WINDOWS FORENSICS

In this course the attendees will learn how to analyze windows operating system. This course is specially designed for Cyber Security professionals who are involved in performing live forensics and investigations during an Incident response process.

In the first part of the course, the attendees will learn different ways to Triage an endpoint using Google Rapid Response, hunt for specific IOC's in multiple endpoints at once. The attendees will also learn how to collect and analyze different types of Artifacts that are present in the system memory, examining and creating Timelines for these Artifacts.

In the second stage, the attendees will learn to analyze raw Disk/Volume. They will be introduced to a tool called Autopsy that will be used throughout the labs to analyze as well as collect Artifacts from raw disk image. Once the Artifacts are collected, they will learn to put those Artifacts in the form of Timeline.

- **2 Days Programme**
- **16 CPE's**
- **Laptop Required**

DETAILED COURSE DESCRIPTION

DAY 1

- Performing Live Forensics and Threat Hunting by using Google Rapid Response.
- Triage and Endpoint Detection and Response using Google Rapid Response.
- Memory Acquisition and Examination
- Memory Analysis Timeline Creation
- Identifying Rogue processes, Process DLLs and Handles in memory.
- Reviewing Network Artefacts, evidence of Code Injection, Check for the signs of Root Kits, Malwares, acquiring Suspicious Processes and Drivers.
- Using Redline for auditing and collecting all running processes and drivers from memory, file system metadata, registry data, event logs, network information, services, tasks and web history.

DAY 2

- Detecting and Analyzing Intrusions through Disk Analysis
- Mounting raw disk file in Windows/Linux
- Understanding Application compatibility Cache, Prefetch, Shimcache, Amcache, RecentFileCache
- Analyzing Windows Volume Shadows
- Detecting Lateral Movements
- Identifying Malware Persistence
- Adversary Tactics, Techniques, and Procedures (TTPs)
- Analyzing windows event logs
- Leveraging Autopsy (Sleuth kit) to examine raw disk
- Filesystem Timeline Creation and Analysis
- Gathering and Analyzing Artifacts from Registry, file system, prefetch, Browser cache, Browser history, Windows event logs stored in raw disk image
- Using Regripper tool to analyze specific content in the registry
- Exporting Registry Artefacts from Autopsy and analyzing them selectively in the Windows Registry Recovery or WRR tool
- Super-timeline Creation, Analysis and Examination

Technical Pre-Requisites

- The attendees should have excellent knowledge of Computers and Operating System Fundamentals.
- Good knowledge of Networking and TCP/IP concepts, basic network troubleshooting, Basic level Knowledge of VMware workstation such as setting up Guest OS, VMware networking.
- The Attendees should have some background in network traffic analysis, log analysis or Security Architecture and system administration.
- The Attendees must have a working knowledge of Windows Operating System, File System, Registry and use of the command line.
- Familiarity with Active Directory and basic Windows security controls, plus common network protocols, is beneficial.

WHO SHOULD ATTEND

- Information security professionals
- Incident response team members
- Law enforcement officers, federal agents, and detectives
- Media exploitation analysts
- Anyone interested in a deep understanding of Windows forensics

Laptop Requirements

- CPU: 64-bit Intel i5/i7 - x64 bit 2.0+ GHz processor or more
- 16 GB RAM or greater, 200 GB of Hard Disk Drive
- VMWare Fusion/Workstation or VMware Workstation player.
- 64-bit version of Windows 7(or above) or Mac OSX
- Install 7-zip on your host OS
- Disable credential guard
- Admin level access to the host operating system as well as guest operating system