Computer Forensic: A Reactive Strategy for Fighting Computer Crime

Abdullahi Mohammed *Abdulmohammedabdul@yahoo.com*
Faculty of Physical Science
Department of Computer Science
University of Port Harcourt
Port Harcourt, 500001, Nigeria

Enoch O. Nwachukwu *Enoch.nwachukwu@uniport.edu.ng*
Faculty of Physical Science
Department of Computer Science
University of Port Harcourt
Port Harcourt, 500001, Nigeria

Abstract

Computer Forensics is the science of obtaining, preserving, documenting and presenting digital evidence, stored in the form of encoded information, from digital electronic storage devices, such as computers, Personal Digital Assistance (PDA), digital cameras, mobile phones and various memory storage devices. All must be done in a manner designed to preserve the probative value of the evidence and to assure its admissibility in legal proceeding. The word forensics means "to bring to the court". Forensics deals primarily with the recovery and analysis of latent evidence. Latent evidence can take many forms, from fingerprints left on a window to deoxyribonucleic acid (DNA) evidence recovered from blood stains to the files on a hard drive. This paper provides a high-level overview on computer forensics investigation phases for both technical and non-technical audience. Although the term "computer" is used, the concept applies to any device capable of storing digital information.

Keywords: Computer Forensic, Digital Evidence, Digital Forensic, Time Stamp, Computer Crime.

1. INTRODUCTION

In a perfect world the need for determining the activity conducted within a computer would not be necessary; however, this is not a perfect world and there are times when it is imperative that the activity of a computer be investigated. There should be a way for an individual to analyze a computer, in times when possible misconduct has occurred. For this reason, computer forensics, a newly developed area of computer science, becomes an increasingly more important aspect daily and will be widely used in the twenty-first century.

The widespread use of computers has caused computer crimes to increase at an alarming rate. Computers have given criminals a new approach to carrying out their misdeeds. After a crime or a questionable act is suspected on a computer, a digital investigation must follow. The investigation is used to determine the scope of the problem. The computers investigated will typically be either those used to commit the crime or those which are the targets of the crime.

Computer security is a vast field that touches all aspects of data confidentiality, integrity and availability for suitably controlling access to data. Access control is only one of the ten domains of Information Systems Security categorized by the International Information Systems Security Certification Consortium (ISC) [2] which is responsible for certifying Information Systems Security professionals globally.

Out of the two aspects of security, the proactive comprises of detective, preventive and deterrent measures while the reactive deals with corrective, investigative, recovery and compensatory measures taken to guarantee a certain degree of data assurance. Most of what is studied today in computer security only emphasizes the proactive components. Owing to many factors, investigating root cause analysis and studying computer usages or file structures to determine exploitable trends have never been the norm in most environments.

This paper introduces the reactive part of computer security otherwise called computer forensics. It attempts to serve as an introduction into the vast field of computer forensics. While defining forensic science holistically and introducing such terms as Computer Forensic Investigation process, digital evidence, chain of custody, event reconstruction and digital forensic process.

2. COMPUTER FORENSIC DEFINED

The term forensics derives from the Latin 'forensis', which meant in open court or public, "which itself comes from the term forum, referring to an actual location, public square or marketplace used for judicial and other business."

Contemporary use of the word forensics, therefore, generally continues to relate to law, and has come to mean \scientific tests or techniques used with the detection of crime." Thus, computer forensics implies a connection between computers, the scientific method, and crime detection. Digital forensics is largely used interchangeably with computer forensics, but implies the inclusion of devices other than general-purpose computer systems, such as network devices, cell phones, and other devices with embedded systems [1]. However, largely everyone except academic computer science researchers use the term in connection with the law. Many computer scientists have simply been using the word "forensics" as a process of logging, collecting, and auditing or analyzing data in a post hoc investigation." 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 [1] [2]. The term digital forensics was originally used as a synonym for computer forensics but has expanded to cover investigation of all devices capable of storing digital data. With roots in the personal computing revolution of the late 1970s and early '80s, the discipline evolved in a haphazard manner during the 1990s, and it was not until the early 21st century that national policies emerged [1].

Digital forensics investigations have a variety of applications. The most common is to support or refute a hypothesis before criminal or civil courts. Forensics may also feature in the private sector; such as during internal corporate investigations or intrusion investigation.

The technical aspect of an investigation is divided into several sub-branches, relating to the type of digital devices involved; computer forensics, network forensics, database forensics and mobile device forensics. The typical forensic process encompasses the seizure, forensic imaging (acquisition) and analysis of digital media and the production of a report into collected evidence.
Carrier [2] points out that as well as identifying direct evidence of a crime, digital forensics can be used to attribute evidence to specific suspects, confirm alibis or statements, determine intent, identify sources, or authenticate documents.

Beckett [3] asserts that the term computer forensics was in informal use in academic publications from at least 1992; however the term remained informally defined for many years. A commonly cited definition of the field in Australian literature is McKemmish's [4] definition of forensic computing:

"The process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable" [4]

The American Academy of Forensic Sciences defines forensics as follows:

"The word forensic comes from the Latin word forensic: public; to the forum or public discussion; argumentative, rhetorical, belonging to debate or discussion. From there it is a small step to the modern definition of forensic as belonging to, used in or suitable to courts of judicature, or to public discussion or debate. Forensic science is a science used in public, in a court or in the justice system. Any science, used for the purpose of the law, is a forensic science." [5]

This broad definition of forensics and McKemmish's earlier definition inform the definition of computer forensics given by the Scientific Working Group on Digital Evidence (SWGDE), whose definition is [6]:

"The scientific, examination, analysis, and/or evaluation of digital evidence in legal matters."

Researchers attending the first Digital Forensic Research Workshop, 2001 defined Digital Forensic Science as [7]:

"The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations"

This broad definition reflects a change in forums in which the techniques of computer forensics are increasingly being applied. While traditionally, computer forensics was exclusively targeted in legal forum, computer forensics is increasingly practiced in non-legal context such as corporate investigations, intelligence and military.

The terms digital forensics, forensic computing and computer forensics are today arguably used interchangeably. Historically, computer forensics and forensic computing related to the interpretation of computer related evidence in courts of law. Technology however does not stand still, nor does language, and the meaning of the term has remained consistently under negotiation. Two factors have been at play underlying this process: the changing state of uptake of digital technologies, and with it moves within organizations to consider governing and regulating the use of information technology [8].

However, many experts feel that a precise definition is not yet possible because digital evidence is recovered from devices that are not traditionally considered to be computers. Some researchers prefer to expand the definition such as definition by Palmer [7] to include the collection and examination of all forms of digital data, including that found in cell phones, PDAs, iPods, and other electronic devices.

It is not just the content of emails, documents and other files which may be of interest to investigators but also the 'metadata' associated with those files [9]. A computer forensic examination may reveal when a document first appeared on a computer, when it was last edited, when it was last saved or printed and which user carried out these actions.

More recently, commercial organizations have used computer forensics to their benefit in a variety of cases such as:

- ≈ Intellectual Property theft
- ≈ Industrial espionage
- ≈ Child exploitation/abuse
- ≈ Employment disputes
- ≈ Economic Fraud investigations
- ≈ Forgeries

- ≈ Matrimonial issues
- ≈ Bankruptcy investigations
- ≈ Inappropriate email and internet use in the work place
- ≈ Regulatory compliance

3. COMPUTER FORENSIC PROCESS

From a technical standpoint, the main goal of computer forensics is to identify, collect, preserve, and analyse data in a way that preserves the integrity of the evidence collected so it can be used effectively in a legal case. Forensic process comprises the following phases [13]:

• Collection
• Examination
• Analysis
• Reporting

3.1 Data Collection Phase

The first step in the forensic process is to identify potential sources of data and acquire data from them. Common data sources include desktop computers, servers, network storage devices, and laptops with internal drives that accept media, such as CDs and DVDs, and also have several types of ports (e.g., Universal Serial Bus (USB), Personal Computer Memory Card International Association (PCMCIA) to which external data storage media and devices can be attached. External storage examples include [14]:

- o Thumb drives
- o Memory and flash cards
- o Optical discs
- o Magnetic disks.

Standard computer systems also contain volatile data that is available until the system is shut down or rebooted.

In addition to computer-related devices, many types of portable digital devices (e.g., PDAs, cell phones, digital cameras, digital recorders, and audio players) may also contain data.

Analysts should be able to survey a physical area, such as an office, and recognize the possible sources of data.

Once exhibits have been seized a forensic duplicate of the media is created, usually via a write blocking device, a process referred to as Imaging or Acquisition [10]. The duplicate is created using a hard-drive duplicator or software imaging tools such as DCFLdd, IXimager, Guymager, TrueBack, EnCase, FTK Imager or FDAS. The original drive is then returned to secure storage to prevent tampering.

The acquired image is verified by using the SHA-1 or MD5 hash functions. At critical points throughout the analysis, the media is verified again, known as "hashing", to ensure that the evidence is still in its original state [16].

Before the analyst begins to collect any data, a decision should be made by the analyst or management on the need to collect and preserve evidence in a way that supports its use in future legal or internal disciplinary proceedings. Furthermore, a clearly defined chain of custody should be followed by keeping a log of every person who had physical custody of the evidence, documenting the actions that they performed on the evidence and at what time, storing the evidence in a secure location when it is not being used, making a copy of the evidence and performing examination and analysis using only the copied evidence, and verifying the integrity of the original and copied evidence [17].

Some proactive measures taken by organizations to collect data for forensic purposes include:

- Configuration of most operating systems (OSs) to audit and record certain event types, such as authentication attempts and security policy changes, as part of normal operations.
- Implementation of centralized logging. Certain systems and applications forward copies of their logs to secure central log servers.
- Performing regular system backups allows analysts to view the contents of the system as they were at a particular time.

In addition, security monitoring controls such as intrusion detection software, antivirus software, and spyware detection and removal utilities can generate logs that show when and how an attack or intrusion took place.

3.2 Examination

The examination process helps make the evidence visible and explain its origin and significance. This process should accomplish several things. First, it should document the content and state of the evidence in its totality. Such documentation allows all parties to discover what is contained in the evidence [16]. Included in this process is the search for information that may be hidden or obscured. Once all the information is visible, the process of data reduction can begin, there by separating the "what" from the "chaff". Giving the tremendous amount of information that can be stored on computer storage media, this part of the examination is critical.

3.3 Analysis

After acquisition the contents of image files are analysed to identify evidence that either supports or contradicts a hypothesis or for signs of tampering (to hide data) [11].

During the analysis an investigator usually recovers evidence material using a number of different methodologies (and tools), often beginning with recovery of deleted material. Examiners use specialist tools (EnCase, ILOOKIX, FTK, etc.) to aid with viewing and recovering data. The type of data recovered varies depending on the investigation; but examples include email, chat logs, images, internet history or documents. The data can be recovered from accessible disk space, deleted (unallocated) space or from within operating system cache files [9].

Once evidence is recovered the information is analysed to reconstruct events or actions and to reach conclusions, work that can often be performed by less specialist staff. Digital investigators, particularly in criminal investigations, have to ensure that conclusions are based upon data and their own expert knowledge **[9]**. In the US, for example, Federal Rules of Evidence state that a qualified expert may testify "in the form of an opinion or otherwise" so long as [12]:

(1) The testimony is based upon sufficient facts or data.

(2) The testimony is the product of reliable principles and methods.

(3) The witness has applied the principles and methods reliably to the facts of the case.

3.4 Reporting

Once the computer forensic analysis is complete, presenting an understandable, defendable and complete report is key. The evidentiary packages produced must be complete, easy to understand and always explained in precise detail. The addition of relationship charts, entity explanations, timelines, histories and mail-thread analysis gives a clear understanding of the issue, as well as the players [15]. The analyst shall be able to defend the process and testify to

the methodologies used relating to the facts in a case, when questions start getting tough during expert witness testimony.

When completed reports are usually passed to those commissioning the investigation, such as law enforcement (for criminal cases) or the employing company (in civil cases), who will then decide whether to use the evidence in court. Generally, for a criminal court, the report package will consist of a written expert conclusion of the evidence as well as the evidence itself [9].

4. CONCLUSION

Given the enormity of task in cybercrime control and policing, the absence of dearth of trained and qualified computer forensics law enforcement officers, there is urgent need for the Federal Government to pay attention to the training of adequate EFCC and police officers in the computer forensic sciences to enhance effective policing of the ever increasing cyber criminals. The problem is serious, particularly now that the Federal Government has passed the information Technology Bill and Electronic Evidence Act for this purpose. A law made but cannot be enforced is no law. Cyber criminals will be forced to retreat if a large percentage of fraudsters are arrested, prosecuted and punished at first attempt. It is strongly recommended that Polytechnics and Universities should establish Computer Forensics certificate, diploma and degree courses to meet the ever-increasing demand for this type of urgently needed personnel. The provision of adequately qualified experts will beef up their deployment in the police and military. This may well be antidote to the fast eroding confidence in e-commerce and international trade in Nigeria.

In this paper, we have reviewed the literatures in computer forensics and identified the four (4) main phases of computer forensics investigation process: *Collection*, *Analysis*, *Examination* and *Reporting*.

Our future research will focus on Computer forensic Investigation Process Models, where we shall apply a risk based approach in computer forensic investigation. The legal aspect on computer forensics is an interesting area that should be further investigated [14]. Probable research area might be a way to categorize and approve computer forensic tools for certain investigations and situations? How cross-country investigations are handled, and how are differences between the countries rules and regulations managed?

5. REFERENCES

[1] M Reith, C Carr and G Gunsch, (2002).“Anexamination of Digital Forensic models”. International Journal of Digital Evidence [online]. Available at: www.acm.org [Accessed on 15/10/2012].

[2] B. Carrier, (2001b). “Defining Digital Forensic examination and Analysis Tools” Digital Research Workshop II. Available at: www.acm.org [Accessed on 15/10/2012].

[3] J. Beckett, J., “Digital Forensics: Validation and Verification in a Dynamic Work Environment”. 40th Annual Hawaii International Conference on System Science. 2007: Hawaii.

[4] R. McKemmish, 1999, “What is Forensic Computing?” Trends and Issues in Crime and Criminal Justice, Australian Institute of Criminology. Available at: http://aic.gov.au/documents/9/C/A/%7B9CA41AE8-EADB-4BBF-9894-64E0DF87BDF7%7Dti118.pdf [Accessed on 20/10/2012]

[5] AAFS. “So you want to be a forensic scientist?” American Academy of Forensic Science, Available at: http://www.aafs.org/default.asp?section_id=resources&page_id=choosing_a_career

[6] N.L Beebe and J.G Clark. “A Hierarchical, Objectives-Based Framework for Digital Investigations Process”, 4th Digital Forensics Research Workshop. 2004: Baltimore, MD.

[7] G. Palmer, G. “A road Map for Digital Forensic Research, in First Digital Forensic Research Workshop”, G. Palmer, Editor. 2001: Ucita, New York. www.acm.org.

[8] B. Schatz. “Digital Evidence: Representation and Assurance”. Doctorate Thesis, Submitted to Information Security Institute, Faculty of Information Technology, Queensland University of Technology, 2010.

[9] C. Eoghan (2004). "Digital Evidence and Computer Crime, Second Edition". Elsevier. ISBN 0-12-163104-4.

[10] A. Richard, H. Val and M. Graham (2012). "'The Advanced Data Acquisition Model (ADAM): A process model for digital forensic practice" Journal of Digital Forensics, Security and Law, Vol. 8(4).

[11] B. Carrier (2001) "Defining digital forensic examination and analysis tools". Digital Research Workshop II. CiteSeerX: 10.1.1.14.8953.

[12] Federal Rule of Evidence. Available at; http://federalevidence.com/rules-of-evidence#Rule702 Retrieved on 2nd May, 2014.

[13] A. J. Marcella, Jr. and D. Menendez. "Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes," (2nd Edition): Taylor & Francis Group, LLC. 2008.

[14] E.O. Nwachukwu, A Mohammed. D.C. Igweze and V.O. Ewulonu "Microsoft Windows Based Computer Forensic" International Journal of Information Technology and Business Management; 2927(1):2012-2014.

[15] National Institute of Justice. "Electronic Crime Scene Investigation: A Guide for First Responder". Washington, D.C.: U.S. Department of Justice, National Institute of Justice, 2004. NCJ 187736. http://www.ojp.usdoj.gov/nij.

[16] S. Garfinkel, "Forensic Feature Extraction and Cross-Drive Analysis". The 6th Annual Digital Forensic Research Workshop Lafayette, Indiana, August 14-16, 2006.

[17] J. E. Regan. "The Forensic Potential of Flash Memory". Master's Thesis. Naval Postgraduate School, Monterey, CA, 2009.

[18] F. Adelstein. "MFP: The Mobile Forensic Platform". International Journal Of Digital Evidence, Spring 2003, Volume 2. Issue 1.