NCS FORUM & WORKSHOP 2026

Building a Practical

DFIR Toolkit

Essential Tools and Techniques for Digital Investigators

Dr. Robinson Tombari Sibe, FNSE

CEO & Lead Forensic Examiner | Digital Footprints Nigeria Limited

Visiting Fellow, Unity of South Wales| Professor of Practice (Cybersecurity), MIVA Open University | AfICTA Board Member

DIGITAL FOOTPRINTS
Digital Forensics and Cybersecurity

Workshop Agenda

What we will cover today

01 **DFIR Fundamentals**

The investigative framework and first principles

02 **Evidence Acquisition**

Write-blockers, imaging tools & forensic soundness

03 **Memory Forensics**

RAM acquisition, Volatility & live artefact recovery

04 **Disk & File System Analysis**

Autopsy, FTK Imager, timeline analysis

05 **Network & Log Forensics**

Wireshark, Zeek, SIEM log correlation

06 **Mobile & Browser Forensics**

UFED, ADB, private-browsing artefact recovery

07 **Reporting & Courtroom**

Chain of custody, expert testimony standards

08 **Toolkit Showcase & Q&A**

Live tool demo — build your go-bag

What is DFIR?

DIGITAL FORENSICS

The scientifically derived process of identifying, preserving, analyzing, and presenting digital evidence in a manner that is legally defensible.

INCIDENT RESPONSE

The structured methodology for detecting, containing, eradicating, and recovering from security incidents — minimizing damage, reducing downtime, and preserving evidence for prosecution.

Branches of Digital Forensics

DIGITAL FOOTPRINTS
Digital Forensics and Cybersecurity

Computer
Hard drives, OS artifacts, file systems, registry, deleted files

Mobile
Smartphones, tablets, app data, geolocation, call records

Network
Packet capture, traffic analysis, intrusion detection, flow data

Cloud
S3 buckets, logs, container forensics, SaaS audit trails

Memory
RAM acquisition, process trees, injected code, crypto keys

IoT / OT
Smart devices, SCADA systems, industrial control artifacts

Video / Image
CCTV footage, metadata, manipulation detection

Drone
Flight logs, GPS coordinates, onboard camera data, firmware

eDiscovery
Litigation hold, email preservation, document review, production

Malware
Reverse engineering, behavioural analysis, sandbox detonation

DFIR Fundamentals

The Six-Phase Investigative Framework

01 PREPARATION
Build the Team, Toolkit, legal authority, evidence SOP

02 IDENTIFICATION
Scope, evidence sources, chain of custody, Triage

03 ACQUISITION
Forensic imaging, write-blocking, hashing

04 PRESERVATION
Verified copies, access control, logs

05 ANALYSIS
Artefact parsing, timeline, attribution

06 REPORTING
Court-ready report, expert testimony

Forensic Soundness
Never alter original evidence — always work on verified forensic copies

Chain of Custody
Document every handler, location, and action from seizure to court

Documentation
If it isn't written down, it didn't happen — contemporaneous notes are mandatory

Legal Authority
Confirm jurisdiction, warrants, and applicable law before any acquisition

Forensic Readiness

An organization's ability to maximize the collection of credible digital evidence while minimizing the cost of an investigation.

Minimizes Investigative Costs

Pre-planned evidence collection eliminates reactive scrambling and reduces remediation time.

Legal & Regulatory Compliance

Evidence collected under a readiness policy is admissible. Ad-hoc collection often is not.

Faster Incident Response

Playbooks, tooling, and trained responders cut mean-time-to-contain dramatically.

Forensic Readiness Policies

DIGITAL FOOTPRINTS
Digital Forensics and Cybersecurity

01 / Readiness Policy

Organizational Commitment

Defines roles, responsibilities, scope, and the organization's explicit commitment to forensic readiness. The legal foundation.

02 / Data Retention

What to Keep & How Long

Log retention windows, secure disposal procedures, archival standards. Drives compliance with GDPR, NDPA, PCI-DSS, and sector regulations.

03 / Access Control

Who Touches Evidence

Only authorized personnel access investigation systems. MFA, privileged access workstations, and detailed audit trails are mandatory.

04 / IR Policy

Response Framework

Step-by-step escalation procedures, communication trees, legal counsel notification triggers, and evidence handling protocols for live incidents.

Incident Response Framework

PHASE 01

Preparation

Build the team, tools, and playbooks before any incident occurs

PHASE 02

Identification

Detect, triage, and classify the scope of the incident

PHASE 03

Containment

Isolate affected systems; prevent lateral movement

PHASE 04

Eradication

Remove malware, close access vectors, patch vulnerabilities

PHASE 05

Recovery

Restore systems, verify integrity, resume operations safely

PHASE 06

Lessons Learned

Document findings, brief stakeholders, improve defenses

Creating a Forensic Toolkit

Creating a comprehensive forensic toolkit is a critical step in establishing a robust cyber forensics capability. Such a toolkit should encompass a wide array of tools and solutions, each carefully selected for its specific functionality in the forensic process.

Hardware Requirements

The hardware requirements for a forensic toolkit can vary based on the specific tools and the scope of the investigations. However, a robust digital forensic workstation typically includes the following components:

- **High-Performance Processor (CPU)**
- **Large and Fast Storage**
- **Substantial Memory (RAM)**
- **Dedicated Graphics Card (GPU)**
- **Reliable Power Supply**
- **High-Speed Connectivity**
- **Write Blockers**
- **Specialized Forensic Hardware** e.g. Forensic duplicators, mobile device acquisition hardware.
- **Cooling Systems**
- **Backup Solutions** e.g. External drives, NAS (Network Attached Storage), or cloud backup solutions

Documentation & Checklists

Documentation and checklists are a vital part of assembling a forensic toolkit. They are important for:

- Ensuring Completeness and Consistency
- Standardizing Procedures
- Maintaining Legal and Evidentiary Integrity
- Enhancing Training and Skill Development
- Lowering the risk factor of human error.
- Supporting Accountability and Auditability

Tools

Open-Source Tools

Open source forensic tools are cost-effective and benefit from strong community support, allowing for frequent updates and customization. Their transparency, with publicly available source code, enables users to inspect and modify the software, making them ideal for educational purposes and rapid innovation.

Commercial Tools

In contrast, commercial forensic tools offer professional support, comprehensive features, and user-friendly interfaces. They ensure reliability and stability, meet legal and regulatory standards, and provide integrated solutions for seamless workflows. Regular updates and dedicated customer service enhance their security and usability in professional forensic investigations.

Essential Software by Category

TOOL CATEGORY	PRIMARY FUNCTION	KEY TOOLS	OUTPUT
Data Acquisition	Forensic imaging of digital media with hash verification	FTK Imager, dd, dc3dd, Guymager	E01 / RAW / AFF images
Disk & File System	File system parsing, artifact extraction, deleted-file recovery	Autopsy, X-Ways Forensics, EnCase	Case reports, artifact exports
Memory Forensics	Volatile data analysis	Volatility 3, Rekall, MemProcFS	Process trees, injected code, IOCs
Network Forensics	Packet capture, traffic reconstruction, intrusion analysis	Wireshark, Zeek, NetworkMiner, Snort	PCAP files, connection logs
Mobile Forensics	Device extraction	Cellebrite UFED, AXIOM, XRY, Oxygen	UFDR reports, extracted artifacts
Timeline & Analysis	Cross-source timeline correlation and visualization	Plaso / log2timeline, TIMESKETCH, Kibana	Super-timelines, pivot dashboards

Evidence Acquisition

Write-Blocking, Imaging & Verification

HARDWARE WRITE-BLOCKERS

Tableau T35u

USB 3.0 • SATA/IDE/SAS

WiebeTech Forensic UltraDock

Handles NVMe + PCIe drives

CRU Forensic RTX

Ruggedised field unit

Logicube Falcon-NEO

Hardware imaging + verification built-in

SOFTWARE IMAGING TOOLS

FTK Imager (Free)

E01/AFF/DD — GUI & CLI; hash verification

dc3dd / dcfldd

Linux CLI; MD5+SHA256; split images

Guymager

FOSS; BitCopy; parallel acquisition

AXIOM / Magnet ACQUIRE

Cloud + device acquisition; evidence container

⚠ **GOLDEN RULE: Always verify acquisition integrity with SHA-256 hash. Source hash = Image hash = Verified copy.**

Disk & File System Analysis

Autopsy, FTK & Timeline Construction

Autopsy

FREE OPEN SOURCE

Built on The Sleuth Kit (TSK) · File system, keyword, registry analysis · Timeline module — MACB timestamps · Hash DB integration (NSRL) · Extensible with Python modules

FTK Imager

FREE ESSENTIAL

View images without a licence · Custom content images · Evidence item export · Registry viewer built-in · Volume shadow copy access

Eric Zimmerman Tools

FREE WINDOWS

MFTECmd — Master File Table parser · PECmd — Prefetch analysis · RECmd — Registry deep-dive · JLECmd — Jump Lists · RLA — Registry Log Analysis

KEY WINDOWS ARTEFACTS

NTFS MFT	$MFT — every file ever created
Registry Hives	SAM, SYSTEM, SOFTWARE, NTUSER.DAT
Event Logs	%SystemRoot%\System32\winevt\Logs
Prefetch	%WINDIR%\Prefetch*.pf — execution evidence
LNK Files	%APPDATA%\Microsoft\Windows\Recent
Browser History	SQLite DBs — Chrome, Firefox, Edge
Shellbags	USRCLASS.DAT — folder access history
Amcache.hve	Application execution & hash evidence
Volume Shadow Copies	Previous file versions — gold for malware

// COMPUTER & DISK FORENSICS

Disk & Computer Forensic Tools

COMMERCIAL

EnCase

Industry-standard forensic platform for disk acquisition, file system analysis, registry parsing, and court-ready reporting. Widely accepted in legal proceedings.

OPEN SOURCE

Autopsy / Sleuth Kit

Powerful open-source platform with a full GUI frontend. Supports NTFS/FAT/exFAT, email analysis, keyword search, hash sets, and timeline generation.

COMMERCIAL

X-Ways Forensics

Portable, resource-efficient forensics platform. Exceptional file carving, disk editor, and RAM analysis. Preferred by examiners requiring speed and precision.

COMMERCIAL

Exterro FTK

Forensic Toolkit with full pre-indexing for rapid search across large datasets. Strong decryption, email parsing, and integrated case management workflow.

COMMERCIAL

OSForensics

Comprehensive investigation tool with web browser artifact recovery, password extraction, deleted file recovery, and system activity timeline.

Network Forensic Tools

OPEN SOURCE

Wireshark

Captures live traffic and dissects hundreds of protocols. Essential for reconstructing attacker communications and data exfiltration paths.

OPEN SOURCE

Zeek (Bro)

Network analysis framework that generates rich logs (DNS, HTTP, SSL, files) from traffic. Superior for long-term monitoring and threat hunting at scale.

OPEN SOURCE

NetworkMiner

Passive network forensic analyzer. Reconstructs files, credentials, and sessions from PCAP files. Useful for rapid triage of captured network evidence.

OPEN SOURCE / COMMERCIAL

Snort / Suricata

Real-time intrusion detection and prevention systems. Signature and rule-based alerting.

OPEN SOURCE

Xplico

Network forensic analysis tool that reconstructs application-layer content from acquired PCAP acquisitions.

Mobile Forensic Tools

COMMERCIAL

Cellebrite UFED

Industry-leading extraction platform supporting 25,000+ device profiles. Physical, logical, and file system extraction across iOS, Android, and legacy devices.

COMMERCIAL

Magnet AXIOM

Complete digital investigation platform. Aggregates mobile, computer, cloud, and vehicle data. Exceptional artifact parsing and case correlation across data sources.

COMMERCIAL

Oxygen Forensic

Specialized in aggregating data from cloud accounts, drones, and wearables in addition to mobile. Strong geolocation mapping and social graph analysis.

COMMERCIAL

MSAB XRY

Field-portable mobile extraction tool with offline decryption capabilities. Trusted by law enforcement agencies globally. Supports encrypted iOS and Android extraction.

COMMERCIAL

MOBILedit Forensic

App data extraction with deep parsing of WhatsApp, Signal, Telegram, and 300+ social apps. Includes deleted message recovery and SIM card analysis.

```
// Always place the device in a Faraday bag immediately on seizure. Remote wipe commands can destroy evidence in minutes.
```

Memory Forensic Tools

OPEN SOURCE · STANDARD

Volatility 3

The premier memory forensics framework. Plugin-based architecture for extracting processes, network connections, DLLs, injected code, and rootkit artifacts from RAM dumps.

OPEN SOURCE

Rekall

Advanced framework with live memory analysis and strong Windows kernel artifact support.

COMMERCIAL

FTK Imager

Reliable RAM acquisition tool. Creates memory images in a format compatible with most analysis frameworks.

FREE

Belkasoft Live RAM Capturer

Lightweight tool for capturing live RAM on running systems, including those protected by anti-debug mechanisms. Essential first-responder tool.

Reporting & Courtroom Readiness

Chain of Custody · Expert Testimony · Admissibility

FORENSIC REPORT STRUCTURE

1. Executive Summary

Non-technical findings for decision-makers (1 page max)

2. Scope & Authority

Examination mandate, legal authority, date range

3. Evidence Received

Each item: hash, seal condition, chain of custody reference

4. Methodology

Tools used (name + version), settings, acquisition method

5. Findings

Factual observations only — no opinion in this section

6. Expert Opinion

Clearly labelled inference drawn from findings

7. Appendices

Hash logs, tool outputs, raw artefact exports

NIGERIAN LEGAL STANDARDS

Evidence Act 2011, S.84

Conditions for admissibility of computer-generated evidence

Cybercrimes Act 2015

S.37–39: digital evidence collection & admissibility

ACJL/ACJA 2015

Electronic records admissibility in Nigerian courts

EXPERT WITNESS — DO / DO NOT

✓ DO	State findings in plain language; qualify uncertainty; only opine within expertise
✓ DO	Cite tool version and settings — reproducibility is key to credibility
✗ DON'T	Speculate beyond the evidence; overstate certainty; be an advocate
✗ DON'T	Dismiss cross-examination — acknowledge limitations honestly

The DFIR Go-Bag: Your Field Toolkit

Everything an Investigator Should Carry

HARDWARE

- Forensic write-blocker (USB 3.0 + SATA)
- 2× external SSDs (min 4TB each) for imaging
- Network tap / passive TAP device
- Faraday bag (phones, tablets, IoT)
- USB hub + adapters (USB-C, Lightning, Micro-USB)
- Bootable forensic USB (CAINE Linux)
- Label printer + tamper-evident evidence bags
- Digital camera (evidence photography)
- Latex gloves + anti-static wrist strap

SOFTWARE (FREE)

- Autopsy + Sleuth Kit
- FTK Imager
- Volatility 3
- Wireshark + tshark
- dc3dd / dcfldd
- Eric Zimmerman Tools Suite
- CAINE Linux Live Distro
- Bulk Extractor
- RegRipper

PROCESS

- Pre-printed Chain of Custody forms
- Evidence receipt templates
- Examination worksheet (SOP-aligned)
- Legal authority checklist
- Hash verification log sheet
- Photography log / sketch form
- Laptop with offline tool access
- Encrypted evidence journal
- Copy of relevant statutes (Cybercrimes Act)

What It Will Cost You

Building a credible DFIR capability requires deliberate investment.

Hardware & Acquisition

Forensic workstations, write blockers, mobile extraction kits

Software & Licensing

Commercial suites, annual renewals, specialist tools

Training & Certification

Initial certs, recertification, lab environment access

Where the Money Goes

Indicative cost ranges for a functional DFIR toolkit in the Nigerian market context

HARDWARE

$8K – $18K

Forensic workstation, two write blockers, mobile extraction device (Spektor), and evidence storage media. One-time capital outlay; replace on a 4 to 5 year cycle.

SOFTWARE

$4K – $12K

Commercial suite license, annual maintenance, and one specialist tool for memory forensics or network analysis. Open-source alternatives reduce this substantially.

PEOPLE & TRAINING

$3K – $9K

Initial CHFI or EnCE certification per analyst, plus annual refresher courses and lab access. An ongoing cost that compounds as team size grows.

Phasing Your Investment

01 **Foundation (Months 1–6)**

$8K – $14K

Write blockers, forensic workstation, open-source suite (Autopsy, Volatility), one CHFI certification

02 **Capability Build (Months 7–12)**

$5K – $12K

Mobile acquisition unit, network forensics tooling, second analyst certification, evidence storage upgrade

03 **Maturation (Year 2)**

$5K – $20K

Commercial license tier-up, memory forensics specialist tool, lab refresh, advanced training access

Budget Considerations

Open source buys you runway.

Autopsy, Volatility, and Wireshark together cover the majority of practical casework. Defer commercial licenses until caseload justifies them.

Certification costs recur.

Certifications carry annual maintenance fees. Budget for renewal from year one, not as an afterthought.

Factor in exchange-rate risk.

Most major forensic tools are USD- or EUR-priced. Naira volatility means a fixed naira budget may not buy the same tool 12 months from now.

Chain of Custody & Documentation

DIGITAL FOOTPRINTS
Digital Forensics and Cybersecurity

// THE EVIDENCE LIFECYCLE

Seizure & Identification
Tag evidence with unique identifier, date/time, case number, and seizing officer details.

Acquisition & Hashing
Create forensic image via write-blocker. Compute and record MD5 + SHA-256 checksums immediately.

Secure Storage
Evidence bag, tamper-evident seals, controlled-access storage. Every transfer logged.

Analysis & Reporting
Work on verified copy only. Document every tool, version, and finding. Hash-verify before court submission.

// DOCUMENTATION STANDARDS

Examination Notes
Real-time notes during examination — tool version, parameters, anomalies observed, and time of each action.

Hash Verification Log
Pre- and post-analysis hash comparison confirming evidence was not altered. sha256 9f86d0...

Final Forensic Report
Executive summary + technical findings + methodology + conclusions. Signed and defensible in court.

Key Takeaways & Resources

1. Acquire volatile evidence FIRST — memory before disk, disk before network logs
2. Use a forensic write-blocker and hash verification
3. Document everything — contemporaneous notes are your strongest credibility asset in court
4. Maintain a sterile examination environment
5. Stay within authorized scope
6. Validate your tool

FREE RESOURCES

Autopsy
sleuthkit.org/autopsy

Volatility 3
volatilityfoundation.org

FTK Imager
exterro.com/ftk-imager

EZ Tools
ericzimmermantools.com

CAINE Linux
caine-live.net

CyberDefenders Labs
cyberdefenders.org

BlueTeamLabs
blueteamlabs.online

DFIR.training
dfir.training/tools

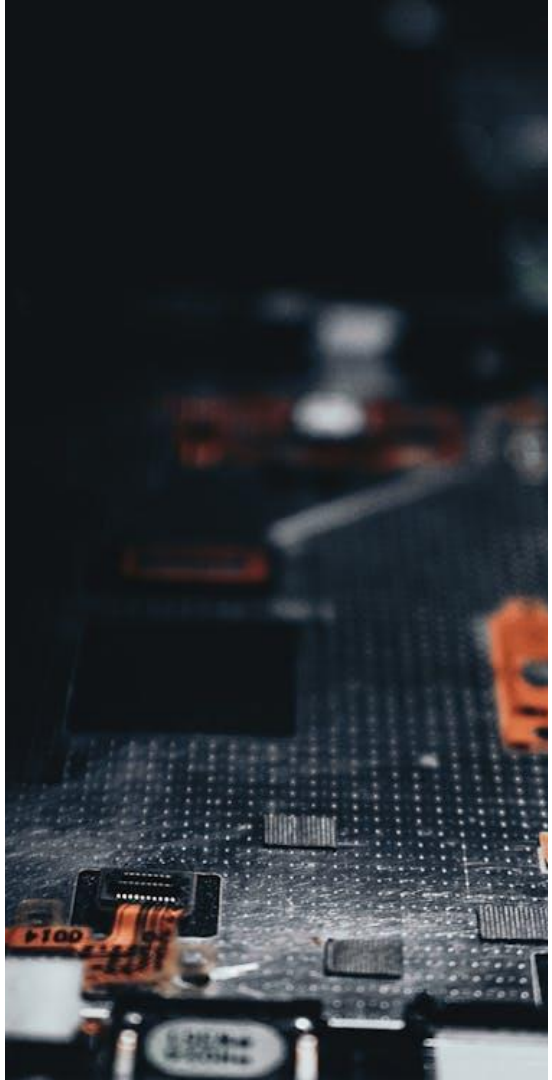
The tools are only as reliable as the process around them. Discipline, documentation, and continuous learning are what make findings defensible.

Conclusion

Forensic tools are extremely essential as a part of the DFIR process.

As technology evolves, so too must our tools, methods and practices in cyber forensics to stay ahead of the ever-evolving cybercrime threat landscape.

We must continuously seek improvement in our tools and techniques to ensure the integrity of our digital investigations.



THANK YOU

09122800800

www.tombarisibe.com

www.digitalfootprints.ng

info@digitalfootprints.ng