Wireshark: Protocols, Troubleshooting, and Network Forensics
July 13-17, 2020

Install Wireshark on your system and join Laura Chappell for an in-depth class focused on detecting network performance issues and suspect traffic. After building a custom profile, you will master key Wireshark functions and filtering techniques before beginning a deep dive into various protocols and applications common on TCP/IP networks. You will focus on protocol and application behavior that causes performance degradation on the network or indicates a network reconnaissance or attack is underway or a system has already been breached. Prior to this course you will receive a link to a pre-course evaluation quiz, a location from which to download the traffic files (trace files) used in the course and your course manual.

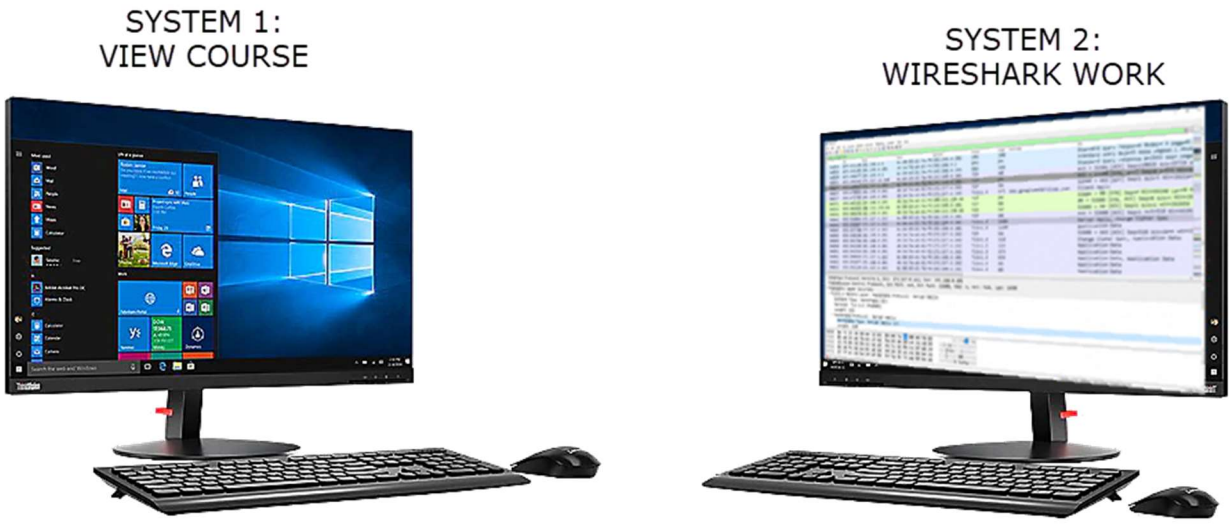
System Requirements

Wireshark can run on various platforms and can be downloaded from https://wireshark.org. Details regarding system requirements can be found online at https://www.wireshark.org/docs/wsug_html_chunked/ChIntroPlatforms.html. Please test your system in advance of the class to ensure you can (a) capture network traffic, and (b) open a capture file.

If you need to download a sample trace file, visit https://www.chappell-university.com/traces.

Recommended Configuration

Although you can take this course using a single computer and toggle between the Zoom session and Wireshark windows, we highly recommend that you have two systems ready for the class. One system would be your course viewing system while the second system would be the system on which you would run Wireshark.



Daily Schedule

Start time: 8:30 am CT
Lunch time: 12:00 pm – 1:00 pm CT
End time: ~4:30 pm CT (Friday end time is 12:30 pm)
Flexible break times through each day

Student Outcomes

- Understand how core protocols communicate on TCP/IP networks
- Use Wireshark to detect and analyze key network performance issues
- Use Wireshark to detect and analyze suspicious network traffic

Course Outline

Section 1: Course Introduction
Section 2: Troubleshooting Focus: The "Golden Rule"
Section 3: Network Forensics: Wireshark's Role
Section 4: Wireshark Essential Elements and Features (Course Profile)
Section 5: Capture Methods and Filters
Section 6: Customization: Wireshark Preferences
Section 7: Navigation, Coloring, and Reassembly
Section 8: Detecting Application and Path Delays (Working with Time)
Section 9: Extract and Interpret Essential Trace File Statistics
Section 10: Focus on Traffic Using Display Filters
Section 11: TCP/IP Communications Overview
Section 12: Analyze DNS Traffic (Problems/Breaches)
Section 13: Analyze ARP Traffic (Problems/Scans/Breaches)
Section 14: Analyze IPv4 Traffic (Problems/Breaches)
Section 15: Analyze ICMP Traffic (Problems/Scans/Breaches)
Section 16: Analyze UDP Traffic (Problems/Scans/Breaches)
Section 17: Analyze TCP Traffic (Problems/Scans/Breaches)
Section 18: Analyze HTTP/HTTPS Traffic (Problems/Breaches)
Section 19: Review of Troubleshooting Steps
Section 20: Review of Network Forensics Steps

Instructor Contact

Laura Chappell
laura@chappellU.com

Please include “Summer Working Connections” in the Subject area.