

## WPA2 Handshake Capture and Analysis

```
File Actions Edit View Help
zsh: corrupt history file /root/.zsh_history
(root@kali)~# airmon-ng
PHY Interface Driver Chipset
phy1 wlan0 88XXau Realtek Semiconductor Corp. Realtek 8812AU/8821AU 802.11ac WLAN Adapter [USB Wireless Dual-Band Adapter 2.4/5Ghz]

(root@kali)~# sudo airmon-ng start wlan0
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
515 NetworkManager
640 wpa_supplicant

PHY Interface Driver Chipset
phy1 wlan0 88XXau Realtek Semiconductor Corp. Realtek 8812AU/8821AU 802.11ac WLAN Adapter [USB Wireless Dual-Band Adapter 2.4/5Ghz]
(monitor mode enabled)
```

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
00:25:00:FF:94:73	CE:5A:6D:6B:51:C3	-83	0 -12	0	1		
00:25:00:FF:94:73	B2:E5:62:80:E1:D7	-69	0 -12	0	1		
14:AB:F0:BE:36:15	04:03:D6:79:3D:DB	-1	24e- 0	0	3		
CH 7 ][ Elapsed: 15 mins ][ 2024-10-14 02:03 ][ WPA handshake: 58:9B:4A:8F:97:71							
CH 13 ][ Elapsed: 21 mins ][ 2024-10-14 02:09 ][ interface wlan0 down							
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH ESSID
F8:5B:3B:5C:3A:31	-87	20	0 0	11	720	WPA2 CCMP	PSK MEEapt3
B0:5A:DA:F8:95:9F	-73	0	0 0	11	65	WPA2 CCMP	PSK DIRECT-9E-HP ENVY 4520 series
F0:09:0D:C7:D5:B4	-63	6	6 0	2	360	WPA2 CCMP	PSK CVN
74:37:5F:90:28:CB	-78	24	0 0	11	720	WPA2 CCMP	PSK Shef Kitchen
74:93:DA:3F:E3:8D	-48	31	4 0	1	720	WPA2 CCMP	PSK MorenoJ

### Acknowledgment (ACK) Frame:

- What It Is: The ACK frame is a type of control frame sent by the receiver to the sender to confirm successful reception of a data frame.
- Purpose: It ensures reliable communication between wireless devices. If a data frame is sent from one device to another (e.g., from a client to an access point), the receiving device must send an ACK frame to let the sender know that the frame was received correctly. If the sender doesn't receive an ACK within a certain time frame, it will assume the transmission failed and will resend the frame.
- In Wi-Fi Handshake: While ACKs aren't directly part of the WPA2 4-way handshake, every data transmission, including the handshake packets (such as EAPOL messages), will involve ACK frames to confirm successful delivery.

Apply a display filter ... <Ctrl-F>					
No.	Time	Source	Destination	Protocol	Length Info
235	13.216410		MurataManufa_c8:73:fd	802.11	10 Acknowledgement, Flags=.....
236	13.274066	AskeyCompute_a4:65:da	AmazonTechno_46:5f:5c	802.11	28 802.11 Block Ack, Flags=.....
237	13.338486		ae:8a:bc:d7:ee:fc	802.11	10 Acknowledgement, Flags=.....
238	13.381820		ae:8a:bc:d7:ee:fc	802.11	10 Acknowledgement, Flags=.....
239	13.381825	SagemcomBroa_df:44:06	ae:8a:bc:d7:ee:fc	802.11	21 VHT/HE/EHT/RANGING NDP Announcement, Sounding Dialog Token=138, Flags=..
240	13.390955		Broadcom_10:be:be	802.11	10 Clear-to-send, Flags=.....
241	13.390958	AskeyCompute_a4:65:da	AmazonTechno_46:5f:5c	802.11	28 802.11 Block Ack, Flags=.....
242	13.496430		Broadcom_10:be:be	802.11	10 Clear-to-send, Flags=.....
243	13.496440		4a:b1:bb:64:d1:a1	802.11	10 Acknowledgement, Flags=.....
244	13.606769		Ring_10:2a:93	802.11	10 Acknowledgement, Flags=.....
245	13.607926		SagemcomBroa_75:c5:1c	802.11	10 Acknowledgement, Flags=.....
246	13.610624		SagemcomBroa_75:c5:1c	802.11	10 Acknowledgement, Flags=.....
247	13.610629		Broadcom_10:c5:1c	802.11	10 Clear-to-send, Flags=.....
248	13.616592		Ring_10:2a:93	802.11	10 Acknowledgement, Flags=.....
249	13.711011	f2:72:ea:2e:ae:2c	ce:f4:11:26:ef:fd	802.11	28 802.11 Block Ack, Flags=.....
250	13.714033	Google_2e:ae:2d	Apple_7e:69:57	802.11	16 Request-to-send, Flags=.....
251	13.721640		Apple_45:30:d7	802.11	10 Clear-to-send, Flags=.....
252	13.721643	SagemcomBroa_57:d7:7d	Apple_45:30:d7	802.11	28 802.11 Block Ack, Flags=.....
▼ Frame 243: 10 bytes on wire (80 bits), 10 bytes captured (80 bits)					
Encapsulation type: IEEE 802.11 Wireless LAN (20)					
Arrival Time: Oct 15, 2024 02:42:06.476650000 EDT					
UTC Arrival Time: Oct 15, 2024 06:42:06.476650000 UTC					
Epoch Arrival Time: 1728974526.476650000					
[Time shift for this packet: 0.000000000 seconds]					
[Time delta from previous captured frame: 0.000010000 seconds]					
[Time delta from previous displayed frame: 0.000010000 seconds]					
[Time since reference or first frame: 13.496440000 seconds]					
Frame Number: 243					
Frame Length: 10 bytes (80 bits)					
Capture Length: 10 bytes (80 bits)					
[Frame is marked: False]					
[Frame is ignored: False]					
[Protocols in frame: wlan]					
IEEE 802.11 Acknowledgement, Flags: .....					
				0000 d4 00 01 00 4a b1 bb 64 d1 a1	....J..d..

## 2. Request to Send (RTS) Frame:

- What It Is: RTS is another type of control frame used to clear the channel before sending large data frames.
- Purpose: RTS is used to avoid collisions in a Wi-Fi network, especially in environments where multiple clients might be trying to communicate with the same access point (AP) at the same time.
  - Before sending a large packet of data, the sender will send an RTS frame to the AP, asking for permission to transmit.
  - The RTS frame contains the duration for which the sender wants to use the wireless channel.
- In Wi-Fi Handshake: RTS is part of the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism in Wi-Fi but is not directly related to the WPA2 handshake. However, before the handshake or any other communication can begin, the client may send an RTS frame to request permission to use the channel.

No.	Time	Source	Destination	Protocol	Length	Info
268	14.583292		Broadcom_10:c5:1c	802.11	16	Clear-to-send, Flags=.....
269	15.057308	BilianElectr_4d:f7:36	SagemcomBroa_75:c5:1c	802.11	16	Request-to-send, Flags=.....
270	15.057312		BilianElectr_4d:f7:36	802.11	16	Clear-to-send, Flags=.....
271	15.057315		BilianElectr_4d:f7:36	802.11	16	Acknowledgement, Flags=.....
272	15.057317	SagemcomBroa_75:c5:1c	BilianElectr_4d:f7:36	802.11	16	Request-to-send, Flags=.....
273	15.057318		SagemcomBroa_75:c5:1c	802.11	16	Clear-to-send, Flags=.....
274	15.057319	BilianElectr_4d:f7:36	SagemcomBroa_75:c5:1c	802.11	28	802.11 Block Ack, Flags=.....
275	15.057321		Broadcom_10:c5:1c	802.11	16	Clear-to-send, Flags=.....
276	15.201958		AmazonTechno_68:a0:00	802.11	16	Acknowledgement, Flags=.....
277	15.215663		AmazonTechno_68:a0:00	802.11	16	Acknowledgement, Flags=.....
278	15.233306		AmazonTechno_68:a0:00	802.11	16	Acknowledgement, Flags=.....
279	15.233309		AmazonTechno_68:a0:00	802.11	16	Acknowledgement, Flags=.....
280	15.593419		AmazonTechno_68:a0:00	802.11	16	Acknowledgement, Flags=.....
281	15.623541		AmazonTechno_68:a0:00	802.11	16	Acknowledgement, Flags=.....
282	15.640002		AmazonTechno_68:a0:00	802.11	16	Acknowledgement, Flags=.....
283	15.655057		AmazonTechno_68:a0:00	802.11	16	Acknowledgement, Flags=.....
284	15.671281		AmazonTechno_68:a0:00	802.11	16	Acknowledgement, Flags=.....
285	15.702252		AmazonTechno_68:a0:00	802.11	16	Acknowledgement, Flags=.....

  

▼ Frame 272: 16 bytes on wire (128 bits), 16 bytes captured (128 bits)	0000	b4 00 be 00 c4 3c b0 4d f7 36 4c 19 5d 75 c5 1c
Encapsulation type: IEEE 802.11 Wireless LAN (20)		
Arrival Time: Oct 15, 2024 02:42:08.037527000 EDT		
UTC Arrival Time: Oct 15, 2024 06:42:08.037527000 UTC		
Epoch Arrival Time: 1728974528.037527000		
[Time shift for this packet: 0.000000000 seconds]		
[Time delta from previous captured frame: 0.000002000 seconds]		
[Time delta from previous displayed frame: 0.000002000 seconds]		
[Time since reference or first frame: 15.057317000 seconds]		
Frame Number: 272		
Frame Length: 16 bytes (128 bits)		
Capture Length: 16 bytes (128 bits)		
[Frame is marked: False]		
[Frame is ignored: False]		
[Protocols in frame: wlan]		
▼ IEEE 802.11 Request-to-send, Flags: .....		
Type/Subtype: Request-to-send (0x001b)		
Frame Control Field: 0xb400		
0000 0000 1011 1110 = Duration: 190 microseconds		
▼ Receiver address: BilianElectr_4d:f7:36 (c4:3c:b0:4d:f7:36)		
.....0..... = LG bit: Globally unique address (factory default)		
.....0..... = LG bit: Individually addressable (unicast)		

### 3. Clear to Send (CTS) Frame:

- What It Is: CTS is the response to an RTS frame, sent by the receiver (typically the AP) to the sender to grant permission to send data.
- Purpose: After receiving an RTS frame, the AP checks whether the channel is free, and if it is, it responds with a CTS frame. This frame grants the sender permission to send data without worrying about interference from other devices during that time window.
  - The CTS frame also contains a duration value that tells other devices in the network to remain silent for a specific period, allowing the sender to transmit its data without interference.
- In Wi-Fi Handshake: Similar to RTS, CTS is not directly part of the WPA2 4-way handshake, but it plays a role in controlling access to the wireless medium before the handshake or other communications take place.

No.	Time	Source	Destination	Protocol	Length	Info
268	14.583292		Broadcom_10:c5:1c	802.11	10	Clear-to-send, Flags=.....
269	15.057308	BilianElectr_4d:f7:36	SagemcomBroa_75:c5:1c	802.11	16	Request-to-send, Flags=.....
270	15.057312	BilianElectr_4d:f7:36	BilianElectr_4d:f7:36	802.11	10	Clear-to-send, Flags=.....
271	15.057315		BilianElectr_4d:f7:36	802.11	10	Acknowledgement, Flags=.....
272	15.057317	SagemcomBroa_75:c5:1c	BilianElectr_4d:f7:36	802.11	16	Request-to-send, Flags=.....
273	15.057318		SagemcomBroa_75:c5:1c	802.11	10	Clear-to-send, Flags=.....
274	15.057319	BilianElectr_4d:f7:36	SagemcomBroa_75:c5:1c	802.11	28	802.11 Block Ack, Flags=.....
275	15.057321		Broadcom_10:c5:1c	802.11	10	Clear-to-send, Flags=.....
276	15.201958		AmazonTechno_68:a0:00	802.11	10	Acknowledgement, Flags=.....
277	15.215663		AmazonTechno_68:a0:00	802.11	10	Acknowledgement, Flags=.....
278	15.233306		AmazonTechno_68:a0:00	802.11	10	Acknowledgement, Flags=.....
279	15.233309		AmazonTechno_68:a0:00	802.11	10	Acknowledgement, Flags=.....
280	15.593419		AmazonTechno_68:a0:00	802.11	10	Acknowledgement, Flags=.....
281	15.623541		AmazonTechno_68:a0:00	802.11	10	Acknowledgement, Flags=.....
282	15.640002		AmazonTechno_68:a0:00	802.11	10	Acknowledgement, Flags=.....
283	15.655057		AmazonTechno_68:a0:00	802.11	10	Acknowledgement, Flags=.....
284	15.671281		AmazonTechno_68:a0:00	802.11	10	Acknowledgement, Flags=.....
285	15.702252		AmazonTechno_68:a0:00	802.11	10	Acknowledgement, Flags=.....

  

Frame 270: 10 bytes on wire (80 bits), 10 bytes captured (80 bits)		0000	c4 00 94 04	c4 3c b0 4d	f7 36
Encapsulation type: IEEE 802.11 Wireless LAN (20)					
Arrival Time: Oct 15, 2024 02:42:08.037522000 EDT					
UTC Arrival Time: Oct 15, 2024 06:42:08.037522000 UTC					
Epoch Arrival Time: 1728974528.037522000					
[Time shift for this packet: 0.000000000 seconds]					
[Time delta from previous captured frame: 0.000004000 seconds]					
[Time delta from previous displayed frame: 0.000004000 seconds]					
[Time since reference or first frame: 15.057312000 seconds]					
Frame Number: 270					
Frame Length: 10 bytes (80 bits)					
Capture Length: 10 bytes (80 bits)					
[Frame is marked: False]					
[Frame is ignored: False]					
[Protocols in frame: wlan]					
IEEE 802.11 Clear-to-send, Flags: .....					
Type/Subtype: Clear-to-send (0x001c)					
Frame Control Field: 0xc400					
0000 0100 1001 0100 = Duration: 1172 microseconds					
Receiver address: BilianElectr_4d:f7:36 (c4:3c:b0:4d:f7:36)					
.....0. .... = LG bit: Globally unique address (factory default)					
.....0. .... = TC bit: Individual address (unicast)					

## How These Frames Relate to the WPA2 Handshake:

- RTS/CTS and ACK frames are part of the medium access control (MAC) layer operations in the 802.11 protocol, and they manage how devices on a Wi-Fi network share the wireless medium and avoid collisions. These frames help ensure that the EAPOL (Extensible Authentication Protocol over LAN) packets used in the WPA2 4-way handshake are delivered reliably.
- The actual WPA2 handshake involves EAPOL packets, which are sent over the wireless medium, but before any transmission occurs, the medium must be clear. RTS/CTS can be used to avoid collisions when multiple clients are attempting to communicate with the same AP.
- After the handshake packets (or any other data packets) are sent, ACK frames confirm their successful reception.

## Trigger-based Beamforming in Wi-Fi 6:

In Wi-Fi 6, **trigger-based beamforming** is a technique where the **access point (AP)** triggers the **client devices** to respond in a certain manner to enable beamforming, which is optimized for multi-user communication. This is crucial for efficient network management, especially in dense environments like offices or public hotspots. Wi-Fi 6 networks are designed to handle a much higher number of connected devices compared to previous generations. The combination of OFDMA and MU-MIMO, along with trigger-based beamforming, allows Wi-Fi 6 to:

- **Improve network efficiency** by serving multiple devices at once.
- **Reduce latency** by handling high traffic more efficiently.
- **Enhance coverage and reliability** through better signal direction and reduced interference.

Apply a display filter ... <Ctrl>					
No.	Time	Source	Destination	Protocol	Length Info
328	16.734383	SagemcomBroa_df:44:07	Intel_0f:6b:f2	802.11	16 Request-to-send, Flags=.....
329	16.734385	SagemcomBroa_df:44:07	SagemcomBroa_df:44:07	802.11	10 Clear-to-send, Flags=.....
330	16.734387	SagemcomBroa_df:44:07	Broadcom_10:44:07	802.11	10 Clear-to-send, Flags=.....
331	16.734390	Netgear_b9:6a:62	AmazonTechno_0c:8b:2e	802.11	20 802.11 Block Ack Req, Flags=.....
332	16.734391	AmazonTechno_0c:8b:2e	Netgear_b9:6a:62	802.11	20 802.11 Block Ack, Flags=.....
333	16.901979	Intel_e0:e7:4b	SagemcomBroa_df:44:07	802.11	16 Request-to-send, Flags=.....
334	16.903636	Intel_e0:e7:4b	Intel_e0:e7:4b	802.11	10 Clear-to-send, Flags=.....
335	16.903641	Intel_e0:e7:4b	Intel_e0:e7:4b	802.11	10 Acknowledgement, Flags=.....
336	16.920915	SagemcomBroa_df:44:07	Intel_e0:e7:4b	802.11	16 Request-to-send, Flags=.....
337	16.920920	SagemcomBroa_df:44:07	SagemcomBroa_df:44:07	802.11	10 Clear-to-send, Flags=.....
338	16.943269	SagemcomBroa_df:44:07	Broadcast	802.11	25 VHT/HE/EHT/RANGING NDP Announcement, Sounding Dialog Token=138, Flags=.....
339	16.943275	SagemcomBroa_df:44:07	Broadcast	802.11	84 Trigger HE Beamforming Report Poll (BRP)[Malformed Packet]
340	17.035315	AskeyCompute_3f:e3:8e	HonHaiPrecis_b7:f3:8b	802.11	19 VHT/HE/EHT/RANGING NDP Announcement, Sounding Dialog Token=60, Flags=.....
341	17.038090	AskeyCompute_3f:e3:8e	30:95:2d:b3:20:d0	802.11	21 VHT/HE/EHT/RANGING NDP Announcement, Sounding Dialog Token=66, Flags=.....
342	17.048026	SagemcomBroa_df:44:07	Broadcast	802.11	25 VHT/HE/EHT/RANGING NDP Announcement, Sounding Dialog Token=142, Flags=.....
343	17.048034	SagemcomBroa_df:44:07	Broadcast	802.11	84 Trigger HE Beamforming Report Poll (BRP)[Malformed Packet]
344	17.089396	aa:7d:24:a3:34:f8	aa:7d:24:a3:34:f8	802.11	10 Acknowledgement, Flags=.....
345	17.329287	Ring_3e:4f:f4	AskeyCompute_ba:f9:5f	802.11	28 802.11 Block Ack, Flags=.....
▼ Frame 338: 25 bytes on wire (200 bits), 25 bytes captured (200 bits) on 0					
Ethernet II, Type: IEEE 802.11 VHT/HE/EHT/CS, LAN (20)					
Arrival Time: Oct 15, 2024 02:42:09.923479000 EDT					
UTC Arrival Time: Oct 15, 2024 06:42:09.923479000 UTC					
Epoch Arrival Time: 1728974529.923479000					
[Time shift for this packet: 0.000000000 seconds]					
[Time delta from previous captured frame: 0.022349000 seconds]					
[Time delta from previous displayed frame: 0.022349000 seconds]					
[Time since reference or first frame: 16.943269000 seconds]					
Frame Number: 338					
Frame Length: 25 bytes (200 bits)					
Capture Length: 25 bytes (200 bits)					
[Frame is marked: False]					
[Frame is ignored: False]					
[Protocols in frame: wlan]					
▼ IEEE 802.11 VHT/HE/EHT/RANGING NDP Announcement, Flags: .....					
Type/Subtype: VHT/HE/EHT/RANGING NDP Announcement (0x0015)					
Frame Control Field: 0x5400					
.000 0000 0110 0100 = Duration: 100 microseconds					
▼ Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)					
.....1..... = LG bit: Locally administered address (this .....					
..... = 10 bits: Group address (multicast/broadcast)					
Encapsulation type (frame.encap_type)					
Packets: 73407					