

# Ultimate Bootcamp®

"Where Great IT Professionals Go For Great Training"

[www.UltimateBootcamp.net](http://www.UltimateBootcamp.net)



## Virtual Infrastructure Forensics

**Examine. Discover. Report.**

### Course Overview

This course attempts to marry two enormously challenging areas facing IT security professionals today: incidence response and virtualization. The cat-and-mouse game between policy enforcers and incident perpetrators within traditional, physical enterprises, is even more pronounced as enterprise architects seek to avail the benefits of virtual platforms, operating systems, applications, processes and desktops.

The great news is that we have an opportunity to embed features within the virtual components of our enterprise architecture, so as to make incidence response that much easier. We will discuss these here. And for those already operating within a virtual environment, we will explore emerging techniques, tools and tips to plan and control virtual incidence response more effectively. This course takes the point of view that forensics is at the heart of incidence response, and so will focus on how to gather evidence relating to an incident – the what, when, where, who and why of an incident – within common virtual environments today.

Digital forensics is the 'forensically-sound' acquisition of evidence from computers, networks, data repositories and fixed or mobile client devices, to support a specific hypothesis. Techniques and tools have been developed to deal with the various scenarios in which forensics investigators find themselves. Increasingly though, forensics investigators have been called on to forensically examine hybrid infrastructures consisting of both physical and virtual entities; some have been asked to examine purely virtual infrastructures. Do current techniques and tools, designed for physical infrastructure-based scenarios, lend themselves naturally to virtual infrastructures? Yes, and, no. This course will dive deeply into what is commonly referred to as a "virtual infrastructure" by three vendors (VMware, Microsoft and Citrix), and contrast the various virtual entities against their physical counterparts, clearly demonstrating the forensically-relevant differences therein; we will then utilize 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
- Be Prepared to take the CVFE Exam

### Audience

This course is designed for the following participant types:

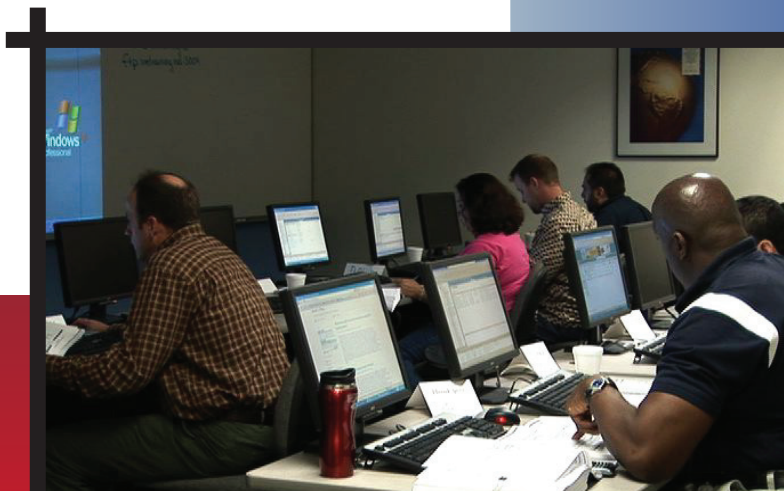
- Virtual infrastructure specialists (architects, engineers, administrators) who desire to augment their virtual infrastructure expertise with forensically-sound best practices knowledge and skills; and
- Forensic investigators who wish to investigate virtual infrastructure components with the same degree of skill and use of best practices they apply to the physical infrastructure components they currently investigate.

### Prerequisites

Must have a Digital or Computer Forensics certification or equivalent knowledge

VIRTUAL INTRASTRUCTURE  
FORENSICS

**Call Ultimate Bootcamp Today!**  
**1-877-484-1182**





## Virtual Infrastructure Forensics

### Course Outline

#### Course Modules

**1. Digital Forensics - the what, where, when, how and why**

#### **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
    - ESX 4.x
    - ESXi 4.x
    - vCenter 4.x
  - Hyper-V
  - XenServer
- Key Differences Between Physical and Virtual Infrastructures

#### **3. Forensic Investigation Process**

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

**4. VI Forensics Scenario 1: Identifying direct evidence of a crime**

**5. VI Forensics Scenario 2: Attributing evidence to specific suspects**

**6. VI Forensics Scenario 3: Confirming (or negating) suspect alibis**

**7. VI Forensics Scenario 4: Confirming (or negating) suspect statements**

**8. VI Forensics Scenario 5: Determining (or negating) suspect intent**

**9. VI Forensics Scenario 6: Identifying sources**

**10. VI Forensics Scenario 7: Authenticating documents**

**11. Putting it all together – course summary**

**Certification Exam –**

**"Certified Virtualization Forensics Expert"**



**Call Ultimate Bootcamp Today! 1-877-484-1182**  
or Visit Us Online at [www.UltimateBootcamp.net](http://www.UltimateBootcamp.net)