POLITECNICO DI TORINO

01NWDBH - Mobile and Sensor Networks

Lab 02

Advanced WI-FI scanning and trace analysis

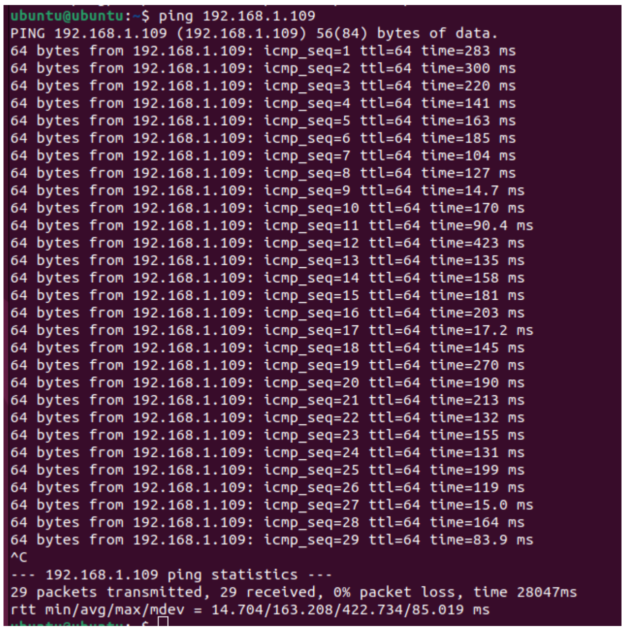
Group ID:
05

Students:

Valerio Collina	333919
Ammar Hussein	329829
Md Ismail Hossain	342704
Md. Ataur Rabby	347363

Academic year 2025/2026

1 Capturing Wi-Fi Frames



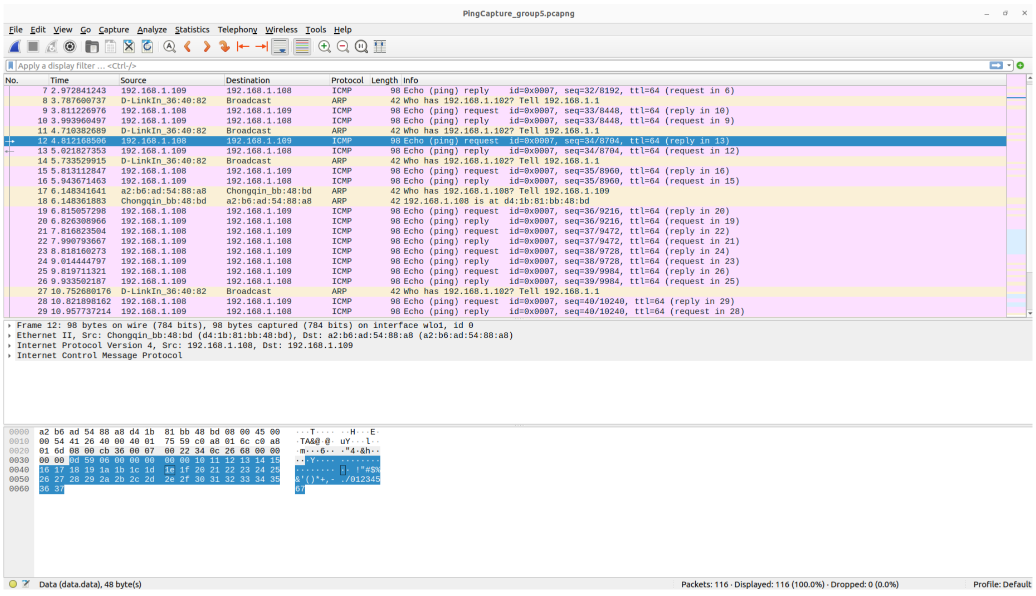
```
ubuntu@ubuntu:~$ ping 192.168.1.109
PING 192.168.1.109 (192.168.1.109) 56(84) bytes of data.
64 bytes from 192.168.1.109: icmp_seq=1 ttl=64 time=283 ms
64 bytes from 192.168.1.109: icmp_seq=2 ttl=64 time=300 ms
64 bytes from 192.168.1.109: icmp_seq=3 ttl=64 time=220 ms
64 bytes from 192.168.1.109: icmp_seq=4 ttl=64 time=141 ms
64 bytes from 192.168.1.109: icmp_seq=5 ttl=64 time=163 ms
64 bytes from 192.168.1.109: icmp_seq=6 ttl=64 time=185 ms
64 bytes from 192.168.1.109: icmp_seq=7 ttl=64 time=104 ms
64 bytes from 192.168.1.109: icmp_seq=8 ttl=64 time=127 ms
64 bytes from 192.168.1.109: icmp_seq=9 ttl=64 time=14.7 ms
64 bytes from 192.168.1.109: icmp_seq=10 ttl=64 time=170 ms
64 bytes from 192.168.1.109: icmp_seq=11 ttl=64 time=90.4 ms
64 bytes from 192.168.1.109: icmp_seq=12 ttl=64 time=423 ms
64 bytes from 192.168.1.109: icmp_seq=13 ttl=64 time=135 ms
64 bytes from 192.168.1.109: icmp_seq=14 ttl=64 time=158 ms
64 bytes from 192.168.1.109: icmp_seq=15 ttl=64 time=181 ms
64 bytes from 192.168.1.109: icmp_seq=16 ttl=64 time=203 ms
64 bytes from 192.168.1.109: icmp_seq=17 ttl=64 time=17.2 ms
64 bytes from 192.168.1.109: icmp_seq=18 ttl=64 time=145 ms
64 bytes from 192.168.1.109: icmp_seq=19 ttl=64 time=270 ms
64 bytes from 192.168.1.109: icmp_seq=20 ttl=64 time=190 ms
64 bytes from 192.168.1.109: icmp_seq=21 ttl=64 time=213 ms
64 bytes from 192.168.1.109: icmp_seq=22 ttl=64 time=132 ms
64 bytes from 192.168.1.109: icmp_seq=23 ttl=64 time=155 ms
64 bytes from 192.168.1.109: icmp_seq=24 ttl=64 time=131 ms
64 bytes from 192.168.1.109: icmp_seq=25 ttl=64 time=199 ms
64 bytes from 192.168.1.109: icmp_seq=26 ttl=64 time=119 ms
64 bytes from 192.168.1.109: icmp_seq=27 ttl=64 time=15.0 ms
64 bytes from 192.168.1.109: icmp_seq=28 ttl=64 time=164 ms
64 bytes from 192.168.1.109: icmp_seq=29 ttl=64 time=83.9 ms
^C
--- 192.168.1.109 ping statistics ---
29 packets transmitted, 29 received, 0% packet loss, time 28047ms
rtt min/avg/max/mdev = 14.704/163.208/422.734/85.019 ms
```

Figure 1: Ping command

To generate traffic between the two devices, we executed `ping 192.168.1.109` from the PC and let it run for approximately 28 seconds. The terminal reported:

- 29 packets transmitted,
- 29 packets received,
- 0% packet loss.

This confirms that all sent packets were successfully received with no loss.



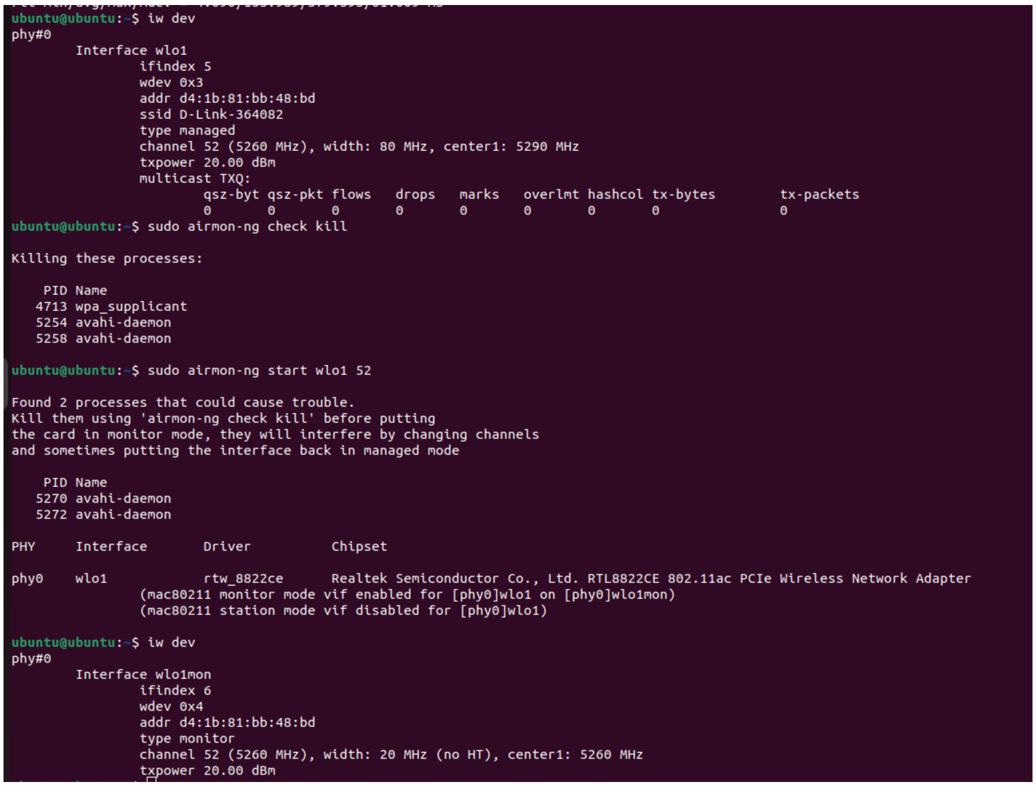
PingCapture_group5.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time          Source              Destination         Protocol Length Info
    7 2.972841243   192.168.1.109       192.168.1.108       ICMP       98 Echo (ping) reply    id=0x0007, seq=32/8192, ttl=64 (request in 6)
    8 3.787600737   D-LinkIn_36:40:82   Broadcast           ARP        42 Who has 192.168.1.102? Tell 192.168.1.1
    9 3.811226976   192.168.1.108       192.168.1.109       ICMP       98 Echo (ping) request  id=0x0007, seq=33/8448, ttl=64 (reply in 10)
   10 3.993960497   192.168.1.109       192.168.1.108       ICMP       98 Echo (ping) reply    id=0x0007, seq=33/8448, ttl=64 (request in 9)
   11 4.710382689   D-LinkIn_36:40:82   Broadcast           ARP        42 Who has 192.168.1.102? Tell 192.168.1.1
   12 4.812168506   192.168.1.108       192.168.1.109       ICMP       98 Echo (ping) request  id=0x0007, seq=34/8704, ttl=64 (reply in 13)
   13 5.021827353   192.168.1.109       192.168.1.108       ICMP       98 Echo (ping) reply    id=0x0007, seq=34/8704, ttl=64 (request in 12)
   14 5.733529915   D-LinkIn_36:40:82   Broadcast           ARP        42 Who has 192.168.1.102? Tell 192.168.1.1
   15 5.813112847   192.168.1.108       192.168.1.109       ICMP       98 Echo (ping) request  id=0x0007, seq=35/8960, ttl=64 (reply in 16)
   16 5.943671463   192.168.1.109       192.168.1.108       ICMP       98 Echo (ping) reply    id=0x0007, seq=35/8960, ttl=64 (request in 15)
   17 6.148341641   a2:b6:ad:54:88:a8   Chongqin_bb:48:bd   ARP        42 Who has 192.168.1.108? Tell 192.168.1.109
   18 6.148361883   Chongqin_bb:48:bd   a2:b6:ad:54:88:a8   ARP        42 192.168.1.108 is at d4:1b:81:bb:48:bd
   19 6.815057298   192.168.1.108       192.168.1.109       ICMP       98 Echo (ping) request  id=0x0007, seq=36/9216, ttl=64 (reply in 20)
   20 6.826308966   192.168.1.109       192.168.1.108       ICMP       98 Echo (ping) reply    id=0x0007, seq=36/9216, ttl=64 (request in 19)
   21 7.816823504   192.168.1.108       192.168.1.109       ICMP       98 Echo (ping) request  id=0x0007, seq=37/9472, ttl=64 (reply in 22)
   22 7.990793667   192.168.1.109       192.168.1.108       ICMP       98 Echo (ping) reply    id=0x0007, seq=37/9472, ttl=64 (request in 21)
   23 8.818160273   192.168.1.108       192.168.1.109       ICMP       98 Echo (ping) request  id=0x0007, seq=38/9728, ttl=64 (reply in 24)
   24 9.014444797   192.168.1.109       192.168.1.108       ICMP       98 Echo (ping) reply    id=0x0007, seq=38/9728, ttl=64 (request in 23)
   25 9.819711321   192.168.1.108       192.168.1.109       ICMP       98 Echo (ping) request  id=0x0007, seq=39/9984, ttl=64 (reply in 26)
   26 9.933502187   192.168.1.109       192.168.1.108       ICMP       98 Echo (ping) reply    id=0x0007, seq=39/9984, ttl=64 (request in 25)
   27 10.752680176  D-LinkIn_36:40:82   Broadcast           ARP        42 Who has 192.168.1.102? Tell 192.168.1.1
   28 10.821898162  192.168.1.108       192.168.1.109       ICMP       98 Echo (ping) request  id=0x0007, seq=40/10240, ttl=64 (reply in 29)
   29 10.957737214  192.168.1.109       192.168.1.108       ICMP       98 Echo (ping) reply    id=0x0007, seq=40/10240, ttl=64 (request in 28)

› Frame 12: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlo1, id 0
› Ethernet II, Src: Chongqin_bb:48:bd (d4:1b:81:bb:48:bd), Dst: a2:b6:ad:54:88:a8 (a2:b6:ad:54:88:a8)
› Internet Protocol Version 4, Src: 192.168.1.108, Dst: 192.168.1.109
› Internet Control Message Protocol

0000  a2 b6 ad 54 88 a8 d4 1b  81 bb 48 bd 08 00 45 00   ···T···· ··H···E·
0010  00 54 41 26 40 00 40 01  75 59 c0 a8 01 6c c0 a8   ·TA&@·@· uY···l··
0020  01 6d 08 00 cb 36 00 07  00 22 34 0c 26 68 00 00   ·m···6·· ·"4·&h··
0030  00 00 0d 59 06 00 00 00  00 00 10 11 12 13 14 15   ···Y···· ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67

Data (data.data), 48 byte(s)          Packets: 116 · Displayed: 116 (100.0%) · Dropped: 0 (0.0%)          Profile: Default
```

Figure 2: Ping capture using Wireshark

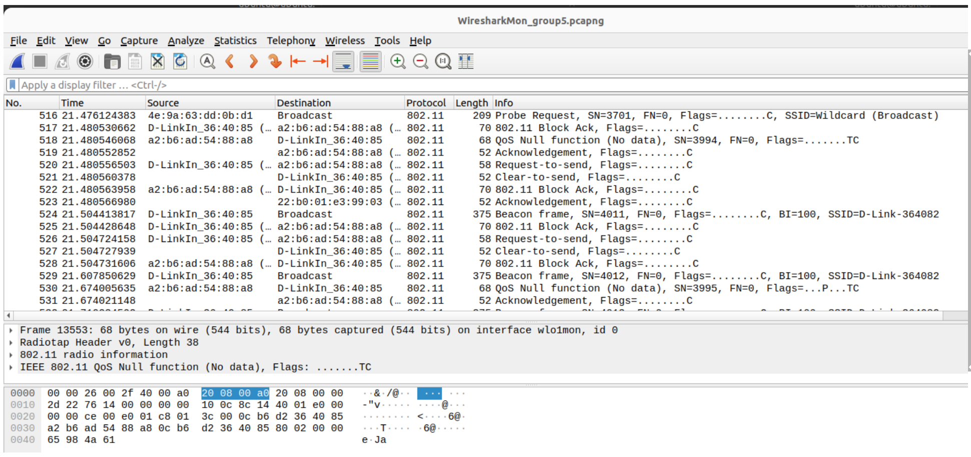
During the ping capture performed without enabling monitor mode, we observed that the packets are ICMP messages encapsulated in Ethernet frames. Since the wireless interface was not set to monitor mode, Wireshark captured traffic only at the data link layer as seen by the operating system—hence, the frames are not IEEE 802.11 frames but standard Ethernet frames. As a result, no Wi-Fi management or control frames are visible in the trace. This limits the level of detail we can observe regarding the wireless protocol itself, as we only see the traffic that was processed by the network stack after being translated by the Wi-Fi interface.

To enable monitor mode and capture raw IEEE 802.11 frames, we used a series of terminal commands on our Linux machine. Once in monitor mode, we initiated ICMP traffic by sending a continuous ping from a smartphone to the local D-Link router. This setup allowed us to capture wireless frames directly from the air, including management and control frames, using Wireshark or `tshark`. A screenshot of the commands used and the capture environment is shown below.



```
ubuntu@ubuntu:~$ iw dev
phy#0
        Interface wlo1
                ifindex 5
                wdev 0x3
                addr d4:1b:81:bb:48:bd
                ssid D-Link-364082
                type managed
                channel 52 (5260 MHz), width: 80 MHz, center1: 5290 MHz
                txpower 20.00 dBm
                multicast TXQ:
                        qsz-byt qsz-pkt flows   drops   marks   overlmt hashcol tx-bytes        tx-packets
                        0       0       0       0       0       0       0       0               0
ubuntu@ubuntu:~$ sudo airmon-ng check kill

Killing these processes:

    PID Name
   4713 wpa_supplicant
   5254 avahi-daemon
   5258 avahi-daemon

ubuntu@ubuntu:~$ sudo airmon-ng start wlo1 52

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
   5270 avahi-daemon
   5272 avahi-daemon

PHY     Interface       Driver          Chipset

phy0    wlo1            rtw_8822ce      Realtek Semiconductor Co., Ltd. RTL8822CE 802.11ac PCIe Wireless Network Adapter
                (mac80211 monitor mode vif enabled for [phy0]wlo1 on [phy0]wlo1mon)
                (mac80211 station mode vif disabled for [phy0]wlo1)

ubuntu@ubuntu:~$ iw dev
phy#0
        Interface wlo1mon
                ifindex 6
                wdev 0x4
                addr d4:1b:81:bb:48:bd
                type monitor
                channel 52 (5260 MHz), width: 20 MHz (no HT), center1: 5260 MHz
                txpower 20.00 dBm
```

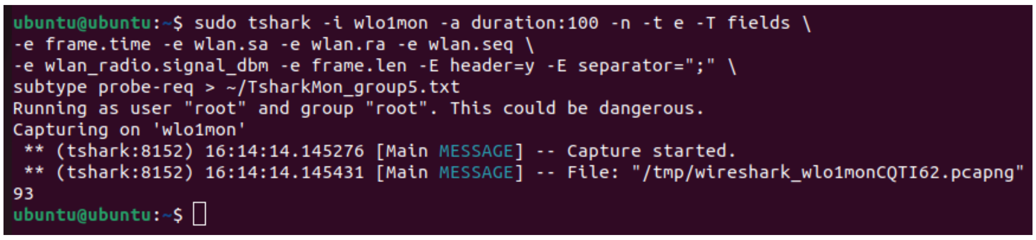
Figure 3: Procedure monitor mode


WiresharkMon_group5.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time          Source               Destination          Protocol Length Info
 516 21.476124383  4e:9a:63:dd:0b:d1    Broadcast            802.11     209 Probe Request, SN=3701, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
 517 21.480530662  D-LinkIn_36:40:85 (… a2:b6:ad:54:88:a8 (… 802.11      70 802.11 Block Ack, Flags=........C
 518 21.480546068  a2:b6:ad:54:88:a8    D-LinkIn_36:40:85    802.11      68 QoS Null function (No data), SN=3994, FN=0, Flags=.......TC
 519 21.480552852                       a2:b6:ad:54:88:a8 (… 802.11      52 Acknowledgement, Flags=........C
 520 21.480556503  D-LinkIn_36:40:85 (… a2:b6:ad:54:88:a8 (… 802.11      58 Request-to-send, Flags=........C
 521 21.480560378                       D-LinkIn_36:40:85 (… 802.11      52 Clear-to-send, Flags=........C
 522 21.480563958  a2:b6:ad:54:88:a8 (… D-LinkIn_36:40:85 (… 802.11      70 802.11 Block Ack, Flags=........C
 523 21.480566980                       22:b0:01:e3:99:03 (… 802.11      52 Acknowledgement, Flags=........C
 524 21.504413817  D-LinkIn_36:40:85    Broadcast            802.11     375 Beacon frame, SN=4011, FN=0, Flags=........C, BI=100, SSID=D-Link-364082
 525 21.504428648  D-LinkIn_36:40:85 (… a2:b6:ad:54:88:a8 (… 802.11      70 802.11 Block Ack, Flags=........C
 526 21.504724158  D-LinkIn_36:40:85 (… a2:b6:ad:54:88:a8 (… 802.11      58 Request-to-send, Flags=........C
 527 21.504727939                       D-LinkIn_36:40:85 (… 802.11      52 Clear-to-send, Flags=........C
 528 21.504731606  a2:b6:ad:54:88:a8 (… D-LinkIn_36:40:85 (… 802.11      70 802.11 Block Ack, Flags=........C
 529 21.607850629  D-LinkIn_36:40:85    Broadcast            802.11     375 Beacon frame, SN=4012, FN=0, Flags=........C, BI=100, SSID=D-Link-364082
 530 21.674005635  a2:b6:ad:54:88:a8    D-LinkIn_36:40:85    802.11      68 QoS Null function (No data), SN=3995, FN=0, Flags=...P...TC
 531 21.674021148                       a2:b6:ad:54:88:a8 (… 802.11      52 Acknowledgement, Flags=........C

› Frame 13553: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface wlo1mon, id 0
› Radiotap Header v0, Length 38
› 802.11 radio information
› IEEE 802.11 QoS Null function (No data), Flags: .......TC

0000  00 00 26 00 2f 40 00 a0  20 08 00 a0 20 08 00 00   ··&·/@·· ········
0010  2d 22 76 14 00 00 00 00  10 0c 8c 14 40 01 e0 00   -"v····· ····@···
0020  00 00 ce 00 e0 01 c8 01  3c 00 0c b6 d2 36 40 85   ········ <····6@·
0030  a2 b6 ad 54 88 a8 0c b6  d2 36 40 85 80 02 00 00   ···T···· ·6@·····
0040  65 98 4a 61                                        e·Ja
```

Figure 4: Wireshark capture using monitor mode

Figure 5: Screenshot phone's MAC address

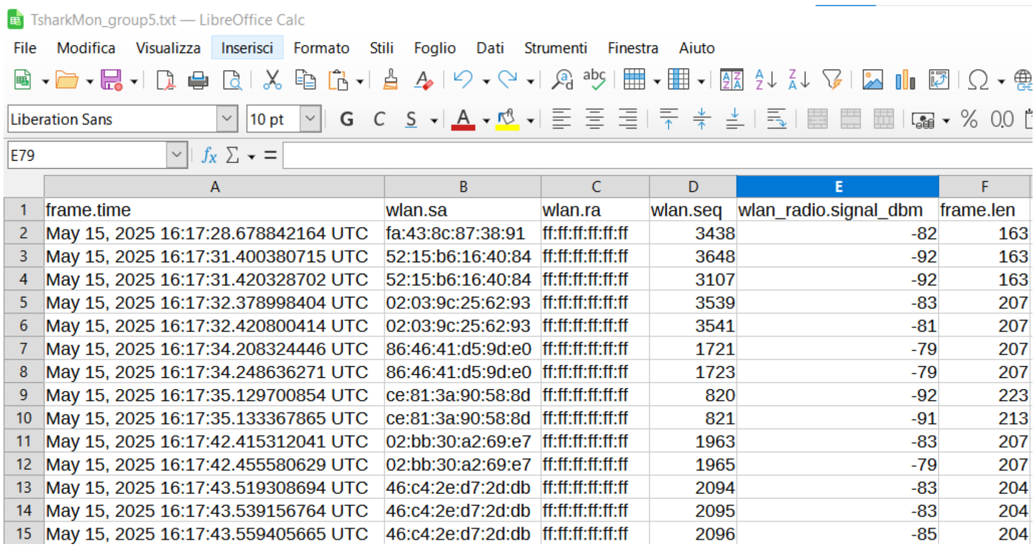


```
ubuntu@ubuntu:~$ sudo tshark -i wlo1mon -a duration:100 -n -t e -T fields \
-e frame.time -e wlan.sa -e wlan.ra -e wlan.seq \
-e wlan_radio.signal_dbm -e frame.len -E header=y -E separator=";" \
subtype probe-req > ~/TsharkMon_group5.txt
Running as user "root" and group "root". This could be dangerous.
Capturing on 'wlo1mon'
 ** (tshark:8152) 16:14:14.145276 [Main MESSAGE] -- Capture started.
 ** (tshark:8152) 16:14:14.145431 [Main MESSAGE] -- File: "/tmp/wireshark_wlo1monCQTI62.pcapng"
93
ubuntu@ubuntu:~$ 
```

Figure 6: Sniffing using Tshark tools

This command captures Wi-Fi traffic for 100 seconds using the selected interface in monitor mode. The `-i` option specifies the interface, `-a duration:100` sets the time limit for the capture, and `-n` disables DNS resolution. The flag `-t e` ensures that timestamps are displayed in epoch format. With `-T fields`, we extract only specific fields, defined by the `-e` options: frame timestamp, source and receiver MAC addresses, sequence number, signal strength in dBm, and frame length. The `-E` parameters configure the output as a CSV-like structure with headers and semicolon delimiters.

We were able to capture several **probe request** frames, which are typically broadcast by devices actively searching for available Wi-Fi access points. The output file was successfully generated during our own capture session using `tshark`, without downloading any sample data from the course portal. The resulting log is clearly structured and suitable for further analysis of wireless activity in the environment.


TsharkMon_group5.txt — LibreOffice Calc
File Modifica Visualizza Inserisci Formato Stili Foglio Dati Strumenti Finestra Aiuto
Liberation Sans
10 pt
E79

	A	B	C	D	E	F
1	frame.time	wlan.sa	wlan.ra	wlan.seq	wlan_radio.signal_dbm	frame.len
2	May 15, 2025 16:17:28.678842164 UTC	fa:43:8c:87:38:91	ff:ff:ff:ff:ff:ff	3438	-82	163
3	May 15, 2025 16:17:31.400380715 UTC	52:15:b6:16:40:84	ff:ff:ff:ff:ff:ff	3648	-92	163
4	May 15, 2025 16:17:31.420328702 UTC	52:15:b6:16:40:84	ff:ff:ff:ff:ff:ff	3107	-92	163
5	May 15, 2025 16:17:32.378998404 UTC	02:03:9c:25:62:93	ff:ff:ff:ff:ff:ff	3539	-83	207
6	May 15, 2025 16:17:32.420800414 UTC	02:03:9c:25:62:93	ff:ff:ff:ff:ff:ff	3541	-81	207
7	May 15, 2025 16:17:34.208324446 UTC	86:46:41:d5:9d:e0	ff:ff:ff:ff:ff:ff	1721	-79	207
8	May 15, 2025 16:17:34.248636271 UTC	86:46:41:d5:9d:e0	ff:ff:ff:ff:ff:ff	1723	-79	207
9	May 15, 2025 16:17:35.129700854 UTC	ce:81:3a:90:58:8d	ff:ff:ff:ff:ff:ff	820	-92	223
10	May 15, 2025 16:17:35.133367865 UTC	ce:81:3a:90:58:8d	ff:ff:ff:ff:ff:ff	821	-91	213
11	May 15, 2025 16:17:42.415312041 UTC	02:bb:30:a2:69:e7	ff:ff:ff:ff:ff:ff	1963	-83	207
12	May 15, 2025 16:17:42.455580629 UTC	02:bb:30:a2:69:e7	ff:ff:ff:ff:ff:ff	1965	-79	207
13	May 15, 2025 16:17:43.519308694 UTC	46:c4:2e:d7:2d:db	ff:ff:ff:ff:ff:ff	2094	-83	204
14	May 15, 2025 16:17:43.539156764 UTC	46:c4:2e:d7:2d:db	ff:ff:ff:ff:ff:ff	2095	-83	204
15	May 15, 2025 16:17:43.559405665 UTC	46:c4:2e:d7:2d:db	ff:ff:ff:ff:ff:ff	2096	-85	204

Figure 7: TsharkMon_group5

2 Analyzing Wi-Fi Traces

As shown in Figure 2, the ping capture in Wireshark displays ICMP request and reply packets. The Layer 2 headers correspond to Ethernet frames rather than 802.11 frames, since the capture was performed in managed mode. As a result, Wi-Fi management and control frames are not present. This behavior is expected and confirms that monitor mode is necessary to view raw Wi-Fi frames.

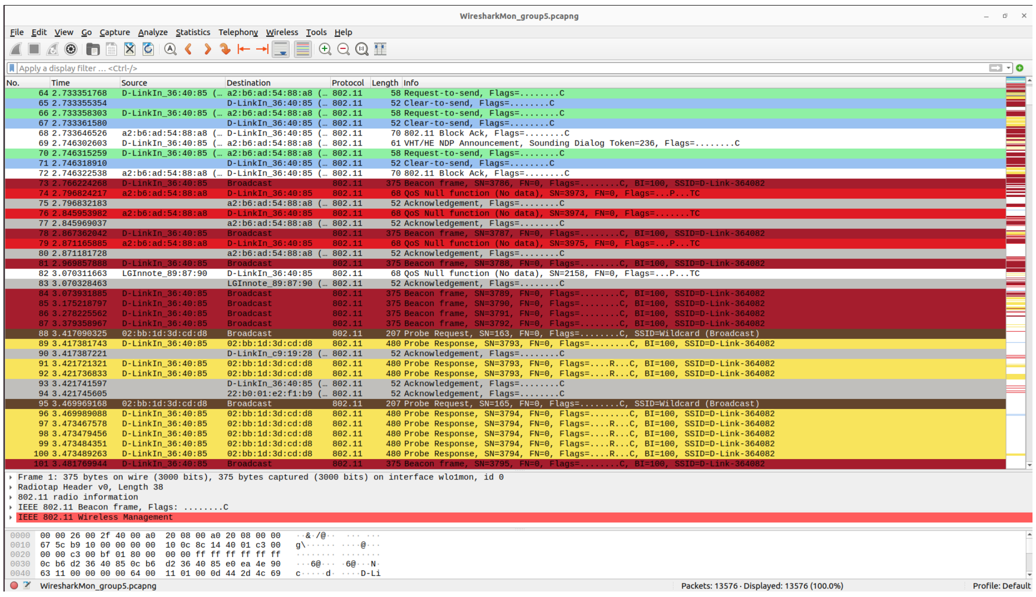
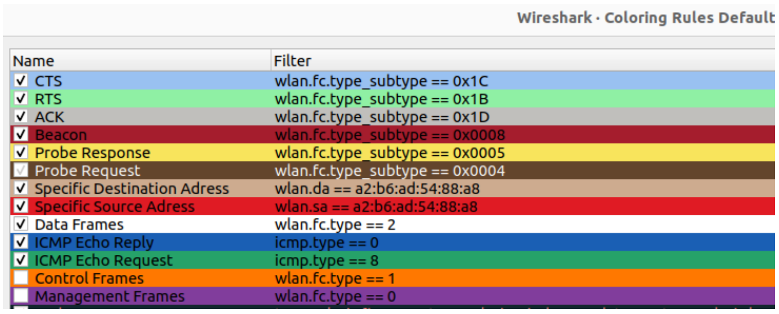

```
WiresharkMon_group5.pcapng
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Wireless  Tools  Help
Apply a display filter ... <Ctrl-/>
No.     Time         Source               Destination          Protocol Length Info
     64 2.733351768  D-LinkIn_36:40:85 (… a2:b6:ad:54:88:a8 (… 802.11    58 Request-to-send, Flags=........C
     65 2.733355354                       D-LinkIn_36:40:85 (… 802.11    52 Clear-to-send, Flags=........C
     66 2.733358303  D-LinkIn_36:40:85 (… a2:b6:ad:54:88:a8 (… 802.11    58 Request-to-send, Flags=........C
     67 2.733361580                       D-LinkIn_36:40:85 (… 802.11    52 Clear-to-send, Flags=........C
     68 2.733646526  a2:b6:ad:54:88:a8 (… D-LinkIn_36:40:85 (… 802.11    70 802.11 Block Ack, Flags=........C
     69 2.746302603  D-LinkIn_36:40:85 (… a2:b6:ad:54:88:a8 (… 802.11    61 VHT/HE NDP Announcement, Sounding Dialog Token=236, Flags=........C
     70 2.746315259  D-LinkIn_36:40:85 (… a2:b6:ad:54:88:a8 (… 802.11    58 Request-to-send, Flags=........C
     71 2.746318910                       D-LinkIn_36:40:85 (… 802.11    52 Clear-to-send, Flags=........C
     72 2.746322538  a2:b6:ad:54:88:a8 (… D-LinkIn_36:40:85 (… 802.11    70 802.11 Block Ack, Flags=........C
     73 2.766224268  D-LinkIn_36:40:85    Broadcast            802.11   375 Beacon frame, SN=3786, FN=0, Flags=........C, BI=100, SSID=D-Link-364082
     74 2.796824217  a2:b6:ad:54:88:a8    D-LinkIn_36:40:85    802.11    68 QoS Null function (No data), SN=3973, FN=0, Flags=...P...TC
     75 2.796832183                       a2:b6:ad:54:88:a8 (… 802.11    52 Acknowledgement, Flags=........C
     76 2.845953982  a2:b6:ad:54:88:a8    D-LinkIn_36:40:85    802.11    68 QoS Null function (No data), SN=3974, FN=0, Flags=.......TC
     77 2.845969037                       a2:b6:ad:54:88:a8 (… 802.11    52 Acknowledgement, Flags=........C
     78 2.867362042  D-LinkIn_36:40:85    Broadcast            802.11   375 Beacon frame, SN=3787, FN=0, Flags=........C, BI=100, SSID=D-Link-364082
     79 2.871165885  a2:b6:ad:54:88:a8    D-LinkIn_36:40:85    802.11    68 QoS Null function (No data), SN=3975, FN=0, Flags=...P...TC
     80 2.871181728                       a2:b6:ad:54:88:a8 (… 802.11    52 Acknowledgement, Flags=........C
     81 2.969857888  D-LinkIn_36:40:85    Broadcast            802.11   375 Beacon frame, SN=3788, FN=0, Flags=........C, BI=100, SSID=D-Link-364082
     82 3.070311663  LGInnote_89:87:90    D-LinkIn_36:40:85    802.11    68 QoS Null function (No data), SN=2158, FN=0, Flags=...P...TC
     83 3.070328463                       LGInnote_89:87:90 (… 802.11    52 Acknowledgement, Flags=........C
     84 3.073931885  D-LinkIn_36:40:85    Broadcast            802.11   375 Beacon frame, SN=3789, FN=0, Flags=........C, BI=100, SSID=D-Link-364082
     85 3.175218797  D-LinkIn_36:40:85    Broadcast            802.11   375 Beacon frame, SN=3790, FN=0, Flags=........C, BI=100, SSID=D-Link-364082
     86 3.278225562  D-LinkIn_36:40:85    Broadcast            802.11   375 Beacon frame, SN=3791, FN=0, Flags=........C, BI=100, SSID=D-Link-364082
     87 3.379358967  D-LinkIn_36:40:85    Broadcast            802.11   375 Beacon frame, SN=3792, FN=0, Flags=........C, BI=100, SSID=D-Link-364082
     88 3.417090325  02:bb:1d:3d:cd:d8    Broadcast            802.11   207 Probe Request, SN=163, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
     89 3.417381743  D-LinkIn_36:40:85    02:bb:1d:3d:cd:d8    802.11   480 Probe Response, SN=3793, FN=0, Flags=........C, BI=100, SSID=D-Link-364082
     90 3.417387221                       D-LinkIn_c9:19:28 (… 802.11    52 Acknowledgement, Flags=........C
     91 3.421721321  D-LinkIn_36:40:85    02:bb:1d:3d:cd:d8    802.11   480 Probe Response, SN=3793, FN=0, Flags=....R...C, BI=100, SSID=D-Link-364082
     92 3.421736833  D-LinkIn_36:40:85    02:bb:1d:3d:cd:d8    802.11   480 Probe Response, SN=3793, FN=0, Flags=....R...C, BI=100, SSID=D-Link-364082
     93 3.421741597                       D-LinkIn_36:40:85 (… 802.11    52 Acknowledgement, Flags=........C
     94 3.421745605                       22:b0:01:e2:f1:b9 (… 802.11    52 Acknowledgement, Flags=........C
     95 3.469969168  02:bb:1d:3d:cd:d8    Broadcast            802.11   207 Probe Request, SN=165, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
     96 3.469989088  D-LinkIn_36:40:85    02:bb:1d:3d:cd:d8    802.11   480 Probe Response, SN=3794, FN=0, Flags=........C, BI=100, SSID=D-Link-364082
     97 3.473467578  D-LinkIn_36:40:85    02:bb:1d:3d:cd:d8    802.11   480 Probe Response, SN=3794, FN=0, Flags=....R...C, BI=100, SSID=D-Link-364082
     98 3.473479456  D-LinkIn_36:40:85    02:bb:1d:3d:cd:d8    802.11   480 Probe Response, SN=3794, FN=0, Flags=....R...C, BI=100, SSID=D-Link-364082
     99 3.473484351  D-LinkIn_36:40:85    02:bb:1d:3d:cd:d8    802.11   480 Probe Response, SN=3794, FN=0, Flags=....R...C, BI=100, SSID=D-Link-364082
    100 3.473489263  D-LinkIn_36:40:85    02:bb:1d:3d:cd:d8    802.11   480 Probe Response, SN=3794, FN=0, Flags=....R...C, BI=100, SSID=D-Link-364082
    101 3.481769944  D-LinkIn_36:40:85    Broadcast            802.11   375 Beacon frame, SN=3795, FN=0, Flags=........C, BI=100, SSID=D-Link-364082
› Frame 1: 375 bytes on wire (3000 bits), 375 bytes captured (3000 bits) on interface wlo1mon, id 0
› Radiotap Header v0, Length 38
› 802.11 radio information
› IEEE 802.11 Beacon frame, Flags: ........C
› IEEE 802.11 Wireless Management
0000  00 00 26 00 2f 40 00 a0  20 08 00 a0 20 08 00 00   ··&·/@··  ··· ···
0010  67 5c b9 10 00 00 00 00  10 0c 8c 14 40 01 c3 00   g\······  ····@···
0020  00 00 c3 00 bf 01 80 00  00 00 ff ff ff ff ff ff   ········  ········
0030  0c b6 d2 36 40 85 0c b6  d2 36 40 85 e0 ea 4e 90   ···6@···  6@···N·
0040  63 11 00 00 00 00 64 00  11 01 00 0d 44 2d 4c 69   c·····d·  ····D-Li
WiresharkMon_group5.pcapng          Packets: 13576 · Displayed: 13576 (100.0%)          Profile: Default
```

Figure 8: Wireshark in monitor mode

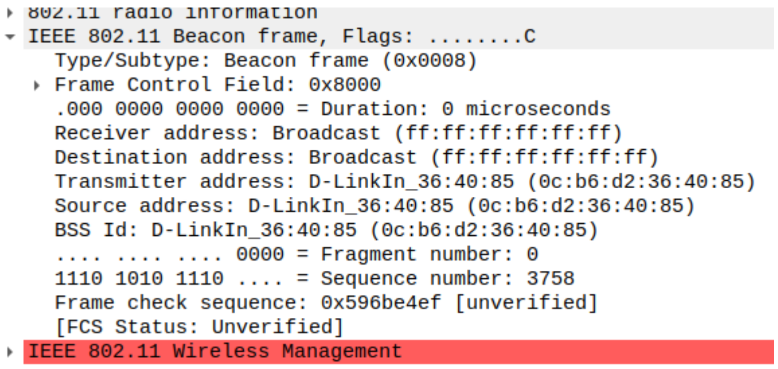

Wireshark · Coloring Rules Default

	Name	Filter
✓	CTS	wlan.fc.type_subtype == 0x1C
✓	RTS	wlan.fc.type_subtype == 0x1B
✓	ACK	wlan.fc.type_subtype == 0x1D
✓	Beacon	wlan.fc.type_subtype == 0x0008
✓	Probe Response	wlan.fc.type_subtype == 0x0005
✓	Probe Request	wlan.fc.type_subtype == 0x0004
✓	Specific Destination Adress	wlan.da == a2:b6:ad:54:88:a8
✓	Specific Source Adress	wlan.sa == a2:b6:ad:54:88:a8
✓	Data Frames	wlan.fc.type == 2
✓	ICMP Echo Reply	icmp.type == 0
✓	ICMP Echo Request	icmp.type == 8
	Control Frames	wlan.fc.type == 1
	Management Frames	wlan.fc.type == 0

Figure 9: Wireshark Coloring Rules

As shown in Figure 8, when analyzing the `WiresharkMon_group5.pcapng` file captured in monitor mode, we were able to see the ping request and reply messages as IEEE 802.11 data frames. Unlike the previous capture, this one includes the complete Layer 2 headers, showing MAC addresses, frame control fields, and sequence numbers. We also observed Wi-Fi management frames (like probe requests and beacons) and control frames (such as ACKs), which were not visible when monitor mode was not enabled.

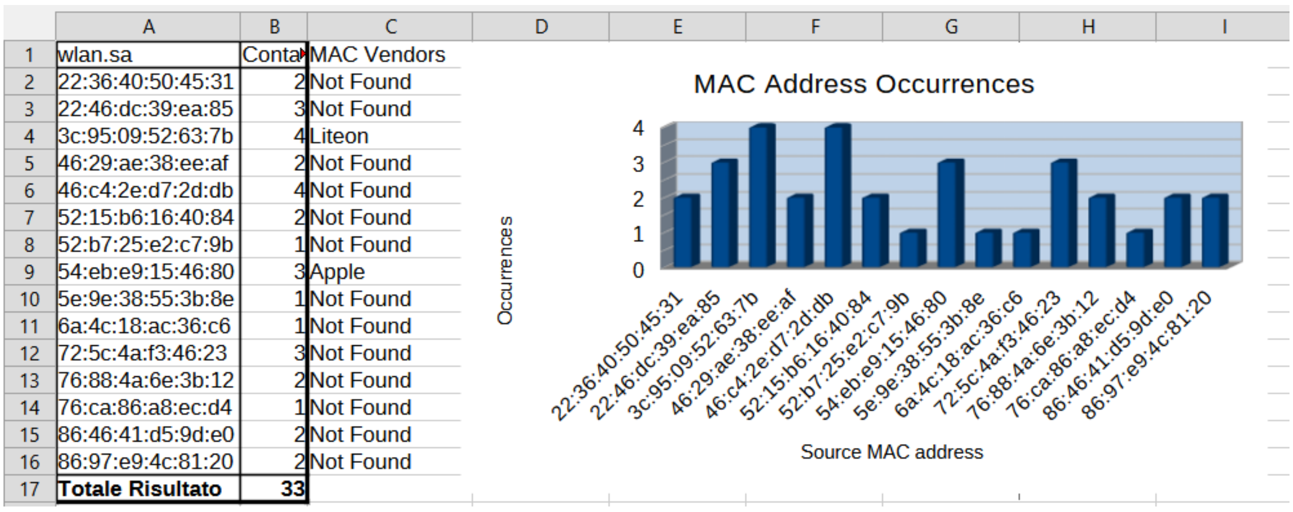
To better analyze the traffic, we added coloring rules in Wireshark to highlight specific types of packets. This helped us identify different conversations more easily. Figure 9 shows the capture with the coloring rules applied, along with the filters we used.



```
▸ 802.11 radio information
▾ IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  ▸ Frame Control Field: 0x8000
    .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: D-LinkIn_36:40:85 (0c:b6:d2:36:40:85)
    Source address: D-LinkIn_36:40:85 (0c:b6:d2:36:40:85)
    BSS Id: D-LinkIn_36:40:85 (0c:b6:d2:36:40:85)
    .... .... .... 0000 = Fragment number: 0
    1110 1010 1110 .... = Sequence number: 3758
    Frame check sequence: 0x596be4ef [unverified]
    [FCS Status: Unverified]
▸ IEEE 802.11 Wireless Management
```

Figure 10: IEEE 802.11 Beacon Frame

Figure 10 shows the detailed view of a beacon frame captured in monitor mode. By expanding the IEEE 802.11 protocol section in Wireshark, it is possible to inspect several fields such as the SSID, supported rates, and capabilities of the access point. This level of detail is only available thanks to the 802.11 headers provided in monitor mode.

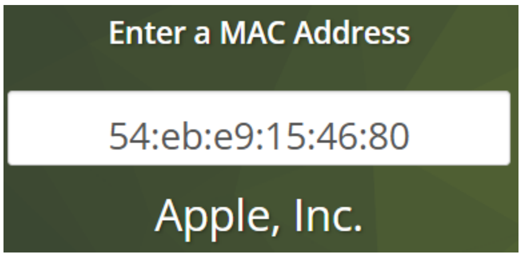


	A	B	C
1	wlan.sa	Conta	MAC Vendors
2	22:36:40:50:45:31	2	Not Found
3	22:46:dc:39:ea:85	3	Not Found
4	3c:95:09:52:63:7b	4	Liteon
5	46:29:ae:38:ee:af	2	Not Found
6	46:c4:2e:d7:2d:db	4	Not Found
7	52:15:b6:16:40:84	2	Not Found
8	52:b7:25:e2:c7:9b	1	Not Found
9	54:eb:e9:15:46:80	3	Apple
10	5e:9e:38:55:3b:8e	1	Not Found
11	6a:4c:18:ac:36:c6	1	Not Found
12	72:5c:4a:f3:46:23	3	Not Found
13	76:88:4a:6e:3b:12	2	Not Found
14	76:ca:86:a8:ec:d4	1	Not Found
15	86:46:41:d5:9d:e0	2	Not Found
16	86:97:e9:4c:81:20	2	Not Found
17	**Totale Risultato**	**33**	

Figure 11: Histogram of the occurrences of the source addresses

After converting the capture file to a readable `.txt` format, we observed several IEEE 802.11 probe request frames. These packets are sent by wireless devices (e.g., smartphones, laptops) when actively scanning for nearby Wi-Fi networks. They are directed to the broadcast address `ff:ff:ff:ff:ff:ff`, meaning no specific access point is targeted.

To better understand which devices were most active, we generated a histogram of MAC address occurrences. As part of the analysis, we also verified the manufacturer of some addresses, like the one shown here, which belongs to Apple Inc.



Enter a MAC Address

54:eb:e9:15:46:80

Apple, Inc.

Figure 12: MAC address associated with Apple Inc.