Practical Cyber Forensics Investigation

40 Hours

Description

The purpose of Wawiwa's Practical Cyber Forensics Investigation program is to get to know the world of computer investigations, with an emphasis on computer investigations in the Windows environment.

This program will train students in the use of various investigation tools for analyzing and deciphering computer crime events, reconstructing and deciphering software and hardware failures, and preventing such events in the future.

The researcher's toolset is designed to provide means for deciphering computer crime incidents, investigating computers after an attack, and finding the root cause.

The use of such tools is usually done in the following cases:

1. In a legal framework - for examining computer systems that were part of the computer offense or used by defendants or plaintiffs
2. To restore information on media that has been damaged due to hardware failure
3. To understand the processes that exist in the system in order to improve the performance or to restore a malfunction in order to prevent it in the future
4. To understand the processes that take place in the system at the time of entry into force, in order to understand and prevent the attack in the future, or to identify the attacker
5. For investigating a computer after a cyber-attack

The program uses Wawiwa's virtual labs, developed in Israel, the Startup Nation.

Expectations and Goals

In this program, you will gain an introduction to Incident Response, learn how to handle common security incidents and perform Digital Forensics deep Investigations during the incidents, deep dive into Insider and Malware Threats from forensics perspectives.

Learning Objectives

- Understand the Incident Response plan and methodologies
- Detect, Identify and contain the most common cyber security incidents
- Look for suspicious activity of malwares and malicious code on endpoints
- Analyze malwares with several techniques (static and dynamic)

- Find, collect, and perform a forensics investigation of digital evidence
- Look for Cyber Threat Intelligence feeds with online and Open Source tools

Target Audience

- Incident handlers and leaders of incident handling teams
- System administrators
- Other security personnel who are TIER2 cybersecurity personae

Prerequisites

- Previous background in managing Windows or Linux networks
- Background in Information Security
- Candidates are required to familiarize themselves with Windows Operating Systems
- Communication protocols (TCP/IP) and familiarity with the Internet.
- Willingness to self-work

What Graduates Receive

- Program presentation as a PDF file
- Cheat sheet and useful documentation
- "Swiss Army Knife" - 3GB of IR tools

Virtual Lab

The course uses envario ™ virtual labs , an Israeli based Cyber virtual lab

Wawiwa provides the center with a unique cloud environment with the following Virtual Machines:

- Clean VM (Win10 64-bit) – For first Lab Installation
- Malware Analysis VM (Win10 64-bit)
- Digital Forensics VM (Win10 64-bit)
- Certificates

Students are expected to bring their own laptops, unless the center has appropriate training classes with computers. Hardware requirements: Intel: i3 or higher, Win 10, Min 8GB RAM

Internet bandwidth at home - minimum base connection speed of 100 Mbps down is required, Internet latency less than 50ms.

Classroom Facility

A fully equipped classroom, with the required multimedia infrastructure. At list 2 screens of 50” or higher connected to the instructor working station

a. Workstations with internet communication,

b. Minimal requirements for student’s workstation (per student) and 1 for Instructor:

1. Windows 10 OS, MS office
2. Intel: i5 processor or higher
3. x64-compatible 2.0 GHz CPU minimum or higher
4. 8 GB RAM minimum
5. 250 GB SSD available hard-drive space
6. Laptop or stationary computer workstation recommended monitors of 22” or larger

c. Minimum base connection speed of 100 Mbps down is required, Internet latency less than 50ms.

Practical Learning (Hands-On)

- 21 hours hands-on activities
- Hands-on activities on local environments

Course Syllabus

Main Module	Hours + Labs
Module 1 – Intro to Incident Response • Threat Actors • SOC Building Blocks • Live Demo - Show Me the Money – Use Case • Hands-On 1-1: Desktop Challenge • Hands-On 1-2: Incident Response Challenge • Assignment: Watch and Relax	**2**
Module 2 – Intro to Practical Malware Analysis • Malware and Malware Analysis • Analysis Techniques • Types of Malwares • Malware Behavior • Live Demo - Persistence Mechanisms • Creating a Safe Analytical Environment • Live Demo - Performing Malware Analysis on windows • Live Demo - Armored Malware • Quiz • Assignment: Introduction to Practical Malware Analysis	**2**
Module 3 – Build Your Malware Analysis Lab • Why do you need a Malware Analysis Lab? • How to build it? • Step 1. Your network • Step 2. Virtualization? • Step 3. Analysis Machines • Step 4. Testing your environment • Step 5. Start your Malware Analysis • Quiz • Assignment: Analyze your Malware	**2**
Module 4 – Intro to Practical Digital Forensics • Introduction and Definition	**4**

• Crime scene • The forensic lab and tools • Quiz • Assignment 4-1: Files True Type	
Module 5 – Know your Forensics Investigation lab and Tools • The Investigator Lab • The Lab • Hardware Prerequisites • The Investigator Software • Conclusion • File Signature Table / Magic Number • Hands-On: What is your type? • Assignment: Job Interview	**4**
Module 6 – Digital Forensics and Enforcement of Law • Cyber Crime Workflow • Digital Forensics and Enforcement of the Law • The Fourth Amendment • Chain of Custody • Anti-computer forensics • Anti-Forensics Methods • Anti-Forensics Tools • Hands-On 1: Steganography • Hands-On 2: Twitter Secret Messages • Assignment: Into the Square	**2**
Module 7a – Practical Windows Forensics Investigation • Practical Windows Forensics • Digital Forensics-Primary Goals • Forensics Analysis Process • Forensics Investigation Process • Forensics Analysis Checklist • Most important Artifacts of Windows 7	**6**
Module 7b – Windows Artifacts • Windows Registry • MRU • Shellbags	**5**

• JumpLists • USB Device • MCAB Times • Recycle Bin • Event Log • RDP • Thumbs.db • Hands-On- USB Investigation • Assignment: Multiple Device	
Module 8 – Memory Forensics • Prefetch • Page Files • Create Memory Dump • Analysis Dump Files: • Volatility • Volix • Memorize	**5**
Module 9 – Reporting and Cleanup • What we need to document • Write the Forensics Investigation Report • Store and Cleanup evidence	**4**
Module 10 – Final Exercise Hands-On Investigation + writing a report	**4**

* Virtual labs are implemented using classroom facilities or can be provided 100% virtual (no need for facility only Bring Your own laptops)