uCertify

Course Outline

Ethical Hacking and Network Analysis with Wireshark

04 Aug 2025

1. Exercises, Quizzes, Flashcards & Glossary

   Number of Questions
2. Expert Instructor-Led Training
3. ADA Compliant & JAWS Compatible Platform
4. State of the Art Educator Tools
5. Award Winning Learning Platform (LMS)
6. Chapter & Lessons

   Syllabus

   Chapter 1: Introduction

   Chapter 2: Ethical Hacking and Networking Concepts

   Chapter 3: Getting Acquainted with Wireshark and Setting up the Environment

   Chapter 4: Getting Started with Packet Sniffing

   Chapter 5: Sniffing on 802.11 Wireless Networks

   Chapter 6: Sniffing Sensitive Information, Credentials and Files

   Chapter 7: Analyzing Network Traffic Based on Protocols

   Chapter 8: Analyzing and Decrypting SSL/TLS Traffic

   Chapter 9: Analyzing Enterprise Applications

   Chapter 10: Analysing VoIP Calls Using Wireshark

   Chapter 11: Analyzing Traffic of IoT Devices

   Chapter 12: Detecting Network Attacks with Wireshark

   Chapter 13: Troubleshooting and Performance Analysis Using Wireshark

   Videos and How To

1. Quiz

Quizzes test your knowledge on the topics of the exam when you go through the course material. There is no limit to the number of times you can attempt it.

2. Expert Instructor-Led Training

uCertify uses the content from the finest publishers and only the IT industry's finest instructors. They have a minimum of 15 years real-world experience and are subject matter experts in their fields. Unlike a live class, you can study at your own pace. This creates a personal learning experience and gives you all the benefit of hands-on training with the flexibility of doing it around your schedule 24/7.

3. ADA Compliant & JAWS Compatible Platform

uCertify course and labs are ADA (Americans with Disability Act) compliant. It is now more accessible to students with features such as:

- Change the font, size, and color of the content of the course
- Text-to-speech, reads the text into spoken words
- Interactive videos, how-tos videos come with transcripts and voice-over
- Interactive transcripts, each word is clickable. Students can clip a specific part of the video by clicking on a word or a portion of the text.

JAWS (Job Access with Speech) is a computer screen reader program for Microsoft Windows that reads the screen either with a text-to-speech output or by a Refreshable Braille display. Student can easily navigate uCertify course using JAWS shortcut keys.

4. State of the Art Educator Tools

uCertify knows the importance of instructors and provide tools to help them do their job effectively. Instructors are able to clone and customize course. Do ability grouping. Create sections. Design grade scale and grade formula. Create and schedule assessments. Educators can also move a student from self-paced to mentor-guided to instructor-led mode in three clicks.

5.  Award Winning Learning Platform (LMS)

uCertify has developed an award winning, highly interactive yet simple to use platform. The SIIA CODiE Awards is the only peer-reviewed program to showcase business and education technology's finest products and services. Since 1986, thousands of products, services and solutions have been recognized for achieving excellence. uCertify has won CODiE awards consecutively for last 7 years:

- **2014**
    1. Best Postsecondary Learning Solution

- **2015**
    1. Best Education Solution
    2. Best Virtual Learning Solution
    3. Best Student Assessment Solution
    4. Best Postsecondary Learning Solution
    5. Best Career and Workforce Readiness Solution
    6. Best Instructional Solution in Other Curriculum Areas
    7. Best Corporate Learning/Workforce Development Solution

- **2016**
    1. Best Virtual Learning Solution
    2. Best Education Cloud-based Solution
    3. Best College and Career Readiness Solution
    4. Best Corporate / Workforce Learning Solution
    5. Best Postsecondary Learning Content Solution
    6. Best Postsecondary LMS or Learning Platform
    7. Best Learning Relationship Management Solution

- **2017**
    1. Best Overall Education Solution
    2. Best Student Assessment Solution
    3. Best Corporate/Workforce Learning Solution
    4. Best Higher Education LMS or Learning Platform

- **2018**
    1. Best Higher Education LMS or Learning Platform
    2. Best Instructional Solution in Other Curriculum Areas
    3. Best Learning Relationship Management Solution

- **2019**
    1. Best Virtual Learning Solution
    2. Best Content Authoring Development or Curation Solution
    3. Best Higher Education Learning Management Solution (LMS)

- **2020**
    1. Best College and Career Readiness Solution
    2. Best Cross-Curricular Solution
    3. Best Virtual Learning Solution

6.  Chapter & Lessons

uCertify brings these textbooks to life. It is full of interactive activities that keeps the learner engaged. uCertify brings all available learning resources for a topic in one place so that the learner can efficiently learn without going to multiple places. Challenge questions are also embedded in the chapters so learners can attempt those while they are learning about that particular topic. This helps them grasp the concepts better because they can go over it again right away which improves learning.

Learners can do Flashcards, Exercises, Quizzes and Labs related to each chapter. At the end of every lesson, uCertify courses guide the learners on the path they should follow.

Syllabus

Chapter 1: Introduction

Chapter 2: Ethical Hacking and Networking Concepts

- Introduction
- Introduction to ethical hacking
- Introduction to networking concepts
- The OSI model
- The TCP/IP model
- IP networks and subnets
- Switching and routing packets
- WAN links
- Wireless networking
- What is network traffic
- Overview of network packet sniffing
- Active and passive sniffing
- Wireshark in ethical hacking and traffic analysis
- Conclusion

Chapter 3: Getting Acquainted with Wireshark and Setting up the Environment

- Introduction
- What is Wireshark
- Downloading and Installing Wireshark with Libraries
- Exploring the Wireshark user interface
- Conclusion

Chapter 4: Getting Started with Packet Sniffing

- Introduction
- Define your sniffing targets
- Choosing network interfaces
- Performing a packet sniffing
- Remote network packet
- Display and capture filters
- Maximizing packet capture performance
- Stop sniffing, saving, and exporting packets
- Challenges/limitations of packet capturing
- Conclusion

Chapter 5: Sniffing on 802.11 Wireless Networks

- Introduction
- 802.11 wireless networks
- 802.11 wireless network architecture
- 802.11 packet structure
- Wireless card modes
- Difference between monitor mode and promiscuous mode
- WLAN capture setup
- Sniffing WLAN Network Traffic
- Wi-Fi sniffer: WPA/WPA2
- 802.11 Sniffer Capture Analysis: Multicast
- 802.11 Sniffer Capture Analysis: Web authentication
- Challenges of sniffing 802.11 wireless networks
- Conclusion

Chapter 6: Sniffing Sensitive Information, Credentials and Files

- Introduction
- Sniffing the activity over USB interfaces
- Capturing credentials on HTTP
- Extracting images from PCAP file using Wireshark

- PDF and ZIP files saving from Wireshark
- Capturing Telnet password
- Capturing SMTP password
- Identifying hosts and users with Wireshark
- Conclusion

Chapter 7: Analyzing Network Traffic Based on Protocols

- Introduction
- IPv4 and IPv6
- ARP
- ICMP
- TCP
- UDP
- HTTP
- FTP
- SMTP
- DHCPv6
- DNS

- Conclusion

Chapter 8: Analyzing and Decrypting SSL/TLS Traffic

- Introduction
- Introduction to SSL/TLS
- The SSL/TLS Handshake
- Key exchange
- Decrypting SSL/TLS traffic using Wireshark
- Conclusion

Chapter 9: Analyzing Enterprise Applications

- Introduction
- Identifying the service running over the network
- Analyzing Microsoft Terminal Server and Citrix communications
- Analyzing the database traffic
- Analyzing SNMP traffic
- Conclusion

Chapter 10: Analysing VoIP Calls Using Wireshark

- Introduction

- Introduction to VoIP technology
- VoIP architecture
- Working of VoIP
- VoIP supporting protocols
- Sniffing VoIP traffic
- SIP call analysis
- Analysing RTP Streams in VoIP Traffic
- Challenges/limitations in analyzing VoIP calls through Wireshark
- Conclusion

Chapter 11: Analyzing Traffic of IoT Devices

- Introduction
- Introduction to IoT
- IoT devices: Use cases for network sniffing
- Sniffing traffic of IoT devices
- Analyzing traffic of IoT devices
- Conclusion

Chapter 12: Detecting Network Attacks with Wireshark

- Introduction
- Detecting suspicious network traffic patterns
- Detecting port scanning
- Detecting Denial of Service and Distributed Denial of Service attacks
- Detecting Brute-force and application attacks
- Detecting ARP poisoning
- Detecting session hijacking
- Detecting honeypot traffic
- Detecting Heartbleed bug
- Challenges/limitations of analysis of network attacks using Wireshark
- Conclusion

Chapter 13: Troubleshooting and Performance Analysis Using Wireshark

- Introduction
- Troubleshooting methodology
- Troubleshooting connectivity issues
- Troubleshooting functional issues
- Performance analysis methodology

- Troubleshooting TCP protocol issues
- Troubleshooting slow application response time
- Conclusion

You can’t stay away! Get

3187 Independence Drive
Livermore, CA 94551,
United States

+1-415-763-6300

support@ucertify.com

www.ucertify.com