ASSIGNMENT 7
Wireshark for Wireless Networks

Submitted By,
SHRUSTI
CS22MTECH11017

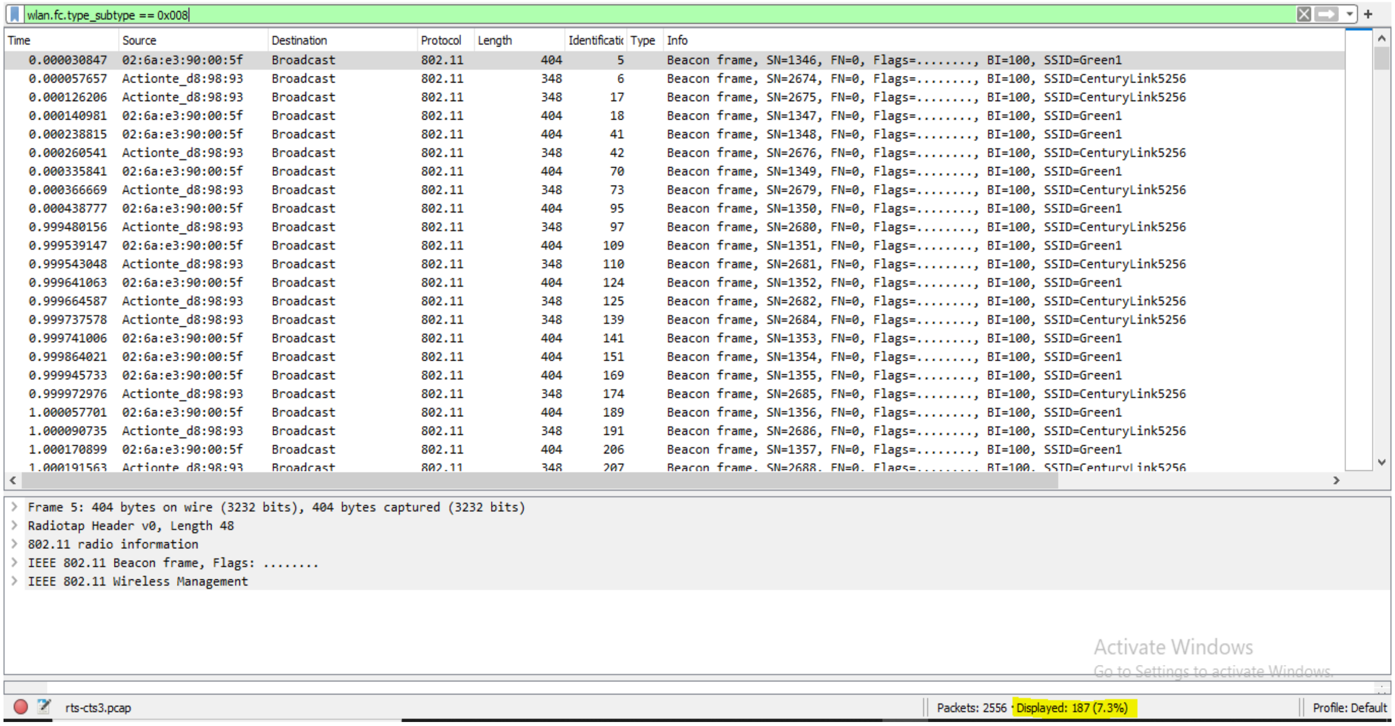
TASK1 : WIFI

1.

a. How many beacon frames are present, How do you find this?. List the SSIDs and the BSS IDs of all the access points that are issuing Beacon frames at various times.

Solution :

To observe the beacon frames captured use the filter “**wlan.fc.type_subtype == 0x8**”. We are comparing it to 0x8 because beacons are included in management frames that have the type field set to 0, and beacons are represented by the hex value 0x8, meaning that their sub-type is 8.



wlan.fc.type_subtype == 0x008

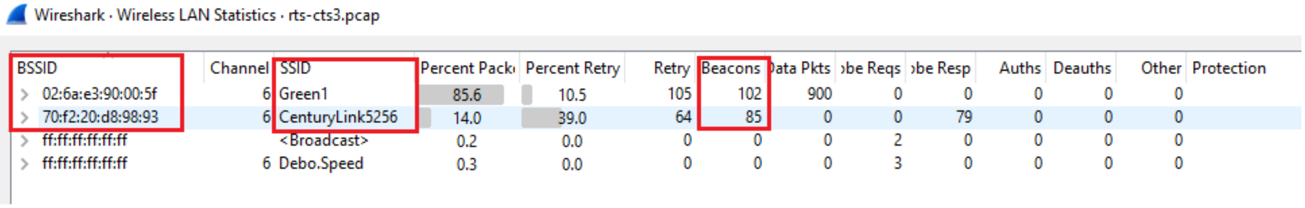
Time	Source	Destination	Protocol	Length	Identificatic	Type	Info
0.000030847	02:6a:e3:90:00:5f	Broadcast	802.11	404	5		Beacon frame, SN=1346, FN=0, Flags=........, BI=100, SSID=Green1
0.000057657	Actionte_d8:98:93	Broadcast	802.11	348	6		Beacon frame, SN=2674, FN=0, Flags=........, BI=100, SSID=CenturyLink5256
0.000126206	Actionte_d8:98:93	Broadcast	802.11	348	17		Beacon frame, SN=2675, FN=0, Flags=........, BI=100, SSID=CenturyLink5256
0.000140981	02:6a:e3:90:00:5f	Broadcast	802.11	404	18		Beacon frame, SN=1347, FN=0, Flags=........, BI=100, SSID=Green1
0.000238815	02:6a:e3:90:00:5f	Broadcast	802.11	404	41		Beacon frame, SN=1348, FN=0, Flags=........, BI=100, SSID=Green1
0.000260541	Actionte_d8:98:93	Broadcast	802.11	348	42		Beacon frame, SN=2676, FN=0, Flags=........, BI=100, SSID=CenturyLink5256
0.000335841	02:6a:e3:90:00:5f	Broadcast	802.11	404	70		Beacon frame, SN=1349, FN=0, Flags=........, BI=100, SSID=Green1
0.000366669	Actionte_d8:98:93	Broadcast	802.11	348	73		Beacon frame, SN=2679, FN=0, Flags=........, BI=100, SSID=CenturyLink5256
0.000438777	02:6a:e3:90:00:5f	Broadcast	802.11	404	95		Beacon frame, SN=1350, FN=0, Flags=........, BI=100, SSID=Green1
0.999480156	Actionte_d8:98:93	Broadcast	802.11	348	97		Beacon frame, SN=2680, FN=0, Flags=........, BI=100, SSID=CenturyLink5256
0.999539147	02:6a:e3:90:00:5f	Broadcast	802.11	404	109		Beacon frame, SN=1351, FN=0, Flags=........, BI=100, SSID=Green1
0.999543048	Actionte_d8:98:93	Broadcast	802.11	348	110		Beacon frame, SN=2681, FN=0, Flags=........, BI=100, SSID=CenturyLink5256
0.999641063	02:6a:e3:90:00:5f	Broadcast	802.11	404	124		Beacon frame, SN=1352, FN=0, Flags=........, BI=100, SSID=Green1
0.999664587	Actionte_d8:98:93	Broadcast	802.11	348	125		Beacon frame, SN=2682, FN=0, Flags=........, BI=100, SSID=CenturyLink5256
0.999737578	Actionte_d8:98:93	Broadcast	802.11	348	139		Beacon frame, SN=2684, FN=0, Flags=........, BI=100, SSID=CenturyLink5256
0.999741006	02:6a:e3:90:00:5f	Broadcast	802.11	404	141		Beacon frame, SN=1353, FN=0, Flags=........, BI=100, SSID=Green1
0.999864021	02:6a:e3:90:00:5f	Broadcast	802.11	404	151		Beacon frame, SN=1354, FN=0, Flags=........, BI=100, SSID=Green1
0.999945733	02:6a:e3:90:00:5f	Broadcast	802.11	404	169		Beacon frame, SN=1355, FN=0, Flags=........, BI=100, SSID=Green1
0.999972976	Actionte_d8:98:93	Broadcast	802.11	348	174		Beacon frame, SN=2685, FN=0, Flags=........, BI=100, SSID=CenturyLink5256
1.000057701	02:6a:e3:90:00:5f	Broadcast	802.11	404	189		Beacon frame, SN=1356, FN=0, Flags=........, BI=100, SSID=Green1
1.000090735	Actionte_d8:98:93	Broadcast	802.11	348	191		Beacon frame, SN=2686, FN=0, Flags=........, BI=100, SSID=CenturyLink5256
1.000170899	02:6a:e3:90:00:5f	Broadcast	802.11	404	206		Beacon frame, SN=1357, FN=0, Flags=........, BI=100, SSID=Green1
1.000191563	Actionte_d8:98:93	Broadcast	802.11	348	207		Beacon frame, SN=2688, FN=0, Flags=........, BI=100, SSID=CenturyLink5256

```
> Frame 5: 404 bytes on wire (3232 bits), 404 bytes captured (3232 bits)
> Radiotap Header v0, Length 48
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ........
> IEEE 802.11 Wireless Management
```

rts-cts3.pcap | Packets: 2556 · Displayed: 187 (7.3%) | Profile: Default

As we can see, a total of **187 beacon frames** are present.

This can also be seen under Wireless → WLAN Traffic.



Wireshark · Wireless LAN Statistics · rts-cts3.pcap

BSSID	Channel	SSID	Percent Pack	Percent Retry	Retry	Beacons	Data Pkts	obe Reqs	obe Resp	Auths	Deauths	Other	Protection
02:6a:e3:90:00:5f	6	Green1	85.6	10.5	105	102	900	0	0	0	0	0	
70:f2:20:d8:98:93	6	CenturyLink5256	14.0	39.0	64	85	0	0	79	0	0	0	
ff:ff:ff:ff:ff:ff		<Broadcast>	0.2	0.0	0	0	0	2	0	0	0	0	
ff:ff:ff:ff:ff:ff	6	Debo.Speed	0.3	0.0	0	0	0	3	0	0	0	0	

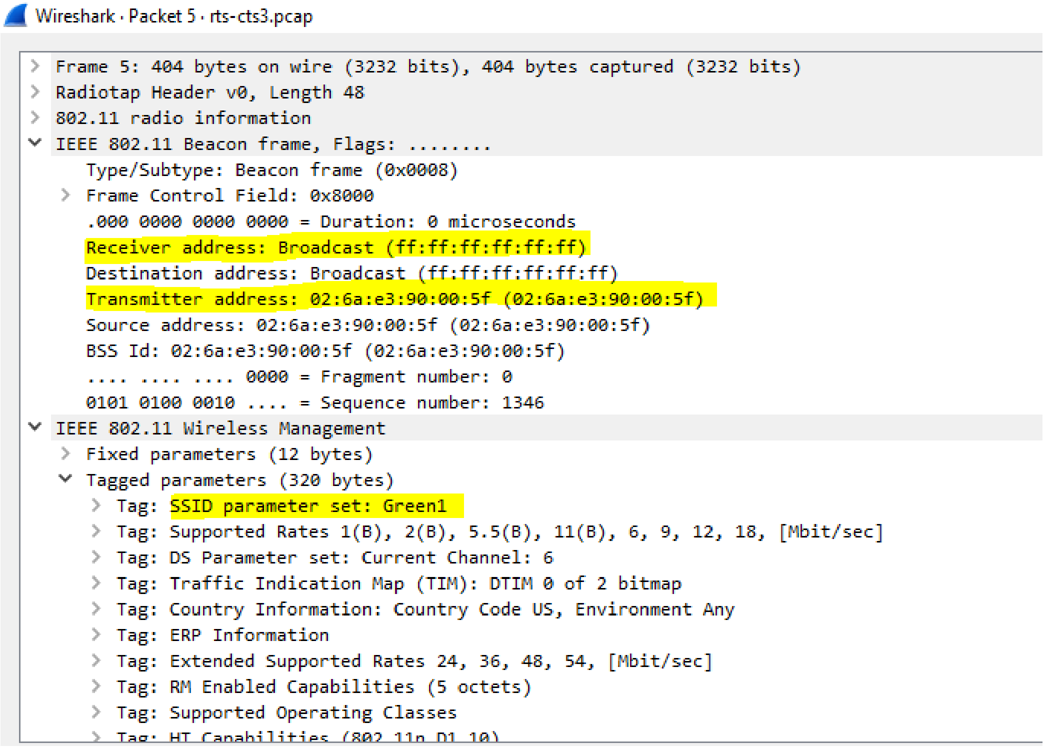
The SSID and BSS ID of different access points are as follows:

SSID	BSS ID
Green1	02:6a:e3:90:00:5f
CenturyLink5256	70:f2:20:d8:98:93

b. Prepare a table showing one of the beacon frames from each of the different SSIDs visible in the trace, Receiver address, and Transmitter address. Comment about your understanding of these fields in the beacon frame. Are all addresses as per the 802.11 frame structure present here? If yes, why? If not, why?
Solution :

SSID	RECEIVER ADDRESS	TRANSMITTER ADDRESS
Green1	Broadcast (ff:ff:ff:ff:ff:ff)	02:6a:e3:90:00:5f (02:6a:e3:90:00:5f)
CenturyLink5256	Broadcast (ff:ff:ff:ff:ff:ff)	Actionate_d8:98:93 (70:f2:20:d8:98:93)

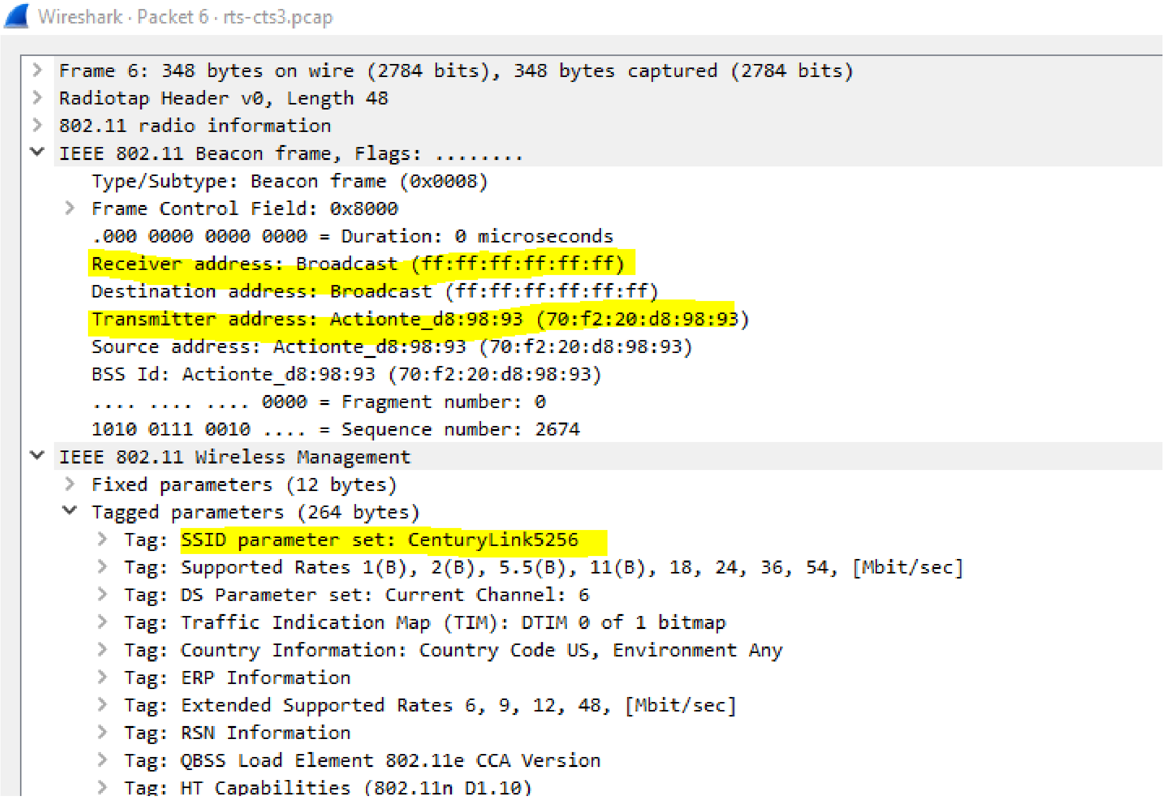
Below screenshot shows the Receiver Address and Transmitter Address of SSID **"Green1".**



Wireshark · Packet 5 · rts-cts3.pcap

```
> Frame 5: 404 bytes on wire (3232 bits), 404 bytes captured (3232 bits)
> Radiotap Header v0, Length 48
> 802.11 radio information
v IEEE 802.11 Beacon frame, Flags: ........
    Type/Subtype: Beacon frame (0x0008)
  > Frame Control Field: 0x8000
    .000 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: 02:6a:e3:90:00:5f (02:6a:e3:90:00:5f)
    Source address: 02:6a:e3:90:00:5f (02:6a:e3:90:00:5f)
    BSS Id: 02:6a:e3:90:00:5f (02:6a:e3:90:00:5f)
    .... .... .... 0000 = Fragment number: 0
    0101 0100 0010 .... = Sequence number: 1346
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (320 bytes)
    > Tag: SSID parameter set: Green1
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 6
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 2 bitmap
    > Tag: Country Information: Country Code US, Environment Any
    > Tag: ERP Information
    > Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    > Tag: RM Enabled Capabilities (5 octets)
    > Tag: Supported Operating Classes
    > Tag: HT Capabilities (802.11n D1.10)
```

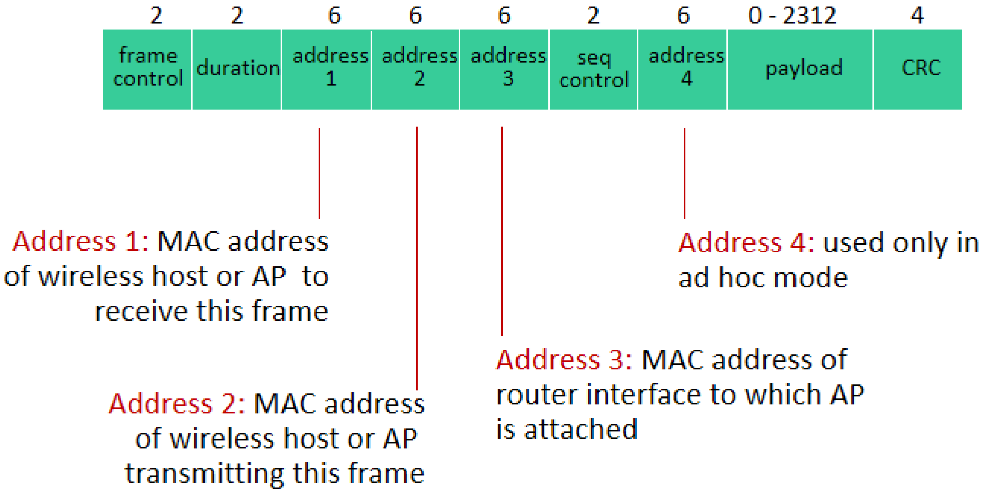
Below screenshot shows the Receiver Address and Transmitter Address of SSID “**CenturyLink5256**”.

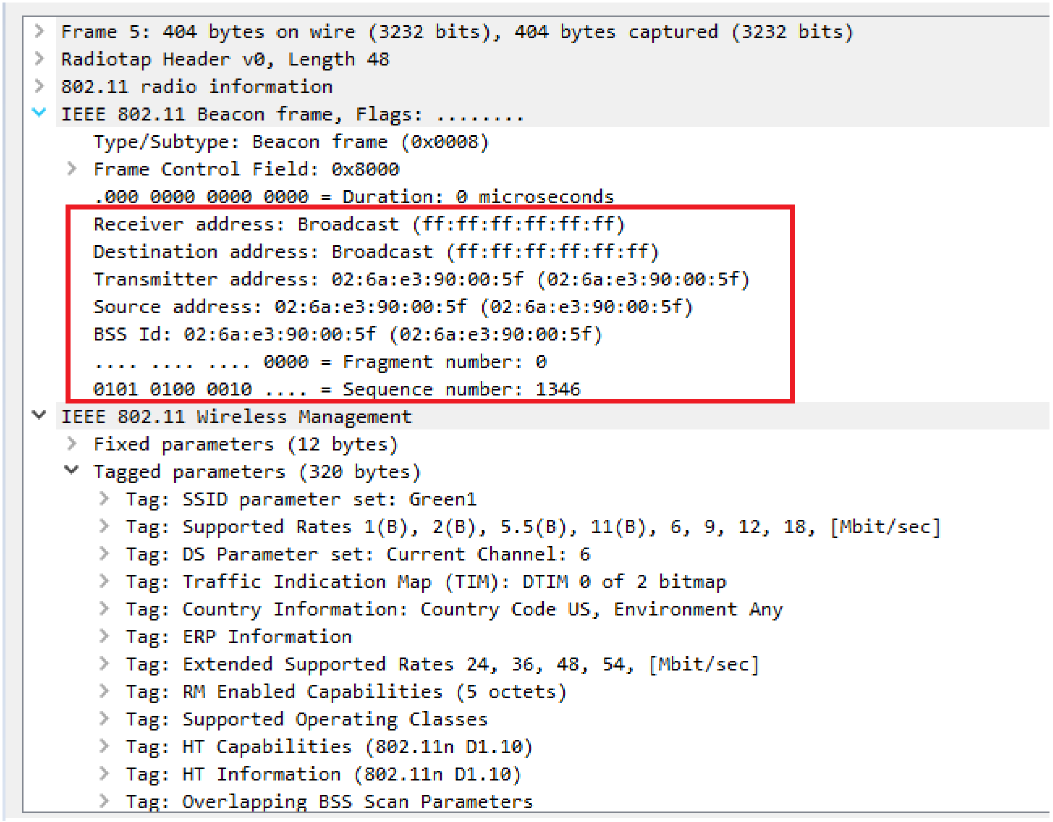


Wireshark · Packet 6 · rts-cts3.pcap

```
> Frame 6: 348 bytes on wire (2784 bits), 348 bytes captured (2784 bits)
> Radiotap Header v0, Length 48
> 802.11 radio information
v IEEE 802.11 Beacon frame, Flags: ........
    Type/Subtype: Beacon frame (0x0008)
  > Frame Control Field: 0x8000
    .000 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: Actionte_d8:98:93 (70:f2:20:d8:98:93)
    Source address: Actionte_d8:98:93 (70:f2:20:d8:98:93)
    BSS Id: Actionte_d8:98:93 (70:f2:20:d8:98:93)
    .... .... .... 0000 = Fragment number: 0
    1010 0111 0010 .... = Sequence number: 2674
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (264 bytes)
    > Tag: SSID parameter set: CenturyLink5256
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 6
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
    > Tag: Country Information: Country Code US, Environment Any
    > Tag: ERP Information
    > Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
    > Tag: RSN Information
    > Tag: QBSS Load Element 802.11e CCA Version
    > Tag: HT Capabilities (802.11n D1.10)
```

As we know 802.11 frame structure is as shown below


2
2
6
6
6
2
6
0 - 2312
4
frame control
duration
address 1
address 2
address 3
seq control
address 4
payload
CRC
Address 1: MAC address of wireless host or AP to receive this frame
Address 2: MAC address of wireless host or AP transmitting this frame
Address 3: MAC address of router interface to which AP is attached
Address 4: used only in ad hoc mode



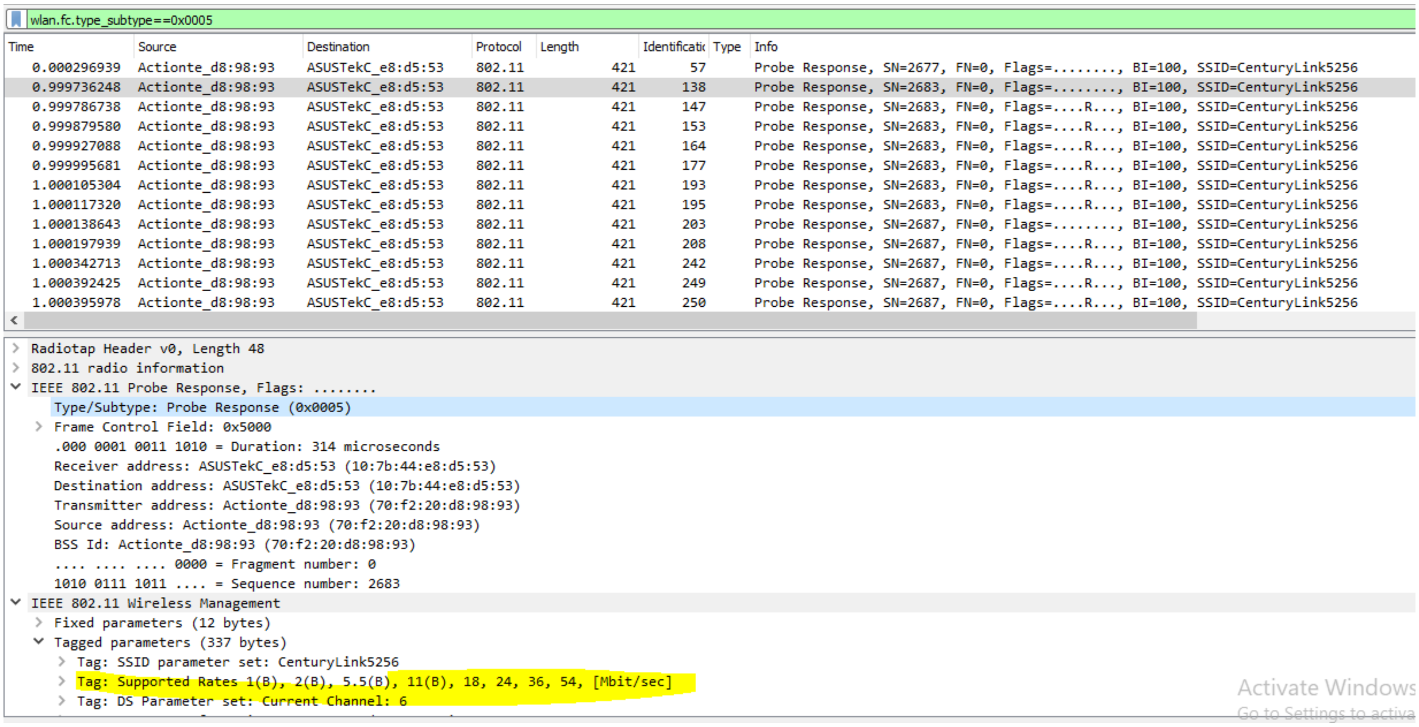
```
> Frame 5: 404 bytes on wire (3232 bits), 404 bytes captured (3232 bits)
> Radiotap Header v0, Length 48
> 802.11 radio information
v IEEE 802.11 Beacon frame, Flags: ........
     Type/Subtype: Beacon frame (0x0008)
   > Frame Control Field: 0x8000
     .000 0000 0000 0000 = Duration: 0 microseconds
     Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
     Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
     Transmitter address: 02:6a:e3:90:00:5f (02:6a:e3:90:00:5f)
     Source address: 02:6a:e3:90:00:5f (02:6a:e3:90:00:5f)
     BSS Id: 02:6a:e3:90:00:5f (02:6a:e3:90:00:5f)
     .... .... .... 0000 = Fragment number: 0
     0101 0100 0010 .... = Sequence number: 1346
v IEEE 802.11 Wireless Management
   > Fixed parameters (12 bytes)
   v Tagged parameters (320 bytes)
      > Tag: SSID parameter set: Green1
      > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
      > Tag: DS Parameter set: Current Channel: 6
      > Tag: Traffic Indication Map (TIM): DTIM 0 of 2 bitmap
      > Tag: Country Information: Country Code US, Environment Any
      > Tag: ERP Information
      > Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
      > Tag: RM Enabled Capabilities (5 octets)
      > Tag: Supported Operating Classes
      > Tag: HT Capabilities (802.11n D1.10)
      > Tag: HT Information (802.11n D1.10)
      > Tag: Overlapping BSS Scan Parameters
```

It has the **Receiver Address, Source Address, and BSS Id,** as we can see, but not Address 4 as it is only used in adhoc mode.

c. Pick any SSID of your choice. What are the data rates supported by this SSID?

How do you know this from the trace?
Solution :

Let us pick the SSID “ **CenturyLink5256** ”. The data rates supported by this SSID is as shown below.



wlan.fc.type_subtype==0x0005

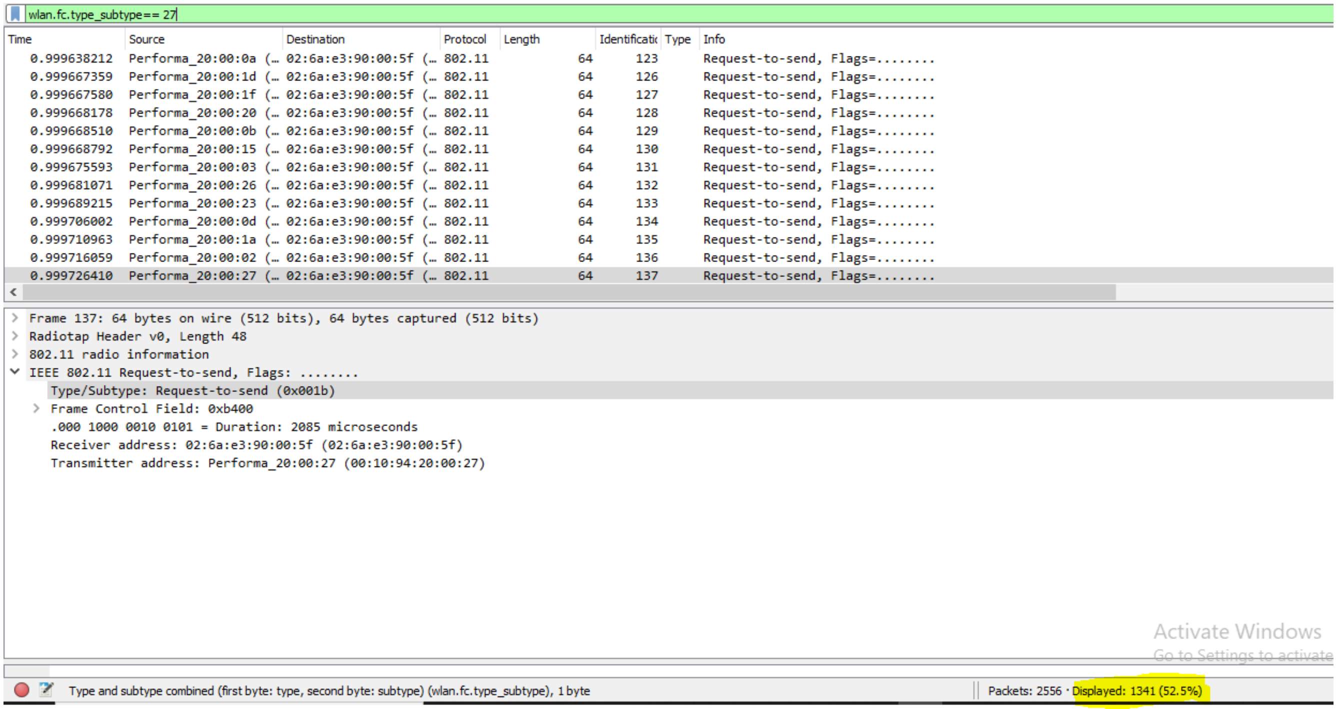
Time	Source	Destination	Protocol	Length	Identificatic	Type	Info
0.000296939	Actionte_d8:98:93	ASUSTekC_e8:d5:53	802.11	421	57		Probe Response, SN=2677, FN=0, Flags=........, BI=100, SSID=CenturyLink5256
0.999736248	Actionte_d8:98:93	ASUSTekC_e8:d5:53	802.11	421	138		Probe Response, SN=2683, FN=0, Flags=........, BI=100, SSID=CenturyLink5256
0.999786738	Actionte_d8:98:93	ASUSTekC_e8:d5:53	802.11	421	147		Probe Response, SN=2683, FN=0, Flags=....R..., BI=100, SSID=CenturyLink5256
0.999879580	Actionte_d8:98:93	ASUSTekC_e8:d5:53	802.11	421	153		Probe Response, SN=2683, FN=0, Flags=....R..., BI=100, SSID=CenturyLink5256
0.999927088	Actionte_d8:98:93	ASUSTekC_e8:d5:53	802.11	421	164		Probe Response, SN=2683, FN=0, Flags=....R..., BI=100, SSID=CenturyLink5256
0.999995681	Actionte_d8:98:93	ASUSTekC_e8:d5:53	802.11	421	177		Probe Response, SN=2683, FN=0, Flags=....R..., BI=100, SSID=CenturyLink5256
1.000105304	Actionte_d8:98:93	ASUSTekC_e8:d5:53	802.11	421	193		Probe Response, SN=2683, FN=0, Flags=....R..., BI=100, SSID=CenturyLink5256
1.000117320	Actionte_d8:98:93	ASUSTekC_e8:d5:53	802.11	421	195		Probe Response, SN=2683, FN=0, Flags=....R..., BI=100, SSID=CenturyLink5256
1.000138643	Actionte_d8:98:93	ASUSTekC_e8:d5:53	802.11	421	203		Probe Response, SN=2687, FN=0, Flags=........, BI=100, SSID=CenturyLink5256
1.000197939	Actionte_d8:98:93	ASUSTekC_e8:d5:53	802.11	421	208		Probe Response, SN=2687, FN=0, Flags=....R..., BI=100, SSID=CenturyLink5256
1.000342713	Actionte_d8:98:93	ASUSTekC_e8:d5:53	802.11	421	242		Probe Response, SN=2687, FN=0, Flags=....R..., BI=100, SSID=CenturyLink5256
1.000392425	Actionte_d8:98:93	ASUSTekC_e8:d5:53	802.11	421	249		Probe Response, SN=2687, FN=0, Flags=....R..., BI=100, SSID=CenturyLink5256
1.000395978	Actionte_d8:98:93	ASUSTekC_e8:d5:53	802.11	421	250		Probe Response, SN=2687, FN=0, Flags=....R..., BI=100, SSID=CenturyLink5256

```
> Radiotap Header v0, Length 48
> 802.11 radio information
v IEEE 802.11 Probe Response, Flags: ........
    Type/Subtype: Probe Response (0x0005)
  > Frame Control Field: 0x5000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: ASUSTekC_e8:d5:53 (10:7b:44:e8:d5:53)
    Destination address: ASUSTekC_e8:d5:53 (10:7b:44:e8:d5:53)
    Transmitter address: Actionte_d8:98:93 (70:f2:20:d8:98:93)
    Source address: Actionte_d8:98:93 (70:f2:20:d8:98:93)
    BSS Id: Actionte_d8:98:93 (70:f2:20:d8:98:93)
    .... .... .... 0000 = Fragment number: 0
    1010 0111 1011 .... = Sequence number: 2683
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (337 bytes)
    > Tag: SSID parameter set: CenturyLink5256
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 6
```

2. How many RTS and CTS frames are present? How do you find this? Also, mention the size of these frames.
Solution:

RTS:

Apply the filter “**wlan.fc.type_subtype==27**” to observe the RTS frames.
As seen in the below screenshot the number of RTS frames present are **1341** and the size of each frame is **64 bytes.**



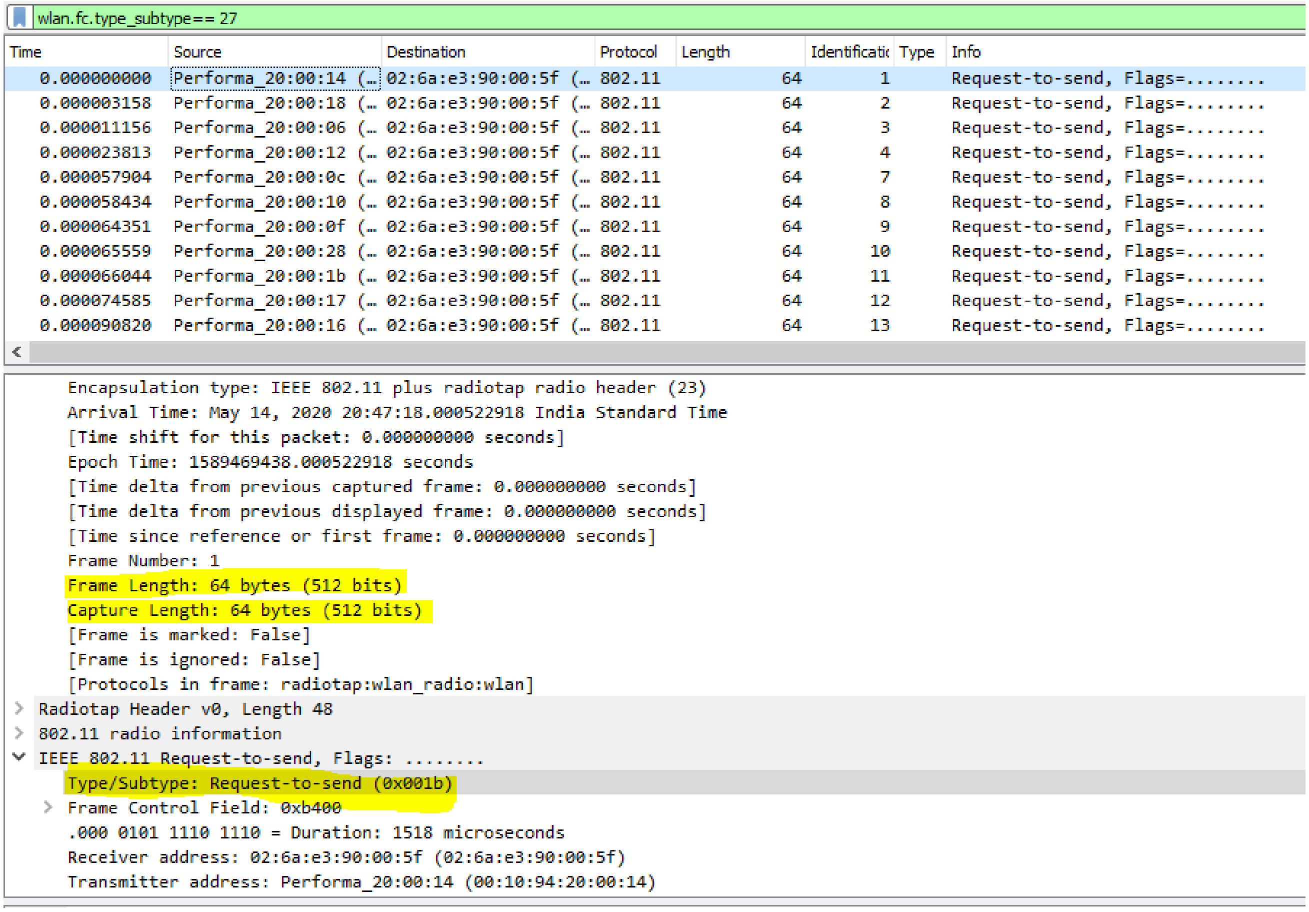
wlan.fc.type_subtype== 27

```
Time          Source                Destination            Protocol   Length   Identificati Type  Info
 0.999638212  Performa_20:00:0a (… 02:6a:e3:90:00:5f (… 802.11          64       123        Request-to-send, Flags=........
 0.999667359  Performa_20:00:1d (… 02:6a:e3:90:00:5f (… 802.11          64       126        Request-to-send, Flags=........
 0.999667580  Performa_20:00:1f (… 02:6a:e3:90:00:5f (… 802.11          64       127        Request-to-send, Flags=........
 0.999668178  Performa_20:00:20 (… 02:6a:e3:90:00:5f (… 802.11          64       128        Request-to-send, Flags=........
 0.999668510  Performa_20:00:0b (… 02:6a:e3:90:00:5f (… 802.11          64       129        Request-to-send, Flags=........
 0.999668792  Performa_20:00:15 (… 02:6a:e3:90:00:5f (… 802.11          64       130        Request-to-send, Flags=........
 0.999675593  Performa_20:00:03 (… 02:6a:e3:90:00:5f (… 802.11          64       131        Request-to-send, Flags=........
 0.999681071  Performa_20:00:26 (… 02:6a:e3:90:00:5f (… 802.11          64       132        Request-to-send, Flags=........
 0.999689215  Performa_20:00:23 (… 02:6a:e3:90:00:5f (… 802.11          64       133        Request-to-send, Flags=........
 0.999706002  Performa_20:00:0d (… 02:6a:e3:90:00:5f (… 802.11          64       134        Request-to-send, Flags=........
 0.999710963  Performa_20:00:1a (… 02:6a:e3:90:00:5f (… 802.11          64       135        Request-to-send, Flags=........
 0.999716059  Performa_20:00:02 (… 02:6a:e3:90:00:5f (… 802.11          64       136        Request-to-send, Flags=........
 0.999726410  Performa_20:00:27 (… 02:6a:e3:90:00:5f (… 802.11          64       137        Request-to-send, Flags=........
```

```
> Frame 137: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)
> Radiotap Header v0, Length 48
> 802.11 radio information
v IEEE 802.11 Request-to-send, Flags: ........
    Type/Subtype: Request-to-send (0x001b)
  > Frame Control Field: 0xb400
    .000 1000 0010 0101 = Duration: 2085 microseconds
    Receiver address: 02:6a:e3:90:00:5f (02:6a:e3:90:00:5f)
    Transmitter address: Performa_20:00:27 (00:10:94:20:00:27)
```

Type and subtype combined (first byte: type, second byte: subtype) (wlan.fc.type_subtype), 1 byte

Packets: 2556 · Displayed: 1341 (52.5%)



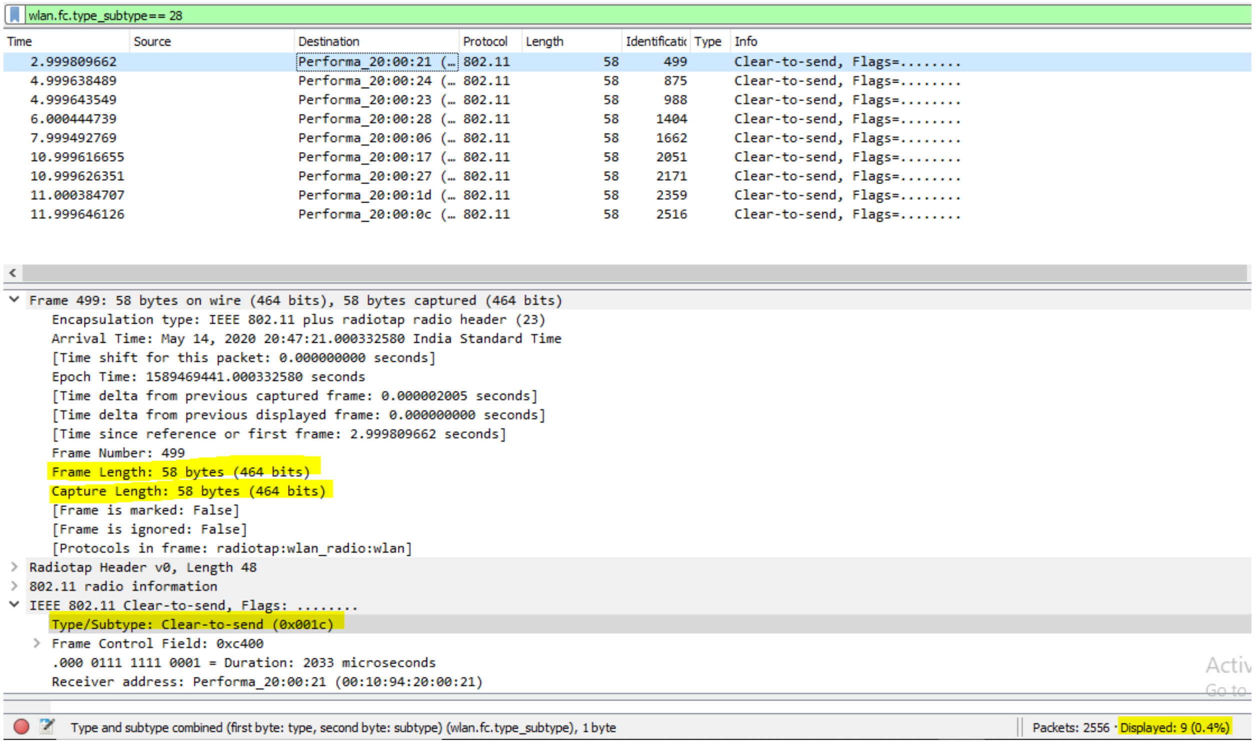
wlan.fc.type_subtype== 27

```
Time          Source                Destination            Protocol   Length   Identificati Type  Info
 0.000000000  Performa_20:00:14 (… 02:6a:e3:90:00:5f (… 802.11          64         1        Request-to-send, Flags=........
 0.000003158  Performa_20:00:18 (… 02:6a:e3:90:00:5f (… 802.11          64         2        Request-to-send, Flags=........
 0.000011156  Performa_20:00:06 (… 02:6a:e3:90:00:5f (… 802.11          64         3        Request-to-send, Flags=........
 0.000023813  Performa_20:00:12 (… 02:6a:e3:90:00:5f (… 802.11          64         4        Request-to-send, Flags=........
 0.000057904  Performa_20:00:0c (… 02:6a:e3:90:00:5f (… 802.11          64         7        Request-to-send, Flags=........
 0.000058434  Performa_20:00:10 (… 02:6a:e3:90:00:5f (… 802.11          64         8        Request-to-send, Flags=........
 0.000064351  Performa_20:00:0f (… 02:6a:e3:90:00:5f (… 802.11          64         9        Request-to-send, Flags=........
 0.000065559  Performa_20:00:28 (… 02:6a:e3:90:00:5f (… 802.11          64        10        Request-to-send, Flags=........
 0.000066044  Performa_20:00:1b (… 02:6a:e3:90:00:5f (… 802.11          64        11        Request-to-send, Flags=........
 0.000074585  Performa_20:00:17 (… 02:6a:e3:90:00:5f (… 802.11          64        12        Request-to-send, Flags=........
 0.000090820  Performa_20:00:16 (… 02:6a:e3:90:00:5f (… 802.11          64        13        Request-to-send, Flags=........
```

```
    Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
    Arrival Time: May 14, 2020 20:47:18.000522918 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1589469438.000522918 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 64 bytes (512 bits)
    Capture Length: 64 bytes (512 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: radiotap:wlan_radio:wlan]
> Radiotap Header v0, Length 48
> 802.11 radio information
v IEEE 802.11 Request-to-send, Flags: ........
    Type/Subtype: Request-to-send (0x001b)
  > Frame Control Field: 0xb400
    .000 0101 1110 1110 = Duration: 1518 microseconds
    Receiver address: 02:6a:e3:90:00:5f (02:6a:e3:90:00:5f)
    Transmitter address: Performa_20:00:14 (00:10:94:20:00:14)
```

CTS:

Apply the filter “**wlan.fc.type_subtype==28**” to observe the CTS frames.
As seen in the below screenshot the number of RTS frames present are **9** and size of each CTS frame is **58 bytes.**



wlan.fc.type_subtype== 28

Time	Source	Destination	Protocol	Length	Identificati	Type	Info
2.999809662		Performa_20:00:21 (…	802.11	58	499		Clear-to-send, Flags=........
4.999638489		Performa_20:00:24 (…	802.11	58	875		Clear-to-send, Flags=........
4.999643549		Performa_20:00:23 (…	802.11	58	988		Clear-to-send, Flags=........
6.000444739		Performa_20:00:28 (…	802.11	58	1404		Clear-to-send, Flags=........
7.999492769		Performa_20:00:06 (…	802.11	58	1662		Clear-to-send, Flags=........
10.999616655		Performa_20:00:17 (…	802.11	58	2051		Clear-to-send, Flags=........
10.999626351		Performa_20:00:27 (…	802.11	58	2171		Clear-to-send, Flags=........
11.000384707		Performa_20:00:1d (…	802.11	58	2359		Clear-to-send, Flags=........
11.999646126		Performa_20:00:0c (…	802.11	58	2516		Clear-to-send, Flags=........

```
Frame 499: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
    Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
    Arrival Time: May 14, 2020 20:47:21.000332580 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1589469441.000332580 seconds
    [Time delta from previous captured frame: 0.000002005 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 2.999809662 seconds]
    Frame Number: 499
    Frame Length: 58 bytes (464 bits)
    Capture Length: 58 bytes (464 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: radiotap:wlan_radio:wlan]
Radiotap Header v0, Length 48
802.11 radio information
IEEE 802.11 Clear-to-send, Flags: ........
    Type/Subtype: Clear-to-send (0x001c)
  > Frame Control Field: 0xc400
    .000 0111 1111 0001 = Duration: 2033 microseconds
    Receiver address: Performa_20:00:21 (00:10:94:20:00:21)
```

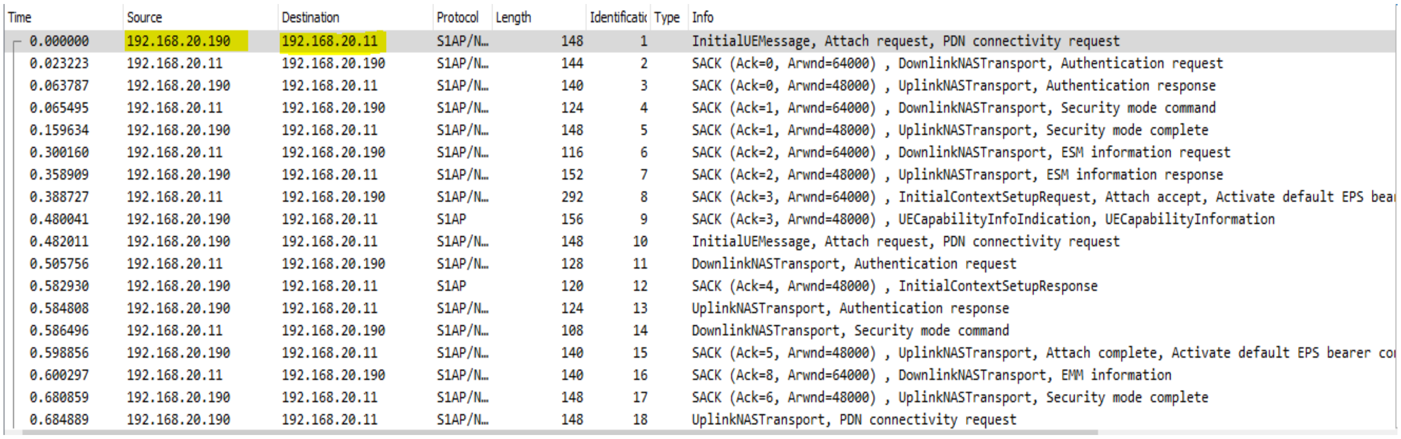
Type and subtype combined (first byte: type, second byte: subtype) (wlan.fc.type_subtype), 1 byte

Packets: 2556 · Displayed: 9 (0.4%)

Task2: 4G-based Cellular Networks

1. Using the attached lte.pcap and the attached LTE attach call flow document lte-attach.pdf, answer the following questions. Note: S1AP is the protocol that carries various attach-related NAS messages between eNodeB and MME. Clearly show the screenshots along with answering each of the questions.

a. List the IP addresses of eNodeB and MME seen in the pcap and explain why so?
Solution :



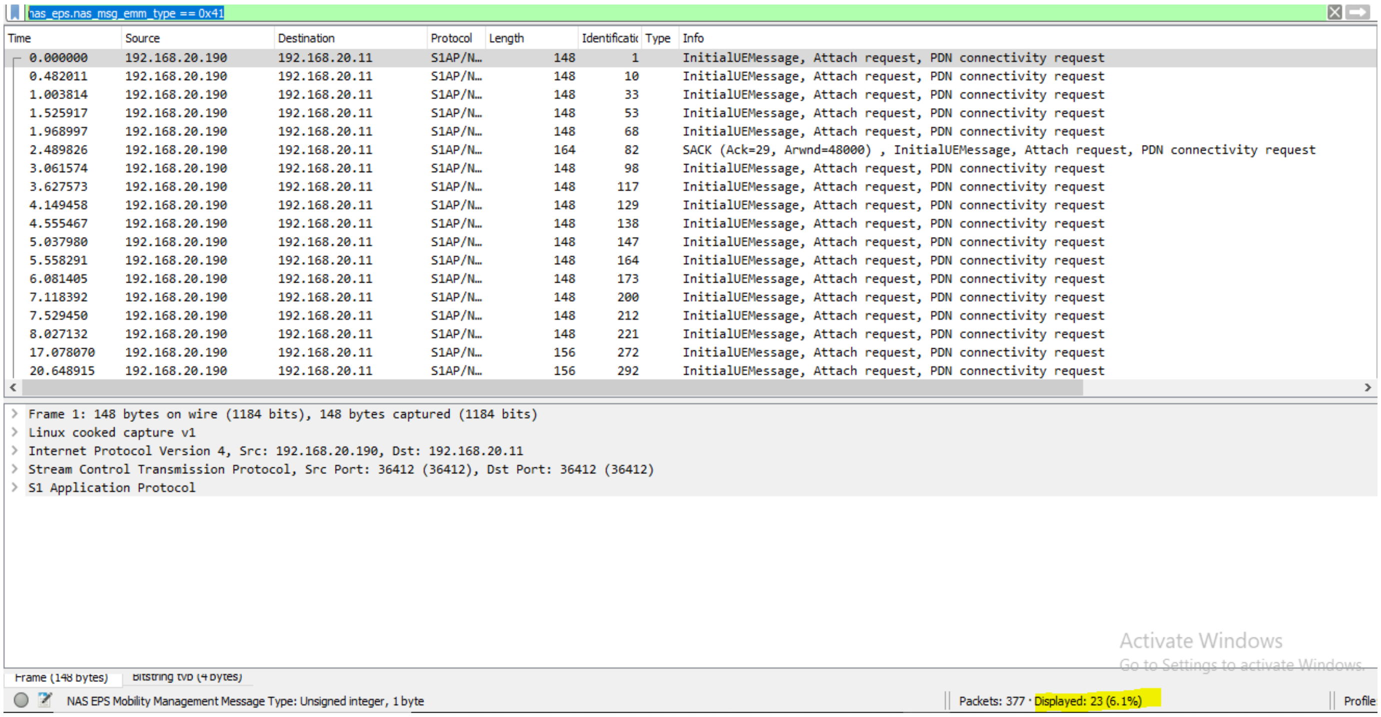
Time	Source	Destination	Protocol	Length	Identificatio	Type	Info
0.000000	192.168.20.190	192.168.20.11	S1AP/N…	148	1		InitialUEMessage, Attach request, PDN connectivity request
0.023223	192.168.20.11	192.168.20.190	S1AP/N…	144	2		SACK (Ack=0, Arwnd=64000) , DownlinkNASTransport, Authentication request
0.063787	192.168.20.190	192.168.20.11	S1AP/N…	140	3		SACK (Ack=0, Arwnd=48000) , UplinkNASTransport, Authentication response
0.065495	192.168.20.11	192.168.20.190	S1AP/N…	124	4		SACK (Ack=1, Arwnd=64000) , DownlinkNASTransport, Security mode command
0.159634	192.168.20.190	192.168.20.11	S1AP/N…	148	5		SACK (Ack=1, Arwnd=48000) , UplinkNASTransport, Security mode complete
0.300160	192.168.20.11	192.168.20.190	S1AP/N…	116	6		SACK (Ack=2, Arwnd=64000) , DownlinkNASTransport, ESM information request
0.358909	192.168.20.190	192.168.20.11	S1AP/N…	152	7		SACK (Ack=2, Arwnd=48000) , UplinkNASTransport, ESM information response
0.388727	192.168.20.11	192.168.20.190	S1AP/N…	292	8		SACK (Ack=3, Arwnd=64000) , InitialContextSetupRequest, Attach accept, Activate default EPS bea
0.480041	192.168.20.190	192.168.20.11	S1AP	156	9		SACK (Ack=3, Arwnd=48000) , UECapabilityInfoIndication, UECapabilityInformation
0.482011	192.168.20.190	192.168.20.11	S1AP/N…	148	10		InitialUEMessage, Attach request, PDN connectivity request
0.505756	192.168.20.11	192.168.20.190	S1AP/N…	128	11		DownlinkNASTransport, Authentication request
0.582930	192.168.20.190	192.168.20.11	S1AP	120	12		SACK (Ack=4, Arwnd=48000) , InitialContextSetupResponse
0.584808	192.168.20.190	192.168.20.11	S1AP/N…	124	13		UplinkNASTransport, Authentication response
0.586496	192.168.20.11	192.168.20.190	S1AP/N…	108	14		DownlinkNASTransport, Security mode command
0.598856	192.168.20.190	192.168.20.11	S1AP/N…	140	15		SACK (Ack=5, Arwnd=48000) , UplinkNASTransport, Attach complete, Activate default EPS bearer co
0.600297	192.168.20.11	192.168.20.190	S1AP/N…	140	16		SACK (Ack=8, Arwnd=64000) , DownlinkNASTransport, EMM information
0.680859	192.168.20.190	192.168.20.11	S1AP/N…	148	17		SACK (Ack=6, Arwnd=48000) , UplinkNASTransport, Security mode complete
0.684889	192.168.20.190	192.168.20.11	S1AP/N…	148	18		UplinkNASTransport, PDN connectivity request

By observing the above screenshot we can see that the IP address of eNodeB and MME are **192.168.20.190** and **192.168.20.11respectively.**

Initial UE Message contains an Attach Request and PDN Connectivity Request. Attach request is initiated by UE to MME. The PDN connectivity procedure is an important process when the LTE communication system accesses to packet data network.

b. How many Attach requests are sent from the user to MME? How do you find this in Wireshark? Also, list the number of Attach Accepts and Attach Completes.

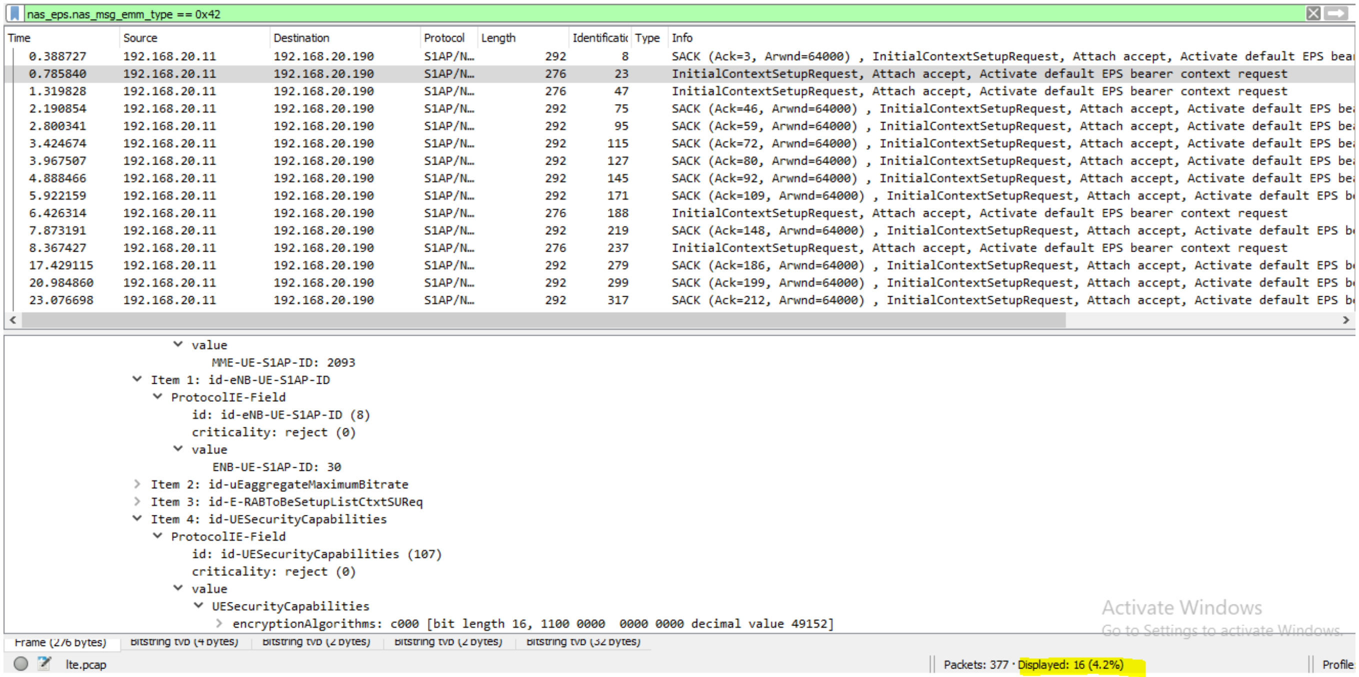
<u>**Attach requests**</u> can be found using the filter **“nas_eps.nas_msg_emm_type == 0x41”**



```
nas_eps.nas_msg_emm_type == 0x41

Time         Source          Destination     Protocol  Length  Identificati Type  Info
 0.000000    192.168.20.190  192.168.20.11   S1AP/N…      148       1     InitialUEMessage, Attach request, PDN connectivity request
 0.482011    192.168.20.190  192.168.20.11   S1AP/N…      148      10     InitialUEMessage, Attach request, PDN connectivity request
 1.003814    192.168.20.190  192.168.20.11   S1AP/N…      148      33     InitialUEMessage, Attach request, PDN connectivity request
 1.525917    192.168.20.190  192.168.20.11   S1AP/N…      148      53     InitialUEMessage, Attach request, PDN connectivity request
 1.968997    192.168.20.190  192.168.20.11   S1AP/N…      148      68     InitialUEMessage, Attach request, PDN connectivity request
 2.489826    192.168.20.190  192.168.20.11   S1AP/N…      164      82     SACK (Ack=29, Arwnd=48000) , InitialUEMessage, Attach request, PDN connectivity request
 3.061574    192.168.20.190  192.168.20.11   S1AP/N…      148      98     InitialUEMessage, Attach request, PDN connectivity request
 3.627573    192.168.20.190  192.168.20.11   S1AP/N…      148     117     InitialUEMessage, Attach request, PDN connectivity request
 4.149458    192.168.20.190  192.168.20.11   S1AP/N…      148     129     InitialUEMessage, Attach request, PDN connectivity request
 4.555467    192.168.20.190  192.168.20.11   S1AP/N…      148     138     InitialUEMessage, Attach request, PDN connectivity request
 5.037980    192.168.20.190  192.168.20.11   S1AP/N…      148     147     InitialUEMessage, Attach request, PDN connectivity request
 5.558291    192.168.20.190  192.168.20.11   S1AP/N…      148     164     InitialUEMessage, Attach request, PDN connectivity request
 6.081405    192.168.20.190  192.168.20.11   S1AP/N…      148     173     InitialUEMessage, Attach request, PDN connectivity request
 7.118392    192.168.20.190  192.168.20.11   S1AP/N…      148     200     InitialUEMessage, Attach request, PDN connectivity request
 7.529450    192.168.20.190  192.168.20.11   S1AP/N…      148     212     InitialUEMessage, Attach request, PDN connectivity request
 8.027132    192.168.20.190  192.168.20.11   S1AP/N…      148     221     InitialUEMessage, Attach request, PDN connectivity request
17.078070    192.168.20.190  192.168.20.11   S1AP/N…      156     272     InitialUEMessage, Attach request, PDN connectivity request
20.648915    192.168.20.190  192.168.20.11   S1AP/N…      156     292     InitialUEMessage, Attach request, PDN connectivity request

> Frame 1: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits)
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 192.168.20.190, Dst: 192.168.20.11
> Stream Control Transmission Protocol, Src Port: 36412 (36412), Dst Port: 36412 (36412)
> S1 Application Protocol

Frame (148 bytes)   Bitstring tvb (4 bytes)

NAS EPS Mobility Management Message Type: Unsigned integer, 1 byte        Packets: 377 · Displayed: 23 (6.1%)        Profile
```

The number of Attach Requests sent are **23** as shown in the above screenshot.

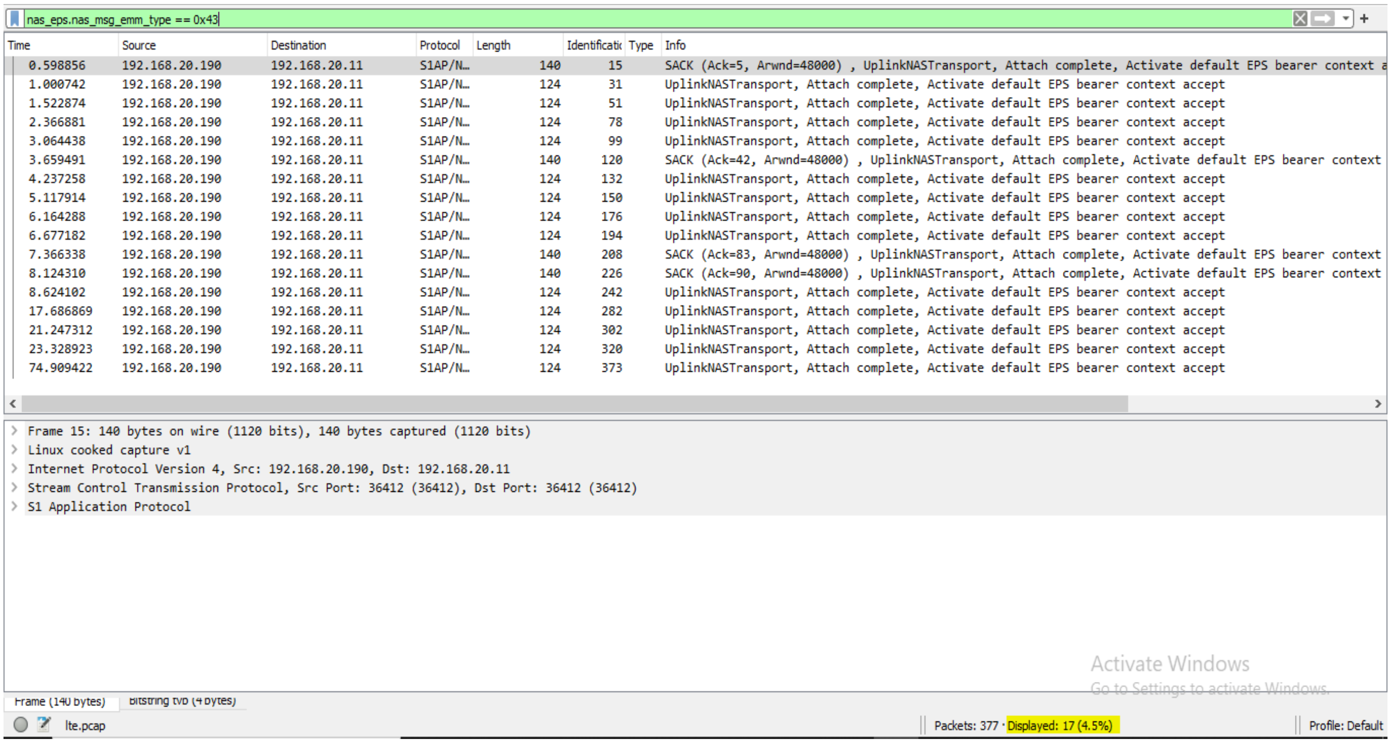
<u>Attach Accept</u> can be found using the filter **“nas_eps.nas_msg_emm_type == 0x42”**



```
nas_eps.nas_msg_emm_type == 0x42

Time         Source          Destination     Protocol  Length  Identificati Type  Info
 0.388727    192.168.20.11   192.168.20.190  S1AP/N…     292       8     SACK (Ack=3, Arwnd=64000) , InitialContextSetupRequest, Attach accept, Activate default EPS bea
 0.785840    192.168.20.11   192.168.20.190  S1AP/N…     276      23     InitialContextSetupRequest, Attach accept, Activate default EPS bearer context request
 1.319828    192.168.20.11   192.168.20.190  S1AP/N…     276      47     InitialContextSetupRequest, Attach accept, Activate default EPS bearer context request
 2.190854    192.168.20.11   192.168.20.190  S1AP/N…     292      75     SACK (Ack=46, Arwnd=64000) , InitialContextSetupRequest, Attach accept, Activate default EPS be
 2.800341    192.168.20.11   192.168.20.190  S1AP/N…     292      95     SACK (Ack=59, Arwnd=64000) , InitialContextSetupRequest, Attach accept, Activate default EPS be
 3.424674    192.168.20.11   192.168.20.190  S1AP/N…     292     115     SACK (Ack=72, Arwnd=64000) , InitialContextSetupRequest, Attach accept, Activate default EPS be
 3.967507    192.168.20.11   192.168.20.190  S1AP/N…     292     127     SACK (Ack=80, Arwnd=64000) , InitialContextSetupRequest, Attach accept, Activate default EPS be
 4.888466    192.168.20.11   192.168.20.190  S1AP/N…     292     145     SACK (Ack=92, Arwnd=64000) , InitialContextSetupRequest, Attach accept, Activate default EPS be
 5.922159    192.168.20.11   192.168.20.190  S1AP/N…     292     171     SACK (Ack=109, Arwnd=64000) , InitialContextSetupRequest, Attach accept, Activate default EPS b
 6.426314    192.168.20.11   192.168.20.190  S1AP/N…     276     188     InitialContextSetupRequest, Attach accept, Activate default EPS bearer context request
 7.873191    192.168.20.11   192.168.20.190  S1AP/N…     292     219     SACK (Ack=148, Arwnd=64000) , InitialContextSetupRequest, Attach accept, Activate default EPS b
 8.367427    192.168.20.11   192.168.20.190  S1AP/N…     276     237     InitialContextSetupRequest, Attach accept, Activate default EPS bearer context request
17.429115    192.168.20.11   192.168.20.190  S1AP/N…     292     279     SACK (Ack=186, Arwnd=64000) , InitialContextSetupRequest, Attach accept, Activate default EPS b
20.984860    192.168.20.11   192.168.20.190  S1AP/N…     292     299     SACK (Ack=199, Arwnd=64000) , InitialContextSetupRequest, Attach accept, Activate default EPS b
23.076698    192.168.20.11   192.168.20.190  S1AP/N…     292     317     SACK (Ack=212, Arwnd=64000) , InitialContextSetupRequest, Attach accept, Activate default EPS b

                  v value
                      MME-UE-S1AP-ID: 2093
              v Item 1: id-eNB-UE-S1AP-ID
                  v ProtocolIE-Field
                        id: id-eNB-UE-S1AP-ID (8)
                        criticality: reject (0)
                      v value
                          ENB-UE-S1AP-ID: 30
              > Item 2: id-uEaggregateMaximumBitrate
              > Item 3: id-E-RABToBeSetupListCtxtSUReq
              v Item 4: id-UESecurityCapabilities
                  v ProtocolIE-Field
                        id: id-UESecurityCapabilities (107)
                        criticality: reject (0)
                      v value
                          v UESecurityCapabilities
                              > encryptionAlgorithms: c000 [bit length 16, 1100 0000  0000 0000 decimal value 49152]

Frame (276 bytes)   Bitstring tvb (4 bytes)   Bitstring tvb (2 bytes)   Bitstring tvb (2 bytes)   Bitstring tvb (32 bytes)

lte.pcap        Packets: 377 · Displayed: 16 (4.2%)        Profile
```

The number of Attach Accepts are **16** as shown in the above screenshot.

<u>Attach Complete</u> can be found using the filter “**nas_eps.nas_msg_emm_type == 0x43**”.



nas_eps.nas_msg_emm_type == 0x43

Time	Source	Destination	Protocol	Length	Identificatic	Type	Info
0.598856	192.168.20.190	192.168.20.11	S1AP/N…	140	15		SACK (Ack=5, Arwnd=48000) , UplinkNASTransport, Attach complete, Activate default EPS bearer context a
1.000742	192.168.20.190	192.168.20.11	S1AP/N…	124	31		UplinkNASTransport, Attach complete, Activate default EPS bearer context accept
1.522874	192.168.20.190	192.168.20.11	S1AP/N…	124	51		UplinkNASTransport, Attach complete, Activate default EPS bearer context accept
2.366881	192.168.20.190	192.168.20.11	S1AP/N…	124	78		UplinkNASTransport, Attach complete, Activate default EPS bearer context accept
3.064438	192.168.20.190	192.168.20.11	S1AP/N…	124	99		UplinkNASTransport, Attach complete, Activate default EPS bearer context accept
3.659491	192.168.20.190	192.168.20.11	S1AP/N…	140	120		SACK (Ack=42, Arwnd=48000) , UplinkNASTransport, Attach complete, Activate default EPS bearer context
4.237258	192.168.20.190	192.168.20.11	S1AP/N…	124	132		UplinkNASTransport, Attach complete, Activate default EPS bearer context accept
5.117914	192.168.20.190	192.168.20.11	S1AP/N…	124	150		UplinkNASTransport, Attach complete, Activate default EPS bearer context accept
6.164288	192.168.20.190	192.168.20.11	S1AP/N…	124	176		UplinkNASTransport, Attach complete, Activate default EPS bearer context accept
6.677182	192.168.20.190	192.168.20.11	S1AP/N…	124	194		UplinkNASTransport, Attach complete, Activate default EPS bearer context accept
7.366338	192.168.20.190	192.168.20.11	S1AP/N…	140	208		SACK (Ack=83, Arwnd=48000) , UplinkNASTransport, Attach complete, Activate default EPS bearer context
8.124310	192.168.20.190	192.168.20.11	S1AP/N…	140	226		SACK (Ack=90, Arwnd=48000) , UplinkNASTransport, Attach complete, Activate default EPS bearer context
8.624102	192.168.20.190	192.168.20.11	S1AP/N…	124	242		UplinkNASTransport, Attach complete, Activate default EPS bearer context accept
17.686869	192.168.20.190	192.168.20.11	S1AP/N…	124	282		UplinkNASTransport, Attach complete, Activate default EPS bearer context accept
21.247312	192.168.20.190	192.168.20.11	S1AP/N…	124	302		UplinkNASTransport, Attach complete, Activate default EPS bearer context accept
23.328923	192.168.20.190	192.168.20.11	S1AP/N…	124	320		UplinkNASTransport, Attach complete, Activate default EPS bearer context accept
74.909422	192.168.20.190	192.168.20.11	S1AP/N…	124	373		UplinkNASTransport, Attach complete, Activate default EPS bearer context accept

```
> Frame 15: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits)
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 192.168.20.190, Dst: 192.168.20.11
> Stream Control Transmission Protocol, Src Port: 36412 (36412), Dst Port: 36412 (36412)
> S1 Application Protocol
```

Packets: 377 · Displayed: 17 (4.5%)

Profile: Default

As seen in above screenshots, the number of Attach Complete is **17**.

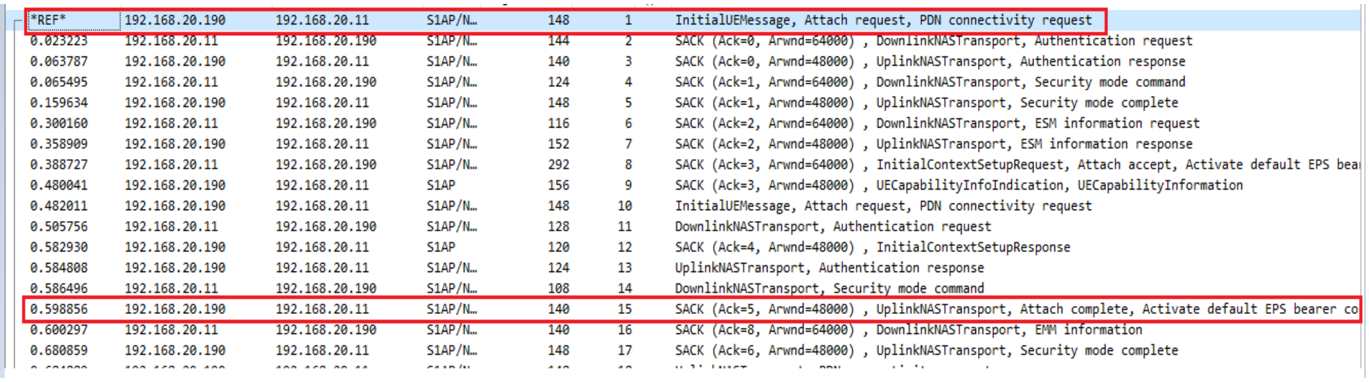
c. Which message confirms the successful attach for a user from MME ? Which message confirms the successful attach from user to MME ?

A user from MME receives a **"Attach Accept"** message to indicate a successful attach. The user's IP address is sent by MME to the UE through eNodeB in the "Attach Accept" message.

The **"Attach Complete**" notification verifies that the user successfully attached to the MME. To recognise and accept the Attach Accept message, UE sends the Attach Complete message. This is sent to the MME.

d. Pick any attach procedure. Calculate the time taken to complete this attach procedure from the user perspective using the Wireshark. Similarly the time taken to complete this attach procedure at MME. Explain how do you find this on Wireshark

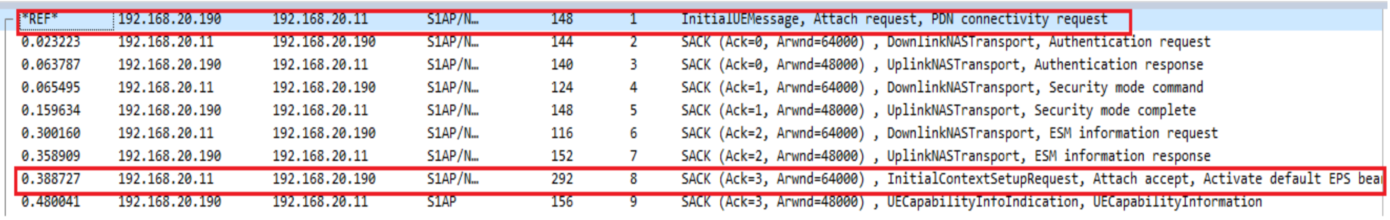
Solution:



```
*REF*       192.168.20.190   192.168.20.11    S1AP/N…    148    1    InitialUEMessage, Attach request, PDN connectivity request
0.023223    192.168.20.11    192.168.20.190   S1AP/N…    144    2    SACK (Ack=0, Arwnd=64000) , DownlinkNASTransport, Authentication request
0.063787    192.168.20.190   192.168.20.11    S1AP/N…    140    3    SACK (Ack=0, Arwnd=48000) , UplinkNASTransport, Authentication response
0.065495    192.168.20.11    192.168.20.190   S1AP/N…    124    4    SACK (Ack=1, Arwnd=64000) , DownlinkNASTransport, Security mode command
0.159634    192.168.20.190   192.168.20.11    S1AP/N…    148    5    SACK (Ack=1, Arwnd=48000) , UplinkNASTransport, Security mode complete
0.300160    192.168.20.11    192.168.20.190   S1AP/N…    116    6    SACK (Ack=2, Arwnd=64000) , DownlinkNASTransport, ESM information request
0.358909    192.168.20.190   192.168.20.11    S1AP/N…    152    7    SACK (Ack=2, Arwnd=48000) , UplinkNASTransport, ESM information response
0.388727    192.168.20.11    192.168.20.190   S1AP/N…    292    8    SACK (Ack=3, Arwnd=64000) , InitialContextSetupRequest, Attach accept, Activate default EPS bea
0.480041    192.168.20.190   192.168.20.11    S1AP       156    9    SACK (Ack=3, Arwnd=48000) , UECapabilityInfoIndication, UECapabilityInformation
0.482011    192.168.20.190   192.168.20.11    S1AP/N…    148    10   InitialUEMessage, Attach request, PDN connectivity request
0.505756    192.168.20.11    192.168.20.190   S1AP/N…    128    11   DownlinkNASTransport, Authentication request
0.582930    192.168.20.190   192.168.20.11    S1AP       120    12   SACK (Ack=4, Arwnd=48000) , InitialContextSetupResponse
0.584808    192.168.20.190   192.168.20.11    S1AP/N…    124    13   UplinkNASTransport, Authentication response
0.586496    192.168.20.11    192.168.20.190   S1AP/N…    108    14   DownlinkNASTransport, Security mode command
0.598856    192.168.20.190   192.168.20.11    S1AP/N…    140    15   SACK (Ack=5, Arwnd=48000) , UplinkNASTransport, Attach complete, Activate default EPS bearer co
0.600297    192.168.20.11    192.168.20.190   S1AP/N…    140    16   SACK (Ack=8, Arwnd=64000) , DownlinkNASTransport, EMM information
0.680859    192.168.20.190   192.168.20.11    S1AP/N…    148    17   SACK (Ack=6, Arwnd=48000) , UplinkNASTransport, Security mode complete
```

According to the user, the attach process begins with UE sending an Attach Request to MME and finishes with UE sending an Attach Complete to MME. Consequently, estimating the time needed to execute this process using wire shark.

Using the Attach Request time as a reference, the amount of time needed for UE to deliver an Attach Complete packet to MME is **0.598856 seconds.**



```
*REF*       192.168.20.190   192.168.20.11    S1AP/N…    148    1    InitialUEMessage, Attach request, PDN connectivity request
0.023223    192.168.20.11    192.168.20.190   S1AP/N…    144    2    SACK (Ack=0, Arwnd=64000) , DownlinkNASTransport, Authentication request
0.063787    192.168.20.190   192.168.20.11    S1AP/N…    140    3    SACK (Ack=0, Arwnd=48000) , UplinkNASTransport, Authentication response
0.065495    192.168.20.11    192.168.20.190   S1AP/N…    124    4    SACK (Ack=1, Arwnd=64000) , DownlinkNASTransport, Security mode command
0.159634    192.168.20.190   192.168.20.11    S1AP/N…    148    5    SACK (Ack=1, Arwnd=48000) , UplinkNASTransport, Security mode complete
0.300160    192.168.20.11    192.168.20.190   S1AP/N…    116    6    SACK (Ack=2, Arwnd=64000) , DownlinkNASTransport, ESM information request
0.358909    192.168.20.190   192.168.20.11    S1AP/N…    152    7    SACK (Ack=2, Arwnd=48000) , UplinkNASTransport, ESM information response
0.388727    192.168.20.11    192.168.20.190   S1AP/N…    292    8    SACK (Ack=3, Arwnd=64000) , InitialContextSetupRequest, Attach accept, Activate default EPS bea
0.480041    192.168.20.190   192.168.20.11    S1AP       156    9    SACK (Ack=3, Arwnd=48000) , UECapabilityInfoIndication, UECapabilityInformation
```

When MME delivers an Attach Accept message to UE, the Attach Procedure at MME is finished. Using the Attach Request time as a reference, the amount of time needed for UE to deliver an Attach Complete packet to MME is **0.388727 seconds.**

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 plagiarized 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 honor violations by other students if I become aware of it.

Name of the student : SHRUSTI
Roll No : CS22MTECH11017