Advances In Multidisciplinary & Scientific Research
A Multidisciplinary & Interdisciplinary Journal

Vol. 1, No. 2, September, 2015

Messaging Cyberforensics Standard for Cybercrime Investigations

Odumesi, J. O.
E-Learning Department
Civil Defence Academy
Abuja, Nigeria
olayemijohn@yahoo.com

ABSTRACT

As the demand for internet usage increase, many people are becoming victims to cybercrime. As such, analysing digital evidence has become a necessity in cybercrime investigations. Nigeria Evidence Act (2011) recognizes electronic, digital and computer generated evidence in a manner that will be admissible in the law courts. However, there are no appropriate standards for the implementation of digital forensic in the Act. Despite the Act for the legal admissibility of digital evidence in law courts, the law enforcement and security agencies are still challenge with the appropriate standards for messaging forensic platform for cybercrime investigations. The purpose of this paper is to provide appropriate technical standard for admissibility of digital evidence in the court of law. To achieve this, existing digital forensic investigation frameworks were reviewed, merging and mapping process was constructed and the result aided in the establishment of a new framework for cyberforensics investigation process.

Keywords: Cyberforensics, Cybercrime, Digital evidence, Forensic models

Aims Research Journal Reference Format:
Odumesi J.O. (2015): Messaging Cyberforensics Standard for Cybercrime Investigations. Advances in Multidisciplinary Research Journal. Vol 1, No. 2 Pp 141-146.

1. INTRODUCTION

Cybercrime investigations are complex and digital evidence for prosecutions are often in an intangible form. The increased use of computer systems and networks in all sphere of life and the growth of the internet has added to this complexity. Basha (2010) argued that, the rapid increase in the use of the internet has led to a string in cybercrime such as online child pornography, cyberterrorism, publishing sexually explicit content in electronic form and video voyeurism. In 2011, Nigeria signed into law the Evidence Act which recognizes electronic, digital and computer generated evidence in a manner that will be admissible in the law courts. However, there is a need to for the development of appropriate standards for the implementation of digital forensic in the Evidence Act (2011). To demonstrate the need for the development of the appropriate standards, draft standards for digital and computer forensics in Nigeria was developed in March, 2014.

Also, the Computer Emergency Readiness Response Team (CERRT.ng) was recently commissioned in Nigeria. This is an anti-cybercrime forensic laboratory technology under the National Information Technology Development Agency (NITDA), which will assist the government, private sector and the general public in responding to computer, network and related cybsecurity attacks or threats. Daura (2014) stated that, "CERRT.ng ecosystem has developed cybersecurity policies, strategies and standards. It will continuously identify existing and potentials computer related threats. According to him, it will notify as appropriate, build capacities, develop the requisite readiness processes, coordinate responses, build relationships and liaise as needed with similar incident response teams locally and worldwide".

2. PROBLEM STATEMENT

Uncontrolled access will create unlimited opportunities for abuse. Dasuki (2014) argued that, every nine seconds, a Nigerian commits crime on the internet with a sharp rise from 0.9% in the 1990s to 9.8% in 2014. He maintained that, cyber threat is real as it poses a national threat and indeed obvious at the national level. Also that, cybercrime in Nigeria has taken advance form and calls for concerns from relevant security quarters to devise means of curbing the menace.

Wando (2014) lamented that, with the growth in the use of computers and internet in Nigeria, cybercrimes have risen significantly as well. He identified that hackers, terrorists and other fraudulent persons most times target establishments and institutions to get attention. He revealed that, the Office of the National Security Adviser (ONSA) has taken significant steps in engaging public-private, incorporation of international law practices, establishment of computer unit in intelligent gathering to building functional system, drafting and electing prominent members to fill up security council seats in the Office of Presidency among others are some of the measures taken to curb crime in Nigeria. Longe (2014) disclosed that, Nigerian banks lost N40bn to cybercrime in 2013. He maintained that, the fight against cybercrimes and other threats to information security could only be won through a robust information security policy framework. Also that, the Central Bank of Nigeria (CBN) had engaged the banks to comply with some basic currently global security standards in the management and security of customer information. He further maintained that, the market value of global cybercrime had reached $288bn as a result of its rising wave and it is about to displace the drug trafficking market valued at $411bn.

Akindele (2011) expressed worry at an attempt to entrench a cashless society in a system that virtually all institutions, including even the banking and government agencies were highly vulnerable to different forms of attack by cybercriminals. He argued that, majority of the institutions do not have any form of protection in place to warn them of such attack or intrusions to their systems. Most organizations in Nigeria are already losing huge sums of money and investment to cybercriminals and the unfortunate thing about it all is that most of them are not even aware of their losses. Despite the passage of Evidence Act 2011 into law in Nigeria for the legal admissibility of digital evidence in law courts, the law enforcement and security agencies are still challenge with the appropriate standards for messaging forensic platform for cybercrime investigations. This is the gap this study hopes to fill.

3. RESEARCH OBJECTIVES

The general objective of this study is to serve as a tool for legal practitioners, security agencies, law enforcement agencies, private sector, educational institutions and the general public in presenting a standard framework for an integrated approach to cybercrime mitigation in Nigeria.

The specific objectives are as follows:

1. To provide practitioners methodology in capturing and preserving digital evidence acquired adequately, and maintains the data volatility.
2. To provide technical support for cybercrime investigation and analysis.
3. To provide framework principles for admissibility of digital evidence in court and increase integrity.

4. METHODOLOGY

The study reviews ten digital forensic investigation frameworks with their respective processes and activities as shown in Table 1 and Table 2. From the existing frameworks or models, it is clear that they build on the experience of the previous. Some of them have similar approaches and frameworks focusing on different areas of investigation. This study proposes a new digital investigation model for cybercrime investigations by mapping and merging of previous frameworks with the same activities or processes that provide the same output into an appropriate phase. The ultimate goal is to provide technical process for analytical findings and methodologies for admissibility of digital evidence in the court of law.

5. CYBERFORENSICS: CONCEPTUALISATION AND DEFINITION

Singh and Rani (2013) argued that, cyberforensics is the unique process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally accepted. It is the process of methodically examining computer media (hard disks, diskettes, tapes, etc.) for evidence. Shridher, et'al (2013) defined cyberforensics as a unique process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally accepted.

Kumar (2013) maintained that, it is a branch of digital forensic science pertaining to legal evidence residing in computers and digital storage media. It deals with acquisition, verification, analysis, preservation and documentation of evidences extracted from a computer system, networks and other peripherals.

A compilation from group suggestions during the Digital Forensics Research Workshop (DFRWS) in 2001 cited in Palmer (2001), defined digital forensic science as 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.

5.1 Classifications of cyberforensics

a. Disk forensic
   This is the act of extracting information from storage media such as, hard disk drive, flash drive, floppy disk drive and other storage media.
b. Network forensic
   This is mainly to monitor and analyse computer network traffic for the purpose of gathering information from the network.
c. Mobile device forensic
   This is for retrieving electronic evidences from a digital device such as mobile phones, tablets, and any device that can store and process information.
d. Cloud forensic
   This applies same forensic process but has the challenges of combining different physical and logical locations.
e. Database forensic
   This is the study of databases and it uses database contents, log files in order to retrieve the relevant information.

6. CYBERCRIME: CONCEPTUALISATION AND DEFINITION

Deshmukh and Chaudhain (2014) maintained that, cybercrimes are technology based crimes and the computer or internet itself can be used as a weapon or means to do such crimes quite freely. Cybercrimes are committed with the help of technology and cybercriminals have deep understanding of technology. Clough (2011) maintained that cybercrime describe a range of circumstances in which technology is involved in the commission of crime. The interconnectivity nature of the internet makes this a global problem. Fafinski, et'al (2010) defined cybercrime as the use of computers to assist traditional offending either within particular systems or across global networks, such as spam mail for example, are solely the product of the internet and could not exist without it. They further maintained that, cybercrime is not a legal term of art; therefore, no legal basis for certain so-called cybercrimes. Muthkumaran (2008) argued that, cybercrime is a term used to broadly describe criminal activity in which computers or networks are a stool, a target or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computer or networks are used to enable the illicit activity.

7. CYBERFORENSICS INVESTIGATIONS

Every cyberforensics investigation is different because of the following reasons:
a. The nature of every computer system and network is different.
b. The level of skill set and experience of the cybercrime investigator.
c. Most forensic tools are based on traditional forensic approaches.
d. The challenges of location and time in the case of cloud forensics.
e. Digital investigations need a generic framework.

Stephenson (2002) cited in Mark (2014) maintained that, for digital evidence to be admissible, cyberforensics investigation must conform to chain of custody requirements and adhere to the following six stages:
1. Preservation of the crime scene
2. Location of the evidence
3. Selection of the critical evidence
4. Analysis of the evidence
5. Validation of the evidence
6. Presentation of the evidence pursuant to evidentiary processes.

Kishore, et al (2014) identified the cardinal rules to be followed while producing digital evidence in the court are:
1. Authenticity
2. Reliability
3. Completeness
4. Conformity with common law and legislative rules
5. Check lists
6. Establish evidence custodian

The draft standards for digital and computer forensics in Nigeria (2014) stated the method for presenting digital evidence as:

1. Acquire the evidence without altering or damaging the original.
2. Authenticate that the recovered evidence is the same as the original seized.
3. Analyze the data without modifying it.

This study adopts the following stages for presenting digital evidence in the court:

1. Preservation
   - Obtaining search authority of the crime scene
   - Proactive analysis
2. Data collection
   - Seizure, imaging or collection of digital evidence
3. Reconnaissance
   - Gathering relevant electronic evidence
4. Examination
   - Examining the authentication of the electronic evidence
5. Analysis
   - Execution of investigative and analytical techniques of the electronic evidence
6. Reporting
   - Documentation of the analytical findings and conclusions for further usage

8. COMPARATIVE ANALYSIS

The existing models were assigned with unique identification based on chronological order. The result is displayed in Table 1 below:

Identity number	Digital Forensic Models	Year	Phases
CF1	Kruse and Heiser Model	2001	3
CF2	DFRWS Investigative Model	2001	6
CF3	Abstract Digital Forensic Model	2002	9
CF4	End to End Digital Investigation	2003	6
CF5	Enhanced Integrated Digital Investigation Process	2004	5
CF6	Computer Forensic Field Triage Process Model	2006	12
CF7	Framework for a Digital Forensic Investigation	2006	3
CF8	Dual Data Analysis Process	2007	4
CF9	Common Process Model for incident and Computer Forensics	2007	3
CF10	Network Forensic Generic Process Model	2010	9

Table 1: Different Models of Digital Forensic Investigation

The phases on the existing models were grouped into the phases in the new model in Table 2 below:

Phases in the new model	Available phases in existing models									
	CF1	CF2	CF3	CF4	CF5	CF6	CF7	CF8	CF9	CF10
Preservation		✓	✓	✓	✓	✓		✓		✓
Data collection	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Reconnaissance										
Examination	✓	✓	✓	✓		✓			✓	✓
Analysis	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Reporting		✓	✓	✓	✓	✓	✓	✓		✓

Table 2: Phases in the new model with existing models

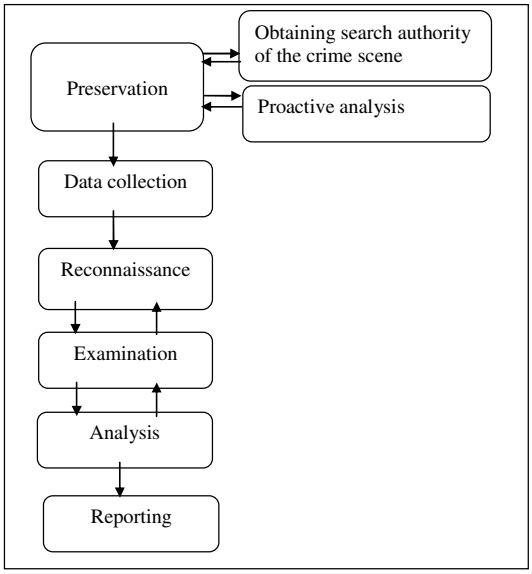

Fig 1: Flow of cyberforensics investigation for the newly proposed model

Preservation: This phase consist of two sub phases. The first relates to legal investigation by obtaining search authority from law or security enforcement agencies as applicable. This is a compulsory process for any form of cybercrime investigation. The second relates to proactive collection, preservation, analysis and preliminary report. Grobler, et al (2010) defined proactive as the digital forensic readiness of the organisation as well as the responsible use of digital forensic tools. The outputs of this phase are warrant and confirmation. Data collection: This phase is on the acquisition of data with seizure, imaging or collection of digital evidence to retrieve any form of breach. This phase is where all data relating to the breach either on the event logs, media storage, network traffic or among others are captured or stored for the next phase. The outputs of this phase are crime type and potential evidence sources.

Reconnaissance: This phase is on the competitive intelligence on the electronic evidence. This is carried out by duplicating the electronic evidences using standardized and accepted procedures. This is to ensure the validity and integrity of evidence for further usage. The output of this phase is event. Examination: This phase is concern with the transformation of the data into a more manageable size and form for analysis. It involves discovering and extracting hidden data, and matching pattern. It also identifies potential electronic evidence possibly within unconventional locations. The output of this phase is data.

Analysis: This phase is concern with organizing the examination results collected from the physical and digital evidence. It eliminates duplication of analysis, construct a hypothesis of the incident and compare the extracted data with the target. The output of this phase is information. Reporting: This phase is concern with the documentation of the findings which are developed in a report. The report provides the analytical findings and methodologies. The findings are presented to the authority usually the law or security enforcement agencies. Basically, the report is concern with legal admissibility of digital evidence presentation of the relevant evidence collected. The output of this phase is evidence.

9. CONCLUSION

The internet provides anonymity unlike traditional crimes wherein the criminal undertakes considerable risk, cybercrime provides the criminal with a cover. However, the lack of standards for forensics implementation against cybercrimes in Nigeria is itself criminal.

Digital evidence of cybercrimes is always in digital form. Law enforcement and security agencies in Nigeria are not only face with the new challenge of dealing with cybercrime but also the application of cyberforensics for cybercrime investigations.

The area of standards for cyberforensics is a technical issue and not a legal issue; thus, there is a need for the development of appropriate standards for the implementation of the Evidence Act (2011) in Nigeria.

FUTURE RESEARCH

The newly proposed model can be furthered map to various digital evidence and incident cases in order to make effective use of the investigation process. Also, there should be more research on cyberforensics so that up to date or appropriate technology can be implemented and acceptable by security agencies and legal institutions in which every organisation and private investigators are bound to follow these methodologies and procedures.

REFERENCES

1. Akindele, O (2011). Vulnerable cyberspace may threaten Nigeria's cashless economy. The Nigerian Voice, November 23, 2011. http://www.thenigerianvoice.com/nvnews/75922/1/vulnerable-cyberspace-may-threaten-nigerias-cashle.html
2. Basha, K.N (2010). Seminar and workshop in detection of cybercrime and investigation. Sarder Vallabhbhai Patel. National Police Academy, Hyderabad-500.052
3. Clough, J. (2011). Principles of cybercrime. West Nyack, NY: Cambridge University Press.
4. Dasuki, S (2014). Rate of cybercrimes in Nigeria is alarming. Saturday Vanguard Newspaper, June 21, 2014. http://issuu.com/vanguardngr/docs/21042014_203901ea7bf6a0
5. Daura, A (2014). FG commissions anti cybercrime forensic technology. ThisDayLive, April 10, 2014. http://www.thisdaylive.com/articles/fg-commissions-anti-cybercrime-forensic-technology/175751/
6. Draft standards for digital and computer forensics in Nigeria (2014). October 21, 2015. www.nitda.gov.ng/download/forensics.pdf
7. Deshmukh, J.J and Chaudhari, S.R (2014). Cyber crime in indian scenario – a literature snapshot. International Journal of Conceptions on Computing and Information Technology. Vol. 2, Issue 2, April 2014. http://www.worldairco.org/IJCCIT/February2014Paper27.pdf 14th July, 2014
8. Ec-council Ethical Hacking and Countermeasures. https://drive.google.com/folderview?id=0B3395G3fbL0ba0tiamZ1eUEyeWs&usp=sharing
9. Evidence Act, 2011. October 21, 2015. http://www.nassnig.org/document/download/5945
10. Fafinski, S., Dutton, W.H and Margetts, H (2010). Mapping and measuring cybercrime. www.oii.ox.ac.uk/publications/FD18.pdf 9th September, 2014.
11. Grobler, C.P., Louwrens, C.P and Solms, S.H (2010). A multi-component view of digital forensics. Availability, Reliability and Security (ARES) 10 International Conference 2010.
12. Kishore, N., Gupta, C and Dawar, D (2014). An insight view of digital forensics. International Journal on Computational Sciences and Applications. Vol. 4, Issue 6, December 2014.
13. Kumar, A.S (2013). Cyber forensics in Kerala. International Journal of Computer Science and Mobile Computing. http://www.ijcsmc.com/docs/papers/ICMIC13/ICMIC13S6.pdf 21st October, 2014
14. Longe, T (2014). UBA customers groan in pains over unresolved internet frauds! As CBN laments cybercrime. YouNewsng, June 19, 2014. http://www.younewsng.com/2014/06/19/uba-customers-groan-in-pains-over-unresolved-internet-frauds-as-cbn-laments-cybercrime/
15. Mark, N (2014). The increasing need for cyber forensic awareness and specialization in Army. September 15, 2015. http://search.informit.com.au/documentSummary;dn=676945662416271;res=IELAPA
16. Muthukumaran, B (2008). Cyber crime scenario in India. Criminal investigation department review. http://www.tnpolice.gov.in/pdfs/ReviewcyberJan08.pdf 22nd June, 2014
17. Palmer, G (2001). A road map for digital forensic research. The MITRE Corporation. July 10, 2015. http://www.dfrws.org/2001/dfrws-rm-final.pdf
18. Singh, N. and Rani, S (2013). The roadmap for cyber crime investigation. International Journal of Electronics and Computer Science Engineering. http://www.ijecse.org/wp-content/uploads/2013/03/Volume-2Number-2PP-497-502x.pdf 10th November, 2014.
19. Shridhar, G.A., Chandrakant, P.R. and Baburao, J.V (2013). Network/Cyber forensics. International Journal of Computer Science and Management Research. http://www.ijcsmr.org/eetecme2013/paper9.pdf 18th November, 2014.
20. Wando, H (2014). Rate of cybercrimes in Nigeria is alarming. Saturday Vanguard Newspaper, June 21, 2014. http://issuu.com/vanguardngr/docs/21042014_203901ea7bf6a0