**Course Introduction:**

This course provides a comprehensive understanding of digital forensics, focusing on methodologies, tools, and practices necessary to conduct effective cybersecurity investigations. Through 20 in-depth modules, learners will develop the skills to collect, preserve, analyze, and report digital evidence across multiple domains including cloud, mobile, and network forensics. The course emphasizes hands-on training with real-world case scenarios, covering the latest industry techniques and anti-forensic methods.

---

**Course Objectives:**

1. Understand the fundamental principles of digital forensics and cybersecurity.
2. Develop skills to handle and process digital evidence in compliance with legal standards.
3. Learn to investigate cyber incidents across various operating systems (Windows, Linux, Mac) and platforms (cloud, mobile, IoT).
4. Gain proficiency in using forensic tools to detect, analyze, and counter cyber threats.
5. Acquire knowledge of forensic methodologies applicable to malware, web applications, and network traffic analysis.
6. Master modern forensic techniques for emerging technologies such as cloud platforms (AWS, Azure, GCP) and IoT devices.
7. Prepare learners to obtain a globally recognized digital forensics certification (C|HFI).

---

**Target Audience:**

- IT Professionals in cybersecurity roles
- Incident Response Teams (IRTs)
- Digital Forensic Analysts and Investigators
- Law Enforcement Personnel involved in cybercrime investigations
- Cybersecurity Consultants and Ethical Hackers
- Network and Security Administrators

---

**Course Pre-requisites:**

- Basic understanding of computer systems and networks.
- Familiarity with IT/cybersecurity concepts and operating systems (Windows, Linux, Mac).

- Knowledge of cyber threats and incident response strategies is advantageous but not mandatory.

**Course Duration:** 40 Hours (20 Modules & 20 Sessions)

**Introduction to Digital Forensics**

- Definition and importance of digital forensics.
- The role of digital forensics in cybersecurity.
- Legal and ethical considerations.
- Types of digital forensics (computer, mobile, network).
- Key challenges in digital forensics investigations.

**Computer Forensics in Today's World**

- Current cybercrime trends and statistics.
- The importance of forensic readiness for organizations.
- Cyber incident case studies.
- Regulatory compliance (ISO 27001, PCI DSS, HIPAA).
- Tools and technologies used in digital forensics.

**Digital Forensics Investigation Process**

- Phases: Identification, preservation, acquisition, analysis, reporting.
- Chain of custody and evidence handling.
- Documentation and reporting techniques.
- Legal admissibility of digital evidence.
- Best practices for conducting investigations.

**Understanding Hard Disks and File Systems**

- Disk types: HDD, SSD, and storage systems (RAID, NAS).
- File system types (FAT, NTFS, ext4, HFS).
- Disk partitioning and boot processes.
- File system analysis tools.
- Recovering deleted data from file systems.

**Data Acquisition and Duplication**

- Imaging techniques (physical vs. logical acquisition).

- Tools for data acquisition (FTK Imager, EnCase).
- Best practices for maintaining evidence integrity.
- Handling encrypted or damaged storage devices.
- eDiscovery and preparing evidence for examination.

**Defeating Anti-Forensics Techniques**

- Common anti-forensics methods (data wiping, steganography).
- Tools to detect and counter anti-forensics techniques.
- Identifying modified or deleted log files.
- Analyzing obfuscated data.
- Case studies on defeating anti-forensic methods.

**Windows Forensics**

- Acquiring volatile and non-volatile data from Windows systems.
- Analyzing Windows registry, memory, and event logs.
- Forensic analysis of artifacts (ShellBags, LNK files).
- Application forensics (Electron apps, web browsers).
- Windows-specific forensic tools (Volatility, Autopsy).

**Linux and Mac Forensics**

- Differences in file system structures (EXT, HFS+).
- Acquiring and analyzing memory and disk data on Linux/Mac.
- Key artifacts in Linux (log files, bash history).
- Mac-specific forensic artifacts (Spotlight, Time Machine).
- Tools for Linux and Mac forensics (Sleuth Kit, mac_apt).

**Network Forensics**

- Capturing and analyzing network traffic (Wireshark, tcpdump).
- Identifying Indicators of Compromise (IOCs) in network logs.
- Network intrusion detection and event correlation.
- Investigating DNS and HTTP traffic anomalies.
- Wireless network forensics (WiFi security and attacks).

**Malware Forensics**

- Static and dynamic malware analysis techniques.
- Identifying malware behavior through sandboxing.
- Ransomware analysis and forensic response.
- Network behavior analysis of malware.
- Case studies on notable malware incidents.

**Web Application Forensics**

- Investigating web application vulnerabilities (SQL injection, XSS).
- Analyzing web server logs (Apache, IIS).
- Tools for web application forensics (Burp Suite, OWASP ZAP).
- Forensic techniques for web shells and code injections.
- Case study: Investigating a web-based cyberattack.

**Dark Web Forensics**

- Understanding the dark web and its use in cybercrime.
- Investigating Tor browser activity.
- Analyzing memory dumps for dark web artifacts.
- Investigating illegal dark web activities (drug trafficking, hacking).
- Tools and techniques for tracking dark web communications.

**Cloud Forensics**

- Challenges in cloud-based investigations.
- Forensic methodologies for AWS, Azure, and GCP.
- Acquiring data from cloud storage (S3 buckets, Blob storage).
- Investigating virtual machines and containers in the cloud.
- Legal and jurisdictional issues in cloud forensics.

**Email and Social Media Forensics**

- Investigating email fraud, phishing, and Business Email Compromise (BEC).
- Analyzing email headers and metadata.
- Social media forensic techniques (Facebook, Twitter, Instagram).
- Tools for social media analysis and evidence extraction.
- Case studies: Email scams and social media fraud.

**Mobile Forensics**

- Mobile OS architecture (Android, iOS).
- Logical and physical acquisition techniques for mobile devices.
- Analyzing mobile data (SMS, call logs, location data).
- Mobile forensics tools (Cellebrite, Oxygen Forensic Suite).
- Investigating mobile app data and cloud sync artifacts.

**IoT Forensics**

- Challenges of investigating Internet of Things (IoT) devices.
- Acquiring data from smart devices and wearables.
- Investigating security breaches on IoT networks.
- Forensic tools for IoT device analysis.
- Case study: Investigating an IoT-based cyber attack.

**Advanced Malware Forensics**

- Analyzing advanced persistent threats (APTs).
- In-depth analysis of recent malware like BlackCat (ALPHV).
- Reverse engineering malware to identify behavior and origin.
- Investigating zero-day exploits and advanced obfuscation techniques.
- Malware detection and mitigation strategies.

**Python Scripting for Forensics**

- Automating digital forensic tasks with Python.
- Writing scripts for data extraction and analysis.
- Using Python for log file parsing and report generation.
- Tools and libraries (Py2exe, Scapy).
- Case study: Custom scripting for a forensic investigation.

**Defeating Anti-Forensic Techniques**

- Investigating attempts to hide or erase digital evidence.
- Techniques for uncovering hidden partitions or files.
- Forensic analysis of Windows ShellBags and jump lists.
- Tools for detecting deleted or altered data (X-Ways Forensics).

- Case study: Successful detection of anti-forensic methods.

**Final Project and Case Study**

- Conducting a full-scale forensic investigation.
- Analyzing evidence from a real-world cyber incident.
- Preparing and presenting forensic reports.
- Cross-platform investigation (Windows, Linux, mobile, cloud).
- Simulated incident response and evidence submission.