The **2-day Digital Forensics - Data Collections for First Responders Course** is ideal for IT staff or members of an incident response team who need to forensically preserve electronically stored information (ESI) following a cybersecurity incident or to support legal action.

The course is designed to provide students with a comprehensive introduction to the field of digital forensics with a focus on the identification, preservation and collection of electronic data from a range of sources. The course also covers chain of custody (COC) and the preparation of acquisition reports

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 how to apply forensic techniques to ensure that fragile electronic data is handled correctly and that potential evidence is not lost or altered.

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 IT staff or members of an incident response team who are required to forensically collect and preserve ESI following a cybersecurity incident or to support legal action.

Outcome

This course will provide you with the forensic knowledge and skills necessary to correctly identify, preserve and collect ESI following a cybersecurity incident or to support legal action.

Length of Course

2 days

Course Content

Day 1

- ***Section 1 – Introduction to Digital Forensics***
  - Define Digital Forensics
  - Define the Types of Digital Forensic Investigations
- ***Section 2 – Investigation Fundamentals***
  - Legal Considerations
  - How Courts Assess the Reliability of Digital Evidence
  - Good Practice Guidelines for Digital Evidence
  - The Four Principles of Computer Based Evidence
  - ISO/IEC 27037:2012
  - Evidence Handling & Chain of Custody
  - Competency
- ***Section 3 Preparation & Precautions for Data Collections***
  - Preparations for Data Collections
  - Precautions for Data Collections
- ***Section 4 – Forensic Acquisitions***
  - Source Integrity
  - Forensic Acquisitions
  - Forensic Image
  - Forensic Clone

Day 2

- ***Section 4 – Forensic Acquisitions - Continue***
  - Forensic Acquisition Tools
  - Hash Values (digital fingerprint)
  - Acquisition of Network Shares
- ***Section 5 – Data Collections***
  - Data Categories
  - Prioritizing collections and acquisitions
  - Identifying Sources of Evidence
  - Data Collection Environments
  - Static Data Collection
  - Booted Data Collection
  - How to Create a Bootable Collection Drive
  - Volatile Data Collection
  - Cloud Data Collection
- ***Section 6 – Preparing Digital Evidence for Court***
  - How to Prepare a Forensic Acquisition 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