CHANAKYA LAW REVIEW (CLR)

Vol. III Issue I, Jan-June 2022, pp.162-176

ACQUISITION & ANALYSIS OF EVIDENCE FROM RANDOM ACCESS MEMORY (RAM) UNDER CYBER CRIME

Rajesh Kumar[1]

Ritwik Tripathi[2]

ABSTRACT

The growing necessity of acquiring Random Access Memory (RAM) data of working computer systems found on crime scenes has been challenging from the very beginning and there is a need to resolve this problem for a better proceeding towards live forensics.When the crime is being committed from a working computer, the RAM (live) data becomes most important from where the crime related evidence from the computer is gathered. Proper acquisition of RAM data is enough for appreciation of the potential digital evidence in a particular cyber-crime and convicts the cybercriminal before the court of law. In this paper, the researchers present a standard method of acquiring and analyzing RAM data from a working computer system found at a crime scene. Starting from the basics of digital forensics, this paper will talk about how the live data should be acquired and analyzed onspot. Finally, an experiment demonstrating what type of data will be acquired and analyzed using the forensic tools.

Keywords: Digital Forensics, Crime Scene, Random Access Memory, Live System, Live Data Acquisition, Live Data Analysis, Forensic Toolkits, Authenticity.

[1] Research Scholar, CNLU, Patna

[2] B.Tech Computer Science, 4th Year

INTRODUCTION

In the age of information technology and communication, crime patterns have been changing and have shifted to cyberspace. Now, computers are being used as a source and as a target of cyber-crime as well as traditional crime. Obviously, in such a situation, the computer is the potential source of digital evidence. It consists of a large amount of evidence in the form of data in different locations of the computer system. These data are volatile and non-volatile in nature. Non-volatile data is permanently stored inside the hard drive. But, volatile data is available only in a running computer system. Volatile data, that includes unsaved tasks, open file and folders, running applications or software, and Internet activities on a computer. Volatile data is also known as live data or RAM (Random access memory) data. These data are very valuable in police investigations. Because, in many cases only such data (evidence) has established the matter before the court. Onspot data acquisition and analysis of RAM play a vital role in the appreciation of digital evidence before the court of law. However, law enforcement agencies usually ignore such data (evidence) because of the complex nature of the acquisition and analysis process and ignorance about their appreciation before a court of law. Therefore, possible evidence is usually left at the crime scene.

Digital forensics or cyber forensics has led to a revolutionary change in helping to put an end towards these crimes by identifying evidence on various storage devices. Traditionally, data was stored on memory devices like, Hard Drives, Magnetic Tapes, Floppy Disk, CD's, DVD's, etc. Nowadays, data is stored on Cloud Storage, Servers, etc. as well.

The traditional process of acquisition and analysis of data has been impactful in cyber forensics, but this method fails to recognize live data as evidence. Live data exists in volatile memory devices like, Random Access Memory, Cache Memory etc. As the name volatile memory suggests, the data inside this memory are flushed out as soon as the power source is switched off or the system is disconnected. This means, once there is no power supply to the CPU, the possibility of recovering the contents inside the volatile memory is zero. So, live data can be prescribed as the critical data that is able to provide with intuition towards as to how the target system was functioning on the time of acquisition [7].The acquisition and analysis of live data will definitely provide a much larger prospect of the crime being committed and we can say this because, when we get evidential data which was being processed on the target system(s) is enough for the judges to convict the criminals.

DIGITAL FORENSICS

The science of obtaining, preserving and documenting evidence from electronic media, such as PC, Network System, Smart Phone and various memory storage devices without altering the authenticity of original evidence[1, 2] is known as Digital Forensics or Cyber Forensics. The main objective of the digital forensic is an acquisition, analysis and documentation of digital evidence, which is presented before the court. Digital forensic process has six major classifications:

- Identification of digital evidence is when an Investigating officer or first responder is reporting a crime scene; the identification of the target system makes it easier to proceed the investigation. Identifying the evidence present in any memory storage device makes it easy to recover useful data within no time.
- Seizure and preservation of digital evidence of memory storage means that whenever any evidence is found, the device containing the evidence must be seized maintaining the seizure list according to chain of custody. The device must be preserved from physical & logical factors which may affect the evidence, for example, if a hard disk is seized from a crime scene which contains potential evidence against

  the suspect, the Investigating team must ensure that the hard disk packed in faraday bag or anti-static bag, so that no harm may come to it.
- Acquisition of digital evidence means making an image of the evidence. An image is the bit-by-bit copy of the original storage device. There are many forensic tools for this process. This step ensures that the authenticity of the device either said to be containing the evidence or containing the evidence is not altered after its seizure and we can freely examine the image copy of the storage device for the evidence.The major feature which makes the acquired image equivalent to the original file is the SHA1 checksum calculation of the acquired extraction dump.
- Analysis of digital evidence is the process of extraction, processing and the interpretation of digital data of the image. Extraction produces a binary junk which is turned into human readability by using forensic tools.[2]
- Documentation of recovered digital evidence means documenting the evidence in a particular format which is easy to understand with other necessary information.

- Presentation of digital evidence means reporting the digital evidence before the court with related documentation and other follow up procedures. This includes thedocumentation of the evidence collected and the evidence itself.

ACQUISITION TYPES

Data acquisition is the process which ensures that the authenticity of the digital evidence is preserved. Some widely used tools are FTK, Wireshark, etc. [5]. There are, basically two methodologies by which we can acquire the image of digital evidence and are as follows:

1. Dead/ Offline Acquisition
2. Live Acquisition.[3]

1. Dead/ Offline Acquisition

Dead acquisition of a target system means creating an image of a system by either powering off the system first or the system found is already either in turned off or offline state. Image creation in such acquisition is done by checking the initial power state first. If the system is turned on, it is turned off first to make sure no further processing takes place. After this, the hard disk is removed from the target system and connecting it to hardware or software writeblocker for its image creation along with forensic tools.

Write-blocker tools help in maintaining the authenticity of data like time stamps, hash value, etc. by disabling write properties on the disk, giving the tools read-only access [3]. This makes the device immutable and no changes can be made.

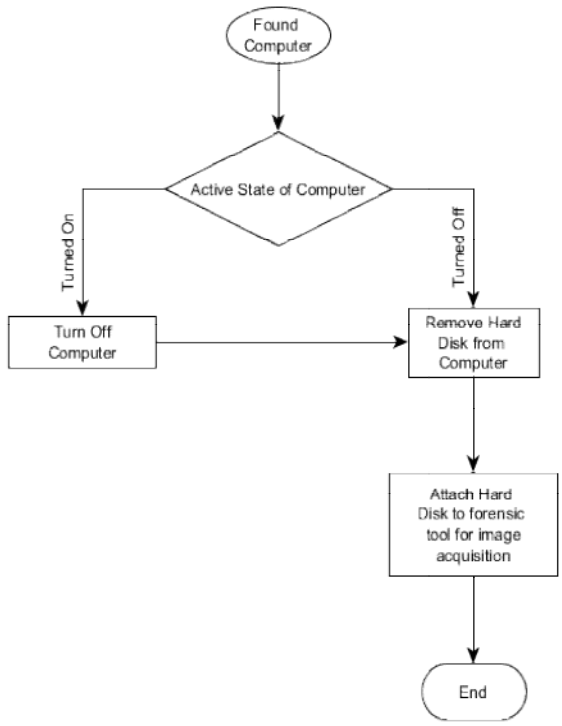

Figure 1. Dead Forensic Image Acquisition Process [3].

2. Live Acquisition

Live Acquisition of a target system means, creating an image of the system while it is functional that is image is created on spot of the crime scene with the help of forensic tools. Image acquisition in such a case is done first checking the state of the computer. If it is turned off, then the investigators must proceed with Dead Acquisition otherwise, acquisition of data should be done by using forensic tools.

Forensic acquisition tools use read only mode in the system for live data acquisition. Care must be taken that the device which contains the image after live acquisition must have write blocker enabled after the process has been finished. This ensures that data authenticity is maintained from live acquisition of the evidence.

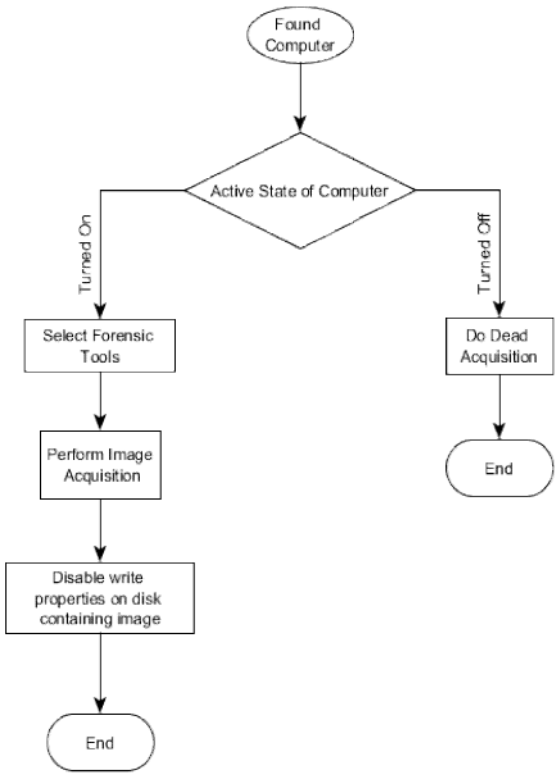

Figure 2. Live Forensic Image Acquisition Process [3].

ANALYSIS TYPES

The data acquired is further subjected to extraction and its interpretation as per the case requirements [3]. Forensic tools like, FTK, Magnet Axiom, EnCase etc.[5] are some commonly used tools for the analysing the image. There are two basic techniques of analysis of acquired data and are as follows:

1. Traditional Analysis
2. Live Analysis [5]

1. Traditional Analysis

Traditional Analysis may also be referred to as static analysis [5] because the data extraction and interpretation is done from the dead acquisition of the target system. This means that the image created during the acquisition is done through dead/ offline acquisition process.

This analysis process has been preferred by the experts in the past, because carrying the forensic tools to each crime scene was pretty hefty back when the companies manufactured

these tools as their hardware version only. So, as a result the target system containing the evidence was brought back to the lab for further process.

However, this process cannot help towards the analysis of live data from the target system. [4] This is so, because the acquisition has been done when the volatile memory was non-function. So, it can be considered as a major drawback of static analysis of data.

2. Live Analysis

Live analysis, as the name suggests is done on a target system when it is in functional state [5]. The most important functionality that live analysis brings with it is that we get to analyse the volatile memory of the system since the acquisition is done by using the Live Acquisition process.

This process also ensures that the data which is being analysed contains the description of live data generated on the system which was acquired during the period when the system is fully functional.

PROCESS MODEL FOR ON- SPOT ACQUISITION AND ANALYSIS OF RAM

Traditionally, whenever an investigation team reports to a crime scene, upon seeing the system, whether they shut down the system procedurally or simply pull the plug out. Pulling the plug preserves the current contents of the hard disk maintaining the time stamps and preserving the contents from overwriting. On the other hand, shutting the power down may alter them [6].

We do know that preservation of nonvolatile memory is possible in both these cases but this process doesn't help in findings of what constitutes where being run while the system was found in running state, because as soon as the power is cut, contents of the volatile memory are completely wiped out. As a result, acquisition of RAM data is not possible and further analysis of the same cannot be done.

In an attempt to reconsider on spot acquisition and analysis of RAM data, we've taken a target system as a computer which is functional and we'll be using two forensic software tools namely Access Data FTK Imager LITE version 4.2.1.4 [for data acquisition and will be referred as FTK Imager LITE (version 4.2.1.4)] and Magnet Axiom version 4.10.0.23663 [for data analysis and will be referred as Magnet Axiom (version 4.10.0.23663)]. These two are very powerful tools for acquisition and analysis of RAM data.

This attempt will basically tell us how RAM data can be acquired and analysed and how much data is gathered on spot of crime scene where we found the target system as functional.

Further, it must be taken care that no software or hardware changes are done on the target system before/ after data acquisition is being done/ has been done on it as doing so will disintegrate the authenticity of the evidence.

The analysed image will be directly stored on the USB hard disk on which write properties will be disabled after the process is finished. This step will ensure that image authenticity is maintained.

The investigating team will be carrying a computer having the analyser software [Magnet Axiom (version 4.10.0.23663)] installed on it which will be used to analyse the acquired image taken from the read-only USB hard disk. The image extraction will produce meta-data, which will further be organised by the software in its report improving user readability and better handson analysis of data.

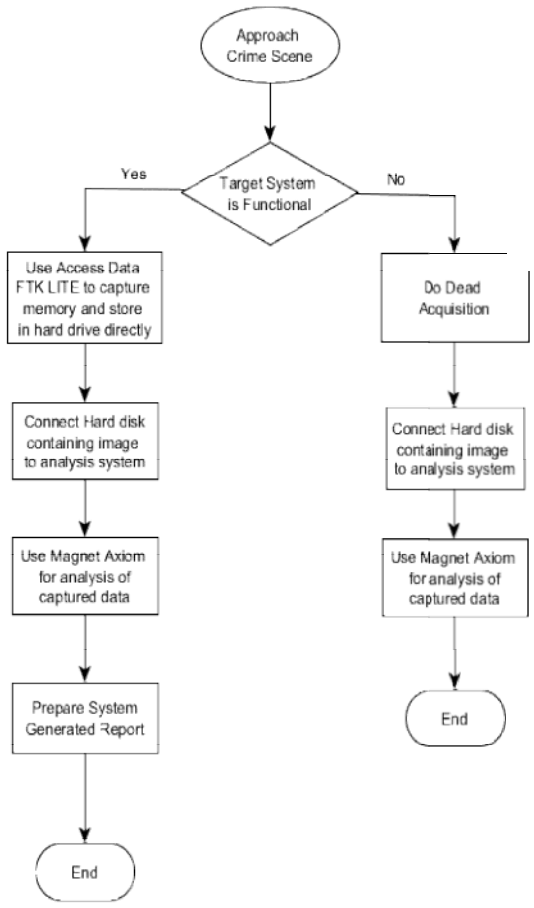

Figure 3. Process Model

IMPLEMENTATION

A. Target System

Our target system will be a desktop pc with Microsoft Windows 10, 64-bit operating system equipped with 32GB RAM, connected to the internet and with the following applications running on it:

- Windows Explorer o FTK Imager Lite (version 4.2.1.4)
- Google Chrome o Webmail o Cisco Webex Meeting
- CDR Analysis Software
- MS PowerPoint
- MS Word

Apart from these end user applications, there were many system applications that accounted to about 40% of the RAM usage i.e., the time when the system was encountered for the very first time 11.45 GB out of 32.0 GB RAM was being used.

As mentioned earlier, the system was connected to the internet through local ethernet cable using RJ-45 jack. The time when the flash pen drive containing FTK Imager LITE (version 4.2.1.4) software was inserted to the target system along with a 1 TB hard drive for data collection was 12:26 P.M. IST on 09th April, 2021.

B. Live Acquisition

As soon as the flash drive and the hard drive were connected, FTK Imager LITE (version 4.2.1.4) folder was opened and details of the end user applications were noted. After noting down all the necessary details for the research purpose, the acquisition process took place.

FTK Imager LITE (version 4.2.1.4) was launched on the target system and Capture Memory option was selected. The essential details were provided to the software like the destination folder where the acquisition dump would be store. A separate folder in the Hard Drive was created and named for the same.

This process started at 12:32 P.M. IST on 09th April, 2021 and ended after 15 minutes on 12:47 P.M. IST on 09th April, 2021. The dump file generated from this process had a size of 24.9 GB. Both the flash drive containing FTK Imager LITE (version 4.2.1.4) and the hard drive containing the Image of the target system were disconnected as soon as this process ended and the target system was powered off.

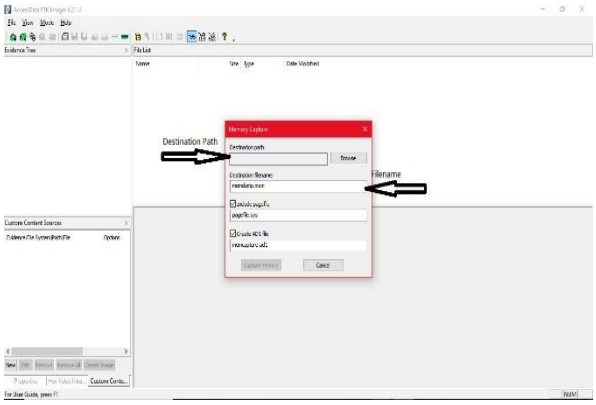

Figure 4. A look into the acquisition process using FTK Imager LITE (version 4.2.1.4). (Note: This image is just for reference and it is in no manner related to the experiment as no external disturbances were created during the experiment)

Live Analysis & Report Generation

The hard drive was connected to our system on which we had Magnet Axiom (version 4.10.0.23663) installed. On launching Magnet Axiom (version 4.10.0.23663) we created a new case for the image prepared and provided essential details to the software like case number, case name, examiner name, etc. in the AXIOM Process software. Magnet Axiom (version 4.10.0.23663) Process Software processes the image acquired. After providing other necessary information related to the Image type, the software started with the analysis phase of the image at 01:23 P.M. IST on 09th April, 2021. This process lasted for around 21 minutes and ended at 01:45 P.M. IST on 09th April, 2021.The Magnet Axiom (version 4.10.0.23663) Examine software analyses the processed image and generates the detailed report of the image.

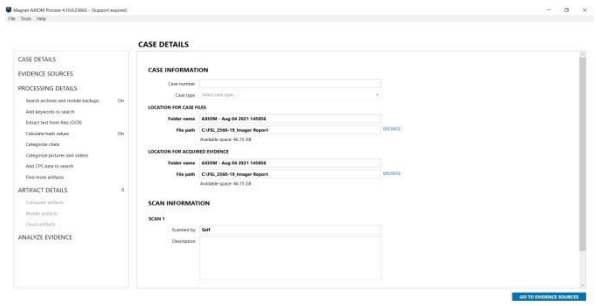

Figure 5. A look into the Magnet Axiom (version 4.10.0.23663) Process Software. (Note: This image is just for reference and it is in no manner related to the experiment as no external disturbances were created during the experiment)

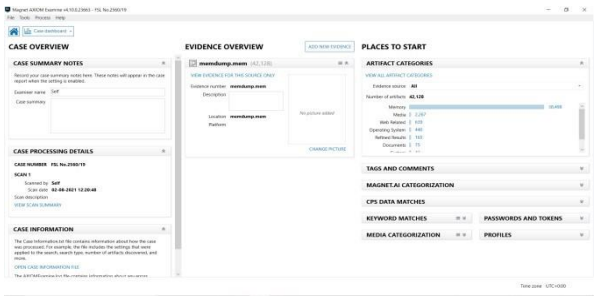

Figure 5. A look into the Magnet Axiom (version 4.10.0.23663) Examine Software.

(Note: This image is just for reference and it is in no manner related to the experiment as no external disturbances were created during the experiment)

The report generated by the software was in .pdf format and it was taken into consideration for analysis of data collected form the target system.

RESULTS & CONCLUSION

Result

Upon opening the report generated by Magnet Axiom (version 4.10.0.23663), the researcher has found that the results obtained in this experiment were astonishing and exceeded their expectation.Apart from the end user applications and system applications that were using the RAM of the target system, there was relevant data regarding social media activities and other profiles as well.

The listed data achieved from this process is as below:

- Carved Archives (content not searched): 46 items
- Carved Audio: 45 items
- Classifieds URLs: 1 items
- Cloud Services URLs: 17 items
- Edge/Internet Explorer 10-11 Content: 61 items
- Edge/Internet Explorer 10-11

Daily/Weekly History: 8 items

- Edge/Internet Explorer 10-11 Main History: 66 items
- Facebook Chat: 4 items
- Facebook Status Updates/Wall Posts/Comments: 1 items
- Facebook URLs: 86 items
- File System Information: 1 items
- Google Maps Tiles: 8 items
- Google Searches: 84 items
- Google WebP Images: 10 items
- Hotmail Webmail: 6 items
- Identifiers - Device: 38 items
- Identifiers - People: 9 items
- IP Addresses - Audio/Video Calls: 10 items
- LinkedIn Emails: 2 items
- LNK Files: 198 items
- Locally Accessed Files and Folders: 50 items
- Parsed Search Queries: 20 items
- PDF Documents: 3 items
- Photoshop Files: 16 items
- Pictures: 6507 items
- Potential Browser Activity: 3223 items
- Prefetch Files - Windows 8/10: 22 items
- RTF Documents: 5 items
- Sina Weibo Carved Searches: 2 items
- Social Media URLs: 11 items
- Twitter: 1 items
- Videos: 42 items

- Web Chat URLs: 3 items
- WebKit Browser Session/Tabs

(Carved): 3 items

- WebKit Browser Web History

(Carved): 617 items

- Windows Event Logs: 1225 items
- Windows Event Logs - Firewall

Events: 1 items

- Windows Event Logs - Office Alert Events: 1 items
- Windows Event Logs - Service

Events: 10 items

- Windows Event Logs - User Events:

  3 items
- Yahoo! Webmail: 16 items

In addition to the above results found in the research, one important thing the researcher found was that if the storage device containing the image was previously used by the investigator, all old deleted or formatted data reappeared. VII.II. Conclusion

As from the above results the researcher has found that, how much relevant RAM (Live) data we can acquire apart from system data. The use of this technique will enable the law enforcement agencies to collect relevant data (Potential evidence) regarding any case on spot.

Recommendations

- Researcher has highly recommended performing live data acquisition on spot in every such condition.
- As researcher has found that storage device containing the image of RAM data was previously used, the all old deleted or formatted data reappeared. Therefore, always use new storage device.

Suggestions

- A proper training is suggested to all investigation officers and first respondent to perform live data acquisition successfully.
- Ensure the appreciation of this digital evidence before the court.

REFERENCES

[1] Yen, Pei-Hua & Yang, Chung-Huang &Ahn, Tae-Nam. (2009). "Design and implementation of a live-analysis digital forensic system."ACM International Conference Proceeding Series. 321. 239-243. 10.1145/1644993.1645038.

[2] Mann, Harnoor Kaur and Chhabra,Gurpal Singh.(2016). "Volatile Memory Forensics: A Legal Perspective." International Journal of Computer Applications 155 (2016): 11-15.

[3] Kolhe, Mahesh and Ahirao, Purnima. (2017). "Live Vs Dead Computer Forensic Image Acquisition."International Journal of Computer Science and Information Technologies, Vol. 8 (3) , 2017, 455-457.

[4] Gupta, Pooja. (2019). "Capturing Ephemeral Evidence Using Live Forensics."IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) eISSN: 2278-2834,p-ISSN: 2278-8735. PP 109-113.

[5] Rafique, M., & Khan, M. (2013). "Exploring Static and Live Digital Forensics: Methods, Practices and Tools." International Journal of Scientific & Engineering Research Volume 4, Issue 10, October-2013 ISSN 2229-5518.

[6] Vidas, T.M. (2006). The Acquisition and Analysis of Random Access Memory. J. Digit. Forensic Pract., 1, 315-323.

[7] Lim, Kyung-Soo &Savoldi, Antonio & Lee, Changhoon& Lee, Sangjin. (2012). “Onthe-spot digital investigation by means of LDFS: Live Data Forensic System.” Mathematical and Computer Modelling. 55. 223-240. 10.1016/j.mcm.2011.05.019.

****