



N X 2 1 2

PRACTITIONER • LEVEL 3

# Windows Forensics

11

MODULES

243

LAB TASKS

154

CTF CHALLENGES

82

TOPICS

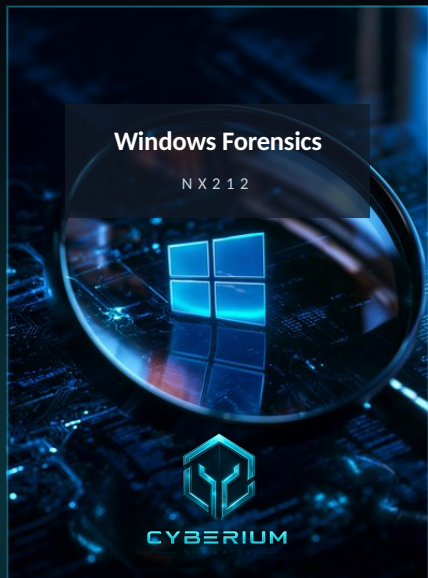
11

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 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| <b>01 Files and Disks</b><br>Digital Storage Units and Disk Sectors · Disk-Level Data Recovery and Forensic Comparison · <a href="#">+6 more</a>        | 21    |
| <b>02 Automatic Carving</b><br>Automatic Offset Detection with Binwalk · Automated Carving with Foremost and Scalpel · <a href="#">+5 more</a>          | 23    |
| <b>03 Metadata</b><br>Tools for Extracting and Inspecting Metadata · Metadata in Audio Files (MP3/ID3 Tags) · <a href="#">+5 more</a>                   | 20    |
| <b>04 Steganography</b><br>Automated File Carving from Data Blobs · File Concatenation Steganography · <a href="#">+3 more</a>                          | 23    |
| <b>05 File System Analysis</b><br>NTFS File System and Its Metadata Files · Parsing and Analyzing the Master File Table (MFT) · <a href="#">+6 more</a> | 20    |
| <b>06 Registry Analysis</b><br>User Account and Authentication Forensics · Persistence and System Event Artifacts · <a href="#">+5 more</a>             | 25    |
| <b>07 Artifacts</b><br>NirSoft Utility Suite for Targeted Artifact Recovery · Network Evidence and Attack Tooling Artifacts · <a href="#">+6 more</a>   | 19    |
| <b>08 Memory Analysis</b><br>System & Timeline Metadata Analysis · Command-Line & Execution History Analysis · <a href="#">+6 more</a>                  | 24    |
| <b>09 Windows Events</b><br>Object Access and System Configuration Events · Configuring Windows Audit Policies · <a href="#">+6 more</a>                | 20    |
| <b>10 Network Analysis</b><br>DNS Resolution and the Dark Web · Extracting Files and Metadata from Traffic · <a href="#">+6 more</a>                    | 24    |
| <b>11 Malware Analysis</b><br>Building a Malware Analysis Sandbox · Static Analysis: Extracting Text and Metadata · <a href="#">+6 more</a>             | 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 2026-09-30 · V260930