

## Instructions for Downloading your CHFIv9 Electronic Courseware, Lab Manuals, and Tools.

### Step 1:

Visit: <https://aspen.eccouncil.org>. If you have an account already, skip to **Step 4**.

### Step 2:

Click **Register** and fill out the registration form. Click the **Register** button.

### Step 3:

Using the email you provided in **Step 2**, follow the instructions in the auto-generated email to activate your EC-Council Aspen Portal account.

### Step 4:

Login using your Username and Password.

### Step 5:

Once successfully logged in, click **Academia** icon under the **Learning Resources** section. It will open the Academia page.

### Step 6:

Enter the access code below in the **Access Code** field and click the **Submit** button.

**Access Code: XXXXXXXXXXXXXXXXX**

### Step 7:

If your Access Code is valid, scroll down and select **CHFIv9 Courseware** in the **Select Courseware** dropdown menu to view the CHFI e-courseware, lab manuals, and tools.

### Support:

E-mail support is available at [academia@eccouncil.org](mailto:academia@eccouncil.org).

### System Requirements:

The Academia page contains details about system requirements and how to download the e-courseware.

## Instructions to Download Digital Copy of your Class Certificate of Attendance



**Step 1:** Complete the official training.

**Step 2:** Visit: <https://aspen.eccouncil.org>. If you have an account already, skip to **Step 5**.

**Step 3:** Click **Register** and fill out the registration form. Click the **Register** button.

**Step 4:** Using the email you provided in **Step 3**, follow the instructions in the auto-generated email to activate your EC-Council Aspen Portal account.

**Step 5:** Login using your Username and Password.

**Step 6:** Click the **Class Eval** icon in the **Student Services** section.

**Step 7:** Enter the **Evaluation Code** (see the code below) in the **Evaluation Code** field and click the **Submit**.

**Step 8:** Fill in the **Course Evaluation Form**. **\*Note:** All fields on this form are mandatory. Click the **Submit Classroom Evaluation** button.

**Step 9:** On the **Course Evaluation Submission** page, click the **Download Certificate of Attendance** button to download your certificate of attendance.

**Evaluation Code: \*\*\*CHFI-\*\*\*\*\***



# **Computer Hacking Forensic Investigator**

**Version 9**

## EC-Council

Copyright © 2017 by EC-Council. All rights reserved. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

Information has been obtained by EC-Council from sources believed to be reliable. EC-Council uses reasonable endeavors to ensure that the content is current and accurate, however, because of the possibility of human or mechanical error we do not guarantee the accuracy, adequacy, or completeness of any information and are not responsible for any errors or omissions or the accuracy of the results obtained from use of such information.

The courseware is a result of extensive research and contributions from subject matter experts from the field from all over the world. Due credits for all such contributions and references are given in the courseware in the research endnotes. We are committed towards protecting intellectual property. If you are a copyright owner (an exclusive licensee or their agent), and if you believe that any part of the courseware constitutes an infringement of copyright, or a breach of an agreed licence or contract, you may notify us at **legal@eccouncil.org**. In the event of a justified complaint, EC-Council will remove the material in question and make necessary rectifications.

The courseware may contain references to other information resources and security solutions, but such references should not be considered as an endorsement of or recommendation by EC-Council.

Readers are encouraged to report errors, omissions and inaccuracies to EC-Council at **legal@eccouncil.org**.

If you have any issues, please contact **support@eccouncil.org**.



# Foreword

Cyber war has begun and we can also see the consequences in our daily lives. With the onset of sophisticated cyber-attacks, the need for advanced cyber security and investigation training is a mandate in present day. If you or your organization requires the knowledge or skills to identify, track, and prosecute the cybercriminal, then CHFI is the course for you.

If you are reading this courseware, it is quite possible to understand the process of detecting hacking attacks and properly extracting evidence to report the crime, and conduct audits to prevent future attacks. However, we would like to put forth our motive behind compiling a resource such as this one, and what you can gain from this course.

You might find yourself asking, why choose this course, when there are several out there. The truth is that there cannot be any single courseware that can address all the investigative methods in a detailed manner. CHFI presents detailed methodological approach to computer forensics and evidence analysis. It 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.

You may also want to know “After this course, what?” CHFI investigators will possess necessary skills to excel in incident handling and investigate various types of security incidents such as data breaches, latest persistent security issues, insider employee threats and intricate digital forensic circumstances and cases. CHFI certified professional will be able to develop effective security policy in the company.

Finally, this is not the end! This courseware is to be considered as a ‘work-in-progress’, because we will be adding value to this courseware over time. You may find some aspects detailed, while others may find it brief. The yardstick that we have used in this respect is simple - “does the content help explain the point at hand?” This doesn’t mean that we would not love to hear from you regarding your viewpoints and suggestions. Do send us your feedback so that we can make this course a more useful one.

# Table of Contents

Module Number	Module Name	Page No.
00	Student Introduction	I
01	Computer Forensics in Today's World	01
02	Computer Forensics Investigation Process	60
03	Understanding Hard Disks and File Systems	228
04	Data Acquisition and Duplication	386
05	Defeating Anti-forensics Techniques	463
06	Operating System Forensics	615
07	Network Forensics	792
08	Investigating Web Attacks	910
09	Database Forensics	962
10	Cloud Forensics	1022
11	Malware Forensics	1103
12	Investigating Email Crimes	1194
13	Mobile Forensics	1262
14	Forensics Report Writing and Presentation	1374
	References	1414



# Welcome to Computer Hacking Forensic Investigator Class!

## Student Introduction

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



## Computer Hacking Forensic Investigator v9

### Module 00: Welcome to Computer Hacking Forensic Investigator Class!

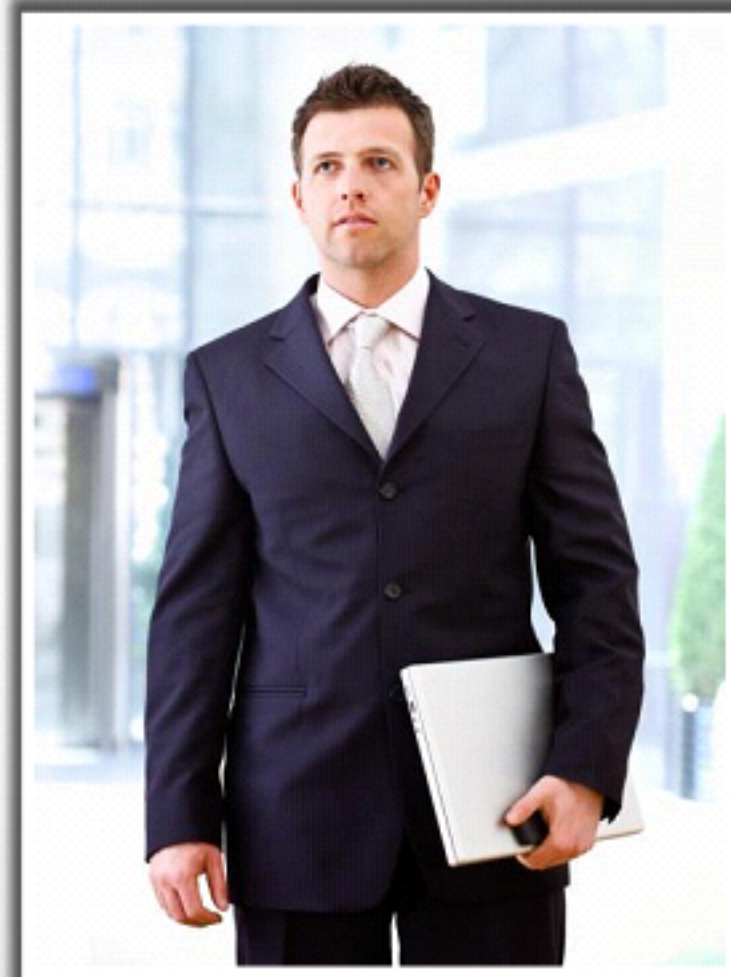
Exam 312-49



# Introduction



- Name
- Company Affiliation
- Title / Function
- Job Responsibility
- System Security related Experience
- Expectations



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Course Materials



**Identity Card**



**Student Courseware**



**CHFI-Tools**



**Lab Manual/  
Workbook**



**Course Evaluation**



**Reference Materials**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



# Course Outline

01

Computer Forensics in Today's World

02

Computer Forensics Investigation Process

03

Understanding Hard Disks and File Systems

04

Data Acquisition and Duplication

05

Defeating Anti-forensics Techniques

06

Operating System Forensics

07

Network Forensics

08

Investigating Web Attacks

09

Database Forensics

10

Cloud Forensics

11

Malware Forensics

12

Investigating Email Crimes

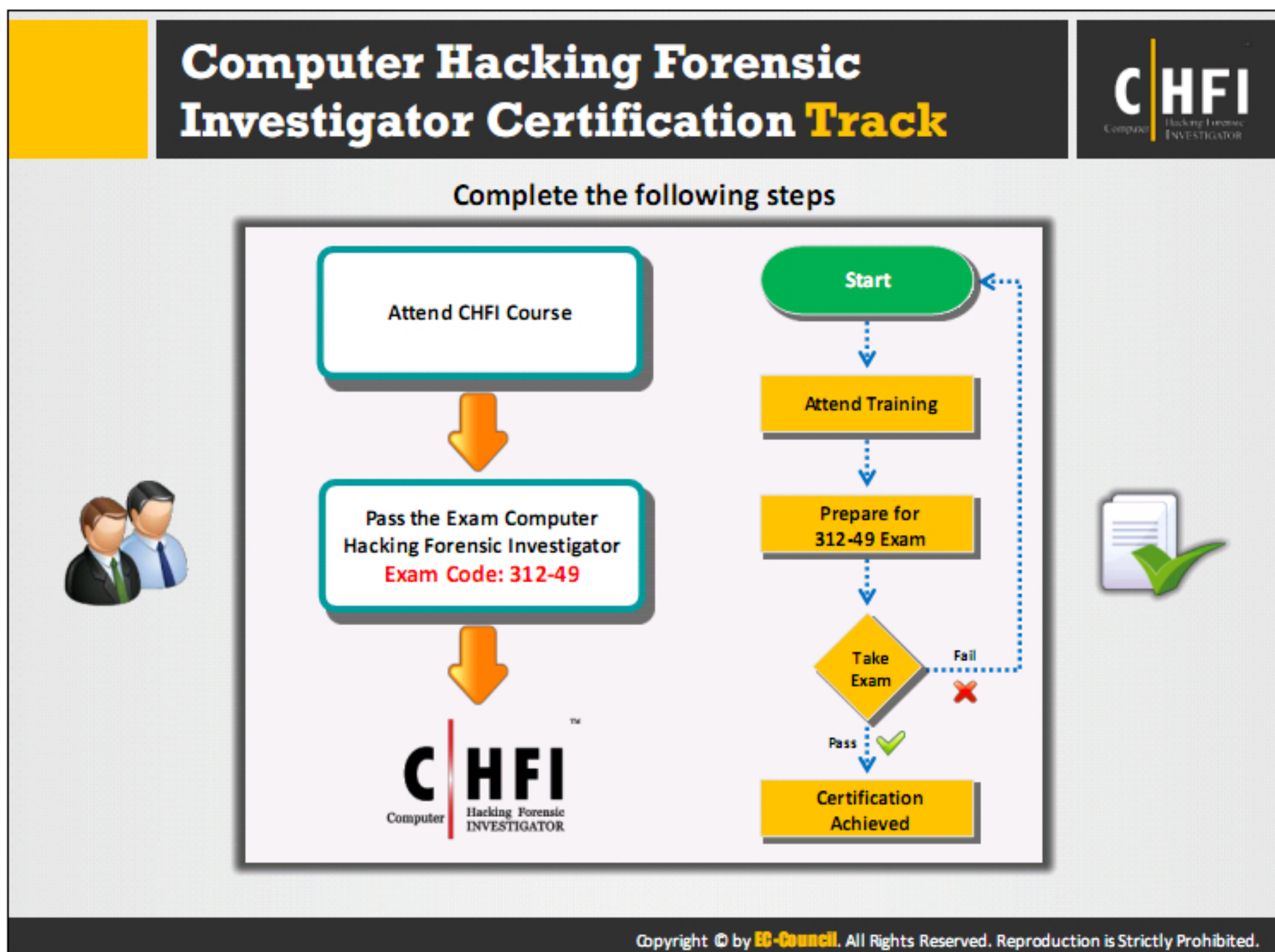
13









Mobile Forensics









14

Forensics Report Writing and Presentation

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



CHFIv9 Exam Information		CHFI Computer Hacking Forensic Investigator
	Exam Title: <b>Computer Hacking Forensics Investigator v9</b>	
	Exam Code: <b>312-49</b>	
	Number of Questions: <b>150</b>	
	Duration: <b>4 hours</b>	
	Availability: <b>ECC Exam</b>	
	Passing Score: <b>70%</b>	
	For questions about the exam voucher/schedule please contact the training center	
	<b>This is a difficult exam and requires extensive knowledge of CHFI Core Modules</b>	
Copyright © by <b>EC-Council</b> . All Rights Reserved. Reproduction is Strictly Prohibited.		

Student Facilities		CHFI Computer Hacking Forensic Investigator	
	<b>Class Hours</b>		<b>Messages</b>
	<b>Building Hours</b>		<b>Restrooms</b>
	<b>Phones</b>		<b>Meals</b>
	<b>Parking</b>		<b>Recycling</b>
Copyright © by <b>EC-Council</b> . All Rights Reserved. Reproduction is Strictly Prohibited.			



## Lab Sessions



- Lab Sessions are designed to **reinforce** the classroom sessions
- The sessions are intended to give a **hands on experience** only and does not guarantee proficiency
- There are plenty of labs in the Lab Manual. Please practice these labs back at home.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## 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 strict 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.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## How CHFI Will Help You – A Checklist for Forensic Investigators (Cont'd)



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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## How CHFI Will Help You – A Checklist for Forensic Investigators (Cont'd)



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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## How CHFI Will Help You – A Checklist for Forensic Investigators (Cont'd)



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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

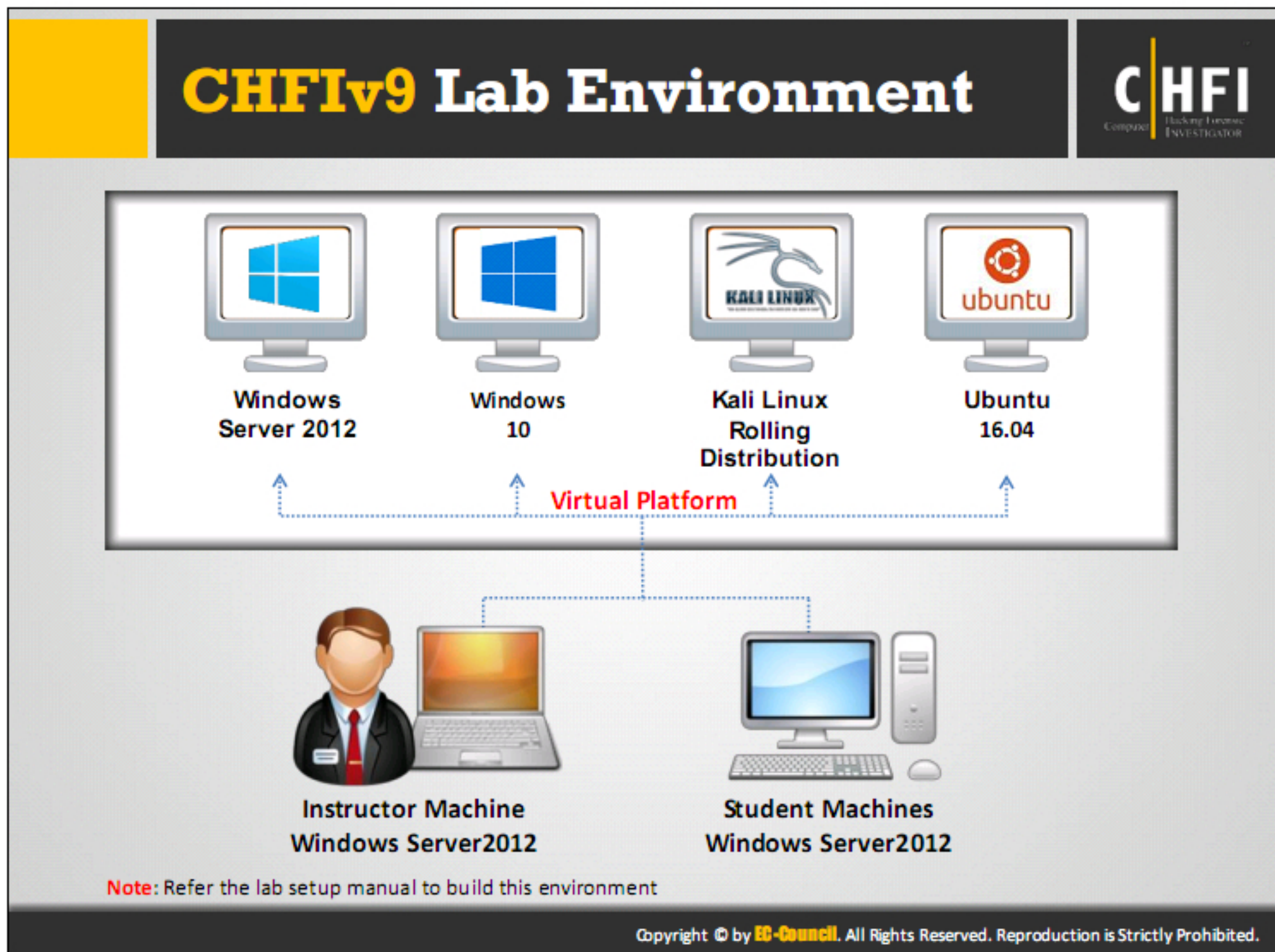
## CHFI Class Speed




- The CHFI class is **extremely fast paced**
- There are tons of forensics **tools** and investigation **technologies** covered in the curriculum
- The instructor **WILL NOT** be able to demonstrate **ALL** the tools in this class
- He will showcase only **selected tools**
- The students are required to **practice with the tools** not demonstrated in the class on their own

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.





	<b>Student Computer Checklist</b>	
✓	Check if your machine has the <b>Windows Server 2012</b> as host, and <b>Windows Server 2012</b> , <b>Windows 10</b> , <b>Kali Linux</b> , and <b>Ubuntu</b> as VMs installed (All Windows Machines Fully Patched)	
✓	Write down IP addresses of the <b>host</b> and the <b>Virtual Machine</b>	
✓	Check if you can ping between the <b>VMs</b>	
✓	Verify that <b>Windows Explorer</b> is set to show all files and file types, including hidden files and extensions in <b>Windows Server 2012</b> and <b>Windows 10</b> VMs	
✓	Make sure that you can access <b>C:\CHFI-Tools</b> directory located on <b>Windows Server 2012</b> from the VM, and mapped as <b>Network Drive (Z:)</b>	
✓	Check if you can access <b>Internet</b> and Browse <a href="https://www.eccouncil.org">https://www.eccouncil.org</a> using <b>Google Chrome</b>	
✓	Check for <b>snapshots</b> of <b>Virtual Machines</b>	
Copyright © by <b>EC-Council</b> . All Rights Reserved. Reproduction is Strictly Prohibited.		



