



Wireshark

Kirsten Hanson
GenCyber Workshop



Agenda

- Wireshark Introduction
- Brief history of Wireshark
- Uses of Wireshark
- Using Wireshark



Learning Objectives

- Establish a basic understanding of Wireshark
- Describe some basic uses of Wireshark



Wireshark Introduction

- Wireshark is a network packet analyzer
 - This presents captured packet data in extreme detail
 - Similar to using a voltmeter to determine what is going on inside of an electric cable, a network packet analyzer helps determine what is going on inside of a network cable
- Wireshark has taken an expensive and often proprietary technology and put it into the hands of any person via free, open-source technology

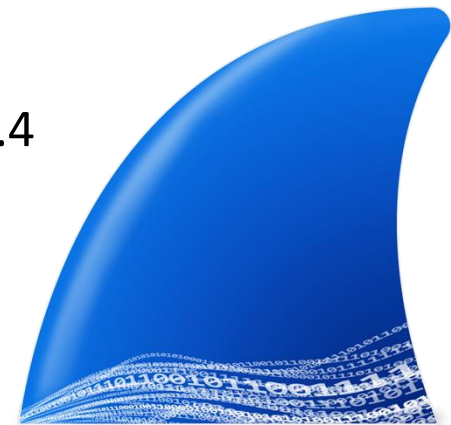
A graphic element consisting of a thick horizontal line with a curved, upward-pointing shape in the center, resembling a shark's dorsal fin.

WIRESHARK



Wireshark History

- Development of Wireshark began in 1997
- The invention of Wireshark actually began as the invention of Ethereal by Gerald Combs
- Many people since then have made significant contributions to the development of Wireshark, such as Gilbert Ramirez, Guy Harris, Richard Sharpe
- The name did not change from Ethereal to Wireshark until 2006
- Version 1.0 of Wireshark was released in 2008
- Version 2.0 of Wireshark was released in 2015
- The current version of Wireshark is Version 3.4.4
- Wireshark now credits over 600 contributors



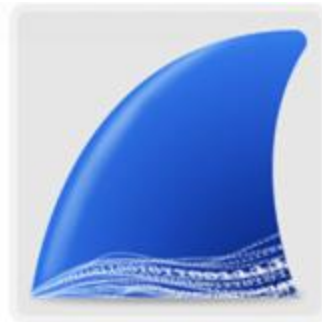
Uses of Wireshark

- Some of the best examples of Wireshark's purposes include:
 - Troubleshoot network problems
 - Examine security problems
 - Verify network applications
 - Debug protocol implementations
 - Learn network protocol internals



Using Wireshark

- Wireshark is free and available for download straight from the Wireshark website
 - The download is available for Windows, Mac, and Linux distributions



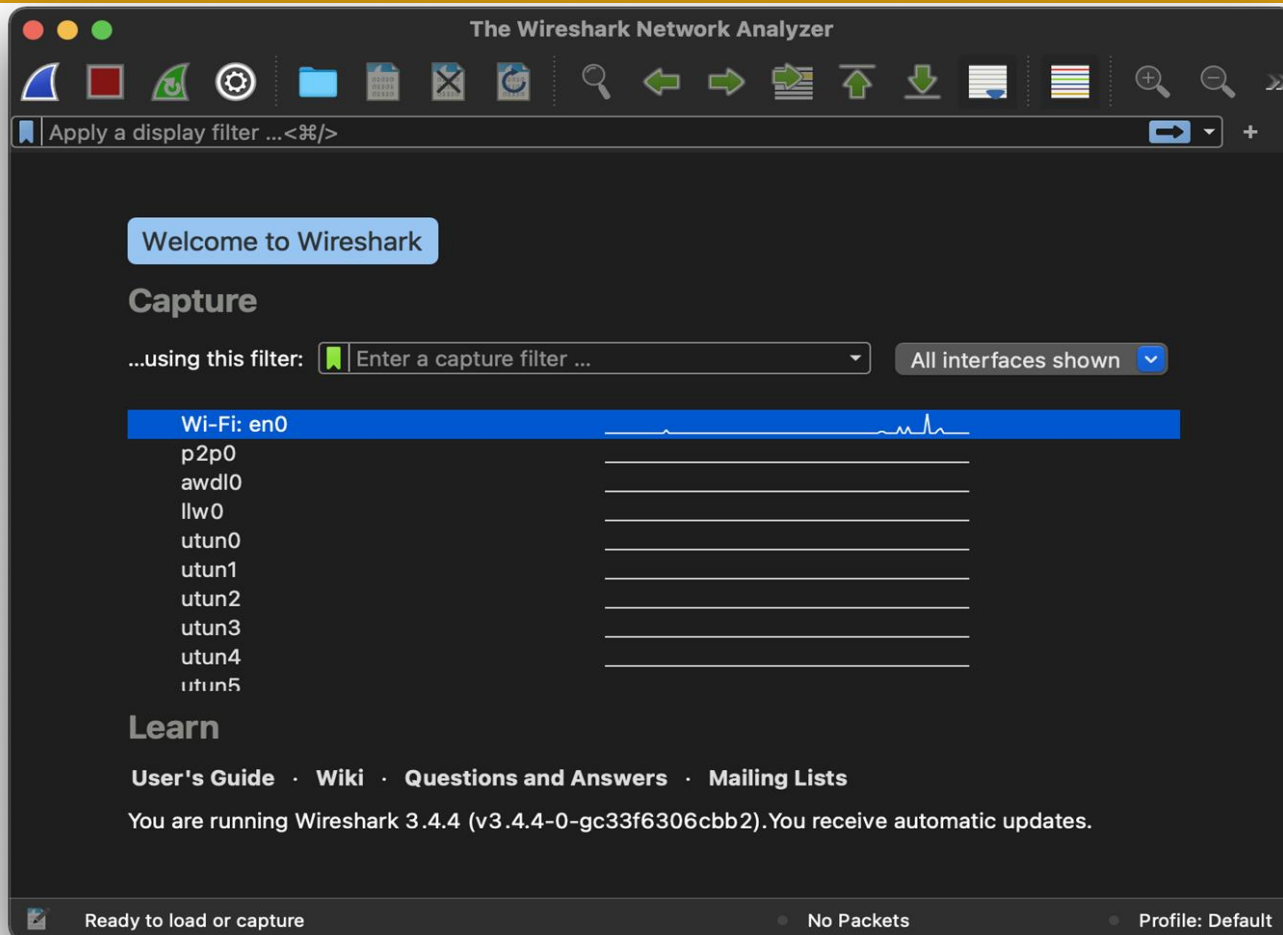
Wireshark



Applications



Using Wireshark





Using Wireshark

- Inside of Wireshark, you can view what is going on inside of the network

Length	Info
82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
127	Standard query 0x0000 SRV google-home-9afbc2d3f4fa108d17daaca24d8d721a._googlecast._tcp.local, "QM" qu.
403	Standard query response 0x0000 PTR Google-Nest-Hub-5510aac52af64d5c9ef823fd47278181._googlecast._tcp.l
414	Standard query response 0x0000 PTR Google-Cast-Group-DB4C9AA24F854C5B9272D96E2F4B933E-1._googlecast._t
420	Standard query response 0x0000 PTR Google-Home-Mini-e4892fc3cfcc7a79fa0de2bd4d4479dc._googlecast._tcp..
407	Standard query response 0x0000 PTR Google-Home-Mini-7fa95863f60fcac08d191139a1842509._googlecast._tcp..
399	Standard query response 0x0000 PTR Google-Home-9afbc2d3f4fa108d17daaca24d8d721a._googlecast._tcp.local
194	Standard query response 0x0000 SRV, cache flush 0 0 8009 9afbc2d3-f4fa-108d-17da-aca24d8d721a.local A,
428	Standard query response 0x0000 PTR Google-Home-Mini-56935242a79c2e22c2a871b8c5db4902._googlecast._tcp..
425	Standard query response 0x0000 PTR Google-Home-Mini-a4a484c382f11e6310c9f1a7289cb384._googlecast._tcp..
82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
131	Standard query 0x0000 SRV google-nest-hub-5510aac52af64d5c9ef823fd47278181._googlecast._tcp.local, "QM.
425	Standard query response 0x0000 PTR Google-Home-Mini-a4a484c382f11e6310c9f1a7289cb384._googlecast._tcp..
82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question



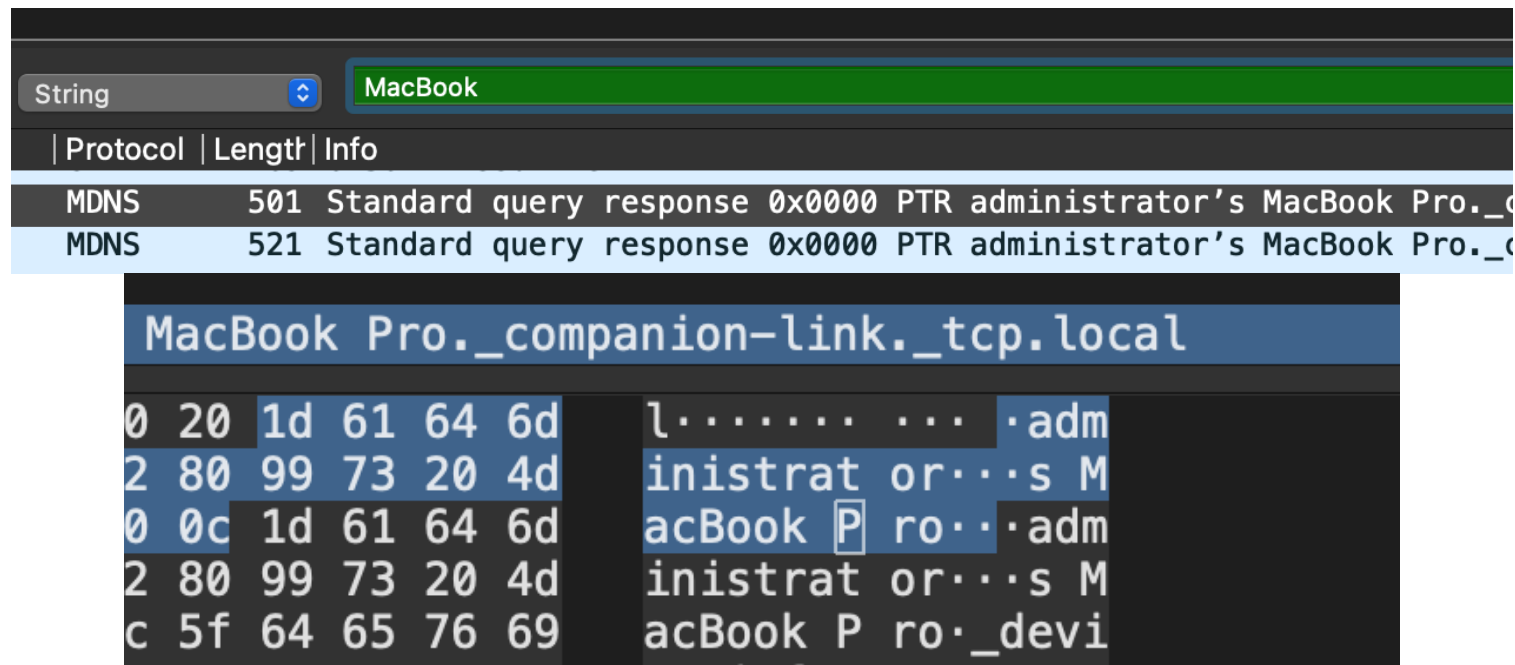
Using Wireshark

- In a live capture, numerous columns of information are displayed
 - No.
 - This is the number order of the packet that got captured. The bracket indicates that this packet is part of a conversation.
 - Time
 - This column shows you how long after you started the capture that this packet got captured.
 - Source
 - The system that sent the packet.
 - Destination
 - The address of the destination of that packet.
 - Protocol
 - This is the type of packet (e.g. TCP, DNS, DHCPv6, or ARP)
 - Length
 - The length of the packet in bytes.
 - Info
 - More information about the packet contents



Using Wireshark

- The information that Wireshark provides is quite comprehensive
- To help you find something specific, there are many search functions put into place





Using Wireshark

- Two of the most useful search functions are `ip.src==IP-address` and `ip.dst==IP-address`
 - For example, if you are looking for traffic coming from the IP address 192.168.1.28 it would look like this

ip.src==192.168.1.28		
Packet list		
Narrow & Wide		
No.	Time	Source
194...	589.874122	192.168.1.28
183...	554.563290	192.168.1.28
183...	553.728485	192.168.1.28
182...	551.544495	192.168.1.28
175...	529.873151	192.168.1.28
164...	491.545286	192.168.1.28
157...	469.865085	192.168.1.28
157...	467.580274	192.168.1.28
156...	466.465594	192.168.1.28
147...	431.543524	192.168.1.28
145...	424.362400	192.168.1.28



Resources

- Wireshark
 - <https://www.wireshark.org>
- Wireshark User's Guide
 - https://www.wireshark.org/docs/wsug_html_chunked/
- How to Use Wireshark: Comprehensive Tutorial + Tips
 - <https://www.varonis.com/blog/how-to-use-wireshark/>



Activity



Please complete the Wireshark activity.