Malware Analysis: Reverse Engineering for Investigators Training Course

Professional Development Training Course Outline

Category	Criminology	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Cybercrime is evolving at an unprecedented pace, with threat actors deploying sophisticated malware to breach systems, steal sensitive data, and disrupt operations. Training Course on Malware Analysis: Reverse Engineering for Investigators equips investigators, cybersecurity analysts, and digital forensic professionals with essential skills to deconstruct, analyze, and trace malware operations. With the rise in ransomware, advanced persistent threats (APTs), and zero-day exploits, law enforcement and cyber professionals must stay ahead by mastering binary analysis, dynamic investigation techniques, and malware behavior profiling.

This hands-on course combines theory with real-world case studies to help learners build proficiency in reverse engineering malicious code, understanding attacker tactics, and employing advanced forensic tools. Through in-depth modules and interactive labs, participants will explore Windows and Linux malware, unpack obfuscated binaries, detect hidden payloads, and apply memory forensics to investigate cyber incidents. Whether you're part of a government agency, corporate security team, or incident response unit, this course prepares you for the real-world battlefield of cybercrime investigations.

Programme Curriculum

Malware Analysis: Reverse Engineering for Investigators Training Course

Introduction

Cybercrime is evolving at an unprecedented pace, with threat actors deploying sophisticated malware to breach systems, steal sensitive data, and disrupt operations. Malware Analysis: Reverse Engineering for Investigators Training Course equips investigators, cybersecurity analysts, and digital forensic professionals with essential skills to deconstruct, analyze, and trace malware operations. With the rise in ransomware, advanced persistent threats (APTs), and zero-day exploits, law enforcement and cyber professionals must stay ahead by mastering binary analysis, dynamic investigation techniques, and malware behavior profiling.

This hands-on course combines theory with real-world case studies to help learners build proficiency in reverse engineering malicious code, understanding attacker tactics, and employing advanced forensic tools. Through in-depth modules and interactive labs, participants will explore Windows and Linux malware, unpack obfuscated binaries, detect hidden payloads, and apply memory forensics to investigate cyber incidents. Whether you're part of a government agency, corporate security team, or incident response unit, this course prepares you for the real-world battlefield of cybercrime investigations.

Course Objectives

1. Understand the fundamentals of malware architecture and behavior analysis
2. Master techniques of static and dynamic malware analysis
3. Use tools like IDA Pro, Ghidra, and x64dbg for reverse engineering malware
4. Analyze PE file structures and identify malware infection vectors
5. Perform sandboxing and behavioral tracking using virtual environments
6. Apply code deobfuscation and unpacking techniques to hidden payloads
7. Identify and track command and control (C2) communication patterns
8. Detect persistence mechanisms used by rootkits and trojans
9. Utilize memory forensics tools for live malware inspection
10. Analyze ransomware encryption mechanisms and recovery strategies
11. Understand the use of cryptographic functions in malicious code
12. Document and report findings with evidence integrity and legal compliance
13. Apply learned skills in real-world malware investigation case studies

Target Audience

1. Cybercrime Investigators
2. Digital Forensic Analysts
3. Incident Response Teams
4. Cybersecurity Professionals
5. Law Enforcement Agencies
6. Threat Intelligence Analysts
7. Security Engineers
8. Penetration Testers and Ethical Hackers

Course Duration: 10 days

Course Modules

Module 1: Introduction to Malware Analysis

- Definition and classification of malware
- Goals and objectives of malware analysis
- Differences between static and dynamic analysis
- Legal and ethical considerations
- Tools overview: Ghidra, IDA Pro, OllyDbg
- **Case Study**: Analyzing a real-world phishing malware sample

Module 2: Setting Up a Safe Malware Analysis Lab

- Virtualization tools and network isolation
- Snapshots and rollback strategies
- Installing analysis tools
- Creating honeypots and test environments
- Securing the analysis machine

- **Case Study**: Lab setup for analyzing WannaCry ransomware

Module 3: Static Analysis Techniques

- PE file structure and headers
- Disassembling executables
- String analysis and metadata
- Import/export table inspection
- Identifying packers and signatures
- **Case Study**: Static analysis of a cryptojacking malware

Module 4: Dynamic Analysis and Behavior Tracking

- API call monitoring
- File system and registry changes
- Network activity and packet capture
- Runtime debugging basics
- Using tools like Process Monitor and Wireshark
- **Case Study**: Behavior analysis of a botnet client

Module 5: Reverse Engineering Essentials

- Assembly language basics
- Control flow graphs
- Stack and heap analysis
- Decompiled code vs disassembly
- Identifying malware routines
- **Case Study**: Reverse engineering an exploit kit payload

Module 6: Unpacking and Deobfuscation

- Manual unpacking techniques
- Common packers and crypters
- XOR and base64 decoding
- Anti-debugging and anti-VM tricks
- Scripted deobfuscation using Python
- **Case Study**: Unpacking and analyzing a packed trojan

Module 7: Memory Forensics

- Memory dumping and acquisition
- Volatility Framework usage
- Analyzing memory-resident malware
- Identifying hidden processes
- Live system triage vs offline analysis
- **Case Study**: Investigating a memory-injected banking trojan

Module 8: Network Forensics in Malware Analysis

- Packet capture tools: Wireshark, TCPdump
- Detecting C2 communications
- DNS tunneling and covert channels
- Protocol analysis and flow correlation
- Indicators of compromise (IoC) extraction
- **Case Study**: Tracing C2 servers from a RAT infection

Module 9: Ransomware Analysis and Decryption Techniques

- Encryption algorithms used in ransomware
- Understanding ransom notes and delivery methods
- File recovery and backup strategies
- Ransomware variants overview
- Working with NoMoreRansom project
- **Case Study**: Decrypting files from a STOP/Djvu ransomware infection

Module 10: Linux Malware Analysis

- ELF file analysis
- Linux persistence mechanisms
- Rootkits and backdoors
- Reverse engineering bash scripts and binaries
- Behavioral analysis on Linux VMs
- **Case Study**: Dissecting a Linux cryptominer

Module 11: Mobile Malware Analysis (Android Focus)

- APK decompilation and smali code
- Mobile sandboxing tools
- Permissions and malicious intents
- Code injection techniques
- Reverse engineering with JADX
- **Case Study**: Analysis of a malicious Android SMS stealer

Module 12: IoT Malware and Embedded Device Analysis

- Architecture of IoT threats
- Reverse engineering firmware
- Static analysis of MIPS/ARM binaries
- Vulnerability discovery in IoT systems
- Behavioral analysis with simulated devices
- **Case Study**: Investigating Mirai botnet malware

Module 13: Malware Attribution and Threat Intelligence

- Malware family classification
- Threat actor profiling
- Tactics, Techniques, and Procedures (TTPs)
- Linking malware to campaigns
- Using platforms like MISP and VirusTotal
- **Case Study**: Attribution of malware to APT29

Module 14: Reporting and Documentation

- Report writing structure
- Technical vs non-technical reporting
- Chain of custody
- Screenshot and evidence management
- Integrating findings into threat feeds
- **Case Study**: Compiling a malware investigation report for court submission

Module 15: Capstone Project

- Students analyze a complex malware
- Prepare static, dynamic, and memory reports

- Present findings with full documentation
- Peer reviews and evaluation
- Integration with SIEM and threat tools
- **Case Study**: Full malware investigation simulation from infection to reporting

Training Methodology

- Hands-on labs and live malware dissection
- Tool-based demonstrations using real-world samples
- Instructor-led walkthroughs of malware behavior
- Interactive Q&A and group discussions
- Case study reviews with guided analysis
- Project-based learning and skill assessments

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com