International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET218370

Advancing Automation in Digital Forensic Investigation

Sathwara Prerna[1], Dr. Chandresh Parekh[2], Priyank Parmar[3]

[1]School of Information Technology, Artificial Intelligence, and Cyber Security , Rashtriya Raksha University, Gandhinagar, Gujarat, India

[2]Dean of School of Information Technology, Artificial Intelligence, and Cyber Security Rashtriya Raksha University, Gandhinagar, Gujarat, India

[3]Assistant Professor, School of Information Technology, Artificial Intelligence, and Cyber Security Rashtriya Raksha University, Gandhinagar, Gujarat, India

Article Info
Volume 8, Issue 3
Page Number: 378-382

Publication Issue :
May-June-2021

Article History
Accepted : 06 June 2021
Published: 12 June 2021

ABSTRACT

This paper represents the thoroughly technical approach to carry out forensics investigation in web applications or computer systems which combines and provided digital evidence from the particular computing device. The main objective is to recover and investigate the material found in digital devices related to cybercrime and maintain the integrity of the evidence collected. The main motive of the scanner is to investigate the system or application and process a stronger result/report of each vulnerable system or application effectively. This tool is the Open source that is used to perform some forensics investigation tasks which is helpful to the investigator to do their job and generate digital evidence which can be used by a court of law.

Keywords : Forensic investigation, Digital evidence.

I. INTRODUCTION

Usage of internet and Digital Equipments has been increased in last few years, so that most of the data are moving toward digital format. Various digital devices like compute, smartphones are core part of our day to day life in which data are in digital format. These devices contain essential information of users. Furthermore, these devices are becoming the essential part of criminal activity, intruders, and IT theft because these all are vulnerable to attackers. So that the result is that, we are may be a target of cyber crime activity. The digital forensic investigation focuses on recover lost or intentionally deleted objective evidence of criminal activity. This paper mainly explains malware analysis open port scanner, Bad cluster scanner, Deleted data recovery, and Browser History examination, RAM analysis. All these tools are currently in a market and all are open source and to built in python language. I have combined them in a tool for easy to use by the user and a forensics investigator this tool allows user to investigate some tasks and to generate digital evidence.

II. TOOLS INFORMATION

A. NTFS (DELETED DATA RECOVER)

Retrieving deleted and lost files/documents from computer hard disk for forensics investigation is most important steps in digital forensic investigation.

NTFS Tool can be used to recover deleted files or files off of damaged drives, although recovery quality will depend on how badly the file data has been damaged or overwritten.

B. NMAP(OPEN PORT ANALYSER)

This is a network scanning tool. This tool is used to collect information such as which devices are connected to a network, which services and operating system running on those devices.

In a port scanning scenario someone transmits sequence of messages to the computer. The purpose behind this is to crack the computer system and retrieve the information like which network service corresponding with which port.

Port scanning is a ideal way to identify weakness of computer so it is most favourite of computer hackers.

C. YARA(MALWARE DETECTION)

YARA forensic investigation tool provide many efficient and effective techniques . These techniques are used to identify and classify the malicious activities which are known as malware. For this purpose, we can also use reverse engineering techniques. Reverse engineering is highly recommendation for this purpose because it gives effective and efficient techniques which can used to investigate malicious files thoroughly. It is ideal way to analyse malware behaviour, and then classify them in different types of malware. But limitations are that it consumes more amounts of time and cost. To overcome the limitations of Reverse Engineering and do their job we can use a tool known as YARA.

YARA tool is first and foremost choice of digital investigator to detect malware and classify its family. It provides an approach which is based on many rules to illustrate malware types based on textual or binary patterns.

D. VOLATILITY(RAM ANALYSIS)

Volatility framework is open source tool which is use to extract digital artifactes from volatile memory. Crash dumps, raw dumps, VMware & VirtualBox dumps are analyzed by this framework. Volatility framework performs some extraction techniques which are completely independent from the system which is currently in investigation but offers visibility into runtime state of system.

E. CRYSTEL DISK INFO(BAD CLUSTER ANALYSYS)

This tool is use to monitor the health of drive on your computer. This tool displays the information which is found on Solid State Drive (SSD), Hard Disk Drives (HDD), and any external drive such as USB. It helps you for detection and prevention of further disk surface errors so that you can take require action immediately. So that data loss could not become irreplaceable.

F. BROWSER HISTORY EXAMINER

Browser History Examiner is a forensic tool for capturing, analyzing, and reporting internet history from the main Desktop Web Browser.

All web browsers store the data which are surfing by the user and history. The intention behind this is to facilitate some tasks like immediate website suggestions or as fast as possible access to previously visited sites. This is superior source of electrical evidence used in cyber crime related investigations because cyber criminals may use the browser to search crime methods or visit many website to gather information, so that web browser forensic is an important field of Digital Forensics investigation.

III. REVIEW OF LITERATURE

In [8] Bolagh & Pondelik both have suggests a decoding keys recovery techniques which is used to recovery of decoded keys from the bunch of live images of volatile memory. These techniques are run on windows as well as Linux environment of free open source tool with precise Crypt which is works on-the-fly disk for encryption. The authors also proposed an approach for reduce size of dump images, mainly in the case in which co encryption uses correct crypt, the size could be bounded to 1-2 MB only. However, in proposed approach have restriction that the image must be present closeup for forensic analysis. Furthermore, decoded keys are discovered by search of content and if some failure of data appears in a disk then after it become unfeasible for give out keys. Techniques of Advances in data encryption having tough job of cyber investigators.

In [9]Natasa Suteva with Aleksandra Mileva, and Mario Loleski have findout that on basis of the pieces of evidence collected by computer forensics attackers are arrested. The suspected Equipment normally shows some useful data which is useful to identify suspects through forensic analysis of their devices like computer system, laptops, tablets, and smartphones. Computer forensic analysis of devices used by the attacker and suspect for finding some artefacts in them, which could be recognize and possibly to re-establish the attack. Further it is primarily use to gain justifiable evidence to presents in court. Traces are found in attacker's machine at the files in browser's history , temporary storage of browser and bash history file. On the suspected system evident, traces are found in the file system and the log files.

In[10] Andrew Marrington & George Mohay, with Hasmukh Morarji & Andrew Clark, have given model approach in automatic computer forensic analysis in which they shows various models and its use in computer forensic analysis. They also established a model for use in computer characterising object model which models of computer used as objects with several attributes and inter relationships. So it is known as info model. It provides a way for development of an automated computer forensic examination and investigation tools. Some tasks like digital evidence which represent and determines computer activity and investigative reasoning are promoted by this model.

In [11] Maximilian Bielecki and Gerald Quirchmayr have describes a strength of automation system and augmentation in support system with an analyzing of cyber crime and criminals same as used in law enforcement work. They had also provides the detail of prototype which is based on an automatic forensic support system and that system called computer forensic analyzer and advisor. This system provide automation and which supports investigators by independently identifying malicious software and programs.

In[12] Jun-Hyung Park & Minsoo Kim with Bong-Nam Noh & James BD Joshi provided representation on the complexity of computer system. They also shows that the production of hacking tools and techniques are significant need for computer forensics analysis. This type of forensic investigation focus on analysis of executable malicious files which can be used by hackers to install in targeted system to hack targeted system. It is very difficult to identify such type of malware in victim's system because the identification of causes of the fragments of executable files is very hard. Without executing the program we can identify modifications done in malicious files. For this purpose we use methods.

In [13] Kyung-Soo Lim & Seung Bong Lee with Sangjin Lee all have focus on requirement of advance process model which is use to gather most important evidence. The Step by step Forensic Process Model gives a stepwise approach which is used for incident

description, recovery, analysis. It advises an advance investigational model. This model is used to select the object and considers the relevant pieces of evidence only. This process is depending on the crime scene situation. To overcome the limitation of traditional forensic model we must requires effectively selecting and inspecting the system.

IV. PROPOSED FRAMEWORK

Advance Digital Investigation is a tool that provides the forensic platform in which 6 tools are available for you to analyze, investigate and generate an actionable report. The advance Digital Investigation tool provides many of tools for some tasks like Deleted data recovery, Open port scanning, Malware detection, RAM analysis, To Find Bad cluster, and Browse History examination.

The operational environment of this tool is designed to provide simple and efficient way to perform digital forensic investigation process including all the phases of it like identification, collection, analysis, and preservation than generate the report which can be present in a court as a digital evidence. It gives graphical user interface environment with forensic tools.

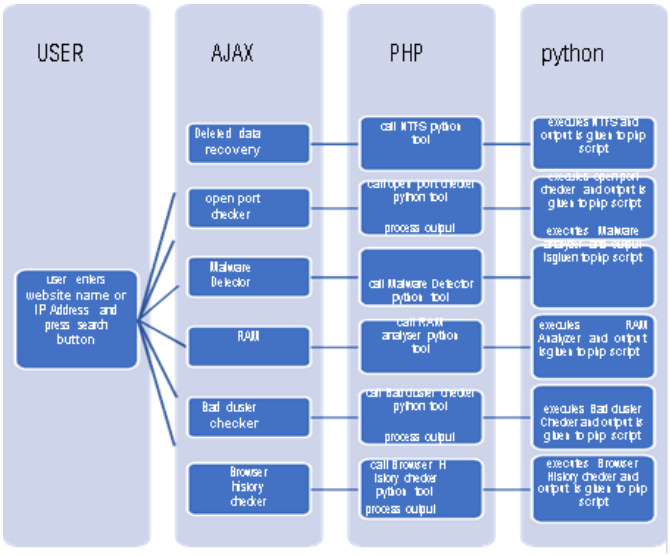
V. METHODOLOGY

The user enters the website name or IP address of victim system and then click on the search button, which calls a function which is developed in JavaScript and then that JavaScript function calls AJAX. There are six AJAX for each request i.e.Deleted data recovery, open port checker, malware detector, RAM analyzer, Bad cluster checker, Browser history checker.

This ajax request sends to the server where every ajax is handled one by one by PHP script for all this ajax Deleted data recovery, open port checker, malware detector, RAM analyzer, Bad cluster checker, Browser history checker.

AJAX call has the website name or IP address pass to PHP script and save in a variable and then PHP script has the command to call python function for Deleted data recovery, open port checker, malware detector, RAM analyzer, Bad cluster checker, Browser history checker than python script is executed by shell_exec() function in PHP where it executes python script than result is stored in a JSON format which is then processed in a PHP script.

And this output is than save in table form to shows at user side in HTML format and given response to ajax function and that shows to the user to screen



VI. FUTURE SCOPE

There is no capping for addition and deletion of number of tools as per requirement of application. It is also possible to make Graphical User Interface (GUI) of the proposed system in future so that it is more convenience to user.

VII. CONCLUSION

In general for different task we have used separate tool for each task while in proposed system all task to do possible in single system. Multitasking is main benefit of this system and it is highly require in cyber security field due to high surge in cyber crime. The proposed system is also save the time to do digital forensic investigation

VIII. REFERENCES

[1]. Sameer H Mahant, B B Meshram ”NTFS Deleted Files Recovery: Forensics View”, IRACST-International Journal Of Computer Science and Information Technology & Security (IJCSITS), ISSN:2249-9555 Vol.2, No.3, June 2012.

[2]. 2014Tariq Ahamad Ahanger, Port Scan – A Security Concern, International Journal of Engineering and Innovative Technology(IJEIT), ISSN-2277-3754, Volume 3 Issue 10 April.

[3]. Nmap Network Scanning Guide – Gordon Lyon.

[4]. Erhan Akbal, Fatma Günes, and Ayhan Akbal. 2016. Digital Forensic Analyses of Web Browser Records. JSW 11, 7 (2016)

[5]. Online "Volatility Framework" Github

[6]. Online “Volatility Framework – Volatile memory extraction utility framework”

[7]. Balogh, Š., & Pondelik, M. (2011, September). In Proceedings of the 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems (Vol. 2, pp. 759-763). IEEE.

[8]. Kaur, M., Kaur, N., & Khurana, S. (2016). A literature review on cyber forensic and its analysis tools. International Journal of Advanced Research in Computer and Communication Engineering, 5(1), 23-28.

[9]. Marrington, A., Mohay, G., Morarji, H., & Clark, A. (2010, February). A model for computer profiling. In 2010 International Conference on Availability, Reliability, and Security (pp. 635-640). IEEE.

[10]. Maximilian Bielecki and Gerald Quirchmayr, "A prototype which supports computer

[11]. forensic analysis in combination with the expected knowledge level of an attacker to achieve more efficient investigation results", International Conference on Availability, Reliability, and Security. PP. no:696- 701,2010.

[12]. Kaur, M., Kaur, N., & Khurana, S. (2016). A literature review on cyber forensic and its analysis tools. International Journal of Advanced Research in Computer and Communication Engineering, 5(1), 23-28.

[13]. Ani, U. P. D., & Agbanusi, N. C. (2014). A comparative assessment of computer security incidence handling. Journal of Advances in Mathematics and Computer Science, 3120-3134.

Cite this article as :

Sathwara Prerna, Dr. Chandresh Parekh, Priyank Parmar, "Advancing Automation in Digital Forensic Investigation", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 8 Issue 3, pp. 378-382, May-June 2021. Available at

doi : https://doi.org/10.32628/IJSRSET218370

Journal URL : https://ijsrset.com/IJSRSET218370