Chappell University™

Network Traffic and Security Analysis

Sample 5-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 4.5 day course offers hands-on training in network traffic security analysis and network forensics. This course begins with the core tasks and techniques for TCP/IP analysis (IP, TCP, UDP, ARP, DHCP, HTTP, POP/SMTP, ICMP, VoIP, WLAN 802.11 traffic, WLAN spectrum analysis) and moves into capture and analysis techniques for evidence of reconnaissance and breach patterns on the network.

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 DVD).

Course Syllabus and Estimated Schedule

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

DAY ONE

Course Set Up and Analyzer Testing

1. Network Analysis Overview

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

2. Wireshark Functionality Overview

2.1. Capturing Packets on Wired or Wireless Networks
2.2. Open Various Trace File Types – Wiretap Library
2.3. How Wireshark Processes Packets – Dissectors, Filters
2.4. 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. Options for Remote Capture
3.4. Using File Sets and Optimizing for Large Capture Quantity
3.5. Conserve Memory with Command-line Capture (Tshark, dumpcap)
3.6. Using Default and Custom Capture Filters
3.7. Filter by a Protocol, Address or Host Name
3.8. Advanced Capture Filters (Operators and Byte Offset Filtering)

4. Define Global and Personal Preferences for Faster Analysis

4.1. Set Global and Personal Configurations
4.2. Customize Your User Interface Settings
4.3. Define Your Capture Preferences
4.4. Define IP and MAC Name Resolution
4.5. Define ARP, TCP, HTTP/HTTPS and Other Protocol Settings
4.6. Use Colors to Distinguish Traffic
4.7. Marking Packets of Interest

5. Defined Time Values and Interpret Summaries

5.1. Use Time to Identify Network Issues
5.2. Create Additional Time Columns

6. Interpret Basic Trace File Statistics to Identify Trends

6.1. Launch Wireshark Statistics for Protocols and Applications
6.2. Identify the Most Active Conversations/Endpoints
6.3. List Endpoints and Map Them on the OpenStreetMap
6.4. List Conversations or Endpoints for Specific Traffic Types
6.5. List All UDP and TCP Ports Used
6.6. Graphic Flow of Traffic
6.7. Analyze HTTP Statistics
6.8. Analyze WLAN Statistics

7. Create and Apply Display Filters for Efficient Analysis

7.1. Create Display Filters Using Auto Complete
7.2. Create and Apply Saved Display Filters
7.3. Use Expressions for Filter System
7.4. Combined Display Filters with Comparison Operators
7.5. Alter Display Filter Meaning with Parentheses
7.6. Filter on Specific Bytes in a Packet
7.7. Use Display Filter Macros for Complex Filtering
7.8. Avoid Common Display Filter Mistakes
7.9. Manually Edit the *dfilters* File

DAY TWO

8. Follow Streams and Reassemble Data

8.1. Follow and Reassemble UDP and TCP Conversations
8.2. Identify Common File Types
8.3. Follow and Reassemble SSL Conversations

9. Use Wireshark's Expert System to Identify Anomalies

9.1. Launch Expert Info Quickly
9.2. Colorize Expert Info Elements
9.3. Filter on TCP Expert Information Elements

9.4. Define TCP Expert Information

10. TCP/IP Analysis Overview

10.1. Define Basic TCP/IP Functionality
10.2. Define the Multistep Resolution Process
10.3. Define Port Number Resolution
10.4. Define Network Name Resolution
10.5. Define Route Resolution for a Local Target
10.6. Define Local MAC Address Resolution for a Target
10.7. Define Route Resolution for a Remote Target
10.8. Define Local MAC Address Resolution for a Gateway

11. Analyze Common TCP/IP Traffic Patterns

11.1. Analyze Normal/Unusual DNS Queries/Responses
11.2. Analyze Normal/Unusual ARP Requests/Responses
11.3. Analyze Gratuitous ARP
11.4. Dissect the ARP Packet Structure
11.5. Analyze Normal/Unusual IPv4 Traffic
11.6. Set Your IP Protocol Preferences
11.7. Analyze Normal/Unusual ICMP Traffic
11.8. Dissect the ICMP Packet Structure
11.9. Analyze Normal/Unusual UDP Traffic
11.10. Analyzed Normal/Unusual TCP Communications
11.11. Define the Establishment of TCP Connections
11.12. Define How TCP-based Services Are Refused
11.13. TCP Sequential Packet Tracking
11.14. Define TCP Flow Control
11.15. Analyze TCP Problems
11.16. Set TCP Protocol Parameters
11.17. Analyze Normal/Unusual DHCP Traffic
11.18. Analyze Normal/Unusual HTTP Communications
11.19. Filter on HTTP or HTTPS Traffic
11.20. Export and Display HTTP Objects
11.21. Graph HTTP Traffic Flows and Set HTTP Preferences
11.22. Analyze HTTPS Communications
11.23. Decrypt HTTPS Traffic
11.24. Analyze Normal/Unusual FTP Communications
11.25. Reassemble FTP Data Transfers
11.26. Analyze Normal/Unusual Email Communications

DAY THREE

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. 802.11 (WLAN) Analysis Fundamentals

13.1. Analyze Signal Strength and Interference
13.2. Capture WLAN Traffic - Compare Monitor Mode and Promiscuous Mode
13.3. Set up WLAN Decryption
13.4. Prepend a Radiotap or PPI Header
13.5. Compare Signal Strength and Signal-to-Noise Ratios
13.6. Describe 802.11 Traffic Basics
13.7. Analyzed Normal 802.11 Communications
13.8. Filter on All WLAN Traffic
13.9. Analyze Frame Control Types and Subtypes

14. Voice over IP (VoIP) Analysis Fundamentals

14.1. Define VoIP Traffic Flows and Analyze VoIP Problems
14.2. Examine SIP and RTP Traffic
14.3. Play Back VoIP Calls
14.4. Create a VoIP Profile and VoIP Filters

15. Network Forensics Fundamentals

15.1. Gather Packet Evidence
15.2. Methods for Avoiding Detection
15.3. Recognize Unusual Traffic Patterns
15.4. Color Unusual Traffic Patterns
15.5. Check out Complementary Forensic Tools

DAY FOUR

16. Detect Scanning and Discovery Processes

16.1. Detect ARP Scans (aka ARP Sweeps)
16.2. Detect ICMP Ping Sweeps
16.3. Detect Various Types of TCP Port Scans
16.4. Detect UDP Port Scans
16.5. Detect IP Protocol Scans
16.6. Define Idle Scans
16.7. Know Your ICMP Types and Codes
16.8. Analyze Traceroute Path Discovery
16.9. Detect Dynamic Router Discovery

16.10. Define Application Mapping Processes
16.11. Use Wireshark for Passive OS Fingerprinting
16.12. Detect Active OS Fingerprinting
16.13. Identify Spoofed Addresses and Scans

17. Analyze Suspect Traffic

17.1. Describe What Is Suspect Traffic
17.2. Identify Vulnerabilities in the TCP/IP Resolution Processes
17.3. Identify Unacceptable Traffic
17.4. Find Maliciously Malformed Packets
17.5. Identify Invalid or Dark Destination Addresses
17.6. Differentiate between Flooding or Standard Denial of Service Traffic
17.7. Find Clear Text Passwords and Data
17.8. Identify Phone Home Behavior
17.9. Catch Unusual Protocols and Applications
17.10. Locate Route Redirection That Uses ICMP
17.11. Catch ARP Poisoning
17.12. Catch IP Fragmentation and Overwriting
17.13. Spot TCP Splicing
17.14. Watch Other Unusual TCP Traffic
17.15. Identify Password Cracking Attempts
17.16. Know Where to Look: Signature Locations

DAY FIVE

18. Use Command-Line Tools

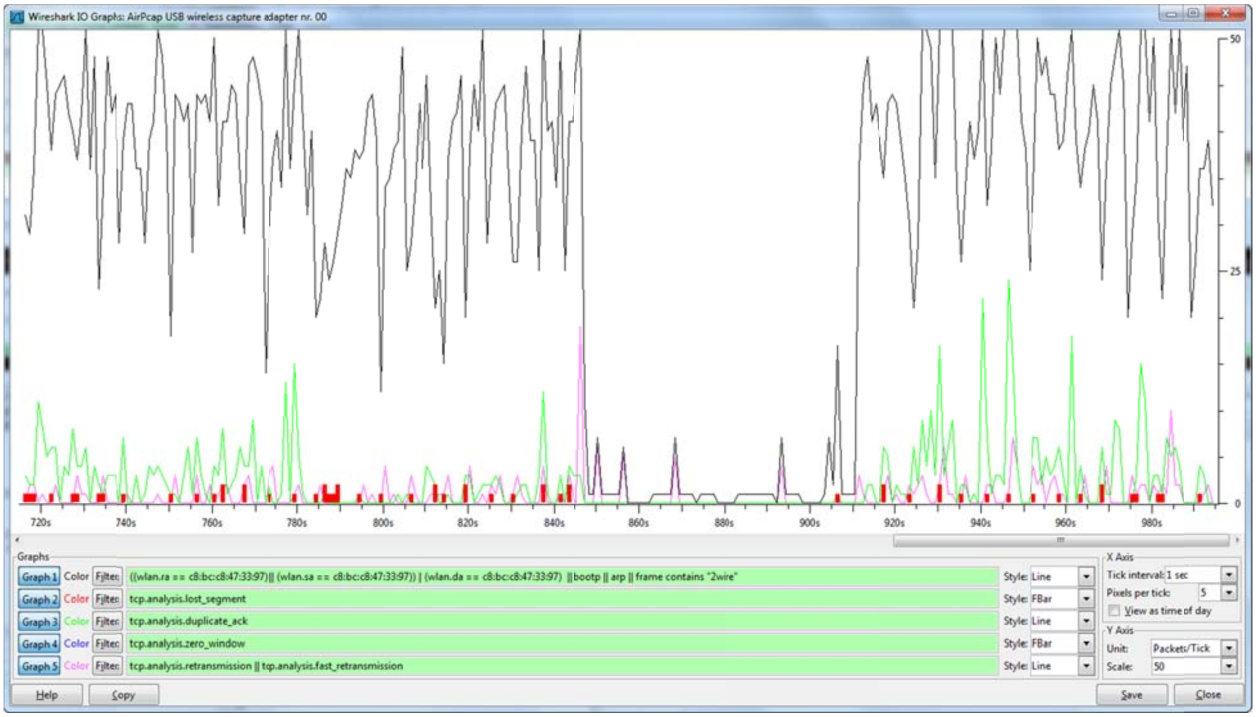
18.1. Use Wireshark.exe (Command-Line Launch)
18.2. Capture Traffic with Tshark
18.3. List Trace File Details with Capinfos
18.4. Edit Trace Files with Editcap
18.5. Merge Trace Files with Mergecap
18.6. Convert Text with Text2pcap
18.7. Capture Traffic with Dumpcap

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.



Wireshark IO Graphs: AirPcap USB wireless capture adapter nr. 00

Graphs

Graph 1 Color Filter: ((wlan.ra == c8:bc:c8:47:33:97)|| (wlan.sa == c8:bc:c8:47:33:97)) | (wlan.da == c8:bc:c8:47:33:97) ||bootp || arp || frame contains "2wire" Style: Line

Graph 2 Color Filter: tcp.analysis.lost_segment Style: FBar

Graph 3 Color Filter: tcp.analysis.duplicate_ack Style: Line

Graph 4 Color Filter: tcp.analysis.zero_window Style: FBar

Graph 5 Color Filter: tcp.analysis.retransmission || tcp.analysis.fast_retransmission Style: Line

X Axis

Tick interval: 1 sec

Pixels per tick: 5

☐ View as time of day

Y Axis

Unit: Packets/Tick

Scale: 50

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.

WIRESHARK UNIVERSITY

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