INTELLIGENCE PRODUCT, DIGITAL DATA AND ELECTRONIC EVIDENCE

PRESENTED @

CYBER X AFRICA 2021 CONFERENCE, GHANA

BY

PROF. PETER OLUBUSOLA OLAYIWOLA,

BBA, MBA, PH.D., FNCS, MCPN, CPA, FCFI, C.ITP, CLWE, ACE, CGEIT, JP+

PRESIDENT & CHAIRMAN, CERTIFICATION BOARD, CFIN

12 NOVEMBER 2021

AGENDA

1. Introduction
2. Overview of the Topic
3. Intelligence Product
4. Digital or Electronic Data or Information
5. Digital or Electronic Evidence
6. Conclusion
7. End

1. INTRODUCTION

- We live in a world where social media has become a main source of news to society
- The young generation depend on it for their news and information
- Social media tend to control opinions formed in society
- Anyone can upload, whether true or false news, fake audios, videos, etc.
- Malicious and libelous

1. INTRODUCTION

- Need to protect society from itself.

2. Overview of the topic

- ❖ Intelligence Product and
- ❖ Electronic Data – contending with:
- ❖ Electronic Evidence
- ❖ In Big Fight in the Courts

❖ 3. Intelligence Product

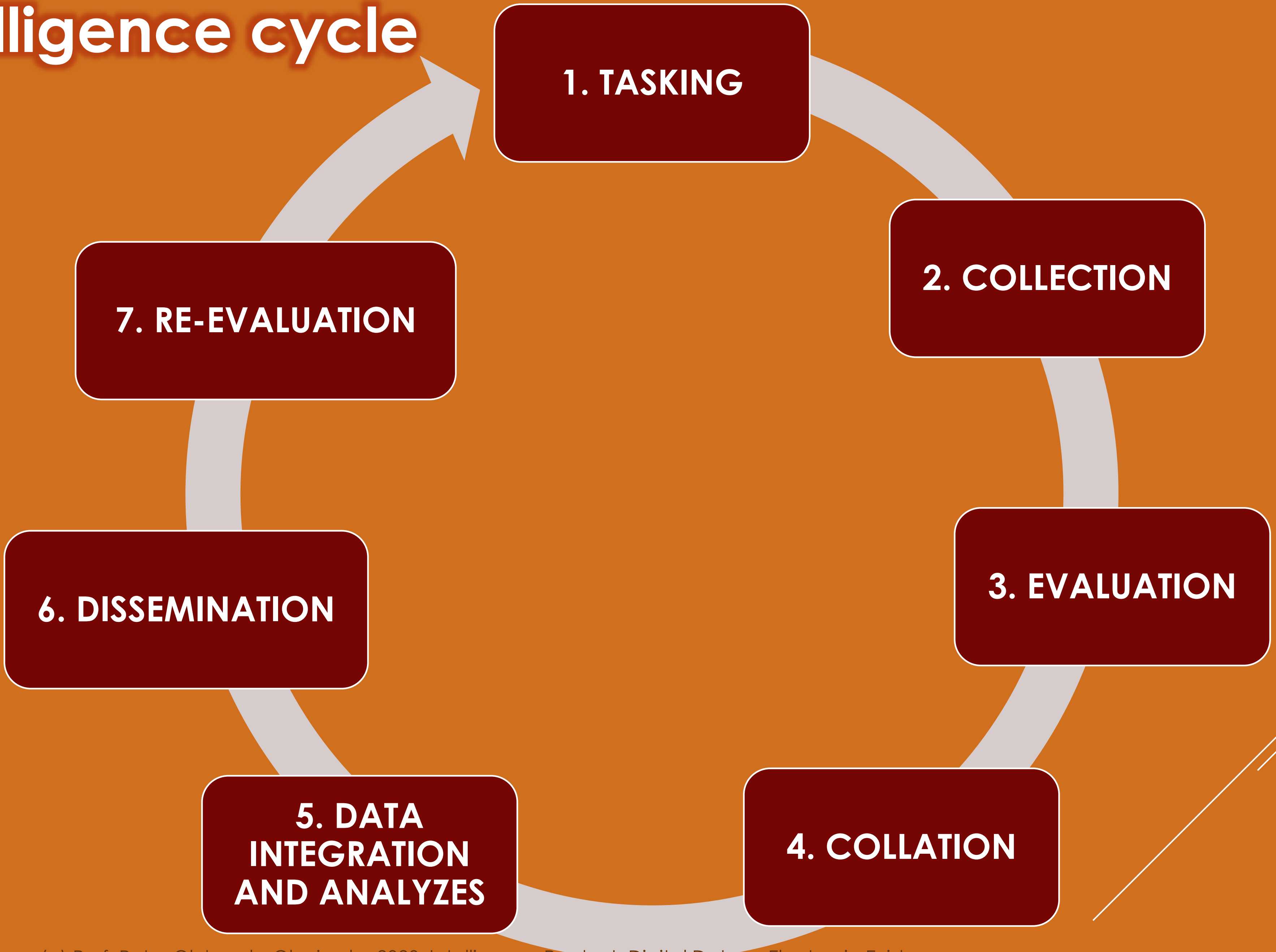
INTELLIGENCE =

INFORMATION + EVALUATION

Intelligence Product =

Output from Step 5 of the Intelligence Cycle

The intelligence cycle



❖ 4. Digital or Electronic Data or Information

- 4. Digital or Electronic Data or Information:

- Types and Sources

Characteristics of digital data:

1. It can be easily changed, manipulated or corrupted
2. It may be invisible to naked eyes, just like latent fingerprint
3. It requires the services of an expert to acquire and process into electronic evidence.
4. Often confused with the evidence.

5. Electronic or Digital Evidence

EVIDENCE:

Data from which to establish proof.

Electronic (Digital) EVIDENCE:

- **Governed by Law and**
- **Internationally-Approved Scientific Methodology**
- **Forensic Science – NOT Computer Science or IT.**

Electronic (Digital) EVIDENCE:

- **ACPO Standards**
- **IOCE Standards**
- **ISO 17025:2017**

ACPO, 2012:

- Contains what I term the “Four pillars of Digital Forensics” (Olayiwola, 2021: Professional Course in Digital Forensics)

- No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

PILLAR 1:

- In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

PILLAR 2:

- An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved.
- An independent third party should be able to examine those processes and achieve the same result.

PILLAR 3:

- The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

PILLAR 4:

DIGITAL FORENSICS: DEFINITIONS

- The application of science and technology to law to determine evidentiary value of items found during a criminal investigation

- Forensic activity conducted using computer-based techniques

DIGITAL FORENSICS: DEFINITION

- **Computer forensics or digital forensics** are the scientific methods and processes for:
  - acquiring,
  - preserving,
  - extracting (digital/electronic data/information),
  - analyzing,
  - reporting and
  - presenting

digital/electronic evidence in a manner that is legally admissible, using an approved digital forensics methodology, and, usually, for legal purpose.

DIGITAL FORENSICS: SUBSETS

- Computer Forensics
- Mobile and Phone Forensics
- Cloud Forensics
- Network Forensics
- Live Forensics
- Triage Forensics
- Drone Forensics
- Vehicle Forensics

DIGITAL FORENSICS: TYPES

- Forensic Photography
- Audio Forensics
- Video Forensics
- Data and Data Base Analytics
- Forensic Malware Analysis

NECESSITY FOR DIGITAL FORENSICS

- **Nigeria has in place the following Acts:**
  - **Evidence Act, 2011 -** makes all forms of electronic evidence admissible in our courts
  - **Cybercrime Act, 2015 –** Criminalizes many acts not hitherto considered criminal
  - **Administration of Criminal Justice System Act, 2015**

DIGITAL FORENSICS

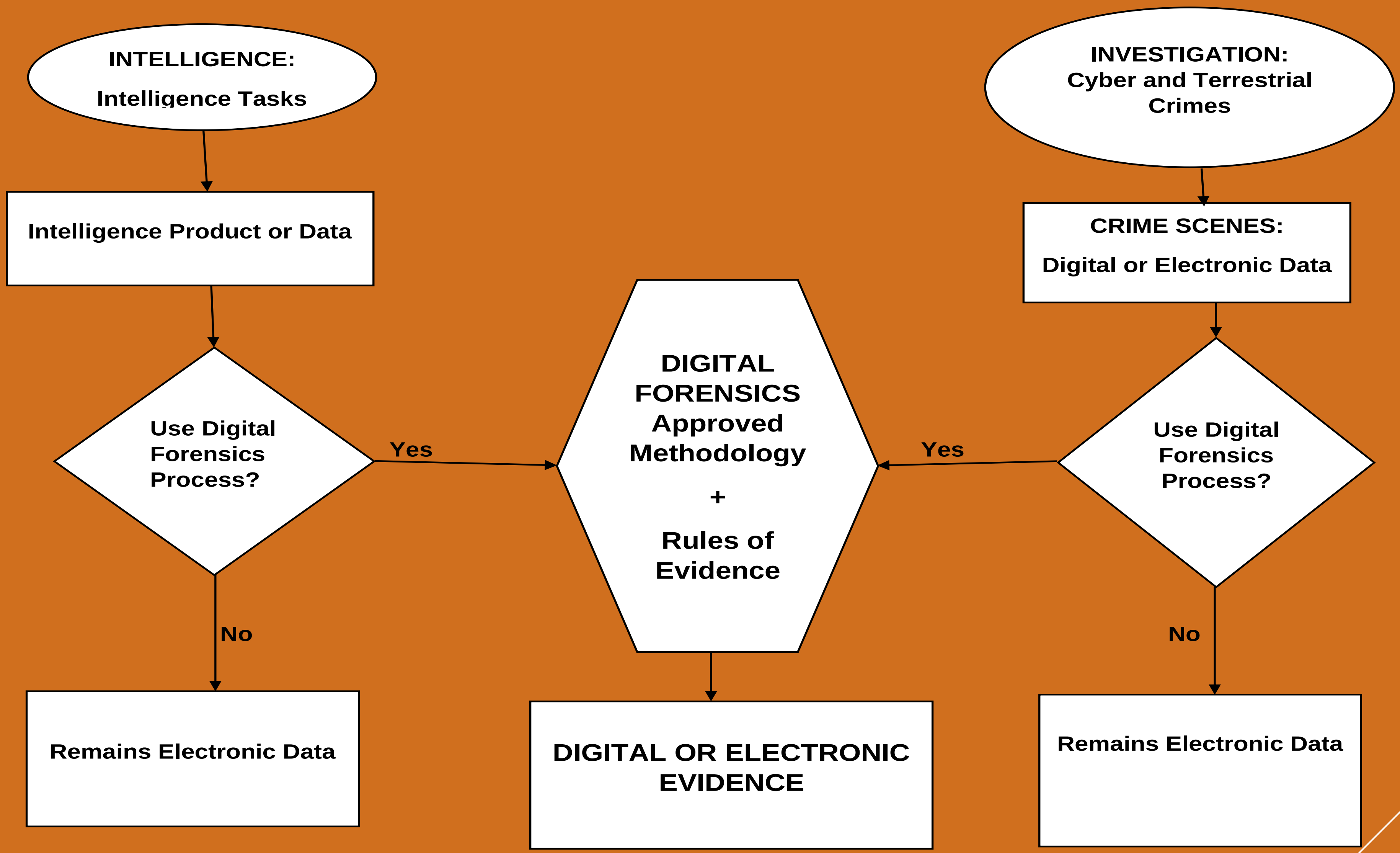
DETECTION OF A CRIME

INVESTIGATION OF A CRIME USING DIGITAL FORENSIC APPROVED METHODOLOGY. OUTPUT = ELECTRONIC EVIDENCE

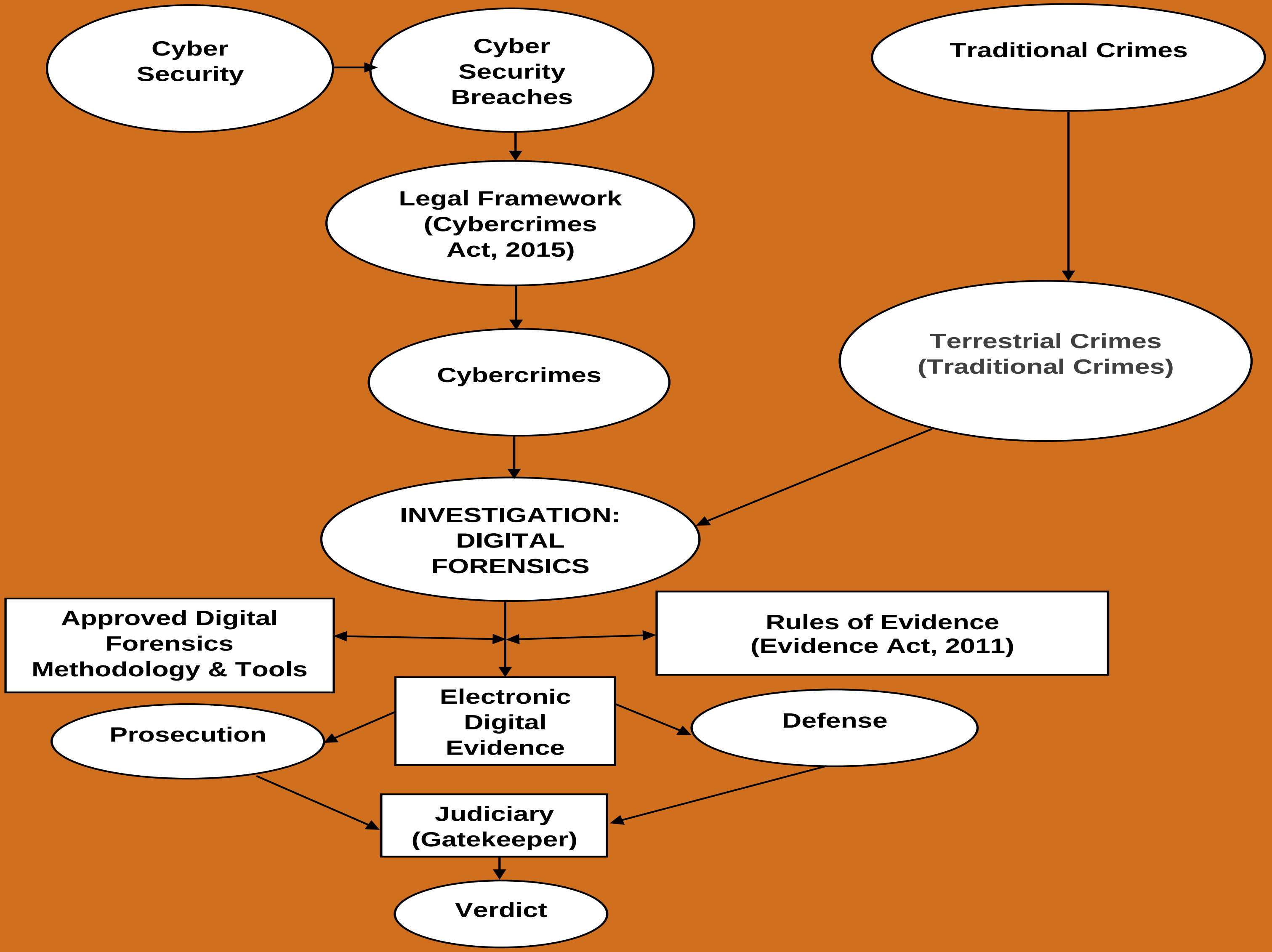
PREVENTION OF CRIME COMMITTED IN THE CYBER SPACE

(CYBER SECURITY)

DIGITAL FORENSICS IN INTELLIGENCE AND INVESTIGATION



CYBER SECURITY, CYBER BREACHES AND DIGITAL FORENSICS



.Homicide

.Terrorism

. Kidnapping

. Robbery

. Burglary

. Arson

. Stealing

. Forgery, etc.

Electronic (Digital) EVIDENCE:

- **Rules of Evidence Guaranteeing the trust-worthiness of an Evidence:**
  - **Foundational Requirement;**
  - **Prohibition on Hearsay; and**
  - **Chain of Custody**

Electronic (Digital) EVIDENCE:

- **Example: Nigeria:**
- **EA, 2011, S.68 – Expert Witness and**
- **S.84 – Admissibility of Computer-generated Evidence**

Electronic (Digital) EVIDENCE:

- The scientific process
- Conducted by experts
- Digital Forensics Processes

Electronic Evidence

- What makes an electronic evidence?
- Following the laid down internationally-approved methodology in computer/digital forensics for the:
  - acquisition,
  - preservation,
  - extraction,
  - analysis and
  - reporting of data captured or stored or found in electronic devices.

Electronic Evidence

- What was extracted as an electronic evidence in an intelligence operation may not be admissible as an electronic evidence –
  - if the digital forensic methodology was not followed in the acquisition, preservation, extraction, analysis of source data and reporting.
- May be useful for intelligence purpose, but NOT as an electronic evidence.

Deep Fake

In an era of 'Deep Fakes', it is important for Law Enforcement Agencies, Security Agencies, Military and the Judiciary to be aware of this and not be carried away by sensational images, photographs, audios and videos.

There are several tools for making fake photos, voices and videos.

(a) Devices (b) Forensically Processed? | Types Of Output

1.(a) Camera itself …………………………………… (b) Video, Photos, audio from the camera. (Processed using approved digital forensic methodology and the rules of evidence?)	(a) Physical Evidence (b) No = Digital data (c) Yes = Electronic Evidence
2.(a) Laptop itself (b) Data inside: emails, documents, files, database, Apps, photos, videos, etc. (Processed using approved digital forensic methodology and the rules of evidence?)	(a) Physical Evidence (b) No = Digital data (c) Yes = Electronic Evidence
3.(a) Phones or handheld devices (b) Data inside incl. chats, document, Apps, etc. (when processed using approved digital forensic methodology and the rules of evidence)	(a) Physical Evidence b) No = Digital data (c) Yes = Electronic Evidence

4.(a) Car or Vehicles (b) Data e,g. GPS, Car Module (Processed using approved digital forensic methodology and the rules of evidence?)	(a) Physical Evidence (b) No = Digital data (c) Yes = Electronic Evidence
5.(a) Black box (b) Data in it (Processed using approved digital forensic methodology and the rules of evidence?)	(a) Physical Evidence (b) No = Digital data (c) Yes = Electronic Evidence
6.(a) Drone (b) Data in it (Processed using approved digital forensic methodology and the rules of evidence?)	(a) Physical Evidence (b) No = Digital data (c) Yes = Electronic Evidence
7.(a) Spy Camera (b) Data in it (Processed using approved digital forensic methodology and the rules of evidence?)	(a) Physical Evidence (b) No = Digital data (c) Yes = Electronic Evidence

SUMMARY & CONCLUSION

- This presentation has been an attempt to provide a clear understanding of the relationship between intelligence product, digital data and electronic evidence; and that of cybersecurity, cybercrimes and digital forensics.

SUMMARY & CONCLUSION

Paying attention to the points raised on electronic evidence in this paper should:

1. Assist Military, Intelligence, Security and LEAs in producing admissible Electronic Evidence needed to prosecute or defend a case in litigation;

2. Assist the Trial of Facts (Judges, Magistrates, Tribunals and Court Martials) in arriving at a just verdict.

3. Protect the innocent from unjust punishments, and to punish the guilty party; and

4. Deter and discourage cybercrimes and facilitate the Implementation of Cybercrimes Act.

Conclusion (cont'd):

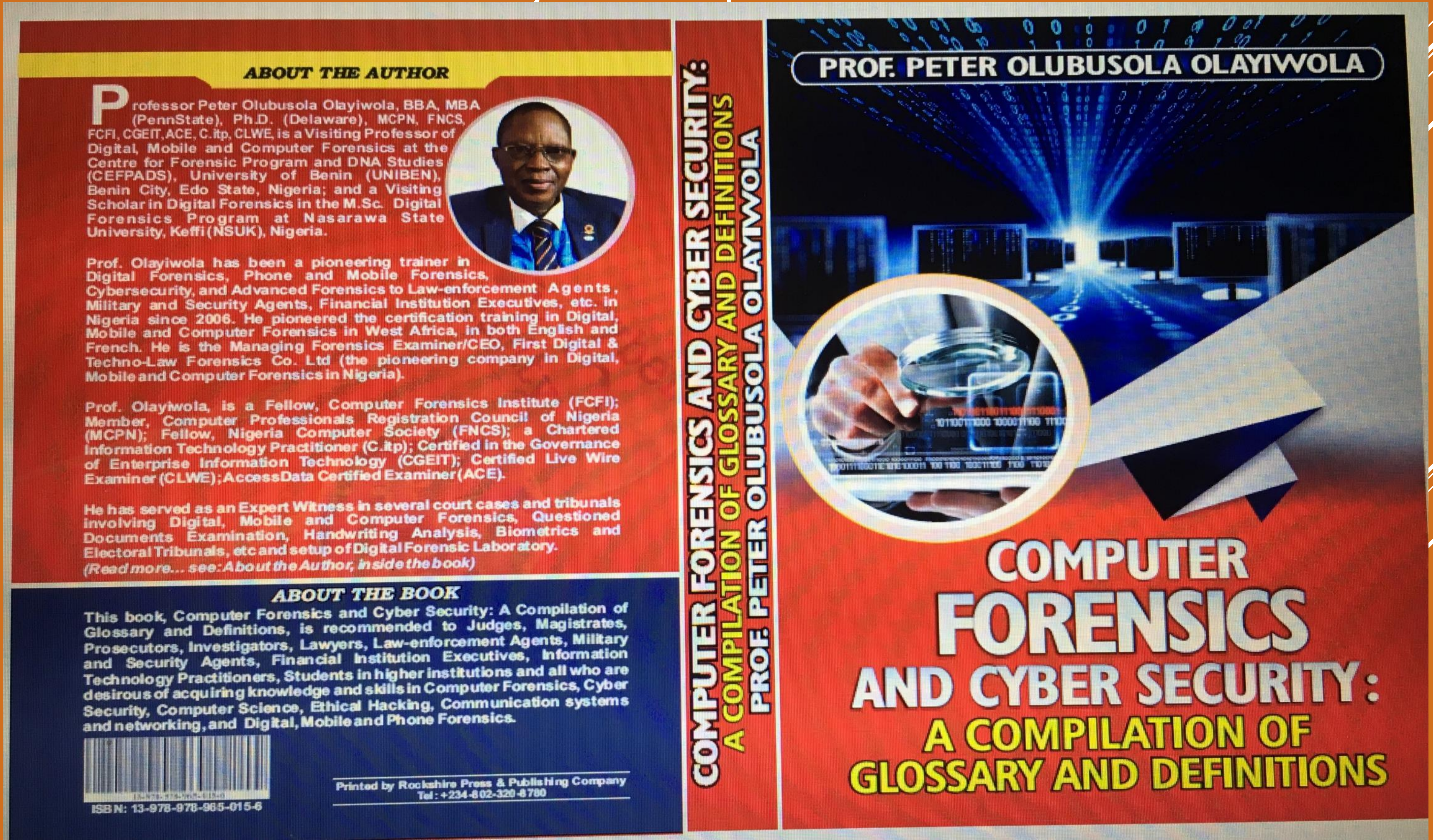
- From the beginning of an intelligence operation, the digital forensic methodology must be followed for an intelligence product to also serve as an electronic evidence.
- The time has come when electronic data should be separated from electronic evidence in the prosecution of civil and criminal cases.
- Protection of the innocent citizens, celebrities, politicians, judges, top government officials, etc. from character assassination, blackmail, cyberbullying, extortion, etc. should be vigorously pursued.
- Let us propagate this to all those concerned!

End

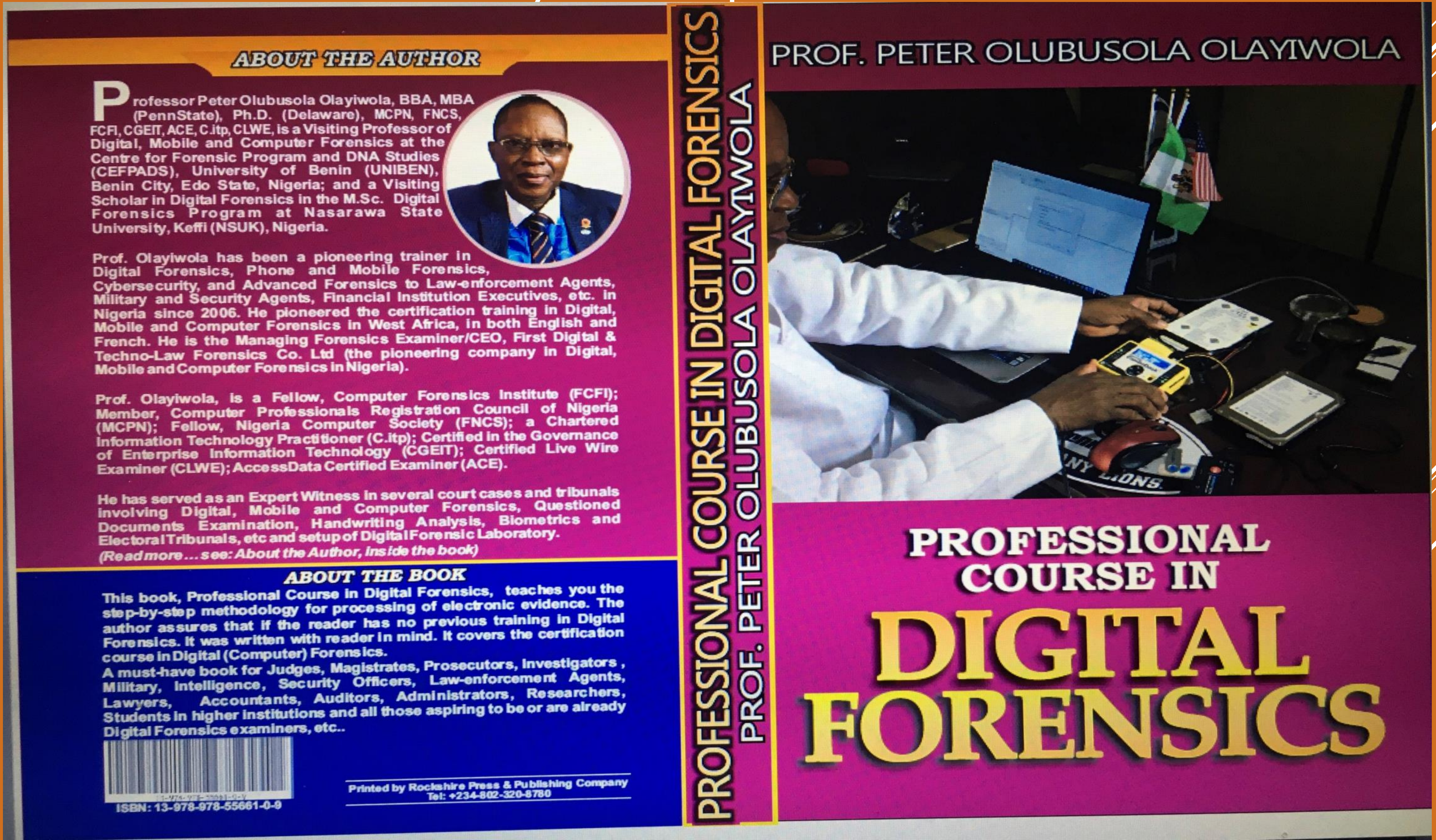
- Thank you.

Q & A

Forensic Books by this Speaker:



Forensic Books by this Speaker:



PROF. P.OLUBUSOLA OLAYIWOLA,

BBA, MBA, Ph.D., FNCS, MCPN, CPA, FCFI, C.ITP, CLWE, ACE, CGEIT

First Digital & Techno-Law Forensics Co. Ltd., Abuja

E-Mail: peterolayiwola@yahoo.com; chairman@firstdigitalforensics.com.ng

Phone: +234-802-320-8780, +234-803-853-3157, +234-706-188-0733

Websites: **https://professorpeteroluolayiwola.net**

https://firstdigitalforensics.com.ng

https://firstdigitalonlineforensicsacademy.com