Wenshing RFID module protocol (UART & USB)

UART Baud rate at 9600 N 8 1 , use option "send new line" for each command

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 0～20 (長度固定) Via UART	Byte 0～19 (長度固定) Via USB
Send	07 00 00 11 86 00 02 00 00 00 0D 8C 00 05 00 00 01 01 00 01 06	07 11 00 86 00 02 00 00 00 0D 8C 00 05 00 00 01 01 00 01 06

Byte	Byte 0～15 (長度固定) Via UART	Byte 0～14 (長度固定) Via USB
Return	71 00 00 0C 05 00 00 00 07 01 00 00 00 A8 0D 0E	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 3=0C 表示後面還有多少 byte 資料

Byte 11=00 表示收到多少 TAG

Byte 13～15=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 0～31 (長度非固定) Via UART	Byte 0～30 (長度非固定) Via USB
Return	71 00 00 1C 05 00 00 00 17 01 00 01 8F FC A8 0D 0E 0E 34 00 E2 00 20 19 77 04 02 25 16 91 72 68	71 1C 00 05 00 00 00 17 01 00 01 8F FC 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 3=1C 表示後面還有多少 byte 資料

Byte 7～8=00 17 表示後面還有多少 byte 資料

Byte 11=01 表示收到多少 TAG

Byte 12=8F 表示該 TAG 的 RSSI 值

Byte 13=FC 表示該 TAG 的 AGC 值

Byte 14～16= A80D0E 代表掃描的頻率，前後 byte 對調再轉 10 進制 0E0DA8=921000KHz=921MHz

Byte 17=0E 代表此 TAG 資料共有多少 byte

Byte 18～19=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 20～End = E2 00 20 19 77 04 02 25 16 91 72 68 都是 TAG 的 EPC 碼

範例:收到 3 張 TAG 的時候

Return: 7E 00 00 44 05 00 00 00 3F 01 00 03 0F EE 72 16 0E 0E 30 00 E2 00 20 19 52 04 00 88 15 90 71 F7 0F FD 72 16 0E 0E 30 00 E2 00 20 19 52 04 00 93 15 90 71 E3 07 EE 72 16 0E 0E 30 00 E2 00 20 19 52 04 00 89 15 90 71 F3

解析如下

7E 00 00 44 05 00 00 00 3F 01 00 03 代表此數據包含了 3 張 TAG 資訊

0F EE 72 16 0E 0E 30 00 E2 00 20 19 52 04 00 88 15 90 71 F7 第 1 張 TAG 資訊

0F FD 72 16 0E 0E 30 00 E2 00 20 19 52 04 00 93 15 90 71 E3 第 2 張 TAG 資訊

07 EE 72 16 0E 0E 30 00 E2 00 20 19 52 04 00 89 15 90 71 F3 第 3 張 TAG 資訊

範例:收到 1 張短 EPC 碼的 TAG

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 0～13(長度固定) Via UART	Byte 0～12(長度固定) Via USB
Send	08 00 00 0A 8C 00 05 00 00 01 00 00 00 00	08 0A 00 8C 00 05 00 00 01 00 00 00 00

Byte	Byte 0～15 (長度固定) Via UART	Byte 0～14 (長度固定) Via USB
Return	8A 00 00 0C 05 00 00 00 07 00 00 00 00 96 10 0E	8A 0C 00 05 00 00 00 07 00 00 00 00 96 10 0E

4. Read Bank Area command

Byte	Byte 0～29 (長度非固定) Via UART	Byte 0～28 (長度非固定) Via USB
Send	81 00 00 1A 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	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 4=06 Select Tag

Byte 17～28=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 0～8 (長度固定) Via UART	Byte 0～7 (長度固定) Via USB
Return	11 00 00 05 06 00 00 00 00	11 05 00 06 00 00 00 00

Byte 3=05 表示後面還有多少 byte 資料

Byte 8=00 表示後面還有多少 byte 資料

Byte	Byte 0～17 (長度固定) Via UART	Byte 0～16 (長度固定) Via USB
Send	82 00 00 0E 08 00 09 00 81 00 00 00 00 00 11 11 11 11	82 0E 00 08 00 09 00 81 00 00 00 00 00 11 11 11 11

Byte 3=0E 表示後面還有多少 byte 資料

Byte 4=08 Read command

Byte 5～6=00 09 表示後面還有多少 byte 有效資料（從 Byte 9 開始計算）

Byte 9=00 選擇要讀取的區塊，對照如下

Bank Area 00 = Reserved
01 = EPC
02 = TID
03 = User

Byte 10～13=00 00 00 00 選擇讀取區塊的起始位置

Byte 14～17=11 11 11 11 輸入要讀取 TAG 的 Access Password

Byte	Byte 0～N (長度非固定) Via UART	Byte 0～N (長度非固定) Via USB
Return	27 00 00 0E 08 00 DE 00 09 00 00 00 00 00 00 00 00 03	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 3=0E 表示後面還有多少 byte 資料

Byte 6=DE 表示讀取狀態，對照如下

DF="No response from tag"
DE="Header bit was set in response"
DD="Preamble error in response"
DC="Invalid size of response"
DB="CRC error"
DA="FIFO under/overflow"
BF="Tag is not in the range of the reader"
BE="Access failed, probably wrong password"
BD="ReqRN failed."
BC="Channel timed out, command took too long."

Byte 8=09 表示後面還有多少 byte 資料

Byte 9=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: 8200000E08000900810000000000000000000
Return:20 00 00 06 08 00 BF 00 01 00 "Tag is not in the range of the reader"

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 BE 00 01 00 "Access failed, probably wrong password"

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 0～29 (長度非固定) Via UART	Byte 0～28 (長度非固定) Via USB
Send	81 00 00 1A 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	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 4=06 Select Tag

Byte 17～28=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 0～8 (長度固定) Via UART	Byte 0～7 (長度固定) Via USB
Return	11 00 00 05 06 00 00 00 00	11 05 00 06 00 00 00 00

Byte 3=05 表示後面還有多少 byte 資料

Byte 8=00 表示後面還有多少 byte 資料

Byte	Byte 0～17 (長度非固定) Via UART	Byte 0～16 (長度非固定) Via USB
Send	82 00 00 12 07 00 0D 00 02 03 00 00 00 00 00 00 00 00 11 11 11 11	82 12 00 07 00 0D 00 02 03 00 00 00 00 00 00 00 00 11 11 11 11

Byte 3=12 表示後面還有多少 byte 資料

Byte 4=07 Write command

Byte 5～6=00 0D 表示後面還有多少 byte 有效資料 (從 Byte 9 開始計算)

Byte 9=03 選擇要讀取的區塊，對照如下

Bank Area 00 = Reserved
01 = EPC
02 = TID
03 = User

Byte 10～13=00 00 00 00 選擇讀取區塊的起始位置

Byte 14～17=00 00 00 00 輸入要讀取 TAG 的 Access Password

Byte 18～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)

Byte	Byte 0～10 (長度固定) Via UART	Byte 0～9 (長度固定) Via USB
Return	2A 00 00 07 07 00 00 00 02 02 A5	2A 07 00 07 00 00 00 02 02 A5

讀取成功的時候

Byte 3=07 表示後面還有多少 byte 資料

Byte 6=00 表示寫入狀態，對照如下

00=" Success"

DF="No response from tag"

DE="Header bit was set in response"

DD="Preamble error in response"

DC="Invalid size of response"

DB="CRC error"

DA="FIFO under/overflow"

BF="Tag is not in the range of the reader"

BE="Access failed, probably wrong password"

BD="ReqRN failed."

BC="Channel timed out, command took too long."

Byte 8=02 表示後面還有多少 byte 資料

Byte 9=02 表示寫入成功的字元數（1 個字元=2 個 Byte）

6. Unlock Lock&Premalock command

Byte	Byte 0～29 (長度非固定) Via UART	Byte 0～28 (長度非固定) Via USB
Send	81 00 00 1A 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	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 4=06 Select Tag

Byte 17～28=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 0～8 (長度固定) Via UART	Byte 0～7 (長度固定) Via USB
Return	11 00 00 05 06 00 00 00 00	11 05 00 06 00 00 00 00

Byte 3=05 表示後面還有多少 byte 資料

Byte 8=00 表示後面還有多少 byte 資料

Byte	Byte 0～15 (長度固定) Via UART	Byte 0～14 (長度固定) Via USB

Send	82 00 00 0C 09 00 07 00 01 C0 00 00 00 00 00 00	82 0C 00 09 00 07 00 01 C0 00 00 00 00 00 00

Byte 3=0C 表示後面還有多少 byte 資料

Byte 4=09 Unlock Lock&Premalock command

Byte 5～6=00 07 表示後面還有多少 byte 有效資料 (從 Byte 9 開始計算)

Byte 9～10=C0 00 選擇要操作的區塊，對照如下

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 11=00 選擇操作指令

Command 00 = Unlock

10 = Premalock

20 = Lock

30 = Lock&Premalock

Byte 12～15=00 00 00 00 輸入 TAG 的 Access Password

Byte	Byte 0～9 (長度固定) Via UART	Byte 0～8 (長度固定) Via USB
Return	22 00 00 06 09 00 DE 00 01 6C	22 06 00 09 00 DE 00 01 6C

讀取成功的時候

Byte 3=06 表示後面還有多少 byte 資料

Byte 6=DE 表示寫入狀態，對照如下

00=" Success"

DF="No response from tag"

DE="Header bit was set in response"

DD="Preamble error in response"

DC="Invalid size of response"

DB="CRC error"

DA="FIFO under/overflow"

BF="Tag is not in the range of the reader"

BE="Access failed, probably wrong password"

BD="ReqRN failed."

BC="Channel timed out, command took too long."

Byte 8=01 表示後面還有多少 byte 資料

7. Kill Tag command

Byte	Byte 0～29 (長度非固定) Via UART	Byte 0～28 (長度非固定) Via USB
Send	81 00 00 1A 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	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 4=06 Select Tag

Byte 17～28=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 0～8 (長度固定) Via UART	Byte 0～7 (長度固定) Via USB
Return	11 00 00 05 06 00 00 00 00	11 05 00 06 00 00 00 00

Byte 3=05 表示後面還有多少 byte 資料

Byte 8=00 表示後面還有多少 byte 資料

Byte	Byte 0～14 (長度固定) Via UART	Byte 0～13 (長度固定) Via USB
Send	82 00 00 0B 0A 00 06 00 01 00 00 00 00 00 00	82 0B 00 0A 00 06 00 01 00 00 00 00 00 00

Byte 3=0B 表示後面還有多少 byte 資料

Byte 4=0A Kill command

Byte 5～6=00 06 表示後面還有多少 byte 有效資料（從 Byte 9 開始計算）

Byte 9～12=00 00 00 00 輸入 TAG 的 Kill password

Byte	Byte 0～9 (長度固定) Via UART	Byte 0～8(長度固定) Via USB
Return	22 00 00 06 0A 00 00 00 01 A5	22 06 00 0A 00 00 00 01 A5

讀取成功的時候

Byte 3=06 表示後面還有多少 byte 資料

Byte 6=00 表示寫入狀態，對照如下

00=" Success"

DF="No response from tag"

DE="Header bit was set in response"

DD="Preamble error in response"

DC="Invalid size of response"

DB="CRC error"

DA="FIFO under/overflow"

BF="Tag is not in the range of the reader"

BE="Access failed, probably wrong password"

BD="ReqRN failed."

BC="Channel timed out, command took too long."

Byte 8=01 表示後面還有多少 byte 資料

8. Set command

範例:link frequency = 320kHz, Session=S1,Coding=FM0,Q_begin=4,Tari=12.5us,Pilot Tone = On

Byte	Byte 0～24 (長度固定) Via UART	Byte 0～23 (長度固定) Via USB
Send	18 00 00 15 03 00 10 00 10 01 0C 01 00 01 01 01 01 01 01 04 00 84 01 00	18 15 00 03 00 10 00 10 01 0C 01 00 01 01 01 01 01 01 01 04 00 84 01 00

Byte 10=0C 表示 Link frequency，對照如下

00= 40KHz

06= 160KHz

08= 213KHz

09= 256KHz

0C= 320KHz

0F= 640KHz

Byte 12=00 表示 Coding，對照如下

00= FM0

01= Miller 2

02= Miller 4

03= Miller 8

Byte 14=01 表示 Session，對照如下

00= S0

01= S1

02= S2

03= S3

Byte 16=01 表示 Pilot Tone，對照如下

00= Pilot Tone Disable

01= Pilot Tone Enable

Byte 18=01 表示 Tari，對照如下

00= 6.25us

01= 12.5us

02= 25us

Byte 20=04 表示 Q_begin，對照如下

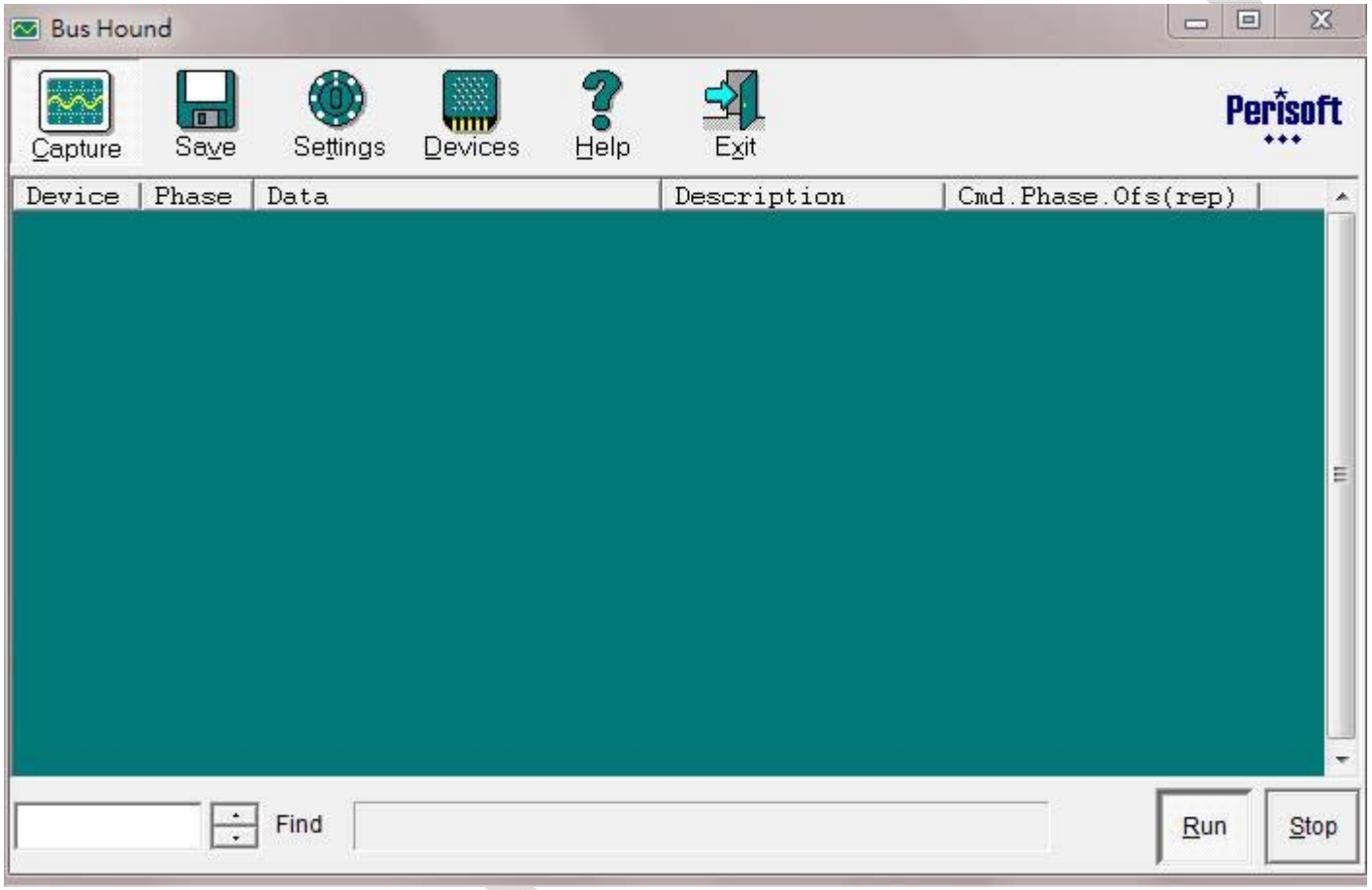
00～0F= 0～15

Byte	Byte 0～24 (長度固定) Via UART	Byte 0～23(長度固定) Via USB

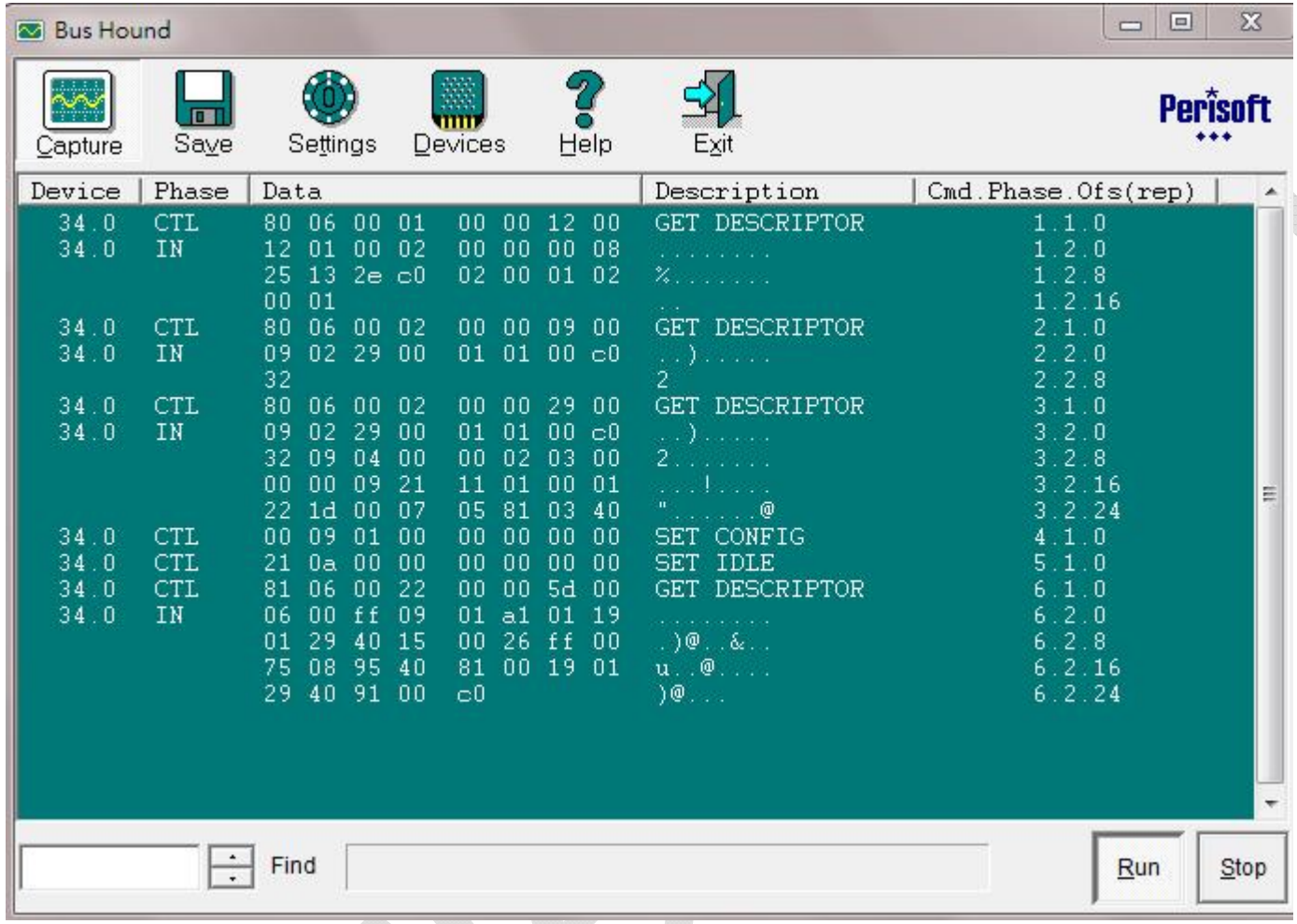
Return	AA 00 00 15 03 00 00 00 10 00 0C 00 00 00 01 00 01 00 01 00 04 00 00 00 00	AA 15 00 03 00 00 00 10 00 0C 00 00 00 01 00 01 00 01 00 04 00 00 00 00

USB 連線測試方式說明

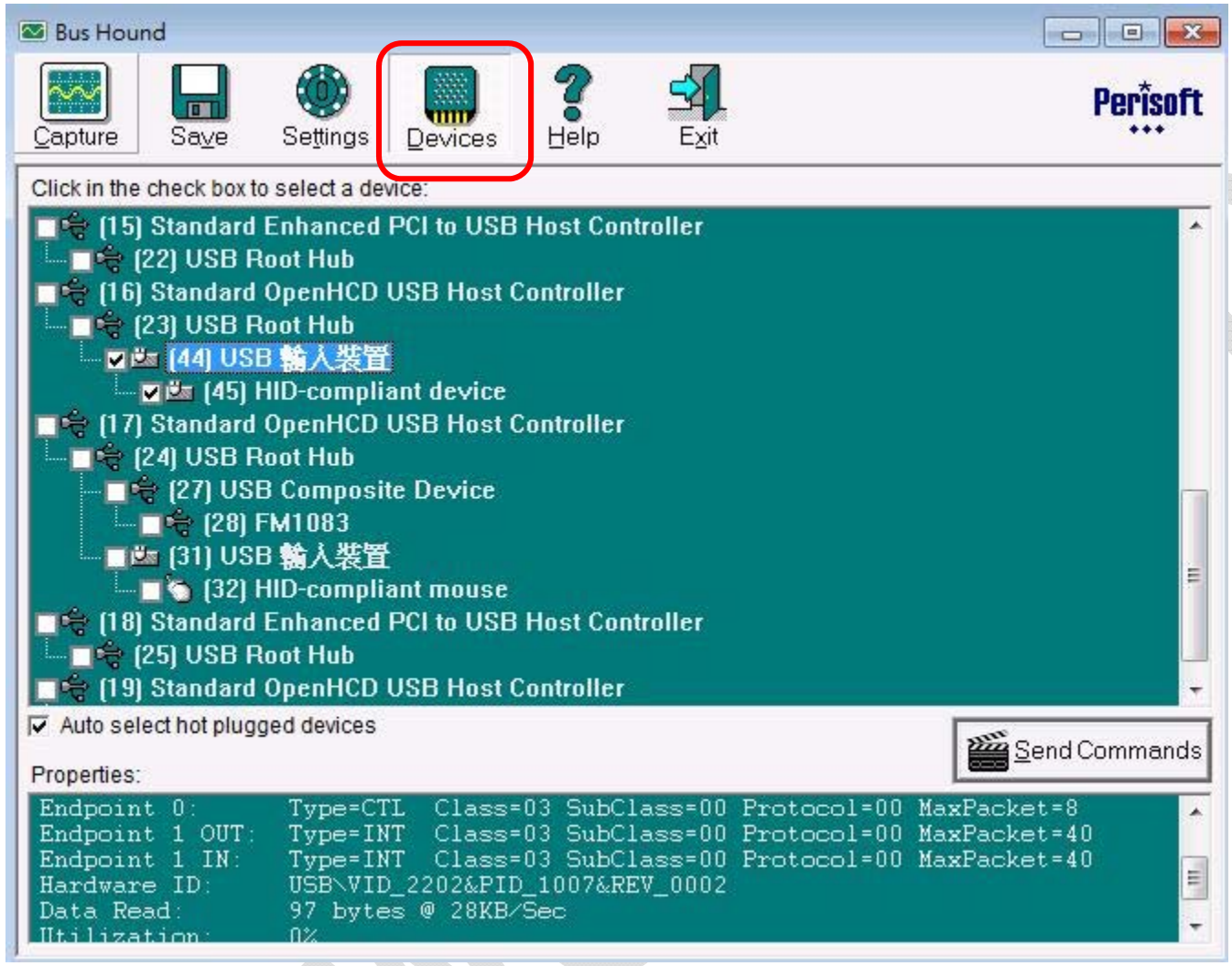
1. 執行 Bus Hound 程式



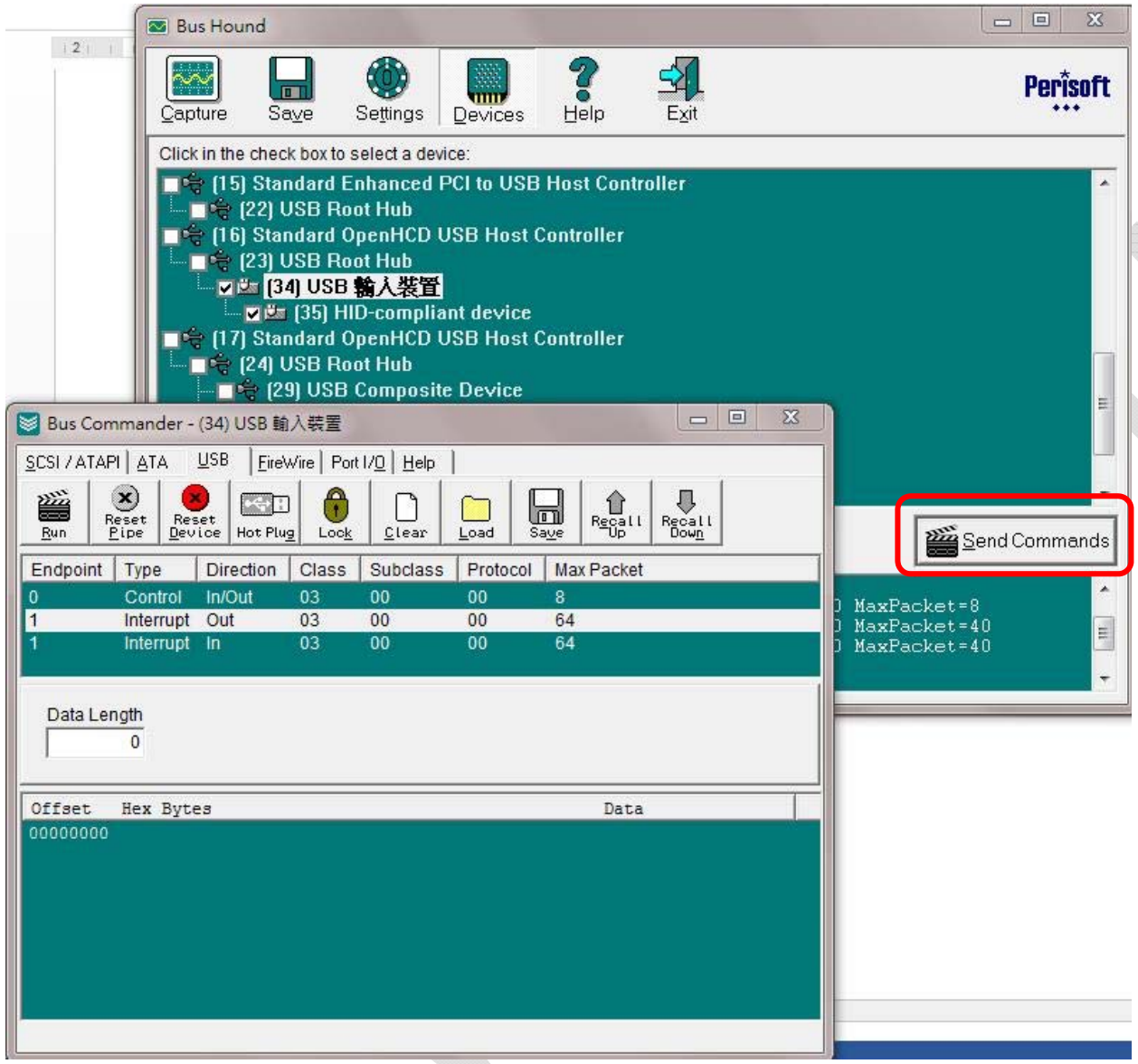
2. RFID module 插入 USB 端口



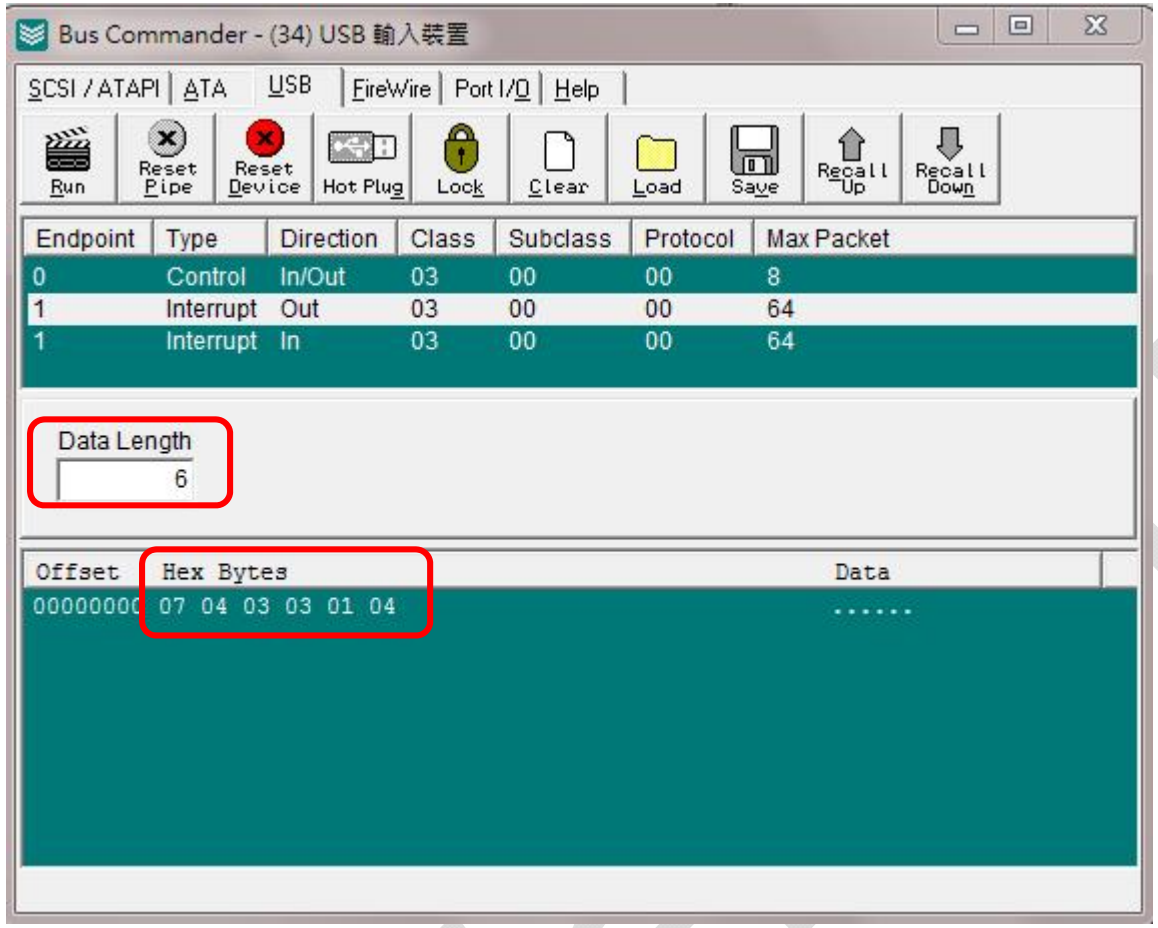
3. 點選 Bus Hound 軟體上 Devices 選單



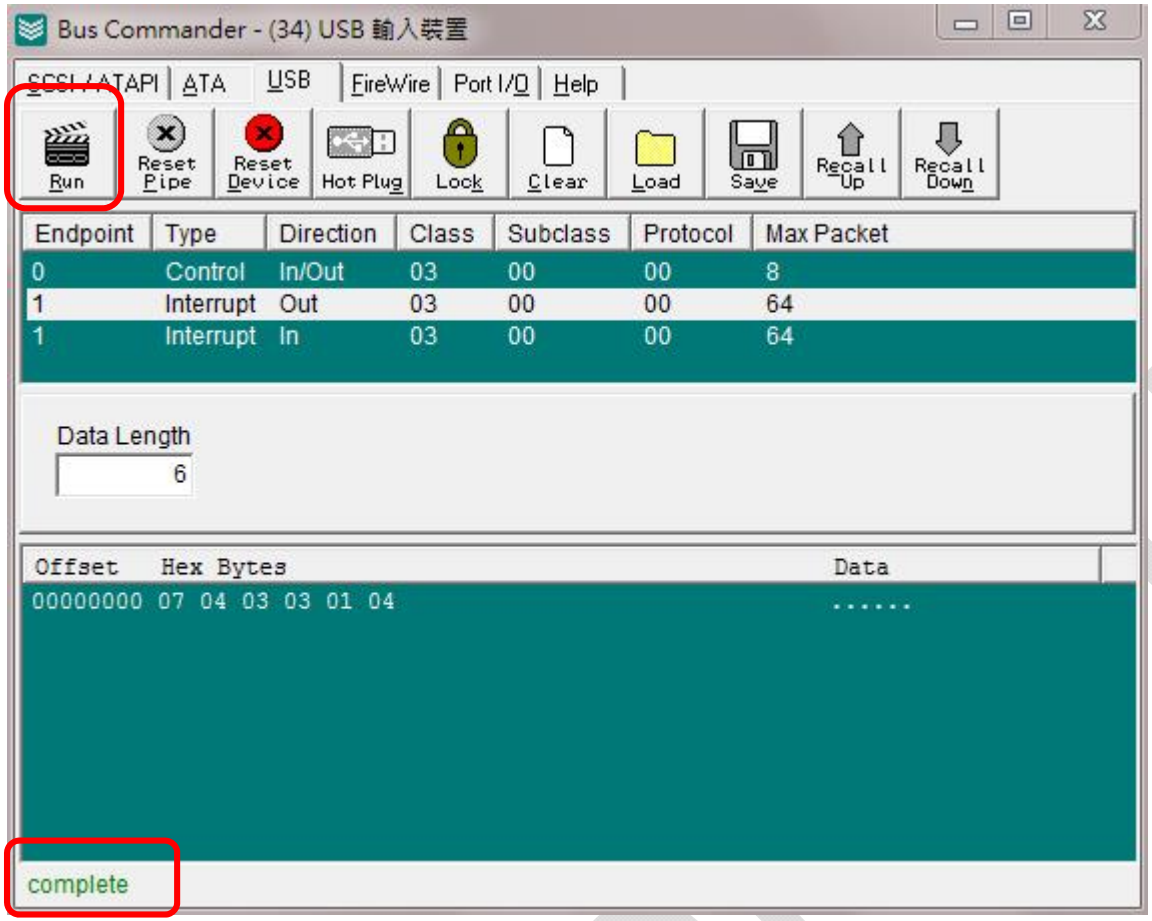
4. 點選 Send commands



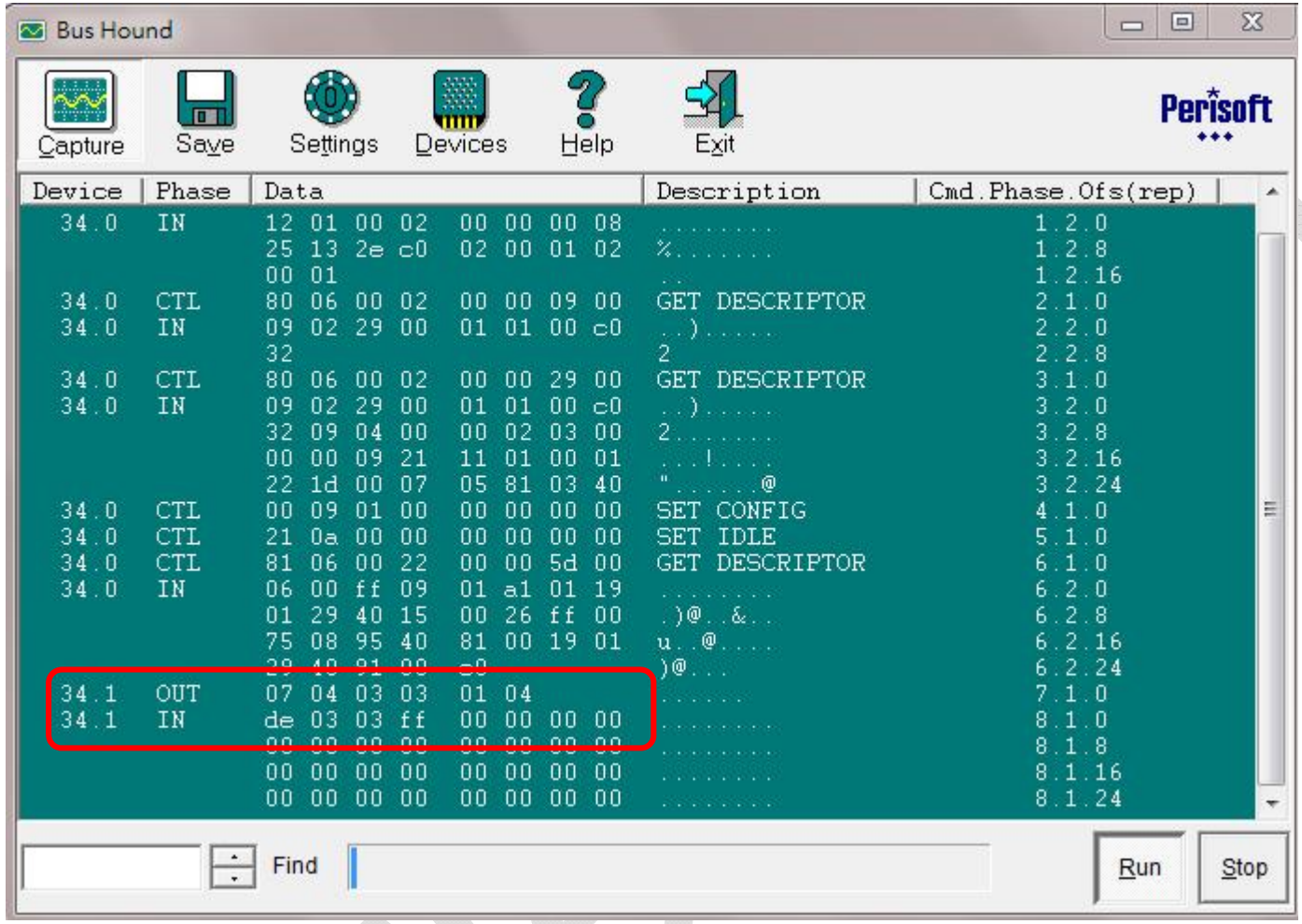
5. 選擇 interrupt out 並在 data length 內填入要輸入的資料長度並將滑鼠點到下列輸入測試指令 07 04 03 03 01 04



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