Certificate in Digital Forensics Fundamentals Training

Duration: **3 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

The **Certificate in Digital Forensics Fundamentals** course provides a solid introduction to the core techniques and tools used in digital forensic investigations.
It equips learners with the knowledge to **identify, preserve, analyse, and report digital evidence** in line with legal and professional standards.

Combining theory with hands-on practice, this course covers key forensic methodologies, evidence handling procedures, and best practices for maintaining admissibility in court.
Learners will also explore modern topics such as **IoT forensics, mobile device analysis, and anti-forensics methods** using open-source tools.

The **Certificate in Digital Forensics Fundamentals** provides essential technical and legal knowledge to handle digital evidence effectively.
Graduates will be able to perform digital investigations, maintain forensic integrity, and produce reports that meet professional and legal standards.

This course serves as an ideal **foundation for advanced digital forensics certifications**.

Prerequisites

There are no formal prerequisites; however, it is recommended that participants:

- Have a **basic understanding of IT systems and cybersecurity fundamentals**, and
- Are familiar with **file structures, operating systems, and storage devices**.

Who Should Attend

This course is ideal for:

- IT and cybersecurity professionals handling digital incidents
- Law enforcement and internal audit teams
- Compliance and regulatory officers managing evidence
- Incident response and digital forensics beginners
- Professionals seeking foundational knowledge in forensic analysis

Certificate in Digital Forensics Fundamentals Training

Duration: **3 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

Upon completion of this course, learners will be able to:

- Explain the purpose and key principles of digital forensics.
- Identify various forensic methodologies and legal considerations.
- Maintain the chain of custody for digital evidence.
- Acquire and validate forensic images using standard tools.
- Analyse file systems, metadata, and system artefacts for digital evidence.
- Investigate deleted files, Windows Registry, and forensic artefacts.
- Conduct mobile and IoT forensic investigations.
- Produce structured forensic reports for legal and regulatory review.

Certificate in Digital Forensics Fundamentals Training

Duration: **3 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Outline

Introduction to Digital Forensics

- Core concepts, objectives, and the role of digital forensics
- Legal and ethical considerations

Digital Evidence Collection Techniques

- Evidence handling, NPCC guidelines, and first responder tools

Legal Framework and Best Practices

- ISO/IEC forensic standards, data protection, and chain of custody

Evidence Imaging and Verification

- Forensic imaging, hashing algorithms, and FTK Imager practice

Computer Hardware and Storage Analysis

- BIOS, boot processes, hidden data, HDD vs SSD differences

Data Representation and File Systems

- Binary/hex decoding, FAT/NTFS analysis, and data recovery

File Signatures and Carving

- File carving, magic number analysis, and recovery techniques

Windows Artefacts and Metadata Analysis

- Registry, event logs, EXIF data, email header, Wireshark analysis

Mobile Device Forensics

- Data extraction and recovery from smartphones and tablets

IoT and Emerging Forensic Technologies

- Smart device forensics, steganography, and password cracking