



只要一張小朋友：
利用樹莓派打造物聯網攻擊工具

—— HackMaster Pi

📌 1Ping Sun





在開始之前

本專案及今
任何違法行
請務必在合
依據刑法第
統、竊取資
責任。

技術能力越
所分享的知



禁止用於
。
入侵他人系
面臨刑事

應用今日

目錄



- 關於我
- 關於 HackMaster Pi
- 功能展示
- 製作步驟
- 結尾



關於我

- 臺北市數位實驗高中高二
-



關於 HackMaster Pi



- 以低成本學習物聯網的攻擊與防禦
- 包含藍牙、Wi-Fi、紅外線、RFID、USB 等相關工具
- 使用 Raspberry Pi Zero 2 W

[成品照片](#)

關於 HackMaster Pi



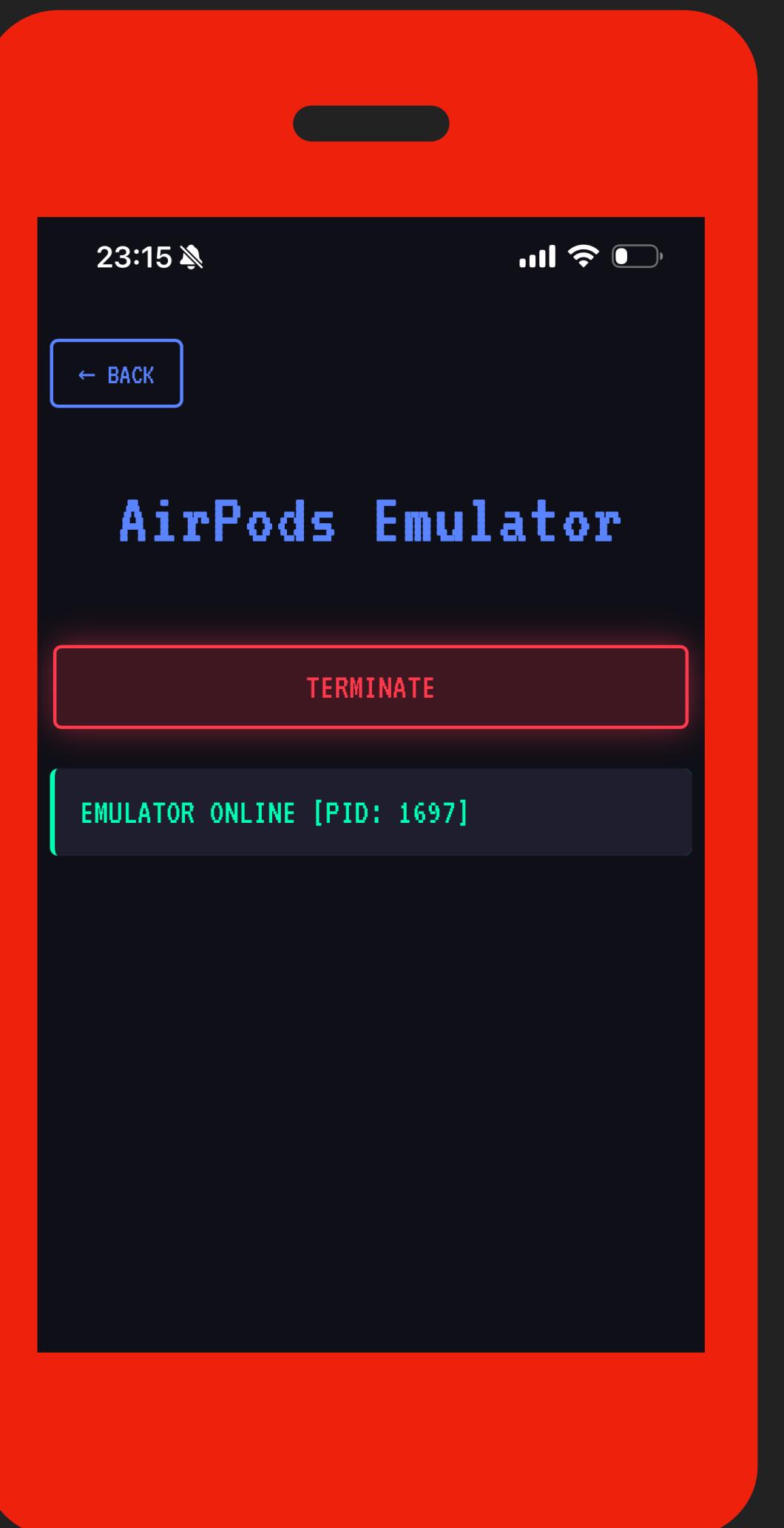
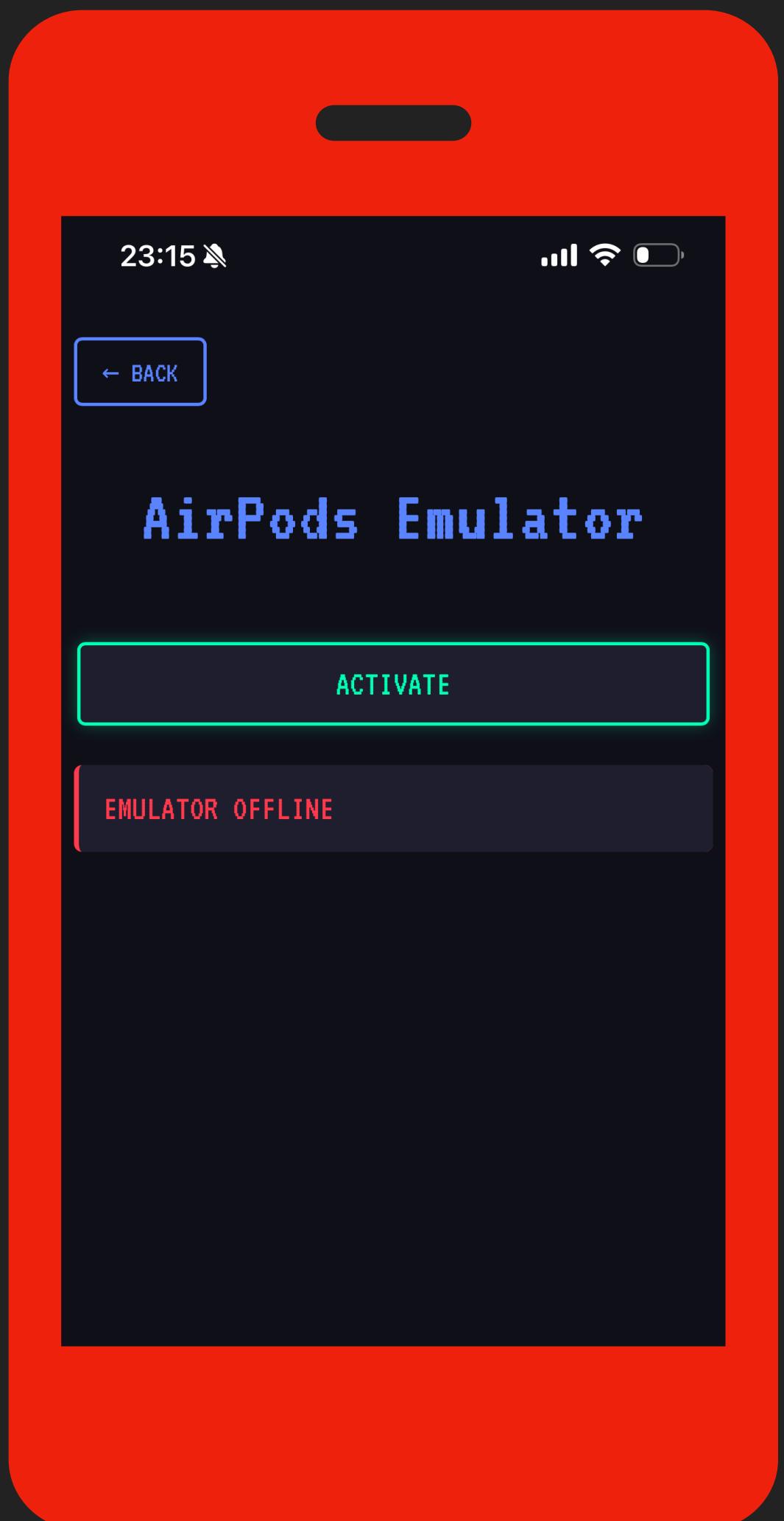
	HackMaster Pi	CapibaraZero	Flipper Zero
運算速度	1 GHz	160 Mhz	64 MHz
價錢	\$15	\$9.99	\$169
藍芽	\$0	\$0	\$0
Wi-Fi	\$0	\$0	\$29
紅外線	\$3	\$3	\$0
125 KHz RFID	\$2	\$2	\$0
13.56 MHz RFID	\$9	\$9	\$0
SubGHz	\$9	\$9	\$0
總計	\$38	\$32.99	\$198





功能展示

Fake Airpods



圖片來源：<https://support.apple.com/zh-tw/104989>

BLE Beacon Emulate



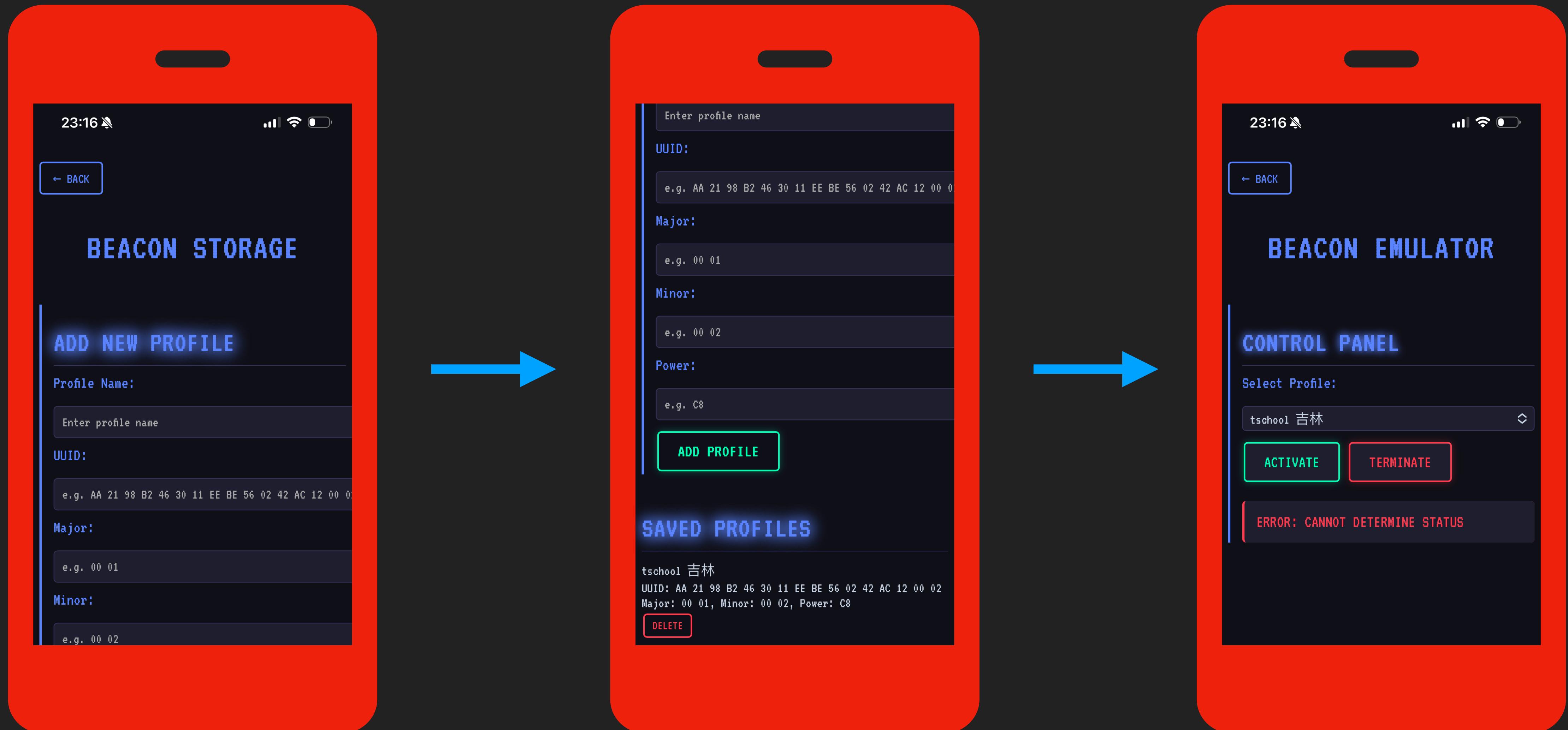
The diagram illustrates the workflow for emulating a BLE Beacon using a mobile application.

Left Screen (Initial State): Shows the app interface at 11:29. It displays a QR code with the identifier "918767" and the text "到離校打卡". Below it, it says "目前所在區域" (Current Location Area) and "持續掃描中...10". It lists the "到校有效打卡時間" (Attendance Effective Time) as "上午 07:30 ~ 08:25" and "下午 11:00 ~ 13:25". It includes two buttons: "到校打卡" (Check-in) and "離校打卡" (Check-out). At the bottom, there are "掃描代碼" (Scan Code) and "輸入驗證碼" (Enter Verification Code) buttons. The date "Mar 31, 2025" is shown in the bottom right. A red arrow points from this screen to the central photograph.

Central Photograph: A Realtek RL400 BLE Beacon device is shown on a wooden surface. The device is white with a blue "Beacon" logo and a blue Wi-Fi signal icon above it. It has a small screen displaying "Realtek RL400 BLE Beacon" and some MAC address information. In the background, there is a tablet displaying a QR code and a bag of snacks.

Right Screen (Final State): Shows the app interface at 23:29. It displays a QR code with the identifier "918767" and the text "到離校打卡". Below it, it says "目前所在區域" (Current Location Area) and "持續掃描中...2". It lists the "到校有效打卡時間" (Attendance Effective Time) as "上午 07:30 ~ 08:25" and "下午 11:00 ~ 13:25". It includes two buttons: "到校打卡" (Check-in) and "離校打卡" (Check-out). At the bottom, there are "掃描代碼" (Scan Code) and "輸入驗證碼" (Enter Verification Code) buttons. The date "Apr 9, 2025" is shown in the bottom right. A red arrow points from the central photograph to this screen.

BLE Beacon Emulate



BLE Beacon Emulate



The screenshot shows a web application interface for BLE Beacon Emulation on the left and the Chrome DevTools Sources tab on the right.

Left Side (BLE Beacon Emulation Interface):

- Top Bar:** 持續掃描中...2
- Current Location:** 目前所在區域
- Attendance Time Range:** 到校有效打卡時間
上午 07:30 ~ 08:25
下午 11:00 ~ 13:25
- Buttons:** 到校打卡, 離校打卡
- Scanning Area:** 捕捉到的 Beacons:
 - REALINK_RL400_V100 (弘道基地) - AA219420-4630-11EE-BE56-0242AC120002, EA:AE:00:00:0B:00
 - REALINK_RL400_V100 (吉林基地) - AA2198B2-4630-11EE-BE56-0242AC120002, EA:AE:00:00:0B:01
- Attendance Record:** 打卡記錄
到校打卡 吉林基地 10:09:53

Right Side (Chrome DevTools Sources Tab):

- Page:** index-DSUzjDtM.js
- Sources:** index-DzEv45s9.js (Selected)
- Code Preview:** Shows JavaScript code defining two beacon objects: one for "REALINK_RL400_V100" (弘道基地) and one for "REALINK_RL400_V100" (吉林基地). Both have the same UUID and MAC address, but different names.

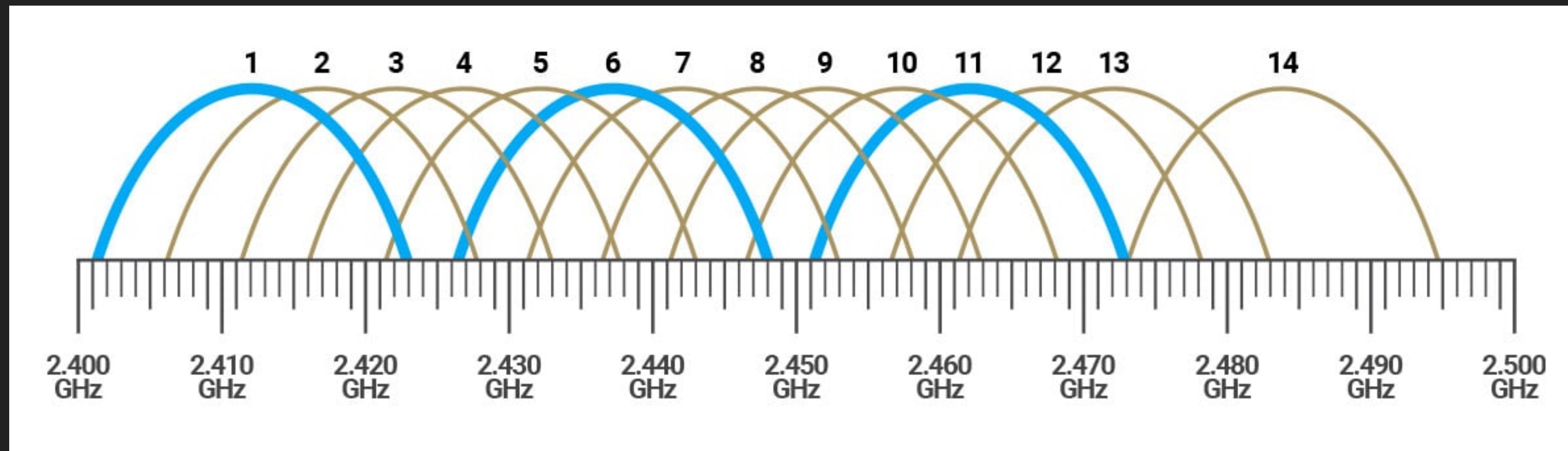
```
const A = [
  {
    identifier: "REALINK_RL400_V100",
    name: "弘道基地",
    uuid: "AA219420-4630-11EE-BE56-0242AC120002",
    mac: "EA:AE:00:00:0B:00"
  },
  {
    identifier: "REALINK_RL400_V100",
    name: "吉林基地",
    uuid: "AA2198B2-4630-11EE-BE56-0242AC120002",
    mac: "EA:AE:00:00:0B:01"
  }
];
```
- Breakpoints:** Paused at Line 1, Column 2459.
- Scope:** Not paused.

Rickroll Wi-Fi



- // 操作步驟

Rickroll Wi-Fi



圖片來源：<https://wattbrother.com/276521>

Rickroll Wi-Fi



示例封包 (16進位表示)

假設 SSID 為 "Never Gonna"，頻道為 1，隨機 MAC 為 `12:34:56:78:9a:bc`，封包可能如下（簡化版）：

text

× 收起 ⌕ 換行 Ⓛ 複製

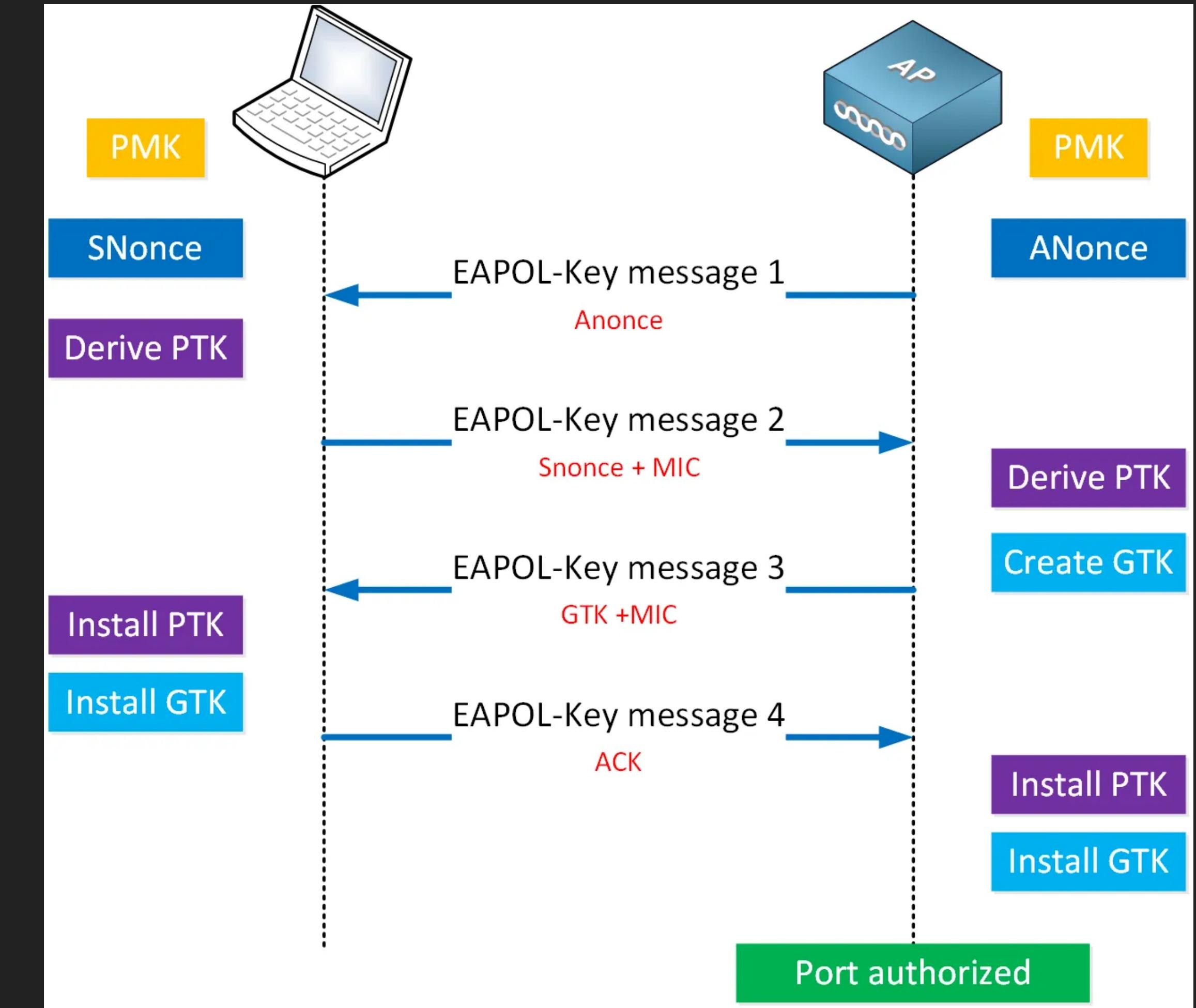
```
RadioTap: 00 18 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
Dot11:    80 00 00 00 ff ff ff ff ff ff 12 34 56 78 9a bc 12 34 56 78 9a bc 00 00  
Beacon:   00 00 00 00 00 00 00 64 00 01 00  
SSID:     00 0b 4e 65 76 65 72 20 47 6f 6e 6e 61
```

- **總長度**：約 50-60 位元組（取決於 `RadioTap` 頭部長度）。
- **內容解釋**：
 - `80 00`：信標框架。
 - `ff ff ff ff ff ff`：廣播地址。
 - `12 34 56 78 9a bc`：隨機 MAC（兩次出現，分別為 addr2 和 addr3）。
 - `00 0b`：SSID 長度 (11)。
 - `4e 65 ... 61`："Never Gonna" 的 ASCII 編碼。

Wi-Fi Password Cracker



- 名詞解釋
 - PSK (pre-share key)
 - 4-Way Handshake



圖片來源：<https://networklessons.com/wp-content/uploads/2023/12/wpa-4-way-handshake-workflow.png>

Wi-Fi Password Cracker



- 安全協議
 - WEP : RC4
 - WPA : RC4 + TKIP
 - WPA2 : AES (128 bits)
 - WPA3 : SAE (256 bits)

Wi-Fi Password Cracker



- 攻擊手法
 - WEP、WPA：爆破 RC4 加密取得 PSK
 - WPA2：使用字典檔或窮舉，離線暴力破解取得 PSK
 - WPA3：降級攻擊、主動式爆破

Wi-Fi Password Cracker



- 防禦方式
 - 高強度密碼
 - 關閉混合模式



<https://reurl.cc/LapRe4>

Wi-Fi Password Cracker



- // 操作步驟

IR Enumerate



- // 操作步驟

BadUSB



- // 操作步驟

MITM USB



- // 操作步驟

專案資源



<https://hackmasterpi.org>



[https://github.com/
1PingSun/HackMaster-Pi](https://github.com/1PingSun/HackMaster-Pi)

Thank you

Contact

- Email: sunyipingtw@icloud.com
- GitHub: <https://github.com/1PingSun>
- Blog: <https://1ping.org/>

