

Q1: The SSIDs of the two access points that are issuing most of the beacon Frames are

1. SSID="30 Munroe St"
2. SSID="linksys_SES_24086"

Q2: Time interval between the transmissions of the beacon frames of linksys_ses_24086 access point : Beacon Interval: 0.102400 [Seconds]

```
802.11 183 Beacon frame, SN=3503, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
802.11 90 Beacon frame, SN=3486, FN=0, Flags=.....C, BI=100, SSID="linksys12"
802.11 132 Beacon frame, SN=3640, FN=0, Flags=.....C, BI=100, SSID="linksys_SES_24086"
802.11 183 Beacon frame, SN=3504, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
802.11 183 Beacon frame, SN=3505, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
802.11 183 Beacon frame, SN=3506, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
802.11 54 QoS Null function (No data), SN=1566, FN=0, Flags=.....TC
(RA) 802.11 38 Acknowledgement, Flags=.....C
802.11 177 Probe Response, SN=3507, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
:1d:51... 802.11 38 Acknowledgement, Flags=.....C
802.11 177 Probe Response, SN=3507, FN=0, Flags=...R...C, BI=100, SSID="30 Munroe St"
:1d:51... 802.11 38 Acknowledgement, Flags=.....C
802.11 54 QoS Null function (No data), SN=1567, FN=0, Flags=...P...TC
802.11 177 Unknown protocol version: 3
```

Frame check sequence: 0x7c0930f2 [unverified]	
[FCS Status: Unverified]	
[WLAN Flags:C]	
IEEE 802.11 Wireless Management	
Fixed parameters (12 bytes)	
Timestamp: 6351964057993	
Beacon Interval: 0.102400 [Seconds]	
Capabilities Information: 0x0011	
Tagged parameters (68 bytes)	
Tag: SSID parameter set: "linksys_SES_24086"	
Tag: Supported Rates 1(R) 2(R) 5 5(R) 11(R) [Mbit/sec]	

Header revision	Header pad
Flags	Data rate (Mb/s)
Channel flags	
Signal Quality	

For 30 Munroe St. access point: Beacon Interval: 0.102400 [Seconds]

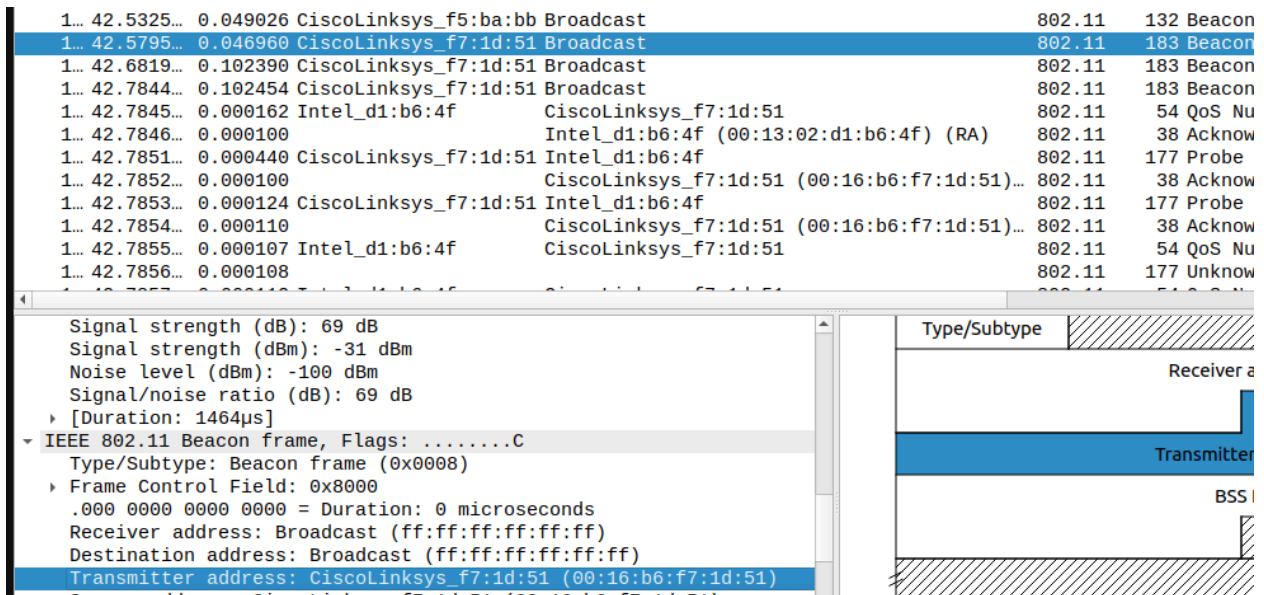
```
802.11 183 Beacon frame, SN=3503, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
802.11 90 Beacon frame, SN=3486, FN=0, Flags=.....C, BI=100, SSID="linksys12"
802.11 132 Beacon frame, SN=3640, FN=0, Flags=.....C, BI=100, SSID="linksys_SES_24086"
802.11 183 Beacon frame, SN=3504, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
802.11 183 Beacon frame, SN=3505, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
802.11 183 Beacon frame, SN=3506, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
802.11 54 QoS Null function (No data), SN=1566, FN=0, Flags=.....TC
(RA) 802.11 38 Acknowledgement, Flags=.....C
802.11 177 Probe Response, SN=3507, FN=0, Flags=.....C, BI=100, SSID="30 Munroe St"
:1d:51... 802.11 38 Acknowledgement, Flags=.....C
802.11 177 Probe Response, SN=3507, FN=0, Flags=...R...C, BI=100, SSID="30 Munroe St"
:1d:51... 802.11 38 Acknowledgement, Flags=.....C
802.11 54 QoS Null function (No data), SN=1567, FN=0, Flags=...P...TC
802.11 177 Unknown protocol version: 3
```

Frame check sequence: 0xa028b529 [unverified]	
[FCS Status: Unverified]	
[WLAN Flags:C]	
IEEE 802.11 Wireless Management	
Fixed parameters (12 bytes)	
Timestamp: 174361600386	
Beacon Interval: 0.102400 [Seconds]	
Capabilities Information: 0x0601	
Tagged parameters (119 bytes)	
Tag: SSID parameter set: "30 Munroe St"	
Tag: Supported Rates 1(R) 2(R) 5 5(R) 11(R) [Mbit/sec]	

Header revision	Header pad
Flags	Data rate (Mb/s)
Channel flags	
Signal Quality	

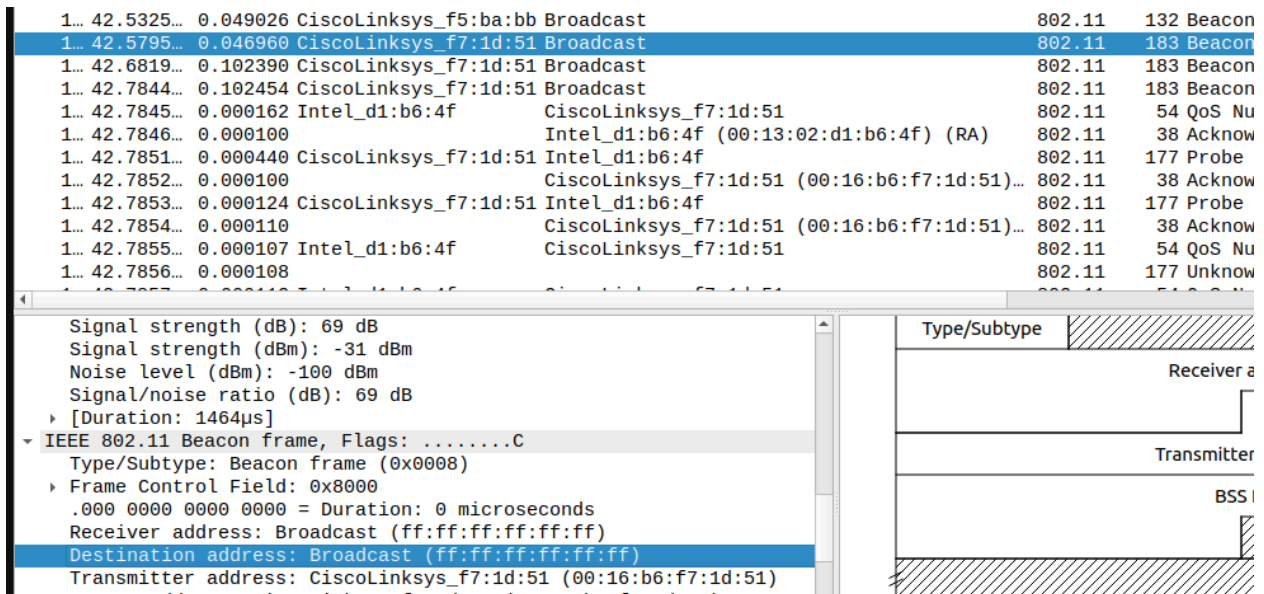
Q3:

The source mac address is 00:16:b6:f7:1d:51



Q4:

Destination address is broadcast address : ff:ff:ff:ff:ff:ff



Q5:

The MAC BSS id is 00:16:b6:f7:1d:51

The image shows a Wireshark packet capture of an IEEE 802.11 Beacon frame. The packet list on the left shows a beacon frame at 42.5795 seconds. The packet details pane on the right shows the frame structure, including the Receiver address, Transmitter address, and BSS Id (00:16:b6:f7:1d:51). The packet structure diagram on the right shows the frame layout with fields like Type/Subtype, Duration, Receiver address, Transmitter address, BSS Id, and Fragment number.

Signal/noise ratio (dB): 69 dB
[Duration: 1464µs]
IEEE 802.11 Beacon frame, Flags:C
Type/Subtype: Beacon frame (0x0008)
Frame Control Field: 0x8000
.....0000 0000 0000 = Duration: 0 microseconds
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
Source address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
.....0000 = Fragment number: 0
1101 1011 0000 = Sequence number: 3504

Type/Subtype: Duration:
Receiver address:
Transmitter address:
BSS Id:
Fragment number:
Sequence number:

Q6:

Tag: Supported Rates are 1, 2, 5.5 and 11 Mbit/sec and Extended Supported Rates 6, 9, 12, 18, 24, 36, 48, 54 Mbit/sec

The image shows a Wireshark packet capture of an IEEE 802.11 Wireless Management frame. The packet list on the left shows a management frame at 42.5795 seconds. The packet details pane on the right shows the frame structure, including the Tag: Supported Rates (1, 2, 5.5, 11) and Tag: Extended Supported Rates (6, 9, 12, 18, 24, 36, 48, 54). The packet structure diagram on the right shows the frame layout with fields like Tag: Supported Rates, Tag: Extended Supported Rates, and Tag: ERP Information.

Tag: SSID parameter set: "30 Munroe St"
Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
Tag Number: Supported Rates (1)
Tag length: 4
Supported Rates: 1(B) (0x82)
Supported Rates: 2(B) (0x84)
Supported Rates: 5.5(B) (0x8b)
Supported Rates: 11(B) (0x96)
Tag: DS Parameter set: Current Channel: 6
Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
Tag: Country Information: Country Code US, Environment Indoor
Tag: EDCA Parameter Set
Tag: ERP Information
Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54
Tag Number: Extended Supported Rates (50)

Tag: Supported Rates:
Tag: Extended Supported Rates:
Tag: ERP Information:
Tag: Extended Supported Rates:

Q7:

Sender MAC address (Host) :00:13:02:d1:b6:4f

Destination address is: 00:16:b6:f4:eb:a8

BSS address 00:16:b6:f7:1d:51

4/3 24.8895... 0.000188 CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)... 802.11 38 Acknowledgement, Flags=.....C

474 24.8110... 0.001580 192.168.1.109 128.119.245.12 TCP 110 2538 → 80 [SYN] Seq=0 Win=16384

475 24.8112... 0.000138 Intel_d1:b6:4f (00:13:02:d1:b6:4f) (RA) 802.11 38 Acknowledgement, Flags=.....C

476 24.8277... 0.016520 128.119.245.12 192.168.1.109 TCP 110 80 → 2538 [SYN, ACK] Seq=0 Ack=1

477 24.8279... 0.000171 CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)... 802.11 38 Acknowledgement, Flags=.....C

478 24.8280... 0.000102 192.168.1.109 128.119.245.12 TCP 102 2538 → 80 [ACK] Seq=1 Ack=1 Win=

479 24.8281... 0.000116 Intel_d1:b6:4f (00:13:02:d1:b6:4f) (RA) 802.11 38 Acknowledgement, Flags=.....C

480 24.8282... 0.000113 192.168.1.109 128.119.245.12 HTTP 537 GET /wireshark-labs/alice.txt HT

481 24.8283... 0.000099 Intel_d1:b6:4f (00:13:02:d1:b6:4f) (RA) 802.11 38 Acknowledgement, Flags=.....C

482 24.8468... 0.018546 128.119.245.12 192.168.1.109 TCP 108 80 → 2538 [ACK] Seq=1 Ack=436 Wi

483 24.8470... 0.000160 CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)... 802.11 38 Acknowledgement, Flags=.....C

Noise level (dBm): -100 dBm
Signal/noise ratio (dB): 62 dB
[Duration: 36µs]
IEEE 802.11 QoS Data, Flags:TC
Type/Subtype: QoS Data (0x0028)
Frame Control Field: 0x8801
.000 0000 0010 1100 = Duration: 44 microseconds
Receiver address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
Destination address: CiscoLinksys_f4:eb:a8 (00:16:b6:f4:eb:a8)
Source address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
STA address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
..... 0000 = Fragment number: 0
0000 0011 0001 = Sequence number: 49

Receiver address
Transmitter address
Destination address
Fragment...
Frame check sequence

The source ip address is 192.168.1.109, which corresponds to the host's ip address

Destination ip address is 128.119.245.12 which corresponds to the destination address(gaia.cs.umass.edu)

4/3 24.8895... 0.000188 CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)... 802.11 38 Acknowledgement, Flags=.....C

474 24.8110... 0.001580 192.168.1.109 128.119.245.12 TCP 110 2538 → 80 [SYN] Seq=0 Win=16384

475 24.8112... 0.000138 Intel_d1:b6:4f (00:13:02:d1:b6:4f) (RA) 802.11 38 Acknowledgement, Flags=.....C

476 24.8277... 0.016520 128.119.245.12 192.168.1.109 TCP 110 80 → 2538 [SYN, ACK] Seq=0 Ack=1

477 24.8279... 0.000171 CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)... 802.11 38 Acknowledgement, Flags=.....C

478 24.8280... 0.000102 192.168.1.109 128.119.245.12 TCP 102 2538 → 80 [ACK] Seq=1 Ack=1 Win=

479 24.8281... 0.000116 Intel_d1:b6:4f (00:13:02:d1:b6:4f) (RA) 802.11 38 Acknowledgement, Flags=.....C

480 24.8282... 0.000113 192.168.1.109 128.119.245.12 HTTP 537 GET /wireshark-labs/alice.txt HT

481 24.8283... 0.000099 Intel_d1:b6:4f (00:13:02:d1:b6:4f) (RA) 802.11 38 Acknowledgement, Flags=.....C

482 24.8468... 0.018546 128.119.245.12 192.168.1.109 TCP 108 80 → 2538 [ACK] Seq=1 Ack=436 Wi

483 24.8470... 0.000160 CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)... 802.11 38 Acknowledgement, Flags=.....C

Internet Protocol Version 4, Src: 192.168.1.109, Dst: 128.119.245.12

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 48
Identification: 0x1324 (4900)
010. = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0xb00a [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.109
Destination Address: 128.119.245.12
Transmission Control Protocol Src Port: 2538 Dst Port: 80 Seq: 0

Version Header ... Differentiated Servic... Total Length
Identification Flags Fragment Offset
Time to Live Protocol Header Checksum
Source Address
Destination Address
Transmission Control Protocol
Source Port Destination Port

Q8:

Access point MAC address is Receiver address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)

BSS address: 00:16:b6:f7:1d:51

Destination address: 91:2a:b0:49:b6:4f

Source address and first hop router address: 00:16:b6:f4:eb:a8

The image shows a Wireshark packet capture of an IEEE 802.11 QoS Data frame. The packet list on the left shows a frame at 474.24.8110.0001580 from 192.168.1.109 to 128.119.245.12. The packet details on the right show the frame structure: Type/Subtype (0x0028), Duration (0x0028), Receiver address (91:2a:b0:49:b6:4f), Transmitter address (00:16:b6:f7:1d:51), Destination address (91:2a:b0:49:b6:4f), Source address (00:16:b6:f4:eb:a8), BSS Id (00:16:b6:f7:1d:51), STA address (91:2a:b0:49:b6:4f), and Frame number (0).

Q9:

Ans: At t=49.583615 we can see a DHCP release message

At t= 49.609617 we can see a deauthentication message

The image shows a Wireshark packet capture of two frames: a DHCP Release message and a Deauthentication message. The packet list on the left shows a frame at 1733.49.583615.0041134 from 192.168.1.109 to 192.168.1.1, and a frame at 1735.49.609617.0025846 from 128.119.245.12 to 128.119.245.12. The packet details on the right show the frame structure: Type/Subtype (0x000c), Duration (0x000c), Receiver address (00:16:b6:f7:1d:51), Destination address (00:16:b6:f7:1d:51), Source address (00:16:b6:f4:eb:a8), BSS Id (00:16:b6:f7:1d:51), STA address (00:16:b6:f4:eb:a8), and Frame number (0).

We cannot see any disassociation request sent.

Ans: Total 6 AUTHENTICATION messages are sent from the host to the linksys_ses_24086 AP

Q11:
Ans The host want authentication to be open

Diagram illustrating the structure of an IEEE 802.11 Wireless Management frame. The frame is divided into several fields:

- Transmitter address (6 bytes)
- BSS Id (2 bytes)
- Fragmentation offset (2 bytes, labeled "Fragmente...")
- Frame check sequence (4 bytes)

The frame body is shaded, indicating variable length. Below the frame, a timeline shows the fixed parameters (6 bytes) and the variable length of the frame body, with bit positions 0, 15, 16, and 31 marked.

Q12:

Ans

No, we can't see an authentication message from linksys_ses_24086 AP

Wlan.ta == 00:18:39:f5:ba:bb

No.	Time	Delta	Source	Destination	Protocol	Length	Info
1499	42.532596	0.000000	CiscoLinksys_f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3640, FN=...
1513	42.839707	0.307111	CiscoLinksys_f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3643, FN=...
1527	43.658960	0.819253	CiscoLinksys_f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3651, FN=...
1557	44.887707	1.228747	CiscoLinksys_f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3663, FN=...
1994	59.325865	14.438...	CiscoLinksys_f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3833, FN=...
2290	69.463202	10.137...	CiscoLinksys_f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3938, FN=...
2296	69.667955	0.204753	CiscoLinksys_f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3940, FN=...
2321	71.101576	1.433621	CiscoLinksys_f5:ba:bb	Broadcast	802.11	132	Beacon frame, SN=3954, FN=...

Frame 1557: 132 bytes on wire (1056 bits), 132 bytes captured (1056) on interface wlan0

Radiotap Header v0, Length 24

802.11 radio information

IEEE 802.11 Beacon frame, Flags:C

Type/Subtype: Beacon frame (0x0008)

Frame Control Field: 0x8000

Duration: 0 microseconds

Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)

Destination address: Broadcast (ff:ff:ff:ff:ff:ff)

Transmitter address: CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb)

Source address: CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb)

BSS Id: c0:74:39:95:ec:15 (c0:74:39:95:ec:15)

Fragment number: 13

Sequence number: 3663

Frame check sequence: 0xe1bbe5b3 [unverified]

Frame Status: Unverified

IEEE 802.11 Wireless Management

Fixed parameters (12 bytes)

Tagged parameters (72 bytes)

Q13:

At t = 63.168087 host sends an authentication request to bss

Ans at t = 63.169071 bss sends an authentication request to host

Apply a display filter ... <Ctrl-/>

No.	Time	Delta	Source	Destination	Protocol	Length	Info
2149	63.094985	0.004014	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	54	Deauthentication, SN=1646
2150	63.116231	0.021246	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	54	Deauthentication, SN=1646
2151	63.135362	0.019131	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	54	Deauthentication, SN=1646
2152	63.140106	0.004744	Intel_d1:b6:4f	Broadcast	802.11	94	Probe Request, SN=1647, F...
2153	63.142451	0.002345	CiscoLinksys_f7:1d:51	Intel_d1:b6:4f	802.11	177	Probe Response, SN=3724, F...
2154	63.142860	0.000409	CiscoLinksys_f7:1d:51	(00:16:b6:f7:1d:51) (RA)	802.11	38	Acknowledgement, Flags=...
2155	63.161272	0.018412	CiscoLinksys_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3725, FN...
2156	63.168087	0.006815	Intel_d1:b6:4f	CiscoLinksys_f7:1d:51	802.11	58	Authentication, SN=1647, F...
2157	63.168222	0.000135	Intel_d1:b6:4f	(00:13:02:d1:b6:4f) (RA)	802.11	38	Acknowledgement, Flags=...
2158	63.169071	0.000849	CiscoLinksys_f7:1d:51	Intel_d1:b6:4f	802.11	58	Authentication, SN=3726, F...
2159	63.169592	0.000521	CiscoLinksys_f7:1d:51	(00:16:b6:f7:1d:51) (RA)	802.11	38	Acknowledgement, Flags=...
2160	63.169707	0.000115	Intel_d1:b6:4f	CiscoLinksys_f7:1d:51	802.11	58	Authentication, SN=1647, F...
2161	63.169814	0.000107	Intel_d1:b6:4f	(00:13:02:d1:b6:4f) (RA)	802.11	38	Acknowledgement, Flags=...
2162	63.169910	0.000096	Intel_d1:b6:4f	CiscoLinksys_f7:1d:51	802.11	89	Association Request, SN=1...

Q14:

Ans

At t=63.169910 ASSOCIATE REQUEST was sent from host to the 30 Munroe St AP and at t= 63.192101 the corresponding ASSOCIATE REPLY was sent

No.	Time	Delta	Source	Destination	Protocol	Length	Info
2155	63.161272	0.018412	CiscoLinksys_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3725, FN=...
2156	63.168087	0.006815	Intel_d1:b6:4f	CiscoLinksys_f7:1d:51	802.11	58	Authentication, SN=1647, Flags=...
2157	63.168222	0.000135	Intel_d1:b6:4f	Intel_d1:b6:4f (00:13:02:d1:b6:4f) (RA)	802.11	38	Acknowledgement, Flags=...
2158	63.169071	0.000849	CiscoLinksys_f7:1d:51	Intel_d1:b6:4f	802.11	58	Authentication, SN=3726, Flags=...
2159	63.169592	0.000521	CiscoLinksys_f7:1d:51	CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51) (RA)	802.11	38	Acknowledgement, Flags=...
2160	63.169707	0.000115	Intel_d1:b6:4f	CiscoLinksys_f7:1d:51	802.11	58	Authentication, SN=1647, Flags=...
2161	63.169814	0.000107	Intel_d1:b6:4f	Intel_d1:b6:4f (00:13:02:d1:b6:4f) (RA)	802.11	38	Acknowledgement, Flags=...
2162	63.169910	0.000096	Intel_d1:b6:4f	CiscoLinksys_f7:1d:51	802.11	89	Association Request, SN=1648, Flags=...
2163	63.170008	0.000098	Intel_d1:b6:4f	Intel_d1:b6:4f (00:13:02:d1:b6:4f) (RA)	802.11	38	Acknowledgement, Flags=...
2164	63.170692	0.000684	CiscoLinksys_f7:1d:51	Intel_d1:b6:4f	802.11	58	Authentication, SN=3727, Flags=...
2165	63.171000	0.000308	CiscoLinksys_f7:1d:51	CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51) (RA)	802.11	38	Acknowledgement, Flags=...
2166	63.192101	0.021101	CiscoLinksys_f7:1d:51	Intel_d1:b6:4f	802.11	94	Association Response, SN=1649, Flags=...
2167	63.192956	0.000855	CiscoLinksys_f7:1d:51	CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51) (RA)	802.11	38	Acknowledgement, Flags=...
2168	63.194842	0.001886	0.0.0.0	255.255.255.255	DHCP	390	DHCP Discover - Transaction ID=...

Q15:

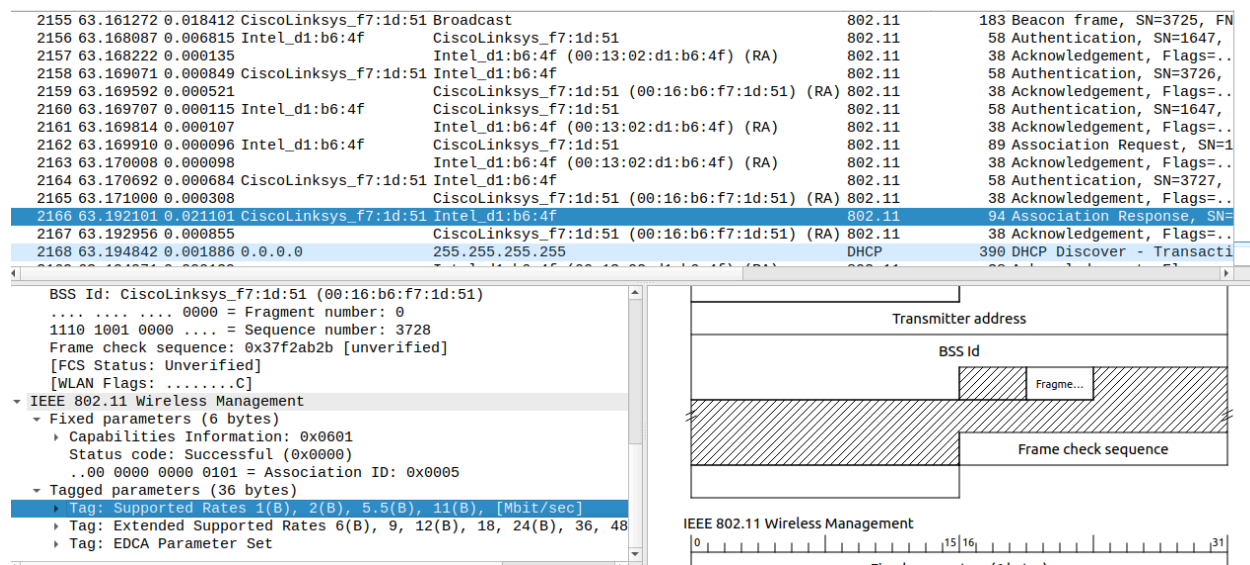
Ans: In association request we can see that the host is willing to sent at 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec] and same at association response.

2155	63.161272	0.018412	CiscoLinksys_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3725, FN=...
2156	63.168087	0.006815	Intel_d1:b6:4f	CiscoLinksys_f7:1d:51	802.11	58	Authentication, SN=1647, Flags=...
2157	63.168222	0.000135	Intel_d1:b6:4f	Intel_d1:b6:4f (00:13:02:d1:b6:4f) (RA)	802.11	38	Acknowledgement, Flags=...
2158	63.169071	0.000849	CiscoLinksys_f7:1d:51	Intel_d1:b6:4f	802.11	58	Authentication, SN=3726, Flags=...
2159	63.169592	0.000521	CiscoLinksys_f7:1d:51	CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51) (RA)	802.11	38	Acknowledgement, Flags=...
2160	63.169707	0.000115	Intel_d1:b6:4f	CiscoLinksys_f7:1d:51	802.11	58	Authentication, SN=1647, Flags=...
2161	63.169814	0.000107	Intel_d1:b6:4f	Intel_d1:b6:4f (00:13:02:d1:b6:4f) (RA)	802.11	38	Acknowledgement, Flags=...
2162	63.169910	0.000096	Intel_d1:b6:4f	CiscoLinksys_f7:1d:51	802.11	89	Association Request, SN=1648, Flags=...
2163	63.170008	0.000098	Intel_d1:b6:4f	Intel_d1:b6:4f (00:13:02:d1:b6:4f) (RA)	802.11	38	Acknowledgement, Flags=...
2164	63.170692	0.000684	CiscoLinksys_f7:1d:51	Intel_d1:b6:4f	802.11	58	Authentication, SN=3727, Flags=...
2165	63.171000	0.000308	CiscoLinksys_f7:1d:51	CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51) (RA)	802.11	38	Acknowledgement, Flags=...
2166	63.192101	0.021101	CiscoLinksys_f7:1d:51	Intel_d1:b6:4f	802.11	94	Association Response, SN=1649, Flags=...
2167	63.192956	0.000855	CiscoLinksys_f7:1d:51	CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51) (RA)	802.11	38	Acknowledgement, Flags=...
2168	63.194842	0.001886	0.0.0.0	255.255.255.255	DHCP	390	DHCP Discover - Transaction ID=...

BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)	
....	Fragment number: 0
0110 0111 0000	Sequence number: 1648
Frame check sequence: 0xfe3badc6 [unverified]	
[FCS Status: Unverified]	
[WLAN Flags:C]	
IEEE 802.11 Wireless Management	
Fixed parameters (4 bytes)	
Capabilities Information: 0xce01	
Listen Interval: 0x000a	
Tagged parameters (33 bytes)	
Tag: SSID parameter set: "30 Munroe St"	
Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]	
Tag: QoS Capability	
Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]	

IEEE 802.11 Wireless Management

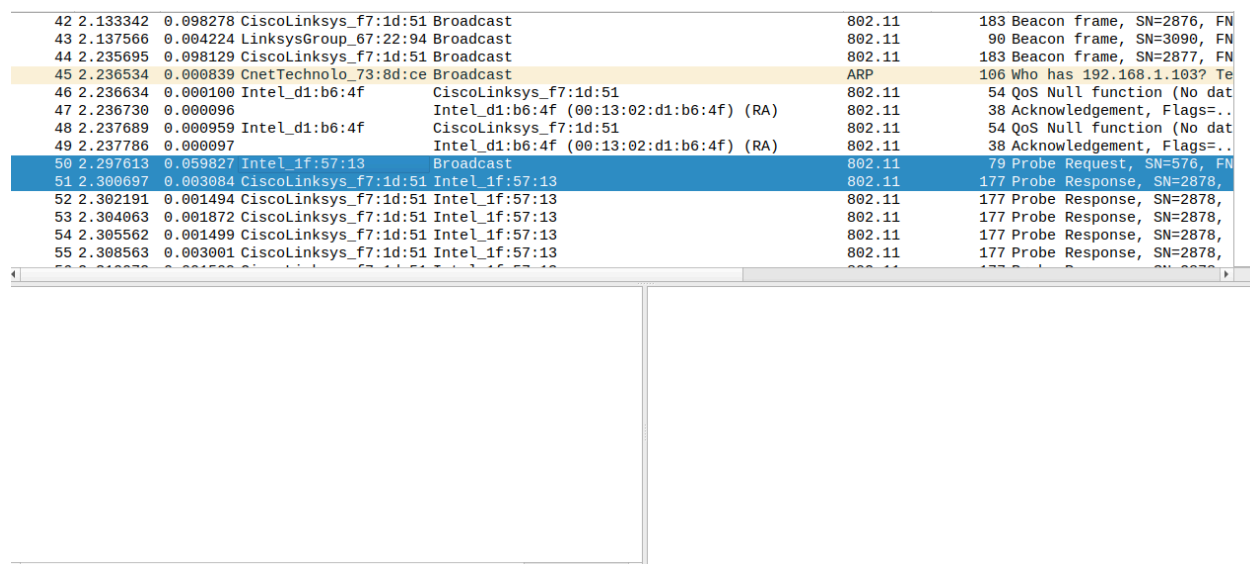
Fixed parameters (4 bytes)



Q16:

The very first probe request is sent at t=2.297613 its senders mac address is 00:12:f0:1f:57:13, destination mac address is ff:ff:ff:ff:ff:ff and bss id is ff:ff:ff:ff:ff:ff.

The probe response received at t=2.300697, senders mac address is 00:16:b6:f7:1d:51, destination mac address is 00:12:f0:1f:57:13 and bss id is 00:16:b6:f7:1d:51,



In active scanning, host send probe request to find an AP and in response AP responds with Probe Response.

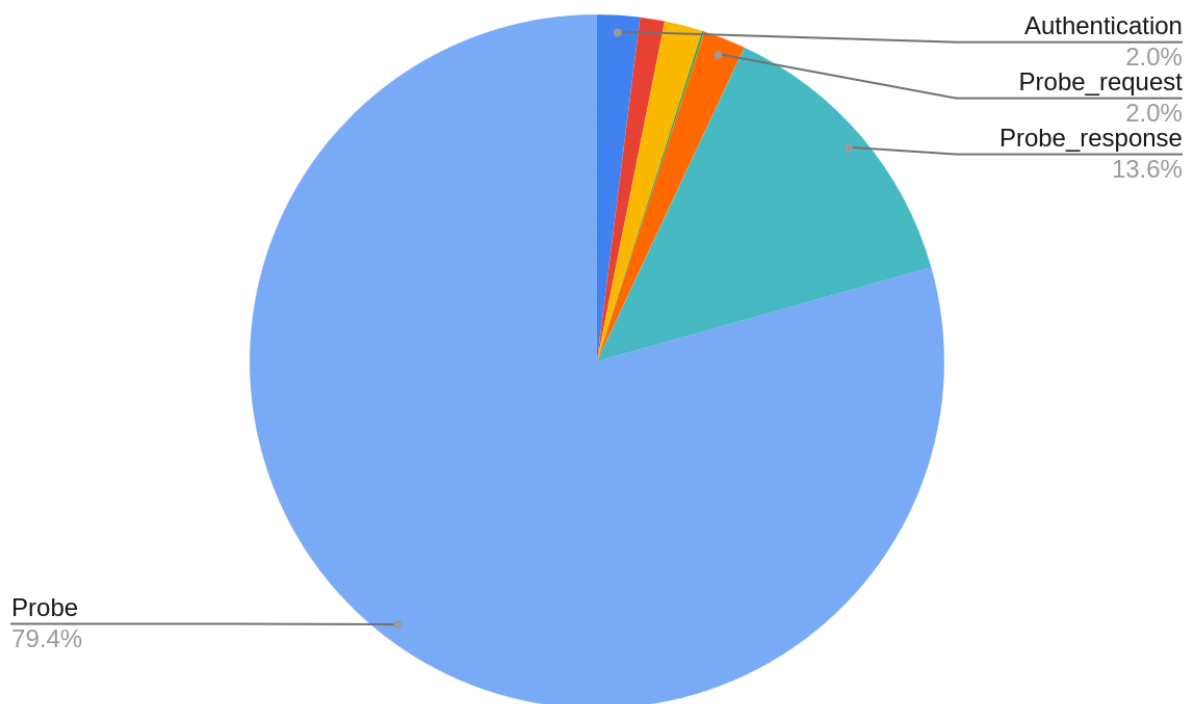
Q1a: Trace 1

Use statscollector.sh file to get MAC Management, Control, Data Traffic.
Run below commands to get the result

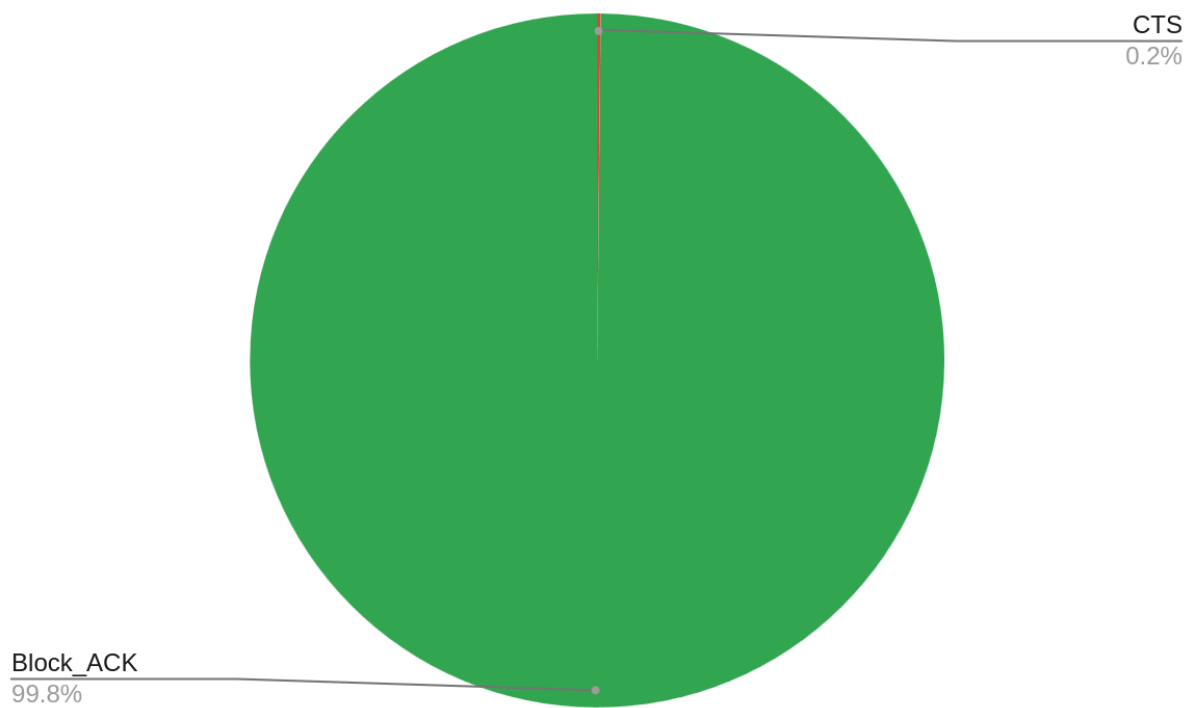
```
chmod +x statscollector.sh  
./statscollector.sh Wireshark_802_11.pcap
```

Output will 3 files which gives the stats

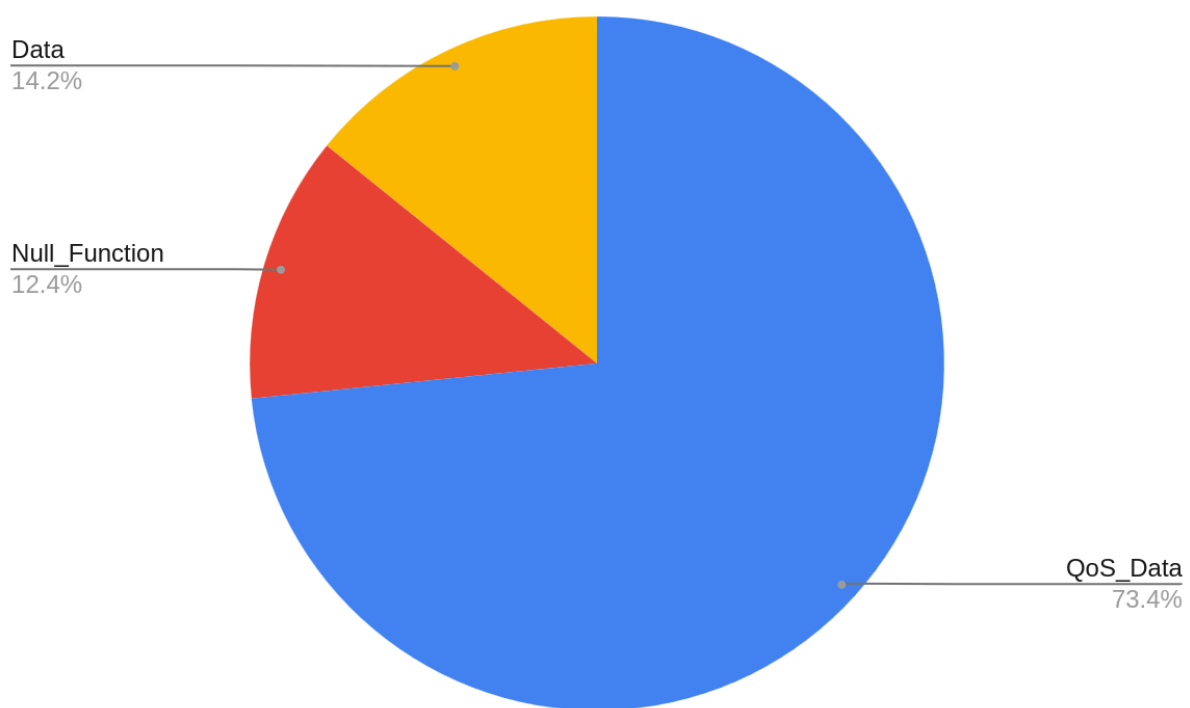
```
abhi@laptop:~$ ./statscollector.sh /home/abhi/Downloads/wireshark-traces/Wireshark_802_11.pcap  
abhi@laptop:~$ cat management.txt  
Authentication 19  
Deauthentication 11  
Association_request 17  
Association_response 1  
Probe_request 19  
Probe_response 131  
Probe 762  
abhi@laptop:~$ cat controls.txt  
RTS 0  
CTS 1  
ACK 0  
Block_ACK 614  
abhi@laptop:~$ cat datas.txt  
QoS_Data 455  
Null_Function 77  
Data 88  
abhi@laptop:~$
```



MAC Management frames



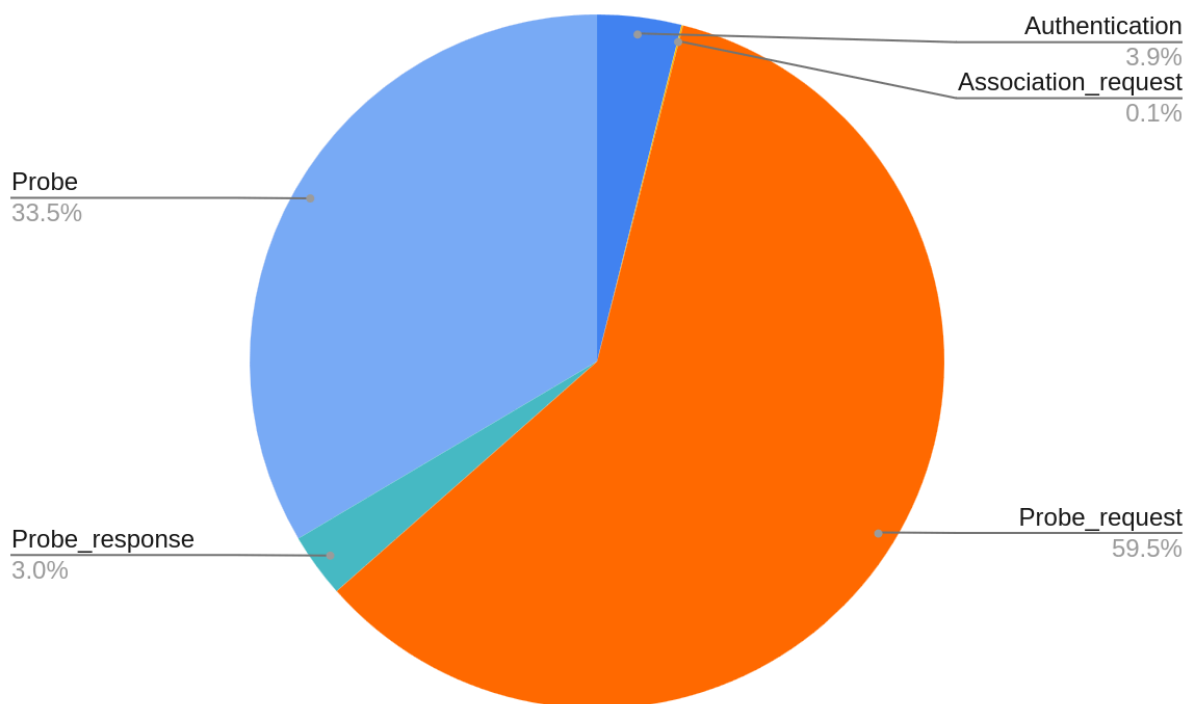
Control Frames



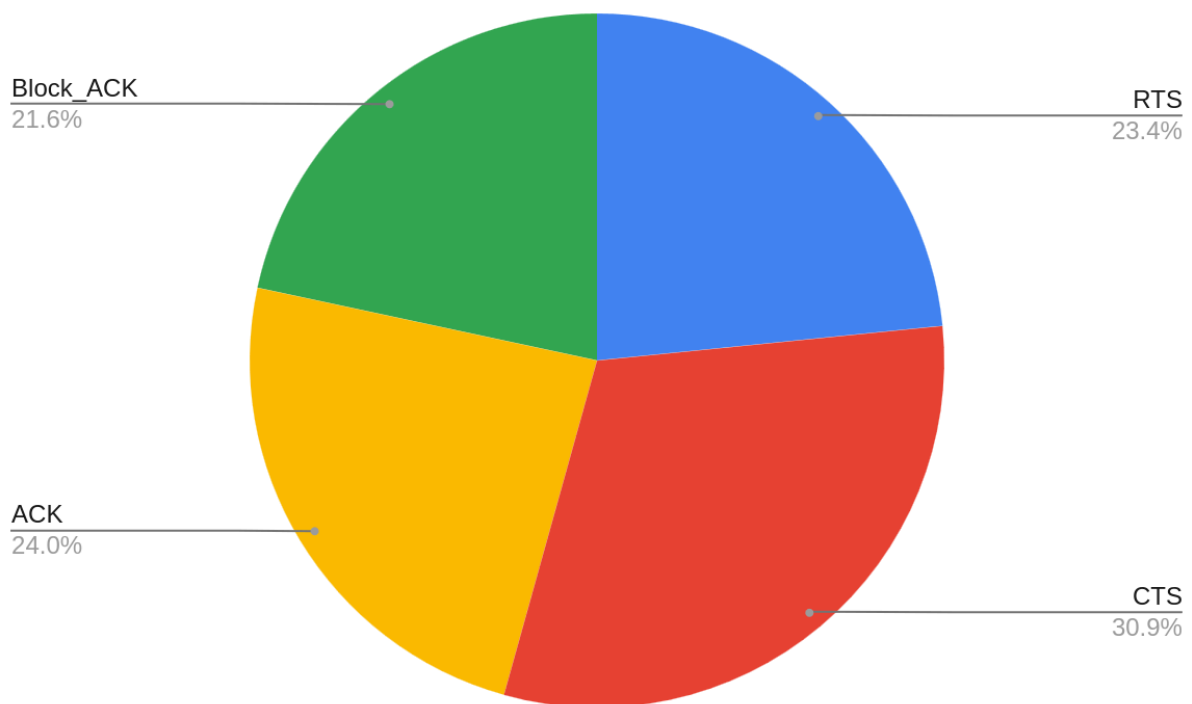
Data frame

Trace 2

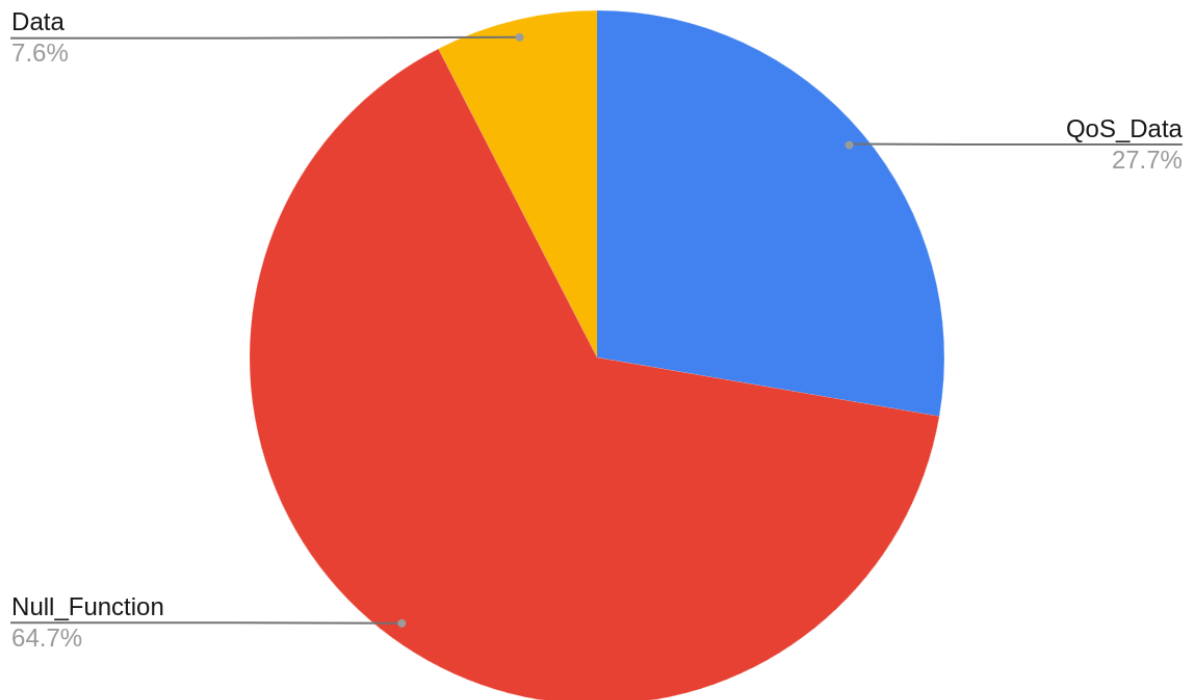
```
abhi@laptop:~$ ./statscollector.sh /home/abhi/Downloads/wireshark-traces/cs23mtech11021_802_11.pcap
abhi@laptop:~$ cat management.txt
Authentication 55
Deauthentication 0
Association_request 1
Association_response 0
Probe_request 836
Probe_response 42
Probe 471
abhi@laptop:~$ cat controls.txt
RTS 1469
CTS 1940
ACK 1509
Block_ACK 1358
abhi@laptop:~$ cat datas.txt
QoS_Data 378
Null_Function 883
Data 103
abhi@laptop:~$
```



MAC Management frames



Control Frames



Data frames

Q1b1

Ans: No. of different APs visible in trace 1 is 9

No. of different APs visible in trace 2 is 5

Protocol	Length	Info
802.11	355	Beacon frame, SN=1329, FN=0, Flags=.....C, BI=100, SSID="IITH"
802.11	357	Beacon frame, SN=3286, FN=0, Flags=.....C, BI=100, SSID="eduroam"
802.11	364	Beacon frame, SN=2398, FN=0, Flags=.....C, BI=100, SSID="Placement-2023"
802.11	364	Beacon frame, SN=2419, FN=0, Flags=.....C, BI=100, SSID="Placement-2023"
802.11	406	Beacon frame, SN=3928, FN=0, Flags=.....C, BI=100, SSID="IITH-Guest-PWD-IITH@20"
802.11	355	Beacon frame, SN=1804, FN=0, Flags=.....C, BI=100, SSID="IITH"
802.11	406	Beacon frame, SN=3958, FN=0, Flags=.....C, BI=100, SSID="IITH-Guest-PWD-IITH@20"
802.11	355	Beacon frame, SN=1834, FN=0, Flags=.....C, BI=100, SSID="IITH"
802.11	364	Beacon frame, SN=2469, FN=0, Flags=.....C, BI=100, SSID="Placement-2023"
802.11	364	Beacon frame, SN=2695, FN=0, Flags=.....C, BI=100, SSID="Placement-2023"
802.11	345	Beacon frame, SN=2608, FN=0, Flags=.....C, BI=100, SSID="A004_Lab"
802.11	355	Beacon frame, SN=2066, FN=0, Flags=.....C, BI=100, SSID="IITH"
802.11	364	Beacon frame, SN=2701, FN=0, Flags=.....C, BI=100, SSID="Placement-2023"
802.11	406	Beacon frame, SN=353, FN=0, Flags=.....C, BI=100, SSID="IITH-Guest-PWD-IITH@20"

Q1b2

Ans: There is only 1 CTS frame in trace 1 which is of size 38B and there is no RTS frame

Filter: wlan.fc.type_subtype == 0x001c

No.	Time	Source	Destination	Protocol	Length
1...	46.595317		LinksysGroup_67:22:94 (00:06:25:67:22:94) (RA)	802.11	

Frame 1601: 38 bytes on wire (304 bits), 38 bytes captured (304 bits) on interface 0

Encapsulation type: IEEE 802.11 plus radiotap radio header (23)

Arrival Time: Jun 29, 2007 07:35:53.667774000 IST

UTC Arrival Time: Jun 29, 2007 02:05:53.667774000 UTC

Epoch Arrival Time: 1183082753.667774000

[Time shift for this packet: 0.000000000 seconds]

[Time delta from previous captured frame: 0.002851000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 46.595317000 seconds]

Frame Number: 1601

Frame Length: 38 bytes (304 bits)

Capture Length: 38 bytes (304 bits)

[Frame is marked: False]

IEEE 802.11 Radiotap Cap

0	
Header revision	
Flags	Da
Channel fla	
Signal Qual	

Minimum size of MAC frame for which CTS is 70B and RTS is 76B

Filter: wlan.fc.type_subtype == 0x001c

No.	Time	Delta	Source	Destination
1...	662.691...	0.002441		MojoNetworks_81:be:21 (30:b6:...
1...	662.695...	0.003717		MojoNetworks_81:be:21 (30:b6:...
1...	662.696...	0.001079		MojoNetworks_81:be:21 (30:b6:...
1...	663.305...	0.608798		MojoNetworks_81:be:20 (30:b6:...
1...	663.615...	0.310659		MojoNetworks_81:be:20 (30:b6:...
1...	663.616...	0.000183		MojoNetworks_81:be:21 (30:b6:...
1...	664.240...	0.624007		MojoNetworks_81:be:20 (30:b6:...
1...	664.335...	0.094922		MojoNetworks_81:be:20 (30:b6:...
1...	664.346...	0.011135		MojoNetworks_81:be:20 (30:b6:...
1...	664.452...	0.106357		MojoNetworks_81:be:20 (30:b6:...
1...	664.454...	0.002099		MojoNetworks_81:be:20 (30:b6:...
1...	664.537...	0.083262		MojoNetworks_81:be:20 (30:b6:...
1...	664.542...	0.004607		MojoNetworks_81:be:20 (30:b6:...
1...	664.543...	0.001052		MojoNetworks_81:be:20 (30:b6:...

Frame 10179: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0

Radiotap Header v0, Length 56

802.11 radio information

IEEE 802.11 Clear-to-send, Flags:C

Type/Subtype: Clear-to-send (0x001c)

Frame Control Field: 0xc400

.000 0000 1001 1110 = Duration: 158 microseconds

Receiver address: MojoNetworks_81:be:20 (30:b6:2d:81:be:20)

Frame check sequence: 0xc0ae3fdd [unverified]

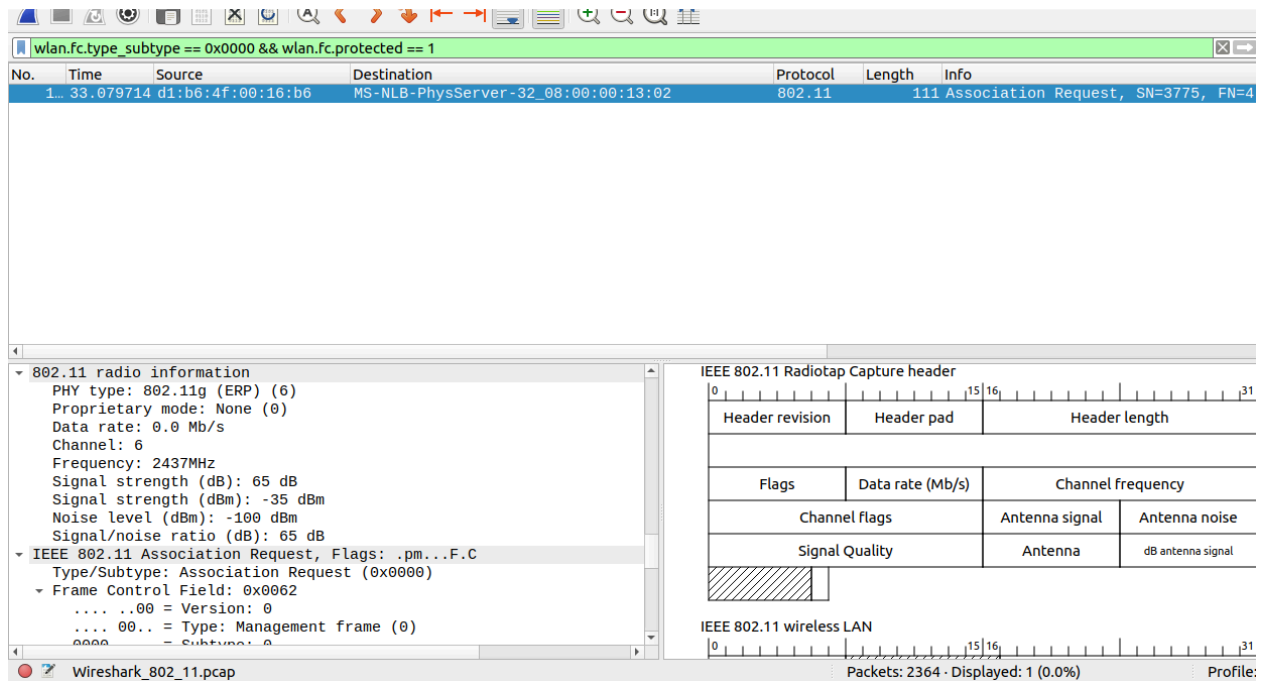
[FCS Status: Unverified]

[WLAN Flags:C]

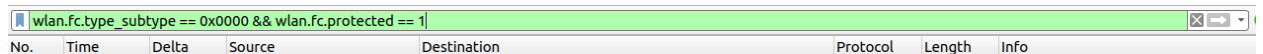
wlan.fc.type_subtype == 0x001b				
No.	Time	Delta	Source	Destination
1...	663.034...	0.327946	CloudNetwork_a6:a3:...	MojoNetworks_81:be:21 (30:b6:
1...	663.242...	0.207875	9a:ba:84:27:91:82 (...)	MojoNetworks_81:be:20 (30:b6:
1...	663.280...	0.038038	9a:ba:84:27:91:82 (...)	MojoNetworks_81:be:20 (30:b6:
1...	663.283...	0.003598	9a:ba:84:27:91:82 (...)	MojoNetworks_81:be:20 (30:b6:
1...	663.305...	0.021661	9a:ba:84:27:91:82 (...)	MojoNetworks_81:be:20 (30:b6:
1...	663.317...	0.012018	CloudNetwork_a6:a3:...	MojoNetworks_81:be:21 (30:b6:
1...	663.511...	0.194345	b6:29:e3:21:6d:b0 (...)	DLinkInterna_cf:af:74 (6c:72:
1...	663.751...	0.240169	9a:ba:84:27:91:82 (...)	MojoNetworks_81:be:20 (30:b6:
1...	663.756...	0.005038	9a:ba:84:27:91:82 (...)	MojoNetworks_81:be:20 (30:b6:
1...	663.759...	0.002764	9a:ba:84:27:91:82 (...)	MojoNetworks_81:be:20 (30:b6:
1...	664.265...	0.506149	9a:ba:84:27:91:82 (...)	MojoNetworks_81:be:20 (30:b6:
1...	664.346...	0.080231	MojoNetworks_81:be:...	9a:ba:84:27:91:82 (9a:ba:84:2
1...	664.613...	0.266902	9a:ba:84:27:91:82 (...)	MojoNetworks_81:be:20 (30:b6:
1...	664.643...	0.030196	9a:ba:84:27:91:82 (...)	MojoNetworks_81:be:20 (30:b6:
1...	664.754...	0.130100	9a:ba:84:27:91:82 (...)	MojoNetworks_81:be:20 (30:b6:
▶ Frame 10180: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) ▶ Radiotap Header v0, Length 56 ▶ 802.11 radio information ▼ IEEE 802.11 Request-to-send, Flags:C Type/Subtype: Request-to-send (0x001b) ▶ Frame Control Field: 0xb400 .000 0000 1101 0100 = Duration: 212 microseconds Receiver address: 9a:ba:84:27:91:82 (9a:ba:84:27:91:82) Transmitter address: MojoNetworks_81:be:20 (30:b6:2d:81:be:20) Frame check sequence: 0x8ed01ecd [unverified] [FCS Status: Unverified] [WLAN Flags:C]				

Q1b3

Ans: 1 out of 2364 MAC frames is encrypted in trace 1



There were no encrypted frame in trace 2



Q1c

Ans:

1. Avg packet size vs Time

Trace1 :

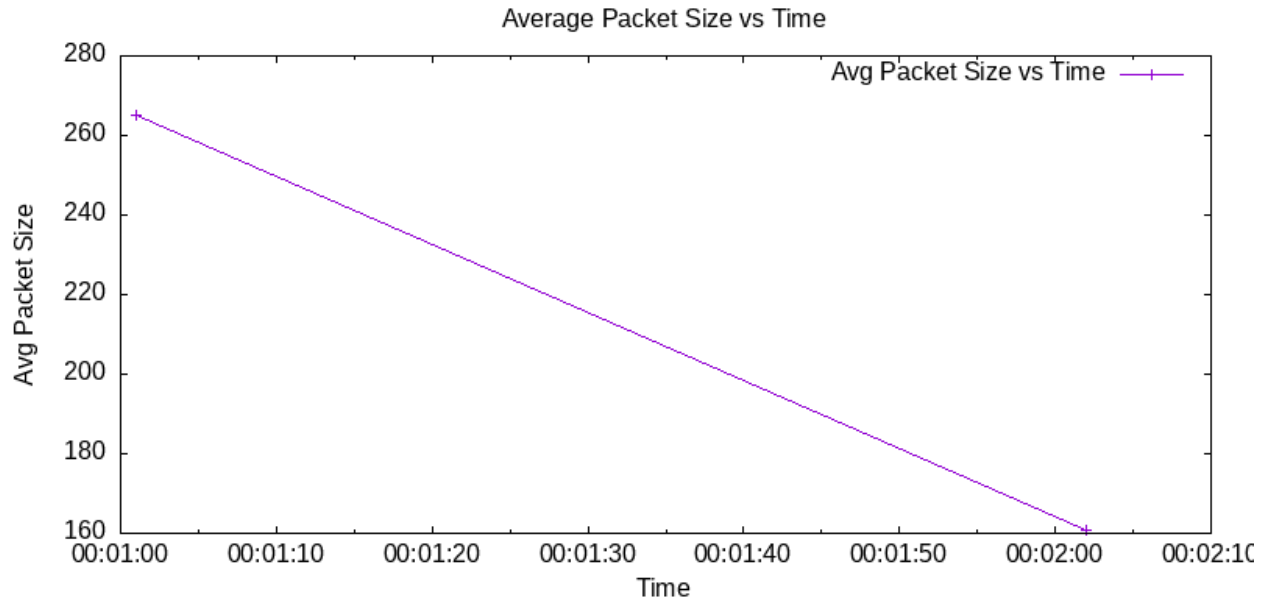
Command:

abhi@laptop:~\$ chmod +x packet_size_time.sh

abhi@laptop:~\$./packet_size_time.sh

/home/abhi/Downloads/wireshark-traces/Wireshark_802_11.pcap

Successfull!



Average packet size has decreased over time

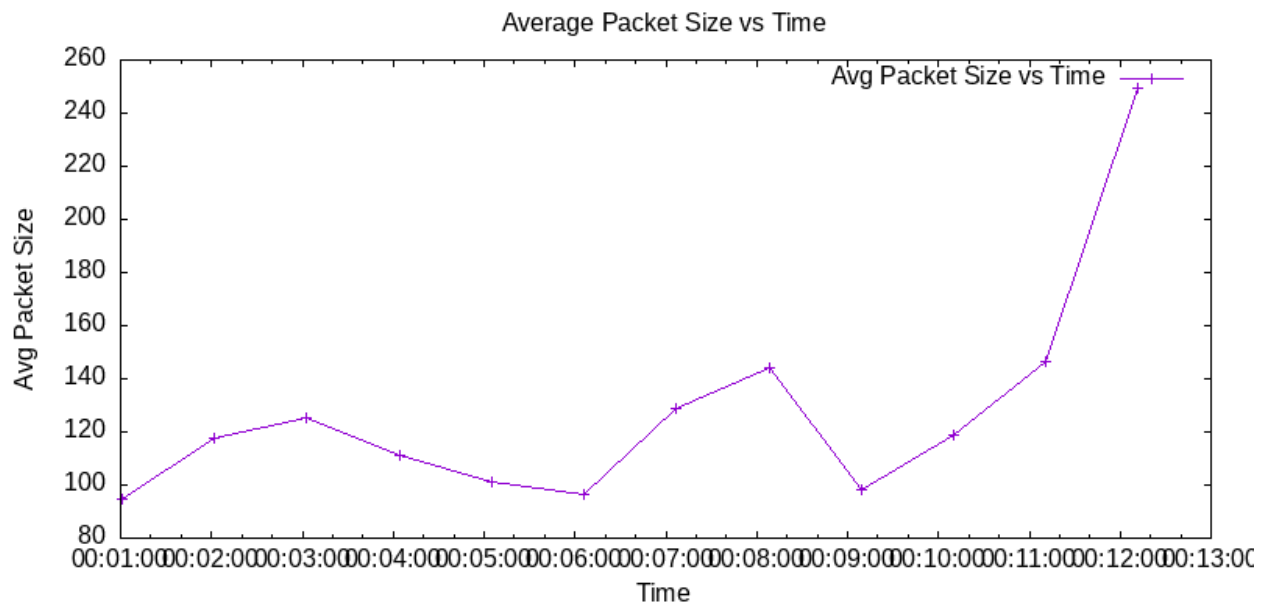
Trace2:

```
abhi@laptop:~$ ./packet_size_time.sh
```

```
/home/abhi/Downloads/wireshark-traces/cs23mtech11021_802_11.pcap
```

```
Successfull!
```

```
abhi@laptop:~$
```

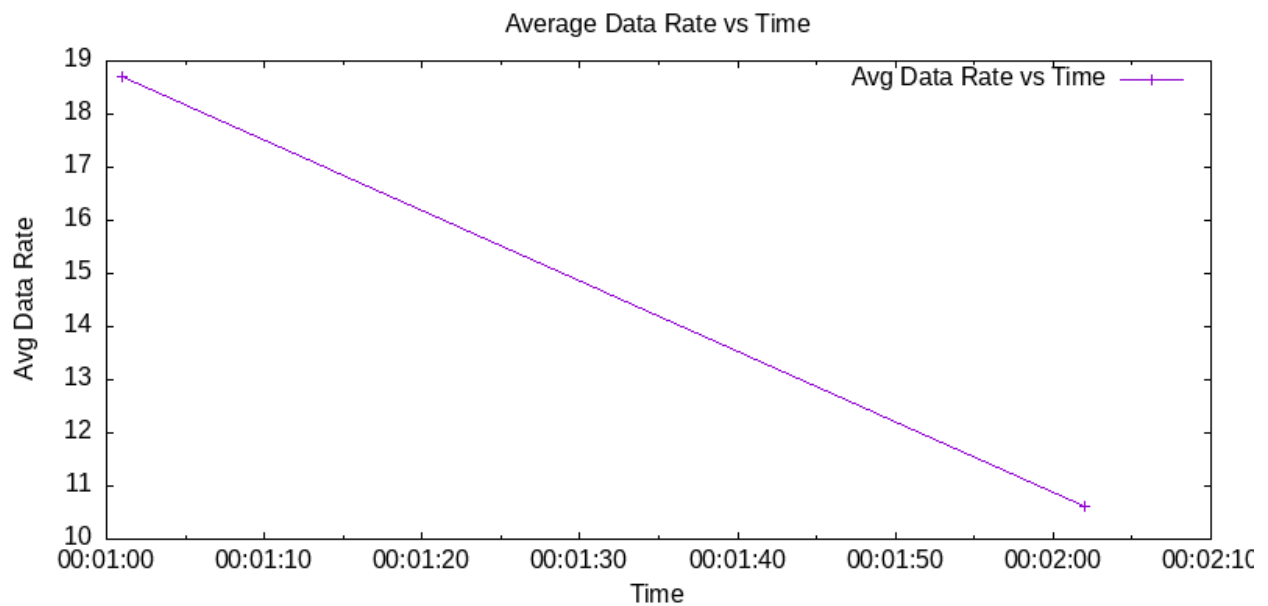


We can see that average packet size was almost same till 10min.

2.Avg PHY datarate vs time

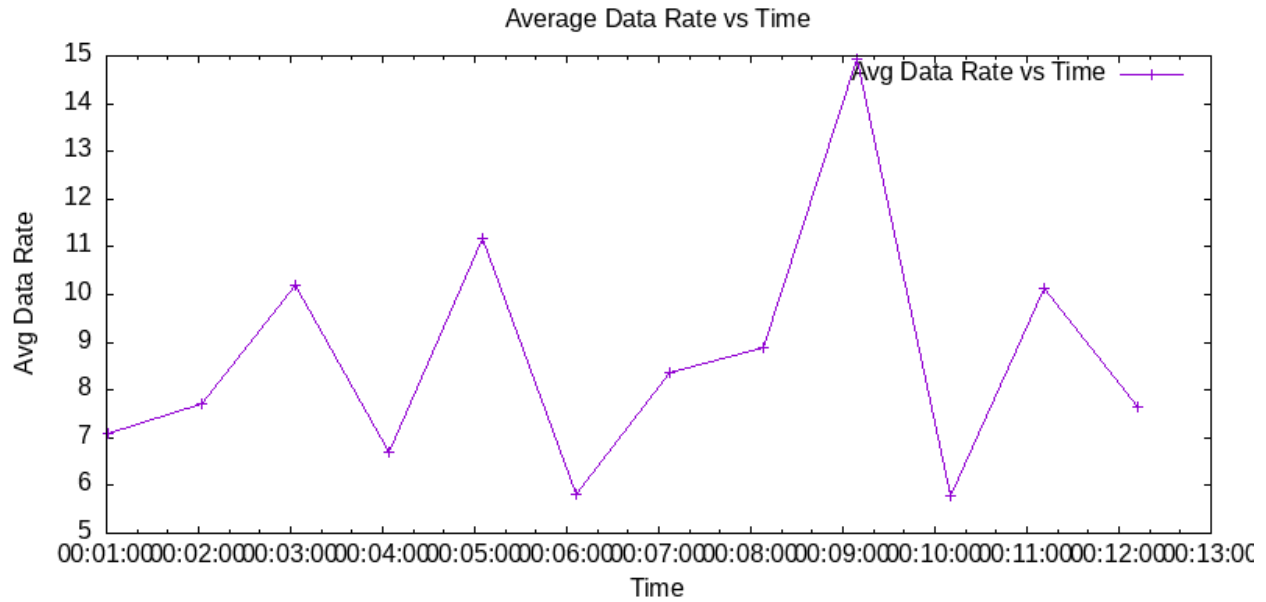
Command:

```
abhi@laptop:~$ ./avg_data_rate_time.sh  
/home/abhi/Downloads/wireshark-traces/Wireshark_802_11.pcap  
Successfull!  
abhi@laptop:~$
```



Trace 2:

```
abhi@laptop:~$ ./avg_data_rate_time.sh  
/home/abhi/Downloads/wireshark-traces/cs23mtech11021_802_11.pcap  
Successfull!  
abhi@laptop:~$
```



We can see that the average data remain almost same

3.RSSI vs time

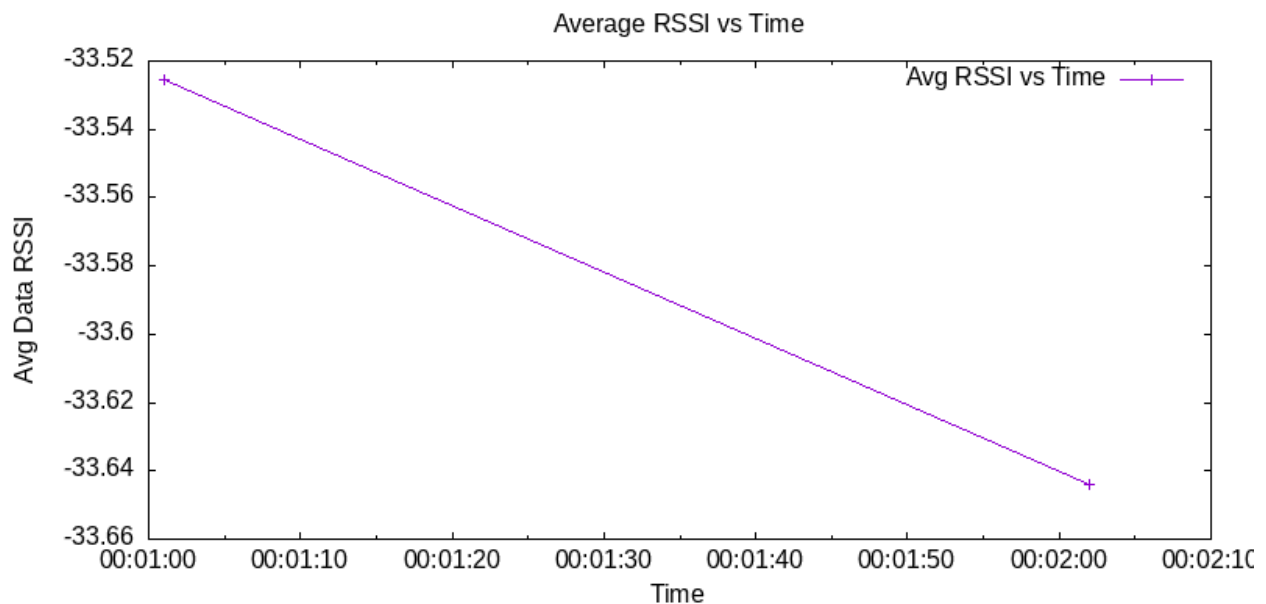
Command:

```
abhi@laptop:~$ ./avg_rssi_time.sh
```

```
/home/abhi/Downloads/wireshark-traces/Wireshark_802_11.pcap
```

Successfull!

```
abhi@laptop:~$
```



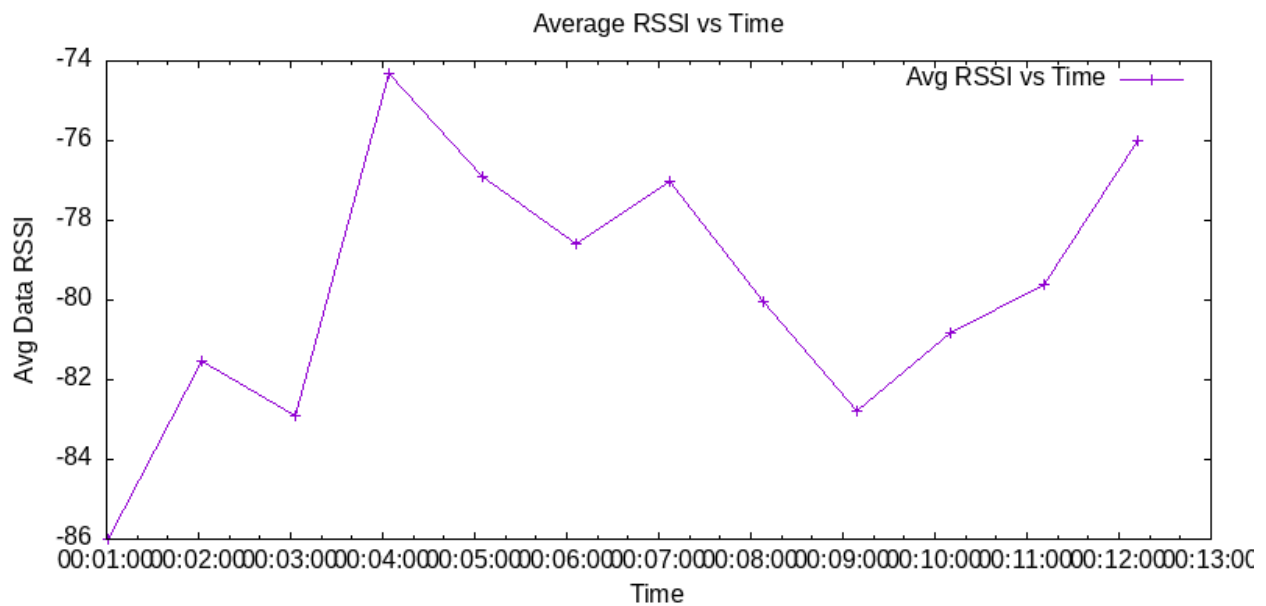
Trace 2:

```
abhi@laptop:~$ ./avg_rssi_time.sh
```

```
/home/abhi/Downloads/wireshark-traces/cs23mtech11021_802_11.pcap
```

Successfull!

```
abhi@laptop:~$
```



4:

Plot Packet rate (pkts/sec) vs Time

Command:

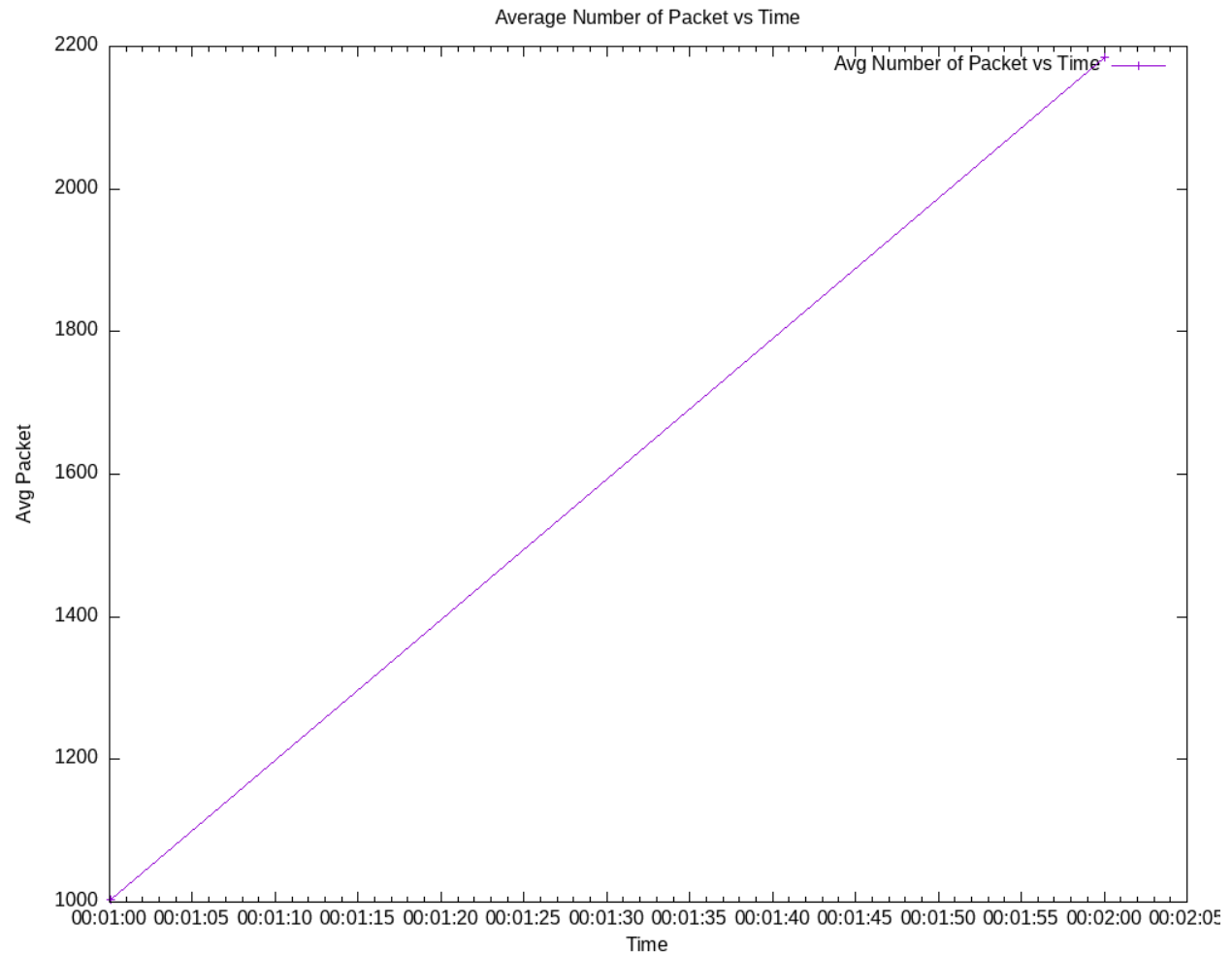
```
abhi@laptop:~$ chmod +x avg_packet_rate_time.sh
```

```
abhi@laptop:~$ ./avg_packet_rate_time.sh
```

```
/home/abhi/Downloads/wireshark-traces/Wireshark_802_11.pcap
```

Successful!

```
abhi@laptop:~$
```



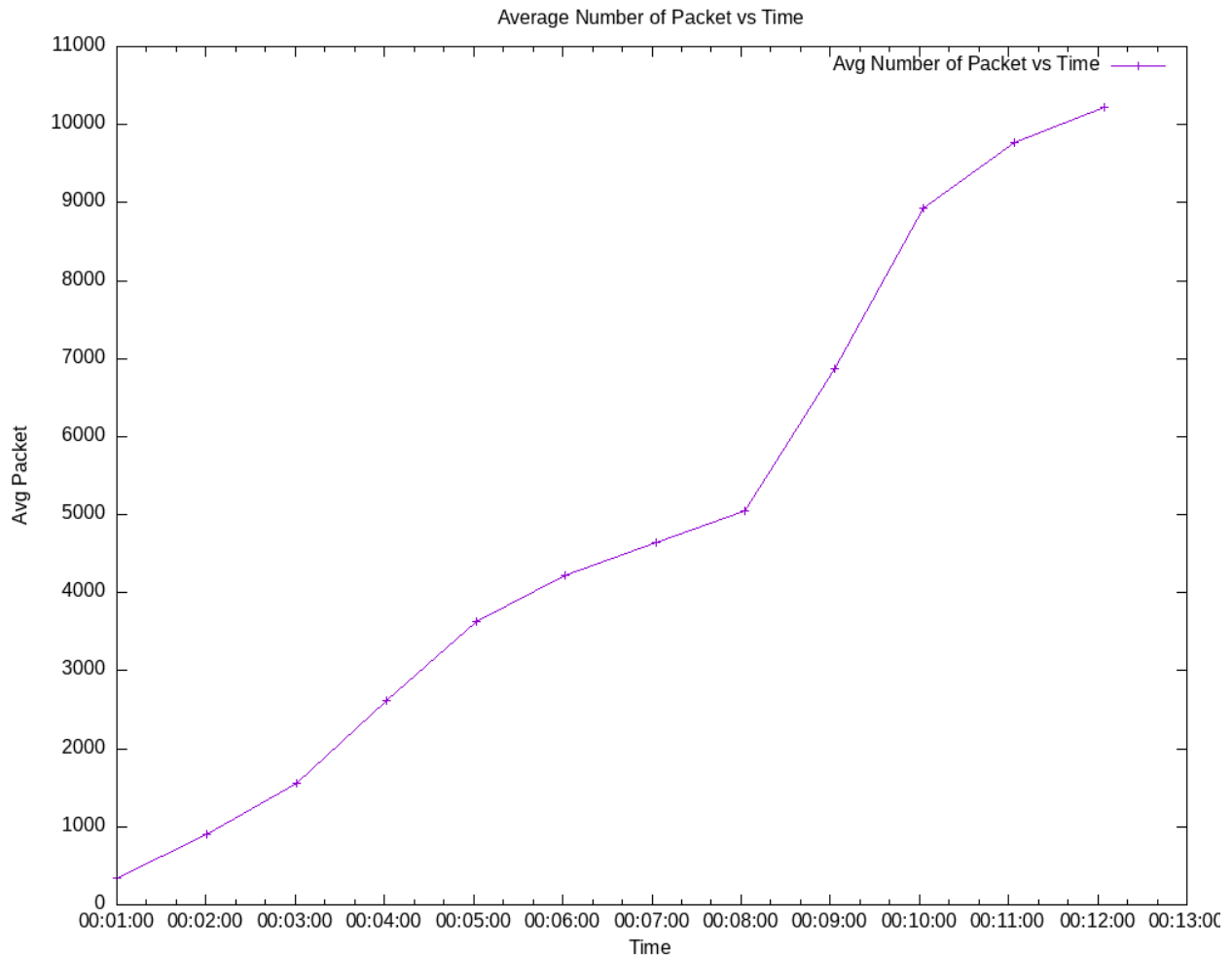
Trace 2

```
abhi@laptop:~$ ./avg_packet_rate_time.sh
```

```
/home/abhi/Downloads/wireshark-traces/cs23mtech11021_802_11.pcap
```

Successful!

```
abhi@laptop:~$
```



We can see that number of packets increased as the time increased

Q1 d:

Ans: Histogram of PHY data rate for trace 1

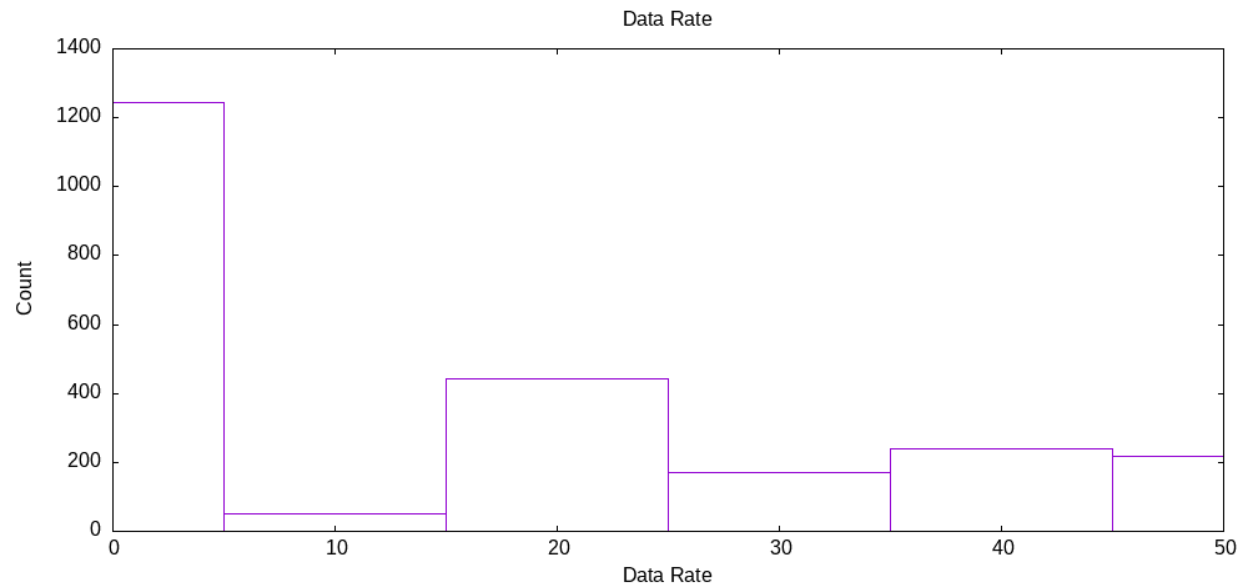
Command:

```
abhi@laptop:~$ chmod +x data_rate.sh
```

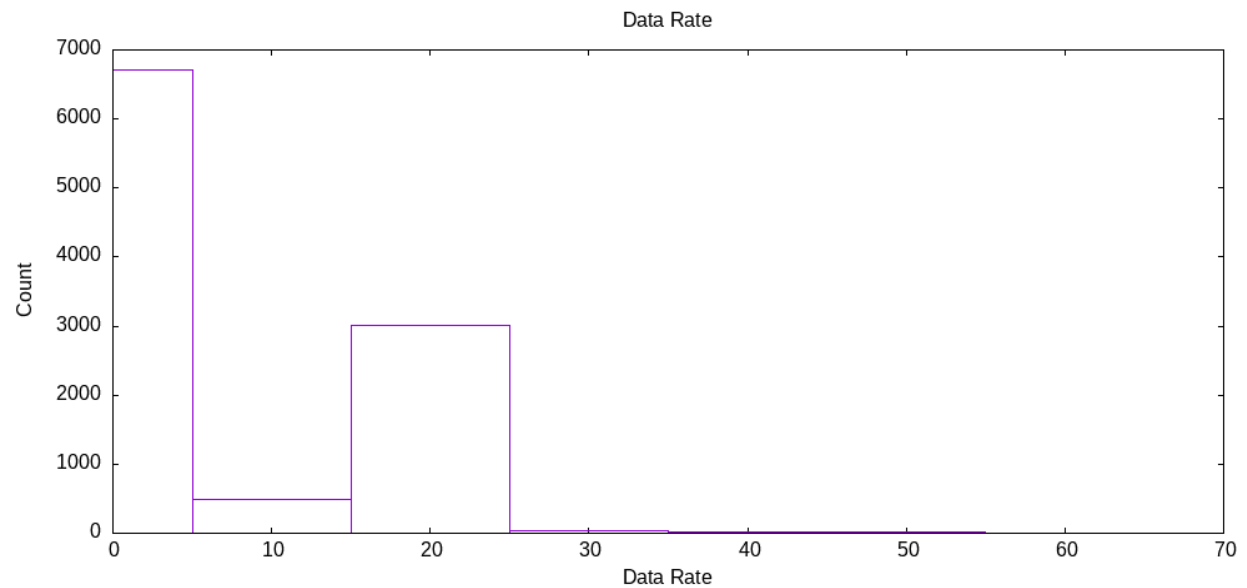
```
abhi@laptop:~$ ./data_rate.sh
```

```
/home/abhi/Downloads/wireshark-traces/Wireshark_802_11.pcap
```

Successful!



Trace 2



Histogram of packet size for trace 1

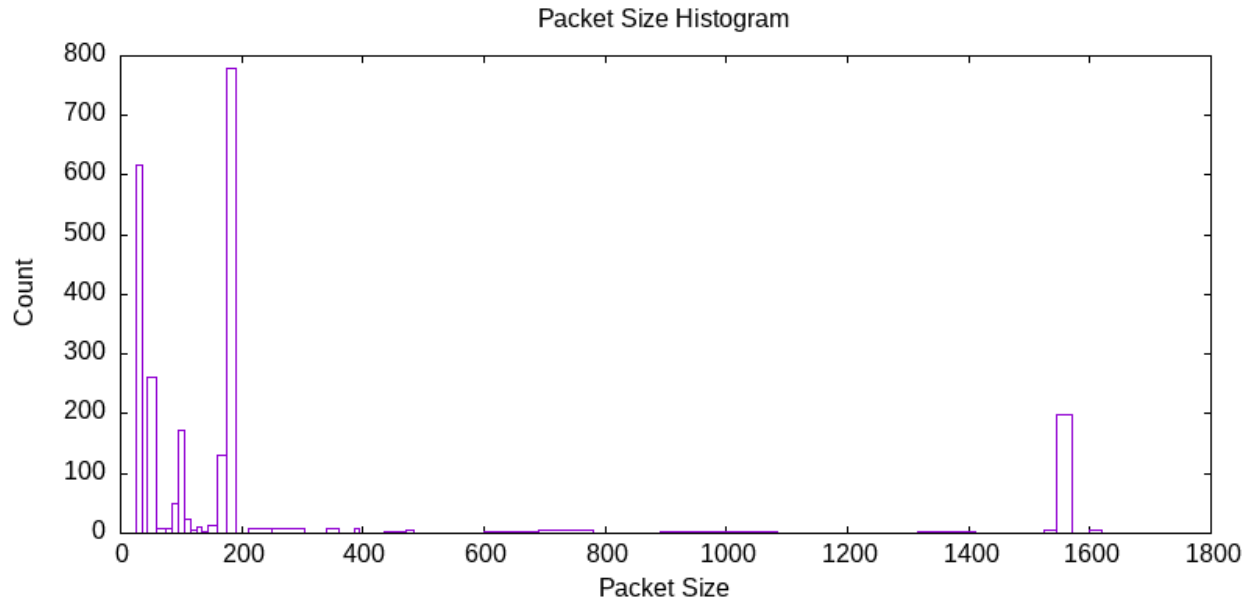
```
abhi@laptop:~$ chmod +x packet_size_rate.sh
```

```
abhi@laptop:~$ ./packet_size_rate.sh
```

```
/home/abhi/Downloads/wireshark-traces/Wireshark_802_11.pcap
```

Successful!

```
abhi@laptop:~$
```

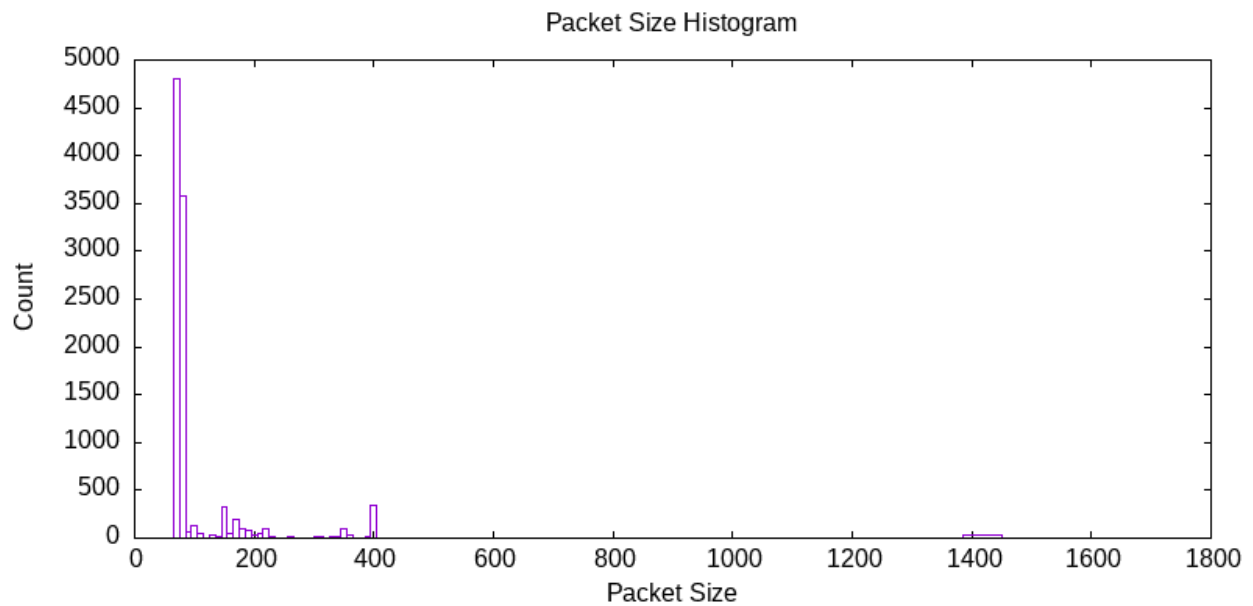


Trace 2:

```
abhi@laptop:~$ ./packet_size_rate.sh
```

```
/home/abhi/Downloads/wireshark-traces/cs23mtech11021_802_11.pcap
```

Successful!



Q2:

B:

Ans:

Configuring Laptop as hotspot

Step 1: Creating interface

Initial list of interfaces

```
abhi@laptop:~$ iw dev
phy#0
    Unnamed/non-netdev interface
        wdev 0x5
        addr 88:b1:11:41:aa:88
        type P2P-device
    Interface wlo1
        ifindex 3
        wdev 0x1
        addr 88:b1:11:41:aa:87
        ssid IITH
        type managed
        channel 116 (5580 MHz), width: 80 MHz, center1: 5610 MHz
        txpower 21.00 dBm
        multicast TXQ:
            qsz-byt qsz-pkt flows drops marks overlmt hashcol tx-bytes tx-packets
            0 0 0 0 0 0 0 0
```

Execute below command to create interface

`sudo iw dev wlo1 interface add wlan1 type __ap`

```
abhi@laptop:~$ iw dev
phy#0
    Interface wlan1
        ifindex 4
        wdev 0x6
        addr 88:b1:11:41:aa:89
        type managed
        multicast TXQ:
            qsz-byt qsz-pkt flows drops marks overlmt hashcol tx-bytes tx-packets
            0 0 0 0 0 0 0 0
    Unnamed/non-netdev interface
        wdev 0x5
        addr 88:b1:11:41:aa:88
        type P2P-device
    Interface wlo1
        ifindex 3
        wdev 0x1
        addr 88:b1:11:41:aa:87
        ssid IITH
        type managed
        channel 116 (5580 MHz), width: 80 MHz, center1: 5610 MHz
        txpower 21.00 dBm
        multicast TXQ:
            qsz-byt qsz-pkt flows drops marks overlmt hashcol tx-bytes tx-packets
            0 0 0 0 0 0 0 0
abhi@laptop:~$
```

Step2: Creating hotspot

`sudo ifconfig wlan1 192.168.10.1 up`

Step 3: Create a hostapd.conf file with content

interface=wlan1

driver=nl80211

```
ssid=Abhishree
channel=7
hw_mode=g
wme_enabled=1
macaddr_acl=0
auth_algs=1
ignore_broadcast_ssid=0
wpa=3
wpa_passphrase=123456789
wpa_key_mgmt=WPA-PSK
wpa_pairwise=TKIP
rsn_pairwise=CCMP
```

Now run the command : `sudo hostapd hostapd.conf`
This will create hotspot with name Abhishree

```
abhi@laptop:~$ sudo hostapd hostapd.conf
[sudo] password for abhi:
wlan1: interface state UNINITIALIZED->ENABLED
wlan1: AP-ENABLED
wlan1: STA 46:82:37:b0:4a:67 IEEE 802.11: authenticated
wlan1: STA 46:82:37:b0:4a:67 IEEE 802.11: associated (aid 1)
wlan1: AP-STA-CONNECTED 46:82:37:b0:4a:67
wlan1: STA 46:82:37:b0:4a:67 RADIUS: starting accounting session 5B0641D59AFD313C
wlan1: STA 46:82:37:b0:4a:67 WPA: pairwise key handshake completed (RSN)
wlan1: EAPOL-4WAY-HS-COMPLETED 46:82:37:b0:4a:67
wlan1: AP-STA-DISCONNECTED 46:82:37:b0:4a:67
wlan1: STA 46:82:37:b0:4a:67 IEEE 802.11: authenticated
wlan1: STA 46:82:37:b0:4a:67 IEEE 802.11: associated (aid 1)
wlan1: AP-STA-CONNECTED 46:82:37:b0:4a:67
wlan1: STA 46:82:37:b0:4a:67 RADIUS: starting accounting session A9F6710B44E8A7BA
wlan1: STA 46:82:37:b0:4a:67 WPA: pairwise key handshake completed (RSN)
wlan1: EAPOL-4WAY-HS-COMPLETED 46:82:37:b0:4a:67
```

Step 4: Configure udhcp.conf file

Edit the following detail

```
start 192.168.50.2 #default: 192.168.0.20
end 192.168.50.254 #default: 192.168.0.254
```

The interface that udhcpd will use

```
interface wlan1 #default: eth0
#Examples
opt dns 8.8.8.8 8.8.4.4
option subnet 255.255.255.0
```

```
opt router 10.5.82.150
opt wins 192.168.10.10
option dns 129.219.13.81 # appened to above DNS servers for a total of 3
option domain local
option lease 864000 # 10 days of seconds
```

Save and run the following commands

```
sudo udhcpd -f
```

This will provide ip to the devices which will connect to the hotspot

```
udhcpd: ts interface wlan1 up and configured.: cannot assign requested address
abhi@laptop:~$ sudo udhcpd -f
udhcpd: started, v1.30.1
udhcpd: can't open '/var/lib/misc/udhcpd.leases': No such file or directory
udhcpd: sending OFFER of 192.168.50.32
udhcpd: sending OFFER of 192.168.50.32
udhcpd: sending ACK to 192.168.50.32
```

Step 5: Configure ip forwarding

Run the following command in root

```
root@laptop:/home/abhi# gedit /etc/sysctl.conf
```

Add command `net.ipv4.ip_forward = 1` in the file and save it.

Then run below commands to make it permanent

```
root@laptop:/home/abhi# sudo sysctl -p
```

Now run this command to forward the packets

```
root@laptop:/home/abhi# echo "1" > /proc/sys/net/ipv4/ip_forward
```

```
root@laptop:/home/abhi# iptables --table nat --append POSTROUTING --out-interface eno1 -j MASQUERADE
```

```
root@laptop:/home/abhi# iptables --append FORWARD --in-interface wlan1 -j ACCEPT
```

This will forward the incoming packet on interface wlan1(hotspot) to eno1(internet)

A.

Unable to get survey dump to which estimates channel utilization


```

abhi@laptop:~$ iw dev
phy#0
    Interface wlan1
        ifindex 9
        wdev 0x13
        addr 88:b1:11:41:aa:89
        type AP
        txpower 22.00 dBm
        multicast TXQ:
            qsz-byt  qsz-pkt  flows  drops  marks  overlmt  hashcol  tx-bytes  tx-packets
            0         0        94     0      0      0        0        16325     94
    Interface wlo1
        ifindex 3
        wdev 0x1
        addr 88:b1:11:41:aa:87
        type managed
        multicast TXQ:
            qsz-byt  qsz-pkt  flows  drops  marks  overlmt  hashcol  tx-bytes  tx-packets
            0         0        27     0      0      0        0        3759     27
abhi@laptop:~$ iw dev wlan1 survey dump
abhi@laptop:~$

```

Step that i would have followed to if survey dump worked

Step1: Get the utilization of all the channels using survey dump and store it in array

Step2: Run a loop through this array and get the channel with least value

Step3: Set the Ap to that channel using iw dev wlo1 set channel command

C.

Ans: Run min_client.sh script to connect to wifi with least number of station

For some reason i'm not able to disconnect using wlo1.

```

abhi@laptop:~$ sudo iw dev wlo1 disconnect
command failed: Operation not permitted (-1)
abhi@laptop:~$

```

PLAGIARISM STATEMENT

I certify that this assignment/report is my own work, based on my personal study and/or research and that I have acknowledged all material and sources used in its preparation, whether they be books, articles, reports, lecture notes, and any other kind of document, electronic or personal communication. I also certify that this assignment/report has not previously been

submitted for assessment in any other course, except where specific permission has been granted

from all course instructors involved, or at any other time in this course, and that I have not copied

in part or whole or otherwise plagiarised the work of other students and/or persons. I pledge to uphold the principles of honesty and responsibility at CSE@IITH. In addition, I understand my

responsibility to report honour violations by other students if I become aware of it.

Name: Abhishree Khangar

Date: 13 March 2024

Signature: AK