

## The image features a word cloud in the shape of the map of India. The words are arranged to fit the geographical outline of the country. The most prominent words, shown in larger fonts, include "ATTACK", "DEFENSE", "LABS", "COURSES", "PENTESTER ACADEMY", "RED TEAM", "ACCESS POINT", "TOOL BOX", "TRAINING", "HACKER", "PATV", "WORLD-CLASS TRAINERS", "PENTESTING", "TEAM LABS", "ACADEMY", "POINT", "DEFENSE L", "ACCESS P", "WORLD-CLAS", "TRAINING", "SPATV ACCESS", "PENTESTER ACADEN", "COURSES PENTESTER ACA", "PENTESTER ACADEMY ATTACK DEFENSE LABS", "TOOL BOX WORLD-CI", "TRAINING CO", "PENTESTER ACADEMY TOOL BOX", and "PENTESTING". The words "ATTACK" and "DEFENSE" are the largest and are colored red and dark blue respectively, while the others are in shades of gray. The background is white.

Name	802.11ac Packet Analysis
URL	<a href="https://www.attackdefense.com/challengedetails?cid">https://www.attackdefense.com/challengedetails?cid</a>
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 antennas were there in the capturing device?**

**Answer:** 2

**Solution:**

In the radiotap header of the captured packet, we can observe the antenna.

```
▼ Radiotap Header v0, Length 48
  Header revision: 0
  Header pad: 0
  Header length: 48
  > Present flags
    MAC timestamp: 1606014154
  > Flags: 0x00
    Data Rate: 6.0 Mb/s
    Channel frequency: 5180 [A 36]
  > Channel flags: 0x0140, Orthogonal Frequency-Division Multiplexing (OFDM), 5 GHz spectrum
    Antenna signal: -30dBm
  > RX flags: 0x0000
  > A-MPDU status
    Antenna signal: -30dBm
    Antenna: 0
    Antenna signal: -73dBm
    Antenna: 2
```

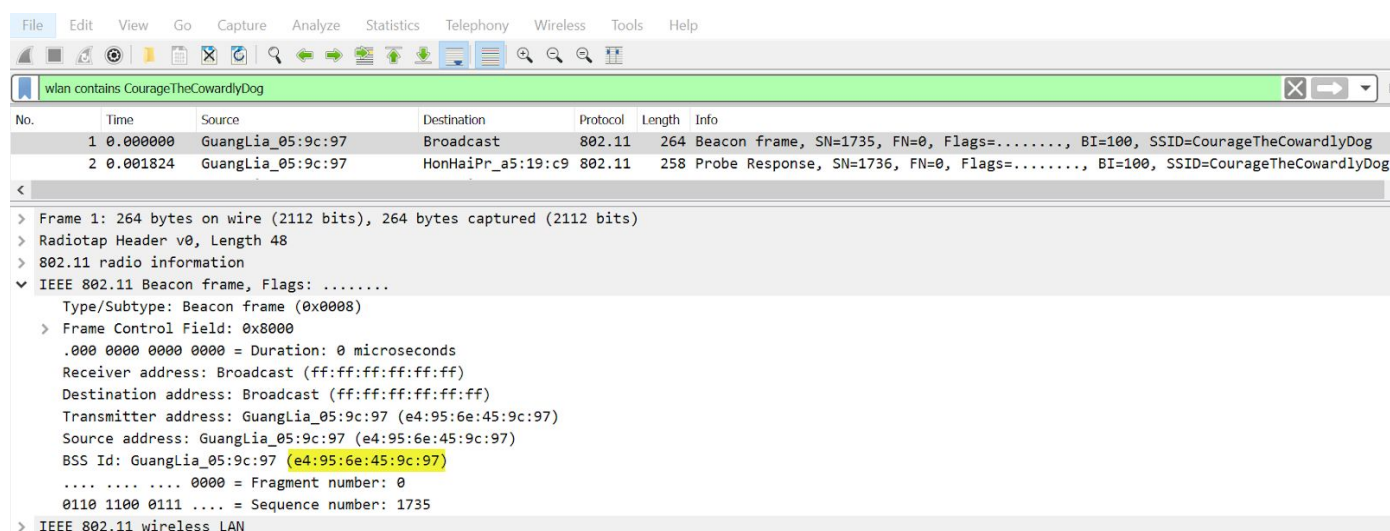
**Q2. A 802.11ac capable client device is using “CourageTheCowardlyDog” SSID. What is the MAC address of this device?**

**Answer:** 34:e6:ad:56:e1:04

**Solution:**

Filter the traffic to just see packets of “CourageTheCowardlyDog” SSID.

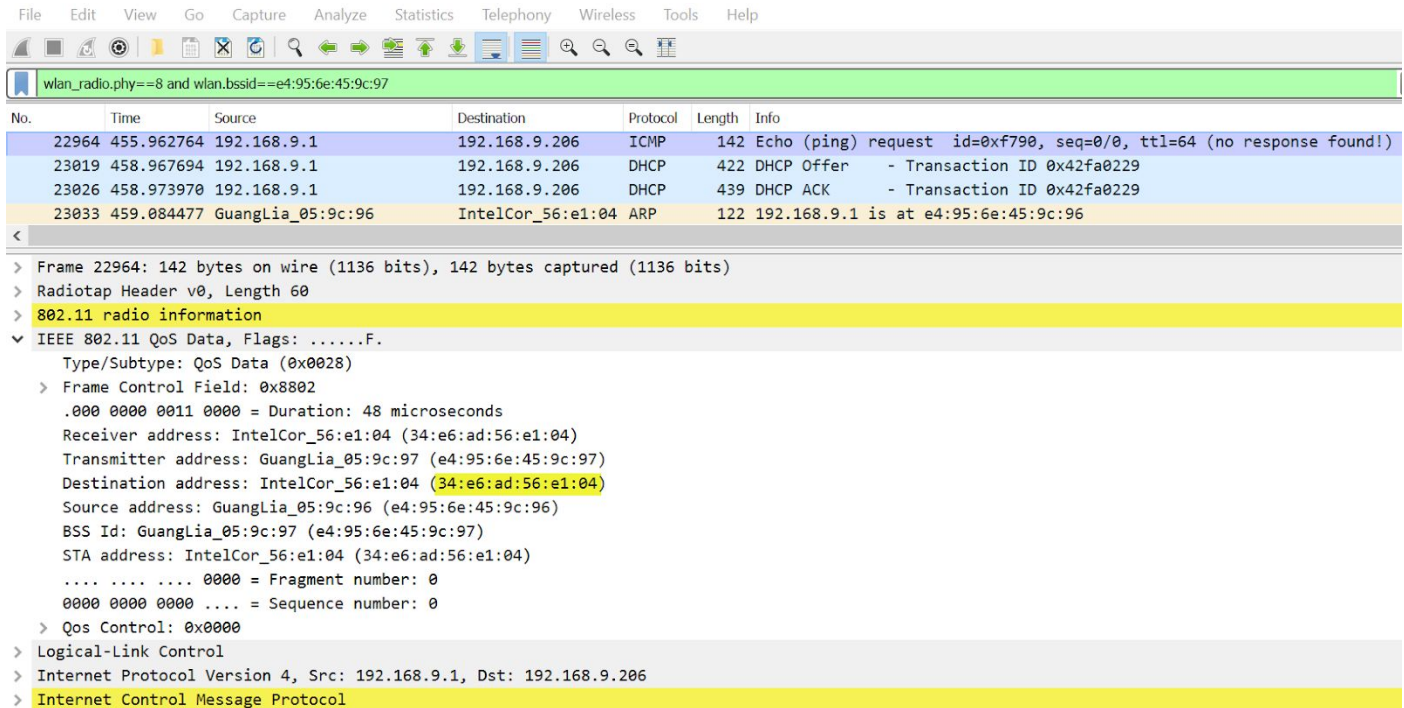
**Filter:** wlan contains CourageTheCowardlyDog



The BSSID related to “CourageTheCowardlyDog” SSID is e4:95:6e:45:9c:97.

Filter the traffic to just see 802.11ac packets from this BSSID.

**Filter:** wlan\_radio.phy==8 and wlan.bssid==e4:95:6e:45:9c:97



The image shows a Wireshark packet capture interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. The packet list pane shows several packets, with packet 23033 selected. The packet details pane shows the structure of the selected packet, including IEEE 802.11 QoS Data, Frame Control Field, and Internet Control Message Protocol.

No.	Time	Source	Destination	Protocol	Length	Info
22964	455.962764	192.168.9.1	192.168.9.206	ICMP	142	Echo (ping) request id=0xf790, seq=0/0, ttl=64 (no response found!)
23019	458.967694	192.168.9.1	192.168.9.206	DHCP	422	DHCP Offer - Transaction ID 0x42fa0229
23026	458.973970	192.168.9.1	192.168.9.206	DHCP	439	DHCP ACK - Transaction ID 0x42fa0229
23033	459.084477	GuangLia_05:9c:96	IntelCor_56:e1:04	ARP	122	192.168.9.1 is at e4:95:6e:45:9c:96

Frame 22964: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits)  
 > Radiotap Header v0, Length 60  
 > 802.11 radio information  
 > IEEE 802.11 QoS Data, Flags: .....F.  
   Type/Subtype: QoS Data (0x0028)  
   > Frame Control Field: 0x8802  
     .000 0000 0011 0000 = Duration: 48 microseconds  
     Receiver address: IntelCor\_56:e1:04 (34:e6:ad:56:e1:04)  
     Transmitter address: GuangLia\_05:9c:97 (e4:95:6e:45:9c:97)  
     Destination address: IntelCor\_56:e1:04 (34:e6:ad:56:e1:04)  
     Source address: GuangLia\_05:9c:96 (e4:95:6e:45:9c:96)  
     BSS Id: GuangLia\_05:9c:97 (e4:95:6e:45:9c:97)  
     STA address: IntelCor\_56:e1:04 (34:e6:ad:56:e1:04)  
     .... .... 0000 = Fragment number: 0  
     0000 0000 .... = Sequence number: 0  
   > Qos Control: 0x0000  
 > Logical-Link Control  
 > Internet Protocol Version 4, Src: 192.168.9.1, Dst: 192.168.9.206  
 > Internet Control Message Protocol

Associated client MAC is 34:e6:ad:56:e1:04

**Q3. In big networks, multiple BSSIDs operate under single/same SSID. Which BSSID is responsible for most traffic of “EASYDAFTAR SOUTH” SSID?**

**Answer:** c8:d7:19:17:7e:3a

**Solution:**

Use “Wireless > WLAN Traffic” option from the Wireless option of the menu bar, to check the Wireless LAN Statistics.



wifi-capture\_1.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Wireshark · Wireless LAN Statistics · wifi-capture\_1.pcap

BSSID	Channel	SSID	Percent Packets	Percent Retry	Retry	Beacons	Data Pkts	Be Req	Be Resp	Auths	Deauths	Other	Pr
> e4:95:6e:45:9c:97	36	CourageTheCowardlyDog	94.8	7.5	2934	3420	35557	1	336	6	1	59	W
> c8:d7:19:17:7e:3a	36	EASYDAFTAR SOUTH	3.4	2.3	33	884	481	0	51	2	0	9	W
> ff:ff:ff:ff:ff:ff	36	<Broadcast>	1.0	0.0	0	0	1	426	0	0	0	0	
> e4:95:6e:45:9c:97	36	norbughangresort	0.1	2.4	1	0	36	4	0	0	0	2	
> ff:ff:ff:ff:ff:ff		AVNB2	0.1	0.0	0	0	0	23	0	0	0	0	
> ff:ff:ff:ff:ff:ff		jio	0.1	0.0	0	0	0	21	0	0	0	0	
> ff:ff:ff:ff:ff:ff		CourageTheCowardlyDog	0.0	0.0	0	0	0	9	0	0	0	0	
> 37:28:e6:e8:81:c5		<Broadcast>	0.0	14.3	1	4	2	0	0	0	0	1	U
> ff:ff:ff:ff:ff:ff		Nokia 5.1 Plus	0.0	0.0	0	0	0	7	0	0	0	0	
> c8:d7:19:17:7e:ba	36	EASYDAFTAR SOUTH	0.0	25.0	1	1	1	1	0	0	0	1	
> dd:31:1d:17:7e:3a	36	norbughangresort	0.0	0.0	0	1	0	2	0	0	0	0	
> 16:95:ecb2:a6:cb		<Broadcast>	0.0	66.7	2	1	0	0	0	0	1	1	W
> 19:62:d8:bb:e2:8d		<Broadcast>	0.0	100.0	3	0	0	0	0	0	0	3	W
> ff:ff:ff:ff:ff:ff		airtel_427990	0.0	0.0	0	0	0	3	0	0	0	0	
> 6c:f0:49:cf:7a:37	36	<Broadcast>	0.0	0.0	0	0	0	0	0	0	0	2	
> c8:d7:19:db:c8:ab	36	norbughangresort	0.0	0.0	0	1	0	1	0	0	0	0	
> ff:ff:ff:ff:ff:ff	36	EASYDAFTAR SOUTH	0.0	0.0	0	0	0	2	0	0	0	0	
> 09:7b:85:a0:2e:47		<Broadcast>	0.0	50.0	1	0	0	0	0	0	0	2	W
> 56:f1:98:df:96:e0		<Broadcast>	0.0	50.0	1	0	0	0	1	0	0	1	U
> 59:06:ac:d6:d2:a6		<Broadcast>	0.0	50.0	1	0	0	0	0	0	0	2	W

Display filter: Enter a display filter ...

Copy Save as... Close Help

On sorting the list by percent packets, it is clear that most traffic for SSID “EASYDAFTAR SOUTH” is contributed by BSSID c8:d7:19:17:7e:3a

**Q4. What is the frequency of operation for the network associated with BSSID e4:95:6e:45:9c:97? Provide value in MHz.**

**Answer:** 5180

**Solution:**

Apply filter to only view the traffic transmitted from the given BSSID.

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



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination
111	5.113989	GuangLia_05:9c:97	Broadcast
113	5.222500	GuangLia_05:9c:97	Broadcast
114	5.318447	GuangLia_05:9c:97	Broadcast

<

> Frame 111: 264 bytes on wire (2112 bits), 264 bytes captured (2112 bits)

> Radiotap Header v0, Length 48

✓ 802.11 radio information

- PHY type: 802.11a (5)
- Turbo type: Non-turbo (0)
- Data rate: 6.0 Mb/s
- Channel: 36
- Frequency: 5180MHz
- Signal strength (dBm): -73dBm
- TSF timestamp: 1165783885
- .... 1 = Last part of an A-MPDU: True
- .... 0 = A-MPDU delimiter CRC error: False
- A-MPDU aggregate ID: 124787

> [Duration: 312µs]

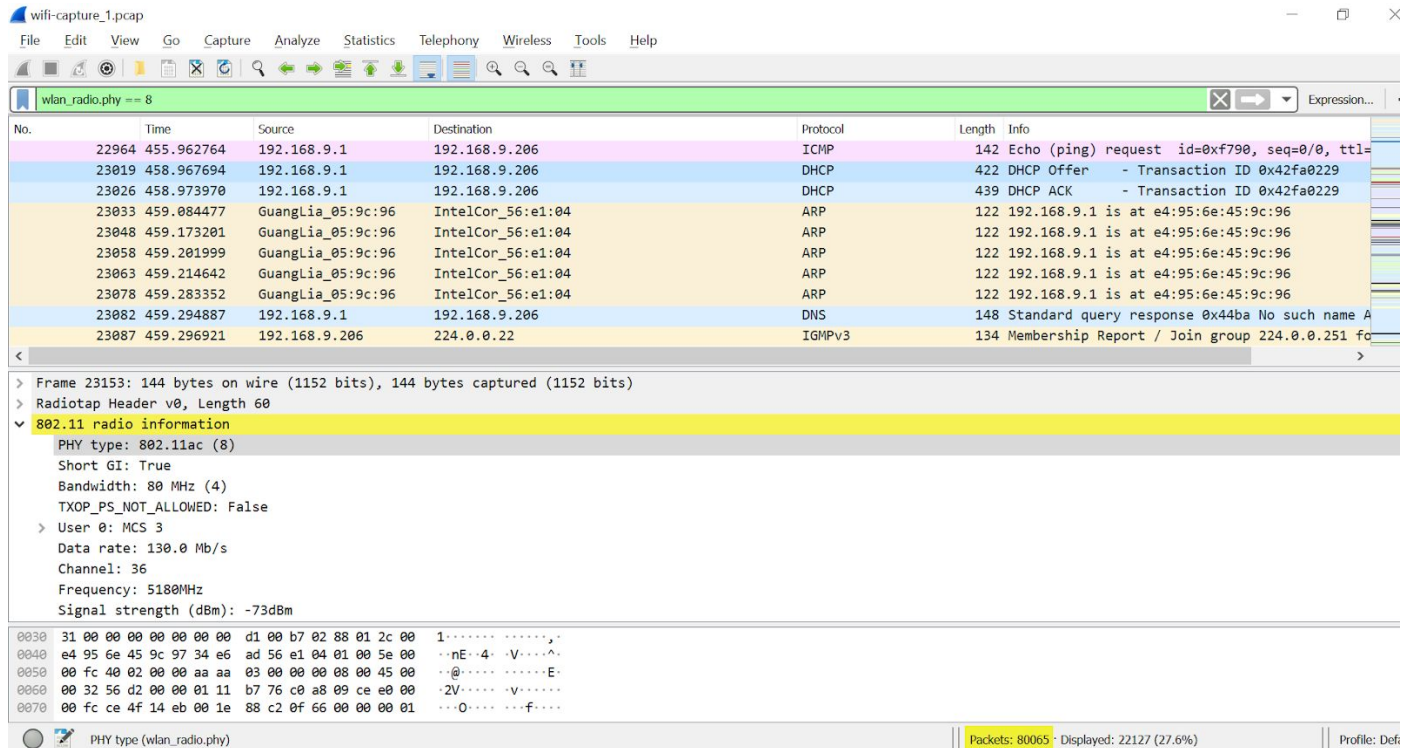
**Q5. How many packets belong to 802.11ac standard?**

**Answer:** 22127

**Solution:**

Filter the traffic to just view the 802.11ac packets.

**Filter:** wlan\_radio.phy==8



## References:

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