# CYBER FORENSIC: AN INSIGHT TO ITS GENERAL PRINCIPLES AND EXPANSE

Jacob Reji Olaserimannil* & Parvathy Manoj**

**Abstract**

*These days, cybercrimes have increased considerably due to the tremendous advance in science and technology. The need to detect, combat and restrict such crimes are well facilitated by cyber forensics, which focuses mainly on identifying, preserving, analyzing and presenting digital evidence in a manner that is legally accepted using various methods of forensic analysis, namely network, disk, and device forensic. It is aimed at procuring the evidence of crime committed, preventing its further occurrence, presenting the evidence before the court of law and prohibiting in the future any kind of similar fraudulent activities. In this article we will discuss the need, prime objectives, tools for cyber forensics and the areas where forensic investigations can be initiated with an in depth discussion on network forensics, meta data, live-box and dead box forensics.*

***Keywords:*** Cyber Crime, Cyber Forensic, Router Log, Network Forensic, Meta data

* Student-B.B.A.LL.B.

** Student-B.B.A.LL.B.

## INTRODUCTION

With the advent of science and technology, the 21st century man has progressed to an extent which was unimaginable 10-15 years back. All the qualifying phrases get prefixed before the word 'man' because of the advent of science and technology. None are the needs today that he can't program and nothing sets a boundary to his imaginations. When all these technological progress are aimed at the betterment of the society, it cannot be ignored that they are used against the society too. The scope of anti-socials to harm the society is now limitless.

Today, Internet has become a way of life for millions and also a way of living, due to its rapid advent. Thus, with the increase in the use of internet and dependency of individuals in almost all fields, a number of new crimes related to computer and internet have evolved in the society. Technology coupled with internet serves both as a benefit to mankind and as a developed platform for crimes to be initiated against society using new and highly sophisticated tools.

Anything related to computer, information technology and virtual reality is collectively termed as 'cyber' and the crimes done with the use of computers coupled with internet as 'cybercrimes'. Hence in the strictest legal parlance, the usage of apt forensic tools and technical knowledge to recover the electronic evidence within the contours of the rules of evidence, for it to be admissible before the court of law can be defined as cyber forensics[1].

Due to the high and exponential growth of Internet, crime rate has also raised up and legal institutions face very serious questions not only about regulating the internet, but also whether it could be regulated and what were the premises in which such criminal activities have taken place.

Traditionally Information Technology infrastructure was used to commit crimes, but with the change in scenario they are now the very target of crime. Examples such as defamation, pornography, sexual harassment, threatening e-mails, SPAM and phishing depicts computers

[1] Santanam , Raghu , *Cyber Security, Cyber Crime ad Cyber Forensics: Applications and Perspctives*, idea Group Inc, December 2010.

as a means to commit crime, when viruses, worms, industrial espionage, software piracy and hacking are examples where computers are the targets of crime[2].

There are two sides to every cybercrime. First, the generation side and second the victimization side. When the reconciliation aspect is taken into consideration, the number of cybercrimes should be related to the number of victimizations experienced. However equal number of correspondence won't be found often as the number of victims for a single cybercrime may be more than one or some may not even result in the same.

The threat of cybercrime should never be viewed from the narrow periscope of statistics; the scenario should be understood from a much wider montage. It is becoming an ever growing dangerous threat landscape, money laundering, terrorist activities, government offices and classified documents are at stake. It is no more a scene of an amateur hacker logging into his friend's e-mail account. Intentions are taking much deeper anti-social roots.

## NEED FOR CYBER FORENSIC

'Forensic' broadly means "relating to or denoting the application of scientific methods and techniques to the investigation of crime". This can be considered a vital process with respect to investigation of any criminal activity as, even if it is for finding out and punishing the wrongdoer or preventing a future criminal activity of the same sort from taking place, the means of commission of the offence should be brought to light. And the very method of applying scientific analysis in a legal context can be termed as forensic science. However not all forensic are done to investigate crimes or present evidences in court; sometimes companies firms or organizations need to do forensic analysis for internal purposes ranging from increasing security, investigations, data recovery so on so forth. Thus, it is the technological and systemic investigation of the computer system for evidence or for supportive evidence of a civil or criminal wrong or a criminal act committed[3].

"Cyber forensics" [4]is the unique process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally accepted. Like any forensic analysis the branch of

[2] Dr. B. Muthukumaran, *Cyber Crime Scenario In India*, Criminal Investigation Department Review, January 2008.

[3] P Tomar, B Rai, L Kharb, *New vision of Computer Forensic Science: Need of Cyber Crime Law* , The International Journal of Law, Healthcare and Ethics, Volume 4, No.2

[4] Albert Marcella, Jr., Robert S. Greenfield, *Cyber Forensics: A field Manual for Collecting, Examining and Preserving Evidence of Computer Crimes*, CRC Press, January 2002

cyber forensics deals with collecting evidences regarding the cybercrime and try to unfold the event happened and brings to light whoever is responsible for it .Ever since technology and internet has taken over a ubiquitous role in our daily lives and the cyber realm is expanding. It does play a role in all criminal activities be cyber or not (Examples.1 You try to hack into a government server; the investigators can identify you by tracking the IP address.2. A plans to murder B. Sends a text message to C notifying him of the plan. Investigators can very well decode the text and use it as evidence against him). Thus the branch of cyber forensics of a country has to be well equipped with recent developments and technically sophisticated so as to crack all types of threats posed by the cyber criminals.[5]

The reality of the information era is having a significant impact on the legal establishments. Just simple collection of evidences of the activity using technical expertise will not get the case solved; it has to be legally admissible. Thus cyber forensic is the application of technical as well as legal interpretation into the evidences acquired. So how can investigation team make evidence admissible in court-:

1. The cyber crime investigators must be skilled competent professionals. This is essential so that they can properly conduct the investigation, collect the relevant evidences and instill confidence in the court about the admissibility of the evidence.

2. The original digital evidence must never be tampered with or altered. As far as practical, investigators must work on the image/clone of the original evidence. If that is not practical then extreme care and caution must be taken while working on the original evidence.

3. A detailed and accurate audit trail must be maintained. The chain of custody forms and other audit trail documents must be meticulously maintained. Any lacuna in these documents casts suspicion on the entire findings of the investigation.[6]

The Cyber forensic is not only useful in solving cybercrimes but also other anti-social and criminal activities like murder, terrorism, tax evasion, drug smuggling and the list goes on.

The need of cyber forensic can be construed into a three P need mix:-

[5] Bill Nelson, Amelia Philips, Christopher Stuart, *Guide to computer Forensics and Investigations*, Cengage Learning, September 2009.
[6] Dr. Swati Mehta, *Cyber Forensics and Admissibility of Digital Evidence*, SCC Journal Section , volume 5 (2011) pg 54.

1. Procuring evidence- The foremost and important step of gathering and analyzing of evidence of cybercrime committed falls under the first aspect procuring of evidence.

2. Prevention- Prevention of a similar attempt of activity by means of cyber tools in the future needs to be done, for which forensics has the most crucial role to play.

3. Presentation of evidences-Presentation the procured evidences in court by drawing conclusion by scientific methods. Courts till date are highly dependent on human witnesses, therefore in order to take the evidence into consideration it must presented in manner accepted by the legal system.

4. Prohibition- Prohibition of sites, blogs, activities, use etc of cyber tools which has proven fatal to interest of the society should be undertaken. Forensics helps in establishing the nexus between the prohibited elements to the offence that has been taken place.

When people's area of activity shifts, criminal activities also shift to the same area. Cyber-crimes can be classified into three types; (1) Crimes directed against the computer (2) Crimes where the computer contain evidences and (3) Crimes where computer is used along with diverse technical tools to commit the crime. Therefore what is then done by the forensic experts is identifying, collecting and preserving evidences from disk, systems, networks and other peripheral components for the 4P mix.

## OBJECTIVES OF CYBER FORENSIC

Cybercrime is among the top five underworld activities in the world. The objectives can be termed as the 6 A'S of Cyber forensics[7] namely

- Assessment- Understanding the premises in which the activity as taken place as well as understanding the nature and scope of the incident
- Acquisition- Acquiring as much as of possible evidences of the incident occurred
- Authentication-Validating and verifying the evidence that has been acquired.
- Analysis-This phase involves the deep understanding of the incident and analysis of the same using tools and techniques.

[7] N. Sridhar , Dr.D.Lalitha Bhaskar, Dr.P.S.Avadhani, *Plethora of Cyber Forensics*, International Journal of Advanced Computer Science and Applications, Vol. 2, 2011, pg 111-114

- Articulation- Writing a report in association with the legal provisions in a clear concise manner.
- Archival- Preservation of all the evidences and record in a secure manner of future references and moreover for taking preventive measures or steps.[8]

## AREAS OF CYBER FORENSIC

Due to its vast extent, Cyber forensics can be divided into;

1. *Network Forensics*- Network forensics is the capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents. It helps in identifying unauthorized access to computer system, and searches for evidence in case of such an occurrence. Network forensics is the ability to investigate, at a network level, things taking place or that have taken place across an IT system.

2. *Disk forensics* - Disk Forensics is the process of scientifically collecting and extracting digital evidence from storage media like Hard disk, USB devices, Fire wire devices, CD, DVD, Flash drives, Floppy disks, etc.

3. *Device forensics* - Device Forensics is the science of gathering digital evidence available in different types of devices such as mobile phones, PDA, iPod, printers, scanners, camera, fax machines, etc.

4. *Peripheral forensics* - This branch is related to forensics on peripheral devices like printers, scanners, plotters etc. [9]

Being of prime importance, network forensic requires detailed discussion.[10]

## NETWORK FORENSICS

The concept of network forensics deals with the data found across a network connection mostly ingress and egress traffic from one host to another. Network Forensics analyzes the traffic from one host to another, the traffic data logged through firewalls or intrusion

[8] K.K Mookhey , *Cyber Crime And Digital Forensics*,.
[9] Mohd Mustafa Choudhary, *Cyber Forensics and Area of Focus,* Tata Consultancy Services White Paper , pg 6-14
[10] www.cyberlawsindia.net/computer-forensics.html; (accessed on 6th march 2015)

detection systems or at network devices like routers[11]. The goal is to trace back the source of the attack so that the cyber criminals are prosecuted.

Technically Network Forensics can be defined as "*the use of scientifically proven techniques to collect, fuse, identify, examine, correlate, analyze, and document digital evidence from multiple, activiely processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities*".[12] Simplified, it uses scientific techniques to collect evidence from different digital sources to uncover the unscrupulous activities that occur in the cyber space.[13]

The large number of incidents affecting different organizations has paved way for extending the technique of forensic analysis towards networks. This branch of forensics monitors network traffic and checks for any anomalies in the traffic and ascertain whether there is any indication of an attack. If so, the nature of attack is being analyzed and network traffic is captured, preserved, analyzed and necessary action is taken in response.[14] It is always desired by the intruder to keep his path of intrusion a mystery. But, with network forensics no such pathways remain a mystery.

*What involves network forensics?*

Unlike other digital forensics, network forensics deal with volatile and dynamic information. For example, if both ends of firewall are monitored, then one can easily get closer to the addresses and understand what was visited, when it was visited, and also the nature of site visited. Now, such findings will prove useful in an investigation to trace back the activities of the accused and prove his guilt or innocence.

Now how is the volatile information obtained; The devices or tools of Network Forensic captures the information packets exchanged across a network and keep a repository of the

[11] Rajdeep Niyogi, R.C. Joshi, Emmanuel S.Pilli , *A Generic Framework of Network Forensics*, , International Journal of Computer Applications (0975-8887) Volume 1- No. 11.

[12] Palmer G., *A Road Map for Digital Forensic Research*, 1st Digital Forensic Workshop 2001. New York, 2001pg 15-30.

[13] Natarajan Meghanathan, Sumanth Reddy Allam and Loretta A. Moore, *Tools and Techniques for Network Forensics*, International Journal of Network Security & Its Applications (IJNSA), Vol .1.April 2009, pg 14-25

[14] N. Sridhar , Dr.D.Lalitha Bhaskar, Dr.P.S.Avadhani, *Plethora of Cyber Forensics*, International Journal of Advanced Computer Science and Applications, Vol. 2, 2011, pg 111-114

same in an inbuilt or attached storage. The Network Interface Card (NIC) of these devices is configured in Promiscuous Mode, Which allows it to sniff all the packets in full packet capture mode. These devices generally keep the data in two formats, RAW packets and statistics or Meta Data. Meta data is data about data. It is the structured data which describes the characteristics of a resource. The Meta Data[15] is of two types, namely – structural Meta data and descriptive Meta Data. Structural Meta data simply means 'data about containers of data' this is because when the data structure is designed, such an application do not have any actual data in it. Now, the descriptive Meta data contains the "data about the data". They have samples of the data of the application and also the content of such data. Meta data offers a forensic investigator, a lot of useful information. They can trace down the original owner in case the investigation is regarding sale of unsuitable material or identify why the device was turned on and off frequently in case of a murder investigation and so on.

## META DATA; REAL LIFE FORENSIC CASES

- The BTK Killer

Dennis Rader, also well-known as the BTK killer, which stands for bind, torture, and kill, started his killing chain in 1974 in Wichita, Kansas. He continued to live a deceiving life of a married father of two children and president of church until his arrest in 2005. He was responsible for 10 murders. There were DNA evidence and also a witness left at the crime scenes but the police and law enforcement were not able to capture him until 2005. After 30 years of deceiving life his murder chain ended in 2005 due to his casualness and lack of knowledge of computer forensic. He sent an email to a Wichita TV station about his crime. After inspecting the file, police and forensic experts were able to identify the author, Dennis and the organization, Christ Lutheran Church, from the metadata involved in file. Upon more investigation more details about the church, forensic experts were able to discover Dennis Rader, who was the president of the church[16]

- *Merck Report*

Merck is a pharmaceutical company which has been involved in various charges related to its arthritis drug medication. In 2005, important information regarding the medication's danger

[15] *An introduction to computer forensics*, Information Security and Forensics Society (ISFS) , April 2004, pg 6
[16] www.acsupport.europe.umuc.edu/~sdean/ProfPaps/Bo_wie/S09/Blakeslee.pdf , *Use of computer forensics technology crime investigation*, Hyechin Blakeslee,

of causing heart attacks was deleted from a document sent by Merck was discovered by the New England Journal of Medicine. The track changes feature was used by the Merck while preparing the informational paper to be sent to the journal. The authors at Merck did not remember to accept the changes made to the original document and therefore released the document with all the metadata intact. Upon detail inspection, the Journal discovered the deleted text and after that released the information regarding the Merck's blunder[17]

To keep data history for backward analysis and Network Behaviour Analysis and Detection (NBAD) is a mandate to perform investigations and to understand the network behavior.

With increasing bandwidth usage and high speed networks going up more than 20 Gbps or more, it has become a challenge to record data.[18] However improvised methods to overcome this are being developed.

- Types of Network Forensic Systems.

1. *Catch-it-as-you-can systems*

All the packets passing through a particular traffic point are captured and written to storage and subsequently analyzed. This requires large amount of storage.

2. *Stop-look-and-listen systems*

Each packet is analyzed fundamentally and only certain information is saved for future analysis. It basically analyses all the data as and when it comes in, filter the necessary ones and store the necessary. Since the pace of incoming traffic of data would be high, this system demands a fast processor. [19]

## TOOLS FOR CYBER FORENSIC

The process of extracting digital evidences from various sources on the course of investigation can be carried out only with the help of specific tools (programs or specially designed circuits) specially designed for the purpose. The main objective of all these tools is

[17] www.forbes.com/2005/12/13/microsoft-word-merck_cx_de_1214word.html , Ewalt, D. "When Words Come Back from the Dead,"

[18] Mohd Mustafa Choudhary ,*Cyber Forensics and Focus Area*, Tata Consultancy Services White Paper pg 6-14

[19] Emmanuel s Pilli, R.C. Joshi, *Rajdeep Niyogi,A generic framework for network forensics, International Journal for Computer Applications*, volume 11, 2010, pg 2

to make the digital or e-evidence admissible in a court of law. Just like a different spanner is required for every different nut, different tools are required for different crimes committed. A tool used for decoding a signal will be different from that used for log analysis. Following are a list of important cyber forensic tools;

1. *TCT or CORONER'S TOOLKIT*- It was created by D.Farmer and W. Venema. Mainly used for the recovery and analysis of data after cyber-attack on a UNIX[20] system.

2. *The Forensic Toolkit (FTK*)- It is a comprehensive forensic toolkit, used for the recovery of passwords, for gaining access to secure files and to crack encrypted files over a network.[21]

3. *NetWitness and security intelligence*-These are network traffic security analyzer tools.

4. *ProDiscover Incident Response (IR)*- This tool is developed by Technology Pathways. It is used to preview, image, search, analyze and report data. IR can used to find data on a system without affecting it or getting it altered.

5. *MailXaminer by Sys Tools*- A forensic tool to extract email evidences from multiple email platforms through its extensive search and recovery mechanism.

These are some of the forensics tools that find application in the area of cyber forensics today.

## CONCLUSION

Techniques and tools of cyber forensic, if duly made use of can reduce the discrepancies in investigations and increase the credibility of evidences produced. Effort must be made to popularize the practice of cyber forensic in all investigative scenarios. Apart from use in procuring evidence, the techniques like network forensic, disk forensic etc., cyber forensic can also be put to use to ensure internal security, data protection, and also restrict unwanted intrusion into the systems. What is required to use such facilities efficiently are qualified technicians, which is definitely in abundance, and our investigators being aware of such a platform for evidence procurement and putting the same to use.

[20] UNIX is a family of multitasking, multiuser computer operating systems that derive from the original AT&T UNIX, developed in the 1970s at the Bell Labs research center by Ken Thompson, Dennis Ritchie and others.

[21] Albert Marcella Jr and Doug Menendez , Cyber Forensics A Field Manual for Collecing, *Examining and Preserving Evidence of Computer Crimes. Aurbach Publications*.2nd edition 2007,. page 35