

Assignment 5

Wireshark assignment for Transport & Link layer

Harsh Agarwal
CS15BTECH11019

Transport Layer

Analysis of downloading ubuntu-16.04.3-desktop-amd64.iso from internet

<http://mirrors.piconets.webwerks.in/ubuntu-mirror/ubuntu-releases/16.04.3/ubuntu-16.04.3-desktop-amd64.iso>

Server IP - 43.240.66.200:80

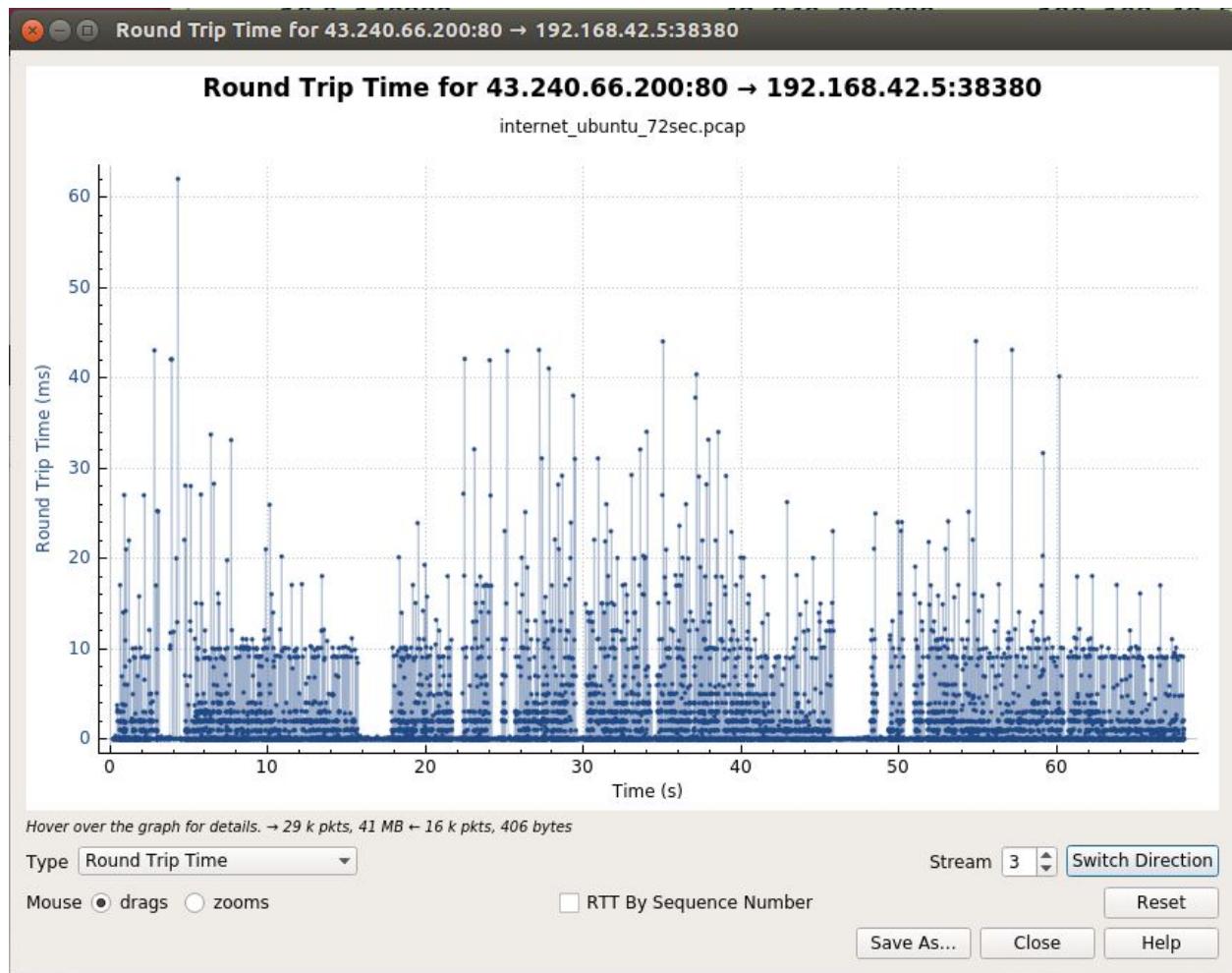
My IP - 192.168.42.5:38380

Capture for 72 seconds

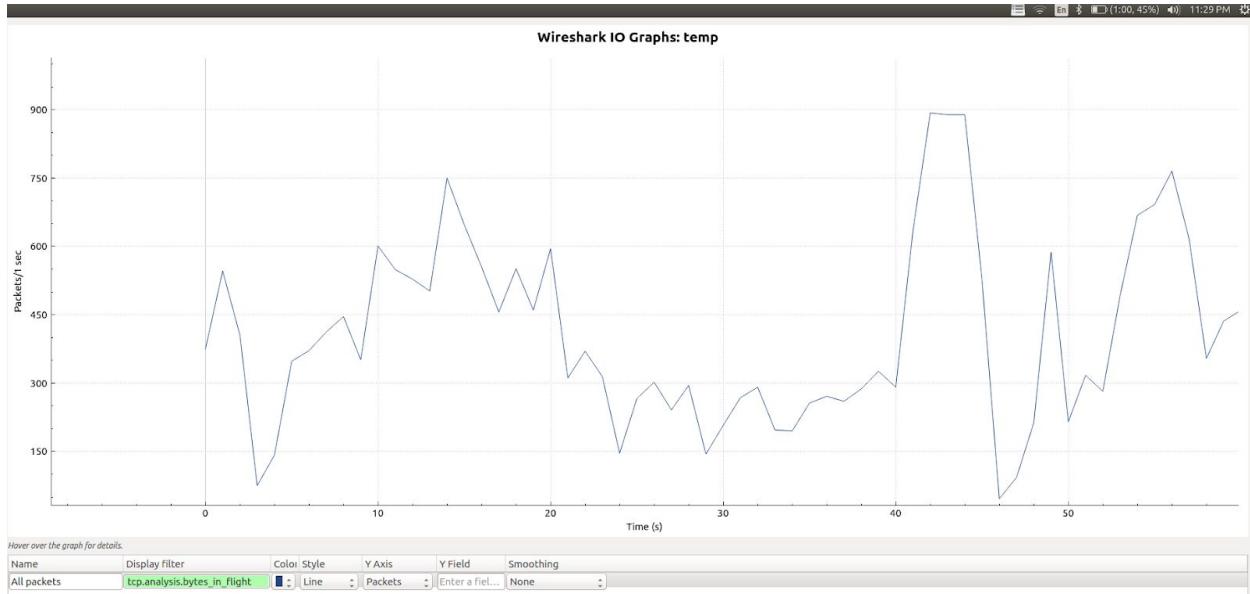
Command to filter this transaction :: **tcp.stream eq 3**

1)

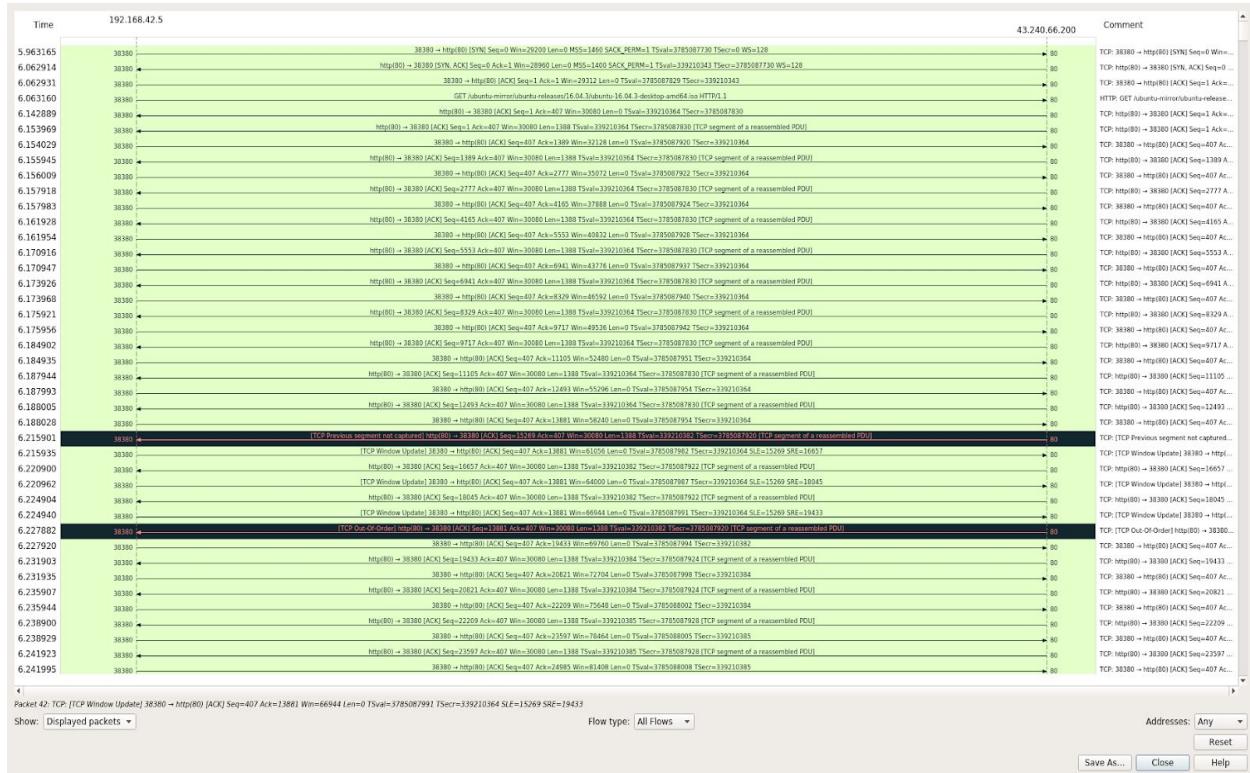
- a) RTT values on an average are same. There are fluctuations in the values but most value were close to 10ms



b) The IO Graph below is for `tcp.analysis.bytes_in_flight` vs time
`bytes_in_flight` tells TCP Congestion window because at any instant this quantity tells exactly how many bytes were in the packet. Since this cannot be more than congestion , hence this is graph of congestion window. There is a lot of fluctuation in this meaning lot of variation in traffic(this is referred from RTT graph also).

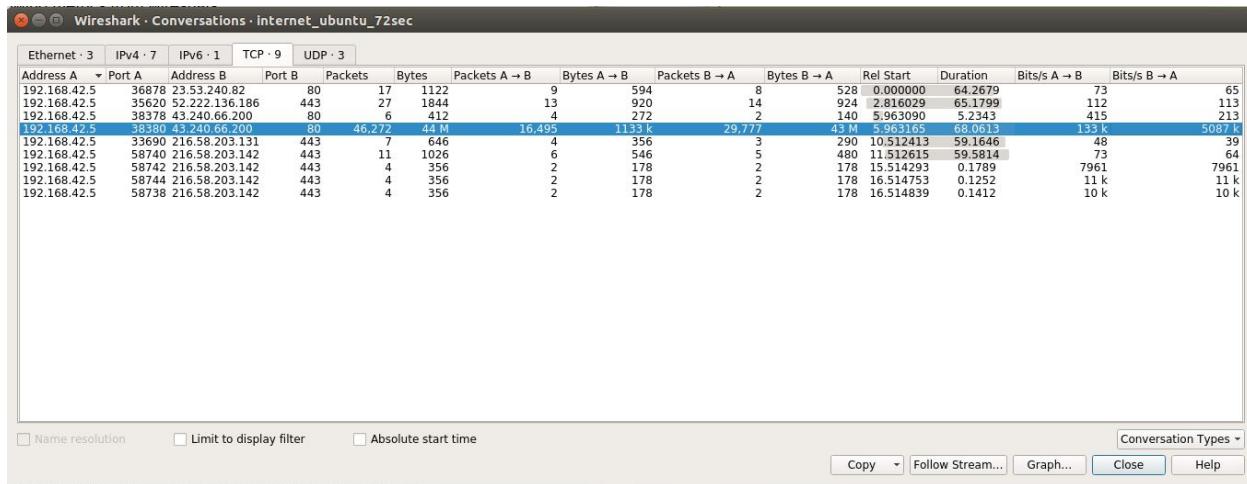


c) The flow graph feature shows a sender and a receiver view of the packet flow. (listing all seq-nos. & ack-nos. , etc). This is a really big graph as it tells of entire conversation



d) Average Throughput from sender -> receiver :: 5087kb/sec

Average Throughput from receiver -> sender :: 133kb/sec

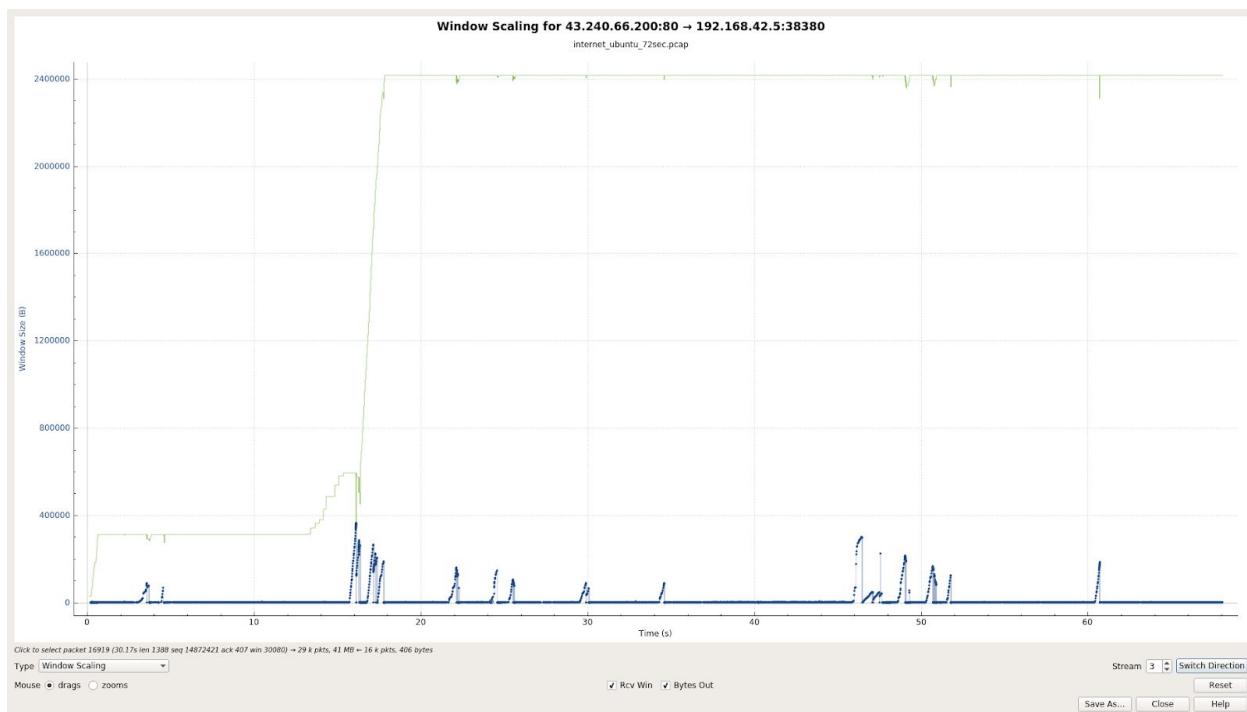


e)

The graph shows The size of the advertised receiver window incl. scaling factor.

The green plot shows receiver_window

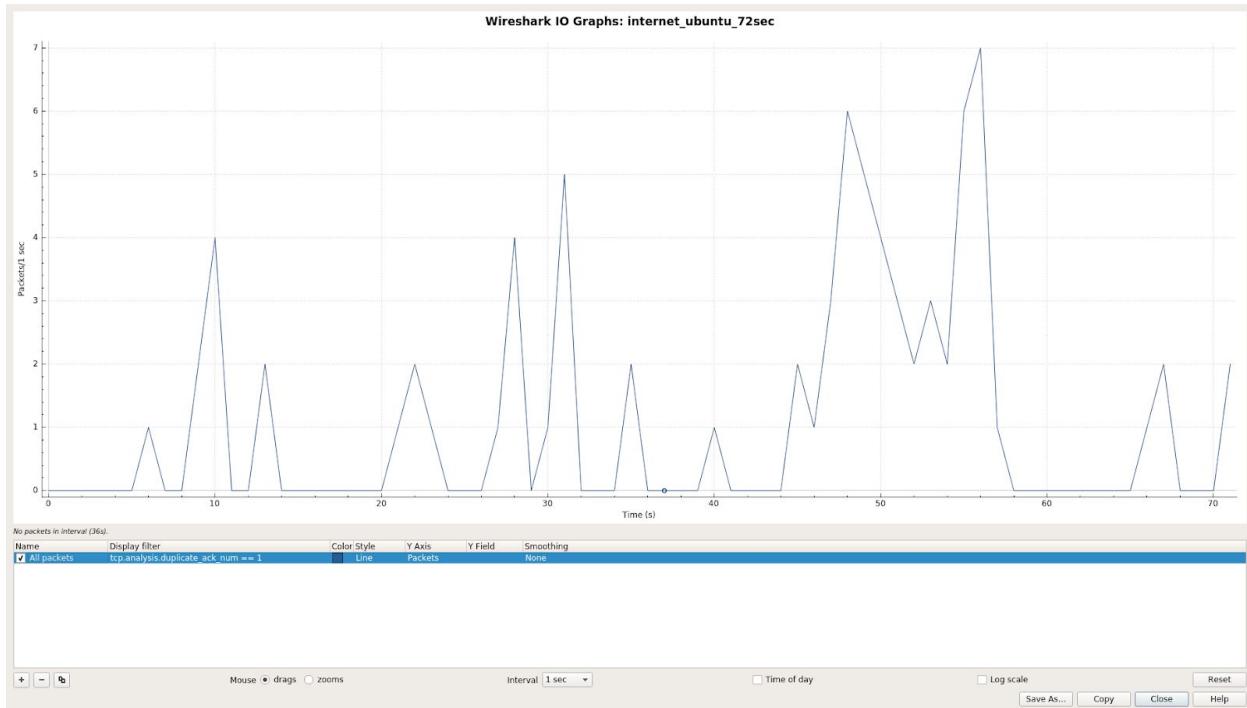
The blue plot shows bytes_out. We can see from the green plot that receiver_window size increases (with fluctuations in the middle) and it gets stabilized at 2400000.



f) 1-duplicate Ack

Fraction :: 77 / 46365 (0.2%)

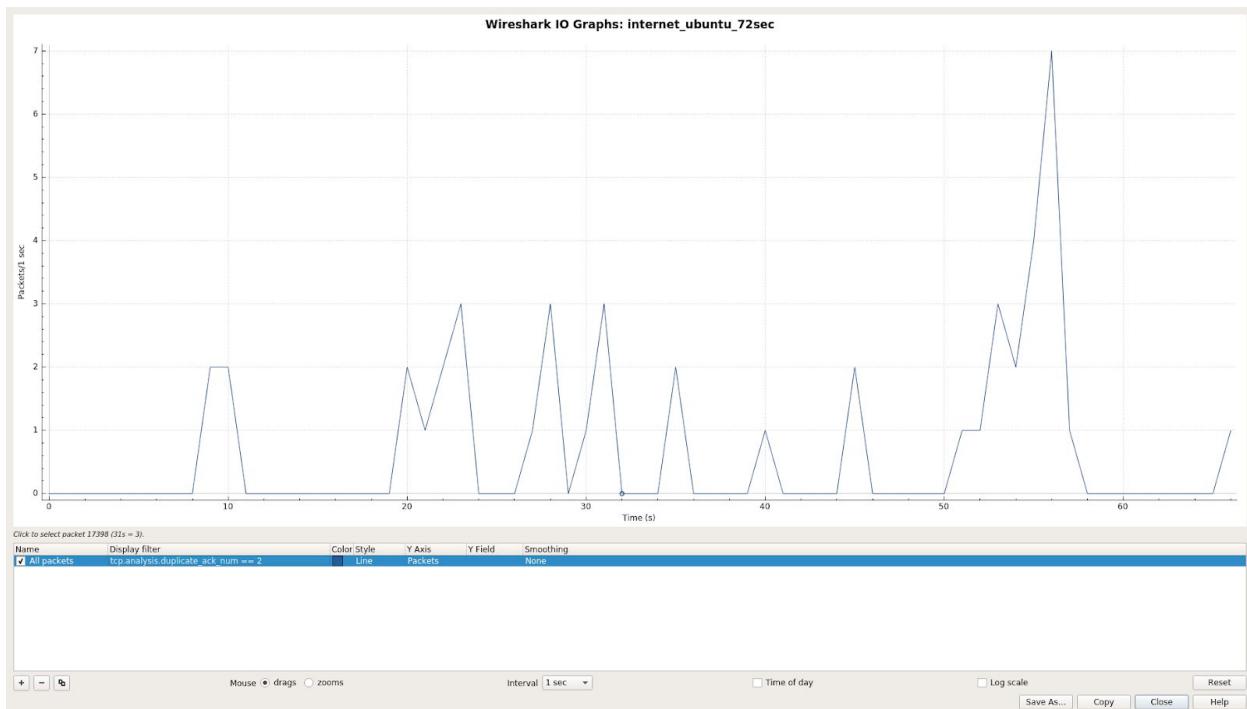
Command used :: **tcp.analysis.duplicate_ack_num == 1**



2-duplicate Ack

Fraction :: 45 / 46365 (0.1%)

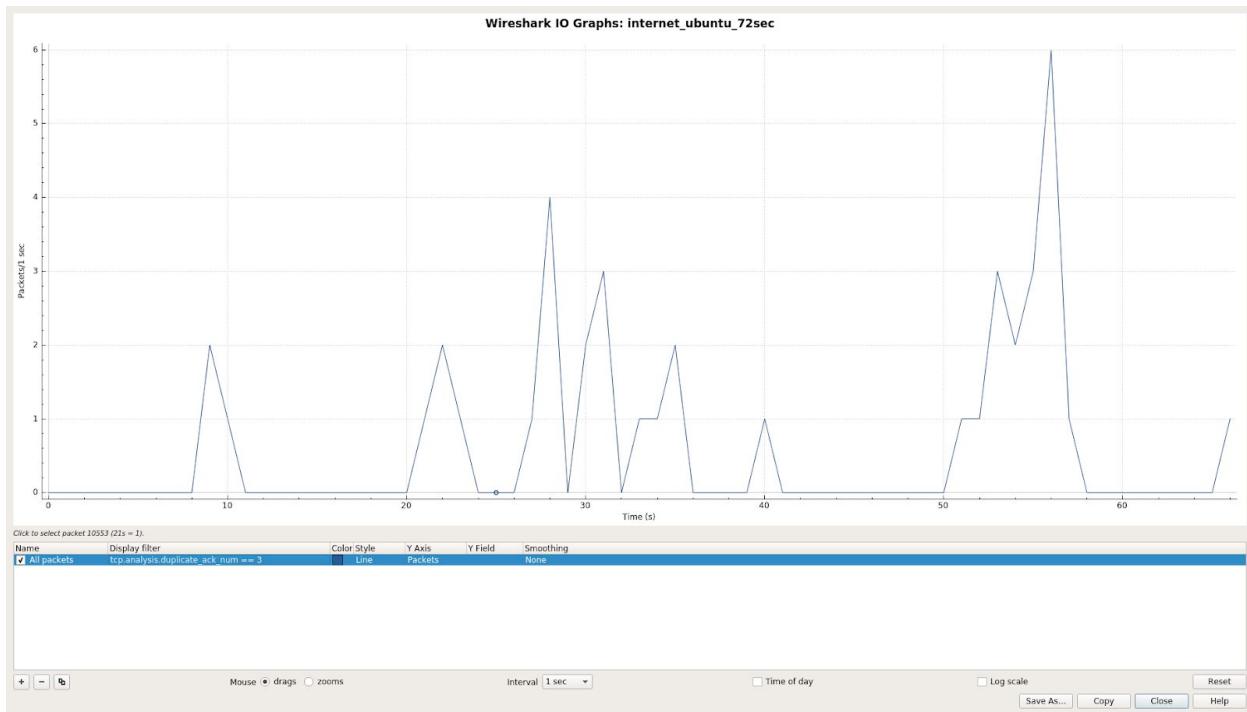
Command used :: **tcp.analysis.duplicate_ack_num == 2**



3-duplicate Ack

Fraction :: 40 / 46365 (0.1%)

Command used :: **tcp.analysis.duplicate_ack_num == 3**



Number of dup-Acks is less compared to other packets. There is difference in the above 3 graphs because for some lost packets it is not needed to go upto 3-dup ACK. 3-dup ACK is mostly used in congestion control (via fast retransmit).

2)

I identified TCP 3-way handshake for the packet captured above.
The first 3 packets in screenshot below illustrate 3-way handshake

No.	Time	Source	Destination	Length	Protocol	Info
10 5. 963165		192.168.42.5	43.240.66.200	74	TCP	38380 → http(80) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK=0
13 6. 062914		43.240.66.200	192.168.42.5	74	TCP	http(80) → 38380 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK=0
14 6. 062931		192.168.42.5	43.240.66.200	66	TCP	38380 → http(80) [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1460.0 TStamp=1460.0
15 6. 063160		192.168.42.5	43.240.66.200	472	HTTP	GET /ubuntu-mirror/ubuntu-releases/16.04.3/ubuntu-16.04.3-
16 6. 142889		43.240.66.200	192.168.42.5	66	TCP	http(80) → 38380 [ACK] Seq=1 Ack=407 Win=30080 Len=0 TSval=1460.0 TStamp=1460.0
17 6. 153969		43.240.66.200	192.168.42.5	1454	TCP	http(80) → 38380 [ACK] Seq=1 Ack=407 Win=30080 Len=1388 TS=1460.0 TStamp=1460.0
18 6. 154029		192.168.42.5	43.240.66.200	66	TCP	38380 → http(80) [ACK] Seq=407 Ack=1389 Win=32128 Len=0 TS=1460.0 TStamp=1460.0
19 6. 155945		43.240.66.200	192.168.42.5	1454	TCP	http(80) → 38380 [ACK] Seq=1389 Ack=407 Win=30080 Len=1384 TS=1460.0 TStamp=1460.0
20 6. 156009		192.168.42.5	43.240.66.200	66	TCP	38380 → http(80) [ACK] Seq=407 Ack=2777 Win=35072 Len=0 TS=1460.0 TStamp=1460.0
21 6. 157918		43.240.66.200	192.168.42.5	1454	TCP	http(80) → 38380 [ACK] Seq=2777 Ack=407 Win=30080 Len=1384 TS=1460.0 TStamp=1460.0
22 6. 157983		192.168.42.5	43.240.66.200	66	TCP	38380 → http(80) [ACK] Seq=407 Ack=4165 Win=37888 Len=0 TS=1460.0 TStamp=1460.0
23 6. 161928		43.240.66.200	192.168.42.5	1454	TCP	http(80) → 38380 [ACK] Seq=4165 Ack=407 Win=30080 Len=1384 TS=1460.0 TStamp=1460.0
24 6. 161954		192.168.42.5	43.240.66.200	66	TCP	38380 → http(80) [ACK] Seq=407 Ack=5553 Win=40832 Len=0 TS=1460.0 TStamp=1460.0
25 6. 170916		43.240.66.200	192.168.42.5	1454	TCP	http(80) → 38380 [ACK] Seq=5553 Ack=407 Win=30080 Len=1384 TS=1460.0 TStamp=1460.0
26 6. 170947		192.168.42.5	43.240.66.200	66	TCP	38380 → http(80) [ACK] Seq=407 Ack=6941 Win=43776 Len=0 TS=1460.0 TStamp=1460.0
27 6. 173926		43.240.66.200	192.168.42.5	1454	TCP	http(80) → 38380 [ACK] Seq=6941 Ack=407 Win=30080 Len=1384 TS=1460.0 TStamp=1460.0
28 6. 173968		192.168.42.5	43.240.66.200	66	TCP	38380 → http(80) [ACK] Seq=407 Ack=8329 Win=46592 Len=0 TS=1460.0 TStamp=1460.0
29 6. 175921		43.240.66.200	192.168.42.5	1454	TCP	http(80) → 38380 [ACK] Seq=8329 Ack=407 Win=30080 Len=1384 TS=1460.0 TStamp=1460.0
30 6. 175956		192.168.42.5	43.240.66.200	66	TCP	38380 → http(80) [ACK] Seq=407 Ack=9717 Win=49536 Len=0 TS=1460.0 TStamp=1460.0
31 6. 184902		43.240.66.200	192.168.42.5	1454	TCP	http(80) → 38380 [ACK] Seq=9717 Ack=407 Win=30080 Len=1384 TS=1460.0 TStamp=1460.0
32 6. 184935		192.168.42.5	43.240.66.200	66	TCP	38380 → http(80) [ACK] Seq=407 Ack=11008 Win=52480 Len=0 TS=1460.0 TStamp=1460.0
33 6. 187944		43.240.66.200	192.168.42.5	1454	TCP	http(80) → 38380 [ACK] Seq=11005 Ack=407 Win=30080 Len=1384 TS=1460.0 TStamp=1460.0
34 6. 187993		192.168.42.5	43.240.66.200	66	TCP	38380 → http(80) [ACK] Seq=407 Ack=12493 Win=55296 Len=0 TS=1460.0 TStamp=1460.0
35 6. 188005		43.240.66.200	192.168.42.5	1454	TCP	http(80) → 38380 [ACK] Seq=12493 Ack=407 Win=30080 Len=1384 TS=1460.0 TStamp=1460.0
36 6. 188028		192.168.42.5	43.240.66.200	66	TCP	38380 → http(80) [ACK] Seq=407 Ack=13881 Win=58240 Len=0 TS=1460.0 TStamp=1460.0
37 6. 215901		43.240.66.200	192.168.42.5	1454	TCP	[TCP Previous segment not captured] http(80) → 38380 [ACK] Seq=0 Ack=0 TS=1460.0 TStamp=1460.0
38 6. 215935		192.168.42.5	43.240.66.200	78	TCP	[TCP Window Update] 38380 → http(80) [ACK] Seq=407 Ack=13881 Win=58240 Len=0 TS=1460.0 TStamp=1460.0
39 6. 220900		43.240.66.200	192.168.42.5	1454	TCP	http(80) → 38380 [ACK] Seq=16657 Ack=407 Win=30080 Len=0 TS=1460.0 TStamp=1460.0
40 6. 220962		192.168.42.5	43.240.66.200	78	TCP	[TCP Window Update] 38380 → http(80) [ACK] Seq=407 Ack=13881 Win=58240 Len=0 TS=1460.0 TStamp=1460.0
41 6. 224904		43.240.66.200	192.168.42.5	1454	TCP	http(80) → 38380 [ACK] Seq=18045 Ack=407 Win=30080 Len=0 TS=1460.0 TStamp=1460.0
42 6. 224940		192.168.42.5	43.240.66.200	78	TCP	[TCP Window Update] 38380 → http(80) [ACK] Seq=407 Ack=13881 Win=58240 Len=0 TS=1460.0 TStamp=1460.0
43 6. 227882		43.240.66.200	192.168.42.5	1454	TCP	[TCP Out-Of-Order] http(80) → 38380 [ACK] Seq=13881 Ack=407 Win=69760 Len=0 TS=1460.0 TStamp=1460.0
44 6. 227920		192.168.42.5	43.240.66.200	66	TCP	38380 → http(80) [ACK] Seq=407 Ack=19433 Win=69760 Len=0 TS=1460.0 TStamp=1460.0
45 6. 231903		43.240.66.200	192.168.42.5	1454	TCP	http(80) → 38380 [ACK] Seq=19433 Ack=407 Win=30080 Len=1384 TS=1460.0 TStamp=1460.0

First packet is from receiver to sender with SYN bit as 1. There is no payload (len = 0) and initial sequence number 0 is exchanged (this is relative sequence number given by wireshark)

```
Wireshark - Packet 10 · internet_ubuntu_7sec

> Frame 10: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: ea:97:d1:56:6d:57 (ea:97:d1:56:6d:57), Dst: 26:8c:a3:8d:bb:9e (26:8c:a3:8d:bb:9e)
> Internet Protocol Version 4, Src: 192.168.42.5, Dst: 43.240.66.200
> Transmission Control Protocol, Src Port: 38380 (38380), Dst Port: http (80), Seq: 0, Len: 0
    Source Port: 38380 (38380)
    Destination Port: http (80)
    [Stream index: 3]
    [TCP Segment Len: 0]
    Sequence number: 0 (relative sequence number)
    Acknowledgment number: 0
    1010... Header Length: 40 bytes (10)
    Flags: 0x002 (SYN)
        000... .... = Reserved: Not set
        ...0.... .... = Nonce: Not set
        ...0.... .... = Congestion Window Reduced (CWR): Not set
        ...0.... .... = ECN-Echo: Not set
        ...0.... .... = Urgent: Not set
        ...0.... .... = Acknowledgment: Not set
        ...0.... .... = Push: Not set
        ...0.... .... = Reset: Not set
        ....0.. = Syn: Set
    > [Expert Info (Chat/Sequence): Connection establish request (SYN): server port 80]
        ....0 = Fin: Not set
    [TCP Flags: .S.]
    Window size value: 29200
    [Calculated window size: 29200]
    Checksum: 0xe6d2 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    > Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale

0000  26 8c a3 8d bb 9e ea 97 d1 56 6d 57 08 00 45 00  &..... .VmW..E.
0010  00 3c 61 f8 40 00 40 06 7f 5e c0 a8 2a 05 2b f0  .<a.@@.^.^.*.+
0020  42 c8 95 ec 00 50 bf 01 83 ea 00 00 00 00 a0 02  B...P. .....
0030  72 10 e6 d2 00 00 02 04 05 b4 04 02 08 0a c1 9b  r..... .....
0040  da f2 00 00 00 00 01 03 03 07  .....
```

Second packet is from sender to receiver with SYN bit as 1 & ACK bit as 1. There is no payload (len = 0) and sequence number 0 , ack number 1(+1 than 1st sequence number) is exchanged (this is relative sequence number given by wireshark).

```

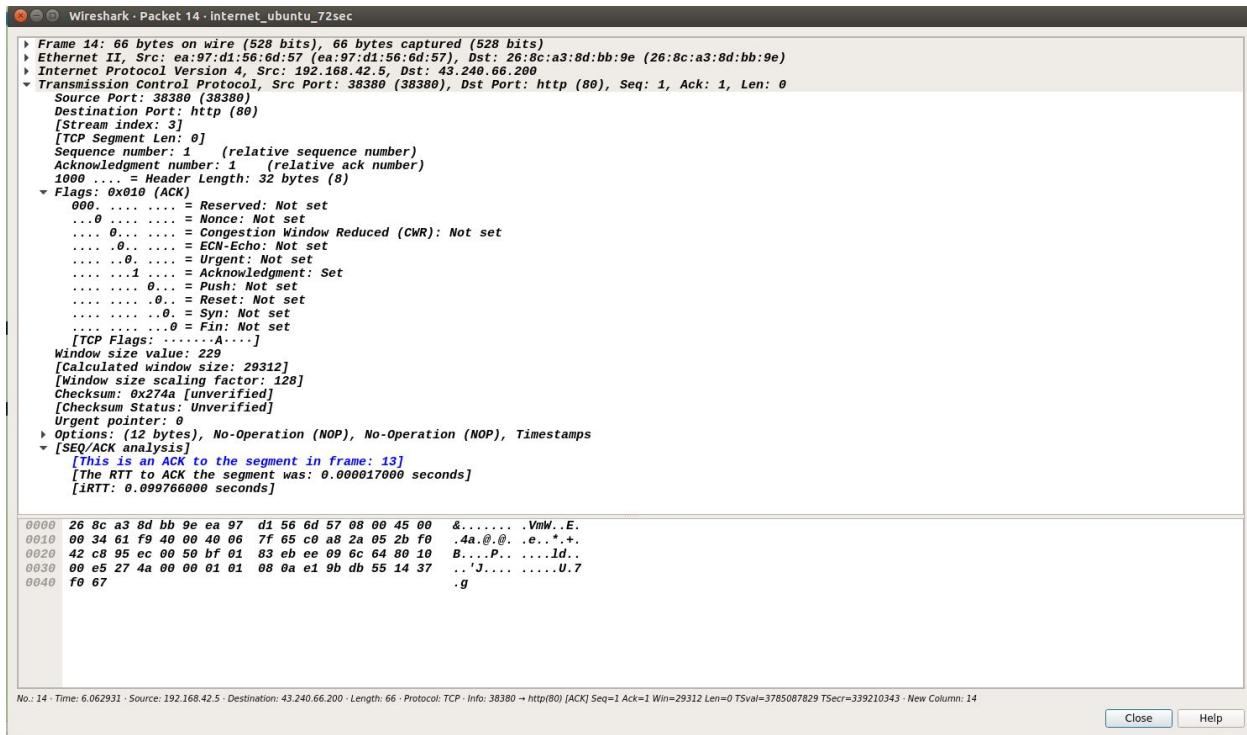
Frame 13: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: 26:8c:a3:8d:bb:9e (26:8c:a3:8d:bb:9e), Dst: ea:97:d1:56:6d:57 (ea:97:d1:56:6d:57)
Internet Protocol Version 4, Src: 43.240.66.200, Dst: 192.168.42.5
Transmission Control Protocol, Src Port: http (80), Dst Port: 38380 (38380), Seq: 0, Ack: 1, Len: 0
    Source Port: http (80)
    Destination Port: 38380 (38380)
    [Stream index: 3]
    [TCP Segment Len: 8]
    Sequence number: 0 (relative sequence number)
    Acknowledgment number: 1 (relative ack number)
    1010 ... = Header Length: 40 bytes (10)
    Flags: 0x012 (SYN, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0.... .... = Congestion Window Reduced (CWR): Not set
        .... .0.... .... = ECN-Echo: Not set
        .... ..0.... .... = Urgent: Not set
        .... .1.... .... = Acknowledgment: Set
        .... ..0.... .... = Push: Not set
        .... ....0.... .... = Reset: Not set
        .... ....1.... .... = Syn: Set
        > [Expert Info (Chat/Sequence): Connection establish acknowledge (SYN+ACK): server port 80]
        .... ..0.... .... = Fin: Not set
    [TCP Flags: ....A-S...]
    Window size value: 28960
    [Calculated window size: 28960]
    Checksum: 0x3861 [Unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
    [This is an ACK to the segment in frame: 10]
    [The RTT to ACK the segment was: 0.099749000 seconds]
    [iRTT: 0.099766000 seconds]
    [SEQ/ACK analysis]

0000  ea 97 d1 56 6d 57 26 8c a3 8d bb 9e 08 00 45 00  ...VmW&. ....E.
0010  00 3c 00 00 40 00 3a 06 e7 56 2b f0 42 c8 c0 a8  .<..@.: .V+.B...
0020  2a 05 00 00 50 95 ec ee 09 6c 63 bf 01 83 eb a0 12  *.P.... 1c. ....

```

No: 13 - Time: 6.062914 - Source: 43.240.66.200 - Destination: 192.168.42.5 - Length: 74 - Protocol: TCP - Info: http(80) → 38380 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1400 SACK PERM=1 TSecr=339210343 TSval=3785087730 WS=128 - New Column: 13

Third packet is from receiver to sender with SYN bit as 0 & ACK bit as 1. There is no payload (len = 0) and sequence number 1 , ack number 1 is exchanged (this is relative sequence number given by wireshark).



Finally a 4th packet is sent as a GET request for the iso file.

3) For pinging I pinged google.com (216.58.203.142) from my host IP(192.168.42.115)
 First a DNS request was made from host followed by a DNS response with the IP address of google.com. The DNS server is at 192.168.42.129.

4 6.290205	192.168.42.115	192.168.42.129	70 DNS	Standard query 0xa310 A google.com
5 6.291516	192.168.42.129	192.168.42.115	86 DNS	Standard query response 0xa310 A google.com A 216.58.203.142

Then repeated ping requests were sent and ping replies were received. The protocol is ICMP , packet length is 98 bytes.

Every request and reply packet has a ttl and a (reply in xx / request in xx). There is also sequence number in the format

<sequence-number-in-big-endian>/<sequence-number-in-little-endian>

No.	Time	Source	Destination	Length	Protocol	Info
6	6.292057	192.168.42.115	216.58.203.142	98	ICMP	Echo (ping) request id=0x1d8c, seq=1/256, ttl=64 (reply in 7)
7	6.402146	216.58.203.142	192.168.42.115	98	ICMP	Echo (ping) reply id=0x1d8c, seq=1/256, ttl=52 (request in 6)
10	7.293649	192.168.42.115	216.58.203.142	98	ICMP	Echo (ping) request id=0x1d8c, seq=2/512, ttl=64 (reply in 15)
15	7.381507	216.58.203.142	192.168.42.115	98	ICMP	Echo (ping) reply id=0x1d8c, seq=2/512, ttl=52 (request in 10)
33	8.295608	192.168.42.115	216.58.203.142	98	ICMP	Echo (ping) request id=0x1d8c, seq=3/768, ttl=64 (reply in 34)
34	8.370720	216.58.203.142	192.168.42.115	98	ICMP	Echo (ping) reply id=0x1d8c, seq=3/768, ttl=52 (request in 33)
61	9.296039	192.168.42.115	216.58.203.142	98	ICMP	Echo (ping) request id=0x1d8c, seq=4/1024, ttl=64 (reply in 62)
62	9.372995	216.58.203.142	192.168.42.115	98	ICMP	Echo (ping) reply id=0x1d8c, seq=4/1024, ttl=52 (request in 61)
75	10.297204	192.168.42.115	216.58.203.142	98	ICMP	Echo (ping) request id=0x1d8c, seq=5/1280, ttl=64 (reply in 76)
76	10.371040	216.58.203.142	192.168.42.115	98	ICMP	Echo (ping) reply id=0x1d8c, seq=5/1280, ttl=52 (request in 75)
81	11.299095	192.168.42.115	216.58.203.142	98	ICMP	Echo (ping) request id=0x1d8c, seq=6/1536, ttl=64 (reply in 82)
82	11.371308	216.58.203.142	192.168.42.115	98	ICMP	Echo (ping) reply id=0x1d8c, seq=6/1536, ttl=52 (request in 81)
83	12.300697	192.168.42.115	216.58.203.142	98	ICMP	Echo (ping) request id=0x1d8c, seq=7/1792, ttl=64 (reply in 84)
84	12.371129	216.58.203.142	192.168.42.115	98	ICMP	Echo (ping) reply id=0x1d8c, seq=7/1792, ttl=52 (request in 83)
85	13.302240	192.168.42.115	216.58.203.142	98	ICMP	Echo (ping) request id=0x1d8c, seq=8/2048, ttl=64 (reply in 86)
86	13.397088	216.58.203.142	192.168.42.115	98	ICMP	Echo (ping) reply id=0x1d8c, seq=8/2048, ttl=52 (request in 85)
90	14.303279	192.168.42.115	216.58.203.142	98	ICMP	Echo (ping) request id=0x1d8c, seq=9/2304, ttl=64 (reply in 91)
91	14.371322	216.58.203.142	192.168.42.115	98	ICMP	Echo (ping) reply id=0x1d8c, seq=9/2304, ttl=52 (request in 90)
93	15.304608	192.168.42.115	216.58.203.142	98	ICMP	Echo (ping) request id=0x1d8c, seq=10/2560, ttl=64 (reply in 96)
95	15.370440	216.58.203.142	192.168.42.115	98	ICMP	Echo (ping) reply id=0x1d8c, seq=10/2560, ttl=52 (request in 93)
97	16.305786	192.168.42.115	216.58.203.142	98	ICMP	Echo (ping) request id=0x1d8c, seq=11/2816, ttl=64 (reply in 98)
98	16.378308	216.58.203.142	192.168.42.115	98	ICMP	Echo (ping) reply id=0x1d8c, seq=11/2816, ttl=52 (request in 97)
99	17.307548	192.168.42.115	216.58.203.142	98	ICMP	Echo (ping) request id=0x1d8c, seq=12/3072, ttl=64 (reply in 100)
1...	17.378415	216.58.203.142	192.168.42.115	98	ICMP	Echo (ping) reply id=0x1d8c, seq=12/3072, ttl=52 (request in 99)
1...	18.308666	192.168.42.115	216.58.203.142	98	ICMP	Echo (ping) request id=0x1d8c, seq=13/3328, ttl=64 (reply in 102)
1...	18.379530	216.58.203.142	192.168.42.115	98	ICMP	Echo (ping) reply id=0x1d8c, seq=13/3328, ttl=52 (request in 101)
1...	19.309764	192.168.42.115	216.58.203.142	98	ICMP	Echo (ping) request id=0x1d8c, seq=14/3584, ttl=64 (reply in 104)
1...	19.399130	216.58.203.142	192.168.42.115	98	ICMP	Echo (ping) reply id=0x1d8c, seq=14/3584, ttl=52 (request in 103)
1...	20.311278	192.168.42.115	216.58.203.142	98	ICMP	Echo (ping) request id=0x1d8c, seq=15/3840, ttl=64 (reply in 111)

▶ Frame 124: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
 ▶ Ethernet II, Src: ba:53:6e:4d:13:d2 (ba:53:6e:4d:13:d2), Dst: 46:a5:bb:0c:07:ab (46:a5:bb:0c:07:ab)
 ▶ Internet Protocol Version 4, Src: 216.58.203.142, Dst: 192.168.42.115
 ▶ Internet Control Message Protocol

4) For nmap I created a VM with IP 192.168.244.128. The VM has 4 apps running.

APP	PORT
SSH	22
HTTP APACHE SERVER	80
PROMETHEUS SERVER	9090
NODE-EXPORTER SERVER	9100

Output produced on running nmap 192.168.244.128

```
harsh@harsh-Inspiron-5558:~$ nmap 192.168.244.128
Starting Nmap 7.01 ( https://nmap.org ) at 2018-03-01 22:12 IST
Nmap scan report for 192.168.244.128
Host is up (0.0017s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9090/tcp  open  zeus-admin
9100/tcp  open  jetdirect

Nmap done: 1 IP address (1 host up) scanned in 13.16 seconds
```

Analysis on wireshark

On running nmap 2012 TCP packets were shared between VM IP and vmware interface IP(192.168.244.1)

4 ARP packets between 2 VMware MAC addresses.

(to find MAC address of 192.168.244.128 & 192.168.244.1)

Nmap scans for open ports by sending TCP packets (with SYN bit as 1) with different destination ports. If it receives an ACK back , then it means port is active.

The screenshot shows a subset of the diff ports nmap has scanned.

No.	Time	Source	Destination	Length	Protocol	Info
12 0.005268		192.168.244.1	192.168.244.128	74	TCP	416544 - smux(199) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658208 TSecr=0 WS=128
13 0.005291		192.168.244.1	192.168.244.128	74	TCP	52478 - submission(587) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658208 TSecr=0 WS=128
14 0.005313		192.168.244.1	192.168.244.128	74	TCP	47682 - rfb(5900) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658208 TSecr=0 WS=128
15 0.005321		192.168.244.128	192.168.244.1	60	TCP	epmap(135) - 56786 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
16 0.005333		192.168.244.128	192.168.244.1	60	TCP	55892 - ms-wbtserver(1270) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658208 TSecr=0 WS=128
17 0.005421		192.168.244.1	192.168.244.128	74	TCP	53549 - ftp(21) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658208 TSecr=0 WS=128
18 0.005426		192.168.244.128	192.168.244.1	60	TCP	blackjack(1028) - 45578 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
19 0.005482		192.168.244.1	192.168.244.128	74	TCP	49072 - dd1-tcp-(8888) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658208 TSecr=0 WS=128
20 0.005491		192.168.244.128	192.168.244.1	60	TCP	sunrpc(111) - 54882 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
21 0.005505		192.168.244.128	192.168.244.1	60	TCP	53545 - ms-wbtserver(1270) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658208 TSecr=0 WS=128
22 0.005537		192.168.244.128	192.168.244.1	74	TCP	http(80) - 51818 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=2369058959 TSecr=895658208
23 0.005545		192.168.244.1	192.168.244.128	74	TCP	37094 - mysql(3306) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658208 TSecr=0 WS=128
24 0.005553		192.168.244.1	192.168.244.128	66	TCP	51810 - http(80) [ACK] Seq=1 Ack=1 Win=29212 Len=0 MSS=1460 SACK_PERM=1 TSval=895658208 TSecr=2369058959
25 0.005567		192.168.244.128	192.168.244.1	60	TCP	38382 - http-alt(8080) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658208 TSecr=0 WS=128
27 0.005593		192.168.244.128	192.168.244.1	60	TCP	aauth(113) - 53314 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
26 0.005594		192.168.244.1	192.168.244.128	66	TCP	51818 - http(80) [RST, ACK] Seq=0 Ack=1 Win=29212 Len=0 MSS=1460 SACK_PERM=1 TSval=895658208 TSecr=2369058959
28 0.005632		192.168.244.128	192.168.244.1	60	TCP	Imaps(993) - 48904 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
29 0.005637		192.168.244.128	192.168.244.1	60	TCP	53546 - ms-wbtserver(1270) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658208 TSecr=0 WS=128
30 0.005657		192.168.244.128	192.168.244.1	74	TCP	33068 - ms-wbtserver(3389) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658208 TSecr=0 WS=128
31 0.005664		192.168.244.128	192.168.244.1	60	TCP	rap(256) - 49456 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
32 0.005674		192.168.244.1	192.168.244.128	74	TCP	42482 - microsoft-ds(445) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658209 TSecr=0 WS=128
33 0.005681		192.168.244.128	192.168.244.1	74	TCP	57458 - pop3(110) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658209 TSecr=0 WS=128
34 0.005689		192.168.244.128	192.168.244.1	60	TCP	51710 - smtp(25) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658209 TSecr=0 WS=128
35 0.005734		192.168.244.128	192.168.244.1	60	TCP	submission(587) - 52478 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
36 0.005750		192.168.244.1	192.168.244.128	74	TCP	38634 - http-alt(8080) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658209 TSecr=0 WS=128
37 0.005763		192.168.244.128	192.168.244.1	60	TCP	rftb(9900) - 47682 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
38 0.005769		192.168.244.128	192.168.244.1	60	TCP	52478 - submission(587) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658209 TSecr=0 WS=128
39 0.005789		192.168.244.1	192.168.244.128	74	TCP	52714 - ms-wbtserver(3389) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658209 TSecr=0 WS=128
40 0.005797		192.168.244.128	192.168.244.1	60	TCP	telnet(23) - 55880 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
41 0.005813		192.168.244.1	192.168.244.128	74	TCP	58568 - rtsp(554) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658209 TSecr=0 WS=128
42 0.005822		192.168.244.128	192.168.244.1	60	TCP	51710 - smtp(25) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658209 TSecr=0 WS=128
43 0.005833		192.168.244.128	192.168.244.1	74	TCP	56152 - http(80) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658209 TSecr=0 WS=128
44 0.005855		192.168.244.1	192.168.244.128	74	TCP	39272 - mysql(3306) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658209 TSecr=0 WS=128
45 0.005867		192.168.244.128	192.168.244.1	60	TCP	dd1-tcp-(1888) - 49672 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
46 0.005896		192.168.244.128	192.168.244.1	60	TCP	domain(53) - 53778 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
47 0.005915		192.168.244.128	192.168.244.1	60	TCP	53545 - ms-wbtserver(1270) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658209 TSecr=0 WS=128
48 0.005927		192.168.244.128	192.168.244.1	60	TCP	mysql(3306) - 37094 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49 0.005937		192.168.244.1	192.168.244.128	74	TCP	58462 - h323hostcall(1720) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658209 TSecr=0 WS=128
50 0.005957		192.168.244.1	192.168.244.128	74	TCP	46164 - bsquarehttp(1232) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658209 TSecr=0 WS=128
51 0.005967		192.168.244.128	192.168.244.1	60	TCP	50901 - http(8080) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658209 TSecr=0 WS=128
52 0.005978		192.168.244.1	192.168.244.128	74	TCP	56152 - http(8080) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658209 TSecr=0 WS=128
53 0.005993		192.168.244.1	192.168.244.128	74	TCP	57112 - 34574 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658209 TSecr=0 WS=128
54 0.006004		192.168.244.128	192.168.244.1	60	TCP	50924 - http(8080) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658209 TSecr=0 WS=128
55 0.006014		192.168.244.128	192.168.244.1	60	TCP	53545 - ms-wbtserver(1270) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658209 TSecr=0 WS=128
56 0.006039		192.168.244.128	192.168.244.1	60	TCP	nebelos-svn(139) - 33068 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
57 0.006041		192.168.244.1	192.168.244.128	74	TCP	49092 - rxapi(10010) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658209 TSecr=0 WS=128
58 0.006062		192.168.244.1	192.168.244.128	74	TCP	51310 - onep-tls(15002) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658209 TSecr=0 WS=128
59 0.006074		192.168.244.128	192.168.244.1	60	TCP	microsoft-ds(445) - 42482 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
60 0.006081		192.168.244.1	192.168.244.128	74	TCP	56568 - device(861) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658209 TSecr=0 WS=128

If a port is not up , the VM send a TCP packet with RST & ACK field set as 1 , meaning port is active.

No.	Time	Source	Destination	Length	Protocol	Info
23 0.005548		192.168.244.1	192.168.244.128	74	TCP	37094 - mysql(3306) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658208 TSecr=0 WS=128
48 0.005927		192.168.244.128	192.168.244.1	60	TCP	mysql(3306) - 37094 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

If port is up , nmap tries to find whether the app is listening at the port or transmitting.

On sending TCP SYN packet to 9090 , it got an ACK back.

On sending TCP ACK packet to 9090 , it got an RST back, meaning port is not transmitting anything.

No.	Time	Source	Destination	Length	Protocol	Info
884 0.024705		192.168.244.1	192.168.244.128	74	TCP	49068 - websm(9090) [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=895658228 TSecr=0 WS=128
1024 0.026487		192.168.244.128	192.168.244.1	74	TCP	websm(9090) - 49068 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=2369058964 TSecr=8956582
1025 0.026500		192.168.244.1	192.168.244.128	66	TCP	49068 - websm(9090) [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=895658229 TSecr=2369058964
1040 0.026649		192.168.244.1	192.168.244.128	66	TCP	49068 - websm(9090) [RST, ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=895658230 TSecr=2369058964

Link Layer

1)

Fraction of Control Packets :: 120394 / 242393 = 49.7%

The command to filter control packets is **wlan.fc.type == 1**

D-LinkIn_80:0f:..	68 802.11	Clear-to-send, Flags=.....c
D-LinkIn_80:0f:..	68 802.11	Clear-to-send, Flags=.....c
D-LinkIn_80:0f:..	68 802.11	Clear-to-send, Flags=.....c
D-LinkIn_80:0f:..	68 802.11	Clear-to-send, Flags=.....c
D-LinkIn_80:0f:..	68 802.11	Clear-to-send, Flags=.....c
D-LinkIn_80:0f:..	68 802.11	Clear-to-send, Flags=.....c
D-LinkIn_80:0f:..	68 802.11	Clear-to-send, Flags=.....c
D-LinkIn_80:0f:..	68 802.11	Clear-to-send, Flags=.....c
D-LinkIn_80:0f:..	68 802.11	Clear-to-send, Flags=.....c
D-LinkIn_80:0f:..	68 802.11	Clear-to-send, Flags=.....c
D-LinkIn_80:0f:..	68 802.11	Clear-to-send, Flags=.....c
D-LinkIn_80:0f:..	68 802.11	Clear-to-send, Flags=.....c
D-LinkIn_80:0f:..	68 802.11	Clear-to-send, Flags=.....c
D-LinkIn_80:0f:..	68 802.11	Clear-to-send, Flags=.....c
D-LinkIn_80:0f:..	68 802.11	Clear-to-send, Flags=.....c
HonHaiPr_98:4f:..	68 802.11	Acknowledgement, Flags=.....c
IntelCor_63:85:..	68 802.11	Acknowledgement, Flags=.....c
IntelCor_92:c7:..	68 802.11	Acknowledgement, Flags=.....c

captured (544 bits)

00 00 ..6./@.

Packets: 242393 · Displayed: 120394 (49.7%) · Load time: 0:3.866

Fraction of Data Packets :: 116030 / 242393 = 47.9%

The command to filter data packets is **wlan.fc.type == 2**

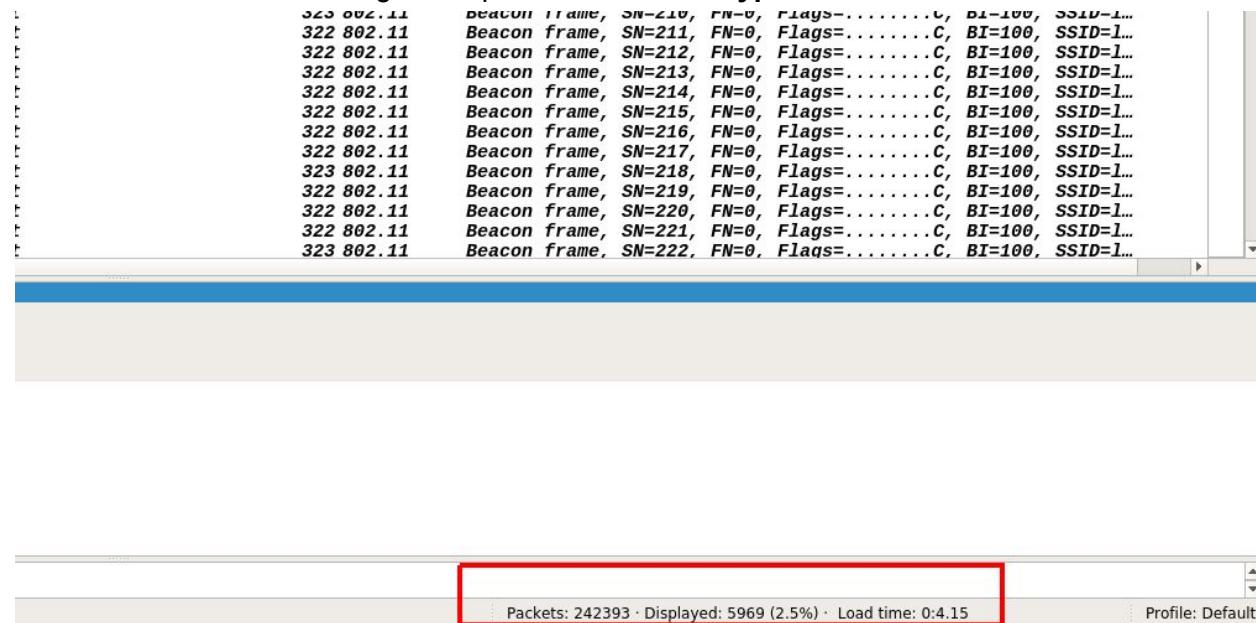
D-LinkIn_80:0f:6b	82 802.11	Null function (No data), SN=3693, FN=0, Flags=...P...
IntelCor_92:c7:eb	152 802.11	QoS Data, SN=959, FN=0, Flags=.p....F.C
D-LinkIn_80:0f:6b	175 802.11	QoS Data, SN=146, FN=0, Flags=.p.....TC
D-LinkIn_80:0f:6b	168 802.11	QoS Data, SN=147, FN=0, Flags=.p.....TC
D-LinkIn_80:0f:6b	175 802.11	QoS Data, SN=148, FN=0, Flags=.p.....TC
IntelCor_18:89:2d	411 802.11	QoS Data, SN=1835, FN=0, Flags=.p....F.C
D-LinkIn_80:0f:6b	175 802.11	QoS Data, SN=149, FN=0, Flags=.p.....TC
IntelCor_18:89:2d	411 802.11	QoS Data, SN=1836, FN=0, Flags=.p....F.C
IntelCor_92:c7:eb	152 802.11	QoS Data, SN=961, FN=0, Flags=.p....F.C
IntelCor_92:c7:eb	152 802.11	QoS Data, SN=962, FN=0, Flags=.p....F.C
D-LinkIn_80:0f:6b	82 802.11	Null function (No data), SN=3694, FN=0, Flags=.....
Motorola_18:5d:36	140 802.11	QoS Data, SN=1630, FN=0, Flags=.p....F.C
D-LinkIn_80:0f:6b	84 802.11	QoS Null function (No data), SN=0, FN=0, Flags=...P..
D-LinkIn_80:0f:6b	160 802.11	QoS Data, SN=1408, FN=0, Flags=.p.....TC

.....

Packets: 242393 · Displayed: 116030 (47.9%) · Load time: 0:3.848

Fraction of Management Packets :: 5969 / 242393 = 2.5%

The command to filter management packets is wlan.fc.type == 0



2)

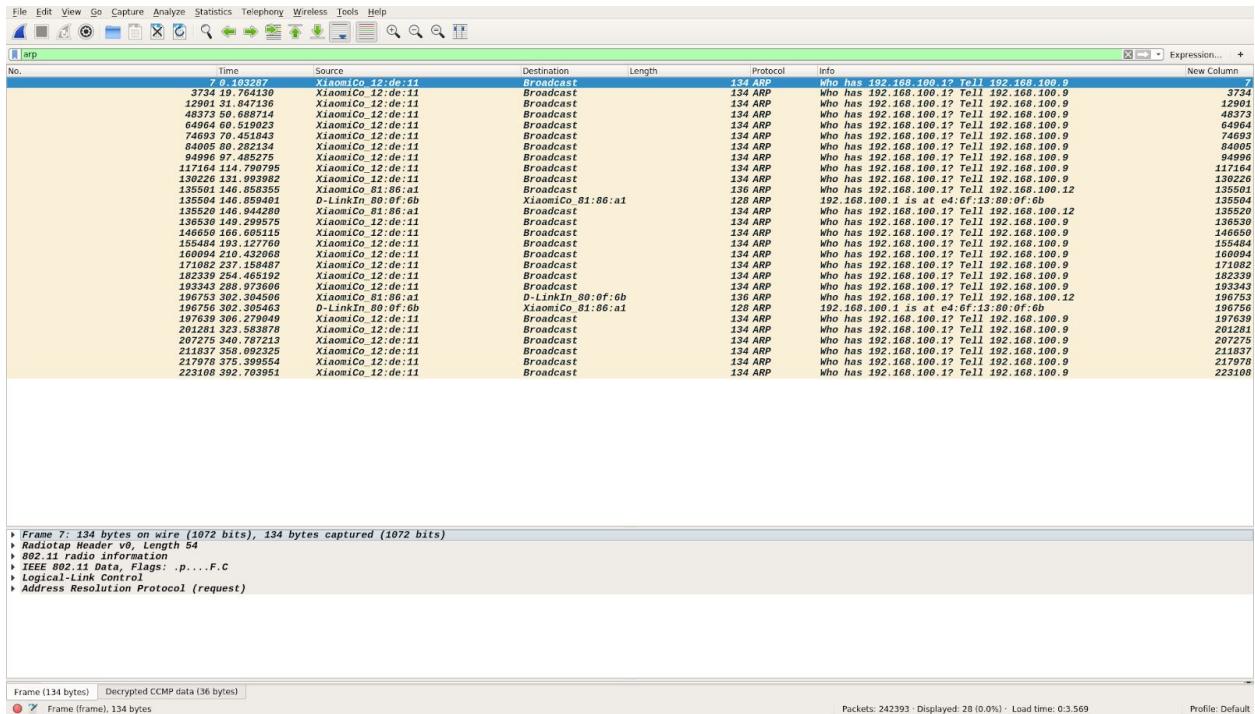
Fraction of ARP :: 28 / 242393 = 0.0%

No.	Time	Source	Destination	Protocol	Info
1	0.000000	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=166, FN=0, Flags=.....C, BT=100, SSID=l...
6	0.102443	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=211, FN=0, Flags=.....C, BT=100, SSID=l...
7	0.103287	XiaomiCo_12:de:11	Broadcast	134 ARP	Who has 192.168.100.17 Tell 192.168.100.9
10	0.204960	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=166, FN=0, Flags=.....C, BT=100, SSID=l...
12	0.205058	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=169, FN=0, Flags=.....C, BT=100, SSID=l...
14	0.409583	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=210, FN=0, Flags=.....C, BT=100, SSID=l...
18	0.512066	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=217, FN=0, Flags=.....C, BT=100, SSID=l...
28	0.614384	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=218, FN=0, Flags=.....C, BT=100, SSID=l...
35	0.614575	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=219, FN=0, Flags=.....C, BT=100, SSID=l...
72	0.819227	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=174, FN=0, Flags=.....C, BT=100, SSID=l...
75	0.921623	D-LinkIn 80:0f:6b	Broadcast	323 802.11	Beacon frame, SN=175, FN=0, Flags=.....C, BT=100, SSID=l...
78	1.024016	D-LinkIn 80:0f:6b	Broadcast	323 802.11	Beacon frame, SN=176, FN=0, Flags=.....C, BT=100, SSID=l...
83	1.124494	D-LinkIn 80:0f:6b	Broadcast	323 802.11	Beacon frame, SN=177, FN=0, Flags=.....C, BT=100, SSID=l...
88	1.228790	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=178, FN=0, Flags=.....C, BT=100, SSID=l...
99	1.332191	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=179, FN=0, Flags=.....C, BT=100, SSID=l...
91	1.433661	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=180, FN=0, Flags=.....C, BT=100, SSID=l...
94	1.532902	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=181, FN=0, Flags=.....C, BT=100, SSID=l...
97	1.632377	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=182, FN=0, Flags=.....C, BT=100, SSID=l...
116	1.740791	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=183, FN=0, Flags=.....C, BT=100, SSID=l...
127	1.843274	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=184, FN=0, Flags=.....C, BT=100, SSID=l...
137	1.945680	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=185, FN=0, Flags=.....C, BT=100, SSID=l...
178	2.044814	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=186, FN=0, Flags=.....C, BT=100, SSID=l...
181	2.159426	D-LinkIn 80:0f:6b	Broadcast	323 802.11	Beacon frame, SN=187, FN=0, Flags=.....C, BT=100, SSID=l...
204	2.252843	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=188, FN=0, Flags=.....C, BT=100, SSID=l...
207	2.355189	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=189, FN=0, Flags=.....C, BT=100, SSID=l...
212	2.457509	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=190, FN=0, Flags=.....C, BT=100, SSID=l...
267	2.569028	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=191, FN=0, Flags=.....C, BT=100, SSID=l...
271	2.662427	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=192, FN=0, Flags=.....C, BT=100, SSID=l...
272	2.764899	D-LinkIn 80:0f:6b	Broadcast	323 802.11	Beacon frame, SN=193, FN=0, Flags=.....C, BT=100, SSID=l...
299	2.867211	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=194, FN=0, Flags=.....C, BT=100, SSID=l...
305	2.969597	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=211, FN=0, Flags=.....C, BT=100, SSID=l...
306	3.072028	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=212, FN=0, Flags=.....C, BT=100, SSID=l...
310	3.174449	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=213, FN=0, Flags=.....C, BT=100, SSID=l...
313	3.276870	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=214, FN=0, Flags=.....C, BT=100, SSID=l...
315	3.379228	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=215, FN=0, Flags=.....C, BT=100, SSID=l...
316	3.481586	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=216, FN=0, Flags=.....C, BT=100, SSID=l...
318	3.583985	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=217, FN=0, Flags=.....C, BT=100, SSID=l...
319	3.686363	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=218, FN=0, Flags=.....C, BT=100, SSID=l...
333	3.788236	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=219, FN=0, Flags=.....C, BT=100, SSID=l...
363	3.891287	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=220, FN=0, Flags=.....C, BT=100, SSID=l...
369	3.993662	D-LinkIn 80:0f:6b	Broadcast	322 802.11	Beacon frame, SN=221, FN=0, Flags=.....C, BT=100, SSID=l...

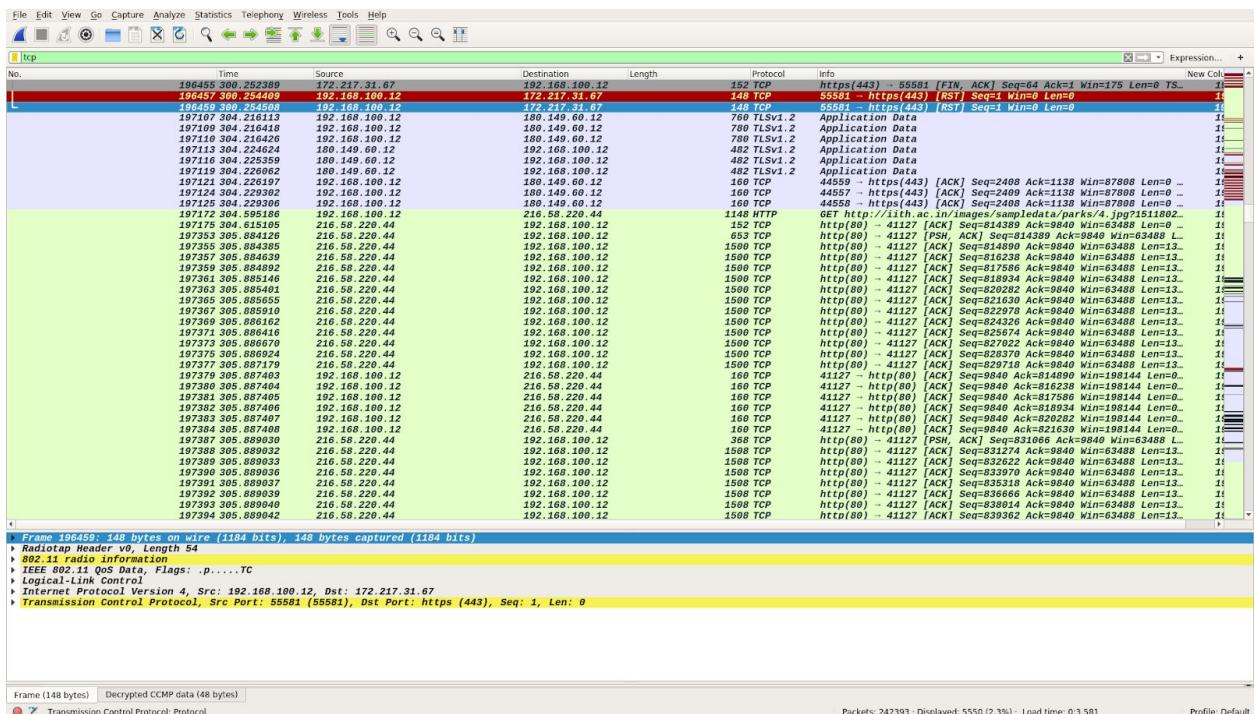
Packets: 242393 · Displayed: 5259 (2.2%) · Load time: 0:4.86 · Profile: Default

Fraction of Broadcast :: 5259 / 242393 = 2.2%

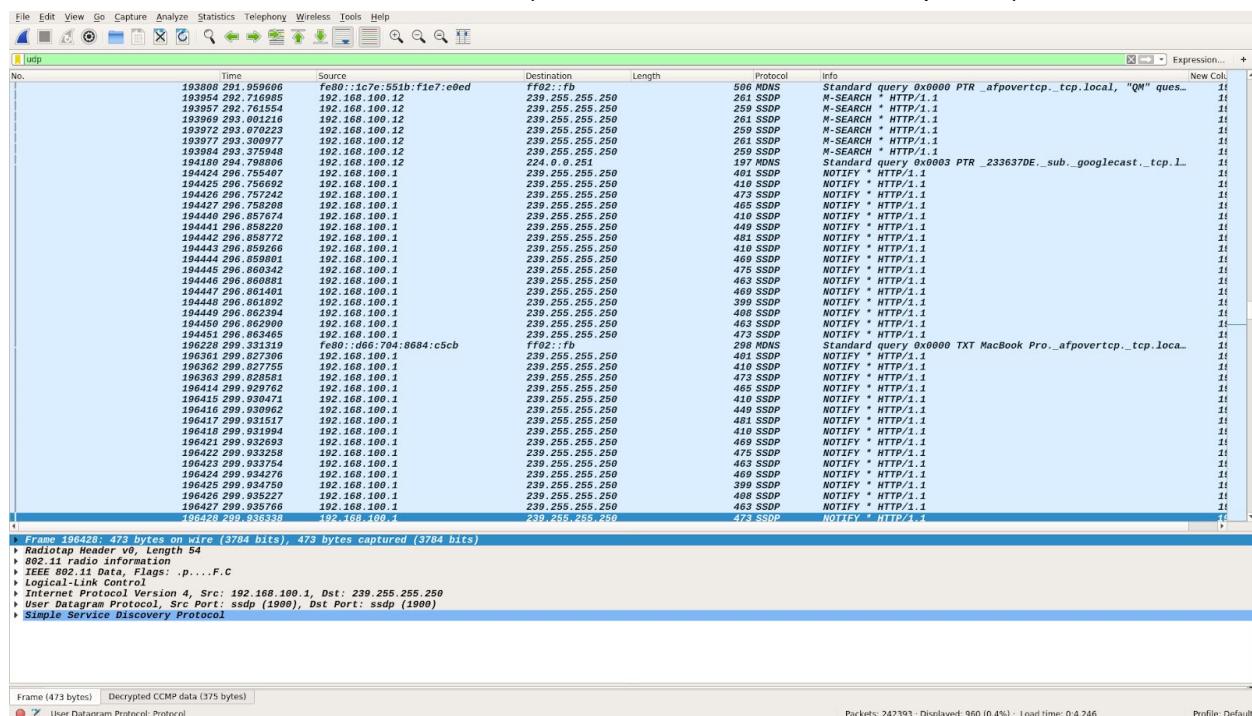
Wireshark Filter :: eth.addr == ff:ff:ff:ff:ff:ff || fddi.addr == ff:ff:ff:ff:ff:ff || tr.addr == ff:ff:ff:ff:ff:ff || wlan.da == ff:ff:ff:ff:ff:ff || wlan.sa == ff:ff:ff:ff:ff:ff || ip.addr == 255.255.255.255



Fraction of TCP :: 5550 / 242393 = 2.3% (TCP packets are maximum)

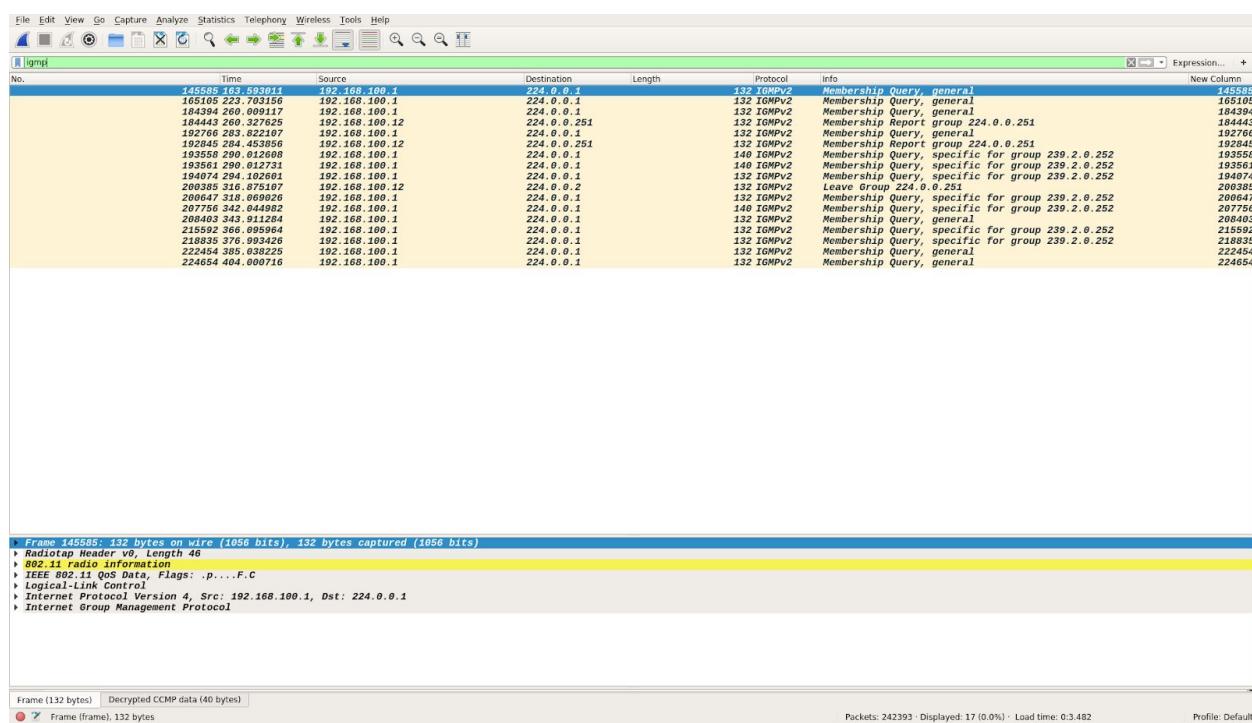


Fraction of UDP :: 960 / 242393 = 0.4% (UDP is lesser than TCP as expected)



Fraction of ICMP :: 0 / 242393 = 0.0% (no ping operation during capture)

Fraction of IGMP :: 17 / 242393 = 0.0%



3)

```
Command used :: tshark -r monitor_mobile_traffic.pcap -T fields -e wlan.sa wlan.da | sort | uniq | wc -l
```

No of unique users (MACs addresses) :: 1134

```

e7:fc:13:80:0f:db
e7:8c:07:61:92:6e
e7:8c:12:12:06:bb
e2:3d:3d:3d:3d:3d
e8:66:7b:4f:ab:fb
e8:67:13:80:0f:db
e8:67:13:80:0f:db
e9:d0:0d:35:aa:ff
e9:e8:0d:ad:45:b1
e9:e8:0d:ad:45:b1
e9:8b:21:33:f8:4a
e9:8b:21:33:f8:4a
e9:7e:a3:e6:39:86
e9:7e:a3:e6:39:86
e9:c1:90:0d:41:43
e9:c1:90:0d:41:43
e9:c1:50:f5:99:a9
e9:c1:50:f5:99:a9
e9:c1:13:80:0f:db
e9:c1:13:80:0f:db
e9:9e:b5:5a:0b:68
e9:9e:b5:5a:0b:68
e9:fa:77:b5:2c:75
e9:fa:77:b5:2c:75
e9:0d:28:02:4e:e7
e9:0d:28:02:4e:e7
ee:0d:24:50:23:88
ee:0d:24:50:23:88
ee:9e:96:98:4f:bb
ee:9e:96:98:4f:bb
ee:9e:2f:0c:83:4f:bb
ee:9e:2f:0c:83:4f:bb
ee:0f:13:90:0e:db
ee:83:32:f7:0f:75
ee:83:32:f7:0f:75
ee:f1:70:ae:83:1a
ef:2f:f5:84:36:aa
f0:3f:96:98:4f:bb
f0:3f:96:98:4f:bb
f0:3f:96:98:4f:bb
f0:7f:dc:83:4f:bb
f0:7f:fc:40:38:02
f0:9b:89:7d:aa:ff
f0:9b:89:7d:aa:ff
f0:ab:75:e2:9c:75
f0:ab:75:e2:9c:75
f1:02:ec:cb:0d:47
f1:37:c5:ae:bd:93
f1:38:0b:80:36:bd
f2:38:0b:80:36:bd
f2:7e:1e:bb:df:1f
f2:50:fb:39:78:15
f4:38:96:98:4f:bb
f4:38:96:98:4f:bb
f6:0f:13:80:0f:db
f6:0f:13:80:0f:db
f6:96:9f:cd:79:b9
f6:9f:32:77:2c:75
f6:9f:32:77:2c:75
f7:8d:35:77:2c:75
f7:be:32:a7:28:f5
f8:98:32:77:2c:75
f8:98:32:77:2c:75
f9:38:be:88:4f:bb
f9:38:be:88:4f:bb
f9:18:92:43:3d:00
f9:38:96:98:4f:bb
fc:0f:13:80:0f:db
fc:99:fe:26:74:5c
fc:99:fe:26:74:5c
fe:32:4c:35:a3:c6
fe:8d:2d:d6:19:47
fe:8d:2d:d6:19:47
ff:0a:9f:d8:7e:33
ff:0f:13:80:0f:db

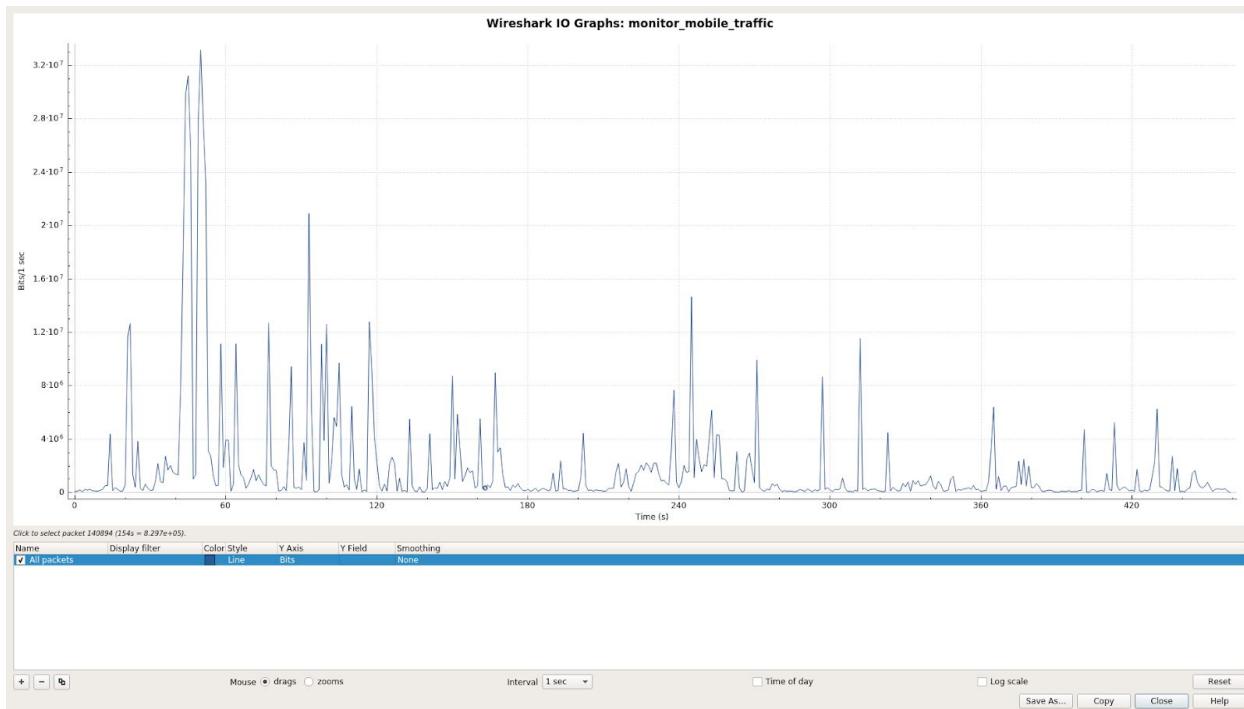
harsh@harsh-Inspiron-5558:~/bttech/sen-6/C3543-computer-networks/Lab-Assigments$ tshark -r monitor_mobile_traffic.pcap -T fields -e wlan.sa wlan.da | sort | uniq | wc -l
1154
harsh@harsh-Inspiron-5558:~/bttech/sen-6/C3543-computer-networks/Lab-Assigments$ 

```

4)

The traffic pattern from IO graph shows Bits/sec on Y-Axis and time on X-Axis

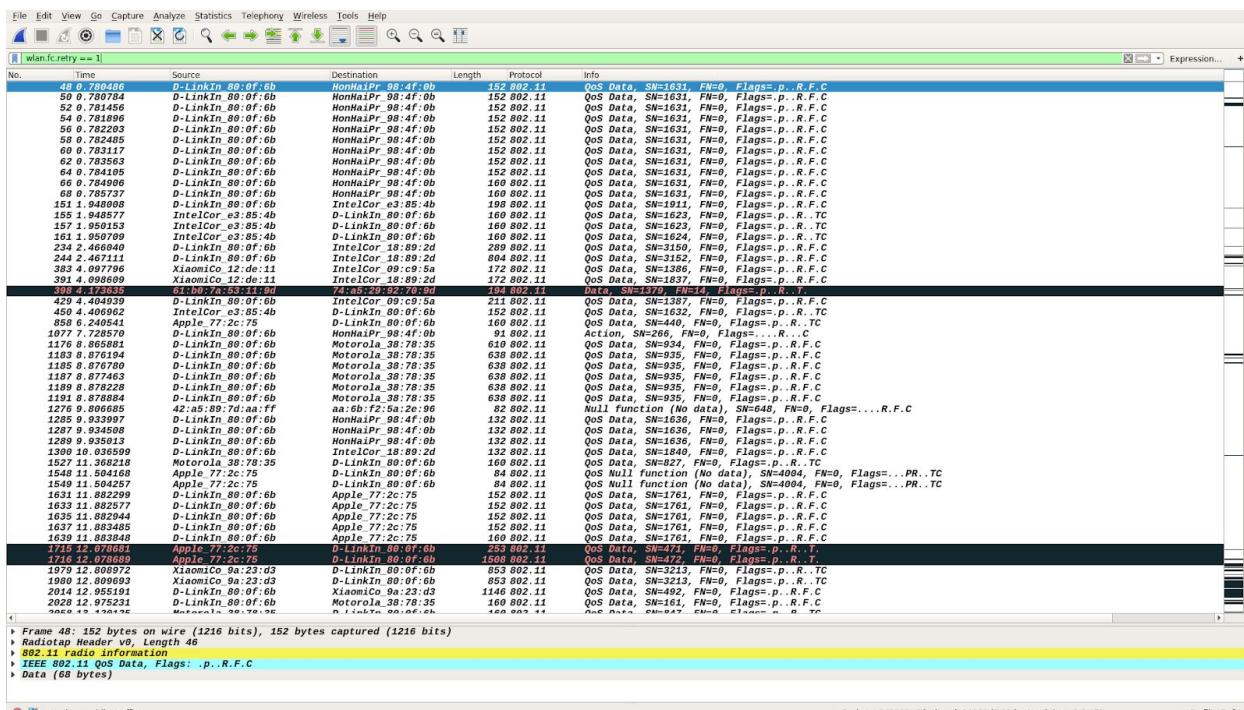
Total packets were captured for 460 seconds . In the beginning seconds there was a sudden burst of traffic. After that traffic was relatively lesser. But small bursts of packets are still there, showing typical internet behaviour.



5)

Command used :: `wlan.fc.retry == 1`

Fraction of retransmission :: $14970 / 242393 (6.2\%)$



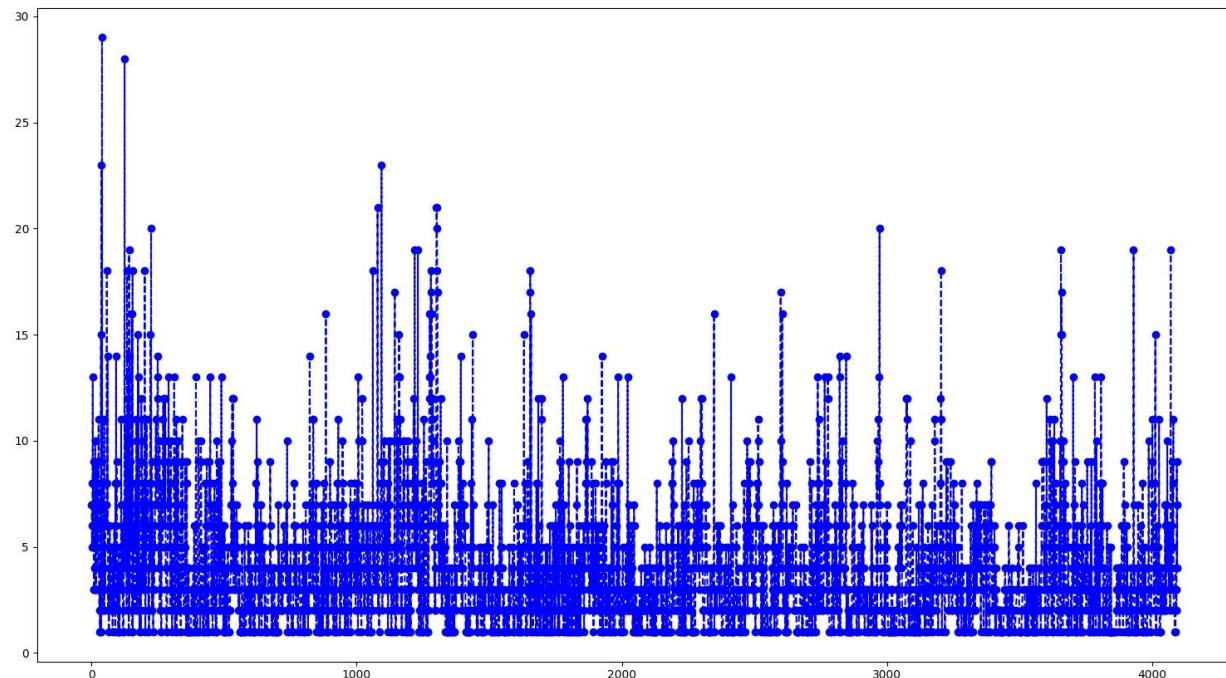
6)

This is a plot of **maximum number of retransmission vs packet number**.

The X axis denotes sequence number & the Y axis denotes no. of retransmissions for that sequence number. The sequence numbers that are not in the graph mean that the no. of retransmissions for them is 0. For the sequence number in graph , they have at least 1 retransmission.

The number of retransmissions vary between 1 and 29 and 6.2% of all packets are link-layer retransmission.

This graph was plotted using numpy and pylab.



Drive Links for PCAP files

Pinging_google_com.pcap (for Transport Layer Q3)

https://drive.google.com/file/d/1jtSLCMuF9Vku_XSk-m-FMeASjRqoAce/view?usp=sharing

Nmap-packets.pcap (for Transport Layer Q4)

<https://drive.google.com/file/d/1LIWDpoEliGoWyxkyEck-61AHG232Vtbp/view?usp=sharing>

Monitor_mobile_traffic.pcap : containing the packet capture in monitor mode of WiFi for Link-Layer

https://drive.google.com/open?id=1p6CYD_zKkbJ8rDPe3Ztf-ZXnWk4xkN8A

Internet_ubuntu_72sec.pcap :: download ubuntu iso

https://drive.google.com/file/d/1JbWS2w0p1Fx_r1tqMjlzdXkNgyEbhzaC/view?usp=sharing