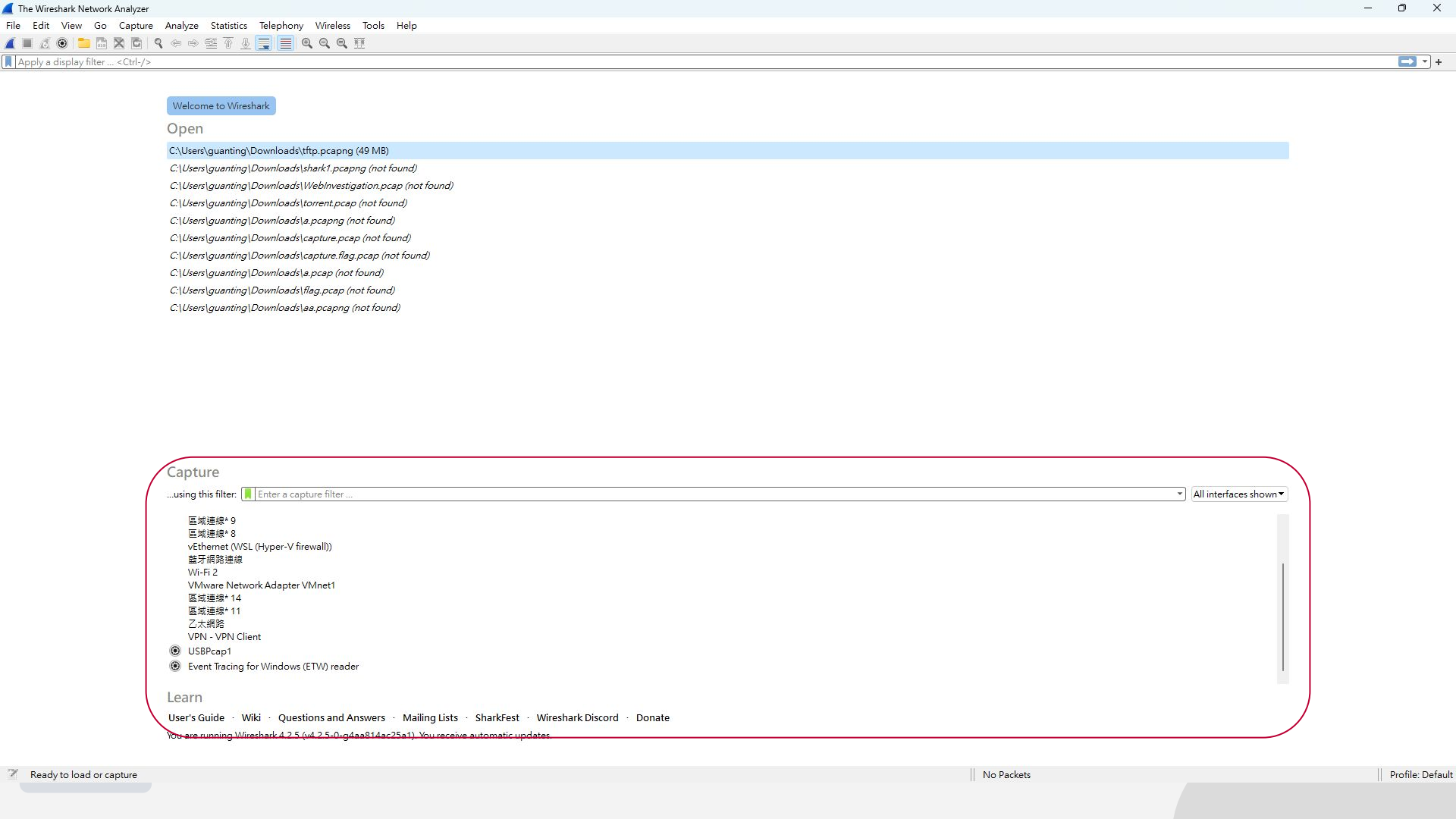
WireShark

官網

隱寫術 (Steganography)

WireShark

一個開源的網路封包剖析器，可即時從網路介面擷取封包中的資料。
它儘可能詳細地顯示擷取的資料以供使用者檢查它們的內容，並支援多協定的網路封包解析。


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Open
C:\Users\guanting\Downloads\tftp.pcapng (49 MB)
C:\Users\guanting\Downloads\shark1.pcapng (not found)
C:\Users\guanting\Downloads\WebInvestigation.pcap (not found)
C:\Users\guanting\Downloads\torrent.pcap (not found)
C:\Users\guanting\Downloads\a.pcapng (not found)
C:\Users\guanting\Downloads\capture.pcap (not found)
C:\Users\guanting\Downloads\capture.flag.pcap (not found)
C:\Users\guanting\Downloads\a.pcap (not found)
C:\Users\guanting\Downloads\flag.pcap (not found)
C:\Users\guanting\Downloads\aa.pcapng (not found)
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
區域連線* 9
區域連線* 8
vEthernet (WSL (Hyper-V firewall))
藍牙網路連線
Wi-Fi 2
VMware Network Adapter VMnet1
區域連線* 14
區域連線* 11
乙太網路
VPN - VPN Client
USBPcap1
Event Tracing for Windows (ETW) reader
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
You are running Wireshark 4.2.5 (v4.2.5-0-g4aa814ac25a1). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default

Capture

...using this filter: Enter a capture filter ...

乙太網路 2

區域連線* 10

區域連線* 9

區域連線* 8

vEthernet (WSL (Hyper-V firewall))

藍牙網路連線

Wi-Fi 2

VMware Network Adapter VMnet8

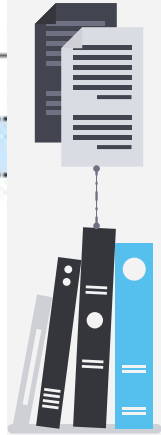
VMware Network Adapter VMnet1

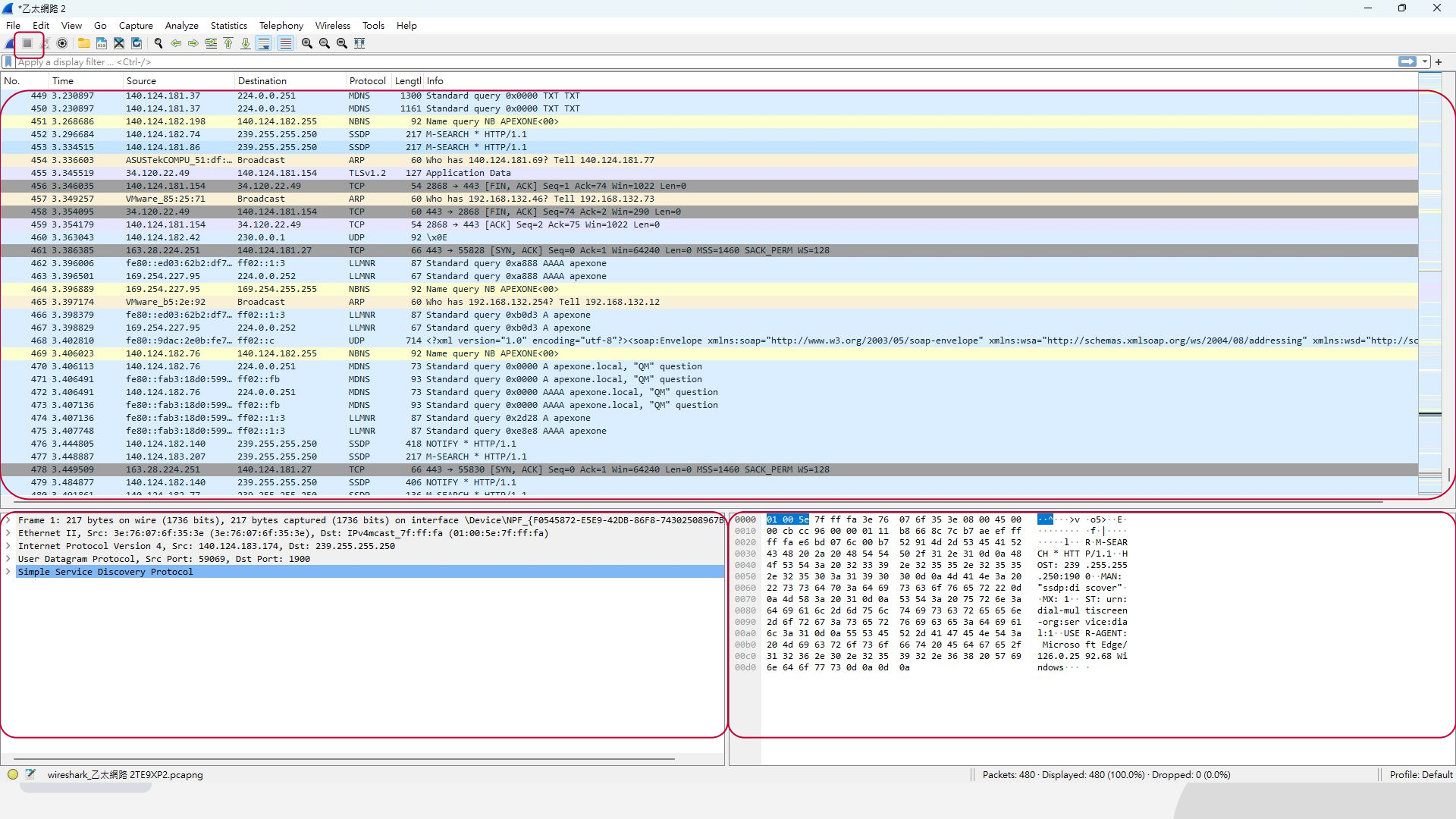
區域連線* 14

區域連線* 11

Adapter for loopback traffic capture

乙太網路

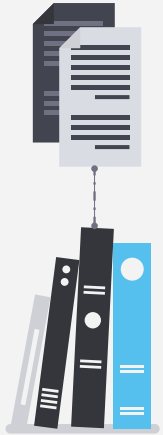



*乙太網路 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Lengtl Info
449 3.230897 140.124.181.37 224.0.0.251 MDNS 1300 Standard query 0x0000 TXT TXT
450 3.230897 140.124.181.37 224.0.0.251 MDNS 1161 Standard query 0x0000 TXT TXT
451 3.268686 140.124.182.198 140.124.182.255 NBNS 92 Name query NB APEXONE<00>
452 3.296684 140.124.182.74 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
453 3.334515 140.124.181.86 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
454 3.336603 ASUSTekCOMPU_51:df:... Broadcast ARP 60 Who has 140.124.181.69? Tell 140.124.181.77
455 3.345519 34.120.22.49 140.124.181.154 TLSv1.2 127 Application Data
456 3.346035 140.124.181.154 34.120.22.49 TCP 54 2868 → 443 [FIN, ACK] Seq=1 Ack=74 Win=1022 Len=0
457 3.349257 VMware_85:25:71 Broadcast ARP 60 Who has 192.168.132.46? Tell 192.168.132.73
458 3.354095 34.120.22.49 140.124.181.154 TCP 60 443 → 2868 [FIN, ACK] Seq=74 Ack=2 Win=290 Len=0
459 3.354179 140.124.181.154 34.120.22.49 TCP 54 2868 → 443 [ACK] Seq=2 Ack=75 Win=1022 Len=0
460 3.363043 140.124.182.42 230.0.0.1 UDP 92 \x0E
461 3.386385 163.28.224.251 140.124.181.27 TCP 66 443 → 55828 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
462 3.396006 fe80::ed03:62b2:df7... ff02::1:3 LLMNR 87 Standard query 0xa888 AAAA apexone
463 3.396501 169.254.227.95 224.0.0.252 LLMNR 67 Standard query 0xa888 AAAA apexone
464 3.396889 169.254.227.95 169.254.255.255 NBNS 92 Name query NB APEXONE<00>
465 3.397174 VMware_b5:2e:92 Broadcast ARP 60 Who has 192.168.132.254? Tell 192.168.132.12
466 3.398379 fe80::ed03:62b2:df7... ff02::1:3 LLMNR 87 Standard query 0xb0d3 A apexone
467 3.398829 169.254.227.95 224.0.0.252 LLMNR 67 Standard query 0xb0d3 A apexone
468 3.402810 fe80::9dac:2e0b:fe7... ff02::c UDP 714 <?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing" xmlns:wsd="http://sc
469 3.406023 140.124.182.76 140.124.182.255 NBNS 92 Name query NB APEXONE<00>
470 3.406113 140.124.182.76 224.0.0.251 MDNS 73 Standard query 0x0000 A apexone.local, "QM" question
471 3.406491 fe80::fab3:18d0:599... ff02::fb MDNS 93 Standard query 0x0000 A apexone.local, "QM" question
472 3.406491 140.124.182.76 224.0.0.251 MDNS 73 Standard query 0x0000 AAAA apexone.local, "QM" question
473 3.407136 fe80::fab3:18d0:599... ff02::fb MDNS 93 Standard query 0x0000 AAAA apexone.local, "QM" question
474 3.407136 fe80::fab3:18d0:599... ff02::1:3 LLMNR 87 Standard query 0x2d28 A apexone
475 3.407748 fe80::fab3:18d0:599... ff02::1:3 LLMNR 87 Standard query 0xe8e8 AAAA apexone
476 3.444805 140.124.182.140 239.255.255.250 SSDP 418 NOTIFY * HTTP/1.1
477 3.448887 140.124.183.207 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
478 3.449509 163.28.224.251 140.124.181.27 TCP 66 443 → 55830 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
479 3.484877 140.124.182.140 239.255.255.250 SSDP 406 NOTIFY * HTTP/1.1
Frame 1: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface \Device\NPF_{F0545872-E5E9-42DB-86F8-74302508967B}
Ethernet II, Src: 3e:76:07:6f:35:3e (3e:76:07:6f:35:3e), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 140.124.183.174, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 59069, Dst Port: 1900
Simple Service Discovery Protocol
0000 01 00 5e 7f ff fa 3e 76 07 6f 35 3e 08 00 45 00 ..^...>v .o5>..E.
0010 00 cb cc 96 00 00 01 11 b8 66 8c 7c b7 ae ef ff ....f.|....
0020 ff fa e6 bd 07 6c 00 b7 52 91 4d 2d 53 45 41 52 .....l.. R.M-SEAR
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HTT P/1.1..H
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 OST: 239 .255.255
0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20 .250:190 0..MAN:
0060 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d "ssdp:di scover".
0070 0a 4d 58 3a 20 31 0d 0a 53 54 3a 20 75 72 6e 3a .MX: 1.. ST: urn:
0080 64 69 61 6c 2d 6d 75 6c 74 69 73 63 72 65 65 6e dial-mul tiscreen
0090 2d 6f 72 67 3a 73 65 72 76 69 63 65 3a 64 69 61 -org:ser vice:dia
00a0 6c 3a 31 0d 0a 55 53 45 52 2d 41 47 45 4e 54 3a l:1..USE R-AGENT:
00b0 20 4d 69 63 72 6f 73 6f 66 74 20 45 64 67 65 2f Microso ft Edge/
00c0 31 32 36 2e 30 2e 32 35 39 32 2e 36 38 20 57 69 126.0.25 92.68 Wi
00d0 6e 64 6f 77 73 0d 0a 0d 0a ndows...
wireshark_乙太網路 2TE9XP2.pcapng
Packets: 480 · Displayed: 480 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

協定統計

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	480	100.0	91962	210 k	0	0	0	480
Ethernet	100.0	480	7.9	7272	16 k	0	0	0	480
Slow Protocols	0.8	4	0.0	4	9	0	0	0	4
Logical-Link Control	0.4	2	0.1	76	174	0	0	0	2
Spanning Tree Protocol	0.4	2	0.1	70	160	2	70	160	2
Internet Protocol Version 6	30.6	147	6.4	5880	13 k	0	0	0	147
User Datagram Protocol	30.2	145							
Multicast Domain Name System	16.9	81							
Link-local Multicast Name Resolution	11.9	57							
DHCPv6	0.6	3							
Internet Control Message Protocol v6	0.4	2							
Internet Protocol Version 4	62.9	302							
User Datagram Protocol	53.8	258							
Simple Service Discovery Protocol	11.9	57							
NetBIOS Name Service	6.7	32							
Multicast Domain Name System	19.8	95	15.3	14051	32 k	95	14051	32 k	95
Link-local Multicast Name Resolution	11.5	55	1.5	1371	3141	55	1371	3141	55
Dropbox LAN sync Discovery Protocol	0.4	2	0.3	268	613	2	268	613	2
Domain Name System	0.6	3	0.6	568	1301	3	568	1301	3
Data	2.9	14	3.6	3283	7521	14	3283	7521	14
Transmission Control Protocol	9.2	44	22.1	20358	46 k	33	799	1830	44
Transport Layer Security	2.3	11	21.0	19339	44 k	11	19339	44 k	11
Data	1.9	9	3.1	2892	6625	9	2892	6625	9
Address Resolution Protocol	5.0	24	1.2	1104	2529	24	1104	2529	24

查看某條流量



```
.2     93 Application Data
.2     89 Application Data
.2     93 Application Data
.2    127 Application Data
.2    119 Application Data
.2   1898 Application Data
.2    119 Application Data
.2   1898 Application Data
.2    112 Application Data
.2     94 Application Data
.2     93 Application Data
.2    102 Application Data
.2    413 Application Data
.2     89 Application Data
.2    102 Application Data
.2    410 Application Data
.2     93 Application Data
.2    106 Application Data
.2     94 Application Data
```

Mark/Unmark Packet(s) Ctrl+M
Ignore/Unignore Packet(s) Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comments ▸

Edit Resolved Name

Apply as Filter ▸
Prepare as Filter ▸
Conversation Filter ▸
Colorize Conversation ▸
SCTP ▸
Follow ▸
Copy ▸

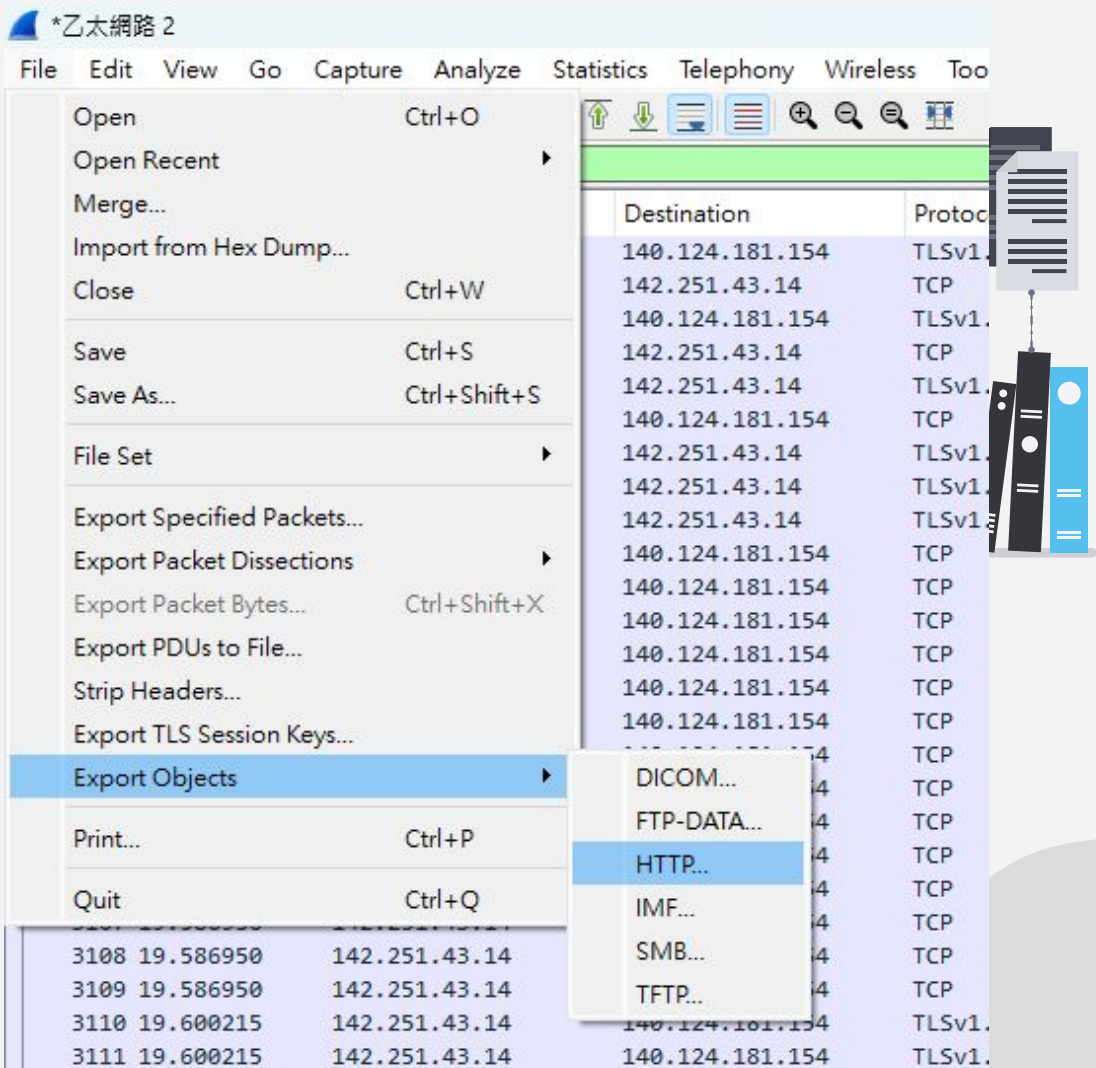
Protocol Preferences ▸
Decode As...
Show Packet in New Window

TCP Stream Ctrl+Alt+Shift+T
TLS Stream Ctrl+Alt+Shift+S

```
) on interface \Device\NPF_{F054
sco_ba:a5:3f (6c:41:6a:ba:a5:3f)
4
28566, Ack: 7779, Len: 39
```

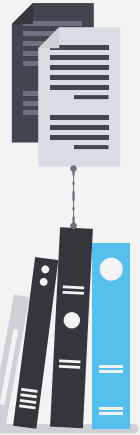
```
41 6a ba a5 3f 50 eb  f6 51 d5 91 08
4f 46 be 40 00 80 06  00 00 8c 7c b5
0e 07 df 01 bb 5e 8a  70 a6 eb 96 3f
01 fc 61 00 00 17 03  03 00 22 f0 4d
7d 22 eb f7 ae ef 60  fb 88 ae 86 09
```

匯出物件


*乙太網路 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Too
Open Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Ctrl+Shift+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Packet Bytes... Ctrl+Shift+X
Export PDUs to File...
Strip Headers...
Export TLS Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q
DICOM...
FTP-DATA...
HTTP...
IMF...
SMB...
TFTP...
Destination
140.124.181.154
142.251.43.14
3108 19.586950 142.251.43.14
3109 19.586950 142.251.43.14
3110 19.600215 142.251.43.14
3111 19.600215 142.251.43.14 140.124.181.154

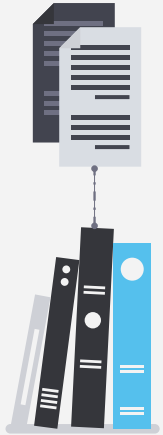
filter

Operators		Logic	
eq or **==**		**and** or **&&**	Logical AND
ne or **!=**		**or** or **||**	Logical OR
gt or **>**		**xor** or **^^**	Logical XOR
lt or **<**		**not** or **!**	Logical NOT
ge or **>=**		**[n] […]**	Substring operator
le or **<=**			



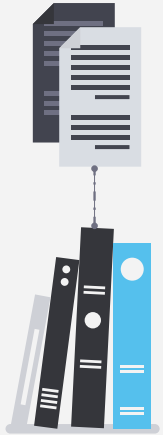
filter

IPv4	
ip.addr	ip.fragment.overlap.conflict
ip.checksum	ip.fragment.toolongfragment
ip.checksum_bad	ip.fragments
ip.checksum_good	ip.hdr_len
ip.dsfield	ip.host
ip.dsfield.ce	ip.id
ip.dsfield.dscp	ip.len
ip.dsfield.ect	ip.proto
ip.dst	ip.reassembled_in
ip.dst_host	ip.src
ip.flags	ip.src_host
ip.flags.df	ip.tos
ip.flags.mf	ip.tos.cost
ip.flags.rb	ip.tos.delay
ip.frag_offset	ip.tos.precedence
ip.fragment	ip.tos.reliability
ip.fragment.error	ip.tos.throughput
ip.fragment.multipletails	ip.ttl
ip.fragment.overlap	ip.version

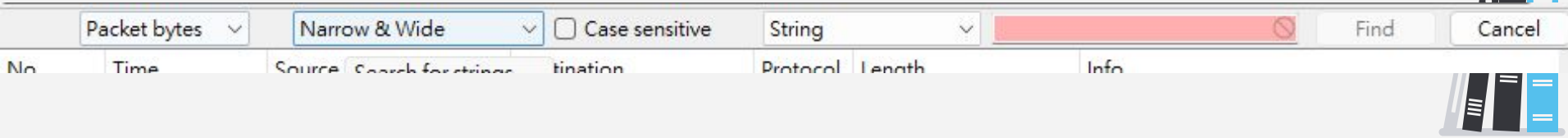


filter

HTTP	
http.accept	http.proxy_authorization
http.accept_encoding	http.proxy_connect_host
http.accept_language	http.proxy_connect_port
http.authbasic	http.referer
http.authorization	http.request
http.cache_control	http.request.method
http.connection	http.request.uri
http.content_encoding	http.request.version
http.content_length	http.response
http.content_type	http.response.code
http.cookie	http.server
http.date	http.set_cookie
http.host	http.transfer_encoding
http.last_modified	http.user_agent
http.location	http.www_authenticate
http.notification	http.x_forwarded_for
http.proxy_authenticate	



封包搜尋

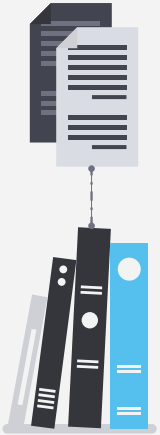

Packet bytes
Narrow & Wide
Case sensitive
String
Find
Cancel
No
Time
Source
Protocol
Length
Info

隱寫術 (Steganography)

一門關於資訊隱藏的技巧與科學，所謂資訊隱藏指的是不讓除預期的接收者之外的任何人知曉資訊的傳遞事件或者資訊的內容。
隱寫術跟密碼學有幾分相似，皆可以用來保護訊息，差異在隱寫術是將原先的資訊隱藏起來，並不像密碼學會將資訊轉化成另一種格式。

現代隱寫術

- 圖片
- 文件
- 影片
- 聲音
- 資料夾



當年的加州州長阿諾史瓦辛格回覆加州議會的信函

圖 1：當年的加州州長阿諾史瓦辛格回覆加州議會的信函，解釋為何他在某議員於演講中羞辱他之後否決了議會的一項決議。其實這是一篇藏頭文，只要將正文的每一行第一個字圈出來就會看到隱藏的訊息：I Fuck You.

經濟間諜案

美國司法部在公告中表示，鄭2008至2018年間在通用電力公司工作，案件在2022年3月結束審訊，鄭某和中國的其他人密謀竊取通用電氣地面和航空渦輪機技術的商業秘密，「知道或打算讓這些技術使中國和一個或多個外國機構受益，包括研究、開發和製造渦輪機部件的中國公司和大學。」

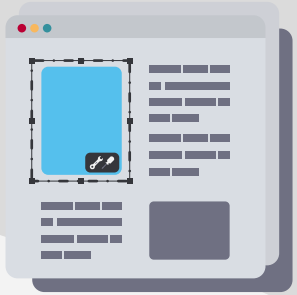
公告還引述美國司法部國家安全司助理司法部長馬修・奧爾森（Matthew G. Olsen）說：「這是一個典型的堪稱教科書式的經濟間諜案。鄭利用公司對他的信任，背叛了僱主，與中國政府合謀竊取美國的創新技術。」

根據美國司法部的起訴書，身為美國公民的鄭孝清將從其僱主那裏偷來的機密文件藏在一張落日美景數位照片的二進制代碼中，將其郵寄給自己。

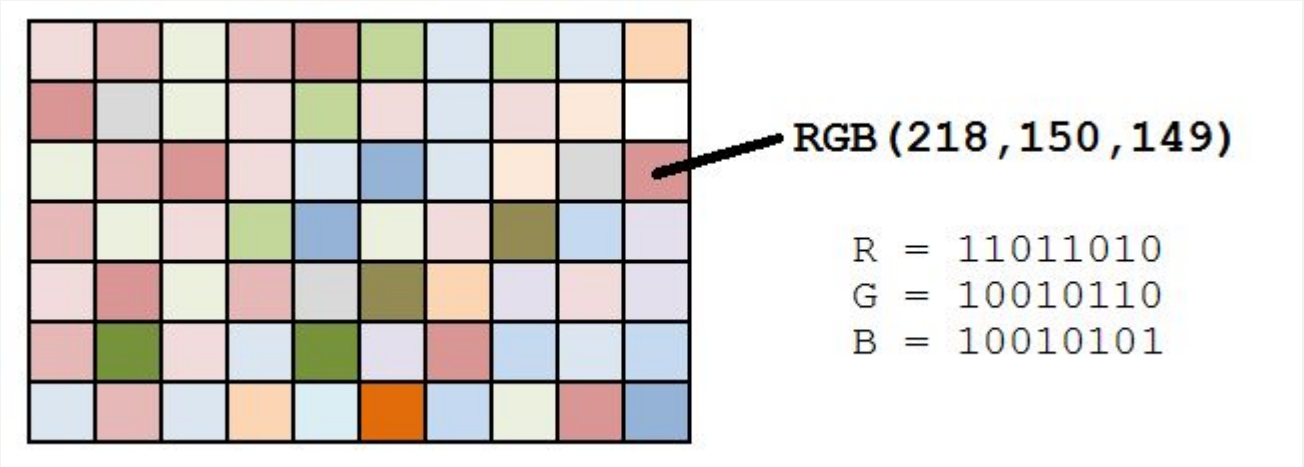
這是一種圖像隱碼術，將數據文件隱藏在另一個數據文件的代碼中。鄭曾經多次利用這種技術從通用電氣公司獲取敏感文件。

通用電氣是一家跨國企業集團，以其在醫療保健、能源和航空航天領域的工作而聞名於世，生產從冰箱到飛機引擎的各種產品。

鄭某竊取的信息與燃氣和蒸汽渦輪機的設計和製造有關，包括渦輪機葉片和渦輪機密封件。這些被認為價值數百萬美元的信息，被發送給他在中國的同伙，最終受益的是中國政府以及設在中國的公司和大學。



LSB



some tools

steg-toolkit
aperisolve