ARTICLE:

The application of forensics examination in crime-related prosecution: The need for standardization and a recognized model in Nigeria

By **Davidson C. Onwubiko** and **Felix E. Eboibi**

The increased use of the internet and information technology in Nigeria has led to the need to utilize technologies to identify and prosecute perpetrators of crimes. In today's world, the application of forensics in the investigation and prosecution of crimes is essential. This paper critically examines the effect of the absence of a coordinated standard for the execution and presentation of forensic investigations utilizing electronic evidence in Nigeria. It examines the nature and scope of the various forensic models proposed, while questioning the appropriateness or otherwise of their usefulness in criminal prosecutions. The paper suggests the need for the regulation of forensics practices, the provision of standards, and a universal model for the successful prosecution of crimes in Nigeria.

Introduction

It is not an exaggeration to say that digital devices have become an integral part of our everyday lives. A great deal of information can be found on devices, which can provide insights into the character, behaviour, and plans of the user. The data captured and stored on a digital device can generally be used in both civil and criminal investigations. Digital forensics can aid an investigator in the analysis of criminal activities. Every online activity leaves a trace that can be followed by an appropriately trained and experienced investigator. Digital forensics can assist an investigator in locating a suspect. People often use their laptop, tablet, smartphone, and smart watch to navigate the world, using online maps and even provide a status update on social media, thereby potentially showing their location, date and time. Hence, an investigator may review a person's Global Positioning System (GPS) history to learn the locations their devices have recorded at particular points in time, although the evidence is not always certain, because the data recorded may be incorrect.[1]

Digital forensics is a new discipline in Nigeria. Following the enactment of the Nigerian Evidence Act, 2011, digital forensics has begun to flourish. Before 2011, digital evidence was not necessarily admissible as evidence in the Nigerian Courts.[2] For instance, in an interlocutory hearing in *Femi Fani-Kayode v The Federal Republic of Nigeria*,[3] the Federal High Court in Lagos rejected as inadmissible digital evidence relating to statements of account tendered by the prosecution in proof of a charge of money laundering against the defendant in the absence of any provision allowing the admissibility of digital evidence.[4] The use of digital forensics to investigate cybercrimes was enabled by the enactment of the Nigerian Cybercrimes (Prohibition, Prevention, etc,) Act 2015. The Act came into force in May 2015.

A digital forensics laboratory was established in Abuja for the Nigerian Police force in 2016. Unfortunately,

[1] R. P. Coutts and H. Selby, 'Problems with cell phone evidence tendered to 'prove' the location of a person at a point in time', 13 *Digital Evidence and Electronic Signature Law Review* (2016), 76-87, available at https://journals.sas.ac.uk/deeslr/issue/view/336 (Further notes that "The use of mobile telephone evidence as a means of accurately locating the telephone and its user is problematic.").

[2] T. Tion, 'Electronic evidence in Nigeria', 11 *Digital Evidence and Electronic Signature Law Review*, (2014), 76 – 84, available at https://journals.sas.ac.uk/deeslr/issue/view/319.

[3] Case No FHC/L/523C/08 of 26/3/2009 (Unreported).

[4] See also *UBA v Sani Abacha Foundations for Peace and Unity* (2004) 3 NWLR (pt 86) 516; *Numba Commercial Farms Ltd & Anor. v NIAL Merchant Bank Ltd & Anor* (2001) 16 NWLR (pt. 740) 510.

most security and law enforcement agencies do not use digital forensics in their investigations, although the Economic and Financial Crimes Commission (EFCC) has pledged to provide forensics assistance to agencies involved in complex criminal investigations.[5] In Nigeria today, the EFCC is seen as the main agency that uses digital forensics in criminal investigations. However, the EFCC faces problems when compared with other security and law enforcement agencies around the world, because their record in court is poor. According to Chijioke,[6] the Nigerian Police Force recorded a total of 1,072,026 cases between 1996 and 2000. Only 43.1 per cent (462,058) cases were prosecuted, while 50.5 per cent (540,899) were either under-investigated or closed for lack of evidence.[7] According to Oko,[8] the Nigerian Police Force has failed in the use of forensics in criminal investigations.

Notwithstanding the use of digital forensics by some security and law enforcement agencies in Nigeria in criminal investigations, the authors consider it is necessary for digital forensics in criminal investigations to be regulated in Nigeria. Not having a regulatory body overseeing digital forensics in Nigeria can cause inconsistencies during the investigation process. Unfortunately, different security and law enforcement agencies in Nigeria have different standards for criminal investigations. These are based on their standard of operation (SOP). The SOP differs between agencies. This means there is no documented digital forensics model for use by the security and law enforcement agencies in Nigeria. The lack of digital forensics model poses great challenges for criminal investigations and prosecution in Nigeria. The admissibility of digital evidence is based on the procedure (a digital forensics model) used for the collection of such evidence. If the correct procedure is not followed when collecting evidence, the evidence will not be admissible. Another challenge is the time spent in investigating a crime. With a digital forensics model, an investigator can save time and resources,[9] since the model guides an investigator on what to do and how to do it.[10] To reiterate, the lack of a digital forensic model in Nigeria has resulted in prolonged investigation and prosecution of criminal cases and conflicting results from digital forensics examinations by forensics units and experts within the Nigerian law enforcement community. Consequently, there is an urgent need to develop a model for the use of digital forensics in Nigeria. Law enforcement agents and prosecuting counsel should be trained and retrained on standard procedures, digital forensics, and best practices.

Tackling crime through forensics examination and investigation: Applicable models and standardization

According to Umesh and Neha, for an outcome of a digital forensics investigation to be admissible in a court of law, the acquisition and analysis of the digital evidence ought to follow the correct procedure.[11] In their analysis of digital forensic investigation models in other jurisdictions, they demonstrate that such models could lead an investigator to relevant information during an investigation. When the investigator adopts the correct procedure, the digital forensic process used should be able to be replicated by any forensics examiner using the same tools and

[5] M. Ogune (January 26, 2018). EFCC promises enforcement agencies of forensic assistance in complex crimes, at https://guardian.ng/news/efcc-promises-enforcement-agencies-of-forensic-assistance-in-complex-crimes/.

[6] C.E. Chijioke (2013). Crime and criminal investigation in Nigeria: A Study of police criminal investigation in Enugu State. *International journal of Africa and Asian studies,* 1, 66 – 72.

[7] O. Soyombo (2005). Integrating empirical research in the planning and training programs of Nigeria Police: options and prospects. In Alemika, Etani E.O (ed.), C*rime and policing in Nigeria: Challenges and option* (126-145). Lagos: Cleen Foundation.

[8] E. Oko (2018). The Nigeria Police force investigation failure. *Journal of forensics Science and crime investigation.* 9(1), 001-007.

[9] Xiaoyu Du, Nhien-An Le-Khac and Mark Scanlon (2017) Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service. Available athttps://www.researchgate.net/publication/318981575.

[10] National information technology development agency [NITDA] (2014). Standards for digital and computer forensics in Nigeria. Draft v0.2. Available athttps://www.scribd.com/document/287428618/Guidelines-on-Digital-Forensic-pdf.

[11] Umesh Singh and Neha Gaud (2015) Analysis of the digital forensic investigation models. Udgam Vigyati, Volume 2, 144-149, online at http://udgamvigyati.org/admin/images/Analysis%20Of%20The%20Digital%20Forensic%20Investigation%20Models-%20Prof%20(Dr)%20Umesh%20Singh;%20Ms%20Neha%20Gaud.pdf.

procedure.[12] Various commentators described different models when describing digital forensics investigations. A model serves as a guide in digital forensics investigations. The model demonstrates to an investigator how an investigation may proceed from beginning to end. Strict adherence to a model should result in a process that can be replicated by another investigator to arrive at the same result. On the other hand, when a model is not strictly and accurately followed, any attempt to replicate the process will produce a result different from that of the investigator. Digital forensics practiced in Nigeria, is in its infancy, according to the National Information Technology Development Agency (NITDA),[13] when compared to other nations such as the USA, UK, and India. Some government agencies such as EFCC, Department of State Security Services (DSSS), and the National Information Technology Development Agency are making great efforts towards the development of digital forensics in Nigeria. However, these agencies do not have a documented standardized model. The standard operating procedure of an agency may be specific to the agency, but it is not the case with a standardized digital forensic model, which should be documented and be made publicly available for other agencies and scholars to make reference to. Several digital forensics models exist around the world. A number of models are reviewed below and compared with the processes used in Nigerian investigations, described thus: When a crime is committed or ongoing it is often reported.[14] Where a complainant does make a complaint, a provision is made for the documentation of the crime,[15] and then the crime is evaluated to identify the skills, tools and the documents[16] required for the investigation. The investigator gathers the evidence in accordance with the Evidence Act 2011, and then the evidence obtained is examined and analyzed. A report is prepared and presented to the jury or investigative panel for administrative purpose. Finally, the evidence is returned to the owner at the end of the investigation and the report archived.[17]

The Digital Forensics Research Working Group

In 2001, the Digital Forensics Research Working Group (DFRW)[18] held the first Digital Forensic Research Workshop in the United States. The group developed a digital forensic model with seven stages, which include: identification; preservation; collection; examination; analysis; presentation, and decision.[19] Each phase is considered a class of activity, which can be performed while carrying out a digital forensic investigation. Each class includes a set of techniques or methods to be performed in that phase.[20] For example, the presentation phase, which is the sixth phase in the model, has the following activities: documentation, expert testimony, clarification, mission impact statement, recommended countermeasure, and statistical interpretation. 'Documentation' is not mentioned as a specific phase in this model. This will make it difficult to adopt in Nigeria, because the legal system operates on the basis of specific rules, and 'documentation' needs to be made explicit throughout the model.

In the Nigerian investigation process, when a crime is reported to a law enforcement agent, the agent is expected to document the crime before commencing an investigation.[21]

[12] National information technology development agency [NITDA] (2014). Standards for digital and computer forensics in Nigeria. Draft v0.2. Available athttps://www.scribd.com/document/287428618/Guidelines-on-Digital-Forensic-pdf.

[13] National information technology development agency [NITDA] (2014). Standards for digital and computer forensics in Nigeria. Draft v0.2.

[14] Administration of Criminal Justice Act 2015, 88(1).

[15] Administration of Criminal Justice Act 2015, 89(1).

[16] Associate, Dewpoint Legal Practitioners. 27 October 2017. Correspondence with Research Directorate.

[17] Nigeria. 31 October 2017 Police Force, Special Fraud Unit. Correspondence form a Police Public relations officer to the Research Directorate.

[18] https://dfrws.org/.

[19] A. Agarwal and M. Gupta (2011). Systematic Digital Forensic Investigation Model. *International Journal of Computer Science and Security*, 5(1), 118 -131.

[20] Digital Forensic Research Workshop (DFRWS) Research Road Map, Utica, NY. (2001) Available at https://www.dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf.

[21] It is appreciated that police forces in other jurisdictions have the same duty.

The Kruse and Heiser digital forensic investigation model

The Kruse and Heiser investigation model consists of three basic stages or components: acquiring evidence, authenticating evidence, and analyzing evidence. In this model, the main focus is on maintaining the integrity of the evidence during the investigation process. Based on the scope of the Nigeria investigation process, the investigation process places a high value on the output of an investigation process. The Kruse and Heiser digital forensic investigation model omits a significant step in the Nigerian investigation process, that is, reporting. The essence of an investigation is to enable a report to be prepared outlining how a crime was committed. This report is available to either an investigating panel or to a jury and judge.

The Casey model

The Casey model focuses mainly on the investigation. It has four stages, namely: recognition, preservation, classification, and reconstruction. This model is highly technical.[22] Casey places the focus of the forensic process on the investigation itself. This model does not emphasize legal adherence, which is an integral part of the investigation process in Nigeria.

Forensic Process Model

One of the models used in the US is the Forensic Process Model. This is a four-step model, namely: collection, examination, analysis, and reporting. This model is published by the U.S. Department of Justice[23] in accordance with the standards published by the Scientific Working Group on Digital Forensics (SWGDE) adopted by Group of eight (G8) in 2001. Since the U.S. Department of Justice itself publishes this model, and National Institute of Standards and Technology[24] has provided both tools[25] and tool testing capability for evidence acquisition,[26] strict adherence to this model should mean the evidence collected would be admissible.

United Kingdom

The police in England and Wales have provided guidance in the form of the *Good Practice Guide for Digital Evidence*,[27] and the Forensic Science Regulator works to provide for UK-wide quality standards.[28] This is a four-step model. It is in line with the four principles published in section 2 of the guide.

Recommendation

The authors recommend a basic forensic model, which can allow for the addition of more phases to suit the Nigeria investigation process. The Forensic Process Model would be a good beginning, because it is a simple model. [29] While phases such as planning, identification, documentation, and presentation can be added to make it much suitable for Nigeria.

Criminal adjudication and the effect of digital forensics: Rethinking the regulation of digital forensics in Nigeria

With the proliferation of ICT and its use in the commission of crimes, prosecutors face a significant

[22] A. Agarwal, M. Gupta, S. Gupta, and S.C. Gupta (2011). Systematic Digital Forensic Investigation Model. *International Journal of Computer Science and Security*, 5(1), 118-131.

[23] V. H. Sarah (2004). Forensic Examination of Digital Evidence: A Guide for Law Enforcement; Technical Work Group for Electronic Crime Scene Investigation (TWGECSI) (2001). Electronic Crime Scene Investigation: A Guide for First Responders. Available at https://www.ncjrs.gov/pdffiles1/nij/187736.pdf.

[24] National Institute of Justice (NIJ) (2001) Electronic crime scene investigation guide: a guide for first responders. National Institute of Justice, Department of Justice (DoJ) 2001. Available at http://www.ncjrs.gov/pdffiles1/nij/187736.pdf.

[25] NIST (2001) Disk imaging tool specification. NIST, Gaithersburg (Unpublished manuscript) Available at https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=51081.

[26] NIST (2007) Test results for hardware write block device: Tableau Forensic SATA Bridge T3u. NIST, Gaithersburg (Unpublished manuscript) Available at https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/cftt-technical/hardware.

[27] Janet Willian QPM (2012). ACPO Good practice guide for digital evidence. Available at https://www.digital-detective.net/acpo-good-practice-guide-for-digital-evidence/.

[28] https://www.gov.uk/government/organisations/forensic-science-regulator/about#responsibilities.

[29] O.L. Carroll, S.K. Brannon, T. Song (2017) 56 U.S Attorney's Bulletin, January 2008 available at https://www.crime-scene-investigator.net/computer-forensics-digital-forensic-analysis-methodology.html.

task in identifying and prosecuting the perpetrators. This is one of the challenges in the administration of criminal justice in Nigeria. This is made worse, because often the accused will not willingly or voluntarily confess to being responsible for an alleged crime. There are, as a result, high rates of denials, even with witnesses to the crimes being committed.[30]

These issues remain, despite a legal framework in place to aid criminal investigators and prosecutors. Sections 56 – 66 of the Nigerian Evidence Act 1945[31] permits criminal investigators to utilize scientific means in the conduct of their investigations. This enables expert or forensic evidence to be tendered in criminal matters in courts of competent jurisdiction. However, forensic evidence was rarely used in criminal matters prior to the enactment of the Nigerian Evidence Act 2011 because electronic evidence was not admissible in evidence in the absence of any specific provision to admit such evidence in the Evidence Act.[32]

Changes occurred when the Nigerian government enacted the Nigerian Evidence Act 2011, which repealed the Evidence Act. The new Act now recognises that forensic evidence may be tendered, and digital evidence is now admissible in criminal matters. Explicitly, sections 66 and 67 of the Evidence Act 2011 allow the use of forensic examination of fingerprints, handwriting, palm prints, voice, electronic and computer devices of perpetrators of crime during a criminal investigation. Also, such evidence by criminal investigators or forensic experts in the course of criminal hearings can assist the court to determine the guilt or otherwise of perpetrators of crime.[33] Section 84 of the Evidence Act 2011 provides for the admissibility of computer evidence, subject to the provision of a certificate that the computer was operating properly.[34]

The application of digital forensics in the investigation and prosecution of crimes has become even more exigent with the enactment of the Nigerian Cybercrimes Act 2015. The Act addresses crimes committed using a computer either as a tool or a target.[35]

In Nigeria, it is rare for law enforcement agencies in criminal investigations to use digital forensics in the collection, analysis and preparation of the evidence for legal proceedings. The corollary is that criminal matters are not properly investigated, and the prosecution is poorly executed, which results in the discharge of cases or acquittal of perpetrators of crimes in Nigeria. For instance, in *Federal Republic of Nigeria v Sunday Lucky Egbefoh*,[36] the respondent was charged with obtaining money by false pretences. At the conclusion of the trial, the respondent was discharged and acquitted on all counts. Dissatisfied with the decision, the prosecutor appealed before the Court of Appeal. In that case, the complainant (PW1) paid his bills from a bank account in the United Kingdom with the help of his friend who lives there. The defence case was that unknown hackers hacked into the complainant's e-mail account and requested the transfer of the sum of £7,000 and £9,000 for payment of bills in the UK. The complainant transferred the money to the designated bank account as directed, but the monies were not received. The complainant subsequently received another e-mail from his friend asking for the payment of the Naira equivalent of the monies requested for

[30] A. M. Adebayo (2018). *Casebook on Nigerian Criminal Law: Texts, Comments & Cases*. Lagos, Princeton & Associates Publishing Co. Ltd., 113.

[31] Cap 112, Laws of the Federation of Nigeria, 1990; Cap E14, Laws of the Federation of Nigeria, 2004.

[32] F. E. Eboibi (2011). Cybercrime Prosecution and the Nigerian Evidence Act 2011: Challenges of Electronic Evidence. *Nigerian Law & Practice Journal*, 10, 139-160.

[33] Nigerian Evidence Act, 2011, ss. 66 and 67.

[34] For the impossibility of demonstrating a computer is operating properly, see Chapter 6 in Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017), Open Access PDF version in the Humanities Digital Library http://ials.sas.ac.uk/digital/humanities-digital-library/observing-law-ials-open-book-service-law/electronic-evidence; for a detailed technological article that makes it clear that the legal provision of 'reliability' is impossible, see Peter Bernard Ladkin, Bev Littlewood, Harold Thimbleby and Martyn Thomas CBE, 'The Law Commission presumption concerning the dependability of computer evidence', 17 *Digital Evidence and Electronic Signature Law Review* (2020) 1 – 14, at https://journals.sas.ac.uk/index.php/deeslr.

[35] F. E. Eboibi (2018). The Regulation of Cybercitizens' Conduct on Cyberspace: The Constitutionality and Applicability of the Nigerian Cybercrimes Act 2015. *National Journal of Cyber Security Law*, 41.

[36] (2019) LPELR- 47872(CA), 1-29.

into a Nigerian Bank account. The complainant became suspicious and consequently alerted the EFCC. The defendant admitted in his statement that payment was made into the Nigerian bank account alleged to be that of the respondent. The officer investigating the case confirmed this. The respondent was arrested when he approached the bank concerning the account. The respondent alleged that he visited the bank to lodge a complaint with respect to the failure of his ATM card and the receipt of a credit alert from a source that was unknown to him. The respondent confessed to the law enforcement agent that he was an internet fraudster. He stated how he facilitated his fraud-related activities against victims with the use of an Apple telephone and the internet, and the fact that he hacked the complainant's e-mail account and posed as his friend to orchestrate the alleged fraud against the victim with the use of his Diamond bank account, where the money was lodged.

The Court of Appeal accepted the evidence of the lead investigator (PW2) when he stated that the e-mail of the complainant was actually hacked into, and as a result his business correspondence was intercepted by fraudsters as claimed by the respondent, that is, someone other than the respondent. The court held:

> 'From the materials and evidence placed before me there is apparently no linkage between the defendant and the designated account domiciled in Metro [sic] Bank Plc UK. Nothing was found in the defendant's email account or other social media accounts scrutinized by PW2, to link the defendant to the said account. Nor was anything incriminating found and recovered from the residence of the defendant when searched by PW2, (and his team) to link the defendant, DW1, to the account in Metro Bank Plc UK... Equally, nothing was available at the hard drive of the defendant's smart phone, which by his own admission he uses to browse the internet. There is no shred of evidence before the Court that he is the owner of the said account or that he made any deposits or withdrawals from the said account. In fact, there is nothing placed before the Court, which ties the account to Lucky Sunday Egbefoh, the defendant herein… (PW2) was unable to precisely tell the Court when the hack took place. Was it before or after 10/11/14, when the email instruction to pay the 7,000 pounds sterling into a designated account domiciled with Metro Bank Plc UK was received by PW1…?'[37]

In the final analysis, while discharging and acquitting the respondent despite the evidence of the lead investigator, the court held that 'the conflating and concatenation of the foregoing is that the appeal is devoid of merit. The same fails and it is hereby dismissed. The decision of the lower Court, with the verdict of discharge and acquittal of the Respondent on all the Counts of the Information is hereby affirmed.'[38] This is a case where the application of a digital forensic investigation by the EFCC would have aided the court in answering the questions posed by it. Obviously, the lead investigator who testified in the matter was not a digital forensic expert. The respondent's smartphone, e-mail, internet facility, and hard drive were not presented before any forensic expert for forensic examination to link the respondent to the commission of the crime. The court was left with no other choice than to discharge and acquit the defendant.

Oluwatomi Ajayi discusses the effectiveness of the application of forensic investigation by law enforcement agents during interrogation:

> 'Essentially, officers interrogating should always strive to go after the facts or assess carefully the information passed to them by suspect. In Adegbaye Ibikunle v State,[39] the Supreme Court stated amongst others that if a **proper method of investigation** were to have been adopted in this case, the true facts would have been apparent.'[40]

He consequently rightly suggested the introduction of proper forensic standards in accordance with global best practices in Nigeria. Moreover, Walmer Dupar

[37] (2019) LPELR- 47872(CA), 1-29, at 15-16.

[38] (2019) LPELR- 47872(CA), 1-29, at 28-29.

[39] SC/220/2005 in O. A. Ajayi (2018). *Crime Scene and Forensic Investigation – Basic Tunnel Vision on Interrogation Process.* Nigeria, Malthouse Press, Ltd., 37 – emphasis added.

[40] O. A. Ajayi (2018). *Crime Scene and Forensic Investigation – Basic Tunnel Vision on Interrogation Process.* Nigeria, Malthouse Press, Ltd., 37, 91.

highlights the danger of the lack of application of digital forensics by the police in the investigation of crimes in Nigeria thus:

> '[there]…is a serious dip in the standard of investigation with a consequent negative effect on quality of investigation with a consequent negative effect on quality of evidence available at criminal trials.'[41]

He notes further that:

> '… it does neither the image of the police force nor confidence in their undoubted ability any good if every time there is a reported crime perpetrators get away scot free due to deficiencies in investigation and discovery capacity... the importance of scientific and forensic support for crime detection should never be underrated.'[42]

Moreover, even when digital forensics are utilized, possibly because there is no acceptable model and no regulatory body to oversee such a model, defendants are still being discharged and acquitted. For instance, in *Federal Republic of Nigeria v Ojo & Anor.,*[43] the respondents were charged with issuance of dishonoured cheques, conspiracy to commit forgery, forgery and uttering of a certificate of occupancy, and obtaining money by false pretences. At the conclusion of the hearing, the respondents were discharged and acquitted. Dissatisfied with the judgment, the prosecution appealed. In affirming the decision of the trial court, the Court of Appeal examined the propriety of the digital forensic evidence vis-à-vis section 84 of the Nigerian Evidence Act 2011. The witness was an officer of the EFCC and the Head of the Telephone Forensic Unit. His evidence was to the effect that he extracted the contents of a telephone (in particular text messages from telephones) using a forensic software programme. He printed the findings on paper. He did not sign the printouts on the premise that he ought not to sign after printing, because they were, more or less, a forensic report. The prosecution did not serve a certificate, contrary to the provisions of section 84(1) and (2) of the Nigerian Evidence Act 2011. The issue was whether the report was admissible pursuant to the provisions of section 85, and the court held thus:

> 'The correct interpretation to be given to this Section 84 of the Evidence Act where electronically generated document is sought to be demonstrated is that such electronically generated evidence must be certified and must comply with preconditions laid down in Section 84(2). Therefore, in the light of the above, Exhibits Q & R not having been backed up is inadmissible. The purpose of a certificate is to authenticate the means of production. They are expunged from the records.'[44]

There are no guiding principles for forensics investigations, from the crime scene through to prosecution of the case at trial. Law enforcement agents use different procedures and models, resulting in conflicting forensic reports and examinations. The forensic reports do not adequately assist the courts in determining the guilt or otherwise of the accused, with the result that confusing evidence is tendered before the courts. The submission of forensic evidence in court is at the whim of the forensic investigator's employer, rather than pursuant to a sound and provable forensic model. This diminishes the integrity of the evidence and the admissibility of such evidence.

An example is the case of *Harrison Odiawa v FRN*[45], which involved internet fraud. The defendant sent an e-mail to the victim (a US citizen resident in Virginia) requesting his interest in the transfer of 20.5 billion dollars. The victim, Mr Blick, accepted and provided a

[41] W. Dupar (2018). Revisiting the impact of scientific investigation on criminal prosecution in Nigeria. *The Nigerian Law Journal,* 21(1), 206.

[42] Revisiting the impact of scientific investigation on criminal prosecution in Nigeria, at 209, 211: 'That is to say that unless a matter is properly investigated, the culprit is properly identified and apprehended and all evidences that will be relied upon by the prosecution to place such a suspect at the scene of crime as the person who perpetrated the offence charged, the prosecution case will fail. Forensic investigation by use of scientific technology provided the needed help in ensuring that perpetrators of criminal activities are identified by providing un-conflicting evidence pointing to no other person but the perpetrator of a criminal act from the bid of evidence of left behind and analyzed at forensic laboratory…').

[43] (2018) LPELR-45541(CA).

[44] (2018) LPELR-45541(CA), at 21-23; see also *Dickson v Chief Timipre Marilin Sylva & Ors* (2016) LPELR – 41257 (SC); *Kubor v Dickson* (2013) ALL FWLR (PT.676) 392 at 429.

[45] (2003 - 2010) ECLR 19 – 99; (2008) All FWLR (pt. 439); LPELR-CA/L/124/2006.

US business bank account for the transfer of the funds. The defendant made demands for several sum of monies in dollars for the deal to go through – which the victim obliged. Subsequently, Mr Blick could not reach the defendant through telephone and e-mail. He consequently reported the matter to the EFCC. Mr Blick had never met the defendant. Upon his arrest, certain documents, e-mails and voice calls that were recorded were sent to the EFCC forensic laboratory for examination – the result matched that of the defendant. A police forensic expert examined these documents at the police forensics laboratory. The report did not link the defendant to the evidence. A forensic examination report was also submitted by the prosecution through an expert witness, Muazu Abdullahi, a forensic expert and member of staff at the EFCC. His report implicated the defendant in the commission of the crime. The prosecution and defence presented both reports to the court. The defence expert witness, Inspector Raphael Onwuzuligbo, a police inspector attached to the forensic laboratory of the Force Criminal Investigation Department (FCID) also assessed the electronic evidence. His report absolved the defendant in the commission of the crime. The court discarded the forensic report of the defence expert witness for two reasons: (i) the defence expert witness report was made to mislead the court, and (ii) the expert witness did not state his qualifications or experience – in fact he had no professional experience. The court relied on that of the prosecution expert witness. The court noted that the purpose of the defence forensic expert report 'was to achieve a preconceived agenda to mislead the Court...').[46]

Most criminal prosecutors do not appreciate the importance of forensic and electronic evidence in assisting the court in the determination of the guilt of an accused person in criminal trials. In the case of *Federal Republic of Nigeria v Ojo & Anor.,*[47] noted above, a criminal prosecutor who is conversant with the applicability and importance of digital forensics and evidence should have known that the admissibility of digital evidence before the courts during criminal proceedings is subject to the fulfilment of the conditions enshrined in section 84(1) and (2) of the Nigerian Evidence Act 2011 – the requirement for a signature on the report or document and the provisions of certification by the forensics examiner or expert. For the prosecutor to have allowed the witness to give evidence in the way he did in the absence of a signature and certification of exhibits shows the exigency of the establishment of a regulatory body concerning digital forensics in criminal investigations and prosecutions in Nigeria. The case of *Federal Republic of Nigeria v Sunday Lucky Egbefoh*[48] serves to illustrate the level of importance criminal prosecutors place on digital forensics evidence. The investigator was not a forensics expert. In order to link the defendant to the crimes alleged against him, prosecuting counsel argued that since the defendant is a graduate of computer science, and the fact that he browses the internet with his Apple device, this justified the commission of the alleged crime by the defendant. In this regard, the Court of Appeal held thus: 'the fact that a person is a computer science graduate and uses a smartphone does not automatically invest him hacking skills.'[49]

It is our contention this is due to the absence of a regulatory body setting the necessary standards for forensic evidence. A regulatory body has the capacity of establishing what is best practice. Such a body could formulate a set of protocols to guide the collection, analysis and presentation of electronic evidence from the crime scene through to prosecution. Such a body could identify and establish essential criteria to assist agencies with the investigation of electronic evidence, and will allow investigators to be trained on how to handle digital evidence and the standard procedures to be followed while performing digital forensics. Training and retraining of all criminal investigators should be created, and prosecutors should be trained on how to manage electronic data. Moreover, document production can provide valuable advice that affects procedures and practices for electronic data or information management.

For instance, in *Federal Republic of Nigeria v Abdul*,[50] the defendant was charged with two-counts of being in possession of documents containing evidence of crimes. A group of EFCC operatives arrested the defendant in a cybercafé in Benin City, based on a petition written to the EFCC by the complainant who

[46] LPELR-CA/L/124/2006 at 38.
[47] (2018) LPELR-45541(CA).
[48] (2019) LPELR- 47872(CA), 1-29.
[49] 2019) LPELR- 47872(CA), 12-14.
[50] (2007) 5 EFCLR 204 at 228.

alleged the perpetration of internet crimes at the cybercafé. Following a search carried out on the defendant and other customers, a handwritten letter and a diary containing several e-mail addresses were recovered from the defendant. On further investigation by the EFCC operatives, e-mails that appeared to demonstrate the accused intended to commit a crime were discovered in the e-mail box of the defendant and were consequently printed. During the trial, the recovered handwritten letter, diary, and printouts were tendered as exhibits by the prosecution. In determining the guilt or otherwise of the defendant, the court examined whether emails not physically in possession of the defendant, that is, found in email only, could be said to be in possession of the defendant. Idahosa J, while discharging and acquitting the defendant in the absence of a forensic expert witness and forensic examination evidence held thus:

> 'The phenomenon of the e-mail box is a new technology. Evidence about how the phenomenon works must be laid before the Court, by a witness who may be regarded as an expert. The Prosecution did not call the said Olaolu Adegbite to tell the Court how he managed to do what PW3 said he did. It must be understood that the Court is not entitled to employ its own knowledge of this new technology, to complete the case of the Prosecution. The problem is that with this new technology, the traditional definitions of possession… seems inadequate, to describe a situation where there are electronic mail boxes, with documents in them floating, about in space. There is a need to explain this to the Court vide an expert witness. This would enable the Court to determine whether or not the fact of a document floating about in space in the mail box of the accused was in his possession.'[51]

Evidence to the effect that the defendant is the holder of the user name and password of the electronic mail box, in the absence of fraudulent use of the username, would have been sufficient.[52] Identifying the accused as the author of the e-mail through evidence would have been enough to assuage the court. Calix, Connors, Levy, Manzar, McCabe, and Wescott note the use of 'stylometry in the identification pertaining to the authorship of e-mail text messages.'[53] They stated that this could be determined through data collection, feature extraction and classification. Thus 'the program was used to analyse, linguistically and stylistically, e-mails by identifying the commonality of symbols, word frequencies and punctuation marks.'[54] However, in a novel approach by Igbal, Hadjidj, Fung, and Debbabi, write-prints could be of help in determining that the accused or defendant actually wrote the e-mail.[55] They note that it is

> 'an innovative data mining method to capture the write-print of every suspect and model it as combinations features that occurred frequently in the suspect's e-mails. This notion is called frequent pattern, which has proven to be effective in many data mining applications, but it is the first time to be applied to the problem of authorship attribution.'[56]

A three-phased methodology is deployed, (1) to identify the write-print of each suspect or accused, (2) to determine the author of the malicious e-mail or subject of criminal intent, and (3) to extract evidence for supporting the conclusion on authorship.[57]

[51] (2007) 5 EFCLR 204 at 226.

[52] See generally *Electronic Evidence*, chapter 7 – Authenticating electronic evidence.

[53] K. Calix, M.Connors, D. Levy, H. Manzar, G. McCabe, and S. Wescott (2008). Stylometry for E-mail Author Identification and Authentication, *Proceedings of CSIS Research Day, Pace University*. Available at http://csis.pace.edu/~ctappert/srd2008/c2.pdf.

[54] Stylometry for E-mail Author Identification and Authentication, at 6 (para. 5 - Conclusion).

[55] F. Igbal, R. Hadjidj, B.C.M. Fund, M. Debbabi (2008). A novel approach of mining write-prints for authorship attribution in e-mail forensics. *Digital Investigation* 5, 42-51. Note: This leads to a different academic debate on the accuracy of such methods and how easy they are to forge.

[56] A novel approach of mining write-prints for authorship attribution in e-mail forensics, 42.

[57] The court could have considered the decision of the Court of Appeal in *R v Mawji (Rizwan)* [2003] EWCA Crim 3067, [2003] All ER (D) 285 (Oct), discussed in *Electronic Evidence* at 7.54-7.55.

Lessons from other jurisdictions

In the US, the American Academy of Forensic Science (AAFS)[58] established the Academy Standard Board (ASB)[59] dedicated to developing documentary standards for forensics and regulation of the profession. The American Board of Criminalistics (ABC)[60] is a certification board that establishes a professionally acceptable level of knowledge, skills, and abilities for the practice of forensics science and sciences of criminalistics. The High Technology Crime Investigation Association (HTCIA)[61] is a non-profit professional international organization charged with the responsibility of prevention, investigation, and prosecution of crimes involving advanced technologies. This association provides law enforcement personnel, investigators, technicians and prosecuting attorneys the opportunity to share knowledge and ideas about methods and processes of investigating crimes in which computer and other advanced technologies are utilized.

Also in the U.S, the Office of Law Enforcement Standards (OLES), the National Institute of Justice (NIJ) and The National Cybercrime Training Partnership (NCTP) joined forces in May 1998 to formulate a set of protocols to guide the process of electronic evidence from the crime scene through to prosecution.[62] With these standards in place, arguably, when a U.S investigator produces a report, the report should not conflict with that of other investigators because they are all guided by the same standards. The collaboration of OLES, NIJ, and NCTP led to the Technical Working Group for Electronic Crime Scene Investigation (TWGECSI), charged with the responsibility to identify and establish basic criteria to assist agencies with electronic investigation and prosecution. NIJ train prosecutors and investigators on how to handle digital evidence and the standard procedures to be followed while performing digital forensics.[63]

The British Standards Institute (BSI) in the UK produced BS10008, titled, 'Evidential weight and legal admissibility of electronic information – Specification'. The standard relates to the production of electronic documents that may be required as evidence of business transactions and provides advice for practices and procedures involving information management systems. The Forensic Science Regulator has a code of practice that enforces the accreditation of digital forensic laboratories (ISO-17025) before it can render services to the criminal justice system.[64] The ISO-27037 is a global standard for digital forensics that promotes good practice, methods, and processes for forensic capturing and investigation of digital evidence.[65] In addition, the Draft Convention on Electronic Evidence[66] takes into account the juridical differences when considering electronic evidence, hence it seeks to promote international co-operation by pursing a common policy towards electronic evidence.[67]

Conclusion

The lack of effective and efficient application of digital forensics in criminal investigations in Nigeria is arguably attributable to the absence of a regulatory body, an acceptable model and standardized processes and procedures for adoption by various law enforcement agents in Nigeria. This has consequently affected criminal hearings, where different standards and models of digital forensics confuse criminal investigations and the presentation of conflicting forensic expert reports. Suggestions have been made for the adaptation of forensic practice and the establishment of a Nigerian regulatory body for the forensic industry to enhance the practice of digital

[58] https://www.aafs.org/.
[59] https://www.asbstandardsboard.org/.
[60] http://www.criminalistics.com/.
[61] https://htcia.org/.
[62] V. H. Sarah (2004). Forensic Examination of Digital Evidence: A Guide for Law Enforcement, available at https://www.ncjrs.gov/pdffiles1/nij/199408.pdf.
[63] E. G. Sean, C. D. Robert, and A. J. Brain (2018). Digital Evidence and the U.S. Criminal Justice System, available at https://www.rand.org/pubs/research_reports/RR890.html.
[64] Interforensics (2017). ISO-17025 mandatory for digital forensics in the criminal justice system. Available at https://www.intaforensics.com/2017/09/19/iso-17025-mandatory-for-digital-forensics-in-the-criminal-justice-system/.
[65] ISO27001Security (2017). Guideline for identification, collection, acquisition and preservation of digital evidence. https://www.iso27001security.com/html/27037.html.
[66] Draft Convention on Electronic Evidence, 13 *Digital Evidence and Electronic Signature Law Review*, (2016), S1-S11, available at https://journals.sas.ac.uk/deeslr/article/view/2321.
[67] See also the relevant chanters in the practitioner text *Electronic Evidence*.

forensics. Moreover, capacity building must be inculcated. It is necessary to conduct training and retraining of law enforcement agents and criminal prosecutors on standard procedures bordering on global best practices, together with the teaching of lawyers about the topic.[68]

Davidson C. Onwubiko is a Lecturer in the Department of Computer Science, Abia State University, Uturu. He is also a PhD candidate at Ebonyi State University, Abakaliki, Nigeria

chisom.onwubiko@abiastateuniversity.edu.ng

davidsononwubiko@gmail.com

Felix E. Eboibi, PhD (Law), LLM (Nig), LLB (Cal.), BL (Nigerian Law School) is a Senior Lecturer at the Faculty of Law, Niger Delta University, Wilberforce Island, Yenagoa, Nigeria

felixeboibi@mail.ndu.edu.ng

lixboibi@yahoo.com

[68] Denise H. Wong, 'Educating for the future: teaching evidence in the technological age,' 10 *Digital Evidence and Electronic Signature Law Review* (2013) 16 – 24; Deveral Capps, 'Fitting a quart into a pint pot: the legal curriculum and meeting the requirements of practice', 10 *Digital Evidence and Electronic Signature Law Review* (2013) 23 – 28, available at https://journals.sas.ac.uk/deeslr/issue/view/310.