MARYLAND RANGE
Cyber Security Training & Simulation Center

Cyber Security Forensics Investigator

Crimes have evolved.

In this digitized world, crimes are easily committed through exploitations of network systems that are vulnerable. Cyber criminals are constantly evolving leading to more sophisticated hacking techniques and increased number of cyber-attacks on enterprises.

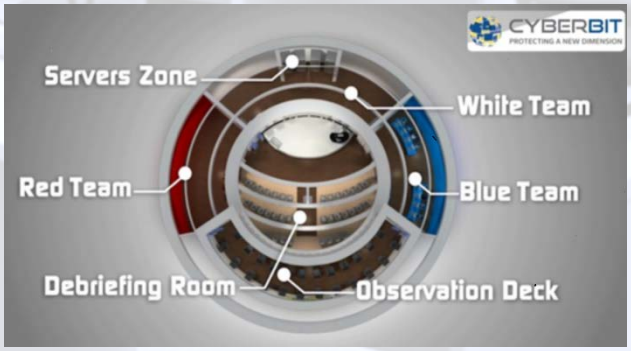
When a cyber-attack incident occurs, cyber forensics plays an imperative role in gathering and extracting evidences from the compromised artefacts for the conduct of cyber forensics investigation. To ensure precision and completeness of the harvested evidences, the conduct of an investigation requires advance knowledge of cyber threats, understanding of technical tools and its functionality, awareness in evidence collection procedures, and techniques in preserving and maintaining the integrity of evidences.

The **Cyber Security Forensics Investigator (CSFI)** training focuses on imparting cyber forensics concepts and processes including acquisition of forensics evidences, preservation and analysis of the gathered evidences, and presentation of the findings. The training also encompasses the conduct of forensics investigation on simulated real-world cyber incidents in an emulated enterprise network environment to instill applicable skillsets and enhances knowledge retention. Whether you are a cyber-security analyst or IT professional who wish to gain better understanding of cyber forensics and acquire investigation skillsets, CSFI is the course that will provide you with a robust cyber forensics investigation training experience.

Training Benefits

Through the Cyber Security Forensics Investigator, trainees will be able to:

- Appreciate the entire cyber forensics investigation processes and procedures
- Understand functionality of various forensic tools and its utilization during investigation
- Develop practical skillsets in forensics investigation from acquisition, preservation, analysis toreporting
- Recommend preventive measures against future cyber incidents



Who Should Attend

- Security analyst looking to expand current job scope and wish to acquire cyber forensic investigations skillsets
- IT Professionals / Engineers requiring a better understanding of cyber forensics
- Information Security Managers and Executives involved in handling cyber forensics data and
- Project Managers, Risk Managers and Compliance Managers who require an understanding of cyber forensics processes and outcomes

Course Structure

Day One
a. Introduction to Computer Forensics b. Forensics Imaging c. Autopsy d. Windows Event Logs e. Demonstration and Hands-on Practical Exercises
Day Two
a. File Systems b. Windows Registry c. Hashing d. Pre-fetch and Shell Bags e. Data Hiding f. Data Carving g. Email Forensics h. Demonstration and Hands-on Practical Exercises
Day Three
a. Browser Forensics b. Memory Forensics c. Cyber Forensic Scenario-based Exercise 1
Day Four
a. Case Study and Report Writing b. Cyber Forensic Scenario-based Exercise 2