Capturing WiFi6E with Wireshark

SharkFest'23 US
San Diego, CA • June 10-15

#sf23us

https://www.ikeriri.ne.jp/sharkfest/CapturingWiFi6EwithWireshark.zip

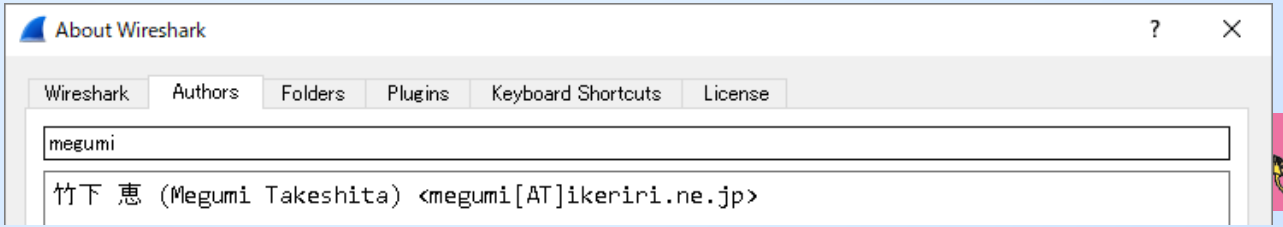
09 17:00 -18:15 PDT

on Tuesday, June 13, 2023

Megumi Takeshita
Ikeriri network service

Megumi Takeshita, packet otaku

- Founder, ikeriri network service co., ltd
- Reseller of CACE technologies in 2008
- Worked SE/IS at BayNetwork, Nortel
- Wrote 10+ books about Wireshark
- Instruct Wireshark to JSDF and other company
- lecturer of CHUO University
- Reseller of packet capture / wireless-tools
- One of the contributors of Wireshark
  Translate Wireshark into Japanese



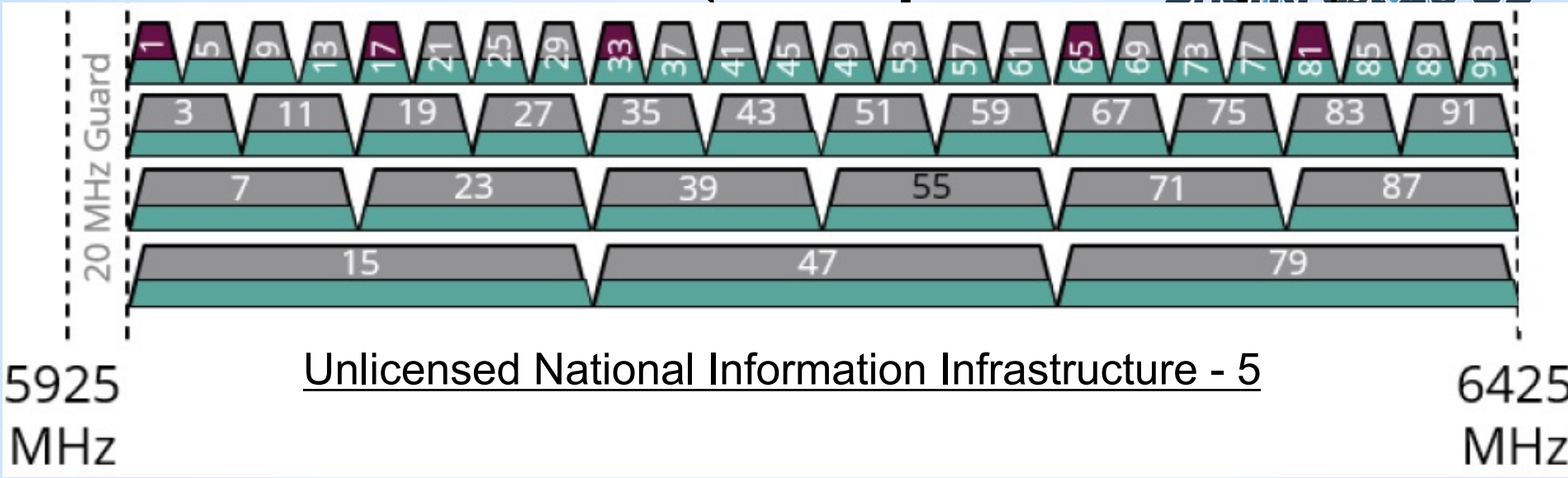
Session Details

WiFi6E implementation is (will be) released in Japan this year, as the United States has already started. Europe and the other world are also ready for 6GHz WiFi bands. It is time to analyse WiFi6E with Wireshark.

In this session, we capture IEEE802.11ax in 6GHz channels. And we dissect specified fields of the radiotap / IEEE 802.11. header in 6E trace files using Wireshark.

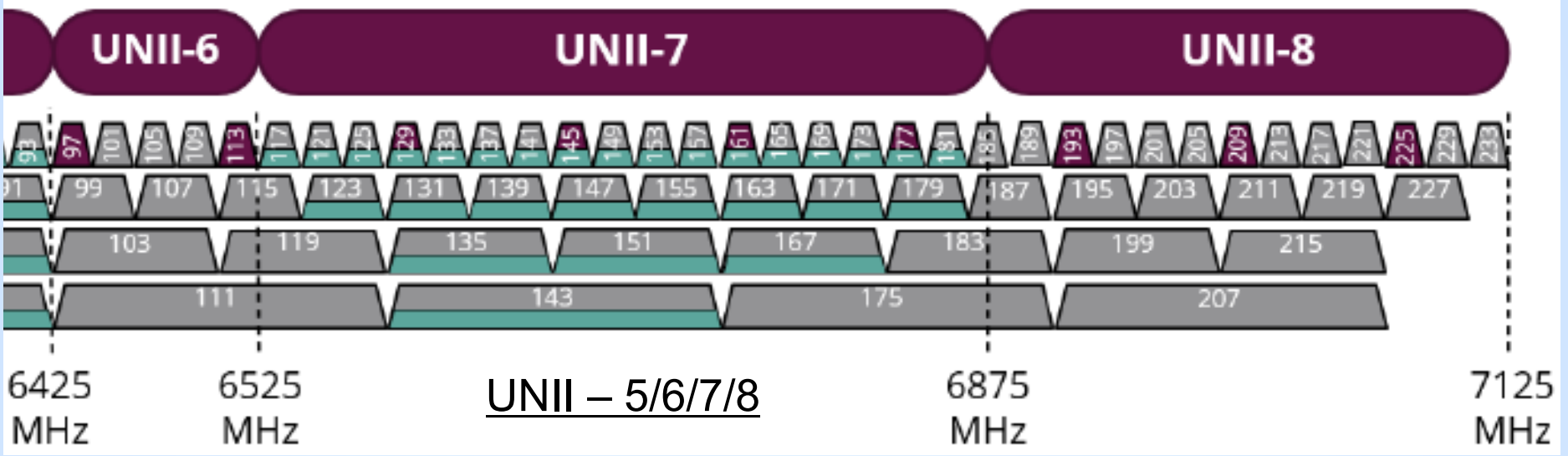
Megumi (JA1UVG) also demonstrates spectrum analysis in the 6GHz band and indicates how to create capture environments in Windows, Linux and macOS. The session also includes basics of radio technology basic and IEEE 802.11 standards.

WiFi6E CH1 to 93 (in Japan/Europe)



- UNII-5 band comes in Japan and Europe
- We can choose bandwidth from 20/40/80/160 using channels 1-93

UNII-5/6/7/8 in US CH1 to 233



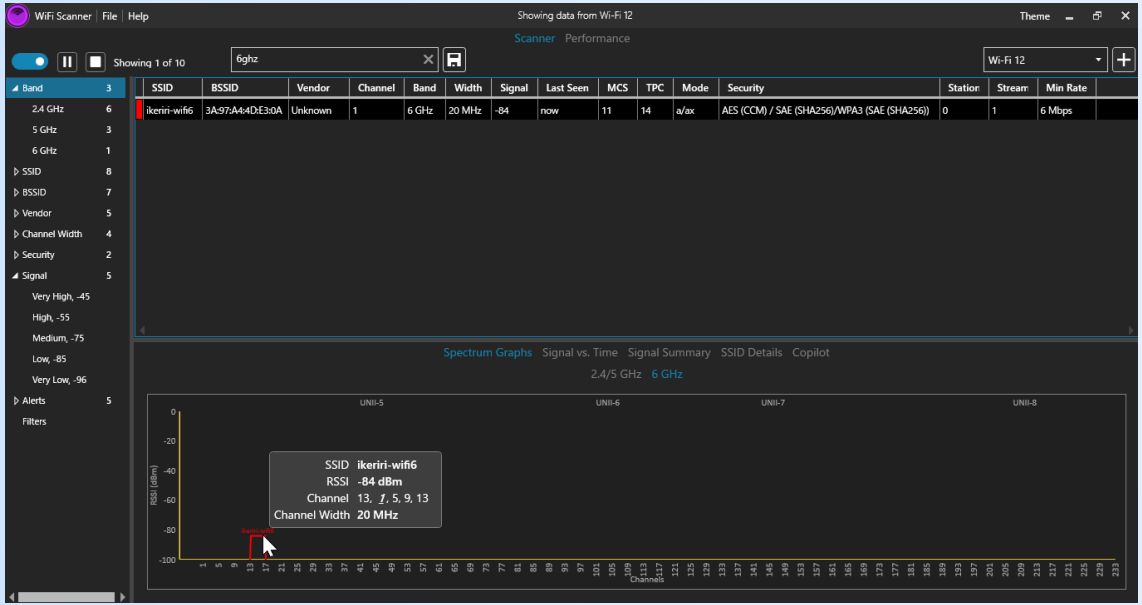
UNII – 5/6/7/8

- We can use additional UNII 6/7/8 bands in the US
- We can choose bandwidth from 20/40/80/160 using channels 1-93/97-233

Live Demo (AccessAgility WiFi Scanner)

SharkFest'23 US
San Diego, CA • June 10-15

#sf23us



- Open WiFi Scanner Application
- Choose a WiFi adapter (friendly name) from list

- Check the access points and right-click.
  > Copy all columns and header name

Live Demo (WiFi Scanner)

SSID: ikeriri-wifi6
BSSID: 3A:97:A4:4D:E3:0A
Vendor: Unknown
Channel: 1 (5,9,13)
Band: 6 GHz
Width: 20 MHz
Signal: -89
Last Seen: now
MCS: 11
TPC: 14 (transmit power control)
Mode: a/ax
Security: AES (CCM) / SAE (SHA256)/WPA3 (SAE (SHA256))
Station Count: 0
Streams: 1
Min Rate: 6 Mbps

- Select the SSID Details tab and check IEEE802.11 management header information

Spectrum Graphs | Signal vs. Time | Signal Summary | SSID Details | Copilot

ID	Length	Name (Expand All)	Details
		+ Fixed Parameters	
	251 Bytes	− Tagged Parameters	20 Parameters
0	13 Bytes	+ SSID parameter set	SSID: ikeriri-wifi6
1	8 Bytes	+ Supported Rates	6 (B) , 9 , 12 (B) , 18 , 24 (B) , 36 , 48 , 54 Mbit/sec
7	10 Bytes	+ Country Information	Country Code: JP | Environment: Unknown environment (4)
32	1 Bytes	+ Power Constraint	Local Power Constraint: 0
35	2 Bytes	+ TPC Report	Transmit Power: 14dBm | Link Margin: 0
50	1 Bytes	+ Extended Supported Rates	251 Unknown Rate. Mbit/sec
48	20 Bytes	+ RSN Information	00:0F:AC | AES (CCM) | SAE (SHA256)
127	11 Bytes	+ Extended Capabilities	Octet 1: 0x04 | Octet 2: 0x00 | Octet 3: 0x4F | Octet 4: 0x02 | Octet 5: 0x00 | Octet 6: 0x00 | Octet 7: 0x00 | Octet: 0x4040 | Octet: 0x41
195	2 Bytes	+ VHT Tx Power Envelope	Parsing not yet implemented
195	2 Bytes	+ VHT Tx Power Envelope	Parsing not yet implemented
244	1 Bytes	+ 244 Reserved	Parsing not yet implemented
255	33 Bytes	+ Ext Tag: HE Capabilities	HE Capabilities
255	12 Bytes	+ Ext Tag: HE Operation	HE Operation
255	2 Bytes	+ Element ID Extension	Parsing not yet implemented
255	14 Bytes	+ Element ID Extension	Parsing not yet implemented
255	3 Bytes	+ Ext Tag: HE 6GHz Band Capabilities	HE 6GHz Band Capabilities
221	23 Bytes	+ Vendor Specific	Qualcomm Inc.
221	24 Bytes	+ Vendor Specific	Microsoft Corp. | WMM/WME (0x02) | Parameter Element (1)
221	22 Bytes	+ Vendor Specific	Qualcomm Inc.
221	7 Bytes	+ Vendor Specific	Qualcomm Inc.

Ext Tag: HE 6GHz Band Capabilities

255	3 Bytes	− Ext Tag: HE 6GHz Band Capabilities	HE 6GHz Band Capabilities
		Number	255
		Length	3 Bytes
		Ext Tag Number	HE 6GHz Band Capabilities (36)
		− Capabilities Information	0xB836
		.... .000	Minimum MPDU Start Spacing: No restriction
		....11 1...	Maximum A-MPDU Length Exponent: 1 048 575
		.... 10..	Maximum MPDU Length: 11 454
		....0	Reserved: 0x0
		.... .11.	SM Power Save: SM Power Save disabled
		.... 0...	RD Responder: Not supported
		...1	Rx Antenna Pattern Consistency: Supported
		..1.	Tx Antenna Pattern Consistency: Supported
		00..	Reserved: 0x0
		Data	3BB836

255	33 Bytes	+ Ext Tag: HE Capabilities	HE Capabilities
255	12 Bytes	+ Ext Tag: HE Operation	HE Operation

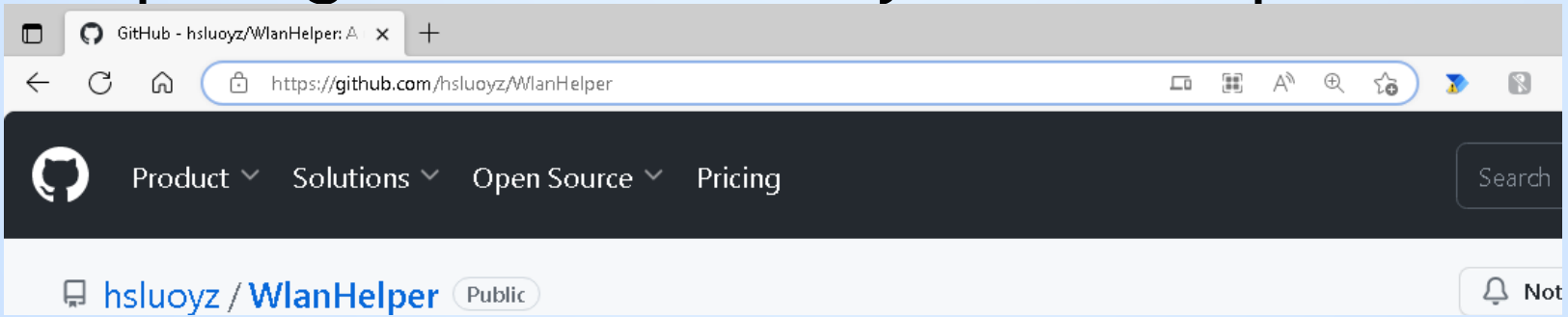
HE 6GHz Band Capabilities

- MPDU setting 802.11 MAC protocol data unit configuration
- Power Saving
- Antenna Pattern

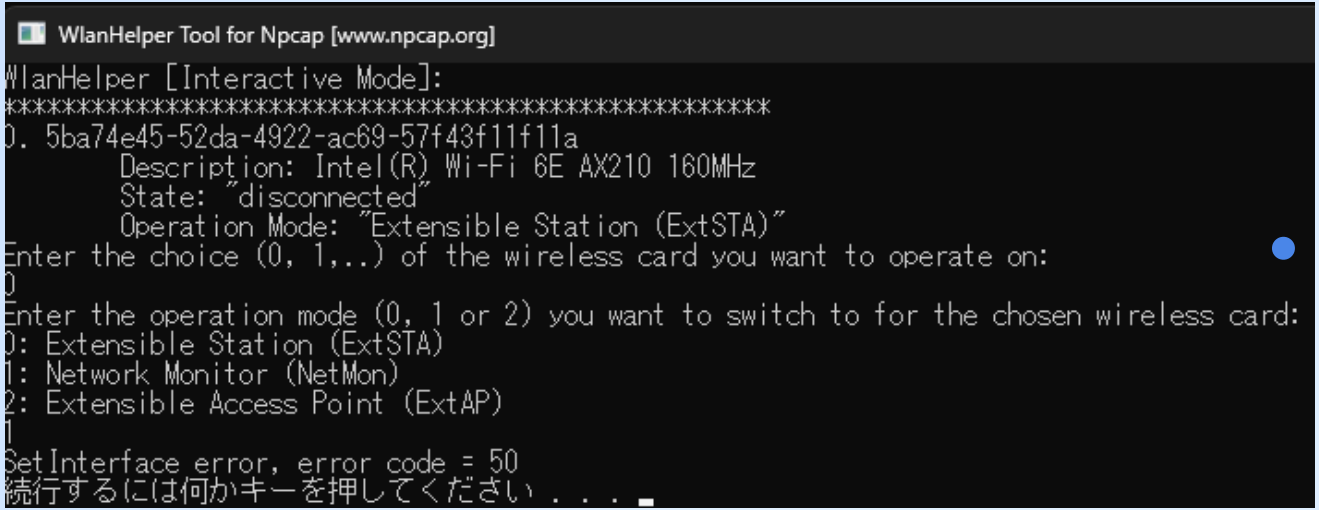
- WiFi6E also uses IEEE802.ax like WiFi6, so the beacon contains HE Capabilities, HE Operation tag
- Both tags show IEEE802.11ax settings

Capturing WiFi6E in Windows environment

- As usual wifi adapter works in managed mode.
- We need to change it into monitor mode.
- Windows OS's NDIS API functions are limited, so we can not change Intel AX adapter into monitor mode.
- You may use WlanHelper in specified environments. https://github.com/hsluoyz/WlanHelper



Live Demo WlanHelper



- One stream only
- basic MCS
- NDIS restriction

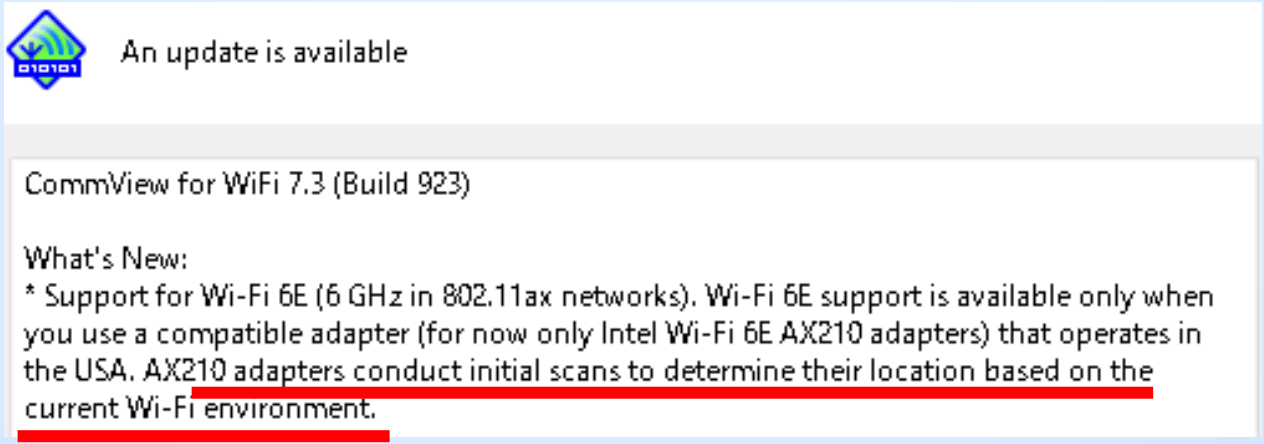
- Open WlanHelper with the administrator right
- Choose wireless adapter
- Choose the operation mode as Network Monitor
- You can capture traffic if succeed

Alternatives Commercial products

- There are some alternative commercial products in the Windows environment
- TamoSoft CommView for WiFi is one of them. https://www.tamos.com/products/commwifi/
- CommView uses its customized monitor mode driver based on Windows wireless driver.
- Intel AX210, AX211, AX411 support 6GHz in the US, but only AX210 works in Japan (maybe another area like Europe) for the initial scan problem.

Initial Scan problem of Intel AX cards

- Intel produces the same M.2 wireless card hardware worldwide, though every country/area has its radio laws/limitations.
- How does it decide this? Intel uses an initial scan to determine the location based on the current WiFi environment. Intel does not show the source…



Let's Alibaba to find RF Shielding room

- There are some solutions to use WiFi6E until last year, we need Electromagnetic Compatibility (EMC) and Radio Frequency (RF) testing environments.
- For example, go Alibaba to find Shielding Room/Box

Home / Electronic Components, Accessories & Telecommunications / Telecommunications / Other Telecommunications Products

Manufacturer Serials RF EMC Shielding Room

1 - 14 pieces	15 - 29 pieces	>= 30 pieces
$9,000.00	$8,500.00	$8,000.00

Benefits: Quick refunds on orders under US $1,000

Specification: HM-MSR

Lead time:

Quantity (pieces)	1 - 1	> 1
Lead time (days)	5000	To be negotiated

HDRF-1560-C RF Shield Test Box

HDRF-1560-C

View product

But pricy….

Create DIY EMC/RF testing chamber / box

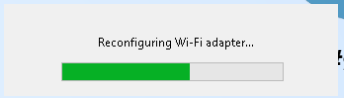
- We need to avoid the other wireless signals
  So go to the kitchen and find steel bowls (may reduce>20dB) or create a DIY testing chamber/box.
- Finally, Intel changed the base driver of AX210, and we do not need a special environment, “netsh wlan sh all” to check version >22.190.0.4 works in Japan

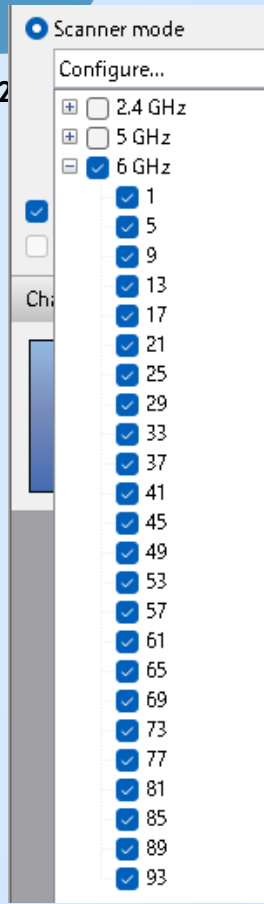
Steel bowl is not perfect but it decreases over 20dB, Sometimes it meets the signal threshold of the wireless card.

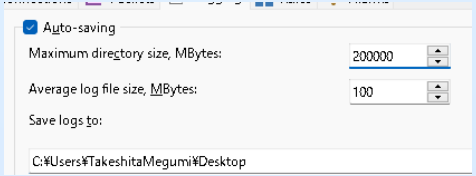
```
C:\Users\TakeshitaMegumi>netsh wlan sh all | more
ワイヤレス システム情報の要約
(時間: 2023/06/03 10:43:21 東京 (標準時))


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


インターフェイス名: Wi-Fi 12

    ドライバー                  : Intel(R) Wi-Fi 6E AX210 160MHz
    ベンダー                    : Intel Corporation
    プロバイダー                : Intel
    日付                        : 2023/03/09
    バージョン                  : 22.200.2.1
    INF ファイル                : oem52.inf
```

Live Demo CommView for WiFi with AX210

- Open CommView for WiFi, automatically install monitor mode, commercial driver
- We test with version 7.3 build 939 choose scanner mode and select all 6GHz channel (from 1 to 93 in Japan)
- Show Logging tab to save packets at Desktop
- Check View>Channnels and Spectrum pane
- Check Data/Management/Control frames







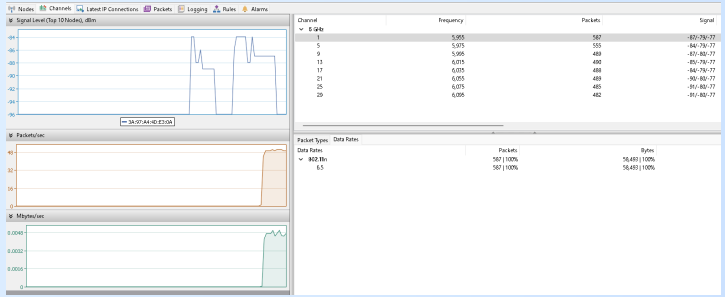
Live Demo CommView for WiFi with AX210

- Click start to hop the 6GHz channel
- We can find the SSID “ikeriri-wifi6” on channel 1(1 and 5 at bandwidth 40MHz, 1,5,9,13 at 80MHz and 1,5,9,13,17,21,25,29 at 160MHz)

Standard / MAC Address	Channel	Type	SSID	Standard	Encryption	Signal	Max Rate	Streams
802.11ax (6 GHz)								
3A:97:A4:4D:E3:0A	1 (1-5@40, 1-13@80, 1-29@160)	AP	ikeriri-wifi6	802.11ax (6 GHz)	WPA3SAE (CCMP)	-91/-83/-77	2041.7	2

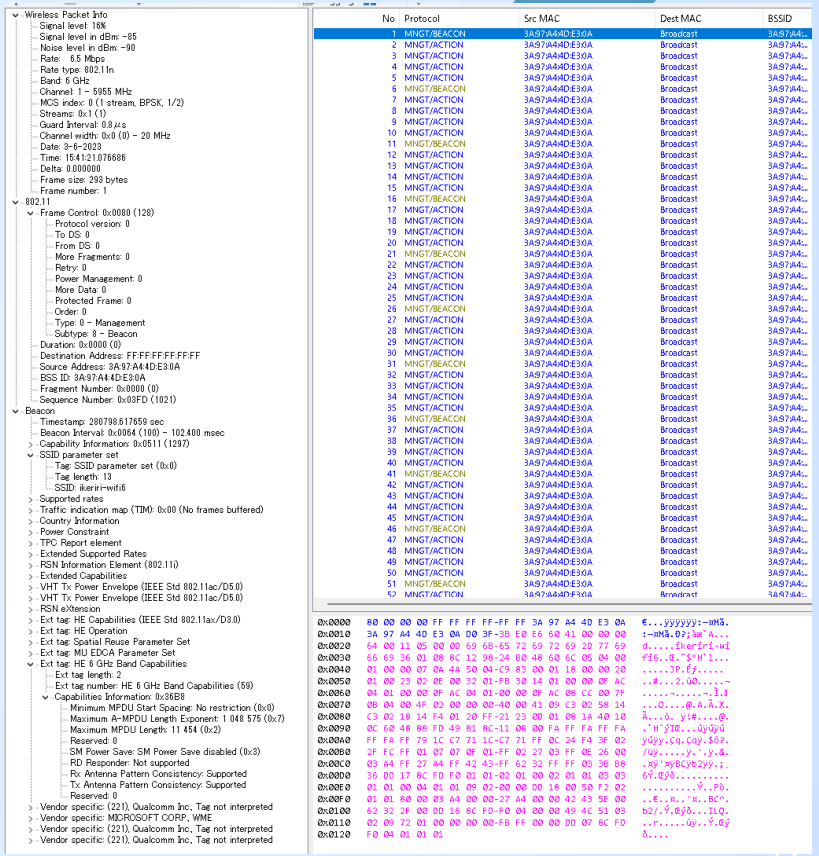
Standards: IEEE802.11ax(6GHz), Security:WPA3SAE Max PHY rate: 2041.7MHz Streams:2 and more.

- Select Channels tab to check the channel from 1 to 29



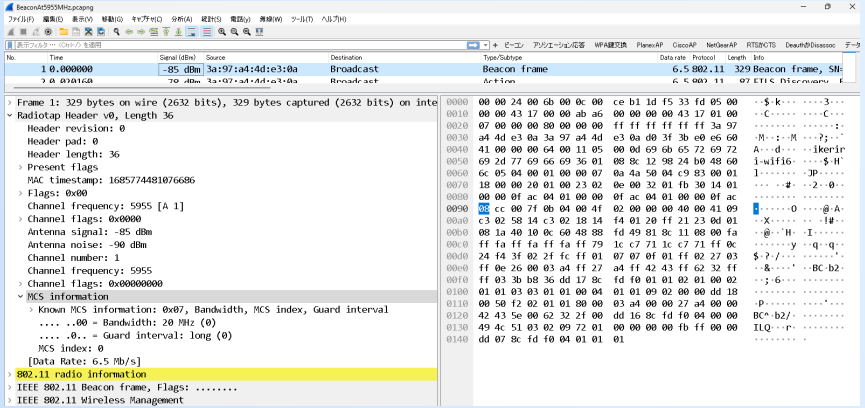
Live Demo CommView for WiFi with AX210

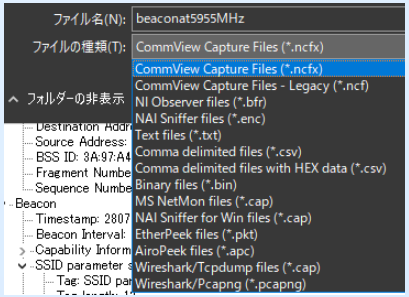
- Select the Packets tab to check the beacon
- Wireless Packet Info shows Band: 6GHz, Channnel:1
- SSID parameter set shows SSID: ikeriri-wifi6
- We can also find IEEE802.11 management header tag HE 6GHz Band Capabilities
- We can also find some action frames too

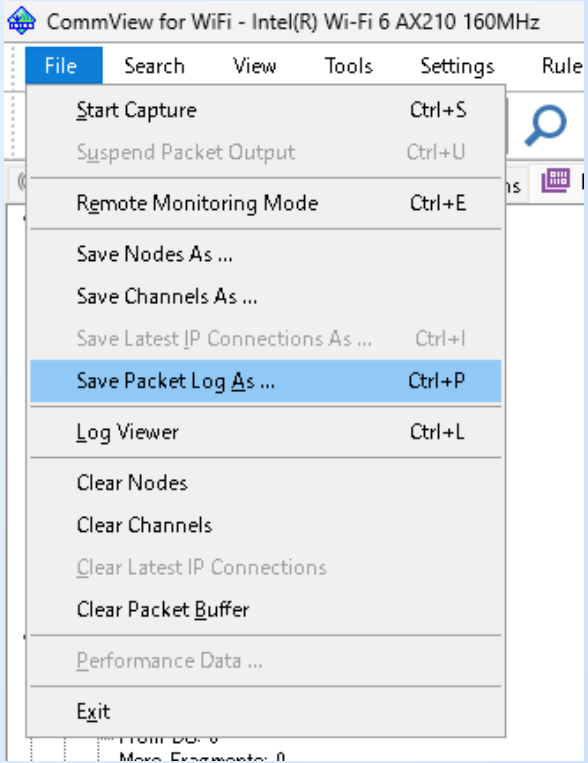


Convert trace file as pcapng

- We export ncfx trace file into pcapng, open the trace file (.ncfx) with CommView for WiFi, Select File>Save Packet Log As … and choose file type as pcapng "BeaconAt5955MHz.pcapng"
- It's the time for Wireshark

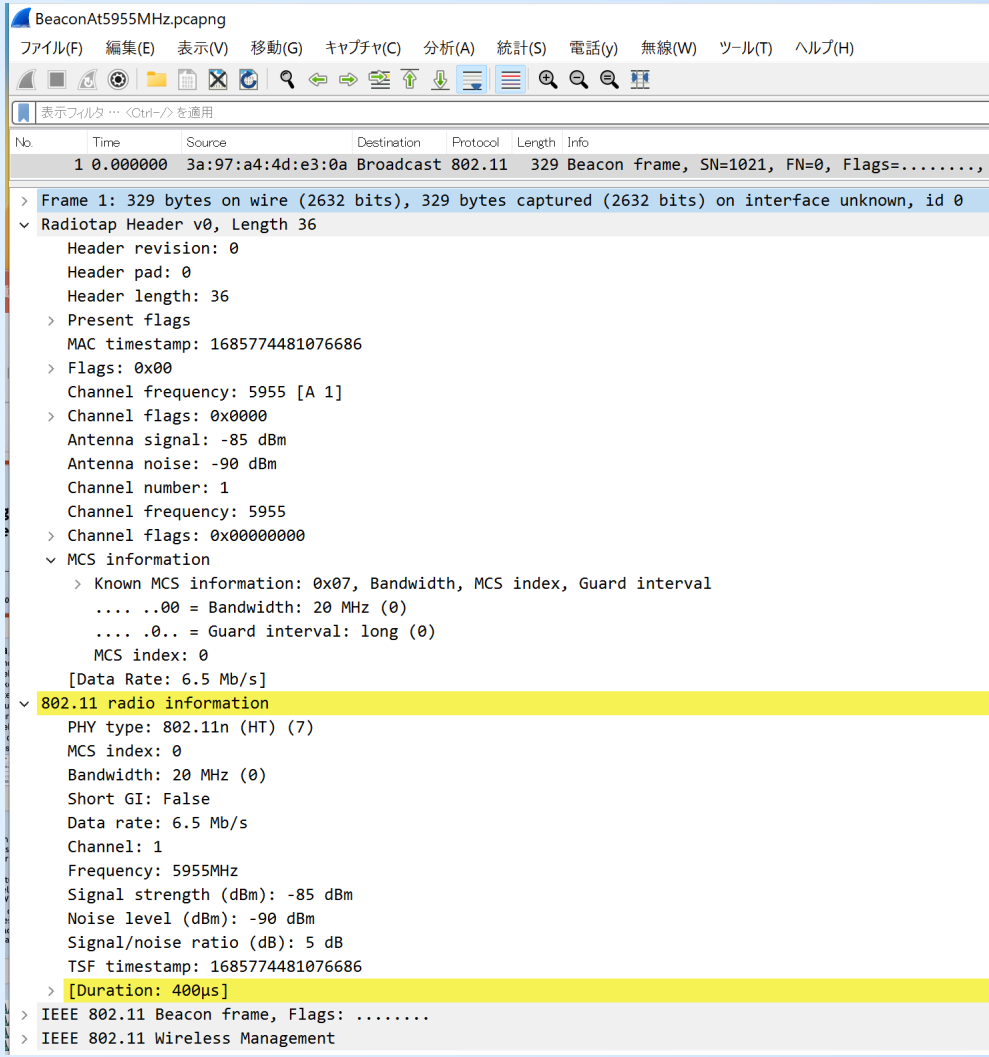






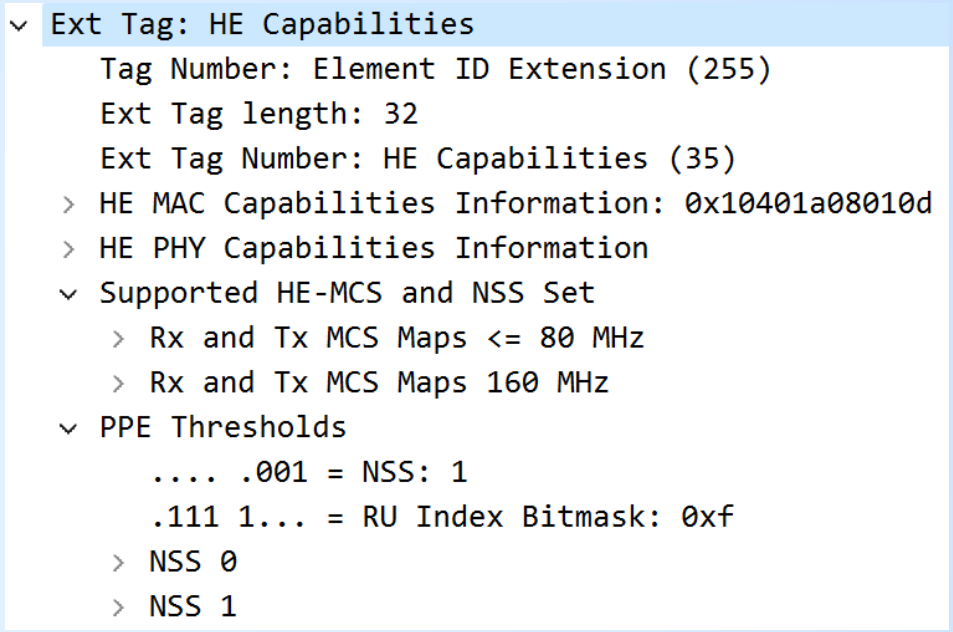
Check dissectors of Radiotap header 802.11 radio info

- Channel frequency
  MCS information
  in Radiotap header
- PHY type
  MCS index
  in 802.11 radio info
- Then open IEEE802.11 Wireless Management



Ext Tag: HE Capabilities

- HE Capabilities shows the spec of IEEE802.11ax
- HE MAC represents MAC layer spec like Aggregation frame MSDU, Trigger frame settings.
- HE PHY shows physical layer specs, Guard Interval, Beamforming



- Supported HE-MCS and NSS contains MCS mapping
- PPE Thresholds show RU MU-OFDMA information

Ext Tag: HE Operation

- HE Operation shows AP settings of WiFi6/6E
  - TWT (Target Wake Time)
  - RTS Threshold
  - VHT(IEEE802.11ac)
  - BSS Coloring
- MCS index settings
- 6GHz Operation Info shows Primary Channel, Channel frequency etc.

```
Ext Tag: HE Operation
    Tag Number: Element ID Extension (255)
    Ext Tag length: 11
    Ext Tag Number: HE Operation (36)
  HE Operation Parameters: 0x023ff4
      .... .... .... .... .... .100 = Default PE Duration: 4
      .... .... .... .... .... 0... = TWT Required: Not required
      .... .... ..11 1111 1111 .... = TXOP Duration RTS Threshold: 1023
      .... .... .0.. .... .... .... = VHT Operation Information Present: False
      .... .... 0... .... .... .... = Co-Hosted BSS: False
      .... ...0 .... .... .... .... = ER SU Disable: False
      .... ..1. .... .... .... .... = 6 GHz Operation Information Present: True
      0000 00.. .... .... .... .... = Reserved: 0x00
  BSS Color Information: 0x2f
      ..10 1111 = BSS Color: 0x2f
      .0.. .... = Partial BSS Color: False
      0... .... = BSS Color Disabled: False
  Basic HE-MCS and NSS Set: 0xfffc
      .... .... .... ..00 = Max HE-MCS for 1 SS: Support for HE-MCS 0-7 (0)
      .... .... .... 11.. = Max HE-MCS for 2 SS: Not supported for HE PPDUs (3)
      .... .... ..11 .... = Max HE-MCS for 3 SS: Not supported for HE PPDUs (3)
      .... .... 11.. .... = Max HE-MCS for 4 SS: Not supported for HE PPDUs (3)
      .... ..11 .... .... = Max HE-MCS for 5 SS: Not supported for HE PPDUs (3)
      .... 11.. .... .... = Max HE-MCS for 6 SS: Not supported for HE PPDUs (3)
      ..11 .... .... .... = Max HE-MCS for 7 SS: Not supported for HE PPDUs (3)
      11.. .... .... .... = Max HE-MCS for 8 SS: Not supported for HE PPDUs (3)
  6 GHz Operation Information
      Primary Channel: 1
    Control: 0x07
        .... ..11 = Channel Width: 160MHz or 80MHz+80MHz (3)
        .... .1.. = Duplicate Beacon: True
        ..00 0... = Regulatory Info: 0
        00.. .... = Reserved: 0
      Channel Center Frequency Segment 0: 7
      Channel Center Frequency Segment 1: 15
      Minimum Rate: 1
```

www.mcsindex.com

MCS

Full MCS Table (HT/VHT/HE) | MCS Table 3SS (HT/VHT/HE) | MCS Table HE | **MCS Table HE (OFDM)** | MCS Table HE (OFDMA) | The Math Behind it | Credit

				OFDM (802.11ax)											
MCS Index	Spatial Stream	Modulation	Coding	20MHz			40MHz			80MHz			160MHz		
				0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI
0	1	BPSK	1/2	8.6	8.1	7.3	17.2	16.3	14.6	36	34	30.6	72.1	68.1	61.3
1	1	QPSK	1/2	17.2	16.3	14.6	34.4	32.5	29.3	72.1	68.1	61.3	144.1	136.1	122.5
2	1	QPSK	3/4	25.8	24.4	21.9	51.6	48.8	43.9	108.1	102.1	91.9	216.2	204.2	183.8
3	1	16-QAM	1/2	34.4	32.5	29.3	68.8	65	58.5	144.1	136.1	122.5	288.2	272.2	245
4	1	16-QAM	3/4	51.6	48.8	43.9	103.2	97.5	87.8	216.2	204.2	183.8	432.4	408.3	367.5
5	1	64-QAM	2/3	68.8	65	58.5	137.6	130	117	288.2	272.2	245	576.5	544.4	490
6	1	64-QAM	3/4	77.4	73.1	65.8	154.9	146.3	131.6	324.3	306.3	275.6	648.5	612.5	551.3
7	1	64-QAM	5/6	86	81.3	73.1	172.1	162.5	146.3	360.3	340.3	306.3	720.6	680.6	612.5
8	1	256-QAM	3/4	103.2	97.5	87.8	206.5	195	175.5	432.4	408.3	367.5	864.7	816.7	735
9	1	256-QAM	5/6	114.7	108.3	97.5	229.4	216.7	195	480.4	453.7	408.3	960.8	907.4	816.7
10	1	1024-QAM	3/4	129	121.9	109.7	258.1	243.8	219.4	540.4	510.4	459.4	1080.9	1020.8	918.8
11	1	1024-QAM	5/6	143.4	135.4	121.9	286.8	270.8	243.8	600.5	567.1	510.4	1201	1134.3	1020.8

WiFi6/6E uses their own MCS index

MCS

Full MCS Table (HT/VHT/HE) | MCS Table 3SS (HT/VHT/HE) | MCS Table HE | MCS Table HE (OFDM) | **MCS Table HE (OFDMA)** | The Math Behind it | Credit

				MU-OFDMA (802.11ax)																
MCS Index	Spatial Stream	Modulation	Coding	26-tone RU			52-tone RU			106-tone RU			242-tone RU			484-tone RU			996-tone RU		
				0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI
0	1	BPSK	1/2	0.9	0.8	0.8	1.8	1.7	1.5	3.8	3.5	3.2	8.6	8.1	7.3	17.2	16.3	14.6	36	34	30.6
1	1	QPSK	1/2	1.8	1.7	1.5	3.5	3.3	3	7.5	7.1	6.4	17.2	16.3	14.6	34.4	32.5	29.3	72.1	68.1	61.3
2	1	QPSK	3/4	2.6	2.5	2.3	5.3	5	4.5	11.3	10.6	9.6	25.8	24.4	21.9	51.6	48.8	43.9	108.1	102.1	91.9
3	1	16-QAM	1/2	3.5	3.3	3	7.1	6.7	6	15	14.2	12.8	34.4	32.5	29.3	68.8	65	58.5	144.1	136.1	122.5
4	1	16-QAM	3/4	5.3	5	4.5	10.6	10	9	22.5	21.3	19.1	51.6	48.8	43.9	103.2	97.5	87.8	216.2	204.2	183.8
5	1	64-QAM	2/3	7.1	6.7	6	14.1	13.3	12	30	28.3	25.5	68.8	65	58.5	137.6	130	117	288.2	272.2	245
6	1	64-QAM	3/4	7.9	7.5	6.8	15.9	15	13.5	33.8	31.9	28.7	77.4	73.1	65.8	154.9	146.3	131.6	324.3	306.3	275.6
7	1	64-QAM	5/6	8.8	8.3	7.5	17.6	16.7	15	37.5	35.4	31.9	86	81.3	73.1	172.1	162.5	146.3	360.3	340.3	306.3
8	1	256-QAM	3/4	10.6	10	9	21.2	20	18	45	42.5	38.3	103.2	97.5	87.8	206.5	195	175.5	432.4	408.3	367.5
9	1	256-QAM	5/6	11.8	11.1	10	23.5	22.2	20	50	47.2	42.5	114.7	108.3	97.5	229.4	216.7	195	480.4	453.7	408.3
10	1	1024-QAM	3/4	13.2	12.5	11.3	26.5	25	22.5	56.3	53.1	47.8	129	121.9	109.7	258.1	243.8	219.4	540.4	510.4	459.4
11	1	1024-QAM	5/6	14.7	13.9	12.5	29.4	27.8	25	62.5	59	53.1	143.4	135.4	121.9	286.8	270.8	243.8	600.5	567.1	510.4

MU-OFDMA divides subcarrier By RU (2MHz)

Ext Tag: HE 6GHz Band Capabilities

- Additional info of WiFI6E
- Aggregation frame A-MPDU settings

```
Ext Tag: HE 6 GHz Band Capabilities
    Tag Number: Element ID Extension (255)
    Ext Tag length: 2
    Ext Tag Number: HE 6 GHz Band Capabilities (59)
  Capabilities Information: 0x36b8
      .... .... .... .000 = Minimum MPDU Start Spacing: No restriction (0x0)
      .... .... ..11 1... = Maximum A-MPDU Length Exponent: 1 048 575 (0x7)
      .... .... 10.. .... = Maximum MPDU Length: 11 454 (0x2)
      .... ...0 .... .... = Reserved: 0x0
      .... .11. .... .... = SM Power Save: SM Power Save disabled (0x3)
      .... 0... .... .... = RD Responder: Not supported
      ...1 .... .... .... = Rx Antenna Pattern Consistency: Supported
      ..1. .... .... .... = Tx Antenna Pattern Consistency: Supported
      00.. .... .... .... = Reserved: 0x0
```

- These Ext Tags are different from each Aps
- Enterprise AP contains a lot of information such as IEEE802.11e QBSS, station number, utilization of bandwidth, and so on.

Live Demo link up process of 6E

- Let’s capture the link up process of WiFi6E
- Open CommView and choose single channel mode, set 1ch (6GHz).
- Start capture and connect Station to AP, Wifi off/on three times
- If you have a WiFi6E device, please try it

Settings	Value
SSID	ikeriri-wifi6
BSSID	3a:97:a4:4d:e3:0a
Channel	1 (5955MHz)
Security	WPA3-SAE
Passphrase	wireshark

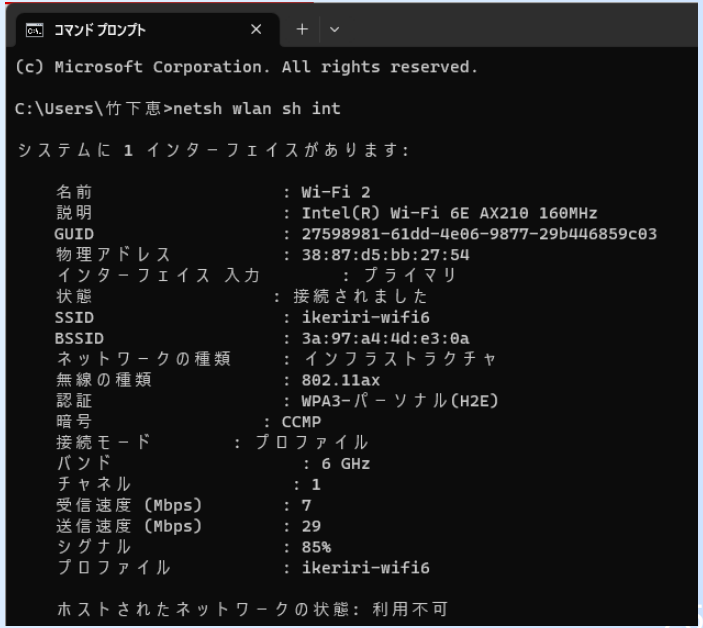
ELECOM
WRC-XE5400GSA-G

Live Demo link up process of 6E

Nodes | Channels | Latest IP Connections | Packets | Logging | Rules | Alarms

Standard / MAC Address	Channel	Type	SSID	Standard	Encryption	Signal
802.11ax (6 GHz)						
3A:97:A4:4D:E3:0A	1 (1-5@40, 1-13@80, 1-29@160)	AP	ikeriri-wifi6	802.11ax (6 GHz)	WPA3SAE (CCMP)	-85/-74/-70
Unassociated						
IntelCor:BB:27:54		STA				-86/-77/-71

- My test AP has no internet connection, but you can confirm “netsh wlan sh int” from Command Prompt
- You can see Wireless type: 802.11ax, Band:6GHz, Channel 1 (sorry in Japanese)



Wireshark profile for dissecting WiFi6/6E

- Wireshark profile makes it easy to dissection, my sample Wireshark profile wifi6 (profiles.zip) adds PHY type, Channel, Bandwidth/Resource unit, signal Strength, Noise, MCS, Stream, Data Rate and Type/Subtype. And some coloring rules and so on.

No.	Time	PHY type	Channel	BW/RU	Signal (dBm)	Noise (dBm)	MCS	Stream	Rate	Type/Subtype	Source	Destination	Length	Info
1	0.000000	802.11n (HT)	1		-76 dBm	-87 dBm			6.5	Probe Request	IntelCor_bb:27:54	Broadcast	138	Probe Request, SN=36, FN=0, Flags=........, SSID=Wildcard (Broadcast)
2	0.001169	802.11n (HT)	1		-72 dBm	-90 dBm			6.5	Probe Response	3a:97:a4:4d:e3:0a	Broadcast	323	Probe Response, SN=626, FN=0, Flags=........, BI=100, SSID="ikeriri-wif
3	63.920617	802.11n (HT)	1		-82 dBm	-92 dBm			6.5	Authentication	IntelCor_bb:27:54	3a:97:a4:4d…	164	Authentication, SN=8, FN=0, Flags=........
4	63.927002	802.11n (HT)	1		-72 dBm	-88 dBm			6.5	Authentication	3a:97:a4:4d:e3:0a	IntelCor_bb…	164	Authentication, SN=0, FN=0, Flags=........
5	63.928784	802.11n (HT)	1		-82 dBm	-88 dBm			6.5	Authentication	IntelCor_bb:27:54	3a:97:a4:4d…	100	Authentication, SN=9, FN=0, Flags=........
6	63.931552	802.11n (HT)	1		-72 dBm	-88 dBm			6.5	Authentication	3a:97:a4:4d:e3:0a	IntelCor_bb…	100	Authentication, SN=1, FN=0, Flags=........
7	63.933076	802.11n (HT)	1		-82 dBm	-88 dBm			6.5	Association Request	IntelCor_bb:27:54	[illegible]		[illegible] SSID="ikeriri-wifi6"
8	64.025355	802.11n (HT)	1		-72 dBm	-86 dBm			6.5	Association Response	3a:97:a4:4d:e3:0a	IntelCor_bb…		
9	64.032546	802.11n (HT)	1		-72 dBm	-90 dBm			6.5	QoS Data	3a:97:a4:4d:e3:0a	IntelCor_bb…		
10	64.042817	802.11n (HT)	1		-82 dBm	-90 dBm			6.5	QoS Data	IntelCor_bb:27:54	3a:97:a4:4d…		
11	64.046339	802.11n (HT)	1		-72 dBm	-90 dBm			6.5	QoS Data	3a:97:a4:4d:e3:0a	IntelCor_bb…		
12	64.048640	802.11n (HT)	1		-81 dBm	-86 dBm			6.5	QoS Data	IntelCor_bb:27:54	3a:97:a4:4d…		
13	64.105119	802.11n (HT)	1		-81 dBm	-89 dBm			6.5	QoS Null function (N…	IntelCor_bb:27:54	3a:97:a4:4d…		
14	64.105643	802.11ax (HE)	1	20	-82 dBm	-89 dBm	0x3	1 spa…	29.3	QoS Data	IntelCor_bb:27:54	3a:97:a4:4d…		
15	64.106440	802.11ax (HE)	1	20	-72 dBm	-89 dBm	0x0	1 spa…	7.3	Data	IntelCor_bb:27:54	3a:97:a4:4d…		
16	64.134835	802.11ax (HE)	1	20	-83 dBm	-88 dBm	0x3	1 spa…	29.3	QoS Data	IntelCor_bb:27:54	3a:97:a4:4d…		

Wireshark · Coloring Rules wifi6

Name	Filter
weak signal	radiotap.dbm_antsignal < -90
association response	wlan.fc.type_subtype==1
4 way handshake	eapol
Retry	wlan.fc.retry==1
Deauthentication	wlan.fc.type_subtype==12
Disassociation	wlan.fc.type_subtype==10

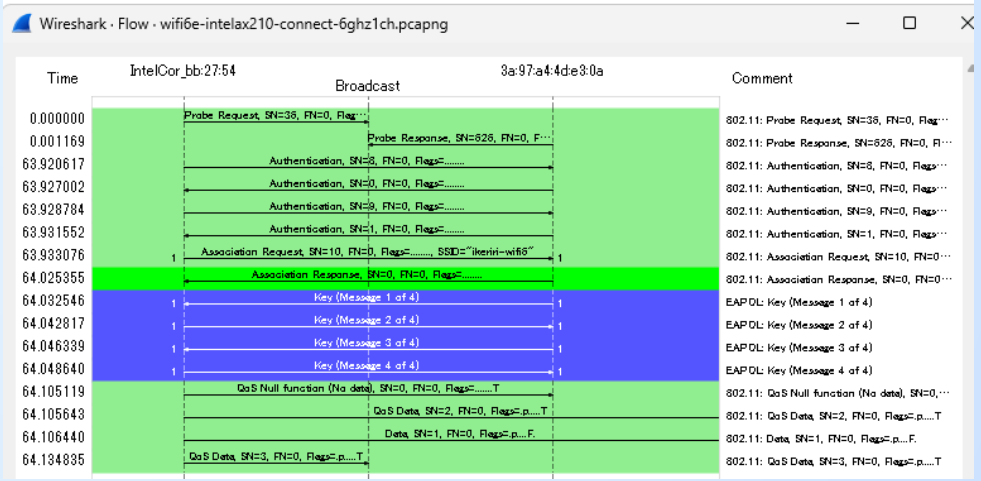
Live Demo link up process of 6E

- Save trace and export as pcapng format, "wifi6e-intelax210-connect-6ghz1ch.pcapng" #sf23us BSSID:3a:97:a4:4d:e3:0a STA:38:87:d5:bb:27:54
- You can filter traffic using a display filter, wlan.addr== Station or AP address
- Mark Probe Request, Probe Response, 4x SAE Authentications, Association Request, Association Response, four-way handshake of EAPOL and some data frames. (I recommend excluding tons of ACKs) then File>Export Specified Packets

wifi6e-intelax210-connect-6ghz1ch.pcapng

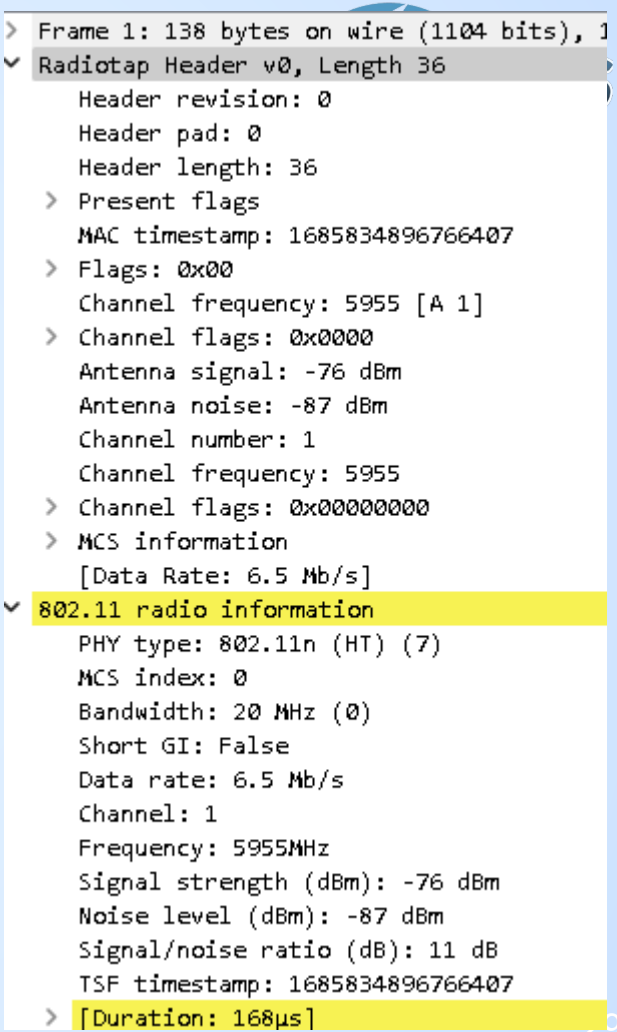
No.	Time	PHY type	Channel	BW/RU	Signal (dBm)	Noise (dBm)	MCS	Stream	Rate	Type/Subtype	Source	Destination	Length	Info
1	0.000000	802.11n (HT)	1		-76 dBm	-87 dBm			6.5	Probe Request	IntelCor_bb:27:54	Broadcast	138	Probe Request, SN=36, FN=0, Flags=........, SSID=Wildcard (Broadcast)
2	0.001169	802.11n (HT)	1		-72 dBm	-90 dBm			6.5	Probe Response	3a:97:a4:4d:e3:0a	Broadcast	323	Probe Response, SN=626, FN=0, Flags=........, BI=100, SSID="ikeriri-wifi
3	63.920617	802.11n (HT)	1		-82 dBm	-92 dBm			6.5	Authentication	IntelCor_bb:27:54	3a:97:a4:4d…	164	Authentication, SN=8, FN=0, Flags=........
4	63.927002	802.11n (HT)	1		-72 dBm	-88 dBm			6.5	Authentication	3a:97:a4:4d:e3:0a	IntelCor_bb…	164	Authentication, SN=0, FN=0, Flags=........
5	63.928784	802.11n (HT)	1		-82 dBm	-88 dBm			6.5	Authentication	IntelCor_bb:27:54	3a:97:a4:4d…	100	Authentication, SN=9, FN=0, Flags=........
6	63.931552	802.11n (HT)	1		-72 dBm	-88 dBm			6.5	Authentication	3a:97:a4:4d:e3:0a	IntelCor_bb…	100	Authentication, SN=1, FN=0, Flags=........
7	63.933076	802.11n (HT)	1		-82 dBm	-88 dBm			6.5	Association Request	IntelCor_bb:27:54	3a:97:a4:4d…	222	Association Request, SN=10, FN=0, Flags=........, SSID="ikeriri-wifi6"
8	64.025355	802.11n (HT)	1		-72 dBm	-86 dBm			6.5	Association Response	3a:97:a4:4d:e3:0a	IntelCor_bb…	229	Association Response, SN=0, FN=0, Flags=........
9	64.032546	802.11n (HT)	1		-72 dBm	-90 dBm			6.5	QoS Data	3a:97:a4:4d:e3:0a	IntelCor_bb…	191	Key (Message 1 of 4)
10	64.042817	802.11n (HT)	1		-82 dBm	-90 dBm			6.5	QoS Data	IntelCor_bb:27:54	3a:97:a4:4d…	200	Key (Message 2 of 4)
11	64.046339	802.11n (HT)	1		-72 dBm	-90 dBm			6.5	QoS Data	3a:97:a4:4d:e3:0a	IntelCor_bb…	257	Key (Message 3 of 4)
12	64.048640	802.11n (HT)	1		-81 dBm	-86 dBm			6.5	QoS Data	IntelCor_bb:27:54	3a:97:a4:4d…	169	Key (Message 4 of 4)
13	64.105119	802.11n (HT)	1		-81 dBm	-89 dBm			6.5	QoS Null function (N…	IntelCor_bb:27:54	3a:97:a4:4d…	62	QoS Null function (No data), SN=0, FN=0, Flags=.......T
14	64.105643	802.11ax (HE)	1	20	-82 dBm	-89 dBm	0x3	1 spa…	29.3	QoS Data	IntelCor_bb:27:54	IPv6mcast_16	170	QoS Data, SN=2, FN=0, Flags=.p.....T
15	64.106440	802.11ax (HE)	1	20	-72 dBm	-89 dBm	0x0	1 spa…	7.3	Data	IntelCor_bb:27:54	IPv6mcast_16	168	Data, SN=1, FN=0, Flags=.p....F.
16	64.134835	802.11ax (HE)	1	20	-83 dBm	-88 dBm	0x3	1 spa…	29.3	QoS Data	IntelCor_bb:27:54	Broadcast	422	QoS Data, SN=3, FN=0, Flags=.p.....T

- Statistics>Flow Graph to visualize ladder diag.
  AP: 3a:97:a4:4d:e3:0a
  STA:IntelCor_bb:27:54



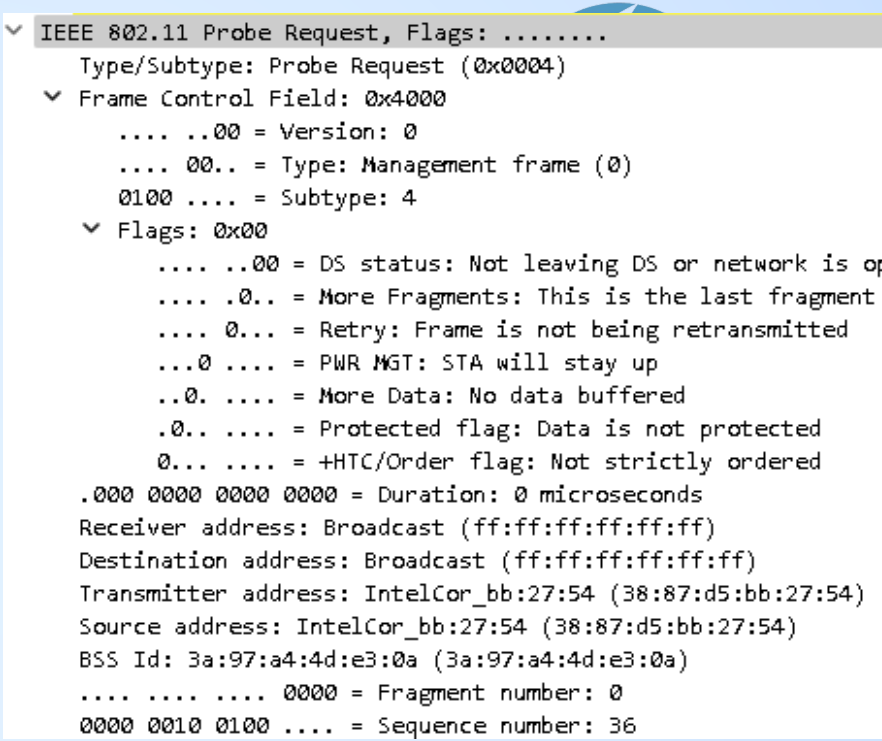
Radiotap, 802.11 radio info

- Select Frame #1
- Check the Channel number, frequency, MCS information in Radiotap header
- We can also find them in the 802.11 radio info header too
- The capture application makes this header, so some fields are different.



IEEE802.11 MAC header

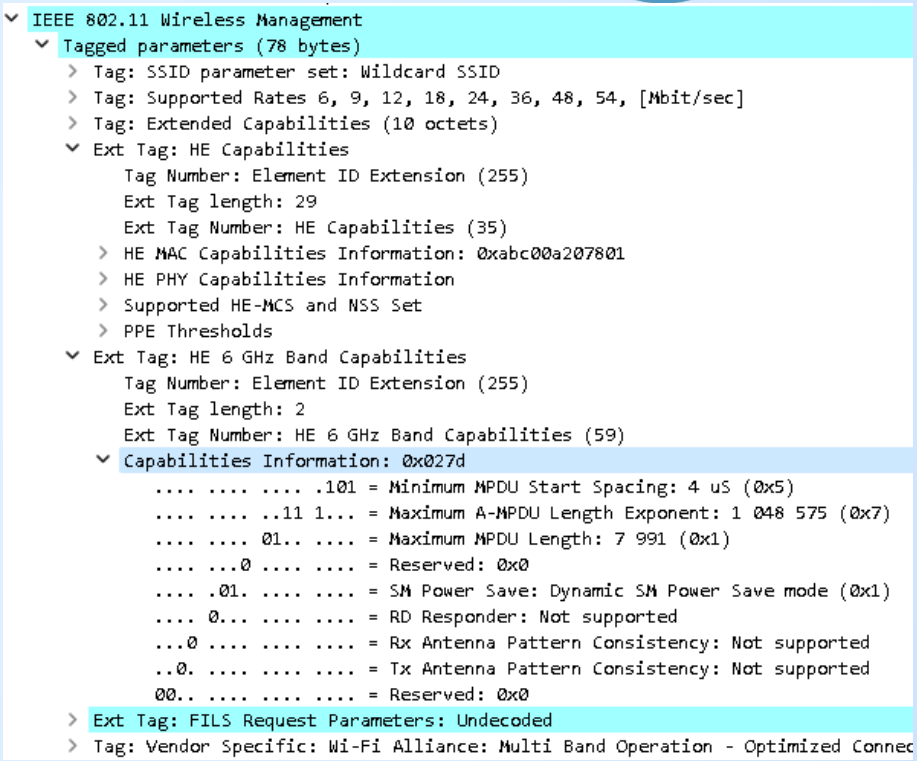
- The 802.11 MAC header has been the same since 1990's
- We can check Type/Subtype, Retry and Protected in Flags, Four addresses (wlan.sa, wlan.da and wlan.ta, wlan.ra for wireless media)
- I recommend remembering famous Type/Subtype.



Type	Wireshark filter Strings
Management frame 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 Responsewlan.fc.type_subtype==1
	Authentication wlan.fc.type_subtype==11
	Deauthentication wlan.fc.type_subtype==12
	Disassociation wlan.fc.type_subtype==10
	Action wlan.fc.type_subtype==13
Control frame 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
	BAR (Block ACK Request) wlan.fc.type_subtype==24
	BA(Block ACK) wlan.fc.type_subtype==25
Data frame wlan.fc.type==2	Data wlan.fc.type_type==2 Null Data wlan.fc.type_subtype==36 QoS Data wlan.fc.type_subtype==40

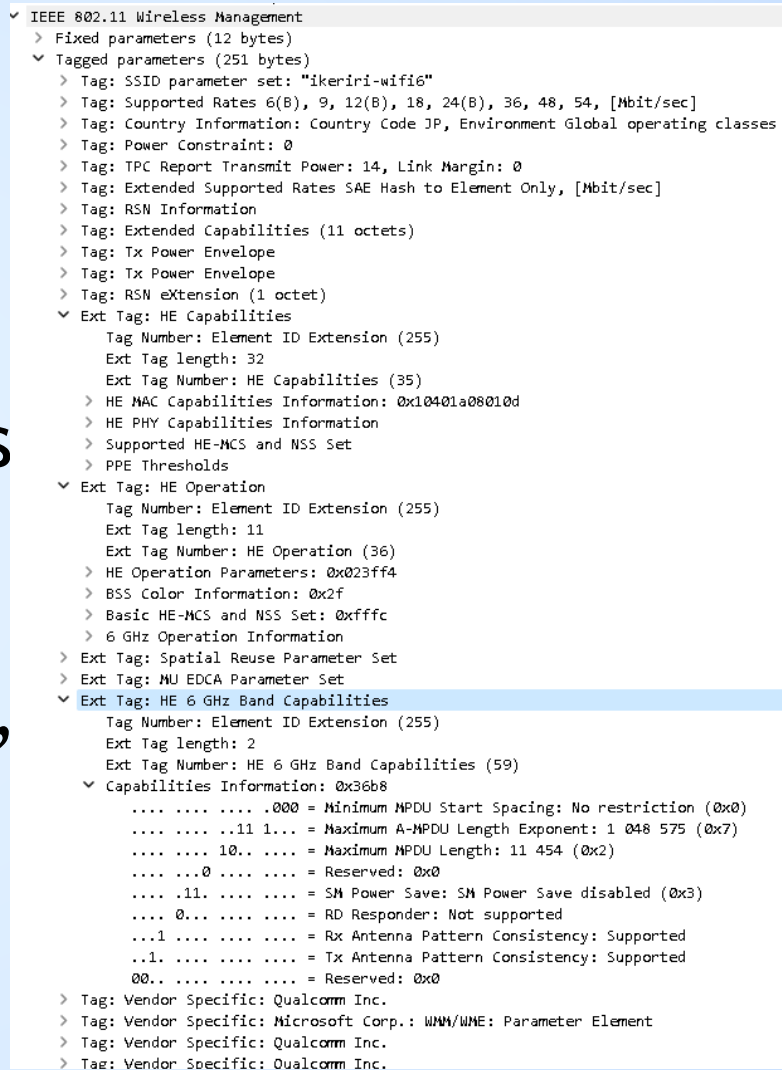
Frame #1: Probe Request

- Expand Wireless Management header
- First probe uses Wildcard SSID (all Access points)
- HE Capabilities and HE 6GHz Band Capabilities shows Client Specs of WiFi6E



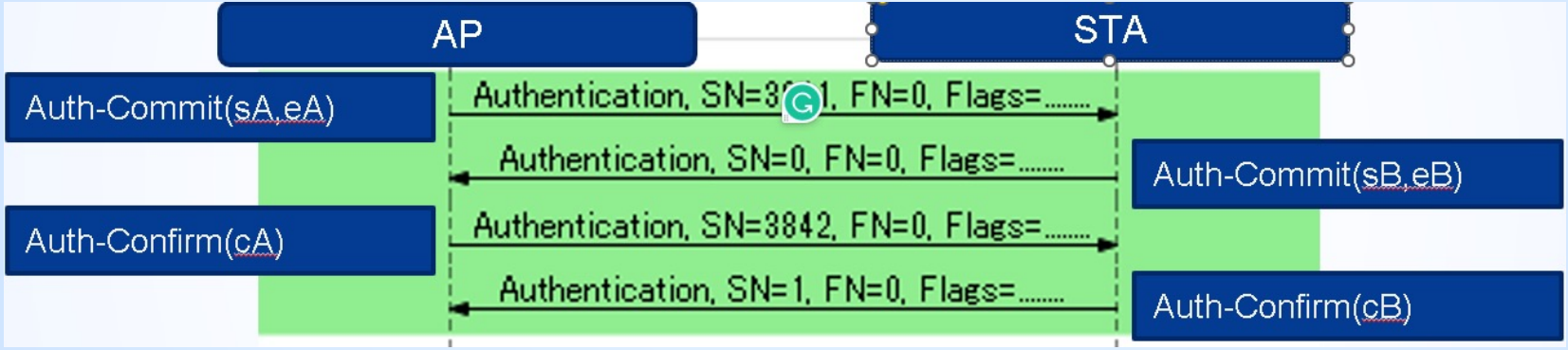
Frame #2: Probe Response

- AP broadcasts its WiFi6E spec.
- Open Wireless Management check HE Capabilities, including MAC/PHY Capabilities (Ch. Bandwidth, MCS etc.)
  HE Operations including BSS coloring, MCS, VHT usage, etc.,
  HE 6GHz Band Capabilities including A-MPDU information



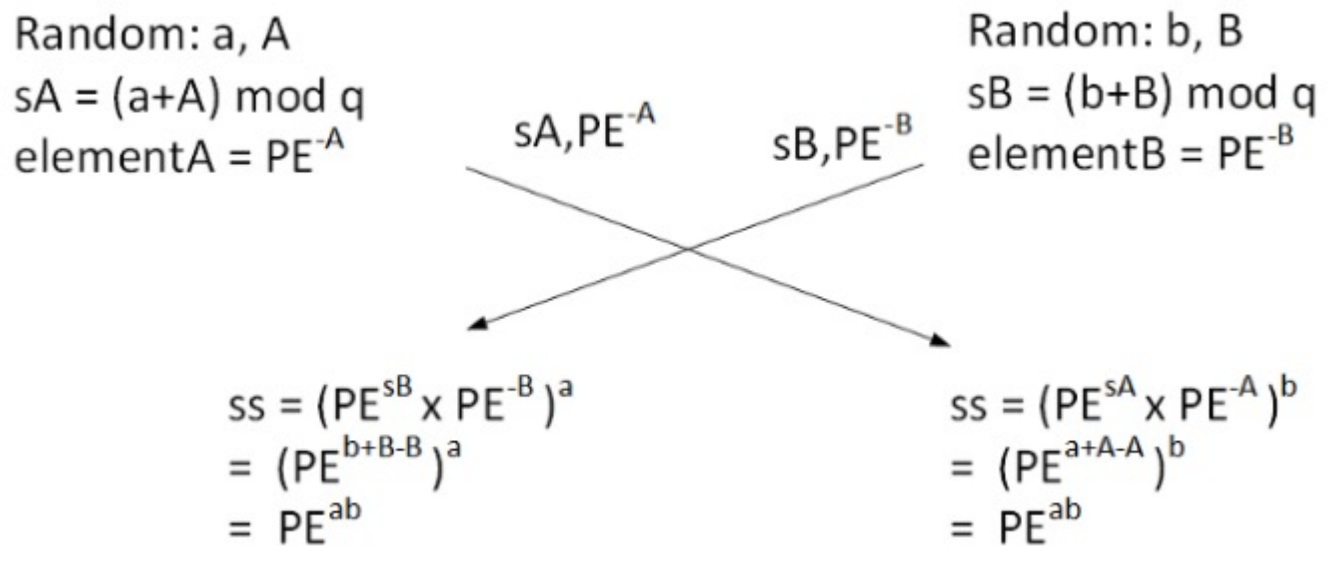
Frame #3 to 6: SAE handshake

- SAE（Simultaneous Authentication of Equals）is known for Dragonfly key exchange in RFC7664 https://www.rfc-editor.org/info/rfc7664
- I talked last year, so omit in detail



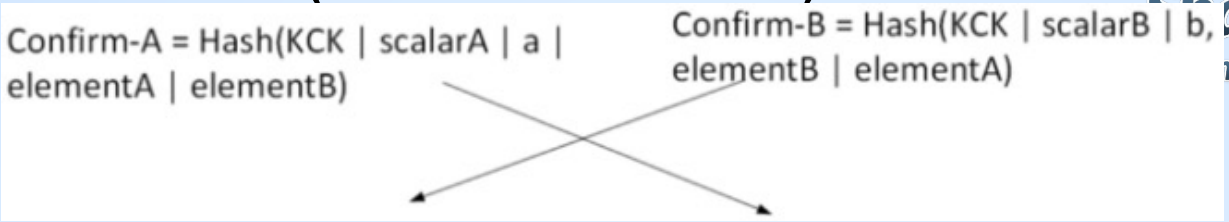
- Both AP and STA send Auth-Commit and Auth-Confirm to each other with scholar and element

Auth-Commit (Scalar, Finite Field Element)



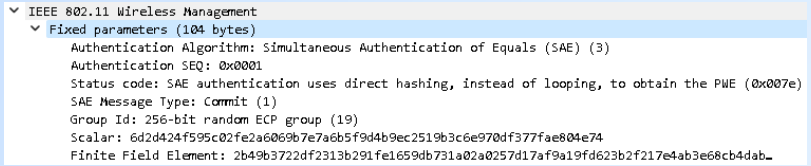
- AP and STA calculate their own and the other side Scalar and Finite field element to create and share PE(Password Equivalent) value using Elliptic Curve cryptography

Auth-Confirm (Confirm value)

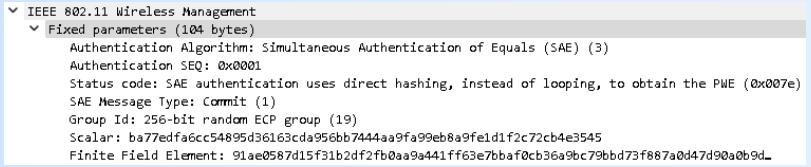


- Each Alice(STA) and Bob(AP) can verify the packet's Confirm value with the calculated Confirm value
- K=rB · (sA · P+eA)
  tr=(sB,eB,sA,eA)
  cB=HMAC(Hash(K),tr)
- K=rA · (sB · P+eB)
  tr=(sA,eA,sB,eB)
  cA=HMAC(Hash(K),tr)
- If the calculated Confirm value is the same as the packet, we can share PE(Password Equivalent) value without sending passphrase information to each other.

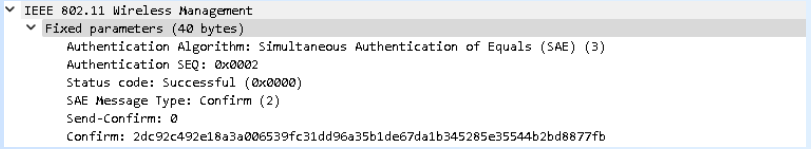
#3 SAE Commit from AP



#4 SAE Commit from STA



#5 SAE Confirm from AP

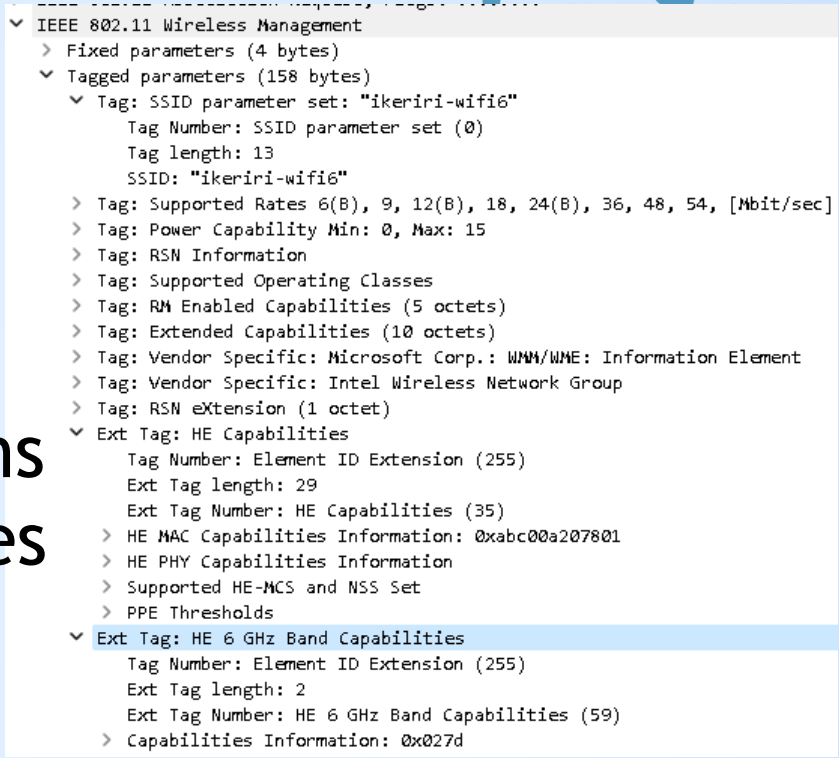


#6 SAE Confirm from STA

- SAE handshake has 2 Auth-Commit and 2 Auth-Confirm message
- Auth-Commit has Scalar(sA,sB) and Finite Field Element (eA,eB)
- Auth-Confirm has a Confirm value
- They create and share PMK during these four packets using dragonfly key exchange

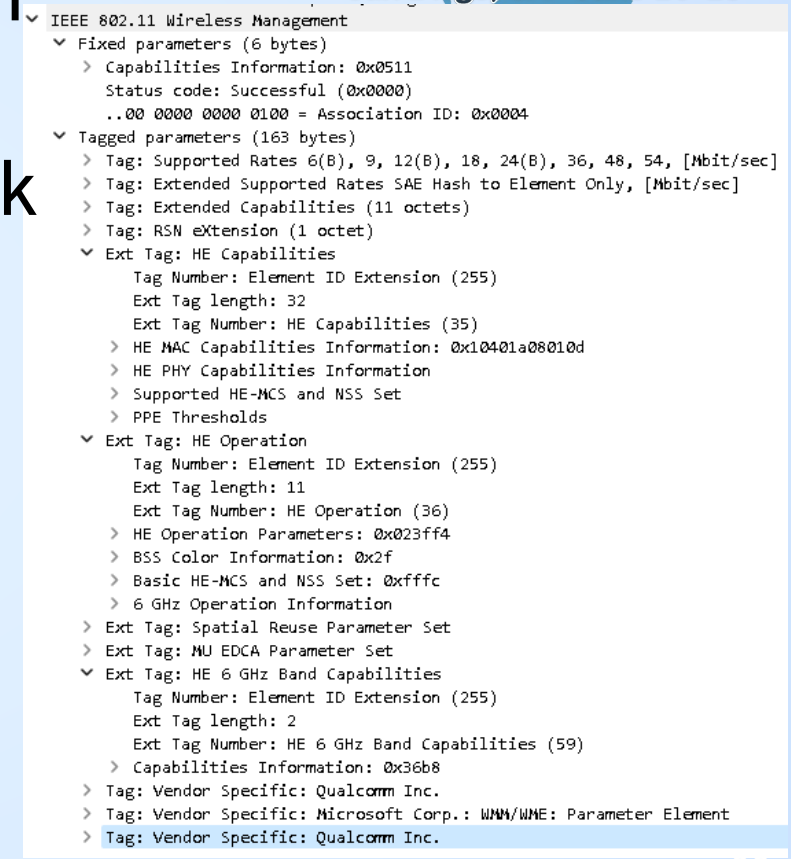
Frame #7: Association Req.

- STA sends WiFi6E connection specs to AP with many Tags
- Open Wireless Management we can find SSID parameter, HE Capabilities, HE Operations and HE 6GHz Band Capabilities Tags including WiFi6E specs



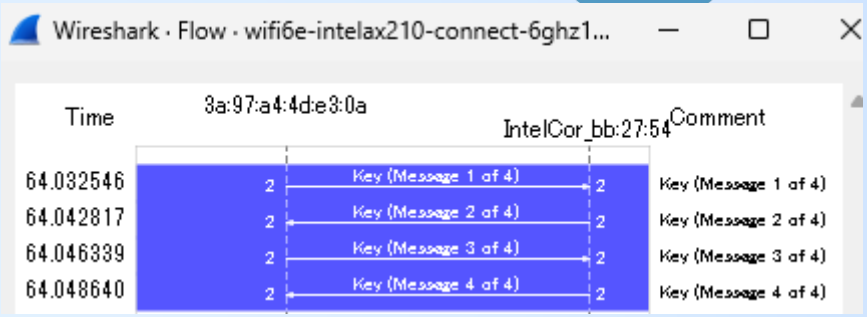
Frame #8: Association Res.

- AP sends Success of Association and logged Association ID
- AP and STA finish basic datalink
- Association Response contains HE Capabilities, HE Operation and HE 6GHz Band Capabilities including connection specs between AP and STA



Frame #9 to 12: EAPOL 4 way handshake

- I talked last year, so omit in details
- AP sends aNonce random and aMAC address in Mes1
- STA sends sNonce random and sMAC address in Mes2

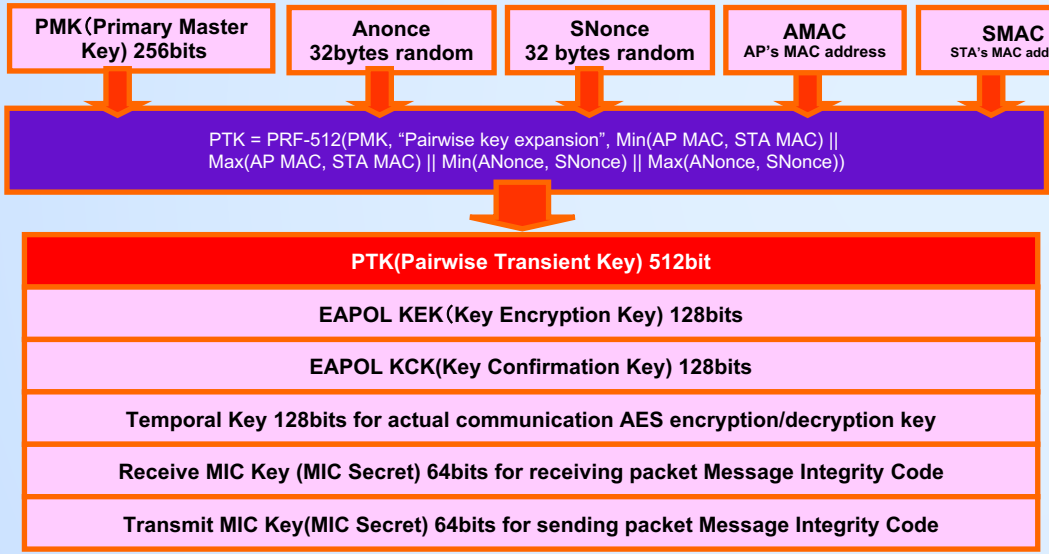


- PTK is created from ANonce, Snonce, AP MAC address and STA mac address

  PTK = PRF-512(PMK, “Pairwise key expansion”, Min(AP MAC, STA MAC) || Max(AP MAC, STA MAC) || Min(ANonce, SNonce) || Max(ANonce, SNonce))
- AP sends GTK, HMAC in Mes3
- STA sends HMAC in Mes4

Frame #9 to 12: EAPOL 4 way handshake

- All WPA1/2/3 use EAPOL 4-way handshake, WPA3 uses PMK derived from SAE Authentication.
- So PMK is different at every time. (PFS)



- PTK(Pairwise Transient Key) is also different
- TK(Temporal Key) is the Actual AES key
- PTK also contains KEK, KCK for key delivery, MIC key for hashing

Frame #9 to 12: EAPOL 4 way handshake

#9 Message 1 of 4 #10 Message 2 of 4 #11 Message 3 of 4

```
802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: Key (3)
    Length: 117
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 1]
  > Key Information: 0x0088
    Key Length: 16
    Replay Counter: 1
    WPA Key Nonce: 99106802fa9ab89f30e5013b6528dd10f9522b9b37981adad4f33ef20dd7a2e5
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 00000000000000000000000000000000
    WPA Key Data Length: 22
  > WPA Key Data: dd14000fac0427a5304ac6214b92fdc1cd8590fd716e
```

```
802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: Key (3)
    Length: 126
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 2]
  > Key Information: 0x0108
    Key Length: 0
    Replay Counter: 1
    WPA Key Nonce: 7443c2968be6a302500a49ed2d9cd6d974070399c3c91928efa07597bcd111d0
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 5ce0ee0ff1418f818a97f3ae5b90d81c
    WPA Key Data Length: 31
  > WPA Key Data: 301a0100000fac040100000fac040100000fac08fc000000000fac06f40120
```

```
802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: Key (3)
    Length: 183
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 3]
  > Key Information: 0x13c8
    Key Length: 16
    Replay Counter: 2
    WPA Key Nonce: 99106802fa9ab89f30e5013b6528dd10f9522b9b37981adad4f33ef20dd7a2e5
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 7a7faf8f6d6d12fa55e75f1e4db51d0a
    WPA Key Data Length: 88
    WPA Key Data: e7ea268f3f98a407952f7500f04c797f1bafaabf202c3ece8e508cfb08c06e90fcb2a52a…
```

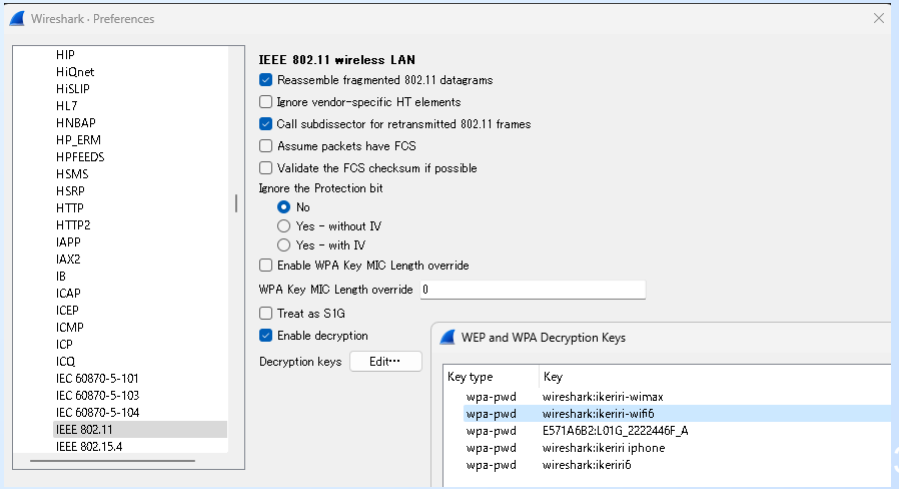
Anonce, AMAC Snonce, SMAC Gnonce, GTK, MIC

#12 Message of 4 contains MIC, confirmation for GTK delivery

Frame #13 to 16 Data frames

- Finally, we got the actual data frames including over layer3 information
- We cannot decrypt WPA3-SAE if we set the decryption key in IEEE802.11 preference (for now…)
- We can check CCMP parameters, including IV

```
IEEE 802.11 QoS Data, Flags: .p.....T
    Type/Subtype: QoS Data (0x0028)
  > Frame Control Field: 0x8841
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: 3a:97:a4:4d:e3:0a (3a:97:a4:4d:e3:0a)
    Transmitter address: IntelCor_bb:27:54 (38:87:d5:bb:27:54)
    Destination address: IPv6mcast_16 (33:33:00:00:00:16)
    Source address: IntelCor_bb:27:54 (38:87:d5:bb:27:54)
    BSS Id: 3a:97:a4:4d:e3:0a (3a:97:a4:4d:e3:0a)
    STA address: IntelCor_bb:27:54 (38:87:d5:bb:27:54)
    .... .... .... 0000 = Fragment number: 0
    0000 0000 0010 .... = Sequence number: 2
  v Qos Control: 0x0000
        .... .... .... 0000 = TID: 0
        [.... .... .... .000 = Priority: Best Effort (Best Effort) (0)]
        .... .... ...0 .... = QoS bit 4: Bits 8-15 of QoS Control field are TXOP Duration Requested
        .... .... .00. .... = Ack Policy: Normal Ack (0x0)
        .... .... 0... .... = Payload Type: MSDU
        0000 0000 .... .... = TXOP Duration Requested: 0 (no TXOP requested)
  v CCMP parameters
        CCMP Ext. Initialization Vector: 0x000000000001
        Key Index: 0
v Data (92 bytes)
    Data: 1a04856f33207b417fd35d14c5add7cb403885e50010261bdf6170fe33b0c0f489057f0c…
    [Length: 92]
```



I do not want to pay for commercial products!!

- Yes, it is the time for Linux, thank you for great Kismet creator, Mike-san (Mike Kershaw)
- Talking about WiFi6, some COMFAST USB3 adapters support IEEE802.11ax monitor mode.
  CF-957AX (upper) CF-953AX (bottom)
  they use mt7921au driver
  https://github.com/morrownr/USB-WiFi/issues/87
  We can get them via AliExpress etc.

- We need >5.18.3 kernel and some interesting techs
- This time I test with CF-953AX with Rasberian

“iw reg set US” to deceive we were in US

- This time we test Raspberry Pi4 with Raspberian OS
- type “uname –a” to check kernel ver >5.18.3
- Check lsusb / iwconfig for adapter recognition
- COMFAST adapters have no initial scan mechanism like Intel AX, they can be configured by commands type “iw reg set US” to deceive we were in the US.
- “iwconfig” to determine interface number (wlanX)
- “airmon-ng start wlanX”, change into monitor mode
- Use Wireshark, tshark, dumpcap, kismet, tcpdump

Live Demo: capturing WiFi6 using Rapsberry

```
root@raspberrypi:~# uname -a
Linux raspberrypi 6.1.31-v8+ #1654 SMP PREEMPT Tue May 30 17:18:56 BST 2023 a
h64 GNU/Linux
root@raspberrypi:~# lsusb
Bus 003 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 001 Device 004: ID 0e8d:7961 MediaTek Inc.
Bus 001 Device 002: ID 2109:3431 VIA Labs, Inc. Hub
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
root@raspberrypi:~# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

usb0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:"aterm-a5e9be-a"
          Mode:Managed  Frequency:2.437 GHz  Access Point: 28:CF:DA:AD:AD:49
          Bit Rate=24 Mb/s   Tx-Power=31 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on
          Link Quality=67/70  Signal level=-43 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:2  Invalid misc:0   Missed beacon:0

wlan1     IEEE 802.11  ESSID:"aterm-a5e9be-a"
          Mode:Managed  Frequency:5.54 GHz  Access Point: 28:CF:DA:AD:AD:4A
          Bit Rate=6 Mb/s   Tx-Power=3 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on
          Link Quality=70/70  Signal level=-39 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:1   Missed beacon:0
```

```
root@raspberrypi:~# iw reg set US
root@raspberrypi:~# iw reg get
global
country 98: DFS-UNSET
        (2402 - 2472 @ 40), (N/A, 20), (N/A)
        (5170 - 5250 @ 80), (N/A, 20), (N/A), AUTO-BW
        (5250 - 5330 @ 80), (N/A, 20), (0 ms), DFS, AUTO-BW
        (5490 - 5710 @ 160), (N/A, 23), (0 ms), DFS
        (57240 - 66000 @ 2160), (N/A, 10), (N/A)

phy#0
country 99: DFS-UNSET
        (2402 - 2482 @ 40), (6, 20), (N/A)
        (2474 - 2494 @ 20), (6, 20), (N/A)
        (5140 - 5360 @ 160), (6, 20), (N/A)
        (5460 - 5860 @ 160), (6, 20), (N/A)
```

- uname -a, lsusb, iwconfig
- iw reg set US, iw reg get we were in the US!!

Live Demo: capturing WiFi6 using Rapsberry


```
root@raspberrypi:~# airmon-ng check kill

Killing these processes:

  PID Name
  445 wpa_supplicant
  519 dhcpcd
  645 wpa_supplicant
 1029 wpa_supplicant
 1217 avahi-daemon

root@raspberrypi:~# airmon-ng start wlan1

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

  PID Name
 1225 avahi-daemon
 1226 avahi-daemon

PHY     Interface       Driver          Chipset

phy0    wlan0           brcmfmac        Broadcom 43430
phy1    wlan1           mt7921u         MediaTek Inc.

                (mac80211 monitor mode vif enabled for [phy1]wlan1 on [phy1]wlan
1mon)
                (mac80211 station mode vif disabled for [phy1]wlan1)
```

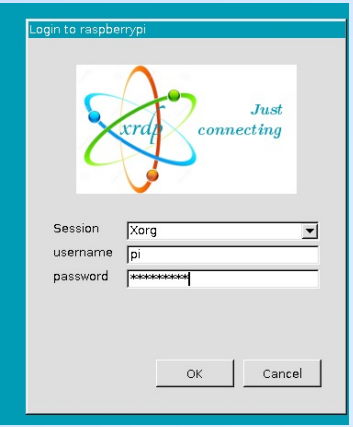
- airmon-ng check kill
  to kill the needless process

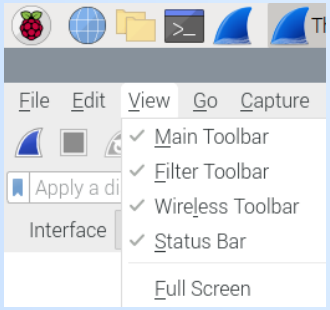
#sf23us

- airmon-ng start wlan1
  to change to monitor
- iwconfig to confirm

```
root@raspberrypi:~# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

usb0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=31 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on

wlan1mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=3 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
```

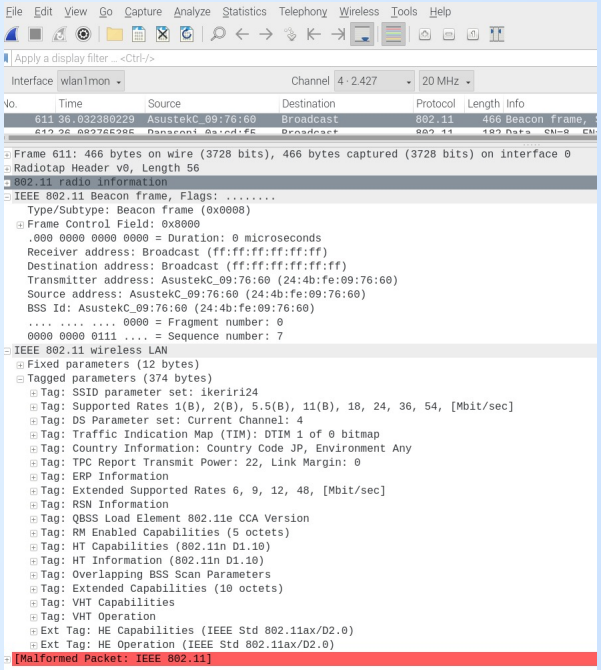
Live Demo: capturing WiFi6 using Rapsberry



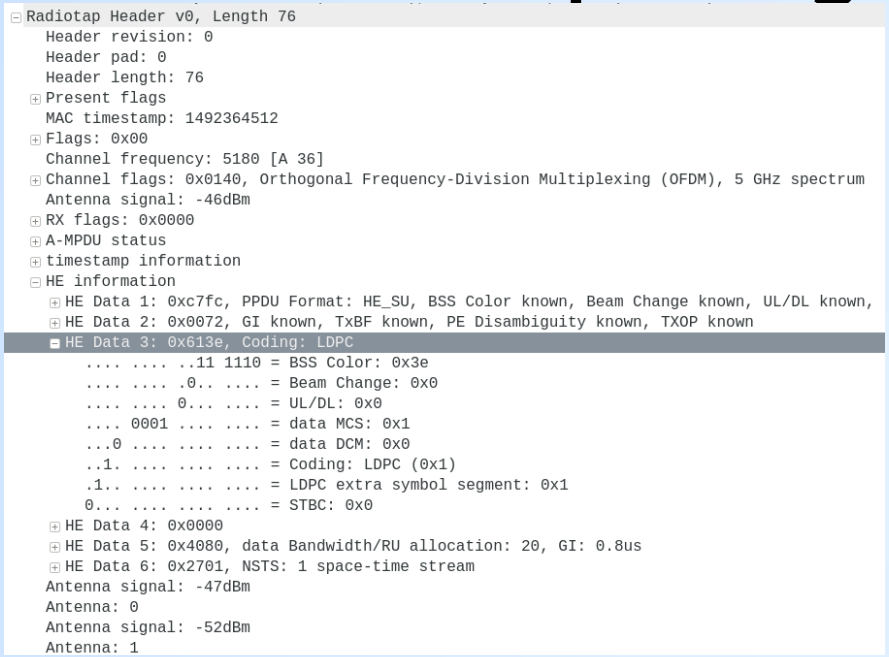


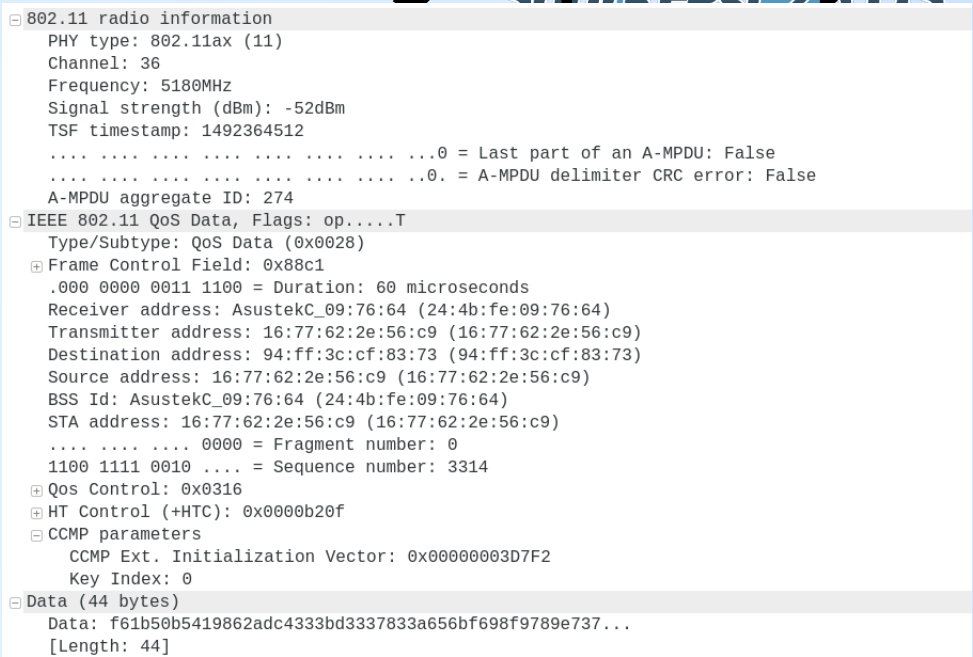
- Connect Raspberry Pi4 via XRDP
- Open Wireshark and View>Wireless Toolbar
- Capture wlan1mon
- We can find some beacons of WiFi6 AP including HE capabilities, HE Operation (SSID: ikeriri24, CH 4)

#sf23us



Live Demo: capturing WiFi6 using Rapsberry

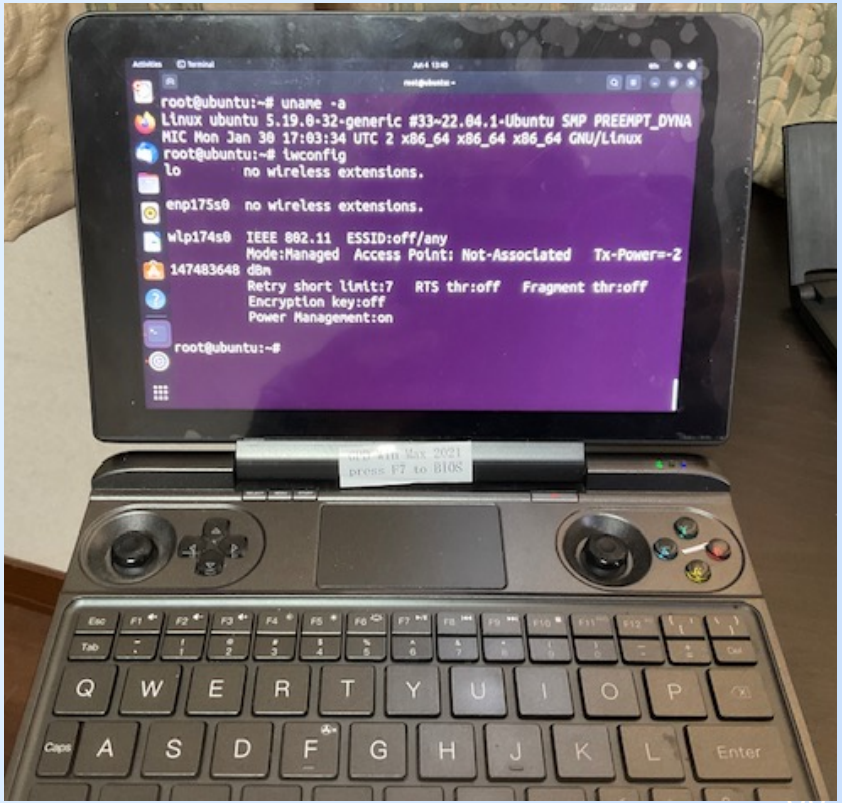




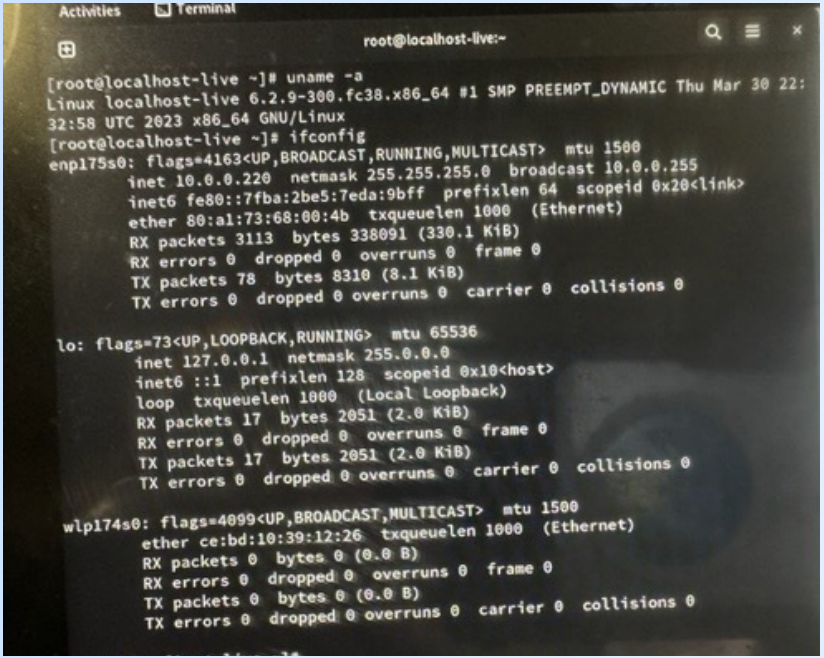
- Here is a sample trace by Comfast CF-953AX
- Channel:36 MCS:1 BW:20MHz Stream:1 in Radiotap
- PHY type: 802.11ax A-MPDU aggregate ID:274

Appendix: Intel AX210 on Linux

- Let's try WiFi6E on Linux with Intel AX210 via M.2 connection
- We test GPD Win Max 2021
- create a boot image from Fedora-Workstation-Live -x86_64-38-1.6.iso
- Any distribution over kernel >5.18.3 works well
- We also need aircrack-ng, Wireshark, and so on.



Appendix: check kernel version



uname –a

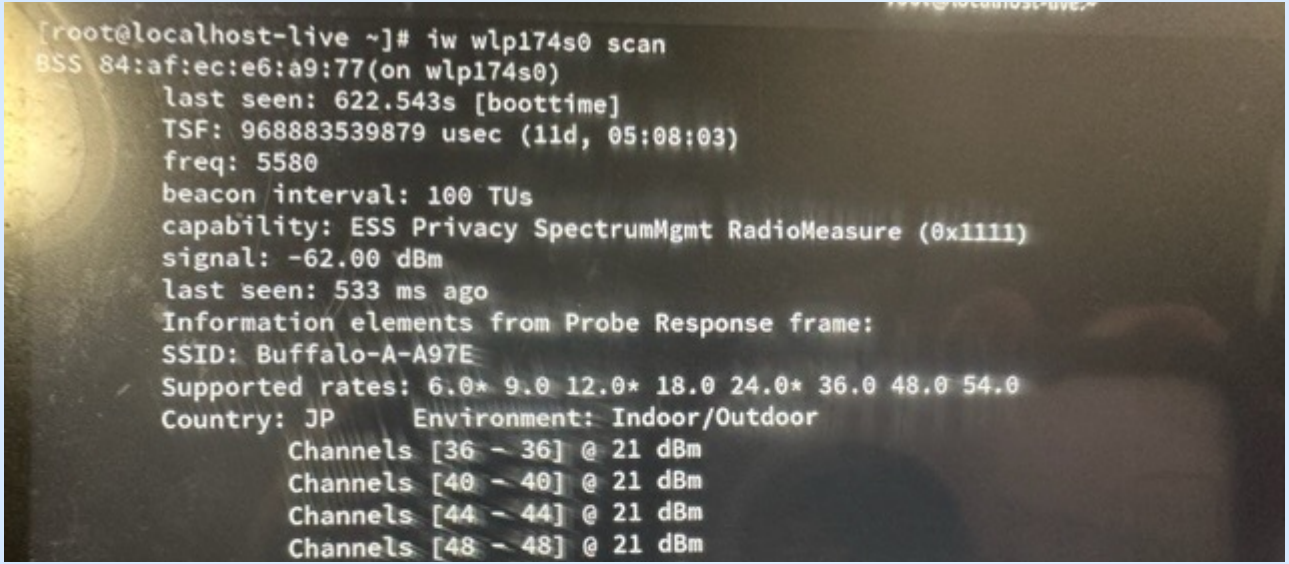
ifconfig (check wlp174s0)

dnf install aircrack-ng

dnf intall wireshark

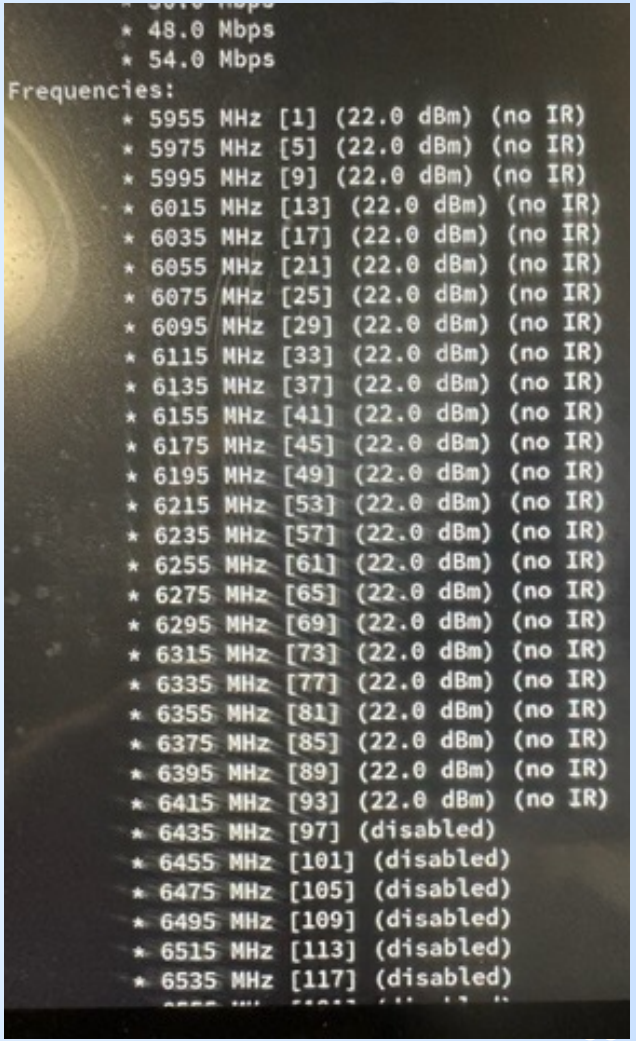
Appendix: Perorm initial scan

- We need to perform AX210 initial scan “iw wlp174s0 scan” to scan to determine the location



Appendix: check frequency

- “iw phy phy0 info”
  or “iwlist”
  check the frequency
  the channels from
  5955MHz[1] to
  6415MHz[93]
  are enabled

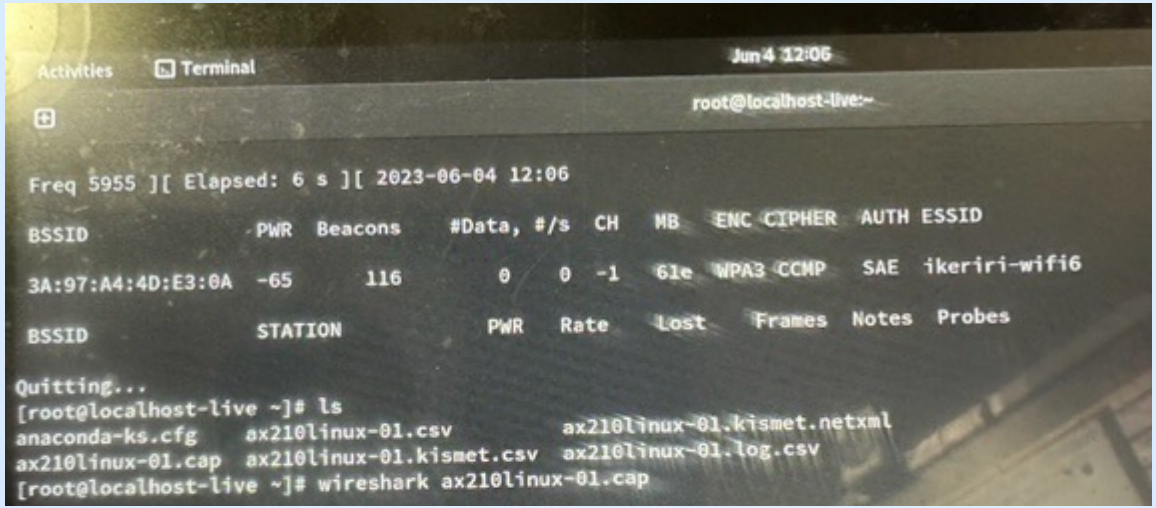


Appendix: change into monitor mode

- Then use airmon-ng to change into monitor mode
  airmon-ng check kill
  airmon-ng start wlp174s0
  ifconfig to find wlp174s0mon

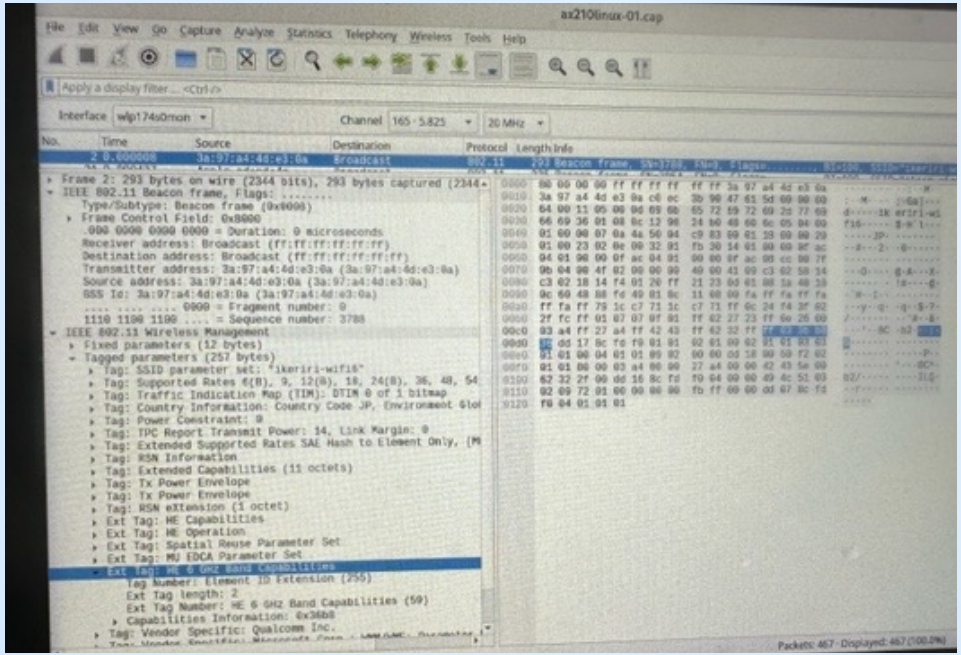
Appendix: use airodump-ng to capture 6E

- airodump-ng wlp174s0mon –C 5955
  to scan beacon frames of “ikeriri-wifi6”



Appendix: use Wireshark to capture 6E

- airodump-ng wlp174s0mon –C 5955 -w ax210linux to create ax210linux.cap
- wireshark ax210linux-01.cap



USE WIRESHARK

SharkFest'23 US
San Diego, CA • June 10-15

#sf23us

Thank you for watching.

Please complete the Google form survey

trace files and Wireshark profiles are here:
https://www.ikeriri.ne.jp/sharkfest/
CapturingWiFi6EwithWireshark.zip

ikeriri network service
http://www.ikeriri.ne.jp