

Digital Forensics: NTFS Analysis & Memory Capture

Learn to acquire, analyse and interpret digital evidence from Windows systems, memory, file systems and logs.

15

MODULES

25

TOPICS

COURSE OVERVIEW

This course covers the digital forensic investigation process, data theft scenarios and data acquisition methods, including solid state devices, Windows domains, RAID's and virtualised systems. It then addresses volatile data and memory capture, collection from sources such as Exchange servers, web-mail, Facebook and Linux or Mac systems, and forensic examination of FAT32, NTFS and ExFAT file structures. Further modules examine data deletion and wiping, tracing system and user activity, log file analysis, databases such as SQLite, Volume Shadow Copies, File History and NTFS journals.

WHO THIS COURSE IS FOR

Digital Forensic Investigators

Incident Responders

IT Security Analysts

Law Enforcement Officers

System Administrators

LEARNING OBJECTIVES

- Describe the digital forensic investigation process and best practice
- Analyse methods of data theft and mitigation approaches
- Apply data acquisition techniques to images, clones and solid state devices
- Gather evidence from Windows Domain Controllers and file shares
- Identify and rebuild RAID's and examine virtualised systems
- Capture and investigate volatile memory using volatility
- Interpret FAT32, NTFS and ExFAT file system structures
- Trace system and user activity through registry and log analysis

15 Modules, 25 Topics

01

Digital Forensic Investigations

TOPICS

- A review of the investigation process, best practice and equipment

02

Data Theft

TOPICS

- How can data be stolen, investigated and possibly mitigated?

03

Data Acquisition

TOPICS

- Images and Clones; Static, Booted and Live; Physical and selective
- Solid State devices
- Considerations and associated problems

04

Windows Domains

TOPICS

- Gathering information from Domain Controllers
- Capturing File Shares and inaccessible systems

05

RAID's and Virtualisation

TOPICS

Identifying and rebuilding RAID's · Capturing and examining virtualised systems

06

Volatile Data

TOPICS

- Memory capture and volatile data collection from 'live' systems
- Investigating memory using volatility

07

Data Collection - Other Sources

TOPICS

Exchange servers and web-mail · Facebook, Websites, Linux and Macs

08

File Systems Revisited

TOPICS

- Understanding FAT32, NTFS and ExFAT data structures from a forensic perspective

09

Data Deletion and Wiping

TOPICS

Windows Recycle Bins · Testing wiping software

10

Tracing System Activity

TOPICS

- Investigating the Windows Registry, User Accounts, Event Logs and USB connected devices

11

Tracing User Activity

TOPICS

- Identifying Program execution, Files opened and Folder navigation
- Windows Object ID's and file tracking

12

Log File Analysis

TOPICS

Web and FTP logs · Examination using Cygwin

13

Databases

TOPICS

SQLite and Chrome browser artefacts

14

Volume Shadow Copies and File History

TOPICS

Approaches to extracting data from VSC's · Windows File History

15

NTFS Journals

TOPICS

- Understand the value of the NTFS journal in investigations

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

ABOUT KOENIG

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

Learn the Way That Suits You

Classroom Training

Live Online Classes (ILO)

Fly-Me-A-Trainer (FMAT)

Flexi (Self-Paced)

1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

[Visit koenig-solutions.com](https://www.koenig-solutions.com)

info@koenig-solutions.com