Chappell University™

Network Traffic Analysis and Troubleshooting

Sample 2-Day Course Outline

Coordinator: Brenda Cardinal
brenda@chappellU.com
Phone: +1 408-378-7841
Fax: +1 408-378-7891
Mail: 5339 Prospect Road, #343
San Jose, California 95129 USA

Websites: www.chappellU.com - Chappell University
www.lcuportal2.com - Online Training Portal
www.wiresharkU.com - Wireshark University

Course Description

This course offers hands-on training in network analysis and troubleshooting. This course begins with the core tasks and techniques for TCP/IP analysis (IP, TCP, UDP, ARP, DHCP, HTTP, ICMP and moves into capture and analysis techniques to spot the most common network problems. **Students must provide their own laptops pre-loaded with Wireshark (www.wireshark.org/download).**
Instructor provides traffic analysis trace files for use in hands-on labs (on CD).

Course Syllabus and Estimated Schedule

The schedule listed is tentative and will fluctuate depending on customer's needs and focus during the course.

Course Set Up and Analyzer Testing

1. Network Analysis Overview

1.1. Troubleshooting Tasks for the Network Analyst
1.2. Application Analysis Tasks for the Network Analyst
1.3. Legal Issues Related to Listening to Network Traffic
1.4. Overcome the "Needle in a Haystack" Issue

2. Wireshark Functionality Overview

2.1. Capturing Packets on Wired or Wireless Networks
2.2. How Wireshark Processes Packets – Dissectors, Filters
2.3. Key Wireshark Techniques – Filter/WLAN Toolbar, Status Bar, Profiles, Right-Click

3. Capturing Wired and Wireless Traffic

3.1. Know Where to Tap into the Network – Wired/WLAN, Duplex Issues, Switches
3.2. Infrastructure Effects – NAT/PAT, QoS Routing, VLANs, APs
3.3. Using File Sets and Optimizing for Large Capture Quantity
3.4. Using Default and Custom Capture Filters
3.5. Filter by a Protocol, Address or Host Name

4. Setting Up Your Troubleshooting Profile for Faster Analysis

4.1. Set Global and Personal Configurations
4.2. Use Time to Identify Network Issues
4.3. Customize Your User Interface Settings
4.4. Define Your Capture Preferences
4.5. Define IP and MAC Name Resolution
4.6. Define ARP, TCP, HTTP/HTTPS and Other Protocol Settings
4.7. Use Colors to Distinguish Traffic ("T-" Set of Coloring Rules)

5. Interpret Basic Trace File Statistics to Identify Trends

5.1. Launch Wireshark Statistics for Protocols and Applications
5.2. Identify the Most Active Conversations/Endpoints
5.3. Graphic Flow of Traffic
5.4. Analyze HTTP Statistics

6. Create and Apply Display Filters for Efficient Analysis

6.1. Create Display Filters Using Auto Complete
6.2. Create and Apply Saved Display Filters
6.3. Use Expressions for Filter System
6.4. Combine Display Filters with Comparison Operators
6.5. Avoid Common Display Filter Mistakes

7. Follow Streams and Reassemble Data

7.1. Follow and Reassemble UDP and TCP Conversations
7.2. Identify Common File Types

8. Use Wireshark's Expert System to Identify Anomalies

8.1. Launch Expert Info Quickly
8.2. Filter on TCP Expert Information Elements
8.3. Define TCP Expert Information

9. TCP/IP Analysis Overview

9.1. Define Basic TCP/IP Functionality and the Multistep Resolution Process
9.2. Define Port Number Resolution (Altering Wireshark's Interpretations)
9.3. Define Network Name Resolution (Using Wireshark's *hosts* file)
9.4. Define Route Resolution for a Local Target
9.5. Define Local MAC Address Resolution for a Target (Altering Wireshark's Interpretations)
9.6. Define Route Resolution for a Remote Target
9.7. Define Local MAC Address Resolution for a Gateway (Altering Wireshark's Interpretations)

10. Analyze Common TCP/IP Traffic Patterns

10.1. Analyze Normal/Unusual DNS Queries/Responses
10.2. Analyze Normal/Unusual ARP Requests/Responses
10.3. Analyze Gratuitous ARP
10.4. Analyze Normal/Unusual IPv4 Traffic
10.5. Analyze Normal/Unusual ICMP Traffic
10.6. Dissect the ICMP Packet Structure
10.7. Analyze Normal/Unusual UDP Traffic
10.8. Analyzed Normal/Unusual TCP Communications
10.9. Define the Establishment of TCP Connections
10.10. Define How TCP-based Services Are Refused
10.11. TCP Sequential Packet Tracking
10.12. Define TCP Flow Control
10.13. Analyze TCP Problems
10.14. Set TCP Protocol Parameters
10.15. Analyze Normal/Unusual DHCP Traffic
10.16. Analyze Normal/Unusual HTTP Communications
10.17. Graph HTTP Traffic Flows and Set HTTP Preferences
10.18. Analyze HTTPS Communications

11. Identify the Cause of Network Performance Problems

11.1. Generate Basic and Advanced I/O Graphs
11.2. Analyzing the cause of high latency
11.3. Defining the location of packet loss
11.4. Comparing path throughput for various applications
11.5. Analyzing window size issues
11.6. Identifying intercepting device issues

12. Graph I/O Rates and TCP Trends

12.1. Generate Basic and Advanced I/O Graphs
12.2. Filter I/O Graphs
12.3. Graph Round Trip Time and Throughput Rates
12.4. Interpret TCP Window Size Issues
12.5. Interpret Packet Loss, Duplicate ACKs and Retransmissions

13. Use Command-Line Tools

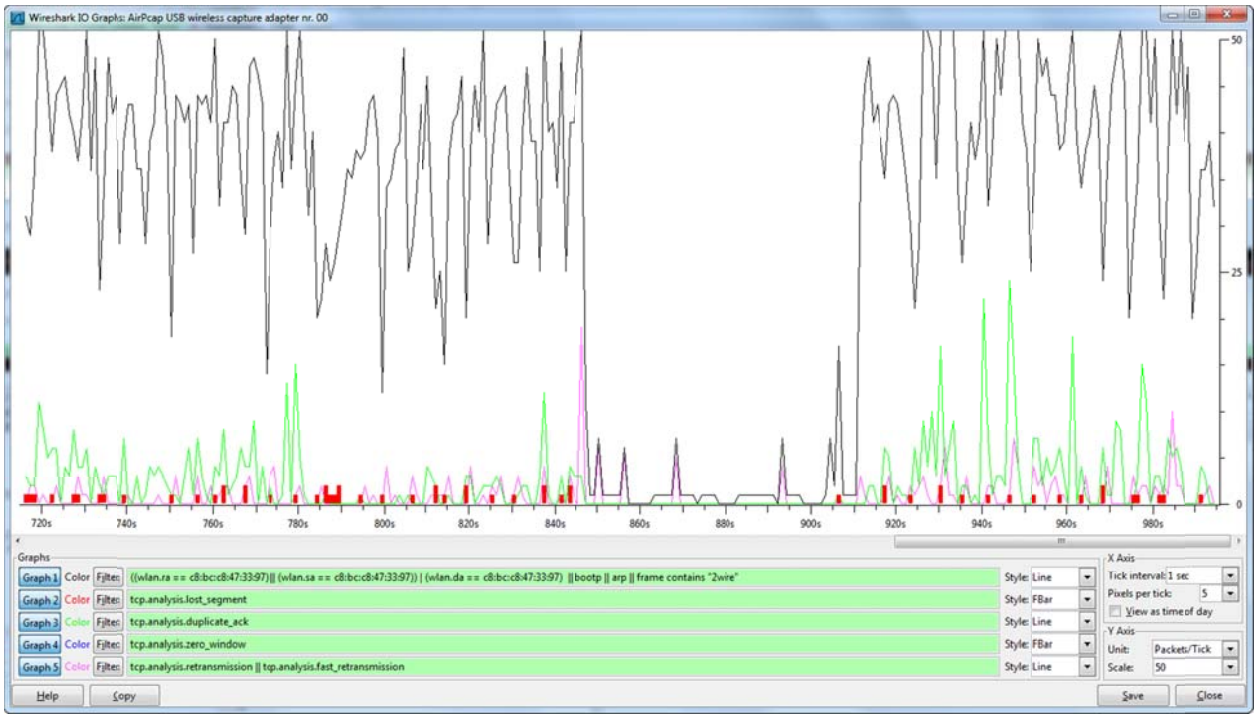
13.1. Command-Line Tool Overview

Course Wrap Up

Course Customization

This course is customized based on the customer's requirements. Ms. Chappell will focus on traffic patterns seen by the customer.

The goal of the course is to teach students a more efficient analysis method for spotting the cause of performance problems using Wireshark's capabilities for capture and analysis.



Training Facility Requirements

Ms. Chappell will need to project her laptop throughout the presentation. Appropriately-sized projection screens should be placed in the room to ensure full visibility of the projected screens. A single projection screen (minimum 12' height) is suggested for smaller audience sizes (less than 50 students); larger and additional projection screens are required for larger audiences. **Inadequate screen visibility for attendees will have a serious negative affect on attendee performance and success.**

In larger venues (typically hosting over 50 attendees), a wireless microphone will be required. Note that wired microphones/stand microphones will *not* work as Ms. Chappell is typing on her keyboard and walking the room through much of the event.

Whiteboards are suggested in smaller venues (hosting less than 50 attendees); they are not used in larger venues.

Please notify Ms. Chappell if she will be joined by assistants for the hearing impaired. Ms. Chappell speaks very quickly and at least two interpreters are suggested for the event.

Laura Chappell, Network Analysis Evangelist

Laura Chappell is a highly-energetic speaker and author of numerous industry titles on network communications, analysis and security. Nicknamed "*Glenda, the Good Witch*," Laura has presented to thousands of State, Federal and international law enforcement officers, judicial members, engineers, network administrators, technicians and developers.

Ms. Chappell is a member of the High Technology Crime Investigation Association (HTCIA) and an Associate Member of the Institute for Electrical and Electronic Engineers (IEEE) since 1989. Ms. Chappell is also a member of the FBI's Infragard organization. Her blend of humor, personal experiences, energy and clarity have earned her a top spot as an industry speaker at Microsoft, Novell, Hewlett-Packard, High Technology Crime Investigation Association and US Court conferences.

Ms. Chappell is the Founder of Chappell University (www.chappellU.com) which develops and delivers onsite and online training in the areas of network protocols, network forensics and network tools.

In 2007, Ms. Chappell founded Wireshark University, an educational firm devoted to teaching the art of wiretapping/communications interception, network forensics, TCP/IP analysis and network troubleshooting.

Laura's network analysis, troubleshooting and security training is available online through the All Access Pass at chappellU.com and through customized online/onsite analysis and training.

Clients Ms. Chappell's client base is global and includes numerous Fortune 100, federal, state and local law enforcement agencies.

- United States Navy
- United States Arsenal
- United States Court of Appeals
- Hong Kong Police Department
- Lockheed Martin
- Cisco Systems
- Dell, Inc.
- IBM Corporation
- Microsoft Corporation
- Sutherland Asbill & Brennan, LLP
- United Bank of Switzerland
- Federal Home Loan Bank of San Francisco
- McAfee Corporation
- Qualcomm Incorporated
- Symantec Corporation
- Riverbed Technologies
- Naval Criminal Investigative Services (NCIS)

- Northern Indiana Power Company
- Microchip Technology, Inc.
- CapitalOne Financial Services
- City of Canberra (Australia)
- Macau Police Department
- Australian High Tech Crime Centre
- Fidelity National Information Services
- City of San Francisco
- … and several unnamed Federal agencies

Conferences Ms. Chappell is consistently a top-rated speaker at numerous industry and private conferences including:

- Microsoft TechEd US
- Microsoft TechEd Europe
- Microsoft TechReady (Internal Technical Conference)
- High Technology Crime Investigation International Conference
- IEEE Regional Conference (California)
- Novell BrainShare Conference
- Novell Advanced Technical Training Conference
- US Courts Technical Training Conference
- United States Secret Service Electronic Crimes Task Force Quarterly Meetings
- OpenSourceWorld/LinuxExpo US
- European Forensics Conference

Publications Ms. Chappell has authored numerous industry titles.

- Wireshark Network Analysis: The Official Wireshark Network Analyst Study Guide *(Chappell University)*
- Wireshark Certified Network Analyst: Official Exam Prep Guide *(Chappell University)*
- Guide to TCP/IP *(Pearson; co-Author Ed Tittel)*
- Introduction to Network Analysis (*podbooks*)
- Network Analysis Case Studies (*podbooks*)
- Introduction to Cisco Router Configuration *(Cisco Press)*
- Advanced Cisco Router Configuration *(Cisco Press)*
- Multiprotocol Internetworking *(Novell Press)*
- NetWare LAN Analysis: IPX/SPX *(Novell Press)*
- Novell's NetWire *(Know, Inc.)*

Contact Information

Coordinator: Brenda Cardinal
brenda@chappellU.com
Phone: +1 408-378-7841
Fax: +1 408-378-7891
Mail: 5339 Prospect Road, #343
San Jose, California 95129 USA

Websites: www.chappellU.com - Chappell University
www.lcuportal2.com - Online Training Portal
www.wiresharkU.com - Wireshark University