Digital Forensic Acquisition and Analysis Tools and its Importance

Inikpi O. Ademu[1], Chris O. Imafidon[2]
[1]School of Architecture, Computing and Engineering, University of East London, Docklands Campus, London, United Kingdom
[2]*School* of Architecture, Computing and Engineering, University of East London, Docklands Campus, London, United Kingdom,
[2]Former Head of Management Unit, Queen Mary, University of London, London, United Kingdom

Abstract *- There are many digital evidence collection and analysis tools that are commercially available. The digital forensic field has created different opportunities for commercial enterprises and open source alternatives. In dealing with digital forensic investigation, in solving digital related crime evidence is gathered and analyzed and presented to a court of law to prove that illegal activity has occurred. It is important that when undertaking digital forensics investigation no alteration, damages or data corruption occurs. Choosing and using the right tools and techniques are very important in digital forensic investigation. The digital forensic techniques mentioned in this thesis are as follows. The aim of this research is to discuss the commonly used digital forensic acquisition and analysis tools and the need for such tools.*

Keywords - ***Acquisition, Analysis, Automated tools, Computer Forensic, Mobile Forensic***

1. Introduction

Casey (2004) defined digital evidence as any data stored or transmitted using a digital device that support or refute a theory of how an offense occurred or that address critical element of the offense such as intent or alibi. Nelson et al (2004) explains that digital forensic involves scientifically examining and analyzing data from digital device storage media so that the data can be used as evidence in court. Investigating digital devices typically includes securely collecting digital data, examining the suspect data to determine details such as origin and content, presenting digital based information to courts, and applying laws to digital practice. Digital forensics investigates stored or transmitted data from any digital devices.

According to Farrell (2009) tools that perform specific functions are constantly being developed and distributed in the academic and open source communities and these new functions are ultimatelly integrated into larger analysis suites. These suites can be large Graphical user interface based programs that allow an analyst to explore and search the data on a hard drive. GUI tools give an option for the investigator who wants to safely preview digital evidence prior to initiating the forensic process. An investigator can have a quick scan of digital media using read-only tools without altering any data in the media Few software developers have recently introduced digital investigation tools that work in windows, Graphical User Interface forensic tools do not require a strong understanding of MS-DOS and the various file system, they can simplify digital forensic investigation (Nelson et al, 2004). These GUI tools have simplified training for beginning examiners in digital forensic. GUI tools aid in logical examination of file structures, image scan, and keyword search.

2. Process of Digital Forensic

In digital forensic expertist as examiners are relied upon to interpret data and information retrieved by tools and provide findings by tools that can be trusted. According to Altheide and Carvey (2011) the process of digital forensic can be broken into acquisition, analysis and presentation. Acquisition refers to the collection of digital devices to be examined, these can be physical hard drive, optical media, storage cards from digital cameras, mobile phones, chips from embedded devices or single document files. The acqisition process should consist of creating a duplicate of the original data as well as maintaining good records of event carried out (Ademu et al, 2011). The goal of digital evidence duplication is to copy the original digital evidence that protects and preserves the evidence from destruction, damage, or alteration prior to analysis by the digital forensic practitioner.

Duplication is an accurate digital reproduction that maintains all contents and attributes, and all slack space is transferred. When duplicating or copying evidence, ensure that the examiner's storage device is forensically sterile. Write protection should be initiated to preserve and protect original evidence. The MD5 or SHA-1 hashing algorithm should be used prior to duplication or copying. The write protection can be performed via either hardware or software. Please note that the formatted area is not the total storage of the drive, there can be some unallocated area of storage in hard drive. Hosted Protect Area (HPA) defined as a reserved area for data storage outside the normal operating file system Nelson et al (2004). The Protected Area of Run Time Interface Extension Services (P.A.R.T.I.E.S) is hidden from the operating system and file system, and that is normally used for specialized application. Duplicate or copy the electronic evidence to the examiner's storage device using the appropriate software and hardware tools.

According to the Digital Forensic Research Workshop (DFRWS) in 2001 Analysis refers to the actual media examination, the identification consist of locating items present in the device in question and then futher reducing this set of items that is needed (Palmer, 2001). This items are then subject to the approprate analysis. The types of analysis carried out can be file system analysis, file content examination, log analysis, statistical analysis etc.the examiner then interprets results of this analysis based on the examiners training, expertise, experimentation and experience. And presentation is when the examiner shares results of the analysis phase with the interested professionals. This involves generating report of actions taken by the examiner, uncovered evidence and the meaning of the evidence.

3. Computer Forensic Tools

Digital evidence is characterized by its fragile nature and it can easily be altered or destroyed, thus rendering it inadmissible in a court of law. Digital investigator should therefore take care to ensure that evidence is not destroyed as a result of a continuous investigation. One of the major time consuming tasks in a digital investigation is the search for digital evidence. Different toolkits have been developed that contain tools to support digital investigators in the process as much as possible in an attempt to increase the efficiency of a digital investigation.

- **Password Recovery Toolkit (PRTK)**

The Password Recovery Toolkit (PRTK) is an AccessData tools which is a Graphical User Interface appliaction for Windows. This tools helps to find and identify encrypted files on handheld, desktop and server computer systems, it can interpret the passwords or hashes of password in application such as Office 2000, WinZip etc. Recently an advance in the encryption function in Microsoft Offic XP, Internet Explorer and Netscape Navigator has posed concern. A new feature is added to PRTK known as the Distributed Network Attack (DNA) application (Aggarwal et al, 2008).

- **Distributed Network Attack (DNA)**

DNA is a password recovery tool with a twist. It uses multiple computers rather than a standalone system to attack a password encrypted file. DNA uses the concept of a network to allocate jobs to client machines to work on. DNA uses the power of multiple processors to make an exhaustive key space attack. The larger the network, the greater the number of machines and password attempts per second that can be tried. With the help of DNA investigators can crack the passwords of numbers of networked workstations, reducing the time needed to crack the most difficult passwords.

- **Forensic Toolkit (FTK)**

Forensic Toolkit is identified as the standard in computer forensic software. It is a court validated digital investigations platform that delivers computer forensic analysis, decryption and password cracking software all within an spontaneous and customizable interface. FTK supports PRTK, password list can be created, these are collection of words that appear to be character strings, a password list generator collects these character strings to create a list that PRTK uses to crack passwords. FTK is the only commercial forensic software product that supports both 32 bit and 64 bit Windows machines. FTK Toolkit is easy to use and understand, it has multiple data views that allow users to analyse files in a number of different ways and create detailed report and output them into native format. According to Jones et al (2005) recent versions of the FTK includes acquisition functionality, a forensic duplication can be acquired using FTK with the same hardware devices. FTK has unique features that index text to produce instant search result, data recovery from file system, e-mail recovery from the leading e-mail services and products along with the recovery of deleted messages, file filtering that eliminate known files and bad files.

- **EnCase**

EnCase is a commercial forensic investigation toolkit that is largely used within the law enforcement agencies. According to Nelson et al (2004) EnCase is able to acquire data in a forensically sound way in which such data can be reviewed by other popular commercial forensic analysis tools. The software can manage large volume of digital evidence, and transfer evidence files directly to law enforcement or legal

representatives as necessary. It enables attorneys to easily review evidence and also enables quick report preparation to be made. EnCase program has initiated Graphical User Interface tools for digital investigations.

A recent features of DOS disk acquisition amd preview tool called En.exe has been added to to EnCase. The GUI EnCase and the DOS En.exe programs create images of a suspect's disk drive. EnCase can also acquire a suspect'd disk drive on a network. Encase version 2.0 supports some Microsoft file system types such as FAT12, FAT16, FAT32, New Technology File System (NTFS), Universal Disk Format (UDF) etc. According to Casey (2002) EnCase provides an incredible amount of features and functionality but no one tool can do it all in forensic investigation. An important feature of the EnCase process is the integrated authentication and verification of evidence files. Throughout the examination process, EnCase verifies the integrity of the evidence by recalculating the Cyclical redundancy check (CRC) and the MD5 hash values and comparing them with the values recorded at the time of acquisition. This verification process is documented within the EnCase generated report. It is important to know that it is impossible for EnCase to write to the evidence file once it is created. Just like in other files, it is possible to alter EnCase evidence file with a disk-editing utilty. Though, if one bit of data on the collected evidentiary bit-stream image is altered after acquisition, EnCase will report a verification error in the report and identify the location of the registered error.

- **Deleted Data (DD)**

The most basic non commercial forensic duplication tools is definitely dd (Jones et al, 2005). One reason examiners use forensic imaging is for completeness. In foresnsic examination the idea of just examining an active file system as presented by the operating system is not sufficient enough. Most volumes contain potentailly required evivence outside of the viewable, allocated files on a mounted file system. Delected files are files that have been unlinked in which the file name entry is no longer presented when a user views a directory and the file name, metadata structure, and data units are marked as free. However the connections between these layers are still undamaged when forensic techniques are applied to the file system. Therefore in recovering the files it consist of recording the relevant file name and metadata structures and then extracting the data units.

- **Coroner Toolkit (TCT)**

TCT is designed by Dan Farmer and Wietse Venema, the Tct is aims primarily at investigating a hacked Unix host. It offers tools with useful investigative capabilities that are available nowhere else Kruse II and Heiser (2001). TCT is designed to help in reconstruction of event on a compromised network host. The most interesting feature of TCT is its ability to analyze activities on a live host and capture current state information that would be impractical to capture manually. TCT comprise a set of tools used to recover deleted auanix files. It contains a tool to attempt to reconstruct rational or logical data from a stream of bits, and it includes a tool for the Unix environment to create such a stream of bits from a file system. The unrm utility is a Unix tool that creates a single object containing everything that is within all the unallocated space on a file system which can be a huge amount of data.

- **Sleuth Kit**

Sleuth Kit is an open source forensic toolkit which is a suite of file system forensic tools designed by Brian Carrier to perform forensic analysis or investigation in Unix environment, the first version of Sleuth Kit was called the @stake Sleuth Kit (TASK) which was based on The Coroner's Toolkit (TCT) and was distributed with similar command line tools Kruse II and Heiser (2001). TCT ia a very powerful forensic analysis tools but its major challenge is the lack of portability between system and lack of support for non Unix-like file systems. Carrier developed the Sleuth Kit to provide a highly portable extensible and useful open source forensic toolkit. Since Sleuth Kit is an open source tool, support for any file system can be added. File system support may be added by users of the toolkit as required. The Sleuth Kit locally supports processing raw disk images but it can also import the ability to process additional image formats from the LibEWF (Expert Witness Format) and AFFLib (Advanced Forensic Format) packages.

Commercial tools such as Carnivore, NetIntercept, NFR Security, NetWitness and SilentRunner have been developed with integrated search, visualisation and analysis features to help digital investigators collect information from network traffic. There has been progression in the development of tools for collecting evidence on embedded computer systems. It is frequently used by digital investigator's to read information from pagers, mobile phones and personal digital assistants directly from the devices. But this approach does not provide access to deleted dtat and may not be possible if the device is password protected. Tools such as ZERT, TULP and Cards4Labs have been developed to access password protected and deleted data.

- **SafeBack**

SafeBack is used for bitstream backup. A bitstream backup is different from the regular copy operation. During the regular coping activities, files are simply

copied from one medium such as a hard drive to another e.g. a tape drive. When performing a bitstream backup of a hard drive, bit by bit copy of the hard drive is obtained and not just the files. Every bit that is on the hard drive is transferred to the backup medium.

- **GetTime**

GetTime is used to document the time and date settings of a victim computer system by reading the system date and time from Complementary Metal Oxide Semiconductor (CMOS). Digital forensic examiner should compare the data/time from CMOS to the current time before processing the computer of evidence.

- **GetSlack**

GetSlack is used to capture the data contained in the file slack of the hard drive. In the process of filling up clusters on the hard drive with files, the segment of a cluster that the file does not completely fill up is called slack space. Slack space is used by the operating system for different thing, but the ordinary computer user cannot view it. Special tools are required to view slack space. It is important to know that valuable information pertaining to an investigation can be found in the slack space.

4. Mobile Forensic Tools

- **Oxygen Forensic Suite**

Oxgen Forensic Suite is a mobile forensic software for analysis of cell phones, smartphones and tablets. Oxygen Forensic Software supports Symbian OS, Nokia S60, Sony Ericsson UIQ, Windows Mobile 5/6, Blackberry, Android and Apple Smartphones etc. Oxygent Software invented an advanced agent approach that allows Oxygen forensic suite to extract much more information from Smartphones than other logical tools.

- **Micro Systemation XRY Software**

XRY Software is a digital forensic tool designed by Micor Systemation used to analyze and recover information from mobile devices such as mobile phones, Smartphones, Gps navigation tools an tablet computers. XRY software is developed to recover the contents of a device in a forensic manner acceptable by many users. The XRY is a complete digital forensic system for mobile devices that can be used on any Windows Operating System.

5. The need for tools and techniques

Previously during digital crime investigation digital forensic investigators widely used the evidentiary computer itself to collect evidence. The main risk of this method was that operating the evidentiary computer could alter the evidence in a way that is untraceable. However UNIX programs like Deleted Data came into existence in the 1980s and was able to capture deleted data stored on a hard drive, but these tools was not widely used and then most digital evidence examinations were performed at the file system level neglecting deleted data. In 1990s tools like SafeBack was created to allow digital investigators collect all data on a computer disk without altering important data. As more people became aware of the value of computers, the need for more advanced tools increased. In order to address this need, integrated tools such as Encase and FTK were created to make the digital investigator's work easier. These tools allow the more efficient examination, by automating routine tasks and display data in a graphical user interface to help the user locate important information (Ademu et al, 2012). Recently Linux has been used as a digital evidence examination platform and tools like The Sleuth kit and SMART have been developed providing a user friendly interface. More advanced tools are available to recover overwritten data from hard drives, but these are expensive for most purposes. Regrettably, many people are still unaware of the need for these tools.

Conclusion

Digital evidence must be precise, authenticated and accurate in order to be accepted in the court. Digital evidence is fragile in nature and they must be handled properly and carefully. Detailed digital forensic investigative processes and good knowlede of digital forensic tools provide important assistance to forensic investigators in establishing digital evidence admissible in the court of law. Digital forensic tools and techniques are developed to achieve the goals of digital evidence searching, retrieval and recovery. The digital forensic investigator analyse a case and select techniques to be used in the process of investigation. Carrying out a digital forensic investigation using a method manually could consume a huge amount of time for example searching all the cluster in a hard disk could take unto few years of work. There is some specific task that could not be performed without the use of specific software tools. There are a large variety of software and hardware that have been developed to help digital forensic investigators in performing a digital forensic investigation.

Acknowledgement

The authors would like to thank Dr David Preston, and the University of Cambridge Computer laboratory for providing support during this research.

References

[1] Ademu, I. Imafidon, C. Preston, D., (2012) Intelligent Software Agent applied to Digital Forensic and its Usefulness Vol. 2 (1) Available at: http://interscience.in/IJCSI_Vol2Iss1/IJCSI_Paper_21.pdf (Accessed 10 April 2012)

[2] Ademu, I. Imafidon, C. I. Preston, D. (2011) A New Approach of Digital Forensic Model for Digital Forensic Investigation Vol. 2, (12) Available at: http://thesai.org/Downloads/Volume2No12/Paper%206-A%20New%20Approach%20of%20Digital%20Forensic%20Model%20for%20Digital%20Forensic%20Investigation.pdf (Accessed 28 April 2012)

[3] Aggarwal, S. Duan, Z. Kermes, L. Medeiros, B (2008) E-Crime Investigative Technologies Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04439186 (Accesseed 5 April 2012)

[4] Altheide, C. Carvey, H (2011) Digital forensics with open source tools Pp 26 – 27 Waltham: Elsevier

[5] Casey, E (2004) Digital evidence and computer crime forensic science, computers and the internet 2nd Edition P 101 London: Academic Press

[6] Casey, E. (2002) Handbook of computer crime and investigation P116 London: Academic Press

[7] Farrell, P. (2009) A framework for Automated Digital Forensic Reporting Available at: http://cisr.nps.edu/downloads/theses/09thesis_farrell.pdf (Accessed 20 March 2012)

[8] Jones, K. Bejtlich, R. Rose, C. (2005) Real digital forensics: Computer security and incident response P 172

[9] Kruse II, W. Heiser, J (2001) Computer Forensics Incident Response Essentials P 170 Indianapolis: Addison

[10] Nelson, B. Phillips, A. Enfinger, F. Steuart. C (2004) Guide to computer forensic and investigation P 377 Canada: Course Technology

[11] Palmer, G. (2001) a road map to digital forensic research Available at: http://www.dfrws.org/2001/dfrws-rm-final.pdf (Accessed 25 October 2011)