FORENSIC TOOLS FOR INVESTIGATING CYBER CRIMES

Ala Berzinji[1,2]

[1]Department of Computer and Systems Sciences, Stockholms Universitet, Stockholm, SWEDEN, &
[2]Department of Computer Science, Faculty of Science and Education Science, University of Sulaimani, Sulaimani, IRAQ.

ABSTRACT

Nowadays in the developed countries, most of the governmental and private organizations use technology for running their activities. Using Internet, is becoming part of daily routine for running the organizations. However, despite all the benefits of information technology systems and internet, there are big risks on the users. Various states and even terrorist groups have benefited from technology for obtaining intelligence data, recruitment, propaganda, and attacking their opponents. Cyber forensics is legally admissible way of collecting, analyzing and reporting on digital data. It can be used in the detection and prevention of crime and finding the digital stored evidence of the crime. Discussion and presenting forensic models and areas in which they are useful and could be augmented is important to reach the goal of this research. This paper presents some cyber forensic methodologies of science of capturing, processing and investigating data from computers to discover evidence that is acceptable in court of law. The evidence samples is founded in the hard disks, file systems, deleted files, partitions with the windows forensics techniques, investigating Volatile Data and non-Volatile data. Then finding the evidence of been a part in the Cyber crime will be presented. Hence, cyber terrorism system emerges which can destroy its opponent systems and all the systems, associated with it. Especially in countries and regions lack a national security agency capable of finding public information. In a country like Iraq there is no any organization responsible for finding cyber attackers. User and administrators of the systems have to find digital evidence by themselves to prove identity of an attacker. Security forensics, the application of investigation and analysis techniques, preserve evidence for cyber crime which is very important to detect cyber criminals in those regions. Thus provides digital evidence which helps in revealing identity of hidden attackers.

Keywords: Cyber Forensic, Cyber Crime, Cyber Terrorism, Security Forensic

INTRODUCTION

Cyber crime is defined as “any illegal act that involves a computer, its systems, or its applications.” Cyber crimes are intentional. Cyber criminals have become more organized than in the past and are considered more technically advanced than the agencies that plan to thwart them. Today’s computer crimes pose new challenges for investigators due to their speed, anonymity, and the fleeting nature of evidence [4].

Cyber crimes are generally consists of the tools of the crime and the target of the crime. The tools of the crime are the evidence that the forensic investigator must analyze, process, and document. This may include various hacking tools used to commit the crime or the computer/workstation where the crime was committed. Forensic investigators usually take the entire system used, including hardware such as the keyboard, mouse, and monitor. And the target of the crime, is the victim. The victim is most often a corporate organization, Web site, consulting agency, or government body. The target of the crime is also usually where the computer forensic investigator examines the crime scene. Since investigators are mainly dealing with digital rather than physical, this can often be a virtual environment. So Cyber

Leena and Luna International, Chikusei, Japan.
(株) リナアンドルナインターナショナル, 筑西市,日本
ISSN: 2186-8476, ISSN: 2186-8468 Print
www.ajsc. leena-luna.co.jp

crime involves illegal exploitation of computer technologies. Some types of cyber crimes are : Hacking, Computer viruses and worms, Identity theft, Webjacking, Denial of Service

The growth of the Internet and the worldwide proliferation of computers have increased the need for computing investigations. Computers can be used to commit crimes, and crimes can be recorded on computers. Law enforcement, now rely on the methods of cyber forensics to investigate criminal and civil cases. This Research is not intended to provide comprehensive training in computer forensics. It does, however, give you a solid foundation by introducing cyber forensics investigation methods and tools [3].

Cyber forensics is the preservation, identification, extraction, interpretation, and documentation of computer evidence, to include the rules of evidence, legal processes, integrity of evidence, factual reporting of the information found, and providing expert opinion in a court of law. Thus In solving Cyber crime cases, Cyber forensics techniques and tools is used to gather evidence, which will be analyzed and presented to a court of law to prove the illegal activity. It is important that when doing computer forensics no alteration, virus introduction, damages or data corruption occurs [2].

In order to do a good analysis the first step is to do secure acquisition of computer evidence. And generate hash to provide the evidential integrity and security of information. The best approach for this matter is to use Data acquisition tools and hashing tools. After that the investigator performs some methods and techniques to extract the data found in the digital evidence found at the crime scene then interpret them and the last step in Forensic Investigation is Documentation which is a major part of any investigative process and it is used as evidence during the trials in a court of law and an investigation document must contains Methods of investigation, Description of data collection, Error Analysis, Results and comments [4].

Data acquisition is the process of copying data. For computer forensics, it's the task of collecting digital evidence from electronic media[7]. There are two types of data acquisition: static acquisitions and live acquisitions. The processes and data integrity requirements for static and live acquisitions are the same. The only shortcoming with live acquisitions is not being able to perform repeatable processes, which are critical for collecting digital evidence. The physical items obtained from the scene of an indent during an investigation. Also called first-hand evidence and best evidence.

Once you have acquired a copy of original evidence you then duplicate copy to make multiple work copies from which you perform your analysis, every copy made must be exact duplicate of an original evidence and verifiably so then the original evidence safely stored in secure location. It is always preferable to work from work copies of evidence rather than working directly of original evidence, if anything happens changing original evidence your investigation could be negatively impacted[8]. Data Acquisition is different than regular copying operation because regular copying operation only copies content of files and folders of media storage however the forensic examiner needs to copy everything on media storage, which includes, Files and folders, Erased files from unallocated space, Boot partition and File system formatting .

Most of this information cannot be copied using regular copying operation, So that is the reason in investigation investigator use data acquisition methods because acquiring an image from digital media storage device requires copying every bit of data from the devices storage media starting with the first sector call "Sector 0" and ending with the last sector on the media storage the copying proceeds in order between these two sectors This type of copying is

called "Bit by Bit Copy" or "sector copy". Therefore Sector is the smallest readable/writable area of digital media and Sector size is typically 512 bytes (4096 bits). The entire sector must be read and written. Remaining sector space (slack) is backfilled with zeros or random byte values copied from RAM. Static Data Acquisition is one of the most basic and common ways of acquiring data in computer forensics. Static acquisition acquires data from a non-volatile source [4].

After Data Acquisition, File verification needs to be done to every acquisition copies that are made in the previous step, so file verification is the process of using an algorithm for verifying the integrity or authenticity of a computer file. This can be done by comparing two files bit-by-bit, but requires two copies of the same file, and may miss systematic corruptions which might occur to both files. A more popular approach is to also store checksums (hashes) (message digests) of files for later comparison [5].

Cyber crimes have been a prevalent topic in the media for several years, although the first computer crime committed was in 1971, it is only since the new forensic science disciple is fast becoming progressively popular as the proliferation of advancing technology is enterprising illegal activities [2]. In past researches a technique to data acquisition from storage device and from memory using only tools in Linux operating system or only tools in windows operating system. But in this research proposed approach works on using tools in both Windows and Linux operating system in detail and how to obtain information from the dump of the live image of a volatile memory and how to recover deleted files, however in this research we described a collection of tools and techniques to perform cyber forensic investigation. Since technology in today's world becomes a critical part of our lives although technology benefits our lives greatly but Technology is not the problem. But it is the way that people use it.

Cyber criminals and even terrorist groups have benefited from technology for obtaining information, financial gain or many purposes .The need for computer forensics has become more apparent with the exponential increase in the number of cyber crimes and litigations in which large organizations are involved. In our research we want our country to be aware of science of cyber forensics which is become a necessity for government agencies and organizations to solve cases involving the use of computers and related technologies. And cyber forensics offers the many benefits to organizations some of them is Ensures the overall integrity and continued existence of an organization's computer system and network infrastructure.

Also helps the organization capture important information if their computer systems or networks are compromised. It also helps prosecute the case, if the criminal is caught. Extracts, processes, and interprets the actual evidence in order to prove the attacker's actions and the organization's innocence in court.

Cyber crimes have been a prevalent topic in the media for several years, although the first computer crime committed was in 1971,it is only since the new forensic science disciple is fast becoming progressively popular as the proliferation of advancing technology is enterprising illegal activities [2]. In past researches a technique to data acquisition from storage device and from memory using only tools in Linux operating system or only tools in windows operating system. But in this research proposed approach works on using tools in both Windows and Linux operating system in detail and how to obtain information from the dump of the live image of a volatile memory and how to recover deleted files, however in this research we described a collection of tools and techniques to perform cyber forensic investigation.

Leena and Luna International, Chikusei, Japan.
(株) リナアンドルナインターナショナル, 筑西市,日本
ISSN: 2186-8476, ISSN: 2186-8468 Print
www.ajsc. leena-luna.co.jp

METHODOLOGY

All Cyber forensic phases are (preservation, identification, extraction, interpretation, and documentation) is to detect a cyber incident, identify the intruder, and prosecute the perpetrator in a court of law. With an increase in computer crime incidents ranging from theft of intellectual property to cyber terrorism, Cyber forensic methodologies play a decisive role in overcoming and tackling computer incidents. Due to the growing misuse of computers in criminal activities, there must be a proper set of methodologies to use in an investigation. The evidence acquired from computers is fragile and can be easily erased or altered, and the seized computer can be compromised if not handled using proper methodologies. The methodologies involved in computer forensics may differ depending upon the procedures, resources, and target company and cases. Forensic tools enable the forensic examiner to recover deleted files, hidden files, and temporary data that the user may not locate [1]. Cyber forensic methodologies consist of the following basic activities:

1- Preservation: The forensic investigator must preserve the integrity of the original evidence. The original evidence should not be modified or damaged. The forensic examiner must make an image or a copy of the original evidence and then perform the analysis on that image or copy. The examiner must also compare the copy with the original evidence to identify any modifications or damage. 2- Identification: Before starting the investigation, the forensic examiner must identify the evidence and its location. For example, evidence may be contained in hard disks, removable media, or log files. Every forensic examiner must understand the difference between actual evidence and evidence containers. Locating and identifying information and data is a challenge for the digital forensic investigator. Various examination processes such as keyword searches, log file analyses, and system checks help an investigation.

3- Extraction: After identifying the evidence, the examiner must extract data from it. Since volatile data can be lost at any point, the forensic investigator must extract this data from the copy made from the original evidence. This extracted data must be compared with the original evidence and analyzed.

4- Interpretation: The most important role a forensic examiner plays during investigations is to interpret what he or she has actually found. The analysis and inspection of the evidence must be interpreted in a lucid manner.

5- Documentation: From the beginning of the investigation until the end (when the evidence is presented before a court of law), forensic examiners must maintain documentation relating to the evidence.

FORENSIC INVESTIGATION TOOLS TO FIND CYBER CRIMES

The first step in our research live acquisitions are especially useful when you're dealing with active network intrusions or attacks or you suspect employees are accessing network areas they shouldn't. Live acquisitions done before taking a system offline are also becoming a necessity because attacks might leave footprints only in running processes or RAM, So we needs a convenient way to take a memory snapshot of the host.

Dump is a convenient tool from MoonSols for Windows Operating System. After Live Acquisition we begin Static acquisition which is one of the most basic and common ways of acquiring data in computer forensics. Static acquisition acquires data from a non-volatile source. For example, a hard drive. In a non-volatile source of data, data still remains on the storage part of the device after a device is turned off. Using FTK Imager tool in Windows

Operating System. Then static Acquisition in Linux operating System by dd tool which Historically, nearly every Linux/UNIX distribution has included a command known as dd (disk-to-disk). And dcfldd tool which is an enhanced version of dd developed by the U.S. Department of Defense Computer Forensics Lab. Then we verify the image acquisition by File verification which is the process of using an algorithm for verifying the integrity or authenticity by generating hashes for every image files after that we analyze our image files by recover my files tool in windows operating system to recover deleted files and partitions in image copy of evidences and analyze memory acquisition by pulling information about running processes and network connection information and pulling out administrator password in RAM.

Then we will try to analyze the image we created by recovering deleted data. There are Many tools on the market to recover deleted files and all of them are adequate to do the job. Here, In this research we will be using a trial version of RecoverMyFiles after we created an image of the Flash drive by static data acquisition technique.

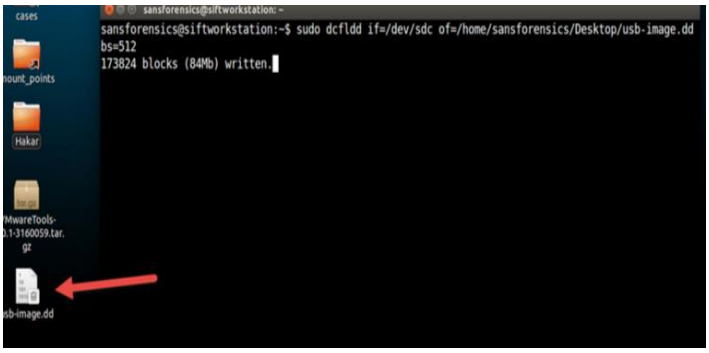
TOOLS AND TECHNIQUES

In this research several software and hardware has been used to fulfill the goal of the work:

1- Operating System (Windows 7, Linux(SIFT , Ubuntu)).
2- Forensic Program Tools (Recovery tool for deleted data (Recover my files), Bit-stream acquiring tools (FTK Imager, dd, dcfldd),memoryAnalysis.
3- (Volatile Framework), Hashing tool(md sum)).
4- Removable Disks.

The following techniques explains the steps involved in a forensic investigation:

1- Live Data Acquisition is performed if the suspected machine is not turned off the first acquisition is live acquisition to create image copy of Random Access Memory.
2- Static Data Acquisition is performed after live acquisition, which the Two bit-stream copies of the evidence are created. The orgin- nal disk must not be tampered with as it might negatively impact the investigation.
3- Hashing after acquisition technique, An MD checksum is generated on the images to pr serve the integrity of the original evidence.
4- The original evidence is stored in a secure location, preferably away from an easily a cessible location.
5- The image copy is analyzed for evidence by searching or recovering deleted data.
6- A forensic report is prepared. It describes the forensic method and recovery tools used.



RESULT

As we discussed methodologies and techniques and tools about how perform to forensic investigation, as the result of this research is to help individual victims and organizations and government agencies to capture important information if their computer systems are compromised. It also helps prosecute the case, if the criminal is caught. And extracts, processes, and interprets and recover the actual evidence in order to prove the attacker's actions and the victim's innocence in court and we can ensure that no possible evidence is damaged, destroyed, or compromised by the forensic procedures used to investigate the crime (preservation of evidence).

To start the work, first Open the DumpIt Tool as showed in figure one and then start the Live acquisition then the snapshot of memory save it in the same directory of the DumpIt Tool as shown in figure 2. Then the command of dd tool to make acquisition image of usb device and /dev/sdb is the address of mounted physical usb device. Then the image.dd will be appear on the desktop and the process of image acquisition begins and the usb-image.dd appears on desktop as shown in figure 3.

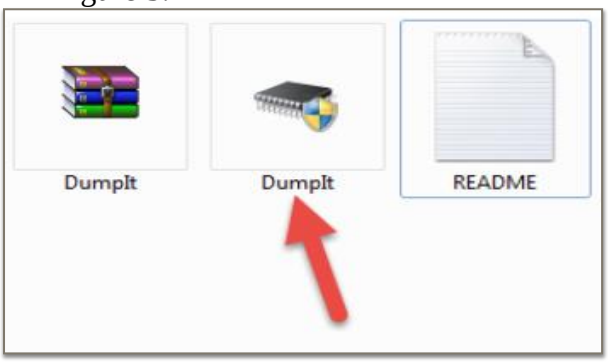


Figure 1: The DumpIt Tool

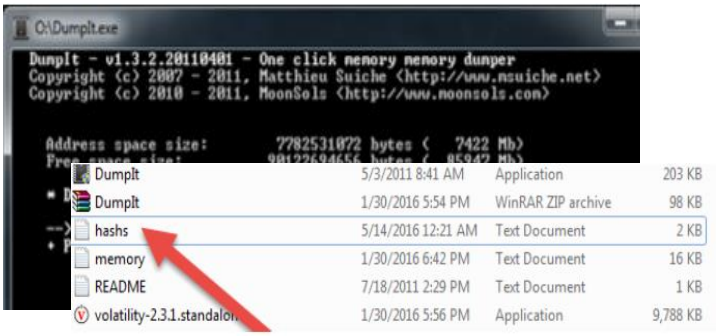


Figure 2: Start the Live acquisition

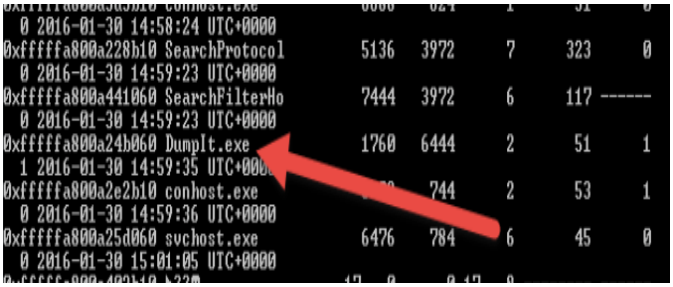
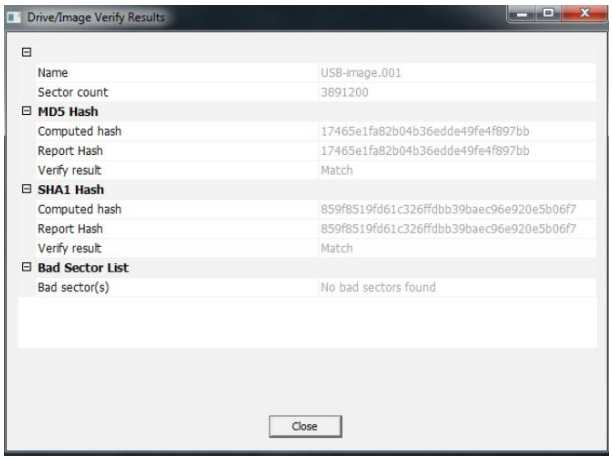


Figure3: Illustrates that the process of image acquisition begins and the usb-image.dd appears on desktop

Then with the FTK Imager program an image acquisition created and shows the source of the device and saved on the computer. The the process of FTK Imager generated MD5 and SHA-1 hash for the image to verify integrity of the image as showed in figure 4.

Figure 4: Illustrates that the process is done and FTK Imager generated MD5 and SHA-1 hash for the image to verify integrity of the image.



After getting a copy of MD5 and Hash file, then we will look for physical address of the System Registry and SAM file and create a text file witch contains hashed passwords of administrator and user accounts. The text file and will be created with hashed passwords as illustrated in the figure 5.

Figure 5: Illustrates that text file which contains hashed passwords of windows accounts.

After that the memory analysis step will start, figure 6 will illustrate the process list of application that were running at the time where we snapshotted the image of the RAM. Figure 6: The process list of application that were running in RAM.

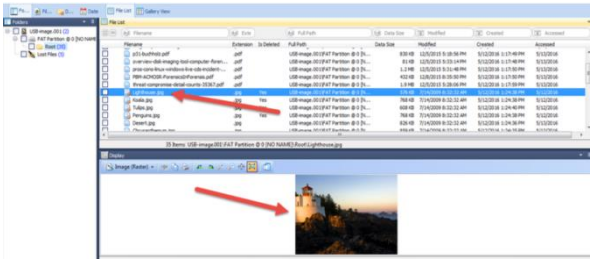


Figure 7: The file types recovered from the selected drive.

After illustrates the command for creating the text file to copy the process, we will start getting the network information of running processes. After that the recovery drive will start wizard to recover deleted files. Finally with a provided path to the image file created with FTK Imager a path to the processing of recovery files will begins and as shown in figure 7, the files will start recovery and appear on the device.

CONCLUSION

In this research, we examined distinctive forensic tools used for investigating cyber crimes in digital forensics and also the detailed review of cyber forensics. Digital evidence can also be obtained from the data structure locate in memory by using different tools and storage devices. The new process model is opted to collect crucial evidence quickly and investigate

Leena and Luna International, Chikusei, Japan.
(株) リナアンドルナインターナショナル, 筑西市,日本
ISSN: 2186-8476, ISSN: 2186-8468 Print
www.ajsc. leena-luna.co.jp

the cases immediately. The Stepwise Forensic Process Model presents the approach provides incident preservation, recovery, analysis. It is based on the crime scene circumstance and is intended to quickly selecting and investigating the system. In forensic preservation process we described in detail how to perform acquisition and verify the files by generating hashes for them. In forensic analysis, the sophisticated forensic tools are required to examine deleted files in unallocated space in storage devices and how to recover them. Due to rapid increase in the number of Internet users across the world, the frequency of digital attacks has increased. Therefore, the need to devise effective methodologies and techniques and develop efficient tools to detect these attacks timely. In this research, we have examined different tools for performing digital forensic investigation. This research provides a provisional This research provides a provisional study of the tools and cyber forensic analysis.

REFERENCE

[1]. Brajendra, P., Giordano, J., & Kalil, D. (2006). Next- Generation CYBER FORENSICS.

[2]. Bill, N., Phillips, A., & Steuart, C. (2009). Guide to Computer Forensics and Investigations 4th Edition.

[3]. EC-Council Press. (2010). Computer Forensics Evidence Collection & Preservation.

[4]. Felix C. F., & Schwittay, B. (2011). A Common Process Model for Incident Response and Computer Forensics.

[5]. Henry, B. W. (2011). Gathering Evidence in a Computing Environment. http://www.moreilly.com/CISSP/DomA-3-Importance of Standard Methodology in Computer Forensics.pdf

[6]. Jim, M. (2000). Importance of a Standard Methodology in Computer Forensics.

[7]. Madihah, M.Si. (2012). An Overview Of Disk Imaging Tool In Computer Forensics.

[8]. Yunus, Y., Ismail, R., & Hassan, Z. (2011). Common Phases Of Computer Forensics Investigation Models.