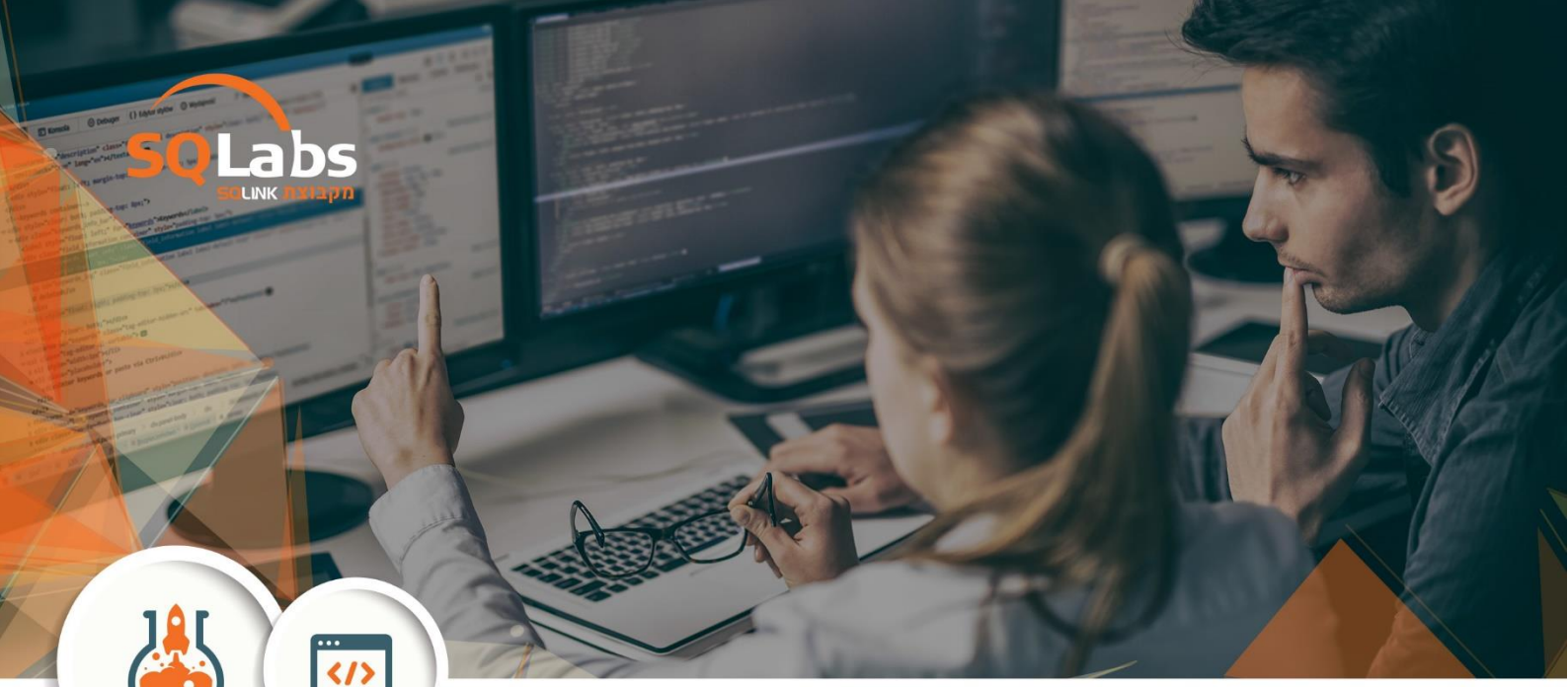

Windows Forensics

Duration**: 40 hours**

Overview

Windows Forensics is an essential skill in the cybersecurity world. Covering a broad spectrum of aspects of the forensic investigation process performed on Windows OS. Participants will learn how different computer components work and how to investigate after a cyber-incident. The training will focus on developing hands-on capabilities of forensics teams or individual practitioners in these areas:

- Searching the hard drive for evidence
- Processing hidden files that are invisible or inaccessible containing past-usage information
- Performing a forensic analysis on a computer to reveal usage details, recover data, and accomplish a full inspection after the machine has been defragged or formatted

במסגרת הקורס יתבצע תרגול ע"י סימולטור ייעודי להכשרה.

Target Audience

This course targets participants with basic knowledge in IT or networking, who wish to have a deeper understanding of cyber investigations and the forensic process

- Law enforcement officers & intelligence corps
- Incident responders
- Computer investigators
- IT/network administrators

Pre-requisites

- הקורס מיועד לבעלי רקע בסיסי עם מערכות הפעלה. לא נדרש רקע קודם בתחום.

Objectives

- Accessing concealed files on the system and extracting relevant information
- Mastering the steps of incident response
- Analyzing relevant case studies

Module 1: Computer Hardware

The first module will cover different components of computer hardware. Students will learn the main components of Storage-Disks, the structure of the Windows OS, and finally, the students will install their first virtual forensics stations.

Drives and Disks

- *The Anatomy of a Drive*
- *Data Sizes*
  - Data Representation
  - Hexadecimal
  - ASCII
  - Binary
- *Volumes & Partitions*
- *Disk Partitioning and the Disk Management Tool*
  - MBR vs. GPT
  - Understanding UEFI
  - The HPA
- *Solid State Drive (SSD) Features*

Understanding Windows OS structure

- *The filesystem*
- *FAT*
  - FAT Structure
  - File Allocation and Deletion
- *NTFS*
  - NTFS Structure
  - Volume Boot Record
  - Master File Table
- *The EFS Encryption*
- *Windows Directory Structure*

Virtualizing a Forensics Workstation

- *Setting up a Virtual Machine*
- *Installing and Configuring the VM*
- *Preparing the Environment*

Module 2: Forensic Fundamentals

This module will expose students to the internal components of the Windows OS. Students will learn about tools that will help them with the Forensics investigation process.

Understanding Hashes and Encodings
- *Hash as a Digital Signature*
- *The Use of Hash for Forensics*
- *Base Encodings*

Windows Artifacts
- *Startup Files*
- *Jump List*
- *Thumbnail Cache*
- *Shadow Copy*
- *Prefetch and Temp Directories*
- *RecentApps*
- *Registry Hives*

Windows Passwords - Bypassing Windows Protection
- *Encryptions in the Windows OS*
  - Bit locker
  - NTLM
  - Kerberos
- *Cracking Windows Passwords*
- *Cracking RAR/ZIP Passwords*

Data and Files structure
- *Hexadecimal Editing Tools*
  - WinHex
  - HxD
- *File Structure*
  - Headers and Trailer
  - Magic Number
- *Embedded Metadata*
- *Working with Clusters*
  - Slack Space
  - Unallocated and Allocated Spaces

Module 3: Collecting Evidence

During this module, students will master techniques for collecting evidence, accessing, and retrieving volatile and non-volatile information. Students will learn techniques for collecting evidence, accessing, and retrieving volatile and non-volatile information.

Forensic Data Carving
- *Using HxD for Forensics Carving*
  - Carving Files from an Existing File
- *Automatic File Carving Tools*
  - Foremost
  - Scalpel
  - Bulk-Extractor

Collecting Information

- *Indenting Evidence of Program Execution*
  - Extracting Registry Artifacts
  - Event Viewer
  - The Audition Policy
  - Windows System Metadata
- *Detecting Hidden Files using ADS*
- *Self-Extracting Archives (SFX)*
- *Collecting Network Information*
  - Network Information
  - Network Connections
- *Sysinternals-Suite Forensic Tools*
- *Extracting Credentials using NirSoft*

Drive Data Acquisition

- *Introduction to FTK-Imager*
  - Exploring System Files
  - Creating an Image
  - DD as an Alternative Image Capture Tool
- *Capturing Volatile-Memory*
  - Capturing a Memory-File
  - Capture Methods and Technics
  - Pagefile
  - Hiberfil.sys

Module 4: Analyzing Forensic Findings

In this module, students will understand how to uncover hidden information, detect tampered files, work with memory, and analyze the Ram.

Analyzing captured images

- *Features of FTK*
  - Extracting Protected Files
  - Mounting an Image as a Drive
  - Volatile Memory Capturing
- *MFT Dump*
  - Identifying Potential Threats
  - Visualizing an MFT Reconstruction using DMDE
- *Analyzing Prefetch Files*
- *Reconstructing Explorer with ShellBags*

Working with Volatile-Memory

- *Extracting Data from RAM*
- *Identifying Network Connections*
- *Dumping Processes from Memory*

Registry analysis

- *Using AccessData Registry Viewer to analyze Registry dumps*
- *Finding user Information using Ntuser.dat and usrclass.dat*
- *Using CLI to Access the Registry*
- *Extracting Data from Registry*
- *Forensics Findings in the Registry*

Anti-Forensics Techniques

- *Wiping Drives*
- *Advanced Stenographic Methods*
- *File Obfuscation Techniques*
- *Data Forgery*
- *Drive and File Encryption*
- *Artifact Removing*

Module 5: Data Labelling and Report Writing

Participants will study different forensics reports prepared by investigators following past incidents and learn how to write a professional report, including which points to consider when addressing the documentation of findings of an event.

Introduction to report writing

- *Device Identification*
- *Preservation of Data*
- *Collecting Evidence*
- *Examination and Analysis*
- Documentation
- Evidence Presentation
- Final Guidelines