Cyber Crime Investigation and Digital Forensics Training Course



19 - 23 Oct 2026

Cairo

3700 € (Per Person)

Ref: #CYB7171_272383

Course Introduction / Overview:

In an era where digital footprints are ubiquitous, the ability to investigate and respond to cybercrime is more critical than ever. This course provides a comprehensive exploration of digital forensics and cybercrime investigation, designed to equip participants with the essential skills to navigate the complex landscape of digital evidence. Drawing upon foundational principles outlined by experts like Eoghan Casey in his seminal work, "Digital Evidence and Computer Crime," this program delves into the systematic processes of evidence acquisition, analysis, and reporting. Participants will learn to maintain the integrity of the chain of custody, a cornerstone of any successful investigation. BIG BEN Training Center has meticulously structured this curriculum to bridge the gap between theoretical knowledge and practical application, covering everything from hard drive and mobile device forensics to advanced network and cloud investigations. This training is not just about learning to use tools; it is about developing an investigative mindset, understanding the legal and ethical frameworks, and preparing to present findings in a clear, defensible manner. By the end of this intensive five-day program, attendees will be proficient in the methodologies required to uncover digital trails and effectively combat cyber threats.

Target Audience / This training course is suitable for:

- IT Security Professionals.
- Law Enforcement Officers and Detectives.
- Digital Forensic Analysts.
- Incident Response Team Members.
- Cybercrime Investigators.
- Corporate Security Managers.
- Legal Professionals and Paralegals.
- System and Network Administrators.
- Compliance and Audit Professionals.
- Government and Intelligence Agency Personnel.

Target Sectors and Industries:

- Banking and Financial Services.
- Information Technology and Telecommunications.
- Healthcare and Pharmaceutical.
- Government, Law Enforcement, and Public Safety.
- Legal and Professional Services.
- Retail and E-commerce.
- Energy and Utilities.
- Consulting and Corporate Investigation Firms.

Target Organizations Departments:

- Information Technology (IT) and Information Security.
- Internal Audit and Corporate Investigations.
- Legal and Compliance Departments.
- Risk Management.
- Human Resources.
- Incident Response and Security Operations Center (SOC).
- Corporate Security and Loss Prevention.
- Fraud Prevention and Investigation Units.

Course Offerings:

By the end of this course, the participants will have able to:

- Master the fundamental principles of digital forensics and cybercrime investigation.
- Properly acquire and preserve digital evidence from various sources while maintaining the chain of custody.
- Conduct in-depth forensic analysis of computer systems, file systems, and operating systems.
- Investigate network-based incidents by analyzing network traffic and logs.
- Perform forensic examinations on mobile devices, including both iOS and Android platforms.
- Understand the legal and ethical considerations surrounding digital investigations.
- Effectively document findings and prepare comprehensive forensic reports.
- Analyze common malware types and understand their behavior.
- Explore forensic techniques for cloud-based environments and IoT devices.
- Develop the skills to potentially serve as a knowledgeable witness in legal proceedings.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be highly interactive, immersive, and practical, ensuring participants gain tangible skills. This course moves beyond traditional lectures by integrating hands-on laboratory exercises that simulate real-world cybercrime scenarios. Participants will work with industry-standard forensic tools and techniques in a controlled environment, allowing them to apply theoretical concepts directly. The curriculum is heavily reliant on case studies drawn from actual digital investigations, providing context and demonstrating the complexities of forensic analysis. Collaborative group work and peer-to-peer discussions are encouraged to foster a dynamic learning environment where diverse perspectives can be shared. Our expert instructors facilitate sessions that include interactive Q&A, practical demonstrations, and continuous feedback to guide participants through challenging topics. The program emphasizes a problem-solving approach, where attendees are tasked with analyzing evidence, identifying threats, and constructing a coherent narrative of events, thereby building not just technical proficiency but also critical thinking and analytical skills essential for a successful career in digital forensics.

Course Agenda (Course Units):

Unit One: Foundations of Digital Forensics and Cybercrime

- Introduction to Digital Forensics and Investigation.
- Understanding Different Types of Cybercrime.
- The Digital Forensic Investigation Process and Methodologies.
- Legal and Ethical Principles in Digital Investigations.
- The Importance of the Chain of Custody.
- Setting Up a Forensic Workstation and Toolkit.
- Introduction to Digital Evidence Categories.

Unit Two: Computer and File System Forensics

- Understanding Hard Drives and Digital Storage Media.
- In-depth Analysis of FAT, NTFS, and Ext File Systems.
- Data Acquisition Techniques and Disk Imaging.
- Forensic Analysis of Windows, macOS, and Linux Systems.
- Recovering Deleted Files and Data Carving Techniques.
- Windows Registry Forensics and Artifact Analysis.
- Keyword Searching and Data Indexing Strategies.

Unit Three: Network and Internet Forensics

- Fundamentals of Network Protocols and Architecture.
- Analyzing Network Traffic with Tools like Wireshark.
- Investigating Web Browser History, Cache, and Cookies.
- Email Forensics and Tracing Email Origins.
- Social Media and Online Communication Investigation Techniques.
- Log Analysis from Firewalls, Routers, and Servers.
- Introduction to Open-Source Intelligence (OSINT) Gathering.

Unit Four: Mobile, Cloud, and IoT Forensics

- Introduction to Mobile Device Forensics (iOS and Android).
- Logical, File System, and Physical Acquisition of Mobile Data.
- Analyzing Call Logs, Messages, and Application Data.
- Fundamentals of Cloud Computing and its Forensic Challenges.
- Techniques for Acquiring and Analyzing Data from Cloud Services.
- Introduction to Internet of Things (IoT) Forensics.
- Investigating Smart Devices and Wearable Technology.

Unit Five: Advanced Forensics and Incident Response

- Introduction to Malware Analysis and Reverse Engineering.
- Memory Forensics (RAM Analysis) Techniques.
- Steganography and Steganalysis Concepts.
- Cryptocurrency and Blockchain Investigation Basics.
- Compiling Findings and Writing Effective Forensic Reports.
- Presenting Digital Evidence in a Courtroom Setting.
- Capstone Project: A Simulated Cybercrime Investigation.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

As digital forensics tools become increasingly automated, what is the evolving role of human intuition and critical thinking in cybercrime investigation?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by focusing on the development of an investigative mindset rather than mere proficiency with software tools. While participants will gain hands-on experience with industry-standard technology, the core emphasis is on the underlying forensic principles and critical thinking skills that are tool-agnostic and timeless. We delve deeply into the 'why' behind the 'how,' ensuring a thorough understanding of file systems, network protocols, and data structures. Unlike programs that may offer a siloed view, our curriculum provides a holistic perspective, seamlessly integrating computer, network, mobile, and cloud forensics into a unified investigative process. Furthermore, the course places significant weight on the legal and ethical dimensions of digital forensics, preparing participants not just to find evidence, but to ensure it is admissible and defensible. The inclusion of a capstone project, which simulates a complex, multi-faceted investigation from start to finish, provides an unparalleled opportunity to synthesize and apply all the learned skills in a realistic context, solidifying knowledge and building the confidence needed to excel in the field.