NATIONAL CYBERSECURITY WORKSHOP 2026

Practical Insights to

Real-Time Cyber Forensics

Threat Mitigation

Mr Emmanuel Livinus

Digital Forensics & Incident Response | AI-Augmented Cybersecurity

PROFESSIONAL TECH CONFERENCE

00:00 – 05:00 · HOOK

The Silent Crime Scene

> *"It's 3:14 AM. A notification fires. An unknown process is running on a domain controller. Eleven minutes later — 4,200 files have been encrypted."*

The question is not whether it will happen to your organisation.

The question is: will you be ready?

277 DAYS

average breach lifecycle — IBM 2024

The Numbers Don't Lie

277

DAYS

Average breach lifecycle
IBM Cost of Data Breach 2024

$4.88M

Average global cost
of a data breach — IBM 2024

68%

Breaches involve a
human element — Verizon DBIR

14s

A ransomware attack
occurs globally

⚠ *"We are not losing the cyber war because we lack technology. We are losing because the gap between when an attacker moves and when we notice is still measured in months — not minutes."*

Speed of response is the only real competitive advantage.

Core Concepts

Understanding DFIR

Digital Forensics (DF)

The science of collecting, preserving, analyzing, and presenting digital evidence in a legally admissible way.

Answers: What happened? When? Who? How?

FOUNDATION

Incident Response (IR)

The operational process of detecting, containing, eradicating, and recovering from a security incident.

Real-time and time-critical. IR without forensics is guessing.

OPERATIONAL

DFIR = DF + IR

Digital Forensics & Incident Response combined. You collect evidence WHILE you respond — ensuring legal admissibility AND speed of containment.

GOLD STANDARD

The Forensics Investigation Chain

Six Steps from Crime Scene to Courtroom

① **IDENTIFICATION**

Identify scope & evidence sources

② **PRESERVATION**

Secure & image without alteration

③ **COLLECTION**

Acquire with chain of custody

④ **EXAMINATION**

Filter & extract relevant artefacts

⑤ **ANALYSIS**

Reconstruct events & timelines

⑥ **REPORTING**

Present for legal / management action

⚡ Order of Volatility (RFC 3227): CPU Cache → RAM → Network State → Running Processes → Disk → Backup. Always collect in this order.

YOUR SIGNATURE FRAMEWORK

The TRACE Framework

Real-Time Digital Forensics & Incident Response

T

TRIAGE

Immediately scope the incident. What systems? What data? What timeframe? Who is affected?

R

RETRIEVE

Acquire evidence in order of volatility. RAM first. Disk image. Logs. Network captures.

A

ANALYZE

Use Autopsy, SIEM, and AI tools to extract and examine artefacts from each evidence source.

C

CORRELATE

Link artefacts across systems. Build the attack timeline. Identify patient zero and lateral movement.

E

ELIMINATE

Eradicate the threat, patch the vector, restore from clean backup, and document lessons learned.

25:00 – 30:00 · TRANSITION

From Theory to Tool

Why Autopsy DFIR?

- Industry-standard open-source DFIR platform
- Used by law enforcement, corporations & national agencies worldwide
- Free — the national gap is trained analysts, not cost
- Supports disk images, memory analysis, email extraction, web artefacts
- AI plugins available for automated malware classification

"What I'm about to show you is what a real investigation looks like."

30:00 – 45:00 · CENTREPIECE DEMO

LIVE: Autopsy DFIR Walkthrough

01 **Case Creation**
Chain of custody begins here
T

02 **Add Evidence Source**
Bit-for-bit forensic image + MD5/SHA hash verification
R

03 **Ingest Modules**
Deploy AI-powered analyst modules simultaneously
R

04 **Deleted File Recovery**
"The drive remembers what you forgot"
A

05 **Keyword Search**
Scan terabytes — every file, email, cache, chat log
A

06 **Timeline Analysis**
"That spike at 2:47 AM — they said they were asleep"
C

07 **Report Generation**
Court-ready. CEO-readable. CISO-actionable.
E

"What you just watched took ten minutes. A manual investigation of the same drive would take days."

Where AI Enters the Forensics Chain

What AI Does Well

- Ingests millions of log events per second
- Detects behavioural anomalies
- Auto-classifies malware families
- Correlates threat intelligence at scale

What Humans Do Better

- Contextual judgement & legal reasoning
- Novel attack pattern recognition
- Communicating findings to courts & boards
- Building trust with victims

AI-Augmented DFIR Stack

- Autopsy + AI plugins → evidence extraction
- Darktrace → network anomaly detection
- Microsoft Sentinel → SIEM correlation
- Human analyst → closes the case

"AI generates leads. Analysts close cases. AI is the world's fastest first responder — but you still need a detective."

Mapping Evidence to Adversary Behaviour

What is MITRE ATT&CK?

A globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

The forensic analyst's attack map.

How Forensics Uses It

Map evidence artefacts to ATT&CK techniques:
- Scheduled task → T1053
- PowerShell execution → T1059.001

You speak the same language as global threat intelligence.

AI + ATT&CK

Modern SIEM and XDR platforms auto-tag alerts with ATT&CK techniques using ML.

Analysts validate and enrich. AI does the tagging; humans do the thinking.

Reference: attack.mitre.org · NIST SP 800-86 · RFC 3227 · SANS FOR500: Windows Forensic Analysis

Where Does Your Organisation Stand?

LEVEL 1 · AD HOC

Reactive — No Playbooks

No documented procedures. Evidence often contaminated on arrival. Most organisations sit here.

LEVEL 2 · DEFINED

Playbooks Exist, Skills Are Patchy

IR playbooks documented. Some trained staff. Tools like Autopsy deployed but underutilised.

LEVEL 3 · MANAGED

DFIR Teams + AI-Assisted Tooling

Dedicated DFIR team. SIEM operational. Threat intel feeds. AI plugins. Response in hours, not days.

LEVEL 4 · OPTIMISED

Proactive, AI-Driven, Nationally Coordinated

Threat hunting. National CERT coordination. AI-driven SOC. Forensics evidence shared across agencies.

58:00 – 60:00 · CLOSING

Five Things That Must Land

01 Speed Is the Only Metric That Matters

02 Forensics = Legal Power

03 Autopsy Is Free. Skill Is Not.

04 AI Generates Leads. Analysts Close Cases.

05 TRACE Is Your Compass

What to Do This Week

Calls to Action — By Audience

Analysts & Practitioners

- Download Autopsy this week
- Load a practice image — digitalcorpora.org
- Complete one full TRACE walkthrough
- Join DFIR communities: SANS, BlueTeamLabs.online

CISOs & Managers

- Audit your IR playbook against TRACE
- Identify your current Maturity Level
- Budget one dedicated DFIR training cycle
- Establish chain-of-custody procedures now

Policymakers

- Advocate for a national DFIR training pipeline
- Push legal recognition of digital evidence chain-of-custody
- Fund national forensics lab capability
- Mandate AI-assisted SOC in critical infrastructure

"Every breach leaves a trail.

Your job — your duty —

is to be fast enough, skilled enough,

and equipped enough to follow it."

Mr Emmanuel Livinus

References & Resources

DATA SOURCES

- IBM Cost of a Data Breach Report 2024
- Verizon Data Breach Investigations Report (DBIR) 2024

FRAMEWORKS & STANDARDS

- MITRE ATT&CK Framework — attack.mitre.org
- NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response
- RFC 3227: Guidelines for Evidence Collection and Archiving

TOOLS & TRAINING

- Autopsy / The Sleuth Kit — sleuthkit.org / autopsy.com
- SANS FOR500: Windows Forensic Analysis · Digital Corpora — digitalcorpora.org
- BlueTeamLabs.online — DFIR community & challenges