Volume 15, April 2021 ISSN 2581-5504

"Cyber Forensic: A New Approach to Combat Cyber Crime[1,2]"

Shubham Maheshwari
Symbiosis Law School,
Hyderabad

****Navnidhi Sharma***
Symbiosis Law School,
Pune

ABSTRACT

With the development of Computers and Internet Technology, the digital crimes are also emerging .All variants of online communication like online chats, email system, various storage mediums i.e. clouds should be kept secure otherwise it will be easy for attackers to steal information like various passwords, credits and other bank credentials etc. Cyber forensics is a branch that combines both element of law and information technology together to collect and analyse data from source computers, networks and various storage devices in a particular format which is admissible in the court of law. This research paper discusses about various cyber forensics tools and techniques which helps in better investigation by drafting and creating hard admissible evidences in cases of cyber terrorism, cyber stalking, spams etc. Cyber forensics also helps investigating authorities to reveal criminal intent and this leads in the prevention of future cyber-crimes. , this paper also discusses five Standard phases of Computer forensic in cyber forensics all of the phases together helps during the investigation procedure and in revealing the investigation. It also discusses about various challenges faced by Cyber Forensics like lack of Standardization data formats slows down progress by which researching authorities are forced to spend more time in acquiring and preparing data. Hence, Cyber Forensics are required to adjust accordingly with new emerging technologies so can current way of investigation can be improvised. And lastly it could be suggested that selection of premium Forensics tools and techniques may aid in successful case resolving even after presence of certain hurdles arising from technology compatibility especially and limitation.

KEYWORDS: Cyber forensic, Cyber tools, Cyber technique, admissibility of evidence

INTRODUCTION

"Forensics is the application of science to the legal process."

In this global environment, the technology is proliferating which also requires to store a large number of information. Currently, every person is dependent on internet and they use it on their personal as well as public devices. This dependence on internet is leading to rapid

[1] Shubham Maheshwari, 5th year, Student, Symbiosis Law School, Hyderabad
[2] Navnidhi Sharma, 5th year, Student, Symbiosis Law School, Pune

increase in crimes. The crimes committed via computer is known as cybercrime or computer crime. Cyber forensic is a branch of Digital forensic science which is used for tackling these crimes.

Cybercrime is increasing at lightning fast speed in the current era. The computers are used from basic to international level such as, in agriculture to nuclear power are run by the computers. "The modern thief is more likely to steal with a machine than with a sword. The terrorist of tomorrow may be able to do more harm with a keyboard than with a bomb."[3]

Digital forensic is a branch of forensic science which is used to deal with the crime relating to computer, mobile phone and other such digital sources. The digital forensic has also been used by the law enforcement agencies, financial and investment companies.[4] The digital forensic is used for investigating and researching crimes related to above mentioned area. Thus, the digital forensic is used for combatting cybercrime.

Cyber forensic or computer forensic is the sub specie of digital forensic which is used to deal with the crimes originated from computer sources. It is used for investigating by a systematic process, by gathering, process and analyze the evidence to assist the ongoing investigation.

The objective of this paper is to show the tools and techniques used in assisting cybercrime and standard method of the investigation. This paper also discusses about the challenges faced by the cyber forensic investigator.

STATEMENT OF PROBLEM

Cyber forensic is more challenging as the techniques and form are continuously changing. Even after the amendment in the Information and Technology Act, 2000, Indian Evidence Act, 1872 and the Indian Penal Code, 1860 the admissibility of the evidence is questionable as well as the jurisdictional issue of the cybercrime as the crime can be done through any country to another or same country, if the crime is conducted through another country the problem arises. The problem arises as the IT Act does not deal with all types of problems and there is also lack of expertise and technique used by investigating officer because of which the concept is still a grey spot in Indian Legal System. The absence of the very same acts as a shield for the culprits and they are set free. The problem lies in the non-awareness of the people of making wrong doers liable for the act done by them. Thus, the current legal framework in needs to be looked as to arrive to a conclusion for determining to taking into consideration of dynamic nature of the crime.

METHODOLOGY

Doctrinal legal methodology will be used for carrying out this Research. Analytical method will be used to identify what law currently is and to evaluate its efficiency. Comparative method will be used to determine if the method of cyber forensic is applied for obtaining the

[3] Stefan Savage and Fred B. Schneider, *Security is Not a Commodity: The Road Forward for Cybersecurity Research*, CCC(Jan. 14,2021, 10:10 PM), http://www.cra.org/ccc/files/docs/init/Cybersecurity.Digital Forensic.html

[4] I. Resendez, P. Martinez, and J. Abraham, *An Introduction to Digital Forensics*, Research Gate (Jan 15, 2021, 6:00 PM),https://www.researchgate.net/publication/228864187_An_Introduction_to_Digital_Forensics

Volume 15, April 2021 ISSN 2581-5504

evidence hold the same kind of admissibility of evidence in the court as the physical documents.

The author has used doctrinal mode of legal research in this paper. The author used descriptive nature of research in this current paper. Not only it tries to describe the existing phenomena but efforts have also been made to study and investigate how things are happening and by doing that attempt have been made to gain insights and to be familiar with the issue being researched. Data sources are an important tool to identify the source of information.The author is fully reliant on the secondary sources for its data. The author based its information from reference books, professional journals, magazines, business news-papers, Government office, Published & unpublished thesis, Industry portable, Journal-articles, newspaper-articles. The author will also study and analyze important cyber forensic. The author also used applied mode of legal research in the conclusion for this paper. The author will also apply analytical mode of legal research in majority of its project. The paper will contain in-depth research and analysis about the various tools and techniques as well as challenges faced by cyber forensics.

LITERATURE REVIEW

B. Vanlalsiama and Nitesh Jha in their work **Cyber Forensic: Introducing A New Approach to Studying Cyber Forensic and Various Tools to Prevent Cybercrimes** (2019), they provide for an enhancement of current tools and technique for the purpose of finding the accurate layers for specialization, certification, and education within the cyber forensics domain. It also highlights the importance and need of Cyber forensics tools to increase its toughness and the ability to combat this persistent threats. They focuses on briefing of Cyber forensics, various phases of cyber forensics, handy tools which will helps in the finding and bring the intruders in the court of law for judgment.

B. V. Prasanthi, Prathyusha Kanakam and S Mahaboob Hussain in their work **Cyber Forensic Science to Diagnose Digital Crimes- A study** (2017) they explores the detailed explanation of existing digital forensics tools and its uses which assists to probe the evidence. They in order to investigate various type of digital fraudulent activities, provides various tools that focuses mostly on existing forensics tools which assist to increase the rate of protection and detection of attacks. The specific tools have its own features to extract evidence from digital data stored in a computer system.

Dr. Anjani Singh Tomar in her work **Cyber Forensics in Combating Cyber Crimes** (2014), she views that the process of acquiring, examining, and applying digital evidence is crucial to the success of prosecuting a cyber-criminal. To effectively combat cybercrime, greater emphasis must be placed in the computer forensic field of study. She also analyse the role of cyber forensics in combating with cybercrimes and use of various emerging tools in the field. She has also highlighted the evidence so collected by the specialist have to be handled and preserved in an appropriate manner, So that they can be produced before the court in its exact

Volume 15, April 2021 ISSN 2581-5504

manner. Any process or methodology breakdown in implementation of the cyber forensics will ultimately lead to jeopardize of the case.

Arunima S Kumar in her work **Cyber Forensics in Kerala** (2013) deals with the application of investigation and analysis techniques to gather and preserve evidence from a computing device in a method accepted by the court of law. She also stated that Mobile Device forensics is an evolving form of cyber forensics. New models of mobile phones are released every few months and thus its usage has also increased tremendously – both for good and bad purposes. This scenario poses new challenges for forensic examiners because acquiring tamper-free data from a mobile device is of great importance in crime investigations. She discusses the capabilities and shortcomings of the forensic tools under study and proposed an enhancement for the currently available tools, to make them a comprehensive set of tools with a set of features that combats a wide range of cyber and mobile device crimes.

Saswati Soumya Sahu in her work **Cyber Forensics: law and practice in India** (2014) stated the requirement techno-legal framework in cyber forensics area. She also discussed various case laws and current legal framework for combatting cybercrime. She also talks about regulatory framework for the effective investigation of the cyber-crimes, the need for uniformity in cyber security control and enforcement practices. Thus, cyber forensics, being a part of the wider enforcement mechanism needs to encapsulate the best practices to give meaning to every fair trial.

Shambhavi Tripathi in her work **Cyber Crimes: Classification and Cyber Forensics** (2019) distinguish between cybercrimes and traditional crimes as they may seem similar on the outside yet there are certain differences between the two, which separate one from another. She also speaks about various issues and to tackle these issues, cyber forensics is being actively used these days to deal with cybercrimes, investigate and collect digital evidence and catch cyber criminals.

David Mugisha is his work **ROLE AND IMPACT OF DIGITAL FORENSICS IN CYBER CRIME INVESTIGATIONS** (2019) talks about the ability law enforcement agencies to investigate and successfully prosecute criminals for these crimes are unclear. While law enforcement agencies have been conducting these investigations for many years, the previously published needs assessments all indicated that there is lack the training, tools, or staff to effectively conduct investigations with the volume or complexity included many of these cases. He mainly focused on Cybercrime and Global Economic Growth, Reasons for Conducting a Digital Forensic Investigation, Various Branches of Digital Forensics in details, Potential Source of Digital Evidence, standard operating procedure for digital evidence, Legal Aspects and What the Future Holds in the field of digital forensics.

Volume 15, April 2021 ISSN 2581-5504

TOOLS USED IN CYBER FORENSICS

The tools and techniques used by the cyber forensic analyst is to analyse the data whether encrypted, deleted or hidden. There are various types of tools and techniques which is used as per the given circumstances and nature of the case. The tools and techniques are used for the producing evidence and to further use the same in the court of law.[5]

1. **X-Ways Forensics:** It is a software which is used in windows, 32 Bit/ 64 Bit with a very detailed and flexible filtering search options and is customizable as per the nature and circumstances of the case. It is comparatively cheaper software and is highly efficient. This a windows based licensed software and portable in nature which can be used without installation anywhere.[6] It is mainly used for recovery of file from digital camera, corrupted file, deleted file, etc.
2. **SLEUTH KIT:** It is both used in UNIC and Window system which gives forensics a wide range to conduct investigation. It is mainly used in analyzing disk images, in-depth analysis of file system as well as recovery of same and also used in the autopsy.[7]
3. **SIFT (SANS Investigative Forensic Toolkit):** It is a multi-purpose toolkit which is embedded with the necessary tool required for investigation. It has guidelines which does not allowed the examined evidence to be changed via converting them into read only file. It has also malware analysis capabilities with indicator of compromise support. The one of best thing is it is free of cost and open source toolkit.[8]
4. **Encase:** It is multipurpose tool which is used to gather data from various devices and examine the evidence without altering the same which may be in form of active, latent and archival data. After analyzing the data it produces a report which can be used in the court of law. It also supports the encryption which is useful in securing data.[9]
5. **CAINE (Computer Aided Investigative Environment):** It is based on Ubuntu Linux while offering a complete integration of software and tools giving a semi-automated compilation report. It conduct investigation in 4 phases and also can be used in recovery of damaged files, virus embedded system, deleted files.[10]
6. **Forensic Toolkit (FTK):** It is used to examine the carious different information such as finding deleted mails, content strings, decrypting the encrypted information. It also

[5]Matthew N. O. Sadiku, Mahamadou Tembely, & Sarhan M. Musa, *Digital Forensics*, 7 INT'L J. ADV. RES. COMPUT SCI. SOFTW. ENG. 274, 274-276 (2017)

[6] Stefan Fleischmann, *X-Ways Software Technology AG*, X-WAYS (14 March 2021, 3:00 PM), http://www.x-ways.net/.html

[7] Brian carrier, *Open Source Digital Forensic*, SLEUTHKIT (14 March 2021, 04:00 AM), http://www.sleuthkit.org/

[8] Rob Lee, SANS Digital Forensics and Incident Response Cheat Sheets and Posters, SANS DFIR (14 March, 2021 01:00 PM), https://digital-forensics.sans.org/

[9] Patrick Dennis, *Encase Forensics*, OPENTEXT (14 March 2021, 01:00 AM), https://www.guidancesoftware.com/encase-forensic

[10] Giancarlo Giustini, Computer Forensic Linux Live Distro(14 March 2021, 01:00 AM), https://www.caine-live.net/

saves a digital image in various format and break into segments which can later on reconstructed.[11]

CYBER FORENSIC TECHNIQUES

1. **Cross-driven analysis**: It is a technique which is used by the investigator to gather information from various sources. This help in assisting the investigation by analyzing the huge data.
2. **Live Analysis**: It analyze computer while the system is running which is different from static analysis. It helps in evading the various encryption to find the data sources.
3. **Deleted file recovery:** It is a common technique which is used to recover the deleted files. It helps in finding other data which, might be helpful in investigation and is offered by various tools.[12]
4. **Stochastic Forensics:** It is used to identify the theft of the insider data. The insider data can only be accessed by someone who can do that as their official job. Thus, it is invisible to find which makes it hard to identify during investigation.
5. **Steganography:** It is a technique which is used to encrypt the message in a hidden form which is often go unnoticed. It is mainly used in the images, text, video, etc. by using dots or invisible ink. Thus, it makes harder to expose this message as the pattern is different each time as per nature and circumstances of case. But, if there is pattern in the hidden message, it will help investigators to spot the sources.[13]

STANDARD PHASES OF COMPUTER FORENSIC INVESTIGATION

The five standard step in the investigation of cyber forensic are:

1. **Policy and Procedure Development:** The specialist must follow procedures and protocols as provided by the law enforcement agencies for the investigation. There must be detailed planning done which need to be followed by the specialist on every aspect so that the authenticity of investigation can be proved.
2. **Evidence Assessment:** The specialist has to take into the account the type which it need to be sought before acquiring evidence. The different cases required different assessment as to the evidence needed for that crime. It is required to understand the case so that the specialist can create an efficient and effective manner to gather data sources.
3. **Evidence Acquisition:** It must be done carefully and legally so that it must be able to authenticate the document which is able to present the evidence in the court of law.

[11] Victor Limongelli, *Forensic Toolkit,* ACCESSDATA (14 March 2021, 02:00 PM), https://accessdata.com/products-services/forensic-toolkit-ftk

[12] Jim Lyle, *Digital Forensic,* NIST (14 March 2021, 02:00 PM), https://www.nist.gov/system/files/documents/2017/05/08/intro-to-digital-forensics.pdf

[13] Anjani Singh Tomar, *Cyber Forensics in Combating Cyber Crimes,* 3 PARIPEX - INDIAN J. RES. 70, 69-71 (2014)

The experts must collect and preserve the integrity of detailed data which must be properly planned and required to follow all the necessary guidelines.

4. **Evidence Examination:** It is done by analyzing the evidence by using a variety of methods with the help of tool and technique such as retrieving the deleted, encrypted files. The time, date and where the data was created or downloaded or made help to establish the timeline and help in deciding the information which can be utilized as evidence.
5. **Documentation and Reporting:** The specialist must fully document all the activity, method, storing, examining and assessing done by him and also the required protocols and procedures must be followed by him. This is the last step where the specialist provides with all the facts, investigation and his opinion on the matter to the authorities. It must give reliability and validity of the data which is used as an evidence.[14]

CHALLENGES FACED BY CYBER FORENSIC

The growth and development in the technology makes it a threat for existing methods of forensic science.[15] Some of the challenges are as follows:

- **Admissibility of evidence**

The main problem after the investigation is to prove the evidence in the court of law. There is also a problem in regard to the collection of the evidence due to the rapid enhancement of technology. There must be an expert to present the opinion on how the information is used while investigation.[16] The digital evidence is only admissible if it is proved that it is not tampered with, since it is most difficult as digital evidences can be tampered easily due to cybercrimes.

- **Advancement of Encryption**

The encryption is evolving with advancement of the technology which gives makes it difficult to decrypt the same for the specialist. As the encrypted messages contain important files which may be important to the case.[17]

- **Backlogs**

There is large backlog cases with cyber forensic analyst which makes it difficult for them to investigate every aspect which needs to be investigated to make the case more concrete by finding some other useful information.

[14] David Mugisha, *Role and impact of digital forensics in cyber-crime investigations*, 13 INT'L J. CYBER CRIMINOLOGY 45, 43-47 (2019)
[15] Diva Rai, *Cyber Crimes: Classification and Cyber Forensics*, IPLEADERS (14 March 2021, 12:00 AM), https://blog.ipleaders.in/cyber-crimes-classification-and-cyber-forensics.html
[16] EC-Council, *the role of cyber forensics in criminal offences*, EC-COUNCIL (14 March 2021, 01:00 AM), https://blog.eccouncil.org/the-role-of-cyber-forensics-in-criminal-offences/.html
[17] N. M. Karie & H. S. Venter, *Taxonomy of challenges for digital forensics*, 60 J. FORENSIC SCI. 890, 885-893 (2015)

Volume 15, April 2021 ISSN 2581-5504

- **Anti-forensics**

It is a method which hurdle the cyber forensic analyst to found data sources by manipulating it, disguising or even make it irrecoverable while examining the sources.[18]

- **Lack of standardization**

The rapid growth in the technology brings the problem in setting of standard and prepare as per that standard. Thus, it makes harder for forensic specialist to establish on the same standard. However, the NIST (National Institute of Standards and Technology) publish guidelines on the standardization of forensic investigation. But, for its effective use it needs to be updated regularly which creates hurdle for its effective use.[19]

ANALYSIS

The cyber forensic analyst has been emerged as a new approach for combatting cyber-crime. Thus, there is need for professionals to be kept updated and regular training which will help them in coping up with the difficulty of crime. There is need for conducting proper and adequate training so that cyber forensic analyst and investigator can be able to cope up with the crime from which the cyber-criminal may not be able to go free. There are various types of training such as three-day workshop, courses by companies, and specialized courses. These will help them to further able to get practical experience which will result in the efficient and optimum utilization of tool and techniques. The tools and techniques as discussed above are some of the leading tools and techniques which are used by various countries and are regularly updated.

The main problem arises after the thorough investigation is the evidence to be presented in the court. The most difficult part after the investigation and analysis is that the evidence must be related to the cyber-criminal. The training as discussed earlier also provide detailed study on this matter so that it will help them while investigating so that the evidence can be admissible in the court. The specialist is working with precision and with full confidentiality so that it cannot be jeopardised in providing the concrete and untampered evidence.[20]

The specialist after gathering all documents and details of the case and compiling it into the report to be presented in the court. They also need to testify as per the nature and the circumstances of the case in the court so that the court can understand all the technicalities and procedures adopted by the specialist.[21]

The other challenges as discussed above, can only be minimized by adequate training of the software and how to efficiently use them and change them according to the requirement. The

[18] S. L. Garfinkel, *Digital forensics research: The next 10 years*, 7 J. DIGIT. INVEST. S67, S64-S73 (2010)
[19] Jim Lyle, *Digital Forensic,* NIST (14 March 2021, 02:00 PM), https://www.nist.gov/system/files/documents/2017/05/08/intro-to-digital-forensics.pdf
[20] B.V. Prasanthi, Prathyusha Kanakam & S Mahaboob Hussain, *Cyber Forensic Science to Diagnose Digital Crimes- A study*, 5 INT'L J. COMPUT. 110, 107-113 (2017)
[21] Supra 12

Volume 15, April 2021 ISSN 2581-5504

NIST guidelines helps the specialist but it also acts as a constraint on them, as it is developed by them to meet the international as well as national requirements and also it is used by various other agencies.

CONCLUSION

The lightning fast paced growth of the technology plays a decisive role in the development of cyber forensic as well as cyber-crimes. The cyber forensic is emerging as a new way to combat cybercrime by using various tools and techniques. There are different companies, agencies and institutional sectors providing training, workshop and courses in cyber forensic to help them by updating them about various new software and optimum utilization of the same. There are experts to gather and collect the evidence by following general guidelines and giving his opinion after investigation as a concrete evidence in the court of law.

The growth in this sector is a dual edge sword which is beneficial for both the cyber forensic analyst as well as criminals. The specialist must not solely depend upon the tool as it has its own limitation and only the specialist by using his knowledge can get best out of that tool. The tool and techniques used by specialist must change as per assigned case, so that it will create room to gather extensive data which can be utilized as evidence.

BIBLIOGRAPHY

Research Articles

- B.V. Prasanthi, Prathyusha Kanakam & S Mahaboob Hussain, *Cyber Forensic Science to Diagnose Digital Crimes- A study*, 5 INT'L J. COMPUT. 107-113 (2017)
- Cameron S. D. Brown, *Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice*, 9 INT'L J. CYBER CRIMINOLOGY 55- 119 (2015)
- David Mugisha, *Role and impact of digital forensics in cyber-crime investigations*, 13 INT'L J. CYBER CRIMINOLOGY 43-47 (2019)
- Anjani Singh Tomar, *Cyber Forensics in Combating Cyber Crimes*, 3 PARIPEX - INDIAN J. RES. 69-71 (2014)
- Matthew N. O. Sadiku, Mahamadou Tembely, & Sarhan M. Musa, *Digital Forensics*, 7 INT'L J. ADV. RES. COMPUT SCI. SOFTW. ENG. 274-276 (2017)
- M. Losavio, K. C. Seigfried-Spellar, & J. Sloan III, *Why digital forensics is not a profession and how it can become one*, 29 CRIM. JUSTICE STUD. 143-162 (2016)
- N. M. Karie & H. S. Venter, *Taxonomy of challenges for digital forensics*, 60 J. FORENSIC SCI. 885-893 (2015)
- Pankaj Gupta, Jaspal Singh, Anterpreet Kaur Arora & Shashi Mahajan, *Digital Forensics- A Technological Revolution in Forensic Sciences*, 33 J INDIAN ACAD FORENSIC MED. 166-170 (2011)
- S. L. Garfinkel, *Digital forensics research: The next 10 years*, 7 J. DIGIT. INVEST. S64-S73 (2010)

Volume 15, April 2021 ISSN 2581-5504

Internet Sources

- Brian carrier, *Open Source Digital Forensic*, SLEUTHKIT (14 March 2021, 04:00 AM), http://www.sleuthkit.org/
- Diva Rai, *Cyber Crimes: Classification and Cyber Forensics,* IPLEADERS (14 March 2021, 12:00 AM), https://blog.ipleaders.in/cyber-crimes-classification-and-cyber-forensics.html
- EC-Council, *the role of cyber forensics in criminal offences,* EC-COUNCIL (14 March 2021, 01:00 AM), https://blog.eccouncil.org/the-role-of-cyber-forensics-in-criminal-offences/.html
- Giancarlo Giustini, *Computer Forensic Linux Live Distro*, CAINE (14 March 2021, 01:00 AM), https://www.caine-live.net/
- I. Resendez, P. Martinez & J. Abraham, *An Introduction to Digital Forensics,* Research Gate (Jan 15, 2021, 6:00 PM), https://www.researchgate.net/publication/228864187_An_Introduction_to_Digital_Forensics
- Jim Lyle, *Digital Forensic*, NIST (14 March 2021, 02:00 PM), https://www.nist.gov/system/files/documents/2017/05/08/intro-to-digital-forensics.pdf
- Patrick Dennis, *Encase Forensics,* OPENTEXT (14 March 2021, 01:00 AM), https://www.guidancesoftware.com/encase-forensic
- Rob Lee, *SANS Digital Forensics and Incident Response Cheat Sheets and Posters*, SANS DFIR (14 March, 2020 01:00 PM), https://digital-forensics.sans.org/
- Scott R. Ellis, *Cyber Forensics,* SCIENCEDIRECT (14 March 2021, 01:00 AM), https://www.sciencedirect.com/topscience/cyber-forensics.html
- Stefan Fleischmann, *X-Ways Software Technology AG*, X-WAYS (14 March 2021, 3:00 PM), http://www.x-ways.net/.html
- Stefan Savage & Fred B. Schneider, *Security is Not a Commodity: The Road Forward for Cybersecurity Research,* CCC (Jan. 14, 2021, 10:10 PM), http://www.cra.org/ccc/files/docs/init/Cybersecurity.Digital Forensic.html
- Victor Limongelli, *Forensic Toolkit,* ACCESSDATA (14 March 2021, 02:00 PM), https://accessdata.com/products-services/forensic-toolkit-ftk