Trace_analysis实验报告

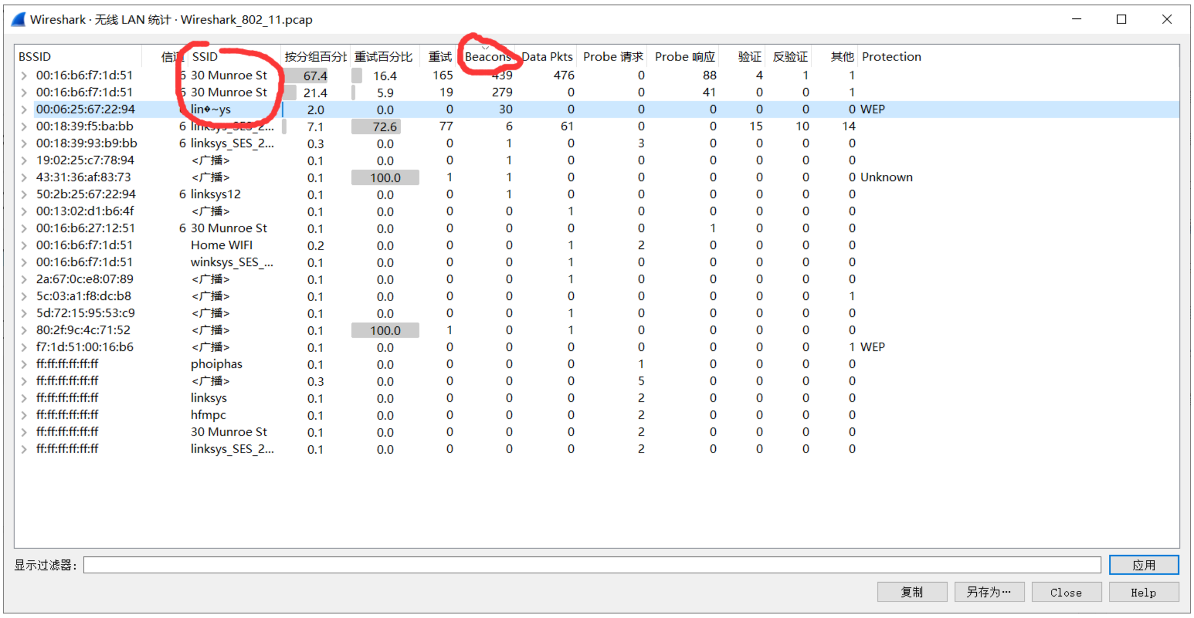
PB19111713钟颖康

Q1: What are the SSIDs of the two APs that are issuing most of the beacon frames in this trace?

A1:

主要是`30 Munroe St`与`lin�~ys`。

截图如下：



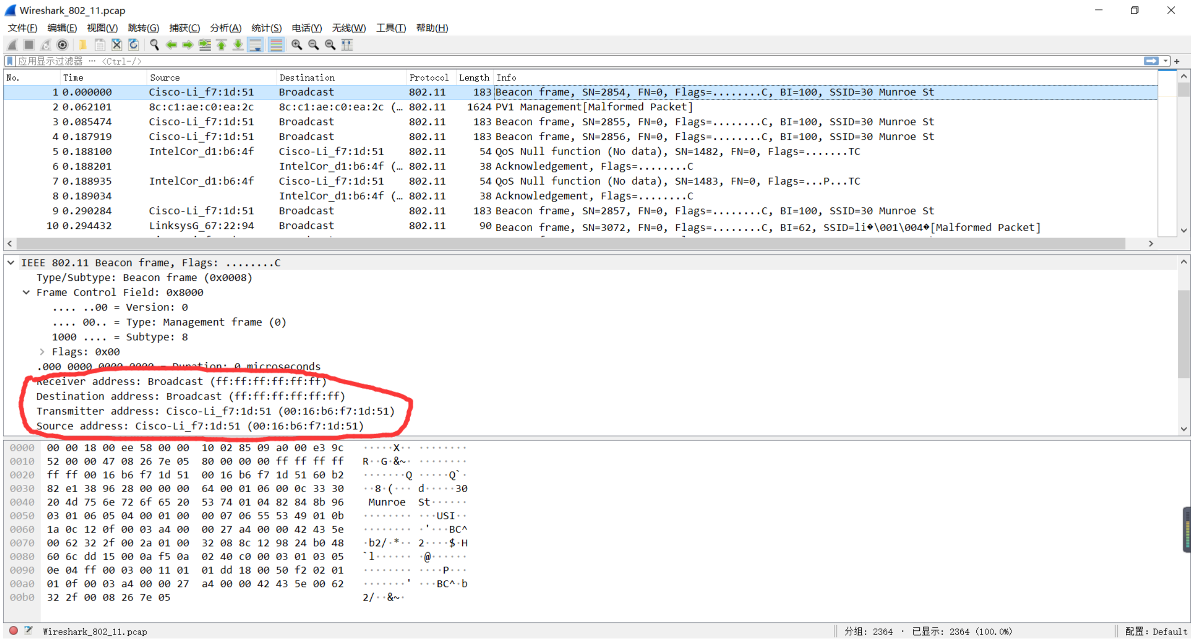
BSSID	信道	SSID	按分组百分	重试百分比	重试	Beacons	Data Pkts	Probe 请求	Probe 响应	验证	反验证	其他	Protection
00:16:b6:f7:1d:51	6	30 Munroe St	67.4	16.4	165	439	476	0	88	4	1	1	
00:16:b6:f7:1d:51	6	30 Munroe St	21.4	5.9	19	279	0	0	41	0	0	1	
00:06:25:67:22:94	[illegible]	lin◆~ys	2.0	0.0	0	30	0	0	0	0	0	0	WEP
00:18:39:f5:ba:bb	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	
00:13:02:d1:b6:4f		<广播>	0.1	0.0	0	0	1	0	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		Home WIFI	0.2	0.0	0	0	1	2	0	0	0	0	
00:16:b6:f7:1d:51		winksys_SES_...	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	
ff:ff:ff:ff:ff:ff		<广播>	0.3	0.0	0	0	0	5	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		hfmpc	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	

Q2: What are the three addresses in the Beacon frame from the two APs respectively.

A2:

	30 Munroe St(00:16:b6:f7:1d:51)	linksys_SES_24086(00:06:25:67:22:94)
Receiver Address	ff:ff:ff:ff:ff:ff	ff:ff:ff:ff:ff:ff
Destination Address	ff:ff:ff:ff:ff:ff	ff:ff:ff:ff:ff:ff
Transmitter/source Address	00:16:b6:f7:1d:51	00:06:25:67:22:94

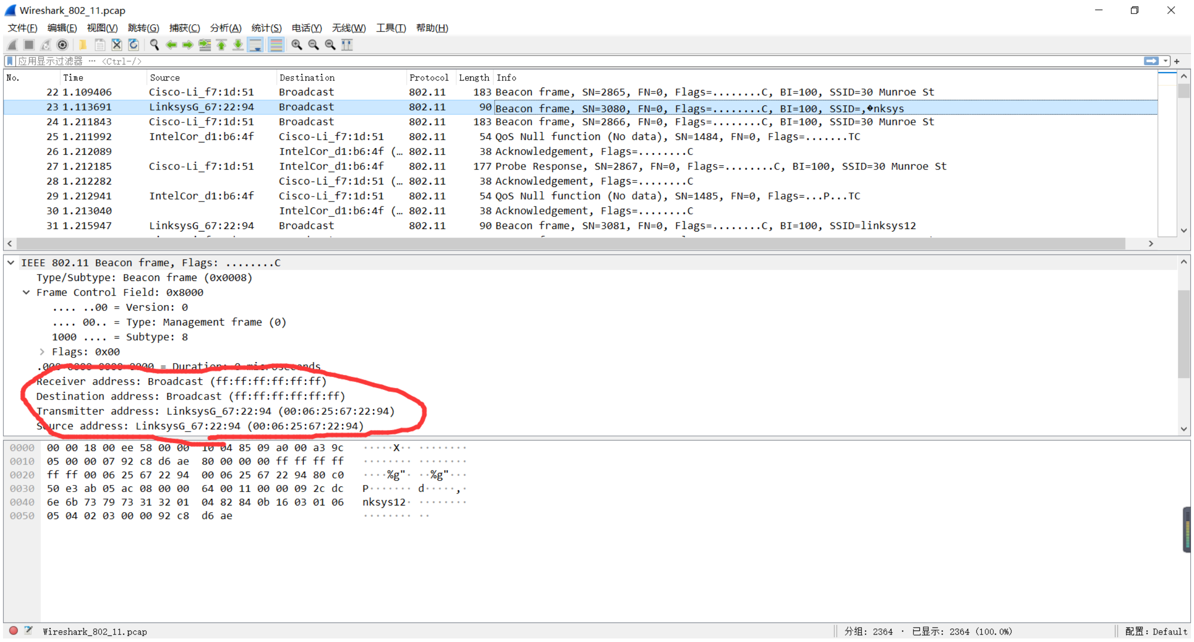
截图如下：


Wireshark_802_11.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>
Wireshark_802_11.pcap
分组: 2364 · 已显示: 2364 (100.0%)
配置: Default

```
No.   Time        Source               Destination            Protocol  Length Info
    1 0.000000    Cisco-Li_f7:1d:51    Broadcast              802.11     183 Beacon frame, SN=2854, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
    2 0.062101    8c:c1:ae:c0:ea:2c    8c:c1:ae:c0:ea:2c (…   802.11    1624 PV1 Management[Malformed Packet]
    3 0.085474    Cisco-Li_f7:1d:51    Broadcast              802.11     183 Beacon frame, SN=2855, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
    4 0.187919    Cisco-Li_f7:1d:51    Broadcast              802.11     183 Beacon frame, SN=2856, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
    5 0.188100    IntelCor_d1:b6:4f    Cisco-Li_f7:1d:51      802.11      54 QoS Null function (No data), SN=1482, FN=0, Flags=.......TC
    6 0.188201                         IntelCor_d1:b6:4f (…   802.11      38 Acknowledgement, Flags=........C
    7 0.188935    IntelCor_d1:b6:4f    Cisco-Li_f7:1d:51      802.11      54 QoS Null function (No data), SN=1483, FN=0, Flags=...P...TC
    8 0.189034                         IntelCor_d1:b6:4f (…   802.11      38 Acknowledgement, Flags=........C
    9 0.290284    Cisco-Li_f7:1d:51    Broadcast              802.11     183 Beacon frame, SN=2857, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   10 0.294432    LinksysG_67:22:94    Broadcast              802.11      90 Beacon frame, SN=3072, FN=0, Flags=........C, BI=62, SSID=li◆\001\004◆[Malformed Packet]

∨ IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  ∨ Frame Control Field: 0x8000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1000 .... = Subtype: 8
    > Flags: 0x00
    .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)

0000  00 00 18 00 ee 58 00 00  10 02 85 09 a0 00 e3 9c   ·····X·· ········
0010  52 00 00 47 08 26 7e 05  80 00 00 00 ff ff ff ff   R··G·&~· ········
0020  ff ff 00 16 b6 f7 1d 51  00 16 b6 f7 1d 51 60 b2   ·······Q ·····Q`·
0030  82 e1 38 96 28 00 00 00  64 00 01 06 00 0c 33 30   ··8·(··· 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 08 26 7e 05                               2/··&~·
```


Wireshark_802_11.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>
Wireshark_802_11.pcap
分组: 2364 · 已显示: 2364 (100.0%)
配置: Default

```
No.   Time        Source               Destination            Protocol  Length Info
   22 1.109406    Cisco-Li_f7:1d:51    Broadcast              802.11     183 Beacon frame, SN=2865, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   23 1.113691    LinksysG_67:22:94    Broadcast              802.11      90 Beacon frame, SN=3080, FN=0, Flags=........C, BI=100, SSID=,◆nksys
   24 1.211843    Cisco-Li_f7:1d:51    Broadcast              802.11     183 Beacon frame, SN=2866, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   25 1.211992    IntelCor_d1:b6:4f    Cisco-Li_f7:1d:51      802.11      54 QoS Null function (No data), SN=1484, FN=0, Flags=.......TC
   26 1.212089                         IntelCor_d1:b6:4f (…   802.11      38 Acknowledgement, Flags=........C
   27 1.212185    Cisco-Li_f7:1d:51    IntelCor_d1:b6:4f      802.11     177 Probe Response, SN=2867, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
   28 1.212282                         Cisco-Li_f7:1d:51 (…   802.11      38 Acknowledgement, Flags=........C
   29 1.212941    IntelCor_d1:b6:4f    Cisco-Li_f7:1d:51      802.11      54 QoS Null function (No data), SN=1485, FN=0, Flags=...P...TC
   30 1.213040                         IntelCor_d1:b6:4f (…   802.11      38 Acknowledgement, Flags=........C
   31 1.215947    LinksysG_67:22:94    Broadcast              802.11      90 Beacon frame, SN=3081, FN=0, Flags=........C, BI=100, SSID=linksys12

∨ IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  ∨ Frame Control Field: 0x8000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1000 .... = Subtype: 8
    > Flags: 0x00
    .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)

0000  00 00 18 00 ee 58 00 00  10 04 85 09 a0 00 a3 9c   ·····X·· ········
0010  05 00 00 07 92 c8 d6 ae  80 00 00 00 ff ff ff ff   ········ ········
0020  ff ff 00 06 25 67 22 94  00 06 25 67 22 94 80 c0   ····%g"· ··%g"···
0030  50 e3 ab 05 ac 08 00 00  64 00 11 00 00 09 2c dc   P······· 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 92 c8  d6 ae                     ········ ··
```

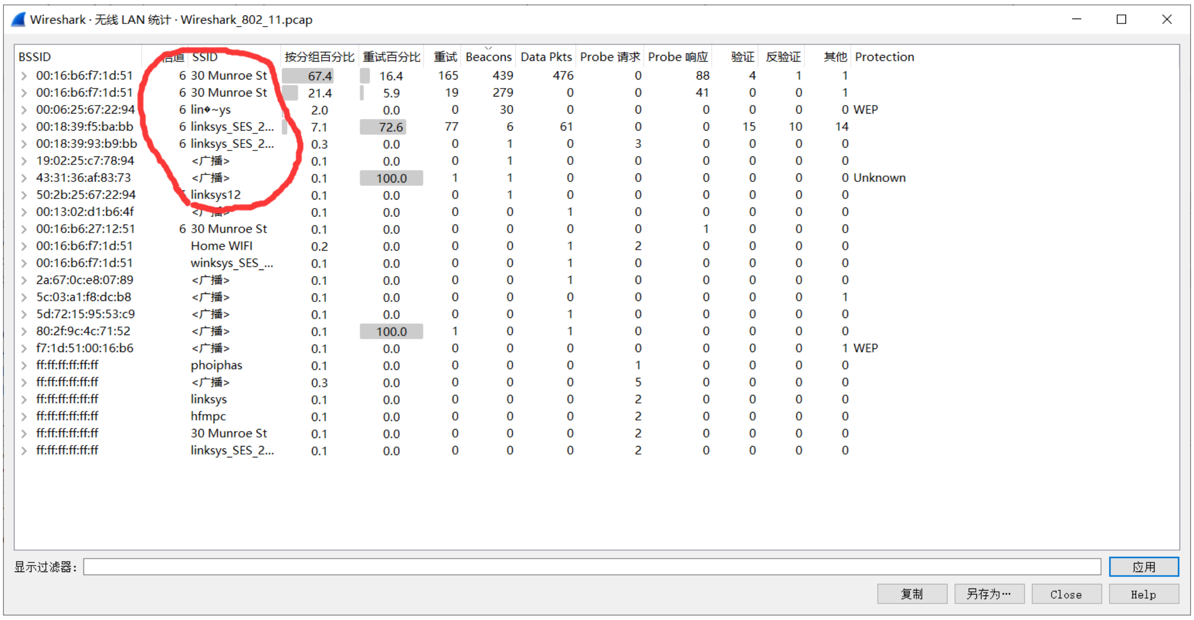
Q3: How many APs the wireless laptop has received Beacon frames from? List their MAC addresses. Why the laptop can receive frames from an AP even though it does not associate with the AP?

A3:

SSID	MAC
30 Munroe St	00:16:b6:f7:1d:51
lin�~ys	00:06:25:67:22:94
linksys_SES_24086	00:18:39:f5:ba:bb
linksys_SES_24086	00:18:39:93:b9:bb
<广播>	19:02:25:c7:78:94
<广播>	43:31:36:af:83:73
linksys12	50:2b:25:67:22:94

原因： "802.11 标准要求每个 AP 周期性地发送信标帧(beacon frame)"，并且无线主机也可以执行主动扫描, 通过向位于无线主机范围内的所有 AP 广播探测帧完成。

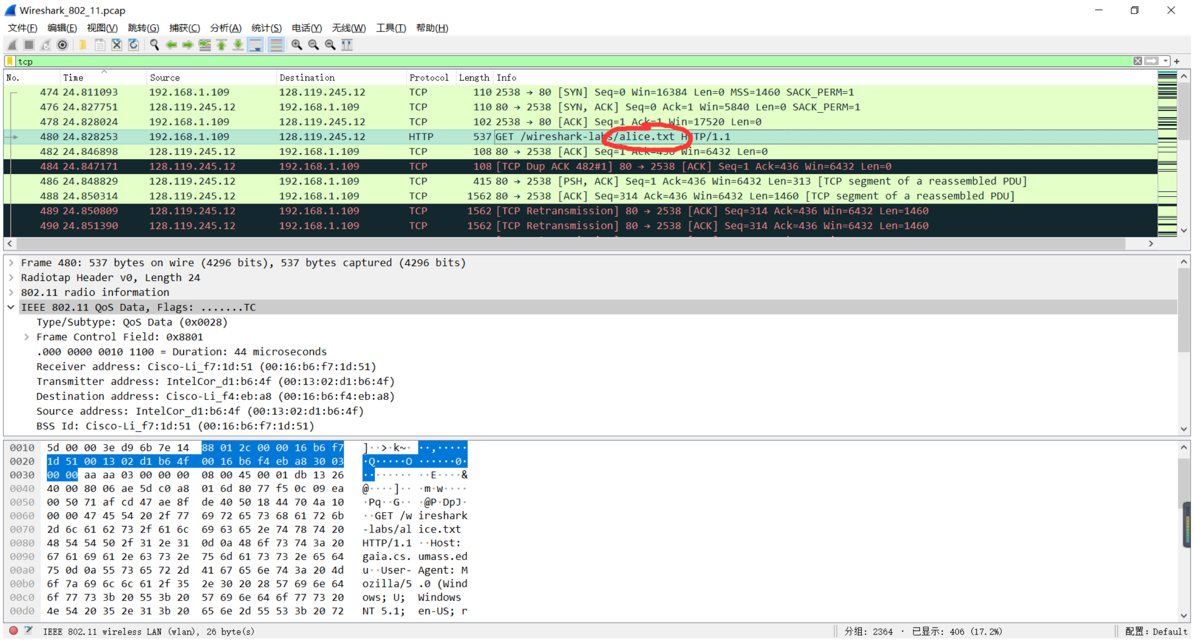
截图如下：



BSSID	信道	SSID	按分组百分比	重试百分比	重试	Beacons	Data Pkts	Probe 请求	Probe 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		linksys12	0.1	0.0	0	1	0	0	0	0	0	0	
00:13:02:d1:b6:4f		<广播>	0.1	0.0	0	0	1	0	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		Home WIFI	0.2	0.0	0	0	1	2	0	0	0	0	
00:16:b6:f7:1d:51		winksys_SES_...	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	
ff:ff:ff:ff:ff:ff		<广播>	0.3	0.0	0	0	0	5	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		hfmpc	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	

Q4: 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?

A4:如下图所示即为一个GET的http请求来请求alice.txt文件


Wireshark_802_11.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

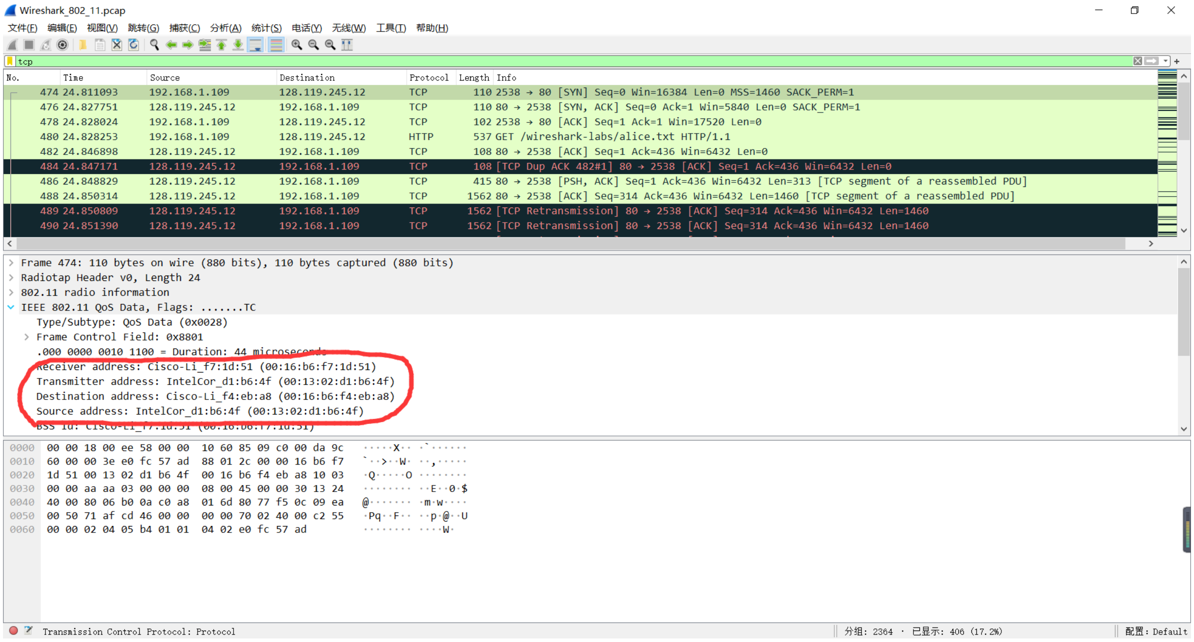
```
tcp
No.     Time          Source            Destination       Protocol  Length  Info
  474 24.811093   192.168.1.109     128.119.245.12    TCP        110 2538 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
  476 24.827751   128.119.245.12    192.168.1.109     TCP        110 80 → 2538 [SYN, 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
  482 24.846898   128.119.245.12    192.168.1.109     TCP        108 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
  484 24.847171   128.119.245.12    192.168.1.109     TCP        108 [TCP Dup ACK 482#1] 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
  486 24.848829   128.119.245.12    192.168.1.109     TCP        415 80 → 2538 [PSH, ACK] Seq=1 Ack=436 Win=6432 Len=313 [TCP segment of a reassembled PDU]
  488 24.850314   128.119.245.12    192.168.1.109     TCP       1562 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
  489 24.850809   128.119.245.12    192.168.1.109     TCP       1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460
  490 24.851390   128.119.245.12    192.168.1.109     TCP       1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460

> Frame 480: 537 bytes on wire (4296 bits), 537 bytes captured (4296 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 QoS Data, Flags: .......TC
    Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8801
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: 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)

0010  5d 00 00 3e d9 6b 7e 14  88 01 2c 00 00 16 b6 f7   ]··>·k~· ··,·····
0020  1d 51 00 13 02 d1 b6 4f  00 16 b6 f4 eb a8 30 03   ·Q·····O ······0·
0030  00 00 aa aa 03 00 00 00  08 00 45 00 01 db 13 26   ········ ··E····&
0040  40 00 80 06 ae 5d c0 a8  01 6d 80 77 f5 0c 09 ea   @····]·· ·m·w····
0050  00 50 71 af cd 47 ae 8f  de 40 50 18 44 70 4a 10   ·Pq··G·· ·@P·DpJ·
0060  00 00 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   ··GET /w ireshark
0070  2d 6c 61 62 73 2f 61 6c  69 63 65 2e 74 78 74 20   -labs/al ice.txt 
0080  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.1 ··Host: 
0090  67 61 69 61 2e 63 73 2e  75 6d 61 73 73 2e 65 64   gaia.cs. umass.ed
00a0  75 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   u··User- Agent: M
00b0  6f 7a 69 6c 6c 61 2f 35  2e 30 20 28 57 69 6e 64   ozilla/5 .0 (Wind
00c0  6f 77 73 3b 20 55 3b 20  57 69 6e 64 6f 77 73 20   ows; U;  Windows 
00d0  4e 54 20 35 2e 31 3b 20  65 6e 2d 55 53 3b 20 72   NT 5.1;  en-US; r

IEEE 802.11 wireless LAN (wlan), 26 byte(s)        分组: 2364 · 已显示: 406 (17.2%)        配置: Default
```

对应的第一个TCP session的SYN TCP segment是No.474报文，截图如下：


Wireshark_802_11.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

```
tcp
No.     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
  482 24.846898   128.119.245.12    192.168.1.109     TCP        108 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
  484 24.847171   128.119.245.12    192.168.1.109     TCP        108 [TCP Dup ACK 482#1] 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
  486 24.848829   128.119.245.12    192.168.1.109     TCP        415 80 → 2538 [PSH, ACK] Seq=1 Ack=436 Win=6432 Len=313 [TCP segment of a reassembled PDU]
  488 24.850314   128.119.245.12    192.168.1.109     TCP       1562 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
  489 24.850809   128.119.245.12    192.168.1.109     TCP       1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460
  490 24.851390   128.119.245.12    192.168.1.109     TCP       1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460

> Frame 474: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 QoS Data, Flags: .......TC
    Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8801
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: 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)

0000  00 00 18 00 ee 58 00 00  10 60 85 09 c0 00 da 9c   ·····X·· ·`······
0010  60 00 00 3e e0 fc 57 ad  88 01 2c 00 00 16 b6 f7   `··>··W· ··,·····
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·$
0040  40 00 80 06 b0 0a c0 a8  01 6d 80 77 f5 0c 09 ea   @······· ·m·w····
0050  00 50 71 af cd 46 00 00  00 00 70 02 40 00 c2 55   ·Pq··F·· ··p·@··U
0060  00 00 02 04 05 b4 01 01  04 02 e0 fc 57 ad         ········ ····W·

Transmission Control Protocol: Protocol        分组: 2364 · 已显示: 406 (17.2%)        配置: Default
```

故对应的三个MAC地址为

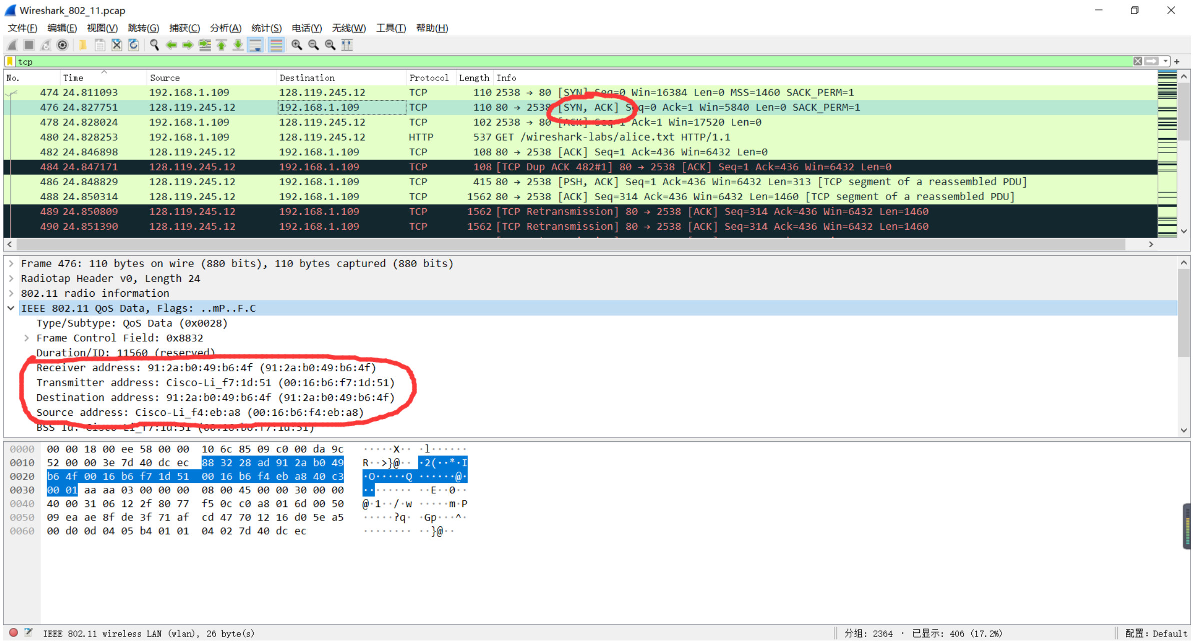
Receiver address	**00:16:b6:f7:1d:51**	**AP**

Source address	**00:13:02:d1:b6:4f**	**wireless laptop**

Destination address	**00:16:b6:f4:rb:a8**	**first-hop router**

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?

A5: No.476 segment即为所要查找的。截图如下：


Wireshark_802_11.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

tcp

```
No.   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
  482 24.846898  128.119.245.12  192.168.1.109   TCP      108 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
  484 24.847171  128.119.245.12  192.168.1.109   TCP      108 [TCP Dup ACK 482#1] 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
  486 24.848829  128.119.245.12  192.168.1.109   TCP      415 80 → 2538 [PSH, ACK] Seq=1 Ack=436 Win=6432 Len=313 [TCP segment of a reassembled PDU]
  488 24.850314  128.119.245.12  192.168.1.109   TCP     1562 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
  489 24.850809  128.119.245.12  192.168.1.109   TCP     1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460
  490 24.851390  128.119.245.12  192.168.1.109   TCP     1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460
```

```
> Frame 476: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 QoS Data, Flags: ..mP..F.C
    Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8832
    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)
```

```
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         ········ ··}@··
```

IEEE 802.11 wireless LAN (wlan), 26 byte(s) | 分组: 2364 · 已显示: 406 (17.2%) | 配置: Default

其中：

Receiver/Destination address	**91:2a:b0:49:b6:4f**	**wireless laptop**

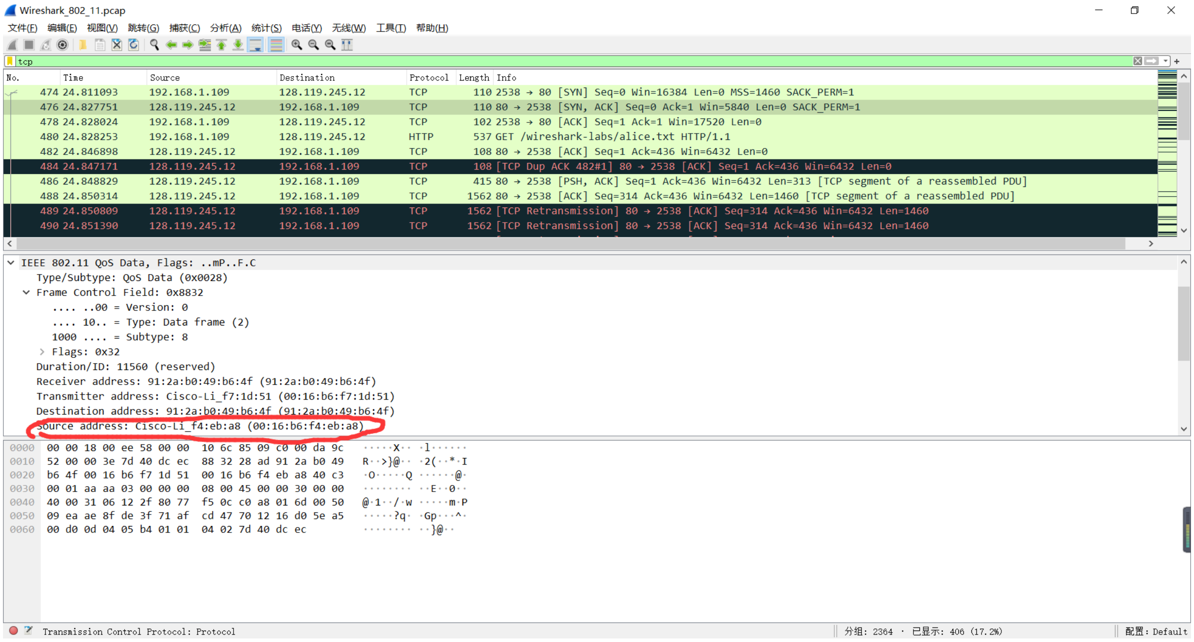
Transmitter address	**00:16:b6:f7:1d:51**	**AP**

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

Q6: For the above mentioned SYN-ACK segment, is the sender MAC address corresponds to the web server’s IP address? Why?

A6:不是对应的。原因如下：

sender的MAC为00:16:b6:f4:eb:a8，截图如下：


Wireshark_802_11.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

```
tcp
```

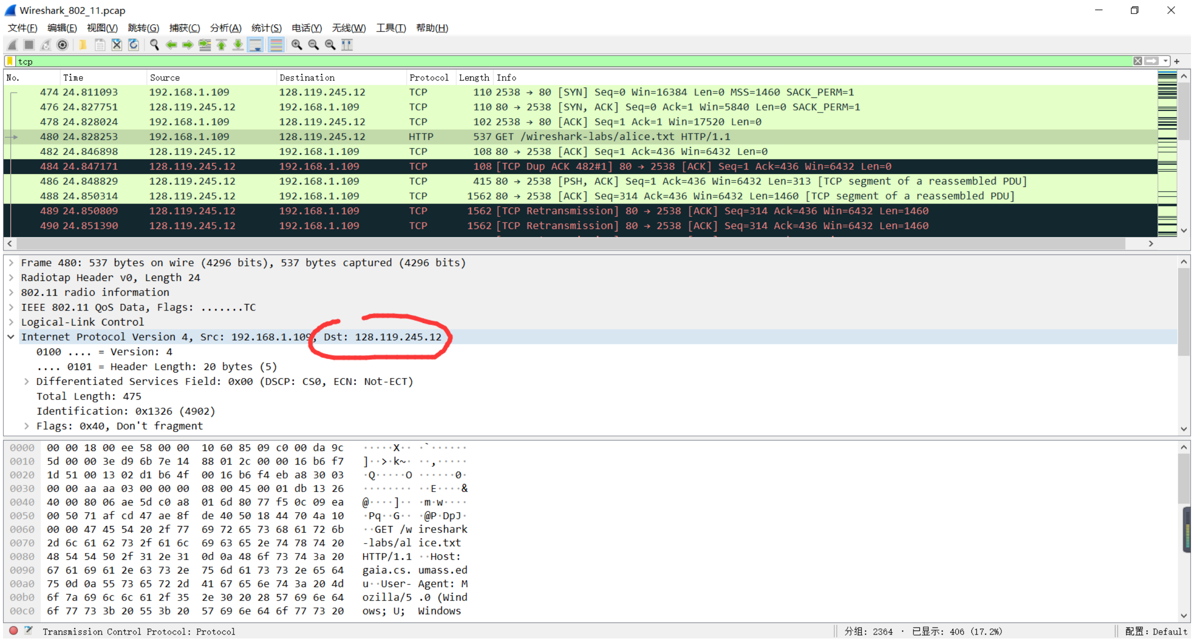
```
No.     Time       Source           Destination      Protocol Length Info
    474 24.811093  192.168.1.109    128.119.245.12   TCP       110 2538 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
    476 24.827751  128.119.245.12   192.168.1.109    TCP       110 80 → 2538 [SYN, ACK] Seq=0 Ack=1 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
    482 24.846898  128.119.245.12   192.168.1.109    TCP       108 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
    484 24.847171  128.119.245.12   192.168.1.109    TCP       108 [TCP Dup ACK 482#1] 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
    486 24.848829  128.119.245.12   192.168.1.109    TCP       415 80 → 2538 [PSH, ACK] Seq=1 Ack=436 Win=6432 Len=313 [TCP segment of a reassembled PDU]
    488 24.850314  128.119.245.12   192.168.1.109    TCP      1562 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
    489 24.850809  128.119.245.12   192.168.1.109    TCP      1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460
    490 24.851390  128.119.245.12   192.168.1.109    TCP      1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460
```

```
v IEEE 802.11 QoS Data, Flags: ..mP..F.C
    Type/Subtype: QoS Data (0x0028)
  v Frame Control Field: 0x8832
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      1000 .... = Subtype: 8
    > Flags: 0x32
    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)
```

```
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         ········ ··}@··
```

```
Transmission Control Protocol: Protocol        分组: 2364 · 已显示: 406 (17.2%)        配置: Default
```

web server的IP为128.119.245.12，截图如下：


Wireshark_802_11.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

```
tcp
```

```
No.     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
    482 24.846898  128.119.245.12   192.168.1.109    TCP       108 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
    484 24.847171  128.119.245.12   192.168.1.109    TCP       108 [TCP Dup ACK 482#1] 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
    486 24.848829  128.119.245.12   192.168.1.109    TCP       415 80 → 2538 [PSH, ACK] Seq=1 Ack=436 Win=6432 Len=313 [TCP segment of a reassembled PDU]
    488 24.850314  128.119.245.12   192.168.1.109    TCP      1562 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
    489 24.850809  128.119.245.12   192.168.1.109    TCP      1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460
    490 24.851390  128.119.245.12   192.168.1.109    TCP      1562 [TCP Retransmission] 80 → 2538 [ACK] Seq=314 Ack=436 Win=6432 Len=1460
```

```
> Frame 480: 537 bytes on wire (4296 bits), 537 bytes captured (4296 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
> IEEE 802.11 QoS Data, Flags: .......TC
> Logical-Link Control
v Internet Protocol Version 4, Src: 192.168.1.109, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 475
    Identification: 0x1326 (4902)
  > Flags: 0x40, Don't fragment
```

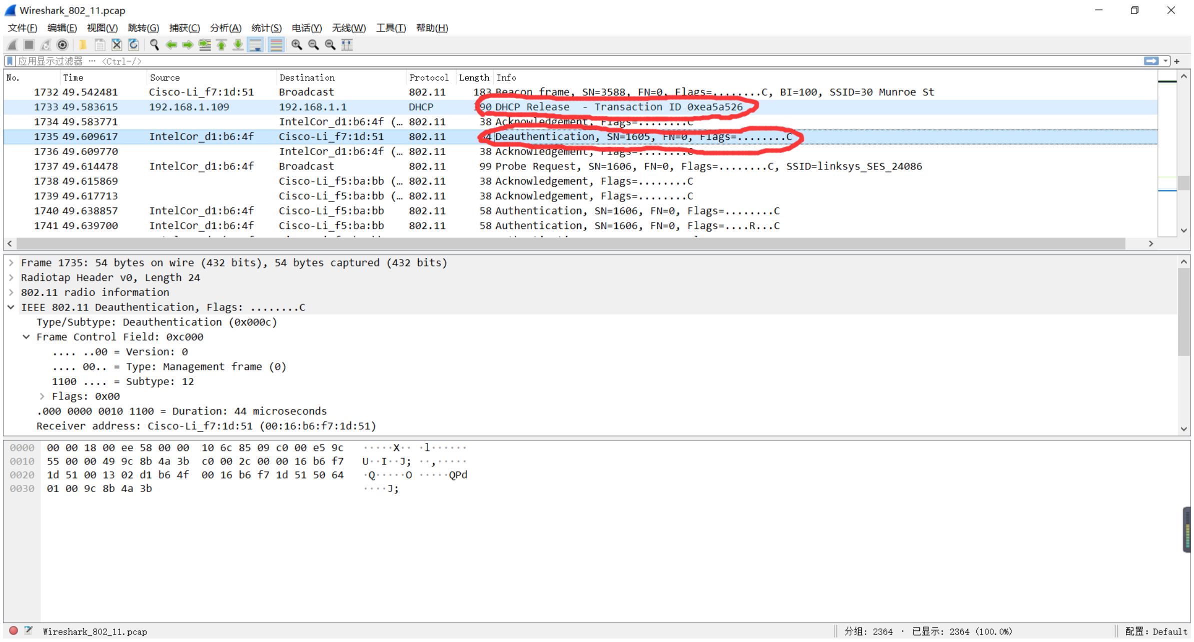
```
0000  00 00 18 00 ee 58 00 00  10 60 85 09 c0 00 da 9c   ·····X·· ·`······
0010  5d 00 00 3e d9 6b 7e 14  88 01 2c 00 00 16 b6 f7   ]··>·k~· ··,·····
0020  1d 51 00 13 02 d1 b6 4f  00 16 b6 f4 eb a8 30 03   ·Q·····O ······0·
0030  00 00 aa aa 03 00 00 00  08 00 45 00 01 db 13 26   ········ ··E····&
0040  40 00 80 06 ae 5d c0 a8  01 6d 80 77 f5 0c 09 ea   @····]·· ·m·w····
0050  00 50 71 af cd 47 ae 8f  de 40 50 18 44 70 4a 10   ·Pq··G·· ·@P·DpJ·
0060  00 00 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   ··GET /w ireshark
0070  2d 6c 61 62 73 2f 61 6c  69 63 65 2e 74 78 74 20   -labs/al ice.txt 
0080  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.1 ··Host: 
0090  67 61 69 61 2e 63 73 2e  75 6d 61 73 73 2e 65 64   gaia.cs. umass.ed
00a0  75 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   u··User- Agent: M
00b0  6f 7a 69 6c 6c 61 2f 35  2e 30 20 28 57 69 6e 64   ozilla/5 .0 (Wind
00c0  6f 77 73 3b 20 55 3b 20  57 69 6e 64 6f 77 73 20   ows; U;  Windows 
```

```
Transmission Control Protocol: Protocol        分组: 2364 · 已显示: 406 (17.2%)        配置: Default
```

服务器和sender不在同一个子网内部，所以sender的MAC地址取决于它子网的情况，如下一跳路由器的MAC地址。当跨越子网的时候，对应MAC地址会发生改变。

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?

A7:第一个动作是向DHCP服务器发送release以释放占用，第二个动作是向主机发送Deauthentication，截图如下：



Wireshark_802_11.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>

```
No.   Time      Source             Destination           Protocol Length Info
 1732 49.542481 Cisco-Li_f7:1d:51  Broadcast             802.11   183 Beacon frame, SN=3588, FN=0, Flags=........C, BI=100, SSID=30 Munroe St
 1733 49.583615 192.168.1.109      192.168.1.1           DHCP     190 DHCP Release  - Transaction ID 0xea5a526
 1734 49.583771                    IntelCor_d1:b6:4f (…  802.11    38 Acknowledgement, Flags=........C
 1735 49.609617 IntelCor_d1:b6:4f  Cisco-Li_f7:1d:51     802.11    54 Deauthentication, SN=1605, FN=0, Flags=........C
 1736 49.609770                    IntelCor_d1:b6:4f (…  802.11    38 Acknowledgement, Flags=........C
 1737 49.614478 IntelCor_d1:b6:4f  Broadcast             802.11    99 Probe Request, SN=1606, FN=0, Flags=........C, SSID=linksys_SES_24086
 1738 49.615869                    Cisco-Li_f5:ba:bb (…  802.11    38 Acknowledgement, Flags=........C
 1739 49.617713                    Cisco-Li_f5:ba:bb (…  802.11    38 Acknowledgement, Flags=........C
 1740 49.638857 IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb     802.11    58 Authentication, SN=1606, FN=0, Flags=........C
 1741 49.639700 IntelCor_d1:b6:4f  Cisco-Li_f5:ba:bb     802.11    58 Authentication, SN=1606, FN=0, Flags=....R...C

> Frame 1735: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
v IEEE 802.11 Deauthentication, Flags: ........C
    Type/Subtype: Deauthentication (0x000c)
  v Frame Control Field: 0xc000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1100 .... = Subtype: 12
    > Flags: 0x00
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)

0000  00 00 18 00 ee 58 00 00  10 6c 85 09 c0 00 e5 9c   ·····X·· ·l······
0010  55 00 00 49 9c 8b 4a 3b  c0 00 2c 00 00 16 b6 f7   U··I··J; ··,·····
0020  1d 51 00 13 02 d1 b6 4f  00 16 b6 f7 1d 51 50 64   ·Q·····O ·····QPd
0030  01 00 9c 8b 4a 3b                                  ····J;

Wireshark_802_11.pcap        分组: 2364 · 已显示: 2364 (100.0%)        配置: Default
```

Q8: Can you capture a similar trace? Why or why not?

A8:可以。 我们只需要在在相应的时刻, 按上面的操作步骤向相同的 AP 和 WebServer 发送相同的请求就可以完成。