

[illegible]

Name	802.11ac Packet Analysis II
URL	https://www.attackdefense.com/challengedetails?cid=1140
Type	WiFi Pentesting: Traffic Analysis

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Q1. How many client devices were connected to BSSID e4:95:6e:45:9c:97 at MAC timestamp 1167524353?

Answer: 1

Solution:

Apply the following filter for given BSSID and MAC timestamp.

Filter: ((wlan.bssid == e4:95:6e:45:9c:97)) && (radiotap.mactime == 1167524353)

wifi-capture_1.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Filter: ((wlan.bssid == e4:95:6e:45:9c:97)) && (radiotap.mactime == 1167524353)

No.	Time	Source	Destination	Protocol	Length	Info
379	6.854489	Guanglia_05:9c:97	Broadcast	802.11	264	Beacon frame, SN=1826, FN=0, Flags=....., BI=100, SSID=CourageTheCowardlyDog

> Frame 379: 264 bytes on wire (2112 bits), 264 bytes captured (2112 bits)

> Radiotap Header v0, Length 48

> 802.11 radio information

> IEEE 802.11 Beacon frame, Flags:

▼ IEEE 802.11 wireless LAN

> Fixed parameters (12 bytes)

▼ Tagged parameters (180 bytes)

> Tag: SSID parameter set: CourageTheCowardlyDog

> Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]

> Tag: DS Parameter set: Current Channel: 36

> Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap

> Tag: Country Information: Country Code US, Environment Any

▼ Tag: QBSS Load Element 802.11e CCA Version

Tag Number: QBSS Load Element (11)

Tag length: 5

QBSS Version: 2

Station Count: 1

Channel Utilization: 81 (31%)

Available Admission Capacity: 0 (0 us/s)

Check QBSS Load Element Information Element (IE) to find the current station count which in this case is 1. So, only one client was connected to that BSSID at that point.

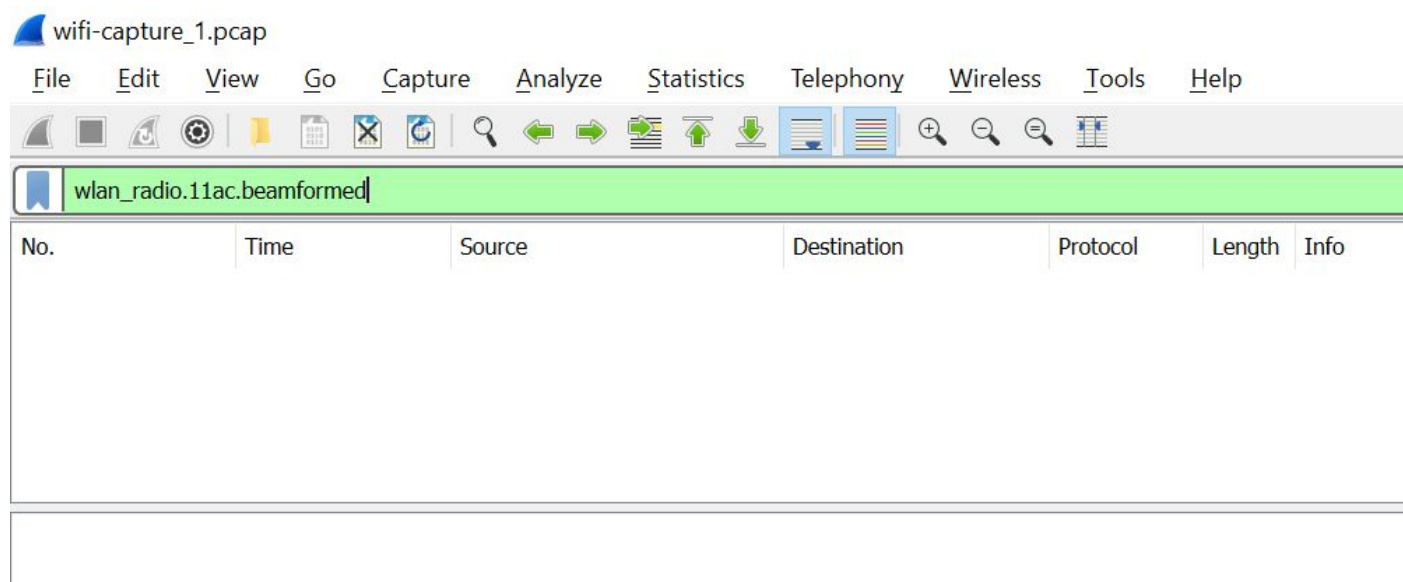
Q2. Are any packets in given traffic capture were transmitted using 802.11ac beamforming? State Yes or No.

Answer: No

Solution:

Filter the traffic to show packets in which beamformed field is present.

Filter: wlan_radio.11ac.beamformed



No packet has the beamformed field which means the answer is No.

Q3. Does BSSID e4:95:6e:45:9c:97 hardware supports MCS9? State Yes or No.

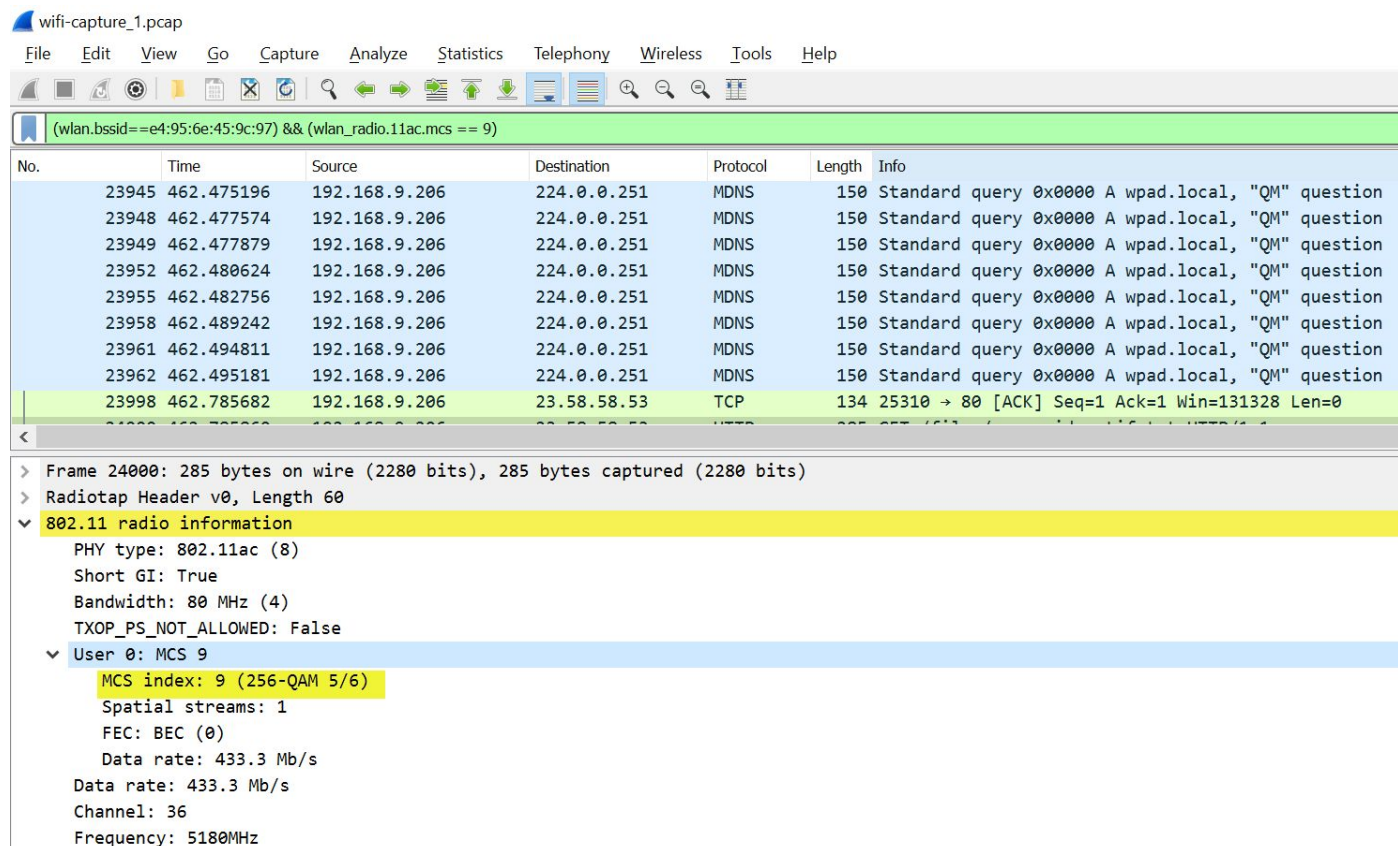
Answer: Yes

Solution:

Apply filter for given BSSID and MCS index.

Filter: (wlan.bssid==e4:95:6e:45:9c:97) && (wlan_radio.11ac.mcs == 9)

In radio information layer, one can check that MCS index 9 is present which means the answer is a yes.



The image shows a Wireshark packet capture of a network traffic. The filter bar at the top displays the filter: (wlan.bssid==e4:95:6e:45:9c:97) && (wlan_radio.11ac.mcs == 9). The packet list shows several MDNS queries and a TCP ACK packet (No. 23998). The packet details pane for the selected TCP ACK packet shows the following information:

- Frame 24000: 285 bytes on wire (2280 bits), 285 bytes captured (2280 bits)
- Radiotap Header v0, Length 60
- 802.11 radio information
 - PHY type: 802.11ac (8)
 - Short GI: True
 - Bandwidth: 80 MHz (4)
 - TXOP_PS_NOT_ALLOWED: False
- User 0: MCS 9
 - MCS index: 9 (256-QAM 5/6)
 - Spatial streams: 1
 - FEC: BEC (0)
 - Data rate: 433.3 Mb/s
 - Data rate: 433.3 Mb/s
 - Channel: 36
 - Frequency: 5180MHz

Q4. What is the value of maximum supported transmission power for AP hosting “CourageTheCowardlyDog” SSID? Provide answer in dBm units.

Answer: 23

Solution:

Apply the following filter to only show the traffic from CourageTheCowardlyDog SSID

Filter: wlan contains CourageTheCowardlyDog

Check VHT Tx Power Envelope Information Element (IE) in any beacon which belongs to this SSID. This will show the maximum supported transmission power.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan contains CourageTheCowardlyDog

No.	Time	Source	Destination	Protocol	Length	Info
22939	455.691302	GuangLia_05:9c:97	Broadcast	802.11	264	Beacon frame, SN=290, FN=0, Flags=....., BI=100, SSID=CourageTheCowardlyDog
22945	455.755299	IntelCor_56:e1:04	GuangLia_05:9c:97	802.11	180	Association Request, SN=52, FN=0, Flags=....., SSID=CourageTheCowardlyDog
22951	455.781809	GuangLia_05:9c:97	Broadcast	802.11	264	Beacon frame, SN=294, FN=0, Flags=....., BI=100, SSID=CourageTheCowardlyDog

<

- > Fixed parameters (12 bytes)
- ▼ Tagged parameters (180 bytes)
 - > Tag: SSID parameter set: CourageTheCowardlyDog
 - > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
 - > Tag: DS Parameter set: Current Channel: 36
 - > Tag: Traffic Indication Map (TIM): DTIM 1 of 0 bitmap
 - > Tag: Country Information: Country Code US, Environment Any
 - > Tag: QBSS Load Element 802.11e CCA Version
 - > Tag: Supported Operating Classes
 - > Tag: HT Capabilities (802.11n D1.10)
 - > Tag: HT Information (802.11n D1.10)
 - > Tag: Extended Capabilities (8 octets)
 - > Tag: VHT Capabilities
 - > Tag: VHT Operation
 - ▼ Tag: VHT Tx Power Envelope
 - Tag Number: VHT Tx Power Envelope (195)
 - Tag length: 4
 - > Tx Pwr Info: 0x02
 - Local Max Tx Pwr Constraint 20MHz: 23.0 dBm
 - Local Max Tx Pwr Constraint 40MHz: 23.0 dBm
 - Local Max Tx Pwr Constraint 80MHz: 23.0 dBm
 - > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element

Q5. Does the Access Point with BSSID e4:95:6e:45:9c:97 have support for SU-Beamforming or MU-Beamforming? State Yes or No.

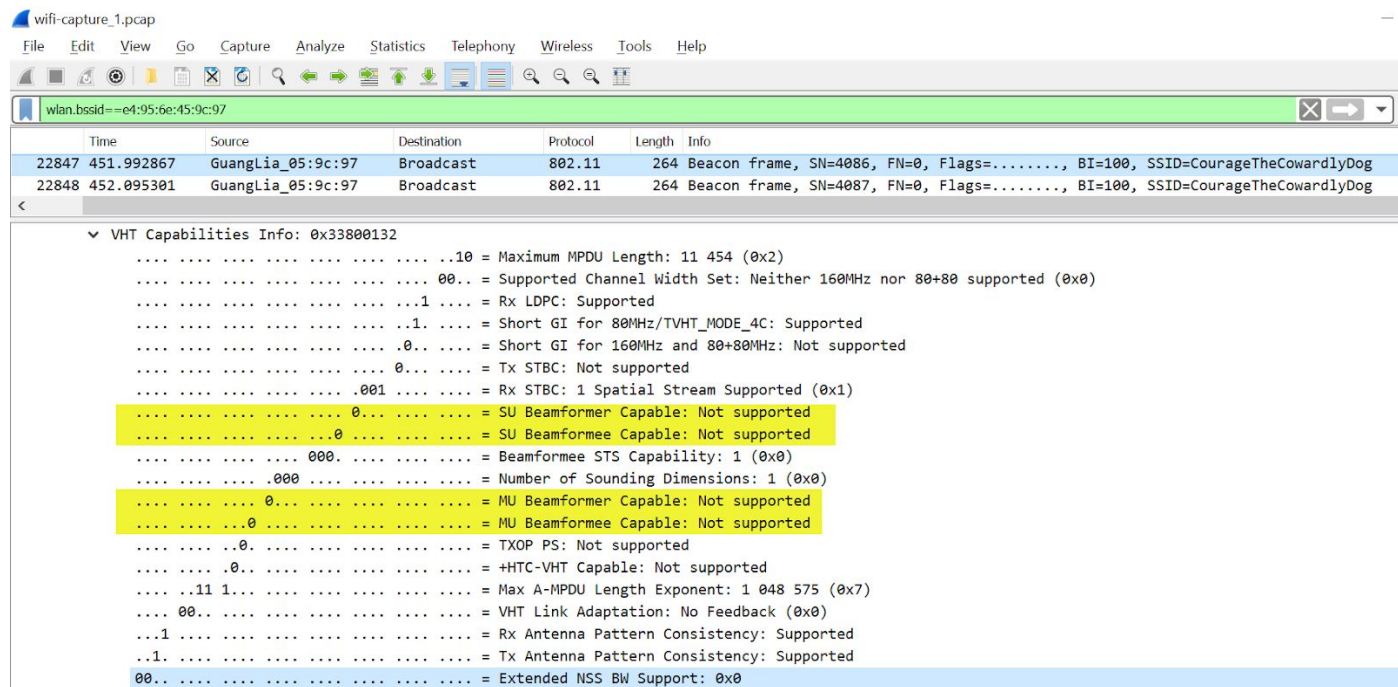
Answer: No

Solution:

Apply the following filter to only view the traffic for given BSSID

Filter: wlan.bssid==e4:95:6e:45:9c:97

Check the VHT Capabilities fields for beamforming. The fields are set to zero which means beamforming was not used.



References:

1. Wireshark (<https://www.wireshark.org/>)
2. 802.11ac standard (https://standards.ieee.org/standard/802_11ac-2013.html)
3. Pentester Academy 802.11 monitoring course (<https://www.pentesteracademy.com/course?id=32>)