# 只要一張小朋友：
# 利用樹莓派打造開源物聯網攻擊工具
## —— 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

# 在開始之前

本專案及今日分享的所有技術內容僅供教育和學習目的，禁止用於任何違法行為。

請務必在合法、合規的環境中使用本工具進行測試和研究。

依據刑法第 36 章關於妨害電腦使用罪的規定，未經授權入侵他人系統、竊取資料或干擾網路設備運作等行為均屬違法，可能面臨刑事責任。

技術能力越強，責任越大，請各位以負責任的態度學習並應用今日所分享的知識。

# 目錄

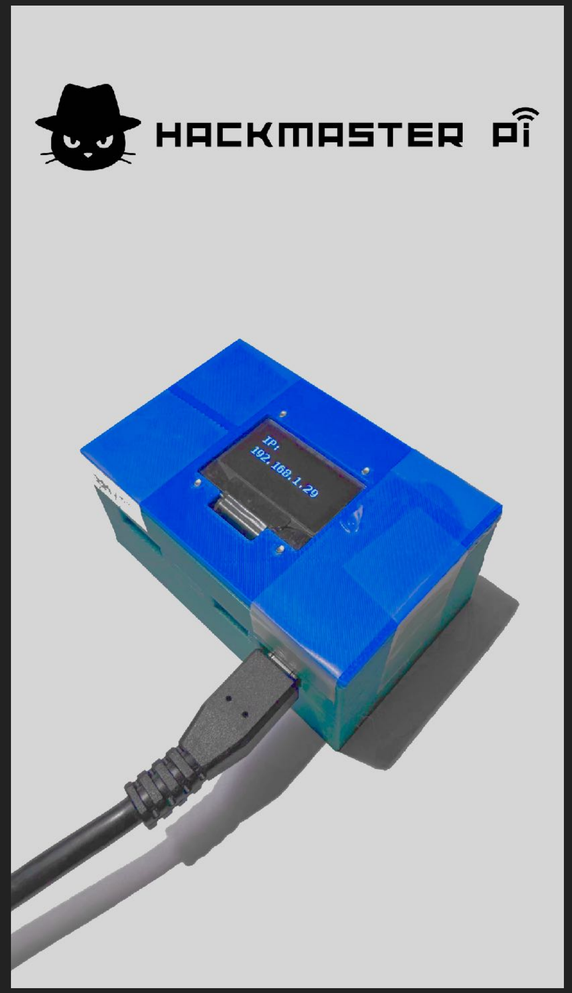
- 關於我
- 關於 HackMaster Pi
- 功能展示
- 製作歷程
- 包裝專案
- Q&A

# 關於我

- HackMaster Pi 作者
- 臺北市數位實驗高中升高三
- EC-Council CEH
- 2024 金盾獎 鋒芒畢露獎
- 2025 MyFirstCTF 金質獎（第一名）
- 奇怪的證照：臺北市街頭藝人證、EMT-1 救護技術員
- Blog：https://1ping.org/

# 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 等相關工具
- 使用 Raspberry Pi Zero 2 W
- 簡單易用的 WebUI
- For more：https://hackmasterpi.org/



# 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 | + $29 | $0 | + $29 |
| 紅外線 | $3 | $3 | $0 |
| 13.56 MHz RFID | $9 | $9 | $0 |
| 總計 | $27 | $21.99 | $169 |

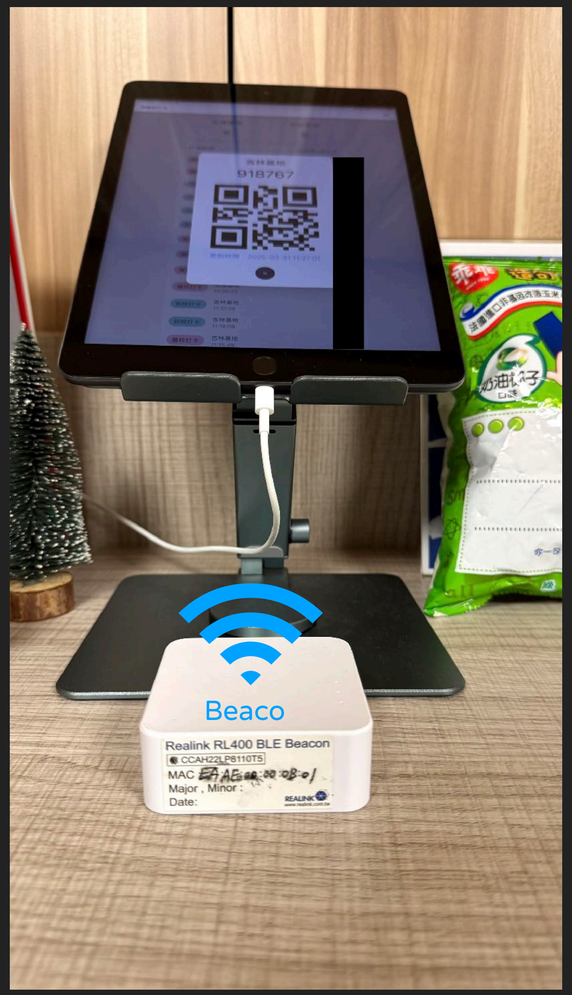

功能展示

# Fake Airpods

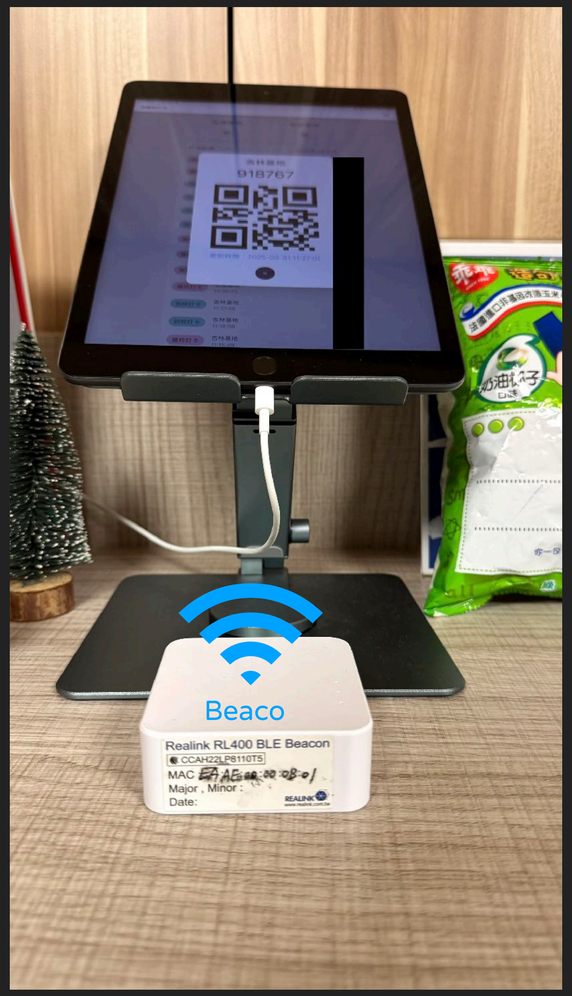


圖片來源：https://support.apple.com/zh-tw/104989

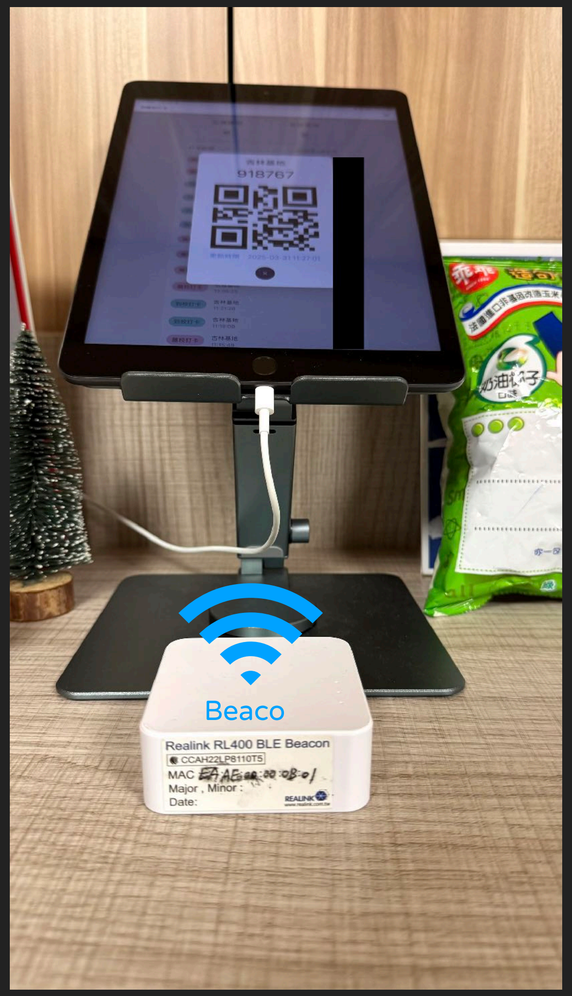
# BLE Beacon Emulate

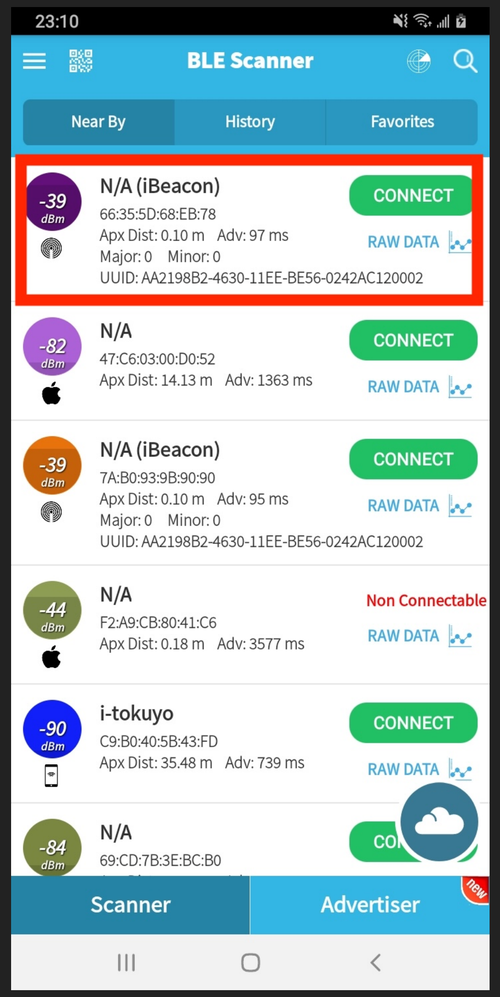
# BLE Beacon Emulate

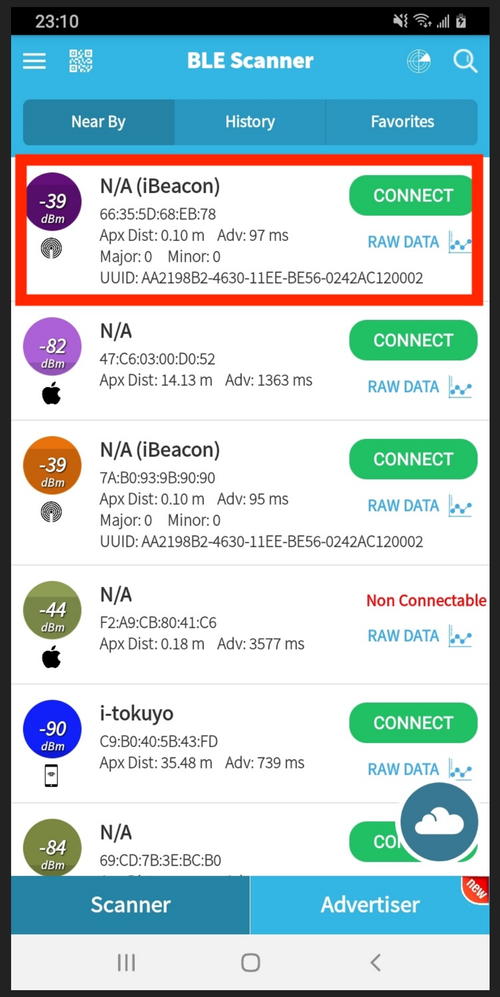
# BLE Beacon Emulate

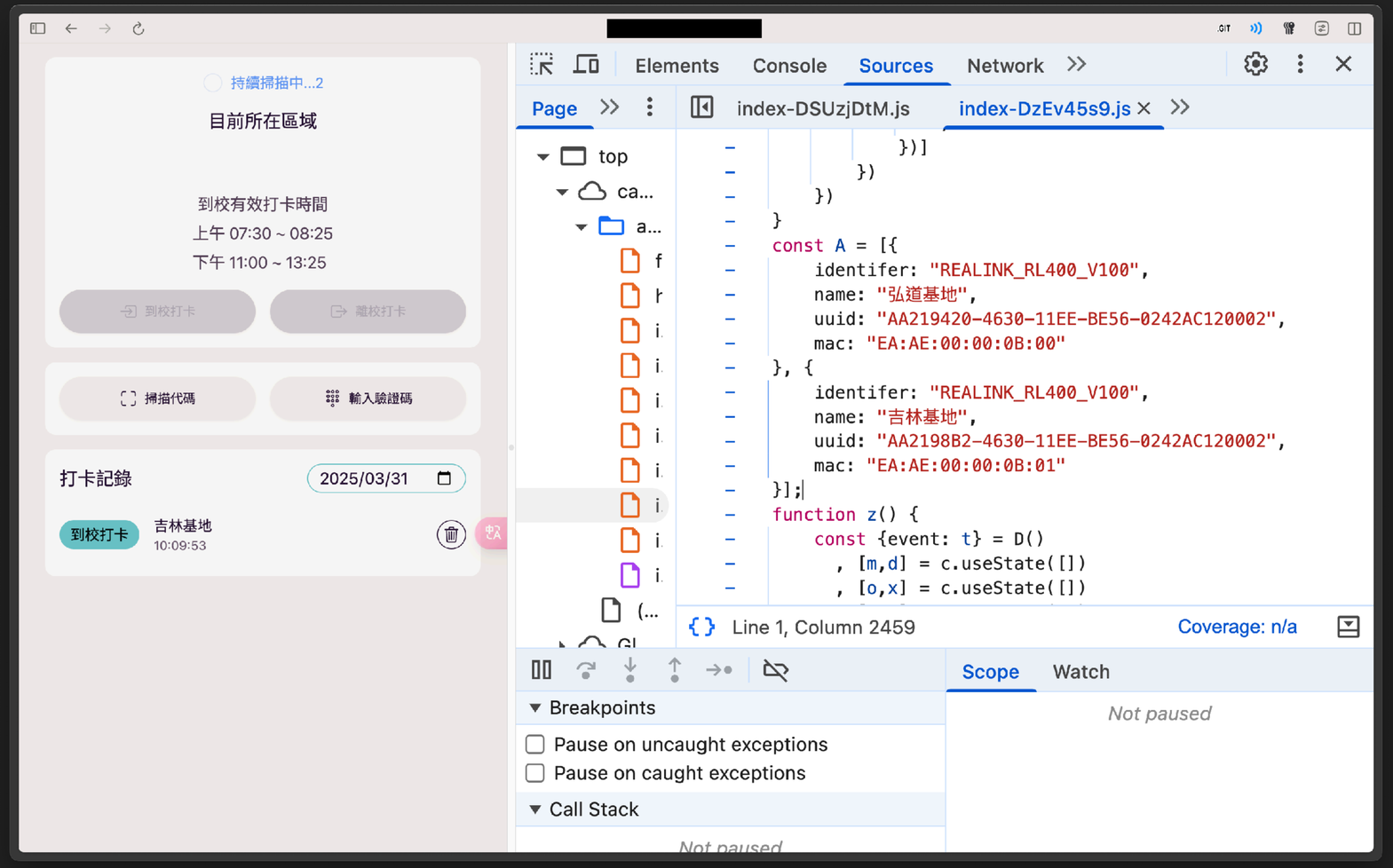




# BLE Beacon Emulate

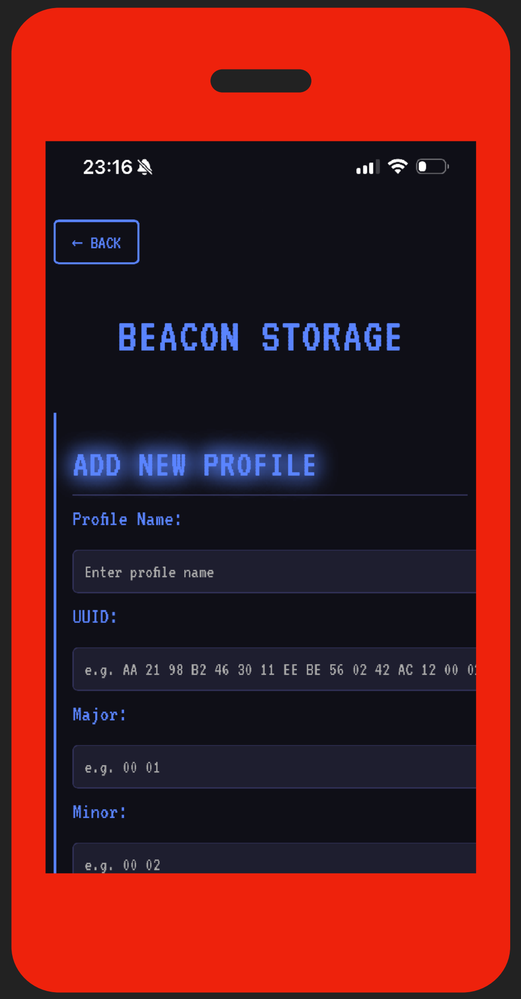


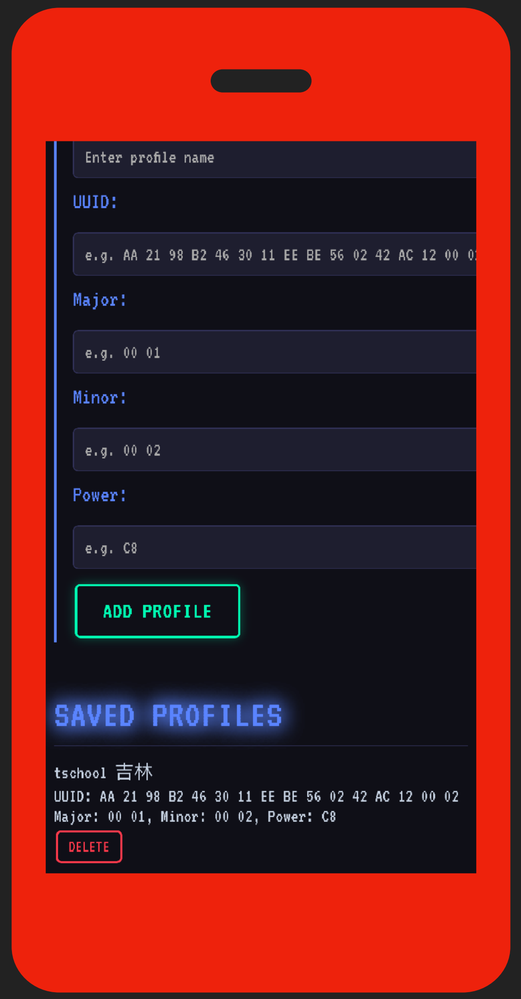
# BLE Beacon Emulate

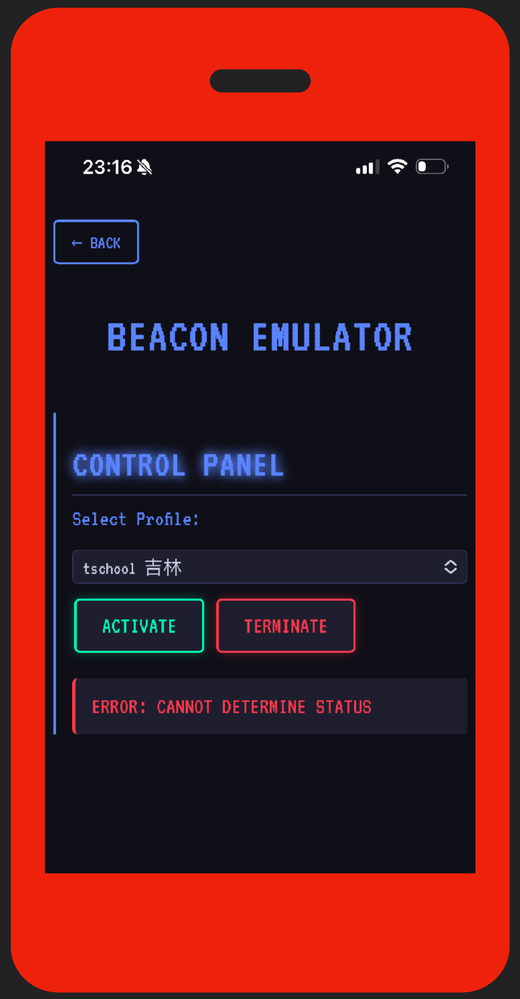


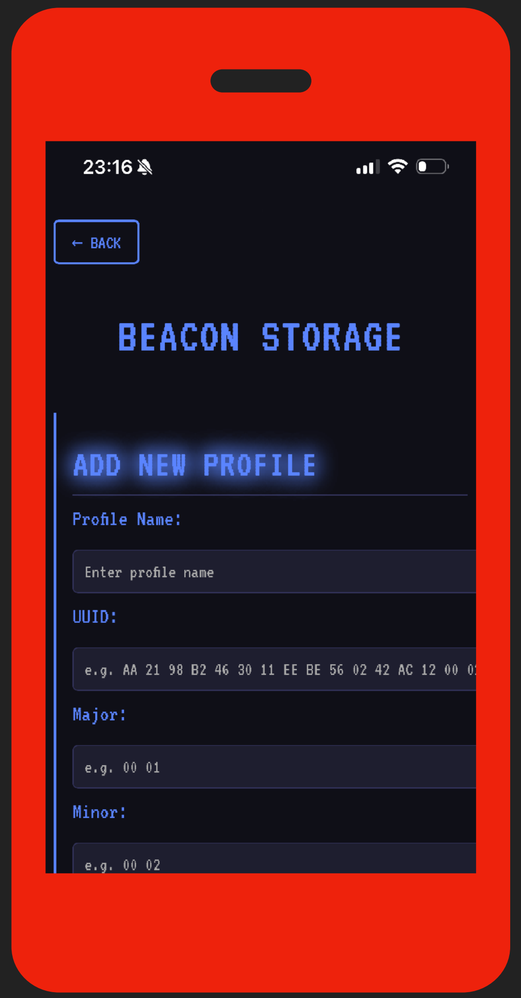
# BLE Beacon Emulate

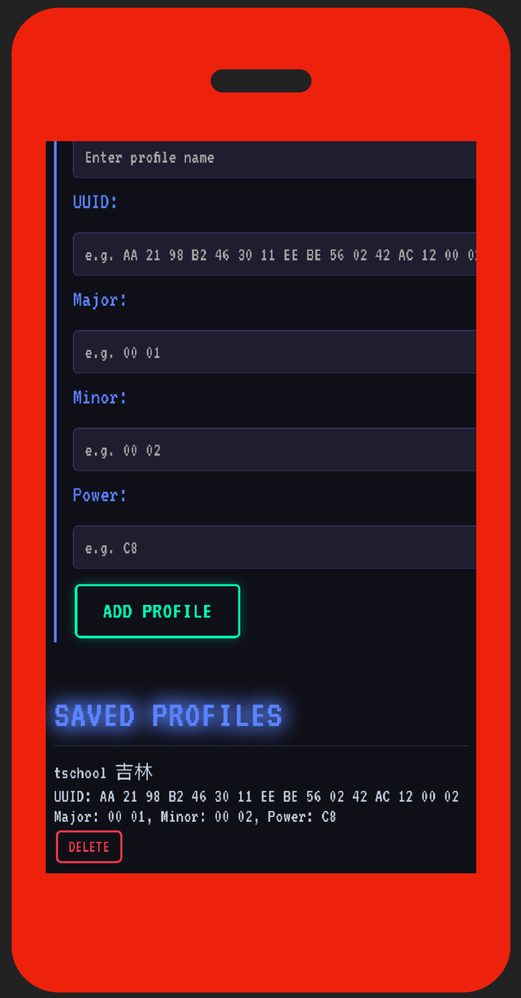


# BLE Beacon Emulate

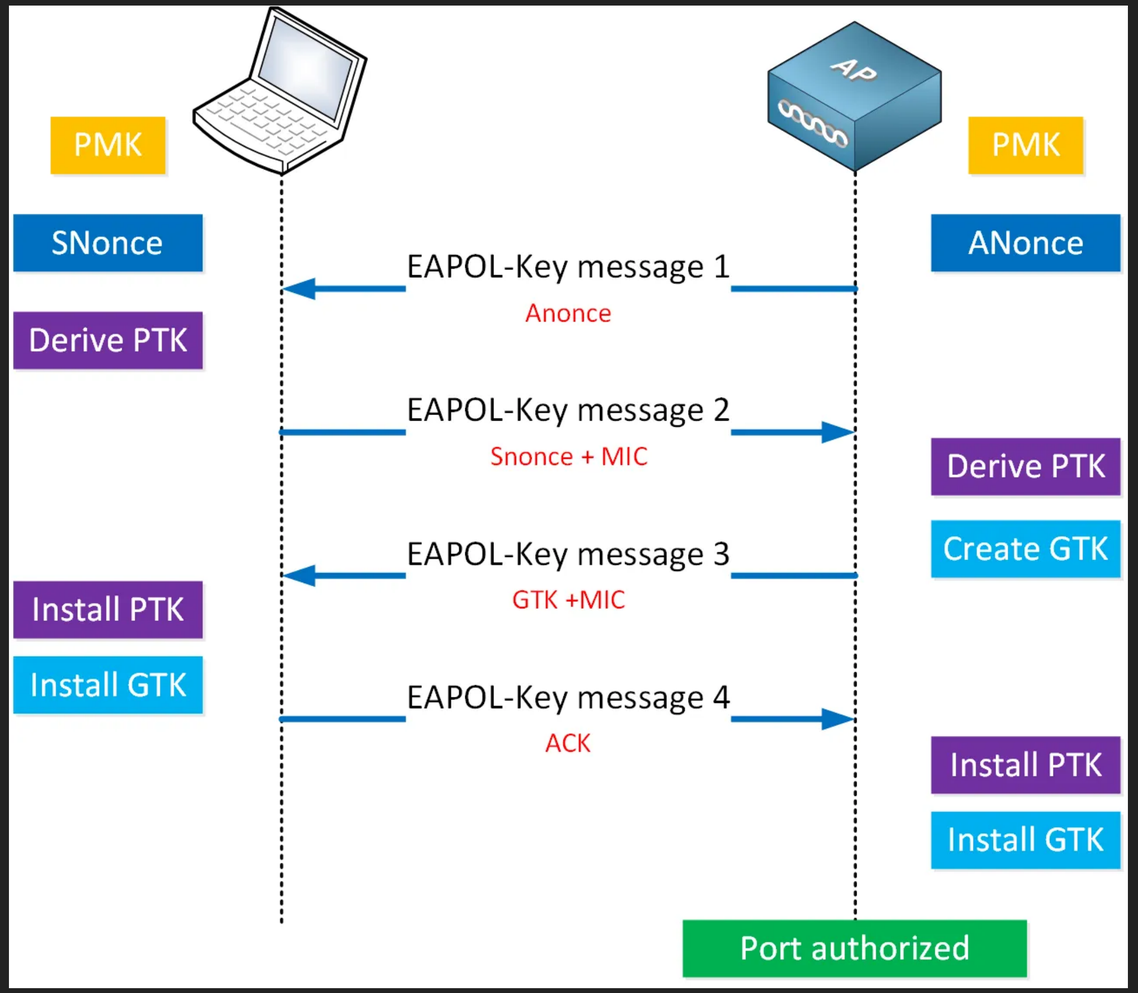



# BLE Beacon Emulate

# 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：破解 IV 取得 PSK
  - 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

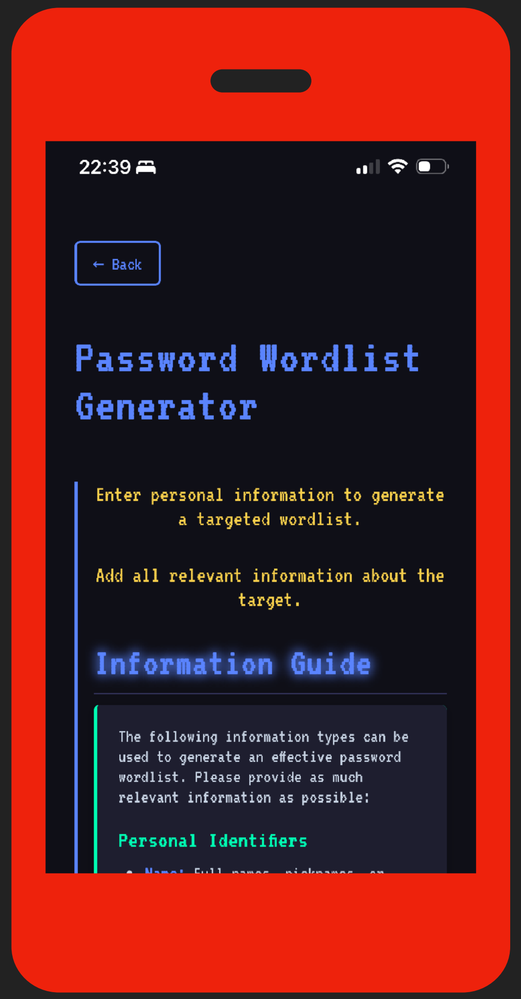
- 防禦方式
  - 高強度密碼
  - 關閉混合模式

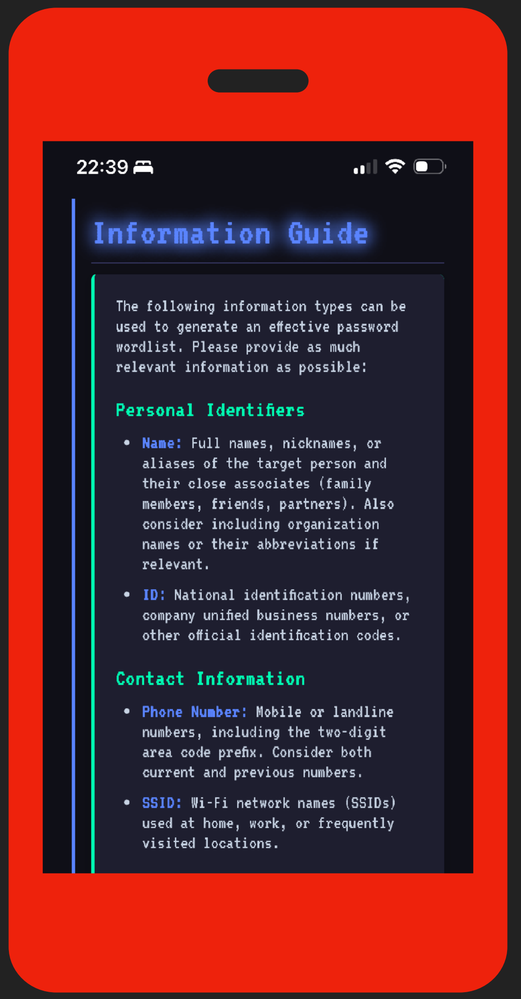
https://reurl.cc/LapRe4

# 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

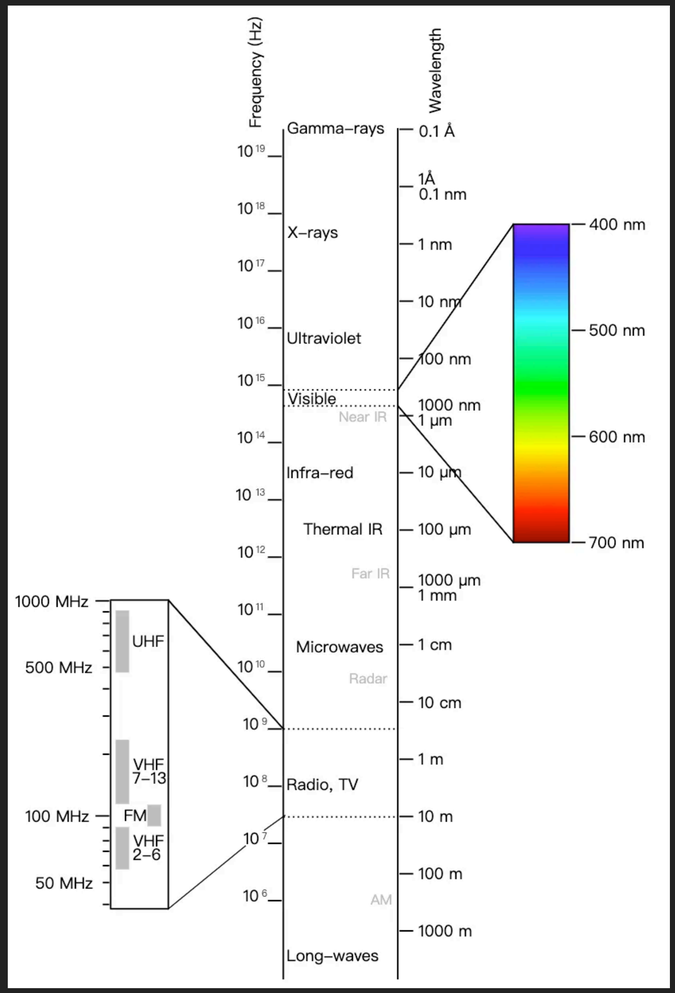
# Password Wordlist Generator



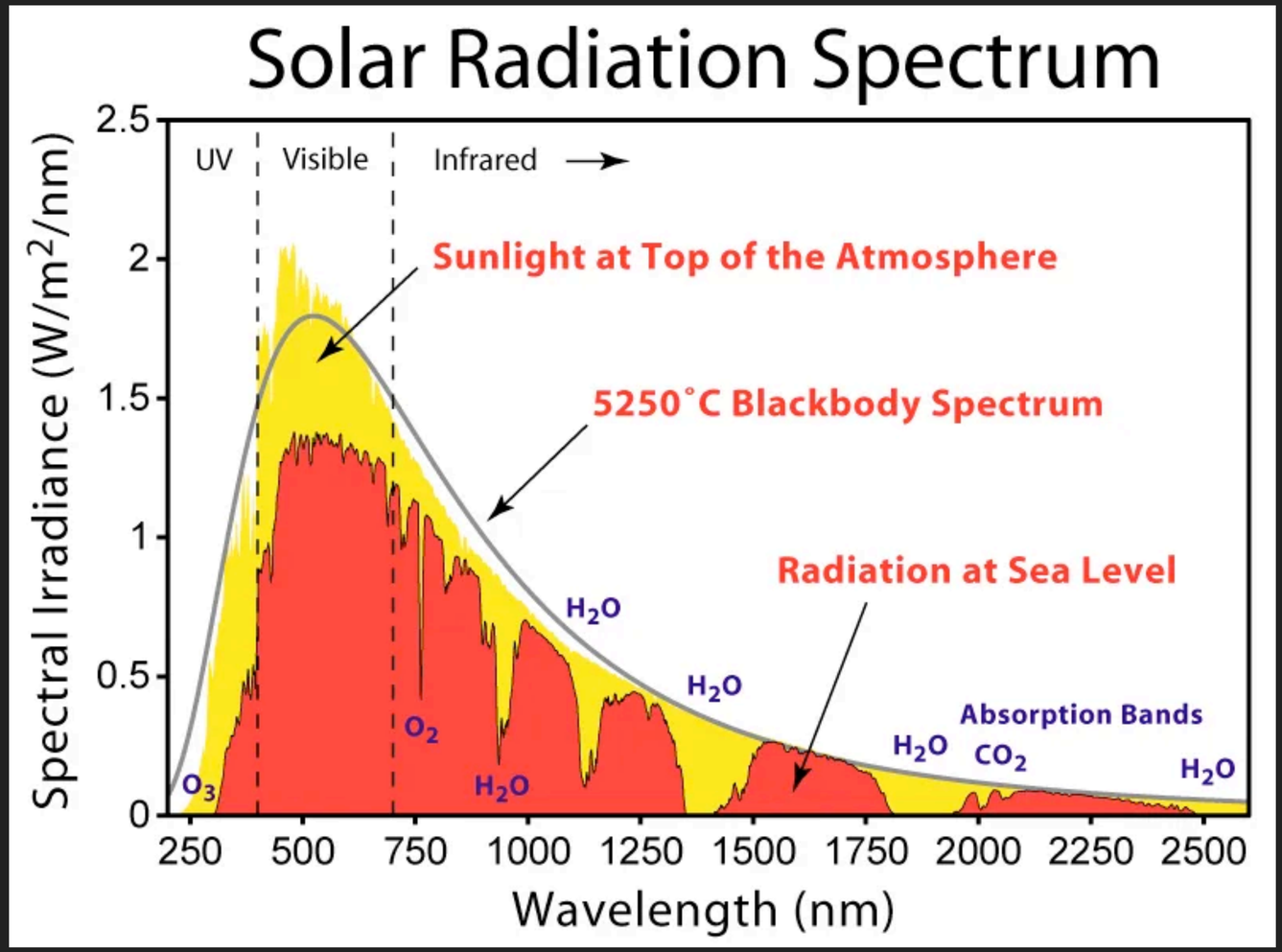

# Introduction of Infrared (IR)

- 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

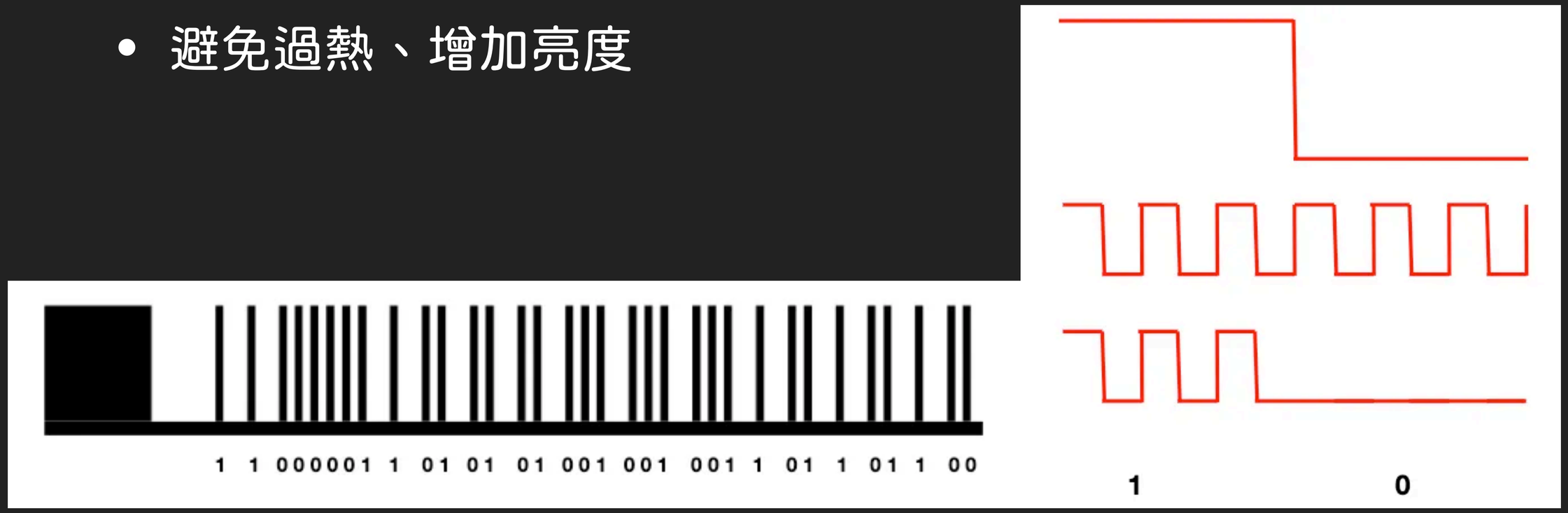
# Introduction of Infrared (IR)




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

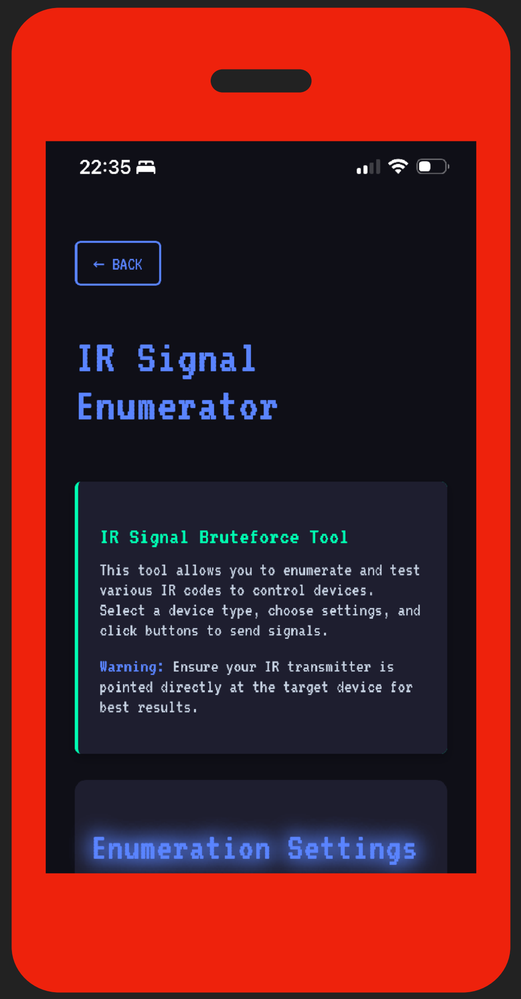
# Introduction of Infrared (IR)

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



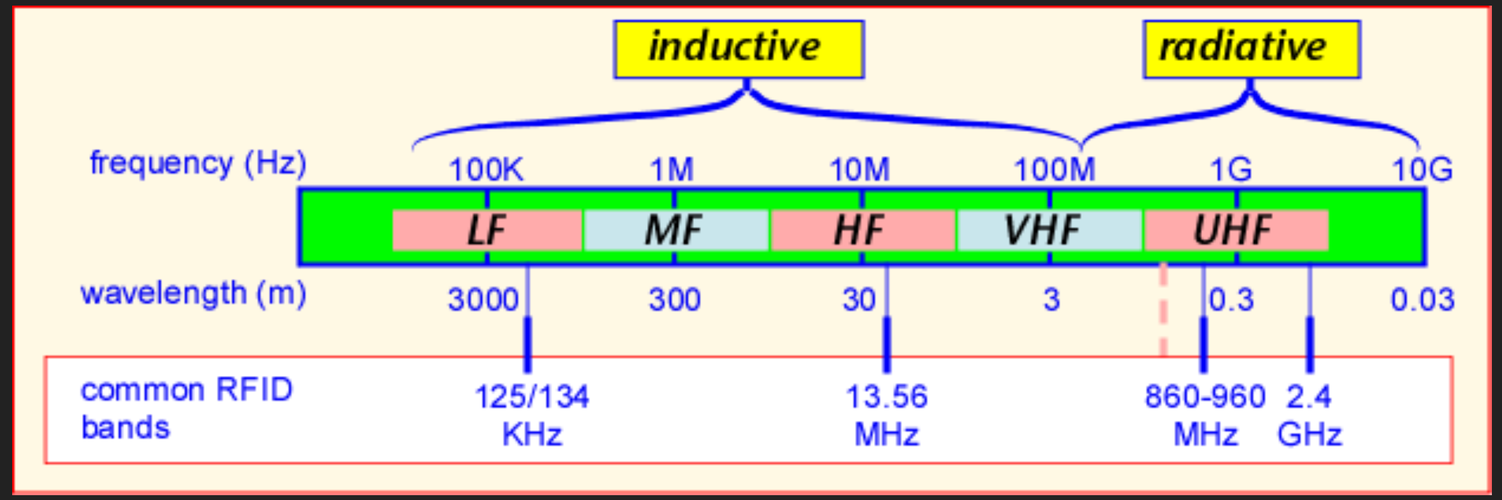

圖片來源：https://medium.com/@tih/關於紅外線控制的那些事-7e9848eb5b7e

# IR Signal Learner and Enumerator


# Introduction of RFID

- RFID
  - LF：門禁卡
  - HF：門禁卡、智慧卡、交通卡
  - UHF：ETC

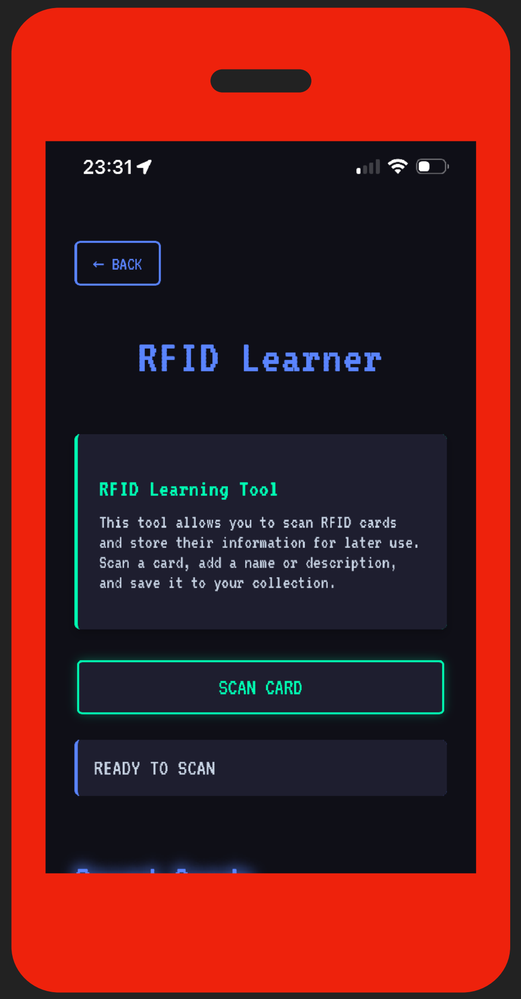



圖片來源： https://polygait.calpoly.edu/what-rfid/types-of-rfid

# Introduction of HF RFID

| 卡片類型 | 標準 | 容量 | 常見應用 |
| --- | --- | --- | --- |
| Mifare Classic | ISO14443A | 1 KB / 4 KB | 門禁卡、悠遊卡 |
| Mifare DESFire | ISO14443A | 8 KB+ | Apple Pay、高安全性需求 |
| NTAG213/215/216 | ISO14443A | 180 B / 540 B / 928 B | 網址分享、聯絡資訊等 |
| FeliCa 系列 | FeliCa | 1-8 KB | 香港八達通、日本西瓜卡 |

# 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:

# 製作歷程

# 人生就是在試錯中成長～～

1. 嘗試正常 Kali OS、P4wnP1 A.L.O.A 都失敗
    - 記得要用 Raspberry Pi Imager
    - 不能用通用的開機碟製作工具，如：Rufus、balenaEtcher
2. 改用 Macbook 搭配外接網卡先做測試：瘋狂尋找 Driver
3. 回到樹莓派並嘗試安裝補丁 nexmon：珍惜生命遠離 AI
4. 改用 Aircrack-ng 支援的外接網卡：反正 Flipper Zero 的網卡也要加購外接


包裝專案

# 官方文件和 README.md

https://hackmasterpi.org

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

# 官方文件和 README.md

https://hackmasterpi.org

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

幫按星星 ⭐

# Logo 設計


HACKMASTER Pi

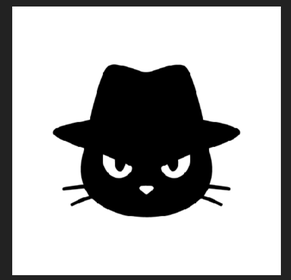

HACKMASTER Pi


HACKMASTER Pi


HACKMASTER Pi


HACKMASTER Pi


HACKMASTER Pi



# Logo 設計

ChatGPT 說：
設計費可以收 6000

# Logo 設計

ChatGPT 說：
設計費可以收 6000

# 維基百科

**您所提交的草稿仍需改善。在2025年7月8日由Bosco Sin (留言)審閱。**

1. 過量粗體
2. 請刪除英文和中文間多餘的空格

維基百科極不鼓勵用戶撰寫條目去介紹自己或有密切關係的事物。若您一定要撰寫，請參見WP:中立的觀點和公開利益衝突。

- 如果您想繼續改善您的草稿再提交，請單擊窗口頂部的「編輯」選項。
- 如果您尚未解決上面列出的問題而直接提交，您的草稿將再次被拒絕並可能被刪除。
- 如果您需要其它的幫助，請在建立條目專題的詢問桌**詢問**或者使用**即時通訊軟體**向我們經驗豐富的編輯尋求即時幫助。
- 在提交被接受之前，請不要刪除審核的評論或此通知。

**如何改善您的草稿** [展開]

在2025年7月8日由Bosco Sin (留言)審閱。 · 最後由1pingsun於1秒編輯。通知作者

使用下面的「發布更改」按鈕保存更改後，您可以通過按此處顯示的「提交」按鈕提交草稿以供審核。

# 宣傳

# Thank you

## Contact

- Email: 52sunyiping@gmail.com
- GitHub: https://github.com/1PingSun
- Blog: https://1ping.org/