International Research Journal of Commerce and Law
Volume 10 Issue 06, June 2022 ISSN: 2349-705X Impact Factor: 6.843
Journal Homepage: http://ijmr.net.in, Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

UNDERSTANDING CYBERCRIME AND ITS INVESTIGATION:ISSUES AND CHALLENGES

Ms. Monika Thakur, Assistant Professor,
Faculty of Law,Shoolini University of Biotechnology and Management Sciences,
Himachal Pradesh, India
Dr. Kalpna Sharma, Assistant Professor,
Faculty of Law, Shoolini University of Biotechnology and Management Sciences,
Himachal Pradesh, India

ABSTRACT

21st Century is the world of Internet Technology, Knowledge, and Global Platform, where every information we need is just a click away. With its pros and cons, cybercrimes have come forward. Several types of Cybercrimes are available in the cyber world. These crimes are difficult to detect and confirm. Whenever a crime is committed, whether traditional or new age, a standard procedure is followed to investigate that crime. The process of investigation is said to be the most crucial and sensitive part in cracking the case. In the said study, the researchers have tried to under the working of different cybercrimes and studied working on the investigation process of cybercrime in India. The process starts with the collection of evidence, and how the process works, having many steps to investigate.

Keywords: **Cyber Crimes; Cyber Investigation; Digital Evidence; Digital Forensic**

INTRODUCTION

Electronic media, computers, and the internet have gone to nearly 360 million users who were online in the year 2018, with an average of 1 million per day in 2020. (Kemp, 2019). With the increase in technology usage, be it in academics, research, health, finance, economic, political, or social, data is being generated and processed at every stage. Every number dialled, every photo clicked, every message shared, and every bank transaction, either online, ATM, or credit card transaction, increases the data and information. In the age of technology and the internet, the data processed cannot be calculated, and neither it can be saved as such a massive amount of data is vulnerable to theft and misuse. Such an enormous amount of data has to lead Cybercrimes. "Cyber Crimes" is a term used to define the illegal actions done by specific offenders for a particular reason to damage or cause loss to an individual or society.

While defining Cybercrime (Wall 2007) tried to understand how cybercrimes have impacted people's lives, growth has impacted information& communication technology. The fast working and potential of cyberspace have given ample opportunities to the offenders who are actively

seeking such opportunities to commit such crimes. Stating forward, Wall (2005), in his earlier work, has already given some points which were," Globalisation, Digital Networks, Digital Surveillance, and loads of data set." Further, Wall (2005) showed in a matrix providing the combination of opportunities and cybercrimes. Several discussions have been done on the scope of cybercrime and how technology has changed traditional crimes and gave them new dimensions. (Johankhani and Ali-Nemrat. 2011, Rowlingston, 2007). If we study the definition by (Hogan-Howe, 2013),' Criminals have realised there are considerable rewards to be reaped from online fraud, while the risk of getting arrested falls way below that of armed robbers." It merely provides the inverse relationship between reward and risk in contradiction to traditional crimes; further cybercrime gives in the following characters to be pulled of, motivated offenders seeking a perfect target with many capabilities having the least protective cover. Here offenders being computer literate having malicious intentions, the ideal target is a person or a firm having something the offender can use and protective cover being lack of security and computer knowledge.

Several Laws have been initiated and developed over time, and these are just to prevent people and safeguard their online identity, information, and abuse. Easy access to technology has increased online transactions from online trading to online shopping, online payment to sharing of reliable information through email. Security in offices is monitored through biometric, Unique Identification Code (UID, Aadhaar in India), making every individual vulnerable to cyber-attacks. Everything online is under continuous threat from identity to intellectual property and all because of virtual I.D.'s. Pornography has also reached a new level and is now more easily accessible.

The process of cyber investigation starts from reporting of a cybercrime leading to a survey, and further precautions start (Y. Chen et al.,2008; M. Geva et al. 2014; N. Jeyanthil et al. 2012; C. Y. Liu et al. 2014; C. Sorrells and L. Qian. 2014; M. Subramanian. 2010; J. Udhayan, T. Hamsapriya. 2011). Several Procedures are considered to protect oneself from cybercrimes. Investigation of such crimes is not just to get to the culprit. Still, it also opens up new options and ways to future attacks and to generate an investigation strategy to detect and stop future cybercrimes.

INVESTIGATION PROCESS (Y.S. Yen, I.L. Lin, and A. Chang, 2012)

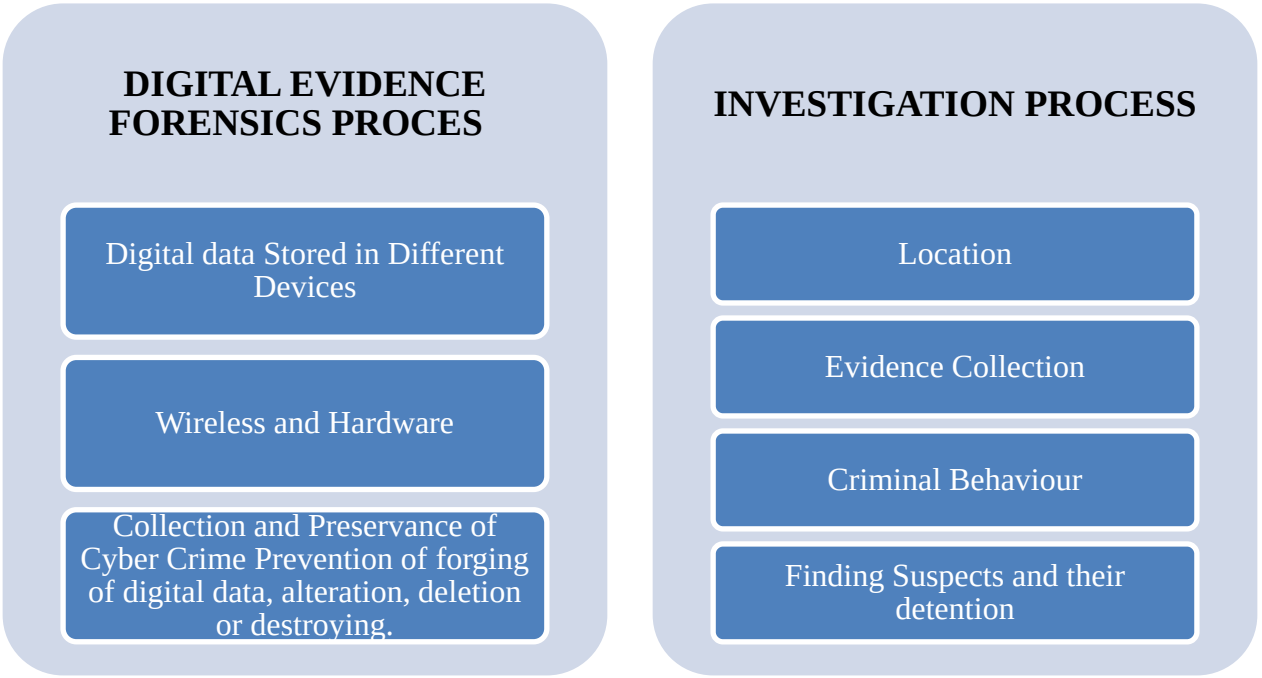


Figure 1. Details of the Investigation Process.

2. DEFINITION OF CYBERCRIME:

In Layman's term, when technology is used to pull up a crime by an individual is called cyber-crime. (P. Hunton, 2009) defined," A crime which is not the usual old school but is a" hi-tech," using technology to commit the same. (R.P. Brayant,2008; E. Moultan, 2008; D.L. Shinder, M. Cross, 2008; D.S. Wall. 2007; M. Yar. 2006) supported the use of network technology to pull these crimes, and it is just different from traditional crimes due to the presence of electronic technology.

3. TYPES OF CYBERCRIME

While studying cybercrimes, new types and forms can be found every day though Yar (2006) divided them into four categories, which can be subdivided further, keeping in mind the structure and usage, even law governing those. These are a) Cyber- trespass: getting into or cross boundaries computer attacks, b) Cyber theft and deceptions: Bank related cybercrime, c) Cyber Pornography: either of any (child or other), and d) Cyber Violence: hate statements between two people, organizations, or countries, and latest Cybercrime against State has been added to the list. Indian Penal Code in India has defined a large number of cybercrimes. They are:

3.1 Internet Auction Fraud: The Internet is full of fake websites and blog selling or auctioning products online. These are counterfeit or stolen products. Here the seller advertises its products, and prices for the same are rock bottom lucrative ones. Some buyers fall prey to these website advertisements and pay the money in advance to claim their products which is not a bank transfer but other online services available, to get instant cash and hidden identity so fewer chances of being caught. Specific examples of Auction Frauds:

a) Either good are not delivered or fake products, bricks, or sand in some cases in delivered.

b) Sellers get fake payment receipts.

c) Goods received are not at all what was advertised and ordered. E.g., A Soap bar is delivered instead of a watch in a packed box.

3.2 Botnets Sending Virus or Malware on the internet infects the Computer without the owner's knowledge. The owners of these Botnet have access to millions of computers on the internet and can use the information they want. Every device which is connected to the internet is under threat through these botnet attack. (M. Thopliyal et al., 2013; F. Corpine and S. Maria, 2013). R.A. Rode et al. (2013) states Botnet as the most dangerous threat to cybersecurity. A combination of BOT, NET, where BOT is an attacker or controller NET being information technology. If we see the trend and study more about Botnet, we can see that this has grown manifold in the past days. Botnet is part of major Cybercrimes (M. Zahid, 2012); they infect the system by sending emails, downloading pirated software, and corrupting the disk drive (Microsoft security Intelligence Report, 2013). In India, a particular cell for BotNet cleaning has been formed under the name of" Cyber Swatch Kendra." Their main targets of Botnet attacks are businesses and government.

3.3 Child Pornography: The existence of Porno goes back to the start of media, and it increased multifold with the introduction and increase in internet usage. It is said that 60% of the web content is pornography, and a half it is a child. Child Pornography is the max watched and paid for online. It is defined as a visual of a minor in sexual activity; it can be consensual of forced and maximum time (Magid, 2002). Though several laws around the world monitor them, they are still in existence and running unstopped.

3.4 Computer Viruses: It is a type of software/program sent to a person through email or message to gain unauthorized access to other people's systems to steal essential data for personal advantage. Organizations and individuals worldwide check and are afraid of threats that they

have from viruses that float freely on the cyber world/Cloud as we know it. Data and the virtual world are full of information, and every bit of information has value. With the increase in online trading and working, the chances of catching viruses have increased. Viruses are said to be the self-replicating programs or set of programs that disturb the working of the system. Paul Royal et al. (2006) said an intentionally made program to create problems for others. It is said that every Virus has three parts a) infectable, b) damaging, c) trigger pulled. The Virus structure is a) Mark, b) Infection, c) Trigger and, d) Payload.

3.5 Cyber Bullying: Every incident of creating a problem for an individual by using technology, electronic communication, and devices, by sending unwanted messages, email, a social media platform with just an intention to bully the person. Sometimes fake and defamatory blogs, websites, and posts on social media are created and shared to attack and destroy an individual's public image. Early (2010) says that unlike a physical fight which is real and has an end, a virtual one starts but cannot be found and tough to finish (Smith et al., 2013) "An intentional act by an individual or a group using information technology over some time creating a false image by floating false information which victim cannot defend easily." Pactchin J (2016) says it is not only boys but also girls who are also the offenders and victims. Some certain used words are" Bitch"," Hate," and "Die," as given found in some cases (Troll Police, 2018). In simple words, it is the most rampant crime committed in the digital world.

3.6 Cyber Laundering: When the power of the internet is used by Money Launders to convert illegally earned money into the mainstream, it is tough to find (Veng Mei Leong, 2007) known as cyber laundering. The characteristics of the internet that attract offenders are Anonymity, No direct Contact, Flexible and Quick with Global positioning having no limitations of borders (GIFI, 2008), depending on the features of the online payment system available internet payment, online banking. The most surprising fact about Cyber Laundering is that it is done by literate and highly Capable individuals as the system and methods which are followed are complex and unconventional. Jyoti and Vijay (2017) supported the thought and added that it is the only reason why such acts are callous to find and investigate.

3.7 Cyber terrorism: The first time this term was used was in the 1980s by Bareey Collins of the Institute for security and Intelligence, California, PanayotisYannakogeorgos (2014) gave in a spectrum of operations by cyber terrorists, which he divided into three steps:

a) Influence: It had a technical edge of the internet with some restrictions for cyber forums for which special training is required.

b) Planning: includes the hiring of special, skilled people and providing them with cut edge technology and massive funds as motivation to find the most appropriate target and plan the action to get the desired results.

c) Execution: Taking the action needed and making it a clean sweep so that they cannot be traced or caught.

Another important term attached to cyber terrorism is cyber warfare, defined by Sersan Brenner (2009) as *"the use of military operation by virtual means to achieve essentially the same ends they pursue through the use of conventional military force: achieving advantages over a competing nation-state or preventing a competing nation-state from achieving advantages over them."*

3.8 Cyberstalking: In its lifetime, if not much, an individual is Stalked openly or secretly. This increases if we talk about females and the cases here are open. With technology coming into play, stalking has gone virtual and is called Cyber Stalking. If talking about cyberstalking contents, we see actions like the following someone, watching over, coming into proximity, trying to contact, missed calls, blank calls, messages, emails, unwanted tags on social media. It is mature conduct but still an offence (Rahman, 2019). It came to light in 80's when such incidences were reported in the USA (Bocij, P 2004). In his research Michelle (2019) gave ways of cyberstalking as a) online sexual harassment, b) Mortification, c) Extortion of Money, d) Isolation of an individual, e) scaring. Thapa and Kumar (2011) gave a) email stalking, b) Computer stalking, c) Internet Stalking as types of cyberstalking.

3.9 Denial of Service attack (DDOS Attack): is the most popular way of hacking. It works by interrupting services and stops the running of networks successfully. The primary purpose is to take advantage of such system failure and hack into the system. Remember the Rio Olympics, the official website, and the Brazilian Sports ministry disclosed that 540 GPPS DDOS attacks took place during the event (Johnson Singh et al., 2016). DDOS attacks are tough to detect at the initial stages as it is at a minimal level. Server using HTTP and HTTPS protocols are both prone to these attacks (H. Beitollahi and G.Deconinch, 2012). In his study, Najafabadi et al. discussed the working of HTTP and how it is designed to look into and act on the request and response. It is like a filter which looks into working of communication as DDOS is the "distributed denial of Service" which are of the following types, a) Session Flooding Attack, b) Request Flooding Attack, c) Asymmetric Attack, d) Slow Response Attack (S.T. Zargar et al., 2013, T, Ni X et al., 2015)

3.10 Evil Twin: The use of WiFi has increased in the last decade, and open wireless available in public places. This has increased both the usage of WiFi and crimes related to it. Evil Twin is

also connected to WiFi, where the predators or hackers miss using the same opportunity. The predators either create a physical Access Point with a similar name and show the same signal name (Volker Roth et al., 2008). With the increase in open WiFi points, users, and an increase in Cyber Crimes, the need for stopping has also increased several hardware and software tools. (Fabian Lanze et al., 2015)

3.11 Fraud: It is a crime to deceive a person to take advantage of and gather vital and essential information. It can be by altering, stealing, destroying, or misusing the data.

3.12 Hacking: Most used for cybercrime of cyber-based criminal activity is Hacking. It is a process in which some partial or complete acquisition of specific functions within the system, network, or website. Yar (2006) said hacking is "to access and fraudulent misuse the information available on someone else Computer unauthorized" It all started as a fun and learning activity where new coders and IT Professionals did it to explore the potential and know how it all can be used. The hacking process is divided into different phases as a) gathering information, b) Finally entering and pulling it off. Hackers use every information from the system from the server to the system's make and configuration, so the action is full proof, and chances of getting caught are minimal. In case it is an organized group, the attack is massive, and the damage is inevitable.

3.13 Identity theft: Gupta C.M. and Kumar (2020) discussed how a small act of identity theft has taken this action and converted them into Big Financial Crimes, which significantly impacted the economy. A study conducted by economic times 2020 gave om some exciting facts about identity fraud in India, stating that four out of 10 Indians have been victims of identity theft, and 63% don't even know what action is to be taken in case of identity theft. When defined, identity theft is an illegal way of using someone else's identity and faking it to be yours to obtain undue advantage from the same. Virtually it is easier for the offenders to receive information of the victims from a vulnerable website, or sometimes such data is available for sale on the darknet. Identity theft can be divided into four types, a) Identity Cloning, b) Financial Identity, c) Criminal Identity Theft, d) Commercial Identity Theft. In this, cybercriminal steal virtual I.D.s of the individual such as UID, password, bank details, credit card or debit card details, and misuse them.

3.14 Key Logger: the system works when software or hardware is installed on a system that records every key pressed, and the data is recorded to be shared with criminals, compromising the security of the system. If used in a proper manner, it is used by parents to keep a check on

children. If hackers install the software in your system, which can be misused as the information on your system can be compromised (Tyagi et al., 2014) gave in a detection technique named Hook Scout and suggested that the user should always go for a license-based operating system.

3.15 Malvertising: To make a computer work, a combination of hardware and software is needed. This software is a set of instructions for the Computer for performing a specific job. When such software is made to work maliciously and used to damage, such is known as Malware. A prediction of electronic devices that are connected to the internet would reach 50 billion by 2020 (W.F.Forum, 2015), which has crossed and is expected to cross 1.3 million by 2023 (Nick. G 2020). The types of Malware explained by J.Mo (2015) are viruses, trojan horses, worms, keyloggers, adware, spammers, rootkits, script, etc. Sometimes it is done through websites that are usually filled with unnatural links and lucrative advertisements, often carrying malicious codes. When clicked, they guide the individual to fake websites that try to extract information or sometimes download malicious programs automatically.

3.16 Man, in Middle (Mit M) attack: The situation when an unwanted individual enters into the conversation of two without being detected or establishes a comfortable position between the two and intercepts is the situation of Man in Middle Cybercrime. The reason why that person is there is to get specific information what he is in for MiTM is an attack allows the interceptor to have control over the data received and sent for someone else for the usage of someone else or is for the person who is not meant to receive it without any information exchanged. Different abbreviations used are MITM, MitM, MiM (Khader & Lai, 2016; Tung et al, 2016; Wallace & Miller, 2017; Conti et al, 2016)

3.17 Phishing: An Act of tricking customers and attempting to extract their personal information from the virtual world such as debit/ Credit Card details, bank account details, email passwords. When received, such messages usually ask customers to update, change, confirm, or validate their information. Phishing is a two-step process where first, the company's data is stolen, and then the same is used against customers. This information to trap customers is frequently used on the social platform as it is easy to do and have less risk. It is done by sending bulk emails, and steps for it are, a) Setting up a fake identical website, b) Floating mail with a link to that website, and c) getting personal information during the process. The most challenging part is b & c. Points to be considered under phishing were given by (APWG 2013):

a. Social Media has a max phishing success rate, with 27% of total attacks being successful.

b. If we consider China's example, e-commerce sites are being more used and have a great success rate.
c. Top brands are being targeted as it has given more success percentage.
d. These only use the loopholes and pull up the crime.
e. The number of impacts and attacks has gone up with the usage of the internet.

As supported by Symantec Intelligence Report (2019), the number has gone up by nearly 25%.

3.18 Ransomeware: A malicious software, who's the main job is to encrypt or delete data and files stored on the system or online, making it impossible for the original owner to surf or use that data (Cadwlader& Toft, 2017). In the past few years, this ransomware has increased, and these attacks have become more frequent and brutal (Balogun, 2018). Luo & Liao (2017) gave the following file, which is attacked by ransomware txt, doc, zip, jpeg, ppt, pdf, Different types of Ransomeware are Crypto Ransomware, Locker Ransomeware.

3.19 Scamming: It is more of hardware and software in which computer repair, network troubleshooting, or any I.T. support services, forcing people to pay much money.

3.20 Screen Logger: these capture screenshots it depends on time intervals, mouse movements, or keystrokes. The process is remotely assessed without any knowledge of the individual.

3.21 Sniffer: involve activities like capturing, inspecting, interpreting, and decoding the information on a network to steal data are I.D., password, and personal details.

3.22 Social engineering: Involvement of humans, social engineering are considered very powerful as they impact the whole online and networking system. The prevention of such social engineering attacks can only be done by human interaction (Aroyo et al., 2018). It is an act where cybercriminals directly try to contact the individual on the phone or through email, or in person. They portray themselves as representatives of the company and try to extract information. Fake call centers and agents are the usual offenders in this.

3.23 Software Piracy: Torrents who do not know about them downloading software, movies, music, or books usually carry a price are software piracy.

3.24 Spamming: Technology and the Internet have given the user the ability to send a set of information to N number of people at a click of a button. When used positively, this can be used to share valuable information and be used to fool, making it spam mail. This option is also available in standard emails. The primary target of such bulk emails is to trap customers where

several price options for rock bottom prices, and some customers fall into that trap. In the process, the Phishers act so hard that the mail looks as genuine as possible as per a report by Kaspersky(2019) 19.8% from the last year 2018.

4. LEGAL FRAMEWORK OF INDIA TO CURB CYBERCRIME

With the increase in cybercrimes, the need for a specific law to govern is required, and a major one came in the year 2000, as the Information Technology Act 2000. Though this is the principal Act that governs every type of cybercrime in India. The major acts governing cybercrimes in India are as follows:

1. Information Technology Act 2000.
2. Indian Penal Code 1860
3. The Indian Evidence Act 1872
4. The Indian Telegraph Act 1985
5. Banker Book of Evidence Act 1891
6. Reserve Bank of India Act 1934
7. Intellectual Property Laws
8. Narcotics Drugs and Psychotropic Substances Act 1985: Online Sale of Drugs
9. Arms Act 1959: Online sale of Arms.

4.1 Legislations in India to curb the issue of cybercrime:

Sec 16 of the criminal procedure code (Cr.P.C) and sec 2 of the Indian penal code (IPC) in India defines the handling of different crimes, including the cybercrimes. Several manuals and operating procedures are suggested to investigate crimes giving in detail of power and limitations for the investigating officer (IO). While handling cybercrimes, which includes every crime defined under cyber law and the I.T. Act involving computers and the internet.

After a cybercrime is reported, a series of steps start right from the collection of evidence to investigation. In India, not every official who is working for the Investigating Agencies are not either equipped or have complete knowledge of the process. These officials are not even qualified to do the investigation, and that is the most significant barrier in the process. Special cybercrime police stations with trained and experts of the field in detection and investigation of cybercrime had to be hired. CERT-In (Indian Computer Emergency Response Team) and CDAC (Center for Development of Advanced Computing) have been set up to provide training to

professionals and Judiciary people so that evidence collected is understood and taken care of.

4.2 Jurisdiction:

It is one of the major and most talked about limitations in cybercrime due to the universal nature of the crime. It can be done from anywhere in the world, impacting anyone in the world. Sec 75 of the I.T. Act in India provides special powers and provisions in handling cybercrimes, which are outside the jurisdiction and allow the investigation officer (IO) to take help from the ones in which authority such cybercrime falls for collection of evidence to arresting of the offenders.

5. INVESTIGATION PROCESS OF CYBERCRIME

Investigation of a crime, right from the crime scene, to the collection of evidence, the investigation process, all of which is essential for cracking the case, makes this process a typical one. The process can be sub-divided into two parts a) pre-investigation assessment and b) standard operating procedure for investigation.

5.1 Pre-Investigation Assessment

Whenever a cybercrime gets reported, the investigating officer (IO) needs to do a pre-investigation assessment of each crime. Before the investigation of any case is initiated, there should be made a few attempts to keep things in mind and making every attempt to be safe. It depends on the nature and type of case reported that the I.O. has to collect the appropriate information from the victim, as part of the pre-investigation to get the best possible results from the same. A crime to be investigated should fulfill the following conditions, a) it should be defined U/S 43 of I.T. Act Amendment 2008 and, b) it should be done with an ill intention.

6. STANDARD OPERATING PROCEDURE FOR CYBER CRIME INVESTIGATION

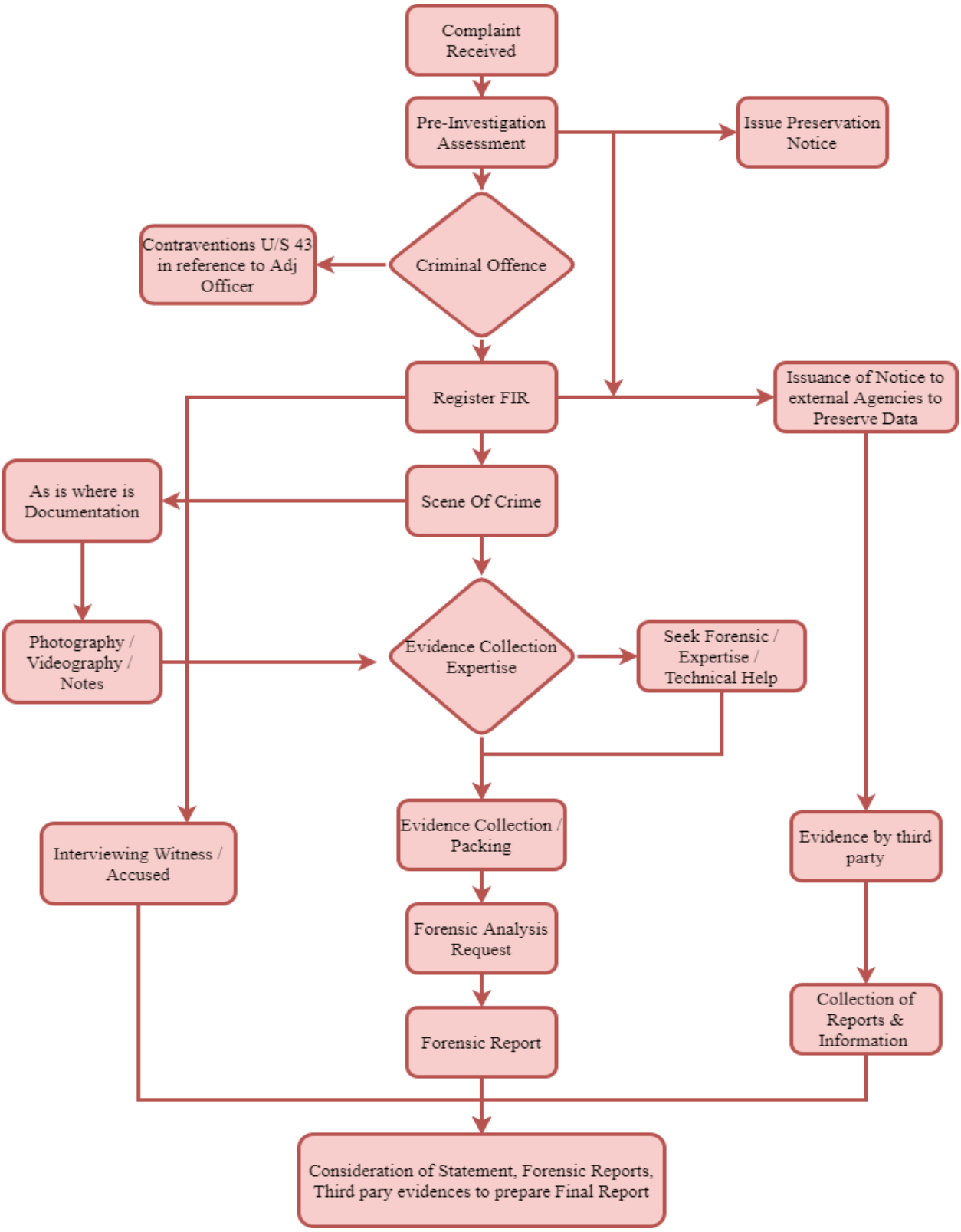
Cybercrime Scene is different from the traditional crime scene. Digital evidence is highly fragile and can be tampered easily. Proper care and precautions are taken during search, seizure, preservation, and examination of evidence. The steps which are commonly taken into account while cybercrime scene investigation is:

1. **Identification of crime scene**: The first step is to identify the exact location of the crime scene, which can be a house, a commonplace commonly known as cybercafé, and it can be a suitable environment wherein the crime takes place, which can be a work area.
2. **Securing the parameter**: Next is to ensure the area and take into account that nothing is touched or shifted till the time I.O. does not reach the place and take charge of the same.

3. **The clicking of photographs** at the crime scene and then documentation of the crime scene.: seizure memo (Panchanama) and seizure proceeding is the first step of the investigation. It is essential to keep every item and record each and everything that is seized in the process.
4. **Collection of evidence**, both switched on and switched off items. After the crime scene is clicked and secured, the I.O. and its team start working and collects different sources of evidence.
5. **Forensic duplication of data**: Once the digital evidence is collected, it is duplicated so that there is no problem with what to lose any data.
6. **Conducting interviews**: after the data is sent in for the forensic investigation, I.O. can question the victims and the offender along with every concerned party to the crime. The same is done to create and collect any detailed data required.
7. **Labeling and documentation of the evidence**: the items collected as a digital proof are labeled and documented to keep in a record the detail of every item taken into custody.
8. **Packaging and transportation of the evidence**: After documentation and labeling of the digital proof, they are carefully packed in the safe boxes and transported to the digital forensic unit for further actions.

International Research Journal of Commerce and Law
Volume 10 Issue 06, June 2022 ISSN: 2349-705X Impact Factor: 6.843
Journal Homepage: http://ijmr.net.in, Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

Standard Operating Procedure Of Cyber Investigation



1The Figure depicts the standard operating process for Cyber Investigation.

illustrated by the author 1

7. Sources of Digital Evidence

To unravel the truth behind crime evidence in favor or against work as an essential tool. In the case of cybercrime, the following are the primary sources of evidence:

1. Central Processing Unit
2. Screens (CRT, LCD, TFT), Printer, Scanner, Keyboard, Mouse
3. Smart cards, Biometric Readers
4. Answering Machines
5. Digital Cameras
6. Personal Digital Assistants
7. Storage devices (Hard Disk, CD, DVD, Memory Cards)
8. LAN, Servers, WiFi, Routers
9. Credit Card Skimmers
10. GPS.

8. CYBER FORENSICS

Cyber Forensics is an upcoming profession that allows the discovery of evidence by investigating the sources of digital evidence. This practice will help prosecute the offenders and provide justice to the victims. Rodney Meckemmish (1999) defined it as" the process of identifying, preserving, and presenting of digital evidence derived from various sources and by using different techniques which is admissible in the court of law." Cyber Forensics can be studied under sub-branches such as, disk forensics, malware forensics, network forensics, mobile device forensics, database forensics, wireless forensics, GPS forensics, memory forensics, email forensics, which help in revealing deleted files, recover and explains the facts, print the overall analysis. Cyber forensics usually have five elements, a) Identification and acquiring of digital evidence, b) Prevention and preservation of digital evidence, c) Analysis of the collected evidence, d) Reporting of the facts found, e) Presentation of the finding in the prescribed format in the court of law.

9. TOOLS OF CYBER CRIME DETECTION

Several methods are available to detect Cybercrimes. These methods can be broadly defined as Physical methods and electronic ones. Both have their importance; may it be hardware or software which are available. Whenever a digital investigation is done, both approaches are checked and worked on accordingly. It works on whether it is an investigation of internal resources or a study of a server breach; there are several tools, software, and techniques unique and specific for specific forensic analysis as memory, hard drive, image exploration, or mobile. Some commonly used tools are provided as under:

9.1 Fast bloc: is a software with a collection of standard tools to read and write on a drive or a memory disk attached to the Computer. It also enables us to drive data from the Disk attached to the system.

9.2 Enterprise: Commonly used as enterprise application software (EAS), is software usually used by professionals such as corporate houses, educational institutions, charitable trust, a government undertaking, and e-commerce giants, etc.

9.3 Encase: is known as an internationally recognized digital investigation tool, which is being used by cyber forensic experts for clean, smooth, productive, and efficient data collection, which can be used for expected details.

9.4 Forensic: As the name defines is a software for the forensic investigation which works on source code or binary code to analyze if data theft related to intellectual property has occurred. It is effectively and efficiently used to settle several trails and lawsuits associated with I.P.

9.5 Guidance Software is a software which provides endpoint detection and response (EDR), in several corporate and legal investigation of cybercrime.

9.6 SANS SIFT: Is SANS investigation forensic toolkit (SIFT) by UBUNTU in the form of a CD having a fleet of tools to unearth in-depth forensic investigation. It supports expert witness format, advanced forensic format (AFF), and RAW (dd) evidence formats.

9.7 Pro Discover Forensic: it is a security tool that allows locating as well as save all the data on a disk and create quality evidence reports for legal proceedings.

9.8 Volatility Framework: This is a work of black hat with the power to find data on RAM also, which is said to be highly volatile. It is a tool to give a live feed of investigation to investigators.

9.9 The Sleuth Kit (+ Autopsy): it allows the investigators to analyze and recover disk images and files. Its strength is to analyze volume and file system data.

9.10 CAINE: Computer-aided investigative environment is a Linux live CD, helps in report creation of data and images recovered on the network and mobile forensic.

9.11 Xplico: is majorly used for network forensics, which is used as a packet sniffer to extract web pages and contents, images with an exception to H.D. images and files, rest no limits to extraction.

9.12 X-Ways Forensic: This is an efficient and fast performer who finds deleted files and other information. It is a portable software that runs on a USB stick and works without installation.

10. DEFENSE MECHANISM AGAINST CYBERCRIME

Several procedures can be used to secure oneself from cybercrime or to detect crime if something happens. Several precautions right from proper hardware safety to licensed software benefit individuals as well as corporates. Taking proper precautions and changing settings and never sharing your passwords will always keep everyone a step ahead to save oneself from hackers' attacks. A few precautions which should be taken are as follows:

10.1 Airgap is a system developed to make a secure flow of data within two networks.

10.2 Antivirus is software installed to the detection of any malicious software or worm from entering into the system.

10.3 Content filtering System as filling of every file, web address, images, programs, software, and even application as per standard instructions.

10.4 Data loss prevention (DLP): it ensures the availability and restricts the usage of specific data to remain in said limits. Which makes it easy to secure the data and prohibit the leakage.

10.5 Digital Signatures: As provided to a single user, it keeps a record of the sender and receiver.

10.6 Electromagnetic Safety: If any attacks are made for data playback, tapping of devices set up on a specific network checked and worked upon. As a defense of the same, physical access to the said networks is stopped or minimized, by using tapping such attacks. Signal mixing or electromagnetic amplifiers are used to prevent such leakages.

10.7 Encryption Systems: data is first encrypted and then stared and shared to secure the same.

10.8 Firewall: It is an inbuilt network security device in almost every system which should be on always as it checks incoming and outgoing traffic on the network and decides whether to allow or block any suspicious traffic as per rules.

10.9 HoneyPot is a security mechanism for computers that detect and deflect a few if not all

counteract attacks or unauthorized entry or use of data.

10.10 Intrusion Detection/Prevention Systems (IDS/IPS): it is the process of examining every packet of information transfer over the network, whether it is coming in or going out.

10.11 NAC: These systems implement different security protocols for a said device or network, making it difficult to access.

10.12 Shorthand: here, usually, encryption of data is not done, but that is hidden in any other way or information.

10.13 Vulnerability Scanner: Programs such as n map, Nessus, the net probe should be used.

11. Conclusion

To conclude, it can be concluded that the advancement in technology is unavoidable, and with the improvement in technology, the criminals have also changed their ways of committing the crime. Thus, it is not only becoming the responsibility of the law agencies to deal with the issue, but the private organizations and the corporations should also change their mechanism to deal with the problem. There is a need for experts who have specialized knowledge of hardware and software, which can help fight with the criminals and also make the process of investigation effective. There is a need for continuous and updated education about cyberspace because of its dynamic nature; today's knowledge becomes obsolete tomorrow. Some of the measures which can be taken for preventing cybercrime can be, use of firewalls; it protects the users from unauthorized attacks while one is on the network.

Another thing that the users, especially the organizations or corporations, should do is the frequent change of passwords and virus check. Thus, to make the process and challenges faced in the process of investigation should be a combined effort. This effort is of the corporations, government, and the law agencies which are working hand in hand to make the online environment safe for the citizens.

References

1. Anti-Phishing Working Group (APWG), 2013. Global Phishing Survey: Trends and Domain Name Use in 1H2013. http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_1H2013.pdf
2. Aroyo, A.M.; Rea, F.; Sandini, G.; Sciutti, A. Trust and social engineering in human robot interaction: Willa robot make you disclose sensitive information, conform to its recommendations or gamble?IEEERobot.Autom. Lett.2018,3, 3701–3708

3. Bednar, A contextual integration of individual and organisational learning perspectives as part of I.S. analysis, Informing Science 3(3) (2000) 145-156
4. Bocij, P. (2004). Cyberstalking: Harassment in the Internet age and how to protect your family. Greenwood Publishing Group. www.praeger.com
5. C. Sorrells and L. Qian, "Quickest detection of denial-of-service attacks in cognitive wireless networks," International Journal of Network Security. 16, no. 6, pp. 468-476, 2014.
6. C.Y. Liu, C.H. Peng, and I.C. Lin, "A survey of botnet architecture and botnet detection techniques, "International Journal of Network Security, vol. 16, no. 2, pp. 81-89, 2014.
7. Cadwlader, W., & Taft, L. (2017). Wannacry Ransomware Attacks Should Be A Wake-Up Call for. Clients & Friends Memo, 1.
8. Conti, M., Dragoni, N., &Lesyk, V. (2016). A survey of man in the middle attacks. IEEE Communications Surveys & Tutorials, 18(3), 2027-2051
9. D. L. Shinder, M. Cross, Scene of the Cybercrime, Second Edition, Syngress, 2008.
10. D. S. Wall, "Cybercrime: The Transformation of Crime in the Information Age," Polity Press, 2007.
11. E. Casey, Digital Evidence and Computer Crime, Academic Press, 2004.
12. E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, Academic Press, pp. 41-46, 2000.
13. E. Casey, Handbook of Digital Forensics and Investigation, Academic Press, 2009.
14. E. Moulton, The Future of Cybercrime, Police Professional, 2008.
15. F. Carpine and S. Maria, "Online IRC Botnet Detection using a SOINN Classifier," pp. 1351–1356, 2013.
16. Fabian Lanze, Andriy Panchenko, Ignacio Ponce-Alcaidey, Thomas Engel, Hacker's Toolbox: Detecting Software-Based 802.11 Evil Twin Access Points, 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), Pg 225-232
17. General Inspector for Financial Information (GIFI, 2008). [Electronic version] (Information of the General Inspector of Financial Information on the execution of the Act of 16 November 2000 on Counteracting Introduction into Financial Circulation of Property Values Derived from Illegal or Undisclosed Sources and on Counteracting the Financing of Terrorism in 2007), Warsaw.

18. Gordon, S., Ford, R., 2006. On the definition and classification of cybercrime. J. Comput.Virol. 2 (1), 13–20.
19. Gupta, C.M. and Kumar, D. (2020), "Identity theft: a small step towards big financial crimes", *Journal of Financial Crime*, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/JFC-01-2020-0014
20. H. Beitollahi and G. Deconinck, "Analysing well-knowncountermeasures against distributed denial of serviceattacks," Computer Communications, vol. 35, no.11,pp. 1312–1332, 2012.
21. Hogan-Howe, Bernard, the Commissioner of Metropolitan Police, 2013. Met to Tackle the wave of cybercrime with 'world-leading unit' published in the Evening Standard, 21st November 2013. http://www.standard.co.uk/news/crime/commentary-sir-bernard-hoganhowe-on-new-cybercrime-push-8954716.html
22. https://digitpol.com/cybercrime-investigation/ accessed on April 20, 2020.
23. https://economictimes.indiatimes.com/tech/internet/4-in-10-indians-have-experienced-identity-theft-report/articleshow/75029916.cms?from=mdr accessed on 10/27/20
24. https://resources.infosecinstitute.com/7-best-computer-forensics-tools/#gref visited on 1/5/2020 at 9:17 PM.
25. https://securitytrails.com/blog/cyber-crime-investigation accessed on April 20, 2020.
26. https://www.cyberswachhtakendra.gov.in/ accessed on 10/27/20.
27. https://www.fbi.gov/investigate/cyber accessed on April 20, 2020
28. https://www.guidepostsolutions.com/investigations/cyber-investigations/ accessed on April 20, 2020
29. https://www.iacpcybercenter.org/officers/cyber-crime-investigations/ accessed on April 20, 2020
30. https://www.theinvestigators.co.nz/news/what-is-a-cyber-investigation/ accessed on April 20, 2020.
31. Ullah, N. Khan, and H. a. Aboalsamh, "Survey on botnet: Its architecture, detection, prevention and mitigation," 2013 10th IEEE Int. Conf. NETWORKING, Sens. Control, pp. 660–665, Apr. 2013.
32. J. Mo, "What Can We Learn from Anti-malware Naming Conventions?" 05 Nov 2015. [Online]. Available: https://www.opswat.com/blog/what-can-we-learn-anti-malware-naming-conventions.

33. J. Udhayan, T. Hamsapriya, "Statistical segregation method to minimise the false detections during DDoS attacks," International Journal of Network Security, vol. 13, no. 3, pp. 152-160, 2011.
34. Jahankhani, H., Al-Nemrat, A., 2010. Cybercrime. In: Jahankhani, et al. (Eds.), Handbook of Electronic Security and Digital Forensics. World Scientific, London, ISBN 9978-981-283-703-5.
35. Jahankhani, H., Al-Nemrat, A., 2011. Cybercrime Profiling and trend analysis. In: Akhgar, B., Yates, S. (Eds.), Intelligence Management, Knowledge Driven Frameworks for Combating Terrorism and Organised Crime. Springer, London, ISBN 978-1-4471-2139-8.
36. Johnson Singh, K.)ongam, and T. De, "Entropy-basedapplication layer DDoS attack detection using artificial neuralnetworks," Entropy, vol. 18, no. 10, p. 350, 2016
37. Jyoti Rattan and Vijay Rattan. (2017), "Cyber Laws & Information Technology" 47 Bharat law publishing, Calcutta, 6th edn
38. Kaspersky, 2019 https://go.kaspersky.com/rs/802-IJN-240/images/KSB_2019_Statistics_EN.pdf accessed on 10/26/20
39. Kemp, S. (2019, January 30). Digital 2019: Global Digital Overview. Retrieved from https://datareportal.com/reports/digital-2019-global-digital-overview?rq=Digital 2019: Global digital overview
40. Khader, A. S., & Lai, D. (2015). Preventing man-in-the-middle attack in Diffie-Hellman key exchange protocol. In 22nd International Conference on Telecommunications: ICT 2015(p. 204). Engineers Australia
41. M. Geva, A. Herzberg, Y. Gev, "Bandwidth distributed denial of service: Attacks and defenses," IEEE Security & Privacy, vol 1, pp. 54-61, 2014.
42. M. M. Najafabadi, T. M. Khoshgoftaar, C. Calvert, andC. Kemp, "User behavior anomaly detection for applicationlayerddos attacks," inProceedings of 2017 IEEE InternationalConference on Information Reuse and Integration (IRI), SanDiego, CA, USA, August 2017.
43. M. Subramanian, T. Angamuthu, "An autonomous framework for early detection of spoofed flooding attacks," International Journal of Network Security, vol. 10, no. 1, pp. 39-50, 2010.
44. M. Thapliyal, N. Garg, and A. Bijalwan, "Botnet Forensics : Survey and Research Challenges," no. April, 2013.
45. M. Yar, Cybercrime and Society, Sage Publishing Ltd, 2006.

46. M. Zahid, A. Belmekki, and A. Mezrioui, "A new architecture for detecting DDoS/brute forcing attack and destroying the botnet behind," 2012 Int. Conf. Multimed. Comput. Syst., pp. 899–903, May 2012
47. Magid, L. (2002, March 21).Net users can help fight child porn.Retrieved March 9, 2006, from http://www.pcanswer.com/articles/sjm_childporn.
48. Mansfield, Michelle. (2019). Illegal Stalking, Surveillance, and Non-Consensual Pornography.
49. Mckemmish, R. (1999) What is Forensic Computing? Trends and Issues in Crime and Criminal Justice.
50. Microsoft Security Intelligence Report, vol. 15, 2013.
51. N. Jeyanthi1, N. Ch. Sriman Narayana Iyengar, "An entropy-based approach to detect and distinguish DDoS attacks from ash crowds in VoIP networks," International Journal of Network Security, vol. 14, no. 5, pp. 257-269, 2012.
52. Nick G.2020," How many IoT Devices Are there in 2020", online https://techjury.net/blog/how-many-iot-devices-are-there/#gref
53. P. Hunton, "The growing phenomenon of crime and the Internet: a cybercrime execution and analysis model," Computer Law & Security Review, vol. 6, no. 6, pp. 528-535, 2009.
54. PA Yannakogeorgos, JII Geis.(2014), Rethinking the threat of Cyberterrorism", cyberterrorism, 43-62.
55. Patchin J. Cyberbullying Data – Cyberbullying Research Center. Cyberbullying Research Center. 2016. Available from: https://www.cyberbullying.org/2016-cyberbullying-data.
56. Paul Royal, Mitch Halpin, David Dagon, Robert Edmonds, and Wenke Lee. PolyUnpack: Automating the Hidden-Code Extraction of Unpack-Executing Malware. In The 22th Annual Computer Security Applications Conference (ACSAC 2006), Miami Beach, FL, December 2006.
57. R. A. Rodr, I. Omez, G. M. A-fern, and P. Garc, "Survey and Taxonomy of Botnet Research through Life-Cycle," vol. 45, no. 4, 2013.
58. R. P. Bryant, Investigating Digital Crime, Wiley, 2008.
59. Rahman, Khalid. Md. (2019). Anti-Stalking Legislation in Bangladesh. A New Frontier in Criminal Law Regime, pp. 1-23. Available from:

https://www.academia.edu/34984044/Anti-Stalking_Legislation_in_Bangladesh_A_New_Frontier_in_Criminal_Law_Regime .

60. Rowlingston, R., 2007. Towards a strategy for E-crime prevention. In: ICGeS Global eSecurity, Proceedings of the 3rd Annual International Conference, London, England, 18–20 April 2007, ISBN 978-0-9550008-4-3.
61. Smith PK, Del Barrio C, Tokunaga RS. Principles of Cyberbullying Research: Definitions, Measures, and Methodology. NYork/Londres: Routledge; 2013. Definitions of bullying and cyberbullying: How useful are the terms; pp. 26–40.
62. SW **Brenner**, M Rehberg - First Amend. L. Rev., (**2009**), "Kiddie Crime-The Utility of Criminal Law in Controlling Cyberbullying "HeinOnline.
63. Symantec, 2019. Intelligence Report: February 2019, https://usa.ingrammicro.com/cms/media/Documents/vendors/s/symantec/istr_24_es.pdf accessed on 10/26/20
64. T. Ni, X. Gu, H. Wang, and Y. Li, "Real-time detection ofapplication-layer DDoS attack using time series analysis," Journal of Control Science and Engineering, vol. 2013, pp. 1–6,2013.
65. Thapa, A., & Kumar, R. (2011). Cyber stalking: crime and challenge at the cyber space. An International Journal of Engineering Sciences, 4, 340-354
66. Troll Police: A Reality Show That Addresses the Issue of Cyber Bullying. 2018. Available from: https://www.mid-day.com/articles/troll-police-a-reality-show-that-addresses-the-issue-of-cyber-bullying/18916156 .
67. Tung, Y. C., Shin, K. G., & Kim, K. H. (2016, July). Analog man-in-the-middle attack against link-based packet source identification. In Proceedings of the 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing(pp. 331-340). ACM.
68. Tyagi, Gaurav, Khaleel Ahmad, and M. N. Doja. "A novel framework for password securing system from keylogger spyware", 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014.
69. V. Katos, P. Bednar, C. Welch, "Dealing with epistemic uncertainty in the SST framework, creativity, and innovation. Decision Making and Decision Support,", Decision Support Press, London, 2006, pp. 886-903.
70. Veng Mei Leong, A. (2007). Chasing dirty money: domestic and international measures against money laundering. Journal of Money Laundering Control, 10(2), 140-156.

71. Volker Roth, Wolfgang Polak and Eleanor Rieffel, "Simple and Effective Defense Against Evil Twin Access Points", 2008 ACM conference on Wireless network security, Pg. 220-235.
72. W. E. Forum, "Is this the future of the Internet of Things?" 27 Nov 2015. [Online]. Available: https://www.weforum.org/agenda/2015/11/is-this-future-of-the-internet-of-things/.
73. W. Jin, Z. Min, Y. Xiaolong, L. Keping, and X. Jie, "HTTP-sCAN: detecting HTTP-flooding attack by modeling multi-features of web browsing behavior from noisy web-logs," China Communications, vol. 12, no. 2, pp. 118–128, 2015
74. Wall, D., 2007. Hunting Shooting, and Phishing: New Cybercrime Challenges for Cybercanadians in The 21st Century. The ECCLES Centre for American Studies. http:// bl.uk/ecclescentre,2009.
75. Wall, D.S., 2005. The internet as a conduit for criminal activity. In: Pattavina, A. (Ed.), Information Technology and the Criminal Justice System. Sage Publications, USA, ISBN 0-7619-3019-1.
76. Wallace, Brian Michael, and Jonathan Wesley Miller. "Endpoint-based man in the middle attack detection using multiple types of detection tests." U.S. Patent 9,680,860, issued June 13, 2017.
77. Wilson, P., Kunz, M., 2004. Computer crime and computer fraud. Report to Montegmery County Criminal Justice Coordination Commission
78. Y. Chen, S. Das, P. Dhar, A. E. Saddik, A. Nayak, "Detecting and preventing IP-spoofed distributed DoS attacks," International Journal of Network Security, vol. 7, no. 1, pp. 69-80, 2008.
79. Y. S. Yen, I. L. Lin, A. Chang, "A study on digital forensics standard operation procedure for wireless cyber-crime," International Journal of Computer Engineering Science, vol. 2, no. 3, pp. 26-39, 2012.
80. Yar, M., 2006. Cybercrime and Society. Sage Publication Ltd, London.
81. Balogun, P. (2018, May 18). Solution to2017 WannaCry Ransomware Attack By Cyber Criminals. Retrieved from Academia: https://www.academia.edu/36712074/SOLUTION_TO_2017_WANNACRY_RANSOMWARE_ATTACKED_BY_CYBER_CRIMINALS
82. Luo, X., & Liao, Q. (2017). Awareness Education as the Key to Ransomware Prevention. Information Systems Security, 16(4), 195-202. doi:10.1080/10658980701576412