
EXPERTS
CHFI
EC-Council

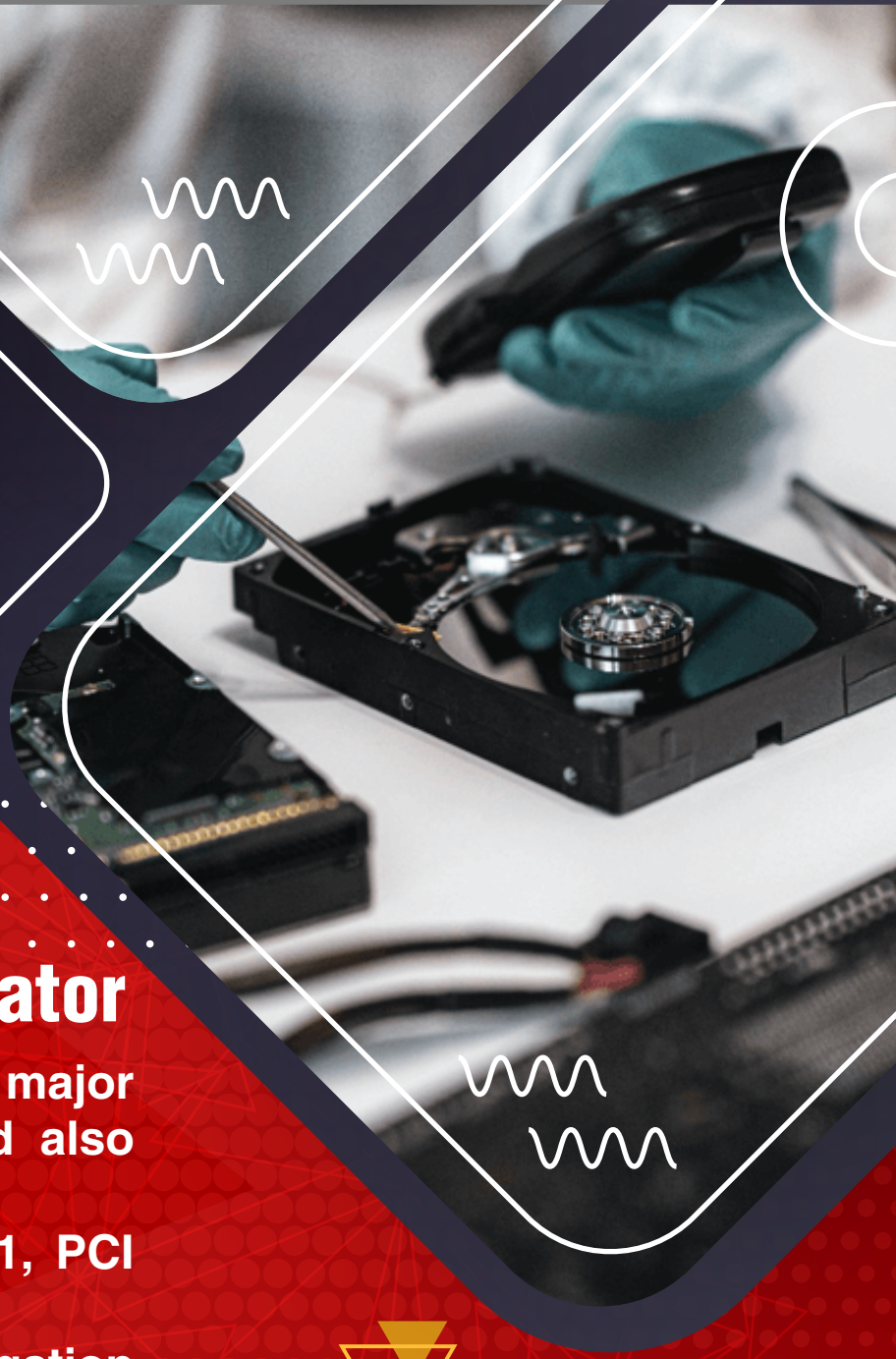
Duration: 40 hours / 5 days

About The Course

Computer Hacking Forensics Investigator

It is a full course of impartial vendor that covers all major criminal investigation techniques and solutions and also covers all knowledge bases and skills needed to meet regulatory compliance standards such as ISO 27001, PCI DSS, SOX, or HIPPA.

The program introduces the iterative forensic investigation methodology required by a versatile digital forensic specialist which increases your employability.



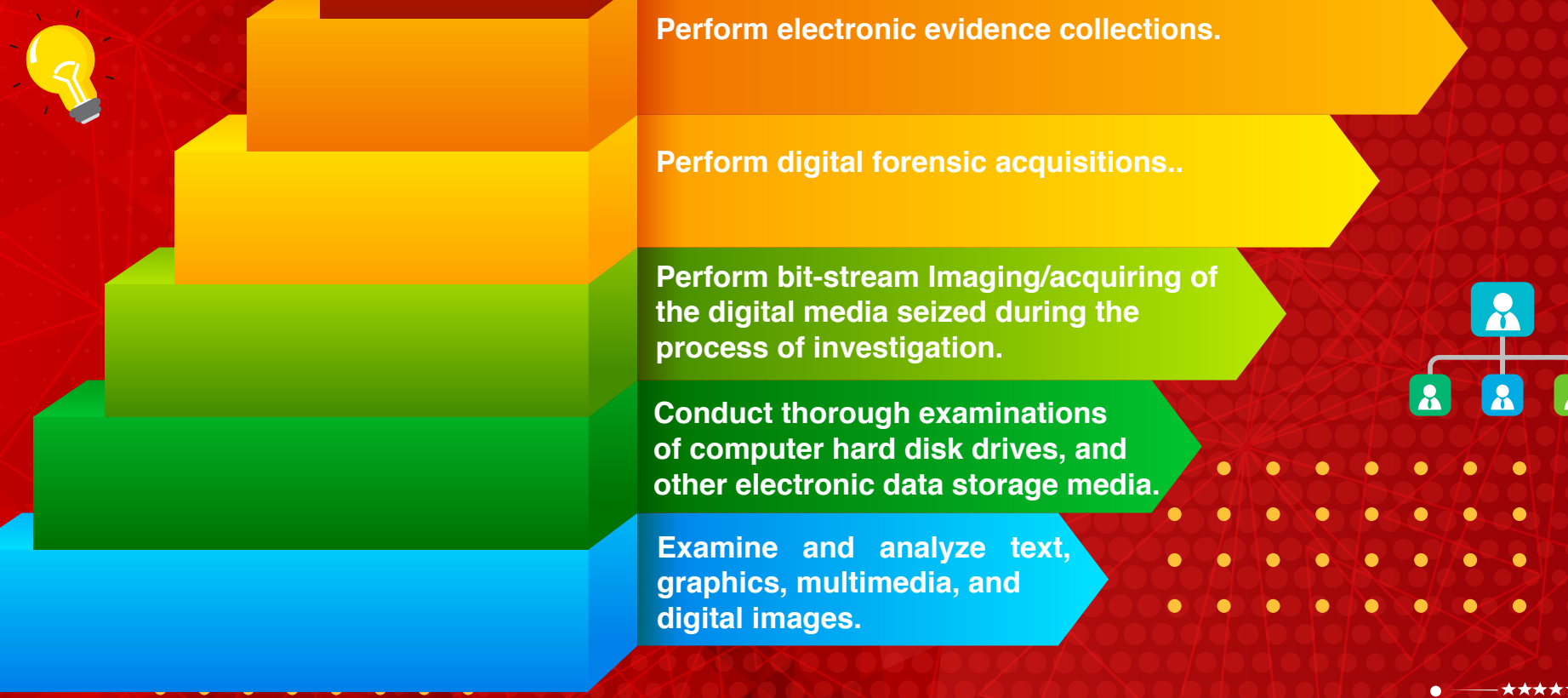
iEXPERTS

Course Outline

- Computer Forensics in Today's World
- Computer Forensics Investigation Process
- Understanding Hard Disks and File Systems
- Operating System Forensics
- Defeating Anti-Forensics Techniques
- Data Acquisition and Duplication
- Network Forensics
- Investigating Web Attacks
- Database Forensics


Cloud Forensics
Malware Forensics
Investigating Email Crimes
Mobile Forensics
Investigative Reports
EXPERTS

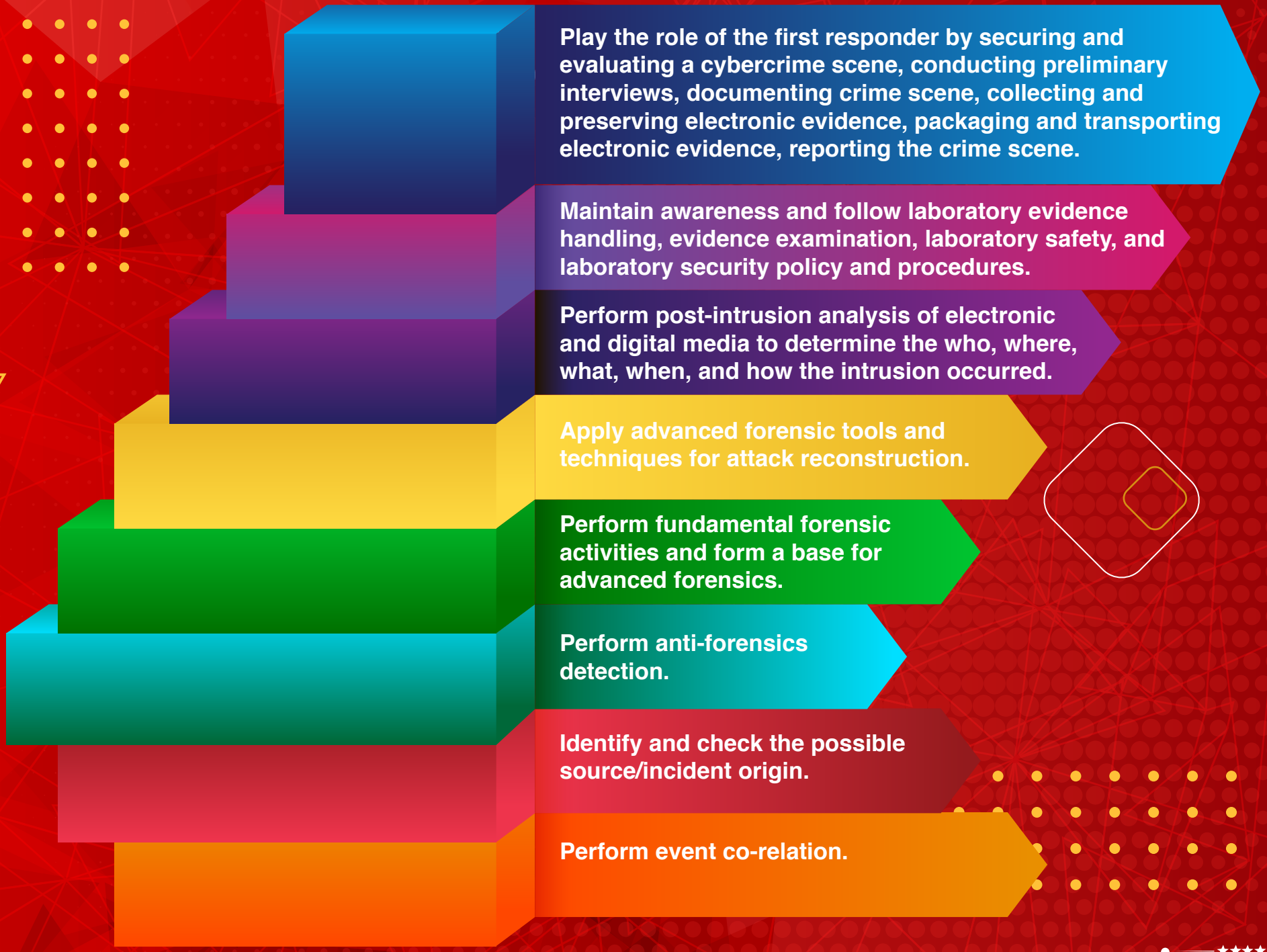
Course Add Value

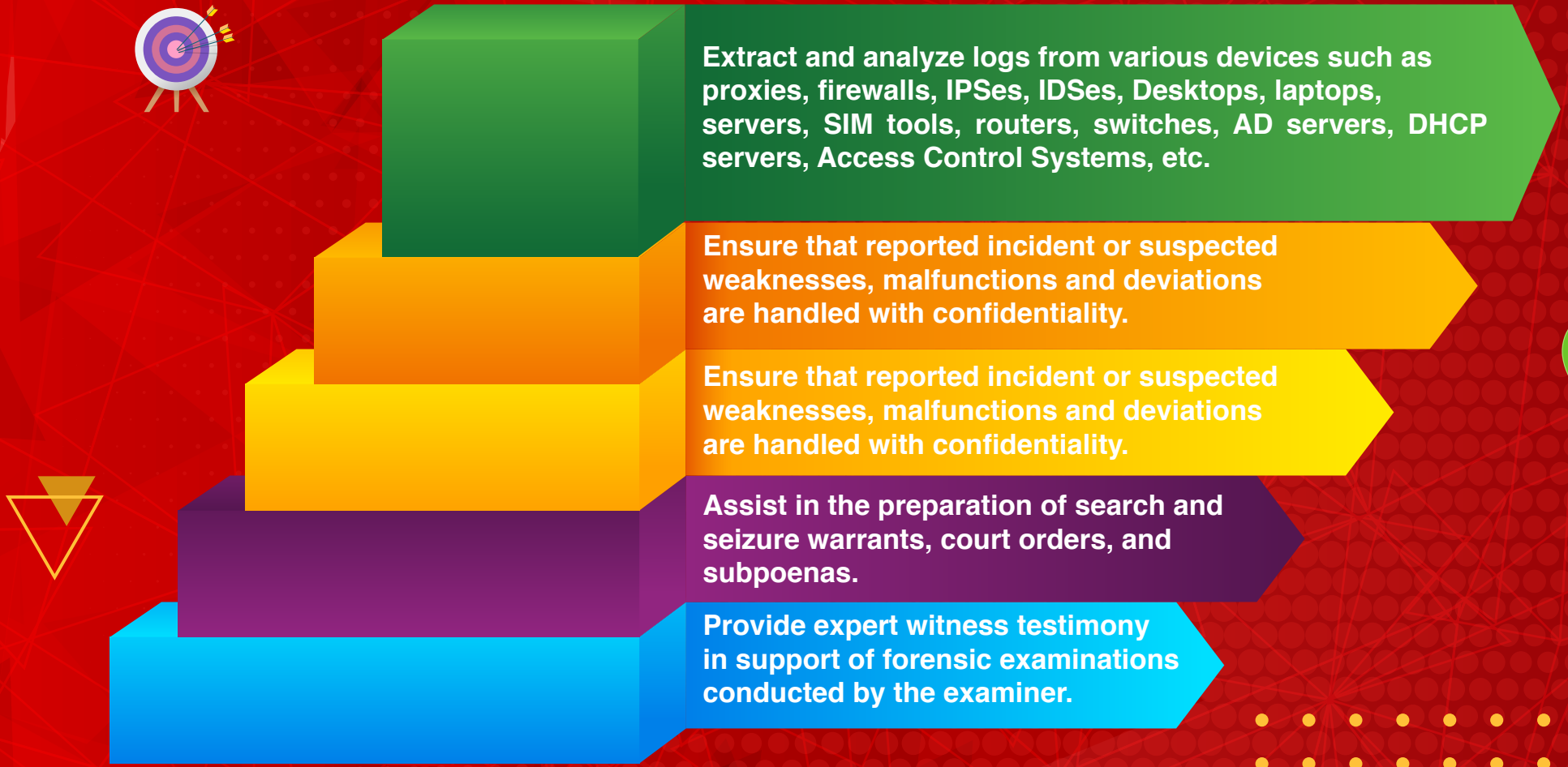



Recover information and electronic data from computer hard drives and other data storage devices.
Utilize forensic tools and investigative methods to find electronic data, including Internet use history, word processing documents, images and other files.
Maintain audit trail (i.e., chain of custody) and evidence integrity.
Work on technical examination, analysis and reporting of computer-based evidence.
Follow strict data and evidence handling procedures.
Prepare and maintain case files.
Gather volatile and non-volatile information from Windows, MAC and Linux.
Recover deleted files and partitions in Windows, Mac OS X, and Linux.
Perform keyword searches including using target words or phrases.


Collect data using forensic technology methods in accordance with evidence handling procedures, including collection of hard copy and electronic documents.
Investigate events for evidence of insider threats or attacks.
Investigate and analyze all response activities related to cyber incidents.
Plan, coordinate and direct recovery activities and incident analysis tasks.
Examine all available information and supporting evidence or artefacts related to an incident or event.
Conduct reverse engineering for known and suspected malware files.
Identify data, images and/or activity which may be the target of an internal investigation.
Identify data, images and/or activi-ty which may be the target of an internal investigation.
Perform detailed evaluation of the data and any evidence of activity in order to analyze the full circumstances and implications of the event.


Generate reports that documents which detail the approach, and an audit trail which documents actions taken to support the integrity of the internal investigation process.
Establish threat intelligence and key learning points to support pro-active profiling and scenario modeling.
Search file slack space where PC type technologies are employed.
File MAC times (Modified, Accessed, and Create dates and times) as evidence of access and event sequences.
Review e-mail communications including webmail and Internet Instant Messaging programs.
Examine file type and file header information.
Examine the Internet browsing history.
Recover active, system and hidden files with date/time stamp information.
Crack (or attempt to crack) password protected files.


Play the role of the first responder by securing and evaluating a cybercrime scene, conducting preliminary interviews, documenting crime scene, collecting and preserving electronic evidence, packaging and transporting electronic evidence, reporting the crime scene.
Maintain awareness and follow laboratory evidence handling, evidence examination, laboratory safety, and laboratory security policy and procedures.
Perform post-intrusion analysis of electronic and digital media to determine the who, where, what, when, and how the intrusion occurred.
Apply advanced forensic tools and techniques for attack reconstruction.
Perform fundamental forensic activities and form a base for advanced forensics.
Perform anti-forensics detection.
Identify and check the possible source/incident origin.
Perform event co-relation.


Extract and analyze logs from various devices such as proxies, firewalls, IPSes, IDSes, Desktops, laptops, servers, SIM tools, routers, switches, AD servers, DHCP servers, Access Control Systems, etc.
Ensure that reported incident or suspected weaknesses, malfunctions and deviations are handled with confidentiality.
Ensure that reported incident or suspected weaknesses, malfunctions and deviations are handled with confidentiality.
Assist in the preparation of search and seizure warrants, court orders, and subpoenas.
Provide expert witness testimony in support of forensic examinations conducted by the examiner.

Course Prerequisite

It is strongly recommended that you attend the CEH class before enrolling in the CHFI program.

GET IN TOUCH

www.iExperts.co

info@iExperts.co

Follow @iExperts10 on :