THE UNIVERSITY OF TENNESSEE CHATTANOOGA

Wireshark

Kirsten Hanson
GenCyber Workshop

Agenda

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

Learning Objectives

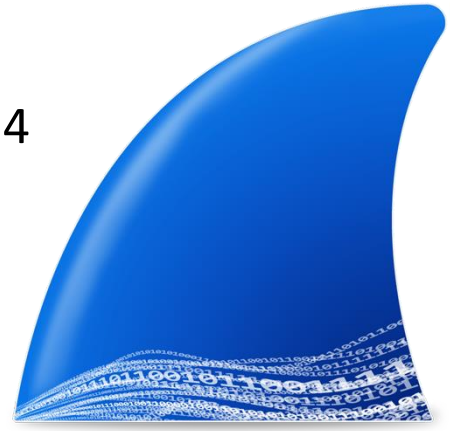
- Establish a basic understanding of Wireshark
- Describe some basic uses of Wireshark

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

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

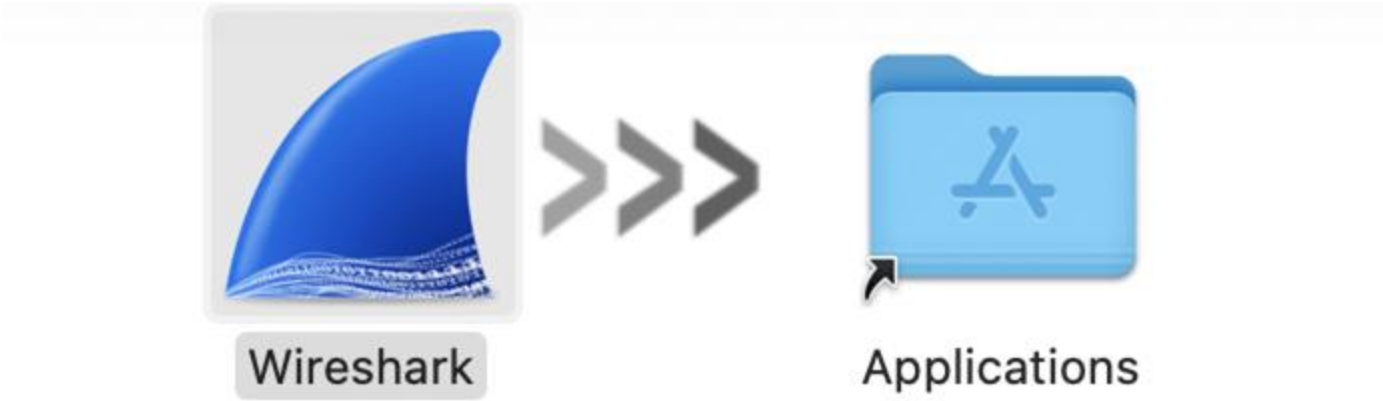


Uses of Wireshark

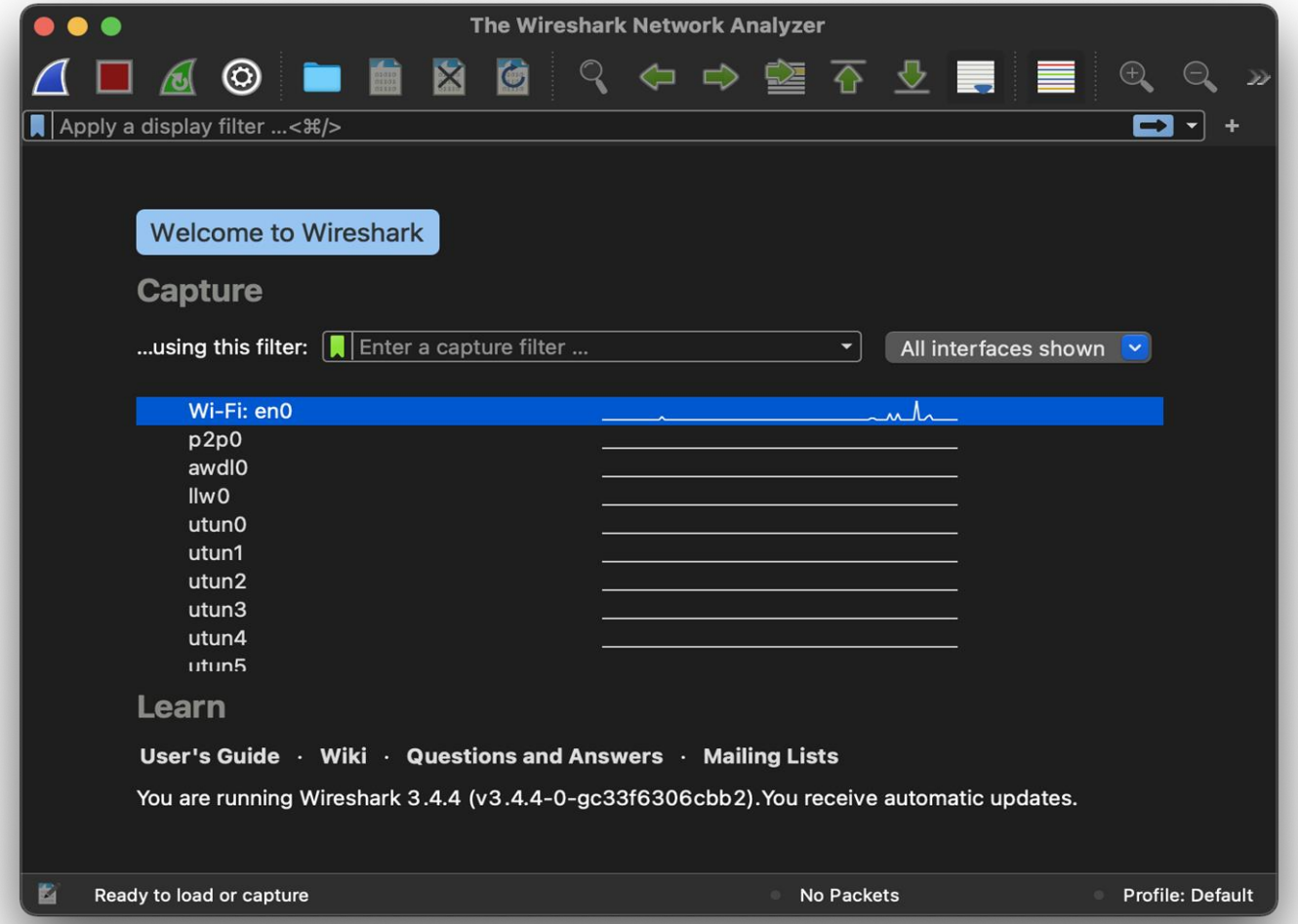
- Some of the best examples of Wireshark's purposes include:
  - Troubleshoot network problems
  - Examine security problems
  - Verify network applications
  - Debug protocol implementations
  - Learn network protocol internals

Using Wireshark

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

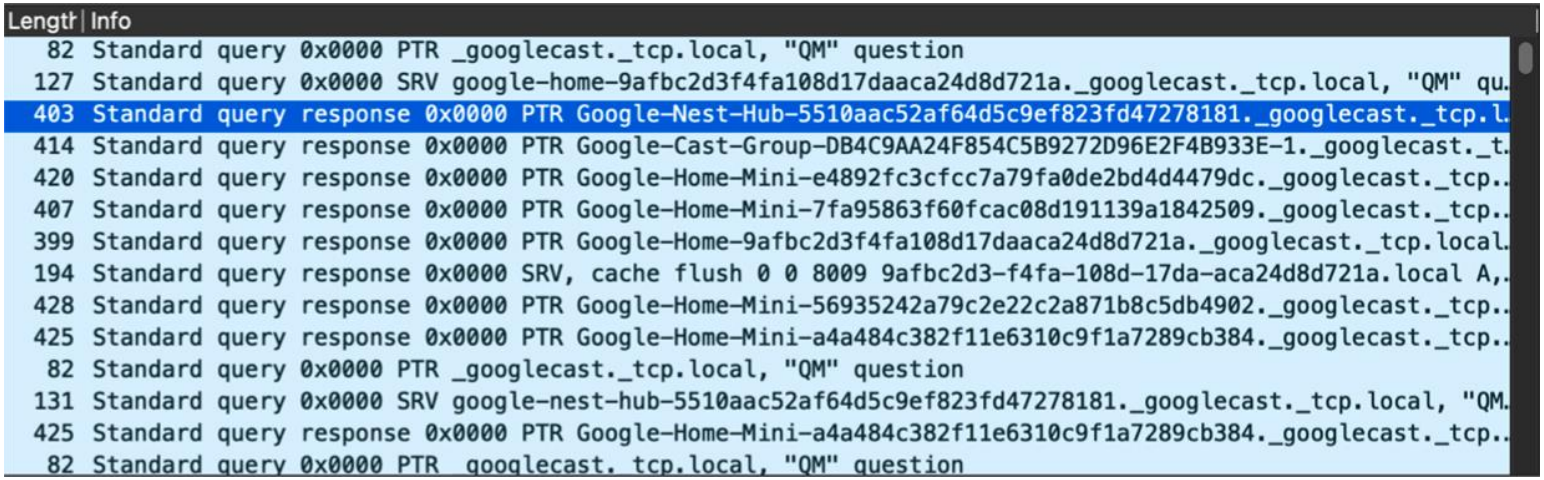


Using Wireshark



Using Wireshark

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

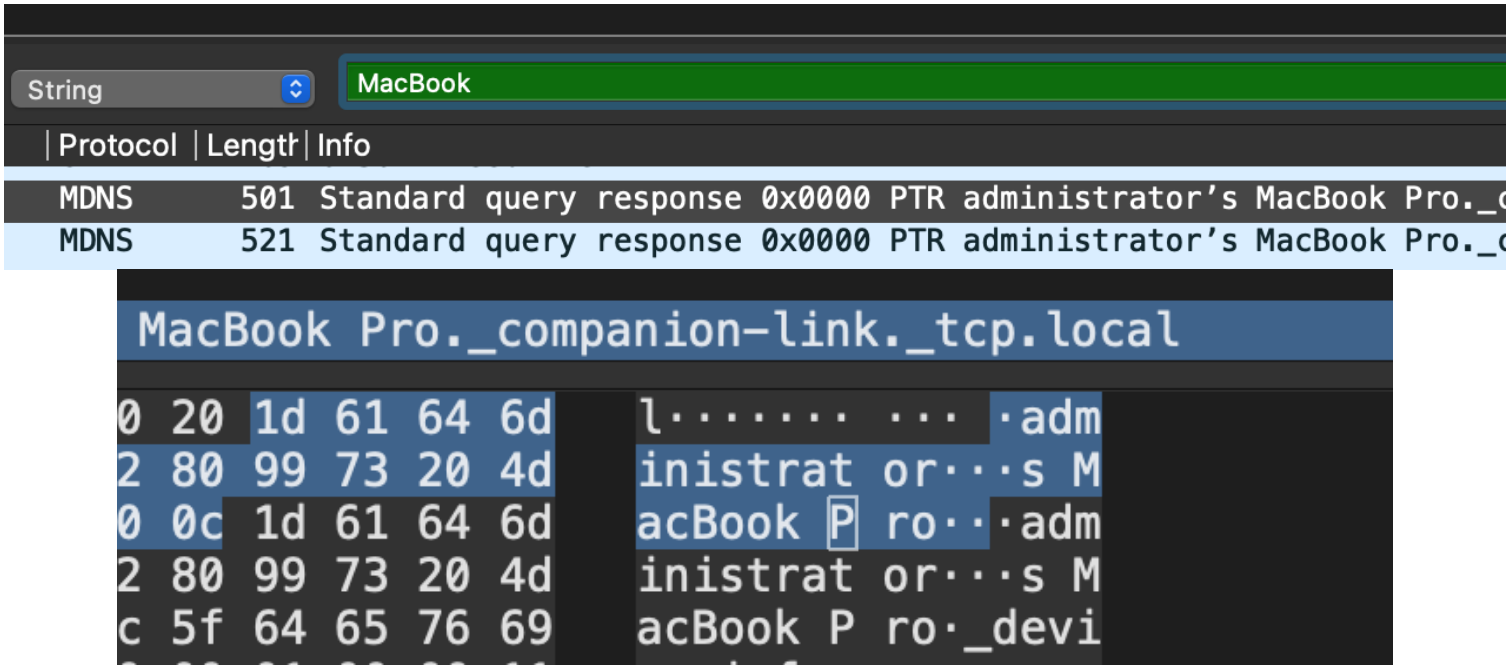


Using Wireshark

- 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

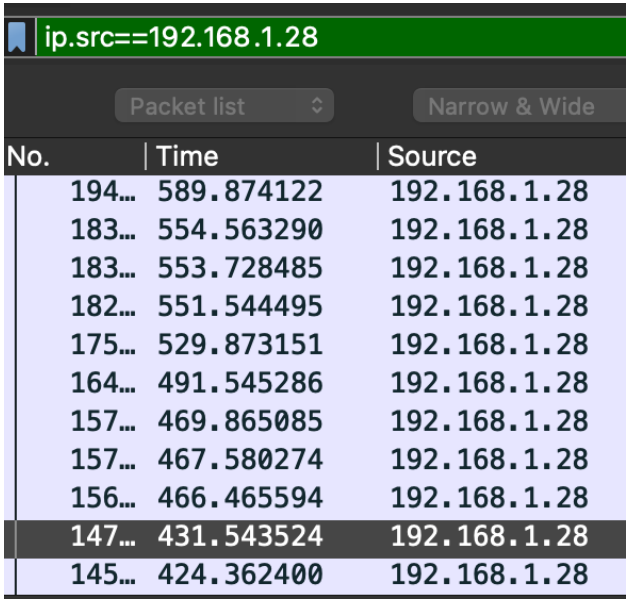
Using Wireshark

- 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



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.