DATA SHEET

# Digital Forensics and Incident Response Fundamentals

Protect your organization from vulnerabilities that can disrupt business operations

## Highlights

### Duration

4 days

### Prerequisites

Students taking this course should have a working knowledge of Windows/Linux/macOS operating systems, and network technologies. Basic understanding of information security, command line syntax, malware, and analytical thinking recommended.

### How to Register

This course is available for purchase at https://training-catalog.trellix.com.

Private sessions are available. For further details and pricing, please contact your Trellix account representative.

Instructor-led sessions are typically a blend of lecture and hands-on lab activities. To view our full course catalog, please visit https://training- catalog.trellix.com.

This entry-level course in digital forensics and incident response provides foundational knowledge in incident response preparation, detection and analysis, containment, eradication, recovery, and post-incident activities, including lessons learned. This course employs open-source tools to perform triage and forensics analysis in hands-on labs, touching on the key artifacts of Microsoft Windows, Linux, and Apple macOS systems.

This course is part of the Trellix Cyber Operations team's Foundations in Incident Response Education (FIRE) track of general defensive security training. Learners are provided a blend of lecture, discussions, and hands-on labs.

## Learning Objectives

After completing this course, learners should be able to:

- Define key terms in digital forensics and incident response
- Describe the U.S. NIST incident response lifecycle
- Apply standard methodologies to artifact collection
- Explain proper evidence handling techniques and chain of custody procedures
- Identify key artifacts and their importance in forensics analysis
- Apply the MITRE ATT&CK framework to DFIR objectives

## Who Should Attend

This course is intended for incident responders, information security staff, auditors, SOC analysts, investigators, and consultants responsible for digital forensics and incident response.

## Course Outline

1. Course Introduction
2. Malware Overview
3. Malware Lab Construction
4. Analysis Techniques
5. Network Analysis
6. Delivery Vectors
7. Executables
8. Defensive Techniques of Malware
9. Modern OS Defenses