Certified Virtualization Forensics Examiner (C)VFE)

Modality: Virtual Classroom

Duration: 5 Days

About this course:

This course endeavors to merge together two extraordinary, tremendously testing features that the experts of present IT security face: incidence virtualization and response. Forensics lies at the occurrence reaction core, and the preparation of this course aims the get-together of proof identified with an episode inside the basic virtual conditions of today by methods for the inquiries of when, what, who, where, and why. Moreover, the course likewise targets around the visual framework, and gives away from between the scope of different virtual elements and their physical partners, subsequently taking into account direct exhibitions of the applicable contrasts between the physical and virtual situations.

This course is based on lab work and uses a situation based methodology, consequently exhibiting the strategy for forensically analyzing every single significant part of the virtual foundation for explicit use cases. Also, this course readies the understudies for the exam of CVFE.

The compensation for a Virtualization Desktop Engineer midpoints $63,383 per annum.

Course Objective:

Upon the fulfillment of this course, understudies will have the option to:

- Set up direct proof of a wrongdoing
- Ascribe proof to explicit suspects.
- Decide (or nullify) suspect statements and suspect alibis
- Decide (or invalidate) suspect expectation
- Set up sources and confirm reports
- Virtual Infrastructure
- Digital Forensics – the where, what, how, when, and why
- Identifying direct evidence of a crime
- Forensic Investigation Process
- Confirming (or negating) suspect alibis
- Attributing Evidence to Specific Requests
- Determining (or negating) suspect intent
- Confirming (or negating) suspect statements
- Identifying sources

Audience:

This course is proposed for:

- Virtual infrastructure architects, specialists, administrators, engineers

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

Prerequisites:

Should have a Computer or Digital Forensics Certification or equal information

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**