UNIT 5 CYBER CRIMES

Structure

5.0 INTRODUCTION

The purpose of the Information Technology Act is to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic commerce, which involve the use of alternatives to paper-based methods of communication and storage of information. It also aims at facilitating electronic filing of documents with the Government agencies.

This law is based on the UN General Assembly resolution A/RES/51/162, dated the 30th January, 1997 the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL). Need was felt for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information;

The act has undergone several amendments since its enactment in the year 2000. The most significant amendment is of 2008 which tried to address a number of issues keeping in view the technological development which facilitated the commission of certain offences which had a greater impact on the society. In this unit the wrongful acts covered in the act will be discussed. Some wrongful acts are civil wrong for which the aggrieved party is entitled to penalty or compensation. Some acts are treated as crime for which punishment is provided. The unit will also touch upon the issues involved in the investigation of these offences. The investigation of these offences requires scientific knowledge which is called Cyber Forensics.

5.1 OBJECTIVES

After reading this unit you should be able to:

1. Describe the acts for which penalties and compensation are provided. Also discuss when these acts become an offence.
2. Discuss the offences for which punishment is provided.
3. Examine the jurisdictional issues involved in the investigation and punishment of the cybercrimes.
4. Discuss the challenges faced by investigation agencies in investigation of cyber crimes, Penalties, compensation and adjudication. .

5.2 CYBER CRIME AND ITS CLASSIFICATION

Cybercrime is defined as crimes committed on the internet using the computer as a tool to target the victim for the execution of the desired crime. Though it is difficult to determine that where the particular cyber crime took place because it can harm its victim even sitting at a far distance. As stated above from the year 1997 to 2008 tremendous changes took place which helps the judicial system to determine the specific kind of cyber crime. However, all cybercrimes involved both the computer and the person behind it as victims, it just depends on which of the two is the main target.

Example 1 – Hacking involves attacking the computer's information and other resources.
Example 2 – Stalking involves attacking the personal space of an individual.

- Cyber crimes are quite different from traditional crimes as they are often harder to detect, investigate and prosecute and because of that cyber crimes cause greater damage to society than traditional crimes. Cyber crime also includes traditional crimes conducted through the internet or any other computer technology. For example; defamation, forgery, identity theft, terrorism, cyber-stalking, hacking, software piracy, web jacking and bullying are considered to be cyber crimes when traditional crimes are committed through the use of a computer and the internet.

The other difference between these two crimes is based on the evidence of the offences. In the traditional crimes the criminals usually leave any proof of that crime like fingerprints or other physical proof. But in the cyber crimes cyber criminals commit their crimes through the internet and there are very less chances of leaving any physical proof.

However, the cyber crimes are broadly classified into different groups:

1 Crime against the individuals – Harassment, cyber-stalking, deformation, indecent exposure, cheating, email spoofing, fraud, etc.

2 Crime against property – Transmitting virus, net-trespass, unauthorized control over computer system, internet thefts, infringement of intellectual property,etc.

3 Crime against organization – Cyber terrorism within government organization, possession of unauthorized information, distribution of pirate software, etc.

4 Crime against society – Child pornography, financial crimes, sale of unlawful articles, trafficking, forgery of records, gambling, etc.

☞ **Check your Progress 1:**

1. Distinguish between cyber crime and traditional crime.

.....

.....

.....

.....

5.3 PENALTY AND COMPENSATION

Section 43 to 45 of Information Technology Act, 2000 provides for the instances where the wrong doer is liable to pay damages by way of compensation to the effected party.

Section 66 of Information Technology Act, 2000 however provides that if any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

Section 43 of Information Technology Act, 2000 provides that any person who without permission of the owner or any other person who is in charge of a computer, computer system or computer network commits the following acts shall be liable to pay damages:

(a) Accesses or secures access;
(b) downloads, copies or extracts any data, computer data base or information;
(c) introduces or causes to be introduced any computer contaminant or computer virus;
Explanation to this section provides:
"Computer contaminant‖ means any set of computer instructions that are designed–
(a) to modify, destroy, record, transmit data or program residing within a computer, computer system or computer network; or
(b) by any means to usurp the normal operation of the computer, computer system, or computer network;
(iii) ―computer virus‖ means any computer instruction, information, data or program that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a program, data or instruction is executed or some other event takes place in that computer resource;"
(d) damages or causes to be damaged data, computer data base or any other programs;
Explanation

(iv) of this section provides, " damage‖ means to destroy, alter, delete, add, modify or rearrange any computer resource by any means."
(e) disrupts or causes disruption;
(f) denies or causes the denial of access to any person authorised to access by any means;
(g) provides any assistance to any person to facilitate access in contravention of the provisions of this Act, rules or regulations made there under;
(h) charges the services availed of by a person to the account of another person by tampering with or manipulating;
(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;
(j) steal, conceal, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;]
[(v) ―computer source code‖ means the listing of program, computer commands, design and
layout and program analysis of computer resource in any form.]

Section 43A of Information Technology Act, 2000 provides for the liability for Compensation of a body corporate for failure to protect data.
Explanation to this section defines a body corporate as: "any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

The explanation also defines reasonable security practices and procedures as, "security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit."

Section 44 of Information Technology Act, 2000 provides for penalty for failure to furnish information, return, etc
"If any person who is required under this Act or any rules or regulations made there under to–
(a) furnish any document, return or report to the Controller or the Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;
(b) file any return or furnish any information, books or other documents within the time specified
therefore in the regulations fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues;
(c) maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues."

Section 45 of Information Technology Act, 2000 provides for the residuary penalty. Contravention of any rules or regulations made under this Act, for the

contravention of which no penalty has been separately provided. The maximum penalty in such cases is 25000 rupees.

5.3.1 Adjudication

Section 46 provides for the adjudication of disputes for awarding compensation. It authorizes the Central Government to appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry. This officer shall exercise jurisdiction to adjudicate matters in which the claim for injury or damage does not exceed rupees five crore. a reasonable opportunity for making representation in the matter and on such inquiry must be given.

Where it accedes 05 (five) crore,The jurisdiction shall vest with the competent civil court:

1. All proceedings before adjudicating officer shall be deemed to be judicial proceedings within the meaning of sections 193 and 228 of the Indian Penal Code, 1860;
2. It shall be deemed to be a civil court for the purposes of sections 345 and 346 of the Code of Criminal Procedure, 1973;
3. It shall be deemed to be a civil court for purposes of Order XXI of the Civil Procedure Code, 1908.

No person shall be eligible to be appointed as an adjudicating officer if he does not possesses such experience in the field of Information Technology and legal or judicial experience which is explicitly prescribed by the Central Government.

5.3.2 Appellate Tribunal–

An appeal tribunal is a special court or committee that is formed to reconsider a decision made by another court or committee.

Section 48 provides that from coming into force of the Finance Act, 2017 Telecom Disputes Settlement and Appellate Tribunal established under section 14 of the Telecom Regulatory Authority of India Act, 1997), shall be the Appellate Tribunal for the purposes of this Act and the said Appellate Tribunal shall exercise the jurisdiction, powers and authority conferred on it by or under this Act.

Section 57 provides the procedure for appeal. Any person aggrieved by an order made by controller or an adjudicating officer under this Act may prefer an appeal to a Appellate Tribunal having jurisdiction in the matter. However no appeal shall lie to the Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties. Every appeal shall be filed within a period of forty-five days from the date on which a copy of the order made by the Controller or the adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed: Provided that Appellate Tribunal may entertain an appeal after the expiry of the said period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.

The appeal shall be dealt with as expeditiously as possible and endeavor shall be made to dispose of the appeal finally within six months from the date of receipt of the appeal.

Section 58 provides that Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, it shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying a suit, in respect of the following matters, namely:–
(a) Summoning and enforcing the attendance of any person and examining him on oath;
(b) Requiring the discovery and production of documents or other electronic records;
(c) Receiving evidence on affidavits;
(d) Issuing commissions for the examination of witnesses or documents;
(e) Reviewing its decisions;
(f) Dismissing an application for default or deciding it ex parte;
(g) Any other matter which may be prescribed.

Section 62 provides for the appeal to high court. Any person aggrieved by any decision or order of the Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order on any question of fact or law arising out of such order:
Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

☞ **Check your progress 2:**

1. Describe in brief the procedure for adjudication under the Information Technology Act, 2000

.....

.....

.....

.....

5.4 OFFENCES

Following acts are considered as offences under the act:

Section 65 provides for tampering, concealing, destroying , or altering any computer source document intentionally. Penalty is up to Rs.2,00,000/-, or Imprisonment up to 03 (three) years, or both.

Section 66 provides for dishonestly, or fraudulently doing any act as referred in Section 43. Penalty is up to Rs.5,00,000/-, or Imprisonment up to 03 (three) years, or both.

Section 66A has been struck down by Supreme Court's Order dated 24th March, 2015 in the landmark precedent of "*Shreya Singhal vs. Union of India*", AIR 2015 SC.1523.25. The court found it as violation of the Freedom of Speech and Expression guaranteed under the Constitution of India.

Section 66B provides for dishonestly, or fraudulently receiving or retaining any stolen computer resource or communication device. Penalty is up to Rs.1,00,000/-, or Imprisonment up to 03 (three) years, or both.

Section 411 of the IPC, 1860 provides punishment for dishonestly receiving stolen property and is worded in a manner that is almost identical to section 66B of the IT Act. The punishment under section 411 of the IPC is imprisonment of either description for a term of up to 3 years,

Section 66C provides for dishonestly, or fraudulently making use of Electronic Signature, Password or any other Unique Identification Feature of any other person. Penalty is up to Rs.1,00,000/-, or Imprisonment up to 03 (three) years, or both.

Section 66D provides for dishonestly, or fraudulently by means of any communication device or computer resource cheating by personating. Penalty up to Rs.1,00,000/-, or Imprisonment up to 03 (three) years, or both.

Section 419 of the IPC, 1860 provides punishment for 'cheating by personating' and provides that any person who cheats by personating shall be punished with imprisonment of either description for a term which may extend to 03 (three) years or with a fine or with both. A person is said to be guilty of 'cheating by personating' if such person cheats by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is.

Section 420 of the IPC, 1860 provides for any person who cheats and thereby dishonestly induces the person deceived to deliver any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security shall be punished with imprisonment of either description for a term which may extend to 07 (seven) years, and shall also be liable to fine.

Section 66E of Information Technology Act, 2000 provides for intentionally capturing, publishing, or transmitting image of private area of any person without consent. Penalty is up to Rs.2,00,000/-, or Imprisonment up to 03 (three) years, or both.'

Section 66F provides for doing any act electronically, or with use of computer with intent to threaten unity, integrity, security, or sovereignty of India. Punishment is Imprisonment for Life.

Section 121 of the IPC, 1860 provides for waging, or attempting to wage war, or abetting waging of war, against the Government of India does cover this offence partially.

Section 67 provides for publishing, or transmitting in electronic form any material which appeals to prurient interest, or if its effect is such as to tend to deprave and corrupt persons who are likely to read, see, or hear matter contained in it. Penalty is up to Rs.5,00,000/-, or Imprisonment up to 03 (three) years, or both, And in the event of second or subsequent conviction, shall be liable to pay penalty up to Rs.10,00,000/-, or Imprisonment up to 05 (five) years, or both.

Section 67A provides for publishing, or transmitting in electronic form any material which contains sexually explicit act, or conduct. Penalty is up to Rs.10,00,000/-, or Imprisonment up to 05 (five) years, or both, And in the event of second or subsequent conviction,

this section however provides that provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form–
(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting representation or figure is the interest
of science, literature, art or learning or other objects of general concern; or
(ii) which is kept or used for bona fide heritage or religious purposes.

The provisions of sections 292 and 294 of the IPC, 1860 would also be applicable for offences of the nature described under sections 67, 67A and 67B of the IT Act. Section 292 of the IPC, 1860 provides that any person who, inter alia, sells, distributes, publicly exhibits or in any manner puts into circulation or has in his possession any obscene book, pamphlet, paper, drawing, painting, representation or figure or any other obscene object whatsoever shall be punishable on a first conviction with imprisonment of either description for a term which may extend to 02 (two) years, and with fine which may extend to Rs. 2,000 (Rupees two thousand) and, in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to 05 years, to be accompanied by a fine which may extend to Rs. 5,000 (Rupees five thousand).

Section 294 of the IPC, 1860 provides for any person who, to the annoyance of others, does any obscene act in any public place, or sings, recites or utters any obscene song, ballad or words, in or near any public place, shall be punished with imprisonment of either description for a term which may extend to 03 months, or with fine, or with both.

Section 68 of IT Act, 2000 provides for the Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under and if any person who intentionally or knowingly fails to comply with the order, shall be liable to pay penalty up to Rs.1,00,000/-, or Imprisonment up to 02 (two) years, or both.

Section 69 provides that where the Central Government or a State Government or any of its officers specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do, in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may with reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource, Any person who fails to comply with the order, then he shall be liable to Imprisonment of 07 (seven) years, along with the fine (amount of fine is not specified in the act).

Section 70authorises the Government to declare by notification in the Official Gazette, any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system. Any person who fails to comply with the notification, shall be liable to Imprisonment of 10 (ten) years, along with the fine.

Section 71 provides that whoever makes any misrepresentation to, or suppresses any material fact from the Controller or the Certifying Authority for obtaining any License or Electronic Signature Certificate, as the case may be, shall be liable to pay penalty up to Rs.1,00,000/-, or Imprisonment up to 02 (two) years, or both.

Section 72 provides that if any person who has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person, shall be liable to pay penalty up to Rs.1,00,000/-, or Imprisonment up to 02 years, or both.

Section 72A provides that if any person who has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, shall be liable to pay penalty up to Rs.5,00,000/-, or Imprisonment up to 03 years, or both.

Section 73 provides that if any person publishes a Electronic Signature Certificate, or make it available to any other person with the knowledge that
- Certifying Authority has not issued it, or
- Subscriber has not accepted it, or
- Certificate has been revoked or suspended shall be liable to pay penalty up to Rs.1,00,000/-, or Imprisonment up to 02 years, or both.

Section 74 provides that if any person knowingly creates, publishes, or otherwise makes available Electronic Signature Certificate for any fraudulent

or unlawful purpose, shall be liable to pay penalty upto Rs.1,00,000/-, or Imprisonment up to 02 (two) years, or both.

☞ **Check your progress 3:**

1. In which Supreme Court case and on what ground section 66A of Information Technology Act, 2000 was struck down.

.....

.....

.....

.....

5.4.1 Liability of Network Service Providers

A 'network service provider' means any person who provides access to information service in electronic form. For example: Internet service provider, cellular mobile services, customer access services, mobile satellite services etc. It essentially performs two tasks-to provide access to the network and to act as intermediary between an originator and addressee with respect to any particular electronic message.

Section 79 provides certain exemptions from liabilities to intermediaries i.e. internet service providers etc. An intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him. This exemption shall apply if–
(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or
(b) the intermediary does not–
(i) initiate the transmission,
(ii) select the receiver of the transmission, and
(iii) select or modify the information contained in the transmission;
(c) the intermediary observes due diligence while discharging his duties under this Act and also
observes such other guidelines as the Central Government may prescribe in this behalf.

The above exemption shall not apply if–
(a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act;
(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its
agency that any information, data or communication link residing in or connected to a computer
resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

☞Check Your Progress 4:

1. What are the grounds which exempt the network service provider from liability?

.....

.....

.....

.....

5.4.2 Investigation

For the purpose of conducting cyber-crime investigation, essential special skills and technical tools are required without which the investigation is next to impossible. After commencement of the Information Technology Act, 2000, some provisions of Criminal Procedure Code, 1973 and the Evidence Act, 1872 have been duly amended. Along with these, certain new rules and regulations had been enforced by the Indian legislative system to meet the need of cyber-crime investigation.

Section 75 deal with the issue of jurisdiction with respect to cyber crimes. As we know, cyber crime knows no boundary. A person sitting in one country can commit offences having its consequences in another country. Section 75 provides that if any person have committed an offence, or contravention committed outside India, and if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India, then the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

Section 76 provides that any computer, computer system, floppies, compact disks, tape drives, or any other accessories related thereto, in respect of which any provision of this Act, rules, orders, or regulations made there under has been, or is being contravened, shall be liable to confiscation. However, if it is proved that such resources were not used in committing fraud then only person in default will be arrested.

Section 77 provides that compensation, penalties or confiscation shall not interfere with other punishment.

Section 77A deals with compounding of offences. A court of competent jurisdiction may compound offences, other than offences for which the punishment for life or imprisonment for a term exceeding 03 (three) years has been provided, under this Act:

Provided that the court shall not compound such offence where the accused is, by reason of his previous conviction, liable to either enhanced punishment or to a punishment of a different kind:

Provided further that the court shall not compound any offence where such offence affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or a woman.

Section 77B provides that offences with three years imprisonment shall be bailable.

Section 78 deals with the power to investigate. It provides that a police officer not below the rank of inspector shall investigate any offence under this Act.

Section 80 deals with the power of police officer and other officers to enter, search etc. It provides that any police officer, not below the rank of a inspector, or any other officer of the Central Government or a State Government authorised by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act. Where any person is arrested by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.

☞ **Check Your Progress 5:**

1. How the issue of jurisdiction of Indian courts with respect to offences committed outside India has been dealt with by the IT Act?

.....

.....

.....

.....

5.5 CYBER FORENSICS

Cyber forensics also known as computer forensics which is the application of investigation and analysis techniques to gather and store evidence from a particular computing system in a way that is appropriate for presentation in a court of law.

Section 79A authorizes Central Government to notify any department, body or agency of the Central Government or a State Government as an Examiner of electronic evidence for the purposes of providing expert opinion on electronic form evidence before any court or other authority.

"Cyber forensics is the process of acquisition, authentication, analysis and documentation of evidence retrieved from the systems or online used to commit the crime. The systems could be from computers, networks, digital media or storage devices that could contain valuable information for the investigators to examine. From online, it could be from e-commerce domains or other websites. In cyber forensics, file or data carving techniques are most

commonly used to extract digital evidence from the source, hard drive or online domain. Computer forensics is important not just because it does recover files hidden or deleted away from storage devices and systems but it can also tell forensics experts whether are there any suspicious activities going on or had the systems been tampered with. Computer forensics had helped solved the issue of recovering information from files where file system is unavailable or file system structure is corrupted. Files may be intentionally deleted or worse formatted to the interest of the suspect to conceal his actions. In today's modern era where technology plays a part in almost all the electronic devices, it is important to know when required, how a trained forensics specialist can perform up to expectation, in collecting and present his evidence findings to corresponding agencies.

Examinations of forensics evidence are normally held in forensics laboratories or clean rooms by computer forensics investigators. A good and knowledgeable forensics expert is best preferred to be in the process of examination, as it is always vital to perverse the integrity of the data and not destroy it. Many forensics experts have their own standards and procedures on how computer forensics examinations are conducted which can be a big issue. Having double standards could jeopardize the integrity, creditably and validity of the digital evidence which could result in serious implications along the way. Therefore, as early as 1991, suggestions were made to streamline and standardize the examination processes and protocols had been raised. The purpose was to smoothen out rough edges approach used in evidence finding. Eventually, all these led to the formation of International Organization on Computer Evidence and Scientific Working Group on Digital Evidence (SWGDE). It became a worldwide effort to help law enforcement agencies around the globe to work together more closely with regards to forensics examinations.

Digital forensics is a branch of forensic science which deals with recovery and investigation of digital or electronic data. This data can be from a computer system, mobile device, cloud service, and so on. Its various sub branches include computer forensics, network forensics, forensic data analysis, and mobile device forensics.

Cyber or computer forensics is the application of forensic science to collect, process, and interpret digital evidence to help in a criminal investigation and presenting digital evidence in a court of law. It is the branch of forensic science in which evidence is found in a computer or any other digital device and with increasing cybercrime, cyber forensics has now become crucial for public safety, national security, and law enforcement**.**

☞Check your progress 6:

1. What is Cyber Forensics?

.....

.....

.....

.....

5.5.1 Cyber Forensic Investigation Tools

Cyber forensic techniques include:

1. Cross-driven analysis that correlates data from multiple hard drives.
2. Live analysis, which obtains data acquisitions before a PC is shut down.
3. Deleted file recovery.
4. Detecting data theft using Stochastic Forensics.
5. Concealing a file, message, image, or video within another file using Steganography.

Computer forensic investigations go through five major standard digital forensic phases:
1. Policy and procedure development,
2. Assessment,
3. Acquisition,
4. Examination, and
5. Reporting.

Digital evidence is so fragile, it can be easily damaged, modified or destroyed purposely. That is why most of the time, original evidence are often duplicated and analysis is carried out on the duplicated copy to prevent any mishap of damaging the original copy. Scope of digital evidence examination can be very broad, it can be either online or offline. Examples of them are credit card transactions, Internet communications history, hard drives and other storage devices.

Digital evidence is very critical to an investigation because the information on the evidence can tell the investigator what really happened and pieced together the whole picture. Forensics experts are looking for any form of metadata, suspicious content and other data residing in the hard drive. Every single click by the user on the computer was recorded by the system and a trained forensics expert can tell from one look what types of activity and desire the user was engaged in. better than anyone else. The recorded logs act like a behavioral database, documenting every single movement on the laptop used by anyone.

There are methods and techniques out there to aid fellow forensics experts to prevent digital evidence from being unintentionally tampered with. Experts can utilize method such as Imaging and Write-block. Imaging is equivalent to ghosting a backup copy of the whole computer hard drive (evidence) into a soft copy. So investigators work on the ghosted copy of the hard drive and the original hard drive is kept one side. In any case, if the ghosted copy is corrupted; investigators can pull out the original hard drive and create another copy to work on. Write-block is another good way to prevent original evidence being altered. The evidence media is connected with a special machine that can prevent any attempt to overwrite the data on the device. Thus, the evidence on the hard drive cannot be altered as any attempt to write on the media had been blocked by the special machine.

The reason behind preservation of digital evidence is simple. When submitting digital evidence for documentations or legal purposes in any court or legal department, legitimate proof is required to show correct findings on the

investigation. It had to show the same as the exhibit seized at the crime scene. This phenomenon is also commonly known as chain of custody. For example, in a cyber-forensics crime environment, such exhibits would be media storage devices, a copy of digital evidence from the hard disk seized and so on. Chain of custody basically is a map that clearly depicts the process of how digital evidence were processed; collected, analyzed and preserved in order to be presented as digital evidence in court. A chain of custody will also be needed to showcase whether the evidence is trustworthy or not. To meet all the requirements for chain of custody, three criteria are essential. Firstly, no alteration must be done to the evidence from the day of seizure. Secondly, a duplicate copy needed to be created and it had to be functional; not corrupted. Lastly, all evidence and media are secured. Able to provide this chain of custody is unbroken is an investigator primary tool in authenticating all the electronic evidence.

If the chain of custody is broken, digital evidence collected from the scene submitted to the court can be denied as the evidence might had been altered and might not tell the truth of the evidence. This is a prosecutor worst nightmare. In any situation, chain of custody is best followed to prove that evidence does not get contaminated and stayed in original state. However, there are occasions where collecting evidence without altering the data is not possible, especially when forensics tools were used. Such act will prove to be a serious implication to justify the evidence is intact and submission of such evidence will be challenged by the opposing team.

Locate Evidence once preserving the evidences is done, it's time to locate relevant evidence that can make a difference in the legal battle. The general first rule of thumb when locating the evidence is do not rush, as one is eager to get the investigation started, wants to find as many evidences as possible. However, the more one rushes the more mistakes the one is likely to make. Rushing into an investigation can have dire consequences, consequences like causing evidence to be lost prematurely or altered unintentionally.

Besides locating evidence, investigators must also maintain high integrity and reliability of the digital evidence, doing so, will minimize metadata being altered and destruction of important evidence. Digital evidence can be in any file format; email, notepad or video or it can have no file format due to the fact that it had been encrypted. Forensics experts need to browse through thousands of files in the computer system or network to spot and collect suspicious files. Forensics experts are trained and taught to focus on area of interests within the system. Examples of such areas are like Recycle bin, Windows Registry and Internet Temp Folder. Focusing on these areas saved tremendous hours of searching. These areas will tell the investigators what took had happened and who did it. To examine such a wide range of file types after taking consideration the area of interests. The process of examination gets whole lot tougher and tedious. Investigators will bring in tools to help facilitate them with locating and collecting of the evidence. Forensics experts often use tools like OS forensics, XYR tools, Quickstego or other sophisticated toolkits to aid them in the finding. All these tools will help investigators to decide whether they are looking at the correct areas or not and whether did they missed out anything important. Such equipment not only uncovers hidden or deleted files, it can also reveal the importance of the file whether it is relevant to the case or not.

☞ **Check your progress 7:**

1. What are the techniques used by forensics experts?

.....

.....

.....

.....

5.6 SUMMARY

In this unit we have discussed the penalties and offences provided under the Information Technology Act, 2000. Any type of unauthorized intrusion in the computer, computer system or network is prohibited and any person who does it is liable to pay compensation.

The penalties include: introducing viruses in the computer system, unauthorized download of copyrighted material, charging services in the name of others etc.

Offences covered in the act are mainly related to hacking, misrepresentation, identity theft, publishing obscene material, child pornography, unauthorized access to protected system etc.

Investigation of cyber crime is a big challenge. Cyber criminals are mainly educated and well versed in technology. Therefore investigation of cyber offences requires training in skills of cyber forensics.

5.7 SOLUTION/ANSWERS

1. **Cyber crime are those offences in which computer is used as tool or target or both in committing offences. The term includes the offences covered under the IT Act such as unauthorized access to a computer or introducing viruses etc and traditional crimes covered under the Indian Penal Code or other legislations such as forgery, defamation etc.**
2. **IT Act provides that for adjudication of penalty and compensation upto 5 crore rupees, there shall be the Adjudication officer. Against its decision, appeal can be filed before the Appellate Tribunal and second appeal to the High Court. Adjudicating Officer have the power of civil court for certain purposes. No appeal will lie where the order is based on the compromise between the parties. For amount acceding 5 crore rupees, the civil courts have the jurisdiction.**

3. "Shreya Singhal vs. Union of India" is the landmark judgment which struck down section 66A of Information Technology Act, 2000 on the

ground that it puts unreasonable restriction on the Freedom of Speech and Expression guaranteed by the Constitution of India.

4. An intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him. This exemption shall apply if–
5. (a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or
   (b) the intermediary does not–
   (i) initiate the transmission,
   (ii) select the receiver of the transmission, and
   (iii) select or modify the information contained in the transmission;
   (c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

6. Section 75 provides that if any person have committed an offence, or contravention outside India, andit involves a computer, computer system or computer network located in India, then the provisions of this Act shall apply also to such person irrespective of his nationality.

7. Cyber forensics also known as computer forensics which is the application of investigation and analysis techniques to gather and store evidence from a particular computing system in a way that is appropriate for presentation in a court of law.

8. The techniques used by forensics experts are as follows:
   Cross-driven analysis that correlates data from multiple hard drives.
   Live analysis, which obtains data acquisitions before a PC is shut down.
   Deleted file recovery.
   Detecting data theft using Stochastic Forensics.
   Concealing a file, message, image, or video within another file using Steganography.

5.8 REFERENCES

- UKEssays. (November 2018). What Is Cyber Forensic Information Technology Essay? Retrieved from https://www.ukessays.com/essays/information-technology/what-is-cyber-forensic-information-technology-essay.php?vref=1
- Vinod Joseph and Deeya Ray (Feb 2020). Cyber Crimes under the IPC and IT Act - An Uneasy Co-Existence. Retrieved fromhttps://www.mondaq.com/india/it-and-internet/891738/cyber-crimes-under-the-ipc-and-it-act--an-uneasy-co-existence.
- Information technology Act, 2000.
- Indiacode, Information Technology Act, 2000 available at https://www.indiacode.nic.in/showdata?actid=AC_CEN_45_76_00001_200021_1517807324077&sectionId=13011&sectionno=2&orderno=2