POLITECNICO
MILANO 1863

Wireless Internet Project

Characterizing MAC Randomization Behavior of iPhone 15 pro max and Xiaomi 11t pro Devices in Wi-Fi Probe Requests

Mostafa Hashemiyan – 10946135

Hamed Lotfalizadeh – 10946486

Abstract

This report analyzes the MAC randomization behavior in Wi-Fi probe requests of the iPhone 15 Pro Max and Xiaomi 11T Pro 5G devices. Using a sniffer in monitor mode and Wireshark, we captured and examined probe request packets under various device states and on different days. Through a thorough sniffing and filtering procedure, we explored the patterns and variations in MAC randomization for both devices. The findings offer valuable insights into the privacy protection mechanisms employed by these devices during Wi-Fi connections.

1. Introduction

In the context of Wi-Fi connections, stations send probe requests to access points (APs) for network discovery and establishment. These probe requests generally include unencrypted information, such as a randomized Media Access Control (MAC) address, to protect user privacy. Understanding the MAC randomization behavior of devices is crucial for evaluating their effectiveness in safeguarding user identities. This report aims to characterize the MAC randomization behavior of iPhone 15 Pro Max and Xiaomi 11T Pro 5G devices through an analysis of their Wi-Fi probe requests.

2. Sniffing Procedure

The study involved the following steps to capture and analyze the Wi-Fi probe requests:

a. Experimental Setup

- The sniffing process was performed using a MacBook Air laptop in monitor mode, alongside Wireshark, a network protocol analyzer, in a controlled environment.

- The mobile device models, iPhone 15 ProMax and Xiaomi 11t pro 5G, were selected for the analysis.

- The sniffing was conducted over two different days to ensure the capture of randomized MAC addresses.

- The sniffing was performed on three channels: 1, 2, and 3.

- To ensure sufficient proximity between the access point and station, the phone roles were interchangeably assigned. One phone functioned as an access point while the other operated as a station, and vice versa, during the sniffing process.

- The mobile device under investigation was positioned approximately 20 cm away from the access point.

b. Device States and Sniffing Duration

To evaluate the MAC randomization behavior under different scenarios, the devices were tested in six distinct states, denoted as A, S, WA, WS, PA, and PS.

- Mode A: Wi-Fi interface and screen were turned on.

- Mode S: Wi-Fi interface was on, but the screen was off.

- Mode WA: Wi-Fi interface was off, but the screen was on.

- Mode WS: Both Wi-Fi interface and screen were off.

- Mode PA: Power mode was on, Wi-Fi interface was on, and the screen was on.

- Mode PS: Power mode was on, Wi-Fi interface was on, and the screen was off.

Sniffing was performed for 20 minutes in each mode on two different days to capture an adequate amount of probe request data.

3. Filtering Procedure

To focus on probe requests and isolate them from other network traffic, the captured packets were filtered as follows:

a. Probe Request Identification

- The following filter was applied to identify packets specifically related to probe requests: (wlan.fc.type_subtype == 0x0004).

- This filtering process helped exclude irrelevant packets and concentrate solely on the probe requests emitted by the devices.

b. Received Signal Strength Indicator (RSSI) Filtering

The RSSI values of the probe requests were leveraged to differentiate devices in close proximity to the sniffer from others.

- A threshold of -55 dBm was set to filter out probe requests from devices within a 20 cm range using the following filter: (wlan_radio.signal_dbm >= -55).

- This RSSI-based filtering allowed us to focus on the probe requests emitted by the iPhone 15 pro max and Xiaomi 11t pro devices under investigation.

4. Analysis

The analysis of MAC randomization behavior in Wi-Fi probe requests yielded the following insights for iPhone 15 pro max and Xiaomi 11t pro devices. The results are also available in Fig.1. Besides, Table 1 shows the original and the randomized MAC addresses after the filtering

Phone model	Original MAC addresses	Randomized MAC addresses
iPhone 15 pro max	A0:52:72:1d:e2:bf	be:3c:53:70:c3:6d 96:20:1c:a3:ce:57
Xiaomi 11t pro	8c:7a:3d:b5:70:22	9e:c5:28:5e:fc:de

Table. 1 The original and randomized MAC addresses per each phone

The following reasons highlight how the different modes and their corresponding device states (Wi-Fi interface, screen, power-saving) directly impact the generation and frequency of probe requests.

Mode A: The high number of probe requests in this mode is due to both the Wi-Fi interface and screen being turned on. When the screen is active, the device frequently searches for available networks and sends out probe requests to discover nearby access points or reconnect to previously connected networks.

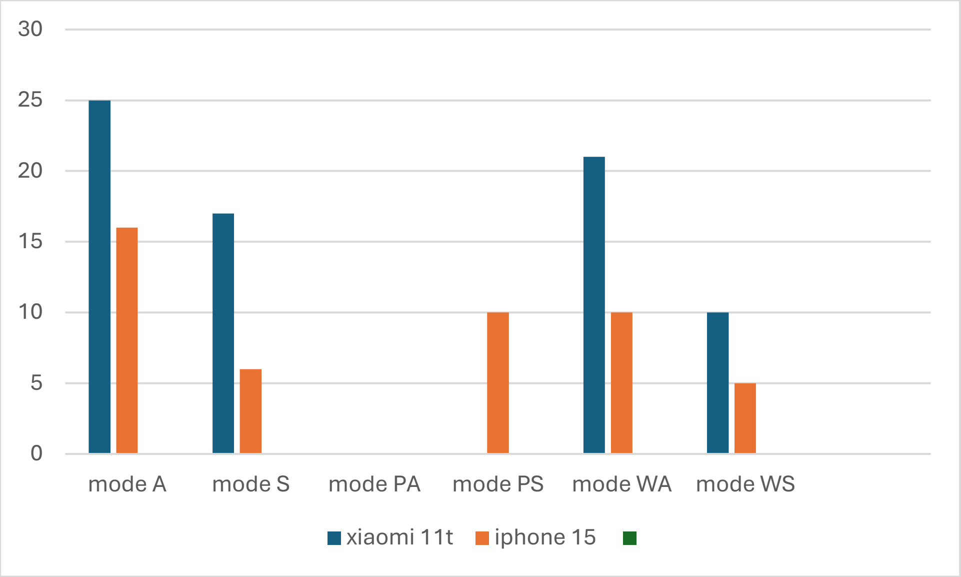
Mode S: The reduced number of probe requests in this mode is due to the screen being off. While the Wi-Fi interface remains on, the lower screen activity likely means less user interaction, resulting in fewer probe requests.

Mode WA: With the Wi-Fi interface turned off, the device cannot send or receive probe requests. Consequently, no probe requests were observed in this mode.

Mode WS: In this mode, both the Wi-Fi interface and screen are turned off, so no probe requests are generated, as the device is not actively searching for or connected to any Wi-Fi networks.

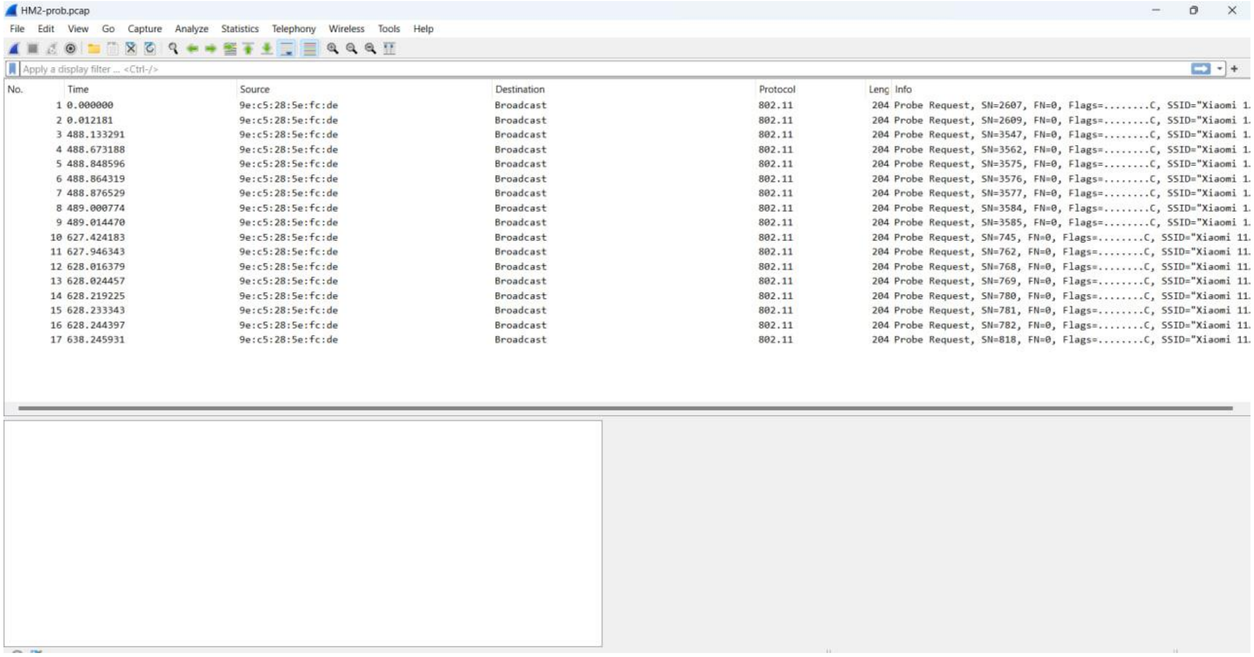
Mode PA: The higher number of probe requests in this mode can be attributed to the combination of the Wi-Fi interface, screen, and power-saving features being active.

Mode PS: In this mode, the screen is off, indicating reduced user interaction. However, the Wi-Fi interface is still on, and power-saving features are active. The decrease in probe requests compared to other modes is due to the device being in a power-saving state with reduced overall network activity. Additionally, the inactive screen further contributes to the reduction in probe requests.



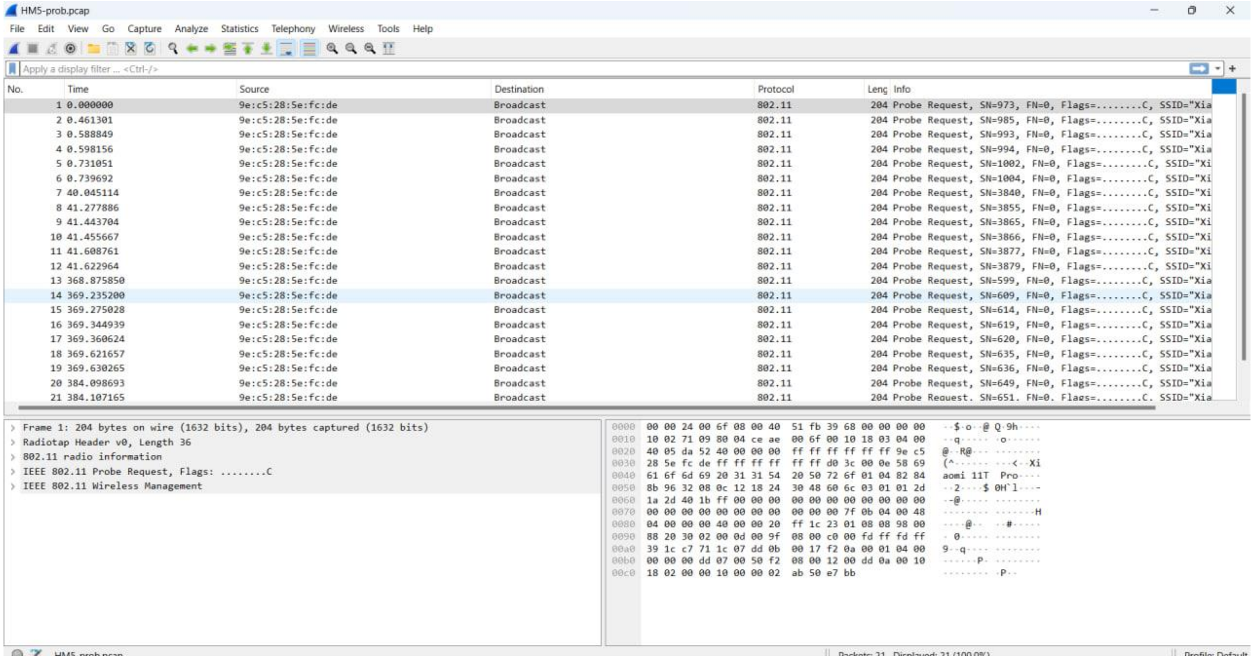
5. Conclusion

This report characterizes the MAC randomization behavior in Wi-Fi probe requests for iPhone 15 pro max and Xiaomi 11t pro 5G devices. Sniffing was conducted for both devices in an isolated room over two different days. The analysis revealed variations in MAC randomization activity based on different device states. When both the Wi-Fi interface and screen are on, probe requests are at their highest. With the screen off, the number of probe requests decreases. When the Wi-Fi interface is off, no probe requests are observed. The power-saving feature reduces network activity and the number of probe requests. Therefore, in power-saving mode with the screen off, the number of probe requests is at its lowest. These findings enhance our understanding of the impact of device states and power-saving features on probe request behavior. They also provide insights into the privacy protection measures employed by these devices during Wi-Fi connections, particularly highlighting the effectiveness of MAC randomization in enhancing user privacy.



```
No.  Time        Source              Destination   Protocol  Leng Info
   1 0.000000    9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=2607, FN=0, Flags=........C, SSID="Xiaomi 1.
   2 0.012181    9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=2609, FN=0, Flags=........C, SSID="Xiaomi 1.
   3 488.133291  9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=3547, FN=0, Flags=........C, SSID="Xiaomi 1.
   4 488.673188  9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=3562, FN=0, Flags=........C, SSID="Xiaomi 1.
   5 488.848596  9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=3575, FN=0, Flags=........C, SSID="Xiaomi 1.
   6 488.864319  9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=3576, FN=0, Flags=........C, SSID="Xiaomi 1.
   7 488.876529  9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=3577, FN=0, Flags=........C, SSID="Xiaomi 1.
   8 489.000774  9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=3584, FN=0, Flags=........C, SSID="Xiaomi 1.
   9 489.014470  9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=3585, FN=0, Flags=........C, SSID="Xiaomi 1.
  10 627.424183  9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=745, FN=0, Flags=........C, SSID="Xiaomi 11.
  11 627.946343  9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=762, FN=0, Flags=........C, SSID="Xiaomi 11.
  12 628.016379  9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=768, FN=0, Flags=........C, SSID="Xiaomi 11.
  13 628.024457  9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=769, FN=0, Flags=........C, SSID="Xiaomi 11.
  14 628.219225  9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=780, FN=0, Flags=........C, SSID="Xiaomi 11.
  15 628.233343  9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=781, FN=0, Flags=........C, SSID="Xiaomi 11.
  16 628.244397  9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=782, FN=0, Flags=........C, SSID="Xiaomi 11.
  17 638.245931  9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=818, FN=0, Flags=........C, SSID="Xiaomi 11.
```

mode s : wifi interference on , screen off , AP : xiaomi 11t pro , staion : IPhone 15 pro

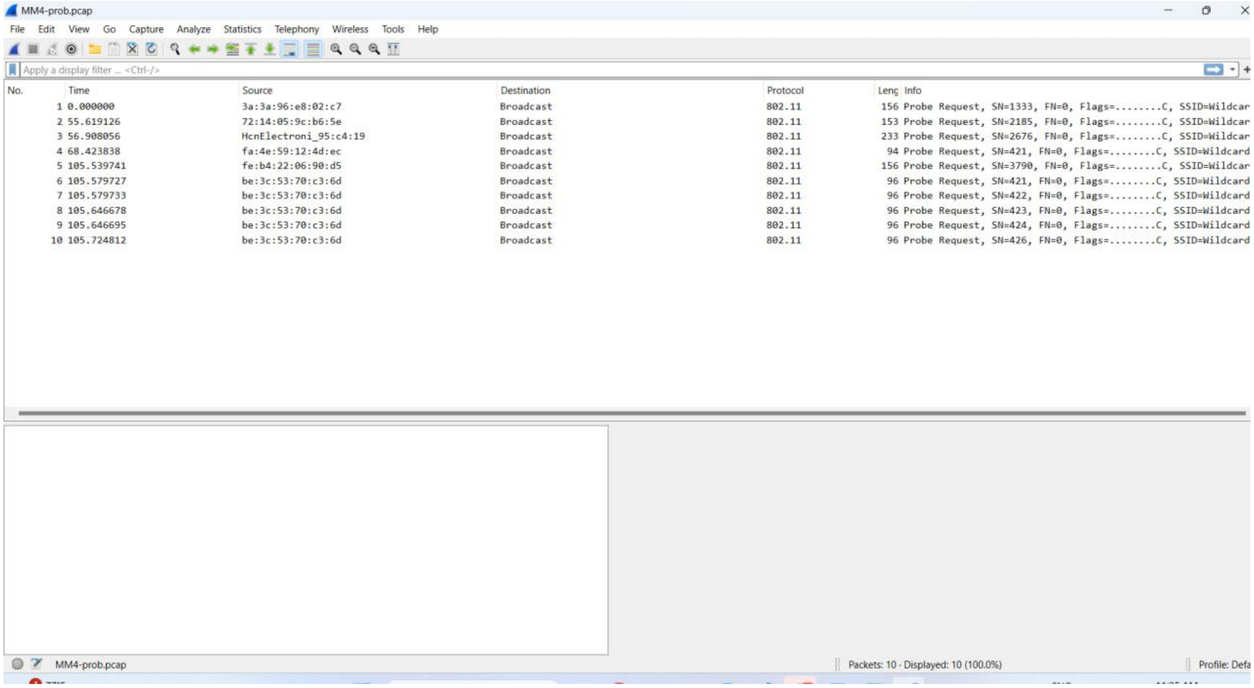


```
No.  Time        Source              Destination   Protocol  Leng Info
   1 0.000000    9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=973, FN=0, Flags=........C, SSID="Xia
   2 0.461301    9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=985, FN=0, Flags=........C, SSID="Xia
   3 0.588849    9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=993, FN=0, Flags=........C, SSID="Xia
   4 0.598156    9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=994, FN=0, Flags=........C, SSID="Xia
   5 0.731051    9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=1002, FN=0, Flags=........C, SSID="Xi
   6 0.739692    9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=1004, FN=0, Flags=........C, SSID="Xi
   7 40.045114   9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=3840, FN=0, Flags=........C, SSID="Xi
   8 41.277886   9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=3855, FN=0, Flags=........C, SSID="Xi
   9 41.443704   9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=3865, FN=0, Flags=........C, SSID="Xi
  10 41.455667   9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=3866, FN=0, Flags=........C, SSID="Xi
  11 41.608761   9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=3877, FN=0, Flags=........C, SSID="Xi
  12 41.622964   9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=3879, FN=0, Flags=........C, SSID="Xi
  13 368.875850  9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=599, FN=0, Flags=........C, SSID="Xia
  14 369.235200  9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=609, FN=0, Flags=........C, SSID="Xia
  15 369.275028  9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=614, FN=0, Flags=........C, SSID="Xia
  16 369.344939  9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=619, FN=0, Flags=........C, SSID="Xia
  17 369.360624  9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=620, FN=0, Flags=........C, SSID="Xia
  18 369.621657  9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=635, FN=0, Flags=........C, SSID="Xia
  19 369.630265  9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=636, FN=0, Flags=........C, SSID="Xia
  20 384.098693  9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request, SN=649, FN=0, Flags=........C, SSID="Xia
  21 384.107165  9e:c5:28:5e:fc:de   Broadcast     802.11    204 Probe Request. SN=651. FN=0. Flags=........C. SSID="Xia
```

```
> Frame 1: 204 bytes on wire (1632 bits), 204 bytes captured (1632 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 Probe Request, Flags: ........C
> IEEE 802.11 Wireless Management
```

```
0000  00 00 24 00 6f 08 00 40  51 fb 39 68 00 00 00 00   ··$·o··@ Q·9h····
0010  10 02 71 09 80 04 ce ae  00 6f 00 10 18 03 04 00   ··q····· ·o······
0020  40 05 da 52 40 00 00 00  ff ff ff ff ff ff 9e c5   @··R@··· ········
0030  28 5e fc de ff ff ff ff  ff ff d0 3c 00 0e 58 69   (^······ ···<··Xi
0040  61 6f 6d 69 20 31 31 54  20 50 72 6f 01 04 82 84   aomi 11T  Pro····
0050  8b 96 32 08 0c 12 18 24  30 48 60 6c 03 01 01 2d   ··2····$ 0H`l···-
0060  1a 2d 40 1b ff 00 00 00  00 00 00 00 00 00 00 00   ·-@····· ········
0070  00 00 00 00 00 00 00 00  00 00 00 7f 0b 04 00 48   ········ ·······H
0080  04 00 00 00 40 00 00 20  ff 1c 23 01 08 08 98 00   ····@··  ··#·····
0090  88 20 30 02 00 0d 00 9f  08 00 c0 00 fd ff fd ff   · 0····· ········
00a0  39 1c c7 71 1c 07 dd 0b  00 17 f2 0a 00 01 04 00   9··q···· ········
00b0  00 00 00 dd 07 00 50 f2  08 00 12 00 dd 0a 00 10   ······P· ········
00c0  18 02 00 00 10 00 00 02  ab 50 e7 bb               ········ ·P··
```

mode wa : , power mode on wifi interference on , screen off , AP : xiaomi 11t pro , staion : IPhone 15 pro



MM4-prob.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time        Source                 Destination   Protocol   Leng Info
    1 0.000000    3a:3a:96:e8:02:c7      Broadcast     802.11      156 Probe Request, SN=1333, FN=0, Flags=........C, SSID=Wildcar
    2 55.619126   72:14:05:9c:b6:5e      Broadcast     802.11      153 Probe Request, SN=2185, FN=0, Flags=........C, SSID=Wildcar
    3 56.908056   HcnElectroni_95:c4:19  Broadcast     802.11      233 Probe Request, SN=2676, FN=0, Flags=........C, SSID=Wildcar
    4 68.423838   fa:4e:59:12:4d:ec      Broadcast     802.11       94 Probe Request, SN=421, FN=0, Flags=........C, SSID=Wildcard
    5 105.539741  fe:b4:22:06:90:d5      Broadcast     802.11      156 Probe Request, SN=3790, FN=0, Flags=........C, SSID=Wildcar
    6 105.579727  be:3c:53:70:c3:6d      Broadcast     802.11       96 Probe Request, SN=421, FN=0, Flags=........C, SSID=Wildcard
    7 105.579733  be:3c:53:70:c3:6d      Broadcast     802.11       96 Probe Request, SN=422, FN=0, Flags=........C, SSID=Wildcard
    8 105.646678  be:3c:53:70:c3:6d      Broadcast     802.11       96 Probe Request, SN=423, FN=0, Flags=........C, SSID=Wildcard
    9 105.646695  be:3c:53:70:c3:6d      Broadcast     802.11       96 Probe Request, SN=424, FN=0, Flags=........C, SSID=Wildcard
   10 105.724812  be:3c:53:70:c3:6d      Broadcast     802.11       96 Probe Request, SN=426, FN=0, Flags=........C, SSID=Wildcard
```

mode wa : , power mode on wifi interference on , screen on , station : xiaomi 11t pro , AP : IPhone 15 pro