Mod 1: Introduction to Computer Forensics

IT6853 Computer Forensics

Introduction

Computer forensics, now most commonly called “digital forensics,” has been a professional field for many years, but most well-established experts in the field have been self-taught. The growth of the Internet and the worldwide proliferation of computers have increased the need for digital investigations. Computers can be used to commit crimes, and crimes can be recorded on computers, including company policy violations, embezzlement, e-mail harassment, murder, leaks of proprietary information, and even terrorism. Law enforcement, network administrators, attorneys, and private investigators now rely on the skills of professional digital forensics experts to investigate criminal and civil cases.[1]

Digital evidence permeates every aspect of the average person’s life in today’s society. No matter what you are doing these days, a digital footprint is probably being created that contains some type of digital evidence that can be recovered. Sending an email, writing a document, taking a picture with your digital camera, surfing the web, driving in your car with the GPS on—all of these activities create digital evidence.

1.1 What is digital Forensics?

The term forensics can be defined as the application of science to a matter of law. The most accepted definition of digital forensics comes from the definition of computer forensics:

“Computer forensics is the collection, preservation, analysis, and presentation of electronic evidence for use in a legal matter using forensically sound and generally accepted processes, tools, and practices.”[2]

Another definition

“Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.”[3]

And, according to Digital Forensic Research Workshop (DFRWS)

“The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.”

[1] Excerpt From: Bill Nelson. “Guide to Computer Forensics and Investigations: Processing Digital Evidence.” iBooks.

[2] Except From: Larry Daniel. “Digital Forensics for Legal Professionals”

[3] https://searchsecurity.techtarget.com/definition/computer-forensics

1.2 An overview of Digital Forensics

1.2.1 Application of Computer Forensics

"The application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence (information of probative value that is stored or transmitted in binary form) after proper search authority, chain of custody, validation with mathematics (hash function), use of validated tools, repeatability, reporting and possible expert presentation"[4]

"Many groups have tried to create digital forensics certifications that could be recognized worldwide but have failed in this attempt. However, they have created certifications for specific categories of practitioners, such as government investigators. With the ubiquitous access to mobile devices now, digital evidence is everywhere, so the need for a global standardized method is even more critical so that companies and governments can share and use digital evidence. In October 2012, an International Organization for Standardization (ISO) standard for digital forensics was ratified. This standard, ISO 27037 "Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence" (see www.iso.org/standard/44381.html), defines the personnel and methods for acquiring and preserving digital evidence. To address the multinational cases that continue to emerge, agencies in every country should develop policies and procedures that meet this standard.

The Federal Rules of Evidence (FRE), signed into law in 1973, was created to ensure consistency in federal proceedings, but many states' rules map to the FRE, too. In another attempt to standardize procedures, the FBI Computer Analysis and Response Team (CART) was formed in 1984 to handle the increase in cases involving digital evidence. By the late 1990s, CART had teamed up with the Department of Defense Computer Forensics Laboratory (DCFL) for research and training. Much of the early curriculum in this field came from the DCFL. For more information on the FBI's cybercrime investigation services, see www.fbi.gov/investigate/cyber."[5]

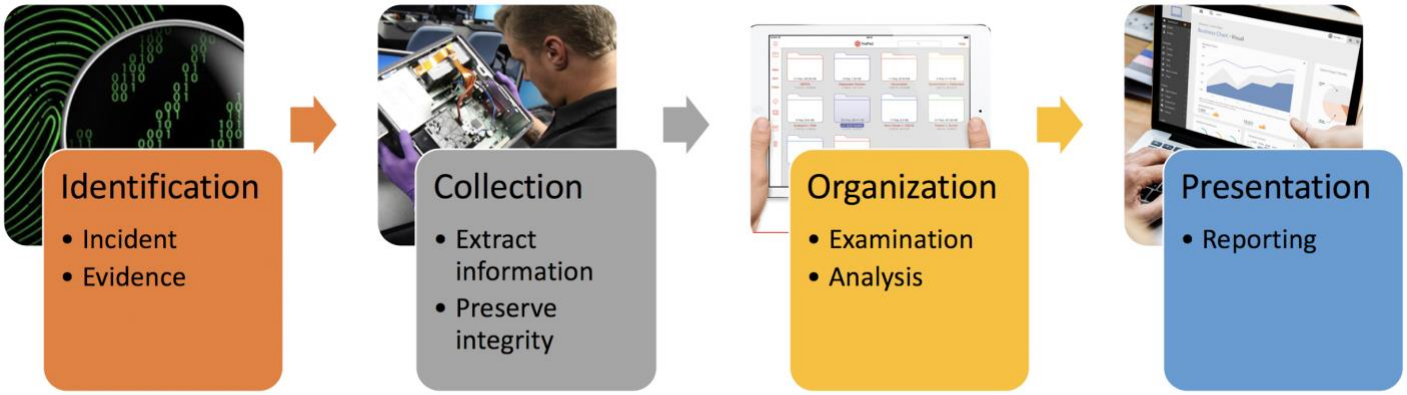
Another important issue on processing digital evidence is the fourth amendment of the U.S Constitution. "The Fourth Amendment to the U.S. Constitution (and each state's constitution) protects everyone's right to be secure in their person, residence, and property from search and seizure. Continuing development of the jurisprudence of this amendment has played a role in determining whether the search for digital evidence has established a different precedent, so separate search warrants might not be necessary. However, when preparing to search for evidence in a criminal case, many investigators still include the suspect's computer and its components in the search warrant to avoid later admissibility problems.

[4] Commentary: Defining Digital Forensics," Forensic Magazine, 2007

[5] Excerpt From: Bill Nelson. "Guide to Computer Forensics and Investigations: Processing Digital Evidence." iBooks.

Every U.S. jurisdiction has case law related to the admissibility of evidence recovered from computers and other digital devices. As you learn in this book, however, the laws on digital evidence vary between states as well as between provinces and countries."[6]

1.2.1 Forensic Procedures



The common steps of computer forensics procedures includes

1.2.1.1 Identification

Examiners determine what type of item it is. If it is not relevant to the forensic request, they simply mark it as processed and move on. Just as in a physical search, if an examiner comes across an item that is incriminating, but outside the scope of the original search warrant, it is recommended that the examiner immediately stop all activity, notify the appropriate individuals, including the requester, and wait for further instructions. For example, law enforcement might seize a computer for evidence of tax fraud, but the examiner may find an image of child pornography. The most prudent approach, after finding evidence outside the scope of a warrant, is to stop the search and seek to expand the warrant's authority or to obtain a second warrant.

If an item is relevant to the forensic request, examiners document it on a third list, the Relevant Data List. This list is a collection of data relevant to answering the original forensic request. For example, in an identity theft case, relevant data might include social security numbers, images of false identification, or e-mails discussing identity theft, among other things. It is also possible for an item to generate yet another search lead. An email may reveal that a target was using another nickname. That would lead to a new keyword search for the new nickname. The examiners would go back and add that lead to the Search Lead List so that they would remember to investigate it completely.

An item can also point to a completely new potential source of data. For example, examiners might find a new email account the target was using. After this discovery, law enforcement may want to subpoena the contents of the new email account. Examiners might also find evidence indicating the target stored files on a removable universal serial bus (USB) drive—one that law enforcement did not find in the original search. Under these circumstances, law

[6] Excerpt From: Bill Nelson. "Guide to Computer Forensics and Investigations: Processing Digital Evidence." iBooks

enforcement may consider getting a new search warrant to look for the USB drive. A forensic examination can point to many different types of new evidence. Some other examples include firewall logs, building access logs, and building video security footage. Examiners document these on a list.

1.2.1.2 Collection

When the examiner's forensic platform is ready, he or she duplicates the forensic data provided in the request and verifies its integrity. This process assumes law enforcement has already obtained the data through appropriate legal process and created a forensic image. A forensic image is a bit-for-bit copy of the data that exists on the original media, without any additions or deletions. It also assumes the forensic examiner has received a working copy of the seized data. If examiners get original evidence, they need to make a working copy and guard the original's chain of custody. The examiners make sure the copy in their possession is intact and unaltered. They typically do this by verifying a hash, or digital fingerprint, of the evidence. If there are any problems, the examiners consult with the requester about how to proceed.

After examiners verify the integrity of the data to be analyzed, a plan is developed to extract data. They organize and refine the forensic request into questions they understand and can answer. The forensic tools that enable them to answer these questions are selected. Examiners generally have preliminary ideas of what to look for, based on the request. They add these to a "Search Lead List," which is a running list of requested items. For example, the request might provide the lead "search for child pornography." Examiners list leads explicitly to help focus the examination. As they develop new leads, they add them to the list, and as they exhaust leads, they mark them "processed" or "done."

1.2.1.3 Organization

In the analysis phase, examiners connect all the dots and paint a complete picture for the requester. For every item on the Relevant Data List, examiners answer questions like who, what, when, where, and how. They try to explain which user or application created, edited, received, or sent each item, and how it originally came into existence. Examiners also explain where they found it. Most importantly, they explain why all this information is significant and what it means to the case.

Often examiners can produce the most valuable analysis by looking at when things happened and producing a timeline that tells a coherent story. For each relevant item, examiners try to explain when it was created, accessed, modified, received, sent, viewed, deleted, and launched. They observe and explain a sequence of events and note which events happened at the same time.

Examiners document all their analysis, and other information relevant to the forensic request, and add it all to a fifth and final list, the "Analysis Results List." This is a list of all the meaningful data that answers who, what, when, where, how, and other questions. The information on this list satisfies the forensic request. Even at this late stage of the process, something might generate new data search leads or a source of data leads. If this happens, examiners add them to the appropriate lists and consider going back to examine them fully.

1.2.1.4 Presentation

Finally, after examiners cycle through these steps enough times, they can respond to the forensic request. They move to the Forensic Reporting phase. This is the step where examiners document findings so that the requester can understand them and use them in the case. Forensic reporting is outside the scope of this article, but its importance can not be overemphasized. The final report is the best way for examiners to communicate findings to the requester. Forensic reporting is important because the entire forensic process is only worth as much as the information examiners convey to the requester. After the reporting, the requester does case-level analysis where he or she (possibly with examiners) interprets the findings in the context of the whole case.

1.3 Computer Forensics and Other disciplines

“In general, digital forensics is used to investigate data that can be retrieved from a computer’s hard drive or other storage media. Like an archaeologist excavating a site, digital forensics examiners retrieve information from a computer or its components. The information retrieved might already be on the drive, but it might not be easy to find or decipher. On the other hand, network forensics yields information about how attackers gain access to a network along with files they might have copied, examined, or tampered with. Network forensics examiners use log files to determine when users logged on and determine which URLs users accessed, how they logged on to the network, and from what location. Network forensics also tries to determine what tracks or new files were left behind on a victim’s computer and what changes were made.

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. In data recovery, typically you know what you’re looking for. Digital forensics is the task of recovering data that users have hidden or deleted, with the goal of 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.

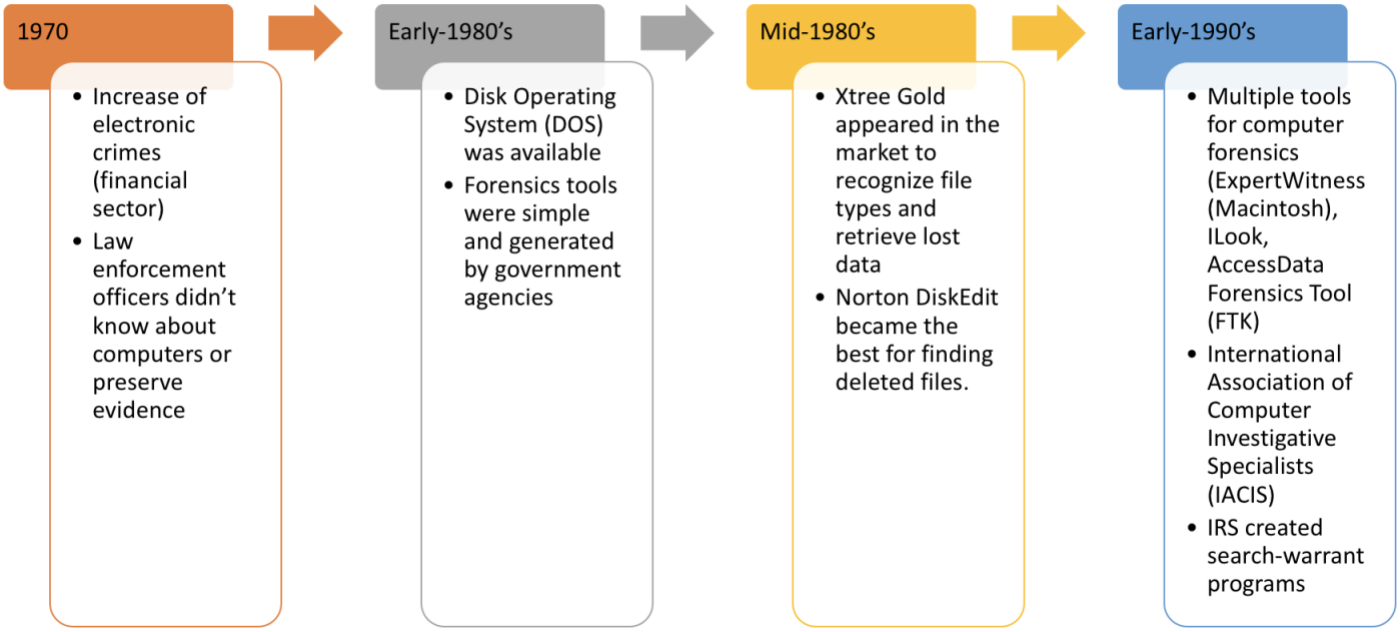
The evidence can be inculpatory evidence (in criminal cases, the expression is “incriminating”) or exculpatory evidence , meaning it tends to clear the suspect.”[7]

On the other side, Cloud Forensics investigates Cloud environments. Cloud Forensics needs to deal with servers around the World hosting customer data (which is known as a multi-tenant challenge) as many things have to be considered like legal jurisdiction, third parties and preservation of data of other tenants.

1.4 Brief history of Digital Forensics

[7] Excerpt From: Bill Nelson. “Guide to Computer Forensics and Investigations: Processing Digital Evidence.” iBooks.

Brief History of Digital Forensics



Until the late 1990s, what became known as digital forensics was commonly termed 'computer forensics'. The first computer forensic technicians were law enforcement officers who were also computer hobbyists. In the USA in 1984 work began in the FBI Computer Analysis and Response Team (CART). One year later, in the UK, the Metropolitan Police set up a computer crime unit under John Austen within what was then called the Fraud Squad.

A major change took place at the beginning of the 1990s. Investigators and technical support operatives within the UK law enforcement agencies, along with outside specialists, realised that digital forensics (as with other fields) required standard techniques, protocols and procedures. Apart from informal guidelines, these formalisms did not exist but urgently needed to be developed. A series of conferences, initially convened by the Serious Fraud Office and the Inland Revenue, took place at the Police Staff College at Bramshill in 1994 and 1995, during which the modern British digital forensic methodology was established.

In the UK in 1998 the Association of Chief Police Officers (ACPO) produced the first version of its *Good Practice Guide for Digital Evidence* (Association of Chief Police Officers, 2012). The ACPO guidelines detail the main principles applicable to all digital forensics for law enforcement in the UK.

As the science of digital forensics has matured these guidelines and best practice have slowly evolved into standards and the field has come under the auspices of the **Forensic Science Regulator** in the UK.

Optional Activity

Search the internet for no more than five minutes for the series of ISO standards relating to digital forensics and list each of the standards you think applies.

1.5 Understanding Case Law

"Existing laws and statutes simply can't keep up with the rate of technological change. Therefore, when statutes or regulations don't exist, case law is used. In common law nations, such as the United States, case law allows legal counsel to apply previous similar cases to current ones in an effort to address ambiguity in laws. Examiners must be familiar with recent court rulings on search and seizure in the electronic environment to avoid mistakes such as exceeding a search warrant's authority. Recent events involving privacy incursions by government agencies have resulted in new laws and policies. Developments in technology have changed how everyday events are viewed. For example, what should be considered private conversations? Which devices are actually protected?

Although law enforcement can certainly confiscate anything an arrested person is carrying and log that "a device, such as a smartphone, was on the person, they don't necessarily have the right or authority to search the device. These actions are being challenged in courts constantly. Remaining vigilant in keeping up with changing case law is critical to being an effective digital forensics investigator."[8]

Additional information of how to understand the digital evidence in the U.S court, you may refer to: https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf

1.6 Developing Forensics Resources

"To be a successful digital forensics investigator, you must be familiar with more than one computing platform. In addition to older platforms, such as DOS, Windows 9x, and Windows XP, you should be familiar with Linux, macOS, and current Windows platforms. However, no one can be an expert in every aspect of computing. Likewise, you can't know everything about the technology you're investigating. To supplement your knowledge, you should develop and maintain contact with digital, network, and investigative professionals."

Join computer user groups in both the public and private sectors. For example:

- Computer Technology Investigators Network (CTIN). → Meets to discuss problems that "digital forensics examiners encounter. Also provide training. (https://ctin.org/)
- International Association of Computer Investigative Specialists (IACIS) (https://www.iacis.com/)
- International Information System Security Certification Consortium (ISC)2 (https://www.isc2.org/)
- InfraGard (https://www.infragard.org/)

User groups can be especially helpful when you need information about obscure OSs.

[8] Excerpt From: Bill Nelson. "Guide to Computer Forensics and Investigations: Processing Digital Evidence." iBooks.

“Outside experts can also give you detailed information you need to retrieve digital evidence. For example, a recent murder case involved a husband and wife who owned a Macintosh store. When the wife was discovered dead, apparently murdered, investigators found that she had wanted to leave her husband but didn’t because of her religious beliefs. The police got a search warrant and confiscated the home and office computers. When the detective on the case examined the home system, he found that the hard drive had been compressed and erased. He contacted a Macintosh engineer, who determined the two software programs used to compress the drive. With this knowledge, the detective could retrieve information from the hard drive, including text files indicating that the husband spent $35,000 in business funds to purchase cocaine and prostitution services. This evidence proved crucial in making it possible to convict the husband of murder.”[9]

1.7 Preparing for Computer Investigations

In Computer Investigations, we have 2 categories:

Public Investigations

Private or corporate investigations

1.7.1 Public Investigations

Public investigators are government law enforcement officers whose mandate is controlled by the U.S laws. Most public investigators include those from the FBI and are majorly engaged in criminal and civil law. Some of the major investigations carried out by these investigators include drug trafficking, child trafficking and kidnapping, bank robbery, fraud, terrorism, abuse of public office and cyber crime (Saferstein, 2000).

FBI investigators are required to work under several terms such as identifying themselves to the suspects before conducting an investigation. This ensures that the correct due process in enforcement of the law is followed. It should be noted that the findings obtained by public investigators form the basis of eventual prosecution and trial in a court of law (Kelly & Phillip, 2004).

[9] Excerpt From: Bill Nelson. “Guide to Computer Forensics and Investigations: Processing Digital Evidence.” iBooks.

“When conducting a computer investigation for potential criminal violations of the law, the legal processes you follow depend on local custom, legislative standards, and rules of evidence. In general, however, a criminal case follows three stages: the complaint, the investigation, and the prosecution. Someone files a complaint, and then a specialist investigates the complaint and, with the help of a prosecutor, collects evidence and builds a case. If the evidence is sufficient, the case might proceed to trial.

A criminal investigation generally begins when someone finds evidence of or witnesses an illegal act. The witness or victim makes an allegation to the police, an accusation of fact that a crime has been committed.

A police officer interviews the complainant and writes a report about the crime. The law enforcement agency processes the report, and management decides to start an investigation or log the information into a police blotter, which provides a record of information about crimes that have been committed previously. Criminals often repeat actions in their illegal activities, and these patterns can be discovered by examining police blotters. This historical knowledge is useful when conducting investigations, especially in high-technology crimes. Blotters now are generally electronic files, often structured as databases, so they can be searched more easily than the old paper blotters.”[10]

The officers that are trained to conduct digital forensics according to ISO standard 27037 are two categories:
DEFR (Digital evidence first responder) that is the first to arrive to the scene
DES (Digital Evidence Specialist) that is the one who analyze the data
“In a criminal or public-sector case, if the police officer or investigator has sufficient cause to support a search warrant, the prosecuting attorney might direct him or her to submit an affidavit (also called a “declaration”). This sworn statement of support of facts about or evidence of a crime is submitted to a judge with the request for a search warrant before seizing evidence. It’s your responsibility to write the affidavit, which must include exhibits (evidence) that support the allegation to justify the warrant. You must then have the affidavit notarized under sworn oath to verify that the information in the affidavit is true. In general, after a judge approves and signs a search warrant, it’s ready to be executed, meaning a DEFR can collect evidence as defined by the warrant. After you collect the evidence, you process and analyze it to determine whether a crime actually occurred. The evidence can then be presented in court in a hearing or trial. A judge or an administrative law judge then renders a judgment, or a jury hands down a verdict (after which a judge can enter a judgment).”[11]

[10] Excerpt From: Bill Nelson. “Guide to Computer Forensics and Investigations: Processing Digital Evidence.” iBooks.
[11] Excerpt From: Bill Nelson. “Guide to Computer Forensics and Investigations: Processing Digital Evidence.” iBooks.

1.7.2 Private Investigations

Private investigators, on the other hand, are also common in the U.S due to the high level of specialization so desired in service delivery. In fact most people consider hiring these investigators for quality of service rendered and also for the high level of professionalism employed.

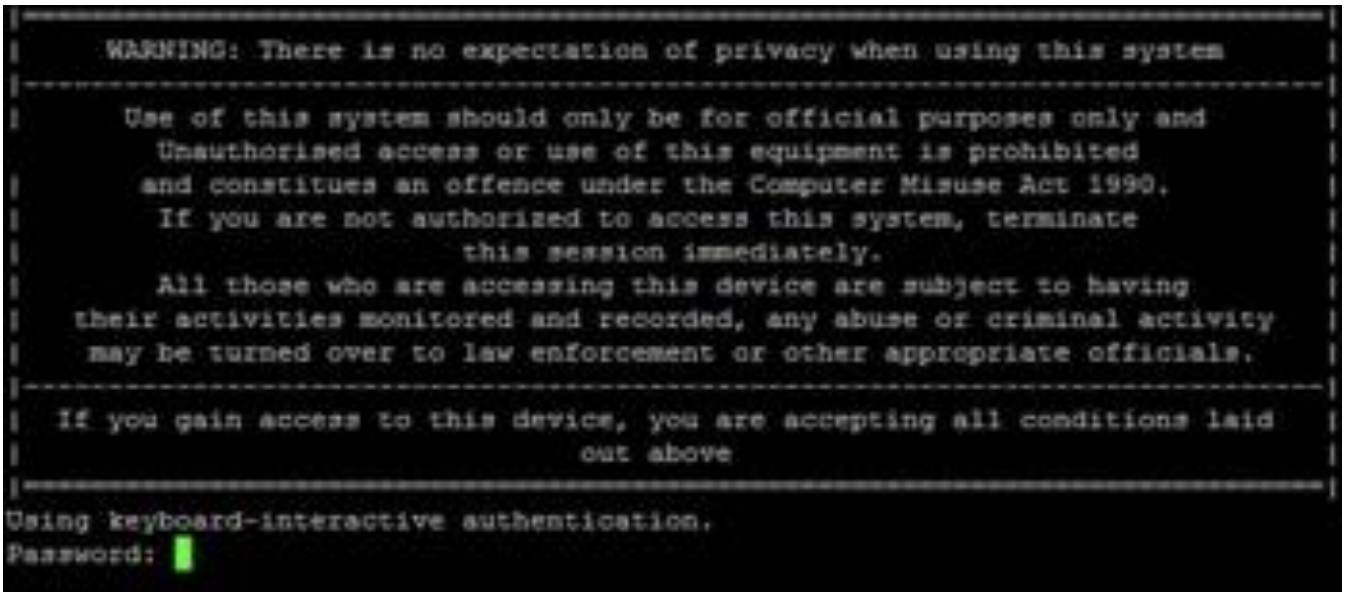
There are different types of investigators including; computer forensic investigators, corporate investigators, legal investigators, financial investigators and loss prevention agents (Saferstein, 2000). The nature of their work makes them give the best since they do what they know best. Most of them are college diploma holders or graduates in their respective fields.

"One way that businesses can reduce the risk of litigation is to publish and maintain policies that employees find easy to read and follow. In addition, these policies can make internal investigations go more smoothly. 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." [11]

"Another way private companies may protect themselves and avoid litigation is to display warning banners. "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." [11]

""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 under Fourth Amendment search-and-seizure rules to seize the equipment. In a company with a well-defined policy, this right to inspect or search at will applies to both criminal activity and company policy violations. Keep in mind, however, that your country's laws might differ."[12]

[12] Excerpt From: Bill Nelson. "Guide to Computer Forensics and Investigations: Processing Digital Evidence." iBooks.



There are many other types of litigations in companies, but the majority of them (that involves digital forensics) are: 1) Abuse or misuse of computing assets; 2) E-mail abuse; 3) Internet abuse; 4) Espionage

1.7.2.1 Abuse or Misuse of computing assets

When the *Arizona Republic* asked readers to write in and tell the newspaper how they or others abused the Internet at their companies' expense, one woman reported to the paper that she spent her day at work shopping on the Internet. To avoid being detected this woman said she kept another window open, which she could click to quickly. One man admitted that he spent most of his workday online chatting with other sports car enthusiasts.

In 1996, Compaq Corporation fired more than a dozen Houston workers because the employees had made more than 1,000 visits to sex sites while on the job. Similarly, Lockheed Martin Space & Missiles fired two employees for visiting sex sites and making financial transactions online.

Additionally, employees are increasingly accessing information off the web and then reconfiguring it for use in their work. In this way, some companies have come into possession of other companies' proprietary information and could be liable for copyright infringement.

1.7.2.2 Email Abuse

Two discrimination cases filed in federal court highlight the potentially disastrous results of offensive E-Mail circulated in the workplace. For example, in *Curtis v. Citibank N.A., 97 Civ. 1065 (S.D.N.Y. 1997)*, two black Citibank employees claimed that many white supervisors exchanged "vulgar and racially vile" E-Mail messages that "demeaned and ridiculed African-American people." In *Owens v. Morgan Stanley & Co., 96 Civ. 9747 (S.D.N.Y. 1996)*, two black Morgan employees filed a $60 million lawsuit claiming they were discriminatorily denied advancement in the company. In their lawsuit, Plaintiffs referenced racist jokes disseminated through the company's E-Mail system.

Employers are also at risk if their workers send or receive E-Mails of a sexual nature. *See Vicarelli v. Business Int'l, Inc., d/b/a Economist Intelligence Unit, 1997 U.S. Dist. LEXIS 12944 (D. Mass., 1997).*

If you are investigating a email abuse case, you probably need:

1. An electronic copy of the offending email that contains message header data
2. If available, e-mail server log records
3. For –mail systems that store user's messages on a central server, access to the server
4. Access to the computer so that you can perform forensics analysis on it
5. Your preferred computer forensics tool

The recommended steps to follow for a computer forensic specialist are:

1. Use the standard forensic analysis techniques
2. Obtain an electronic copy of the suspect's and victim's e-mail folder or data
3. For Web-based e-mail investigations, use tools such as FTK's Internet Keyword Search option to extract all related e-mail address information
4. Examine header data of all messages of interest to the investigation

1.7.2.3 Internet Abuse

Workplace Internet abuse is often much more subtle, including brief interludes of employees checking their personal email while on the clock or using the company computer to book campground reservations for that upcoming holiday weekend. While some people might ask "what is the big deal?" Others might agree that personal use of the company computer system, especially when the employee is supposed to be working, does constitute an abuse of company assets. So how do you know when Internet use at work turns into Internet abuse? When company policy tells you so.

But, other cases can be more problematic. Just ask the company that got a letter from the FBI last November that said one of its employees was accessing child pornography sites from the workplace. As if that news wasn't bad enough, the company in question had not developed an Internet policy.

If you are investigating a Internet abuse case, you probably need:

1. Organization's Internet proxy server logs
2. Suspect computer's IP address
3. Suspect computer's disk drive
4. Your preferred computer forensics analysis tool.

The recommended steps to follow for a computer forensic specialist are:

1. Use standard forensics analysis techniques and procedures
2. Use appropriate tools to extract all Web page URL information
3. Contact the network firewall administrator and request a proxy server log
4. Compare the data recovered from forensics analysis to the proxy server log
5. Continue analyzing the computer's disk data

1.7.2.3 Industrial Espionage

The term industrial espionage refers to the illegal and unethical theft of business trade secrets for use by a competitor to achieve a competitive advantage. This activity is a covert practice often done by an insider or an employee who gains employment for the express purpose of spying and stealing information for a competitor. Industrial espionage is conducted by companies for commercial purposes rather than by governments for national security purposes.

Also referred to as corporate spying or espionage or economic espionage, industrial espionage is most commonly associated with technology-heavy industries—particularly the computer, biotechnology, aerospace, chemical, energy, and auto sectors—in which a significant amount of money is spent on research and development (R&D).

The world's biggest practitioners of industrial espionage correspond to companies in countries with the biggest economies. One of the reasons why corporations engage in industrial espionage is to save time as well as huge sums of money. After all, it can take years to bring products and services to market—and the costs can add up.

In recent years, industrial espionage has grown with the help of the internet and lax cybersecurity practices, though such acts have become easier to detect. Social media is a new frontier for industrial espionage and its full impact and utility are still being measured. Penalties for industrial espionage can be significant, as seen in 1993 when Volkswagen stole trade secrets from General Motors which led to a $100 million fine.

If you are investigating a Internet abuse case, you probably need:

1. Determine whether the investigation involves possible industrial espionage incident
2. Consult with corporate attorneys and upper management
3. Determine the information you need
4. Initiate the investigation
5. Place surveillance systems at key locations
6. Gather additional evidence
7. Collect all log data
8. Report regularly

1.8 Systematic Approach for Conducting Digital Forensics

“When preparing a case, you can apply standard systems analysis steps, explained in the following list, to problem solving. Later in this chapter, you apply these steps to cases.

- **Make an initial assessment about the type of case you’re investigating**—To assess the type of case you’re handling, talk to others involved in the case and ask questions about the incident. Have law enforcement or company security officers already seized the computer, disks, peripherals, and other components? Do you need to visit an office or another location? Was the computer used to commit a crime, or does it contain evidence about another crime?

- **Determine a preliminary design or approach to the case**—Outline the general steps you need to follow to investigate the case. If the suspect is an employee and you need to acquire his or her system, determine whether you can seize the computer during work hours or have to wait until evening or weekend hours. If you're preparing a criminal case, determine what information law enforcement officers have already gathered.
- **Create a detailed checklist**—Refine the general outline by creating a detailed checklist of steps and an estimated amount of time for each step. This outline helps you stay on track during the investigation.
- **Determine the resources you need**—Based on the OS of the computer you're investigating, list the software you plan to use for the investigation, noting any other software, tools, or expert assistance you might need.
- **Obtain and copy an evidence drive**—In some cases, you might be seizing multiple computers along with CDs, DVDs, USB drives, mobile devices, and other removable media. (For the examples in this chapter, you're using only USB drives.) Make a forensic copy of the disk.
- **Identify the risks**—List the problems you normally expect in the type of case you're handling. This list is known as a standard risk assessment. For example, if the suspect seems knowledgeable about computers, he or she might have set up a logon scheme that shuts down the computer or overwrites data on the hard disk when someone tries to change the logon password.
- **Mitigate or minimize the risks**—Identify how you can minimize the risks. For example, if you're working with a computer on which the suspect has likely password-protected the hard drive, you can make multiple copies of the original media before starting. Then if you destroy a copy during the process of retrieving information from the disk, you have additional copies.
- **Test the design**—Review the decisions you've made and the steps you've completed. If you have already copied the original media, a standard part of testing the design involves comparing hash values (discussed in Chapters 3 and 4) to ensure that you copied the original media correctly.
- **Analyze and recover the digital evidence**—Using the software tools and other resources you've gathered, and making sure you've addressed any risks and obstacles, examine the disk to find digital evidence.
- **Investigate the data you recover**—View the information recovered from the disk, including existing files, deleted files, e-mail, and Web history, and organize the files to help find information relevant to the case.
- **Complete the case report**—Write a complete report detailing what you did and what you found.
- **Critique the case**—Self-evaluation and peer review are essential parts of professional growth. After you complete a case, review it to identify successful decisions and actions and determine how you could have improved your performance."[13]

1.9 Planning your investigation

A basic digital forensic investigation should include:

1. Acquire the evidence
2. Complete an evidence form and establish a **chain of custody**
3. Transport the evidence to a computer forensics lab
4. Secure evidence in an approved secure container

[13] Excerpt From: Bill Nelson. "Guide to Computer Forensics and Investigations: Processing Digital Evidence." iBooks.

5. Prepare your forensics workstation
6. Retrieve the evidence from the secure container
7. **Make a forensic copy of the evidence**
8. Return the evidence to the secure container
9. Process the copied evidence with computer forensics tools.

1.10 Important concepts in digital forensics

1.10.1 Evidence Custody Form

The evidence custody form includes the detail of each and every evidence that was collected at the time of investigation done by the agenda. It also includes the name of the people who have collected that evidence. There are two types 1) The single evidence form and 2) the multi evidence form.

1.10.1.1 Single Evidence Form

This form is to be used when collecting a hardware device containing data that may be of interest in a case. The form only refers to one item of evidence and that one is completed

The following is an example:

Single Evidence Form

Case No. | Evidence No.

Digital Forensics Lab

PLEASE COMPLETE FORM IN UPPERCASE

Section B: Evidence Collection

Date/Time Collected D D / M M / Y Y H H : M M	Collected by

Site Address

Section C: Evidence Details

Date/Time Stored D D / M M / Y Y H H : M M

Storage Location

Device Type	Capacity
Manufacturer	Model

Serial No.

MD5 Sum

SHA-1 Sum

Additional Information...

Note any damage, marks and scratches

Digital Image Taken ☐ Yes ☐ No

Section D: Image Details

Date/Time Imaged D D / M M / Y Y H H : M M	Imaged by

Storage Location

Image Filename	Image Size (inc. unit)

Additional Information

1.10.1.2 Multiple Evidence Form

List multi-piece of evidence on the same page

EVIDENCE/PROPERTY CUSTODY DOCUMENT

For use of this form see AR 190-45 and AR 195-5; the proponent agency is US Army Criminal Investigation Command

MPR/CID SEQUENCE NUMBER

CRD REPORT/CID ROI NUMBER

RECEIVING ACTIVITY	LOCATION
NAME, GRADE AND TITLE OF PERSON FROM WHOM RECEIVED ☐ OWNER ☐ OTHER	ADDRESS *(Include Zip Code)*

LOCATION FROM WHERE OBTAINED	REASON OBTAINED	TIME/DATE OBTAINED

ITEM NO.	QUANTITY	DESCRIPTION OF ARTICLES *(Include model, serial number, condition and unusual marks or scratches)*

CHAIN OF CUSTODY

ITEM NO.	DATE	RELEASED BY	RECEIVED BY	PURPOSE OF CHANGE OF CUSTODY
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	

1.10.2 Chain of Custody

Chain of custody (CoC), in legal contexts, is the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence. Of particular importance in criminal cases, the concept is also applied in civil litigation—and sometimes more broadly in drug testing of athletes, and in supply chain management, e.g. to improve the traceability of food products, or to provide assurances that wood products originate from sustainably managed forests. It is often a tedious process that has been required for evidence to be shown legally in court. Now however, with new portable technology that allows accurate laboratory quality results from the scene of the crime, the chain of custody is often much shorter which means evidence can be processed for court much faster.

1.10.3 Bit-Stream Copies

Bit stream copy (also referred to as mirror image) involves the backup of all areas of a computer hard disk drive or another type of storage media. Such a backup exactly replicates all sectors on a given storage device. Thus, all files and ambient data storage areas are copied.

1.11 Starting your abilities as digital forensic specialist

Because you are going to deal with multiple OS during the study of digital forensic cases, you must be familiar with the main commands that provide information about the case.

One of the OS that provides more details using command prompt is Linux. Let's remember some Linux commands that help you to retrieve forensic data.

File Commands

ls – directory listing
ls -al – formatted listing with hidden files
cd *dir* - change directory to *dir*
cd – change to home
pwd – show current directory
mkdir *dir* – create a directory *dir*
rm *file* – delete *file*
rm -r *dir* – delete directory *dir*
rm -f *file* – force remove *file*
rm -rf *dir* – force remove directory *dir* *
cp *file1 file2* – copy *file1* to *file2*
cp -r *dir1 dir2* – copy *dir1* to *dir2*; create *dir2* if it doesn't exist
mv *file1 file2* – rename or move *file1* to *file2* if *file2* is an existing directory, moves *file1* into directory *file2*
ln -s *file link* – create symbolic link *link* to *file*
touch *file* – create or update *file*
cat > *file* – places standard input into *file*
more *file* – output the contents of *file*
head *file* – output the first 10 lines of *file*
tail *file* – output the last 10 lines of *file*
tail -f *file* – output the contents of *file* as it grows, starting with the last 10 lines

Process Management

ps – display your currently active processes
top – display all running processes
kill *pid* – kill process id *pid*
killall *proc* – kill all processes named *proc* *
bg – lists stopped or background jobs; resume a stopped job in the background
fg – brings the most recent job to foreground
fg *n* – brings job *n* to the foreground

File Permissions

chmod *octal file* – change the permissions of *file* to *octal*, which can be found separately for user, group, and world by adding:

- 4 – read (r)
- 2 – write (w)
- 1 – execute (x)

Examples:
chmod 777 – read, write, execute for all
chmod 755 – rwx for owner, rx for group and world
For more options, see **man chmod**.

SSH

ssh *user@host* – connect to *host* as *user*
ssh -p *port user@host* – connect to *host* on port *port* as *user*
ssh-copy-id *user@host* – add your key to *host* for *user* to enable a keyed or passwordless login

Searching

grep *pattern files* – search for *pattern* in *files*
grep -r *pattern dir* – search recursively for *pattern* in *dir*
command* | grep *pattern – search for *pattern* in the output of *command*
locate *file* – find all instances of *file*

System Info

date – show the current date and time
cal – show this month's calendar
uptime – show current uptime
w – display who is online
whoami – who you are logged in as
finger *user* – display information about *user*
uname -a – show kernel information
cat /proc/cpuinfo – cpu information
cat /proc/meminfo – memory information
man *command* – show the manual for *command*
df – show disk usage
du – show directory space usage
free – show memory and swap usage
whereis *app* – show possible locations of *app*
which *app* – show which *app* will be run by default

Compression

tar cf *file.tar files* – create a tar named *file.tar* containing *files*
tar xf *file.tar* – extract the files from *file.tar*
tar czf *file.tar.gz files* – create a tar with Gzip compression
tar xzf *file.tar.gz* – extract a tar using Gzip
tar cjf *file.tar.bz2* – create a tar with Bzip2 compression
tar xjf *file.tar.bz2* – extract a tar using Bzip2
gzip *file* – compresses *file* and renames it to *file.gz*
gzip -d *file.gz* – decompresses *file.gz* back to *file*

Network

ping *host* – ping *host* and output results
whois *domain* – get whois information for *domain*
dig *domain* – get DNS information for *domain*
dig -x *host* – reverse lookup *host*
wget *file* – download *file*
wget -c *file* – continue a stopped download

Installation

Install from source:
./configure
make
make install
dpkg -i *pkg.deb* – install a package (Debian)
rpm -Uvh *pkg.rpm* – install a package (RPM)

Shortcuts

Ctrl+C – halts the current command
Ctrl+Z – stops the current command, resume with **fg** in the foreground or **bg** in the background
Ctrl+D – log out of current session, similar to **exit**
Ctrl+W – erases one word in the current line
Ctrl+U – erases the whole line
Ctrl+R – type to bring up a recent command
!! - repeats the last command
exit – log out of current session

* use with extreme caution.

Privileges

sudo *command* – run *command* as root
sudo -s – open a root shell
sudo -s -u *user* – open a shell as *user*
sudo -k – forget sudo passwords
gksudo *command* – visual sudo dialog (GNOME)
kdesudo *command* – visual sudo dialog (KDE)
sudo visudo – edit /etc/sudoers
gksudo nautilus – root file manager (GNOME)
kdesudo konqueror – root file manager (KDE)
passwd – change your password

Display

sudo /etc/init.d/gdm restart – restart X and return to login (GNOME)
sudo /etc/init.d/kdm restart – restart X and return to login (KDE)
(file) **/etc/X11/xorg.conf** – display configuration
sudo dexconf – reset xorg.conf configuration
Ctrl+Alt+Bksp – restart X display if frozen
Ctrl+Alt+*FN* – switch to tty *N*
Ctrl+Alt+F7 – switch back to X display

System Services[1]

start *service* – start job *service* (Upstart)
stop *service* – stop job *service* (Upstart)
status *service* – check if *service* is running (Upstart)
/etc/init.d/*service* start – start *service* (SysV)
/etc/init.d/*service* stop – stop *service* (SysV)
/etc/init.d/*service* status – check *service* (SysV)
/etc/init.d/*service* restart – restart *service* (SysV)
runlevel – get current runlevel

Package Management[1]

apt-get update – refresh available updates
apt-get upgrade – upgrade all packages
apt-get dist-upgrade – upgrade with package replacements; upgrade Ubuntu version
apt-get install *pkg* – install *pkg*
apt-get purge *pkg* – uninstall *pkg*
apt-get autoremove – remove obsolete packages
apt-get -f install – try to fix broken packages
dpkg --configure -a – try to fix broken packages
dpkg -i *pkg.deb* – install file *pkg.deb*
(file) **/etc/apt/sources.list** – APT repository list

Network

ifconfig – show network information
iwconfig – show wireless information
sudo iwlist scan – scan for wireless networks
sudo /etc/init.d/networking restart – reset network for manual configurations
(file) **/etc/network/interfaces** – manual configuration
ifup *interface* – bring *interface* online
ifdown *interface* – disable *interface*

Special Packages

ubuntu-desktop – standard Ubuntu environment
kubuntu-desktop – KDE desktop
xubuntu-desktop – XFCE desktop
ubuntu-minimal – core Ubuntu utilities
ubuntu-standard – standard Ubuntu utilities
ubuntu-restricted-extras – non-free, but useful
kubuntu-restricted-extras – KDE of the above
xubuntu-restricted-extras – XFCE of the above
build-essential – packages used to compile programs
linux-image-generic – latest generic kernel image
linux-headers-generic – latest build headers

Firewall[1]

ufw enable – turn on the firewall
ufw disable – turn off the firewall
ufw default allow – allow all connections by default
ufw default deny – drop all connections by default
ufw status – current status and rules
ufw allow *port* – allow traffic on *port*
ufw deny *port* – block *port*
ufw deny from *ip* – block *ip* adress

Application Names

nautilus – file manager (GNOME)
dolphin – file manager (KDE)
konqueror – web browser (KDE)
kate – text editor (KDE)
gedit – text editor (GNOME)

System

Recovery - Type the phrase "REISUB" while holding down Alt and SysRq (PrintScrn) with about 1 second between each letter. Your system will reboot.
lsb_release -a – get Ubuntu version
uname -r – get kernel version
uname -a – get all kernel information