Mindluster Platform

About the course Digital Forensics

Course Presenter : Louay Karadsheh, PhD, CISSP, CEH, CASP

Digital Forensics course provides comprehensive training in investigating and analyzing digital evidence to uncover cybercrimes. Explore techniques for data acquisition, preservation, and analysis. Learn about computer systems, networks, and mobile devices forensics. Develop skills to identify and track digital footprints, recover deleted data, and present findings in legal proceedings. Gain hands-on experience with forensic tools and methodologies. Join this course to become a proficient digital forensics investigator and contribute to combating cybercrime. Louay Karadsheh, PhD, CISSP, CEH, CASP

Computer Science Category's Courses

Course Lesson(48)

Lesson 1 : **An Introduction to the field of Digital Forensics**

Lesson 2 : **How to learn Digital Forensics by yourself**

Lesson 3 : **What are the top skills you must learn in Digital Forensics**

Lesson 4 : **Kill Chain and the MITRE Matrix**

Lesson 5 : **How do Digital Forensics skill augment other cyber domains**

Lesson 6 : **Introduction to Windows Forensics**

Lesson 7 : **Setting up a lab to practice Windows Forensics**

Lesson 8 : **Introduction to Linux Forensics**

Lesson 9 : **Top 10 forensic artefacts and data sources on Linux**

Lesson 10 : **What is a structured investigation process**

Lesson 11 : **Setting up a lab to practice Linux Forensics**

Lesson 12 : **Introduction to Memory Forensics**

Lesson 13 : **Setting up a lab to practice Memory Forensics**

Lesson 14 : **The Memory Forensics tools you need to learn and master**

Lesson 15 : **The Linux Forensics tools you need to learn and master**

Lesson 16 : **Top 10 forensic artefacts and data sources on Windows**

Lesson 17 : **The Windows Forensics tools you need to learn and master**

Lesson 18 : **A simple process for performing a digital forensics investigation on Windows**

Lesson 19 : **The Rootkit Paradox**

Lesson 20 : **How to investigate Windows Event Logs**

Lesson 21 : **How to investigate Windows Prefetch Files**

Lesson 22 : **How to investigate the Windows Registry**

Lesson 23 : **How to investigate Linux System Logs**

Lesson 24 : **How to investigate Linux Systemd Journal**

Lesson 25 : **How to investigate Linux User Artefacts**

Lesson 26 : **A Simple Process to Analyse Malware Samples with Memory Forensics**

Lesson 27 : **Analyzing a malware sample with Memory Forensics**

Lesson 28 : **Memory Dump Formats and Memory Acquisition Types**

Lesson 29 : **Understanding file formats and magic numbers**

Lesson 30 : **Lab Setup for Analyzing Malicious Files and Executables**

Lesson 31 : **Executable File Types in Windows and Linux**

Lesson 32 : **Introduction to Email Forensics**

Lesson 33 : **How to investigate malicious Microsoft Office files**

Lesson 34 : **How to investigate a malicious disk image file**

Lesson 35 : **How to investigate Firefox browser artefacts**

Lesson 36 : **How to investigate Chrome browser artefacts on Linux**

Lesson 37 : **Getting started with the Volatility Framework**

Lesson 38 : **Investigating Processes with Volatility Part 1**

Lesson 39 : **Investigating Processes with Volatility Part 2**

Lesson 40 : **Using Community Plugins with Volatility**

Lesson 41 : **Investigating Network Artefacts with Volatility**

Lesson 42 : **Investigating Registry Artefacts with Volatility**

Lesson 43 : **Recovering Windows Event Logs from a Memory Dump**

Lesson 44 : **Investigating Disk Artefacts with Volatility**

Lesson 45 : **Using YARA Rules with Volatility**

Lesson 46 : **How to perform Email Forensics on a Gmail account**

Lesson 47 : **How to investigate a malicious batch script**

Lesson 48 : **How to investigate a malicious DLL**

Related courses

Linear Algebra for Computer Scientists

Insertion Sort

Bubble Sort

GCSE Computer Science

Random Access Memory



for Business Contact
business@mindluster.com