Lab 2 - Wireshark

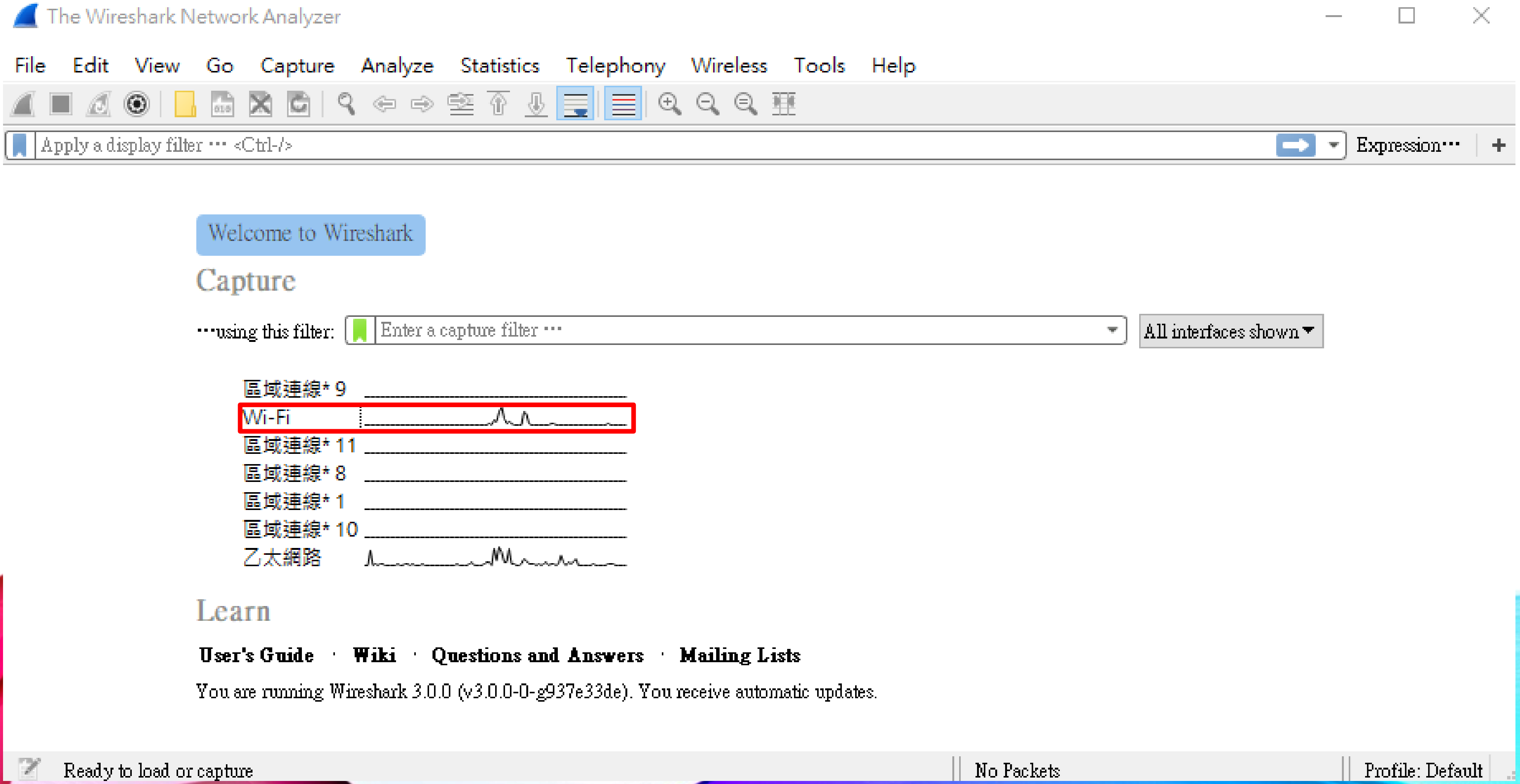
Introduction to Computer Networks

Download and Install

Wireshark download

- https://www.wireshark.org/#download

Wireshark



The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ··· <Ctrl-/>
Expression···
+
Welcome to Wireshark

Capture

···using this filter: Enter a capture filter ··· All interfaces shown

區域連線* 9

Wi-Fi

區域連線* 11

區域連線* 8

區域連線* 1

區域連線* 10

乙太網路

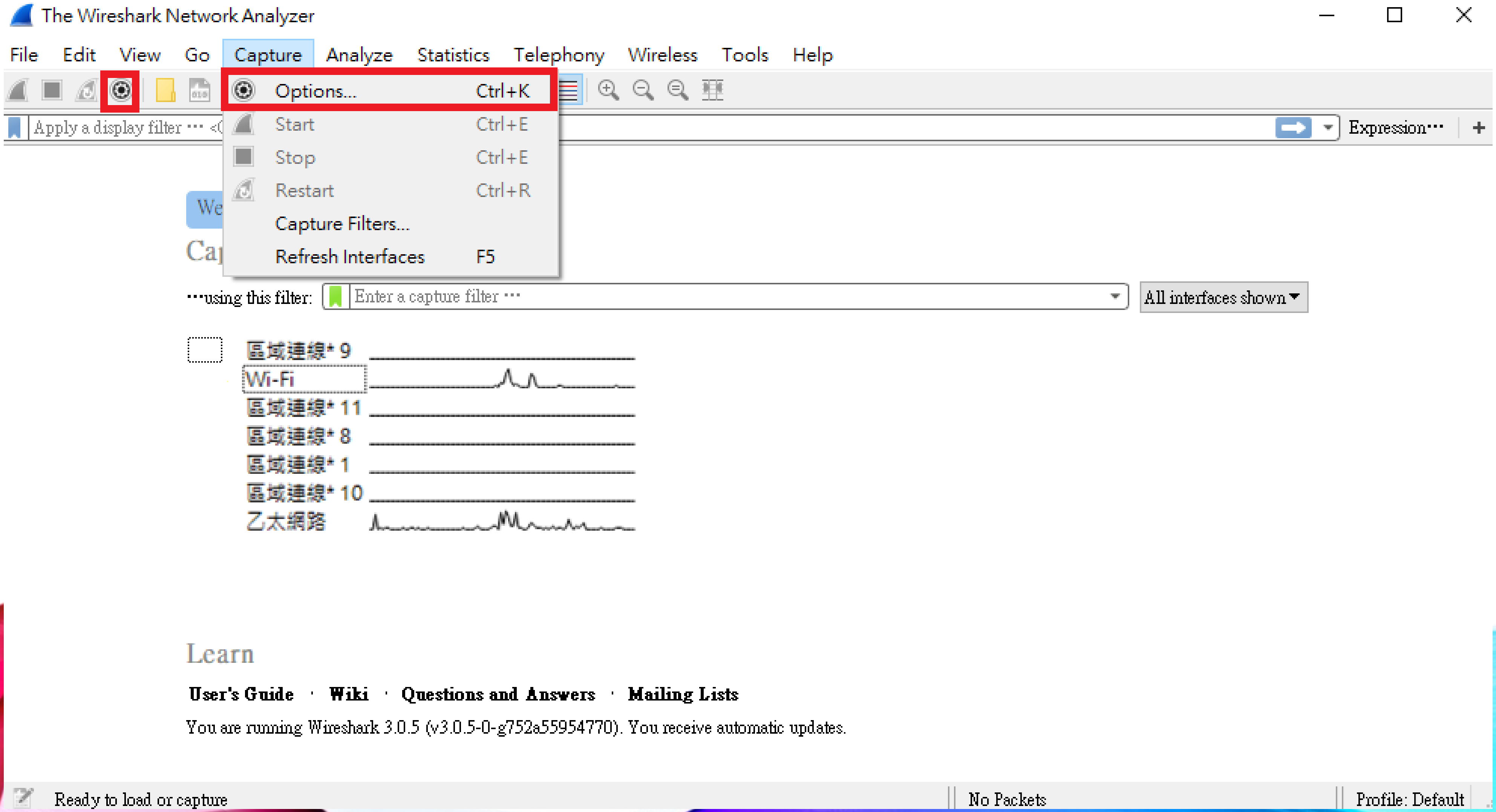
Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 3.0.0 (v3.0.0-0-g937e33de). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

Capture interface



The Wireshark Network Analyzer

⋯using this filter: Enter a capture filter ⋯

All interfaces shown

區域連線* 9
Wi-Fi
區域連線* 11
區域連線* 8
區域連線* 1
區域連線* 10
乙太網路

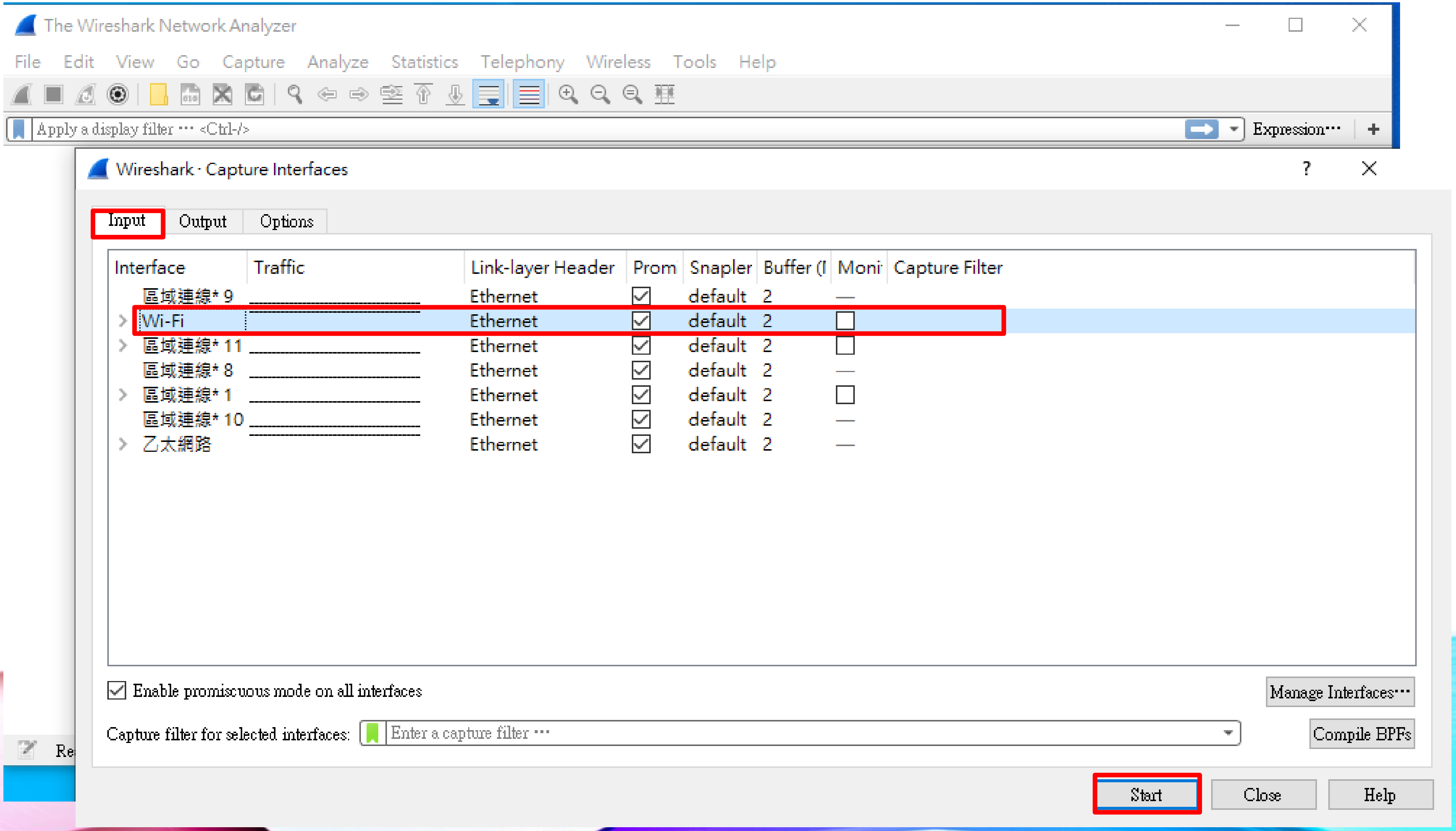
Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 3.0.5 (v3.0.5-0-g752a55954770). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

Capture interface

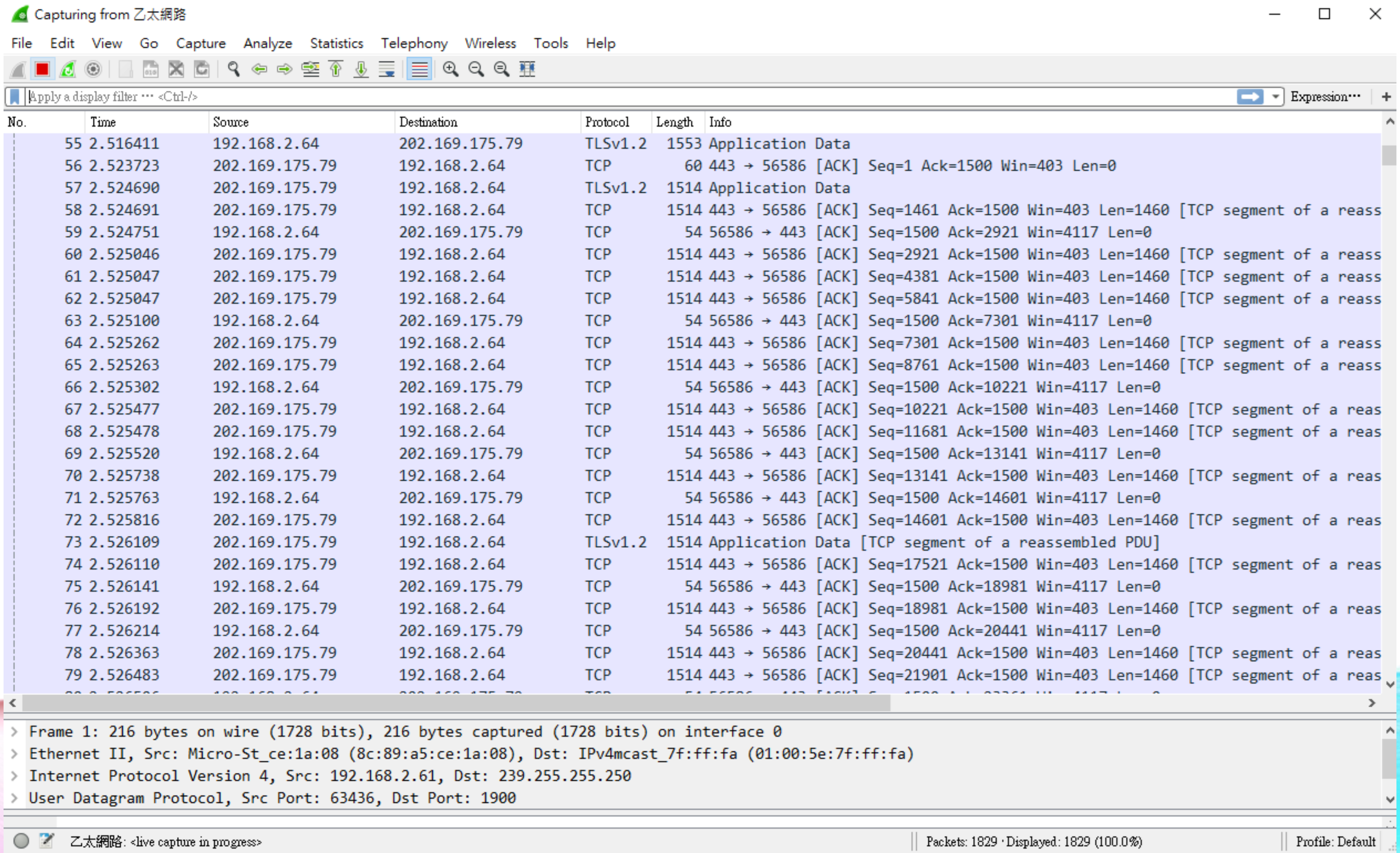

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
Wireshark · Capture Interfaces
Input
Output
Options
Manage Interfaces…
Compile BPFs
Start
Close
Help
Re

Interface	Traffic	Link-layer Header	Prom	Snapler	Buffer (I	Moni	Capture Filter
區域連線* 9		Ethernet	☑	default	2	—	
Wi-Fi		Ethernet	☑	default	2	□	
區域連線* 11		Ethernet	☑	default	2	□	
區域連線* 8		Ethernet	☑	default	2	—	
區域連線* 1		Ethernet	☑	default	2	□	
區域連線* 10		Ethernet	☑	default	2	—	
乙太網路		Ethernet	☑	default	2	—	

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter …

Data interface

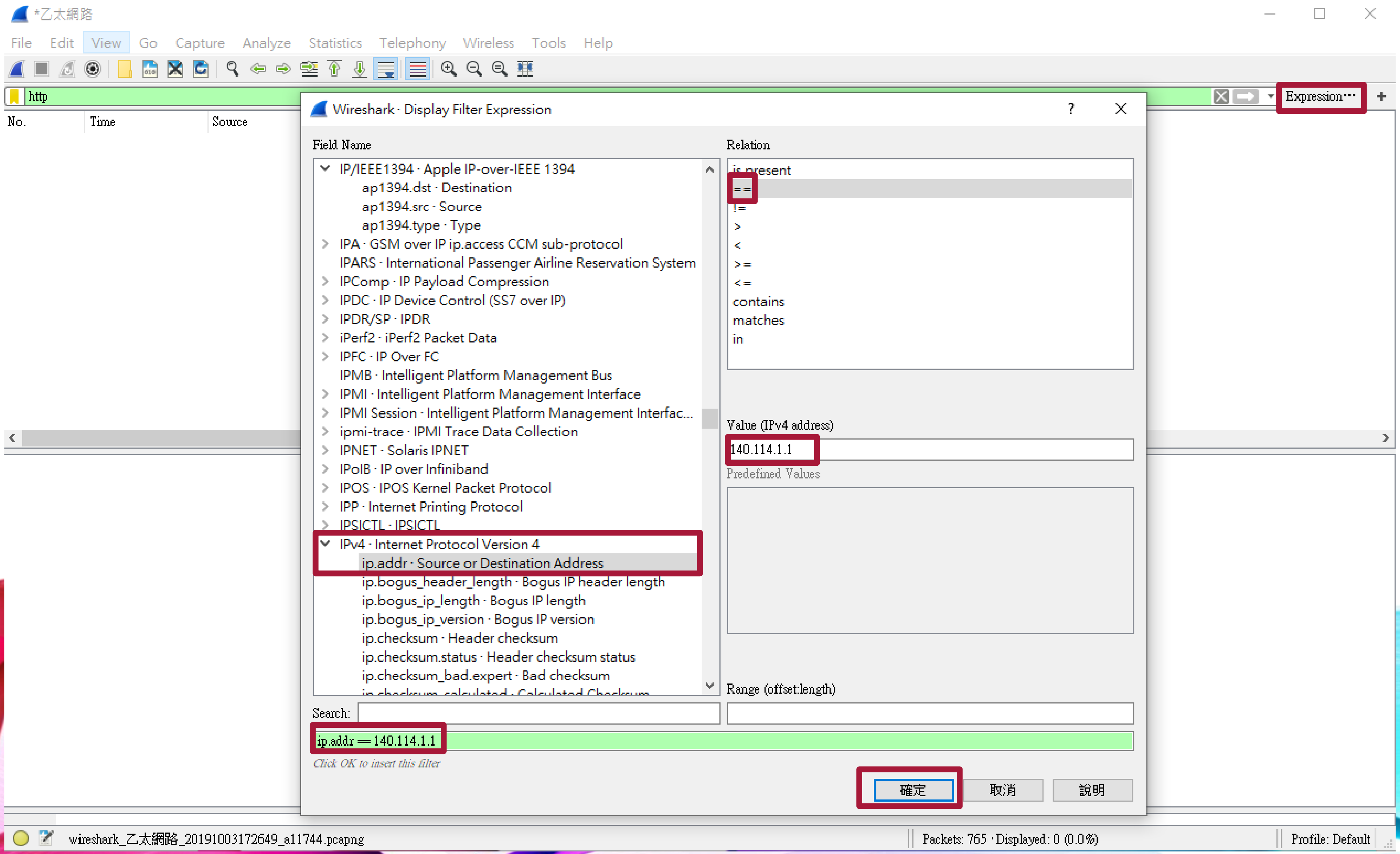

Capturing from 乙太網路
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

```
No.   Time      Source          Destination     Protocol Length Info
   55 2.516411  192.168.2.64    202.169.175.79  TLSv1.2  1553 Application Data
   56 2.523723  202.169.175.79  192.168.2.64    TCP        60 443 → 56586 [ACK] Seq=1 Ack=1500 Win=403 Len=0
   57 2.524690  202.169.175.79  192.168.2.64    TLSv1.2  1514 Application Data
   58 2.524691  202.169.175.79  192.168.2.64    TCP      1514 443 → 56586 [ACK] Seq=1461 Ack=1500 Win=403 Len=1460 [TCP segment of a reass
   59 2.524751  192.168.2.64    202.169.175.79  TCP        54 56586 → 443 [ACK] Seq=1500 Ack=2921 Win=4117 Len=0
   60 2.525046  202.169.175.79  192.168.2.64    TCP      1514 443 → 56586 [ACK] Seq=2921 Ack=1500 Win=403 Len=1460 [TCP segment of a reass
   61 2.525047  202.169.175.79  192.168.2.64    TCP      1514 443 → 56586 [ACK] Seq=4381 Ack=1500 Win=403 Len=1460 [TCP segment of a reass
   62 2.525047  202.169.175.79  192.168.2.64    TCP      1514 443 → 56586 [ACK] Seq=5841 Ack=1500 Win=403 Len=1460 [TCP segment of a reass
   63 2.525100  192.168.2.64    202.169.175.79  TCP        54 56586 → 443 [ACK] Seq=1500 Ack=7301 Win=4117 Len=0
   64 2.525262  202.169.175.79  192.168.2.64    TCP      1514 443 → 56586 [ACK] Seq=7301 Ack=1500 Win=403 Len=1460 [TCP segment of a reass
   65 2.525263  202.169.175.79  192.168.2.64    TCP      1514 443 → 56586 [ACK] Seq=8761 Ack=1500 Win=403 Len=1460 [TCP segment of a reass
   66 2.525302  192.168.2.64    202.169.175.79  TCP        54 56586 → 443 [ACK] Seq=1500 Ack=10221 Win=4117 Len=0
   67 2.525477  202.169.175.79  192.168.2.64    TCP      1514 443 → 56586 [ACK] Seq=10221 Ack=1500 Win=403 Len=1460 [TCP segment of a reas
   68 2.525478  202.169.175.79  192.168.2.64    TCP      1514 443 → 56586 [ACK] Seq=11681 Ack=1500 Win=403 Len=1460 [TCP segment of a reas
   69 2.525520  192.168.2.64    202.169.175.79  TCP        54 56586 → 443 [ACK] Seq=1500 Ack=13141 Win=4117 Len=0
   70 2.525738  202.169.175.79  192.168.2.64    TCP      1514 443 → 56586 [ACK] Seq=13141 Ack=1500 Win=403 Len=1460 [TCP segment of a reas
   71 2.525763  192.168.2.64    202.169.175.79  TCP        54 56586 → 443 [ACK] Seq=1500 Ack=14601 Win=4117 Len=0
   72 2.525816  202.169.175.79  192.168.2.64    TCP      1514 443 → 56586 [ACK] Seq=14601 Ack=1500 Win=403 Len=1460 [TCP segment of a reas
   73 2.526109  202.169.175.79  192.168.2.64    TLSv1.2  1514 Application Data [TCP segment of a reassembled PDU]
   74 2.526110  202.169.175.79  192.168.2.64    TCP      1514 443 → 56586 [ACK] Seq=17521 Ack=1500 Win=403 Len=1460 [TCP segment of a reas
   75 2.526141  192.168.2.64    202.169.175.79  TCP        54 56586 → 443 [ACK] Seq=1500 Ack=18981 Win=4117 Len=0
   76 2.526192  202.169.175.79  192.168.2.64    TCP      1514 443 → 56586 [ACK] Seq=18981 Ack=1500 Win=403 Len=1460 [TCP segment of a reas
   77 2.526214  192.168.2.64    202.169.175.79  TCP        54 56586 → 443 [ACK] Seq=1500 Ack=20441 Win=4117 Len=0
   78 2.526363  202.169.175.79  192.168.2.64    TCP      1514 443 → 56586 [ACK] Seq=20441 Ack=1500 Win=403 Len=1460 [TCP segment of a reas
   79 2.526483  202.169.175.79  192.168.2.64    TCP      1514 443 → 56586 [ACK] Seq=21901 Ack=1500 Win=403 Len=1460 [TCP segment of a reas
```

```
> Frame 1: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface 0
> Ethernet II, Src: Micro-St_ce:1a:08 (8c:89:a5:ce:1a:08), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 192.168.2.61, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 63436, Dst Port: 1900
```

乙太網路: <live capture in progress>   Packets: 1829 · Displayed: 1829 (100.0%)   Profile: Default

Filter expression



http

Wireshark · Display Filter Expression

Field Name

- IP/IEEE1394 · Apple IP-over-IEEE 1394
  - ap1394.dst · Destination
  - ap1394.src · Source
  - ap1394.type · Type
- IPA · GSM over IP ip.access CCM sub-protocol
- IPARS · International Passenger Airline Reservation System
- IPComp · IP Payload Compression
- IPDC · IP Device Control (SS7 over IP)
- IPDR/SP · IPDR
- iPerf2 · iPerf2 Packet Data
- IPFC · IP Over FC
- IPMB · Intelligent Platform Management Bus
- IPMI · Intelligent Platform Management Interface
- IPMI Session · Intelligent Platform Management Interfac...
- ipmi-trace · IPMI Trace Data Collection
- IPNET · Solaris IPNET
- IPoIB · IP over Infiniband
- IPOS · IPOS Kernel Packet Protocol
- IPP · Internet Printing Protocol
- IPSICTL · IPSICTL
- IPv4 · Internet Protocol Version 4
  - ip.addr · Source or Destination Address
  - ip.bogus_header_length · Bogus IP header length
  - ip.bogus_ip_length · Bogus IP length
  - ip.bogus_ip_version · Bogus IP version
  - ip.checksum · Header checksum
  - ip.checksum.status · Header checksum status
  - ip.checksum_bad.expert · Bad checksum
  - ip.checksum_calculated · Calculated Checksum

Relation

- is present
- ==
- !=
- >
- <
- >=
- <=
- contains
- matches
- in

Value (IPv4 address): 140.114.1.1

Predefined Values

Range (offset:length)

Search:

```
ip.addr == 140.114.1.1
```

Click OK to insert this filter

wireshark_乙太網路_20191003172649_a11744.pcapng

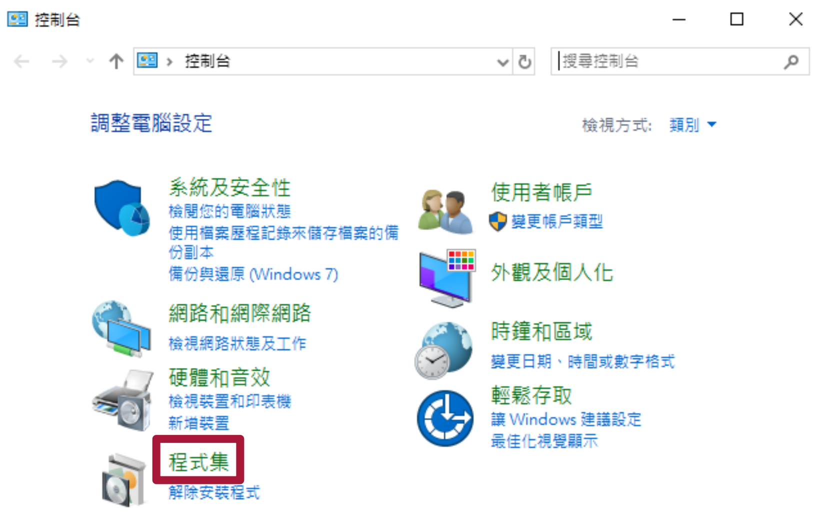
Packets: 765 · Displayed: 0 (0.0%)

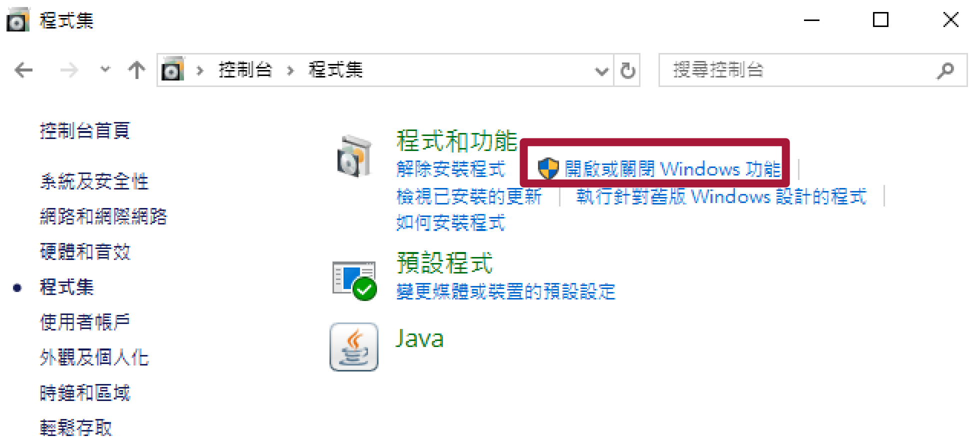
Profile: Default

Demo

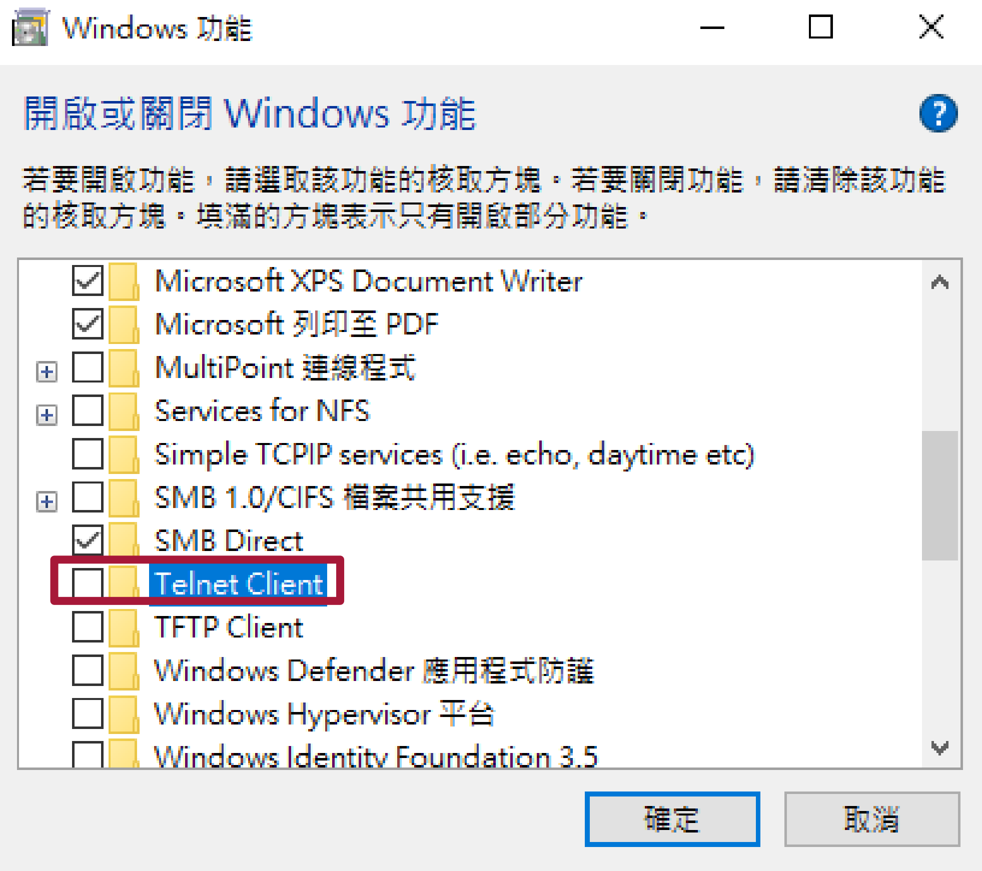
- TELNET
- HTTP

TELNET – Windows GUI





TELNET – Windows GUI



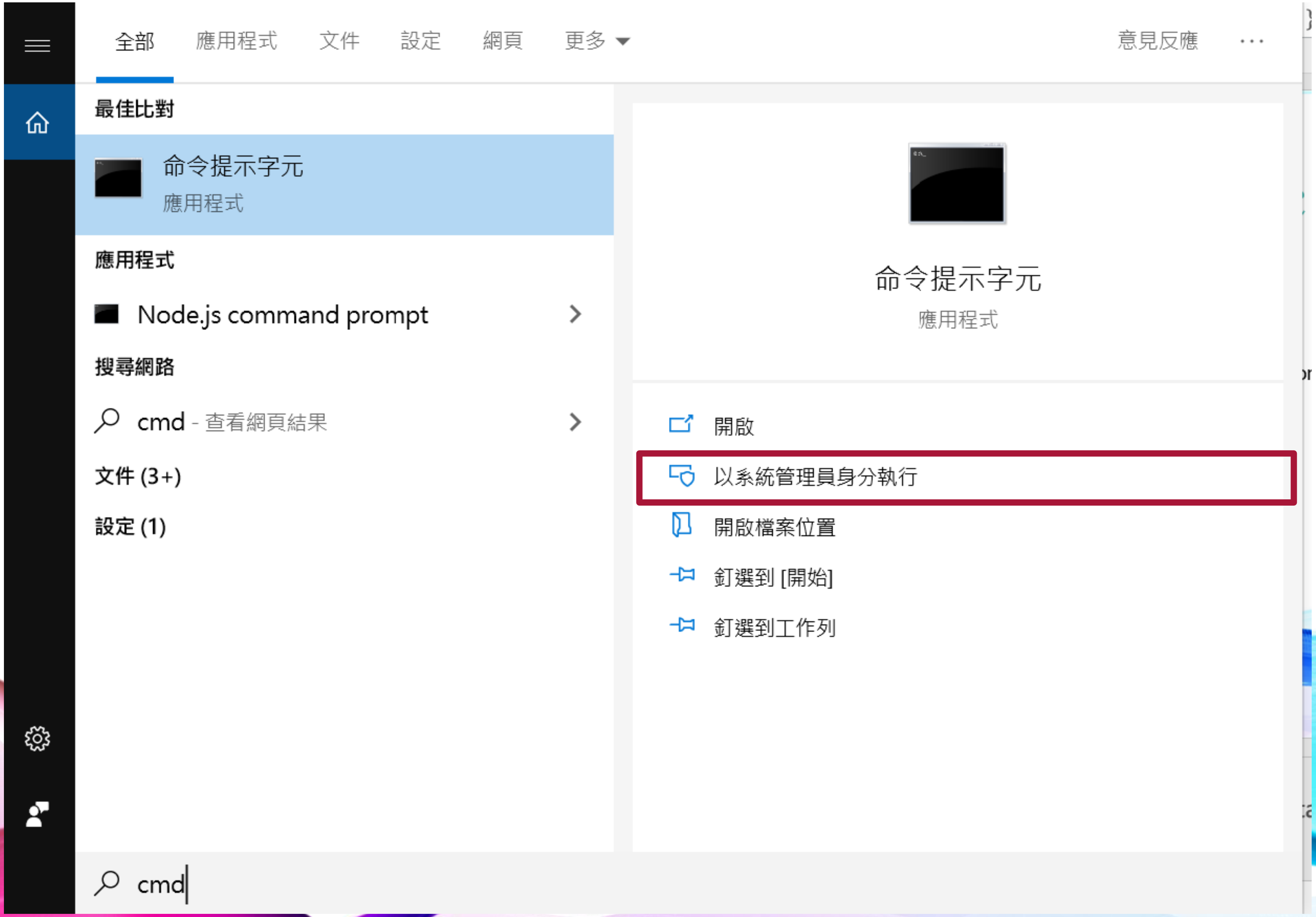
Windows 功能

開啟或關閉 Windows 功能

若要開啟功能，請選取該功能的核取方塊。若要關閉功能，請清除該功能的核取方塊。填滿的方塊表示只有開啟部分功能。

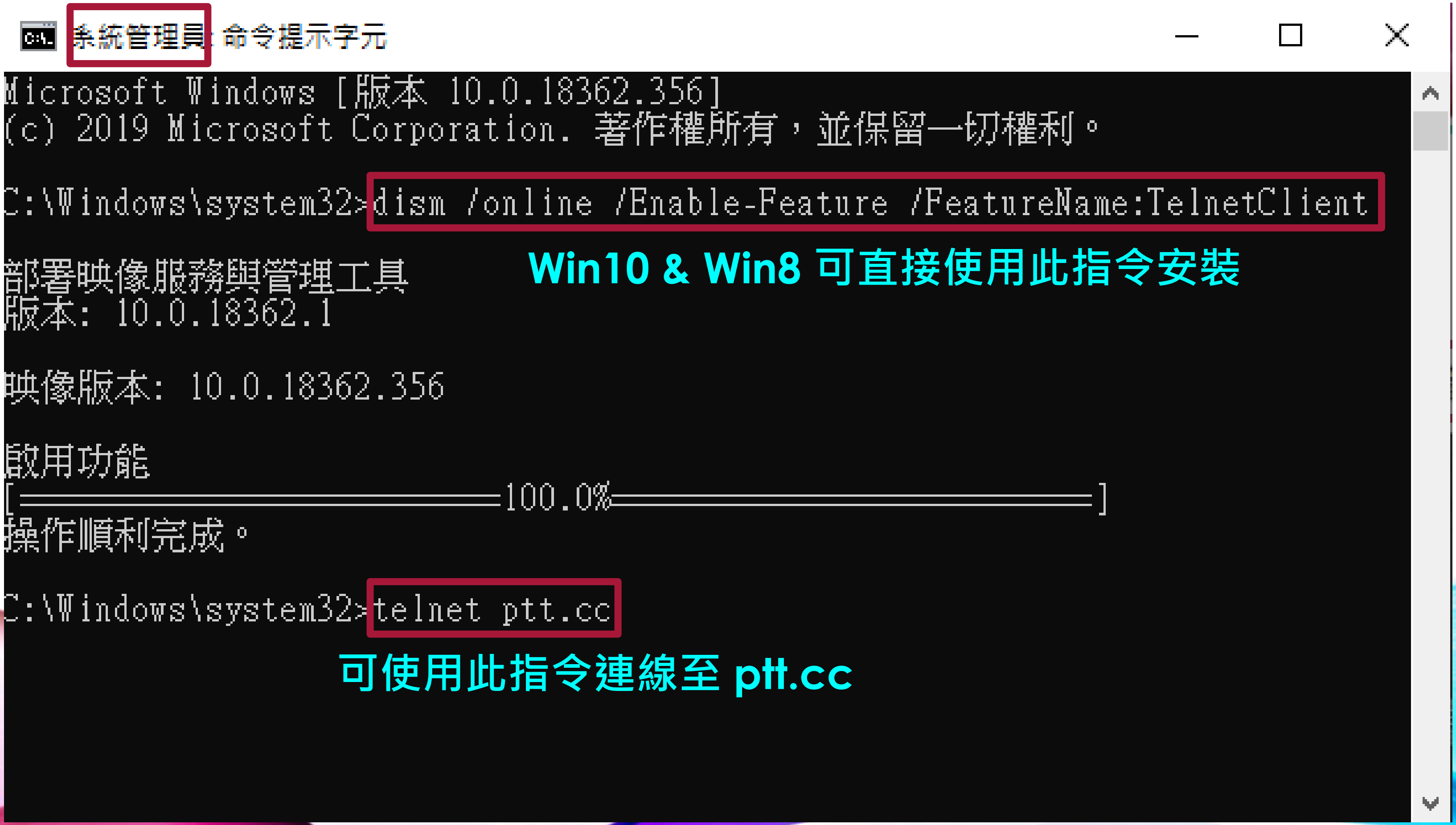
- ☑ Microsoft XPS Document Writer
- ☑ Microsoft 列印至 PDF
- ⊞ □ MultiPoint 連線程式
- ⊞ □ Services for NFS
- □ Simple TCPIP services (i.e. echo, daytime etc)
- ⊞ □ SMB 1.0/CIFS 檔案共用支援
- ☑ SMB Direct
- □ Telnet Client
- □ TFTP Client
- □ Windows Defender 應用程式防護
- □ Windows Hypervisor 平台
- □ Windows Identity Foundation 3.5

TELNET – Windows cmd



TELNET – Windows cmd

指令：dism /online /Enable-Feature /FeatureName:TelnetClient



```
Microsoft Windows [版本 10.0.18362.356]
(c) 2019 Microsoft Corporation. 著作權所有，並保留一切權利。

C:\Windows\system32>dism /online /Enable-Feature /FeatureName:TelnetClient

部署映像服務與管理工具
版本: 10.0.18362.1

映像版本: 10.0.18362.356

啟用功能
[==========================100.0%==========================]
操作順利完成。

C:\Windows\system32>telnet ptt.cc
```

Win10 & Win8 可直接使用此指令安裝

可使用此指令連線至 ptt.cc

TELNET – Mac OS

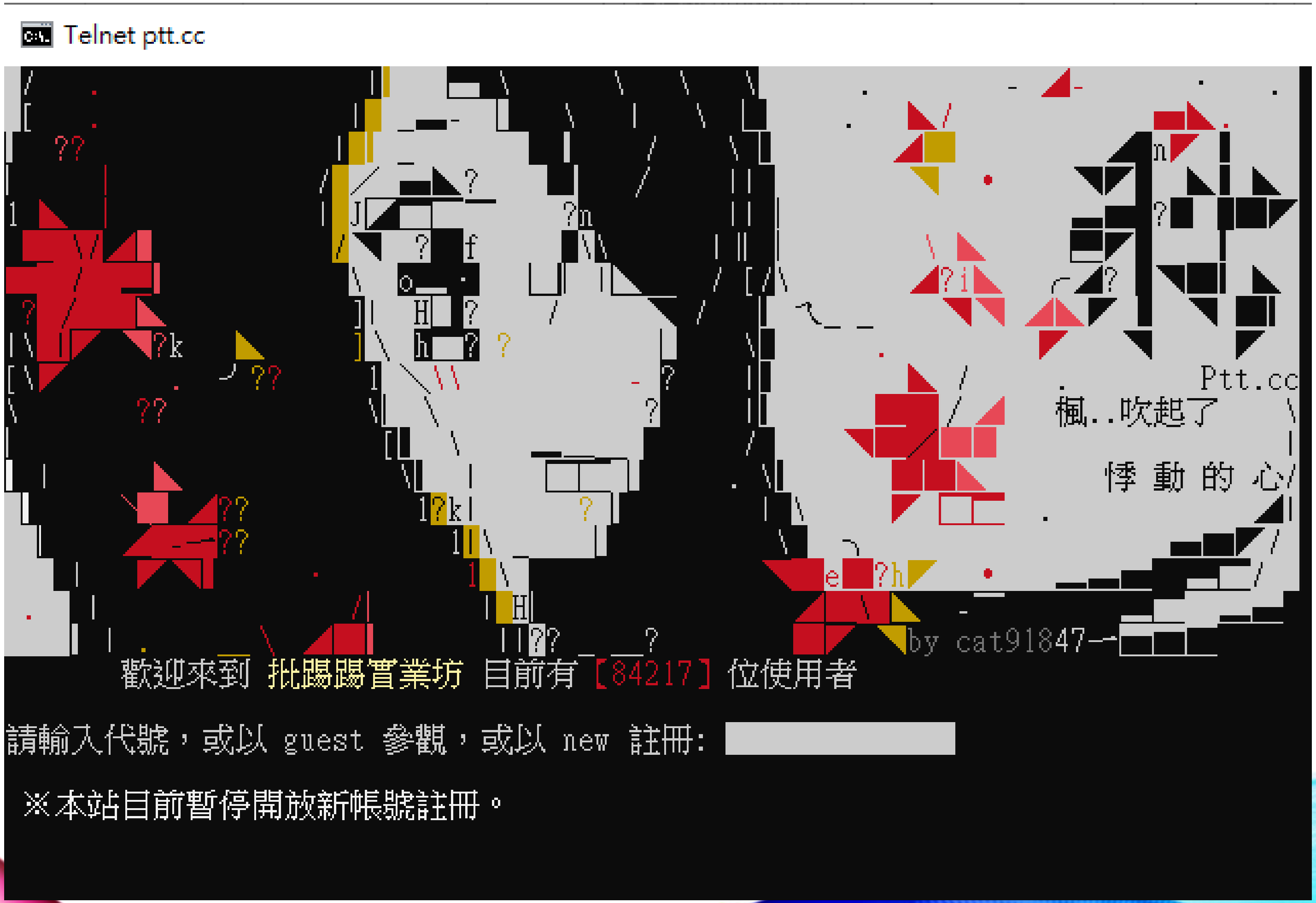
- **Install command**

```
/usr/bin/ruby -e "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/master/install)"
```

- **Brew command**

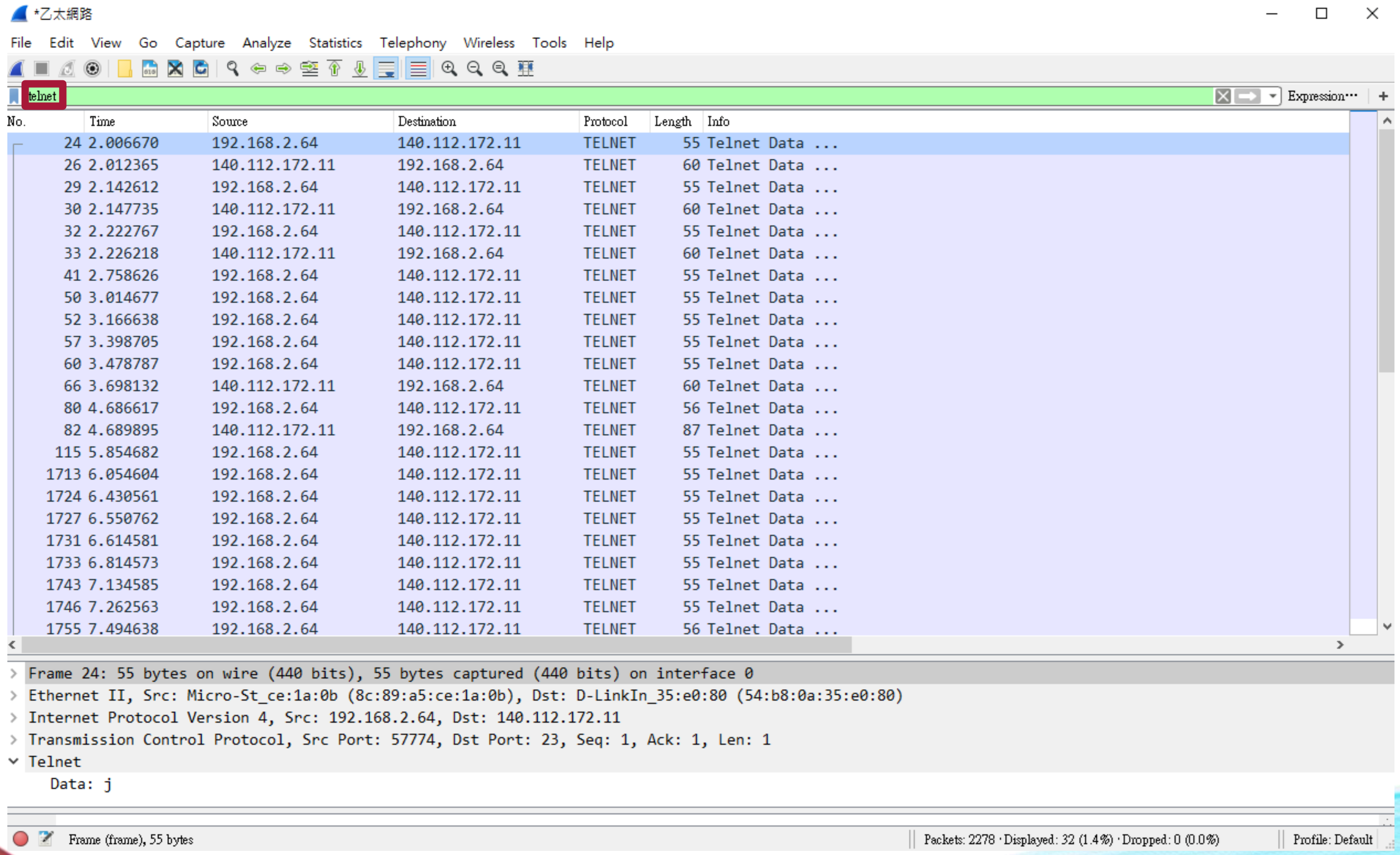
```
brew install telnet
```

TELNET – ptt.cc



```
    歡迎來到 批踢踢實業坊 目前有 [84217] 位使用者
請輸入代號，或以 guest 參觀，或以 new 註冊:
 ※本站目前暫停開放新帳號註冊。
```

TELNET – login


*乙太網路
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

telnet

```
No.   Time       Source          Destination     Protocol Length Info
   24 2.006670   192.168.2.64    140.112.172.11  TELNET     55 Telnet Data ...
   26 2.012365   140.112.172.11  192.168.2.64    TELNET     60 Telnet Data ...
   29 2.142612   192.168.2.64    140.112.172.11  TELNET     55 Telnet Data ...
   30 2.147735   140.112.172.11  192.168.2.64    TELNET     60 Telnet Data ...
   32 2.222767   192.168.2.64    140.112.172.11  TELNET     55 Telnet Data ...
   33 2.226218   140.112.172.11  192.168.2.64    TELNET     60 Telnet Data ...
   41 2.758626   192.168.2.64    140.112.172.11  TELNET     55 Telnet Data ...
   50 3.014677   192.168.2.64    140.112.172.11  TELNET     55 Telnet Data ...
   52 3.166638   192.168.2.64    140.112.172.11  TELNET     55 Telnet Data ...
   57 3.398705   192.168.2.64    140.112.172.11  TELNET     55 Telnet Data ...
   60 3.478787   192.168.2.64    140.112.172.11  TELNET     55 Telnet Data ...
   66 3.698132   140.112.172.11  192.168.2.64    TELNET     60 Telnet Data ...
   80 4.686617   192.168.2.64    140.112.172.11  TELNET     56 Telnet Data ...
   82 4.689895   140.112.172.11  192.168.2.64    TELNET     87 Telnet Data ...
  115 5.854682   192.168.2.64    140.112.172.11  TELNET     55 Telnet Data ...
 1713 6.054604   192.168.2.64    140.112.172.11  TELNET     55 Telnet Data ...
 1724 6.430561   192.168.2.64    140.112.172.11  TELNET     55 Telnet Data ...
 1727 6.550762   192.168.2.64    140.112.172.11  TELNET     55 Telnet Data ...
 1731 6.614581   192.168.2.64    140.112.172.11  TELNET     55 Telnet Data ...
 1733 6.814573   192.168.2.64    140.112.172.11  TELNET     55 Telnet Data ...
 1743 7.134585   192.168.2.64    140.112.172.11  TELNET     55 Telnet Data ...
 1746 7.262563   192.168.2.64    140.112.172.11  TELNET     55 Telnet Data ...
 1755 7.494638   192.168.2.64    140.112.172.11  TELNET     56 Telnet Data ...
```

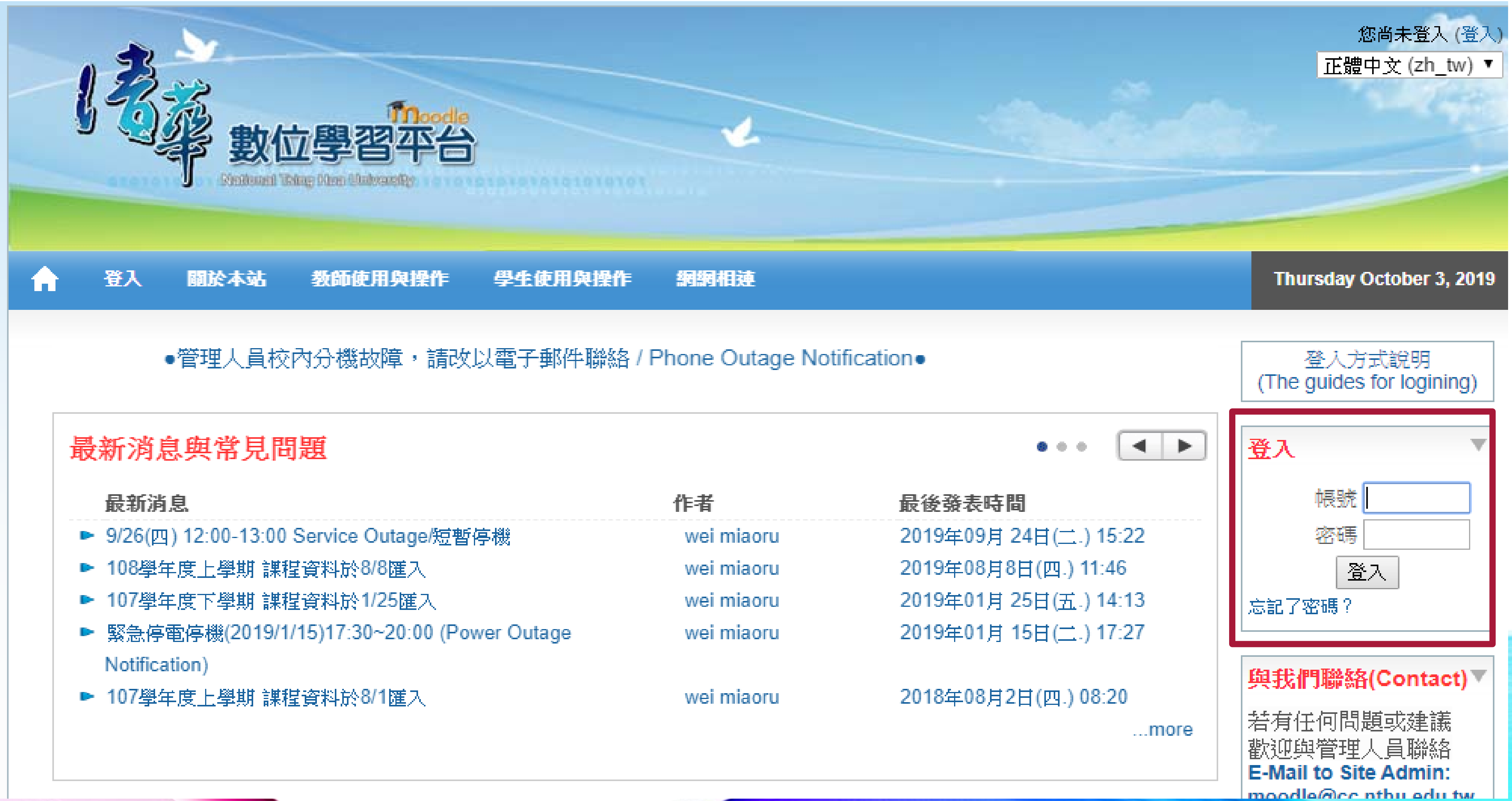
```
> Frame 24: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
> Ethernet II, Src: Micro-St_ce:1a:0b (8c:89:a5:ce:1a:0b), Dst: D-LinkIn_35:e0:80 (54:b8:0a:35:e0:80)
> Internet Protocol Version 4, Src: 192.168.2.64, Dst: 140.112.172.11
> Transmission Control Protocol, Src Port: 57774, Dst Port: 23, Seq: 1, Ack: 1, Len: 1
v Telnet
    Data: j
```

Frame (frame), 55 bytes | Packets: 2278 · Displayed: 32 (1.4%) · Dropped: 0 (0.0%) | Profile: Default

Http Request Method

- GET
- POST
- PUT
- DELETE

HTTP – NTHU moodle



•管理人員校內分機故障，請改以電子郵件聯絡 / Phone Outage Notification•

最新消息與常見問題

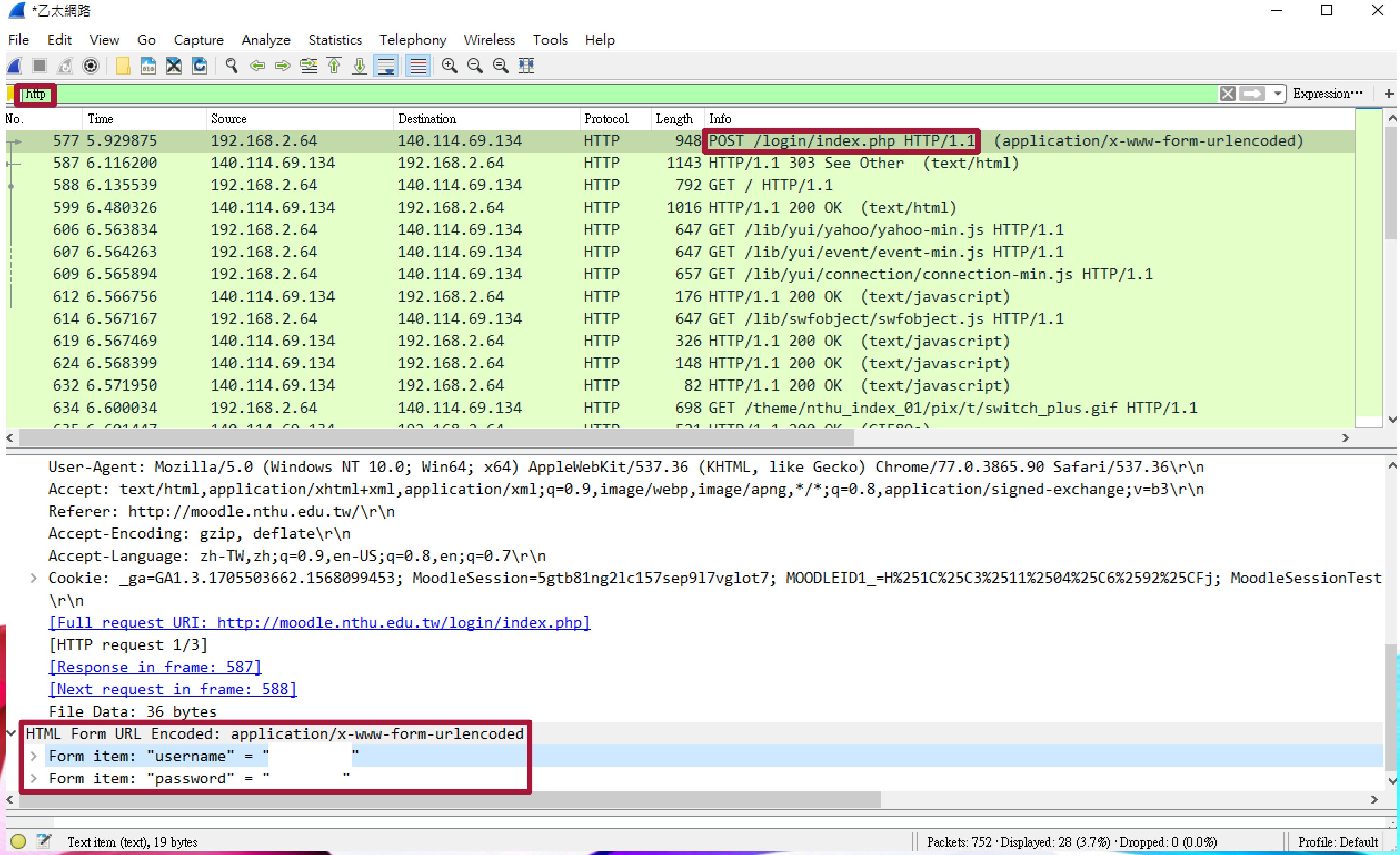
最新消息	作者	最後發表時間
9/26(四) 12:00-13:00 Service Outage/短暫停機	wei miaoru	2019年09月 24日(二.) 15:22
108學年度上學期 課程資料於8/8匯入	wei miaoru	2019年08月8日(四.) 11:46
107學年度下學期 課程資料於1/25匯入	wei miaoru	2019年01月 25日(五.) 14:13
緊急停電停機(2019/1/15)17:30~20:00 (Power Outage Notification)	wei miaoru	2019年01月 15日(二.) 17:27
107學年度上學期 課程資料於8/1匯入	wei miaoru	2018年08月2日(四.) 08:20

...more

與我們聯絡(Contact)

若有任何問題或建議
歡迎與管理人員聯絡
E-Mail to Site Admin:
moodle@cc.nthu.edu.tw

HTTP - login



http

```
No.  Time      Source          Destination     Protocol Length Info
 577 5.929875  192.168.2.64    140.114.69.134  HTTP      948 POST /login/index.php HTTP/1.1  (application/x-www-form-urlencoded)
 587 6.116200  140.114.69.134  192.168.2.64    HTTP     1143 HTTP/1.1 303 See Other  (text/html)
 588 6.135539  192.168.2.64    140.114.69.134  HTTP      792 GET / HTTP/1.1
 599 6.480326  140.114.69.134  192.168.2.64    HTTP     1016 HTTP/1.1 200 OK  (text/html)
 606 6.563834  192.168.2.64    140.114.69.134  HTTP      647 GET /lib/yui/yahoo/yahoo-min.js HTTP/1.1
 607 6.564263  192.168.2.64    140.114.69.134  HTTP      647 GET /lib/yui/event/event-min.js HTTP/1.1
 609 6.565894  192.168.2.64    140.114.69.134  HTTP      657 GET /lib/yui/connection/connection-min.js HTTP/1.1
 612 6.566756  140.114.69.134  192.168.2.64    HTTP      176 HTTP/1.1 200 OK  (text/javascript)
 614 6.567167  192.168.2.64    140.114.69.134  HTTP      647 GET /lib/swfobject/swfobject.js HTTP/1.1
 619 6.567469  140.114.69.134  192.168.2.64    HTTP      326 HTTP/1.1 200 OK  (text/javascript)
 624 6.568399  140.114.69.134  192.168.2.64    HTTP      148 HTTP/1.1 200 OK  (text/javascript)
 632 6.571950  140.114.69.134  192.168.2.64    HTTP       82 HTTP/1.1 200 OK  (text/javascript)
 634 6.600034  192.168.2.64    140.114.69.134  HTTP      698 GET /theme/nthu_index_01/pix/t/switch_plus.gif HTTP/1.1
 635 6.601447  140.114.69.134  192.168.2.64    HTTP      521 HTTP/1.1 200 OK  (GIF89a)
```

```
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\n
    Referer: http://moodle.nthu.edu.tw/\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7\r\n
  > Cookie: _ga=GA1.3.1705503662.1568099453; MoodleSession=5gtb81ng21c157sep917vglot7; MOODLEID1_=H%251C%25C3%2511%2504%25C6%2592%25CFj; MoodleSessionTest
    \r\n
    [Full request URI: http://moodle.nthu.edu.tw/login/index.php]
    [HTTP request 1/3]
    [Response in frame: 587]
    [Next request in frame: 588]
    File Data: 36 bytes
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "username" = "          "
  > Form item: "password" = "         "
```

Text item (text), 19 bytes | Packets: 752 · Displayed: 28 (3.7%) · Dropped: 0 (0.0%) | Profile: Default

Lab

- 找http開頭且有送出表單的網站
- 將Wireshark中的封包資料截圖並附上說明
- 評分標準包含資料有趣性與獨特性

Lab

- Deadline : **10/13 23:59** 前

- 檔名：<學號>_lab2.pdf
  (ex: 108XXXXXX_lab2.pdf)

- 遲交一週分數打8折、兩週打6折，以此類推