Vendor-Neutral Global IT Certifications

Star Forensic Investigator Computer Hacking 007

007 **Proficient in Detection & Prevention of Cyber Crime Investigation**

SFICH 007

Star   Forensic   Investigator   Computer   Hacking

LEARN + **EXAM** = **CERTIFIED**

🌐 www.starcertification.org

✉ info@starcertification.org

Star Forensic Investigator Computer Hacking 007

Cyber-attacks are the fastest growing crime in the world, and they are increasing in size, sophistication, and cost. It is therefore imperative to understand ways and means to investigate the various cybercrimes committed. Forensic investigation is the practice of collecting, analyzing and reporting on digital data in a way that is legally admissible. Star Forensic Investigator Computer Hacking (SFICH – 007) is a detailed course that explains the intricacies of a cybercrime and helps deduce its origin.

The program helps the learners acquire a fundamental understanding of tools and techniques to conduct forensic investigations, detailing all aspects of digital forensics from detecting an intruder's footprints, to take necessary preventive steps, and to properly gather and process the evidence to prosecute in the court of law. The course aims to teach the learners about various investigation tools, eDiscovery, digital evidence collection, evidence preservation, e-mail investigation and recovery, e-mail and IP tracking, encryption and decryption methods, search and seizure of computers, recovering deleted evidences and password cracking.

Audience:

EHE (Ethical Hacking Expert), Network Operation Center (NOC), Security Operational Center (SOC), Cyber Crime Officer, Cyber Crime Investigator, Defence, Military, E-Business Security Professionals, System Administrator, Legal Professionals, Banking Professionals, Insurance Professionals ,IT Managers, Government Agencies etc.

Course Objectives:

In this course, you will learn about:
* Investigating cybercrime
* Types of digital evidence and evaluating digital evidence and Examining and securing crime scenes
* Recovering of files and partitions on different OS platforms and Computer forensics processes
* Password breaking and investigation techniques for password attacks and Capturing and managing logs
* Investigating techniques related to attacks on network, cloud and virtual systems and E-mail crime investigation
* Investigating attacks on mobile and resolving and Using forensic tools and preparing documentations

Course Outcome:

After completing this course, you will be able to:
* Identify types of digital evidence
* Recover lost files and partitions on different OS platforms
* Carry out computer forensics process
* Capture and manage logs
* Apply different investigating techniques to solve attacks on network, cloud and virtual systems
* Perform e-mail crime investigation
* Investigate attacks on mobile devices
* Use forensic tools and preparing documentations

Course Outline:

PART 1
1. INTRODUCTION TO COMPUTER FORENSICS
2. INTRODUCTION TO DIGITAL EVIDENCE
3. UNDERSTANDING HARD DISKS
4. FILE SYSTEMS: WINDOWS, LINUX AND MAC OSX
5. COMPUTER FORENSICS INVESTIGATION PROCESS
6. SEARCHING AND SEIZING APPENDIX

PART 2
7. DATA ACQUISITION AND DUPLICATION
8. UNDERSTANDING INCIDENT RESPONSE PROCEDURES
9. FORENSICS AND OPERATING SYSTEMS
10. STEGANOGRAPHY: AN OVERVIEW
11. INVESTIGATING EMAIL CRIMES

PART 3
12. NETWORK FORENSICS
13. INVESTIGATING WEB ATTACKS
14. MOBILE FORENSICS
15. CLOUD FORENSICS
16. VIRTUALISATION AND FORENSICS
17. DATABASE FORENSICS
18. DEALING WITH ANTI-FORENSICS TECHNIQUES
19. MALWARE FORENSICS
20. DIGITAL FORENSIC INVESTIGATION USING ENCASE FORENSIC
21. FORENSICS REPORT WRITING

Exam Information:

Exam Code	:	S09-007	Exam Pattern	:	Multiple Choice
Exam Duration	:	3 Hrs	Exam Delivery	:	AEPTC (ACADEMIC EDUCATION & PROFESSIONAL TESTING CENTER)
Passing Score	:	70%			

Course Duration:

60 Hrs