RESEARCH ARTICLE OPEN ACCESS

Optimizing Cyber Forensic Framework: A Study on the Effectiveness of Forensic Tools and Technologies

Prof. Alex Roney Mathew
Department of Computer Science - (**Cyber Security**)
Bethany College, West Virginia
USA

ABSTARCT

In today's world of IT era, with the extensive use of digital sources misuse of digital technology is also at its verge. Internet is as advantageous as threat. System security has become one of the major aspect of internet. Although, detection tools have also evolved over the span of time, there is serious requirement of more advanced cyber tools for the in-depth detection. The use of appropriate tool and technique is an important step towards making the task of the investigators easy. The paper has explored the best type of cyber tools and techniques available within the digital forensic framework. To prevent any future cyber disaster, our research has identified the top techniques and tools of forensic framework that can optimise the process the cyber investigation. Also, this paper is providing a comparative analysis of various techniques in forensic investigation along with their benefits and challenges.

Kewords:- Cyber Security

I. INTRODUCTION

In today's IT enabled era many techniques are available for crime prevention and investigation. The study was conducting by studying various digital forensic tools and is included in the review of literature. The main aim of this section is to provide an overview of the forensic framework that are used in the cyber forensic investigation system. Prasanthi (2016) proposed a ***Virtual forensic framework,*** is one such system that enables the effective and secured process of investigation and prevention of internet threats. Digital forensic framework is an important platform for the forensic investigator to prevent crime. The virtual forensic framework is a digital

open source platform that could be used either by the experts or any non-professionals. This device is easy to use in a systematic manner without any hassle or complicacy. This system of device could be applied for virtual series of custody in order to obtain access to enter any remote local device. Apart from that, this device can provide access to home operating system devices, windows or Linux operating system. This system can provide more advance accessing features in the form of extracting data from deleted files, locked or hidden files. Another framework OCFA (***Open Computer Forensic Architecture)***, proposed by **Schatz & Clark (2006),** is one of the popular modes of distributed open-source Cyber forensic framework. The framework is built on the platform of Linux and they use PostgreSQL database in order to maintain storing of records. This system of framework is formulated by a Dutch National Police business enterprise. The framework is automated in assessing its features. This system is also requiring GPL License for downloading (öhn, Olivier & Eloff, 2006).

II. PROBLEM STATEMENT

Internet threat is a dangerous issue that disrupt or corrupt the entire system of network. Malware is one such cyber threat that is purpose for performing malicious activities and they even work with anti-detection system. The cybercrimes are performed in a very complex manner. They are minutely difficult to identify the exact cause of the and the source of threat, due to the complex system of programs developed by the malicious programmers. Therefore, the cyber forensic tools are required to be updated in a regular manner and most workable framework has to be created or identified in order to deal with the complex nature of cyber threats. Our research is mainly focused on the review of the most effective tools and techniques that can cover any complex possibilities.

III. LITERATURE REVIEW

This research study conducts a review of various tools used in digital authentication techniques of forensic framework. Optimisation of the cyber forensic framework is possible with the consideration of all the

possible threats that might have occurred in the past. Thus, the paper reviews the most advanced and efficient tools of cyber detection process based on the patterns of cyber threats occurred till the period.

3.1Sans Sift: Sans sift is a collection documentation comprised of various options in order to provide forensic investigatory analysis. It is based on Ubuntu Live CD The various tools and techniques used in the investigation of cyber forensic are the sleuth kit, volatility framework, sans sift etc. According to a research study the first SAN can predict the landmarks in a fast pace with complete accuracy and is enough to predict within the preliminary stage, by considering a low-resolution taking as input version of the detected part (Zhang et al, (2014). SIFT features can be easily extracted for a local SANs, with each landmark. SANs can be utilized for obtaining the resolution of face images in each layer with higher and higher local successions. This way the subsequent SANs take as input of the shape-index with local features at a higher and higher resolution by refining a better investigatory objective.

3.2Volatility framework: The **Volatility Framework** is a completely open collection of tools which is implemented in Python under the GNU General Public License, in order to extract the digital artifacts from volatile memory (RAM) samples (Haastrecht, Plat and Pelsser 2010). It helps in the valuation of guaranteed annuity options with the help of a stochastic volatility model for small equity prices.

3.3The Sleuth Kit: The Sleuth Kit is a library collection and comprise of Unix- and Windows-based utilities by facilitating the forensic task analysis of computer systems. It was well mentioned and is maintained primarily by digital investigator Brian Carrier. According to Hilgert, Lambertz & Plohmann (2017) the Sleuth Kit is an implementation of Carrier's model and it is still widely applied for forensic analyses now a days. While the Sleuth Kit is highly actively maintained, this model has not seen much updates. Moreover, there is no support for modern file systems for implementing new paradigms in the form of pooled storage.

3.4ExifTool: It is a free and open-source software program used for the purpose of reading, writing, and manipulating images, audio, video and PDF metadata. It is platform independently available for both Perl library and command-line application. According to Orozco et al. (2015) in a recent study the multiple anomalies found in the Exif specification can be found during our study and thus can produce a serious problem in classical tools in order to extract images with metadata, including crashes and wrong results with even interoperability problems among the various devices.

3.5USBDeview: As mentioned in HELIX3 (2015), this tool enables the operating system to record all the minute data from the removable devices like USB storage devices, iPods, thumb drives, HDD, digital camera etc. Registry analysis is one of the application used for solving forensic issues where this USBDeview tools is used.

3.6Award Keylogger: HxD (2015) has mentioned this fast, invisible and easy applicative surveillance tool efficiently records the entire user activity into a log file. The Log file is sent along with email or FTP to the attacker and used for the detection process in the form of specified keywords. Thereby screenshot is taken whenever the typed and detected data can be viewed in a log viewer 6.

3.7Mandiant RedLine: Mandiant RedLine (2015) presented this highly effective tool in the data accessing, processing and recovery of data from the memory devices. File analysis and memory analysis of a particular host is being carried out with the help of this tool. The tools is also effective in the extraction of data about any running processes along with drivers and memory. The system is well equipped to gather information form the file system metadata, events logs, registry data, network information, tasks and services.

3.8LastActivityView: The tool is helpful in the recording of user actions and it can be viewed easily about the previous events. The number of sequential events took place within the system can also be easily identified with the help of this tool. Any situation of events could be recorder with the help of this tool in the form of running or executing any file, opening any folder from nay of the offline or online sources, running an application etc. Even the activities like installing and uninstalling any soft or application or extension or drivers that could be logged within this detection tool (LastActivityView, 2015).

3.9Caine: Digital Forensic Framework (2015) provided a platform of Linux Live CD that involves a wide variety of cyber forensic tools. It stands for Computer Aided Investigative environment. The package of multiple applications within this system tools comprises of data extraction features like semi-automated report creation, GUI enabled services, mobile enables forensic tools, network data recovery etc.

3.10DFF: Volatility (2015) explored digital forensic framework. The system is an open source software. The software helps to gather information, collecting hidden data, invisible data, in order to reveal the digital evidence to the forefront. The software system has the

feature to extract and read RAW, AFF file formats. The software also allows accessing of hidden and deleted form of data from the remote devices and can recover data based on the investigation requirement.

3.11EnCase: This forensic platform is highly popular with many exceptional features to explore the invisible data for the required investigation (Guidance Software, 2002). The tool is also accepted in the cyber forensic world and in court of law as well. court of law he software is well-utilized in wide scenarios of forensic investigation situation. Diverse mode of device could also be connected in order to gather any required set of information in the form of data under suspicion with a considerable amount of potential proof. The software is commonly used by the forensic investigators in order to acquire private data, followed by classification, analyzation and reconstruction of past events of information.

In this section a literature review is conducted which include cyber forensic techniques proposed by different authors. In section 3, a comparative analysis of different tools and techniques for forensic data collection is presented with its advantages and disadvantages. Finally, section 4 concludes the paper with a forwarding recommendation in terms of future direction.

IV. COMPARISON OF VARIOUS TECHNIQUES

The comparative analysis of various techniques of identity-based authentication is shown in Table1. This comparison table provides advantages and research gap of each technique.

Table1: Comparative analysis of various identity-based authentication

S.No	Source Title	Tools and Technique used
1	HELIX3, Incident Response and E Discovery tool, http://www.e-fense.com/products.php, January 2015.	USBDeview
2	HxD Freeware Hex Editor and Disk Editor, http://mh-nexus.de/en/hxd/ , January 2015	Award Keylogger
3	MandiantRedLine https://www.mandiant.com/resources/download/redline, January 2015.	Mandiant RedLine
4	Digital Forensic Framework. (Re)Discover DigitalInvestigation http://www.sleuthkit.org/sleuthkit/ January 2015. Prasanthi, B. V. (2016). Cyber Forensic Tools: A Review. *International Journal of Engineering Trends and Technology (IJETT)*, *41*(5), 266-271.	CAINE
5	Jain, N., & Kalbande, D. D. R. (2014). A Comparative Study based Digital Forensic Tool: Complete Automated Tool. *The International Journal of Forensic Computer Science*.	DFF
6	Guidance Software. EnCase Legal Journal, Second Edition. March 2002. Available at: http://www.encase.com/support/downloads/LegalJournal.pdfAvailableat:http://www.encase.com/support/downloads/LegalJou rnal.pdf	EnCase
7	LastActivityViewhttp://www.nirsoft.net/utils/ computer_activity_view.html, February 2015	LastActivityView
8	Zhang, J., Shan, S., Kan, M., & Chen, X. (2014, September). Coarse-to-fine auto-encoder networks (cfan) for real-time face alignment. In European Conference on Computer Vision (pp. 1-16). Springer, Cham.	Sans Sift
9	Van Haastrecht, A., Plat, R., Pelsser, A., 2010. Valuation of guaranteed annuity options using a stochastic volatility model for equity prices. Insurance Math. Econom. 47 (3), 266–277.	Volatility framework
10	Hilgert, J. N., Lambertz, M., &	The

	Plohmann, D. (2017). Extending The Sleuth Kit and its underlying model for pooled storage file system forensic analysis. Digital Investigation, 22, S76-S85.	Sleuth Kit

Table1 has presented the collection of tools and techniques for cyber forensic investigation system along with their merits and gaps. The purpose of table is to obtain the most effective tools and techniques of cyber investigation. As shown in the table all the tools have their own distinct features and capabilities of solving the complex cyber queries.

V. CONCLUSION

The purpose of the paper is to study the important tools and techniques of cyber forensic and to determine the most effective tool and technique. This has led to the best usage of advanced form of forensic tools and techniques in order to provide safety and security for digital applications. In the future we can further enhance reliability, accuracy, data privacy and future occurrence security measures of a crime based on data mining system. Moreover there is a need to improve the prediction system, which can be explored further with the conceptual technique of data mining.

RERERENCES

[1] Prasanthi, B. V. (2016). Cyber Forensic Tools: A Review. *International Journal of Engineering Trends and Technology (IJETT)*, *41*(5), 266-271..

[2] Jain, N., & Kalbande, D. D. R. (2014). A Comparative Study based Digital Forensic Tool: Complete Automated Tool. *The International Journal of Forensic Computer Science*.

[3] Köhn, M., Olivier, M. S., & Eloff, J. H. (2006, July). Framework for a Digital Forensic Investigation. In *ISSA* (pp. 1-7).

[4] HxD Freeware Hex Editor and Disk Editor, http://mh-nexus.de/en/hxd/ , January 2015.

[5] Digital Forensic Framework. (Re)Discover Digital Investigation http:// www.sleuthkit.org / sleuthkit / January 2015.

[6] https:// www.volatilesystems.com / default / volatility, February 2015.

[7] Guidance Software. EnCase Legal Journal, Second Edition. March 2002. Available at: http://www.encase.com/support/downloads/LegalJou rnal.pdf

[8] Zhang, J., Shan, S., Kan, M., & Chen, X. (2014, September). Coarse-to-fine auto-encoder networks (cfan) for real-time face alignment. In *European Conference on Computer Vision* (pp. 1-16). Springer, Cham.

[9] Van Haastrecht, A., Plat, R., Pelsser, A., 2010. Valuation of guaranteed annuity options using a stochastic volatility model for equity prices. Insurance Math. Econom. 47 (3), 266–277.

[10] Computer Aided Investigative Environment http://www.caine-live.net/