Forensic Techniques for Auditors

Uncover the Truth
Strengthen Your Skills

A 1-day course designed to provide auditors and IT staff with an in-depth understanding of various forensic techniques which can be used to supplement their internal audit processes. The course covers the key principles of digital forensics. Participants will learn how to correctly handle electronic data, forensically preserve and extract data, and locate evidence using open source and free tools. Furthermore, participants will gain practical hands-on experience in applying these techniques in actual audit scenarios.

Aim

This course will equip participants with the necessary skills and knowledge to supplement their internal audits processes by using the latest forensic techniques.

Outcome

Upon completion of the course, participants will have a strong understanding of how to use digital forensic techniques to supplement their internal audit processes.

Course Content

- Introduction
- Define Digital Forensics
- Legal Consideration
- Evidence Handling & Chain of Custody
- How Courts Assess the Reliability of Digital Evidence
- Good Practice Guidelines for Digital Evidence
- The Four Principles of Computer Based Evidence
- Forensic Acquisitions
- Forensic Acquisition Tools
- Windows Registry
- Identifying Installed Software
- Volume Shadow Copies
- Identifying Executed Programs
- Link File Analysis
- USB Forensics
- Searching the Registry
- Event Logs
- Summary

Further Information

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