International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 03 | Mar 2021 www.irjet.net p-ISSN: 2395-0072

Study of Cybercrimes and Digital Forensics

Ms. Shambhavi A. Gupte[1], Dr. Pradnya Muley [2]

[1]Student, Masters of Computer Application Dept., P.E.S Modern Collage of Engineering, Pune, Maharashtra, India.
[2]Associate HOD, Masters of Computer Applications Department, P.E.S Modern Collage of Engineering, Pune Maharashtra, India
[1,2]P.E.S Modern Collage of Engineering, Savitribai Phule Pune University, Maharashtra, India.

Abstract - *With the innovations and constant development in technology the rate of cybercrimes is also on the rise. There is the potential for maximum of people to become victims to the growing pool of criminals. Digital forensics is an emerging technique that applies detection and investigation of computer based crimes and gathering digital evidences suitable for presentation in court.*

This paper provides foundational concept of cybercrimes and digital forensics in countering cybercrimes.

***Key Words*: Cybercrime, Digital Forensics, Cyber Forensics, Cyber-attack, Digital evidence.**

1. INTRODUCTION

Although the Internet brings people together than ever before, it also provides criminals with limitless opportunities to prey on others' weaknesses. Cybercrime is a criminal activity committed using computer to transmit, manipulate or illegally access the data. The computer crimes majorly involve hacking, extortion, money laundering, fraud, software pirating. The emergence of digital crimes has created a new branch of forensic science known as digital forensics. Digital forensics is research area that applies computer based crime investigation and gathering of digital evidence suitable for presentation in courts.

Digital forensics is the science of identifying, preserving, analyzing, documenting and presenting information and evidence gathered from electronic and digital devices. Security experts, academics, and law enforcement agencies use digital forensics to tackle the increasing number of cyber anomalies [5].

To collect digital evidence, such experts use scientific methods such as recognition, confirmation, analysis, and documentation on digital devices such as RAM, tablets, memory cards, floppy discs, and flash drives.

2. Cyber crimes

Cybercrime encompasses a wide range of crimes including stealing people's identity, fraud and financial crimes, selling contraband items, downloading illegal files etc. and any crime involving a computer and Internet is called cybercrime [2].

Types of cybercrime:

2.1 Malicious Code – Viruses, Worms and Trojans

2.1.1 Virus - A computer virus is a programme that infects a computer. It modifies the other computer programs when executed and replicates itself by modifying other computer programs and inserting its own code [6]. Not all viruses cause damage to its host. A virus is usually transmitted from one computer to another via e-mail or an infected disc. A virus, on the other hand, cannot infect another machine until the programme is completed [6]. A common method of virus execution is when a computer user is duped into opening a virus-infected file attached to an e-mail, believing the file is a harmless programme from a trustworthy source.

2.1.2 Worm - A computer worm is a self-replicating programme designed to spread to other computers. Usually spreads through computer network. For example, the loss caused by the I loveYou worm in 2001 was estimated to be $US 10.7 billion [6].

2.1.3 Trojan – Trojan is a kind of malware that looks useful but can cause serious damage to the system. In nutshell, it can mislead the users of its true intent.

Trojans can give the access to the criminals to spy on you, steal the information and manipulate your system

2.2 Cyber stalking

When a person is followed and pursued online, this is referred to as cyber stalking. Their privacy is invaded, their every move watched. It is a form of harassment, and can disrupt the life of the victim and leave them feeling very afraid and threatened [6].
Cyber stalking can be realtime or offline. The crimes caused due to cyber stalking may include threats, vandalism, identity theft, monitoring etc.

Stalker can be anyone, a stranger or a known person!

2.3 Phishing attack

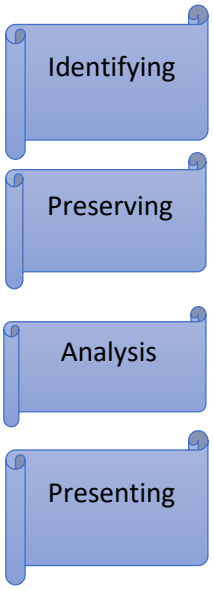
Phishing attack is a type of cybercrime where in the attacker can obtain sensitive information like usernames, passwords, credit card numbers, photos or other personal information. The attack can be carried out by email spoofing, messaging, fake sites.

2.4 Financial crimes

This would include cheating, credit card frauds, money laundering etc. [6].
Ransomware is a type of malware that encrypts the files of a victim. The attacker then demands a ransom from the victim in exchange for restoring access to the data[6].
Attackers may target universities because they have smaller security teams and a diverse user base that engages in a lot of file sharing, making it easier for them to breach their defences.

3. Digital Forensics

"Forensic computing is the process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable." (Rodney Mckemmish 1999)[9].



3.1 Identifying

It is the first step of digital forensics. This is the process of determining what evidence exists, where and how it is stored, and which operating system is being used. The sources to acquire data can be desktops, laptops, storage media, social media, routers, cell phones, digital camera, fitbits etc.

3.2 Preserving

After identifying and collecting the data from the sources, the data is preserved to maintain the integrity of the digital evidence. The data is copied on stable media like CD-ROM. The steps taken to investigate and preserve data are documented. If any change in the evidence are again modified in the document.

3.3 Analysis

The data extracted from the sources is reviewed and analyzed to draw conclusions.

Several decisions are taken out from the analysis. The conclusions drawn from the analyzed data can be used for further investigation and can be used to catch the criminal. The analyzed data is maintained in the report from.

3.4 Presenting

The analyzed data is collected to form a report. This report defines the way of crime occurred and sometimes accusations against the criminal. This process involves the process of presenting the evidence in the court. The presentation should be understandable to the jury as well as lay man.

4. Need of Digital Forensics

On the basis of above information about cybercrime and digital forensics one can say that the steps involved in digital forensics are important not only on security of lay man but also to other levels of security. The cybercrimes can affect the corporate world, defense forces and these breaches can be dreadful and threatening to the security of the country. Digital forensics not only used for investigation and finding the criminal but also to protect from further such attacks.

5. CONCLUSIONS

The digital forensics process is just like the process of investigating other non-digital crimes. The computer forensic needs and challenges can be accomplished only with the cooperation of the private, public, and international sectors [9]. Computer forensics has recently gained significant popularity with many local law enforcement agencies [3].

This paper explains the cybercrimes and digital forensic process. The first section of the paper explains the cybercrimes and types of cybercrimes. The second section explains the digital forensic process and how digital forensics is used to find the cybercrimes occurred and cyber criminals. Also, the need of digital forensics. In nutshell, the digital forensics plays an important role in cyber world.

REFERENCES

[1] A study of Cybercrime and perpetration of Cybercrime in India by Saurabh Mittal, Dr. Ashu Singh

Asia Pacific Institute of Management, New Delhi, India

[2] A Study on the Cyber - Crime and Cyber Criminals: A Global Problem

[3] Research and Review on Computer Forensics by Hong Guo, Bo Jin, and Daoli Huang

[4] Digital Forensics and Cyber Crime Datamining by K. K. Sindhu, B. B. Meshram

[5] Digital forensics in cyber security -recent trends, threats, and opportunities

[6] "CYBER CRIME CHANGING EVERYTHING – AN EMPIRICAL STUDY by Nilesh Jain

[7] Digital forensics- A technological revolution in forensic science by Antepreet Arora

[8] https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html

[9] Seminar Report on Computer Forensics - Faculty of engineering and technology RBS college, bichpuri , Agra