UNIT-I

Introduction and Overview of Cyber Crime

WHAT IS CYBER CRIME:

cybercrime, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government.

Because of the early and widespread adoption of computers and the Internet in the United States, most of the earliest victims and villains of cybercrime were Americans. By the 21st century, though, hardly a hamlet remained anywhere in the world that had not been touched by cybercrime of one sort or another.

Cybercrime Introduction :

Cybercrime refers to criminal activities carried out through digital means or the internet. It encompasses a broad range of illegal activities that target individuals, organizations, or even governments with the intent of causing harm, stealing sensitive information, financial gains, or disrupting normal operations. Cybercriminals utilize sophisticated techniques and tools to exploit computer systems, networks, and digital device vulnerabilities.

As technology advances, cybercrime remains a constantly evolving and complex challenge. Prevention of cybercrime requires a combination of cybersecurity measures, user awareness, cybercrime information, and responsible digital practices to safeguard personal and sensitive data from falling into the wrong hands.

How to Prevent Cybercrime :

- Keep Software Updated: Regularly update operating systems, applications, and antivirus software. These updates often include critical security patches that help defend against known vulnerabilities.

- Strong Passwords: Use unique passwords for all your online accounts and devices. Avoid using easily guessable information; consider using a password manager to keep track of complex passwords.

- Enable Multi-Factor Authentication (MFA): Implement MFA whenever possible. This adds an extra layer of security by requiring additional verification beyond just a password, such as a one-time code sent to your mobile device.

- Be Cautious with Emails: Avoid clicking links or downloading attachments from unknown or suspicious sources. Be vigilant for phishing attempts and verify the sender's authenticity before sharing sensitive information.

- Secure Wi-Fi Networks: Use strong passwords for your Wi-Fi networks and enable WPA2 or WPA3 encryption. Avoid using public Wi-Fi for sensitive activities like online banking or accessing personal accounts.

- Install Firewalls: Implement firewalls to control incoming and outgoing network traffic and prevent unauthorized access.

- Secure Mobile Devices: Use passcodes or biometric authentication on your mobile devices. Install security apps that remotely locate, lock, or erase your device in case of loss or theft.

Fundamental knowledge about cybercrime is also essential before you implement all these measures. By implementing these preventive measures and staying vigilant, you can significantly reduce the risk of falling victim to cybercrime and protect your digital assets and personal information. Cybersecurity is an ongoing process, and staying proactive is key to maintaining a safe online environment.

Cybercrime Examples :

- Phishing: Attempting to deceive individuals into sharing sensitive information such as passwords, credit card details, or personal data by posing as a trustworthy entity.

- Malware Attacks: Distributing malicious software like viruses, worms, ransomware, or spyware to infect and gain unauthorized access to computer systems.

- Hacking: Unauthorized entry into computer systems or networks to access, modify, or steal information.

- Identity Theft: Stealing personal information to assume another person's identity for fraudulent purposes.

- Distributed Denial of Service (DDoS) Attacks: Overloading a website or online service with excessive traffic to disrupt its normal functioning and make it unavailable to users.

- Cyberstalking and Cyberbullying: Harassment or threatening behavior directed at individuals using digital communication channels.

- Data Breaches: Unauthorized access and exposure of sensitive information from databases, resulting in potential misuse.

- Online Scams: Deceptive schemes, such as fake online marketplaces or investment opportunities, to defraud victims of their money.

- Social Engineering: Manipulating individuals through psychological tactics to divulge confidential information or perform specific actions.

- Cyber Espionage: Illegally gathering confidential information from organizations or governments for political, economic, or competitive advantage.

Understanding Cyber Crime

Cyber crime refers to illegal activities conducted via the internet or through the use of information technology. It encompasses a wide range of offences including hacking, data theft, online fraud, cyber terrorism and identity theft. The anonymity provided by the digital space allows cyber criminals to operate with a degree of impunity, making cyber crime an appealing avenue for illicit activities.

Nature of Cyber Crime in India

The nature of cyber crime in India is multifaceted and constantly evolving. The most common forms of cyber crime in the country include:

- **Phishing:** Fraudulent attempts to obtain sensitive information such as usernames, passwords and credit card details by disguising as a trustworthy entity in an electronic communication.
- **Ransomware**: A type of malicious software designed to block access to a computer system until a sum of money is paid.
- **Data Breaches:** Unauthorised access and theft of personal or corporate data.
- **Online Scams:** Various schemes that deceive users into paying money for fraudulent services or goods.
- **Cyber Stalking and Harassment:** Using the internet to stalk or harass an individual, group or organisation.
- **Identity Theft:** Stealing personal information to impersonate someone else for financial gain or other benefits.

Scope of Cyber Crime in India

The scope of cyber crime in India is expansive and growing. Factors contributing to the rise in cyber crime include:

- **Rapid Digitisation:** As more services move online, from banking to government documentation, the opportunities for cyber crimes increase.
- **Lack of Cybersecurity Awareness:** Many users lack basic cybersecurity knowledge, making them easy targets for cyber criminals.
- **Inadequate Cybersecurity Infrastructure:** Despite improvements, many Indian businesses and organisations still do not invest sufficiently in cybersecurity measures.
- **High Internet Penetration:** With over 700 million internet users, the sheer volume of digital transactions in India presents numerous opportunities for cyber criminals.

Impacts of Cyber Crime

The impacts of cyber crime are profound and varied, affecting economic, social and personal dimensions. Economically, cyber crime leads to significant financial losses for individuals and businesses. Socially, it undermines trust in digital transactions. On a personal level, victims of cyber crimes like identity theft or online harassment can suffer severe emotional and psychological distress.

Combatting Cyber Crime in India

The Indian government, along with private sector stakeholders, has taken several steps to combat cyber crime:

- **Legal Framework:** India has enacted various cyber laws, such as the Information Technology Act, 2000, which provides legal recognition and protection for transactions carried out by means of electronic data interchange and other means of electronic communication.
- **Cyber Police Units:** Specialised cyber crime police units and cells have been established across the country to handle cyber crimes specifically.
- **Awareness Campaigns:** The government and various NGOs are regularly conducting awareness programs to educate the public about the risks of cyber crime and the importance of cybersecurity.
- **Collaboration with International Agencies:** India collaborates with international bodies and foreign governments to enhance cyber security measures and tackle cross-border cyber crimes.

The IT Act, 2000: Foundation and Framework

The Information Technology Act, 2000, marks a significant step in Indian legal history, being the first law aimed at regulating cyber activities in the country. It was based on the United Nations Model Law on Electronic Commerce 1996 (UNCITRAL Model), which was recommended by the General Assembly of the United Nations. The main objective of the IT Act is to provide a legal framework for electronic governance by giving recognition to electronic records and digital signatures.

Types of Cyber Crime: Social Engineering

1. Phishing

Phishing is one of the most common social engineering techniques. With phishing scams, attackers send emails that appear to be from reputable sources to trick individuals into revealing sensitive information like passwords and credit card numbers.

These emails often inspire a sense of urgency, prompting the victim to click on a malicious link. This link leads them to a fake website where they are asked to enter personal data such as login credentials, account information, social security numbers, or other confidential information.

In 2013, Target Corporation fell victim to a phishing attack where attackers initially gained access to their network through a phishing email sent to an HVAC company that had connections with Target. This led to a data breach that compromised the credit card information of over 40 million customers.

Target isn't the only organization to suffer a cyberattack in this way: a 2022 study conducted by Ponemon Institute revealed 54% of organizations experienced a data breach caused by one of their third-party vendors in the previous 12 months.

2. Clone phishing

Clone phishing is a special type of phishing attack where a legitimate email is used to create an almost identical or "cloned" email but with some critical changes.

Here is how clone phishing campaigns typically work:

1. **Email selection**: The attacker selects a legitimate email that was sent to the intended victim. This email could be anything from a routine company announcement to an invoice or an account notification.

2. **Creating the clone**: The attacker makes a copy or "clone" of the email, reproducing it as closely as possible to the original.

3. **Altering the content**: The attacker alters some elements of the cloned email. This usually involves changing the links or attachments within the email to malicious ones. For example, where the original email might have contained a link to an online invoice, the clone could contain a link to a malicious website designed to harvest login credentials.

4. **Resending the email**: The attacker sends the cloned email to the original recipients but makes it appear as if it's coming from the same sender as the original email. This might be accompanied by a pretext such as an updated link, a corrected version of the attachment, or any excuse that seems plausible.

5. **Victim's response**: If recipients of the cloned email believe it's a legitimate follow-up to the previous email, they might click on the link or download the attachment without suspicion. This can lead to the compromise of sensitive data or malware infection.

Clone phishing is particularly effective because it uses the trust established by the original, legitimate email to bypass the victim's defenses. It's always important to verify the authenticity of email communications, especially those containing links or attachments, even if they appear to come from a known source. It’s advisable to contact the person or company directly to confirm the legitimacy of the email, especially if the email seems unexpected or slightly different from the usual communication style.

3. Pretexting

Pretexting involves an attacker creating a fabricated scenario to obtain information from a target. They often impersonate someone in a position of authority or someone with a legitimate reason for needing the information.

The attacker builds a story that convinces the victim to divulge sensitive information or perform an action that compromises security.

Pretexting as a tactic is used in a variety of social engineering attacks, particularly phishing, whaling, and business email compromise. But cybercriminals can also use pretexting on its own to steal valuable information from their victims.

In 2016, a hacker gained access to data for thousands of employees at the Justice Department and Department of Homeland Security, including email addresses and phone numbers, by impersonating a government employee. They later published the information online.

4. Baiting

Baiting is similar to phishing but involves the promise of a specific item that the attacker uses as bait. This could be free software, gift cards, movie or music downloads, or anything else that seems appealing to the target. The attacker uses this bait to entice the victim into downloading malicious software or revealing login credentials.

USB drops are a classic example of baiting. The US Department of Homeland Security once ran a test on government employees to see how easy it would be for hackers to install malware or gain access to computer systems. USB drives were dropped in parking lots of government agencies and private contractors — and 60% of the people who picked them up plugged them into their devices. If the drive had an official logo on it, 90% were plugged in.

5. Quid pro quo

With quid pro quo attacks, threat actors prey on the law of psychological reciprocity — when someone helps us out, we want to return the favor.

Often, quid pro quo attacks happen when cybercriminals pose as IT or tech support. They may offer to install anti-virus software or resolve an issue with a computer system in exchange for sensitive information like login credentials. Once they gain access, they install malware or steal other sensitive data.

6. Business email compromise & CEO fraud

Business Email Compromise (BEC) is when an attacker gains access to a corporate email account and impersonates the owner to defraud the company or its employees, customers, or partners. They usually focus on employees who have access to company finances and trick them into conducting money transfers to bank accounts thought to be trusted.

CEO fraud is a specific type of BEC scam where attackers impersonate a CEO or another high-ranking managerial official. The attacker leverages the authority of the CEO to pressure an employee into conducting unauthorized transactions or sending sensitive data.

7. Deepfaking

Deepfaking involves using AI technologies to create realistic images, videos, or audio to manipulate or deceive. Attackers can create audio and video that looks authentic, showing individuals saying or doing things they did not actually say or do.

8. Tailgating

Tailgating, also known as piggybacking, involves an unauthorized person physically following an authorized person into a restricted area.

The attacker may strike up a conversation or carry something to manipulate the authorized person into holding the door open for them.

While tailgating and piggybacking attacks typically refer to unauthorized physical access, in one interesting case a tech worker admitted to piggybacking off a hacker’s extortion attempt.

9. Spear phishing & whaling

Spear Phishing is a more targeted form of phishing. The attacker customizes their deceptive messages to a specific individual or organization.The emails appear more legitimate and are often meticulously crafted to appeal to the victim.Whaling targets high-profile individuals, such as executives, celebrities, or politicians. The tactics are similar to spear-phishing but on a grander scale.

. 10. Smishing & vishing

Smishing (SMS phishing) uses text messages, while Vishing (voice phishing) uses phone calls to scam the victim. These attacks are designed to steal sensitive data or money by posing as a legitimate entity.

In July 2020, Twitter famously suffered a hack of 130 blue-check verified accounts of some of the world's most famous people — from politicians like Barack Obama and Joe Biden, celebrities and entrepreneurs like Bill Gates and Elon Musk, and global brands like Apple.

11. Watering hole attacks

In a watering hole attack, the attacker identifies a website or resource their target group frequently uses and infects it with malware to compromise members of the group. For example, if the target group is in the financial sector, the attacker might infect a popular financial news website.

In February 2021, hackers used a watering hole attack to gain access to a water treatment facility in Florida. They remotely changed a setting that drastically raised the amount of sodium hydroxide (lye) in the water to toxic levels. Luckily, an astute operator was able to catch the manipulation as it was happening and restored the levels to their normal range with no damage done.

12. Scareware

Scareware tricks individuals into thinking their computer is infected with malware, urging them to install software that is actually malware itself. This is often encountered as pop-up advertisements or warnings while browsing the web.

In one famous example, the "Antivirus XP" scareware tricked users into paying for fake antivirus software by aggressively advertising security alerts on users' computers.

13. Ransomware

Ransomware is a type of malicious software, or malware, that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment. Users are typically shown instructions for how to pay a fee to get the decryption key. The costs can range from a few hundred dollars to thousands, payable to cybercriminals typically in bitcoin.

Categories of Cyber Crime

Cybercrime can be defined as "The illegal usage of any communication device to commit or facilitate in committing any illegal act".

A cybercrime is explained as a type of crime that targets or uses a computer or a group of computers under one network for the purpose of harm.

Cybercrimes are committed using computers and computer networks. They can be targeting individuals, business groups, or even governments.

Investigators tend to use various ways to investigate devices suspected to be used or to be a target of a cybercrime.

Who are The Cybercriminals?

A cybercriminal is a person who uses his skills in technology to do malicious acts and illegal activities known as cybercrimes. They can be individuals or teams.

Cybercriminals are widely available in what is called the "Dark Web" where they mostly provide their illegal services or products.

Not every hacker is a cybercriminal because hacking itself is not considered a crime as it can be used to reveal vulnerabilities to report and batch them which is called a "white hat hacker".

However, hacking is considered a cybercrime when it has a malicious purpose of conducting any harmful activities and we call this one "black hat hacker" or a cyber-criminal.

It is not necessary for cybercriminals to have any hacking skills as not all cyber crimes include hacking.

Cybercriminals can be individuals who are trading in illegal online content or scammers or even drug dealers. **So here are some examples of cybercriminals:**

- Black hat hackers

- Cyberstalkers

- Cyber terrorists

- Scammers

Two Main Types of Cyber Crimes

- Targeting computers

This type of cybercrimes includes every possible way that can lead to harm to computer devices for example malware or denial of service attacks.

- Using computers

This type includes the usage of computers to do all the classifications of computer crimes.

Classifications of Cybercrimes

Cybercrimes in general can be classified into four categories:

1. Individual Cyber Crimes:

This type is targeting individuals. It includes phishing, spoofing, spam, cyberstalking, and more.

2. Organisation Cyber Crimes:

The main target here is organizations. Usually, this type of crime is done by teams of criminals including malware attacks and denial of service attacks.

3. Property Cybercrimes:

This type targets property like credit cards or even intellectual property rights.

4. Society Cybercrimes:

This is the most dangerous form of cybercrime as it includes cyber-terrorism.

Most Common Cyber Crimes

Now that you understand what cybercrimes are, let’s discuss some common cybercrimes.

1. Phishing and Scam:

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

2. Identity Theft

Identity theft occurs when a cybercriminal uses another person’s personal data like credit card numbers or personal pictures without their permission to commit a fraud or a crime.

3. Ransomware Attack

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

4. Hacking/Misusing Computer Networks

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

5. Internet Fraud

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

Other Types of Cybercrime

Here are another 9 types of cybercrimes:

1. Cyber Bullying

It is also known as online or internet bullying. It includes sending or sharing harmful and humiliating content about someone else which causes embarrassment and can be a reason for the occurrence of psychological problems. It became very common lately, especially among teenagers.

2. Cyber Stalking

Cyberstalking can be defined as unwanted persistent content from someone targeting other individuals online with the aim of controlling and intimidating like unwanted continued calls and messages.

3. Software Piracy

Software piracy is the illegal use or copy of paid software with violation of copyrights or license restrictions.

An example of software piracy is when you download a fresh non-activated copy of windows and use what is known as "Cracks" to obtain a valid license for windows activation. This is considered software piracy.

Not only software can be pirated but also music, movies, or pictures.

4. Social Media Frauds

The use of social media fake accounts to perform any kind of harmful activities like impersonating other users or sending intimidating or threatening messages. And one of the easiest and most common social media frauds is Email spam.

5. Online Drug Trafficking

With the big rise of cryptocurrency technology, it became easy to transfer money in a secured private way and complete drug deals without drawing the attention of law enforcement. This led to a rise in drug marketing on the internet.

Illegal drugs such as cocaine, heroin, or marijuana are commonly sold and traded online, especially on what is known as the "Dark Web".

6. Electronic Money Laundering

Also known as transaction laundering. It is based on unknown companies or online business that makes approvable payment methods and credit card transactions but with incomplete or inconsistent payment information for buying unknown products.

It is by far one of the most common and easy money laundering methods.

8. Cyber Extortion

Cyber extortion is the demand for money by cybercriminals to give back some important data they've stolen or stop doing malicious activities such as denial of service attacks.

9. Intellectual-property Infringements

It is the violation or breach of any protected intellectual-property rights such as copyrights and industrial design.

9. Online Recruitment Fraud

One of the less common cybercrimes that are also growing to become more popular is the fake job opportunities released by fake companies for the purpose of obtaining a financial benefit from applicants or even making use of their personal data.

Property Cyber Crime

Types of cybercrimes

The following are the various types of cybercrimes:

- **Theft via cyberspace**: Cyber theft is a sort of cybercrime that includes an individual infiltrating another person’s or company’s system in order to steal wealth, private information, financial information, or proprietary information. Identity theft and embezzlement are examples of fraudulent crimes that might be classified as cyber theft crimes.

- **Cyberbullying**: Bullying an individual online is referred to as cyberbullying. Cyberbullying includes any threat to a person’s safety, coercion of a person to say or do anything, and expressions of hatred or subjectivity against someone. While children are more likely to be victims of cyberbullying, adults are not exempt. According to a survey, 40% of polled teens said they had encountered online harassment, while 24% of adults aged 26–35 said they had experienced cyberbullying.

- **Malware**: Malware is a term that refers to any software program that is meant to infiltrate or harm a device. Viruses are a type of software that falls under the malware category. Viruses may cause a range of problems once they enter a device. They may delete files, record your keystrokes, erase your disk drive, or otherwise corrupt your data.

- **Phishing**: Phishing happens when fraudsters act as an organisation in order to dupe victims into disclosing important information. Scare techniques, such as notifying the victim that their bank account or personal device is under assault, are frequently used by cybercriminals to effectively fulfil their phishing aims.

- **Extortion via the internet**: Cyber extortion is a type of blackmail that takes place through the internet. In these occurrences, cybercriminals target or try to harm the person and demand pay or a reaction in order to halt their threats.

- **Ransomware**: Ransomware is a sort of cyber extortion that uses malware to achieve its purpose. This software threatens to disclose the victim's data or to block the user from retrieving his/her data unless the cybercriminal gets a predetermined sum of money.

- **Cryptojacking**: When hackers utilise other people's processing resources to mine cryptocurrency without their permission, this is referred to as cryptojacking. Cryptojacking varies from cyber crimes that utilise malware to enter the device of a victim to steal data whereas the cryptojackers are not interested in stealing a victim's data. Cryptojackers, on the other hand, employ the computing power of their victim's gadget. Despite appearing to be less harmful than other cybercrimes, cryptojacking should not be taken lightly because falling prey to it can drastically delay one's device and render it vulnerable to further cyber assaults.

- Cyber spying: Cyber spying occurs when hackers target a public or private entity's network in order to gain access to classified data, private information, or intellectual property. Cybercriminals may utilise the sensitive information they discover for a variety of purposes, including blackmail, extortion, public humiliation, and monetary gain.

- Spyware: Spyware is a software that cybercriminals employ to monitor and record their victims' actions and personal information. Often, a victim unintentionally downloads spyware onto their device, giving a cybercriminal unwitting access to their data. Cybercriminals can access a victim's credit card data, passwords, web cam, and microphone depending on the type of spyware employed.

- Adware: Adware is software that you may unintentionally download and install when installing another program. Every time someone views or clicks on an advertisement window, the developers of adware programs profit financially from their actions on people's computers. Although some adware software is lawful and innocuous, others are invasive due to the type and number of ads they display. Many nations consider some adware applications to be unlawful because they contain spyware, malware, and other dangerous software.

- **Botnets**: Botnets are malware-infected computer networks. Malicious hackers infiltrate and gain control of these machines in order to do things online without the user's consent, allowing them to commit fraudulent crimes while remaining undetected. They may send spam emails and conduct targeted hacks into a company's assets, financial records, data analyses, and other vital information.

- **Dating hoodwinks**: Some hackers utilise dating websites, chat rooms, and online dating apps to pose as possible mates and attract people in order to have access to their data.

- **Hacking**: Any illegal access to a computer system is generally referred to as hacking. When a hacker gains unauthorised access to a company's or an individual's computers and networks, they can obtain access to important corporate information as well as personal and private data. Despite this, not all hackers are crooks. Some "white hat" hackers are employed by software businesses to identify faults and gaps in their surveillance systems. These hackers get into a company's network in order to uncover existing holes in their clients' systems and provide fixes to such issues.

Cybercriminals or "black hat" hackers may desire to go clean and abandon their criminal activities occasionally.

The consequences of cyber crimes

The actual extent of cyber crime is hard to determine. Because of the significant danger of data loss, the consequences of cyber crime may be disastrous. The consequences of cyber crime may be divided into three categories:

Individual

Individuals bear the brunt of the consequences of cyber crime. With the gadgets, there may be difficulties such as data breaches, identity theft, or trafficking to harmful websites, among other things. As a result, one may notice unusual purchases on their credit cards and lose access to their financial accounts. Furthermore, fraudsters may utilise data saved on smartphones to harass and blackmail victims.

Business

Businesses may suffer from the loss of sensitive data, financial loss, or brand harm, among other things. It can have a direct impact on the value of a firm, and the stock value can result in a loss of reputation, clients, and so on. Companies that fail to secure client data will face fines and penalties. Furthermore, a malicious user may discreetly sell critical data from the firm to other businesses.

Government

Gaining access to government information with the purpose of misusing it, is a serious breach of data. Cybercriminals employ cutting-edge tools and technology to obtain access to extremely sensitive government data. The primary goal of attacking government data is to corrupt or sell national defence and security information.

Cybercrime as a business

The dark web, which is distinct from the deep web, has its own economy where cybercrime occurs. Criminals purchase and sell adware, botnets, data lists, and other items in order to conduct fraud and identity theft. However, there is a darker side to the dark web.

The dark web is used for a variety of purposes, including sex trafficking, the spread of child pornography, hitmen, and much more. There’s a sector of the internet, hidden behind many redirection and encrypted pages, that allows such heinous actions to take place. We’re referring to it as the “cyber crime economy.”

UNIT –II

Cyber Crime Issues

Unauthorized access presents significant risks to businesses, jeopardizing sensitive data and disrupting operations. Cybercriminals exploit vulnerabilities through sophisticated phishing attacks and API security gaps, making it imperative for organizations to adopt robust security measures. This blog post highlights the critical need to defend against unauthorized access and shares proven as well as advanced tactics to prevent it.

What Is Unauthorized Access?

Unauthorized access is the unauthorized entry or use of an organization's systems, networks, or data by individuals without permission. It's a common way for bad actors to exfiltrate data, inject malicious code, and take advantage of all types of breaches, and can have severe consequences for an enterprise and its customers.

The Risk and Impact of Unauthorized Access

The risk your business faces from unauthorized access goes beyond just data breaches, however. The results of unauthorized access can lead to financial losses, reputation damage, and legal implications.

Why Unauthorized Access Matters

Individuals who access your organization's systems or data without permission can:

- Steal or manipulate sensitive information, including customer data, financial records, intellectual property, and trade secrets.
- Disrupt day-to-day business operations, causing downtime, loss of productivity, and potential financial losses.
- Violate compliance regulations and legal requirements, such as the General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA). If your organization is found non-compliant, you may face legal penalties and will likely require significant, arduous auditing processes.

Types of Unauthorized Access

Cybercriminals use various techniques to breach organizational defenses and gain unauthorized access, including these common methods:

1. Brute force attacks: Cybercriminals use automated tools to test many combinations of usernames and passwords until they find the right credentials to access to your organization's systems.
2. Phishing: One of the most common ways cybercriminals try to trick people into revealing their login credentials is through deceptive emails, messages, or websites that look like they’re from legitimate sources.

3. Social engineering: This involves manipulating people through psychological tricks to gain unauthorized access. Social engineering tactics can include impersonation, pretexting, or baiting.

Unauthorized Access Examples

With so many cases of unauthorized access in recent years, it's hard to keep up. Here are some recent high-profile unauthorized access examples:

Trello: In January 2024, attackers scraped the data of 15 million users from the Trello site and posted it on the dark web.

Bank of America: A ransomware attack starting in November 2023 exposed the data of about 57,000 Bank of America customers.

Indian Council of Medical Research: A data breach exposed health information of approximately 815 million Indian citizens in October 2023, making it one of the largest unauthorized access examples in India's history.

Ontario Birth Registry: In September 2023, attackers accessed health information of around 3.4 million people.

Norton Healthcare: In May 2023, unauthorized access exposed personal information of roughly 2.5 million patients.

5 New and Dangerous Methods of Gaining Unauthorized Access

While phishing remains one of the most common unauthorized access examples, cybercriminals are becoming more sophisticated by the day. Attackers constantly develop and use new tactics to bypass security measures. Some of the latest threats include:

1. AI-Powered Phishing Campaigns

Phishing campaigns have become more sophisticated as cybercriminals use AI to create more convincing and personalized phishing emails, messages, or websites. These campaigns can slip past traditional email filters and deceive even tech-savvy individuals into revealing their login credentials or other sensitive information.

2. Exploiting API Access Vulnerabilities and Broken User Authentication

The complexity that makes APIs (Application Programming Interfaces) customizable also introduces the chance of security misconfigurations. Attackers can access data by exploiting unique vulnerabilities, such as exposed endpoints from broken object-level authorization, broken authentication mechanisms, weak input validation, or excessive data exposure

3. DNS Tunneling

DNS (Domain Name System) tunneling involves bypassing network security measures to gain unauthorized access. Attackers hide unauthorized data within DNS queries or responses to create secret communication channels and extract sensitive information from your organization's network without detection.

4. Cloud or Network Hopping

Cloud or network hopping occurs when cybercriminals move laterally within your organization's network or between different cloud environments. They exploit vulnerabilities or weak access controls to navigate through your organization's infrastructure and access sensitive data or systems.

5. Compromising Access to Third-party Service Providers

Another often overlooked unauthorized access example involves third-party service providers who have access to your organization's systems or data to offer their services. If these service providers are compromised, cybercriminals can gain unauthorized access to your organization's sensitive information through them.

5 Proven Tactics to Block and Prevent Unauthorized Access

Implementing effective security measures helps protect your organization's systems and data against unauthorized access. Here are some examples of proven tactics to protect your system:

1. Implement Strong Password Policies and MFA

A simple yet effective method of how to prevent unauthorized access is by enforcing strong password policies. Require employees to use complex and unique passwords, regularly change them, and avoid using the same passwords across multiple accounts.

Implementing Multi-Factor Authentication (MFA) adds an extra layer of security by requiring users to provide additional verification beyond passwords, such as a fingerprint scan or a unique code sent to a mobile device. The safest MFA is FIDO2 MFA, a passwordless authentication that uses unique cryptographic login credentials, preventing any password-based attack.

Make it easy: StrongDM provides detailed audit logs and monitoring capabilities to track user access and authentication events, including MFA attempts and failures, to ensure compliance and detect suspicious activity.

2. Regularly Update and Patch Systems

Software vendors often release updates and patches to fix security vulnerabilities. Regularly updating and patching software systems is a reliable way to prevent unauthorized access. You should promptly apply updates so your systems are protected against known vulnerabilities.

Make it easy: Enforce security policies with StrongDM to ensure that only updated and compliant devices can connect to your sensitive data.

3. Use Advanced Encryption Techniques

Encryption lets you protect sensitive data from unauthorized access by making it unreadable without a unique digital encryption key. Encrypting data while it’s at rest and in transit ensures that even if cybercriminals gain access to the data, they won’t be able to read or use it.

Make it easy: Enforce StrongDM encrypts data while it’s in transit and integrates with systems that encrypt data at rest.

4. Network Segmentation and Microsegmentation

Network segmentation is breaking down your organization's network into smaller, isolated segments to minimize the impact of unauthorized access. If an attacker gains access to one segment, they will be confined there and won't be able to move laterally to other parts of the network. Microsegmentation takes this further, creating even smaller segments within segments for additional isolation and control over network traffic.

▯**Make it easy:** Enforce network segmentation by using StrongDM to design a secure architecture that reduces your threat surfaces without creating roadblocks for staff.

5. Monitor and Analyze User Behavior

Monitoring and analyzing user behavior helps you spot suspicious activities and unauthorized access attempts. Advanced security tools can detect deviations from normal user behavior patterns, while continuously monitoring user behavior and analyzing patterns lets you proactively identify and respond to potential unauthorized access attempts before they cause significant damage.

▯**Make it easy:** StrongDM makes it easy for you to monitor database and server access in real-time, while robust logging lets you analyze user behavior and patterns.

5 Advanced Tactics to Block and Prevent Unauthorized Access

As attacks become more sophisticated, consider adopting more advanced strategies to combat cyber threats. Here are five advanced tactics to block unauthorized access:

1. Honeypots and Deception Technology

Honeypots are decoy systems or networks designed to lure attackers away from your actual systems and gather valuable information about their techniques and tactics. Deception technology goes beyond honeypots by deploying fake assets, such as files or credentials, to mislead attackers and detect unauthorized access attempts.

▯**Make it easy:** Secure your network with StrongDM's Infrastructure Access Platform, which uses the highest security standards to keep hackers out.

2. Authorization Through Behavioral Biometrics

Behavioral biometrics analyze and authenticate users based on their unique behavioral patterns, such as typing speed, mouse movements, or touchscreen interactions. Behavioral biometrics provide a way to prevent unauthorized access even if an attacker has valid credentials that have been stolen.

▯**Make it easy:** Protect your organization with StrongDM's comprehensive access management solutions and full-stack observability.

3. AI-driven Predictive Threat Intelligence

AI-driven predictive threat intelligence analyzes data to identify anomalies and predict potential threats in real-time, detecting and blocking unauthorized access attempts before they cause significant damage.

▯**Make it easy:** Protect Get advanced threat protection with StrongDM to provide simplified access and auditing across your entire stack.

4. Quantum Cryptography for Data in Transit

Quantum cryptography leverages principles from quantum physics to provide security that is theoretically unbreakable. It applies quantum key distribution to create and distribute encryption keys and exchange them so they cannot be intercepted or tampered with.

⍰**Make it easy:** StrongDM can manage access to systems and applications where encryption keys are stored or used. Controlling access to these systems mitigates the risk of unauthorized access to encryption keys. Protect data in transit with end-to-end encryption across all protocols. StrongDM ensures data remains secure using TLS 1.2 and TLS 1.3 encryption protocols.

5. Context-Based Signals

Context-based signals use contextual factors like user location, device, time of access, and past behavior to determine whether access requests are legitimate and make informed decisions about granting or denying them.

Computer Intrusion

A 'Computer Intrusion' refers to an unauthorized attempt to compromise the Confidentiality, Integrity, or Availability (CIA) of a computer or network system by bypassing security mechanisms, leading to potential serious disasters.

Intrusion detection system: A comprehensive review

1 Introduction

3W?>Over the past decades, Internet and computer systems have raised numerous security issues due to the explosive use of networks. CERT statistics (CERT) reports that the amount of intrusions has excessively increased year by year. Any malicious intrusion or attack on the network vulnerabilities, computers or information systems may give rise to serious disasters, and violate the computer security policies, i.e., *Confidentiality, Integrity and Availability* (CIA). Up to now, the threats on network and information security are still significant research issues. Though there is a number of existing literatures to survey IDS and its taxonomy (Denning, 1987; Lunt, 1993; Mukherjee et al., 1994; Debar et al., 1999; Axelsson, 2000; Mishra et al., 2004; Krugel and Toth, 2000; Jones and Sielken, 2000; Debar et al., 2000; Mukkamala and Sung, 2003; Estevez-Tapiador et al., 2004; Delgado et al., 2004; Kabiri and Ghorbani, 2005; Anantvalee and Wu, 2007; Patcha and Park, 2007; Tucker et al., 2007; Mandala et al., 2008; Garcia-Teodoro et al., 2009; Amer and Hamilton, 2010; Xie et al., 2011), we try to give a more systematic, architectural and contemporary image for a comprehensive review.

At first, we make a clear distinction about intrusion, intrusion detection, intrusion detection system (IDS) and intrusion prevention system (IPS). NIST (Bace and Mell, 2001) describes the intrusion as an attempt to compromise CIA, or to bypass the security mechanisms of a computer or network, intrusion detection is the process of monitoring the events occurring in a computer system or network, and analyzing them for signs of intrusions. Especially, wireless networks have recently been gaining widespread deployment, and they are much easier to attack than any wired network. In recent studies (Pelechrinis et al., 2011; Tan et al., 2011), many types of wireless denial of service (WDoS) attacks have been analyzed. Therefore, we categorize IDS into wireless-based and other technology types. The intrusion detection system is the software or hardware system to automate the intrusion detection process (Bace and Mell, 2001; Stavroulakis and Stamp, 2010). Moreover, the intrusion prevention system (IPS) is the system having all IDS capabilities, and could attempt to stop possible incidents (Stavroulakis and Stamp, 2010). In few articles, the terms of intrusion detection and prevention system (IDPS) and IPS are synonyms, where the term IDPS is seldom used in the security community. In this paper, we focus on the survey and classification of IDS related techniques, and give a brief comparison among them.

On the other hand, cloud computing leverages existing technologies, such as virtualization and distributed computing, and has recently emerged as a new paradigm for hosting and delivering services over the Internet. Virtualization is a technology that abstracts away the details of physical hardware and provides the capability of pooling computing resources from clusters of servers, storages and networks for high-level applications. Cloud platforms leverage virtualization technology to achieve the goal of providing computing resources as a utility. Therefore, we also study security issues on *Virtual Machines* (VMs).

The reminder of this paper is organized as follows. We describe IDS methodologies in Section 2, and the classification of IDS approaches in Section 3. Section 4 introduces four classes of IDS technologies. We study IDS issues on VMs in Section 5. Subsequently, two software-oriented solutions, Snort and ClamAV, are studied in Section 6, as they are most widely used open-source tools. Section 7 draws our conclusion, and gives future challenges.

Read more

Viral Influence

On first impression, the concept of “cyber attacks” intuitively elicits the contemplation of computer intrusions or malicious code infection events, allowing the attacker(s) to breach or damage a victim system. To be certain, both types of events describe a broad spectrum of attacks with varying scope of tools, techniques, and procedures leveraged by the attacker(s). These attacks may range from advanced and protracted to unsophisticated, uneventful, and brief. Techniques used to deceive victims into clicking on malicious links or opening/executing malicious files are generally classified as *social engineering*, or psychological manipulation to cause a person to perform a compromising action or reveal sensitive information. While this is a powerful, pervasive, and enduring element of cyber attacks, it is not the only human factor vector targeted and exploited by attackers. A less frequently examined concept of human manipulation in the information security community is *psychological influence*, the purpose of which is to affect perceptions, emotions, cognitions, motives, or behavior of a victim.[1]

Privacy on the Internet

In recent years, large-scale computer networks have become an essential aspect of our daily computing environment. We often rely on a global information infrastructure for ebusiness activities such as home banking, ATM transactions, or shopping online. One of the main scientific and technological challenges in this setting has been to provide security to individuals who operate in possibly untrusted and unknown environments. However, beside threats directly related to computer intrusions, epidemic diffusion of malwares, and outright frauds conducted online, a more subtle though increasing erosion of individuals’ privacy has progressed and multiplied. Such an escalating violation of privacy has some direct harmful consequences—for example, identity theft has spread in recent years—and negative effects on the general perception of insecurity that many individuals now experience when dealing with online services. Nevertheless, protecting personal privacy from the many parties—business, government, social, or even criminal—that examine the value of personal information is an old concern of modern society, now increased by the features of the digital infrastructure. In this chapter, we address these privacy issues in the digital society from different points of view, investigating: The various aspects of the notion of privacy and the debate that the intricate essence of privacy has stimulated; the most common privacy threats and the possible economic aspects that may influence the way privacy is (and especially is not, in its current status) managed in most firms; the efforts in the computer science community to face privacy threats, especially in the context of distributed networks; and, the network-based technologies available to date to provide anonymity in user communications over a private network.

Foreword

For most companies and individuals, protecting against the loss of proprietary and personal information is nothing more than ensuring that a firewall is in place. Sadly though, this does little to protect against today's threats to information security. Individuals and companies alike need to be proactive against the growing threats and need to take their information governance planning seriously. It appears that everyone is aware of the potential for a computer intrusion, but little efforts are directed toward any of the threats from within, whether they are nefarious or unintentional.

Read full chapter View PDF Explore book

Active Response

In Snort Intrusion Detection and Prevention Toolkit, 2007

Active Response versus Intrusion Prevention

If you are reading this chapter, chances are good that you have heard the term *intrusion prevention* in the context of network security. When referring to network-based security techniques, the term *network intrusion prevention* is usually applied to an *inline* device (such as an Ethernet bridge or firewall) that has the capability of modifying or discarding individual attack packets as they attempt to traverse the device's interfaces. Unfortunately, marketing and sales teams have redefined and abused this term to the point that many security professionals have a completely reasonable allergic reaction when hearing it and refuse to have anything to do with it. This is a shame, because there are legitimate uses for the term. There are also a number of host-based tools in the increasingly inclusive "intrusion prevention" category that implement mechanisms such as stack canaries and system call interception, but they are beyond the scope of this book.

What Is White-Collar Crime?

White-collar crime is a nonviolent crime often characterized by deceit or concealment to obtain or avoid losing money or property, or to gain a personal or business advantage.

Examples of white-collar crimes include securities fraud, embezzlement, corporate fraud, and money laundering. Entities that investigate white-collar crime include the Securities and Exchange Commission (SEC), the Financial Industry Regulatory Authority (FINRA), the Federal Bureau of Investigation (FBI), and state authorities.

Understanding White-Collar Crime

"White-collar crime" is a term first coined by sociologist Edwin Sutherland in 1939 who defined it as a crime committed by a person of respectability and high social status during his occupation. White-collar workers historically held non-laboring office positions while blue-collar workers traditionally wore blue shirts and worked in plants, mills, and factories.1

Federal Bureau of Investigation. "The Measurement of White-Collar Crime Using Uniform Crime Reporting (UCR) Data." Page 1.

High-profile individuals convicted of white-collar crimes include Ivan Boesky, Bernard Ebbers, Michael Milken, and Bernie Madoff. Their crimes have included insider trading, accounting scandals, securities fraud, and Ponzi schemes.

Malicious code definition

Malicious code is harmful computer programming scripts designed to create or exploit system vulnerabilities. This code is designed by a threat actor to cause unwanted changes, damage, or ongoing access to computer systems. Malicious code may result in back doors, security breaches, information and data theft, and other potential damages to files and computing systems.

What is malicious code?

Malicious code is the language hostile parties "speak" to manipulate computer systems into dangerous behaviors. It is created by writing changes or add-ons to the existing programming of computer programs, files, and infrastructure.

This threat is the foundational tool used to carry out the vast majority of cybersecurity attacks. Hackers probe and find weaknesses that are based on the languages used to program computers. They then create "phrases" known as scripts or lists of commands to abuse these vulnerabilities in these languages. These scripts can be re-used and automated via macroinstructions, or macros for short.

Hackers and other threat actors would move very slowly if they were restricted to manual methods of exploiting computer systems. Unfortunately, malicious code allows them to automate their attacks. Some codes can even replicate, spread, and cause damage on their own. Other types of code may need human users to download or interact with it.

The consequences of malicious code may often lead to any of the following:

- Corruption of data
- **Distributed denial-of-Service (DDoS)**
- Credential theft and private info theft
- Ransom and extortion
- Nuisance and inconvenience

To help you protect yourself, let's explore how these threats work.

How does a malicious code work?

Any programmed component of a computer system can be manipulated by malicious code. Large-scale components such as computer networking infrastructure and smaller components like mobile or desktop apps are all common targets. Web services, such as websites and online servers, can also be targets. Malicious code can infect any device using a computer to operate, such as:

- Traditional computer devices — desktops, laptops, mobile phones, tablets.

- IoT devices — smart home devices, in-vehicle infotainment systems (IVI).
- Computer network devices — modems, routers, servers.

Attackers use malicious scripts and programs to breach trusted parts of computer systems. From this point, they aim to do one or more of the following:

1. Expose users to malicious code, to infect them and spread it further.
2. Access private information on the breached systems.
3. Monitor the use of a breached system.
4. Breach deeper into a system.

Malicious code is created and used in a few distinct phases. The malicious scripted code may need human interaction or other computer actions to trigger the next event at each stage. Notably, some code can even operate entirely autonomously. Most malicious code follows this structure:

1. **Probe** and investigate for vulnerabilities.
2. **Program** by writing code to exploit vulnerabilities.
3. **Expose** computer systems to malicious code.
4. **Execute** the code through a related program or on its own.

Probing and programming are the setup phase of an attack. Before an attacker can breach a system, they must first have the tools to break in. They'll need to make the code if it doesn't already exist but may also use or modify existing malicious code to prepare their attack.

The result of malicious scripting is either an auto-executable application that can activate itself and take various forms. Some may include macros and scripts in JavaScript, ActiveX controls, Powershell misuse, pushed content, plug-ins, scripting languages, or other programming languages that are designed to enhance Web pages and email.

Exposing computer systems may occur through direct interface ports like USB or online network connections like mobile and Wi-Fi. Successful exposure only requires a way for the malicious code to travel to your machine.

Exposure in widespread attacks relies on high-contact channels such as popular websites and email spam, while more targeted efforts use social engineering methods like spear phishing. Some insider efforts can even plant malicious code into a private network like a corporate intranet by direct USB drive connection on a local end-user computer.

Execution occurs when an exposed system is compatible with the malicious code. Once a targeted device or system is exposed to malicious code, the resulting attack may include unauthorized attempts of any of the following:

- Modify data — unpermitted encryption, weaken security, etc.
- Delete or corrupt data — website servers, etc.
- Obtain data — account credentials, personal information, etc.

- Access to restricted systems — private networks, email accounts, etc.
- Executing actions — replicating itself, spreading malicious code, remote device control, etc.

How does malicious code spread?

Malicious code may be used to breach systems on its own, enable secondary malicious activity, or to replicate and spread itself. In any case, the original code must move from one device to another.

These threats can spread over nearly any communications channel that transmits data. Often, the vectors of spread include:

- **Online networks** — intranets, P2P file-sharing, public internet websites, etc.
- **Social communications —** email, SMS, push content, mobile messaging apps, etc.
- **Wireless connectivity —** Bluetooth, etc.
- **Direct device interfaces —** USB, etc.

Visiting infected websites or clicking on a bad email link or attachment are standard gateways for malicious code to sneak its way into your system. However, this threat can enter from legitimate sources as well as explicitly malicious ones. Anything from public USB charging stations to exploited software update tools has been misused for these purposes.

The "packaging" of malicious code isn't always obvious, but public data connections and any messaging service are the most important paths to watch. Downloads and URL links are often used by attackers to embed dangerous code.

Types of malicious code

Many malicious code types can harm your computer by finding entry points that lead to your precious data. Among the ever-growing list, here are some common culprits.

Viruses

Viruses are self-replicating malicious code that attaches to macro-enabled programs to execute. These files travel via documents and other file downloads, allowing the virus to infiltrate your device. Once the virus executes, it can self-propagate and spread through the system and connected networks.

Worms

Worms are also self-replicating and self-spreading code like viruses but do not require any further action to do so. Once a computer worm has arrived on your device, these malicious threats can execute entirely on their own — without any assistance from a user-run program.

Trojans

Trojans are decoy files that carry malicious code payloads, requiring a user to use the file or program to execute. These threats cannot self-replicate or spread autonomously. However, their malicious payload could contain viruses, worms, or any other code.

Cross-site scripting (XSS)

Cross-site scripting interferes with the user's web browsing by injecting malicious commands into the web applications they may use. This often changes web content, intercepts confidential information, or serves an infection to the user's device itself.

Backdoor attacks

Application backdoor access can be coded to give a cybercriminal remote access to the compromised system. Aside from exposing sensitive data, such as private company information, a backdoor can allow an attacker to become an advanced persistent threat (APT).

Cybercriminals can then move laterally through their newly obtained access level, wipe out a computer's data, or even install spyware. These threats can reach a high level: The U.S. Government Accountability Office has even warned about the threat of malicious code against national security.

What is Hacking and Cracking in Cybersecurity?

Sometimes the definition of a word changes over the years. For example, the word "fun" today means to have a good time or engage in an enjoyable activity. But in the 17th century the word actually meant, "to cheat or hoax." When it comes to cybersecurity, imagine this same principle--only sped up with the whir of technology behind it!

On the internet, words and symbols change meaning almost daily. When it comes to the cybersecurity terms "hacker" and "cracker," their meanings have evolved and changed a great deal over the years. Let's take a look at where they got started and what the current state of these labels are.

Where Did the Terms Hacker and Cracker Originate?

It seems that most internet users are more familiar with the term "hacker" and indeed, it has quite a long history. The term started out at MIT in the 1950s. It originally meant to deal with a technical problem in a creative way without any negative connotations. By 1975, a jargon dictionary for computer programmers contained multiple definitions of the word with only one of them meaning a person who was up to no good. The final definition reads:

Where do the "Hat" Hackers Come in?

You've probably heard the terms; white hat, black hat, etc. But what do these hat colors ultimately mean and what do they do? Let's take a look.

- **White Hat**: These are the good hackers. They engage in ethical hacking. For example, a penetration tester, one type of white hat, might be hired by a company to try to break into their system. This is to test their digital realm for weaknesses that individuals might exploit.
- **Black Hat**: These are the stereotypical bad people. Their goals and methods may very, but a black hat hacker is someone who accesses digital information or accounts which are not theirs. Some hackers commit these crimes for pranks or to embarrass users. Others want to steal money and personal information, which can be sold for a great deal on the darknet.

- **Gray Hat**: These hackers are neither white hats nor black hats, but somewhere in the middle. For example, a gray hat hacker might break into a government agency's computer system and then message them the details about weaknesses in their network. They have committed a crime by breaking into the system in the first place, but they used the information to help out the government agency. Unfortunately, intentions don't matter in cases like this--that gray hat hacker will be prosecuted if tracked.

What Does "Hacker" and "Cracker" Mean Today?

Although these terms continue to evolve, most cybersecurity experts choose to use the Hat definitions to describe hackers. The terms have changed over the years. This article from 2005 identifies crackers as the baddies who broke into systems, and hackers as the good people who tried to keep them out and stop their attacks.

But in an ever-evolving digital world, there is little doubt that these terms might change again over the years. As the world becomes more reliant on computers and more and more information becomes digitized, there will be an increased need for cybersecurity. While there are black hats out there, there have to be white hats to keep the internet safe for users everywhere.

Computer Virus Definition

Chances are you've heard how important it is to keep viruses out, but what is a computer virus exactly? 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.

Common Signs of Computer Viruses

Chances are you've heard how important it is to keep viruses out, but what is a computer virus exactly? A computer virus will more than likely have an adverse effect on the device it resides on and may be discoverable through common signs of performance loss, including:

1. Speed of system

2. Pop-up windows

3. Programs self-executing

4. Accounts being logged out

5. Crashing of the device

6. Mass emails being sent from your email account

7. Changes to your homepage

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

There are several types of computer viruses that can infect devices. This section will cover computer virus protections and how to get rid of computer viruses.

1. Resident virus

2. Multipartite virus

3. Direct action

4. Browser hijacker

5. Overwrite virus

6. Web scripting virus

7. File infector

8. Network Virus

9. Boot Sector Virus

Pornography (colloquially known as **porn** or **porno**) has been defined as sexual subject material such as a picture, video, text, or audio that is intended for sexual arousal.[a] Made for consumption by adults, pornography depictions have evolved from cave paintings, some forty millennia ago, to virtual reality presentations. A general distinction of adult content is made classifying it as pornography or erotica.

The oldest artifacts considered pornographic were discovered in Germany in 2008 CE and are dated to be at least 35,000 years old.[b] Throughout the history of erotic depictions, various people made attempts to suppress them under obscenity laws, censor, or make them illegal. Such grounds and even the definition of pornography have differed in various historical, cultural, and national contexts. The Indian Sanskrit text *Kama Sutra* (3rd century CE) contained prose, poetry, and illustrations regarding sexual behavior, and the book was celebrated; while the British English text *Fanny Hill* (1748), considered "the first original English prose pornography," has been one of the most prosecuted and banned books. In the late 19th century, a film by Thomas Edison that depicted a kiss was denounced as obscene in the United States, whereas Eugène Pirou's 1896 film *Bedtime for the Bride* was received very favorably in France. Starting from the mid-twentieth century on, societal attitudes towards sexuality became more lenient in the Western world where legal definitions of obscenity were made limited. In 1969, *Blue Movie* became the first film to depict unsimulated sex that received a wide theatrical release in the United States. This was followed by the "Golden Age of Porn" (1969–1984). The introduction of home video and the World Wide Web in the late 20th century led to global growth in the pornography business. Beginning in the 21st century, greater access to the Internet and affordable smartphones made pornography more mainstream.

.

The Definition of Software Piracy

Software piracy is the intentional or unintentional illegal copying, selling, using, or sharing of legally protected software. When you buy any program, you become a licensed user and are allowed a specific number of licenses. Pirating software involves cracking or changing specific software files so the license-checking system can be disabled or fooled, leaving additional features unlocked.

In most cases, you'll have a chance to copy the software you purchased as a backup if you accidentally delete it or no longer have access to your device. However, **suppose you copy and share** the software with someone else. In that case, you're in **direct copyright violation** and could face legal repercussions.

Internet users often indulge in activities they deem completely legal without even realizing they're committing software piracy. To stay within the bounds of the law, **we should be able to recognize piracy types** and stop ourselves from taking part in damaging the owners, writers, and developers of the software we use.

Types of Software Piracy

There are five different types of software piracy. While you may have heard of some, others may be entirely new to most people. These are:

Counter feiting

The **illegal copying or distribution of software that's copyright-protected is called counterfeiting.** It's typically done to imitate the original product and redistribute it. Other than the counterfeit software, security features, license agreements, labels, packaging, and registration cards can also be copied.

Many users aren't always able to tell that a software program is counterfeit and, therefore, an illegal copy since the program itself and any additional elements have been carefully made to seem almost entirely authentic. **These products are usually sold at lower prices** than the original software programs to attract more buyers.

Intellectual property (IP) refers to creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce.

IP is protected in law by, for example, patents, copyright and trademarks, which enable people to earn recognition or financial benefit from what they invent or create. By striking the right balance between the interests of innovators and the wider public interest, the IP system aims to foster an environment in which creativity and innovation can flourish.

Types of intellectual property

Do you know what the difference is between a patent and an industrial design, how to protect your photo with a copyright, or why you would want to obtain a protected designation of origin? Discover everything you ever wanted to know about IP rights.

What is a mail bomb?

A mail bomb is a form of a denial-of-service (DoS) attack designed to overwhelm an inbox or inhibit a server by sending a massive number of emails to a specific person or system. The aim is to fill up the recipient's disk space on the server or overload a server to stop it from functioning.

Also known as *email bombs* and *letter bombs*, mail bombs inconvenience not only the intended target but everyone who uses the server. When a server is unresponsive, it can degrade network performance and potentially lead to downtime.

Exploitation

In her first term, Scholten has introduced legislation cracking down on child labor ***exploitation***.—*Detroit Free Press*, 15 July 2024This ongoing lack of improvement underscores the persistent challenges and ***exploitation*** faced by farmworkers in Michigan.

Introduction

One example of this kind of cybercrime is cyberstalking, also known as online stalking or internet stalking. Cyberstalking, or the stalking of a person by electronic means (often the internet), is a kind of electronic harassment. Harassment takes many forms and might include monitoring someone's online behavior, making threats, stealing their identity or data, or even faking their data.

In cyberstalking, one individual illegally and repeatedly stalks another person via their online actions.

"Stalking is an obvious violation of Article 21 of the Indian Constitution, which protects the right to privacy. The case was *Justice K.S. Puttaswamy and Others v. Union of India and Others,* and this was the decision." Its primary function is to make individuals feel afraid, but a secondary consequence is social isolation.

Negative mental states such as extreme narcissism, rage, vengeance, envy, obsession, psychiatric condition, desire for control, sadomasochistic fantasies, sexual deviance, internet addiction, and religious fanaticism may all contribute to the development of stalker behavior. Different types of mental disturbance might lead to cyberstalking. A few examples are as follows:

1. **Jealousy:** Anxiety is an unpleasant feeling. Jealousy may play a role in a person's decision to stalk, particularly when it concerns a current or former romantic relationship.

2. **Obsession and attraction:** Stalking may also stem from unhealthy obsession or desire. The stalker could have an intensely emotional or sexual pull toward the target. There is a fine line between admiration and stalking.

3. **Erotomania:** As a kind of stalking, this theory holds that the target, who is often a stranger or a famous person, secretly has romantic feelings for the stalker. The attraction of a sexual nature is a necessary condition.

4. **Sexual harassment:** Sexual harassment is often believed to be the primary motivator for cyberstalking. The reason for this is that online life generally resembles the actual world.

5. **Revenge and hate:** The victim may not always be the initial inspiration for the stalker's feelings of rage and resentment, but he or she may nonetheless become the stalker' primary focus anyway. It would seem that the stalker uses the internet as a means of venting their rage and seeking revenge.

UNIT-III

Introduction to Cyber Crime Investigation

Introduction: What are Investigative Tools and Techniques :

Investigative tools and techniques are a set of aids and skills that investigators use to gather information to solve crimes. This blog will cover five different investigative tools and techniques used by law enforcement agencies to give you a better understanding of the power that law enforcement has at their fingertips.

The investigative process is a systematic way of solving crimes by gathering, analyzing, and interpreting evidence. Investigators use investigative tools and techniques to quickly collect information about witnesses, suspects, crime scenes, and other evidence.

With the rise of SaaS business models, investigative tools used by law enforcement have become more accessible, meaning anyone can act as an investigative journalist to analyse and document events.

5 Investigative Tools Used by Law Enforcement Agencies

The following is a list of investigative tools and techniques that can be used by law enforcement agencies to solve crimes.

Many investigative tools and techniques may not be included in this blog - if you have anything else to add, please get in touch with the Hunt Intel Team!

1. OSINT Tools

Open Source Intelligence (OSINT) is a term used to describe intelligence gathering from publicly available sources.

Legitimate OSINT techniques are often used either as a precursor to or even during an illegal attack, but the techniques themselves are generally not unlawful. Law enforcement agencies usually try to stay ahead of the game by using advanced OSINT tools to spot trends and information before an event happens.

An example of OSINT tools used by law enforcement agencies is Hunt Intel's geographical open-source intelligence tool (below) that allow investigators to view social media posts and activities around a geographical point.

Sorting through the vast amounts of social media data allows agencies to find and validate data quickly to make correct decisions. Making the correct decision fast is a vital part of any investigation process - which is why as of March 2024, over 100,000 people have used Hunt's range of OSINT tools.

2. DNA Testing

Genetic evidence is one of the most reliable forms of evidence in many criminal cases. This kind of evidence can be collected from different body fluids and parts, such as blood and hair. Once blood or hair is captured, DNA testing (sometimes referred to as DNA or genetic typing) allows investigators to investigate unique sequences on areas of a chromosome to identify someone.

DNA testing has been widely used in forensic science, as well as in genealogical research. It has become a powerful diagnostic tool for identifying hereditary diseases or other conditions and pinpointing a suspect at a crime scene.

There are three types of DNA tests:

1. Autosomal DNA test: it identifies genetic information that is not gender-specific and is inherited from both parents.
2. Mitochondrial DNA test: it examines only the mother's genetic information and can be used to identify maternal lineage.
3. Y-chromosome DNA test: it examines only the male's genetic information and can be used to identify paternal lineage.

The accuracy of DNA tests makes it one of the most common investigative tools and techniques used by law enforcement agencies. Moreover, it is so powerful that it can even be used to solve old crimes prior to the development of DNA-testing technology.

3. CCTV Data Analysis

CCTV cameras are becoming more common and advanced - meaning there is more footage being collected by the day, and there is more valuable data that we can extract.

High-definition digital cameras with night viewing capability can capture footage at any time of the day or night, meaning investigators can understand what is happening in real-time and analyse footage against existing data. Hidden cameras are also used during undercover operations, meaning data can be analysed even when the suspect thinks they're hidden.

For example, the use of AI in CCTV data analysis has been on the rise. AI can identify and track objects that move in front of a camera, count people and vehicles, or even measure traffic flow. Not only is footage being used as evidence, but AI can also pinpoint who was present in the footage and cross-reference this to social media activity to pinpoint someone to a crime.

4. Computer Forensics

Computer forensics is the process of examining digital media to find out what happened. It is a branch of forensic science that deals with collecting and analysing data from computers, mobile devices, and other electronic storage media.

A computer forensics expert will often be asked to examine a system to answer questions like:

- What was the last thing that person did on their computer?
- How did the hacker get in?
- Who else has been using this machine?
- Where has the data been copied or sent?
- Is this data encrypted?
- How long ago was this machine used last?

Computer forensics is different from traditional forensics, where tools like fingerprint kits, casting kits, and sterile swabs are used to collect evidence behind crime scene tape.

5. Interviews and Interrogations

Interrogations are a vital component of the criminal justice system. They are used to collect information from suspects and witnesses.

Police officers should always be aware of their surroundings and never interrogate a victim or witness without a partner present. This is because interviews can pressure people into giving false information - check out this paper covering "Techniques and Controversies in the Interrogation of Suspects' to find out more.

Despite how many investigative tools law enforcement use have moved online, there will always be a case for interviews and interrogations in-person, as picking up the body language of someone can be a key part of any investigation.

Definition- E-discovery

E-discovery is a form of digital investigation that attempts to find evidence in email, business communications and other data that could be used in litigation or criminal proceedings. The traditional discovery process is standard during litigation, but e-discovery is specific to digital evidence. The evidence from electronic discovery could include data from email accounts, instant messages, social profiles, online documents, databases, internal applications, digital images, website content and any other electronic information that could be used during civil and criminal litigation.

But most processes include a few common stages. These e-discovery stages were created to improve collection, preservation and presentation of potentially relevant information. E-discovery typically includes nine stages. Here’s how they work:

- **Information governance (IG):** IG is an umbrella term used to describe the procedures, controls and policies for data collection and preservation. Best practices are managed by the IGRM model, which provides a framework for all e-discovery agencies to follow.

- **Identification:** When litigation is imminent, all parties must attempt to preserve evidence. But how do you know what data to save? In the identification phase, a team determines what data must be preserved by interviewing key stakeholders, reviewing case facts and analyzing the digital environment.

- **Preservation:** After data is identified, data owners are formally instructed to preserve data (and to not delete it).

- **Collection:** Several technologies exist to collect data, but the chosen application must follow a defined legal process. The team responsible for collecting data must ensure that digital assets are preserved without altering essential metadata such as file creation dates, size, and audit logs attached to each file.

- **Processing:** Raw collected data is usually unorganized and ill-suited to present to attorneys or the court. The processing phase of electronic discovery involves organizing data and finding the right assets for analysis. This phase can also be automated using software to extract important information from a sea of irrelevant data.

- **Review:** Reviewing documentation and digital assets can be done manually or by using artificial intelligence. During the review stage, pertinent information is separated from unnecessary data that is not relevant for the ongoing litigation. This phase also identifies documents subject to client-attorney privilege.

- **Analysis:** At this stage in e-discovery, digital assets become more organized for presentation. Reviewers identify patterns and key information critical for litigation and design a presentation layout used during trial or deposition.

- **Production:** Digital assets must be turned into physical documentation. After key data is identified, attorneys turn it into presentable evidence.

- **Presentation:** Evidence in litigation must be presented to other attorneys, judges, juries, mediators, and deposition participants. During the final presentation phase, data is organized in a way that makes it easy to parse and then convey to an audience.

Digital Evidence Collection in Cyber security

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

Digital Evidence Collection in Cyber Security – Challenges Faced

There are numerous challenges in collecting digital evidence in cyber security because technology changes all the time and many new issues come up like the inconsistency of cyber environments. Initially, the data volatility is a big challenge because important evidence is completely altered or lost with ease in running systems if not captured on time. Also accessing encrypted information or data that is protected poses its own difficulties thus one requires more than just ordinary passwords but decryption methods as well as legal authorization in order to access such information.

Ensuring data integrity and authenticity is critical, as any alteration during collection can render the evidence inadmissible in court. Additionally, **legal and jurisdictional issues** often arise, especially when evidence spans multiple regions or countries, necessitating compliance with diverse legal frameworks and international cooperation. Finally, the **rapid phase of technological advancement** means forensic tools and methodologies must constantly evolve to keep up with new forms of digital evidence and cyber threats, demanding continuous training and adaptation by cybersecurity professionals.

Digital Evidence Preservation – Digital Forensics

As the realm of the Internet, Technology, and Digital Forensics constantly expand, there is a need for you to become familiar with the ways they contribute to preserving digital evidence. The fundamental importance of digital evidence preservation is quite clear. Through this article, we want to highlight the necessity to follow a series of steps in order to preserve digital evidence, as even a small inattentive move could lead to a loss of evidence and the break of a case.

In this article, we will be covering the following topics:

1. Top 11 Critical Steps in Preserving Digital Evidence.
2. Details You Should Plan To Share.
3. Three Methods to Preserve Digital Evidence.
4. Problems in Preserving Digital Evidence.

Let’s start discussing each section in detail.

Top 11 Critical Steps in Preserving Digital Evidence

In this section, we will be discussing the critical steps that need to be followed to prevent loss of data before bringing to the forensic experts. Time is highly important in preserving digital evidence.

1. Do not change the current state of the device: If the device is OFF, it must be kept OFF and if the device is ON, it must be kept ON. Call a forensics expert before doing anything.
2. Power down the device: In the case of mobile phones, If it is not charged, do not charge it. In case, the mobile phone is ON power it down to prevent any data wiping or data overwriting due to automatic booting.
3. Do not leave the device in an open area or unsecured place: Ensure that the device is not left unattended in an open area or unsecured area. You need to document things like- where the device is, who has access to the device, and when it is moved.
4. Do not plug any external storage media in the device: Memory cards, USB thumb drives, or any other storage media that you might have, should not be plugged into the device.
5. Do not copy anything to or from the device: Copying anything to or from the device will cause changes in the slack space of the memory.
6. Take a picture of the piece of the evidence: Ensure to take the picture of the evidence from all the sides. If it is a mobile phone, capture pictures from all the sides, to ensure the device has not tampered till the time forensic experts arrive.
7. Make sure you know the PIN/ Password Pattern of the device: It is very important for you to know the login

Role of Email in Investigation

Emails play a very important role in business communications and have emerged as one of the most important applications on internet. They are a convenient mode for sending messages as well as documents, not only from computers but also from other electronic gadgets such as mobile phones and tablets.

The negative side of emails is that criminals may leak important information about their company. Hence, the role of emails in digital forensics has been increased in recent years. In digital forensics, emails are considered as crucial evidences and Email Header Analysis has become important to collect evidence during forensic process.

An investigator has the following goals while performing email forensics −

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

Challenges in Email Forensics

Email forensics play a very important role in investigation as most of the communication in present era relies on emails. However, an email forensic investigator may face the following challenges during the investigation −

Fake Emails

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

Spoofing

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

Anonymous Re-emailing

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

Techniques Used in Email Forensic Investigation

Email forensics is the study of source and content of email as evidence to identify the actual sender and recipient of a message along with some other information such as date/time of transmission and intention of sender. It involves investigating metadata, port scanning as well as keyword searching.

Some of the common techniques which can be used for email forensic investigation are

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

In the following sections, we are going to learn how to fetch information using Python for the purpose of email investigation.

What is Email Tracking ?

Email tracking is the process of monitoring actions taken on sent emails. The most common metrics tracked are email opens and email clicks.
Most email tracking tools report on dates & times of events captured, and some report location as well.
Email tracking can serve several important functions. Depending on which tools you use and how you use them, you can use email tracking apps to:

- Determine your team's workload (and rebalance it)
- Identify unproductive patterns in your own work
- Analyze your sales efforts to see which strategies are most effective
- Track email opens and clicks

7- Best Email Tracking Apps for Gmail & Outlook

1. **Email Analytics (Gmail & Outlook)**
2. **Hub Spot (Gmail & Outlook)**
3. **Right Inbox (Gmail only)**
4. **Sales Handy (Gmail & Outlook)**
5. **Mail track (Gmail only)**
6. **Vocus.io (Gmail only)**
7. **Yes ware (Gmail & Outlook)**

what is the IP address?

IP stands for internet protocol. The protocol means the guidelines or the rules and regulations to govern the connectivity on the internet. Moreover, address refers to the unique numeric string identifier that links all your internet activities.

Therefore, the Internet Protocol (IP) address is defined as a unique numeric string identifier separated by the periods and allocated to each Internet device. The device can be a computer, mobile, tablet, or any other machine that is part of the TCP/IP-based network. The IP addresses are assigned to devices, not to humans.

The most likely format of the IP address has four numbers separated by periods—each with one to three digits and falling between 0 to 255.

Whenever you connect to the internet, your Internet service provider (ISP) assigns you the IP address. Through which you are recognized and identified on the internet.

Versions of the IP address

Two versions of IP addresses exist on the global internet.

- **IP version 4 (IPv4)**
- **IP version 6 (IPv6)**

IP version 4 (IPv4) is old and was the first to be assigned. It is the most common version of the IP address. IPv4 addresses are 32 bits long and have five classes, ranging from A to E. When IPv4 was introduced, at that time, computers were big and rare. The IPv4 had space for 4 billion IP addresses. However, due to rapid internet growth, the IP addresses are not used constructively. That is why the 4 billion number seemed large initially but became smaller in 2014.

IP version 6 (IPv6) is the latest version of the IP. The IPv6 address is a hexadecimal-based IP address separated by colons. IPv6 addresses are 128 bits long and will eventually replace IPv4 in the years to come.

You can use IPv4 and IPv6 for the foreseeable future and convert your IPv4 address to IPv6 by using the IPv4 to IPv6 Online Conversion Tool.

How to recover your Google Account or Gmail

If you forgot your password or username, or you can’t get verification codes, follow these steps to recover your Google Account. That way, you can use services like Gmail, Photos, and Google Play.

Tips:

- Wrong guesses won’t kick you out of the account recovery process. There's no limit to the number of times you can attempt to recover your account.
- If you use an account through your work, school, or other group, these steps might not work. Check with your administrator for help.
- To recover an account for a child under 13 (or the applicable age in your country) you can reset your child's password.

Forgot your password

1. Follow the steps to recover your Google Account or Gmail.
   - You'll be asked some questions to confirm it's your account. Answer the questions as best as you can.
   - If you have trouble, try the tips to complete account recovery steps.
2. Reset your password when prompted. Choose a strong password that you haven't already used with this account. Learn how to create a strong password.

Forgot the email address you use to sign in

1. To find your username, follow these steps. You need to know:
   - A phone number or the recovery email address for the account.
   - The full name on your account.
2. Follow the instructions to confirm it’s your account.
3. You’ll find a list of usernames that match your account.

Someone else is using your account

If you think someone is using your Google Account without your permission, follow the steps to recover a hacked or hijacked Google Account or Gmail.

Can’t sign in for another reason

If you have another problem, get help signing in.

Recover a deleted Google Account

If you recently deleted your Google Account, you can follow the steps to recover your account.

Still can’t sign in

Create a new account

If you can’t sign in, try these tips for account recovery.

If you still can’t recover your account, you can create a new Google Account. When you do, you can follow these steps to avoid getting locked out of your Google Account.

Avoid account & password recovery services

For your security, you can't call Google for help to sign into your account. We don’t work with any service that claims to provide account or password support. Do not give out your passwords or verification codes.

Hands-on Case Studies: Applying Machine Learning to Solve Real-World Challenges in Various Industries:

Machine Learning (ML), a subset of artificial intelligence, has revolutionized the way we approach problem-solving in diverse industries. Its ability to analyze vast datasets, identify patterns, and make predictions has opened up new avenues for innovation and efficiency. In this blog, we will delve into hands-on case studies that showcase the application of ML to address real-world challenges across different sectors.

1. Healthcare: Predictive Diagnostics and Personalized Medicine

In the healthcare industry, ML algorithms are being employed to enhance diagnostics and treatment plans. Case studies demonstrate the use of ML in predicting diseases such as diabetes, cancer, and heart conditions based on patient data. Additionally, Machine Learning is contributing to personalized medicine by analyzing genetic information to tailor treatment plans for individuals, leading to more effective and targeted interventions.

2. Finance: Fraud Detection and Risk Management

Financial institutions face the constant challenge of identifying fraudulent activities and managing risks. ML algorithms are proving invaluable in detecting anomalous patterns in financial transactions, reducing false positives, and improving overall fraud detection accuracy. Case studies in finance highlight the implementation of ML for credit scoring, portfolio optimization, and predicting market trends.

3. Manufacturing: Predictive Maintenance and Quality Control

In the manufacturing sector, machine failures and production defects can result in significant losses. ML is being used for predictive maintenance, analyzing equipment sensor data to anticipate potential issues before they occur. Quality control processes are also benefitting from ML applications, ensuring that defects are identified and corrected in real-time, improving overall product quality and reducing waste.

4. Retail: Personalized Recommendations and Demand Forecasting

E-commerce platforms leverage ML to provide personalized product recommendations, enhancing the customer shopping experience. Case studies in retail demonstrate how ML algorithms analyze customer behavior, purchase history, and preferences to suggest products tailored to individual tastes. Furthermore, ML aids in demand forecasting, optimizing inventory management and reducing excess stock or stockouts.

5. Transportation: Route Optimization and Traffic Prediction

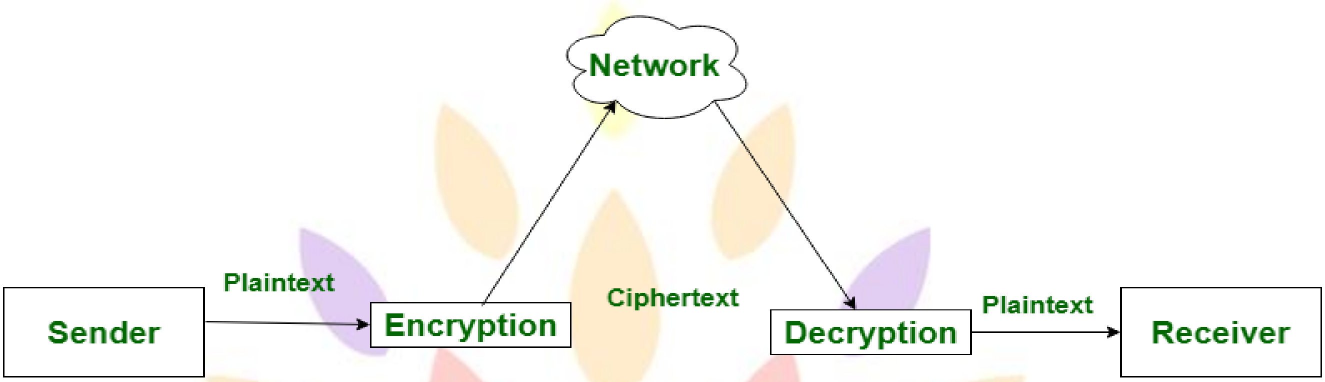
ML plays a crucial role in optimizing transportation systems by analyzing traffic patterns and predicting congestion. Case studies showcase the implementation of ML algorithms in route optimization for delivery services, reducing travel time and fuel consumption. Additionally, predictive modeling helps city planners and transportation authorities make informed decisions to alleviate traffic congestion.

6. Education: Adaptive Learning Platforms and Student Performance Prediction

In the education sector, ML is reshaping traditional teaching methods through adaptive learning platforms. These platforms analyze students' learning styles and performance to tailor educational content, providing a personalized learning experience. Case studies also highlight the use of ML in predicting student performance, enabling early intervention to address academic challenges and improve educational outcomes.

Difference between Encryption and Decryption :

Encryption is the process of converting normal message (plaintext) into meaningless message (Ciphertext). Whereas **Decryption** is the process of converting meaningless message (Ciphertext) into its original form (Plaintext). The major distinction between secret writing associated secret writing is that the conversion of a message into an unintelligible kind that's undecipherable unless decrypted. whereas secret writing is that the recovery of the first message from the encrypted information.



Let's see that the difference between encryption and decryption:

S.NO	Encryption	Decryption
1.	Encryption is the process of converting normal message into meaningless message.	While decryption is the process of converting meaningless message into its original form.
2.	Encryption is the process which take place at sender's end.	While decryption is the process which take place at receiver's end.
3.	Its major task is to convert the plain text into cipher text.	While its main task is to convert the cipher text into plain text.
4.	Any message can be encrypted with either secret key or public key.	Whereas the encrypted message can be decrypted with either secret key or private key.
5.	In encryption process, sender sends the data to receiver after encrypted it.	Whereas in decryption process, receiver receives the information(Cipher text) and convert into plain text.

Seizure of the Computer :

A how-to for law enforcement officers on gathering computer evidence -- and avoiding common booby traps that can destroy evidence with the click of a mouse:

The rapid acceptance of computer technology by all segments of our society has created new and interesting challenges for law enforcement agencies and prosecuting attorneys. Computer evidence has become a fact of life for essentially all law enforcement agencies, and many are just beginning to explore their options with this new technology. Almost overnight, personal computers have changed the way the world does business.

Computers have also changed the world's view of evidence, because computers are used more and more as tools in the commission of "traditional" crimes. Embezzlements, theft, extortion and even murders are now committed with the aid of personal computers. This new technology twist in crime patterns has brought computer evidence to the forefront in law enforcement circles. Computer evidence concerns are not limited to computer crime specialists in the Federal Bureau of Investigation or United States Secret Service. Every law enforcement agency now has the potential of encountering computer evidence, and many are actively seeking training and information on the topic.

This article is intended to provide guidance and an awareness to law enforcement agencies that are just now beginning to explore the issues surrounding computer evidence. The article is not intended as a substitute for training. There is more than one way to skin a cat and this information is certainly not intended to be the only true way. However, the information should help law enforcement agencies get started in the right direction. It should also act as a refresher for those agencies that have experience in processing computer evidence.

Been Rigged To Destroy Evidence

Computer evidence, by its nature, is extremely fragile and is easily modified. This situation is complicated by the fact that potential evidence exists in places of which many law enforcement officers are unaware. To make matters worse, computers can easily be rigged by the crooks to destroy evidence. Some refer to personal computers as a law enforcement nightmare and a crook's dream. Because of its fragile nature, the first and most important step in dealing with computer evidence involves the preservation of the "electronic crime scene." No law enforcement professional would allow evidence to be disturbed or destroyed at a traditional crime scene. The same is true of computer evidence. However, because the nature of the evidence is different, the rules change a bit.

When it comes to computer evidence, paranoia is a good personality trait to have. Don't operate a suspect computer until a complete backup has been made of all storage devices. Normal computer backups won't do -- a full bit stream backup is necessary. In the bizarre world of computer evidence, you always must assume that things will go wrong. Once computer evidence has been destroyed or altered, it is unlikely that it can ever be reconstructed. What can go wrong surely will go wrong. Complete backups eliminate most of the potential problems.

Law enforcement officials normally seize computers during the execution of a search warrant. Depending on the circumstances and scope of the search warrant involved, all computer hardware, software and manuals should be taken for evaluation as potential evidence. Some prosecutors may view this as overly broad. However, the ability to process and examine the evidence may be directly tied to special hardware, software and/or written instructions contained in manuals. Because computer technology changes so quickly, it may be impossible to obtain similar or outdated hardware or instruction manuals from other sources. Printers, tape drives, optical drives, hardware and software manuals should not be left behind. Also, pay particular attention to possible passwords that may have been written down near the computer. Encrypted files can cause you serious grief, and finding a password scrawled on a desk or on a calendar can help make your case.

More and more, corporations and government agencies are involved with computer evidence pertaining to internal investigations and internal audits. The same law enforcement procedures should be followed by corporate computer specialists because it is usually unknown if criminal violations are involved. Following accepted computer evidence processing procedures will ensure the case meets the requirements for both civil and criminal trial purposes. Every case should be treated as though it will go to trial. However, some things are a bit different when it comes to corporations. In a corporate or government setting, the ability to 'seize' a computer and evaluate the data stored on the computer's hard disk drives and floppy diskettes may be ruled by corporate policy and privacy laws. For this reason, it is essential that corporate legal counsel be consulted before taking any steps to seize or process a corporate computer. In the absence of a corporate policy covering computer evidence and privacy issues, corporate computer specialists could be exposing themselves and the corporation to a potential lawsuit.

Shutdown Procedure

Caution should always be used in the shutdown and transport of the subject computer. To preserve the image on the screen, a quick photograph of the screen display may be appropriate. Then a decision has to be made as to whether or not the computer will be unplugged from the wall or shut down systematically based on the requirements of the operating system. Unfortunately, there is no correct answer, and there are risks in taking either course of action. Your decision will depend on the particular facts involved, the operating system involved, and your good judgment. Usually, networked computers should be shut down following normal shutdown procedures as dictated by the operating system involved. Usually, stand-alone computers can be unplugged as long as background processes are not active, e.g. disk defragmentation.

Issues Of Evidence

If at all possible, avoid running any programs on the subject computer. Doing so can create temporary files that may overwrite valuable evidence. Also, be careful using the keyboard to enter standard operating system commands. Even one wrong press of a key can trigger destructive memory resident programs that may have been planted on the computer.

Your initial and primary job is to preserve the computer evidence and to transport the computer to a safe location where a complete bit stream backup of all stored data areas can be made. You also want to ensure that the computer system can be reconfigured to match the configuration in which it was found. For this purpose, it is wise to take pictures of the complete computer system from all angles. Wires should be marked such that they can be easily reconnected. Also, the computer should be clearly marked as evidence and stored out of reach of inquiring co-workers. Chain of custody is as relevant when it comes to computers as any other form of evidence.

Law enforcement agencies have come under scrutiny in recent times regarding evidence issues. For this reason, it is important to do things right. Be sure to properly document the time, date and circumstances surrounding the actual seizure of the computer. This helps rebut the contention later on that the evidence on the computer was planted by the computer specialist. Every effort must be made to show that no one could have made changes to the information contained on a seized computer system. Without such assurances, countless hours of processing effort may prove to be wasted time and the case may be lost at trial.

If seizure of the computer is carried out when the system is attended, any individual attending the computer should be immediately removed from the vicinity. One press of a pre-arranged key combination can potentially destroy all evidence stored on a hard disk. A destructive process can be initiated in a heartbeat and the results can be disastrous. Consider using a subterfuge to remove the operator from the computer to eliminate the possibility of them destroying potential evidence. Raid planning is very important, and this is especially true if the probability of destructive processes exist.

Recovering Deleted Digital Evidence:

According to a survey, 93% of all information never leaves the digital form. The majority of information these days is being created, modified, and consumed entirely in digital form. This means most spreadsheets and databases never make it on paper, and most digital snapshots never get printed. In this article, we will discuss methods and techniques to recover deleted digital evidence.

What is Digital Evidence?

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

Destroyed Evidence

In a criminal or cyber-criminal case, the attempts to destroy the evidence are very common. Such attempts can be more or less successful depending upon the following conditions:

- Action is taken to destroy the evidence.

- Time Available to destroy the evidence.
- Type of storage device like magnetic hard drive, flash memory card, or SSD drive.

In this section, we will be discussing some of the **methods to destroy the evidence** and **ways**

What is Password Cracking?

Password Cracking is a technique used to gain access starting from personal information and applies to organizational security. As with the ongoing advancement of technology data protection and management are very important and have a vital role in the prevention of cyber fraud and hacking.

Creation and management of unique and strong passwords are the ways to enforce data security and as well as periodically make necessary updates. However, hackers or cybercriminals can steal and get access to personal and sensitive data by employing the password cracking technique also for individuals and businesses.

What Does Password Cracking Mean ?

Password cracking refers to the process of attempting to decipher passwords by using various techniques, such as dictionary attacks, brute force attacks, and rainbow table attacks, and is used by hackers to gain access to sensitive data, financial information, or personal accounts.

Password cracking involves the illicit process of obtaining unauthorized access to a computer system an online account or any personal accounts by decrypting passwords.

UNIT-IV
Digital Forensics

What is Digital Forensics?

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

History of Digital forensics

Here, are important landmarks from the history of Digital Forensics:

- Hans Gross (1847 -1915): First use of scientific study to head criminal investigations
- FBI (1932): Set up a lab to offer forensics services to all field agents and other law authorities across the USA.
- In 1978 the first computer crime was recognized in the Florida Computer Crime Act.
- Francis Galton (1982 – 1911): Conducted first recorded study of fingerprints
- In 1992, the term Computer Forensics was used in academic literature.
- 1995 International Organization on Computer Evidence (IOCE) was formed.
- In 2000, the First FBI Regional Computer Forensic Laboratory established.
- In 2002, Scientific Working Group on Digital Evidence (SWGDE) published the first book about digital forensic called “Best practices for Computer Forensics”.
- In 2010, Simson Garfinkel identified issues facing digital investigations
- Objectives of computer forensics

Here are the essential objectives of using Computer forensics:

- It helps to recover, analyze, and preserve computer and related materials in such a manner that it helps the investigation agency to present them as evidence in a court of law.
- It helps to postulate the motive behind the crime and identity of the main culprit.
- Designing procedures at a suspected crime scene which helps you to ensure that the digital evidence obtained is not corrupted.
- Data acquisition and duplication: Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.
- Helps you to identify the evidence quickly, and also allows you to estimate the potential impact of the malicious activity on the victim
- Producing a computer forensic report which offers a complete report on the investigation process.
- Preserving the evidence by following the chain of custody.
- **Process of Digital forensics :**

Digital forensics entails the following steps:

- Identification
- Preservation
- Analysis
- Documentation
- Presentation

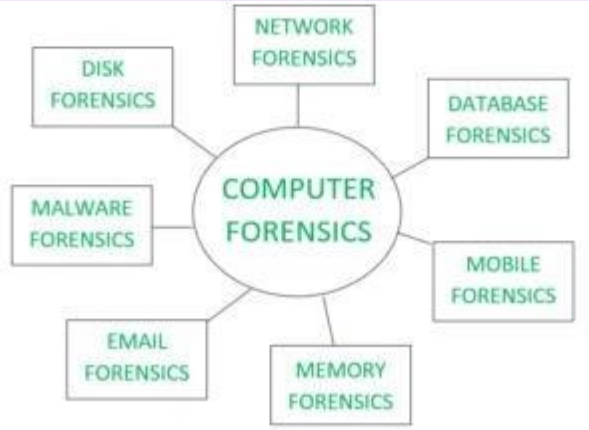
Introduction of Computer Forensics :

INTRODUCTION

Computer Forensics is a scientific method of investigation and analysis in order to gather evidence from digital devices or computer networks and components which is suitable for presentation in a court of law or legal body. It involves performing a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computer and who was responsible for it.

TYPES :

- Disk Forensics: It deals with extracting raw data from the primary or secondary storage of the device by searching active, modified, or deleted files.
- Network Forensics: It is a sub-branch of Computer Forensics that involves monitoring and analyzing the computer network traffic.
- Database Forensics: It deals with the study and examination of databases and their related metadata.
- Malware Forensics: It deals with the identification of suspicious code and studying viruses, worms, etc.
- Email Forensics: It deals with emails and their recovery and analysis, including deleted emails, calendars, and contacts.
- Memory Forensics: Deals with collecting data from system memory (system registers, cache, RAM) in raw form and then analyzing it for further investigation.
- Mobile Phone Forensics: It mainly deals with the examination and analysis of phones and smartphones and helps to retrieve contacts, call logs, incoming, and outgoing SMS, etc., and other data present in it.



Forensic hardware and software tools for computer forensics include[12]:

- **Forensic Toolkit (FTK)**: An inexpensive software tool with an easy-to-use interface.

- **Forensic Recovery of Evidence Device (FRED)**: A forensic workstation with an interface for various occasions.
- **EnCase Forensic**: A widely used computer forensic software.
- **Tableau Forensic Imager TX1**: A hardware solution for connecting computer's physical parts.
- **Magnet Forensics AXIOM**: Another software solution for digital forensic investigations.
- What is advanced analytics?

  Advanced analytics refers to a collection of sophisticated techniques and tools that are used to analyze large volumes of data, uncover hidden patterns and provide actionable insights.

- These techniques go beyond traditional business intelligence (BI) and descriptive statistics by employing methods such as predictive analytics, artificial intelligence (AI), machine learning (ML), data mining and statistical analysis. The goal of advanced analytics is to enable organizations to make data-driven decisions, predict future trends and optimize business processes. By using advanced algorithms and computational power, advanced analytics can handle complex data sets and deliver deeper insights, ultimately leading to improved performance, innovation and competitive advantage.

  The history of advanced analytics

  The history of advanced analytics is rooted in the evolution of data analysis and computing technology, which has progressed significantly over several decades.

  In the early 20th century, data analysis was primarily manual, involving basic statistical methods and simple calculations. The advent of computers in the mid-20th century revolutionized data processing, allowing for more complex analyses. During the 1960s and 1970s, the development of databases and data management systems laid the groundwork for storing and retrieving large volumes of data efficiently.

  The 1980s and 1990s saw the rise of BI tools, which enabled organizations to generate reports and conduct descriptive analysis. These tools provided insights based on historical data but were limited in their predictive capabilities. Concurrently, advancements in statistical software and methodologies emerged, paving the way for more sophisticated data analysis techniques.

ADVANCES IN FORENSIC SCIENCE TECHNOLOGIES (2024)

Automated Firearm Identification

The Integrated Ballistic Identification System (IBIS) offered by Forensic Technology is a cutting-edge solution for firearm and tool mark identification. This advanced system facilitates the sharing, comparison, and automated identification of significant quantities of exhibit information and images across a network of imaging sites. The latest generation of IBIS technology boasts exceptional 3D imaging, advanced comparison algorithms, and a robust infrastructure. It’s designed to meet the needs of police and military organizations, providing actionable information derived from firearms and their fired ammunition components.

Blood Pattern Analysis Software

Bloodstain pattern analysis (BPA) software is an emerging technology in forensic science that seeks to reconstruct crime scenes by analyzing blood and bloodstains. This computer-based software can estimate the Area(s) of Origin (AO) of a bloodletting event, providing crucial insights into the sequence of events at a crime scene. However, according to a study published in “Forensic Science International,” only two validation studies have involved impact patterns created more than 1 meter from the main target surface. Furthermore, using BPA software in actual criminal cases is not well documented. Thus, while promising, this technology requires further research and validation to ensure it meets the rigorous standards required for court admissibility.

Mass Spectrometry Techniques

The paper published in the Journal of Analytical Methods in Chemistry presents an advanced technique for identifying and quantifying synthetic cannabinoids using liquid chromatography-tandem mass spectrometry (LC-MS/MS). This technology, which contributes to forensic toxicology, offers high selectivity and sensitivity, making it an invaluable tool for analyzing complex biological samples. Synthetic cannabinoids, often referred to as ‘Spice’ or ‘K2’, are a significant challenge in drug abuse due to their structural diversity and continually changing compositions. The LC-MS/MS method developed can simultaneously identify and quantify 24 synthetic cannabinoids in urine, making it a potent tool in testing for the presence of cannabis in humans.

Sensitive Detection Methods

Sensitive detection in the field of medicine and dentistry refers to the use of advanced technologies to detect minute amounts of specific substances or changes in the body. This is crucial for early diagnosis, monitoring disease progression, and assessing the effectiveness of treatment. Techniques like mass spectrometry, fluorescence detection, and molecular imaging are commonly utilized for sensitive detection. For instance, mass spectrometry has become an invaluable tool in clinical laboratories due to its high sensitivity and specificity for identifying biomarkers and drugs. Similarly, fluorescence detection methods are widely used in biological research and medical diagnostics for their high sensitivity and non-invasive nature.

Omics Techniques

The use of omics techniques in forensic entomology, as discussed in an article published in “Forensic Science International”, represents a significant advancement in the field. These techniques, which include genomics, transcriptomics, proteomics, metabolomics, and microbiome analysis, allow for a comprehensive and systematic study of biological samples. In the context of forensic entomology, they are used for species identification, phylogenetics, and screening for developmentally relevant genes, among other applications. They also play a crucial role in interpreting the behavioral characteristics of species related to forensics at the genetic level.

Carbon Dot Powders

Fingerprints are essential for analyzing many crime scenes. However, there are many reasons why it may be hard to see one clearly, including low sensitivity, low contrast, or high toxicity.

Researchers have developed a fluorescent carbon dot powder that can be applied to fingerprints, making them fluorescent under UV light and subsequently much easier to analyze. With this new application, fingerprints will glow red, yellow, or orange.

Artificial Intelligence

While artificial intelligence (AI) has been used in many other fields for decades, it is relatively new to forensic science. This is primarily because all evidence and the analysis must stand up in court. However, recent advancements have seen AI utilized successfully in all forensic components of a criminal case. While AI is most often used in digital forensics, it is increasingly used to analyze a crime scene, compare fingerprint data, draw conclusions from photograph comparisons, and more.

Nanotechnology

Atomic and molecular technology are finding their way into forensic science. Analyzing forensic materials at this minute level can offer scientists insights that previously weren’t accessible.

Nanosensors are being utilized to examine the presence of illegal drugs, explosive materials, and biological agents on the molecular level. Specific advancements this past year have included scientists’ ability to analyze the presence of carbon and polymer-based nanomaterials to make their determinations and aid investigators.

Proteomes

Forensic scientists have traditionally relied heavily on DNA to determine a suspect or victim. However, advances in detecting and identifying proteins have made proteomes an essential forensic science tool. Proteomes are a complete set of proteins produced by an organism.

Scientists can find proteomes in blood, bones, and other biological materials and analyze them to find answers, such as if a victim came in contact with an otherwise undetectable venom or matching a severely degraded body fluid sample to a perpetrator. One aspect of proteomes that differs from DNA is that they change over time, offering scientists valuable insights into a victim’s age or other environmental factors at the time of death that are impossible to detect through other methods.

Foldscope

The Foldscope is a small, disposable, inexpensive paper microscope that has been around since 2014. However, just recently, it has found its way from third-world country applications into the world of forensic science. Due to its portability and low cost, the Foldscope can be used in the field to make on-the-spot determinations about forensic samples, including blood, hair, and soil.

While the conclusions drawn with Foldscope are only preliminary, they can aid law enforcement early on in an investigation and speed up the discovery process. Using a Foldscope in the field can also lighten the load for forensic laboratories, which are often backlogged and can take significant time to deliver results.

METHODOLOGY FOR THE FEATURED FORENSIC SCIENCE TECHNOLOGIES :

Several factors were considered when deciding which technologies to include on this list.

- **Relevance to the Topic of Forensic Technology:**
  The said technology must be actively used in the field of Forensic Science and can be taught at the college level. Widely regarded technologies were considered first, while more experimental technologies were included only based on reputable peer-reviewed documentation.
- **Novelty in the Field of Forensic Science:**
  More experimental technologies were given higher priority based on whether the technology gave advanced information that is not readily available by using other technologies. These “cutting-edge” technologies were thoroughly vetted to ensure that they have become accepted techniques by leaders in the field.
- **Reliability of Technology:**
  Finally, only techniques used with more than 80 percent reliability were included in this list. Factors affecting reliability include case closure, successful conviction, and correct identification rates.

Unit – V

Laws and Acts

Law and Ethics

Law and ethics in the context of social sciences refer to the importance of legal regulations and moral principles in guiding the behavior of healthcare practitioners and ensuring the well-being of patients.

Ethical Foundations

INTRODUCTION

This chapter defines and describes morals, ethics, and law; describes the four foundational biomedical ethical principles of beneficence, nonmaleficence, justice, and autonomy; and offers a systems approach to health care professional ethical decision making. The modern "blending" of legal and professional ethical obligations is addressed, under which a substantive violation of law by a health care provider-fiduciary (person in a position of special trust) more often than not also constitutes a violation of professional ethics.

What is digital evidence

The evidence is generally termed as proof of records or any relevant information. The explanation to Section 79A of the Information Technology (Amendment) Act (2008) defined the electronic evidence, as any information with values that is stored or transmitted electronically, and it includes evidence such as computer data, digital audio, digital video, cell phones and digital fax machines.

Digital evidence refers to stored, transmitted, or collected information that is used as proof before the court of justice. The information is stored, transmitted, or collected in digital media like computers, mobiles, and other electronic devices. The digital evidence may be in numerous forms including, messages, pictures, videos, and other digital forms. There is no need for handwritten notes or fingerprint tests during an investigation with regard to digital evidence. The digital evidence is always stored in electronic form, not in traditional paper documents.

Scope of digital evidence

Nowadays, the scope of digital evidence is widening because of continued growth in the digital world. Digital evidence plays a major role in different areas that include legal proceedings, cyber security, corporate investigation, e-discovery, intellectual property theft, forensic analysis, and many other areas. Digital evidence is in many forms including electronic communications, digital documents, multimedia files, internet browsing history, computer data, network data, mobile device data, digital signatures, certificates, and many others.

Need for digital evidence

In India, digital evidence plays a significant role in establishing the claims of each party before the court of law. Some of the major reasons for the need for digital evidence are as follows:

- Digital evidence serves as a detailed and authentic record of electronic records such as emails, text messages, and social media interactions, and helps to present the comprehensive facts in an easier manner.
- In criminal and civil cases, digital evidence assists legal professionals and law enforcement agencies such as the judiciary to investigate and reconstruct events. Digital evidence assists in identifying people, tracing financial transactions and discovering connections between people and entities.
- Well-established digital evidence is more trustworthy and reliable. Electronic records are maintained safely by putting passwords and security. It is hard to change or mess up as compared to traditional paper documents.
- Digital evidence helps to establish intellectual property theft, copyright infringement, or violation of digital rights by providing a clear record of data through different digitised methods. It helps to establish ownership and provides proof of unauthorized use or distribution of digital assets.
- Digital evidence plays a crucial role in establishing facts in concern with the cyber crimes, which have been occurring more recently. In order to combat cyber crimes like cyber harassment, online bullying, online fraud and other related offences, digital proof is essential to establish real facts.
- The role of digital records in electronic contracts and transactions is pivotal. Due to growth in the digital world, almost every business prefers to engage in electronic contracts and many electronic transactions. In such situations, a digital proof is required to establish the reliability of these documents. This includes emails, digital contracts, and records of transactions.
- When there are issues with keeping information safe or if someone’s private details get leaked, digital evidence plays a very important role in order to prove what actually happened.
- In matters that deal with national security, the role of digital evidence is phenomenal. Due to technological advancements, the government stores its important documents in the form of electronic records by establishing its official sites. If any security issues arise then it assists in enhancing accessibility, efficiency and facilitates the secure management of sensitive information. Digital evidence helps to determine cybercriminals by finding out where attracts come from and giving proof to court. It also helps to stop future attacks by finding weaknesses in a system and fixing them. For instance, if there’s a pattern that shows a possible threat, digital evidence can help to take action before an attack happens. Thus, it protects the national interest.
- The matter deals with border issues, digital evidence is very essential. The digital technology is used to monitor border security issues. In order to analyse and monitor activities related to potential threats, it plays a role in verifying identities, tracking the movement of individuals, and preventing illegal activities across borders.
- Digital evidence is essential for establishing the facts concerned with public safety. Police and security teams use digital information to monitor online activities and, they can investigate as early as possible.
- In the healthcare sector, the adoption of digital technology is important to make sure that information about the patient is kept private and secret. It helps in checking if someone is misusing medical records or doing something wrong with the patient’s information. It can be used as digital evidence if any issues arise in future.

Types of digital evidence

Digital evidence is the information or data which is in the electronic forms. The widespread use of technology in different aspects of life has led to an increase in the different forms of digital evidence. Here are some of the types of digital evidence:

- Communications through text messages, emails, instant messaging, and other electronic messaging platforms can be used as digital evidence.
- Social media posts, comments, messages, and other content from any other social media platforms like Facebook, Twitter, Instagram, etc., can be used as valuable digital evidence.
- Digital documents, spreadsheets, presentations, and other file types are also forms of digital evidence. Metadata within these files may also provide important information.
- Digital photos and videos can be powerful evidence. Metadata, such as timestamps, and geolocation data, can be crucial in order to establish authenticity and context of media files.
- Logs that record computer and internet activities, including browsing history, file access and system logs, can be analysed as digital evidence.
- Mobile devices and some digital cameras record GPS and location data, and are also considered as digital evidence.
- Records of phone calls, including call logs, durations and time stamps, can be treated as digital evidence.
- Digital records of financial transactions are considered digital evidence. That includes bank statements, online purchases and electronic fund transfers, which can be important in financial investigations.
- Fingerprints, facial recognition data, and recording of unique voice characteristics may be used as digital evidence.
- Information related to network traffic, IP addresses, and connection logs can be important for cybersecurity and digital forensics.
- Information that is related to software usage, application logs and system configurations can be treated as digital evidence.
- Data which is stored in cloud services such as Google Drive, Dropbox, or One drive, can be used as evidence.
- Metadata associated with digital files, such as creation data, modification history, and user information is also considered digital evidence that is used for forensic purposes.
- Cryptocurrencies, and blockchain transactions, can also serve as digital evidence.

Admissibility of digital evidence in Indian Law

In India, the admissibility of digital evidence depends on the different laws, and courts rulings. The Indian legal system has given legal recognition to digital evidence and such recognition of digital evidence is covered under different laws that include as following:

Indian Evidence Act, 1872

The Indian Evidence Act, of 1872 is one of the foundational legislation that continues to be highly relevant in the Indian legal system. Under this legislation, certain provisions direct how evidence is treated in the court. Initially, the Indian Evidence Act didn’t bear direct provisions for the admissibility of digital evidence. Later in the year 2000, an amendment was made to the Indian Evidence Act, accordingly, Section 65B of the Indian Evidence Act, has given legal recognition to digital evidence. Section 65B specifically addresses the admissibility of the electronic records before the court. As per the section, the electronic records include emails, or digital documents or other documents acceptable as evidence in Court. This document can be used as evidence in court without having to show the original digital file, subject to some conditions mentioned in the section that needs to be followed. This allows easier use of electronic information as evidence.

Guide on Evidence Handling and Procedures

Importance: Evidence Handling and Procedures form a critical part of any legal investigation in information security, particularly in situations involving breaches or potential criminal activity. Mishandled evidence can compromise cases and result in legal setbacks.

What it is: Evidence Handling and Procedures refers to the proper approach to collection, documentation, storage, and preservation of evidence in legal investigations tied to information security. This includes accurate recording of its origin, strict adherence to chain of custody protocols, and maintaining its integrity until formally required.

How it works: Evidence is first identified and then collected using forensically sound methods. It is documented meticulously, including its origin, the person collecting it, and any actions taken. The evidence is then stored and preserved securely to maintain its integrity, and a strict chain of custody is maintained to ensure it hasn't been tampered with.

How to answer questions in an exam: Familiarize yourself with core principles of evidence handling, such as the importance of the chain of custody, baseline knowledge of local legislation, and the need for proper documentation. Understand the difference between volatile and non-volatile evidence, and the appropriate methods for collecting and preserving each.

Exam Tips - Answering Questions on Evidence Handling and Procedures: Remember that maintaining the integrity of the evidence is paramount. Any hint of tampering or mishandling will render the evidence useless in a court of law. Be aware that some questions might try to trick you into selecting an answer that involves improper handling or storage techniques. Stick to the principles of strict documentation and adherence to chain of custody.

Basics of Indian Evidence ACT IPC and CrPC :

The **IPC** defines the offenses and their penalties, the **CrPC** guides the procedural journey from investigation to resolution, and the **Indian Evidence Act** ensures a reliable basis for decision-making through rules governing evidence presentation. This symbiotic relationship is crucial for the effective functioning of India’s criminal justice system

Difference Between IPC and CrPC :

The difference between IPC and CrPC lies in their respective roles in the Indian criminal justice system. IPC serves as the substantive law that outlines the definition and punishment for various criminal offenses. It focuses on the specific acts that constitute a crime and the corresponding consequences.

On the other hand, CrPC plays a procedural role in the criminal justice system. It governs the process followed by the police, courts, and correctional institutions during the investigation, prosecution, and trial of criminal offenses. It lays down a framework for the enforcement of IPC.

Therefore, it is important to note that the difference between IPC and CrPC lies in their distinct functions. IPC provides the substance of criminal law, while CrPC provides the procedure for its enforcement. Without CrPC, the criminal justice system would be unable to enforce IPC's provisions effectively. Thus, both IPC and CrPC play crucial roles in maintaining law and order in India.

Indian Penal Code (IPC)	**Criminal Procedure Code (CRPC)**
Deals with criminal offenses and their punishments	Deals with the procedures for enforcing the criminal laws laid out in the IPC
Defines what actions are considered crimes and the punishments for those crimes	Outlines the process for investigating, trying, and punishing criminals
Consists of various sections, each dealing with a specific type of crime	Consists of various sections, each dealing with a specific aspect of the criminal justice process, such as arrest, bail, and appeals
Is a substantive law	Is a procedural law
It is a central law	It is a central law

What is Indian Penal Code (IPC)?

Indian Penal Code (IPC) lays down the laws that define crimes and their punishments. The IPC was written in 1860 and is applicable to all citizens of India and other persons within Indian territory. It covers a wide range of offenses, including theft, fraud, assault, murder, and other crimes. The IPC is enforced by the police and the courts.

Advantages of Indian Penal Code (IPC)

India's main criminal code is the Indian Penal Code (IPC), which has several advantages, including:

1. Clarity: A wide range of people can understand the IPC because it is written in clear, easy-to-understand language.

2. Comprehensive coverage: A variety of criminal offenses are covered under the IPC, including murder, theft, and fraud.
3. Historical significance: Originally enacted in 1860, the IPC has been amended several times to adapt to changing societal norms and legal requirements over the years.
4. Legal consistency: All citizens are treated equally under the IPC, which provides a **consistent framework for dealing with criminal offenses across the country.**
5. Recognized globally: Internationally, the IPC has been adopted as a criminal code by many countries.
6. Help in maintaining law and order: By providing them with the necessary legal tools to combat crime, the IPC assists law enforcement agencies in India in maintaining law and order.

Electronic Communications Privacy Act of 1986 (ECPA),

View Federal Statutes

Description

Background

The Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act are commonly referred together as the Electronic Communications Privacy Act (ECPA) of 1986. The ECPA updated the Federal Wiretap Act of 1968, which addressed interception of conversations using "hard" telephone lines, but did not apply to interception of computer and other digital and electronic communications. Several subsequent pieces of legislation, including The USA PATRIOT Act, clarify and update the ECPA to keep pace with the evolution of new communications technologies and methods, including easing restrictions on law enforcement access to stored communications in some cases.

General Provisions

The ECPA, as amended, protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers. The Act applies to email, telephone conversations, and data stored electronically.

Civil Rights and Civil Liberties

"The structure of the SCA reflects a series of classifications that indicate the drafters' judgments about what kinds of information implicate greater or lesser privacy interests. For example, the drafters saw greater privacy interests in the content of stored emails than in subscriber account information. Similarly, the drafters believed that computing services available 'to the public' required more strict [sic] regulation than services not available to the public…To protect the array of privacy interests identified by its drafters, the [Act] offers varying degrees of legal protection depending on the perceived importance of the privacy interest involved. **Some information can be obtained from providers with a subpoena; other information requires a special court order; and still other information requires a search warrant.** In addition, some types of legal process require notice to the subscriber, while other types do not."

The Act reflects a general approach of providing greater privacy protection for materials in which there are greater privacy interests. For a more in-depth analysis

Specific Provisions

The ECPA has three titles:

Title I of the ECPA, which is often referred to as the Wiretap Act, prohibits the intentional actual or attempted interception, use, disclosure, or "procure[ment] [of] any other person to intercept or endeavor to intercept any wire, oral, or electronic communication." Title I also prohibits the use of illegally obtained communications as evidence.

Exceptions. Title I provides exceptions for operators and service providers for uses "in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service" and for "persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act (FISA) of 1978." . It provides procedures for Federal, State, and other government officers to obtain judicial authorization for intercepting such communications, and regulates the use and disclosure of information obtained through authorized wiretapping. . A judge may issue a warrant authorizing interception of communications for up to 30 days upon a showing of probable cause that the interception will reveal evidence that an individual is committing, has committed, or is about to commit a "particular offense" listed in Section 2516.

Title II of the ECPA, which is called the Stored Communications Act (SCA), protects the privacy of the contents of files stored by service providers and of records held about the subscriber by service providers, such as subscriber name, billing records, or IP addresses.

Title III of the ECPA, which addresses pen register and trap and trace devices, requires government entities to obtain a court order authorizing the installation and use of a pen register (a device that captures the dialed numbers and related information to which outgoing calls or communications are made by the subject) and/or a trap and trace (a device that captures the numbers and related information from which incoming calls and communications coming to the subject have originated).

. No actual communications are intercepted by a pen register or trap and trace. The authorization order can be issued on the basis of certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by the applicant's agency.

Amendments

The ECPA was significantly amended by the Communications Assistance to Law Enforcement Act (CALEA) in 1994, the USA PATRIOT Act in 2001, the USA PATRIOT reauthorization acts in 2006, and the FISA Amendments Act of 2008 .Other acts have made specific amendments of lesser significance.

Socio-Legal Perspectives

Introduction

There is a tendency among housing policy scholars to see law as merely a tool of policy implementation, and/or as a neutral background to the provision and consumption of housing. These views underestimate the importance of the legal frameworks that shape every aspect of housing. A thorough and systematic engagement with the law, which is the foundation of socio-legal research, is necessary for a full understanding of housing and home.

Seen from the socio-legal perspective, law is a dynamic force that affects every type of housing decision-maker and the everyday lives of all housing occupiers. Socio-legal scholarship has a long history, which differentiates it from traditional legal analysis. The more conventional approach to researching law in relation to housing would focus on how particular legal doctrines have developed, through close reading and analysis of legislation and the decisions of the higher courts. In contrast, a socio-legal perspective emphasises law in action (also sometimes referred to as law in the real world, and as living law), in contrast to the law found in legal texts. This approach involves looking at the impact of law on the social world, and considering law itself as a field or aspect of social experience. Empirical socio-legal research often focuses on the mundane workings of law, and on the operation of law by frontline actors (e.g., housing officers and district judges hearing and deciding housing cases in court). It can also take into account how an understanding of the law is developed by these actors, and by each housing occupier, by exploring how their participation in everyday activities contributes to law in the social world.

The full range of methodologies developed in the social science field may be used by socio-legal scholars – quantitative, qualitative, ethnographic, and so on. A significant proportion of socio-legal research takes the form of evidence-based applied research, often funded by government, which can be used to underpin legal and social policy and recommendations for legal reform. The results from such studies should inform housing-related decisions of the legislature, law reform bodies, the judiciary, and various regulatory housing organisations.

Specialisation within socio-legal studies may be based on the relevant area for research (housing being the area of research under consideration here); on the primary social science discipline that is drawn on for theorisation (e.g., sociology or anthropology); on the basis of the most relevant methods and techniques of law (dispute resolution or regulatory enforcement, e.g., in the field of housing); or on a combination of these factors. The following discussion illustrates the wide scope of this perspective through socio-legal studies related to housing and the home.

Psychology and the Law, Overview

3.1 Legal Competency

The article on legal competency by Poythress delineates the types of decision-making abilities or competencies at discrete moments in the civil and criminal legal process about which courts most frequently seek advice from psychologists trained in forensic assessment and evaluation. The accompanying tables and charts succinctly illustrate the legal standards or issues in the cases and the related psychological competencies that bear on them. Three elements that must be addressed by a forensic psychologist in each case involving an assessment of fitness or competency are (1) the presence of a mental condition that causes an impairment, (2) specifications of the functional impairment, and (3) the distinct legal abilities key to the case that are affected.

The article begins by orienting practitioners to the context of the task by outlining a framework within the law that psychologists are well advised to understand in order to offer more useful information to the courts. A helpful conceptual tool for practitioners and psycholegal researchers is a table listing the five aspects of legal competencies identified by Grisso, as it sets forth those aspects of the task most clearly within the province of the forensic psychologist, and those aspects most clearly within the province of the fact finder (judge or jury). In particular, it is important to note that the legal standards or tests for fitness vary from one circumstance to the next. Accordingly, the psychologist must appropriately tailor the information critical to the fact finders in applying the legal standard appropriate to a given case. Many of the competence tests and standards pertinent to civil cases have received less research attention than those pertinent in criminal cases, i.e., criteria relevant to determinations of fitness to make decisions about guardianship, treatment, research participation, and testamentary capacity.

A point of significance is the limited utility of a diagnosis in many legal proceedings. Although the goal or end point of many clinical mental health inquiries is a diagnosis, legally, the diagnosis itself is of little value to a court charged with determining whether someone meets the criteria for a defense of insanity or otherwise lacks fitness to proceed to trial. The fact finder seeks a functional description or understanding of the nature and scope of an individual's impairment from the consulting expert. A diagnosis by a mental health professional of a mentally disabling condition or disorder does not guarantee that the applicable legal test will be met, but the diagnosis may be of some relevance. Severe mental disturbance or lack of a diagnosis neither guarantees nor is fatal to a claim of incompetence or insanity.

The terms insanity and incompetence are legal, not psychological, concepts. The legal test for insanity varies from one jurisdiction or community to another, although most tests incorporate the offender's cognitive awareness of the consequences of the conduct at issue. Tests that address some of the "irresistible impulse" standards have in some cases devolved into a question as to whether the accused would engage in the same conduct were there a policeman present. In some states or countries, the standard of "guilty but mentally ill" has been adopted as a variant of "not guilty by reason of insanity." In other communities, legal policy reforms have established that voluntary conduct that produces diminished capacities, such as drinking alcohol or taking drugs, obviates resort to this defense. Finkel points out that policies along these lines conform with the results of studies of juror decision making in insanity cases, which revealed that jurors often take into account the offender's capacity to make responsible choices and whether the offender was negligent or reckless in bringing about his or her mental disability.

In his article, Poythress adroitly sets controversial topics such as the insanity defense in context by pointing out the infrequency of its use and its low success rate. He also emphasizes the importance of and demand for many other fitness determinations by psychologists, such as fitness to stand trial, or when the death penalty applies, fitness to be executed. Although it is difficult to obtain precise figures of the number of evaluations prepared annually on issues of fitness or competence, Costanzo shows that approximately 5% of all criminal defendants are assessed for competence to stand trial. Thus, Zapf and Roesch provide estimates that between 25,000 and 39,000 psychological evaluations for competence to stand trial are performed annually in the United States, making this one of the most frequently requested psychological services. Of the group of offenders evaluated for this purpose, Melton *et al.* indicate that a relatively small proportion, 12%, is found incompetent.

This article provides an excellent overview of methodological issues facing professionals who are bound to offer evidence-based conclusions to the court. The article includes practical advice to practitioners, such as avoiding controversy as an expert by refusing to prepare a report that addresses more than one type of fitness. Similarly, psychologists are advised to avoid making any statement about the "ultimate legal issue." As Poythress points out, to do so mixes moral and professional standards.

Critical Legal Studies

1 Antecedents of CLS

To critique the orthodoxies of their legal culture, American critics in the first phase of their movement found resources in various European theories, especially Western neo-Marxist theories of law as ‘ideology’ and an instrument of ‘hegemony’ (Gramsci 1971), humanist social histories of subordinated groups (Hay 1975, Thompson 1971), structuralism, and phenomenology. But their main resource turned out to be their domestic forerunners, the American legal realists of the 1920s and 1930s who critiqued the classical–formalist legal orthodoxy of their own day (see *Legal Realism*; *Legal Formalism*). That orthodoxy had claimed that the operating rules of the legal system could be derived from a few basic principles induced from a scientific arrangement of precedents, such as the protection of property, the basing of liability to others on ‘fault,’ and the enforcement of the ‘free will’ of parties to contracts. This system added up to a natural and neutral mode of ordering private life, and legislative interferences with this system of rules would be struck down as unconstitutional unless they met strict tests of validity.

The realists' critique, in brief, was that (a) the principles were too vague, and the precedents too flexible, to determine outcomes, and in actual operation produced results varying over time and with contexts; (b) the actual determinants of results were latent and unarticulated policies, ideologies, and social vision; and (c) the ‘private’ law rules of property-tort-contract that undergirded the natural-seeming private sphere of free choice in free markets, protected against interference by constitutional law, were no less artificial, no less exercises of state policy, and no less coercive, than the ‘public’ rules of legislation and administration. A property right, for example, delegated to its owner the ultimate power to use state force (self-help, private guards, the police or the army) to exclude others (such as union members or black people) he did not want to hire or deal with, and to condition access to his property (tools, land, wages, the assets of a marriage) on those others' submitting to his orders. The coercive state was always involved in the market and business firms and family life; the issues for legal policy were thus not *whether* the state should be involved, but *how*, and *to what ends*—issues that courts, as well as legislatures and administrative agencies, could not avoid and had to resolve.

THE END

NRCM

your roots to success...