TRAINING PROGRAM FOR JUDICIAL OFFICERS OF ZIMBABWE. JAN 2020

BY HON. JUSTICE LAWRENCE GIDUDU, High Court of Uganda. lgidudu8@gmail.com

ADMISIBILITY OF DIGITAL EVIDENCE

- EVIDENCE IS THE BASIS UPON WHICH FACTS OR ISSUES ARE PROVED OR DISPROVED IN COURT.
- COURTS RELY ON EVIDENCE TO DECIDE CASES ONE WAY OR THE OTHER.
- ADMISSIBILITY OF EVIDENCE DEPENDS ON ITS RELEVANCY TO THE ISSUES IN COURT. S 252 Criminal Procedure and Evidence Act. Cap 9:07

BACKGROUND

- **ADVANCEMENT IN TECHNOLOGY: Has led to the use of digital devices such as mobile phones, computers and tablets which have become indispensable in modern society. Communication of this nature has led to migration from physical to digital data**

BACKGROUND

- **MIGRATION FROM ANALOGUE TO DIGITAL PLATFORMS HAS REVOLUTIONALISED TRANSACTIONS IN THE WORLD. (Second Industrial revolution- The Internet and computer networks)**
- **E-Governments, E-Commerce, E-Banking, E-Photography/Photoshop, E-recording, E-passports, E-transport, E-security**
- **The good life that comes with technology has also bred criminals who take advantage of the speed which is awesome and the results which are mind boggling.**

CYBER CRIMES

- **HACKING, MALWARE, INTERNET FRAUD- embezzlement, theft, bribery, cheating-Corruption**
- **TECHNOLOGY HAS ALSO FACILITATED TRADITIONAL CRIMES SUCH MUDER, DRUG TRAFFICKING, HUMAN TRAFFICKING, MONEY LAUNDERING AND TERRORISM**

DIGITAL FORENSICS

- **COURTS MUST EMBRACE DIGITAL TECHNOLOGY AND RESPOND APPROPRIATELY TO TECHNICAL CHANGES TAKING PLACE IN CYBER SPACE.**
- **REPOSITORIES OF DIGITAL EVIDENCE:- Computers, storage devices, telephone, networks(servers), cloud servers and e-mails. Judges must know this**

DIGITAL EVIDENCE

- Digital evidence or electronic evidence is any probative information stored or transmitted in digital form
- It is data which is recorded or stored in any medium in or by a computer or other similar device

DIGITAL EVIDENCE

- **It should be read or perceived by a person or computer system or other similar device and includes a display, print out or other output of that data.**
- **It includes text images, sounds, codes, computer programs, soft ware and data bases**

DIGITAL FORENSICS

- **Techniques used to collect, validate, identify, analyse, interpret, document and present digital evidence.**
- **Admissibility of digital evidence depends on the credibility and authenticity of the above processes.**

DIGITAL FORENSICS

- **Techniques used to collect, validate, identify, analyse, interpret, document and present digital evidence.**
- **Admissibility of digital evidence depends on the credibility and authenticity of the above processes.**

DIGITAL FORENSIC EVIDENCE

- IDENTIFY *DIGITAL EVIDENCE*
- PRESERVE *DIGITAL EVIDENCE*
- COLLECT *DIGITAL EVIDENCE*
- ANALYSE *DIGITAL EVIDENCE*
- PRESENT *DIGITAL EVIDENCE*
- **LOCATE-SECURE-ANALYSE-PRESENT**.

ADIMISSIBILITY

- RULES OF EVIDENCE SHALL NOT BE APPLIED SO AS TO DENY ADMISSIBILITY OF A DATA MESSAGE OR ELECTRONIC MESSAGE(Computer Misuse Act and Electronic transactions Act of Uganda)
- IT IS ADMISSIBLE IF THAT THE BEST EVIDENCE THE PERSON ADDUCING COULD REASONABBLY BE EXPECTED TO OBTAIN
- IT IS ADMISSIBLE EVEN IF IT IS NOT THE ORIGINAL

COMPUTER CRIME AND CYBER CRIME BILL(ACT?)ZIMBABWE

- S.28(1) In any criminal proceedings under this Act the rules of evidence shall apply in so far as the admissibility of evidence generated from a computer system or information system in permissible under the laws of Zimbabwe
- (2) Evidence in electronic form shall be given evidential weight if:-
- (3) it is reliable in the manner it was generated, stored or communicated;

COMPUTER CRIME AND CYBER CRIME BILL(ACT?)ZIMBABWE

- The reliability of the manner in which the integrity of the data or data massage was maintained;
- The manner in which the originator or recipient of the data or data massage was identified and any other relevant factors.

CONDITIONS FOR ADIMISSION

- **AUTHENTICITY:**
- **The capacity to prove that the digital object is what it purports to be. Techniques should be applied to prevent the data from being manipulated, altered or falsified deliberately or inadvertently.**
- **Changes may occur by merely turning on a computer.**

CONDITIONS

- INTEGRITY
- How sound is the data? It should not be changed from say PDF to WORD
- Provide an audit trail
- Record of the process of recovery of data. Eg video recording, screen shots
- Evidence that the computer System was operating properly

CONDITIONS

- RELIABILITY
- Capacity of a digital object to stand for the facts to which it purports to be.
- It should be incapable of unauthorized alterations
- The presenter must demonstrate a degree of control against alteration
- Competency of a witness is important

GOOD PRACTICE GUIDE FRO DIGITAL EVIDENCE- 2012

- **PRINCIPLE 1: No action taken by Law Enforcement Agencies, person employed within those Agencies or their agents should change data which may subsequently be relied upon in court**
- **DO NOT MODIFY DATA/ EVIDENCE**
- **See Sec 7 of Computer Misuse Act, 2011**

GOOD PRACTICES

- **PRINCIPLE 2**
- **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 relevancy of the implications of their actions.**
- **BE COMPETENT TO EXPLAIN**

GOOD PRACTICES

- **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.**
- **DOCUMENT EVERYTHING**

GOOD PRACTICES

- **PRINCIPLE 4.**
- **The person in charge of the investigation has the overall responsibility for ensuring that the law and these principles are adhered to.**
- **FOLLOW THE LAW**

DIGITAL FORENSIC HANDLING

- **AUDIBILITY: Investigators should record all actions in the audit trail to ensure that an independent assessor for the interested party gets the same result.**
- **JUSTIFIABILITY: Investigators should justify the method used as the most effective in getting the data**

DIGITAL FORENSIC HANDLING

- **REPEATABILITY: It should be possible for an independent assessor to repeat or reproduce the tasks in the audit trial.**
- **REPRODUCIBILITY: It may be necessary to obtain the same results in a different testing environment.**

DIGITAL EVIDENCE

- **BEAUTY OF DIGITAL FORENSIC EVIDENCE IS THAT IT SPEAKS FOR ITSELF- species of circumstantial evidence**
- **IT IS A SMARTER WAY OF ESTABLISHING A CRIME AND IDENTFYING AN ACCUSED.**
- **IT IS BETTER THAN EYE WITNESSES WHO MAY BE HONEST BUT MISTAKEN**
- **IT IS CAPABLE OF PROVING A CASE WITH THE EXACTNESS OF MATHMATICS.**

CHALLENGES

- LAY INVESTIGATORS OPERATING IN A DIGITAL ENVIRONMENT
- STORAGE. DIGITAL DEVICES HAVE DIFFERENT OPERATING SYSTEMS
- EXPENSIVE EQUIPMENT TO USE IN TRACING HIDDEN OR ERASED DATA(FTK, EN-Case)
- VIRTUAL STORAGE LIKE CLOUD AND USE OF VIRTUAL PRIVATE NETWORKS (VPN)
- VOLATILITY OF E-DATA. NEED TO USE PROFESSIONALS WITH APPRPRIATE TOOLS
- LIMITED KNOWLEDGE OF IT BY LAWYERS

GIDUDU LAWRENCE
+256 772 502629