如何使用 wireshark 觀察 MODBUS TCP 通訊封包

元米科技 2017/4/14

本文目的

本文的對象是針對應用 MODBUS TCP 通訊，但不熟悉 MODBUS TCP 協定與 Wireshark 操作的工程人員。說明如何利用免費的網路封包軟體 Wireshark，判讀 MODBUS TCP 的封包，進而幫助專案異常排除。

文中將依序說明 如何安裝 Wireshark，並以 ICDT MODBUS TCP Client 免費軟體連接 ICDT 網站 MODBUS TCP Server 為例，展示 Wireshark 的分析結果。

由於 Wireshark 只能分析電腦網卡收到的訊息，因此 Wireshark 軟體必須與 ICDT MODBUS TCP Client 安裝在同一台電腦。

關於 wireshark

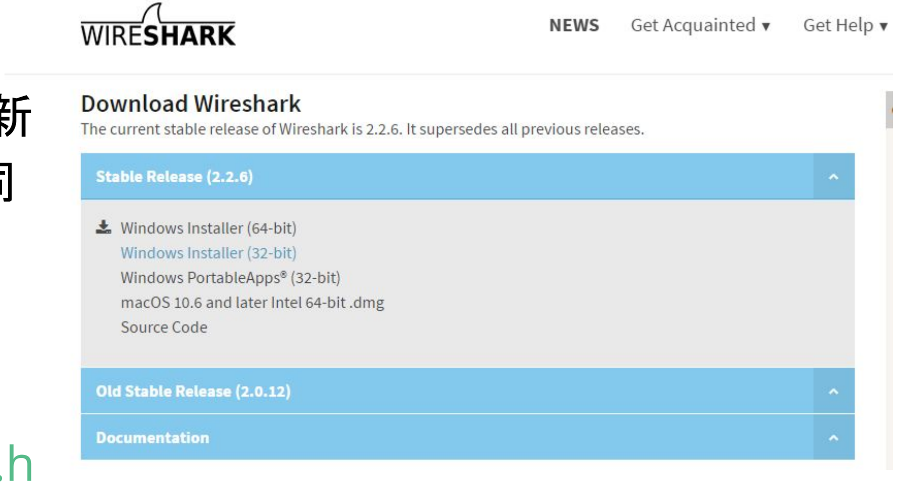
維基百科：Wireshark（前稱Ethereal）是一個免費開源的網路封包分析軟體。網路封包分析軟體的功能是截取網路封包，並盡可能顯示出最為詳細的網路封包資料。
在過去，網路封包分析軟體是非常昂貴，或是專門屬於營利用的軟體，Wireshark的出現改變了這一切。在GNU通用公眾授權條款的保障範圍底下，使用者可以以免費的代價取得軟體與其程式碼，並擁有針對其原始碼修改及客製化的權利。Wireshark是目前全世界最廣泛的網路封包分析軟體之一。

安裝 Wireshark

至 Wireshark 官網依照電腦版本下載最新版的 Wireshark 後進行安裝，安裝時連同相關的程式一起安裝。

Wireshark 下載處:

https://www.wireshark.org/download.html



Download Wireshark

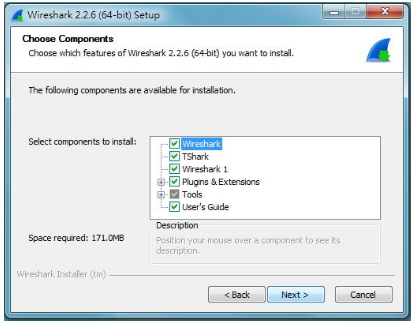
The current stable release of Wireshark is 2.2.6. It supersedes all previous releases.

Stable Release (2.2.6)

- Windows Installer (64-bit)
- Windows Installer (32-bit)
- Windows PortableApps® (32-bit)
- macOS 10.6 and later Intel 64-bit .dmg
- Source Code

Old Stable Release (2.0.12)

Documentation


Wireshark 2.2.6 (64-bit) Setup

Choose Components

Choose which features of Wireshark 2.2.6 (64-bit) you want to install.

The following components are available for installation.

Select components to install:

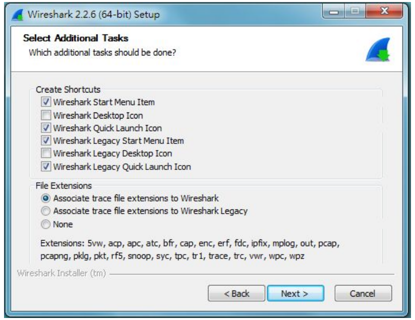
- ☑ Wireshark
- ☑ TShark
- ☑ Wireshark 1
- ☑ Plugins & Extensions
- ☑ Tools
- ☑ User's Guide

Space required: 171.0MB

Description

Position your mouse over a component to see its description.

Wireshark Installer (tm)


Wireshark 2.2.6 (64-bit) Setup

Select Additional Tasks

Which additional tasks should be done?

Create Shortcuts

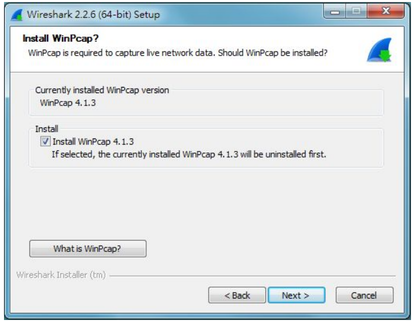
- ☑ Wireshark Start Menu Item
- □ Wireshark Desktop Icon
- ☑ Wireshark Quick Launch Icon
- ☑ Wireshark Legacy Start Menu Item
- □ Wireshark Legacy Desktop Icon
- ☑ Wireshark Legacy Quick Launch Icon

File Extensions

- ● Associate trace file extensions to Wireshark
- ○ Associate trace file extensions to Wireshark Legacy
- ○ None

Extensions: 5vw, acp, apc, atc, bfr, cap, enc, erf, fdc, ipfix, mplog, out, pcap, pcapng, pklg, pkt, rf5, snoop, syc, tpc, tr1, trace, trc, vwr, wpc, wpz

Wireshark Installer (tm)


Wireshark 2.2.6 (64-bit) Setup

Install WinPcap?

WinPcap is required to capture live network data. Should WinPcap be installed?

Currently installed WinPcap version

WinPcap 4.1.3

Install

☑ Install WinPcap 4.1.3

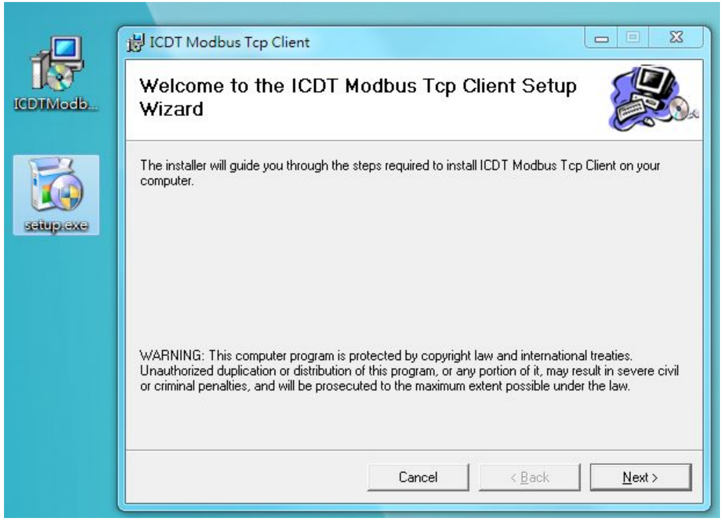
If selected, the currently installed WinPcap 4.1.3 will be uninstalled first.

Wireshark Installer (tm)

安裝 ICDT MODBUS TCP Client 免費軟體

自 元米科技 MODBUS 免費工具軟體 區下載 最新版 ICDT MODBUS TCP Client 免費軟體

安裝在與 Wireshark 相同的電腦中，如果已安裝較舊的版本，必須先移除後安裝。



Welcome to the ICDT Modbus Tcp Client Setup Wizard

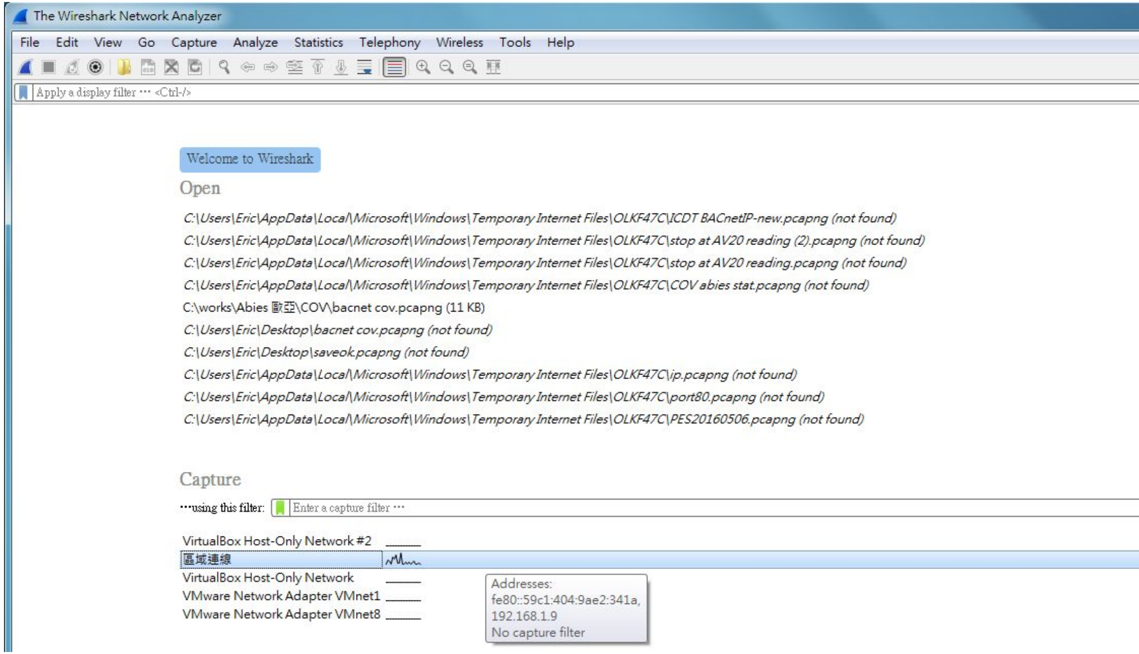
The installer will guide you through the steps required to install ICDT Modbus Tcp Client on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

執行 Wireshark

執行 wireshark 後在正確的網路卡上點兩下，以進行記錄。

由於電腦本身可能有乙太網路、無線網路或者多個虛擬網路，請選擇已連接到網際網路的網路介面，範例中為"區域網路"也就是乙太網路。如圖看到 區域網路 右邊資料量的曲線，表示該網路是目前主要運作的網路。


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark
Open
Capture
…using this filter:
Enter a capture filter …

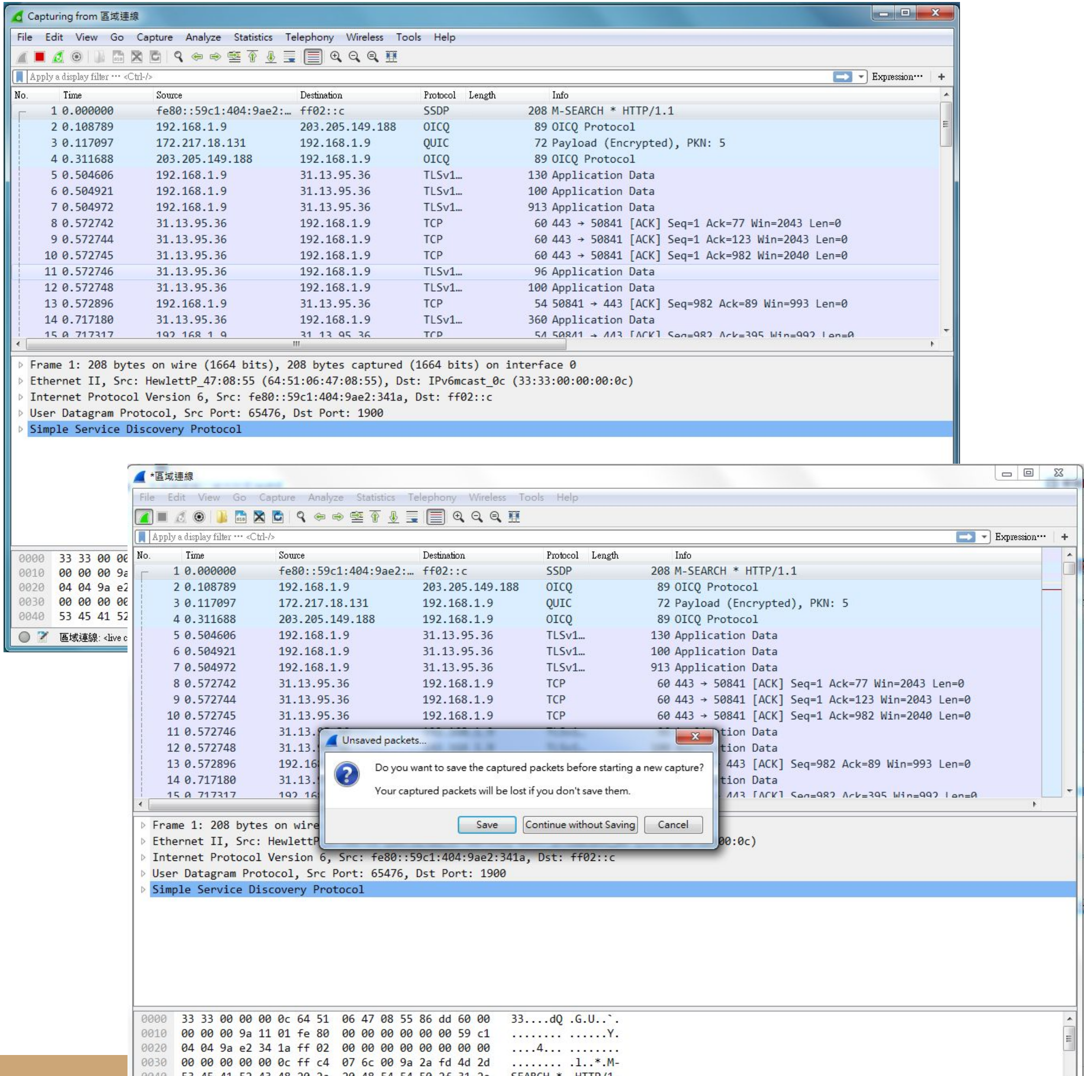
```
C:\Users\Eric\AppData\Local\Microsoft\Windows\Temporary Internet Files\OLKF47C\ICDT BACnetIP-new.pcapng (not found)
C:\Users\Eric\AppData\Local\Microsoft\Windows\Temporary Internet Files\OLKF47C\stop at AV20 reading (2).pcapng (not found)
C:\Users\Eric\AppData\Local\Microsoft\Windows\Temporary Internet Files\OLKF47C\stop at AV20 reading.pcapng (not found)
C:\Users\Eric\AppData\Local\Microsoft\Windows\Temporary Internet Files\OLKF47C\COV abies stat.pcapng (not found)
C:\works\Abies 歐亞\COV\bacnet cov.pcapng (11 KB)
C:\Users\Eric\Desktop\bacnet cov.pcapng (not found)
C:\Users\Eric\Desktop\saveok.pcapng (not found)
C:\Users\Eric\AppData\Local\Microsoft\Windows\Temporary Internet Files\OLKF47C\ip.pcapng (not found)
C:\Users\Eric\AppData\Local\Microsoft\Windows\Temporary Internet Files\OLKF47C\port80.pcapng (not found)
C:\Users\Eric\AppData\Local\Microsoft\Windows\Temporary Internet Files\OLKF47C\PES20160506.pcapng (not found)
```

```
VirtualBox Host-Only Network #2
區域連線
VirtualBox Host-Only Network
VMware Network Adapter VMnet1
VMware Network Adapter VMnet8
```

```
Addresses:
fe80::59c1:404:9ae2:341a,
192.168.1.9
No capture filter
```

Wireshark 記錄中

如果電腦對外有網路通訊，wireshark 就開始記錄通訊封包。按下左上的紅色停止鍵會停止記錄，再按下旁邊的綠色鯊魚鰭會詢問儲存或放棄記錄，如果不儲存，則先前的記錄將會被放棄。


Capturing from 區域連線
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
區域連線: <live c
*區域連線

```
No.  Time      Source                Destination      Protocol Length Info
  1 0.000000  fe80::59c1:404:9ae2:… ff02::c          SSDP     208 M-SEARCH * HTTP/1.1
  2 0.108789  192.168.1.9           203.205.149.188  OICQ      89 OICQ Protocol
  3 0.117097  172.217.18.131        192.168.1.9      QUIC      72 Payload (Encrypted), PKN: 5
  4 0.311688  203.205.149.188       192.168.1.9      OICQ      89 OICQ Protocol
  5 0.504606  192.168.1.9           31.13.95.36      TLSv1…   130 Application Data
  6 0.504921  192.168.1.9           31.13.95.36      TLSv1…   100 Application Data
  7 0.504972  192.168.1.9           31.13.95.36      TLSv1…   913 Application Data
  8 0.572742  31.13.95.36           192.168.1.9      TCP       60 443 → 50841 [ACK] Seq=1 Ack=77 Win=2043 Len=0
  9 0.572744  31.13.95.36           192.168.1.9      TCP       60 443 → 50841 [ACK] Seq=1 Ack=123 Win=2043 Len=0
 10 0.572745  31.13.95.36           192.168.1.9      TCP       60 443 → 50841 [ACK] Seq=1 Ack=982 Win=2040 Len=0
 11 0.572746  31.13.95.36           192.168.1.9      TLSv1…    96 Application Data
 12 0.572748  31.13.95.36           192.168.1.9      TLSv1…   100 Application Data
 13 0.572896  192.168.1.9           31.13.95.36      TCP       54 50841 → 443 [ACK] Seq=982 Ack=89 Win=993 Len=0
 14 0.717180  31.13.95.36           192.168.1.9      TLSv1…   360 Application Data
 15 0.717317  192.168.1.9           31.13.95.36      TCP       54 50841 → 443 [ACK] Seq=982 Ack=395 Win=992 Len=0
```

```
▷ Frame 1: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface 0
▷ Ethernet II, Src: HewlettP_47:08:55 (64:51:06:47:08:55), Dst: IPv6mcast_0c (33:33:00:00:00:0c)
▷ Internet Protocol Version 6, Src: fe80::59c1:404:9ae2:341a, Dst: ff02::c
▷ User Datagram Protocol, Src Port: 65476, Dst Port: 1900
▷ Simple Service Discovery Protocol
```

Unsaved packets...

Do you want to save the captured packets before starting a new capture?

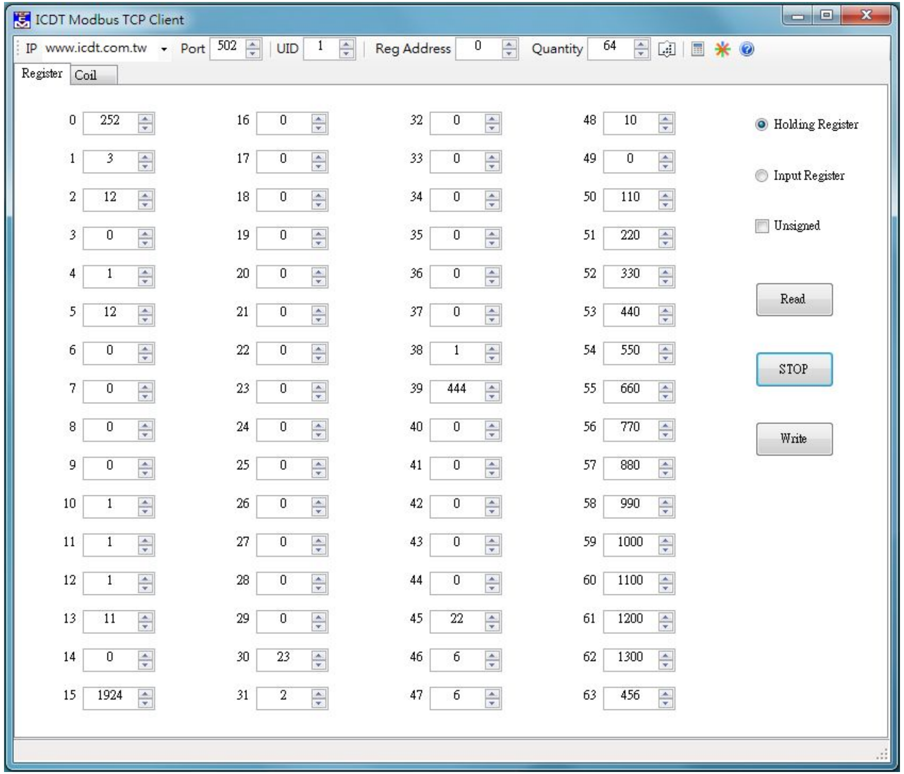
Your captured packets will be lost if you don't save them.

Save | Continue without Saving | Cancel

```
0000  33 33 00 00 00 0c 64 51  06 47 08 55 86 dd 60 00   33....dQ .G.U..`.
0010  00 00 00 9a 11 01 fe 80  00 00 00 00 00 00 59 c1   ........ ......Y.
0020  04 04 9a e2 34 1a ff 02  00 00 00 00 00 00 00 00   ....4... ........
0030  00 00 00 00 00 0c ff c4  07 6c 00 9a 2a fd 4d 2d   ........ .l..*.M-
```

執行 ICDT MODBUS TCP Client 讀取數值

執行 ICDT MODBUS TCP Client 程式並按下 RUN，此時會不斷自 www.icdt.com.tw 位置 502 Port 讀取 UID 為 1 的 64 個 Register，並且可以看到目前數值。



ICDT Modbus TCP Client

IP www.icdt.com.tw Port 502 UID 1 Reg Address 0 Quantity 64

Register Coil

0	252	16	0	32	0	48	10
1	3	17	0	33	0	49	0
2	12	18	0	34	0	50	110
3	0	19	0	35	0	51	220
4	1	20	0	36	0	52	330
5	12	21	0	37	0	53	440
6	0	22	0	38	1	54	550
7	0	23	0	39	444	55	660
8	0	24	0	40	0	56	770
9	0	25	0	41	0	57	880
10	1	26	0	42	0	58	990
11	1	27	0	43	0	59	1000
12	1	28	0	44	0	60	1100
13	11	29	0	45	22	61	1200
14	0	30	23	46	6	62	1300
15	1924	31	2	47	6	63	456

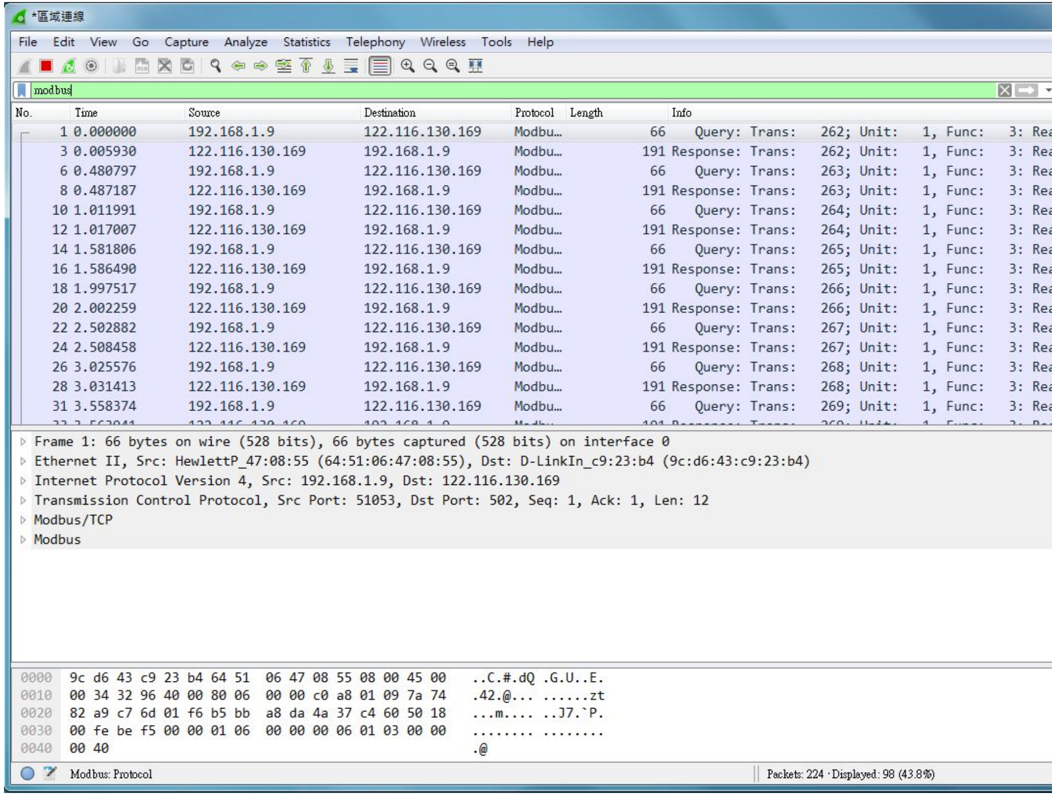
● Holding Register

○ Input Register

□ Unsigned

Wireshark 記錄 MODBUS TCP 封包

在 MODBUS TCP 讀取的同時按下左上綠色鯊魚鰭進行記錄，將看到 MODBUS 封包與其他封包混雜，此時在左上記錄與停止鍵下欄位輸入 modbus (必須為小寫)則可以濾除其他的封包，只保留 modbus 封包。



modbus

```
No.  Time       Source           Destination      Protocol  Length  Info
   1 0.000000   192.168.1.9      122.116.130.169  Modbu…        66     Query: Trans:   262; Unit:   1, Func:   3: Rea
   3 0.005930   122.116.130.169  192.168.1.9      Modbu…       191 Response: Trans:   262; Unit:   1, Func:   3: Rea
   6 0.480797   192.168.1.9      122.116.130.169  Modbu…        66     Query: Trans:   263; Unit:   1, Func:   3: Rea
   8 0.487187   122.116.130.169  192.168.1.9      Modbu…       191 Response: Trans:   263; Unit:   1, Func:   3: Rea
  10 1.011991   192.168.1.9      122.116.130.169  Modbu…        66     Query: Trans:   264; Unit:   1, Func:   3: Rea
  12 1.017007   122.116.130.169  192.168.1.9      Modbu…       191 Response: Trans:   264; Unit:   1, Func:   3: Rea
  14 1.581806   192.168.1.9      122.116.130.169  Modbu…        66     Query: Trans:   265; Unit:   1, Func:   3: Rea
  16 1.586490   122.116.130.169  192.168.1.9      Modbu…       191 Response: Trans:   265; Unit:   1, Func:   3: Rea
  18 1.997517   192.168.1.9      122.116.130.169  Modbu…        66     Query: Trans:   266; Unit:   1, Func:   3: Rea
  20 2.002259   122.116.130.169  192.168.1.9      Modbu…       191 Response: Trans:   266; Unit:   1, Func:   3: Rea
  22 2.502882   192.168.1.9      122.116.130.169  Modbu…        66     Query: Trans:   267; Unit:   1, Func:   3: Rea
  24 2.508458   122.116.130.169  192.168.1.9      Modbu…       191 Response: Trans:   267; Unit:   1, Func:   3: Rea
  26 3.025576   192.168.1.9      122.116.130.169  Modbu…        66     Query: Trans:   268; Unit:   1, Func:   3: Rea
  28 3.031413   122.116.130.169  192.168.1.9      Modbu…       191 Response: Trans:   268; Unit:   1, Func:   3: Rea
  31 3.558374   192.168.1.9      122.116.130.169  Modbu…        66     Query: Trans:   269; Unit:   1, Func:   3: Rea
```

```
▷ Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▷ Ethernet II, Src: HewlettP_47:08:55 (64:51:06:47:08:55), Dst: D-LinkIn_c9:23:b4 (9c:d6:43:c9:23:b4)
▷ Internet Protocol Version 4, Src: 192.168.1.9, Dst: 122.116.130.169
▷ Transmission Control Protocol, Src Port: 51053, Dst Port: 502, Seq: 1, Ack: 1, Len: 12
▷ Modbus/TCP
▷ Modbus
```

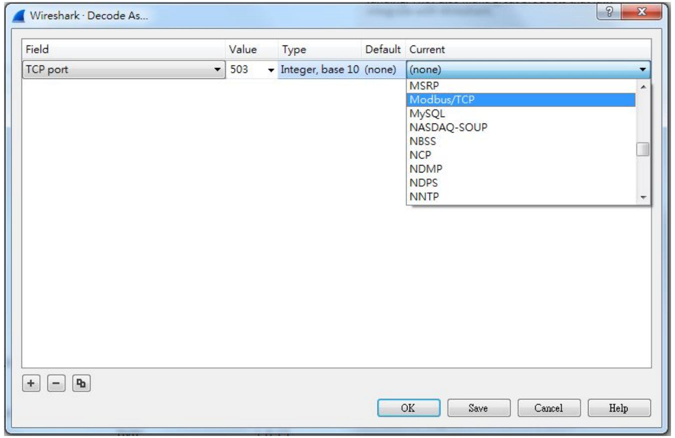
```
0000  9c d6 43 c9 23 b4 64 51  06 47 08 55 08 00 45 00   ..C.#.dQ .G.U..E.
0010  00 34 32 96 40 00 80 06  00 00 c0 a8 01 09 7a 74   .42.@... ......zt
0020  82 a9 c7 6d 01 f6 b5 bb  a8 da 4a 37 c4 60 50 18   ...m.... ..J7.`P.
0030  00 fe be f5 00 00 01 06  00 00 00 06 01 03 00 00   ........ ........
0040  00 40                                              .@
```

Modbus: Protocol

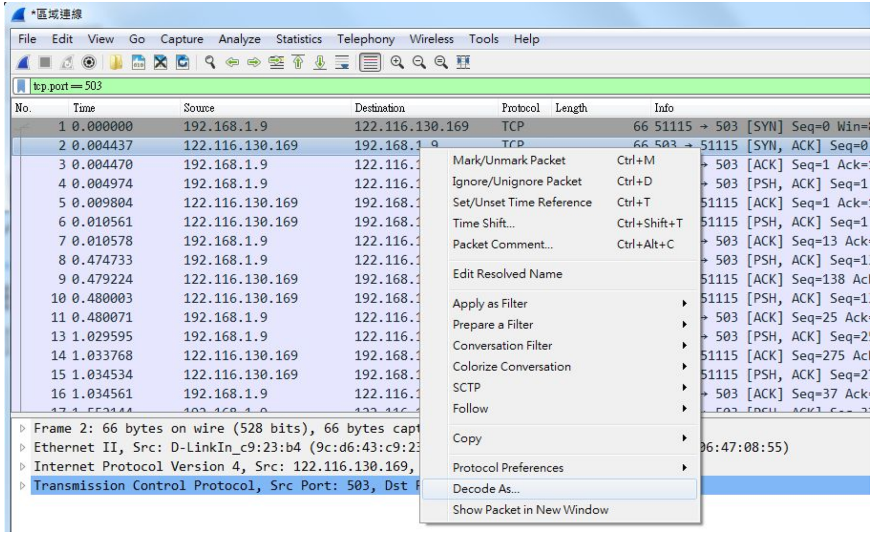
Packets: 224 · Displayed: 98 (43.8%)

如果不是 502 port

MODBUS TCP 不一定得採用 502 port，此時輸入 modbus 並不適用。以503 port 為例，可以試著輸入 tcp.port==503，再按右鍵選擇 Decode As ,如圖選擇 Modbus/TP 後即可看到效果。

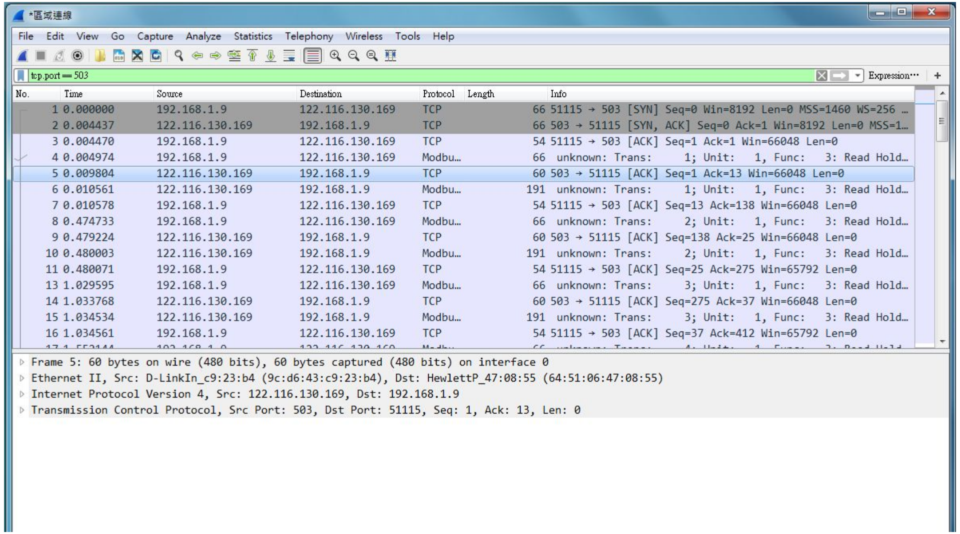


Field	Value	Type	Default	Current
TCP port	503	Integer, base 10	(none)	(none)


*區域連線
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window

```
tcp.port == 503
No.  Time        Source            Destination       Protocol  Length  Info
  1 0.000000    192.168.1.9       122.116.130.169   TCP       66 51115 → 503 [SYN] Seq=0 Win=
  2 0.004437    122.116.130.169   192.168.1.9       TCP       66 503 → 51115 [SYN, ACK] Seq=0
  3 0.004470    192.168.1.9       122.116.1                      → 503 [ACK] Seq=1 Ack=
  4 0.004974    192.168.1.9       122.116.1                      → 503 [PSH, ACK] Seq=1
  5 0.009804    122.116.130.169   192.168.1                      51115 [ACK] Seq=1 Ack=
  6 0.010561    122.116.130.169   192.168.1                      51115 [PSH, ACK] Seq=1
  7 0.010578    192.168.1.9       122.116.1                      → 503 [ACK] Seq=13 Ack
  8 0.474733    192.168.1.9       122.116.1                      → 503 [PSH, ACK] Seq=1
  9 0.479224    122.116.130.169   192.168.1                      51115 [ACK] Seq=138 Ac
 10 0.480003    122.116.130.169   192.168.1                      51115 [PSH, ACK] Seq=1
 11 0.480071    192.168.1.9       122.116.1                      → 503 [ACK] Seq=25 Ack
 13 1.029595    192.168.1.9       122.116.1                      → 503 [PSH, ACK] Seq=2
 14 1.033768    122.116.130.169   192.168.1                      51115 [ACK] Seq=275 Ac
 15 1.034534    122.116.130.169   192.168.1                      51115 [PSH, ACK] Seq=2
 16 1.034561    192.168.1.9       122.116.1                      → 503 [ACK] Seq=37 Ack

▷ Frame 2: 66 bytes on wire (528 bits), 66 bytes capt
▷ Ethernet II, Src: D-LinkIn_c9:23:b4 (9c:d6:43:c9:2                 06:47:08:55)
▷ Internet Protocol Version 4, Src: 122.116.130.169,
▷ Transmission Control Protocol, Src Port: 503, Dst F
```

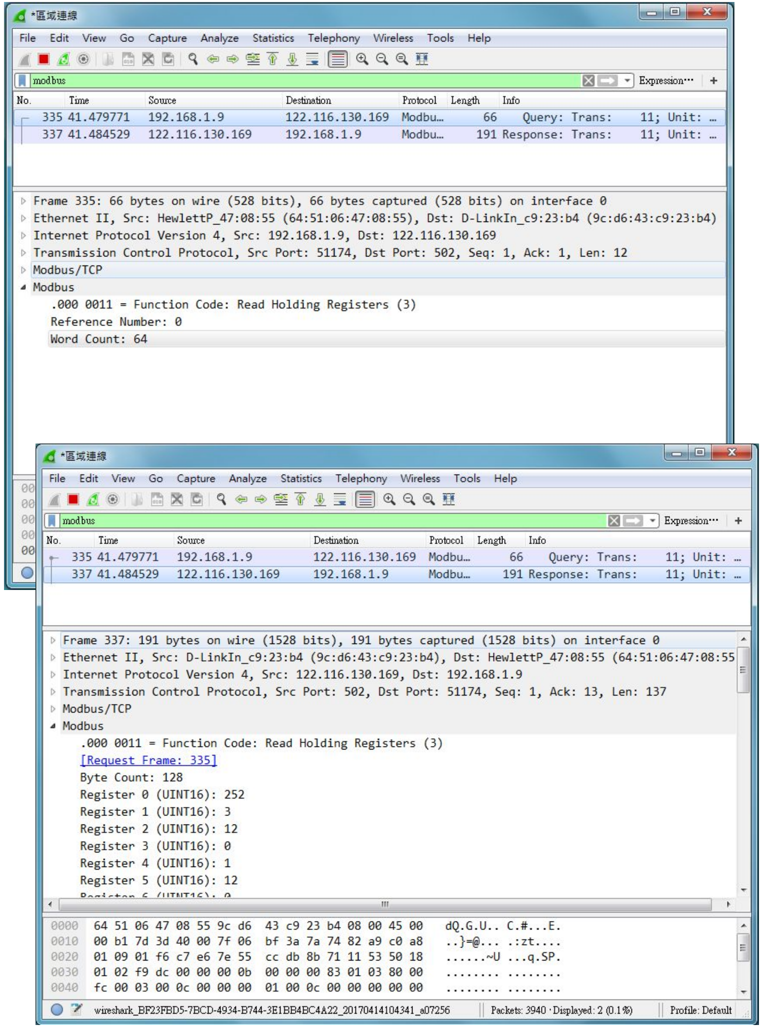

*區域連線
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

```
tcp.port == 503
No.  Time        Source            Destination       Protocol  Length  Info
  1 0.000000    192.168.1.9       122.116.130.169   TCP        66 51115 → 503 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 …
  2 0.004437    122.116.130.169   192.168.1.9       TCP        66 503 → 51115 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1…
  3 0.004470    192.168.1.9       122.116.130.169   TCP        54 51115 → 503 [ACK] Seq=1 Ack=1 Win=66048 Len=0
  4 0.004974    192.168.1.9       122.116.130.169   Modbu…     66  unknown: Trans:     1; Unit:   1, Func:   3: Read Hold…
  5 0.009804    122.116.130.169   192.168.1.9       TCP        60 503 → 51115 [ACK] Seq=1 Ack=13 Win=66048 Len=0
  6 0.010561    122.116.130.169   192.168.1.9       Modbu…    191  unknown: Trans:     1; Unit:   1, Func:   3: Read Hold…
  7 0.010578    192.168.1.9       122.116.130.169   TCP        54 51115 → 503 [ACK] Seq=13 Ack=138 Win=66048 Len=0
  8 0.474733    192.168.1.9       122.116.130.169   Modbu…     66  unknown: Trans:     2; Unit:   1, Func:   3: Read Hold…
  9 0.479224    122.116.130.169   192.168.1.9       TCP        60 503 → 51115 [ACK] Seq=138 Ack=25 Win=66048 Len=0
 10 0.480003    122.116.130.169   192.168.1.9       Modbu…    191  unknown: Trans:     2; Unit:   1, Func:   3: Read Hold…
 11 0.480071    192.168.1.9       122.116.130.169   TCP        54 51115 → 503 [ACK] Seq=25 Ack=275 Win=65792 Len=0
 13 1.029595    192.168.1.9       122.116.130.169   Modbu…     66  unknown: Trans:     3; Unit:   1, Func:   3: Read Hold…
 14 1.033768    122.116.130.169   192.168.1.9       TCP        60 503 → 51115 [ACK] Seq=275 Ack=37 Win=66048 Len=0
 15 1.034534    122.116.130.169   192.168.1.9       Modbu…    191  unknown: Trans:     3; Unit:   1, Func:   3: Read Hold…
 16 1.034561    192.168.1.9       122.116.130.169   TCP        54 51115 → 503 [ACK] Seq=37 Ack=412 Win=65792 Len=0

▷ Frame 5: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▷ Ethernet II, Src: D-LinkIn_c9:23:b4 (9c:d6:43:c9:23:b4), Dst: HewlettP_47:08:55 (64:51:06:47:08:55)
▷ Internet Protocol Version 4, Src: 122.116.130.169, Dst: 192.168.1.9
▷ Transmission Control Protocol, Src Port: 503, Dst Port: 51115, Seq: 1, Ack: 13, Len: 0
```

試著解讀封包

停止 MODBUS TCP Client 程式，將wireshark 重新以 modbus 關鍵字進行記錄，按下 MODBUS TCP Client Read 鍵，以產生一組封包。點選第一組詢問封包 Query，可以知道是從 192.168.1.9 就是電腦 IP 詢問 122.116.130.169 也就是 元米網站 IP，由中間 MODBUS -> Word Count:64 等知道是讀取(Function code :Read Holding Registers) 位置0開始的64個。點選第二組 Response 則可以看到 122.116.130.169 回應訊息，以及 64 個 Register 的個別數值



```
No.   Time        Source            Destination       Protocol  Length  Info
  335 41.479771   192.168.1.9       122.116.130.169   Modbu…        66     Query: Trans:    11; Unit: …
  337 41.484529   122.116.130.169   192.168.1.9       Modbu…       191  Response: Trans:    11; Unit: …
```

```
▷ Frame 335: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
▷ Ethernet II, Src: HewlettP_47:08:55 (64:51:06:47:08:55), Dst: D-LinkIn_c9:23:b4 (9c:d6:43:c9:23:b4)
▷ Internet Protocol Version 4, Src: 192.168.1.9, Dst: 122.116.130.169
▷ Transmission Control Protocol, Src Port: 51174, Dst Port: 502, Seq: 1, Ack: 1, Len: 12
▷ Modbus/TCP
◢ Modbus
    .000 0011 = Function Code: Read Holding Registers (3)
    Reference Number: 0
    Word Count: 64
```

```
No.   Time        Source            Destination       Protocol  Length  Info
  335 41.479771   192.168.1.9       122.116.130.169   Modbu…        66     Query: Trans:    11; Unit: …
  337 41.484529   122.116.130.169   192.168.1.9       Modbu…       191  Response: Trans:    11; Unit: …
```

```
▷ Frame 337: 191 bytes on wire (1528 bits), 191 bytes captured (1528 bits) on interface 0
▷ Ethernet II, Src: D-LinkIn_c9:23:b4 (9c:d6:43:c9:23:b4), Dst: HewlettP_47:08:55 (64:51:06:47:08:55
▷ Internet Protocol Version 4, Src: 122.116.130.169, Dst: 192.168.1.9
▷ Transmission Control Protocol, Src Port: 502, Dst Port: 51174, Seq: 1, Ack: 13, Len: 137
▷ Modbus/TCP
◢ Modbus
    .000 0011 = Function Code: Read Holding Registers (3)
    [Request Frame: 335]
    Byte Count: 128
    Register 0 (UINT16): 252
    Register 1 (UINT16): 3
    Register 2 (UINT16): 12
    Register 3 (UINT16): 0
    Register 4 (UINT16): 1
    Register 5 (UINT16): 12
```

```
0000  64 51 06 47 08 55 9c d6  43 c9 23 b4 08 00 45 00   dQ.G.U.. C.#...E.
0010  00 b1 7d 3d 40 00 7f 06  bf 3a 7a 74 82 a9 c0 a8   ..}=@... .:zt....
0020  01 09 01 f6 c7 e6 7e 55  cc db 8b 71 11 53 50 18   ......~U ...q.SP.
0030  01 02 f9 dc 00 00 00 0b  00 00 00 83 01 03 80 00   ........ ........
0040  fc 00 03 00 0c 00 00 00  01 00 0c 00 00 00 00 00   ........ ........
```

```
wireshark_BF23FBD5-7BCD-4934-B744-3E1BB4BC4A22_20170414104341_a07256 | Packets: 3940 · Displayed: 2 (0.1%) | Profile: Default
```

產生其他封包

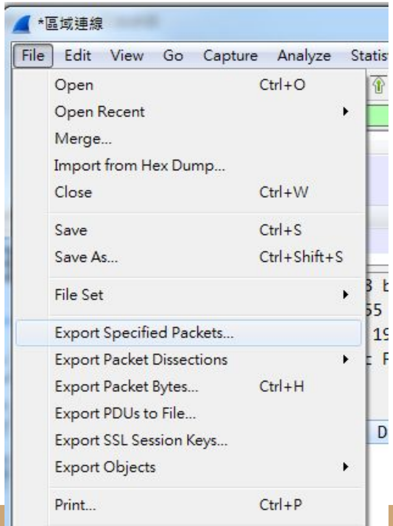
試著操作 MODBUS TCP Client 程式：改變一個 Register 後按下 Write 以產生 Write Single Register; 改變連續兩個Register 後按下 Write 以產生 Write Multiple Registers; 改點選右上 Input Register 按下 Read 以產生 Read Input Registers。

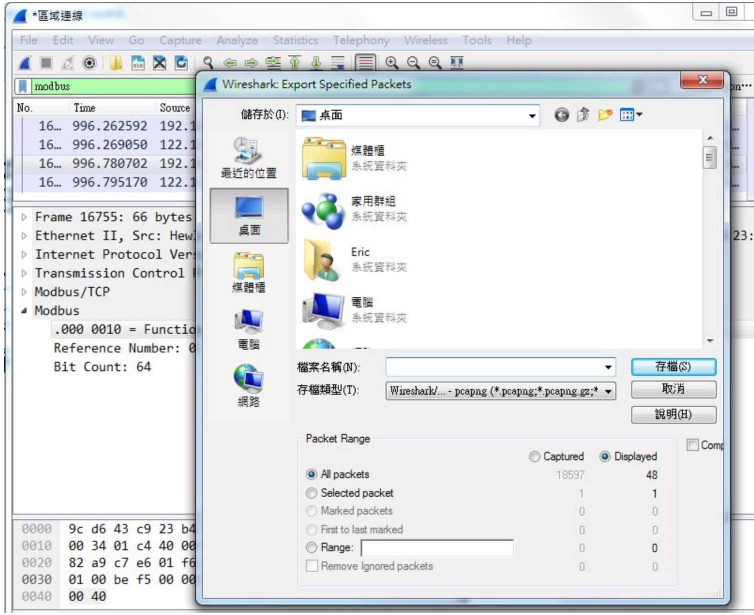
換點選 COIL 頁面，按下 Read 產生 Read Coils; 點選一個點改變狀態後按下 Write 以產生 Write Single Coil; 點選兩個點改變狀態後按下 Write 以產生 Write Multiple Coils; 改點選右上 Input 按下 Read 以產生 Read Discrete Inputs。如此常用的 MODBUS TCP Function code 讀取與回應訊息，都可以獲得驗證。

儲存記錄

停止記錄後按下 save 可以記錄所有封包，但必須注意這會記錄下包含 modbus 以及其他通訊的所有封包，如果將這樣的封包存檔對外提供，除了檔案過大外，也會有將電腦中要資訊外流的風險。

選擇 File->Export Specified Packets.. 將 All Packets Displayed 進行存檔，此時只存檔看到的 MODBUS 封包，就沒有上述疑慮了。





modbus

```
No.    Time         Source
 16…   996.262592   192.1
 16…   996.269050   122.1
 16…   996.780702   192.1
 16…   996.795170   122.1

▷ Frame 16755: 66 bytes
▷ Ethernet II, Src: Hew
▷ Internet Protocol Ver
▷ Transmission Control P
▷ Modbus/TCP
◢ Modbus
    .000 0010 = Functio
    Reference Number: 0
    Bit Count: 64

0000  9c d6 43 c9 23 b4
0010  00 34 01 c4 40 00
0020  82 a9 c7 e6 01 f6
0030  01 00 be f5 00 00
0040  00 40
```

儲存於(I): 桌面

檔案名稱(N):

存檔類型(T): Wireshark/... - pcapng (*.pcapng;*.pcapng.gz;*

Packet Range

	○ Captured	● Displayed
● All packets	18597	48
○ Selected packet	1	1
○ Marked packets	0	0
○ First to last marked	0	0
○ Range:	0	0
□ Remove Ignored packets	0	0

□ Comp

關於 MODBUS 封包

完整版可參考這篇
http://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf

如果要先從簡易版 MODBUS ASCII/RTU 開始學習
http://modbus.org/docs/PI_MBUS_300.pdf 是不錯的選擇

元米科技提供 MODBUS 相關軟硬體設計服務，如有需求請洽
eric.icdt@msa.hinet.net，更進一步資訊請上元米網站 http://www.icdt.com.tw