



# 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  
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

# 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



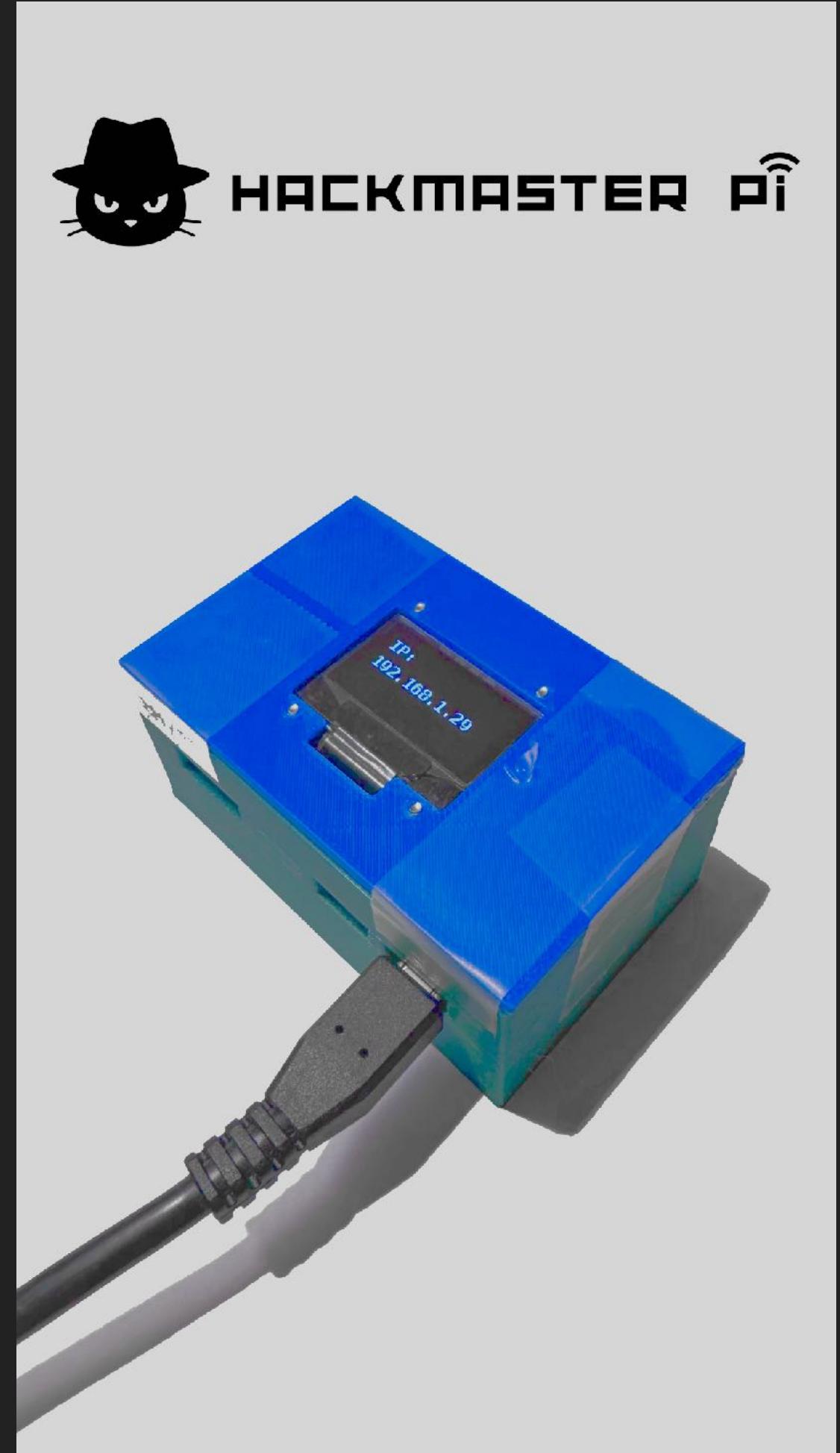
- HackMaster Pi 作者
- 臺北市數位實驗高中升高三
- EC-Council CEH
- 2024 金盾獎 鋒芒畢露獎
- 2025 MyFirstCTF 金質獎 (第一名)
- 奇怪的證照：臺北市街頭藝人證、EMT-1 救護技術員
- Blog：<https://1ping.org/>



# 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



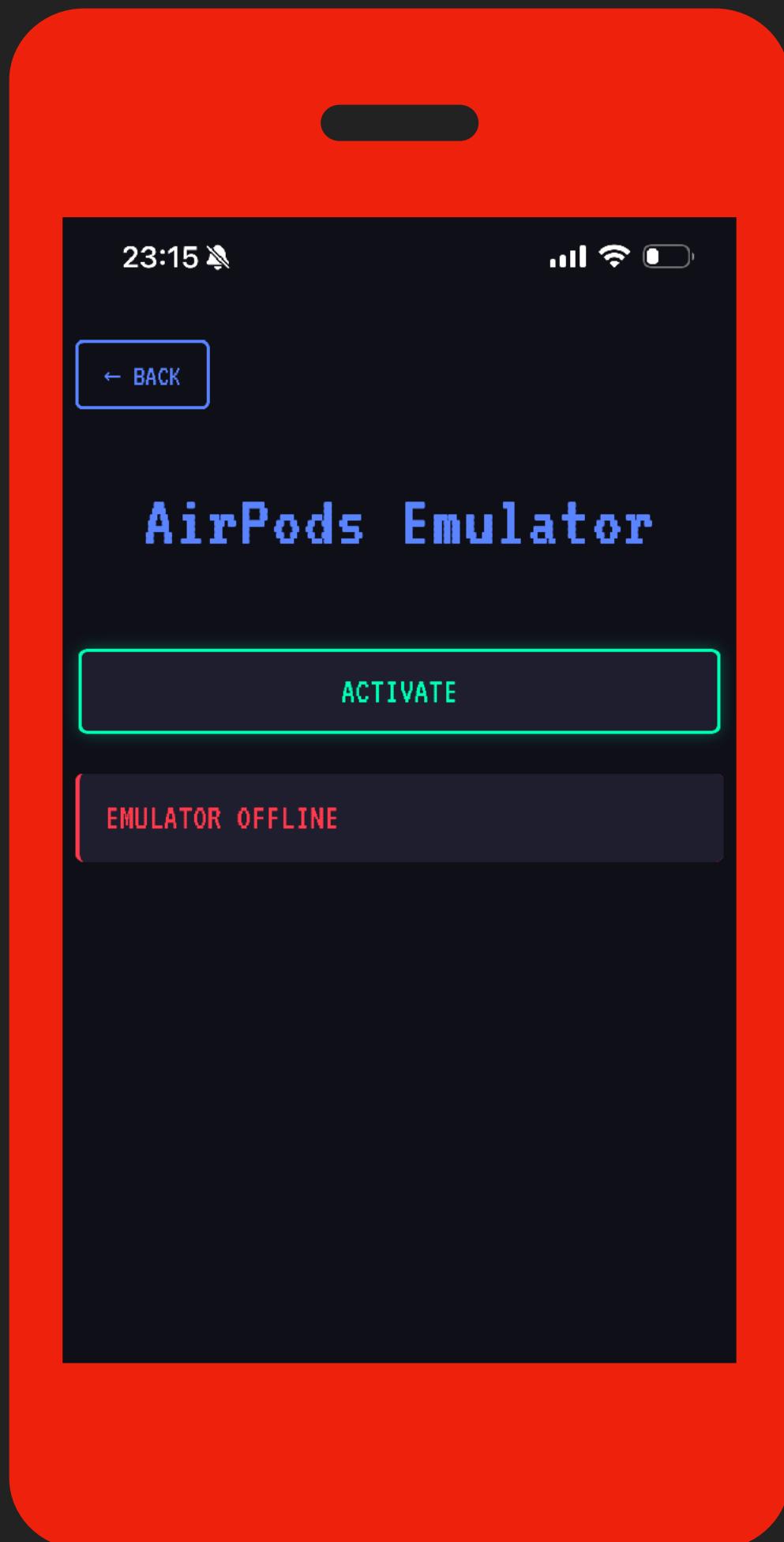
	HackMaster Pi	CapibaraZero	Flipper Zero
運算速度	1 GHz	160 Mhz	64 MHz
價錢	\$15	\$9.99	\$169
藍芽	\$0	\$0	\$0
Wi-Fi	+ \$29	\$0	+ \$29
紅外線	\$3	\$3	\$0
13.56 MHz RFID	\$9	\$9	\$0
總計	\$27	\$21.99	\$169





功能展示

# Fake Airpods

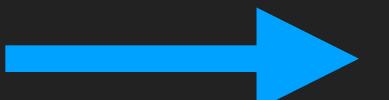


圖片來源：<https://support.apple.com/zh-tw/104989>

# BLE Beacon Emulate



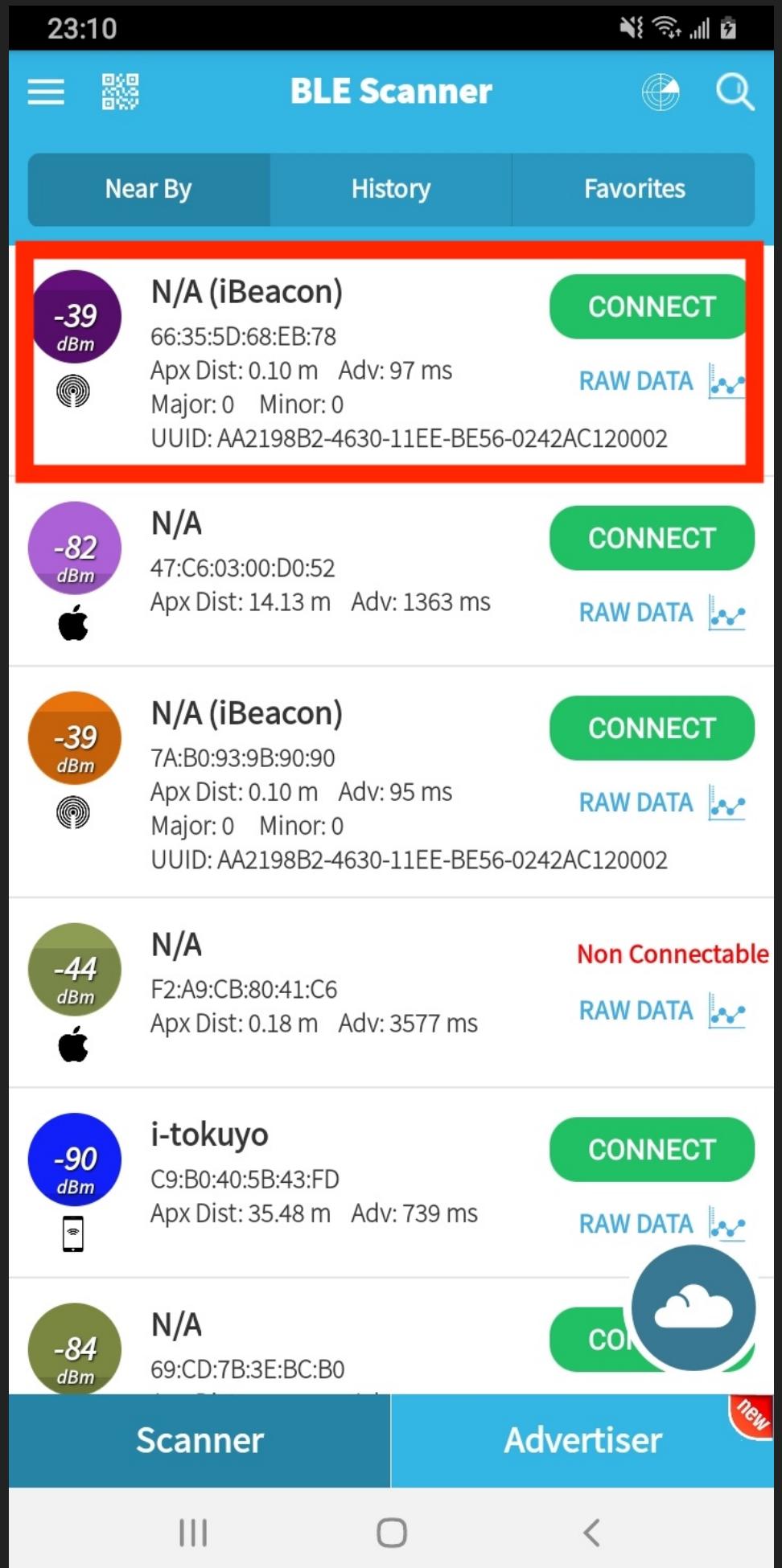
# BLE Beacon Emulate



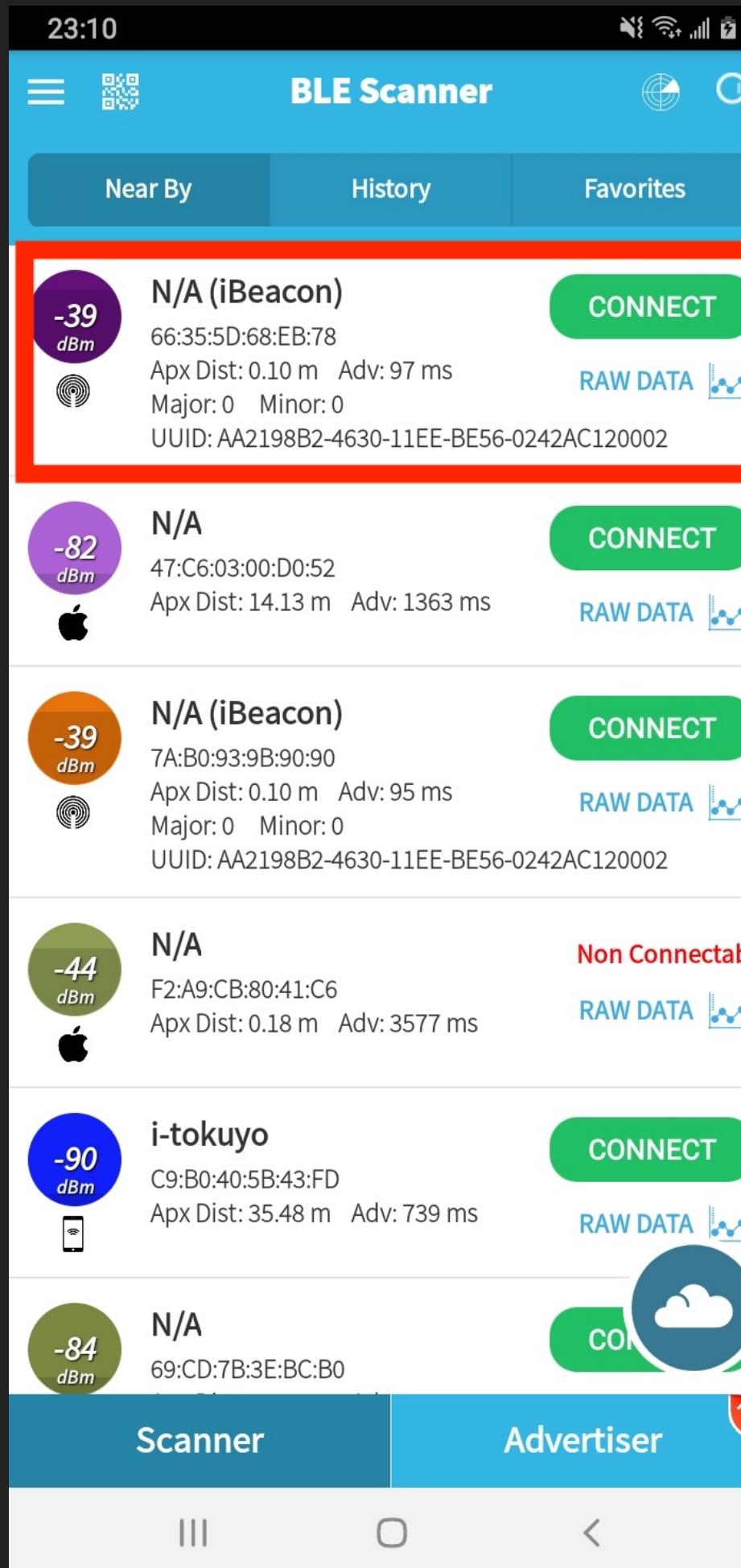
# BLE Beacon Emulate



# BLE Beacon Emulate

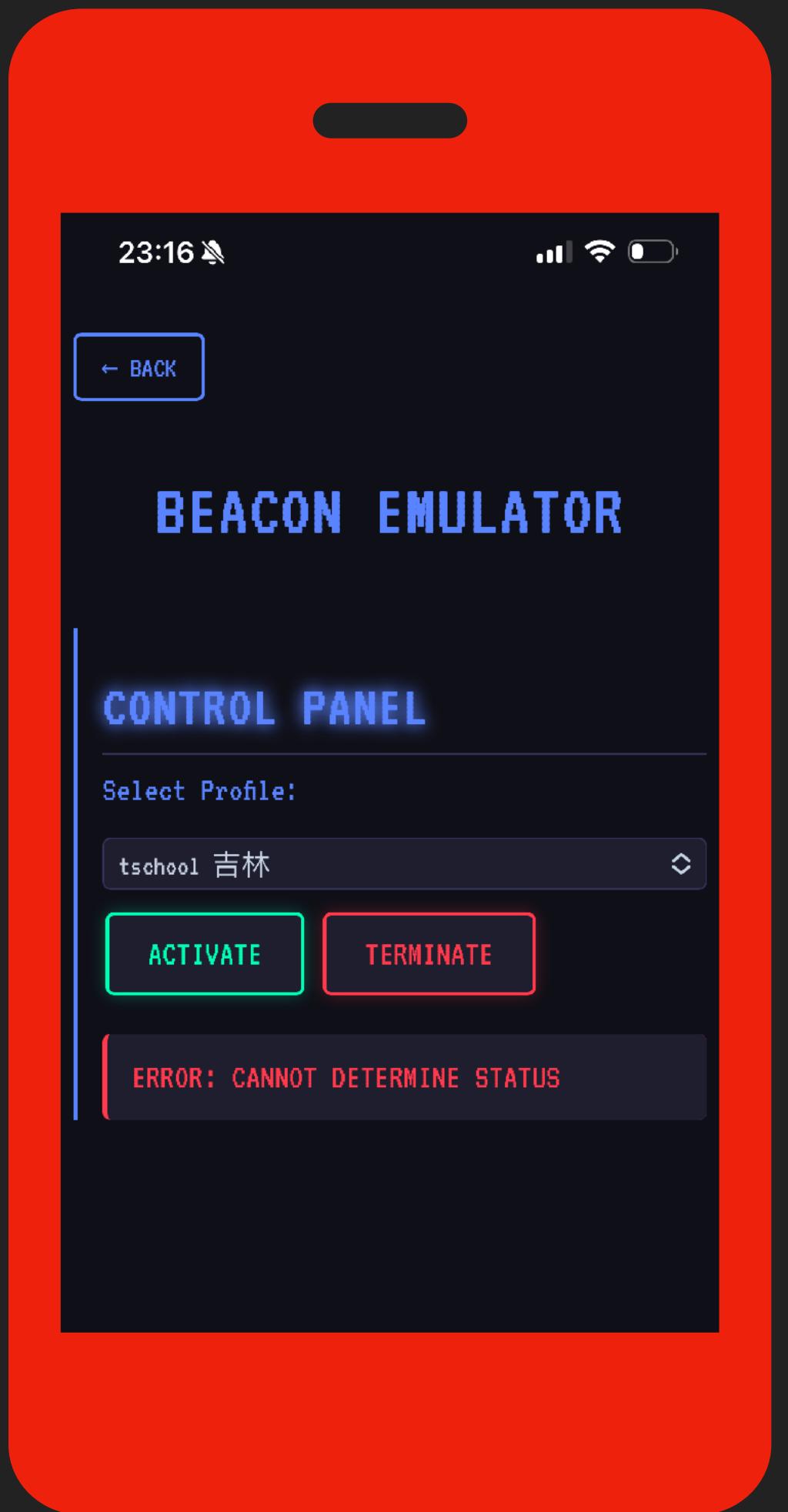
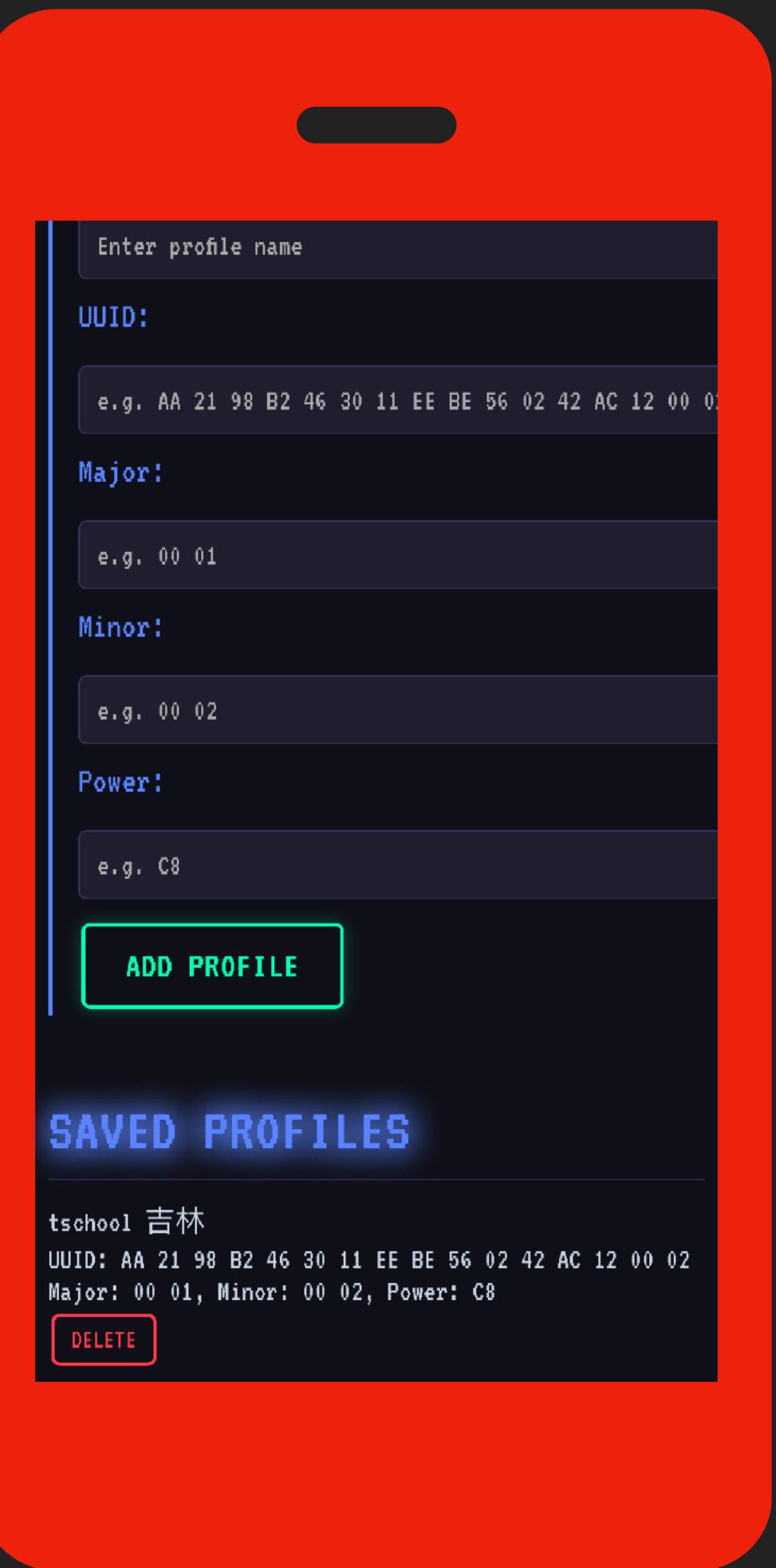


# BLE Beacon Emulate

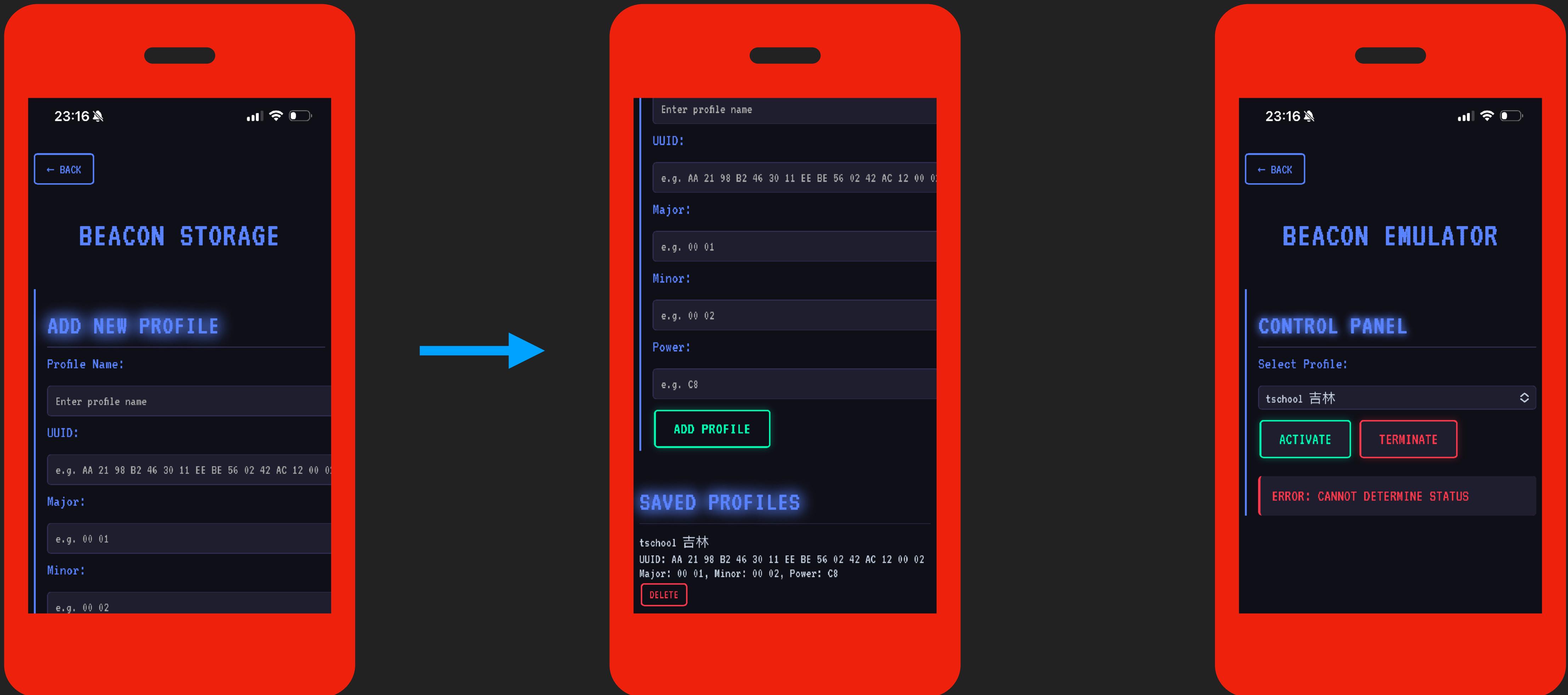


```
const A = [
  {
    identifier: "REALINK_RL400_V100",
    name: "弘道基地",
    uuid: "AA219420-4630-11EE-BE56-0242AC120002",
    mac: "EA:AE:00:00:0B:00"
  },
  {
    identifier: "REALINK_RL400_V100",
    name: "吉林基地",
    uuid: "AA2198B2-4630-11EE-BE56-0242AC120002",
    mac: "EA:AE:00:00:0B:01"
  }
];
function z() {
  const {event: t} = D(),
    [m,d] = c.useState([])
  , [o,x] = c.useState([])
```

# BLE Beacon Emulate



# BLE Beacon Emulate



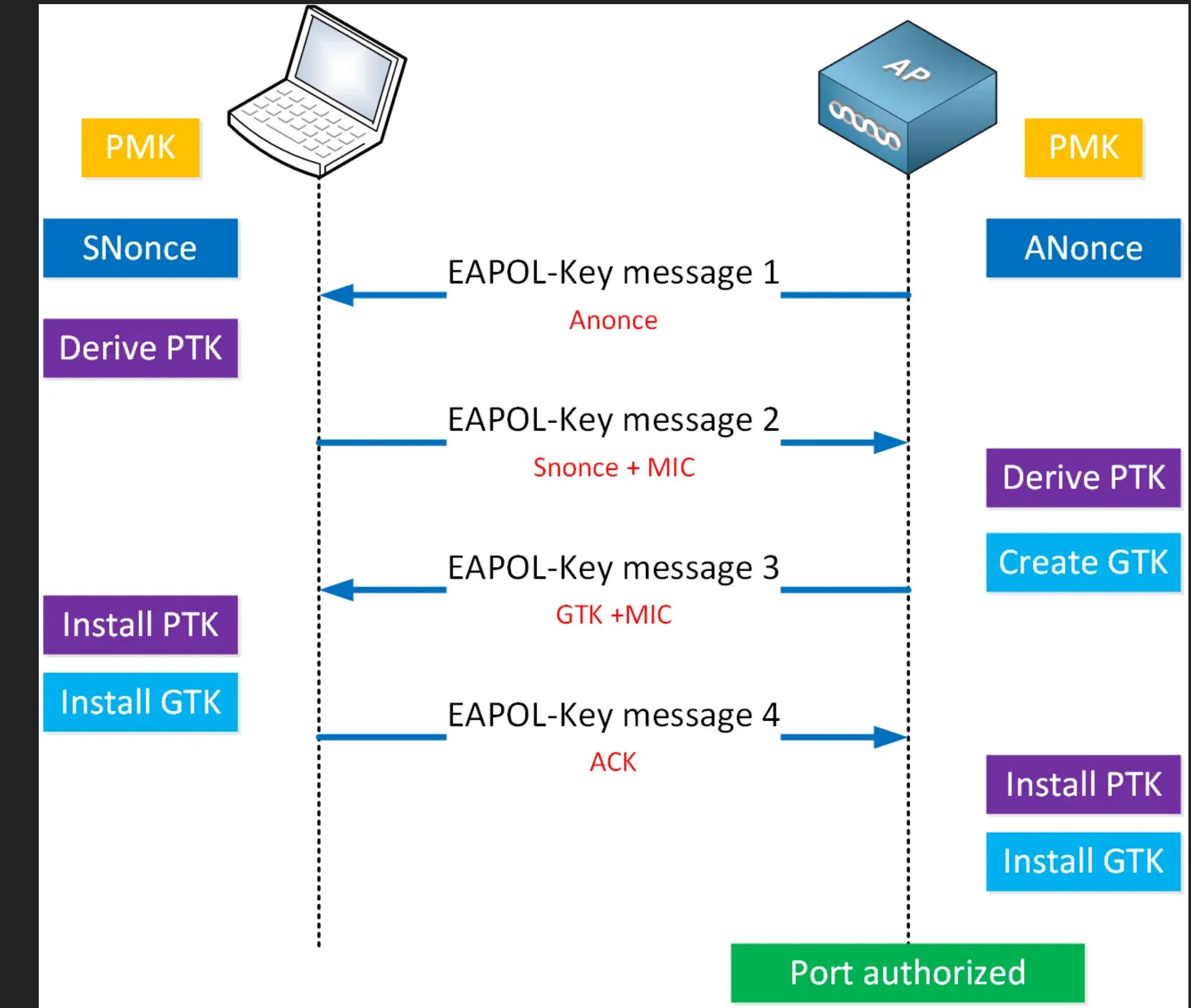
# BLE Beacon Emulate



# 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



The image displays three screenshots of a mobile application for generating password wordlists. The app has a dark-themed interface with orange-red highlights.

**Screenshot 1: Main Screen**

- Time: 22:39
- Buttons: Back
- Title: Password Wordlist Generator
- Text: Enter personal information to generate a targeted wordlist. Add all relevant information about the target.
- Section: Information Guide
- Text: The following information types can be used to generate an effective password wordlist. Please provide as much relevant information as possible:
- Section: Personal Identifiers
- List:
  - Name: Full names, nicknames, or aliases of the target person and their close associates (family members, friends, partners). Also consider including organization names or their abbreviations if relevant.
  - ID: National identification numbers, company unified business numbers, or other official identification codes.
- Section: Contact Information
- List:
  - Phone Number: Mobile or landline numbers, including the two-digit area code prefix. Consider both current and previous numbers.
  - SSID: Wi-Fi network names (SSIDs) used at home, work, or frequently visited locations.

**Screenshot 2: Information Guide**

- Time: 22:39
- Title: Information Guide
- Text: The following information types can be used to generate an effective password wordlist. Please provide as much relevant information as possible:
- Section: Personal Identifiers
- List:
  - Name: Full names, nicknames, or aliases of the target person and their close associates (family members, friends, partners). Also consider including organization names or their abbreviations if relevant.
  - ID: National identification numbers, company unified business numbers, or other official identification codes.
- Section: Contact Information
- List:
  - Phone Number: Mobile or landline numbers, including the two-digit area code prefix. Consider both current and previous numbers.
  - SSID: Wi-Fi network names (SSIDs) used at home, work, or frequently visited locations.

**Screenshot 3: Personal Information Input**

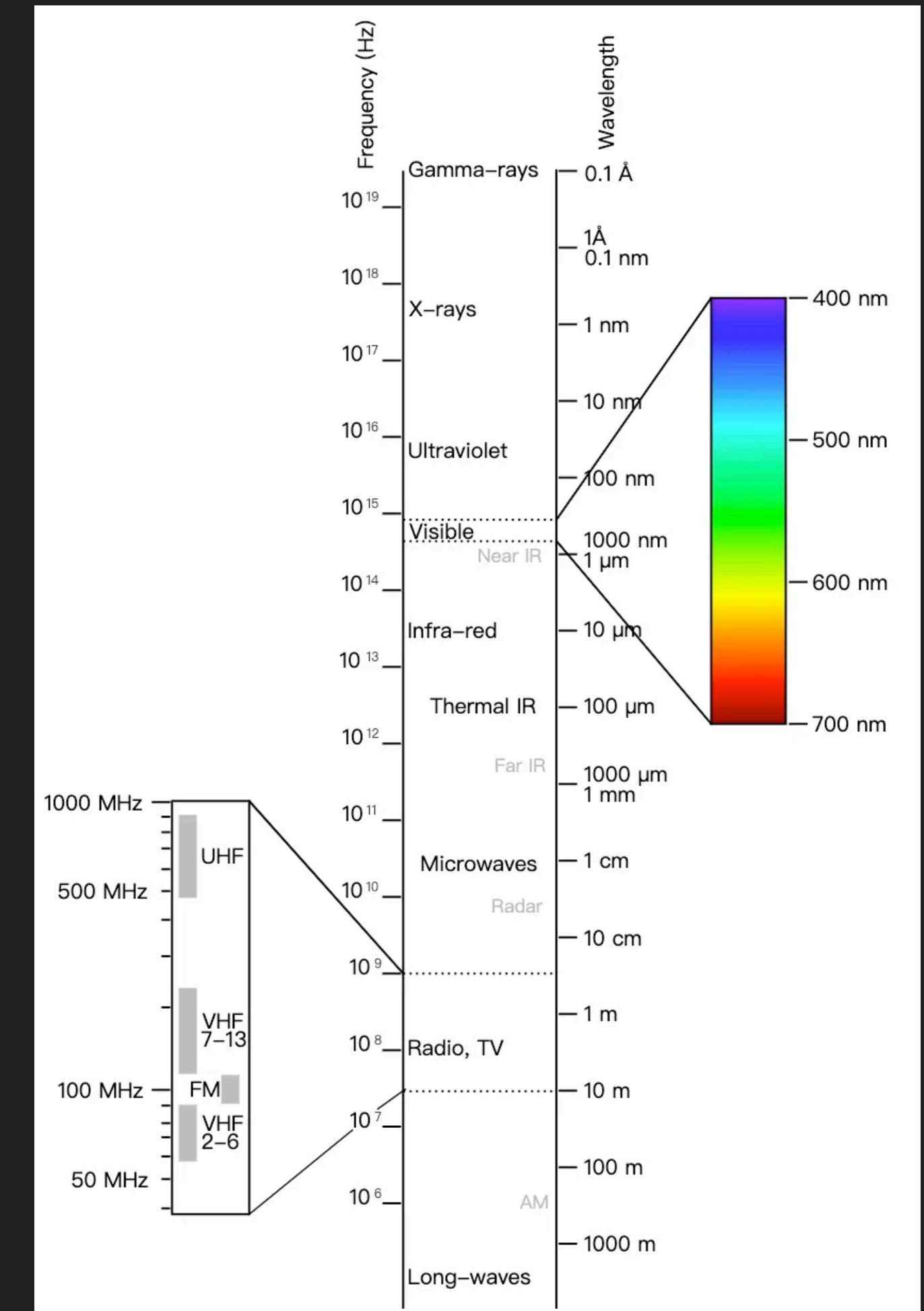
- Time: 22:40
- Text: Output Filename: wordlist.txt
- Section: Personal Information
- Form:

Date
✓ Phone Number
Name
ID Number
Wi-Fi SSID
- Text: + Add Info Type
- Text: Generate Wordlist

# Introduction of Infrared (IR)

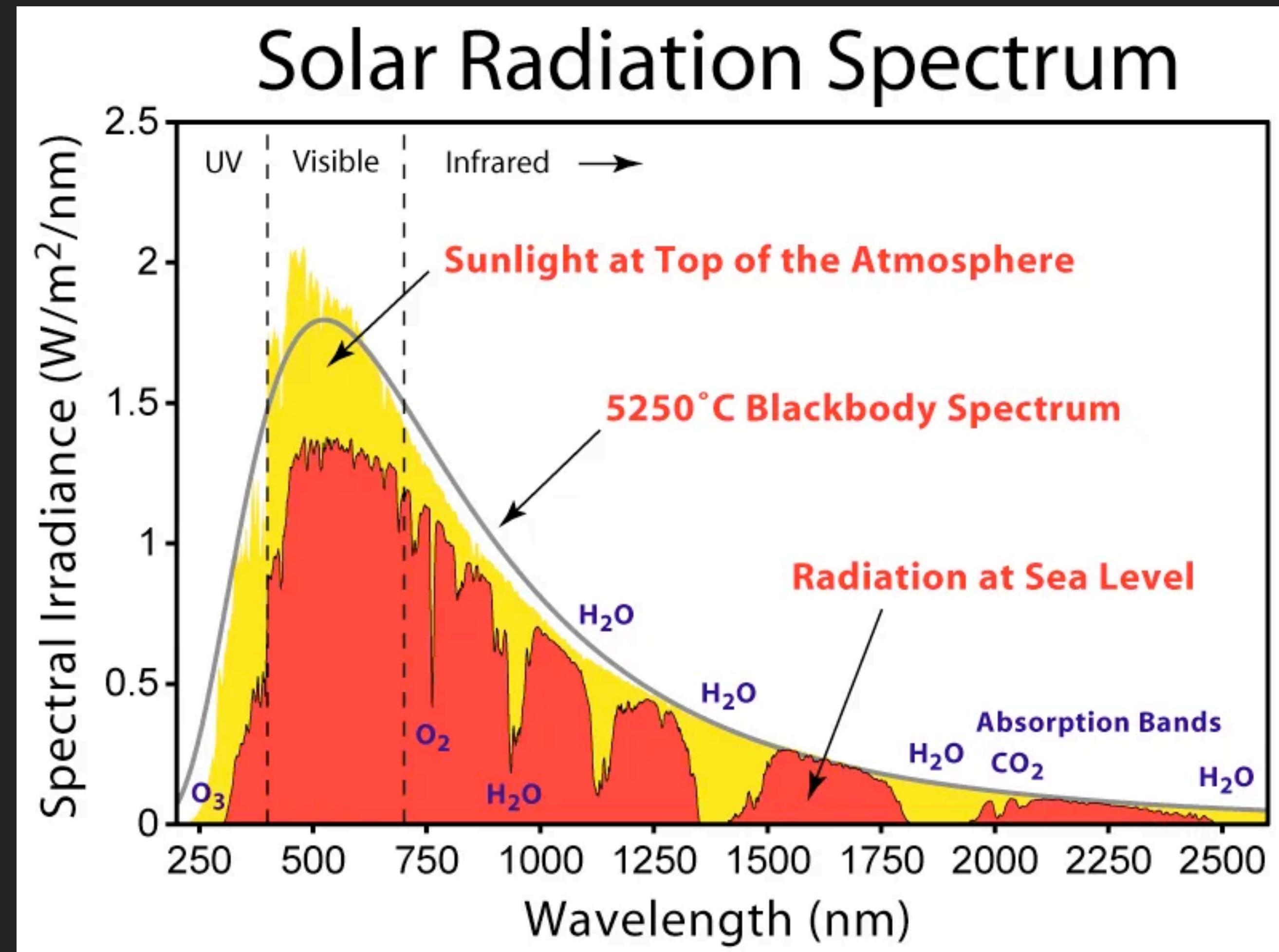


- 波長：950 nm
- 頻率
  - NEC : 38Khz
  - RC-5 : 36Khz
  - RC-6 : 36 KHz
  - Panasonic : 36.7 KHz
  - Sharp : 38KHz
  - Sony : 40KHz
  - RCA : 56Khz



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

# Introduction of Infrared (IR)

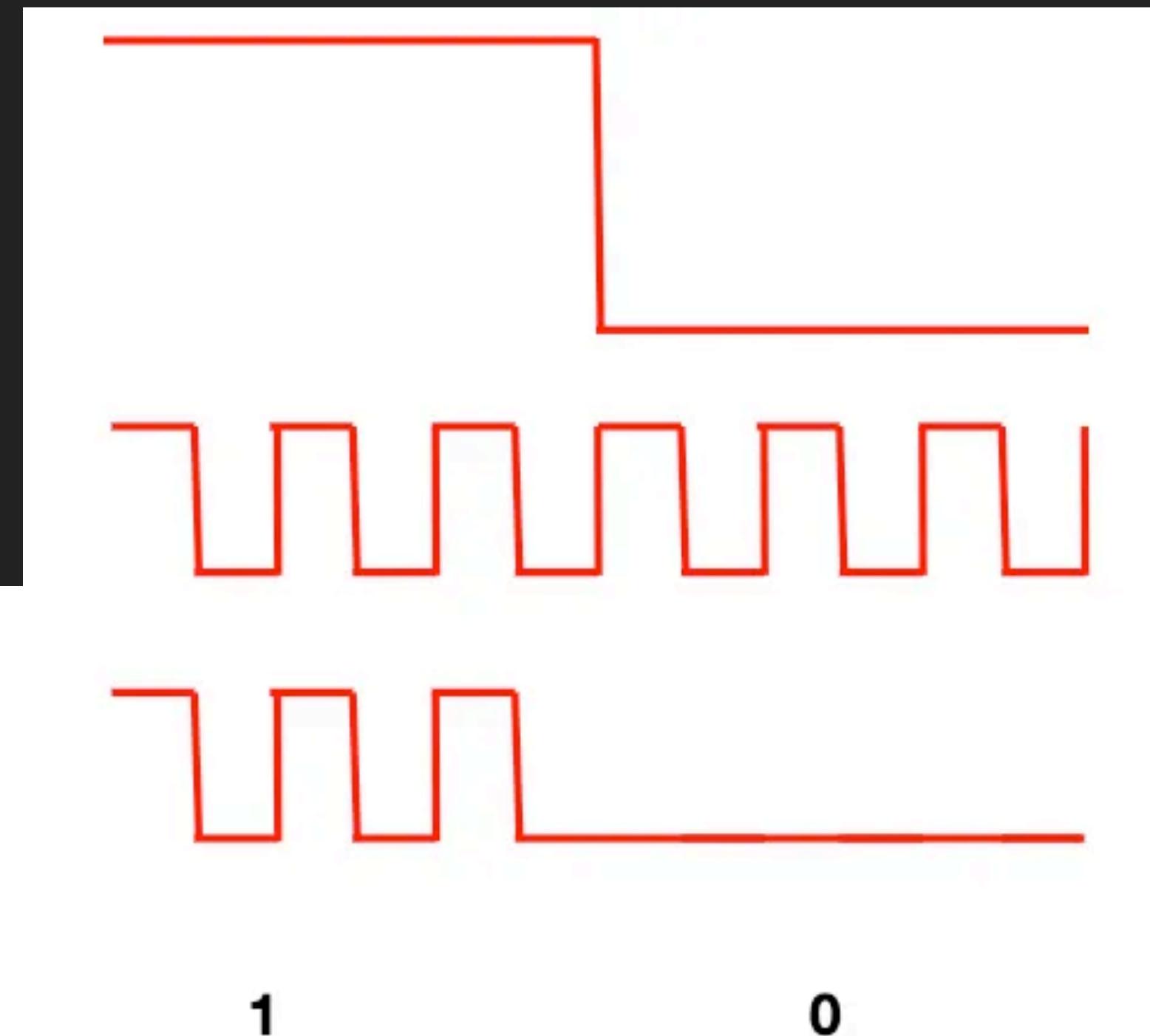


圖片來源：<https://commons.wikimedia.org/w/index.php?curid=2623187>

# Introduction of Infrared (IR)

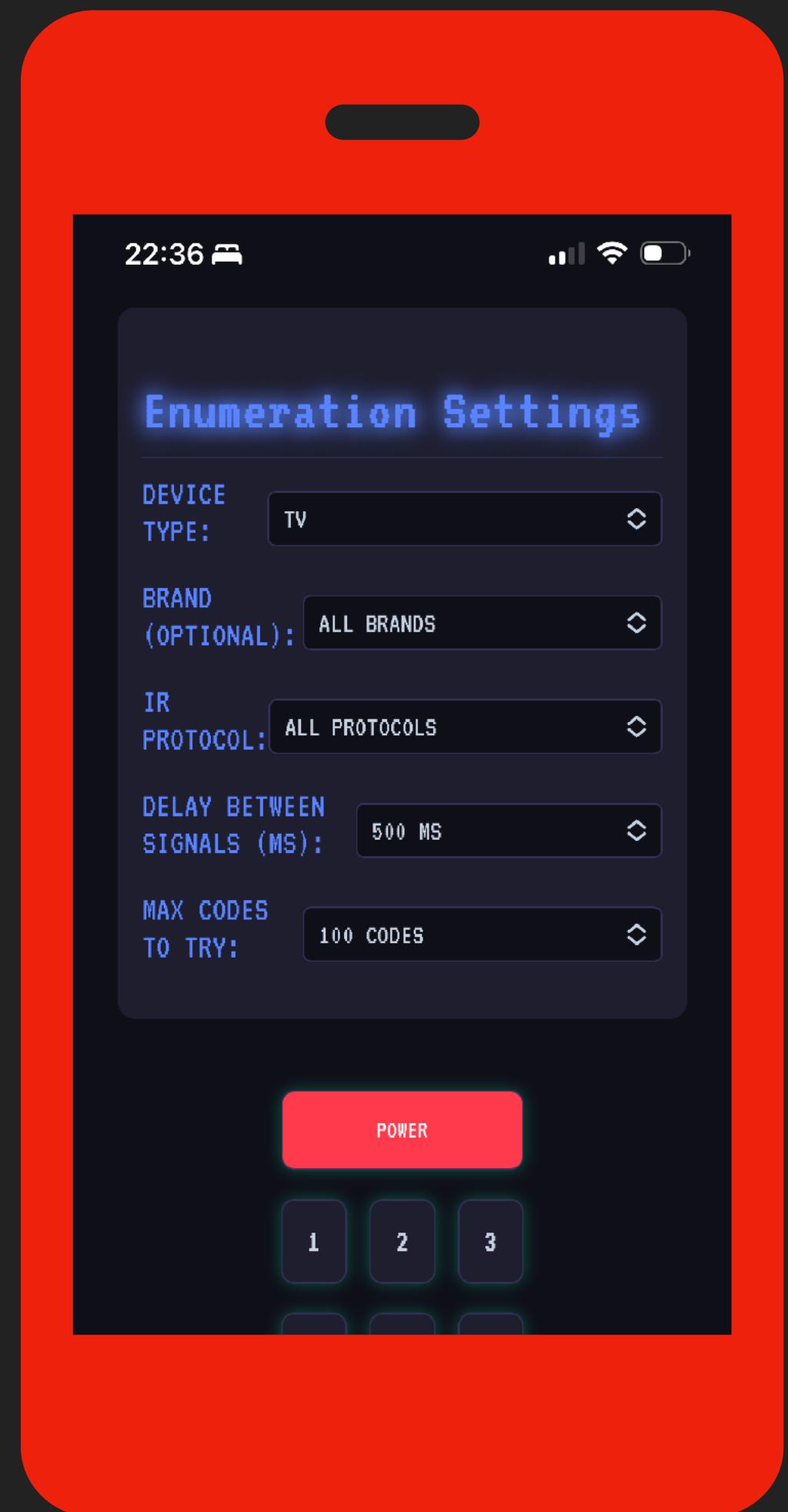


- 使用載波 (carrier wave)
  - 減少干擾
  - 避免過熱、增加亮度



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

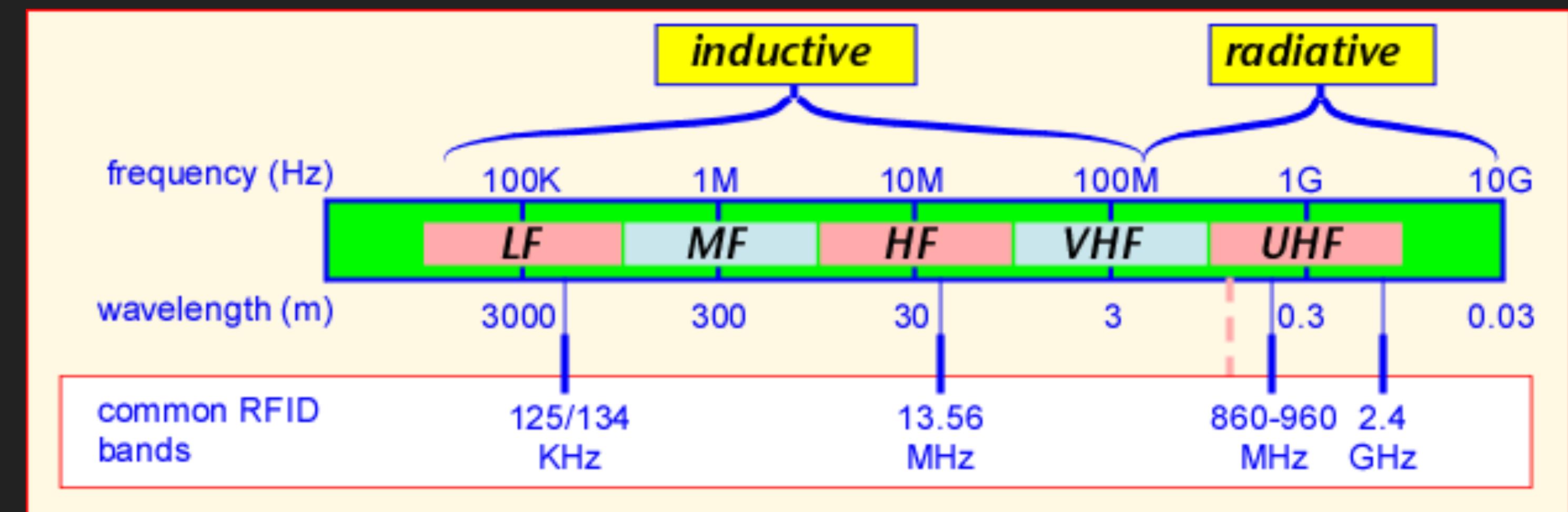
# IR Signal Learner and Enumerator



# Introduction of RFID



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



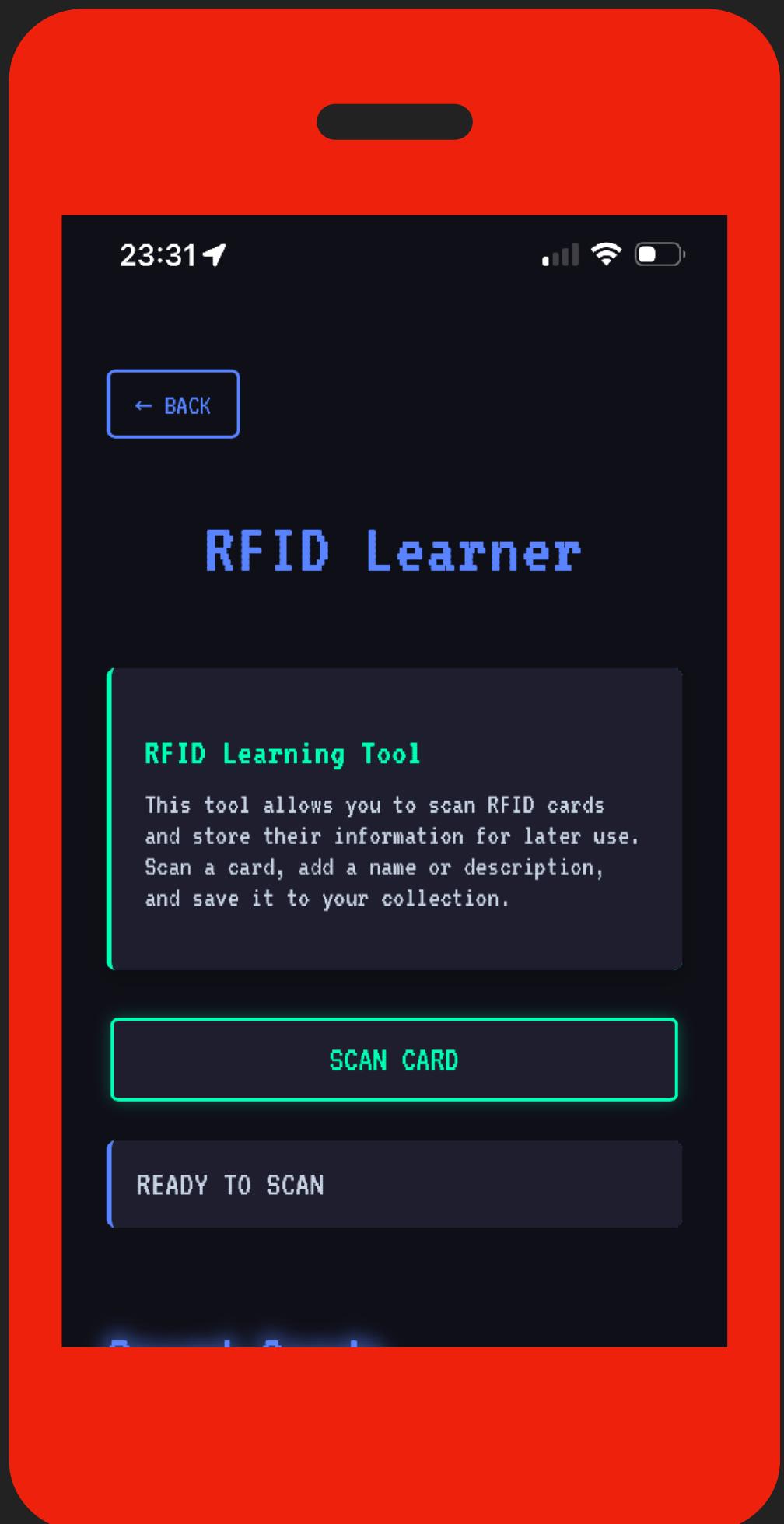
圖片來源：<https://polygait.calpoly.edu/what-rfid/types-of-rfid>

# 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





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

# 官方文件和 README.md



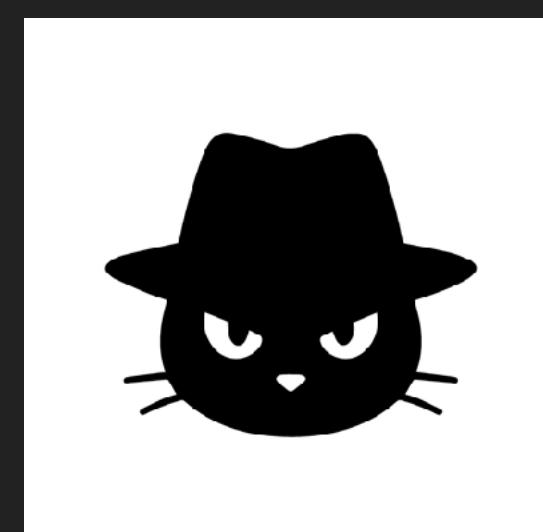
<https://hackmasterpi.org>



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

幫按星星

# Logo 設計



# Logo 設計



ChatGPT 說：  
設計費可以收 6000

# Logo 設計



ChatGPT 說：  
設計費可以收 6000

< 發票明細 條碼

新光三越百貨股份有限公司台...  
114年05-06月  
尚未開獎 NC73471769  
2025/05/13 18:04:52 手機條碼 /HB2MYXZ

交易明細

營業人統編:28433909	小計
門市地址:台北市中山區南京西路15號	165
品名(數量)	
小吃 Food Court(1)	
共 1 項	合計 165

# 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。



您所提交的草稿仍需改善。在2025年7月29日由Shawwww (留言)審閱。

過於依賴第一手來源，即非常接近於事件本身的來源。請補充更多可靠的、第三方的、公開的來源。

宣傳語氣較強烈，維基百科不是宣傳工具，無論是對公司、產品、個人還是觀點介紹的條目，必須客觀且不偏頗及避免宣傳語調。所有條目都必須附有獨立第三方來源以備查證。

• 另請參見Wikipedia:如何介紹自己的公司和公開利益衝突

- 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29日由Shawwww (留言)審閱。 · 最後由Shawwww於1小時前編輯。通知作者

再次提交 請注意，如果問題未得到解決，草稿將再次被拒絕。

您所提交的草稿仍需改善。在2025年7月28日由Kanshui0943 (留言)審閱。

許多段落無來源，WP:CITE

如何改善您的草稿 [展開]

在2025年7月28日由Kanshui0943 (留言)審閱。 ·

您所提交的草稿仍需改善。在2025年7月17日由Sakurase (留言)審閱。

前述問題未解決。

如何改善您的草稿 [展開]

在2025年7月17日由Sakurase (留言)審閱。 ·

您所提交的草稿仍需改善。在2025年7月17日由Sakurase (留言)審閱。

條目中很少或者沒有獨立於主題實體的可靠來源，只有符合收錄標準的條目才會被維基百科收錄。如果一個主題得到了可靠來源的有效介紹，而且這些來源獨立於主題實體，則可假定該主題或符合獨立條目的收錄標準。

- 「可靠來源」：包括但不限於媒體報道、學術文獻、書籍等。滿足收錄標準的來源，應該是第二手來源（二次文獻），並且能經得起可靠來源指引對收錄標準進行的可供查證性評定，多方來源會更受歡迎。
- 「獨立於主題實體」：自我宣傳、廣告、自身發表的個人出版物、自傳、新聞稿等均不算在內。
- 「有效介紹」：來源直接、詳細講解了主題的實體，而非僅僅是順帶提及，編者無需通過原創研究來發掘條目的內容。

如何改善您的草稿 [展開]

在2025年7月17日由Sakurase (留言)審閱。 ·

需要補充更多的可靠來源，維基百科需要以具有公信力的出版者記錄或發表過的事件、主張、理論、概念、意見和論證作為編寫依據，使得內容符合可供查證的方針。請多使用第二手來源（二次文獻），並且能經得起可靠來源指引對收錄標準進行的可供查證性評定，多方來源會更受歡迎。如果您在如何添加來源上存在困難，請參見幫助:如何引用來源。

如何改善您的草稿 [展開]

在2025年7月17日由Sakurase (留言)審閱。 ·

# 宣傳



# Thank you

## Contact

- Email: [52sunyiping@gmail.com](mailto:52sunyiping@gmail.com)
- GitHub: <https://github.com/1PingSun>
- Blog: <https://1ping.org/>

