Computer Networks

Wireshark and Traceroute
Spring 2023

Administrivia

- Homework-2 is due April 24th at 11:00pm
- Project-1 is due April 17th 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.

Wireshark

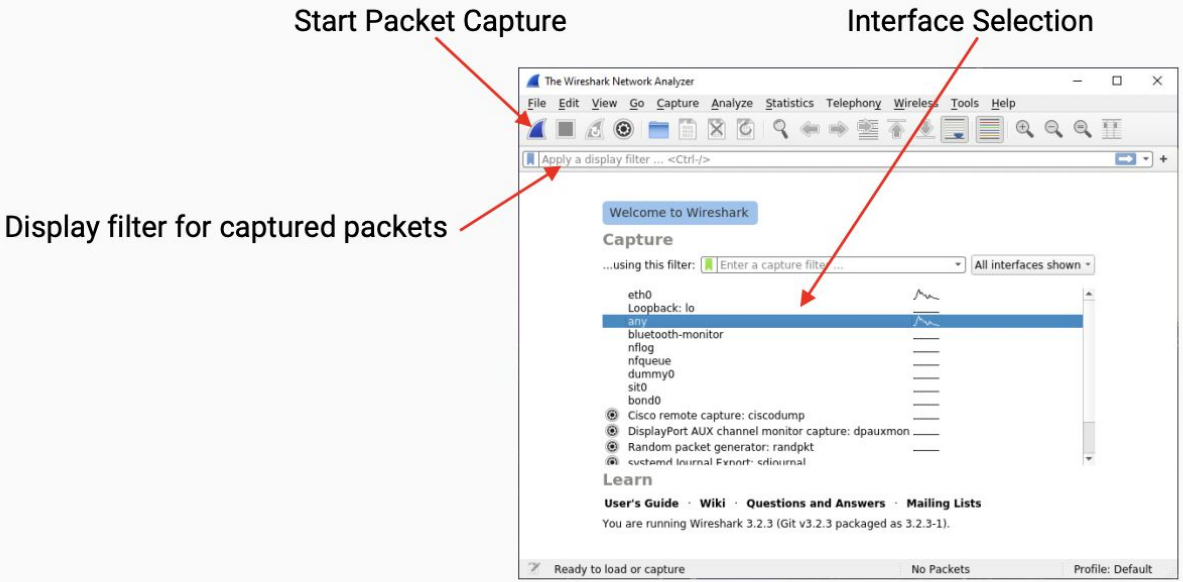
- Download : https://www.wireshark.org/download.html
- User’s guide: https://www.wireshark.org/docs/wsug_html_chunked/

What is Wireshark

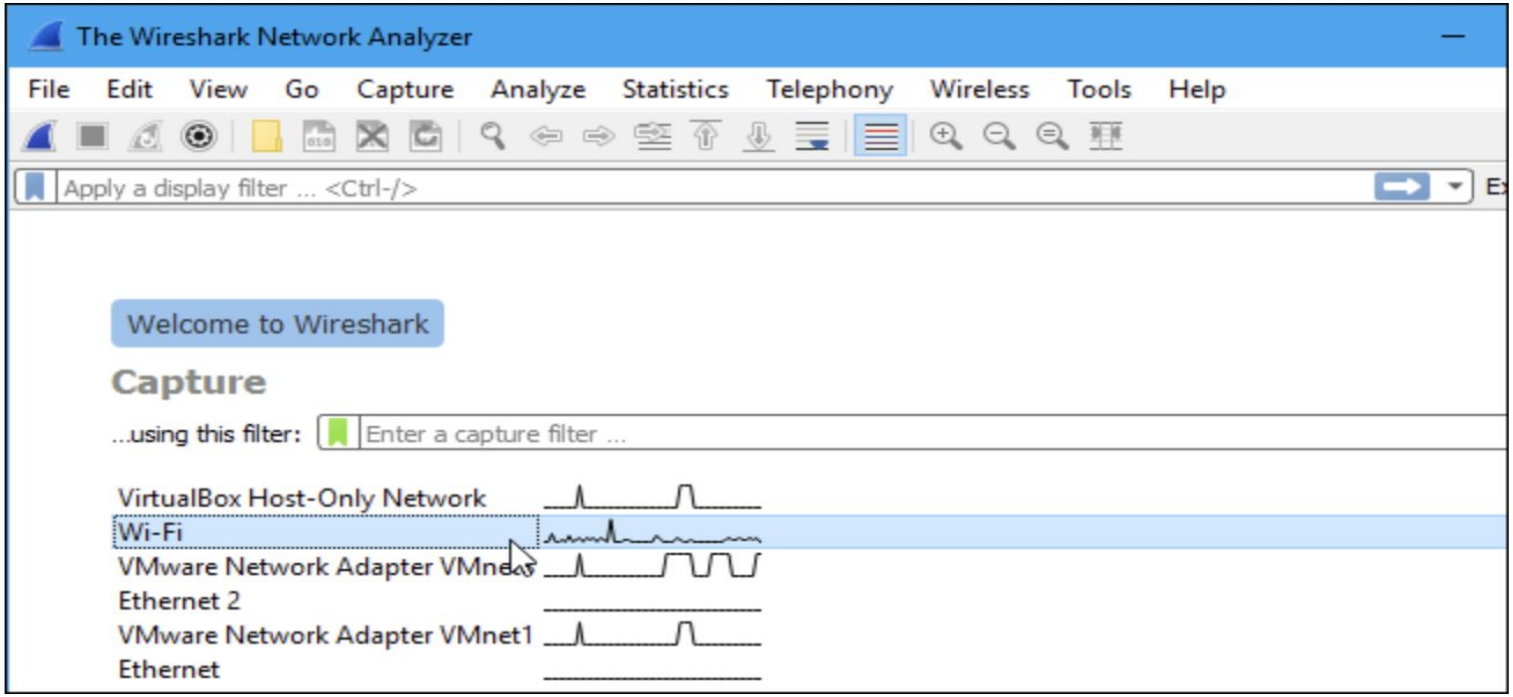
It’s a tool that captures and analyzes packets sent over the network

- 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

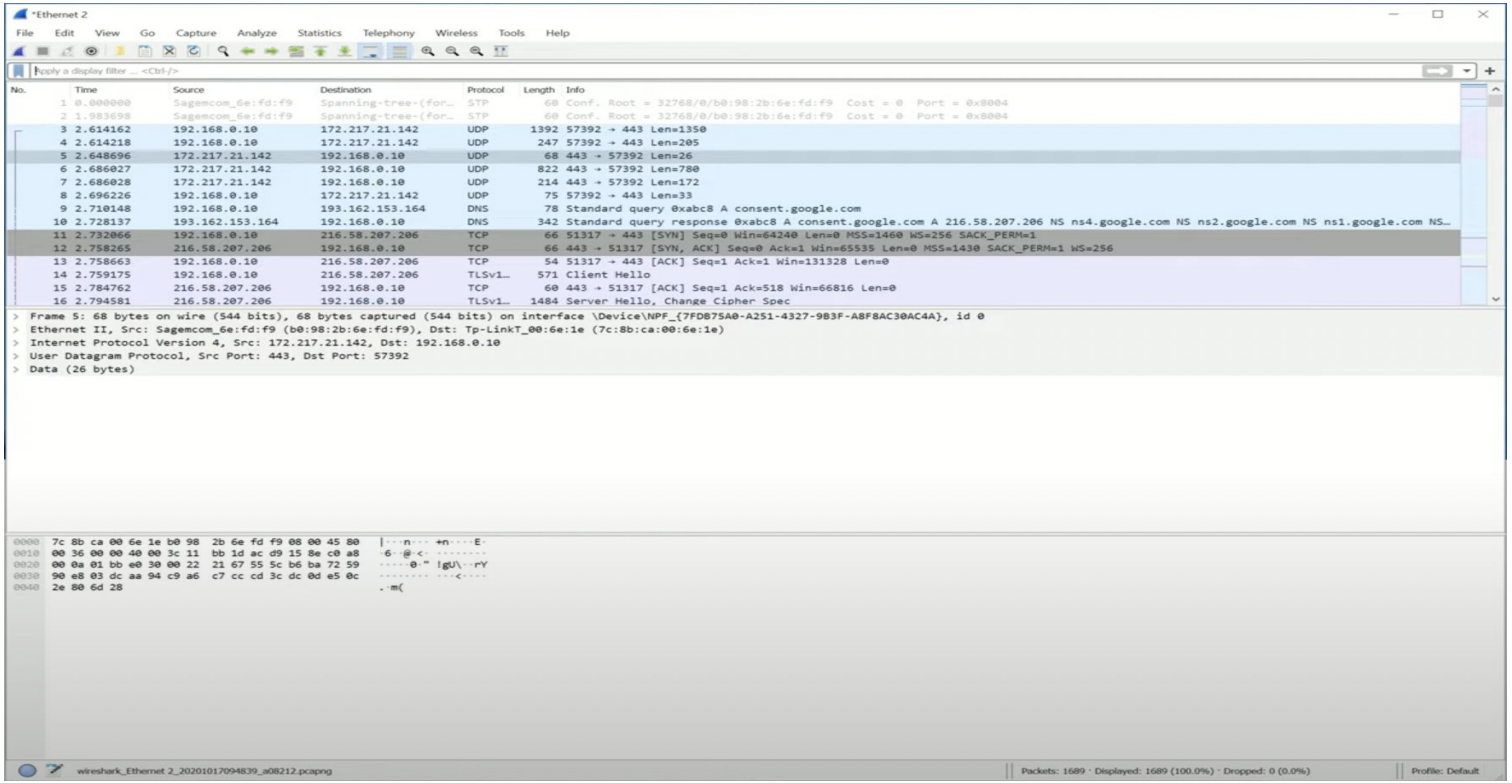
Wireshark Interface



Wireshark Interface



Wireshark Interface



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

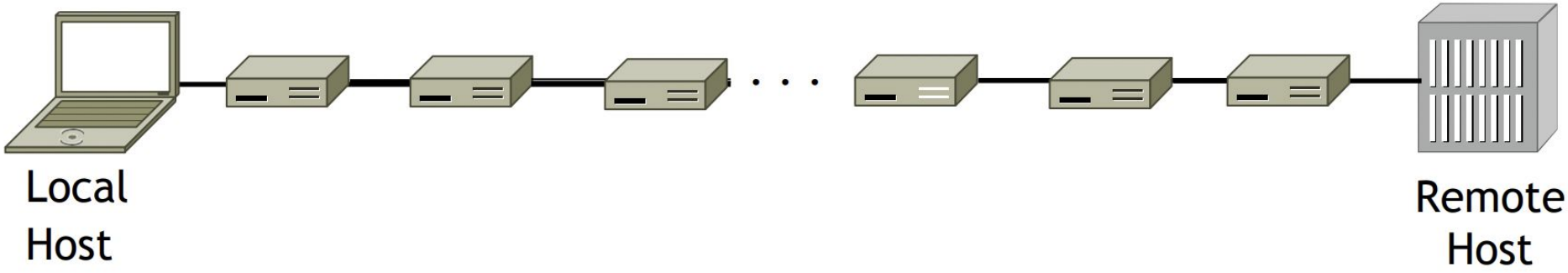
- This is very basic of Wireshark. It is capable of a lot more.
- Additional links:

https://www.wireshark.org/docs/

https://www.wireshark.org/docs/man-pages/wireshark-filter.html

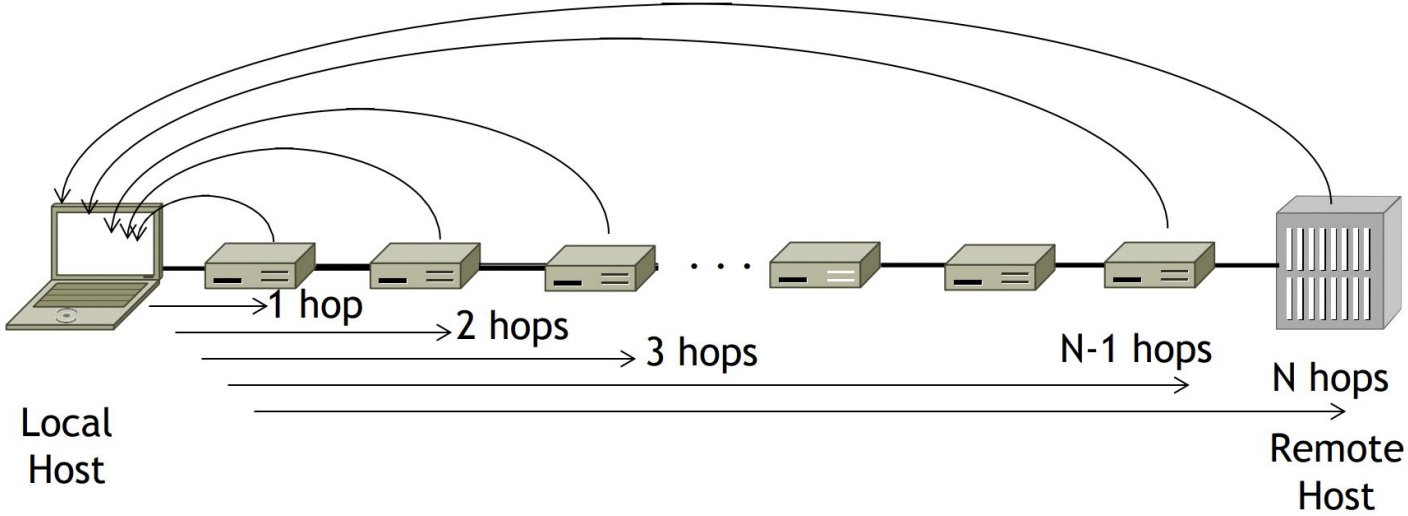
Traceroute

- We want to find network path from our system to a given remote host
- Core mechanism: Time-To-Live(TTL)
    - TTL defines the number of hops a packet will travel through until it is dropped
        - TTL is decremented every hop
        - Once TTL is 0 then the packet is dropped and a report is sent to the source



Traceroute

- Traceroute sends out three packets per TTL increment
    - To have 3 trials of data for each hop distance
- Each data point corresponds to the total RTT time



Using Traceroute

```
mohankukreja@Mohans-MacBook-Pro ~ % traceroute edstem.org
traceroute: Warning: edstem.org has multiple addresses; using 104.18.2.201
traceroute to edstem.org (104.18.2.201), 64 hops max, 52 byte packets
 1  * * *
 2  24.124.128.221 (24.124.128.221)  28.904 ms  37.510 ms  22.907 ms
 3  be-501-arsc1.seattle.wa.seattle.comcast.net (24.124.128.121)  18.038 ms  16.902 ms  19.033 ms
 4  be-36131-cs03.seattle.wa.ibone.comcast.net (68.86.93.9)  17.178 ms
    be-36111-cs01.seattle.wa.ibone.comcast.net (68.86.93.1)  18.991 ms
    be-36121-cs02.seattle.wa.ibone.comcast.net (68.86.93.5)  22.447 ms
 5  be-2212-pe12.seattle.wa.ibone.comcast.net (96.110.34.134)  40.134 ms
    be-2412-pe12.seattle.wa.ibone.comcast.net (96.110.34.142)  18.890 ms  16.272 ms
 6  50.208.235.222 (50.208.235.222)  18.734 ms  18.604 ms  29.908 ms
 7  108.162.243.11 (108.162.243.11)  23.056 ms
    172.71.140.3 (172.71.140.3)  112.339 ms
    172.71.144.3 (172.71.144.3)  33.574 ms
 8  104.18.2.201 (104.18.2.201)  26.846 ms  17.782 ms  19.221 ms
```

Thank You