Cyber Forensics Professional

- ❖ Expertise in forensic techniques and procedures, standards of practice, and legal and ethical principles to assure accurate, complete and reliable digital evidence admissible to a court of law.
- ❖ Knowledge and skills necessary to conduct forensically sound and accurate investigations.
- ❖ Knowledge or skill set to identify, track and bring the cyber criminals to justice (prosecute the cybercriminals)
- ❖ Various forensic investigation techniques and standard tools such as EnCase and Access Data FTK which are necessary to successfully carry-out a computer forensic investigation
- ❖ Knowledge in digital evidence acquisition, handling and analysis in a forensically sound manner which is acceptable in a court of law

What You'll Learn

- The computer forensic investigation process and the various legal issues involved
- Evidence searching, seizing and acquisition methodologies in a legal and forensically sound manner
- Different types of digital evidence, rules of evidence, digital evidence examination process, and electronic crime and digital evidence consideration by crime category
- How to set up a computer forensics lab and the tools involved in it
- Gathering volatile and non-volatile information from Windows
- Data acquisition and duplication rules, validation methods and tools required
- How to recover deleted files and deleted partitions in Windows and Linux
- The process involved in forensic investigation using Access Data FTK and EnCase
- Password cracking concepts, tools, types of password attacks & how to investigate password protected files
- How to investigate logs, network traffic, wireless attacks, and web attacks
- How to track e-mails and investigate e-mail crimes
- Steganography and its techniques, Steganalysis, and image file forensics
- Mobile forensics and mobile forensics software and hardware tools

C|HFI™
Computer Hacking Forensic INVESTIGATOR
Investigate Computer Crimes.
Prosecute Cyber Criminals.
Become a CHFI.