International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3407-3412 www.ijaem.net ISSN: 2395-5252

Digital Forensic Evidence Tools Applicability in Digital Crime Investigation

Adamu Abdullahi Garba*[1], Ibrahim Bukar Dauda[2,] Aliyu Musa Bade[3]
[1,2,3]*Department of Computer Science, Yobe State University Damaturu, Nigeria*

Submitted: 15-07-2021 Revised: 29-07-2021 Accepted: 31-07-2021

ABSTRACT
The internet has made many commercial activities in organizations to be operated automatically, this has open potentially dangerousunexpected information security incidents with the potential to cause harm to the organization business. Therefore, if an organization does not prepare itself for such incidents, it's likely that important digital evidence will be damage. Therefore an organization needs to know the forensic tools to be applied when any cyber bridge occurs. This paper provides an insight of Digital Forensic Evidence Tools Applicability in Digital Crime Investigation fororganizationreadiness to exploit its prospective to use digital evidence whilst minimizing the cost of an investigation.
Keywords: Digital forensic, Digital evidence, Digital forensic tools

I. INTRODUCTION

There are many definitions given to digital forensic from various researchers and books, According to the Oxford dictionary, forensic can be defined as linking to the usage of systematic approaches to the investigation of crime and of or relating to courts of law. The practice of science and expertise to examine and institute facts in an illegal or civil court of law can be referring to as forensic (Farlex, 2014).Digital forensics (DF) is the systematic proposition of the procedures involved in the recapture, safeguarding and investigation of digital evidence, including audio, imaging and communication devices (TC-11, 2006). DF is the division of computer science that emphasizes evolving evidence related to the digital world for use in civil or criminal court proceedings (Reith, 2002).

DF evidence can also be found in digital documents, emails, digital photographs, software programs, or other digital archives and network metadata, which may be a question in a legal circumstance to win a case (Marangos, 2012).Digital forensic is the accomplishment of a suitable level of competence by an organization for it to accumulate, preserve, shield, and analyze any digital evidence so that the evidence can be excellently used in any courts of law, in corrective matters (CESG, 2009).In another context, some authors have recognized three modules in digital forensic: Proactive, Active, and Reactive DF. These modules are linked to one another. Proactive means before an incident alert, actively refer to real-time happening and reactive refers to afterward an incident (Grobleret al., 2012). Proactive DF is for the preparation of organizations for investigations; Active DF refers to consideration, the procurement, and exploration of live evidence; and Reactive DF is the real 'post-action forensic investigation. Nowadays many organizations only invest in reactive DF rather than all the components. Even with the advancement of alertness and educational research on proactive forensic, its description and enactment are still not reliable in the digital forensic domain (Frinckeet al., 2006).

HISTORY OF DIGITAL FORENSIC

The field of digital forensic has undergone many series of transitional states because it always faces practical and problems of evidence related to investigations lead by law enforcement agenesis. According to David et al., (2014) computer forensic was dated back to 1970, when students in the US discover how to bypass authentication to get access to shared computers. From there in 1978 the Florida Computer Crime Act was the first law to be enacted to deal with computer fraud and intrusion.

The first program to be design related to computer forensic was dated back in 1984; When the FBI magnetic media was created which is the name later as CART computer Analysis and Respond Team. In the mid's 90 due to the use of technology by many organizations crimes started to evolve. Law enforcement personal is also trained in the field of cybercrime and Internet investigation to overcome those challenges. Many researchers

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3407-3412 www.ijaem.net ISSN: 2395-5252

believed that computer forensic advancement is surrounded by threestages of evolution, which are: Ad hoc, structured and enterprise phase.

- **Ad hoc**: This phase can be described as when there is a lack of structured, clear goals and adequate tools, processes, and procedures to be used in conducting an investigation, some literature calls it the pre-forensic period. In this phase, no acceptable use policy and procedures are implemented.
- **Structure phase**: This phase can be characterized by the development of a more complex solution for computer forensic, this includes recognize and acceptable procedures, tested tools that were developed to tackle computer-related problems.
- **Enterprise phase**: This phase can be referred to as the current state of the computer forensic and is the advance of all the phases. In this current time, Computer Forensic (CF) is widely considered as actual science, which involvesa real-time collection of evidence, using effective tools and processes. CF is widely accepted by the international community. CF also allows proactive collection and detection and can be accomplished in a way that is consistent with the process approved by the law (NIST, 2006).

According to Dlamini and Grobler (2010) stated that there is no single internationally acceptable statement of standard or best practice in this field. This section shows laws and crimes vary with countries, the main challenge in this field is to have standard policies and procedures to be followed in investigating a crime as each country has its law that will suit their people.

A conference gathering organizes by the FBI in 1993 was appeared by 70 legislatures of countless US federal, state, and local law hearings organizations. These agencies approved that principles for forensic discipline were requiring and obligatory to tackle computer crimes (Morgan, 2001). A common example is the smoking of marijuana in some countries is considers being a crime like Nigeria, China, and Malaysia while Uruguay, Peru, and Ecuador for personal use are legal, with these diverse rules and opinions it will be quite difficult to have a standard law to tackle crime conducted with computers either traditional crimes or modern once.

DIGITAL EVIDENCE

According to Chawki (2004) stated that evidence is roughly inclined to establish or refute a fact. Digital evidence can be documents, testimony, audio, video, and other objects. There isa various category of evidence; the scientific working group on digital forensic standard categorizes evidence into three main sections: digital evidence, physical evidence, and data (SWGDE and IOCE, 2000).

- **Digital Evidence Category:** Digital evidence includes: email, backups, recovered data using a forensic method, logging data which can easily be transferred via various mediums like in electronic or magnetic form. The data can be original digital evidence (obtained from the scene or seize) like on CD. The data can also be identical digital E.g. backup duplicate or an image of a hard disk the data can be a copy, as an MS Word file. (SWGDE and IOCE, 2000).
- **Physical Digital Category:** Physical digital evidence includes: flash drives, where the information is stored and transmitted when necessary via physical media.
- **Data Object Category:** Data objects include: metadata, directory data, where information is connected to the digital evidence.
- From the legal point of view, numerous types of evidence exist, According to Chawki, (2004), again identified three categories:
- **Real or physical evidence:** which consists of a tangible object like HDD, flash drives, floppy diskette videodisc, etc.
- **Testimonial evidence**: witness given by a person in a hearing based on surveillance.
- **Circumstantial evidence**: evidence that is based on comments of truths that tend to back up a conclusion but not to verify it.
- Other kinds of evidence do exist as well like:
- **Technical evidence or opinion evidence**: This form of evidence comes from a forensic expert that has carried out some steps on the unusual evidence and has come up with a result (Sommer, 2005).
- **Expert evidence**: This evidence is based on the opinion of an expert in the field of computer forensic or the conclusion of an expert after investigation (Sommer, 2005)
- **Drive evidenc**e: This evidence is from a chart, or video, generated from the original evidence to show how conclusions were drawn.
- **Evidence of tempering**: the evidence that is not related to theory, but indicates that the system has been tempered.

CHARACTERISTIC OF GOOD DIGITAL EVIDENCE

Many factors can be used to define the value, applicability, acceptability, and reliability of evidence. Digital evidence can be easily destroyed, compromised, or modified when handled incorrectly. Failure to present relevant and

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3407-3412 www.ijaem.net ISSN: 2395-5252

admissible evidence often can lead to many losses (financial) and filed investigation (Sommer, 2005). Still, there are no international specifications for digital evidence to be acceptable in a Supreme Court of law. Several countries have different requirements. The Electronic Communication and Transaction Act of South Africa (2002) describe the following requirement aimed at defining the acceptability of digital information in a Supreme Court of law:

- Trustworthiness of nature in which the evidence was transferred and deposited
- How well the reliability of the documents was kept.
- The nature in which the initiator of the record is recognized.

The growing numbers of commercial organizations, law enforcement agencies, and recovery teams have given rise to the need for DF tools and technology. Digital forensic tools and technology are generally used to gather as much evidence. Recently, digital evidence is becoming a business enabler. DF investigators usually gather an investigation outline to conduct an investigation or to acquire relevant evidence by using published best practices. The success of an investigation can be determined by the use of accurate and acceptable DF tools and methods in the court of law, some investigations are flexible that allows multiple usages of DF tools to ensure accuracy of the result of the tools. In the next section of this project, the author has explained more about the DF tools and their applications in the investigation process.

TYPE OF CRIME THAT MIGHT INVOLVE DIGITAL FORENSIC EVIDENCE

Many crimes are being conducted with computer devices either traditional or modern crimes that might lead to digital forensic investigation to gather information and facts, these crimes include:

- Connected auction fraud
- Child exploitation
- Computer interference
- Homicide
- Domestic ferocity
- Economic fraud, Counterfeiting
- Threat, provocation

COMPUTER FORENSIC TOOLS

Evidence in digital forensic is the most valuable information, and the need to extract that information correctly without tempering is very critical. Digital forensic processes have been established to achieve the goal of data location, data seizure, and data recovery (Jahankhaniet al., 2010. Therefore, there is a need to understand the forensic tools that will be used in a case as there is no comprehensive tool that can do all the needed investigation.

Types of Computer Forensic Tools

Computer forensic tools are categorized into two main categories: hardware and software.

- **Hardware forensic tools:** Hardware forensic tools range from simple, single-purpose modules to complete computer systems. The single-purpose components can be a device like FireWire Drivedock and lockdown.
- **Software forensic tools:** In software forensic tools they are grouped into command-line applications and GUI applications. Some tools are specialized to only perform one task like SafeBack. The tools are normally used to copy data from a suspect's disk drive to an image file.

According to Nelson et al., (2008) stated that all computer forensic tools be it hardware or software, perform specific functions. These functions are grouped into five major categories:

- Acquisition
- Validation and discrimination
- Extraction
- Reconstruction
- Reporting

- **Acquisition**: In computer forensic, the first task is an investigation that is creating a copy of the original drive. This method preserves the original drive to make sure it does not become corrupt and damage. Acquisition functions include physical data copy, logical data copy, data acquisition format, command-line acquisition, GUI acquisition remote acquisition, and verification. Both hardware and software tools can be used in this phase. Software tools like EnCase provide tools for acquiring image data and hardware devices like Talon from Logicube can be used to acquire an image of data, this hardware has their in-built software for data acquisition from a suspect drive.
- **Validation and Discrimination**: Computer evidence deals with two major issues, which are very critical. The first is confirming the reliability of data being copied. Second is the discrimination of data, which involves cataloging and searching through all the investigation data. The sub-function of the validation and discrimination includes hashing, filtering, and analyzing file headers.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3407-3412 www.ijaem.net ISSN: 2395-5252

- **Extraction**: The process of extracting evidence in a computer system. Recovering data is the first step in examining an investigation's data. The following sub-functions are used for extraction in the investigation: data viewing, keyword searching, decompressing, caving, decrypting, and bookmarking. Software tools such as ProDiscover, FTK, SMART, and ILook, and others offer several ways to view data including logical drive structure, such as folders and files.
- **Reconstruction:** The main idea of having a restoration feature in a forensic tool is to redesign a suspect drive to show what happens throughout a crime or an incident. These are the sub-function of reconstruction: Disk-to-disk copy, Image-to-disk copy, Partition-to-partition copy, and Image-to-partition copy. The simplest way to duplicate a drive is using a tool that makes a direct disk-to-disk copy from the original suspect drive to the target drive. Many tools are available to perform this task like UNIX/Linux dd command. Table 2.1 shows the lists of software tools that can be used in the reconstruction of data using its sub-functions.

Table 1 Reconstructive Function and Software Tools

No	Reconstruction function	Software tools
1	Disk-to-disk copy	Logicube, Forensic Talon, Forensic MD5
2	Image-to-disk and image-to-partition copies	SafeBack, SnapBack, EnCase, FTK Imager and ProDiscover

- **Reporting:** A comprehensive forensic disk exploration and examination needs to be documented. Previously, the investigator must do this process manually, but the newer windows-based forensic tools can create an automated report in a multiplicity of formats such as word processing, HTML, PDF, etc. Reporting sub-function includes Log report, and Report generator. Some software is used to produce reports generators that display bookmarked evidence such software are: ProDiscover and EnCase.

FORENSIC HARDWARE TOOLS REFERENCE

Table 2 shows forensic hardware tools reference available on the market, this Table shows tool name, description, the operating system it supports, and device applicable to it.

Table 2 Forensic Hardware Tools

Name	Description	Operating system	Device
Ferd (www.digitalintelligence.com/products/fred/, 2015)	The forensic recovery of evidence device (FRED) is a forensic workstation from digital intelligence has an interface for all occasion. Is a collection of software package like EnCase, FTK, etc.	Server 2008 R2 / Windows7 64-bits	Hard drives (IDE/EIDE/ ATA/SATA/ATAPI/SCSI I/SCSI II/SCSI II), DVD, CD, Memory stick, Cards secure digital media, etc.
Logicube (http://www.logicube.com/, 2015)	Logicube provides the fastest disk-to-disk and disk-to-image transfer.	Windows XP Or Later Windows Server 2003 Or Later Mac OS X	Compact Flash SD Card Memory Stick USB Thumb Drives USB Drives via USB Cable

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 3407-3412 www.ijaem.net ISSN: 2395-5252

FORENSIC SOFTWARE TOOLS REFERENCE

Table 3 Shows forensic software tools reference available on the market, this Table shows tool name, description, and operating system applicable to it.

Table 3 Forensic Software Tools

Name	Description	Operating system
DBXanalyzer(http://www.di-mgt.com.au/dbxanalyzer/, 2015)	Reads analyzes and manages e-mail data files created by Microsoft outlook express version 5 and 6	Windows
Digital image recovery(http://www.z-a-recovery.com/tutorials/digital-image-recovery.aspx, 2015)	This software recuperates lost data from the multimedia device, including digital audio recorders, MP3, etc.	Windows 98/Me/NT/2000 /XP/2003/Vista/Server 2008/7
Fatback(http://xsanlahci.org/2013/03/24/fatback-forensics-tool/, 2015)	This software is used to undeletes files from the FAT file system	Linux/BSD/UNIX-like OS

II. CONCLUSION

In conclusion, Form above Table 2.2 and Table 2.3, we can see that there are many varieties of computer forensic hardware and software that can be used in an investigation. The problem now is finding the right tools by the investigator. The efficiency and effectiveness of any hardware device used during an investigation depend highly on the investigator's skill and talent.

REFERENCE

[1]. Farlex, (2014), digital forensic, retrieved on 15/10/2014, available at" http://www.thefreedictionary.com/

[2]. TC-11 I, (2006), Digital Forensics - Fact sheet.[online], retrieve on 10/10/2-14, Available from: http://www.tc11.uni-frankfurt.de/WG/Factsheet_WG_11-9.pdf

[3]. Reith M, Carr C, &Gunsch G, (2002), An examination of digital forensic models. Retrieved on 26/10.2014 available at:https://www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6F2C1-98F94F16AF57232D.pdf

[4]. Marangos N, Panagiotis R, and Lilian M, (2012), Time Synchronization: Pivotal Element in Cloud Forensics, Dep. of Information and Communication Systems Engineering University of the Aegean Karlovassi GR-83200, Samos, Greece

[5]. CESG Good Practice Guide No. 18, (2009) Forensic Readiness, Issue No: 1.0, accessed on 15/0/2014, available at http://www.nationalarchives.gov.uk/documents/information-management/forensic-readiness.pdf

[6]. Grobler C, P, Louwrens C and Solmam S V, (2012), A Framework to guide the implementation of proactive Digital forensic in organization. In workshop for digital forensic Krakow, Poland.

[7]. Frincke D, A, Taylor C B, Endicott-Popovsky, (2007) , Specifying digital forensics: A forensics policy approach. Digital investigation, 2007. 4: p. 101-104.

[8]. David L, Jahankhani H, W, Gianluigi Me, Frank L,(2010), Handbook of Electronic Security and Digital Forensics, World Scientific.

[9]. NIST, (2006), Guide to Integrating Forensic Techniques into Incident NIST Response http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

[10]. Dlamini I, Grobler M, (2010), Managing digital evidence: the governance of digital forensics, Journal of Contemporary Management. retrieved on 10/10/2014, Available: http://www.researchspace.csir.co.za

[11]. Morgan C, and Whitcomb,(2001), An Historical Perspective of Digital Evidence: A Forensic Scientist's, National Center for Forensic Science, International Journal of Digital Evidence Spring, 2002. Volume 1, Issue 1

[12]. Chawki M, (2004). The Digital Evidence in the Information Era Computer Crime Research Center, Accessed 20/10/ 214, Available from: http://www.crime-research.org/articles/chawki1/2

[13]. SWGDE and IOCE, (2000). Digital Evidence: Standards and Principles. Forensic Science Communications, April 2000

Volume 2 (2), Accessed, 21/10/2014, Available from: http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm.

[14]. Sommer P, (2005), Directors and Corporate Advisors' Guide to Digital Investigations and Evidence, Information Assurance Advisory Council, retrieved on 22/10/2014, at: http://www.iaac.org.uk/Portals/0/Evidence%20of%20Cyber-Crime%20v12-rev.pdf

[15]. Jahankhani H, David L, W, Gianluigi Me, And Frank L,(2010), Handbook of Electronic Security and Digital Forensics, World Scientific.

[16]. Fred, (20105) Explanation of Fred. Viewed 18/5/2015, Available at: www.digitalintelligence.com/products/fred/

[17]. Logicube, (2015) Logicube Overview. Viewed 18/5/2015, Available at: http://www.logicube.com/

[18]. DbXanalyzer, (2015) DbXanalyzer Overview. Viewed 18/5/2015, Available at: http://www.di-mgt.com.au/dbxanalyzer/

[19]. Digital image recovery, (2015) Digital image recovery, Viewed 18/5/2015, Available at: http://www.z-a-recovery.com/tutorials/digital-image-recovery.aspx

[20]. Fatback, (2015) Definition of Fatback, Viewed 18/5/2015, Available at: http://xsanlahci.org/2013/03/24/fatback-forensics-tool/