Computer Forensic Guidelines: A Requirement for fighting Cyber Crime in Nigeria now?

Rukayat A. Ajetunmobi[1], Charles O. Uwadia[2], Florence A. Oladeji[3]
[1,2,3]Department of Computer Sciences, University of Lagos
[1]rajetunmobi@unilag.edu.ng, [2]couwadia@unilag.edu.ng , [3]foladeji@unilag.edu.ng

ABSTRACT

Computer Forensics in digital evidence collection regarding Cybercrime in the last few years by IT savvy countries has played very important role in case prosecution. However, that is not the case in Nigeria, a country that has vast human resources to battle Cybercrime, but is seriously lacking in using modern tools and knowledge to fight it. With the prominent, albeit negative role that cybercrime now occupies in Nigeria, it has become pertinent for the authors to raise the issue of using Computer Forensics for digital evidence collection which will in turn facilitate minimal amount of time used during physical evidence collection. Currently, there is no proper guideline in place for digital evidence gathering and this loophole is exploited by defence counsels during prosecution of cyber-related crimes. Since there are gaps between the laws used for prosecution of cybercriminals and enforcement procedures in Nigeria, the authors' work on Computer Forensics guidelines will serve as a midpoint that will hopefully bridge the gap and improve the performance rating of the Nigerian law enforcement agencies. In this paper, the authors are proposing standard Computer Forensics guidelines that will improve the investigation procedure to encourage admissibility of digital evidence in any court of law.

Keywords: Admissibility, chain of custody, computer forensics, cybercrime, digital evidence, Legislation.

1. INTRODUCTION

It has been an established fact that Cybercrime cases in Nigeria are mainly prosecuted by the Economic and Financial Crimes Commission (herein referred to as 'the EFCC') using documentary evidence collected during 'search and seizure' raids carried out by law enforcement agents. With the way cybercrime evidence is collected in Nigeria, all options must therefore be duly explored during digital evidence acquisition from collection, through processing, to preservation to ensure that when tendered in court, the suspect(s) related to the crime is/are undeniably and positively linked to the evidence for admissibility purposes.

Considering the fact that digital evidence exist in abundance on computer systems, communications systems, and embedded computer systems as well as organizers and storage devices, Computer forensics' procedure can be used to acquire these evidence in any crime investigation, process it according to laid down guidelines which will in turn make them admissible in any court by attorneys (both prosecution and defence) who must also learn to discover digital evidence and defend it against common arguments (Casey, 2004)

In the last few years, Nigeria has experienced a sharp increase in crimes involving disappearances and kidnappings of its citizens. Although the law enforcement agents are trying their best to solve these crimes, unfortunately, it is not enough. Using computer forensics as a mode of technology towards resolving these crimes will go a long way towards assisting the law enforcement agencies to solve and minimise these crimes.

Computer forensics is a branch of Forensic Science relevant to legal evidence found in computers and other forms of digital storage media. It can also be considered as the general name for obtaining, preserving, documenting, analysing and reporting on findings from forensic analysis of all digital –related media. It involves the utilization of digital technology, forensic tools and software to track and resolve issues in a way to preserve the originality, integrity and authenticity of the evidence and ensure its admissibility during legal proceedings.

Within the digital environment, there is evidence and indication that organisations and Governments of countries are discovering that without the effective usage of Computer Forensics, successful prosecution of its crimes committed using Information and Communication Technology would be impossible. An example of the unsuccessful prosecution due to lack of conclusive and admissive digital evidence here in Nigeria is the EFCC vs. James Ibori Case (BBC News, 2009), although James Ibori was later successfully prosecuted and jailed in the UK based on similar set of charges but using admissible forensically gathered evidence for his trial (Sahara reporters, 2012). Other unsuccessful prosecutions include high profile cases as those of the former Speaker of the House of Representatives, Hon. Dimeji Bankole; former Ogun State Governor, Chief Gbenga Daniel; Member of House of Representatives, Hon. Ndudi Elumelu all of which have been struck out by the courts respectively. The case involving the former Chief Executive Officer of the defunct Intercontinental Bank, Dr. Erastus Akingbola, and the three persons named in the $180m Halliburton bribery scandal were both dismissed within a space of one week interval. These were attributed to either lack of diligent prosecution on the part of EFCC's lawyers or for lack of substantive evidence (The Young News, 2012). Because of inadequate facilities and procedure during 'search and seizure' used by the Nigerian law enforcement agents, these lapses are often exploited by defence counsels when evidence tendered are found to be tainted and inconclusive to be admissible for successful prosecution of cases. The paper shall outline and illustrate how the proper, effective, but simplest means of practising Computer Forensics can be achieved (as defined by the Legal and ICT governing bodies, guidelines, laws and amendments with other regulatory policies complimenting). An example of the issue of admissibility of computer generated evidence is the appeal filed by former Nigerian Aviation Minister, Mr Femi Fani-Kayode, who was challenging the admissibility of computer generated statement of accounts under the old Evidence Act, Cap. E14 (Sahara Reporters, 2012) (Ask the Lawyer online, 2012).

Today, many messages and documents are exchanged over the internet and are read on the computer screen but not printed out. Information is also stored on USB drives, memory cards, and other storage devices that are easily transported without carrying any bulk (Information Security and Forensics Society, 2004). The convenience attached to IT and internet usage has now been exploited to serve criminal purposes.

With the above activities, it has been discovered that Nigeria needs a well-defined structural plan modelled to suit its socio-cultural and ethnic diversity. A proper Computer Forensics Guideline will serve as a good starting point towards achieving this goal. Currently, Nigeria has no digital forensics laboratory, while the procedure utilized is the normal 'search and seizure' process when suspect locations are raided by law enforcement agents.

2. RELATED LITERATURE REVIEW

The issue of cybercrime has been discussed by many people with various perspectives towards handling the issue. Cybercrime has gone beyond traditional criminal acts with far-reaching impact nationally and internationally due to the technology of the Internet being used. According to International Law, the United Nations has Cybercrime divided into two categories and defined accordingly (Shinder, 2002):

a. Cybercrime in a narrow sense (computer crime): Any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them.
b. Cybercrime in a broader sense (computer-related crime): Any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession (and) offering or distributing information by means of a computer system.

Professor Augustine Odinma stated that "cybercrime is any illegal act perpetrated in, on or through the Internet with the intent to cheat, defraud or cause the malfunction of a network device that may include a computer, phone, etc." (Background Check International, n.d.). Statistically, Nigeria is ranked 16th in the Q1 cyber-attacks vulnerability index in the world (Adepetun, 2016). Nigeria is also ranked 3rd in the world in cybercrime according to a cyber survey conducted. The report was contained in a global computer crime and security survey. (Babajide, 2016).

With Cyber crime's continuous erosion of global economy, statistics indicate that the financial sector of the global economy is worst hit. Nigerian banks over the years lost over N159 Billion to cybercrime between 2000 and 2013 (Akwaja, 2014). This amount increased to approximately N165 billion in 2014; the actual value lost in 2014 alone was put at N6.21 billion by the Nigeria Interbank Settlement System Plc. (NIBBS) (Enejeta, 2016). According to experts, from a report in the Global Trade Review (GTR), the traditional approach of all-in-one handling in Information Technology (IT) was no longer applicable for financial institutions. They were advised to build IT systems tailored specifically to handle each asset class, giving priority to the most lucrative ones (The Guardian, 2015). In 2015, Nigeria lost N40 billion to cybercrime from the statistics published by the Central Bank of Nigeria, according to Michael Oseji, the President/Chief Executive Officer, Integrated Cyber Security Solutions Limited. (Today Newspaper, 2016).

Though Nigeria is a signatory to treaties overseeing cybercrime activities, she has no set guideline to monitor and regulate its usage. In addition to this, Nigeria has also been identified by the International Communications Union as a weak link in the fight against cybercrime (Oladeinde, 2015). To combat some of these problems, The Nigerian Cybercrime Project was launched with the aim of ensuring the security of Computer Systems and Networks and the protection of Critical ICT infrastructure in Nigeria. This project was launched at AFRINET 2005 as a result of the Presidential Committee on Cybercrime's report stating the following points (Udotai, 2005) -

i. Recommendation of the creation of a legal and institutional framework for Cybercrime in Nigeria;
ii. creation of a central agency to enforce Cybercrime laws or situate responsibility within existing law enforcement institutions,

iii. creation of the Nigerian Cybercrime Working Group (NCWG) as an interagency body of law enforcement, intelligence, security and ICT institutions, including the private sector, and
iv. Proposal of a Draft Nigerian Computer Security and Protection Act.

According to Professor Oliver Osuagwu, he related cybercrime in Nigeria to the collapse of the educational sector; he pointed out that cybercrime was causing near total collapse of the education community especially in Nigeria with over 90% of the criminals coming from this sector. Having the wrong value system was identified as being a key factor that encourages cybercrime in Nigeria. The absence of enabling laws and guidelines makes policing of the situation even more difficult (Umo, 2010).

The cost incurred by the government due to the rise in cybercrime was separated into four categories, according to the Detica Report: costs in anticipation of cybercrime, costs as a consequence of cybercrime, costs in response to cybercrime, and indirect costs such as loss of confidence in cyber transaction (Anderson et al., 2012)

3. Overview of Cybercrime, Computer Forensics and Computer Forensic Guidelines

Cybercrime, a fast-growing area of crime is broadly defined as a crime conducted using electronic medium to perpetrate it. According to Interpol, law enforcement generally makes a distinction between the two main types of Internet-related crimes (Interpol, 2016) :

i. Advanced cybercrime – these are sophisticated attacks against computer hardware and software;
ii. Cyber-enabled crime – they are 'traditional' crimes that have evolved with the advent of the Internet, such as financial crimes, terrorism, and pornography.

A more comprehensive definition of cybercrime by (Laura, 1995) is given as "A criminal activity involving an information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft), and electronic fraud".

The Nigerian Cybercrime can be defined as computer-aided crime originating from Nigeria or has similarities to Nigerian scams. It can be categorised under three parts:

i. computer-aided crimes committed by Nigerians internationally,
ii. Non-Nigerian computer-aided crime giving the semblance of a "Nigerian" origin, and
iii. Crimes committed against Nigerian information and telecommunications assets.

Computer Forensics, which is a branch of Digital Forensics, can be defined as the use of specialized techniques for the specific purpose of *preservation, identification, extraction, authentication, examination, analysis, interpretation* and *precise documentation* of digital information (Cartel Working Group, 2010). It could also be defined 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." (Palmer, 2001)

Bearing in mind that computer-based electronic evidence is information of investigative value which is stored on or transmitted by a computer, it can be compared to fingerprints of DNA (deoxyribonucleic acid) evidence which are often indisputable in any court of law when presented leading to greater efficiencies and higher chances of success of admissibility in courts. Based on this, the need to have appropriate guidelines in place is necessary. These guidelines should serve to both guide the people working on the evidence and protect the human rights of the individuals involved (both the prosecution and the defendant parties).

In the UK, the ACPO (Association of Chief Police Officers (ACPO) have four basic guiding principles that govern digital evidence acquisition (Williams, 2012) –
Principle 1: No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.
Principle 2: In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
Principle 3: An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
Principle 4: The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.
The Nigerian Police also subscribes to the ACPO as well as the Interpol.

3.1 Goals of Computer Forensics Guidelines

The following are the goals of Computer Forensics Guidelines

i. Identification of the evidence
ii. Document the crime (usage of sketch and pictures)
iii. Collection and preservation of the evidence
iv. Proper packaging and transportation of the evidence, including signing all relevant forms by both all relevant parties.

4. Laws currently used for cybercrime Prosecution in Nigeria

i. Cybercrime (Prohibition, Prevention, etc.) Act, 2015
ii. Advanced Fee Fraud and other Fraud Related Offences Act 2006, Part II, section 13
iii. Money Laundering Prohibition Act 2003
iv. Economic and Financial Crimes Commission (Establishment) Act 2002
v. Failed Banks (recovery of debts) and Financial Malpractices Decree 1994, (amended) 1995, (amended) 1999
vi. Criminal Code Act 1990 (Part 6, Division 1, Chapter 34)
vii. The Central Bank of Nigeria Act 1991 (Part 7)
viii. Banks and other Financial Institutions Decree 1991 (Parts I and III)
ix. Evidence Act 2011

(Links to the laws are available in Appendix 1)

5. Proposed Computer Forensics Guidelines for Nigeria

For the purpose of this paper, the guidelines have been categorised into the following sections –

a. The Physical Environment Crime Scene

i. The crime scene should be cleared of personnel directly or indirectly related to the crime scene especially away from electronic devices and mains power switch in order to prevent the evidence being tampered with knowingly or unknowingly.
ii. Photographs and/or video recording of the scene should be taken to identify location. Where this is not possible, a sketch is drawn.
iii. Do not allow any person to touch the devices, open or close any programs. Where this cannot be avoided, follow the standard procedure and record all actions.
iv. Do not switch on any device.
v. Allow the printers to finish printing.
vi. Look out for notebooks, jotters, dairies, or other pieces of paper that may contain passwords, email or web addresses that may relate or not to the environment from where the evidence is being collected.
vii. Ensure that all items have signed and completed exhibit labels attached to them. Failure to do so may create difficulties with continuity and cause the equipment to be rejected by the forensic examiner that could lead to non-admissibility of the evidence in court later.

b. The Computer Equipment Crime Scene

viii. Where the computer/laptop is switched on, photograph the monitor (where possible) or record the contents displayed on the screen. Also take note of any other connected appliance (i.e. printer, scanner, etc.) and the connections at the back of the computer and/or laptop.
ix. Make sure that the computer is switched off – some screen savers may give the appearance that the computer is switched off, but hard drive and monitor activity lights may indicate that the machine is switched on.
x. Be aware that some laptop computers may power on by opening the lid.
xi. Remove the main power source battery from laptop computers. However, prior to doing so, consider if the machine is in standby mode. In such circumstances, battery removal could result in avoidable data loss.
xii. Ensure that the ports and cables are duly labelled so that the computer may be reconstructed at a later date.
xiii. If hard disks, flash drives or other storage devices are found at the suspected crime location, photograph, and then carefully bag and itemise each seized article.
xiv. Consider asking the user about the setup of the system, including any passwords, if circumstances warrant it. If these are given, record them accurately.
xv. Make detailed notes of all actions taken in relation to the computer equipment (i.e. keep contemporaneous notes up to date).

Since there are many data storage devices/media that may be encountered while searches are being conducted during criminal investigations, the following are often valuable sources of evidence and if dealt with in an evidentially acceptable manner, may enhance and quicken the investigation. If digital evidence cannot be acquired using any of the mobile forensic tools available, then the following items may be retrieved as evidence for further examination:

c. Items that can be considered as evidence

The following items should be examined during the search and seizure procedure:

i. Main unit: usually the box to which the monitor and keyboard are attached.

ii. Monitor, keyboard and mouse (only necessary in certain cases. If in doubt, seek expert advice).
iii. Leads (again only necessary in certain cases. If in doubt, seek expert advice).
iv. Power supply units.
v. Hard disks not fitted inside the computer.
vi. Modems (some contain phone numbers).
vii. External drives and other external devices.
viii. Wireless network cards
ix. Routers.
x. Digital cameras and memory cards.
xi. Floppy disks.
xii. Backup tapes.
xiii. CDs and DVDs.
xiv. Memory sticks, memory cards and all USB connected devices.

d. Miscellaneous items that can be retrieved from the crime scene

Always label the bags containing these items, not the items themselves. Other items that may be seized to assist in the examination of the equipment include –

i. Manuals of computer and software.
ii. Anything that may contain a password.
iii. Encryption keys.
iv. Security keys – required to physically open computer equipment and media storage boxes.
v. For comparisons of printouts, seize Printers, printouts and printer paper for forensic examination, if required.

Source: (Ajetunmobi, 2009)

If the aforementioned guidelines (5a – d) are followed for collection of evidence at site, the evidence can then be properly analysed and examined either at the crime scene, or in a computer forensic laboratory using any of the digital forensic investigative models, tools and techniques available.

6. Conclusion

Considering the current economic situation in the country, there is a high tendency for people to lean towards making quick money via unscrupulous means like cybercrime. If the guidelines proposed are followed, the search and seizure process will be eased, chain of custody of the evidence traceable and successful prosecution of cases easier.

7. Reference

Adepetun, A., 2016. *Nigeria ranks 16th in Q1 cyber attacks vulnerability index*. [Online] Lagos: The Guardian Newspaper Available at: http://guardian.ng/business-services/nigeria-ranks-16th-in-q1-cyber-attacks-vulnerability-index/ [Accessed 30 September 2016].

Ajetunmobi, R., 2009. *Cyber Crime - A Case for Computer Forensic Guidelines in Nigeria*. MSc Thesis. London: University of East London University of East London.

Akwaja, C., 2014. *Banks lose N159bn to Cybercrime*. [Online] Available at: http://www.leadership.ng/news/375560/banks-lose-n159bn-cyber-crime [Accessed 30 September 2016].

Anderson, R. et al., 2012. Measuring the Cost of Cybercrime. In *11th Workshop on the Economics of Information Security (June 2012)*., 2012. WEIS2.

Ask the Lawyer online, 2012. *COMPUTER GENERATED EVIDENCE---(THE LAW THEN, THE LAW NOW),(FEDERAL REPUBLIC OF NIGERIA v. FEMI FANI-KAYODE and MRS. ELIZABETH N. ANYAEBOSI v. R. T BRISOE (NIG.) LTD*. [Online] Available at: http://askthelawyeronline.com/version2/members/casesummaries/details.php?id=2 [Accessed 24 October 2012].

Babajide, L., 2016. *Nigeria ranked third in the world for cyber crime*. [Online] Available at: http://crimeworldnaija.blogspot.com.ng/2016/07/nigeria-ranked-third-in-world-for-cyber.html [Accessed 30 September 2016].

Background Check International, n.d. *Information Technology/Cyber Security Solutions*. Report. Background Check International.

BBC News, 2009. *BBC News*. [Online] Available at: news.bbc.co.uk/hi/africa/8418302.stm [Accessed 19 January 2012].

Cartel Working Group, 2010. Anti-Cartel Enforcement Manual. *International Competition Network*, pp.2-27.

Casey, E., 2004. *Digital Evidence and Computer Crime*. 2nd ed. London: Academic Press.

Enejeta, E., 2016. *Cyber security threats heighten in financial sector*. [Online] (http://www.financialwatchngr.com/2016/05/27/cyber-security-threats-heighten-financial-sector/) [Accessed 30 September 2016].

Information Security and Forensics Society, 2004. *Computer Forensics*. [Online] Available at: http://www.isfs.org.hk/publications/ComputerForensics/ComputerForensics_part1.pdf [Accessed 2 December 2008].

Interpol, 2016. *Cybercrime*. [Online] Available at: http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime [Accessed 30 September 2016].

Laura, A., 1995. *Cyber Crime and National Security: The Role of the Penal and Procedural Law*. [Online] Available at: http://nials-nigeria.org/pub/lauraani.pdf [Accessed 30 September 2016].

Oladeinde, K., 2015. *Nigeria ranked 134th on global ICT DEvelopment Index*. [Online] Available at: http://technologytimes.ng/nigeria-ranked-134th-global-ict-development-index/ [Accessed 30 September 2016].

Palmer, G.L., 2001. *A Road Map for Digital Forensic Research*. Utica: DFRWS.

Sahara reporters, 2012. *Sahara Reporters*. [Online] Available at: http://saharareporters.com/2012/04/17/nigeria-uk-conviction-james-ibori-blow-against-corruption-human-rights-watch [Accessed 17 April 2012].

Sahara Reporters, 2012. *Supreme Court Dismisses Fani-Kayode's Appeal*. [Online] Available at: http://saharareporters.com/2012/05/04/supreme-court-dismisses-fani-kayode%E2%80%99s-appeal [Accessed 04 May 2012].

Shinder, D.L., 2002. *Scene of the cybercrime: computer Forensics Handbook*. Syngress.

The Guardian, 2015. *Financial institutions and challenges of cyber crime*. [Online] The Guardian Newspaper Nigeria Available at: http://guardian.ng/business-services/money/financial-institutions-and-challenges-of-cyber-crime/ [Accessed 30 September 2016].

The Young News, 2012. *The Young News Blogspot*. [Online] Available at: http://theyoungnews.blogspot.com.ng/2012/05/ibori-and-nigerias-faltering-anti-graft.html [Accessed 12 May 2012].

Today Newspaper, 2016. *Nigeria lost N40bn to cybercrime in 2015*. [Online] Available at: https://www.today.ng/technology/123740/nigeria-lost-n40bn-cybercrime-2015-expert [Accessed 30 September 2016].

Udotai, B.E., 2005. *The Nigerian Cybersecurity Project: Initiative to secure the Internet for Economic Developmnet and Growth*. Communique. http://www.ncc.gov.ng/AFRINET/Afrinet2005/Afrinet2k5papers&communique/Nigerian%20Cybersecuirty%20Project%20-%20Barr.pdf.

Umo, M.G.G.G., 2010. *Cyber Threats: Implications for Nigeria's National Interest*. [Online] Available at: https://docs.google.com/file/d/0B9sby6N_v5O3M2FlNWIzZjgtMDRiOS00NjI1LThmMjItNmI0Nzg5NGVlNTM2/edit?num=50&sort=name&layout=list&pli=1 [Accessed 30 September 2016].

Williams, J.Q.D., 2012. *ACPO Good Practice Guide for Digital Evidence*. [Online] Metropolitan Police Service: Metropolitan Police Service (5.0) Available at: http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf [Accessed 4 October 2016].

Appendix 1

https://cert.gov.ng/images/uploads/CyberCrime_(Prohibition,Prevention,etc)_Act,_2015.pdf

http://www.nigeria-law.org/LFN-comprehensiveIndex.htm

http://www.nigeria-law.org/Advance%20Fee%20Fraud%20and%2 0other%20Fraud %20Related%20Offences%20Act%202006.htm

http://www.nigeria-law.org/BanksAndOtherFinancialInstitutionsDecree1991.htm

http://www.nigeria-law.org/CentralBankOfNigeriaDecree.htm

http://www.nigeria-law.org/Criminal%20Code%20Act-Tables.htm

http://www.nigeria-law.org/Economic%20And%20Financial%20Crimes %20Commission%20(Establishment)%20Act.htm

http://www.nigeria-law.org/Money%20Laundering%20(Prohibition)%20Act%202003.htm.

http://www.nassnig.org/document/download/5945