DIGITAL FORENSICS WORKSHOP | COURSE OUTLINE

CYBER ZONES
Cyber Security Services

Course Title:
Digital Forensics Workshop

Duration:
5 -6 sessions

Class Format Options:
Instructor-led classroom – Practical Training.

Who Should Attend:

- Cyber Security Professionals
- SOC Managers
- SOC Engineers
- IT Auditors
- System Administrators
- IS Managers
- IT Managers

Prerequisites:

- Cyber Security Plus
- Incident handling & Response Workshop.
- Cyber Threat Intelligence & Spyware Hunting

Cyber Zones RED team track is highly recommended

Provided Materials:

- Softcopy Materials.
- Digital Forensics tools.

This training course is practical training course on which each trainee will learn on the proper technique to conduct a digital forensics service.

Course Overview

The **Digital Forensics Workshop** is an advanced **defensive cyber security course** from BLUE Team training path aims to teach trainees to manage & investigate cyber crime by understanding how attackers operate and what piece of information is crucial for investigators, **Digital Forensics Workshop** will allow trainees to gain the practical experience to manage and interact with cyber crime, furthermore cyber crime and fraud investigators whereby "trainees" are taught electronic discovery and advanced investigation techniques in **a pure practical manner**.

Digital Forensics Workshop is designed for those people who wish to become cyber security professionals, SOC engineers, SOC Managers, Information Security Assurance specialists, the course covers:

- Ways for discovering network breaches - *Practical using commands/tools*.
- *Perform network traffic forensics - Practical using commands/tools.*
- Malware and spy software both in computers and mobiles - *Practical using commands/tools*.
- Perform RAM dumps - *Practical using commands/tools.*
- Perform disk based forensics - *Practical using commands/tools.*
- Perform forensics imaging - *Practical using commands/tools.*
- identify important information that will support the forensics investigation.
- Digital forensics reporting.

Upon completion trainees will be able to:

- Establish industry acceptable digital forensics standards with current best practices and policies.
- Have the knowledge to perform network forensic examinations.
- Have the knowledge to accurately report on findings from examinations.

Final Scenario should be completed by the trainee to receive attendance certificate. (6 hours).