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

本專案及今禁止用於任何違法行

請務必在合。

依據刑法第入侵他人系統、竊取資面臨刑事責任。

技術能力越應用今日所分享的知

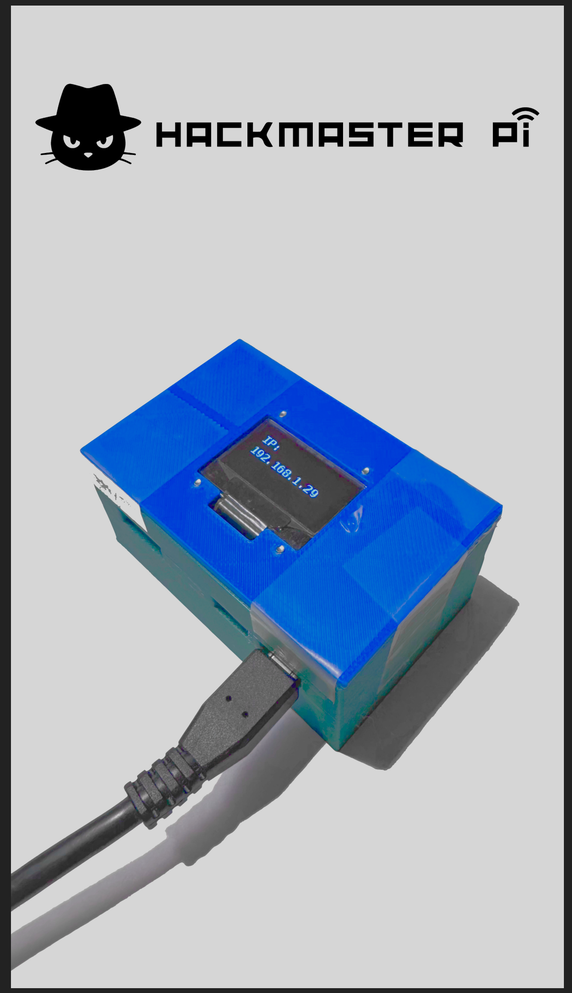
目錄

關於我

- HackMaster Pi 作者
- 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



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

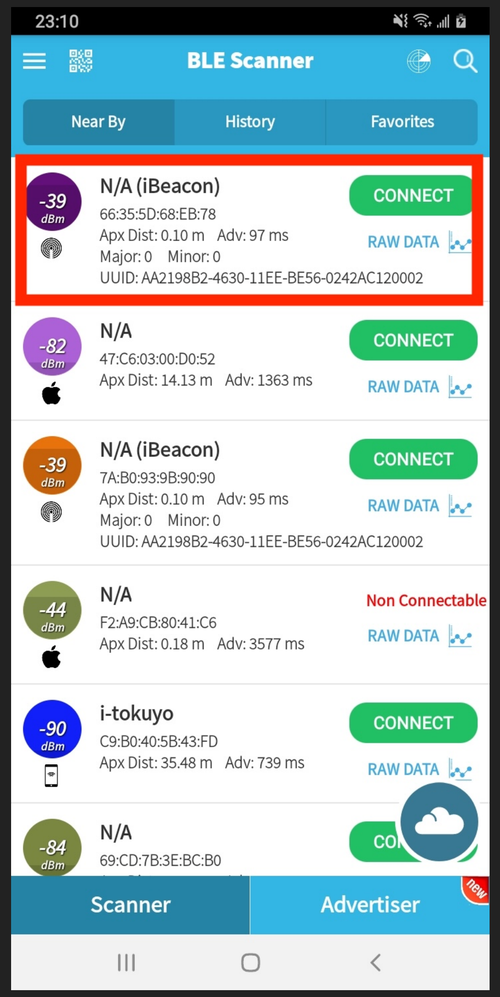

功能展示

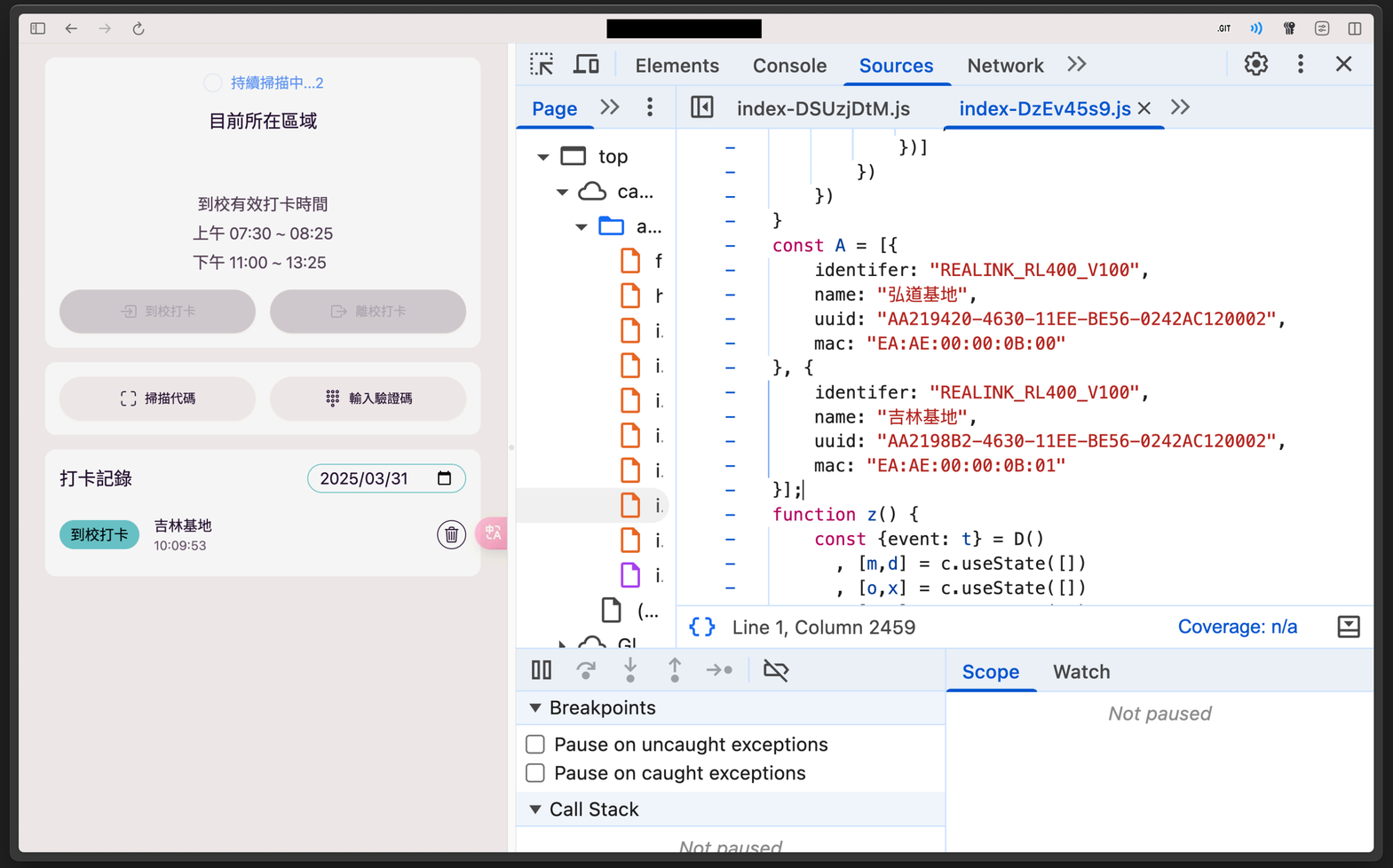
Fake Airpods

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

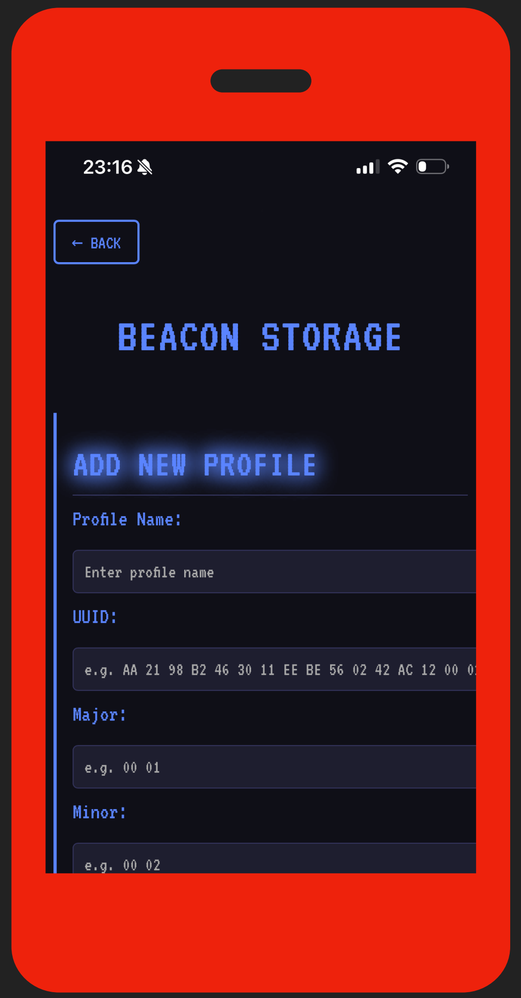
BLE Beacon Emulate

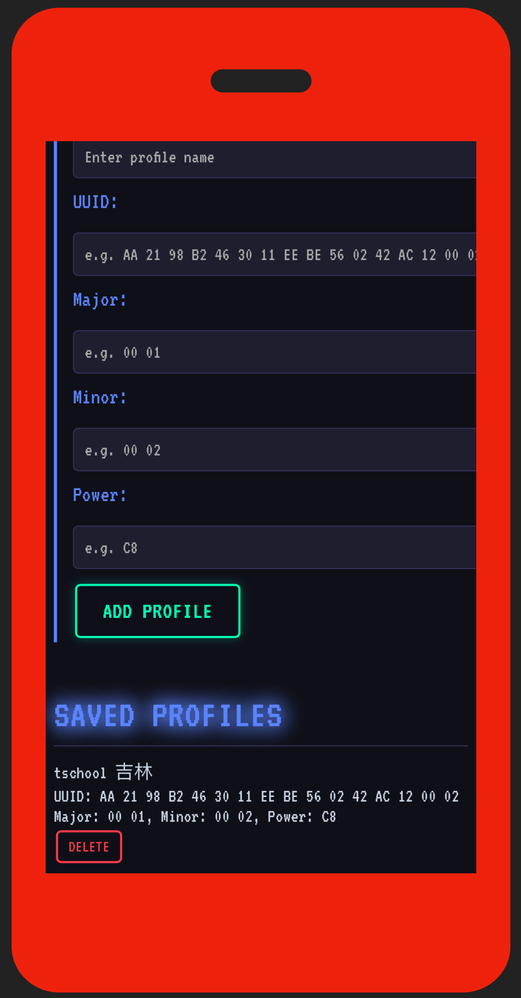
BLE Beacon Emulate

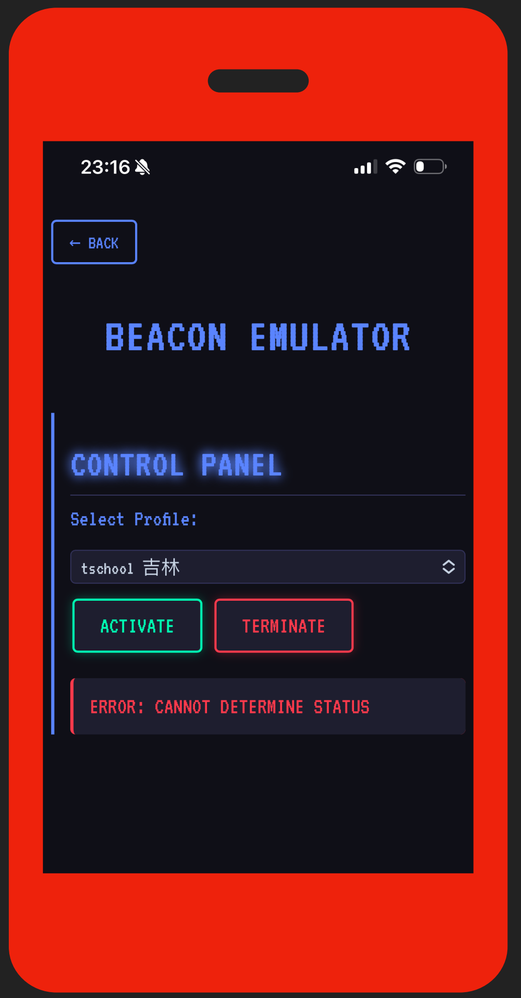




BLE Beacon Emulate

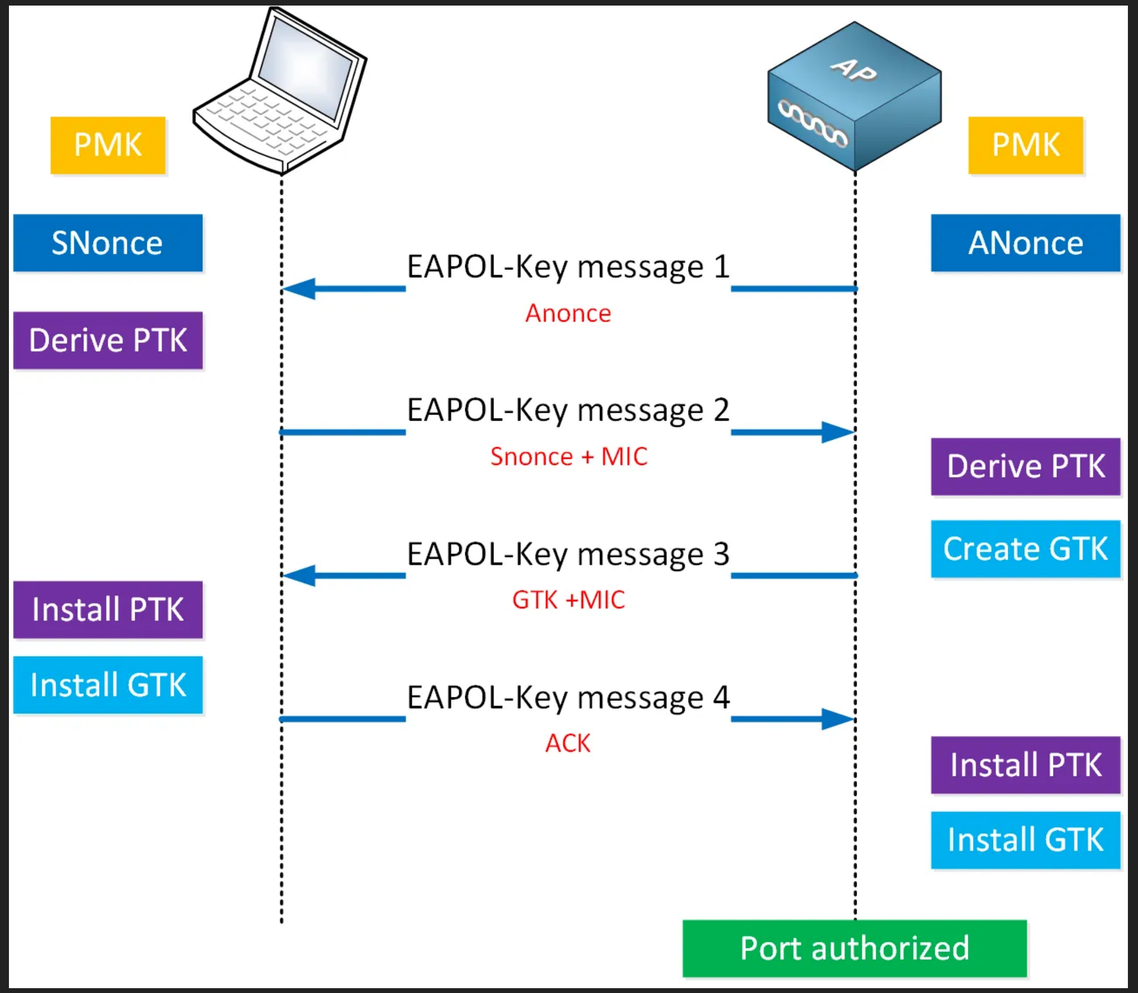






Wi-Fi Password Cracker

- 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

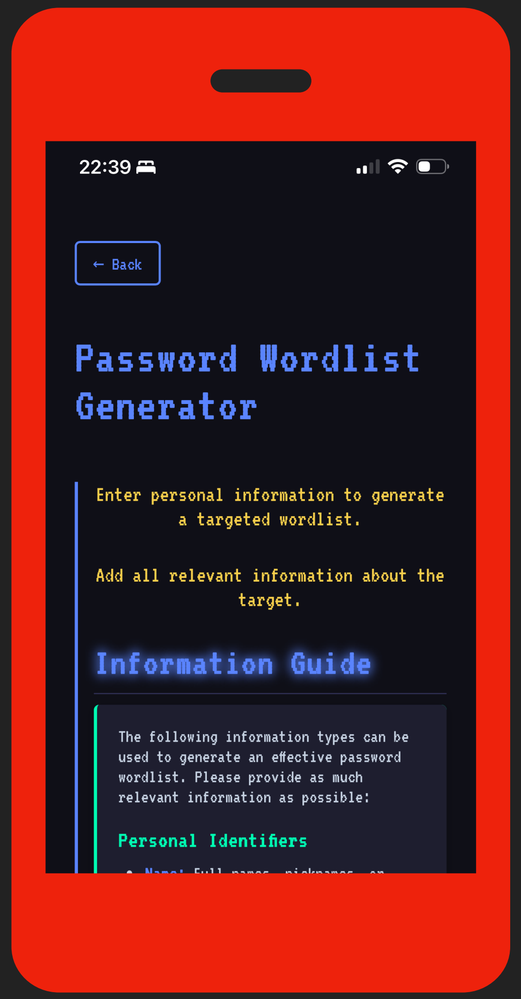
- 防禦方式
  - 高強度密碼
  - 關閉混合模式

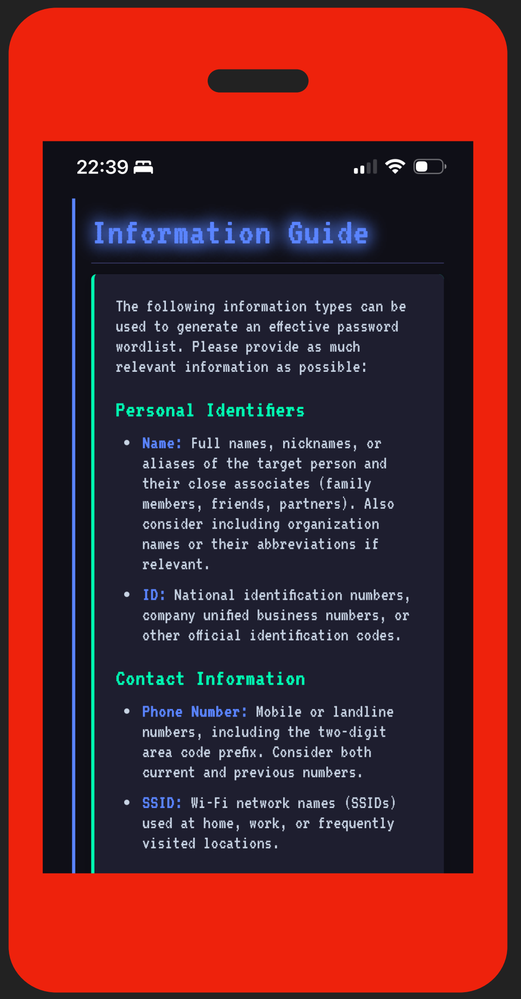
https://reurl.cc/LapRe4

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

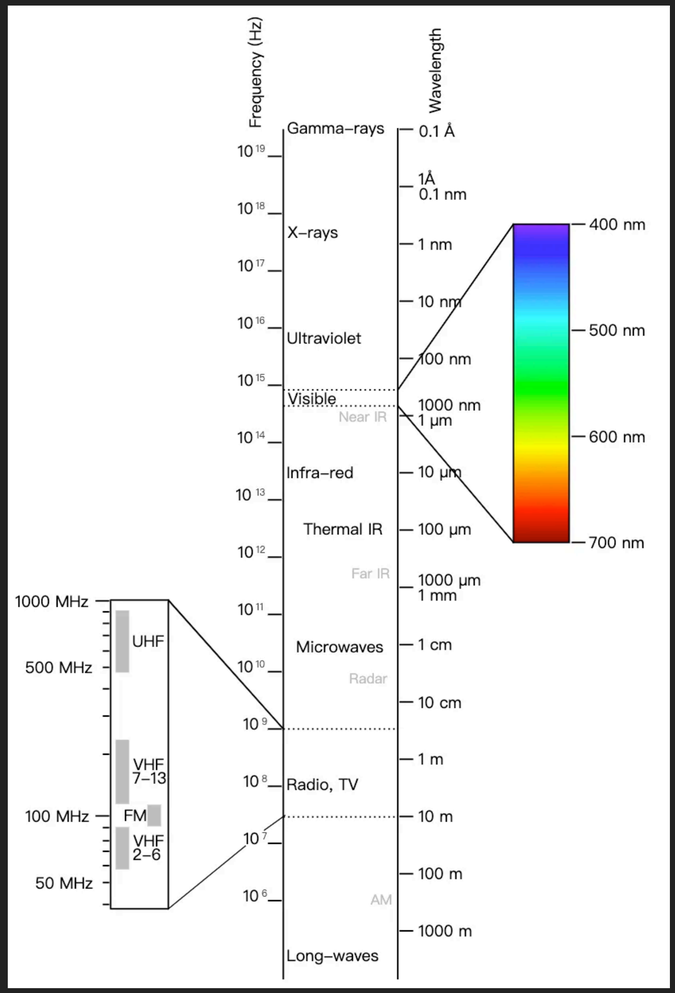
Password Wordlist Generator





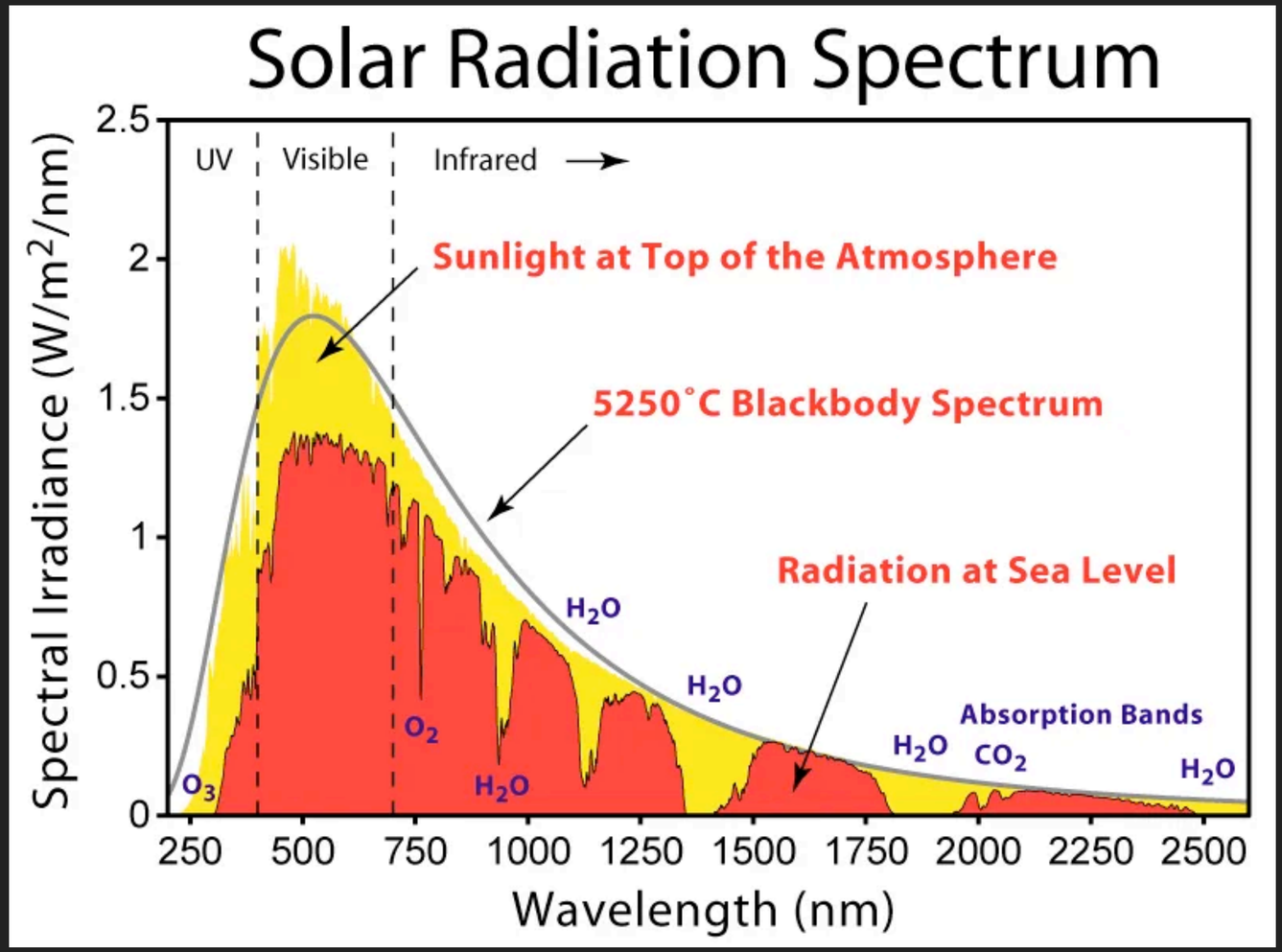
Introduction of Infrared (IR)

- 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

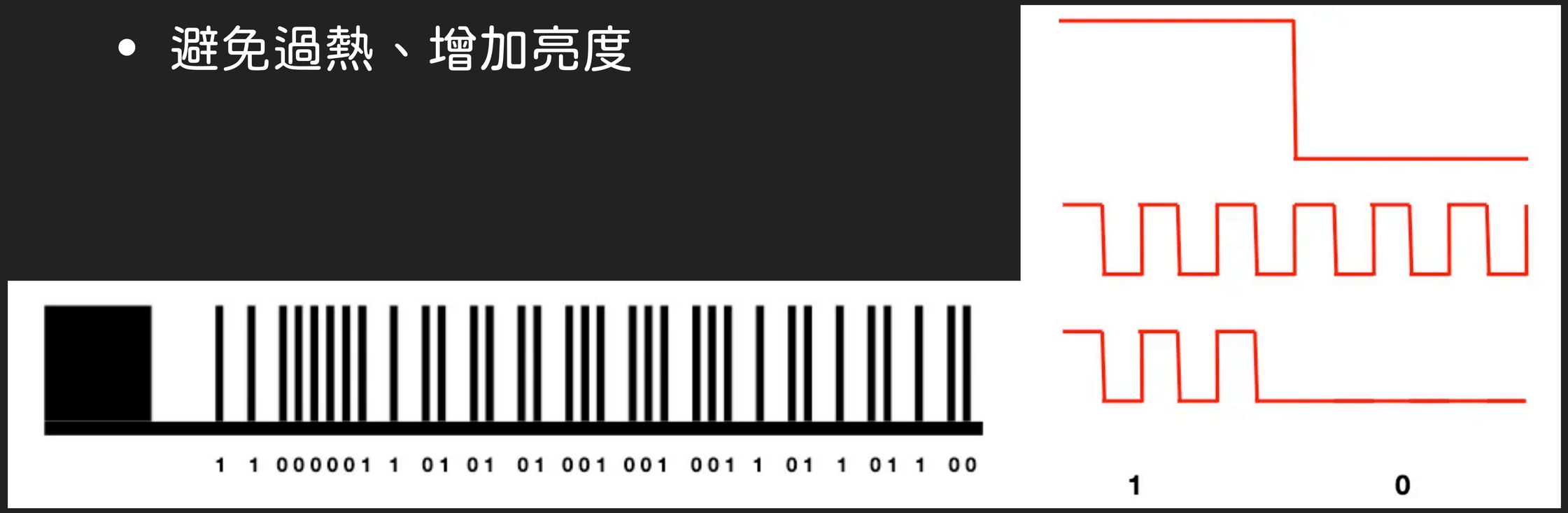
Introduction of Infrared (IR)



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

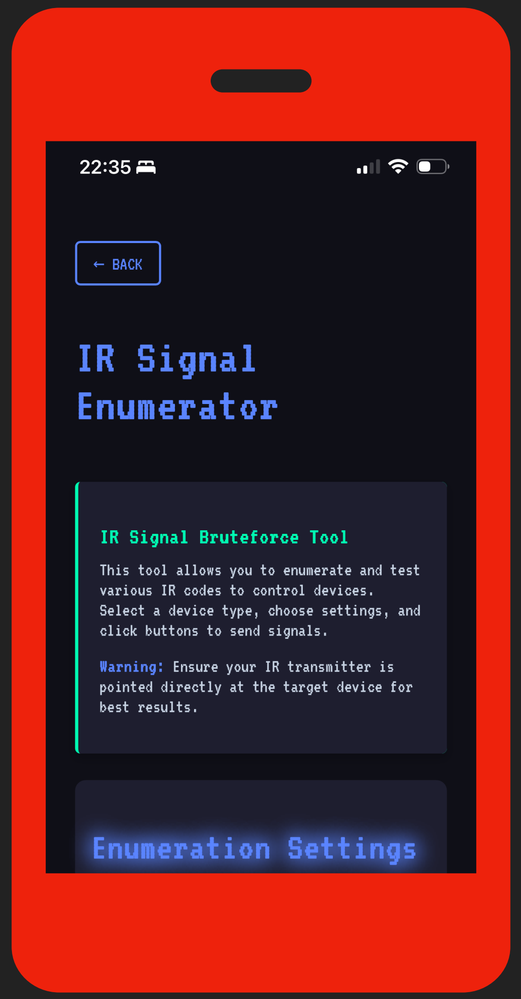
Introduction of Infrared (IR)

- 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

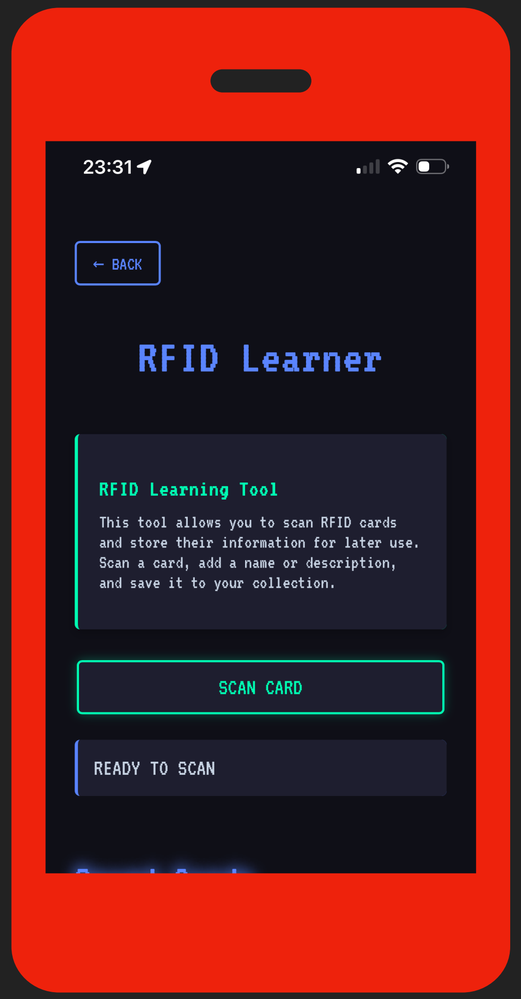
IR Signal Learner and Enumerator



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


23:31
← BACK
RFID Learner
RFID Learning Tool
This tool allows you to scan RFID cards and store their information for later use. Scan a card, add a name or description, and save it to your collection.
SCAN CARD
READY TO SCAN


23:31
← BACK
RFID Writer
RFID Writing Tool
Use this tool to write data to RFID cards. You can either select from your saved cards or enter custom data.
Write Mode
SELECT WRITING MODE:
FROM SAVED CARDS


23:32
← BACK
RFID Emulator
RFID Emulation Tool
This tool allows you to emulate RFID cards by specifying custom UID and data. Use your Raspberry Pi to simulate a physical RFID card.
Note: This feature requires compatible NFC hardware with card emulation capability.
Emulation Settings
EMULATION MODE:

專案資源

https://hackmasterpi.org

https://github.com/1PingSun/HackMaster-Pi

Thank you

Contact

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