UNIT-IV

Cyber-crime and the legal landscape around the world:

Cybercrime law includes laws related to computer crimes, internet crimes, information crimes, communications crimes, and technology crimes. While the internet and the digital economy represent a significant opportunity, they're also an enabler for criminal activity. Cybercrime laws are laws that create the offences and penalties for cybercrimes.

Cybercrime describes:

- Crimes directed at computers, data or information communications technologies (ICTs), and
- Crimes committed by people using computers or ICT.

Cybercrime is a global problem, which requires a coordinated international response.

In Simple way we can say that cyber-crime is unlawful acts wherein the computer is either a tool or a target or both. Cybercrimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

We can categorize Cyber-crimes in two ways

- The Computer as a Target:-using a computer to attack other computers. E.g. Hacking, Virus/Worm attacks, DOS attack etc.
- The computer as a weapon:-using a computer to commit real world crimes. E.g. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc.

Cyber law (also referred to as cyber law) is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace", i.e. the Internet. It is less a distinct fielding of law in the way that property or contract is as it is an intersection of many legal fields, including intellectual property, privacy, freedom of expression, and jurisdiction. In essence, cyber law is an attempt to integrate the challenges presented by human activity on the Internet with legacy system of laws applicable to the physical world.

Cyber Law in INDIA

When Internet was developed, the founding fathers of Internet hardly had any inclination that Internet could transform itself into an all pervading revolution which could be misused for criminal activities and which required regulation. Today, there are many disturbing things happening in cyberspace. Due to the anonymous nature of the Internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. Hence the need for Cyber laws in India.

What is the importance of Cyber law?

Cyber law is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. Initially it may seem that Cyber laws are a very technical field and that it does not have any bearing to most activities in Cyberspace. But the actual truth is that nothing could be further than the truth. Whether we realize it or not, every action and every reaction in Cyberspace has some legal and Cyber legal perspectives.

Does Cyber law concern me?

Yes, Cyber law does concern you. As the nature of Internet is changing and this new medium is being seen as the ultimate medium ever evolved in human history, every activity of yours in Cyberspace can and will have a Cyber legal perspective. From the time you register your Domain Name, to the time you set up your web site, to the time you promote your website, to the time when you send and receive emails, to the time you conduct electronic commerce transactions on the said site, at every point of time, there are various Cyber law issues involved. You may not be bothered about these issues today because you may feel that they are very distant from you and that they do not have an impact on your Cyber activities. But sooner or later, you will have to tighten your belts and take note of Cyber law for your own benefit.

Advantages of Cyber Laws

The IT Act 2000 attempts to change out-dated laws and provides ways to deal with cyber-crimes. We need such laws so that people can perform purchase transactions over the Net through credit cards without fear of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.

In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format. The Act has also proposed a legal framework for the authentication and origin of electronic records / communications through digital signature.

- From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects. Firstly, the implications of these provisions for the e-businesses would be that email would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law.
- Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act.
- Digital signatures have been given legal validity and sanction in the Act.
- The Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates.
- The Act now allows Government to issue notification on the web thus heralding e-governance.
- The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.
- The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the Government at a later date.

- Under the IT Act, 2000, it shall now be possible for corporates to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages, not exceeding Rs. 1 crore.

Challenges to INDIAN law and Cybercrime Scenario in INDIA

With India carving a niche for itself in the IT sector, dependence on technology is also increasing. However, there are two things that set India aside from the players in the big leagues, like the United States and China, and that is design and density. With Indians using the internet for all their needs, ranging from shopping to banking, studying to storing data, cyber crimes have also increased in proportion to usage.

Some of the Cyber security challenges in India are as follows:

1. Lack of uniformity in devices used for internet access – With varying income groups in India, not everyone can afford expensive phones. In the US, Apple has over 44% market share. However, in India the iPhones with their higher security norms are used by less than 1% of mobile users. The widening gap between the security offered by the high-end iPhone and lower cost mobiles make it almost impossible for legal and technical standards to be set for data protection by the regulators.

2. Lack of national level architecture for Cyber security – Critical infrastructure is owned by private sector, and the armed forces have their own fire fighting agencies. However there is no national security architecture that unifies the efforts of all these agencies to be able to assess the nature of any threat and tackle them effectively. The Prime Minister's Office has created a position towards this cause but there is a long way to go before India has the necessary structure in place.

3. Lack of separation – Unlike countries or states, in cyberspace there are no boundaries, thus making the armed forces, digital assets of ONGC, banking functions, etc. vulnerable to cyber-attacks from anywhere. This could result in security breaches at a national level, causing loss of money, property or lives. To respond to possible threats on the country's most precious resources, there is a need for a technically equipped multi-agency organization that can base its decisions on policy inputs and a sound strategy.

4. Lack of awareness – As there is no National regulatory policy in place for cyber security there is a lack of awareness at both company level as well as individual level. Domestic netizens can protect and be protected from the cyber-attacks only if there is a guided and supervised legal framework.

Information Technology Act

The Information Technology Act, 2000 also Known as an IT Act is an act proposed by the Indian Parliament reported on 17th October 2000. This Information Technology Act is based on the United

Nations Model law on Electronic Commerce 1996 (UNCITRAL Model) which was suggested by the General Assembly of United Nations by a resolution dated on 30th January, 1997. It is the most important law in India dealing with Cybercrime and E-Commerce.

The main objective of this act is to carry lawful and trustworthy electronic, digital and online transactions and alleviate or reduce cybercrimes. The IT Act has 13 chapters and 90 sections. The last four sections that starts from 'section 91 – section 94', deals with the revisions to the Indian Penal Code 1860.

The IT Act, 2000 has two schedules:

- First Schedule –
  Deals with documents to which the Act shall not apply.
- Second Schedule –
  Deals with electronic signature or electronic authentication method.

The offences and the punishments in IT Act 2000: 

The offences and the punishments that falls under the IT Act, 2000 are as follows:-

1. Tampering with the computer source documents.
2. Directions of Controller to a subscriber to extend facilities to decrypt information.
3. Publishing of information which is obscene in electronic form.
4. Penalty for breach of confidentiality and privacy.
5. Hacking for malicious purposes.
6. Penalty for publishing Digital Signature Certificate false in certain particulars.
7. Penalty for misrepresentation.
8. Confiscation.
9. Power to investigate offences.
10. Protected System.
11. Penalties for confiscation not to interfere with other punishments.
12. Act to apply for offence or contravention committed outside India.
13. Publication for fraud purposes.
14. Power of Controller to give directions.

Sections and Punishments under Information Technology Act, 2000 are as follows :

SECTION	PUNISHMENT
Section 43	This section of IT Act, 2000 states that any act of destroying, altering or stealing computer system/network or deleting data with malicious intentions without authorization from owner of the computer is liable for the payment to be made to owner as compensation for damages.
Section 43A	This section of IT Act, 2000 states that any corporate body dealing with sensitive information that fails to implement reasonable security practices causing loss of other person will also liable as convict for compensation to the affected party.

Section 66	Hacking of a Computer System with malicious intentions like fraud will be punished with 3 years imprisonment or the fine of Rs.5,00,000 or both.
Section 66 B, C, D	Fraud or dishonesty using or transmitting information or identity theft is punishable with 3 years imprisonment or Rs. 1,00,000 fine or both.
Section 66 E	This Section is for Violation of privacy by transmitting image or private area is punishable with 3 years imprisonment or 2,00,000 fine or both.
Section 66 F	This Section is on Cyber Terrorism affecting unity, integrity, security, sovereignty of India through digital medium is liable for life imprisonment.
Section 67	This section states publishing obscene information or pornography or transmission of obscene content in public is liable for imprisonment up to 5 years or fine of Rs. 10,00,000 or both.

Introduction of Cyber Forensics

Cyber forensics is a process of extracting data as proof for a crime (that involves electronic devices) while following proper investigation rules to nab the culprit by presenting the evidence to the court. Cyber forensics is also known as computer forensics. The main aim of cyber forensics is to maintain the thread of evidence and documentation to find out who did the crime digitally. Cyber forensics can do the following:

- It can recover deleted files, chat logs, emails, etc
- It can also get deleted SMS, Phone calls.
- It can get recorded audio of phone conversations.
- It can determine which user used which system and for how much time.
- It can identify which user ran which program.

Why is cyber forensics important?

In today's technology driven generation, the importance of cyber forensics is immense. Technology combined with forensic 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.

The Process Involved in Cyber Forensics

1. Obtaining a digital copy of the system that is being or is required to be inspected.
2. Authenticating and verifying the reproduction.
3. Recovering deleted files (using Autopsy Tool).
4. Using keywords to find the information you need.
5. Establishing a technical report.

How did Cyber Forensics Experts work?

Cyber forensics is a field that follows certain procedures to find the evidence to reach conclusions after proper investigation of matters. The procedures that cyber forensic experts follow are:

- **Identification:** The first step of cyber forensics experts is to identify what evidence is present, where it is stored, and in which format it is stored.
- **Preservation:** After identifying the data the next step is to safely preserve the data and not allow other people to use that device so that no one can tamper data.
- **Analysis:** After getting the data, the next step is to analyse the data or system. Here the expert recovers the deleted files and verifies the recovered data and finds the evidence that the criminal tried to erase by deleting secret files. This process might take several iterations to reach the final conclusion.
- **Documentation:** Now after analysing data a record is created. This record contains all the recovered and available (not deleted) data which helps in recreating the crime scene and reviewing it.
- **Presentation:** This is the final step in which the analysed data is presented in front of the court to solve cases.

Types of computer forensics

There are multiple types of computer forensics depending on the field in which digital investigation is needed. The fields are:

- **Network forensics:** This involves monitoring and analysing the network traffic to and from the criminal's network. The tools used here are network intrusion detection systems and other automated tools.
- **Email forensics:** In this type of forensics, the experts check the email of the criminal and recover deleted email threads to extract out crucial information related to the case.
- **Malware forensics:** This branch of forensics involves hacking related crimes. Here, the forensics expert examines the malware, Trojans to identify the hacker involved behind this.

- **Memory forensics:** This branch of forensics deals with collecting data from the memory (like cache, RAM, etc.) in raw and then retrieve information from that data.
- **Mobile Phone forensics:** This branch of forensics generally deals with mobile phones. They examine and analyse data from the mobile phone.
- **Database forensics:** This branch of forensics examines and analyses the data from databases and their related metadata.
- **Disk forensics:** This branch of forensics extracts data from storage media by searching modified, active, or deleted files.

Techniques that cyber forensic investigators use

Cyber forensic investigators use various techniques and tools to examine the data and some of the commonly used techniques are:

- **Reverse steganography:** Steganography is a method of hiding important data inside the digital file, image, etc. So, cyber forensic experts do reverse steganography to analyze the data and find a relation with the case.
- **Stochastic forensics:** In Stochastic forensics, the experts analyze and reconstruct digital activity without using digital artifacts. Here, artifacts mean unintended alterations of data that occur from digital processes.
- **Cross-drive analysis:** In this process, the information found on multiple computer drives is correlated and cross-references to analyze and preserve information that is relevant to the investigation.
- **Live analysis:** In this technique, the computer of criminals is analyzed from within the OS in running mode. It aims at the volatile data of RAM to get some valuable information.
- **Deleted file recovery:** This includes searching for memory to find fragments of a partially deleted file in order to recover it for evidence purposes.

Advantages

- Cyber forensics ensures the integrity of the computer.
- Through cyber forensics, many people, companies, etc. get to know about such crimes, thus taking proper measures to avoid them.
- Cyber forensics finds evidence from digital devices and then presents them in court, which can lead to the punishment of the culprit.
- They efficiently track down the culprit anywhere in the world.
- They help people or organizations to protect their money and time.
- The relevant data can be made trending and be used in making the public aware of it.

Historical background of cyber forensics

Until the late 1990s, what became known as digital forensics was commonly termed ‘computer forensics’. The first computer forensic technicians were law enforcement officers who were also computer hobbyists. In the USA in 1984 work began in the FBI Computer Analysis and Response Team (CART). One year later, in the UK, the Metropolitan Police set up a computer crime unit under John Austen within what was then called the Fraud Squad.

A major change took place at the beginning of the 1990s. Investigators and technical support operatives within the UK law enforcement agencies, along with outside specialists, realised that digital forensics (as with other fields) required standard techniques, protocols and procedures. Apart from informal guidelines, these formalisms did not exist but urgently needed to be developed. A series of conferences, initially convened by the Serious Fraud Office and the Inland Revenue, took place at the Police Staff College at Bramshill in 1994 and 1995, during which the modern British digital forensic methodology was established.

In the UK in 1998 the Association of Chief Police Officers (ACPO) produced the first version of its Good Practice Guide for Digital Evidence (Association of Chief Police Officers, 2012). The ACPO guidelines detail the main principles applicable to all digital forensics for law enforcement in the UK.

As the science of digital forensics has matured these guidelines and best practice have slowly evolved into standards and the field has come under the auspices of the Forensic Science Regulator in the UK.

Cyber forensics and digital evidence

Computers are used for committing crime as well as it is also used to fight crimes. Digital Evidence is commonly associated with electronic crime, or e-crime, such as identity theft, cyber stalking, virtual rape, credit card fraud, cyber terrorism and etc. The tools of cyber forensics investigations are X-ways WinHex, Rifiuti, Pasco, Galleta/Cookie, NMap, Ethereal, BinText, etc. Rifuti helps in collecting all the deleted and undeleted documents whereas Pasco helps in gathering records of internet activities carried out from the targeted computer.

Generally, criminals leave a digital footprint such as the suspect's IP address, social media posts or using of their mobile for everyday use in change of traditional things. This could expose the evidence through intent, position and time of crime, relationship with victim(s), and correlation with other suspect(s).

Link based Evidence, Real Evidence, Hearsay Digital, Best Evidence are some sorts of digital evidence that is related to observing and investigation of computer network.

The computer forensics, mobile forensics, network forensics, forensic data analysis, legal considerations and data base forensics are some of the branches of digital forensics.

The availability of high speed internet, the explosion of complexity, legitimacy, privacy preserving investigation and increase in anti- forensic techniques are some of the challenges for digital evidence to curb cybercrime.

In testimony, proper preparation for trial makes all the difference. For digital investigators, preparing for trial can involve meeting with attorneys in the case to review the forensic findings, address any questions and the preparation of how to present it in the court. Scripting direct examination or rehearsing it may not be permitted in some contexts, but some discussion with the

attorney ahead of time is generally permissible and provides an opportunity to identify areas that need further explanation and to anticipate questions that the opposition might raise during cross examination.

Indian security officials frequently complain that getting data under the Mutual Legal Assistance Treaty (MLAT) has been a huge challenge. The Budapest Convention came into force on November 23, 2001 as a first multilateral effort by member signatories to address jurisdictional issues.

The main principles of digital forensics are applied with the following areas:-

Identification, Acquisition, Preservation, Examining and analyzing.

Data View Inconsistency is often to discover that the visualized content over cyberspace does not always represent the same saved copy on the disk which creates confusion and even inaccurate results in forensic analysis. This opens an area for investigation on how one can solve this issue and which protocols, tools, upgrades, etc., can be used to alleviate the impact of this scenario.

The gap between the emerging smart technologies and forensic tools are one the challenge with cybercrime digital forensics. There is an obvious technology gap between cyber criminals and combating tools and software kits and, unfortunately, it is in the favor of cybercriminals.

Digital Forensic

The production of electronic evidence has become a need in most cases to show the guilty of the accused or the accountability of the defendant. The future of computer forensics is limitless. The evidence is collected by the specialist in such a way that it has to be handled in an appropriate manner. This will help the court to provide justice to the victim. Thanks to the rising impact of technology in everyday life. Most legal systems throughout the world have updated their statutes to fit this movement in judicial attitude, which occurred largely in the past twenty years.

Some examples of Digital Forensic usage are as follows:-

- Intellectual Property theft
- Industrial espionage
- Bankruptcy investigations
- Employment disputes
- Fraud investigations

The technical conditions for the use of electronic records as evidence lay down in Section 65B (2) of the Indian Evidence Act, 1872 are that:

1. The computer used in entering and storing the electronic record was in regular use by an authorized person at the time of such entry and storage;
2. The entry of the data was in the ordinary course of activities;
3. The computer use was operating properly at the time of entry;

4. Storage of the data and that the data contents have not been affected by operational issues with the computer.

Amendment to Section 17 of the Indian Evidence Act, 1872 defines the term admission will include statements in electronic form also. Addition of Section 22A of the same Act says about to make oral admission of the contents of an electronic record irrelevant unless the genuineness of the record is in question. Addition of Section 39 talks about the part of an electronic record which is to be submitted to fully understand the nature and effect of the evidence and the circumstances under which it was made. Sections 81A, 85A, 85B, 85C, 88A, and 90A of Indian Evidence Act is to provide a presumption of authenticity to certain electronic messages etc.

The investigators create a second document for use in court. They are:-

1. Telecom Forensics
2. Grey Market/SIM box fraudulently
3. KYC forgery by TSP/managed services
4. Network intrusion and sabotage
5. Business losses
6. Fraudulent calls/SMSs/ Financial forgery

Section 43, Section 43A, Section 66, Section 66A, Section 66 B, C, D, Section 66 E, Section F, Section 67 of Information Technology Act, 2000 deals with punishment related to digital forensics.

Thus, we can say that computerized control systems manage banks, factories, retail inventories, air traffic control, hospitals, schools, corporations, and government organizations. Computers and their software programs are embedded in our cars, boats, trains and planes, in tools, equipment, and machinery, in telecommunications systems and public switched networks, even in our bodies. Each of them is a potential source of digital evidence, the collection, storage, analysis, and presentation of which is and will be constrained by evolving legal standards and constraints that we fail to understand at our peril.

Forensics analysis of email

With the prominence of the internet, emails have emerged as the most popular application for business communication, document transfers and transactions from computers and mobile phones. With this emergence, email security protocols have also been implemented to mitigate the illegitimate actions of criminals, such as business email compromise, phishing emails, and ransomware. However, there comes a time when specific emails need to be examined and data extracted for legal matters such as civil litigation and legally aided criminal investigations. This is where email forensics is applied.

What is email forensics?

Email forensics is exactly what it sounds like. The analysis of emails and the content within to determine the legitimacy, source, date, time, the actual sender, and recipients in a forensically sound manner. The aim of this is to provide admissible digital evidence for use in civil or criminal courts.

Admissible evidence

Most organisations have specific internal and external email policies in place to help safeguard their data, intellectual property, finances, and reputation. However, this does not always stop individuals (employees for example) from violating these policies to the detriment of their employer. These violations can present themselves in the form of forbidden file transfers, data breaches, indecent imagery, and incriminating email threads. Should a company suspect foul play, the application of email forensics to suspected email accounts can provide admissible evidence for disciplinary or legal purposes.

Can a solicitor or IT manager not just extract the emails?

They certainly can and may think that downloading a PST file (personal storage file) will glean all the information they require. However, as technically savvy as they may be, they are not digital forensic professionals. Forensic experts have the correct qualifications, accreditations, and technology to ascertain digital evidence in the most secure, efficient, and cost-effective manner, ensuring that it is court-admissible.

They possess expertise that allows them to identify hidden and manipulated email metadata fields, recover deleted files and are knowledgeable of the methods individuals use in an attempt to cover their digital tracks. For someone other than an expert to extract the data in an incorrect manner could jeopardise the integrity of the data, altering the metadata and complicating legal proceedings.

Email forensics experts

Email data should always be extracted by digital forensic professionals. This is highly recommended as they do so in a forensically sound manner ensuring that:

- The email data is extracted in full and there is no question whether all data has been recovered
- The validity of the data can be relied upon in both civil and criminal courts as admissible evidence
- Ensures that no changes are made to the email metadata
- It is compliant with the ACPO guidelines and the quality standards set out within the ISO17025 documentation and Forensic Science Regulator’s Codes of Good Practice and Conduct.
- Any deleted emails and files are recovered where possible

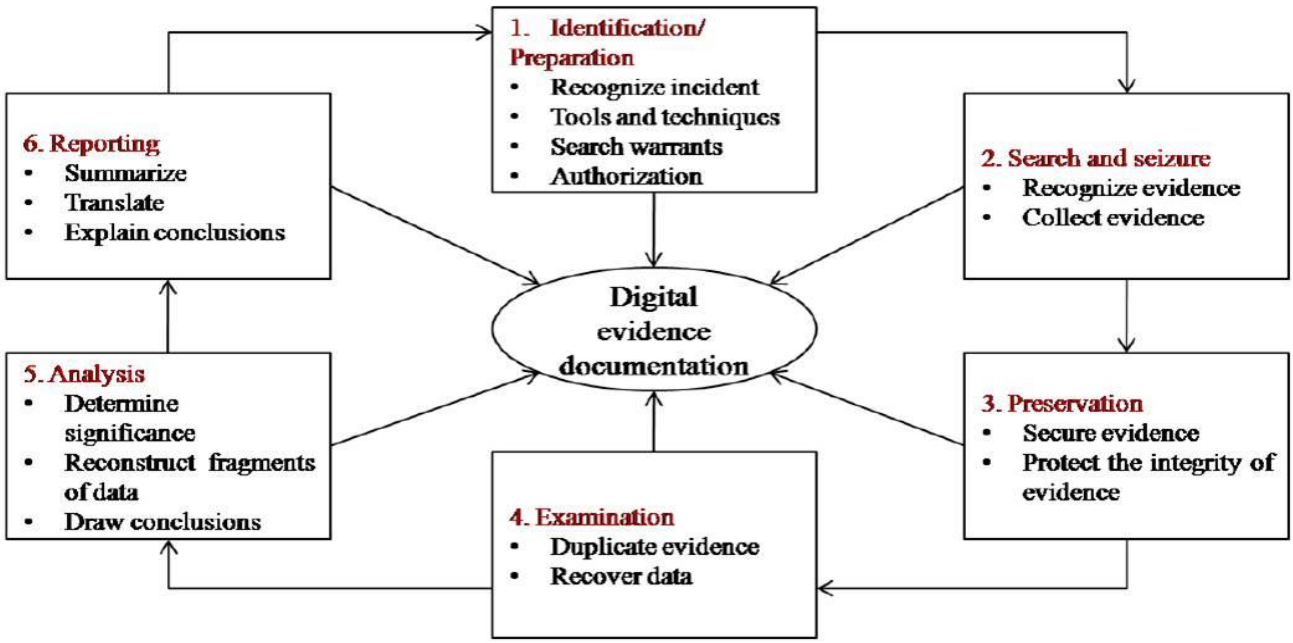
Why instruct CYFOR?

- As a leading authority in digital forensics, CYFOR has vast experience in email data extraction, data analysis and authentication for criminal and civil legal proceedings. Our team of digital forensic investigators come from a variety of high-integrity technical investigative backgrounds including law enforcement, military, academic and cyber security. This combined experience allows CYFOR to provide a leading digital evidence investigative service, backed by a dedicated quality management department that operates to ISO accreditations. This ensures that our clients receive the utmost quality of service and professionalism that is expected while meeting standards that can be relied upon in court.

Digital forensics life cycle

The digital forensics process is shown in the following figure. Forensic life cycle phases are:

1. Preparation and identification
2. Collection and recording
3. Storing and transporting
4. Examination/investigation
5. Analysis, interpretation, and attribution
6. Reporting
7. Testifying



1. Preparing for the Evidence and Identifying the Evidence

In order to be processed and analysed, evidence must first be identified. It might be possible that the evidence may be overlooked and not identified at all. A sequence of events in a computer might include interactions between:

- Different files
- Files and file systems
- Processes and files
- Log files

In case of a network, the interactions can be between devices in the organization or across the globe (Internet). If the evidence is never identified as relevant, it may never be collected and processed.

2. Collecting and Recording Digital Evidence

Digital evidence can be collected from many sources. The obvious sources can be:

- Mobile phone
- Digital cameras
- Hard drives
- CDs
- USB memory devices

Non-obvious sources can be:

Digital thermometer settings

Black boxes inside automobiles

RFID tags

Proper care should be taken while handling digital evidence as it can be changed easily. Once changed, the evidence cannot be analysed further. A cryptographic hash can be calculated for the evidence file and later checked if there were any changes made to the file or not. Sometimes important evidence might reside in the volatile memory. Gathering volatile data requires special technical skills.

3. Storing and Transporting Digital Evidence

Some guidelines for handling of digital evidence:

- Image computer-media using a write-blocking tool to ensure that no data is added to the suspect device
- Establish and maintain the chain of custody
- Document everything that has been done
- Only use tools and methods that have been tested and evaluated to validate their accuracy and reliability

Care should be taken that evidence does not go anywhere without properly being traced. Things that can go wrong in storage include:

- Decay over time (natural or unnatural)

- Environmental changes (direct or indirect)
- Fires
- Floods
- Loss of power to batteries and other media preserving mechanisms

Sometimes evidence must be transported from place to place either physically or through a network. Care should be taken that the evidence is not changed while in transit. Analysis is generally done on the copy of real evidence. If there is any dispute over the copy, the real can be produced in court.

4. Examining/Investigating Digital Evidence

Forensics specialist should ensure that he/she has proper legal authority to seize, copy and examine the data. As a general rule, one should not examine digital information unless one has the legal authority to do so. Forensic investigation performed on data at rest (hard disk) is called dead analysis.

Many current attacks leave no trace on the computer's hard drive. The attacker only exploits the information in the computer's main memory. Performing forensic investigation on main memory is called live analysis. Sometimes the decryption key might be available only in RAM. Turning off the system will erase the decryption key. The process of creating and exact duplicate of the original evidence is called imaging. Some tools which can create entire hard drive images are:

- DCFLdd
- Iximager
- Guymager

The original drive is moved to secure storage to prevent tampering. The imaging process is verified by using the SHA-1 or any other hashing algorithms.

5. Analysis, Interpretation and Attribution

In digital forensics, only a few sequences of events might produce evidence. But the possible number of sequences is very huge. The digital evidence must be analyzed to determine the type of information stored on it. Examples of forensics tools:

- Forensics Tool Kit (FTK)
- EnCase
- Scalpel (file carving tool)
- The Sleuth Kit (TSK)
- Autopsy

Forensic analysis includes the following activities:

- Manual review of data on the media
- Windows registry inspection
- Discovering and cracking passwords
- Performing keyword searches related to crime
- Extracting emails and images

Types of digital analysis:

- Media analysis
- Media management analysis
- File system analysis
- Application analysis
- Network analysis
- Image analysis
- Video analysis

6. Reporting

After the analysis is done, a report is generated. The report may be in oral form or in written form or both. The report contains all the details about the evidence in analysis, interpretation, and attribution steps. As a result of the findings in this phase, it should be possible to confirm or discard the allegations. Some of the general elements in the report are:

- Identity of the report agency
- Case identifier or submission number
- Case investigator
- Identity of the submitter
- Date of receipt
- Date of report
- Descriptive list of items submitted for examination
- Identity and signature of the examiner
- Brief description of steps taken during examination
- Results / conclusions

7. Testifying

This phase involves presentation and cross-examination of expert witnesses. An expert witness can testify in the form of:

- Testimony is based on sufficient facts or data
- Testimony is the product of reliable principles and methods
- Witness has applied principles and methods reliably to the facts of the case

Experts with inadequate knowledge are sometimes chastised by the court. Precautions to be taken when collecting digital evidence are:

- No action taken by law enforcement agencies or their agents should change the evidence
- When a person to access the original data held on a computer, the person must be competent to do so
- An audit trial or other record of all processes applied to digital evidence should be created and preserved
- The person in-charge of the investigation has overall responsibility for ensuring that the law and these are adhered to

Chain of Custody

A chain of custody is the process of validating how evidences have been gathered, tracked, and protected on the way to the court of law. Forensic professionals know that if you do not have a chain of custody, the evidence is worthless.

The chain of custody is a chronological written record of those individuals who have had custody of the evidence from its initial acquisition to its final disposition. A chain of custody begins when an evidence is collected and the chain is maintained until it is disposed off. The chain of custody assumes continuous accountability.

Approaching a Computer Forensics Investigation

The phases in a computer forensics investigation are:

- Secure the subject system
- Take a copy of hard drive/disk
- Identify and recover all files
- Access/view/copy hidden, protected, and temp files
- Study special areas on the drive
- Investigate the settings and any data from programs on the system
- Consider the system from various perspectives
- Create detailed report containing an assessment of the data and information collected

Things to be avoided during forensics investigation:

- Changing date/timestamps of the files
- Overwriting unallocated space

Things that should not be avoided during forensics investigation:

- Engagement contract
- Non-Disclosure Agreement (NDA)

Elements addressed before drawing up a forensics investigation engagement contract:

- Authorization
- Confidentiality
- Payment
- Consent and acknowledgement
- Limitation of liability

General steps in solving a computer forensics case are:

- Prepare for the forensic examination
- Talk to key people about the case and what you are looking for
- Start assembling tools to collect the data and identify the target media
- Collect the data from the target media
- Use a write blocking tool while performing imaging of the disk
- Check emails records too while collecting evidence
- Examine the collected evidence on the image that is created
- Analyze the evidence
- Report your finding to your client

Relevance of OSI model to computer forensic

OSI model

Before going into security, it is necessary to know the basics of networking and its models - the OSI model. It is a hypothetical networking framework that uses specific protocols and mechanisms in every layer of it. This model is used to divide the network architecture into seven different layers conceptually. These layers are:

- Physical layer.
- Datalink layer.
- Network layer.

Transport layer.

- Session layer.
- Presentation layer.
- Application layer.

There also involves some security postures and mechanisms that a security professional must know to detect and put the security method effectively in every layer.

Implementation of cyber security methods within the OSI Model

The first three layers of the OSI model are called the media layers.

1. Physical Layer is used for defining the technical qualifications of the data connectivity. Since the security in this layer is critical, so in case of any cyber danger (DoS attack), it is recommended to unplug the cable from the primary system. Safeguarding this layer needs bio-metric security, camera-based surveillance, key cards, and other physical monitoring.
2. Data Link Layer comprises of data packets transported from the physical layer. Any malfunctioning in this layer or data breach can impede the working of the network layer. Vulnerabilities that can be used and attacks that can be made in this layer are MAC address spoofing and virtual-LAN circumvention.
   So for protecting your system, common security mechanisms are MAC address filtering, assessment of wireless applications, checking of proper data encryption standards.
3. Network Layer is the last of the media layer and has an association with the real world. It deals with the addressing and routing of packets. IP address spoofing is one o the common attack of this phase. Strengthening this layer needs the techniques of firm anti-spoofing, proper implementation of firewalls and routing filters, and secure routing protocols.

The subsequent four layers are host layers:

1. Transport Layer - comes under the logical layer, which helps in transferring variable-length data sequence. The reliability of this layer can be achieved by ensuring the segmentation and de-segmentation mechanism and error control. For security purposes, this layer needs an appropriate firewall, restrictive admission of transmission protocols, and appropriate port number.
2. Session Layer - essentially manages the inter-system communication and sessions. The handling of local and remote application's interaction is done in this layer. In case of weak authentication methods, it can help attackers to perform a brute force. So the effective way of securing this layer is by ensuring appropriate encrypted key exchange, along with the restriction of unsuccessful session attempts using timing methods.
3. Presentation Layer - is used to standardize data with the help of various conversion schemes. But if there is poor conduct of malicious input, it can help cybercriminals exploit the system or even crash a system. Separate sanitized input and proper input validation can help protect the system from attackers.
4. Application Layer - contain the UI and the closest of all layers for the user-end. The widest range of cyber-attacks and security breaches is possible in this layer. It can lead to shutting down the network, stealing data, crashing the application, manipulating the information sent from source to destination, and many more.

So every layer needs proper security postures. Different ports and protocols are used for different scenarios

Challenges in computer forensics

Property	Relation to (digital) forensic investigation	Exemplary challenges
Density of device deployment	Influences the resolution of events that took place in a physical environment.	Reconstruct physical events on the basis of unevenly deployed devices (for example, not all the space has the same density of Internet of Things [IoT] nodes and information). This can also vary according to the considered environment.
Device type	Influences the type of information (sensor data such as temperature, humidity, pressure, or motion detection as well as the history of actuator states such as door status, pump pressure, or heating level).	Provision of a computer-aided, evidence-driven, and court-proof frameworks for the reconstruction of events. Such software should be able to take into account a mixed/increasing set of devices, for instance by means of a plug-in architecture.
Device location	Influences physical accessibility of the device for a digital forensic investigation (the device might be placed behind country borders) and influences which area of a physical environment was covered by the device (the part of a forensic site that has been influenced).	Develop a cost–benefit analysis to determine whether IoT devices located in hard-to-reach areas are worth accessing. One idea is to use databases that point out device properties useful for forensics investigations and additional details such as the accuracy of onboard sensors.
Recording history	All available information on an IoT device can be recorded locally or in the cloud. Local storage is usually limited; thus, the number of recorded sensor values/actuator states is kept under a certain threshold. Older data might not be accessible.	Automatic integration of IoT devices into the reconstruction process of physical events. This requires fetching the recording history of sensors and correctly placing it within the time frame of the event to be reconstructed. It could entail the support of visual analytics tools capable of handling devices that provide data with inconsistent or inaccurate timing and spatial positions.
Device interfaces	The interfaces used to access evidence highly influence the amount of information that can be retrieved. Some types of information might not be provided by certain interfaces while others are. In several cases, interfaces might be undocumented by the vendor.	Provision of a unified metainterface for IoT forensics covering a large spectrum of different devices and low-level interfaces of several vendors. This can likely be adequately addressed by larger community projects.

Challenges in network forensics

- Networks span multiple time zones and multiple jurisdictions
- Network data will be available offline and online (real-time)
- Real-time data requires ability to capture and analyze data on the fly
- The data may involve different protocols
- The data may be huge due to increasing bandwidth
- A protocol might also involve multiple layers of signal (VoIP, HTTP tunneling)
- Current forensic tools will not be able to handle real-time data and huge amount of data

There need to be a paradigm shift for network forensics techniques to analyze the real-time data and huge amounts of data. Duration of forensics investigation may vary, some simple cases might take a few hours and complex cases may take some years to solve.

Certain digital information other than the data itself may help in solving the case. Such information might include, data and timestamps of files, folder structure and message transmission tags. Real-time data collection is more complex as it needs to address legalities and privileges involved in surveillance.

Technical Challenges

The two challenges faced in a digital forensic investigation are complexity and quantity. The complexity problem refers to the data collected being at the lowest level or in raw format. Non-technical people will find it difficult to understand such data.

Tools can be used to transform the data from low level format to readable format. The quantity problem refers to the amount of data that needs to be analyzed. Data reduction techniques can be used to group data or remove known data. Data reduction techniques include:

- Identifying known network packets using IDS signatures
- Identifying unknown entries during log processing
- Identifying known files using hash databases
- Sorting files by their types

Legal challenges

Digital evidence can be tampered easily, sometimes, even without any traces. It is common for modern computers to have multiple gigabyte sized disks. Seizing and freezing of digital evidence can no longer be accomplished just by burning a CD-ROM. Failure to freeze the evidence prior to opening files has invalidated critical evidence.

There is also the problem of finding relevant evidence within massive amounts of data which is a daunting task. The real legal challenges involve the artificial limitations imposed by constitutional, statutory and procedural issues. There are many types of personnel involved in digital/computer forensics like technicians, policy makers, and professionals.

Technicians have sound knowledge and skills to gather information from digital devices, understand software and hardware as well as networks. Policy makes establish forensics policies that reflect broad considerations. Professionals are the link between policy and execution who have extensive technical skills as well as good understanding of the legal procedures.