The main object in the digital forensic analysis is the digital device related to the security incident under investigation. The digital device was either used to commit a crime, to target an attack, or is a source of information for the analyst. The goals of the analysis phase in the digital forensics process differ from one case to another. It can be used to support or refute assumptions against individuals or entities, or it can be used to investigate information security incidents locally on the system or over a network.

Digital Forensics Training

Digital Forensics Team

Part I: Introduction to Digital Forensics

This part explains the importance of the principles of the digital forensics process and the approaches that are usually used to conduct an analysis.

Module 1: Intro	What is digital Crime? Digital Forensic Digital evidence Digital Forensic goals Analysis Approach summary

Part II: Data Acquisition

This part discusses hardware and software that are used during acquisition and how to handle the investigation in the crime scene and how to collect volatile data from crime scene.

Module 2: Live Response from Digital Forensics View	Personal Skills Written communication oral communication presentation skills Knowing's one limits Technical skills Security Fundamentals Security principles Risk Network protocols Network security issues Host or system security issues Malicious code Incident Handling skills
Module 3: Volatile Data	Live Acquisition and Jump Bags Hardware duplicator Software duplicator Volatile Data Nonvolatile Data TCPDUMP Wireshark Traffic capturing and analysis Lab Tools: Debian/Kali Linux with: TCPDUMP Wireshark
Module 4: Non volatile Data	Forensic Image from Hard Disk FTK Imager Imaging over network with FTK

	Imaging Over network with DD Virtualization Data Acquisition Wipe Disk in Linux Lab1&2 Tools: Virtual Machine with Debian or Kali Virtual Machine with windows 10 dd tool for windows and Debian Linux with shred command FTK imager for windows

Part III: Windows Artifact	
This Part discuss how to analyze collected data during forensic investigation in a forensically sound manner and how to recover data from FAT/NTFS filesystem and how to examine windows artifacts to get evidence that will prove or refuse hypotheses for the case under investigation.	
Module 5: File System & Data Recovery	Hard drive structure MBR GPT Filesystem Area FAT Filesystem FAT component FAT Limitation NTFS Filesystem NTFS Components MFT Superblock Sleuthkit Volume Layer Filesystem Layer Data layer Lab Tools: Autopsy Foremost Binwalk
Module 6: Registry analysis	Registry Structure Backing up Registry Extracting Registry hives Parsing Registry Hives Autorun keys Lab Extracting Autoruns and installed Application from registry hives Lab Tools:

	Regripper Sysinternals Registry Explorer/RECMD FTK imager
Module 7: Windows Artifacts analysis	Microsoft Edge History Cache Cookies Session Restore Firefox Places.sqlite Cookie.sqlite Cache Other Browser PST Email Investigation Leaking Data Case Lab Tools: Sqlite Viewer SQLECMD Autopsy
Module 8: Memory Forensics	Memory Structure Memory Acquisition Sources of memory dump Hibernation file Crash dump Page files Process in memory Network Connection DLL injection Remote DLL injection Remote Code injection reflective DLL injection Memory analysis Volatility Framework Redline Memory Forensics Lab Lab Tools: Debian or Kali virtual machine Volatility Rekall Redline

Part IV: Mobile Forensics	
This part will discuss mobile forensics and how to acquire and analyze a mobile device and what are the shortfalls to data extraction and acquisition and shortfalls for the analysis tools	
Module 9: Mobile Forensics	Introduction to smartphones Smartphone Components and Identifiers Common File Systems Smartphone Handling Preserving smartphone Evidence Preventing Data Destruction Forensic Acquisition of smart phone Logical Acquisition Physical Acquisition Advanced Acquisition tools and tech Smartphone Tools overview Oxygen Forensics XRY AXIOM Android Forensics Overview IOS Forensics Overview Cloud Data Extraction Lab Mobile Forensics Tools: Magnet Axiom or Oxygen forensics

Notes

- There’ll be slides for the covered modules
- All attendance should bring their own laptop as there’ll be lots of hands-on exercises during the training.