Application Note
Wireshark with Linux/Mac

Document Number:	N1- 4947
Version:	1.0
Release Date:	2018/4/16

Murata Manufacturing Co., Ltd.

Revision History

Revision Number	Release Date	Comments
Revision 1.0	2018/4/16	Initial

Contents

1. About this Document

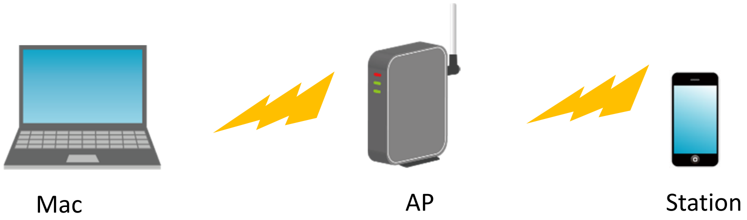
1.1. Purpose and Scope

This document provides the instructions to use Wireshark with Linux/Mac.

There are two methods to capture Wi-Fi packets.

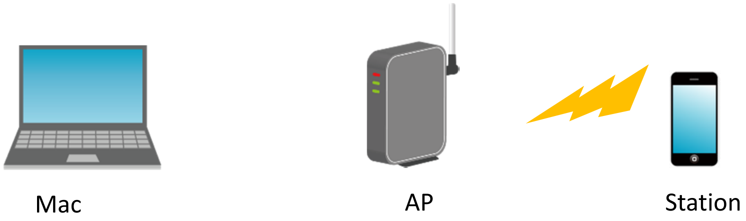
A) Connection Mode

Mac connects the target AP previously. Mac can capture packets on the connected channel.



B) Connectionless Mode

Mac needs not to connect the target AP, but must set the target channel from a terminal.



2. Set up Wireshark

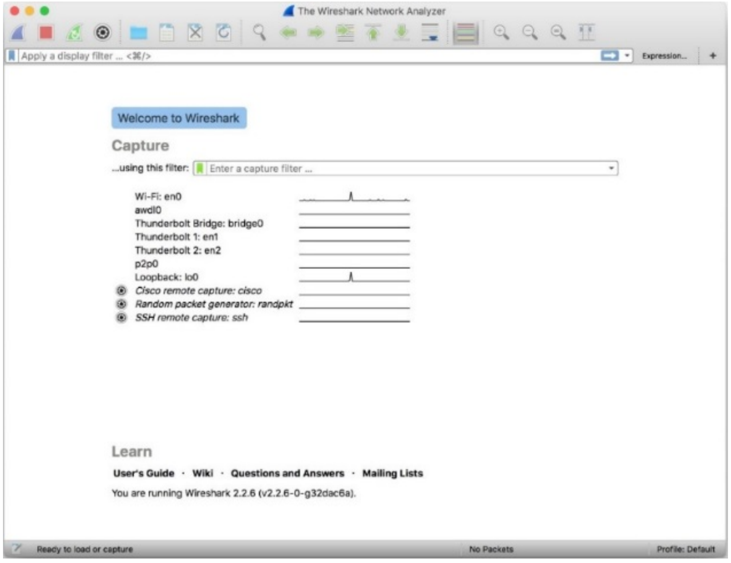
2.1. Download the Wireshark installer from WIRESHARK website

https://www.wireshark.org/

2.2. Install Wireshark application

2.3. Start Wireshark.

Start Wireshark by selecting *Application* > *Wireshark*. After startup, the following screen will appear.


The Wireshark Network Analyzer
Apply a display filter ... <⌘/>
Expression...
+

Welcome to Wireshark

Capture

...using this filter: Enter a capture filter ...

Wi-Fi: en0
awdl0
Thunderbolt Bridge: bridge0
Thunderbolt 1: en1
Thunderbolt 2: en2
p2p0
Loopback: lo0
◉ *Cisco remote capture: cisco*
◉ *Random packet generator: randpkt*
◉ *SSH remote capture: ssh*

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 2.2.6 (v2.2.6-0-g32dac6a).

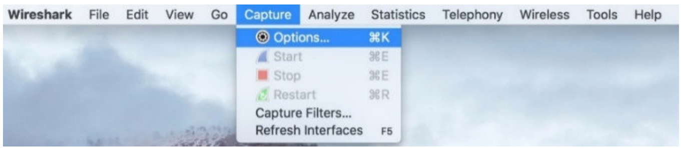
Ready to load or capture | No Packets | Profile: Default

3. Capture Wi-Fi packets

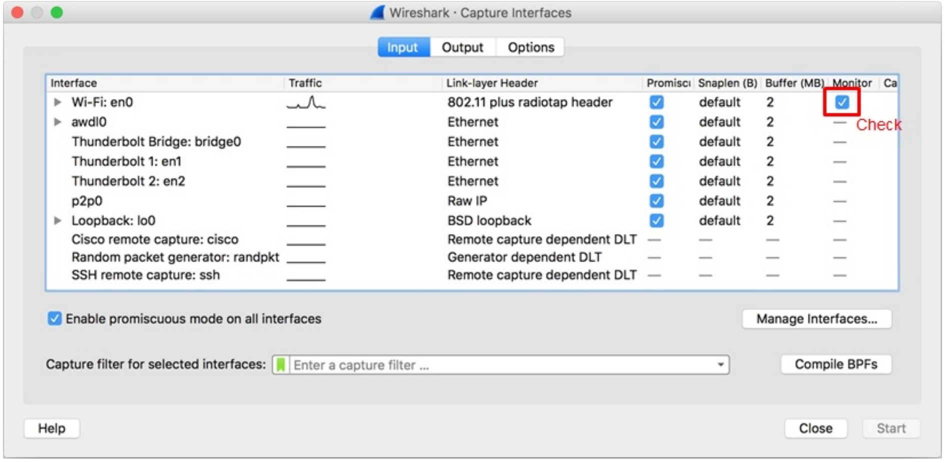
3.1. Connection Mode

A) Mac connect to the target AP.

B) Select "Capture" > "Options…" in menu.



C) Check "Monitor Mode" at Wi-Fi.



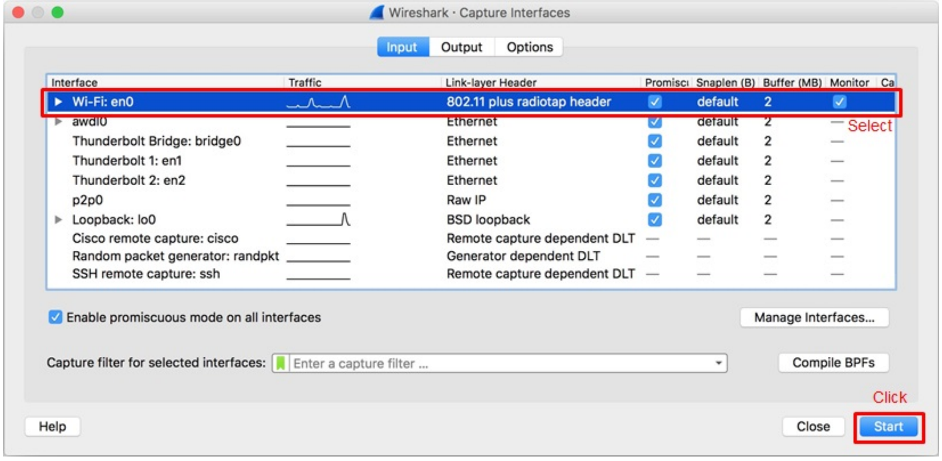
Interface	Traffic	Link-layer Header	Promiscı	Snaplen (B)	Buffer (MB)	Monitor	Ca
▸ Wi-Fi: en0		802.11 plus radiotap header	☑	default	2	☑	
▸ awdl0		Ethernet	☑	default	2	—	
Thunderbolt Bridge: bridge0		Ethernet	☑	default	2	—	
Thunderbolt 1: en1		Ethernet	☑	default	2	—	
Thunderbolt 2: en2		Ethernet	☑	default	2	—	
p2p0		Raw IP	☑	default	2	—	
▸ Loopback: lo0		BSD loopback	☑	default	2	—	
Cisco remote capture: cisco		Remote capture dependent DLT	—	—	—	—	
Random packet generator: randpkt		Generator dependent DLT	—	—	—	—	
SSH remote capture: ssh		Remote capture dependent DLT	—	—	—	—	

Check

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter …

D) Select "Wi-Fi" and click "Start" button.



Interface	Traffic	Link-layer Header	Promiscı	Snaplen (B)	Buffer (MB)	Monitor	Ca
▸ Wi-Fi: en0		802.11 plus radiotap header	☑	default	2	☑	
▸ awdl0		Ethernet	☑	default	2	—	
Thunderbolt Bridge: bridge0		Ethernet	☑	default	2	—	
Thunderbolt 1: en1		Ethernet	☑	default	2	—	
Thunderbolt 2: en2		Ethernet	☑	default	2	—	
p2p0		Raw IP	☑	default	2	—	
▸ Loopback: lo0		BSD loopback	☑	default	2	—	
Cisco remote capture: cisco		Remote capture dependent DLT	—	—	—	—	
Random packet generator: randpkt		Generator dependent DLT	—	—	—	—	
SSH remote capture: ssh		Remote capture dependent DLT	—	—	—	—	

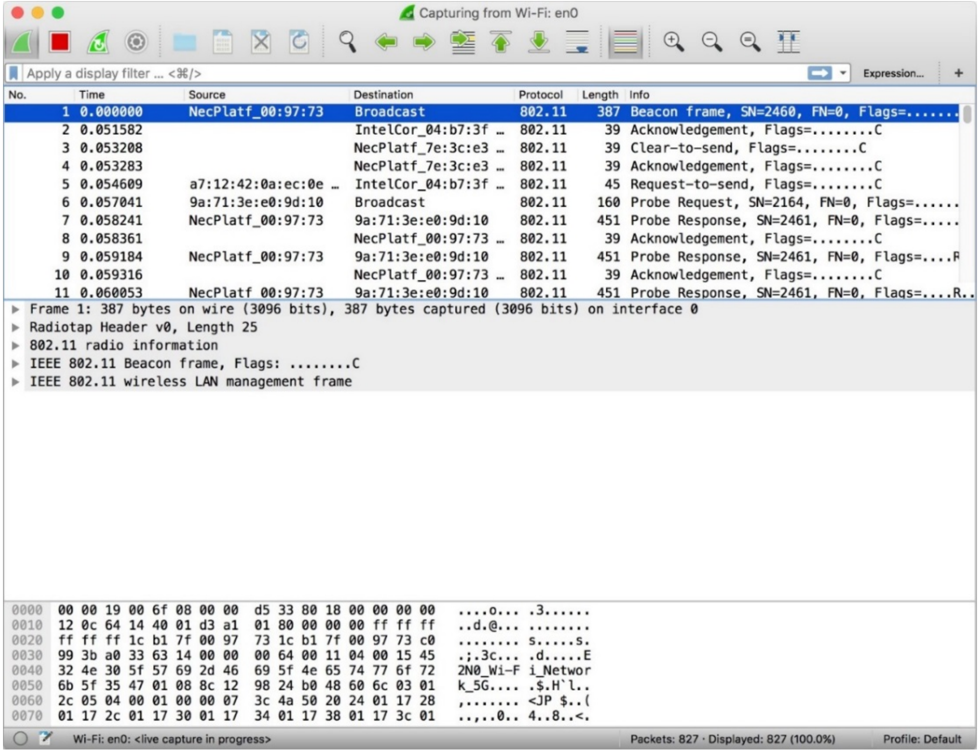
Select

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter …

Click

E) Ensure that the Wi-Fi capture window is displayed and Wi-Fi packets are captured.



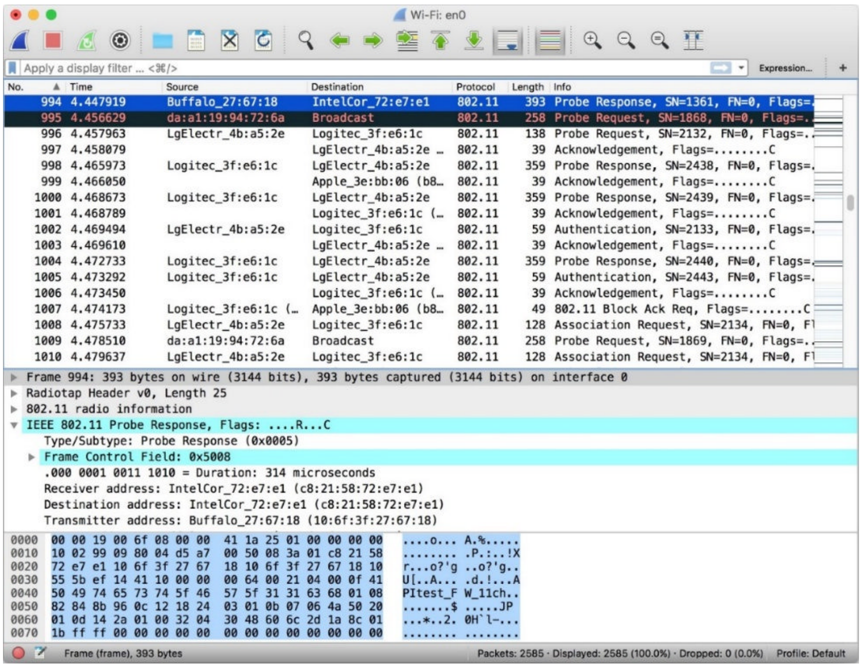
```
No.   Time      Source              Destination          Protocol Length Info
    1 0.000000  NecPlatf_00:97:73   Broadcast            802.11   387 Beacon frame, SN=2460, FN=0, Flags=......
    2 0.051582                      IntelCor_04:b7:3f …  802.11    39 Acknowledgement, Flags=........C
    3 0.053208                      NecPlatf_7e:3c:e3 …  802.11    39 Clear-to-send, Flags=........C
    4 0.053283                      NecPlatf_7e:3c:e3 …  802.11    39 Acknowledgement, Flags=........C
    5 0.054609  a7:12:42:0a:ec:0e … IntelCor_04:b7:3f …  802.11    45 Request-to-send, Flags=........C
    6 0.057041  9a:71:3e:e0:9d:10   Broadcast            802.11   160 Probe Request, SN=2164, FN=0, Flags=......
    7 0.058241  NecPlatf_00:97:73   9a:71:3e:e0:9d:10    802.11   451 Probe Response, SN=2461, FN=0, Flags=.....
    8 0.058361                      NecPlatf_00:97:73 …  802.11    39 Acknowledgement, Flags=........C
    9 0.059184  NecPlatf_00:97:73   9a:71:3e:e0:9d:10    802.11   451 Probe Response, SN=2461, FN=0, Flags=....R
   10 0.059316                      NecPlatf_00:97:73 …  802.11    39 Acknowledgement, Flags=........C
   11 0.060053  NecPlatf_00:97:73   9a:71:3e:e0:9d:10    802.11   451 Probe Response, SN=2461, FN=0, Flags=....R..
▶ Frame 1: 387 bytes on wire (3096 bits), 387 bytes captured (3096 bits) on interface 0
▶ Radiotap Header v0, Length 25
▶ 802.11 radio information
▶ IEEE 802.11 Beacon frame, Flags: ........C
▶ IEEE 802.11 wireless LAN management frame

0000  00 00 19 00 6f 08 00 00  d5 33 80 18 00 00 00 00   ....o... .3......
0010  12 0c 64 14 40 01 d3 a1  01 80 00 00 00 ff ff ff   ..d.@... ........
0020  ff ff ff 1c b1 7f 00 97  73 1c b1 7f 00 97 73 c0   ........ s.....s.
0030  99 3b a0 33 63 14 00 00  00 64 00 11 04 00 15 45   .;.3c... .d.....E
0040  32 4e 30 5f 57 69 2d 46  69 5f 4e 65 74 77 6f 72   2N0_Wi-F i_Networ
0050  6b 5f 35 47 01 08 8c 12  98 24 b0 48 60 6c 03 01   k_5G.... .$.H`l..
0060  2c 05 04 00 01 00 00 07  3c 4a 50 20 24 01 17 28   ,....... <JP $..(
0070  01 17 2c 01 17 30 01 17  34 01 17 38 01 17 3c 01   ..,..0.. 4..8..<.

Wi-Fi: en0: <live capture in progress>     Packets: 827 · Displayed: 827 (100.0%)     Profile: Default
```

F) A station (iPhone, smart phone, etc.) connects to the target AP.

G) Ensure that Wi-Fi packets such as Authentication, Association are captured.



```
No.  ▲ Time      Source              Destination          Protocol Length Info
   994 4.447919  Buffalo_27:67:18    IntelCor_72:e7:e1    802.11   393 Probe Response, SN=1361, FN=0, Flags=.
   995 4.456629  da:a1:19:94:72:6a   Broadcast            802.11   258 Probe Request, SN=1868, FN=0, Flags=.
   996 4.457963  LgElectr_4b:a5:2e   Logitec_3f:e6:1c     802.11   138 Probe Request, SN=2132, FN=0, Flags=..
   997 4.458079                      LgElectr_4b:a5:2e …  802.11    39 Acknowledgement, Flags=........C
   998 4.465973  Logitec_3f:e6:1c    LgElectr_4b:a5:2e    802.11   359 Probe Response, SN=2438, FN=0, Flags=.
   999 4.466050                      Apple_3e:bb:06 (b8…  802.11    39 Acknowledgement, Flags=........C
  1000 4.468673  Logitec_3f:e6:1c    LgElectr_4b:a5:2e    802.11   359 Probe Response, SN=2439, FN=0, Flags=.
  1001 4.468789                      Logitec_3f:e6:1c (…  802.11    39 Acknowledgement, Flags=........C
  1002 4.469494  LgElectr_4b:a5:2e   Logitec_3f:e6:1c     802.11    59 Authentication, SN=2133, FN=0, Flags=.
  1003 4.469610                      LgElectr_4b:a5:2e …  802.11    39 Acknowledgement, Flags=........C
  1004 4.472733  Logitec_3f:e6:1c    LgElectr_4b:a5:2e    802.11   359 Probe Response, SN=2440, FN=0, Flags=.
  1005 4.473292  Logitec_3f:e6:1c    LgElectr_4b:a5:2e    802.11    59 Authentication, SN=2443, FN=0, Flags=.
  1006 4.473450                      Logitec_3f:e6:1c (…  802.11    39 Acknowledgement, Flags=........C
  1007 4.474173  Logitec_3f:e6:1c (… Apple_3e:bb:06 (b8…  802.11    49 802.11 Block Ack Req, Flags=........C
  1008 4.475733  LgElectr_4b:a5:2e   Logitec_3f:e6:1c     802.11   128 Association Request, SN=2134, FN=0, Fl
  1009 4.478510  da:a1:19:94:72:6a   Broadcast            802.11   258 Probe Request, SN=1869, FN=0, Flags=..
  1010 4.479637  LgElectr_4b:a5:2e   Logitec_3f:e6:1c     802.11   128 Association Request, SN=2134, FN=0, Fl
▶ Frame 994: 393 bytes on wire (3144 bits), 393 bytes captured (3144 bits) on interface 0
▶ Radiotap Header v0, Length 25
▶ 802.11 radio information
▼ IEEE 802.11 Probe Response, Flags: ....R...C
    Type/Subtype: Probe Response (0x0005)
  ▶ Frame Control Field: 0x5008
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: IntelCor_72:e7:e1 (c8:21:58:72:e7:e1)
    Destination address: IntelCor_72:e7:e1 (c8:21:58:72:e7:e1)
    Transmitter address: Buffalo_27:67:18 (10:6f:3f:27:67:18)

0000  00 00 19 00 6f 08 00 00  41 1a 25 01 00 00 00 00   ....o... A.%.....
0010  10 02 99 09 80 04 d5 a7  00 50 08 3a 01 c8 21 58   ........ .P.:..!X
0020  72 e7 e1 10 6f 3f 27 67  18 10 6f 3f 27 67 18 10   r...o?'g ..o?'g..
0030  55 5b ef 14 41 10 00 00  00 64 00 21 04 00 0f 41   U[..A... .d.!...A
0040  50 49 74 65 73 74 5f 46  57 5f 31 31 63 68 01 08   PItest_F W_11ch..
0050  82 84 8b 96 0c 12 18 24  03 01 0b 07 06 4a 50 20   .......$ .....JP
0060  01 0d 14 2a 01 00 32 04  30 48 60 6c 2d 1a 8c 01   ...*..2. 0H`l-...
0070  1b ff ff 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........

Frame (frame), 393 bytes     Packets: 2585 · Displayed: 2585 (100.0%) · Dropped: 0 (0.0%)     Profile: Default
```

3.2. Connectionless Mode

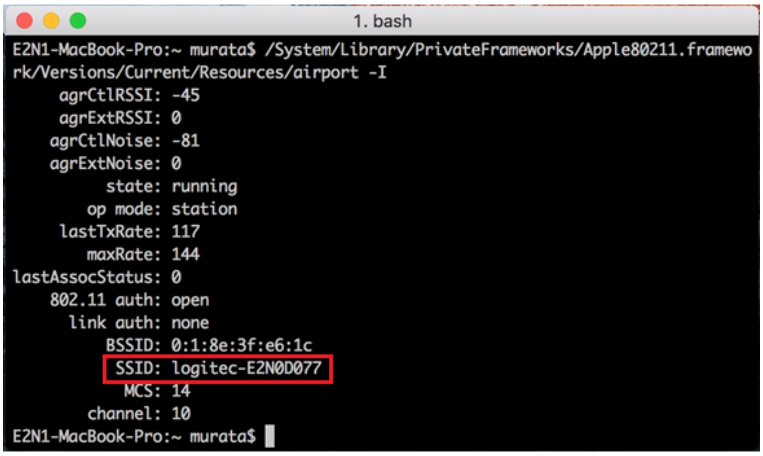
A) Start iTerm by selecting *Application > iTerm*.

B) Check the connection condition and change the channel to capture.

Input the following command:

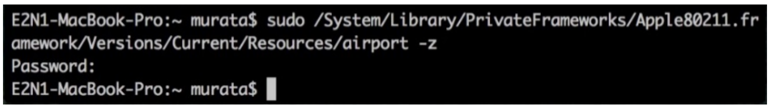
```
/System/Library/PrivateFrameworks/Apple80211.framework/Versions/Current/Resources/airport -I
```

The current state Mac Wi-Fi will appears.

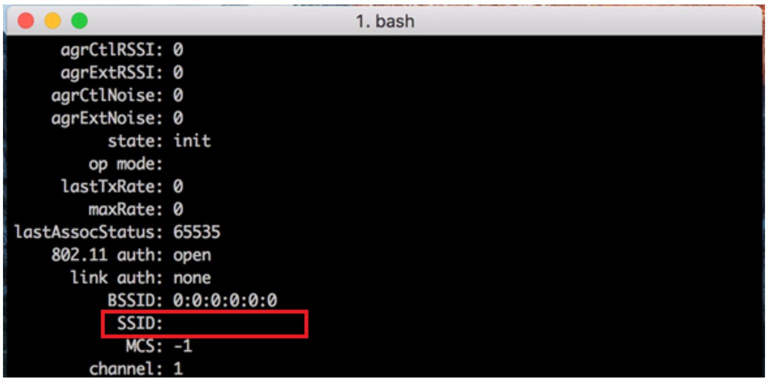


```
E2N1-MacBook-Pro:~ murata$ /System/Library/PrivateFrameworks/Apple80211.framewo
rk/Versions/Current/Resources/airport -I
     agrCtlRSSI: -45
     agrExtRSSI: 0
    agrCtlNoise: -81
    agrExtNoise: 0
          state: running
        op mode: station
     lastTxRate: 117
        maxRate: 144
lastAssocStatus: 0
    802.11 auth: open
      link auth: none
          BSSID: 0:1:8e:3f:e6:1c
           SSID: logitec-E2N0D077
            MCS: 14
        channel: 10
E2N1-MacBook-Pro:~ murata$ 
```

If SSID is not blank, input "airport -z" and ensure that SSID is cleared inputting "airport -I" again.



```
E2N1-MacBook-Pro:~ murata$ sudo /System/Library/PrivateFrameworks/Apple80211.fr
amework/Versions/Current/Resources/airport -z
Password:
E2N1-MacBook-Pro:~ murata$ 
```

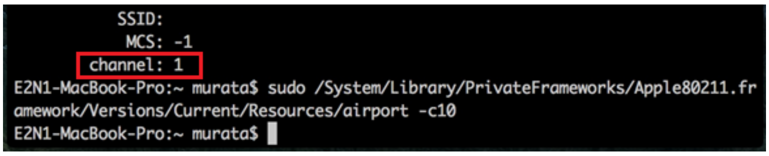


```
     agrCtlRSSI: 0
     agrExtRSSI: 0
    agrCtlNoise: 0
    agrExtNoise: 0
          state: init
        op mode: 
     lastTxRate: 0
        maxRate: 0
lastAssocStatus: 65535
    802.11 auth: open
      link auth: none
          BSSID: 0:0:0:0:0:0
           SSID: 
            MCS: -1
        channel: 1
```

If the current channel is different from the target AP's channel, input the following command:

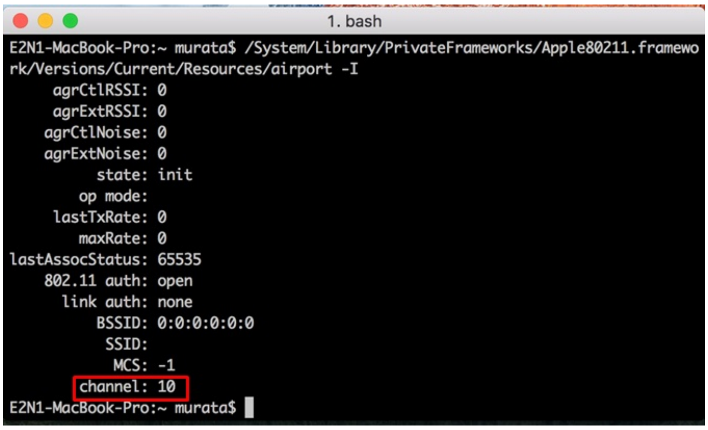
```
sudo /System/Library/PrivateFrameworks/Apple80211.framework/Versions/Current/Resources/airport -c10
```

Note: Set the channel using "-cxx". For example, "-c10" means 10ch.



```
           SSID: 
            MCS: -1
        channel: 1
E2N1-MacBook-Pro:~ murata$ sudo /System/Library/PrivateFrameworks/Apple80211.fr
amework/Versions/Current/Resources/airport -c10
E2N1-MacBook-Pro:~ murata$ 
```

Input "airport -I" and ensure that the channel is changed to 10.



```
E2N1-MacBook-Pro:~ murata$ /System/Library/PrivateFrameworks/Apple80211.framewo
rk/Versions/Current/Resources/airport -I
     agrCtlRSSI: 0
     agrExtRSSI: 0
    agrCtlNoise: 0
    agrExtNoise: 0
          state: init
        op mode:
     lastTxRate: 0
        maxRate: 0
lastAssocStatus: 65535
    802.11 auth: open
      link auth: none
          BSSID: 0:0:0:0:0:0
           SSID:
            MCS: -1
        channel: 10
E2N1-MacBook-Pro:~ murata$
```

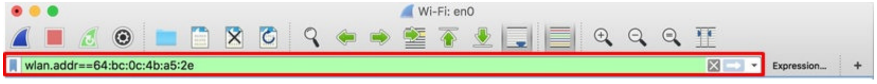
C) The following steps are the same as after Step B) of 3.1.

4. Set the filter under the specific condition

Example: Set the filter of the station mac address.

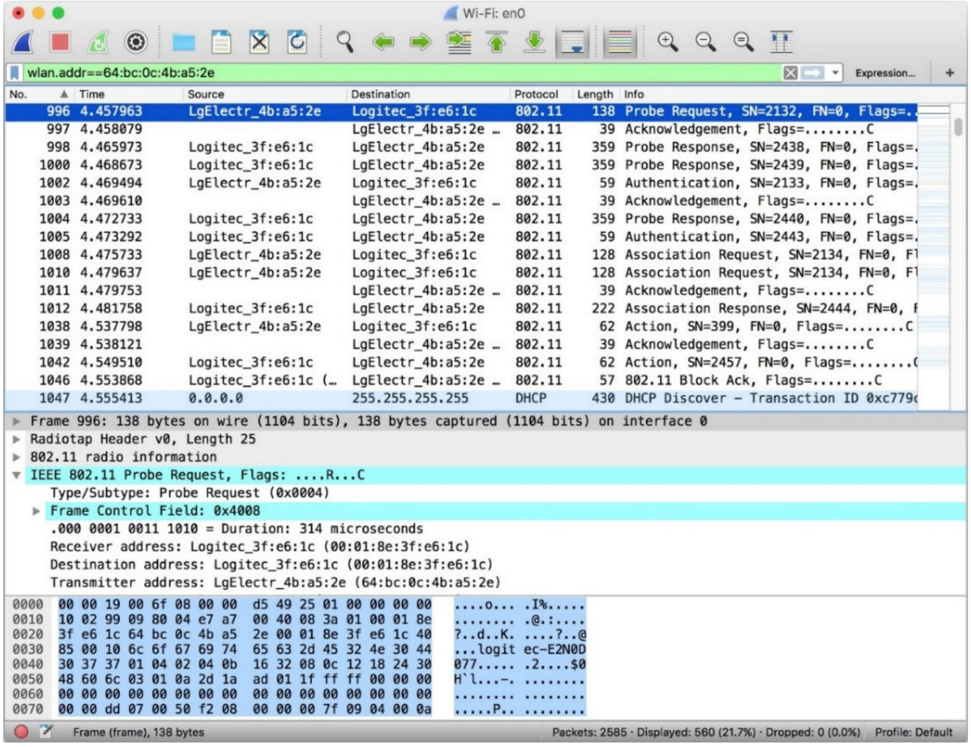
A) Input the following string in the "Apply a display filter" window.

wlan.addr == XX:XX:XX:XX:XX:XX



wlan.addr==64:bc:0c:4b:a5:2e

B) Check the filtered packets.



wlan.addr==64:bc:0c:4b:a5:2e

```
No.   ▲ Time        Source                Destination           Protocol  Length  Info
  996 4.457963     LgElectr_4b:a5:2e     Logitec_3f:e6:1c      802.11     138 Probe Request, SN=2132, FN=0, Flags=.
  997 4.458079                           LgElectr_4b:a5:2e …   802.11      39 Acknowledgement, Flags=........C
  998 4.465973     Logitec_3f:e6:1c      LgElectr_4b:a5:2e     802.11     359 Probe Response, SN=2438, FN=0, Flags=.
 1000 4.468673     Logitec_3f:e6:1c      LgElectr_4b:a5:2e     802.11     359 Probe Response, SN=2439, FN=0, Flags=.
 1002 4.469494     LgElectr_4b:a5:2e     Logitec_3f:e6:1c      802.11      59 Authentication, SN=2133, FN=0, Flags=.
 1003 4.469610                           LgElectr_4b:a5:2e …   802.11      39 Acknowledgement, Flags=........C
 1004 4.472733     Logitec_3f:e6:1c      LgElectr_4b:a5:2e     802.11     359 Probe Response, SN=2440, FN=0, Flags=.
 1005 4.473292     Logitec_3f:e6:1c      LgElectr_4b:a5:2e     802.11      59 Authentication, SN=2443, FN=0, Flags=.
 1008 4.475733     LgElectr_4b:a5:2e     Logitec_3f:e6:1c      802.11     128 Association Request, SN=2134, FN=0, Fl
 1010 4.479637     LgElectr_4b:a5:2e     Logitec_3f:e6:1c      802.11     128 Association Request, SN=2134, FN=0, Fl
 1011 4.479753                           LgElectr_4b:a5:2e …   802.11      39 Acknowledgement, Flags=........C
 1012 4.481758     Logitec_3f:e6:1c      LgElectr_4b:a5:2e     802.11     222 Association Response, SN=2444, FN=0, F
 1038 4.537798     LgElectr_4b:a5:2e     Logitec_3f:e6:1c      802.11      62 Action, SN=399, FN=0, Flags=........C
 1039 4.538121                           LgElectr_4b:a5:2e …   802.11      39 Acknowledgement, Flags=........C
 1042 4.549510     Logitec_3f:e6:1c      LgElectr_4b:a5:2e     802.11      62 Action, SN=2457, FN=0, Flags=........(
 1046 4.553868     Logitec_3f:e6:1c (…   LgElectr_4b:a5:2e …   802.11      57 802.11 Block Ack, Flags=........C
 1047 4.555413     0.0.0.0               255.255.255.255       DHCP       430 DHCP Discover - Transaction ID 0xc779c
```

```
▶ Frame 996: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface 0
▶ Radiotap Header v0, Length 25
▶ 802.11 radio information
▼ IEEE 802.11 Probe Request, Flags: ....R...C
    Type/Subtype: Probe Request (0x0004)
  ▶ Frame Control Field: 0x4008
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: Logitec_3f:e6:1c (00:01:8e:3f:e6:1c)
    Destination address: Logitec_3f:e6:1c (00:01:8e:3f:e6:1c)
    Transmitter address: LgElectr_4b:a5:2e (64:bc:0c:4b:a5:2e)
```

```
0000  00 00 19 00 6f 08 00 00  d5 49 25 01 00 00 00 00   ....o... .I%.....
0010  10 02 99 09 80 04 e7 a7  00 40 08 3a 01 00 01 8e   ........ .@.:....
0020  3f e6 1c 64 bc 0c 4b a5  2e 00 01 8e 3f e6 1c 40   ?..d..K. ....?..@
0030  85 00 10 6c 6f 67 69 74  65 63 2d 45 32 4e 30 44   ...logit ec-E2N0D
0040  30 37 37 01 04 02 04 0b  16 32 08 0c 12 18 24 30   077..... .2....$0
0050  48 60 6c 03 01 0a 2d 1a  ad 01 1f ff ff 00 00 00   H`l...-. ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 dd 07 00 50 f2 08  00 00 00 7f 09 04 00 0a   .....P.. ........
```

Frame (frame), 138 bytes   Packets: 2585 · Displayed: 560 (21.7%) · Dropped: 0 (0.0%)   Profile: Default

(END)