ISSN:0975-9646

Live Vs Dead Computer Forensic Image Acquisition

Mahesh Kolhe,
PG Scholar, Dept. Information Technology,
K. J. Somaiya College of Engineering, Vidyavihar, Mumbai 77.

Purnima Ahirao,
Asst. professor, Dept. Information Technology,
K. J. Somaiya College of Engineering, Vidyavihar, Mumbai 77.

Abstract - In this paper, we tend to review the new opportunities for securing massive data generated from sensible resources. The paper will be a detailed introduction of malware analysis for security professionals. This paper would be an excellent fit to the Security Essentials track by providing information to assist in the gap that exists in the field, as malware issues are common in computer security today.
We tend to review the new software and hardware tools to examine the computer system. The paper will be a detailed introduction to computer forensics. This paper would be an excellent fit to the Indian scenario of computer forensics to assist in the gap that exists in the field, as issues are common in computer forensics today.
This paper will begin with introduction of computer forensic. In computer forensics for students beginning in computer forensics industry, the concepts are really confusing to understand forensic imaging. There are two different methodologies or algorithms. This paper will clear for such students to clear there perspective of forensics. we will present the instructive clarification of what a forensic and which methodology is suitable for different cases. We are going to suggest best method to apply for which case.

Keywords: Computer Forensics, Cyber Forensic Investigation, Live Acquisition, Dead Acquistion, Memory Live Acquisition.

I. INTRODUCTION

Computers undeniably make a large part of human activity faster, safer, and more interesting. They create new modes of work and play. They continually generate new ideas and offer many social benefits, yet at the same time they present increased opportunities for social harm. The same technologies powering the information revolution are now driving the evolution of computer forensics. "Computer Forensics involves the preservation, identification, extraction and documentation of computer evidence stored in the form of magnetically encoded information (data) [6]." Computer Forensics is the science of obtaining, preserving and documenting evidence from digital electronic devices such as computers, PDAs, digital cameras, mobile phones, and various memory storage devices [5].

In the last decade there has been an enormous increase in computer usage. The development of digital equipment and the availability of computer networks have had a great impact on business today. A lot of transactions that were earlier done by regular mail are today conducted through automated processes on the Internet. This shift has made corporations dependent on computers and computer networks. In the past, information was stored in large archives as paper documents. Today information is stored electronically in database and often made available over networks. All of these changes have made a lot of the work easier for companies but the downside is that companies (and private persons) are more prone to attacks in cyberspace [8].

The way of criminals committing crime is changing. There are billions of dollars are lost to teach savvy criminals by making use of computers. In such cases computer is the main evidence in cyber crimes [7]..

Cyber forensics investigation is not new field of committing crime but still based on new practice and new threats occurring. forensic investigation is totally depends on collection or acquiring of digital evidence. Cyber forensics investigation is depends on vital phase of acquisition and legal investigation process is being carried out by cyber forensic experts. Digital evidence is the integral part of digital forensic. In Indian scenario the computer forensics is used in different government department such as Income Tax , Sales Tax , cyber crime , ATS(Anti Terrorist Squad) and Intelligence bureau and in private sectors for unfriendly termination , Whistleblower etc [7].

II METHODS OF ACQUISITION

In most computer forensic examinations, the next step is to make an exact copy of the data residing on the evidence hard disk (or other electronic digital storage device). The need to create such a copy is consistent with the essential concern not to change the evidence.

There are two type of methodology can be followed for acquiring the image of digital evidences such as follows [2]:

A. Live Acquisition
B. Dead/Offline Acquisition

II.A Live Acquisition

When the investigator is to confiscate a live system there are some issues to consider before cutting the power. A live system refers to system that are up and

running where information may be altered as data is continuously processed [3]..

There is a lot of information of evidentiary value that could be found in a live system. Switching it off may cause loss of volatile data such as running processes, network connections and mounted file systems. In contrast, leaving a computer running may cause evidence to be altered or deleted. The investigator therefore needs to decide what alternative is best in a given situation. Another approach is to use specialized tools to extract volatile data from the computer before shutting it down [3].

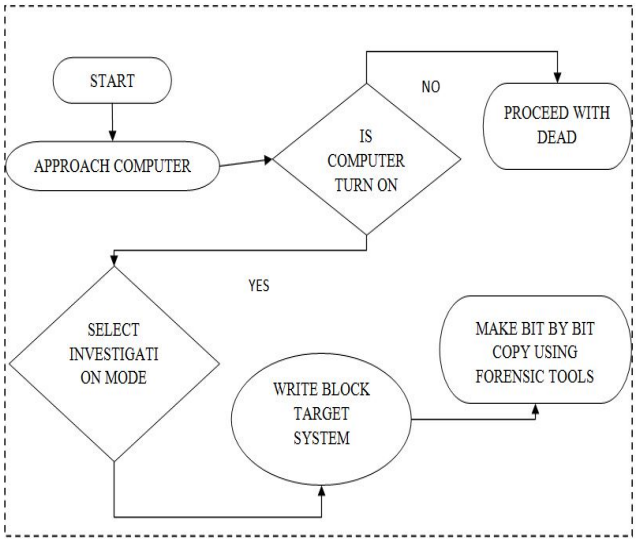

Fig 1. Live Forensic Image Acquisition

In Live Acquisition Technique is real world live digital forensic investigation process. for example a common approach to live digital forensic involves an acquisition tool into read only mode in system. then attaching writable media or disk to system and using the tool to start Live imaging in that tool by using Graphic User Interface(GUI) if available or use Command Line Interface(CUI) [2].

Myth #1

A Digital Forensics Practitioner conducting live forensics upon a system will inevitably alter that system in some manner, thus live forensics cannot be conducted as a truly forensic process [8].

Reality:

While true that conducting live forensics upon a system will inevitably alter that system in some manner, the flawed statement, here, is that this precludes the process from being a truly forensic process. In fact, there is no such requirement levied by the Court. In almost every other forensic discipline, we destroy or adulterate the evidence during the collection and analysis process [8].

II.B. Dead/Offline Acquisition

Dead system forensic can produce some information, they can't recover everything. In order to create a forensic image of an entire disk, best practice dictates that the imaging process should not alter any data on the disk and that all data, metadata and unallocated space be included [1].Traditionally, forensic investigators accomplish this by powering down the system and removing the disk (or disks) in order to connect it to a forensic workstation or hardware or software write-blocker to create the image [3]. This is referred to as dead imaging.

A write-blocker, as its name implies, will prevent any data from being written to the disk, allowing read access only. Removing a disk from a running system prevents any further changes due to normal system operations or process and user interactions. Using a write-blocker during evidence acquisition preserves the integrity of the file metadata, such as timestamps that may be relevant to the investigation [1].

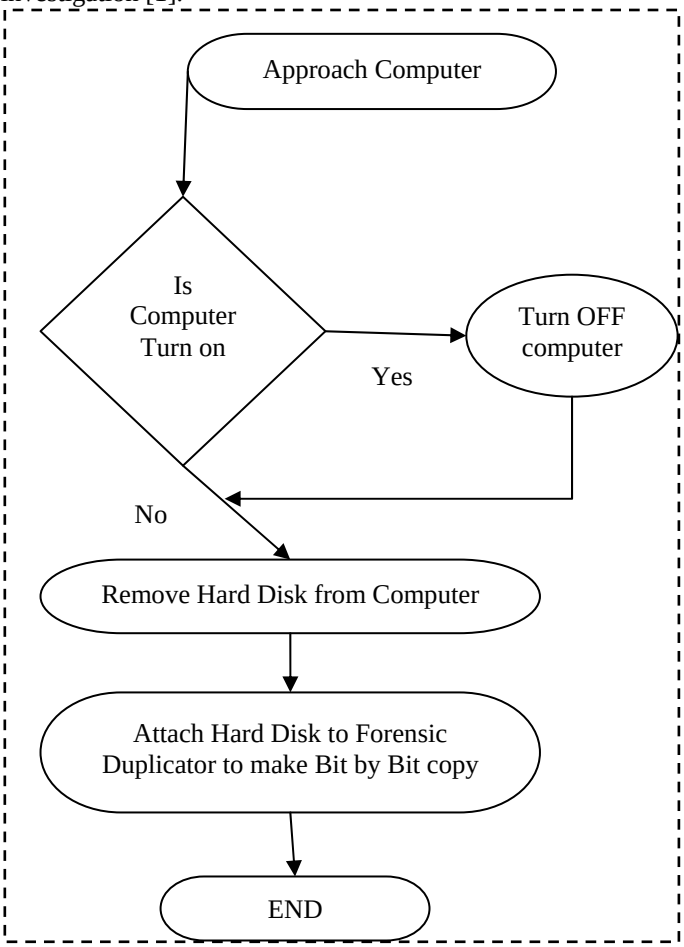

Fig.2 Dead Forensic Image Acquisition [1]

Dead systems are systems that are switched off and no data processing is taking place. To retain the integrity of the data it is often considered appropriate to cut the power supply to the computer, but this will have other implications [1].

III BEST APPROACH FOR COMPUTER FORENSIC ACQUISITION

When Computer forensic expert identify the case what are the requirements of client it totally depends on the requirements of client then Forensic investigator can decide which methodology to apply or forensic image acquiring [3].

Traditionally computer forensic investigator us the forensic Duplicator to create the clone copy or forensic image for further processing and investigating and preparing report is done in Dead Acquisition. But this method is not capturing volatile data.

When computer forensic investigator working on cases like malware forensics or need to identify the most recently file used and devices like SSD hard disks need to be acquired by live Acquisition methodology [4].

While in Computer forensics the Live Acquisition performance good as compared with Dead Acquisitions but Dead Acquisition take less time as compared to Live Because the Speed of Creating copy depend on Speed of system on processing is being carried out. In capturing RAM or Memory Live Acquisition is helpful but there is no Provision for performing or Capturing RAM in Dead Acquisition [3].

IV CONCLUSION

This included discussion of what a forensic image is and why it is useful to forensic analysts. It described common tools to create forensic images, as well as, common tools to access the images either by viewing the image file directly or by performing a file system mount to access the files. The method chosen depends on the target data. Computer forensics is important

In this work, we review advantages and disadvantages of different techniques about live forensic analysis and static/dead image analysis, we analyze that due to increase in cyber crime the live analysis is the best way to investigate the target system, also live forensic analysis have so many advantages over static analysis or Dead Acquisition.

REFERENCES

[1] Safer live forensic acquisition Ryan Jones University of Kent: Canterbury, UK, 2007.

[2] Modeling Live Forensic Acquisition M.M. Grobler1 and S.H. von Solms Proceedings of the Fourth International Workshop on Digital Forensics & Incident Analysis (WDFIA 2009).

[3] Live Forensic Acquisition as Alternative to Traditional Forensic Processes , Marthie Lessing

[4] SWGDE Best Practices for Computer Forensics Version 2.1 (July 2006).

[5] An Overview of Computer Forensics , Journal of Innovation in Computer Science and Engineering, Vol. 2(2), Jan - Jun 2013 @ ISSN 2278-0947

[6] EFFECTIVE DIGITAL FORENSIC ANALYSIS OF THE NTFS DISK IMAGE, UbiCC Journal – Volume 4 No. 3,Special Issue on ICIT 2009 Conference - Applied Computing.

[7] An Insight View of Digital Forensics, International Journal on Computational Sciences & Applications (IJCSA) Vol.4, No.6, December 2014.

[8] Dispelling Common Myths of "Live Digital Forensics" By Matthew J. Decker, DFCP, Warren G. Kruse II, DFCP, Bill Long, DFCP, Greg Kelley, DFCP.