A Comparative Study of Digital Forensics and Cybercrime Investigation

Khalida Nadeem
Department of Criminology, Karachi University, Pakistan
Email: khalidanadeem579@gmail.com

Dr. Naima Saeed
Assistant Professor, Department of Criminology, Karachi University, Pakistan
Email: naimasaeed@uok.edu.pk

Nadeem Ahmed
System Administrator, Main Communication Network Department, Karachi University, Pakistan
Email: nadeem@uok.edu.pk

Abstract: With the Creation of the Universe, criminals have been there, since immemorial. Where it is good, there is bad, where there is a virtue, there is sin, when there are the people of justice, there are the trouble makers. According to the metamorphic equation “0=2”, every force or equation in the universe, no matter how complicated it is, sums up to 0. Similarly, with the development of technology, innovations were made to ease Human lifestyle and raise the standards of living; however, criminals were also utilizing those achievements for their own sinuous use. Thus, after the invention of Computers, came digital hoodlums. In order to counter them, security measures were taken by law enforcement agencies. Those were called cybersecurity; thus, the criminals were called cybercriminals. This study critically analyzes previous researches and sums up all the possible tactics used by cybercriminals in order to commit a crime, and how can we prevent it through investigation procedures and digital forensics is discussed.

Keywords: Cybercrime, Law, Digital forensic, Cybercriminals, Investigation, Digital Evidence.

Introduction:

With the advancement of technology, standards of living were improved. As we rode down the road of triumph, obstacles were met in form of people promoting sinuous activities and violence.

In the early age, it was done through robbing, bloodsheds, threats; however, as the time passed, people started using technology to perform criminal activities, and as the World is a “Global Village”, it started affecting “Not” an individual, but the world as a whole. Tactics were used by criminals in order to harm innocents “digitally”. These types of network attacks were called as cybercrimes.

For the sake of security and privacy, the aid from investigations and “digital forensic” was taken by the concerned authorities on the government level and defense systems were made to tackle the criminals which include;

---

1 Corresponding author
i. Cybercrime investigation procedure
ii. Digital evidence forensics process

Literature Review:

According to the metamorphic equation “0=2” (Morgue, 2020), all of the equations of the universe, no matter how complicated they are, sum up to 0. Conclusively, positive energy has to be neutralized by negative energy. Thus, with programmers, came hackers. Although not all hackers are cybercriminals, the intent is what makes them different. Moreover, it is not obliged that the crime is committed physically; you can also make an impact by attacking them ‘digitally’. This is what cybercriminals do. Is it only about messing with someone’s computer? Obviously NOT! Stealing personal or sensitive information, blackmailing, harassment, etc., are a few of the malicious crimes, among the long list of notorious activities which could greatly expand, if not worked upon. And as the new era would be of artificial intelligence (Hawkings, 2018), this could make someone’s hair curl and can lead to some serious consequences.

Cyberstalking, cyber harassment, spoofing, spamming, extortion, kidnapping, terrorism is a serious predicament, in Pakistan. In 2016 the “Prevention of Electronic Crime Act” was legislated by the government. It; undoubtedly, helped the Federal Investigation Agency (FIA) a ton. Yet at the same time, there were numerous blemishes. With no policy on cybercrime, no proper investigation techniques lack latest systems, experts in computer and digital forensics the problem still remains. The function of the academia, specialists, and military in battling cybercrime is unavoidable. Such problems should be dealt with on emergency basis while maintaining the equilibrium among cybersecurity and the rights of a citizen; or else, the former would go-phut, if it violates either the cybersecurity or national citizens (Islam et al., 2019).

Objectives of the Study:

i. To let the reader aware of the cybercriminals and the crimes committed.
ii. What techniques do they use to make their plans successful?
iii. What could be done in order to prevent it from occurring?

Origin of Cybercrime:

In the early 1970s, it was firstly reported when computerized phone systems became a target. Acumens of technology, known as “Phreakers” discovered the correct codes and tones, which resulted in free long distance service. They dug through Bell Telephone Company garbage to find superstitious information and performed countless experiments on early telephone hardware to learn how to exploit the system and steal long-distance telephone time.

Due to the lack of skilled investigators of technology at that time, computer systems were open to performing criminal activities and as the communication system got complexed, it invited more cybercriminals to commit a crime (Tech, 2020).

Cyber Criminals:

Those individuals or teams which use technology as a tool in overruling laws are categorized as cybercriminals. Such as stealing sensitive company’s data, and generating profit from it. (Micro, 2020). Rarely, cybercrime aims to damage computers for reasons other than
profit. These could be political or personal (Kaspersky, 2020). Cybercriminals are known to get to the cybercriminal secret business sectors found in the profound web to exchange malignant products and enterprises, for example, hacking apparatuses and stolen information. Cybercriminal black business sectors are known to represent considerable authority in specific items or administrations.

The laws on cybercrime have been evolving in countries across the globe; however, the law enforcers are constantly challenged in order to maintain privacy by finding, arresting, charging, and proving cybercrimes. Hacking is not really considered a cybercrime; in that capacity, not all hackers are cybercriminals. Cybercriminals hack and penetrate PC frameworks with pernicious plans, while programmers just try to discover new and inventive approaches to utilize a framework, be it for good or bad.

Cybercriminals additionally contrast incredibly from threat actors in a different manner, the first is intent. Threat actors are people who direct target assaults, which effectively seek after and bargain a target entity’s infrastructure. Cybercriminals are probably not going to zero in on a solitary entity; however, lead operations on broad masses of victims defined only by similar platform types, online behavior, or programs utilized. Furthermore, they vary in the way that they direct their operations. Threat Actors follow a six-venture process, which incorporates exploring targets and moving along the side inside a network. Cybercriminals, on the contrary, are probably not going to follow characterized steps to get what they need from their victims.

Note, in any case, if cybercriminals have likewise been known to receive targeted assault methodologies in their activities (Sun et al., n.d.).

Cybercrime:

The usage of ‘digital’ or ‘hi-tech’ equipment as a primary or secondary tool in order to perform a crime is categorized as cybercrime. It includes physical or mental harm to the victim, directly or indirectly, via modern technology (Islam et al., 2019). This equipment or technology includes Computers or the Internet. In this crime, digital evidence are collected, there is no fixed location, and the offender does not have to meet the victim directly. Therefore, the content of the cybercrime investigation procedure must contain the methods which include the finding of real perpetrators, digital evidence forensics, and analysis of crime. Likewise, the investigators aren’t restricted to utilize just a single technique in the cybercrime investigation, and they will exploit numerous strategies to gather proves and recognize the culprits as long as the techniques aren’t unlawful. Consequently, if these are proposed cybercrime examination strategies, they can be utilized to locate the genuine culprits, gather proves, and dissect the technique for cybercrime, so this method will be referred to and used by the agents. In the accompanying, we will depict the proposed cybercrime investigation procedures.

Types of Cybercrime:

Data theft is the most common cybercrime which takes place; however, it also includes other malicious activities, such as;

i. Hacking
ii. Cyberbullying,
iii. Phishing Scammers,
iv. Planting worms or viruses,
v. Social network fraud,
vi. Cyber extortion,
vii. Cyber Terrorists
viii. Child pornography,
ix. Identity theft,
x. Unauthorized system access.

Baits by Cybercriminals:

A number of tactics are used by cybercriminals to have access to personal and private networks. Some of the common techniques used are:

i. Botnet: A strategically developed network of bots that slither the backend of the web to spread malware with next to no recognition.

ii. Zombie Computer: A computer that is intentionally hacked by cybercriminals to access and/or assault a private network.

iii. Distributed Denial of Service (DDoS): With a DDoS assault, cybercriminals are not always looking to get information or access, rather are planning to shut a network down through an over-burden of junk data. An illustration of a DDoS assault happened on Friday, October 21, 2016, when cybercriminals shut down various profoundly used sites, including Twitter, Spotify, and Amazon.

iv. Metamorphic Malware: One of the most developed methods, metamorphic malware, consistently changes its code, making it very hard to distinguish by even the most exceptional anti-virus software. Specialists foresee that before the finish of 2017, there will be a development of malware that can invade networks, take data and conceal their activities. These types of malware will make it strenuous for government organizations and businesses to establish to the degree to which information has been altered; moreover, keep law enforcers from seeking after and indicting the offenders (Online, 2017).

How to prevent Cyber-attacks?

i. Network Encryption: A security protocol implemented at the network level which encrypts data, so network access is restricted to authorized computers.

ii. Proxies: A security strategy which interfaces clients to a remote location with the purpose of keeping their information and data encrypted. Proxies can permit clients the capacity to control their shared data so a potential hacker would acquire wrong or deluding information.

iii. Firewalls: A network wall which helps users prevent access from dangerous parties.

iv. Cyber Liability Insurance: Legitimate security that can protect a business or organization from risk, during a data breach. Cyber Liability Insurance has gotten significant with the expanding number of social security and stolen credit card numbers. Cybercrime has consistently become one of the drawbacks of mechanical progression. Cybercriminals are progressively utilizing first-class apparatuses and strategies to complete very well-planned assaults on the web. To help forestall and
ensure against future cybersecurity attacks, data security experts should adopt a comprehensive strategy to ensure their framework, joining countermeasures, for example, network encryption [protocols infographic], proxies, firewalls, and cyber liability insurance. Moreover, network safety professions ought to stay proactive in instructing themselves on the most recent strategies and innovations inside the business for overseeing cyber-attacks (Online, 2017).

v. **Keep Softwares, Operating Systems, and antiviruses updated:** Keeping the system updated would provide you access to the latest security patches, and would benefit your computer.

vi. **Use a strong Password:** To maintain security, strong passwords play a vital role. Ensure that you have a strong password so that, no one could break-in.

vii. **Do not open attachments from spam emails:** Most common way of getting a computer affected by malware attacks or other forms of cybercrime is through spam emails. **DO NOT** receive files from an unknown sender (Kaspersky, 2020).

**Law Enforcement:**

In 1990, during a venture named Operation Sundevil, FBI specialists seized around 40 PCs and more than 20,000 floppy disks that were purportedly being utilized by hoodlums for unlawful credit card use and telephone utilities. This two-year exertion included 150 specialists. In spite of the low number of prosecutions, the activity was viewed as an effective advertising exertion by law implementation authorities.

In spite of the fact that these were truly compelling, yet they are not generally great. In this way, botches by law-authorities may cause the general population to endure (Tech, 2020).

**Law in Pakistan:**

In 2002, Pakistan's First Law on Digital wrongdoing was ordered through Electronic Transactions Ordinance, which just tended to a couple of violations, as the fundamental reason for the Ordinance was to perceive and encourage reports, records, data, interchanges, and exchanges in electronic structure, and to accommodate the accreditation of affirmation specialist co-ops (Ullah, 2019).

On August 11, 2016, Pakistan's lower house, the National Assembly, passed a dubious cybercrime law called the Prevention of Electronic Crimes Act, 2016 (Ahmad, 2016):

> “Whoever intentionally and publicly exhibits or displays or transmits any information through any information system, which he knows to be false, and intimidates or harms the reputation or privacy of a natural person, shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to one million rupees or with both.”

**Digital Forensics:**

The process of preservation, identification, extraction, and documentation of computer evidence which can be used by the court of law, is known as Digital Forensics (Guru, 2020).

Digital Forensics helps the forensic team to analyzes, inspect, identifies, and preserve the digital evidence residing on various types of electronic devices. It provides the forensic team with the best tools and techniques to solve complicated digital-cases. It follows processes elaborated in Table 1 below:
Table 1: The process of digital forensic

<table>
<thead>
<tr>
<th>Process</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification</td>
<td>• Identify the purpose of the investigation</td>
</tr>
<tr>
<td></td>
<td>• Identify the resources required.</td>
</tr>
<tr>
<td>Preservation</td>
<td>• Data is isolate, secure and preserve.</td>
</tr>
<tr>
<td>Analysis</td>
<td>• Identify tools and techniques to use</td>
</tr>
<tr>
<td></td>
<td>• Process Data</td>
</tr>
<tr>
<td></td>
<td>• Interpret Analysis Results.</td>
</tr>
<tr>
<td>Documentation</td>
<td>• Documentation of the crime scene along with photographing, sketching, and crime-scene mapping.</td>
</tr>
<tr>
<td>Presentation</td>
<td>• Process of summarization and explanation of conclusions is done with the help to gather facts.</td>
</tr>
</tbody>
</table>

Origin of Digital Forensic:

With the invention of the internet, it has been acknowledged with both arms wide open; thus, the numbers of users are increasing rapidly, day-by-day. And due to this expansion, the frequency of digital attacks has increased. Consequently, effective methodologies and efficient tools were framed in order to detect those attacks and to prevent them from happening (Kaur, et al., 2016);

i. Hans Gross (1847 - 1915): First utilization of logical examination to head criminal examinations

ii. FBI (1932): Set up a lab to offer criminology administrations to all handle specialists and other law specialists over the USA.

iii. In 1978, the first PC crime was perceived in the Florida Computer Crime Act.

iv. Francis Galton (1982 - 1911): Conducted first recorded investigation of fingerprints

v. In 1992, the term Computer Forensics was utilized in scholarly writing.

vi. 1995, International Organization on Computer Evidence (IOCE) was shaped.

vii. In 2000, the First FBI Regional Computer Forensic Laboratory set up.

viii. In 2002, the Scientific Working Group on Digital Evidence (SWGDE) distributed the main book about advanced criminology called "Best practices for Computer Forensics".


Types of Digital Forensics:

i. Disk Forensics

ii. Network Forensics

iii. Wireless Forensics

iv. Database Forensics

v. Malware Forensics

---

2 Guru, 2020
vi. Email Forensics
vii. Memory Forensics
viii. Mobile Phone Forensics

Law:
“The Fourth Amendment Protection Act protects against unlawful search and seizure and serves as a deciding factor in all governmental investigations. Any evidence obtained in violation of the Fourth Amendment is inadmissible in a court of law. The Fourth Amendment does not apply to certain aspects of information access by law enforcement, such as information that is knowingly given to others, like on a shared drive. Private searches are not covered as well, and information found by private citizens, like computer technicians, is admissible in a court of law” (Lytle et al., 2018).

Investigation Procedures:
Judicial Systems vary in different countries. The purpose of these procedures is to investigate the facts of the crime, collect evidence, find the suspects, and arrest the suspects. Moreover, these cases are further divided into:

i. **Public Persecution**: The event that requires the victim to report the crime to police or the judiciary to accept the criminal case.

ii. **Private Persecution**: While in this, reporting of crime by the victim is not awaited, and judicial investigators can actively investigate on the case.

This classification will affect the investigation procedures. The beginning of the investigation must be legal; or else, it would not be accepted by the court after prosecution. If the beginning of the investigation is legal, the suspects would be distinct through the evidence of legal collection. Afterward, criminals are summoned and probed; innocents are released, while the criminals are arrested. And finally, the criminals are prosecuted (Sun et al., n.d.).

Digital Evidences:
Digital evidence is information stored or transmitted in binary form that may be relied on in court. It can be found on a computer hard drive, a mobile phone; among other places. Digital evidence is commonly associated with electronic crime or e-crime (Justice, 2020). Evidence is classified as:

i. **Witnesses**: It is the evidence which is personally experienced though, it does not include speculation. It includes victims, defendants or expert testimony.

ii. **Physical evidence**: It is evidence which can be used to prove the facts of the time. Such as the tool used to commit the crime.

iii. **Documentary evidence**: It is the evidence which refers to the content of the file. Such as written reports of the victim.

The witnesses might be changed with time or meddled by different variables and the actual proof and narrative proof is generally simple to leave the hints of alteration. Hence, under the typical conditions, the probative power (i.e. credibility) of physical and narrative proof is
higher than witness proof. Digital evidence is stored in data storage devices; generally, through the electromagnetic record type, and the content of digital evidence can be understood through printing, playing, and execution, etc. From the aforementioned, the digital evidence has both characteristics of physical evidence and documentary evidence. In addition, since the digital evidence exists by the electromagnetic record, it has the following features: easy to modify and copy, hard to understand the content directly without the conversion process, and not easy to retain its original state (Sun, et al., n.d.).

Analysis Model:

The investigation of the Cybercrime model is characterized by a Cybercrime Execution Stack in this paper. This model is influenced by three factors:

i. Criminal or Illicit intent
ii. Globalized Environment
iii. Evasion and Concealment

In the various nations, the Criminal or Illicit intent of cybercrime is specified in their own criminal law, and it will influence if the offense is established. The factor of Globalized Environment will influence the degree of offense in various nations. On the off chance that a cybercrime crosses a few regions of legal locale, the degree of offense might be extraordinary or disregard the various codes of law. Since the Internet has obscurity, the conduct of Evasion and Concealment in the crime will expand the trouble of criminal investigation and data assortment. Along these lines, the evasion and concealment of cybercrime; additionally, is one of the warmth factors in cybercrime investigation.

Cybercrime Execution Stack has 4 main stacks: Data Objectives, Exploitation Tactics, Example Attack Methods, and Networked Technology.

Data Objectives can be divided into groups: data collection, data supply, and distribution, and data use. The cybercrime tactics will be found out from the target type of attacks and criminal behavior. Therefore, in the Exploitation Tactics, it includes three groups: Attack Vectors, Social Engineering, and Illicit Collusion. In the above Exploitation Tactics, it can produce lots of different attack methods, and the Attack Vectors include malware, Trojans, spyware, worms or viruses; Social Engineering includes impersonation, email, phishing, blogs or social networking; Illicit Collusion includes private web- sites, email, Internet Relay Chat (IRC), Peer-to-Peer data sharing. Finally, Networked Technology is used to find and collect evidence and information on cybercrime. These technical characteristics are communication channels, network entry point, access device, network resources, and the infrastructure devices (Sun et al., n.d.).
Conclusion:

Prior motive of the study was to give the audience awareness of cybercrime and its hazards. All of its fundamentals are covered in detail to give proper information to reader. For it,

\(^3\) (Sun et al., n.d.).
other studies were critically analyzed and brought onto conclusion. It could be safely concluded that any crime, via digital interface as predominant or subordinate tool, is classified as cybercrime. And the committers of those crimes are called as cybercriminals, who mainly aim to either steal sensitive information or generate profit. Law enforcement agencies use investigation procedures and digital forensics to give the victims, the justice they deserve. It is done with the aid of digital evidences. It includes witnesses, physical evidence and documentary evidence. Among these, physical and documentary is given preference over witnesses as witnesses could play foul.

In order to avoid from being a victim of cybercrimes, systems should be updated, anti-viruses should be installed, strong passwords should be kept, and should avoid receiving any file from an unknown source. These are basic approaches, while the use of network encryption, proxies, firewalls, and cyber liability insurances would also be the icings on the cake.

References:


