Digital Forensic Foundation Course

Uncover the Truth
Strengthen Your Skills

The 4-day Digital Forensic Foundation Course is ideal for those wishing to pursue a career as a digital forensic investigator or for those cyber security specialists who wish to enhance their incident response skills.

The course is designed to provide students with a comprehensive introduction to the field of digital forensics. It covers a wide range of topics, including the basics of computer forensics, digital evidence, its collection and analysis, report writing and how to present evidence in court as an expert witness.

Through hands-on exercises using free and open source tools, the course allows students to develop a foundational understanding of the field of digital forensics and its associated concepts and technologies.

The course has been designed by experienced forensic investigators ensuring the content is both relevant and practical.

Who Should Attend

The course is ideal for those wishing to pursue a career as a digital forensic investigator or for those cyber security specialists who wish to enhance their incident response skills.

Outcome

This course will provide you with the basic knowledge and skills necessary to pursue further study in the field.

Length of Course

4 days

Course Content

Day 1

- ***Section 1 – Introduction to Digital Forensics***
  - Define Digital Forensics
  - Define the Types of Digital Forensic Investigations
  - Legal Considerations
- ***Section 2 – Investigation Fundamentals***
  - Good Practice Guidelines for Digital Evidence
  - The Four Principles of Computer Based Evidence
  - The Basics of a Digital Forensic Investigation
- ***Section 3 – Identification & Seizure of Digital Equipment***
  - Evidence Handling & Chain of Custody
  - Identifying Electronic Sources of Evidence
  - Dealing with Live Systems
  - Seizure of Electronic Devices
- ***Section 4 – Forensic Acquisitions***
  - Source Integrity
  - Data Acquisition Types
  - Forensic Acquisitions
  - Forensic Image
  - Forensic Clone
  - Forensic Acquisition Tools (FTK Imager)
  - Acquisition of Network Shares

Day 2

- ***Section 4 – Forensic Acquisitions - Continue***
  - Mounting a Forensic Image
  - How to create a bootable drive for Acquisitions?
  - Capturing RAM Memory
  - Hash Values (digital fingerprint)
- ***Section 5 – Understanding Hard Drive Terminology***
  - Traditional Hard Drives
  - SSD Hard Drives
  - Understanding Hard Drive Terminology
  - Unified Extensible Firmware Interface (UEFI)
  - GUID Partition Table (GPT)
- ***Section 6 – File Systems & Data Storage***
  - NFTS File System
  - Data Storage
  - Introduction to Metadata
  - Date and Time Stamps
  - NTFS Encryption

Day 3

- ***Section 7 – Forensic Analysis Techniques***
  - Analysis Environments
  - Case Preparation
  - File/Folder Recovery
  - File Signatures
  - Data Carving
  - Data Reduction Methods
  - Corroborating Evidence
- ***Section 8 – Windows Forensic Artefacts***
  - Windows Registry
  - USB Forensics
  - Internet History
  - Prefetch Files

Day 4

- ***Section 8 – Windows Forensic Artefacts (continue)***
  - Identifying Installed Software
  - Volume Shadow Copies
  - Link File Analysis
  - Identifying Executed Programs
  - Searching the Registry
  - Event Logs
- ***Section 9 – Dealing with Digital Evidence for Court***
  - How to Prepare a Forensic Report?
  - How to Prepare Evidence for Court?
  - Giving Evidence as an Expert Witness

Further Information - For further information, please contact E5h Forensic Solutions. Email: training@e5hforensics.com