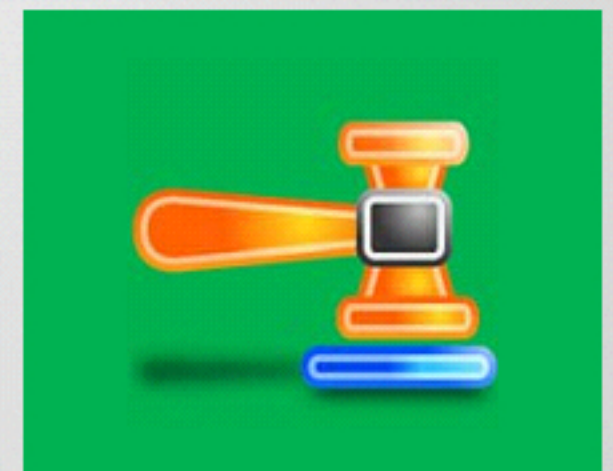


CHFI v9

Instructor Guide

Designed by **Cyber Crime Investigators**. Presented by Professionals.



Welcome to CHFI v9!

What is CHFI?

- Computer Hacking Forensic Investigator (CHFI) course will give participants the necessary skills to perform an effective **digital forensics investigation**
- CHFI presents **a methodological approach** to computer forensics including searching and seizing, chain-of-custody, acquisition, preservation, analysis and reporting of digital evidence
- It is a comprehensive course covering major forensic investigation scenarios that enables students to acquire necessary **hands-on experience** on various forensic investigation techniques and standard forensic tools necessary to successfully carryout a computer forensic investigation leading to prosecution of perpetrators

Course Outline

- | | | | |
|-----------|---|-----------|--|
| 01 | Computer Forensics in Today's World | 08 | Investigating Web Attacks |
| 02 | Computer Forensics Investigation Process | 09 | Database Forensics |
| 03 | Understanding Hard Disks and File Systems | 10 | Cloud Forensics |
| 04 | Data Acquisition and Duplication | 11 | Malware Forensics |
| 05 | Defeating Anti-forensics Techniques | 12 | Investigating Email Crimes |
| 06 | Operating System Forensics | 13 | Mobile Forensics |
| 07 | Network Forensics | 14 | Forensic Report Writing and Presentation |

How CHFI Will Help You – A Checklist for Forensic Investigators



After attending the CHFI training, students will be able to:

- ✓ Perform incident response and forensics
- ✓ Perform electronic evidence collections
- ✓ Perform digital forensic acquisitions
- ✓ Perform Bit stream imaging/acquiring of the digital media seized during the process of investigation
- ✓ Examine and analyze text, graphics, multimedia, and digital images.
- ✓ Conduct thorough examinations of computer hard disk drives and other electronic data storage media
- ✓ Recover information and electronic data from computer hard drives and other data storage devices
- ✓ Follow data and evidence handling procedures
- ✓ Maintain audit trail (i.e. chain of custody) and/or evidence of integrity
- ✓ Work on technical examination, analysis and reporting of computer based evidence
- ✓ Prepare and maintain case files
- ✓ Utilize forensic tools and investigative methods to find electronic data, including Internet use history, word processing documents, images and other files.

How CHFI Will Help You – A Checklist for Forensic Investigators



After attending the CHFI training, students will be able to:

- ✓ Gather volatile and non-volatile information from Windows, MAC and Linux
- ✓ Recover deleted files and partitions in Windows, Mac OS X, and Linux
- ✓ Perform keyword searches including using target words or phrases
- ✓ Investigate events for evidence of insider threats or attacks
- ✓ Support the generation of Incident Reports and other collateral
- ✓ Investigate and analyze all response activities related to cyber incidents
- ✓ Plan, coordinate and direct recovery activities and incident analysis tasks
- ✓ Examine all available information and supporting evidence or artifacts related to an incident or event
- ✓ Collect data using forensic technology methods in accordance with evidence handling procedures, including collection of hard copy and electronic documents
- ✓ Conduct reverse engineering for known and suspected malware files
- ✓ Identify of data, images and/or activity which may be the target of an internal investigation
- ✓ Perform detailed evaluation of the data and any evidence of activity in order to analyze the full circumstances and implications of the event

How CHFI Will Help You – A Checklist for Forensic Investigators



After attending the CHFI training, students will be able to:

- ✓ Establish threat intelligence and key learning points to support pro-active profiling and scenario modeling
- ✓ Search file slack space where PC type technologies are employed
- ✓ File MAC times (Modified, Accessed, and Create dates and times) as evidence of access and event sequences
- ✓ Examine file type and file header information
- ✓ Review e-mail communications; including web mail and Internet Instant Messaging programs.
- ✓ Examine the internet browsing history
- ✓ Generate reports which detail the approach and an audit trail which documents actions taken in order to support the integrity of the internal investigation process
- ✓ Recover active, system and hidden filenames with date/time stamp information.
- ✓ Crack (or attempt to crack) password protected files
- ✓ Perform anti-forensic methods detection
- ✓ Execute a file and view the data contents
- ✓ Maintain awareness and follow laboratory evidence handling, evidence examination, laboratory safety, and laboratory security policy and procedures

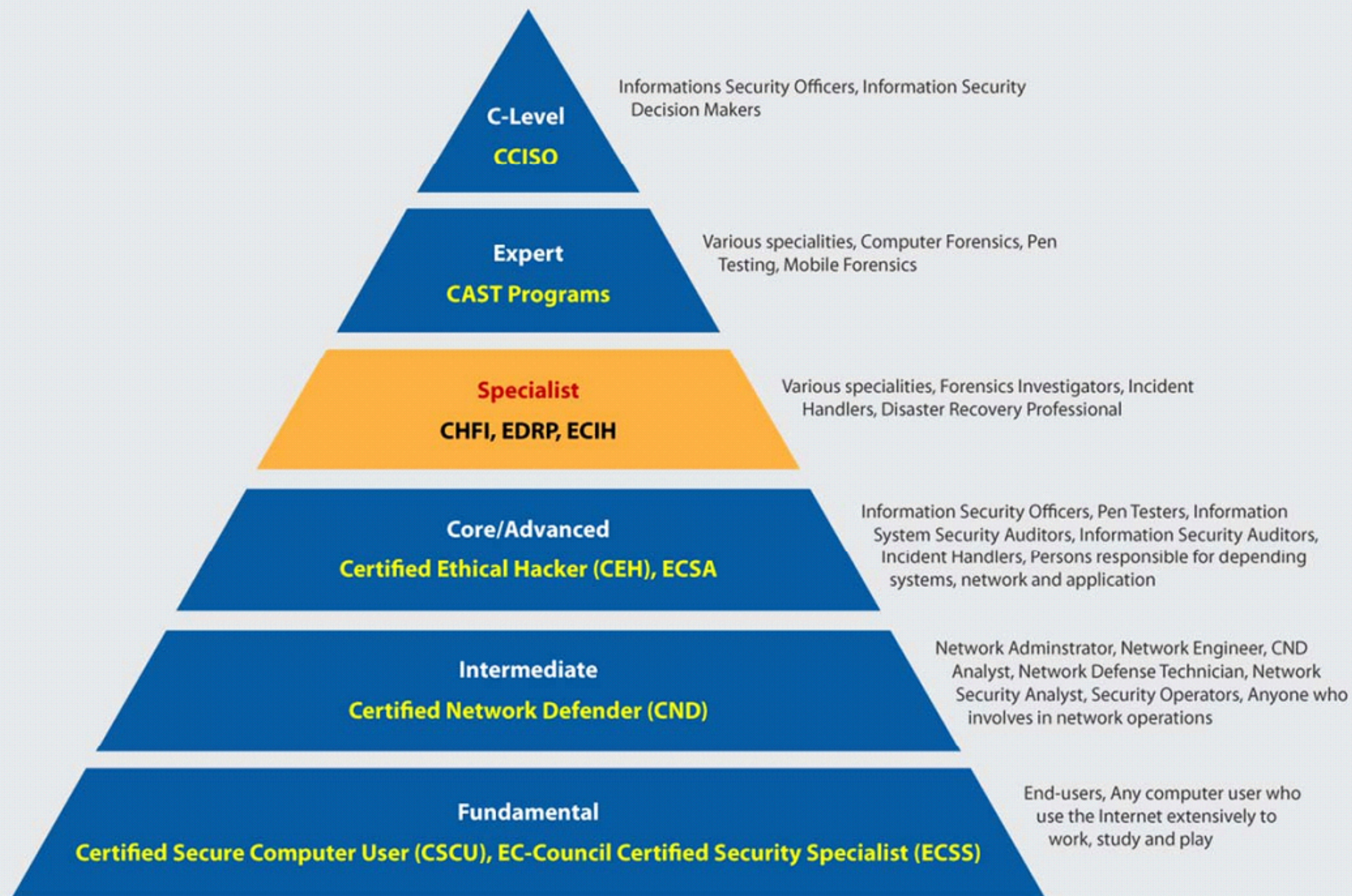
How CHFI Will Help You – A Checklist for Forensic Investigators



After attending the CHFI training, students will be able to:

- ✓ Play a role of first responder by securing and evaluating cyber crime scene, conducting preliminary interviews, documenting crime scene, collecting and preserving electronic evidence, packaging and transporting electronic evidence, reporting of the crime scene
- ✓ Perform post-intrusion analysis of electronic and digital media to determine the who, where, what, when, and how the intrusion occurred
- ✓ Apply advanced forensic tools and techniques for attack reconstruction
- ✓ Perform fundamental forensic activities and form a base for advanced forensics
- ✓ Identify & check the possible source/incident origin
- ✓ Perform event co-relation
- ✓ Extract and analyze of logs from various devices like proxy, firewall, IPS, IDS, Desktop, laptop, servers, SIM tool, router, firewall, switches AD server, DHCP logs, Access Control Logs & conclude as part of investigation process.
- ✓ Ensure reported incident or suspected weaknesses, malfunctions and deviations are handled with confidentiality
- ✓ Verify the correctness of the computer's internal clock
- ✓ Assist in the preparation of search and seizure warrants, court orders, and subpoenas
- ✓ Provide expert witness testimony in support of forensic examinations conducted by the examiner

Where Does **CHFI** Fits in EC-Council Career Path?



Why CHFI?



- The program is developed after a thorough job tasks analysis and market research
- It is designed and developed by experienced SMEs and digital forensics practitioners
- A vendor neutral course covering all major forensics investigations technologies and solutions
- Detailed labs for hands-on learning experience; approximately 40% of training time is dedicated to labs

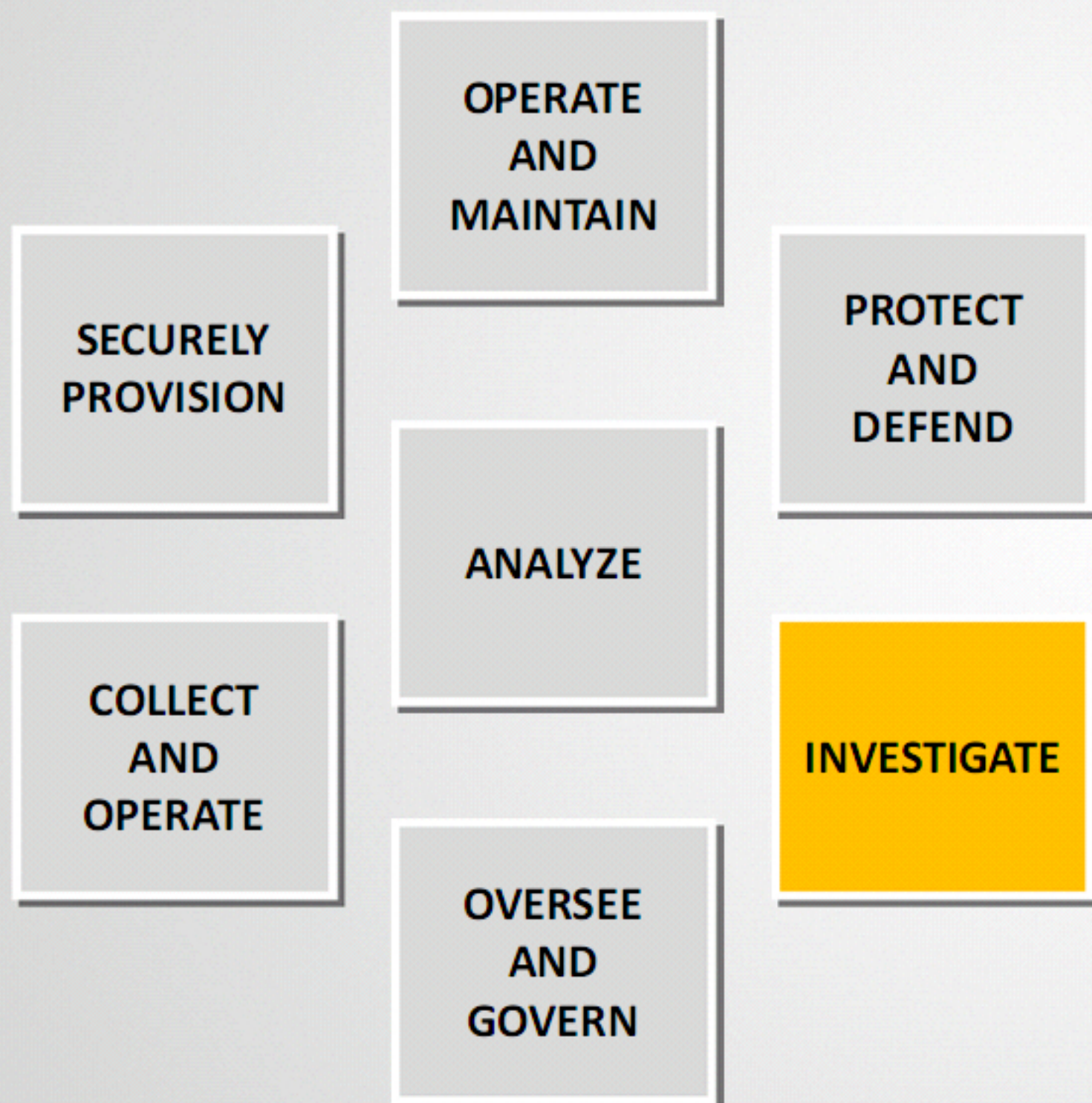
Why CHFI?



- It covers all the relevant knowledge-bases and skills to meets with regulatory compliance standards such as ISO 27001, PCI DSS, SOX, HIPPA, etc.
- More than 40 GB of digital forensics and evidence analysis tools
- The student kit contains large number of white papers for additional reading

- The program presents a repeatable forensics investigation methodology required from a versatile digital forensic professional which increases your employability
- The student kit contains a large number of forensics investigation templates for evidence collection, chain-of-custody, final investigation reports, etc.
- The program comes with cloud-based virtual labs enabling students to practice various investigation techniques in a real time and simulated environment

CHFI Maps to NICE Framework



Compliance with National Initiative for Cybersecurity Education (NICE)
“Investigate” specialty area

Individuals with this specialty hold following job titles:

- Computer Forensic Analyst
- Computer Network Defense (CND) Forensic Analyst
- Digital Forensic Examiner
- Digital Media Collector
- Forensic Analyst
- Forensic Analyst (Cryptologic)
- Forensic Technician
- Network Forensic Examiner
- Computer Crime Investigator
- Special Agent

EC-Council's **Strengths** in This Domain



- EC-Council is one of the largest information security training provider
- EC-Council's courses are **delivered with a strong emphasis of hands on techniques** that will enable you to apply what you have learnt as soon as you complete your class
- CHFIv9 is a **comprehensive course** covering all possible forensic investigation scenarios that enables students to acquire necessary hands-on experience on various forensic investigation techniques and standard **forensic tools necessary to successfully carryout a computer forensic investigation** leading to prosecution of perpetrators
- EC-Council's coursewares are **developed by subject matter experts** from all over the world and are constantly updated to ensure that you are exposed to the latest advances in the space
- EC-Council's courses feature some of the best names in the **InfoSec world**. EC-Council Master trainers are practitioners and experts in their respective fields
- EC-Council's courses are extremely advanced and can be **delivered in a number of formats** including, **Live, Online, Instructor Led, Custom Classes, Blended Learning** and much more
- EC-Council's courses are **CNSS 4011 – 4016 Certified** from the US National Security Council

What's New in CHFI v9?



Updated information as per the latest developments with a proper flow



New investigation techniques and updated **forensic investigation tools**



Classroom friendly with **graphical** representation of concepts and attacks



Exclusive section for **best practices** to follow during forensic investigation



Exclusive section for disk acquisition **tools requirements** to carryout successful investigation



New and rich presentation style with **engaging graphics**



What's New in CHFI v9?



Latest OS covered and a patched testing environment



Well tested, result oriented, descriptive and **analytical lab manual** to evaluate the presented concepts



Sample evidence files (~ 6GB) are provided that assist students to carryout analysis



CHFIv9 is accompanied with **ilabs**



Forensic challenges based **real time scenarios** are provided in Lab manual to practice



CHFIv9 Version Change Summary



CHFIv9	CHFIv8
Module 01: Computer Forensics in Today's World	Module 01: Computer Forensics in Today's World
Module 02: Computer Forensics Investigation Process	Module 02: Computer Forensics Investigation Process
	Module 03: Searching and Seizing Computers
	Module 04: Digital Evidence
	Module 05: First Responder Procedures
	Module 06: Computer Forensics Lab
Module 03: Understanding Hard Disks and File Systems	Module 07: Understanding Hard Disks and File Systems
Module 04: Data Acquisition and Duplication	Module 09: Data Acquisition and Duplication
Module 05: Defeating Anti-forensics Techniques	Module 10: Recovering Deleted Files and Deleted Partitions
	Module 13: Steganography and Image File Forensics
	Module 14: Application Password Crackers
Module 06: Operating System Forensics (Added Linux and MAC Forensics in CHFI version 9)	Module 08: Windows Forensics
Removed this module	Module 11: Forensics Investigation using AccessData FTK

CHFIv9 Version Change Summary

CHFIv9	CHFIv8
Removed this module	Module 12: Forensics Investigation Using EnCase
Module 07 Network Forensics	Module 15: Log Capturing and Event Correlation
	Module 16: Network Forensics, Investigating Logs and Investigating Network Traffic
	Module 17: Investigating Wireless Attacks
Module 08: Investigating Web Attacks.	Module 18: Investigating Web Attacks
Module 09: Database Forensics (New Module)	
Module 10: Cloud Forensics (New Module)	
Module 11: Malware Forensics (New Module)	
Module 12: Investigating Email Crimes	Module 19: Tracking Emails and Investigating Email Crimes
Module 13: Mobile Forensics	Module 20: Mobile Forensics
Module 14: Forensics Report Writing and Presentation	Module 21: Investigative Reports
	Module 22: Becoming an Expert Witness

CHFIv9 Version Change Summary

CHFIv8	CHFIv9
	Updated information as per the latest developments with a proper flow
	Classroom friendly with diagrammatic representation of concepts and attacks
	New and rich presentation style with eye catching graphics
	Latest OS covered and a patched testing environment
	Well tested, result oriented, descriptive and analytical lab manual to evaluate the presented concepts
22 Modules	14 Modules
42 Labs	39 Labs
2400 Slides	1222 Slides (concise, yet more information has been covered)

Content Flow

How to
Access CEI
Material



Training
Schedule



Lab Setup
Requirement



How to
Teach
CHFIv9




iLabs



Sample
Evidence
Files

Accessing CHFI Courseware

- Aspen is a **one-step gateway to multiple portals, products, and services** provided by EC-Council for its registered members
- You can download instructor slides, lab setup guide, e-courseware, lab manuals, and tools at <https://aspen.eccouncil.org>



The screenshot shows the ASPEN login interface. At the top left is the ASPEN logo (a blue triangle) and the text "ASPEN". To its right are two buttons: "My Account" and "Contact Us". Below the logo is a "Home" button and a "Login" button. In the top right corner, there are links for "Register" and "Login". The main content area is divided into two columns. The left column is titled "Please Login" and contains a "Username" field, a "Password" field, a "Login" button with a lock icon, and two buttons at the bottom: "Register" and "Forgot Password". The right column is titled "What is ASPEN?" and contains the ASPEN logo and a paragraph of text explaining the platform.

ASPEN

My Account Contact Us

Home Login

Register Login

Please Login

Username

Password


Login

Register Forgot Password

What is ASPEN?

Aspen is a one-step gateway to multiple portals, products and services provided by EC-Council for its registered members. It is an integrated environment and a user friendly portal, where a user can navigate to various web pages through a single login. Aspen registered users can place orders for various products and courseware at their convenience with just a few mouse clicks. Aspen not only acts as a transit to EC-Council's services, but also as a social communication medium between its users. Aspen is an innovative concept that offers an easy access to a wide variety of EC-Council's contributions to the Computer security arena under one platform.


Accessing CHFI Courseware




HomeMy AccountContact Us

HomeHome


Student Services




Class Eval




EC-Council Exam Center




Certificate




Ticketing




Contact Us




Settings



Applications




My Contributions




Announcements

Learning Resources



Academia



eBooks

Download PDF Courseware

You will need Adobe Acrobat 10.x or later versions to view the DRM documents. These documents are not viewable on non-acrobat products such as Preview, Nero Viewer, etc. [Click here to download the latest version of Acrobat Reader](#) (You may require your System Administrator to open port 8443. Ensure that the SSL and/or https access are open to the system IP in order for you to access the secure PDF file.)

If you have trouble viewing this document, please contact academia@eccouncil.org

CHFIv9 Courseware

	File Name	File Size
<input type="checkbox"/>	CHFIv9 Lab Manuals.zip	56.225 MB
<input type="checkbox"/>	CHFIv9 Module 00.pdf	2.998 MB
<input type="checkbox"/>	CHFIv9 Module 01 Computer Forensics in Today's World .pdf	8.930 MB
<input type="checkbox"/>	CHFIv9 Module 02 Computer Forensics Investigation Process .pdf	16.763 MB
<input type="checkbox"/>	CHFIv9 Module 03 Understanding Hard Disks and File Systems.pdf	20.658 MB
<input type="checkbox"/>	CHFIv9 Module 04 Data Acquisition and Duplication.pdf	10.933 MB
<input type="checkbox"/>	CHFIv9 Module 05 Defeating Anti-forensics Techniques.pdf	15.425 MB
<input type="checkbox"/>	CHFIv9 Module 06 Operating System Forensics.pdf	14.219 MB
<input type="checkbox"/>	CHFIv9 Module 07 Network Forensics.pdf	10.505 MB
<input type="checkbox"/>	CHFIv9 Module 08 Investigating Web Attacks.pdf	9.954 MB
<input type="checkbox"/>	CHFIv9 Module 09 Database Forensics.pdf	14.116 MB
<input type="checkbox"/>	CHFIv9 Module 10 Cloud Forensics.pdf	7.462 MB
<input type="checkbox"/>	CHFIv9 Module 11 Malware Forensics .pdf	7.069 MB
<input type="checkbox"/>	CHFIv9 Module 12 Investigating Email Crimes.pdf	6.825 MB
<input type="checkbox"/>	CHFIv9 Module 13 Mobile Forensics.pdf	8.943 MB
<input type="checkbox"/>	CHFIv9 Module 14 Forensics Report Writing and Presentation.pdf	4.700 MB
<input type="checkbox"/>	CHFIv9 References.pdf	2.247 MB

Download Selected Files

Download your **e-courseware**, **Lab Manuals**, and **Tools** from **Academia** section

Accessing CEI Material

Learning Resources



Academia



eBooks

Partner Services



Accredited
Training Center



Certified EC-Council
Instructor



Certified iBusin
Instructor

Certified EC-Council Instructor

Certified EC-Council Instructor

Announcement

CEI Agreement

Instructor Material

CND Material

Download Courseware

Teaching Resources

Download Tools

Download Certificate

Download Logos

Submit Feedback

You will need Adobe Acrobat 10.x or later versions to view the DRM documents. These documents are not viewable on non-acrobat products such as Preview, Nero Viewer, etc. [Click here to download the latest version of Acrobat Reader](#) (You may require your System Administrator to open port 8443. Ensure that the SSL and/or https access are open to the system IP in order for you to access the secure PDF file.)

If you have trouble viewing this document, please contact academia@eccouncil.org

CHFiv9 Instructor Slides

CHFiv9 Instructor Slides.zip

CHFiv9 Lab Setup Manual.zip

- Download your **Instructor Slides** and **Lab Setup Guide** from **Certified EC-Council Instructor** section

Content Flow

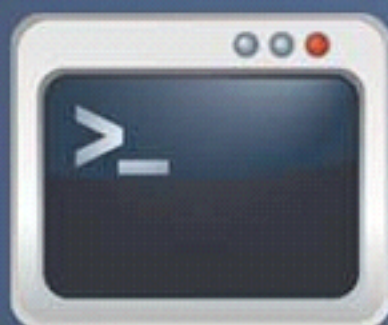
How to
Access CEI
Material



Training
Schedule



Lab Setup
Requirement



How to
Teach
CHFIv9



iLabs



Sample
Evidence
Files

Training Information



Title of the Course: **Computer Hacking Forensic Investigator**



Version: **9**



Training Duration: **5 Days**



Training Timing: **9.00 AM to 6.30 PM**

Note: The CHFI v9 is an advanced forensics investigation training program. Proper preparation is required before conducting the CHFI class.

Training Session: Day 1

Start	End	Module
9:00	9:15	Module 00: Student Introduction
9:15	10:30	Module 01: Computer Forensics in Today's World Module 02: Computer Forensics Investigation Process
10:30	10:40	Break
10:40	12:30	Module 02: Computer Forensics Investigation Process
12:30	1:30	Lunch Break
1:30	3:00	Module 02: Computer Forensics Investigation Process
3:00	3:10	Break
3:10	4:50	Module 02: Computer Forensics Investigation Process Module 03: Understanding Hard Disks and File Systems
4:50	5:00	Break
5:00	6:30	Module 03: Understanding Hard Disks and File Systems

Training Session: Day 2

Start	End	Module
9:00	10:30	Module 03: Understanding Hard Disks and File Systems Module 04: Data Acquisition and Duplication
10:30	10:40	Break
10:40	12:30	Module 04: Data Acquisition and Duplication
12:30	1:30	Lunch Break
1:30	3:00	Module 05: Defeating Anti-forensics Techniques
3:00	3:00	Break
3:10	4:50	Module 05: Defeating Anti-forensics Techniques
4:50	5:00	Break
5:00	6:30	Module 06: Operating System Forensics

Training Session: Day 3

Start	End	Module
9:00	10:30	Module 06: Operating System Forensics
10:30	10:40	Break
10:40	12:30	Module 06: Operating System Forensics
12:30	1:30	Lunch Break
1:30	3:00	Module 06: Operating System Forensics Module 07: Network Forensics
3:00	3:00	Break
3:10	4:50	Module 07: Network Forensics
4:50	5:00	Break
5:00	6:30	Module 07: Network Forensics

Training Session: Day 4

Start	End	Module
9:00	10:30	Module 08: Investigating Web Attacks Module 09: Database Forensics
10:30	10:40	Break
10:40	12:30	Module 09: Database Forensics
12:30	1:30	Lunch Break
1:30	3:00	Module 09: Database Forensics Module 10: Cloud Forensics
3:00	3:00	Break
3:10	4:50	Module 10: Cloud Forensics
4:50	5:00	Break
5:00	6:30	Module 11: Malware Forensics

Training Session: Day 5

Start	End	Module
9:00	10:30	Module 11: Malware Forensics
10:30	10:40	Break
10:40	12:30	Module 11: Malware Forensics Module 12: Investigating Email Crimes
12:30	1:30	Lunch Break
1:30	3:00	Module 12: Investigating Email Crimes Module 13: Mobile Forensics
3:00	3:00	Break
3:10	4:50	Module 13: Mobile Forensics
4:50	5:00	Break
5:00	6:30	Module 13: Mobile Forensics Module 14: Forensics Report Writing and Presentation

**Instructors may Adjust Class
Timings as per Requirement**

Content Flow

How to
Access CEI
Material



Training
Schedule



Lab Setup
Requirement



How to
Teach
CHFIv9



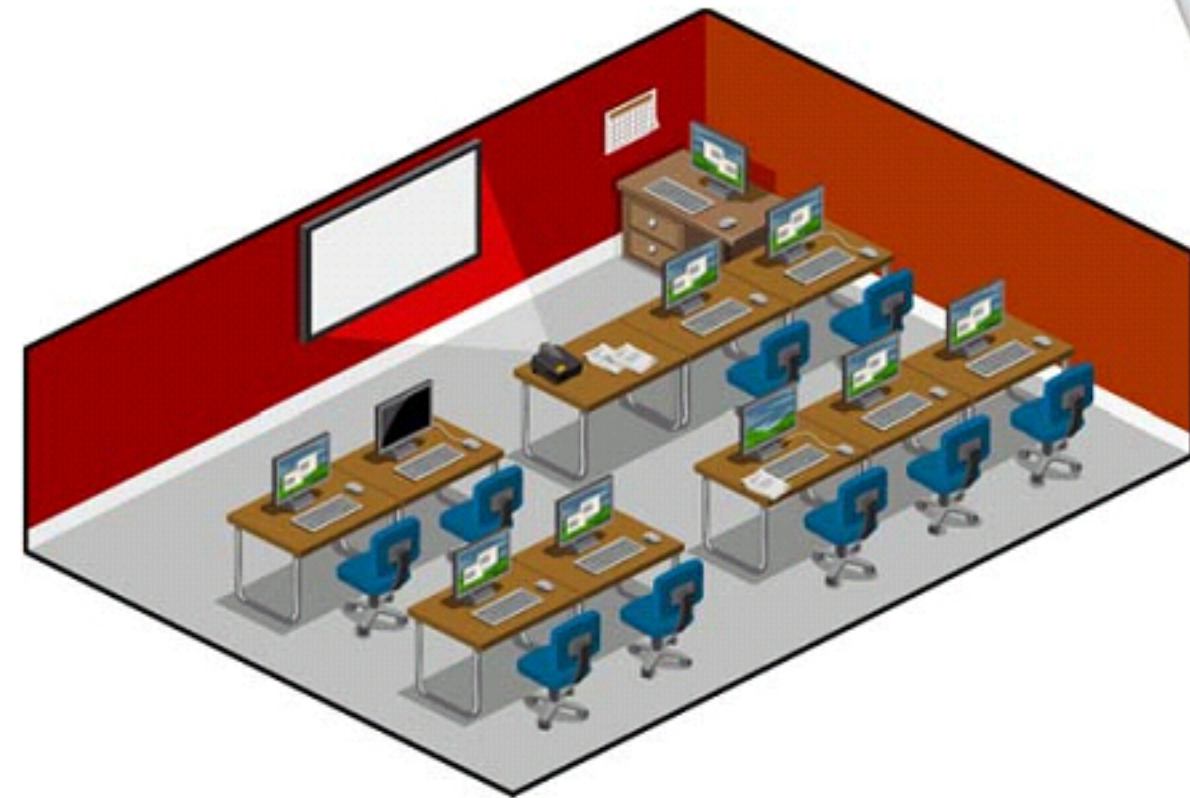
iLabs



Sample
Evidence
Files

Minimum System Requirements

- **Intel® Core™ i5** with 300 GB disk space
- **16 GB** or more **RAM**
- **2 NIC** (disable or unplug extras)
- **18.5-inch monitor** and VGA cards to drive at 1366 x 768 (or at monitor's native resolution) and configured at 16 million colors
- Compatible **keyboard** and **mouse**
- **Wireless Card** for Wi-Fi access



Basic Lab Setup Requirements

Windows Server 2012 R2 or later* (Standard Edition) with full patches applied

Microsoft Windows 10 with full patches applied

MS Internet Information Server 8 (IIS 8)

Microsoft .NET Framework 4.5 or higher version

Adobe Reader 11.0.10 or later version

winrar-x64-54b1 or later version

Kali Linux 2016 Rolling Release (x64)

Ubuntu Linux 16.04 LTS (x64)

Basic Lab Setup Requirements

Web Browsers: Internet Explorer, Firefox, and Chrome

Android Software Development Toolkit

WinPcap driver

Notepad++

Java SE Development Toolkit

Java SE Run Time Environment

Word, Excel, and PowerPoint Viewers or Microsoft Office 2016

Hyper-V (Built-in role in Windows Server 2008)

Content Flow

How to
Access CEI
Material



Training
Schedule



Lab Setup
Requirement



How to
Teach
CHFIv9



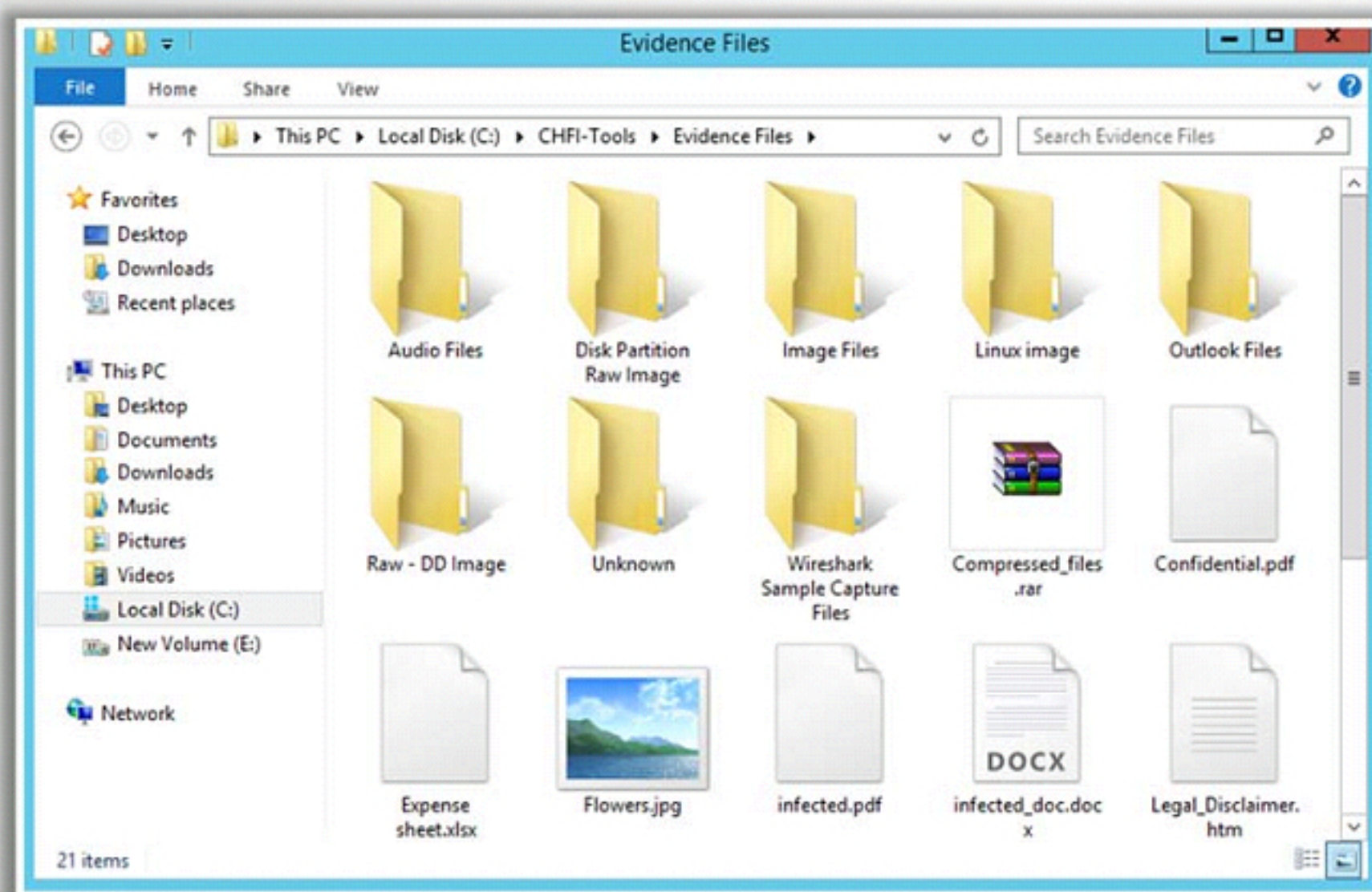
iLabs



Sample
Evidence
Files

Sample Evidence Files

- This course gives you a **hands-on** experience with sample evidence files for practicing the skills acquired in the class
- Evidence files are available in the at <https://aspen.eccouncil.org>
- Download the evidence files to **Evidence Files** folder in **C:** drive of Windows Server 2012 VM for easy access



Note: Lab Manual refers to the **C:\CHFI-Tools\Evidence Files** folder for sample evidence files

Content Flow

How to
Access CEI
Material



Training
Schedule



Lab Setup
Requirement



How to
Teach
CHFIv9

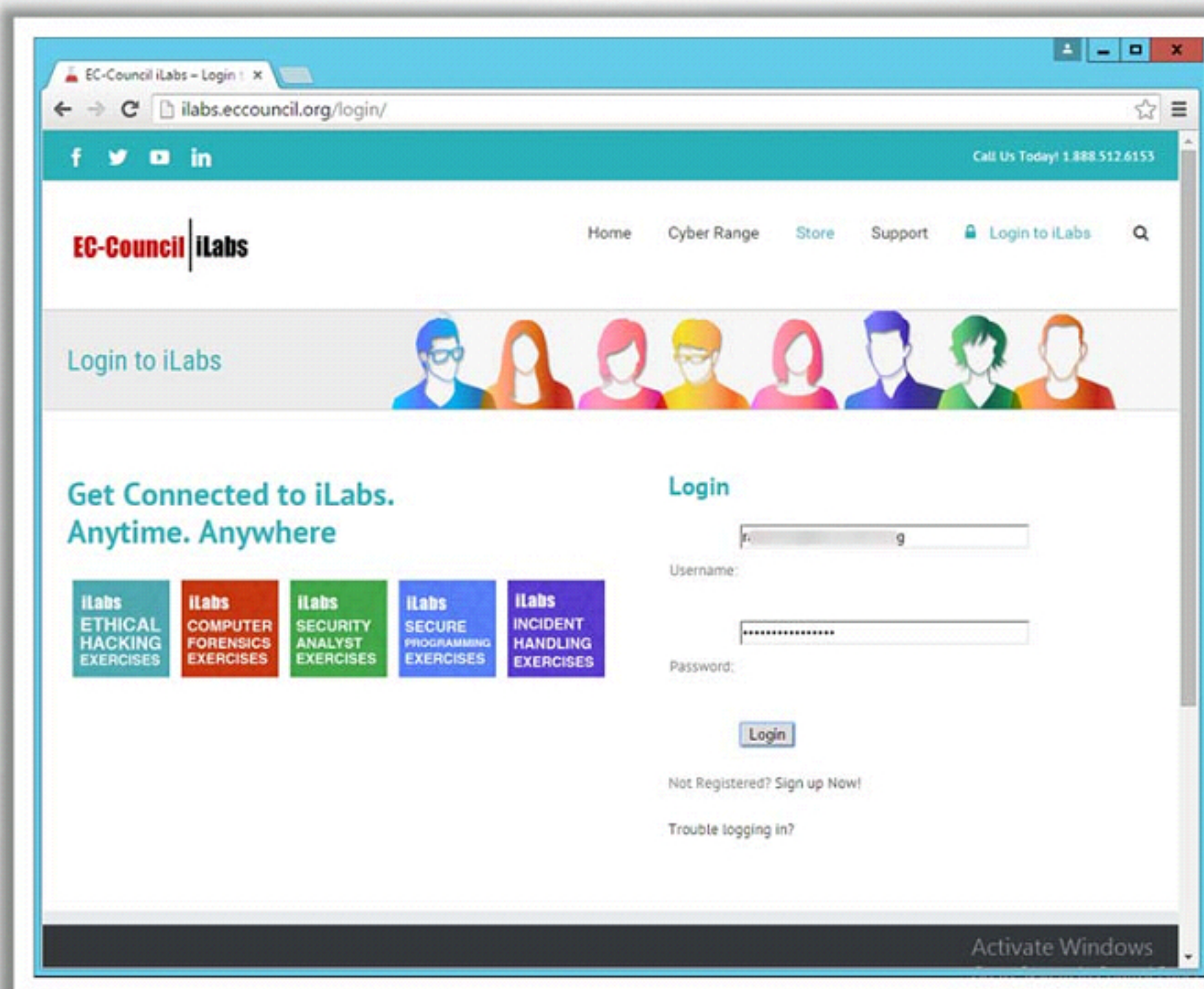


iLabs



Sample
Evidence
Files

iLabs is a subscription-based service that allows students to log on to preconfigured **Virtual Machines** and perform various exercises featured in the CHFI Lab Guide



Module 02: Computer Forensics Investigation Process

Windows Server 2012

Developer

Display

Commands

16 Hr 34 Min Remaining

Exit

Content

Machines

Support

5:27

Press Ctrl+Alt+Delete to sign in.

5:27

Friday, December 16

Logon to Windows 10

Click Windows 10 machine from Machines pane. Click Ctrl+Alt+Delete button under the machine to login.

Done

Task 1 of 101

Exercise 1, Task 1 of 15

Username Administrator

Password Pa\$\$w0rd

Load Files

Ctrl+Alt+Delete

Windows Server 2012

Windows 10

Ubuntu

Kali Linux

Student Benefits

- Fully Automated Lab Environment
- Unlimited Access over Subscription Term
- Simple clientless connection through web browser
- Fully loaded with Windows Server 2012 64-bit, Windows 10 64-bit, Ubuntu, and Kali Linux
- Save-State Technology enabled
- **Labs can be performed from HOME!**



Instructor/ATC Benefits

- No more difficult Lab Setup
- No Software licensing Fees
- No Hardware to maintain
- Full Controls to reset or re-spin systems live
- Instant recovery



Content Flow

How to
Access CEI
Material



Training
Schedule



Lab Setup
Requirement



How to
Teach
CHFIv9



iLabs



Sample
Evidence
Files

Module 00: Student Introduction

Student Introduction

- Welcome the students to the course and introduce yourself
- Provide a **brief overview** of your background to establish credibility
- **Ask students to introduce themselves** and provide their background, security related experience, and expectations from the course
- **Write your name on the whiteboard corner** and do not erase this for the duration of the class so that the students will know your name
- Inform the students in your class **what is required for the CHFI course**. Describe the contents of the course materials and explain how the tools are used.

Student Introduction



- Tell students about the **modules that will be covered in the class**



- Explain the **CHFIv9 exam process**. Provide information on when the exam will be conducted, the cost of the exam, the total number of questions, the passing score, etc. (consult with the training center regarding the exam delivery, they might have prepaid exam vouchers)



- Ask the students to **sign the CHFI NDA document**. Submit the signed documents to the training center operations manager or the person in charge of the training

Module 01: Computer Forensics in Today's World

What is Covered in **Module 01**?

- Understanding Computer Forensics
- Why and When Do You Use Computer Forensics?
- Cyber Crime (Types of Computer Crimes)
- Case Study
- Challenges Cyber Crimes Present For Investigators
- Cyber Crime Investigation
- Rules of Forensics Investigation
- Understanding Digital Evidence
- Types of Digital Evidence
- Characteristics of Digital Evidence
- Role of Digital Evidence
- Sources of Potential Evidence
- Rules of Evidence
- Forensics Readiness
- Computer Forensics as part of an Incident Response Plan
- Need for Forensic Investigator
- Roles and Responsibilities of Forensics Investigator
- What makes a Good Computer Forensics Investigator?
- Investigative Challenges
- Legal and Privacy Issues
- Code of Ethics
- Accessing Computer Forensics Resources

How to **Teach** this Module?

- Start the module with a discussion on some **real time cyber forensics case studies** and news
- Explain **Computer forensics** and its objectives
- Explain the **importance of computer forensics** with respect to different cybercrimes
- Help students understand how **computer forensics** could have **helped organizations** (that were a victim of cyber attacks) in better handling of the cyber attacks
- Discuss the various **challenges** cybercrimes present to investigators

How to **Teach** this Module?

- Explain the **different types of cybercrime investigations** and general rules of forensics
- Help students understand the **rules of evidence** and explain the different types of digital evidence
- Talk about the **role of computer forensics** and forensics readiness in incident response plans
- Explain the **need for forensic investigators** and their roles and responsibilities
- Talk about the legal, privacy and **code of ethics** issues in computer forensics

Module 02: Computer Forensics Investigation Process

What is Covered in **Module 02**?

- Importance of Computer Forensics Process
- Phases Involved in the Computer Forensics Investigation Process
- Pre-investigation Phase
 - Setting Up a Computer Forensics Lab
 - Build the Investigation Team
 - Review Policies and Laws
 - Establish Quality Assurance Processes
 - Data Destruction Industry Standards
 - Risk Assessment
- Investigation Phase
 - Investigation Process
 - Computer Forensics Investigation Methodology: First Response

- Computer Forensics Investigation Methodology: Search and Seizure
- Computer Forensics Investigation Methodology: Collect the Evidence
- Computer Forensics Investigation Methodology: Secure the Evidence
- Computer Forensics Investigation Methodology: Data Acquisition
- Computer Forensics Investigation Methodology: Data Analysis
- Post-investigation Phase
 - Computer Forensics Investigation Methodology: Evidence Assessment
 - Computer Forensics Investigation Methodology: Documentation and Reporting
 - Computer Forensics Investigation Methodology: Testify as an Expert Witness

How to **Teach** this Module?

- Explain the importance of **computer forensics process**
- Demonstrate the various **phases of the computer forensics investigation** process
- Discuss about the **requirements for building a computer forensics lab** and an investigation team
- Explain the **roles of a first responder**, and talk about chain of custody and its importance
- Talk about **search and seizure**, evidence collection, management and preservation
- Explain **chain of custody** and its importance
- Discuss about **data duplication**, deleted data recovery and evidence examination
- Talk about **investigative reports** and how to testify in a court room

Exercise

1



Recovering Data Using the EaseUS Data Recovery Wizard

2



Performing Hash, Checksum, or HMAC Calculations Using the HashCalc Tool

3



Generating MD5 Hashes Using MD5 Calculator

4



Viewing Files of Various Formats Using the File Viewer Tool

5



Handling Evidence Data Using the P2 Commander Tool

6



Creating a Disk Image File of a Hard Disk Partition Using the R-Drive Image Tool

Module 03: Understanding Hard Disks and File Systems

What is Covered in **Module 03**?

● Hard Disk Drive Overview

- Types of Disk Drives: HDD and SSD
- Physical and Logical Structures of a Hard Disk
- Types of Hard Disk Interfaces
- Tracks, Sector, Cluster and Bad Sectors
- Hard Disk Data Addressing
- Hard Disk Data Densities and Disk Capacity Calculation
- Measuring the Performance of the Hard Disk

● Disk Partitions and Boot Process

- Windows Boot Process
- Macintosh Boot Process
- Linux Boot Process

● Understanding File Systems

- Windows File Systems
- Linux File Systems
- Mac OS X File Systems
- Oracle Solaris 11 File System: ZFS
- CD-ROM / DVD File System
- Compact Disc File System (CDFS)
- Virtual File System (VFS) and Universal Disk Format File System (UDF)

● RAID Storage System

- Levels of RAID Storage System
- Host Protected Areas (HPA) and Device Configuration Overlays (DCO)

● File System Analysis

How to **Teach** this Module?

- Explain the different **types of disk drives** and their characteristics
- Demonstrate **physical and logical structure** of a hard disk
- Talk about the **types of hard disk interfaces** and discuss the various hard disk components
- Explain the **hard disk partitions**
- Demonstrate the Windows, Mac, and Linux **boot Processes**
- Explain the various Windows, Linux and Mac OS X **file systems**
- Discuss about the various **RAID storage systems**
- Explain **file system analysis**

Exercise

01

Recovering Deleted Files from Hard Disks Using WinHex

02

Analyzing File System Types Using The Sleuth Kit (TSK)

03

Analyzing Raw image using Autopsy

Module 04: Data Acquisition and Duplication

What is Covered in **Module 04**?

● Data Acquisition and Duplication Concepts

- Live Data Acquisition
- Volatile Data Collection Methodology

● Static Acquisition

- Rules of Thumb
- Why to Create a Duplicate Image?
- Bit Stream Image Vs. Backups
- Issues with Data Duplication
- Data Acquisition and Duplication Steps
- Prepare a Chain of Custody Document
- Enable Write Protection on the Evidence Media
- Sanitize the Target Media: NIST SP 800-88 Guidelines
- Data Acquisition Methods

- Determine the Best Acquisition Method
- Select the Data Acquisition Tool
- Acquiring Data on Linux: dd Command
- Acquiring Data on Linux: dcfldd Command
- Acquiring Data on Windows: AccessData FTK Imager
- Acquiring RAID Disks
- Remote Data Acquisition
- Data Acquisition Mistakes
- Plan for Contingency

● Validate Data Acquisitions

- Linux Validation Methods
- Windows Validation Methods

● Acquisition Best Practices

How to **Teach** this Module?

- Discuss about **data acquisition** and its importance
- Explain **live data acquisition**
- Explain **static data acquisition**
- Talk about data **acquisition** and **duplication steps**
- Discuss the **steps** required to **keep a device unaltered**
- Talk about the **best acquisition method** and select appropriate data acquisition tool
- Demonstrate data acquisition on **Windows** and **Linux** Machines
- Discuss the data acquisition **best practices**

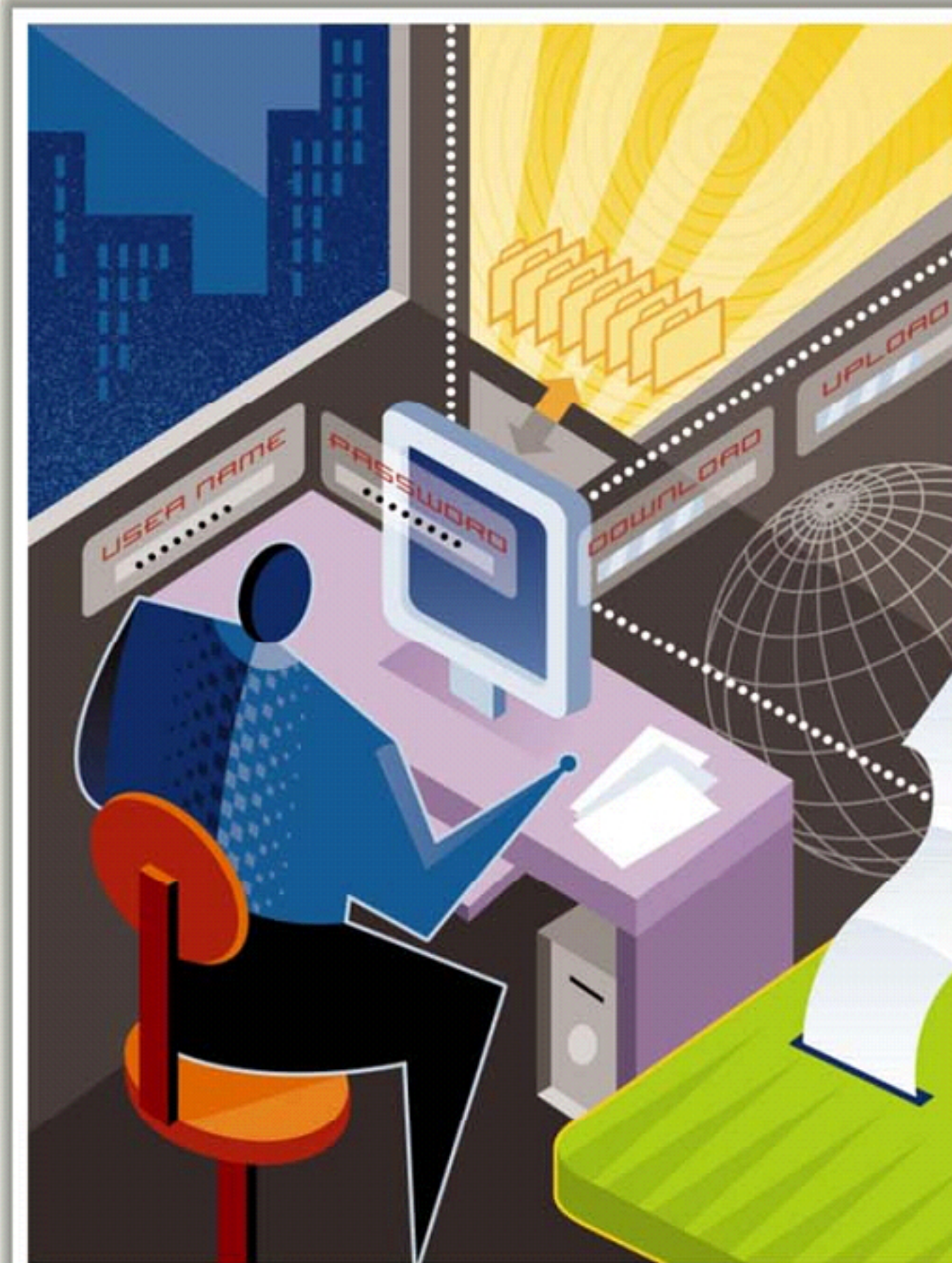
Exercise

Investigating NTFS Drive
Using DiskExplorer for NTFS

1

Viewing Content of Forensic
Image Using AccessData FTK
Imager Tool

2



Module 05: Defeating Anti-forensics Techniques

What is Covered in **Module 05**?

- What is Anti-Forensics?
 - Goals of Anti-Forensics
- Anti-Forensics techniques
 - Data/File Deletion
 - Password Protection
 - Steganography
 - Data Hiding in File System Structures
 - Trail Obfuscation
 - Artifact Wiping
 - Overwriting Data/Metadata
- Encryption
- Encrypted Network Protocols
- Program Packers
- Rootkits
- Minimize Footprint
- Exploiting Forensic Tools Bugs
- Detecting Forensic Tool Activities
- Anti-Forensics Countermeasures
- Anti-Forensics Challenges
- Anti-forensics Tools

How to **Teach** this Module?

- About **anti-forensics** and the goals of anti-forensics
- Discuss the **anti-forensics techniques**
- Help students understand **how to extract evidence** from deleted files/partitions, password protected files, and stego material
- Explain about trial **obfuscation identification**, artifact wiping, data/metadata overwriting, and encryption
- Talk about encrypted **network protocols identification**, program packers, rootkits and detection methods
- Examine different **techniques** attackers use to **avoid detection** during investigation
- Talk about anti-forensics **countermeasures**
- Discuss about the **challenges** faced by Investigators to defeat anti-forensics

Exercise

Cracking Application
Password

Detecting Steganography



Module 06: Operating System Forensics

What is Covered in **Module 06**?

Windows Forensics

- Collecting Volatile Information
- Collecting Non-Volatile Information
- Analyze the Windows thumb caches
- Windows Memory Analysis
- Windows Registry Analysis
- Cache, Cookie, and History Analysis
- Windows File Analysis
- Metadata Investigation
- Text Based Logs
- Other Audit Events
- Forensic Analysis of Event Logs
- Windows Forensics Tools

Linux Forensics

- Shell Commands
- Linux Log files
- Collecting Volatile Data
- Collecting Non-Volatile Data

MAC Forensics

- Introduction to MAC Forensics
- MAC Forensics Data
- MAC Log Files
- MAC Directories
- MAC Forensics Tools

How to **Teach** this Module?

- Help students understand how to **collect and examine volatile and non-volatile data** in Windows machines
- Explain windows **memory** and **registry analysis**
- Help students understand how to **examine the cache**, cookie, and history recorded in web browsers
- Discuss about Windows **files** and **metadata examination**
- Demonstrate text based logs and Windows event **logs Analysis**
- Discuss the various **Linux based shell commands** and log files
- Help students understand how to collect and examine volatile and non-volatile information in **Linux machines**
- Talk about the need for **Mac forensics** and examine Mac forensics data and log files

Exercise

01

Discovering and Extracting
Hidden Forensic Material on
Computers Using OSForensics

02

Extracting Information
about Loaded Processes
Using Process Explorer

03

Viewing, Monitoring, and
Analyzing Events Using the
Event Log Explorer Tool

04

Performing a Computer
Forensic Investigation
Using the Helix Tool

05

Analyzing Volatile Data in Linux
System

06

Analyzing Non-volatile
Data in Linux System

Module 07: Network Forensics

What is Covered in **Module 07**?

- Introduction to Network Forensics
 - Postmortem and Real-Time Analysis
 - Where to Look for Evidence
- Fundamental Logging Concepts
 - Log Files as Evidence
 - Laws and Regulations
 - Records of Regularly Conducted Activity as Evidence
- Event Correlation Concepts
 - Types of Event Correlation
 - Event Correlation Approaches
- Network Forensic Readiness
 - Ensuring Log File Accuracy
 - Implement Log Management
 - Ensure System's Integrity
 - Control Access to Logs
- Network Forensics Steps
 - Ensure Log File Authenticity
 - Work with Copies
 - Maintain Chain of Custody
 - Analyze Logs
- Network Traffic Investigation
 - Why Investigate Network Traffic?
 - Evidence Gathering via Sniffing
 - Gathering Evidence from an IDS
- Documenting the Evidence
- Evidence Reconstruction

How to **Teach** this Module?

- Explain the importance of **network forensics**
- Discuss the fundamental **logging concepts**
- Talk about **event correlation** concepts
- Explain **network forensic readiness** and network forensics steps
- Demonstrate the Router, Firewall, IDS, DHCP and ODBC **logs examination**
- Discuss about the **network traffic examination**
- Talk about the **evidence gathered on a network**
- Help students understand how to perform **evidence reconstruction** for investigation

Exercise

1

Capturing and Analyzing the Logs of a Computer Using GFI
EventsManager

2

Investigating System Log Data Using XpoLog Center Suite

3

Investigating Network Attacks Using Kiwi Log Viewer

4

Investigating Network Traffic Using Wireshark

Module 08: Investigating Web Attacks

What is Covered in **Module 08**?

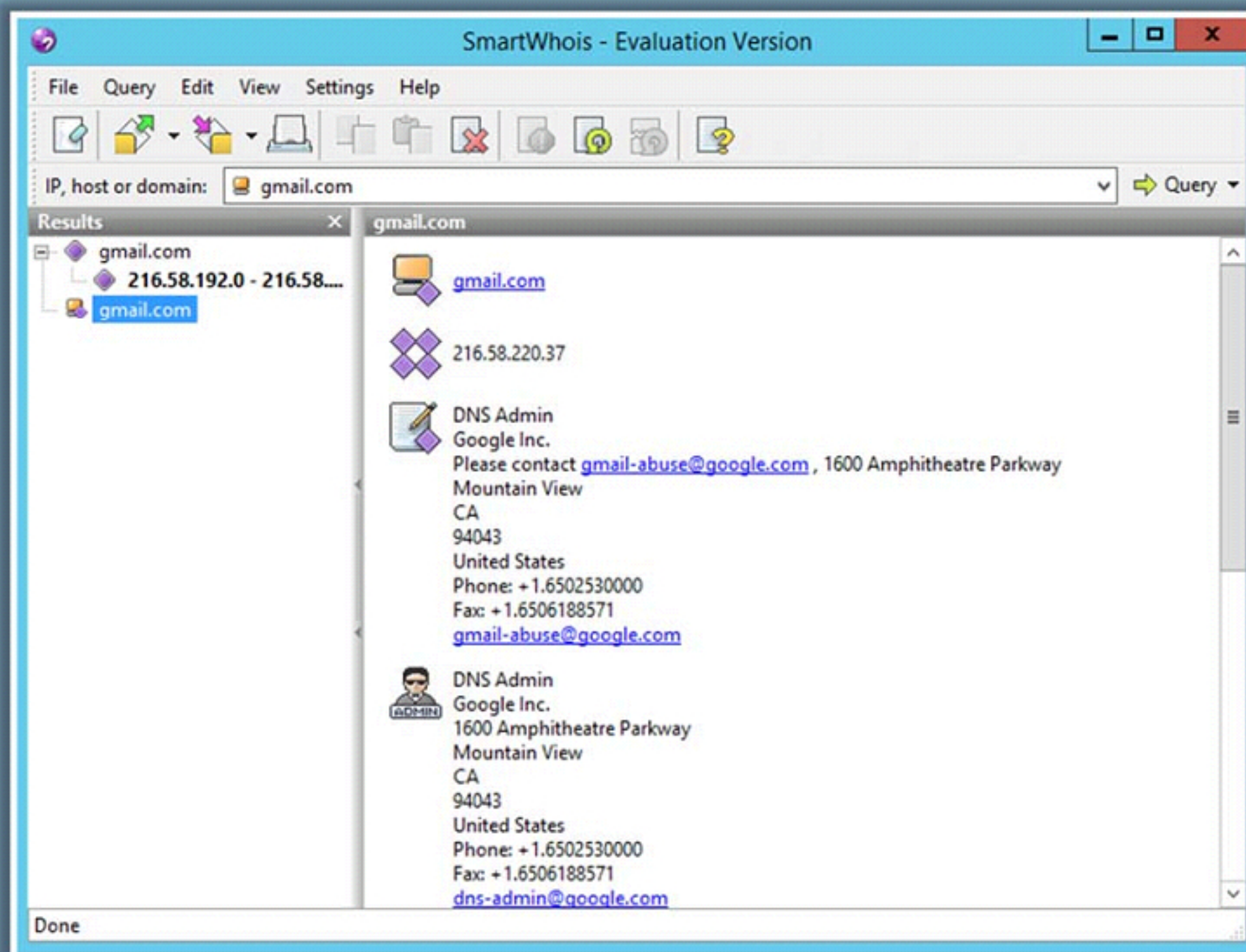
- Web Attack Investigation
 - Web Application Architecture
 - Challenges in Web Application Forensics
- Introduction to Web Application Forensics
 - Web Application Threats - 1
 - Web Application Threats - 2
 - Investigating a Web Attack
 - Investigating Web Attacks in Windows-Based Servers
- Investigating Web Server Logs
 - Internet Information Services (IIS) Logs
 - Investigating Apache Logs
- Investigating Cross-Site Scripting (XSS)
- Investigating XSS: Using Regex to Search XSS Strings
- Investigating SQL Injection Attacks
- Pen-Testing CSRF Validation Fields
- Investigating Code Injection Attack
- Investigating Cookie Poisoning Attack
- Web Attack Detection Tools
 - Web Log Viewers
- Tools for Locating IP Address
- WHOIS Lookup Tools

How to **Teach** this Module?

- Talk about the importance of **web application forensics**
- Demonstrate the **web application architecture** and talk about the challenges faced while conducting web application forensics
- Help students understand **how to indicate web attacks**, and define all the web application threats
- Discuss the steps involved in **web attacks investigation**
- Demonstrate web attacks **investigation on Windows-based servers**
- Discuss about the IIS web server architecture and **IIS logs investigation**
- Explain Apache web server architecture and demonstrate **Apache logs investigation**
- Help students understand how to **investigate various attacks on web applications**

Exercise

1 Analyzing Domain and IP Address Queries Using SmartWhois Tool



Module 09: Database Forensics

What is Covered in **Module 09**?

Database Forensics and Its Importance

MSSQL Forensics

Data Storage in SQL Server

Database Evidence Repositories

Collecting Volatile Database Data

- Collecting Primary Data File and Active Transaction Logs Using SQLCMD
- Collecting Primary Data File & Transaction Logs
- Collecting Active Transaction Logs Using SQL Server Management Studio
- Collecting Database Plan Cache
- Collecting Windows Logs
- Collecting SQL Server Trace Files
- Collecting SQL Server Error Logs

Database Forensics Using SQL Server Management Studio

Database Forensics Using ApexSQL DBA

MySQL Forensics

Internal Architecture of MySQL

Structure of the Data Directory

MySQL Forensics

- Viewing the Information Schema
- MySQL Utility Programs For Forensic Analysis
- Common Scenario for Reference
- MySQL Forensics for WordPress Website Database: Scenario 1
- MySQL Forensics for WordPress Website Database: Scenario 2

How to **Teach** this Module?

- Explain **database forensics** and its importance
- Help students understand how to perform **MSSQL forensics**
- Show how to determine the database evidence repositories and **collect the evidence files**
- Demonstrate how to examine evidence files using **SQL Server Management Studio** and **ApexSQL DBA**
- Explain how to perform **MySQL forensics**
- Talk about the architecture of MySQL and the **structure of data directory**
- Discuss the **MySQL** utilities used to perform **forensic analysis**
- Help students understand the **steps to perform MySQL forensics** on WordPress web application database

Exercise

➤ 01

Extracting the Databases of an Android Device Using Andriller

➤ 02

Analyzing SQLite Databases using DB Browser for SQLite

➤ 03

Performing Forensic Investigation on a MySQL Server Database

Module 10: Cloud Forensics

What is Covered in Module 10?

- Introduction to Cloud Computing
 - Types of Cloud Computing Services
 - Separation of Responsibilities in Cloud
 - Cloud Deployment Models
 - Cloud Computing Threats
 - Cloud Computing Attacks
- Cloud Forensics
 - Usage of Cloud Forensics
 - Cloud Crimes
 - Case Study: Cloud as a Subject
 - Case Study: Cloud as the Object
 - Case Study: Cloud as a Tool
 - Cloud Forensics: Stakeholders and their Roles
- Cloud Forensics Challenges
 - Architecture and Identification
 - Data Collection
 - Legal
 - Analysis
 - Cloud Forensics Challenges
- Investigating Cloud Storage Services
- Investigating Dropbox Cloud Storage Service
 - Artifacts Left by Dropbox Web Portal
 - Artifacts Left by Dropbox Client on Windows
- Investigating Google Drive Cloud Storage Service
 - Artifacts Left by Google Drive Web Portal
 - Artifacts Left by Google Drive Client on Windows

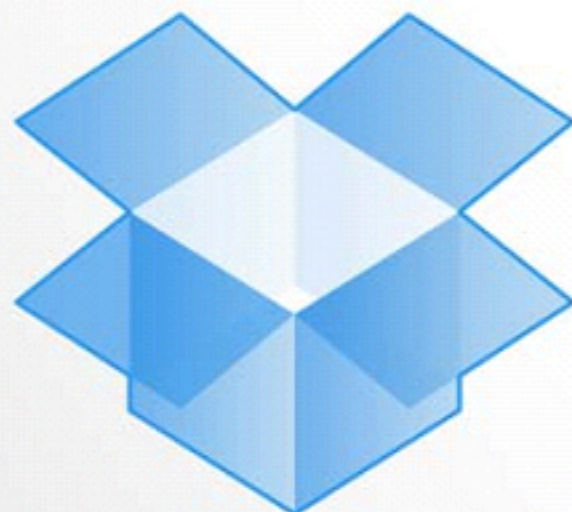
How to **Teach** this Module?

- Explain **cloud computing** concepts
- Discuss all the **cloud computing attacks**
- Explain **importance** of cloud forensics
- Talk about the **usage of cloud forensics**
- Explain the various **types of cloud forensics**
- Discuss the **roles of stake holders** in cloud forensics
- Discuss the **challenges** faced by investigators while performing cloud forensics
- Demonstrate **Dropbox** and **Google Drive** cloud storage services Investigation

Exercise

1

Investigating Dropbox



Dropbox

2

Investigating Google Drive



Google Drive

Module 11: Malware Forensics

What is Covered in **Module 11**?

● Introduction to Malware

- Different Ways a Malware can Get into a System
- Common Techniques Attackers Use to Distribute Malware on the Web
- Components of Malware

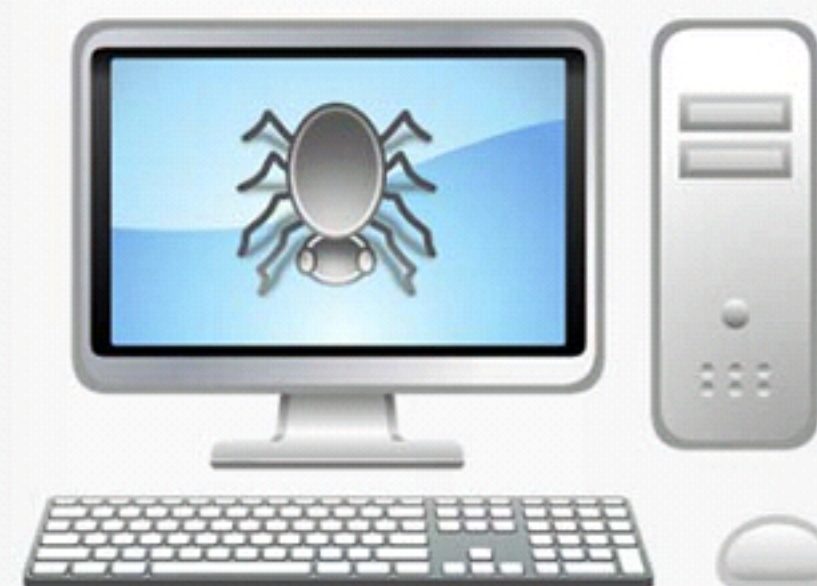
● Introduction to Malware Forensics

- Why Analyze Malware
- Identifying and Extracting Malware
- Prominence of Setting up a Controlled Malware Analysis Lab
- Preparing Testbed for Malware Analysis
- Supporting Tools for Malware Analysis
- General Rules for Malware Analysis

● Documentation Before Analysis

● Types of Malware Analysis

- Malware Analysis: Static
- Malware Analysis: Dynamic



How to **Teach** this Module?

- Talk about **malware** and the discuss the different ways a malware can get into a system
- Discuss the **techniques** attackers use to **spread malware**, and the basic malware components
- Discuss the **malware forensics** concepts, including identification and extraction of malware from live and dead systems
- Explain about the prominence of setting up a **controlled malware analysis lab**
- Talk about preparing **testbed for malware analysis**
- Discuss the general rules to **perform malware analysis**
- Help students understand the **Static and Dynamic malware analysis** and malicious documents analysis
- Discuss the **challenges** faced while performing malware analysis

Exercise

1

Perform Static Analysis of the Suspicious File

2

Dynamic Malware Analysis

3

Analyze Malicious PDF File

4

Scanning PDF files using online Resources

5

Scan suspicious MS-office file for Malice

Module 12: Investigating Email Crimes

What is Covered in **Module 12**?

- Email System
 - Email Clients
 - Email Server
 - SMTP and POP3 Server
 - Importance of Electronic Records Management
- Email Crimes (Email Spamming, Mail Bombing/Mail Storm, Phishing, Email Spoofing, Crime via Chat Room, Identity Fraud/Chain Letter)
 - Crime Via Chat Room
- Email Message
 - Sample of Email Header
 - List of Common Headers and X-Headers
- Steps to Investigate Email Crimes and Violation
 - Obtain a Search Warrant and Seize the Computer and Email Account
 - Examine E-mail Messages
 - Acquire Email Archives
 - Recover Deleted Emails
 - Examining Email Logs
- Email Forensics Tools
 - Recover My Email
 - MailXaminer
- Laws and Acts against Email Crimes
 - U.S. Laws Against Email Crime: CAN-SPAM Act

How to **Teach** this Module?

- Explain **Email System**, Email Clients and Email Servers, along with their characteristics
- Explain the importance of **electronic records management**
- Discuss about **email crimes** and the crimes committed via chat room
- Talk about the **components of an Email message**
- Help students understand the **Common Headers** and **X-Headers**
- Discuss the steps to **investigate email crimes** and violations
- Demonstrate **email forensics tools**
- Discuss about the **U.S. Law against email crime**: CAN-SPAM act and its characteristics

Exercise

Recovering Deleted Emails Using the Recover My Email

1

Investigating Email Crimes Using Paraben's Email Examiner Tool

2

Tracing an Email Using the eMailTrackerPro Tool

3

Module 13: Mobile Forensics

What is Covered in **Module 13**?

● Mobile Device Forensics

- Why Mobile Forensics?
- Top Threats Targeting Mobile Devices
- Mobile Hardware and Forensics
- Mobile OS and Forensics
 - Architectural Layers of Mobile Device Environment
 - Android Architecture Stack
 - Android Boot Process
 - iOS Architecture
 - iOS Boot Process
 - Normal and DFU Mode Booting
 - Booting iPhone in DFU Mode
 - Mobile Storage and Evidence Locations
- What Should You Do Before the Investigation?

● Mobile Forensics Process

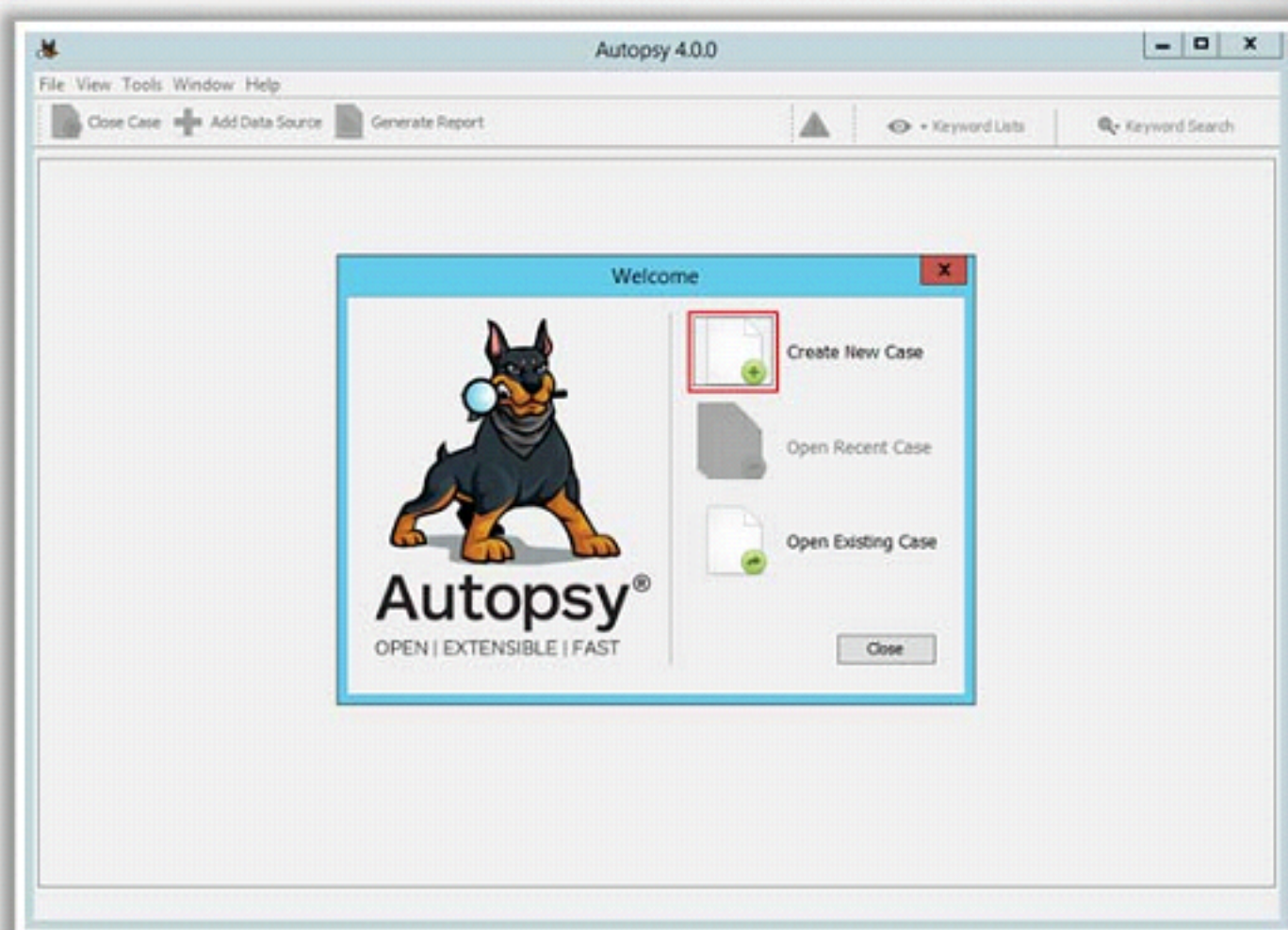
- Collecting the Evidence
- Document the Scene and Evidence
- Evidence Preservation
- Set of Rules for Switching ON/OFF Mobile Phone
- Forensics Imaging
- Phone Locking
- Enabling USB Debugging
- Mobile Evidence Acquisition
- Logical Acquisition
- Physical Acquisition
- File System Acquisition
- File Carving
- iPhone Data Extraction
- Generating Investigation Report

How to **Teach** this Module?

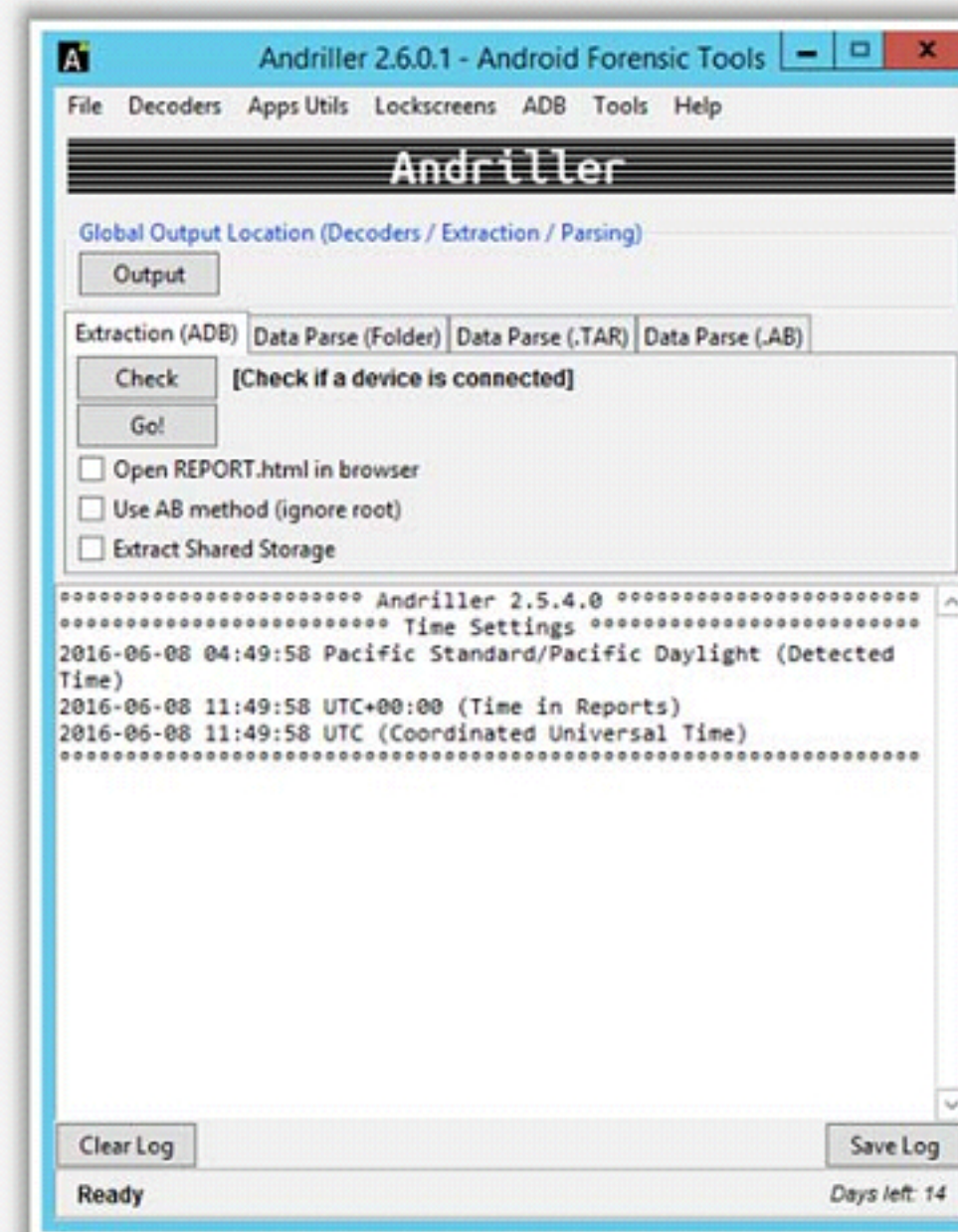
- Explain **mobile device forensics** and the need for mobile device forensics
- Explain the **role of mobile hardware** and OS while conducting forensics on mobiles
- Talk about the **architectural layers** of mobile device environment
- Discuss about **Android architecture stack** and Android boot process
- Discuss about **iOS architecture stack** and iOS boot process
- Talk about the mobile **storage** and **evidence locations**
- Discuss the **steps** you need to follow **before performing investigation**
- Help students understand how to perform **mobile forensics**

Exercise

1 Analyzing the Forensic Image and Carving the Deleted Files Using Autopsy



2 Investigating an Android Device using Andriller



Module 14: Forensic Report Writing and Presentation

What is Covered in **Module 14**?

- Writing Investigation Reports
 - Forensic Investigation Report
 - Important Aspects of a Good Report
 - Forensic Investigation Report Template
 - Report Classification
 - Guidelines for Writing a Report
 - Other Guidelines for Writing a Report
- Expert Witness Testimony
 - What is an Expert Witness?
 - Roles of an Expert Witness
 - Technical Witness Vs. Expert Witness
 - Daubert Standard
 - Frye Standard.
 - What Makes a Good Expert Witness?
- Importance of Curriculum Vitae
- Professional Code of Conduct for an Expert Witness
- Preparing for a Testimony
 - Testifying in the Court
 - General Order of Trial Proceedings
 - General Ethics While Testifying
 - Importance of Graphics in a Testimony
 - Helping your Attorney
 - Avoiding Testimony Issues
 - Testifying during Direct Examination
 - Testifying during Cross- Examination
 - Testifying during Cross- Examination: Best Practices
- Guidelines to Testify at a Deposition
- Dealing with Media

How to **Teach** this Module?

- Talk about the importance of **forensic investigation reports**
- Discuss the important aspects of a **good report**
- Explain the contents of a forensics **investigation report template**
- Talk about **investigation reports** and the **guidelines** for writing a report
- Discuss about an **expert witness** and the **roles** of expert witness
- Explain the Difference between **Technical Witness** Vs. **Expert Witness**
- Discuss about **Daubert** and **Fyre** Standards
- Help students understand how to **testify in a court** and the general ethics while testifying

How to **Become** a Certified Computer Hacking Forensic Investigator?



To achieve **EC-Council Certified Forensic Investigator (CHFI)**, pass EC-Council's Certified Forensic Investigator 312-49 exam

1 Number of Questions: **150**

2 Passing Score: **70%**

3 Test Duration: **4 Hours**

4 Test Format: **Multiple Choice**

5 Test Delivery: **ECC Exam Portal**

Thank you!