DIGITAL NOTES
ON
CYBER CRIME INVESTIGATIONS
AND
DIGITAL FORENSICS
(R22A6205)

B.TECH III YEAR – II SEM (R22)

(2024-2025)

DEPARTMENT OF EMERGING TECHNOLOGIES

MALLA REDDY COLLEGE OF ENGINEERING & TECHNOLOGY

(Autonomous Institution – UGC, Govt. of India)

Recognized under 2(f) and 12 (B) of UGC ACT 1956

(Affiliated to JNTUH, Hyderabad, Approved by AICTE - Accredited by NBA & NAAC – 'A' Grade - ISO 9001:2015 Certified)

Maisammaguda, Dhulapally (Post Via. Hakimpet), Secunderabad – 500100, Telangana State, India

MALLA REDDY COLLEGE OF ENGINEERING ANDTECHNOLOGY

III Year B.Tech CSE (CyS) – II Sem **L/T/P/C**

3/0/0/3

(R22A6205) CYBER CRIME INVESTIGATIONS AND DIGITAL FORENSICS

Course Objectives: To analyze how to conduct a digital forensics investigation and validate forensics data.

Course Outcomes:

1. Understand the fundamentals of cybercrime and issues.
2. Understand different investigation tools for cybercrime.
3. Understand basics of Forensic Technology and Practices.

Analyze different laws, ethics and evidence handling procedures

UNIT - I

Introduction: Introduction and Overview of Cyber Crime, Nature and Scope of Cyber Crime, Types of Cyber Crime: Social Engineering, Categories of Cyber Crime, Property Cyber Crime.

UNIT - II

Cyber Crime Issues: 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.

UNIT - III

Investigation: Introduction to Cyber Crime Investigation, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Hands on Case Studies. Encryption and Decryption Methods, Search and Seizure of Computers, Recovering Deleted Evidences, Password Cracking.

UNIT - IV

Digital Forensics: 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.

UNIT - V

Laws and Acts: Laws and Ethics, Digital Evidence Controls, Evidence Handling Procedures, Basics of Indian Evidence ACT IPC and CrPC, Electronic Communication Privacy ACT, Legal Policies.

UNIT 1

Introduction:

Cyber crime is a global threat and the evidence suggests that this threat will continue to rise. It is defined as any criminal activity which takes place on or over the medium of computers or internet other technology recognized by the information technology act. There are number of illegal activities which are committed over the internet by technically skilled criminals.

Cyber crime is an uncontrollable evil having its base in the misuse of growing dependence on computers in modern life.

NATURE AND SCOPE OF CYBER CRIME:

As we all know, we live in era where most things are done over the internet, from online dealing to online transactions because the internet technology is considered a global stage.

What is Cybercrime?

Cybercrime can be defined as "The illegal usage of any communication device to commit or facilitate in committing any illegal act" or in other terms "A crime or an unlawful act where unauthorized access to some computer system without the permission of rightful owner or place of criminal activity and includes everything from online cracking to denial of service attacks.

Criminal activity is a social concept we will never be able to live in a society without cybercrime no matter how hard we try.

CHARACTERISTICS OF CYBERCRIME:

- Cybercrimes are unlawful Act.
- Computer is essentially an element of cyber criminality and it is either a tool or target of cybercrimes.
- Cybercrimes are harmful Act.
- Cybercrimes are committed in cyber space with the help of computer networking.
- Cybercrime is a criminal activity where computer can be used to perpetuate further crime.

WHAT IS 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 involves the use of specialized tools and techniques to investigate various types of cybercrimes, such as hacking, phishing, malware, data breaches, and identity theft.

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 tool in order to effectively investigate and mitigate cybercrimes.

TYPES OF CYBERCRIMES:

Cybercrime take many different forms, criminal who infiltrate computers and networks have developed a variety of malicious software and social engineering techniques used individually or in combination when use in in committing different types of cybercrimes. A few of the most common cybercrimes are described below.

❖ DDOS ATTACKS:

DDoS attacks are used to make an online service unavailable and take the network down by overwhelming the site with traffic from a variety of sources. Large networks of infected devices known as Botnets are created by depositing malware on users' computers. The hacker then hacks into the system once the network is down.

❖ MALWARE:

Malware or malicious software refers to any code designed to interfere with a computers normal functioning or commit a cyber crime. Common types of malware includes viruses, worms, trojans, rootkit, rogue software and various hybrid programs as well as adware, spyware, scareware and ransomware. Malware can be used to exfiltrate data, steal passwords, lock users out of their environment, destroy network resources or commandeer them to power botnets–regardless of the tactic the consequences of a successful malware attack can be severe.

❖ CYBER STALKING:

This kind of cybercrime involves online harassment where the user is subjected to a plethora of online messages and emails. Typically cyberstalkers use social media, websites and search engines to intimidate a user and instill fear. Usually, the cyberstalker knows their victim and makes the person feel afraid or concerned for their safety.

❖ IDENTITY THEFT:

Identity theft occurs when someone "unlawfully obtains another individuals personal information and uses it to commit theft or fraud". Malware such as trojans and spyware are often used to steal personal information. Identity theft includes personal information such as name, Aadhar number, drivers license number, credit card number, or other identifying information.

❖ BOTNETS:

Botnets are networks from compromised computers that are controlled externally by remote hackers. The remote hackers then send spam or attack other computers through these botnets. Botnets can also be used to act as malware and perform malicious tasks.

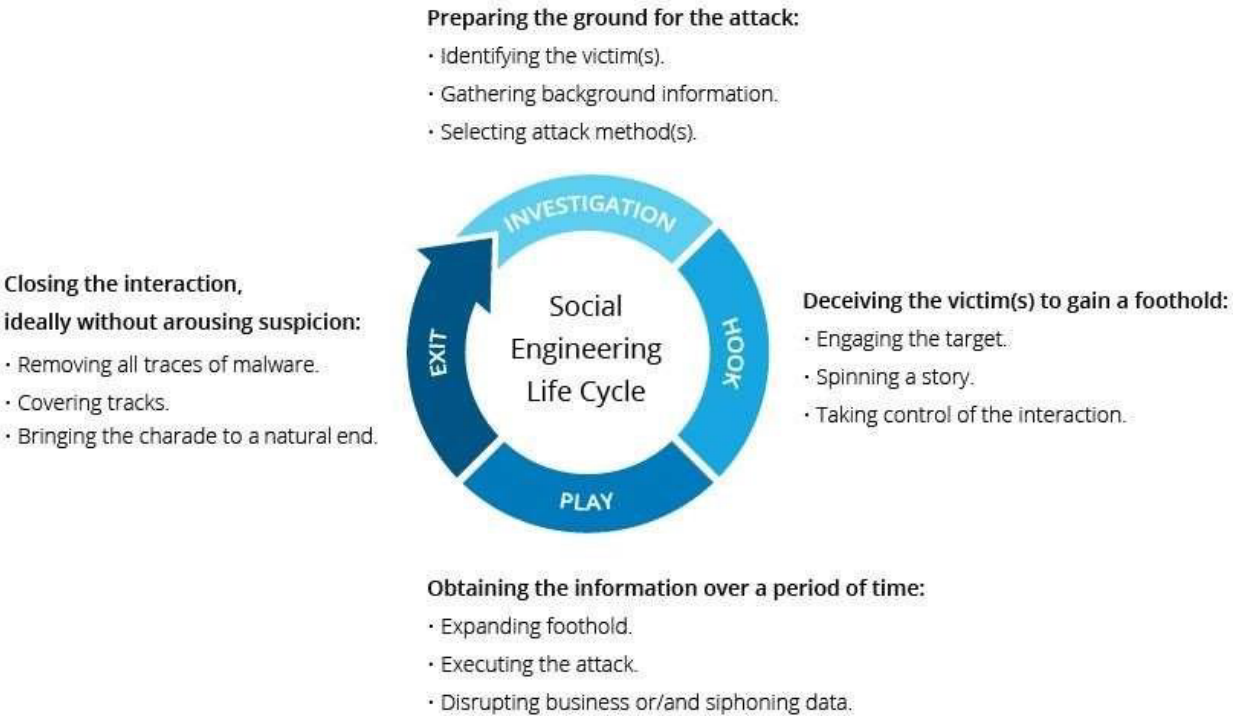
One of the example of Botnet is Fraud Online Review, where some fake reviews are generally posted on the device of the user.

❖ SOCIAL ENGINEERING:

Social engineering is the psychological manipulation of people into performing actions or divulging confidential information. Cyber criminals use social engineering to commit fraud online.

One of the biggest weaknesses in any organization cybersecurity strategy is human error. Social engineering attacks take advantage of this vulnerability by conning unsuspecting people into compromising security and giving out sensitive information. Social engineers use various psychological hacks to trick you into trusting them or create a false sense of urgency and anxiety to lower your natural defenses.

Scammers use many different types of social engineering attacks, but some common giveaways can help you spot and avoid them.



TYPES OF SOCIAL ENGINEERING ATTACKS:

- **Phishing:**

Phishing is the most common type of social engineering attack, typically using spoofed email addresses and links to trick people into providing login credentials, credit card numbers, or other personal information. Variations of phishing attacks include:

- Angler phishing – using spoofed customer service accounts on social media
- Spear phishing – phishing attacks that target specific organizations or individual

- **Whaling:**

Whaling is another common variation of phishing that specifically targets top-level business executives and the heads of government agencies. Whaling attacks usually spoof the email addresses of other high-ranking people in the company or agency and contain urgent messaging about a fake emergency or time-sensitive opportunity. Successful whaling attacks can expose a lot of confidential, sensitive information due to the high-level network access these executives and directors have.

- **Diversion Theft:**

In an old-school diversion theft scheme, the thief persuades a delivery driver or courier to travel to the wrong location or hand off a parcel to someone other than the intended recipient. In an online diversion theft scheme, a thief steals sensitive data by tricking the victim into sending it to or sharing it with the wrong person. The thief often accomplishes this by spoofing the email address of someone in the victim's company—an auditing firm or a financial institution, for example.

- **Baiting:**

Baiting is a type of social engineering attack that lures victims into providing sensitive information or credentials by promising something of value for free. For example, the victim receives an email that promises a free gift card if they click a link to take a survey. The link might redirect them to a spoofed Office 365 login page that captures their email address and password and sends them to a malicious actor.

- **Honey Trap:**

In a honey trap attack, the perpetrator pretends to be romantically or sexually interested in the victim and lures them into an online relationship. The attacker then persuades the victim to reveal confidential information or pay them large sums of money.

- **Pretexting:**

Pretexting is a fairly sophisticated type of social engineering attack in which a scammer creates a pretext or fabricated scenario—pretending to be an IRS auditor, for example—to con someone into providing sensitive personal or financial information, such as their social security number. In this type

of attack, someone can also physically acquire access to your data by pretending to be a vendor, delivery driver, or contractor to gain your staff's trust.

- **SMS Phishing:**

SMS phishing is becoming a much larger problem as more organizations embrace texting as a primary method of communication. In one method of SMS phishing, scammers send text messages that spoof multi-factor authentication requests and redirect victims to malicious web pages that collect their credentials or install malware on their phones.

Scareware:

Scareware is a form of social engineering in which a scammer inserts malicious code into a webpage that causes pop-up windows with flashing colors and alarming sounds to appear. These pop-up windows will falsely alert you to a virus that's been installed on your system. You'll be told to purchase and download their security software, and the scammers will either steal your credit card information, install real viruses on your system, or (most likely) both.

Tailgating/Piggybacking:

Tailgating, also known as piggybacking, is a social engineering tactic in which an attacker physically follows someone into a secure or restricted area. Sometimes the scammer will pretend they forgot their access card, or they'll engage someone in an animated conversation on their way into the area so their lack of authorized identification goes unnoticed.

Watering Hole:

In a watering hole attack, a hacker infects a legitimate website that their targets are known to visit. Then, when their chosen victims log into the site, the hacker either captures their credentials and uses them to breach the target's network, or they install a backdoor trojan to access the network.

CATEGORIES OF CYBER CRIME

There are three major categories of cyber crimes:

1. Crimes Against People:

These crimes include cyber harassment and stalking, distribution of child pornography, credit card fraud, human trafficking, spoofing, identity theft, and online libel or slander.

Harassment via E-Mails: This is very common type of harassment through sending letters, attachments of files & folders i.e. via e-mails. At present harassment is common as usage of social sites i.e. Facebook, Twitter, Orkut etc. increasing day by day.

Cyber-Stalking: It is expressed or implied a physical threat that creates fear through the use to computer technology such as internet, e-mail, phones, text messages, webcam, websites or videos.

Defamation: It involves any person with intent to lower down the dignity of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.

Hacking: It means unauthorized control/access over computer system and act of hacking completely destroys the whole data as well as computer programs. Hackers usually hacks telecommunication and mobile network.

Cracking: It is act of breaking into your computer systems without your knowledge and consent and has tampered with precious confidential data and information.

E-Mail Spoofing: A spoofed e-mail may be said to be one, which misrepresents its origin. It shows it's origin to be different from which actually it originates.

SMS Spoofing: Spoofing is a blocking through spam which means the unwanted uninvited messages. Here a offender steals identity of another person in the form of mobile phone number and sending SMS via internet and receiver gets the SMS from the mobile phone number of the victim. It is very serious cyber crime against any individual.

Carding: It means false ATM cards i.e. Debit and Credit cards used by criminals for their monetary benefits through withdrawing money from the victim's bank account. There is always unauthorized use of ATM cards in this type of cyber crimes.

Cheating & Fraud: It means the person who is doing the act of cyber crime i.e. stealing password and data storage has done it with having guilty mind which leads to fraud and cheating.

Child Pornography: In this cyber crime defaulters create, distribute, or access materials that sexually exploit underage children.

Assault by Threat: It refers to threatening a person with fear for their lives or lives of their families through the use of a computer network i.e. E-mail, videos or phones.

2. Crimes Against Property:

This is similar to a real-life instance of a criminal illegally possessing an individual's bank or credit card details. The hacker steals a person's bank details to gain access to funds, make purchases online or run phishing scams to get people to give away their information. They could also use a malicious software to gain access to a web page with confidential information.

Intellectual Property Crimes: Any unlawful act by which the owner is deprived completely or partially of his rights is an crime. The most common type of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.

Cyber Squatting: It involves two persons claiming for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously.

Cyber Vandalism: Vandalism means deliberately damaging property of another it includes destroying or damaging the data or information stored in computer when a network service is stopped or disrupted. These acts may take the form of the theft of a computer, some part of a computer.

Hacking Computer System: Hackers attacks those included Famous Twitter, blogging platform by unauthorized access/control over the computer. Those attacks were not mainly intended for financial gain too and to diminish the reputation of particular person or company. As in April, 2013 MMM India attacked by hackers.

Transmitting Virus: Viruses are programs written by programmers that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network with intent of altering or deleting it.

Cyber Trespass: It means to access someone's computer or network without the right authorization of the owner and disturb, alter, misuse, or damage data or system by using wireless internet connection.

Internet Time Thefts: Basically, Internet time theft comes under hacking. It is the use by an unauthorized person, of the Internet hours paid for by another person. The person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge.

3. Crimes Against Government:

When a cybercrime is committed against the government, it is considered an attack on that nation's sovereignty.

This is the least common cybercrime, but is the most serious offense. A crime against the government is also known as cyber terrorism. Government cybercrime includes hacking government websites, military websites or distributing propaganda. These criminals are usually terrorists or enemy governments of other nations.

Cyber Terrorism: Cyber terrorism is a issue in the domestic as well as global concern. Terrorist attacks on the Internet are by distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer network etc. Cyber terrorism activities endanger the sovereignty and integrity of the nation.

Cyber Warfare :- It refers to politically motivated hacking to conduct sabotage and espionage.

Distribution of printed software:- It means distributed printed software from one computer to another intending to destroy the data and official records of the Government.

Possession of unauthorized information:- It is very easy to access any information by the terrorist with the aid of internet and to possess that information for political, religious, social, ideological objectives

ACCORDING TO INDIAN CYBERCRIME COORDINATION CENTRE(I4C)
CYBERCRIME CATEGORIES :

1. **CRYPTOCURRENCY CRIME**:

   - **Crypto jacking:** Cryptojacking is a type of cybercrime where a criminal secretly uses a victim's computing power to generate cryptocurrency.
   - **Crypto Mining & Cloud Mining Scams:** Cryptocurrency-mining malware steal the resources of infected machines, significantly affecting their performance, power consumption and increasing their wear and tear.
   - **Cryptocurrency Investment Frauds:** Fraudulent opportunity to invest in a cryptocurrency with guaranteed high returns e.g. "pump and dump" scams, giveaway scams, etc.

2. **CYBER TERRORISM**:

   Cyber Terrorism" is committed with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

   - denying or cause the denial of access to any person authorised to access computer resource; or
   - attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or
   - introducing or causing to introduce any computer contaminant, and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure.

   Cyberterrorism is also committed when somebody knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer data base that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer data base, with reasons to believe that such information, data or

computer data base so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

3. **HACKING/DAMAGE TO COMPUTER SYSTEMS**:

The act of compromising computer resources through unauthorized access to an account or computer system. It is accessing of a computer system without the express or implied permission of the owner of that computer system.

Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking. Hacking / Damage to Computer Systems includes;

- Damage to computer, computer systems, etc.
- Email Hacking.
- Tampering with computer source documents.
- Unauthorised Access / Data Breach.
- Website Defacement / Hacking.

4. **ONLINE AND SOCIAL MEDIA RELATED CRIME**:

Online and Social media crimes in the country have been rising, posing new challenges as cyber criminals keep evolving their methods, using emerging technology. Various Cybercrimes categorized under Online and Social Media Related Crime in the portal are as follows:

- Cheating by Impersonation

- Cyber Bullying / Stalking / Sexting
- E-Mail Phishing
- Fake/Impersonating Profile
- Impersonating Email
- Intimidating Email
- Online Job Fraud
- Online Matrimonial fraud
- Profile Hacking / Identity Theft
- Provocative Speech for unlawful acts

5. **ONLINE FINANCIAL FRAUD**:
   Online Financial Cybercrimes include unauthorized access, sabotage, or use of computer systems with the intention to cause financial gain by cyber criminals or financial loss to the victims. It may involve computer fraud or forgery, hacking to steal personal or valuable data for commercial gain. With the increase in the use of the internet and mobile banking, online financial frauds are increasing.

Various Cybercrimes categorized under the category of Online financial fraud are as follows:

- Business Email Compromise/Email Takeover
- Debit/Credit Card Fraud/Sim Swap Fraud
- Demat/Depository Fraud
- E-Wallet Related Fraud
- Fraud Call/Vishing
- Internet Banking Related Fraud
- UPI Fraud

6. **Publishing/Transmitting Of Explicit Material In Electronic Form**:

Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which contains sexually explicit act or conduct, or any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it shall be punished under Section 67 or 67A of IT Act.

7. RANSOMWARE:

Ransomware is a rapidly evolving form of Cybercrime, through which cyber criminals remotely compromise and encrypt computer systems and demand a ransom in return for restoring and/or for not exposing data. Ransomware attacks target individuals and Organisations.

Ransomware attack blocks user's access to the data stored in the computer systems. More menacing versions of ransomware can encrypt files and folders on local drives, attached drives, and even networked computers.

8. CHILD PORNOGRAPHY/CHILD SEXUAL ABUSE MATERIAL(CSAM):

Child sexually abusive material (CSAM) refers to a material containing sexual image(s) in any form, of a child who is abused or sexually exploited. It is punishable to publish or transmit material

depicting children in sexually explicit act or conduct in any electronic form. It is covered under **Section 67B of IT Act 2000**. Child pornography is a form of child sexual exploitation. The production, distribution, importation, reception, or possession of any image of child pornography is prohibited. Violation of child pornography/CSAM laws is a serious crime.

PROPERTY CYBER CRIME : 3rd category as mention above which includes intellectual property.

UNIT-2 Cyber Crime Issues

UNAUTHORIZED ACCESS TO COMPUTERS:

Unauthorized access is when someone, internally or externally, gains access to a computer system, network, or data without permission. Here's how you can detect and prevent anyone gaining unauthorized access on your devices.

Definition: Unauthorized access is the process of gaining entry to computer resources without permission. It could be a system, network, software, or data. Sometimes a person has permission to access certain resources, but their device doesn't (like when someone uses a personal laptop to connect to the work environment) — it all depends on the company's security policy.

Unauthorized access is typically committed by hackers, and sometimes unwitting users. Someone who already has access to a system could accidentally stumble upon unsecured files that weren't meant for their eyes. Either way, someone having access to unauthorized computer systems or data is typically a violation of a company or businesses' security and privacy policy.
People can gain unauthorized access through a whole number of reasons, some as simple as a user accidentally guessing a password for sensitive files or data. Others, however, can be sophisticated attacks that take weeks of planning and could even involve corporate espionage. Cybercriminals could even go so far with their deception to gain enough trust to be an authorized person.

RISKS OF UNAUTHORIZED ACCESS:

The risks of unauthorized access are severe enough to warrant immediate protection. Those who specifically seek out accessing unauthorized spaces usually do so for one of the following purposes:

- Disrupt electronic systems. Some hackers just want to be an annoyance or play pranks. Accessing unauthorized data is a good way for them to instantly have a company or business forced into high-alert, and potentially instigate a shutdown of all systems.

- **Harm the target.** Unauthorized data is usually sensitive and could be damaging or damaging to the victim. If someone without permission gains access, they can cause a major headache for the victim, including instigating a data breach.

- **Steal data.** Stealing data is probably the most common way someone would want to access unauthorized data. Once the data is stolen, it can be used to hold a person, business, or company ransom. Exposed and stolen credentials are often the first victim of a data breach.

- **Cause physical damage.** Depending on the systems accessed without permission, a hacker can cause physical damage to devices connected to the network

What is the long-term damage of unauthorized access?

- **Damage to the reputation of the company**. Depending on how public facing the victim's company or business is, it could cause a loss of trust among its users or customers. Lose enough trust, and users will move on to another platform.

- **Government fines**. In most parts of the world, many organizations and companies need to adhere to a specific set of online security measures and regulations. If your systems are weak enough that someone gained unauthorized access and caused damage to potentially thousands of people, it could result in the government or security agencies coming down hard on your company with a heavy fine.

- **Fallout costs.** Not only do you risk government fines after someone has gained unauthorized access, but you will also have to pay for repairs and business down time. To compound the problem even more, you may even have to pay out to the various victims who were affected by shoddy cybersecurity. Reparations could cost upwards of tens of millions of dollars

Tips to detect and prevent unauthorized access

1. **Adopt the principle of least privilege** The principle of least privilege calls for establishing user access review procedures and regularly checking user privileges to ensure that users have minimal access to sensitive data and critical systems. Consider giving your employees just enough access privileges to perform their core responsibilities. With that, you can implement a just-in-time approach to grant them temporary additional access when needed.
2. **Implement a strong password management policy** Consider implementing a strong password management policy that will help you with creating, managing, and safeguarding user credentials. The right policy can also help you to adopt healthy password habits and maintain adequate password complexity, length, and uniqueness, as well as to regularly rotate passwords. For example, you can stick to HIPAA, NIST, or PCI DSS compliance password policy depending on the industry your organization operates in. Furthermore, a password management policy should outline the individuals or roles accountable for generating and overseeing user passwords within your organization. By adhering to a well-defined policy, your organization can enhance its overall password security and reduce the risk of unauthorized access.
3. **Use multi-factor authentication** Along with protecting your passwords, the next big step to protect your accounts is to apply multi-factor authentication (MFA). Unauthorized access frequently occurs due to the exploitation of a single compromised account or user credentials. Enforcing multi-factor authentication, though, can effectively stop such unauthorized access attempts. Requiring an additional identity verification step, such as sending a one-time passcode to a user's mobile device, will prevent unauthorized actors from proceeding. CISA emphasizes that MFA is a simple way to protect your organization against account compromise attacks. According to Microsoft, adopting MFA can prevent approximately 99.9% of account compromise cases, significantly bolstering security measures against unauthorized access.
4. **Monitor user activity** Monitoring user activity can help you detect and prevent unauthorized access, insider threats, and potential security breaches. By monitoring who does what in your

organization's IT infrastructure, you'll be able to quickly detect signs of unauthorized activity. That's why it's crucial to set up a comprehensive user activity monitoring (UAM) solution that can capture and analyze user activity within your system. UAM solutions typically provide lots of different features. We recommend choosing session recording software that enables monitoring of log files, system events, network traffic, and other user activity to help you identify any unusual or suspicious patterns that may indicate unauthorized access or other cybersecurity incidents

5. **Maintain secure IT infrastructure** To enhance protection against unauthorized access, combine your monitoring software with a resilient firewall. Whereas monitoring software can detect insider threats in real time, a firewall can serve as a protective barrier, shielding networks, web applications, databases, and critical systems from unauthorized intrusions. It's also critical for organizations to conduct regular vulnerability assessments and penetration testing of corporate IT infrastructure. One of the most neglected security threats is failing to update protection systems promptly. The 2023 MOVEit transfer data breach, during which the data of multiple global organizations was compromised, is a telling example of how system vulnerabilities can lead to catastrophic consequences. Cybercriminals exploited a critical zero-day vulnerability in MOVE it systems and compromised data from more than 2,500 organizations, which affected approximately 60-65 million individuals.
6. **Employ user behavior analytics** Consider implementing user entity and behavior analytics (UEBA) to analyze user activity patterns, access logs, and behavior profiles. By establishing a baseline of normal user behavior, UEBA tools automatically identify anomalies that may indicate unauthorized access, malicious activity, and account compromise. For example, if a user suddenly logs in to a system at an unusual time or from an unknown device, UEBA tools may notify your security officers. The security team can then investigate the issue and respond quickly.
7. **Promptly respond to cybersecurity incidents** Your security team needs to respond to security alerts immediately. For example, if you detect suspicious login attempts from an account, your security officers should be able to revoke account access immediately and block the session to prevent an intrusion. Ideally, you should also have a well-structured incident response plan outlining the responsibilities of your incident response team and providing clear steps to follow in case of an unauthorized access attempt or a security incident.
8. **Conduct security awareness training** As attackers frequently target people rather than machines, you should shift from a technology-centric to a people-centric cybersecurity approach and make your employees your first line of defense. For this, regularly conduct security awareness training to keep employees up-to-date with the latest cybersecurity threats and educate them about security best practices, including how to identify suspicious activities.

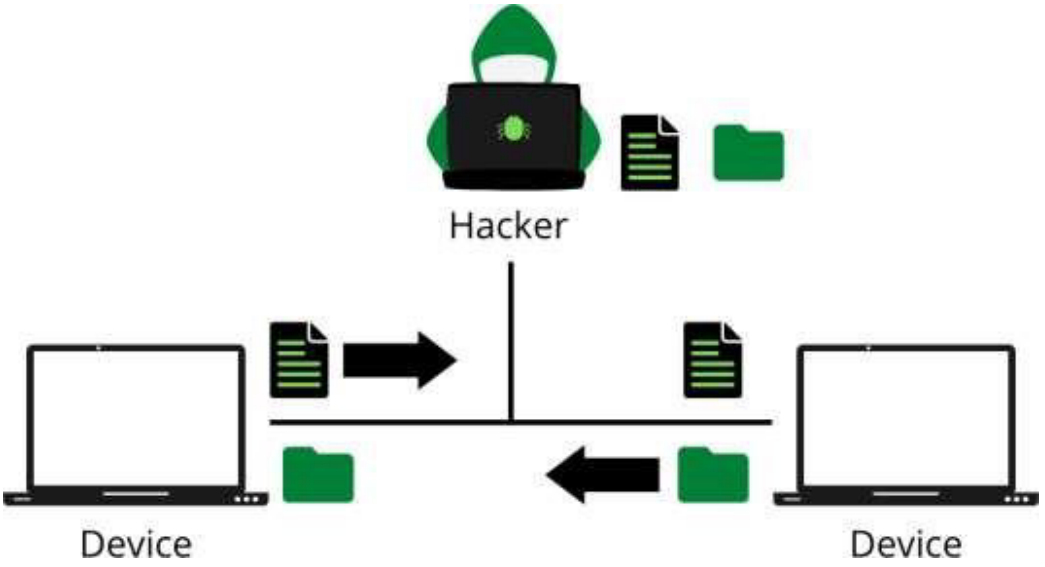
Computer Intrusions:

When someone tries to access any part of our personal computer system then PC intrusion occurs. Every Personal Computer (PC) which is connected to the internet is a target of hackers and cybercriminals.

There are several ways an intruder can try to gain access to your computer. They can:

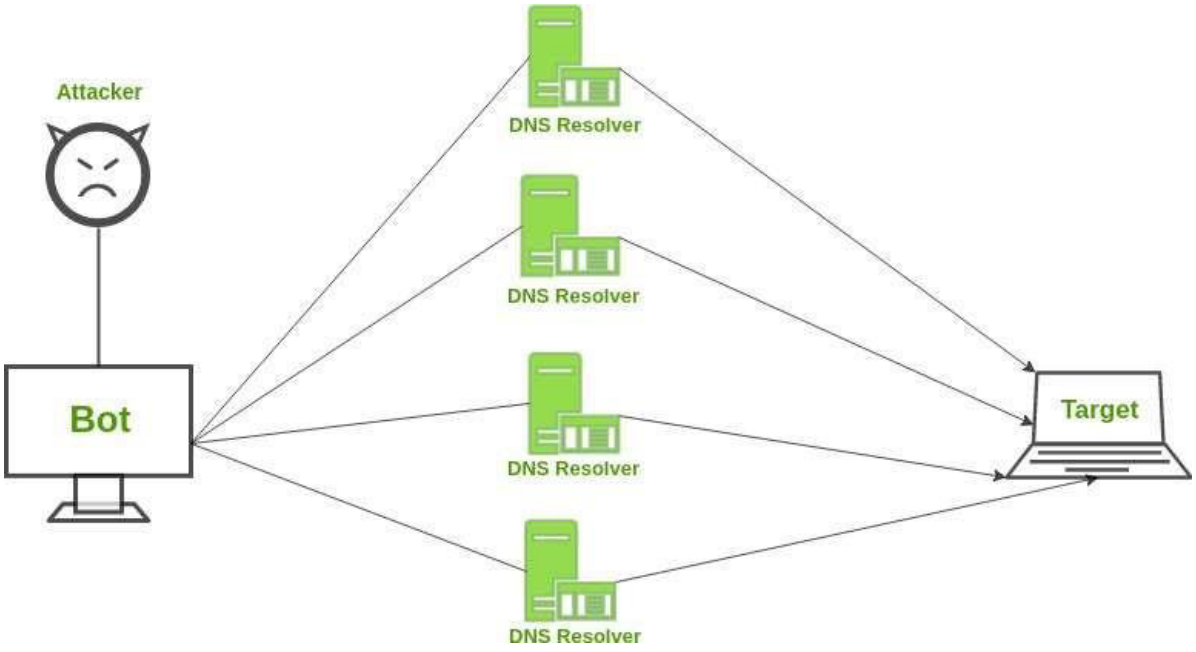
1. Access your computer to view, change, or delete information from your computer: Once the attacker got access to the computer, initially attacker will attempt to view the information, if the information is valuable attacker may sell the collection information to gain financial benefits. An attacker may delete or change information if the objective of the attack is to distract the smooth functionality of computer.

2. Crash or slow down your computer: The system may get crash if the attacker deletes system files, bootstrap loader file, bootstrap loader file is responsible to load the operating system. System performance may get slow if the system file is deleted or modified.
3. Access your private data by examining the files on your system: Once the attacker got access to the system, he may access private or sensitive data of the system. After analysis of this data, an attacker may get valuable information that may be misused or sold to a third party for financial gain.
4. Use your computer to access other computers on the Internet User's computer is connected in network, if the attacker got access user's system. He may use the user machine to get access to another network machine by executing various commands such as ping, traceroute, dig, etc.

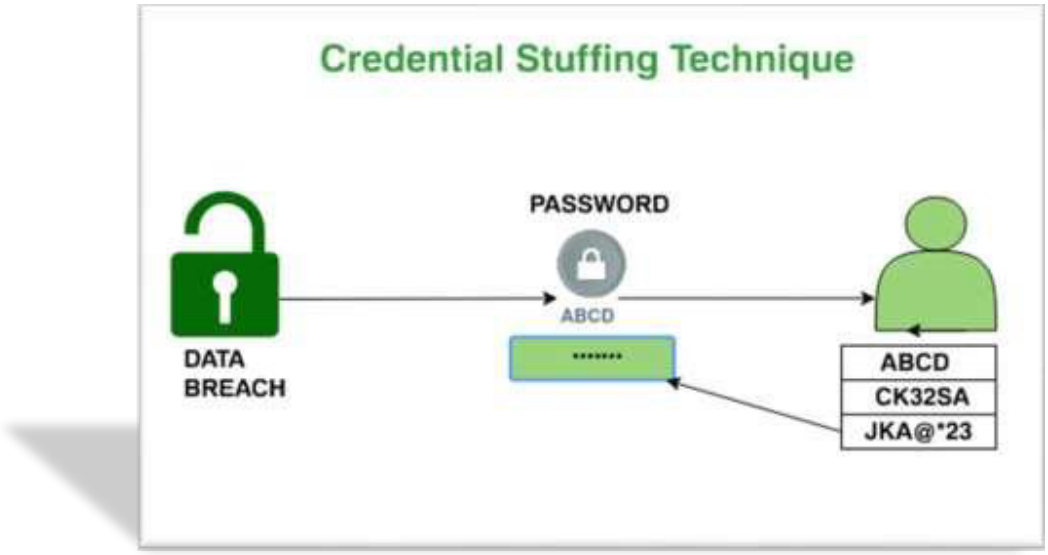


Personal Computer Intrusion can occur in any of the following forms:

- **Sweeper Attack:** Cybercriminals erase all the information or data like cache, cookies, internet history, or documents from the system by a malicious program.
- **Denial of Services:** DDos type of attack in which attackers may shut down the PC services making it irascible to its original user. All the system applications and stored resources come to a halt.



- **Password Guessing:** Most hackers crack passwords of system accounts by guessing and gaining remote entry into our personal computer system. Hackers can use this form and may damage the security system in our PC.



- **Snooping:** Snooping refers to opening and looking through files in an unauthorized manner. Snooping may involve many types of things such as gaining access to data in an unauthorized way, casually observing someone else's email, or monitoring the activity of someone else's computer through sophisticated snooping software. It involves monitoring keystrokes pressed

on the keyboard, capturing of passwords and login information, interception of emails and other private communication, and data transmission.

- **Eavesdropping:** When cyber vandals or attackers listen to a conversation that is traveling over devices like computers, servers, or other network devices, it is called eavesdropping. Formally we can say that the intentional interception of someone else's data as it passes through a user's computer to a server or vice-versa is called eavesdropping.

White collar crimes:

A white-collar crime is defined as a crime involving the theft of money from a place of business. The persons committing these crimes are usually those in influential positions, such as CEOs and management. Crimes of this type can cost citizens a great deal of money.

These crimes are different from other forms of crime because white-collar crimes are complex and challenging to take legal action against, entailing elaborate systems and encompass numerous people, making the case difficult to prosecute. Some white-collar crime examples are:

- Fraud
- Bribery
- Extortion
- Embezzlement
- Cybercrime

White-Collar Crime Meaning: Sociologist Edwin Sutherland first coined the term white-collar in 1949; he defined white-collar crime as a crime committed against a company. The person committing this crime holds respect and high social status within the business and often the community.

These types of workers wear a shirt and tie to work, thus the white-collar reference. Criminals of this type often work in an office setting and do not get their hands dirty, so to speak.

Fraud occurs when an employee lies about company facts to achieve financial gain and is told under pretense, which means a lie is told in the hopes the victim will act upon the false facts. If the victim does take action, the result is financial injury. Fraud is the most common white-collar crime because it covers many offenses.

Types of white-collar fraud include:

- Corporate Fraud
- Money Laundering
- Securities and Commodities Fraud

- Corporate fraud is usually committed on a large scale. Many people throughout the company are involved in this type of crime. The FBI names corporate fraud as its highest priority when it comes to prosecution because this crime brings significant loss to investors and harm to the U.S. economy and its citizens.
- Money Laundering occurs when unclean cash is filtered through a legitimate business. Unclean cash is any money made through illicit means, such as drug trafficking and terrorist activities. The money needs to be clean or laundered through a legitimate business to make it look like it was earned lawfully.

- Securities and commodities fraud is an umbrella term for investment fraud such as Ponzi and pyramid schemes. The perpetrators of this type of fraud are often stockbrokers, investment banks, or brokerage firms. The criminals falsify corporate information to con future investors into making a deal.

Bribery: It is a form of cyber corruption that involves offering or accepting gifts, entertainment, or payments to gain an advantage or retain business. This can include offering or accepting payments from government officials or other entities in exchange for favorable treatment.

Extortion: Extortion involves obtaining something, especially money, through force or threats. It's a white collar crime often committed by individuals in positions of power. An example of extortion could involve a public official who demands bribes in return for granting contracts. The victims of extortion can suffer financial loss, emotional distress, and in the case of businesses, reputational damage.

Extortionists may use threats of violence, expose damaging information, or manipulate the victim's fears to get what they want. Extortion is a criminal act punishable by law, with penalties varying based on the severity of the act and the laws of the jurisdiction.

Embezzlement: Another form of white collar crime is embezzlement, which occurs when an individual entrusted with someone else's money or property illegally takes it for personal use. This could involve a company employee embezzling funds from their employer, or a financial advisor misappropriating clients' investments. Embezzlement can have severe consequences for both businesses and individuals, resulting in significant financial losses and trust issues. A famous example of embezzlement is the case of Bernard Madoff, who was convicted of several embezzlement charges and sentenced to 150 years in prison for running a massive Ponzi scheme that defrauded investors of billions of dollars.

Viruses and Malicious Code:

Viruses are a type of malicious code, which is a broad category of harmful software or scripts that can damage or compromise a system's security. Malicious code can include viruses, worms, Trojans, backdoors, and other types of cyber threats.

Viruses are self-replicating malicious code that can attach to macro-enabled programs to execute. They can't spread automatically, but they can travel through USB connections or downloaded files from the internet. Once a virus is on a device, it can spread through the system and connected networks. Different types of viruses include polymorphic, compression, macro, boot sector, multipart, and stealth viruses

Malicious code can sneak into a system by visiting infected websites or clicking on a bad email link or attachment. Firewalls can be an important tool in protecting a network-connected environment, but they should be part of a larger, comprehensive security strategy Malicious code comes in many forms:

- Trojans
- Viruses
- Worms
- Ransomware
- Backdoor attacks

Malicious code can cause major disruptions on your computer and in your network. Files can be deleted, a hacker might gain control of your computer, passwords may become compromised and daily operations can be halted. These dangers make compliance with the NIST SP security control guidelines vitally important in the United States. The code inserted inside your system gives a bad actor access. The damage caused depends on the type of malicious code used and the attacker's intent.

Examples of Malicious Code:

Malicious code has been around as long as computers, though its form has changed over the years. In the 1980s, malicious code came in the form of file infectors spread by using a floppy disk. With the standardization of technology came an increase in instances of malicious code and malware, which was accelerated by broad adoption of Web 2.0.

Different types of malicious code attack systems in different ways:

- Backdoor attacks are designed to use a virus or technology to bypass all security measures to gain unauthorized access to a system or network.
- Scripting attacks inject malicious script into trusted websites, usually as browser side script via a web application. TweetDeck suffered a scripting attack that caused all who fell victim to retweet it, resulting in quick and expansive spread.
- Computer worms are a type of virus designed to self-replicate and spread across computers in a network. In 2004 the authors of MyDoom, Bagle and Netsky spread email worms to each other, eventually leading to better email scanning implementation.
- A trojan horse is malware that disguises itself as legitimate code or software. When inside a network, attackers have the same access that a legitimate user does and can make changes to files and data.
- Spyware is designed to stay hidden so that attackers can collect information and transmit data from a computer's hard drive. This also gives attackers access to things like screen grabbing, keylogging and camera control.
- Ransomware is malicious software that blocks access to a system until money is paid to the attacker

Detection and Removal of Malicious Code:

There are several common warning signs that your computer or network has fallen victim to malicious code or malware.

- Your computer slows down significantly overnight.
- Computer programs frequently begin crashing, even after restarting.
- Pop-ups spamming your screen often indicate there is spyware on a computer.
- Having access to network activity while offline is a sign of a virus.
- You experience a sudden increase or decrease in your hard drive's capacity.
- Your contacts might be receiving strange messages from your email.

Once you've seen these signs, you can be sure you already have malicious code in your system. There are types of antivirus software and antimalware to find and remove this malicious code. Removing this code involves manually disconnecting from the internet, entering safe mode, and deleting temporary files.

How can you protect against malicious code:

Following these security practices can help you reduce the risks associated with malicious code:

- **Install and maintain antivirus software.** Antivirus software recognizes malware and protects your computer against it. Installing antivirus software from a reputable vendor is an important step in preventing and detecting infections. Always visit vendor sites directly rather than clicking on advertisements or email links. Because attackers are continually creating new viruses and other forms of malicious code, it is important to keep your antivirus software up-to-date.
- **Use caution with links and attachments.** Take appropriate precautions when using email and web browsers to reduce the risk of an infection. Be wary of unsolicited email attachments and use caution when clicking on email links, even if they seem to come from people you know.
- **Block pop-up advertisements.** Pop-up blockers disable windows that could potentially contain malicious code. Most browsers have a free feature that can be enabled to block pop-up advertisements.
- **Use an account with limited permissions.** When navigating the web, it's a good security practice to use an account with limited permissions. If you do become infected, restricted permissions keep the malicious code from spreading and escalating to an administrative account.
- **Disable external media AutoRun and AutoPlay features.** Disabling AutoRun and AutoPlay features prevents external media infected with malicious code from automatically running on your computer.
- **Change your passwords.** If you believe your computer is infected, change your passwords. This includes any passwords for websites that may have been cached in your web browser. Create and use strong passwords, making them difficult for attackers to guess. (See Choosing and Protecting Passwords and Supplementing Passwords for more information.)
- **Keep software updated.** Install software patches on your computer so attackers do not take advantage of known vulnerabilities. Consider enabling automatic updates, when available. (See Understanding Patches and Software Updates for more information.)
- **Back up data.** Regularly back up your documents, photos, and important email messages to the cloud or to an external hard drive. In the event of an infection, your information will not be lost.
- **Install or enable a firewall.** Firewalls can prevent some types of infection by blocking malicious traffic before it enters your computer. Some operating systems include a firewall; if the operating system you are using includes one, enable it. (See Understanding Firewalls for Home and Small Office Use for more information.)

- **Use anti-spyware tools.** Spyware is a common virus source, but you can minimize infections by using a program that identifies and removes spyware. Most antivirus software includes an anti-spyware option; ensure you enable it.
- **Monitor accounts.** Look for any unauthorized use of, or unusual activity on, your accounts—especially banking accounts. If you identify unauthorized or unusual activity, contact your account provider immediately.
- **Avoid using public Wi-Fi.** Unsecured public Wi-Fi may allow an attacker to intercept your device's network traffic and gain access to your personal information.

Internet Hacking and Cracking:

Hacking and cracking are both terms used in cybersecurity to describe unauthorized access to a computer system or network Hacking is entering a network which is intended to be private, changing the content of another person's web site, redirecting elsewhere anyone trying to access a particular web site or overwhelming a site with countless messages to slow down or even crash the server.

Ethical hackers, also known as white-hat hackers, work with organizations to identify vulnerabilities and help strengthen their security measures. They are usually programmers with advanced knowledge of operating systems and programming languages who use their skills to find and fix loopholes in a system

A hacker is a person who is proficient with computers and/or programming to an elite level where they know all of the in's and out's of a system. There is NO illegality involved with being a hacker

Cracking: It the act of breaking into a computer system, often on a network. A cracker can be doing this for profit, maliciously, for some altruistic purpose or cause, or because the challenge is there

A cracker is hacker who is their proficiency for personal gains outside of the law. For example stealing data, changing bank accounts, distributing viruses etc. Hacker is a malicious meddler who tries to discover sensitive information by poking around.

Hence "password hacker", "network hacker", The correct term for this sense Is Cracker.

Crackers, on the other hand, use their hacking skills for illegal and malicious purposes, such as gaining unauthorized access to systems, stealing sensitive data, or disrupting services. Cracking techniques often involve repeatedly using a few known tricks to break into systems, rather than exploiting the system's weaknesses. Examples of cracking include using public WiFi networks to examine private information, sending phishing emails, or breaking into software. Cracking is illegal and punishable by law in most jurisdictions

Types of Cracking

Cracking is a technique used to breach computer software or an entire computer security system, and with malicious intent. Though functionally the same as hacking, cracking is strictly used in a criminal sense. The process of attempting to gain unauthorized access to a computer system or network by exploiting vulnerabilities or weaknesses in its security is called **cracking.** Cracking specifically refers to same as hacking, but with criminal intent.

Cracking relies more on persistent repetition of a handful of fairly known tricks is order to break into systems, rather than cleverly exploiting the system's weakness.

Cracking can be recognized by, for example, software companies don't come to know the whether their software has been cracked, public WiFi networks being cracked and examined by individuals to hamper their private information, somebody sending phishing emails to other people from your email address.
Types of Cracking

1. Password Cracking
2. Software cracking
3. Network cracking
4. Application cracking
5. Wireless cracking

Password Cracking

Password cracking refers for Finding password from stored data.This is the most typical techniques for password cracking.

- **Brute force cracking:** Until it finds a match the cracking algorithm outputs random sequences of characters.
- **Dictionary cracking:** This is similar to brute-force cracking tictionary tracking restrict itself to words rather than utilising random letters.
- **Rainbow table cracking :** It is used to determine the encryption used to hash a password, a rainbow table leverages previously computed hashed values.

Software Cracking

Software cracking is the process of modifying software to completely or partially eliminate one or more of its functions. At least one of the following tools or methods is used in the majority of software cracking.

- **Keygen:** A keygen, which stands for "key generator," is a programme that a cracker creates to produce legitimate serial numbers for software products.
- **Patch:** Patches are compact pieces of code that alter already-running applications. Every day, software fixes are released by developers. They can also be created by crackers, and when they do, the patch's task is to change the way the software functions by eliminating the undesirable characteristics.
- **Loader:** The function of a loader is to prevent the software's security features from being activated. While some loaders are used to get around copy controls, others are used by players who want to cheat in online multiplayer games.

Network Cracking

Network cracking is when a LAN, or "local area network," is breached by an outsider. A wireless network can be cracked considerably more easily than a cable one since the cracker only has to be in close proximity to the wireless signal. The Wi-fi system in your house is a typical illustration of a wireless LAN. Cracking a wired network requires a direct connection, but cracking a wireless network is much more convenient, because the cracker just needs to be close to the wireless signal.

Application Cracking

Application cracking refers to the process of modifying software to remove or disable its copy protection or licensing mechanisms. Application cracking can also be used as a method of bypassing authentication mechanisms and gaining access to otherwise secure systems.This involves exploiting vulnerabilities in software applications to bypass authentication mechanisms, access sensitive data or execute arbitrary code. Application cracking poses several risks.

Wireless Cracking

Wireless cracking is a form of cyber attack that involves gaining unauthorized access to a wireless network by exploiting vulnerabilities in its security protocols. This type of attack is particularly relevant in the context of Wi-Fi networks, which are widely used in homes, businesses, and public places. Wireless cracking can be used for a variety of purposes, including stealing sensitive information, intercepting communications, and launching other types of attacks on the network or its users

The 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 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.

Virus Attacks:

A computer virus is a type of malicious software, or malware, that spreads between computers and causes damage to data and software.

Computer viruses aim to disrupt systems, cause major operational issues, and result in data loss and leakage. A key thing to know about computer viruses is that they are designed to spread across programs and systems. Computer viruses typically attach to an executable host file, which results in their viral codes executing when a file is opened. The code then spreads from the document or software it is attached to via networks, drives, file-sharing programs, or infected email attachments

How Do Computer Viruses Attack and Spread

In the early days of computers, viruses were spread between devices using floppy disks. Nowadays, viruses can still be spread via hard disks and Universal Serial Bus (USB) devices, but they are more likely to be passed between devices through the internet.

Computer viruses can be spread via email, with some even capable of hijacking email software to spread themselves. Others may attach to legitimate software, within software packs, or infect code, and other viruses can be downloaded from compromised application stores and infected code repositories. A key feature of any computer virus is it requires a victim to execute its code or payload, which means the host application should be running.

Types of Computer Viruses:

1. Resident virus

Viruses propagate themselves by infecting applications on a host computer. A resident virus achieves this by infecting applications as they are opened by a user. A non-resident virus is capable of infecting executable files when programs are not running.

2. Multipartite virus
A multipartite virus uses multiple methods to infect and spread across computers. It will typically remain in the computer's memory to infect the hard disk, then spread through and infect more drives by altering the content of applications. This results in performance lag and application memory running low.
Multipartite viruses can be avoided by not opening attachments from untrusted sources and by installing trusted antivirus software. It can also be prevented by cleaning the boot sector and the computer's entire disk.

3. Direct action
A direct action virus accesses a computer's main memory and infects all programs, files, and folders located in the autoexec.bat path, before deleting itself. This virus typically alters the performance of a system but is capable of destroying all data on the computer's hard disk and any USB device attached to it. Direct action viruses can be avoided through the use of antivirus scanners. They are easy to detect, as is restoring infected files

4. Browser hijacker
A browser hijacker manually changes the settings of web browsers, such as replacing the homepage, editing the new tab page, and changing the default search engine. Technically, it is not a virus because it cannot infect files but can be hugely damaging to computer users, who often will not be able to restore their homepage or search engine. It can also contain adware that causes unwanted pop-ups and advertisements.
Browser hijackers typically attach to free software and malicious applications from unverified websites or app stores, so only use trusted software and reliable antivirus software.

5. Overwrite virus
Overwrite viruses are extremely dangerous. They can delete data and replace it with their own file content or code. Once files get infected, they cannot be replaced, and the virus can affect Windows, DOS, Linux, and Apple systems. The only way this virus can be removed is by deleting all of the files it has infected, which could be devastating. The best way to protect against the overwrite virus is to use a trusted antivirus solution and keep it updated.

6. Web scripting virus
A web scripting virus attacks web browser security, enabling a hacker to inject web-pages with malicious code, or client-side scripting. This allows cyber criminals to attack major websites, such as social networking sites, email providers, and any site that enables user input or reviews. Attackers can use the virus to send spam, commit fraudulent activity, and damage server files.
Protecting against web scripting is reliant on deploying real-time web browser protection software, using cookie security, disabling scripts, and using malicious software removal tools.

7. File infector
A file infector is one of the most common computer viruses. It overwrites files when they are opened and can quickly spread across systems and networks. It largely affects files with .exe or .com extensions. The best way to avoid file infector viruses is to only download official software and deploy an antivirus solution.

8. Network Virus
Network viruses are extremely dangerous because they can completely cripple entire computer networks. They are often difficult to discover, as the virus could be hidden within any computer on an infected network. These viruses can easily replicate and spread by using the internet to transfer to devices connected to the network. Trusted, robust antivirus solutions and advanced firewalls are crucial to protecting against network viruses.

9. Boot Sector Virus
A boot sector virus targets a computer's master boot record (MBR). The virus injects its code into a hard disk's partition table, then moves into the main memory when a computer restarts. The presence of the virus is signified by boot-up problems, poor system performance, and the hard disk becoming unable to locate. Most modern computers come with boot sector safeguards that restrict the potential of this type of virus.
Steps to protecting against a boot sector virus include ensuring disks are write-protected and not starting up a computer with untrusted external drives connected.

- **How To Prevent Your Computer From Viruses**

1. Use a trusted antivirus product

2. Avoid clicking pop-up advertisements

3. Scan your email attachments

4. Scan the files that you download using file-sharing programs

Mitigation and Recovery: In case of an infection, mitigation involves isolating affected systems, removing the virus using antivirus tools, and restoring data from backups if necessary.

PORNOGRAPHY:

The prevalence of pornography in cybercrime is a complex issue with far-reaching implications. While pornography itself is not inherently illegal, its role in facilitating and enabling various cybercrimes has become a significant concern.

How Pornography is Used in Cybercrime:

- **Child Sexual Exploitation:** The internet has made it easier for offenders to access, produce, and distribute child sexual abuse material (CSAM). This heinous crime exploits and harms children, causing lifelong trauma.

- **Revenge Porn:** Non-consensual distribution of sexually explicit images or videos, often used to blackmail, harass, or humiliate victims.

- **Cyberbullying and Harassment:** Pornography can be weaponized to target individuals with sexually suggestive or explicit content, often accompanied by threats or intimidation.

- **Sextortion**: Offenders exploit explicit images or videos to extort money or other favors from victims.

Sextortion is a type of cybercrime where a criminal threatens to share nude or explicit images of a victim, often obtained through cheating, in order to blackmail them for money or other demands.

- **Trafficking:** Online platforms are used to advertise and facilitate sex trafficking, often involving minors.

Pornography involving exploitation or trafficking of individuals, especially minors, is a serious concern. The internet provides a platform for perpetrators to share and monetize such content, exacerbating the exploitation of vulnerable individuals.

One of the most critical issues is the distribution and consumption of illegal pornography, such as child sexual abuse material (CSAM). This type of content is not only morally abhorrent but also illegal in most jurisdictions worldwide. Cybercriminals may exploit various platforms and technologies to distribute and profit from such illegal material, which poses significant legal and ethical challenges.

Challenges in Addressing the Issue:

- Anonymity and Accessibility: The internet's nature provides anonymity, making it difficult to identify and apprehend offenders. The ease of accessing and sharing content exacerbates the problem.
- Global Nature: Cybercrime often transcends borders, making international cooperation crucial but challenging due to differing legal frameworks.
- Technological Advancements: New technologies like deepfakes can create highly realistic but manipulated sexual content, blurring the lines between real and fabricated, and complicating investigations.

Software Piracy:

Software piracy in cybercrime refers to the unauthorized use, distribution, or reproduction of software without proper licensing or legal rights from the copyright owner.

While it might seem like a victimless crime, it has significant implications for both individuals and businesses

Types of Software Piracy:

1 Softlifting or end-user piracy:

Softlifting, also known as end-user piracy, is the most common type of software piracy. It happens when you purchase a piece of software and share it with people who are not authorized to use it. This practice is common in corporate and educational environments, where the user only pays the software vendor a licensing fee for one software program or application but downloads it on multiple computers.

Softliftin also includes benefiting from software upgrades without having a licensed version of the old software being upgraded as well as using non-commercial software (meant for one computer only) or academic or restricted software without a proper license.

2 Counterfeiting:

Software counterfeiting is the illegal copying, distribution, and/or selling of licensed computer software. Other elements that come with the software may be also counterfeited, for example, the license agreement, packaging, registration information, and security features. Cybercriminals usually present counterfeit software as authentic but sell it for a lower price than the original.

3 Hard-disk loading:

Hard disk loading is a form of commercial software piracy in which a PC reseller buys a legal piece of computer software, copies it, installs it on a computer's hard disk, and sells the computer. Having software already installed makes the business' offer more attractive to customers, most of whom aren't even aware that they are also purchasing unlicensed software.

4 Client-server overuse:

Client-server overuse occurs when a company allows the number of users of a particular software to exceed the number of licenses the company has for the software. This happens when the company installs the software on its local area network instead of an individual computer, making it possible for multiple users to use the same software at the same time.

5 Online piracy:

Online piracy, also known as internet piracy, is the illegal sharing, selling, and acquiring of software on the internet. Online piracy is committed on:

- Online auction sites that sell counterfeit, outdated, and pirated software.
- Peer-to-peer file sharing networks that allow users to download and distribute copyrighted software, films, music, and games.
- Usenet, the worldwide distributed discussion system, which offers anonymity and is known for pirated content distribution.
- Websites that allow users to exchange pirated software.
- Websites that offer to download pirated software programs for free.

Impact on Industry:

- **Financial Losses:** Software piracy results in substantial revenue losses for software developers and companies. It undermines their ability to invest in research, development, and customer support.
- **Market Distortion:** Piracy can distort market dynamics by undercutting legitimate software sales, affecting competition and innovation

Legal and Regulatory Issues:

❑ **Copyright Violations:** Piracy constitutes copyright infringement, which is illegal and subject to civil and criminal penalties under international copyright laws.
❑ **Enforcement Challenges:** Enforcing copyright laws across different jurisdictions and combating online piracy pose significant challenges for law enforcement agencies.

Risks of using pirated software:

Using pirated software might be cheaper than buying original software, but you should be aware of the dangers that await a software pirate.

- As an unauthorized user, you will not receive any updates or customer support from the software manufacturer.
- You will face an increased risk of the unlicensed software malfunctioning or crashing.
- You will put your online security at risk because illegal and counterfeit software might infect your device with viruses, malware, or adware.
- Visiting pirating websites is a danger in itself — they contain malicious ads, let alone infected files.
- You may face legal consequences due to copyright violation, including financial penalties.
- Malware Distribution: Pirated software often includes malware or malicious code that can compromise users' systems, steal data, or create vulnerabilities.
- Lack of Updates and Support: Users of pirated software miss out on security patches, updates, and technical support provided to legitimate users, making their systems more vulnerable to cyber attacks.

Preventive Measures:

❑ **Education and Awareness:** Promoting awareness about the consequences of software piracy among businesses, organizations, and individuals can help reduce its prevalence.
❑ **Software Licensing and Auditing:** Implementing effective software asset management practices and conducting regular audits can help organizations ensure compliance with licensing agreements.
❑ **Legal Alternatives:** Providing affordable and accessible legal alternatives to pirated software can incentivize users to choose legitimate options.

INTELLECTUAL PROPERTY:

Intellectual property (IP) in the context of cybercrime refers to the legal rights and protections afforded to creations of the mind, such as inventions, literary and artistic works, designs, symbols, names, and images used in commerce. Protecting intellectual property in the digital age presents unique challenges due to the ease of reproduction, distribution, and manipulation facilitated by digital technologies and the internet.

Types of Intellectual Property:

- **Copyright:** Protects original works of authorship fixed in a tangible medium, such as literary works, music, films, and software.
- **Patents:** Grants exclusive rights to inventors for new and useful inventions, such as processes, machines, or compositions of matter.
- **Trademarks**: Protects distinctive signs, symbols, or logos used to distinguish goods or services in the marketplace.
- **Trade Secrets:** Confidential business information that provides a competitive advantage and is not generally known or readily ascertainable by others.

Cybercrime Issues Involving Intellectual Property

- Online Piracy
- Counterfeiting
- Cyber Espionage
- Domain Name Hijacking

Impacts of Intellectual Property Theft:

❑ **Economic Losses:** Businesses and creators suffer financial losses due to lost sales, decreased market share, and erosion of competitive advantage caused by intellectual property theft.

❑ **Innovation and Creativity:** Theft of intellectual property discourages innovation and creativity by undermining the incentive for creators and inventors to invest in research and development.

❑ **Reputation Damage:** Counterfeit or pirated products can damage the reputation of brands and creators if they are of inferior quality or misrepresent the original product.

Legal and Regulatory Framework:

- Copyright and Patent Laws: Governments enforce laws and regulations to protect intellectual property rights, including civil and criminal penalties for infringement.
- International Cooperation: Given the global nature of the internet, international cooperation and treaties are crucial for combating cross-border intellectual property theft and enforcing rights globally.

Mail Bombs

A mail bomb is a form of cyberattack where a large volume of emails is sent to a specific email address or server, overwhelming the recipient's system. This deluge of emails can cause significant disruption and is often used as a denial-of-service (DoS) attack.

The primary goal of a mail bomb is to disrupt the normal functioning of the target's email service. By flooding the inbox with a large number of emails, legitimate communication may be blocked, and the recipient may experience difficulty accessing or managing their emails.

How Mail Bombs Work

- Overwhelming the Inbox: The primary goal is to flood the target's inbox with emails, rendering it unusable.
- Server Overload: If the attack is intense enough, it can overload the email server, causing it to crash or slow down significantly.
- Disruption: The intended effect is to disrupt the target's communication and productivity.

Types of Mail Bombs

- **Mass Mailing:** Sending multiple copies of the same email to the same address.
- **List Linking:** Subscribing the victim to multiple mailing lists, creating a constant influx of emails.
- **Zip Bombing:** Attaching large, compressed files to emails, overloading the recipient's email system.

Motivations for Mail Bombing

- Harassment: Targeting individuals with a malicious intent.
- Denial of Service: Disrupting a service or individual's ability to use email.
- Distraction: Concealing other cyberattacks by creating a smokescreen.
- Fun or Vandalism: Some individuals may engage in mail bombing for amusement.

Techniques Used:

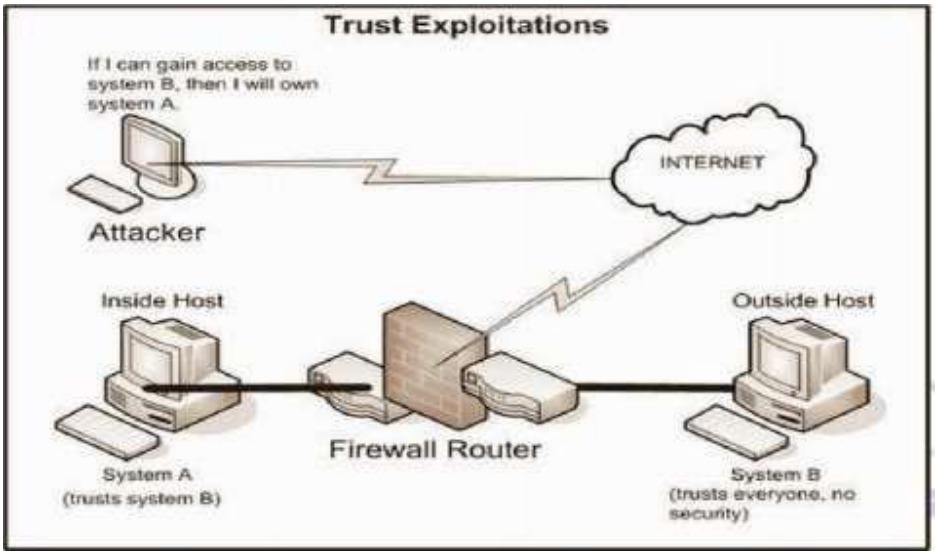
- **Automated Scripts:** Attackers often use automated scripts or software tools designed to generate and send a high volume of emails rapidly.
- **Botnets:** Compromised computers (botnets) can be used to distribute mail bombs, making it difficult to trace the source of the attack.

Protection Against Mail Bombs

- **Robust Email Filters:** Implementing strong spam filters can help block a significant portion of mail bombs.
- **Email Limits:** Setting limits on the number of emails that can be received per hour or day can mitigate the impact.
- **Dedicated Spam Servers:** Using separate servers for spam can isolate the attack and protect primary email systems.
- **Network Security:** Implementing firewalls and intrusion prevention systems can help prevent mail bomb attacks.
- **User Education:** Educating users about the risks of opening suspicious emails can help prevent accidental participation in mail bomb attacks.

Exploitation:

Exploitation in cybercrime refers to the malicious use of vulnerabilities in systems, networks, or individuals to achieve illicit gains. Cybercriminals exploit weaknesses to steal data, disrupt services, or commit financial fraud.



Types of Exploitation in Cybercrime

1. **Vulnerability Exploitation:**
   - Software vulnerabilities: Exploiting bugs or flaws in software applications to gain unauthorized access.
   - System vulnerabilities: Targeting weaknesses in operating systems or network infrastructure.
   - Hardware vulnerabilities: Exploiting flaws in physical devices.
2. **Human Exploitation:**
   - Social engineering: Manipulating people to divulge sensitive information or perform actions that compromise security.
   - Phishing: Deceiving users into clicking malicious links or providing personal data.
   - Spear phishing: Targeted phishing attacks aimed at specific individuals or organizations.
   - Identity theft: Stealing personal information to impersonate victims.
3. **Data Exploitation:**
   - Data breaches: Unauthorized access to sensitive data.
   - Data leakage: Accidental or intentional release of confidential information.
   - Data misuse: Using stolen data for fraudulent activities.

Understanding exploitation in cybercrime is crucial for developing effective cybersecurity measures, including regular software updates, strong authentication methods, employee training on social engineering tactics, and comprehensive threat detection and response strategies.

Stalking and Obscenity in Internet:

Stalking and obscenity on the internet are serious issues that can have profound impacts on individuals and communities. Here's a breakdown of each:

Stalking on the Internet:

Internet stalking, also known as cyberstalking, involves the repeated use of electronic communication to harass or frighten another person. This can include:

- Sending unwanted messages: Emails, texts, or social media messages.
- Monitoring online activity: Tracking a person's social media posts, location, or browsing history.
- Impersonating the victim: Creating fake profiles to deceive others.
- Threatening or harassing behavior: Using electronic communication to intimidate or threaten the victim.

Types of Cyberstalking

Let us explore the various kinds of Cyberstalking that are prevalent:

- **Catfishing:** The creation of fake profiles or copying of existing ones on social media to approach victims.
- **Monitoring check-ins on social media:** Keeping an eye on the activities of a victim on social media to accurately gauge their behavior pattern.
- **Spying via Google Maps and Google Street View**: Using Street View to spy on a victim and find their location from posts or photos on social media.
- **Hijacking webcam:** Webcams can be hijacked by introducing malware-infected files into the victim’s computer.

- **Installing stalkerware:** Stalkerware tracks the location, enables access to texts and browsing history, makes audio recordings, etc., without the victim's knowledge.

Some of the common examples of cyberstalking are:

- Making rude, offensive, or suggestive online comments
- Joining the same groups and forums to follow the target online
- Sending the target threatening, controlling, or lewd messages or emails
- Making a fake social media profile to follow the victim
- Gaining access to the victim's online accounts
- Posting or disseminating real or fictitious photos of the victim
- Attempting to obtain explicit photographs of the victim
- Tracking the victim's online movements using tracking devices
- Mailing explicit photos of themselves to the victim on a regular basis, etc.

Obscenity on the Internet:

Internet obscenity involves the dissemination or display of sexually explicit or offensive content online that is deemed to be morally offensive or inappropriate by societal standards. Obscenity refers to sexually explicit material that is offensive to community standards and lacks artistic, literary, or scientific value. Online,
Cyber obscenity, or cyber pornography, is a threat to internet users worldwide because there are no territorial limits for committing the crime.

_ **Sharing explicit images or videos**: Distributing sexually suggestive or explicit content without consent.
❑ **Child pornography:** Creating, distributing, or possessing images or videos depicting children engaged in sexually explicit conduct.

❑ **Cyberbullying:** Using obscene language or images to harass or intimidate others.

Stalking and obscenity are serious issues that can have a devastating impact on victims. It's essential to be aware of the risks and take steps to protect yourself and others.

Digital laws and legislation

Digital laws and legislation related to cybercrime are essential for addressing the increasingly complex challenges posed by criminal activities in the digital realm.

Digital laws, also known as cyber laws or internet law, are a set of legal regulations and frameworks governing digital activities. They encompass a wide range of issues, from online communication and e-commerce to digital privacy and cybercrime prevention.

Importance of Digital Laws

The rapid evolution of technology and its integration into our daily lives has necessitated the development of specific legal frameworks to address the unique challenges posed by the digital world. Digital laws serve several critical purposes:

- **Protecting individuals:** Safeguarding personal information, privacy, and online safety.
- **Facilitating e-commerce:** Creating a legal environment that supports online transactions and consumer protection.
- **Combating cybercrime:** Establishing legal frameworks for investigating, prosecuting, and preventing cybercrimes.
- **Intellectual property protection:** Safeguarding digital content and inventions.

Example of Digital Laws

The Information Technology Act (ITA) of India is a prominent example of a digital law. It covers a wide range of cybercrimes, including hacking, identity theft, and data theft. Other countries have similar comprehensive cybercrime laws.

Legislation:

Cybercrime legislation is a set of laws and regulations that protect individuals and organizations online, and promote the responsible use of technology. Cybercrime laws can address a wide range of issues.

_ **Cybercrime Laws:** These laws explicitly define and criminalize cyber offenses such as hacking, unauthorized access, data theft, cyberstalking, and online fraud.
❑ **Data Protection Laws:** These laws regulate the collection, storage, processing, and transfer of personal data, ensuring privacy and data security.
❑ **E-commerce Laws:** These laws govern online transactions, consumer protection, and electronic contracts.

❑ **Intellectual Property Laws:** These laws protect digital content, software, and inventions from unauthorized use or distribution.

Law Enforcement Roles and Responses

Law enforcement plays a critical role in addressing and responding to cybercrime issues. As technology continues to advance, so do the methods and tactics used by cybercriminals. Law enforcement agencies around the world must adapt to combat these evolving threats effectively.

Here are some key law enforcement roles and responses in cybercrime issues:

1. **Investigation**: Law enforcement agencies investigate cybercrimes, including hacking, data breaches, online fraud, cyberbullying, and more. This involves collecting digital evidence, tracking down perpetrators, and building cases against them.
2. **Forensics:** Digital forensics experts are essential in cybercrime investigations. They analyze digital evidence from computers, smartphones, servers, and other devices to uncover crucial information that can be used in court.
3. **Cybercrime Units:** Many law enforcement agencies have specialized cybercrime units or divisions focused exclusively on cyber-related offenses. These units often consist of specially trained personnel with expertise in digital investigations.
4. **International Cooperation**: Since cybercrime is often transnational in nature, law enforcement agencies cooperate with their counterparts in other countries. This cooperation is essential for tracking down cybercriminals who may operate across borders.
5. **Public Awareness and Education:** Law enforcement agencies often engage in public awareness campaigns to educate individuals and businesses about online threats and best practices for cybersecurity. This proactive approach can help reduce the incidence of cybercrimes.

6. **Cybersecurity Partnerships:** Collaboration with private sector organizations, including cybersecurity firms and internet service providers, is crucial. These partnerships can facilitate information sharing and help identify and mitigate cyber threats.
7. **Legislative Advocacy:** Law enforcement agencies may work with legislators to advocate for and influence cybersecurity-related legislation and regulations. This can include proposing new laws or amendments to existing ones to better address cybercrime.
8. **Incident Response:** Law enforcement agencies often respond to cyber incidents, such as data breaches. They work to contain the breach, identify the perpetrators, and assist victims in mitigating the damage.
9. **Training and Capacity Building:** Continuous training and skill development are vital for law enforcement personnel to keep up with evolving cyber threats. Many agencies offer specialized training programs to ensure their staff is well-prepared.
10. **Preventive Measures:** Law enforcement agencies may work on preventive measures, such as developing threat intelligence, monitoring cyber threats, and conducting outreach to potential targets to enhance their cybersecurity posture.
11. **Prosecution:** Once cybercriminals are apprehended, law enforcement agencies work with prosecutors to build strong cases for prosecution in court. This involves presenting digital evidence and expertise to secure convictions.
12. **Victim Support:** Providing support to cybercrime victims is an essential aspect of law enforcement's role. This can include guidance on reporting incidents, assistance in recovering stolen funds, and counseling for emotional and psychological distress.
13. **Policy Development:** Law enforcement agencies often contribute to the development of national and international cybersecurity policies, strategies, and frameworks

Law enforcement agencies play a crucial role in combating cybercrime. Their responsibilities range from prevention and detection to investigation, prosecution, and rehabilitation.

UNIT-3
INVESTIGATION

Definition:

Cybercrime investigation is a specialized field that involves the systematic process of identifying, collecting, preserving, analyzing, and presenting digital evidence to uncover criminal activities conducted through computer networks. It requires a deep understanding of technology, law, and investigative techniques.

Cybercrime investigation is a specialized field within law enforcement and forensic science focused on detecting, analyzing, and solving crimes committed using or involving digital technology and networks.

UNIT-III

Investigation to cyber crime investigation:

Cyber crime investigation play a vital role in the modern world, addressing emerging threats and helping to maintain the safety of our Digital Spaces.

"Cyber crime investigation involves the process of: Investigation involves:

→ Identifying, Analyzing, and tracking Digital evidence to uncover the perpetrators and their motives.

→ conducting the initial investigation.

→ Identifying potential evidence.

→ Securing Devices

→ Obtaining court orders

→ Analyzing results with the prosecutors and proper handling of Digital evidence.

In simple terms cyber crime investigation Aim to identify the source of the crime, gather evidence and present that evidence in a manner suitable for court proceedings to prosecute".

Investigation Tools:

The cybercrime investigators use both technical & Non-technical methods while investigat

1. Digital Forensics Tools

Digital forensic is a crucial aspect of Cybercrime Investigation, involving the collection, analysis and preservation of electronic evidence.

This Digital forensic tools include Software programs like "Encase, FTK, Autopsy".

→ **Encase:** It is used to collect, analyze and store the electronic evidence using the Mathematical and Scientific techniques.

It helps in data acquisition from the hardware smart devices. and this encases S/W generates reports regarding the cybercrime investigat

→ **FTK:** FTK means "Forensic Toolkit" that used to analyze and recover the digital data from Storage devices. This provides analyzing files, recovering files and keyword searching services.

→ **Autopsy:** This tool is used to analyze the Hard drives and smart devices. and provides user friendly web interface. It helps to recover deleted or missing tools.

2. Network Analysis Tools:

Network analysis tool is used to detect the network traffic and also these network analysis tool could identify the suspicious changes in the system and track the data flow.

Tools - Wireshark, tcpdump, Netcop.

Wireshark: It is most famous network security tool and give a very keen and vivid overview of your network and captures N/w traffic packets.

tcpdump: It is used in Unix operating systems. it's have the ability to capture the packets (TCP/IP) that tranferring thrugh a network.

3. Malware Analysis Tools.

These malware analysis tools could use to identify the behavior and identify its source of the malware.

IDA: Stands for interactive Dissembler, is used in reverse engineering and malware analysis. This helps to view the binary files in a human viewable way.

OllyDbg: used to reverse engineering, Software tracking and in the debugging process. this allows user to debug real time program.

Other tools like Cuckoo Sandbox, Virus Total, and CrowdStrike Falcon to analyse malicious code

4. Social media Analysis Tools:

This Social media tool use to gather the acts relating to the cyber crime using the Social media platforms.

Tools: Hootsuite helps to track the constant changes in Social media.

5. Memory Analysis Tool:

Memory analysis is essential for uncovering sophisticated attacks that manipulate system memory.

Tools such as Volatility and Rekall enable experts to analyse volatile memory to identify malicious processes. and other signs of compromise

6. Network Security Monitoring tools:

These tools are designed to monitor the network security and network failures.

Tools: Argus provides customize reporting servi
Nagios: used to identify the issues in the computer infrastructure system

7. Encryption Tools:

These tools also used to protect the gathered evidence and other specific data

tools'.

Two fish is the fastest data algorithm method and used in both hardware and slw

AES, RSA, Triple DES, Ax Crypt.

8. Firewall tools

These firewall tools are used to complete the security management regarding the firewall. firewall are responsible for the incoming and outgoing data.

Tools: Firemon, Red Seal

9. cybersecurity Monitoring Tools:

These tools will monitor malicious cyber threats.

Tools: Site lock helps to safeguard to our site.

10. Network Intrusion detection tool:

These tool are detect the network intrusion

Tools: Aunetix, Snort.

11. Defensive A-I: powered by machine learning algorithms, play crusial role in identify and mitigating cyber threats.

Electronic Discovery (or) ediscovery

e-discovery is the process of obtaining and exchanging evidence in legal case or investigation.

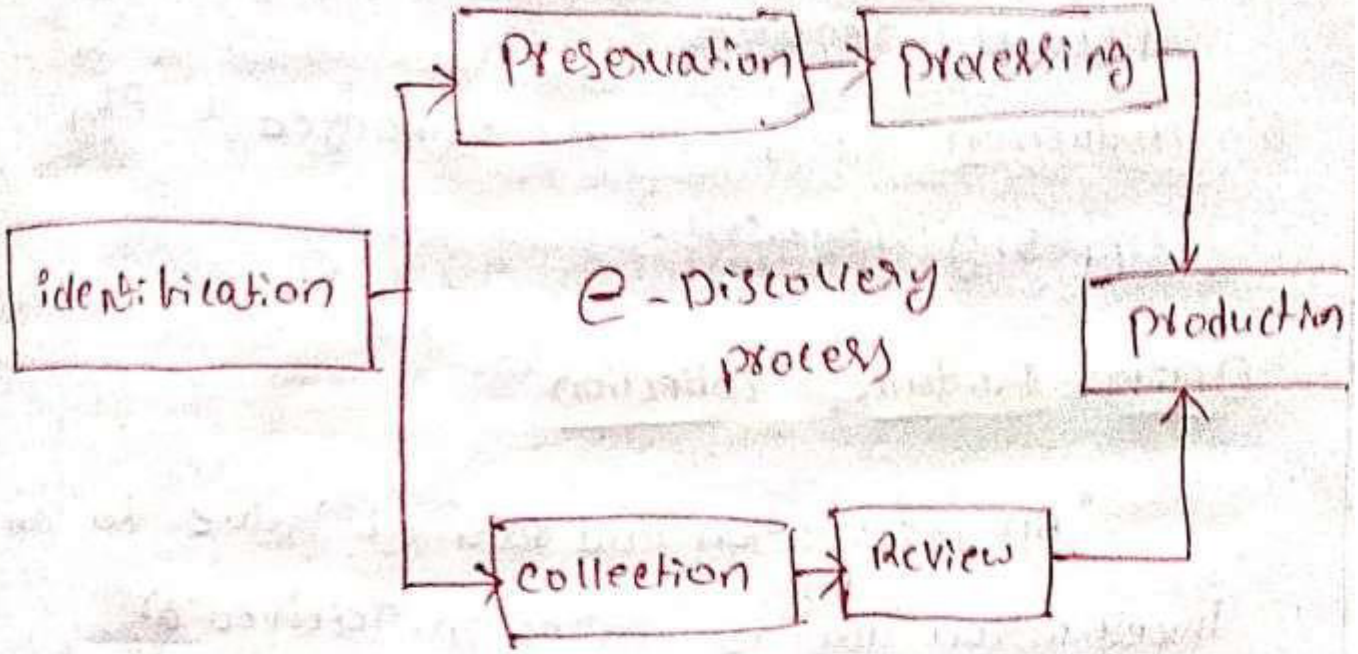
It is a digital investigation process that helps find evidence in electronic data that can be used in legal proceedings or criminal cases.

e-discovery can have all type of data can serve as evidence. This includes electronic documents such as text, images, audio, video, calendars, instant messages, cellphone data, databases, spreadsheets, animation, websites and computer programs.

→ E-discovery brodened this process to include electronical stored information (ESI)

The e-discovery process

The process of discovery begins when a lawsuit appears imminent, up to when Digital evidence is presented in court. Attorney from both sides will determine the scop of e discovery.



1. Identification: ESI is identified by attorney. request and challenges are made.
2. Preservation: Data that is identified as potentially relevant is placed under legal hold so it cannot destroyed
3. Collection: Data is transfered from a company to legal counsel, legal counsel determines the data's relevance
4. Processing: Files are loaded into a review Platform. Data is usally converted into PDF or TIFF (Tag image file format) for court.

5. Review: The review process assesses documents for privilege and responsiveness to discovery requests.

6. Production: Documents are exchanged with opposing counsels.

Digital Evidence collection

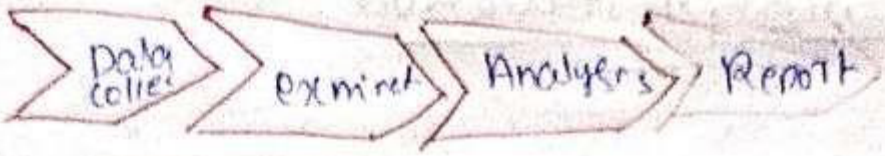
"An information and data of value to an investigation that is stored on, received or transmitted by an electronic device".

Ensuring data integrity and authenticity is critical.

process involved in Digital evidence collection

The main process in Digital evidence collection

- Data collection: In this process, data is identified & collected for investigation
- Examination: In the scond step the collected data is examined carefully.
- Analysis: In this process, different tools and technique are used and collected evidence is analyzed to reach some conclusions.
- Reporting: all the documents & reports are compiled so that can submit in court



Types of collectible Data :-

There are two types of Data. that can be collected in computer investigation.

* **persistent data:**

It is the data that is stored on a non-volatile memory type storge device such as a local hard drive, external storage devices like SSDs, HDDs, pen drives, CDs.

* **Volatile Data:**

It is the data that is stored on a volatile memory such as memory, registers, cache, RAM, or it exists in transit.

Five Rules of Evidence collection

1) **Admissible**: must be preserved & gathered in such a way that it can be used in court.
2) **Authentic** - must be relavent for case to prove something
3) **complete** - clear & complete evidence
4) **Reliable** - evidence collected from device must be reliable
5) **Believable** - able explain with clarity and conciseness

Digital Evidence preservation

Preservation of evidence is the process of saving information that may be relevant to a potential or going lawsuit so that it cannot be altered, lost, or destroyed.

Three Methods To preserve a Digital Evidence

1) Drive Imaging:

Imaging a drive is forensic process in which an analyst will create a bit-by-bit duplicate of the drive.

→ This forensic image of all digital media helps retain evidence for the investigation. When analyzing an image forensic expert need to keep in mind. Some points

- Even wiped driver can retain important and recoverable data to identify.
- Forensic expert can recover all deleted files using forensic technique.
- Never perform forensic analysis on the orginal media, Always operate on the duplicate image.

(ii) Hash Values:

Where 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 original media.

→ hash values will generate as altering even the smallest bit of data. generate completely new Hash values.

→ If the Hash value of the image & original evidence do not match then serious concerns may raise.

(iii) 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 hand off

- To preserve the integrity of the evidence.
- Impotance to Examiner & to the court.

E-Mail Investigation

"E-mail investigation is a digital forensics process of finding out evidences from our evidence from Suspet emails. That allows investigator to examine, preserve and reveal Digit evidence' it is also recover deleted emails from mail servers.

Requirements of E-mail Investigation.

- To carve evidence
- To ensure the reliability of e-mails.
- To pointing on illegal acts and interfuine them.
- presenting an evidence in front of legal authorities

Techniques used in Email Investigation

It involves investigating metadata, port scanning as well as key word searching. Here Some common techniques.

- Header Analysis
- Server Investigation

- Network Device Investigation
- Sender mailer Fingerprints
- Slw embedded Identifiers

Header contains useful information

- Unique identifying number
- Sending time.
- Ip address of sending e-mail server
- IP address of e-mail client.

E-mail Investigation tools

i) Access Data's FTK Imager.

ii) Mailxaminer.

iii) Encase

iv) DBxtract and paraben, etc.

* E-Mail Tracking.

Email tracking is a way of gathering information on how recipients interact with emails. Tracking can show when emails were opened, what browser and device were used. whether recipients clicked any links and even their approximate location at that time.

It focus on

→ Recovering deleted emails messages and attachments.

→ Recovering message contacts

→ Tracking Sender IP address

→ Recovering and saving deleted emails.

→ Tracing an email to its true geographical source

→ collecting Network (ISP) and Domain whois information for any email traced.

Here some Techniques that can be used in email -Tracking

* Email Headers:

Email headers contain information about the Sender, Recipient, data and time, and Subject.

For example: you can use the email headers to find the mail server that sent the email, and then use whois.net to find who owns the Domain name of where they are located. and you can also get the IP address.

* Email attachments:

Email attachments can contain malware or other malicious code, or they can used to steal sensitive data.

* Deleted emails:

Deleted emails can be recovered from email server or backup tapes, which can be important if the suspect has tried to destroy evidence.

IP Tracking:-

IP tracking refers to the process of identifying the geographical location or other details of a user based on their IP address.

Here's how it typically fits into the process:

i) Identifying Suspicious Activity: helps identify unusual or suspicious online behaviour that may indicate criminal activity.

ii) Geolocation: By tracking IP address investigators can estimate the geographical location of the suspect. but suspect might use VPN's or proxies to obscure their true location

(iii) Tracing connections: Investigators can use IP addresses to trace connections between different activities or incidents.

(iv) Coordinating with ISPs: Law enforcement can work with ISPs to obtain additional information about the user associated with an IP address.

(v) Cross-Referencing Evidence: IP tracking is often combined with other digital evidence, such as email headers, logs, and device information to build a more comprehensive picture of crime.

* E-mail Recovery:-

email recovery in a cybercrime investigation involves retrieving and analyzing email data to uncover evidence of criminal activity.

It involves a systematic approach to retrive lost or compromised emails.

Here's a general outline of how it is done.

(i) Determine the scope, identify which email accounts or system need recover and understand the nature of problem.

(ii) For compromised accounts work with email service providers to access compromised accounts.

(iii) For personal Recovery use account recovery option provided by the email service.

(iv) Access and restore from backups if available.

(v) Use email forensic tools to extract data from email servers or client applications, ensuring data integrity and preserving evidence.

(vi) Check the email services trash or recovery folders.

(vii) Access archived emails or backup files to restore.

(viii) Create forensic copies of recovered emails and Analyze And examine Data.

→ Store Data Securely to prevent tampering or loss

→ Create detailed reports outlining the recovery process and findings.

Hands on case studies:

Hands-on case studies in cybercrime investigation often involve practical exercises where participants simulate real-world scenarios.

These case studies provide practical experience in handling various types of cybercrime incidents,

common examples of case studies

1. Phishing attack investigation:

It involves different tasks like Email Analysis, Recovery, Forensic analysis, Response.

2. Data breach Investigation

a company experiences a data breach, here tasks like Incident Detection, Scope Assessment, mitigation Reporting.

3. These above case study would gain hands-on experience with real-world and understand the process of investigating and how to respond effectively.

Encryption and Decryption methods:-

In cyber crime investigations, encryption and decryption methods play a crucial role.

⇒ Encryption in cybercrime:

Attackers use encryption to secure their communications and and malicious payloads

common Algorithms.

- AES (Advanced Encryption Standard): often used for encrypting data due to its strength and efficiency key size: 128, 192, or 256 bits.
- RSA (Rivest-Shamir-Adleman): Used for secure data transmission, particularly in establishing secure channels.
- ECC (Elliptic curve Cryptography): used for creating small, efficient keys in secure communicat.
- Hash Functions:
  - → SHA-256 (Secure Hash Algorithm 256-bit)
  - → MD5 (Message Digest algorithm 5) produce a 128-bit hash value.

→ Hybrid Encryption.

→ Encryption protocols like SSL/TLS to secure communication over a network.

⇒ Decryption in cyber crime investigation :-

Investigators need to decrypt encrypted files or communication to analyze the attack, recover data or gather evidence.

- Key Recovery: If the encryption key is known or can be recovered, it can be used to decrypt the files. This is often a challenge in ransome -ware cases.

- Cryptanalysis: Analyzing encrypted data to break the encryption without the key. Techniques includes bruteforce attacks, dictionary attack, or exploiting weaknesses in encryption algo

Tools are like! :-

- OpenSSL: provides tools for implementing and managing cryptographic alogorithms.

- Gpg (GNU privacy Guard): an open source implementation of Pgp for emails and files.

- Emsisoft Decryptor: offers decryption solution for various ransomware families.
- Kaspersky Rakhni Decryptor: Decrypt files without paying the ransom.
- Bitdefender Decryption tool
- Recuva: recover files
- online Decryption services.

* Search and Seizure of computers:-

A Search and Seizure is an examination used by law enforcement to analyze a suspected person's electronic devices or computer suspected to contain evidence of a cyber crime.

Execution of Search:

The Search involves reviewing or analyzing the individual's property to find clues.

The Criminal procedure act governs this process, Court will issue a warrant this must includes: Name of suspect,

→ In law enforcement takes possession of any of the person's item during the search, this is considered the "seizure".

→ After a search, the investigator must create a seizure report on the spot to follow the Law.

Recovering Deleted evidenles

Recovering deleted evidenle in a cyber crime investigation involves mixe of technical expertise and legal knowledge.

Data recovery Techniques

Recovering deleted evidenles involves using different types of methods like:-

- File carving: This involves searching for file signatures and patterns in unallocated space on a hard drives.
- Unallocated Space Analysis: Look for remnants of deleted files in the areas of the disk that are marked as available for new data but may still contain fragments of old files.

- Disk Analysis Tools:

Utilize specialized forensic s/w like Enease, FTK imager, or x, for in-depth analyses and recovery

These tools can help in locating and restoring deleted files, emails, or other artifacts.

other methods like

- Data base and Log Recovery
- metadata examination involves Timestamp analysis and review metadata from file systems.

Password cracking:

Password cracking refers to the "process of attempting to decipher passwords by using various techniques. such as dictionary attacs, etc"

It is a process used to gain unauthorized access to system. also required to access encrypted files.

Password Cracking Techiques

(i) Brute force attacks like Hashcat, John the Ripper

(ii) Dictionary Attacks and Hash analysis.

(iii) Rainbow table

(iv) Hybrid attack - combined BF force + Dictionary attack

(v) Social engineering used manipoulte for their passwords.

(vi) password cracking and credential stuffing.

preventive measures

→ Implement and enforce strong passwords policies and multifactor authentication to reduce risk of cracking.

→ Educate users on the best practices for password security and recognize strategies.

Social engineering

UNIT – 4

DIGITAL FORENSICS

Introduction to Digital Forensics

- Digital forensics is a branch of forensic science that focuses on the identification, preservation, extraction and analysis of electronic data.
- It is the process of using special tools and techniques to examine and analyse electronic devices such as computer, smartphones and tablets, in order to find evidence that can be used in a criminal or civil case.
- Digital forensics is often used to investigate cybercrimes, such as hacking, identity theft and child pornography, but it can also be used in other types of cases, such as financial fraud or civil disputes.
- The goal of digital forensics is to provide reliable and accurate information that can be used to help solve crimes or resolve disputes.

Process of Digital forensics

Digital forensics entails the following steps:

- Identification
- Preservation
- Extraction
- Analysis
- Documentation
- Presentation

Identification: The first step in a digital forensic investigation is to identify the devices and data that may be relevant to the case. This may include computers, smartphones, tablets, servers, and other types of electronic devices.

Preservation: Once the relevant devices and data have been identified, it is important to preserve them in order to maintain the integrity of the evidence. This may involve making copies of the data, or taking steps to prevent any changes from being made to the original data.

Extraction: The next step is to extract the data from the devices and prepare it for analysis. This may involve using specialized software or hardware tools to access the data and make copies of it.

Analysis: Once the data has been extracted, it must be analyzed in

order to identify any relevant information or evidence. This may involve using specialized software to search for keywords, examine patterns of activity, or reconstruct deleted files.

Presentation: The final step in the process is to present the results of theanalysis in a clear and concise manner. This may involve creating reports, charts, or other types of documentation to explain the findings of the investigation.

Types of digital forensics

Computer forensics: This type of digital forensics involves the investigation of computers and other types of electronic devices in order to identify and analyse evidence. This may include examining hard drives, analysing network traffic, and reconstructing deleted files.

Mobile device forensics: This type of digital forensics involves the investigation of smartphones, tablets, and other types of portable devices in order to identify and analyse evidence. This may include examining call logs, text messages, and other types of data stored on the device.

Network forensics: This type of digital forensics involves the investigation of networks and communication systems in order to identify and analyse evidence. This may include examining network traffic, analysing log files, and reconstructing packets of data.

Cloud forensics: This type of digital forensics involves the investigation of cloud-based systems and services in order to identify and analyse evidence. This may include examining logs and other types of data stored in the cloud.
There are several different types of evidence that can be found during a digital forensic investigation, including:

- **Text files:** These can include documents, emails, and other types of written communication that may be relevant to the case.
- **Images:** This can include photographs, graphics, and other types of visual media that may be relevant to the case.
- **Audio files:** This can include recordings of conversations, lectures, or other types of audio that may be relevant to the case.
- **Video files:** This can include footage from security cameras, video recordings, or other types of videos that may be relevant to the case.
- **Internet history:** This can include information about websites that have been visited, as well as search terms that have been used, and may be relevant to the case.

- **System files:** These can include operating system files, application files, and other types of data that may be relevant to the case.

There are several different types of electronic devices that may be examined during a digital forensic investigation, including:

1. Computers: This can include desktop computers, laptops, and servers, and may be used to examine hard drives, network traffic, and other types of data.

2. Mobile devices: This can include smartphones, tablets, and other types of portable devices, and may be used to examine call logs, text messages, and other types of data stored on the device.

3. Network devices: This can include routers, switches, and other types of network equipment, and may be used to examine network traffic and logs.

4. Cloud-based systems: This can include cloud-based storage and other types of cloud-based services, and may be used to examine data stored in the cloud.

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.

Uses of Digital Forensics

In recent time, commercial organizations have used digital forensics in following a type of cases:

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

Overall, the goal of digital forensics is to provide reliable and accurate information that can be used to help solve crimes or resolve disputes. It is an important tool in today's digital world, and is used by law enforcement agencies, businesses, and other organizations to understand and prevent digital wrongdoing.

Forensic Software and Hardware

Forensic software and hardware are tools that are used to extract and analyse electronic data in a digital forensic investigation. These tools can include software programs such as EnCase, FTK, and X-Ways, as well as hardware devices such as write blockers and forensic workstations.

Forensic software and hardware are tools that are used to extract and analyse electronic data in a digital forensic investigation. These tools can include:

1. Forensic software: This type of software is designed specifically for use in digital forensic investigations and can include programs such as EnCase, FTK, and X-Ways. These programs can be used to extract data from electronic devices, analyse the data, and create reports or other documentation of the findings.

2. Write blockers: A write blocker is a device that is used to prevent any changes from being made to the data on an electronic device. This is important in order to maintain the integrity of the evidence and prevent any contamination of the data.

3. Forensic workstations: A forensic workstation is a specialized computer that is used for digital forensic investigations. These workstations often have multiple hard drives and other specialized hardware and software tools that are used to extract and analyse data from electronic devices.

In addition to the forensic software and hardware tools that are commonly used in digital forensic investigations, there are also a number of other tools and techniques that may be employed, depending on the specific needs of the case. Some of these tools and techniques include:

1. Data carving: Data carving is a technique that is used to extract data from a storage device, even if it has been deleted or partially overwritten. This can be useful in cases where the data may have been intentionally or accidentally deleted.

2. Keyword searches: Keyword searches are used to search for specific words or phrases within a large amount of data. This can be useful in cases where there may be a specific piece of information that is relevant to the investigation.

3. Hash analysis: Hash analysis is a technique that is used to verify the integrity of the data on an electronic device. It involves calculating a unique numerical value, or "hash," for each piece of data and comparing it to a known value in order to ensure that the data has not been altered.

4. Network forensics: Network forensics involves the examination of network traffic and other data in order to identify patterns of activity or identify specific individuals or devices.

5. Cloud forensics: Cloud forensics involves the examination of data stored in cloud-based systems and services in order to identify and analyse evidence.

Overall, forensic software and hardware are an important part of the digital forensic process and are used to extract and analyse electronic data in a reliable and accurate manner.

Computer Forensics and Law Enforcement

Computer forensics is often used by law enforcement agencies to investigate and prosecute cybercrimes, such as hacking, identity theft, and child pornography. In these cases, computer forensics plays a critical role in identifying and analysing the electronic devices and data that may be relevant to the case.

The process of computer forensics in a law enforcement context typically involves the following steps:

1. Seizure: The first step in a computer forensic investigation is to seize the electronic devices and data that may be relevant to the case. This may

involve obtaining a search warrant and collecting the devices from the location where the crime was committed.

2. Preservation: Once the devices and data have been seized, it is important to preserve them in order to maintain the integrity of the evidence. This may involve making copies of the data , or taking steps to prevent any changes from being made to the original data.

3. Extraction: The next step is to extract the data from the devices and prepare it for analysis. This may involve using specialized software or hardware tools to access the data and make copies of it.

4. Analysis: Once the data has been extracted, it must be analyzed in order to identify any relevant information or evidence. This may involve using specialized software to search for keywords, examine patterns of activity, or reconstruct deleted files.

5. Presentation: The final step in the process is to present the results of the analysis in a clear and concise manner. This may involve creating reports, charts, or other types of documentation to explain the findings of the investigation.

Computer forensics is an important tool for law enforcement agencies in investigating and prosecuting cybercrimes. It involves the use of specialized techniques and tools to extract, analyse, and present digital evidence that may be relevant to a criminal case.

In a law enforcement context, computer forensics may be used to:

- Investigate cybercrimes: Computer forensics can be used to identify and track the activities of individuals or groups who are suspected of committing cybercrimes, such as hacking, identity theft, or child pornography.

- Collect and preserve digital evidence: Computer forensics can be used to collect and preserve digital evidence that may be relevant to a criminal case, such as emails, text messages, and other types of electronic communication.
- Analyse electronic devices and data: Computer forensics can be used to analyse the data on electronic devices, such as computers, smartphones, and tablets, in order to identify patterns of activity or extract relevant information.
- Present evidence in court: Computer forensics experts may be called upon to present the results of their analysis in court in order to help prosecute cybercrimes and bring perpetrators to justice.

- Identify suspects: Computer forensics can be used to identify the individuals or groups who are suspected of committing cybercrimes, such as hacking or identity theft. This may involve analysing electronic devices, such as computers and smartphones, in order to identify patterns of activity or extract relevant information.

- Track cyber-criminal activity: Computer forensics can be used to track the activities of individuals or groups who are suspected of committing cybercrimes. This may involve examining log files, analysing network traffic, or reconstructing packets of data in order to understand how the crimes were committed and identify the perpetrators.

- Collect and preserve digital evidence: Computer forensics can be used to collect and preserve digital evidence that may be relevant to a criminal case, such as emails, text messages, and other types of electronic communication. This may involve making copies of the data or taking steps to prevent any changes from being made to the original data.

- Present evidence in court: Computer forensics experts may be called upon to present the results of their analysis in court in order to help prosecute cybercrimes and bring perpetrators to justice. This may involve creating reports, charts, or other types of documentation to explain the findings of the investigation.

There are a number of challenges that law enforcement agencies may face when using computer forensics to investigate and prosecute cybercrimes. Some of these challenges include:

1. Keeping up with technology: The field of computer forensics is constantly evolving as new technologies are developed and new cyber-crimes are committed. This can make it difficult for law enforcement agencies to keep up with the latest techniques and tools and to effectively investigate and prosecute cybercrimes.

2. Maintaining the integrity of the evidence: It is important to maintain the integrity of the evidence in a computer forensic investigation in order to ensure that it is admissible in court. This can be challenging, as it is easy to alter or delete digital evidence, and there may be multiple copies of the data that need to be tracked.

3. Dealing with large amounts of data: Computer forensic investigations often involve analysing large amounts of data, which can be time-consuming and resource-intensive. This can make it difficult for law enforcement agencies to efficiently investigate and prosecute cybercrimes.
4. Limited resources: Law enforcement agencies often have limited resources, including staff and funding, which can make it difficult to effectively investigate and prosecute cybercrimes.

Overall, law enforcement agencies face a number of challenges when using computer forensics to investigate and prosecute cybercrimes. These challenges can include keeping up with technology, maintaining the integrity of the evidence, dealing with large amounts of data, and limited resources.

Overall, computer forensics is an important tool for law enforcement agencies in investigating and prosecuting cyber crimes. It involves the use of specialized techniques and tools to extract, analyze, and present digital evidence in a reliable and accurate manner.

Indian Cyber Forensic

Indian cyber forensics is the branch of digital forensics that specifically focuses on the investigation of cyber crimes in India. It involves the use of specialized techniques and tools to extract, analyze, and present digital evidence that may be relevant to a criminal case in India.

In India, cyber forensics is used by law enforcement agencies and other organizations to investigate and prosecute cyber crimes, such as hacking, identity theft, and child pornography. It is also used by businesses and individuals to resolve disputes and protect against cyber threats.

The process of Indian cyber forensics typically involves the following steps:

1. Identification: The first step in a cyber forensic investigation is to identify the devices and data that may be relevant to the case. This may include computers, servers, and other types of electronic devices.

2. Preservation: Once the relevant devices and data have been identified, it is important to preserve them in order to maintain the integrity of the evidence. This may involve making copies of the data, or taking steps to prevent any changes from being made to the original data.

3. Extraction: The next step is to extract the data from the devices and prepare it for analysis. This may involve using specialized software or hardware tools to access the data and make copies of it.

4. Analysis: Once the data has been extracted, it must be analyzed in order to identify any relevant information or evidence. This may involve using specialized software to search for keywords, examine patterns of activity, or reconstruct deleted files.
5. Presentation: The final step in the process is to present the results of the analysis in a clear and concise manner. This may involve creating reports, charts, or other types of documentation to explain the findings of the investigation.

Indian cyber forensics is an important tool for law enforcement agencies and other organizations in India in investigating and prosecuting cyber crimes. It involves the use of specialized techniques and tools to extract, analyze, and present digital evidence that may be relevant to a criminal case in India.

In India, cyber forensics may be used to:

- Investigate cyber crimes: Indian cyber forensics can be used to identify and track the activities of individuals or groups who are suspected of committing cyber crimes, such as hacking, identity theft, or child pornography.

- Collect and preserve digital evidence: Indian cyber forensics can be used to collect and preserve digital evidence that may be relevant to a criminal case, such as emails, text messages, and other types of electronic communication.

- Analyze electronic devices and data: Indian cyber forensics can be used to analyze the data on electronic devices, such as computers, smartphones, and tablets, in order to identify patterns of activity or extract relevant information.

- Present evidence in court: Indian cyber forensics experts may be called upon to present the results of their analysis in court in order to help prosecute cyber crimes and bring perpetrators to justice.

There are a number of challenges that law enforcement agencies and other organizations in India may face when using cyber forensics to investigate and prosecute cyber crimes. Some of these challenges include:

1. Limited resources: Like many other countries, India faces challenges in terms of limited resources, including staff and funding, which can make it difficult to effectively investigate and prosecute cybercrimes.

2. Lack of trained personnel: There is often a shortage of trained personnel in India who are skilled in cyber forensics and other areas of digital forensics. This can make it difficult for law enforcement agencies and other

organizations to effectively investigate and prosecute cybercrimes.

3. Technological challenges: Cyber forensic investigations can be complex and time-consuming, and may involve dealing with a large amount of data and a wide range of technologies. This can present challenges for law enforcement agencies and other organizations in India.
4. Legal challenges: There may be legal challenges associated with the use of cyber forensics in India, including issues related to admissibility of digital evidence in court and privacy concerns.

There are a number of best practices that law enforcement agencies and other organizations in India can follow in order to effectively use cyber forensics to investigate and prosecute cyber crimes. Some of these best practices include:

- Training: It is important for law enforcement agencies and other organizations in India to ensure that their staff are trained in the latest cyber forensic techniques and tools. This can help them to effectively extract, analyze, and present digital evidence in a reliable and accurate manner.

- Maintaining the chain of custody: It is important to maintain the chain of custody of digital evidence in order to ensure that it is admissible in court. This involves documenting the handling of the evidence at every stage of the investigation and keeping track of who has had access to it.

- Using forensic-grade tools: It is important to use forensic-grade tools when extracting and analyzing digital evidence in order to ensure the integrity of the evidence. These tools are designed specifically for use in forensic investigations and can help to prevent any contamination of the data.

- Following established protocols: It is important to follow established protocols when conducting a cyber forensic investigation in order to ensure that the evidence is collected, preserved, and analyzed in a reliable and accurate manner.

- Documenting the process: It is important to carefully document the process of the investigation in order to be able to present the results

in court. This may involve creating reports, charts, or other types of documentation to explain the findings of the investigation.

Forensic technology and practices refer to the tools, techniques, and processes that are used in forensic science to investigate and analyse evidence in criminal cases. These tools and techniques can be used to identify, preserve, extract, and analyze physical, chemical, or digital evidence in order to help solve crimes and bring perpetrators to justice.

Some common types of forensic technology and practices include:

1. Forensic ballistics: This involves the use of tools and techniques to analyse the characteristics of bullets and other types of ballistic evidence in order to determine the type of firearm that was used in a crime.

2. Forensic photography: This involves the use of specialized cameras and techniques to document crime scenes and other types of evidence in a way that is suitable for presentation in court.

3. Face, iris, and fingerprint recognition: These technologies involve the use of algorithms **and** specialized software to identify and analyse facial features, iris patterns, and fingerprints in order to identify individuals or determine their involvement in a crime.

4. Audio and video analysis: This involves the use of specialized software and techniques to analyse audio and video evidence, such as recordings of conversations or surveillance footage, in order to extract relevant information or identify individuals.

5. Forensics of handheld devices: This involves the use of specialized tools and techniques to extract and analyse data from handheld devices, such as smartphones and tablets, in order to identify relevant evidence or track patterns of activity.

Forensic ballistics

Forensic ballistics involves the use of tools and techniques to analyse the characteristics of bullets and other types of ballistic evidence in order to determine the type of firearm that was used in a crime. This may involve examining the rifling patterns on bullets, analysing the markings on cartridge cases, or comparing the characteristics of bullets and cartridge cases to those of known firearms.

The goal of forensic ballistics is to provide reliable and accurate information

about the type of firearm that was used in a crime, as well as any other relevant information about the firearm, such as its caliber or manufacturer. This information can be used to help solve crimes and bring perpetrators to justice.

There are a number of tools and techniques that are used in forensic ballistics,

including:

1. Microscopes: Microscopes are used to examine the rifling patterns on bullets and cartridge cases in order to determine the type of firearm that was used.

2. Comparison microscopes: Forensic ballistics experts may use comparison microscopes or other specialized tools to compare the characteristics of bullets and cartridge cases to those of known firearms in order to determine the type of firearm that was used.

3. Database searches: Forensic ballistics experts may use databases, such as the National Integrated Ballistics Information Network (NIBIN), to search for matches between bullets and cartridge cases found at crime scenes and those recovered from known firearms.

There are a number of steps that are typically followed in a forensic ballistics investigation:

- Collection of evidence: The first step in a forensic ballistics investigation is to collect the ballistic evidence from the crime scene. This may include bullets, cartridge cases, and any other related evidence, such as bullet fragments or damaged objects.

- Examination and analysis: The next step is to examine and analyse the ballistic evidence in order to determine the type of firearm that was used. This may involve using microscopes or other specialized tools to examine the rifling patterns on bullets and cartridge cases, or comparing the characteristics of the evidence to those of known firearms. Comparison to database: Forensic ballistics experts may use databases, such as the National Integrated Ballistics Information Network (NIBIN), to search for matches between bullets and cartridge cases found at crime scenes and those recovered from known firearms.

- Presentation of findings: The final step in the process is to present the findings of the investigation in a clear and concise manner. This may involve creating reports, charts, or other types of documentation to explain the results of the analysis.

Forensic photography

Forensic photography is a specialized field of photography that involves the use of specialized cameras and techniques to document crime scenes and other types of evidence in a way that is suitable for presentation in court. It is an important tool in the field of forensic science, as it provides a visual record of the crime scene and any relevant evidence that may be used to help solve a crime or bring perpetrators to justice.

There are a number of steps that are typically followed in forensic photography:

1. Planning: The first step in forensic photography is to plan the documentation of the crime scene or other evidence. This may involve determining the type of camera and lighting equipment that will be used, as well as the angles and perspectives that will be captured.

2. Documentation: The next step is to document the crime scene or other evidence using specialized cameras and techniques. This may involve using

specialized lighting or filters to capture detailed images of evidence, such as fingerprints or tire tracks.

3. Analysis: Once the images have been captured, they may be analysed in order to identify any relevant information or evidence. This may involve using specialized software to enhance the images or identify specific features or patterns.

4. Presentation: The final step in the process is to present the results of the analysis in a clear and concise manner. This may involve creating reports, charts, or other types of documentation to explain the findings of the investigation.

There are a number of considerations that forensic photographers must take into account when documenting crime scenes or other evidence, including:

1. Lighting: Proper lighting is crucial in forensic photography in order to capture clear and detailed images of evidence. This may involve using specialized lighting equipment, such as floodlights or lasers, or taking photographs at different times of day in order to capture the best lighting conditions.
2. Angle and perspective: It is important for forensic photographers to capture images from a variety of angles and perspectives in order to document the crime scene or other evidence as accurately as possible. This may involve using tripods, ladders, or other specialized equipment to capture images from different heights or angles.
3. Camera and lens selection: The choice of camera and lens can have a significant impact on the quality of the images captured in forensic photography. Forensic photographers often use high-quality digital cameras and lenses that are specifically designed for capturing detailed images in a variety of lighting conditions.
4. Image enhancement: Forensic photographers may use specialized software to enhance the images they have captured in order to make them clearer or to highlight specific features or patterns.

Face, iris, and fingerprint recognition:

Face, iris, and fingerprint recognition are technologies that involve the use of algorithms and specialized software to identify and analyse facial features, iris patterns, and fingerprints in order to identify individuals or determine their involvement in a crime. These technologies are often used to help identify suspects or to confirm the identity of individuals in cases where traditional methods, such as eyewitness testimony, may be unreliable.

- Face recognition: Face recognition is a technology that involves the use of algorithms and specialized software to analyse the unique characteristics of an individual's face in order to identify them. This may involve analyzing the shape, size, and placement of facial features, such as the eyes, nose, and mouth. Face recognition technology is often used to identify individuals in security or surveillance applications, such as border control or access control.

- Iris recognition: Iris recognition is a technology that involves the use of algorithms and specialized software to analyze the unique patterns in an individual's iris, the coloured part of the eye, in order to identify them. This technology is often used in security applications, such as border control or access control, as the iris is relatively stable and does not change over time.

- Fingerprint recognition: Fingerprint recognition is a technology that involves the use of algorithms and specialized software to analyze the unique patterns in an individual's fingerprints in order to identify them. Fingerprint recognition technology is often used in law enforcement and security applications to help identify individuals or confirm their identity.

There are a number of factors that can impact the accuracy and reliability of face, iris, and fingerprint recognition technologies, including:

- Quality of the image: The quality of the image is an important factor in the accuracy and reliability of these technologies. Poor quality images may contain noise, blur, or other distortions that can make it difficult for the algorithms to accurately analyze the facial features, iris patterns, or fingerprints.

- Environmental conditions: Environmental conditions, such as lighting and weather, can also impact the accuracy and reliability of these technologies. For example, low light conditions or rain may make it difficult to capture clear images of facial features, iris patterns, or fingerprints.

- Age of the image: The age of the image can also impact the accuracy and reliability of these technologies. As an individual's facial features, iris patterns, or fingerprints may change over time, older images may be less reliable for identification purposes.

- Diversity of the population: The diversity of the population can also impact the accuracy and reliability of these technologies. Systems that have been trained on a diverse population may be more accurate and reliable at identifying individuals from a wide range of backgrounds and ethnicities.

Audio Video Analysis

Audio and video analysis is a field of forensic science that involves the use of specialized software and techniques to analyze audio and video evidence, such as recordings of conversations or surveillance footage, in order to extract relevant information or identify individuals. This may involve enhancing the audio or video to make it clearer, or using software to analyze the content of the recording in order to identify voices or other relevant information.

Authentication of recordings- In many criminal cases, the authenticity of the recording and the content of the recording may be called in to question. Forensic audio and video experts can examine a variety of characteristics of the audio or video recording to determine whether the

evidence has been altered. This includes confirming the integrity (verification) of the recording, as well as authenticating that the content of the image or audio is what it purports to be.

If the ambient sound present on an audio recording changes abruptly, this could indicate that the environment where the recording took place suddenly changed.

The volume and tone of a voice on the recording can provide clues as to distance and spatial relationships within a scene.

Lighting conditions can be examined to estimate the time of day or environmental conditions at the time of the recording.

Technical details may also confirm information about a recording. For instance, an unnatural waveform present in the audio or video signal may indicate that an edit has been made.

A physical identifier may be present in the signal on magnetic tape that can identify it as a copy or indicate that it was recorded on a particular device. Sometimes a perpetrator will try to destroy Audio or video evidence;

however, using thesemethods, the recording can be analyzed to determine what occurred.

There are a number of tools and techniques that are used in audio and video analysis, including:

1. Audio enhancement: Audio enhancement involves the use of specialized software to improve the clarity and quality of audio recordings. This may involve removing background noise, increasing the volume, or enhancing the clarity of the audio in order to make it easier to understand.
2. Audio enhancement: Audio enhancement involves the use of specialized software to improve the clarity and quality of audio recordings. This may involve removing background noise,

increasing the volume, or enhancing the clarity of the audio in order to make it easier to understand.

Audio Enhancement Techniques -- For audio recordings. a variety of filters can be applied to enhance the material, bringing out specific aspects or events contained in the recording.

Frequency Equalization - Highly precise equalizers can be used to boost or cut specific bands of frequencies. To help make speech more intelligible, the frequency band containing most speech content, 200Hz-5000Hz, can be amplified or isolated If amplification is applied to a frequency range, other information residing in this frequency range will be boosted as well. If noise resides in this same range, this noise will also be increased, limiting the ability to clarify voices.

Loud background noises may be analyzed by a spectrum analyser and the corresponding frequencies reduced so that these noises are less noticeable.

Compression -Faint sounds in the recording can be boosted by compressing or levelling the signal so that the dynamic range of the material is reduced, making soft sounds more apparent.

3. Voice identification: Voice identification involves the use of specialized software to analyze the unique characteristics of an individual's voice in order to identify them. This may involve analyzing the pitch, tone, and other characteristics of the voice in order to create a unique voiceprint that can be used for identification purposes.

4. Video enhancement: Video enhancement involves the use of specialized software to improve the clarity and quality of video footage. This may involve increasing the resolution, removing noise or blur, or enhancing the contrast in order to make the footage easier to see and analyze.

Video Enhancement Techniques-A variety of enhancement techniques can be employed on video evidence. It is important that the best video recording be submitted to obtain the best enhancement results. Limitations on the enhancement process may exist if an analog copy or digital file that has undergone additional compression is submitted for analysis.

Techniques can include:

Sharpening: Makes edges of images in the recording become clearer and more distinct.

Video stabilization: Reduces the amount of movement in the video, producing the smoothest possible playback.

Masking: Covers the face or areas of the video that may protect a witness, victim or law enforcement officer.

Interlacing: In an analog system, interlaced scanning is used to record images (a technique of combining two television fields in order to produce a full frame of video). A process called de- interlacing may be used to retrieve the information in both fields of video.

Demultiplexing-Allows for isolation of each camera. In CCTV systems, a device called a multiplexer is used to combine multiple video signals into a single signal or separate a combined signal. These devices are frequently used in security and law enforcement applications for recording and/or displaying multiple camera images simultaneously or in succession.

5. Facial recognition: Facial recognition technology may be used in conjunction with video analysis in order to identify individuals in the footage. This involves the use of algorithms and specialized software to analyze the unique characteristics of an individual's face in order to identify them.

There are a number of steps that are typically followed in an audio and video analysis investigation:

1. Collection of evidence: The first step in an audio and video analysis investigation is to collect the audio or video evidence that is relevant to the case. This may involve collecting audio or video recordings from a variety of sources, such as surveillance cameras, smartphones, or other devices.
2. Analysis: The next step is to analyze the audio or video evidence in order to extract relevant information or identify individuals. This may involve using specialized software to enhance the audio or video, or using algorithms and software to analyze the content of the recording in order to identify voices or other relevant information.
3. Comparison to databases: In some cases, audio and video analysis experts may use databases, such as the National Crime Information Center (NCIC), to search for matches between individuals identified in the audio or video evidence and known individuals in order to confirm their identity.
4. Presentation of findings: The final step in the process is to present the findings of the analysis in a clear and concise manner. This may involve creating reports, charts, or other types of documentation to explain the results of the analysis.

Forensics of Handheld devices

Forensics of handheld devices involves the use of specialized tools and techniques

to extract, preserve, and analyze digital evidence from handheld devices, such as smartphones, tablets, and wearable devices. This type of forensic investigation may be used to help solve crimes or to gather evidence in civil or criminal cases. There are a number of steps that are typically followed in a forensic investigation of handheld devices:

1. Collection of evidence: The first step in a forensic investigation of handheld devices is to collect the device and any relevant evidence, such as SIM cards or memory cards. It is important to handle the device carefully to avoid damaging it or altering any evidence that may be present.
2. Preservation of evidence: The next step is to preserve the evidence on the device in order to ensure that it is not altered or damaged during the investigation. This may involve making a copy of the device's memory or creating a forensic image of the device.
3. Analysis: The next step is to analyze the device in order to extract relevant evidence. This may involve using specialized software to search for specific types of data, such as text messages, emails, or photos, or analyzing the device's logs or other system data in order to identify any relevant activity.
4. Presentation of findings: The final step in the process is to present the findings of the investigation in a clear and concise manner. This may involve creating reports, charts, or other types of documentation to explain the results of the analysis.

Forensics of Handheld devices

Forensic investigations of handheld devices involve the use of specialized tools and techniques to extract, preserve, and analyze digital evidence from handheld devices, such as smartphones, tablets, and wearable devices. This type of forensic investigation may be used to help solve crimes or to gather evidence in civil or criminal cases

There are a number of considerations that forensic experts must take into account when conducting a forensic investigation of handheld devices, including:

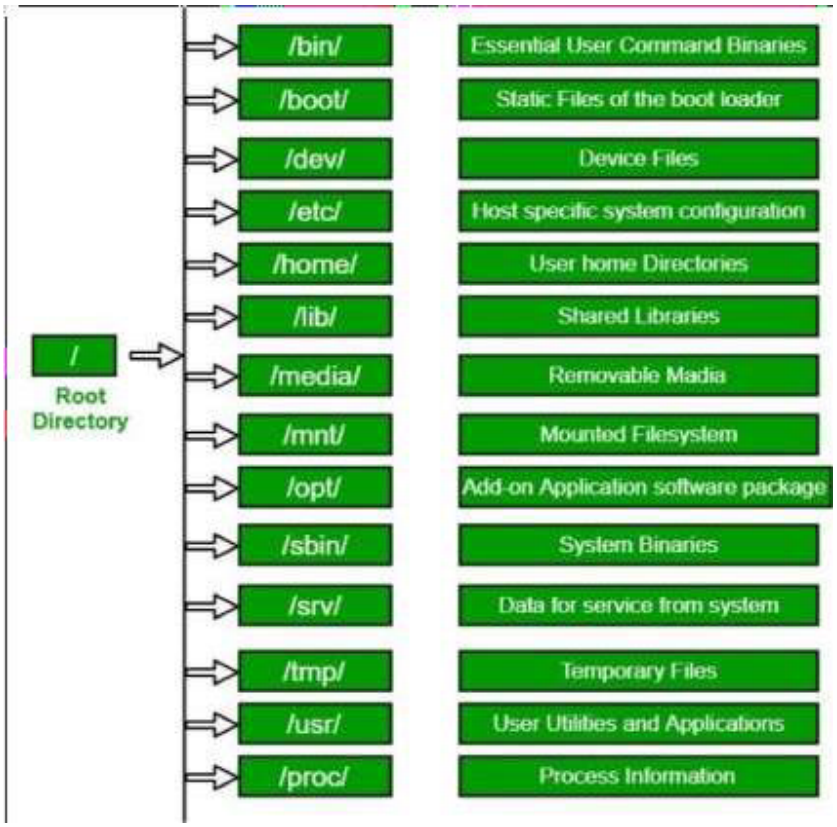
1. Device type: Different types of handheld devices may have different operating systems and hardware configurations, which can impact the tools and techniques that are used in the forensic investigation. It is important for forensic experts to be familiar with the specific characteristics of the device they are analyzing in order to ensure that they are using the appropriate tools and techniques.
2. Data types: Handheld devices may contain a wide range of data types, including text messages, emails, photos, videos, and social media posts. It is important for forensic experts to be aware of the types of data that may be present on the device and to use the appropriate tools and techniques to extract and analyze this data.
3. Data storage: Handheld devices may store data in a variety of locations, including internal memory, removable storage devices, and cloud storage. It is important

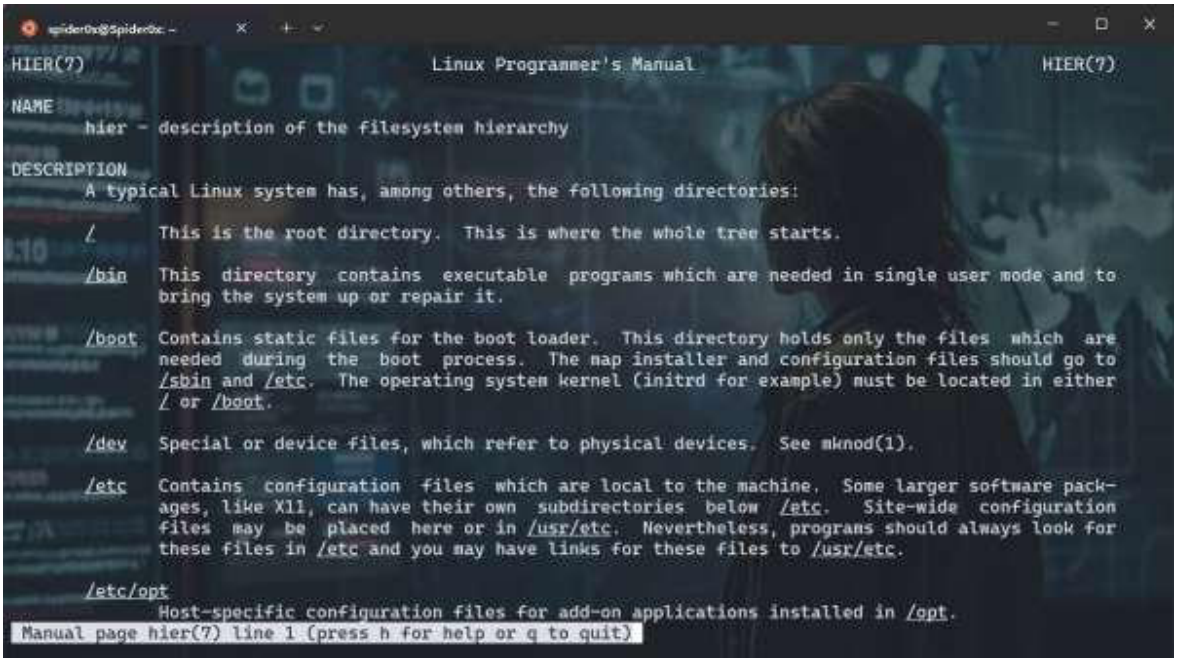
   for forensic experts to be familiar with the different storage locations and to use the appropriate tools and techniques to extract and analyze data from each location.
4. Encryption: Some handheld devices may be encrypted, which can make it difficult to extract and analyze data from the device. Forensic experts must be familiar with the various encryption technologies that may be used on handheld devices and use the appropriate tools and techniques to bypass or decrypt the data.

Linux Forensics:

Linux is a big target as almost every server is running some sort of Linux.

Linux Directory Layout





There is no stander specification forced to follow for every folder and what should be stored there so every distribution document it's file structure in `hier` man page, but always top directories remain the same.

/boot/ and efi

These directories contain files related to boot process configurations like kernel parameters and previous Linux kernels and initial ramfs.

/etc/

System wide configurations are stored here and most of them are stored in plaintext format, looking at modification and creation timestamp here is good in any forensics investigation.

/srv/

this folder contains servers' data like FTP, HTTP…

/tmp/

This folder stores temporary data and based on the distribution configuration it may be deleted periodically or on boot.

/run/

On a running system, this directory contains runtime information like PID and lock files, system runtime configuration, and more. In a forensic image it will likely be empty.

/home/ and /root/

This is home folder for any user in the system and the root user folder also.

/bin/, /sbin/, /usr/bin/, and /usr/sbin/

These are the folders storing executables in the system

/lib/ and /usr/lib/

this directory contains libraries needed by applications to run.

/usr/

The /usr/ directory contains the bulk of the system's static read-only data. This includes binaries, libraries, documentation, and more.

/var/

The /var/ directory contains system data that is changing (variable) and usually persistent across reboots. The subdirectories below /var/ are especially interesting from a forensics perspective because they contain logs, cache, historical data, persistent temporary files, the mail and printing subsystems, and much more.

/dev/, /sys/, and /proc/

These directories provide representations of devices or kernel data structures but the contents don't actually exist on a normal filesystem. When examining a forensic image, these directories will likely be empty.

/media/

The /media/ directory is intended to hold dynamically created mount points for mounting external removable storage, such as CDROMs or USB drives. When examining a forensic image, this directory will likely be empty. References to /media/ in logs, filesystem metadata, or other persistent data may provide information about user attached (mounted) external storage devices.

/opt/

The /opt/ directory contains add-on packages, which typically are grouped by vendor name or package name. These packages may create a self-contained directory tree to organize their own files (for example, bin/, etc/, and other common subdirectories).

/lost+found/

A /lost+found/ directory may exist on the root of every filesystem. If a filesystem repair is run (using the fsck command) and a file is found without a parent directory, that file (sometimes called an orphan) is placed in the /lost+found/ directory where it can be recovered. Such files don't have their original names because the directory that contained the filename is unknown or missing.

The "." files

Applications saves It's cashed and history and whatever the developer decided to store in hidden files or directories in the system, these hidden contents start with ".", there is no specifications for forcing the developer to store it in a specific place.

Interesting hidden folder is ".ssh" folder where you can look for hashed names on "known_hosts", you can't unhash them but you can find the deviations by hashing the known ones and comparing.

Although there is no standard place to store this kind of files, there is a specification for best practice recommended, The specification defines environment variables and default locations that operating systems and applications may use instead of creating their own proprietary files and directories in the user's home directory. These location environment variables and associated default locations are:

Data files: $XDG_DATA_HOME or default ~/. local/share/*

Configuration files: $XDG_CONFIG_HOME or default ~/.config/*

Non-essential cache data: $XDG_CACHE_HOME or default ~/. cache

Runtime files: $XDG_RUNTIME_DIR or typically /run/user/UID (where UID is the numeric ID of the user)

These Data, Configuration and Cache directories will contain amount of useful information for forensics investigation.

one small example of data that can be found there is in "~/.local/share/" is `*.xbel` file which contains recently used files, **Trash** which is like a recycle bin.

Crashes & Dumps

Crash Dumps can provide a significant amount of evidence in forensics investigation as it saves the content of the memory in the time of a crash that can give us a lot of information if a process was under attack or someone was trying to exploit it, we can get a list of crashes and their time stamp using the following command.

/coredumpctl.

where logs and crash files is saved is different from distribution to another so You need to conduct a small search of where this files resides in your distribution.

Linux Logs

/var/log/ is not the only place where logs are stored but definetly it's the most important one, the logs file stored there varies between different distriputions but here some geberal ones.

auth.log or /var/log/secure: Logs related to authentication and security, including login attempts, authentication failures, and security-related events.

syslog or /var/log/messages: General system logs that capture a wide range of system events, including kernel messages and system daemon messages.

kern.log: Kernel-specific logs that contain messages related to the Linux kernel.

dmesg: Kernel boot messages and hardware-related messages.

boot.log: Logs related to the system boot process.

cron: Logs for the cron scheduling daemon, which records scheduled job executions.

mail.log or /var/log/maillog: Logs for mail-related services, such as Sendmail or Postfix.

httpd/ or /var/log/apache2/: Logs for the Apache web server.

nginx/: Logs for the Nginx web server.

mysql/ or /var/log/mariadb/: Logs for the MySQL or MariaDB database server.

audit/: Audit logs that record security events and access control-related information.

auth.log: SSH login logs.

wtmp and btmp: Logs that track login and logout events. wtmp records successful logins, while btmp records failed login attempts.

lastlog: Records the last login information for each user.

ufw.log: Logs for the Uncomplicated Firewall (UFW) on Ubuntu systems.

secure: Additional security-related logs, often found on CentOS and Red Hat-based systems.

auth.log: Authentication logs on Debian and Ubuntu systems.

alternatives.log: Logs related to the alternatives system, which manages symbolic links for system commands and libraries.

Logs in Linux have the following severities.

0 emergency (emerg or panic): system is unusable

1 alert (alert): action must be taken immediately

2 critical (crit): critical conditions

3 error (err): error conditions

4 warning (warn): warning conditions

5 notice (notice): normal but significant condition

6 informational (info): informational messages

7 debug (debug): debug-level messages

you can find rsyslog configuration in

/etc/rsyslog.conf

/etc/rsyslog.d/*.conf

where you can see in the first one where the logs are stored locally the “@” means stored in another place over network.

Programs can generate messages with any facility and severity they want.

Syslog messages sent over a network are stateless, unencrypted, and based on UDP, which means they can be spoofed or modified in transit.

Syslog does not detect or manage dropped packets. If too many messages are sent or the network is unstable, some messages may go missing, and logs can be incomplete.

Text-based logfiles can be maliciously manipulated or deleted.

the Journal system is well documented in man page systemd-journald.

you can view a .journal file content using “journalctl –file filename”

There is also non stander logs that applications and servers can create its own log files to store it’s logs, these also can provide a huge amount of foresically important data that depends on the nature of the case.

Software Installation

The initial state of the distribution after installation can be found in /var/log/installer here you can see different logs about installed drivers and packages and a lot of others.

*.deb files which are package installers this is actually a compressed file containing three components

debian-binary A file containing the package format version string

control A compressed archive with scripts/metadata about the package

data A compressed archive containing the files to be installed

From a forensics perspective, we can ask many questions related to package management, such as the following:

- What packages are currently installed, and which versions?
- Who installed them, when, and how?
- Which packages were upgraded and when?
- Which packages were removed and when?
- Which repositories were used?
- Can we confirm the integrity of the packages?
- What logs, databases, and cached data can be analyzed?
- Given a particular file on the filesystem, to which package does it belong?
- What other timestamps are relevant?

package manager apt

we can get a list of installed packages in /var/lib/dpkg/status file

here are some files to look for artifacts in:

/var/log/dpkg.log dpkg activity, including changes to package status (install, remove, upgrade, and so on)

/var/log/apt/history.log Start/end times of apt commands and which user ran them

/var/log/apt/term.log Start/end times of apt command output (stdout) /var/log/apt/eipp.log.* Logs the current state of the External Installation Planner Protocol (EIPP), a system that manages dependency ordering

/var/log/aptitude Aptitude actions that were run

/var/log/unattended-upgrades/* Logs from automated/unattended upgrades

/etc/dpkg/ Configuration information for dpkg is stored here

/etc/apt/ Configuration information for apt and the sources.list and sources.list.d/* files. These files are interesting because they define the configured external repositories for a particular release is stored here

/var/lib/dpkg/info/ directory contains several files for each installed package (this is the metadata from the DEB files). This information includes the file list (*.list), cryptographic hashes (*.md5sums), preinstall/postinstall and remove scripts, and more.

/var/cache/apt/archives/ directory contains *.deb files that have been downloaded in the past.

/var/cache/debconf/ directory is a central location for package configuration information and templates.

/var/lib/snapd/snaps/ Contains downloaded snaps

~/.local/lib/python/ site-packages and ~/usr/lib/python/ site-packages are where pip installed packeges saved.

Login & User Interaction Forensics

/var/log/wtmp History of successful logins and logouts(can be parsed using “last -f filename”)

/var/log/btmp History of failed login attempts(can be parsed using “lastb -f filename”)

/var/log/lastlog Most recent user logins

/var/run/utmp Current users logged in (only on running systems)

An Interesting place to look at a forensics investigation is initialization scripts

/etc/profile

/etc/profile.d/*

~/.bash_profile

/etc/bash.bashrc

~/.bashrc

the profile file runs once at the first shell and “*rc” files runs every time you open a shell.

/etc/bash.bash_logout

~/.bash_logout

these files also run one on exit and logout.

Environment variables

Environment variables are also a good place to look where you can find more about the user's default editor which may tell you where to look for more evidence and customized environment variables which can give you good hints.

here are some places to look at default environment variables at login.

/etc/security/pam_env.conf

/etc/environment

/etc/environment.d/*.conf

/usr/lib/environment.d/*.conf

~/.config/environment.d/*.conf

"HIST*" environment variables where the shell history is configured that will tell you about where the shell history stored and how it's configured.

Another note here is that command history of a shell is written only after the shell exits.

Also, note that the newly written bash history dropped to the disk is written to a new inode and the old one is still there in the disk unallocated so you can find old bash history files using carving.

Windows managers also have some start-up "*.desktop" files have the applications to start at start-up.

/etc/xdg/autostart/*

~/.config/autostart/*

For the Desktop setting, there is a database called dconf which is much like the Windows registry where the data is stored in hierarchy key-value pairs.

"GNOME" desktop manager

tool to parse this database content:

the "dconf" files can be found in "~/.config/dconf/" and "/etc/dconf/db/" as example you can look at "user" database where user setting can be found.

There is alot of Clipboard managers out there that stores from 5-20 history copied data but as there is alot out there you will need to search for where your manager stores this data.

Recent Documents and favourites in linux are kept track of for every user in linux in different places like…

.local/share/recently-used.xbel

.local/user-places.xbel

.local/share/Recent Documents/

Search history also is kept track of for every user each desktop manger has it's own way, for example in GNOME search is saved to

"~/.cache/tracker3/files" as sqlite databases.

3.5 Network Forensics Overview

Network forensics is the process of collecting and analyzing raw network data and tracking network traffic systematically to ascertain how an attack was carried out or how an event occurred on a network. Because network attacks are on the rise, there's more focus on this field and an increasing demand for skilled technicians. Labour forecasts predict a shortfall of 50,000 network forensics specialists in law enforcement, legal firms, corporations, and universities.

Network forensics can also help you determine whether a network is truly under attack or a user has inadvertently installed an untested patch or custom program, for example. A lot of time and resources can be wasted determining that a bug in a custom program or an untested open-source program caused the —attack.‖

Network forensics examiners must establish standard procedures for how to acquire data after an attack or intrusion incident. Typically, network administrators want to find compromised.

3.5.1 Securing a Network

Network forensics is used to determine how a security breach occurred; however, steps must be taken to harden networks before a security breach happens, particularly with recent increases in network attacks, viruses, and other security incidents. Hardening includes a range of tasks, from applying the latest patches to using a layered network defense strategy, which sets up layers of protection to hide the most valuable data at the innermost part of the network. It also ensures that the deeper into the network an attacker gets, the more difficult access becomes and the more safeguards are in place. The National Security Agency (NSA) developed a similar approach, called the defense in depth (DiD) strategy. DiD have three modes of protection:

- People
- Technology
- Operations

If one mode of protection fails, the others can be used to thwart the attack.
Listing people as a mode of protection means organizations must hire well-qualified people and treat them well so that they have no reason to seek revenge. In addition, organizations should make sure employees are trained adequately in security procedures and are familiar with the organize- tion's security policy. Physical and personnel security measures are included in this mode of protection.

The technology mode includes choosing strong network architecture and using tested tools, such as intrusion detection systems (IDSs) and firewalls. Regular penetration testing coupled with risk assessment can help improve network security, too. Having systems in place that allow quick and thorough analysis when a security breach occurs is also part of the technology mode of protection.

Operation mode addresses day to day operations. Updating security patches, antivirus software and operating systems falls into this category. Assessment and

monitoring procedures and disaster recovery plans.

3.5 Performing Live Acquisitions

The problem investigators face is the order of volatility (OOV), meaning how long a piece of information lasts on a system. Data such as RAM and running processes might exist for only milliseconds; other data, such as files stored on the hard drive, might last for years. The fol- lowing steps show the general procedure for a live acquisition, although investigators differ on exact steps:

- Create or download a bootable forensic CD, and test it before using it on a suspect drive. If the suspect system is on your network and you can access it remotely, add the appropriate network forensics tools to your workstation. If not, insert the bootable forensics CD in the suspect system.
- Make sure you keep a log of all your actions; documenting your actions and reasons for these actions is critical.
- A network drive is ideal as a place to send the information you collect.If you don't have one available, connect a USB thumb drive to the suspect system for collecting data. Be sure to note this step in your log.
- Next, copy the physical memory (RAM). Microsoft has built-in tools for this task, or you can use available freeware tools, such as mem fetch (*www.freshports.org/sysutils/ memfetch*) and Back Track

The next step varies, depending on the incident you're investigating. With an intrusion, for example, you might want to see whether a rootkit is present by using a tool such as Root Kit Revealer (*www.microsoft.com/technet/sysinternals/Utilities/ RootkitRevealer.mspx*).

- You can also access the system's firmware to see whether it has

changed, create an image of the drive over the network, or shut the system down and make a static acquisition later.

- Be sure to get a forensically sound digital hash value of all files you recover during the live acquisition to make sure they aren't altered later.

Performing a Live Acquisition in Windows

Live acquisitions are becoming more necessary, and several tools are available for capturing RAM. ManTech Memory DD (*www.mantech.com/msma/MDD.asp*) can access up to 4 GB RAM in standard did format. Another freeware tool, Win32dd (*http://win32dd.msuiche.net*), runs from the command line to perform a memory dump in Windows. In addition, comer- coal tools, such as Guidance Software Winen.exe, can be used.

Another popular tool is Backtrack (*www.remote-exploit.org/backtrack.html*), which combines tools from the White Hat Hackers CD and The Auditor CD (see Figure 11-3). More than 300 tools are available, including password crackers, network sniffers, and freeware forentices tools. Backtrack has become popular with penetration testers and is used at the annual Collegiate Cyber Defense Competitions.

Fig:Some of the tools available in BackTrack

3.6 Developing Standard Procedures for Network Forensics

Network forensics is a long, tedious process, and unfortunately, the trail can go cold quickly. A standard procedure often used in network forensics is as follows:

- Always use a standard installation image for systems on a network. This image isn't a bit-stream image but an image containing all the standard applications used. You should also have the MD5 and SHA-1 hash values of all application and OS files.
- When an intrusion incident happens, make sure the vulnerability has been fixed to prevent other attacks from taking advantage of the opening.
- Attempt to retrieve all volatile data, such as RAM and running processes, by doing a live acquisition before turning the system off.
- Acquire the compromised drive and make a forensic image of it.
- Compare files on the forensic image to the original installation image. Compare hash values of common files, such as Win.exe and standard DLLs, and ascertain whether they have changed.

In computer forensics, you can work from the image to find most of the deleted or hidden files and partitions. Sometimes you restore the image to a physical drive so that you can run programs on the drive. In network forensics, you have to restore the drive to see how malware attackers have installed on the system works. For example, intruders might have transmitted a Trojan program that gives them access to the system and then installed a root kit, which is a collection of tools that can perform network reconnaissance tasks (using the ls or net stat command to collect information, for instance), key logging, and other actions.

3.7 Using Network Tools

A variety of tools are available for network administrators to perform remote

shutdowns, monitor device use, and more. The tools covered in this chapter are freeware and work in Windows and UNIX. Sysinternals (*www.microsoft.com/technet/sysinternals/*) is a collection of free tools for examining Windows products. They were created by Mark Russinovich and Bryce Cogs well and acquired by Microsoft.

Fig: Opening page of Sysinternals

The following list describes a few examples of the powerful Windows tools available at Sysinternals:

- RegMon shows all Registry data in real time.
- Process Explorer shows what files, Registry keys, and dynamic link libraries (DLLs) are loaded at a specific time.
- Handle shows what files are open and which processes are using these files.
- Filemon shows file system activity.

Far too many tools are available to list here, but you should take some time to explore the site and see what's available. One in particular that's worth investigating is PsTools, a suite created by Sysinternals that includes the following tools:

- *PsExec*—Runs processes remotely

- *PsGetSid*—Displays the security identifier (SID) of a computer or user

- *PsKill*—Kills processes by name or process ID

- *PsList*—Lists detailed information about processes

- *PsLoggedOn*—Displays who's logged on locally

- *PsPasswd*—Allows you to change account passwords

- *PsService*—Enables you to view and control services

- *PsShutdown*—Shuts down and optionally restarts a computer

- *PsSuspend*—Allows you to suspend processes

UNIT – 5

LAWS and ACTS

UNIT 5

Laws and Acts: Laws and Ethics

I. Introduction

- Cybercrime and digital forensics as emerging fields
- The need for laws and acts to govern cybercrime investigations
- The importance of ethics in handling digital evidence

- Federal law in the United States that criminalizes unauthorized access to computer systems
- Provisions for penalties, including fines and imprisonment

B. Cybersecurity Information Sharing Act (CISA)

- Promotes the sharing of cybersecurity threat information between private and public entities
- Encourages the protection of information systems and facilitates the investigation of cybercrimes

- Regulates the interception of electronic communications and unauthorized access to stored electronic communications
- Defines legal requirements for law enforcement in obtaining electronic evidence

C. Electronic Communications Privacy Act (ECPA)

D. General Data Protection Regulation (GDPR)

II. Laws and Acts related to Cyber Crime Investigations

A. Computer Fraud and Abuse Act (CFAA)

- European Union regulation that protects the privacy and personal data of EU citizens
- Sets guidelines for data protection, data breach reporting, and consent for data processing

III. Laws and Acts related to Digital Forensics A. Federal Rules of

- Governs the admissibility of digital evidence in U.S. federal courts
- Establishes standards for authentication and reliability of electronic evidence

B. Digital Millennium Copyright Act (DMCA)

- Protects copyrighted material in the digital realm
- Prohibits the circumvention of technological measures used to protect copyrighted works

C. Law Enforcement Tools and Techniques Act (LETTA)

- Preservation of integrity, confidentiality, and professionalism in handling digital evidence
- Compliance with legal and regulatory requirements
- Respect for privacy rights and protection of personal information
- Proper documentation and reporting of findings
- Continuous professional development and adherence to ethical standards

- Addresses issues related to the use of investigative tools and techniques in digital forensics
- Ensures proper authorization and oversight when conducting forensic examinations

IV. Ethics in Cyber Crime Investigations and Digital Forensics

V. International Cooperation and Treaties

- Mutual legal assistance treaties (MLATs) for cross-border collaboration in cybercrime investigations
- Budapest Convention on Cybercrime as an international framework for combating cybercrime
- Extradition treaties to facilitate the prosecution of cybercriminals across jurisdictions

VI. Challenges and Future Developments

- Rapidly evolving nature of technology and the need for laws to keep pace
- Jurisdictional issues in cross-border investigations
- Balancing privacy rights and law enforcement needs
- Advancements in encryption and anonymization techniques and their impact on investigations

Digital Evidence Controls

I. Introduction

- Importance of digital evidence in investigations and legal proceedings
- Need for proper controls to ensure the integrity, authenticity, and admissibility of digital evidence

II. Chain of Custody

A. Definition and Purpose

- Chain of custody as the documented record of the movement and handling of evidence
- Ensures the integrity and admissibility of evidence in court

B. Key Elements of Chain of Custody

1. Documentation
- Detailed records of evidence collection, storage, and transfers
- Includes date, time, location, individuals involved, and any relevant observations
2. Security and Storage
- Secure and controlled storage of digital evidence to prevent tampering, loss, or unauthorized access
- Use of tamper-evident seals, locked containers, and access controls
3. Transfer and Transport
- Proper packaging and labeling of evidence during transfers
- Use of secure and tracked transportation methods when necessary
4. Logging and Monitoring
- Regular monitoring and logging of access to evidence storage areas
- Controls to prevent unauthorized access and detect any suspicious activities

III. Authentication and Verification

A. Digital Signature

- Use of cryptographic techniques to ensure the authenticity and integrity of digital evidence
- Digital signatures provide a unique identifier and verify the identity of the sender

B. Hash Functions

- Calculating and verifying cryptographic hash values to ensure data integrity
- Hash functions generate a unique string of characters that represents the data

C. Time Stamping

- Assigning a trusted timestamp to digital evidence to establish the chronological order of events
- Ensures the integrity and prevents backdating or tampering with evidence

IV. Preservation and Imaging

A. Preservation

- Preventing alteration, loss, or destruction of digital evidence during storage
- Use of write-protect mechanisms, storage in controlled environments, and regular backups

B. Imaging

- Creating a forensic image or bit-by-bit copy of digital storage media
- Ensures preservation of evidence while allowing analysis without altering the original data

V. Access Controls and Security

A. Access Authorization

- Restricting access to digital evidence to authorized personnel only
- Use of access control lists, user authentication, and role-based permissions

B. Encryption and Password Protection

- Encrypting digital evidence to protect it from unauthorized access or disclosure
- Use of strong passwords and encryption algorithms

C. Physical Security

- Safeguarding physical storage media to prevent theft, loss, or damage
- Locked cabinets, restricted access areas, and surveillance systems

VI. Documentation and Reporting A. Case Documentation

- Detailed documentation of all actions taken during the investigation, including evidence handling

B. Expert Testimony

- Clear and concise reports to provide a transparent account of the investigation process

- Preparation of expert testimony to explain the technical aspects of digital evidence to the court
- Clear and understandable communication to assist the judge and jury in making informed decisions

VII. Legal and Regulatory Compliance

- Adherence to applicable laws, regulations, and standards related to digital evidence
- Compliance with data protection and privacy requirements during the investigation process

VIII. Continuous Training and Quality Assurance

- Ongoing training and education for investigators and forensic examiners
- Quality assurance procedures to ensure adherence to best practices and standards

Evidence handling procedures in cybercrime investigation and forensic analysis:

- Identification: Clearly identify and document the evidence, including the date, time, location, and any relevant details.

- Preservation: Take necessary steps to preserve the integrity of the evidence. This may involve creating a forensic copy of the original data or device to prevent any modifications.

- Chain of Custody: Maintain a detailed record of everyone who has accessed or handled the evidence. Document the date, time, and purpose of each interaction to ensure the integrity and admissibility of the evidence in legal proceedings.

- Documentation: Thoroughly document the evidence, including its source, location, and relevant metadata. Record any relevant observations or findings during the investigation process.

- Packaging and Labeling: Properly package the evidence in appropriate containers to prevent contamination, damage, or loss. Label each item with a unique identifier, description, and other relevant information.

- Transport and Storage: Safely transport the evidence to a secure storage facility or laboratory. Follow appropriate protocols to protect the evidence during transportation and ensure its secure storage to prevent unauthorized access.

- Analysis and Examination: Conduct forensic analysis on the evidence using approved methods and tools. Follow best practices and adhere to legal requirements when examining the evidence to maintain its integrity.

- Reporting: Prepare detailed reports that document the analysis procedures, findings, and conclusions. Include any relevant information that may be required in legal proceedings.

- Retention and Disposal: Establish retention policies for retaining evidence based on legal requirements and organizational guidelines. Properly dispose of evidence when it is no longer needed, adhering to relevant regulations and protocols.

- Compliance with Legal and Ethical Standards: Ensure that all evidence handling procedures comply with applicable laws, regulations, and ethical standards. Adhere to privacy and data protection requirements during the investigation and handling of sensitive information.

Brief overview of the basics of the Indian Evidence Act, Indian Penal Code (IPC), and Code of Criminal Procedure (CrPC):

1. Indian Evidence Act:
- The Indian Evidence Act, 1872, is the legislation that governs the rules and procedures related to the admissibility and proof of evidence in Indian courts.
- It applies to all judicial proceedings in both civil and criminal cases.
- The act defines various types of evidence, such as oral evidence, documentary evidence, expert evidence, and circumstantial evidence.
- It outlines the rules for relevancy, admissibility, and examination of evidence.
- The act also covers provisions related to burden of proof, presumption of facts, and estoppel.
- It provides guidelines on the examination and cross-examination of witnesses, including the competency and compellability of witnesses.

2. Indian Penal Code (IPC):
- The Indian Penal Code, 1860, is the primary criminal code of India that defines and classifies various criminal offenses and their punishments.
- It applies to all offenses committed within the territory of India.
- The IPC categorizes offenses into different chapters based on their nature, such as offenses against the human body, property, public tranquility, the state, and more.
- Each offense is described with its essential elements and the corresponding punishment.

3. Code of Criminal Procedure (CrPC):
- The Code of Criminal Procedure, 1973, is the legislation that governs the procedural aspects of criminal law in India.
- It lays down the procedures for the investigation, trial, and punishment of criminal offenses.
- The CrPC establishes the powers and jurisdiction of criminal courts, the rights of accused persons, and the roles of various stakeholders in the criminal justice system.
- It covers procedures for the arrest, bail, remand, and release of accused individuals.

- The code also outlines the rules for the conduct of trials, including the examination of witnesses, recording of statements, framing of charges, and pronouncement of judgments.

It's important to note that the Indian Evidence Act, IPC, and CrPC are extensive pieces of legislation, and this overview provides only a general understanding of their basics. For detailed and accurate information, it is advisable to refer to the official texts of these acts or consult legal professionals who are well-versed in Indian law.

Electronic Communications Privacy Act (ECPA) in the context of cybersecurity, laws, and ethics.

The Electronic Communications Privacy Act (ECPA) is a United States federal law enacted in 1986 to establish privacy protections for electronic communications. The law addresses the interception, use, and disclosure of electronic communications and provides guidelines for law enforcement activities related to accessing electronic communications data.

Key provisions of the ECPA include:

1. Title I: Wiretap Act
   - Title I of the ECPA, also known as the Wiretap Act, governs the interception of wire, oral, and electronic communications.
   - It establishes requirements for obtaining warrants to intercept electronic communications in real-time or to access stored electronic communications.
   - The Wiretap Act generally prohibits the interception of electronic communications unless authorized by a warrant or certain exceptions apply.

2. Title II: Stored Communications Act (SCA)

- Title II of the ECPA, known as the Stored Communications Act (SCA), regulates access to stored electronic communications and records held by third-party service providers.
- It establishes rules for government access to emails, text messages, and other electronic communications stored by internet service providers (ISPs) or other communication service providers.
- The SCA provides different standards and procedures for accessing different types of stored communications, such as opened emails, unopened emails, and electronic records.

3. Title III: Pen Register and Trap-and-Trace Device Act
- Title III of the ECPA governs the use of pen register and trap-and-trace devices by law enforcement agencies.
- It allows the government to collect non-content information, such as phone numbers dialed, email addresses contacted, or IP addresses visited, to investigate criminal activities.
- The Pen Register and Trap-and-Trace Act requires law enforcement to obtain court orders to install and use these devices, except under specific circumstances.

4. Additional Amendments and Protections
- Over the years, the ECPA has undergone various amendments to adapt to changing technologies and address emerging privacy concerns.
- Amendments have been made to extend the protections of the ECPA to emerging communication technologies, such as VoIP, web-based email, and cloud storage.
- The law includes provisions to protect the privacy of electronic communications, establish limitations on government surveillance, and provide remedies for violations.

Ethical considerations in cybersecurity:
In addition to legal requirements, ethical considerations play a crucial role in cybersecurity. Ethical practices involve:

1. Protecting User Privacy: Respecting and safeguarding the privacy of individuals' electronic communications, data, and personal information.

2. Ensuring Security: Taking appropriate measures to protect systems, networks, and data from unauthorized access, breaches, and cyber threats.

3. Responsible Vulnerability Disclosure: Following responsible vulnerability disclosure practices to report discovered security flaws to relevant parties, allowing them to address and fix vulnerabilities without causing harm.

4. Compliance with Ethical Standards: Adhering to professional codes of ethics and industry best practices in the field of cybersecurity.

It's important to consult legal experts and ethical guidelines specific to your jurisdiction and organization for a comprehensive understanding of laws, regulations, and ethical practices related to cybersecurity and privacy protection.

legal policies:

1. Privacy Policies:
   - Privacy policies outline how organizations collect, use, store, and disclose personal information of individuals.
   - They inform individuals about their rights and provide transparency regarding data handling practices.
   - Privacy policies are essential for complying with data protection laws and building trust with users.

2. Acceptable Use Policies (AUP):
   - Acceptable use policies establish guidelines for the acceptable and appropriate use of organizational resources, such as computer networks, systems, and internet access.
   - AUPs define prohibited activities, including unauthorized access, distribution of malware, harassment, or copyright infringement.

- These policies promote responsible and lawful use of resources and protect organizations from legal and security risks.

3. Information Security Policies:
- Information security policies outline the procedures and guidelines for protecting sensitive information and maintaining the security of organizational systems and networks.
- They cover aspects such as access control, password management, incident response, data classification, and employee responsibilities.
- Information security policies help mitigate risks and ensure the confidentiality, integrity, and availability of data and systems.

4. Data Retention and Deletion Policies:
- Data retention and deletion policies define how long organizations retain different types of data and specify the procedures for securely deleting data when it is no longer needed.
- These policies ensure compliance with legal requirements and help manage data storage efficiently.
- Organizations should consider data minimization principles and the principles of purpose limitation and storage limitation when creating these policies.

5. Intellectual Property Policies:
- Intellectual property policies protect an organization's intellectual property rights, including copyrights, trademarks, and patents.
- They outline guidelines for the use, protection, and enforcement of intellectual property assets.
- These policies help prevent unauthorized use, misuse, or infringement of intellectual property and support the organization's innovation and competitive advantage.

6. Incident Response Policies:
- Incident response policies provide a framework for handling security incidents, such as data breaches, cyber-attacks, or system compromises.

- They define roles, responsibilities, and procedures for detecting, reporting, containing, investigating, and recovering from security incidents.
- Incident response policies help minimize damage, facilitate effective incident management, and support compliance with legal obligations.

These are just a few examples of legal policies commonly implemented by organizations. The specific policies needed may vary depending on the nature of the organization, its industry, and applicable legal requirements. It's important to tailor policies to the organization's specific needs and consult legal professionals to ensure compliance with relevant laws and regulations.