# WiFi Security: Evil Twin & Deauthentication Simulation (ESP32)

This project demonstrates two common WiFi vulnerabilities — \*\*deauthentication attacks\*\* and \*\*Evil Twin access points\*\* — using an ESP32 NodeMCU.

It is based on the open-source [PhiSiFi](https://github.com/p3tr0s/PhiSiFi) project, with my own modifications, documentation, and testing setup.

⚠️ \*\*Disclaimer:\*\* This project is for educational and research purposes only. Do \*\*not\*\* use it on networks you do not own or have explicit permission to test.

---

## 📌 Features

- 🔍 Scan nearby WiFi networks

- 🎭 Launch Evil Twin with cloned SSID

- 🌐 Captive portal login page for credential capture

- 📡 Deauthentication attack to force reconnections

- 📝 Logging of captured credentials/attempts

---

## 🛠 Hardware & Tools

- ESP32 NodeMCU

- Arduino IDE / PlatformIO

- USB cable + laptop

- Libraries: `WiFi`, `WebServer`, `DNSServer`

---

## 🚀 Implementation

1. ESP32 scans available SSIDs.

2. Creates a fake AP (Evil Twin) with the same SSID.

3. Deauth packets are sent to disconnect victims.

4. Victim reconnects to the fake AP.

5. Captive portal appears and logs login attempts.

---

## 📷 Results

Tested on a private WiFi lab network.

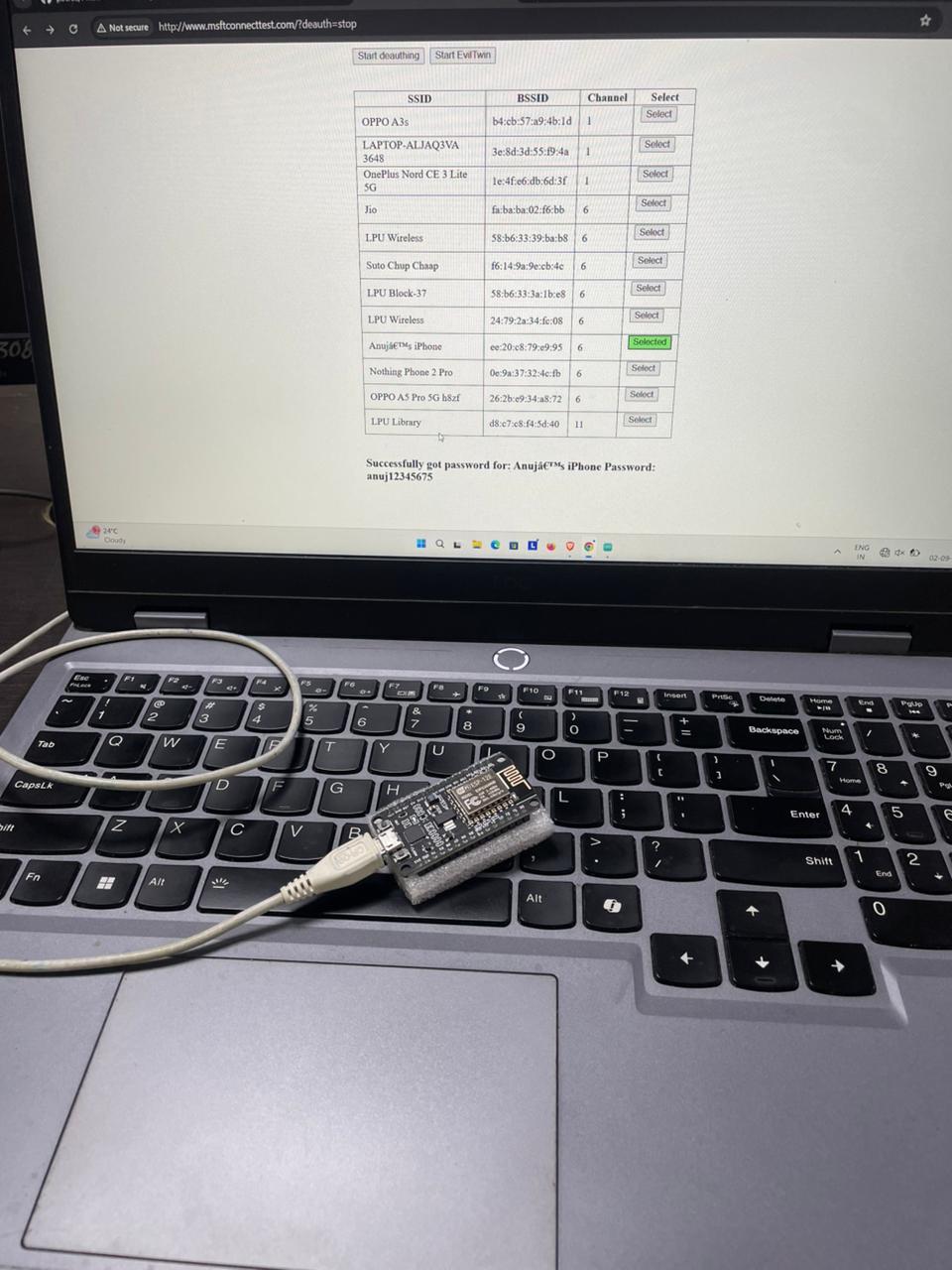
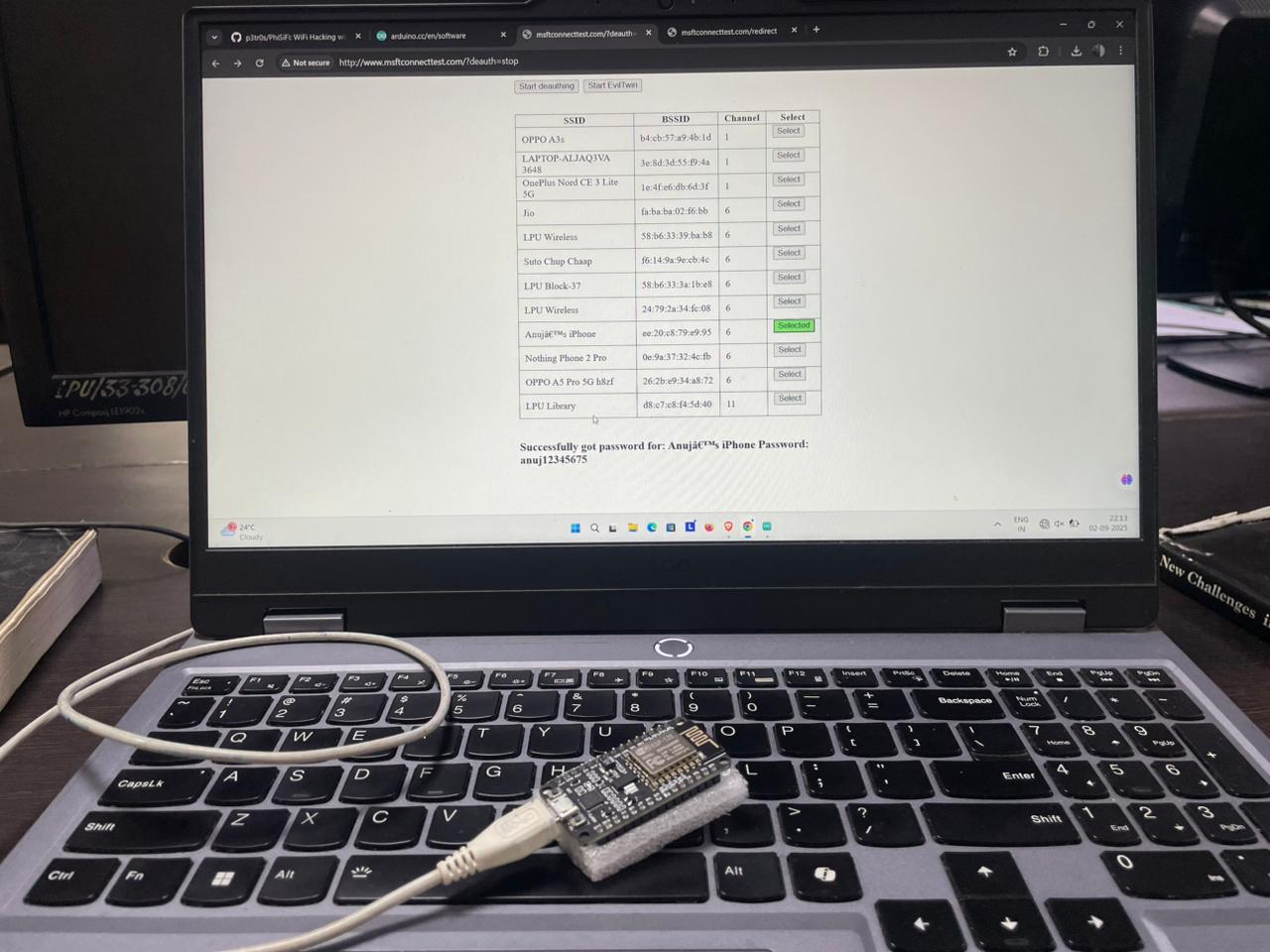
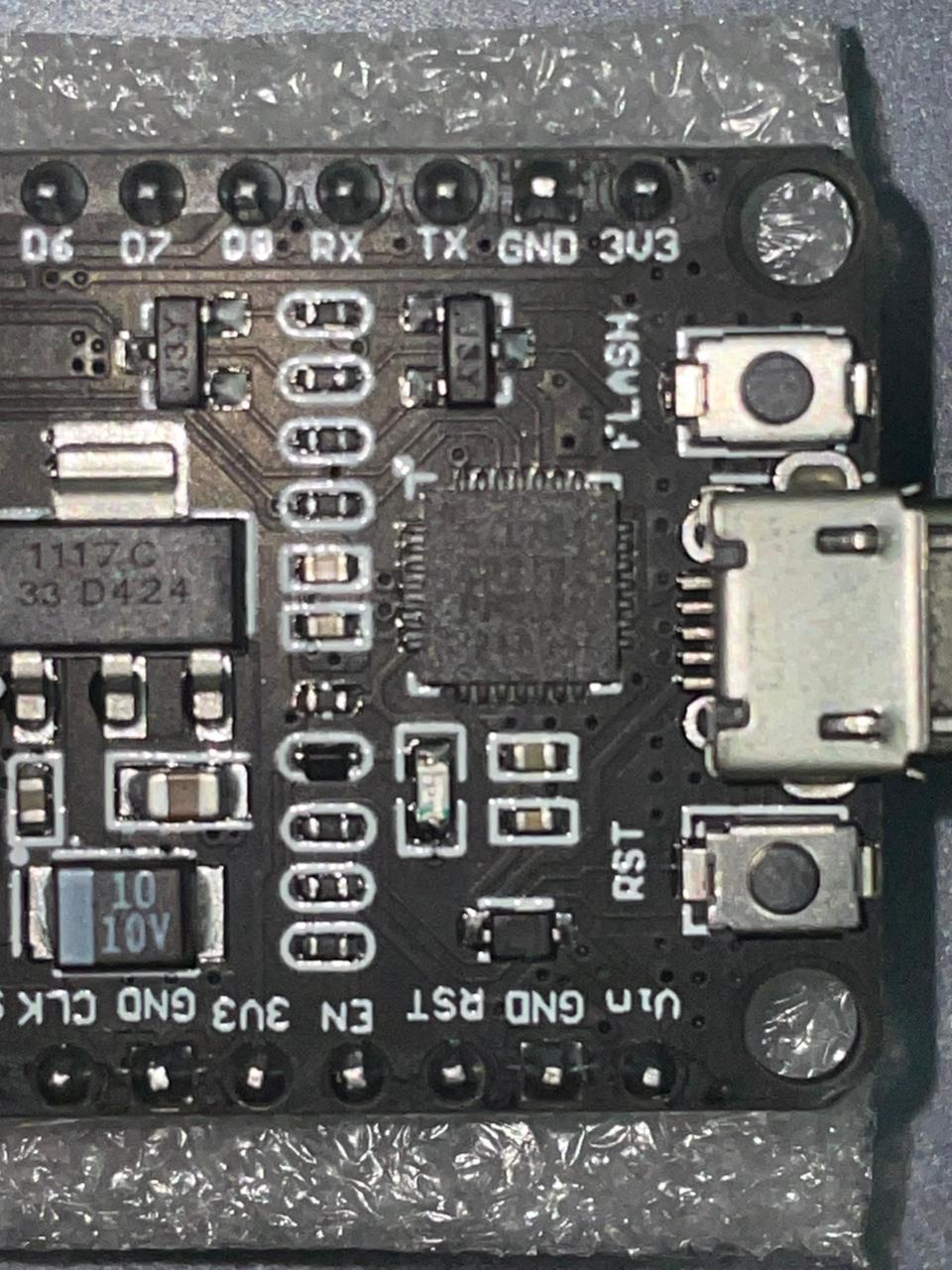
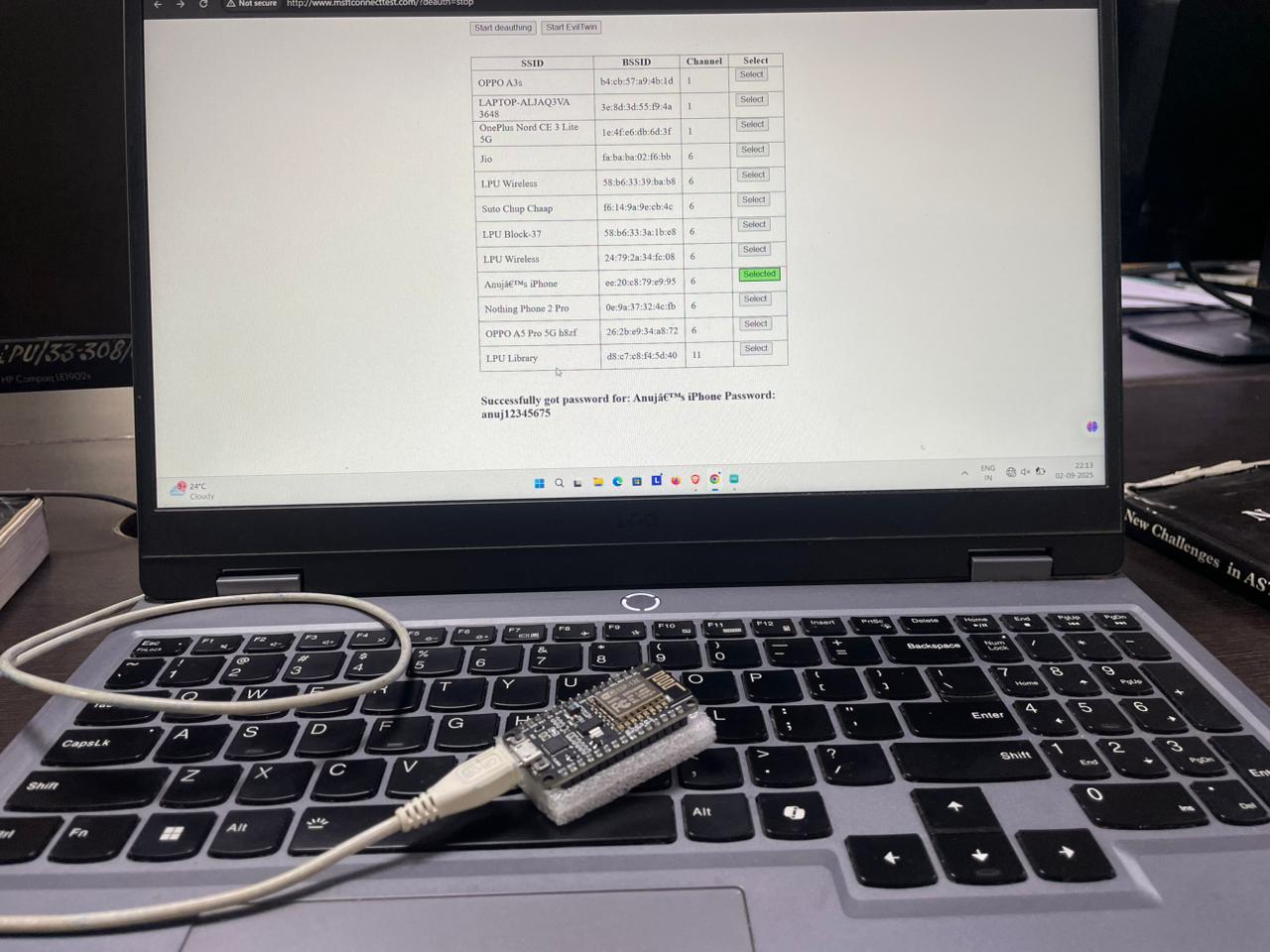
- Successfully cloned target SSID.

- Captured password attempts via captive portal.

Screenshots from my test setup:

![ESP32 Evil Twin Setup]

![Captured Password Example]



---

## 🔐 Defensive Measures

This project is not just about demonstrating the attack, but also about learning \*\*how to defend against it\*\*:

- ✅ Use \*\*WPA3\*\* instead of WPA2

- ✅ Disable \*\*auto-connect\*\* on devices

- ✅ Deploy \*\*Enterprise authentication (EAP)\*\* in organizations

- ✅ Monitor WiFi for duplicate SSIDs using tools like \*\*Wireshark\*\* or \*\*Kismet\*\*

---

## 📂 Repository Structure