IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.
PP 109-113
www.iosrjournals.org

Capturing Ephemeral Evidence Using Live Forensics

Ms. Pooja Gupta
Assistant Professor, Uttaranchal Institute of Management
Uttaranchal University, Dehradun, Uttrakhand, India
Email- poojagupta010@gmail.com Mobile No: 09897858129

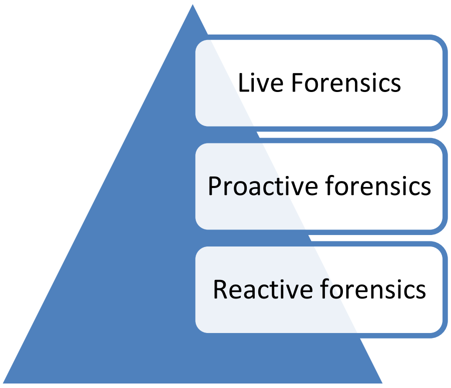
ABSTRACT: *Live forensics is a sprouting branch of digital forensics that performs the forensics analysis on active system; Active systems are normally running systems. Live forensics provides accurate and consistent data for investigation compared to incomplete data provided by traditional digital forensics process. But Live forensics still need to be tested thoroughly before the law enforcement discipline will adopt them. Therefore, in this paper, we perform the comparison of traditional forensics and live forensics. We have also highlighted the main objectives, benefits and challenges faced by live forensics.*

Keywords: *Digital Forensics, Digital Forensics Readiness, Ephemeral Evidence, Live Forensics, Proactive Forensics.*

I. INTRODUCTION

Digital crimes have increased in frequencies, and their degrees of sophistication have also advanced. There is a significant technological gap between the rate at which digital crime is increasing and the rate at which research in this direction is growing. Evidence handling is clearly a critical aspect in the expanding field of digital forensics. One of the more recent invocation 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. The emergence of highly technical nature of digital crimes has created a new branch of Digital forensics known as Live forensics. Live forensics is different from traditional digital forensics because it is applied on running system. But there are other related fields of digital forensics like proactive forensics and forensics readiness that creates a state of confusion. According to Grobler et al, Digital Forensics consists of three components: Pro-active Forensics, Active/Live Forensics and Re-active Forensics. Proactive forensics focuses on Digital Forensics Readiness. Live Forensics considers the gathering of live evidence during an ongoing attack with a limited live investigation element whilst Reactive Forensics deals with the traditional Digital Forensics [1].

Fig 1: Components of Digital Forensics



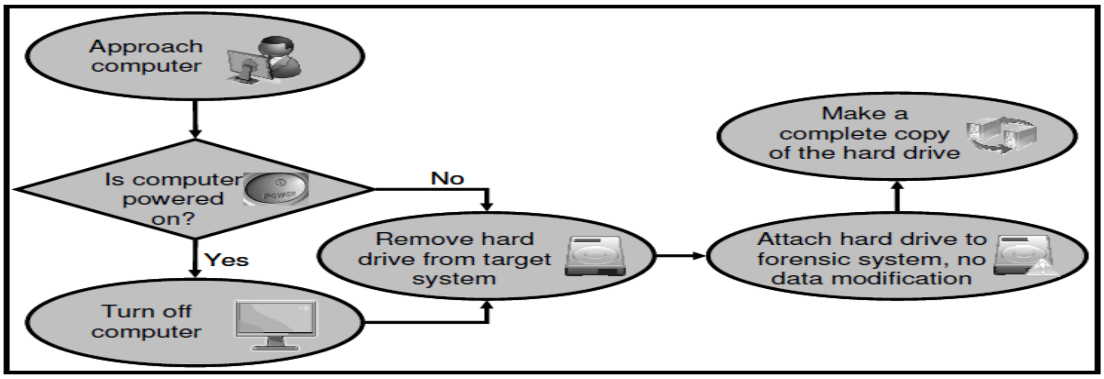
II. DIGITAL FORENSICS PROCESS

Digital forensics is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime. Murphy defines Digital Forensics as the application of science to the identification, collection, analysis and examination of digital evidence, whilst preserving the integrity of the information and maintaining a strict chain of custody for the evidence [2]. In dead acquisition analysis, analysis of data is done on a powered off computer” [3].

The Traditional forensics process cycle including the eight major phases [4]:

1. Acquiring Subpoena: Digital Forensics Investigators require search warrant/subpoena in order to conduct a search of data and seize evidence.
2. Chain of custody: In multi-jurisdictional environments. Chronological ordered documentation of evidences is required to avoid allegations of evidence tampering or misconduct.
3. Imaging/hashing function: When digital evidence is found, it should be carefully duplicated and then hashed to validate the integrity of the copy.
4. Validated tools: When possible, tools used for forensics should be validated to ensure reliability and correctness.
5. Analysis: Forensic analysis is the execution of investigative and analytical techniques to examine the evidence.
6. Quality assurance: The procedures and conclusions of forensic analysis should be repeatable and reproducible by the forensic analysts.
7. Reporting: The forensic analyst must document his or her analytical procedure and conclusions for use by others.
8. Possible presentation: In some cases, the forensic analyst will present his or her findings and conclusions to a court or other audience.

Fig-2: Traditional forensics analysis [3]


Approach computer
Is computer powered on?
No
Yes
Turn off computer
Remove hard drive from target system
Attach hard drive to forensic system, no data modification
Make a complete copy of the hard drive

III. PROACTIVE FORENSICS

Traditional forensics works on reactive approach principle:"wait until something fails and then take the necessary steps to fix it", this often results in hours or even days of lost productivity. Proactive Forensics adopts automation to make the forensic evidence gathering process proactively, allowing the digital devices (computer) to adaptively focus resources on identifying and collecting possible traces to potential transgressors, in advance of an incident alert or evidence request [5]. It involves the analytical and investigative techniques used for the identification, extraction, preservation, documentation, analysis and interpretation of digital evidence. Even though Proactive Forensics is still a young branch of Digital Forensics, the academic researchers have already had a reasonably different perspective on the focus and spirit of Proactive Forensics [6].

3.1. Definition of proactive forensics

Among all the definition of proactive forensics given by many researchers, fortoo et al. (2010) gave a more comprehensive definition covering all of the points:

"A forensic approach that focuses efforts and resources to facilitate dynamic evidence collection behavior upon detection of activities prior to an incident, storing the evidence proactively to make them amendable for future analysis and judicial review" [6]. There are three main special features of Proactive Forensics: dynamic evidence Collection, storage of relevant information, and judicial review standard evidence.

IV. RELATED DISCIPLINES

4.1. Forensic readiness

Forensics Readiness (FR) is defined as the ability of an organization to maximize its potential, in terms of preparing its system, physical and procedural security of data, and staff security-awareness, to gather data of evidential standards for admissibility, and at the same time minimizing the cost of investigation [7].

4.1.1. Definition of DFR

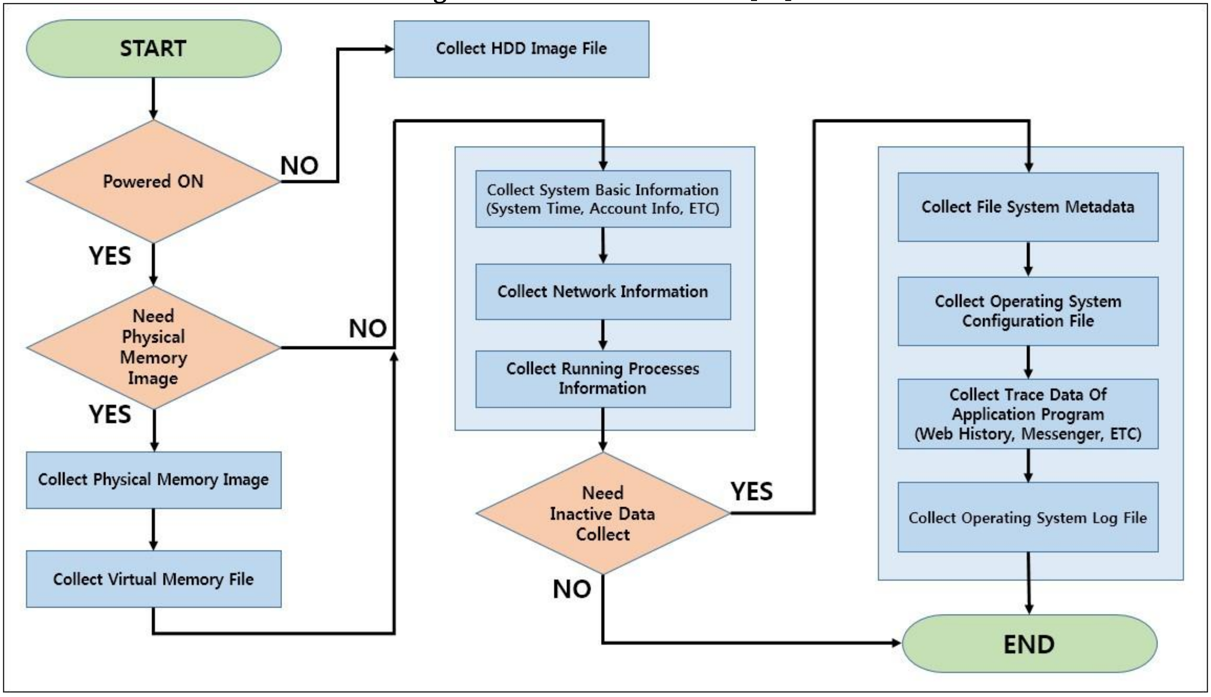
There are different definition of DFR proposed by different researchers, some of them are:

- Forensic readiness is the ability of an organization to maximize its potential to use digital evidence whilst minimizing the costs of an investigation [8]. Benefits of achieving a high level of digital forensic investigation readiness include, but are not limited to, higher admissibility of digital evidence in a court of law, better utilization of resources (including time and financial resources) and higher awareness of forensic investigation readiness [9].
- "Digital Forensic Readiness is defined as the pre-incident plan that deals with an organization's ability to maximize digital evidence usage and anticipate litigation [10].
- Digital forensic readiness is defined as the ability of an organization to maximize its potential to use digital evidence whilst minimizing the costs of an investigation [11].

4.2. Active (live) forensics

Active (Live) Forensics is another stream of digital forensics gaining notice in the recent years as an alteration to the traditional digital forensics [6]. However, its focus is on gathering relevant evidence while minimizing the effect of the incident during an on-going incident [5]. As opposed to traditional (dead) digital forensics, live forensics works to achieve retention of volatile data, and countermeasures for encrypted files on a live system, while the incident is taking place. So far the ideal existence of Proactive Forensics has been discussed through different researchers' view on its focus, the elements that it deals with, as well as how Proactive Forensics fits into the different current technologies [12].

Fig-3: Live Forensics Process [16]


START
Powered ON
NO
Collect HDD Image File
YES
Need Physical Memory Image
NO
YES
Collect Physical Memory Image
Collect Virtual Memory File
Collect System Basic Information (System Time, Account Info, ETC)
Collect Network Information
Collect Running Processes Information
Need Inactive Data Collect
YES
NO
Collect File System Metadata
Collect Operating System Configuration File
Collect Trace Data Of Application Program (Web History, Messenger, ETC)
Collect Operating System Log File
END

4.2.1. Top 10 objectives of live forensics

1. To acknowledge the importance of ephemeral data that may be lost by powering down a system.
2. To collect data while the system is still running.
3. To minimize impacts to the integrity of data while collecting evidence from the suspect system [5].
4. To gather admissible evidence legally.
5. To shorten to process of evidence collection
6. To allow an investigation to proceed at a cost in proportion to the incident.
7. To minimize interruption to the business from any investigation.
8. To ensure that evidence makes a positive impact on the outcome of any legal action
9. To maximize an environment's ability to harvest credible evidence
10. To maximize the potential to use comprehensive digital evidence.

4.2.2. Benefits of implementing live forensics

- Shortened investigation process.
- Cost efficinecy-due to short investigaton process.
- Collect better and more evidences.
- Proper acquisition and analysis of volatile data in RAM.
- Quick access to court-admissible evidence.
- Improved chances for successful litigation.

4.2.3. Table 1: Traditional Forensics vs. Live Forensics

S.No	Traditional Forensics	Live Forensics
1	Traditional forensics is performed on dead system.	Live forensics is performed on running system.
2	Traditional forensics is a reactive approach.	Live forensics is a proactive approach.
3	Ephemeral data is lost.	Ephemeral data is analyzed for the possibility of evidence.
4	Traditional forensics works on the principle:"wait until something fails and then take the necessary steps to fix it", this often results in hours or even days of lost productivity.	Live Forensics adopts automation to make the forensic evidence gathering process proactively, allowing the digital devices (computer) to adaptively focus resources on identifying and collecting possible evidences.
5	Traditional forensics cannot acquire live, volatile data. Once the computer is unplugged, the machine loses all the volatile memory in the RAM.	Live forensics collect live data - starting with RAM image and then collecting other live data "as required" such as network connection state, logged on users, currently executing processes etc.
6	If the hard drive is encrypted then it is of no use even if investigators have a complete bit for bit hard drive image of the suspect system.	If the same encrypted disk was acquired with live forensic acquisition, investigators would be able to access the disk.
7	To comply with traditional forensic requirements, all data must be gathered and examined for evidence. When dealing with computers and electronic data, the volume of data cannot only be overwhelming for digital investigators and complicate the investigation process.	Live forensic limits the amount of data gathered. Often investigators investigate large parts of the system, but only gather the relevant pieces of information [13].

4.2.4. Challenges faced by live forensics [14]

- Live forensic analysis, only provides principles of live acquisition but it is up to the interpretation of the investigator to analyze the situation, and apply the forensic principles in such a way that his/her actions can be justified in a court of law.
- Main challenges during data acquisition process are: Data modification and dependence on the suspect system's operating system, if the acquisition process alters/modify the data, courts will dismiss the data as forensically unsound.

- Slurred images are also a challenge during data acquisition process, slurred images is the result of acquiring a file system while some program modifies it. The smallest modification may cause a problem, since the file system first reads the metadata section of the hard disk. If the files or folders on the file system change after the file system have read the meta-data, but before the files system acquires the data, the meta-data and sectors do not correlate anymore [3].
- Authenticity and reliability in distrusted networks is another recurring problem concerning live forensic analysis. Anti-forensic toolkits are also widely available, and may obstruct the collection of evidence from live network sources [15].
- In some cases of live forensic acquisition, limited amounts of information is gathered. This may not always constitute a complete representation of the original affected system, and can be interpreted as possible data corruption [13].

V. CONCLUSION

We conclude that Live Forensics is a sure way to advance the digital investigation process, it is better than traditional methods of digital forensics in terms of evidence collection from volatile data in RAM, minimizing overall time of investigation. It also solves the problem of encrypted disks faced by traditional forensics, but Live forensics is still at its infancy and faces a lot of challenges. We also concluded that Live forensics is a blend of proactive forensics and Digital forensics Readiness because if evidences are to be collected from a running system then organization should be prepared in advance for investigation process.

REFERENCES

[1]. Grobler, C.P. ; Acad. for Inf. Technol., Univ. of Johannesburg, Johannesburg, South Africa ; Louwrens, C.P. ; von Solms, S.H.” A Multi-component View of Digital Forensics.

[2]. J. J. Murphey, “Forensic readiness’,” 2007. [Online]. Available: www.dexisive.com/wp-content/.../06/Forensic-Readiness.pdf.

[3]. Jones, R. 2007. Safer Live Forensic Acquisition. University of Kent at Canterbury, Available from: http://www.cs.kent.ac.uk/pubs/ug/2007/co620-projects/forensic/report.pdf

[4]. Zatyko, K. (2007). Defining Digital Forensics, Forensic Magazine.

[5]. Grobler, M(2010), ‘Digital Forensics Standards: International progress,’ Proceedings of the South African Information Security Multi-conference(SAISMC 2010).

[6]. ForToo: Forensic Tools Against Illegal Use of the Internet HOME/2010/ISEC/AG/INT/002 www.fortoo-project.eu.

[7]. Robert Rowlings on. (2004) A Ten Step Process for Forensic Readiness. International Journal of Digital Evidence. Volume 2, Issue 3.

[8]. An introduction to forensic readiness planning technical note 01/2005 27 may 2005.

[9]. Report from Dagstuhl Seminar 14092: Digital Evidence and Forensic Readiness, Edited by Glenn S. Dardick1, Barbara Endicott-Popovsky2.

[10]. Mouhtaropoulos et al, JICLT Journal of International Commercial Law and Technology, Vol.9, No.3 (2014) 173 Digital Forensic Readiness: Are We There Yet?

[11]. Tan, J. (2001); ”Forensic readiness”; Technical. Cambridge USA: @stake, Inc.

[12]. Yunting Lei, Yuyin Cui : Research on Live Forensics in Cloud Environment.

[13]. Leigland, R. & Krings, AW. 2004. A Formalisation of Digital Forensics. International Journal of Digital Evidence. Volume 3, Issue 2. Pp 1 – 32.

[14].]Lessing1 et al: Live Forensic Acquisition as Alternative toTraditional Forensic Processes”.

[15]. [15] Nikkel, BJ. 2006. Improving evidence acquisition from live network sources. Digital Investigation. Volume 3, Issue 2. Pp 89 – 96.

[16]. Available online: http://forensic.korea.ac.kr/project/livesystem.html.