BOOK CHAPTER | Criminal Hosts

Host-Based Forensic – Analyzing Criminal Action Using Computer-Based Data

Richard Sefah Kwame
Digital Forensics and Cyber Security Graduate Programme
Department of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: richard.sefah@st.gimpa.edu.gh
Phone: +233507113437

ABSTRACT

Computer forensic science is largely a response to a demand for service from the law enforcement community. As early as (1984), the federal bureau of investigation Laboratory and other law enforcement agencies began development programs to examine computer evidence. Currently the company is using delays to process the required information in an urgent time. Therefore, the main focus for the researcher is to analyze the computer forensic system and to come up with a new system. Therefore, the researcher will aim at analyzing the computer forensic activities in a data network in order to gather evidence of criminal activity that can be admissible in a court of law. This paper examines the analysis of criminal actions using host-based Forensic method.

Keywords: Cybersecurity; Host-Based Forensic, Criminal Action, Computer-Based Data

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free
Citation: Richard Sefah Kwame (2022): Host-Based Forensic – Analyzing Criminal Action Using Computer-Based Data
Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics.
Pp 99-102 www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P16

1. INTRODUCTION

The world is becoming a smaller place in which to live and work. A technological revolution in communication and information exchange has taken place within business, industry, and our homes. America is substantially more invested in information processing and management than manufacturing goods, and this has affected the professional and personal lives. The users can bank and transfer money electronically, and many e-mails are received more than letters if is estimated that the worldwide Internet population is 349 million. In this Information Technology age, the needs of law enforcement are changing as well. Some traditional crimes, especially those concerning finance and commerce, continue to be upgraded technologically. Paper trails have become electronic trails. Crimes associated with the theft and manipulations of data are detected daily. Crimes of violence also are not immune to the effects of the information age.

A serious and costly terrorist act could come from the Internet instead of a truck bomb. The diary of a serial killer may be recorded on a floppy disk or hard disk drive rather than on paper in a notebook. Just as the workforce has gradually converted from manufacturing goods to processing information, criminal activity has, to a large extent, also converted from a physical dimension, in which evidence and investigations are described in tangible terms, to a cyber-dimension, in which evidence exists only electronically and investigations are conducted online.

1.1 Backgroud Of Study

Computer forensic science is largely a response to a demand for service from the law enforcement community. As early as (1984), the federal bureau of investigation Laboratory and other law enforcement agencies began development programs to examine computer evidence. Currently the company is using delays to process the required information in an urgent time. Therefore, the main focus for the researcher is to analyze the computer forensic system and to come up with a new system. Therefore, the researcher will aim at analyzing the computer forensic activities in a data network in order to gather evidence of criminal activity that can be admissible in a court of law.

In this Information Technology age, the needs of law enforcement are changing. Some traditional crimes. Especially those concerning finance and commerce, continue to be upgraded technologically. Paper trails have become electronic trails. Crimes associated with the theft and manipulations of data are detected daily. According to the website www.cybercrime.com an attack is defined as any kind of malicious activity targeted against computer system resource. Including, but not limited to, a break-in (any unauthorized access), virus infestation, data or destruction, or distributed denial of service attacks. In addition, some suggest attackers are likely to strike in the midst of confusion that people expect with the arrival of the Year 2000 computer problem. Tribe and Trinoo also may be more powerful than previous programs of the same kind. The duo, which started appearing in recent months are steps above what has happened before.

2. RELATED LITERATURE

What follows is a table summarizing reviewed literature and findings from literature

Table 1: Reviewed Literature and Findings

Document	Authors	Work on Host Based Forensic – Analyzing criminal actions by computer-based data
With major, large-scale banks investing heavily in cyber security and advancing their defensive posture, organized cybercrime groups are increasingly turning to new targets to maintain acceptable levels of criminal return on investment per attack.	Pierluigi, P	*This Analysis by David Shipley is a co-founder and CEO of Beauceron Security Inc., a new start-up focused on strategic cybersecurity management and the human aspects of cybersecurity risk and defence. He writes frequently about cybersecurity issues and has spoken at regional, national and global cybersecurity conferences.*

Document	Authors	Work on Host Based Forensic – Analyzing criminal actions by computer-based data
, cyber-crimes in Ghana have taken a rudimentary form of internet fraud targeting gullible foreigners, known locally as sakawa or "419.	Ashiadey, Bernard Yaw	This policy briefs seeks to analyze the nature of cyber security threats in Ghana and evaluate the progress that the government has made in readying itself for future challenges. The report will explore recent legislative efforts in Ghana, across West Africa, and in Africa as a whole. Finally, the report will provide recommendations to the Ghanaian government on how to structure a workable framework for dealing with future cyber security threats.
data acquisition system in kernel mode is briefly mentioned in Chou [43]. In this paper, we put forth a proposal which accomplishes the crime and criminal profiling, using the data collected from a sophisticated operating system level evidence acquisition scheme thus achieving integrity and correctness of the forensic analysis results from distributed and non-distributed systems.	Bennett, David. W	Forensic computing and cybercrime investigation emerged because of increase in digital crime due to the development of the Internet and proliferation of computer technology. In this paper, we reviewed the literatures in computer forensics and identified many categories of activity research in computer forensics. A few research categories are framework, trustworthiness, computer forensics in networked /virtualized environments and acquisition and analysis of evidence data. The advances such as components, approaches, process of each category have been reviewed and discussed.

3. RESEARCH DIRECTIONS

An early problem addressed by law enforcement was identifying resources within the organization that could be used to examine computer evidence. Crimes associated with the theft and manipulations of data are detected daily. The researcher therefore aims at collecting evidence of an attack from a computer system, how the attacker penetrated the system, deduce what was done gather evidence of criminal activity that can be admissible in a court of law. Research is therefore warranted into the analysis of computer forensic activities in data network that collected evidence of an attack from a computer system by deducing their actions, and gather evidence of criminal activities that can be admissible in a court of law.

This will enable the following:

1. An investigation of various computer crimes that attack the computer system.
2. An analysis of different approaches on how the computer system are compromised
3. Implementation of mechanisms that will prevent the motivation and intent of the attackers to the computer system

4. RECOMMONDATION

Despite the fact that general methods like software diversification and compile/run-time protection should he effective against many stealth worms, their use requires deployment on every host and thus is complicated by the social/administrative reasons. Fortunately, relatively slow spread of topological worms makes it possible to counter them using signature—based detection methods. So far security experts pushed by the competitive antiviral market demands demonstrated that a slow spreading worm-like threat could be identified and confirmed by humans within one day while some signatures can be created even before the worm outbreaks. This gives a chance that topological worms can be filtered out by the signature-based filters before such worms are widely spread especially if the signatures are distributed in the fast and automatic way. As well as any other conclusion this one has some exceptions. Thus, P2P networks have a very high degree of connectivity and the process of creation of many new connections have to be considered normal.

5. CONCLUSION

Law enforcement agencies face many challenges in responding to information attacks in cyber space particularly attacks that cross national and regional borders and exploit technologies of concealment. It can be difficult to locate a hacker who has looped through multiple systems, used anonymous services. or entered through a wireless connection from a mobile unit. Another challenge is collection and preservation of evidence. Evidence may be encrypted or dispersed across several countries. Tracking an intruder who has used a computer located in the United States will require searches and seizures or wiretaps.

REFERENCES

1. Adelman, C. (2000), the Certification System in Information Technology. Washington: US Department of Education
2. Anderson, D. (2000), managing information systems. Codd, F. (1970), A relational model of data for large shared data Banks. 13 (6): Pp377 – 387
3. Darwen, H. (2000), Foundation for Filtering for Internet Service," 4th USENIX Hutchinson. S. and Sawyer, S. (2000). Computers Communications information. Seventh Edition, pp12.13.
4. Breslau, P. Cao, L Fan G. Philips, and S. Shenker, "On the implications of Zipf's law for web caching," Technical Report CS-TR-1998-1371, University of Wisconsin, Madison, Apr. 1998
5. McFadden, R and Hoffer, A. (1993), Modern database management. Fourth Edition, P30
6. O'Brien, J. (2001), introduction to information systems. Tenth Edition. Ramakrishnan, G (2000), Database management system. Second Edition.
7. Schultheis, S. (1989), Management information system. Second Edition, pp207. Symposium on Internet Technologies and Systems, March 2000 Jamadi, N.A., Siraj, M.M., Din, M.M., Mammy, H.K. and Ithnin, N. (2018) Privacy Preserving Data Mining Based on Geometrical Data Transformation Method (GDTM) and K-Means Clustering Algorithm. International Journal of Innovative Computing, 8, 1-7.