WHAT, WHEN, WHERE, WHO, AND WHY:

RECONSTRUCTING EVENTS WITH DIGITAL FORENSICS

DIGITAL FOOTPRINTS
Digital Forensics and Cybersecurity

DR R. TOMBARI SIBE
CEO/Lead Forensic Examiner
Digital Footprints Ltd

About Speaker

PROFILE SUMMARY

Dr. Robinson Tombari Sibe is a Cybersecurity and Digital Forensic Expert. He is the **Co-Founder and CEO/Lead Forensic Examiner of Digital Footprints Nig. Ltd**. He has over 2 decades of experience. He has led several complex investigations and projects. He is a member of the Forbes Technology Council. He has mixed experience at both the industry and the academia. **He is a Fellow of University of South Wales and an Advisory Board Member of the University of the Cumberlands PhD IT Programme**. He also Lectures at RSU and the NOUN.

EDUCATION

- **University of the Cumberlands, Kentucky, USA**

PhD Information Technology – Digital Forensics Specialty

- **University of the Cumberlands, Kentucky, USA**

Master of Science (MS) in Digital Forensics

- **University of Port Harcourt, Nigeria.**

Masters in Electrical/Electronic (Telecommunication Option) Engineering

- **Rivers State University, Nigeria.**

B.Tech Computer Engineering (Second Class Upper Division)

DIGITAL FOOTPRINTS
Digital Forensics and Cybersecurity

About Speaker

TRAINING/CERTIFICATIONS

- EC-Council Certified Chief Information Security Officer (CCISO)
- PECB Certified Chief Information Security Officer
- PECB Certified Lead Forensic Examiner
- PECB Lead Cybersecurity Manager
- Certified Cyber Crime Examiner (3CE) - National White Collar Crime Center, USA
- Certified Economic Crime Forensic Examiner - National White Collar Crime Center, USA
- Cellebrite Certified Mobile Examiner (CCME) - Cellebrite
- Cellebrite Certified Physical Analyst (CCPA) - Cellebrite
- Cellebrite Certified Operator (CCO) – Cellebrite
- Cellebrite Certified Mobile Fundamentals (CMFF)- Cellebrite
- Mobile Communication and Cell Forensic Analyst
- DSMO-DS Certified Mobile Operator (Paraben)
- P2CO-P2C Certified Operator
- Mobile Device Investigator – ADF Solutions Inc.

DIGITAL FOOTPRINTS
Digital Forensics and Cybersecurity

About Digital Footprints

- **Digital Forensics**
    - Computer forensics
    - Mobile forensics
    - Network Forensics
    - Incident Response
    - Cloud Forensics
    - IoT Forensics
    - SCADA Forensics
    - Data Recovery
    - OSINT
    - Set up of Digital Forensic Laboratory
    - Training
    - Expert Witness and Litigation
    - Employee Device Misuse Investigation

ABOUT DIGITAL FOOTPRINTS

DIGITAL FOOTPRINTS
Digital Forensics and Cybersecurity

DIGITAL FORENSIC LABORATORY

TABLE OF CONTENTS

- Digital Forensics: Quick Intro
- Digital Evidence
- Evidence Examination and Analysis
- Investigative Reconstruction
- Case Studies
- Quick Hands-on

DIGITAL FOOTPRINTS
Digital Forensics and Cybersecurity

DIGITAL FORENSICS: QUICK INTRO

WHAT IS DIGITAL FORENSICS?

In order to accomplish our learning objective, we must comprehend digital forensics after defining cybersecurity and its foundational ideas.

McKemmish (1999), defined digital forensics as "the process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable"

The Digital Forensics Research Workshop (DFRWS) (2001) defines digital forensics as "the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations".

DIGITAL FOOTPRINTS
Digital Forensics and Cybersecurity

PRINCIPLES OF DIGITAL FORENSICS

- Evidence Exchange
- Evidence Characteristics
- Forensic soundness
- Authentication
- Chain of Custody
- Evidence Integrity
- Objectivity
- Repeatability

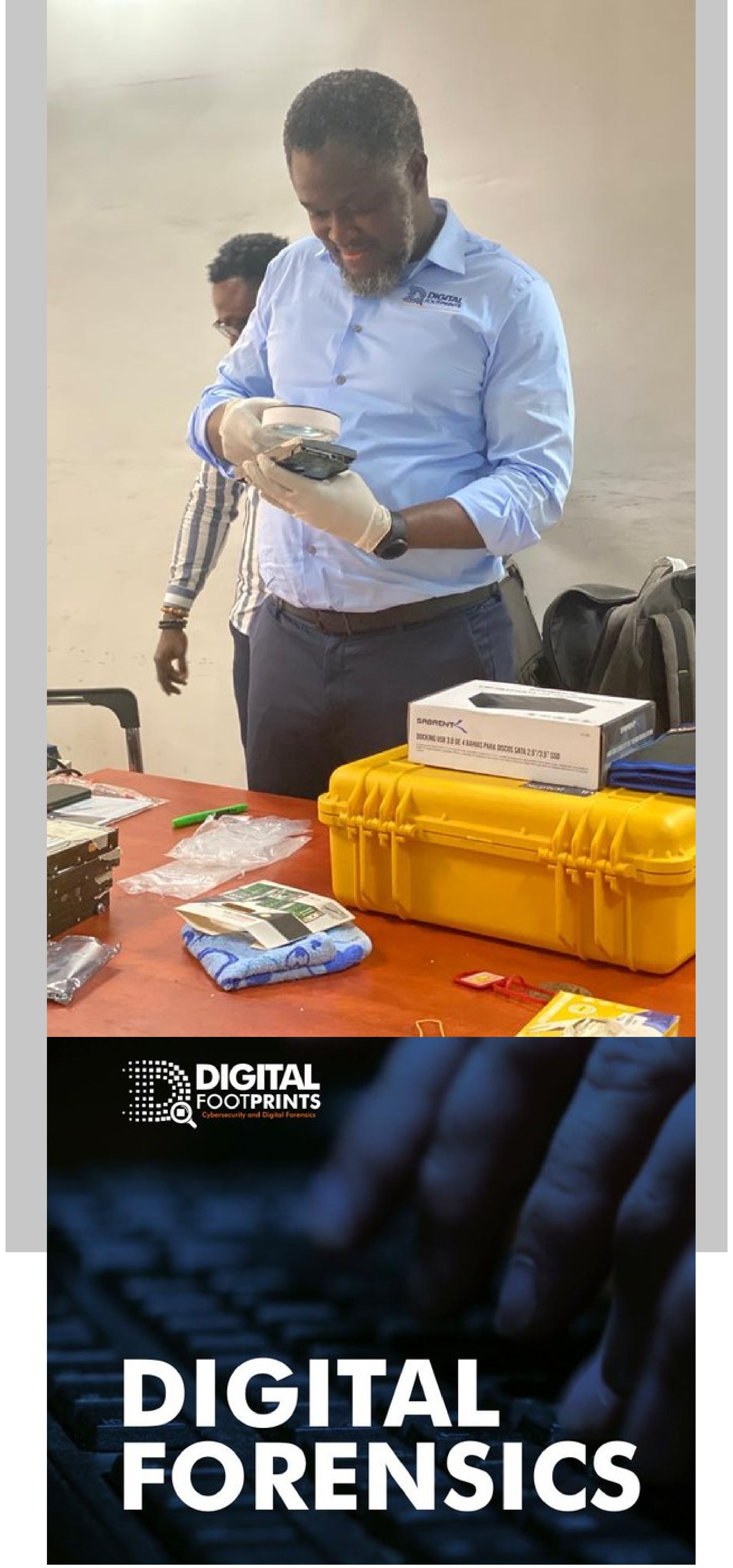
BRANCHES OF DIGITAL FORENSICS

These branches are grouped according to the source of the acquired digital evidence.

- Computer Forensics
- Mobile Forensics
- Network Forensics
- Cloud Forensics
- IoT Forensics
- Drone Forensics
- Video Forensics
- Image Forensics
- SCADA (Supervisory Control and Data Acquisition) forensics
- Chip-Off Forensics

DIGITAL FORENSIC PROCESS

- Identification
- Preservation
- Collection
- Examination
- Analysis
- Documentation
- Presentation
- Review



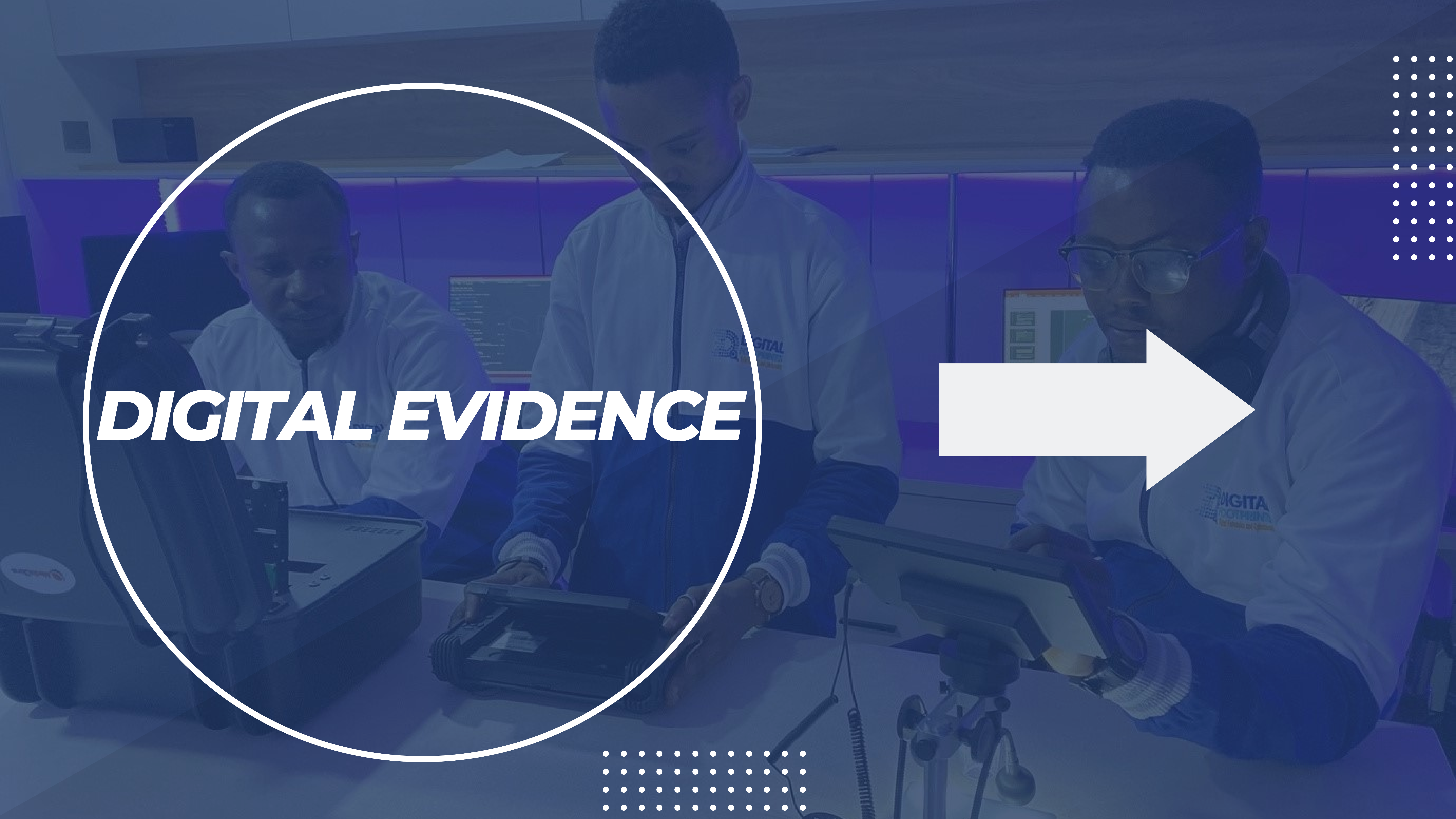
CHALLENGES IN DIGITAL FORENSICS

- Locating Relevant Evidence
- Anti-Forensic Techniques
- Data Fragmentation
- Encryption and Lack of Passwords
- Cloud and Remote Storage
- Volatility
- Rapidly evolving technological landscape
- Legal and Privacy Constraints
- Legacy Systems
- Delays

```
is example of
Single::ToString( ),
Single::ToString( String* ),
Single::ToString( IFormatProvider* ), and
Single::ToString( String*, IFormatProvider* )
enerates the following output when run in the [en-US] culture.
 Single number is formatted with various combinations of format
trings and IFormatProvider.

FormatProvider is not used; the default culture is [en-US]:
 No format string:                    11876.54
 'N5' format string:                  11,876.54000
 'E' format string:                   1.187654E+004
 'E5' format string:                  1.18765E+004

A CultureInfo object for [nl-NL] is used for the IFormatProvider:
  No format string:                   11876,54
  'N5' format string:                 11.876,54000
  'E' format string:                  1,187654E+004

 A NumberFormatInfo object with digit group size = 2 and
 digit separator = '_' is used for the IFormatProvider:
   'N' format string:                 1_18_76,54
   'E' format string:                 1,187654E+004
 Press any key to continue . . . _
```

DIGITAL FOOTPRINTS
Digital Forensics and Cybersecurity

DIGITAL EVIDENCE



DIGITAL EVIDENCE

Definition:
Any information of probative value that is either stored or transmitted in digital form – SWGDE

Information stored or transmitted in binary form that may be relied on in court – National Justice Institute.

Admissibility of Digital Evidence

Challenges

- Abstract, delicate nature and complexity of digital evidence
- Volatile nature
- Low capability maturity and readiness of the justice system and other stakeholders
- Rapidly evolving technological landscape (Emerging technologies)
- Need to update laws

SOURCES OF DIGITAL EVIDENCE

Digital evidence can be found in various forms across different types of digital devices and technologies. Here are some common sources of digital evidence:

Devices

Computers

Mobile Phones

Tablets

Smart Watch

IoT, etc.

Storage Media

Hard Drives

USB Drives

SD Cards

Networks

Internet Traffic

Communication Logs

Cloud Services

Data in the Cloud

SOURCES OF DIGITAL EVIDENCE CONT..

Computers and Laptops	• Internal Hard Drives • RAM (Random Access Memory)
Mobile Devices	• Smartphones and Tablets • SIM Cards
External Storage Devices	• USB Drives • External Hard Drives
Cloud Storage	• Services like Google Drive, Dropbox, iCloud
Network Traffic	• Logs • Packets
Emails	• Email Servers • Clients
Internet Browsing	• Web Browsers (History, bookmarks, cookies, and cached data)

Social Media	• Platforms like Facebook, Twitter, Instagram
Digital Cameras and Multimedia Devices	• Cameras • Audio Recorders
IoT Devices	• Smart Home Devices • Wearables
Server Logs	• Web Servers • Application Servers
Databases	• SQL and NoSQL Databases
Operating System Artifacts	• Registry Entries (Windows) • Log Files
GPS and Location Data	• Mobile Devices • Navigation Systems

DIGITAL EVIDENCE ACQUISITION

Live Acquisition

- Definition: Examining a system while it is running.
- Advantage: Provides insights into active processes, network connections, and volatile data.
- Disadvantage: Higher risk of data alteration and potential system instability.

Post-Mortem Analysis

- Definition: Examining a system after it has been powered down.
- Advantage: Reduced risk of data alteration, allows for thorough analysis of static data.
- Disadvantage: Volatile data is lost, might miss insights from active system states.

CHAIN OF CUSTODY AND OTHER DOCUMENTATION

The chain of custody is a process that documents the handling of evidence from its collection to its presentation in court. This documentation ensures the integrity and admissibility of evidence in legal proceedings.

It includes detailed logs that record who accessed the evidence, when it was accessed, and for what purpose, preserving the authenticity and reliability of the evidence throughout the investigation and judicial processes.

This rigorous documentation is vital for upholding the credibility of the forensic analysis and supporting the pursuit of justice.

BEST PRACTICES IN DIGITAL FORENSICS

- Maintain Chain of Custody
- Use Write Blockers
- Create Forensic Images
- Document Everything
- Preserve Volatile Data First
- Ensure Proper Storage
- Follow Standard Operating Procedures (SOPs)
- Verify Evidence Integrity
- Use Reliable and Validated Tools
- Minimize Data Handling
- Secure Transport of Evidence
- Adhere to Legal and Ethical Standards

EVIDENCE EXAMINATION & ANALYSIS

COMPUTER FORENSICS

COMPUTER FORENSICS PROCESSES

- Several stages are involved in the computer forensics process – Identification, Collection, Examination, Analysis, Reporting and Presentation.

Identification

- Obtain Legal Consent
  - Warrants or
  - Consent to search and seizure
- Search and Seizure
- Isolate and Document the Crime Scene
  - Photographs,
  - Video,
  - Sketches etc.
- Identify Items of Forensic Value
  - Laptops,
  - Mobile phones,
  - Tablets,
  - Drones,
  - Removable drives,
  - Sticky notes,
  - Notepads etc.
- Establish Chain of Custody

Collection

- Establish Order of Volatility
  - Cache,
  - Pagefile,
  - RAM content,
  - Hard drive,
  - Removable drives,
  - Backup media)
- Preserve Evidence
  - Destination Disk Wiping,
  - Disk cloning,
  - Write Protection,
  - Forensic Image
  - Hashing
- Documentation of all Action

Examination

- Quick triage of evidence
  - check date and time
  - check for relevant artifacts such as:
    * System Information
    * User Accounts
    * File System Volumes
    * Encrypted Files etc.

COMPUTER FORENSICS PROCESSES

Analysis

- Set of Tools are Used
  - Open-source Tools
  - Commercial Tools
- Deeper Examination of Evidence
  - Extracting Unallocated Files
  - Cracking Passwords
  - Analyzing File MIME Type
  - Registry Analysis
  - Event Reconstruction
  - Keyword Searches and Indexing
- Cross-validation of Analysis Result with Other Tools
- Peer Review
- Documentation of all Actions

Report & Presentation

- Production of Structured Report
  - Examiner’s Background
  - Executive Summary
  - Case Background
  - Summary of Tools
  - Methodology Employed
  - Limitations
  - Analysis Findings
  - Opinion and Recommendation
- Presentation
  - To Court or Judicial panel as Expert Witness
  - To Executives and Decision-makers
- Ensure Understanding of Technical Concept by Non-technical Audience

COMPUTER FORENSICS: ARTIFACTS OF INTERESTS

- Computer evidence are artifacts generated either by the computer during operation or by the users, which can be used to establish guilt or innocence of an accused person.

User-generated evidence includes:

- Text files
- Spreadsheets
- Database
- Video and audio file,
- Digital images
- Address book and calendar
- Hidden and encrypted files
- Email messages and attachments
- Call history and messages
- Web pages
- Social media accounts
- Cloud accounts

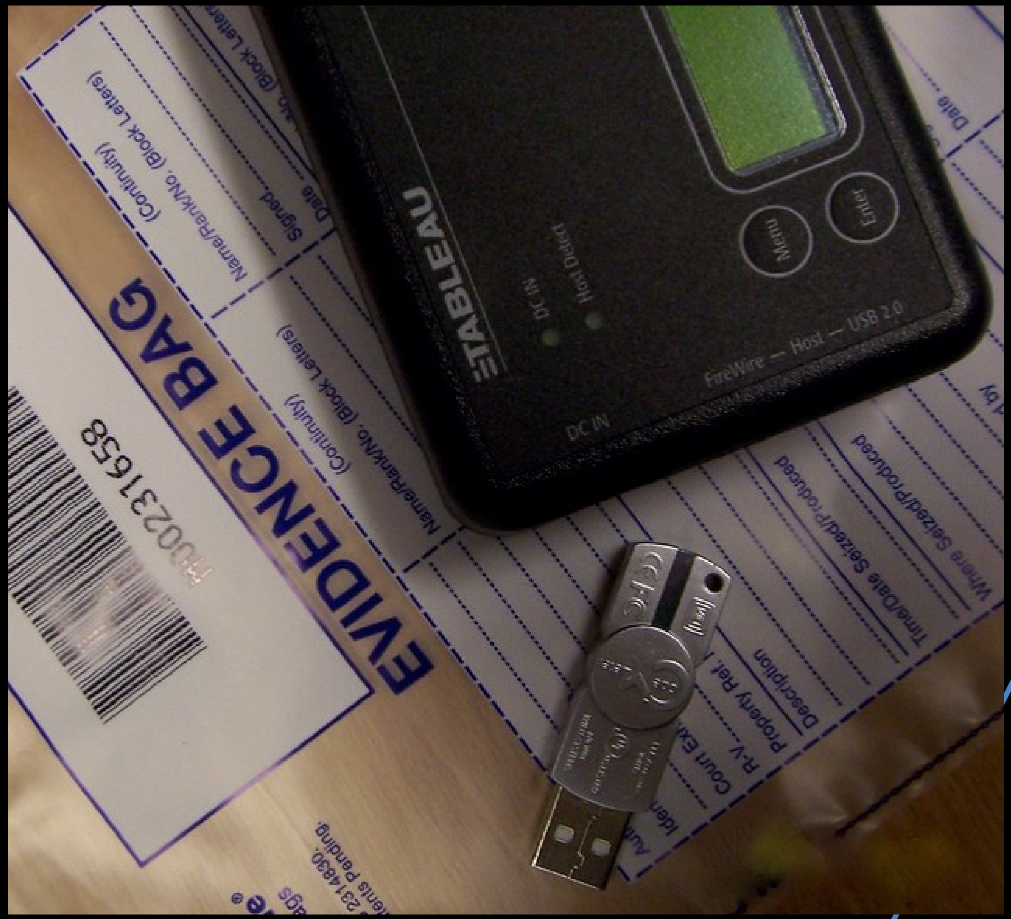
Computer-generated evidence consist of:

- System logs
- Browser data such as browser history, cookies and download history
- Applications history (e.g., recently opened file on MS Office) and windows history
- Restore points under Windows machines
- Temporary files
- E-mail header information
- Registry files in Windows OS
- System files (both hidden and ordinary)
- Metadata etc.

COMPUTER EVIDENCE ACQUISITION METHODS

- The main task of a computer forensics investigator is to acquire and analyze computing devices' memory images. In a nutshell, a memory image—widely known as a forensic image—is a static snapshot of all or part of the data on a computing devices' secondary storage (e.g., HDD, SSD), attached storage device (e.g., USB thumb drive, external hard drive, magnetic tape), or RAM memory (when performing live acquisition on running systems).

- ➢Acquisition Types
- ➢Forensic Image File Formats
- ➢Device Preparation and Sanitization



COMPUTER EVIDENCE ACQUISITION METHODS

FORENSIC IMAGE FILE FORMATS

- Raw (DD) Format
- Advanced Forensic Format (AFF)
- EnCase Expert Witness **Format (E01)**

DIGITAL FOOTPRINTS
Digital Forensics and Cybersecurity

ACQUISITION TYPES

- **Dead Acquisition:** This is the type of acquisition made when the system is powered down and the storage media is removed. It is the most common type of forensic acquisition. Acquisition tools such as write-blockers, forensic acquisition software and hardware are use.
- **Live Acquisition:** This is the type of acquisition performed when a system is in active operation. It is majorly conducted during the acquisition of volatile memory such as RAM. Several tools exist to perform a live memory capture, examples are: Belkasoft RAM capturer, Magnet RAM capturer, DumpIt etc.

COMPUTER EVIDENCE ACQUISITION METHODS

EVIDENCE PRESERVATION WITH WRITE BLOCKERS

Write-blockers are electronic devices which protect the evidence item from alteration or modification during acquisition process.

Write protection ensures data are not written into the evidence item thereby preserving the integrity of the drive and the acquired forensic image.

Hardware Write-blockers are recommended for use; however, software write protection is also feasible.

HASHING FOR VERIFICATION AND VALIDATION

To verify that the exact copy of the evidence item was produced during acquisition, hashing techniques are employed to ascertain the integrity of the acquired image.

Hash values are unique irreversible strings of characters generated using a hashing algorithm such as MD5, SHA1, SHA256, HMAC etc.

Integrity is said to be maintained when the hash value of the forensic copy is the same as the hash value of the original item.

MEMORY ACQUISITION

- Acquiring volatile memory image could be quite crucial in computer forensic investigation. The following are types of information that can be found in volatile memory:

✓Cryptographic keys
✓Running processes
✓Executed console commands
✓Registry hives
✓Deleted files
✓Open/active registry keys
✓Internet account passwords (e.g., e-mail, social media, and cloud storage)
✓Exploit-related information

✓Malware (rootkits and Trojan horses)
✓Evidence of activity not typically stored on the local hard disk.
✓Clipboard contents
✓Text files and images
✓Encrypted contents
✓Instant messages

COMPUTER FORENSIC ANALYSIS TECHNIQUES

- File System Analysis
- Registry Analysis
- Internet Artifacts Analysis (Email, Instant Messaging, Cloud and Web Brower artifacts)
- Application Data Analysis
- Log Analysis
- Memory Analysis
- Timeline Analysis
- Data Recovery

ANALYSIS WITH OPEN-SOURCE TOOLS

OPEN-SOURCE TOOL ARE SOFTWARE TOOLS WITH OPEN LICENSE, FREELY AVAILABLE FOR THE USE OF FORENSIC EXPERTS TO ACCOMPLISH SPECIFIC TASK. THE FOLLOWING ARE LIST OF OPEN-SOURCE FORENSIC TOOLS.

Open-Source Tools

- Autopsy
- *Scalpel
- Log2Timeline
- *Foremost
- Plaso
- *Volatility WorkBench
- Windows Registry Recovery

- *Volatility Framework
- RegRipper
- Registry Editor
- Browsing History View
- Internet History Browser
- Internet Explorer History View
- Event Viewer
- Event Log Parser
- FullEventLogView
- Redline

OPEN SOURCE TOOLS

ANALYSIS WITH COMMERCIAL FORENSIC TOOLS

- Commercial tools are all-in-one proprietary tools with the capability to perform automated analysis of various forensic artefact such as the file system, registry, email, internet, cloud data, application data, encryption detection, timeline analysis, keyword search and geo-location data analysis. They generate automated report of tagged artefacts of interest and correlate event from previous cases.

Commercial Forensics Tools

- AccessData FTK (Forensic Toolkits)
- Guidance EnCase
- X-Way
- OSForensics
- Magnet Forensics
- Belkasoft Evidence Center
- Oxygen Forensic etc.

DIGITAL FOOTPRINTS
Digital Forensics and Cybersecurity

MOBILE FORENSICS

MOBILE FORENSICS

Mobile forensics is a subset of digital forensics that focuses on obtaining digital evidence from mobile devices. Mobile devices are any computing device (such as phones, smartphones, tablets, and wearable devices such as smart watches) that can make phone calls or access the internet over standard communication networks such as GSM, 3G, and 4G.

MOBILE FORENSICS PROCESSES

- Seizure and Isolation
- Acquisition (Identification and Extraction)
- Examination and Analysis
- Reporting

MOBILE FORENSICS CONTD..

What Data is Recoverable?

Information that resides on mobile devices (a non-exhaustive list):

- Phonebook data
- Pictures, videos, and audio files and sometimes voicemail messages
- Internet browser data
- Geolocation data, Call Detail Record(CDR) data, Wi-Fi connection information
- Data from various installed apps
- System files, usage logs, error messages
- Deleted data from all of the above
- Documents, spreadsheets, presentation files and other user-created data
- Passwords, user account credentials

Non-invasive extraction methods – Manual Extraction, Logical Extraction, JTAG method, Hex Dump

Invasive extraction methods – Chip-off, Micro Read

NETWORK FORENSICS

NETWORK FORENSICS

This branch of digital forensics is concerned with monitoring and analyzing traffic flow in computer networks in order to extract incriminating evidence (for example, determining the source of security attacks) or detect intrusions. Unlike other types of digital forensics, network forensics only deals with volatile (live) data.

DATA SOURCES FOR NETWORK FORENSICS

- Log analysis
- User and Entity Behavior Analytics (UEBA)
- Network Traffic Analysis
- Network Evidence Acquisition
    - Physical Interception
    - Active/Live acquisition
    - Traffic Acquisition Software

INVESTIGATIVE RECONSTRUCTION

INVESTIGATIVE RECONSTRUCTION IN DIGITAL FORENSICS

Investigative reconstruction in digital forensics is the process of recreating events, actions, or incidents to understand how a crime or security breach occurred.

Objectives of Investigative Reconstruction

- Understanding Events
- Establishing Timelines
- Identifying Actors
- Recovering Evidence
- Corroborating Evidence

KEY TECHNIQUES IN INVESTIGATIVE RECONSTRUCTION

- Timeline Analysis
- File System & Metadata Examination:
- Log Analysis & Correlation
- Network Traffic Analysis
- Memory & Volatile Data Forensics:
- Malware Analysis

CHALLENGES IN INVESTIGATIVE RECONSTRUCTION

⚠ **Incomplete or Altered Data:** Deleted files, encrypted information, or anti-forensic tactics.

⚠ **Timestamp Manipulation:** Attackers may change file timestamps to mislead investigators.

⚠ **Large Data Volumes:** Processing huge datasets requires automation and expertise.

⚠ **Legal & Ethical Constraints:** Maintaining chain of custody and ensuring compliance with privacy laws.

⚠ **Emerging Technologies**: Anti-forensics, AI, Encryption, etc.

DIGITAL FOOTPRINTS
Digital Forensics and Cybersecurity

CASE STUDIES

THE CASE OF HUSHPUPPI

Credit: US DoJ

CASE SUMMARY

Accused of BEC and Money Laundering

DIGITAL FORENSIC INVESTIGATION

- ✓ Affidavit suggested valuable evidential artifacts gotten through **mobile forensics, computer forensics, social media investigations, OSINT, email forensics, and others**.
- ✓ The FBI also relied on records provided by Snap Inc and Apple to correlate and establish connection between chat histories, email addresses, and phone contacts

THE CASE OF HUSHPUPPI

<u>FACTS ESTABLISHED</u>

1. That suspect was same person known as “Hushpuppi” on Social Media.
2. That suspect was involved in complex BEC scheme defrauding high profile victims
3. Fraudulent wire transfers and Money Laundering
4. Suspect pleaded guilty for roles played (with other co-conspirators in the following:
    i. Foreign Financial Institution (Maltese Bank): approximately $14,700,000.00 (€13,000,000);
    ii. Victim Companies in the U.K.: approximately $7,740,000.00
    iii. Victim Law Firm: $922,857.76; and
    iv. Victim Businessperson and Qatari Victim Company: $809,983.58.

Credit: R.T. Sibe and C. Kaunert (Book title: Cybercrime, Digital Forensic Readiness, and Financial Crime Investigation in Nigeria)

FRAUD INVESTIGATION OF FORMER EMPLOYEE

Case Summary

A former staff of a company was fired on suspected fraud. Suspect was accused of forging company documents and fraudulently opening an account where cheques were cleared and withdrawn. The company decided to seek the services of a digital forensic examiner to uncover potential evidence that could be used to prosecute the suspect. The employer seized suspect's official laptop for investigation.

Processes for Evidence Recovery

- Receive and Document: **Chain of custody.**
- Forensic duplication: **Hard drive was connected to a write blocker and forensically duplicated.**
- Examine forensic copy
- Perform analysis: **Registry forensics. Keyword search. Timelining. Browser history. Deleted files. Search history, etc.**
- **Produce report**

Tools Used

- **FTK Imager: Forensic Duplication**
- **Autopsy: Windows Forensics**
- **Belkasoft: Windows Forensic**
- **EaseUS Data Recovery Wizard**

Artefacts Extracted

- **Doctored Company Documents**
- **Bank Transfer Receipts**
- **Email and Chats**
- **Deleted files (EXIF, docs, etc)**

FRAUD INVESTIGATION OF FORMER EMPLOYEE

Facts Established

- Established User Identity
- Established user used complex anti-forensic tools (VPN, Tor, etc).
- User Deleted Files of Evidential Value (now recovered)
- User has a private company registered with same address as former employer
- Suspect paid $10,000 to an Offshore FX Trading Company. Possible Proceeds of Crime
- Several transactions linked to suspect
- Several keyword searches showing the suspect had interest in bitcoin and other digital assets.
- Recovered board resolution, confirmed to be forged by client.
- Recovered documents and conversations showing suspect presenting fraudulently opened account number to a company.
- Recovered bank statement of suspect showing heavy movement of funds from the fraudulently opened account, and for other procurements.
- Documents suggesting suspect procured a house. Transaction receipts suggesting renovation work, post-purchase.

WEBSITE DEFACEMENT INVESTIGATION

Processes for Evidence Recovery

- Network Traffic Analysis: **Captured network traffic to identify suspicious activity**
- System Log Analysis: **Analyzed Apache logs to identify unauthorized access**
- File System Analysis: **Analyzed file system to identify modified files**
- Database Forensics: **Analyzed database to identify unauthorized modifications**
- Social Media Monitoring: **Monitored social media for attacker's claims**

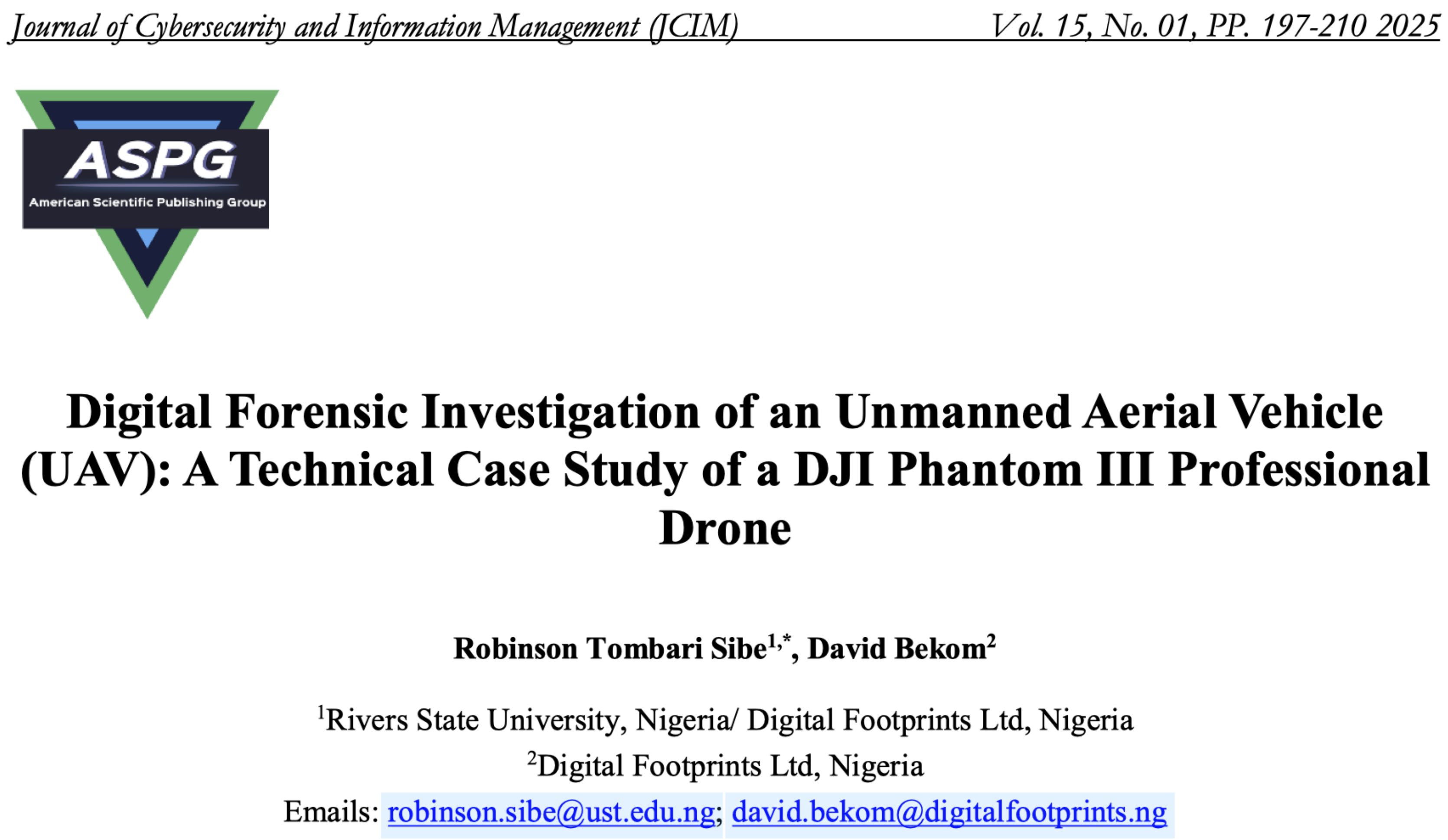
Tools Used

- **Wireshark: Network traffic analysis**
- **Splunk: System log analysis**
- **EnCase: File system analysis**
- **SQL Server Management Studio: Database forensics**
- **Hootsuite: Social media monitoring**

Artefacts Extracted

- **Defacement page: Recovered from file system**
- **Unauthorized access logs: Identified from Apache logs**
- **Modified files: Identified from file system analysis**
- **Database modifications: Identified from database forensics**
- **Attacker's claim: Identified from social media monitoring**

DRONE INVESTIGATION



Journal of Cybersecurity and Information Management (JCIM) *Vol. 15, No. 01, PP. 197-210 2025*

ASPG
American Scientific Publishing Group

Digital Forensic Investigation of an Unmanned Aerial Vehicle (UAV): A Technical Case Study of a DJI Phantom III Professional Drone

Robinson Tombari Sibe[1,*], David Bekom[2]

[1]Rivers State University, Nigeria/ Digital Footprints Ltd, Nigeria
[2]Digital Footprints Ltd, Nigeria
Emails: robinson.sibe@ust.edu.ng; david.bekom@digitalfootprints.ng

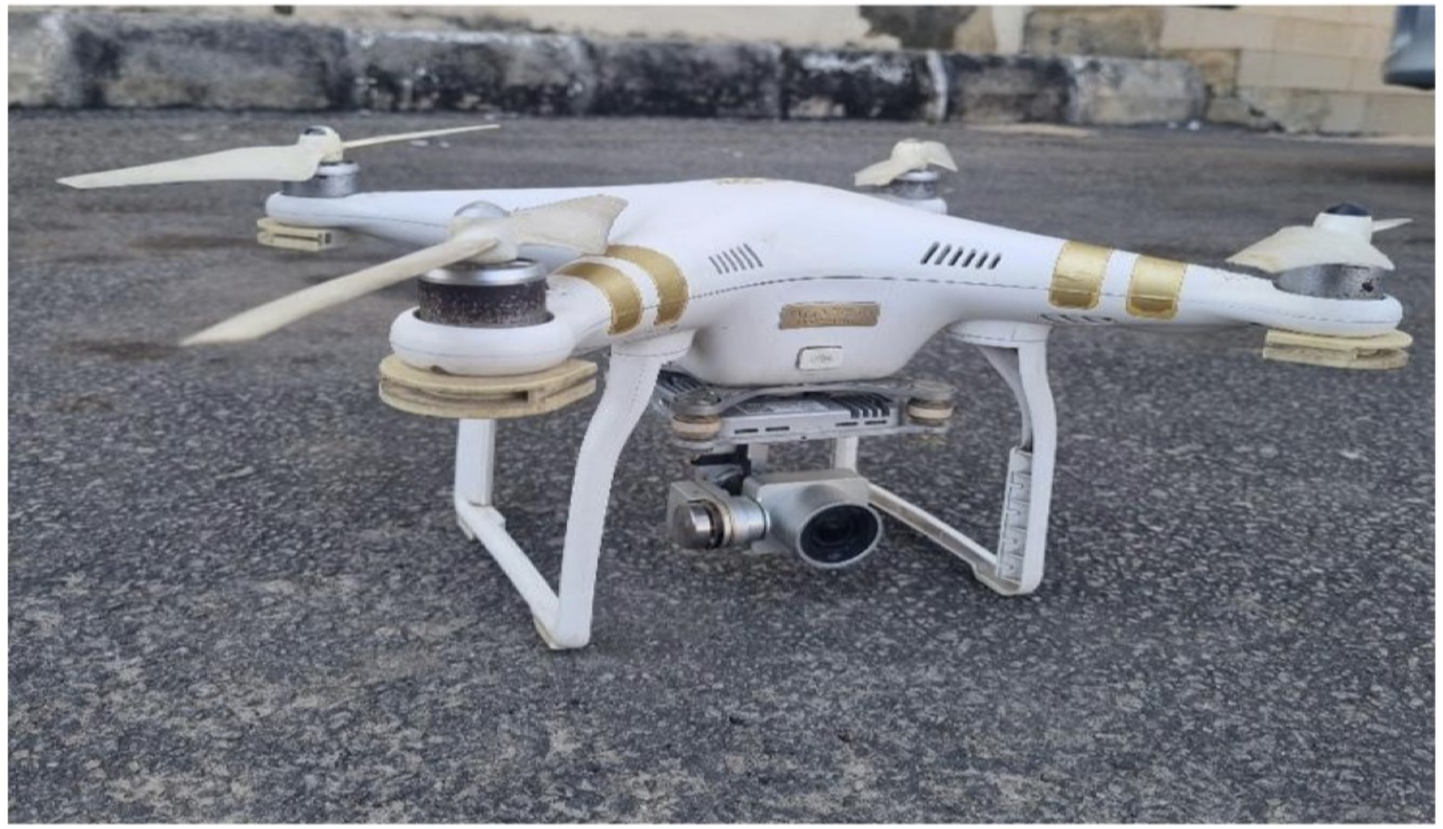


Figure 1. DJI Phantom III Professional drone.

DRONE INVESTIGATION

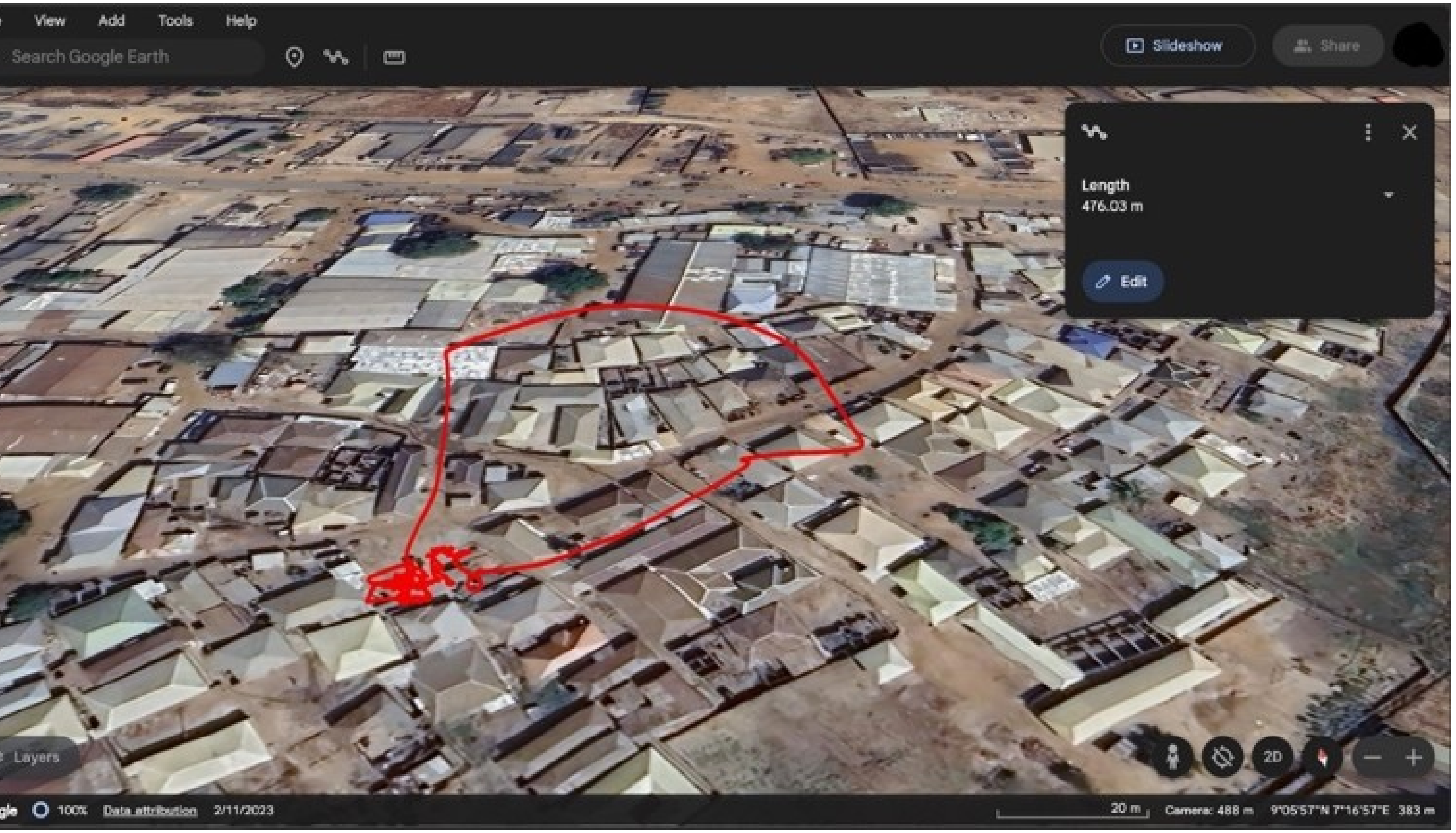
Case Summary: Artifacts Recovered

- EXIF Data
- Deleted Pictures and Videos
- DAT Binary (stored device logs and flight path)
- Inertial Measurement Unit (IMU)

Facts Established

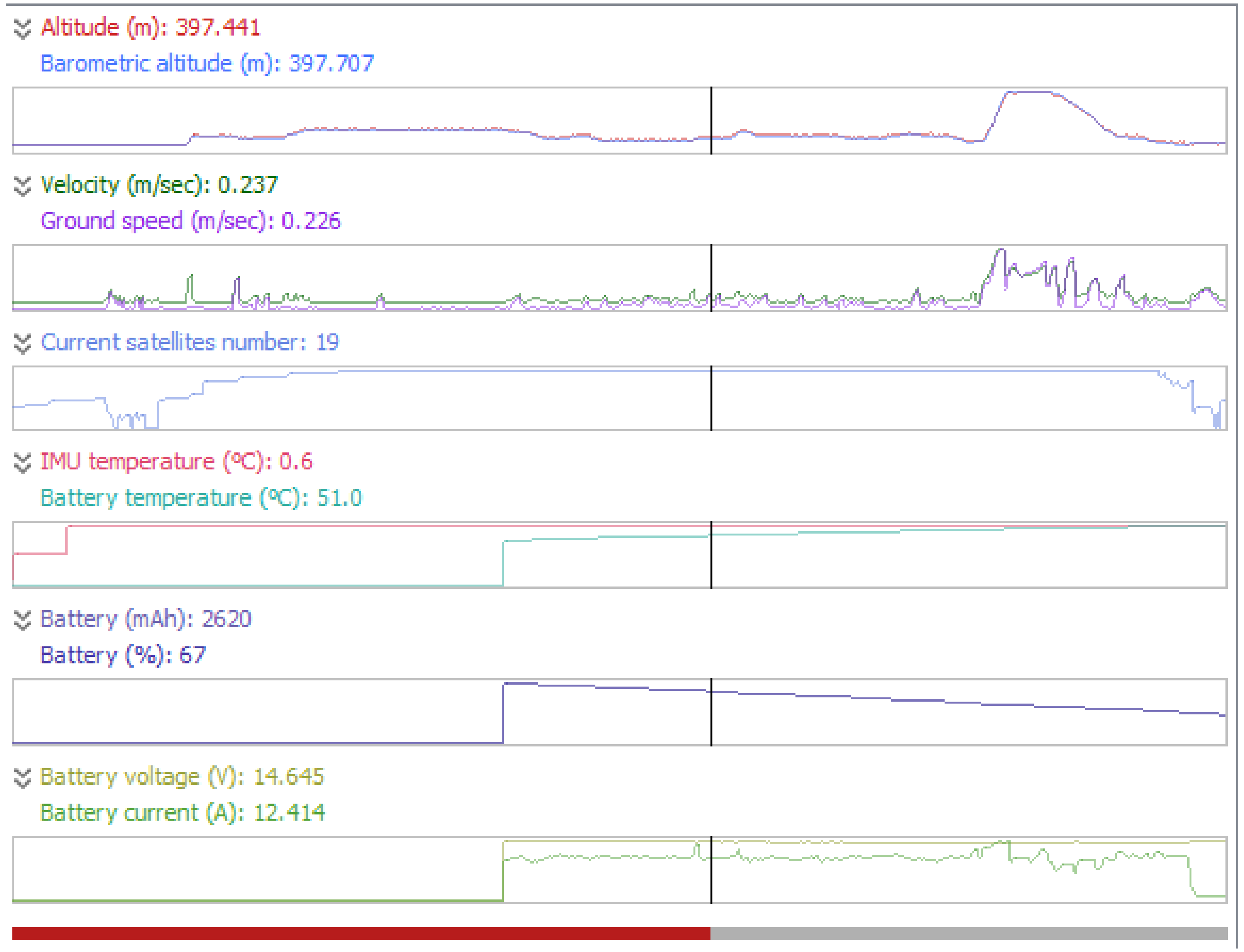
- Flight Path
- GPS coordinates, altitude, speed, battery level, and sensor readings.
- the flight operated around the Abuja metropolis on the 26th of November 2022.
- Drone had a travel length of 419m and total travel time of 12 minutes 18 seconds
- 40 image files, 34 audio files, 1 database file, 2 text files)
- Summary of facts established: when, where, what, who, and how

DRONE INVESTIGATION



Length
476.03 m

Camera: 488 m 9°05'57"N 7°16'57"E 383 m



Altitude (m): 397.441
Barometric altitude (m): 397.707

Velocity (m/sec): 0.237
Ground speed (m/sec): 0.226

Current satellites number: 19

IMU temperature (ºC): 0.6
Battery temperature (ºC): 51.0

Battery (mAh): 2620
Battery (%): 67

Battery voltage (V): 14.645
Battery current (A): 12.414

THANK YOU

Email: ***sibe@digitalfootprints.ng***
Website: ***www.digitalfootprints.ng***
Linked: www.linkedin.com/in/tombarisibe