COURSE SYLLABUS

Malware Analysis Fundamentals (Intermediate) Course

Work through both static analysis (examining files without running them) and dynamic analysis (interpreting behavior from sandbox and monitoring reports), and build the judgment to know which technique fits each situation. Following NIST SP 800-83 Rev. 1, the course brings in the tools analysts rely on — disassemblers, sandboxes, YARA, network capture, and CISA's Malware Next-Gen — with a federal thread on sample sensitivity and data handling throughout.

> Group classes in Live Online and onsite training is available for this course. For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/courses/intermediate-malware-analysis-fundamentals

support@graduateschool.edu •
(888) 744-4723

Course Outline

Module 1

Foundations & Isolated Analysis Environments

Module 2

Static Analysis Fundamentals

Module 3

Static Analysis: Disassembly & Code-Level Review

Module 4

Dynamic Analysis Fundamentals — via example reports, no lab

Module 5

Network & Behavioral Analysis

Module 6

Toolkits & Federal Analysis Platforms

Module 7

Reporting, MARs & Best Practices

Module 8

Capstone Analysis Exercise & Program Development