CA201: Digital Forensic and Incident Response

18 Instructional Hours 27 CPEs 9 Labs

LIVE ONLINE OR ON-DEMAND ACCESS OR IN PERSON

BEGINNER / INTERMEDIATE

This course provides a comprehensive, hands-on introduction to Digital Forensics and Incident Response (DFIR), focusing on the structured identification, collection, analysis, and preservation of digital evidence within modern security operations. It covers both foundational and advanced concepts, including detection and triage, incident response lifecycle, evidence acquisition, host and memory forensics, threat intelligence integration, and real-world investigation workflows. Learners are guided through practical methodologies used in enterprise environments, emphasizing analytical reasoning, evidence correlation across systems, and defensible decision-making during active security incidents.

You Will Be Able To

- Conduct structured digital investigations from alert triage to full incident reconstruction
- Acquire, preserve, and validate digital evidence while maintaining chain of custody
- Analyze host, disk, and memory artifacts to identify attacker behavior
- Apply threat intelligence and MITRE ATT&CK to guide investigations and detection
- Perform incident response activities including containment, eradication, and recovery
- Correlate multi-source evidence (endpoint, network, identity, cloud) to build attack timelines

Who Should Attend

This course is designed for students and cybersecurity professionals with a foundational understanding of security concepts who want to specialize in DFIR. It is suitable for aspiring incident responders, SOC analysts, and digital forensic practitioners seeking practical, real-world skills in investigating and responding to cyber incidents. It is also valuable for professionals transitioning into blue team roles or aiming to deepen their investigative and analytical capabilities.

Relevant Combat Roles

- SOC Analyst (Tier 1–3)
- Incident Responder
- Digital Forensic Analyst
- Threat Hunter
- Cyber Threat Intelligence Analyst
- Security Operations Engineer

Topics Covered

DFIR Basics: Mindset, workflows, SOC roles

Detection & Intel: Triage, ATT&CK, threat intelligence

Incident Response: Lifecycle, containment, recovery

Forensics & Evidence: Collection, validation, analysis

Threat Analysis: Malware, phishing, lateral movement

Advanced & Reporting: Hunting, automation, reporting

Labs

DFIR Lab Environment Design & Setup
(virtual machines, logging pipelines, Autopsy, FTK Imager, and Volatility setup)

Disk Forensics & Evidence Analysis
(forensic imaging, deleted file recovery, file-system artifact analysis, and SleuthKit/Autopsy investigations)

Incident Triage & Investigation Operations
(alert triage, affected system scoping, attacker activity reconstruction, and telemetry analysis)

Memory Forensics & Timeline Reconstruction
(RAM capture, Volatility analysis, process investigation, anomaly detection, and attack timeline creation)

Digital Forensics & Memory Analysis
(Volatility, Autopsy, Foremost, Windows artifacts, and memory forensics)