BASIRAT A. **AKINTUNDE**

basirataakintunde@gmail.com | linkedin.com/in/basirat-akintunde | ceo.mideaybrownie.com

Security+ certified digital forensics and cybersecurity professional with a MBA in Cybersecurity in progress and hands-on experience in evidence acquisition, file system and mobile forensics, network traffic analysis, and incident response support.

EDUCATION & CERTIFICATIONS

CompTIA Security+ | *Certified **2026*** Gained skills in threat analysis, vulnerability management, network security, identity and access management, risk management, incident response, security operations, and cryptography

M.B.A in Cybersecurity and Organizational Resilience ***2026-2027*** University of Baltimore
Notable Coursework: Principles of Information Security Management, Information Security & Business Continuity, IT for Business Transformation, Business Analytics, Visual Business Intelligence, Strategic Management, Corporate Finance, Financial Statement Analysis & Management Control, Operations & Supply Chain Management, Organizational Behavior for Leaders

B.Sc in Digital and Cyber Forensic Science ***2023 – 2025*** University of Baltimore
Notable Coursework: Digital Forensics & Cybercrime Investigation, Computer Forensics, Mobile Device Forensics, Network Forensics, Digital Evidence Acquisition & Analysis, Cybersecurity & Information Security, Computer Networks, Operating Systems & Linux, Database Systems & SQL, Incident Response, Malware Analysis, Cybercrime & Digital Law

A.A.S in Cybersecurity ***2021 – 2023*** Prince George's Community College
Notable Coursework: Network Access Control, Advanced Network Security, Linux Administration, Cybersecurity Operations, Systems Analysis & Project Management

CORE SKILLS

Operating Systems: Windows, MacOS, Linux
Tools: Wireshark, Autopsy, Magnet AXIOM, FTK Imager, Paraben, VMware, VirtualBox, PowerShell
Relevant: Evidence Acquisition & Preservation, Forensic Imaging, Chain of Custody, Cryptographic Hashing, SIEM Monitoring, Windows & Registry Analysis, Browser Artifact Analysis, Timeline Analysis, Mobile/Android Forensics, Incident Response, Security Log Analysis, Network Traffic Analysis, Active Directory, Technical Documentation

EXPERIENCES

Operations Supervisor: Tireco Distributors, Jessup, Maryland ***2025 – 2026*** • Investigated discrepancies across customer accounts, orders, payments, returns, and credits, tracing root causes and escalating issues for corrective action. • Recovered approximately $20,000 in uncollected revenue within three months through detailed transaction research and account analysis in NetSuite. • Handled sensitive customer, financial, and operational data while maintaining confidentiality and company data-handling procedures.

IT Intern: Maryland Department of Environment, Baltimore, Maryland ***2024 – 2025*** • Supported IT security operations in a large-scale environment: applied cybersecurity policies and chain of custody procedures and configured backup infrastructure tools to strengthen device security.
• Led the policy audit for the new administrative year and contributed to the agency's updated disaster recovery plan for the fiscal year. • Extracted and analyzed data from SQL Server databases and contributed to automated analytics processes.
• Built workflows, reports, and dashboards in Smartsheet and interactive Power BI visualizations to support data-driven infrastructure decisions. • Installed and configured software, reimaged Dell laptops, and set up workstations to user requirements.

PROJECTS

Digital Forensics Investigation — Case-001: DomexUsers
Autopsy | *FTK Imager* | *SHA-1* | *Timeline Analysis* | *Evidence Correlation*

- Conducted a structured forensic examination of a digital evidence image using industry-standard forensic analysis techniques. • Verified evidence integrity using cryptographic hashing and documented acquisition and examination procedures.
- Analyzed filesystem artifacts, timestamps, and forensic evidence to establish relevant investigative findings.

Mobile Device Forensics Investigation — Black Box Case Study (In progress)
Open-Source Forensic Tools | *Android Forensics* | *Artifact Analysis* | *Timeline Analysis*

- Conducting a simulated criminal investigation using a realistic mobile-device forensic dataset.
- Examining mobile artifacts including communications, application data, device activity, and timestamps.
- Developing an evidence-driven investigative timeline and documenting findings according to forensic reporting practices.

Android Mobile Forensics Examination
Android Forensics | *Evidence Analysis* | *Forensic Reporting*

- Analyzed Android-device evidence as part of a mobile forensics laboratory investigation.
- Examined digital artifacts and documented relevant investigative findings using forensic examination procedures.