Computer Forensics and Investigation

Duration 4 Days

COURSE DESCRIPTION

This course provides technical techniques and processes to handle and analyze digital evidences.

COURSE OUTLINE

- Digital evidence acquisition techniques and tools for Windows and Linux, Triage process and tools, Static evidence gathering techniques, Live evidence acquisition techniques and tools
- Windows registry analysis techniques and tools, Additional key artifacts analysis, System and events log analysis
- Internet and Web browser artifacts, Network traffic aggregation and analysis, Network traffic analysis techniques and tools, Network Log aggregation and analysis
- Computer and Network forensic case study and challenges

PREREQUISITES

- General knowledge of computer and operating system.
- Some experience in computer programming languages.
- Background in Computer Network and Tools such as Wireshark.
- Some basic of Linux command.

WHO SHOULD ATTEND

A system administrator, a security analyst, and a forensic investigator with some background in conducting forensic analysis, network traffic analysis, log analysis, and security assessments. It is also well suited for those managing CIRT / incident response teams, or those in roles that require oversight of forensic analysis and other investigative tasks.

SKILL LEVEL

Intermediate.