
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

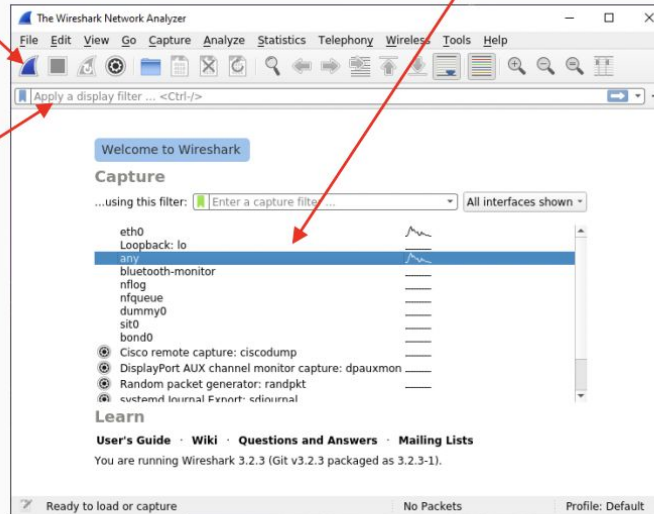
- Very commonly used in Network Forensics
- Captures all packets through a network interface (ethernet, WiFi)
- Analyzes packets and decodes raw data if the protocol is recognized
- Filters packets based on user's input

Wireshark Interface

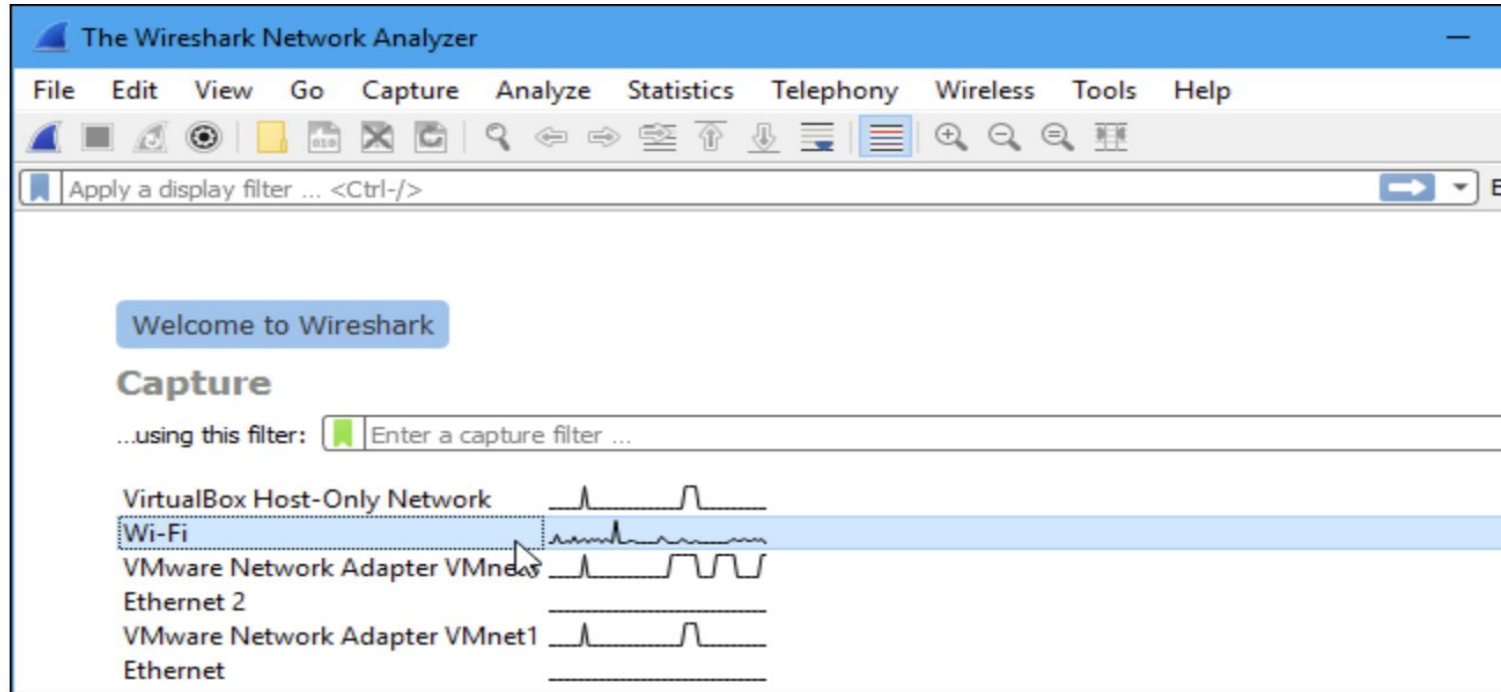
Start Packet Capture

Interface Selection

Display filter for captured packets



Wireshark Interface



Wireshark Interface

The screenshot displays the Wireshark interface for an Ethernet 2 capture. The main pane shows a list of 16 captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The selected packet (No. 5) is a UDP packet from 192.168.0.10 to 172.217.21.142, port 57392. The details pane below shows the structure of this packet: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Data (26 bytes). The hex dump at the bottom shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Sagemcom_6e:fd:f9	Spanning-tree-(for...	STP	60	Conf: Root = 32768/0/b0:98:2b:6e:fd:f9 Cost = 0 Port = 0x8004
2	1.983698	Sagemcom_6e:fd:f9	Spanning-tree-(for...	STP	60	Conf: Root = 32768/0/b0:98:2b:6e:fd:f9 Cost = 0 Port = 0x8004
3	2.614162	192.168.0.10	172.217.21.142	UDP	1392	57392 → 443 Len=1350
4	2.614218	192.168.0.10	172.217.21.142	UDP	247	57392 → 443 Len=205
5	2.648696	172.217.21.142	192.168.0.10	UDP	68	443 → 57392 Len=26
6	2.686027	172.217.21.142	192.168.0.10	UDP	822	443 → 57392 Len=780
7	2.686028	172.217.21.142	192.168.0.10	UDP	214	443 → 57392 Len=172
8	2.696226	192.168.0.10	172.217.21.142	UDP	75	57392 → 443 Len=33
9	2.710148	192.168.0.10	193.162.153.164	DNS	78	Standard query response 0xabc8 A consent.google.com A 216.58.207.206 NS ns4.google.com NS ns2.google.com NS ns1.google.com NS...
10	2.728137	193.162.153.164	192.168.0.10	DNS	342	Standard query response 0xabc8 A consent.google.com A 216.58.207.206 NS ns4.google.com NS ns2.google.com NS ns1.google.com NS...
11	2.732066	192.168.0.10	216.58.207.206	TCP	66	51317 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
12	2.758265	216.58.207.206	192.168.0.10	TCP	66	443 → 51317 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1430 SACK_PERM=1 WS=256
13	2.758663	192.168.0.10	216.58.207.206	TCP	54	51317 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
14	2.759175	192.168.0.10	216.58.207.206	TLSv1	571	Client Hello
15	2.784762	216.58.207.206	192.168.0.10	TCP	60	443 → 51317 [ACK] Seq=1 Ack=518 Win=66816 Len=0
16	2.794581	216.58.207.206	192.168.0.10	TLSv1	1484	Server Hello, Change Cipher Spec

> Frame 5: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface \Device\NPF_{7FD875A0-A251-4327-983F-ABF8AC30AC4A}, id 0
> Ethernet II, Src: Sagemcom_6e:fd:f9 (b0:98:2b:6e:fd:f9), Dst: Tp-LinkT_00:6e:1e (7c:8b:ca:00:6e:1e)
> Internet Protocol Version 4, Src: 172.217.21.142, Dst: 192.168.0.10
> User Datagram Protocol, Src Port: 443, Dst Port: 57392
> Data (26 bytes)

```
0000 7c 8b ca 00 6e 1e b0 98 2b 6e fd f9 08 00 45 80 |.....en....E-
0010 00 36 00 00 40 00 3c 11 bb 1d ac d9 15 Be c0 a8 |6.@<.....
0020 00 0a 01 b0 00 22 21 67 53 5c b6 ba 72 59 .....0 *lgU\rv
0030 90 e8 03 dc aa 94 c9 a6 c7 cc cd 3c dc 0d e5 0c |.....<.....
0040 2e 80 6d 28 |..=(
```

wireshark_Ethernet_2_20201017094839_j08212.pcapng | Packets: 1689 - Displayed: 1689 (100.0%) - Dropped: 0 (0.0%) | Profile: Default

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

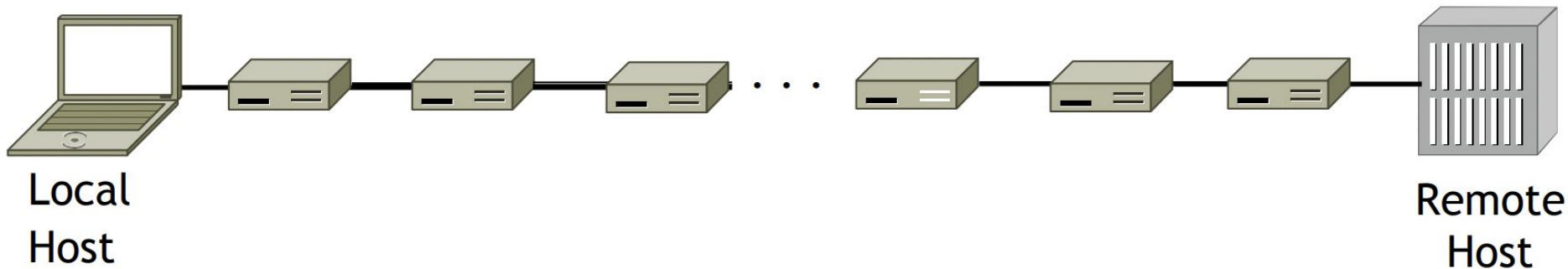
- Let's try to hack password of a not secure website.
 - <http://vbsca.ca/login/login.asp>
- This is very basic of Wireshark. It is capable of a lot more.
- Additional links:

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

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

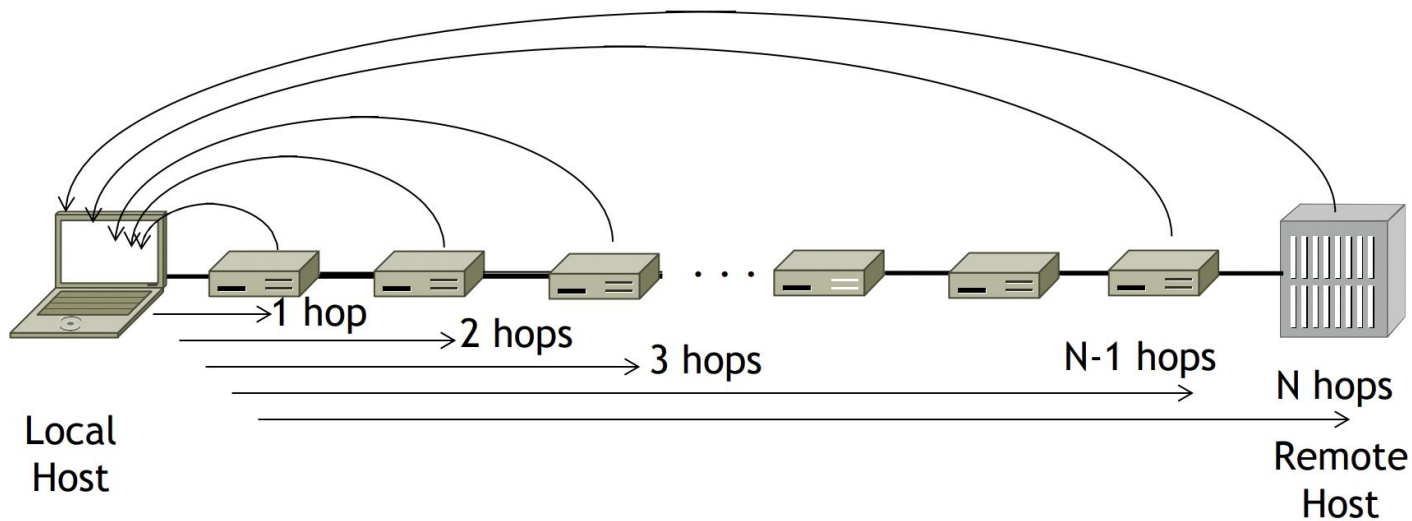
Traceroute

- 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-arisc1.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