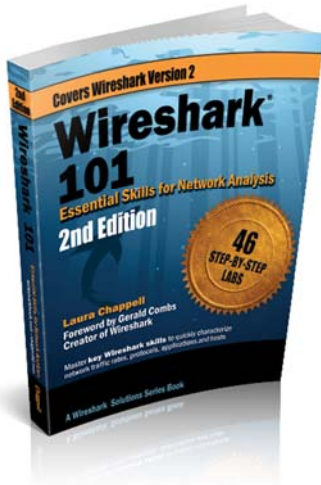


CHAPPELLUNIVERSITY

Wireshark 101 Course Set

Essential Skills for Network Analysis



Nine separate online courses focusing on essential network analysis skills. These courses are based on the best-selling Wireshark 101: Essential Skills for Network Analysts (2nd Edition) book which focuses on Wireshark v2 functions.

Author and Instructor: Laura Chappell
Founder, Chappell University/Wireshark University

Wireshark 101: Essential Skills for Network Analysis

Instructor: Laura Chappell, Chappell University/Wireshark University

Contents

All Access Pass Order Form	2
Section 0: Explore Key Wireshark Elements and Traffic Flows	3
Section 1: Customize Wireshark Views and Settings	4
Section 2: Determine the Best Capture Method and Apply Capture Filters	5
Section 3: Apply Display Filters to Focus on Specific Traffic	6
Section 4: Color and Export Interesting Packets	8
Section 5: Build and Interpret Tables and Graphs.....	9
Section 6: Reassemble Traffic for Faster Analysis	10
Section 7: Add Comments to Your Trace Files and Packets	11
Section 8: Use Command-Line Tools to Capture, Split, and Merge Traffic	12

Wireshark 101: Essential Skills for Network Analysis

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
 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.

Wireshark 101: Essential Skills for Network Analysis

Section 0: Explore Key Wireshark Elements and Traffic Flows

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.

Module	[mm:ss]
0.0 Section Introduction	05:40
0.1 Wireshark Capabilities and Tour	17:13
0.2 Wireshark Versions and Resources (wireshark.org)	19:45
0.3 Wireshark Capture Elements	12:39
0.4 Demo: Analysis Session (Latency Time and Application Error).....	11:40
0.5 Frames vs. Packets vs. Segments	05:36
0.6 Follow a Packet Through a Network	12:16
0.7 Access Resources from Inside Wireshark	11:14
0.8 Analyze Traffic Using the Main Wireshark View	30:13
Lab 1 Use Packets to Build a Picture of the Network	12:26
0.9 Analyze Typical Network Traffic.....	18:51
Lab 2 Capture and Classify Your Own Background Traffic	03:53
0.10 Open Trace Files Captured with Other Tools.....	04:44
Lab 3 Open a Network Monitor .cap Trace File.....	02:45
CH0 Challenge 0.....	06:57

Trace Files: **WS101v2TraceFilesSection0.zip**

- ✓ challenge101-0.pcapng
- ✓ general101.pcapng
- ✓ http-google101.pcapng
- ✓ http-wincap101.cap
- ✓ mybackground101.pcapng

CPEs: 4

Wireshark 101: Essential Skills for Network Analysis

Section 1: Customize Wireshark Views and Settings

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.

Module	[mm:ss]
1.0 Section Introduction	05:50
1.1 Add, Edit, Export Columns	10:27
Lab 4 Add the HTTP Host Field as a Column.....	04:56
1.2 Dissect the Wireshark Dissectors.....	08:09
1.3 Analyze Traffic that Uses Non-Standard Ports.....	15:29
1.4 Define Preferences Settings.....	18:39
Lab 5 Set Key Wireshark Preferences (IMPORTANT LAB)	09:46
1.5 Creating Profiles.....	12:49
Lab 6 Create a New Profile Based on the Default Profile.....	04:51
1.6 Locate Key Configuration Files.....	06:06
Lab 7 Import a DNS/HTTP Errors Profile.....	05:28
1.7 Configure Time Column to Spot Delays	25:50
Lab 8 Spot Path and Server Latency Problems.....	09:18
CH1 Challenge 1.....	05:09

Trace Files: **WS101v2TraceFilesSection1.zip**

- ✓ challenge101-1.pcapng
- ✓ dns-nmap101.pcapng
- ✓ http-chappellu101.pcapng
- ✓ http-disney101.pcapng
- ✓ http-espn101.pcapng
- ✓ http-google101.pcapng
- ✓ http-nonstandard101.pcapng
- ✓ http-openoffice101b.pcapng
- ✓ http-pcaprnet101.pcapng
- ✓ http-slow101.pcapng
- ✓ tcp-decodeas.pcapng

CPEs: 3.5

Wireshark 101: Essential Skills for Network Analysis

Section 2: Determine the Best Capture Method and Apply Capture Filters

This third course focuses on initial analyzer placement for wired and wireless packet capture, capture filtering, unattended capture, and capture filter techniques for addresses and applications.

Module	[mm:ss]
2.0 Section Introduction	08:49
2.1 Identify the Best Capture Location	03:08
2.2 Capture on an Ethernet Network	08:56
2.3 Capture on a Wireless Network	16:48
2.4 Identify Active Interfaces	10:56
2.5 Deal with Tons of Traffic (File Sets)	07:48
Lab 9 Capture to File Sets	05:33
2.6 Use Special Capture Techniques to Spot Sporadic Problems (Ring Buffer)	06:26
Lab 10 Use a Ring Buffer to Conserve Drive Space	04:26
2.7 Reduce the Amount of Traffic You Have to Work With	15:52
2.8 Capture Traffic Based on Addresses (MAC/IP)	15:33
Lab 11 Capture Only Traffic to or from Your IP Address	04:34
Lab 12 Capture Only Traffic to or from Everyone Else's MAC Address	06:05
2.9 Capture Traffic for a Specific Application	04:37
2.10 Capture Specific ICMP Traffic	04:29
Lab 13 Create, Save, and Apply a DNS Capture Filter	06:45
CH2 Challenge 2	10:30

Trace Files: ***ws101v2-tracefiles-s3.zip***

- ✓ sec-nessus101.pcapng
- ✓ wlan-ipadstartstop101.pcapng

CPEs: 3.5

Wireshark 101: Essential Skills for Network Analysis

Section 3: Apply Display Filters to Focus on Specific Traffic

This fourth course delves deeply into display filtering – the ultimate way to find the “needle in the haystack.” This course defines display filtering methods and must-know syntax information for include/exclude filters using standard filters and regular expressions. Learn tips and tricks for filtering on addresses, subnets, applications, and keywords. Learn how to add wildcards to your filters and buttons to your profile!

Module	[mm:ss]
3.0 Section Introduction	06:55
3.1 Display Filter Methods and Syntax	32:24
Lab 14 Use Auto-Complete to Find Traffic to a Specific HTTP Server	10:14
3.2 Edit and Use the Default Display Filters.....	08:06
Lab 15 Use a Default Filter as a “Seed” for a New Filter	04:57
3.3 Filter Properly on HTTP Traffic	04:03
Lab 16 Filter on HTTP Traffic the Right Way.....	03:50
3.4 Determine Why Your dhcp Filter Doesn’t Work	03:25
3.5 Apply Display Filters Based on an IP Address, Range of Addresses or a Subnet	07:03
Lab 17 Filter on Traffic to or from Online Backup Subnets	03:17
3.6 Quickly Filter on a Field in a Packet	10:44
Lab 18 Filter on DNS Name Errors or HTTP 404 Responses	05:58
3.7 Filter on a Single TCP or UDP Conversation.....	10:44
Lab 19 Detect Background File Transfers on Startup.....	04:18
3.8 Expand Display Filters with Include and Exclude Conditions.....	06:44
3.9 Use Parentheses to Change Filter Meaning.....	02:15
Lab 20 Locate TCP Connection Attempts to a Client.....	04:07
3.10 Determine Why Your Display Filter Area is Yellow	02:00
3.11 Filter on a Keyword in a Trace File	10:42
Lab 21 Use a Regular Expression Filter to Locate a Set of Key Words in a Trace File	04:09
3.12 Use Wildcards in Your Display Filters.....	04:50
Lab 22 Filter with Wildcards between Words	04:26
3.13 Use Filters to Spot Communication Delays.....	12:08
Lab 23 Import Display Filters into a Profile	05:31
3.14 Turn Your Key Display Filters into Buttons	09:39
Lab 24 Create and Import HTTP Filter Expression Buttons	08:13
CH3 Challenge 3.....	04:23

Wireshark 101: Essential Skills for Network Analysis

Trace Files: ***ws101v2-tracefiles-s3.zip***

- ✓ http-browse101.pcapng
- ✓ http-sfgate101.pcapng
- ✓ http-wiresharkdownload101.pcapng
- ✓ http-espn101.pcapng
- ✓ http-errors101.pcapng
- ✓ http-disney101.pcapng
- ✓ dhcp-serverdiscovery101.pcapng
- ✓ mybackground101.pcapng
- ✓ general101b.pcapng
- ✓ gen-startupchatty101.pcapng
- ✓ ftp-crack101.pcapng
- ✓ ftp-clientside101.pcapng
- ✓ http-pictures101.pcapng
- ✓ http-download101d.pcapng
- ✓ http-download-a.pcapng
- ✓ challenge101-3.pcapng

CPEs: 5

Wireshark 101: Essential Skills for Network Analysis

Section 4: Color and Export Interesting Packets

This fifth course begins with a focus on using temporary coloring, coloring rules, and the intelligent scrollbar to speed up detection of problems captured in trace files. Next, this course demonstrates how to create trace file subsets and extract characteristics of packets for further analysis in spreadsheet programs.

Module	[mm:ss]
4.0 Section Introduction	05:52
4.1 Identify Applied Coloring Rules.....	03:50
Lab 25 Add a Column to Display Coloring Rules in Use.....	03:29
4.2 Disable Coloring Rules.....	06:42
4.3 Build a Coloring Rule to Highlight Delays.....	06:57
Lab 26 Build a Coloring Rule to Highlight FTP User Names, Passwords, and More	04:49
4.4 Quickly Colorize a Single Conversation (Temporary Coloring Rules).....	05:29
Lab 27 Create Temporary Conversation Coloring Rules.....	05:25
4.5 Master the Intelligent Scrollbar	04:41
Lab 28 Use the Intelligent Scrollbar to Quickly Find Problems	04:53
4.6 Export Packets of Interest.....	03:53
Lab 29 Export a Single TCP Conversation	04:28
4.7 Export Packet Details (Excel Analysis).....	06:58
Lab 30 Export a List of HTTP Host Field Values from a Trace File	05:36
CH4 Challenge 4.....	10:12

Trace Files: **ws101v2-tracefiles-s4.zip**

- ✓ challenge101-4.pcapng
- ✓ ftp-bounce.pcapng
- ✓ ftp-crack101.pcapng
- ✓ http-au101b.pcapng
- ✓ http-browse101.pcapng
- ✓ http-browse101d.pcapng
- ✓ http-jezebel101.pcapng
- ✓ http-misctrffic101.pcapng
- ✓ http-sfgate101.pcapng
- ✓ net-lost-route.pcapng
- ✓ sec-nessus101.pcapng

CPEs: 2.5

Wireshark 101: Essential Skills for Network Analysis

Section 5: Build and Interpret Tables and Graphs

This sixth course focuses on finding the top talkers and most active network conversations, identifying protocols in use, detecting suspicious traffic, and creating comparative graphs based on hosts and applications in use. This section also defines how to use the Wireshark Expert to quickly detect the cause of network performance problems.

Module	[mm:ss]
5.0 Section Introduction	05:36
5.1 Find Out Who's Talking to Whom on the Network	14:59
5.2 Locate the Top Talkers	06:42
Lab 31 Filter on the Most Active TCP Conversation	03:41
Lab 32 Set Up GeoIP to Map Targets Globally.....	04:27
5.3 List Applications Seen on the Network.....	08:36
Lab 33 Detect Suspicious Protocols and Applications.....	03:54
5.4 Graph Application and Host Bandwidth Usage	24:58
Lab 34 Compare Traffic to/from a Subnet to Other Traffic.....	03:39
5.5 Identify TCP Errors on the Network.....	09:47
5.6 Understand What those Expert Errors Mean	04:25
Lab 35 Identify an Overloaded Client.....	03:35
5.7 Graph Various Network Errors.....	07:35
Lab 36 Detect and Graph File Transfer Problems.....	05:16
CH5 Challenge 5.....	05:11

Trace Files: **ws101v2-tracefiles-s5.zip**

- ✓ challenge101-5.pcapng
- ✓ general101c.pcapng
- ✓ general101d.pcapng
- ✓ http-browse101.pcapng
- ✓ http-browse101b.pcapng
- ✓ http-browse101c.pcapng
- ✓ http-download101.pcapng
- ✓ http-espn101.pcapng
- ✓ http-misctrffic101.pcapng
- ✓ sec-nessus101.pcapng
- ✓ tr-twohosts.pcapng

CPEs: 2.5

Wireshark 101: Essential Skills for Network Analysis

Section 6: Reassemble Traffic for Faster Analysis

This seventh course focuses on reassembling streams to analyze application-layer communications, reassembling HTTP objects and FTP files.

Module	[mm:ss]
6.0 Section Introduction	05:00
6.1 Reassemble Web Browsing Sessions	07:07
Lab 37 Use Reassembly to Find a Web Site's Hidden HTTP Message	04:41
6.2 Reassemble a File Transferred via FTP.....	04:17
Lab 38 Extract a File from an FTP File Transfer	06:40
6.3 Export HTTP Objects Transferred in a Web Browsing Session	06:56
Lab 39 Carve Out an HTTP Object from a Web Browsing Session	05:18
CH6 Challenge 6.....	05:22

Trace Files: **ws101v2-tracefiles-s6.zip**

- ✓ challenge101-6.pcapng
- ✓ ftp-clientside101.pcapng
- ✓ ftp-download101.pcapng
- ✓ http browse101.pcapng
- ✓ http-college101.pcapng
- ✓ http-espn101.pcapng
- ✓ http-wiresharkdownload101.pcapng

CPEs: 1

Wireshark 101: Essential Skills for Network Analysis

Section 7: Add Comments to Your Trace Files and Packets

This course focuses on adding comments to trace files and to individual packets, viewing all annotations, and exporting annotations to create a network report.

Module	[mm:ss]
7.0 Section Introduction	03:37
7.1 Add Your Comments to Trace Files.....	03:33
7.2 Add Your Comments to Individual Packets.....	03:04
Lab 40 Read Analysis Notes in a Malicious Redirection Trace File.....	04:04
7.3 Export Packet Comments for a Report	05:58
Lab 41 Export Malicious Redirection Packet Comments.....	04:56
CH 7 Challenge 7.....	04:14

Trace Files: **ws101v2-tracefiles-s7.zip**

- ✓ challenge101-7.pcapng
- ✓ http-cheez101.pcapng
- ✓ sec-suspicious101.pcapng

CPEs: 2.5

Wireshark 101: Essential Skills for Network Analysis

Section 8: Use Command-Line Tools to Capture, Split, and Merge Traffic

This course focuses using Capinfos, Tshark, Dumpcap, Editcap and Mergecap to split, merge, and obtain information about trace files. In addition, this course covers the process of command-line capture, field extraction, and creation of trace file subsets.

Module	[mm:ss]
8.0 Section Introduction	06:23
8.1 Split a Large Trace File into a File Set.....	09:26
Lab 42 Split a File and Work with Filtered File Sets.....	04:46
8.2 Merge Multiple Trace Files	07:09
Lab 43 Merge a Set of Files using a Wildcard	03:24
8.3 Capture Traffic at Command Line	12:15
Lab 44 Use Tshark to Capture to File Sets with an Autostop Condition.....	07:12
8.4 Use Capture Filters during Command-Line Capture	06:25
8.5 Use Display Filters during Command-Line Capture	04:48
Lab 45 Use Tshark to Extract HTTP GET Requests.....	03:38
8.6 Use Tshark to Export Specific Field Values and Statistics from a Trace File	08:01
Lab 46 Use Tshark to Extract HTTP Host Names and IP Addresses	05:15
CH 8 Challenge 8	05:57

Trace Files: **ws101v2-tracefiles-s8.zip**

- ✓ challenge101-8.pcapng
- ✓ http download-c.pcapng
- ✓ http-esp101.pcapng

CPEs: 2