

Chappell University™

All Access Pass Course List

May 2011



List of Courses

Syllabus for 'AAP-Core 1-Wireshark Functions & TCP/IP'	1
Syllabus for 'AAP-Core 2-Troubleshoot/Secure Networks with Wireshark'	2
Syllabus for 'AAP-CS41 Wireshark Jumpstart 101'	3
Syllabus for 'AAP-CS42 Hacked Hosts'	4
Syllabus for 'AAP-CS43 Analyze and Improve Throughput'	5
Syllabus for 'AAP-CS44 Top 10 Reasons Your Network is Slow'	6
Syllabus for 'AAP-CS45 TCP Analysis In-Depth'	7
Syllabus for 'AAP-CS46 DHCP/ARP Analysis'	8
Syllabus for 'AAP-CS47 Nmap Network Scanning 101'	9
Syllabus for 'AAP-CS50 WLAN Analysis 101'	10
Syllabus for 'AAP-CS52 Wireshark 201 Filtering'	11
Syllabus for 'AAP-CS53 New Wireshark 1.4 Features'	12
Syllabus for 'AAP-CS54 ICMP Analysis'	13
Syllabus for 'AAP-CS55 Analyzing Google Secure Search'	14
Syllabus for 'AAP-CS56 Slow Networks - NOPs/SACK'	15
Syllabus for 'AAP-CS57 TCP Vulnerabilities (MS09-048)'	16
Syllabus for 'AAP-CS58 Packet Crafting to Test Firewalls'	17
Syllabus for 'AAP-CS59 Capturing Packets (Security Focus)'	18
Syllabus for 'AAP-CS60 Troubleshooting with Coloring'	19
Syllabus for 'AAP-CS61 Tshark Command-Line Capture'	20
Syllabus for 'AAP Event: Analyzing the Window Zero Condition'	21
Syllabus for 'Trace File Analysis - Set 1'	22
Syllabus for 'Trace File Analysis - Set 2'	23
Syllabus for 'Trace File Analysis - Set 3'	24
Syllabus for 'Whiteboard Lecture Series 1'	25

Syllabus for 'AAP-Core 1-Wireshark Functions & TCP/IP'

Purchase an All Access Pass (1 Year Subscription) to access this module.

In this self-based lab-intensive course, you will discover effective Wireshark operations and packet-level TCP/IP communications by examining both properly and poorly performing networks as you prepare for the Wireshark Certification Exam. One-half of this class focuses on the features of Wireshark, the world's most popular analyzer. After that, this course focuses on reviewing both the normal and abnormal communication patterns of the TCP/IP suite and most common applications, including DHCP, DNS, FTP, Telnet, HTTP, POP, and SMTP. With a strong emphasis on hands-on lab exercises and real-world case studies in this course, you'll gain skills that can be used immediately following the class.

Instructor:

Laura A. Chappell

Sections:

- | | |
|---|---------------------|
| 1: Course Introduction | 17: IPv4 Analysis |
| 2: Introduction to Wireshark | 18: ICMP Analysis |
| 3: Capture Filters | 19: UDP Analysis |
| 4: Global Configuration Preferences | 20: TCP Analysis |
| 5: Navigate and Colorize | 21: DHCP Analysis |
| 6: Time Values and Summaries | 22: HTTP Analysis |
| 7: Basic Statistics | 23: Telnet Analysis |
| 8: Advanced Statistics | 24: FTP Analysis |
| 9: Display Filters | 25: POP Analysis |
| 10: Save and Export | 26: SMTP Analysis |
| 11: Expert Info and Miscellaneous Tasks | 27: Labs 1-10 |
| 12: Command Line Tools | 28: Labs 11-20 |
| 13: Course Labs | 29: Labs 21-30 |
| 14: TCP/IP Flows | 30: Labs 31-40 |
| 15: DNS Analysis | 31: Labs 41-46 |
| 16: ARP Analysis | |

Guides:

- 1: Core 1 Lab Workbook
- 2: Trace File Log Book
- 3: Wireshark Accelerators Quick Reference
- 4: Core 1 Trace Files
- 5: Core 1 Exam Information

Tests:

- 1: Course Exam - Core 1 AAP

Syllabus for 'AAP-Core 2-Troubleshoot/Secure Networks with Wireshark'

Purchase an All Access Pass (1 Year Subscription) to access this module.

In this self-based lab-intensive course, you will discover effective Wireshark techniques for troubleshooting and securing networks by examining both properly and poorly performing networks, trace file evidence of reconnaissance processes and evidence of breached security. With a strong emphasis on hands-on lab exercises and real-world case studies in this course, you'll gain skills that can be used immediately following the class.

Instructor:

Laura A. Chappell

Sections:

- | | |
|---------------------------------------|---------------------------------|
| 1: Course Introduction | 14: Reconnaissance Processes |
| 2: Analysis Overview | 15: Analyzing ICMP Traffic |
| 3: Normal Network Communications | 16: TCP Security |
| 4: Causes of Performance Problems | 17: Address Spoofing |
| 5: Functions for Troubleshooting | 18: Building Firewall ACL Rules |
| 6: Latency Issues | 19: Signatures of Attacks |
| 7: Packet Loss and Retransmissions | 20: Additional Security Labs |
| 8: Misconfigurations and Redirections | 21: Labs 1-10 |
| 9: Dealing with Congestion | 22: Labs 11-20 |
| 10: Baselining Network Communications | 23: Labs 21-30 |
| 11: Additional Troubleshooting Labs | 24: Labs 31-40 |
| 12: Setting Up Your Security Lab | 25: Labs 41-50 |
| 13: Unusual Network Communications | 26: Labs 51-53 |

Guides:

- 1: Core 2 Lab Workbook
- 2: Trace File Log Book
- 3: Wireshark Accelerator Quick Reference
- 4: Core 2 Trace Files
- 5: Core 2 Exam Information

Tests:

- 1: Course Exam - Core 2 AAP

Syllabus for 'AAP-CS41 Wireshark Jumpstart 101'

Purchase an All Access Pass (1 Year Subscription) to access this module.

Bonus: Laura's Capture, Display and Color Filter sets plus video instructions on creating a "Laura's Stuff" profile and importing these files. Over 7,000 people have registered to attend this class live. Now you can take it anytime. This is the ideal class to get your feet wet with Wireshark - learn where and how to tap into network traffic, the two types of filters used to focus on network traffic, the basic layout of the Wireshark configuration, how Wireshark does what it does - dissectors, engine and graphing. Laura works with Wireshark to show you how to quickly spot network problems using Wireshark's Expert Info Composite and specific Time Column settings. Get up to speed fast on Wireshark's capabilities and begin troubleshooting and optimizing your networks today!

Instructor:

Laura A. Chappell

Sections:

- | | |
|-----------------------------|--|
| 1: Introduction | 12: Capture Options |
| 2: Capturing Traffic | 13: Working with Profiles and Time |
| 3: Processing Packets | 14: Display Filters |
| 4: Key Tasks | 15: Expert Infos Composite |
| 5: Placing the Analyzer | 16: Graphing Traffic |
| 6: Full-Duplex Tapping | 17: Reassemble Streams |
| 7: Port Spanning | 18: Capture Filters in the Default Profile |
| 8: Wireless Capture Options | 19: Command-Line Tools |
| 9: Spectrum Analysis Demo | 20: Your To-Do List |
| 10: Key Wireshark Functions | 21: Bonus Materials |
| 11: Choosing the Interface | |

Guides:

- 1: CS41 Course Handouts
- 2: CS41 Wireshark Configuration Guides
- 3: CS41 Trace Files

Syllabus for 'AAP-CS42 Hacked Hosts'

Purchase an All Access Pass (1 Year Subscription) to access this module.

Network forensics comes into play in this online course by Laura Chappell. Based on numerous trace files of breached hosts, Ms. Chappell explains the first steps to identifying suspect traffic patterns. How do you identify a breached host? What are the signs that a bot has invaded your network? How can you find IRC traffic running over port 80, or 25, or 21? What is the first step to dealing with a compromised machine? This online course will get you up to speed on the top items to look for when analyzing the security of your network through network forensics.

Instructor:

Laura A. Chappell

Sections:

- | | |
|---------------------------------------|--|
| 1: Introduction | 9: Reconnaissance - Application Scans |
| 2: Network Forensics Overview | 10: Filtering for OS Fingerprinting |
| 3: Tools and Tap-In Points | 11: Analyzing a Nessus Scan |
| 4: Reconnaissance - TCP Scans | 12: Evidence of a Breached Host |
| 5: Reconnaissance - UDP Scans | 13: Analyzing Macof Traffic |
| 6: Reconnaissance - IP Scans | 14: Analyzing a Bot-Infected Host |
| 7: Reconnaissance - OS Fingerprinting | 15: Analyzing Another Breached Host |
| 8: Reconnaissance - Address Scans | 16: Other Questionable Traffic (P2P/Games) |

Guides:

- 1: CS42 Course Handouts
- 2: CS42 Trace Files

Syllabus for 'AAP-CS43 Analyze and Improve Throughput'

Purchase an All Access Pass (1 Year Subscription) to access this module.

What are the main factors affecting throughput and how can you pinpoint why your throughput is so low? How do you take a quick snapshot of round trip latency times? What about graphing out the round trip times calculated from traffic captured? How do you use the BDP calculation to determine the ideal TCP receive buffer size? How does the network recover from packet loss on UDP and TCP networks? How does Selective ACK help ease the pain of packet loss? How can you tell if queuing along a path is affecting performance? Laura examines numerous trace files from low-throughput networks and performs some live throughput tests during this detailed training course.

This course includes live trace file analysis, latency testing and throughput tests using Wireshark, iPerf and NetScanTools Pro.

Instructor:

Laura A. Chappell

Sections:

- | | |
|---|---|
| 1: Introduction | 8: TCP Recovery with SACK |
| 2: Packet Loss - How Bad Is It? | 9: Latency - What Affects It |
| 3: TCP Flow Control | 10: Wireshark Analysis of Packet Loss/Latency |
| 4: UDP - In the Hands of the Developers | 11: Latency Types and Causes |
| 5: Tools of the Trade | 12: Window Zero Condition |
| 6: Traceroute/Ping for Path Discovery | 13: iPerf Throughput Testing/Graphing |
| 7: NetScanTools Graphical Ping/Traceroute | |

Guides:

- 1: CS43 Course Handouts
- 2: CS43 Trace File

Syllabus for 'AAP-CS44 Top 10 Reasons Your Network is Slow'

Purchase an All Access Pass (1 Year Subscription) to access this module.

Network monitoring helps discover the cause of slow network performance. Using Wireshark to monitor network communications, Laura Chappell demonstrates network traffic on poorly performing networks. Save yourself hours of research by getting the inside tips and tricks on locating the cause of network problems. From bandwidth monitoring and latency monitoring to packet loss and wireless network interference, this online course is worth your time to attend.

Instructor:

Laura A. Chappell

Sections:

- | | |
|-------------------------------------|---|
| 1: Introduction | 8: Inside Window Scaling Issues |
| 2: The Top 10 List | 9: Analyzing a Zero Window Condition |
| 3: TCP vs. UDP Packet Loss/Recovery | 10: Examining Network Design Issues |
| 4: Analyzing Packet Loss/Latency | 11: Prioritization of Traffic |
| 5: Graphing Throughput Problems | 12: Examining Interference/Noise (WLAN) |
| 6: Packet Loss and Expert Info | 13: Timing Problems |
| 7: Latency Lab Results | 14: User Issues |

Guides:

- 1: CS44 Course Handouts
- 2: CS44 Trace Files
- 3: CS44 Chanalyzer Recording

Syllabus for 'AAP-CS45 TCP Analysis In-Depth'

Purchase an All Access Pass (1 Year Subscription) to access this module.

TCP is the basic communication used for most important network traffic - web browsing, database access, email, file transfers, etc. In this course, Laura takes you through various trace files of normal and abnormal TCP communications and explains the handshake process, TCP options, window size, packet loss and recovery, selective ACKs, timeouts, session tear down processes and TCP reassembly. Laura shows graphs of TCP traffic that 'scream the story' of why communications are so lousy.

Instructor:

Laura A. Chappell

Sections:

- | | |
|--|---------------------------------------|
| 1: Introduction | 8: TCP Sliding Window |
| 2: TCP Functionality | 9: TCP Service Refusal |
| 3: TCP Packet Structure | 10: TCP Window Scaling |
| 4: TCP Handshake Problems | 11: TCP Selective Acknowledgments |
| 5: TCP Options | 12: TCP Latency Issues |
| 6: Filtering on TCP Traffic | 13: Graphing TCP Traffic |
| 7: TCP Sequence/Acknowledgment Process | 14: Analyzing a Window Zero Condition |

Guides:

- 1: CS45 Course Handouts
- 2: CS45 Trace Files

Syllabus for 'AAP-CS46 DHCP/ARP Analysis'

Purchase an All Access Pass (1 Year Subscription) to access this module.

Accelerate your learning speed by watching Laura open and analyze a series of trace files. In this course Laura concentrates on the typical startup sequence of a host and analyzes the DHCP process and the gratuitous ARP process. Laura explains the various options seen in DHCP bootup processes - including the use of DHCP Relay Agents and methods to filter on various DHCP packet fields. In examining ARP traffic, Laura shows how ARP can be used to discover firewalled local devices and what an ARP scan looks like on the network.

Instructor:

Laura A. Chappell

Sections:

- | | |
|-----------------------------------|-------------------------------------|
| 1: Introduction | 11: Analyze a Slow DHCP Server |
| 2: Overview of DHCP | 12: Other DHCP Filtering |
| 3: DHCP Packet Structure Overview | 13: Relay Agent Traffic |
| 4: DHCP Bootup Sequence | 14: DHCP Declines |
| 5: DHCP Packet Structure Analysis | 15: Overview of ARP |
| 6: DHCP Options | 16: ARP Filtering/Packet Structures |
| 7: DHCP Offer Process | 17: Analyzing Unusual ARP Traffic |
| 8: DHCP Filtering | 18: ARP Poisoning Analysis |
| 9: Analyze a DHCP Problem | 19: Weird ARP |
| 10: Renewal and Rebind Process | |

Guides:

- 1: CS46 Course Handouts
- 2: CS46 Trace Files

Syllabus for 'AAP-CS47 Nmap Network Scanning 101'

Purchase an All Access Pass (1 Year Subscription) to access this module.

It's time to get a handle on that tangled mess you call a network! Oh... and let's do it on a budget, ok? No... this isn't a drug-induced fantasy - Laura will show you methods for scanning your network using OS fingerprinting and service scans to identify the types of hosts running and their services. Her weapon of choice in this online course will be Nmap/Zenmap. This course includes live mapping processes of remote and local hosts, OS fingerprinting, service discovery and graphing of network devices using Nmap.

Instructor:

Laura A. Chappell

Sections:

- | | |
|--------------------------------|--------------------------------------|
| 1: Introduction | 11: Zenmap Topology Controls |
| 2: Methods of Mapping | 12: Review an Interesting Scan |
| 3: Mapping Tools | 13: TCP Scan Variations |
| 4: Passive Discovery Processes | 14: Nmap Results |
| 5: Active Discovery Processes | 15: IP Scan Process |
| 6: ARP vs. Ping Scan | 16: Topology View/nmap-services File |
| 7: Nmap Regular Scan | 17: Optimizing Your Scans |
| 8: Nmap Demo | 18: Analysis of Nmap Scan Traffic |
| 9: Import/Run Nmap Scans | 19: Relaunching a Scan |
| 10: Intense Nmap Scan | 20: Analyzing More Nmap Scans |

Guides:

- 1: CS47 Course Handouts
- 2: CS47 Nmap Cheat Sheet
- 3: CS47 Intense Scan with UDP (XML File)
- 4: CS47 Trace Files

Syllabus for 'AAP-CS50 WLAN Analysis 101'

Purchase an All Access Pass (1 Year Subscription) to access this module.

In this course Laura begins from the ground up - beginning with a demonstration of Chanalyzer and the Wi-Spy Adapter used to identify WLAN signal strength and interference. Next, Laura takes you into the world of capturing WLAN traffic using Wireshark - explaining the purpose of the AirPcap adapters and the set-up process to capture and aggregate traffic on multiple channels, create a WLAN-specific profile for the two types of WLAN headers (Radiotap and PPI). You'll learn the tricks to identify the types of WLAN traffic and apply decryption methods to the traffic.

Instructor:

Laura A. Chappell

Sections:

- | | |
|-------------------------------|-------------------------------------|
| 1: Introduction | 7: 802.11 Frame Basics (Overview) |
| 2: WLAN Basics | 8: Create a WLAN Profile |
| 3: WLAN Analysis Elements | 9: Filter and Graph on Type/Subtype |
| 4: Signal Strength and Noise | 10: Analyze WLAN Problems |
| 5: Capturing WLAN Traffic | 11: WLAN Throughput Testing |
| 6: WLAN Setup Recommendations | 12: Course Supplements Information |

Guides:

- 1: CS50 Course Handouts
- 2: CS50 Course Supplements (ZIP)

Syllabus for 'AAP-CS52 Wireshark 201 Filtering'

Purchase an All Access Pass (1 Year Subscription) to access this module.

Learn how Wireshark applies capture and display filters, what filters you might use in various situations, where the capture/display filter files are kept, how to create numerous hot filters including coloring filters.

Instructor:

Laura A. Chappell

Sections:

- | | |
|---|---|
| 1: Introduction | 11: Creating New Display Filters |
| 2: Processing Packets (Networks vs. File | 12: Setting Display Filter Preferences |
| 3: Capture Filter List | 13: Create Conversation Display Filters |
| 4: Capture Filter Examples | 14: Using Display Filters as Coloring Rules |
| 5: Capture Filter File Editing | 15: Display Filters on Protocol Hierarchy |
| 6: Create, Apply and Save Capture Filters | 16: Using Expression... |
| 7: My MAC/Not My MAC Capture Filters | 17: Using Auto-Complete |
| 8: Display Filtering Methods | 18: Follow Streams and Use Find |
| 9: Common Filter Mistakes | 19: Tshark with Filtering |
| 10: Viewing Saved Display Filters | 20: Your To Do List |

Guides:

- 1: CS52 Course Handouts

Syllabus for 'AAP-CS53 New Wireshark 1.4 Features'

Purchase an All Access Pass (1 Year Subscription) to access this module.
This course covers the new features of Wireshark version 1.4.

Instructor:

Laura A. Chappell

Sections:

- 1: Introduction
- 2: Development Process/Sites
- 3: New Features List
- 4: New Features Demo

Guides:

- 1: CS53 Course Handouts

Syllabus for 'AAP-CS54 ICMP Analysis'

Purchase an All Access Pass (1 Year Subscription) to access this module.

Laura explains the newest dissector for ICMP traffic (including LE/BE designations), what types of ICMP traffic you DON'T want to see and how to create three must-have butt-ugly color filters to identify suspect ICMP traffic.

Instructor:

Laura A. Chappell

Sections:

- | | |
|-------------------------------|---|
| 1: Introduction | 8: ICMP Redirect Analysis |
| 2: ICMP Definition | 9: ICMP Router Solicitation Analysis |
| 3: Capturing ICMP Traffic | 10: ICMP Destination Unreachable Analysis |
| 4: ICMP Packet Structures | 11: Analyzing ICMP in a Penetration Test |
| 5: ICMP Type and Code Numbers | 12: ICMP Traffic of Concern |
| 6: ICMP Ping Analysis | 13: Butt-Ugly Coloring Rules for ICMP |
| 7: ICMP Traceroute Analysis | |

Guides:

- 1: CS54 Course Handouts

Syllabus for 'AAP-CS55 Analyzing Google Secure Search'

Purchase an All Access Pass (1 Year Subscription) to access this module.

This course analyzes a standard Google search (<http://www.google.com>) and then looks at the communications during a "Google Secure Search" (announced in 2010). Key features of Google's Secure Search were touted as "encrypted searches" and no REFER information being passed on to the target site. We examine the traffic to see if we can really hide our search terms and not let the target know from whence we came. Interesting.

Instructor:

Laura A. Chappell

Sections:

- | | |
|---|--------------------------------------|
| 1: Introduction | 6: Capturing/Marking the Traffic |
| 2: Google HTTP Traffic Analysis | 7: Analyzing the Results |
| 3: Google HTTPS Traffic Analysis | 8: Analyzing Clicks on a Cached Page |
| 4: What about Cached Links in Secure Search | 9: Do It Yourself |
| 5: Set Up Wireshark for Capture | |

Guides:

- 1: Google Search Trace Files (ZIP)

Syllabus for 'AAP-CS56 Slow Networks - NOPs/SACK'

Purchase an All Access Pass (1 Year Subscription) to access this module.

Learn how 4 NOPs indicate problems with interconnecting devices and create traffic problems. Includes TCP Options analysis and creation of a "4 NOPs" butt-ugly coloring rule.

Instructor:

Laura A. Chappell

Sections:

- | | |
|---------------------------------|---|
| 1: Introduction | 5: Interpreting TCP Option Values/Lengths |
| 2: What is a NOP | 6: Example of NOP Problem |
| 3: Options in the TCP Handshake | 7: Identifying a SACK Problem |
| 4: TCP Options List | 8: 4 NOP Butt-Ugly Coloring Rule |

Syllabus for 'AAP-CS57 TCP Vulnerabilities (MS09-048)'

Purchase an All Access Pass (1 Year Subscription) to access this module.

This course covers the TCP vulnerabilities announced by Microsoft - MS09-048. You need to know that one of the vulnerabilities affects Cisco, Linux, OpenBSD, and more – it's not just a Microsoft issue. The video shows you what the vulnerabilities are based on and how to create Wireshark filters (display and color filters) to see problem communications easier. There are trace files in the Course Guides section. I reference the Recorded Wireshark Jumpstart + Bonus (you all have access to that course - CS41 - as part of your membership. The profile included with that video will already catch 2 of the 3 DoS attacks listed in MS09-048.

Instructor:

Laura A. Chappell

Sections:

- 1: Introduction
- 2: CVE 2008-4609
- 3: CVE 2009-1925
- 4: CVE 2009-1926

Guides:

- 1: CS57 Trace Files

Syllabus for 'AAP-CS58 Packet Crafting to Test Firewalls'

Purchase an All Access Pass (1 Year Subscription) to access this module.

Learn to use a seed packet, edit the packet contents, reply the packet on the network, capture the packet in Wireshark and locate it quickly using a color filter in Wireshark. (Tools: Wireshark, Colasoft Packet Builder, NetScanTools Pro).

Instructor:

Laura A. Chappell

Sections:

- | | |
|---|--|
| 1: Introduction | 5: Building a Malicious Packet |
| 2: Why Learn Packet Crafting | 6: Send and Test Your Malicious Packet |
| 3: About SMB Versions and Compatibility | 7: Other Packet Crafting Tools |
| 4: The Test Scenario | |

Guides:

- 1: CS58 Course Handouts
- 2: CS58 Packet Builder Application

Syllabus for 'AAP-CS59 Capturing Packets (Security Focus)'

Purchase an All Access Pass (1 Year Subscription) to access this module.

CS59 - Capturing Packets (Security Focus) is based on the Jumpstart 101 Course (CS41), this course takes a security angle to packet capture including information on capturing in stealth mode.

Instructor:

Laura A. Chappell

Sections:

- | | |
|--|--|
| 1: Course Introduction | 8: Examining the Interfaces (Wired/Wireless) |
| 2: Security Tasks for Network Analysts | 9: Setting a Capture Filter |
| 3: Where to Tap In | 10: Capturing the Traffic |
| 4: Wireshark Info and Reading the Code | 11: Graphing the Traffic |
| 5: Capturing Traffic vs. Opening Trace Files | 12: Creating a Profile |
| 6: Capturing on a Switched Network | 13: Working with Display Filters |
| 7: Wireless Capture Options | 14: Saving Displayed Traffic |

Guides:

- 1: CS59 Course Handouts

Syllabus for 'AAP-CS60 Troubleshooting with Coloring'

Purchase an All Access Pass (1 Year Subscription) to access this module.

Learn to speed up your troubleshooting processes by coloring packets of interest. In this course, Laura goes through the fundamentals of coloring in Wireshark and gives you numerous examples of coloring rules you absolutely must have.

Instructor:

Laura A. Chappell

Sections:

- | | |
|--|-------------------------------|
| 1: Course Introduction | 6: Sample Coloring Rules |
| 2: Default Coloring Rules | 7: Coloring Rules in Profiles |
| 3: Disable Coloring Rules | 8: Edit the Colorfilters File |
| 4: Conversation Coloring | 9: Share Coloring Rules |
| 5: Add Coloring Rules - Best Practices | |

Guides:

- 1: CS60 Course Handouts
- 2: CS60 Trace Files

Syllabus for 'AAP-CS61 Tshark Command-Line Capture'

Purchase an All Access Pass (1 Year Subscription) to access this module.

Learn to use Tshark - Wireshark's command-line capture tool. This course covers interface selection, saving to file sets, using the ring buffer, filtering traffic, viewing traffic statistics and exporting specific field information.

Instructor:

Laura A. Chappell

Sections:

- | | |
|---|---|
| 1: Introduction | 8: Display Filters and Infile Definitions |
| 2: Why Use Tshark | 9: Name Resolution Options |
| 3: Tshark Setup | 10: Tshark Statistics |
| 4: Tshark Help and Interface Listing | 11: Examples to Try |
| 5: Interface, Capture Filter and Output | 12: Extracting Field Information |
| 6: Capture Size and Autostop | 13: Tshark Questions |
| 7: Creating File Sets/Using a Ring Buffer | |

Syllabus for 'AAP Event: Analyzing the Window Zero Condition'

Purchase an All Access Pass (1 Year Subscription) to access this module.

This recording is based on the AAP Live Event that took place on March 16, 2011. In this course you will analyze three trace files depicting Window Zero conditions. You will learn that even small window sizes can stop network data flow and how to find those issues quickly with a coloring rule. Finally, Laura takes you into the packet-tcp.c dissector to view each of the Expert Info notifications regarding window size issues.

Instructor:

Laura A. Chappell

Syllabus for 'Trace File Analysis - Set 1'

Purchase an All Access Pass (1 Year Subscription) to access this module.

Watch Laura analyze various traffic patterns including:

- honeypots attacking each other
- a printing problem
- illegal source IP address
- someone sneaking traffic through the network
- a network scan
- a lousy hotel network
- ARP process during a bootup sequence
- ARP used to ping a local host
- ARP used for discovery
- bruteforce password cracking

This class includes the trace files (click the Documents button on the icon toolbar) for you to practice on!

Instructor:

Laura A. Chappell

Syllabus for 'Trace File Analysis - Set 2'

Purchase an All Access Pass (1 Year Subscription) to access this module.

Watch Laura analyze various traffic patterns including:

- character generator behavior
- breached client
- DHCP server discovery types
- DHCP ACK information
- normal DHCP boot process
- DHCP renew to rebind process
- dictionary attack
- DNS domain errors
- DNS MX record lookup
- DNS PTR queries.

This class includes the trace files (click the Documents button on the icon toolbar) for you to practice on!

Instructor:

Laura A. Chappell

Syllabus for 'Trace File Analysis - Set 3'

Purchase an All Access Pass (1 Year Subscription) to access this module.

Watch Laura analyze various traffic patterns including:

- DNS root server queries
- Sloooow DNS response
- DNS TTL issue
- DNS walking
- Lousy HTTP file download
- Comparing HTTP performance
- Somewhat OK HTTP performance
- Ettercap checking for a poisoner
- Another breached host
- FTP cracking attempt

This class includes the trace files (click the Documents button on the icon toolbar) for you to practice on!

Instructor:

Laura A. Chappell

Syllabus for 'Whiteboard Lecture Series 1'

Purchase an All Access Pass (1 Year Subscription) to access this module.

In this series of courses, Laura takes to the whiteboard to draw out some basic network concepts such as switching vs. routing, Manchester encoding and the beloved Ethernet frame structure.

Topics include:

- Tapping In to Wired Networks
- Inside Manchester Encoding
- CSMA/CD (Carrier Sense Multiple Access, Collision Detection)
- Reading/Writing Binary
- Switched and Routed Network Traffic
- The Ethernet Frame Structure
- The Resolution Processes
- The TCP Handshake

Instructor:

Laura A. Chappell