

# Digital Forensics and Computer Examiner Training

This Digital Forensics and Computer Examiner training covers how to collect, preserve, analyze and report digital evidence of network behavior, intrusions and security incidents.

[CBT Nuggets course material](#) →

## WEEK 1

### Digital Forensics Introduction

153 min.

Artifacts	9
Who are we investigating for?	7
What tools do we use?	8
Outside considerations	6
Ethical Considerations	4

### Federal Rules of Evidence

Overview	1
Federal Rules of Evidence	6
Daubert Standard	12
Rule 702	6
Rule 701	5
Rule 901	6
Rule 902	6
Tying it all together	4

### Chain of Custody

Ensuring Chain of Custody	6
Documentation	9
Bag it and tag it	9
But what about digital evidence bags?	5
Secure Storage	8
Challenge	6

### Software Loadout

Identify those software needs	1
Virtualization	14

Investigation Software 14

## WEEK 2

156 min.

Specific Case Software (inside and outside the Operating System) 10

Challenge 7

### Installing and Configuring Kali

What is Kali? 7

Picking our Kali 10

Downloading and installing Kali 23

Live Kali 3

Challenge 6

### Monitoring with Kali

Kali being used for good 16

Monitoring and discovering networks 21

Monitoring for hidden networks 6

Challenge 12

### Metasploit Framework

Overview 1

Metasploit Framework 5

Metasploit on Kali 11

Systems Without Metasploit 11

How to Prep the Target 7

## WEEK 3

155 min.

Other Metasploit Add-Ins 6

Options Outside of Metasploit 5

### Looking at the Files

What's in a name? 18

Metadata 11

Alternate Data Streams 10

Challenge 4

### File Steganography

File Steganography 12

OpenStego 10

What about finding the hidden files? 14

Challenge 6

### Digital Artifacts within Windows

What are Artifacts? 3

Artifacts within the File System 20

Internet Artifacts 9

Network Artifacts 8

Challenge 4

### Unallocated Artifacts within Windows

Unallocated Artifacts within Windows 14

## WEEK 4

152 min.

Methods of examining Unallocated Space 11

Automated Methods 15

But what about virtual machines?	5
Extracting Unallocated Space	8
Challenge	5

### Examining Unallocated Data

Before we begin...	13
Identify Unallocated Space	10
Orphans	8
Recovery from Unallocated Space	8
Challenge	5

### Examining Volatile Memory

Volatile Memory	14
Tools to extract	19
Wait! Memory examination is more than just RAM	12
Challenge	4

### Learning About Our System with Volatility

Retrieving detailed information	15
---------------------------------	----

## WEEK 5

**76 min.**

How did our system connect to the Network?	5
Can we look at the Registry?	9
Are virtual machines any different?	7
Challenge	7

### Analyze RAM while Learning Volatility

Learning Volatility	4
---------------------	---

Prepare to examine	12
Installing Volatility	14
Using Basic Volatility Commands	15
Challenge	3