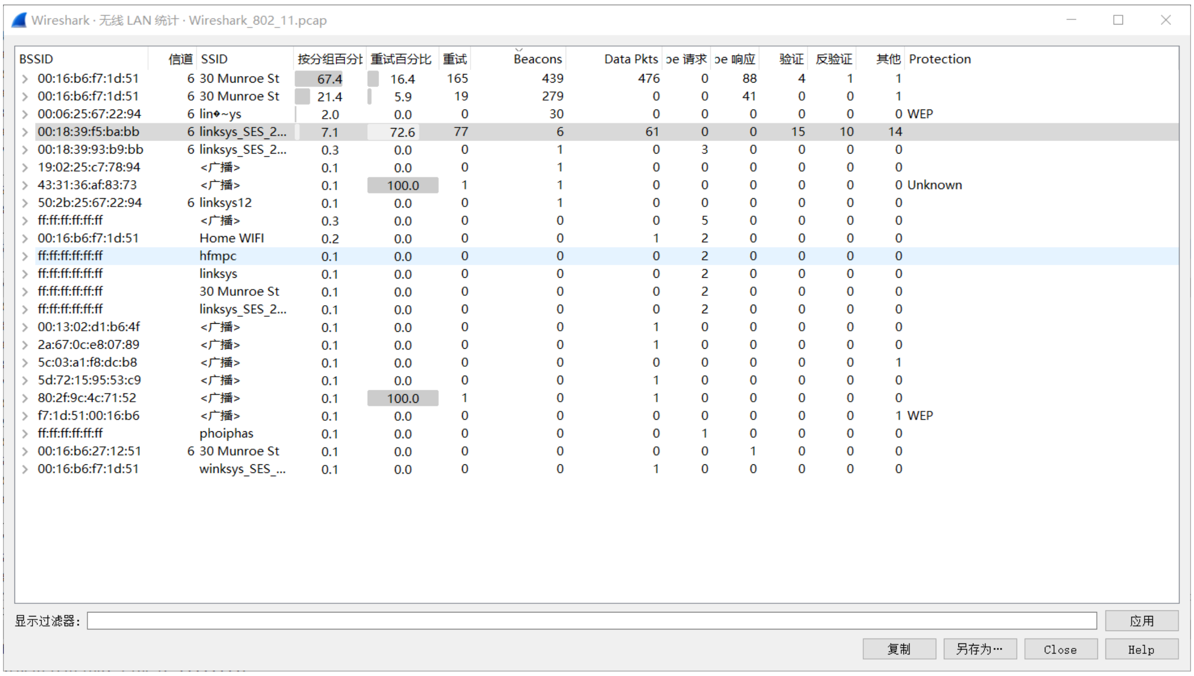
Q1

- What are the SSIDs of the two APs that are issuing most of the beacon frames in this trace?

统计结果按Beacons排序：

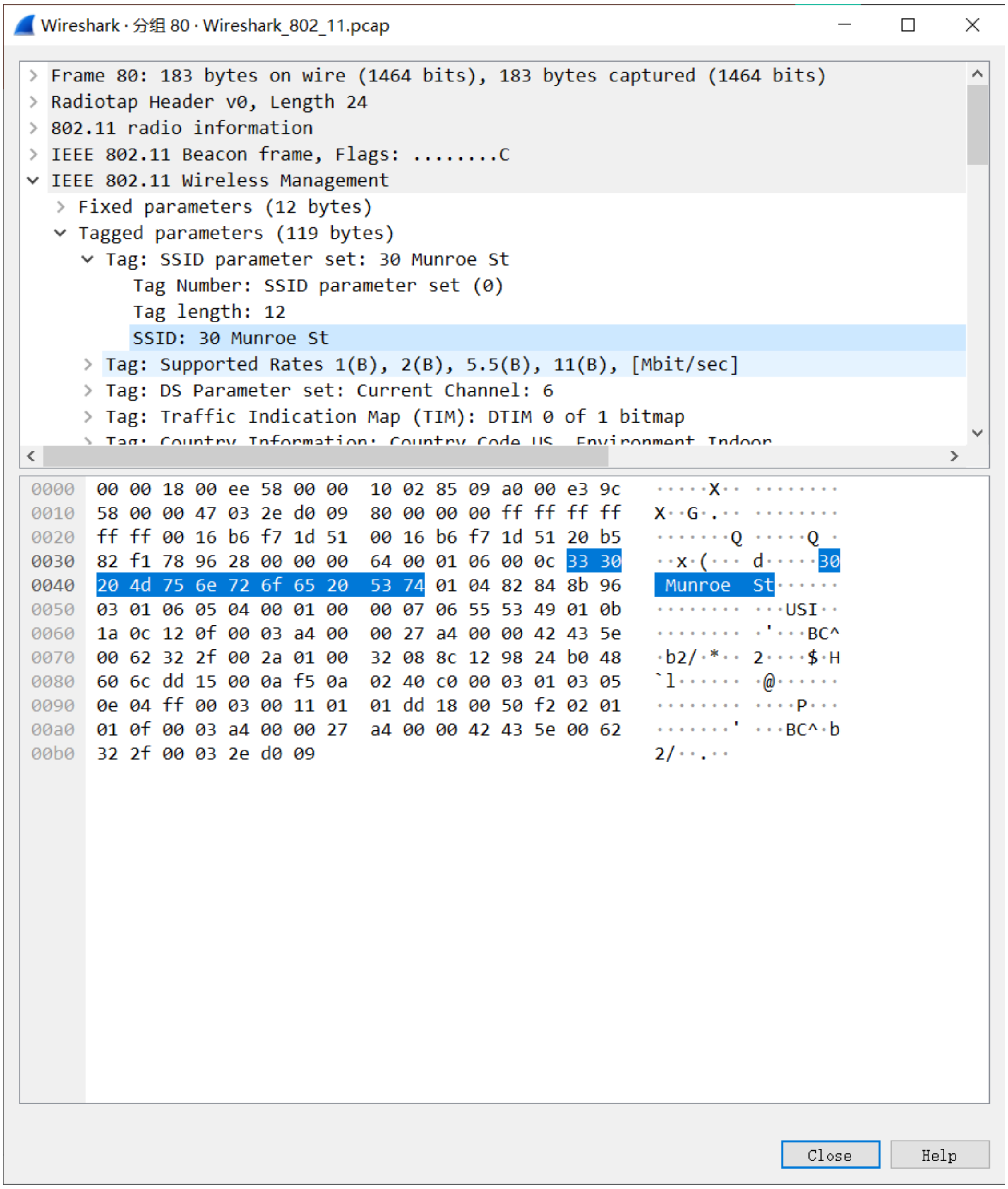


Wireshark · 无线 LAN 统计 · Wireshark_802_11.pcap

BSSID	信道	SSID	按分组百分	重试百分比	重试	Beacons	Data Pkts	be 请求	be 响应	验证	反验证	其他	Protection
00:16:b6:f7:1d:51	6	30 Munroe St	67.4	16.4	165	439	476	0	88	4	1	1	
00:16:b6:f7:1d:51	6	30 Munroe St	21.4	5.9	19	279	0	0	41	0	0	1	
00:06:25:67:22:94	6	lin◆~ys	2.0	0.0	0	30	0	0	0	0	0	0	WEP
00:18:39:f5:ba:bb	6	linksys_SES_2...	7.1	72.6	77	6	61	0	0	15	10	14	
00:18:39:93:b9:bb	6	linksys_SES_2...	0.3	0.0	0	1	0	3	0	0	0	0	
19:02:25:c7:78:94		<广播>	0.1	0.0	0	1	0	0	0	0	0	0	
43:31:36:af:83:73		<广播>	0.1	100.0	1	1	0	0	0	0	0	0	Unknown
50:2b:25:67:22:94	6	linksys12	0.1	0.0	0	1	0	0	0	0	0	0	
ff:ff:ff:ff:ff:ff		<广播>	0.3	0.0	0	0	0	5	0	0	0	0	
00:16:b6:f7:1d:51		Home WIFI	0.2	0.0	0	0	1	2	0	0	0	0	
ff:ff:ff:ff:ff:ff		hfmpc	0.1	0.0	0	0	0	2	0	0	0	0	
ff:ff:ff:ff:ff:ff		linksys	0.1	0.0	0	0	0	2	0	0	0	0	
ff:ff:ff:ff:ff:ff		30 Munroe St	0.1	0.0	0	0	0	2	0	0	0	0	
ff:ff:ff:ff:ff:ff		linksys_SES_2...	0.1	0.0	0	0	0	2	0	0	0	0	
00:13:02:d1:b6:4f		<广播>	0.1	0.0	0	0	1	0	0	0	0	0	
2a:67:0c:e8:07:89		<广播>	0.1	0.0	0	0	1	0	0	0	0	0	
5c:03:a1:f8:dc:b8		<广播>	0.1	0.0	0	0	0	0	0	0	0	1	
5d:72:15:95:53:c9		<广播>	0.1	0.0	0	0	1	0	0	0	0	0	
80:2f:9c:4c:71:52		<广播>	0.1	100.0	1	0	1	0	0	0	0	0	
f7:1d:51:00:16:b6		<广播>	0.1	0.0	0	0	0	0	0	0	0	1	WEP
ff:ff:ff:ff:ff:ff		phoiphas	0.1	0.0	0	0	0	1	0	0	0	0	
00:16:b6:27:12:51	6	30 Munroe St	0.1	0.0	0	0	0	0	1	0	0	0	
00:16:b6:f7:1d:51		winksys_SES_...	0.1	0.0	0	0	1	0	0	0	0	0	

显示过滤器：

1. 30 Munroe St

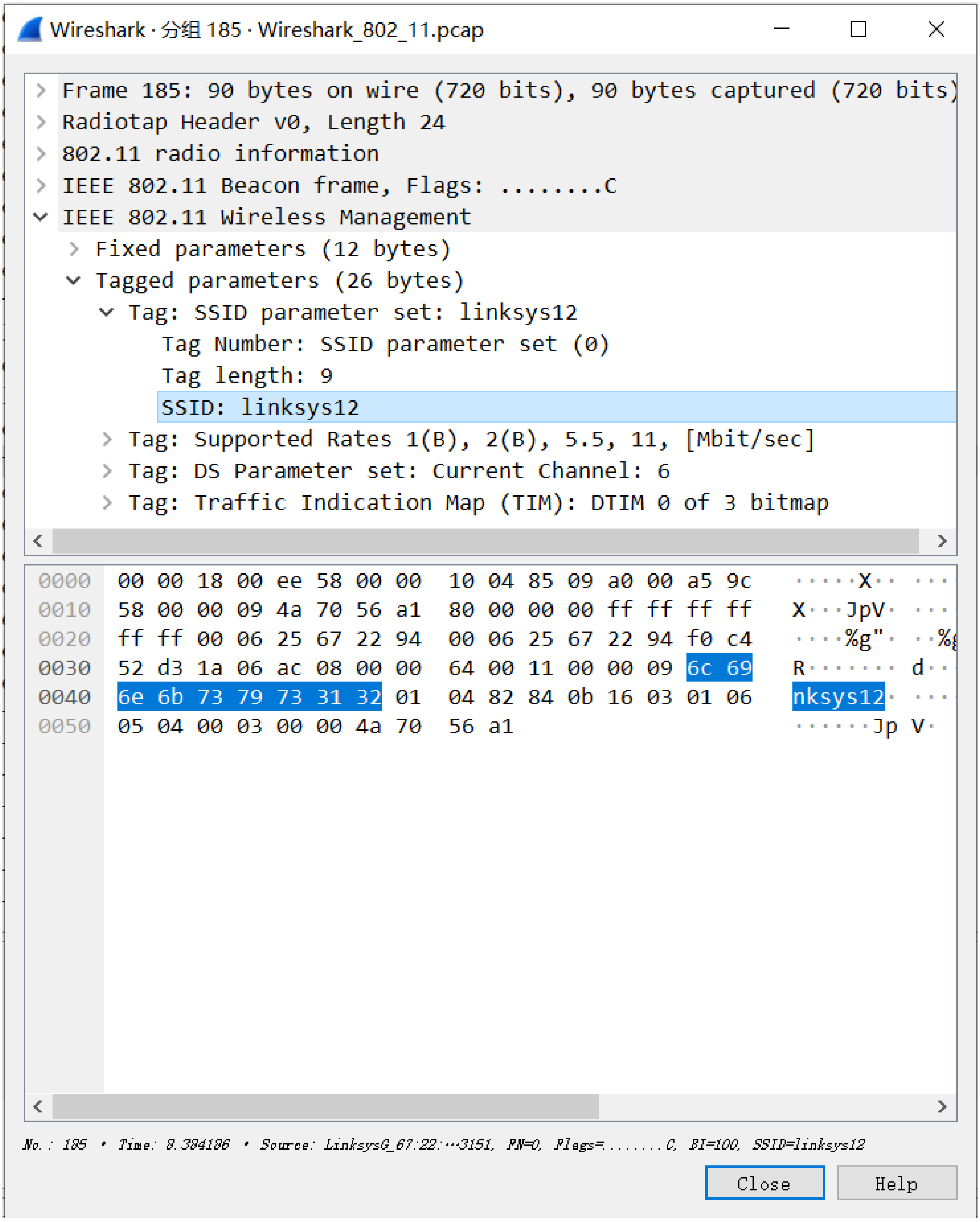


Wireshark · 分组 80 · Wireshark_802_11.pcap

```
> Frame 80: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ........C
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (119 bytes)
    v Tag: SSID parameter set: 30 Munroe St
        Tag Number: SSID parameter set (0)
        Tag length: 12
        SSID: 30 Munroe St
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [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 Indoor
```

```
0000  00 00 18 00 ee 58 00 00  10 02 85 09 a0 00 e3 9c   ·····X·· ········
0010  58 00 00 47 03 2e d0 09  80 00 00 00 ff ff ff ff   X··G·.·· ········
0020  ff ff 00 16 b6 f7 1d 51  00 16 b6 f7 1d 51 20 b5   ·······Q ·····Q ·
0030  82 f1 78 96 28 00 00 00  64 00 01 06 00 0c 33 30   ··x·(··· d·····30
0040  20 4d 75 6e 72 6f 65 20  53 74 01 04 82 84 8b 96    Munroe  St······
0050  03 01 06 05 04 00 01 00  00 07 06 55 53 49 01 0b   ········ ···USI··
0060  1a 0c 12 0f 00 03 a4 00  00 27 a4 00 00 42 43 5e   ········ ·'···BC^
0070  00 62 32 2f 00 2a 01 00  32 08 8c 12 98 24 b0 48   ·b2/·*·· 2····$·H
0080  60 6c dd 15 00 0a f5 0a  02 40 c0 00 03 01 03 05   `l······ ·@······
0090  0e 04 ff 00 03 00 11 01  01 dd 18 00 50 f2 02 01   ········ ····P···
00a0  01 0f 00 03 a4 00 00 27  a4 00 00 42 43 5e 00 62   ·······' ···BC^·b
00b0  32 2f 00 03 2e d0 09                               2/··.··
```

2. linksys12



```
> Frame 185: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ........C
v IEEE 802.11 Wireless Management
    > Fixed parameters (12 bytes)
    v Tagged parameters (26 bytes)
        v Tag: SSID parameter set: linksys12
              Tag Number: SSID parameter set (0)
              Tag length: 9
              SSID: linksys12
        > Tag: Supported Rates 1(B), 2(B), 5.5, 11, [Mbit/sec]
        > Tag: DS Parameter set: Current Channel: 6
        > Tag: Traffic Indication Map (TIM): DTIM 0 of 3 bitmap
```

```
0000  00 00 18 00 ee 58 00 00  10 04 85 09 a0 00 a5 9c   ·····X·· ···
0010  58 00 00 09 4a 70 56 a1  80 00 00 00 ff ff ff ff   X···JpV· ···
0020  ff ff 00 06 25 67 22 94  00 06 25 67 22 94 f0 c4   ····%g"· ··%
0030  52 d3 1a 06 ac 08 00 00  64 00 11 00 00 09 6c 69   R······· d··
0040  6e 6b 73 79 73 31 32 01  04 82 84 0b 16 03 01 06   nksys12· ···
0050  05 04 00 03 00 00 4a 70  56 a1                     ······Jp V·
```

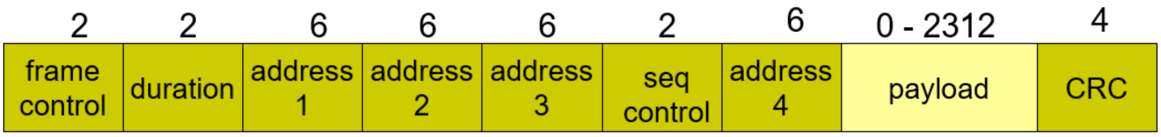
No.: 185 • Time: 8.394186 • Source: LinksysG_67:22:…3151, FN=0, Flags=.......C, BI=100, SSID=linksys12

（统计结果排在linksys_SES_24086前面的，应该是linksys12，只是由于部分frame有bit error，所以没有显示正确SSID名称）

Q2

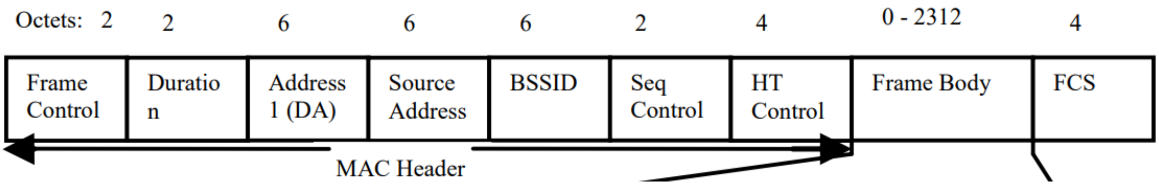
- What are the three addresses in the Beacon frame from the two APs respectively?

802.11 frame的格式：



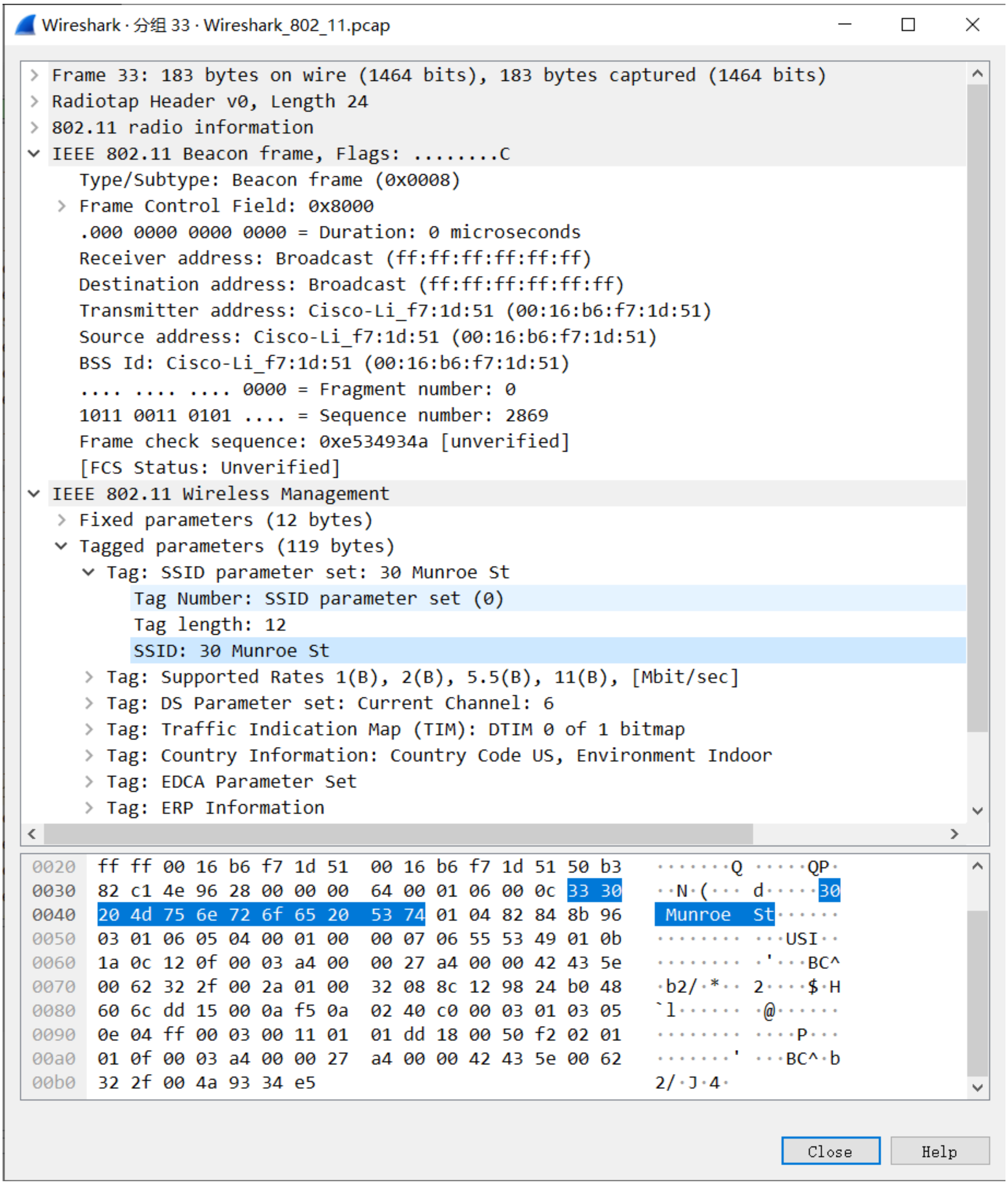
2	2	6	6	6	2	6	0 - 2312	4
frame control	duration	address 1	address 2	address 3	seq control	address 4	payload	CRC

802.11 beacon frame的格式：



Octets: 2	2	6	6	6	2	4	0 - 2312	4
Frame Control	Duration	Address 1 (DA)	Source Address	BSSID	Seq Control	HT Control	Frame Body	FCS

1. 30 Munroe St

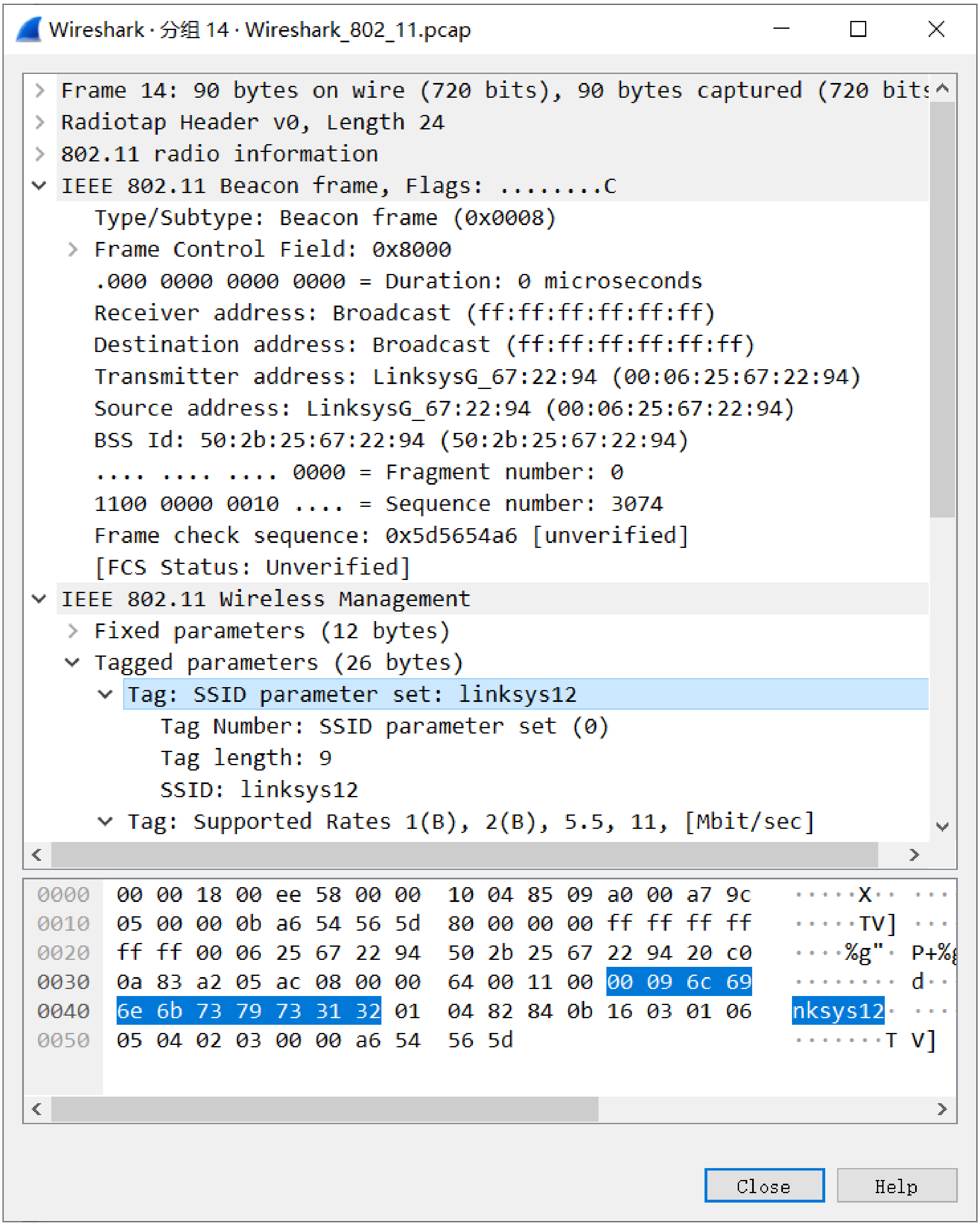


```
> Frame 33: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  > Frame Control Field: 0x8000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Source address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    .... .... .... 0000 = Fragment number: 0
    1011 0011 0101 .... = Sequence number: 2869
    Frame check sequence: 0xe534934a [unverified]
    [FCS Status: Unverified]
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (119 bytes)
    v Tag: SSID parameter set: 30 Munroe St
        Tag Number: SSID parameter set (0)
        Tag length: 12
        SSID: 30 Munroe St
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [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 Indoor
    > Tag: EDCA Parameter Set
    > Tag: ERP Information
```

```
0020  ff ff 00 16 b6 f7 1d 51  00 16 b6 f7 1d 51 50 b3   ·······Q ·····QP·
0030  82 c1 4e 96 28 00 00 00  64 00 01 06 00 0c 33 30   ··N·(··· d·····30
0040  20 4d 75 6e 72 6f 65 20  53 74 01 04 82 84 8b 96    Munroe  St······
0050  03 01 06 05 04 00 01 00  00 07 06 55 53 49 01 0b   ········ ···USI··
0060  1a 0c 12 0f 00 03 a4 00  00 27 a4 00 00 42 43 5e   ········ ·'···BC^
0070  00 62 32 2f 00 2a 01 00  32 08 8c 12 98 24 b0 48   ·b2/·*·· 2····$·H
0080  60 6c dd 15 00 0a f5 0a  02 40 c0 00 03 01 03 05   `l······ ·@······
0090  0e 04 ff 00 03 00 11 01  01 dd 18 00 50 f2 02 01   ········ ····P···
00a0  01 0f 00 03 a4 00 00 27  a4 00 00 42 43 5e 00 62   ·······' ···BC^·b
00b0  32 2f 00 4a 93 34 e5                              2/·J·4·
```

- address 1(who receives this frame): `ff:ff:ff:ff:ff:ff`
- address 2(who transmits this frame): `00:16:b6:f7:1d:51`
- address 3(BBSID): `00:16:b6:f7:1d:51`

2. linksys12



Wireshark · 分组 14 · Wireshark_802_11.pcap

```
> Frame 14: 90 bytes on wire (720 bits), 90 bytes captured (720 bits
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Beacon frame, Flags: ........C
    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: LinksysG_67:22:94 (00:06:25:67:22:94)
    Source address: LinksysG_67:22:94 (00:06:25:67:22:94)
    BSS Id: 50:2b:25:67:22:94 (50:2b:25:67:22:94)
    .... .... .... 0000 = Fragment number: 0
    1100 0000 0010 .... = Sequence number: 3074
    Frame check sequence: 0x5d5654a6 [unverified]
    [FCS Status: Unverified]
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (26 bytes)
    v Tag: SSID parameter set: linksys12
        Tag Number: SSID parameter set (0)
        Tag length: 9
        SSID: linksys12
    v Tag: Supported Rates 1(B), 2(B), 5.5, 11, [Mbit/sec]
```

```
0000  00 00 18 00 ee 58 00 00  10 04 85 09 a0 00 a7 9c   ·····X·· ····
0010  05 00 00 0b a6 54 56 5d  80 00 00 00 ff ff ff ff   ·····TV] ····
0020  ff ff 00 06 25 67 22 94  50 2b 25 67 22 94 20 c0   ····%g"· P+%
0030  0a 83 a2 05 ac 08 00 00  64 00 11 00 00 09 6c 69   ········ d···
0040  6e 6b 73 79 73 31 32 01  04 82 84 0b 16 03 01 06   nksys12· ····
0050  05 04 02 03 00 00 a6 54  56 5d                     ········T V]
```

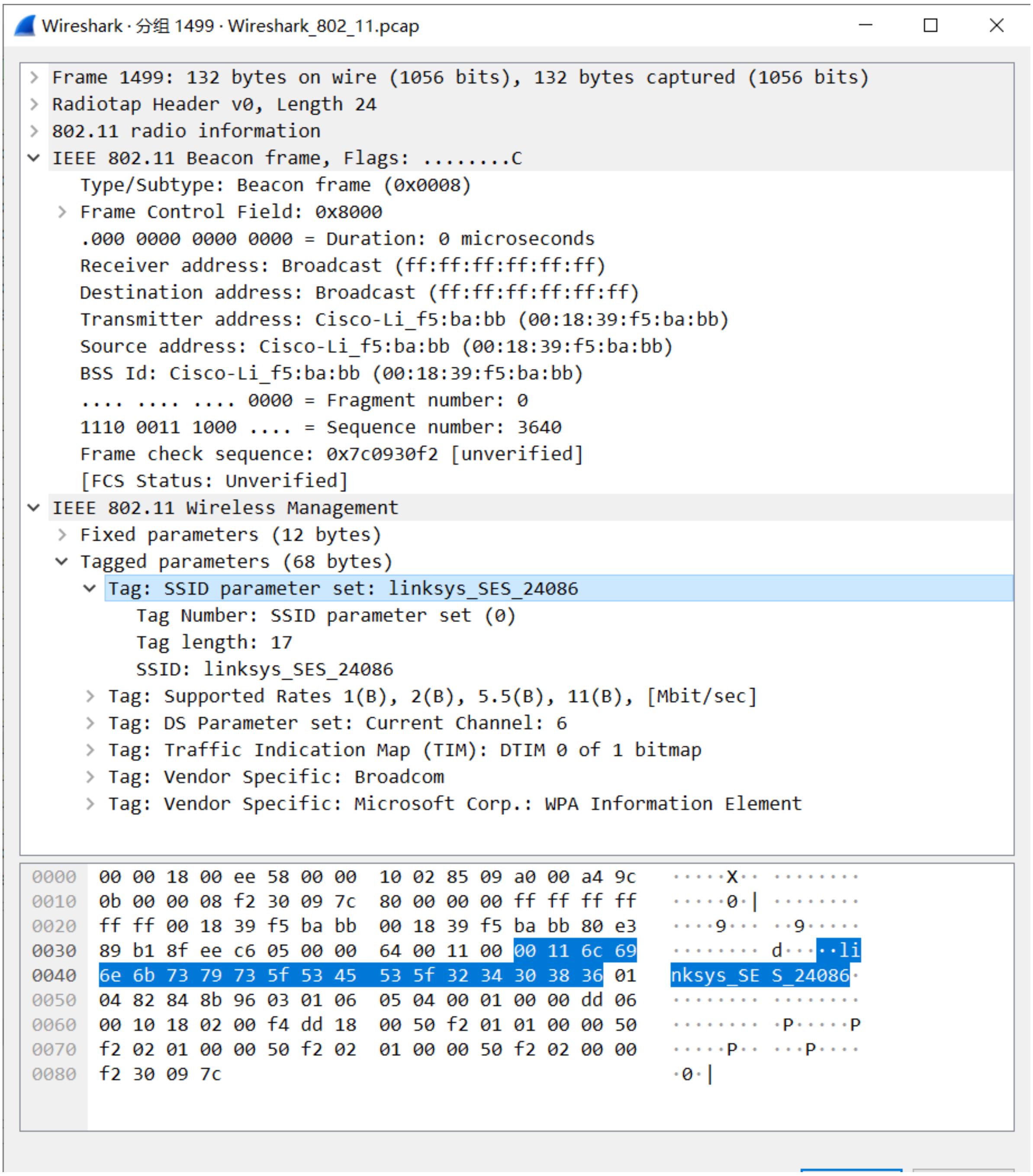
- address 1(who receives this frame): `ff:ff:ff:ff:ff:ff`
- address 2(who transmits this frame): `00:06:25:67:22:94`
- address 3(BBSID): `50:2b:25:67:22:94`

Q3

- How many APs the wireless laptop has received Beacon frames from? List their MAC addresses. Why the laptop can receive frames from an AP even though it does not associate with the AP?

The wireless laptop has received beacon frames from 3 APs.

1. 30 Munroe St: `00:16:b6:f7:1d:51`, screenshot see above
2. linksys12: `00:06:25:67:22:94`, screenshot see above
3. linksys_SES_24086: `00:18:39:f5:ba:bb`, screenshot see below:



```
> Frame 1499: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Beacon frame, Flags: ........C
    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: Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb)
    Source address: Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb)
    BSS Id: Cisco-Li_f5:ba:bb (00:18:39:f5:ba:bb)
    .... .... .... 0000 = Fragment number: 0
    1110 0011 1000 .... = Sequence number: 3640
    Frame check sequence: 0x7c0930f2 [unverified]
    [FCS Status: Unverified]
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (68 bytes)
    v Tag: SSID parameter set: linksys_SES_24086
        Tag Number: SSID parameter set (0)
        Tag length: 17
        SSID: linksys_SES_24086
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 6
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
    > Tag: Vendor Specific: Broadcom
    > Tag: Vendor Specific: Microsoft Corp.: WPA Information Element
```

```
0000  00 00 18 00 ee 58 00 00  10 02 85 09 a0 00 a4 9c   ·····X·· ········
0010  0b 00 00 08 f2 30 09 7c  80 00 00 00 ff ff ff ff   ·····0·| ········
0020  ff ff 00 18 39 f5 ba bb  00 18 39 f5 ba bb 80 e3   ····9··· ··9·····
0030  89 b1 8f ee c6 05 00 00  64 00 11 00 00 11 6c 69   ········ d·····li
0040  6e 6b 73 79 73 5f 53 45  53 5f 32 34 30 38 36 01   nksys_SE S_24086·
0050  04 82 84 8b 96 03 01 06  05 04 00 01 00 00 dd 06   ········ ········
0060  00 10 18 02 00 f4 dd 18  00 50 f2 01 01 00 00 50   ········ ·P·····P
0070  f2 02 01 00 00 50 f2 02  01 00 00 50 f2 02 00 00   ·····P·· ···P····
0080  f2 30 09 7c                                        ·0·|
```

另外还有一些SSID比较奇怪的包，应该是出现了bit error，所以主要的AP就只有上述三个。

Laptop 收到AP的beacon frame，因为AP会定期发包（at its channel），然后host可以请求连接，并最终建立连接——这被称为passive scanning.

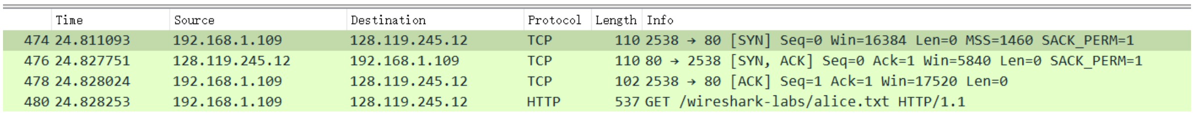
Q4

In 802.11 frame:

$Source \rightarrow Transmitter \rightarrow Receiver \rightarrow Destination$

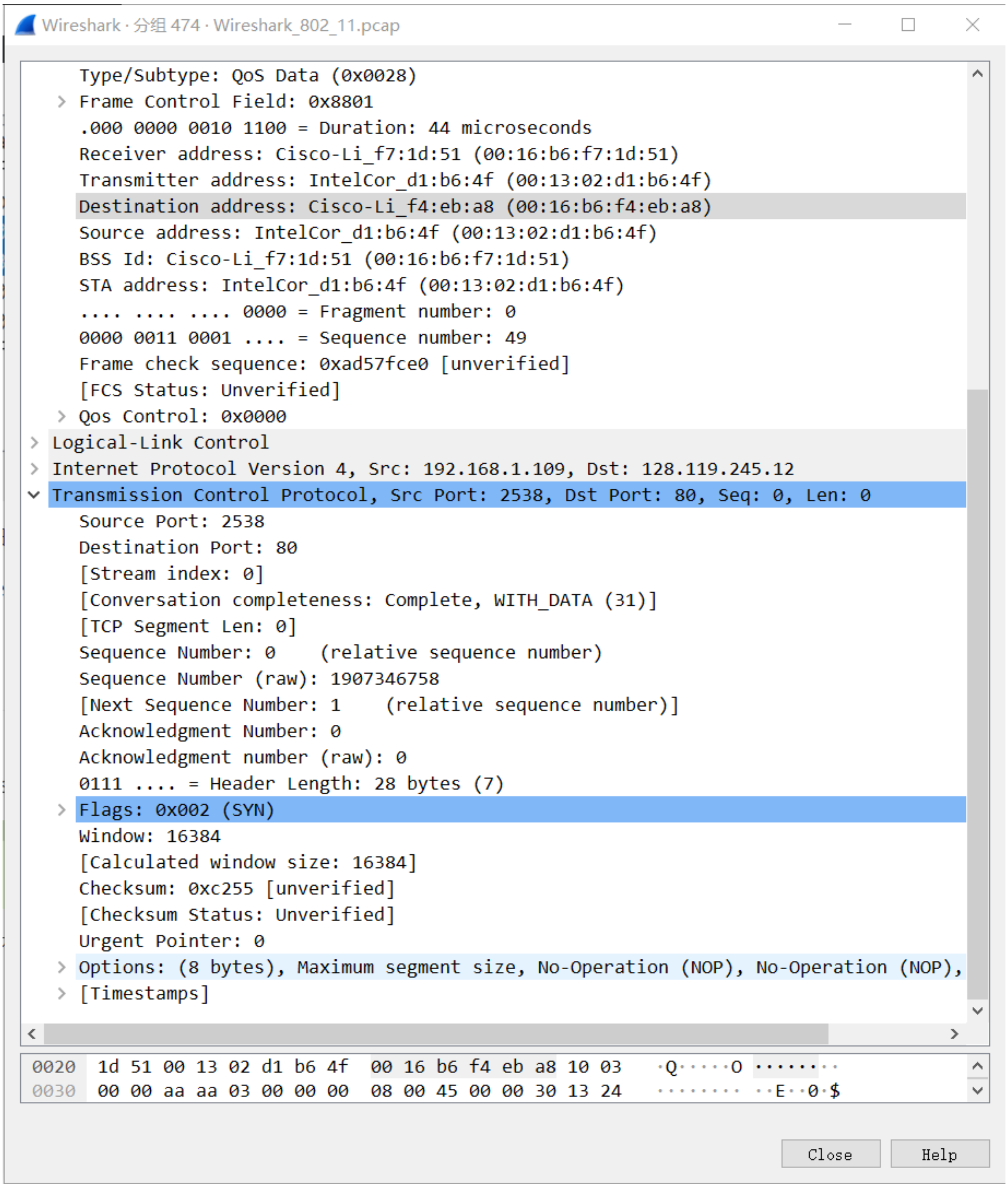
其中 $Source$ 和 $Transmitter$ 可以重叠， $Receiver$ 和 $Destination$ 可以重叠。

- Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt). What are the three MAC addresses in the frame, which is the address for wireless laptop / AP / first-hop router?



```
    Time       Source          Destination     Protocol Length Info
474 24.811093  192.168.1.109   128.119.245.12  TCP         110 2538 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
476 24.827751  128.119.245.12  192.168.1.109   TCP         110 80 → 2538 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM=1
478 24.828024  192.168.1.109   128.119.245.12  TCP         102 2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
480 24.828253  192.168.1.109   128.119.245.12  HTTP        537 GET /wireshark-labs/alice.txt HTTP/1.1
```

上图所示为建立TCP连接的过程，其中第一个为SYN TCP segment，内容如下：



```
        Type/Subtype: QoS Data (0x0028)
      > Frame Control Field: 0x8801
        .000 0000 0010 1100 = Duration: 44 microseconds
        Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
        Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
        Destination address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
        Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
        BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
        STA address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
        .... .... .... 0000 = Fragment number: 0
        0000 0011 0001 .... = Sequence number: 49
        Frame check sequence: 0xad57fce0 [unverified]
        [FCS Status: Unverified]
      > Qos Control: 0x0000
    > Logical-Link Control
    > Internet Protocol Version 4, Src: 192.168.1.109, Dst: 128.119.245.12
    v Transmission Control Protocol, Src Port: 2538, Dst Port: 80, Seq: 0, Len: 0
        Source Port: 2538
        Destination Port: 80
        [Stream index: 0]
        [Conversation completeness: Complete, WITH_DATA (31)]
        [TCP Segment Len: 0]
        Sequence Number: 0    (relative sequence number)
        Sequence Number (raw): 1907346758
        [Next Sequence Number: 1    (relative sequence number)]
        Acknowledgment Number: 0
        Acknowledgment number (raw): 0
        0111 .... = Header Length: 28 bytes (7)
      > Flags: 0x002 (SYN)
        Window: 16384
        [Calculated window size: 16384]
        Checksum: 0xc255 [unverified]
        [Checksum Status: Unverified]
        Urgent Pointer: 0
      > Options: (8 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP),
      > [Timestamps]

0020  1d 51 00 13 02 d1 b6 4f  00 16 b6 f4 eb a8 10 03   ·Q·····O ········
0030  00 00 aa aa 03 00 00 00  08 00 45 00 00 30 13 24   ········ ··E··0·$
```

Src IP address: 192.168.1.109; Dst IP address: 128.119.245.12

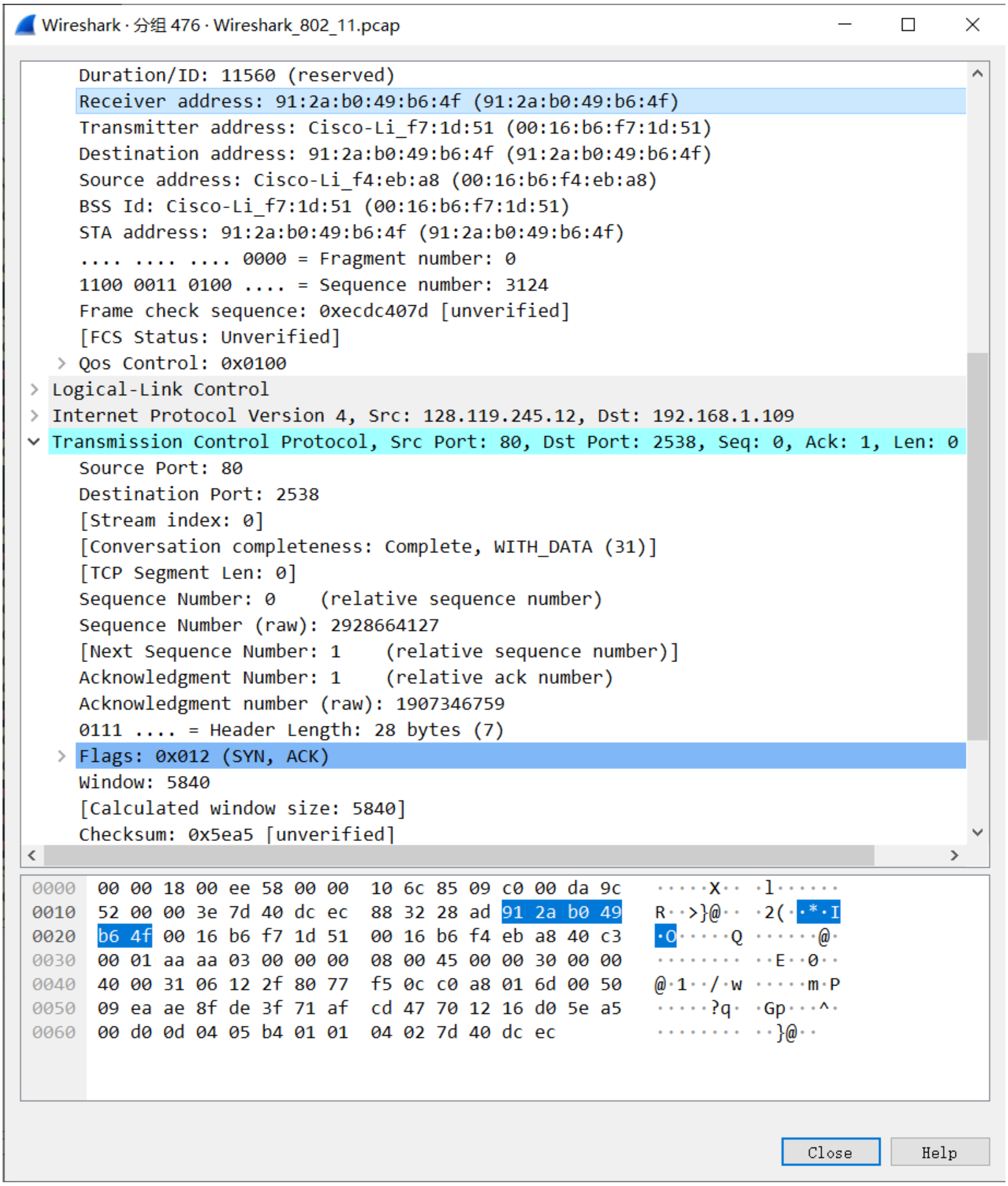
- address1: `00:16:b6:f7:1d:51`
- address2: `00:13:02:d1:b6:4f`
- address3: `00:16:b6:f4:eb:a8`

- laptop's MAC address(Transmitter/Source address): `00:13:02:d1:b6:4f`
- AP's MAC address(Receiver address): `00:16:b6:f7:1d:51`
- first-hop router's MAC address(Destination address): `00:16:b6:f4:eb:a8`

Q5

- For the SYN-ACK segment of the first TCP session, what are the three MAC addresses in the frame, and which is the address for wireless laptop / AP / first-hop router?

建立TCP连接中，SYN-ACK的包内容如下：



```
    Duration/ID: 11560 (reserved)
    Receiver address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
    Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Destination address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
    Source address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    STA address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
    .... .... .... 0000 = Fragment number: 0
    1100 0011 0100 .... = Sequence number: 3124
    Frame check sequence: 0xecdc407d [unverified]
    [FCS Status: Unverified]
  > Qos Control: 0x0100
> Logical-Link Control
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.109
v Transmission Control Protocol, Src Port: 80, Dst Port: 2538, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 2538
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 2928664127
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1907346759
    0111 .... = Header Length: 28 bytes (7)
  > Flags: 0x012 (SYN, ACK)
    Window: 5840
    [Calculated window size: 5840]
    Checksum: 0x5ea5 [unverified]
```

```
0000  00 00 18 00 ee 58 00 00  10 6c 85 09 c0 00 da 9c   ·····X·· ·l······
0010  52 00 00 3e 7d 40 dc ec  88 32 28 ad 91 2a b0 49   R··>}@·· ·2(··*·I
0020  b6 4f 00 16 b6 f7 1d 51  00 16 b6 f4 eb a8 40 c3   ·O·····Q ······@·
0030  00 01 aa aa 03 00 00 00  08 00 45 00 00 30 00 00   ········ ··E··0··
0040  40 00 31 06 12 2f 80 77  f5 0c c0 a8 01 6d 00 50   @·1··/·w ·····m·P
0050  09 ea ae 8f de 3f 71 af  cd 47 70 12 16 d0 5e a5   ·····?q· ·Gp···^·
0060  00 d0 0d 04 05 b4 01 01  04 02 7d 40 dc ec         ········ ··}@··
```

Src IP address: 128.119.245.12; Dst IP address: 192.168.1.109

- address1: `91:2a:b0:49:b6:4f`
- address2: `00:16:b6:f7:1d:51`
- address3: `00:16:b6:f4:eb:a8`

- laptop's MAC address(Destination/Receiver address): `91:2a:b0:49:b6:4f` （可能 因为发送给另一张网卡？）
- AP's MAC address(Transmitter address): `00:16:b6:f7:1d:51`
- first-hop router's MAC address(Source address): `00:16:b6:f4:eb:a8`

Q6

- For the above mentioned SYN-ACK segment, is the sender MAC address corresponds to the web server's IP address? Why?

应该不是，因为Sender(source) MAC address是first-hop router的MAC address，不是web server的MAC address

Q7

- What two actions are taken (i.e., frames are sent) by the host in the trace just after *t=49*, to end the association with the *30 Munroe St* AP?

在t=49.58的时候，host与30 Munroe St AP断开连接，进行的操作是：

1. t=49.583615的时候，发送`DHCP Release`包；
2. t=49.609617的时候，发送`Deauthentication`包。

Q8

- Can you capture a similar trace? Why or why not?

不可以，需要进行一些特殊的配置，比如在Wireshark Q&A中提到：

one way to go is having a dedicated machine with a wireless card in promiscuous mode somewhere near the AP acting as a monitor node.

并且由于Windows系统的限制，这几乎是不可能做到的：（见WLAN (wireshark.org)）

Unfortunately, changing the 802.11 capture modes is very platform/network adapter/driver/libpcap dependent, and might not be possible at all (Windows is very limited here).

- 具体解释如下：

通常情况下，网络适配器（network adaptor）的SSID filter只会保留它当前连接的AP的SSID，而过滤掉其他的SSID；

如果使用Monitor mode，SSID filter就会被禁止，所有AP（不同SSID）的所有包都会被捕获到。

但是Monitor mode不被Windows支持（`WinPcap`，`Wireshark` or `TShark`）；只有一些Linux版本，如`FreeBSD`，`NetBSD`，`OpenBSD`，`DragonFly BSD`，以及macOS支持。