DIGITAL EVIDENCE AND CROSS EXAMINATION OF EXPERT WITNESS

BY

OKAY BENEDICT AGU, LL.B (HONS) CALABAR,
(M.H.R.S, LL.M) LAGOS, (B.L), NIGERIA.

RESEARCH FELLOW/COORDINATOR, CENTRE FOR CASE LAW AND LITIGATION (CCL&L) NIALS

PAPER PRESENTED AT

THE 5TH INTERNATIONAL DIGITAL AND MOBILE FORENSICS CONFERENCE LAGOS

17TH – 19TH OCTOBER 2016

Goal of Discussion

To enhance the knowledge of those who testify in Court/Tribunal as Digital Forensic Experts on computer generated evidence issues in Cross -examination. This is to assist the court get to the truth and not to obscure it. And enable it do justice between parties in a matter.

Outline of Discussion

- Goal of Discussion
- Introduction
- Clarification of Terms
- Types of Digital Storage Media for Evidence (E-picture)
- Objects of Cross-Examination
- Scope of Cross-Examination
- Who May Cross-Examine the Expert
- Understanding the Expert's Tool
- Understanding Chain of Custody (CoC)
- Admissibility of Digital Forensic/Evidence Act 2011
- Admissibility/Evidence Act/ Cross – Examination
- Digital Forensic Report/Validation
- Digital Forensics/Admissibility/Int'l Best Practices
- Conclusion
- Appreciation

Introduction

- The emergence of information technologies for daily living makes it inevitable that these technologies make their way into the court room during trials/hearings as 'Digital Forensic' evidence. Law must keep pace with technological development. "The law cannot be and is not ignorant of modern business methods and must not shut its eyes to the mysteries of the computer". (*See, Esso West Africa Inc. v. T. Oyegbola ((1969) NMLR 194 at 198)*
- Digital Forensic is the preservation and the analysis of electronic data for use in the court. It entails the preservation, identification, extraction, interpretation and presentation of computer evidence .
- It is information and data of value to an investigation/court that is stored on, received or transmitted by electronic device.(*See, U.S National Institute of Justice NJC (2008)*

Clarification of Terms

- The word 'Digital' is defined as processing, storing, transmitting, representing or displaying data in the form of numerical digits, as in a computer. (See, *Microsoft Encarta Dictionary 2008)*
- 'Digital Evidence/Forensic' include the primary substantive data and the secondary data attached to the primary data such as data trails and time/date stamps. These data trails and other metadata markers are often the key to establishing a timeline and correlating important events (See, D.B Carie and J.D Morrissy; 'Digital Forensic Evidence in the Courtroom: Understanding Content and Quality' *12 Nw.J Tech & Intell. Prop. 121 (2014) 122*

  'Digital evidence' 'Electronic evidence or 'E-evidence' and 'Computer evidence' are used interchangeably
- 'Expert' A person who through education or experience , has developed skill or knowledge in a particular subject, so that he or she may form an opinion that will assist the fact finder/court/tribunal. (See,*B. A. Garner, 'Black's Law Dictionary'* (7th edn Westgroup, St. Paul, Minn., 1999) 600. See section 68(1) (2) Evidence Act 20911 *See also Azu v. State (1993) 6NWLR (Pt 229) 303; Shell Petroleum Co. Ltd v. Otoko (1990) 6 NWLR (Pt. 159) 693, See section 68 (1) (2) Evidence Act 2011*

Clarification Contd.

- 'Witness' One who sees, knows and vouches for something. One who gives testimony under oath or affirmation, in person, by oral or written deposition or by affidavit (*Ibid at 1596*)
- Expert Witness – *'An expert witness is a person who by a formal and organised training in his chosen profession has acquired a deep knowledge of the area he is called to give evidence. He is the master of the subject upon which he is called to give evidence… Being the master of the subject, the Judge, the layman or the novice and that he is generally and which the law so presumes normally expected to rely upon the expert. A trial judge will not generally throw overboard the evidence of an expert witness and substitute his own market place knowledge… for that of the expert just for the fun of it' Michael Alake v. The State (1991) 7 NWLR (Pt 205) 567 at 592 Per Tobi JCA at page 592*

Clarification Contd.

- Information technology devices that may come into court as digital evidence/forensic include, but may not be limited to: Internet/e-mail, portable electronics devices (cell phones, camera, Ipod, Ipad, Tablets) social media (Twitter, Face book, Whatsapp, Instagram, You tube videos) DVDs, CDs, Flash Disc, Zip disc, ATM Machines, Satellite Devices. Documents/data from Cloud computing.
- Digital Evidence/Forensic also include – PDAs, Music players, Wi-Fi, Bluetooth, Calculators, Car tracking devices, Geo-fencing devices, IBMS,GPS,CCTV and indeed any computer.

TYPES OF DIGITAL STORAGE MEDIA FOR EVIDENCE

Clarification Contd.

- 'Evidence' is something that gives a sign or proof of existence or truth of something or that helps somebody to come to a particular conclusion. (*Microsoft Encarta (ibid)*
- Computer is any electronic device that accepts, processes, stores and outputs data at a high speed according to programmed instruction. (*See, Microsoft Encarta Dictionary) (supra)*
- However, S. 258 Evidence Act 2011 defines Computer as **'Any device for storing and processing information, and any reference to information being derived from other information is a reference to its being derived from it by calculation comparison or any other process.'**
- 'Cross examination' The questioning of a witness at a trial or hearing by the party opposed to the party who called the witness to testify.

Objects of Cross Examination

- The law is that Counsel can deploy the devise of cross examination to weaken, qualify or destroy the case of the opponent, or to establish the party's own case by means of the opponent's witnesses. (*See Kuti v Alashe (2005) 17NWLR (pt. 955) 625, Ajao v Ajao (1986) NWLR 1*

Scope of Cross Examination

- Cross examination in many ways contributes to a qualitative system of Justice. It may provide the best opportunity to lose a case, just as the Examination in Chief may provide the best opportunity for Counsel to win a case.
- Counsel is allowed wide latitude to ask questions during cross examination.
- Such questions are not restricted to the issues raised by the witness during examination in chief. See section 215 (2) Evidence Act 2011
- Counsel may ask leading questions.
- Counsel may ask questions which tend to test the accuracy, veracity and credibility of the witness, or discover who the witness is and what is his station in life, or shake the witness' credibility by injuring his character. Section 223 (a) (b) (c) ibid

Scope of Cross - examination contns…

- Expect questions about your qualification/certification, CV.
- Lists of cases in which the expert has testified in the preceding years.
- Real world experience.
- Publications authored, Statement of Compensation for the digital forensic work and testimony in the case

Who May Cross-examine the Expert

- Depending on whose behalf the expert is testifying, The following categories of lawyers are noteworthy: law Officers – Ministry of Justice, Police Service, Intelligence Services, Anti Corruption Agencies, Private Law Practitioners/In-HouseCounsel/Opposing Counsel.

Understanding The Expert's Tool

- Digital Forensic experts use various tools
- Gain a good understanding of the use and work of these tools.
- For example, Evidor (Hard Drive Search Tool) will search for keyword such as people's names, e-mail addresses and names of traded good etc in the hard drive.
- Ontrack (File Recoverer) recovers file and file fragments that have been deleted and repairs such files as Word document or zipped files.
- Coroner's Toolkit - a collection of tools for examining UNIX system
- There are other tools that will sort and organise the contents of a disk to make it easier for the experts to find what they are looking for.
- Encase Software by Guidance System for imaging data

- Master these tools and don't be a Tool Tyke

- Any assumptions about the tools by the examiner, any limitations about the tools?

Understanding Chain of Custody (CoC) Issues

- CoC - legally refers to the chronological documentation or paper trail showing the seizure, custody, control, transfer, analysis and disposition of physical or electronic evidence.
- A person identifiable must have physical custody of a piece of digital evidence.
- The collection and every other process involved in handling the evidence before its tendering in the court should be documented in a chronological order to withstand the legal challenges about the authenticity/integrity of the evidence
- Documentation – conditions under which the evidence is gathered, the identity of all the evidence handlers and the manner the evidence is transferred to subsequent handlers/custodians.
- At each step/segment of the handling of the evidence, signatures of the persons involved must be identifiable.
- At the trial under cross-examination, it must be proved that the digital evidence tendered is the same as the one found at the scene of crime.
- Otherwise, CoC is broken and the evidence should be declared inadmissible.

Admissibility of Digital Forensic and Evidence Act 2011

- Relevancy – S. 1 EA 2011 provides: *'Evidence may be given in any suit or proceedings of the existence or non-existence of every fact in issue and of such other facts as are hereafter declared to be relevant, and of no other'* (see, *Ogu v. M.T & M. C. S Ltd (2011) 8NWLR (Pt. 1249) 345*
- S. 84 EA provides that: '*In any proceedings a statement contained in a document produced by a computer shall be admissible as evidence of any fact stated in it of which direct oral evidence would be admissible, if it is shown that the conditions in subsection(2) of this section are satisfied in relation to the statement and computer in question.*
- *(2) the conditions referred to in subsection (1) of this section are:*
- *(a) that the document containing the statement was produced by the computer during a period over which the computer was used regularly to store or process information for the purpose of any activities regularly carried on over that period,*

Admissibility; Evidence Act 2011, contns…

- *whether for profit or not, by anybody, whether corporate or not, or by any individual; (b) that over that period there was regularly supplied to the computer in the ordinary course of those activities information of the kind contained in the statement or of the kind from which the information so contained is derived; (c) that that throughout the material part of the period the computer was operating properly or, if not, that in any respect in which it was not operating properly or was out of operation during that part of that period was not such as to affect the production of the document or the accuracy of it contents; and (d) that the information contained in the statement reproduces or is derived from information supplied to the computer in the ordinary course of those activities.*

Admissibility; Evidence Act 2011, contns…

- *(3) Where over a period the function of storing or processing information for*
- *the purposes of any activities regularly carried on over that period as mentioned in*
- *subsection (2)) (a) of this section was regularly performed by computers, whether:*
- *(a) by a combination of computers operating over that period;*
- *or*
- *(b) by different computers operating in succession over that*
- *period; or (c) by different combinations of computers operating*
- *in succession over that period; or*
- *(d) in any other manner involving the successive operation over*
- *that period, in whatever order, of one or more computers and*
- *one or more combinations of computers, all the computers used*
- *for that purpose during that period shall be treated for the*
- *purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.*

Admissibility; Evidence Act 2011, contns…

- *(4) In any proceedings where it is desired to give a statement in evidence*
- *by virtue of this section, a certificate doing any of the following things, that*
- *is to say:*
- *(a) identifying the document containing the statement and*
- *describing the manner in which it was produced;*
- *(b) giving such particulars of any device involved in the production*
- *of that document as may be appropriate for the purpose of*
- *showing that the document was produced by a computer;*
- *(c) dealing with any of the matters to which the conditions*
- *mentioned in subsection (2) above relate, and purporting to be*
- *signed by a person occupying a responsible position in relation*
- *to the operation of the relevant device or the management of the*
- *relevant activities, as the case may be, shall be evidence of the*
- *matter stated in the certificate, and for the purpose of this*
- *subsection it shall be sufficient for a matter to be stated to the*
- *best of the knowledge and belief of the person stating it*

Admissibility; Evidence Act 2011, contns…

- For the purposes of this section—
- (a) information shall be taken to be supplied to a computer if it is supplied to it in any appropriate form and whether it is supplied directly or (with or
- without human intervention) by means of any appropriate equipment;
- (b) where, in the course of activities carried on by any individual or body,
- information is supplied with a view to its being stored or processed for the
- purposes of those activities by a computer operated otherwise than in the
- course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities; (c) a document shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

Admissibility/Evidence Act/Cross-examination

- S. 84 requires the laying of proper evidential foundation – (See, **Dr. Imoro Kubor &Anor v Hon. Seriake Henry Dickson & Ors** (2013) 4 NWLR (Pt.1345), 534

- Computer must be shown to be in **regular use** for storage or processing of information with regard to activity in question

- Computer should be **operating properly** or if temporarily out of service, that condition did not affect production and accuracy of content of computer

- Information tendered as evidence is **derived from** information supplied to computer
- Information stored or processed by single, combination or network of computers will be treated as information derived from a single computer
- Information may be supplied to computer directly or indirectly with or without human intervention

Admissibility/Cross-examination contns…

- Transferred or processed information moving from another computer (e.g handheld device) to the main storage computer is admissible so long as it is supplied in **appropriate** form (84(5)
- Information **produced** or **processed** with or without human intervention is admissible
- A certificate must be produced signed by a person **responsible** for management of the activities for which the computer is used Certificate must describe manner in which document was produced and provide **particulars of device** involved in its production;
- It is sufficient if certificate states that it is to the best knowledge and belief of person issuing it

Issues contns..

Other Issues –

Bit Stream/Hard drive/Forensic imaging. Be prepared to answer the question : 'Did you obey the golden rule of electronic evidence before your analysis of the subject computer?'

Hard drive hashing – be prepared to answer the question:'Did you generate a digital fingerprint of the particular media?

So make sure that the integrity of the evidence is maintained, CoC established and harsh values documented.

Digital Forensic Report (Validation of Report)

- Be prepared to explain the mechanism deployed to collect the digital evidence.
- Can an independent third party replicate the conclusion reached by the examiner? (Availability of forensic images)
- Report should not contain superfluous information or technical arcana or minutiae
- Facts discovered and opinion formed need be documented and referenced to the original source (any exhibits to support) (See, clark v. Taka Corp) Bases and reasons for the opinion. (Facts and data considered in forming the opinion)

International Best Practices

- Always link your findings to International best practice (See, Daubert v. Merrel Dow Pharmaceautical Inc.) standard (509 U.S. 579 (1993)
- whether the technique has been tested.
- 2. whether it has undergone peer review
- 3. whether there is no error rate
- 4. whether there is in existence maintenance standard controlling its operation or methodology
- 5 whether the technique is generally acceptable to the scientific community

Int'l Best Practices contns…… 'The Five As'

- Admissibility must guide all actions – document everything that is done
- Acquire the evidence without damaging the original
- Authenticate your copy to be certain it is identical to the source data
- Analyse the data while retaining its integrity
- Anticipate the unexpected
- Identify illegal activities with respect to 5 Ws (why, when, where, what and who)

Conclusion

- Recognise the limits of computer forensics
- Do not concede to the cross - examiner some of the things a digital forensic expert cannot ascertain how a particular computer was used or who used it.
- Do not over reach yourself in attempting to answer any question at cross-examination, or try to obscure the truth but uphold it.
- Recognise that the quality of an expert witness is in preparation, knowledge, experience, effective communication, integrity and demeanor.
- Always be prepared

Thank You

- THANK YOU FOR LISTENING
- Contact
  - 08033000753
- agubenedict@yahoo.com
- okaybenedictagu@gmail.com