Digital Forensic Foundation Course Content -4 Days



Day 1

Section 1 – Introduction to Digital Forensics

- Define Digital Forensics
- Define the Types of Digital Forensic Investigations
- Legal Considerations

Section 2 – Investigation Fundamentals

- Good Practice Guidelines for Digital Evidence
- o The Four Principles of Computer Based Evidence
- o The Basics of a Digital Forensic Investigation

Section 3 – Identification & Seizure of Digital Equipment

- Evidence Handling & Chain of Custody
- o Identifying Electronic Sources of Evidence
- Dealing with Live Systems
- Seizure of Electronic Devices

❖ Section 4 – Forensic Acquisitions

- Source Integrity
- Data Acquisition Types
- o Forensic Acquisitions
- o Forensic Image
- o Forensic Clone
- Forensic Acquisition Tools (FTK Imager)
- Acquisition of Network Shares

Day 2

Section 4 – Forensic Acquisitions - Continue

- Mounting a Forensic Image
- O How to create a Ventoy bootable drive?
- Capturing RAM Memory
- Hash Values (digital fingerprint)

Section 5 – Understanding Hard Drive Terminology

- Traditional Hard Drives
- SSD Hard Drives
- o Understanding Hard Drive Terminology
- Unified Extensible Firmware Interface (UEFI)
- GUID Partition Table (GPT)

Section 6 – File Systems & Data Storage

- NFTS File System
- Data Storage
- o Introduction to Metadata
- Date and Time Stamps
- NTFS Encryption



Day 3

Section 7 – Forensic Analysis Techniques

- Analysis Environments
- o Case Preparation
- File/Folder Recovery
- File Signatures
- o Data Carving
- Data Reduction Methods
- Corroborating Evidence

❖ Section 8 – Windows Forensic Artefacts

- Windows Registry
- o USB Forensics
- Internet History
- Prefetch Files

Day 4

Section 8 – Windows Forensic Artefacts (continue)

- Identifying Installed Software
- Volume Shadow Copies
- Link File Analysis
- Identifying Executed Programs
- Searching the Registry
- Event Logs

❖ Section 9 – Dealing with Digital Evidence for Court

- O How to Prepare a Forensic Report?
- O How to Prepare Evidence for Court?
- Giving Evidence as an Expert Witness

Contact: smith.na@orioninv.co.th