RESEARCH ARTICLE OPEN ACCESS

Automated Live Forensics Analysis for Volatile Data Acquisition

Bharath B, Nagoor Meeran A R
Department of Information Technology M.TechInformation Security and Cyber Forensics SRM University Chennai, India
Department of Information Technology Faculty of Information Security and Cyber Forensics SRM University Chennai, India

Abstract
The increase in sophisticated attack on computers needs the assistance of Live forensics to uncover the evidence since traditional forensics methods doesn't collect volatile data. The volatile data can ease the difficulty towards investigation in fact it can provide investigator with rich information towards solving a case. Here we are trying to eliminate the complexity involved in normal process by automating the process of acquisition and analyzing at the same time providing integrity towards evidence data through python scripting.
Keywords – Live forensic, Live acquisition, RAM dump, Network, HDD, Windows registry.

I. INTRODUCTION

During the incident response process we often come across a situation where a compromised system wasn't powered off by a user or administrator.To pull or not to pull the plug, that is the question today cyber-crime investigators are faced with the grueling task of deciding whether shutting down a computer system is the most efficient and effective method to gather potential electronic evidence.

One of the more recent change in evidence handling has been the shift away from simply "pulling the plug" as a first step in evidence collection to the adoption of methodologies to acquire evidence "Live" from a suspect computer. All of this data can help the investigator in finding forensics evidence.

The live forensics procedure is the only way to acquire those data but the amount of data that need to be considered during acquisition is vast and spread over the various locations on a computer. It often becomes a tedious and time consuming task for an investigator to acquire all data manually since investigator has to be aware of multiple tools along with their functionality and techniques to perform a successful live forensics.

After considering the time complexity and enormous data involved in live forensics the only solution to the problem is to provide a toolkit that can automate the process of acquiring and analysing evidence data.

This toolkit can be easily deployed through a USB drive and it is capable of maintaining integrity and reliability towards evidence data throughout the process.

II. LITERATURE SURVEY

2.1Forenscope: A Framework for Live Forensics [1]

Forenscope team describes the traditional forensics (post-mortem cyber-forensic) techniques may cause significant disruption to the evidence gathering process by breaking active network connections and un-mounting encrypted disks and their Forenscope preserves the state of the running system and allows running processes, open files, encrypted file systems and open network sockets to persist during the analysis process. They do this by the process of reviving the native operating system and performing analysis on it.

Itconsiders Taint and blurriness as the concepts related to the use of forensics tools. Taint is a measurement of change in the system induced by the use of a forensic tool and it may be present both in memory and on disk.Blurriness refers to the inconsistency of a memory snapshot taken while a system is running. Which they avoid implementing the principles of introspection to provide a consistent analysis environment free of taint and blurriness which they term as the golden state.

Although they have good techniques towards live forensics but the method suggesting reviving an operating system is not a best practise.

2.2 Safer Live Forensic Acquisition [2]

The current methods of computer forensic acquisition, identifying and explaining the shortcomings and discussing about Possible improvements to the methodology as Proof of Concept (PoC) to demonstrate the improved method.

The strength of dead acquisition as a clear merits principle due to its simplicity; its main strength is the clearly defined and straightforward stages of the acquisition, which can be verified at any time but clearly the weakness lies on having an exact copy of an encrypted hard disk is no use

to a forensic examiner as analysis of random data is impossible.Encrypted volumes, files which contain an encrypted file system, are widely used by criminals. These files can be opened with a very same program which they used to encrypt the data. When it comes to encrypted volumes on the file system once a key has been provided to the program the file system can be mounted and accessed like any other file system; encryption and decryption are transparent. Encrypted volumes are useless if a forensic practitioner can assess a computer while the volume is still mounted.

To combat the problems of how dead acquisition is ineffective against encryption and loss of volatile data, they suggest live forensic methodology since it allows an computer forensic practitioners to run programs on suspect's computers to acquire RAM, unencrypted files and any other data they saw fit. Live forensics clearly solves the problems detailed above as now we are able to acquire unencrypted data, if present, and also contents of RAM. Performing a full dead acquisition of the computer is recommended, if it is possible to do so after live acquisition.

Safer live forensic acquisition has certain Constraints due to following parameters such as, slurred images: slurred images are produced when the file system being acquired is modified during acquisition.Potential for hard disk modification by forensic practitioners: to perform live acquisition forensic practitioners must execute code which will run on the CPU of the suspect system. The code will change data in the CPU registers and RAM. It may also change data on the hard disk: We may ruin all evidence when inappropriate action is taken by forensic examiners. Errors in a forensic examination can cause an unnecessary amount of data to be changed. This may be due to something as simple as running an application on the suspect hard drive.Anti-forensic programs: Criminals who are forensically aware are liable to take steps to reduce the effectiveness of a potential investigation.

Even though they discuss about the problem involved in live forensics they don't provide solution to this problem as they can significantly affect the live forensics.

2.3 Live Forensic Acquisition as Alternative to Traditional Forensic Processes [3]

It presents their current research with regards to the forensic soundness of evidence retrieved through live forensic acquisition. They describe development of live forensic acquisition in general presents a remedy for some of the problems introduced by traditional forensic acquisition. However, this live forensic acquisition introduces a variety of additional problems, unique to this discipline.

They suggest three important principles to follow during live forensic process:

- Acquire the evidence without altering or damaging the original
- Authenticate that the recovered evidence is the same as the originally seized data and
- Analyse the data without modifying it.

Further itexplain about the core forensics process of collection, examination, analysis and reporting along with their issues in each phase with respect to forensic law.

2.5 Performing Live Forensics on Insider Attacks [5]

To perform a meaningful forensic trace back, it is useful to preserve as much volatile evidence as possible. This includes the entire state of the running system with its open network sockets, encrypted file systems and processes. Preserving these resources can be helpful in identifying live ongoing attacks, dormant sleepers, and identifying the perpetrator.

The guidelines are aimed at analysing standard computer attacks. In contrast, analysing an insider attack demands comprehensive real-time forensics to track the motives and actions performed by the insider. To uncover and investigate these attacks, live forensics tools are preferred, given their ability to provide access to the state of volatile resources such as active SSH and VPN sessions, file transfers etc.

Then they suggest to follow up the Forenscope procedure to gather evidence but we already know that reviving a system is not a best practise.

2.6 Fast Deployment of Computer Forensics with USBs[6]

In this research, they integrate several open source digital forensics tools and create a graphic user interface to develop a user-friendly environment for investigators. To avoid evidence loss due to shutdown of target hosts, they use the live analysis technique to collect volatile data with executing commands from an external USB. They also create a live USB so that target hosts can boot from the USB which contains a functional operating system with tools for forensic discovery.

Here they compare the already existing forensics tools such as FTK, EnCase, SMART, PyFlag and The Sleuth Kit, on their performance towards live forensics from a USB drive.

However, most existing digital forensics software are commercial version which are expensive and offer less support towards live forensics which makes the investigator to perform a lot of task towards.

The best way to avoid all these issues is to provide a toolkit that can automate task and provide

same integrity towards data as those commercial tool's do.

III. DESIGN

The Automated Live Forensics Analyser (ALFA) is composed of several modules (which is discussed below) where each modules is designed to perform a specific task during the process of live acquisition which gives ALFA the power to identify and acquire data.By designing the tools as modules it gives the flexibility to analyser to choose upon the different modules at the time of acquisition.

The entire tool and its modules are created using python (compatible with 2.7.x) it gives the greater advantage to the forensic tool in terms of power and performance.

The main advantage with the tool is that its designed to be plug on play so once you insert the USB with ALFA on to the target machine it will right away start the process and gives a good representation of on-going process on the screen and alerts the investigator if any conflicts involved. Once the process is completed successfully you will be given with a report file which gives the detailed statistics of the process.

3.1 MODULES

As mentioned earlier the each module is designed to perform individual task which can be enabled or disabled at during run time the modules along with the functionality is discussed below

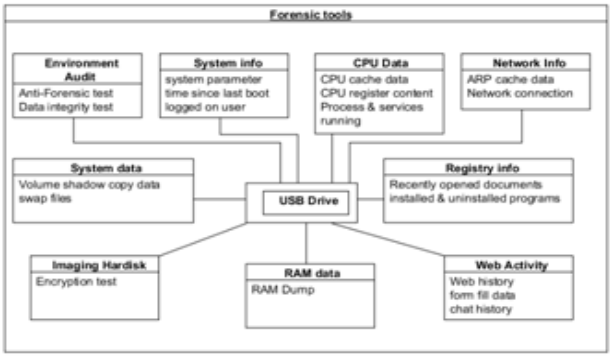
The different modules are

- Environment-audit.
- RAM data.
- CPU data.
- Network information.
- System information.
- Application data.
- HDD data.
- Registry information.
- Browser information.

3.1.1ENVIRONMENT AUDIT

The environment audit module will perform two important task before we begin the process of acquisition they are anti-forensics test and data integrity test.

The anti-forensic test is to ensure that the evidence data are not tampered while analysing and data integrity test is to ensure that only our program is accessing target media. It's often common that an infected computer will try access, alter or add data to a connected USB device.



3.1.2 RAM DATA

The RAM data and virtual memory files are dumped. This can help in finding the recent activities associated with user and applications.

3.1.3 CPU DATA

The CPU data include CPU register contents, program and services that are running. This helps to see through CPU activity and understand about unknown application activity or abnormal behaviour by an application or service.

3.1.4 NETWORK INFORMATION

The network information are the crucial volatile data. Here we'll collect network communication details such as open ports and application responsible for it along with information about network and network adapter.

These details can give a clear view about the computer network communication and to find evidence on network based attack.

3.1.5 SYSTEM INFORMATION

This module is about collecting information about the evidence computer which is operating system information, hardware information, current logged on user and up time of the system. This helps in understanding the target environment better.

3.1.6 APPLICATION DATA

Application data include listing installed application to identify hacking application or data manipulation tool.

3.1.7 HDD DATA

It includes recovering deleted files, finding hidden data from a slack space, detecting data scrub and detecting encrypted volumes in HDD.

Detecting an encrypted hard disk is useful since once the computer is powered off it's impossible to access data without encryption key. If necessary interested data can be copied at the time of acquisition.

3.1.8 REGISTRY INFORMATION

Data from registry crucial in live forensics since it can reveal the MRU (most recently used) list of application, file, folders, USB artefacts and other information too.

These data can help the investigator to understand the user activity and system activity better.

3.1.9 BROWSER INFORMATION

The common internet activity happens through the browser and it known to have rich information on user internet activity. Here we'll search for form fill data, browsing history and cookies.

IV. CONCLUSION

The key to using live response successfully is being very specific and focused on what to examine. Traditional forensics will always be needed to provide in depth analysis identifying how the incident happen on the system and what activities took place while it was active. Where live response excels is at quickly identifying and containing an active threat. The quicker we can identify the threat the quicker containment and remediation will take place.

References

[1] Forenscope: A Framework for Live Forensics by Ellick Chan, Shivaram Venkataraman, Francis Davi.
[2] Safer Live Forensic Acquisition by Ryan Jones.
[3] Live Forensic Acquisition as Alternative to Traditional Forensic Processes by Marthie Lessing and Basie von Solms.
[4] Live Data Acquisition: The New Default Standard for Capturing ESI by David Greetham, National Director of Forensics, Legal Enterprise Solutions.
[5] Performing Live Forensics on Insider Attacks by Ellick Chan, Amey Chaugule, Kevin Larson and Roy Campbell.
[6] Fast Deployment of Computer Forensics with USBs by Chung-Huang Yang, Pei-Hua Yen.