Wireshark Essential Training

with Lisa Bock

Hyperlinks for each chapter

Chapter 1. Traffic Capture Overview

Download and install on a PC or Mac

- To get a copy of Wireshark, go to: https://www.wireshark.org

Getting help

- To view the Wireshark Wiki, go to: https://gitlab.com/wireshark/wireshark/-/wikis/home
- Here you'll find the Wireshark user's guide: https://www.wireshark.org/docs/wsug_html_chunked/
- If you have questions, you can post them to the Wireshark community here: https://ask.wireshark.org/questions/
- For a capture repository, visit: https://wiki.wireshark.org/SampleCaptures or the newer GitHub site at https://gitlab.com/wireshark/wireshark/-/wikis/SampleCaptures

Chapter 2. Getting Started with Wireshark

Challenge: Recognize the Wireshark Interface

Questions

1. By default, Wireshark saves packets to a temporary file. To save files using a ring buffer, select _____.
   a. Edit
   b. Go
   c. Capture
   d. Tools
2. In frame 714, what represents the transport layer header?
   a. Ethernet II
   b. Transmission Control Protocol
   c. Hypertext Transport Protocol
3. In frame 714, what represents the frame header?
   a. Ethernet II
   b. Frame 714
   c. Hypertext Transport Protocol

Chapter 3. Examining the Internet Suite

Explaining Transmission Control Protocol

- If you would like to follow along with the demonstration, visit: https://www.cloudshark.org/captures/0012f52602a3

Recognizing the TCP connection process

- If you would like to follow along with the presentation, visit: https://www.cloudshark.org/captures/923901f326f8

Viewing the TCP handshake and teardown

- If you would like to follow along with the demonstration, visit: https://www.cloudshark.org/captures/923901f326f8

Breaking down User Datagram Protocol

- If you would like to follow along with the demonstration, visit: https://www.cloudshark.org/captures/00089db884f6

Comprehending ICMP

- Visit https://packetlife.net/captures/protocol/icmp/ to get a copy of two packet captures, icmp fragmented and traceroute_MPLS
- Go to https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml to learn more about icmp types and codes

Discovering ICMPv6

- Visit https://packetlife.net/captures/protocol/icmpv6/ to get a copy of a pcap so you can follow along with the demonstration

Challenge: Evaluating a pcap

- For this challenge, use the exercise file to find the links and follow along

Chapter 4. Deep Packet Analysis of Common Protocols

Dissecting DNS

- For an extensive list of RFCs on DNS, visit: https://www.statdns.com/rfc/

Using HTTP

- Visit https://developer.mozilla.org/en-US/docs/Web/HTTP/Status to see a list of HTTP status codes

Understanding ARP

- Visit https://packetlife.net/captures/protocol/arp/ to get a copy of a pcap so you can follow along with the demonstration

Chapter 5. Working with Packet Captures

Using CloudShark

- To learn more about CloudShark, visit: https://www.cloudshark.org/captures/c109b95db0af
- See the power of the Cisco Meraki: https://documentation.meraki.com/zGeneral_Administration/Tools_and_Troubleshooting/Capturing_Traffic_on_Multiple_Interfaces
- Visit PacketLife for a variety of precaptured packets: https://packetlife.net/captures/protocol/telnet/
- For examples on malware analysis, visit: https://www.malware-traffic-analysis.net/2017/01/28/index.html

Summary

What's Next?

- To see a list of courses on my homepage, visit: https://www.linkedin.com/learning/instructors/lisa-bock