



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



- HackMaster Pi 作者
- 臺北市數位實驗高中高一
-



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



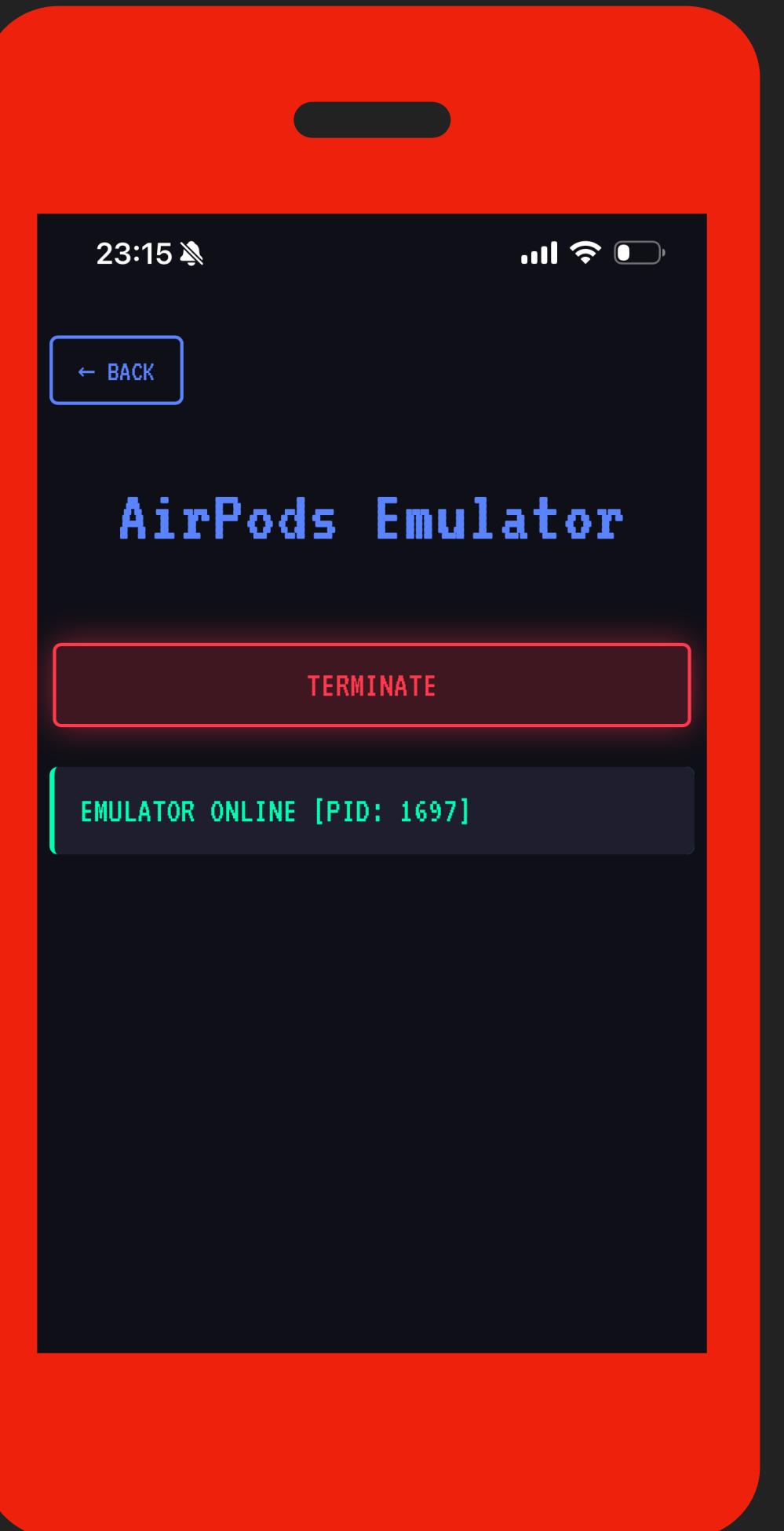
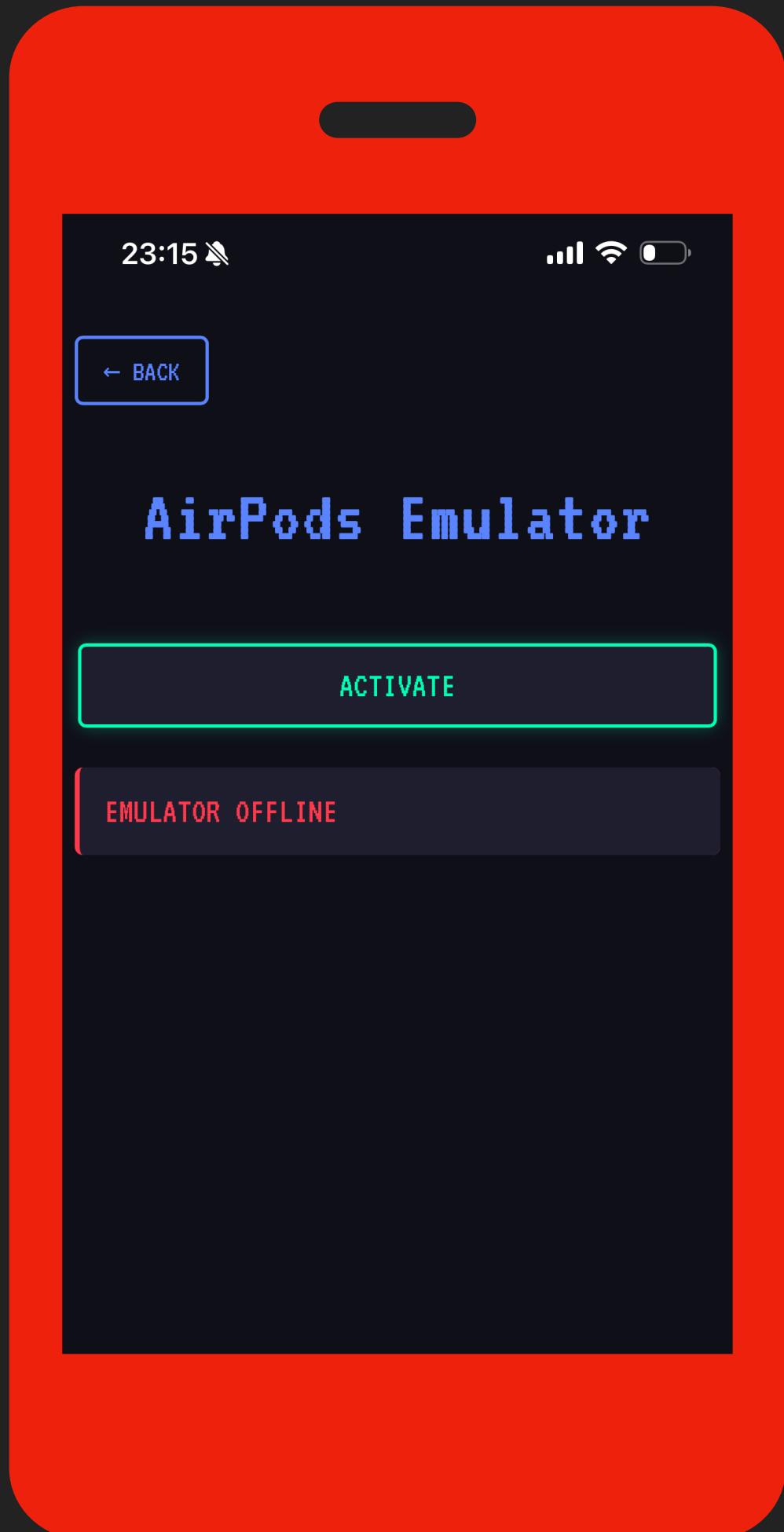
	HackMaster Pi	CapibaraZero	Flipper Zero
運算速度	1 GHz	160 Mhz	64 MHz
價錢	\$15	\$9.99	\$169
藍芽	\$0	\$0	\$0
Wi-Fi	\$0	\$0	\$29
紅外線	\$3	\$3	\$0
13.56 MHz RFID	\$9	\$9	\$0
總計	\$27	\$21.99	\$198





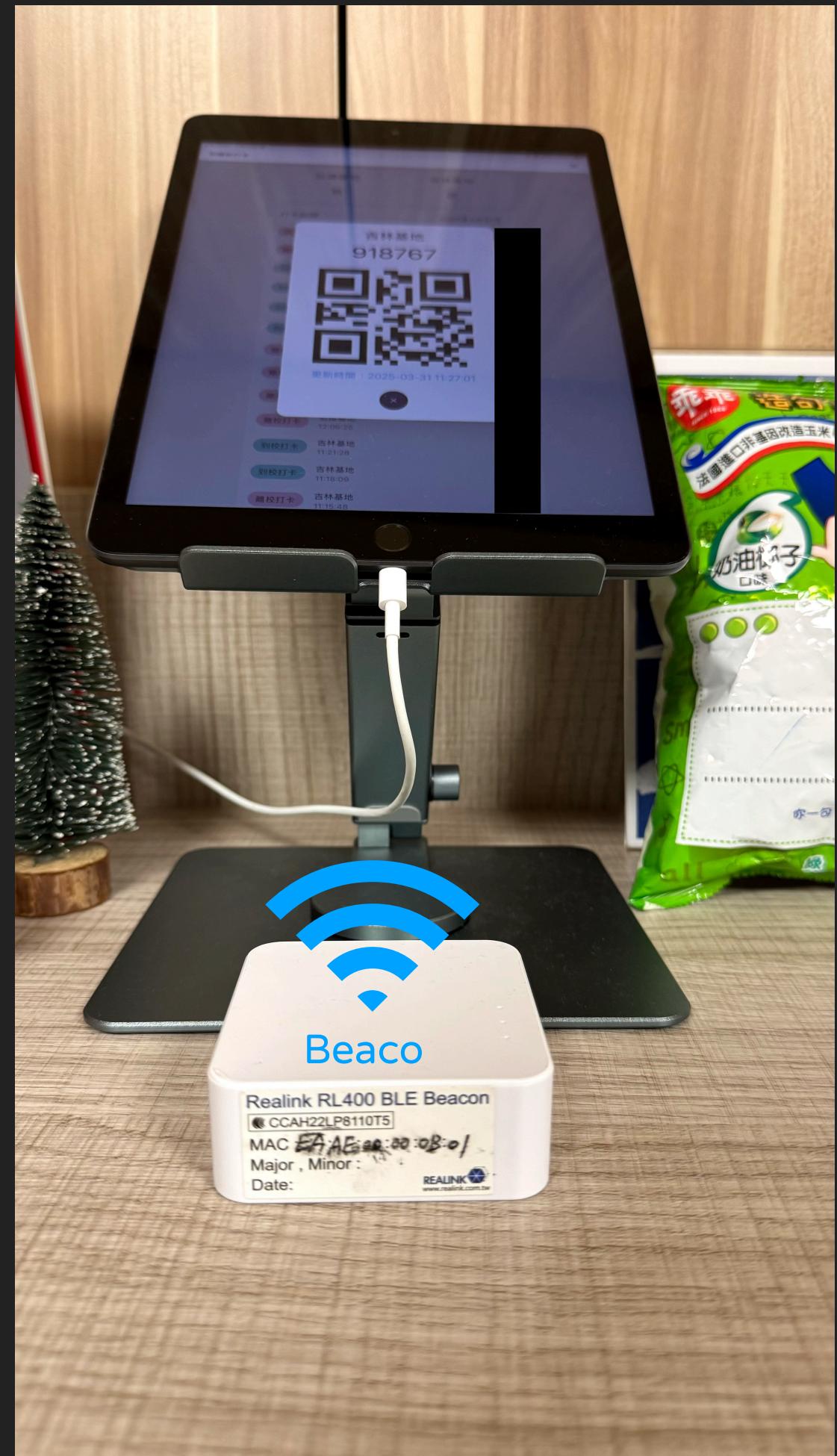
功能展示

Fake Airpods

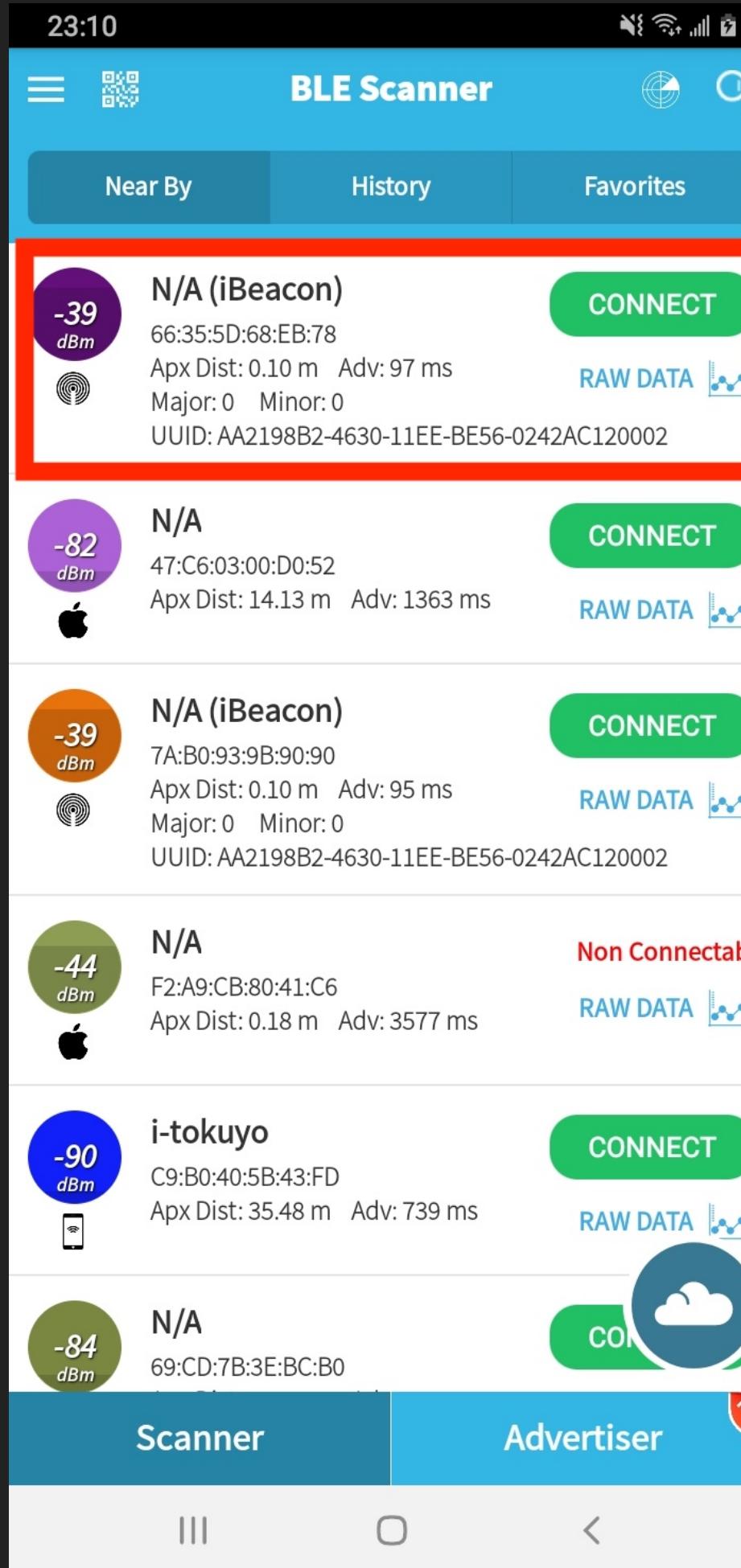


圖片來源：<https://support.apple.com/zh-tw/104989>

BLE Beacon Emulate



BLE Beacon Emulate



```
const A = [
  {
    identifier: "REALINK_RL400_V100",
    name: "弘道基地",
    uuid: "AA2198B2-4630-11EE-BE56-0242AC120002",
    mac: "EA:AE:00:00:0B:01"
  },
  {
    identifier: "REALINK_RL400_V100",
    name: "吉林基地",
    uuid: "AA219420-4630-11EE-BE56-0242AC120002",
    mac: "EA:AE:00:00:0B:01"
  }
];
```

The screenshot shows the browser's developer tools open to the 'Sources' tab, displaying the code for 'index-DzEv45s9.js'. The code defines an array 'A' containing two objects. Each object has properties for identifier, name, uuid, and mac. The identifiers and names are identical for both objects, while the uuids and macs differ slightly. The code is annotated with red boxes highlighting the 'identifier', 'name', 'uuid', and 'mac' fields.

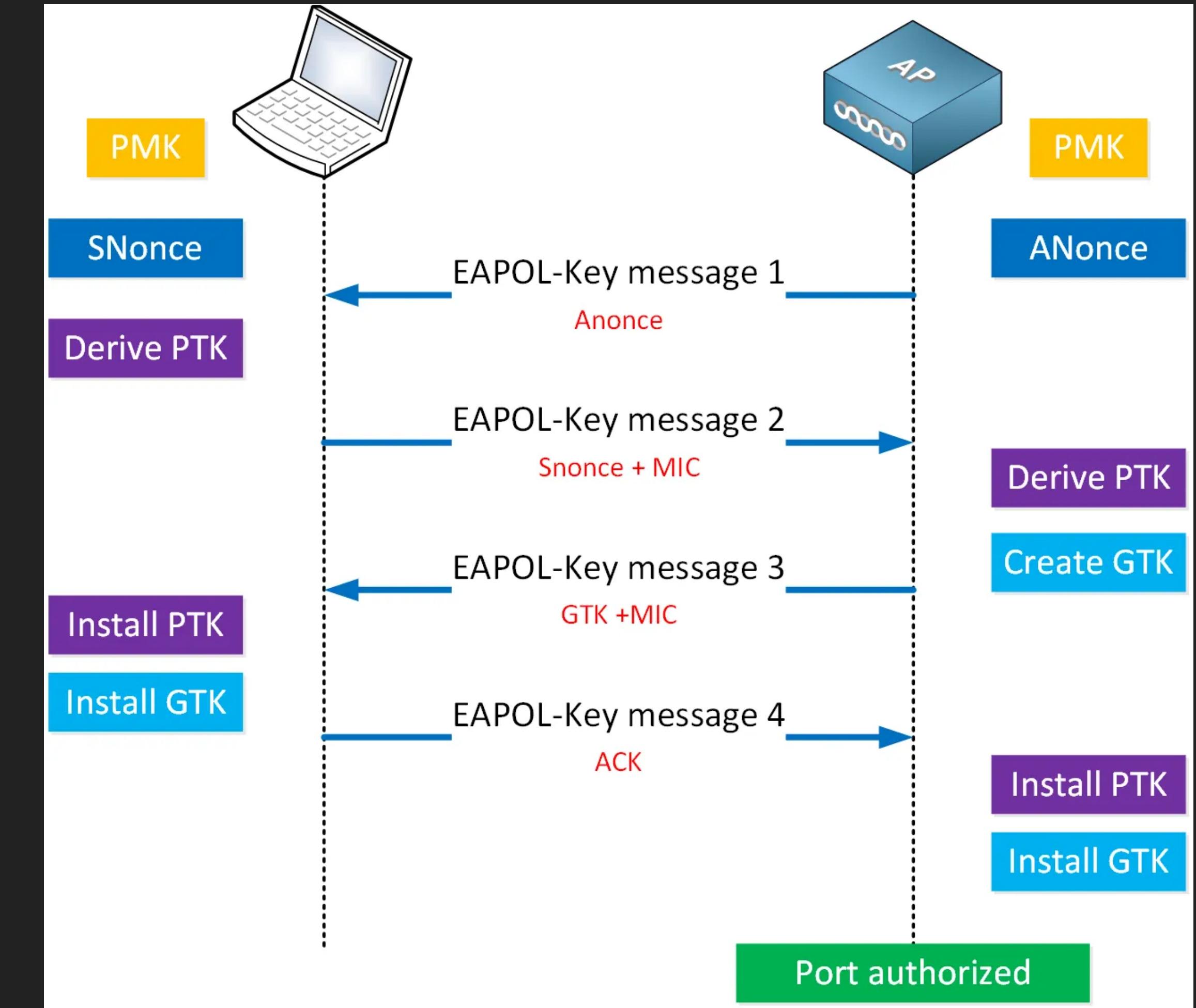
BLE Beacon Emulate



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



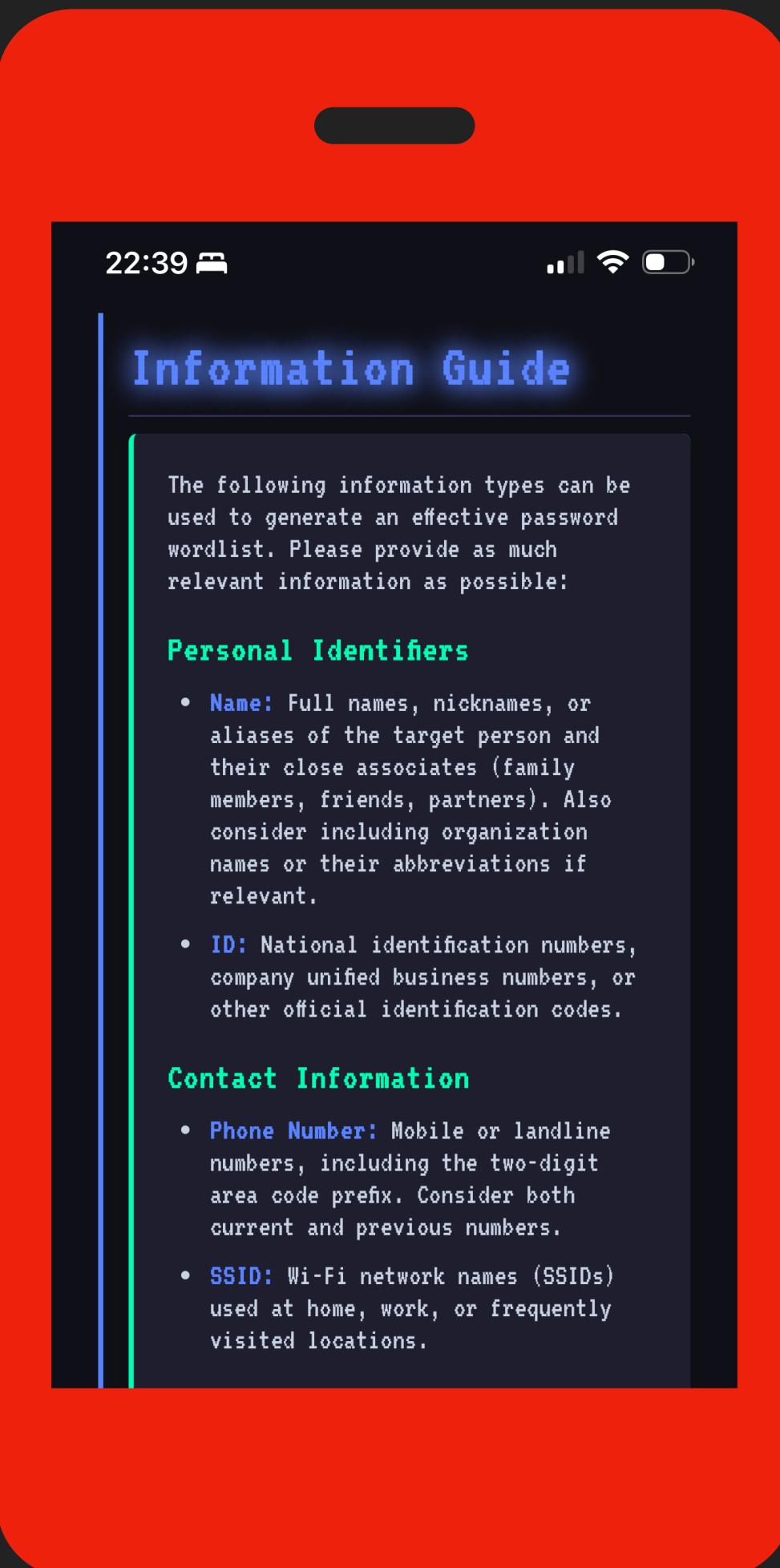
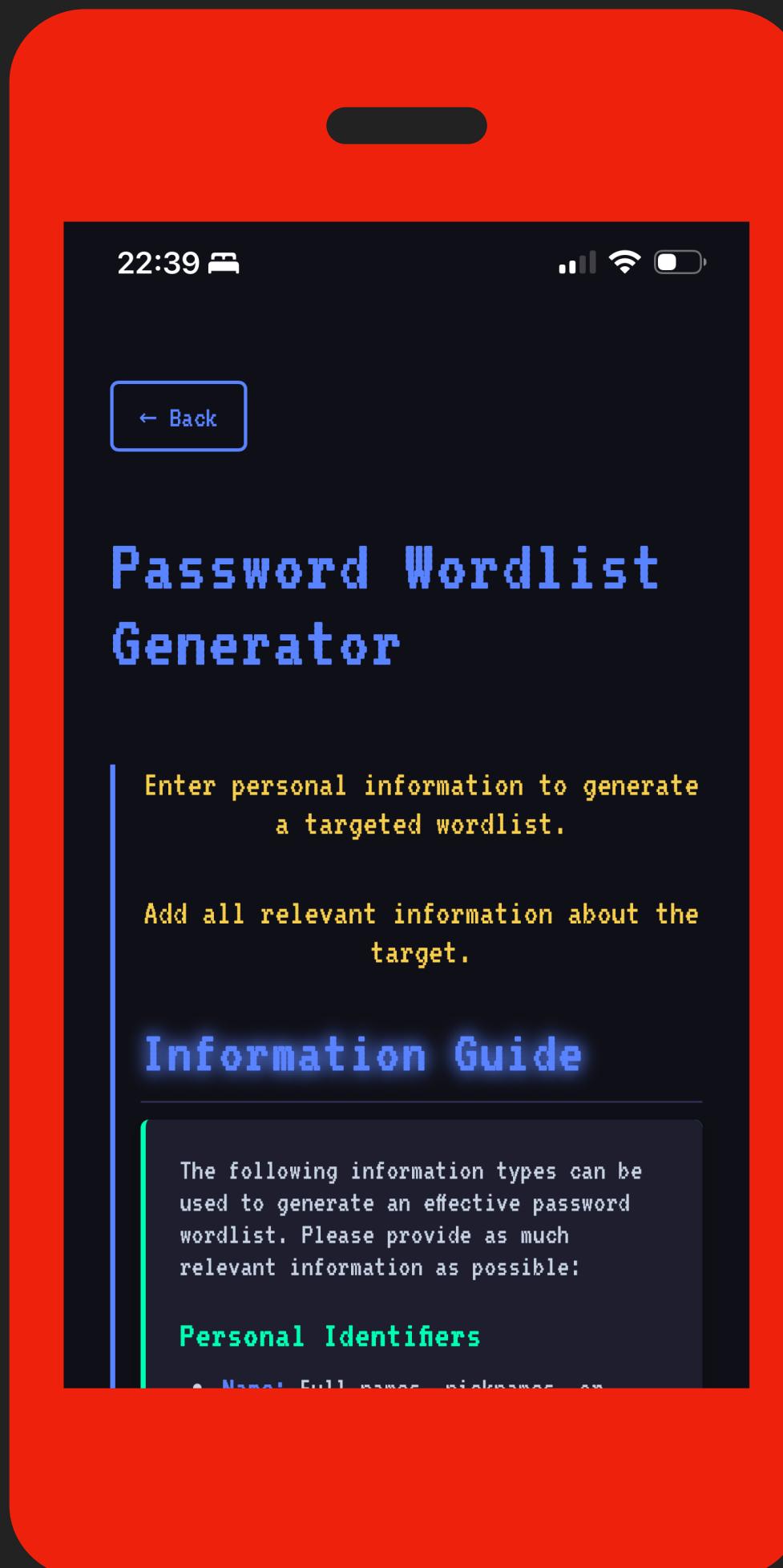
<https://reurl.cc/LapRe4>

Wi-Fi Password Cracker



1. 新增虛擬監聽網卡
2. 掃描附近的 Wi-Fi AP
3. 選擇 Wi-Fi 目標後監聽封包
4. 對目標 Wi-Fi 發送斷線訊號
5. 確認有錄到斷線訊號
6. 透過字典檔進行破解
7. 獲得 Wi-Fi 密碼

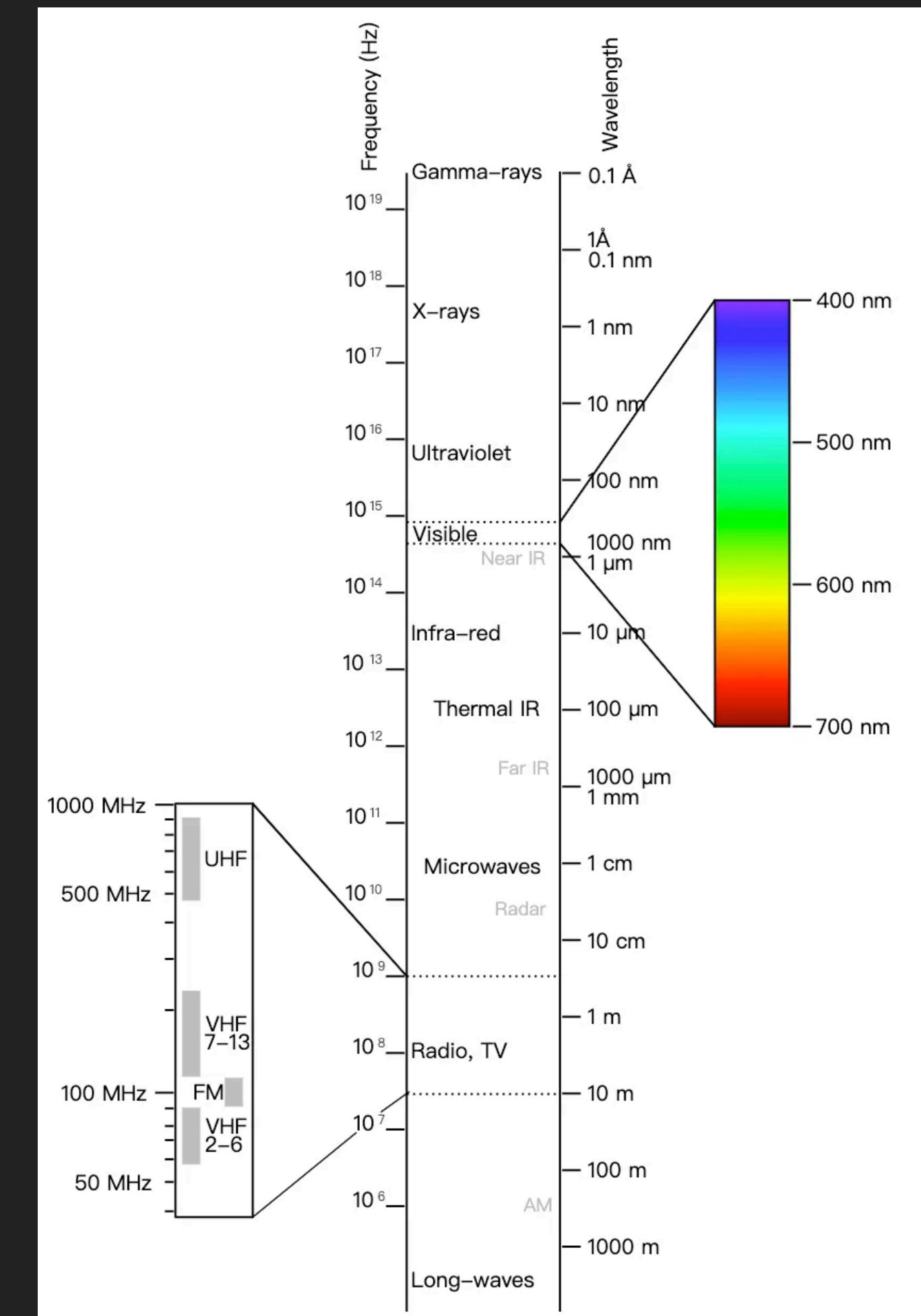
Password Wordlist Generator



Introduction of Infrared (IR)

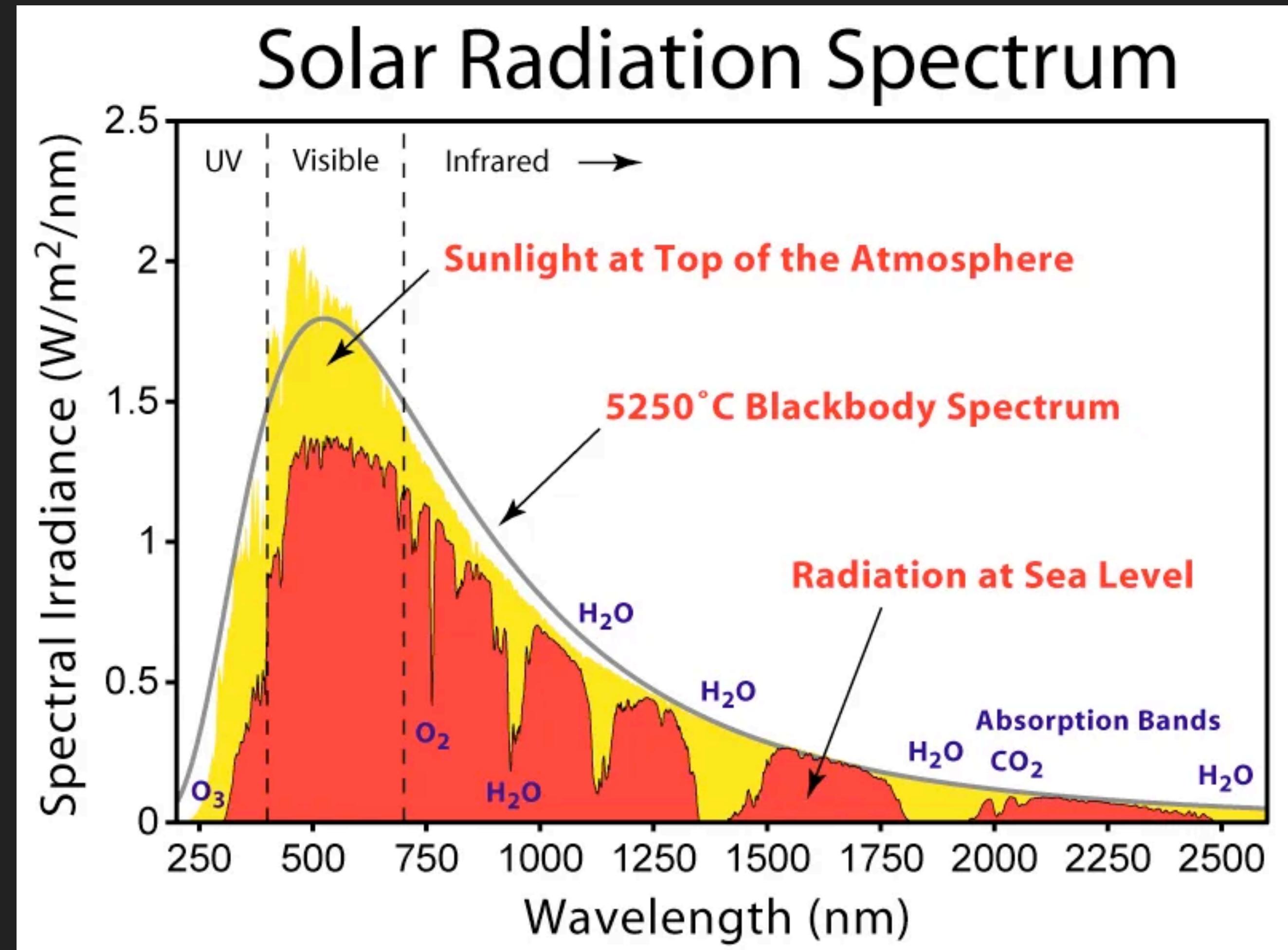


- 波長：950 nm
- 頻率
 - NEC : 38Khz
 - RC-5 : 36Khz
 - RC-6 : 36 KHz
 - Panasonic : 36.7 KHz
 - Sharp : 38KHz
 - Sony : 40KHz
 - RCA : 56Khz



圖片來源：<https://commons.wikimedia.org/w/index.php?curid=22428451>

Introduction of Infrared (IR)

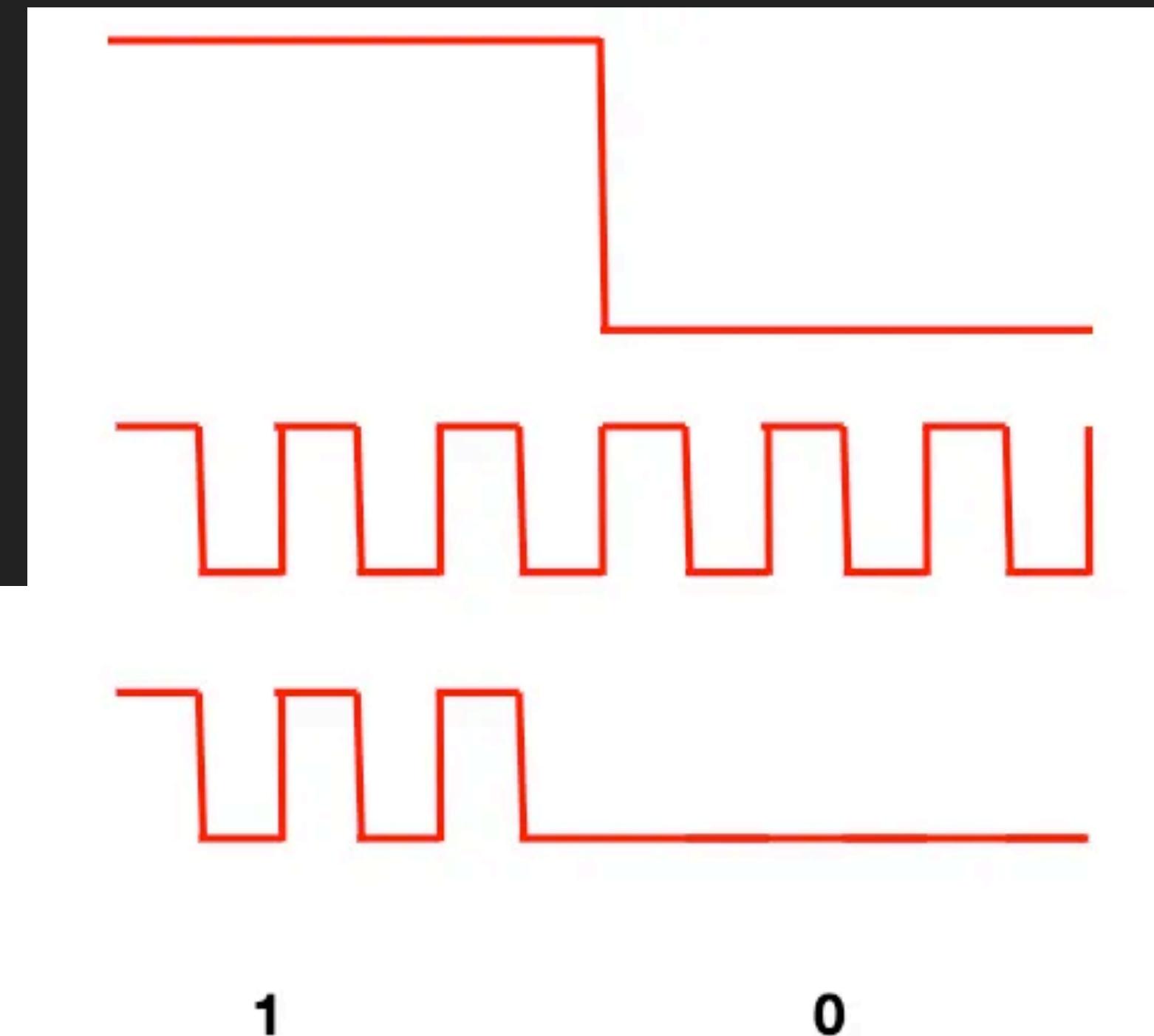


圖片來源：<https://commons.wikimedia.org/w/index.php?curid=2623187>

Introduction of Infrared (IR)

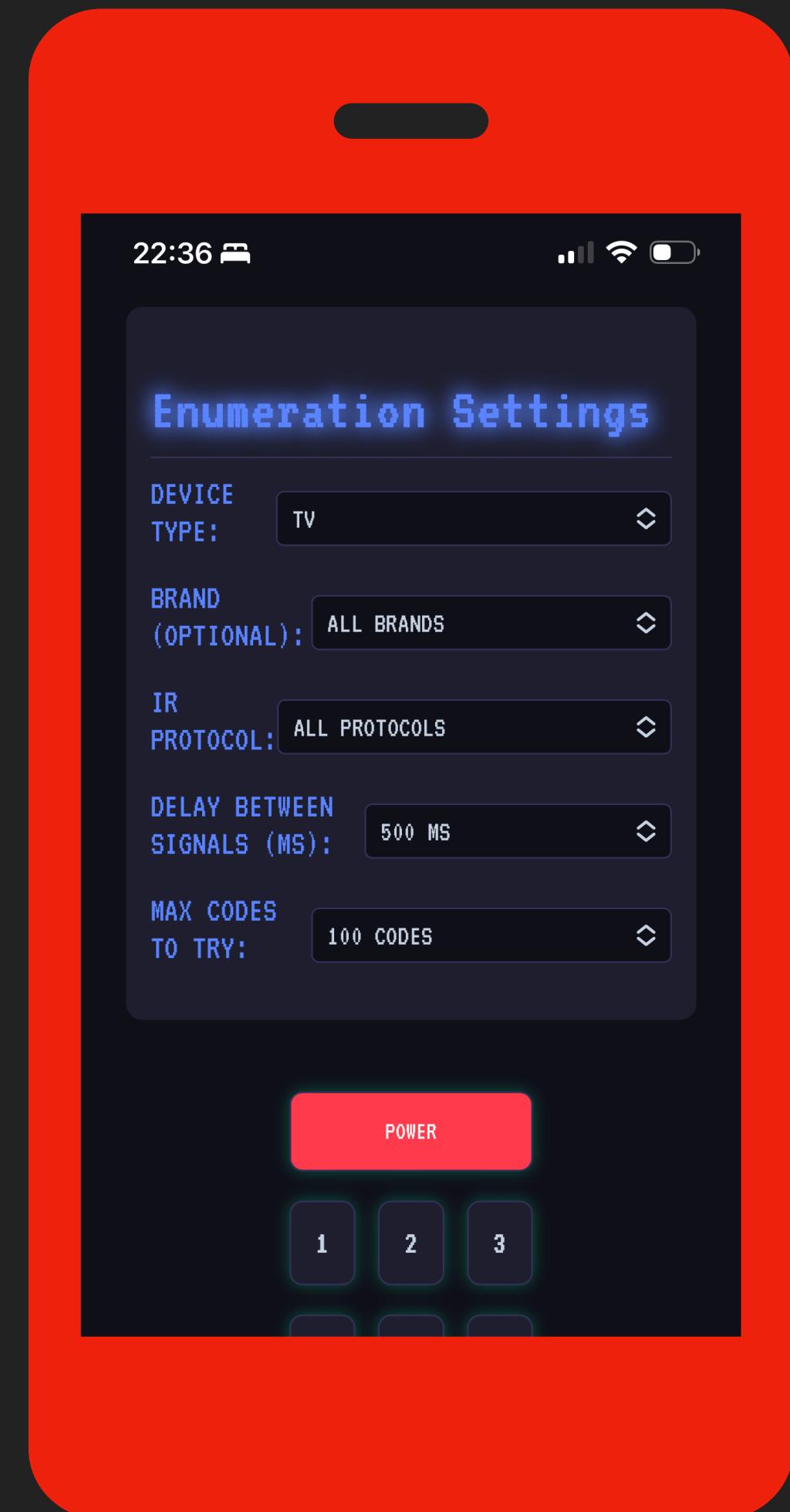


- 使用載波 (carrier wave)
 - 減少干擾
 - 避免過熱、增加亮度



圖片來源：<https://medium.com/@tih/關於紅外線控制的那些事-7e9848eb5b7e>

IR Signal Learner and Enumerator

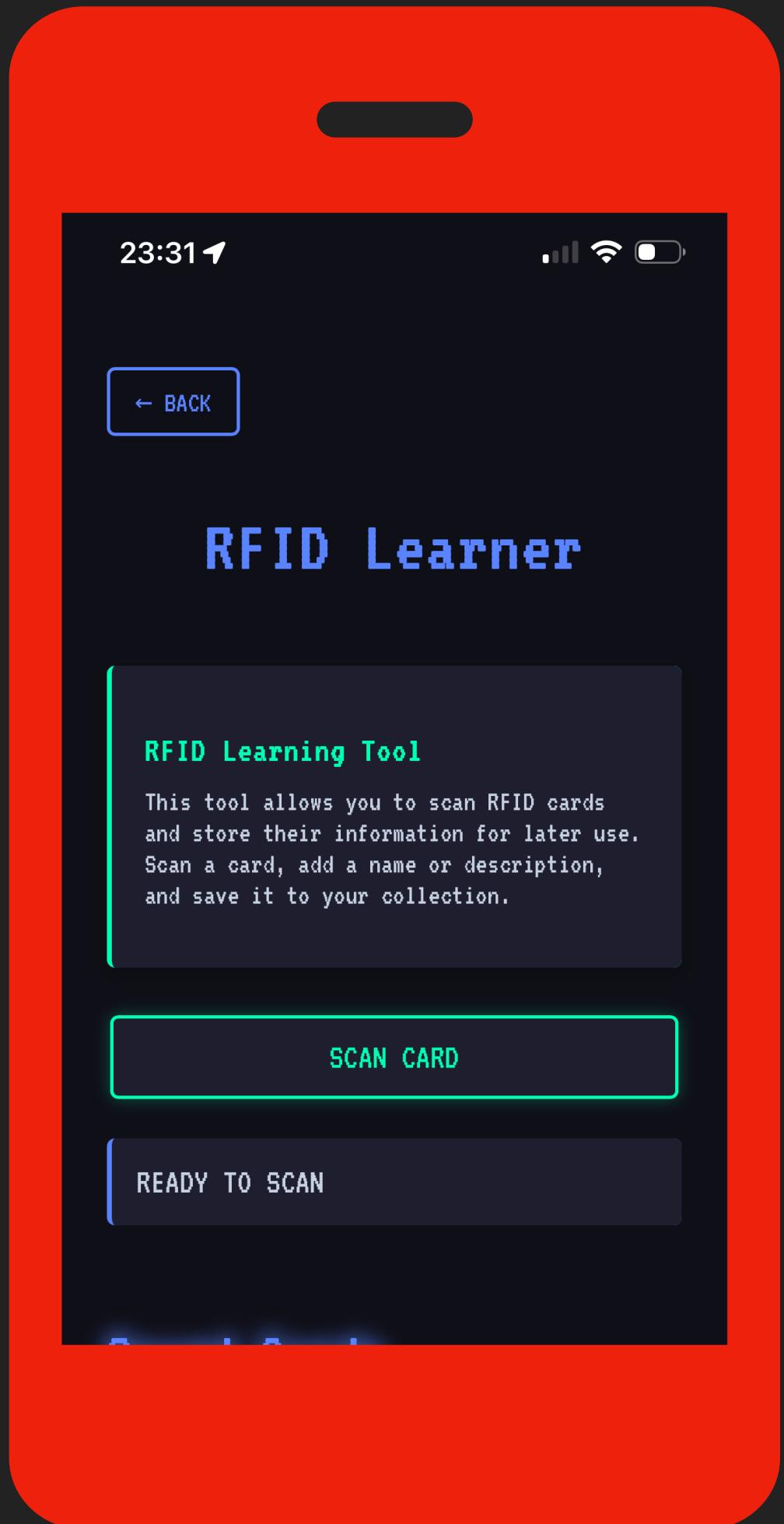


Introduction of RFID and NFC



- RFID
 - LF : 門禁卡
 - HF : 智慧卡、交通卡
 - UHF : ETC
- NFC (13.56 MHz)
 - MIFARE Classic : 悠遊卡
 - MIFARE Ultralight : Apple Pay
 - MIFARE Plus
 - etc.

RFID Tools



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/>

