AMRITA VISHWA VIDYAPEETHAM
श्रद्धावान् लभते ज्ञानम्
DEEMED TO BE UNIVERSITY UNDER SECTION 3 OF THE UGC ACT, 1956

19ENG111 TECHNICAL COMMUNICATION

CYBER FORENSICS

Submitted by:

Arjun C Santhosh	CB.EN.U4CYS21010
G R Nitin	CB.EN.U4CYS21017
Gokulachselvan C D	CB.EN.U4CYS21019
Suganth Sarvesh. S	CB.EN.U4CYS21076
Venkata Revan. Nagireddy	CB.EN.U4CYS21083
Yaswanth. Gadamsetti	CB.EN.U4CYS21089

ACKNOWLEDGEMENT

This project has been made possible by the genuine and dedicated efforts of many. We like to thank our technical communication teacher, Mr.Saravana Prabu, and our Cyber Forensics Teacher Mr. Ashok Kumar Mohan for their counsel and support due to which this project was made possible. We also take this opportunity to thank our fellow teammates for their support.

TABLE OF CONTENT

ABSTRACTION

The Internet is growing strongly, as it stands the number of crimes committed against or using computers. As a response to the growth of calculating crime, the field of calculating forensics has surfaced. Computer forensics involves precisely collecting and examining electronic substantiation that not only assesses the damage to a calculating as a result of an electronic attack, but also to recover misplaced information from aforementioned a system to make a miscreant. With the growing significance of calculating security moment and the soberness of cyber-crime, it's important for calculating pros to understand the science that's used in calculating forensics. This paper will bandy the need for calculating forensics to be rehearsed in an effective and legal way. It advances the idea that the competent practice of calculating forensics and mindfulness of applicable laws is essential for moment's associations

CHAPTER - 1

INTRODUCTION TO CYBER FORENSICS

We live in a technologically advanced world where computers are used on daily basis for everything from studying to business wise. Electronic devices such a hard disks and flash drives, as well as cloud storage, are the most common information storage medium. As most the communication and transactions are conducted online, this increases the risk of the cyber-crime. As a result, the attackers online use the online vulnerabilities to steal information. In this scenario if a cyber-crime takes place, we need Cyber forensics.

Cyber forensics is the process of extracting data as evidence for a crime while following proper investigation standards in order to identify the suspect and present the evidence in court. The primary goal of the cyber forensics is to keep track of evidence and documents in order to figure out who committed the digital crime. Cyber forensics is also known as Computer forensics.

Cyber Forensics types:

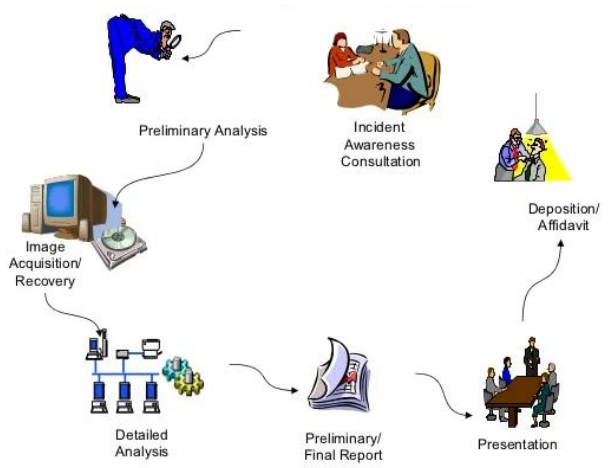
Depending on the field in which digital investigation is required, there are various types of computer forensics. The fields are;

- Network Forensics
- Email Forensics
- Malware Forensics
- Memory Forensics
- Mobile Phone Forensics
- Disk Forensics

What were the methods used by Cyber Forensic Expert?

Cyber Forensics experts follows certain procedures to find the evidence to reach conclusions after proper investigation of matters. The procedures that experts follow is:

- **Identification:** In the attacker's system, forensic experts will determine what evidence is present, where it is sored, and in what format it is stored.
- **Preservation:** They will safely keep the data after identifying it and will not allow other people to use the gadget so that no one can tamper with it.
- **Analysis:** Here, the expert recovers the deleted files, verifies the data, and identifies evidence that the thief attempted to conceal by deleting secret files. To get the ultimate conclusion, this process may require numerous iterations.
- **Documentation:** The documentation record contains all of the recovered and available data that aids in recreating and examining the crime scene.
- **Presentation:** This is the final step in which the analyzed data is presented in front of the court to solve cases.



CHAPTER – 2

CYBER CRIMES

Cybercrime is not an old type of crime in the world**.** It's defined as any criminal activity taking place on or with the aid of a computer or Internet or other technology recognized by the Information Technology Act. Cybercrime is the most prevalent crime that plays a devastating role in the Modern India. Not only the culprits are causing enormous losses to the society and the government but are also suitable to conceal their identity to a great extent. There are number of illegal activities which are committed over the internet by technically professed criminals. Taking a wider interpretation, it can be said that, Cybercrime includes any illegal activity where computer or internet is either a tool or target or both. The term cybercrime may be judicially interpreted in some judgments passed by courts in India; however, it is not defined in any act or statute passed by the Indian Legislature.

Cybercrime includes any crime deals with computers and networks. It includes crimes committed over the Internet. The Internet is principally the network of networks used across for communication and sharing of data. Cybercrime also known as the computer crime is the use of an instrument for illegal ends, such as committing fraud, intellectual property, stealing identities, or violating privacy. With the advancement of internet technologies such as 4G and 5G, the global village is efficiently sharing and communicating vital data over the network. However, some intentionally try to illegally track and extract vital and confidential information for their personal use or financial fulfillment and many more

Classification Of Cyber Crimes:

Cyber-crimes can be classified in to 4 major categories as the following:

1. Cyber-crime against Individual
2. Cyber-crime Against Property
3. Cyber-crime Against Organization
4. Cyber-crime Against Society

Against Individuals:

- **Email Spoofing:** A spoofed email is an email in which the email header is forged in such a way that the email appears to come from one source but is actually from another source was sent.
- **Spamming:** Spamming means sending multiple copies of unsolicited emails or bulk emails such as chain letters.
- **Cyber Defamation:** This occurs when defamation takes place with the help of computers and/or the Internet. E.g., someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information
- **Harassment & Cyber stalking:** Cyber Stalking means that following an individual' activity over internet.

Against Property:

- **Credit Card Fraud:** As the name suggests, this is a fraud that happens by the use of a credit card. This generally happens if someone gets to know the card number or the card gets stolen.
- **Intellectual Property crimes:** These include Software piracy: Illegal copying of programs, distribution of copies of software. Copyright infringement: Using copyrighted material without proper permission. Trademarks violations: Using trademarks and associated rights without permission of the actual holder. Theft of computer source code: Stealing, destroying or misusing the source code of a computer.
- **Internet time theft:** This happens by the usage of the Internet hours by an unauthorized person which is actually paid by another person.

Against Organizations:

- **Unauthorized access of the computer:** Access to the computer / network without permission of the owner. Unauthorized Accessing of Computer: Accessing the computer/network without permission from the owner. It can be of 2 forms:

  a) Changing/deleting data: Unauthorized changing of data.

  b) Computer voyeur: The criminal reads or copies confidential or proprietary information, but the data is neither deleted nor changed.

- **Denial Of Service:** When Internet server is flooded with continuous bogus requests so as to denying legitimate users to use the server or to crash the server.
- **Computer contamination / Virus attack:** A computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of it. Viruses can be file infecting or affecting boot sector of the computer. Worms, unlike viruses do not need the host to attach themselves to.
- **Email Bombing:** Sending large numbers of mails to the individual or company or mail servers thereby ultimately resulting into crashing.
- **Salami Attack:** When negligible amounts are removed & accumulated in to something larger. These attacks are used for the commission of financial crimes
- **Logic Bomb:** It is an event dependent program. Once the designated event occurs, it crashes the computer, releases a virus or some other harmful possibility.
- **Trojan horse:** This is an unauthorized program that works inside an apparently authorized program, thereby disguising what it is actually doing.
- **Data manipulation:** In this type of attack, raw data is altered by a computer just before it is processed, and altered back after processing is complete.

Against Society:

- **Forgery:** Banknotes, revenue stamps, stamp sheets, etc. They can be counterfeited using high-quality computers, scanners and printers.
- **Cyber Terrorism:** Using computer resources to intimidate or coerce people and to carry out terrorist activities.
- **Web Jacking:** Hackers gain access to and control over another's website, even if they change the content of the website to achieve a political goal or to make money.

How to Fight Cybercrime

- Become vigilant when browsing websites.
- Flag and report suspicious emails.
- Never click on unfamiliar links or ads.
- Use a VPN whenever possible.
- Ensure websites are safe before entering credentials.
- Keep antivirus/application systems up to date.
- Use strong passwords with 14+ characters

Criminal behavior on the Internet, or cyber-crime, presents as one of the Major challenges of the future to India and International law enforcement. As ICT become even more pervasive, aspects of electronic crime will feature in all forms of criminal behavior, even those matters currently regarded as more traditional offences. It already features in many international crime involving drug trafficking, people smuggling, terrorism and money laundering. Digital evidence will become more commonplace, even in traditional crimes, and we must be prepared to deal with this new challenge.

CHAPTER – 3

MALWARE FORENSICS

What are Malware Forensics?

The term malware itself is derived from the incorporation of two words – malicious and software which is used to interpret a wide range of software that only functions for the sole purpose of disruption of computer services, information theft or the compromission of user safety. These types of software are specifically designed for malicious intent and hostile intentions. The malware scripting business has evolved to become a multibillion-dollar business as the scripters who create the malware have started to create powerful malware with the intent to cause damage in billions. Such malware is hard to be detected by the system, these cause massive damage due to breach of sensitive information.

The science of discovering, analyzing and investigating the various characteristics and behavior of malware to nab the culprits is called Malware Forensics. Malware forensics are done by academic researchers and industrial research experts for research purposes, while the law enforcement agencies such as National Cybercrime Threat Analytics Unit (TAU), National Cybercrime Forensic Laboratory Ecosystem do it for crime-related malware forensics.

Types of Malware:

- **Viruses:** The most common type of malware that almost every user is acquainted with. It is a type of software which upon being triggered infect the system and spreads to other computers via vectors. They are usually destructive in nature and cause harm to the computer processes. Some of these viruses are covert and hard to detect as they modify themselves when they replicate in order to avoid string detection.
- **Worms:** A piece of self-replicating software that spread across networks and consume a large amount of bandwidth. This type of malware doesn't need any container files. Some worms might even have payloads that are designed to manipulate data on a computer system. Usually worms in fact through mass emails with infected attachments that contain the worm.

- **Trojan:** Malicious software that disguises itself and deceives the user. The name itself is derived from an ancient Trojan story, which follows the Greeks constructing a large wooden horse that secretly contained the Greek soldiers through which they entered Troy. Trojans are often used as social engineering tools as purely relies on the user to install them on their system. Some common types of Trojans are:

-->Remote Access Trojans - It is often called a RAT. A dangerous Trojan that installs backdoors on a target system for the hacker to operate it remotely. This type of trojan is often used by hackers for information theft.

-->Data Destruction Trojans - The Trojan that is specifically designed to destroy the data on the computer system.

-->Software Disabler Trojans - The trojan when once installed on a target system, kills a particular service or programs.

Trojans are often considered to be the most dangerous of all malware as these is used as vectors to spread other malware.

- **Spyware:** A type of malware that is designed specifically to spy on the users of the infected system and log their activities. This malware collection logs the user information such as browsing histories, keystrokes and user credentials.

- **Adware:** A Completely different type of malware that is used as a revenue-generating source. It is generally used by some companies as an income source. A common example of this malware is pop-up ads.
- **Ransomware:** The advanced type of malware encrypts and blocks access to a computer system and threatens the user to expose or wipe the data in exchange for a ransom. Once the ransom has met the hacker since the decryption key to the user, but there is no guarantee that the hacker will send the decryption key.

ANALYSIS OF MALWARE:

Malware analysis is a process that determines what the acquired malware's actions are. It is an important process to get the internal working of the malware code which helps in identifying the malware's type, actions, properties, etc., and to prevent these attacks in the future. The important steps of malware analysis are given below:

- **Hashing** – All malware suspected must be hashed prior to analysis. The conversion of character strings into a shorter value is called as hashing. This helps in easily searching the database due its shorter value, it is also an indicator of the integrity of the data. It is a standard practice of all cyber forensic investigations.
- **Antivirus Check** – Before examining the suspected malware, it is a smart strategy to check the infected files with a malware database by using antivirus tools. This software compares the files with its database malware file signatures and if the suspected malware is already in the database, the search results are positive and the investigators directly proceed to the conclusion or diagnosis.
- **String Analysis** – A string is a sequence of characters in a program. If a program is executed, the copied or printed message or files are usually contained within the strings. The analysis of these strings helps forensic experts collect evidence connected to the malware. By analyzing the strings, forensic experts may even get clues from the language used to write the malware script and find its country of origin.
- **Detection of Obfuscation and Packed Archives** – If initial analysis of the malware proves to be non-sufficient, forensic experts proceed to disassemble the malware binary. The disassembled malware binary code is translated into a valid x86 assembly language. As malware binary is usually written in high-level languages like C and C++, which are compiled using compilers to convert the source code into x86 binary code. This makes the forensic experts easily read the source code. If this provides no conclusive results the forensic experts proceed to dynamic analysis of the malware.
- **Dynamic Analysis** – A very advanced method of analysis that involves, executing the malware in a controlled environment and studying its behavior. This allows the forensic experts to find out the functioning of the malware. This technique is said to be the riskiest analysis, as the forensic experts have to run the unknown malware sample in their system. The technology used for the dynamic analysis is called sandboxing which helps the investigators to execute out malware analysis by executing it and studying its behavior in real-time.

Some Tools used for Malware Analysis:

- **Cuckoo Sandbox:** Popular and efficient sandboxing software that is used in malware analysis, that is used to simulate Windows, Mac, Linux and Android environments.
- **Yara Rules:** A powerful tool that helps forensic experts to identify malware samples.
- **REMnux:** REMnux is a free Linux toolkit that is used to analyze and reverse engineer the given sample of malware.
- **Virus Total:** A free online database utility that is used to scan the uploaded against various online malware databases.

The gradual rise of malware threat has now surged to a new height with global attacks have increased significantly. As hackers find new modes and platforms to siphon money through illegal means. These can be prevented after analyzing their crimes and diagnosing them to prevent future crimes of such manner.

CHAPTER – 4

NETWORK FORENSICS

Big companies in the IT industry are concerned about their data and security as they are targeted by hackers every day. The frequency of attacks has gone up, which is a matter of concern for not just the companies but also their customers and clients because from payments to emails, e-commerce to dating. All the data is being stored by companies making the hackers go after them more frequently. So, to provide proper security in place, to expose vulnerabilities in the system here comes the hero "**Network forensics**".

Network forensics is a branch of digital forensics that focuses on surveillance, analysis, recording, and interpreting real-time network traffic. It deals with volatile and dynamic data like firewalls, IDS.

In the recent advances in Internet technologies, the aspects of our lives are being shifted to online and database systems.

Techniques used for this Forensics:

We need a sophisticated analysis tool to secure them and watch them with proper concern. The network forensics are quite good at this surveillance stuff like,

- Analyzing computer systems belonging to defendants or litigants.
- Recovering data in the event of a hardware or software failure.
- Gaining information about how computer systems work to debug them, optimize their performance, or reverse-engineering them.
- Collecting and analyzing live data packets to detect and potentially prevent a malicious attack.

- Learn more about zero-day attacks, particularly through the use of honey pots and honeynets.

This list above only just scratches the surface of the rick assessment that a network forensic should go to recover data. TCP/IP/UPD of protocols carry most of today's online data and transfer it. The hackers can manipulate these protocols to spoof addresses or embed malware.

As we know the network forensics can do real-time recovery so, this can be analyzed and understood. But recently the work has stepped up that is to focus on live packet capture, because these live packets are not stored upon arrival leaving no trace on the computer's hardware. They can exploit volatile memory like encryption keys.

If an attacker managed to delete or steal data from a compromised host, network-based evidence might be the only material to work on for forensic experts.

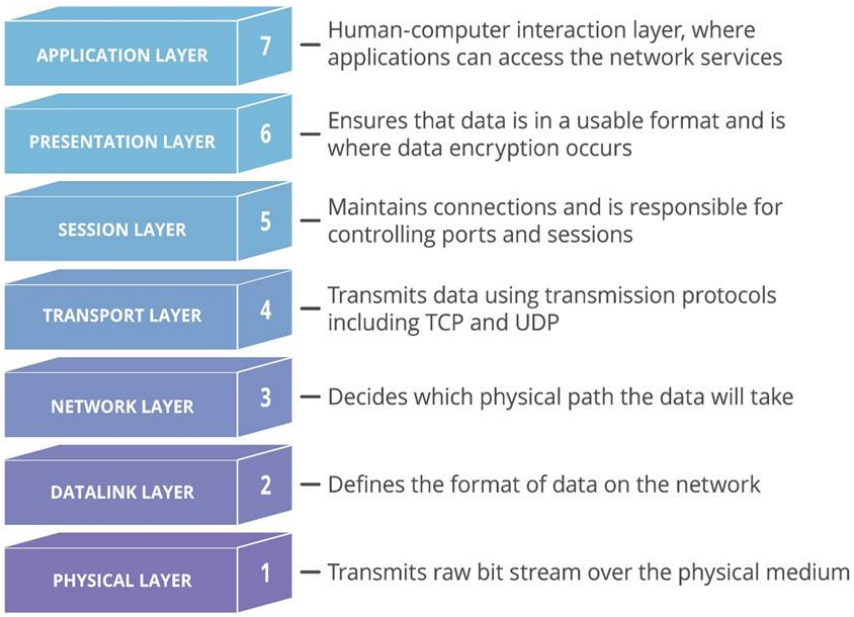
Tools used for Network Forensics:

The network forensic will retrieve both traffic and ports used to access the network. They use a lot of tools to investigate it. Current examples are Wireshark, TCPDump, NetScanToolsProtoolKit, ccze, Lnav, Multitail, CapAnalysis, Driftnet, Ettercup, Nmap, Tshark, Xplico, Kismet, Aircrack-ng.

These tools include network gathering and security testing; IP/MAC ranges and locations; TCP/UDP ports and DHCP analysis; SMTP and SNMP activities; live packet viewer.

Forensic Foot Prints: The network forensic has to scour through the internet to obtain tracks of attackers. The network travels via packets which contains data, destination and source information. Sometimes the attackers might leave behind some traces like logging information. When an attacker passes through a network the device or ISP gets digitally logged. The forensic can examine the log information and extract useful information of attacker. The timeline when that log created can give the time of attack.

Some interesting attacks – ICMP, ICMP Sweep, Traceroute, Inverse mapping, ICMP Smurf.



Network forensic Artifacts are those artifacts related to network and communication. These provide evidence or insights of network. It can be generated from Dynamic Host Configuration Protocol (DHCP) servers, Domain Name System (DNS) servers, Web Proxy Servers, Intrusion Detection Systems (IDS), Intrusion Prevention System (IPS), and firewalls.

1. Dynamic Host Configuration Protocol (DHCP): Before sending any data on the network, the computer must contact the DHCP server to assign it an IP address, the forensic investigator can know when a computer joined the network, when it was present on the network, and the time frame when it left the network.

2. Network Time Protocol (NTP): It provides accurate time services on the network and allows for consistency among computers on a network.

3. Domain Name Server (DNS): DNS request/response traffic provides valuable information about when communication with a particular host began since the first step, it shows IP address.

4. Web Proxy logs: They capture web traffic requests and response. They also have cache copies of resources retrieved from the web servers, which include copies of files, like malware, that was retrieved from a web server.

5. Firewalls: Firewall perform packet inspection and make decisions on what traffic should be forwarded, logged, and blocked. these logs can be used by the forensic investigator for analysis.

6. Intrusion Detection System (IDS): IDS monitors the network interface and examines network traffic and compares it against the patterns of known malicious traffic to identify suspicious network traffic. If IDS finds anything suspicious, it logs the traffic in an alert file.

From routers, we can extract logs, ping requests, and information about connected devices; from firewalls, we can get dropped and denied IPs and logs; and from emails, we can get headers and email addresses that can later be used by forensics investigators for further analysis.

CHAPTER – 5

NEED OF CYBER FORENSICS

Cyber forensics is becoming increasingly important as the world is becoming more digitalized so does the number of cybercrimes ease Cyber-forensic is needed where the prevention fails

As we all use digital device day to day life amount of data that is accumulated in them is quite large. The average person never sees much of the information modern devices collect for example a smart refrigerator can contain its user's data regarding when does user eat at what time does he wake up to have a drink etc.

However, information's like this can prove critical in solving a legal matter or a crime, and a Cyber forensics often plays a role in identifying and preserving that information.

In cases where data is either stolen modified or deleted cyber forensics can identify who has stolen it to where all has it been distributed, if the data has been modified or deleted it is possible for an expert to recover the original data.

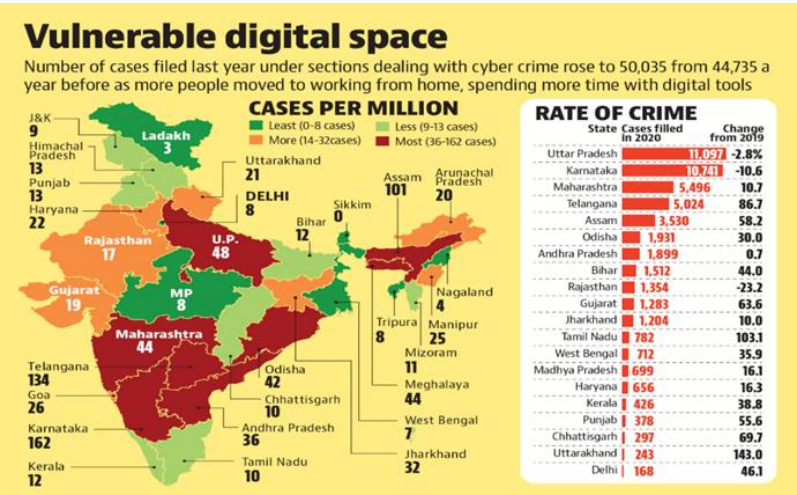
CHAPTER - 6

CYBER LAWS

Cyber Laws are the laws that govern the virtual world of the internet called "Cyberspace". Cyberspace is a wide area including computers, networks, software, data storage devices (like HDD, SSD), internet, websites, emails, and electronic devices like cellphones, ATMs, etc. These are the laws that have been approved by the government and must be obeyed by all persons in that territory.

Violation of these could lead to strict government action such as imprisonment or a fine or an order to pay compensation.

Need for Cyber Laws in India:



In today's highly digitalized world, almost everyone is affected by cyber law. For example:

- Most people are using cell phones, email, and social media for communication.
- Consumers are increasingly using credit cards for shopping.
- Almost all transactions in shares are done in Demat form.
- Almost all companies depend upon their computer networks and store their data in electronic form.
- Government forms including income tax returns, company law forms, etc. are now filled in electronic form.

- Digital signatures and e-contracts are fast replacing conventional methods of transacting business.
- Even in "non-cyber-crime" cases, important evidence is found in computers/cellphones, for example: in cases of divorce, murder, kidnapping, tax evasion, organized crime, terrorist operations, etc.
- Cybercrime cases such as online banking frauds, online share trading fraud, source code theft, credit card fraud, tax evasion, virus attacks, cyber sabotage, phishing attacks, email hijacking, denial of service, hacking, pornography, etc. are becoming common.
- Cybercrime in India resulted in 29.9 million people being victim to it involving direct financial losses of up to $4 billion and $3.6 billion spent for resolving these crimes.

All these and other varied considerations created a conducive atmosphere for the need for enacting cyber laws in India.

Evolution of Cyber laws in India:

- The Information Technology Act is an outcome of the resolution dated on 30th January 1997 of the General Assembly of the United Nations which adopted the Model Law on Electronic commerce.
- This made India take its first step in framing Cyber Law.
- The Department of Electronics (DoE) in July 1998 drafted the IT bill. However, it could only be introduced in the House on December 16, 1999, but the bill was dropped by the IT Ministry in its final draft.
- Finally, The Union Cabinet approved the bill on May 13, 2000, and on May 17, 2000, both the houses of the Indian Parliament passed the Information Technology Bill.
- The Bill received the assent of the President on 9th June 2000 and came to be known as the **Information Technology Act, 2000.** The Act came into force on 17th October 2000.

- As the technology developed further and new methods of committing a crime using Internet & computers were found, fixing the loopholes of IT Act 2000 was demanded.
- This led to the formation of the Information Technology (Amendment) Act, 2008 which was made effective on 27 October 2009.
- This Information Technology (Amendment) Act, 2008 is still in effect.

Cyber laws in India:

-> Intellectual property law: Intellectual property (IP) is referred to a brand, invention, design, or other creations, which a person or a business has legal rights over them. Almost all businesses own some Intellectual property which could be their business asset. The laws which deal with Intellectual property are called Intellectual property laws.

Some common types of Intellectual property laws are:

Copyright law: This law protects written or published works such as books, songs, films, web content that is owned by the creator.

Patents law: This law protects commercial inventions, for example, a new business product.

Designs law: This law protects designs, such as drawings or computer models that are owned by the creator.

Trademark law: This law protects signs, symbols, logos, words that distinguish your products and services from your competitors.

Some of the rules and laws governing Intellectual Property Rights in India are as follows:

1) The Copyright Act, 1957, The Copyright Rules, 1958, and International Copyright Order, 1999.

2) The Patents Act, 1970 and The Patents Rules, 2003.

3) The Trade Marks Act, 1999 and The Trade Marks Rules, 2002.

4) The Designs Act, 2000 and The Designs Rules, 2001.

-> The Information Technology Act, 2000:

- The Information Technology Act, 2000 (IT Act), came into force on 17 October 2000.
- This Information Technology Act, 2000 consisted of 94 sections segregated into 13 chapters.
- The main purpose of this Act is to provide legal recognition to electronic commerce and to facilitate the filing of electronic records within the Government.

Some important sections of the Information Technology Act, 2000 are:

OFFENCE	SECTION
Tampering with Computer source documents	Sec.43
Hacking with Computer systems, Data alteration	Sec.66
Sending offensive messages through communication services	Sec.66A
Retains any stolen computer resource or communication device dishonestly	Sec.66B
Identity theft	Sec.66C
Cheating by personation using computer's resources	Sec.66D
Publishing obscene images	Sec.66E
Cyber terrorism	Sec.66F
Transmitting or publishing obscene materials in electronic form	Sec.67
Publishes or transmits sexually explicit material	Sec.67A
Abusing children online	Sec.67B
Preservation of information by intermediary	Sec.67C
Un-authorized access to protected system	Sec.70
Penalty for misrepresentation	Sec.71
Breach of confidentiality and privacy	Sec.72
Publishing false digital signature certificates	Sec.73 & 74
Sending threatening messages by email	Sec.503 IPC
Sending defamatory messages by email	Sec.499 IPC
Forgery of electronic records	Sec.463 IPC
Cyber frauds	Sec.420 IPC
Email spoofing	Sec.463 IPC
Web-Jacking	Sec.383 IPC
E-mail Abuse	Sec.500 IPC

-> The Information Technology Amendment Act, 2008:

- The Information Technology Amendment Act, 2008 has been passed by the parliament on 23rd December 2008.
- It received the assent of the President on 5th February 2009.
- It has been notified on October 27, 2009.
- It is a new version of the IT Act, 2000.
- It provides additional focus on Information security.
- This Information Technology Amendment Act, 2008 consisted of 124 sections segregated into 14 chapters.

The following important sections have been substituted and inserted by the IT Amendment Act, 2008:

CHANGES/INCLUSION	SECTION
Compensation for failure to protect data	Sec.43A
Powers to issue directions for interception of any information through computer resource	Sec.69
Power to issue directions for blocking public access of information through computer resource	Sec.69A
Power to monitor and collect traffic information through computer resource for cyber security	Sec.69B
Punishment for disclosure of information in breach of lawful contract	Sec.72A
Exemption from liability of intermediary in certain cases	Sec.79
Modes or methods for encryption	Sec.84A
Punishment for abetment of offences	Sec.84B
Punishment for attempt to commit offences	Sec.84C

Aftermath of IT Acts in India:

- Digital signatures are given legal validity and sanction in this act.
- It allows Government to issue notifications through the internet.
- It allows corporate companies for issuing Digital signatures or certificates in the business of being Certifying Authorities.
- Organizations can now, carry out e-commerce using the legal infrastructure given by this act.
- It gives authority to the companies to file any application or any other document with any office, authority, body, or agency owned or controlled by the suitable Government in digital format.

CHAPTER – 7

CONCLUSION

Why is Cyber Forensic Important:

In today's technology driven generation, the importance of cyber forensics is immense. Technology combined with forensics, paves the way for quicker investigations and accurate results. Below are the points depicting the importance of cyber forensics:

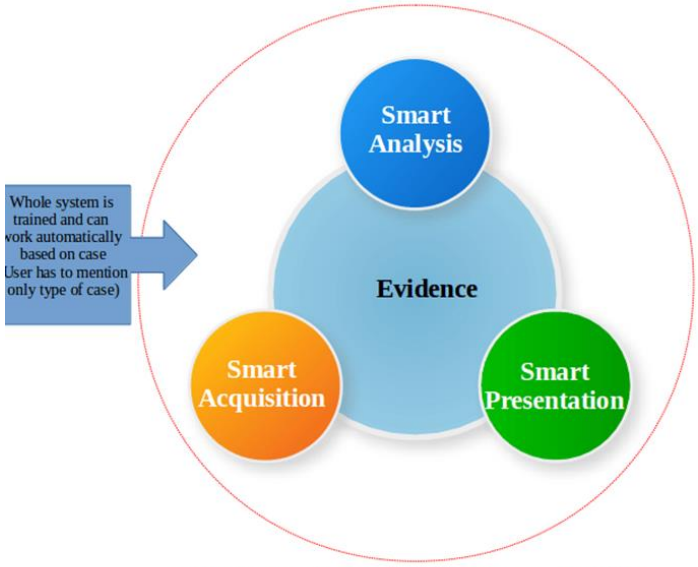
- Cyber forensics helps in collecting important digital evidence to trace the criminal.
- Electronic equipment stores massive amounts of data that a normal person fails to see. For example: in a smart house, for every word we speak, actions performed by smart devices, collect huge data which is crucial in cyber forensics.
- It is also helpful for innocent people to prove their innocence via the evidence collected online.
- It is not only used to solve digital crimes but also used to solve real-world crimes like theft cases, murder, etc.
- Businesses are equally benefitted from cyber forensics in tracking system breaches and finding the attackers.

Future of cyber forensics:

The ever-evolving nature of technology will inevitably create new tools that will be useful for forensic investigations.

Improvement of already existing tools such that data analyzing will be faster and simplified.

One of the major developments will use of Artificial intelligence in forensics as AI has the potential to multitask and give accurate and precise response.



Proposed AI based Digital Forensic Framework

BIBLIOGRAPHY:

→ Cyber Forensics | How it Works | Skills & advantages| Career and Future (educba.com)
→ An Introduction to Computer Forensics - Infosec Resources (infosecinstitute.com)
→ https://www.bbau.ac.in/dept/Law/TM/1.pdf
→ (PDF) A Study on the Cyber - Crime and Cyber Criminals: A Global Problem (researchgate.net)
→ https://www.pandasecurity.com/en/mediacenter/panda-security/types-of-cybercrime/#:~:text=There%20are%20three%20major%20categories,%3A%20individual%2C%20property%20and%20government.&text=A%20crime%20against%20the%20government,military%20websites%20or%20distributing%20propaganda.
→ https://www.lawyersclubindia.com/articles/classification-of-cybercrimes--1484.asp
→ http://www.cyberlawclinic.org/
→ https://www.meity.gov.in/content/cyber-laws
→ https://taxguru.in/finance/overview-cyber-laws-india.html
→ A brief study on Cyber Crime and Cyber Laws of India- Animesh Sarmah, Roshmi Sarmah, Amlan Jyoti Baruah.
→ IPR & Cyberspace – Indian Perspective-Rohas Nagpal.