APPLICATION OF ICT AND OTHER FORENSIC TOOLS IN INVESTIGATION AND PROSECUTIONS

BY

CHINWE NDUBEZE

AT

THE NJI NATIONAL WORKSHOP FOR INVESTIGATORS AND PROSECUTORS

ON

28TH AUGUST 2019

INTRODUCTION

- The onset of the "digital age," has led to increase in the number of computer users. A significant part of our lives can now be conducted on the internet like shopping, government business, dating, chatting etc.
- The growth of mobile communication and convergence of technologies has further impacting our daily reality. Gone are the days when you require a camera to take a picture, a computer to send emails, a board to play a game, a telephone to make a call as any of these activities can be performed by one smart device.
- Similarly, cyber criminals have also become smarter in the way they perform their sordid enterprise and digital crime has increased exponentially.

Turning The Tables

- As life is getting smarter, there is also the consequential need for investigations to become even smarter and this underscores the need for ICT and other forensic tools and expertise by law enforcement in the investigation and prosecution of cases.
- Computer forensics is now commonly used for different areas of criminal investigations.
- Computers have been widely known for being used in committing crimes but now the tables have turned and forensics has the edge.
- Instead of playing catch up to criminals, ICT and other forensic tools are currently used to expose criminals who believe they do not leave an imprint when committing certain crimes.

Forensic Investigation

- Forensic science generally relate to the scientific methods used to solve a crime. It involves the scientific analysis of physical evidence collected in the course of investigation for presentation to a court in the course of trial.
- **Forensic investigation** therefore is the gathering and analysis of all crime-related physical evidence such as documents, fingerprints, body fluid, computers, or other technology in order to come to a conclusion about a suspect or to establish how a crime took place.
- There are different types of forensic investigations such as forensic accounting/auditing, forensic archaeology, forensic dentistry, forensic entomology, forensic science, forensic toxicology, computer/cyber/digital forensic, etc.
- Our focus would be on computer/digital forensics.

Computer/Digital Forensics

- **Digital Forensics** is the science or process through which digital evidence on computer systems, media, and storage devices is identified, preserved, recovered, restored, and presented.
- Simply put, these processes investigate what happened on a system, when it happened, how it may have happened and steps to recover any losses or repair any damage that may have occurred as a result
- By virtue of **Section 58** of the Cybercrime Act, 2015, a computer is defined to include any device with data processing capabilities including, but not limited to, computers and mobile phones, computer data storage devices etc.

- Computer/digital forensics is the new frontier of criminal investigation.
- Computer forensics is widely known for discovering criminals in various types of fraud. However, investigators are now using computer forensics to detect murderers, and access encrypted data daily that will stand as evidence in a court of law.
- Therefore modern day investigation employ forensic experts in order to help identify criminals and analyze evidence against them.

Role of The Computer Forensic Expert

- Computer forensic is a rapidly growing discipline with its own area of scientific expertise, with accompanying training and certifications such as:
- CCFE- Certified Computer Forensics Examiner
- CHFI – Certified Hacking Forensics Examiner who is trained in detecting hacking attacks and properly extracting evidence to report the crime and conduct audits to prevent future attacks.
- A computer forensic expect is responsible for the identification, collection, acquisition, authentication, preservation, examination, analysis, and presentation of evidence for prosecution purposes.

Benefit of Forensic Investigation

- Forensic investigation tools can be used to:
- Recover deleted files, deleted passwords, encrypted data or data hidden in the folds of mobile devices technology, etc;
- Check for breaches of security for cyber-crime.
- Extract crucial data from electronic devices belonging to the affected parties.
- Verify offenders' alibis, examination of Internet abuse, misuse of computing resources and network usage in making computer-related threats etc. For instance, the BTK Killer was caught and evidence was used in his court trial from computer forensics discovered in a search of his home.

- Re-open and solve cold case files because as technology grows so do the ways to collect information from old hard drives to solve crimes that have gone unsolved for years. The simple gathering and organization of old forensics from unsolved cases have brought forward details that investigators might have missed in initial investigations. These innovations are helping to change the face of the criminal investigation.
- Explore the cyber-trail left by the offender.
- Enhance the quality of prosecution.
- Clearly, digital forensics is needed to assist for law enforcement in retrieving information that can be used as evidence in this digital age.

Sources of Computer Forensic Evidence

- Text Messages
- Internet History
- Emails
- Social media
- Files and Images.

3 A's of Computer Forensics Process

- The three important steps in computer forensics are:
- Acquire - Collection stage through search and seizure of digital evidence and any other means of acquiring data.
- Authenticate - Examination of acquired devices and data and applying techniques to identify and extract data.
- Analyze - using data and resources to prove a case.
- Reporting is then necessary to present the information gathered (e.g., written case report).

Keys To Success

- Surveillance - audio recording, videotaping, internet content filters, and access logs so as to accurately identify all target devices. A failure to capture all the devices of interest can virtually guarantee that tampering will occur.
- Surprise - Catching a target off guard before they can alter, delete, or steal the data.
- Speed – leave no opportunity for a subject to launch a destructive attack on data and ensure that the data on the target devices be **imaged** immediately after securing the drive.
- Security – proper handling to preserve admissible evidence and rebut any claims of contamination or improper handling- breaking the chain of custody allows argument that the evidence is tainted.

Legal Basis For Digital Forensic Investigation

- Lawful Interception **section 39** of the Cybercrime Act states:
- Where there are reasonable grounds to suspect that the content of any electronic communication is reasonably required for the purposes of a criminal investigation or proceedings, a Judge may on the basis of information on oath;
- (a) order a service provider, through the application of technical means to intercept, collect, record, permit or assist competent authorities with the collection or recording of content data and/or traffic data associated with specified communications transmitted by means of a computer system; or
- (b) authorize a law enforcement officer to collect or record such data through application of technical means.

- Section 40 -(1) stipulâtes That:
- It shall be the duty of every service provider in Nigeria to comply with all the provisions of this Act and disclose information requested by any law enforcement agency or otherwise render assistance howsoever in any inquiry or proceeding under this Act.
- (2) Without prejudice to the generality of the foregoing, a service provider shall, at the request of any law enforcement agency in Nigeria or at its own initiative, provide assistance towards –
- (a) the identification, apprehension and prosecution of offenders;
- (b) the identification, tracking and tracing of proceeds of any offence or any property, equipment or device used in the commission of any offence; or

- the freezing, removal, erasure or cancellation of the services of the offender which enables the offender to either commit the offence, hide or preserve the proceeds of any offence or any property, equipment or device used in the commission of the offence.
- (3) Any service provider who contravenes the provisions of subsection (1) and (2) of this section, commits an offence and shall be liable on conviction to a fine of not more than ₦10,000,000.00.
- (4) In addition to the punishment prescribed under subsection (3) of this section and subject to the provisions of section 20 of this Act, each director, manager or officer of the service provider shall be liable on conviction to imprisonment for a term of not more than 3 years or a fine of not more than ₦7,000,000.00 or to both such fine and imprisonment.

Some Tools in Digital Forensics

- Digital Forensics tools include: Email Analysis tools; Internet analysis tools; Data Recovery Tools; Network scanner. Examples are:
- **ComputerCOP**
- ComputerCOP is a software that monitors and controls the content traffic in a system. It has the ability to scan and analyze content on a computer for objectionable or unacceptable traffic on that system. All data is scanned: files, images, browsing history, and videos. It possesses a key logging component which is extremely useful in monitoring web traffic. Parents can monitor their children's computer activity, receive notifications when internet traffic by their children contains certain words using computerCOP . It is an internet traffic policeman.

- **Digital Detective**
- It is a suite of products designed and geared towards addressing all aspects of digital forensics.
- It has a network analysis tool that efficiently facilitates the extraction, analysis, and presentation of the system's network protocols, traffic, and user activities. It handles web browser forensics, enables network filtering and searching, and facilitates cache exports and web page building. It also offers a forensic data recovery solution. This includes a fast and accurate advanced built-in validation and interpretation routine that enables absolute data recovery. The suite of tools is coupled with sound reporting systems.

- DFF – Digital Forensic Framework- is an Open Source computer forensics platform built on top of a dedicated Application Programming Interface (API). DFF proposes an alternative to the aging digital forensics solutions used today. Designed for simple use and automation, DFF interface guides the user through the main steps of a digital investigation so it can be used by both professional and non-expert to quickly and easily conduct a digital investigation and perform incident response.
- Others include: Open Computer Forensic Architecture; Caine; X-ways Forensics; EnCase; Registry Recon; The Sleuth Kit; LlibForensics; Volatility; WindowScope etc.

CONCLUSION

- The digital age is now upon us and we need to embrace the challenges and benefits that come with it.
- We really cannot afford to be analogue in the digital age. A situation where criminals are steps ahead of law enforcement is most undesirable.
- It is a welcome development that the tables have finally turned in favour of law enforcement , whereby offenders have no option than to plead guilty because of the undisputable and overwhelming evidence against them. Obtained through ICT and other forensic tools.
- These tools are available and we must up our game to effectively detect, fight, investigate and prosecute crimes in our society.
- **THANK YOU FOR YOUR TIME**