

**CHAPPELLUNIVERSITY**

# **All Access Pass**

## **Course List**

**[as of February 2017]**



# Table of Contents

Welcome to the All Access Pass (AAP) ..... 3

    All Access Pass Features ..... 3

    Train Your Entire IT Team ..... 3

All Access Pass Order Form..... 4

All Access Pass Course List (as of February 2017)..... 6

    Wireshark 101 Labs (Second edition) ..... 6

    Wireshark 101 Course: Section 0 - Explore Key Wireshark Elements and Traffic Flows ..... 6

    Wireshark 101 Course: Section 1 – Customize Wireshark Views and Settings ..... 6

    Network Forensics with Wireshark..... 7

    WCNA Exam Prep Questions ..... 7

    Lab Solutions for Wireshark 101: Essential Skills for Network Analysis ..... 7

    Analyzing the Window Zero Condition ..... 7

    Build Wireshark Filters from Snort Rules..... 8

    Wireshark Display Filter Tips and Tricks ..... 8

    Create a Security Profile ..... 8

    Find Stuff Fast with Wireshark Filter Expression Buttons..... 8

    Wireshark 1.8 Update - 19 Hot Features ..... 9

    CS42: Hacked Hosts ..... 9

    CS43: Analyze and Improve Throughput ..... 9

    CS44: Top 10 Reasons Your Network is Slow ..... 10

    CS45: TCP Analysis in-Depth ..... 10

    CS46: DHCP/ARP Analysis ..... 10

    CS47 Nmap Network Scanning 101 ..... 11

    CS48: Wireshark 101 Jumpstart..... 11

    CS50: WLAN Analysis 101 ..... 11

    CS52: Wireshark 201 Filtering ..... 11

    CS54: ICMP Analysis..... 12

    CS55: Analyzing Google Secure Search..... 12

    CS56: Slow Networks - NOPs/SACK ..... 12

    CS57: TCP Vulnerabilities..... 12

    CS58: Packet Crafting to Test Firewalls ..... 13

    CS59: Capturing Packets (Security Focus)..... 13

    CS60: Troubleshooting with Coloring ..... 13

    CS61: Tshark Command-Line Capture ..... 13

    CS62: Troubleshooting with Expert Info ..... 14

    CS63: 10 Essential Wireshark Skills..... 14

    CS64: Regex Primer..... 14

    CS65: Detecting Delays: Troubleshooting with Time..... 14

    CS66: Key TCP Settings ..... 15

    Trace File Analysis - Set 1..... 15

    Trace File Analysis - Set 2..... 15

    Trace File Analysis - Set 3..... 15

    Whiteboard Lecture Series 1 ..... 16

    Core 1: Wireshark Functionality and TCP/IP Analysis..... 16

    Core 2: Troubleshoot/Secure Networks with Wireshark..... 16

    [Retired] CS53: New Wireshark 1.4 Features ..... 17

[Retired] Wireshark 1.7 Update.....17  
[Retired] CS41: Wireshark 101 Jumpstart - Original.....17

## Welcome to the All Access Pass (AAP)



- Save time.
- Save money.
- Acquire in-demand skills.

Acquire valuable skills to quickly spot the source of network problems, identify breached hosts and determine the overhead of network applications.

### ALL ACCESS PASS FEATURES

- **Online training on key IT topics** – master in-demand skills
- **Videos filled with demonstrations** – watch how key skills are performed
- **Downloadable course documents** – reference course supplements offline
- **Industry-leading training from Laura Chappell, Founder of Wireshark University** – learn from an expert
- **CPE credit tracking system** – submit credits to certification programs
- **Course transcripts with in-progress percentages** – track your progress through classes
- **Course Completion Certificates** – print serialized certificates for each completed course
- **Categorized courses** – focus on specific topics
- **Unlimited access to recorded courses** – repeat courses as needed
- **Live events** – join Laura online for live course on hot topics

### TRAIN YOUR ENTIRE IT TEAM

Get your entire team trained on Wireshark, network analysis, TCP/IP communications, troubleshooting and network forensics.

- **Help Desk team:** Learn to capture traffic and identify the primary cause of performance problems
- **Infrastructure Team:** Learn to identify problems related to infrastructure devices
- **Server Team:** Quickly identify server error responses and high server latency
- **Security Team:** Detect recon processes and indications of breached hosts
- **Network Design Team:** Determine network capabilities and application loads

Group discounts are available when you sign up 5 or more students. See the All Access Pass Order Form (located on the next page).

# All Access Pass Order Form

Date	
Name	
Company	
Billing Address	
City	
State/Province	
Zip/Postal Code	
Country	
Email	
Phone	
Fax	

Return form to Chappell University  
[info@chappellU.com](mailto:info@chappellU.com)  
 59 Damonte Ranch Pkwy, 340, Reno NV 89521  
 Phone: (408) 378-7841

**Credit Card Information**

Credit Card Number	
Billing Address	
Expiration Date	
CVV	

Item	Description	Quantity	Unit Price	Amount
AAP1	All Access Pass <i>Single</i> 1-Year Subscription Plan		\$699.00	
AAP5	All Access Pass <i>Group</i> 1-Year Subscription Plan (Group Discount for 5 Students) Number of Students: _____		To be determined	
			Total:	

Check or credit cards accepted. Purchase Orders must be paid in full prior to account activation.

**Subscriber Information**

First Name		Last Name		Email Address	
First Name		Last Name		Email Address	
First Name		Last Name		Email Address	
First Name		Last Name		Email Address	
First Name		Last Name		Email Address	
First Name		Last Name		Email Address	
First Name		Last Name		Email Address	
First Name		Last Name		Email Address	
First Name		Last Name		Email Address	
First Name		Last Name		Email Address	
First Name		Last Name		Email Address	

Please list additional subscribers on a separate page.

Comments:

Note: All Access Pass Subscriptions are single-seat licenses.



## All Access Pass Course List (as of February 2017)

### WIRESHARK 101 LABS (SECOND EDITION)

Book Videos



Author: Laura Chappell  
 Category: Book Videos  
 CPE Credits: 4

Wireshark 2 is stable enough to start updating all the AAP content to this version. No more GTK+ interface, folks - we're now all Qt (pronounced "cute"). This 4-hour course (4 CPE credits) has the results of the 46 labs covered in the Second Edition of the Wireshark 101 book. The book is going to press and should be on shelves/Amazon/Kindle within a couple weeks.

### WIRESHARK 101 COURSE: SECTION 0 - EXPLORE KEY WIRESHARK ELEMENTS AND TRAFFIC FLOWS

Wireshark 101: Essential Skills



Author: Laura Chappell  
 Category: Wireshark 101: Essential Skills  
 CPE Credits: 4

This is the first course in a set of courses focusing on essential network analysis skills. Each of these courses are based on the best-selling Wireshark 101: Essential Skills for Network Analysts (2<sup>nd</sup> Edition) which focuses on Wireshark v2 functions.

This first course provides an overview of Wireshark functionality, features, resources, and uses. This is a recommended starting point for the Wireshark 101 series of courses.

### WIRESHARK 101 COURSE: SECTION 1 – CUSTOMIZE WIRESHARK VIEWS AND SETTINGS

Wireshark 101: Essential Skills



Author: Laura Chappell  
 Category: Wireshark 101: Essential Skills  
 CPE Credits: 3.5

This is the second course in a set of courses focusing on essential network analysis skills. Each of these courses are based on the best-selling Wireshark 101: Essential Skills for Network Analysts (2<sup>nd</sup> Edition) which focuses on Wireshark v2 functions.

This second course delves into Wireshark customization for a more efficient analysis process. This section contains the important Lab 5 which is referenced throughout the Wireshark 101 curriculum.

**NETWORK FORENSICS WITH WIRESHARK****Security and Network Forensics**

Author: Laura Chappell  
Category: Security and Network Forensics  
CPE Credits: 8

This 8-hour course (8 CPE credits) covers the essentials (network forensics methodology, essential Wireshark skills, locating the suspicious traffic) and includes the analysis of numerous malicious trace files from Laura's collection and from malware-traffic-analysis.net (Brad Duncan).

**WCNA EXAM PREP QUESTIONS****Wireshark Certification**

Author: Laura Chappell  
Category: Book Videos  
CPE Credits: 4

Many of our All Access Pass members are seeking the Wireshark Certified Network Analyst designation. This module provides over 300 practice quiz questions based on the thirty-three areas of study defined for the Wireshark Certified Network Analyst™ Exam. After answering each question you will be informed if you answered correctly or given a detailed explanation of the correct answer. You can take the practice exam as many times as you wish.

**LAB SOLUTIONS FOR WIRESHARK 101: ESSENTIAL SKILLS FOR NETWORK ANALYSIS****Book Videos**

Author: Laura Chappell  
Category: Book Videos  
CPE Credits: 3

This course contains the video solutions to the 46 labs contained in Wireshark 101: Essential Skills for Network Analysis. Based on Wireshark Version 10x

**ANALYZING THE WINDOW ZERO CONDITION****Troubleshooting**

Author: Laura Chappell  
Category: Troubleshooting  
CPE Credits: 1.5

This course is based on an AAP Live Event. 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.



**BUILD WIRESHARK FILTERS FROM SNORT RULES****Security and Network Forensics**

Author: Laura Chappell  
Category: Security and Network Forensics  
CPE Credits: 1

Interpret, translate and build Wireshark filters from Snort rules. Learn how to use Regex for more advanced filtering. Test your filters on the included trace file. Filters include Rimecud, Sykipot, LDPinch and LOIC (by Anonym9us). Other tools covered: Regex Buddy; Colasoft Packet Builder.

**WIRESHARK DISPLAY FILTER TIPS AND TRICKS****Wireshark Functionality and Tips**

Author: Laura Chappell  
Category: Wireshark Functionality and Tips  
CPE Credits: 1

Learn new display filtering techniques including filtering based on fields/strings, using the dreaded "!=" operator, and building offset (and bit-level) filters. This course includes two Notepad++ macros that you can use to convert coloring rules to Filter Expression buttons and convert Filter Expression buttons to coloring rules.

**CREATE A SECURITY PROFILE****Security and Network Forensics**

Author: Laura Chappell  
Category: Security and Network Forensics  
CPE Credits: 1

Learn how to get the best out of Wireshark by making it a security tool. In this 1-hour course, build a Security profile and create key security coloring rules using specific coloring rule names and colors. Finally, build a set of Filter Expression buttons to quickly locate packets of concern. Learn to use regex in your coloring rules and filters and where to find the latest security detection rules.

**FIND STUFF FAST WITH WIRESHARK FILTER EXPRESSION BUTTONS****Wireshark Functionality and Tips**

Author: Laura Chappell  
Category: Wireshark Functionality and Tips  
CPE Credits: 1

Learn how to locate the needle(s) in the haystack faster with Filter Expression Buttons. The course includes a set of general, troubleshooting and security Filter Expression Buttons and instructions to import these into your Wireshark profiles.

**WIRESHARK 1.8 UPDATE - 19 HOT FEATURES**

Wireshark Functionality and Tips

Author: Laura Chappell  
Category: Wireshark Functionality and Tips  
CPE Credits: 1

Learn the newest features of Wireshark - at least 19 of the hottest new features that were added to Wireshark 1.8.

**CS42: HACKED HOSTS**

Security and Network Forensics

Author: Laura Chappell  
Category: Security and Network Forensics  
CPE Credits: 1.5

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.

**CS43: ANALYZE AND IMPROVE THROUGHPUT**

Troubleshooting

Author: Laura Chappell  
Category: Troubleshooting  
CPE Credits: 1.5

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.

**CS44: TOP 10 REASONS YOUR NETWORK IS SLOW**

Troubleshooting



Author: Laura Chappell  
Category: Troubleshooting  
CPE Credits: 1.5

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.

**CS45: TCP ANALYSIS IN-DEPTH**

TCP/IP Communications

Author: Laura Chappell  
Category: TCP/IP Communications  
CPE Credits: 1.5

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.

**CS46: DHCP/ARP ANALYSIS**

TCP/IP Communications

Author: Laura Chappell  
Category: TCP/IP Communications  
CPE Credits: 1.5

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.

**CS47 NMAP NETWORK SCANNING 101****Other Tools**

Author: Laura Chappell  
Category: Other Tools  
CPE Credits: 1.5

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.

**CS48: WIRESHARK 101 JUMPSTART****Wireshark Functionality and Tips**

Author: Laura Chappell  
Category: Wireshark Functionality and Tips  
CPE Credits: 1.5

Laura and Gerald Combs (creator of Wireshark) hosted a new Wireshark Jumpstart webinar. Within 48 hours over 5,000 people had registered for the event. Laura demonstrates capture filters, display filters, IO graphing, coloring traffic and more. Download the Event Notes document for 60-pages of instructions, Q&A and more.

**CS50: WLAN ANALYSIS 101****Other**

Author: Laura Chappell  
Category: Other  
CPE Credits: 1.5

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.

**CS52: WIRESHARK 201 FILTERING****Wireshark Functionality and Tips**

Author: Laura Chappell  
Category: Wireshark Functionality and Tips  
CPE Credits: 1.5

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.

**CS54: ICMP ANALYSIS**

TCP/IP Communications

Author: Laura Chappell  
 Category: TCP/IP Communications  
 CPE Credits: 1.5

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.

**CS55: ANALYZING GOOGLE SECURE SEARCH**

Other

Author: Laura Chappell  
 Category: Other  
 CPE Credits: 1.5

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.

**CS56: SLOW NETWORKS - NOPS/SACK**

Troubleshooting



Author: Laura Chappell  
 Category: Troubleshooting  
 CPE Credits: 1.5

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.

**CS57: TCP VULNERABILITIES**

Security and Network Forensics

Author: Laura Chappell  
 Category: Security and Network Forensics  
 CPE Credits: 1.5

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.

## CS58: PACKET CRAFTING TO TEST FIREWALLS

Security and Network Forensics

Author: Laura Chappell  
Category: Security and Network Forensics  
CPE Credits: 1.5

Learn to use a seed packet, edit the packet contents, replay 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)

## CS59: CAPTURING PACKETS (SECURITY FOCUS)

Security and Network Forensics

Author: Laura Chappell  
Category: Security and Network Forensics  
CPE Credits: 2

This course is based on the Jumpstart 101 Course (CS41), this course takes a security angle to packet capture including information on capturing in stealth mode.

## CS60: TROUBLESHOOTING WITH COLORING

Troubleshooting

Author: Laura Chappell  
Category: Troubleshooting  
CPE Credits: 1.5

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.

## CS61: TSHARK COMMAND-LINE CAPTURE

Wireshark Functionality and Tips

Author: Laura Chappell  
Category: Wireshark Functionality and Tips  
CPE Credits: 1.5

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.

**CS62: TROUBLESHOOTING WITH EXPERT INFO**

Wireshark Functionality and Tips

Author: Laura Chappell  
Category: Wireshark Functionality and Tips  
CPE Credits: 1.5

The nine sections in this course focus on using the Expert Info to quickly detect the cause of network performance problems. This course includes reading Expert Info details in the TCP dissector, causes of various Expert Info Errors, Warnings and Notes, and fabulous graphing techniques to correlate throughput problems with Expert Info details.

**CS63: 10 ESSENTIAL WIRESHARK SKILLS**

Wireshark Functionality and Tips

Author: Laura Chappell  
Category: Wireshark Functionality and Tips  
CPE Credits: 1.5

This course is based on a live AAP event. Laura demonstrates the following 10 essential Wireshark skills: Key Word Filtering, Set up Unattended Capture with the Ring Buffer, Profile Importing, Add Filter Expression Buttons, Advanced IO Graphing with Logarithmic Scales, TCP Delta Graphing, Export Column Information to .csv Format, Use "Follow stream" to Filter out Normal Traffic, Splitting Trace Files (Capinfos then Editcap), Host Name Extraction and Use (Tshark).

**CS64: REGEX PRIMER**

Wireshark Functionality and Tips



Author: Laura Chappell  
Category: Wireshark Functionality and Tips  
CPE Credits: 1.5

This course takes you through the key concepts of using Regular Expressions with Wireshark. Topics include Regex flavors, metacharacters, sample use in emerging-threats.net Snort rule, searching for a character/word/hex string/number, and searching with a wildcard/group/integral qualifier/anchors/character classes. This course includes a Regex with Wireshark Quick Reference Guide.

**CS65: DETECTING DELAYS: TROUBLESHOOTING WITH TIME**

Troubleshooting

Author: Laura Chappell  
Category: Wireshark Functionality and Tips  
CPE Credits: 2

In this recorded AAP event, we look at two types of delays - round trip time delays and response time delays. We will adjust required protocol/application preferences, add custom columns for sorting, and build new buttons to quickly identify issues related to time.

**CS66: KEY TCP SETTINGS**

Wireshark Functionality and Tips

Author: Laura Chappell  
Category: Wireshark Functionality and Tips  
CPE Credits: 2

Examine Wireshark's 12 TCP preference settings and their effect on the traffic and your analysis. Includes coverage of TCP reassembly, bytes in flight usage, and TCP calculated timestamps.

**TRACE FILE ANALYSIS - SET 1**

Trace File Analysis

Author: Laura Chappell  
Category: Trace File Analysis  
CPE Credits: 1

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 \* brute force password cracking This class includes the trace files (click the Documents button on the icon toolbar) for you to practice on!

**TRACE FILE ANALYSIS - SET 2**

Trace File Analysis

Author: Laura Chappell  
Category: Trace File Analysis  
CPE Credits: 1

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!

**TRACE FILE ANALYSIS - SET 3**

Trace File Analysis

Author: Laura Chappell  
Category: Trace File Analysis  
CPE Credits: 1

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!



**WHITEBOARD LECTURE SERIES 1****Whiteboard Lecture Series**

Author: Laura Chappell  
Category: Whiteboard Lecture Series  
CPE Credits: 1.5

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.

**CORE 1: WIRESHARK FUNCTIONALITY AND TCP/IP ANALYSIS****Wireshark Certification**

Author: Laura Chappell  
Category: Wireshark Certification  
CPE Credits: 23

[To be replaced with the WCNA Boot Camp Class in 2013] 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.

**CORE 2: TROUBLESHOOT/SECURE NETWORKS WITH WIRESHARK****Wireshark Certification**

Author: Laura Chappell  
Category: Wireshark Certification  
CPE Credits: 25

[To be replaced with the WCNA Boot Camp Class in 2013] 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.

## [RETIRED] CS53: NEW WIRESHARK 1.4 FEATURES

Wireshark Functionality and Tips

Author: Laura Chappell  
Category: Wireshark Functionality and Tips  
CPE Credits: 1.5

This course covers the new features of Wireshark version 1.4.0.

## [RETIRED] WIRESHARK 1.7 UPDATE

Wireshark Functionality and Tips

Author: Laura Chappell  
Category: Wireshark Functionality and Tips  
CPE Credits: 1.5

Learn the new features of Wireshark 1.8 by looking at the Wireshark 1.7 development release - check out the hot Filter Expression buttons feature!

## [RETIRED] CS41: WIRESHARK 101 JUMPSTART - ORIGINAL

Wireshark Functionality and Tips

Author: Laura Chappell  
Category: Wireshark Functionality and Tips  
CPE Credits: 2

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!