Unit II

CYBER FORESENICS

Cyber forensics is the process of obtaining data as evidence for a crime (using electronic equipment) while adhering to correct investigative procedures to apprehend the offender by presenting the evidence to the court. Computer forensics is another name for cyber forensics. Maintaining the chain of evidence and documentation to identify the digital criminal is the primary goal of cyber forensics.

It is crucial to make a digital copy of the system's unique storage cell during the examination. To identify who is responsible for a security breach, a thorough cyber forensics investigation is conducted. While assuring that the system is not impacted, a full investigation is conducted on the software copy.

Cyber forensics is an unavoidable and crucial element in the modern era, thus cyber forensics plays a huge role in incident response.

What makes cyber forensics crucial?

The field of cyber forensics is growing as more and more things are digitalized. Locating the underlying offenders aids us in battling aggressive activities. Cybersecurity experts can identify hackers and crackers with the help of the data obtained via investigations.

Due to the rise in cybercrime, the work of cyber forensic specialists is becoming increasingly important. The **NCRB reports** thats from 2016 to 2018, cybercrime doubled and that it might rise to four times more than it is now. This demonstrates the significance of law enforcement in combating cybercrime and the difficulties cyber professionals face when dealing with cyber forensics.

Specialists may remotely evaluate any crime scene using cyber forensics by looking at the surfing history, email correspondence, or digital traces.

Cyber forensics is extremely important in today's technologically advanced age. Forensic forensics and technology work together to speed up investigations and produce reliable findings. The following examples illustrate the significance of cyber forensics:

- Cyber forensics aids in gathering crucial digital evidence to track down the offender.

- Electronic devices store enormous volumes of data that are invisible to the naked eye. As an illustration, every time we talk in a smart home, activities taken by smart gadgets generate enormous amounts of data that are essential to cyber forensics.

- The evidence gathered online may also be used by innocent persons to demonstrate their innocence.

The Methodology Used in Cyber Forensics

- acquiring a digital replica of the system that is being or must be examined.

- confirming and authenticating the copy.

- Getting back erased files (using Autopsy Tool).

- To discover the information you need, use keywords.

- the creation of a technical report.

How do Computer/Cyber Forensics Experts work?

During an investigation, computer forensic professionals gather and analyze potential evidence, including deleted, encrypted, or corrupted data. To avoid the evidence from being changed, tainted, or destroyed, all actions conducted during this procedure are documented and adhered to protocols.

A cyber forensic specialist investigates each event using cutting-edge methods. Their thorough inquiry focuses on building a solid chain of evidence. They can settle legal disputes and convict cybercriminals thanks to the admissible proof they create.

To gather data and draw conclusions after thorough research, the area of cyber forensics adheres to a set of rules. The steps that cyber forensic specialists take are:

- **Identification:** Cyber forensics professionals identify the evidence that is present, where it is stored, and in what format it is stored as their first step.

- **Preservation:** The next step after locating the data is to carefully preserve it and prevent anyone from using the device so that the data cannot be altered.

- **Analysis:** The next step after obtaining the data is to examine the data or system. Here, the expert identifies the evidence that the criminal attempted to erase by erasing hidden files, recovers the erased files, checks the recovered data, and restores the data. The ultimate result may need numerous cycles of this method.

- **Documentation:** After data analysis, a record is now produced. This file contains all of the retrieved and readily accessible (not deleted) data that is useful for evaluating and reconstructing the crime scene.

- **Presentation:** The studied data is finally provided to the court at this phase to help resolve cases.

So at the end of the day What cyber forensics can accomplish is

- It can retrieve deleted data, chat histories, emails, and more.

- Calls and SMS can also be erased.

- Phone calls can be recorded and played back afterward.

- It can track who utilized which system when and for how long.

- Which user executed which application can be determined.

Types of Computer/Cyber forensics

Depending on the industry that requires digital inquiry, there are many forms of computer forensics. Here are the fields:

- **Network forensics:** This entails keeping an eye on and examining network traffic going to and coming from the criminal's network. Network intrusion detection systems and other automated techniques are the technologies in use here.

- **Email forensics:** In this kind of forensics, the specialists examine the criminal's email and recover deleted email threads to extract important case-relevant data.

- **Malware forensics:** This area of forensics focuses on crimes connected to hacking. To determine who is responsible for this breach, the forensics specialist looks at the malware and trojans in this case.

- **Memory forensics:** This area of forensics works with extracting information from raw memory data (such as cache, RAM, etc.) after it has been collected.

- **Mobile Phone forensics:** Generally speaking, this area of forensics focuses on cell phones. They look over and evaluate the cell phone's data.

- **Database forensics:** This area of forensics looks at and evaluates database data as well as any associated information.

- **Disk forensics:** This area of forensics searches updated, active, or deleted files to retrieve data from storage media.

To investigate the data, cyber forensic investigators employ various methods and technologies, some of which include:

- **Reverse steganography:** Steganography is a technique for concealing crucial data within a digital file, picture, etc. Therefore, reverse steganography is used by cyber forensic specialists to examine the data and discover a connection to the case.

- **Stochastic forensics:** Without employing digital artifacts, stochastic forensics professionals examine and recreate digital activities. In this context, artifacts refer to unintentional data changes that result from digital operations.

- **Cross-drive analysis:** In this procedure, data from several computer discs are correlated and cross-referenced to preserve and evaluate data that is pertinent to the inquiry.

- **Live analysis:** In this method, the operating system of the culprits' computer is examined from within. To obtain certain important data, it targets the volatile RAM data.

- **Deleted file recovery:** This involves looking through memory for remnants of a file that was partially destroyed to recover it for use as evidence.

Advantages

- Cyber forensics ensures the computer's integrity.

- Many people, businesses, and other entities learn about these crimes thanks to cyber forensics, and they then take the necessary precautions to prevent them.

- Cyber forensics collect evidence from digital devices and offer it to the court so that the offender may be punished.

- They locate the offender quickly and effectively anywhere in the world.

- They support those who want to save their resources, such as time and money.

- The audience can be made aware of the pertinent facts by making it a trend.

Historical background of Cyber forensics

Evolution Of Cyber Forensics

The 1980s was the era when computer forensics came into existence after personal computers became a viable option for consumers. FBI had created a program in 1984 named as the 'Magnetic Media Program', in the current era, it is known as the Computer Analysis and Response Team (CART). Michael Anderson was known as the father of computer forensics because he had started developing measures in this field. He was a special agent in criminal investigation division. He had served the American government until the mid-1990s, after which he founded New Technologies, Inc., a leading computer forensics firm (H. Armstrong, 2004).

Until the late 1990s, what became known as digital forensics was commonly termed 'computer forensics. At 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, realized that digital forensics (as with other fields) required standard techniques, protocols, and procedures. Apart from informal guidelines, these standard tools and techniques did not exist and 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 had matured, these guidelines and best practices have slowly evolved into standards and the field has come under the auspices of the Forensic Science Regulator in the UK.

Formation of Cyber Forensic Investigation Agencies

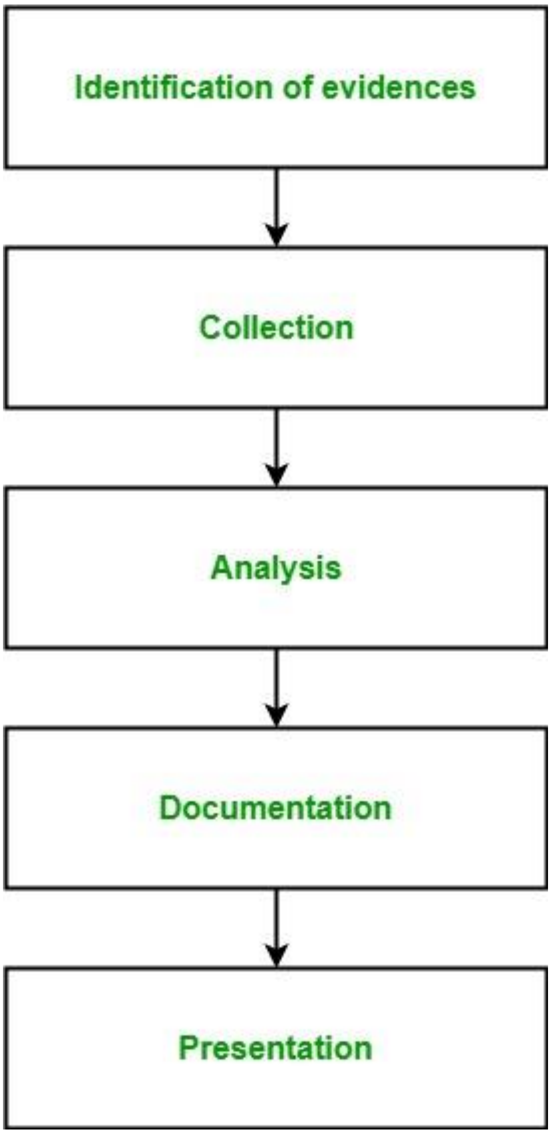
In the year 1988, a meeting was organized in Oregon that led to the formation of the International Association of Computer Investigative Specialists (IACIS). Soon after that, the first module was designed to teach SCERS (Seized Computer Evidence Recovery Specialists) (M. Meyers, M. Rogers, 2006).

Digital Forensics Science

Digital Forensics is a branch of forensic science which includes the identification, collection, analysis and reporting any valuable digital information in the digital devices related to the computer crimes, as a part of the investigation.

In simple words, Digital Forensics is the process of identifying, preserving, analyzing and presenting digital evidences.

The first computer crimes were recognized in the 1978 Florida computers act and after this, the field of digital forensics grew pretty fast in the late 1980-90's. It includes the area of analysis like storage media, hardware, operating system, network and applications. It consists of 5 steps at high level:



1. **Identification of evidence:** It includes of identifying evidences related to the digital crime in storage media, hardware, operating system, network and/or applications. It is the most important and basic step.
2. **Collection:** It includes preserving the digital evidences identified in the first step so that they doesn’t degrade to vanish with time. Preserving the digital evidences is very important and crucial.
3. **Analysis:** It includes analyzing the collected digital evidences of the committed computer crime in order to trace the criminal and possible path used to breach into the system.
4. **Documentation:** It includes the proper documentation of the whole digital investigation, digital evidences, loop holes of the attacked system etc. so that the case can be studied and analysed in future also and can be presented in the court in a proper format.
5. **Presentation:** It includes the presentation of all the digital evidences and documentation in the court in order to prove the digital crime committed and identify the criminal.

Branches of Digital Forensics:

- **Media forensics:** It is the branch of digital forensics which includes identification, collection, analysis and presentation of audio, video and image evidences during the investigation process.
- **Cyber forensics:** It is the branch of digital forensics which includes identification, collection, analysis and presentation of digital evidences during the investigation of a cyber crime.
- **Mobile forensics:** It is the branch of digital forensics which includes identification, collection, analysis and presentation of digital evidences during the investigation of a crime committed through a mobile device like mobile phones, GPS device, tablet, laptop.
- **Software forensics:** It is the branch of digital forensics which includes identification, collection, analysis and presentation of digital evidences during the investigation of a crime related to softwares only.

The Need for Computer Forensics, Cyber Forensics and Digital evidence

Cyber forensics is a process of extracting data as proof for a crime (that involves electronic devices) while following proper investigation rules to nab the culprit by presenting the evidence to the court. Cyber forensics is also known as computer forensics. The main aim of cyber forensics is to maintain the thread of evidence and documentation to find out who did the crime digitally. Cyber forensics can do the following:

- It can recover deleted files, chat logs, emails, etc
- It can also get deleted SMS, Phone calls.
- It can get recorded audio of phone conversations.
- It can determine which user used which system and for how much time.
- It can identify which user ran which program.

Why is cyber forensics important?

in todays technology driven generation, the importance of cyber forensics is immense. Technology combined with forensic forensics paves the way for quicker investigations and accurate results. Below are the points depicting the importance of cyber forensics:

- Cyber forensics helps in collecting important digital evidence to trace the criminal.
- Electronic equipment stores massive amounts of data that a normal person fails to see. For example: in a smart house, for every word we speak, actions performed by smart devices, collect huge data which is crucial in cyber forensics.
- It is also helpful for innocent people to prove their innocence via the evidence collected online.
- It is not only used to solve digital crimes but also used to solve real-world crimes like theft cases, murder, etc.
- Businesses are equally benefitted from cyber forensics in tracking system breaches and finding the attackers.

The Process Involved in Cyber Forensics

1. Obtaining a digital copy of the system that is being or is required to be inspected.
2. Authenticating and verifying the reproduction.
3. Recovering deleted files (using Autopsy Tool).
4. Using keywords to find the information you need.
5. Establishing a technical report.

How did Cyber Forensics Experts work?

Cyber forensics is a field that follows certain procedures to find the evidence to reach conclusions after proper investigation of matters. The procedures that cyber forensic experts follow are:

- **Identification:** The first step of cyber forensics experts are to identify what evidence is present, where it is stored, and in which format it is stored.
- **Preservation:** After identifying the data the next step is to safely preserve the data and not allow other people to use that device so that no one can tamper data.
- **Analysis:** After getting the data, the next step is to analyze the data or system. Here the expert recovers the deleted files and verifies the recovered data and finds the evidence that the criminal tried to erase by deleting secret files. This process might take several iterations to reach the final conclusion.
- **Documentation:** Now after analyzing data a record is created. This record contains all the recovered and available(not deleted) data which helps in recreating the crime scene and reviewing it.
- **Presentation:** This is the final step in which the analyzed data is presented in front of the court to solve cases.

Types of computer forensics

There are multiple types of computer forensics depending on the field in which digital investigation is needed. The fields are:

- **Network forensics:** This involves monitoring and analyzing the network traffic to and from the criminal's network. The tools used here are network intrusion detection systems and other automated tools.
- **Email forensics:** In this type of forensics, the experts check the email of the criminal and recover deleted email threads to extract out crucial information related to the case.
- **Malware forensics:** This branch of forensics involves hacking related crimes. Here, the forensics expert examines the malware, trojans to identify the hacker involved behind this.
- **Memory forensics:** This branch of forensics deals with collecting data from the memory(like cache, RAM, etc.) in raw and then retrieve information from that data.
- **Mobile Phone forensics:** This branch of forensics generally deals with mobile phones. They examine and analyze data from the mobile phone.
- **Database forensics:** This branch of forensics examines and analyzes the data from databases and their related metadata.

- **Disk forensics:** This branch of forensics extracts data from storage media by searching modified, active, or deleted files.

Techniques that cyber forensic investigators use

Cyber forensic investigators use various techniques and tools to examine the data and some of the commonly used techniques are:

- **Reverse steganography:** Steganography is a method of hiding important data inside the digital file, image, etc. So, cyber forensic experts do reverse steganography to analyze the data and find a relation with the case.
- **Stochastic forensics:** In Stochastic forensics, the experts analyze and reconstruct digital activity without using digital artifacts. Here, artifacts mean unintended alterations of data that occur from digital processes.
- **Cross-drive analysis:** In this process, the information found on multiple computer drives is correlated and cross-references to analyze and preserve information that is relevant to the investigation.
- **Live analysis:** In this technique, the computer of criminals is analyzed from within the OS in running mode. It aims at the volatile data of RAM to get some valuable information.
- **Deleted file recovery:** This includes searching for memory to find fragments of a partially deleted file in order to recover it for evidence purposes.

Advantages

- Cyber forensics ensures the integrity of the computer.
- Through cyber forensics, many people, companies, etc get to know about such crimes, thus taking proper measures to avoid them.
- Cyber forensics find evidence from digital devices and then present them in court, which can lead to the punishment of the culprit.
- They efficiently track down the culprit anywhere in the world.
- They help people or organizations to protect their money and time.
- The relevant data can be made trending and be used in making the public aware of it.

What are the required set of skills needed to be a cyber forensic expert?

The following skills are required to be a cyber forensic expert:

- As we know, cyber forensic based on technology. So, knowledge of various technologies, computers, mobile phones, network hacks, security breaches, etc. is required.

- The expert should be very attentive while examining a large amount of data to identify proof/evidence.
- The expert must be aware of criminal laws, a criminal investigation, etc.
- As we know, over time technology always changes, so the experts must be updated with the latest technology.
- Cyber forensic experts must be able to analyse the data, derive conclusions from it and make proper interpretations.
- The communication skill of the expert must be good so that while presenting evidence in front of the court, everyone understands each detail with clarity.
- The expert must have strong knowledge of basic cyber security.

Need for Digital Forensics: Why Digital Forensics is Important?

One of the controls financial institutions develop and implement is digital forensics, which involves the recovery and investigation of information or data related to cybercrime incidents or suspicions found or stored in the financial institution's core application system or electronic or digital devices.

Digital forensics is performed by a team of specialists and experts knowing the process and digital devices being investigated to explore facts and evidence related to particular cybercrime. Cyber forensic specialists are experts in performing investigations of encrypted data using different types of forensics software, tools, and techniques. They can crack passwords, recover deleted files, etc., to find evidence supporting the cybercrime incident. The digital forensics process includes investigating devices that may store digital data or information.

The digital forensics process requires identification, preservation, assessment, and evaluation of the digital evidence gathered. Uncovering and interpreting electronic data or information requires subject matter expertise, which is performed to identify the root cause of the particular cybercrime incident. The purpose of digital forensics is to identify and preserve the digital evidence in its most-purest form, to make it possible for relevant investigation procedures to be performed and conclusions made.

For corporates and businesses, digital forensics is a very important part related to the incident response process. The digital evidence gathered from electronic devices may be asked to be presented in a court of law. Therefore, organizations or businesses perform forensics reviews diligently and with the required care.

After an appropriate assessment of gathered digital evidence, the facts are consolidated concerning the reported digital crime or cybercrime. The findings or digital forensic reports are compiled by the digital forensic specialists and presented to the organization's senior management for review and necessary actions. Digital forensics reports may also be presented to the regulatory authorities per applicable requirements.

Specialists possess expertise in performing forensics investigations to conclude criminal or cybercrime incidents. They are experienced in searching and gathering digital evidence, considering the technical flow of data and digital footprints stored or recorded in electronic or digital devices.

Forensics Analysis of Email

The reason **email forensics** come into part of the digital forensics investigation is due to the massive and common use of emails among people nowadays.

People's using email to communicate with their friends, schoolmates, colleagues and a variety of people. Hence, numerous data and information is transmitted across its use and meanwhile some of those are illegal not surprisingly just like what other common communication approach, e.g. mobile phone, has happened as well when it was popularized to certain extend.

In fact, it's already a severe public concern that a majority of criminals are using email for their crime committed in recent years, especially when it comes to cyber security and digital crime. Not only that, increasingly noncomputer crimes and even civil litigation, has been related to emails.

That's being said, we do want to unveil the operation theory of email and thus extract **email related crimes** via email forensics to bring the criminals to justice.

What is Email Forensics?

Email forensics is dedicated to investigating, extracting, and analyzing emails to collect digital evidence as findings in order to crack crimes and certain incidents, in a forensically sound manner.

The process of email forensics, it's conducted across various aspects of emails, which mainly includes

- Email messages
- Email addresses(sender and recipient)
- IP addresses
- Date and time
- User information
- Attachments
- Passwords
- logs (Cloud, server, and local computer)

To deeply and overall investigate the above crucial elements of email, potential clues are going to be obtained to help push the progress of a criminal investigation.

Hence, knowing how to conduct scientific and effective email forensics has come into account.

But before diving deep into practical email forensics, without a full understanding of the operation and theory of emails themselves, the forensic work is likely to be stuck.

How Email Works?

Just like other digital forensics technology, it's not easy to conduct forensics without understanding the basis of the underlying technologies. Emails are probably generated from various mediums and approaches and thus different technologies are applied accordingly.

Commonly speaking, a man writes an email on his digital device, maybe a phone or computer, and then sends it to the one he wants to. Though it's seemingly the man has finished his work, the upon email processing work just starts in order to successfully and correctly be delivered to the recipient.

When an email is sent out, countless servers are actually undertaken the whole information of the email before it can really arrive in the recipient's inbox, which is said that we have to understand what's proceeding after we click the "send" button.

Email Programs and Protocols

During the process, there are 3 protocols and 3 email programs tightly related and are vital to be known.

- Simple Mail Transfer Protocol (SMTP): it is the standard Protocol used to transmit and send emails.
- Internet Message Access Protocol (IMAP): it is one of the standard protocols used for receiving emails.
- POP3 (Post Office Protocol 3): it is one of the standard protocols used to receive mail.
- Mail Transfer Agent (MTA): sends and forwards emails through SMTP. e.g. Sendmail, postfix.
- Mail User Agent (MUA): mail client used to receive emails, which uses IMAP or POP3 protocol to communicate with the server. e.g. Outlook, Apple Mail, Gmail.
- Mail Delivery Agent (MDA): saves the mails received by MTA to local, cloud disk or designated location, meanwhile it usually scans for spam mails and viruses. e.g. Promail, Dropmail.
- Mail Receive Agent (MRA): implements IMAP and POP3 protocol, and interacts with MUA. e.g. dovecot

The theory of email running

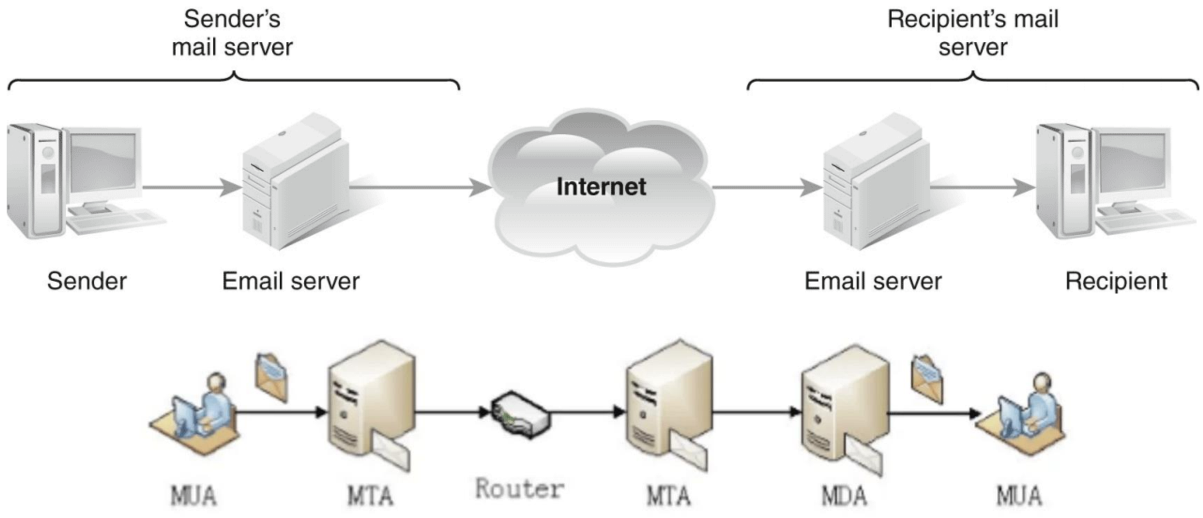


Figure 1: E-mail architecture
Source: Guo,Hong. Jin,Bo. Qian, Wei. 2013 [1]

Let's take an example below for instance to better explain the theory of email running.

- **STEP 1:** To start, someone creates an email with a Mail User Agent (MUA), typical MUAs include Gmail, Apple Mail, Mozilla Thunderbird, and Microsoft Outlook Express.
- **STEP 2:** Regardless of the MUA used, the mail is created and sent to the user's mail transfer agent (MTA) – the delivery process uses the SMTP protocol.
- **STEP 3:** The MTA then checks the recipient of the message (here we assume it is you), queries the DNS server for the domain name corresponding to the recipient MTA, and sends the message to the recipient MTA – again using the SMTP protocol.

At this moment, the mail has been sent from the remote user's workstation to his ISP(Internet Server Provider)'s a mail server and forwarded to your domain.
What will happen next?
Considering different network configurations, it is very likely that the mail will be transferred to another MTA during the transmission process, but eventually, an MTA will take over the mail and be responsible for delivery. Then, the MTA will deliver the mail to a mail delivery agent (MDA).
The main function of the MDA is to save the mail to the local disk. Specific MDAs can also be developed with other functions, such as mail filtering or direct mail delivery to other file locations. Thus, it should be noted that it is MDA that completes the function of storing mail on the server.

- **STEP 4:** Now, it’s time for you to check your mail.

Running MUA, you can use the IMAP protocol or POP3 protocol to query the mail server for your mail. The mail server first confirms your identity, then retrieves the mailing list from the mail store and returns the list to the MUA.

Now you can read the message.

Message location of an email

Even if we know the running theory of emails, it’s recommended to be noted that different configuration on the recipient’s email client varies the copies of the message to be saved.

Additionally, any server that sends a message from a party to a recipient can keep a copy of the email.

With the above root principle, it’s going to equip your initial ideas before conducting your **email investigation**.

How to Conduct Email Forensics Investigation?

With the increasing popularity of the use of email based on the boom of the internet, some typical crimes are tied to email. For instance, financial crime, cyber security, and extortion software, to name a few.

To bring **email criminals** to justice, it’s crucial to look into **email investigation in cyber security**.

Before we can dive into the major investigative extraction working directions of email forensics, be noted:

1. Local Computer-based emails: For local computer-based email data files, such as Outlook .pst or .ost files, it’s recommended to follow our following techniques directly.
2. （Cloud）Server-based emails: For （Cloud）Server based email data files, it’s not possible to conduct complete forensic work until you obtain the electronic copies in the (Cloud)server database under the consent of the service providers.
3. Web-based emails: For Web-based e-mail (e.g. Gmail,) investigations, it’s more likely possible to just filter specific keywords to extract email address-related information instead of the overall email data and information compared to local computer-based emails.

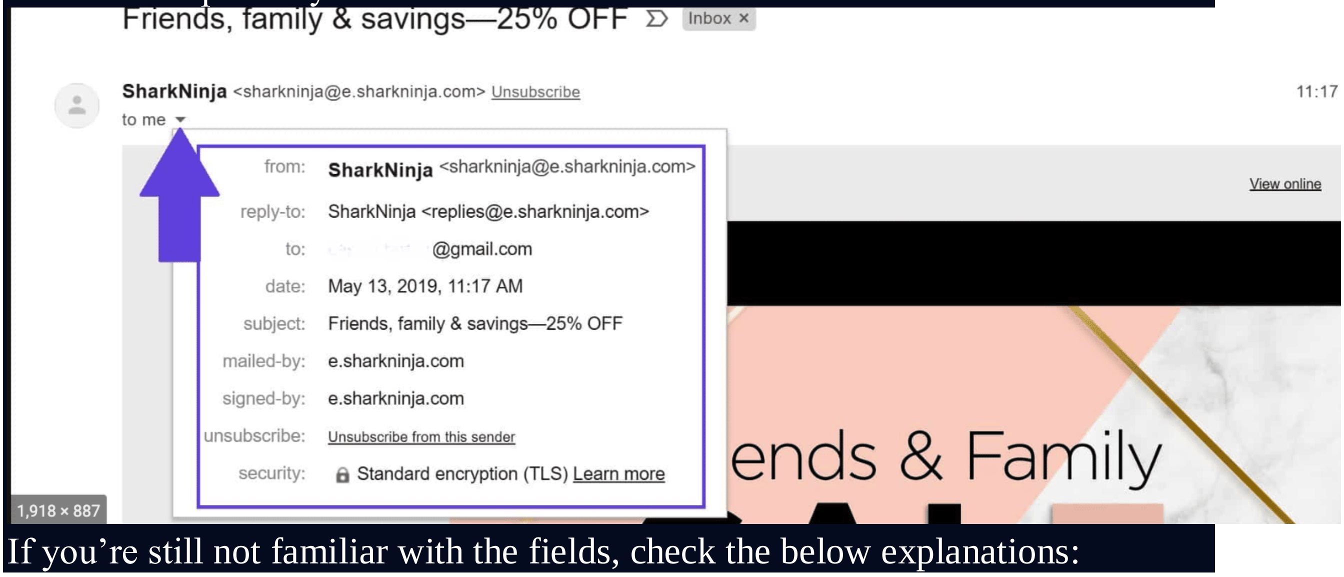
Viewing and Analyzing E-mail Headers

The primary evidence in email investigations is the email header where massive and valuable information could be found.

When carrying out the analysis, you'd be advised to get started from the bottom to the top, since the most crucial information from the sender would be on the bottom while information about the receiver would be on the topmost.

Since we already talked about MTAs where you could find out the route of the email transferred, it should be good for you to give it a detailed scan of the email header.

Here's a sample for your information:



Friends, family & savings—25% OFF

SharkNinja <sharkninja@e.sharkninja.com> Unsubscribe
to me
11:17

from: SharkNinja <sharkninja@e.sharkninja.com>
reply-to: SharkNinja <replies@e.sharkninja.com>
to: [redacted]@gmail.com
date: May 13, 2019, 11:17 AM
subject: Friends, family & savings—25% OFF
mailed-by: e.sharkninja.com
signed-by: e.sharkninja.com
unsubscribe: Unsubscribe from this sender
security: 🔒 Standard encryption (TLS) Learn more

If you're still not familiar with the fields, check the below explanations:

- From: Address of the actual sender acting on behalf of the author listed in the From field
- To: The email address and, optionally, the name of the message's primary recipient(s)
- Cc: Carbon copy; a copy is sent to secondary recipients
- Bcc: Blind carbon copy; a copy is sent to addresses added to
- Subject: A brief summary of the topic of the message
- Date: A brief summary of the topic of the message
- (In)Reply-To: The message-ID of the message that this is a reply to; used to link related messages together
- Message-ID: An automatically generated field
- Content-Type: Information about how the message is to be displayed, usually a Multipurpose Internet Mail Extensions (MIME) type
- Precedence: —Commonly with values "bulk," "junk," or "list"; used to indicate that automated "vacation" or "out of office" responses should not be returned for this mail, for example, to prevent vacation notices from being sent to all other subscribers of a mailing list
- Received: Tracking information generated by mail servers that have previously handled a message, in reverse order (last handler first)
- References: Message-ID of the message to which this is a reply

The main piece of information you're looking for is the originating e-mail's domain address or IP address. Other than that, helpful information includes the date and time the message was sent, filenames of any attachments, and unique message number, if it's supplied.

Give all of them a complete analysis before you move to the next step.

Email Server Investigation

To locate the source of an email, it's required to investigate the email's servers. Since it's not surprising criminals tend to delete their emails in case of being caught or accused of sensitive emails.

However, there is still a chance to get them back.

In extreme cases, even though both emails have been deleted from both sides between senders and recipients, a copy might be still on the server, since there is always retention on the server after the email is successfully delivered each time due to specific government regulations for email.

Whereas, you don't want to miss out on investigating the log before it is archived after a certain period.

For your better work implementation, take below most popular email server software under consideration:

- Exchange Server (.edb)
- Exchange Public Folders (pub.edb)
- Exchange Private Folders (priv.edb)
- Streaming Data (priv.stm)
- Lotus Notes (.nsf)
- GroupWise (.db)
- GroupWise Post Office Database (wphost.db)
- GroupWise User Databases (userxxx.db)
- Linux Email Server Logs/var/log/mail.*

Network Devices

If there is no log from the email server due to various reasons, for instance, incorrect configuration on the email server, another approach is worth trying, which is the network service.

In certain cases, an internet service provider (ISP) or any other communications network stores an email. Therefore, investigators are recommended to examine the network devices such as routers and there might be chances for some clue of the source of an email.

Software embedded identifiers

When looking deep enough at the email software, a higher level analysis of the extra information on it comes into account.

Actually, information about the sender and attached files could be found sometimes in an email when you technically examine it, since in most cases, the senders tend to customize their header under Multipurpose Internet Mail Extensions (MIME) with a Transport Neutral Encapsulation Format(TNEF).

Attachment Analysis

As is known to us all, sometimes, our computer gets infected when we surf the Internet and open specific files. To cause the issue, viruses and malware are most skeptical.

When it comes to emails, it's also very common for a problematical attachment to be found and thus it's really worth investigating the attached files.

However, if the files happened to be deleted, you're suggested to consult with a digital forensic agency or use **email forensics tools** like DRS to recover files so that you could better examine every piece of them.

After the attachment's retrieval, you'd better analyze those suspicious files under a sandbox environment in case the file is malware and do harm to your computer.

Bulk Email Forensics

Significant mailbox collections tend to be examined, analyzed, and used as proof in legal instances. Therefore, legal experts have to work with large mailboxes in many circumstances. Most email service applications, like Perspective and Gmail, give a dashboard embedded with several valuable functions.

However, you might not get the desired results by only using keywords in the interface. Day and time are two attributes of emails considered necessary if they are produced as evidence related to an instance.

Also, email messages can be forged like physical documents, and hackers may tamper with these attributes. Moreover, since an email doesn't directly reach the receiver to the sender, recording its actual way with accurate timings is a challenging aspect.

MD5 and SHA1 Hash Values

MD5 and SHA1 would be the two most crucial hashing algorithms utilized by digital forensics professionals since it's standard practice to make use of MD5 and SHA1 hashing algorithms in email forensics brought on. These algorithms enable forensic investigators to aid digital evidence as soon as they acquire this until it finally is created in a courtroom of law.

One more reason why hash values are crucial is usually that electronic documents are shared with legal professionals and various other parties in the analysis.

Therefore, making certain every person has identical replicates of the data files is vital.

Consider how many places an email may well be saved. This could be preserved on the sender's equipment, around the recipient's machine, on either the sender's or recipient's email server, or both, and in backup media with regard to either server. In the event that you consider the many places the email could stay, that should indicate to you that that is rare for an email is usually ever truly deleted. It may always be quite difficult to get, yet it probably is out there somewhere. This is definitely one of the reasons for this why email forensics is so important.

One will need to sign into the e-mail support in order to be able to analyze emails. Google mail and similar services do not provide any kind of mechanism to access a message if that has been wiped from the trash folder.
In that circumstance, it's likely not possible to be covered.
In some cases, some sort of subpoena can be issued to the service agency, and it may well search backups intended for the missing electronic mail

Email Tracking in Cyber Security

- Js code tracking

To better locate or identify a suspect email address, it's important to attract the suspect to open a trackable email. Across cases like kidnapping and murder, it's commonly used to identify criminals.

By inserting a specific J.S code along HTTP: "   img sr" tag on an image within the body of your email, it's going to be able to record at least the IP address after the suspect clicks the image, especially when the location of a suspect or cybercriminal is unknown.

- Traced information identify

When acquiring tracking information, it's no doubt to identify the information in hand to look for some clues that will benefit your forensic investigation in a way. Below is the manual method for IP address identification where you could figure out detailed information about the IP's owner.

- http://www.whois.net
- http://www.networksolutions.com/whois/index.jsp

- http://www.who.is
- http://www.internic.net/whois.html
- http://cqcounter.com/whois/

Smart Email Forensic Investigation Suggestions

Whenever there are suspects coming to you, you're bound to be monitoring their activities. As an example, administrators might obtain security checks by collaborating with an employee who definitely seems to be disgruntled or that has access to sensitive information.

This employee's **email logs** and network use may, for example, show the puppy sending innocent family images to a Hotmail account, but no traffic heading back from that Hotmail account. These kinds of seemingly innocent pics might carry steganographically hidden messages, and so provide proof of the employee's part in corporate espionage.

Forensic email doing a trace is similar to traditional gumshoe investigator work, which involves looking at each point through which an email passed.

An individual works comprehensively back to the beginning computer and, eventually, the perpetrator.

Correctly manage the email forensic evidence

Digital evidence in the form of email data can be crucial in civil and criminal cases. However, be sure it is extracted in the correct manner using email forensics.

- The email data is extracted in full and there is no question whether all data has been recovered
- The validity of the data can be relied upon in both civil and criminal courts as admissible evidence
- Ensures that no changes are made to the email metadata
- It is compliant with the ACPO guidelines and the quality standards set out within the ISO17025 documentation and Forensic Science Regulator's Codes of Good Practice and Conduct.
- Any deleted emails and files are recovered where possible

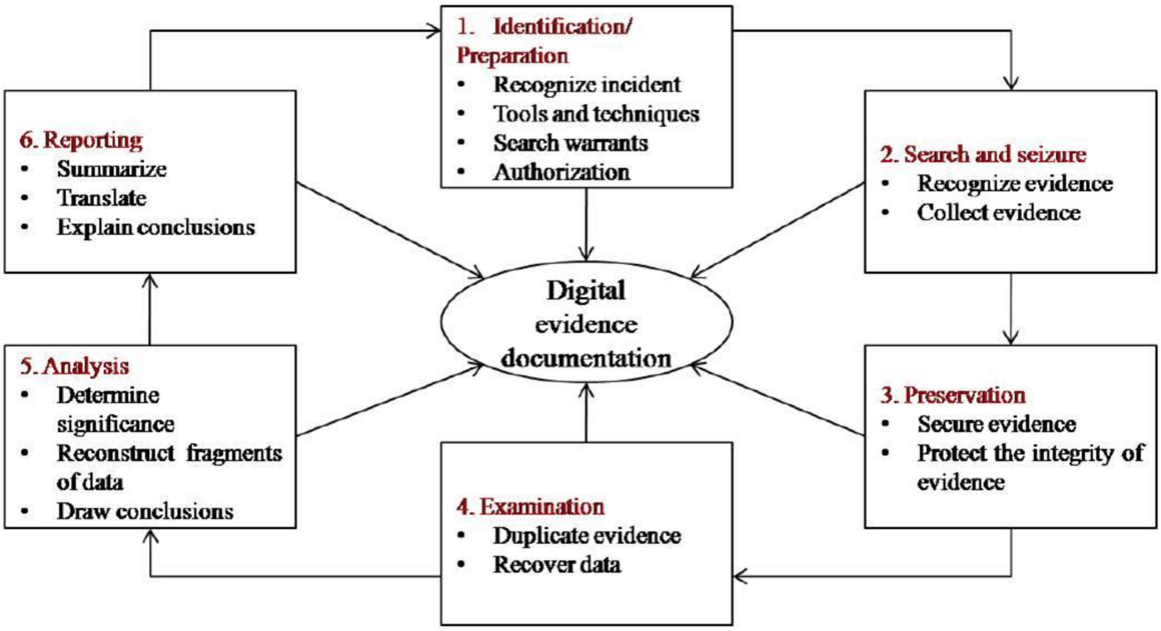
Digital Forensics Lifecycle

The digital forensics process is shown in the following figure.

Forensic life cycle phases are:

1. Preparation and identification
2. Collection and recording
3. Storing and transporting
4. Examination/investigation
5. Analysis, interpretation, and attribution
6. Reporting
7. Testifying

Watch the below video to learn about digital forensics life cycle:



1. Preparing for the Evidence and Identifying the Evidence

In order to be processed and analysed, evidence must first be identified. It might be possible that the evidence may be overlooked and not identified at all. A sequence of events in a computer might include interactions between:

- Different files
- Files and file systems
- Processes and files
- Log files

In case of a network, the interactions can be between devices in the organization or across the globe (Internet). If the evidence is never identified as relevant, it may never be collected and processed.

2. Collecting and Recording Digital Evidence

Digital evidence can be collected from many sources. The obvious sources can be:

- Mobile phone
- Digital cameras
- Hard drives
- CDs
- USB memory devices

Non-obvious sources can be:

- Digital thermometer settings
- Black boxes inside automobiles
- RFID tags

Proper care should be taken while handling digital evidence as it can be changed easily. Once changed, the evidence cannot be analysed further. A cryptographic hash can be calculated for the evidence file and later checked if there were any changes made to the file or not. Sometimes important evidence might reside in the volatile memory. Gathering volatile data requires special technical skills.

3. Storing and Transporting Digital Evidence

Some guidelines for handling of digital evidence:

- Image computer-media using a write-blocking tool to ensure that no data is added to the suspect device
- Establish and maintain the chain of custody
- Document everything that has been done
- Only use tools and methods that have been tested and evaluated to validate their accuracy and reliability

Care should be taken that evidence does not go anywhere without properly being traced. Things that can go wrong in storage include:

- Decay over time (natural or unnatural)
- Environmental changes (direct or indirect)
- Fires
- Floods
- Loss of power to batteries and other media preserving mechanisms

Sometimes evidence must be transported from place to place either physically or through a network. Care should be taken that the evidence is not changed while in transit. Analysis is generally done on the copy of real evidence. If there is any dispute over the copy, the real can be produced in court.

4. Examining/Investigating Digital Evidence

Forensics specialist should ensure that he/she has proper legal authority to seize, copy and examine the data. As a general rule, one should not examine digital information unless one has the legal authority to do so. Forensic investigation performed on data at rest (hard disk) is called dead analysis.

Many current attacks leave no trace on the computer's hard drive. The attacker only exploits the information in the computer's main memory. Performing forensic investigation on main memory is called live analysis. Sometimes the decryption key might be available only in RAM. Turning off the system will erase the decryption key. The process of creating and exact duplicate of the original evidence is called imaging. Some tools which can create entire hard drive images are:

- DCFLdd
- Iximager
- Guymager

The original drive is moved to secure storage to prevent tampering. The imaging process is verified by using the SHA-1 or any other hashing algorithms.

5. Analysis, Interpretation and Attribution

In digital forensics, only a few sequences of events might produce evidence. But the possible number of sequences is very huge. The digital evidence must be analyzed to determine the type of information stored on it. Examples of forensics tools:

- Forensics Tool Kit (FTK)
- EnCase
- Scalpel (file carving tool)
- The Sleuth Kit (TSK)
- Autopsy

Forensic analysis includes the following activities:

- Manual review of data on the media
- Windows registry inspection
- Discovering and cracking passwords
- Performing keyword searches related to crime
- Extracting emails and images

Types of digital analysis:

- Media analysis
- Media management analysis
- File system analysis
- Application analysis
- Network analysis
- Image analysis
- Video analysis

6. Reporting

After the analysis is done, a report is generated. The report may be in oral form or in written form or both. The report contains all the details about the evidence in analysis, interpretation, and attribution steps. As a result of the findings in this phase, it should be possible to confirm or discard the allegations. Some of the general elements in the report are:

- Identity of the report agency
- Case identifier or submission number

- Case investigator
- Identity of the submitter
- Date of receipt
- Date of report
- Descriptive list of items submitted for examination
- Identity and signature of the examiner
- Brief description of steps taken during examination
- Results / conclusions

7. Testifying

This phase involves presentation and cross-examination of expert witnesses. An expert witness can testify in the form of:

- Testimony is based on sufficient facts or data
- Testimony is the product of reliable principles and methods
- Witness has applied principles and methods reliably to the facts of the case

Experts with inadequate knowledge are sometimes chastised by the court. Precautions to be taken when collecting digital evidence are:

- No action taken by law enforcement agencies or their agents should change the evidence
- When a person to access the original data held on a computer, the person must be competent to do so
- An audit trial or other record of all processes applied to digital evidence should be created and preserved
- The person in-charge of the investigation has overall responsibility for ensuring that the law and these are adhered to

Chain of Custody

A chain of custody is the process of validating how evidences have been gathered, tracked, and protected on the way to the court of law. Forensic professionals know that if you do not have a chain of custody, the evidence is worthless.

The chain of custody is a chronological written record of those individuals who have had custody of the evidence from its initial acquisition to its final disposition. A chain of custody begins when an evidence is collected and the chain is maintained until it is disposed off. The chain of custody assumes continuous accountability.

Forensics Investigation

What is forensic investigation? Forensics is the scientific method used to solve a crime. Forensic investigation is the gathering and analysis of all crime-related physical evidence to conclude a suspect. Forensic investigation is the gathering and analysis of all physical evidence related to a crime in order to reach a conclusion about a suspect. To determine how a crime occurred, investigators will examine blood, fluid, or fingerprints, residue, hard drives, computers, or other technology.

What Is Forensic Investigation?

A forensic investigation is a practice of lawfully establishing pieces of evidence that have to be presented in a court of law. It includes all investigations, ranging from cases of financial fraud to murder. When most people think about forensics, they think about crime scene investigation, in which physical evidence is gathered. There are other forms of forensic investigation, however, such as computer forensics and sub-fields that focus on dentistry or insects and crime scenes.

Crime scenes forensics

The type of forensic investigation revolves around crimes. Forensics used in these investigations can uncover scientific evidence that may provide enough proof or evidence to convict a criminal. These methods can also help disprove outdated evidence that could lead to the release of someone who was wrongly convicted.

One of the main kinds of evidence this form of forensic investigation yields is biological evidence. Impression evidence, like fingerprints, helps connect people to a crime scene or victim. After the evidence is carefully collected, it is sent for processing.

Computer forensics

A fast-growing division of forensics involves digital or computer investigations. It is a branch of science that involves evidence found in digital storage mediums and computers. This field of forensic investigation has several subdivisions.

Digital forensic investigation is useful in a variety of situations. Investigators use different programs and utilities to recover lost data after a system-wide computer crash. Careful handling and presentation of digital evidence are necessary for it to remain admissible in a courtroom setting.

Other forensic fields

There are several other subdivisions of forensic investigation that can be used for the collection of evidence. Investigators specializing in entomology conduct examinations of insects on or near human remains, which can help determine the location and time of death. Forensic odontology is the investigation of dentition, or teeth, which is often crucial in identifying the remains of a victim. Other subdivisions include forensic anthropology, geology, and toxicology. Investigators in all of these divisions use exacting techniques to collect data to help prove or disprove accusations of criminal or civil wrongdoing.

Forensic Accounting / Auditing

Victims of fraud or financial crimes benefit from forensic accounting investigations. This type of analysis, also known as financial investigation, employs intelligence gathering techniques, accounting, business, and communication skills to provide evidence to attorneys involved in criminal and civil investigations. They conduct investigations by sifting through a large amount of relevant data, looking for irregularities or illegal financial practices. Tax evasion and asset theft are examples of crimes. They also investigate insurance claims and large payouts.

Challenges in Computer Forensics

Challenges with cyber forensics

Cyber forensics experts extract data from a variety of sources — any technologies that may be used by an end-user. These include mobile devices, cloud computing services, IT networks and software applications.

These technologies are developed and operated by distinct vendors. The technology limitations and privacy measures tend to restrict investigative capacity of an individual InfoSec expert as they face the following challenges:

- **Data recovery.** If the data is encrypted, the investigator will not be able to decrypt the information without access to encryption keys. New storage tools such as SSD devices may not offer immediate factory access to recover lost data, unlike traditional magnetic tape and hard disk drive systems.
- **Visibility into cloud system.** Investigators may only have access to metadata but not the information content of the files. The underlying resources may be shared and allocated dynamically. That lack of access to physical storage systems means that lost data may not be recovered by third party investigators.
- **Network log big data.** Network log data grows exponentially and requires advanced analytics and AI tools to connect the dots and find insightful relationships between networking activities.
- **Multi-jurisdiction data storage.** If the data is stored in a different geographic location, cyber forensics investigators may not have the legal authority to access the required information.

Challenges in network forensics

- Networks span multiple time zones and multiple jurisdictions
- Network data will be available offline and online (real-time)
- Real-time data requires ability to capture and analyze data on the fly
- The data may involve different protocols
- The data may be huge due to increasing bandwidth
- A protocol might also involve multiple layers of signal (VoIP, HTTP tunneling)
- Current forensic tools will not be able to handle real-time data and huge amount of data

There need to be a paradigm shift for network forensics techniques to analyze the real-time data and huge amounts of data. Duration of forensics investigation may vary, some simple cases might take a few hours and complex cases may take some years to solve.

Certain digital information other than the data itself may help in solving the case. Such information might include, data and timestamps of files, folder structure and message transmission tags. Real-time data collection is more complex as it needs to address legalities and privileges involved in surveillance.

Technical Challenges

The two challenges faced in a digital forensic investigation are complexity and quantity. The complexity problem refers to the data collected being at the lowest level or in raw format. Non-technical people will find it difficult to understand such data.

Tools can be used to transform the data from low level format to readable format. The quantity problem refers to the amount of data that needs to be analyzed. Data reduction techniques can be used to group data or remove known data. Data reduction techniques include:

- Identifying known network packets using IDS signatures
- Identifying unknown entries during log processing
- Identifying known files using hash databases
- Sorting files by their types

Legal challenges

Digital evidence can be tampered easily, sometimes, even without any traces. It is common for modern computers to have multiple gigabyte sized disks. Seizing and freezing of digital evidence can no longer be accomplished just by burning a CD-ROM. Failure to freeze the evidence prior to opening files has invalidated critical evidence.

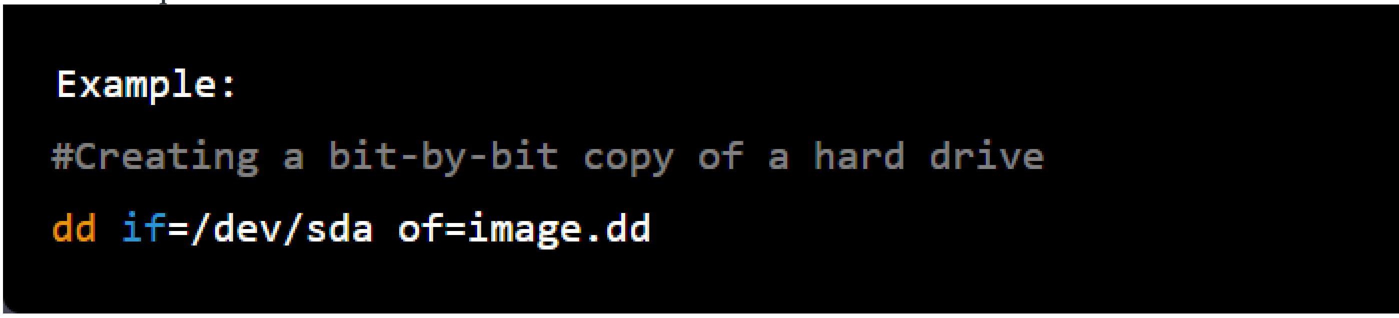
There is also the problem of finding relevant evidence within massive amounts of data which is a daunting task. The real legal challenges involve the artificial limitations imposed by constitutional, statutory and procedural issues. There are many types of personnel involved in digital/computer forensics like technicians, policy makers, and professionals.

Technicians have sound knowledge and skills to gather information from digital devices, understand software and hardware as well as networks. Policy makes establish forensics policies that reflect broad considerations. Professionals are the link between policy and execution who have extensive technical skills as well as good understanding of the legal procedures.

Digital forensics also known as computer forensics, is the application of scientific methods and techniques to identify, preserve, analyze, and present digital evidence in a manner that is legally admissible. It is a branch of forensic science that deals specifically with digital devices, networks, and storage media.

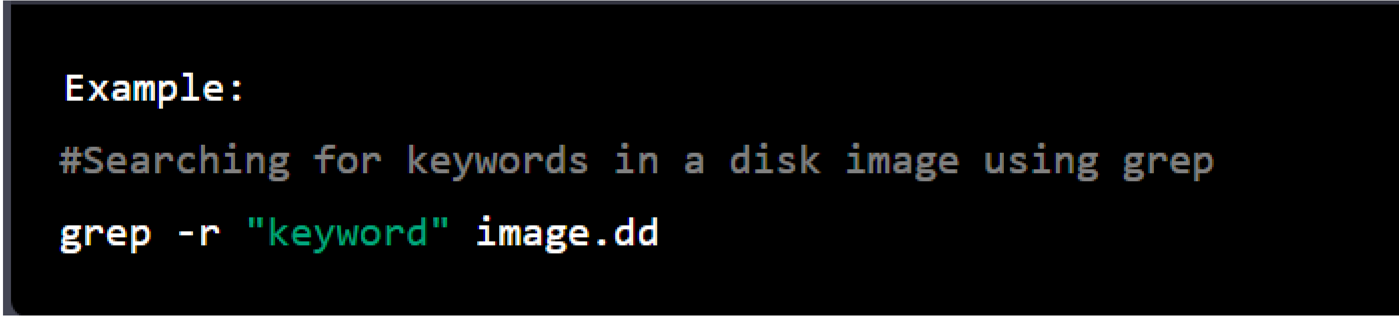
Techniques Used in Digital Forensics

- **Acquisition:** The process of collecting digital evidence from a device or network. This is done through various methods such as imaging, logging, and live acquisition.



```
Example:
#Creating a bit-by-bit copy of a hard drive
dd if=/dev/sda of=image.dd
```

Analysis: The process of examining the acquired evidence to identify relevant information. This can be done through manual or automated means.

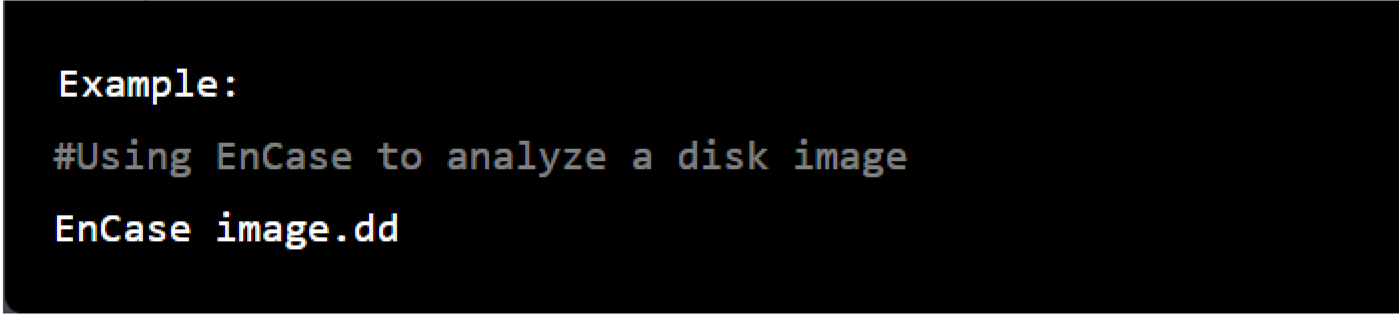


```
Example:
#Searching for keywords in a disk image using grep
grep -r "keyword" image.dd
```

- **Reporting:** The process of documenting the findings of the analysis and presenting them in a clear and concise manner. This can include creating a detailed report, as well as providing expert testimony in court.

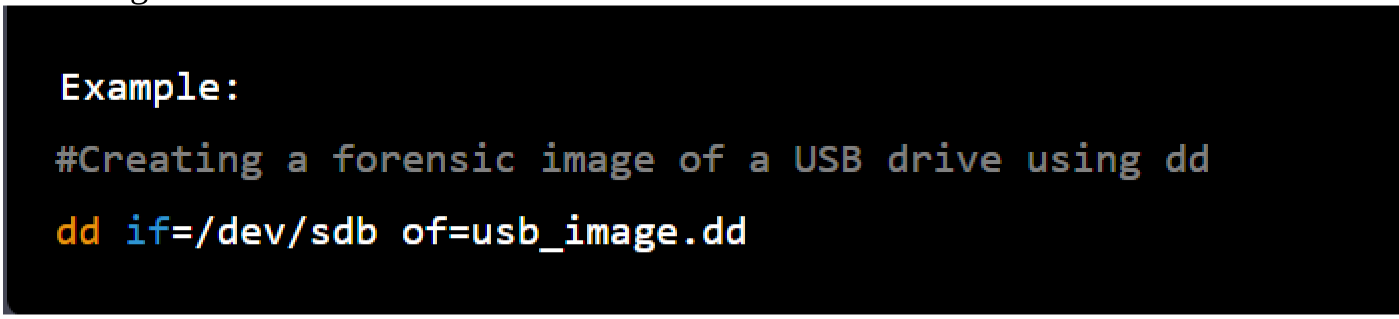
Tools Used in Digital Forensics

- **Forensic Software:** Specialized software that can analyze and extract data from digital devices and networks. Some examples include EnCase, FTK, and X-Ways Forensics.



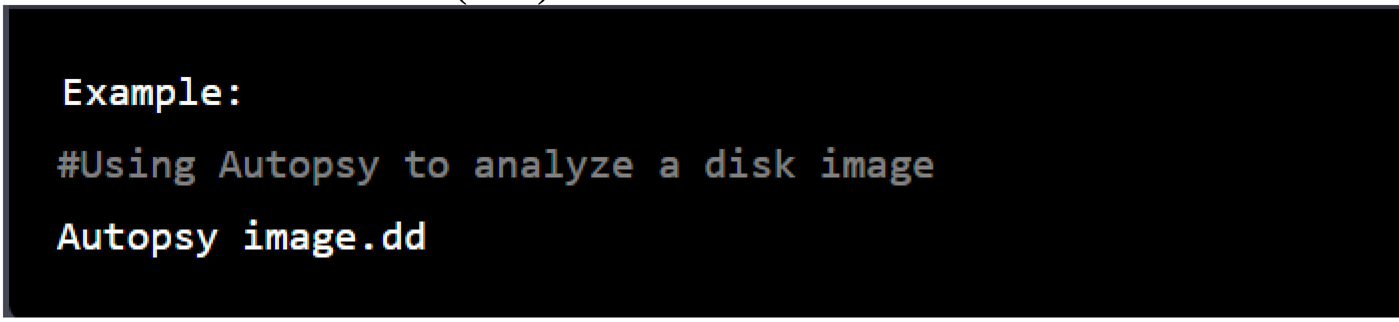
```
Example:
#Using EnCase to analyze a disk image
EnCase image.dd
```

- **Forensic Imaging:** The process of making a bit-by-bit copy of a digital device or network, also known as disk cloning or disk imaging. This can be done through hardware or software means.



```
Example:
#Creating a forensic image of a USB drive using dd
dd if=/dev/sdb of=usb_image.dd
```

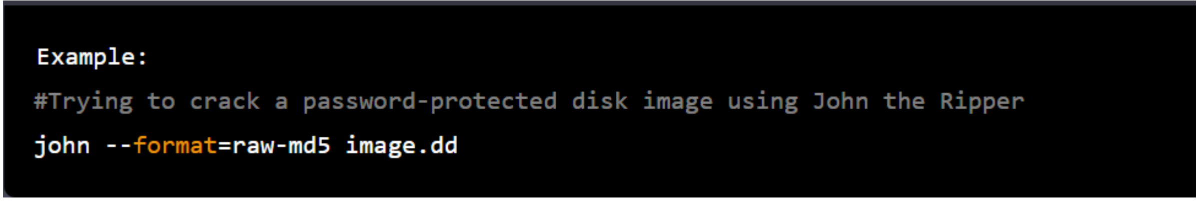
- **Forensic Analysis Software:** Used to analyze the data from a forensic image. Examples include Sleuth Kit, Autopsy, and the open-source toolkit The Coroner’s Toolkit (TCT).



```
Example:
#Using Autopsy to analyze a disk image
Autopsy image.dd
```

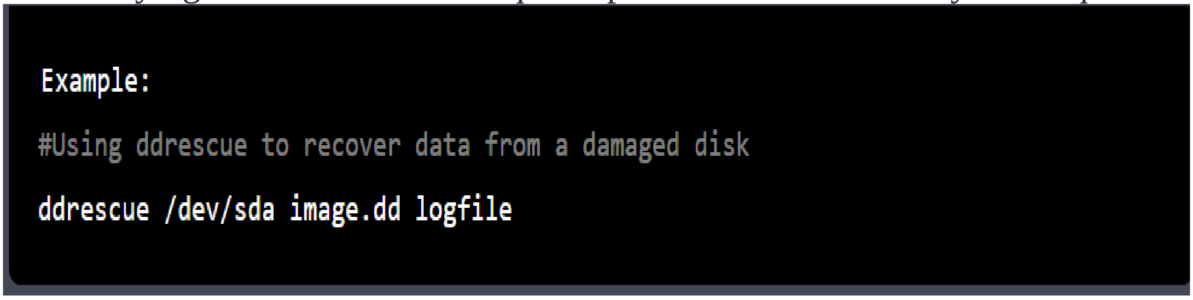
Challenges in Digital Forensics

Data Encryption: Encryption can make it difficult to access the data on a device or network, making it harder for forensic investigators to collect evidence. This can require specialized decryption tools and techniques.



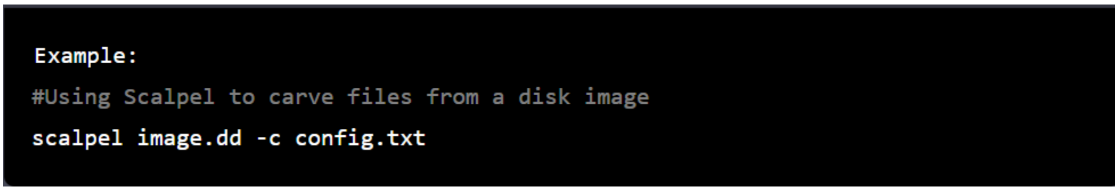
```
Example:
#Trying to crack a password-protected disk image using John the Ripper
john --format=raw-md5 image.dd
```

Data Destruction: Criminals may attempt to destroy digital evidence by wiping or destroying devices. This can require specialized data recovery techniques.



```
Example:
#Using ddrescue to recover data from a damaged disk
ddrescue /dev/sda image.dd logfile
```

Data Storage: The sheer amount of data that can be stored on modern digital devices can make it difficult for forensic investigators to locate relevant information. This can require specialized data carving techniques to extract relevant information.



```
Example:
#Using Scalpel to carve files from a disk image
scalpel image.dd -c config.txt
```

Digital forensics is a rapidly evolving field that requires a combination of technical knowledge, an understanding of legal principles, and investigative skills to be successful.