# RFID module protocol (RFIDUSBE1)

## 1.Test command

| Byte | Byte 0～5 (長度固定) |
|---|---|
| Send | 07 04 03 03 01 04 |

| Byte | Byte 0～4 (長度固定) |
|---|---|
| Return | DE 03 03 FF 00 |

## 2.Scan command

| Byte | Byte 0～19 (長度固定) Via USB |
|---|---|
| Send | 07 11 00 86 00 02 00 00 00 0D 8C 00 05 00 00 01 01 00 01 06 |

| Byte | Byte 0～14 (長度固定) Via USB |
|---|---|
| Return | 71 0C 00 05 00 00 00 07 01 00 00 00 A8 0D 0E |

沒有 Tag 的時候

Byte 0=71 代表流水號

Byte 1=0C 表示後面還有多少 byte 資料

Byte 6～7=00 07 表示後面還有多少 byte 資料

Byte 10=00 表示收到多少 TAG

Byte 12～14=A80D0E 代表掃描的頻率，前後 byte 對調再轉 10 進制 0E 0D A8=921000KHz=921MHz

| Byte | Byte 0～30 (長度非固定) Via USB |
|---|---|
| Return | 71 1C 00 05 00 00 00 17 01 00 01 AA C9 A8 0D 0E 0E 34 00 E2 00 20 19 77 04 02 25 16 91 72 68 |

有 Tag 的時候

Byte 0=71 代表流水號

Byte 1=1C 表示後面還有多少 byte 資料

Byte 6～7=00 17 表示後面還有多少 byte 資料

Byte 8 當設備處於掃描狀態時，此 BYTE 一直為 01，當設備接收到停止掃描命令後，此 BYTE 會變成 0

Byte 10=01 表示收到多少 TAG,現固定為 1

Byte 11=AA 如果 Tag 在之前出現過，輸出為 AA；如果沒有在收到的最後 64 張 Tag 中，則以流水號出現；如果輸出為 0x80，則說明有超過 64Byte 的 Tag 有收到

Byte 12=C9 表示該 TAG 的 RSSI 值：0x100-0xC9=0x37(-55dBm)

Byte 13～15= A80D0E 代表掃描的頻率，前後 byte 對調再轉 10 進制 0E0DA8=921000KHz=921MHz

Byte 16=0E 代表此 TAG 資料共有多少 byte：PC+EPC

Byte 17～18=34 00 是 TAG 的 PC(Tag assortment)，EPC 碼的長度由 TAG 的 PC 來決定輸出多少 Byte 的資料，計算方式如下

3400/400 = 0D (13 Byte)由於是用字元為單位所以把只算雙數.所以是輸出 12 Byte EPC

Byte 19～End = E2 00 20 19 77 04 02 25 16 91 72 68 都是 TAG 的 EPC 碼

範例:收到 1 張短 EPC 碼的 TAG，注：新板都只有 1 張 Tag 的資料上傳，由於 USB 協定以塊為單位傳送，如果收到的資料包超過定義的格式，需由軟體自動丟棄多餘的資料。

Return: 71 00 00 16 05 00 00 00 11 01 00 01 8F FB A8 0D 0E 08 18 00 E2 00 20 47 35 08

解析如下

71 00 00 16 05 00 00 00 11 01 00 01 代表此數據包含了 1 張 TAG 資訊

8F FB A8 0D 0E 08 18 00 E2 00 20 47 35 08 TAG 資訊， 18 00/400 = 06 (6 Byte)所以是輸出 6 Byte EPC

# 3.Stop command

| Byte | Byte 0～12(長度固定) Via USB |
|---|---|
| Send | 08 0A 00 8C 00 05 00 00 01 00 00 00 00 |

| Byte | Byte 0～14 (長度固定) Via USB |
|---|---|
| Return | 8A 0C 00 05 00 00 00 07 00 00 00 00 96 10 0E |
| | 返回參數見上說明 |

# 4.Read Bank Area command

| Byte | Byte 0～28 (長度非固定) Via USB |
|---|---|
| Send | 81 1A 00 06 00 15 00 00 02 00 00 01 20 00 60 00 99 99 99 99 99 99 99 99 99 99 99 99 99 AA |

Byte 1=1A 表示後面還有多少 byte 資料 (從 Byte 3 開始計算)

Byte 3=06 Select Tag

Byte 5=15 表示後面還有多少 byte 有效資料 (從 Byte 8 開始計算)

Byte 16～27=99 99 99 99 99 99 99 99 99 99 99 99 輸入要讀取 TAG 的 EPC，位元數依照 EPC 長度變化

| Byte | Byte 0～7 (長度固定) Via USB |
|---|---|
| Return | 11 05 00 06 00 00 00 00 |

Byte 1=05 表示後面還有多少 byte 資料 (從 Byte 3 開始計算)

Byte 7=00 表示後面還有多少 byte 資料

| Byte | Byte 0～16 (長度固定) Via USB |
|---|---|
| Send | 82 0E 00 08 00 09 00 81 00 00 00 00 06 11 11 11 11 |

Byte 1=0E 表示後面還有多少 byte 資料 (從 Byte 3 開始計算)

Byte 3=08 Read command

Byte 4～5=00 09 表示後面還有多少 byte 有效資料 (從 Byte 9 開始計算)

Byte 8=00 選擇要讀取的區塊，對照如下

Bank Area 00 = Reserved

01 = EPC

02 = TID

03 = User

Byte 9～11=00 00 00 選擇讀取區塊的起始位置，低位在前：如從 01 位址開始，則為 01 00 00

Byte 12=06 從指定的記憶體中讀多少個字，必須指定，如果為 0，則默認讀 8 個字

Byte 13～16=11 11 11 11 輸入要讀取 TAG 的 Access Password，訪問密碼必須跟 Tag 的一樣，否則讀不出資料

| Byte | Byte 0～N (長度非固定) Via USB |
|---|---|
| Return | 27 0E 00 08 00 DE 00 09 00 00 00 00 00 00 00 00 03 |

讀取成功的時候

Byte 1=0E 表示後面還有多少 byte 資料 (從 Byte 3 開始計算)

Byte 5=DE 表示讀取狀態，對照如下

09=讀 TAG 存儲區失敗

16=訪問密碼不對

A3=讀的資料長度超過 TAG 的長度，或不支援的卡片類型

A4=指定的 TAG 存儲區被鎖定並且是永久鎖定，而且鎖定狀態為不可讀寫

AB=TAG 離 reader 太遠

A0=其它錯誤

AF=其它錯誤

Byte 7=09 表示後面還有多少 byte 資料

Byte 8=00 00 00 00 00 00 00 00 表示讀出的資料

範例: 讀取 TAG EPC 為 333332CDE549503131DD9540 的 Reserved 區塊失敗的時候資料如下

Send: 8100001A06001500000200000120006000333332CDE549503131DD9540AA

Return: 1F 00 00 05 06 00 00 00 00

Send: 8200000E0800090081000000000000000000

Return:20 00 00 06 08 00 09 00 01 00

範例: 讀取 TAG EPC 為 333332CDE549503131DD9540 的 Reserved 區塊密碼錯誤的時候

資料如下

Send: 8100001A06001500000200000120006000333332CDE549503131DD9540AA

Return: 1C 00 00 05 06 00 00 00 00

Send: 8200000E08000900810000000000000000011

Return:2E 00 00 06 08 00 16 00 01 00

範例: 讀取 EPC 區塊成功

資料如下

Send: 8100001A06001500000200000120006000333332CDE549503131DD9540AA

Return: 13 00 00 05 06 00 00 00 00

Send: 8200000E08000900810100000000000000000

Return: 24 00 00 1A 08 00 DE 00 15 2C 5D 34 00 33 33 32 CD E5 49 50 31 31 DD 95 40 31 DD 95 40 03

# 5.Write Bank Area command

| Byte | Byte 0～28 (長度非固定) Via USB |
|---|---|
| Send | 81 1A 00 06 00 15 00 00 02 00 00 01 20 00 60 00 99 99 99 99 99 99 99 99 99 99 99 99 AA |

Byte 1=1A 表示後面還有多少 byte 資料(從 Byte 3 開始計算)

Byte 3=06 Select Tag

Byte 5=15 表示後面還有多少 byte 有效資料 (從 Byte 8 開始計算)

Byte 16～27=99 99 99 99 99 99 99 99 99 99 99 99 輸入要讀取 TAG 的 EPC，位元數依照 EPC 長度變化

| Byte | Byte 0～7 (長度固定) Via USB |
|---|---|
| Return | 11 05 00 06 00 00 00 00 |

Byte 1=05 表示後面還有多少 byte 資料(從 Byte 3 開始計算)

Byte 7=00 表示後面還有多少 byte 資料

| Byte | Byte 0～16 (長度非固定) Via USB |
|---|---|
| Send | 82 12 00 07 00 0D 00 02 03 00 00 00 00 00 00 00 00 11 11 11 11 |

Byte 1=12 表示後面還有多少 byte 資料(從 Byte 3 開始計算)

Byte 3=07 Write command

Byte 4～5=00 0D 表示後面還有多少 byte 有效資料 (從 Byte 8 開始計算)

Byte 8=03 選擇要讀取的區塊，對照如下

Bank Area 00 = Reserved

01 = EPC (byte 9~12 需填入 02 00 00 00)

02 = TID

03 = User

Byte 9～12=00 00 00 00 選擇讀取區塊的起始位置(若是 01 00 00 00 則表示從第 1 個字元開始寫入,若是 03 00 00 00 擇從第 3 個字元開始寫入)

Byte 13～16=00 00 00 00 輸入要讀取 TAG 的 Access Password

Byte 17～N=11 11 11 11 輸入要寫入 TAG 的資料，最少需要輸入 1 個字元(1 個字元=2 個 Byte)

若修改 EPC 碼的長度必須要從位置 01 開始寫入，修改成 12 碼時 01 位置要填入 3000，修改成 14 碼時 01 位置要填入 3800，修改成 16 碼時 01 位置要填入 4000 以下是範例從 12 碼修改成 16 碼

81 1A 00 06 00 15 00 00 02 00 00 01 20 00 60 00 20 13 09 24 87 26 03 00 01 02 00 22 AA

82 20 00 07 00 1B 00 02 01 01 00 00 00 00 00 00 00 40 00 E2 00 10 21 50 07 00 52 20 20 44 0C 12 34 56 78

| Byte | Byte 0～9 (長度固定) Via USB |
|---|---|
| Return | 2A 07 00 07 00 00 00 02 02 A5 |

讀取成功的時候

Byte 1=07 表示後面還有多少 byte 資料(從 Byte 3 開始計算)

Byte 5=00 表示寫入狀態，對照如下

10=寫 TAG 存儲區失敗

16=訪問密碼不對

B3=讀的資料長度超過 TAG 的長度，或不支援的卡片類型

B4=指定的 TAG 存儲區被鎖定並且是永久鎖定，而且鎖定狀態為不可讀寫

BB=TAG 離 reader 太遠

B0=其它錯誤

BF=其它錯誤

Byte 7=02 表示後面還有多少 byte 資料

Byte 8=02 表示寫入成功的字元數 (1 個字元=2 個 Byte)

# 6. Unlock Lock&Premalock command

| 7. Byte | Byte 0～28 (長度非固定) Via USB |
|---|---|
| Send | 81 1A 00 06 00 15 00 00 02 00 00 01 20 00 60 00 99 99 99 99 99 99 99 99 99 99 99 99 99 AA |

Byte 1=1A 表示後面還有多少 byte 資料(從 Byte 3 開始計算)

Byte 3=06 Select Tag

Byte 5=15 表示後面還有多少 byte 有效資料 (從 Byte 8 開始計算)

Byte 16～27=99 99 99 99 99 99 99 99 99 99 99 99 輸入要讀取 TAG 的 EPC，位元數依照 EPC 長度變化

| Byte | Byte 0～7 (長度固定) Via USB |
|---|---|
| Return | 11 05 00 06 00 00 00 00 |

Byte 1=05 表示後面還有多少 byte 資料(從 Byte 3 開始計算)

Byte 7=00 表示後面還有多少 byte 資料

| Byte | Byte 0～14 (長度固定) Via USB |
|---|---|
| Send | 82 0C 00 09 00 07 00 01 C0 00 00 00 00 00 00 |

Byte 1=0C 表示後面還有多少 byte 資料

Byte 3=09 Unlock Lock&Premalock command

Byte 4～5=00 07 表示後面還有多少 byte 有效資料 (從 Byte 9 開始計算)

Byte 8～9=C0 00 選擇要操作的區塊，對照如下（其中 BYTE9 的 BIT7~6，是選擇區操作）

Bank Area C0 00 = Kill password 區

30 00 = Access password 區

0C 00 = EPC 區

03 00 = TID 區

00 C0 = User 區

Byte 9~10=00 00 選擇操作指令

BYTE9 的 BIT5~4：指示對 Kill 密碼區操作

BYTE9 的 BIT3~2：指示對訪問密碼區操作

BYTE9 的 BIT1~0：指示對 EPC 區操作

BYTE10 的 BIT7~6：指示對 TID 區操作

BYTE10 的 BIT5~4：指示對 USER 區操作

Command 00 = Unlock

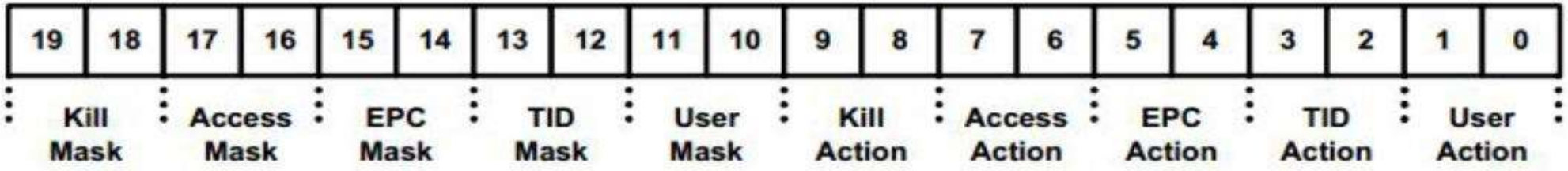
01 = Premalock

10 = Lock

11 = Lock&Premalock

Byte 11～14=00 00 00 00 輸入 TAG 的 Access Password

## Lock-Command Payload




## Masks and Associated Action Fields

| | Kill pwd | | Access pwd | | EPC memory | | TID memory | | User memory | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 |
| *Mask* | skip/ write | skip/ write | skip/ write | skip/ write | skip/ write | skip/ write | skip/ write | skip/ write | skip/ write | skip/ write |
| | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| *Action* | pwd read/ write | perma lock | pwd read/ write | perma lock | pwd write | perma lock | pwd write | perma lock | pwd write | perma lock |

| Byte | Byte 0～8 (長度固定) Via USB |
|---|---|
| Return | 22 06 00 09 00 DE 00 01 6C |

讀取成功的時候

Byte 1=06 表示後面還有多少 byte 資料

Byte 5=DE 表示寫入狀態，對照如下

13=寫 TAG 存儲區失敗

16=訪問密碼不對

C3=讀的資料長度超過 TAG 的長度，或不支援的卡片類型

C4=指定的 TAG 存儲區被鎖定並且是永久鎖定，而且鎖定狀態為不可讀寫

CB=TAG 離 reader 太遠

C0=其它錯誤

CF=其它錯誤

Byte 7=01 表示後面還有多少 byte 資料

# 8.Kill Tag command

| Byte | Byte 0～28 (長度非固定) Via USB |
|---|---|
| Send | 81 1A 00 06 00 15 00 00 02 00 00 01 20 00 60 00 99 99 99 99 99 99 99 99 99 99 99 99 99 AA |

Byte 3=06 Select Tag

Byte 16～27=99 99 99 99 99 99 99 99 99 99 99 99 輸入要讀取 TAG 的 EPC，位元數依照 EPC 長度變化

| Byte | Byte 0～7 (長度固定) Via USB |
|---|---|

| Return | 11 05 00 06 00 00 00 00 |
|---|---|

Byte 1=05 表示後面還有多少 byte 資料

Byte 7=00 表示後面還有多少 byte 資料

| Byte | Byte 0～13 (長度固定) Via USB |
|---|---|
| Send | 82 0B 00 0A 00 06 00 01 00 00 00 00 00 00 |

Byte 1=0B 表示後面還有多少 byte 資料

Byte 3=0A Kill command

Byte 4～5=00 06 表示後面還有多少 byte 有效資料 (從 Byte 9 開始計算)

Byte 8～11=00 00 00 00 輸入 TAG 的 Kill password

| Byte | Byte 0～8(長度固定) Via USB |
|---|---|
| Return | 22 06 00 0A 00 00 00 01 A5 |

讀取成功的時候

Byte 1=06 表示後面還有多少 byte 資料

Byte 5=00 表示寫入狀態，對照如下

00=" Success"

12=滅活 TAG 失敗

16=訪問密碼不對

D3=讀的資料長度超過 TAG 的長度，或不支援的卡片類型

D4=指定的 TAG 存儲區被鎖定並且是永久鎖定，而且鎖定狀態為不可讀寫

DB=TAG 離 reader 太遠

D0=其它錯誤

DF=其它錯誤

Byte 7=01 表示後面還有多少 byte 資料

# 9.Set command

範例:接收感度 = 0110 Session=S1,Coding=FM0,Q_begin=4,Tari=12.5us,Pilot Tone = On

| Byte | Byte 0～23 (長度固定) Via USB |
|---|---|
| Send | 18 15 00 03 00 10 00 10 01 10 01 00 01 01 01 01 01 01 04 00 84 01 00 |

Byte 8~9=01 10 表示接收感度(範圍：0030~0130)十六制數據，共 16 階(0x30/0x40/0x50/…/0xF0/0x100/0x110/0x120/0x130)

Byte 13=01 表示 Session，對照如下

00= S0

01= S1

02= S2

03= S3

Byte 15=01 表示 Pilot Tone，對照如下

01= 固定為 01

Byte 17=01 表示 Tari，對照如下

01= 固定為 01

Byte 19=04 表示 Q_begin，對照如下

00～07= 0～7

| Byte | Byte 0～23(長度固定) Via USB |
|---|---|
| Return | AA 15 00 03 00 00 00 10 01 10 00 00 00 01 00 01 00 01 00 04 00 00 00 00 |

# 10. 修改功率(RFIDUSB9 只支持功率設定)

範例: 綠色區域：最小為 0x10(16)，最大為 0x2F(47)

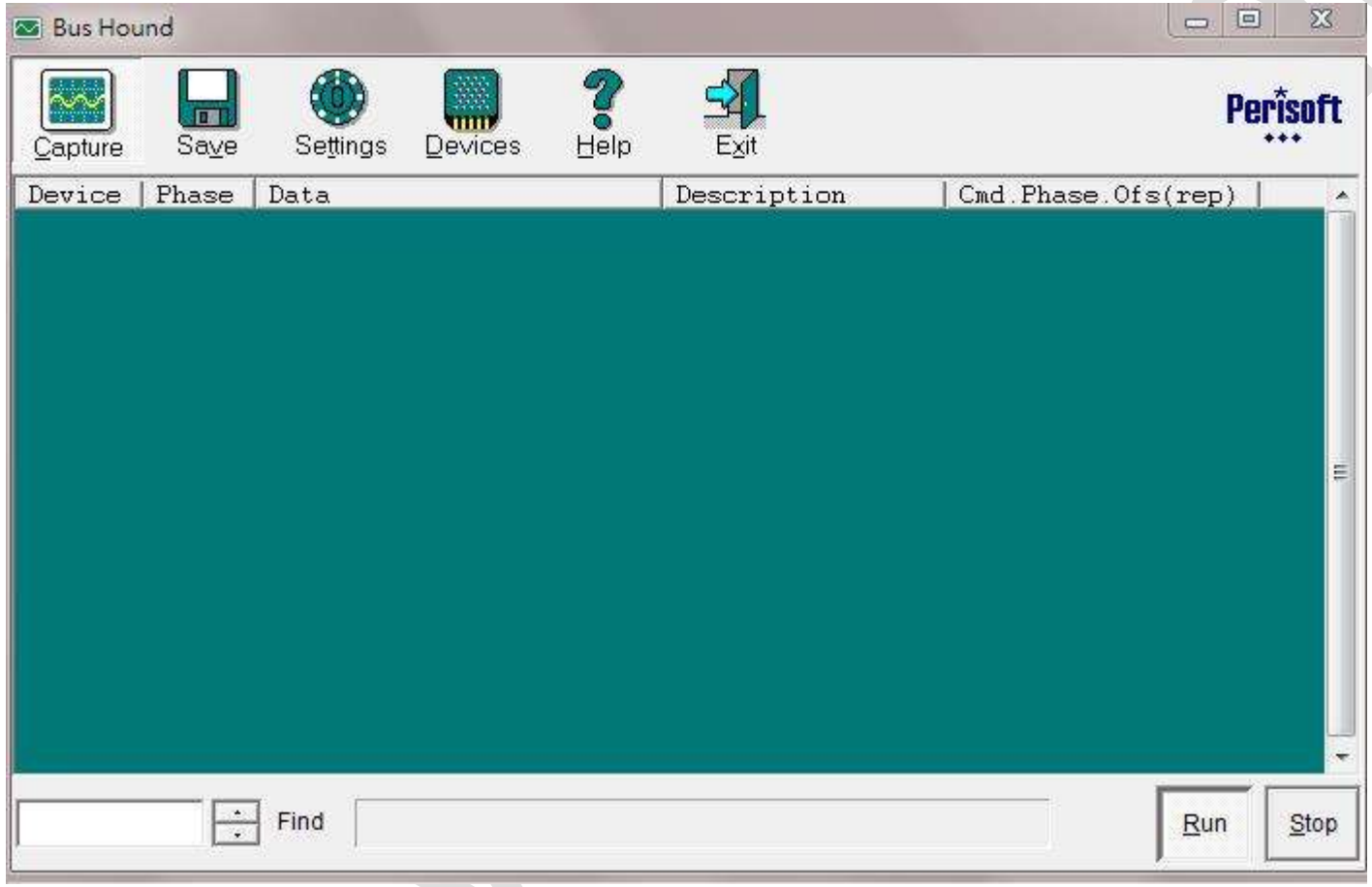
| Byte | Byte 0～13 (長度固定) Via USB |
|---|---|
| Send | C0 0A 00 69 00 05 00 04 02 00 1A 03 00 |

Byte 10=1A 代表功率大小，數值越大功率越大，調整範圍 11~1A(對應 17~26dBm)，

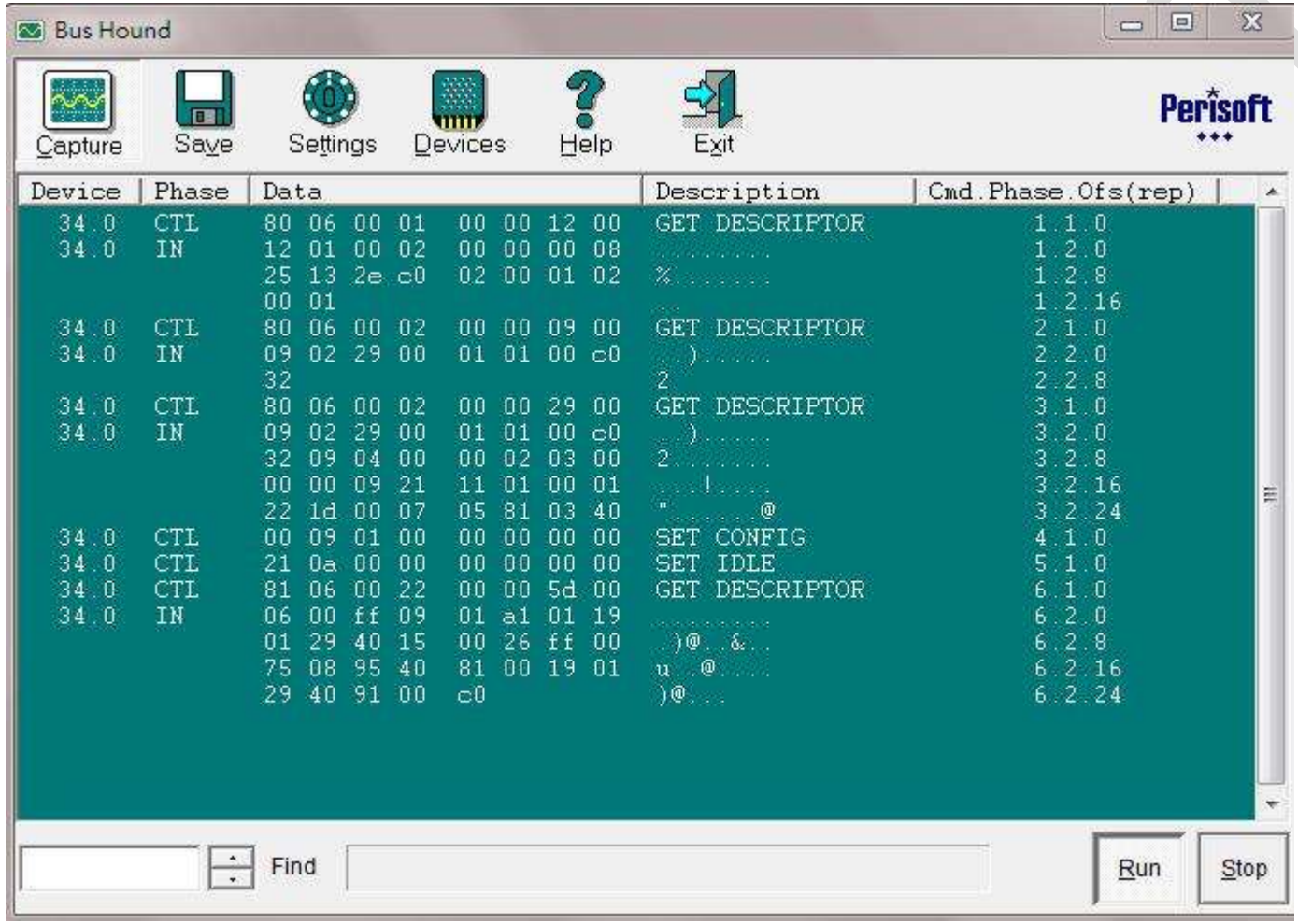
| | | | | |
|---|---|---|---|---|
| 0x11 – 17dBm | 0x12 – 18dBm | 0x13 – 19dBm | 0x14 – 20dBm | 0x15 – 21dBm |
| 0x16 – 22dBm | 0x17 – 23dBm | 0x18 – 24dBm | 0x19 – 25dBm | 0x1A – 26dBm |

# USB 連線測試方式說明

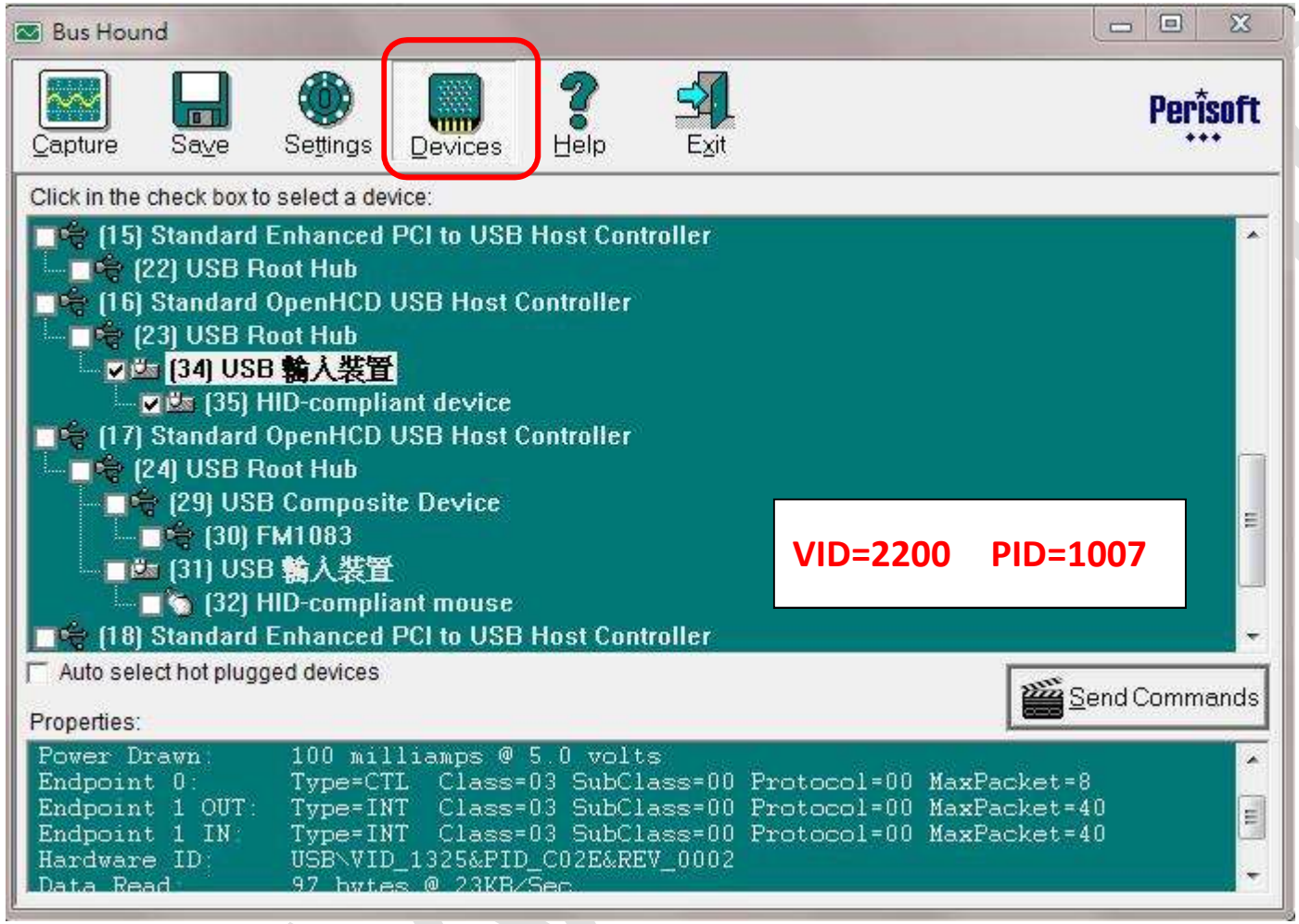
1. 執行 Bus Hound 程式



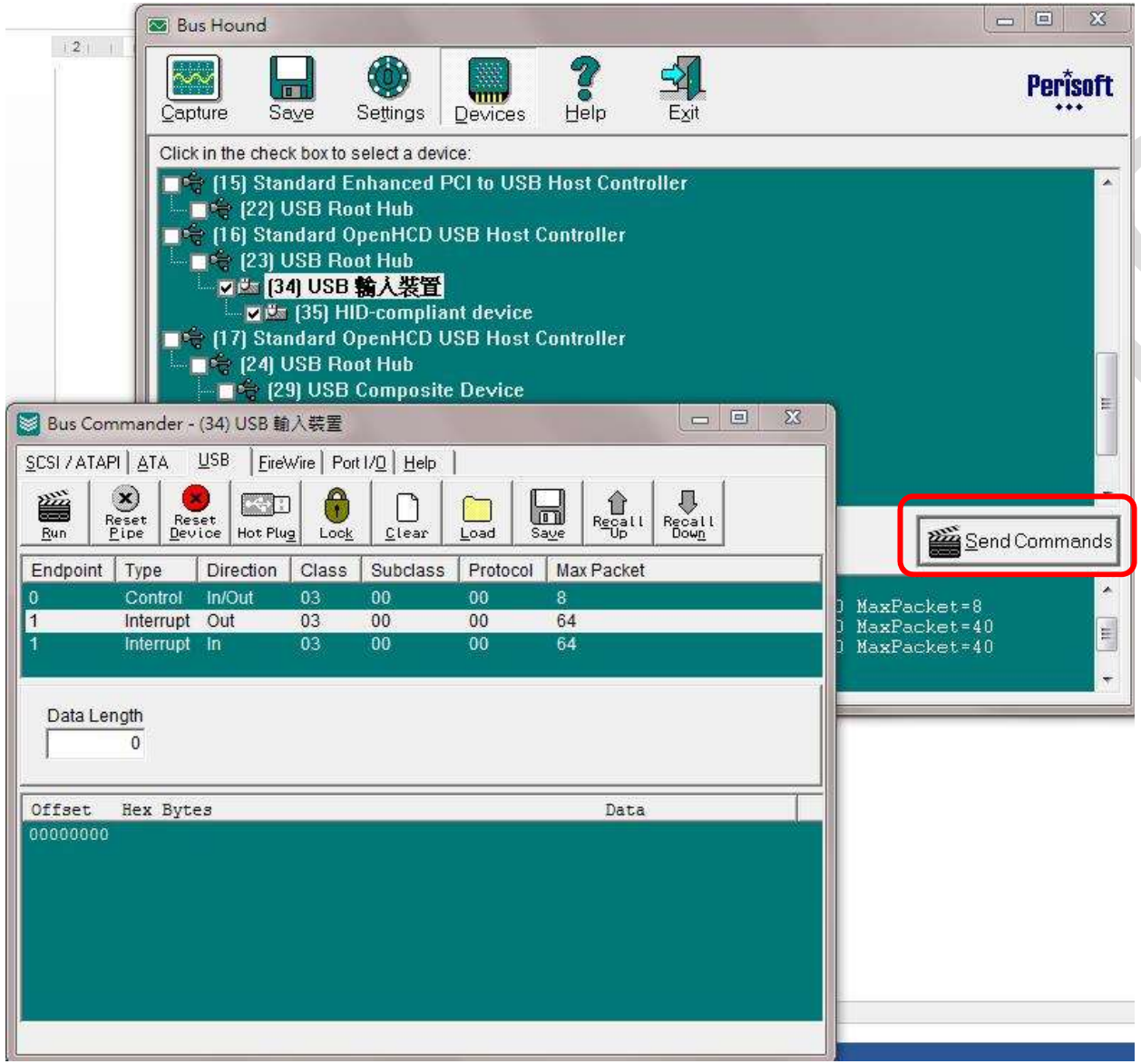
2. RFID module 插入 USB 埠



3. 點選 Bus Hound 軟體上 Devices 選單

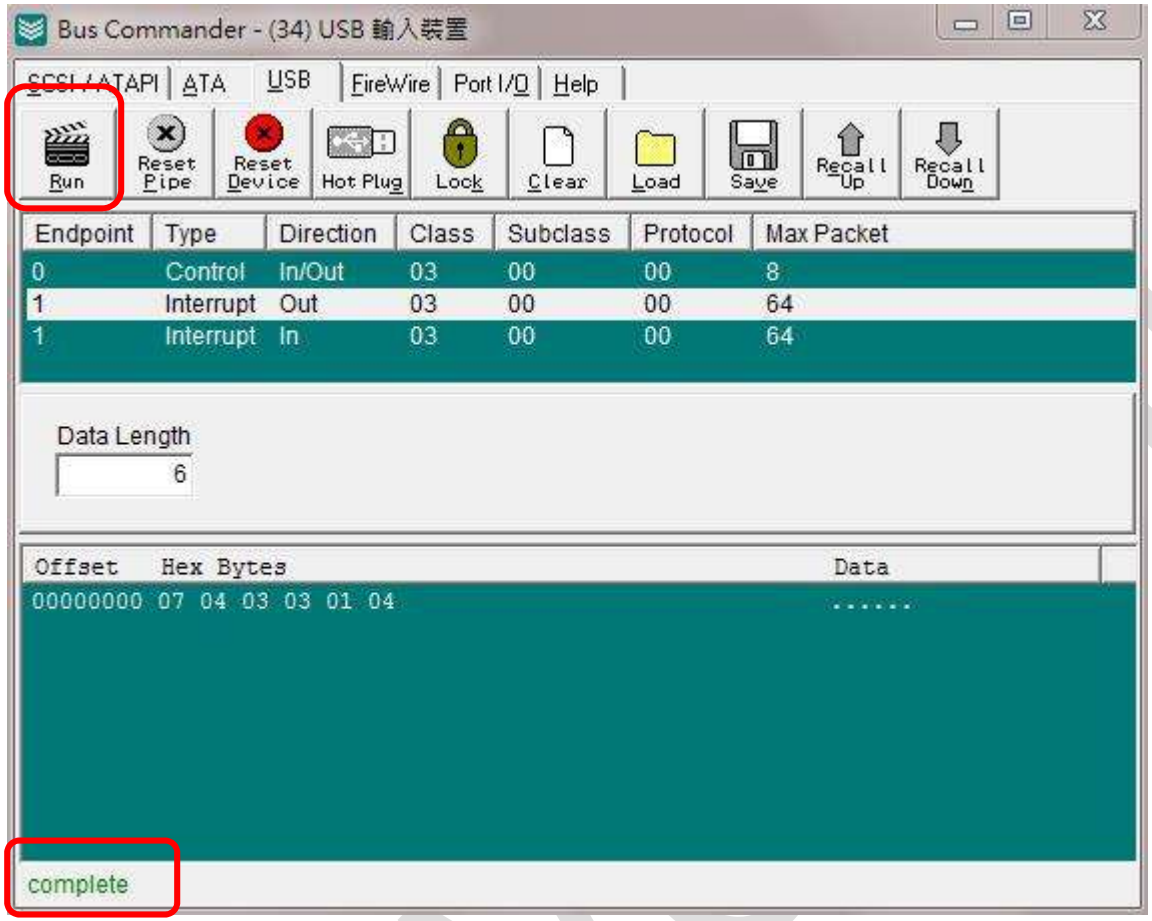


4. 點選 Send commands

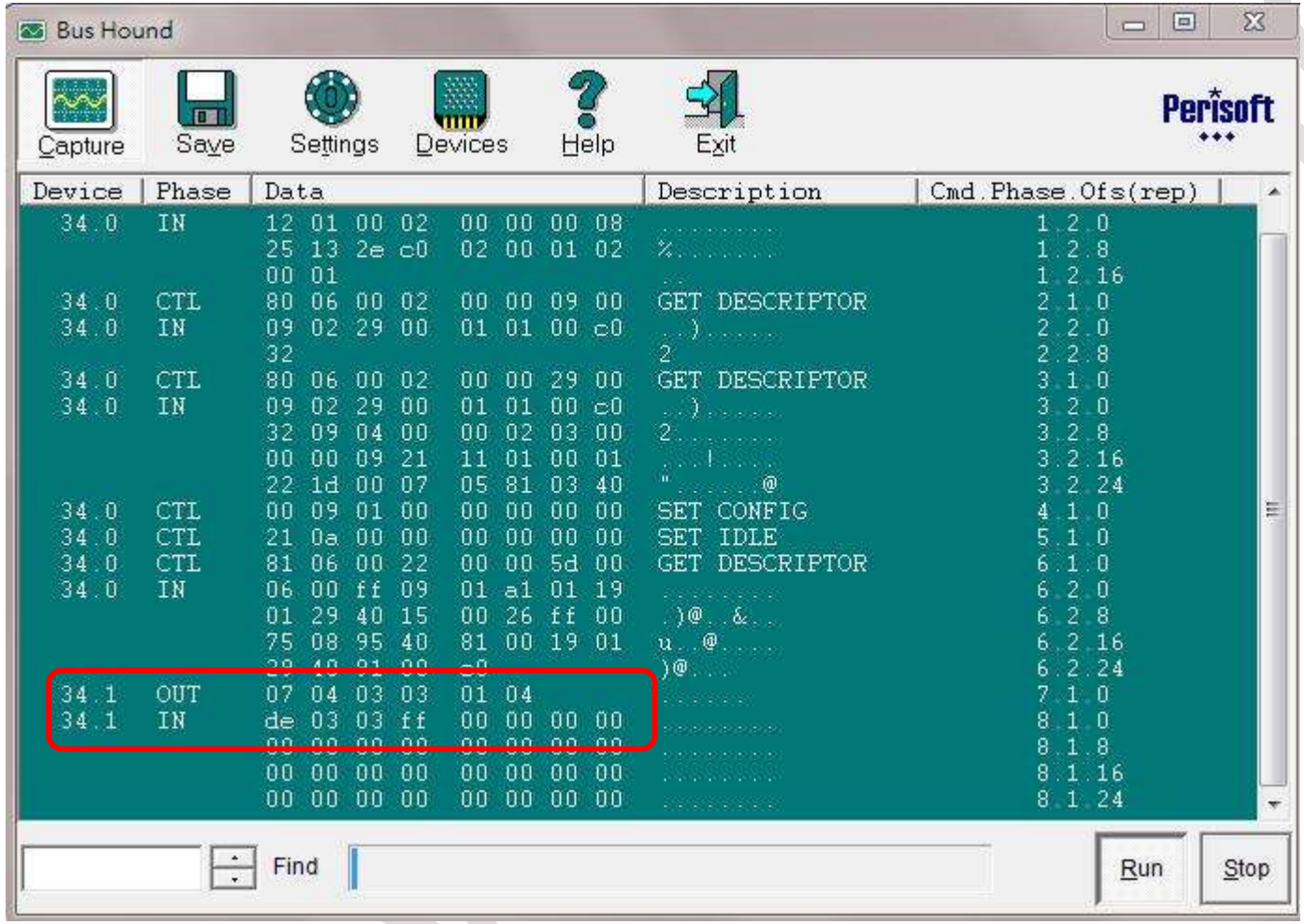


5. 選擇 interrupt out 並在 data length 內填入要輸入的資料長度並將滑鼠點到下列輸入測試指令 07 04 03 03 01 04

6. 點擊 Run 按鍵後在下方提示出現 complete 表示執行完畢



7. 切換回到 Bus Hound 並點選 Capture 觀察發出及接收到的 command



8. OUT 代表 PC 發出給 RFID module 的指令，IN 代表 RFID module 發出給 PC 的回應值