DIGITAL FORENSICS WORKSHOP | COURSE OUTLINE

CYBER ZONES
Cyber Security Services

Course Title:

Digital Forensics Workshop

Duration:

15 - 20 Hrs

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:

A general knowledge of information systems and security including Incident Handling experience.

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.

DIGITAL FORENSICS WORKSHOP| COURSE OUTLINE

CYBER ZONES
Cyber Security Services

Day 1 Agenda

> Training Course Paths
> BLUE Team vs RED Team
> Training Course Type
> What is Digital Forensics?
> Digital Forensics vs Computer Forensics
> What is Network Forensics?
> What is Chain of Custody?
> Verify the Integrity of the Image
> Day 1 | Review & discussion
> Preparing Forensics Workstation
> **Exiftool Introduction**
> ExifTool – Exercise 1
> ExifTool – Exercise 2
> Exiftool Lab
> Type of Media – Few Examples
> Data of Interest
> Forensics vs Incident Response
> **Last Activity View Introduction**
> Last Activity Viewer – Exercise 1
> Last Activity Viewer – Exercise 2
> Last Activity View Lab
> Forensics Best Practice
> **NTFS Walker Introduction**
> NTFS Walker Overview
> **Disk Digger Introduction**
> Disk Digger Overview
> Disk Digger Exercise 1
> Exercise – Recover files from your USB
> **Memory Dumping tools Lab**
> **Magnet Overview**
> Magnet Exercise

Day 2 Agenda

> Why is Evidence Important?
> What is Digital Evidence?
> Digital Forensics Examples
> Digital Forensics - **Sample Questions**
> Important Rules
> Computer Forensic Activities
> Who needs Digital Forensics? Few Reasons
> Reasons for a Forensic Analysis
> Types of Forensic Requests
> Forensics Phases
> Forensics Phases – I prefer this!
> Phase 1: Preparation
> Phase 2: Imaging
> Phase 3: Examination
> Phase 4: Documentation
> **FTK Imager Introduction**
> FTK Imager Overview
> Installing FTK Imager
> The FTK Imager User Interface
> The FTK Imager Capturing RAM Exercise
> The FTK Imager Creating Forensic Images
> Forensic Images Extensions
> **FTK Imager Lab**

Day 3 Agenda

> Evidence Processing Guidelines
> 16 steps in processing evidence
> Digital Forensics Investigation Kit
> Seizure Plan
> Evidence Store – Secure Storage
> The Chain of Custody
> RFC 3227
> Most 2 Least Volatile
> Practical RFC 3227
> Network Traffic Forensics
> Memory Forensics
> How to Evade Memory Dumps?
> Physical Disks Forensics

Day 3 Agenda - Cont

> External Disks Forensics
> USB Devices Forensics
> Who Performs Data Acquisition
> 3 Way Handshake
> Windows 7 Event Viewer
> Event Log Classifications
> Application Logs
> Security Logs
> Security Audit Categories
> Security Audit – Auditpol Command
> Exporting Event Logs
> Important Windows Event Logs
> Account Usage
> Account Usage – Logon Types
> Introduction to Network Miner
> Network Miner Overview
> Lab – Acceptable Use Policy Breach
> Introduction to Bulk Extractor
> Bulk Extractor Overview
> Lab – Bulk Extractor and Bulk Viewer

Day 4 Agenda

> Capturing Volatile Memory
> Volatile Memory Overview
> Memory Dumping Tools
> Memory Dumping Tools – Magnet Dump
> Memory Dumping Tools –Dumpit
> Memory Dumping Tools –FTK Imager
> Reporting and Documentation
> Sample Digital Forensics Report
> Autopsy lab

Day 5 Agenda

> Course Review
> Final Scenario