A Study on Cyber and Network Forensic in Computer Security Management

Article · August 2017

DOI: 10.29027/IJIRASE.v1.i2.2017.51-57

2 authors:

Baboloki Janet Phuthologo
Botho University
1 PUBLICATION **0** CITATIONS
SEE PROFILE

Srinath Doss
Botho University
22 PUBLICATIONS **62** CITATIONS
SEE PROFILE

A Study on Cyber and Network Forensic in Computer Security Management

Baboloki Janet Phuthologo[1] and Srinath Doss[2]

[1]PG Student, Faculty of Computing, Botho University, Botswana

[2]Head of Department, Faculty of Computing, Botho University, Botswana

janet.phuthologo@bothouniversity.ac.bw, srinath.doss@bothouniversity.ac.bw

Abstract

Cybercrime has become more popular in the World of internet. The paper here will outline more on cyber and network forensics. There is lot of crime related cases nowadays that needs digital or electronic proof as a form of evidence. For evidence to be presented, certain procedures need to be followed from the collection of data to keeping it safe for the evidence time in a particular case. This paper shall try summarizes information relevant to security and cyber Forensics in general and how those cases are solved.

1. INTRODUCTION

We are living in a world of technology where computers are being used every day from personal use, social interaction to business wise. Most storage medium of information relies on electronic devices like hard disks and flash, as well as cloud storage. Also the trending of smartphone usage nowadays also increases the risk of cybercrime as most transactions and communication online is done over smartphones. That poses vulnerabilities to attackers online to steal information such passwords, credit and bank credentials, etc[1][2].

The paper will then highlight basics associated with computer and network security. Also information beneficial to prosecutors as well as Law enforcement on the guidelines and procedures for making use of digital evidence as well as obtaining it. Also to ensure the collected evidence information is made admissible to be used in court. The paper will generalize on the world of forensics and how it all works [4][5][6].

II. Literature Review

Compare and Contrast Authors/ Researcher findings:

Both authors state computer security as about confidentiality and protection of information from exposure to unauthorized entities. One author mentioned it as related to the protection of information from damage to both hardware and software as together with services disruption, whilst another author Detlev Gabel et al, defined it using 3 triangular security trends being CIA Confidentiality, Integrity and Availability as well as authentication[3][6][7].

Paul Ragusa went on and explained the importance of Cyber Security. He showed statistics of hoe cybercrime endangers global economy, an estimated of US$400 million per year was given as evidence.

Crimes commonly associated with cyber include credit card information, money theft, and industrial espionage. And many institutions like government and private are finding ways to prevent such attacks[4][5].

Also according to another researcher, 80% of US Companies has suffered these cyber-attacks las year and most of attack done via emails. Hundreds and hundreds of consumers have been victims of credit card number, email addresses and other personal information attack from online intruders. Research showed around $445 billion costs were exceeded each [8].

Method used for these studies or investigations were conducted via survey done from different writers under forensics. The study demonstrations were compiled from a collective of different authors' information. Existing papers and articles on the forensic topic made the research a success.

III. Need for security in computer networks

With so much communication over the web, lot of exchange going through applications and data. Security should be a greater concern amongst all. Both individuals, companies, organizations dealing with sensitive information should ensure its highly protected since most attacks does that online through computer and mobile usage[1][5].

Most businesses are trying to find ways to prevent such attacks. And these kinds of attacks are mostly via electronic devices, software piracy, movies, online games and many more [1].

Forensics

Forensics is termed as scientific methods or applications in association with the judicial system or court of laws. The purpose behind these methods is to unveil the digital evidence to be used in court for solving crime cases. This kind of technology wasn't practiced before therefore most criminals tend to get away with their criminal acts without valid proof to incriminate or prosecute them. During that time the oaths, confessions, testimonies from witnesses were the only determining factors of evidence [4].

Now with the enhancement in the technological world forensics has brought new and advanced methods in a digital format for the investigation part. There are procedures and principals to be followed for performing or undertaking such crime investigations. Those include usage of certain measures like blood DNA printing, palm printing, foot prints and finger prints [4].

Why Forensics is needed?

There have been challenges when it comes to providing evidence that is digital related. For such crimes like online fraud, money theft and so on. With forensics in place, unveiling digital proof is essential, retrieving proof that seems impossible is possible with forensics technology. That includes retrieval of information that was somehow deleted, destroyed or lost in order to make evidence disappears. Forensics tactics are good at recovering such gone information with their methods of investigation [3][9].

Where exactly is Forensics used?

Forensics is used in crime investigations in criminal laws. It helps with the identification, collection and analysis of data that can be used as digital evidence for a particular crime case. Set of policies are followed, this being techniques, procedures and principles associated with forensics[3][12][13][14].

Who uses Forensics?

- Any law enforcement
- Both personal or Private Computer Forensic Organizations
- The Computer Security professionals and IT Professionals
- Military departments

Forensics categories:

i) Computer/cyber Forensics and ii) Network Forensics

Cyber Forensics (computer forensics):

It is all about provision of digital evidence usually retrieved from digital devices like hard disks, cameras. Set of analysis techniques are used to achieve this by gathering data to be used as evidence. Each process done need to be documented until final report is produced. This starting from the onset which is crime scene until last stage. And the powerful ability behind computer forensics is that even damaged, deleted or lost data from devices can still be recovered[5][6].

Investigation Steps in Forensics:

4 Main Steps are involved

Acquiring of evidence: This is the very first step in gathering information for evidence purposes. Is it done immediately after the occurrence of an incident? There are tools (sniffer and monitor) used for collecting such evidence and bend preserved until court case. A duplication or copy is made since during court case original copy is not used.

Identification: here comes the second step after acquisition step. Collected information from crime scene is then going to be analyzed for it to be able to be used as evidence. It also entails the use of methodologies and procedures that are even capable of retrieving the damaged/destroyed or deleted data from a device. The results here can be presented in either hardware or a soft copy format.

Evaluation: third step after identification, a collective o parties (Team) from forensics investigator, examiners now working together to determine whether identification information is that valid and valuable to be used. This might even involve the conductions of DNA investigations if necessary.

Presentation: Last stage of forensic investigation. This is where a final report (document) from previous stages is now taken to relevant officials to determine if it admissible to be used in court. It is actually a summary of all findings in each stages from different parties involved in an investigation [6][10][11].

Types of Cyber-crimes associated with Forensics:

Computer used an Object (Target) of crime; it entails where unauthorized entities trying to access information/systems then cause damage to storage data like file and devices, information theft, virus infection etc.

Crime where computer is a Subject (tool) crime; example here includes electronic theft, money laundry, child pornography

Computer contains evidence of crime; crime evidence information being kept in the machine, hence some of those machines can also be used as zombies to attack other systems

Types of Investigations associated with Forensics:

Criminal Investigation; those crimes had been committed or allegedly committed and usually this matter handled by law enforcement

Corporate investigation; those involve the violation of corporate polices commission of crime. This could be unlawful accessing of certain things like websites, also sabotage within an organization, etc.

Private or Civil investigation; collection of investigation cases ranging from personal ones e.g. divorce cases, misunderstanding between 2 parties. Also those within the business world like working as business partners

Computer Crime Law;

This difference form the country set laws.

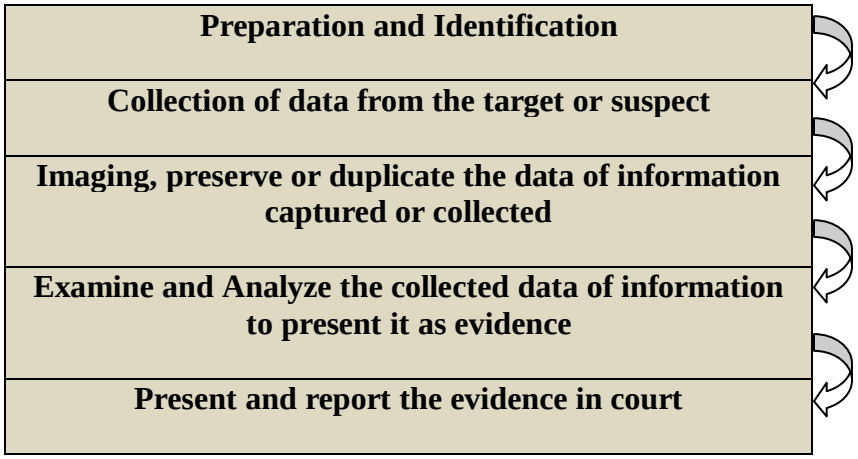

Figure: Digital Forensic Process

Cyber forensic techniques

Below are techniques used in Cyber Forensics

Cross-drive analysis: deals with correlating that information that is contained in different storage media devices for evidence process detection

Live Analysis: it entails usage of methods and tools for examining of computer so as to unveil or extract evidence.

Retrieval of files deleted: certain software capable for recovering deleted data is used

Stochastic forensics: only applies to those activities that do not require any form of digital observations

Steganography: tool used against the original image for diminishing that is inside the picture. This sis done through using harsh algorithm techniques

The following are additional requirements:

Digital Forensic Technician – useful at a crime scene for evidence gathering and processing. These technicians are provided with training in order to be able to carry out such duties. They can still be part of "Live Analysis"
Digital Evidence Examiners: these ones focus on certain digital evidence e.g. sub specialist that is image analyst

Digital forensic tools

Digital Forensic Framework; used for local or remote device accessing

Architecture of Open Computer Forensic; platform (distributed one) used for storing data using PostgreSQL for computer forensics

Computer Aided Investigative Environment (CAINE): it deals with integration of software tools for digital forensics purposes

X-Way Forensics; examiners use this for auto detecting files that somehow no longer exist in the device, also for authentication purposes.

Tool Kit-SIFT for investigation; known as multipurpose program for all types of forensics processes

EnCase; another multipurpose platform used in all processes involved

Drawbacks and limitation of Cyber Forensics

- The cost of digital evidence is generally high that is from production of that electronic information to preserving it
- It is still quite a challenge since some legal practitioners like judges still lacks valid knowledge on computer forensics and computer systems
- Confidentiality is still a main concern more so that such cases tend to deal with sensitive information hence those documents can somehow be exposed

Network Forensics

Unlike cyber forensics, network forensics mainly deals with the capturing of data, storing it as well as performing filtration analysis on data packets. For security purposes e ach packet of data passing is recorded. All form of communication on the web from email systems, web browsing to database queries. Capturing is done through usage of finger prints in post attack analysis.

With network forensic it is possible to analyze how attack happened and the actual person who did it as well as the duration of the incident. Therefore network forensic is regarded as the powerful tool when it comes to network analysis [7][8].

Network Forensics Systems Approaches

1. "Catch-it-as-you-can" system; each data packet is captured as it passes through network points, analysis done and stored

2. "Stop, look and listen" system; also deals with analysis of each packet and then stored for future purposes [7].

Network Forensic Parts:

Intrusion Detection; this monitor any form of packet movement within a network for any attack possibility

Since network deals with too much amount of data, this becomes a challenge when looking for that data evidence since it requires lots of technical skills.

The most targeted areas or sections are IP addresses, email addresses through spoofing form of attack

Compatibility between existing techniques being used and the new emerging ones ted to cause problems and that could affect the investigating

2. Logging; for tracking purposes through the help of Intrusion Detection System (IDS), all network activities are recorded.

3. Correlating Intrusion Detection and Logging

Correlation of data with variety of logs so as to enhance the IDS accuracy

Network Forensic Investigative Methodology or process

- The acquiring of needed information
- Brainstorming on that strategies to use
- Evidence needed being acquired
- Analysis requirement performed
- Final report produced[11]

Crime related to network forensics:

Data theft industrial, fraud, hacking, credit card cloning, sexual harassment online, etc.

Drawback or challenges pertaining network forensics

The need to adjust to new emerging technologies that can somehow affect the current ways of doing investigations.

The not so good efficient methods used in digital evidence. Some technical challenges that might arise during the process of collection and production of digital evidence.

Cyber forensic Verses Network Forensic

CYBER FORENSICS	NETWORK FORENSICS
The acquired evidence is commonly preserved on disk	Examinations of Intrusion Detection System (IDS), firewalls, and packer filters are done here
Data at rest is taken care of here	Information that is dynamic and volatiles is dealt with in this section
Both the culprit or person being investigated together with the investigator holds different levels regarding forensics and computer system skills	Here same skills are portrayed by both parties

Conclusion

In conclusion understanding forensics world from both cyber and network perspective would actually help individuals, private companies, businesses,organizations to be able to know how to protect their data more especially in a digital way. All forms of

communication from storage mediums to online charts (via network) as well as cloud storage, email systems should be kept as secure as possible.

Having knowledge about forensics also helps knowing that it doesn't only applies to crime investigations but also to other matters like social ones. That could be family disputes investigations, work place disputes, transport or even fire incidents.

And finally when it comes to choice of best forensic tools, with that forensic background knowledge this will allow or help you make the right choice that could actually benefit you. Choosing best techniques and tools would lead to successful resolving of a case even though challenges are always there, those that could be from technological compatibility and limitations.

REFERENCES

[1] Katie Macdonald, 'Why is Home Network Security Important", Digicert, 1.801.701.9600, 22 September, 2015

[2] Jager et al., "Network Security assessment-An Important Task in Distribution Systems with dispersed generation", 22 September 2009

[3] Marilyn Miller, "Crime Scene Investigation Laboratory Manual", Elsevier, 28 January 2014

[4] Yizhen Huang et al., "Learning from Interpolated images using neural networks for digital forensics, IEEE, 2010

[5] Binti et al., "Digital Forensics & CyberSecurity",IEEE,11.1109/WorldCIS.2015.7359428, 2015

[**6]** Jones et al., "Information Security and Digital Forensics in the World of Cyber Physical Systems", IEEE, 10.1109/ICDIM.2016.782979526 January 2017

[7] Choi et al.2016, "Introduction to a Network Forensics Systems for Cyber IncidentsAnalysis",IEEE,10.1109/ICACT.2016.7423270, 03 March 2016

[8] Gulshan Shrivasta, "Network Forensics: Methodical Literature Review, IEEE, 31 October 2016

[9] Cameron S.D Brown, "Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice, "International Journal of Cyber Criminology, Vol. 9 Issue 1, January-June 2015

[10] Simson L. Garfinkel, "Digital Forensics: Modern Crime leaves an Electronic trail. Finding and preserving that evidence requires careful methods as well as technical skill, September-October 2013

[11]Sujitha S,Parkava R, "Cybersecurity Breaches and Issues Surrounding Online Threat Protection, Published by Moore, Michelle, India, 12 December 2016

[12] John Horsewell, "International Forensic Science and Investigation Series: The Practice of Crime Investigation, London New York Washington DC, 2004

[13] Philippe Dubord, "Investigating Cybercrime", "Springer Link", 10.1007/978-1-59745-577-0_6, 2008

[14] Eva A. Vincze, "Challenges in Digital Forensics", "Police Practice and Research; an International Journal', Vol.17, 2016 Issue 2, 4 June 2016