# Certified Virtualization Forensics Examiner (C)VFE)

**Modality: Virtual Classroom**

**Duration: 5 Days**

**SATV Value:**

**CLC:**

**NATU:**

**SUBSCRIPTION: No**

## About this course:

This course attempts to meld together two different, immensely challenging facets that today's IT security professionals face: incidence response and virtualization. Forensics lies at the core of incidence response, and the training in this course centers around the gathering of evidence related to an incident within the common virtual environments of today by means of the questions of what, when, where, who, and why. Furthermore, the course also focuses on visual infrastructure, and provides clear contrasts between the range of various virtual entities and their physical counterparts, hence allowing for straightforward demonstrations of the relevant differences between the virtual and physical environments.

This course is centered around lab work and uses a scenario-based approach, hence demonstrating the method of forensically examining all relevant components of a virtual infrastructure for specific use cases. This course also prepares the students for the C)VFE Exam.

The salary for a Virtualization Desktop Engineer averages **$63,383** per annum.

## Course Objective:

Upon the completion of this course, students will be able to:

- Establish direct evidence of a crime
- Ascribe evidence to specific suspects
- Determine (or negate) suspect alibis and suspect statements
- Determine (or negate) suspect intent
- Establish sources and authenticate documents

## Audience:

This course is intended for:

- Virtual infrastructure specialists (architects, engineers, administrators)
- Forensic investigators

## Prerequisites:

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

## Suggested prerequisites courses:

- Virtualization Technologies Introduction

## Course Outline:

- **Module 1 – Digital Forensics – the what, where, when, how and why**
- **Module 2 – Virtual InfrastructureModule 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**