

## Advanced Computer Forensics Boot Camp

### Overview

This in-depth course teaches you advanced computer forensics. This course is intended for those that have either taken the InfoSec Institute Computer Forensics Boot Camp, or have experience in the computer forensic profession.

### Target Audience

### Course Objectives

Apply advanced computer forensic analysis concepts to live case work  
Respond appropriately to immediate response situations  
Perform Volume Shadow Copy (VSC) analysis  
Advanced level file and data structure analysis for XP, Windows 7 and Server 2008/2012 systems  
Registry analysis for XP and Windows 7/8 systems  
Malware detection and analysis  
Timeline Analysis  
Windows Application Analysis  
Mobile Forensics

### Course Outline

#### Advanced Analysis Concepts

Windows Versions  
Analysis Principles  
Goals  
Tools Versus Processes  
Locard's Exchange Principle  
Avoiding Speculation  
Direct and Indirect Artifacts  
Least Frequency of Occurrence  
Documentation  
Convergence  
Virtualization

#### Immediate Response

Prepared to Respond  
Questions  
The Importance of Preparation  
Logs  
Data Collection

[Register Online](#)

### Schedule

Class Length: 5 Days

G2R = "Guaranteed to Run" | OLL = "Online LIVE"  
ILT = "Instructor-Led-Training"

*This course is not currently available on the public schedule. Please contact us using the information in the footer below to inquire about future dates or to schedule a private class.*

## VSC Analysis

What Are "Volume Shadow Copies"?

Registry Keys

Live Systems

Pro Discover

F-Response

Acquired Images

VHD Method

VMware Method

Automating VSC Access

Pro Discover

## File Analysis

MFT

File System Tunneling

Event Logs

Windows Event Log

Recycle Bin

Prefetch Files

Scheduled Tasks

Jump Lists

Hibernation Files

Application Files

Antivirus Logs

Skype

Apple Products

Image Files

## Registry Analysis

Registry Nomenclature

The Registry as a Log File

USB Device Analysis

System Hive

Services

Software Hive

Application Analysis

NetworkLst

NetworkCards

Scheduled Tasks

User Hives

WordWheeQuery

Shell bags

MUICache

UserAssst

Virtual PC

Typed Paths

Additional Sources

RegIdleBackup

Volume Shadow Copies

Virtualization

Memory

Tools

## Malware

- Introduction and Overview
- Malware Characteristics
- Initial Infection Vector
- Propagation Mechanism
- Persistence Mechanism
- Artifacts
- Detecting Malware
- Log Analysis
- Dr Watson Logs
- Antivirus Scans
- AV Write-ups
- Digging Deeper
- Packed Files
- Digital Signatures
- Windows File Protection
- Alternate Data Streams
- PE File Compile Times
- MBR Infectors
- Registry Analysis
- Internet Activity
- Additional Detection
- Seeded Sites
- Summary

## Timeline Analysis

- Timeline Analysis
- Introduction
- Timelines
- Data Sources
- Time Formats
- Concepts
- Benefits
- Format
- Time
- Source
- System
- Benefits
- Format
- Time
- Source
- System
- User
- Description
- TLN Format
- Creating Timelines
- File System Meta data
- Event Logs
- Windows XP
- Windows
- Prefetch Files
- Registry Data
- Additional Sources
- Parsing Events into a Timeline
- Case Study

## Application Analysis

Introduction  
Log Files  
Dynamic Analysis  
Network Captures  
Application Memory Analysis

## Mobile Forensics

Keyboard caches containing usernames, passwords, search terms, and historical fragments of typed communication.  
Screenshots preserved from the last state of an application  
Deleted images from the suspect's photo library, camera roll, and browsing cache.  
Deleted address book entries, contacts, calendar events, and other personal data.  
Exhaustive call history  
Map tile images from the iPhone's Google Maps application,  
Lookups and longitude/latitude coordinates of previous map searches, and coordinates of the last GPS fix.  
Browser cache and deleted browser objects  
Cached and deleted email messages  
SMS messages  
Deleted voicemail recordings  
Pairing records establishing trusted relationships between the device and one or more desktop computers.

## Related Courses, Certifications, Exams

---

- Certified Computer Forensics Examiner
- CCFE