Unit V: Collecting Evidence: Crime Scenes and collecting Evidence – Documenting the Scene – Chain of Custody – Cloning- Live Stream versus Dead System – Hashing – Final report. Mobile Device Forensics: Cellular Networks – Operating Systems – Cell phone evidence – Cell phone Forensic Tools.

COLLECTING EVIDENCE

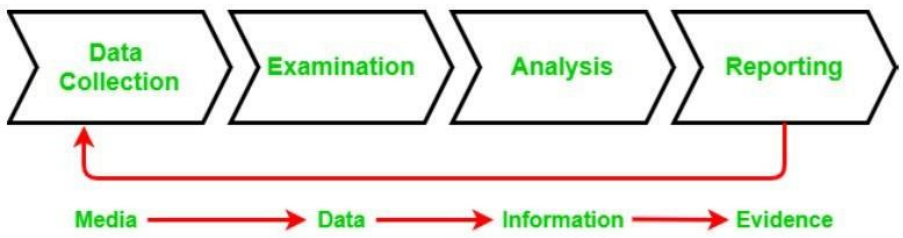
In the early 80s PCs became more popular and easily accessible to the general population, this also led to the increased use of computers in all fields and criminal activities were no exception to this. As more and more computer-related crimes began to surface like computer frauds, software cracking, etc. the computer forensics discipline emerged along with it. Today digital evidence collection is used in the investigation of a wide variety of crimes such as fraud, espionage, cyberstalking, etc. The knowledge of forensic experts and techniques are used to explain the contemporaneous state of the digital artifacts from the seized evidence such as computer systems, storage devices (like SSDs, hard disks, CD-ROM, USB flash drives, etc.), or electronic documents such as emails, images, documents, chat logs, phone logs, etc.

CRIME SCENES AND COLLECTING EVIDENCE

Process involved in Digital Evidence Collection:

The main processes involved in digital evidence collection are given below:

- **Data collection:** In this process data is identified and collected for investigation.
- **Examination:** In the second step the collected data is examined carefully.
- **Analysis:** In this process, different tools and techniques are used and the collected evidenceis analyzed to reach some conclusion.
- **Reporting:** In this final step all the documentation, reports are compiled so that they can be submitted in court.



Types of Collectible Data:

The computer investigator and experts who investigate the seized devices have to understand what kind of potential shreds of evidence could there be and what type of shreds of evidence they are looking for. So, that they could structure their search pattern. Crimes and criminal

activities that involve computers can range across a wide spectrum; they could go from trading illegal things such as rare and endangered animals, damaging intellectual property, to personal data theft, etc.

The investigator must pick the suitable tools to use during the analysis. Investigators can encounter several problems while investigating the case such as files may have been deleted from the computer, they could be damaged or may even be encrypted, So the investigator should be familiar with a variety of tools, methods, and also the software to prevent the data from damaging during the data recovery process.

There are two types of data, that can be collected in a computer forensics investigation:

- **Persistent data:** It is the data that is stored on a non-volatile memory type storage device such as a local hard drive, external storage devices like SSDs, HDDs, pen drives, CDs, etc. the data on these devices is preserved even when the computer is turned off.
- **Volatile data:** It is the data that is stored on a volatile memory type storage such as memory, registers, cache, RAM, or it exists in transit, that will be lost once the computer is turned off or it loses power. Since volatile data is evanescent, it is crucial that an investigator knows how to reliably capture it.

Types of Evidence:

Collecting the shreds of evidence is really important in any investigation to support the claims in court. Below are some major types of evidence.

- **Real Evidence:** These pieces of evidence involve physical or tangible evidence such as flash drives, hard drives, documents, etc. an eyewitness can also be considered as a shred of tangible evidence.
- **Hearsay Evidence:** These pieces of evidence are referred to as out-of-court statements. These are made in courts to prove the truth of the matter.
- **Original Evidence:** These are the pieces of evidence of a statement that is made by a person who is not a testifying witness. It is done in order to prove that the statement was made rather than to prove its truth.
- **Testimony:** Testimony is when a witness takes oath in a court of law and gives their statement in court. The shreds of evidence presented should be authentic, accurate, reliable, and admissible as they can be challenged in court.

Challenges Faced During Digital Evidence Collection:

- Evidence should be handled with utmost care as data is stored in electronic media and itcan get damaged easily.
- Collecting data from volatile storage.
- Recovering lost data.
- Ensuring the integrity of collected data.

Recovering information from devices as the digital shreds of evidence in the investigation are becoming the fundamental ground for law enforcement and courts all around the world. The methods used to extract information and shreds of evidence should be robust to ensure that all the related information and data are recovered and is reliable. The methods must also be legally defensible to ensure that original pieces of evidence and data have not been altered in any way and that no data was deleted or added from the original evidence.

DOCUMENTING THE SCENE

Digital Crime Scène Documentation In recent years an important progress has been achieved in the digital documentation of crime scenes. Processing and documentation have been made more efficient and now provide complete, 360 degree, and even 3D documentation of the crime scene. The documentation of the digital crime scene involves properly documenting the digital evidence when it is found. The exact copy of the system has the same role as the sketches and video of a physical crime scene. Each piece of digital evidence that is found during the analysis of the image must be clearly documented [13]. A record of all visible data must be created, which helpsin recreating the scene and reviewing it at time. This is particularly important when the forensic specialist has to give a testimony in a court, which could be several months after the investigation [6]. For example, a file can be documented using its full file name path, the clustersin the file system that it uses, and the sectors on the disk that it uses. Network data can be documented with the source and target addresses at various network layers. Finally, the need requires proper documentation of the digital crime scene and physical crime scene perspectives. And different forms of camera/video photography, graphics are used, and notes are made on the document and all relevant information relating to the crime scene. Documentation at the scene is also the starting point for the chain-custody. Table (3) gives a comparison between the physical crime scene documentation and digital crime scene documentation

Physical Crime Scène Documentation	*Digital Crime Scène Documentation*
Physical evidence has existed for thousands of years.	Digital evidence has recently become more common.
Documentation aims at producing a permanent, objective record of the scene, of the physical evidence and of any changes that take place.	Documentation aims at producing permanent, objective of the scene of each piece of information on digital evidence found.
Physical evidence (the actual computer, hard disk, PDA, and CD-ROM).	Digital evidence (the data in memory, on the hard disk, or in a cell phone, etc).
The laws of nature bind the physical world.	The instructions in hardware and software bind the digital world.
Documenting the physical evidence by the sketches and vides and other.	Documenting the digital evidence by exact copy of the system.
All items that are used to document are non-volatile	Most items that are documented are volatile data and there is always a possibility for the perpetrator to erase them.
The time within which the evidences are secured is less important.	The time within which the evidences are secured is more important.

CHAIN OF CUSTODY

Chain of Custody refers to the logical sequence that records the sequence of custody, control, transfer, analysis and disposition of physical or electronic evidence in legal cases.Each step in the chain is essential as if broke, the evidence may be rendered inadmissible. Thus we can say that preserving the chain of custody is about following the correct and consistent procedure and hence ensuring the quality of evidence.

In this article, we will be discussing-

1. ***What Chain of Custody entails in Digital Forensics.***
2. ***Importance of maintaining Chain of Custody.***
3. ***Chain of Custody Process.***
4. ***The Chain of Custody Form.***
5. ***Procedure to establish the Chain of Custody***
6. ***How Chain of Custody can be assured?***

Let's get started with each section in detail.

What the Chain of Custody entails in Digital Cyber Forensics?

If you are in the field of Cyber Security, you will be at one point in your career will be involved in Digital Forensics. One of the concepts that is most essential in Digital Forensicsis the Chain of Custody.

The chain of custody in digital cyber forensics is also known as the paper trail or forensiclink, or chronological documentation of the evidence.

- Chain of custody indicates the collection, sequence of control, transfer and analysis.
- It also documents details of each person who handled the evidence, date and time itwas collected or transferred, and the purpose of the transfer.
- It demonstrates trust to the courts and to the client that the evidence has nottampered.

Digital evidence is acquired from the myriad of devices like a vast number of IoT devices, audio evidence, video recordings, images, and other data stored on hard drives, flash drives,and other physical media.

Importance of maintaining Chain of Custody?

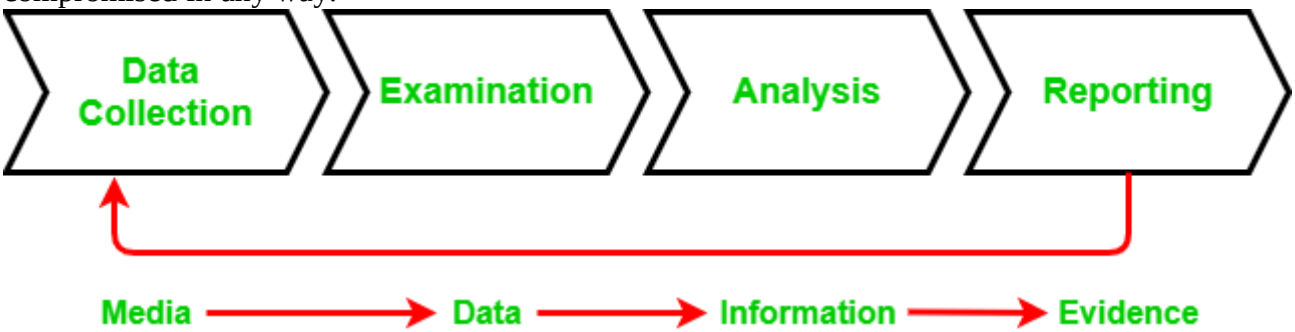
Importance to Examiner:

- To preserve the integrity of the evidence.
- To prevent the evidence from contamination, which can alter the state of theevidence.
- In case you obtained metadata for a piece of evidence but unable to extract any meaningful information from the metadata. In such a case, the chain of custody helpsto show where possible evidence might lie, where it came from, who created it, and the type of equipment used. This will help you to generate an exemplar and compare it to the evidence to confirm the evidence properties.

Importance to the Court: If not preserved, the evidence submitted in the court might be challenged and ruled inadmissible.

Chain of Custody Process

In order to preserve digital evidence, the chain of custody should span from the first step ofdata collection to examination, analysis, reporting, and the time of presentation to the Courts. This is very important to avoid the possibility of any suggestion that the evidence has been compromised in any way.



Let's discuss each stage of the chain of custody in detail:

1. **Data Collection:** This is where chain of custody process is initiated. It involves identification, labeling, recording, and the acquisition of data from all the possiblerelevant sources that preserve the integrity of the data and evidence collected.
2. **Examination:** During this process, the chain of custody information is documentedoutlining the forensic process undertaken. It is important to capture screenshots throughout the process to show the tasks that are completed and the evidence uncovered.
3. **Analysis:** This stage is the result of the examination stage. In the Analysis stage, legally justifiable methods and techniques are used to derive useful information toaddress questions posed in the particular case.
4. **Reporting:** This is the documentation phase of the Examination and Analysis stage.Reporting includes the following:

- Statement regarding Chain of Custody.
- Explanation of the various tools used.
- A description of the analysis of various data sources.
- Issues identified.

- Vulnerabilities identified.
- Recommendation for additional forensics measures that can be taken.

THE CHAIN OF CUSTODY FORM

In order to prove a chain of custody, you'll need a form that lists out the details of how the evidence was handled every step of the way. The form should answer the following questions:

- **What is the evidence?:** For example- digital information includes the filename, md5hash, and Hardware information includes serial number, asset ID, hostname, photos, description.
- **How did you get it?**: For example- Bagged, tagged or pulled from the desktop.
- **When it was collected?:** Date, Time
- **Who has handle it?**
- **Why did that person handled it?**
- **Where was it stored?:** This includes the information about the physical location in which proof is stored or information of the storage used to store the forensic image.
- **How you transported it?:** For example- in a sealed static-free bag, or in a securestorage container.
- **How it was tracked?**
- **How it was stored?:** For example- in a secure storage container.
- **Who has access to the evidence?:** This involves developing a check-in/ check-outprocess. The CoC form must be kept up-to-date. This means every time the best evidence is handledoff, the chain of custody form needs to be updated.

PROCEDURE TO ESTABLISH THE CHAIN OF CUSTODY

In order to assure the authenticity of the chain of custody, a series of steps must be followed. It is important to note that the more information Forensic expert obtains concerning the evidence, the more authentic is the created chain of custody. You should
ensure that the following procedure is followed according to the chain of custody forelectronic devices:

- Save the original material
- Take photos of the physical evidence
- Take screenshots of the digital evidence.
- Document date, time, and any other information on the receipt of the evidence.
- Inject a bit-for-bit clone of digital evidence content into forensic computers.
- Perform a hash test analysis to authenticate the working clone.

How can the Chain of Custody be assured?

A couple of considerations are involved when dealing with digital evidence and Chain of Custody. We shall discuss the most common and globally accepted and practiced best practices.

1. **Never ever work with the Original Evidence:** The biggest consideration that needsto be taken care of while dealing with digital evidence is that the forensic expert has to make a full copy of the evidence for forensic analysis. This cannot be overlooked as when errors are made to working copies or comparisons need to be done, then, in that case, we need an original copy.
2. **Ensuring storage media is sterilized:** It is important to ensure that the examiner's storage device is forensically clean when acquiring the evidence. Suppose if the examiner's storage media is infected with malware, in that case, malware can escapeinto the machine being examined and all

of the evidence will eventually get compromised.

3. **Document any extra scope:** During the process of examination, it is important to document all such information that is beyond the scope of current legal authority andlater brought to the attention of the case agent. A comprehensive report must contain following sections:

- Identity of the reporting agency.
- Case identifier.
- Case investigator.
- Identity of the submitter.
- Date of receipt.
- Date of report.
- Descriptive list of items submitted for examination: This includes the serialnumber, make, and model.
- Identity and signature of the examiner
- Brief description of steps taken during the examination: For example- stringsearches, graphics image searches, and recovering erased files.
- Results.

4. **Consider the safety of the personnel at the scene:** It is very important to ensure that the crime scene is fully secure before and during the search. In some cases, theexaminer may only be able to do the following while onsite:

- Identify the number and type of computers.
- Interview the system administrator and users.
- Identify and document the types and volume of media: This includesremovable media also.
- Determine if a network is present.
- Document the information about the location from which the media wasremoved.
- Identify offsite storage areas and/or remote computing locations.
- Identify proprietary software.
- Determine the operating system in question.

The Digital evidence and Digital Chain of Custody are the backbones of any action taken by digital forensic specialists. In this article, we have examined the seriousness of the digital evidence and what it entails and how slight tampering with the digital evidence can change the course of the forensic expert's investigation.

Cloning

Hard disk forensic cloning, also known as disk imaging, is the process of creating an exact copy,or "image," of a hard disk drive (HDD) or other digital storage media. This process is commonlyused in forensic investigations to preserve the original data on a suspect's hard drive while also allowing for a separate, write-protected copy to be examined and analyzed.

The process of forensic cloning begins with the acquisition of the original hard drive or storage media. This can be done in a number of ways, including physically removing the drive from the computer, connecting the drive to a forensic workstation via a write-blocker, or connecting to the drive over a network.

Once the original drive is connected, a forensic cloning software is used to create a bit-by-bit copy of the entire drive, including all of the data, metadata, and unallocated space. This copy is known as an "image" and it is an exact replica of the original drive. The image is then saved to aseparate storage device, such as an external hard drive or a network-attached storage device.

It is important to note that the process of forensic cloning must be done in a forensically sound manner to maintain the integrity of the evidence. This means that the process must be done in a way that does not alter the original data in any way, and that the process is properly documentedand verified.

Once the forensic cloning process is complete, the image can be used for various analysis and investigation purposes. For example, the image can be examined using forensic software tools to

recover deleted files, recover lost data, or identify patterns of use. Additionally, the image can be used to create virtual machines or emulators, to run the clone and examine the data in a controlled environment.

Overall, hard disk forensic cloning is an essential process in digital forensics, as it allows for the preservation and examination of digital evidence while maintaining the integrity of the original data.

LIVE STREAM VERSUS DEAD SYSTEM

METHODS OF ACQUISITION

In most computer forensic examinations, the next step is to make an exact copy of the data residing on the evidence hard disk (or other electronic digital storage device). The need to createsuch a copy is consistent with the essential concern not to change the evidence. There are two type of methodology can be followed for acquiring the image of digital evidences such as follows [2]:

A. Live Acquisition
B. Dead/Offline Acquisition

II.A Live Acquisition

When the investigator is to confiscate a live system there are some issues to consider before cutting the power. A live system refers to system that are up and running where information maybe altered as data is continuously processed [3].. There is a lot of information of evidentiary value that could be found in a live system. Switching it off may cause loss of volatile data such as running processes, network connections and mounted file systems. In contrast, leaving a computer running may cause evidence to be altered or deleted. The investigator therefore needs to decide what alternative is best in a given situation. Another approach is to use specialized tools to extract volatile data from the computer before shutting it down In Live Acquisition Technique is real world live digital forensic investigation process. for example a common approach to live digital forensic involves an acquisition tool into read only mode in system. thenattaching writable media or disk to system and using the tool to start Live imaging in that tool byusing Graphic User Interface(GUI) if available or use Command Line Interface(CUI) [2].

Myth #1

A Digital Forensics Practitioner conducting live forensics upon a system will inevitably alter that system in some manner, thus live forensics cannot be conducted as a truly forensic process[8].

Reality:

While true that conducting live forensics upon a system will inevitably alter that system in some manner, the flawed statement, here, is that this precludes the process from being a truly forensic process. In fact, there is no such requirement levied by the Court. In almost every other forensic discipline, we destroy or adulterate the evidence during the collection and analysis process

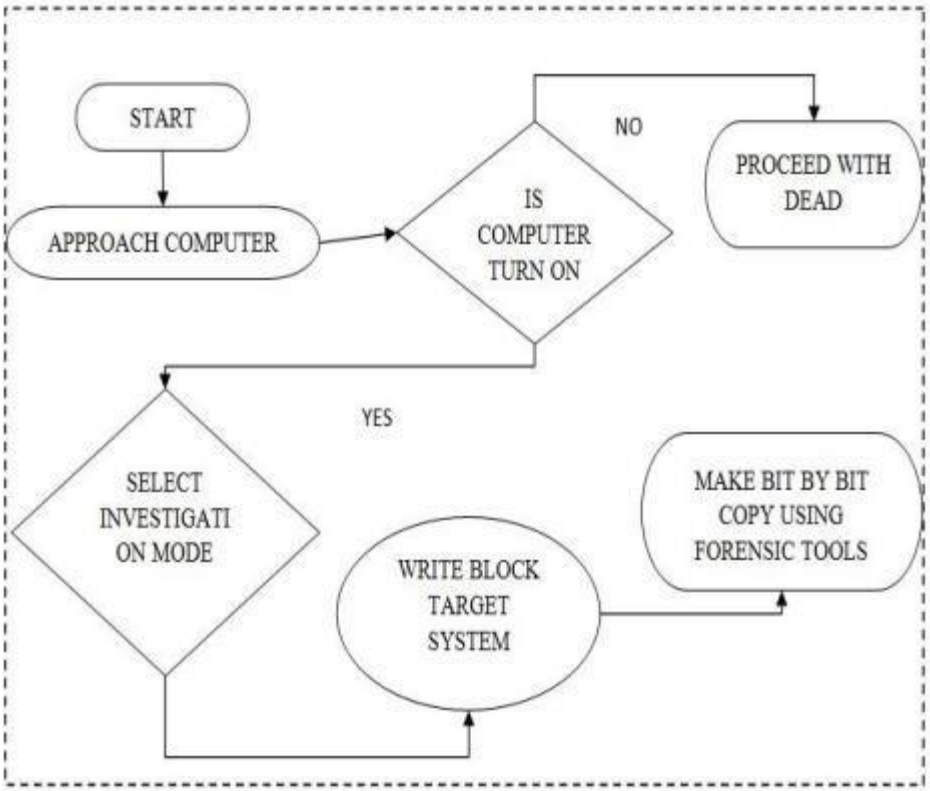
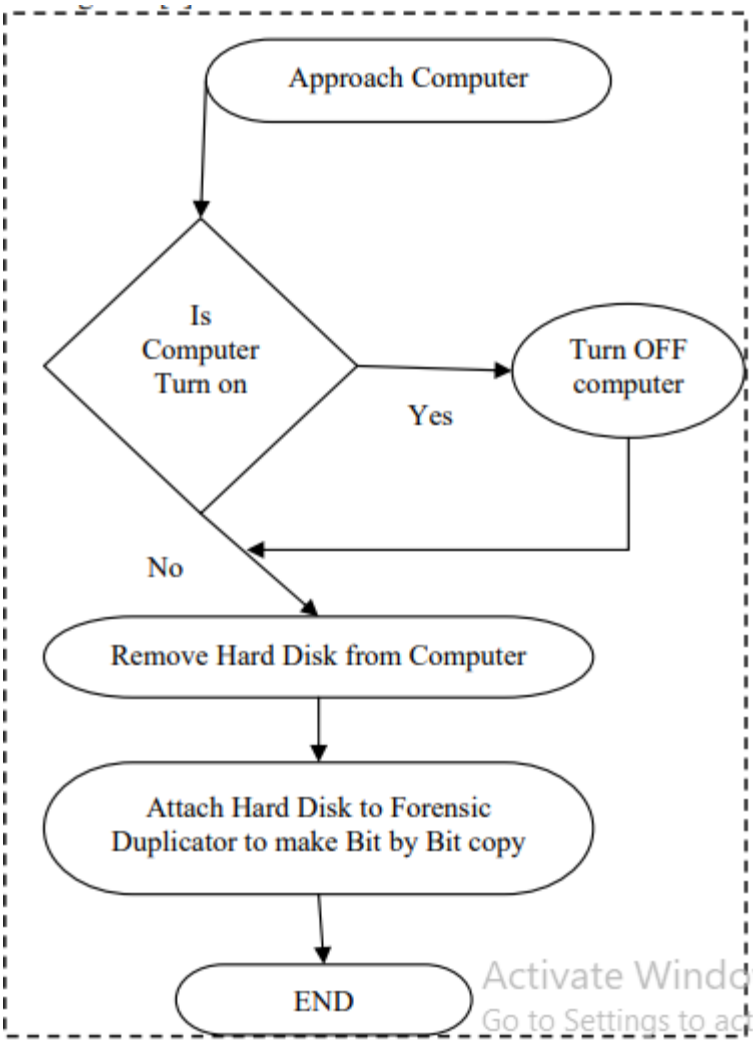


Fig 1. Live Forensic Image Acquisition

Dead/Offline Acquisition

Dead system forensic can produce some information, they can't recover everything. In order to create a forensic image of an entire disk, best practice dictates that the imaging process should not alter any data on the disk and that all data, metadata and unallocated space be included [1].

Traditionally, forensic investigators accomplish this by powering down the system and removingthe disk (or disks) in order to connect it to a forensic workstation or hardware or software write-blocker to create the image [3]. This is referred to as dead imaging. A write-blocker, as its name implies, will prevent any data from being written to the disk, allowing read access only. Removing a disk from a running system prevents any further changes due to normal system operations or process and user interactions. Using a write-blocker during evidence acquisition preserves the integrity of the file metadata, such as timestamps that may be relevant to the investigation



Activate Windov
Go to Settings to acti

Fig.2 Dead Forensic Image Acquisition [1]

Dead systems are systems that are switched off and no data processing is taking place. To retainthe integrity of the data it is often considered appropriate to cut the power supply to the computer, but this will have other implications

HASHING

What is Hashing?

Hashing is a programming technique in which a string of characters (a text message, for instance) is converted into a smaller, fix-sized value, also known as a hash value. This hash valueis always unique and has a fixed length, representing the original string. However, the hash valuecan’t be used to recover the original message. This ensures privacy and security while sharing the message.

Hashing is generally used to index and access items in a database since finding a shorter hash value of the item is faster than finding the original data directly. In digital forensics, however, hash values are calculated with the help of a hashing algorithm to ensure eDiscovery integrity.

What is a Hashing Algorithm?

An algorithm used in hashing is called the **hash function**. The value returned by this function is called a **hash value**. Hash values are a fast, robust, and computationally efficient way to comparethe contents of files under forensic investigation. Each hashing algorithm uses a specific number of digits to store a unique "thumbprint" or a "digital fingerprint" of the file contents. Just as fingerprints are considered a unique biometric modality, the hash value generated by a hash function provides a unique characteristic of contents under forensic investigation. The unique hash value can be extracted for a single file, a group of files, or even entire disk space. This is a crucial process for deduplication and empirical evidence verification in ediscovery and forensic investigation. The following are some characteristics of hash functions:

- Hash functions are complex one-way functions, meaning you cannot reverse a hashing process to extract original data from a hash value. Reverse engineering is not possible,given a hash value.
- The hash value size is permanently fixed, and it's independent of the input data size.
- Two different input files cannot produce the same hash value.

- Hash values don’t depend on the name of the file. Even if the file names are different andtheir contents are identical, it will produce the same hash values corresponding to these files.
- Different hash functions will produce different hash values corresponding to the samecontents in the respective files.
- Some hash functions are more secure than others. For example, the MD5 hashing algorithm can be cracked with a fair amount of computational power. Hence, two different files having different contents can be created to produce the same MD5 hashvalue. This scenario is called a **hash collision**.

Figure 1: Working of a Hashing Algorithm

Mathematically, a hash function **T** also called the transformation function, takes a variable-sized input **x** and returns a fixed-size string, called a hash value **y** . Here, **y=T(x)**

The fundamental features of a hash function are as follows:

- The input string **x** can be of any length.
- Output string **y** has a fixed length.
- For any given **x**, **T(x)** is easy to compute, given the mathematical steps.
- **T(x)** is a one-way function and is collision-free.

Collision-free hash functions can be classified into two categories: strong collision-free hash functions and weak collision-free hash functions.

A strong collision-free hash function **T** is the one, in which, it is computationally infeasible to find two messages **a** and **b**, where **T(a)=T(b)**. Given a weak collision-free hash function, it is computationally difficult to find a message **a** not equal to **b**, such that **T(a)= T(b)**.

MD5 and SHA1 Hashing Algorithms

MD5 and SHA1 are the two most popular hashing algorithms used by digital forensicsprofessionals today.

MD5: MD5 or Message-Digest algorithm 5 is a hashing algorithm that was created by Ron Rivest to replace the previous hashing algorithm MD4. MD5 is the fifth and latest version of theoriginal hashing algorithm MD and it creates hash values of 128 bits.

SHA1: SHA1 or Secure Hash Algorithm 1 is another popular hashing algorithm that is modeled after MD5. It is more powerful than MD5 and produces hash values of 160 bits.

The following are the main differences between MD5 and SHA1 hashing algorithms:

Let us take a sample string which we enter in an MD5 hashing algorithm and obtain its hashvalue:
String Input: Sam is eating apple
Hash Value: 387f51d0ccbab6be677275c9933c250eNow, let's modify the string by just one character:
String Input: Sam is eating apples
Hash Value: c77426fb082c588cfe5583f7eee73309
You can see that appending just one character to the input string changes the entire hash value.This demonstrates the security quotient of hash functions.
The use of MD5 and SHA1 hashing algorithms is a standard practice in digital forensics. These algorithms allow forensic investigators to preserve digital evidence from the moment they acquire it, till the time it's produced in court. There are many email forensics and eDiscovery software available. Stellar Email Forensic is one such software, that allows extensive and hassle-free case management during criminal investigations. One of the advanced features of thissoftware is deleted email recovery.

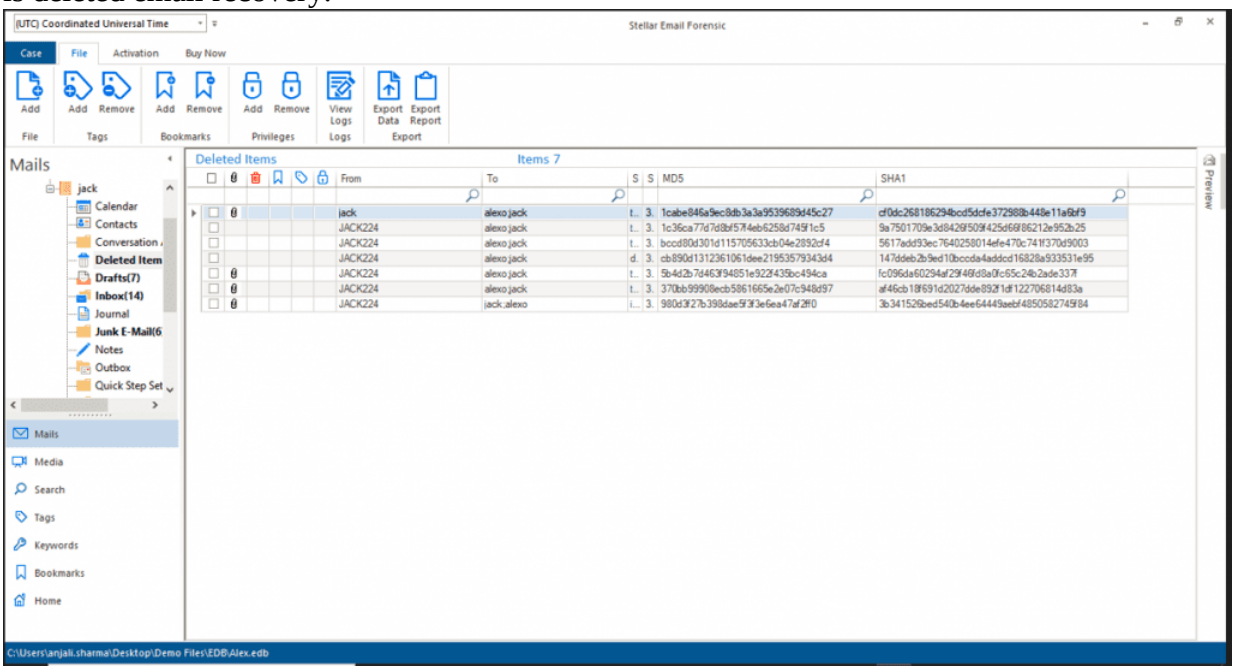
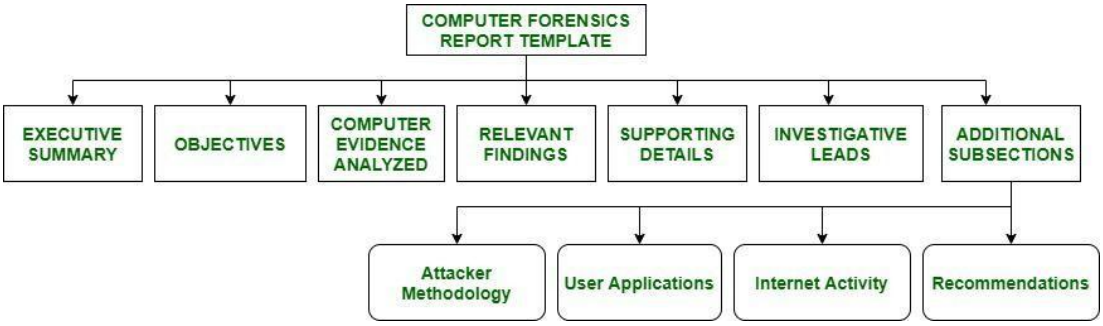


Figure 2: MD5 and SHA1 hash values corresponding to emails.
Stellar Email forensic is state-of-the-art software that allows forensic analysis of emailseffectively and efficiently. Stellar Email forensic automatically calculates hash values corresponding to individual emails in the entire mailbox data under consideration.

COMPUTER FORENSIC REPORT FORMAT

The main goal of Computer forensics is to perform a structured investigation on a computing device to find out what happened or who was responsible for what happened, while maintaining a proper documented chain of evidence in a formal report. Syntax or template ofa Computer Forensic Report is as follows :



1. **Executive Summary :**
   Executive Summary section of computer forensics report template provides background data of conditions that needs a requirement for investigation. Executive Summary or theTranslation Summary is read by Senior Management as they do not read detailed report.This section must contain short description, details and important pointers. This section could be one page long. Executive Summary Section consists of following :

- Taking account of who authorized the forensic examination.
- List of the significant evidences in a short detail.
- Explaining why a forensic examination of computing device was necessary.
- Including a signature block for the examiners who performed the work.
- Full, legitimate and proper name of all people who are related or involved in case, JobTitles, dates of initial contacts or communications.

2. **Objectives :**
   Objectives section is used to outline all tasks that an investigation has planned to complete. In some cases, it might happen that forensics examination may not do a full fledged investigation when reviewing contents of media. The prepared plan list must be discussed and approved by legal council, decision makers and client before any forensic analysis. This list should consist tasks undertaken and method undertaken by an examinerfor each task and status of each task at the end of report.

3. **Computer Evidence Analyzed :**
   The Computer Evidence Analyzed section is where all gathered evidences and its interpretations are introduced. It provides detailed information regarding assignment ofevidence's tag numbers, description of evidence and media serial numbers.

4. **Relevant Findings :**
   This section of Relevant Findings gives summary of evidences found of **probative Value** When a match is found between forensic science material recovered from a crime scene e.g., a fingerprint, a strand of hair, a shoe print, etc. and a reference sample provided by a suspect of case, match is widely considered as strong evidence that suspect

is source of recovered material. However, probative value of evidence can vary widely depending on way in which evidence is characterized and hypothesis of its interest. It answers questions such as “What related objects or items were found during investigationof case ?”.

5. **Supporting Details :**
   Supporting Details is section where in-depth analysis of relevant findings is done. ‘How we found conclusions outlined in Relevant Findings?’, is outlined by this section. It contains table of vital files with a full path name, results of string searches, Emails/URLs reviewed, number of files reviewed and any other relevant data. All tasks undertaken to meet objectives is outlined by this section. In Supporting Details we focus more on technical depth. It includes charts, tables and illustrations as it conveys much more than written texts. To meet outlined objectives, many subsections are also included. This section is longest section. It starts with giving background details of media analyzed. It is not easy to report number of files reviewed and size of hard drive in a human understandable language. Therefore, your client must know how much data you wanted toreview to arrive at a conclusion.

6. **Investigative Leads :**
   Investigative Leads performs action items that could help to discover additional information related to the investigation of case. The investigators perform all outstandingtasks to find extra information if more time is left. Investigative Lead section is very critical to law enforcement. This section suggests extra tasks that discovers information needed to move on case. e.g. finding out if there are any firewall logs that date any far enough into past to give a correct picture of any attacks that might have taken place. Thissection is important for a hired forensic consultant.

7. **Additional Subsections :**
   Various additional subsections are included in a forensic report. These subsections are dependent on clients want and their need. The following subsections are useful in specificcases :

- **Attacker Methodology –**
  Additional briefing to help reader understand general or exact attacks performed is given in this section of attacker methodology. This section is useful in computer intrusion cases. Inspection of how attacks are done and what bits and pieces of attackslook like in standard logs is done here.
- **User Applications –**
  In this section we discuss relevant applications that are installed on media analyzed because it is observed that in many cases applications present on system are very relevant. Give a title to this section, if you are investigating any system that is used byan attacker .e.g Cyber Attack Tools.
- **Internet Activity –**
  Internet Activity or Web Browsing History section gives web surfing history of user of media analyzed. The browsing history is also useful to suggest intent, downloadingof malicious tools, unallocated space, online researches, downloading of secure deleted programs or evidence removal type programs that wipe files slack and temporary files that often harbor evidence very important to an investigation.
- **Recommendations –**
  This section gives recommendation to posture client to be more prepared and trainedfor next computer security incident. We investigate some host-based, network-basedand procedural countermeasures are given to clients to reduce or eliminate risk of incident security

MOBILE DEVICE FORENSICS

Mobile forensics, a subtype of digital forensics, is concerned with retrieving data from an electronic

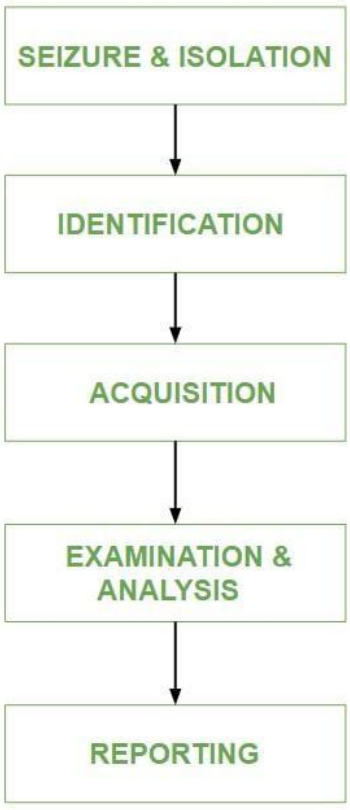
source. The recovery of evidence from mobile devices such as smartphones and tablets is the focus of mobile forensics. Because individuals rely on mobile devices for so much of their data sending, receiving, and searching, it is reasonable to assume that these devices hold a significant quantity of evidence that investigators may utilize.
Mobile devices may store a wide range of information, including phone records and text messages, as well as online search history and location data. We frequently associate mobile

forensics with law enforcement, but they are not the only ones who may depend on evidence obtained from a mobile device.

Uses of Mobile Forensics:

The military uses mobile devices to gather intelligence when planning military operations or terrorist attacks. A corporation may use mobile evidence if it fears its intellectual property is being stolen or an employee is committing fraud. Businesses have been known to track employees' personal usage of business devices in order to uncover evidence of illegal activity. Law enforcement, on the other hand, may be able to take advantage of mobile forensics by using electronic discovery to gather evidence in cases ranging from identity theft to homicide.

PROCESS OF MOBILE DEVICE FORENSICS:



- **Seizure and Isolation:** According to digital forensics, evidence should always be adequately kept, analyzed, and accepted in a court of law. Mobile device seizures are followed by a slew of legal difficulties. The two main risks linked with this step of the mobile forensic method are lock activation and network / cellular connectivity.
- **Identification:** The identification purpose is to retrieve information from the mobile device. With

the appropriate PIN, password, pattern, or biometrics, a locked screen may be opened. Passcodes are protected, but fingerprints are not. Apps, photos, SMSs, and messengers may all have comparable lock features. Encryption, on the other hand, provides security that is difficult to defeat on software and/or hardware level.

- **Acquisition:** Controlling data on mobile devices is difficult since the data itself is movable. Once messages or data are transmitted from a smartphone, control is gone. Despite the fact that various devices are capable of storing vast amounts of data, the data itself may be stored elsewhere. For example, data synchronization across devices and apps may be done either directly or via the cloud. Users of mobile devices commonly utilize services such as Apple's iCloud and Microsoft's One Drive, which exposes the possibility of data harvesting. As a result, investigators should be on the lookout for any signs that data may be able to transcend the mobile device from a physical object, as this might have an impact on the data collecting and even preservation process.
- **Examination and analysis:** Because data on mobile devices is transportable, it's tough to keep track of it. When messages or data from a smartphone are moved, control is lost. Despite the fact that numerous devices can hold vast amounts of data, the data itself may be stored elsewhere.
- **Reporting:** The document or paper trail that shows the seizure, custody, control, transfer, analysis, and disposition of physical and electronic evidence is referred to as forensic reporting. It is the process of verifying how any type of evidence was collected, tracked,and safeguarded.

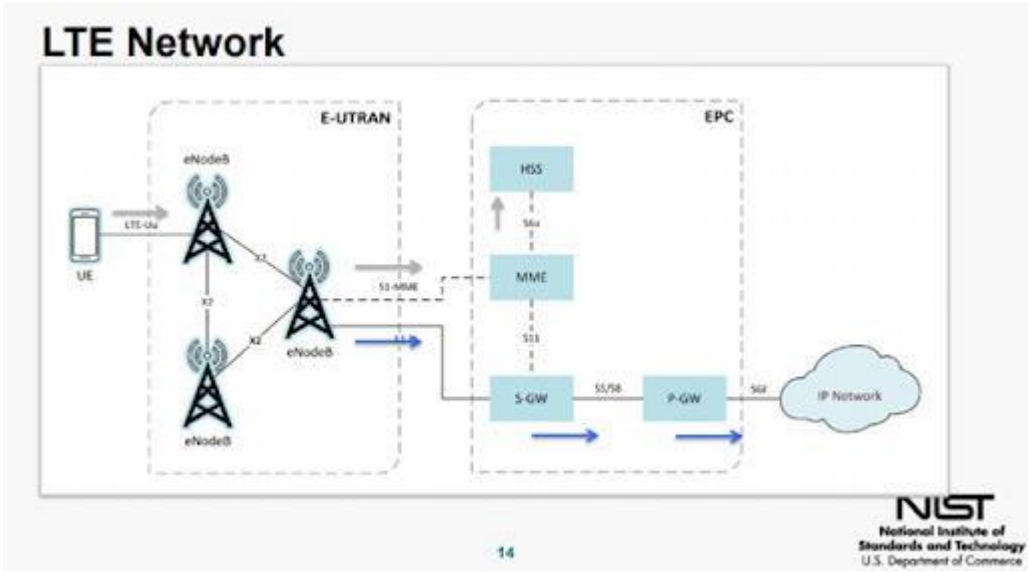
Principles of Mobile Forensics:

The purpose of mobile forensics is to extract digital evidence or relevant data from a mobile device while maintaining forensic integrity. To accomplish so, the mobile forensic technique must develop precise standards for securely seizing, isolating, transferring, preserving for investigation, and certifying digital evidence originating from mobile devices.
The process of mobile forensics is usually comparable to that of other fields of digital forensics. However, it is important to note that the mobile forensics process has its own unique characteristics that must be taken into account. The use of proper methods and guidelines is a must if the investigation of mobile devices is to give positive findings.

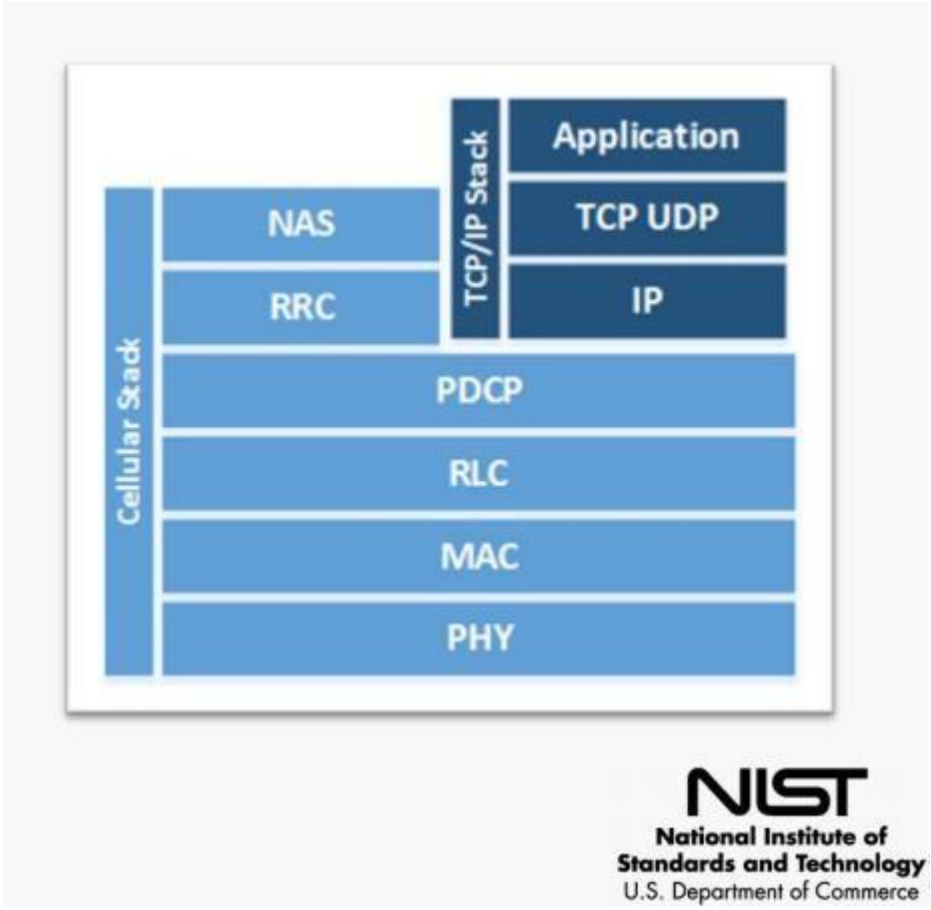
CELLULAR NETWORKS

Cellular networks

There are a number of different communication technologies that most users are at least somewhat familiar with but are tied to particular 'Generations' of devices and their associated networks- GSM (Global System for Mobiles) and CDMA (Code Division Multiple Access) werecommonplace during the 2G and 3G era, LTE (Long Term Evolution) for 4G, and 5G-NR for 5Gnetworks that are still being rolled out. Starting with 4G, most major vendors globally converted over to the LTE standard, allowing for far less fragmentation of device compatibility. We're going to be referring to a presentation from the National Institute for Standards and Technology on "LTE Security- How Good Is It?" for a considerable amount of the breakdown of functionality.
Access to LTE Networks as a rule is provided through a series of mesh-style base stations which send and receive signals from user devices which then forward requests onto a backend core network. The core network itself processes authentication and subscriber services along with connecting users to the rest of the Internet.



Much like the OSI model, the cellular stack provides connectivity from the physical layer all theway up through application, with TCP/IP doing its own thing and not really lining up properly with the standards. TCP/IP however does sit on top of the packet data convergence protocol (PDCP), which provides header compression and radio encryption.



The IMSI (International Mobile Subscriber Identity) is a unique id for every subscriber. Whileyou might think at first glance that it would just be the user's phone number, it actually has nothing to do with it. This is usually a 15 digit numeric value stored on the UICC (Universal Integrated Circuit Card), which can be considered a next-gen SIM (Subscriber Identification Module) card. The IMSI contains three separate values- 3 digits comprising the MCC (Mobile Country Code), 2 to 3 digits for the MNC (Mobile Network Code), and then the MSIN (MobileSubscription Identification

Number) from the provider itself.
The UICC operates the same conceptually as a smart card- providing a basis for encrypting communications and authentication. This is far from the only encryption method used for protecting data transfers and calls, as the Authentication and Key Agreement (AKA) protocol isfirst used to authenticate devices to the network, and only after this has been completed are the crypto keys for encrypting calls generated. As we go up the Cellular Stack, multiple 128-bit and256-bit keys are used to help protect both internal communications and user traffic.

Once traffic has been received by the base stations from the user, IPsec protects communicationson the backend from the base stations to the core network, both of which use PKI certificates to authenticate to each other. Problems come into play however when data has to abide by legacy rules such as the GSM downgrading noted above. This also means that services that exploit elements that cannot be updated or the human factor could still gain access to user data despite strong protections. Let's quickly go over a few of these Potential Security Issues.

2FA via SMS

Multiple methods have been revealed over the years that allow unauthorized users to gain accessto text messages. Sometimes this has been by obtaining access via employees at the cellular provider, 3rd party services that can operate without verification, or malicious apps with elevatedpermissions. Because of this, 2FA (2 Factor Authentication) via SMS is considered potentially insecure and exploitable to the point where it is recommended to use any alternative to this system.

Compromised Wi-Fi networks

If a user connects to a compromised Wi-Fi network, most of the protections on the Cellular Network will not apply because it's not being used. Making sure that Wi-Fi is turned off whenever leaving a safe area is critical for users to avoid accidentally connecting to a networkthat they don't want to.

Out of support devices

The supported lifetime for most mobile devices is significantly less than that of their desktop or laptop counterparts. This means that security updates may possibly stop being received by user devices just a few years after the initial release of the device. If users continue to use these devices long after this date, they run the risk of having their devices exploited through any number of means.
While purchasing new devices and moving over to them can be difficult, the benefits outweighthe potential costs.

App leaks

App developers do not have unlimited resources. They put together a product, ship it out and tryto get it approved and on their respective stores as quickly as possible. This means that some legitimate apps may have higher than intended permissions, which would give them access to a significant amount of non-essential data, but without adequate protections for that data because they didn't need it in the first place. Because of this, other apps that have been installed may beable to sniff around for this information and send it off to third parties.
Being careful about what apps we permit on our devices and regularly updating the ones we do have are both excellent ideas. What we can also do though is audit App Permissions on a regular basis and see what apps have been granted which permissions. Removing permissions from apps may cause unexpected errors, but least privilege is worth investigating when it comes to sensitive information.

Social engineering

Social Engineering in the modern age can involve sending SMS messages, emails, phone calls, browser popups, full screen ads and more to users with prompts ranging to polite requests to threatening legal action if they don't do some specific action. This could potentially convince users to give whatever information they are being asked for to a 3rd party that definitely shouldnot have access to it, and cost them dearly as a result.

Some protections have been built into Mobile OS's already, along with spam protection andcaller id's flagging potentially suspicious numbers. These bad callers can then be sent to voicemail directly without the user having to deal with it

OPERATING SYSTEMS

What are the types of Operating systems?

The most popular types of Operating Systems are Windows, Linux, Mac, iOS, and Android.

Windows

Windows is a widely used OS designed by Microsoft. The file systems used by Windows include FAT, exFAT, NTFS, and ReFS. Investigators can search out evidence by analyzing the following important locations of the Windows:

- **Recycle Bin:** This holds files that have been discarded by the user. When a user deletes files, acopy of them is stored in recycle bin. This process is called "Soft Deletion." Recovering files from recycle bin can be a good source of evidence.
- **Registry:** Windows Registry holds a database of values and keys that give useful pieces of information to forensic analysts. For example, see the table below that provides registry keys and associated files that encompasses user activities on the system.

Registry Key	Abbr.	Associated files	Incorporates
HKEY_LOCAL_MACHINE	HKLM		System settings
HKEY_USERs	HKU	NTUSER.DAT	Settings related to all currently logged-in users
HKEY-CURRENT_USER	HKCU		Both system and application Settings with regard to all currently logged-in users
HKEY_CURRENT_CONFIG	HKCC		Registry will be created at runtime and contains hardware settings and performance details
HKLM\SYSTEM		System	File involves system settings about services and hardware
HKLM\SOFTWARE		Software	File incorporates configuration settings for all installed applications including windows
HKLM\SAM		Sam	Includes security info and user password hashes for all users on the system

Cell phone evidence

Students should understand data types before the collection of data from a mobile device. The common data types include contacts list, call log, SMS, images, audio, video, GPS data, and apps data. Also, both current and deleted data types can be extracted from a mobile device.

Call Detail Records (CDRs): Service providers frequently use CDRs to improve network performance. However, they can provide useful information to investigators, as well. CDRs can show:

- Call started and ended date/time
- The terminating and originating towers
- Whether the call was outgoing or incoming
- Call time duration
- Who was called and who made the call

Almost all service providers retain these important records for a certain time. The forensic specialist can collect these records if he requires. However, the collection of this information depends on the policies of the concerned state. Every state has different laws in this regard. **Global Positioning System (GPS):** GPS data is an excellent source of empirical evidence. If thesuspect has an active mobile device at the crime scene, GPS can pinpoint his location as well as his criminal acts. GPS also locates the movements of the suspect from a crime scene to the hideout. Furthermore, it helps in finding phone call logs, images, and SMS messages. Presently, a GPS system includes 27 satellites in operation.

App Data: Many apps store and access data the user is not aware of. In fact, many apps seek permission during the installation process to access these data. For example, photo or video editing apps request permission to access media files, camera, and GPS for navigation. This datacan be a primary source of evidence to the court.

SMS: Text messaging is a widely used way of communication. Text messages leave electronic records of dialogue that can be presented in the court as evidence. They include the relevant information such as:

- Date/time of each message
- Phone number of sender and receiver

Photos and Videos as Evidence: They can be a tremendous source of evidence, but theirrelevance to crime and authentication is crucial.

CELL PHONE FORENSIC TOOLS.

Data acquisition is that the method of gathering information from mobile devices and their associated media. This method reduces the possibilities of information loss thanks to injury or battery depletion throughout storage and transportation. Mobile device identification is necessary at the start of the forensic examination. The identification method includes understanding of the type of mobile phone, its operating system, and alternative essential characteristics to create a legal copy of the mobile device's content.

There are several tools and techniques available in mobile forensics. However, the selection of tools and techniques throughout an investigation depends on the type of mobile device and its associated media.

How do you gather data from mobile devices?

The data can be gathered from mobile devices in two ways that, namely, physical acquisition and logical acquisition.

Physical Acquisition, also called aa a physical memory dump, it is a technique for capturing all the information from the memory chips on the mobile device. It permits the forensic tool to gather remnants of deleted data. Initially, the received information is in raw format and can't be read. Later on, some strategies are applied to convert that information into a human readable form.

Logical Acquisition, or logical extraction, could be a technique for extracting the files and folders without any of the deleted data from a mobile device. However, some vendors describe logical extraction narrowly because the ability to assemble a specific data type, like picture, call history,

text messages, calendar, videos, and ringtones. A software application is used to create a copy of the files. For instance, iTunes backup is used to make a logical image of AN iPhone or iPad.

What data types are you able to collect from a mobile device?

Students should understand data types before the collection of information from a mobile device. The common data types include contacts list, call log, SMS, images, audio, video, GPS data, and apps data. Also, both current and deleted data types can be extracted from a mobile device.

Call Detail Records (CDRs): Service providers oft use CDRs to boost network performance. However, they can provide useful information to investigators, as well. CDRs can show:

- Call started and all ended date/time
- The terminating and originating towers
- Whether the call was outgoing or incoming
- Call time period
- Who was called and who made the call?

Almost all service providers retain these important records for an exact time. The forensic professionals will collect these records if he needs. However, the gathering of this information depends on the policies of the concerned state. Each state has totally different laws during this regard.

Global Positioning System (GPS): GPS data is an excellent source of empirical proof. If the suspect has an active mobile device at the crime scene, GPS will pinpoint his location as well as his criminal acts. GPS additionally locates the movements of the suspect from crime scene to the hiding place. Furthermore, it helps in finding call logs, images, and SMS. Presently, a GPS system includes approx. 27 satellites operative.

App Data: Several apps store and access data the user isn't aware of it. In fact, several apps seek permission throughout the installation method to access these data. For instance, photo or video editing apps request permission to access media files, camera, and GPS for navigation. This data can be a primary source of evidence to the court.

SMS: Text messaging is a widely used way of communication. Text messages leave electronic records of dialogue that can be presented within the court as proof. They include the relevant information such as:

- Date/time of every message
- Phone number of sender and receiver

Photos and Videos as Evidence: They can be a tremendous source of proof, however their relevance to crime and authentication is crucial.

What tools & techniques are commonly used in mobile forensics?

Forensic software application is regularly developing new techniques for the extraction of information from several cellular devices. The two most common techniques are physical and logical extraction. Physical extraction is completed through JTAG or cable connection, whereas logical extraction happens via Bluetooth, infrared, or cable connection.

There are various types of tools available for mobile forensic purposes. They can be categorized as open source, commercial, and non-forensic tools. Each non-forensic and forensic tools frequently use the equivalent techniques and protocols to interact with a mobile device.

Tools Classification System: Forensic analysts must understand the many types of forensic tools. The tools classification offers a framework for forensic analysts to check the acquisition techniques used by totally different forensic tools to capture data.

Manual Extraction

The manual extraction technique permits investigators to extract and view data through the device's touchscreen or input device. At a later stage, this data is documented photographically. Furthermore, manual extraction is long and involves an excellent chance of human error. For instance, the data may be accidentally deleted or modified throughout the examination. Popular tools for manual extractions include:

- Project-A-Phone
- Fernico ZRT
- EDEC Eclipse

Logical Extraction

In this technique, the investigators connect the cellular device to a digital forensic workstation or hardware via Bluetooth, Infrared, RJ-45 cable, or USB cable. The computer—using a logical extraction tool—sends a series of commands to the mobile device. As a result, the specified knowledge is collected from the phone's memory and sent back to the digital forensic workstation for analysis purposes. The tools used for logical extraction include:

- XRY Logical
- Oxygen rhetorical Suite
- Lantern

Hex Dump

A hex dump, also known as physical extraction, extracts the raw image in binary format from the mobile device. The forensic professionals connect the device to a digital forensic workstation and pushes the boot-loader into the device, that instructs the device to dump its memory to the computer. This method is cost-efficient and provides more information to the investigators, including the recovery of phone's deleted files and unallocated space. The common tools used for hex dump include:

- XACT
- Cellebrite UFED Physical analyser
- Pandora's Box

Chip-Off

The chip-off technique permits the examiners to extract information directly from the memory of the cellular device. They remove the phone's memory chip and create its binary image. This method is costly and needs an ample data of hardware. Improper handling may cause physical damage to the chip and renders the data impossible to retrieve. The popular tools and equipment's used for chip-off include:

- iSeasamo Phone Opening Tool
- Xytronic 988D Solder Rework Station
- FEITA Digital inspection station
- Chip Epoxy Glue Remover
- Circuit Board Holder