Section 2: Wireshark + Physical Layer

CSE 461 Winter 2024

Administrivia

- Homework 1 is due Tomorrow (Jan 19th) 11:00 pm
- Project 1 is due January 25th at 11:00pm

Wireshark

- Let's retrospect why some of us started studying CS in the first place.
- It is shown in movies, coders having fancy screens hacking all sorts of stuff.
- Let’s try to do an in-class activity where we will actually hack a password from the network packets.

Download Wireshark!

- Download : https://www.wireshark.org/download.html

- User’s guide: https://www.wireshark.org/docs/wsug_html_chunked/

What is Wireshark

It’s a tool that captures and analyzes packets sent over the network

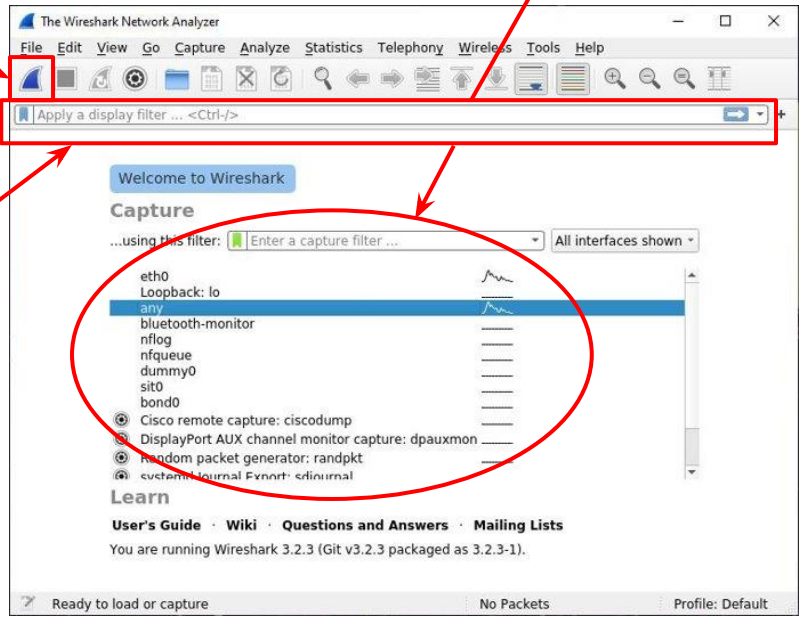
- Very commonly used in Network Forensics
- Captures all packets through a network interface (ethernet, WiFi)
- Analyzes packets and decodes raw data if the protocol is recognized
- Filters packets based on user’s input

Wireshark Interface

Start packet capture

Interface selection

Display filter for captured packets



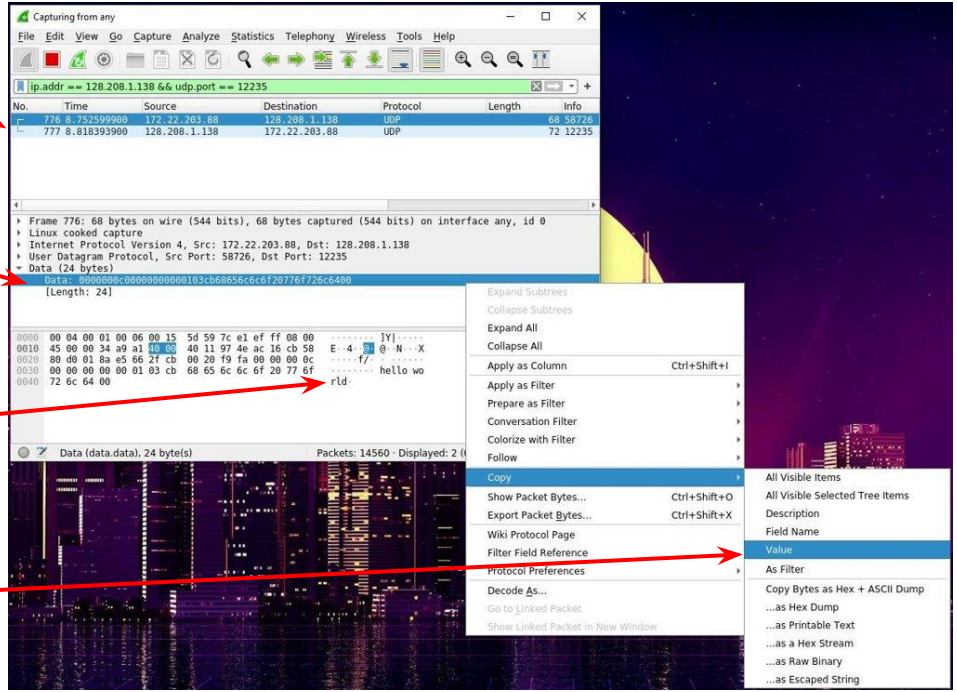
Wireshark Captured Packets Interface

Captured packets

Hexadecimal data contained in the UDP packet

ASCII decoding of data

Copy data value as hex string



Wireshark Filtering

- If you want to capture all TCP packets, write TCP in the filter. Same for UDP
- You can also track the packets going to a particular host using tcp contains “host”
- You can track packets going and coming back to a particular IP address.

Wireshark filtering

- Let’s try to hack password of a not secure website.
  - http://vbsca.ca/login/login.asp

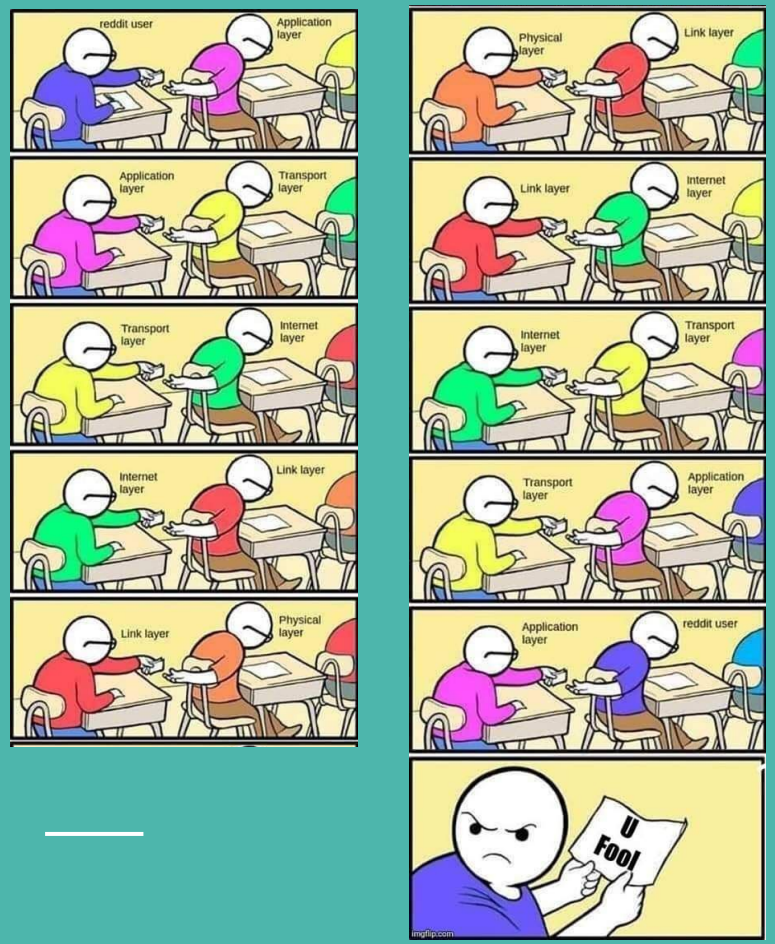
- This is very basic of Wireshark. It is capable of a lot more.
- Additional links:
  - https://www.wireshark.org/docs/
  - https://www.wireshark.org/docs/man-pages/wireshark-filter.html

Debugging P1 with Wireshark

Lots of packets are being sent while your computer is connected to a network.

- *Filtering packets to/from **attu's IP address***
  - How to find the IP address of attu?
    - Run `ifconfig` on attu (through SSH)
    - `nslookup attu2.cs.washington.edu` (from any computer)
    - traceroute will print out the IP address as well
  - `ip.addr == 128.208.1.138`
- *Filtering on the **port number***
  - `udp.port == 12235`
  - `tcp.port == <portNumber>`
- *Applying boolean logic to combine filters: ==, &&, ||, !*
  - ip.addr == 128.208.1.138 **&&** udp.port == 12235
  - Will only show packets to/from attu2 on udp port 12235

Exercises!


reddit user
Application layer
Application layer
Transport layer
Transport layer
Internet layer
Internet layer
Link layer
Link layer
Physical layer
Physical layer
Link layer
Link layer
Internet layer
Internet layer
Transport layer
Transport layer
Application layer
Application layer
reddit user
U Fool
imgflip.com

Ex1 - Network Stack

Read the following statements, and state whether they are TRUE or FALSE!

(a) The protocol stack of the Internet has an hourglass shape with a “narrow waist”. At the waist is the transport layer.

False. The network (IP) layer is at the waist.

(b) Packets traverse from the “topmost” layers to the “bottom-most” layers at the transmitter.

True. They traverse from the application layer to PHY.

(c) Alice has a noise-free channel and can transmit a single-tone to Bob. Since she can send only a single tone, i.e. Bandwidth = 0, her Shannon capacity is also zero.

False. Since the channel is “noise free”, her capacity is infinite.

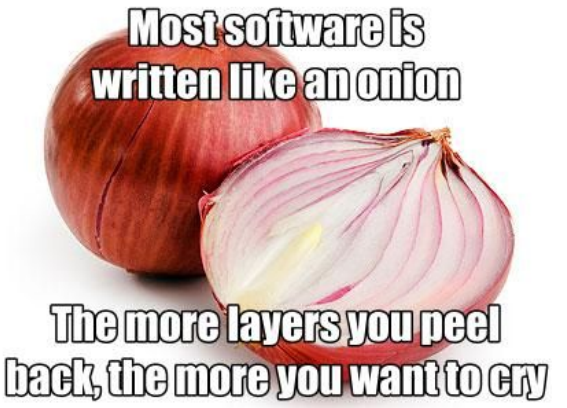
Ex1 - Network Stack

(d) The Internet mandates that if Apple Inc. makes the physical and datalink layer, Apple must implement corresponding the network layer as well.

False. IP does not depend on which lower layers it operates on

(e) If I inspect at a packet inside a wire, the PHY header will be the outermost header.

True. The lowermost layer has the outermost header.



Ex2 - Shannon Capacity

Find the Shannon channel capacity for a Wi-Fi channel with W_c = 80 MHz and SNR = 40 dB.

SNR (in dB) = 40 dB corresponds to
SNR (actual ratio) = 10^(40/10) = 10000

$C = 80 \log_2 (1+10000)$ Mbps
$= 80 \log_{10} (10001) / \log_{10} 2 = 1063$ Mbps

Ex3 - Shannon Capacity

Congrats! You've just won the Comcast '2Xfinity' offer. Comcast offered you one of the following upgrades to your wireless router. Either:

(Option #1) 2XPower - Double your transmission power, OR

(Option #2) 2XBandwidth: Double your bandwidth.

(a) As a greedy customer, which of these two schemes would you choose? Justify.

2XBandwidth... It is outside the log so can double your data rate.

(b) Comcast then noticed that they were using grossly sub-optimal pulse modulation to send you your data given your SNR and bandwidth. As a bonus, they offered to double the number of points in your constellation diagram. If you were getting 10 bits per pulse earlier, what percentage speedup do you expect? Justify.

You can send 11 bits now per pulse vs. 10, so it is a 10% speedup.