CHAPPELL UNIVERSITY

Wireshark® Protocols and Troubleshooting

V2.2A

SAMPLE COURSE OUTLINE

STUDENT MANUAL

COURSE OUTLINE

Section 1: Course Introduction and Resources
Section 2: Wireshark Essential Features for Troubleshooting (Course Profile)
Section 3: Capture Methods and Capture Filters
Section 4: Customization - Wireshark Preferences
Section 5: Navigation, Coloring, and Reassembly
Section 6: Detect Application and Path Delays (Working with Time)
Section 7: Extract and Interpret Essential Trace File Statistics
Section 8: Focus on Traffic Using Display Filters
Section 8: TCP/IP Communications Overview
Section 10: Analyze Domain Name System (DNS) Traffic
Section 11: Analyze Address Resolution Protocol (ARP) Traffic
Section 12: Analyze Internet Protocol (IPv4) Traffic
Section 13: Analyze Internet Control Message Protocol (ICMP) Traffic
Section 14: Analyze User Datagram Protocol (UDP) Traffic
Section 15: Analyze Transmission Control Protocol (TCP) Traffic
Section 16: Analyze Hypertext Transfer Protocol (HTTP) Traffic
Section 17: Decrypting Traffic
Section 18: Command-Line and 3rd-Party Tools
Appendix A: Advanced Display Filters
Appendix B: Analyze VoIP Traffic
Appendix C: Analyze Dynamic Host Configuration Protocol (DHCP) Traffic
Appendix D: Analyze File Transfer Protocol (FTP) Traffic

LAB LIST

Lab 1: Create Your Troubleshooting Profile
Lab 2: Use GeoIP Mapping to Find an Issue
Lab 3: Build a Coloring Rule to Differentiate DNS Traffic
Lab 4: Detect and Differentiate Delays
Lab 5: Find the Top Talkers and Protocols/Applications on a Network
Lab 6: Create and Use an I/O Graph to Spot Performance Issues
Lab 7: Practice Display Filtering
Lab 8: Catch DNS Errors and Slow DNS Responses
Lab 9: Find the Fault – Network Disconnects
Lab 10: Filter on Problem Addresses
Lab 11: Analyze and Color ICMP Traffic
Lab 12: Analyze UDP-based Multicast Streams and Queuing Delays
Lab 13: Use an IO Graph to Locate TCP Performance Issues
Lab 14: Determine the Cause of Slow Page Loading
Lab 15: Create a Button to Detect HTTP Error Responses
Lab 16: Export an HTTP Object (Carving)
Lab 17: Decrypt HTTPS Communications
Lab 18: Evaluate, Extract, and Capture with CLI Tools

Chappell University® Course:
Wireshark® Protocols and Troubleshooting Student Manual

ISBN13: N/A

Student Manual Part Number: TR6L-A v3.1B

Distributed worldwide for Chappell University through Protocol Analysis Institute, Inc.

For general information on Chappell University or Protocol Analysis Institute, Inc, including information on corporate licenses, updates, future titles, or courses, contact Protocol Analysis Institute, Inc. at info@chappellU.com.

For authorization to photocopy items for corporate, personal or educational use, contact Protocol Analysis Institute, Inc. at info@chappellU.com.

Protocol Analysis Institute, Inc.
dba Chappell University
720 N. 10th Street, Suite A352
Renton, WA 98057 USA

Chappell University®
720 N. 10th Street, Suite A352
Renton, WA 98057 USA
info@chappellU.com
www.chappellU.com

ADD-ONS

All-Access Pass The All Access Pass provides full-time access to recorded courses focusing on Wireshark functionality, network troubleshooting, network forensics, and more. Visit https://chappellu.com for more information.

WCNA Exam Vouchers Purchase in bulk to take the WCNA Exam (online proctored or at a Kryterion testing center worldwide). The WCNA Certification Exam focuses on analyzing packets and protocols, for network troubleshooting, optimization, and security. For more information, visit https://wcnacertification.com.

For more information, email info@chappellU.com.

About the Course Author
Chappell University Founder

Laura Chappell
Founder, Chappell University
Sr. Protocol Analyst, Protocol Analysis Institute, Inc.
Creator, WCNA Certification Program

Ms. Chappell researches, documents, and presents information on network protocols, analysis, Wireshark, network forensics, and interplanetary communications. Ms. Chappell is the creator of the WCNA Certification program (formerly referred to as the Wireshark Certified Network Analyst Certification program). Ms. Chappell also founded the original Wireshark University, Wireshark University Instructor Program, and Wireshark University Training Partner Program.

Ms. Chappell is often called in to analyze more complex network problems that require visibility into the communications system. Her clients include the U.S. Navy, IBM Corporation, Apple, Cisco Systems, Disney, U.S. Court of Appeals, United Bank of Switzerland, Australian High Tech Crime Centre, Capital One Financial Services, U.S. Armory, Hong Kong Police Department, Symantec Corporation, McAfee Corporation, Microsoft, Bank of San Francisco, Beth Israel Medical Center (Harvard), U.S. Joint Warfare Analysis Center, and the Federal Aviation Administration (FAA).

Ms. Chappell mixes onsite analysis services with live analysis training to develop self-sufficient IT teams within her client organizations.

As a member of the High Technology Crime Investigation Association (HTCIA) and the FBI's Infragard, Ms. Chappell has trained local, regional, national, and international law enforcement officers, as well as corporate security professionals on the methods and tools used to attack and defend networks. Ms. Chappell is also a voting member of Institute for Electrical and Electronics Engineers (IEEE) (member since 1990).

Ms. Chappell's enthusiasm for her topics, sense of humor and preference for working "live" during sessions has consistently ranked her as a top presenter at numerous industry conferences including Microsoft TechEd North America, Microsoft TechEd Europe, HP Technical Forum, Cisco Live, HTCIA International Conference, SharkFest, and InterOp.

In addition, Ms. Chappell is currently an active member of the Interplanetary Networking Special Interest Group focused on the documentation of deep space networking communication protocols. Ms. Chappell regularly lectures on the Deep Space Network (DSN) and Delay and Disruption Tolerant Networking (DTN).

Ms. Chappell can be reached via email at *laura@chappellu.com*.

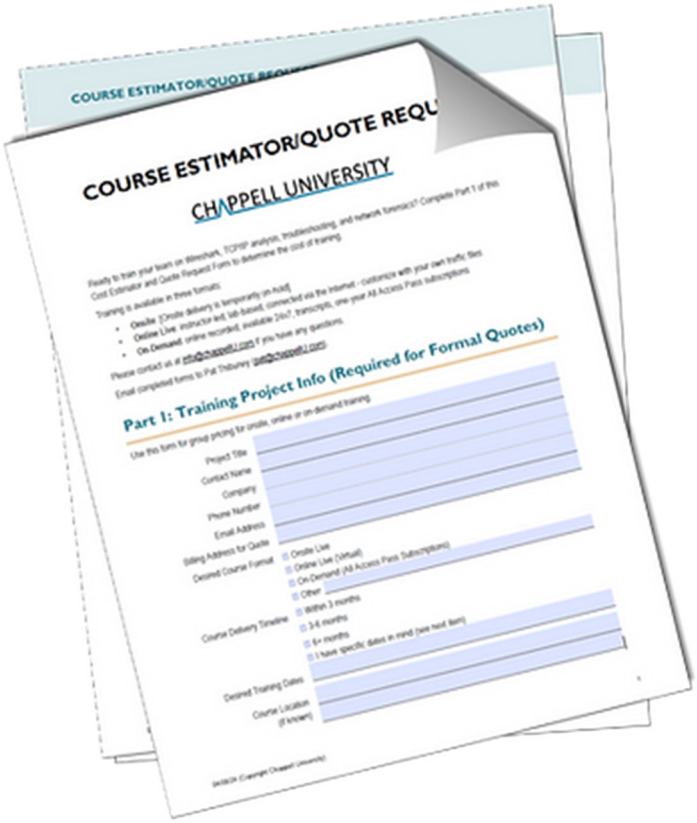
CHAPPELL UNIVERSITY

HOW TO PURCHASE A CUSTOM COURSE

Bring Laura Chappell online or onsite to speed up your team's trobleshooing and forensics processes.

Complete and submit the Course Estimator/Quote Request (Course Designer) document or simply let us know the following:

1. **Course Focus**: Do you want the course to focus on troubleshooting, network forensics, and/or general Wireshark functionality
2. **Course Length**: Minimum course length is 2 days. Laura's maximum course length is 10 days.
3. **Date Range**: Let us know which in which months you'd like the course delivered. We typically need at least 2 months advance preparation time.



Questions? Contact us at info@chappellu.com.

Table of Contents

Section 15: Analyze Transmission Control Protocol (TCP) Traffic 217

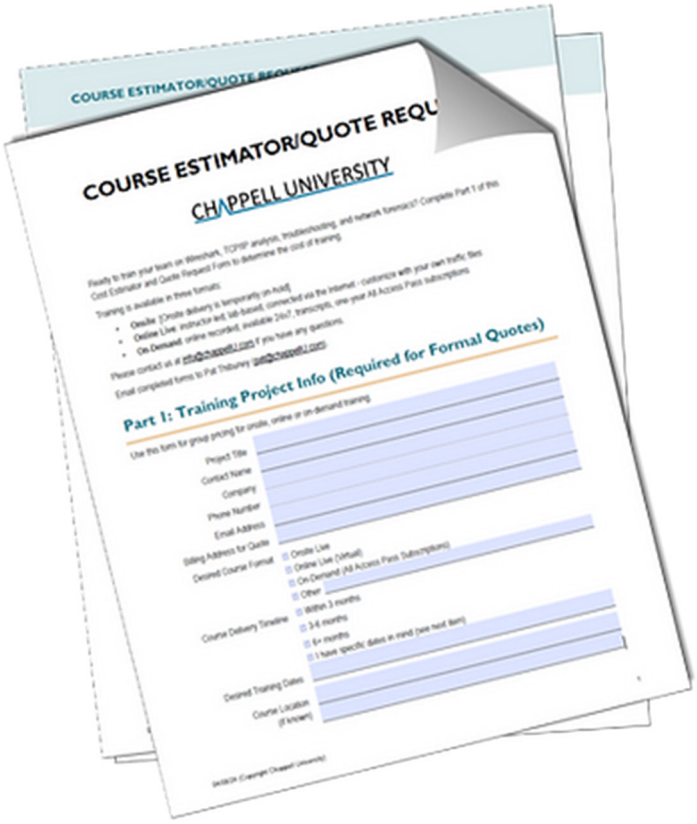
CHAPPELL UNIVERSITY

HOW TO PURCHASE A CUSTOM COURSE

Bring Laura Chappell online or onsite to speed up your team's trobleshooing and forensics processes.

Complete and submit the Course Estimator/Quote Request (Course Designer) document or simply let us know the following:

1. **Course Focus**: Do you want the course to focus on troubleshooting, network forensics, and/or general Wireshark functionality
2. **Course Length**: Minimum course length is 2 days. Laura's maximum course length is 10 days.
3. **Date Range**: Let us know which in which months you'd like the course delivered. We typically need at least 2 months advance preparation time.



Questions? Contact us at info@chappellu.com.