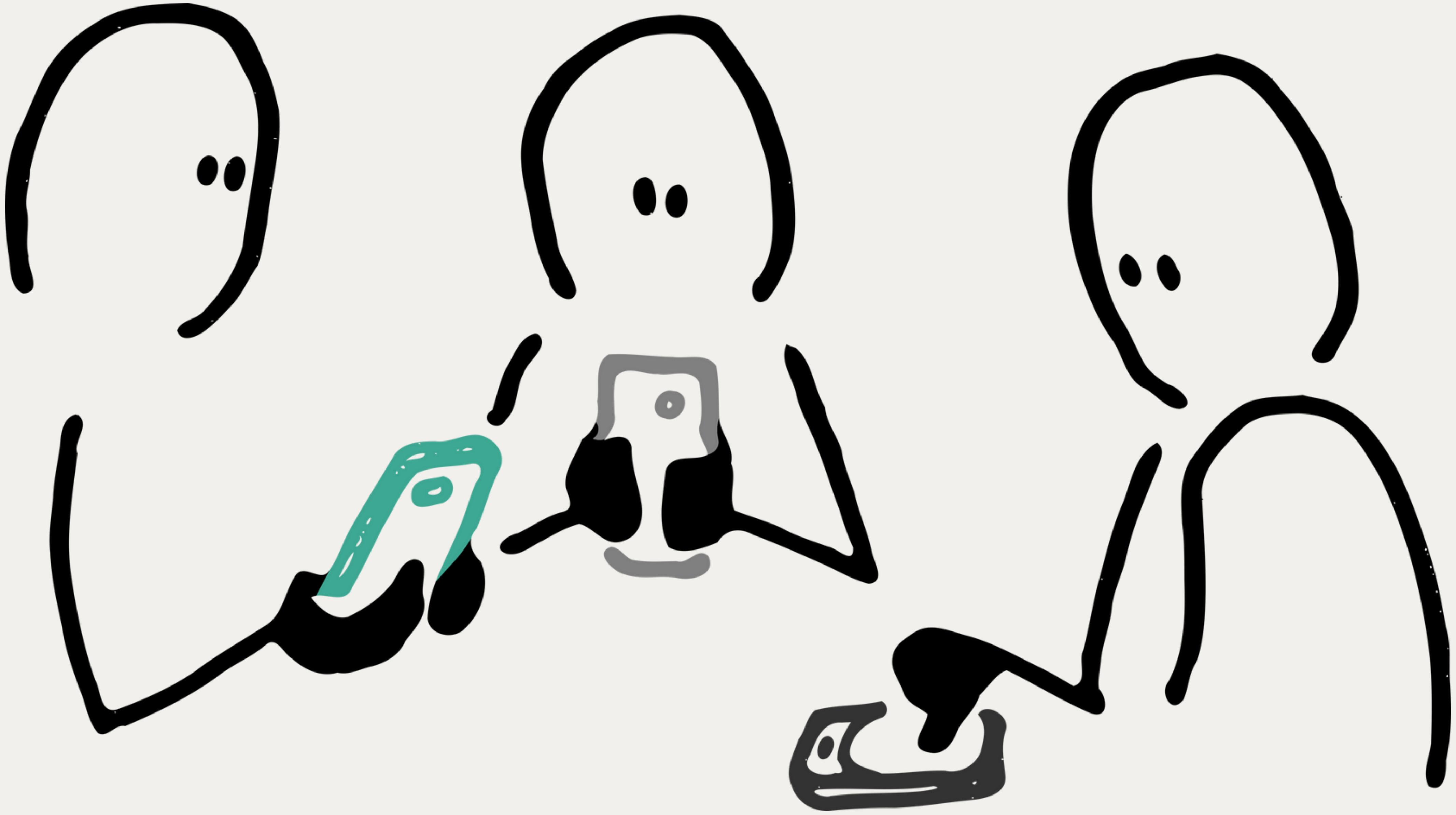
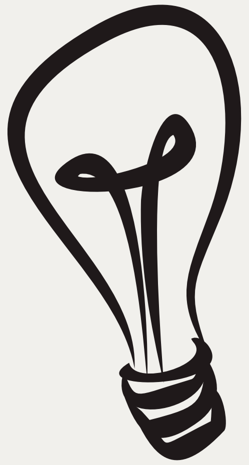
GROUP 10

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**

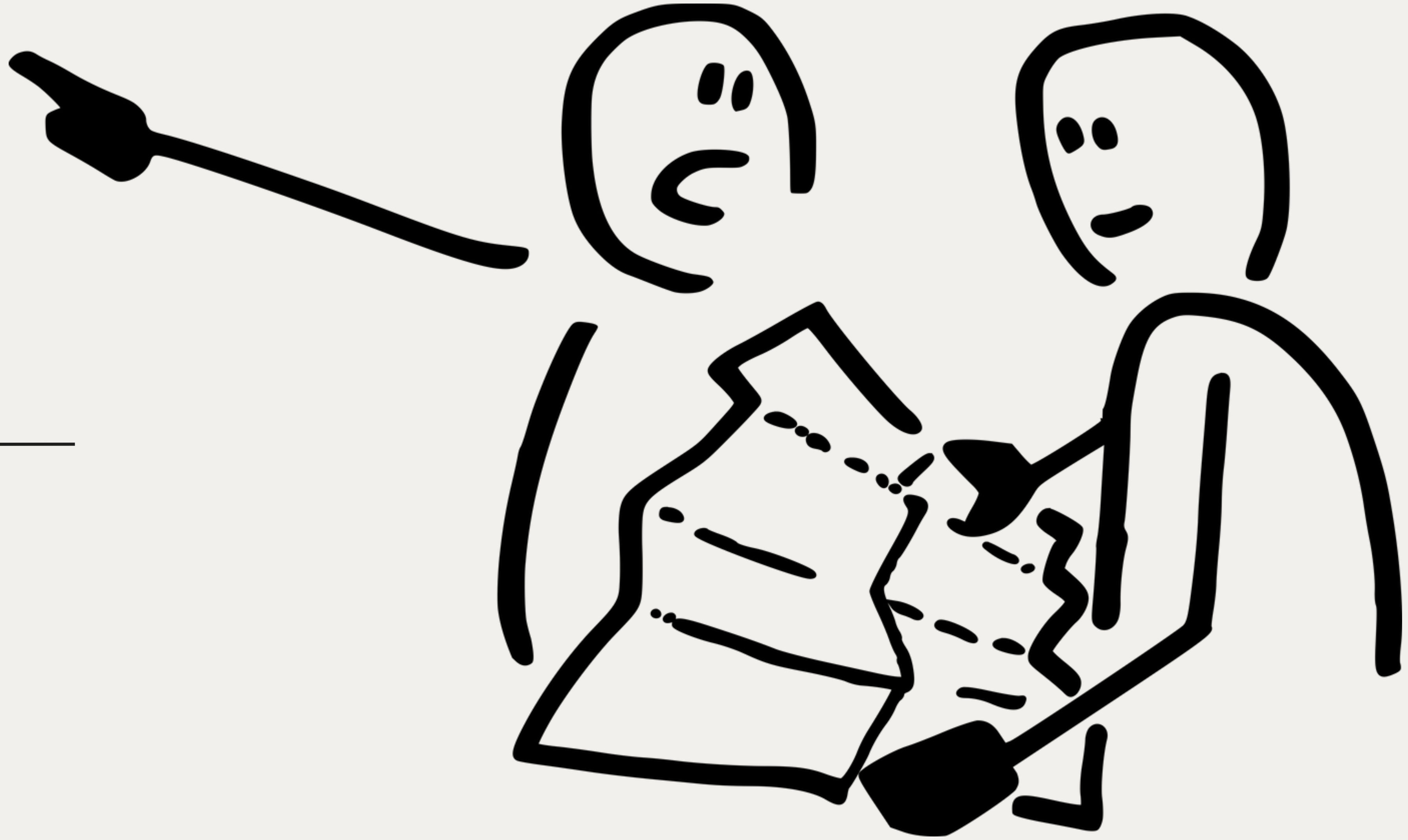
through a user-friendly interface.

PROBLEM STATEMENT

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

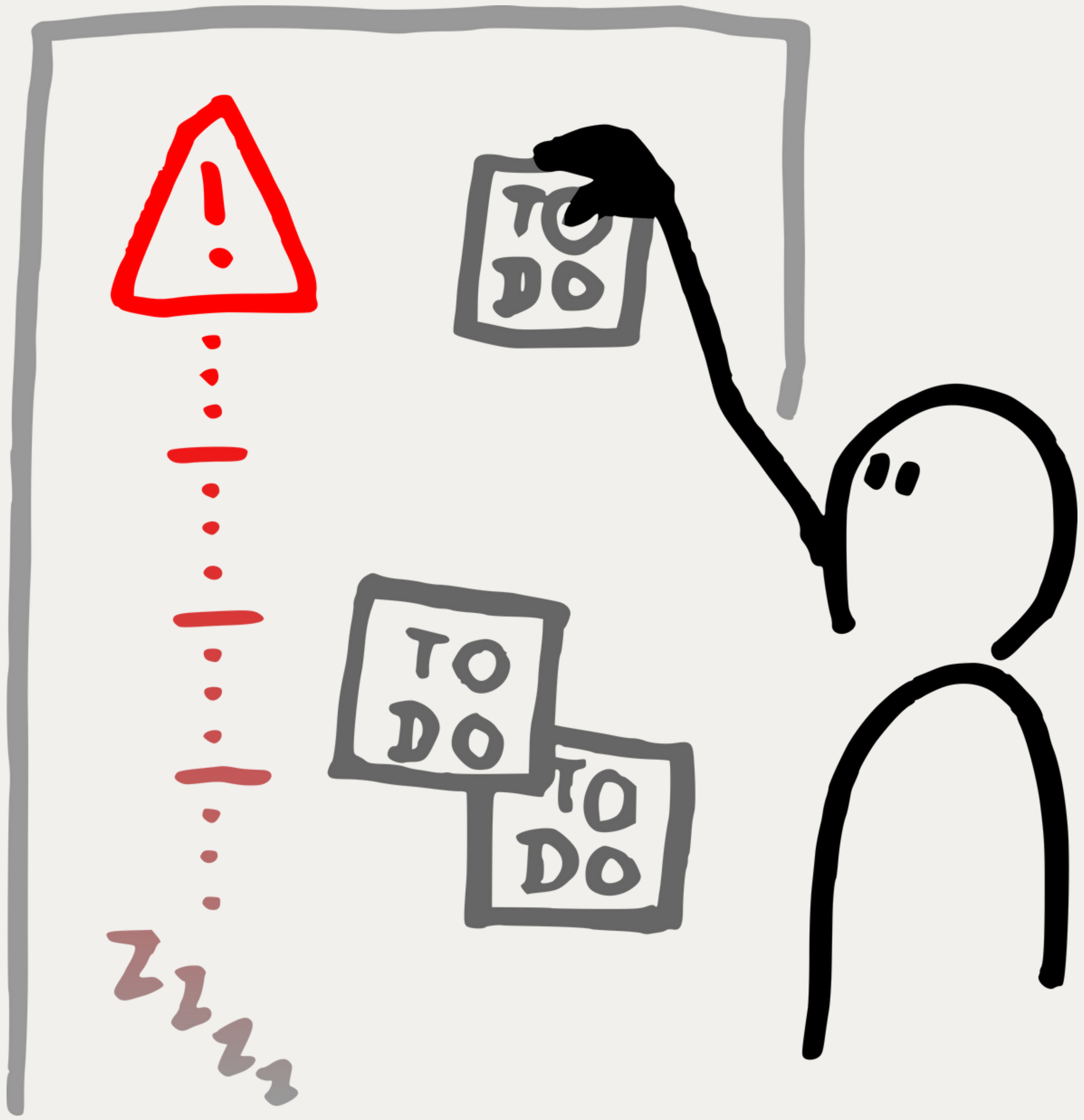
OBJECTIVE

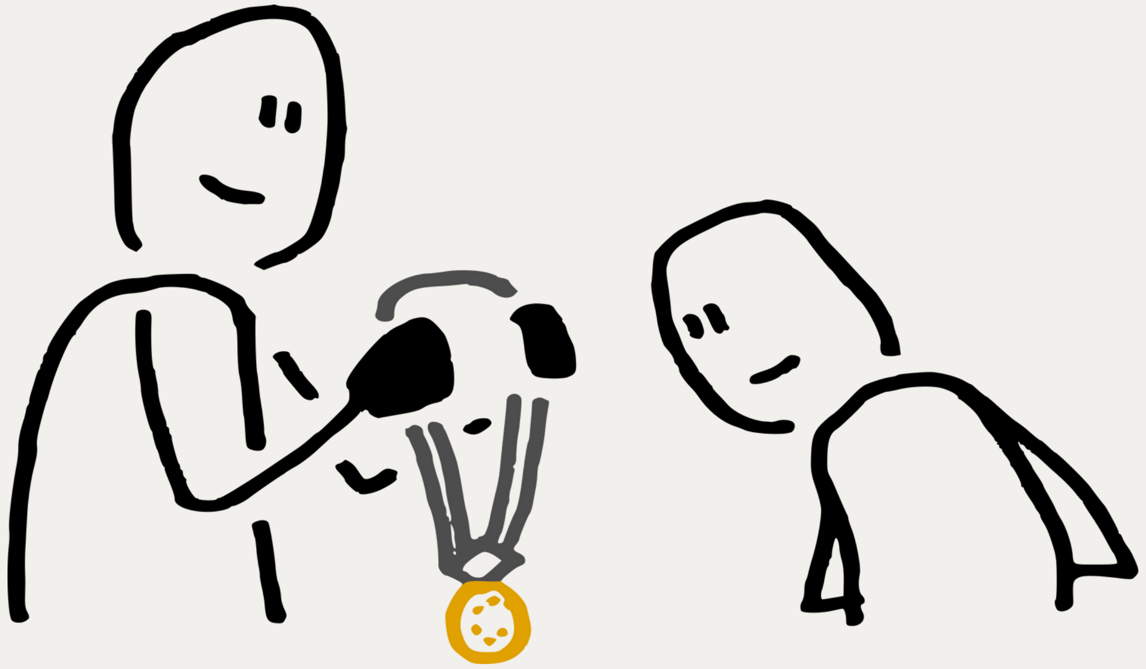
- To develop a secure, portable Wi-Fi/Bluetooth penetration testing tool that works in noisy and high-traffic environments using ESP32, enhanced for reliability, and controlled via an intuitive touch interface.



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

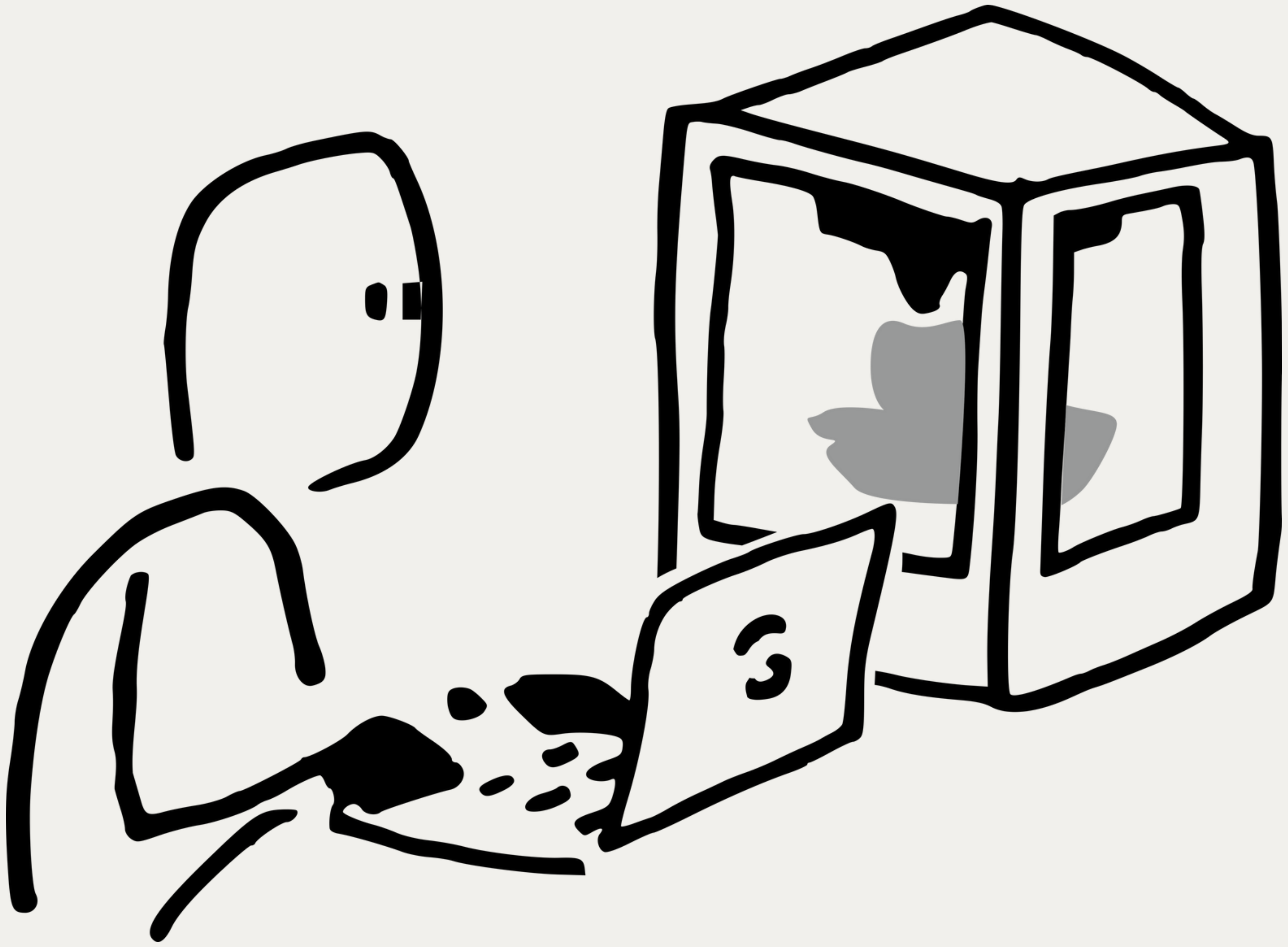
- Bluetooth scanner
- BLE shutdown
- Skimmer detection
- Probe and beacon sniffing
- Pwnagotchi/Espressif Detection

UI/UTILITIES

- TFT GUI
- Touch navigation
- OTA/SD firmware updates
- PCAP logging

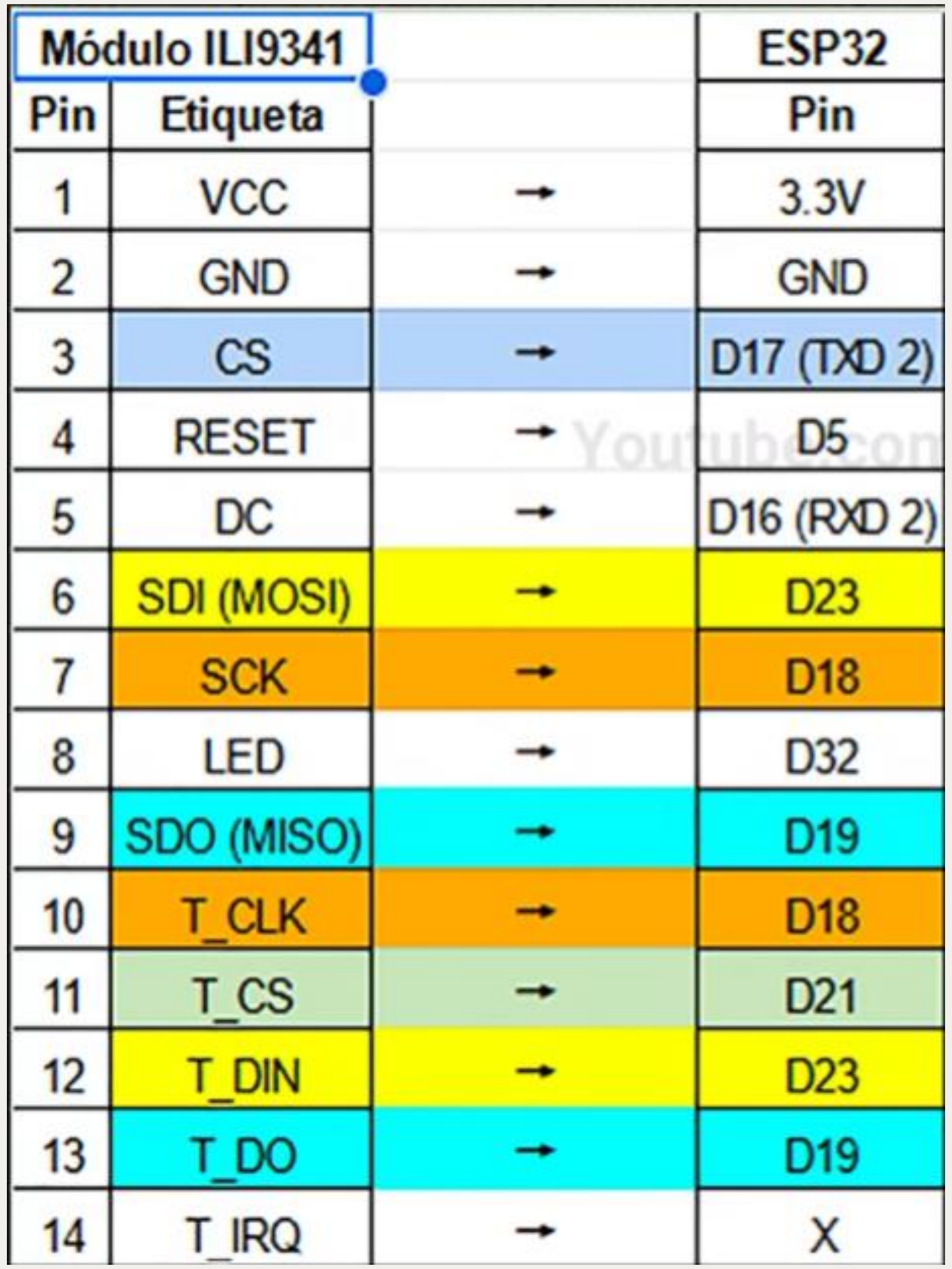
KEY COMPONENTS

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



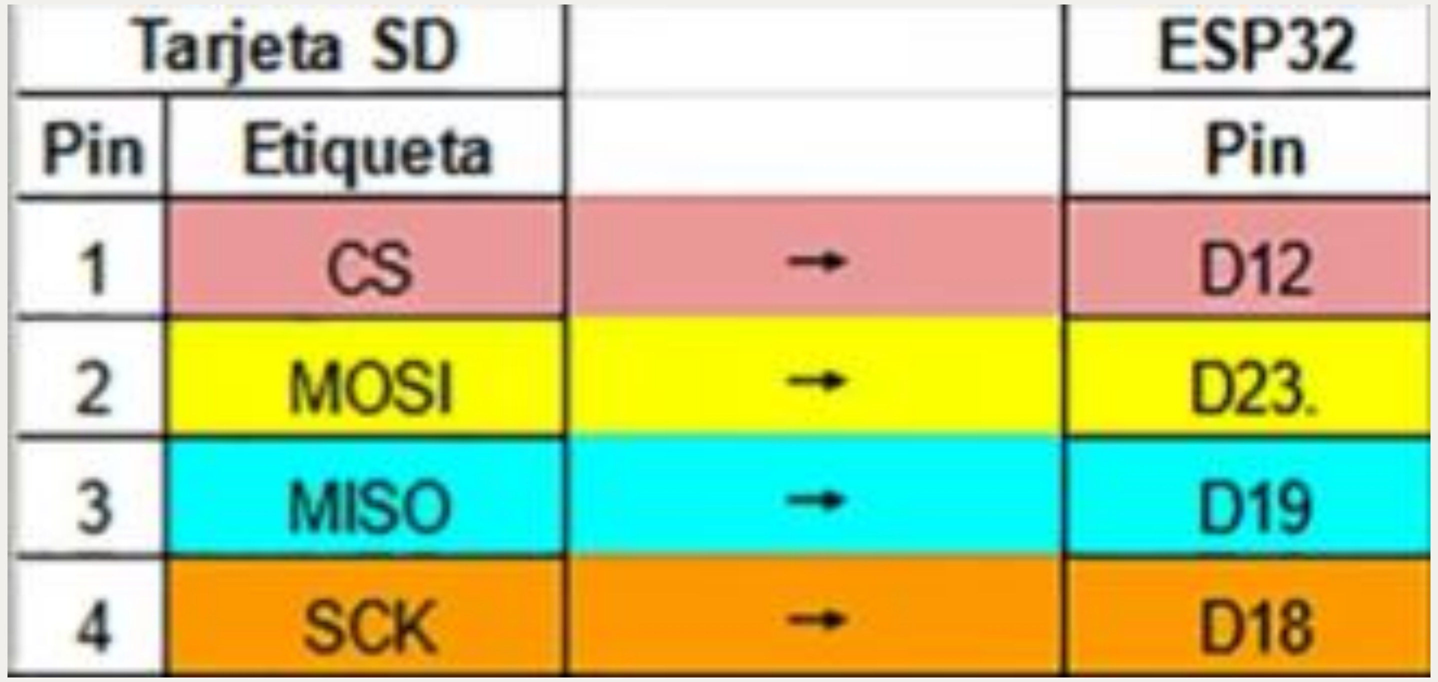
PIN CONNECTIONS

TOUCH SCREEN DISPLAY



Módulo ILI9341			ESP32
Pin	Etiqueta		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	→	X

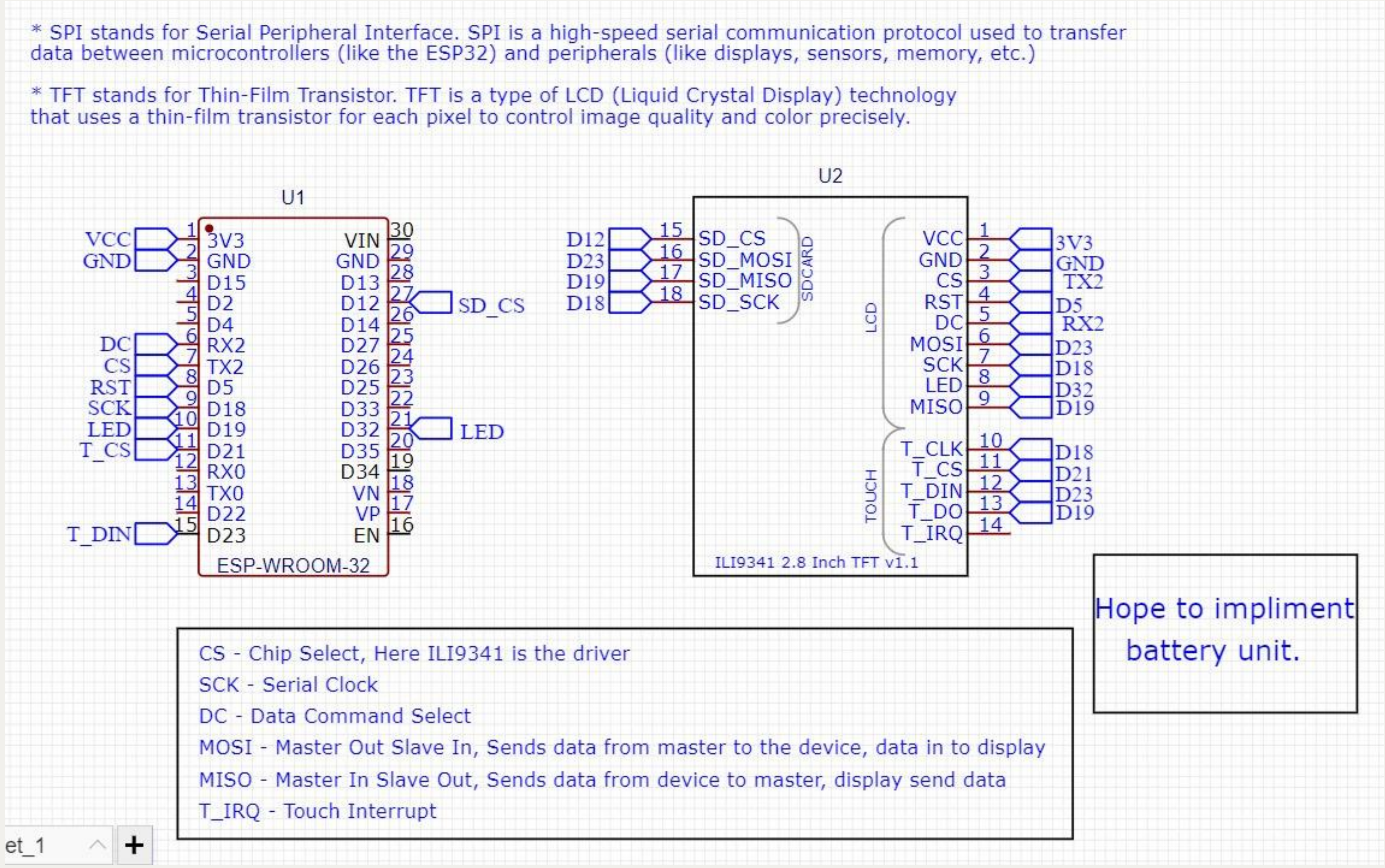
SD CARD MODULE



Tarjeta SD			ESP32
Pin	Etiqueta		Pin
1	CS	→	D12
2	MOSI	→	D23.
3	MISO	→	D19
4	SCK	→	D18

SCHEMATIC OF THE CIRCUIT

USING EASY EDA SOFTWARE



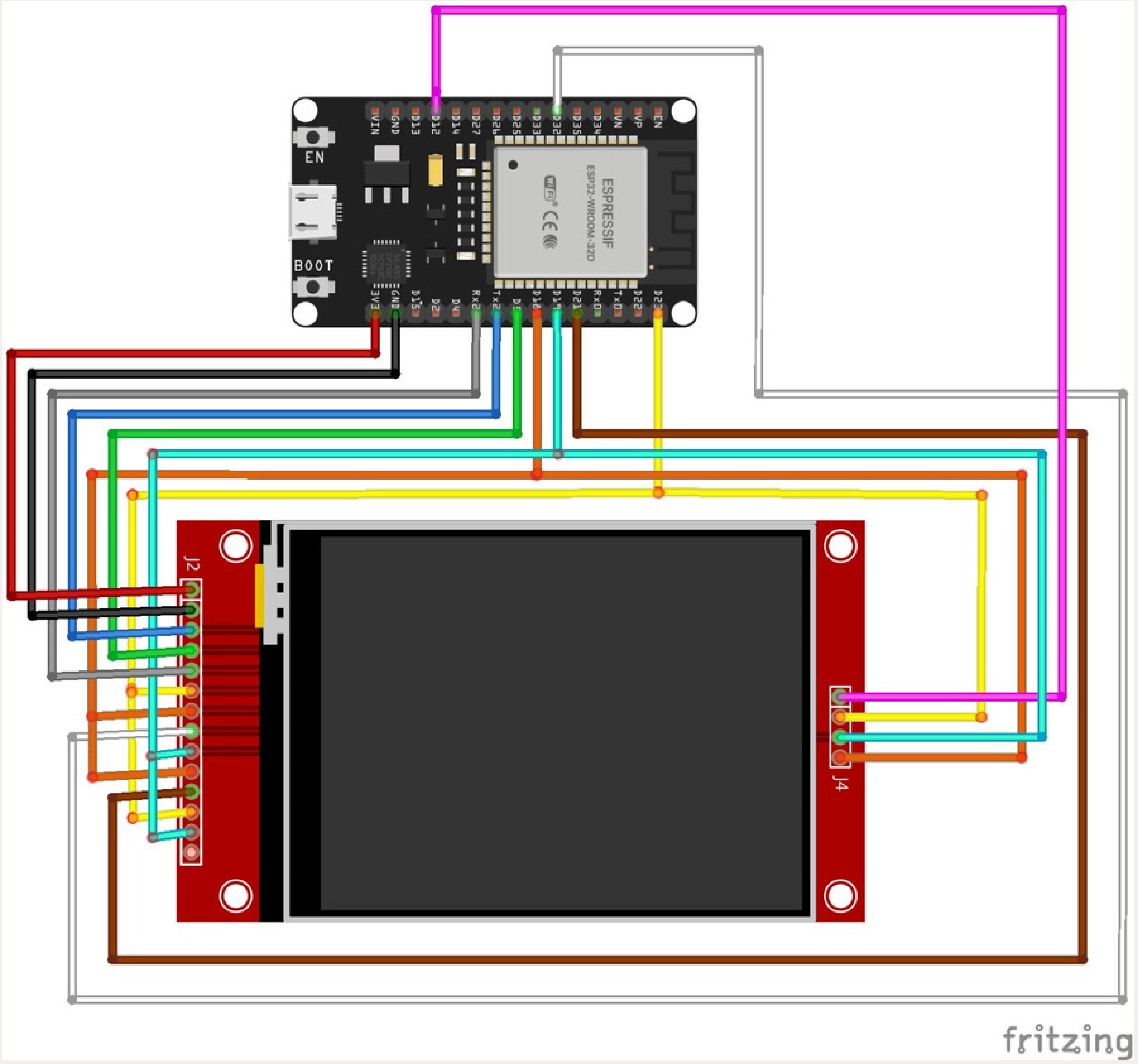
* SPI stands for Serial Peripheral Interface. SPI is a high-speed serial communication protocol used to transfer data between microcontrollers (like the ESP32) and peripherals (like displays, sensors, memory, etc.)

* 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, encryption)
- Bluetooth scan (Classic + BLE)
- 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 – follows local cyber laws

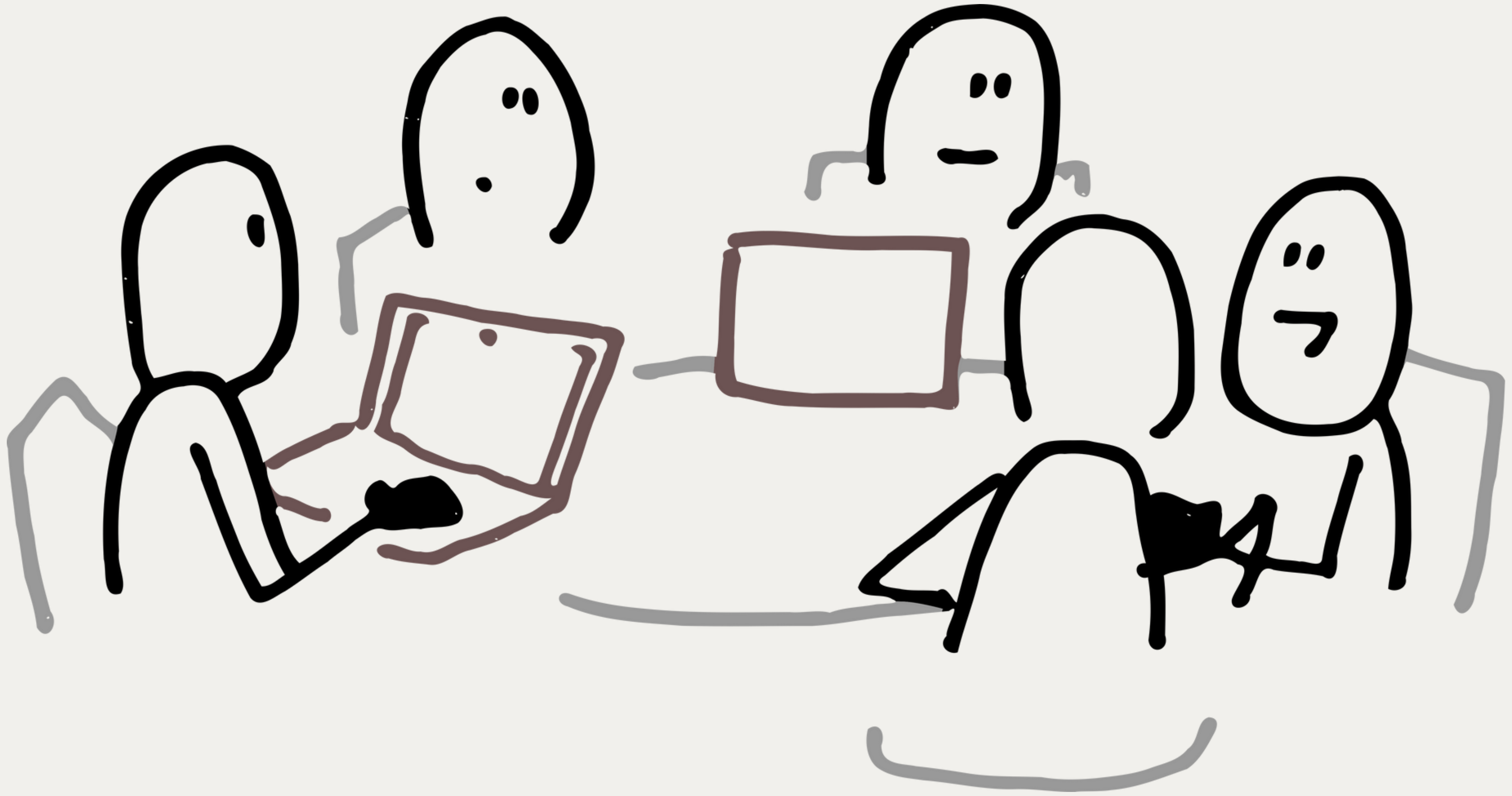
OFFLINE ANALYSIS FEATURES

- 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.



CONCLUSION

- ESP32 Marauder 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!