Digital Media Investigations

Course Overview

This two-day course is designed for the investigator/examiner entering the field of digital forensics and provides the fundamental knowledge to comprehend and investigate incidents involving electronic devices. Participants are introduced to baseline concepts to ensure they gain the prerequisite knowledge to understand issues surrounding the handling of electronic evidence and to attend the next in the series of the Spyder Forensic Certification Training curriculum.

What You Will Learn

- **What is Digital Forensics**
  - General overview of the world of digital forensic investigations.
- **Reasons for a Forensic Investigation**
  - Discussions on the events that would lead to a request for a forensic examination.
- **Discuss the types of forensic analysis**
  - Outline the different types of analysis the examiner will encounter
  - Discuss the challenges of each and questions that need to be asked before an examination begins
  - Describe the forensic and incident response process.
- **Incident Response Process**
  - Discuss the role of the first responder
  - Outline the stages of the incident response
  - Review best practices in evidence collection
  - Practical's in evidence recovery
  - Review the concept of a digital fingerprint, HASHing.
- **Microsoft Windows Triage Analysis**
  - Review the forensic examination steps on a Windows system
  - Learn of key areas of evidential interest pertaining to user activity on the host system
  - Exercises in the analysis of collected evidence using industry standard tools.

Course Type
Foundation

Course Length
2 days

Course Code
DF – IDF