Certified Virtualization Forensics Examiner

KEY DATA

Course Name: Certified Virtualization Forensics Examiner

Duration: 5 Days

Language: English

Format
Instructor Led Training
Instructor Led Online Training

Prerequisites:
Must have a Digital or Computer Forensics Certification or equivalent knowledge

Student Materials:
Student Workbook
Student Lab Guide

Certification Exams:
Certified Virtualization Forensics Examiner

CEUs: 40

WHO SHOULD ATTEND?

Virtual infrastructure specialists
(Architects, engineers, Administrators), Forensic investigators Forensic investigators

COURSE OVERVIEW

This course takes two enormously challenging areas facing IT security professionals today: incident response and virtualization and attempts to meld these together. 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. Additionally, the course will take a deep dive into the virtual infrastructure, and contrast the various virtual entities against their physical counterparts. This will allow a clear demonstration of the forensically-relevant differences between the virtual and physical environments. The course uses a lab-centric, scenario-based approach to demonstrate how to forensically examine relevant components of a virtual infrastructure for specific use cases.

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
- Identifying sources
- Authenticating documents

Career Specialized

All combos Include:

- Online Video
- Electronic Book (Workbook/Lab guide*)
  *in technical classes only
- Exam Prep Questions
- Exam

C)VFE™

mile2®
CYBER SECURITY CERTIFICATIONS

ACCREDITATIONS

COMMITTEE ON NATIONAL SECURITY SYSTEMS
CNSS
SYSTEMS SECURITY FOR THE 21st CENTURY

NICCS™
NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY BRAVERY INTEGRITY

mile2 is **ACCREDITED** by the **NSA CNSS 4011-4016**
Is **MAPPED** to NIST/Homeland Security NICCS's Cyber Security Workforce Framework
is **APPROVED** on the **FBI Cyber Security Certification Requirement list (Tier 1-3)**

UPON COMPLETION

Students will:

Have knowledge to perform virtualization forensic examinations.
Have knowledge to accurately report on their findings from examinations
Be ready to sit for the **C)VFE** Exam

EXAM INFORMATION

The **Certified Virtualization Forensics Examiner** exam is taken online through Mile2's Assessment and Certification System ("MACS"), which is accessible on your mile2.com account. The exam will take 2 hours and consist of 100 multiple choice questions. The cost is $500 USD and must be purchased from Mile2.com.

macs
Assessment & Certification System

OUTLINE

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

COURSE DETAILS

Module 1: Digital Forensics - the what, where, when, how and why
Module 2: Virtual Infrastructure

- Vendor-neutral VI Architecture Principals
  - Hypervisors
  - Virtual Machines
  - Virtual Networks
  - Virtual Disks
  - Virtual File Systems
  - Migration of Virtual Components
- Vendor-specific VI Architecture
  - vSphere
  - Hyper-V
  - XenServer
- Key Differences Between Physical and Virtual Infrastructures

Module 3: Forensic Investigation Process

- Physical Infrastructure Best Practices
  - Practices Equally Applicable Within Virtual Infrastructures
- Virtual Infrastructure Best Practices
  - Practices Unique To Virtual Infrastructures

Module 4: VI Forensics Scenario 1: Identifying direct evidence of a crime
Module 5: VI Forensics Scenario 2: Attributing evidence to specific suspects
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