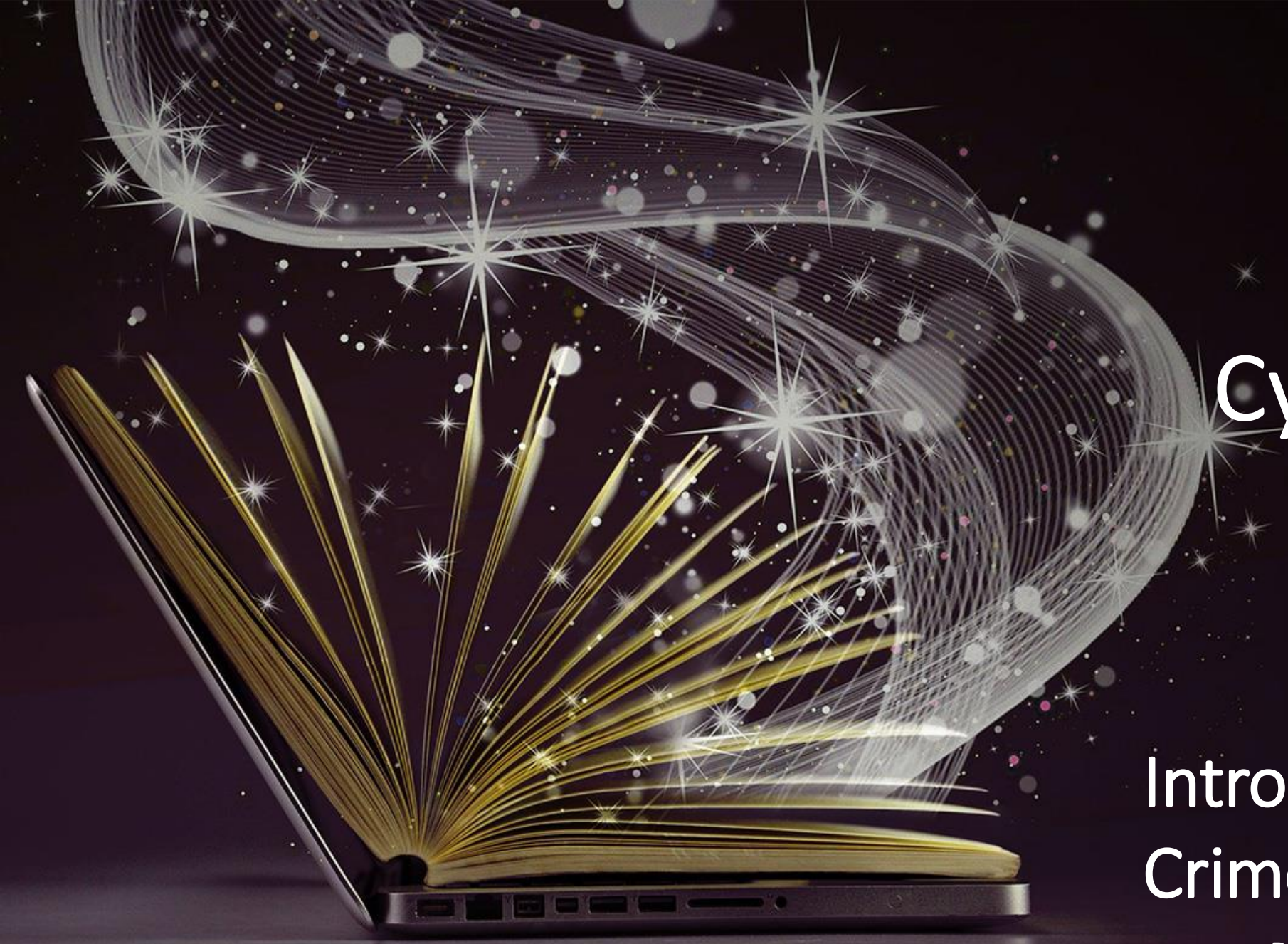


# Cyber security (3150714)

## Module 04

## Introduction to Cyber Crime and law

Prof. Tushar Gohil, Assistant Professor
Sarvajanik College of Engineering and Technology, Surat.

# Cyber Crimes

**Types of Cybercrime, Hacking, Attack vectors, Cyberspace and Criminal Behavior, Clarification of Terms**

# Cyber Crime

- ***Cyber Crime*** is criminal activity that either targets or uses a computer, a computer network or a networked device.
- Most, but not all, cybercrime is committed by cybercriminals or hackers who want to make money. Cybercrime is carried out by individuals or organizations.
- Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers.
- Rarely, cybercrime aims to damage computers for reasons other than profit. These could be political or personal.
- While that image is in the public consciousness thanks to movies and TV, the real picture of a cybercriminal is much different: cybercrime is incredibly organized and professionalized.

# Cyber Criminals

- ***Cyber Criminals*** are individuals or teams of people who use technology to commit malicious activities on digital systems or networks with the intention of stealing sensitive company information or personal data and generating profit.
- Cybercriminals are known to access the cybercriminal underground markets found in the deep web to trade malicious goods and services, such as hacking tools and stolen data. Cybercriminal underground markets are known to specialize in certain products or services.
- Hacking does not necessarily count as a cybercrime; as such, not all hackers are cybercriminals. Cybercriminals hack and infiltrate computer systems with malicious intent, while hackers only seek to find new and innovative ways to use a system, be it for good or bad.
- Cybercriminals also differ greatly from threat actors in various ways, the first of which is intent. Threat actors are individuals who conduct targeted attacks, which actively pursue and compromise a target entity’s infrastructure.

# Hacking

- ***Hacking*** is an attempt to exploit a computer system or a private network.
- Simply put, it is the unauthorized access to or control over computer network security systems for some illicit purpose.
- **The objectives of hacking**
  - The intent of hacking is mostly malafide i.e. criminal or malicious intent, either to commit some fraud or to cause some financial or reputational harm to the person, group or entity so hacked.
  - This is done through stealing of confidential data or embezzlement of funds or other monetary resources, causing business disruptions, spreading of incorrect and malicious rumors, other misleading information which is socially detrimental.
  - Many a time, hacking is also defined as a form of cyber or internet crime which is punishable by law.
  - However, there is another side to hacking which is done on a professional level by accredited institutions and government law agencies. This is to counter the wrong intentions of the hackers or to prevent any harm being caused to individuals, bodies or associations. It is also undertaken for the safety and protection of the citizens and society at large.

# Hackers

- To better describe hacking, one needs to first understand hackers.
- A ***Hacker*** is a person who finds and exploits the weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security.
- One can easily assume them to be intelligent and highly skilled in computers.
- In fact, breaking a security system requires more intelligence and expertise than creating one.
- There are no hard and fast rules whereby we can categorize hackers into neat compartments.
- However, in general computer parlance, we can categorize hackers into three types.
    - **White Hat Hackers** : Professionals hack to check their own security systems to make it more hack-proof. In most cases, they are part of the same organization.
    - **Black Hat Hackers** : Professionals hack to take control over the system for personal gains. They can destroy, steal or even prevent authorized users from accessing the system. They do this by finding loopholes and weaknesses in the system. Some computer experts call them crackers instead of hackers.
    - **Grey Hat Hackers** : Curious people who have just about enough computer language skills to enable them to hack a system to locate potential loopholes in the network security system. Grey hats differ from black hats in the sense that the former notify the admin of the network system about the weaknesses discovered in the system, whereas the latter is only looking for personal gains.

# Types of Cyber Crimes

- **Malware** : It is the collective name for several malicious software variants, including viruses, ransomware and spyware.
- **Cyberbullying** : Refers to all kinds of online harassment, including stalking, sexual harassment, doxing (exposing someone's personal information, like their physical address, online without their consent), and fraping (breaking into someone's social media and making fake posts on their behalf).
- **Crypto Jacking :** when hackers break into your device and use it to mine cryptocurrency without your knowledge or consent. Crypto miners do this by using JavaScript to infect your device after you visit an infected website. This can cause performance issues and high electric bills for you — and earn big profits for the crypto jackers.
- **Cyberextortion :** is just what it sounds like — a digital version of the nightmare that is extortion. One of the most common forms is ransomware, when hackers infect your computer with malware that encrypts all your files until you pay them a ransom to unlock them. Cyberextortion can also refer to blackmailing victims using their personal info, photos, and video; or threatening businesses using methods like botnet-driven DDoS attacks.

# Types of Cyber Crimes

- **Cyber Espionage :** As mentioned, many cybercriminals these days are actually state-sponsored groups. Whether it's the North Koreans, the Iranians, or even the US's own NSA-affiliated Equation Group, world powers use hacker groups as one weapon in the complicated matrix of global politics. Stealing classified intelligence and using malware to attack nuclear plants are just two ways in which state-sponsored groups can do some frightening things on the world stage.
- **DDoS Attack :** A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic.
- **PUPs(Potentially Unwanted Programs) :** less threatening than other cybercrimes but are a type of malware. They uninstall necessary software in your system including search engines and pre-downloaded apps. They can include spyware or adware, so it's a good idea to install an antivirus software to avoid the malicious download.
- **Botnets :** networks from compromised computers that are controlled externally by remote hackers. The remote hackers then send spam or attack other computers through these botnets. Botnets can also be used to act as malware and perform malicious tasks.

# Types of Cyber Crimes

- **Online Scams :** These are usually in the form of ads or spam emails that include promises of rewards or offers of unrealistic amounts of money. Online scams include enticing offers that are “too good to be true” and when clicked on can cause malware to interfere and compromise information.
- **Exploit Kits :** An exploit kit is a type of toolkit cybercriminals use to attack vulnerabilities in systems so they can distribute malware or perform other malicious activities. Exploit kits are packaged with exploits that can target commonly installed software. Due to their highly automated nature, exploit kits have become one of the most popular methods of mass malware or remote access tool (RAT) distribution by criminal groups, lowering the barrier to entry for attackers.
- **Prohibited and illegal content :** This cybercrime involves criminals sharing and distributing inappropriate content that can be considered highly distressing and offensive. Offensive content can include, but is not limited to, sexual activity between adults, videos with intense violent and videos of criminal activity. Illegal content includes materials advocating terrorism-related acts and child exploitation material.

# Attack Vectors

- In cyber security, an attack vector is a method or pathway used by a hacker to access or penetrate the target system. Hackers steal information, data and money from people and organizations by investigating known attack vectors and attempting to exploit vulnerabilities to gain access to the desired system. Once a hacker gains access to an organization's IT infrastructure, they can install a malicious code that allows them to remotely control IT infrastructure, spy on the organization or steal data or other resources.
- **How do Hackers Exploit Attack Vectors?**
  - Hackers identify a target system that they wish to penetrate or exploit
  - Hackers use data collection and observation tools such as sniffing, emails, malware or social engineering to obtain more information about the target
  - Hackers use this information to identify the best attack vector, then create tools to exploit it
  - Hackers break the security system using the tools they created, then install malicious software applications
  - Hackers begin to monitor the network, stealing your personal and financial data or infecting your computers and other endpoint devices with malware bots

# Cyberspace and Criminal behaviour

- The word "cyberspace" is credited to William Gibson, who used it in his book, Neuromancer, written in 1984.
- Gibson defines cyberspace as "a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts.
- Cyberspace defined in other way – A fast growing area of crime
- A graphical representation of data abstracted from the banks of every computer in the human system.
- Cyber space is an electronic medium used to form a global computer network to facilities online communication.
- It is a large computer network made up of many worldwide computer networks that employ TCP/IP protocol to aid in communication and data exchange activities.
- Crimes are now being perpetrated through cyberspace . This includes the production and distribution of child pornography and child exploitation conspiracies, banking and financial fraud , intellectual property violations.
- Nigeria’s economic vitality and national security depend on a vast array of interdependent and critical networks, systems and  resources known as cyberspace.

# Cyberspace and Criminal behaviour

- Technological advances have impacted CRIMINAL BEHAVIOR IN THREE WAYS:
- Mass communication Technology has transformed media and popular culture into a powerful influence on offender behavior.
- Computer Technology has created new avenues and different opportunities for criminal behavior.
- Investigation Technology has altered methods used by offenders and types of crimes they engaged in.
- **Criminal behavior**
  - In common fraud scams the criminal gathers the information by phishing and spoofing leading to identity theft . The imposter pretends to be the other person and uses their information without their knowledge to commit theft or fraud. Crimes related to health care; insurances are also performed by hacking .
  - The frauds like auction frauds, non delivery of existent/non-existent merchandize, the seller responds to the victim of the auction fraud and poses to be in a region outside the place indicating emergency leaving.
  - Cyber harassment and defamation especially the cases of paedophiles and stalker use false identities to trap the children and teenagers. Social media sites, chat rooms etc. are a major source for harassment and defamation.

# Few Terms

- **Identity theft :** This cybercrime occurs when a criminal gains access to a user's personal information to steal funds, access confidential information, or participate in tax or health insurance fraud.
- **Access controls :** Measures that establish privileges, determine authorized access, and prevent unauthorized access.
- **Back door :** A way to access an electronic system by bypassing some or all security mechanism.
- **Cookies :** An information pack sent from a website o a web browser ha records a user's activity on that website.
- **Anonymity :** The shielding of one's identity to enable individuals to engage in activities without revealing themselves and/or their actions to others.
- **Anti-digital forensics :** Tools and techniques used to obfuscate cybercrime investigation and digital forensics efforts. Also known as anti forensics.
- **Bulletproof hosting :** A service that enables criminals to utilize servers to commit cybercrime, store illicit content, and protect illicit content from being accessed by law enforcement authorities and/or being taken offline.
- **Clearnet :** Indexed websites that are accessible and available to the public and can be searched using traditional search engines. Also known as Surface Web or Visible Web.

# Few Terms

- **Spam** : Sending of unsolicited emails.
- **Cryptocurrency** : A form of digital currency secured utilizing advanced encryption.
- **Cybermarine** : Posting or otherwise distributing of false information or rumors about an adult or child to damage the victim's social standing, interpersonal relationships, and/or reputation.
- **Dark Web** : The part of the World Wide Web, which is known for its obscure and hidden websites that host illicit activities, goods, and services, and can only be accessed using specialised software. Also known as darknet.
- **Doxing** : Personal information about individuals posted online to cause the individual some form of harm.
- **Smishing** : Phishing via text messaging. Also known as SMS phishing.
- **Hacktivism** : A politically or ideologically motivated cuber attack or hack.
- **Micro laundering** : A form of money-laundering whereby the perpetrators launder a significant amount of money through multiple small transactions.
- **Spyware** : Malware designed to surreptitiously monitor infected systems and collect and relay information back to creator and/or user of the spyware.
- **Traffic data** : Data transmitted over a computer network (or network).
- **Whaling** : Pretending to be higher level executives in a company, lawyers, accountants, and others in positions of authority and trust, in order to trick employees into sending them funds.

# Traditional Problems Associated with Computer Crime, Introduction to Incident Response, Digital Forensics

# Traditional Problems Associated With Computer Crimes

- **Lack of skill** : Individuals seeking a crime have always displayed a remarkable ability to adapt to changing technologies, environments, and lifestyles. This adaptability has often placed law enforcement at a disadvantage, struggling to keep up with criminal innovations. Indeed, the law enforcement community has often failed to recognize the criminal potentiality of emerging technologies until it is almost too late.
- **Perceived Insignificance, Stereotypes, and Incompetence :** investigators and administrators have displayed great unwillingness to pursue computer criminals. A lack of knowledge coupled with general apathy toward cyber criminality has resulted in an atmosphere of indifference. Many stereotype computer criminals as nonthreatening, socially challenged individuals (i.e., nerds or geeks) and fail to see the insidious nature of computer crime; 36.3 percent of officers believe that the investigation of computer crime interferes with their ability to concentrate on “traditional” crime
- **Prosecutorial Reluctance :** many prosecutors, particularly those in local, nonmetropolitan areas, lack sufficient knowledge and experience to effectively prose-cute computer crime. Traditionally, federal and local prosecutors alike did not perceive electronic crime as serious and often granted it the lowest priority.

# Traditional Problems Associated With Computer Crimes

- **Lack of Reporting :**
  - Fortune 500 companies have been electronically compromised to the tune of at least $10 Billion/year
  - Although this number is increasing, early studies indicated that only 17% of such victimizations were reported to the police.
  - Reasons for non-reporting
    - Consumer confidence – must assure consumers that their personal data is safe. (ex., Citibank)
    - Corporate interests – do not want to lose control over their investigation. They wish to control level of access and scope of investigation. They naively believe that if criminal activity is uncovered, they can simply report their findings to the police.
    - Cost/benefit analysis – believe that the low likelihood of enforcement and prosecution vs. the high likelihood of lost consumer confidence is simply not worth it
    - Jurisdictional uncertainty – many companies are unclear as to which agency to report to.

# Traditional Problems Associated With Computer Crimes

- **Lack of Resources**
  - Traditional budget constraints
  - Nature of technology
  - Cost of training
  - Cost of additional personnel
  - Cost of hardware
  - Cost of software
  - Cost of laboratory
  - Inability to compete with private industry

# Introduction to Incident Response

- Incident response is an organized approach to addressing and managing the aftermath of a cyber attack, also known as an IT incident, computer incident or security incident. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.
- An incident response plan helps ensure an orderly, effective response to cyber security incidents, which in turn can help protect  an organization’s data, reputation, and revenue.
- **Incident response plan**
  - An incident response plan is the set of instructions an incident response team follows when an event occurs. If developed correctly, it should include procedures for detecting, responding to and limiting the effects of a security incident.
  - Incident response plans usually include directions on how to respond to potential attack scenarios, including data breaches, denial of service/distributed denial of service attacks, network intrusions, malware outbreaks or insider threats.
  - Without an incident response plan in place, an organization may not detect the attack, or it may not follow proper protocol to contain the threat and recover from it when a breach is detected. A formally documented IR plan helps businesses respond rather than react. When incident response procedures are not developed in advance, the resulting efforts end up making the situation worse, including looking on professional and ultimately being indefensible if lawyers get involved.

# Introduction to Incident Response : Incident response plan


- **Preparation** – Planning in advance how to handle and prevent security incidents
- **Detection and Analysis** – Encompasses everything from monitoring potential attack vectors, to looking for signs of an incident, to prioritization
- **Containment, Eradication, and Recovery** - Developing a containment strategy, identifying and mitigating the hosts and systems under attack, and having a plan for recovery
- **Post-Incident Activity** – Reviewing lessons learned and having a plan for evidence retention

# Introduction to Incident Response : Incident Response Team

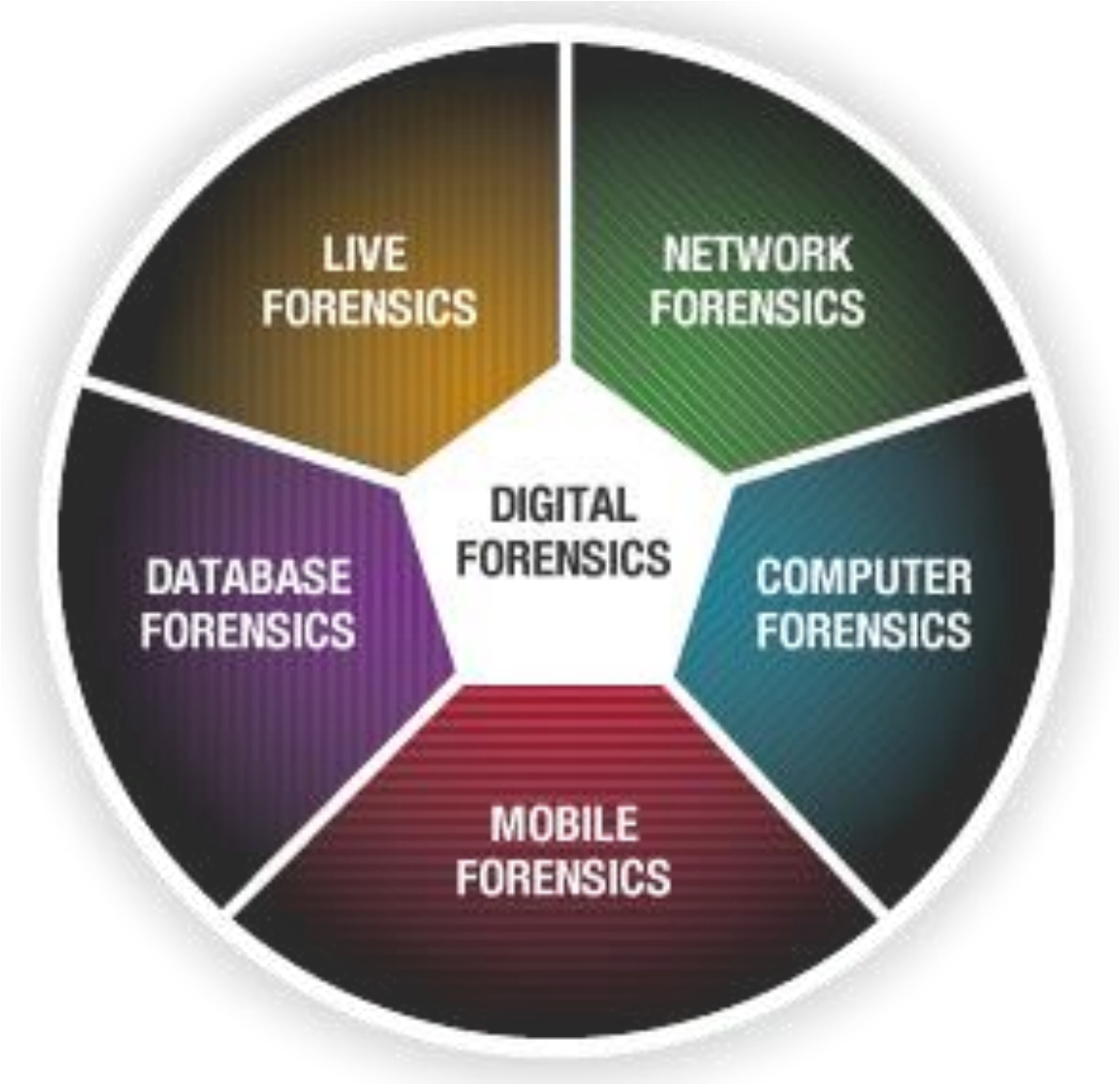
- Ideally, incident response activities are conducted by the organization's ***computer security incident response team (CSIRT),*** a group that has been previously selected to include information security and general IT staff . The incident response team follows the organization's incident response plan (IRP), which is a set of written instructions that outline the organization's response to network events, security incidents and confirmed breaches.
- **An incident response manager**, usually the director of IT, who oversees and prioritizes actions during the detection, analysis and containment of an incident.
- **Security analysts** who support the manager and work directly with the affected network to research the time, location and details of an incident. Triage analysts filter out false positives and keep an eye out for potential intrusions.
- **Forensic analysts** recover key artifacts (residue left behind that can provide clues about an intruder) as well as maintain the integrity of evidence and the investigation.
- **Threat researchers** that provide threat intelligence and context for an incident. They scour the internet and identify information that may have been reported externally. Threat researchers combine this data with an organization's records of previous incidents to build and maintain a database of internal intelligence. If this level of expertise does not exist in house, it can be outsourced.

# Introduction to Incident Response : Why is it Important?

- Any incident that is not properly contained and handled can, escalate into a bigger problem that can ultimately lead to a damaging system, large expense or system collapse. Responding to an incident quickly will help an organization minimize losses, mitigate exploited vulnerabilities, restore services and processes and reduce the risks that future incidents pose.
- Incident response enables an organization to be prepared for the unknown as well as the known and is a reliable method for identifying a security incident immediately when it occurs.

# Digital Forensics

- Digital forensic science is a branch of forensic science that focuses on the recovery and investigation of material found in digital devices related to cybercrime.
- Digital forensics is the process of identifying, preserving, analyzing, and documenting digital evidence. This is done in order to present evidence in a court of law when required



# Digital Forensics : How is Digital Forensics used in an investigation?

- Digital footprint is the information about a person that exists on the system such as, the webpages they have visited, when they were active, and what device they were using.
- By following the digital footprints, the investigator will be able to retrieve the data critical to solving the crime case

# Digital Forensics : Steps of Digital Forensics

- **Identification**
  - First, find the evidence, noting where it is stored.
- **Preservation**
  - Next, isolate, secure, and preserve the data. This includes preventing people from possibly tampering with the evidence.
- **Analysis**
  - Next, reconstruct fragments of data and draw conclusions based on the evidence found.
- **Documentation**
  - Following that, create a record of all the data to recreate the crime scene.
- **Presentation**
  - Lastly, summarize and draw a conclusion

# Digital Forensics : Digital Forensics Tools

- **The Sleuth Kit**
  - It is a collection of Unix- and Windows-based utilities that extract data from computer systems.
  - It is an open–source software.
  - It analyzes disk images created by “dd” and recovers data from them.
  - With this software, professionals can gather data during incident response or from live systems.
- **FTK Imager**
  - It is an acquisition and imaging tool responsible for data preview that allows the user to assess the device in question quickly.
  - The tool can also create forensic images (copies) of the device without damaging the original evidence.
- **Xplico**
  - It is a network forensic analysis tool (NFAT) that helps in reconstructing the data acquired using other packet sniffing tools like Wireshark.
  - It is free and open-source software that uses Port Independent Protocol Identification (PIPI) to recognize network protocols.
  - The tool is built on four key components: Decoder Manager, IP Decoder, Data Manipulators, and Visualization System.

# Cyber Crimes

**Realms of the Cyber world, Recognizing and Defining Computer Crime, Contemporary Crimes, Contaminants and Destruction of Data**

# Realms of the Cyber world : Cyberspace

- Two decades ago, the term cyberspace seemed right out of a science fiction movie.
- In the second decade of the twenty-first century, cyberspace is probably the place where most of us spend a major part of our lives. It has become an inseparable element of our existence. In this article, we will look at what form of cyberspace and the reasons why laws are important to ensure cyber security.
- **What is Cyberspace?**
  - We have all seen that technology is a great leveler.
  - Using technology, we created machine-clones – computers, which are high-speed data processing devices.
  - They can also manipulate electrical, magnetic, and optical impulses to perform complex arithmetic, memory, and logical functions. The power of one computer is the power of all connected computers termed as a network-of-network or the internet.
  - Cyberspace is the dynamic and virtual space that such networks of machine-clones create. In other words, cyberspace is the web of consumer electronics, computers, and communications network which interconnect the world.

# Realms of the Cyber world : Cyberspace : History of Cyberspace

- In 1984, Wiliam Gibson published a science fiction book – Necromancer, which describes an online world of computers and elements of the society who use these computers. The word cyberspace first appeared in this book.
- In the book, a hacker of databases stole data for a fee.
- The author portrayed cyberspace as a three-dimensional virtual landscape. Also, a network of computers creates this space.
- According to him, cyberspace looked like a physical space but was a computer-generated construction. Also, it represented abstract data.
- The book caught the imagination of many writers and in 1986, major English language dictionaries introduced the word ‘cyberspace’. According to the New Oxford Dictionary of English, ‘Cyberspace’ is the notional environment in which people communicate over computer networks.
- Since cyberspace is a virtual space, it has no boundaries, mass, or gravity. It simply represents the interconnected space between computers, systems, and other networks.
- It exists in the form of bits and bytes – zeroes and ones (0’s and 1’s). In fact, the entire cyberspace is a dynamic environment of 0’s and 1’s which changes every second. These are simply electronic impulses. Also, it is an imaginary location where the words of two parties meet in conversation.

# Realms of the Cyber world : Cyberspace : Cyberspace vs. Physical World

Firstly, cyberspace is a digital medium and not a physical space. It is an interactive world and is not a copy of the physical world. Here are some differences between cyberspace and the physical world:

| Physical World | Cyberspace |
| --- | --- |
| Static, well-defined, and incremental | Dynamic, undefined, and exponential |
| Has fixed contours | Is as vast as the human imagination and has no fixed shape |

In a human brain, there are countless neurons which create a spectre of life. Similarly, the cyberspace represents millions of computers creating a spectre of digital life. Therefore, cyberspace is a natural extension of the physical world into an infinite world.

# Recognizing and Defining Computer Crime

Covered in previous slides

# Contemporary Crimes

- Crime can also be defined as “violation of prevalent group, including conduct”.
- Contemporary means existing at the same time or of the present time period.
- ***Contemporary crime*** is a modern or present or future version of crime which is a violation of the person’s privacy and security.
- Crime , security, and criminal justice are highly debated in contemporary societies.

- Few Examples of Contemporary crimes
  - Online impersonation
  - Online solicitation
  - Internet piracy
  - Grooming
  - Cyberbullying
  - Cyber extortion
  - Trafficking passwords

# Contamination and Destruction of data

- A ***contamination*** means ,intentional or accidental alteration of data.
- ***Data destruction*** is “the process of destroying data stored on tapes, hard disks and other forms of electronic media so that it is completely unreadable and cannot be accessed or used for unauthorized purposes.”
- Different forms of data destruction
  - Delete/Reformat
  - Wipe
  - Overwriting data
  - Erasure
  - Degaussing
  - Physical destruction (drill/band/crush/hammer)
  - Electronic shredding
  - Solid state shredding

# Indian IT ACT 2000

# Indian IT ACT 2000

- India is the one of the few country other than USA , Singapore , Malaysia in the world that have Information Technology Act to promote E-commerce and electronic transaction.
- It is based on the “United Nations Commission on International Trade Law” (UNCITRAL model) recommended by general assembly of United Nations by a resolution dated 30 January 1997.
- Information Technology is one of the important law relating to Indian Cyber Laws.
- Information Technology Act 2000 has 13 chapter , 94 sections and 4 schedules.
- It also has set of rules and regulations which apply on any electronic business transaction.
- **Need of Indian IT ACT 2000**
  - The Act provides a legal framework for electronic governance by giving recognition to electronic records and digital signatures.
  - Contains cyber laws
  - Provides legal framework
  - Safeguards E-commerce and E-data interchange.

# Indian IT ACT 2000 : Objectives

- To suitably amend existing laws in India to facilitate e-commerce.
- To provide legal recognition of electronic records and digital signatures.
- To provide legal recognition to the transactions carried out by means of Electronic Data Interchange (EDI) and other means of electronic communication.
- To provide legal recognition to business contacts and creation of rights and obligations through electronic media.
- To establish a regulatory body to supervise the certifying authorities issuing digital signature certificates.
- To create civil and criminal liabilities for contravention of the provisions of the Act and to prevent misuse of the e-business transactions.
- To facilitate e-governance and to encourage the use and acceptance of electronic records and digital signatures in government offices and agencies. This would also make the citizen-government interaction more hassle free.
- To make consequential amendments in the Indian Penal Code, 1860 and the Indian Evidence Act, 1872 to provide for necessary changes in the various provisions which deal with offences relating to documents and paper-based transactions.
- To amend the Banker’s Books Evidence Act, 1891 so as to give legal sanctity for books of accounts maintained in the electronic form by the banks.
- To make law in tune with Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) adopted by the General Assembly of the United Nations.

# Indian IT ACT 2000 : Components

- Legal Recognition to Digital Signatures
  - The authentication to be affected by use of asymmetric crypto system and hash function.
  - Verification of electronic record possible
- Electronic Governance
  - In this components, Section 4 to 8 and Section 10 are included.
- Mode of Attribution, Acknowledgement and Dispatch of Electronic Records
  - In this components, Section 11 to 13 are included.
- Secure Electronic Records
  - In this components, Section 14 to 16 are included.
- Regulation of Certification Authorities
  - In this components, Section 17 to 19, Section 27 & Section 28 are included.
- Digital Certificates
  - In this components, Section  35 to 39 are included.

# Indian IT ACT 2000 : Offences under The Information Technology Act, 2000

**Section** : 65
**Offence**: Tampering with computer source documents
**Penalty**: Imprisonment up to **three** years, or/and with fine up to **₹2,00,000**

**Section** : 66
**Offence**: Hacking with computer system
**Penalty**: Imprisonment up to **three** years, or/and with fine up to **₹5,00,000**

**Section** : 67
**Offence**: Publishing information which is obscene in electronic form.
**Penalty**: Imprisonment up to **five** years, or/and with fine up to **₹10,00,000**

**Section** : 68
**Offence**: Failure/refusal to comply with orders
**Penalty**: Imprisonment up to **three** years, or/and with fine up to **₹2,00,000**

**Section** : 69
**Offence**: Failure/refusal to decrypt data
**Penalty**: Imprisonment up to **seven** years and possible fine.

**Section** : 70
**Offence**: Securing access or attempting to secure access to a protected system
**Penalty**: Imprisonment up to **ten** years, or/and with fine.

**Section** : 71
**Offence**: Misrepresentation
**Penalty**: Imprisonment up to **three** years, or/and with fine up to **₹1,00,000**

# Indian IT ACT 2000 : Major Amendments

- Electronic signatures introduced
- Corporate responsibility introduced in S.43 A
- Legal validity of electronic documents re-emphasized
- New cybercrimes as offences under amended Act
- Section 69 Power of the controller to intercept amended
- Power to block unlawful websites should be exercised with Caution
- Liability of intermediary amended

# Indian IT ACT 2000 : Advantages & Disadvantages

- **Advantages**
  - Make our digital life safe
  - Tackles cyber crimes
  - Protects our privacy
  - Trusted digital payment

- **Disadvantages**
  - Identity theft
  - Cyber war
  - Intellectual property rights
  - Phishing

# THANK YOU