

CVFE Certified Virtualization Forensics Examiner

Overview

This course brings together two challenging areas facing IT security professionals today: incident response and virtualization. Forensics is at the heart of incident response, and therefore this training will focus on how to gather evidence relating to an incident – the what, when, where, who and why of an incident – within today’s common virtual environments.

Upon Completion

Students will:

- Have knowledge to perform network forensic examinations.
- Have knowledge to accurately report on their findings from examinations
- Be ready to sit for the C)NFE Exam

Course Length

5 days

Format

- Instructor-led classroom
- Instructor-led Online Training

Prerequisites

- Must have a Digital or Computer Forensics Certification or equivalent knowledge

Student Materials

- Student workbook
- Student lab guide

Who Should Attend?

- Digital & Network Forensic Engineers
- IS & IT managers
- Network Auditors

Exam Information

The Certified Virtualization Forensics Examiner exam is taken online through your Mile2.com account. The exam will take 2 hours and consists of 100 multiple choice questions.

Course Objectives

- Participants will be able to apply forensically-sound best practice techniques against virtual infrastructure entities in the following use case scenarios:
- Identifying direct evidence of a crime
- Attributing evidence to specific suspects
- Confirming (or negating) suspect alibis
- Confirming (or negating) suspect statements
- Determining (or negating) suspect intent
- Determining (or negating) Identifying sources
- Determining (or negating) Authenticating documents

Course Contents

- Module 1 –Digital Forensics –the what, where, when, how and why
- Module 2 –Virtual Infrastructure
- Module 3 –Forensic Investigation Process
- Module 4 –VI Forensics Scenario 1: Identifying direct evidence of a crime
- Module 5 –VI Forensics Scenario 2: Attributing Evidence to Specific Requests
- Module 6 –VI Forensics Scenario 3: Confirming (or negating) suspect alibis
- Module 7 –VI Forensics Scenario 4: Confirming (or negating) suspect statements
- Module 8 –VI Forensics Scenario 5: Determining (or negating) suspect intent
- Module 9 –VI Forensics Scenario 6: Identifying sources
- Module 10 –VI Forensics Scenario 7: Authenticating documents
- Module 11 –Putting it all together –Course Summary