



N X 2 1 2

PRACTITIONER • LEVEL 3

Windows Forensics

11

MODULES

243

LAB TASKS

158

CTF CHALLENGES

82

TOPICS

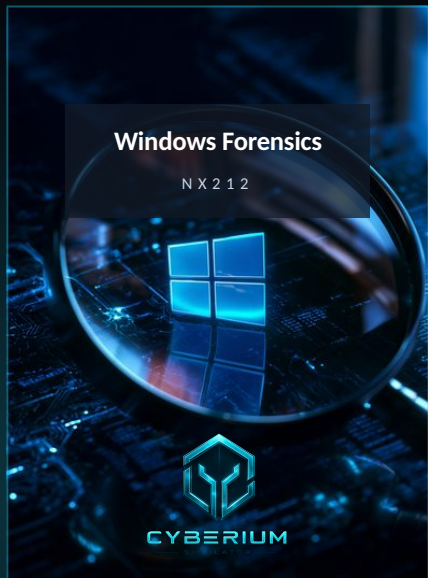
11

COURSE BOOKS

128

SLIDES

11 COURSE BOOKS INCLUDED



This program transforms students into digital investigators by diving deep into the world of data forensics. Participants master the art of file and disk handling, learning to uncover hidden information through steganography and advanced encoding techniques. Using industry-standard tools like the Forensic Toolkit (FTK), students gain hands-on experience in hard disk analysis and registry investigation. The journey culminates in high-level cyber forensics-including memory, network, and malware analysis-equipping graduates with the comprehensive toolkit needed to lead complex digital investigations.

CURRICULUM & WHAT EACH MODULE COVERS

MODULE	TASKS
01 Files and Disks Digital Storage Units and Disk Sectors · Disk-Level Data Recovery and Forensic Comparison · +6 more	21
02 Automatic Carving Automatic Offset Detection with Binwalk · Automated Carving with Foremost and Scalpel · +5 more	23
03 Metadata Tools for Extracting and Inspecting Metadata · Metadata in Audio Files (MP3/ID3 Tags) · +5 more	20
04 Steganography Automated File Carving from Data Blobs · Password-Protected Steganography with Steghide and StegSeek · +3 more	23
05 File System Analysis NTFS File System and Its Metadata Files · Parsing and Analyzing the Master File Table (MFT) · +6 more	20
06 Registry Analysis User Account and Authentication Forensics · Persistence and System Event Artifacts · +5 more	25
07 Artifacts NirSoft Utility Suite for Targeted Artifact Recovery · Network Evidence and Attack Tooling Artifacts · +6 more	19
08 Memory Analysis System & Timeline Metadata Analysis · Command-Line & Execution History Analysis · +6 more	24
09 Windows Events Object Access and System Configuration Events · Configuring Windows Audit Policies · +6 more	20
10 Network Analysis DNS Resolution and the Dark Web · Extracting Files and Metadata from Traffic · +6 more	24
11 Malware Analysis Building a Malware Analysis Sandbox · Static Analysis: Extracting Text and Metadata · +6 more	24

GOOD TO KNOW

Best after a level 1–2 programme · Self-paced or trainer-led · Cy, the AI helper, answers in the student’s own language

HOW EVERY MODULE RUNS

Lab

→

Extra at 80%

→

Timed test at 85%

→

Slides at 90%

A REAL TASK FROM MODULE 9 — WINDOWS EVENTS

“Use Hydra to brute-force the RDP service, then check the TerminalServices-RemoteConnectionManager logs for the event ID of a successful login.”

Finish with a capstone project · interview preparation · City & Guilds Assured certificate

DATA AS OF 2026-10-12 · V261012