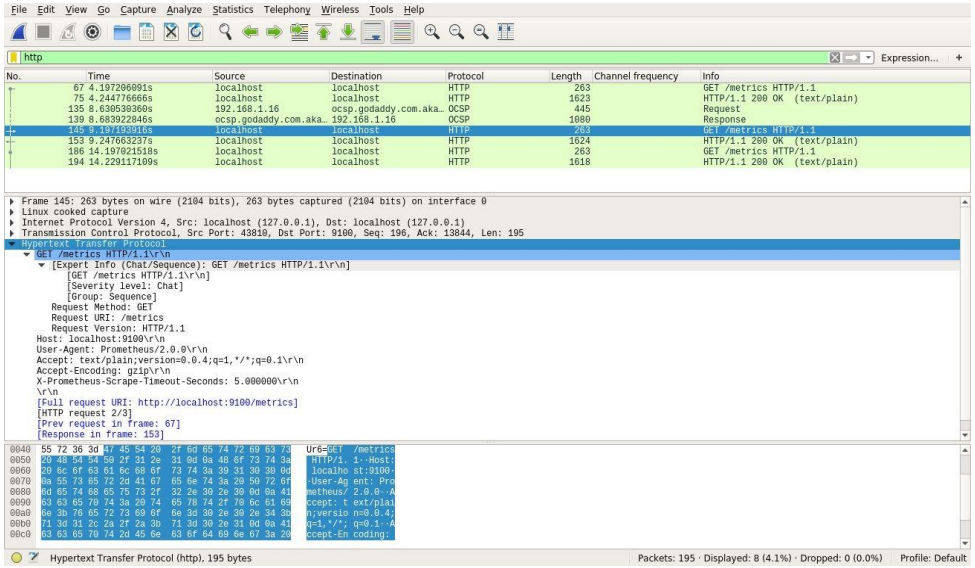
Computer Networks Tutorial
COL 334/ COL 672

What is it

- Wireshark is an Open Source Software packet sniffing tool
- It copies messages being sent from and received by your computer.
- It displays the contents of various protocol fields of the captured messages.
- It is mainly used for troubleshooting or debugging network problems.



Features

- Available for Unix (flavors) and Windows.
- Capture live packet data from a network interface.
- Save captured packet data.
- Export some or all packets in a number of capture file formats.
- Filter packets on many criteria.
- Search for packets on many criteria.
- Create various statistics.
- Colorize packet display based on filters.
- Display packets with very detailed protocol information.
- Open files containing packet data captured with tcpdump/WinDump
- Import packets from text files containing hex dumps of packet data.

Install and Use Wireshark on Ubuntu Linux

- *sudo apt install wireshark*
- Check for the latest version of wireshark using the following command
  - *apt show wireshark*
  - current stable release of Wireshark is 3.6
  - Update using:
    - *sudo add-apt-repository ppa:wireshark-dev/stable*
    - *sudo apt update*
    - *sudo apt install wireshark*
- To run wireshark after installation:
  - *sudo wireshark*

Installing from source code (ubuntu) – Download Wireshark

Unpack the source from its compressed tar file. If you are using Linux or your version of UNIX uses GNU tar you can use the following command:

tar xJf wireshark-3.4.7.tar.xz

In other cases you will have to use the following commands:

xz -d wireshark-3.4.7.tar.xz

1. tar xf wireshark-3.4.7.tar
2. Create a directory to build Wireshark in and change to it.
   a. mkdir build
   b. cd build

3. Configure your source so it will build correctly for your version of UNIX. You can do this with the following command:

   cmake ../wireshark-3.4.7

   Build the sources.

   make

   Once you have built Wireshark with make above, you should be able to run it by entering run/wireshark.

4. Install the software in its final destination.
5. make install
   Once you have installed Wireshark with make install above, you should be able to run it by entering wireshark.

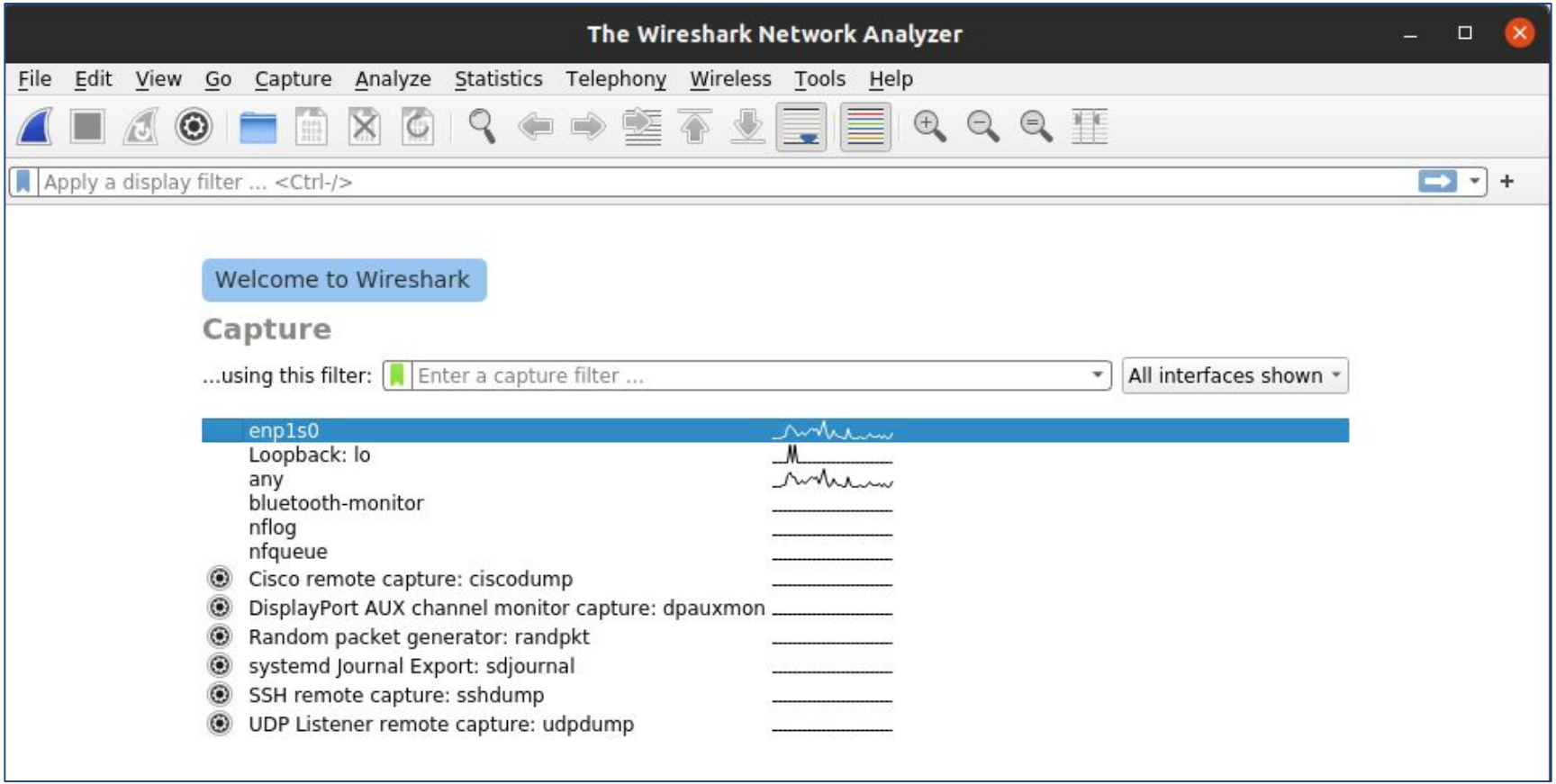
Install and Use Wireshark on Windows and Mac

Download & Installation

- Visit https://www.wireshark.org/download.html
- Identify the required OS
- Download and save the latest stable release

Windows

Install the downloaded executable <stable version>.exe


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
enp1s0
Loopback: lo
any
bluetooth-monitor
nflog
nfqueue
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump

Statistics Analysis

- Capture File Properties
- Conversations:
  - A network conversation is the traffic between two specific endpoints.
- Packet Lengths:
  - Shows the distribution of packet lengths and related information.
- Endpoints
  - Details on specific endpoints
- HTTP Statistics
  - Requests, Responses
- I/O Graphs
- Flow Graphs

Statistics Analysis

Wireshark · Capture File Properties · wlp2s0

Details

File

Name:	/tmp/wireshark_wlp2s0_20200908223533_eOj3go.pcapng
Length:	36 kB
Hash (SHA256):	f44d7c65022bb6ae9a7df965e64a6654e6bbc145a9fc71bdd2481b71efc62e35
Hash (RIPEMD160):	80d2606ec840d4d4ca01631b619bd8136f73bd56
Hash (SHA1):	53750fcf87d22774c2e00396afe3b8d6f79ae0dd
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet

Time

First packet:	2020-09-08 22:35:34
Last packet:	2020-09-08 22:35:39
Elapsed:	00:00:04

Capture

Hardware:	Intel(R) Core(TM) i7-8550U CPU @ 1.80GHz (with SSE4.2)
OS:	Linux 4.15.0-112-generic
Application:	Dumpcap (Wireshark) 3.0.10 (Git commit aa0261e8ddf3)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit
wlp2s0	0 (0.0%)	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	132	132 (100.0%)	—
Time span, s	4.830	4.830	—
Average pps	27.3	27.3	—
Average packet size, B	241	241	—

Capture file comments

Refresh | Save Comments | Close | Copy To Clipboard | Help

Wireshark · Conversations · wlp2s0

Ethernet · 2 | IPv4 · 6 | IPv6 | TCP · 5 | UDP · 2

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
34.73.232.153	192.168.1.16	3	270	2	166	1	104	4.390208	0.2819	4,711	2,951
172.217.26.206	192.168.1.16	20	7,851	10	1,458	10	6,393	0.021021	0.4638	25 k	110 k
172.217.160.142	192.168.1.16	69	15 k	37	5,325	32	10 k	0.006470	4.8237	8,831	17 k
172.217.163.110	192.168.1.16	9	4,986	5	2,093	4	2,893	0.167444	0.1122	149 k	206 k
192.168.1.1	192.168.1.16	26	2,661	13	1,641	13	1,020	0.000000	4.7788	2,747	1,707
192.168.1.16	213.227.170.132	2	156	1	90	1	66	3.212738	0.1668	4,317	3,166

Name resolution | Limit to display filter | Absolute start time | Conversation Types

Copy | Follow Stream... | Graph... | Close | Help

What is it not

- An intrusion detection system.
- Manipulate things on the network, it will only “measure” things from it.
- Send packets on the network or do other active things

Iperf /iperf3

Install iperf3 on Linux Ubuntu
sudo apt install iperf3

Windows/Others:
Download from https://iperf.fr/iperf-download.php

#Know about iperf3 usage
iperf3 -help

#In Server Mode
iperf3 -s

#In Client Mode
iperf3 -c <connect to host ip address>

Task 1

Capture Internet traffic using Wireshark for 5 minutes, check for TCP, UDP, ICMP packets in the trace by using appropriate filters. Check the conversations, flow graphs, I/O graphs

- UDP : Take DNS Packets (Run "nslookup www.cse 8.8.8.8" during the capture from terminal)

```
C:\Users\Prachi>ipconfig/flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\Prachi>nslookup www.cse 8.8.8.8
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    www.cse.iitd.ac.in
Address:  103.27.9.152
```

flush DNS for mac

1. Open the terminal by using Spotlight Search or by pressing Command + Space and then type Terminal.
2. Double click the application icon for Terminal to open it.
3. Type in “*sudo dscacheutil -flushcache;sudo killall -HUP mDNSResponder” without quotes*
4. Enter your Mac’s password
5. Press Enter to complete

flush DNS for ubuntu

Command for ubuntu:

```
sudo systemd-resolve --flush-caches
```

Ref: https://constellix.com/news/how-to-flush-dns-cache-windows-mac

udp

No.	Time	Source	Destination	Protocol	Length	Info
4575	36.371105	114.29.212.57	192.168.0.105	UDP	250	9000 → 62881 Len=208
4576	36.376389	114.29.212.57	192.168.0.105	UDP	186	9000 → 62881 Len=144
4577	36.387191	192.168.0.105	114.29.212.57	UDP	210	62881 → 9000 Len=168
4578	36.389710	114.29.212.57	192.168.0.105	UDP	250	9000 → 62881 Len=208
4579	36.395866	114.29.212.57	192.168.0.105	UDP	106	9000 → 62881 Len=64
4580	36.411048	114.29.212.57	192.168.0.105	UDP	266	9000 → 62881 Len=224
4581	36.431939	114.29.212.57	192.168.0.105	UDP	250	9000 → 62881 Len=208
4582	36.449614	114.29.212.57	192.168.0.105	UDP	218	9000 → 62881 Len=176
4583	36.468634	114.29.212.57	192.168.0.105	UDP	218	9000 → 62881 Len=176
4584	36.479965	114.29.212.57	192.168.0.105	UDP	218	9000 → 62881 Len=176
4585	36.509307	192.168.0.105	192.168.0.1	DNS	73	Standard query 0x6c26 A onlinesbi.com
4586	36.511928	114.29.212.57	192.168.0.105	UDP	202	9000 → 62881 Len=160
4587	36.512475	192.168.0.105	114.29.212.57	UDP	86	62881 → 9000 Len=44
4595	36.524513	192.168.0.1	192.168.0.105	DNS	228	Standard query response 0x6c26 A onlinesbi.com A 103.68.221.190 NS pdns.satyam.net.in NS s
4597	36.529413	114.29.212.57	192.168.0.105	UDP	202	9000 → 62881 Len=160
4599	36.550018	114.29.212.57	192.168.0.105	UDP	202	9000 → 62881 Len=160
4600	36.569062	114.29.212.57	192.168.0.105	UDP	202	9000 → 62881 Len=160
4601	36.586426	114.29.212.57	192.168.0.105	UDP	138	9000 → 62881 Len=96
4602	36.589134	114.29.212.57	192.168.0.105	UDP	202	9000 → 62881 Len=160
4603	36.602947	114.29.212.57	192.168.0.105	UDP	170	9000 → 62881 Len=128
4604	36.609000	114.29.212.57	192.168.0.105	UDP	234	9000 → 62881 Len=192

```
> Frame 4595: 228 bytes on wire (1824 bits), 228 bytes captured (1824 bits) on interface \Device\NPF_{FC5BDD9A-D442-4B15-9100-9E8F91F625C8}, id 0
> Ethernet II, Src: TendaTec_d7:03:28 (04:95:e6:d7:03:28), Dst: IntelCor_99:64:34 (18:5e:0f:99:64:34)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.105
v User Datagram Protocol, Src Port: 53, Dst Port: 51267
    Source Port: 53
    Destination Port: 51267
    Length: 194
    Checksum: 0x52df [unverified]
    [Checksum Status: Unverified]
    [Stream index: 17]
  > [Timestamps]
> Domain Name System (response)
```

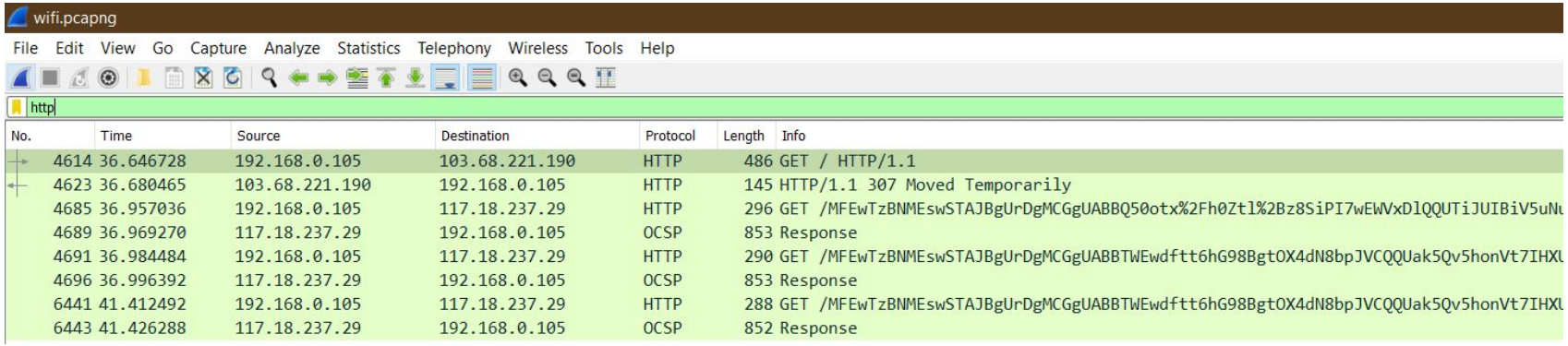
dns

No.	Time	Source	Destination	Protocol	Length	Info
3	0.103796	10.194.98.7	10.10.2.2	DNS	91	Standard query 0x1159 A settings-win.data.microsoft.com
4	0.106534	10.10.2.2	10.194.98.7	DNS	356	Standard query response 0x1159 A settings-win.data.microsoft.com CNAME atm-settingsfe-prod-geo2.trafficmanager.net CNAME set.
47	1.704677	10.194.98.7	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
48	1.710391	8.8.8.8	10.194.98.7	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
49	1.713399	10.194.98.7	8.8.8.8	DNS	78	Standard query 0x0002 A www.cse.iitd.ac.in
50	1.724162	8.8.8.8	10.194.98.7	DNS	94	Standard query response 0x0002 A www.cse.iitd.ac.in A 103.27.9.152
51	1.728592	10.194.98.7	8.8.8.8	DNS	78	Standard query 0x0003 AAAA www.cse.iitd.ac.in
52	1.740007	8.8.8.8	10.194.98.7	DNS	129	Standard query response 0x0003 AAAA www.cse.iitd.ac.in SOA dns8.iitd.ac.in

Network & internet > Wi-Fi > Wi-Fi

SSID:	IITD_WIFI
Protocol:	Wi-Fi 4 (802.11n)
Security type:	WPA2-Enterprise
Manufacturer:	Realtek Semiconductor Corp.
Description:	Realtek RTL8822CE 802.11ac PCIe Adapter
Driver version:	2024.0.10.226
Type of sign-in info:	Microsoft: Protected EAP (PEAP)
Network band:	2.4 GHz
Network channel:	6
Link speed (Receive/Transmit):	144/144 (Mbps)
Link-local IPv6 address:	fe80::346f:7893:caa7:6c3%9
IPv4 address:	10.194.98.7
IPv4 DNS servers:	10.10.2.2 (Unencrypted) 10.10.1.2 (Unencrypted)
Primary DNS suffix:	iitd.ac.in
DNS suffix search list:	iitd.ac.in cc.iitd.ac.in
Physical address (MAC):	90-E8-68-80-CC-5F

TCP: Take HTTP/SSL Packets from your most favourite university website in India



No.	Time	Source	Destination	Protocol	Length	Info
4614	36.646728	192.168.0.105	103.68.221.190	HTTP	486	GET / HTTP/1.1
4623	36.680465	103.68.221.190	192.168.0.105	HTTP	145	HTTP/1.1 307 Moved Temporarily
4685	36.957036	192.168.0.105	117.18.237.29	HTTP	296	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu
4689	36.969270	117.18.237.29	192.168.0.105	OCSP	853	Response
4691	36.984484	192.168.0.105	117.18.237.29	HTTP	290	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTWEwdftt6hG98BgtOX4dN8bpJVCQQUak5Qv5honVt7IHXU
4696	36.996392	117.18.237.29	192.168.0.105	OCSP	853	Response
6441	41.412492	192.168.0.105	117.18.237.29	HTTP	288	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTWEwdftt6hG98BgtOX4dN8bpJVCQQUak5Qv5honVt7IHXU
6443	41.426288	117.18.237.29	192.168.0.105	OCSP	852	Response

ICMP: Ping iitd.ac.in from terminal

```
C:\Users\SHIVANGI BITHEL>ping google.com

Pinging google.com [172.217.161.14] with 32 bytes of data:
Reply from 172.217.161.14: bytes=32 time=10ms TTL=120
Reply from 172.217.161.14: bytes=32 time=11ms TTL=120
Reply from 172.217.161.14: bytes=32 time=9ms TTL=120
Reply from 172.217.161.14: bytes=32 time=11ms TTL=120

Ping statistics for 172.217.161.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 11ms, Average = 10ms
```

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
1800	16.509682	192.168.0.105	172.217.161.14	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 1802)
1802	16.520159	172.217.161.14	192.168.0.105	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=120 (request in 1800)
1916	17.516408	192.168.0.105	172.217.161.14	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 1917)
1917	17.527642	172.217.161.14	192.168.0.105	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=120 (request in 1916)
2001	18.527322	192.168.0.105	172.217.161.14	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 2003)
2003	18.536690	172.217.161.14	192.168.0.105	ICMP	74	Echo (ping) reply id=0x0001, seq=7/1792, ttl=120 (request in 2001)
2133	19.546352	192.168.0.105	172.217.161.14	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 2135)
2135	19.557259	172.217.161.14	192.168.0.105	ICMP	74	Echo (ping) reply id=0x0001, seq=8/2048, ttl=120 (request in 2133)
8727	51.800260	192.168.0.1	192.168.0.105	ICMP	70	Destination unreachable (Port unreachable)
8730	51.803044	192.168.0.104	192.168.0.105	ICMP	70	Destination unreachable (Port unreachable)
8735	51.846469	192.168.0.101	192.168.0.105	ICMP	98	Destination unreachable (Port unreachable)
8765	52.000544	192.168.0.102	192.168.0.105	ICMP	98	Destination unreachable (Port unreachable)
8785	52.113659	192.168.0.100	192.168.0.105	ICMP	98	Destination unreachable (Port unreachable)

Task 2

Run iperf3 communication program locally using server-client modes. Capture its Wireshark trace and check for IP Addresses, TCP/UDP conversation being used in the communication, Ports, Ethernet interface.

Ubuntu:

server: iperf3 -s

client: iperf3 -c <connect to host ip address>

ip address – check using ifconfig

TCP

IPERF3
SERVER

```
C:\Users\Prachi>cd Downloads\iper

C:\Users\Prachi\Downloads\iper>iperf3.exe -s
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
Accepted connection from ::1, port 54596
[  5] local ::1 port 5201 connected to ::1 port 54597
[ ID] Interval           Transfer     Bandwidth
[  5]   0.00-1.01   sec   287 MBytes  2.38 Gbits/sec
[  5]   1.01-2.00   sec   221 MBytes  1.87 Gbits/sec
[  5]   2.00-3.01   sec   290 MBytes  2.41 Gbits/sec
[  5]   3.01-4.01   sec   237 MBytes  1.99 Gbits/sec
[  5]   4.01-5.01   sec   426 MBytes  3.58 Gbits/sec
[  5]   5.01-6.01   sec   439 MBytes  3.67 Gbits/sec
[  5]   6.01-7.01   sec   408 MBytes  3.44 Gbits/sec
[  5]   7.01-8.01   sec   346 MBytes  2.90 Gbits/sec
[  5]   8.01-9.00   sec   345 MBytes  2.91 Gbits/sec
[  5]   9.00-10.01  sec   461 MBytes  3.85 Gbits/sec
[  5]  10.01-10.01  sec  0.00 Bytes  0.00 bits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  5]   0.00-10.01  sec  0.00 Bytes  0.00 bits/sec                  sender
[  5]   0.00-10.01  sec  3.38 GBytes  2.90 Gbits/sec                  receiver
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
```

IPERF3
CLIENT

```
C:\Users\Prachi>cd Downloads\iper

C:\Users\Prachi\Downloads\iper>iperf3.exe -c localhost
Connecting to host localhost, port 5201
[  4] local ::1 port 54597 connected to ::1 port 5201
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-1.01   sec   287 MBytes  2.38 Gbits/sec
[  4]   1.01-2.01   sec   221 MBytes  1.86 Gbits/sec
[  4]   2.01-3.01   sec   290 MBytes  2.43 Gbits/sec
[  4]   3.01-4.01   sec   236 MBytes  1.98 Gbits/sec
[  4]   4.01-5.01   sec   426 MBytes  3.58 Gbits/sec
[  4]   5.01-6.01   sec   439 MBytes  3.67 Gbits/sec
[  4]   6.01-7.01   sec   408 MBytes  3.44 Gbits/sec
[  4]   7.01-8.01   sec   346 MBytes  2.91 Gbits/sec
[  4]   8.01-9.00   sec   345 MBytes  2.91 Gbits/sec
[  4]   9.00-10.01  sec   461 MBytes  3.84 Gbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  4]   0.00-10.01  sec  3.38 GBytes  2.90 Gbits/sec                  sender
[  4]   0.00-10.01  sec  3.38 GBytes  2.90 Gbits/sec                  receiver

iperf Done.

C:\Users\Prachi\Downloads\iper>
```

tcp.port==5201

No.	Time	Source	Destination	Protocol	Length	Info
3	3.021093	::1	::1	TCP	76	55990 → 5201 [SYN] Seq=0 Win=65535 Len=0 MSS=65475 WS=4 SACK_PERM=1
4	3.022673	::1	::1	TCP	76	5201 → 55990 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65475 WS=4 SACK_PERM=1
5	3.022749	::1	::1	TCP	64	55990 → 5201 [ACK] Seq=1 Ack=1 Win=212992 Len=0
6	3.022851	::1	::1	TCP	101	55990 → 5201 [PSH, ACK] Seq=1 Ack=1 Win=212992 Len=37
7	3.022884	::1	::1	TCP	64	5201 → 55990 [ACK] Seq=1 Ack=38 Win=212952 Len=0
8	3.023115	::1	::1	TCP	65	5201 → 55990 [PSH, ACK] Seq=1 Ack=38 Win=212952 Len=1
9	3.023158	::1	::1	TCP	64	55990 → 5201 [ACK] Seq=38 Ack=2 Win=212988 Len=0
10	3.023397	::1	::1	TCP	68	55990 → 5201 [PSH, ACK] Seq=38 Ack=2 Win=212988 Len=4
11	3.023429	::1	::1	TCP	64	5201 → 55990 [ACK] Seq=2 Ack=42 Win=212948 Len=0
12	3.023460	::1	::1	TCP	146	55990 → 5201 [PSH, ACK] Seq=42 Ack=2 Win=212988 Len=82

```
> Internet Protocol Version 6, Src: ::1, Dst: ::1
v Transmission Control Protocol, Src Port: 55990, Dst Port: 5201, Seq: 0, Len: 0
    Source Port: 55990
    Destination Port: 5201
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Sequence number (raw): 3231154013
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
    Window size value: 65535
    [Calculated window size: 65535]
    Checksum: 0x4608 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
  > [Timestamps]
```

```
0000  18 00 00 00 60 04 20 1c  00 20 06 80 00 00 00 00   ····`· ·· ········
0010  00 00 00 00 00 00 00 00  00 00 00 01 00 00 00 00   ····· ····· ····
0020  00 00 00 00 00 00 00 00  00 00 00 01 da b6 14 51   ····· ····· ····Q
0030  c0 97 7f 5d 00 00 00 00  80 02 ff ff 46 08 00 00   ···]···· ····F···
0040  02 04 ff c3 01 03 03 02  01 01 04 02               ····· ····
```

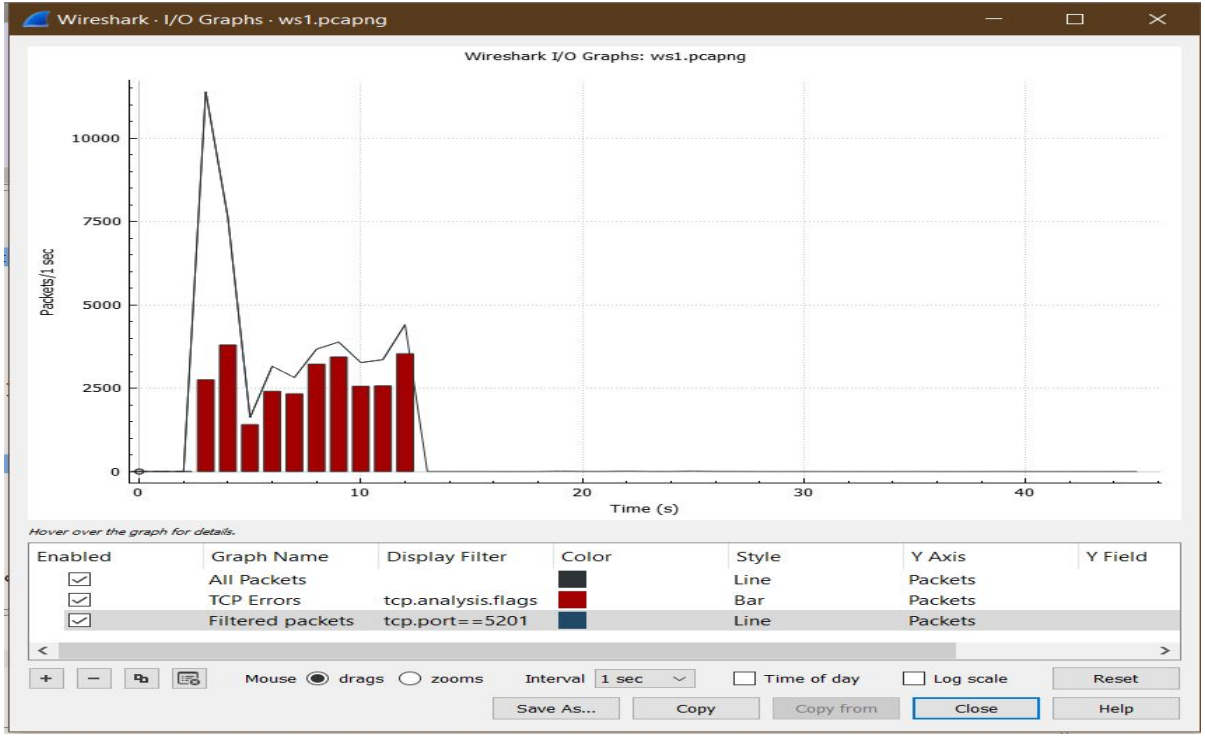
Statistics
|
Conversations

Wireshark · Conversations · ws1.pcapng

Ethernet | IPv4 · 3 | IPv6 · 3 | TCP · 2 | UDP · 7

Address A	Port A	Address B	Port 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
::1	55990	::1	5201	17	1239	9	711	8	528	3.021093	0.0127	446 k	
::1	55991	::1	5201	45,154	635 M	24,268	634 M	20,886	1336 k	3.027361	9.9138	511 M	

Statistics
|
I/O Graph



UDP

IPERF3
SERVER

```
C:\Users\Prachi\Downloads\iper>iperf3.exe -s
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
Accepted connection from ::1, port 61681
[  5] local ::1 port 5201 connected to ::1 port 49290
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagram
s
[  5]   0.00-1.00   sec   120 KBytes   983 Kbits/sec  0.087 ms  0/15 (0%)
[  5]   1.00-2.01   sec   128 KBytes  1.04 Mbits/sec  0.196 ms  0/16 (0%)
[  5]   2.01-3.00   sec   128 KBytes  1.06 Mbits/sec  0.175 ms  0/16 (0%)
[  5]   3.00-4.00   sec   128 KBytes  1.05 Mbits/sec  0.259 ms  0/16 (0%)
[  5]   4.00-5.01   sec   128 KBytes  1.04 Mbits/sec  0.238 ms  0/16 (0%)
[  5]   5.01-6.01   sec   128 KBytes  1.05 Mbits/sec  0.223 ms  0/16 (0%)
[  5]   6.01-7.01   sec   136 KBytes  1.11 Mbits/sec  0.236 ms  0/17 (0%)
[  5]   7.01-8.01   sec   120 KBytes   986 Kbits/sec  0.207 ms  0/15 (0%)
[  5]   8.01-9.00   sec   136 KBytes  1.12 Mbits/sec  0.153 ms  0/17 (0%)
[  5]   9.00-10.00  sec   120 KBytes   979 Kbits/sec  0.094 ms  0/15 (0%)
[  5]  10.00-10.00  sec  0.00 Bytes  0.00 bits/sec  0.094 ms  0/0 (0%)
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagram
s
[  5]   0.00-10.00  sec  0.00 Bytes  0.00 bits/sec  0.094 ms  0/159 (0%)
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
```

IPERF3
CLIENT

```
C:\Users\Prachi\Downloads\iper>iperf3.exe -c localhost -u
Connecting to host localhost, port 5201
[  4] local ::1 port 49290 connected to ::1 port 5201
[ ID] Interval           Transfer     Bandwidth       Total Datagrams
[  4]   0.00-1.00   sec   128 KBytes  1.05 Mbits/sec  16
[  4]   1.00-2.01   sec   128 KBytes  1.04 Mbits/sec  16
[  4]   2.01-3.00   sec   128 KBytes  1.06 Mbits/sec  16
[  4]   3.00-4.00   sec   128 KBytes  1.05 Mbits/sec  16
[  4]   4.00-5.01   sec   128 KBytes  1.04 Mbits/sec  16
[  4]   5.01-6.01   sec   128 KBytes  1.05 Mbits/sec  16
[  4]   6.01-7.01   sec   136 KBytes  1.11 Mbits/sec  17
[  4]   7.01-8.01   sec   120 KBytes   986 Kbits/sec  15
[  4]   8.01-9.00   sec   128 KBytes  1.05 Mbits/sec  16
[  4]   9.00-10.00  sec   128 KBytes  1.04 Mbits/sec  16
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagram
s
[  4]   0.00-10.00  sec  1.25 MBytes  1.05 Mbits/sec  0.094 ms  0/159 (0%)
[  4] Sent 159 datagrams

iperf Done.

C:\Users\Prachi\Downloads\iper>
```

*Adapter for loopback traffic capture

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp

No.	Time	Source	Destination	Protocol	Length	Info
27	1.691798	192.168.0.105	239.255.255.250	SSDP	308	NOTIFY * HTTP/1.1
110	6.710323	192.168.0.105	239.255.255.250	SSDP	308	NOTIFY * HTTP/1.1
160	8.728141	::1	::1	UDP	56	56107 → 5201 Len=4
161	8.728720	::1	::1	UDP	56	5201 → 56107 Len=4
166	8.751705	::1	::1	UDP	8244	56107 → 5201 Len=8192
169	8.851695	::1	::1	UDP	8244	56107 → 5201 Len=8192
170	8.951643	::1	::1	UDP	8244	56107 → 5201 Len=8192

```
> Frame 160: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \Device\NPF_Loopback, id 0
> Null/Loopback
> Internet Protocol Version 6, Src: ::1, Dst: ::1
v User Datagram Protocol, Src Port: 56107, Dst Port: 5201
    Source Port: 56107
    Destination Port: 5201
    Length: 12
    Checksum: 0x9f83 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
  > [Timestamps]
v Data (4 bytes)
    Data: 15cd5b07
    [Length: 4]
```

Wireshark · Conversations · udp2.pcapng

Ethernet | IPv4 · 2 | IPv6 · 1 | TCP · 2 | UDP · 2

Address A	Port A	Address B	Port 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
192.168.0.105	60466	239.255.255.250	1900	5	1540	5	1540	0	0	1.691798	19.9993	616	
::1	56107	::1	5201	164	1335 k	163	1335 k	1	56	8.728141	10.0238	1065 k	

References

- https://www.wireshark.org/
- https://www.wireshark.org/docs/wsug_html_chunked/AppProtocols.html
- https://www.wireshark.org/docs/wsug_html_chunked/
- https://packetlife.net/media/library/13/Wireshark_Display_Filters.pdf
- https://jvns.ca/blog/2018/06/19/what-i-use-wireshark-for/
- https://iperf.fr/
- https://itsfoss.com/install-wireshark-ubuntu/