UNIT -6

DIGITAL FORENSIC

FORENSIC SCIENCE :

Definition

Forensic science involves the application of the natural, physical, and social sciences to matters of law.

Forensic science refers to the application of natural, physical, and social sciences to matters of the law. Most forensic scientists hold that investigation begins at the scene, regardless of their associated field. The proper investigation, collection, and preservation of evidence are essential for fact-finding and for ensuring proper evaluation and interpretation of the evidence, whether the evidence is bloodstains, human remains, hard drives, ledgers, and files or medical records. Scene investigations are concerned with the documentation, preservation, and evaluation of a location in which a criminal act may have occurred and any associated evidence within the location for the purpose of reconstructing events using the scientific method. The proper documentation of a scene and the subsequent collection, packaging, and storage of evidence are paramount. Evidence must be collected in such a manner to maintain its integrity and prevent loss, contamination, or deleterious change. Maintenance of the chain of custody of the evidence from the scene to the laboratory or a storage facility is critical. A chain of custody refers to the process whereby investigators preserve evidence throughout the life of a case. It includes information about: who collected the evidence, the manner in which the evidence was collected, and all individuals who took possession of the evidence after its collection and the date and time which such possession took place.

Significant attention has been brought to the joint scientific and investigative nature of scene investigations. Proper crime scene investigation requires more than experience; it mandates analytical and creative thinking as well as the correct application of science and the scientific method. There is a growing movement toward a shift from solely experiential-based investigations to investigations that include scientific methodology and thinking. One critic of the experience based approach lists the following pitfalls of limiting scene investigations to lay individuals and law enforcement personnel: lack of scientific supervision and oversight, lack of understanding of the scientific tools employed and technologies being used at the scene, and an overall lack of understanding of the application of the scientific method to develop hypotheses supported by the evidence (Schaler 2012). Another criticism is that some investigators (as well as attorneys) will draw conclusions and then obtain (or present) evidence to support their version of events while ignoring other types of evidence that do not support their version or seem to contradict their version (i.e., confirmation bias). Many advocates of the scientific-based approach believe that having scientists at the scene will minimize bias and allow for more objective interpretations and reconstructions of the events under investigation.

COMPUTER FORENSIC

WHAT IS COMPUTER FORENSICS?

Computer forensics is the process of methodically examining computer media (hard¬ disks, diskettes, tapes, etc.) for evidence. In other words, computer forensics is the collection, preservation, analysis, and presentation of computer-related evidence. Computer forensics also referred to as computer forensic analysis, electronic discovery,¬ electronic evidence discovery, digital discovery, data recovery, data discovery, computer analysis, and computer examination. Computer evidence can be useful in criminal cases, civil disputes, and human resources/¬ employment proceedings.

1.2 USE OF COMPUTER FORENSICS IN LAW ENFORCEMENT

Computer forensics assists in Law Enforcement. This can include:

Recovering deleted files such as documents, graphics, and photos.¬

Searching unallocated space on the hard drive, places where an abundance of data often¬ resides.

Tracing artifacts, those tidbits of data left behind by the operating system. Our expert know how to find these artifacts and, more importantly, they know how to evaluate the value of the information they find.

Processing hidden files — files that are not visible or accessible to the user that contain past usage information. Often, this process requires reconstructing and analyzing the date codes for each file and determining when each file was created, last modified, last accessed and when deleted.

Running a string-search for e-mail, when no e-mail client is obvious.

COMPUTER FORENSICS SERVICES

Computer forensics professionals should be able to successfully perform complex evidence recovery procedures with the skill and expertise that lends credibility to your case. For example, they should be able to perform the following services:

1. DATA SEIZURE

Following federal guidelines, computer forensics experts should act as the⎞ representative, using their knowledge of data storage technologies to track down evidence.

The experts should also be able to assist officials during the equipment seizure process.

2. DATA DUPLICATION/PRESERVATION

When one party must seize data from another, two concerns must be addressed; the data must not be altered in any way the seizure must not put an undue burden on the responding party

The computer forensics experts should acknowledge both of these concerns by making an exact duplicate of the needed data. ‘

When experts works on the duplicate data, the integrity of the original is maintained.

3. RECOVERY

Using proprietary tools, your computer forensics experts should be able to safely recover
and analyze otherwise inaccessible evidence.

The ability to recover lost evidence is made possible by the expert’s advanced⎞ understanding of storage technologies

4. DOCUMENT SEARCHES

Computer forensics experts should also be able to search over 200,000 electronic documents in seconds rather than hours.

The speed and efficiency of these searches make the discovery process less complicated and less intrusive to all parties involved.

5. MEDIA CONVERSION

Computer forensics experts should extract the relevant data from old and un-readable devices, convert it into readable formats, and place it onto new storage media for analysis.

6. EXPERT WITNESS SERVICES

Computer forensics experts should be able to explain complex technical processes in an easy-to-understand fashion. This should help judges and juries comprehend how computer evidence is found, what it consists of, and how it is relevant to a specific situation.

7. COMPUTER EVIDENCE SERVICE OPTIONS

Computer forensics experts should offer various levels of service, each designed to suit your individual investigative needs. For example, they should be able to offer the following services:

Standard service: Computer forensics experts should be able to work on your case during nor-mal business hours until your critical electronic evidence is found.

On-site service: Computer forensics experts should be able to travel to your location to
per-form complete computer evidence services. While on-site, the experts should quickly be able to produce exact duplicates of the data storage media in question.

Emergency service: Your computer forensics experts should be able to give your case the highest priority in their laboratories. They should be able to work on it without interruption until your evidence objectives are met.

Priority service: Dedicated computer forensics experts should be able to work on your case during normal business hours (8:00 A.M. to 5:00 P.M., Monday through Friday) until the evidence is found. Priority service typically cuts your turnaround time in half.

Weekend service: Computer forensics experts should be able to work from 8:00 A.M. to 5:00 P.M., Saturday and Sunday, to locate the needed electronic evidence and will continue 14 Computer Forensics, Second Edition working on your case until your evidence objectives are met.

8. OTHER MISCELLANEOUS SERVICES

Computer forensics experts should also be able to provide extended services. These services include:

Analysis of computers and data in criminal investigations On-site seizure of computer data in criminal investigations Analysis of computers and data in civil litigation.On-site seizure of computer data in civil litigation Analysis of company computers to determine employee activity Assistance in preparing electronic discovery requests Reporting in a comprehensive and readily understandable manner Court-recognized computer expert witness testimony Computer forensics on both PC and Mac platforms Fast turnaround time.

BENEFITS OF PROFESSIONAL FORENSIC METHODOLOGY

A knowledgeable computer forensics professional should ensure that a subject computer system is carefully handled to ensure that:

1. No possible evidence is damaged, destroyed, or otherwise compromised by the procedures used to investigate the computer.
2. No possible computer virus is introduced to a subject computer during the analysis process.
3. Extracted and possibly relevant evidence is properly handled and protected from later mechanical or electromagnetic damage.
4. A continuing chain of custody is established and maintained.
5. Business operations are affected for a limited amount of time, if at all.
6. Any client-attorney information that is inadvertently acquired during a forensic exploration is ethically and legally respected and not divulged.

DIGITAL FORENSIC

Digital forensics or digital forensic science is a branch of cybersecurity focused on the recovery and investigation of material found in digital devices and cybercrimes. Digital forensics was originally used as a synonym for computer forensics but has expanded to cover the investigation of all devices that store digital data.

As society increases reliance on computer systems and cloud computing, digital forensics becomes a crucial aspect of law enforcement agencies and businesses.

Digital forensics is concerned with the identification, preservation, examination and analysis of digital evidence, using scientifically accepted and validated processes, to be used in and outside of a court of law.

While its root stretch back to the personal computing revolution in the late 1970s, digital forensics begun to take shape in the 1990s and it wasn't until the early 21st century that countries like the United States begun rolling out nation-wide policies.

Today, the technical aspect of an investigation is divided into five branches that encompass the seizure, forensic imaging and analysis of digital media.

What is the Purpose of Digital Forensics?

The most common use of digital forensics is to support or refute a hypothesis in a criminal or civil court:

- **Criminal cases:** Involve the alleged breaking of laws and law enforcement agencies and their digital forensic examiners.
- **Civil cases:** Involve the protection of rights and property of individuals or contractual disputes between commercial entities where a form of digital forensics called electronic discovery (eDiscovery) may be involved.

Digital forensics experts are also hired by the private sector as part of cybersecurity and information security teams to identify the cause of data breaches, data leaks, cyber attacks and other cyber threats. Digital forensic analysis may also be part of incident response to help recover or identify any sensitive data or personally identifiable information (PII) that was lost or stolen in a cybercrime.

What is Digital Forensics Used For?

Digital forensics is used in both criminal and private investigations.

Traditionally, it is associated with criminal law where evidence is collected to support or negate a hypothesis before the court. Collected evidence may be used as part of intelligence gathering or to locate, identify or halt other crimes. As a result, data gathered may be held to a less strict standard than traditional forensics.

In civil cases, digital forensics may help with electronic discovery (eDiscovery). A common example is following unauthorized network intrusion. A forensics examiner will attempt to understand the nature and extent of the attack, as well as try to identify the attacker.

As encryption becomes more widespread, forensic investigation becomes harder, due to the limited laws compelling individuals to disclose encryption keys.

What is the Digital Forensics Investigation Process?

There are a number of process models for digital forensics, which define how forensic examiners should gather, process and analyze data. That said, digital forensics investigations commonly consist of four stages:

1. **Seizure:** Prior to actual examination digital media is seized. In criminal cases, this will be performed by law enforcement personnel to preserve the chain of custody.
2. **Acquisition:** Once exhibits are seized, a forensic duplicate of the data is created. Once created using a hard drive duplicator or software imaging tool then the original drive is returned to a secure storage to prevent tampering. The acquired image is verified with SHA-1 or MD5 hash functions and will be verified again throughout analysis to verify the evidence is still in its original state.
3. **Analysis:** After acquisition, files are analyzed to identify evidence to support or contradict a hypothesis. The forensic analyst usually recovers evidence material using a number of methods (and tools), often beginning with the recovery of deleted information. The type of data analyzed varies but will generally include email, chat logs, images, internet history and documents. The data can be recovered from accessible disk space, deleted space or from the operating system cache.

4. **Reporting:** Once the investigation is complete, the information is collated into a report that is accessible to non-technical individuals. It may include audit information or other meta-documentation.

What is the History of Digital Forensics?

Before the 1970s, cybercrimes were dealt with existing laws.

The first cyber crimes were recognized in the 1978 Florida Computer Crimes Act. The 1978 Florida Computer Crimes Act included legislation against the unauthorized modification or deletion of data.

As the range of computer crimes increased, state laws were passed to deal with copyright, privacy, harassment and child pornography.

In the 1980s, federal laws began to incorporate computer offences. Canada was the first country to pass legislation in 1983, with the United States following in 1986, Australia in 1989 and Britain's Computer Misuse Act in 1990.

1980s-1990s

The growth in cyber crime in the 1980s and 1990s force law enforcement agencies to establish specialized groups at a national level to handle technical investigations.

In 1984, the FBI launched a *Computer Analysis and Response Team* and in 1985, the British Metropolitan Police fraud squat launched a computer crime department.

One of the first practical examples of digital forensics was Cliff Stoll's pursuit of Markus Hess in 1986. Hess is best known for hacking networks of military and industrial computers based in the United States, Europe and East Asia. He then sold the information to the Soviet KGB for $54,000. Stoll was not a digital forensic expert but used computer and network forensic techniques to identify Hess.

In the 1990s there was a high demand for digital forensic resources and the strain on the central units led to regional or even local groups to handle the load. This led to the science of digital forensic maturing from an ad-hoc set of tools and techniques to a more developed discipline.

By 1992, "computer forensics" was used in academic literature in a paper by Collier and Spaul that attempted to justify digital forensics as a new discipline. That said, digital forensic remained a haphazard discipline due to a lack of standardization and training.

By the late 1990s, mobile phones were more widely available and advancing beyond simple communication devices. Despite this, digital analysis of cell phones has lagged behind traditional computer media due to the proprietary nature of devices.

2000s

Since 2000, various bodies and agencies have published guidelines for digital forensics in response to the need for standardization. Standardization became more important as law enforcement agencies moved away from central units to regional or even local units to try keep up with demand.

For example, the British National Hi-Tech Crime Unit was set up in 2001 to provide national infrastructure for computer crime, with personnel located centrally in London and with the various regional police forces.

In 2002, the Scientific Working Group on Digital Evidence (SWGDE) produced *Best practices for Computer Forensics.*

A European lead international treaty, the Convention of Cybercrime came into force in 2004 with the aim of reconciling national computer crime laws, investigation techniques and international cooperation. The treaty has been signed by 43 nations (including the United States, Canada, Japan, South Africa, United Kingdom and other European nations) and ratified by 16.

In 2005, an ISO standard for digital forensics was released in ISO 17025, *General requirements for the competence of testing and calibration laboratories.*

This was when digital forensics training began to receive more attention with commercial companies beginning to offer certified forensic training programs.

The field of digital forensics still faces issues. A 2009 paper, *Digital Forensic Research: The Good, the Bad and the Unaddressed* identified a bias towards Windows operating systems in digital forensics research despite widespread use of smartphones, unix and linux based operating systems.

In 2010, Simson Garfinkel pointed out the increasing size of digital media, widespread encryption, growing variety of operating systems and file formats, more individuals owning multiple devices and legal limitations as key risks to digital forensics investigations. The paper also identified training issues and the high cost of entering the field as key issues. Other key issues include the shift toward Internet crime, cyber warfare and cyber terrorism.

What Tools Do Digital Forensic Examiners Use?

In the 1980s, very few digital forensic tools existed forcing forensic investigators to perform live analysis, using existing sysadmin tools to extract evidence. This carried the risk of modifying data on the disk which led to claims of evidence tampering.

The need for software to address this problem was first recognized in 1989 at the Federal Law Enforcement Training Center and resulted in the creation of IMDUMP and SafeBack. DIBS, a hardware and software solution, was released commercially in 1991.

These tools create an exact copy of a piece of digital media to work on while leaving the original disk intact for verification.

By the end of the 1990s, the demand for digital evidence meant more advanced tools such as EnCase and FTK were developed, allowing analysts to examine copies of media without live forensics.

There is now a trend towards live memory forensics using tools such as WindowsSCOPE and tools for mobile devices.

Today, there are single-purpose open-source tools like Wireshark, a packet sniffer, and HashKeeper, a tool to speed up examination of database files. As well as commercial platforms with multiple functions and reporting capabilities like Encase or CAINE, an entire Linux distribution designed for forensics programs.

In general tools can be broken down into the following ten categories:

1. Disk and data capture tools
2. File viewers

3. File analysis tools
4. Registry analysis tools
5. Internet analysis tools
6. Email analysis tools
7. Mobile devices analysis tools
8. Mac OS analysis tools
9. Network forensics tools
10. Database forensics tools

What are the Legal Considerations of Digital Forensics?

The examination of digital media is covered by national and international legislation. For civil investigations, laws may restrict what can be examined. Restrictions against network monitoring or reading personal communications are common.

Likewise, criminal investigations may be restricted by national laws that dictate how much information can be seized. As an example, seizure of evidence by law enforcement is governed by the PACE act in the United Kingdom. The 1990 computer misuse act legislates against unauthorized access to computer material which makes it hard for civil investigators in the UK.

One of the common considerations which is largely undecided is an individual's right to privacy. The US Electronic Communications Privacy Act places limitations on the ability for law enforcement and civil investigators to intercept and access evidence.

The act makes a distinction between stored communication (e.g. email archives) and transmitted communication (e.g. VOIP). Transmitted communication is considered more of a privacy invasion and is harder to obtain a warrant for.

Digital evidence falls into the same legal guidelines as other evidence.

In general, laws dealing with digital evidence are concerned with:

- **Integrity:** Ensuring the act of seizing and acquiring digital media does not modify the evidence (either the original or the copy).
- **Authenticity:** The ability to confirm the integrity of information. The chain of custody from crime scene through analysis and ultimately to the court, in the form of an audit trail, is an important part of establishing the authenticity of evidence.

Each of the branches of digital forensics have their own guidelines on how to conduct investigations and handle data.

What are the Different Branches of Digital Forensics?

Digital forensics is no longer synonymous with computer forensics. It is increasingly concerned with data from other digital devices such as tablets, smart phones, flash drives and even cloud computing.

In general, we can break digital forensics into five branches:

1. Computer forensics
2. Mobile device forensics
3. Network forensics
4. Forensic data analysis
5. Database forensics

What is Computer Forensics?

Computer forensics or computer forensic science is a branch of digital forensics concerned with evidence found in computers and digital storage media. The goal of computer forensics is to examine digital data with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.

It is used in both computer crime and civil proceedings. The discipline has similar techniques and principles to data recovery, with additional guidelines and practices designed to create a legal audit trail with a clear chain of custody.

Evidence from computer forensics investigations is subjected to the same guidelines and practices of other digital evidence.

What is Mobile Device Forensics?

Mobile device forensics is a branch of digital forensics focused on the recovery of digital evidence from mobile devices using forensically sound methods.

While the phrase mobile device generally refers to mobile phones, it can relate to any device that has internal memory and communication ability including PDA devices, GPS devices and tablets.

While the use of mobile phones in crime has been widely recognized for years, the forensic study of mobile phones is a new field, beginning in the late 1990s.

The growing need for mobile device forensics is driven by:

- Use of mobile phones to store and transmit personal and corporate information
- Use of mobile phones in online transactions

That said, mobile device forensics is particularly challenging due to:

- Evidential and technical challenges such as cell site analysis which makes it possible to determine roughly the cell site zone from which a call was made or received but not a specific location such as an address
- Changes in mobile phone form factors, operating systems, data storage, services, peripherals and even pin connectors and cables
- Storage capacity growth
- Their proprietary nature
- Hibernation behavior where processes are suspended when the device is off or idle

As a result of these challenges, many tools exist to extract evidence from mobile devices. But no one tool or method can acquire all evidence from all devices. This has forced forensic examiners, especially those who wish to be expert witnesses, to undergo extensive training to understand how each tool and method acquires evidence, how it maintains forensic soundness and how it meets legal requirements.

What is Network Forensics?

Network forensics is a branch of digital forensics focused on monitoring and analyzing computer network traffic for information gathering, legal evidence or intrusion detection.

Unlike other branches of digital forensics, network data is volatile and dynamic. Once transmitted, it is gone so network forensics is often a proactive investigation.

Network forensics has two general uses:

1. Monitoring a network for anomalous traffic and identifying intrusions.
2. Law enforcement may analyze capture network traffic as part of criminal investigations.

What is Forensic Data Analysis?

Forensic data analysis (FDA) is a branch of digital forensics that examines structured data in regards to incidents of financial crime. The aim is to discover and analyze patterns of fraudulent activities. Structured data is data from application systems or their databases.

This can be contrasted to unstructured data that is taken from communication, office applications and mobile devices. Unstructured data has no overarching structure and analysis therefore means applying keywords or mapping patterns. Analysis of unstructured data is usually done by computer forensics or mobile device forensics experts.

What is Database Forensics?

Database forensics is a branch of digital forensics related to databases and their related metadata. Cached information may also exist in a server's RAM requiring live analysis techniques.

A forensic examination of a database may relate to timestamps that apply to the update time of a row in a relational database that is being inspected and tested for validity to verify the actions of a database user. Alternatively, it may focus on identifying transactions within a database or application that indicate evidence of wrongdoing, such as fraud.

CHALLENGES FACED BY DIGITAL FORENSIC

Development is severely challenged by the growing popularity of digital devices and the heterogeneous hardware and software being utilised.

- The increasing variety of file formats and OSs hampers the development of standardized DF tools and processes.
- The emergence of smart phones that increasingly utilize encryption renders the acquisition of digital evidence an intricate task.

Also, advancements in cybercrime have culminated in the substantial challenge, such as Crime as a Service (CaaS), which provides the attackers with easy access to the tools, programming frameworks, and services needed to conduct cyber attacks.

- Digital forensics has become an important tool in the investigation/identification of computer-based and computer-assisted crime.
- Eric Holder (Deputy Attorney General of the United States Subcommittee on Criminal Oversight for the Senate) has classified the challenges into three categories

1. Technical challenges
2. Legal challenges
3. Resource challenge

Technical challenges:Finding the forensics evidences have been hindered by:

➢Different Media format

➢Encryption

➢Anti-forensics

➢ Steganography.

➢Live acquisition and analysis

Legal challenges:

➢ Jurisdictional issue.

➢ Lack of standard legislation creates the legal challenges.

➢ Status as scientific evidence.

➢ What is the known or potential rate of error of the method used.

➢ whether the theory or method has been generally accepted by the scientific community.

Resource challenges: It is severely challenged by the growing popularity of digital devices and the heterogeneous hardware and software platforms being utilized.

➢ Volume of data.

➢ Time taken to acquire and analyze forensic media.

➢ To ensure to satisfied critical investigative and prosecutorial needs at all levels of government

COMPUTER CRIME

Alternatively referred to as **cyber crime**, **e-crime**, **electronic crime**, or **hi-tech crime**. **Computer crime** is an act performed by a knowledgeable computer user, sometimes referred to as a hacker that illegally browses or steals a company's or individual's private information. In some cases, this person or group of individuals may be malicious and destroy or otherwise corrupt the computer or data files.

Why do people commit computer crimes?

In most cases, someone commits a computer crime to obtain goods or money. Greed and desperation are powerful motivators for some people to try stealing by way of computer crimes. Some people may also commit a computer crime because they are pressured, or forced, to do so by another person.

Some people also commit a computer crime to prove they can do it. A person who can successfully execute a computer crime may find great personal satisfaction in doing so. These types of people, sometimes called black hat hackers, like to create chaos, wreak havoc on other people and companies.

Another reason computer crimes are sometimes committed is because people are bored. They want something to do and don't care if they commit a crime.

Examples of computer crimes

Below is a list of the different types of computer crimes today. Clicking any of the links gives further information about each crime.

- **Child pornography** - Making, distributing, storing, or viewing child pornography.
- **Copyright violation** - Stealing or using another person's Copyrighted material without permission.
- **Cracking** - Breaking or deciphering codes designed to protect data.
- **Cyber terrorism** - Hacking, threats, and blackmailing towards a business or person.
- **Cyberbully or Cyberstalking** - Harassing or stalking others online.

- **Cybersquatting** - Setting up a domain of another person or company with the sole intention of selling it to them later at a premium price.
- **Creating Malware** - Writing, creating, or distributing malware (e.g., viruses and spyware.)
- **Data diddling** - Computer fraud involving the intentional falsification of numbers in data entry.
- **Denial of Service attack** - Overloading a system with so many requests it cannot serve normal requests.
- **Doxing** - Releasing another person's personal information without their permission.
- **Espionage** - Spying on a person or business.
- **Fraud** - Manipulating data, e.g., changing banking records to transfer money to an account or participating in credit card fraud.
- **Green Graffiti** - A type of graffiti that uses projectors or lasers to project an image or message onto a building.
- **Harvesting** - Collect account or account-related information on other people.
- **Human trafficking** - Participating in the illegal act of buying or selling other humans.
- **Identity theft** - Pretending to be someone you are not.
- **Illegal sales** - Buying or selling illicit goods online, including drugs, guns, and psychotropic substances.
- **Intellectual property theft** - Stealing practical or conceptual information developed by another person or company.
- **IPR violation** - An intellectual property rights violation is any infringement of another's Copyright, patent, or trademark.
- **Phishing** or **vishing** - Deceiving individuals to gain private or personal information about that person.
- **Ransomware** - Infecting a computer or network with ransomware that holds data hostage until a ransom is paid.
- **Salami slicing** - Stealing tiny amounts of money from each transaction.
- **Scam** - Tricking people into believing something that is not true.
- **Slander** - Posting libel or slander against another person or company.
- **Software piracy** - Copying, distributing, or using software that was not purchased by the user of the software.
- **Spamming** - Distributed unsolicited e-mail to dozens or hundreds of different addresses.

- **Spoofing** - Deceiving a system into thinking you are someone you're not.
- **Swatting** - The act of calling in a false police report to someone else's home.
- **Theft** - Stealing or taking anything (e.g., hardware, software, or information) that doesn't belong to you.
- **Typosquatting** - Setting up a domain that is a misspelling of another domain.
- **Unauthorized access** - Gaining access to systems you have no permission to access.
- **Vandalism** - Damaging any hardware, software, website, or other object.
- **Wiretapping** - Connecting a device to a phone line to listen to conversations.

CRIMINALISTICS

The criminal justice system in America is the overarching establishment through which crimes and those who commit them are discovered, tried, and punished. This includes all of the institutions of government aimed at upholding social order, deterring and mitigating crime, and sanctioning those who violate the law, such as law enforcement and the court and jail systems.

Criminology and criminalistics are two subsets of the criminal justice system. Criminology relates to studying and preventing crime—typically with behavioral sciences like sociology, psychology, and anthropology. Criminalistics refers to a type of forensics—the analysis of physical evidence from a crime scene.

While criminology has preventative components, criminalistics comes into effect only after a crime has been committed. A criminalist applies scientific principles to the recognition, documentation, preservation, and analysis of physical evidence from a crime scene. Criminalistics can also include crime scene investigations. The Bureau of Labor Statistics (BLS) classifies criminalists as forensic science technicians. Most professionals regard criminalistics as a specialty within the field of forensic science.

WHAT DO CRIMINALISTS DO?

Criminalists use their knowledge of physical and natural science to examine and analyze every piece of evidence from a crime scene. They prepare written reports of their findings and may have to present their conclusions in court. A criminalist is not involved in determining the guilt or innocence of an accused individual. Their job, rather, is to present an objective analysis of the evidence.

There are several critical skills that criminalists need to be successful in their work. First, they must be detail-oriented and have excellent written and verbal communication skills. Second, they should also have strong critical-thinking and problem-solving skills and a solid background in science, statistics, physics, math, and ethics. Finally, criminalists should be comfortable testifying in court.

Most of a criminalist's work is performed in a laboratory unless they specialize in crime scene investigation. Their job typically includes recognizing what information is important, collecting and analyzing evidence without contaminating it, and organizing all information and evidence coherently.

Criminalistics has many fields of specialization. Specialties include, but are not limited to:

- Alcohol and drugs
- Arson
- Blood and tissue spatter
- Computer forensics
- DNA
- Explosions
- Serology (examining and analyzing body fluids)
- Toxicology
- Firearms and tool marks
- Trace evidence
- Wildlife (analyzing evidence against poachers)

As long as crimes continue to be committed, there will always be work for criminalists. A criminal will always leave evidence, no matter how minute, according to forensic scientist and "Father of Criminalistics" Paul L. Kirk:

> "Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as silent evidence against him. Not only his fingerprints or his footprints, but his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen that he deposits or collects – all these and more bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent

> because human witnesses are. It is factual evidence. Physical evidence cannot be wrong; it cannot perjure itself; it cannot be wholly absent. Only its interpretation can err. Only human failure to find it, study and understand it, can diminish its value."

As soon as a crime is reported, an investigation is opened by the police or law enforcement agency with jurisdiction.

Police detectives and investigators use criminalistics in crime-scene investigations. Criminalistics is "the scientific study and evaluation of physical evidence in the commission of crimes." Criminalistics plays a vital role in organizing crime scenes, helping victims, ensuring justice, and serving the public.

Criminalists cover a broad range of criminal justice jobs within the forensic science field that examine physical evidence to link crime scenes with victims and offenders. Criminalists are sometimes referred to as lab technicians or crime scene investigators, a term made famous by the TV drama *CSI*.

These criminalists consult with experts, examine and analyze a variety of evidence including fingerprints, hair, fibers, skin, blood, and more. The criminalists then use their analysis to determine answers to how a crime was committed.

CRIMINALISTICS IN POLICE INVESTIGATIONS

A report from the National Institute of Justice outlined the role of criminalistics in police work. Criminalists investigate a variety of crimes, including domestic and aggravated assaults, burglary, robbery, sexual violence, and homicide.

Here are the basic functions completed by criminalists:

Establishing an element of the crime

- It’s important for criminalists to establish proof that a crime occurred and to determine the cause and manner of death. Autopsies will help confirm the latter, while sending crime scene samples of blood, drugs, or semen, for example, could help determine the crime itself.

Identification of a suspect or victim

- Fingerprint and DNA testing are two examples of forensic evidence that criminalists use to identify an offender.

Associative evidence

- This type of scientific finding can help link the offender to the victim. Examples of associative evidence include hair follicles, blood, semen, fingerprints left on an object, foot impressions, and more.

Reconstruction

- Criminalists try to reconstruct how the crime happened using evidence from the crime scene. For example, certain evidence on a gunshot victim can discern the distance between a victim and the shooter.

Corroboration

- Physical evidence from a crime scene can corroborate or refute information that investigators collect during interviews with witnesses, victims and suspects.

CRIMINALISTICS IN REAL TIME

The FBI and U.S. Department of Justice distribute a guide for criminalist protocols when responding to a crime scene.

Here’s what the Justice Department recommends takes place.

Arrival/Initial Response

- Upon arriving on the scene, criminalists should attempt to preserve the crime scene with minimal disturbance of the physical evidence.
- Criminalists should make initial observations to assess the scene while ensuring officer safety and security.
- They should react with caution. Offenders could still be at the crime scene and criminalists should remain alert and attentive until the crime scene is declared clear of danger.

Documentation and Evaluation

- The investigator(s) in charge should set responsibilities, share preliminary information and develop investigative plans in compliance with department policy and local, state and federal laws.
- Criminalists should speak with the first responders regarding observations from the crime scene before evaluating safety issues at the scene, establishing a path of exit and entry, and initial scene boundaries.
- If multiple scenes exist, criminalists should establish and maintain communication with personnel at those sites.

Processing the Scene

- Based on the type of incident and complexity of the crime scene, criminalists should determine team composition on site.
- Criminalists will assess the scene to determine which specialized resources are required. For example, forensic examiners could be called to the scene, or a coroner to investigate a cadaver.

Completing and Recording the Crime Scene Investigation

- Criminalists should establish a crime scene debriefing team, which enables all law enforcement bodies to share information about findings before the scene is released.
- Criminalists determine what evidence was collected, discuss the preliminary scene findings with scene personnel, discuss potential forensic tests that will take place, and initiate any action required to complete the crime scene investigation.

Crime scene investigation

The key role of the crime scene investigation (or CSI) is the comparison between an object's material condition and trace evidence obtained from this object, as well as their mutual relationship. The core of the CSI lies in direct observation of the scene and the object while searching for material changes in the object, which can become evidence. However, this process is not just mere observation. It is also empirical examination, continuous evaluation and documentation of a crime scene's physical condition and objects connected to it. Observation can be made by the senses or using electronic/technical equipment.

The goal of the CSI is to (a) find evidence, (b) discover relationships and associations, and (c) detect other circumstances, such as conditions, motives and hypotheses for the creation of criminalistics versions51. The significance of the CSI as one of criminalistic methods is remarkable. It enables investigators to understand the characteristics of the event that took place at the crime scene including plausible causes and conditions that gave rise to the criminal event, or to understand the offender who committed crime. Success of a criminal investigation often depends on the quality of the CSI, which is one criminalistic tactic that cannot be replaced by any other method. The level of its quality essentially influences the quality of the gathered evidence. Insufficient knowledge and skills or an irresponsible approach of law enforcement officers may lead to a lesser punishment or even acquittal of a true offender. CSI provides initial information about evidence and the event itself which took place at the crime scene. A shoe print might be an example, as it may lead to knowledge one's height. Facts derived from preliminary information about evidence depend considerably on experience and knowledge. The crime scene investigation is considered to be a team effort made by the police officers, investigators, and forensic specialists52. The first officers at the crime scene are the members of the “permanent access group”. Additional participants of the CSI are witnesses, any victims or even the accused. It is crucial to use good judgement in deciding whether the attendance of such people is necessary or not because it might put the investigation at risk. A phone call made to 112 initiates four major tasks: (a) completion of initial, emergency activities, (b) preparation for crime scene examination, (c) completion of crime scene examination along with proper documentation of its results and (d) evaluation of accomplished results and their application53 .

Criminalistic documentation

The aim of criminalistic documentation is to secure trace evidence (verbally and acoustically) and to take control of the course and outcome of the criminal investigation. In criminalistic examination, (investigation), trace evidence and comparing material have the nature of documented marks and seized objects54. Documented marks are delivered in written form, (transcript), phonogram (audio recording), photographic form (photographs, hologram video, film, and digital recording), and topographic form (sketch, plan, and drawing). Standard criminalistic documentation comes in the form of a transcript. In other words, it describes a situation that was observed by its author. A transcript must consist of objectively true statement of facts – the subjective feelings of the author are not allowed. In addition to an oral description of the observed situation, investigators can choose the form of an audio (phonographic) recording. Furthermore, this form of documentation is frequently used at the interrogation/interview, where the statements made by the accused, witnesses or the victim are recorded. However, photographic form provides the most precise documentation. Written, phonographic and photographic forms are supplemented by topographic form, usually consisting of sketches, plans, and drawings. Seized objects are submitted in their natural form, and the exact location where they were found is documented along with all of the circumstances and conditions surrounding their discovery. Not only trace evidence but also any manipulation to it must be documented in order to protect the chain of evidence. Each and every piece of evidence, its manipulation and the circumstances around it is important for a criminal investigation, therefore thorough documentation is crucial.

Identifying digital evidence:

Digital evidence can be any information stored or transmitted in digital form. Because you can't see or touch digital data directly, it's difficult to explain and describe. Is digital evidence real or virtual? Does data on a disk or other storage medium physically exist, or does it merely represent real information? U.S. courts accept digital evidence as physical evidence, which means that digital data is treated as a tangible object, such as a weapon, paper document, or visible injury, that's related to a criminal or civil incident. Courts in other countries are still updating their laws to take digital evidence into account. Some require that all digital evidence be printed out to be presented in court. Groups such as the Scientific Working Group on Digital Evidence (SWGDE; www.swgde.org) and the International Organization on Computer Evidence (IOCE; www.ioce.org) set standards for recovering, preserving, and examining digital evidence. For more information on digital evidence, visit www.ojp.usdoj.gov/nij/ pubs-sum/187736.htm and read "Electronic Crime Scene Investigation: A Guide for First Responders," which provides guidelines for U.S. law enforcement and other responders who protect an electronic crime scene and search for, collect, and preserve electronic evidence.

Following are the general tasks investigators perform when working with digital evidence:

- Identify digital information or artifacts that can be used as evidence.
- Collect, preserve, and document evidence.
- Analyze, identify, and organize evidence.
- Rebuild evidence or repeat a situation to verify that the results can be reproduced reliably.Collecting computers and processing a criminal or incident scene must be done systematically.

To minimize confusion, reduce the risk of losing evidence, and avoid damaging evidence, only One person should collect and catalog digital evidence at a crime scene or lab, if practical. If there's too much evidence or too many systems to make it practical for one person to perform these tasks, all examiners must follow the same established operating procedures, and a lead or managing examiner should control collecting and cataloging evidence. You should also use standardized forms (discussed later in “Documenting Evidence”) for tracking evidence to ensure that you consistently handle evidence in a safe, secure manner. An important challenge investigators face today is establishing recognized standards for digital evidence.

For example, cases involving several police raids are being conducted simultaneously in several countries. As a result, you have multiple sites where evidence was seized and hundreds of pieces of digital evidence, including hard drives, cell phones, memory sticks, PDAs, and other storage devices. If law enforcement and civil organizations in those countries have agreed on proper procedures (generally, the highest control standard should be applied to evidence collection in all jurisdictions), the evidence can be presented in any jurisdiction confidently.

Mobile Forensics – Definition, Uses, and Principles

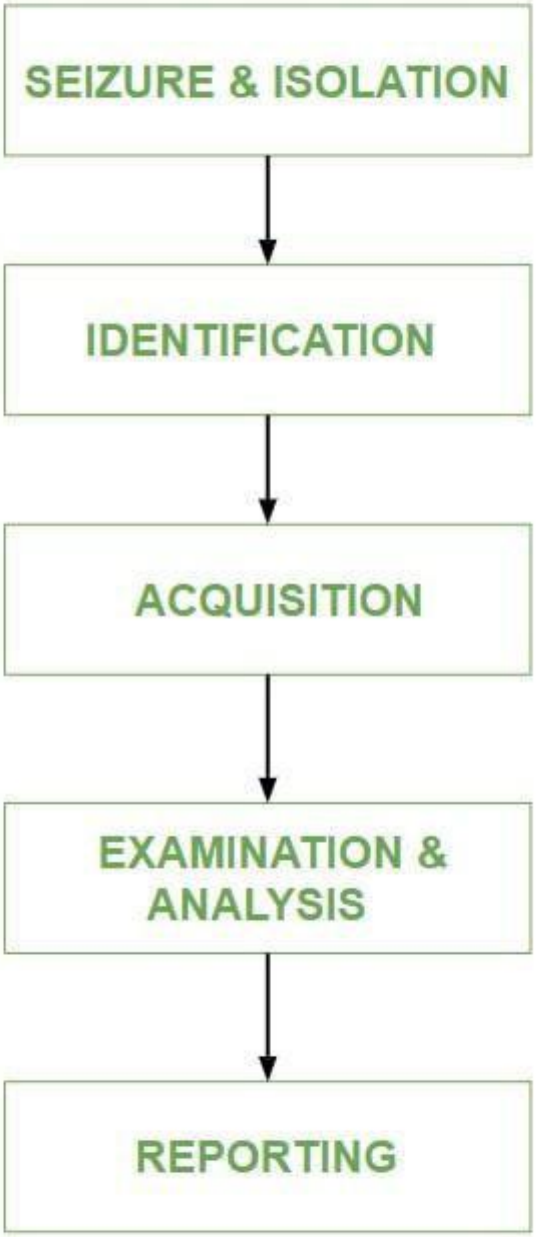
Mobile forensics, a subtype of digital forensics, is concerned with retrieving data from an electronic source. The recovery of evidence from mobile devices such as smartphones and tablets

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

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.

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.

III. CHALLENGES ASSOCIATED WITH MOBILE PHONE FORENSICS A. Mobile phone forensics is challenging field due to fast changes in technology. Several models of mobile phones exist in the world today. Manufacturers lack standardized methods of storing data. Most of the mobile phones use closed operating systems and has proprietary interfaces. To meet this challenge there is always a need for development of new forensics tools and techniques.

B. Signals of mobile phone need to be blocked while carrying forensics analysis. Blocking RF signals quickly drains the battery. This can be minimized while carrying forensics analysis of mobile phones in properly shielded labs. Shielding methods for lab include such as EMI/EMC protection.

C. Large variety of data cables exist for mobile phones. Identification and collection of cables required for forensics analysis of mobile phones is challenging task. Small databases for defining mobile phone models and their associated cables with tags can help a great deal.

D. Most of the commercially available forensic tools do not provide solutions to deal with physically damaged mobile phones. Forensic examiners must be trained and equipped to handle such situations.

E. Conflicts can occur due to different operating system, vendor and version specific device drivers. It is therefore recommended to have separate machines for each type of forensic software. However to economize resources Virtual Machine environments can be created.

F. Data on active mobile phone tends to change constantly due to lack of conventional write-blocking mechanism. Analysis must be done on a phone that is powered ON but it is ideal that the phone does not receive any calls, text messages, or other communications. Shielded labs can address this issue.

G. Most of the international trainings available in the field are vendor specific. There is need of for neutral and standard trainings.

H. Status of unopened emails and messages will change after reading them. Care must be taken while recoding such type of evidence.

J. Mobile phones may lose data or ask for security measures on next restart once shut down. Owner of the mobile phone (if available) may be asked about security codes.

K. Authentication mechanisms can confine access to data. Finding of Personal Identification Number (PIN), Phone Unlock Key (PUK), and handset and memory card passwords can become difficult at times.

L. Now days there are various methods available to remotely destroy or change data on a mobile phone. Such happening can be avoided in shielded lab environments while carrying forensic investigations. Care must also be taken to protect mobile phones while carrying them to labs.

M. Data from mobile phone internal memory is restricted without the use of SIM card. Inserting another SIM can cause the loss of mobile phone data.

N. Many commercial mobile phone forensic tools only provide logical acquisition of data. Deleted data can only be recovered using physical acquisition.

O. Introduction of Mobile Number Portability (MNP) can result into improper identification of subscriber. Mobile Phone network operators may be consulted for proper identification.

P. IMEI changing for few mobile handsets is possible with the use flashing tools like Universal Flasher UFS-3. This can result improper identification of phones. These illegal activities shall be banned.

IT act 2000

The Act **provides a legal framework for electronic governance by giving recognition to electronic records and digital signatures**. It also defines cyber crimes and prescribes penalties for them. The Act directed the formation of a Controller of Certifying Authorities to regulate the issuance of digital signatures.

The Information Technology Act, 2000 also Known as an **IT Act** is an act proposed by the Indian Parliament reported on 17th October 2000. This Information Technology Act is based on the United Nations Model law on Electronic Commerce 1996 (UNCITRAL Model) which was suggested by the General Assembly of United Nations by a resolution dated on 30th January, 1997. It is the most important law in India dealing with Cybercrime and E-Commerce.

The main objective of this act is to carry lawful and trustworthy electronic, digital and online transactions and alleviate or reduce cybercrimes. The IT Act has 13 chapters and 90 sections. The last four sections that starts from 'section 91 – section 94', deals with the revisions to the Indian Penal Code 1860.

The IT Act, 2000 has two schedules:

- **First Schedule –**

  Deals with documents to which the Act shall not apply.
- **Second Schedule –**

  Deals with electronic signature or electronic authentication method.

The offences and the punishments in IT Act 2000 :

The offences and the punishments that falls under the IT Act, 2000 are as follows :-

1. Tampering with the computer source documents.

2. Directions of Controller to a subscriber to extend facilities to decrypt information.
3. Publishing of information which is obscene in electronic form.
4. Penalty for breach of confidentiality and privacy.
5. Hacking for malicious purposes.
6. Penalty for publishing Digital Signature Certificate false in certain particulars.
7. Penalty for misrepresentation.
8. Confiscation.
9. Power to investigate offences.
10. Protected System.
11. Penalties for confiscation not to interfere with other punishments.
12. Act to apply for offence or contravention committed outside India.
13. Publication for fraud purposes.
14. Power of Controller to give directions.

Sections and Punishments under Information Technology Act, 2000 are as follows :

SECTION	PUNISHMENT
Section 43	This section of IT Act, 2000 states that any act of destroying, altering or stealing computer system/network or deleting data with malicious intentions without authorization from owner of the computer is liable for the payment to be made to owner as compensation for damages.
Section 43A	This section of IT Act, 2000 states that any corporate body dealing with sensitive information that fails to implement reasonable security practices causing loss of other person will also liable as convict for compensation to the affected party.
Section 66	Hacking of a Computer System with malicious intentions like fraud will be punished with 3 years imprisonment or the fine of Rs.5,00,000 or both.
Section 66 B, C,	Fraud or dishonesty using or transmitting information or identity theft is punishable with 3 years imprisonment or Rs. 1,00,000 fine or both.

D	
Section 66 E	This Section is for Violation of privacy by transmitting image or private area is punishable with 3 years imprisonment or 2,00,000 fine or both.
Section 66 F	This Section is on Cyber Terrorism affecting unity, integrity, security, sovereignty of India through digital medium is liable for life imprisonment.
Section 67	This section states publishing obscene information or pornography or transmission of obscene content in public is liable for imprisonment up to 5 years or fine of Rs. 10,00,000 or both.

Amendment of it act 2008:

The IT (Amendment) Act, 2008 (ITAA 2008) has established a strong data protection regime in India. It addresses industry's concerns on data protection, and creates a more predictive legal environment for the growth of e-commerce that includes data protection and cyber crimes measures, among others.

These changes included expanding the definition of cybercrime and adding new penalties for offenses such as identity theft, publishing private images without consent, cheating by impersonation, and sending offensive messages or those containing sexually explicit acts through electronic means.