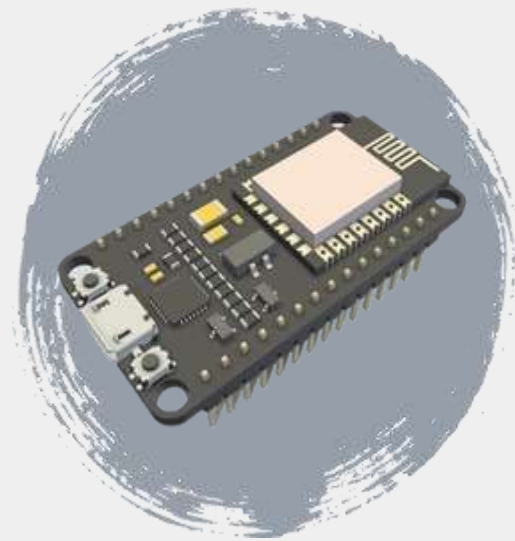


Wi-Fi 2.4GHz Attacking Tools

WIFUSION | SERIALADAPT-HUNT | WIFI-RHAPSODY



AGENDA



WIFUSION

WiFi Hacking Watch



SERIALADAPT-HUNT

WiFi Adapter

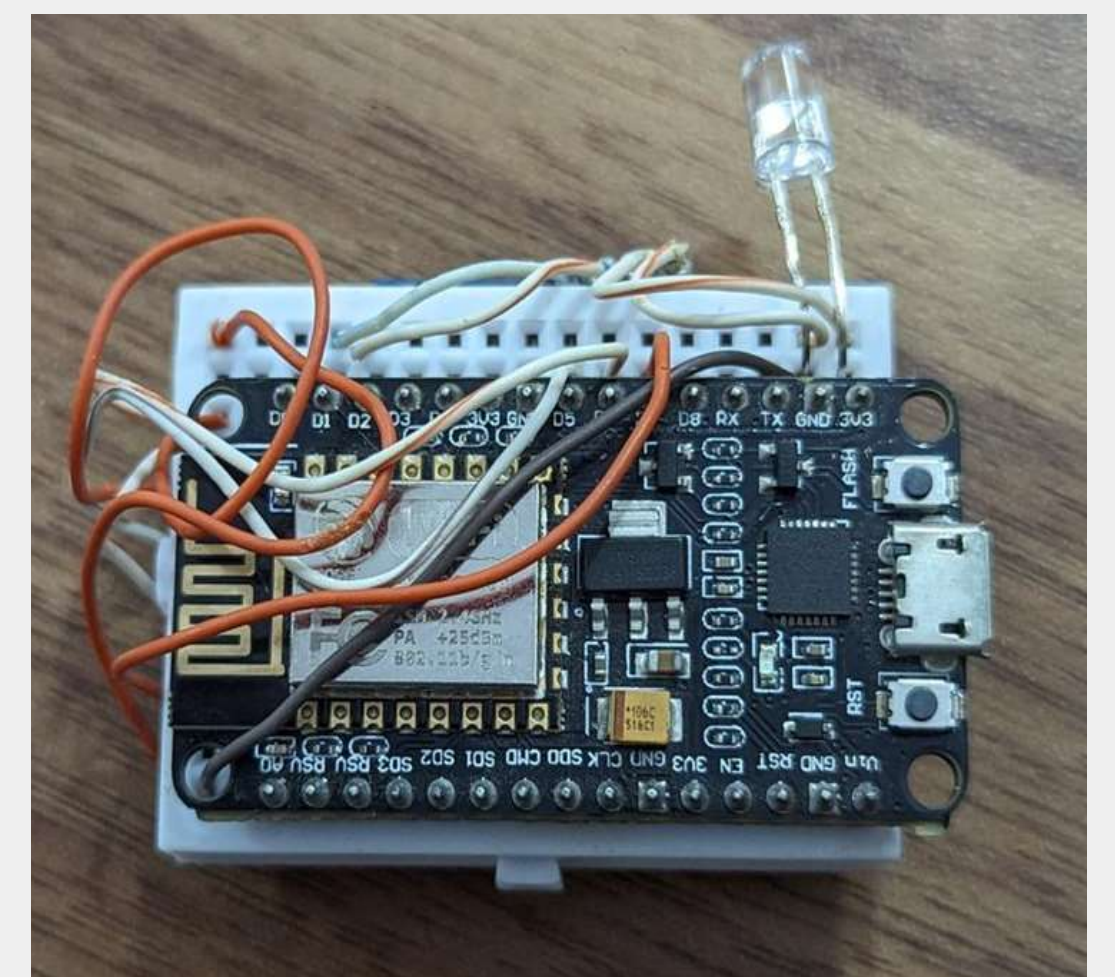
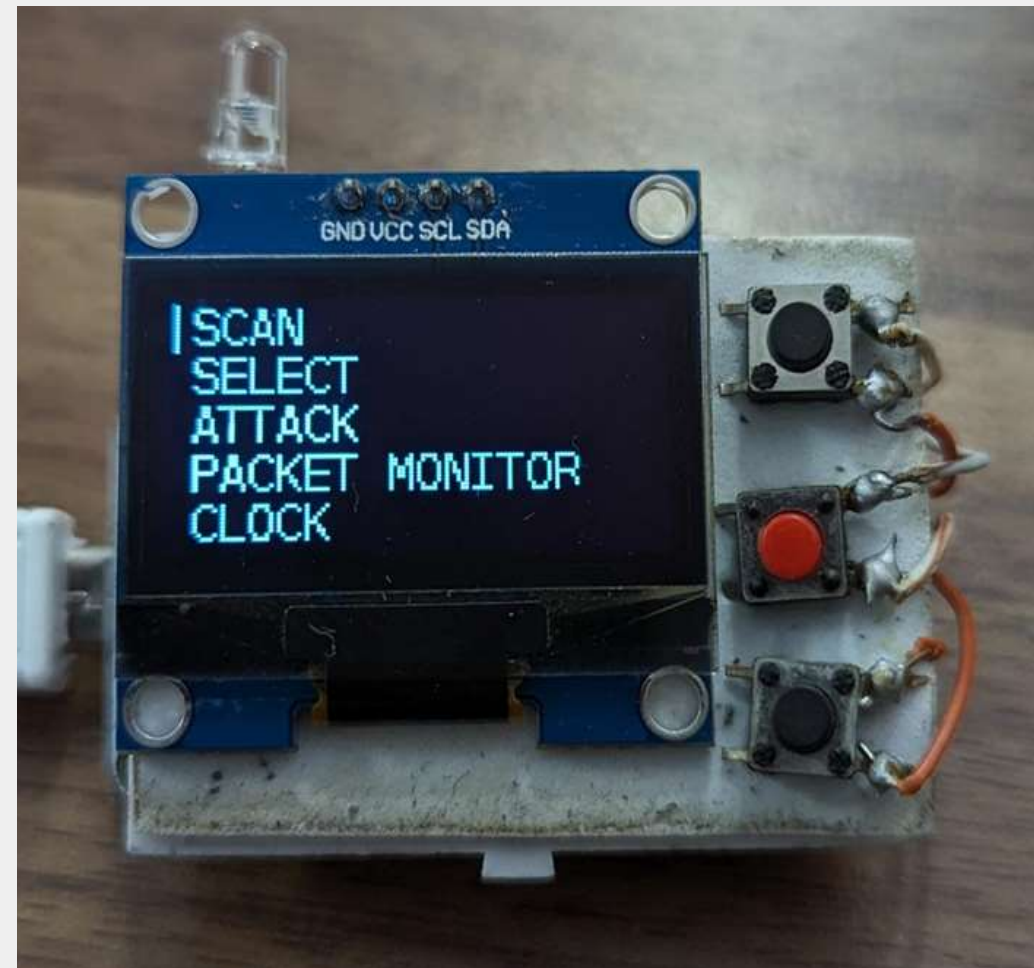
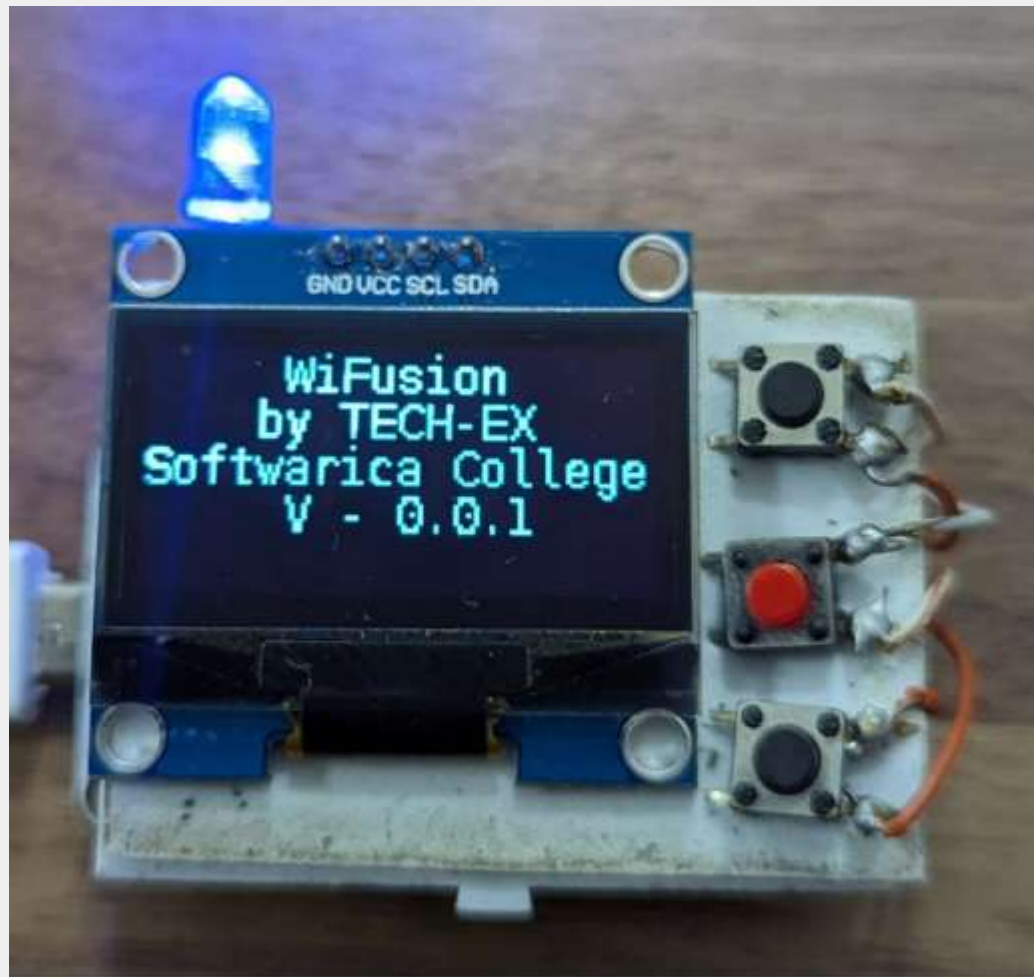


WIFI RHAPSODY

WiFi Monitoring Device

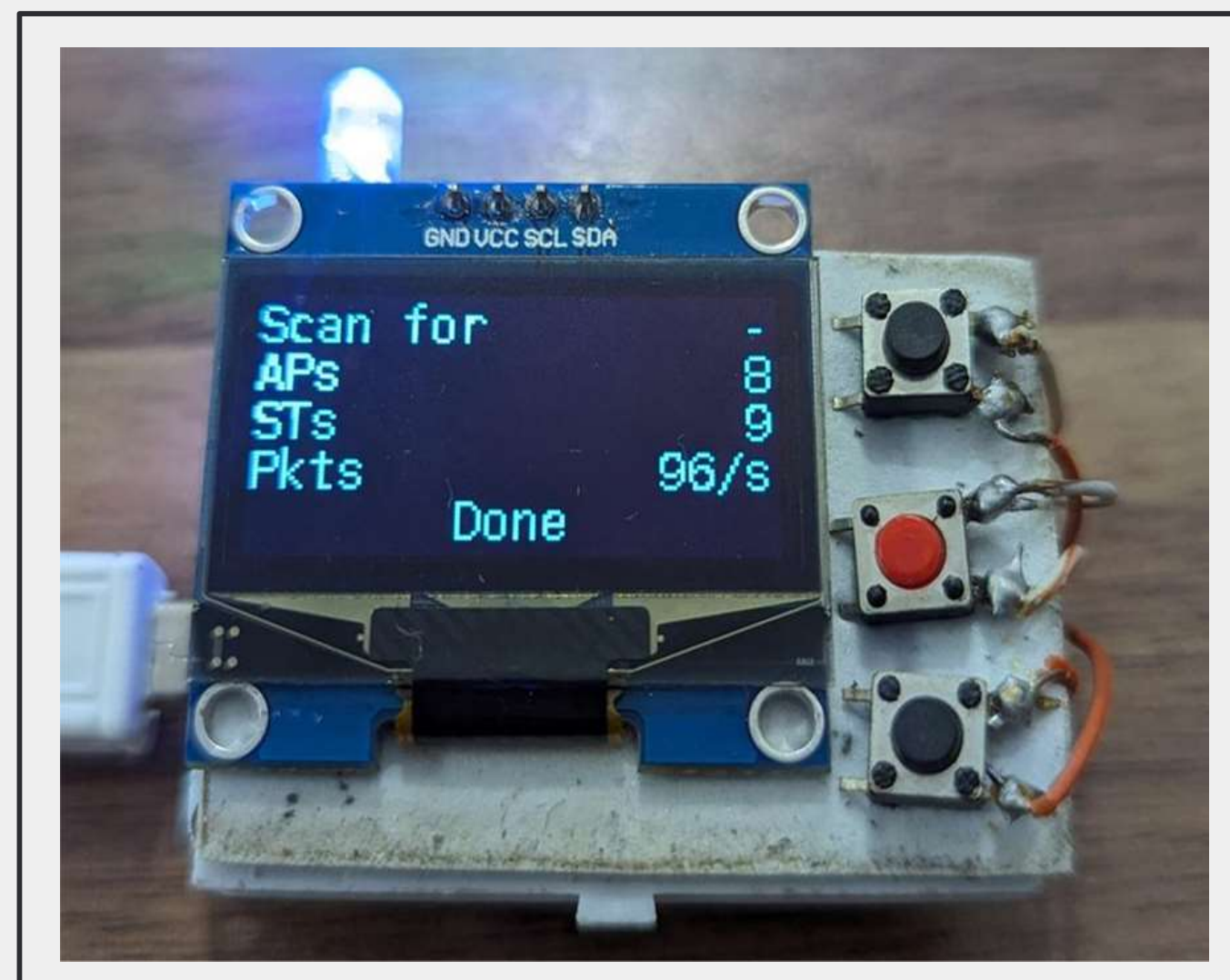
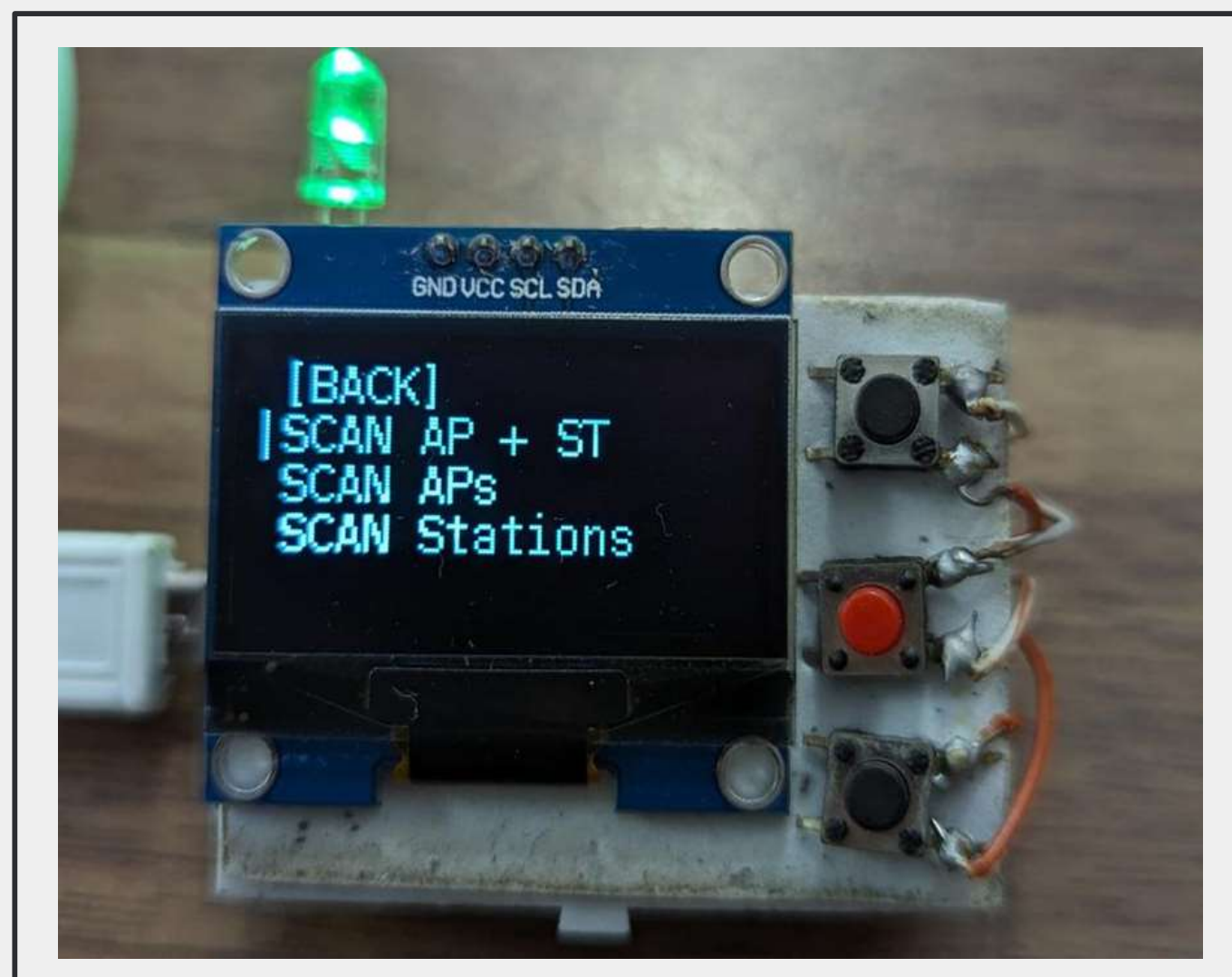
WIFUSION

WiFsuion is a device using ESP32, SH1106, push buttons, and a LED for wireless attacks. It scans nearby access points and devices and performs deauthentication, beacon, and probe attacks with options to target multiple APs or devices. It also includes packet monitoring for efficient attack selection.



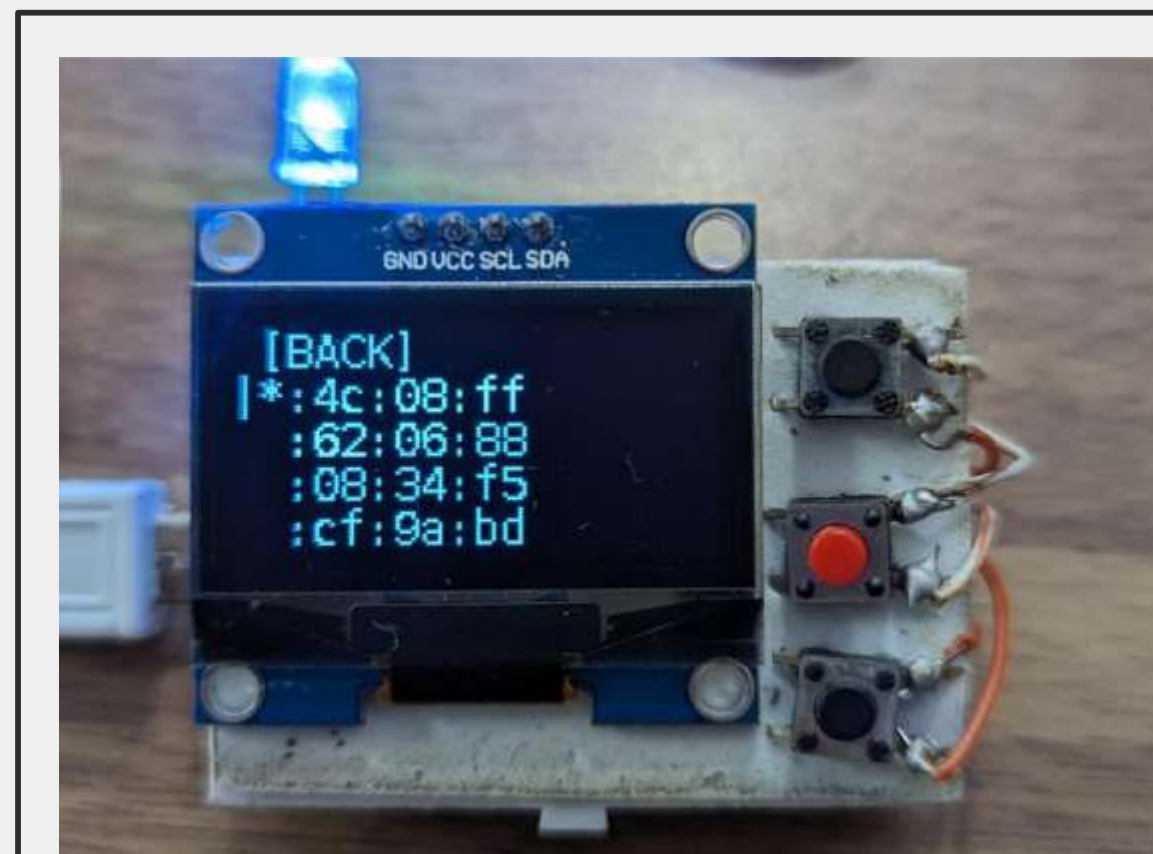
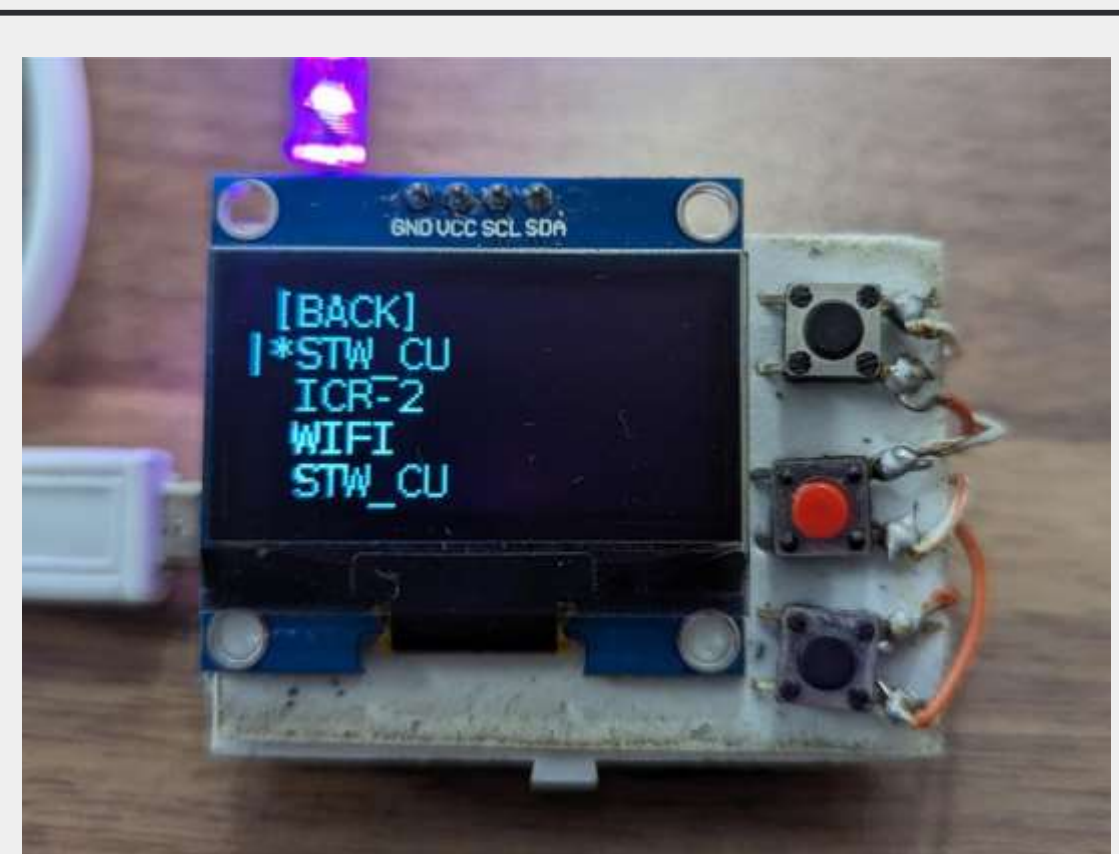
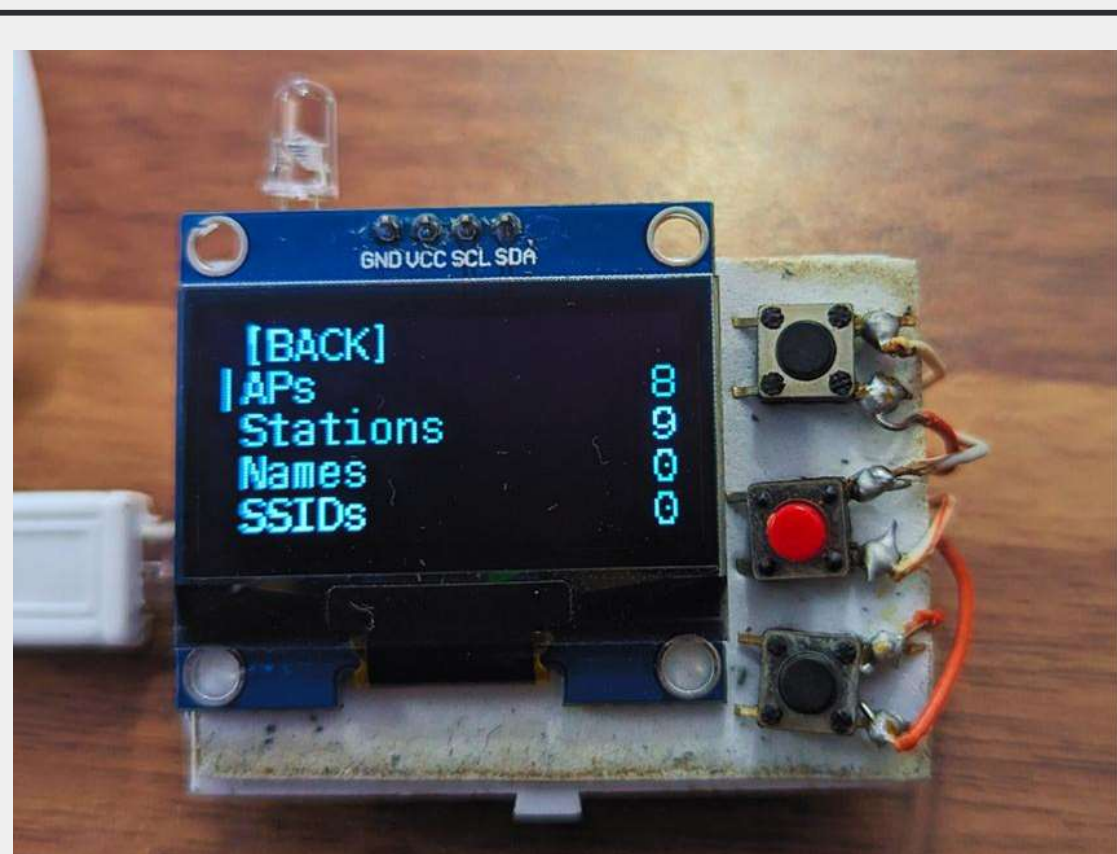
WiFusion - Scanning

In the scan menu, WiFusion offers three types of scans: nearby Wi-Fi Access Points (APs), Wi-Fi Client Stations (STs), or a combined scan for both APs and STs.



WiFusion - Select

In the select menu, users can choose attack targets by accessing the scanned WiFi Access Points (APs) and WiFi Client Stations (STs). Additionally, specific SSIDs can be selected for a beacon attack or saved devices under Names can be targeted for various attacks.

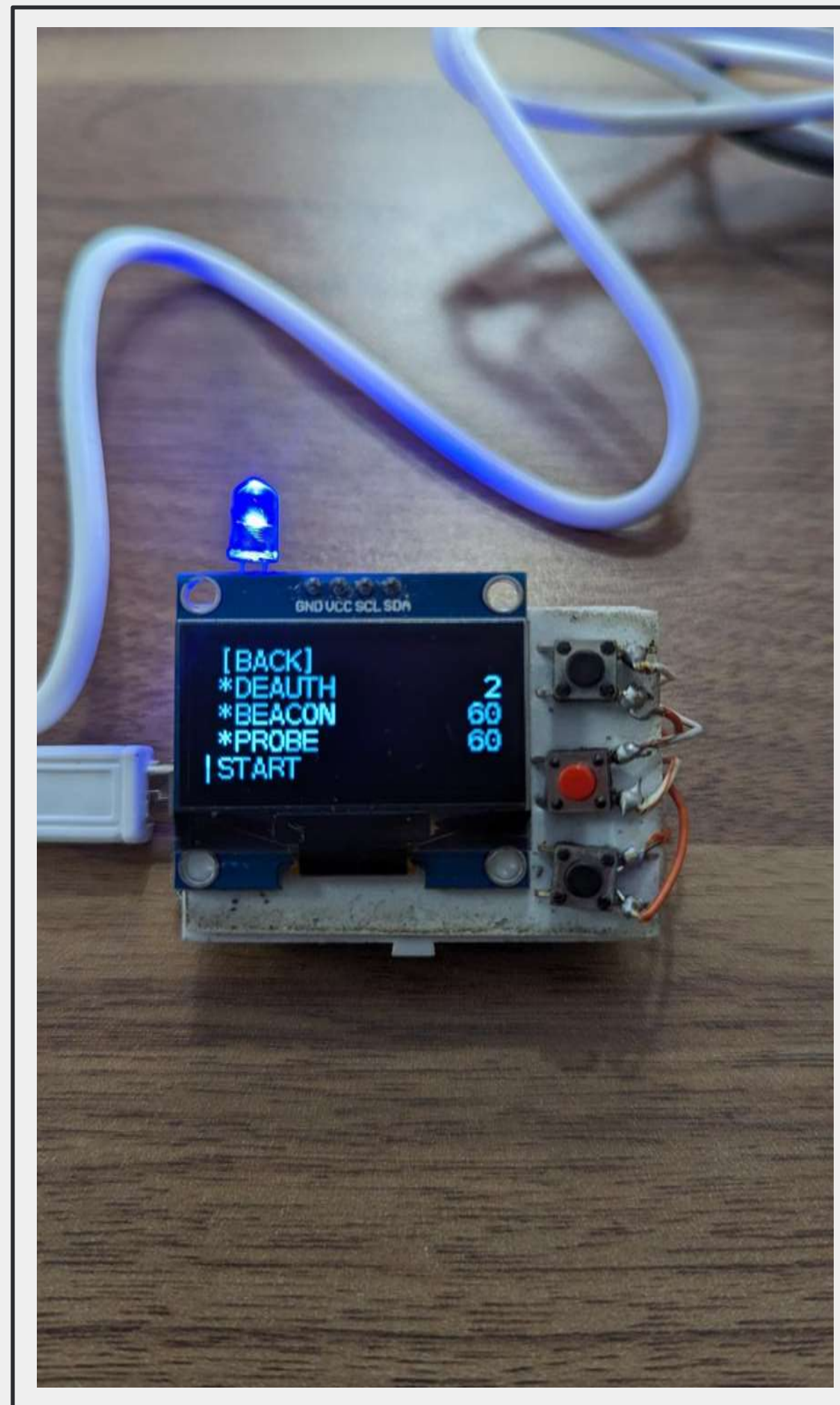
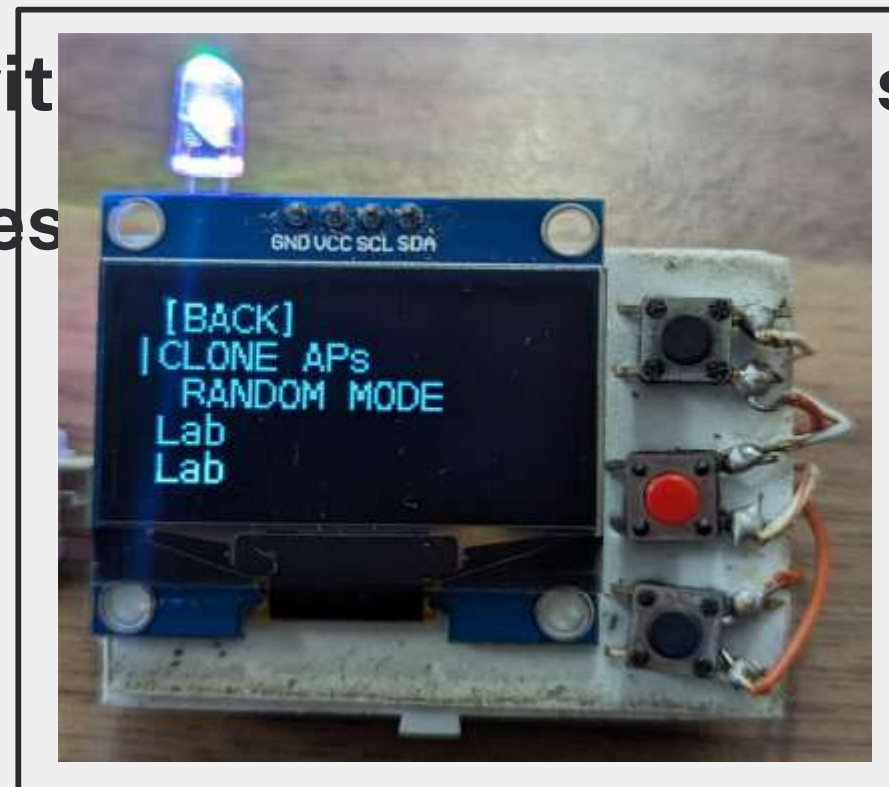
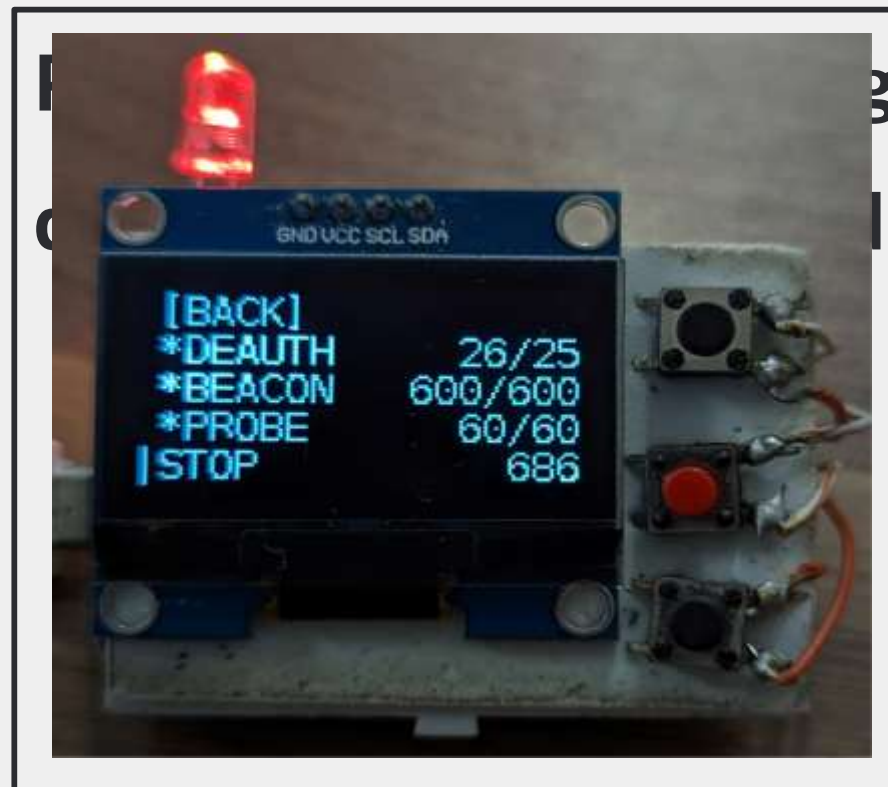


WiFusion - Attack

On the attack page, users can execute different WiFi attacks:

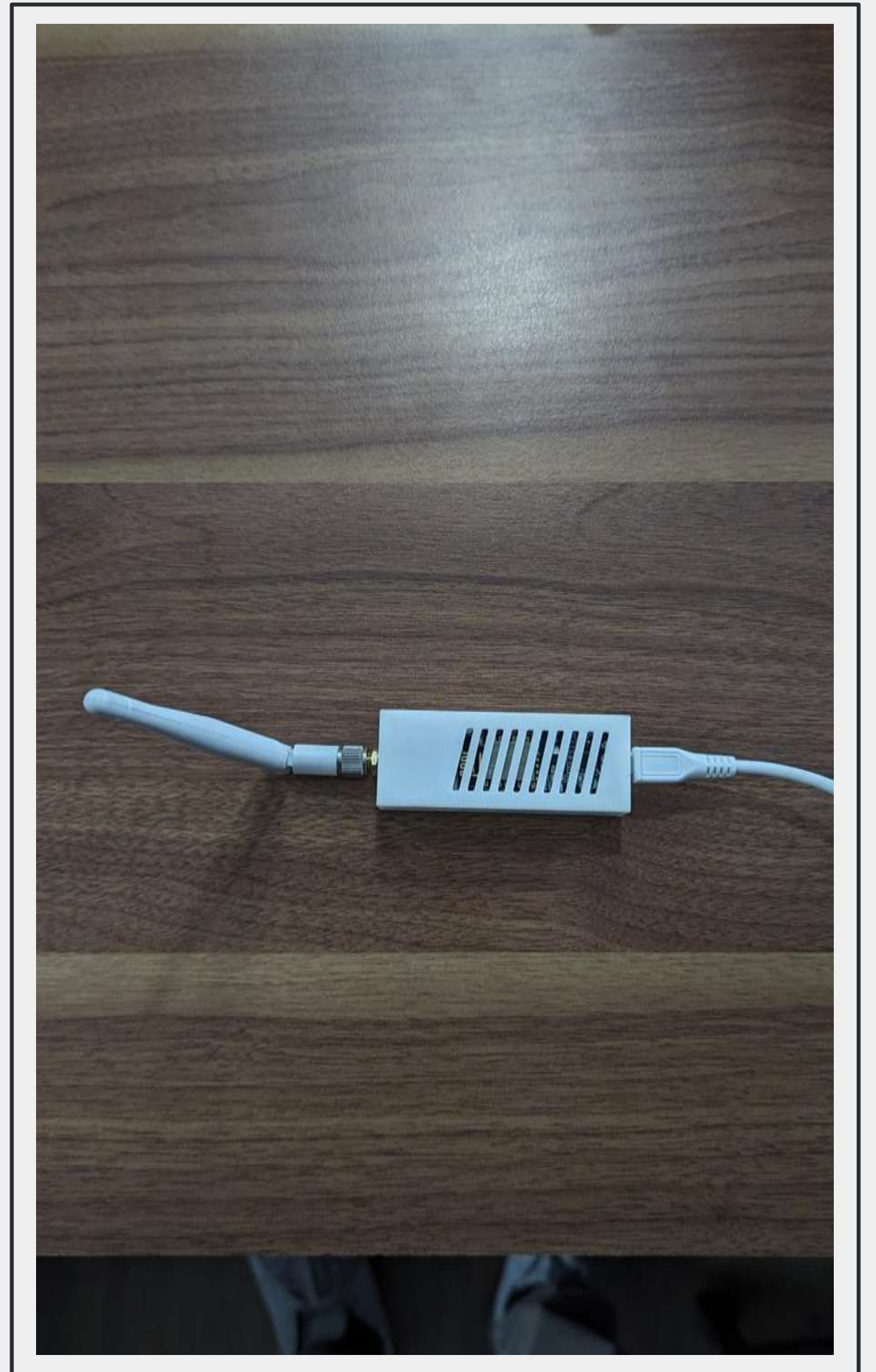
- **DEAUTH:** Disconnects selected devices (APs or STs) through deauthentication.
- **BEACON:** Floods the target with fake SSIDs using beacon frames.

- **FLOOD:** Floods the target with fake SSIDs using beacon frames, devices



SERIALADAPT-HUNT

WiFusion and SerialAdapt-Hunt share common functionalities like Deauth, Beacon, and Probe attacks, as well as network scanning for access points and clients. However, they differ in control methods; WiFusion uses a display and buttons, while SerialAdapt-Hunt connects via USB and is controlled through a serial terminal. SerialAdapt-Hunt prioritizes a powerful command-line interface (CLI) to fully utilize hardware capabilities like CPU, memory, and the WiFi transceiver.



SerialAdapt-Hunt

Terminal

SerialAdapt-Hunt provides a user-friendly terminal interface, offering a simple manual or step-by-step guide to navigate and initiate attacks efficiently.

```
PowerShell

# help

welcome
  Print welcome screen including version and disclaimer

help [-cmd,command <value>] [-s/hort]
  Print the list of commands that you see right now

start [-cmd <value>]
  Start a guided tour through the functions of this device

scan [-m/ode <ap+st>] [-t/ime <20s>] [-ch/annel <all>] [-ct/ime <284>] [-r/etain]
  Scan for WiFi devices
  -m: scan mode [ap,st,ap+st] (default=ap+st)
  -t: station scan time (default=20s)
  -ch: 2.4 GHz channels for station scan [1-14] (default=all)
  -ct: channel scan time in milliseconds (default=284)
  -r: keep previous scan results

auth [-bssid <value>] [-ap <value>] [-t/ime <0>] [-ch/annel <all>] [-ct/ime <284>]
  Authentication scan
  -bssid: filter by BSSID(s)
  -ap: filter by access point ID(s)
  -ch: 2.4 GHz channels for auth. scan [1-14] (default=all)
  -ct: channel scan time in milliseconds (default=284)
  -t: scan timeout (default=none)
  -save: save recorded probe requests

rssi [-mac <value>] [-ap <value>] [-st/ation <value>] [-ch/annel <all>] [-ct/ime <120>]
  Signal Strength scan
  -mac: filter by MAC(s)
  -ap: filter by AP(s)
  -st: filter by Station(s)
  -ch: 2.4 GHz channel(s) for scan [1-14] (default=all)
  -ct: channel scan time in milliseconds (default=120)
```


SerialAdapt-Hunt

Scanning

On the scanning side, SerialAdapt-Hunt provides insights into probe requests from nearby devices, revealing their previously connected networks.

Furthermore, users can view the MAC addresses of devices attempting to connect to networks advertised through the beacon attack. The option to alias MAC addresses adds convenience in recognizing known devices. Furthermore, all the results can be saved for future use. These comprehensive features make SerialAdapt-Hunt a powerful tool

PowerShell

```
# scan ap+st -r

[ ===== Scan for Access Points ===== ]
Channels:      1,2,3,4,5,6,7,8,9,10,11,12,13,14,

Type 'stop scan' to stop the scan

> Stopped access point scan

[ ===== Access Points ===== ]
ID SSID (Network Name)                RSSI Mode Ch BSSID (MAC Addr.) Vendor
-----
0 "minila_2.4"                        -77 WPA* 10 04:75:f9:04:18:f9 TaicangT
1 *HIDDEN-NETWORK*                   -77 WPA2 10 06:75:f9:44:18:f9
2 "Lab"                               -58 WPA2  3 10:27:f5:89:ad:d6 TP-Link
3 "OPPO A53"                          -83 WPA2  6 12:0c:4e:24:f4:39
4 "Achyut_NTFiber"                   -88 WPA2  1 20:57:af:86:12:46 Shenzhen
5 "STW_CU"                           -72 Open  6 68:21:5f:9d:09:bf Edgecore
6 "testsunnfun"                      -86 WPA* 11 9c:2b:a6:7a:ca:37 RuijieNe
7 "IPC_9CA3A9242114"                 -86 WPA2 14 9e:a3:a9:24:21:14
8 "DIGICOM"                          -91 WPA*  1 a8:32:9a:0c:63:8b DigicomF
9 "SBH_BOTTOM_FLOOR"                 -87 WPA*  1 a8:32:9a:0f:3f:bb DigicomF
10 "Sweet Home"                      -89 WPA2  9 b4:cf:e0:01:c0:78 Sichuant
11 "STW_CU"                           -48 Open  1 b8:6a:97:14:3f:7e Edgecore
12 "STW_CU"                           -78 Open  6 b8:6a:97:44:6f:25 Edgecore
13 "hariamala13"                     -87 WPA*  1 dc:8d:8a:36:62:4a NokiaSol
14 *HIDDEN-NETWORK*                  -85 WPA2  1 de:8d:8a:46:62:4a
15 "STW_CU"                           -73 Open 11 e0:01:a6:60:35:b2
16 "ICR-2"                           -58 Open  6 e0:01:a6:60:36:3a

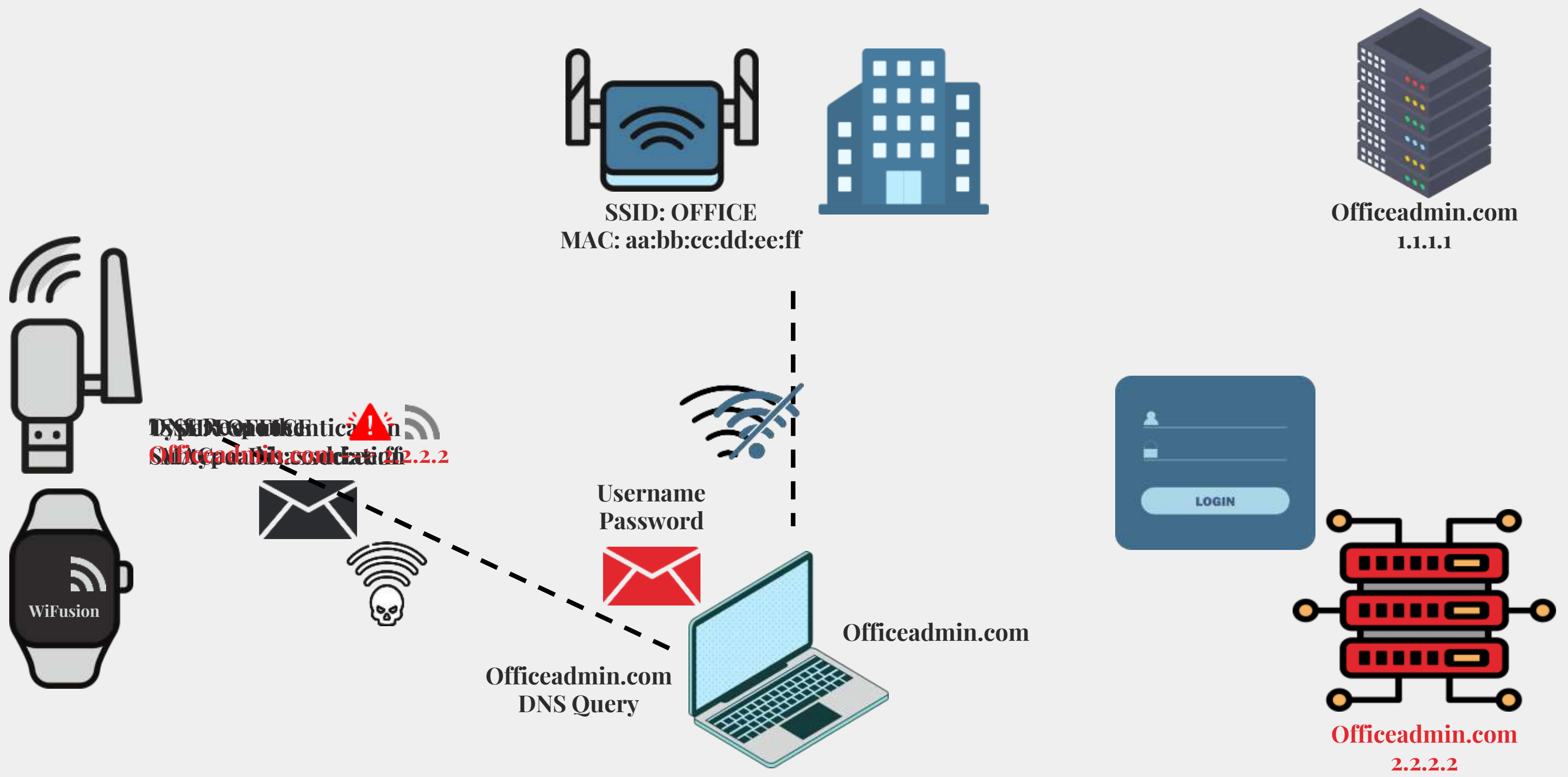
Ch = 2.4 GHz Channel , RSSI = Signal strength , WPA* = WPA & WPA2 auto mode
WPA(2) Enterprise networks are recognized as Open

[ ===== Scan for Stations ===== ]
Scan time:      20s
Channel time:   284ms
Channels:      1,2,3,4,5,6,7,8,9,10,11,12,13,14,

Type 'stop scan' to stop the scan

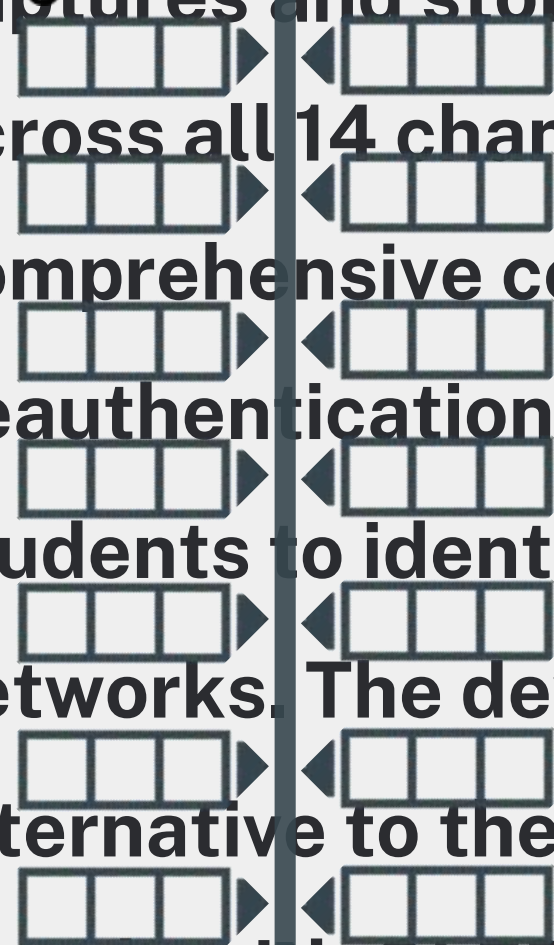
ID Pkts RSSI Vendor  MAC-Address  AccessPoint-SSID  AccessPoint-BSSID  Probe-Requests
-----
-   1  -82      ca:c2:ec:e4:6d:65 "OPPO A53"      12:0c:4e:24:f4:39
-   2  -33 IntelCor f0:b6:1e:36:90:f2 "STW_CU"        e0:01:a6:60:35:b2
-   2  -74 IntelCor 20:1e:88:dc:09:01 "STW_CU"
```

THE MAIN IDEA



WIFI RHAPSODY

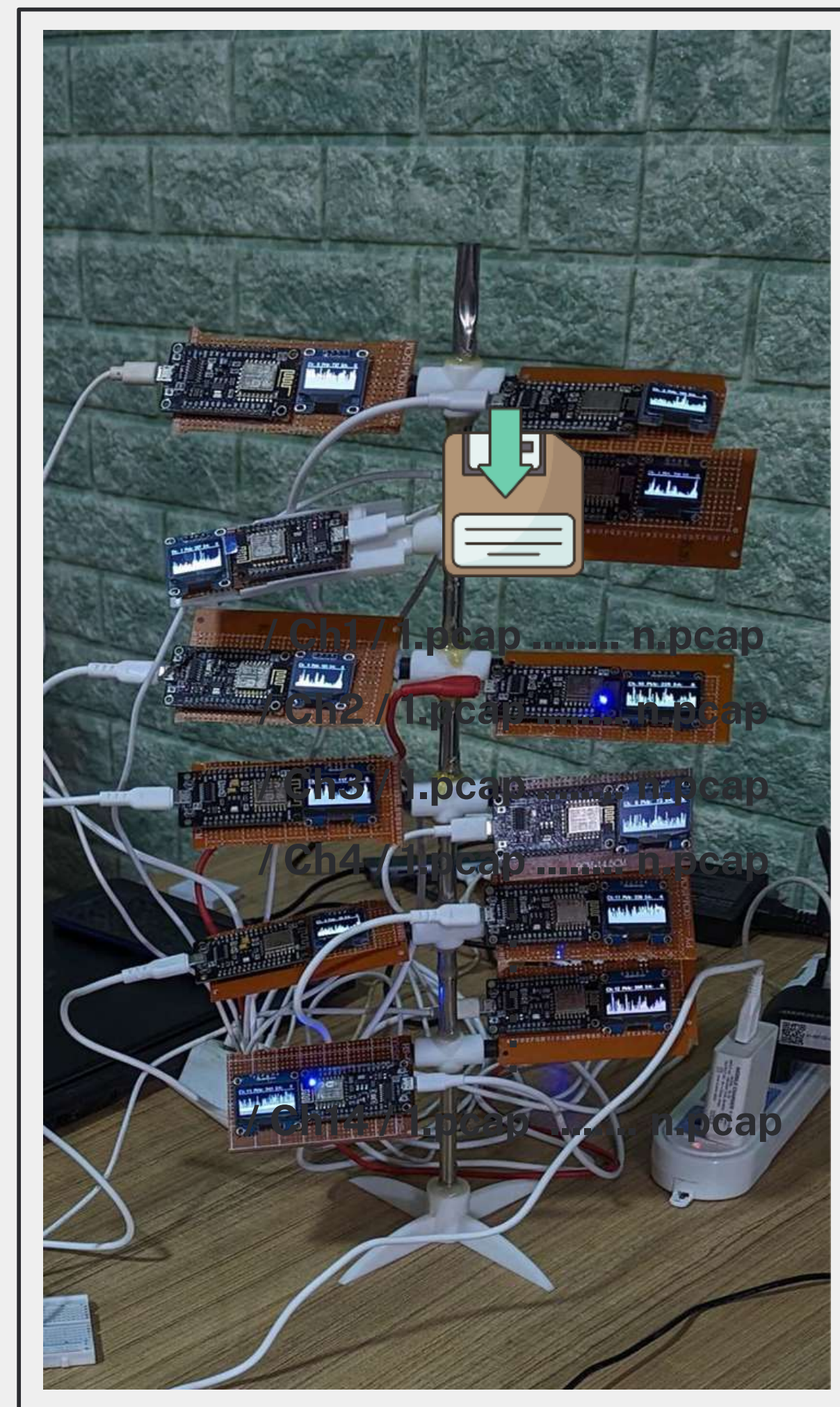
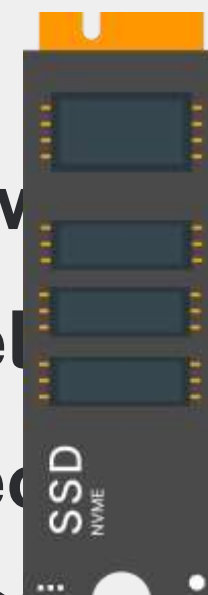
WiFiRhapsody is a monitoring device that efficiently captures and stores packets on the 2.4GHz band across all 14 channels simultaneously, providing comprehensive coverage. Its valuable deauthentication packet detection feature allows students to identify potential threats from wireless networks. The device is designed as a cost-effective alternative to the Wifi Cactus, utilizing 14 ESP32 boards with OLED screens and a storage device (like an SD card) to display and log the traffic from the 2.4GHz channels. All captured data is saved in .pcap format, ensuring convenient and compatible storage



Probes

Beacons

Authentications



Thank you!
