Name: **Mareena Fernandes**
Roll No.: **8669**
Class: **TE IT**
Batch: **B**

EXPERIMENT NO: 6

Capturing and analyzing packets with tcpdump:

1)

```
mareenalinux@mareenalinux:~Desktop$ sudo apt install tcpdump -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
tcpdump is already the newest version (4.9.3-4).
0 upgraded, 0 newly installed, 0 to remove and 112 not upgraded.
```

2)

```
mareenalinux@mareenalinux:~Desktop$ tcpdump -D
1.eth0 [Up, Running]
2.lo [Up, Running, Loopback]
3.any (Pseudo-device that captures on all interfaces) [Up, Running]
4.bluetooth-monitor (Bluetooth Linux Monitor) [none]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
7.dummy0 [none]
8.sit0 [none]
9.bond0 [none]
```

3)

```
mareenalinux@mareenalinux:~Desktop$ sudo tcpdump -i eth0 -v
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
21:47:41.368975 IP (tos 0x0, ttl 1, id 22328, offset 0, flags [none], proto UDP (17), length 201)
LAPTOP-N17SJKFE.mshome.net.49634 > 239.255.255.250.1900: UDP, length 173
21:47:41.369946 IP (tos 0x0, ttl 64, id 47916, offset 0, flags [DF], proto UDP (17), length 74)
192.168.229.244.58104 > LAPTOP-N17SJKFE.mshome.net.domain: 40051+ PTR? 250.255.255.239.in-addr.arpa. (46)
21:47:41.396463 IP (tos 0x0, ttl 1, id 50673, offset 0, flags [none], proto UDP (17), length 80)
^C
LAPTOP-N17SJKFE.mshome.net.mdns > 224.0.0.251.mdns: 0 PTR (QM)? 250.255.255.239.in-addr.arpa.local. (52)
```

```
3 packets captured
27 packets received by filter
0 packets dropped by kernel
```

4)

```
mareenalinux@mareenalinux:~Desktop$ sudo tcpdump -c 8 -tttt -i eth0 -v
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
2020-11-11 21:49:41.365934 IP (tos 0x0, ttl 1, id 22332, offset 0, flags [none], proto UDP (17), length
201)
LAPTOP-N17SJKFE.mshome.net.62741 > 239.255.255.250.1900: UDP, length 173
2020-11-11 21:49:41.366510 IP (tos 0x0, ttl 64, id 52670, offset 0, flags [DF], proto UDP (17), length
74)
^C
192.168.229.244.32776 > LAPTOP-N17SJKFE.mshome.net.domain: 28935+ PTR? 250.255.255.239.in-
addr.arpa. (46)
2 packets captured
19 packets received by filter
0 packets dropped by kernel
```

5)

```
mareenalinux@mareenalinux:~Desktop$ sudo tcpdump -w savetcpdump_eth0.pcap -i eth0
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
1 Packet captured
1 packet received by filter
0 packets dropped by kernel
```

6)

```
mareenalinux@mareenalinux:~Desktop$ ls
savetcpdump_eth0.pcap
```

7)

```
mareenalinux@mareenalinux:~Desktop$ sudo tcpdump -r savetcpdump_eth0.pcap
reading from file savetcpdump_eth0.pcap, link-type EN10MB (Ethernet)
21:55:50.810625 IP6 fe80::215:5dff:fe9f:300c > ip6-allrouters: ICMP6, router solicitation, length 16
```

8)

```
mareenalinux@mareenalinux:~Desktop$ sudo tcpdump -n -i eth0 -v
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
22:17:41.376339 IP (tos 0x0, ttl 1, id 22388, offset 0, flags [none], proto UDP (17), length 201)
192.168.229.241.62590 > 239.255.255.250.1900: UDP, length 173
22:17:42.376862 IP (tos 0x0, ttl 1, id 22389, offset 0, flags [none], proto UDP (17), length 201)
192.168.229.241.62590 > 239.255.255.250.1900: UDP, length 173                                        ^C
2 packetscaptured
2 packets received by filter
0 packets dropped by kernel
```

9)

```
mareenalinux@mareenalinux:~Desktop$ sudo tcpdump -i eth0 tcp -v
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C                                               0 packets captured
0 packets received by filter
0 packets dropped by kernel
```

10)

```
mareenalinux@mareenalinux:~Desktop$ sudo tcpdump -n -i eth0 src 169.144.0.10
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
23:03:45.912733 IP 169.144.0.10.amqp > 169.144.0.20.57800: Flags [.], ack 526623844, win 243,
options [nop,nop,TS val 84981008 ecr 84982372], length 0
23:03:46.376926 IP 169.144.0.10.amqp > 169.144.0.20.57808: Flags [.], ack 175946224, win 252,
options [nop,nop,TS val 84981472 ecr 84982836], length 0
23:03:46.809344 IP 169.144.0.10.amqp > 169.144.0.20.57814: Flags [.], ack 2781799939, win 252,
options [nop,nop,TS val 84981904 ecr 84983268], length 0
23:03:46.809485 IP 169.144.0.10.amqp > 169.144.0.20.57816: Flags [.], ack 1662816815, win 252,
options [nop,nop,TS val 84981904 ecr 84983268], length 0
23:03:47.033301 IP 169.144.0.10.amqp > 169.144.0.20.57818: Flags [.], ack 2387094362, win 252,
options [nop,nop,TS val 84982128 ecr 84983492], length 0
^C
10 packets captured
12 packets received by filter
0 packets dropped by kernel
```

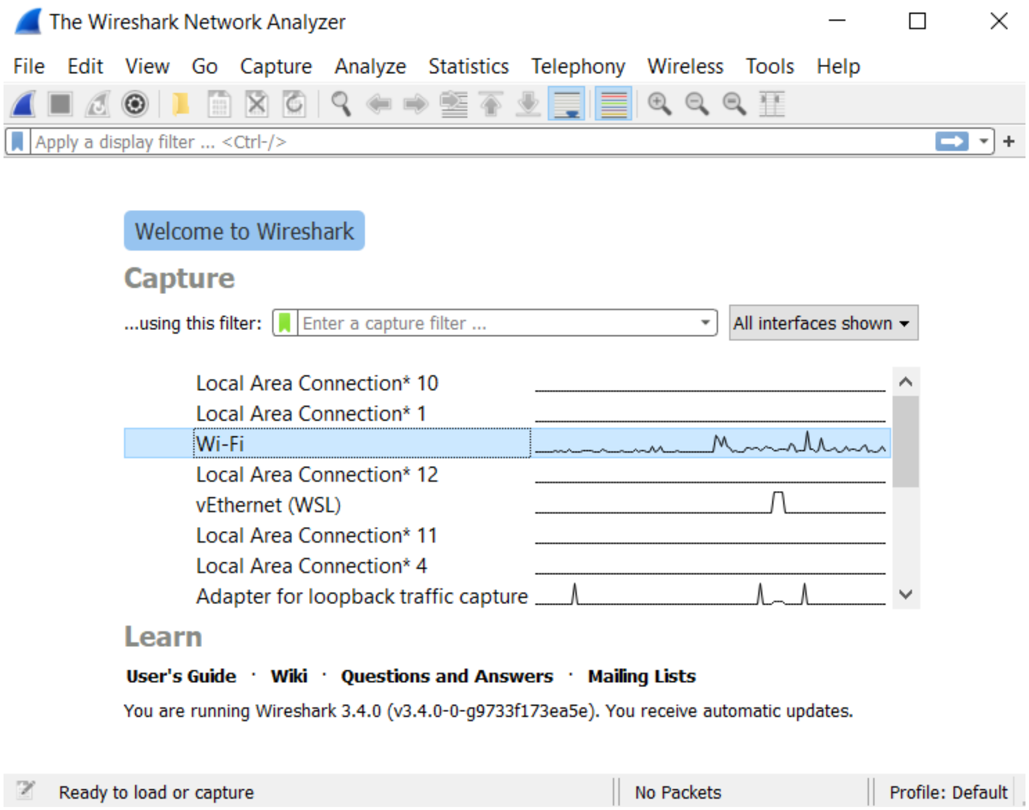
11)

```
mareenalinux@mareenalinux:~Desktop$ sudo tcpdump -c 10 -A -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes ^C
00:37:10.520060 IP compute-0-1.example.com.ssh > 169.144.0.1.39406: Flags [P.], seq
1452637331:1452637519, ack 3062125586, win 333, options [nop,nop,TS val 90591987 ecr
22687106], length 188
E...[.@.@..............V.|...T....MT.......fR..Z-
....b.:..Z5...{.'p....]."}...Z..9.?.......".@<.....V..C.....{,...OKP.2.*...`..-sS..1S...........:.O[.....{G..%ze.Pn.T..N....
....qB..5...n.....`...:=...[..0....k.....S.:..5!.9..G....!-..'..00:37:10.520319 IP 169.144.0.1.39406 > compute-0-
1.example.com.ssh: Flags [.], ack 188, win 13930, options [nop,nop,TS val 22687109 ecr 90591987],
length 0E..4kS@.@.|+.............T.V.}O..6j.d......Z-..fR.
```

12)

```
mareenalinux@mareenalinux:~Desktop$ sudo tcpdump -c 10 -XX -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decodelistening on eth0, link-type
EN10MB (Ethernet), capture size 262144 bytes00:39:15.124363 IP compute-0-1.example.com.ssh >
169.144.0.1.39406: Flags [P.], seq 1452640859:1452641047, ack 3062126346, win 333, options
[nop,nop,TS val 90716591 ecr 22718257], length 188
0x0000: 0a00 2700 0000 0800 27f4 f935 0800 4510 ..'.....'..5..E.
0x0010: 00f0 5bc6 4000 4006 8afc a990 0014 a990 ..[.@.@........
0x0020: 0001 0016 99ee 5695 8a5b b684 570a 8018 ......V..[..W...
0x0030: 014d 5418 0000 0101 080a 0568 39af 015a .MT........h9..Z
0x0040: a731 adb7 58b6 1a0f 2006 df67 c9b6 4479 .1..X......g..Dy
```

With Wireshark:


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

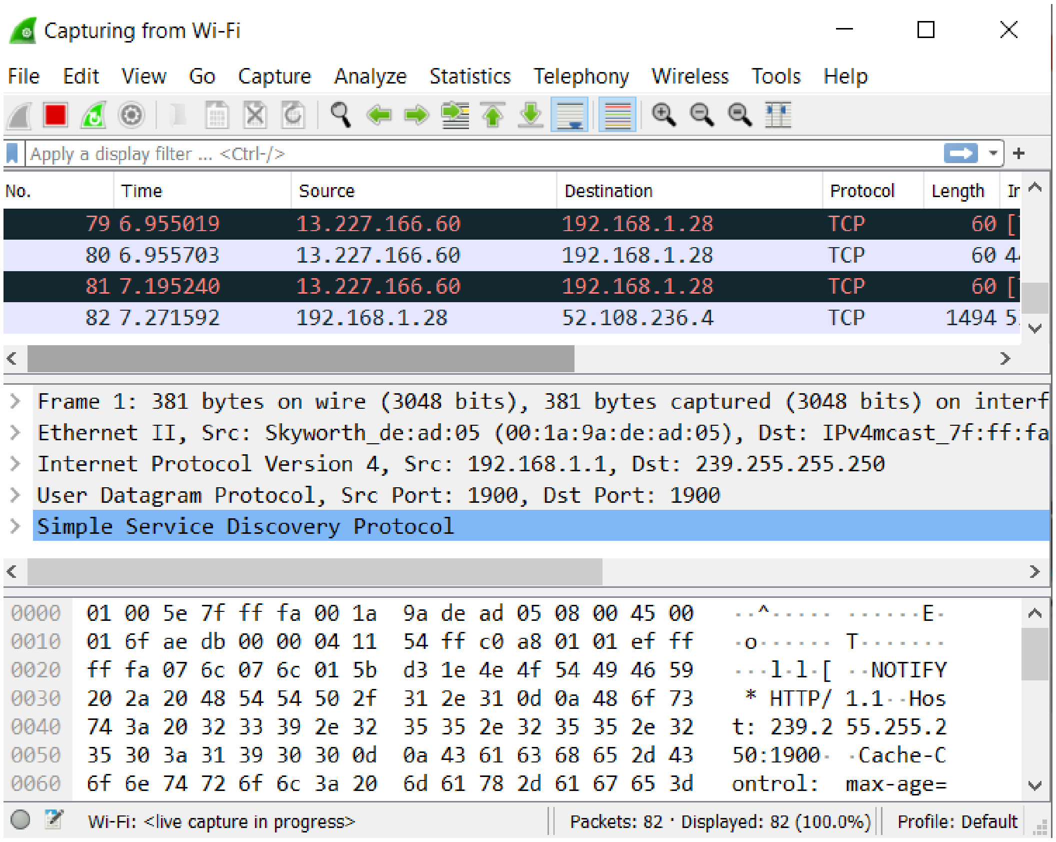
- Local Area Connection* 10
- Local Area Connection* 1
- Wi-Fi
- Local Area Connection* 12
- vEthernet (WSL)
- Local Area Connection* 11
- Local Area Connection* 4
- Adapter for loopback traffic capture

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 3.4.0 (v3.4.0-0-g9733f173ea5e). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

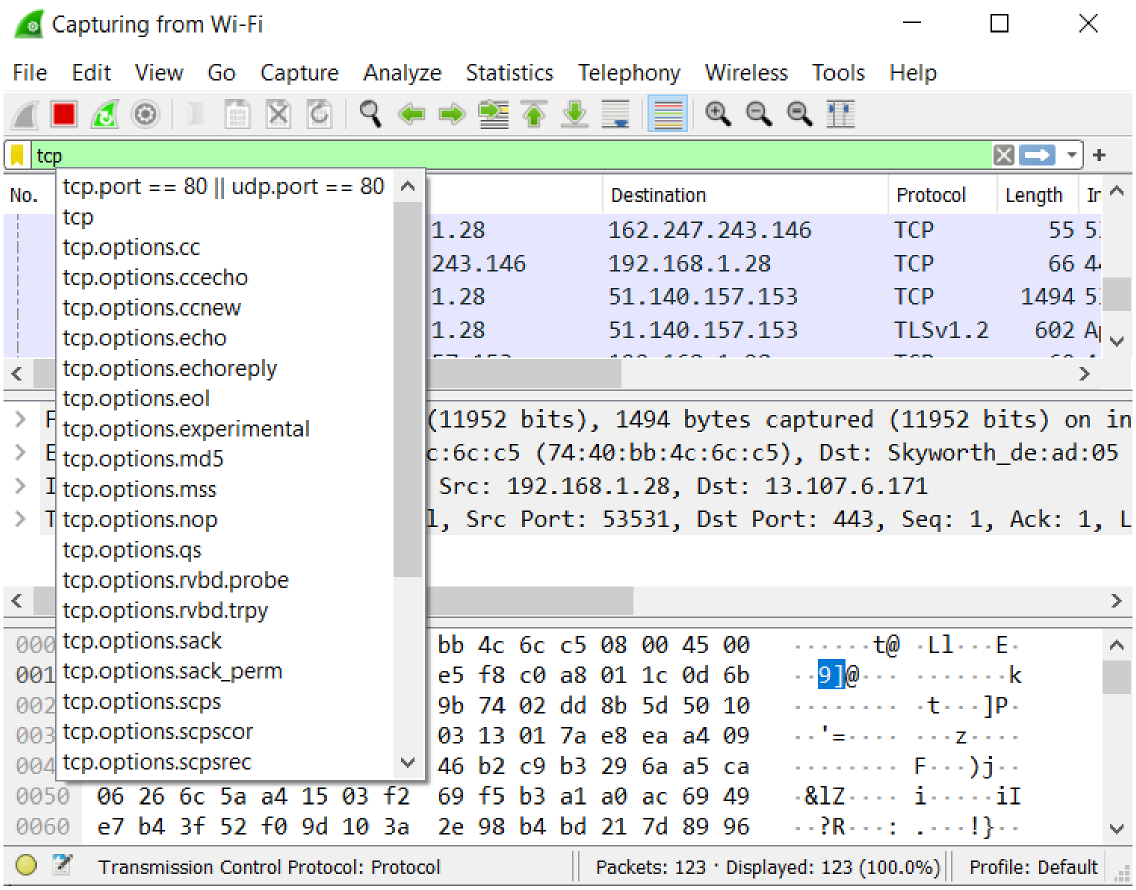

Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Ir
79	6.955019	13.227.166.60	192.168.1.28	TCP	60	[
80	6.955703	13.227.166.60	192.168.1.28	TCP	60	4
81	7.195240	13.227.166.60	192.168.1.28	TCP	60	[
82	7.271592	192.168.1.28	52.108.236.4	TCP	1494	5

```
> Frame 1: 381 bytes on wire (3048 bits), 381 bytes captured (3048 bits) on interf
> Ethernet II, Src: Skyworth_de:ad:05 (00:1a:9a:de:ad:05), Dst: IPv4mcast_7f:ff:fa
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 1900, Dst Port: 1900
> Simple Service Discovery Protocol
```

```
0000  01 00 5e 7f ff fa 00 1a  9a de ad 05 08 00 45 00   ··^····· ······E·
0010  01 6f ae db 00 00 04 11  54 ff c0 a8 01 01 ef ff   ·o······ T·······
0020  ff fa 07 6c 07 6c 01 5b  d3 1e 4e 4f 54 49 46 59   ···l·l·[ ··NOTIFY
0030  20 2a 20 48 54 54 50 2f  31 2e 31 0d 0a 48 6f 73    * HTTP/ 1.1··Hos
0040  74 3a 20 32 33 39 2e 32  35 35 2e 32 35 35 2e 32   t: 239.2 55.255.2
0050  35 30 3a 31 39 30 30 0d  0a 43 61 63 68 65 2d 43   50:1900· ·Cache-C
0060  6f 6e 74 72 6f 6c 3a 20  6d 61 78 2d 61 67 65 3d   ontrol:  max-age=
```

Wi-Fi: <live capture in progress> | Packets: 82 · Displayed: 82 (100.0%) | Profile: Default


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp
```

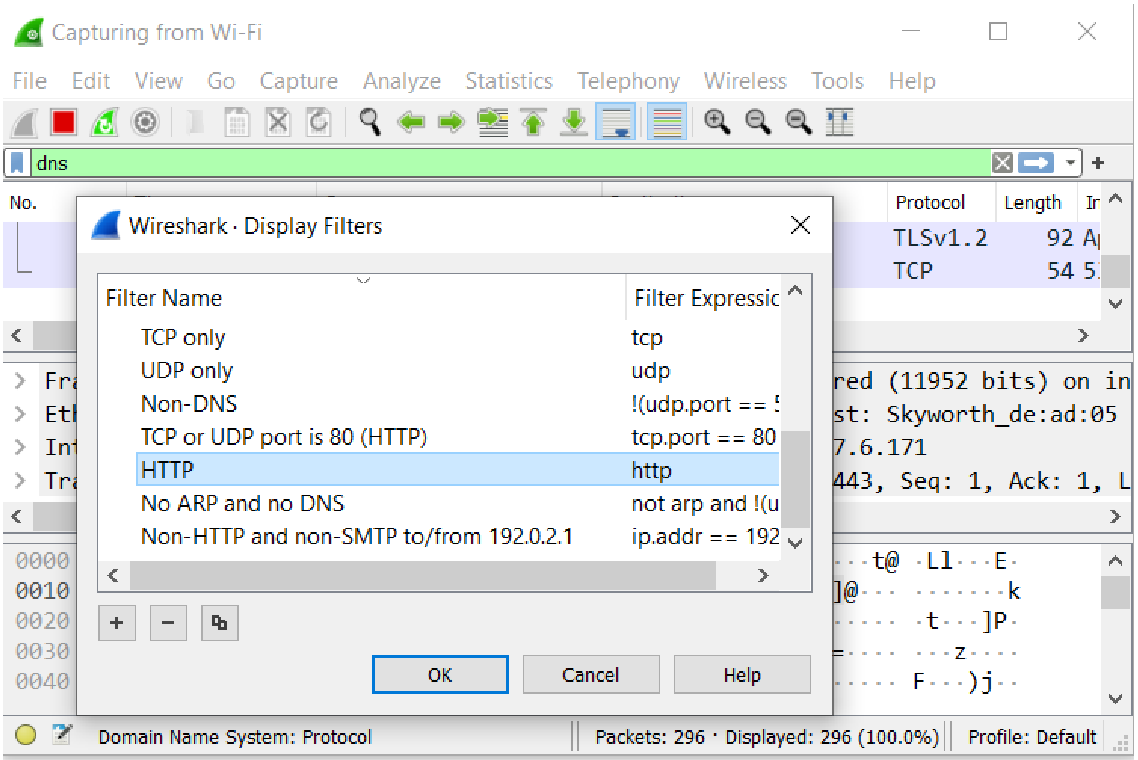
```
tcp.port == 80 || udp.port == 80
tcp
tcp.options.cc
tcp.options.ccecho
tcp.options.ccnew
tcp.options.echo
tcp.options.echoreply
tcp.options.eol
tcp.options.experimental
tcp.options.md5
tcp.options.mss
tcp.options.nop
tcp.options.qs
tcp.options.rvbd.probe
tcp.options.rvbd.trpy
tcp.options.sack
tcp.options.sack_perm
tcp.options.scps
tcp.options.scpscor
tcp.options.scpsrec
```

```
No.    Destination        Protocol  Length  Ir
1.28   162.247.243.146    TCP          55  5
243.146 192.168.1.28      TCP          66  4
1.28   51.140.157.153     TCP        1494  5
1.28   51.140.157.153     TLSv1.2     602  A
```

```
> F (11952 bits), 1494 bytes captured (11952 bits) on in
> E c:6c:c5 (74:40:bb:4c:6c:c5), Dst: Skyworth_de:ad:05
> I  Src: 192.168.1.28, Dst: 13.107.6.171
> T l, Src Port: 53531, Dst Port: 443, Seq: 1, Ack: 1, L
```

```
000   bb 4c 6c c5 08 00 45 00   ······t@ ·Ll···E·
001   e5 f8 c0 a8 01 1c 0d 6b   ··9]@··· ·······k
002   9b 74 02 dd 8b 5d 50 10   ········ ·t···]P·
003   03 13 01 7a e8 ea a4 09   ··'=···· ···z····
004   46 b2 c9 b3 29 6a a5 ca   ········ F···)j··
0050  06 26 6c 5a a4 15 03 f2  69 f5 b3 a1 a0 ac 69 49   ·&lZ···· i·····iI
0060  e7 b4 3f 52 f0 9d 10 3a  2e 98 b4 bd 21 7d 89 96   ··?R···: .···!}··
```

Transmission Control Protocol: Protocol | Packets: 123 · Displayed: 123 (100.0%) | Profile: Default


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Display Filters
+
−
OK
Cancel
Help

```
dns
```

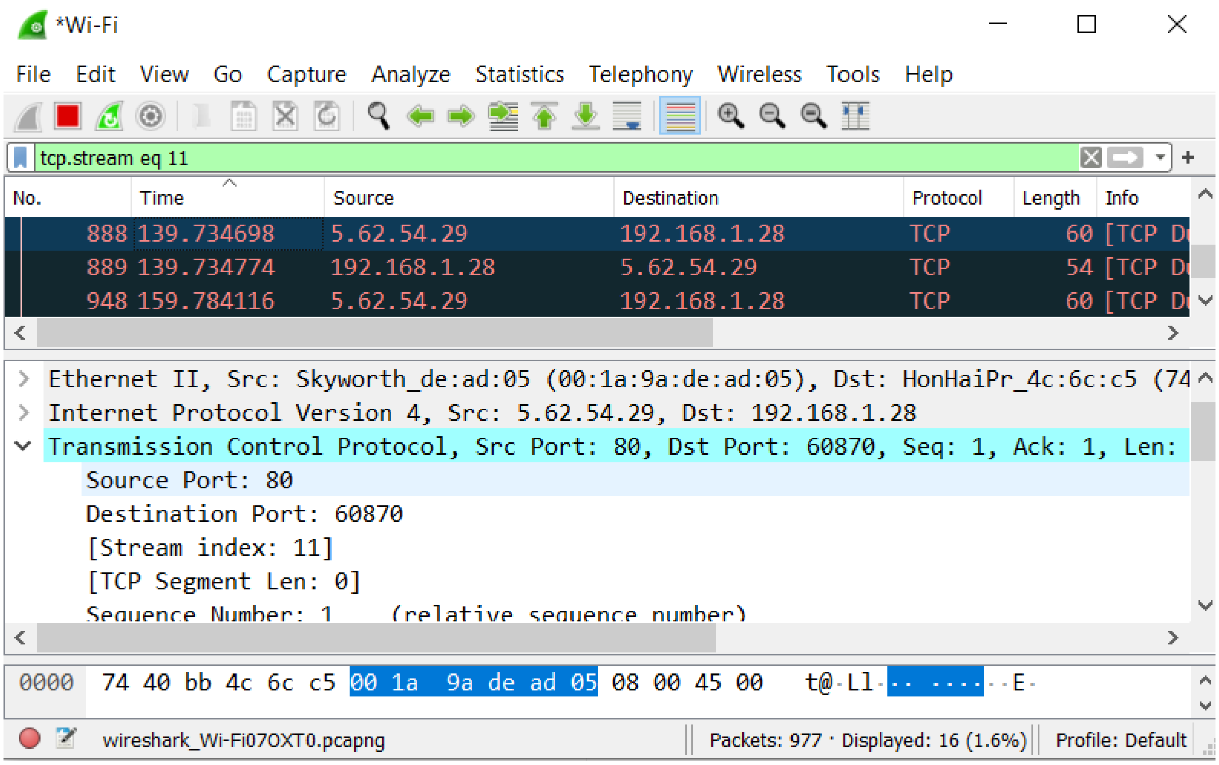
```
No.   Protocol  Length  Ir
      TLSv1.2      92  A
      TCP          54  5
```

Filter Name	Filter Expressic
TCP only	tcp
UDP only	udp
Non-DNS	!(udp.port == 5
TCP or UDP port is 80 (HTTP)	tcp.port == 80
HTTP	http
No ARP and no DNS	not arp and !(u
Non-HTTP and non-SMTP to/from 192.0.2.1	ip.addr == 192

```
> Fra  red (11952 bits) on in
> Etl  st: Skyworth_de:ad:05
> Int  7.6.171
> Tra  443, Seq: 1, Ack: 1, L
```

```
0000  ···t@ ·Ll···E·
0010  ]@··· ·······k
0020  ····· ·t···]P·
0030  =···· ···z····
0040  ····· F···)j··
```

Domain Name System: Protocol | Packets: 296 · Displayed: 296 (100.0%) | Profile: Default


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.stream eq 11
```

```
No.    Time          Source         Destination    Protocol  Length  Info
   888 139.734698    5.62.54.29     192.168.1.28   TCP           60 [TCP D
   889 139.734774    192.168.1.28   5.62.54.29     TCP           54 [TCP D
   948 159.784116    5.62.54.29     192.168.1.28   TCP           60 [TCP D
```

```
> Ethernet II, Src: Skyworth_de:ad:05 (00:1a:9a:de:ad:05), Dst: HonHaiPr_4c:6c:c5 (74
> Internet Protocol Version 4, Src: 5.62.54.29, Dst: 192.168.1.28
v Transmission Control Protocol, Src Port: 80, Dst Port: 60870, Seq: 1, Ack: 1, Len:
     Source Port: 80
     Destination Port: 60870
     [Stream index: 11]
     [TCP Segment Len: 0]
     Sequence Number: 1    (relative sequence number)
```

```
0000  74 40 bb 4c 6c c5 00 1a  9a de ad 05 08 00 45 00   t@·Ll·········E·
```

wireshark_Wi-Fi07OXT0.pcapng
Packets: 977 · Displayed: 16 (1.6%)
Profile: Default

Post labs:

1. **A user is unable to ping a system on the network. How can Wireshark be used to solve the problem.**

Ans:
Ping uses ICMP. Wireshark can be used to check if ICMP packets are being sent out from the system. If it is sent out, it can also be checked if the packets are being received.

2. **Filter all source, destination and ignore ICMP**

Ans:
tcpdump dst net and src net and not icmp