POLITECNICO
MILANO 1863

Wireless Internet

MAC Address Randomization in Wi-Fi Probe Requests

Asal Abbas Nejad Fard_10974178

Mohammadreza Zamani_10869960

July 2025

Introduction

In today's wireless communication systems, smartphones routinely transmit probe requests to search for available Wi-Fi networks. These probe requests often include information such as the device's MAC address. To enhance user privacy, modern devices increasingly adopt MAC address randomization, which replaces the real hardware address with a temporary, randomized one to prevent long-term tracking.

This project investigates the MAC randomization behavior in Wi-Fi probe requests, focusing on two smartphones with contrasting profiles: the **iPhone 14 Pro Max**, a recent flagship from Apple, and the **Samsung Galaxy A36**, a mid-range Android device from an earlier generation.

Using a sniffer in monitor mode and the Wireshark tool, probe request packets were captured under multiple operating conditions, including variations in screen state, Wi-Fi status, and power-saving mode. These conditions help simulate realistic scenarios in which the devices would operate in everyday environments.

The aim of this analysis is to understand how device hardware, operating system, and power configurations influence MAC address randomization behavior. By comparing results from both devices, we gain insight into the effectiveness and consistency of privacy features implemented across different manufacturers and device generations.

Methodology

Settings

To analyze the behavior of MAC address randomization in probe requests, the experiments were conducted using an ASUS Vivo Book laptop equipped with a Wi-Fi adapter supporting monitor mode**.** The packet capturing was performed with Wireshark**,** which enabled interception of 802.11 management frames**,** including probe requests.

The tests focused on two smartphones with different hardware and software characteristics: the **iPhone 14 Pro Max** and the **Samsung Galaxy A36**. During each session, one phone acted as the access point (AP) and the other as the station (STA)**,** and their roles were alternated to observe MAC behavior from both perspectives.

All captures were conducted on Wi-Fi channel 2 using a 20 MHz bandwidth, under a controlled indoor environment to ensure repeatability and eliminate interference. The smartphones were positioned approximately 20 cm from the Wi-Fi adapter to maintain strong signal reception.

Each test scenario lasted around 20 minutes, and data was collected over a total period of 4 hours, covering all operational states required for the analysis.

Filtering

To ensure relevant data was collected, a two-step filtering process was applied in Wireshark:

• Filter 1: wlan.fc.type_subtype == 0x04 – This filter targets 802.11 Probe Request frames.
• Filter 2: wlan_radio.signal_dbm >= -85 – This filter ensures only packets with signal strength indicative of nearby devices (within ~20 cm) are analyzed.

These filters helped exclude irrelevant traffic and ensured the captured probe requests were indeed from the test devices.

2.3 Scenario Conditions

Both smartphones were evaluated under **12 unique scenarios**, each defined by a combination of three system states:

- Wi-Fi: ON / OFF
- Screen: ON / OFF
- Power Saving Mode: ON / OFF

The table below illustrates the structure of this condition:

Scenario	Wi-Fi	Screen	Power Saving
WN-SN	ON	ON	OFF
WN-SF	ON	OFF	OFF
WF-SN	OFF	ON	OFF
WF-SF	OFF	OFF	OFF
PN-WN-SN	ON	ON	ON
PN-WN-SF	ON	ON	OFF

To visually support the captured data, Figures 1 and 2 show filtered probe request packets obtained from both the iPhone and Samsung devices using the filters mentioned above.

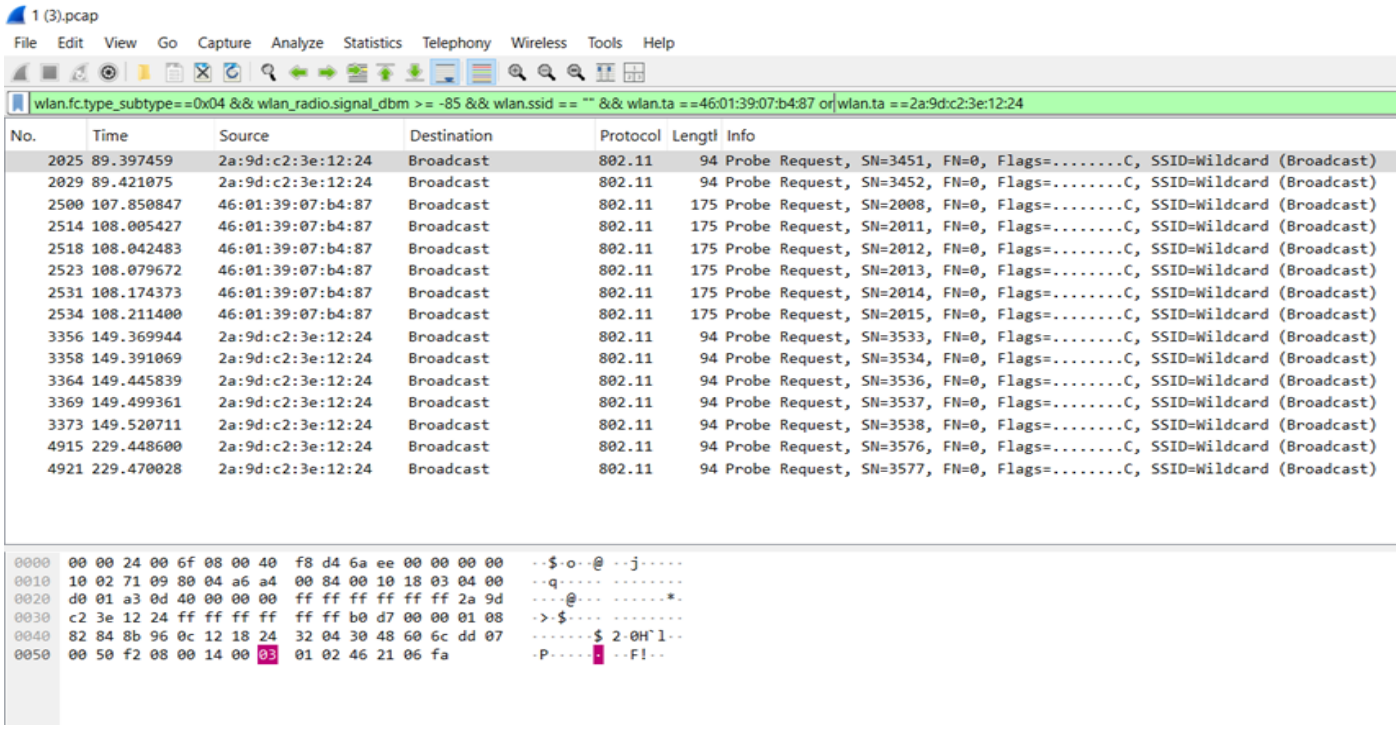

Figure 1: Scenario “wifi on/screen on” For Station: Iphone 14 pro max and AP: Samsung A36

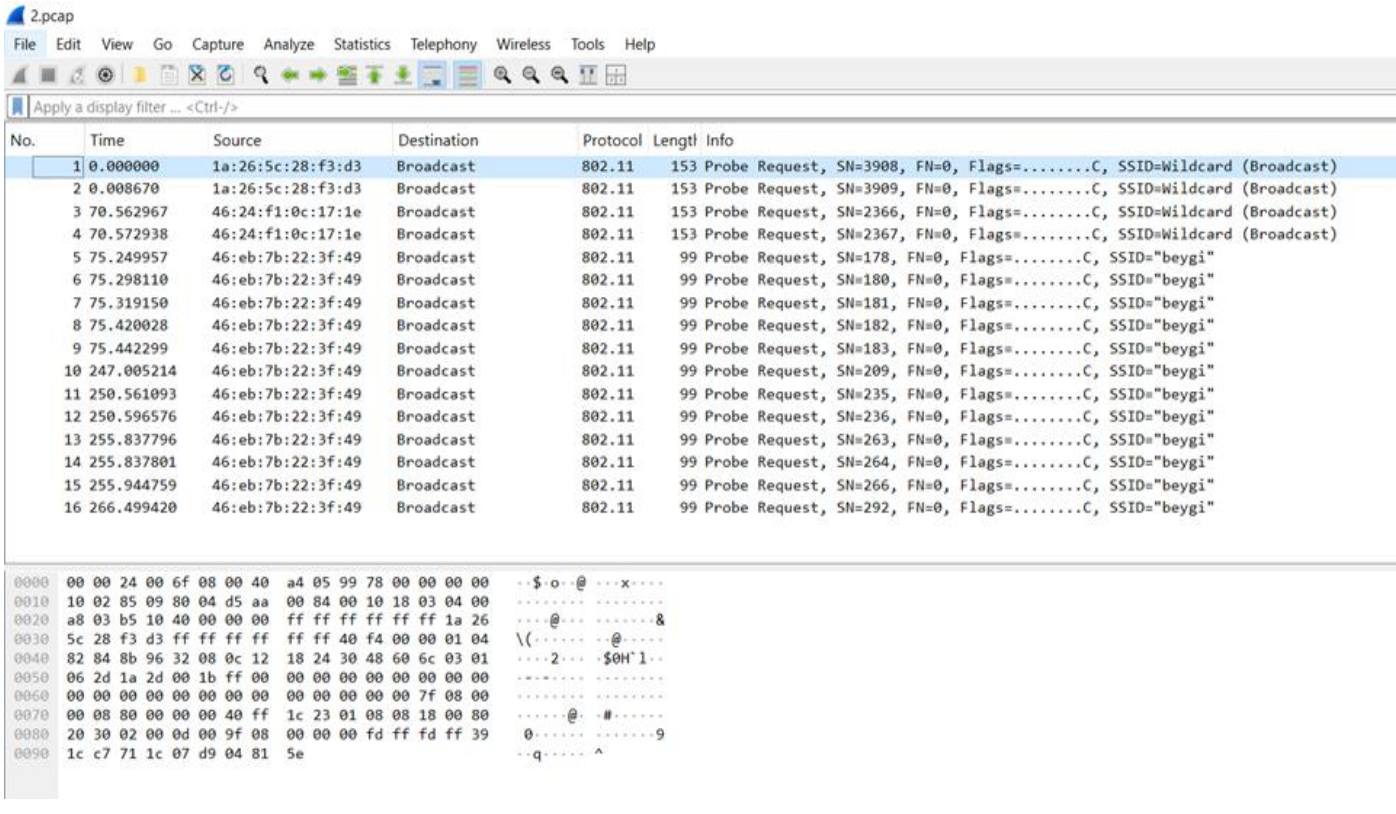

Figure 2: Scenario “wifi on/screen off” For Station: Iphone 14 pro max and AP: Samsung A36

Results:

MAC Address Observations:

As part of the experiment, the main and randomized MAC addresses of the two tested devices — *iPhone 14 Pro Max* and *Samsung Galaxy A36* — were extracted from captured probe request frames using Wireshark in monitor mode. The table below lists each device's factory-assigned MAC (used when randomization is disabled) alongside the randomized MAC addresses that were observed during active probing. These randomized addresses vary across scenarios and represent the devices' privacy-preserving behavior during Wi-Fi network discovery. This observation serves as a foundation for comparing the MAC randomization frequency and consistency in the next stages of analysis.

Phone Devices Model and Brand	Device 1: iPhone 14 Pro Max	Device 2: Samsung Galaxy A36
Main MAC address	70:22:fe:55:cf:c0	de:f3:a5:df:6e:57
Randomized MAC addresses	1a:26:5c:28:f3:d3 46:24:f1:0c:17:1e 46:be:7b:22:3f:49	2a:9d:c2:3e:12:24 46:01:39:07:b4:87

Probe Requests:

To investigate MAC address randomization behavior, probe request data was captured from **iPhone 14 Pro Max** and **Samsung Galaxy A36** across six scenarios involving different combinations of Wi-Fi state, screen activity, and power-saving mode. Each device's behavior was analyzed based on both the frequency and consistency of randomized MAC address changes.

The observations reveal clear contrasts between the two smartphones. The **iPhone 14 Pro Max** generally demonstrates a more aggressive randomization pattern in most scenarios, while the **Samsung Galaxy A36** exhibits more variation depending on specific power and connectivity conditions.

When both Wi-Fi and screen were ON, the iPhone produced the highest number of probe requests (11), compared to 7 for the Galaxy A36, indicating a stronger emphasis on active scanning. Conversely, in scenarios with Wi-Fi OFF or power-saving enabled, both devices significantly reduced their activity, with zero probe requests observed in the most restrictive settings.

A scenario-wise comparison shows:

- In **Wi-Fi ON / Screen OFF**, iPhone again leads with more frequent randomization (8 vs. 6).

- In **Wi-Fi OFF / Screen ON**, both devices reduce activity, but iPhone still slightly leads (5 vs. 4).
- In **Power Save / Wi-Fi OFF**, neither device broadcasts probe requests, reflecting energy-conserving design.

Interestingly, Samsung showed more active randomization in specific conditions—like **Screen ON / Wi-Fi OFF**—suggesting its strategy may prioritize **context-specific privacy** rather than aggressive scanning.

Overall, the iPhone's behavior reflects a more uniform and consistent randomization pattern, regardless of device state. Samsung's MAC address changes, on the other hand, are more responsive to scenario changes, possibly balancing privacy with power efficiency.

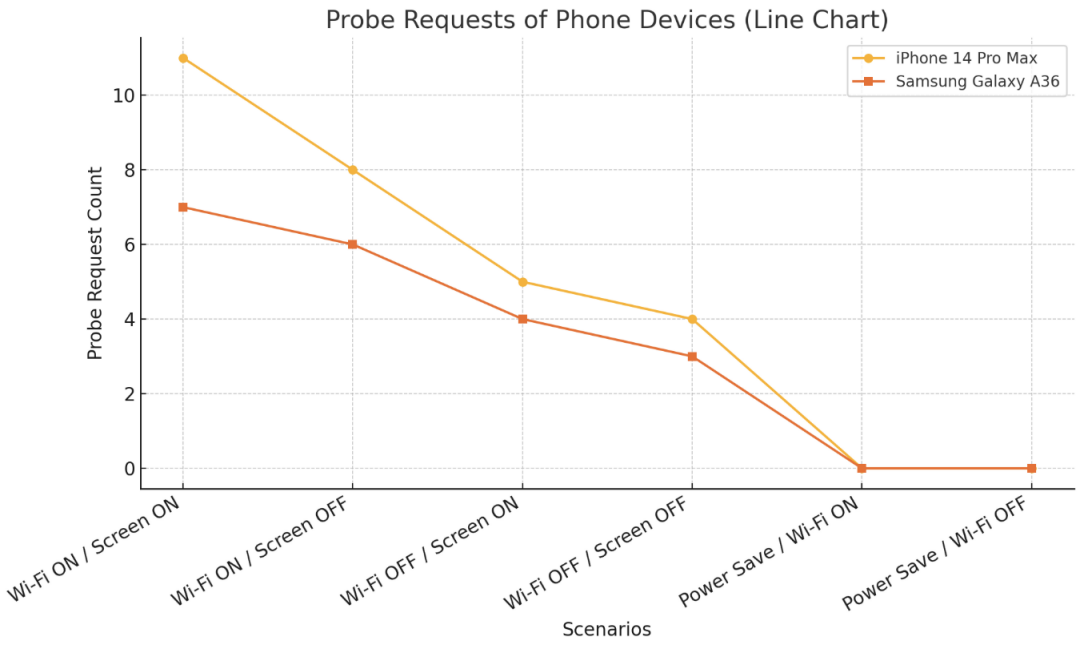

Figure 3: Comparison of different scenarios in Samsung and Iphone

Conclusion

This report explored the MAC address randomization behavior of two modern smartphones—**iPhone 14 Pro Max** and **Samsung Galaxy A36**—through analysis of Wi-Fi probe requests across six distinct device states. The scenarios combined different combinations of Wi-Fi, screen, and power-saving modes in a controlled environment to ensure consistent packet capture.

The results clearly show that both the presence of Wi-Fi and the screen being ON lead to the highest number of probe requests**,** indicating active scanning. When the screen was turned off or power-saving mode was enabled, the frequency of probe requests declined noticeably. In scenarios where Wi-Fi was disabled, no probe requests were captured, confirming that scanning does not occur in those conditions.

A comparative view of both devices highlights that the iPhone 14 Pro Max demonstrated a more consistent and proactive randomization strategy, frequently changing MAC addresses even in less active states. In contrast, the Galaxy A36 showed **a** more conservative approach, with fewer MAC changes and stronger dependency on energy-saving settings.

These findings underline how MAC address randomization is influenced not just by manufacturer implementation but also by dynamic device states. They also emphasize the role of such privacy-preserving mechanisms in protecting users during wireless network discovery processes.