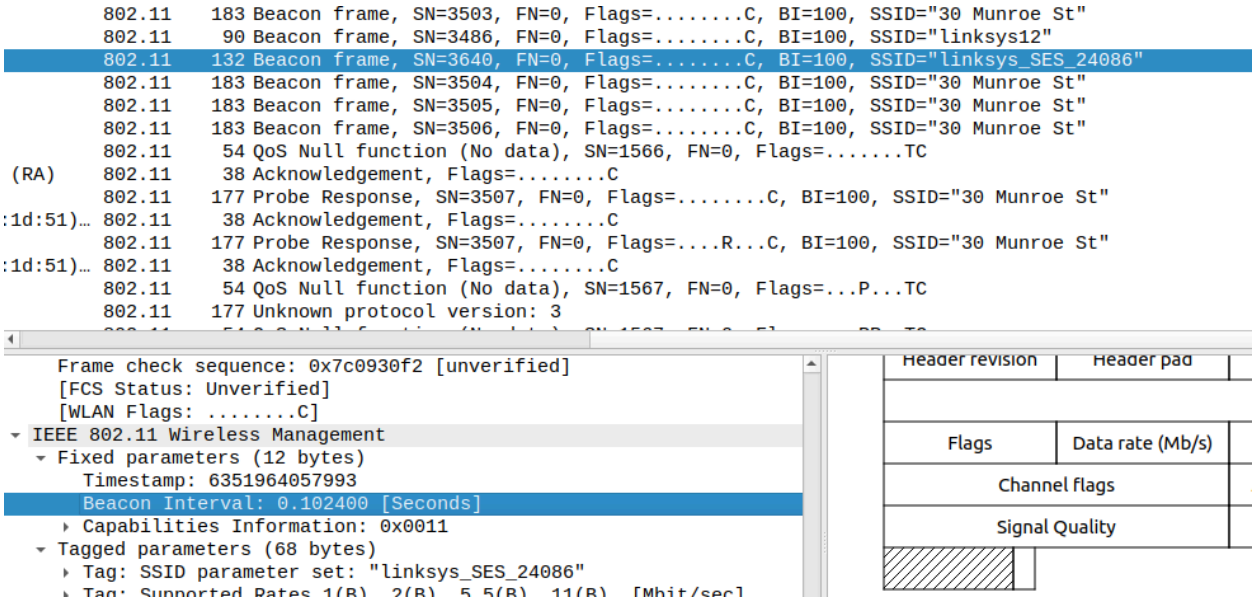
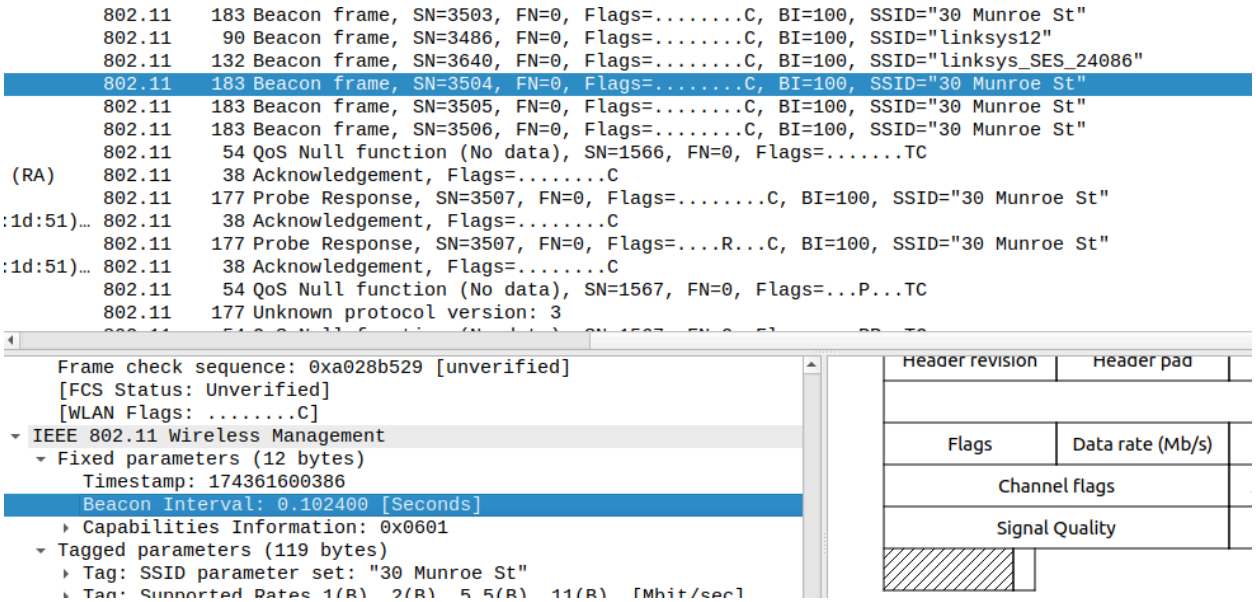
Q1: The SSIDs of the two access points that are issuing most of the beacon Frames are

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]

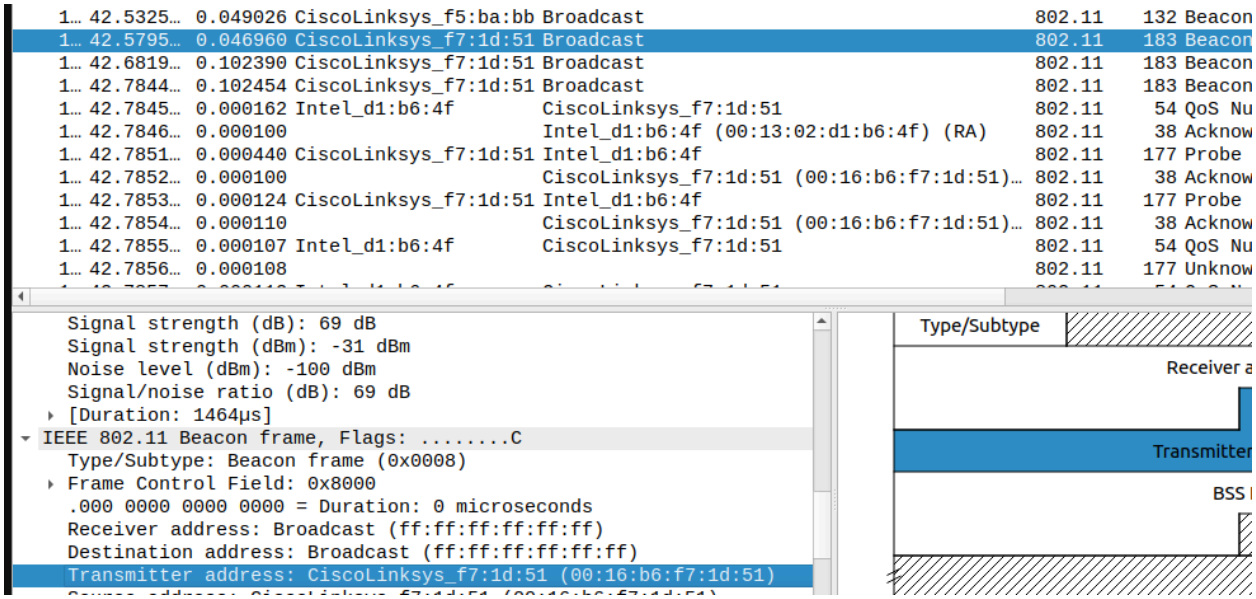


For 30 Munroe St. access point: Beacon Interval: 0.102400 [Seconds]



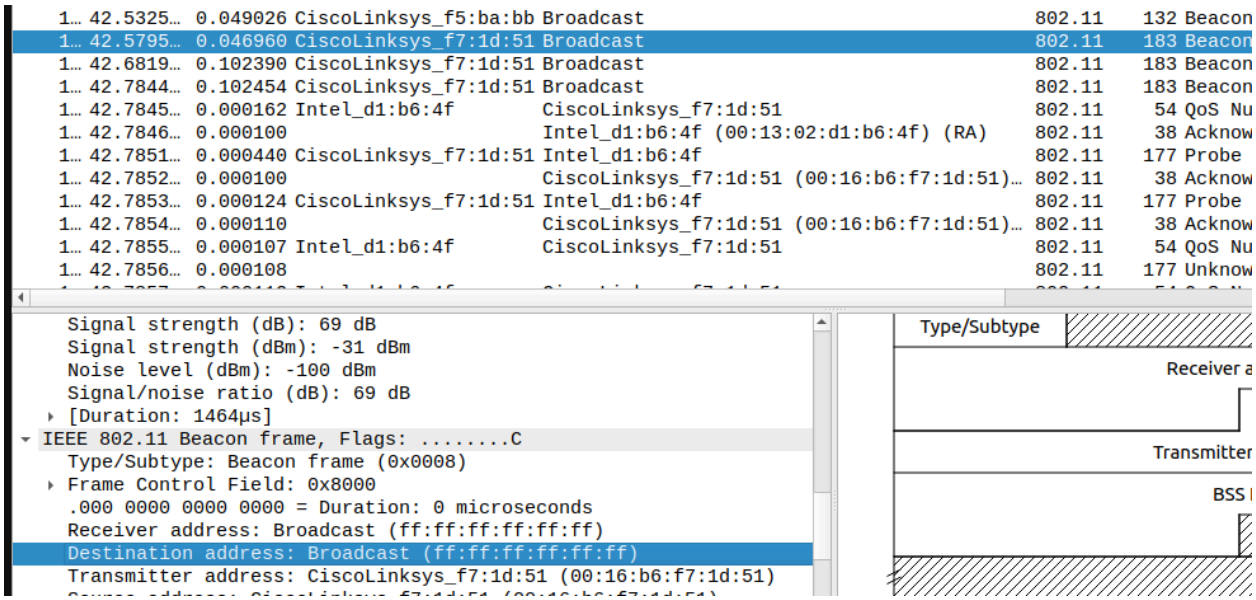
Q3:

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



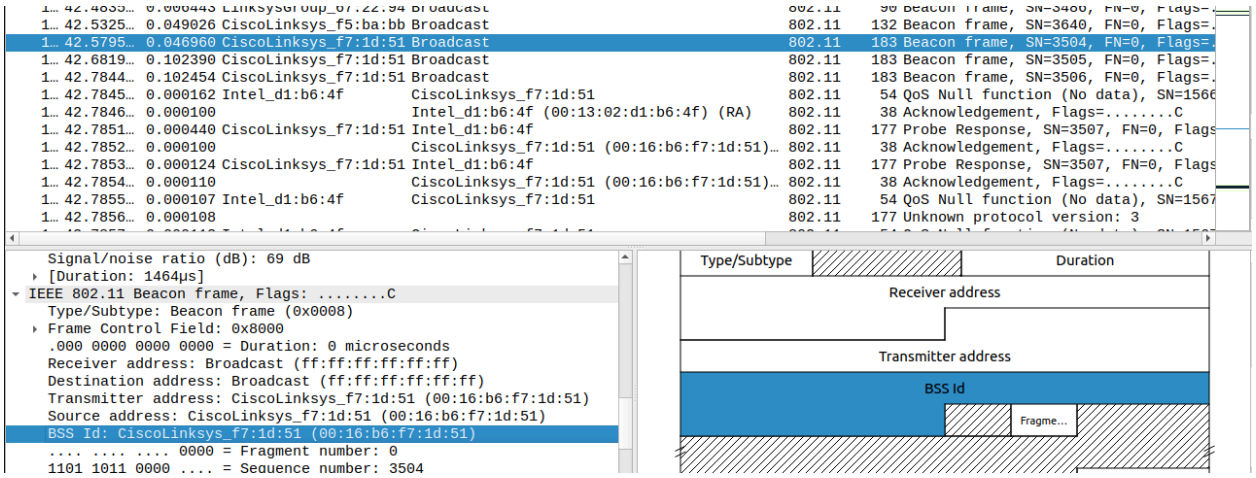
Q4:

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



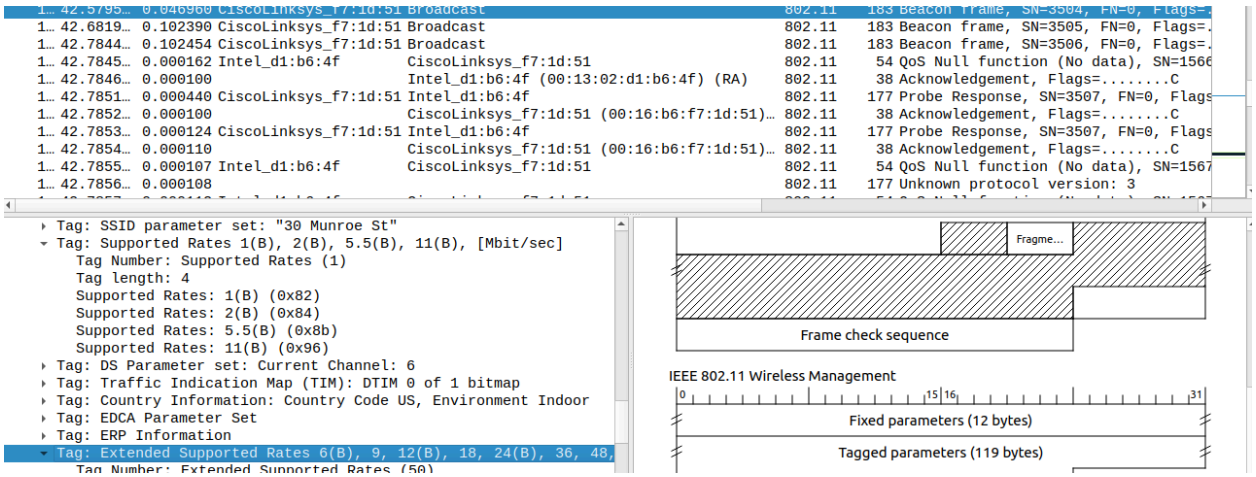
Q5:

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

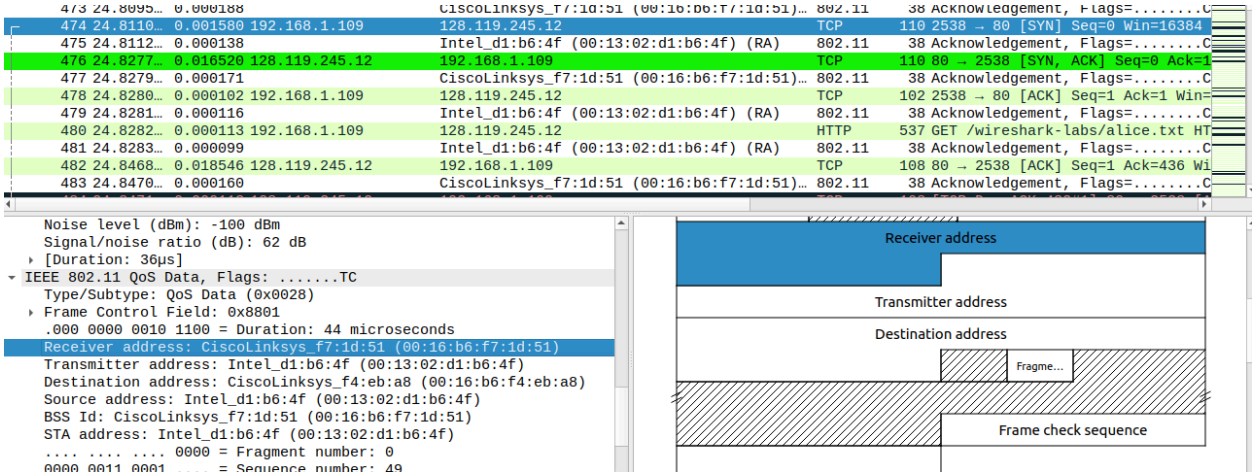


Q6:

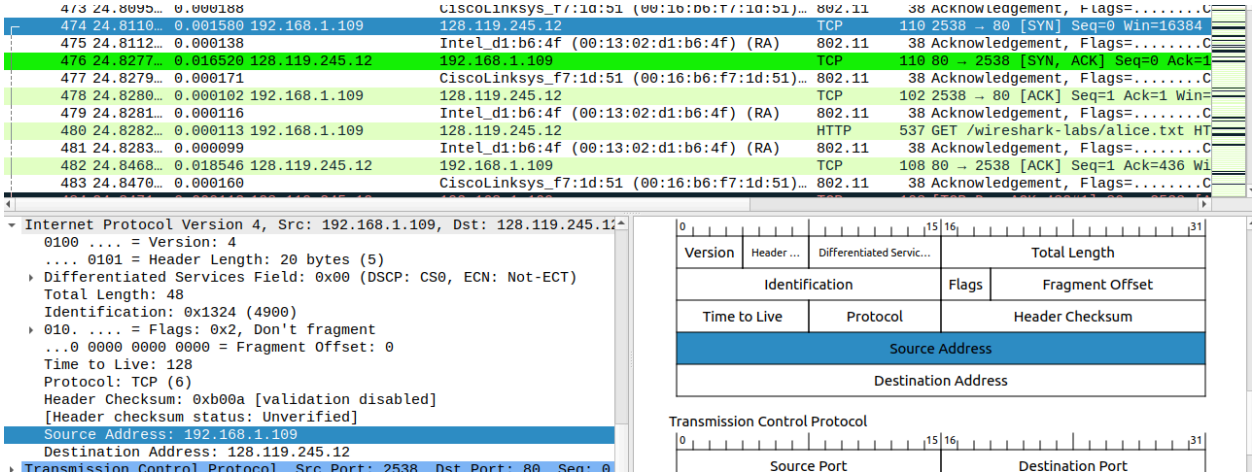
Tag: Supported Rates are 1, 2, 5.5 and 11 Mbit/sec and Extended Supported Rates 6, 9, 12, 18, 24, 36, 48, 54 Mbit/sec



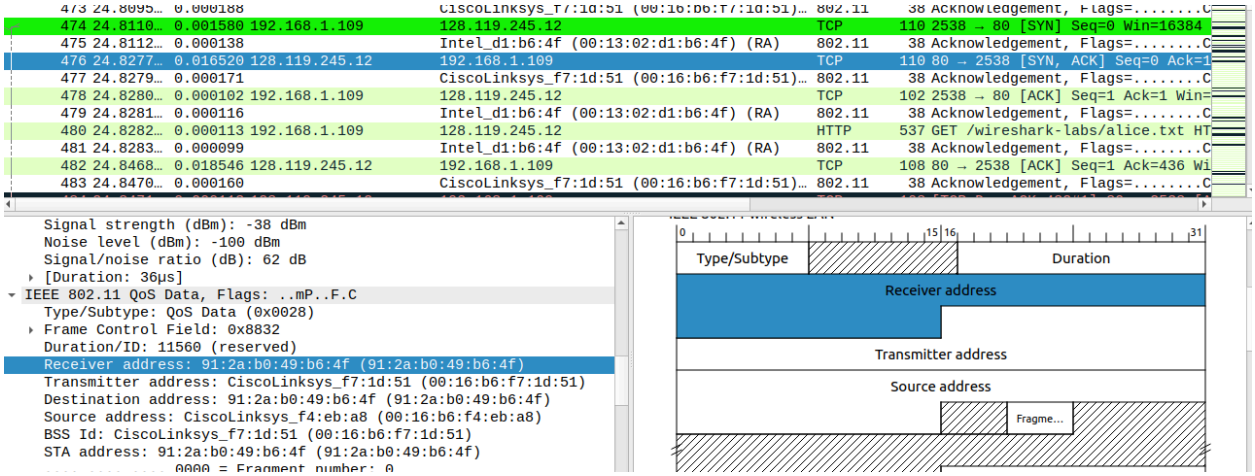
Q7:
Sender MAC address (Host) :00:13:02:d1:b6:4f
Destination address is: 00:16:b6:f4:eb:a8
BSS address 00:16:b6:f7:1d:51



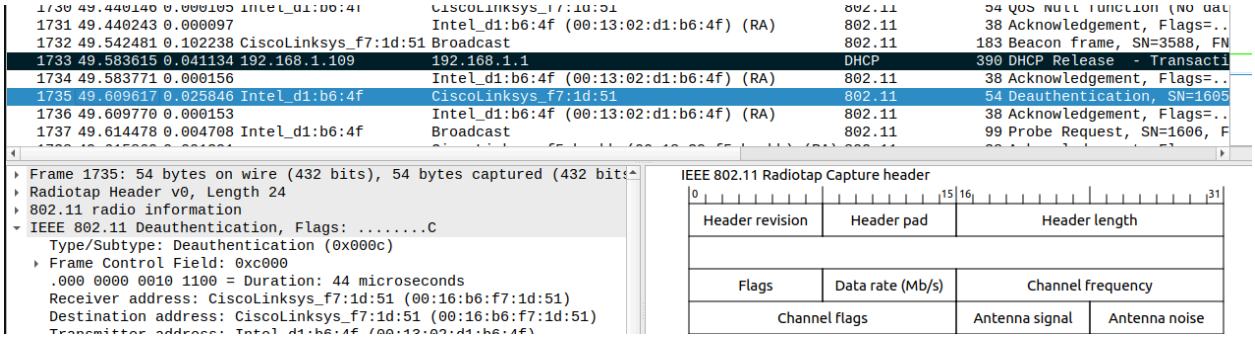
The source ip address is 192.168.1.109, which corresponds to the host's ip address
Destination ip address is 128.119.245.12 which corresponds to the destination address(gaia.cs.umass.edu)



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



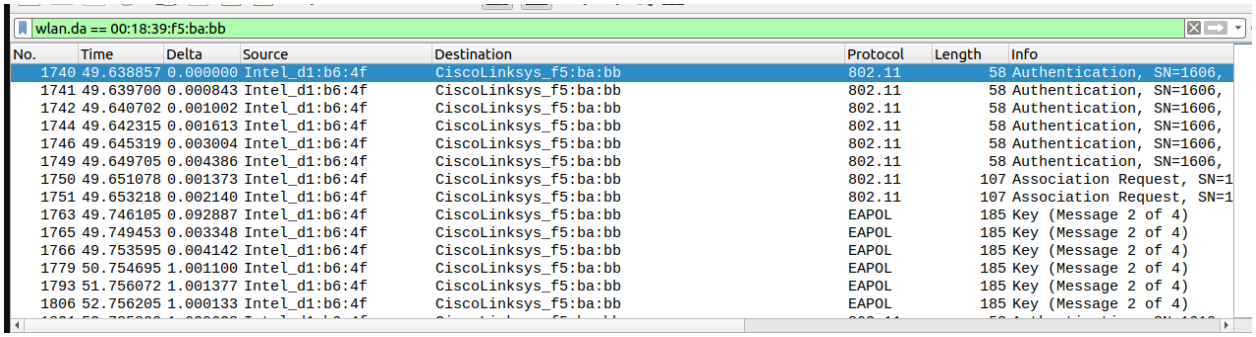
Q9:
Ans: At t=49.583615 we can see a DHCP release message
At t= 49.609617 we can see a deauthentication message



We cannot see any disassociation request sent.

Q10

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

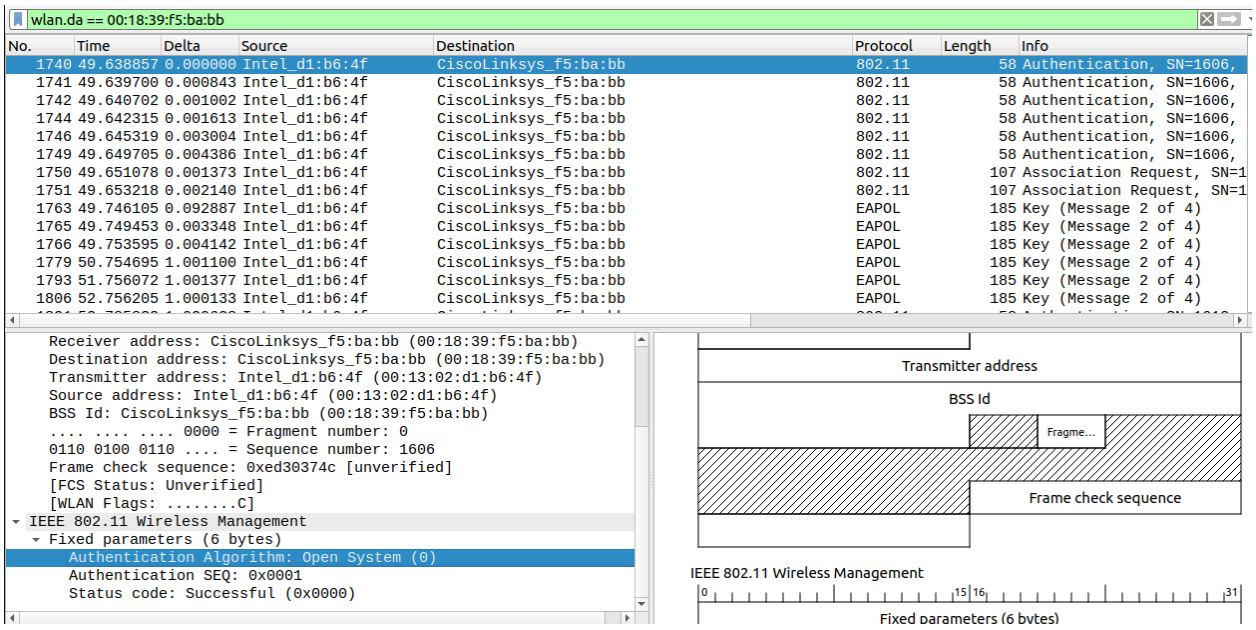


wlan.da == 00:18:39:f5:ba:bb

No.	Time	Delta	Source	Destination	Protocol	Length	Info
1740	49.638857	0.000000	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606,
1741	49.639700	0.000843	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606,
1742	49.640702	0.001002	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606,
1744	49.642315	0.001613	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606,
1746	49.645319	0.003004	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606,
1749	49.649705	0.004386	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606,
1750	49.651078	0.001373	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	107	Association Request, SN=1
1751	49.653218	0.002140	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	107	Association Request, SN=1
1763	49.746105	0.092887	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	EAPOL	185	Key (Message 2 of 4)
1765	49.749453	0.003348	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	EAPOL	185	Key (Message 2 of 4)
1766	49.753595	0.004142	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	EAPOL	185	Key (Message 2 of 4)
1779	50.754695	1.001100	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	EAPOL	185	Key (Message 2 of 4)
1793	51.756072	1.001377	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	EAPOL	185	Key (Message 2 of 4)
1806	52.756205	1.000133	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	EAPOL	185	Key (Message 2 of 4)

Q11:

Ans The host want authentication to be open



wlan.da == 00:18:39:f5:ba:bb

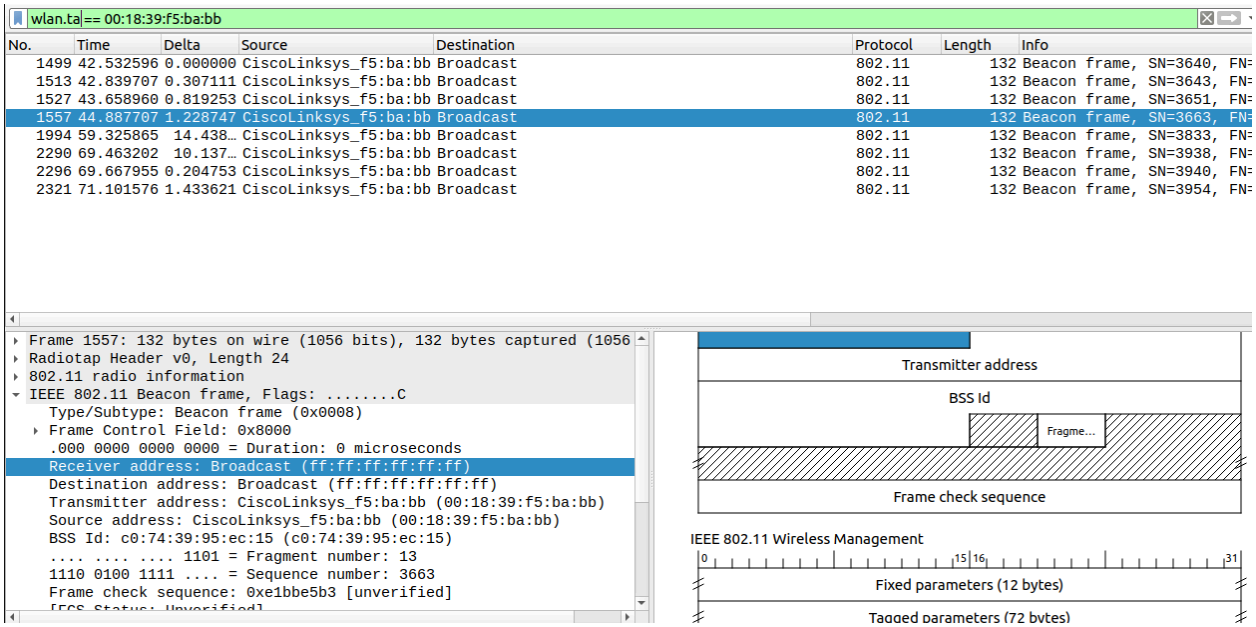
No.	Time	Delta	Source	Destination	Protocol	Length	Info
1740	49.638857	0.000000	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606,
1741	49.639700	0.000843	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606,
1742	49.640702	0.001002	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606,
1744	49.642315	0.001613	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606,
1746	49.645319	0.003004	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606,
1749	49.649705	0.004386	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	58	Authentication, SN=1606,
1750	49.651078	0.001373	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	107	Association Request, SN=1
1751	49.653218	0.002140	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	802.11	107	Association Request, SN=1
1763	49.746105	0.092887	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	EAPOL	185	Key (Message 2 of 4)
1765	49.749453	0.003348	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	EAPOL	185	Key (Message 2 of 4)
1766	49.753595	0.004142	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	EAPOL	185	Key (Message 2 of 4)
1779	50.754695	1.001100	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	EAPOL	185	Key (Message 2 of 4)
1793	51.756072	1.001377	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	EAPOL	185	Key (Message 2 of 4)
1806	52.756205	1.000133	Intel_d1:b6:4f	CiscoLinksys_f5:ba:bb	EAPOL	185	Key (Message 2 of 4)

```
Receiver address: CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb)
Destination address: CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb)
Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
Source address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
BSS Id: CiscoLinksys_f5:ba:bb (00:18:39:f5:ba:bb)
.... .... .... 0000 = Fragment number: 0
0110 0100 0110 .... = Sequence number: 1606
Frame check sequence: 0xed30374c [unverified]
[FCS Status: Unverified]
[WLAN Flags: ........C]
IEEE 802.11 Wireless Management
  Fixed parameters (6 bytes)
    Authentication Algorithm: Open System (0)
    Authentication SEQ: 0x0001
    Status code: Successful (0x0000)
```

Q12:

Ans

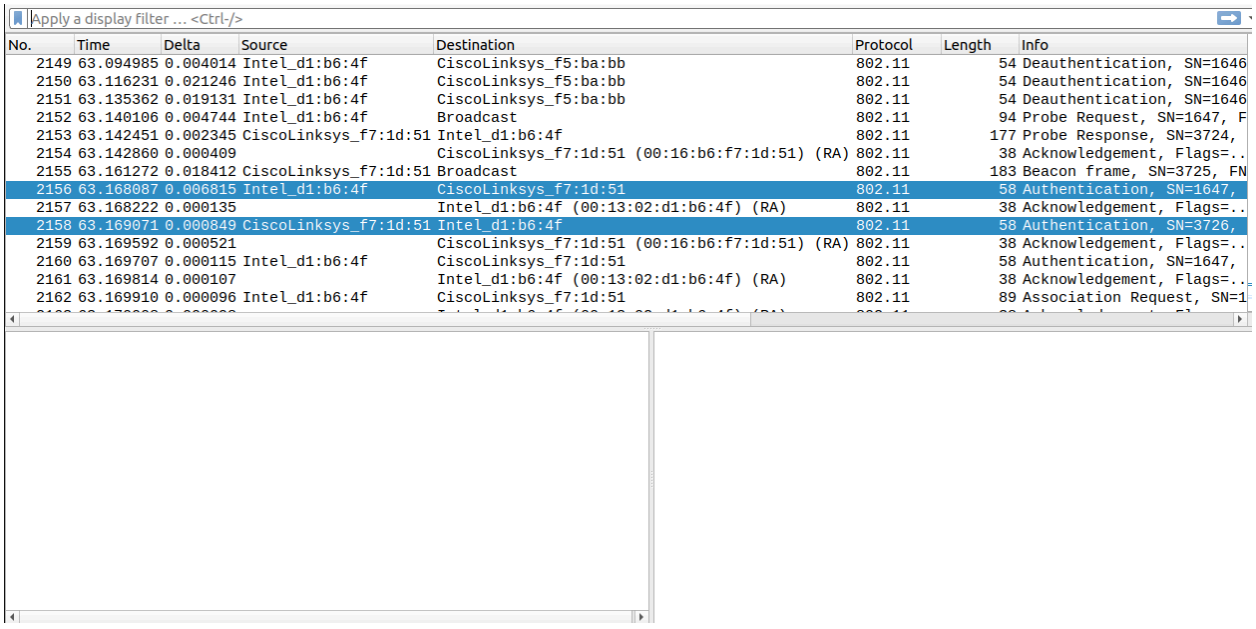
No,we can’t see a authentication message from linksys_ses_24086 AP



Q13:

At t= 63.168087 host sends an authentication request to bss

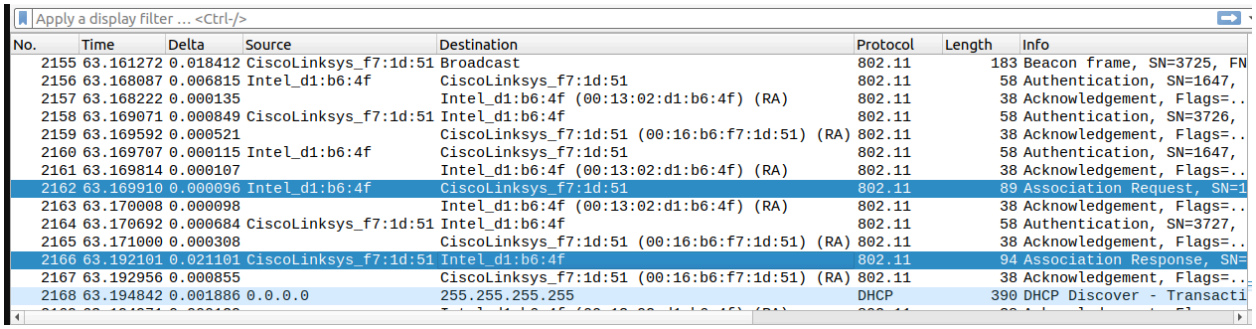
Ans at t = 63.169071 bss sends and authentication request to host



Q14:

Ans

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

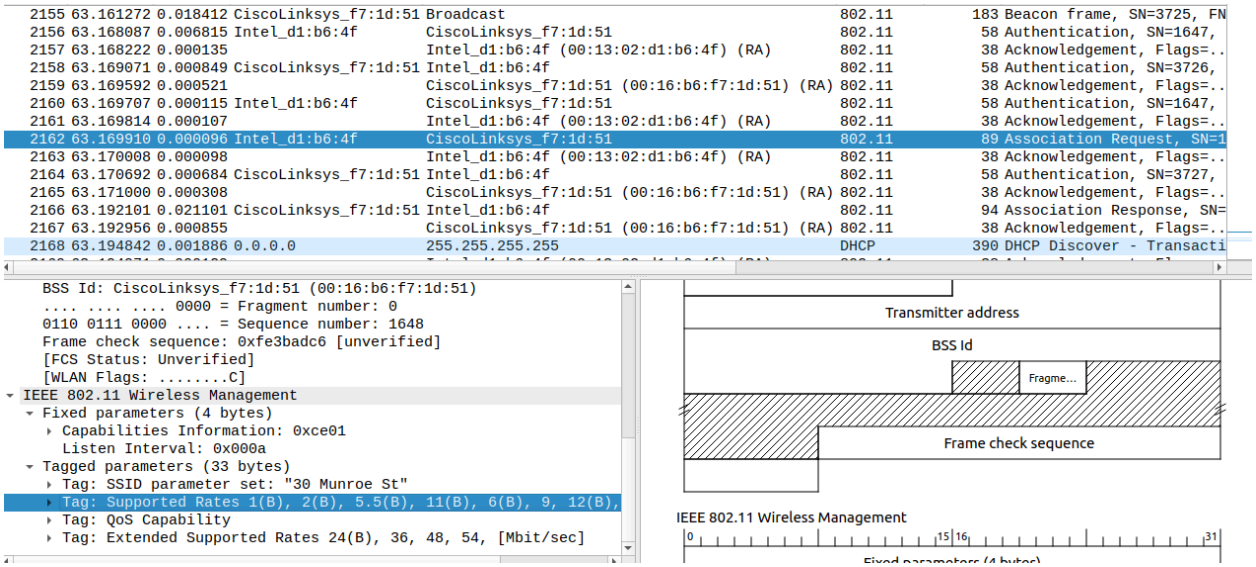


Apply a display filter ... <Ctrl-/>

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,
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,
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,
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
2163	63.170008	0.000098		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,
2165	63.171000	0.000308		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=
2167	63.192956	0.000855		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 - Transacti

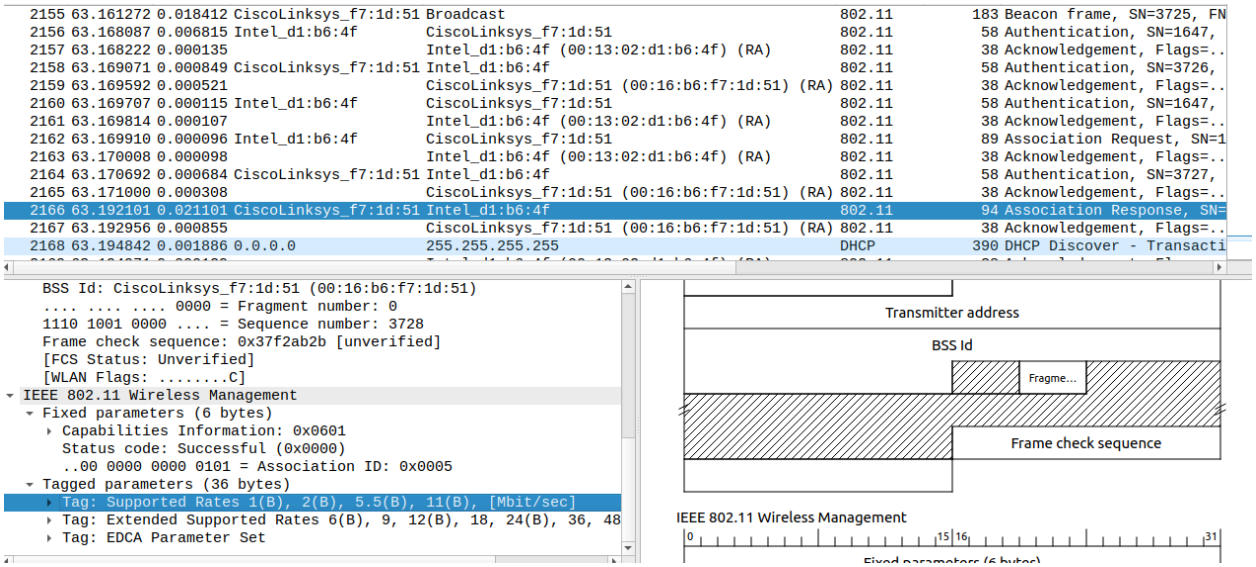
Q15:

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,
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,
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,
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
2163	63.170008	0.000098		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,
2165	63.171000	0.000308		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=
2167	63.192956	0.000855		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 - Transacti

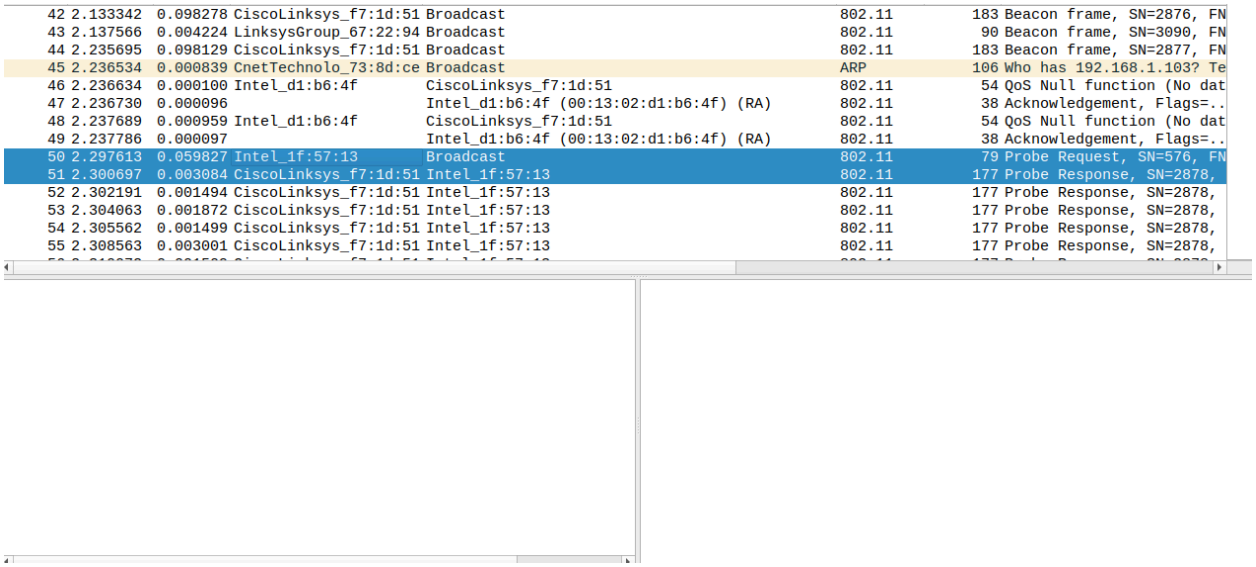
```
BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
.... .... .... 0000 = Fragment number: 0
0110 0111 0000 .... = Sequence number: 1648
Frame check sequence: 0xfe3badc6 [unverified]
[FCS Status: Unverified]
[WLAN Flags: ........C]
IEEE 802.11 Wireless Management
  Fixed parameters (4 bytes)
    Capabilities 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),
    Tag: QoS Capability
    Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]
```



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,



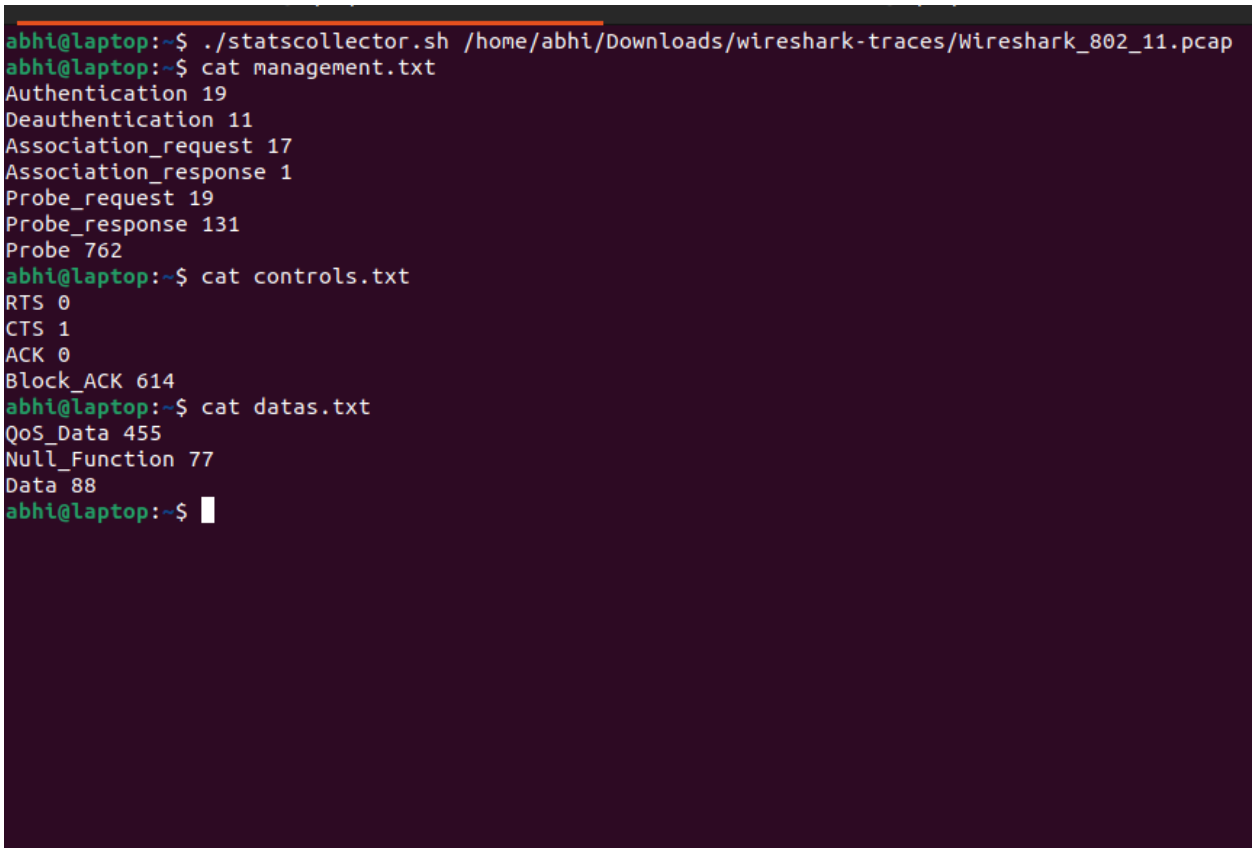
In active scanning, host send probe request to find an AP and in response AP responds with Probe Response.

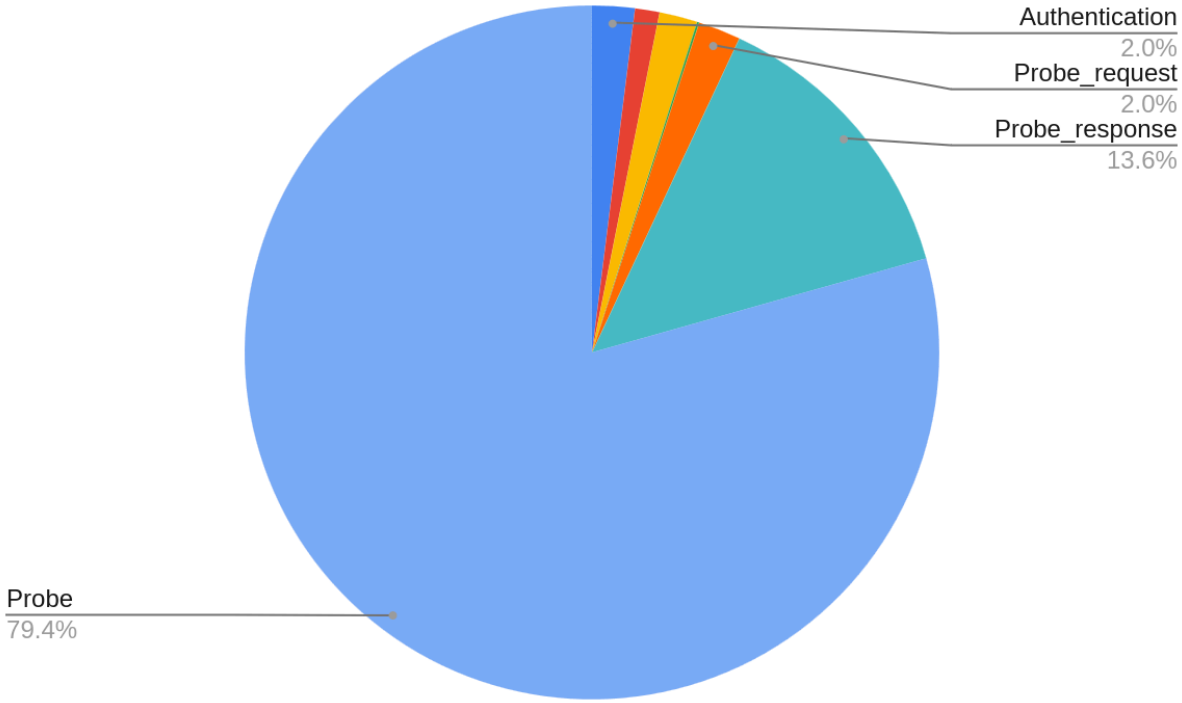
Q1a: Trace 1

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

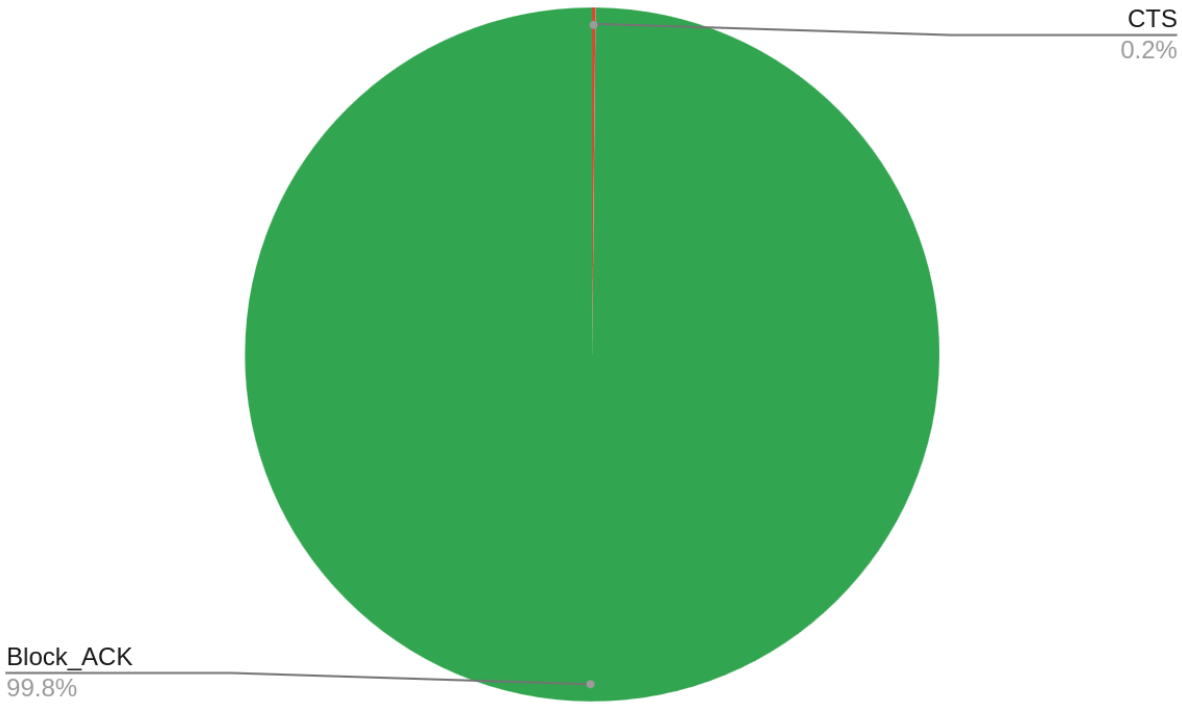
chmod +x statscollector.sh
./statscollector.sh Wireshark_802_11.pcap

Output will 3 files which gives the stats

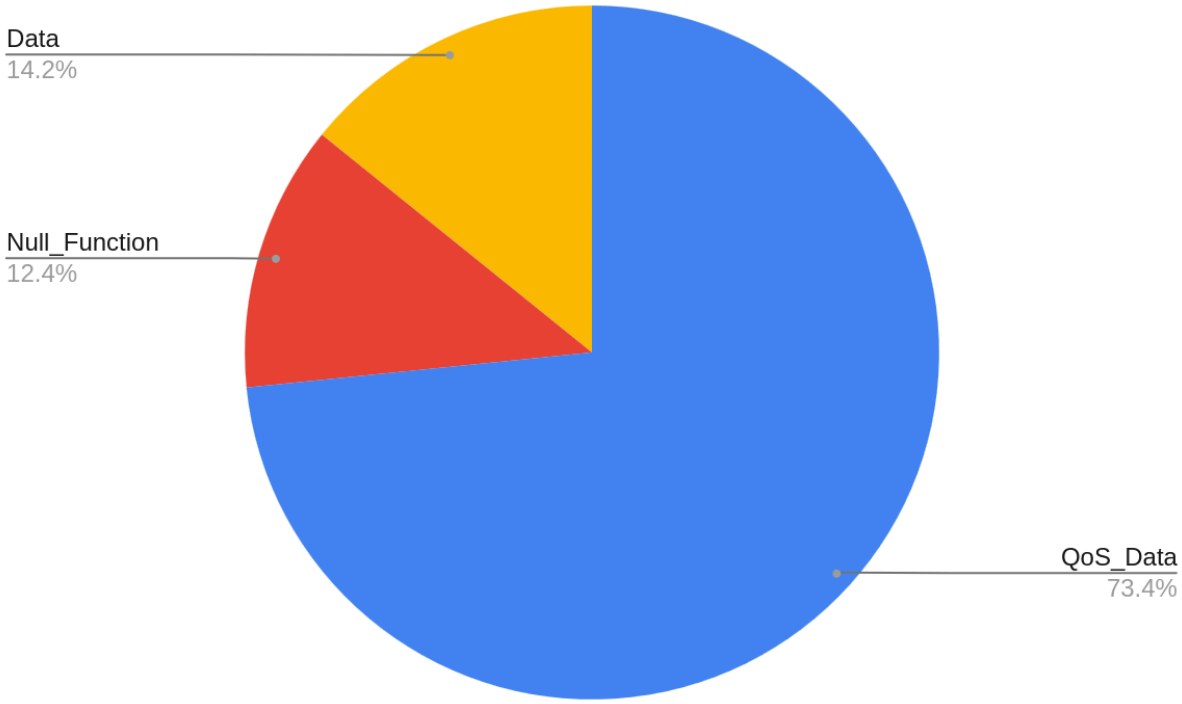




MAC Management frames



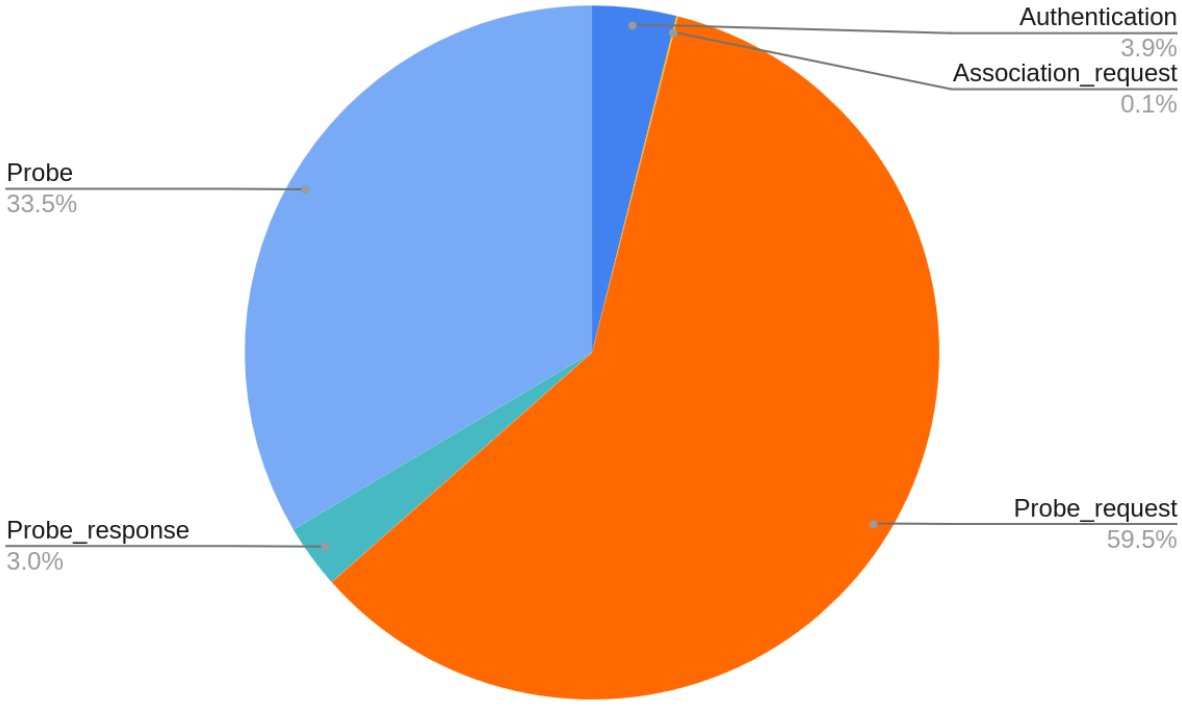
Control Frames



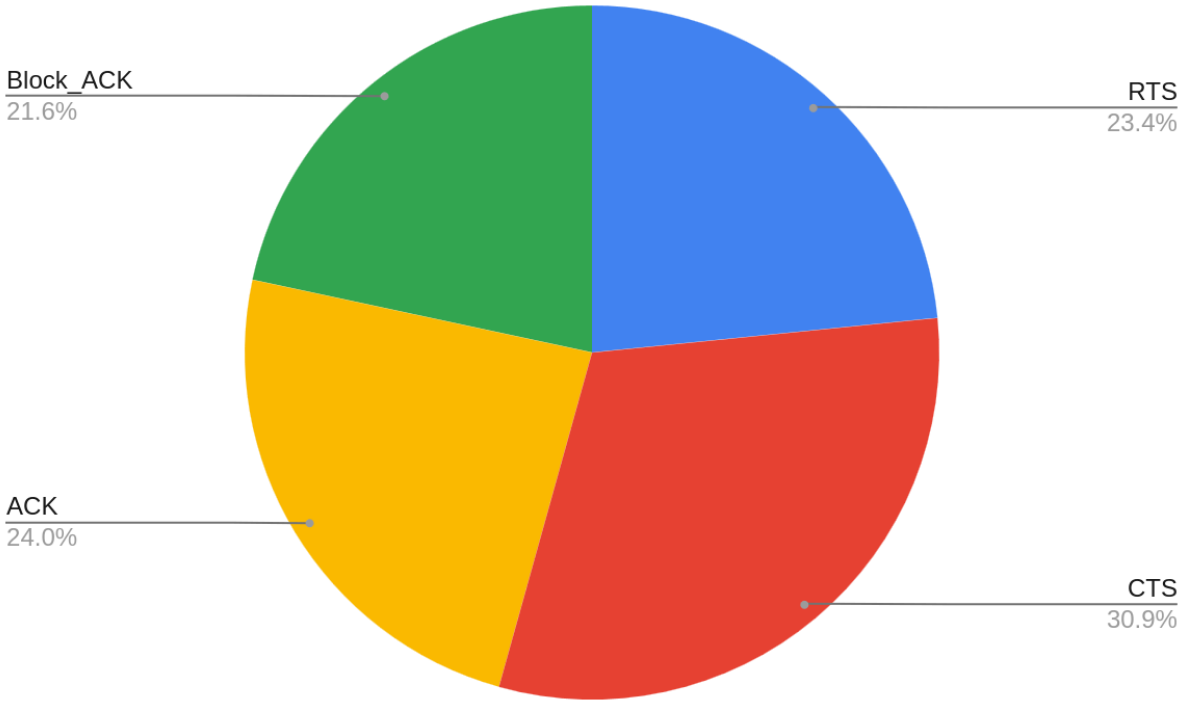
Data frame

Trace 2

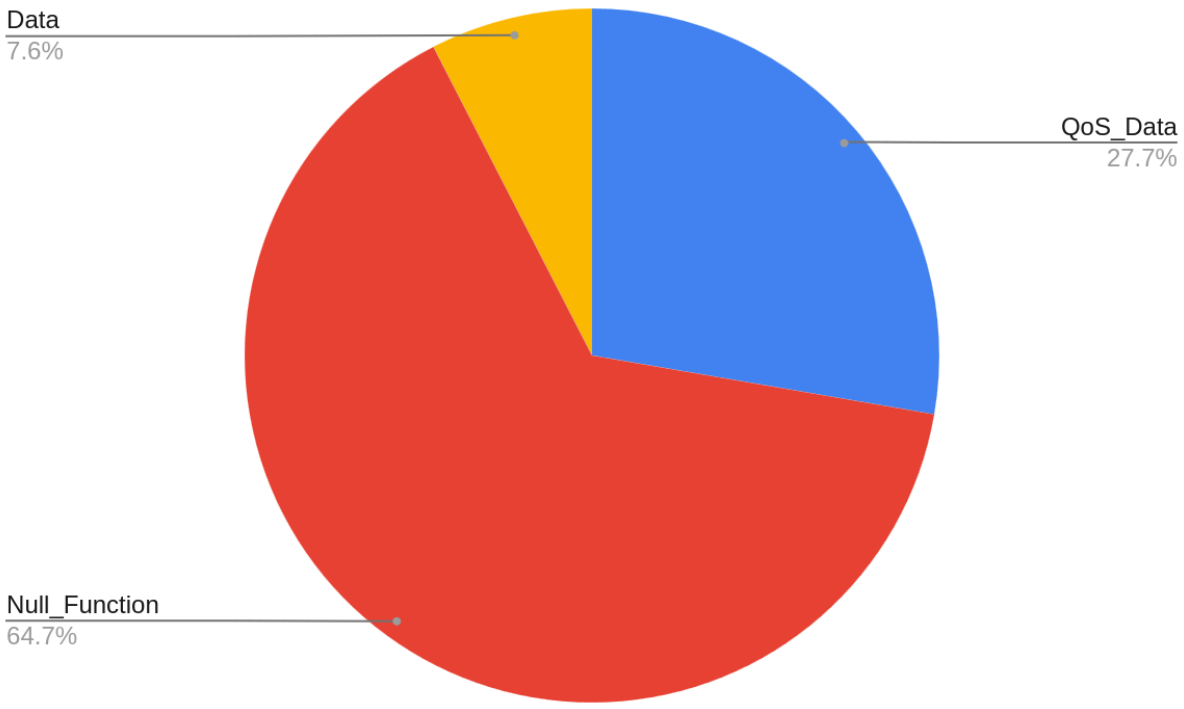
```
abhi@laptop:~$ ./statscollector.sh /home/abhi/Downloads/wireshark-traces/cs23mtech11021_802_11.pcap
abhi@laptop:~$ cat management.txt
Authentication 55
Deauthentication 0
Association_request 1
Association_response 0
Probe_request 836
Probe_response 42
Probe 471
abhi@laptop:~$ cat controls.txt
RTS 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

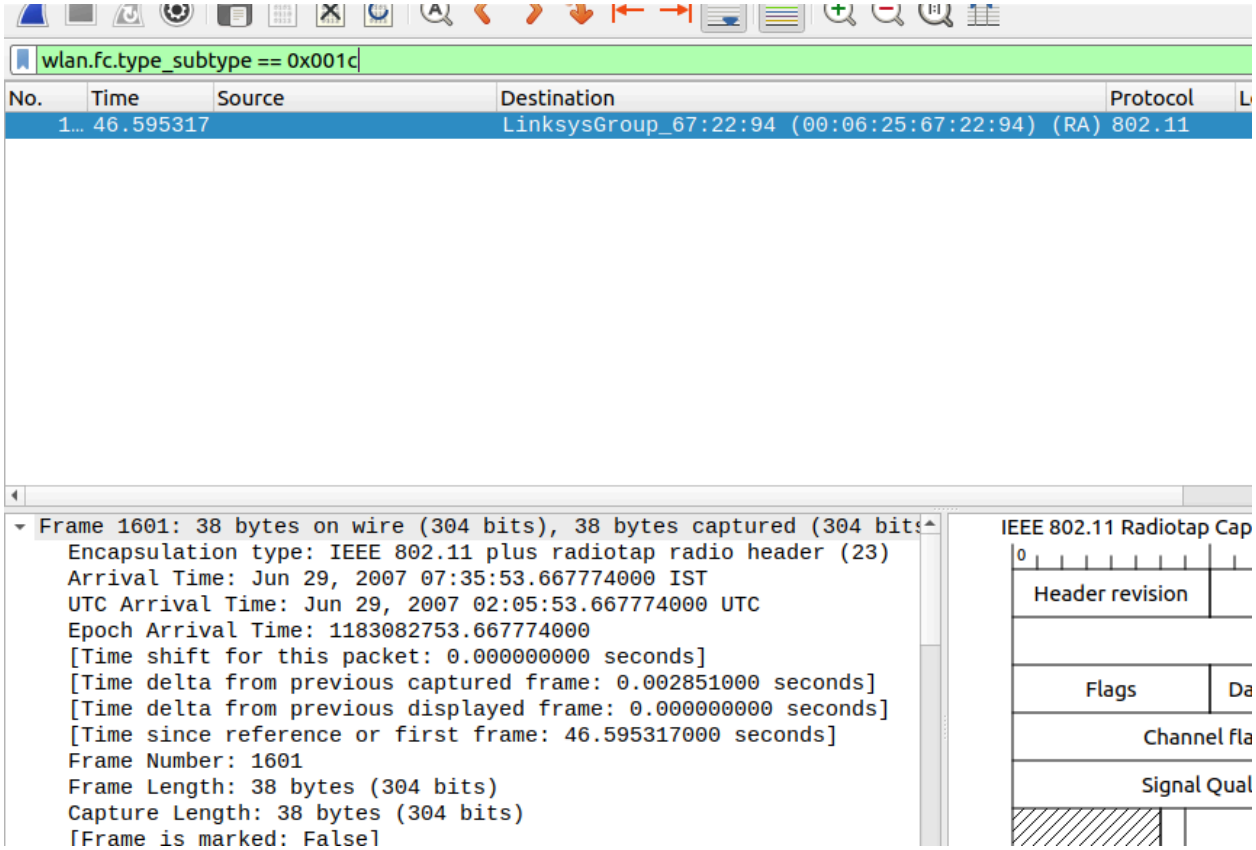


Data frames

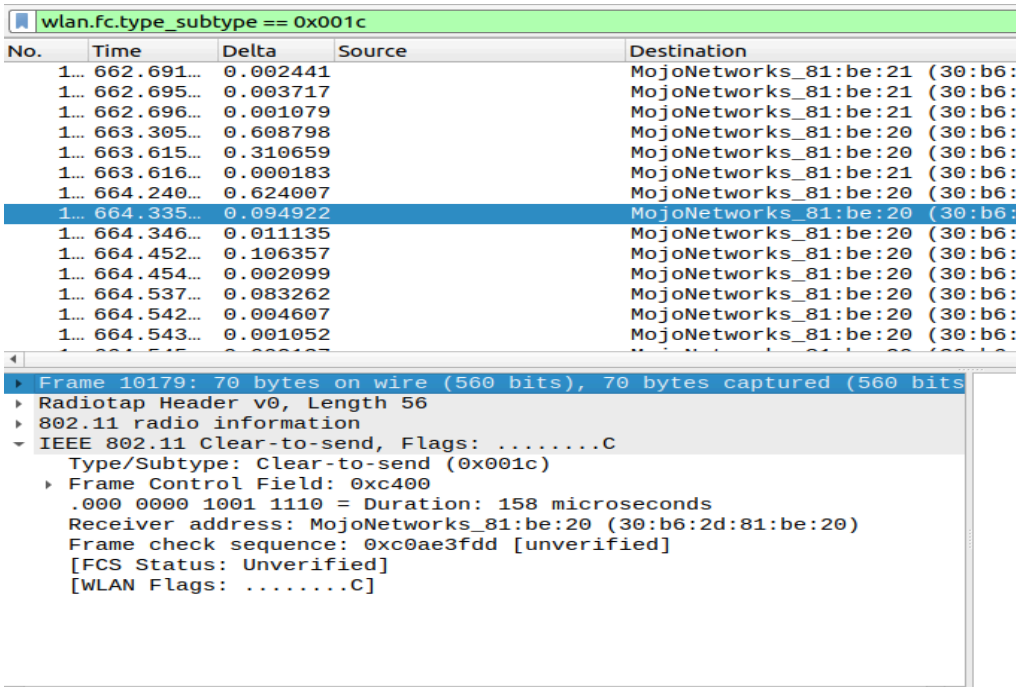
Q1b1
Ans: No. of different APs visible in trace 1 is 9
No. of different APs visible in trace 2 is 5

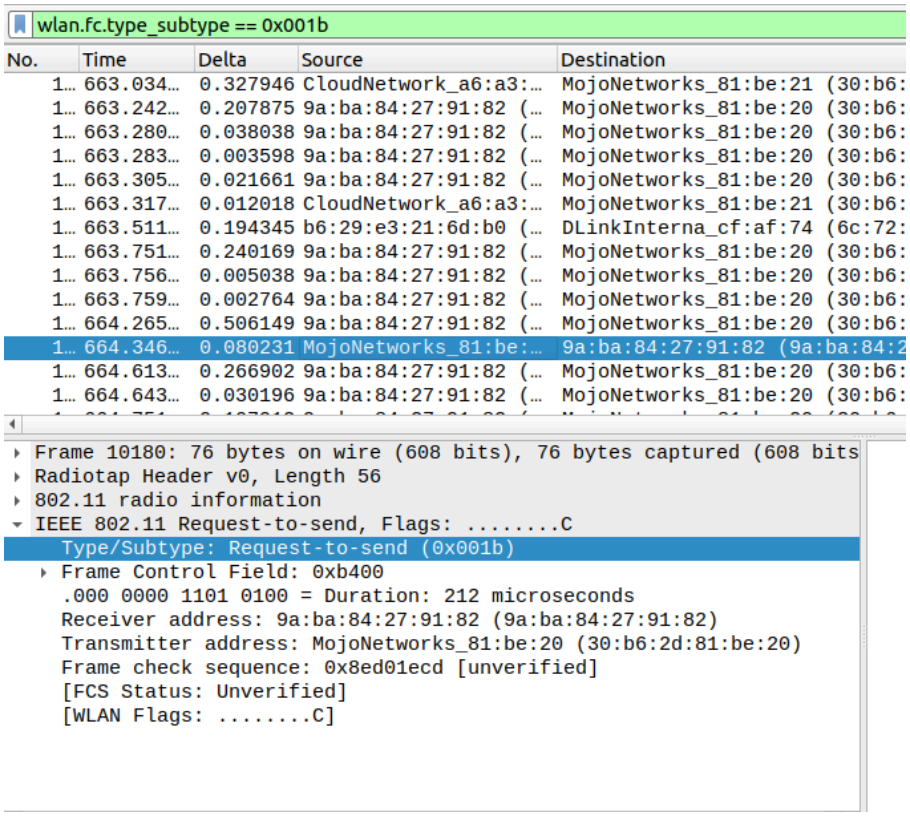
Protocol	Length	Info
802.11	355	Beacon frame, SN=1329, FN=0, Flags=........C, BI=100, SSID="IITH"
802.11	357	Beacon frame, SN=3286, FN=0, Flags=........C, BI=100, SSID="eduroam"
802.11	364	Beacon frame, SN=2398, FN=0, Flags=........C, BI=100, SSID="Placement-2023"
802.11	364	Beacon frame, SN=2419, FN=0, 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@2(
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@2(
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

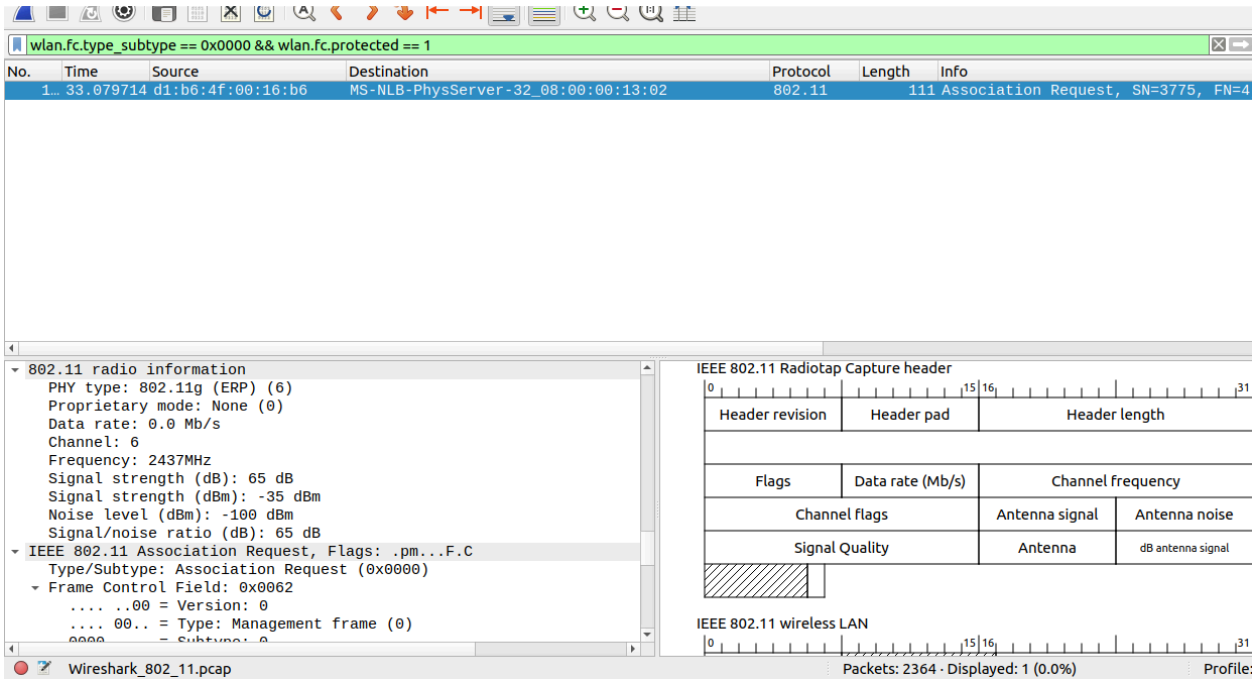


Minimum size of MAC frame for which CTS is 70B and RTS is 76B




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:
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]

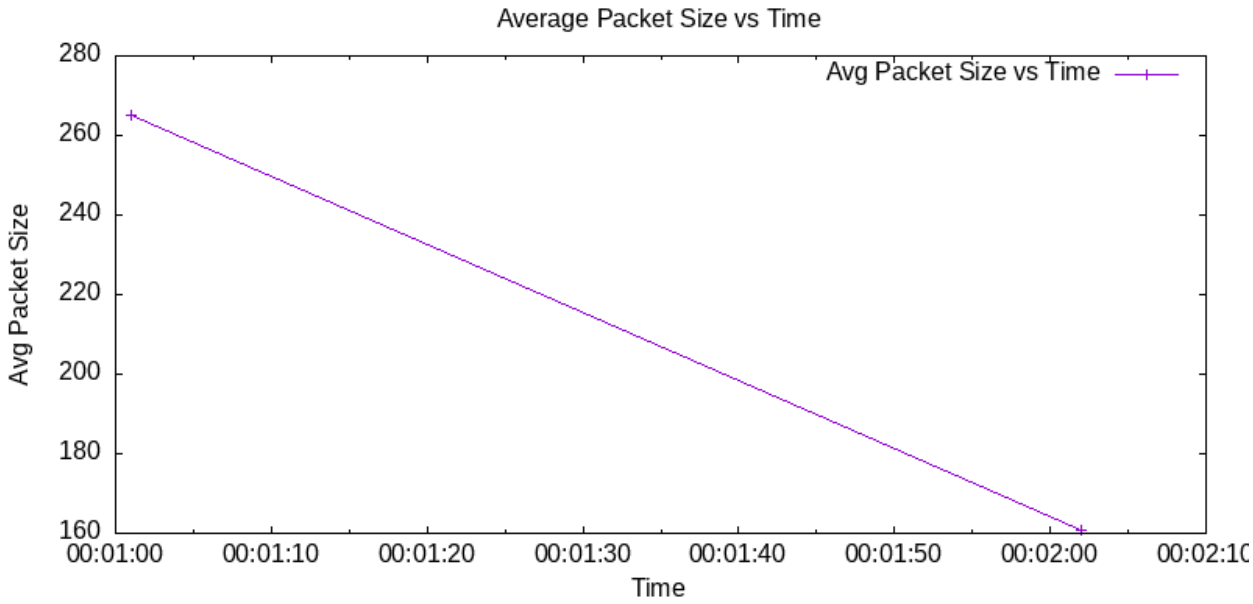
Q1b3
Ans: 1 out of 2364 MAC frames is encrypted in trace 1



There were no encrypted frame in trace 2

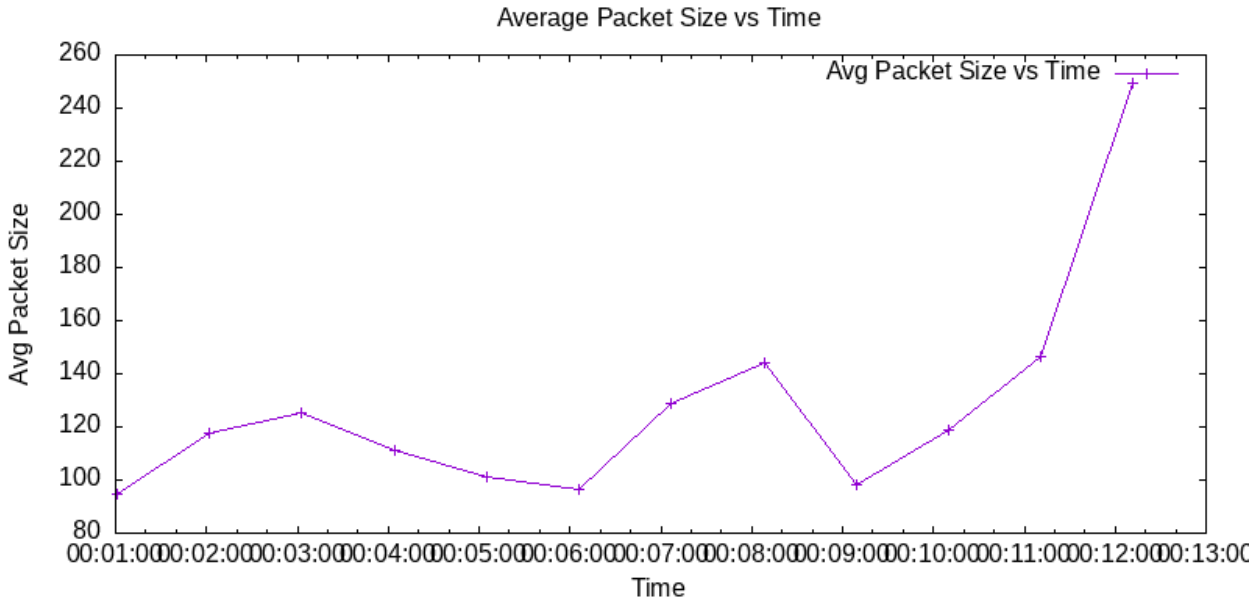
Q1c
Ans:
1. Avg packet size vs Time

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

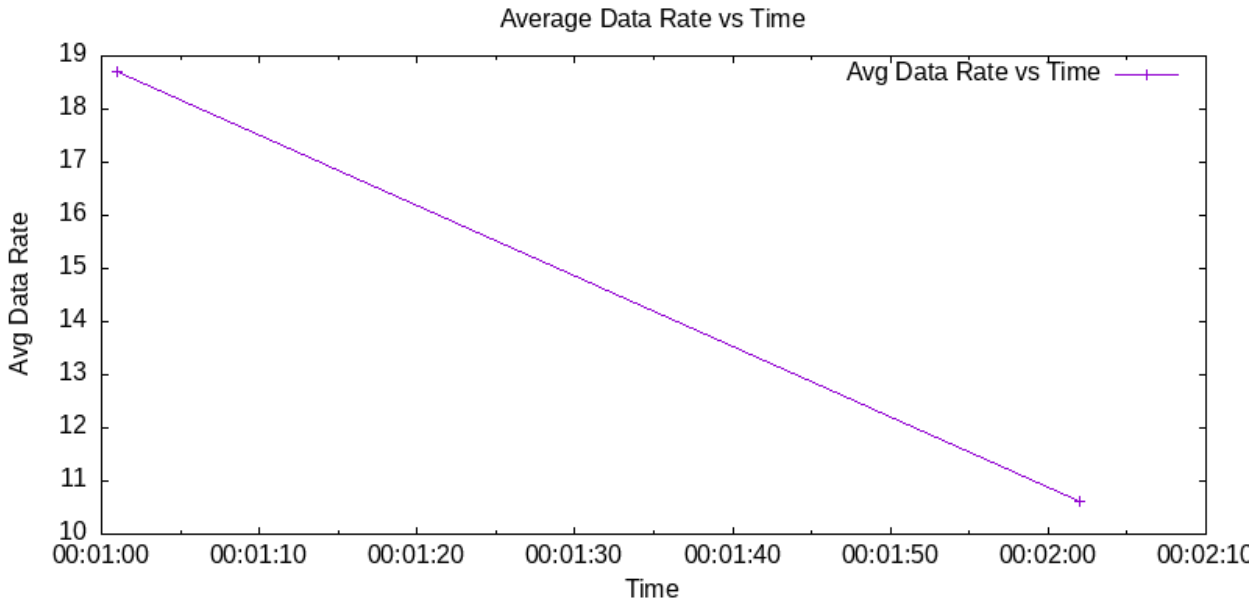
Trace2:
abhi@laptop:~$ ./packet_size_time.sh
/home/abhi/Downloads/wireshark-traces/cs23mtech11021_802_11.pcap
Successfull!
abhi@laptop:~$



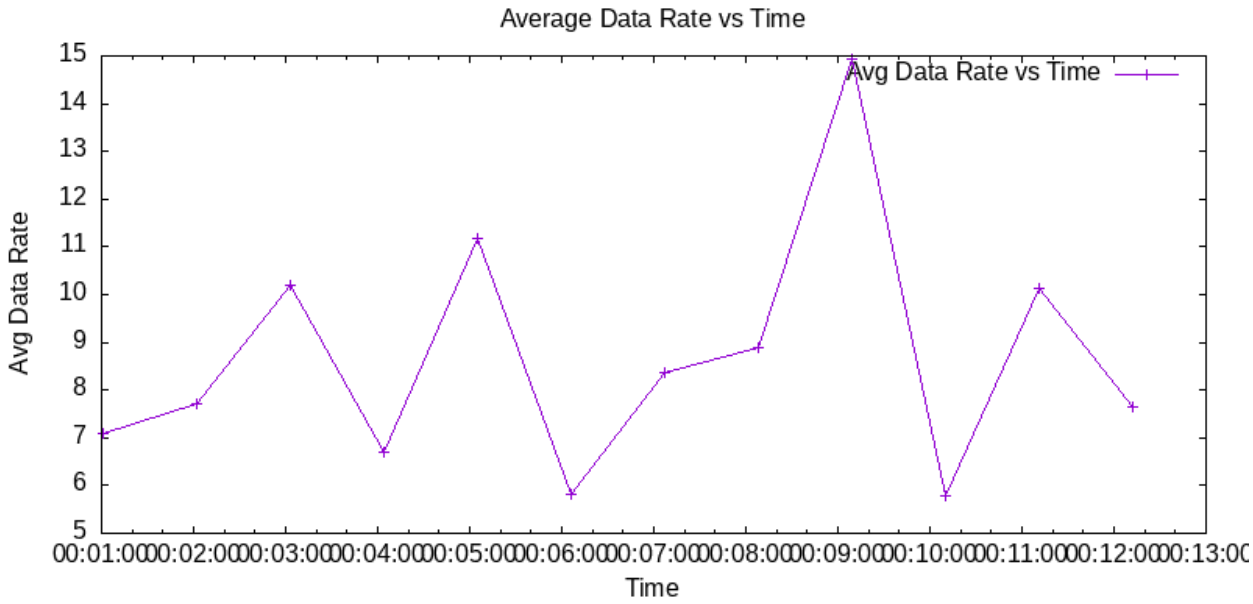
We can see that average packet size was almost same till 10min.

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:~$

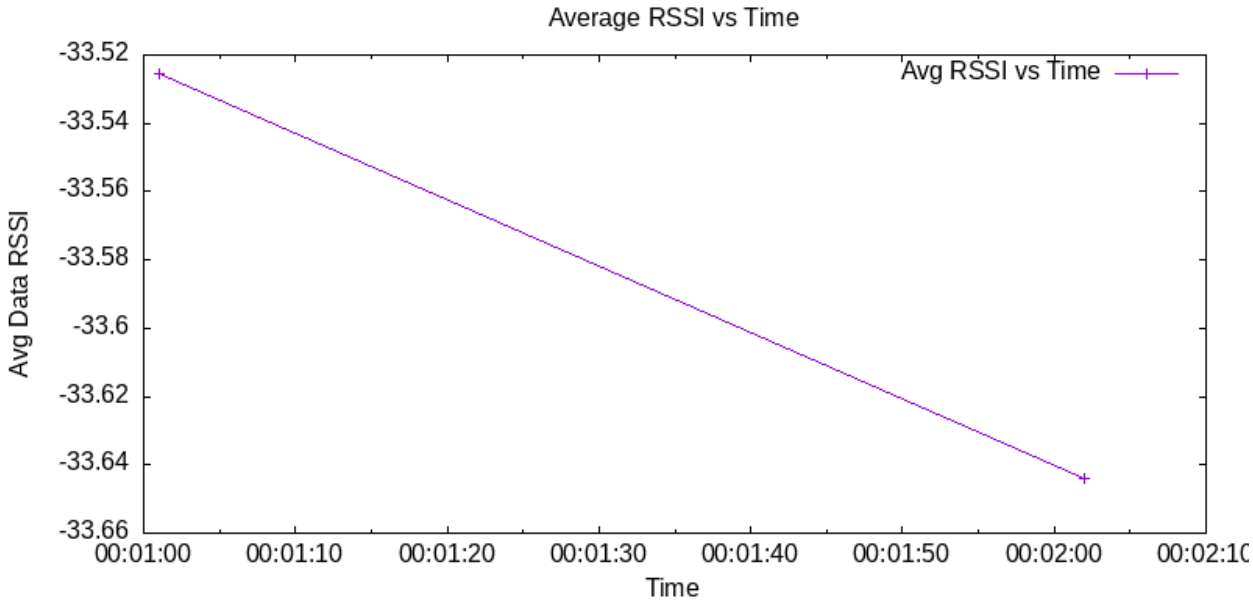


Trace 2:
abhi@laptop:~$ ./avg_data_rate_time.sh
/home/abhi/Downloads/wireshark-traces/cs23mtech11021_802_11.pcap
Successfull!
abhi@laptop:~$

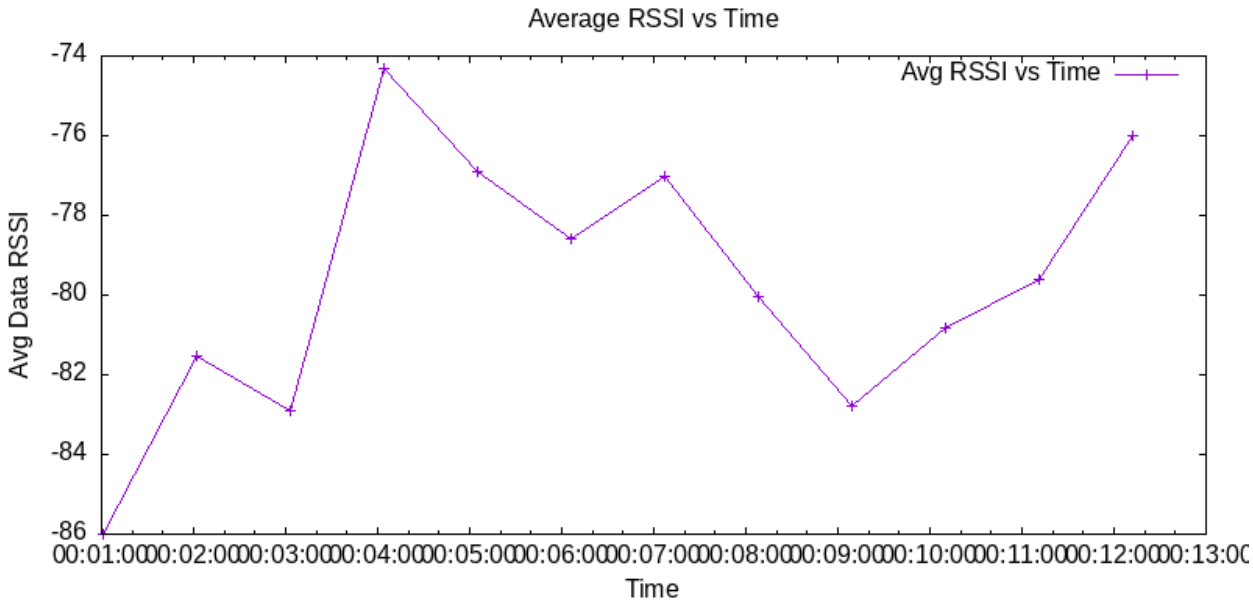


We can see that the average data remain almost same

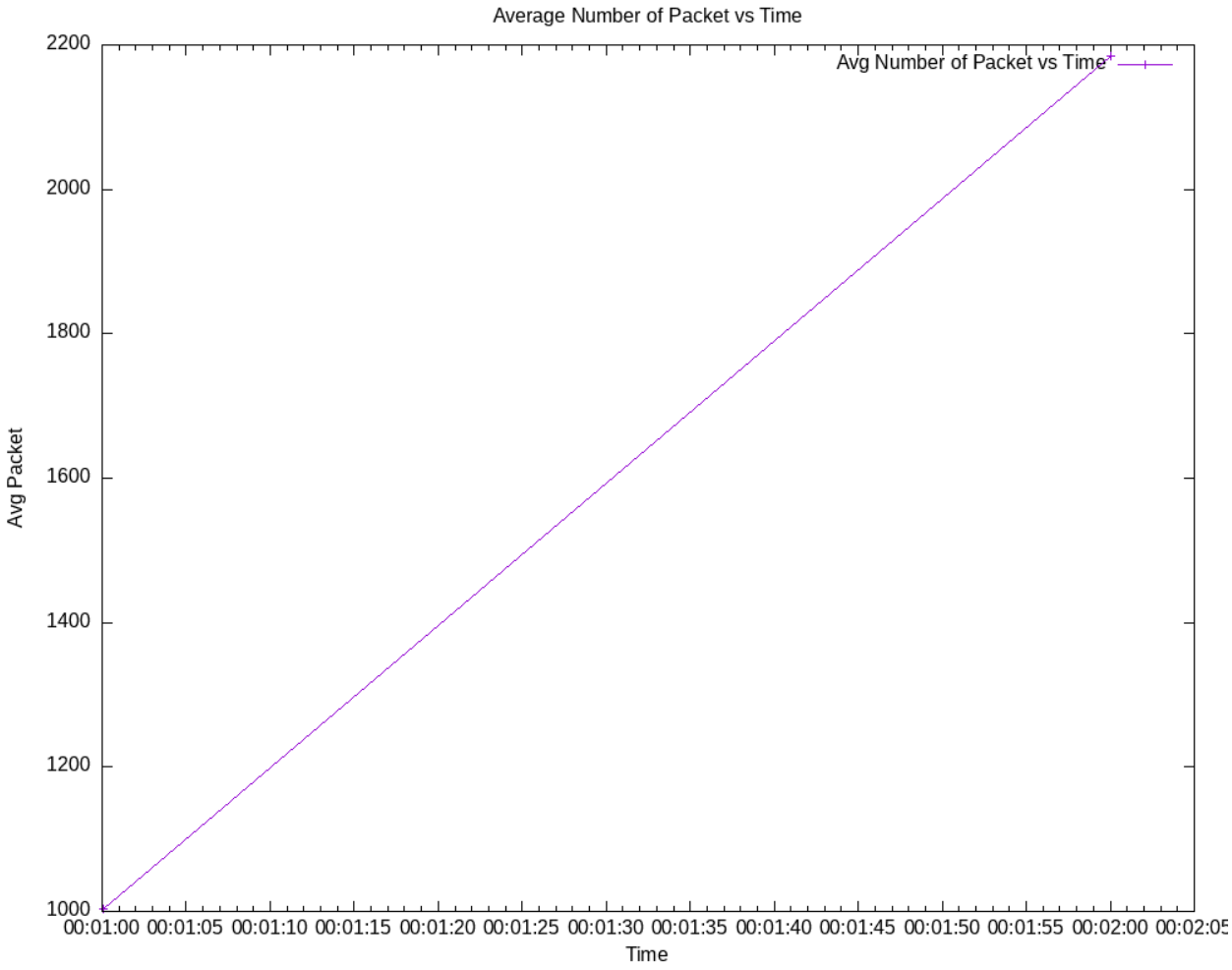
3.RSSI vs time
Command:
abhi@laptop:~$ ./avg_rssi_time.sh
/home/abhi/Downloads/wireshark-traces/Wireshark_802_11.pcap
Successfull!
abhi@laptop:~$



Trace 2:
abhi@laptop:~$ ./avg_rssi_time.sh
/home/abhi/Downloads/wireshark-traces/cs23mtech11021_802_11.pcap
Successfull!
abhi@laptop:~$

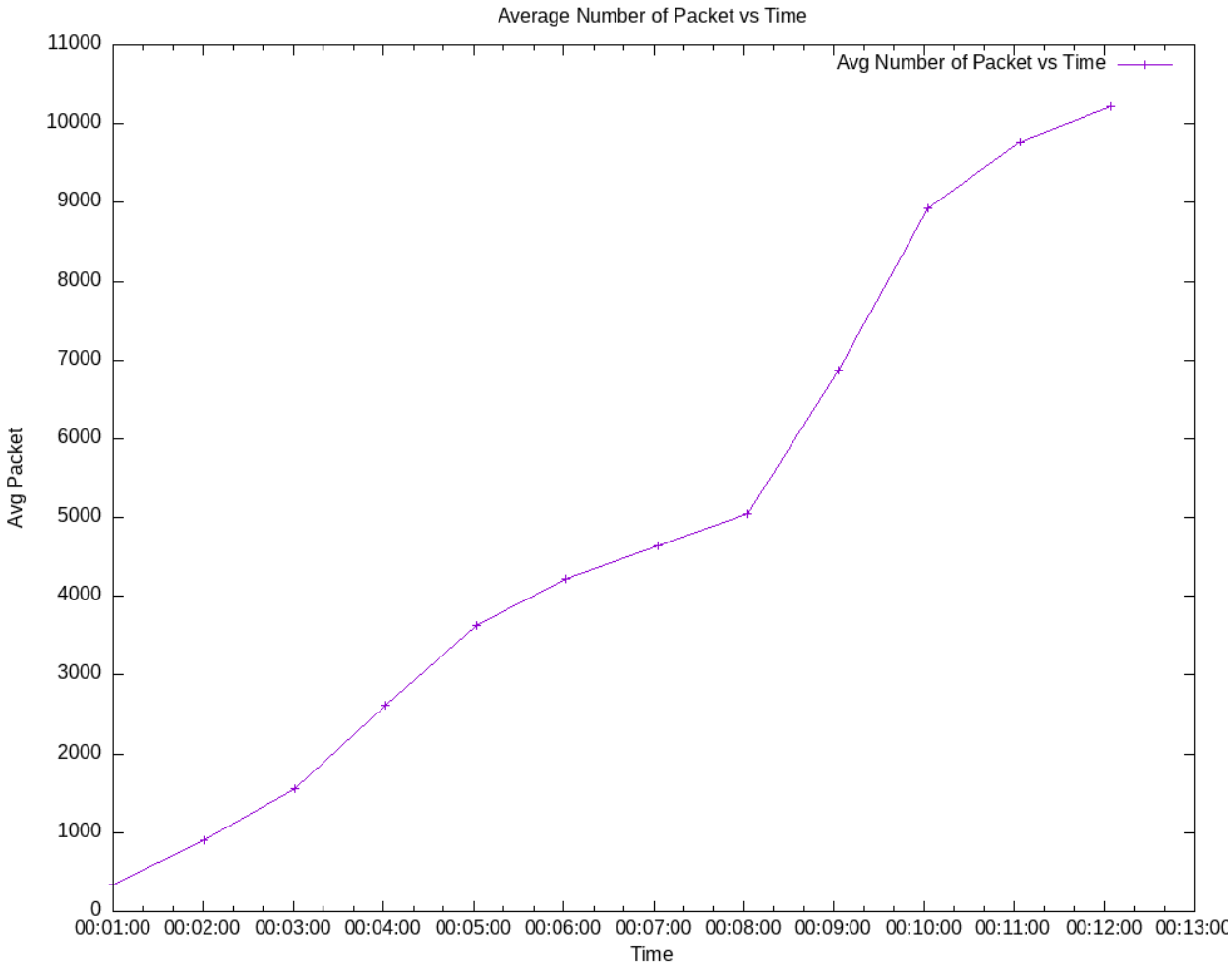


4:
Plot Packet rate (pkts/sec) vs Time
Command:
abhi@laptop:~$ chmod +x avg_packet_rate_time.sh
abhi@laptop:~$ ./avg_packet_rate_time.sh
/home/abhi/Downloads/wireshark-traces/Wireshark_802_11.pcap
Successful!
abhi@laptop:~$



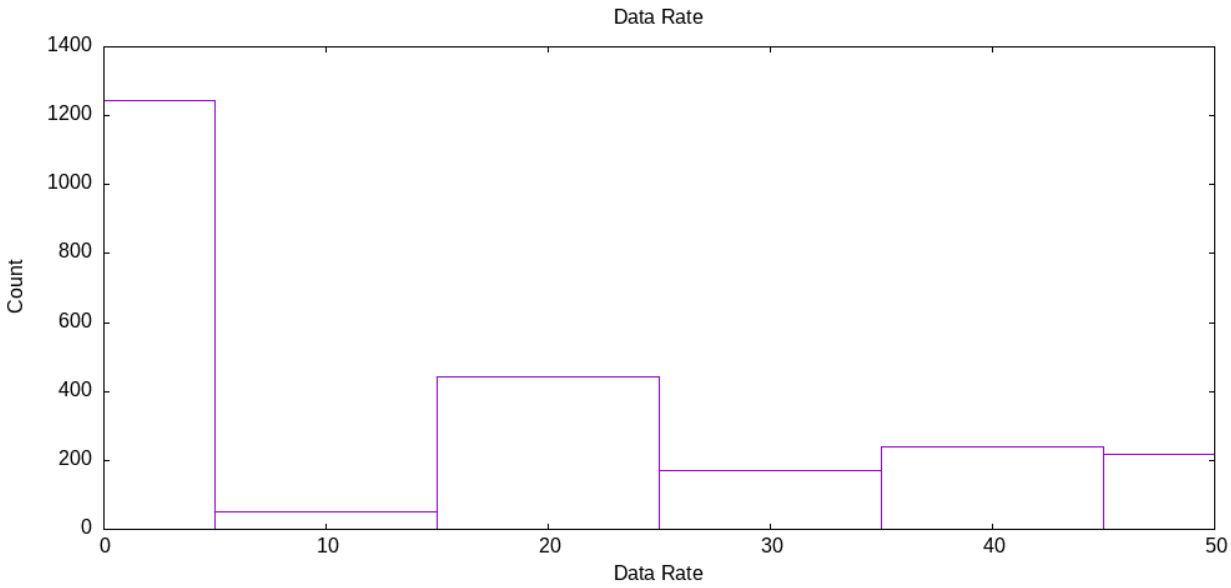
Trace 2

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

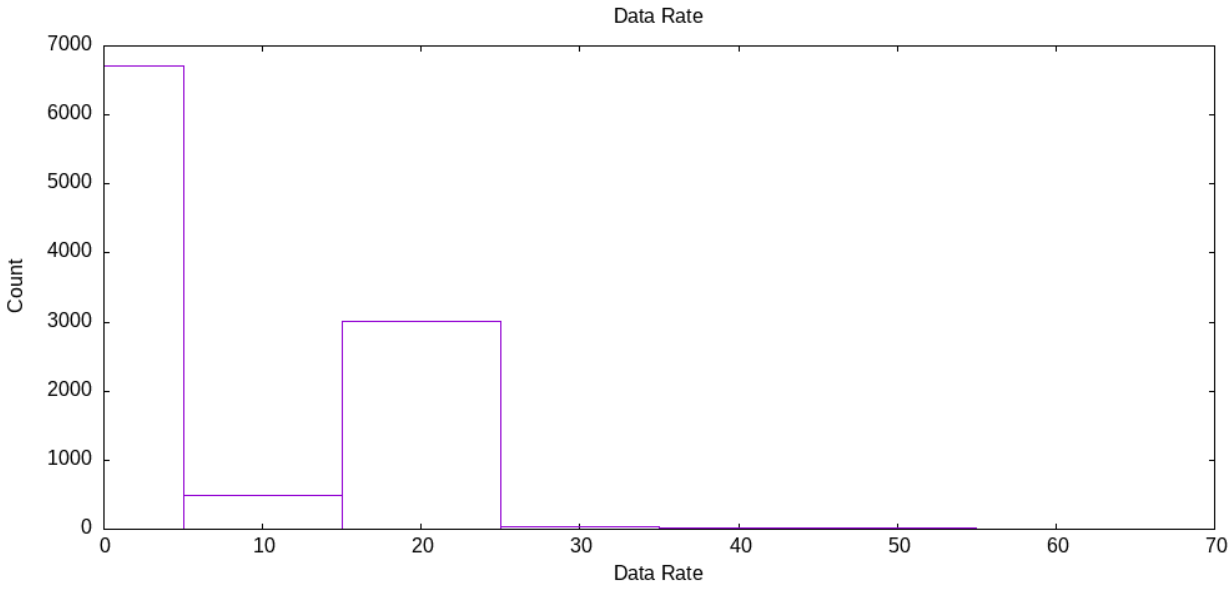


We can see that number of packets increased as the time increased

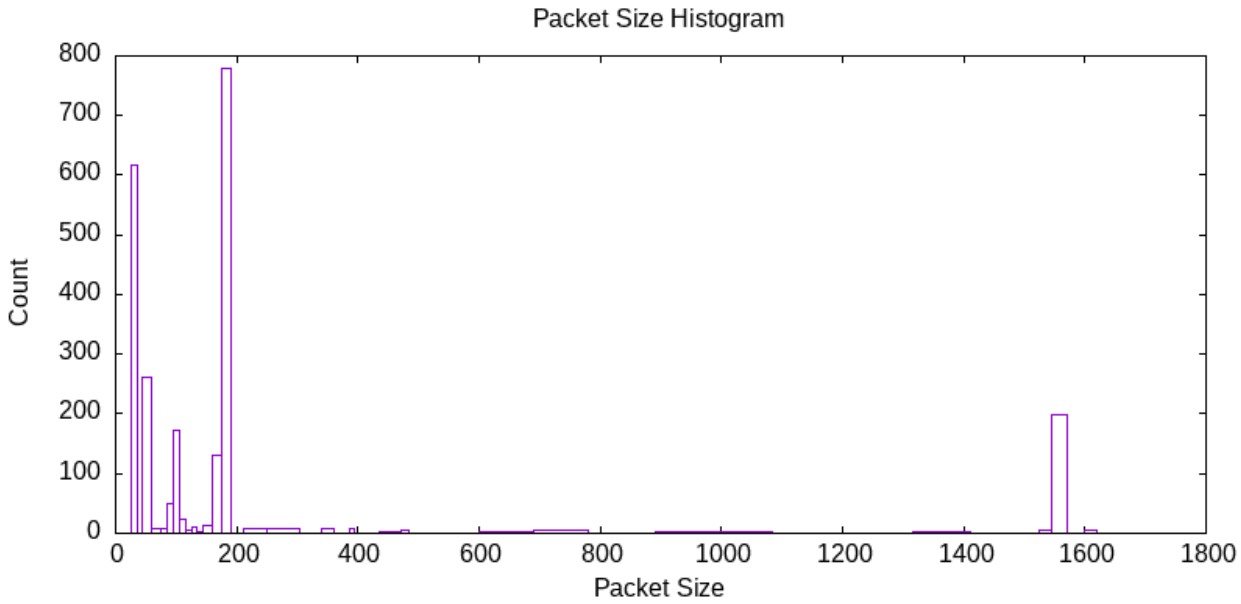
Q1 d:
Ans: Histogram of PHY data rate for trace 1
Command:
abhi@laptop:~$ chmod +x data_rate.sh
abhi@laptop:~$ ./data_rate.sh
/home/abhi/Downloads/wireshark-traces/Wireshark_802_11.pcap
Successful!



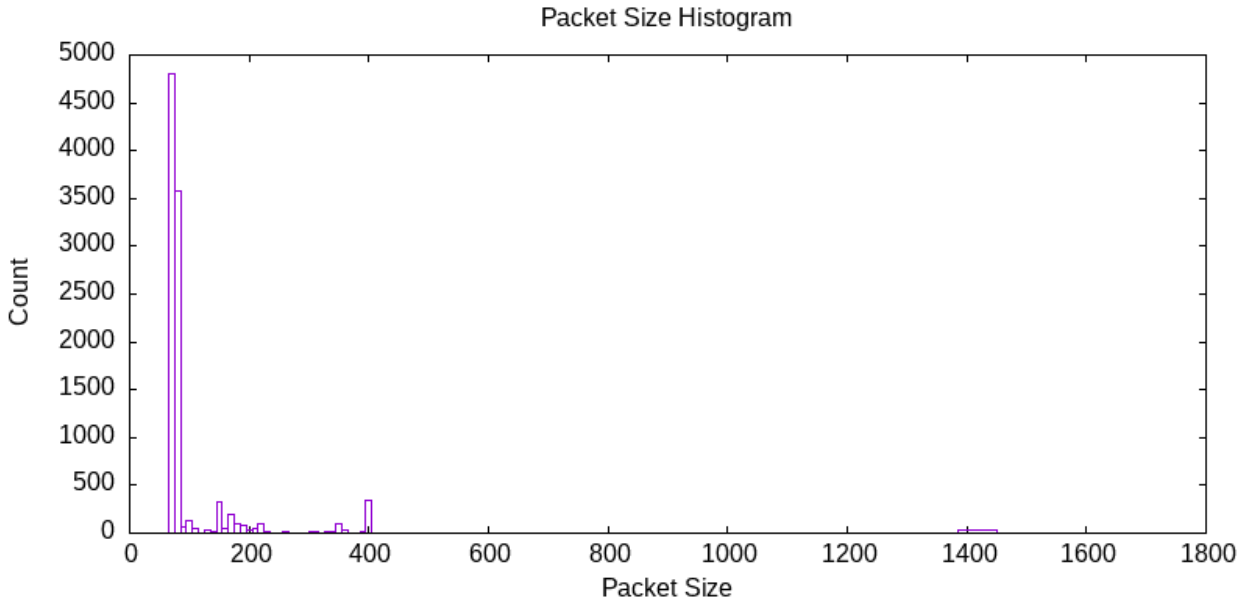
Trace 2



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!

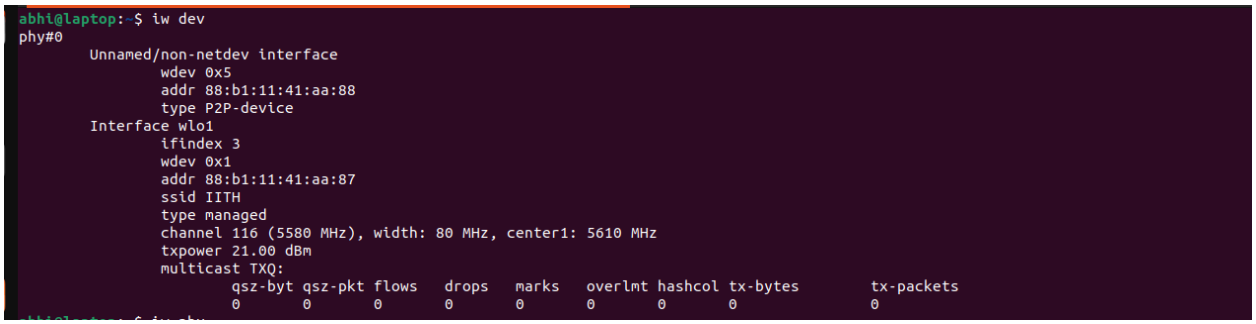


Q2:

B:
Ans:
Configuring Laptop as hotspot

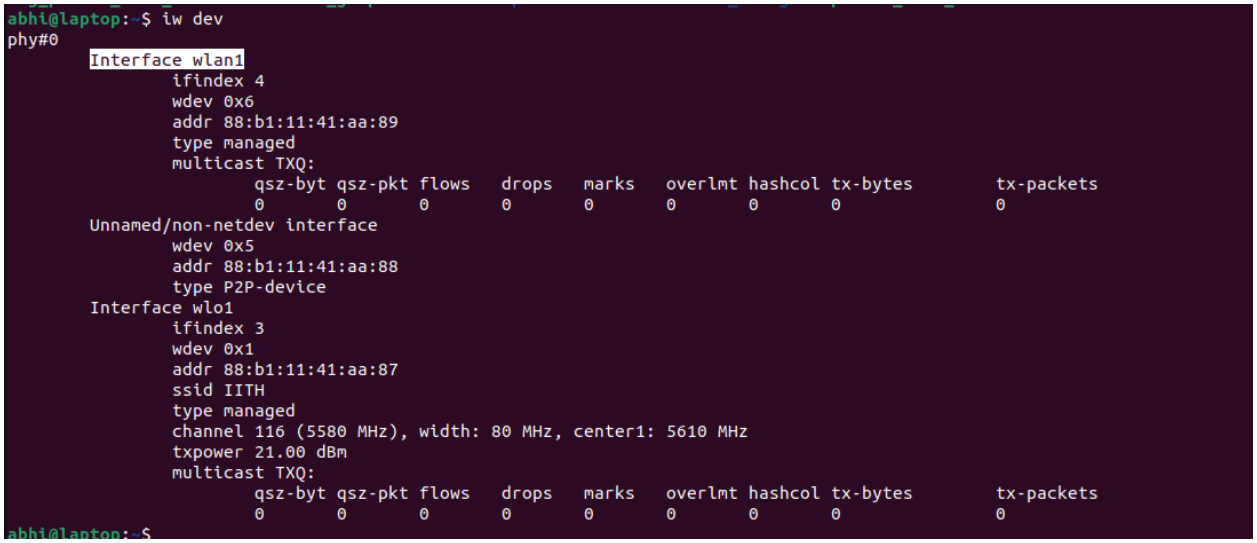
Step 1: Creating interface

Initial list of interfaces



Execute below command to create interface

sudo iw dev wlo1 interface add wlan1 type __ap



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

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

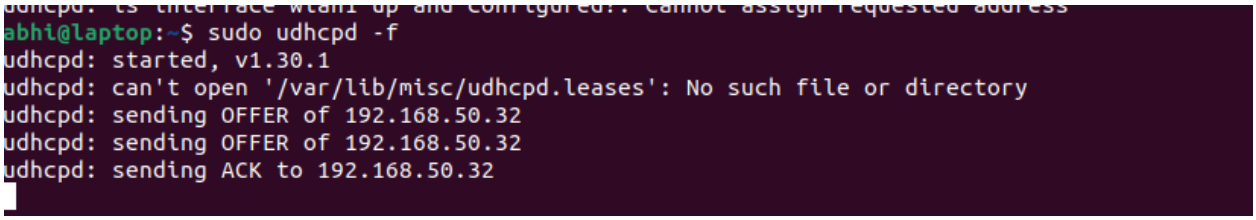
The interface that udhcpd will use

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



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 wl01 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