CYBER CRIME & CYBER FORENSICS-191CSED

SYNOPSIS

- INTRODUCTION AND OVERVIEW
- NATURE AND SCOPE
- TYPES
- SOCIAL ENGINEERING
- CATEGORIES
- PROPERTY

CRIME

- Crime generally refers to an illegal act that's punishable by law and regulation.

1. **Conventional Crime:** Conventional crime typically involves physical force or the threat of physical force to commit the crime. Ex: Theft, assault, and burglary.

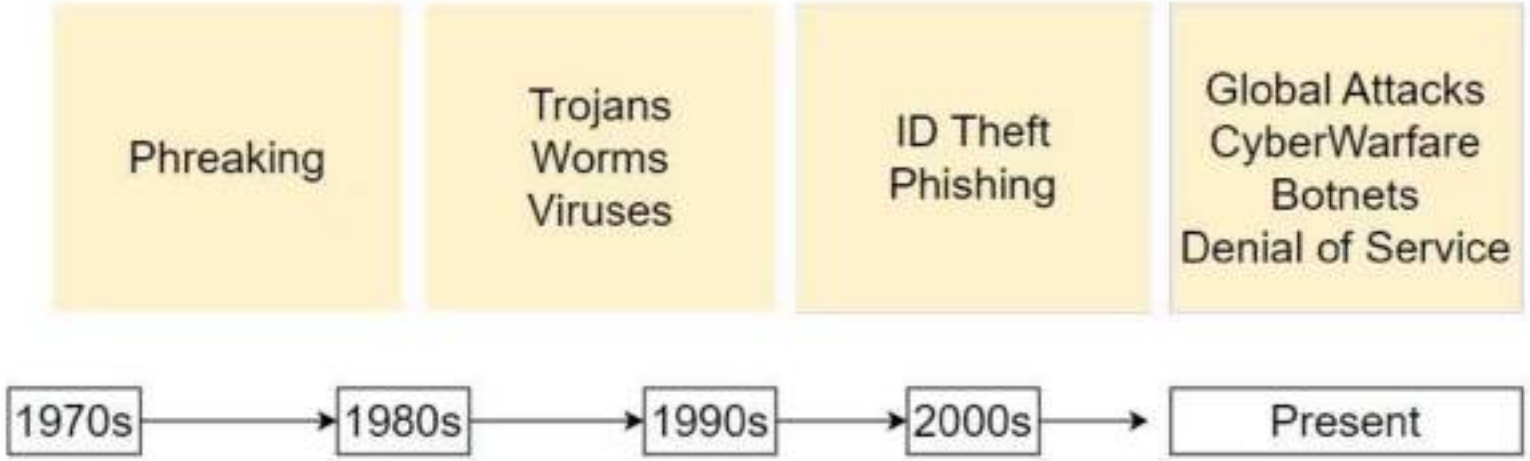
- It tends to target individuals or physical assets such as offices, relatives, and homes.
- **Cyber Crime:**
- These crimes basically involve the use of computers, the internet, or other digital devices to commit a crime. Examples of cybercrimes include malware attacks, identity theft, and online fraud.
- Remain undetected for a long period as there is no physical presence and no on-ground evidence.EX:**Hacking, Cyberbullying, Cyberstalking, Malware**,

CYBER CRIME

CYBER CRIME

- **Cyber-Computer ,crime-unfair and illegal**
- Any **criminal** activity carried out over the **internet** is referred to as cybercrime.
- The first incident of cybercrime was documented in **1970's**.
- Cybercrime refers to criminal conduct committed with the **aid of a computer or other electronic equipment** connected to the internet.
- Individuals or small groups of people with little technical knowledge and highly organized worldwide criminal groups with relatively talented developers and specialists can engage in cybercrime.

History of cyber crime



Examples of Basic Cyber Crimes

- **Stolen credit card information-**person's credit card **information** is stolen and used unlawfully .
- **Hacking into a government website-**Another type of cybercrime is **tampering** with **sensitive government data**.
- **Theft of user accounts-**The attackers gained access to **private** information and passwords that were used to **access user accounts** in other online services. Most of this data is available even today on the dark web.

Types of cyber crime

Cybercrimes are broadly categorized into three fields:

- **Individual**
- It is a cybercrime that entails a **single individual disseminating malicious or unlawful material** via the internet. For example, distributing pornography, human trafficking, and online stalking.
- **Property**
- This cybercrime involves obtaining access to **individuals' bank or credit card information, accessing their funds, making online transactions**, or executing phishing schemes to persuade individuals to give away **personal information**.
- **Government**
- While these cybercrimes are uncommon, they are nevertheless considered significant offenses. It entails breaking into government databases and hacking official websites.

Sub-Types of Cybercrime

There are 5 types

1.Cyber Terrorism

2.Cyber Extortion

3.Cyber Warfare

4.Internet Fraud

5.Cyber Stalking

Types of Cybercrime

1.Cyber Terrorism

- Cyber terrorism can be defined as an **act of terrorism committed** through the use of **cyberspace** or computer resources.
- This may include different type of activities either by **software or hardware for threatening life of citizens.**
- Cyber terrorism is the use of the computer and internet to perform violent acts that result in **loss of life**.

2.Cyber Extortion

- Cyber extortion occurs when **a website, e-mail server or computer system** is subjected to or **threatened** with repeated **denial of service** or other attacks by malicious hackers.
- These hackers **demand huge money** in return for assurance to **stop the attacks** and to offer protection.

3.Cyber Warfare

- Cyber warfare is the use or targeting in a battle space or warfare context of computers, **online control systems** and networks.
- It involves both **offensive** and **defensive** operations concerning to the threat of cyber attacks, **espionage** and **sabotage.**

4.Internet Fraud

- Internet fraud is a type of fraud or deceit which makes use of the Internet and could include **hiding of information or providing incorrect information** for the purpose of deceiving victims for **money or property**.
- Internet fraud is not considered a **single, distinctive** crime but covers a range of **illegal and illicit actions** that are committed in cyberspace.

5.Cyber Stalking

- This is a kind of **online harassment** wherein the victim is subjected to a barrage of **online messages and emails**.
- In this case, these stalkers know their victims and instead of offline stalking, they use the Internet to stalk.
- However, if they notice that cyber stalking is not having the desired effect, they begin **offline stalking** along with cyber stalking to make the victims' lives more miserable.

Types of Cybercrime-attacks

- There are various forms of Cybercrime, namely- phishing, malware, cyberbullying, crypto-jacking, Cyber espionage, etc, and we have discussed these below in brief.
- **Phishing**– Phishing attacks take place when **spam or fraudulent emails** or other forms of communication are sent to people through a source that seems **reputable**.
- **Malware**– It is a type of Cyber Attack where **malicious software**, programs, or codes are used to **corrupt data and damage or disables** computers or other devices such as mobiles, tablets, networks, etc.

Cont…

- **Cyberbullying**– It is also a Cybercrime where computers, tablets, or mobile phones are used to send, post, or share private, negative, or **false information** about someone **without their consent** to cause embarrassment or humiliation.
- **Cryptojacking**– The attacker breaks into a **person's computing device** to extract money from the target in the form of **cryptocurrency** without their consent or knowledge.
- **Cyber Espionage**– Cyber espionage occurs when an **attacker illicitly steals** or gains access to a **company's or government's** classified, **sensitive data or intellectual property** to gain an advantage over the entity.

Malware

- **Malware- malicious software**
- It refers to any intrusive software developed by cybercriminals (often called hackers) to steal data and damage or destroy computers and computer systems.
- **Example**: **viruses, worms, Trojan viruses, spyware, adware, and ransomware.**
- Recent malware attacks have exfiltrated data in mass amounts.

Prevention of Cyber Crime:

1.Use strong password:

Maintain **different** password and username **combinations** for each account and resist the temptation to write them down.

Weak passwords can be easily cracked using certain attacking methods like **Brute force attack, Rainbow table attack** etc, So make them complex.

- That means combination of letters, numbers and special characters.

2.Use trusted antivirus in devices:

Always use t**rustworthy** and highly **advanced antivirus software** in mobile and personal computers.

- This leads to the prevention of different virus attack on devices.

Cont…

3.Keep social media private:

Always keep your **social media accounts** data privacy only to **your friends.**

Also make sure only to make friends who are **known to you**.

4.Keep your device software updated:

Whenever you get the **updates** of the system **software update** it at the same time because sometimes the **previous version can be easily attacked.**

Cont…

5.Use secure network:

Public Wi-Fi are vulnerable. Avoid conducting **financial or corporate transactions** on these networks.

6.Never open attachments in spam emails:

A computer get infected by malware attacks and other forms of cybercrime is via **email attachments in spam emails**.

Never open an attachment from a sender you do not know.

7.Software should be updated: Operating system should be updated regularly when it comes to internet security.

This can become a potential threat when cybercriminals exploit flaws in the system.

Challenges of Cyber Crime:

- **People are unaware of their cyber rights:**
  The Cybercrime usually happen with **illiterate** people around the world who are **unaware** about their **cyber rights** implemented by the government of that particular country.
- **Anonymity:**
  Those who Commit cyber crime are **anonymous** for us so we cannot do anything to that person.
- **Less numbers of case registered:**
  Every country in the world faces the challenge of cyber crime and the **rate of cyber crime is increasing** day by day because the people who even don't register a case of cyber crime and this is major challenge for us as well as for authorities as well.

- **Mostly committed by well educated people:**
  Committing a cyber crime is not a cup of tea for every individual. The person who commits cyber crime is a very **technical** person so he knows how to commit the crime and not get caught by the authorities.

- **No harsh punishment:**
  In Cyber crime there is no harsh punishment in every cases. But there is harsh punishment in some cases like when somebody commits **cyber terrorism in that case there is harsh punishment for that individual**. But in other cases there is no harsh punishment so this factor also gives encouragement to that person who commits cyber crime.

Crimes associated with mobile-ECD

- ECD- laptop,tab,PC's,Smart phone as these devices widely used as a
- Tool for cybercrime as they are **portable & cheap** alternative to computer
- Serve as a **personal** & **difficult to locate**.
- Some forms of cybercrime are exclusive to mobile ECD's are listed below:
- **Handset theft:**
- To **get valuable** information from SMS,Contacts etc from financial gain by selling it.

- **SMS related crimes:**
- SMishing,Flashing or auto deletion of S**MS,tampering,altering** the dates in SMS & SMS Spoofing.
- **SMishing:**
- SMS Phising –attacker dupes the victim with message in such a way as to **reveal their personal data**.
- **Flashing SMS:**
- Sort of message flashes on screen & automatically **gets deleted once the user exists the application.**

- **Altering dates in SMS:**
- This refers to **sending back dated or post dated** SMSes by changing the message time stamp.
- **SMS spoofing:**
- **Masquerading** the identity of an offender & sending Messages to the victim as a genuine user.
- **Bluetooth Mobile Hacking:**
- If it is enable there is **Possibility of remote control** of mobile handset.

- **Crime with calls:**
- **Voice Phishing(vishing)**-either information or money stolen from the victim using telephone network.
- It is in two forms

1. Wardialing: asking of Pin,cvv
2. Dumpster diving:Target them

- **MMS crime**:Scandals & Morphing
- **SIM card Cloning**:Making duplicate copy of it.

Cyber criminals

- They are categorized into two as

1. **Expertise-8**
2. **Intention-2**

Classification of cyber criminals

- Cyber crime is refered to as a white collar crime.

1.Mules:

They **are unaware** that they are the part of the criminal gang in money laundering.

2.Toolkit newbies or getaways:

Having **limited technical skills ,just follow the guidelines** & documentation,more possible to transform into serious criminals.

3.Activists:To **promote religion,politics**

They can steal the data or cause damage to IT infrastructure.

4.Cyberpunks:

Capability to **develop a small programs** to steal credit cards or spamming.

5.Internals:

Employees seek revenge with the goal of disturbing the security of information and **cause damage.**

6.Nation state actors:

People who work for **one government** to **disturb enemies IT** infrastructure,steal sensitive information,even create other intentional activities.

7.Coders:

Develop code to damage others.

8.Professionals:

Associate cyber crime as their **profession** and use **technology to hide** the occurrence of crime.

Depending upon the **intention of offenders** ,they are categorized as follows:

Cont…

- **Black hats:**
- Commit illegical acts with the intention of causing harm to the information system,steal information.
- **Gray hats:**
- Either good or bad
- Penetrated to the info system but doesn't harm.
- **White hats:**
- Posses knowledge and skills as black hats but work together with authorities or companies.

Types of Cyber Criminals:

1. Hackers: refer to anyone with **technical skills**, it typically refers to an individual who uses his or her **skills to achieve unauthorized access** to systems or networks so as to **commit crimes.**

- White hat attackers burgled networks or PC systems to get weaknesses so as to boost the protection of those systems.
- The owners of the system offer permission to perform the burglary, and they receive the results of the take a look at.
- On the opposite hand, black hat attackers make the most of any vulnerability for embezzled personal, monetary or political gain.
- hat attackers are somewhere between white and black hat attackers.
- Grey hat attackers could notice a vulnerability and report it to the owners of the system if that action coincides with their agenda.

White Hat Hackers

- These hackers utilize their programming **aptitudes for a good and lawful reason.**
- These hackers may perform network penetration tests in an attempt to compromise networks to discover network vulnerabilities.
- **Security vulnerabilities** are then reported to developers to fix them and these hackers can also work together as a blue team.
- They always use the limited amount of resources which are ethical and provided by the company, they basically perform pen testing only to check the security of the company from external sources

Gray Hat Hackers

- These hackers carry **out violations** and do seemingly deceptive things however **not for individual addition or to cause harm**.
- These hackers may disclose a vulnerability to the affected organization after having compromised their network and they may exploit it .

Black Hat Hackers

- These hackers are unethical criminals who **violate network security for personal gain.**
- They misuse vulnerabilities to bargain PC frameworks.
- These hackers always exploit the information or any data they got from the unethical pen testing of the network.

Organized Hackers:

- These criminals embody organizations of cyber criminals, hacktivists, terrorists, and state-sponsored hackers.
- Cyber criminals are typically teams of skilled criminals targeted on control, power, and wealth.
- These criminals are extremely subtle and organized, and should even give crime as a service.
- These attackers are usually profoundly prepared and well-funded.

Internet stalkers:

- Internet stalkers are people who **maliciously monitor** the web activity of their victims to **acquire personal data**.
- This type of cyber crime is conducted through the use of social networking platforms and malware, that are able to track an individual's PC activity with little or no detection.

Execution of cyber crime

- Cyber crimes associated with the **level of risk,associated cost and complexity.**
- Offenders intend to indulge in crime to **high profit.**
- Depending upon the impact of cybercrime executed ,it is executed as follows:

1. **Foreign intelligence services**:highly organized & sophisticated techniques.
2. **Large organized crime networks** :low risk with minimal investment.
3. **Disreputable but legitimate organization**:IP theft to obtain sensitive information.
4. **Individuals or small group of opportunistic cyber criminals**: target on particular person or organization.

Tools used in cybercrime

- Proxy servers
- Phishing
- Malware
- Spyware,keyloggers
- Virus and worm
- Trojan
- Dos attacks
- Rootkit
- Cracking
- Hijackware
- Pharming
- spoofing

social engineering

- Social engineering is a **manipulation technique** that exploits human error to **gain private information**, **access, or valuables**.
- In cybercrime, "**human hacking**" scams tend to unsuspecting users into **exposing data, spreading malware infections, or giving access to restricted systems**.
- Attacks can happen **online, in-person**, and via **other interactions**.

Characteristics (Traits)of Social Engineering Attack

- Social engineering attacks center around the attacker's use of persuasion
- **High emotions**: **Emotional manipulation** gives attackers the upper hand in any conversation.
- **Fear,Excitement,Curiosity,Anger,Crime,Sadness**
- Time-sensitive occasions or requests are other reliable tools in an attacker's arsenal.
- **Confidence(Trust):** Credibility is invaluable and necessary for a social engineering attack. If the attacker is lying to us, confidence plays an important role. They have done **enough research to prepare a narrative for us** that is **easy to believe** and is unlikely to **reduce suspicion.**

CONT….

- **Urgency:** **Time-sensitive** opportunities or requests are another reliable tool in an attacker's arsenal.
- You may be **motivated** to **compromise yourself** under the guise of a **serious problem** that needs **immediate attention**.
- Alternatively, you may be exposed to a prize or reward that may disappear if you **don't act** quickly.
- Either approach overrides your **critical thinking ability**.

Phases:

- There are 7 phases in a total of Social Engineering Attack.

1. **Identifying the goal:**
   First phase consists of Attack formulation and in accordance, **identifying target necessary** to fulfill goal.
2. **Information gathering**:
   social engineers assess and **identify potential information sources** and begin information gathering and assessment.
3. **Preparation**:
   social engineers **analyze information and develop an action plan and methodology** to begin approaching the target.
4. **Establishing a relationship**:
   establish a **line of communication and begin to build a relationship**.

5.Exploit the relationship –
The exploitation stage uses different methods of misleading to evoke right type of emotions and prime the target to right emotional stage.

6.Debrief:
social engineer returns to victim and **maintains desired emotional state**. The goal is that the victim will **not feel like** anything in relationship was **odd,** and they **will not understand that they have been under attack**.

7.Goal Satisfaction –
After a successful social engineering attack, they will **exploit information they have gathered.** the social engineer will either **return to the victim for more information or slowly close relationship.**

Risk in social engineering

- The attacks **don't have to work against everyone**.
- A **single** successfully fooled victim can provide enough information to trigger an attack that can **affect an entire organization**.
- Not only do **fake websites or emails** look realistic enough to fool **victims into revealing data** that can be used for **identity theft,** social engineering has also become one of the most common ways for attackers to breach an organization's initial defenses in order to cause further disruption and harm.

Protection against social engineering

- **Training** helps teach employees to **defend** against such attacks.
- **Password management**: Guidelines such as the **number and type** of characters that each password must include, how often a password must be changed, and even a simple rule that employees should not disclose passwords to anyone--regardless of their position--will help secure information assets.
- **Multi-factor authentication**: Authentication for high-risk network services such as **modem pools and VPNs(virtual)** should use **multi-factor authentication** rather than fixed passwords.
- **Email security with anti-phishing defenses**: **Multiple layers of email** defenses can **minimize the threat** of phishing and other social-engineering attacks. Some email security tools have anti-phishing measures built in.

Types of social engineering attacks

1. Phising
2. Watering hole attacks
3. Business email compromise attacks
4. Physical social engineering
5. USB baiting

Phishing:

- Phishing is a type of social engineering attack that involves sending an email or message that appears to be from a legitimate source, such as a bank, in an attempt to trick the recipient into revealing their login credentials or other sensitive information.

Watering hole attacks

- Watering hole attacks are a **very targeted** type of social engineering.
- An attacker will set a **trap** by compromising a website that is likely to be **visited** by a **particular group of people**, rather than targeting that group directly.
- An example is **industry websites** that are frequently visited by employees of a certain sector, such as **energy or a public service**.
- The perpetrators behind a watering hole attack will compromise the website and **aim to catch out an individual from that target group**.
- They are likely to carry out further attacks once that **individual's data or device has been compromised.**

Business email compromise attacks

- Business email compromise (BEC) attacks are a **form of email fraud**
- where the attacker masquerades as a C-level executive and attempts to trick the recipient into performing their business function,for an **illegitimate purpose**, such as **wiring them money**.
- Sometimes they go as far as **calling the individual and impersonating the executive.**

Physical social engineering

- When talking about cybersecurity, we also need to talk about the physical aspects of **protecting data and assets.**
- Certain people in your organization--such as help **desk staff, receptionists, and frequent travelers** are more at risk from physical social engineering attacks, which happen in person.
- Your organization should have effective physical security controls such as **visitor logs, escort requirements, and background checks**.
- Employees in positions at higher risk for social-engineering attacks may benefit from **specialized training** from physical social engineering attacks.

USB baiting

- USB baiting sounds a bit **unrealistic**, but it happens **more often** than our thinking.
- Essentially cybercriminals install **malware onto USB sticks** and leave them in strategic places, hoping that someone will **pick the USB up and plug it into a corporate environment**, thereby unwittingly **unleashing malicious code** into their organization.

Cyber war

- It is a web based battle intended to **attack computer** systems & network for **showing patriotism or revenge**.
- It targets **military,government** and **financial institutions** & IT industries.
- Prevented by **installing security updates**.
- Cyber war tool is a **logical tool**
- Tool are **open source** & they are categorized into **reconnaissance,scanning,acess,escalation,assault tools.**

- Cryptocurrency
- Bitcoin
- Etherum
- Blockchain
- Ransomware
- Deep web & dark web

Cryptocurrency

- not a type of currency -used to **perform transactions** only in the **digital world-**has to be **converted from a digital form** to some **existing currency** that is used in the real world.
- It is a **digital payment system** that does not rely on banks to verify transactions. Cryptocurrency payments exist purely as **digital entries to an online database.** When cryptocurrency funds are transferred, the transactions are recorded in a **public ledger**.
- Example: **Dollars, Rupees**, etc. Cryptocurrencies **don't have a central issuing authority** instead using a decentralized system to record transactions and issue new units.

Bitcoin

- Bitcoin is the most widely **accepted cryptocurrency** & still the most commonly traded. It is a decentralized digital currency that can be transferred on a **peer-to-peer bitcoin** network.
- It is an **innovative digital payment** system and the next big thing in finance.
- It is a **virtual currency designed to act as money and outside** the control of any person or group **thus eliminating the need for third-party in financial transactions.**
- It is used as a reward for the miners in bitcoin mining.
- It can be **purchased on several exchanges.**

Etherum

- **Etherum** is a **Blockchain network** that introduced a built-in Turing-complete programming language that can be used **for creating** various **decentralized applications**.
- The Etherum network is fueled by its **own cryptocurrency** called **'ether'.**

Ransomware

- Ransomware is a form of **malicious software** that prevents computer users from accessing their data by encrypting it.
- Cybercriminals use it to **extort money from individuals** or organizations whose data they have **hacked**, and **they hold the data hostage until the ransom is paid.**
- If the cybercriminals **do not pay the ransom within the specified time frame, the data may leak to the public or be permanently damaged**.
- One of the most **serious issues that business** face is ransomware.

Deep web

- It is the web which **cannot be accessed by the search engines**, like government private data, bank data, cloud data etc.
- These data are **sensitive and private**, kept out of reach.
- It is used to provide **access to a specific to a specific group of people**.

Dark web

- The Dark Web(Dark Net) is a network within the Internet which is **only accessible using certain software and protocols**.
- The Dark Web has many names, example: **Tor Network or Onion Router.**
- **Anyone** can **access** to the Dark Web by simply **downloading software** for it. A popular and very much used browser is the Tor Project's Tor Browser
- just like any other browser such as Google Chrome or Microsoft Edge, except it can also access special website addresses which **ends in .onion instead of .com**.
- Any traffic sent through Tor Browser is **automatically anonymized** and **encrypted** via many different hosts.
- The browser also has **built-in protection** for many kinds of **tracking** and de-anonymization features.

UNIT-2

CYBER SECURITY

TOPICS

- Unauthorized Access to Computers, Computer Intrusions, White collar Crimes, Viruses and Malicious Code, Internet Hacking and Cracking, Virus Attacks, Pornography, Software Piracy, Intellectual Property, Mail Bombs, Exploitation, Stalking and Obscenity in Internet, Digital laws and legislation, Law Enforcement Roles and Responses

CYBER SECURITY

- Cyber Security is the set of principles and practices designed to **protect our computing resources** and **online information** against threats.
- It is all about **reducing threats** when people are in the process of **dealing with technology.**
- It encompasses the full range of protection **against any online risk or vulnerability,** which comprises information security assurance and cyber law enforcement.
- It is the **protection of cyber-space** (which includes hardware, software, networks, and their servers, peripheral devices, data and information, and all other components associated with technology) and internet-connected systems from **both internal as well as external threats and cybercriminals**.

Types of cyber security

Every organization's assets are the combinations of a **variety of different systems**.

These systems have a strong cybersecurity posture that requires coordinated efforts across all of its systems.

categorize cybersecurity in the following sub-domains:

Network Security

- It involves implementing the **hardware and software** to **secure** a computer network from **unauthorized access**, intruders, attacks, disruption, and misuse.
- This security helps an organization to protect its assets **against external and internal threats.**

Application Security

- It involves protecting the **software** and devices from unwanted threats.
- This protection can be done by **constantly updating** the apps to ensure they are **secure from attacks**.
- Successful security begins in the design stage, writing source code, validation, threat modeling, etc., **before** a program or device is **deployed.**

- **Information or Data Security:** It involves **implementing a strong data storage mechanism** to maintain the **integrity and privacy** of data, both in storage and in transit.
- **Identity management:** It deals with the procedure for **determining** the **level of access** that each **individual** has within an organization.
- **Operational Security:** It involves **processing and making decisions** on handling and securing data assets.

Cont….

- **Mobile Security:** It involves securing the **organizational and personal data stored on mobile devices** such as cell phones, computers, tablets, and other similar devices against various malicious threats. Ex: **threats are unauthorized access, device loss or theft, malware, etc.**
- **Cloud Security:** It involves in **protecting the information stored in the digital environment or cloud architectures** for the organization. It uses various cloud service providers such as AWS, Azure, Google, etc., to ensure security against multiple threats.

Cyber Security Goals

- main **objective is to ensure data protection**.
- The security community provides a **triangle of three** related principles to **protect the data** from cyber-attacks.
- This principle is called the **CIA triad**. The CIA model is designed to guide policies for an organization's **information security infrastructure**.
- When any security breaches are found, one or more of these principles has been violated.
- We can break the **CIA model into three parts**: **Confidentiality, Integrity, and Availability.** It is actually a security model that helps people to think about various parts of IT security.

1.Confidentiality

- Confidentiality is equivalent to privacy that **avoids unauthorized access** of information.
- It involves ensuring the data is **accessible** by those who are **allowed to use it** and **blocking access** to others.
- It **prevents essential information** from reaching the wrong people.
- **Data encryption** is an excellent example of ensuring confidentiality.

2.Integrity

- This principle ensures that the data is **authentic, accurate, and safeguarded** from **unauthorized** modification by threat actors or accidental user modification.
- If any modifications occur, certain measures should be taken to **protect the sensitive data from corruption or loss** and **speedily recover** from such an event.
- It indicates to make the **source of information genuine**.

3. Availability

- This principle makes the information to be **available and useful for its authorized people always**.
- It ensures that these accesses are **not hindered by system malfunction or cyber-attacks.**

Challenges of Cybersecurity

1.Constantly Evolving Threat Landscape:

Cyber threats are constantly evolving, and attackers are **becoming increasingly sophisticated.**

This makes it challenging for cybersecurity professionals to keep up with the **latest threats and implement effective measures to protect against them**.

2.Lack of Skilled Professionals:

There is a **shortage of skilled cybersecurity professionals**, which makes it difficult for organizations to find and **hire qualified staff to manage** their **cybersecurity** programs.

3.Limited Budgets:

Cybersecurity can be expensive, and many organizations have **limited budgets to allocate towards cybersecurity initiatives.**

This can result in a **lack of resources and infrastructure** to effectively protect **against cyber threats**.

4.Insider Threats:

- threats can be just as **damaging as external threats**.
- Employees or contractors who have access to sensitive information can intentionally or unintentionally **compromise data security**.

5.Complexity of Technology:

With the rise of cloud computing, IoT, and other technologies, the **complexity of IT infrastructure** has increased significantly.

This complexity makes it **challenging to identify and address vulnerabilities and implement effective cybersecurity measures**.

Strategies for Addressing Cybersecurity Challenges

1.Comprehensive Risk Assessment:

A comprehensive risk assessment can help organizations identify potential vulnerabilities and **prioritize cybersecurity initiatives** based on their **impact and likelihood.**

2.Cybersecurity Training and Awareness:

Cybersecurity training and awareness programs can help employees understand the **risks** and **best practices** for **protecting** against cyber threats.

3.Collaboration and Information Sharing:

Collaboration and information sharing between organizations, industries, and government agencies can help **improve cybersecurity strategies and response to cyber threats.**

4.Cybersecurity Automation:

Cybersecurity automation can help organizations **identify and respond** to threats in real-time, reducing the risk of data breaches and other cyber attacks.

5.Continuous Monitoring:

Continuous monitoring of IT infrastructure and data can **help identify potential threats and vulnerabilities,** allowing for **proactive measures** to be taken to prevent attacks.

White-collar crimes

- White-collar crimes refer to the **non-violent, illegal activities** that are committed by individuals or businesses for financial gain or **personal gain.**
- **Examples** : **bribery**, insider trading, cybercrime, **credit card fraud**, **copyright infringement** ETC..
- The white-collar criminals can cause **massive** damage to society .
- crime is **non-violent** and especially motivated towards **financial gain** then it becomes a White-collar cybercrime.

Examples of White-collar cybercrimes

- **Credit-card fraud:** This refers to stealing another person's credit-cards details to make purchases.
- **Identity Theft:** This involves assuming another person's identity information such as name, address, date of birth, or Aadhaar number to commit financial fraud. Fake passports and Fake IDs are commonly used to commit crimes and evade captures.
- **Computer Intrusion:** It is one of the most common white-collar cybercrime that occurs instantly on the Internet. It involves accessing of computer or internet without having proper authorization. Hackers attack and try to obtain personal information for monetary benefits.
- **Insider Trading:** This involves using non-public information to make investment decisions or trading securities for personal financial gain.

- **Cyberstalking and Harassment:** This refers to using digital technologies to stalk or harass individuals, such as sending threatening emails or messages, spreading false rumors, or posting private photos or videos online without consent.
- **Intellectual Property Theft:** This involves stealing or copying copyrighted materials, such as software, music, or films, for personal financial gain.
- **Ransomware Attacks:** This involves using malware to encrypt an individual's or organization's data and demanding payment in exchange for the decryption key.
- **Cyberbullying:** This refers to using digital technologies to bully, harass, or intimidate individuals, such as through social media, messaging apps, or online forums.

Computer Intrusions

- **Unauthorized access** to your computer or **illegal entry** .
- Computer intrusions occur when someone tries to **gain access** to any part of your computer system.
- Computer i**ntruders** or hackers typically use automated computer programs when they try to **compromise** a **computer's security**.
- There are several ways an intruder can try to gain access to your computer. They can:

1. Access your computer to **view, change, or delete** information on your computer.
2. **Crash or slow down** your computer.
3. **Access** your **private** data by **examining the files** on your system.
4. Use your computer **to access other** computers on the Internet.

Malicious Code

- Malicious code- malware, is a type of computer code that is designed to **cause damage** to a computer system or **network**.
- It is a form of cyber attack that is used to gain unauthorized access to a system or network, steal data, or **disrupt the normal functioning** of the system.
- Malicious code can **be spread** through **email, websites, and other online sources,** and can be used to launch a variety of attacks, including **denial of service, data theft, and identity theft**.
- Malicious code can also be used to spread viruses, worms, and other malicious software.

Types of Malware

- **Viruses –** Attach itself to program and propogates copies of itself to other programs. Once a program virus is active, it will infect other programs on the computer.
- **Worms –** Worms replicate themselves on the system, attaching themselves to different files and looking for pathways between computers, such as computer network that shares common file storage areas. Worms usually slow down networks. A virus needs a host program to run but worms can run by themselves. After a worm affects a host, it is able to spread very quickly over the network.
- **Trojan horse –** A Trojan horse is malware that carries out malicious operations under the appearance of a desired operation such as playing an online game. A Trojan horse varies from a virus because the Trojan binds itself to non-executable files, such as image files, and audio files.
- **Ransomware** – Ransomware grasps a computer system or the data it contains until the victim makes a payment. Ransomware encrypts data in the computer with a key that is unknown to the user. The user has to pay a ransom (price) to the criminals to retrieve data. Once the amount is paid the victim can resume using his/her system
- **Adware** – It displays unwanted ads and pop-ups on the computer. It comes along with software downloads and packages. It generates revenue for the software distributer by displaying ads.

Cont…

- **Spyware** – Its purpose is to steal private information from a computer system for a third party. Spyware collects information and sends it to the hacker.
- **Logic Bombs –** A logic bomb is a malicious program that uses a trigger to activate the malicious code. The logic bomb remains non-functioning until that trigger event happens. Once triggered, a logic bomb implements a malicious code that causes harm to a computer. Cybersecurity specialists recently discovered logic bombs that attack and destroy the hardware components in a workstation or server including the cooling fans, hard drives, and power supplies. The logic bomb overdrives these devices until they overheat or fail.
- **Rootkits –** A rootkit modifies the OS to make a backdoor. Attackers then use the backdoor to access the computer distantly. Most rootkits take advantage of software vulnerabilities to modify system files.
- **Backdoors** – A backdoor bypasses the usual authentication used to access a system. The purpose of the backdoor is to grant cyber criminals future access to the system even if the organization fixes the original vulnerability used to attack the system.
- **Keyloggers –** Keylogger records everything the user types on his/her computer system to obtain passwords and other sensitive information and send them to the source of the keylogging program.

Internet Hacking and Cracking

- **Hacking** may be defined as the **technique** or planning which is done to get **access to unauthorized** systems.
- gaining access to a network or a computer for **illegal purposes**.
- **Cracking** means trying to get into computer systems in order to steal, corrupt, or illegitimately view data.
- That person is exceptionally intelligent and proficient with computers. The skilled person in hacking is divided into two categories:
- **Hackers**
- **Crackers**

Difference between Hackers and Crackers

HACKER	CRACKER
The good people who hack for **knowledge** purposes.	The evil person who breaks into a system for **benefits.**
They are skilled and have advanced knowledge of **computers OS and programming languages.**	They may or may not be skilled, some crackers just know a **few tricks to steal data.**
They work in an organization to help **protect** their data and give them **expertise** in internet security.	These are the person from which hackers **protect individual organizations.**
Hackers share the knowledge and **never damages** the data.	If they found any **loophole** they just delete the data or **damages** the data.
Hackers are the **ethical professionals**.	Crackers are **unethical** and want to benefit themselves from illegal tasks.
Hackers program or hacks to check the **integrity and vulnerability strength** of a network.	Crackers **do not make new tools** but use someone else tools for their **cause and harm** the network.
Hackers have legal certificates with them e.g **CEH certificates**.	Crackers may or may not have certificates, as their motive is to stay anonymous.
They are known as **White hats** or saviors.	They are known as **Black hats** or evildoers.

Cyber Pornography

- Cyber Pornography means the **publishing, distributing** or designing pornography by using cyberspace.
- The technology has its pros and cons and cyber pornography is the result of the advancement of technology.
- With the easy availability of the Internet, people can now view thousands of porn on their mobile or laptops, they even have access to upload pornographic content online.

Scope of cyber security

- monitoring security access and will also conduct **internal and external audits** to ensure there are no potential threats to network securities. Following jobs are available by gaining knowledge in cyber security
- **Cyber Security Analyst**
- **Security Architect**
- **cyber Security Manager**
- **Chief Information Security Officer**
- **Network Security Engineer**
- **Ethical Hacker**
- **Cloud Security Engineer**
- **Incident Response Manager**
- **Cybersecurity Consultant**

https://www.careerera.com/blog/the-future-scope-of-cyber-security-in-india

Software Piracy

- It is the **illegal** approach of **copying, distributing, modifying, selling,** or using the software which is legally protected.
- It is the act of **stealing legal software** in an **illegal way**.
- This software piracy refers to the unauthorized copy and **use of legal software.**
- This critical problem has turned into a **global issue** now.
- **End-User License Agreement**(EULA) is a license agreement which is mostly used for software to **protect its legality.**

1.Softlifting:

- In this the **legal** owner of the software is **one**, but the **users** are **multiple.**
- someone purchases the **genuine software**, and others will **illegally use** that software by downloading the software to their computer.
- ex: many times we **borrow** the software from our colleague and install a **copy** of that on our computer just to save the money which rises to softlifting one type of software piracy.

2.Hard-disk Loading

- It mainly happens in **PC resell** shops.
- The shop owner buys a **legal copy** of the software and reproduces its copies in multiple computers by installing it.
- Most of the time **customers/PC users** are **not aware** of these things and get the pirated version of the software in the original S/W price or **less than the original price**.
- It is one type of **Commercial software privacy**.

3.Counterfeiting-

- In this **duplicates** are created of **genuine/legal** software programs with the appearance of authenticity.
- Then these **duplicate software** are sold out at **less price**.

4. Client-Server overuse

- In this **more copies** of the **software are installed** than it has licensed for.
- Mainly it has seen in local business sectors when they work under a local area n/w and install the software in all the computers for use by a number of employees which is an unauthorized practice.

5.Online Piracy

- The illegal software is acquired from online auction sites and blogs which is mainly achieved through the **P2P**(Peer to Peer) **file-sharing system.**
- As it is acquired by means of the Internet, often it is called **Internet Piracy.**

Intellectual Property Rights

- Intellectual property rights are the **legal rights** that cover the privileges given to individuals who are the owners and inventors of a work, and have created something with their intellectual creativity.
- Individuals related to areas such as literature, music, invention, etc., can be granted such rights, which can then be used in the business practices by them.
- It is important to stimulate and promote research and development.

Types of IPR

The 4 main types of intellectual property are listed below.

- **Patents** – It is used for protecting new inventions, ideas, or processes. Patent holders need to pay periodic government renewal fees. An approved patent is for a limited time period. Know more about Patents Act in India.
- **Copyrights** – It protects the ideas, examples would be written works, music, art, etc.
- **Trademarks** – It is something that protects the symbols, colors, phrases, sounds, design etc.
- **Trade Secrets** – It may be strategies, systems, formulas, or other confidential information of an organization that provides them a competitive advantage in the market.

Advantages of Intellectual Property Rights

- It provides exclusive rights to the creator's or inventor's.
- It gives freedom to inventor to share his knowledge without keeping its secret.
- It helps to creator financially.
- It provides legal defence to the creator.

MAIL BOMB

- A mail bomb is a form of a **denial-of-service (DoS)** attack designed to **overwhelm an inbox** or inhibit a server by sending a **massive number of emails** to a specific person or system.
- The aim is to fill up the recipient's disk space on the server or overload a **server to stop it from functioning**.
- The damage caused by a mail bomb can range from a **minor inconvenience** to a **total disruption** of **services.**
- Mail bomb attacks are usually initiated **intentionally or unintentionally** by a **botnet**, a **single** actor or a **group of actors**

Types of mail bomb attacks

- **Attachment.** An attachment attack occurs when **multiple emails** with large **attachments** are sent.
  - They are designed to **overload server storage space quickly** and render it unresponsive.
- **List linking.** A list linking attack is a tactic used by threat actors to sign up **targeted emails** to **multiple email subscription services**.
  - The goal is to flood email addresses indirectly with **subscribed content**.
  - This is possible because many **subscription services** do **not require verification**.
  - If they did, the **verification emails** could be used as a **list linking mail bomb attack.**
  - It is difficult to **defend against** list linking attacks because the **traffic originates from legitimate sources.**

- **Mass mailing.** Mass mailing is a type of mail bomb that is **not always intentional.**
  - Ex: instead of clicking on one email address, a user may accidentally select all and **mistakenly send** the email to **hundreds or thousands of targeted** email addresses.
    - **Intentional** mass mail bombs are often initiated by using **botnets or malicious scripts.**
    - For example, threat actors can automate the filling of **online forms with the target email address as the requesting/return address.**

- **Reply all:**
  - When a user responds by clicking Reply All to an extensive list of email addresses instead of just the original sender, inboxes are flooded with emails.
  - Automated replies, such as out-of-office messages, often compound these emails.
  - Often, reply-all mail bombs are accidental rather than an email bomb attack.
  - However, threat actors can spoof email addresses and **related automatic replies and direct them to spoofed addresses.**
- **Zip bomb.**
  - A zip bomb, also known as a **decompression bomb** or **zip *of death attack***,
  - It is a large and compressed archive file sent to an email address that, when **decompressed**, **consumes available server resources and impacts server performance.**

- To defend against or prevent mail bombs, organizations must enforce security policies that address **user behavior** and **technical processes**.

Cyber Stalking

- cyberstalking is a general term for **online harassment**.
- Cyberstalking is a crime in which someone harasses or stalks a victim **using electronic or digital** means, such as social media, email, instant messaging (IM), or messages posted to a discussion group or forum.
- Cyberstalkers take advantage of the anonymity afforded by the internet to stalk or harass their victims, sometimes **without being caught, punished or even detected.**

Prevent Cyberstalking

- Make Security a Priority
- Create strong passwords.
- Be sure to log out every time
- Keep track of your devices
- Use caution on public wi-fi
- Practice online safety habits

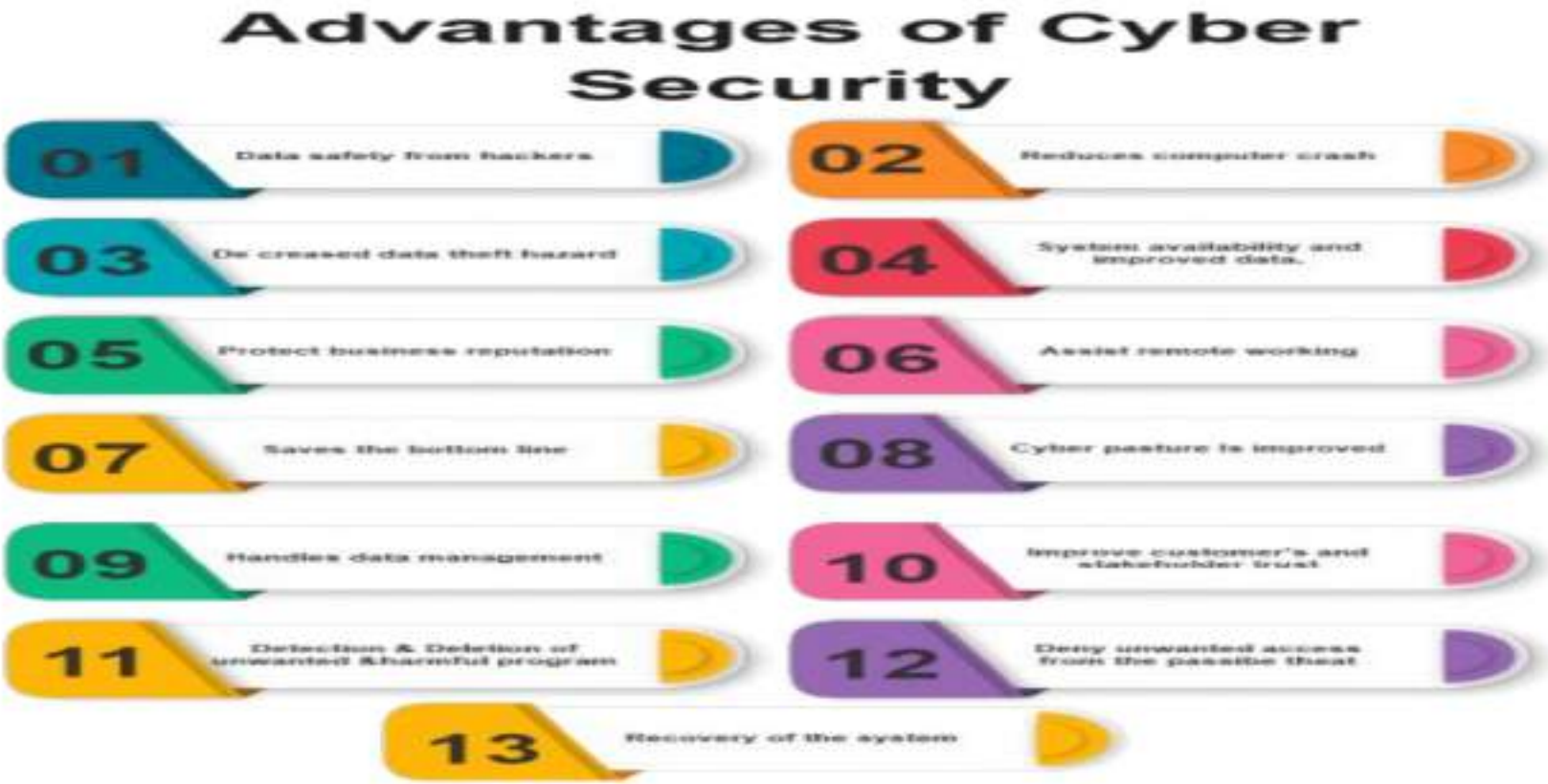
Types of Cyberstalking

- The three most common types of cyber stalking are as follows:
- **Email stalking:** This type of stalking involves the **sender sending** hateful, obscene, or **threatening emails** to the **recipient**. Sometimes the attacker may also include **viruses and spam in the email**.
- **Internet stalking:** This type of stalking occurs when an individual **spreads rumors or tracks victims** on the internet. The goal of spreading rumors is to slander the victim.
- **Computer stalking:** This type of stalking occurs when an individual hacks into a victim's computer and **takes control of it**. This requires advanced computer skills however, one can find guidelines on the web.

Difference between Cyberstalking and Cyberbullying

- **Cyberstalking** occurs when a victim is harassed online via electronic channels, text messaging, social networking sites, discussion forums, and so on for retaliation, anger, or control. A stalker could be a stranger or a friend of the victim. **When adults are involved, it is referred to as cyberstalking.**
- ***Cyberbullying*** occurs when a **child or a teenager** is mistreated, disrespected, tormented, intimidated, humiliated, or **aimed at by another individual of the same age range** via the internet.

ADVANTAGES OF CYBER SECURITY



ADVANTAGES OF CYBER SECURITY

- Data safety from hackers
- Reduces computer crash
- Decreased data theft hazard
- System availability and improved data
- Protect business reputation
- Assist remote working
- Handles data management
- Improve customer's and stakeholders' trust
- Detection and deletion of unwanted and harmful programs
- Deny unwanted access from the possible threat
- Recovery of the system

DISADVANTAGES OF CYBER SECURITY

- Not affordable to everyone
- Can be complicated
- Security patches may backfire
- Need of constant monitoring
- Slow down the system
- Can be risky
- Incorrect configured system blocks firewall
- Only some updations are suitable for the system

Cyber law

- Cyber law, also known as **Internet Law**
- It is the part of the overall **legal** system that is related to legal informatics and **supervises the digital circulation** of **information**, e-commerce, software and information security.
- It is associated with legal informatics and electronic elements, including **information systems, computers, software, and hardware.**
- It covers many areas, such as **access to and usage of the Internet, encompassing various subtopics** as well as freedom of expression, and online privacy.
- Cyber Laws yields **legal recognition to electronic documents** and a structure to support e-filing and e-commerce transactions and also provides a legal structure to reduce cyber crime.

Need of cyber law

- There are many security issues with using the Internet and also available different **malicious people** who try to **unauthorized access** your computer system to perform potential fraud.
- cyber law is created to **protect online organizations** and people on the network from unauthorized access and malicious people.
- If someone does any **illegal activity or breaks the cyber rule**, it offers people or organizations to have that persons **sentenced to punishment** or take action against them.

Importance of Cyber Law:

- When users apply transactions on the Internet, cyber law covers **every transaction and protect** them.
- It touches every **reaction and action** in **cyberspace**.
- It captures **all activities** on the **Internet.**

Areas(Roles) involving in Cyber Laws

- There are various broad categories that come under cyber laws; some are as follows:
- **Fraud**
- **Copyrighting Issues**
- **Scam/ Treachery**
- **Freedom of Speech**
- **Contracts and Employment Law**
- **Defamation**

Fraud

- Cyber laws are formed to prevent **financial crimes** such as **identity theft, credit card theft** and other that occurring **online**.
- A person may face confederate or state criminal charges if he commits any type of identity theft.
- These laws have explained **strict policies** to prosecute and defend **against allegations** of using the internet.

Copyrighting Issues

- The Internet is the source that contains different types of data, which can be **accessed anytime, anywhere**.
- But it is the **authority of anyone** to copy the content of any other person.
- The **strict rules** are defined in the cyber laws if anyone goes against copyright **that protects the creative work of individuals** and companies.

Scam/ Treachery

- There are different frauds and scams available on the Internet that can be personally harmful to any company or an individual. Cyber laws offer many ways to **protect** people and **prevent** any identity theft and financial crimes that happen online. **Online Harassment and Stalking**
- Harassment is a big issue in cyberspace, which is a **violation of both criminal laws and civil.** In cyber laws, there are some **hard laws** defined to **prohibit** these kinds of **despicable crimes**.

Contracts and Employment Law

- For every website, there are **terms and conditions** available that are associated with **privacy concerns**.
- When you are visiting a website, you click a button that gives a message to ask you to agree for terms and conditions;
- if you **agree** with it, that **ensures** you have **used cyber law**.

Trade Secrets

- There are many organizations that are doing **online business**, which are often **relying** on cyber laws to protect their trade secrets.
- For example, online search engines like Google spend much time to **develop the algorithms that generate a search result.**
- They also **spend lots of time developing** other **features** such as intelligent assistance, flight search services, to name a few and maps.
- Cyber laws help these organizations to perform **legal action by describing necessary legal laws for protecting their trade secrets**.

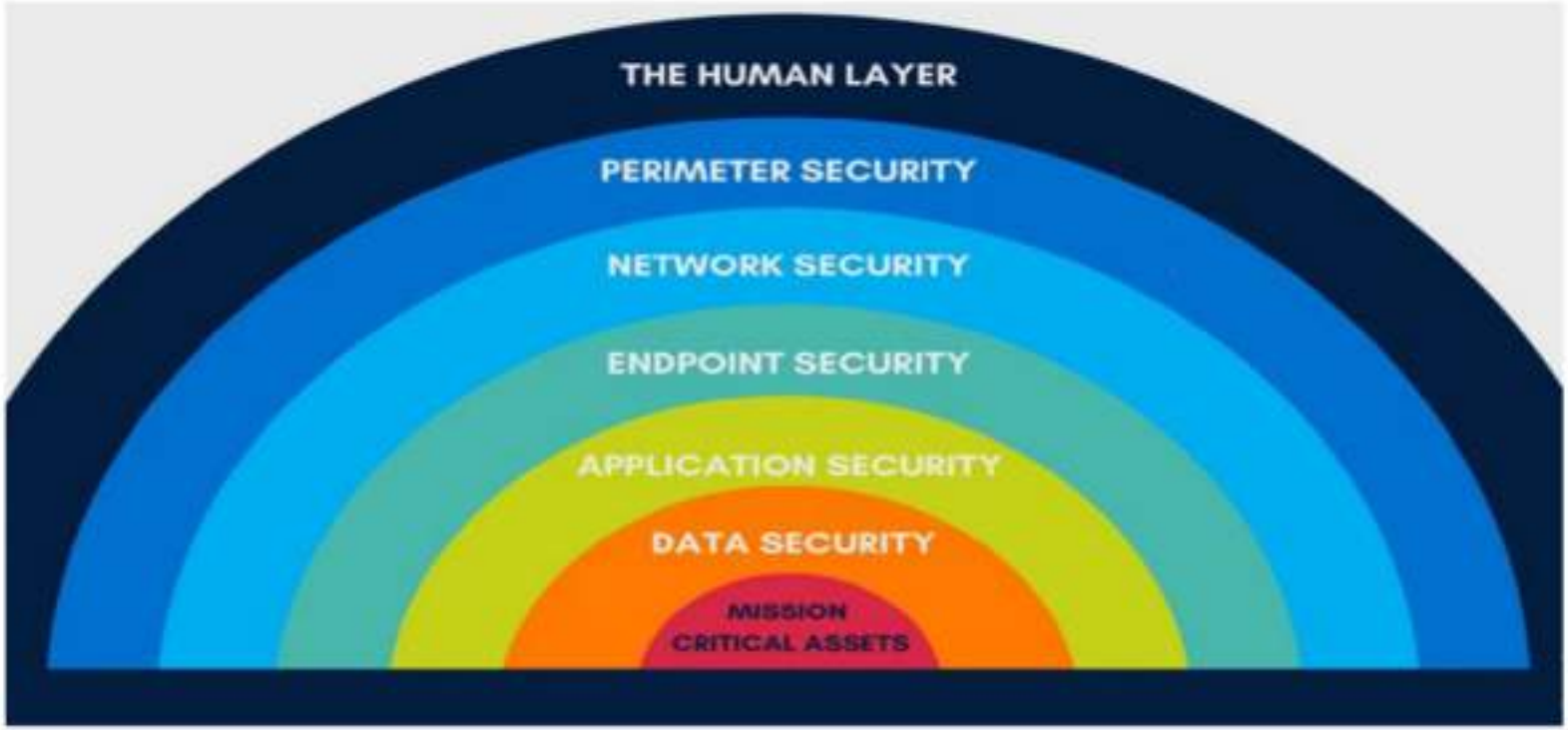
Advantages of Cyber Law:

- **Protecting personal information** – It helps to ensure that our **sensitive personal information**, such as our financial and medical records, are **kept secure online**.
- **Combatting cybercrime** –It helps to **detect and punish** those who **engage in illegal activities** on the internet, such as hacking and identity theft
- **Promoting fair competition** –It helps to level the playing field for businesses by **prohibiting unfair practices** such as **cyber espionage(SPY) and false advertising.**
- **Facilitating e-commerce** –It helps to **establish rules and regulations** for buying and selling goods and services online, **making it easier** and safer for consumers to make transactions.

Disadvantages of Cyber Law:

- **Complexity and confusion** – Cyber law can be **difficult to understand and apply**, leading to **confusion** for individuals and businesses trying to comply with it.
- **Limited jurisdiction** – Cyber law can only be **enforced within the borders** of a particular country, making it **challenging to address cross-border cyber issues**.
- **Encroachment on civil liberties** – Some argue that cyber law may infringe upon civil liberties, such as **freedom of speech and privacy, in the name of protecting national security or public order.**
- **Slowing down innovation** – Cyber law may **impose burden some regulations on new technologies and innovations,** stifling their development and adoption.
- **Lack of universal standards** – There is currently a **lack of universally agreed** upon cyber laws, leading to discrepancies and conflicts between different countries' legal systems.

LAYERS OF CYBER SECURITY



LAYERS OF CYBER SECURITY

- The 7 layers of cybersecurity should center on the mission critical assets you are seeking to protect.
- 1.**Mission Critical Assets** – This is the data you **need to protect**
- 2.**Data Security** – Data security **controls protect the storage and transfer of data**.
- 3.**Application Security** – Applications security controls protect access to an application, an application's access to your mission critical assets, and the internal security of the application.
- 4.**Endpoint Security** – Endpoint security controls protect the connection between devices and the network.
- 5.**Network Security** – Network security controls protect an organization's network and prevent unauthorized access of the network.
- 6.**Perimeter Security** – Perimeter security controls include both the physical and digital security methodologies that protect the business overall.
- 7.**The Human Layer** – Humans are the weakest link in any cybersecurity posture. Human security controls include phishing simulations and access management controls that protect mission critical assets from a wide variety of human threats, including cyber criminals, malicious insiders, and negligent users.

1: Mission critical assets

- This is data that is **absolutely critical to protect.** Whether businesses would like to admit it or not, they face malicious forces daily.
- An example of mission-critical assets in the **Healthcare industry** is **Electronic Medical Record** (EMR) software.
- In the financial sector, its customer's financial records
- This is your data equivalent of the Crown Jewels. Anything that your **business can't survive without, software, hardware, financial records**, etc.

2.Data layer

- This is the **first target** for a **cyber criminal** and needs to get **your full attention.**
- Depending on your business, this will include **client information, payment details, sensitive data and IP.**
- Losing this data **will** impact your business.
- Use encryption, regularly back up your data, have authentication systems in place and tight policies and procedures. If you don't have these, ILUX can **help**
- Data security is to protect both the **transfer** and the **storage of data**. There has to be a **backup security** measure in place to **prevent the loss of data**, This will also require the **use of encryption** and archiving.
- Data security is an important focus for all businesses as a breach of data can have consequences.

3.Application layer

- This covers the software and apps that we use. Our day-to-day operations would be virtually impossible without applications including **Microsoft Office, Teams, Zoom**, etc. These must be **secure.**
- **Update software regularly** with the latest versions as these will include extra security measures.
- This involves the security features that control access to an application and that application's access to your assets. It also includes the **internal security of the app itself.**
- Most of the time, **applications are designed with security measures** that continue to **provide protection** when the app is in use.

4.End Point layer

- This is **any device that is connected to our network**. This is often a large number, particularly with the development of hybrid working. You will need robust measures to that **every** device is secure.
- End-to-end encryption key. Managing your **mobile devices is also a critical part of end point security. MDM (Mobile Device Management**) means you can restrict access to any device and manage all the devices remotely
- This layer of security makes sure that the endpoints of user devices are not exploited by breaches. This includes the protection of **mobile devices, desktops, and laptops.**
- Endpoint security systems enable protection **either** on a **network** or in the **cloud depending on the needs of a business**.

5. Network Security

- The layer also deals with **connected devices and the activities** you and your staff team do once they are on your system.
- Only **give access** that is **enough for each person to do their job**. If you limit access where possible, any potential damage is contained to the **individual rather than your whole system**.
- This is where security controls are put in place to protect the business's network. The goal is to **prevent unauthorized access to the network.**
- It is crucial to regularly update all systems on the business network with the necessary security patches, including encryption. It's always best **to disable unused interfaces** to further guard against any threats.

6. Perimeter Security

- This is the **outer layer** of your network where all your devices sit (both onsite and from home) including wireless connections. With the development of IoT (Internet of Things) devices.
- Know where your **perimeter ends** and what **devices are connected, both onsite or if you are working from home, and what critical data is passing through these systems**. Make sure all the devices are secure (or **contact us** and we can run a free test for you).
- This security layer ensures that both the **physical and digital security** methods protect a business as a whole. It includes things like **firewalls** that protect the business network against external forces.

7. The Human Layer

- Despite being known as the **weakest link** in the security chain, the human layer is **a very necessary** layer. It incorporates management controls and phishing simulations as an example.
- These human management controls aim to protect that which is most critical to a business in terms of security. This includes the **very real threat that humans, cyber attackers, and malicious users pose to a business.**
- Arguably the most important layer of defence from a potential attack, that typically manifests as:
- a **spam email** that makes it to your inbox, generally asking you to input personal information, make a payment or open an unverified attachment
- a **phone call** asking for some personal/company details
- a **text message** inciting a response that would contain sensitive information
- Cyber criminals will even try and impersonate key people within the organisation to gain your trust, but you or your staff are not communicating with who you think you are.

Cyber Security Tools

Cyber Security Tools

1. Firewalls

- The firewall is the **core of security tools**, and it becomes one of the **most important** security tools.
- Its job is to **prevent unauthorized access** to or from a private network. It can be implemented as hardware, software, or a combination of both.
- The firewalls are used to prevent unauthorized internet users from accessing private networks connected to the Internet.
- All messages are **entering or leaving the internet pass** through the firewall.
- The firewall examines each message and blocks those messages that do not meet the specified security criteria.
- The Firewall is very useful, but it has **limitations also**. A **skilled hacker** knew how to create data and programs that are believing like trusted firewalls.
- Despite these limitations, firewalls are still very useful in the **protection of less sophisticated malicious attacks** on our system.

2. Antivirus Software

- Antivirus software is a **program** which is designed to **prevent, detect, and remove viruses and other malware attacks** on the **individual computer, networks, and IT systems.**
- It also protects our computers and networks from the variety of **threats and viruses** such as Trojan horses, worms, key loggers, browser hijackers, rootkits, spyware, botnets, adware, and ransomware.
- Most antivirus program comes with an **auto-update feature** and enabling the system to check for new viruses and threats regularly.
- It provides some additional services such as **scanning emails** to ensure that they are **free from malicious attachments** and web links.

PKI

- PKI stands **for Public Key Infrastructure**.
- This tool supports the **distribution and identification** of **public encryption keys.**
- It enables users and computer systems to **securely exchange data** over the internet and **verify the identity** of the **other party**.
- It is the technology which **encrypts** the **server communication** and is responsible for HTTPS that we can see in our **browser address bar**.
- PKI solve many numbers of **cybersecurity problems** and deserves a place in the organization security suite.

PKI also used in

- Enable Multi-Factor **Authentication** and **access control**
- Create compliant, **Trusted Digital Signatures**.
- Encrypt email communications and **authenticate the sender's identity.**
- **Digitally sign** and protect the code.
- Build identity and trust into **IoT ecosystems.**

Managed Detection and Response Service (MDR)

- **The managed detection and response has the following characteristics:**
- MDR also uses **Artificial Intelligence** and **machine learning** to **investigate**, **auto detect threats,** and **orchestrate response** for faster result.
- Managed detection and response is focused on threat detection, rather than compliance.
- MDR relies heavily on **security event management** and **advanced analytics.**
- While some **automation** is used, MDR also involves **humans to monitor our network.**
- MDR service providers also perform **incident validation and remote response**

5. Penetration Testing

- Penetration testing, or **pen-test**, is an important way to **evaluate our business's security** systems and security of an **IT infrastructure** by safely trying to **exploit vulnerabilities**.
- These vulnerabilities exist in **operating systems, services and application, improper configurations or risky end-user behavior.**
- In Penetration testing, cybersecurity professionals will use **the same techniques** and processes utilized by **criminal hackers to check for potential threats** and areas of weakness.
- A pen test attempts the password cracking, code injection, and phishing. It involves a simulated real-world attack on a network or application.
- This tests can be performed by **using manual or automated technologies** to systematically **evaluate servers, web applications, network devices, endpoints, wireless networks, mobile devices** and other potential points of vulnerabilities.
- Once the pen test has successfully taken place, the testers will present us with their **findings threats** and can help by recommending potential changes to our system

6.Staff Training

- Staff training is **not a 'cybersecurity tool'** but ultimately, having **knowledgeable employees** who understand the cybersecurity which is one of the **strongest forms of defense** against cyber-attacks.
- Today's many training tools available that can **educate company's staff** about the best cybersecurity practices.
- Every business can organize these training tools to educate their employee who can **understand their role in cybersecurity**.

UNIT-3

DIGITAL FORENSICS

TOPICS

- Introduction to Digital Forensics- Forensic Software and Hardware,-Analysis and Advanced Tools,-Forensic Technology and Practices-Forensic Ballistics and Photography-Face, Iris and Fingerprint Recognition- Audio Video Analysis, Windows System Forensics, Linux System Forensics, Network Forensics

Introduction to Digital Forensics

- Digital Forensics is defined as the process of **identification, extraction, preservation, and documentation** of computer evidence which can be used by the court of law.
- It is a science of **finding evidence from digital media** like a computer, mobile phone, server, or network.
- It provides the **forensic team** with the **best techniques** and **tools** to **solve complicated digital-related** cases.
- It helps the forensic team to **analyzes, inspect, identifies, and preserve the digital evidence** residing on various types of electronic devices

Process(CHARACTER) of Digital forensics

Cont....

1.Identification

- It is the **first** step in the forensic process. The identification process mainly includes things like **what evidence is present, where it is stored**, and lastly, **how it is stored (in which format).**
- Electronic storage media can be personal computers, Mobile phones, PDAs, etc.

2.Preservation

data is **isolated, secured, and preserved**. It includes **preventing people from using the digital device** so that digital evidence is **not tampered** with.

3.Analysis

- In this investigation agents **reconstruct fragments of data and draw conclusions based on evidence** found. However, it might take **numerous iterations** of examination to support a specific crime theory.

4.Documentation

- In this process, a **record of all the visible data** must be **created**. It helps in **recreating the crime scene and reviewing** it.
- It Involves proper documentation of the crime scene along with **photographing, sketching,** and **crime-scene mapping**.

5.Presentation

- In this last step, the process of **summarization** and **explanation** of conclusions is done.
- However, it should be written in a layperson's terms using **abstracted terminologies**. All abstracted terminologies should reference the specific details.

Different types of digital forensics

1. **Computer Forensics** – the identification, preservation, collection, analysis and reporting on evidence found on computers, laptops and storage media in support of investigations and legal proceedings.
2. **Network Forensics** – the monitoring, capture, storing and analysis of network activities or events in order to discover the source of security attacks, intrusions or other problem incidents, i.e. worms, virus or malware attacks, abnormal network traffic and security breaches.
3. **Mobile Devices Forensics** – the recovery of electronic evidence from mobile phones, smartphones, SIM cards, PDAs, GPS devices, tablets and game consoles.
4. **Digital Image Forensics** – the extraction and analysis of digitally acquired photographic images to validate their authenticity by recovering the metadata of the image file to ascertain its history.
5. **Digital Video/Audio Forensics** – the collection, analysis and evaluation of sound and video recordings. The science is the establishment of authenticity as to whether a recording is original and whether it has been tampered with, either maliciously or accidentally.
6. **Memory forensics** – the recovery of evidence from the RAM of a running computer, also called **live acquisition**.

APPLICATIONS

- Intellectual Property theft
- Industrial espionage
- Employment disputes
- Fraud investigations
- Misuse of the Internet and email in the workplace
- Forgeries related matters
- Bankruptcy investigations
- Issues concerned the regulatory compliance

Challenges faced by Digital Forensics

- The increase of PC's and extensive use of internet access
- Easy availability of hacking tools
- Lack of physical evidence makes prosecution difficult.
- The large amount of storage space into Terabytes that makes this investigation job difficult.
- Any technological changes require an upgrade or changes to solutions.

Advantages of Computer Forensics :

- To produce **evidence** in the **court**, which can lead to the **punishment** of the culprit.
- It helps the companies **gather important information** on their computer systems or networks potentially being compromised.
- Efficiently **tracks down cyber criminals** from anywhere in the world.
- Helps to **protect** the **organization's money** and **valuable time**.
- Allows to **extract**, **process and interpret** the **factual evidence**, so it proves the cybercriminal action's in the court.

Disadvantages of Computer Forensics

- Before the digital evidence is accepted into court it must be **proved** that it is **not tampered** with.
- Producing and keeping electronic records **safe is expensive**.
- **Legal practitioners** must have **extensive computer knowledge**.
- Need to produce **authentic** and **convincing** evidence.
- If the tool used for digital forensics is not according to **specified standards,** then in a **court of law**, the evidence can **be disapproved** by justice.
- A **lack of technical knowledge** by the **investigating officer** might not offer the desired result.

Forensic Software and Hardware

- Digital forensics software is used **to investigate and examine IT systems** after security incidents or for security-related **preventive maintenance.**
- These tools help business perform **in-depth analysis of IT systems** to identify the cause of **security incidents**, outline vulnerabilities, and assist security teams in facilitating incident response processes.
- These tools aggregate **security information** from hardware, network logs, and files to present security professionals with a full picture of the likely causes of security incidents.
- many tools identify the steps necessary to **remediate the vulnerability and update policies and configurations** to **prevent the situation from arising again.**
- Companies use these tools after security incidents to identify **the cause and root out any flaws or bugs that would allow a repeat scenario.**
- They also use these tools to **investigate systems, networks, and software to identify risks and remediate them before an incident occurs.**

Forensic Hardware

- In Digital Forensics, Examiners need to follow certain steps starting from evidence identification to final submission of report in court of law.
- Forensic Hardware play the **major** role in digital forensics process. **evidence imaging** is the **foremost task** in forensic investigation. The imaging can be done through **multiple type of software** and equipment.
- The hardware tools are **more powerful** in comparison of software extraction tools because they are fast, easy to use and can work in stand alone mode. It means **no extra plug**-in required to image the SATA hard drive and it can image in very less time in comparison of imaging through software tools.

Forensic Technology and Practices

- Forensic -the application of s**cientific knowledge** to **legal** problems.
- a field of technology that uses investigation techniques to help **identify, collect, and store evidence from an electronic device.**
- **Massively Parallel Sequencing (MPS)**
- **Time-Tracing Fingerprint Technology**
- **3-D Models to Help Examine Victims**
- **Link Analysis Software**
- **Computer-based Facial Reconstruction**
- **Artificial Intelligence**

Massively Parallel Sequencing (MPS)

- MPS gives more information about **DNA evidence** than ever before, which will be critical in helping to **solve missing persons cases**, or situations where there has been a large disaster with many deaths.
- **Time-Tracing Fingerprint Technology**

With the availability of this advanced fingerprint technology, the crime investigators can find out the **timeframe** when a fingerprint was left behind, thereby helping to **eliminate the innocent suspects who left the scene of crime long before crime was committed.**

- **3-D Photography Technology**
- Jurors and others find it difficult to properly examine the crime scene/morgue photographs because these 2-dimensional photographs don't show the intricate details of relevant internal damage, old/repeated injury marks, and others on a corpse.
- New and advanced 3-D Photography forensic technology uses **image layering**, which helps crime scene investigators analyze more closely about the crime and **consequently share more evidence with the jurors.**

- **Computer-based Facial Reconstruction**

Even if the appearance of a victim is **damaged or decomposed**, **forensic software** can be fed with user **inputs data** (especially remains of the decomposed/damaged human body) so that the facial/physical appearance of the person can be deducted or reconstructed.

- **Alternative Light Photography**

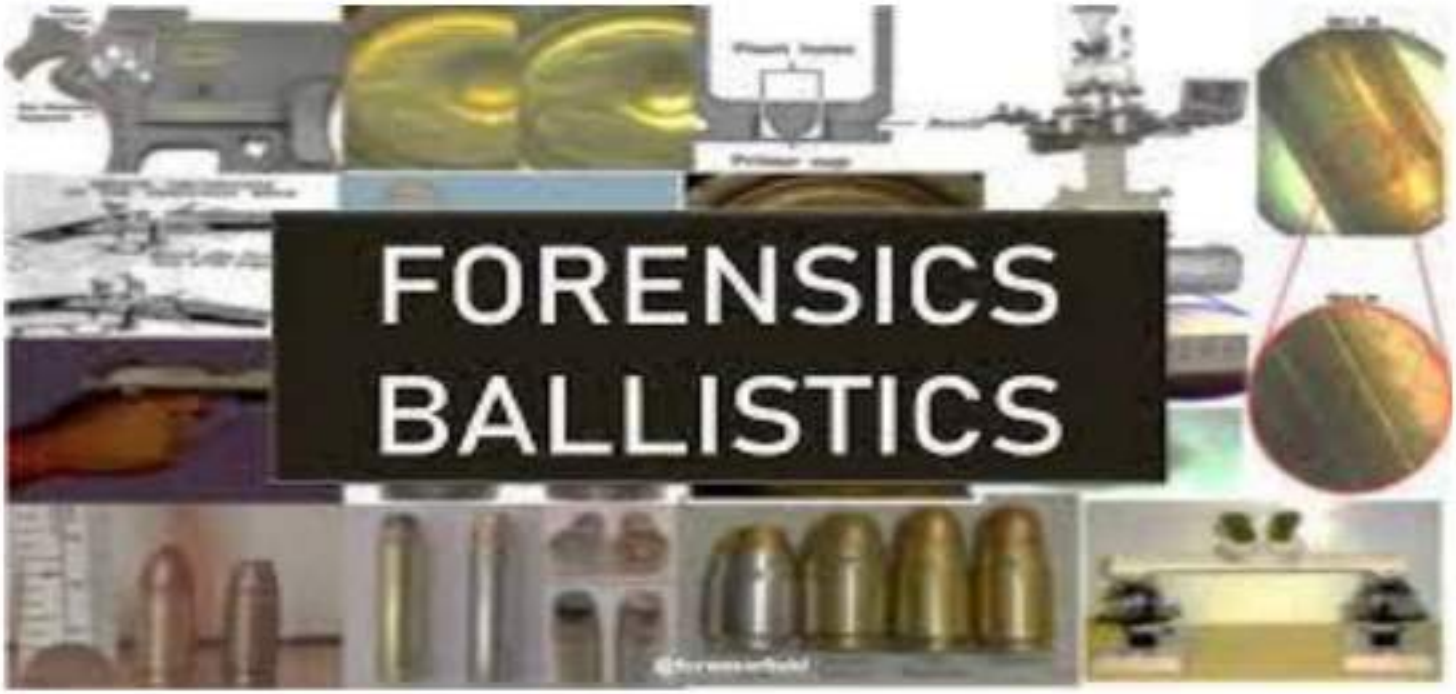
A specialized camera uses **blue light** and **orange filters** to view whether any **bruising** has taken place **below the surface** of the **skin.**

This helps the forensic people to **detect body damage** even before it has surfaced on the skin.

Automated Fingerprint Identification

- **Magnetic fingerprinting dust** enables forensic investigators to get **a perfect fingerprint impression** without compromising.
- Once a perfect fingerprint is found, the forensic scientists can feed the data in **specialized software for comparing** it with the **match of an extensive digital database** of fingerprints of millions or even billions of people.
  Integrated Automatic Fingerprint Identification System **(IAFIS)** and Micro-X-Ray Fluorescence **(MXRF)** are some of the **advanced latent print analysis** used by forensic experts.

- **Link Analysis Software**
- This software helps **financial investigators in tracking funds**, especially any **strange financial activity found in the paper trail**.
- The financial transactions of a person are analyzed by the Enter Link Analysis Software (with the **help of statistical models**) for **finding out possible illegal financial behavior.**



Components of Forensic Ballistics:-

- Firearm

- Ammunition

- Target

Forensic Ballistics

- Ballistics refers to the study that deals with the projectile motion in flight, especially in the **case of bullets**.
- Ballistics can be defined as a field of study that deals with flight, behavior as well as characteristics of any projectile and also **evaluates firearm functioning, the process of firing, the flight process as well as the effects that the projectile has on the target.**
- https://www.slideshare.net/DeepikaDubey8/forensic-ballistics-91291961

- Application of Ballistics for **aiding law and legal agencies** so as to maintain law and order in our society is referred to as FORENSIC BALLISTICS. It basically aims at **identifying the offender and linking him/her to the scene of crime as well as a weapon of offence**. To achieve this purpose forensic ballistic expert performs the following tasks:-
- Collection of all the **physical evidence** at the crime scene such as **fired cartridges, wads, bullets or shots, firearm, clothes** of the **deceased** and **accused** etc.
- **Analysing** the **physical evidence collected**.
- Studying in details the **different types of marks** found on the projectile as well as the cartridge case.
- **Analysing and evaluating** the projectile wounds (living target), impact of projectile (inanimate objects) **and fate of the projectile** after hitting the target.

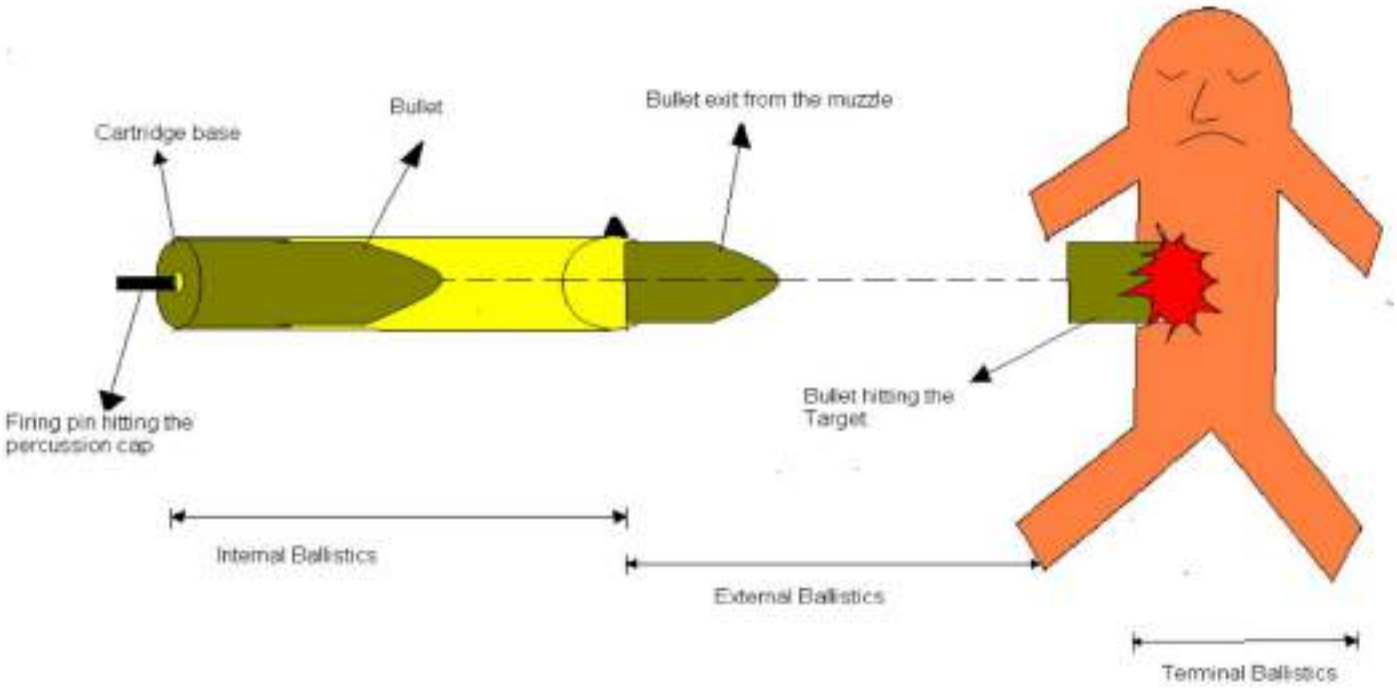
- The identification of the weapon of offence and linking it to the scene of crime as well as the offender/suspect is the primary aim of a forensic ballistic expert and this is carried out by ascertaining various aspects which are as follows:-
- **Nature** of Crime (homicide, suicide, assault etc.)
- **Number of rounds fired** from a **single firearm** and the total number of shooters.
- **Range** from which firing took place.
- **Crime Scene Reconstruction**
- **Distance between victim** and **offender**
- **Identification** of **weapon of offence (**aided by analysis of projectile injuries)

DIVISIONS OF FORENSIC BALLISTICS

Forensic Ballistics is studied under 3 broad headings

- Internal Ballistics
- External Ballistics
- Terminal/Wound Ballistics

EXAMPLE



Internal Ballistics

- Internal Ballistics studies the motion of projectile **inside the barrel of the firearm** i.e the flight of the projectile from the moment the **firing pin strikes the percussion cap to the moment** just before the projectile leaves the muzzle of the firearm barrel.
- It deals with the **factors that affect motion of projectile** when it travels inside the firearm, such as the **primer and propellant composition, their quantity, rifling,, internal barrel diameter, choke** etc.

External Ballistics

- External Ballistics deals with the study of flight of the projectile in the sir i.e. **from the moment the projectile just leaves the barrel till the moment just before it hits the target**.
- Factors like **rifling, air pressure, resistance, gravity, friction, angle of fire, distance of the target** etc.
- play a key role in studying the flight as well as efficiency of any projectile

Terminal/Wound Ballistics

- Terminal Ballistics deals with the study of the impact of the projectile on the **target which it hits and the subsequent path the projectile traverses inside the target**.
- Factors like **elasticity, friction, resistance** etc. of the target, play a very important role in ascertaining the projectile path/motion after hitting the target.

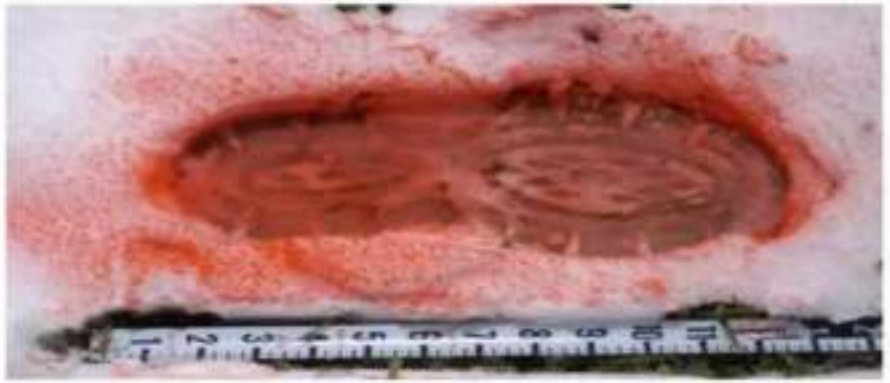
FORENSIC PHOTOGRAPHY

It is referred to as forensic imaging or crime scene photography, is the art of producing an accurate reproduction of a crime scene or an accident scene using photography for the benefit of a court or to aid in an investigation. It is the part of evidence collecting. It provides investigators with photos of victims, places and items involved in the crime

Photographing the crime scene

Basic reason

- To record the scene and associated areas.
- To record the appearance of physical evidence as first encountered.
- To provide investigators with a photographic record of the scene to assist them with their investigations.
- To present the crime scene at court for the edification of judges, juries and counsel alike.



Admissibility of photographic evidence

Points of qualification of a photograph in court

- Object pictured must be material or relevant to the point in issue.
- The photograph must not appeal to the emotions or tend to prejudice the court or jury.
- The photograph must be free from distortion and not misrepresent the scene or the object it purports to reproduce

PHOTOGRAPHS

1.BIG PHOTOGRAPH

2.MIDRANGE PHOTOGRAPH

3.CLOSEUP PHOTOGRAPH

The Big photograph

The mid-range photographs

METHODS

Crime or accident scene photographs usually capture images in color but also in Black and white. There are different methods of photography like digital, Aerial, Surveillance photography.

Digital photography:- It has an automatic date and time marker on each image, so that authenticity can be verified.

Aerial Photography

Taking of photographs of the ground from an elevated position. Platforms for aerial photography include helicopters, kites & air craft. The use of aerial photography for military purposes was expanded during World war.

These are used for taking photographs of a big crime scene. Ex- arson case etc.

CAMERA USED

Aerial camera systems are fitted with pan, tilt, roll and 10x zoom cameras which allows the aircraft to record and transmit to the ground and Internet live HD video via either a wireless digital video link of a 3G/4G wireless internet connection.

HELICOPTER USED

Octocopters also known as Coptercam Aerial Camera System
: Has 8 aerial camera

Hexacopters
: Has 6 aerial camera

Quadcopters
: Has 4 aerial camera

Surveillance Photography

Photographing the behavior activities, or other changing information, usually of people. This can include observation from a distance by means of electronic equipment (such as CCTV cameras).

Surveillance is very useful to maintain social control and prevent/investigate criminal activity.

FIT FOR COURT

The images must be clear and usually have scales. They serve to not only remind investigators of the scene, but also to provide a tangible image for the court to better enable them to understand what happened. The use of several views taken from the different angles helps to minimize the problem of parallax. Overall images do not have scales and serve to show the general layout.

BLOOD SPLASH PATTERNS

Photographs of blood splash patterns, whether they be on a floor, on a vertical surface such as a wall or even overhead on a ceiling, must be photographed with the film plane parallel to the surface bearing the stain. A scale must be included on the same plane as the surface.

MOTOR VEHICLE CRASHES

These photographs must show the relationships of each vehicle to the other; the view each driver had on approach to the point of impact; the direction from which each driver came; debris and marks on the roadway.

Technical photographs showing damage to the vehicles.

BIOMETRICS

- It is **identification** of **humans** by their **traits** related to **physical features.**
- Biometrics is defined as the applicable means of **identifying and authenticating individuals** in a reliable and fast way through the use of **unique biological characteristics** and technologies that lead to the **acceptable way of solving the crime**.

https://forensicfield.blog/biometrics-and-cyber-security/

THREE TYPES OF BIOMETRICS SECURITY

Biometrics can be used for various purposes, they are most commonly utilized in security. Biometrics are divided into three categories:

- Biometrics in **biology**
- Biometrics based on **morphology**
- Biometrics of **behavior**

Cont….

- In **biological** biometrics, genetic & molecular features are used
- They could include DNA or Blood, which could be analyzed using a sample of bodily fluids
- In **morphological** biometrics the structure of your body is taken into account
- More bodily traits can be mapped to be used with security scanners,eyes,fingerprint or face shape.
- **Behavioral** biometrics are based on patterns that are specific to each individual
- EX: walking, speaking or typing habits are recorded,they can reveal personal information

- **Sensitive documents and valuables** are protected using advanced biometrics.
- **EX: Citibank** already utilizes **speech recognition**, and Halifax, a British bank, with **gadgets** that **monitor** a customer's **heartbeat** to **authenticate their identity**. **Ford** is exploring incorporating biometric sensors into its vehicles.
- Biometrics are used in **electronic passports** all around the world.
- **E-passports** in the United States include a **chip** worth a digital photograph of the bearer's face,fingerprint, or iris, as well as technology that **prohibits** the chip from being read - and the data skimmed - by unauthorized data readers.

EXAMPLES OF BIOMETRIC SECURITY

These are some common examples of biometric security:

- Voice Recognition
- Fingerprint Scanning
- Facial Recognition
- Iris Recognition
- Heart-Rate Sensors

- **FINGER OR PALM VEINS RECOGNITION**
- The **unique pattern** of **blood veins** on a person's finger (or hand) is used to identify them in **vein recognition**. It uses **infrared light** to map the veins beneath the skin of **your fingerprints** or hands.
- **IRIS/RETINA RECOGNITION**
  In iris or retina recognition, a **person's unique pattern** of **retina or iris** is utilized to **identify t**hem. This technique of biometric verification is more difficult to deploy since it requires minimal light pollution, a **camera** that can see **infrared,** and an **infrared light source** to ensure **accuracy.**
- **FACE RECOGNITION**
- Face recognition systems employ a person's **unique facial anatomy** to identify them. It has a wide range of applications, including **law enforcement, credit card payments, and smartphones.**

FINGERPRINT RECOGNITION

Fingerprint authentication uses a person's unique fingerprint to verify their identification.

It's one of the most extensively used biometric verification systems, with uses ranging from cell phones to autos to even buildings. Behavioral biometrics, on the other hand, assesses an individual's distinct ways of acting or any pattern of behavior that can be attributed to a certain individual.

Behavioral biometrics include the following:

- Walking Gait
- Keystroke Dynamics
- Finger and Mouse Movements
- Signature
- Typing Patterns
- Speaker Recognition
- Walking Gait Recognition

A person's walking style is used to identify them in gait recognition. Because everyone walks a bit differently, paying attention to how they put one foot in front of the other is a smart way to establish their identity.

SPEAKER RECOGNITION

- Voice recognition (or voice **biometry** for cybersecurity purposes) uses the **distinctive frequencies, pitch,and tone of a person's** voice to authenticate their identity.
- When users **call a call center for customer service help,** such as online banking, this is now the most generally used method of **validation.**
- Some of these behavioral biometrics provide **continuous authentication rather than a single one-time check.**
- Biometric security solutions, both in banking and retail, as well as on mobile devices, are becoming increasingly popular. Biometrics is being used in a **variety of sectors**

Cont…

- **HOME SECURITY**
  Biometric security systems are used to **verify a person's identity before allowing them into a home**. They also give people access to specific rooms, houses, and office buildings.
- As a result, **keys are no longer required**, and admission to buildings can be granted with the **swipe of a fingertip.**
- **AIRPORT SECURITY**
- Biometrics are commonly used for airport security.
- Many airports use **iris recognition to verify** the identity of an individual

- **MONEY SECURITY**
- Biometric payment security is one of the financial uses of biometrics.
- Fingerprint scans are commonly employed for this technology, which is used to authorize **transact ion operations**.
- **HEALTHCARE**
- Biometric security is also employed in the healthcare industry for **identity cards and health insurance plans**. The most common type of biometrics utilized in the healthcare profession for identification is fingerprints.

- **LAW ENFORCEMENT**
- **Criminal identification** systems also use biometric security. For **example,palm print or fingerprint** authentication are widely used in criminal IDs
- **BANKING**
- Many clients in the banking industry have grown tired of having to confirm their identity frequently, yet without it, the **risk of identity theft will continue to rise.**
- Biometric security systems for banks are therefore in **high demand.** Many banks utilize biometrics in **their smartphone apps, such as fingerprint scanning, facial recognition, and voice verification.**
- A **combination of biometrics** is also used by some banks. When **multi-factor authentication and biometrics are integrated**, an almost impenetrable layer of security is generated.

BENEFITS OF BIOMETRICS

- **Convenience-** Biometrics eliminate the **need to re-enter passwords** if they are forgotten**. Once** the biometrics have been **activated**, they can **be integrated into the system** or device of your choice.
- **Spoofing** - Because biometric data is extremely difficult to steal or forge, hackers may be unable or unwilling to invest the time and effort required to crack a biometric security system.

DRAWBACKS OF BIOMETRICS

- **Costs** - As one might expect, modern systems necessitate l**arge investments**, which many business people cannot afford. It's the most common reason why **businesses don't use biometric authentication**.
- **Breach of Data** - Hackers may find it difficult to recreate biometric data, but it is not impossible. There is **no way to replace a** person's biometric data after it has been hacked Biometrics, unlike **passwords are irreplaceable since each person's biometric identity is unique and cannot be altered.**

- **Tracking** - When using technologies like facial recognition, it's important to keep privacy in mind.
- When biometrics are converted to data and stored, users incur the risk of leaving a permanent digital record that might be monitored by threat actors, especially in areas with extensive surveillance.
- Face-recognition software may be used by businesses and governments to follow and identify people with alarming accuracy,drastically limiting privacy.

Audio and video forensics methodology

- audio and video recordings can provide evidences **of crime scene which assist the digital investigators to view or hear real time like situation .**
- Audio and Video evidence can be analyzed based on the **types of examination associated with crime.**
- Similarly, **Video Authentication, Video Enhancement, Audio Authentication, Audio Enhancement, Audio Recordings and Speaker Identification are part the forensics**.

General procedure audio and video forensics

- Digital forensics approach for handling audio video files after obtaining the audio or video related devices, **proper backup** should be taken on a long lasting storage which should forensically accepted.
- Required **suitable tools** can be utilized for this purpose. It is essential to generate the **hash values** and record this **information properly** for proving the **integrity of the data** and procedures adopted.
- By utilizing suitable tools meta data can be generated for obtaining details like**, file size, file profile, format, name, duration, bit rate, channel details, compression details, sampling rate, codec detail, encoding particulars, overall bit rate, format settings, resolution, display aspect ratio, frame rate mode** etc.

•After taking the backup, it is necessary to record procedures adopted properly.

It is required to be noted the crime scene details, photographs, and available information related to the job assigned

•●

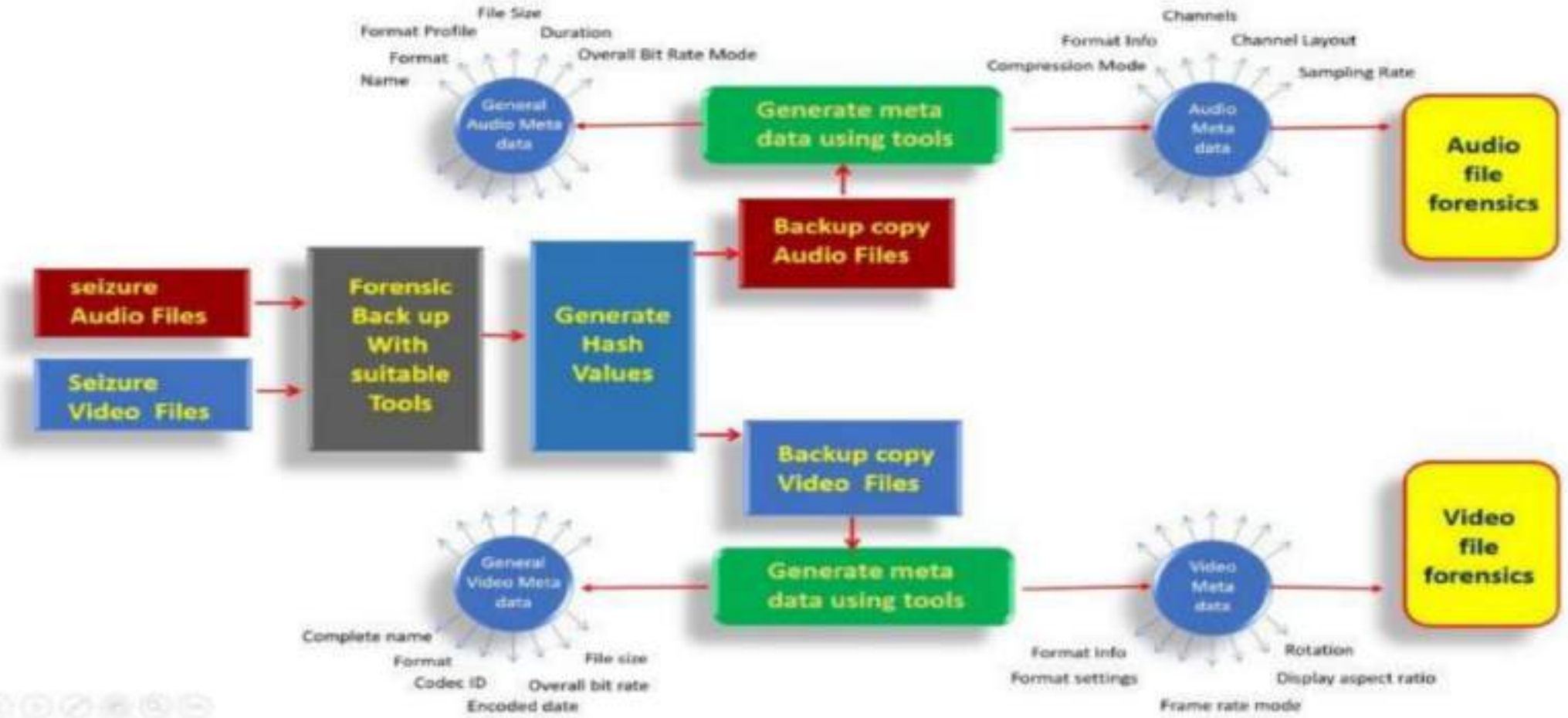
Identification of the devices, and collection of data using suitable tools and devices.

•●

Initially, check the Metadata, check the hash values and save it before processing the data file.

•●

Based on the type of case suitable Hash tool need to be selected and hash values are noted properly to prove the integrity and prove the case.



The process of Audio - Video files Forensic Analysis.

-)**Obtaining media information for Document file forensics**:

By using the media info tool, the results can be obtained in various formats based on the tool selected.

Example like XML formatted information and HTML format based information is obtained and this media information can be obtained for analyzing files like the document file (docx) information.

Obtaining Media information for Audio files forensics

- By utilizing the media info tool for examining the audio files is one of the approaches.
- The output of the media info tool is available different formats like XML, HTML along with various formats based on the selected audio file which is helpful in audio file analysis.
- During the investigation, one can view the file information, format particulars, track details, file extension details, file size, duration of the audio file, Bit rate details, performer details, file creation details, sampling rate, sampling count, compression details, streaming details etc.

Obtaining Media information for Video Files Forensics:

- During the video, file, forensics can be done using different tools.
- The file outputs can be like XML, HTML based on the requirement one can select the type of file.
- During video file analysis, one can observe the details like file information, format particulars, track details, file extension details, file size, duration of the audio file, Bit rate details, performer details, file creation details, sampling rate, sampling count, compression details, streaming details, pixel aspect ratio, bit rate mode, channel positions, frame rate and count, encoded and tagged details, codec configuration details etc.
- This data can be viewed in various formats like HTML, text etc
- By utilizing this type of data, the investigator can draw good conclusions based on the reliable data collected from the crime scene.
- Audio video forensics and its data analysis during cybercrime Investigations provide better results to present before the law enforcement.

Audio file forensics:

- The spectrum can be used for frequency analysis of a particular audio. Investigators can observe the spectrum to find any abnormality in the audio flow, sound etc.
- There are various types of spectrum analysis features based on the tool selected. Investigators must select suitable tools based on the requirement and type of analysis.
- The waveform layer of the tool provides audio data in a traditional waveform peak display.
- Activity log of audio-video files provides good information for analysis.

Video file forensics:

- video file forensics, it is necessary to backup and note hash values and then the video is converted into multiple jpg files (or any picture format).
- Tool like video to jpg converter for splitting the video file into number of jpg format pictures for video file analysis and digital forensics investigation
- Which is useful to view each frame in depth for detailed analysis. A typical output of a video capture is shown in which is a thumb view of the converted video files into multiple-jpg file. Each jpg file is name based on the file name selected.

Windows System Forensics

- Windows Forensic Analysis is **a process that involves collecting and analyzing digital evidence to gain insights into how a computer or network breach occurred**.
- Skilled forensic professionals use this information to determine the type of attacker, their methods, and the data they accessed.
- Most of the systems store data related to the current session in temporary form across registries, cache, and RAM. This data is easily lost when the user switches the system off, resulting in loss of the session information.
- Therefore, the **investigators need** to extract it as a priority. This section will help you understand the volatile data, its importance and ways to extract it.

Collecting Volatile Information

- Volatile Information refers to the data stored in the registries, cache, and RAM of digital devices.
- This information is usually lost or erased whenever the system is turned off or rebooted.
- The volatile information is dynamic in nature and keeps on changing with time; so the investigators should be able to collect the data in real time.
- Volatile data exists in physical memory or RAM and consists of process information, process-to-port mapping, process memory, network connections, clipboard contents, state of the system, etc.
- The investigators must collect this data during the live data acquisition process.
- The investigators follow the Locard's Exchange Principle and collect the contents of the RAM right at the onset of investigation, so as to minimize the impact of further steps on the integrity of the contents of the RAM. Investigators are well aware of the fact that the tools they are running to collect other volatile information cause modification of the contents of the memory.
- Based upon the collected volatile information, the investigators can determine the user logged on, timeline of the security incident, programs and libraries involved, files accessed and shared during the suspected attack, as well as other details.

System Time

- The first step while investigating an incident is the collection of the system time. System time refers to the exact date and time of the day when the incident happened, as per the coordinated universal time (UTC). The system provides the system time so that the applications launched have access to the accurate time and date.
- The knowledge of system time will give a great deal of context to the information collected in the subsequent steps. It will also assist in developing an accurate timeline of events that have occurred on the system. Apart from the current system time, information about the amount of time that the system has been running, or the uptime, can also provide a great deal of context to the investigation process.
- Investigators also record the real time, or wall time, when recording the system time. Comparison of both the timings allows the investigator to further determine whether the system clock was accurate or inaccurate. The investigators can extract system time and date with the help of the date / t& time /t command or use the net statistics server command.
- An alternative way for obtaining the system time details is by using the GetSystemTime function. This function copies the time details to a SYSTEMTIME structure that contains information of individual logged in members and the exact information of month, day, year, weekday, hour, minute, second, and milliseconds. Hence, this function provides better accuracy to the system time details.

Logged-On Users

- During an investigation, an investigator must gather details of all the users logged on to the suspected system.
- This not only includes the information of people logged on locally (via the console or keyboard) but also those who had remote access to the system (e.g. – via the net use command or via a mapped share).
- This information allows an investigator to add context to other information collected from the system, such as the user context of a running process, the owner of a file, or the last access times on files.
- It is also useful to correlate the collected system time information with the Security event log, particularly if the admin has enabled appropriate auditing.

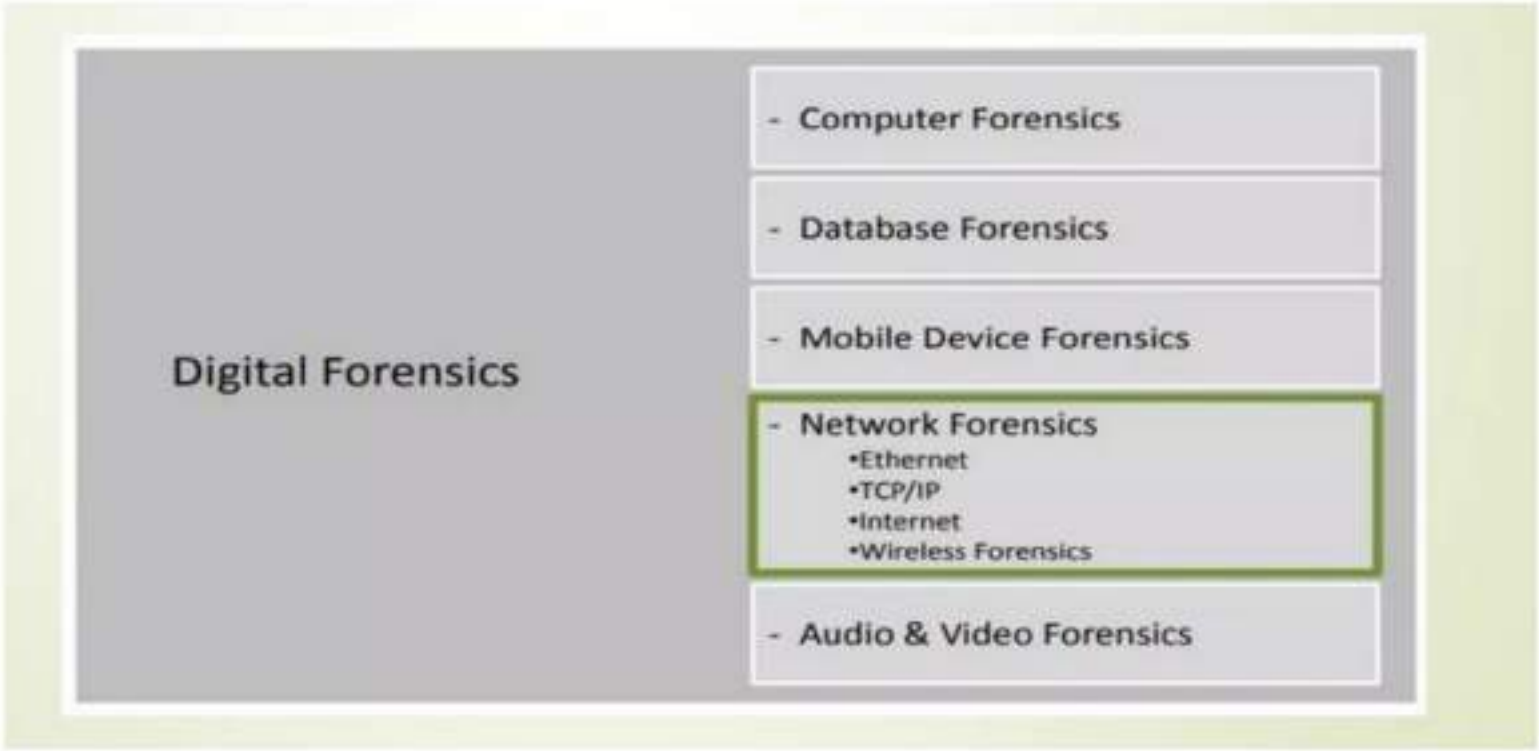
Open-Source Tools for Windows Forensic Analysis

- **1. Magnet Encrypted Disk Detector:** This tool is used to check the encrypted physical drives. This tool supports PGP, Safe boot encrypted volumes, Bitlocker, etc.
- **2. Magnet RAM Capture:** This tool is used to analyze the physical memory of the system.
- **3. Wireshark:** This is a network analyzer tool and a capture tool that is used to see what traffic is going in your network.
- **4. RAM Capture:** As the name suggests, this is a free tool that is used to extract the entire contents of the volatile memory i.e. RAM..
- **5. NMAP:** This is the most popular tool that is used to find open ports on the target machine. Using this tool you can find the vulnerability of any target to hack.
- **6. Network Miner:** This tool is used as a passive network sniffer to capture or to detect the operating systems ports, sessions, hostnames, etc.

- **7. Autopsy:** This is the GUI based tool, that is used to analyze hard disks and smartphones
- **8. Forensic Investigator:** This is a Splunk toolkit which is used in HEX conversion, Base64 conversion, metascan lookups, and many more other features that are essential in forensic analysis
- **9. HashMyFiles:** This tool is used to calculate the SHA1 and MD5 hashes. It works on all the latest websites. You can download it from here.
- **10. Crowd Response:** This tool is used to gather the system information for incident response.
- **11. ExifTool:** This tool is used to read, write, and edit meta information from a number of files
- **12. FAW (Forensic Acquisition of Websites):** This tool is used to acquire web pages image, HTML, source code of the web page. This tool can be integrated with Wireshark..

Linux Forensics Tool

- The use of advanced Linux forensic analysis tools can help an examiner locate crucial evidence in a more efficient manner. Some of these tools are extremely powerful and provide the capability to quickly index, search, and extract certain types of files.
- Creating a disk image: "dd" command
- Image verification
- Mounting and unmounting a disk image:
- File carving
- Creating a timeline of events
- Searching a disk image



Network Forensics

- Network forensics is a **subcategory of digital forensics**
- It deals with the **examination** of the **network** and its **traffic** going across a network that is suspected to be involved in malicious activities, and its investigation
- Ex: a network that is **spreading malware** for **stealing credentials** or for the purpose analyzing the cyber-attacks.
- the **entire data** can be **retrieved** including messages, file transfers, e-mails, and, web browsing history, and reconstructed to expose the original transaction.
- It is also possible that the **payload in the uppermost layer packet** might wind up on the disc, but the envelopes used for delivering it are only captured in network traffic.
- For identifying the attacks investigators must **understand the network protocols and applications** such as **web** protocols, **Email** protocols, **Network** protocols, file transfer protocols, etc.

ETHERNET

- Methods are achieved with eavesdropping bit streams (on the Ethernet layer).
- Uses monitoring tools or sniffers (Wireshark ,Tcpdump)
- Protocols can be consulted for filter traffic and reconstruct attachment transmitted, such as the Address Resolution Protocol (ARP)
- Network Interface Card (NIC), but can be averted with encryption
- Disadvantage is large storage Capacity.

TCP/IP

- Methods are achieved with router information investigations (on the Network layer).
- Each router includes routing tables to pass along packets.
- These are some of the best information sources for data tracking .
- Follow compromised packets, reverse route, ID the source
- Network layer also provides authentication log evidence

INTERNET

- Methods are achieved by identifying server logs (on the Internet).
- Includes web-browsing, email, chat, and other types of traffic & communication
- Server logs collect information
- Email accounts have useful information except when email headers are faked

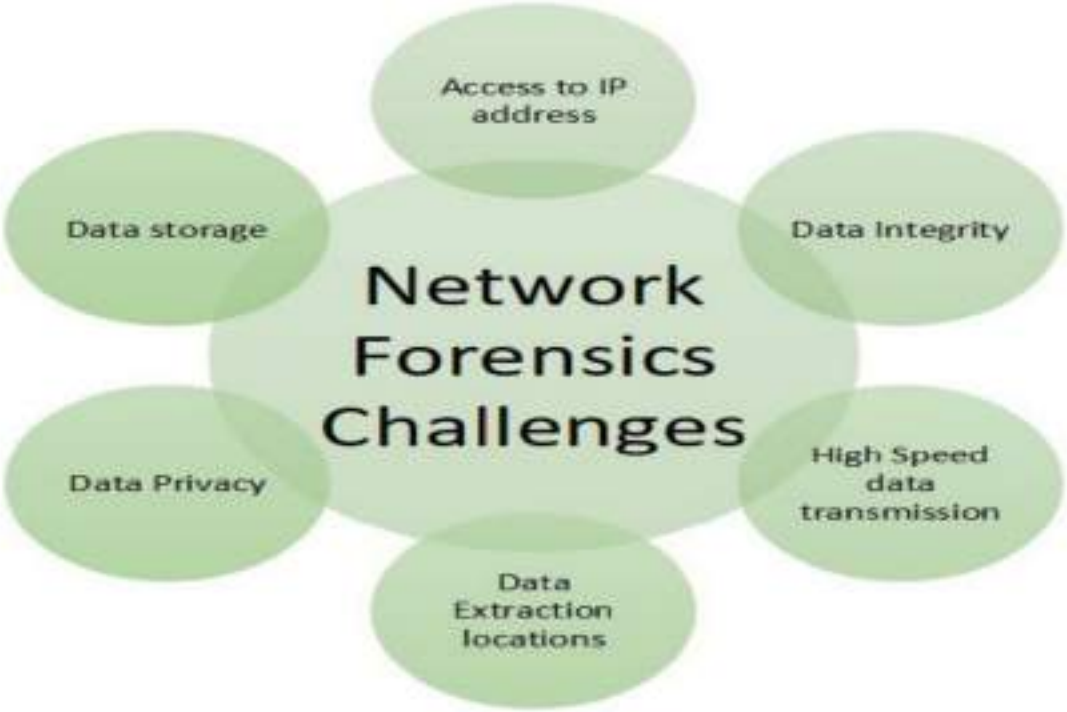
Wireless Forensic

- Methods are achieved by collecting & analyzing wireless traffic (Wireless Networks). Mobile Phones
- A sub-discipline of the field
- To get that which is considered "valid digital evidence"
- This can be normal data OR voice communications via VoIP
- Analysis is similar to wired network situations, with different security issues

Processes Involved in Network Forensics:

- **Identification:** investigators **identify** and **evaluate t**he incident based on the **network pointers**.
- **Safeguarding:** The investigators **preserve** and **secure** the data so that the tempering can be prevented.
- **Accumulation:** detailed report of the crime scene is **documented** and all the **collected digital shreds** of evidence are **duplicated**.
- **Observation:** all the **visible data is tracked along with the metadata.**
- **Investigation:**final conclusion is **drawn from the collected shreds of evidence.**
- **Documentation:** all the shreds of evidence, reports,conclusions are **documented and presented** in court.

Challenges in Network Forensics:



ADVANTAGES & DISADVANTAGES

- Network forensics helps in **identifying security threats** and **vulnerabilities.**
- It **analyzes and monitors** network **performance demands**.
- Network forensics helps in **reducing downtime**.
- Network resources can be used in a better way by **reporting and better planning.**
- It helps in a **detailed network search** for any **trace of evidence** left on the network
- The only **disadvantage** of network forensics is that it is **difficult to implement.**

Forensic Tools

Network Forensic Analysis Tools

Functions of a Network Forensic Analysis Tool:

- Network traffic capturing and analysis
- Evaluation of network performance
- Detection of anomalies and misuse of resources
- Determination of network protocols in use
- Aggregating data from multiple sources
- Security investigations and incident response
- Protection of intellectual property

Forensic Tools

Tools	Description
Binwalk	It is a tool for searching a given binary image for embedded files and executable code.
bulk-extractor	It extracts information without parsing file systems such as e-mail addresses, credit card numbers, URLs, and other types of details from digital evidence files.
Capstone	It is a framework used for binary analysis and reversing. It supports multiple hardware architectures and provides semantics of the disassembled instruction.
chntpw	It is used to view information and change user passwords in Windows NT/2000 user database file.
Cuckoo	It is a malware analysis system that can provide you the details of suspicious files you asking for.
dc3dd	It is a patched version of GNU dd with added features for computer forensics.
ddrescue	It duplicates data from one file or block device to another specified file or block.
DFF	DFF stands for Digital Forensic Framework. It is used to quickly and easily collect, preserve, and reveal digital evidence without compromising systems and data.
diStorm3	It is a lightweight, easy-to-use, and fast decomposer library that disassembles a staged reverse shell generated by msfpayload.
Dumpzilla	Dumpzilla is a tool to extract all forensic related information of Firefox, Iceweasel, and Seamonkey browsers to analyse.

extundelete	This tool is used to recover deleted files from ext3/ext4 file system partition.
Foremost	It is a forensic tool to recover lost files based on their headers, footers, and internal data structures.
Galleta	It is a forensic tool that examines the content of cookies produced by Internet explorer.
Guymager	It is a free forensic imager for media access. It generates flat, EWF, and AFF images support disk cloning.
iPhone Backup Analyzer	It is a backup utility designed to browse easily through the backup folder of an iPhone.
p0f	It is a traffic fingerprinting mechanism to identify the process behind any incidental TCP/IP communications without disturbing the process in any way.
Pdf-parser	It is used to parse a PDF document to identify the fundamental elements used in the analysed file.
pdfid	It scans a file to look for certain pdf keywords, allowing you to identify PDF documents that contain JavaScript.
pdgmail	It extracts Gmail artefacts from a pd process memory dump
peepdf	It is a pdf analysis tool to explore PDF files in order to find if the file can be harmful or not.
RegRipper	It extracts information from the windows registry and presents it for analysis.
Volatility	It is a memory forensic analysis platform to extracts the digital artefacts from the RAM samples.
Xplico	It is a network forensic analysis tool that extracts application data from internet traffic.

Linux System Forensics

- https://www.sciencedirect.com/topics/computer-science/linux-forensics

UNIT-4

CYBER CRIME INVESTIGATION

CYBERCRIME INVESTIGATION

- Cybercrime investigation is the process of **identifying, analyzing, and mitigating computer-based crimes and other forms of malicious activity that occur in cyberspace.**
- It is the process **of analyzing, investigating, and recovering critical forensic digital data/evidence** from the networks or systems associated in the cyber attack that could be the Internet or a local network in order to identify the executor of the cyber/ digital crime and their main motive behind the attack.
- It involves the use of **specialized tools and techniques to investigate** various types of cyber crimes, such as **hacking, phishing, malware, data breaches, and identity theft.**
- The investigation process **is conducted** by cyber crime **investigators,** who are responsible for conducting **thorough and accurate investigations**, preserving evidence, and collaborating with law enforcement agencies to bring cybercriminals to justice.
- Cybercrime investigation is **essential for businesses and individuals** to **protect against the growing threat of cybercrime**, and to ensure that justice is served for victims of cybercrime.

- Cybercrime investigators should be **experts in computer science**, understanding not only computer software, file systems and operating systems, but also the working of networks/software and hardware in a computer system.
- They should have enough **knowledge to determine how the inter-linking connection between all these components** occur, in order to get a full description of **what has happened, why it was happened, when it was happened, who has performed the cybercrime or cyber attack**, and how can be victims will protect themselves or there near ones in the future against these types of cyber attacks.
- Cybercrime investigation is a **complex and constantly** evolving field, as new threats and technologies emerge.
- As a result, investigators must stay **up-to-date** with the **latest techniques** and tools in order to effectively investigate and mitigate cyber crimes.

Top 5 Cybercrimes

1. Phishing and Scam

Phishing is a type of social engineering attack that targets the user and tricks him by **sending fake messages and emails** to get **sensitive information** about the user or trying to **download malicious software** and exploit it on the target system.

2. Identity Theft

Identity theft occurs when a cybercriminal uses another person's data like **credit card numbers** and **personal pictures without the permission** of that person to commit fraud or a crime.

3. Ransomware Attack

Ransomware attacks are a very common type of cybercrime, ransomware is a type of malware that has the capability to prevent users from accessing all of their personal data on the system by encrypting them, and then **asking for a ransom in order to give access to the encrypted data**.

4. Hacking/Misusing Computer Networks

This term refers to the crime of **unauthorized access to private computers** or networks and misuse of it either by **shutting it down or tampering** with the data stored or other illegal approaches.

5. Internet Fraud

Internet fraud is a type of cybercrime that makes use of the internet and it can be considered a general term that groups all of the crimes that happen over the internet like **spam, banking fraud, theft of service, and so on.**

How to Become a Cyber Crime Investigator?

1. Get the Right Education

- A **degree** in computer science, cybersecurity, or a related field is a good starting point for a career in cybercrime investigation.

2. Develop the Necessary Skills

- Cybercrime investigators need a wide range of **technical and non-technical skills**, including **knowledge of computer systems and networks, an understanding of cybercrime laws and regulations, critical thinking skills, and the ability to work well under pressure**.

3. Gain Experience

- **Internships, volunteer work, or entry-level positions in cyber security or computer forensics** can provide valuable experience and help you build a network of contacts in the field.to work with **law enforcement agencies, government agencies, or private companies** that specialize in cyber security.

4. Stay Up-to-Date

- Cybercrime investigation is a **constantly evolving field,** and it's important to stay up-to-date with **the latest trends, threats, and technologies**. Attend **conferences, read industry publications, and participate in online forums** to stay informed and connected to the cybersecurity community.

5. Consider Certification

- Professional certifications, such as the **Certified Ethical Hacker (CEH), or Certified Information Systems Security Professional (CISSP)** can demonstrate your expertise and help you stand out in a competitive job market.

Cybercrime investigation Methods

1. Background Information or facts

- **Developing and defining the background** of the cyberattack with the known facts that will help the **investigators or investigating company a commencing point** to establish what they are facing, and how much information they have when handling the initial cybercrime report of that particular cyberattack.

2. Collecting Information about the cybercrime/cyberattack

- This is One of the most important step any cybercrime investigator must do is **collect as much information/facts** as possible about the cyberattack.

3. Tracking and identifying the Cyber Criminal

- This next step is oftenly performed during the **information-gathering process**, depending on how much information and facts is **already gathered in.**
- In order to identify the criminals behind the cyber attack, both **private and public** security agencies often work with **Internet Service Providers** (ISPs) and networking companies to get **critical log information** about their connections and networks, as well as **historical services, websites and protocols** used during the time they were connected.
- This is often the **slowest phase**, as it requires **legal permission** from the **prosecutors** and a court order to **access the needed data.**

4. Digital Forensics

- Once the Investigator have **collected enough data and facts** about the cyberattack, it's time to **examine the digital systems** that **were affected**, or those supposed to be involved in the **execution of the attack**.
- This process involves **analyzing network connection raw data, hard drives, file systems, caching devices, RAM memory and other potential evidences.**
- Once the forensic work starts, the involved investigator will follow up on all the involved trails looking for **fingerprints in system files, network and service logs, emails, web-browsing history,** etc

INVESTIGATION TOOLS

- Cybercrime investigation requires the use of **specialized tools and software** to collect, preserve, and analyze digital evidence. These tools can be used to **identify suspects, track their activities, and gather evidence** to build a case against them.

Here are some of the most common cybercrime investigation tools used by investigators:

1. Digital Forensics Software

- It is used to **recover deleted files, analyze metadata, and examine network traffic logs**. Popular digital forensics software includes tools like **EnCase, FTK, and Autopsy**.

2. Network Analysis Tools

- They are used to **monitor network traffic, identify suspicious activity**, and **track the flow** of data. Network analysis tools include tools like **Wireshark, tcpdump, and Netscout**.

3. Malware Analysis Tools

- They are used to analyze and reverse engineer malware to understand its behavior and **identify its source**. Malware analysis tools include **IDA Pro, OllyDbg, and Binary Ninja**.

4. Password Recovery Tools

- They are used to **recover passwords from encrypted files**, databases, or other sources of digital evidence. Password recovery tools include tools like **Cain and Abel, John the Ripper, and Hashcat.**

- **5. Social Media Analysis Tools**
- They are used to **track suspects' activities and gather evidence from social media platforms.** Social media analysis tools include tools like Hootsuite, Follower wonk,etc…
- It's important for investigators to have a deep understanding of these tools, as well as knowledge of the **latest trends and techniques** in cybercrime investigation.
- By using these tools effectively, investigators can help to **identify and prosecute cyber criminals and protect individuals and organizations** from the growing threat of cybercrime.
- It is a growing threat to **individuals, businesses, and governments** around the world. As more and **more sensitive information** is stored and transmitted digitally, the risk of cyber-attacks and data breaches continues to increase.
- Cybercrime can take many forms, including hacking, identity theft, fraud, and cyberterrorism.
- Investigating cybercrime requires **specialized techniques, tools, and training to identify, analyze, and report** evidence related to these crimes.

Differences between e-discovery and digital forensics

- Computer forensics, also called ***cyber forensics***, is a specialized form of e-discovery in which an investigation is carried out on the **contents of the hard drive of a specific computer.** After **physically isolating the computer, investigators make a digital copy of the hard drive**. Then, the original computer is locked in a secure facility to maintain its pristine condition. All investigation is done on the digital copy.
- E-discovery and digital forensics are similar processes, as **both involve identifying, collecting and preserving data.** However, the main differences between the terms are in **how the data is presented** and **who is analyzing** it.
- In **computer forensics**, a **forensics expert is in charge of protecting data integrity** and bringing forth stored data. In **e-discovery, attorneys handle these processes.** Digital forensics also uses different software applications.
- E-discovery firms also **do not analyze the data they collect, nor do they determine the intent of a user or provide legal advice** -- as forensic experts do. Rather, e-discovery gathers and organizes information for others to view.

E-DISCOVERY

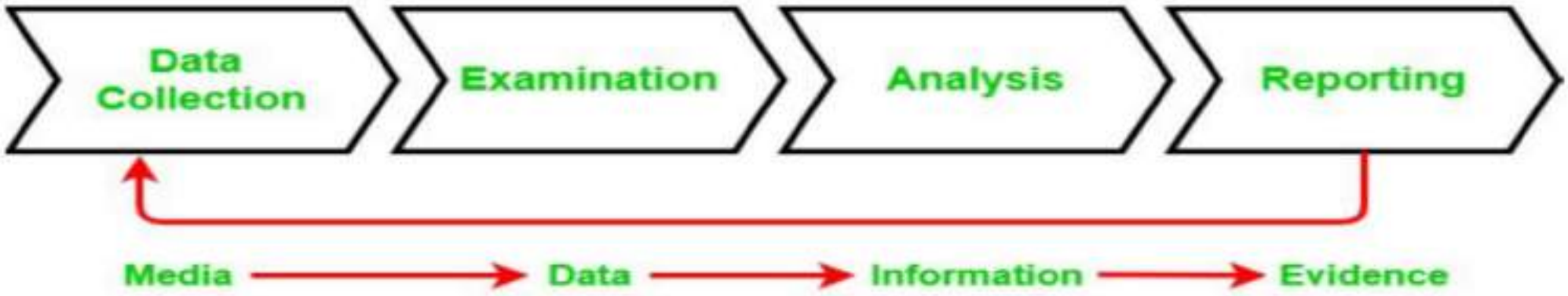
- **Electronic discovery** (also known as e-discovery, ediscovery, eDiscovery, or e-Discovery) **is the *electronic* aspect of identifying, collecting and producing electronically stored information** (ESI) **in response to a request for production in a law suit or investigation.**
- It is the process of **obtaining and exchanging evidence in a legal case or investigation.**
- E-discovery is used in the **initial phases of litigation** when involved parties are required to **provide relevant records and evidence related to a case**.
- This process includes **obtaining and exchanging electronic data that is sought, located, secured** and searched for with the intent of using it as evidence

e-discovery process

- **Identification.** ESI is identified by **attorneys**. E-discovery requests and challenges are made.
- **Preservation.** Data that is **identified as potentially relevant** is placed under legal hold so **it cannot be destroyed**. Failure to preserve data will lead to sanctions and fines if the lost data puts the defense at a disadvantage.
- **Collection.** Data is **transferred from a company to legal counsel**. The legal counsel determines the data's relevance.
- **Processing.** Files are loaded into a review platform. Data is usually converted into a PDF (Portable Document Format) or TIFF (Tag Image File Format) for court.
- **Review.** The review process assesses documents for **privilege and responsiveness** to discovery requests.
- **Production.** Documents are exchanged with opposing counsels.

DIGITAL EVIDENCE COLLECTION

- Digital evidence is the kind of information in **binary form** which is mainly associated with **e-crimes**
- **finding digital evidence** within a process to **analyze, inspect, identify** and **preserve digital evidence** associated with **electronic devices**
- 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.



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 evidence is **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

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

1. **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**.
2. **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.ex:human agents,oral,sign….
- **Documentary**
- **Digital**

Challenges Faced During Digital Evidence Collection:

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

Evidence Preservation

- **Once data is acquired, the data and device need to be securely stored until they're needed for further investigation**.
- Preservation is usually done in either **physical or digital storage** systems or preferably in a smart management system that can integrate with evidence management systems
- Effective evidence preservation includes **appropriate packaging with correct and consistent information on labeling and procedural documentation for all items**.
- **Biological evidence** should be **air-dried before packaging** to **minimize degradation**.

Critical Steps in Preserving Digital Evidence

- **Do not change the current state of the device:** If the device is OFF, it must be kept OFF and if the device is ON, it must be kept ON. Discuss with forensics expert before doing anything.
- **Power down the device:** In the case of mobile phones, If it is not charged, do not charge it. In case, the mobile phone is ON power it down to prevent any data wiping or data overwriting due to automatic booting.
- **Do not leave the device in an open area or unsecured place:** Ensure that the device is not left unattended in an open area or unsecured area. You need to document things like- where the device is, who has access to the device, and when it is moved.
- **Do not plug any external storage media in the device:** Memory cards, USB thumb drives, or any other storage media that you might have, should not be plugged into the device.
- **Do not copy anything to or from the device:** Copying anything to or from the device will cause changes in the slack space of the memory.

- **Take a picture of the piece of the evidence:** Ensure to take the picture of the evidence from all the sides. If it is a mobile phone, capture pictures from all the sides, to ensure the device has not tampered till the time forensic experts arrive.
- **Make sure you know the PIN/ Password Pattern of the device:** It is very important for you to know the login credentials of the device and share it with the forensic experts, for them to carry their job seamlessly.
- **Do not open anything like pictures, applications, or files on the device:** Opening any application, file, or picture on the device may cause losing the data or memory being overwritten.
- **Do not trust anyone without forensics training:** Only a certified Forensics expert should be allowed to investigate or view the files on the original device. Untrained Persons may cause the deletion of data or the corruption of important information.
- **Make sure you do not Shut down the computer, If required Hibernate it:** Since the digital evidence can be extracted from both the disk drives and the volatile memory. Hibernation mode will preserve the contents of the volatile memory until the next system boot.

Three Methods To Preserve a Digital Evidence

1. **Drive Imaging:** Before forensic investigators begin analyzing evidence from a source, they need to create an **image of the evidence**. Imaging a drive is a forensic process in which an analyst will create a **bit-by-bit duplicate of the drive**. When analyzing an image forensic experts need to keep in mind the following points:

- Even **wiped drives** can retain **important and recoverable** data to **identify**.
- Forensic experts can **recover all deleted files** using **forensic techniques**.
- Never **perform forensic analysis on the original media**. Always Operate on the **duplicate image**.
- A piece of **hardware or software** that helps facilitate the legal defensibility of a forensic image is a "write blocker", which forensic investigators should use to create the image for analysis.

- **Hash Values:** When a forensic investigator creates an image of the evidence for analysis, the process generates **cryptographic hash values like MD5, SHA1, etc**. Hash Values are critical as:
- They are used to **verify the Authenticity and Integrity** of the image as an **exact replica** of the **original media**.
- When admitting evidence in the court, **hash values are critical as altering even the smallest bit of data will generate a completely new hash value**.
- When you perform any **modifications** like creating a new file or editing an existing file on your computer, a **new hash value is generated** for that file.
- **Hash value** and other **file metadata** are **not visible in a normal file explorer** window but analysts can access this information using **special software**.
- If the hash values of the **image** and the **original evidence do not match**, it may **raise concerns in court that the evidence has been tampered with.**

- **Chain of Custody:** As forensic investigators collect media from the client and transfer it, they should document all the steps conducted during the transfer of media and the evidence on the Chain of Custody (CoC) forms and capture signatures, date, and time upon the media handoff.
- It is essential to **conduct CoC paperwork** due to the following reasons:
- CoC demonstrates that the image has been under **known possession** since the time the **image was created**.
- Any lapse in the CoC **nullifies the legal value of the image**, and thus the analysis.
- Any gaps in the procession record like any time the **evidence was left unattended in an open space or an unsecured location are problematic**.

Problems in Preserving Digital Evidence

- **Legal Admissibility:** The highest risk is legal admissibility, If the evidence of a crime is a piece of digital media, it should be **immediately quarantined and put under the CoC** – an investigator can **create an image later**.
- **Evidence Destruction:** If in case, threat actors have installed an application on a server, the future forensic analysis will rely on the application being available and not deleted from the system.
- **Media is still in Service:** If the media is still in service, the risk of vital evidence destruction grows with the amount of time that has elapsed since the incident took place.

Email Programs and Protocols

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

E-Mail Investigation

- Emails play a very important role in **business communications** and have emerged as one of the most important applications on internet.
- With the increasing popularity of the use of email based on the boom of the internet, some typical crimes are tied to email. For instance, financial crime, cyber security, and extortion software.
- To bring **email criminals** to justice, it's crucial to look into **email investigation in cyber security**.
- Before we can dive into the major investigative extraction working directions of email forensics:
- **Local Computer-based emails**: For local computer-based email data files, such as **Outlook .pst or .ost files**, it's recommended to follow our following techniques directly.
- **(Cloud) Server-based emails**: For (Cloud Server based email data files, it's not **possible to conduct complete forensic work until you obtain the electronic copies** in the (Cloud)server database under the consent of the service providers.
- **Web-based emails**: For Web-based e-mail (e.g. Gmail,) investigations, it's more likely possible to just **filter specific keywords to extract email** address-related information instead of the overall email data and information compared to local computer-based emails.

GOALS OF E-Mail Investigation

- To identify the main criminal
- To collect necessary evidences
- To presenting the findings
- To build the case

Challenges

- **Fake Emails**

The biggest challenge in email forensics is the use of fake e-mails that are created by **manipulating and scripting headers** etc. In this **category criminals** also **use temporary email which is a service** that allows a registered user to receive email at a temporary address that **expires after a certain time period**.

- **Spoofing**

Another challenge in email forensics is spoofing in which criminals used to **present an email as someone else**. In this case the **machine will receive both fake as well as original IP address.**

- **Anonymous Re-emailing**

The Email server strips **identifying information from the email message before forwarding it further.** This leads to another big challenge for email investigations.

Techniques Used in Email Forensic Investigation

- Header Analysis
- Server investigation
- Network Device Investigation
- Sender Mailer Fingerprints
- Software Embedded Identifiers

Email Header Analysis

- Email headers contain essential information, including the **name of the sender and receiver, the path** (servers and other devices) through which the message **has traversed,** etc.
- The vital details in email headers help investigators and forensics experts in the email investigation. For instance, the Delivered-To field contains the recipient's email address, and the Received-By field contains:
- The **last** visited **SMTP server's IP address**.
- It's **SMTP ID**.
- The **date and time** at which the email is **received**.
- field provides necessary details like the sender's IP address and hostname. Again, such information can be instrumental in identifying the culprit and collecting evidence.

Email Server Investigation

- Email servers are investigated to locate the source of an email. For example, if an email is
- deleted from a client application, sender's, or receiver's, then related ISP or Proxy servers are
- scanned as they usually save copies of emails after delivery. Servers also maintain logs that can be analyzed to identify the computer's address from which the email originated.
- It is worth noting that HTTP and SMTP logs are archived frequently by large ISPs. If a log is archived, tracing relevant emails can take a lot of time and effort, requiring decompressing and extraction techniques. Therefore, it is best to examine the logs as soon as possible

3.Investigation of Network Devices

- In some cases, **logs of servers** are **not available**. This can happen for many reasons, such as when **servers are not configured** to **maintain logs** or when an **ISPs refuses to share the log files**.
- In such an event, investigators can refer to the logs maintained by network devices such as switches, firewalls, and routers to trace the source of an email message.

4. Sender Mailer Fingerprints

- X-headers are email headers that are **added to messages along with standard headers, like Subject** .
- These are often added for **spam filter information**, **authentication** results,etc., and can be used to identify the **software handling** the email at the client.

E-Mail Tracking

- Tracking is a method for **monitoring whether the email messages is read by the intended recipient**.
- Most tracking technologies use some form of **digitally time-stamped record** to reveal the **exact time and date** that an email was received or opened, as well as the **IP address** of the recipient.
- Email tracking is useful for when the sender wants to know whether the **intended recipient actually received the email or clicked the links**. However, due to the nature of the technology, email tracking cannot be considered an absolutely **accurate indicator** that a message was opened or read by the recipient.

Ways to block Email tracking

- **mail Hyperlinks**-Be **cautious about clicking on any links** in the email.
- **External Images**-It's simple to **turn off automatic picture downloads**. You may do so with a variety of email providers, as shown below.

EMAIL RECOVERY

- One of the most important aspects of investigating a cybercrime is the ability to **recover and analyze emails** that may have been involved in the incident.
- Email recovery is the **process of retrieving emails** that have been **deleted or otherwise lost**, in order to gather evidence or other information related to a cybercrime investigation.

1.Emails are often a **key source of evidence** in cybercrime investigations, as they can provide information on the perpetrators, victims, and the nature of the crime.

2. Deleted or lost emails can be recovered using a variety of methods, including **server backups, email recovery software**, and **forensic analysis**.

3. **Recovered emails** can be **analyzed for a range of information**, including the sender, recipient, date and time sent, and content of the email.

4. Email headers can provide valuable information in cybercrime investigations, such as the **IP address** of the **sender** and the email **client** used.

5. Emails can also contain **attachments,** such as documents or images, that may **provide additional evidence** of cybercrime.

6. Recovery of deleted or lost emails can be **time-sensitive,** as email servers may have retention policies that **automatically delete emails after a certain period of time.**
7. Email recovery may require **specialized technical knowledge** and expertise, particularly in cases where forensic analysis is necessary.
8. **Chain of custody protocols** must be followed when handling recovered emails to ensure that the evidence is admissible in court.
9. Recovered emails must be **analyzed** in the context of other available evidence, such as **computer logs, network traffic data, and witness statements.**
10. Email recovery can be a **complex and time-consuming process**, but it is an essential to identify and prosecute cybercriminal

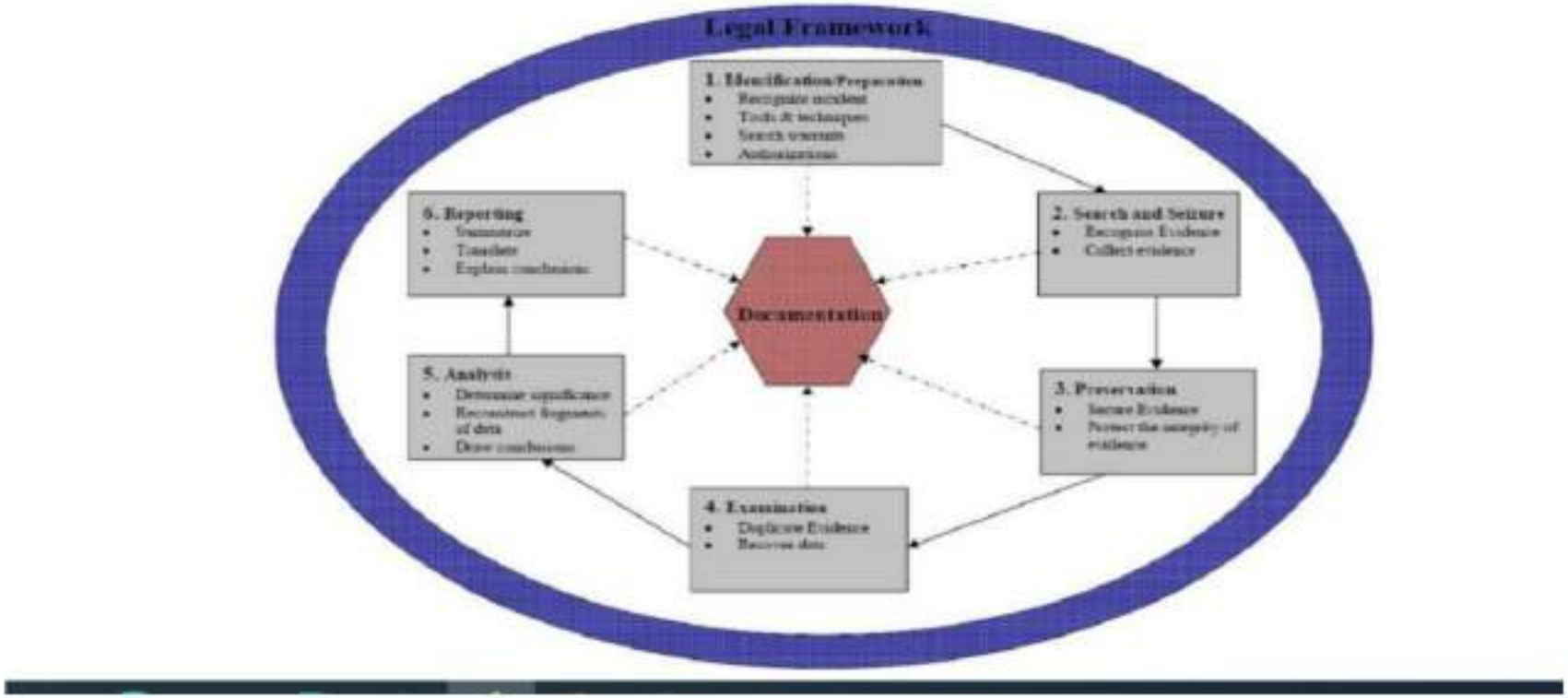
IP Tracking

- When you connect to the internet, your device uses an address to connect with called an IP address. With IP tracking, every time you visit a website, the website knows what IP address
- you are accessing the website from, which means your location, and in the case of businesses,company identities can be determined. This information can be very powerful in determining the demand for your product and services, especially for business-to-business companies.
- Cookies, or behavioral targeting, allow the website you visit to place a cookie on your browser to collect your web-browsing behaviour including time on page, clicks, and other websites you visit. The technology is used primarily by publishers to create "audience profiles," which are basically a bunch of information about you. Cookies will live in your browser until you clear your cache.
- Another approach is to use cookie data to understand the individuals that visit your website, including what department they work in or their job level. You can build an audience profile and market to more people like them to drive relevant traffic to your website.
- Use both IP tracking and cookies simultaneously — this way, not only will you know what companies are visiting your website, but you'll also know what kinds of people are visiting.

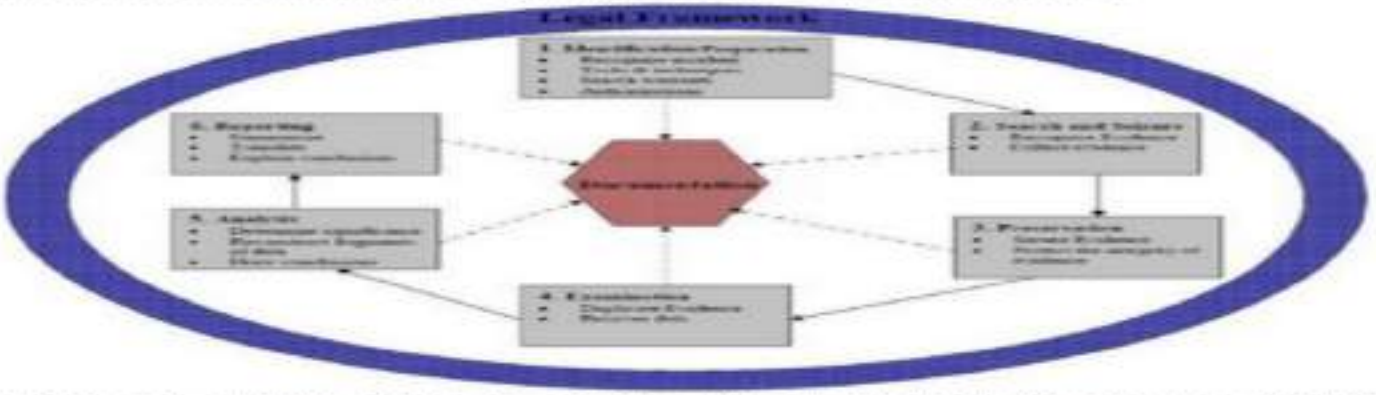
Search and Seizure of Computers

Search and seizure of computers is a common practice in cybercrime investigations. It involves the lawful collection and examination of electronic devices, including computers, laptops, smartphones, and storage media, to gather evidence of criminal activity. The process of search and seizure of computers in cybercrime investigations involves the following steps:

1. Obtaining a warrant: Before conducting a search and seizure operation, investigators must obtain a search warrant from a court. The warrant must describe the specific location to be searched and the items to be seized.
2. Securing the location: Once a warrant is obtained, investigators will secure the location to prevent any tampering or destruction of evidence.
3. Identifying and seizing electronic devices: Investigators will identify and seize electronic devices, such as computers and storage media, that are believed to contain evidence of criminal activity. Devices are typically labeled and secured in bags or boxes to prevent damage.
4. Conducting a forensic examination: Once electronic devices are seized, forensic examiners will conduct a thorough examination of the devices to gather evidence of criminal activity. This may include extracting data from hard drives, analyzing network traffic, and examining deleted files.



5. Documenting the evidence: All evidence collected during the search and seizure operation must be thoroughly documented, including the date and time of seizure, the location of the device, and the condition of the device when seized.



There are various types of search and seizure methods used in cybercrime investigations, including:

1. Physical search and seizure: This method involves physically seizing and searching computers or other digital devices at the location where the crime was committed or where the evidence is believed to be located. This method is often used in cases where there is a warrant or other legal authority to search and seize the devices.

2. Remote search and seizure: This method involves accessing and searching computers or other digital devices remotely, without physically seizing the devices. This method

2. Remote search and seizure: This method involves accessing and searching computers or other digital devices remotely, without physically seizing the devices. This method can be useful in cases where the devices are located in another jurisdiction or country, or where the physical seizure of the devices is not possible.

3. Consent search: This method involves obtaining the consent of the owner or user of the device to search and seize the device. This method can be useful in cases where the owner or user is cooperative and willing to allow access to the device.

4. Emergency search and seizure: This method involves seizing and searching the device without a warrant or consent in cases where there is an immediate threat to public safety or where evidence is in danger of being destroyed.

Recovering Deleted Evidences

- Digital Evidence is any information that is **stored or transmitted** in the **digital form** that a party at court can use at the **time of trial.**
- Digital evidence can be Audio files, and voice recordings, Address books and contact lists, Backups to various programs, including backups to mobile devices, Browser history, Cookies, Database, Compressed archives (ZIP, RAR, etc.) including encrypted archives, etc.

Techniques for recovering deleted evidence

- **File carving**: File carving involves using specialized software to identify and extract data fragments from unallocated space on a storage device. This technique can be useful for recovering deleted files or parts of files that have been partially overwritten.
- **Forensic imaging:** Forensic imaging involves creating a complete copy or image of a storage device or system, including all deleted data. This technique can be useful for preserving and analyzing the deleted data without modifying the original device.
- **Data carving:** Data carving involves searching for specific patterns or file types within the storage device, such as email messages or image files. This technique can be useful for recovering specific types of data that may have been deleted.

- **Backup analysis**: Backup analysis involves examining backup systems for any copies of the deleted data. This technique can be useful if the deleted data was backed up prior to its deletion.
- **Log analysis:** Log analysis involves examining system logs, network logs, or application logs for evidence of the deleted data being accessed or transmitted over the network. This technique can be useful for identifying when and where the data was deleted.

- **Slack space analysis**: Slack space refers to the unused portion of a file cluster that may contain fragments of deleted files. Slack space analysis involves searching for and recovering these fragments to reconstruct deleted files.
- **Registry analysis**: The registry is a database used by Windows to store system configuration information. Registry analysis involves examining the registry for evidence of deleted or modified keys or values related to the deleted data.
- **RAM analysis**: Random Access Memory (RAM) is volatile memory that stores data temporarily while a computer is in use. RAM analysis involves examining the contents of RAM to recover deleted or modified data that may not have been saved to disk

Password Cracking

- Password cracking is a technique used in cybercrime investigations **to gain access to password-protected data or systems.**
- Passwords are commonly used to **protect sensitive information**, and in cases where the **password is unknown or forgotten, cracking the password** can be a necessary step in the investigation.
- **Dictionary Attack**: This method uses a pre-defined list of common passwords, words, or phrases to guess a user's password. It works when the password is too simple or based on a common dictionary word.
- **Brute-Force Attack**: This technique involves trying all possible combinations of characters to guess the password. It is an effective method but can take a lot of time, depending on the length and complexity of the password

- **Hybrid Attack**: This method combines both the dictionary and brute-force attacks by using variations of words and phrases from a dictionary to create different password combinations.
- **Rainbow Table Attack**: This technique uses pre-computed tables that contain encrypted passwords and their corresponding plaintext values. Cybercriminals use these tables to quickly reverse the hashed password to its original form.
- **Social Engineering**: This technique involves tricking users into revealing their passwords through phishing scams, malicious websites, or other methods of deception

- **Shoulder Surfing**: This technique involves observing the user as they enter their password, either physically or remotely, to gain unauthorized access.
- **Man-in-the-Middle (MITM) Attack**: This technique involves intercepting communication between the user and the server to steal their login credentials.
- **Password Guessing**: This technique involves guessing the password based on personal information, such as the user's name, birthdate, or pet's name.

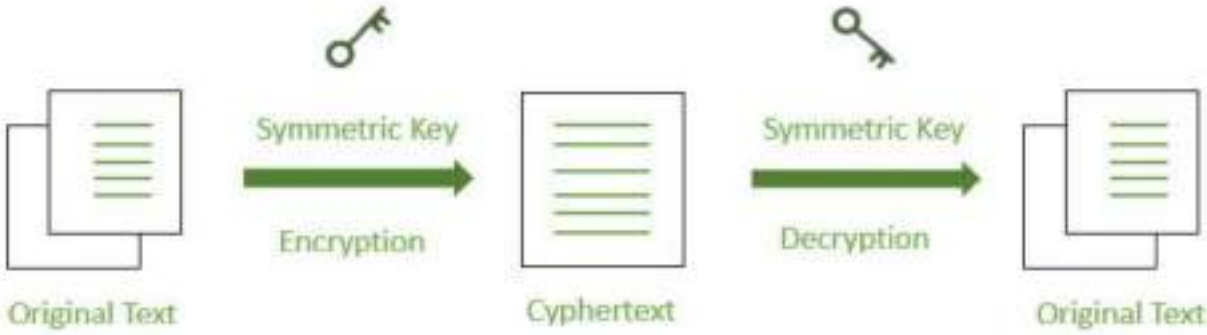
Data encryption

- It is a method of **preserving data confidentiality by transforming it into ciphertext,** which can only **be decoded using a unique decryption key produced at the time of the encryption or prior to it**.
- It converts data into a **different form (code**) that can only be accessed by people who have a **secret key** (**decryption key) or password**.
- Data that has **not been encrypted** is referred to as **plaintext**, and data that has been **encrypted** is **referred** to as **ciphertext**.
- It is one of the most widely used and **successful data protection technologies** in today's **corporate world**.
- It is a **critical tool for maintaining data integrity,** and its importance cannot be overstated.

Types of Data Encryption

- Symmetric Encryption
- Asymmetric Encryption

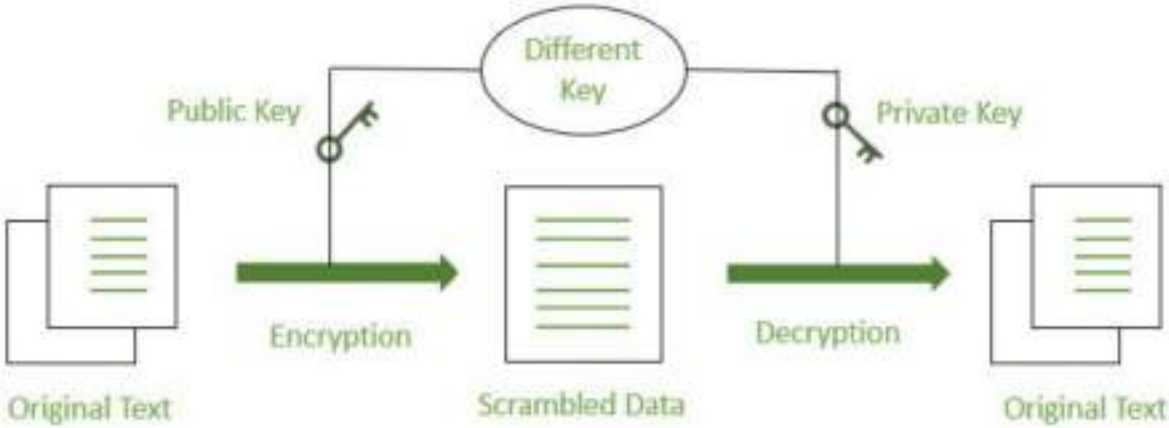
Symmetric Key Encryption:



Symmetric Key Encryption:

- It is called private-key cryptography or a secret key algorithm,this method requires the sender and the receiver to have access to the same key.
- So, the recipient needs to have the key before the message is decrypted. This method works best for closed systems, which have less risk of a third-party intrusion.
- On the positive side, symmetric encryption is faster than asymmetric encryption

Asymmetric Key Encryption

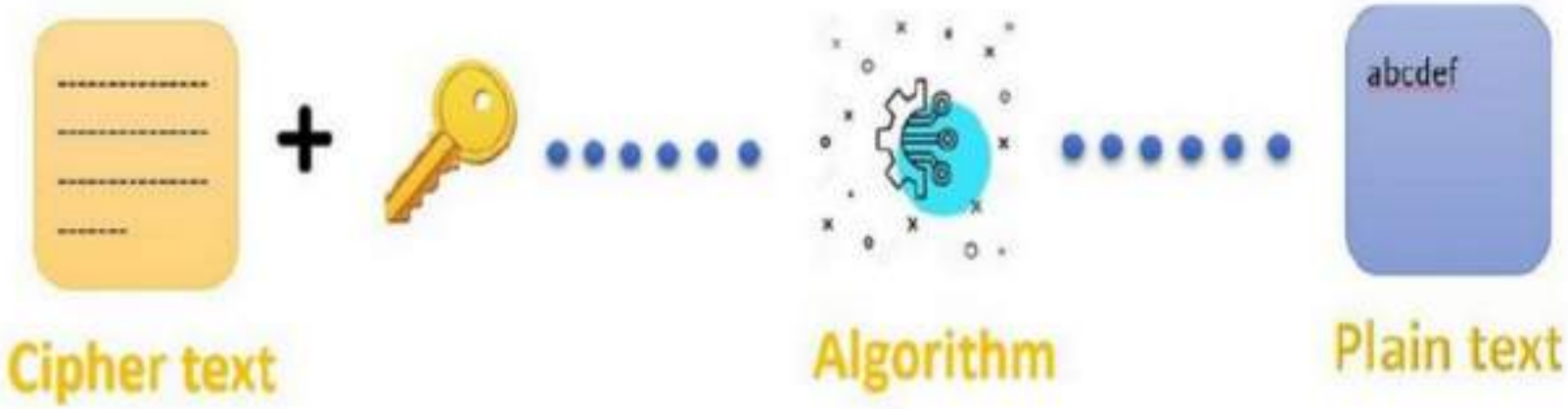


Asymmetric Key Encryption

- It is called **public-key cryptography**, this method uses **two keys** for the **encryption** process, a **public and a private key**, which are **mathematically linked**.
- The user employs **one key for encryption and the other for decryption**, though it doesn't matter which you choose first.
- As the name implies, the public key is freely available to anyone, whereas the private key remains with the intended recipients only, who need it to decipher the messages.
- Both keys are simply large numbers that **aren't identical** but are paired with each other, which is asymmetric

Decryption

- Decryption techniques is the process in which the **encrypted code or data is converted back to a form that is easily understandable** and readable by a human or machine.
- This is basically known as **decoding encrypted** data. It takes place at the **receiver end**.
- The message can be **decrypted either with the secret key or the private key.**



- **Symmetric Key**:
- This key helps in performing Symmetric Encryption also known as the Symmetric-key encryption algorithm. It uses the **same cryptographic keys for performing both the encryption of plaintext from the sender's side and the decryption of the cipher text on the receiver side**.

Asymmetric Key:

- Asymmetric key encryption algorithm uses two pairs of keys, which are used for encryption. These **two different keys are used for encrypting the data an for decrypting the data**. The **public key** is made available to anyone whereas the **secret key** is only made available to **the receiver side** of the message. This provides **more security as compared to symmetric key encryption.**

- **Public Key:**
- Public keys are the keys that are basically used to **encrypt the message** for the **receiver**. This cryptography is an encryption system that is **based on two pairs of keys.**
- **Private Key:**
- The private key usually used with the **asymmetric encryption** algorithm as one can use the **same key for encrypting and decrypting** the data. It also may be a part of the **public/private asymmetric key pair**.
- **Pre-Shared Key:**
- It also known as PSK, is a **shared secret key** that was earlier shared between **two different organizations** or people using a **secure channel** before it is used

1. Laws and Ethics:

Laws and ethics in the context of digital evidence handling concern the framework that guides the collection, preservation, analysis, and presentation of digital evidence in a manner that is legally admissible, ethical, and does not violate privacy rights.

- **Digital Evidence Control**: This pertains to the practices and policies that govern the access, handling, storage, and examination of digital data. This includes ensuring the integrity of the data by preventing tampering or unauthorized access.
- **Ethics in Digital Evidence**: It includes maintaining the confidentiality, privacy, and integrity of evidence, ensuring unbiased analysis, and adhering to the principles of fairness and justice in legal processes. Ethical concerns also include respecting human rights during investigations, avoiding misuse of power, and safeguarding data from illegal or malicious tampering.

2. Digital Evidence Controls:

Digital evidence refers to information stored or transmitted in digital form that can be used in legal proceedings. It includes data from computers, smartphones, cloud services, emails, social media platforms, and other electronic devices.

- **Chain of Custody**: The procedure to document and secure the evidence from the time it is collected until it is presented in court. Proper documentation ensures that the evidence has not been tampered with or altered in any way.
- **Authentication**: Evidence must be authenticated to prove that it is genuine and has not been altered. Techniques like hash functions (e.g., MD5, SHA-1) are often used to verify the integrity of digital files.
- **Data Collection and Preservation**: Digital evidence should be collected in a forensically sound manner using approved methods to avoid contamination. For example, using write-blockers to prevent altering the data on the source device during collection.

3. Evidence Handling Procedures:

- **Collection**: Evidence should be collected as soon as possible after an incident is detected to prevent data degradation or loss. Devices should be secured and turned off (if necessary) to preserve the data.
- **Preservation**: Ensuring that evidence is stored in a secure, unaltered environment. This could include creating duplicates of the original evidence (forensic imaging) and preserving the original data in a way that maintains its integrity.
- **Analysis**: The forensic analysis of digital evidence must be done by trained professionals using validated tools and methodologies. The goal is to extract, examine, and interpret data in a way that is admissible in court.
- **Presentation**: The evidence is then presented in court, and it must be clear, relevant, and obtained following proper legal procedures. The expert presenting the evidence must be able to explain the methodology used to acquire and analyze the data.

4. Basics of the Indian Evidence Act (IEA):

The **Indian Evidence Act (IEA)** governs the law of evidence in India, outlining the rules and regulations for admissibility of evidence, including digital evidence.

- **Section 65B (Admissibility of Electronic Records)**: This section deals with the admissibility of electronic records in court. Electronic records (such as emails, documents stored in computers, etc.) are admissible in court if they are accompanied by a certificate from the person responsible for managing the device or system, affirming that the record was created and maintained in the usual course of business.
- **Section 45A (Opinion of an Expert)**: Allows an expert to testify about the interpretation of electronic records or digital data. This is important in digital forensics, as experts may be needed to explain the significance of data recovered from electronic devices.

5. Indian Penal Code (IPC):

The **Indian Penal Code (IPC)** outlines offenses and penalties for various crimes, including those related to digital crimes:

- **Section 66 (Computer-related offenses)**: Deals with offenses like hacking, identity theft, cyberstalking, and data theft.
- **Section 66C (Identity Theft)**: Penalties for identity theft, including unauthorized access to or use of someone's personal data.
- **Section 67 (Publishing or transmitting obscene material in electronic form)**: Punishes the act of publishing or transmitting obscene content in any form, including through digital channels.

6. Criminal Procedure Code (CrPC):

The **Criminal Procedure Code (CrPC)** governs the procedures for the investigation and prosecution of criminal offenses in India. It outlines the powers of police and authorities in relation to digital evidence.

- **Section 91 (Summons to produce document or thing)**: This allows authorities to summon a person to produce digital evidence during investigations. For example, this could apply to producing emails, chat logs, or digital files.
- **Section 165 (Searches and Seizures)**: Allows police officers to seize digital evidence during searches, which can include computers, smartphones, or any digital device suspected of containing evidence relevant to a crime.

7. The Electronic Communications Privacy Act (ECPA):

This is a US-based legislation, but the principles of protecting electronic communications are mirrored in India's laws.

- **ECPA** protects the privacy of electronic communications by restricting unauthorized interception or access to communications while they are being transmitted or stored.
- **In India**, the **Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011**, and **Section 72A of the IT Act (Disclosure of information in breach of lawful contract)** offer similar privacy protections for communications and personal data.

8. Legal Policies Related to Digital Evidence:

Legal policies governing digital evidence ensure that evidence handling, collection, and analysis adhere to ethical and legal standards.

- **Information Technology Act, 2000 (IT Act)**: Governs offenses related to computers and digital communication, including hacking, identity theft, and cybercrime. It also deals with legal aspects of digital signatures, electronic records, and online contracts.
- **Data Privacy and Protection Laws**: The **Personal Data Protection Bill, 2023** is a significant step in data privacy, outlining how organizations should handle, process, and store personal data, particularly in the digital space.

Conclusion:

The handling of digital evidence in India requires a sound understanding of legal frameworks such as the Indian Evidence Act, IPC, and CrPC, along with careful compliance with procedures for evidence collection and analysis. Digital evidence policies and laws, including the IT Act and the Electronic Communications Privacy Act, protect privacy and ensure fairness in legal proceedings involving electronic data. Ethical considerations, such as ensuring the integrity of digital evidence and respecting privacy rights, are fundamental in the digital age.