EXPERT BRIEFING

Digital Evidence Lifecycle: From Collection to Adjudication

Desmond Israel, Esq. CISSP, CIPM

Desmond Israel, Esq
CISSP, CIPM, CC, CCT
Partner, AGNOS Legal Company
Lecturer, GIMPA Law School

PROFILE

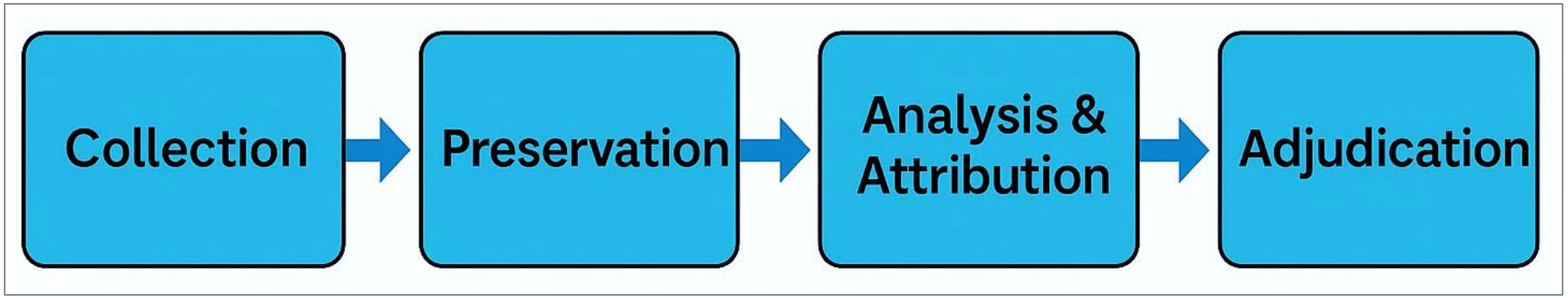
- **Partner (Cyberlaw and Technology Practice), AGNOS Legal Company**
- **Lecturer, GIMPA Law School**
- **Lead Consultant, Information Security Architects Ltd**
- **Training Consultant, National Banking College**
- **Non-Executive Director, Zerone Analytiqs (Canada)**
- **Member, EC-Council BETA Testing Committee (United States of America)**
- **Volunteer, ISC2 Exam Development**
- **Research Lead, XRSI Guardian Safety Framework (California)**
- **Former Research Fellow, Center for AI and Digital Policy (Washington DC)**
- **Alumni LLM’23, The George Washington Law School (Washington DC)**

OVERVIEW OF THE FULL VALUE CHAIN OF ELECTRONIC EVIDENCE

Context

- **Global Reality**: **90%+ of today's evidentiary traces**—text messages, GPS logs, CCTV, social media metadata, financial trails—are **electronic**.
- **African Trend**: From mobile money fraud to cyberbullying, digital evidence now underpins everything from high-tech crimes to mundane civil disputes.
- **Challenge**: Many courts remain **unprepared** to deal with the **technical complexity, volume, volatility, and verification** needs of digital evidence.

Relevance and Radiality = Admissible



Discussing the Lifecycle

Phase	Key Actors	Core Functions	Legal/Technical Risks
1. Collection	Police, Forensic Units	Seizure of digital devices, capturing logs, imaging of data	Insecure chain of custody, destruction/modification of data, lack of protocols
2. Preservation	Law enforcement, ISPs, Cloud Providers	Ensuring integrity via hash values, secure storage, metadata protection	Data volatility, storage abroad, unauthorized access
3. Analysis & Attribution	Digital forensic labs, cybercrime units	Recovering deleted files, correlating sources, identifying users	Errors in forensic analysis, misattribution, tool biases
4. Transmission & Disclosure	Police → Prosecution → Defence	Secure transfer, timely disclosure, protective orders	Withholding evidence, breaches of fair trial rights, lack of parity in access
5. Admissibility & Authentication	Prosecutors, Defence Lawyers	Establishing evidentiary standards, proving origin, reliability	Absence of legal standards, overreliance on presumption of authenticity
6. Evaluation by Judges/Jurors	Judges, Assessors, Magistrates	Weighing probative value, excluding prejudicial or irrelevant digital evidence	Limited digital literacy, undue deference to digital "truths"
7. Judicial Decision	Judiciary	Delivering rulings based on digital evidence	Decisions influenced by poor digital governance or technical confusion

Scenarios and Pitfalls

Scenario 1:
Device search without a warrant on suspicion of CSAM possession.

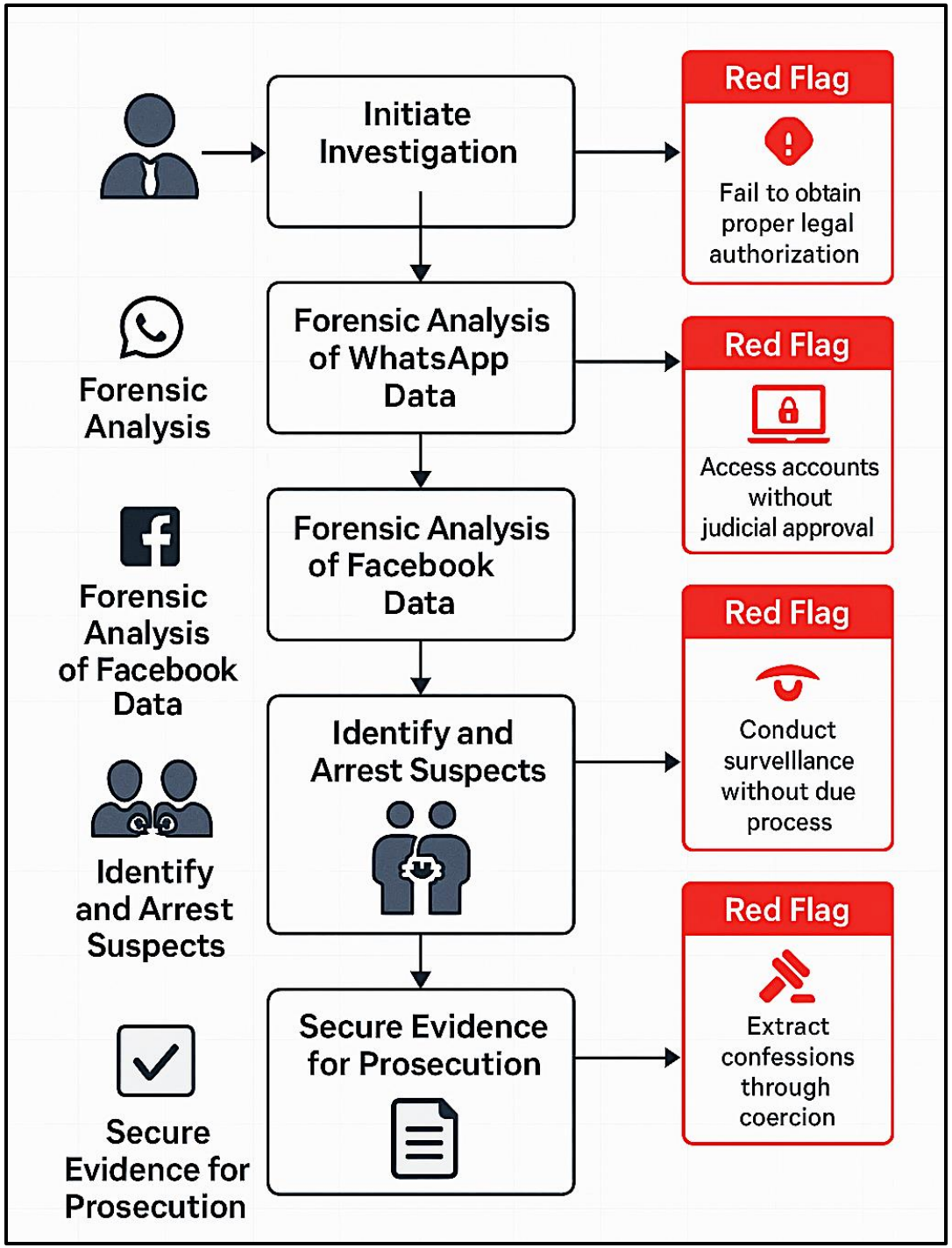
✅ Correct: Apply for High Court warrant under relevant law

❌ Wrong: Searching without judicial approval → evidence thrown out.

Scenario 3:
Interviewing a minor suspect alone, recording confession

✅ Correct: Legal rep present, psychologist support

❌ Wrong: Breach of Children's Act, Juvenile Justice Act → confession inadmissible



DEEP-DIVE :
LEGAL & TECHNICAL CONCERNS

Critical Technical & Legal Issues in Evidence Preservation – Example Email Forensics

Technical Issues:

- Altering timestamps or headers during export (e.g. MBOX conversion may drop metadata)
- Missing attachments if the viewer doesn't support embedded content
- Encoding errors (especially non-English characters)

Legal Issues:

- Emails are often private communications — **privacy laws may restrict review without warrants** or proper authorization.
- Chain of custody must prove **who accessed the mailbox and how exports were handled**.
- Courts may challenge authenticity if there's no evidence the emails weren't altered during extraction.

Best Practice:

- Export entire mailboxes in **native format** (e.g. PST, MBOX).
- **Hash exported files.**
- Document software used and extraction steps.

Show DEMO

The Legal and Evidentiary Issues (Admissibility, Authenticity, Preservation)

Admissibility Issues:

- **Statutory Gaps**: Many African Evidence Acts lag behind digital realities.
- **Judicial Discretion**: Over-reliance on judge's "common sense" to admit tech-based evidence.
- **Chain of Custody**: Frequently undocumented or improperly preserved.

Authenticity and Integrity:

- How do we verify a WhatsApp message or an image's source?
- Need for **digital hashing**, **time-stamping**, and **audit logs**.

Preservation Protocols:

- **Volatility** of digital records (deleted messages, auto-expiring data).
- Absence of **standard forensic preservation protocols** in local law enforcement.
- **Cloud storage and jurisdictional dilemmas**: Who preserves and where?

Legal and Technical Complexities in Practice

1

Device Seizure & Data Extraction:

- Inconsistent policies on phone/laptop seizures.
- Often violates right to privacy and due process.
- Lack of standard **search-and-seizure protocols** for digital devices.

2

Technological Gaps:

- Courts lack trained personnel and forensic tools.
- Police lack resources to extract, interpret, and explain metadata convincingly.
- **Dependency on third parties** (e.g., telcos, ISPs) with opaque cooperation regimes.

3

Cross-border Legal Inaccessibility:

- Electronic data often stored in **foreign jurisdictions** (e.g., US-based cloud providers).
- **MLATs** (Mutual Legal Assistance Treaties) are slow, bureaucratic, and underused.

Rights-Based Perspectives: Access, Fairness & Privacy

Right to Access Digital Evidence:

- Accused persons often denied **full access** to digital evidence used against them.
- Lack of **defence-side forensic capacity** creates evidentiary imbalance.

Due Process & Right to Fair Trial:

- Digital evidence is frequently **presented as infallible**, though prone to tampering.
- Judges must be equipped to **question reliability**, not just relevance.

Privacy and Proportionality:

- In surveillance and digital tracing, African police must balance **security with rights**.
- Legal frameworks for **data interception, retention, and destruction** must exist.

Legal Checklist and Q&A

✅ **Digital Rights Compliance Checklist:**

- ☐ Do you have a valid warrant?
- ☐ Was data collected under lawful grounds (consent, exemption, order)?
- ☐ Is chain of custody documented?
- ☐ Was the suspect's right to counsel observed?
- ☐ Is the victim/suspect treated with protective protocols?

Note: Without a warrant, evidence is likely **inadmissible**.

DEEP-DIVE:
PHASE CHALLENGES AND STRATEGIC RECOMMENDATIONS

Investigation Phase: Forensic Ground Zero

Challenges:

- **Lack of SOPs**: No unified standard for digital seizure, imaging, or documentation.
- **Low forensic literacy**: Police often mishandle devices, fail to document digital trails.
- **Third-party control**: Telcos/ISPs reluctant or slow to cooperate without MLATs.

Recommendations:

- Develop **National Digital Evidence Manuals**.
- Train first responders in **device seizure and triage**.
- Establish **fast-track cooperation protocols** with tech companies and telecoms.

Prosecution Phase: From Bits to Briefs

Challenges:

- Prosecutors struggle to **interpret digital reports**, reducing prosecutorial confidence.
- **Late or selective disclosure** of digital evidence affects **defence rights**.
- **Forensic expert shortages** result in weak or overburdened testimony.

Recommendations:

- Mandatory **digital evidence preparation training** for prosecutors.
- Create a **roster of accredited forensic experts** to support both sides.
- Encourage use of **electronic evidence pre-trial hearings** to test admissibility early.

Judicial Phase: From Admission to Verdict

Challenges:

- Judges face **technical overload**—limited tools to verify the authenticity or context of digital data.
- Risk of **digital determinism**: treating electronic data as inherently trustworthy.
- **Absence of case law consistency** or precedent guiding judicial evaluation.

Recommendations:

- Develop **judicial digital evidence toolkits** (checklists, benchmarks, questions).
- Build **digital bench books** with regional best practices and case digests.
- Incorporate **privacy and due process checklists** for evaluating digital surveillance-derived evidence.

CONCLUSION

Take-Aways: Prospects and Innovation Pathways

Judicial Innovation:

E-Court Platforms: Secure case management systems should embed digital evidence controls.

Digital Bench Books: Judicial guides on handling e-evidence should be institutionalized.

Capacity Building & Specialized Courts:

Establish **cybercrime benches** in national courts with trained judges and digital forensic liaisons.

Bar associations and **judicial colleges** must develop tailored CPD programs.

Standard-Setting and Harmonization:

Push for **Model African Framework** on digital evidence governance (possibly AU-led)

Encourage **inter-jurisdictional dialogue** among judges, police, and digital rights experts.

THANK YOU

+233244284133
www.desmondisrael.legal
desmond.israel@gmail.com