ZICTA

Digital Forensics Guidelines

Table of Contents

1. INTRODUCTION

The Zambia Information and Communications Technology Authority (Authority) is provided for under section 4 of the Information and Communication Technologies Act No. 15 of 2009 (ICT Act). The Authority is mandated to regulate Cyber Security in the Republic. Section 5 (o) of the Cyber Security and Cyber Crimes Act No. 2 of 2021 further mandates the Authority to issue guidelines relating to digital forensics. Additionally, section 88 (2) of the Cyber Security and Cyber Crimes Act empowers the Authority to issue guidelines for the better carrying out of its mandate. Pursuant to the mandate referred to above, the Authority issues these guidelines.

2. STATUS OF GUIDELINES

These guidelines shall be read as one with the Cyber Security and Cyber Crimes Act, any Regulations issued under this Act, license terms and conditions and any other relevant laws.

3. DEFINITIONS

In these Guidelines, unless the context otherwise requires –

Contamination	Means compromising the integrity of the data or device subject to an investigation during the digital forensic process;
Cyber Inspector	has the meaning assigned to the word in the Cyber Security and Cyber Crimes Act No. 2 of 2021;
Device	has the meaning assigned to the word in the Cyber Security and Cyber Crimes Act No. 2 of 2021;
Digital forensic imaging	means the process of creating a bit by bit copy or clone of a physical storage media for the purpose of conducting investigations and gathering evidence;
Extraction	means obtaining data from an electronic device which include physical, logical and file system;
Faraday Bag	means an enclosure that blocks electromagnetic fields and signals;

Forensic tools	means hardware or software applications that are used to extract, preserve, identify and document digital evidence; and
Law enforcement agency	means a) Zambia police service b) The Anti Corruption Commission c) The Zambia Security Intelligence Service d) Drug enforcement Commission
Licensee	a person licensed to provide digital forensics services.

4. APPLICATION

4.1. These guidelines shall apply to law enforcement agencies and any person conducting digital forensics in the Republic.

4.2. A law enforcement officer or any person may conduct the following types of digital forensics, among others:

a) mobile forensics;
b) computer forensics;
c) network forensics;
d) live forensics; and
e) database forensics.

5. PRINCIPLES OF DIGITAL FORENSICS

The following are the guiding principles of digital forensics:

5.1. PRINCIPLE 1

a) A law enforcement officer or any person shall, prior to conducting digital forensics, ensure that there is –
   i. a course of action;
   ii. a search warrant;
   iii. an affidavit;
   iv. a request letter; or
   v. any other relevant documentation as the Authority may determine.

5.2. PRINCIPLE 2

a) The law enforcement officer or any person conducting digital forensics shall adhere to the applicable laws and policies of the matter under investigation.

5.3. PRINCIPLE 3

a) The law enforcement officer or any person conducting digital forensics shall take reasonable effort to identify all sources of potential evidence relevant to the investigation. In conducting an investigation, a law enforcement officer or any person shall take into consideration the scope of the investigation regarding any interrogation of the data or the device subject to an investigation.

5.4. PRINCIPLE 4

a) A law enforcement officer or any person conducting digital forensics shall ensure that all reasonable measures are taken to prevent or limit contamination of the data or the device subject to an investigation.

b) These measures may include –

   i. imaging;

   ii. the use of tools and technology that prevent data alteration; or

   iii. any other relevant measures.

c) Where the data or the device subject to an investigation is contaminated, the law enforcement officer or any person shall document the events that led to the contamination and the changes to the data or device subject to the investigation.

5.5. PRINCIPLE 5

a) A law enforcement officer or any person conducting digital forensics shall only access digital data targeted by their investigation using a suitable method that is compliant with principles 3 and 4.

5.6. PRINCIPLE 6

a) A law enforcement officer or any person conducting digital forensics shall take reasonable measures to preserve the integrity of any data or device subject to an investigation.

5.7. PRINCIPLE 7

a) A law enforcement officer or any person conducting digital forensics shall ensure that all extracted and interpreted data has undergone robust testing and validation using accepted testing methods in order to verify its accuracy.

b) The testing methods shall include –

   i. peer review;

   ii. use of alternative tools; or

   iii. hash values.

5.8. PRINCIPLE 8

a) A law enforcement officer or any person conducting digital forensics shall document all the stages of the investigation, forming an audit trail which can be used to describe the processes implemented during that investigation. Where necessary, these procedures may be repeated by a third party in order to obtain comparable results.

6. PROCEDURE FOR DIGITAL FORENSICS

The following procedure shall be used when conducting digital forensics:

6.1 Preliminary Assessment

a) A law enforcement officer or any person conducting digital forensics shall analyse the data or a device subject to investigation in order to determine the scope and the course of action.

b) In analysing the data or device subject to an investigation, a law enforcement officer or any person conducting digital forensics shall assess the data or the device by –

   i. identifying the source of the request;

   ii. reviewing the case details in any written correspondence that clearly outlines the matter being examined;

   iii. considering the possibility of pursuing other investigative avenues to obtain additional information or data that may be relevant to the investigation including identifying remote storage locations;

   iv. reviewing chain of custody;

v. reviewing search warrant;
vi. reviewing any other legal authorisation;
vii. determining the physical state of the hardware;
viii. determining the operational status of the device;
ix. identifying the information or data sought;
x. storing the data or device subject to an investigation in a secure environment;
xi. investigating other sources of information such as internet related data or information, and servers located outside the Republic; and
xii. conducting any other relevant activities for purposes of the preliminary assessment.

6.2 Acquisition

a) A law enforcement officer or any person conducting digital forensics shall take the measures provided in clause 6.2 to preserve the data or device subject to an investigation in order to prevent it from being altered, damaged or destroyed. Failure to do so may lead to an inaccurate conclusion.

b) The following measures shall apply during acquisition:

i. verify and document the hardware and software configurations such as the system date, time, operating system for the system that will be used to conduct digital forensics prior to using it for digital forensics;
ii. obtain access to the storage media of the device subject to an investigation while ensuring that the device is protected from static electricity, magnetic fields and any other potential source of damage or disruption;
iii. ensure that the examiner's storage device is forensically clean before utilising it as a target storage media during acquisition;
iv. ensure that a digital forensic image of the storage media of the device subject to an investigation is created using specialised digital forensics imaging tools to produce an identical copy or image of the original data;
v. ensure the use of technologies such as software and hardware write-blockers, that prevent data alteration during digital forensic imaging to preserve and protect the original data;

vi. employ the use of validation or integrity monitoring mechanisms such as hashing on the digital forensic image created;

vii. retrieve system configuration information from the image created of the device that is subject to investigation; and

viii. any other measures that may be used to preserve data.

6.3 Examination

6.3.1 A law enforcement officer or any person conducting digital forensics shall, in examining the data or device subject to an investigation –

a) extract and conduct analysis of data or information from the image or copies of the data. For purposes of this clause 7, analysis refers to the interpretation of the recovered data and presentation of the data in a logical and useful format.

b) undertake the following:

i. prepare a working directory on separate storage media to which evidentiary files and data can be recovered or extracted;

ii. extract the information or data that is subject to the investigation using forensic methods and tools;

iii. conduct analysis of the extracted data;

iv. conduct examination using alternative methods or tools where the results obtained are inconclusive;

v. review the examination process by considering the results of the extraction and analysis in their entirety; and

vi. employ the use of integrity monitoring mechanisms such as hashing on the image or copies of the data after concluding the examination.

6.3.2 The following and any other extraction methods shall be utilized during examination;

i. physical extraction;

ii. logical extraction;

iii. file system extraction; and

iv. any other method of extraction.

6.4 Documenting

A law enforcement officer or any person conducting digital forensics shall in documenting -

a) record all processes undertaken and observations made;
b) ensure that the documentation is complete, accurate, and comprehensive; and
c) Undertake the following:
    i. take notes when consulting and during the digital forensic process. The notes should include relevant dates, times, descriptions and results of processes undertaken;
    ii. maintain a copy of the correspondence that clearly outlines the matter being examined; and
    iii. maintain a copy of chain of custody documentation.

6.5 Reporting

A law enforcement officer or any person conducting digital forensics shall -

a) produce a report following the digital forensics process that will include-
    i. the identity of the source of the request for digital forensics and date of receipt of the request;
    ii. unique case identifier or submission number;
    iii. scope of the investigation;
    iv. description and clear photographs of items submitted for digital forensics;
    v. brief description of all the steps taken during examination;
    vi. the identity and signature of the law enforcement officer or person that conducted digital forensics;
    vii. technologies and tools used during the examination;
    viii. findings;
    ix. conclusion;
    x. date of report handover; and
    xi. any other relevant information.
b) handover the report and all devices subject to an investigation; and

c) ensure that the chain of custody is completed upon handover of the digital forensics report and devices.

7 HANDLING OF DIGITAL EVIDENCE AT A CRIME SCENE

7.1 A law enforcement officer or any person appointed to conduct digital forensics under the Cyber Crimes and Cyber Security Act or any other relevant law shall, before collecting evidence at a crime scene –

a) obtain a search warrant;

b) ensure that appropriate personal protective equipment is used; and

c) where necessary, obtain the following information:

i. names of all users of the computers and devices;

ii. all computer and Internet user information;

iii. all login names and user account names;

iv. purpose and use of computers and devices;

v. all passwords;

vi. any automated applications in use;

vii. type of Internet access;

viii. any offsite storage;

ix. internet service provider;

x. installed software documentation;

xi. all e-mail accounts;

xii. security provisions in use;

xiii. web mail account information;

xiv. data access restrictions in place;

xv. all instant message screen names;

xvi. all destructive devices or software in use; and

xvii. any other relevant information.

7.2 A law enforcement officer or any person appointed to conduct digital forensics shall, among others –

a) recognize, identify, seize and secure all devices at the scene;

b) document the entire scene and the specific location of the evidence found;

c) collect, label and preserve the digital evidence; and

d) package and transport digital evidence in a secure manner.

7.3 A law enforcement officer or any person appointed to conduct digital forensics shall conduct digital forensics on the following devices among others –

a) all system units and laptop computers;

b) hard disks which may or may not be fitted inside a computer;

c) external drives;

d) mobile phones;

e) smart devices such as smart watches;

f) drones;

g) digital tapes;

h) Compact Discs (CD);

i) Digital Video Discs (DVD);

j) modems;

k) routers;

l) digital cameras and associated storage media; and

m) gaming devices.

7.4 A law enforcement officer or any person appointed to conduct digital forensics shall, when conducting digital forensics on the above mentioned devices or any other device for the purposes of digital forensics, take into account the following –

a) secure and take control of the area containing the equipment;

b) move people away from any device that is the subject to an investigation and power supplies of the device;

c) where necessary, the device that is subject to an investigation should not be powered on or interacted with;

d) where the device is a printer, it should be allowed to complete the running printing job;

e) photograph or take a video footage of all the components on site or draw a sketch plan on paper;

f) where necessary, unplug the power from the power connector unit of the device that is subject to an investigation;

g) where necessary, remove all cables connected to the device that is subject to an investigation;

h) where the device is a laptop computer, remove the battery from the laptop;

i) when seizing a device, it may be necessary to seize cables and connectors associated to the device;

j) label all seized devices, place them in the appropriate evidence bags and document chain of custody;

k) where a device is found to be operating with data displayed on a monitor or screen, the contents of the screen shall, where necessary, be recorded by photograph, video or documenting the content of the screen; and

l) where the device is a mobile device-

   i. attempts should be made to block incoming and outgoing signals to the mobile device by using measures such as placing the mobile device in a faraday bag, changing the mobile device settings to flight mode or switching off the device; and

   ii. undertake an examination of any external components associated to the device subject to an investigation.

8 HANDLING OF DEVICE BY LICENSEE

A licensee conducting digital forensics shall, among others –

a) recognize, identify and secure all devices;

b) document the chain of custody;

c) collect, label and preserve the device subject to investigation or evidence; and

d) package and transport device subject to investigation in a secure manner.

9 EXEMPTION

Where there is an emergency, a law enforcement officer or a person conducting digital forensics may conduct manual examination on the device that is the subject of an investigation.

For purposes of this clause, an emergency includes threat to life, damage to property or financial loss.

10 HANDLING OF DEVICE SUBJECT TO AN INVESTIGATION

A law enforcement officer or a person conducting digital forensics shall keep, store and transport the device that is the subject of an investigation in a manner that will protect the device from magnetic sources, extremes of humidity, liquids, heat, loud sound, radio frequency and any other possible source of damage or disruption.

11 DIGITAL FORENSICS ON DEVICES CONTAINING INDECENT CONTENT OF CHILDREN

11.1 A person conducting digital forensics shall, when dealing with indecent content of a child on a device subject to an investigation, limit access to the indecent content and report the matter to the relevant law enforcement agency.

11.2 A law enforcement officer shall, when dealing with indecent content of a child on a device subject to an investigation, limit access to the indecent content.

12 CHAIN OF CUSTODY

A law enforcement officer or any person shall complete the chain of custody form set out in the Schedule for each device that is subject to an investigation, prior to conducting digital forensics.

13 QUALIFICATION OF PERSON CONDUCTING DIGITAL FORENSICS

A person shall not conduct digital forensics if that person is not licensed by the Authority or appointed under any relevant law.

14 SUBMISSION OF MANUAL FOR APPROVAL

A law enforcement officer or a person conducting digital forensics shall within ninety (90) days of the publication of these guidelines, submit to the Authority a manual on digital forensics.

15 AUDIT

The Authority shall audit law enforcement agencies and persons conducting digital forensics from time to time to ensure compliance.

SCHEDULE
(Clause 15)

Case/Request Reference Number:

DIGITAL EVIDENCE CHAIN OF CUSTODY FORM

Investigating Agency: _____

Station/Section/Unit/Dept: _____

Evidence Collected By: _____

Type of Offence: _____

The item(s) described below were obtained as evidence from the undersigned during an official investigation.

Device Type:	Model No :	Serial No :
Manufacturer:	Other: (Colour, Memory Storage Size, Condition, Accessories etc)	
Password/Pattern Lock (if any)		

FORENSIC BAG SERIAL NO. :

OBTAINED FROM:

Full Name: _____

Location of Collection:_____

Date of Collection: _____

Time of Collection:_____

☐ I, _____the undersigned, do hereby acknowledge ownership of the artifacts that were obtained from my possession.

Suspect Signatrue:_____

☐ I, _____, do hereby acknowledge having obtained the above listed artifacts from the suspect/victim named above.

Investigating officers Signature:_____

Chain of Custody				
No.	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location
1				
2				
3				
4				
5				
6				
7				