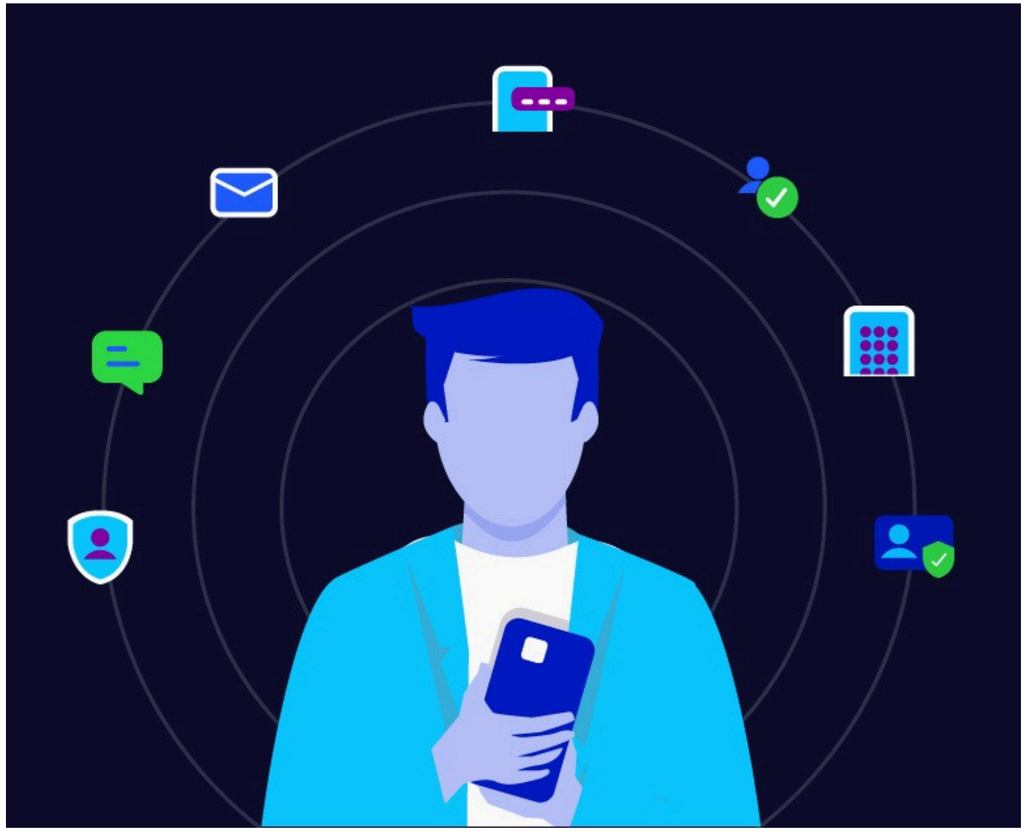
LEVERAGING DIGITAL FOOTPRINTS IN CYBERCRIME INVESTIGATION

ENHANCINGINTELLIGENCE-LEDINVESTIGATIONS,FINANCIAL INTEGRITY, AND NATIONAL SECURITY

PRESENTER: AISHATU ADAMS

KEY MESSAGE – FROM DIGITAL TRACES TO ACTIONABLE INTELLIGENCE

In todays interconnected world, everydigital interaction leaves traces. When lawfully collected, preserved, analyzed, and presented, these digital footprints become critical evidence in combating cybercrime, financial fraud, corruption, money laundering, terrorism financing, and other threats to national security.



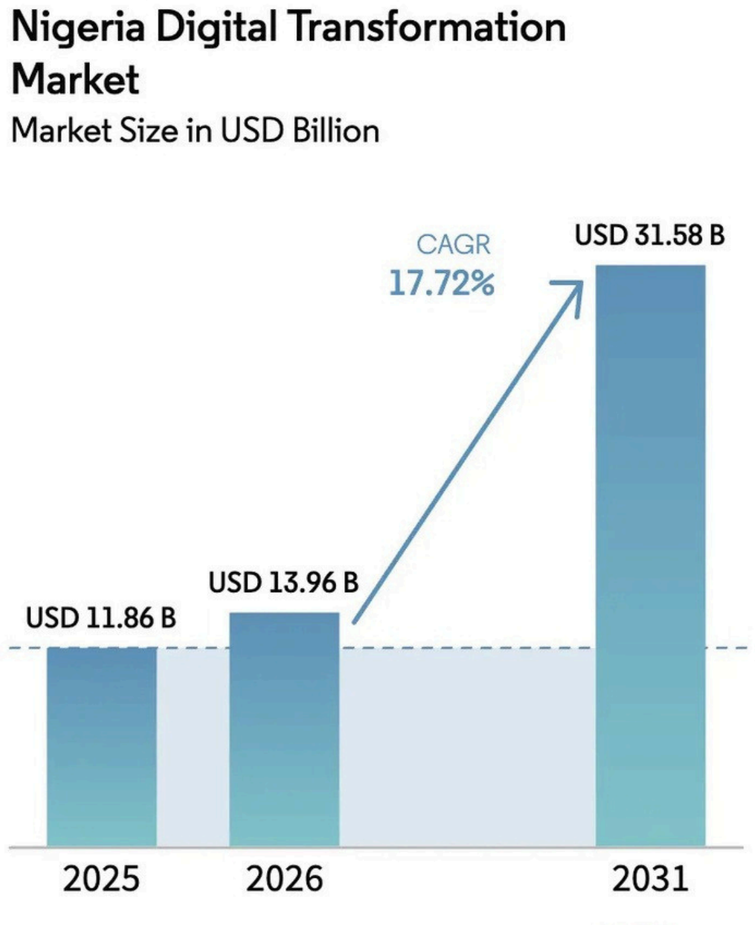
Every criminal leaves a footprint. The challenge is no longer obtaining data but turning data into intelligence and intelligence into prosecution.

THE DIGITAL REALITY: NIGERIA'S EXPANDING DIGITAL ECOSYSTEM

Digital Transformation in Nigeria has created new opportunities such as Digital banking and fintech growth, E-commerce expansion, Mobile connectivity, Social media adoption, Digital government services, and cross-border digital transactions.

But it has also expanded criminal opportunities, such as Business Email Compromise (BEC), Identity theft, Investment scams, Cryptocurrency-enabled crimes, Insider threats, Financial fraud, and Money laundering networks.

Criminals increasingly operate digitally, leaving behind digital footprints that can reveal identities, movements, communications, financial activities, and criminal associations.



UNDERSTANDING DIGITAL FOOTPRINTS I

A **digital footprint** is the record of activities, interactions, and transactions generated through the use of digital technologies.

Examples include Mobile phone records, Internet activity logs, Email metadata, IP addresses, Banking transactions, ATM usage records, Cryptocurrency transactions, Social media activities, Device information, Cloud storage records, Geolocation data, CCTV and digital surveillance records.

UNDERSTANDING DIGITAL FOOTPRINTS II

Active Footprints: Data deliberately created and shared by the user, such as Social media posts, Emails, Transactions, and registrations.

Passive Footprints: Data collected without the user's direct knowledge such as IP logs, Cookies, Cell tower records, CCTV timestamps, Metadata, Geolocation, and device identifiers.

Every digital action creates data.

Every data point tells a story.

Every story may become evidence.

THE DIGITAL FOOTPRINT ECOSYSTEM

Digital footprints are generated across a layered ecosystem. Understanding each layer helps investigators know where to look:

- **Network Layer:** IP addresses, MAC addresses, DNS queries, routing logs, VPN/proxy usage, ISP records

- **Device Layer:** Operating system artefacts, browser history, USB connection logs, application data, registry entries (Windows), syslog (Linux/macOS)

- **Application Layer:** Social media activity, email headers, messaging metadata, cloud storage access logs, API call records

- **Financial Layer:** Transaction metadata, cryptocurrency wallet addresses, blockchain transaction graphs, mobile money records

- **Physical (Digital) Layer:** Geolocation data, CCTV metadata, ATM withdrawal timestamps, smart device telemetry

KEY SOURCES OF DIGITAL FOOTPRINTS

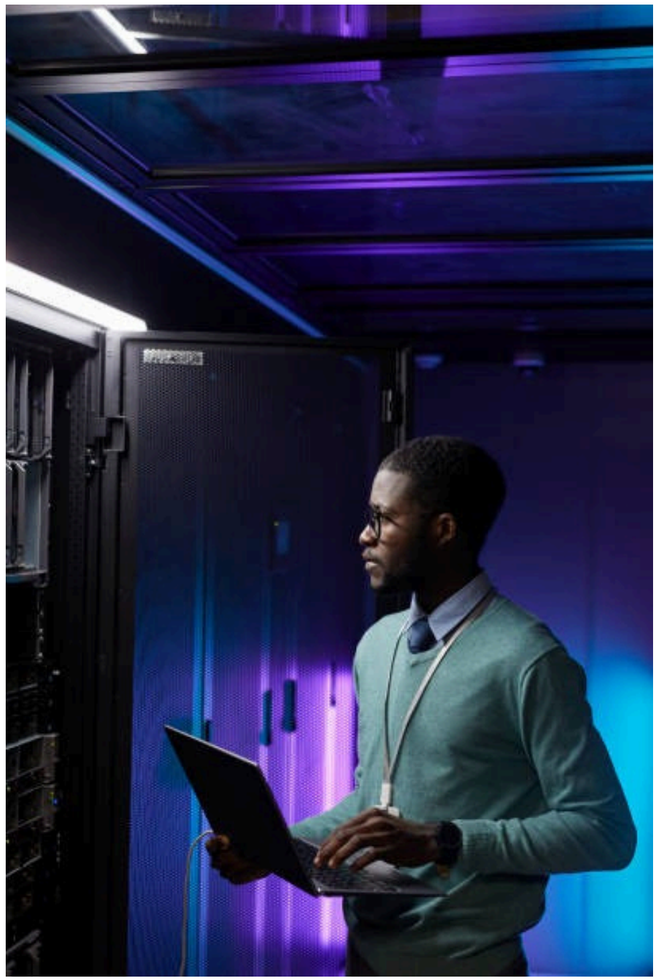
Telecommunications: Call detail records, Subscriber information, Location records.

Financial Institutions: Transaction histories, Account activities, Payment records.

Digital Platforms: Social media, Messaging platforms, Online marketplaces.

Enterprise Systems: Access logs, Authentication records, User activity records.

Open Source Intelligence: Publicly available information, Digital identities, Online associations.



THE CYBERCRIME INVESTIGATION LIFECYCLE

Professional cybercrime investigation follows a structured lifecycle that ensures evidence integrity, chain of custody, and legal admissibility. The framework below indicates digital footprint analysis at each stage.

Phase 1 – Detection and Intelligence Gathering

- Incident reports
- OSINT
- Intelligence gathering
- Complaints
- Suspicious transaction reports

Phase 2 – Lawful Collection and Preservation

All collection must be conducted within the authority of Nigerian law. Evidence improperly collected risks inadmissibility under Section 84 of the Evidence Act 2011 (as amended).

- Securing evidence
- Maintaining a physical chain of custody log
- Preventing alteration

Phase 3 – Analysis and Correlation

- Forensic examination
- Timeline Reconstruction
- Correlation of evidence
- Attribution(Cause/Origin)
- Cryptocurrency Tracing
- Communication Analysis

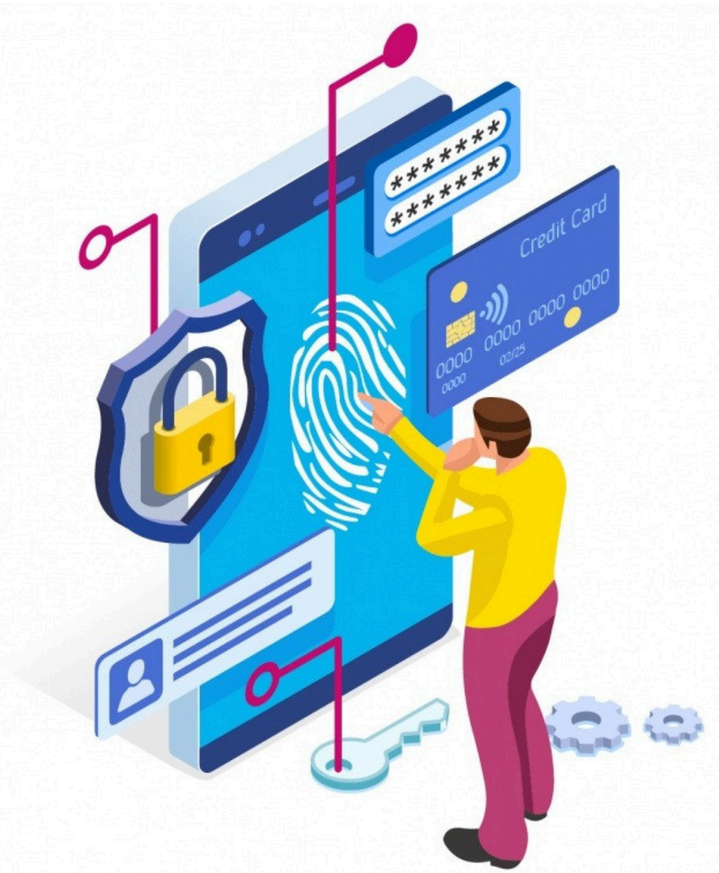
Phase 4 – Documentation and Reporting

Investigative findingsmust be documented in a form that is comprehensible to prosecutors, courts, and non-technical stakeholders.

- Formal Digital Evidence Report
- Visual Timeline Diagrams
- Evidential integrity

HARNESSING AI IN DIGITAL FOOTPRINT ANALYSIS

The volume of digital data generated in any cybercrime investigation can be overwhelming. A single smartphone may contain hundreds of thousands of files, messages, and metadata records. AI tools address three critical investigative bottlenecks:



- **Volume:** Processing gigabytes or terabytes of data far faster than manual review.

- **Pattern Recognition:** Identifying behavioural signatures, anomalies, and criminal TTPs across large datasets.

- **Correlation:** Linking disparate data points across sources that a human analyst might miss.

AI AS A FORCE MULTIPLIER

The following AI tools are either freely available or accessible through government/international partnerships:

- **Maltego (Community Edition):** Link analysis and OSINT aggregation; maps digital relationships visually
- **SpiderFoot HX:** Automated OSINT collection across 200+ data sources
- **Chainalysis Reactor/Breadcrumbs:** AI-powered cryptocurrency tracing
- **Hunchly:** AI-assisted web investigation session capture and logging
- **Autopsy + AI Plugins:** Open-source forensic analysis with ML-based categorisation
- **Google Lens/PimEyes:** Reverse image search for identity verification
- **OSINT Combine tools:** Aggregators for social media, domain, and IP intelligence

MORE AI TOOLS

Tool	Category	Access	Primary Use
Maltego Community Ed.	Link Analysis / OSINT	Free (maltego.com)	Relationship mapping, entity pivoting
SpiderFoot	OSINT Automation	Free / Open Source	Automated footprint collection across 200+ sources
Sherlock / Maigret	Username Enumeration	Free / GitHub	Cross-platform username search
theHarvester	Email/Domain OSINT	Free / Open Source	Email, subdomain, and IP harvesting
Recon-ng	Modular OSINT	Free / Open Source	Modular web reconnaissance
Autopsy	Digital Forensics	Free (sleuthkit.org)	Device forensic analysis, artefact extraction
FTK Imager	Forensic Imaging	Free (exterro.com)	Bit-for-bit device imaging with hash verification
Wireshark	Network Forensics	Free (wireshark.org)	Packet capture and network traffic analysis
Plaso / log2timeline	Timeline Analysis	Free / Open Source	Multi-source timeline reconstruction
Breadcrumbs.app	Crypto Tracing	Free tier + Pro	Blockchain transaction visualisation

NIGERIAN LEGAL FRAMEWORK FOR DIGITAL EVIDENC

LEGISLATION	RELEVANT PROVISIONS	INVESTIGATIVE SIGNIFICANCE
Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended 2024)	Sections 6–18: Computer-related offences; S.38: Interception of communications; S.45–46: Electronic evidence admissibility	Primary authority for cybercrime prosecution; defines computer-related offences and grants interception powers to designated agencies
Evidence Act 2011 (as amended)	Section 84: Admissibility of computer-generated evidence; S.258: Definition of document	Requires evidence to come from a computer 'used to store or process information' in the ordinary course of business; establishes reliability standard
EFCC (Establishment) Act 2004	Section 6: Investigative powers; S.13: Warrants for search and seizure	Grants EFCC authority to obtain digital evidence through search warrants
Nigeria Data Protection Act (NDPA) 2023	Data protection principles, lawful processing, security safeguards, and law enforcement exemptions.	Ensures digital evidence involving personal data is collected, processed, and shared lawfully while protecting privacy and maintaining public trust.
NCC Act/Subscriber Registration Regulations	Subscriber data obligations on telecoms; mandatory KYC records	Basis for lawful requests for subscriber identity, call records, and SIM registration data from MNOs
Mutual Legal Assistance Treaties (MLATs)	Bilateral treaties with US, UK, UAE, and others	Mechanism for obtaining evidence from foreign platforms and jurisdictions

MITRE ATT&CK FOR ATTRIBUTION AND TTPS

The MITRE ATT&CK framework provides a structured matrix for mapping adversary behaviour. For digital footprint investigations, the following techniques are most relevant:

ATT&CK Tactic	Technique ID	Digital Footprint Indicator
Reconnaissance	T1589 — Gather Victim Identity Information	Social media scraping; victim profiling artefacts; search query logs
Resource Development	T1583 — Acquire Infrastructure	WHOIS registration records; hosting provider logs; SSL certificate history
Initial Access	T1566 — Phishing	Email headers; domain lookalike registration; landing page server logs
Persistence	T1078 — Valid Accounts	Abnormal login timestamps; geolocation anomalies in authentication logs
Command & Control	T1071 — Application Layer Protocol	Unusual outbound traffic; beaconing patterns in network logs; encrypted channel metadata
Exfiltration	T1041 — Exfil Over C2 Channel	Volume anomalies; after-hours file access logs; large upload events in cloud storage logs
Impact	T1657 — Financial Theft	Fraudulent transaction records; beneficiary account data; cryptocurrency flows

PRACTICAL INVESTIGATION SCENARIO I

Scenario A: Tracing a Romance Fraud Syndicate via Social Media Footprint

Scenario Background: A victim reports sending4.2 million nairaover six months to a person presenting asaUSmilitary officer named “Colonel JamesMitchell” on Facebook. The account has since been deactivated. The victim has WhatsApp chat exports, and the suspect's phone number.

Investigation Steps

Preserve: Screenshotandarchive all available social media profile data; export WhatsApp chats; preservethephonenumber for further contact.

Phone Number Lookup: Use TrueCaller and HLR lookup tools to identify the registered subscriber and country of registration.

Reverse Image Search: Extract all photos shared by the suspect; run through Google Reverse Image SearchandPimEyes;identify stock photos or photos stolen from real persons.

Username Enumeration: If an email address or username is recovered from WhatsApp, run it through Sherlock to identify linked accounts on other platforms.

Financial Trace: Obtain beneficiary account details from the victim's bank; request transaction records viacourtorder;tracereceiving accounts through CBN-regulated financial intelligence.

MLAT/Platform Request: Submit preservation and disclosure request to Meta (Facebook) via law enforcementportal(transparency.meta.com), citing the Cybercrimes Act and applicable MLAT.

Build Link Chart: Mapall identified accounts, phone numbers, email addresses, and financial accounts to visualise the network.

PRACTICAL INVESTIGATION SCENARIO II

Scenario B: Cryptocurrency Fraud — Tracing a Wallet

Scenario Background: A corporate victim reportsthatan employee's email was compromised and 85 million nairaequivalent was diverted toa cryptocurrency wallet during a vendor payment. The BTC wallet address is known from the transaction record: bc1q[redacted].

Investigation Steps

- **Wallet Attribution:** Enterthe wallet address into Breadcrumbs.app or blockchain.com to view all transactions;identifyexchange deposit addresses.
- **Cluster Analysis:** UseChainalysis Reactor (if available via INTERPOL partnership) to identify co-spendingpatternsandlink wallets to known entities.
- **Exchange KYC Request:** Once a regulated exchange deposit is identified, submit a law enforcement requesttothe exchange for KYC records; include a court order.
- **Email Header Analysis:** Obtain the fraudulent emails from the victim's mail server; extract originatingIP addresses; geo-locate and cross-reference with ISP subscriber records.
- **Device Forensics:** Ifa suspect’s device is recovered, extract browser history, clipboard data, and cryptocurrency wallet appdata.

PRACTICAL INVESTIGATION SCENARIO III

Scenario C: AI-Assisted Analysis of BUSINESS EMAIL COMPROMISE

Scenario Background: TheEFCCreceives atipinvolvingasuspected BEC group that has targeted 14 companiesacrossthree states.Evidence includes847emailsacross 12 compromised accounts and 6TB of seized server data.

AI-Assisted Approach

- Ingestemaildatainto an NLP analysis pipeline (e.g., Autopsy with custom scripts, or a Python-based NLP tool using spaCy) to extract named entities: names, companies, bank accounts, phone numbers, addresses.
- Apply timeline analysis using Plaso/log2timeline to reconstruct the chronology of intrusions across all 12 accounts.
- Use graph analytics (Maltego or NetworkX) to identify common infrastructure: shared IP addresses, domain registrars, payment accounts used across multiple victims.
- Apply anomaly detection to identify the initial access event in each account, including the first login from an unusual IP or geolocation.
- Consolidate findings into a unified threat actor profile: TTPs mapped to MITRE ATT&CK, attributed infrastructure, and recommended attribution indicators.

RECOMMENDATIONS FOR NIGERIAN CYBERCRIME INVESTIGATORS I

For Individual Practitioners

- Obtain formal digital forensics certification (EnCE, GCFE, or CDFP) to establish professional competence in court.
- Develop OSINT skills through practical platforms such as TryHackMe (OSINT rooms), Bellingcat OSINT courses, and SANS FOR578.
- Maintain a personal tool kit with documented versions and validation records for all forensic software.
- Build relationships with telecom compliance teams and platform law enforcement portals for faster response to evidence requests.
- Stay current on cryptocurrency investigation techniques as financial crime increasingly migrates to blockchain.

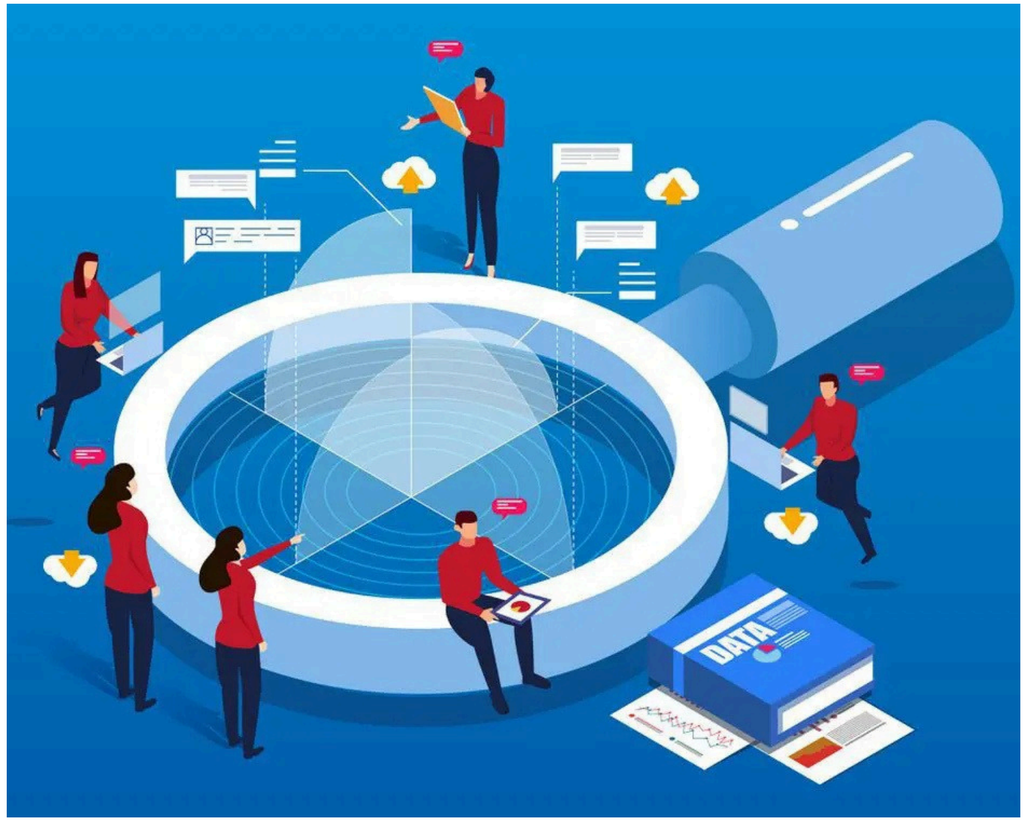
RECOMMENDATIONS FOR NIGERIAN CYBERCRIME INVESTIGATORS II

For Agencies and Institutions

- Establish a dedicated Digital Forensics Laboratory with write-blocked workstations, licensed forensic software, and secure evidence storage.
- Formalise data preservation and evidence handling Standard Operating Procedures aligned to ISO/IEC 27037 (Digital Evidence Collection).
- Pursue bilateral and multilateral data-sharing frameworks with major platform providers through the Ministry of Communications.
- Integrate MITRE ATT&CK-based threat intelligence into investigative workflows for structured attribution.
- Invest in AI-assisted analytics platforms through INTERPOL WACFC and international partnerships.

CONCLUSION

As Nigeria continues to evolve, with its large digital economy, sophisticated cybercrime ecosystem, and growing investigative capacity, the systematic exploitation of digital footprint evidence represents one of the highest-return investments available in national cyber resilience.



In the digital age, evidence does not simply disappear; it evolves. Our responsibility is to ensure that we have the capability, legal framework, and collaborative ecosystem required to uncover the truth hidden within digital footprints.

THANK YOU