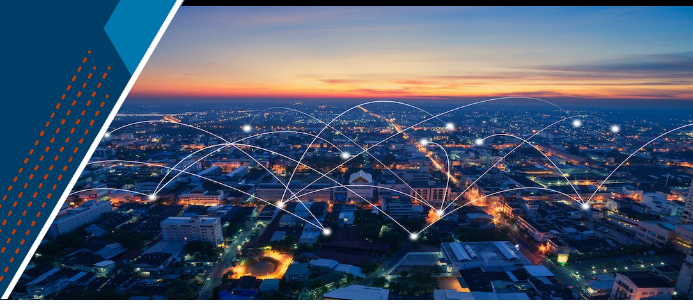
DIGITAL FORENSICS PATHWAY



DIGITAL FORENSICS PATHWAY

The **Digital Forensics Pathway** is a comprehensive 4-week, instructor-led cybersecurity training course designed to develop expertise in conducting thorough and legally sound digital investigations. Starting with foundational forensic concepts, participants progress through device-level, network, and cloud forensics while gaining hands-on experience with professional tools and techniques. The course emphasizes proper evidence handling, chain of custody, and analysis methodologies across various digital platforms. By completion, students gain introductory skills to conduct comprehensive forensic investigations, document findings professionally, and adapt to emerging forensic challenges in hybrid environments, all while maintaining legal and ethical compliance.

KEY LEARNING OUTCOMES

- Apply core cybersecurity principles to digital forensic investigations
- Analyze Windows system artifacts for forensic evidence
- Capture and analyze network traffic using Wireshark
- Conduct forensic investigations in cloud environments

CAREER OPPORTUNITIES RELATED TO THIS SUBJECT

- Digital Forensics Investigator
- Incident Response Analyst
- Computer Crime Investigator
- Forensics Consultant
- eDiscovery Specialist
- Law Enforcement Digital Forensics Expert
- Corporate Forensics Analyst
- Cybersecurity Investigator

PATHWAY METRICS

- Course Duration: 4-Weeks (160 hours)
- CPE Credits: 160
- Certification: EC-Council Computer Hacking Forensic Investigator (CHFI)

This document is marked TLP:CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp.

PROFICIENCY LEVEL: ENTRY-LEVEL CYBERSECURITY PROFESSIONAL

Participants should have a solid foundational understanding of basic IT and cybersecurity principles. Participants do not need prior hands-on experience in digital forensics, but they should have a basic understanding of operating systems, and networks. The course builds on foundational forensic knowledge and progresses through increasingly complex concepts and practical applications in analysis techniques for devices, networks, and cloud environments.

Although this course is open to entry-level professionals, it includes hands-on practice, lab exercises, and real-world simulations, offering more advanced professionals the opportunity to further refine their skills and core competencies in practical scenarios.

TARGET AUDIENCE

This pathway is designed for individuals interested in developing practical, hands-on skills in digital forensics and cyber investigations. It is ideal for:

- Aspiring digital forensic analysts, incident responders, or cybersecurity investigators
- IT and cybersecurity professionals looking to expand into forensics and evidence analysis
- Law enforcement or military personnel supporting cybercrime investigations
- Government personnel involved in audits, internal investigations, or SOC operations

RECOMMENDED PREREQUISITES

While the prerequisites listed are recommended to help you successfully complete the course, they are not mandatory. If you are confident in your skills and capabilities and can dedicate the time needed to fully engage in the training material, we encourage you to apply. All Pathway courses are live instructor-led to help facilitate learning and skill development for participants across broad skill levels.

To ensure readiness for the hands-on technical aspects of the course, participants should ideally have the following exposure and proficiencies prior to enrolling:

- Basic proficiency with computers and operating systems (Windows/Linux), command-line navigation, and general understanding of file systems, folders, and application usage.
- Basic understanding of IT systems, including patch management, software updates, and common misconfigurations. *No prior experience in system hardening, vulnerability scanning, or deep operating systems knowledge is needed.*
- Familiarity with basic cybersecurity concepts including the CIA triad (confidentiality, integrity, availability), basic threat types (i.e., malware, phishing), software patching, and high-level understanding on security vulnerabilities.
- Comfort using basic command-line, including directory navigation, file operations, user commands, and introductory scripting capabilities. *No automation or tool-specific experience is required; however, it may be advantageous during training in lab environments*
- Comfort with technical tools and digital environments, including using a web browser, basic system configuration, and following multi-step technical instructions. *Students will be guided through forensic tool installation and usage during labs.*
- Familiarity with the concept of evidence or documentation, particularly in regulated or security-sensitive environments. *Legal and procedural content is introduced in Week 1, including a chain of custody and compliance.*

DIGITAL FORENSICS COURSE OUTLINE

Week 1: The Foundation Week: *A comprehensive introduction to digital forensics fundamentals, combining legal frameworks and evidence handling protocols with hands-on experience in forensic workstation setup and preliminary investigations through supervised lab exercises.*

Week 1 Learning Outcomes:

- Apply core cybersecurity principles to digital forensic investigations
- Implement proper evidence handling procedures following legal requirements
- Set up and configure a forensic workstation with essential tools
- Create and verify forensic images using industry-standard tools
- Document chain of custody procedures accurately
- Conduct preliminary file system analysis while maintaining evidence integrity
- Demonstrate proper documentation methods for digital investigations
- Explain the legal framework governing digital forensics
- Apply basic forensic methodology to preliminary investigations
- Validate forensic tool installations and configurations

Week 2: The Device Deep Dive: *An intensive exploration of device-level forensics across multiple platforms, focusing on operating system artifacts, mobile device analysis, and memory forensics through hands-on practice with professional tools.*

Week 2 Learning Outcomes:

- Analyze Windows system artifacts for forensic evidence
- Extract and interpret Linux system forensic data
- Perform macOS-specific forensic analysis
- Conduct mobile device data acquisition for iOS devices
- Execute Android forensic procedures and analysis
- Capture and analyze volatile memory data
- Use memory forensics tools like Volatility effectively
- Cross-reference findings across multiple operating systems
- Reconstruct user activities from system artifacts
- Document platform-specific forensic findings professionally

Week 3: The Network Navigator: *A practical immersion in network forensics and complex investigations, combining traffic analysis and attack investigation through realistic scenarios and professional tools.*

Week 3 Learning Outcomes:

- Capture and analyze network traffic using Wireshark
- Interpret network protocols for forensic investigation
- Investigating network-based attacks including DDoS
- Analyze wireless network traffic for evidence
- Reconstruct network-based incidents
- Implement network logging and monitoring solutions
- Detect and analyze man-in-the-middle attacks
- Create timeline analysis of network events
- Generate comprehensive network forensic reports

Week 4: The Cloud Capstone: *An advanced study of cloud forensics and emerging technologies, integrating certification preparation with practical experience in hybrid environment investigations through comprehensive projects.*

Week 4 Learning Outcomes:

- Conduct forensic investigations in cloud environments
- Apply forensic techniques across
- different cloud service models
- Analyze IoT devices for digital evidence
- Investigating cryptocurrency-related incidents
- Prepare for professional forensic certifications
- Execute integrated forensic investigations in hybrid environments
- Present forensic findings to technical and non-technical audiences
- Develop comprehensive forensic investigation reports
- Implement emerging forensic investigation techniques
- Demonstrate mastery through capstone project completion