true procedures for documenting the analysis's conclusions, and they must allow other competent examiners to read through and duplicate the results.

Presentation

The collection of digital information, which may entail removing electronic devices from the crime/incident scene and copying or printing the device(s), is critical to the investigation.

Objectives of Digital Forensics

Knowing the primary objectives of using digital forensics is essential for a complete understanding of what is digital forensics:

- It aids in the recovery, analysis, and preservation of computers and related materials for the investigating agency to present them as evidence in a court of law
- It aids in determining the motive for the crime and the identity of the primary perpetrator
- Creating procedures at a suspected crime scene to help ensure that the digital evidence obtained is not tainted
- Data acquisition and duplication: The process of recovering deleted files and partitions from digital media in order to extract and validate evidence

- Assists you in quickly identifying evidence and estimating the potential impact of malicious activity on the victim
- Creating a computer forensic report that provides comprehensive information on the investigation process
- Keeping the evidence safe by adhering to the chain of custody

Types of Digital Forensics

As digital data forensics evolves, several sub-disciplines emerge, some of which are listed below

Computer Forensics

It analyzes digital evidence obtained from laptops, computers, and storage media to support ongoing investigations and legal proceedings.

Mobile Device Forensics

It entails obtaining evidence from small electronic devices such as personal digital assistants, mobile phones, tablets, sim cards, and gaming consoles.

Network Forensics

Network or cyber forensics depends on the data obtained from monitoring and analyzing cyber network activities such as attacks, breaches, or system collapse caused by malicious software and abnormal network traffic.

Digital Image Forensics

This sub-specialty focuses on the extraction and analysis of digital images to verify authenticity and metadata and determine the history and information surrounding them.

Digital Video/Audio Forensics

This field examines audio-visual evidence to determine its authenticity or any additional information you can extract, such as location and time intervals.

Memory Forensics

It refers to the recovery of information from a running computer's RAM and is also known as live acquisition.

Challenges Faced by Digital Forensics

Due to the evidentiary nature of digital forensic science, rigorous standards are required to withstand cross-examination in court.

Challenges faced by digital forensics are:

- Extracting data from locked, or destroyed computing devices is one of the challenges that digital forensic investigators face

- Finding specific data entries within massive amounts of data stored locally or in the cloud
- Keeping track of the digital chain of custody
- Ensuring data integrity throughout an investigation

Advantages of Digital Forensics

- Enables Digital Evidence Analysis

Computer forensics uses investigation and analysis techniques to collect and preserve evidence from a specific computing device to present it in court.

- Aids in the Identification of Criminals

Law enforcement officers can frequently track down suspects and piece evidence together to prosecute them by analyzing data on computers and other digital devices.

- It Is Capable of Recovering Deleted Data

One advantage of using computer forensics to recover deleted data is that it is relatively simple to do. Most of the time, all you need is the right software and a little know-how.

- Enlightens on How Crimes Are Committed

Computer forensics can shed light on how crimes are committed by analyzing digital evidence.

- It Has the Potential to Be Used to Prevent Future Crimes

Law enforcement can better target their investigative efforts if they understand how criminals use computers to commit crimes.

Disadvantages of Digital Forensics

The following are some disadvantages of digital forensics:

- Prolonged Procedure

Computer forensics is a lengthy process. Data collection and analysis can take days or weeks.

- Requires Specialized Knowledge and Skills

Computer forensics is a process that collects, examines, and reports digital evidence using specialized skills and knowledge.

- Can Be Costly

Computer forensics can be costly because it requires specialized equipment and software and is frequently performed by a specialist.

- Obtaining Evidence May Necessitate a Court Order

Obtaining the evidence may necessitate a court order. It means there could be a delay in getting the evidence, giving the perpetrator time to destroy or tamper with it.

- Evidence Can Be Easily Destroyed or Manipulated

One of the most severe issues with computer forensics is the ease with which evidence can be destroyed or tampered with. Even if investigators successfully recover deleted files or damaged hard drives, there is no guarantee that the evidence has not been tampered with.

History of Digital Forensics

The term "digital forensics" is relatively new, having first appeared in the late 1900s after being known as "computer forensics." The first group of computer forensic analysts consisted of law enforcement officers who enjoyed playing with computers. The Federal Bureau of Investigation (FBI) established the Computer Analysis and Response Team (CART) in 1984, followed by the Metropolitan Police in the United Kingdom a year later.

At the turn of the century, law enforcement, investigators, and specialists recognized the need for standard techniques, procedures, and protocols in digital forensics and other forensic sciences. Many informal guidelines were used until discussions and conferences were held to establish computer forensic methodology and practices on what computer forensics is today.

Phases of Digital Forensics

The following are the phases of digital forensics:

Phase I - Initial Response

The first response is the action taken immediately following a security incident. The nature of the incident heavily influences it.

Phase II - Seizure and Search

During this phase, the professionals look for the devices used in the crime. These devices were then carefully seized to extract information from them.

Phase III - Gather Evidence

Following the search and seizure phase, professionals collect data using the acquired devices. They have well-defined forensic methods for handling evidence.

Phase IV: Protect the Evidence

The forensic team should have access to a secure location where they can store the evidence. They determine whether the information gathered is correct, authentic, and accessible.

Phase V - Data Collection

Data acquisition is when Electronically Stored Information (ESI) from suspected digital assets is retrieved. It aids in gaining insights into the incident, whereas an improper process can alter the data, jeopardizing the evidence's integrity.

Phase VI - Data Analysis

The accountable staff scans the acquired data to identify the evidentiary information that can be presented to the court during data analysis. This phase involves examining, identifying, separating, converting, and modeling data to convert it into useful information.

Phase VII - Evidence Evaluation

The evidence assessment process connects the evidential data to the security incident. Based on the scope of the case, a thorough assessment should be performed.

Phase VIII - Reporting and Documentation

It is the post-investigation phase, which includes reporting and documenting all findings. In addition, the report should contain sufficient and acceptable evidence following the court of law.

Phase IX - Testify as an Expert Witness

Forensic investigators should approach the expert witness to confirm the evidence's accuracy. An expert witness is a professional who investigates a crime to obtain evidence.

What Are Digital Forensics Tools?

Digital forensic tools were developed to examine data on a device without causing damage to it. Digital forensic tools can also assist ICT managers in proactively identifying risk areas. Digital forensic tools are currently classified as digital forensic open-source tools, digital forensic hardware tools, and various others.

Popular instruments include:

- Forensic disc controllers: enable the investigator to read the data from a target device while preventing it from being modified, corrupted, or erased.
- Hard-drive duplicators: enable the investigator to copy data from a suspect thumb drive, hard drive, or memory card to a clean drive for analysis.
- Password recovery devices: crack password-protected storage devices using machine learning algorithms.

Here are some of the most popular digital investigation tools:

- The SleuthKit
- OSForensic
- FTK Imager
- Hex Editor Neo
- Bulk Extractor

Overview of Digital Forensics

The definition of **digital forensics** has evolved over the years from simply involving securing and analyzing digital information stored on a computer for use as evidence in civil, criminal, or administrative cases.

The former director of the Defense Computer Forensics Laboratory, Ken Zatyko, wrote a treatise on the many specialties including

- computer forensics,
- network forensics,
- video forensics, and
- a host of others.

Digital forensics is also different from **data recovery**, which involves retrieving information that was deleted by mistake or lost during a power surge or server crash,for example.

Digital forensics is the task of recovering data that users have hidden or deleted, with the goalof ensuring that the recovered data is valid so that it can be used as

evidence. In this regard, digital forensics differs from other types of evidence recovered from a scene. When investigators in a crime scene unit retrieve blood or hair or bullets, they can identify what it is. When a laptop, smartphone, or other digital device is retrieved, its contents are unknown and pose a challenge to the examiner.

The evidence can be
Inculpatory evidence(in criminal cases, the expression is "incriminating")or
Exculpatory evidence, meaning it tends to clear the suspect.

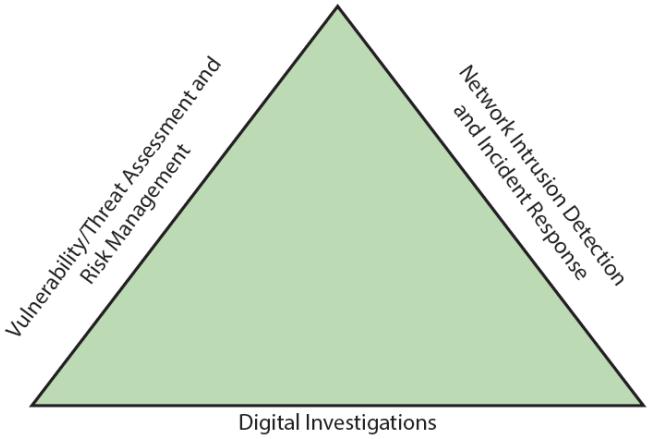


Figure shows the investigations triad made up of these functions:

• Vulnerability/threat assessment and risk management
• Network intrusion detection and incident response
• Digital investigations

Each side of the triad in the figure represents a group or department responsible for performing the associated tasks. Although each function operates independently, all three groups draw from one another when a large-scale digital investigation is being conducted.
By combining these three groups into a team, all aspects of a digital technology investigation can be addressed without calling in outside specialists. In smaller companies, one group might perform all the tasks shown in the investigations triad, or a small company might contract with service providers to perform these tasks.

Vulnerability/threat assessment and risk management

In this group, you test and verify the integrity of stand-alone workstations and network servers. This integrity check covers the physical security of systems and the security of operating systems (OSs) and applications. People working in this group called as penetration testers test for vulnerabilities of OSs and applications used in the network and conduct authorized attacks on the network to assess vulnerabilities.

Typically, people performing this task have several years of experience in system administration. Their job is to poke holes in the network to help an organization be better prepared for a real attack.

Network intrusion detection and incident response.

This group detects intruder attacks by using automated tools and monitoring network firewall logs. When an external attack is detected, the response team tracks, locates, and identifies the intrusion method and denies further access to the network. If an intruder launches an attack that causes potential damage, this team collects the necessary evidence, which can be used for civil or criminal litigation against the intruder and to prevent future intrusions.

If an internal user is engaged in illegal acts or policy violations, the network intrusion detection and incident response group might assist in locating the user.

For example, someone at a community college sends e-mails containing a worm to other users on the network. The network team realizes the e-mails are coming from a node on the internal network, and the security team focuses on that node.

The **digital investigations** group manages investigations and conducts forensics analysis of systems suspected of containing evidence related to an incident or a crime. For complex casework, this group draws on resources from
personnel in

- vulnerability assessment,
- risk management, and
- network intrusion detection and incident response.

Digital Investigations

Digital investigations can be categorized several ways.
There are two main categories:

- public-sector investigations and
- private-sector investigations

In general, public-sector investigations involve government agencies responsible for criminal investigations and prosecution.
Government agencies range from municipal, county, and state or provincial police departments to federal law enforcement agencies.
These organizations must observe legal guidelines of their jurisdictions.

Private-sector investigations focus more on policy violations, such as not adhering to Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations. However, criminal acts, such as corporate espionage, can also occur. So although private-sector investigations often start as civil cases, they can develop into criminal cases likewise, a criminal case can have implications leading to a civil case. If

you follow good forensics procedures, the evidence found in your examinations can make the transition between civil and criminal cases.

Legal Investigation:

Not every police officer is a computer expert. Some are computer novices; others might be trained to recognize what they can retrieve from a computer disk.

To differentiate the training and experience officers have

ISO standard 27037 (*www.iso.org/standard/44381.html*) defines two categories:

Digital Evidence First Responder (DEFR):

A DEFR has the skill and training to arrive on an incident scene, assess the situation, and take precautions to acquire and preserve evidence.

Digital Evidence Specialist (DES)

A has DES the skill to analyze the data and determine when another specialist should be called in to assist with the analysis.

Understanding Private-Sector Investigations

Private-sector investigations involve private companies and lawyers who address company policy violations and litigation disputes, such as wrongful termination. When conducting an investigation for a private company, remember that business must continue with minimal interruption from your investigation. Because businesses usually focus on continuing their usual operations and making profits, many in a private-sector environment consider your investigation and apprehension of a suspect secondary to stopping the violation and minimizing damage or loss to the business.

Businesses also strive to minimize or eliminate litigation, which is an expensive way to address criminal or civil issues.

Private-sector computer crimes can involve

e-mail harassment;

gender and age discrimination;

white-collar crimes (defined by the FBI, *www.fbi.gov/investigate/white-collar-crime*), such as falsification of data, Embezzlement, and sabotage; and **industrial espionage**, which involves selling sensitive or confidential company information to a competitor. Anyone with access to a computer can commit these crimes.

Establishing Company Policies

One way that businesses can reduce the risk of litigation is to publish and maintain policies that employees find easy to read and follow.

The most important policies are those defining rules for using the company's computers and networks; this type of policy is commonly known as an "acceptable use policy."

Organizations should have all employees sign this acceptable use agreement.

Published company policies also provide a **line of authority** for conducting internal investigations; it states who has the legal right to initiate an investigation, who can take possession of evidence, and who can have access to evidence.

Well-defined policies give computer investigators and forensics examiners the authority to conduct an investigation.

Without defined policies, a business risks exposing itself to litigation from current or former employees. The person or committee in charge of maintaining company policies must also stay current with applicable laws, which can vary depending on the city, state, and country.

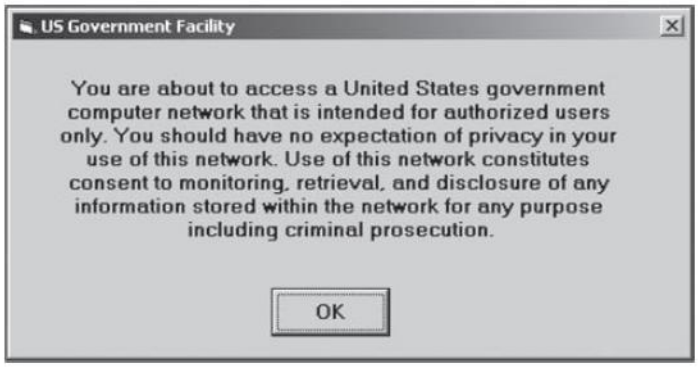
In addition, training and updates on standards and policies should be scheduled regularly to keep employees informed of what should and shouldn't be done on the organization's network.

Displaying Warning Banners

Another way a private or public organization can avoid litigation is to display a warning banner on computer screens.

A **warning banner** usually appears when a computer starts or connects to the company intranet, network, or virtual private network (VPN) and informs end users that the organization reserves the right to inspect computer systems and network traffic at will. (An end user is a person using a computer to perform routine tasks other than system administration.)

If this right isn't stated explicitly, employees might have an assumed right of privacy when using a company's computer systems and network accesses. Figure 1-7 shows a sample warning banner.



A warning banner asserts the right to conduct an investigation and notifies the user. By displaying a strong, well-worded warning banner, an organization owning computer equipment doesn't need a search warrant or court order as required.

Depending on the type of organization, the following text can be used in internal warning banners:

- Access to this system and network is restricted.
- Use of this system and network is for official business only.
- Systems and networks are subject to monitoring at any time by the owner.
- Using this system implies consent to monitoring by the owner.
- Unauthorized or illegal users of this system or network will be subject to discipline or prosecution.
- Users of this system agree that they have no expectation of privacy relating to all activity performed on this system.

Guests, such as employees of business partners, might be allowed to use the system. The text that's displayed when a guest attempts to log on can include warnings similar to the following:

- This system is the property of Company X.
- This system is for authorized use only; unauthorized access is a violation of law and violators will be prosecuted.
- All activity, software, network traffic, and communications are subject to monitoring.

Conducting Security Investigations

Conducting a digital investigation in the private sector is not much different from conducting one in the public sector.

During public investigations, you search for evidence to support criminal allegations. During private investigations, you search for evidence to support allegations of violations of a company's rules or an attack on its assets.

Three types of situations are common in private-sector environments:

1. Abuse or misuse of digital assets
2. E-mail abuse
3. Internet abuse

Maintaining Professional Conduct

Your professional conduct as a digital investigator is critical because it determines your credibility.

Professional conduct, includes

- Ethics,
- Morals, and
- Standards of behavior.

As a professional, you must exhibit the highest level of professional behavior at all times.

To do so, you must

- Maintain objectivity and confidentiality during an investigation,
- Expand your technical knowledge constantly, and

- Conduct yourself with integrity.

Maintaining objectivity means you form opinions based on your education, training, experience, and the evidence in your cases.
Avoid making conclusions about your findings until you have exhausted all reasonable leads and considered the available facts.
Your ultimate responsibility is to find relevant digital evidence. You must avoid prejudice or bias to maintain the integrity of your fact-finding in all investigations.

For example, if you're employed by an attorney, don't allow the attorney's agenda to dictate the outcome of your investigation.

- Your reputation depends on maintaining your objectivity.
- You must also maintain confidentiality.
- Discuss the case only with people who need to know about it, such as other investigators involved in the case or someone in the line of authority.
- All investigations you conduct must be kept confidential, until you're designated as a witness or required by the attorney or court to release a report.
- In the private-sector environment, confidentiality is critical, especially when dealing with employees who have been terminated.
- The agreement between the company and the employee might have been to represent the termination as a layoff
- or resignation in exchange for no bad references.
- If you give case details and the employee's name to others, your company could be liable for breach of contract.
- In some instances, a civil case might become a criminal case, and it could be years before the case finally goes to trial or is settled.
- If an investigator talks about evidence with unauthorized people, the case could be damaged.
- In addition to maintaining objectivity and confidentiality, you can enhance your professional conduct by continuing your training.
- The field of digital investigations and forensics is changing constantly. You should stay current with the latest technical changes in computer hardware and software, networking, and forensic tools.
- You should also learn about the latest investigation techniques you can use in your cases.
- To continue your professional training, you should attend workshops, conferences, and vendor courses. You might also need to continue or enhance your formal education, such as pursuing certifications.

You must update your qualification by an advanced degree, consider graduate-level studies in a complementary area of study, such as business law or e-commerce. Several colleges and universities now offer associate's, bachelor's, and master's degrees and certificate programs in digital forensics.

In addition to education and training, membership in professional organizations adds to your credentials. These organizations often sponsor training and publications on the latest technical improvements and trends in digital forensic examinations.
Also, keep up to date with the most current publications on digital forensics examination tools and techniques.

As a digital investigator and forensics professional, you're expected to maintain **honesty and integrity**.
You must conduct yourself with the highest levels of integrity in all aspects of your life. Any indiscreet actions can embarrass you and give opposing attorneys opportunities to discredit you during your testimony in court or in depositions.

Procedures for Private-Sector High-Tech Investigations

- As an investigator, you need to develop formal procedures and informal checklists to cover all issues important to high-tech investigations.
- These procedures are necessary to ensure that correct techniques are used in an investigation. Use informal checklists to be certain that all evidence is collected and processed correctly.

Some sample procedures that digital investigators commonly use in private-sector high-tech investigations:

- Employee Termination Cases
- Internet Abuse Investigations
- E-mail Abuse Investigations
- Attorney-Client Privilege Investigations
- Industrial Espionage Investigations

Employee Termination Cases

Most investigative work for termination cases involves employee abuse of company resources. Incidents that create a hostile work environment, such as viewing pornography in the workplace and sending inappropriate e-mails, are the predominant types of cases investigated. The following are some key points for conducting an investigation that might lead to an employee's termination. Consult with organization's general counsel and Human Resources Department for specific directions on how to handle these investigations is recommended.

Internet Abuse Investigations

To conduct an investigation involving Internet abuse, you need the following:
• The organization's Internet proxy server logs

• Suspect computer's IP address obtained from your organization's network administrator.
• Suspect computer's disk drive.
• Your preferred digital forensics analysis tool.

The following steps outline the recommended processing of an Internet abuse case:
1. Use the standard forensic analysis techniques and procedures
2. Search for and extract all Web page URLs and other associated information.
3. Contact the network firewall administrator and request a proxy server log, if it's available, of the suspect computer's network device name or IP address for the dates of interest.

Consult with your organization's network administrator to confirm that these logs are maintained and how long the time to live (TTL) is set for the network's IP address assignments using Dynamic Host Configuration Protocol (DHCP).

4. Compare the data recovered from forensics analysis with the network server log data to confirm that they match.
5. If the URL data matches the network server log and the forensic disk examination, continue analyzing the suspect computer's drive data, and collect any relevant photos or Web pages that support the allegation.

If there are no matches between the network server logs, and the forensic examination shows
no contributing evidence, report that the allegation is unsubstantiated.

Before investigating an Internet abuse case, research your state or country's privacy laws. Many countries have unique privacy laws that restrict the use of computer log data, such as network server logs or disk drive cache files, for any type of investigation.

Some state or federal laws might supersede your organization's employee policies.
Always consult with your organization's attorney. For companies with international business operations, jurisdiction is a problem; what's legal in the United States, such as examining and investigating a network server log, might not be legal in Germany, for example.

For investigations in which the network server log doesn't match the forensics analysis that found inappropriate data, continue the examination of the suspect computer's disk drive.

Determine when inappropriate data was downloaded to the computer and whether it was through an organization's intranet connection to the Internet. Employees might have used their employer's laptop computers to connect to their own ISPs to download inappropriate Web content. For these situations, you need to consult your organization's employee policy guidelines for what's considered appropriate use of the organization's digital resources.

E-mail Abuse Investigations

E-mail investigations typically include spam, inappropriate and offensive message content, and harassment or threats.

E-mail is subject to the same restrictions as other computer evidence data, in that an organization must have a defined policy, as described previously. The following list is what you need for an investigation involving e-mail abuse:

- An electronic copy of the offending e-mail that contains message header data; consult with e-mail server administrator
- If available, e-mail server log records; consult with e-mail server administrator to see whether they are available
- For e-mail systems that store users' messages on a central server, access to the server; consult with e-mail server administrator
- For e-mail systems that store users' messages on a computer as an Outlook.pst or .ost file, for example, access to the computer so that you can perform a forensic analysis on it
- Your preferred digital forensics analysis tool

The following steps outline the recommended procedure for e-mail investigations:

1. For computer-based e-mail data files, such as Outlook .pst or .ost files, use the standard forensics analysis techniques and procedures described in this book for the drive examination.
2. For server-based e-mail data files, contact the e-mail server administrator andobtain an electronic copy of the suspect's and victim's e-mail folder or data.
3. For Web-based e-mail (Gmail, for example) investigations, search for Internet keywords to extract all related e-mail address information.
4. Examine header data of all messages of interest to the investigation.

Attorney-Client Privilege Investigations

When conducting a digital forensics analysis under **attorney-client privilege (ACP)** rules for an attorney, you must keep all findings confidential. The attorney you're working for is the ultimate authority over the investigation.

For investigations of this nature, attorneys typically request that you extract all data from drives.

It's your responsibility to comply with the attorney's directions.

The following list shows the basic steps for conducting an ACP case:

1. Request a memo from the attorney directing you to start the investigation. The memorandum must state that the investigation is privileged communication and list your name and any other associates' names assigned to the case.

2. Request a list of keywords of interest to the investigation.

3. After you have received the memorandum, initiate the investigation and analysis. Any findings you made before receiving the memorandum are subject to discovery by the opposing attorney.

4. For drive examinations, make two bit-stream images of the drive, using a different tool for each image. This approach is advisable because every tool has its strengths and weaknesses.

5. Verify the hash values on all files on the original and re-created disks or its image file.

6. Methodically examine every portion of the drive (both allocated and unallocated data areas) and extract all data.

7. Run keyword searches on allocated and unallocated disk space.

8. For Windows OSs, use specialty tools to analyze and extract data from the Registry, such as Access Data Registry Viewer or a Registry viewer program Use the Edit, Find menu option in Registry Editor, for example, to search for keywords of interest to the investigation.

9. For binary files, such as CAD drawings, find the correct program and, if possible, make printouts of the binary file content. If the files are too large, load the specialty program on a separate workstation with the recovered binary files so that the attorney can view them.

10. For unallocated data recovery, use a tool that removes or replaces nonprintable data.

11. Consolidate all recovered data from the evidence bit-stream image into well organized
folders and subfolders. Store the recovered data output, using alogical and easy-to-follow storage method for the attorney or paralegal.

Industrial Espionage Investigations

Industrial espionage cases can be time consuming and are subject to scope creep (time consuming)problems

The following list includes staff you might need when planning an industrial espionage investigation.

- The digital investigator who's responsible for disk forensic examinations

- The technology specialist who is knowledgeable about the suspected compromised technical data
- The network specialist who can perform log analysis and set up network monitors to trap network communication of possible suspects
- The threat assessment specialist (typically an attorney) who's familiar with federal and state laws and regulations related to International Traffic in Arms Regulations(ITAR) or Export Administration

Regulations (EAR) and industrial espionage

Guidelines when initiating an international espionage investigation:

- Determine whether this investigation involves a possible industrial espionage incident, and then determine whether it falls under ITAR or EAR.
- Consult with corporate attorneys and upper management if the investigations must be conducted discreetly.
- Determine what information is needed to substantiate the allegation of industrial espionage.
- Generate a list of keywords for disk forensics and network monitoring.
- List and collect resources needed for the investigation.
- Determine the goal and scope of the investigation; consult with management and the company's attorneys on how much work you should do.
- Initiate the investigation after approval from management, and make regular reports of your activities and findings.

The following are planning considerations for industrial espionage investigations:

- Examine all e-mail of suspected employees, both company-provided e-mail andfree Web-based services.
- Search Internet forums or blogs for any postings related to the incident.
- Initiate physical surveillance with cameras on people or things of interest to the investigation.
- If available, examine all facility physical access logs for sensitive areas, which might include secure areas where smart badges or video surveillance recordings are used.
- If there's a suspect, determine his or her location in relation to the vulnerable resource that was compromised.
- Study the suspect's work habits.
- Collect all incoming and outgoing phone logs to see whether any unique or unusual places were called.

When conducting an industrial espionage case, follow these basic steps:

1. Gather all personnel assigned to the investigation and brief them on the plan and any concerns.
2. Gather the resources needed to conduct the investigation.

3. Start the investigation by placing surveillance systems, such as cameras and network monitors, at key locations.
4. Discreetly gather any additional evidence, such as the suspect's computer drive,and make a bit-stream image for follow-up examination.
5. Collect all log data from networks and e-mail servers, and examine them forunique items that might relate to the investigation.
6. Report regularly to management and corporate attorneys on your investigation's status and current findings.
7. Review the investigation's scope with management and corporate attorneys to determine whether it needs to be expanded and more resources added.

Understanding Data Recovery Workstations and Software

Difference between data recovery and digital forensics

In data recovery, typically, the customer or your company just wants the data back.
In data recovery, you usually know what you're trying to retrieve.

In digital forensics, you might have an idea of what you're searching for, but not necessarily.

To conduct your investigation and analysis, you must have a specially configured PC known as a **forensic workstation**, which is a computer loaded with additional bays and forensics software. Depending on your needs, a forensic workstation can use the following operating systems:

- MS-DOS 6.22
- Windows 95, 98, or Me
- Windows NT 3.5 or 4.0
- Windows 2000, XP, Vista, 7, 8, or 10
- Linux
- Mac OS X and macOS

Of all the Microsoft OSs, the least intrusive (in terms of changing data) to disks is MS-DOS 6.22.
Many older digital forensics acquisition tools work in the MS-DOS environment. These tools can operate from an MS-DOS window in Windows 98 or from the command prompt in Windows 2000 and later. Some of their functions are disabled or generate error messages when run in these OSs, however.Many hardware write-blockers that connect to USB or FireWire ports are on the market.
Several vendors sell write-blockers, including Digital Intelligence Ultra-Kit, Ultra Block, FireFly, FireChief 800, and USB Write Blocker; Wiebe TECH Forensic Drive Dock;
Guidance Software FastBloc; Paralan's SCSI Write Blockers;
Tableu Ultra Block SAS Write Blocker; and Intelligent Computer Solutions (*www.ics-iq.com*)

Conducting an Investigation

To begin conducting an investigation, you start by copying the evidence, using a variety of methods.
No single method retrieves all data from a disk, so using several tools to retrieve and analyze data is a good idea.
Start by gathering the resources you identified in your investigation plan.

You need the following items:
• Original storage media
• Evidence custody form
• Evidence container for the storage media, such as an evidence bag
• Bit-stream imaging tool; in this case, FTK Imager Lite
• Forensic workstation to copy and examine the evidence
• Secure evidence locker, cabinet, or safe

Gathering the Evidence
Remember that you need antistatic bags and pads with wrist straps to prevent static electricity from damaging digital evidence. Perform the following steps to collect the storage media from the department:

1. Arrange to meet the IT manager to interview him and pick up the storage media.
2. After interviewing the IT manager, fill out the evidence form, have him sign it, and then sign it yourself.
3. Store the storage media in an evidence bag, and then transport it to your forensic facility.
4. Carry the evidence to a secure container, such as a locker, cabinet, or safe.
5. Complete the evidence custody form. If you're using a multiple forms, you can store them in the file folder for the case.
6. Secure the evidence by locking the container.

Understanding Bit-stream Copies
A **bit-stream copy** is a bit-by-bit copy (also known as a "forensic copy") of the original drive or storage medium and is an exact duplicate. The more exact the copy, the better chance you have of retrieving the evidence you need from the disk.
This process is usually referred to as "acquiring an image" or "making an image" of a suspect drive.

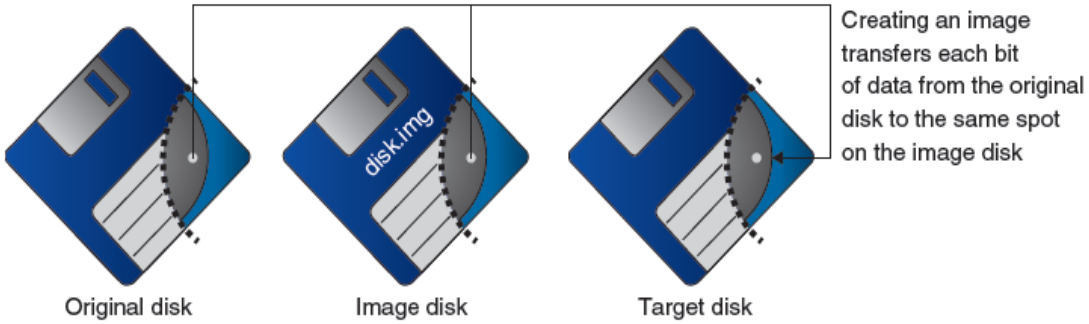
A bit-stream copy is different from a simple backup copy of a disk.
Backup software can copy or compress only files that are stored in a folder or are of a known file type.
Backup software can't copy deleted files and e-mails or recover file fragments.

A **bit-stream image** is the file containing the bit-stream copy of all data on a diskor disk partition. For simplicity, it's usually referred to as an "image," "image save,"or "image file."

To create an exact image of an evidence disk, copying the image to atarget disk that's identical to the evidence disk is preferable.

The target disk's manufacturer and model, in general, should be the same as the original disk's manufacturer and model.
If the target disk is identical to the original, the size in bytes and sectors of both disks should also be the same. Some image acquisition tools can accommodate a target disk that's a different size than the original.

Older digital forensics tools designed for MS-DOS work only on a copied disk. Current GUI tools can work on both a disk drive and copied data sets that many manufacturers refer to as "image saves."

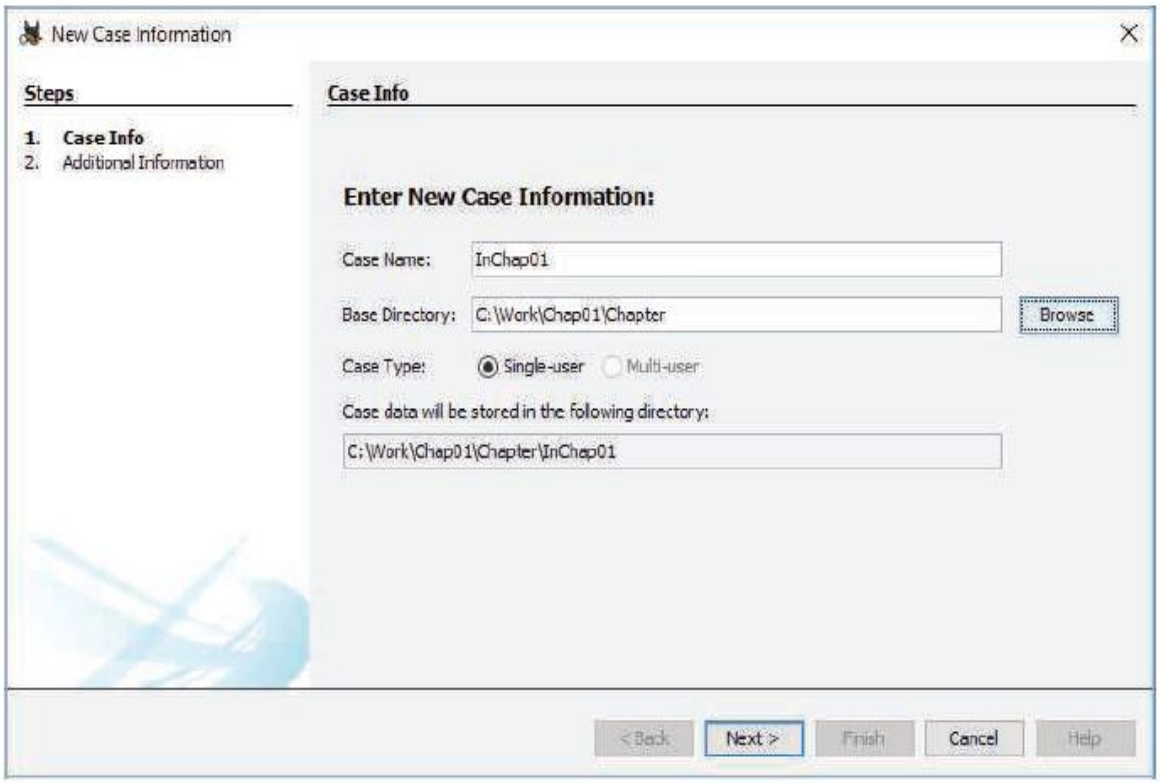


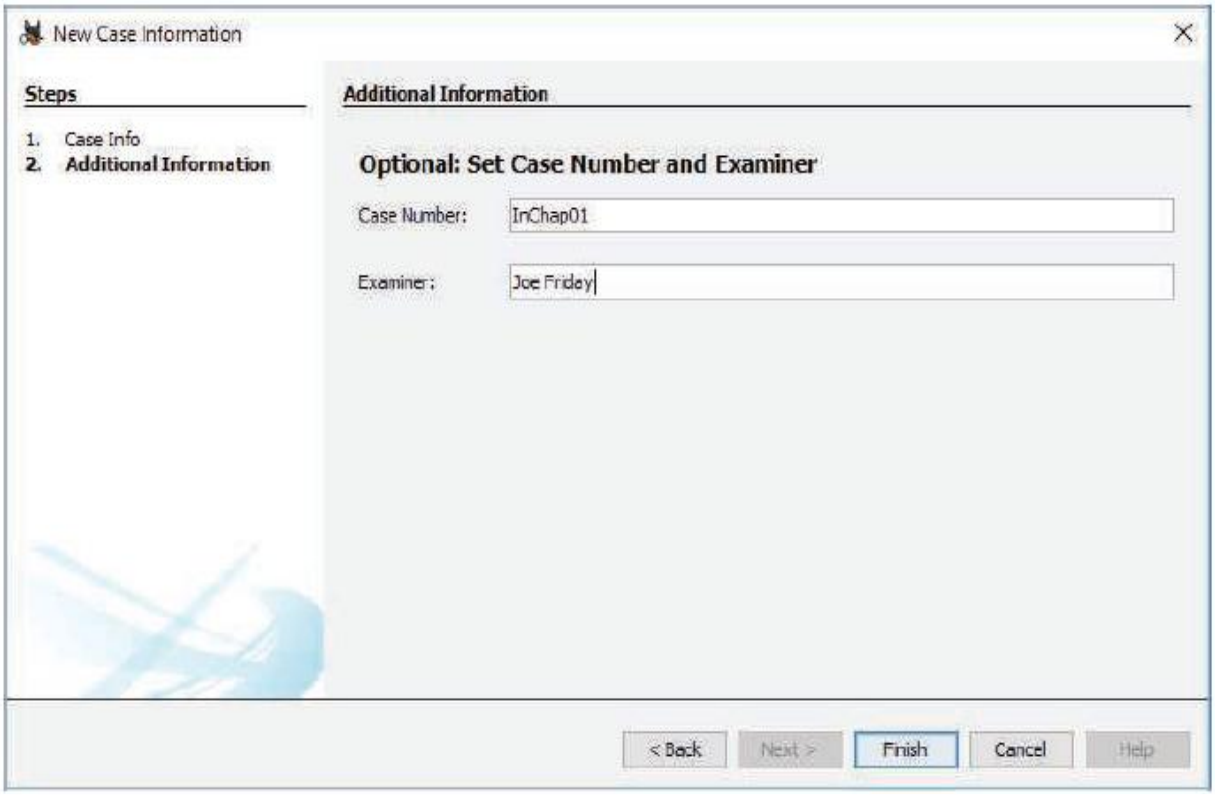
Acquiring an Image of Evidence Media

- After you retrieve and secure the evidence, you're ready to copy the evidence mediaand analyze the data.
- The first rule of digital forensics is to preserve the original evidence.
- Then conduct your analysis only on a copy of the data—the image ofthe original medium.
- Several vendors offer Windows and Linux acquisition tools.

Analyzing Your Digital Evidence

- When you analyze digital evidence, your job is to recover the data.
- If users have deleted or overwritten files on a disk, the disk contains deleted files and file fragments in addition to existing files.
- Remember that as files are deleted, the space they occupied becomes free space meaning it can be used for new files that are saved or files that expand as data is added to them.
- The files that were deleted are still on the disk until a new file is saved to the same physical location, overwriting the original file.
- In the meantime, those files can still be retrieved. Forensics tools such as Autopsy can retrieve deleted files for use as evidence.


New Case Information
Steps
1. Case Info
2. Additional Information
Case Info
Enter New Case Information:
Case Name:
InChap01
Base Directory:
C:\Work\Chap01\Chapter
Browse
Case Type:
Single-user
Multi-user
Case data will be stored in the following directory:
C:\Work\Chap01\Chapter\InChap01
< Back
Next >
Finish
Cancel
Help


New Case Information
Steps
1. Case Info
2. Additional Information
Additional Information
Optional: Set Case Number and Examiner
Case Number:
InChap01
Examiner:
Joe Friday
< Back
Next >
Finish
Cancel
Help