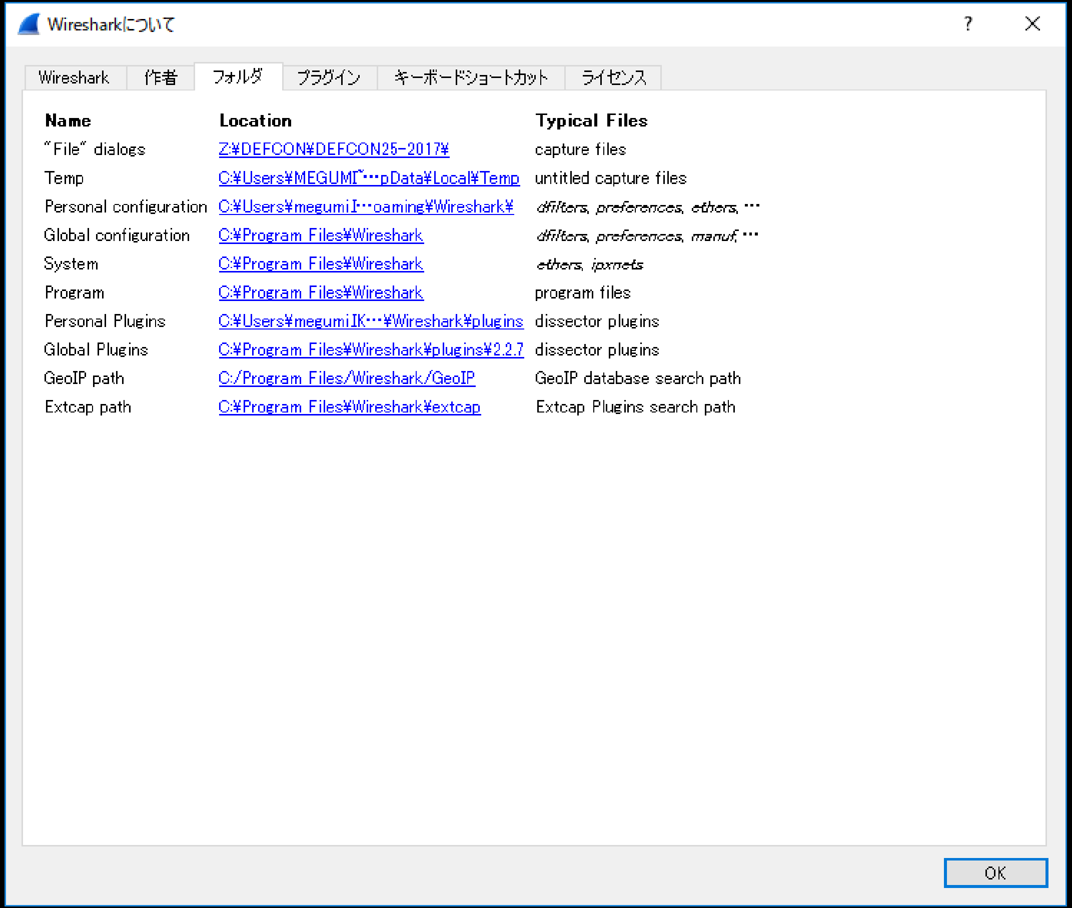
Basic workshop of IEEE802.11 packet dissection

Sample trace and supplemental files are located
http://www.ikeriri.ne.jp/download/defcon

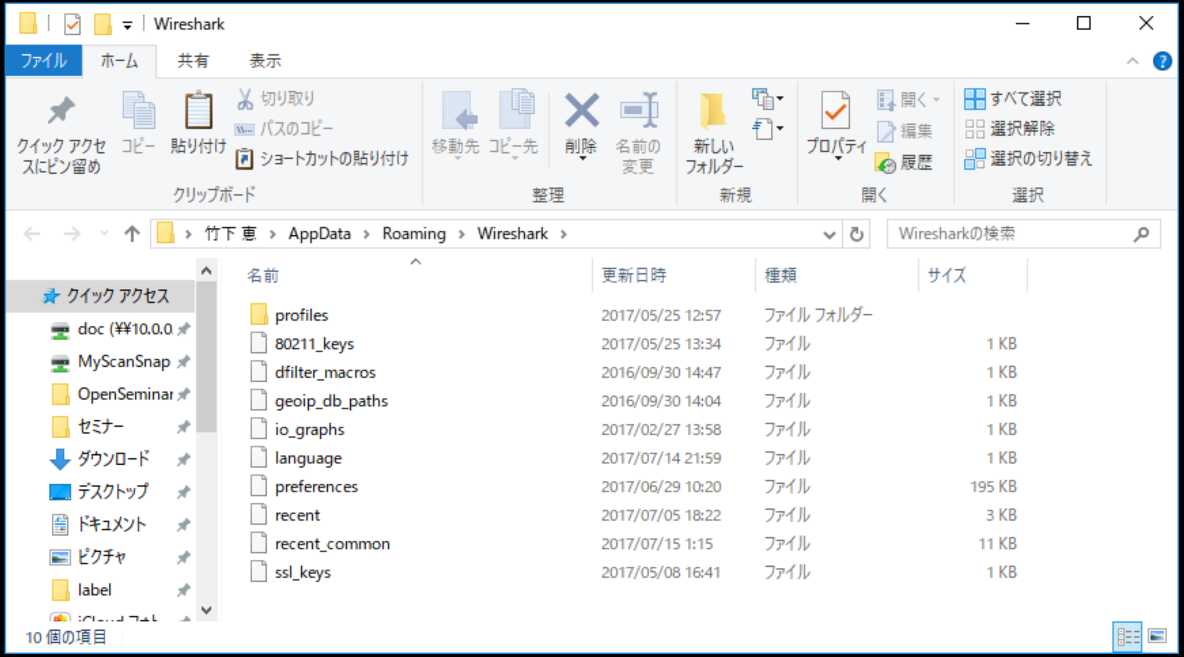
Megumi Takeshita
Packet Otaku | ikeriri network service co.,ltd

Please cooperate clearing the environments

- Open Wireshark
- Help > About Wireshark > Folder
- Open link of Personal configuration
- Clear files and copy the profile



Name	Location	Typical Files
“File” dialogs	Z:¥DEFCON¥DEFCON25-2017¥	capture files
Temp	C:¥Users¥MEGUMI˜…pData¥Local¥Temp	untitled capture files
Personal configuration	C:¥Users¥megumiI…oaming¥Wireshark¥	*dfilters, preferences, ethers,* …
Global configuration	C:¥Program Files¥Wireshark	*dfilters, preferences, manuf,* …
System	C:¥Program Files¥Wireshark	*ethers, ipxnets*
Program	C:¥Program Files¥Wireshark	program files
Personal Plugins	C:¥Users¥megumiIK…¥Wireshark¥plugins	dissector plugins
Global Plugins	C:¥Program Files¥Wireshark¥plugins¥2.2.7	dissector plugins
GeoIP path	C:/Program Files/Wireshark/GeoIP	GeoIP database search path
Extcap path	C:¥Program Files¥Wireshark¥extcap	Extcap Plugins search path

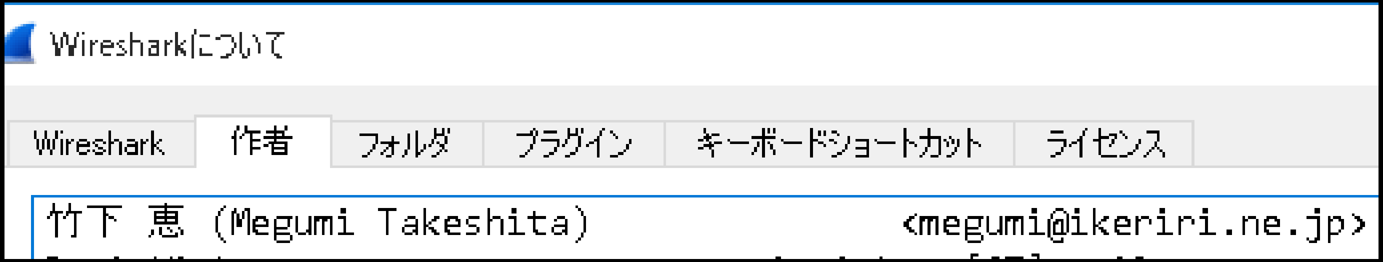


名前	更新日時	種類	サイズ
profiles	2017/05/25 12:57	ファイル フォルダー	
80211_keys	2017/05/25 13:34	ファイル	1 KB
dfilter_macros	2016/09/30 14:47	ファイル	1 KB
geoip_db_paths	2016/09/30 14:04	ファイル	1 KB
io_graphs	2017/02/27 13:58	ファイル	1 KB
language	2017/07/14 21:59	ファイル	1 KB
preferences	2017/06/29 10:20	ファイル	195 KB
recent	2017/07/05 18:22	ファイル	3 KB
recent_common	2017/07/15 1:15	ファイル	11 KB
ssl_keys	2017/05/08 16:41	ファイル	1 KB

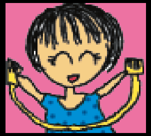
Megumi Takeshita, ikeriri network service a.k.a. packet otaku

パケットキャプチャ
実践技術
第2版
packet capture
WIRESHARK
Wiresharkの日本語化担当者が
パケット取得・解析のノウハウを徹底公開!

- Founder, ikeriri network service co.,ltd
- Wrote 10+ books of Wireshark and capturing and network analysis.
- Reseller of Riverbed Technology (former CACE technologies) and Metageek, Dualcomm etc. in Japan
- Contributor to Wireshark project
  ex. translator of QT Wireshark into Japanese



竹下 恵 (Megumi Takeshita) <megumi@ikeriri.ne.jp>

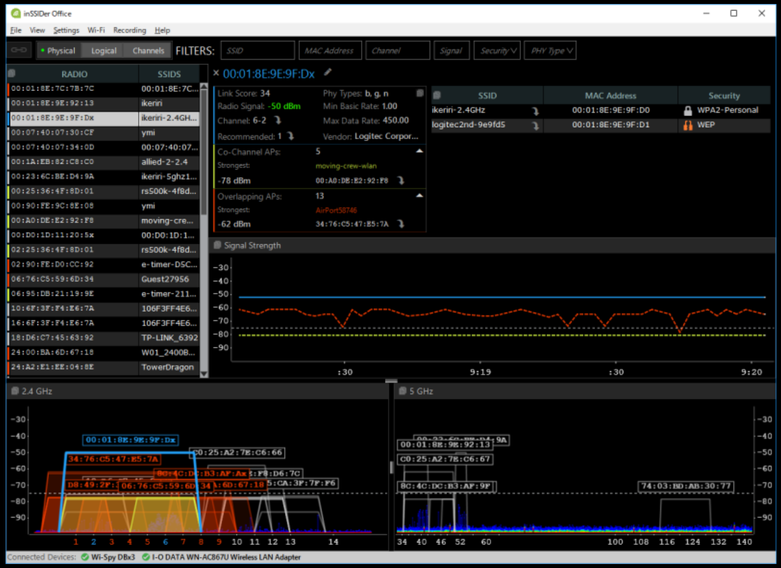


Workshop index (60 min)

We play this workshop in offline (no internet access)

0. Live RF Demonstration (6 min)
1. Collecting Wireless information using Windows (6 min)
2. Checking 2 types of physical layer (6 min)
3. Picking up basic link-up process (10 min)
4. Decrypting WPA2(PSK) (6 min)
5. Troubleshooting (12 min)
   - #1 my WiiU failed to connect AP (6 min)
   - #2 Wi-Fi connection is down ? (6 min)
6. Inspecting suspicious packets. (6 min)

#0 Live RF Demonstration



RADIO	SSIDS
00:01:8E:7C:7B:7C	00:01:8E:7C...
00:01:8E:9E:92:13	ikeriri
00:01:8E:9E:9F:Dx	ikeriri-2.4GH...
00:07:40:07:30:CF	ymi
00:07:40:07:34:0D	00:07:40:07...
00:1A:EB:82:C8:C0	allied-2-2.4
00:23:6C:BE:D4:9A	ikeriri-5ghz1...
00:25:36:4F:8D:01	rs500k-4f8d...
00:90:FE:9C:8E:08	ymi
00:A0:DE:E2:92:F8	moving-cre...
00:D0:1D:11:20:5x	00:D0:1D:1...
02:25:36:4F:8D:01	rs500k-4f8d...
02:90:FE:D0:CC:92	e-timer-D5C...
06:76:C5:59:6D:34	Guest27956
06:95:DB:21:19:9E	e-timer-211...
10:6F:3F:F4:E6:7A	106F3FF4E6...
16:6F:3F:F4:E6:7A	106F3FF4E6...
18:D6:C7:45:63:92	TP-LINK_6392
24:00:BA:6D:67:18	W01_2400B...
24:A2:E1:EE:04:8E	TowerDragon

00:01:8E:9E:9F:Dx

Link Score: 34
Radio Signal: -50 dBm
Channel: 6-2
Recommended: 1
Phy Types: b, g, n
Min Basic Rate: 1.00
Max Data Rate: 450.00
Vendor: Logitec Corpor...
Co-Channel APs: 5
Strongest: moving-crew-wlan
-78 dBm 00:A0:DE:E2:92:F8
Overlapping APs: 13
Strongest: AirPort58746
-62 dBm 34:76:C5:47:E5:7A

SSID	MAC Address	Security
ikeriri-2.4GHz	00:01:8E:9E:9F:D0	WPA2-Personal
logitec2nd-9e9fd5	00:01:8E:9E:9F:D1	WEP

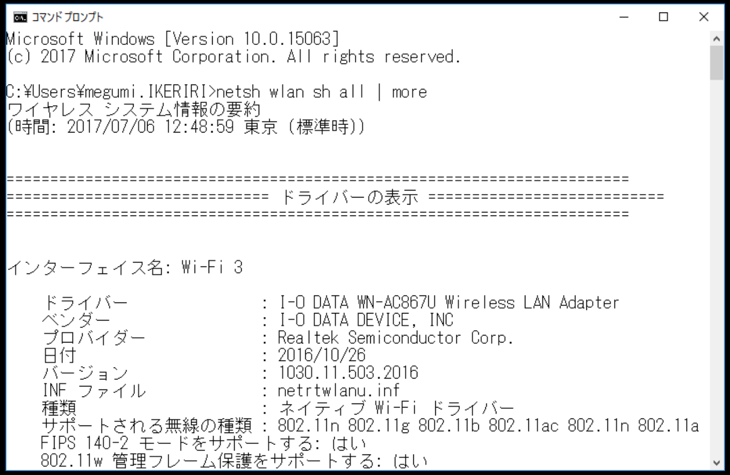
Connected Devices: ✓ Wi-Spy DBx3 ✓ I-O DATA WN-AC867U Wireless LAN Adapter

- Now I introduce the live wireless environment at Packet Hacking Village, DEFCON 25, Vegas
- At First it is good idea to collect RF signal at 2.4GHz and 5GHz, including other waves except for Wi-Fi
- We can know channel usage, and other wave without IEEE802.11
- Now I test some devices that does not use Wi-Fi, but use 2.4GHz.
- Next collecting some important packet such as Deauthentication and Disassociation,
- Using capture filter is the best way to capture the specified packet
- Using AirPcap and dumpcap, you can collect only Deauthentication/Disassociation
  tshark -i 1 -f “subtype deauth or subtype disassoc"

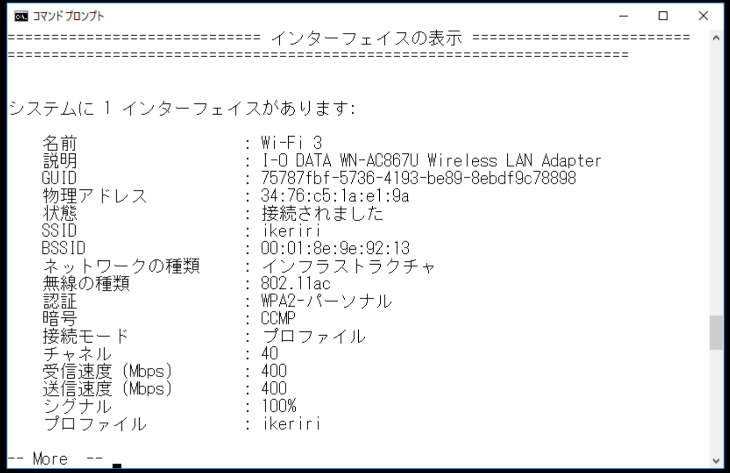
#1 Collecting Wireless information using Windows

- You want to collect Wi-Fi information
- But you have just a Windows PC, no apps
- Please open command prompt and collect Wi-Fi information.
- You need to collect
  Driver description / Driver version / Interface name / MAC address
  SSID / BSSID / authentication/encryption / Channel / speed /signal
  and other AP's information (SSID / BSSID / Power / Authentication / encryption)
- Hint "netsh"

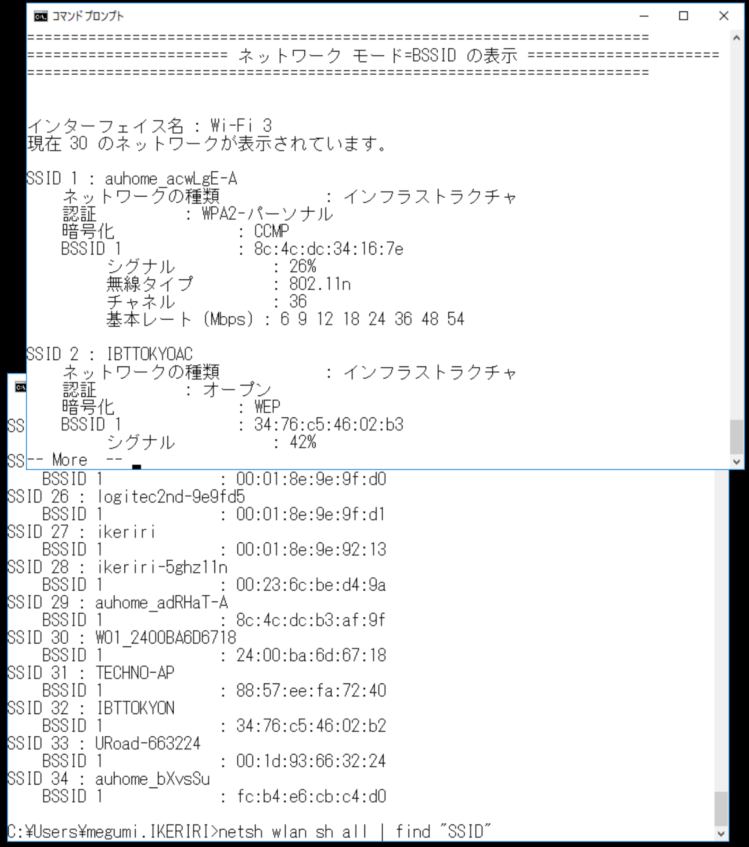
- “netsh wlan sh all | more “
- Driver section
  Driver name, version,
  Physical types of Wi-Fi
- Interface section
  MAC Address
  connected or not connected
  SSID / BSSID / network types
  PHY / Channel / Speed / Power
- Network mode = BSSID display section
  SSID / authentication / encryption / BSSID / Power /
  Channel / Rate
- Use redirect and pipe
  netsh wlan sh all | find “BSSID“ > BSSID.txt
  netsh wlan sh all | find “SSID” > SSIDandBSSID.txt



```
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:¥Users¥megumi.IKERIRI>netsh wlan sh all | more
ワイヤレス システム情報の要約
(時間: 2017/07/06 12:48:59 東京 (標準時))


=======================================================================
============================ ドライバーの表示 ==========================
=======================================================================


インターフェイス名: Wi-Fi 3

    ドライバー               : I-O DATA WN-AC867U Wireless LAN Adapter
    ベンダー                 : I-O DATA DEVICE, INC
    プロバイダー             : Realtek Semiconductor Corp.
    日付                     : 2016/10/26
    バージョン               : 1030.11.503.2016
    INF ファイル             : netrtwlanu.inf
    種類                     : ネイティブ Wi-Fi ドライバー
    サポートされる無線の種類 : 802.11n 802.11g 802.11b 802.11ac 802.11n 802.11a
    FIPS 140-2 モードをサポートする: はい
    802.11w 管理フレーム保護をサポートする: はい
```



```
=========================== インターフェイスの表示 ========================
=======================================================================


システムに 1 インターフェイスがあります:

    名前                   : Wi-Fi 3
    説明                   : I-O DATA WN-AC867U Wireless LAN Adapter
    GUID                   : 75787fbf-5736-4193-be89-8ebdf9c78898
    物理アドレス           : 34:76:c5:1a:e1:9a
    状態                   : 接続されました
    SSID                   : ikeriri
    BSSID                  : 00:01:8e:9e:92:13
    ネットワークの種類     : インフラストラクチャ
    無線の種類             : 802.11ac
    認証                   : WPA2-パーソナル
    暗号                   : CCMP
    接続モード             : プロファイル
    チャネル               : 40
    受信速度 (Mbps)        : 400
    送信速度 (Mbps)        : 400
    シグナル               : 100%
    プロファイル           : ikeriri

-- More  --
```

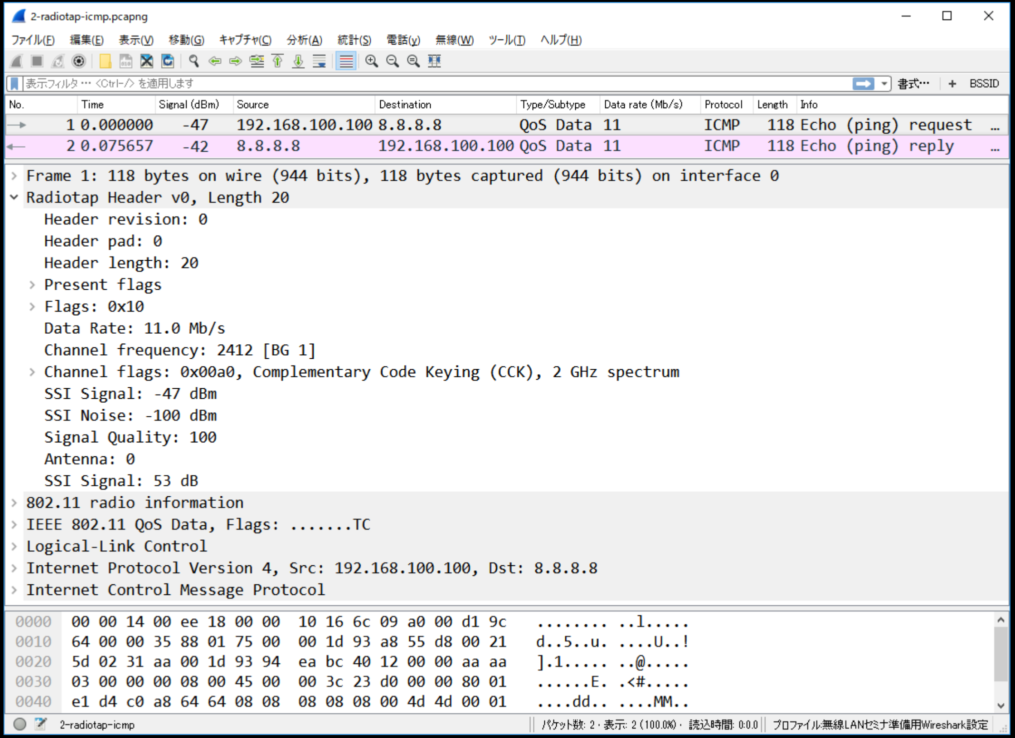


```
=======================================================================
===================== ネットワーク モード=BSSID の表示 ====================
=======================================================================


インターフェイス名 : Wi-Fi 3
現在 30 のネットワークが表示されています。

SSID 1 : auhome_acwLgE-A
    ネットワークの種類            : インフラストラクチャ
    認証            : WPA2-パーソナル
    暗号化                 : CCMP
    BSSID 1                : 8c:4c:dc:34:16:7e
         シグナル              : 26%
         無線タイプ            : 802.11n
         チャネル              : 36
         基本レート (Mbps) : 6 9 12 18 24 36 48 54

SSID 2 : IBTTOKYOAC
    ネットワークの種類            : インフラストラクチャ
    認証            : オープン
    暗号化                 : WEP
    BSSID 1                : 34:76:c5:46:02:b3
         シグナル              : 42%
-- More  --
```

```
SS
SS
   BSSID 1                 : 00:01:8e:9e:9f:d0
SSID 26 : logitec2nd-9e9fd5
   BSSID 1                 : 00:01:8e:9e:9f:d1
SSID 27 : ikeriri
   BSSID 1                 : 00:01:8e:9e:92:13
SSID 28 : ikeriri-5ghz11n
   BSSID 1                 : 00:23:6c:be:d4:9a
SSID 29 : auhome_adRHaT-A
   BSSID 1                 : 8c:4c:dc:b3:af:9f
SSID 30 : W01_2400BA6D6718
   BSSID 1                 : 24:00:ba:6d:67:18
SSID 31 : TECHNO-AP
   BSSID 1                 : 88:57:ee:fa:72:40
SSID 32 : IBTTOKYON
   BSSID 1                 : 34:76:c5:46:02:b2
SSID 33 : URoad-663224
   BSSID 1                 : 00:1d:93:66:32:24
SSID 34 : auhome_bXvsSu
   BSSID 1                 : fc:b4:e6:cb:c4:d0

C:¥Users¥megumi.IKERIRI>netsh wlan sh all | find "SSID"
```

#2 Checking 2 types of physical layer (6 min)

- Let`s open 2 trace files that contains same ICMP request/response “2-radiotap-icmp.pcapng” and “2-ppi-icmp.pcapng”
- please compare two packets especially at physical layer header, Radiotap header and Per Packet Information header

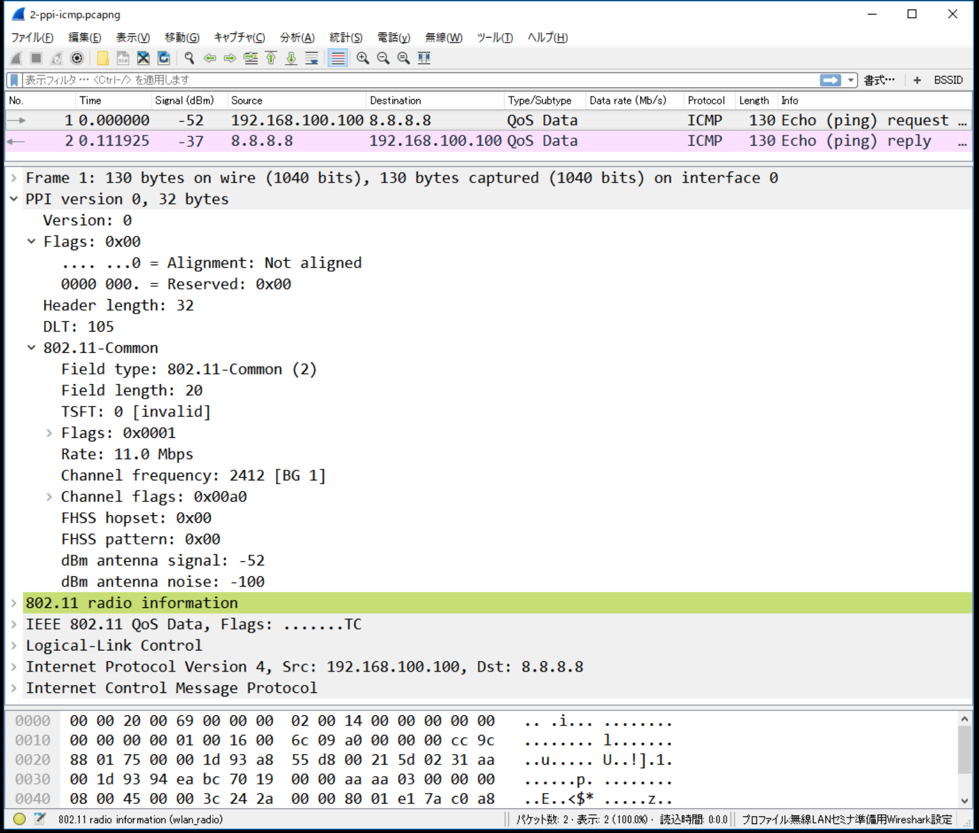

2-radiotap-icmp.pcapng
ファイル(F) 編集(E) 表示(V) 移動(G) キャプチャ(C) 分析(A) 統計(S) 電話(y) 無線(W) ツール(T) ヘルプ(H)
表示フィルタ … <Ctrl-/> を適用します
書式…
+ BSSID

```
No.     Time       Signal (dBm)  Source           Destination      Type/Subtype  Data rate (Mb/s)  Protocol  Length  Info
      1 0.000000   -47           192.168.100.100  8.8.8.8          QoS Data      11                ICMP      118     Echo (ping) request …
      2 0.075657   -42           8.8.8.8          192.168.100.100  QoS Data      11                ICMP      118     Echo (ping) reply   …
```

```
> Frame 1: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0
v Radiotap Header v0, Length 20
    Header revision: 0
    Header pad: 0
    Header length: 20
  > Present flags
  > Flags: 0x10
    Data Rate: 11.0 Mb/s
    Channel frequency: 2412 [BG 1]
  > Channel flags: 0x00a0, Complementary Code Keying (CCK), 2 GHz spectrum
    SSI Signal: -47 dBm
    SSI Noise: -100 dBm
    Signal Quality: 100
    Antenna: 0
    SSI Signal: 53 dB
> 802.11 radio information
> IEEE 802.11 QoS Data, Flags: .......TC
> Logical-Link Control
> Internet Protocol Version 4, Src: 192.168.100.100, Dst: 8.8.8.8
> Internet Control Message Protocol
```

```
0000  00 00 14 00 ee 18 00 00  10 16 6c 09 a0 00 d1 9c   ........ ..l.....
0010  64 00 00 35 88 01 75 00  00 1d 93 a8 55 d8 00 21   d..5..u. ....U..!
0020  5d 02 31 aa 00 1d 93 94  ea bc 40 12 00 00 aa aa   ].1..... ..@.....
0030  03 00 00 00 08 00 45 00  00 3c 23 d0 00 00 80 01   ......E. .<#.....
0040  e1 d4 c0 a8 64 64 08 08  08 08 08 00 4d 4d 00 01   ....dd.. ....MM..
```

2-radiotap-icmp ‖ パケット数: 2 · 表示: 2 (100.0%) · 読込時間: 0:0.0 ‖ プロファイル:無線LANセミナ準備用Wireshark設定

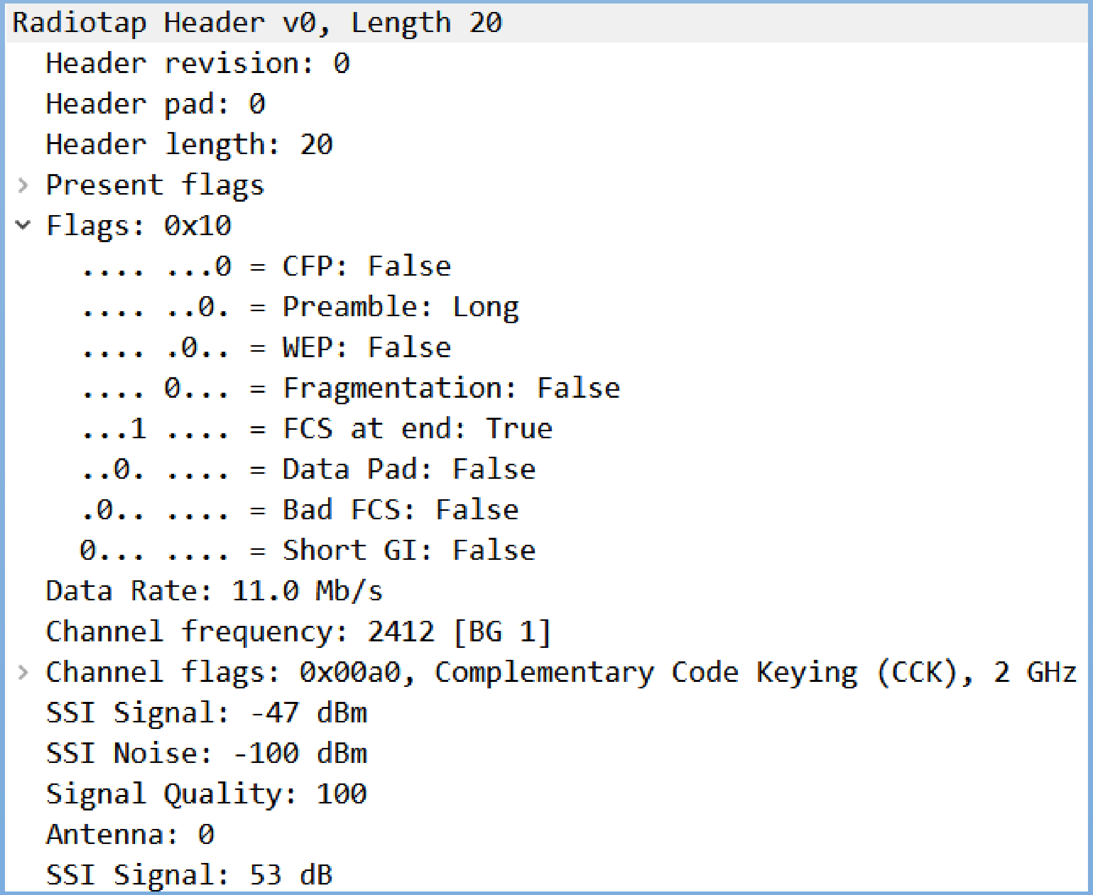
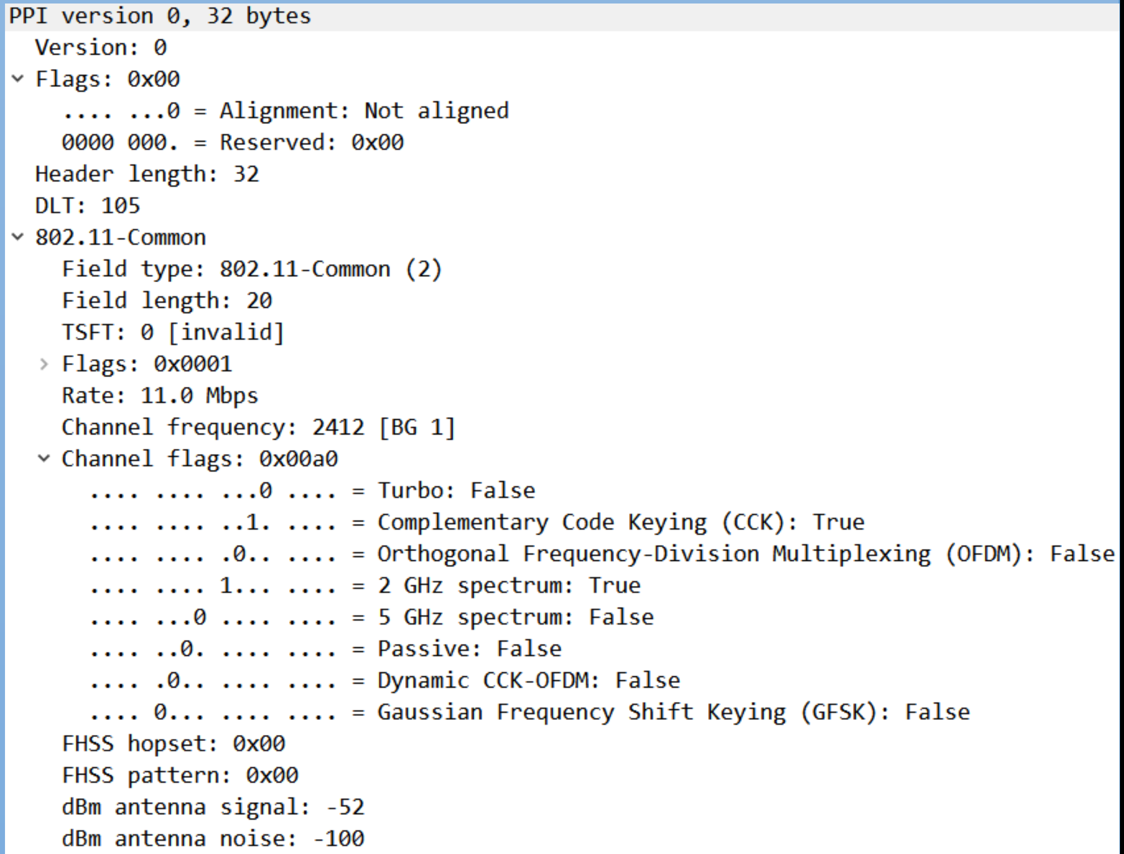

2-ppi-icmp.pcapng
ファイル(F) 編集(E) 表示(V) 移動(G) キャプチャ(C) 分析(A) 統計(S) 電話(y) 無線(W) ツール(T) ヘルプ(H)
表示フィルタ … <Ctrl-/> を適用します
書式…
+ BSSID

```
No.     Time       Signal (dBm)  Source           Destination      Type/Subtype  Data rate (Mb/s)  Protocol  Length  Info
      1 0.000000   -52           192.168.100.100  8.8.8.8          QoS Data                        ICMP      130     Echo (ping) request …
      2 0.111925   -37           8.8.8.8          192.168.100.100  QoS Data                        ICMP      130     Echo (ping) reply   …
```

```
> Frame 1: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface 0
v PPI version 0, 32 bytes
    Version: 0
  v Flags: 0x00
      .... ...0 = Alignment: Not aligned
      0000 000. = Reserved: 0x00
    Header length: 32
    DLT: 105
  v 802.11-Common
      Field type: 802.11-Common (2)
      Field length: 20
      TSFT: 0 [invalid]
    > Flags: 0x0001
      Rate: 11.0 Mbps
      Channel frequency: 2412 [BG 1]
    > Channel flags: 0x00a0
      FHSS hopset: 0x00
      FHSS pattern: 0x00
      dBm antenna signal: -52
      dBm antenna noise: -100
> 802.11 radio information
> IEEE 802.11 QoS Data, Flags: .......TC
> Logical-Link Control
> Internet Protocol Version 4, Src: 192.168.100.100, Dst: 8.8.8.8
> Internet Control Message Protocol
```

```
0000  00 00 20 00 69 00 00 00  02 00 14 00 00 00 00 00   .. .i... ........
0010  00 00 00 00 01 00 16 00  6c 09 a0 00 00 00 cc 9c   ........ l.......
0020  88 01 75 00 00 1d 93 a8  55 d8 00 21 5d 02 31 aa   ..u..... U..!].1.
0030  00 1d 93 94 ea bc 70 19  00 00 aa aa 03 00 00 00   ......p. ........
0040  08 00 45 00 00 3c 24 2a  00 00 80 01 e1 7a c0 a8   ..E..<$* .....z..
```

802.11 radio information (wlan_radio) ‖ パケット数: 2 · 表示: 2 (100.0%) · 読込時間: 0:0.0 ‖ プロファイル:無線LANセミナ準備用Wireshark設定

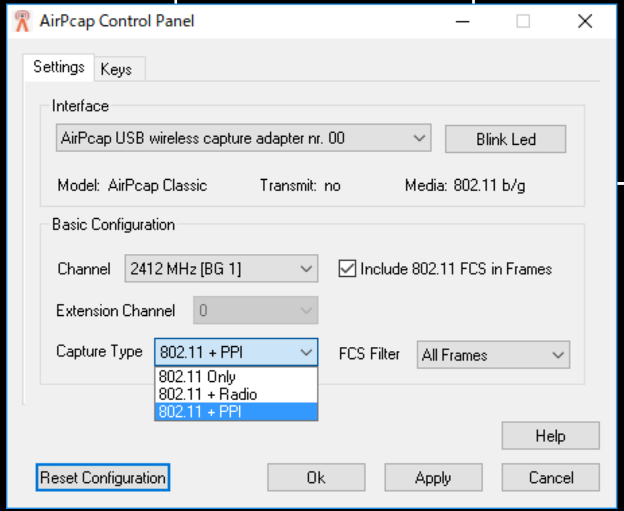
Type	Radiotap header	PPI header
Packet		

```
Radiotap Header v0, Length 20
  Header revision: 0
  Header pad: 0
  Header length: 20
› Present flags
⌄ Flags: 0x10
    .... ...0 = CFP: False
    .... ..0. = Preamble: Long
    .... .0.. = WEP: False
    .... 0... = Fragmentation: False
    ...1 .... = FCS at end: True
    ..0. .... = Data Pad: False
    .0.. .... = Bad FCS: False
    0... .... = Short GI: False
  Data Rate: 11.0 Mb/s
  Channel frequency: 2412 [BG 1]
› Channel flags: 0x00a0, Complementary Code Keying (CCK), 2 GHz
  SSI Signal: -47 dBm
  SSI Noise: -100 dBm
  Signal Quality: 100
  Antenna: 0
  SSI Signal: 53 dB
```

```
PPI version 0, 32 bytes
  Version: 0
⌄ Flags: 0x00
    .... ...0 = Alignment: Not aligned
    0000 000. = Reserved: 0x00
  Header length: 32
  DLT: 105
⌄ 802.11-Common
    Field type: 802.11-Common (2)
    Field length: 20
    TSFT: 0 [invalid]
  › Flags: 0x0001
    Rate: 11.0 Mbps
    Channel frequency: 2412 [BG 1]
  ⌄ Channel flags: 0x00a0
      .... .... ...0 .... = Turbo: False
      .... .... ..1. .... = Complementary Code Keying (CCK): True
      .... .... .0.. .... = Orthogonal Frequency-Division Multiplexing (OFDM): False
      .... .... 1... .... = 2 GHz spectrum: True
      .... ...0 .... .... = 5 GHz spectrum: False
      .... ..0. .... .... = Passive: False
      .... .0.. .... .... = Dynamic CCK-OFDM: False
      .... 0... .... .... = Gaussian Frequency Shift Keying (GFSK): False
    FHSS hopset: 0x00
    FHSS pattern: 0x00
    dBm antenna signal: -52
    dBm antenna noise: -100
```

We can capture wireless frames as 2 kinds of frame format in Physical layer using AirPcap and Wireshark

Type	Radiotap	PPI
GOOD	• Easy to read, simple • Fixed format • Easy filter radiotap.dbm_antsignal	• Extensible format future info 11ac, etc • Includes multiple antenna information
BAD	• Cannot collect multiple anntena information	• Hard to read, complex • Long filter ppi.80211n-mac-phy.dbmant0.signal



Interface

AirPcap USB wireless capture adapter nr. 00

Model: AirPcap Classic Transmit: no Media: 802.11 b/g

Basic Configuration

Channel 2412 MHz [BG 1]

☑ Include 802.11 FCS in Frames

Extension Channel 0

Capture Type 802.11 + PPI

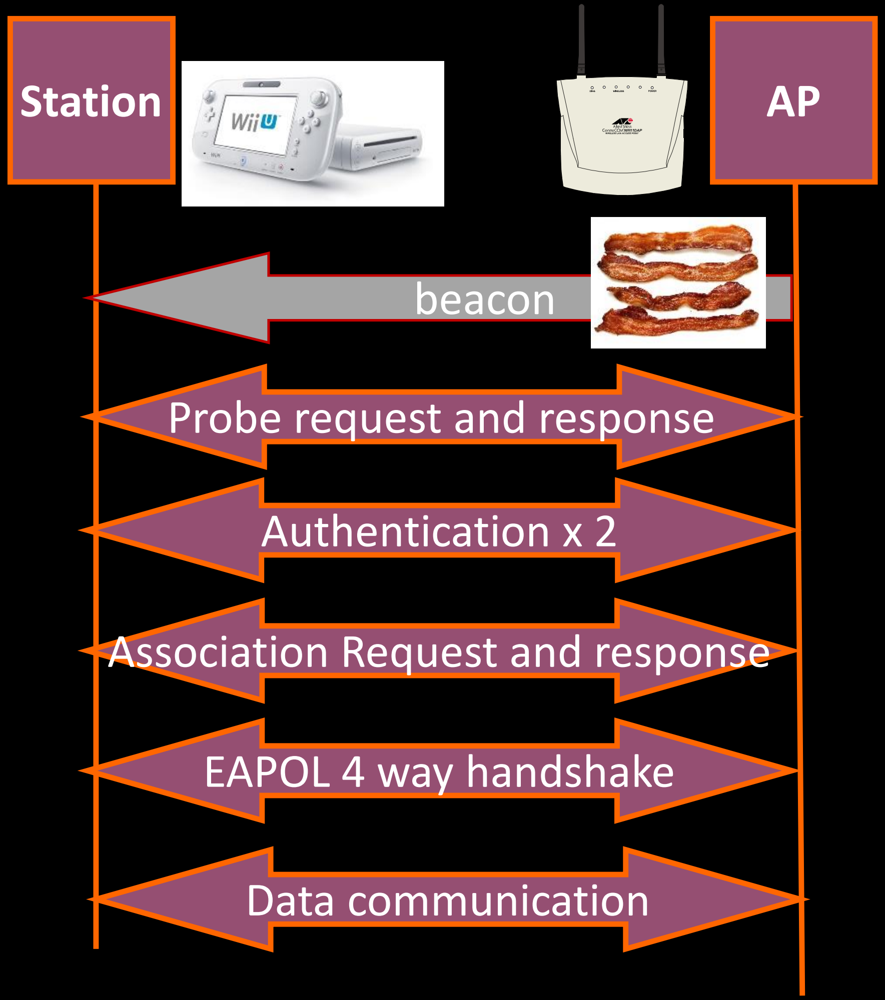
FCS Filter All Frames

RECOMMEND Radiotap in 11a/b/g/n(20MHz)
Demonstration Wireless toolbar> setting

#3 Picking up basic link-up process

- My Nintendo WiiU connect AP that SSID is “DEFCON” at 1ch (2412MHz)
- Now we open trace file “3-WiiU.pcapng”,
  filter using Wireshark display filter,
  mark the connection (Ctrl + M),
  export specified packet as another trace file.
  “linkup.pcapng”
- You think there are tons of other packets in trace file.
- You do not have to mark “ACK” packet (sometimes sender is blank)
- It is usual in wireless packet capturing, so display filter is important
- Hint: the link-up process ends in a seconds,
  so you find some important packet, you can find the other packet at near time.

The link-up process of Wi-Fi (WPA2 AES-PSK)



You need to mark 10 more packets including
1: Beacon from AP

2: Probe Request from STA / Response from AP

3: Authentication from STA and from AP

4: Association Request from STA / Response from AP

5: EAPOL 4 way handshake (4 message)

6: some data packets
Hint 0 all packet is captured at 1ch

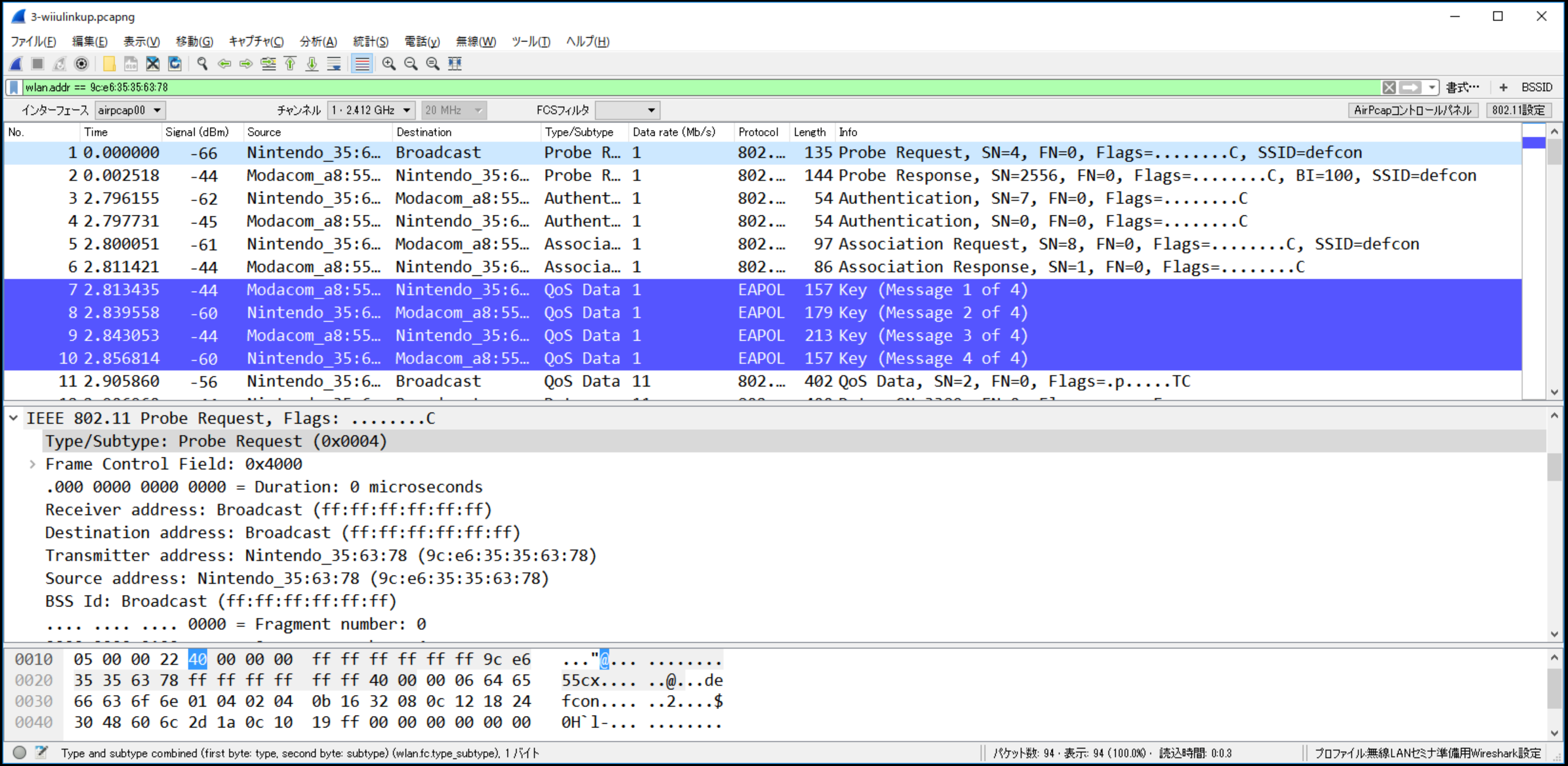
- Hint 1 My WiiU mac address
  wlan.addr eq 9c:e6:35:35:63:78
- Hint 2: My AP mac address (BSSID)
  wlan.addr eq 00:1d:93:a8:55:d8
- Hint 3: You can refer display filter list.

Frame Type	Explanation
Management wlan.fc.type==0	Beacon wlan.fc.type_subtype==8
	Probe request wlan.fc.type_subtype==4
	Probe Response wlan.fc.type_subtype==5
	Association Request wlan.fc.type_subtype==0
	Association Response wlan.fc.type_subtype==1
	Authentication wlan.fc.type_subtype==11
	Deauthentication wlan.fc.type_subtype==12
	Disassociation wlan.fc.type_subtype==10
Control wlan.fc.type==1	RTS （Request To Send） wlan.fc.type_subtype==27
	CTS （Clear To Send） wlan.fc.type_subtype==28
	ACK （ACKnowledge） wlan.fc.type_subtype==29
Data wlan.fc.type==2	wlan.fc.type_type==2 Null data wlan.fc.type_subtype==36

Pick up and mark packet

- Mark Beacon
  Filter packets using type_subtype of Beacon (8) of IEEE802.11 frame, wlan.fc.type_subtype==8, then search packet that SSID is defcon
- Mark connection
  Filter packets using STA MAC address wlan.addr == 9c:e6:35:35:63:78,
  next look for association response, then you can find entire connection process near here in a seconds (beacon, probe, auth, assoc, eapol, data)
- File > Export specified packets and select marked packets button to export the another trace file such as 3-wiiulinkup.pcapng
- Note you may not have to collect ACK, and collect all 4 way handshake packets.

3-wiiulinkup.pcapng



wlan.addr == 9c:e6:35:35:63:78

インターフェース airpcap00 チャンネル 1 · 2.412 GHz 20 MHz FCSフィルタ

No.	Time	Signal (dBm)	Source	Destination	Type/Subtype	Data rate (Mb/s)	Protocol	Length	Info
1	0.000000	-66	Nintendo_35:6…	Broadcast	Probe R…	1	802.…	135	Probe Request, SN=4, FN=0, Flags=........C, SSID=defcon
2	0.002518	-44	Modacom_a8:55…	Nintendo_35:6…	Probe R…	1	802.…	144	Probe Response, SN=2556, FN=0, Flags=........C, BI=100, SSID=defcon
3	2.796155	-62	Nintendo_35:6…	Modacom_a8:55…	Authent…	1	802.…	54	Authentication, SN=7, FN=0, Flags=........C
4	2.797731	-45	Modacom_a8:55…	Nintendo_35:6…	Authent…	1	802.…	54	Authentication, SN=0, FN=0, Flags=........C
5	2.800051	-61	Nintendo_35:6…	Modacom_a8:55…	Associa…	1	802.…	97	Association Request, SN=8, FN=0, Flags=........C, SSID=defcon
6	2.811421	-44	Modacom_a8:55…	Nintendo_35:6…	Associa…	1	802.…	86	Association Response, SN=1, FN=0, Flags=........C
7	2.813435	-44	Modacom_a8:55…	Nintendo_35:6…	QoS Data	1	EAPOL	157	Key (Message 1 of 4)
8	2.839558	-60	Nintendo_35:6…	Modacom_a8:55…	QoS Data	1	EAPOL	179	Key (Message 2 of 4)
9	2.843053	-44	Modacom_a8:55…	Nintendo_35:6…	QoS Data	1	EAPOL	213	Key (Message 3 of 4)
10	2.856814	-60	Nintendo_35:6…	Modacom_a8:55…	QoS Data	1	EAPOL	157	Key (Message 4 of 4)
11	2.905860	-56	Nintendo_35:6…	Broadcast	QoS Data	11	802.…	402	QoS Data, SN=2, FN=0, Flags=.p.....TC

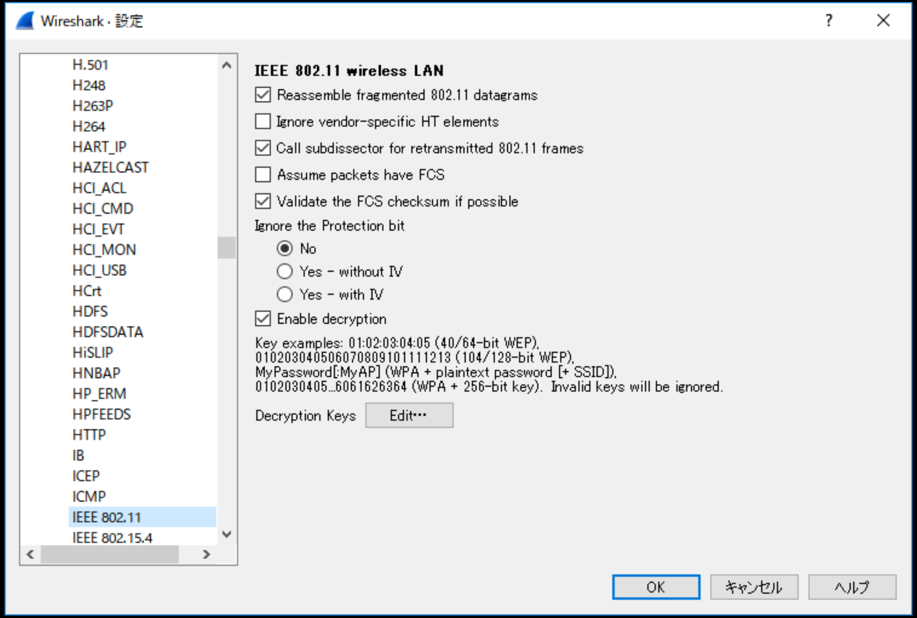
```
v IEEE 802.11 Probe Request, Flags: ........C
    Type/Subtype: Probe Request (0x0004)
  > Frame Control Field: 0x4000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: Nintendo_35:63:78 (9c:e6:35:35:63:78)
    Source address: Nintendo_35:63:78 (9c:e6:35:35:63:78)
    BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
    .... .... .... 0000 = Fragment number: 0
```

```
0010  05 00 00 22 40 00 00 00  ff ff ff ff ff ff 9c e6   ..."@... ........
0020  35 35 63 78 ff ff ff ff  ff ff 40 00 00 06 64 65   55cx.... ..@...de
0030  66 63 6f 6e 01 04 02 04  0b 16 32 08 0c 12 18 24   fcon.... ..2....$
0040  30 48 60 6c 2d 1a 0c 10  19 ff 00 00 00 00 00 00   0H`l-... ........
```

Type and subtype combined (first byte: type, second byte: subtype) (wlan.fc.type_subtype), 1 バイト | パケット数: 94 · 表示: 94 (100.0%) · 読込時間: 0:0.3 | プロファイル:無線LANセミナ準備用Wireshark設定

#4 Decrypting WPA2

- Open 4-wiiulinkup.pcapng (same as last trace file we filtered)
- Please look at data frame using display filter (wlan.fc.type==2)
- You can find all data section is encrypted by WPA2(AES-PSK) but you capture all 4 way handshake message (eapol)
- Select some data packet and click IEEE802.11 header, right click > protocol preferences > Open IEEE802.11 wirelss LAN preferences…



IEEE 802.11 wireless LAN

☑ Reassemble fragmented 802.11 datagrams

□ Ignore vendor-specific HT elements

☑ Call subdissector for retransmitted 802.11 frames

□ Assume packets have FCS

☑ Validate the FCS checksum if possible

Ignore the Protection bit

● No

○ Yes - without IV

○ Yes - with IV

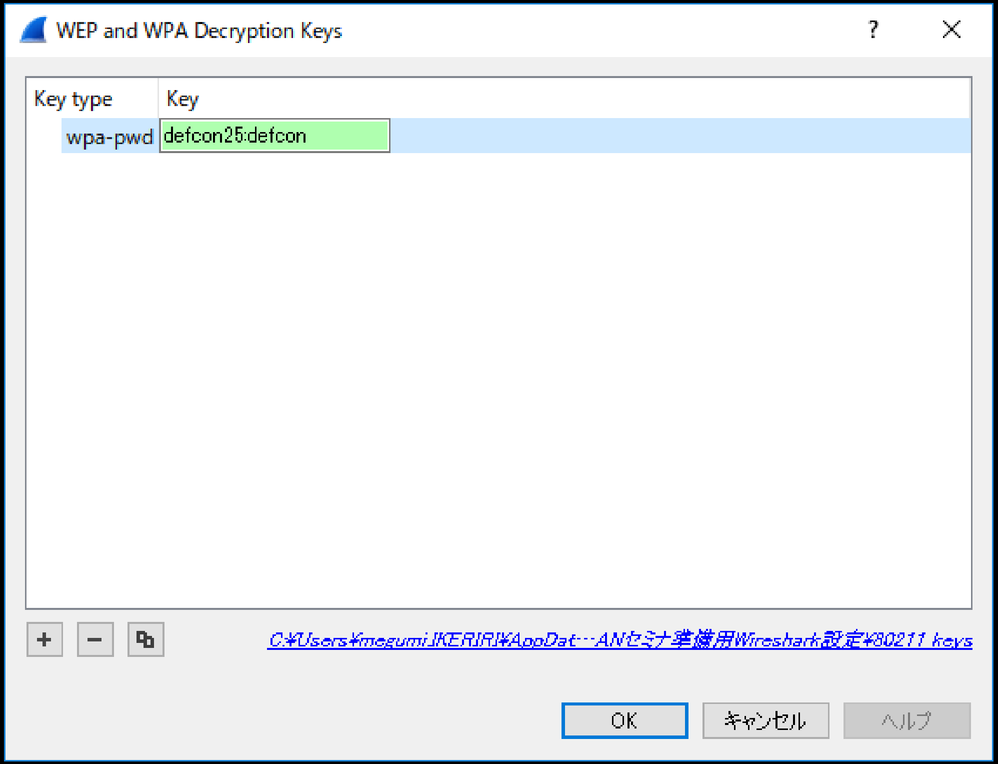
☑ Enable decryption

Key examples: 01:02:03:04:05 (40/64-bit WEP),
010203040506070809101111213 (104/128-bit WEP),
MyPassword[:MyAP] (WPA + plaintext password [+ SSID]),
0102030405…6061626364 (WPA + 256-bit key). Invalid keys will be ignored.

Decryption Keys Edit…

#4 Decrypting WPA2

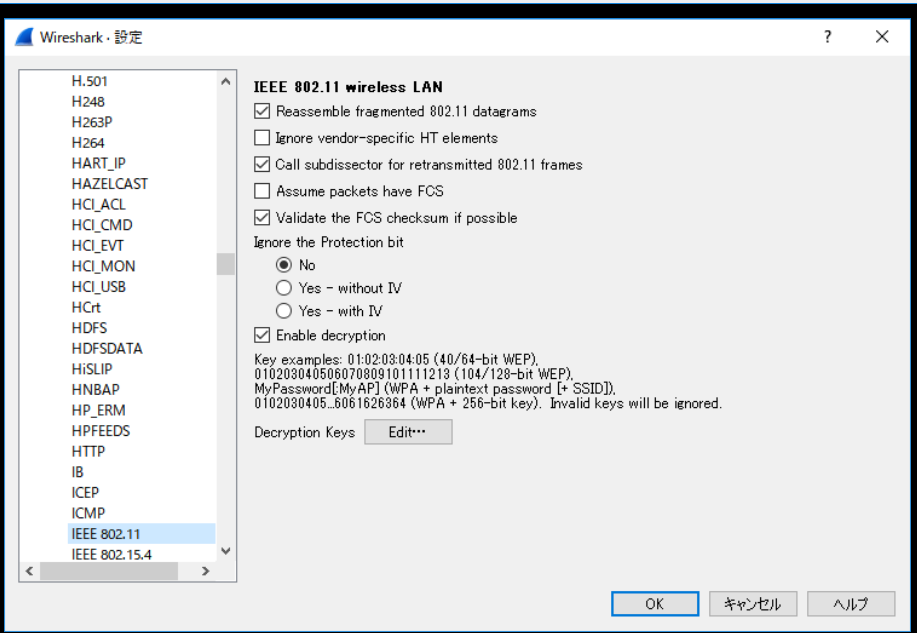
- Confirm Enable decryption is checked
- Select Edit button of Decryption Keys
- Push “+” button, and select wpa-pwd in Key type, then input the PSK:SSID defcon25:defcon
- Note: You must collect all 4 message of EAPOL 4 way handshake, because it contains information of creating PTK(pairwise transient key) such as nonce, MAC, SSID, etc.



WEP and WPA Decryption Keys

Key type	Key
wpa-pwd	defcon25:defcon

C:¥Users¥megumi.IKERIRI¥AppDat…ANセミナ準備用Wireshark設定¥80211_keys



Wireshark · 設定

IEEE 802.11 wireless LAN

☑ Reassemble fragmented 802.11 datagrams

□ Ignore vendor-specific HT elements

☑ Call subdissector for retransmitted 802.11 frames

□ Assume packets have FCS

☑ Validate the FCS checksum if possible

Ignore the Protection bit

● No

○ Yes - without IV

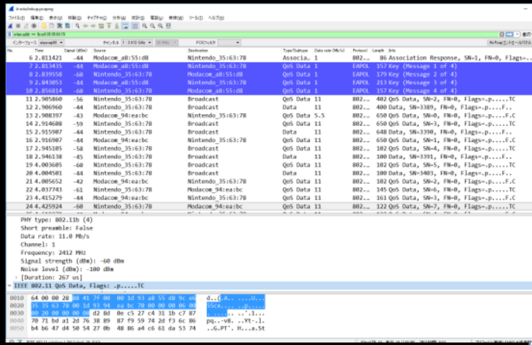
○ Yes - with IV

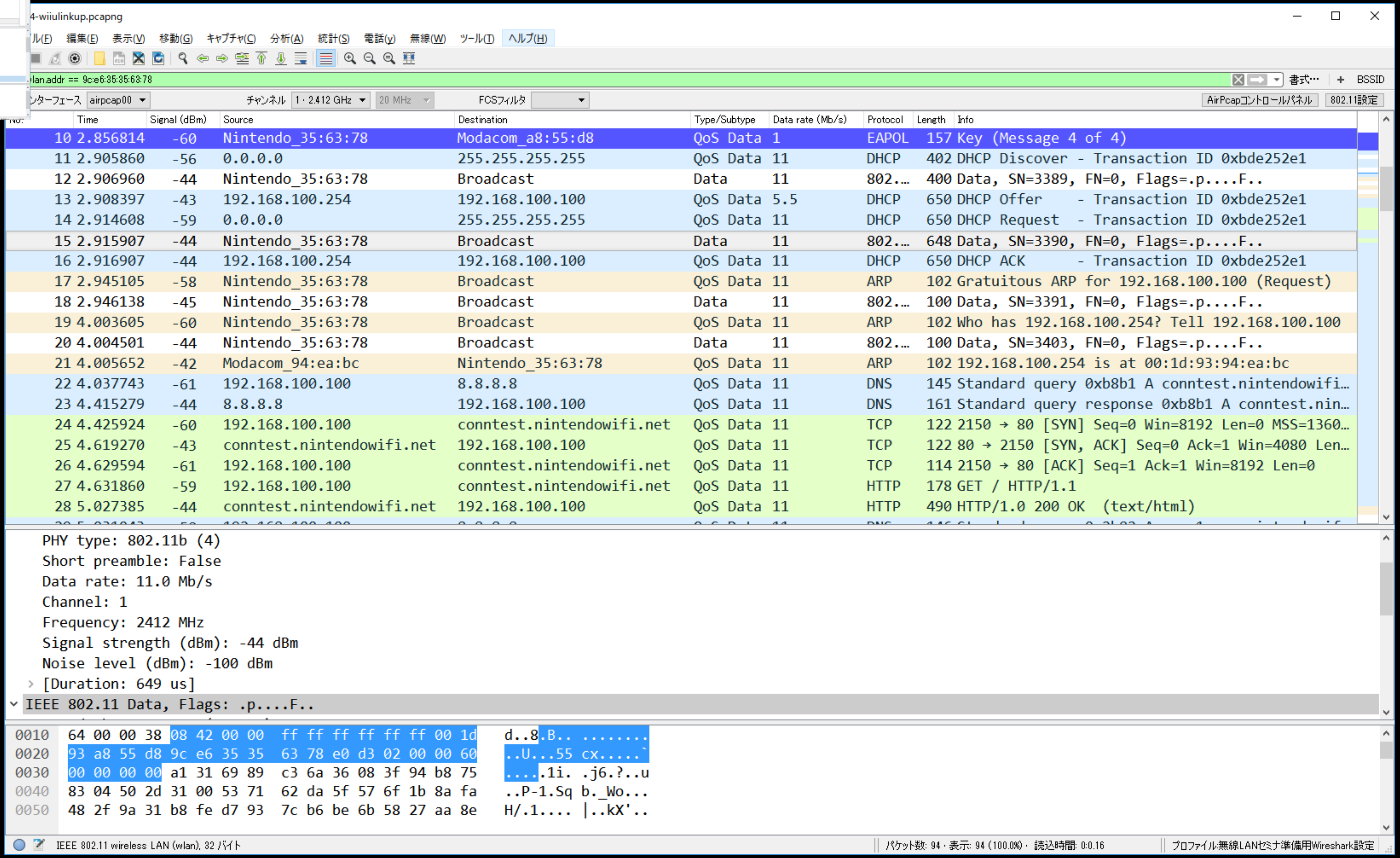
☑ Enable decryption

Key examples: 01:02:03:04:05 (40/64-bit WEP),
0102030405060708091011111213 (104/128-bit WEP),
MyPassword[:MyAP] (WPA + plaintext password [+ SSID]),
0102030405…6061626364 (WPA + 256-bit key). Invalid keys will be ignored.

Decryption Keys Edit…

Please check the trace file is decrypted





4-wiiulinkup.pcapng
ル(E) 編集(E) 表示(V) 移動(G) キャプチャ(C) 分析(A) 統計(S) 電話(y) 無線(W) ツール(T) ヘルプ(H)
書式··· + BSSID
AirPcapコントロールパネル
802.11設定

```
lan.addr == 9c:e6:35:35:63:78
ンターフェース airpcap00    チャンネル 1 · 2.412 GHz   20 MHz   FCSフィルタ
```

```
No.    Time      Signal (dBm) Source                     Destination                Type/Subtype Data rate (Mb/s) Protocol Length Info
   10 2.856814  -60  Nintendo_35:63:78          Modacom_a8:55:d8           QoS Data  1    EAPOL  157 Key (Message 4 of 4)
   11 2.905860  -56  0.0.0.0                    255.255.255.255            QoS Data  11   DHCP   402 DHCP Discover - Transaction ID 0xbde252e1
   12 2.906960  -44  Nintendo_35:63:78          Broadcast                  Data      11   802.…  400 Data, SN=3389, FN=0, Flags=.p....F..
   13 2.908397  -43  192.168.100.254            192.168.100.100            QoS Data  5.5  DHCP   650 DHCP Offer    - Transaction ID 0xbde252e1
   14 2.914608  -59  0.0.0.0                    255.255.255.255            QoS Data  11   DHCP   650 DHCP Request  - Transaction ID 0xbde252e1
   15 2.915907  -44  Nintendo_35:63:78          Broadcast                  Data      11   802.…  648 Data, SN=3390, FN=0, Flags=.p....F..
   16 2.916907  -44  192.168.100.254            192.168.100.100            QoS Data  11   DHCP   650 DHCP ACK      - Transaction ID 0xbde252e1
   17 2.945105  -58  Nintendo_35:63:78          Broadcast                  QoS Data  11   ARP    102 Gratuitous ARP for 192.168.100.100 (Request)
   18 2.946138  -45  Nintendo_35:63:78          Broadcast                  Data      11   802.…  100 Data, SN=3391, FN=0, Flags=.p....F..
   19 4.003605  -60  Nintendo_35:63:78          Broadcast                  QoS Data  11   ARP    102 Who has 192.168.100.254? Tell 192.168.100.100
   20 4.004501  -44  Nintendo_35:63:78          Broadcast                  Data      11   802.…  100 Data, SN=3403, FN=0, Flags=.p....F..
   21 4.005652  -42  Modacom_94:ea:bc           Nintendo_35:63:78          QoS Data  11   ARP    102 192.168.100.254 is at 00:1d:93:94:ea:bc
   22 4.037743  -61  192.168.100.100            8.8.8.8                    QoS Data  11   DNS    145 Standard query 0xb8b1 A conntest.nintendowifi…
   23 4.415279  -44  8.8.8.8                    192.168.100.100            QoS Data  11   DNS    161 Standard query response 0xb8b1 A conntest.nin…
   24 4.425924  -60  192.168.100.100            conntest.nintendowifi.net  QoS Data  11   TCP    122 2150 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1360…
   25 4.619270  -43  conntest.nintendowifi.net  192.168.100.100            QoS Data  11   TCP    122 80 → 2150 [SYN, ACK] Seq=0 Ack=1 Win=4080 Len…
   26 4.629594  -61  192.168.100.100            conntest.nintendowifi.net  QoS Data  11   TCP    114 2150 → 80 [ACK] Seq=1 Ack=1 Win=8192 Len=0
   27 4.631860  -59  192.168.100.100            conntest.nintendowifi.net  QoS Data  11   HTTP   178 GET / HTTP/1.1
   28 5.027385  -44  conntest.nintendowifi.net  192.168.100.100            QoS Data  11   HTTP   490 HTTP/1.0 200 OK  (text/html)
```

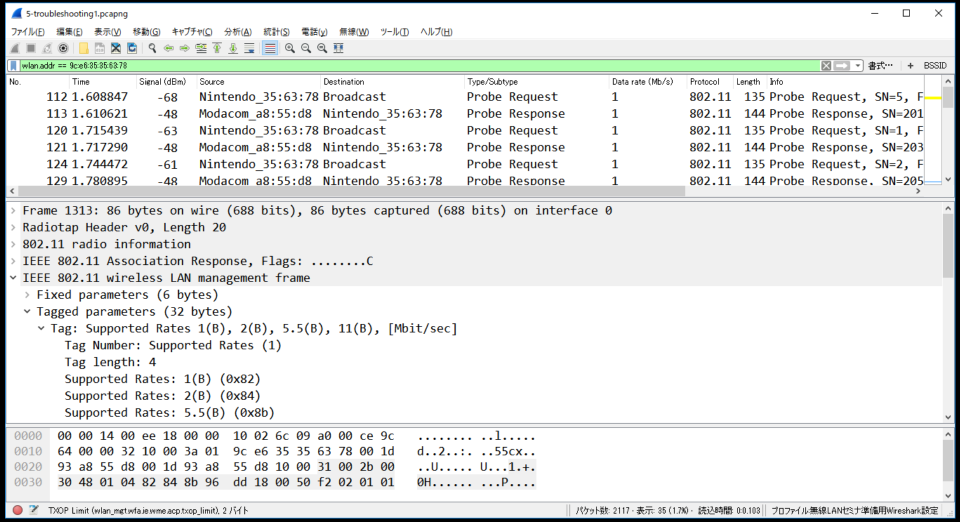
```
    PHY type: 802.11b (4)
    Short preamble: False
    Data rate: 11.0 Mb/s
    Channel: 1
    Frequency: 2412 MHz
    Signal strength (dBm): -44 dBm
    Noise level (dBm): -100 dBm
  > [Duration: 649 us]
v IEEE 802.11 Data, Flags: .p....F..
```

```
0010  64 00 00 38 08 42 00 00  ff ff ff ff ff ff 00 1d   d..8.B.. ........
0020  93 a8 55 d8 9c e6 35 35  63 78 e0 d3 02 00 00 60   ..U...55 cx.....`
0030  00 00 00 00 a1 31 69 89  c3 6a 36 08 3f 94 b8 75   .....1i. .j6.?..u
0040  83 04 50 2d 31 00 53 71  62 da 5f 57 6f 1b 8a fa   ..P-1.Sq b._Wo...
0050  48 2f 9a 31 b8 fe d7 93  7c b6 be 6b 58 27 aa 8e   H/.1.... |..kX'..
```

```
IEEE 802.11 wireless LAN (wlan), 32 バイト    パケット数: 94 · 表示: 94 (100.0%) · 読込時間: 0:0.16    プロファイル:無線LANセミナ準備用Wireshark設定
```

#5 Troubleshooting #1 my WiiU failed to connect AP

- Open trace 5-troubleshooting1.pcapng
- My WiiU (9c:e6:35:35:63:78)
  failed to connect AP (00:1d:93:a8:55:d8)
- Why ? Please look for the reason
- Hint1: Filter packets by STA mac address
- Hint2: Look in detail in IEEE802.11 frame



5-troubleshooting1.pcapng
ファイル(F) 編集(E) 表示(V) 移動(G) キャプチャ(C) 分析(A) 統計(S) 電話(y) 無線(W) ツール(T) ヘルプ(H)
書式…
BSSID

```
wlan.addr == 9c:e6:35:35:63:78
```

```
No.  Time      Signal (dBm) Source              Destination         Type/Subtype    Data rate (Mb/s) Protocol Length Info
 112 1.608847  -68  Nintendo_35:63:78 Broadcast          Probe Request   1   802.11  135 Probe Request, SN=5, F
 113 1.610621  -48  Modacom_a8:55:d8  Nintendo_35:63:78  Probe Response  1   802.11  144 Probe Response, SN=201
 120 1.715439  -63  Nintendo_35:63:78 Broadcast          Probe Request   1   802.11  135 Probe Request, SN=1, F
 121 1.717290  -48  Modacom_a8:55:d8  Nintendo_35:63:78  Probe Response  1   802.11  144 Probe Response, SN=203
 124 1.744472  -61  Nintendo_35:63:78 Broadcast          Probe Request   1   802.11  135 Probe Request, SN=2, F
 129 1.780895  -48  Modacom_a8:55:d8  Nintendo_35:63:78  Probe Response  1   802.11  144 Probe Response, SN=205
```

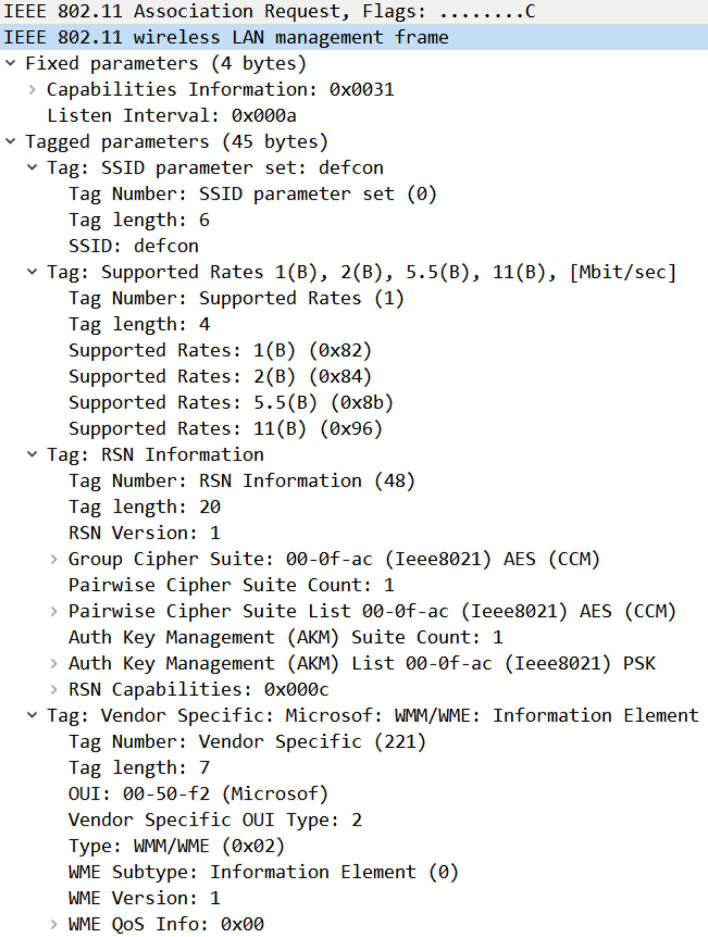
```
> Frame 1313: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
> Radiotap Header v0, Length 20
> 802.11 radio information
> IEEE 802.11 Association Response, Flags: ........C
v IEEE 802.11 wireless LAN management frame
  > Fixed parameters (6 bytes)
  v Tagged parameters (32 bytes)
    v Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
        Tag Number: Supported Rates (1)
        Tag length: 4
        Supported Rates: 1(B) (0x82)
        Supported Rates: 2(B) (0x84)
        Supported Rates: 5.5(B) (0x8b)
```

```
0000  00 00 14 00 ee 18 00 00  10 02 6c 09 a0 00 ce 9c   ........ ..l.....
0010  64 00 00 32 10 00 3a 01  9c e6 35 35 63 78 00 1d   d..2..:. ..55cx..
0020  93 a8 55 d8 00 1d 93 a8  55 d8 10 00 31 00 2b 00   ..U..... U...1.+.
0030  30 48 01 04 82 84 8b 96  dd 18 00 50 f2 02 01 01   0H...... ...P....
```

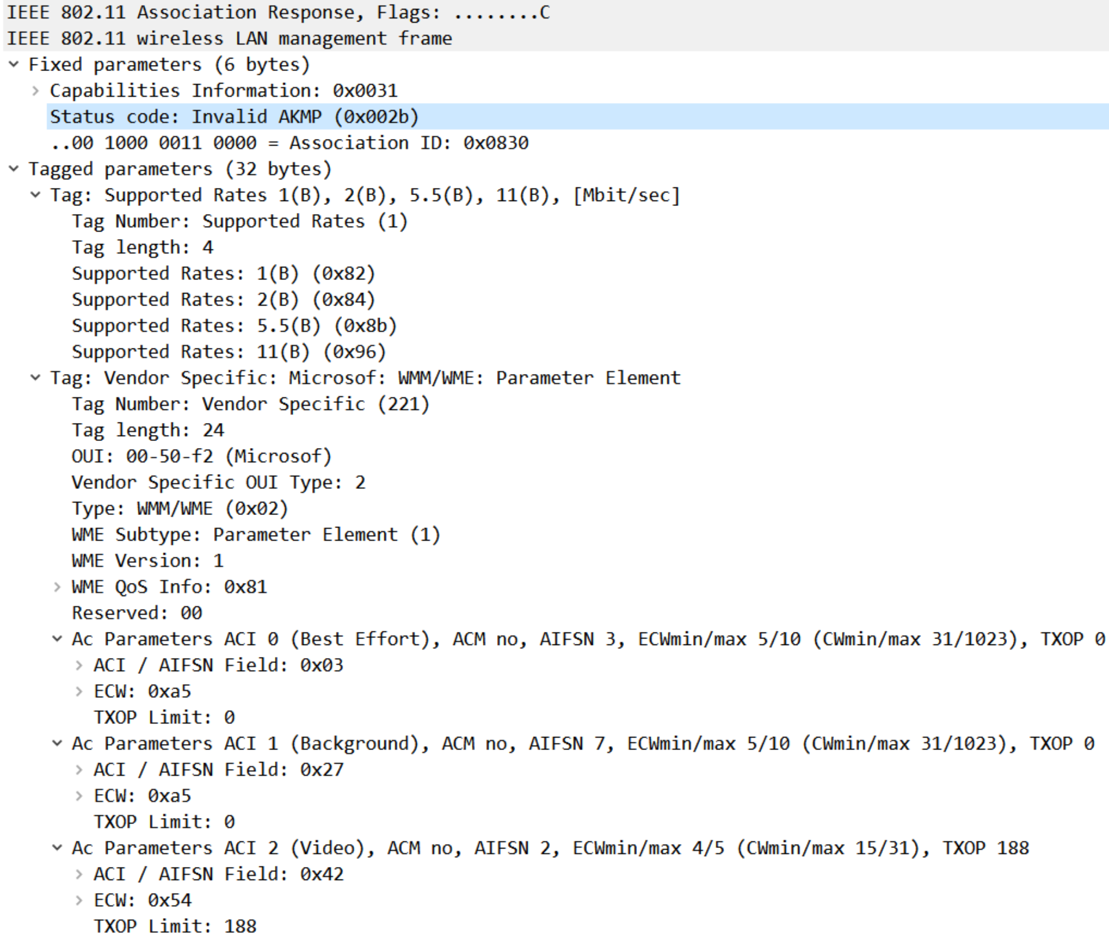
TXOP Limit (wlan_mgt.wfa.ie.wme.acp.txop_limit), 2 バイト | パケット数: 2117 · 表示: 35 (1.7%) · 読込時間: 0:0.103 | プロファイル:無線LANセミナ準備用Wireshark設定

Invalid AKMP (Specification mismatch between STA and AP)

- Invalid AKMP (0x002b) in Fixed parameters, IEEE802.11 Association response frame from AP, it means mismatch of IEEE802.1x setting AKMP : IEEE 802.1X Authentication and Key Management Protocol).



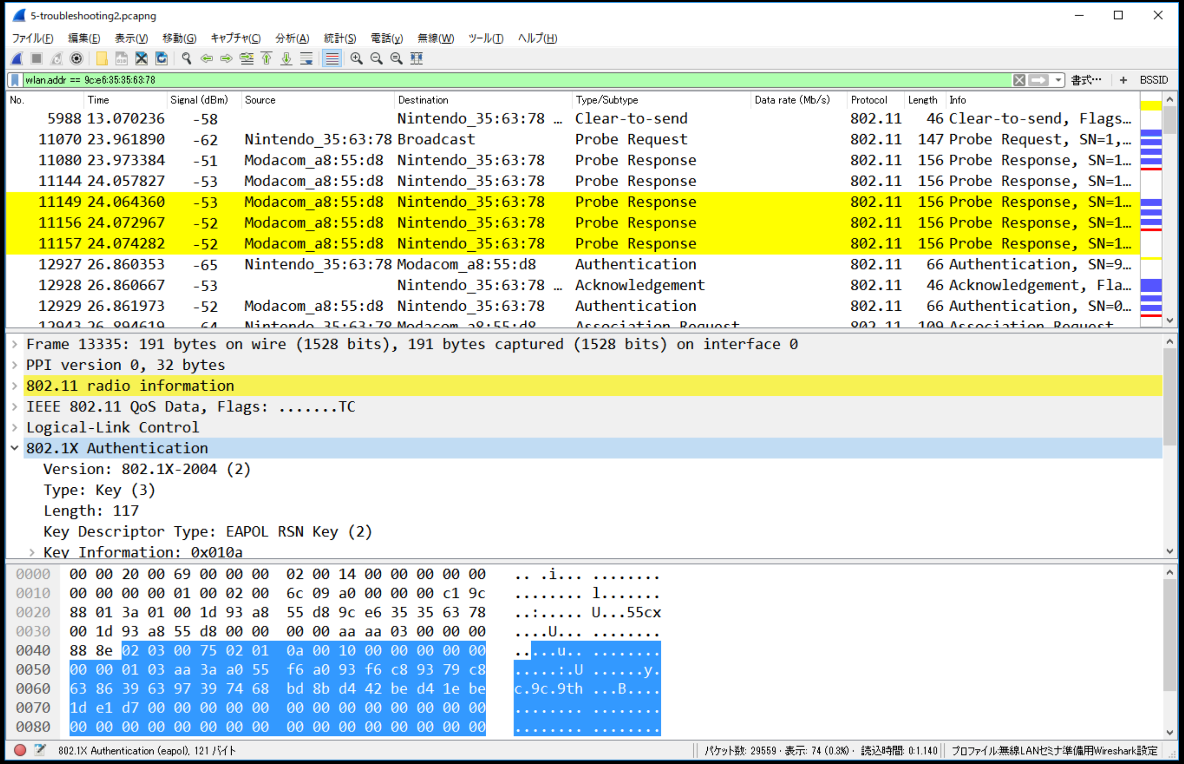
```
IEEE 802.11 Association Request, Flags: ........C
IEEE 802.11 wireless LAN management frame
⌄ Fixed parameters (4 bytes)
  › Capabilities Information: 0x0031
    Listen Interval: 0x000a
⌄ Tagged parameters (45 bytes)
  ⌄ Tag: SSID parameter set: defcon
      Tag Number: SSID parameter set (0)
      Tag length: 6
      SSID: defcon
  ⌄ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
      Tag Number: Supported Rates (1)
      Tag length: 4
      Supported Rates: 1(B) (0x82)
      Supported Rates: 2(B) (0x84)
      Supported Rates: 5.5(B) (0x8b)
      Supported Rates: 11(B) (0x96)
  ⌄ Tag: RSN Information
      Tag Number: RSN Information (48)
      Tag length: 20
      RSN Version: 1
    › Group Cipher Suite: 00-0f-ac (Ieee8021) AES (CCM)
      Pairwise Cipher Suite Count: 1
    › Pairwise Cipher Suite List 00-0f-ac (Ieee8021) AES (CCM)
      Auth Key Management (AKM) Suite Count: 1
    › Auth Key Management (AKM) List 00-0f-ac (Ieee8021) PSK
    › RSN Capabilities: 0x000c
  ⌄ Tag: Vendor Specific: Microsof: WMM/WME: Information Element
      Tag Number: Vendor Specific (221)
      Tag length: 7
      OUI: 00-50-f2 (Microsof)
      Vendor Specific OUI Type: 2
      Type: WMM/WME (0x02)
      WME Subtype: Information Element (0)
      WME Version: 1
    › WME QoS Info: 0x00
```



```
IEEE 802.11 Association Response, Flags: ........C
IEEE 802.11 wireless LAN management frame
⌄ Fixed parameters (6 bytes)
  › Capabilities Information: 0x0031
    Status code: Invalid AKMP (0x002b)
    ..00 1000 0011 0000 = Association ID: 0x0830
⌄ Tagged parameters (32 bytes)
  ⌄ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
      Tag Number: Supported Rates (1)
      Tag length: 4
      Supported Rates: 1(B) (0x82)
      Supported Rates: 2(B) (0x84)
      Supported Rates: 5.5(B) (0x8b)
      Supported Rates: 11(B) (0x96)
  ⌄ Tag: Vendor Specific: Microsof: WMM/WME: Parameter Element
      Tag Number: Vendor Specific (221)
      Tag length: 24
      OUI: 00-50-f2 (Microsof)
      Vendor Specific OUI Type: 2
      Type: WMM/WME (0x02)
      WME Subtype: Parameter Element (1)
      WME Version: 1
    › WME QoS Info: 0x81
      Reserved: 00
    ⌄ Ac Parameters ACI 0 (Best Effort), ACM no, AIFSN 3, ECWmin/max 5/10 (CWmin/max 31/1023), TXOP 0
      › ACI / AIFSN Field: 0x03
      › ECW: 0xa5
        TXOP Limit: 0
    ⌄ Ac Parameters ACI 1 (Background), ACM no, AIFSN 7, ECWmin/max 5/10 (CWmin/max 31/1023), TXOP 0
      › ACI / AIFSN Field: 0x27
      › ECW: 0xa5
        TXOP Limit: 0
    ⌄ Ac Parameters ACI 2 (Video), ACM no, AIFSN 2, ECWmin/max 4/5 (CWmin/max 15/31), TXOP 188
      › ACI / AIFSN Field: 0x42
      › ECW: 0x54
        TXOP Limit: 188
```

#5 Troubleshooting #2 Wi-Fi connection is down ?

- Open trace 5-troubleshooting2.pcapng
- I fixed the AP setting and try again
- My WiiU (9c:e6:35:35:63:78)
  failed to connect AP (00:1d:93:a8:55:d8) Wi-Fi connection is down ?
- Why ? Please look for the reason
- Hint1: Look for stack point
- Hint2: Repetition of the packet
  implies some trouble


5-troubleshooting2.pcapng
ファイル(F) 編集(E) 表示(V) 移動(G) キャプチャ(C) 分析(A) 統計(S) 電話(y) 無線(W) ツール(T) ヘルプ(H)
書式…
BSSID

wlan.addr == 9c:e6:35:35:63:78

```
No.   Time      Signal (dBm) Source            Destination         Type/Subtype        Data rate (Mb/s) Protocol Length Info
 5988 13.070236  -58                           Nintendo_35:63:78 … Clear-to-send                        802.11    46 Clear-to-send, Flags…
11070 23.961890  -62  Nintendo_35:63:78 Broadcast           Probe Request                        802.11   147 Probe Request, SN=1,…
11080 23.973384  -51  Modacom_a8:55:d8  Nintendo_35:63:78   Probe Response                       802.11   156 Probe Response, SN=1…
11144 24.057827  -53  Modacom_a8:55:d8  Nintendo_35:63:78   Probe Response                       802.11   156 Probe Response, SN=1…
11149 24.064360  -53  Modacom_a8:55:d8  Nintendo_35:63:78   Probe Response                       802.11   156 Probe Response, SN=1…
11156 24.072967  -52  Modacom_a8:55:d8  Nintendo_35:63:78   Probe Response                       802.11   156 Probe Response, SN=1…
11157 24.074282  -52  Modacom_a8:55:d8  Nintendo_35:63:78   Probe Response                       802.11   156 Probe Response, SN=1…
12927 26.860353  -65  Nintendo_35:63:78 Modacom_a8:55:d8    Authentication                       802.11    66 Authentication, SN=9…
12928 26.860667  -53                    Nintendo_35:63:78 … Acknowledgement                      802.11    46 Acknowledgement, Fla…
12929 26.861973  -52  Modacom_a8:55:d8  Nintendo_35:63:78   Authentication                       802.11    66 Authentication, SN=0…
12943 26.894619  -64  Nintendo_35:63:78 Modacom_a8:55:d8    Association Request                  802.11   109 Association Request
```

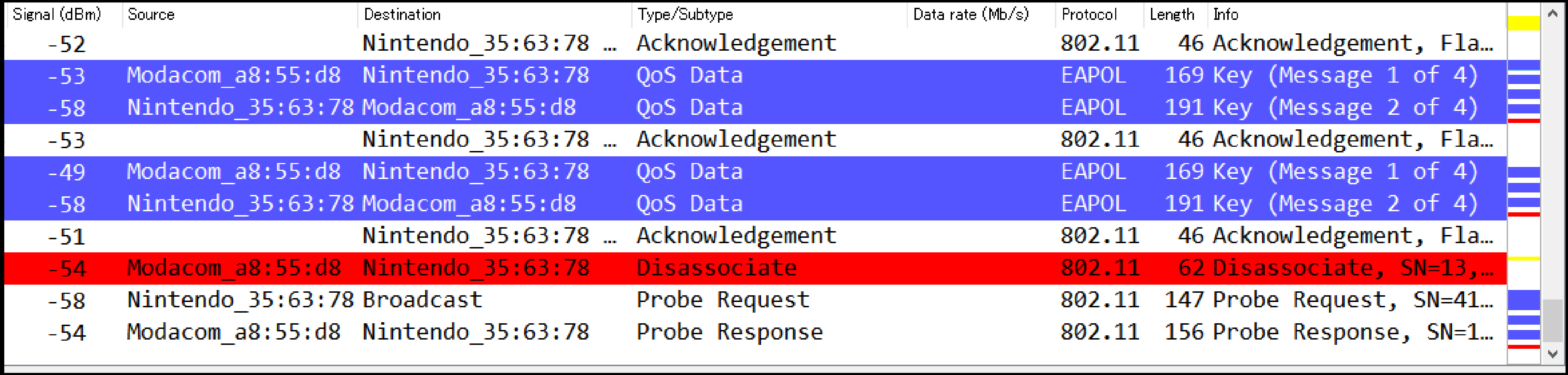
```
> Frame 13335: 191 bytes on wire (1528 bits), 191 bytes captured (1528 bits) on interface 0
> PPI version 0, 32 bytes
> 802.11 radio information
> IEEE 802.11 QoS Data, Flags: .......TC
> Logical-Link Control
v 802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: Key (3)
    Length: 117
    Key Descriptor Type: EAPOL RSN Key (2)
  > Key Information: 0x010a
```

```
0000  00 00 20 00 69 00 00 00  02 00 14 00 00 00 00 00   .. .i... ........
0010  00 00 00 00 01 00 02 00  6c 09 a0 00 00 00 c1 9c   ........ l.......
0020  88 01 3a 01 00 1d 93 a8  55 d8 9c e6 35 35 63 78   ..:..... U...55cx
0030  00 1d 93 a8 55 d8 00 00  00 00 aa aa 03 00 00 00   ....U... ........
0040  88 8e 02 03 00 75 02 01  0a 00 10 00 00 00 00 00   .....u.. ........
0050  00 00 01 03 aa 3a a0 55  f6 a0 93 f6 c8 93 79 c8   .....:.U ......y.
0060  63 86 39 63 97 39 74 68  bd 8b d4 42 be d4 1e be   c.9c.9th ...B....
0070  1d e1 d7 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

802.1X Authentication (eapol), 121 バイト | パケット数: 29559 · 表示: 74 (0.3%) · 読込時間: 0:1.140 | プロファイル:無線LANセミナ準備用Wireshark設定

Pre-Shared-Key mismatch

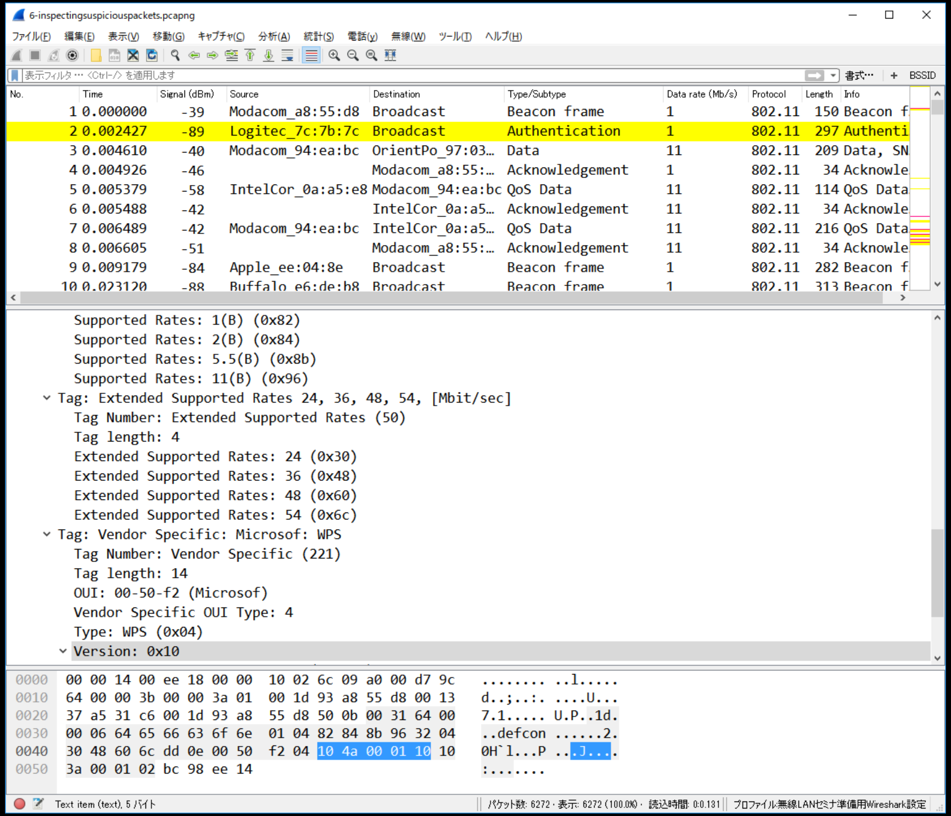
- Datalink layer is up because you can find association response,
- But EAPOL 4 way handshake is failed between message 2 and 3. then AP sends Disassociate frame to STA
- Message 2 of 4 way handshake sends Nonce, MIC (Hash), MAC address (then creates PTK off-line)
- Message 3 is not sent because calculated PTK is not the same



Signal (dBm)	Source	Destination	Type/Subtype	Data rate (Mb/s)	Protocol	Length	Info
-52		Nintendo_35:63:78 …	Acknowledgement		802.11	46	Acknowledgement, Fla…
-53	Modacom_a8:55:d8	Nintendo_35:63:78	QoS Data		EAPOL	169	Key (Message 1 of 4)
-58	Nintendo_35:63:78	Modacom_a8:55:d8	QoS Data		EAPOL	191	Key (Message 2 of 4)
-53		Nintendo_35:63:78 …	Acknowledgement		802.11	46	Acknowledgement, Fla…
-49	Modacom_a8:55:d8	Nintendo_35:63:78	QoS Data		EAPOL	169	Key (Message 1 of 4)
-58	Nintendo_35:63:78	Modacom_a8:55:d8	QoS Data		EAPOL	191	Key (Message 2 of 4)
-51		Nintendo_35:63:78 …	Acknowledgement		802.11	46	Acknowledgement, Fla…
-54	Modacom_a8:55:d8	Nintendo_35:63:78	Disassociate		802.11	62	Disassociate, SN=13,…
-58	Nintendo_35:63:78	Broadcast	Probe Request		802.11	147	Probe Request, SN=41…
-54	Modacom_a8:55:d8	Nintendo_35:63:78	Probe Response		802.11	156	Probe Response, SN=1…

#6 Inspecting suspicious packets

- Open trace 6-inspectingsuspiciouspackets.pcapng
- What is the problem ?
- Which device is the cause of the issue ?
- Hint1 Use the wireless statistics
- Hint2 Look for repetition of the packet
- Hint3 the interval of Association Request



No.	Time	Signal (dBm)	Source	Destination	Type/Subtype	Data rate (Mb/s)	Protocol	Length	Info
1	0.000000	-39	Modacom_a8:55:d8	Broadcast	Beacon frame	1	802.11	150	Beacon f
2	0.002427	-89	Logitec_7c:7b:7c	Broadcast	Authentication	1	802.11	297	Authenti
3	0.004610	-40	Modacom_94:ea:bc	OrientPo_97:03…	Data	11	802.11	209	Data, SN
4	0.004926	-46		Modacom_a8:55:…	Acknowledgement	1	802.11	34	Acknowle
5	0.005379	-58	IntelCor_0a:a5:e8	Modacom_94:ea:bc	QoS Data	11	802.11	114	QoS Data
6	0.005488	-42		IntelCor_0a:a5…	Acknowledgement	11	802.11	34	Acknowle
7	0.006489	-42	Modacom_94:ea:bc	IntelCor_0a:a5…	QoS Data	11	802.11	216	QoS Data
8	0.006605	-51		Modacom_a8:55:…	Acknowledgement	11	802.11	34	Acknowle
9	0.009179	-84	Apple_ee:04:8e	Broadcast	Beacon frame	1	802.11	282	Beacon f
10	0.023120	-88	Buffalo_e6:de:b8	Broadcast	Beacon frame	1	802.11	313	Beacon f

```
      Supported Rates: 1(B) (0x82)
      Supported Rates: 2(B) (0x84)
      Supported Rates: 5.5(B) (0x8b)
      Supported Rates: 11(B) (0x96)
  ⌄ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
      Tag Number: Extended Supported Rates (50)
      Tag length: 4
      Extended Supported Rates: 24 (0x30)
      Extended Supported Rates: 36 (0x48)
      Extended Supported Rates: 48 (0x60)
      Extended Supported Rates: 54 (0x6c)
  ⌄ Tag: Vendor Specific: Microsof: WPS
      Tag Number: Vendor Specific (221)
      Tag length: 14
      OUI: 00-50-f2 (Microsof)
      Vendor Specific OUI Type: 4
      Type: WPS (0x04)
    ⌄ Version: 0x10
```

```
0000  00 00 14 00 ee 18 00 00  10 02 6c 09 a0 00 d7 9c   ........ ..l.....
0010  64 00 00 3b 00 00 3a 01  00 1d 93 a8 55 d8 00 13   d..;..:. ....U...
0020  37 a5 31 c6 00 1d 93 a8  55 d8 50 0b 00 31 64 00   7.1..... U.P..1d.
0030  00 06 64 65 66 63 6f 6e  01 04 82 84 8b 96 32 04   ..defcon ......2.
0040  30 48 60 6c dd 0e 00 50  f2 04 10 4a 00 01 10 10   0H`l...P ...J....
0050  3a 00 01 02 bc 98 ee 14                             :.......
```

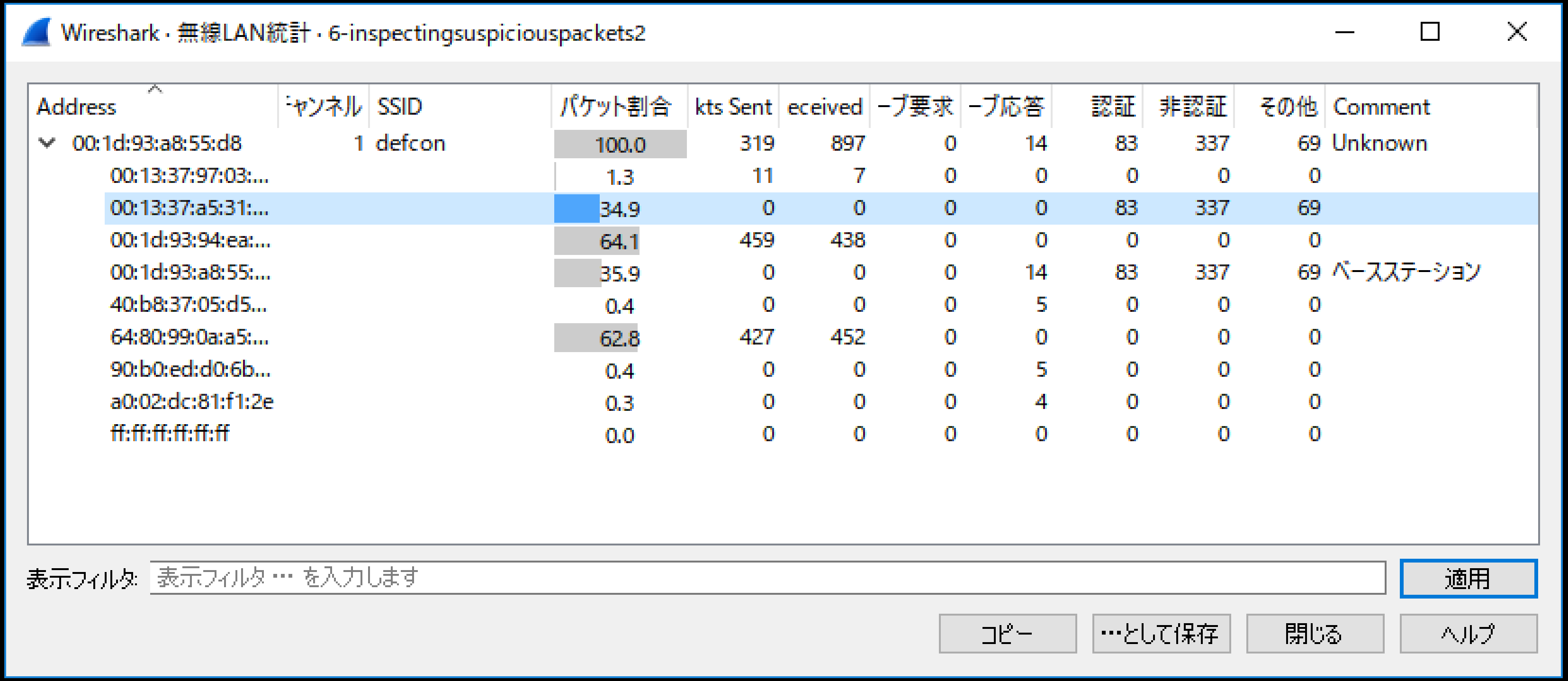
Text item (text), 5 バイト

パケット数: 6272 · 表示: 6272 (100.0%) · 読込時間: 0:0.131

プロファイル:無線LANセミナ準備用Wireshark設定

Find Abnormal traffic using wireless LAN traffic

- Wireless > Wireless LAN traffic show you the statistics of wireless packets, and the trend of the traffic
- Please refer the abnormal packets of Deauthentication.
- Select the address and right click and filter the packets.



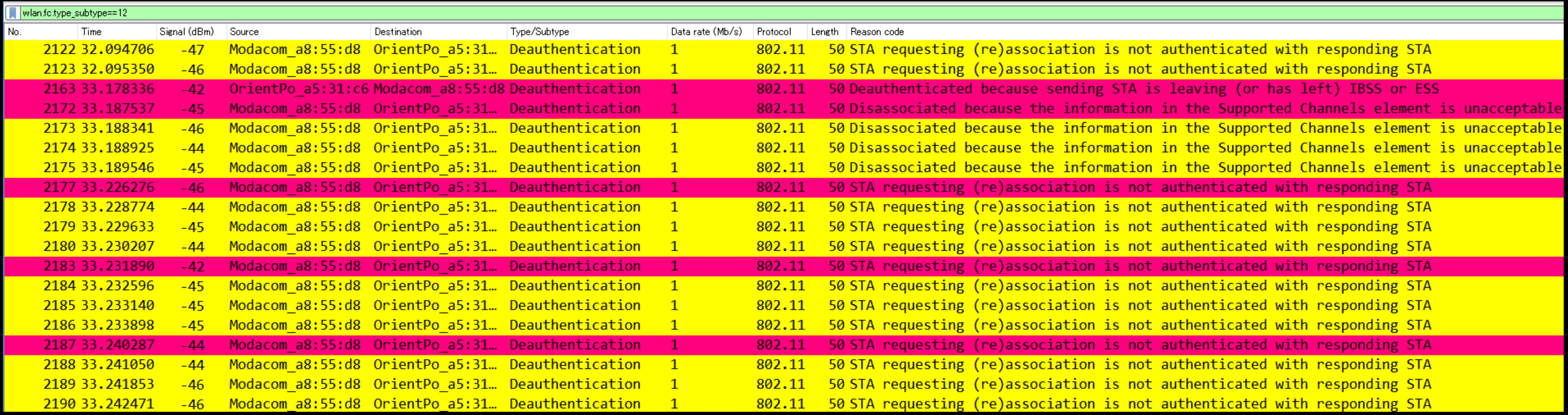
Wireshark · 無線LAN統計 · 6-inspectingsuspiciouspackets2

Address	ャンネル	SSID	パケット割合	kts Sent	eceived	ーブ要求	ーブ応答	認証	非認証	その他	Comment
00:1d:93:a8:55:d8	1	defcon	100.0	319	897	0	14	83	337	69	Unknown
00:13:37:97:03:...			1.3	11	7	0	0	0	0	0	
00:13:37:a5:31:...			34.9	0	0	0	0	83	337	69	
00:1d:93:94:ea:...			64.1	459	438	0	0	0	0	0	
00:1d:93:a8:55:...			35.9	0	0	0	14	83	337	69	ベースステーション
40:b8:37:05:d5...			0.4	0	0	0	5	0	0	0	
64:80:99:0a:a5:...			62.8	427	452	0	0	0	0	0	
90:b0:ed:d0:6b...			0.4	0	0	0	5	0	0	0	
a0:02:dc:81:f1:2e			0.3	0	0	0	4	0	0	0	
ff:ff:ff:ff:ff:ff			0.0	0	0	0	0	0	0	0	

表示フィルタ: 表示フィルタ … を入力します

Reaver attack to brute force crack WPA Password

- Please check reason code of Deauthentication frame
  filter deauth (wlan.fc.type_subtype ==12)



wlan.fc.type_subtype==12

No.	Time	Signal (dBm)	Source	Destination	Type/Subtype	Data rate (Mb/s)	Protocol	Length	Reason code
2122	32.094706	-47	Modacom_a8:55:d8	OrientPo_a5:31…	Deauthentication	1	802.11	50	STA requesting (re)association is not authenticated with responding STA
2123	32.095350	-46	Modacom_a8:55:d8	OrientPo_a5:31…	Deauthentication	1	802.11	50	STA requesting (re)association is not authenticated with responding STA
2163	33.178336	-42	OrientPo_a5:31:c6	Modacom_a8:55:d8	Deauthentication	1	802.11	50	Deauthenticated because sending STA is leaving (or has left) IBSS or ESS
2172	33.187537	-45	Modacom_a8:55:d8	OrientPo_a5:31…	Deauthentication	1	802.11	50	Disassociated because the information in the Supported Channels element is unacceptable
2173	33.188341	-46	Modacom_a8:55:d8	OrientPo_a5:31…	Deauthentication	1	802.11	50	Disassociated because the information in the Supported Channels element is unacceptable
2174	33.188925	-44	Modacom_a8:55:d8	OrientPo_a5:31…	Deauthentication	1	802.11	50	Disassociated because the information in the Supported Channels element is unacceptable
2175	33.189546	-45	Modacom_a8:55:d8	OrientPo_a5:31…	Deauthentication	1	802.11	50	Disassociated because the information in the Supported Channels element is unacceptable
2177	33.226276	-46	Modacom_a8:55:d8	OrientPo_a5:31…	Deauthentication	1	802.11	50	STA requesting (re)association is not authenticated with responding STA
2178	33.228774	-44	Modacom_a8:55:d8	OrientPo_a5:31…	Deauthentication	1	802.11	50	STA requesting (re)association is not authenticated with responding STA
2179	33.229633	-45	Modacom_a8:55:d8	OrientPo_a5:31…	Deauthentication	1	802.11	50	STA requesting (re)association is not authenticated with responding STA
2180	33.230207	-44	Modacom_a8:55:d8	OrientPo_a5:31…	Deauthentication	1	802.11	50	STA requesting (re)association is not authenticated with responding STA
2183	33.231890	-42	Modacom_a8:55:d8	OrientPo_a5:31…	Deauthentication	1	802.11	50	STA requesting (re)association is not authenticated with responding STA
2184	33.232596	-45	Modacom_a8:55:d8	OrientPo_a5:31…	Deauthentication	1	802.11	50	STA requesting (re)association is not authenticated with responding STA
2185	33.233140	-45	Modacom_a8:55:d8	OrientPo_a5:31…	Deauthentication	1	802.11	50	STA requesting (re)association is not authenticated with responding STA
2186	33.233898	-45	Modacom_a8:55:d8	OrientPo_a5:31…	Deauthentication	1	802.11	50	STA requesting (re)association is not authenticated with responding STA
2187	33.240287	-44	Modacom_a8:55:d8	OrientPo_a5:31…	Deauthentication	1	802.11	50	STA requesting (re)association is not authenticated with responding STA
2188	33.241050	-44	Modacom_a8:55:d8	OrientPo_a5:31…	Deauthentication	1	802.11	50	STA requesting (re)association is not authenticated with responding STA
2189	33.241853	-46	Modacom_a8:55:d8	OrientPo_a5:31…	Deauthentication	1	802.11	50	STA requesting (re)association is not authenticated with responding STA
2190	33.242471	-46	Modacom_a8:55:d8	OrientPo_a5:31…	Deauthentication	1	802.11	50	STA requesting (re)association is not authenticated with responding STA

- Many Deauthentication frames in a seconds, it is a symptom of attack, Reaver that exploits a security hole in wireless routers using WPS brute force attack. But now many routers are patched and protected, and WPS tend to be disabled.

Thank you