DEVSECOPS 2025

How AI Enhances Digital Forensic Analysis and Evidence Collection

Speaker: **Victor Agboola**

Table of contents

DEVSECOPS 2025

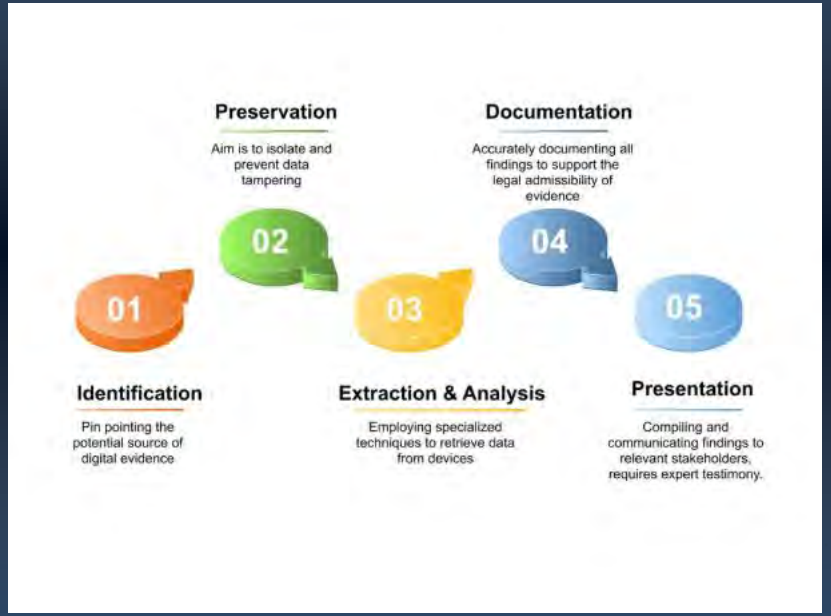
Purpose statement

Digital forensics meets AI exploring practical techniques, tools, and ethical frameworks for modern investigations.

DIGITAL FORENSICS MEETS AI

Digital evidence now spans mobile, computer, cloud, vehicles, and IoT devices creating unprecedented data volumes.

- **Data Volume Challenge:** 3–4 week backlogs in forensic labs
- **AI Augmentation:** Automates routine tasks, surfaces critical signals
- **Key Outcomes:** Faster triage, higher recall, defensible workflows



AI TECHNOLOGIES IN DIGITAL FORENSICS

Machine Learning

- Pattern recognition and anomaly detection in system logs, network traffic, and user behaviour
- Clustering algorithms for grouping similar artifacts and identifying attack campaigns
- Malware classification and attribution using supervised learning

Deep Learning

- Computer vision for image/video content analysis, facial recognition, and object detection
- Neural networks for malware behavior analysis and classification
- Advanced media forensics including tamper detection and source identification

Natural Language Processing (NLP)

- Entity extraction from emails, chats, documents
- Sentiment analysis for threat assessment

KEY APPLICATIONS & USE CASES

AI is revolutionizing digital forensics through automated analysis, pattern detection, and intelligent data processing across multiple domains.

Automated Evidence Triage
AI tools sift through terabytes of data to prioritize relevant evidence, reducing manual sorting time and focusing investigator attention on critical findings.

Media Analysis
Advanced neural networks analyze images and videos to detect explicit content, weapons, faces, and objects, enabling rapid categorization of visual evidence.

Network Traffic Analysis
Real-time AI monitoring of network traffic flags suspicious activities like data exfiltration, brute-force attacks, or lateral movement attempts.

Pattern Recognition
Machine learning models identify recurring patterns in cybercrime activities, including phishing campaigns, fraud schemes, and malware distribution networks.

Behavioral Analysis
AI monitors user behavior patterns to detect anomalies indicating insider threats, unauthorized access, or suspicious account activities.

Data Recovery
Deep learning models like Carve-DL reconstruct fragmented files from damaged storage devices, achieving up to 85% clustering accuracy in recovery efforts.

AI-POWERED TOOLS & PLATFORMS

Leading forensic platforms integrate AI to accelerate investigations while maintaining evidence integrity and chain of custody.

Cellebrite Pathfinder/Autonomy
- Automated ingestion and case graphing
- Parallel device processing
- AI-driven evidence correlation

Magnet Griffeye
- Specialized AI for media analysis
- CSA detection, facial recognition, object identification

Magnet Copilot
- AI assistant surfacing high-priority evidence
- Provides contextual recommendations for investigators

Magnet Axiom
- Artifact-first AI with NLP for communications analysis
- Automated artifact identification and extraction

Belkasoft X with BelkaGPT
- LLM-powered analysis of case artifacts
- Cloud, mobile, and computer forensics with grounded summaries

Other Platforms
- ADF Digital Evidence Investigator
- OSINT tools like Maltego for link analysis and automated workflows

BENEFITS & IMPACT

Survey-backed results from Cellebrite's 2025 Industry Trends Survey across 97 countries show overwhelming positive perception of AI in digital forensics.

90%
Positive impact on investigations

86%
Faster data analysis

82%
Automates repetitive tasks

61%
View AI as a valuable tool

51%
Plan AI adoption within 2 years

64%
Believe AI reduces crime

- Reduces 3–4 week forensic backlogs through automated processing
- Improves consistency across investigations with standardized AI workflows
- Enables teams to scale capacity without increasing headcount
- Enhances defensibility of evidence through reproducible AI analysis

REAL-WORLD IMPLEMENTATION

AI-powered forensic tools are transforming investigations across law enforcement, demonstrating measurable improvements in case resolution times and evidence discovery.

Law Enforcement Automated Triage

- AI systems automatically process and prioritize evidence from multiple devices, reducing case backlog from 3-4 weeks to days. Automated triage identifies high-priority artifacts from immediate investigator review.

Impact: Up to 75% time reduction

CSAM Detection Workflow

- AI-assisted detection tools rapidly identify potential child sexual abuse material, reducing investigator exposure while maintaining accuracy. Automated classification exports results to specialized analysis tools.

Impact: 95% accuracy in detection

Data Recovery with Deep Learning

- Deep learning models like Carve-DL reconstruct fragmented files from damaged storage devices. Supportive Clustering with Contrastive Learning achieves ~85% clustering accuracy in recovery efforts.

Impact: ~85% clustering accuracy

CHALLENGES & ETHICAL CONSIDERATIONS IN AI

- **Bias & Fairness:** AI models can inherit biases from training data. Robust validation and diverse datasets are needed to ensure equitable outcomes across demographic groups.
- **Privacy & Legality:** AI processing must comply with data protection laws, warrant requirements, and cross-border regulations while respecting individual privacy rights.
- **Explainability & Auditability:** AI decisions must be transparent and reproducible, maintaining chain of custody and enabling court-admissible evidence with clear documentation.
- **Reliability & Hallucination:** AI outputs must be cross-validated against source evidence to mitigate false positives and ensure investigative accuracy.
- **Governance & Oversight:** Responsible AI deployment requires established policies, regular audits, and human oversight.
- **Human Expertise:** AI should enhance not replace human investigators, preserving the critical role of intuition, context, and ethical judgment in complex cases.

FUTURE TRENDS IN AI FORENSICS

- **LLM Copilots Embedded** AI assistants integrated across DFIR workflows for grounded analysis of case artifacts
- **Automated Cloud Forensics** Multi-cloud timeline reconstruction with automated evidence capture
- **IoT & Vehicle Forensics** Expanding data sources from drones, smart vehicles, and IoT devices
- **Counter Anti-Forensics** Advanced detection of tampering, steganography, and data manipulation
- **Standardized Automation** Pipeline-based workflows for consistent, scalable investigations
- **Training at Scale** Addressing personnel gaps through AI-powered education and upskilling

Key Takeaway

Pair AI speed with human judgment for defensible outcomes—technology amplifies expertise, never replaces it.

Thanks!

Do you have any questions?

agboolavictor367@gmail.com

Victor Agboola