Windows Forensic Analysis

Course Introduction

Windows Forensic Analysis is a 5-day instructor led course focused on investigating Microsoft Windows-based corporate assets. The course was built with all members of IT Security and management staff in mind, but especially those who wish to expand their skills from single system incidents to incidents at the corporate scale.

After completing this course, the student will possess improved skills in event triage with EDR solutions and other live data, data collection, proper evidence handling and in-depth event and system timelining.

Trustwave SpiderLabs is an industry leader in providing Digital Forensics and Incident Response (DFIR) consulting services to worldwide customers from multiple industries that have suffered data compromises or security breaches involving APTs, unauthorized access, credit card fraud, data theft, insider threat, and malware outbreaks. This training is based on our experience and has been built and is focused on teaching and demonstrating the various aspects related to developing and building a Computer Security Incident Response capability that works in the real world.

Learning Objectives

At the conclusion of this course students will have the foundation skills needed to analyze a Microsoft Windows system or network for evidence of a computer security breach.

By the end of this course students will be able to:
1. Acquire memory and volatile data from live Windows systems.
2. Analyze memory images of Windows systems.
3. Identify the risks and benefits of conducting live analysis versus powering down the system.
5. Describe the different partition and volume systems frequently used on Windows systems.
6. Analyze common Windows filesystems, including FAT, exFAT and NTFS.
7. Analyze the main artefacts of Windows filesystems.
8. Judge how different user and operation systems actions will change filesystem date time records.
9. Evaluate how key artefacts can be used to identify user activity.
10. Analyze event logs in order to describe user activity.
11. Evaluate event logs to detect anomalous activity.
12. Use built-in Windows utilities to conduct analysis.
13. Prioritize analysis steps in sequence most likely to address investigation needs.
14. Write an analysis report of a Windows system.

**Course Length**

Five days, 8 hours per day, total of 40 hours.

**Intended Audience**

This course is designed for staff responsible for extracting and interpreting evidence from Microsoft Windows based systems. This expertise may be used in civil or criminal investigations or in responding to a computer security breach.

**Prerequisites**

It is expected that students have knowledge of the identification, collection and acquisition of electronic evidence, both volatile and non-volatile. They should be familiar with the windows family of operating systems, and aware of the security sub-system, key operating system files and user management. In addition, familiarity with the windows command shell and PowerShell would be useful.

**Topic Outline**

The course is divided into four main topic areas, starting with a deep dive into the operating system artifacts that are stored on disk. We then move to using volatile data from live systems before getting even more technical with memory analysis. Finally, we examine how these concepts translate to analysis of an enterprise environment, covering topics such as Office365, active directory and tools and techniques than can be used across thousands of systems at a time.

**The Windows Operating System**

*File systems and disk management*

The filesystem is the foundation of the operating system. This session will examine how files are stored within key Microsoft filesystems (FAT, NTFS and exFAT) and how the data stored within the filesystem can be used to recreate system activity. It will also examine how the operating system interacts with disks, from identifying which drive letters have been assigned to which volume to linking external devices back to a specific system. We will then review volume and disk level encryption mechanisms, including how to identify when they are in use and techniques that can be used to circumvent the encryption.

*The Registry*

The registry is the primary location used to store system and user configuration information, from user accounts and passwords to the default browser. This session will cover the logical and physical structure of the registry, important registry keys, tools that can be used for analysis, how changes can be tracked, how user (both legitimate and malicious) activity can be identified and how the registry can be used by malware.

*Volume shadow copies*

*Tracking user activity*

- Shortcut files
- Shellbags
- Jump lists
- Recycle bin

**Network configuration**
- Network activity
- Event logs

**Live system evidence collection and analysis**
- Evidence collection
- Process monitoring

**Network traffic analysis**
- Windows protocols

**User management**
- SAM
- Home directories

**Application execution**
- Process and threads
- File handles
- Windows APIs

**Memory**

**Acquisition (remote and local)**

**Data structures**

**Services**

**Malware**

**Networking**

**Windows Applications**

**Services and service management**

**Web browsers**

**Email**

**Social Media applications**

**Windows in the Enterprise**

**Event logs**

**User management**

**Office365**
- Logging and auditing
- Access control and tracking
- Email
- Applications
DNS

Remote access and control

- RDP
- Group Policy
- SCCM

Teaching Methods

Lectures
Hands-on labs
Demonstrations

Classroom Environment

This training environment takes advantage of Virtual Machines located on your course drive. Using this technology, you will engage in hands-on labs and instructor demos of network intrusion concepts in a "real-world" environment. Each VM is pre-configured to mimic the different operating systems, network environments and intrusion issues that may encountered in the wild. You will also be given memory samples, packet captures and volatile data samples for hands-on exercises and labs.

Class Size

Maximum 25 per instructor.

Materials Provided

To achieve the course objectives, you will learn through instructor-led training, demos and hands-on activities and labs. The course materials used in this course include:

- **Student Guides** – The Student Guide contains all speaking points that the instructor will deliver throughout this course. The headings in the student guide correspond directly to the headings in the Instructor slides to make it easy for you to follow along. Many of the concepts and tools that you will learn about throughout this course are presented graphically to help you better understand the course content. To help you practice and test your knowledge, the following hands-on elements, as appropriate, are included in the Student Guide.

- **Activities** – Modules have paper-based hands-on activities that enable you to check your knowledge of the lesson content.

- **Labs** – Modules have hands-on case-based lab exercises where you use the Virtual Machine (VM) to perform technical tasks. Each lab identifies high-level tasks to perform as well as step-by-step instruction. More complex labs will be instructor-led.

Equipment/Software Students Must Furnish:

Students must furnish their own laptop capable of running VMware Workstation or Player (preferably Workstation) and approximately 50GB of free disk space.