



UNIVERSITY OF
CALGARY

WIRESHARK

CPSC 441 - Winter 2020
University of Calgary

Sina Keshvadi

In this presentation, I used slides from **Reza Gholizadeh** and Prof. **Mea Wang**.



What is Wireshark?

- **Wireshark is an open source packet analyzer**
 - Runs in Linux, Mac and Windows
 - Free of cost
- It is used for network troubleshooting, analysis, software and communication protocol development, and education.
- It is installed in lab machines, but need root access for full features



Wireshark Installation

- Unix System:
 - `sudo apt-get install wireshark`
- Windows:
 - <http://www.wireshark.org/download.html>
 - Tutorial in next slide



UNIVERSITY OF
CALGARY



tshark

- Terminal version of Wireshark
- Typically used when interactive user interface is not available

Install on Unix Machines by:

- `sudo apt-get install tshark`



BEFORE CAPTURING

Are you allowed to do this?

- Ensure that you have permission to capture packets from the network you are connected with
- Corporate policies or applicable laws may prohibit capturing data from the network

General Setup

- Operating system must support packet capturing, e.g. capture support is enabled
- You must have sufficient privileges to capture packets, e.g. root / administrator privileges
- Your computer's time and time zone settings should be correct



Choosing the Network Interface

Capture

...using this filter:

| | |
|-----------------|--|
| eno1 | |
| wlxc4e98410c50c | |
| any | |
| Loopback: lo | |
| nflog | |
| nfqueue | |
| usbmon1 | |
| usbmon2 | |
| usbmon3 | |
| usbmon4 | |

- Cisco remote capture: ciscodump
- Random packet generator: randpkt
- SSH remote capture: sshdump
- UDP Listener remote capture: udpdump



START CAPTURING PACKETS

After c
packet

The screenshot shows the Wireshark interface with a packet capture in progress on the Ethernet interface. The packet list shows several packets, with the selected packet (No. 1) being a Name query from 172.17.14.28 to 172.17.14.255. The packet details pane shows the following structure:

- Ethernet II, Src: Dell_7c:76:6a (00:26:b9:7c:76:6a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 172.17.14.28, Dst: 172.17.14.255
- User Datagram Protocol, Src Port: 137, Dst Port: 137
- NetBIOS Name Service

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000  ff ff ff ff ff ff 00 26  b9 7c 76 6a 08 00 45 00  .....& .|vj..E.
0010  00 4e 53 0a 00 00 80 11  72 57 ac 11 0e 1c ac 11  .NS.....rW.....
0020  0e ff 00 89 00 89 00 3a  db 78 df 32 01 10 00 01  .....:x.2....
0030  00 00 00 00 00 00 20 45  4d 45 50 45 48 45 4a 45  .....E MEPEHEJE
0040  4f 45 46 45 4f 43 4f 44  48 46 41 45 4c 43 4f 45  OEFEOD HFAELCOE
0050  44 45 50 45 4e 41 41 00  00 20 00 01              DEPENAA. . . .
```

The status bar at the bottom indicates: Ethernet: <live capture in progress> | Packets: 30 • Displayed: 30 (100.0%) | Profile: Default



ANALYZE CAPTURED PACKETS

Download the sample packet trace from my webpage and we will analyze that traffic.

<https://pages.cpsc.ucalgary.ca/~sina.keshvadi1/cpsc441/>



Capture Traffic

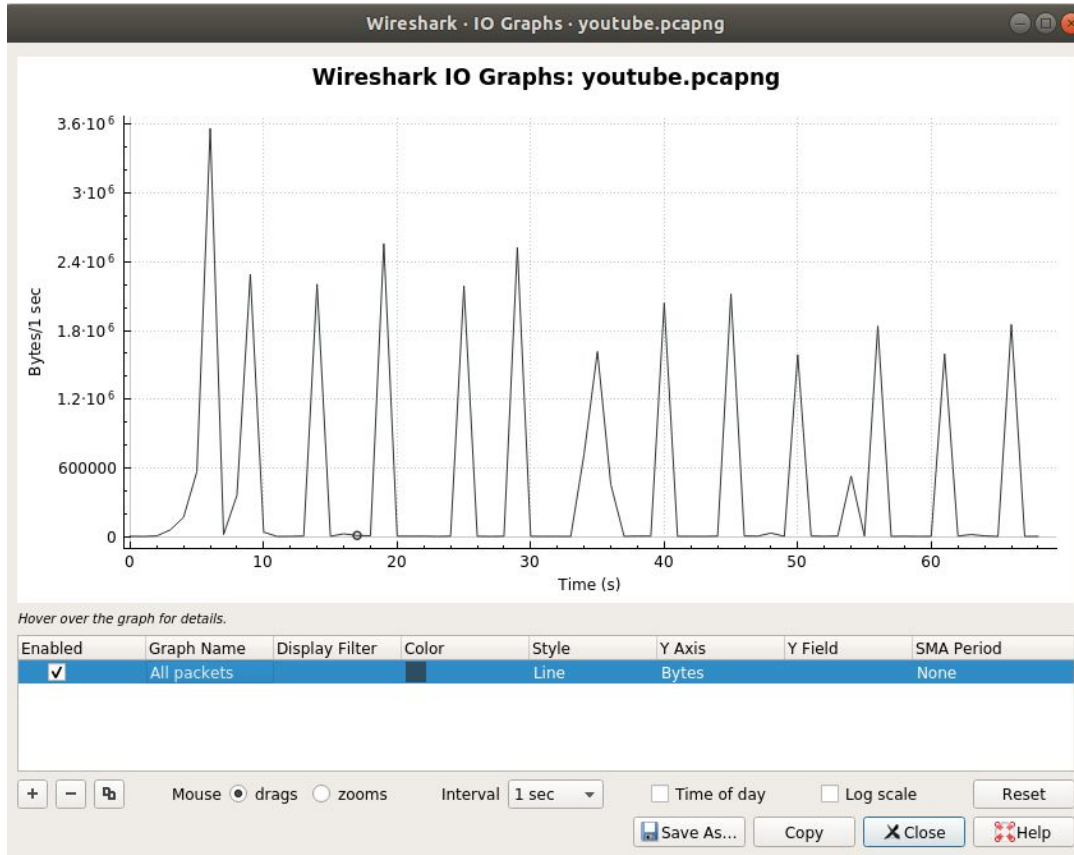
- From TED.Com
- From YouTube.com



Analyze Traffic

- Statistics -> I/O Graph
- Statistics -> Conversations
- Apply as Filters
- Follow -> TCP Stream
- Colors in Wireshark
- Packet Details

Statistics -> I/O Graph





Statistics -> Conversations

Wireshark · Conversations · youtube.pcapng

| Ethernet · 75 | IPv4 · 83 | IPv6 · 23 | TCP · 11 | UDP · 168 | | | | | | | |
|----------------|-----------------|-----------|----------|---------------|-------------|---------------|-------------|------------|----------|--------------|--------------|
| Address A | Address B | Packets | Bytes | Packets A → B | Bytes A → B | Packets B → A | Bytes B → A | Rel Start | Duration | Bits/s A → B | Bits/s B → A |
| 172.17.20.22 | 173.194.152.89 | 25,706 | 29 M | 5,066 | 1,182 k | 20,640 | 28 M | 5.916209 | 60.7824 | 155 k | 3,761 |
| 172.17.20.22 | 172.217.14.214 | 534 | 630 k | 66 | 6,366 | 468 | 624 k | 3.671211 | 2.9286 | 17 k | 1,704 |
| 172.17.20.22 | 172.217.3.174 | 187 | 184 k | 51 | 7,098 | 136 | 177 k | 6.101118 | 59.9985 | 946 | 23 |
| 172.17.20.22 | 216.58.193.78 | 233 | 178 k | 104 | 84 k | 129 | 94 k | 2.853510 | 60.4379 | 11 k | 12 |
| 172.17.20.22 | 216.58.193.65 | 70 | 61 k | 25 | 1,930 | 45 | 59 k | 5.784519 | 15.5652 | 991 | 30 |
| 172.17.20.22 | 172.217.14.206 | 54 | 35 k | 33 | 27 k | 21 | 7,814 | 3.548987 | 59.8682 | 3,730 | 1,04 |
| 172.17.20.125 | 239.242.6.7 | 35 | 30 k | 35 | 30 k | 0 | 0 | 0.530170 | 68.0183 | 3,564 | |
| 172.17.20.7 | 172.17.20.255 | 69 | 21 k | 69 | 21 k | 0 | 0 | 0.263677 | 68.0040 | 2,475 | |
| 172.17.20.186 | 172.17.20.255 | 68 | 20 k | 68 | 20 k | 0 | 0 | 0.292654 | 67.9402 | 2,442 | |
| 172.17.20.197 | 255.255.255.255 | 32 | 13 k | 32 | 13 k | 0 | 0 | 0.1796125 | 30.2702 | 3,678 | |
| 172.17.20.22 | 172.217.14.195 | 37 | 13 k | 19 | 7,597 | 18 | 5,930 | 25.890196 | 37.5242 | 1,619 | 1,26 |
| 172.17.20.22 | 172.217.3.163 | 21 | 12 k | 11 | 5,600 | 10 | 7,297 | 51.557281 | 15.0413 | 2,978 | 3,88 |
| 172.17.20.22 | 172.217.14.197 | 29 | 12 k | 13 | 3,227 | 16 | 9,630 | 63.695681 | 0.2578 | 100 k | 298 |
| 172.17.20.173 | 255.255.255.255 | 16 | 6,944 | 16 | 6,944 | 0 | 0 | 0.14021595 | 0.0269 | 2,067 k | |
| 172.17.20.173 | 172.17.20.255 | 57 | 6,612 | 57 | 6,612 | 0 | 0 | 0.000000 | 64.4656 | 820 | |
| 172.17.20.7 | 230.0.0.1 | 69 | 6,348 | 69 | 6,348 | 0 | 0 | 0.869501 | 68.0325 | 746 | |
| 172.17.20.238 | 230.0.0.1 | 69 | 6,348 | 69 | 6,348 | 0 | 0 | 0.766105 | 68.0241 | 746 | |
| 172.17.20.173 | 230.0.0.1 | 67 | 6,164 | 67 | 6,164 | 0 | 0 | 0.418415 | 68.0323 | 724 | |
| 172.17.20.22 | 216.58.217.46 | 13 | 4,950 | 7 | 2,265 | 6 | 2,685 | 23.494252 | 45.0710 | 402 | 47 |
| 172.17.20.197 | 239.255.255.250 | 7 | 4,886 | 7 | 4,886 | 0 | 0 | 0.18656657 | 7.5300 | 5,190 | |
| 172.17.20.22 | 172.217.3.170 | 10 | 4,851 | 5 | 2,437 | 5 | 2,414 | 48.213855 | 15.0650 | 1,294 | 1,28 |
| 172.17.20.22 | 199.212.24.45 | 15 | 4,587 | 7 | 2,013 | 8 | 2,574 | 5.533255 | 15.1997 | 1,059 | 1,35 |
| 172.17.20.173 | 224.0.0.252 | 68 | 4,468 | 68 | 4,468 | 0 | 0 | 0.48505565 | 14.8691 | 2,403 | |
| 172.17.20.132 | 239.255.255.250 | 27 | 3,969 | 27 | 3,969 | 0 | 0 | 0.343650 | 67.3126 | 471 | |
| 172.17.20.193 | 255.255.255.255 | 9 | 3,834 | 9 | 3,834 | 0 | 0 | 0.3771153 | 60.4133 | 507 | |
| 172.17.20.197 | 172.17.20.255 | 8 | 3,480 | 8 | 3,480 | 0 | 0 | 0.17808419 | 30.2577 | 920 | |
| 3.215.41.219 | 172.17.20.22 | 10 | 3,392 | 4 | 847 | 6 | 2,545 | 2.873304 | 63.2245 | 107 | 32 |
| 172.17.20.125 | 255.255.255.255 | 14 | 2,968 | 14 | 2,968 | 0 | 0 | 0.9365840 | 30.4140 | 780 | |
| 162.125.35.134 | 172.17.20.22 | 5 | 2,448 | 3 | 413 | 2 | 2,035 | 38.530763 | 0.0871 | 37 k | 186 |
| 172.17.20.193 | 172.17.20.255 | 5 | 2,068 | 5 | 2,068 | 0 | 0 | 0.3773864 | 60.4104 | 273 | |
| 74.125.20.189 | 172.17.20.22 | 18 | 1,687 | 10 | 880 | 8 | 807 | 1.970613 | 62.4284 | 112 | 10 |
| 172.17.12.101 | 172.17.20.22 | 14 | 1,494 | 7 | 846 | 7 | 648 | 5.830754 | 57.8648 | 116 | 8 |
| 172.17.20.27 | 224.0.0.22 | 24 | 1,440 | 24 | 1,440 | 0 | 0 | 0.8223769 | 56.2951 | 204 | |
| 172.17.20.186 | 239.255.255.250 | 6 | 1,050 | 6 | 1,050 | 0 | 0 | 0.46675647 | 15.0113 | 559 | |
| 172.17.20.5 | 239.255.255.250 | 4 | 864 | 4 | 864 | 0 | 0 | 0.39300153 | 3.0022 | 2,302 | |
| 172.17.20.27 | 239.255.255.250 | 4 | 864 | 4 | 864 | 0 | 0 | 0.42249183 | 3.0022 | 2,302 | |
| 172.17.20.173 | 239.255.255.250 | 4 | 864 | 4 | 864 | 0 | 0 | 0.53461949 | 3.0016 | 2,302 | |
| 172.17.20.238 | 239.255.255.250 | 4 | 864 | 4 | 864 | 0 | 0 | 0.37387638 | 3.0010 | 2,303 | |
| 172.17.20.22 | 239.255.255.250 | 4 | 856 | 4 | 856 | 0 | 0 | 0.8551270 | 3.0012 | 2,281 | |
| 172.17.20.160 | 239.255.255.250 | 4 | 836 | 4 | 836 | 0 | 0 | 0.53500108 | 3.0037 | 2,238 | |

☐ Name resolution☐ Limit to display filter☐ Absolute start time

Conversation Types ▾

CopyFollow Stream...Graph...CloseHelp



Wireshark Coloring Rules

Wireshark · Coloring Rules · Default

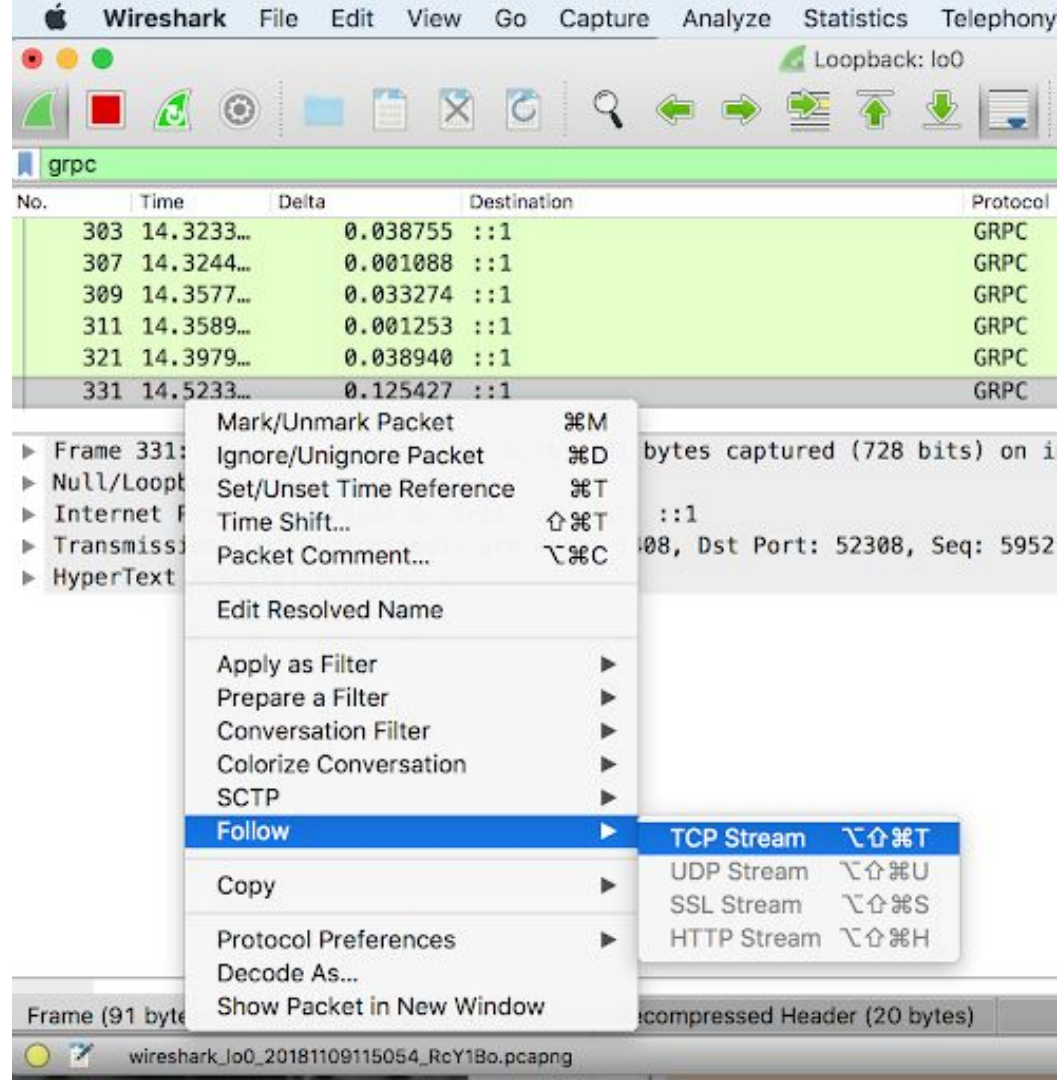
| Name | Filter |
|---|---|
| <input checked="" type="checkbox"/> Bad TCP | tcp.analysis.flags && !tcp.analysis.window_update |
| <input checked="" type="checkbox"/> HSRP State Change | hsrp.state != 8 && hsrp.state != 16 |
| <input checked="" type="checkbox"/> Spanning Tree Topology Change | stp.type == 0x80 |
| <input checked="" type="checkbox"/> OSPF State Change | ospf.msg != 1 |
| <input checked="" type="checkbox"/> ICMP errors | icmp.type eq 3 icmp.type eq 4 icmp.type eq 5 icmp.type eq 11 icmpv6.type eq 1 icmpv6.type eq 2 |
| <input checked="" type="checkbox"/> ARP | arp |
| <input checked="" type="checkbox"/> ICMP | icmp icmpv6 |
| <input checked="" type="checkbox"/> TCP RST | tcp.flags.reset eq 1 |
| <input checked="" type="checkbox"/> SCTP ABORT | sctp.chunk_type eq ABORT |
| <input checked="" type="checkbox"/> TTL low or unexpected | (! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && ! ipim) (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.1) |
| <input checked="" type="checkbox"/> Checksum Errors | eth.fcs_bad==1 ip.checksum_bad==1 tcp.checksum_bad==1 udp.checksum_bad==1 sctp.checksum_bad==1 |
| <input checked="" type="checkbox"/> SMB | smb nbss nbns nbipx ipxsap netbios |
| <input checked="" type="checkbox"/> HTTP | http tcp.port == 80 http2 |
| <input checked="" type="checkbox"/> IPX | ipx spx |
| <input checked="" type="checkbox"/> DCERPC | dcerpc |
| <input checked="" type="checkbox"/> Routing | hsrp eigrp ospf bgp cdp vrrp carp gvrp igmp ismp |
| <input checked="" type="checkbox"/> TCP SYN/FIN | tcp.flags & 0x02 tcp.flags.fin == 1 |
| <input checked="" type="checkbox"/> TCP | tcp |
| <input checked="" type="checkbox"/> UDP | udp |
| <input checked="" type="checkbox"/> Broadcast | eth[0] & 1 |

Double click to edit. Drag to move. Rules are processed in order until a match is found.

+ - [icon] Foreground Background

Help Import... Export... Cancel OK

Follow a TCP stream





Handshaking in a TCP stream

| Time in this TCP stream | Info |
|-------------------------|---|
| 0.000000000 | 46839 → 8888 [SYN] Seq=0 Win=65535 Len=0 MSS=1386 SACK_PERM=1 TSval=2408036 TSecr=1796839275 |
| 0.000015368 | 8888 → 46839 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=1796839283 TSecr=2408039 |
| 0.007223869 | 46839 → 8888 [ACK] Seq=1 Ack=1 Win=87808 Len=0 TSval=2408039 TSecr=1796839275 |
| 0.000886199 | CONNECT e.serverbid.com:443 HTTP/1.1 |
| 0.000018615 | 8888 → 46839 [ACK] Seq=1 Ack=233 Win=65024 Len=0 TSval=1796839283 TSecr=2408039 |
| 0.048549447 | HTTP/1.1 200 Connection established |
| 0.004299781 | 46839 → 8888 [ACK] Seq=233 Ack=40 Win=87808 Len=0 TSval=2408055 TSecr=1796839331 |
| 0.009252944 | Client Hello |
| 0.000006288 | 8888 → 46839 [ACK] Seq=40 Ack=750 Win=64512 Len=0 TSval=1796839345 TSecr=2408057 |
| 0.117146695 | Server Hello |
| 0.057843697 | 46839 → 8888 [ACK] Seq=750 Ack=139 Win=87808 Len=0 TSval=2408107 TSecr=1796839462 |
| 0.000022824 | Change Cipher Spec, Encrypted Handshake Message |
| 0.009846804 | 46839 → 8888 [ACK] Seq=750 Ack=190 Win=87808 Len=0 TSval=2408112 TSecr=1796839520 |
| 0.000373294 | Change Cipher Spec, Encrypted Handshake Message |
| 0.000004096 | 8888 → 46839 [ACK] Seq=190 Ack=801 Win=64512 Len=0 TSval=1796839530 TSecr=2408112 |
| 0.000505466 | Application Data |
| 0.000003867 | 8888 → 46839 [ACK] Seq=190 Ack=894 Win=64512 Len=0 TSval=1796839531 TSecr=2408113 |
| 0.000863764 | Application Data, Application Data |
| 0.000004633 | 8888 → 46839 [ACK] Seq=190 Ack=1699 Win=64128 Len=0 TSval=1796839532 TSecr=2408113 |
| 0.042017285 | Application Data |



Packet in network layers

- Layers
 - Frame
 - Ethernet
 - IP
 - TCP

Wireshark · Packet 37349 · wireshark.pcap.pcapng

▶ Frame 37349: 116 bytes on wire (928 bits), 116 bytes captured (928 bits) on interface 0

▶ Ethernet II, Src: Tp-LinkT_10:c5:0c (c4:e9:84:10:c5:0c), Dst: Cisco_ff:fc:30 (00:08:e3:ff:fc:30)

▶ Internet Protocol Version 4, Src: 10.13.126.184, Dst: 10.13.135.6

▶ Transmission Control Protocol, Src Port: 8888, Dst Port: 46839, Seq: 190, Ack: 1699, Len: 50

▶ Hypertext Transfer Protocol

▶ Secure Sockets Layer

| | | |
|------|---|------------------------|
| 0000 | 00 08 e3 ff fc 30 c4 e9 84 10 c5 0c 08 00 45 00 |0.. ..E. |
| 0010 | 00 66 f8 ee 40 00 40 06 27 cb 0a 0d 7e b8 0a 0d | ..f..@..@.. '.....~... |
| 0020 | 87 06 22 b8 b6 f7 b4 3c d5 e3 3d 50 88 b6 80 18 | ..".< ..=P.... |
| 0030 | 01 f5 0b 48 00 00 01 01 08 0a 6b 19 98 97 00 24 | ...H.....k....\$ |
| 0040 | be b2 17 03 03 00 2d 00 00 00 00 00 00 01 7a | ...-.....z |
| 0050 | d7 0e 0b 7b 62 f0 47 7a 53 89 c0 6f 79 41 a2 a1 | ...{b·Gz S...oyA... |
| 0060 | ea 85 04 5b fd 6c a7 80 2b ec 04 9d 8e 49 41 50 | ...[·1... +....IAP |
| 0070 | 7a 2e 4f a1 | z.0. |



WIRESHARK FILTERS

- Capture Filters
 - Removes unwanted packets from a packet trace and only retrieve the packets of interest
- Display Filters
 - Hides unwanted packets based on your filter definition



DISPLAY FILTER EXAMPLE

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 80 || udp.port == 80

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|------------|----------------|----------------|----------|--------|-----------------------------------|
| 3786 | 124.288732 | 172.17.14.47 | 34.204.112.229 | TCP | 66 | 64679 → 80 [SYN] Seq=0 Win=642... |
| 3867 | 124.346886 | 34.204.112.229 | 172.17.14.47 | TCP | 66 | 80 → 64679 [SYN, ACK] Seq=0 Ac... |
| 3869 | 124.346930 | 172.17.14.47 | 34.204.112.229 | TCP | 54 | 64679 → 80 [ACK] Seq=1 Ack=1 W... |
| 3870 | 124.347015 | 172.17.14.47 | 34.204.112.229 | HTTP | 954 | GET /master/?1=1&HASH=83ec&RED... |
| 3872 | 124.347860 | 34.204.112.229 | 172.17.14.47 | TCP | 60 | 80 → 64679 [ACK] Seq=1 Ack=901... |
| 4020 | 124.419284 | 34.204.112.229 | 172.17.14.47 | TCP | 60 | [TCP Window Update] 80 → 64679... |
| 4021 | 124.420773 | 34.204.112.229 | 172.17.14.47 | HTTP | 1169 | HTTP/1.1 302 Found |
| 4113 | 124.460181 | 172.17.14.47 | 54.85.54.13 | TCP | 66 | 64693 → 80 [SYN] Seq=0 Win=642... |
| 4117 | 124.461311 | 172.17.14.47 | 34.204.112.229 | TCP | 54 | 64679 → 80 [ACK] Seq=901 Ack=1... |
| 4258 | 124.523126 | 54.85.54.13 | 172.17.14.47 | TCP | 66 | 80 → 64693 [SYN, ACK] Seq=0 Ac... |

> Frame 3786: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

> Ethernet II, Src: Dell_dc:22:2d (34:17:eb:dc:22:2d), Dst: HewlettP_9d:62:00 (58:20:b1:9d:62:00)

> Internet Protocol Version 4, Src: 172.17.14.47, Dst: 34.204.112.229

> Transmission Control Protocol, Src Port: 64679, Dst Port: 80, Seq: 0, Len: 0

0000 58 20 b1 9d 62 00 34 17 eb dc 22 2d 08 00 45 00 X ..b.4. .."-...E.

0010 00 34 36 ba 40 00 80 06 00 00 ac 11 0e 2f 22 cc .46.@.../".

Frame (frame), 66 bytes | Packets: 10289 · Displayed: 16 (0.2%) | Profile: Default



ANALYZE web.pcap file

- Write **http** as filter
- Find request to Prof. Carey's page
- Right click on it and then Follow → TCP Stream
 - Could you recognize handshaking?
 - SYN and ACK?
 - GET request?
 - Response?
 - Could you read the transferred data? Why?
 - **Not Modified!** What means?



ANALYZE A HTTP REQUEST

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

| No. | Time | Source | Destination | Protocol | Length | Time since previous frame in this TCP stream | Info |
|------|--------------|--------------|--------------|----------|--------|--|---|
| 3125 | 15.321548394 | 136.159.2.17 | 172.17.20.22 | HTTP | 5732 | 0.000621352 | HTTP/1.1 200 OK (text/html) |
| 3142 | 15.853575291 | 172.17.20.22 | 136.159.2.17 | HTTP | 2558 | 0.538671408 | GET /~carey/CPSC441/exams.html HTTP/1.1 |
| 3144 | 15.854445825 | 136.159.2.17 | 172.17.20.22 | HTTP | 2835 | 0.000677697 | HTTP/1.1 200 OK (text/html) |
| 3161 | 16.392075017 | 172.17.20.22 | 136.159.2.17 | HTTP | 2554 | 0.548011620 | GET /~carey/CPSC441/grading.html HTTP/1.1 |
| 3163 | 16.392944351 | 136.159.2.17 | 172.17.20.22 | HTTP | 2628 | 0.000676794 | HTTP/1.1 200 OK (text/html) |
| 3170 | 16.400360757 | 172.17.20.22 | 136.159.2.17 | HTTP | 2554 | 0.544006708 | GET /~carey/CPSC441/links.html HTTP/1.1 |

▶ Frame 3144: 2835 bytes on wire (22680 bits), 2835 bytes captured (22680 bits) on interface 0
▶ Ethernet II, Src: HewlettP_9d:62:00 (58:20:b1:9d:62:00), Dst: Dell_e0:73:46 (98:90:96:e0:73:46)
▶ Internet Protocol Version 4, Src: 136.159.2.17, Dst: 172.17.20.22
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 41616, Seq: 1, Ack: 2493, Len: 2769
▼ Hypertext Transfer Protocol
▶ HTTP/1.1 200 OK\r\n
Date: Fri, 24 Jan 2020 22:53:08 GMT\r\n
Server: Apache/2.2.15 (Scientific Linux)\r\n
Last-Modified: Mon, 06 Jan 2020 20:18:05 GMT\r\n
ETag: "442465f-9b7-59b7e5b7164ab"\r\n
Accept-Ranges: bytes\r\n
▼ Content-Length: 2487\r\n
[Content length: 2487]
Connection: close\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.000870534 seconds]
[Request in frame: 3142]
[Request URI: http://pages.cpsc.ucalgary.ca/~carey/CPSC441/exams.html]
File Data: 2487 bytes
▼ Line-based text data: text/html (84 lines)
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">\r\n\r\n<html>\r\n\r\n<meta content="text/html; charset=utf-8" http-equiv="Content-Type" >\r\n<link href="cpsc441.css" rel="stylesheet" type="text/css" >\r\n



Filters

- `tcp.port == 443`
- `ip.addr == 10.43.54.65`
- `ip.src == 10.43.54.65`
- `ip.dst == 10.43.54.65`
- `ip.addr != 10.43.54.65`
- `http`
- `dns`
- `http.request.method == "GET"`



FILTER EXAMPLES

In display Filter

- `tcp.port == 80`
- `eth.addr == 00:00:5e:00:53:00`
- `tcp.port == 80 || udp.port == 80`
- `tcp.port == 80 && ip.src == 172.17.14.47`
- `http.request.version=="HTTP/1.1"`
- `tcp.dstport == 25`

In capture filter

- `tcp port 80`
- `ip src host 136.159.5.20`
- `host 136.159.5.1`
(source/destination)
- (src host 23.36.178.81 and not
dst host 172.17.14.47) and tcp
dst portrange 200-10000



Capture Traffic

- tshark has to be run with “root” privileges
 - sudo (superuser mode) while running tshark
- Identify the network interface to monitor
 - To list all interfaces in a machine: `ifconfig -a`
- Create a destination folder to save the packet trace file
 - In your home directory (/home/ubuntu): `mkdir dump`
 - Change ownership of the dump folder to root: `sudo chown -R root dump`
- Capture traffic
- `sudo tshark -i eth0 -w dump/filedump0`
 - Option “i” to specify interface name
 - Option “w” to specify destination of packet trace file



UNIVERSITY OF
CALGARY

More Wireshark Exercise?

Please refer to Wireshark exercise in TextBook.

Email me if you have questions.



REFERENCES

- <https://en.wikipedia.org/wiki/Wireshark>
- <https://wiki.wireshark.org>
- <https://www.wireshark.org>