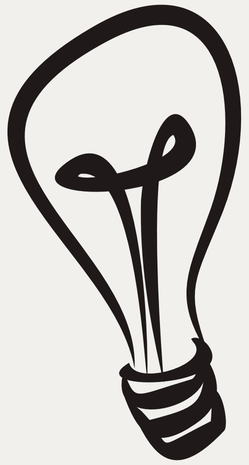
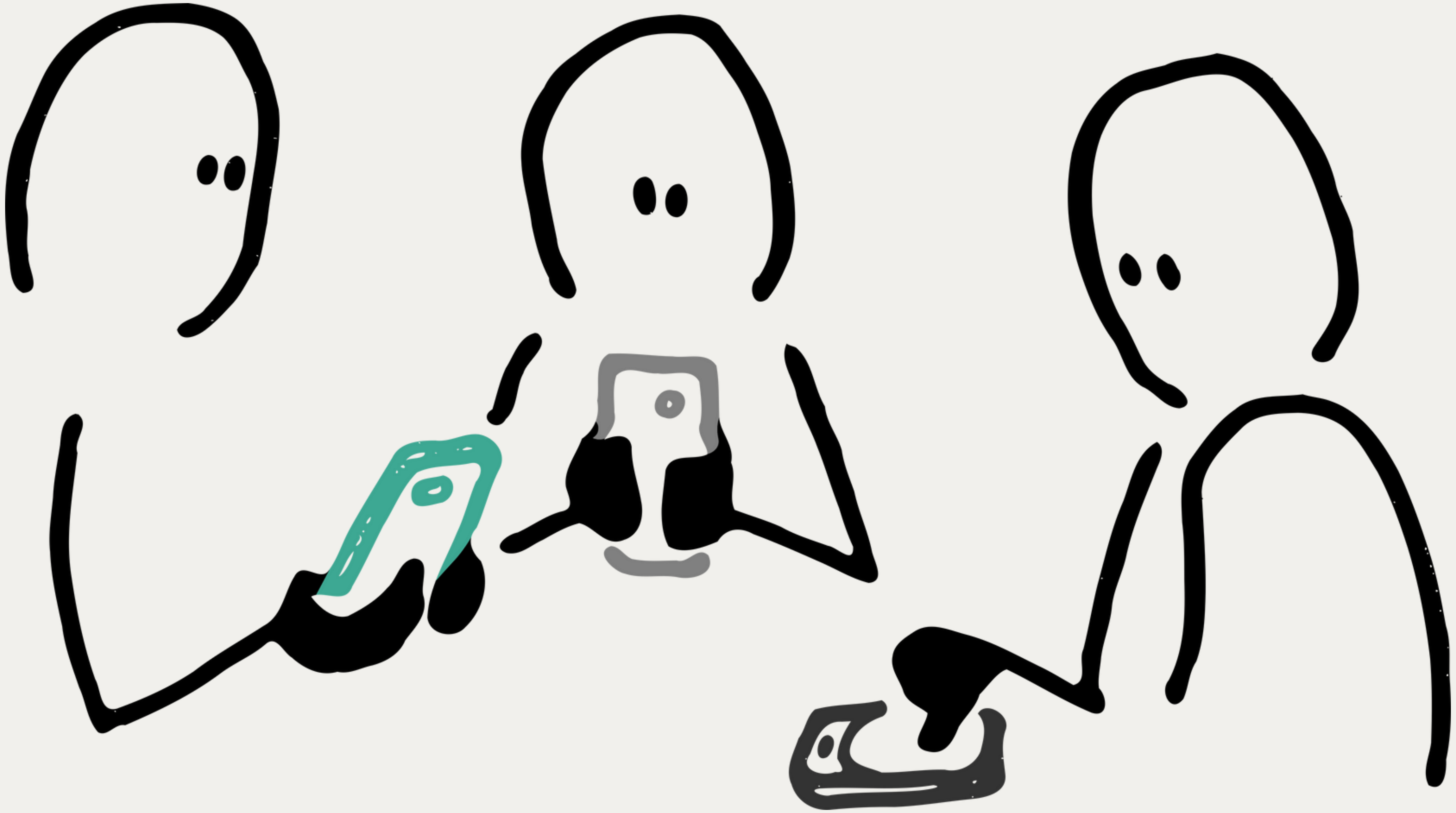
## GROUP 10

EG/2021/4474
EG/2021/4781
EG/2021/4807





# OFFENSIVE AND DEFENSIVE WI-FI/BLUETOOTH PEN TOOL

# INTRODUCTION TO THE PEN TOOL

- Wireless technologies like Wi-Fi and Bluetooth are widely used but are increasingly vulnerable to cyber threats such as deauthentication attacks, rogue access points and device tracking.
- Ethical penetration testing is essential to identify and address these risks.
- However, most existing tools are complex, costly, and not easily portable.

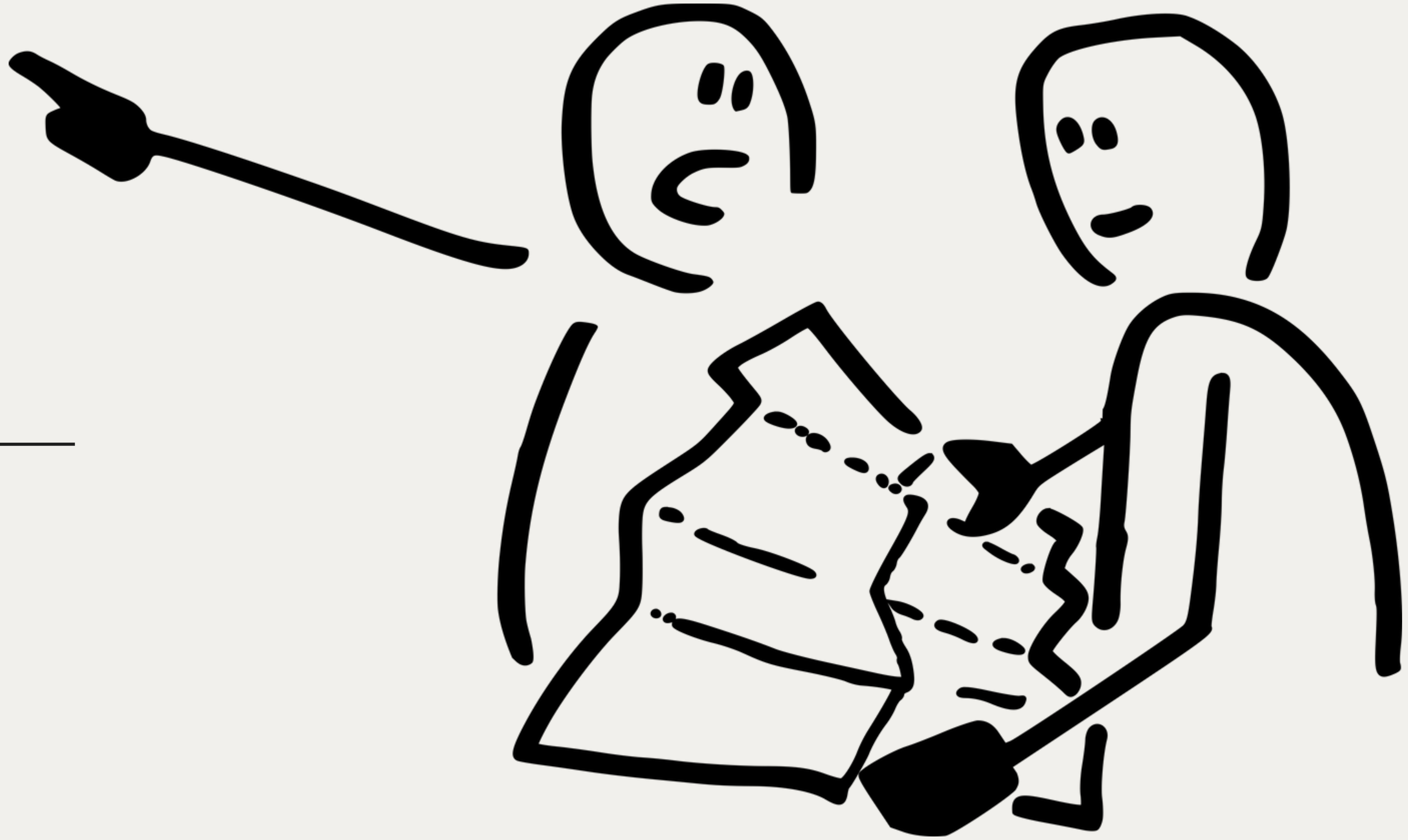
Our project introduces a

- **compact, low-cost and portable penetration testing tool**
- based on the **ESP32 microcontroller with a TFT touch screen**
- offering both **offensive and defensive wireless testing capabilities**

through a user-friendly interface.

# PROBLEM STATEMENT

- Increasing threats to wireless networks such as deauthentication attacks, rogue access points and device MAC address identification.
- Lack of affordable and accessible testing tools.
- Need for a device that supports both offensive and defensive testing modes.

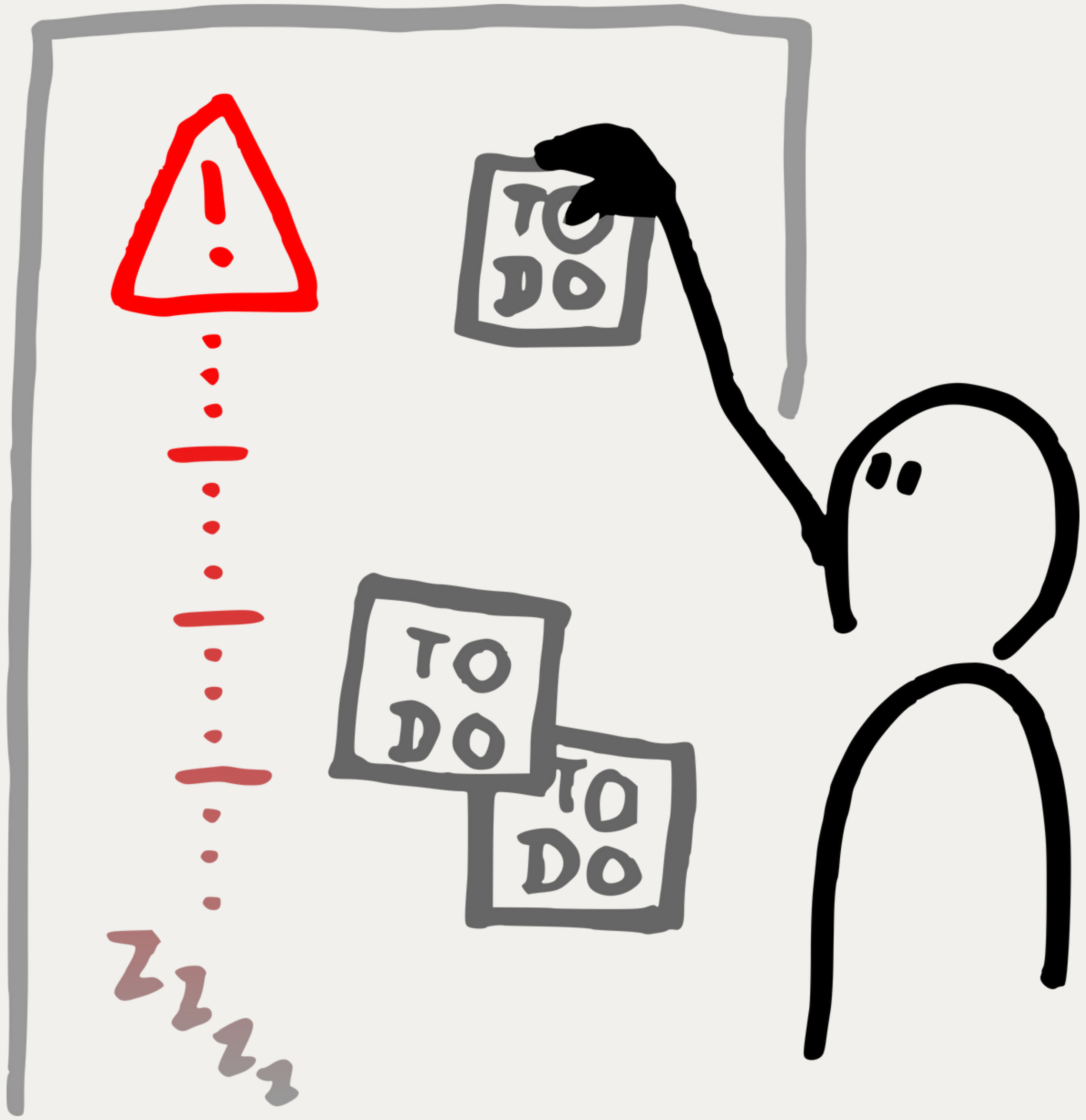


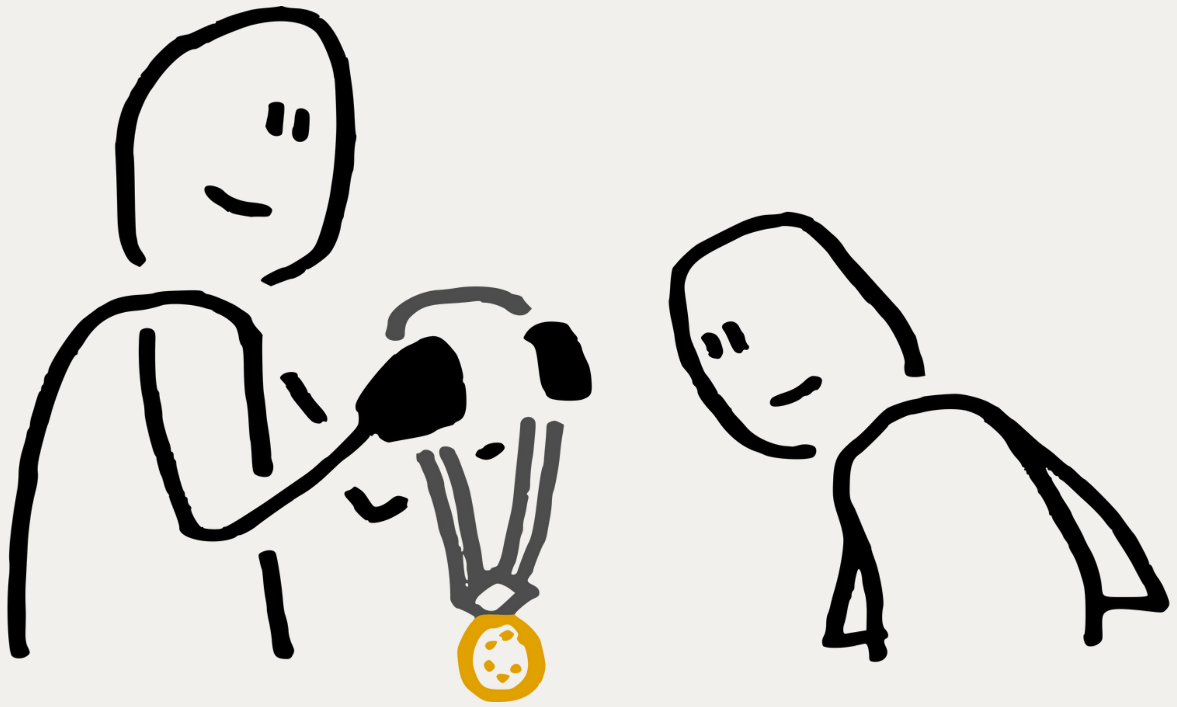
# OBJECTIVE

- To develop a secure, portable Wi-Fi/Bluetooth penetration testing tool that works in noisy and high-traffic environments using ESP32, enhanced for reliability, and controlled via an intuitive touch interface.

# PROJECT SCOPE

1. Wi-Fi & Bluetooth scanning
2. Packet sniffing & logging
3. Fake AP simulation & SSID flooding
4. Offline PCAP analysis via SD card
5. TFT-based GUI for real-time interaction





# PEN TOOL CAPABILITIES

### WI-FI

- Join/shutdown Wi-Fi
- SSID generation
- Beacon spam
- Probe and beacon sniffing

### BLUETOOTH

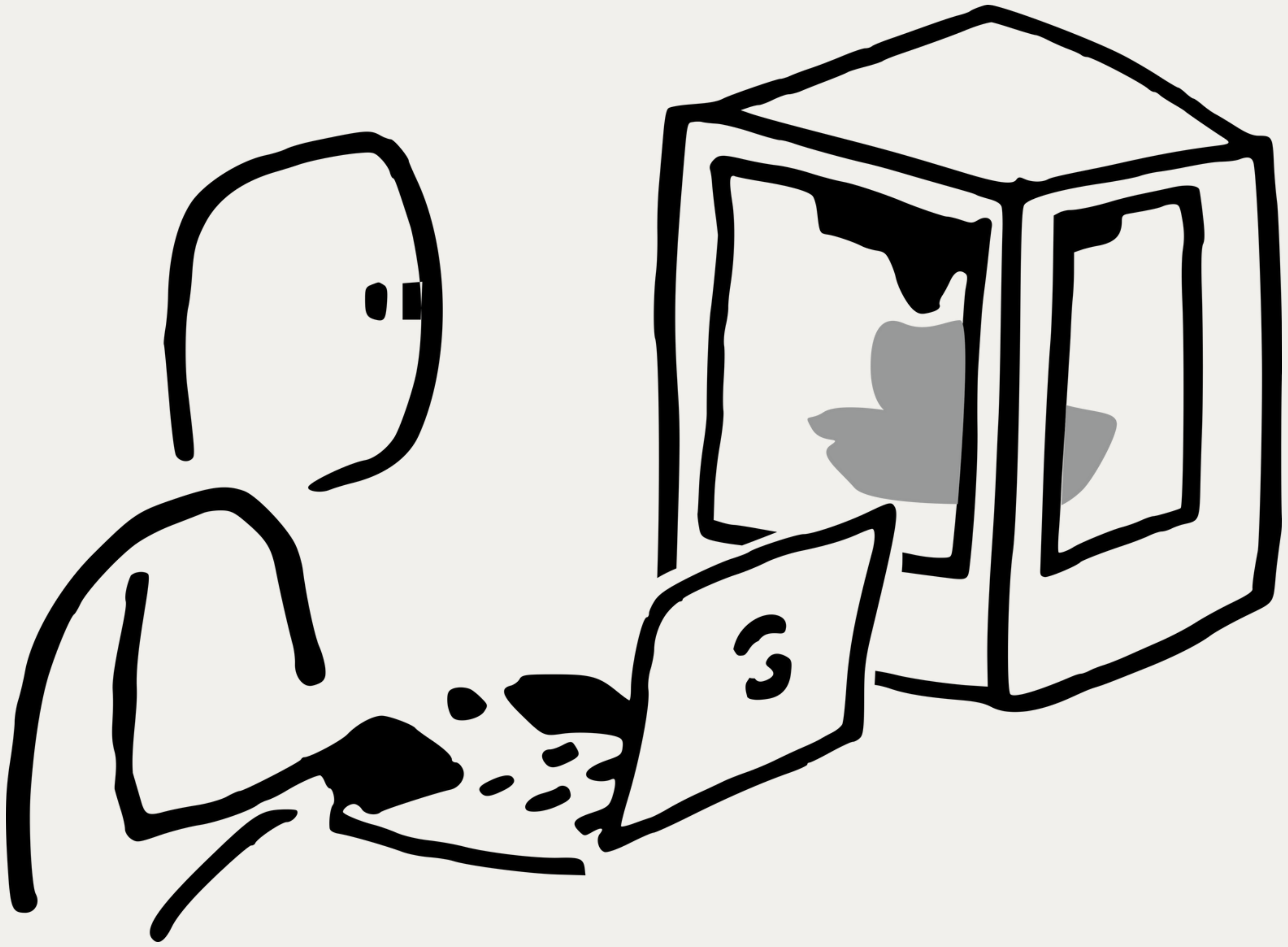
- Bluetooth scanner
- BLE shutdown
- Skimmer detection
- Probe and beacon sniffing

### UI/UTILITIES

- TFT GUI
- Touch navigation
- PCAP logging

# KEY COMPONENTS

- ESP32 microcontroller
- 2.8” ILI9341 TFT touchscreen
- SD card module
- Battery power supply



# PIN CONNECTIONS

## TOUCH SCREEN DISPLAY

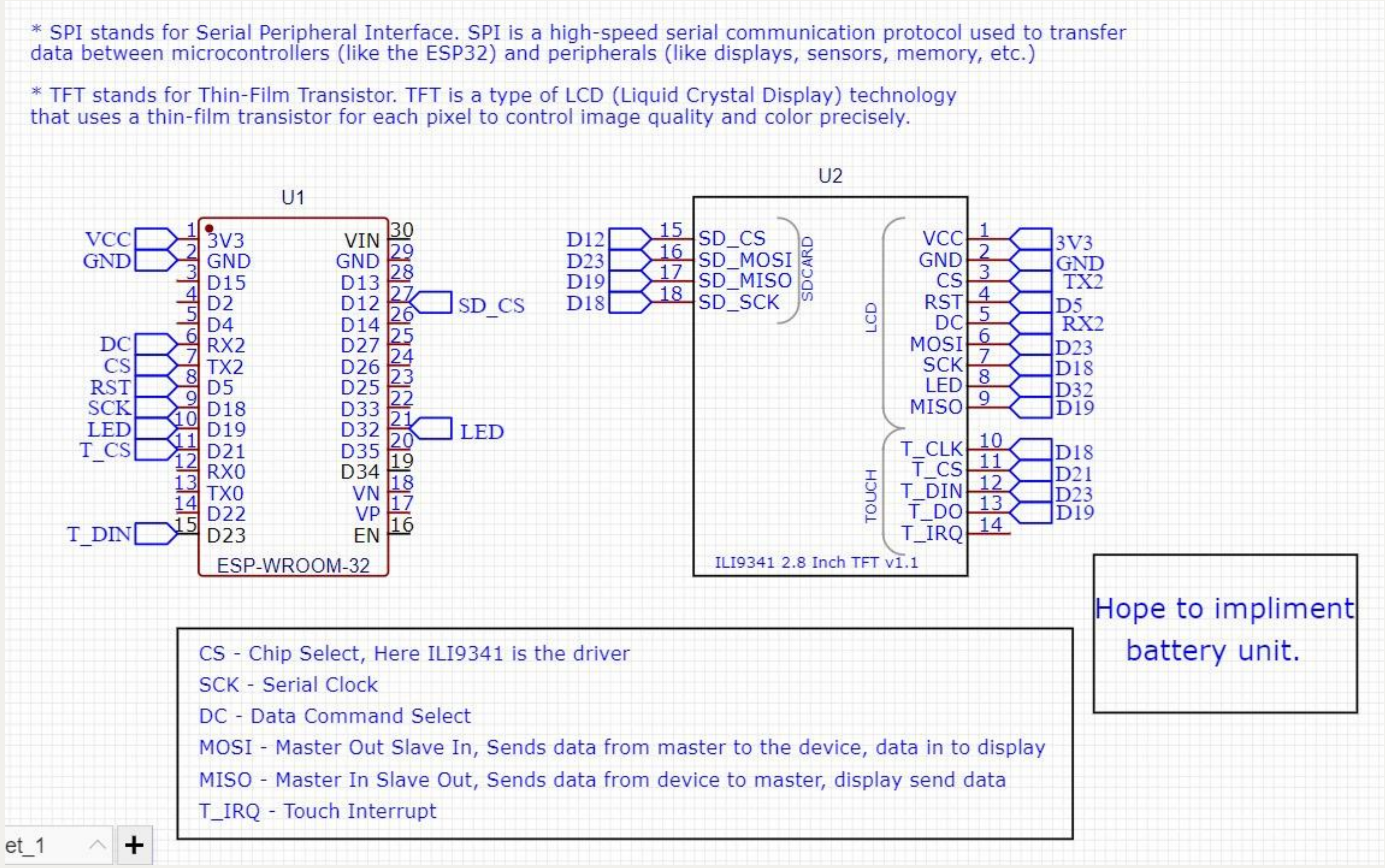
| ILI9341 Pin | Label | ESP32 Pin |
|---|---|---|
| 1 | VCC | 3.3V |
| 2 | GND | GND |
| 3 | CS | D17 (TXD 2) |
| 4 | RESET | D5 |
| 5 | DC | D16 (RXD 2) |
| 6 | SDI (MOSI) | D23 |
| 7 | SCK | D18 |
| 8 | LED | D32 |
| 9 | SDO (MISO) | D19 |
| 10 | T_CLK | D18 |
| 11 | T_CS | D21 |
| 12 | T_DIN | D23 |
| 13 | T_DO | D19 |
| 14 | T_IRQ | Not Connected (X) |

## SD CARD MODULE

| SD Card Pin | Label | ESP32 Pin |
|---|---|---|
| 1 | CS | D12 |
| 2 | MOSI | D23 |
| 3 | MISO | D19 |
| 4 | SCK | D18 |

# SCHEMATIC OF THE CIRCUIT

## USING EASY EDA SOFTWARE



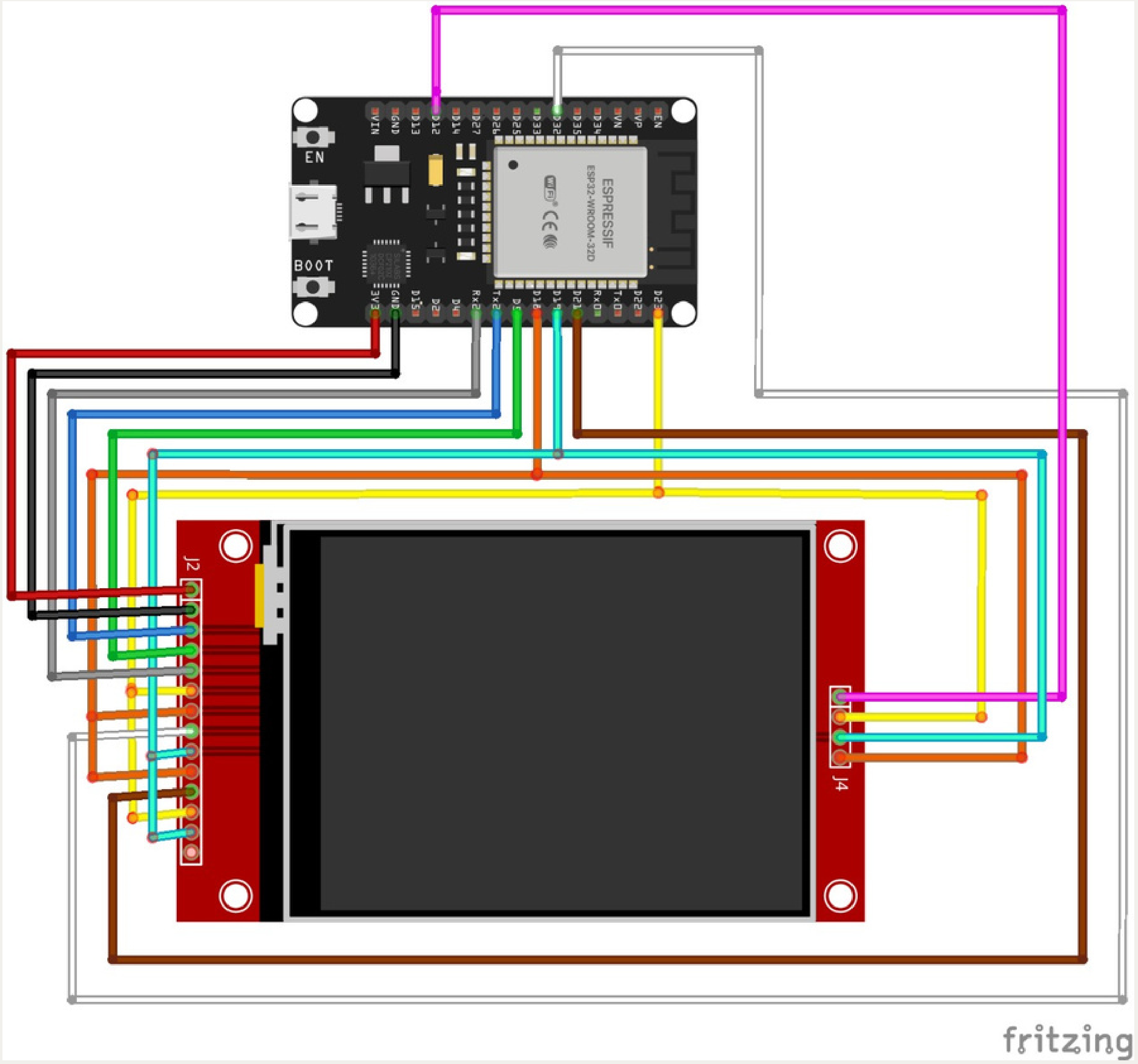
* SPI stands for Serial Peripheral Interface. SPI is a high-speed serial communication protocol used to transfer data between microcontrollers (like the ESP32) and peripherals (like displays, sensors, memory, etc.)

* TFT stands for Thin-Film Transistor. TFT is a type of LCD (Liquid Crystal Display) technology that uses a thin-film transistor for each pixel to control image quality and color precisely.

Hope to impliment battery unit.

CS - Chip Select, Here ILI9341 is the driver
SCK - Serial Clock
DC - Data Command Select
MOSI - Master Out Slave In, Sends data from master to the device, data in to display
MISO - Master In Slave Out, Sends data from device to master, display send data
T_IRQ - Touch Interrupt

## USING FRITZING SOFTWARE



## ONLINE REAL TIME FEATURES

- Wi-Fi scan (SSID, RSSI)
- Bluetooth scan
- SSID flooding, fake APs
- Channel analyzer, packet density monitor

## CONSTRAINTS

- No deauth frame transmission (ESP32 limitation)
- Range varies with antenna setup (50–100m)
- No cloud support (for privacy & safety)
- Ethical use required – used to test own networks

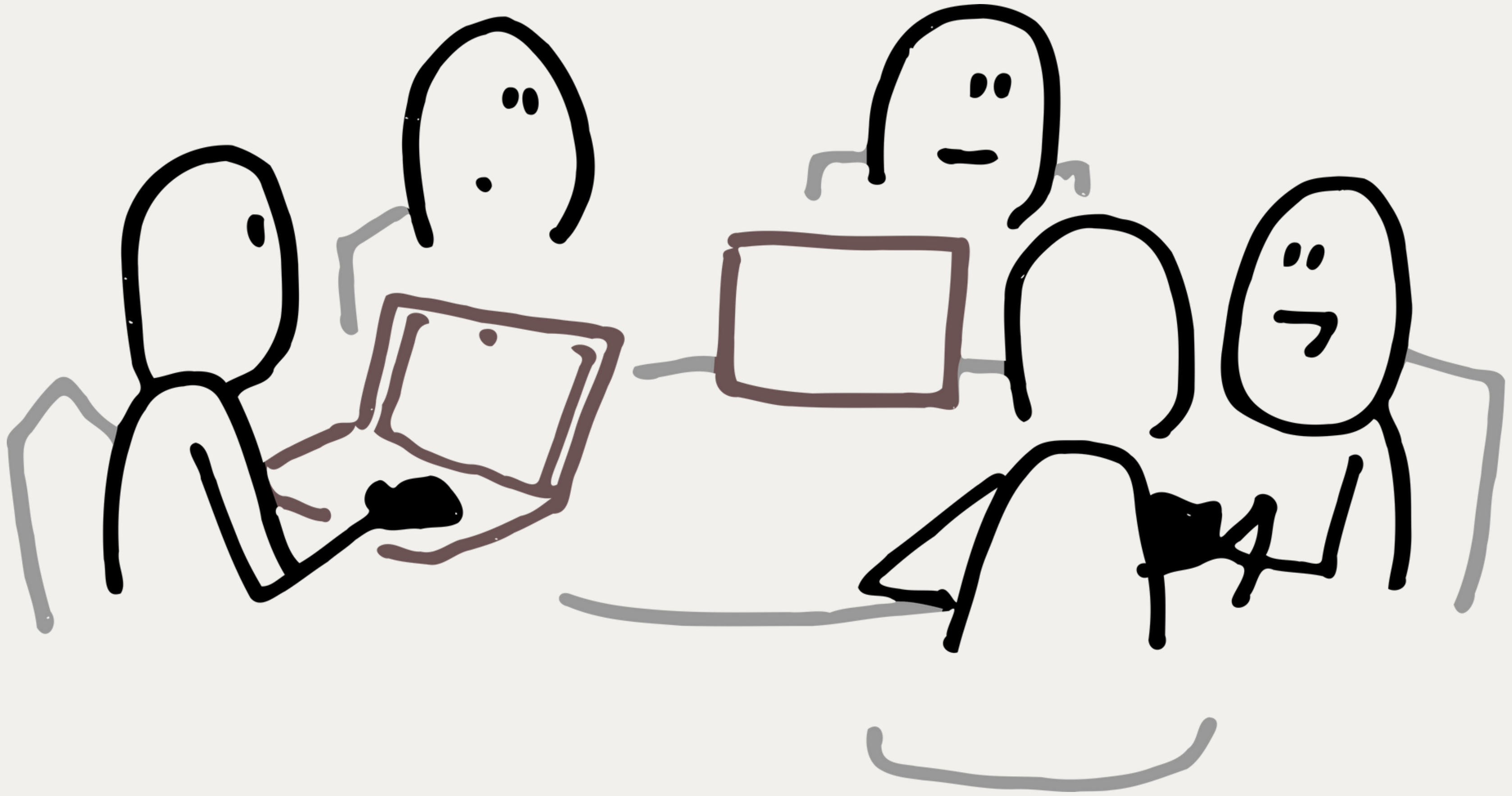
## OFFLINE ANALYSIS FEATURES

- Capture PCAP logs
- View scan logs
- Analyze via Wireshark

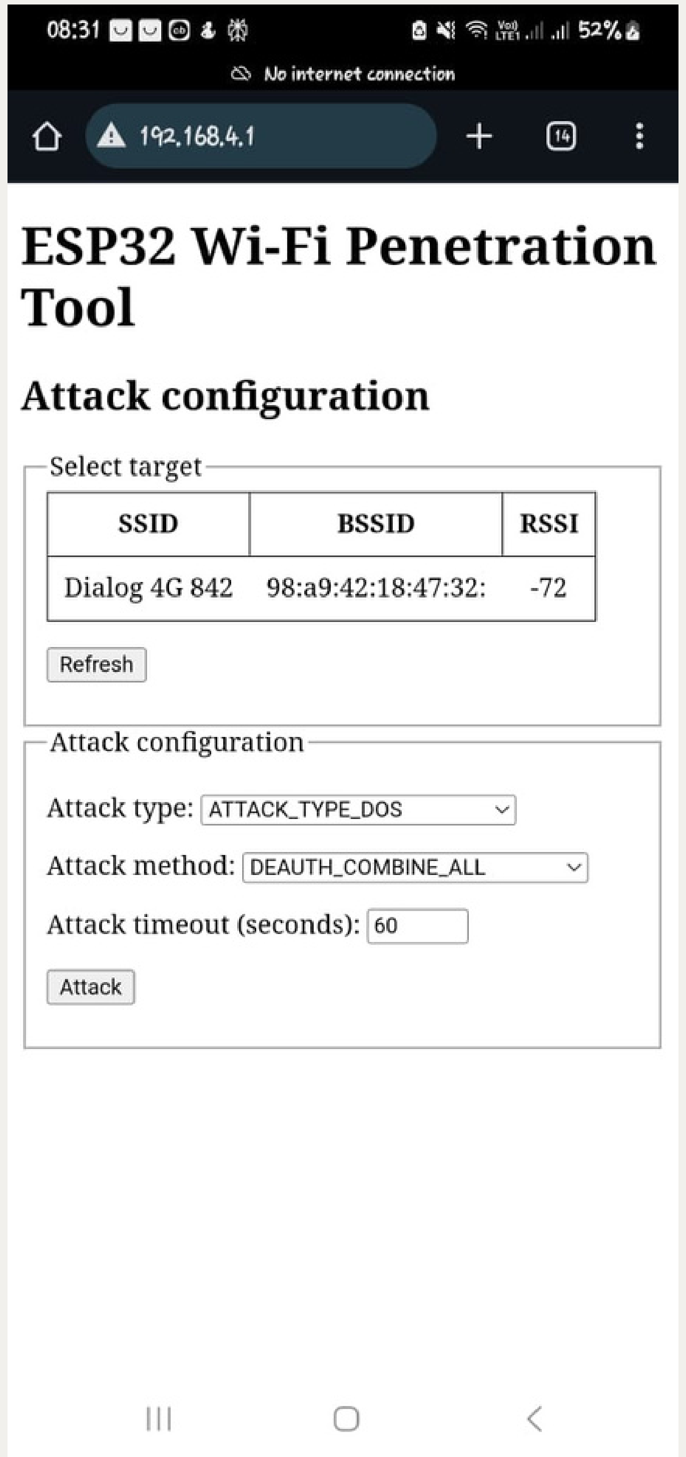
# FEATURES & CONSTRAINTS

# EXPECTED OUTCOMES

- Identify wireless vulnerabilities
- Provide recommendations for wireless security hardening
- Increase team expertise in embedded systems, wireless protocol analysis etc.



# TESTING



08:31 52%

No internet connection

192.168.4.1

## ESP32 Wi-Fi Penetration Tool

### Attack configuration

Select target

| SSID | BSSID | RSSI |
|---|---|---|
| Dialog 4G 842 | 98:a9:42:18:47:32: | -72 |

Refresh

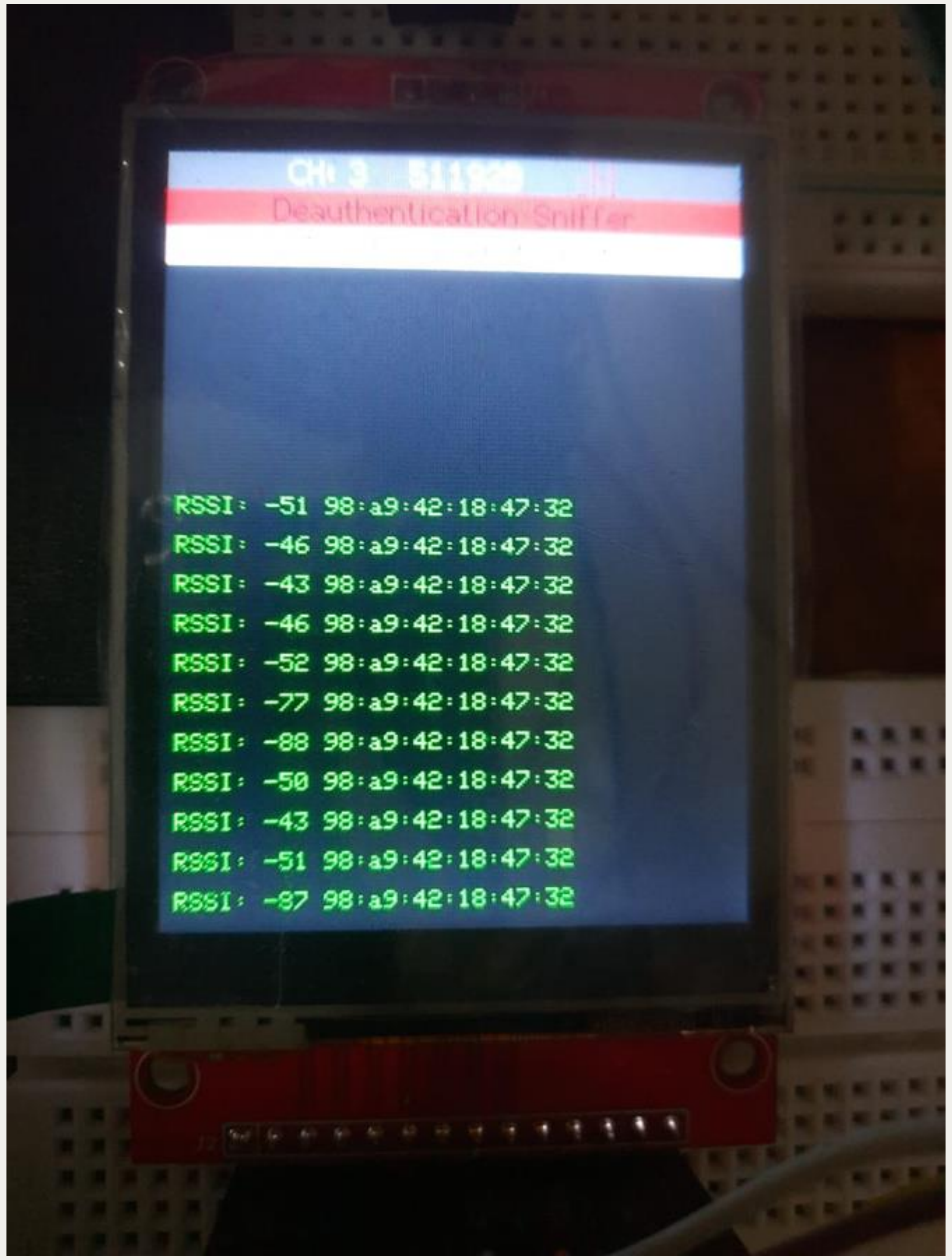
Attack configuration

Attack type: ATTACK_TYPE_DOS

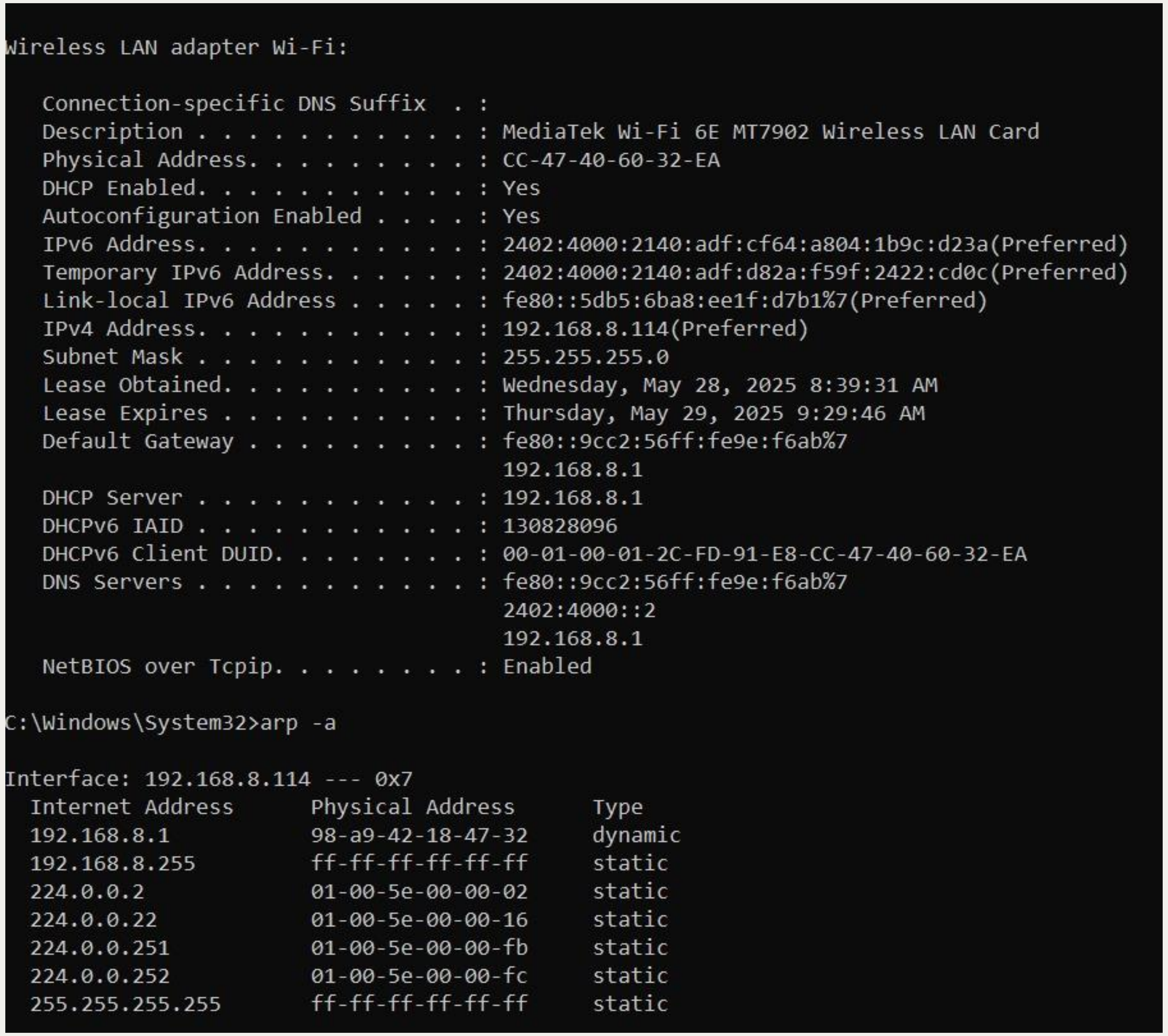
Attack method: DEAUTH_COMBINE_ALL

Attack timeout (seconds): 60

Attack



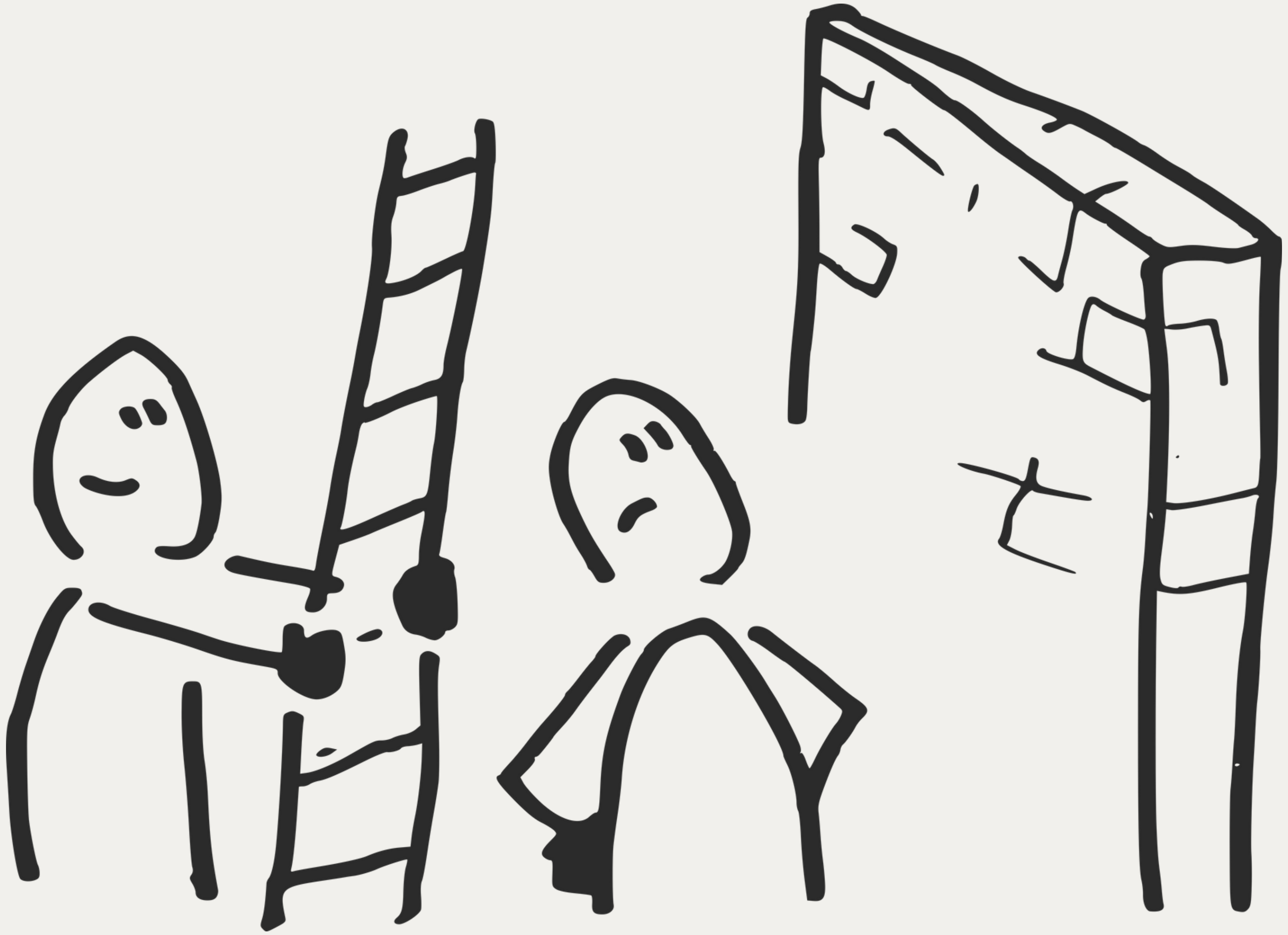
```
CH: 3  511929
Deauthentication Sniffer

RSSI: -51 98:a9:42:18:47:32
RSSI: -46 98:a9:42:18:47:32
RSSI: -43 98:a9:42:18:47:32
RSSI: -46 98:a9:42:18:47:32
RSSI: -52 98:a9:42:18:47:32
RSSI: -77 98:a9:42:18:47:32
RSSI: -88 98:a9:42:18:47:32
RSSI: -50 98:a9:42:18:47:32
RSSI: -43 98:a9:42:18:47:32
RSSI: -51 98:a9:42:18:47:32
RSSI: -87 98:a9:42:18:47:32
```



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : MediaTek Wi-Fi 6E MT7902 Wireless LAN Card
   Physical Address. . . . . . . . . : CC-47-40-60-32-EA
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2402:4000:2140:adf:cf64:a804:1b9c:d23a(Preferred)
   Temporary IPv6 Address. . . . . . : 2402:4000:2140:adf:d82a:f59f:2422:cd0c(Preferred)
   Link-local IPv6 Address . . . . . : fe80::5db5:6ba8:ee1f:d7b1%7(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.8.114(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, May 28, 2025 8:39:31 AM
   Lease Expires . . . . . . . . . . : Thursday, May 29, 2025 9:29:46 AM
   Default Gateway . . . . . . . . . : fe80::9cc2:56ff:fe9e:f6ab%7
                                       192.168.8.1
   DHCP Server . . . . . . . . . . . : 192.168.8.1
   DHCPv6 IAID . . . . . . . . . . . : 130828096
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2C-FD-91-E8-CC-47-40-60-32-EA
   DNS Servers . . . . . . . . . . . : fe80::9cc2:56ff:fe9e:f6ab%7
                                       2402:4000::2
                                       192.168.8.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Windows\System32>arp -a

Interface: 192.168.8.114 --- 0x7
  Internet Address      Physical Address      Type
  192.168.8.1           98-a9-42-18-47-32     dynamic
  192.168.8.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

# WHAT'S NEXT

- Implementing the battery to use as a portable device
- Enclosure setup
- Implementation of further Bluetooth capabilities
- Evil portal attacks and PCAP file analyzing on Wireshark



# CONCLUSION

- ESP32 PEN tool is a powerful, low-cost solution for real-time wireless security assessment.
- Designed for education, ethical hacking, and research.
- Expandable, customizable, and user-friendly.
- A practical embedded systems project with real-world applications.

# THANK YOU!