NSPA/NTPA

手機網路封包分析-基礎篇

作者: 劉得民 Te-Min Liu (Diamond Liu)

NTPA 中華民國 網路封包分析協會

手機網路封包分析-基礎篇

01 錄製手機網路封包的方式

介紹 On Host, On Cell, On Air, On Line, 與 Middle Man等等方式。

02 解析手機通訊的目標資訊

網際網路IP位址的配發，有相關的資料可以查詢。特別是錄製分析手機與內部網路的異常正常通訊活動，需要迅速解析IP位址資訊。

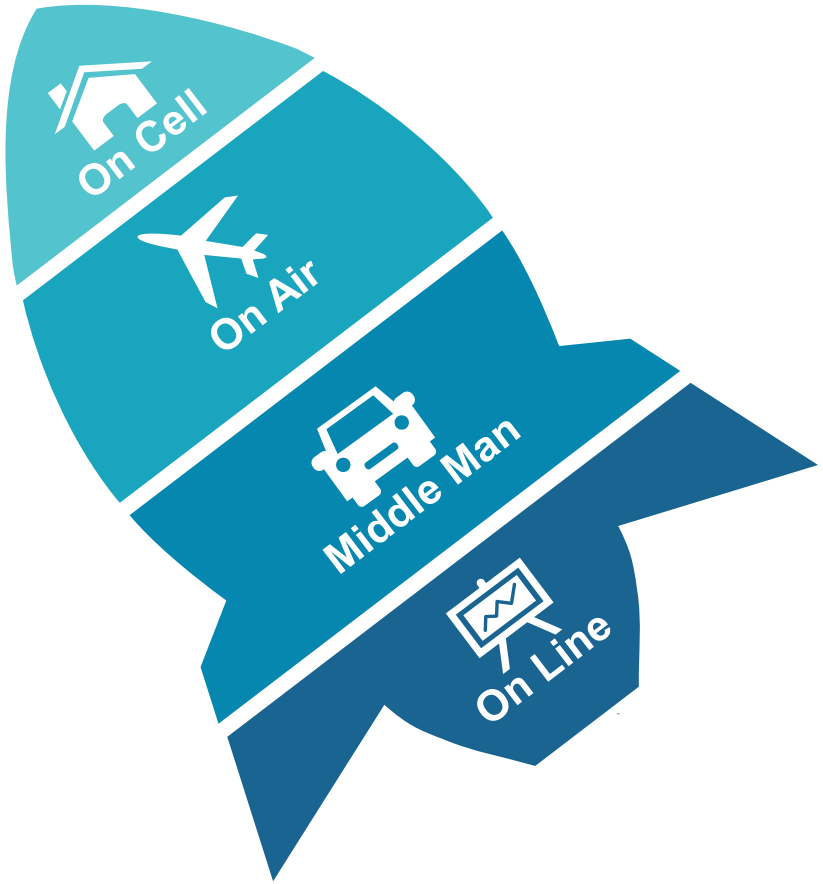
03 常見正常手機的網路通訊

各種典型網路封包行為，包括正常瀏覽網站、遊戲程式、電子郵件等等通訊，也可以發現惡意程式或是異常通訊的封包活動。

04 實作與結論

結合理論與實際操作的網路封包分析，並且討論進一步的學習。

錄製手機網路封包的方式



4G/5G 通訊封包 On Cell 擷取方式

透過特殊設備，在GSM通訊中，從4G/5G訊號，解譯TCP/IP網路封包。

WIFI 無線封包 On Air 擷取方式

在 802.11各類通訊電波，使用特殊設備，擷取 WEP/WPA 通訊內容。

WIFI 無線封包 Middle Man 擷取方式

在Windows/Linux系統設定『行動熱點』，
採用Wifi繞接Ethernet的方式，擷取TCP/IP網路封包。

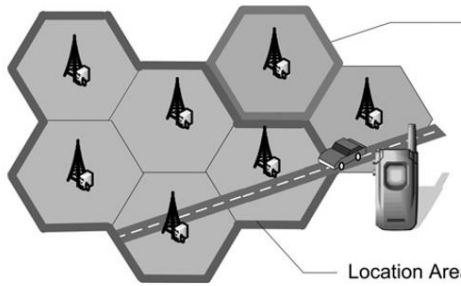
WIFI 無線封包 On Line 擷取方式

在網路交換器(Switch)設備，設定Port Mirror或是Y-TAP方式，
從Ethernet擷取TCP/IP網路封包。

手機 On Host 擷取方式

錄製手機網路封包的方式

On GSM Cell



ISP局端設備的擷取成本很高，一般系統無法執行。
另外有GSM-SIM Card的解密問題需要克服。

On WIFI Air

使用 AirPCAP 的 USB設備，直接擷取 WEP/WPA的802.11封包。只有 802.11a/b是明碼傳送封包，可以直接解譯。而802.11g/n則是需要特殊解密過程, 稱為 WEP Crack 或是 WPA Crack。

On Switch Line

接收各個802.11的頻段，並且在網路 Switch 設備擷取網路封包。通常需要設定Port Mirror功能，或是採用VLAN複製封包方式。

Middle Man

設定行動熱點後，關閉手機GSM功能，並且開啟WIFI通訊，連接前述行動熱點，可以跡近無成本。

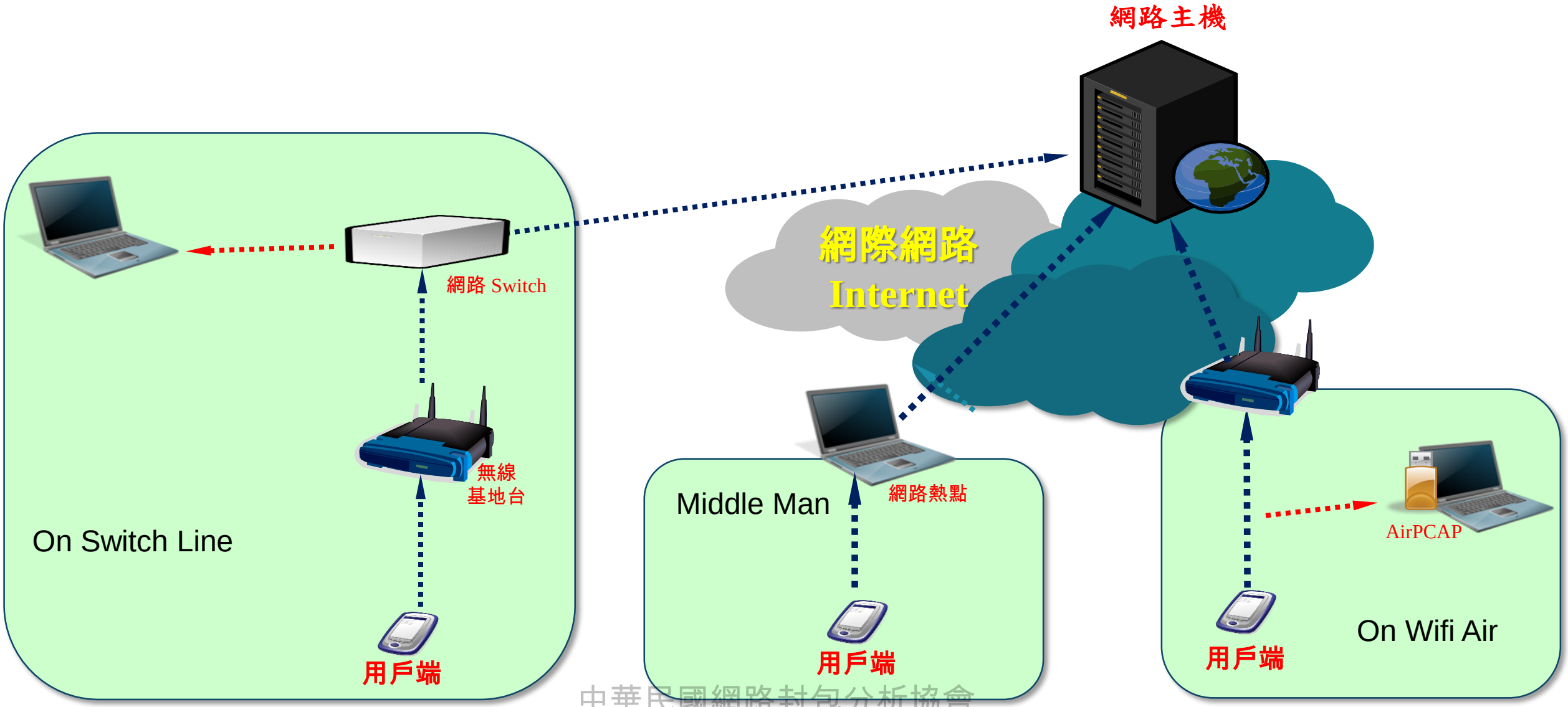
On Device Host

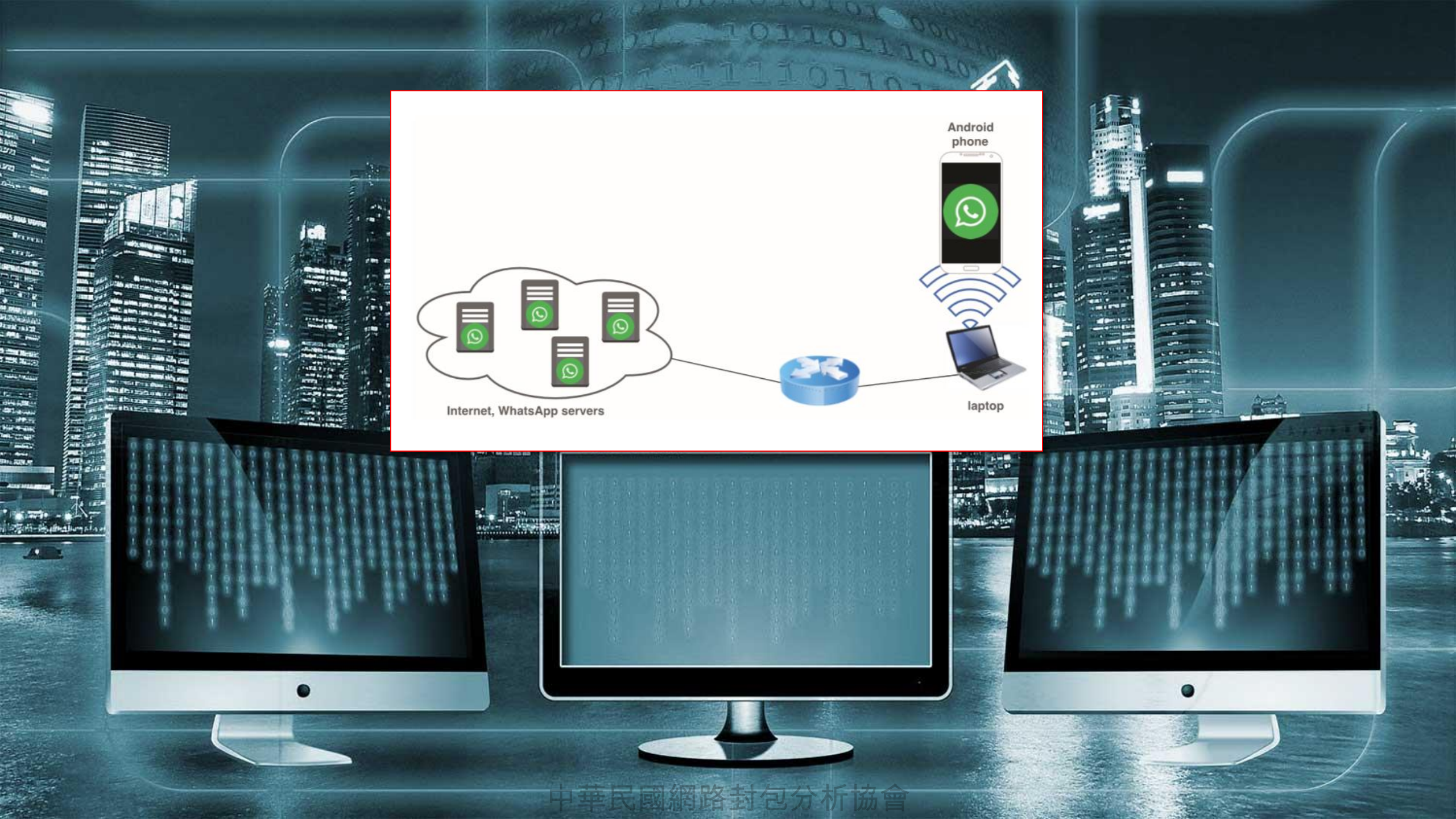
在智慧手機安裝錄製封包的App軟體，可以擷取許多特殊網路封包括TLS加密封包與VPN封包。

Other Approach

除了前述5種方式外，其他擷取網路封包方式，較為罕見，需要特別研究。

常用錄製手機網路封包的方式





錄製手機網路封包 - 行動熱點

01

準備Laptop筆電, 要連接 Ethernet

這部筆電要同時使用無線與有線的網路通訊，透過類似轉送封包的方式，完成 Middle Man 機制。

設定 Laptop 無線網路的『行動熱點』

在Windows7以上，可以設定『行動熱點』，並且將無線網路封包轉換到Ethernet有線網路。

02

03

啟動Wireshark，指定適當網路卡，擷取封包

這是一個重要而關鍵的動作，在此(Laptop行動熱點)的情況下，Wireshark的網路卡清單，會多一個網路項目，要選擇這個新的網路項目，而不能選擇原本的Wifi網路項目。

手機設定連接Laptop筆電的行動熱點

將智慧手機的GSM功能關閉(取出SIM Card, 或是採用飛航模式，並開啟無線網路)將此行動設備的無線網路，重新設定為Laptop筆點的行動熱點名稱。

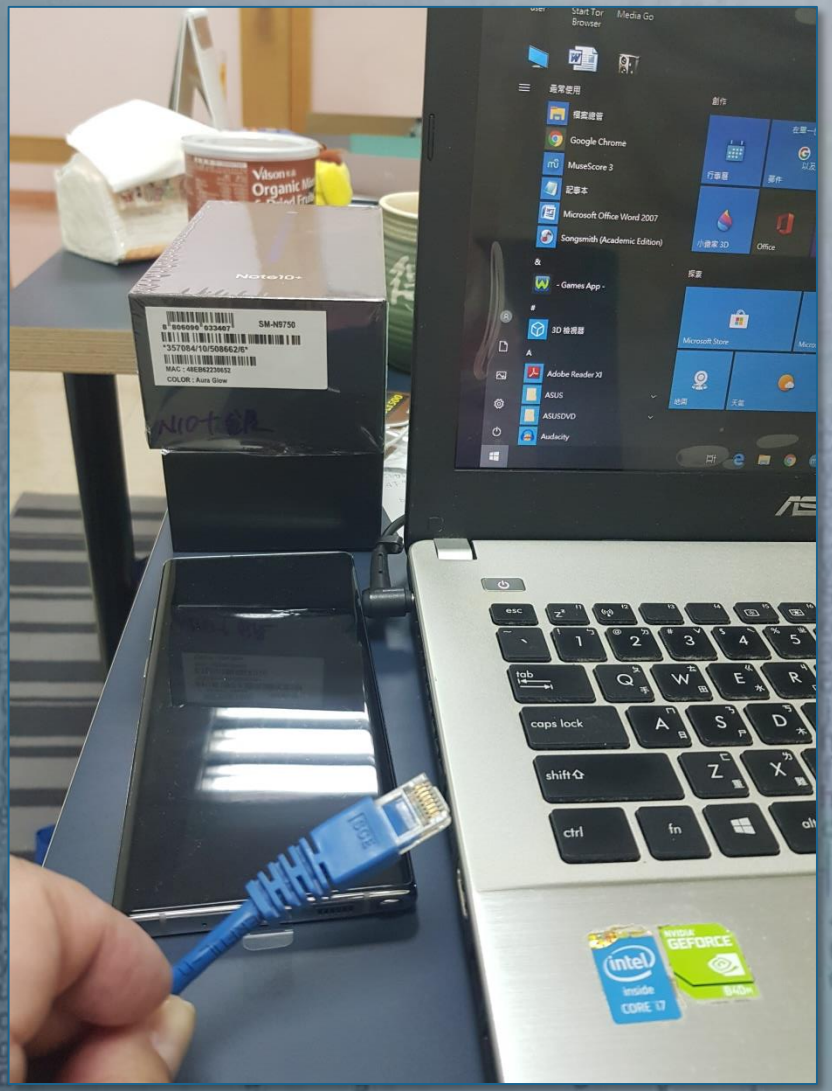
04

05

手機重新開機，在Laptop筆電檢視其網路活動

前述動作皆已完成後，將智慧手機重新啟動，強迫連接至Laptop筆電的行動熱點，並且觀察Wireshark的活動紀錄，藉此瞭解手機網路活動有無異常？

準備Laptop筆電，要連接 Ethernet



設定 Laptop 無線網路的『行動熱點』

設定 Laptop 無線網路的『行動熱點』

設定 Laptop 無線網路的『行動熱點』

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wire

Apply a display filter ··· <Ctrl-/>

No.	Time	Source

Wireshark · Capture Interfaces

Input Output Options

Interface	Traffic	Link-layer Header	Prom	Snapler	Buffer (I	Moni	Capture Filter
VirtualBox Host-Only Network		Ethernet	☑	default	2	—	
區域連線* 9		Ethernet	☑	default	2	—	
乙太網路		Ethernet	☑	default	2	—	
區域連線* 2		Ethernet	☑	default	2	☐	
Wi-Fi		Ethernet	☑	default	2	☐	
區域連線* 3		Ethernet	☑	default	2	☐	
區域連線* 10		Ethernet	☑	default	2	—	
區域連線* 11		Ethernet	☑	default	2	—	
Adapter for loopback traffic capture		BSD loopback	☑	default	2	—	

☑ Enable promiscuous mode on all interfaces

Manage Interfaces···

Capture filter for selected interfaces: Enter a capture filter ···

Compile BPFs

Start Close Help

啟動Wireshark
指定適當網路卡
擷取封包

Wireshark · Capture Interfaces

Input | Output | Options

Interface	Traffic	Link-layer Header	Prom	Snapler	Buffer (I	Moni	Capture Filter
VirtualBox Host-Only Network	_	Ethernet	☑	default	2	—	
區域連線* 9	_	Ethernet	☑	default	2	—	
乙太網路	_	Ethernet	☑	default	2	—	
區域連線* 2	_	Ethernet	☑	default	2	☐	
Wi-Fi	_	Ethernet	☑	default	2	☐	
區域連線* 3	_	Ethernet	☑	default	2	☐	
區域連線* 10	_	Ethernet	☑	default	2	—	
區域連線* 11	_	Ethernet	☑	default	2	—	
Adapter for loopback traffic capture	_	BSD loopback	☑	default	2	—	

☑ Enable promiscuous mode on all interfaces — Manage Interfaces…

Capture filter for selected interfaces: Enter a capture filter … — Compile BPFs

Start | Close | Help

Capturing from 區域連線* 3

File Edit View Go Capture Analyze Statistics Telephony Wireless

Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info

啟動Wireshark
指定適當網路卡
擷取封包

手機設定連接Laptop筆電的行動熱點

手機設定連接Laptop筆電的行動熱點

手機重新開機，
在Laptop筆電檢視其網路活動

Capturing from 區域連線* 3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ··· <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	2020-06-09 18:03:39.562082	::	ff02::1:ffa2:626d	ICMPv6	86	Neighbor Solicitation for fe80::28d8:9aff:fea2:626d
2	2020-06-09 18:03:39.577031	::	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
3	2020-06-09 18:03:39.735126	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x6fa7b4e5
4	2020-06-09 18:03:39.740642	192.168.137.1	192.168.137.252	DHCP	344	DHCP Offer - Transaction ID 0x6fa7b4e5
5	2020-06-09 18:03:39.783751	0.0.0.0	255.255.255.255	DHCP	356	DHCP Request - Transaction ID 0x6fa7b4e5
6	2020-06-09 18:03:39.788923	192.168.137.1	192.168.137.252	DHCP	344	DHCP ACK - Transaction ID 0x6fa7b4e5
7	2020-06-09 18:03:39.928540	::	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
8	2020-06-09 18:03:39.939857	2a:d8:9a:a2:62:6d	Broadcast	ARP	42	Who has 192.168.137.1? Tell 192.168.137.252
9	2020-06-09 18:03:39.939870	2a:ee:65:44:e0:15	2a:d8:9a:a2:62:6d	ARP	42	192.168.137.1 is at 2a:ee:65:44:e0:15
10	2020-06-09 18:03:39.946882	192.168.137.252	192.168.137.1	DNS	74	Standard query 0xef3b A www.google.com
11	2020-06-09 18:03:39.946882	192.168.137.252	192.168.137.1	DNS	89	Standard query 0xce30 A connectivitycheck.gstatic.com
12	2020-06-09 18:03:39.976860	2a:d8:9a:a2:62:6d	Broadcast	ARP	42	Who has 192.168.137.1? Tell 192.168.137.252
13	2020-06-09 18:03:39.976861	192.168.137.252	192.168.137.1	DNS	76	Standard query 0xa46f A time.android.com
14	2020-06-09 18:03:39.976873	2a:ee:65:44:e0:15	2a:d8:9a:a2:62:6d	ARP	42	192.168.137.1 is at 2a:ee:65:44:e0:15
15	2020-06-09 18:03:39.986333	192.168.137.1	192.168.137.252	DNS	90	Standard query response 0xef3b A www.google.com A 216.58.
16	2020-06-09 18:03:39.993352	192.168.137.1	192.168.137.252	DNS	105	Standard query response 0xce30 A connectivitycheck.gstati
17	2020-06-09 18:03:40.000934	192.168.137.1	192.168.137.252	DNS	140	Standard query response 0xa46f A time.android.com A 216.2
18	2020-06-09 18:03:40.017885	192.168.137.252	216.239.35.8	NTP	90	NTP Version 3, client
19	2020-06-09 18:03:40.017885	192.168.137.252	192.168.137.1	DNS	76	Standard query 0x43ce A mtalk.google.com
20	2020-06-09 18:03:40.035454	192.168.137.252	216.58.200.35	TCP	74	36976 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
21	2020-06-09 18:03:40.042440	192.168.137.252	216.58.200.36	TCP	74	60114 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PER
22	2020-06-09 18:03:40.047370	192.168.137.1	192.168.137.252	DNS	121	Standard query response 0x43ce A mtalk.google.com CNAME m
23	2020-06-09 18:03:40.050889	216.239.35.8	192.168.137.252	NTP	90	NTP Version 3, server
24	2020-06-09 18:03:40.057254	192.168.137.252	192.168.137.1	DNS	82	Standard query 0x5aa4 A eu-segd-api.secb2b.com
25	2020-06-09 18:03:40.057255	192.168.137.252	216.58.200.35	TCP	74	49781 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
26	2020-06-09 18:03:40.057284	192.168.137.1	192.168.137.252	ICMP	102	Time-to-live exceeded (Time to live exceeded in transit)
27	2020-06-09 18:03:40.061356	216.58.200.35	192.168.137.252	TCP	74	80 → 36976 [SYN, ACK] Seq=0 Ack=1 Win=60192 Len=0 MSS=138
28	2020-06-09 18:03:40.061642	216.58.200.36	192.168.137.252	TCP	74	443 → 60114 [SYN, ACK] Seq=0 Ack=1 Win=60192 Len=0 MSS=13
29	2020-06-09 18:03:40.061880	192.168.137.252	192.168.137.1	DNS	86	Standard query 0x9058 A android.clients.google.com

Section Break

實作練習與休息

解析手機通訊的目標資訊

Wifi 行動熱點

使用Wireshark, Tshark, Tcpdump, Windump
等等工具，擷取智慧手機的網路通訊封包。

智慧型手機

手機的OS, App對外通訊的網路活動

網際網路服務

- 網路服務
- 目標 IP 位址
- IP位址的國家與機構
- 不同通訊模式
- 不同通訊內容

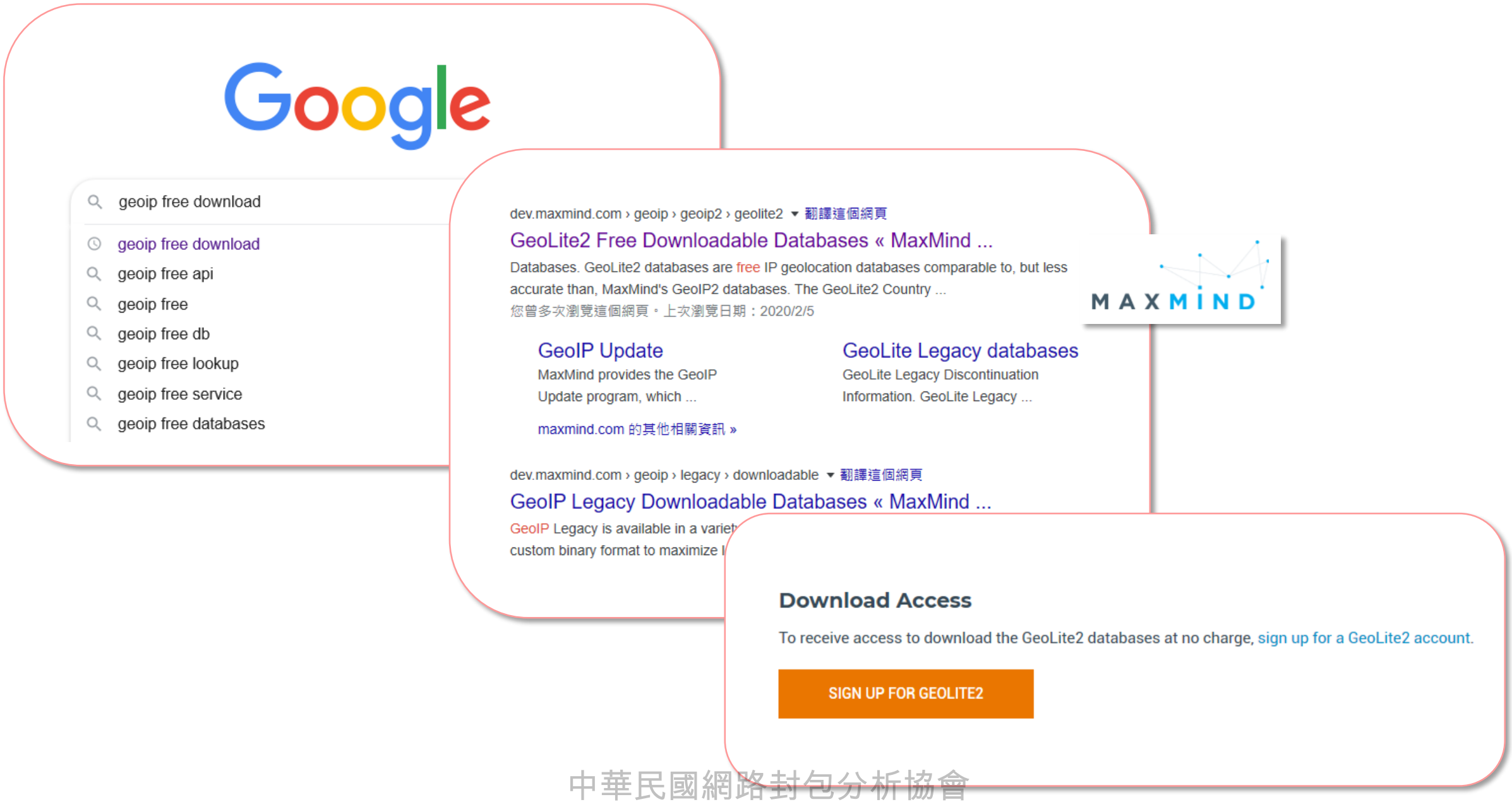
解析手機通訊的目標資訊

重新開始錄製網路封包

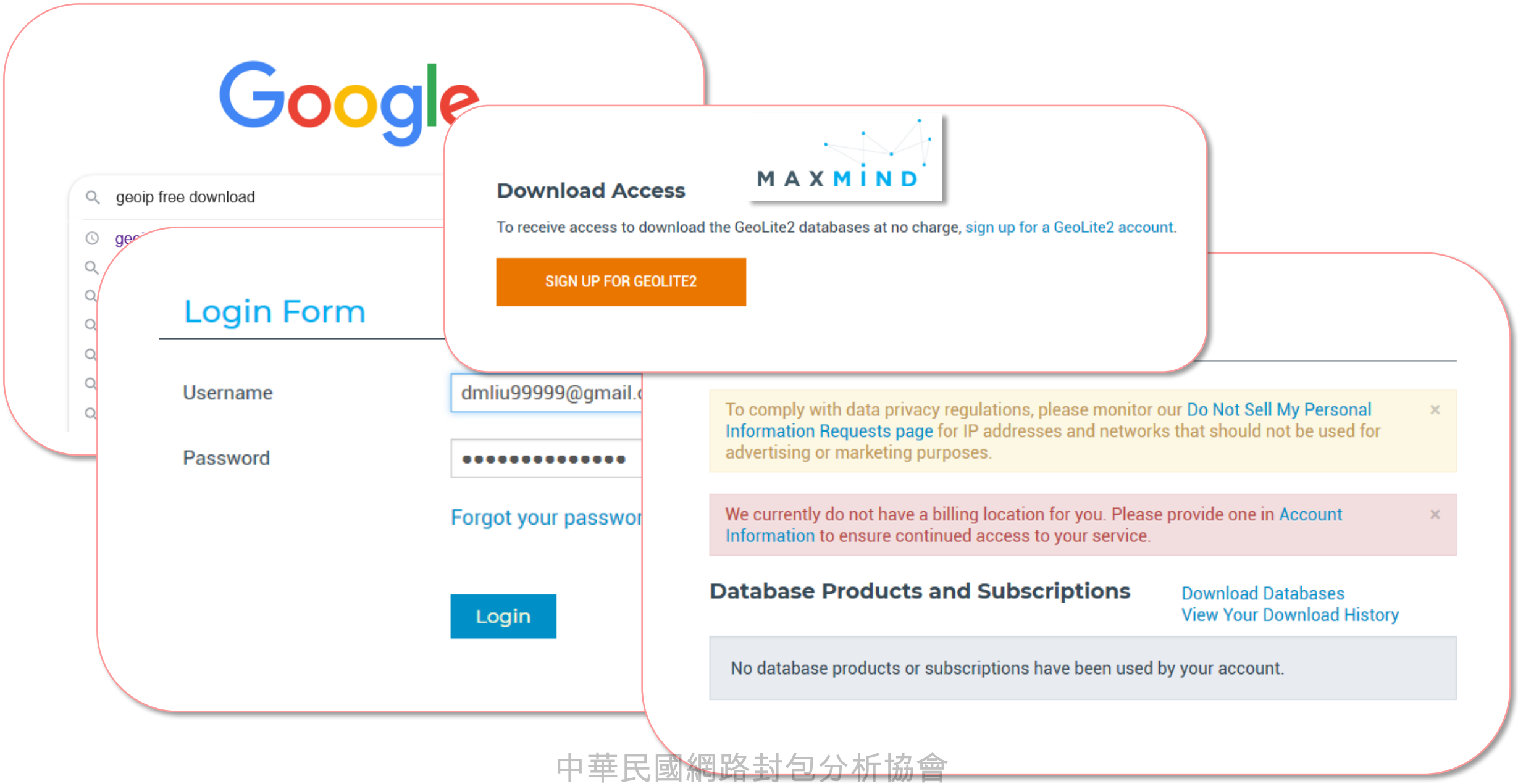
我們為了確定Wireshark 在電腦錄製正確的網路封包，
可以透過先前的DOS介面，輸入PING 168.95.1.1

如果網路有接通，則Wireshark應該會錄製到自己電腦與168.95.1.1的ICMP封包。

(1) 第一步，尋找並下載 GEOIP 資料庫



(1) 第一步，尋找並下載 GEOIP 資料庫



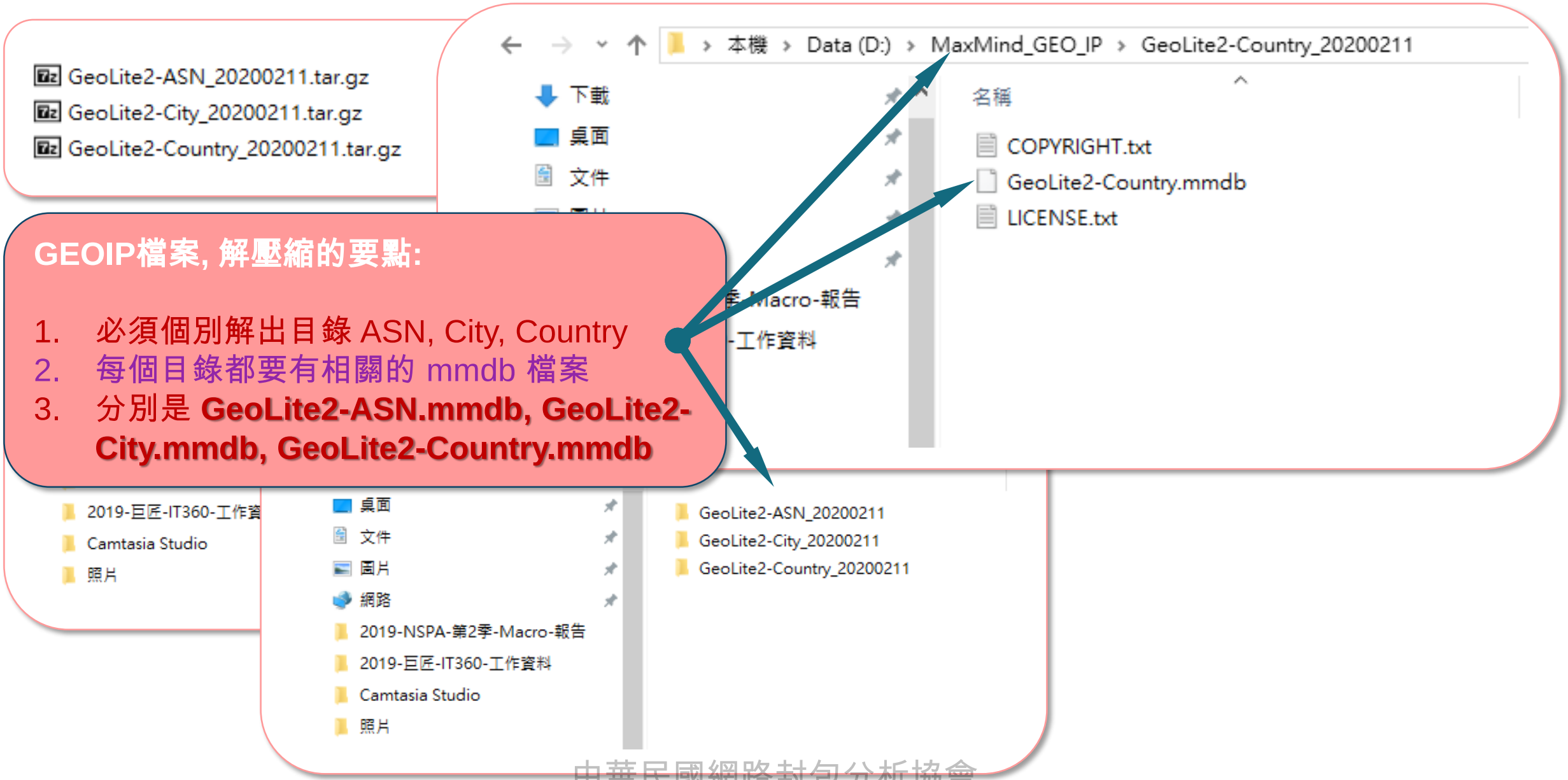
(1) 第一步，尋找並下載 GEOIP 資料庫

GEOIP檔案, 下載的三大要點:

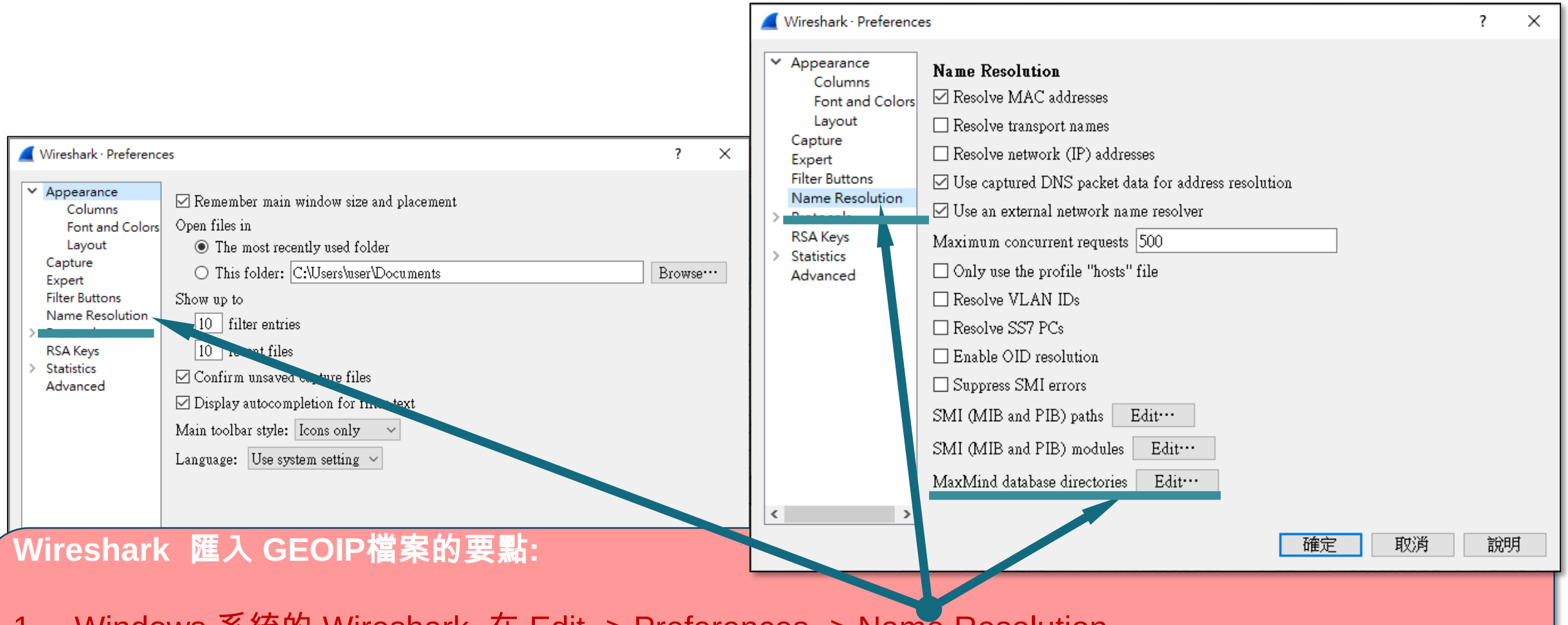
1. 下載格式 Format -> **GeoIP2 Binary** 格式
2. 下載檔案 Download -> **GZIP** 檔案
3. 分別下載 **GeoLite2-ASN, GeoLite2-City, GeoLite2-Country**

		Format	Date Updated	Download
		GeoIP2 Binary (APIs)	2020-02-11	GZIP (MD5)
GeoLite2-ASN-CSV	GeoLite2 ASN: CSV Format	GeoIP2 CSV (docs)	2020-02-11	ZIP (MD5)
GeoLite2-City	GeoLite2 City	GeoIP2 Binary (APIs)	2020-02-11	GZIP (MD5)
GeoLite2-City-CSV	GeoLite2 City: CSV Format	GeoIP2 CSV (docs)	2020-02-11	ZIP (MD5)
GeoLite2-Country	GeoLite2 Country	GeoIP2 Binary (APIs)	2020-02-11	GZIP (MD5)
GeoLite2-Country-CSV	GeoLite2 Country: CSV Format	GeoIP2 CSV (docs)	2020-02-11	ZIP (MD5)

(2) 第二步，建立新目錄，解壓縮 GEOIP 資料庫檔案



(3) 第三步，設定 Wireshark 匯入 GEOIP 資料檔案

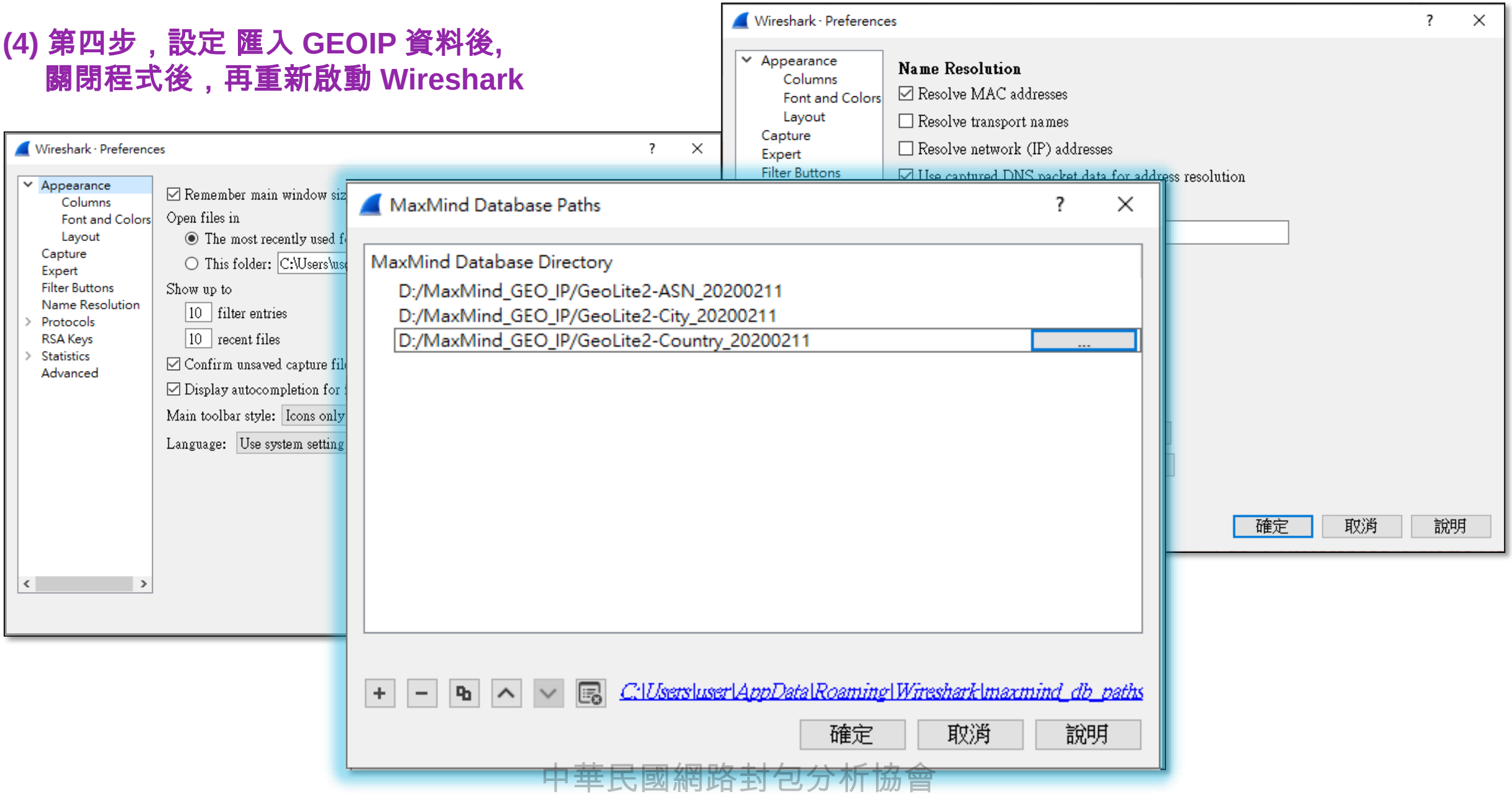


Wireshark 匯入 GEOIP檔案的要點:

1. Windows 系統的 Wireshark, 在 Edit -> Preferences -> Name Resolution
2. 在對話視窗的 右下角, 有 MaxMind Database 的 Edit 按鍵
3. 在新出現的對話視窗, 分別加入 **GeoLite2-ASN, GeoLite2-City, GeoLite2-Country 目錄**
4. MaxOS 系統的 Wireshark, 在 Wireshark -> Preferences -> Name Resolution (其餘步驟，與 2, 3 相同)

(3) 第三步，設定 Wireshark 匯入 GEOIP 資料檔案

(4) 第四步，設定 匯入 GEOIP 資料後，
關閉程式後，再重新啟動 Wireshark



錄製Hinet的網路封包

請使用 PING 指令，測試 168.95.1.1 的網路連線，同時錄製其網路封包。

亦即 PING 168.95.1.1

錄製Google的網路封包

請使用 PING 指令，測試 www.google.com 的網路連線，同時錄製其網路封包。

亦即 PING www.google.com

錄製微軟的網路封包

請使用 PING 指令，測試 www.microsoft.com 的網路連線，同時錄製其網路封包。

亦即 PING www.microsoft.com

實作題目 (範例操作)

擷取過濾與顯示過濾的使用方式

請同學練習錄製自己電腦本機封包，確定能夠錄製到對外網路通訊的封包。

Network Traffic Filters

Wireshark
有2種過濾條件

(1) 擷取過濾 Capture Filter
(2) 顯示過濾 Display Filter

如果沒有適當的封包擷取過濾條件(Capture Filter)，錄製網路封包的時候，會造成大量封包。在時效上，封包分析的工作可能會窒礙難行。另外一方面，若是封包顯示過濾條件(Display Filter) 設定不適當，則可能會造成封包篩選結果誤判，導致分析結論產生錯誤。

不論是哪種過濾條件，對分析人員來說，都必須瞭解這些過濾條件的作用與影響。

擷取過濾條件 (Capture Filter)

原則: 越寬鬆越好

一般來說，在資訊安全與鑑識的立場，如果不是關於APT攻擊、網路蠕蟲、電腦病毒、木馬程式的問題，通常只要忽略廣播封包(Broadcast)與 群播封包 (Multicast) 即可。

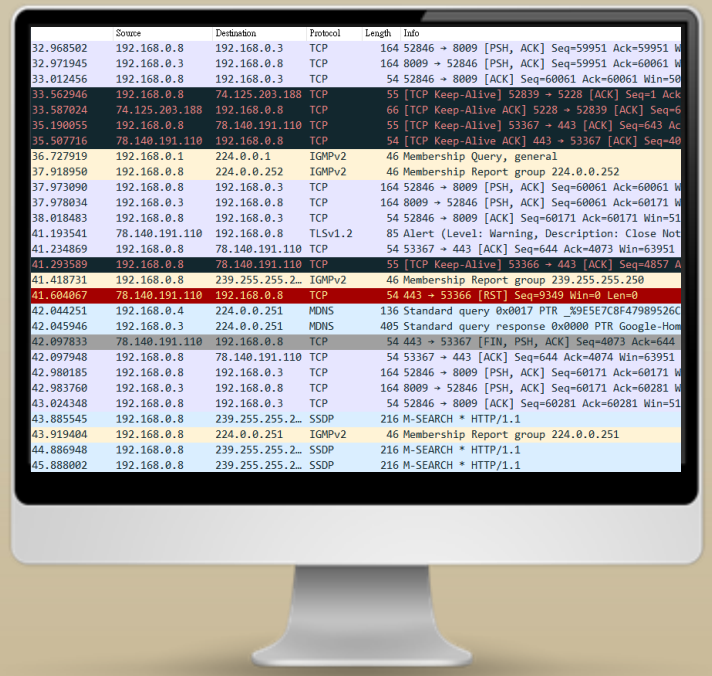
顯示過濾條件 (Display Filter)

原則: 越精確越好

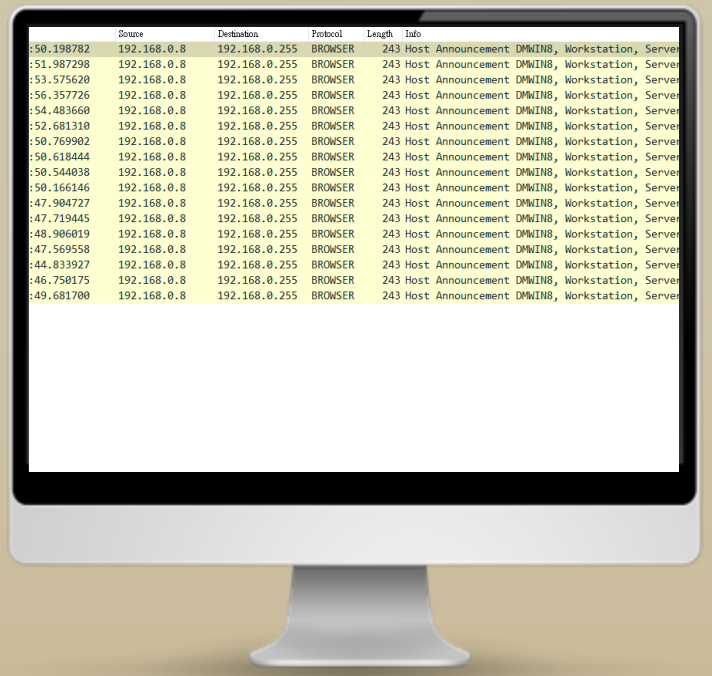
這個過濾設定，是在擷取網路封包後，進行個案分析的時候，郵分析人員輸入的封包過濾條件。依照案件特性與分析者的經驗，會有不同的顯示過濾條件。為了能有效找出網路安全問題，這個過濾條件，越精準越好。

善用過濾條件，加強分析效率

同時使用 Capture Filter 與 Display Filter



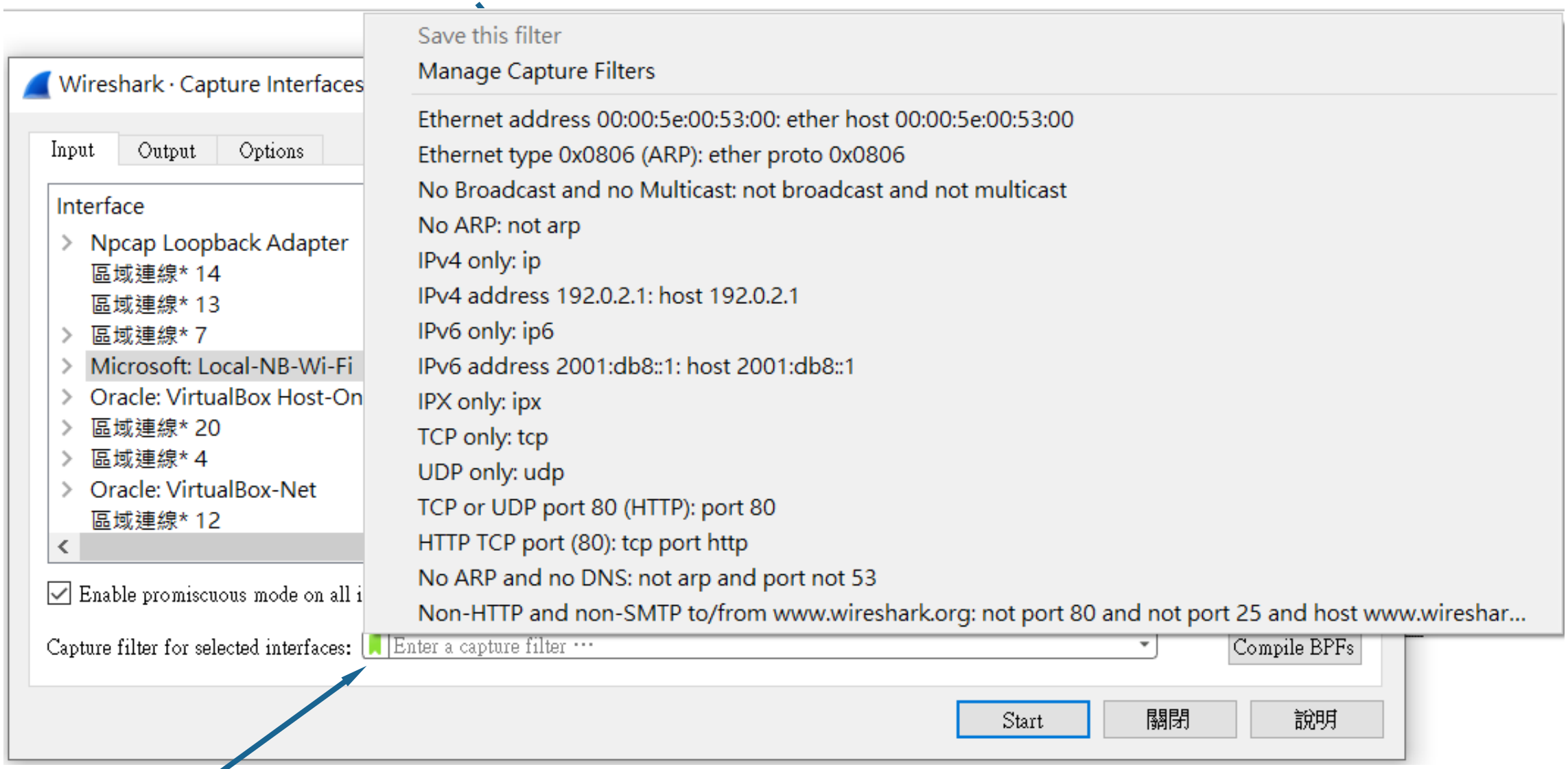
	Source	Destination	Protocol	Length	Info
32.968502	192.168.0.8	192.168.0.3	TCP	164	52846 → 8009 [PSH, ACK] Seq=59951 Ack=59951 W
32.971945	192.168.0.3	192.168.0.8	TCP	164	8009 → 52846 [PSH, ACK] Seq=59951 Ack=60061 W
33.012456	192.168.0.8	192.168.0.3	TCP	54	52846 → 8009 [ACK] Seq=60061 Ack=60061 Win=50
33.562946	192.168.0.8	74.125.203.188	TCP	55	[TCP Keep-Alive] 52839 → 5228 [ACK] Seq=1 Ack
33.587024	74.125.203.188	192.168.0.8	TCP	66	[TCP Keep-Alive ACK] 5228 → 52839 [ACK] Seq=6
35.190055	192.168.0.8	78.140.191.110	TCP	55	[TCP Keep-Alive] 53367 → 443 [ACK] Seq=643 Ac
35.507716	78.140.191.110	192.168.0.8	TCP	54	[TCP Keep-Alive ACK] 443 → 53367 [ACK] Seq=40
36.727919	192.168.0.1	224.0.0.1	IGMPv2	46	Membership Query, general
37.918950	192.168.0.8	224.0.0.252	IGMPv2	46	Membership Report group 224.0.0.252
37.973090	192.168.0.8	192.168.0.3	TCP	164	52846 → 8009 [PSH, ACK] Seq=60061 Ack=60061 W
37.978034	192.168.0.3	192.168.0.8	TCP	164	8009 → 52846 [PSH, ACK] Seq=60061 Ack=60171 W
38.018483	192.168.0.8	192.168.0.3	TCP	54	52846 → 8009 [ACK] Seq=60171 Ack=60171 Win=51
41.193541	78.140.191.110	192.168.0.8	TLSv1.2	85	Alert (Level: Warning, Description: Close Not
41.234869	192.168.0.8	78.140.191.110	TCP	54	53367 → 443 [ACK] Seq=644 Ack=4073 Win=63951
41.293589	192.168.0.8	78.140.191.110	TCP	55	[TCP Keep-Alive] 53366 → 443 [ACK] Seq=4857 A
41.418731	192.168.0.8	239.255.255.2…	IGMPv2	46	Membership Report group 239.255.255.250
41.604067	78.140.191.110	192.168.0.8	TCP	54	443 → 53366 [RST] Seq=9349 Win=0 Len=0
42.044251	192.168.0.4	224.0.0.251	MDNS	136	Standard query 0x0017 PTR _%9E5E7C8F47989526C
42.045946	192.168.0.3	224.0.0.251	MDNS	405	Standard query response 0x0000 PTR Google-Hom
42.097833	78.140.191.110	192.168.0.8	TCP	54	443 → 53367 [FIN, PSH, ACK] Seq=4073 Ack=644
42.097948	192.168.0.8	78.140.191.110	TCP	54	53367 → 443 [ACK] Seq=644 Ack=4074 Win=63951
42.980185	192.168.0.8	192.168.0.3	TCP	164	52846 → 8009 [PSH, ACK] Seq=60171 Ack=60171 W
42.983760	192.168.0.3	192.168.0.8	TCP	164	8009 → 52846 [PSH, ACK] Seq=60171 Ack=60281 W
43.024348	192.168.0.8	192.168.0.3	TCP	54	52846 → 8009 [ACK] Seq=60281 Ack=60281 Win=51
43.885545	192.168.0.8	239.255.255.2…	SSDP	216	M-SEARCH * HTTP/1.1
43.919404	192.168.0.8	224.0.0.251	IGMPv2	46	Membership Report group 224.0.0.251
44.886948	192.168.0.8	239.255.255.2…	SSDP	216	M-SEARCH * HTTP/1.1
45.888002	192.168.0.8	239.255.255.2…	SSDP	216	M-SEARCH * HTTP/1.1



	Source	Destination	Protocol	Length	Info
:50.198782	192.168.0.8	192.168.0.255	BROWSER	243	Host Announcement DMWIN8, Workstation, Server
:51.987298	192.168.0.8	192.168.0.255	BROWSER	243	Host Announcement DMWIN8, Workstation, Server
:53.575620	192.168.0.8	192.168.0.255	BROWSER	243	Host Announcement DMWIN8, Workstation, Server
:56.357726	192.168.0.8	192.168.0.255	BROWSER	243	Host Announcement DMWIN8, Workstation, Server
:54.483660	192.168.0.8	192.168.0.255	BROWSER	243	Host Announcement DMWIN8, Workstation, Server
:52.681310	192.168.0.8	192.168.0.255	BROWSER	243	Host Announcement DMWIN8, Workstation, Server
:50.769902	192.168.0.8	192.168.0.255	BROWSER	243	Host Announcement DMWIN8, Workstation, Server
:50.618444	192.168.0.8	192.168.0.255	BROWSER	243	Host Announcement DMWIN8, Workstation, Server
:50.544038	192.168.0.8	192.168.0.255	BROWSER	243	Host Announcement DMWIN8, Workstation, Server
:50.166146	192.168.0.8	192.168.0.255	BROWSER	243	Host Announcement DMWIN8, Workstation, Server
:47.904727	192.168.0.8	192.168.0.255	BROWSER	243	Host Announcement DMWIN8, Workstation, Server
:47.719445	192.168.0.8	192.168.0.255	BROWSER	243	Host Announcement DMWIN8, Workstation, Server
:48.906019	192.168.0.8	192.168.0.255	BROWSER	243	Host Announcement DMWIN8, Workstation, Server
:47.569558	192.168.0.8	192.168.0.255	BROWSER	243	Host Announcement DMWIN8, Workstation, Server
:44.833927	192.168.0.8	192.168.0.255	BROWSER	243	Host Announcement DMWIN8, Workstation, Server
:46.750175	192.168.0.8	192.168.0.255	BROWSER	243	Host Announcement DMWIN8, Workstation, Server
:49.681700	192.168.0.8	192.168.0.255	BROWSER	243	Host Announcement DMWIN8, Workstation, Server

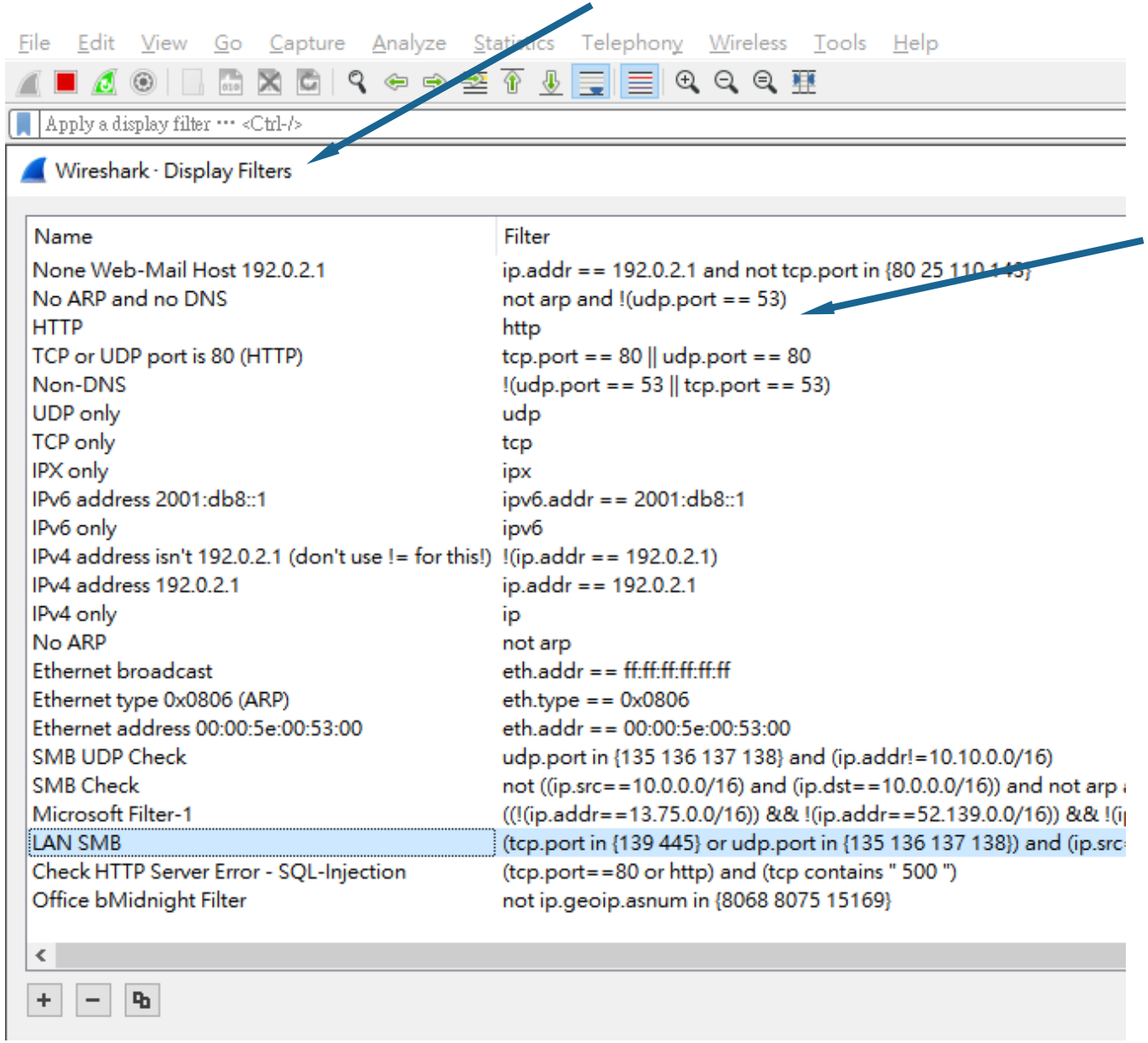
- Capture Filter 是用於 網路卡擷取網路封包的時候，就發生效用的過濾條件。要非常謹慎使用，以避免漏失網路封包。
- Display Filter 是用於 已經擷取後的網路封包，進行各種分析，用來找出影響資訊安全的網路封包。特別要注意的是，網路活動的互動行為，例如DNS與HTTPS的互動、網路芳鄰的連接互動、ARP與TCP的互動等等。不同的網路互動過程，就如同程式執行的網路行為一樣，可以看出許多異於正常的通訊行為，此為異常程式通訊行為分析的基本觀念。

在功能選單，選取 Capture 的 Options 項目，會出現這個對話視窗



擷取過濾條件 Capture Filter

在功能選單，選取 Analyze 的 Display Filters 項目，會出現這個對話視窗



顯示過濾條件 Display Filter

Display Filter 基本語法

- **欄位名稱 == 數值或字串**
- **欄位名稱 in {數值 數值 數值 “字串”}**
- **欄位名稱 contains “字串”**
- **欄位名稱 matches “正規表示字串”**

- 可以使用 and 或 or 或 not
- 可以使用 && 或 || 或 !
- 可以使用 (與)
- 可以使用 > 或 < 或是 >= 或 <=

Display Filter 常用欄位與範例

網路 IP 位址 欄位

- ip.addr
- ip.src
- ip.dst
- ipv6.addr

網路 通訊埠 欄位

- tcp.port
- tcp.srcport
- tcp.dstport

網路通訊協定 欄位

- arp
- dns
- http
- tls

網路封包內容

- tcp contains “字串”
- tcp matches “Perl 正規字串”
- tcp matches “(?i)s.e.l.e.c.t”

顯示過濾條件範例

01 **顯示特定 IP 位址的通訊**

ip.addr == xxx.xxx.xxx.xxx
ip.addr == xxx.xxx.0.0/16
Ip.src == xxx.xxx.0.0/16

02 **忽略特定 IP 位址的通訊**

ip.addr != xxx.xxx.xxx.xxx
not ip.addr == xxx.xxx.xxx.xxx

03 **顯示特定 TCP/UDP Port 通訊**

tcp.port == 80
http

04 **忽略特定 TCP/UDP Port 通訊**

tcp.port != 80
not tcp.port == 80
not http

顯示過濾條件範例

05 顯示多個 TCP/UDP Port 通訊

tcp.port in {80 443}
tcp.port in {80 8000 8080 10000}

06 顯示特定IP位址與特定Port通訊

Ip.addr== *C&C中繼站位址* and tcp.port in {80 443}
Ip.addr!=192.168.x.x/16 and tcp.port in {139 445}

07 觀察DNS與HTTP/HTTPS 互動

dns or http or tcp.port in {80 443} or tls
udp.port==53 or tcp.port in {80 8000 8080 10000}

08 觀察特定通訊的封包內容

(tcp contains “MZ” and tcp contains “PE”) and ftp
tcp contains “MZ” and (http or tcp.port in {80 8000})

顯示過濾條件範例

09 顯示特定 機構(公司) 通訊

ip.geoip.asnum==15169
ip.geoip.org==“GOOGLE“
ip.geoip.asnum in {8068 8075}

10 顯示特定 國家(城市) 通訊

ip.geoip.country=="Taiwan“
ip.geoip.city=="Tokyo"

11 顯示 TCP 通訊 連線或斷線

tcp.flags.syn==1
tcp.flags.syn==1 or tcp.flags.fin==1 or
tcp.flags.reset==1

12 網路芳鄰 異常連接到外網電腦

(smb or smb2) and (ip.addr!=10.10.0.0/16)
(tcp.port in {139 445}) and (ip.addr!=10.10.0.0/16)

(tcp.port in {139 445}) and (not ((ip.src==10.10.0.0/16) and (ip.dst==10.10.0.0/16)))

擷取過濾與顯示過濾的使用方式

設定 擷取過濾條件 Capture Filter

基本過濾條件是: 忽略廣播封包與群播封包
Capture Filter: not broadcast and not multicast

準備DOS程式介面，預備執行命令列

這個動作，是為方便執行 PING 指令，產生封包

開始錄製網路封包

記得, 要選擇正確 有線網路卡 或是 Wifi 無線卡

開啟網頁瀏覽器, 瀏覽特定網站

1.先在cmd.exe裡面，執行 PING 168.95.1.1
2.瀏覽 https://www.nspa-cert-tw.org/ 網站

輸入 顯示過濾條件 Display Filter

雖然我們不知道 目標網站的IP位址，但是,
因為先前的DOS介面，已經輸入PING 168.95.1.1
並且, 使用 HTTPS 瀏覽這個網站 www.nspa-cert-tw.org 所以顯示過濾條件可以設定為:

display filter: **icmp or dns or (tcp.port==443 and tcp.flags.syn==1)**

顯示連線微軟的網路封包

錄製 ping www.microsoft.com 封包，並且根據微軟的機構代碼(ORG ID) 為 8068與8075，設定顯示過濾條件，同時過濾(顯示)本機對微軟機構的通訊封包。

顯示ARP封包 (內網活動)

由於Ethernet網路卡對於網路資料的傳送，網卡位址(MAC Address)是做基本的資料，並且透過ARP封包行為可以取得這個網卡位址資料。

顯示非台灣的網路封包

請設定顯示過濾條件，將不是台灣的外網通訊，全部顯示出來。

特別注意，只要**對外部網路的通訊封包**，要忽略內部網路互傳的通訊封包。

實作題目 (範例操作)

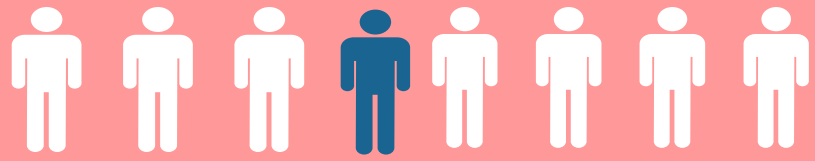
匯出網路通訊封包資料檔案

請同學預先練習錄製自己電腦本機封包，
確定能夠錄製到自己對外網路通訊的封包。

匯出網路通訊封包資料檔案

1. 原始封包數量龐大，內容複雜

一般來說，在企業內部網路錄製網路封包，通常網路封包數量會非常大，這些原始封包資料(Raw Data)同時包括各式各類通訊行為(下載、電郵、ERP等等)，因此要找出威脅網路安全的通訊封包，需要許多技巧，不然會徒勞無功。



Raw Data

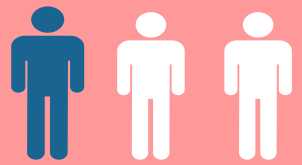
2. 針對網路資安問題，擷取過濾適當封包

透過擷取過濾條件(Capture Filter)與顯示過濾條件(Display Filter)的協助，我們可以去蕪存菁，找到異常通訊行為(不符合正常工作的通訊行為)

Filters

3. 過濾後的封包，尋找有無資安問題的段落

過濾後的網路封包，還需要各種判讀技巧(Skills)這些技巧，也就是異常網路封包的判讀經驗累積後，得到的判讀通則，並能引導我們尋找威脅網路安全的通訊封包段落。



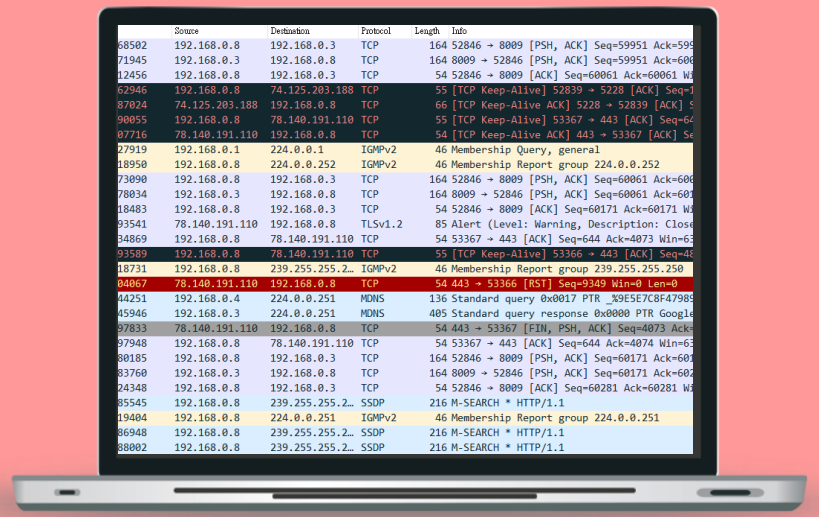
Skills

4. 將有資安問題的封包，匯出成為獨立檔案

我們將這些有問題的通訊段落，單獨儲存為網路封包檔案，也就是匯出為獨立的網路封包檔案，以利於後續報告整理與威脅研判的用途。

Export

匯出網路通訊封包資料檔案



不論那種封包工具，PCAP檔案格式，是所有作業系統的通用封包格式。

PCAP檔案格式，同時考慮作業系統 與 數值資料 的 Hi-Byte, Low-Byte問題，支援Unix, Windows, Linux, iOS等等系統，是一種網路封包的通用檔案格式。

封包數量與電腦機台數量、網路頻寬、網路行為量、錄製時間成正比

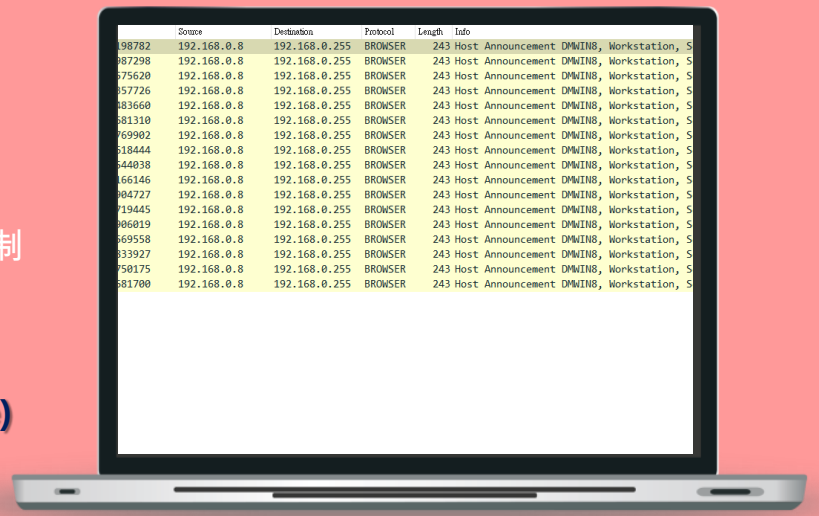
網路封包數量越多，越難以分析。原則上要降低網路封包數量，就需要控制這五個變數:

- **電腦數量 (Active Hosts Count)**
- **網路頻寬 (Bandwidth)**
- **行為複雜度 (Network Behavior)**
- **錄製時間 (Capture Time Range)**
- **擷取過濾條件 (Capture Filter)**

過濾分析，精確匯出資安問題封包

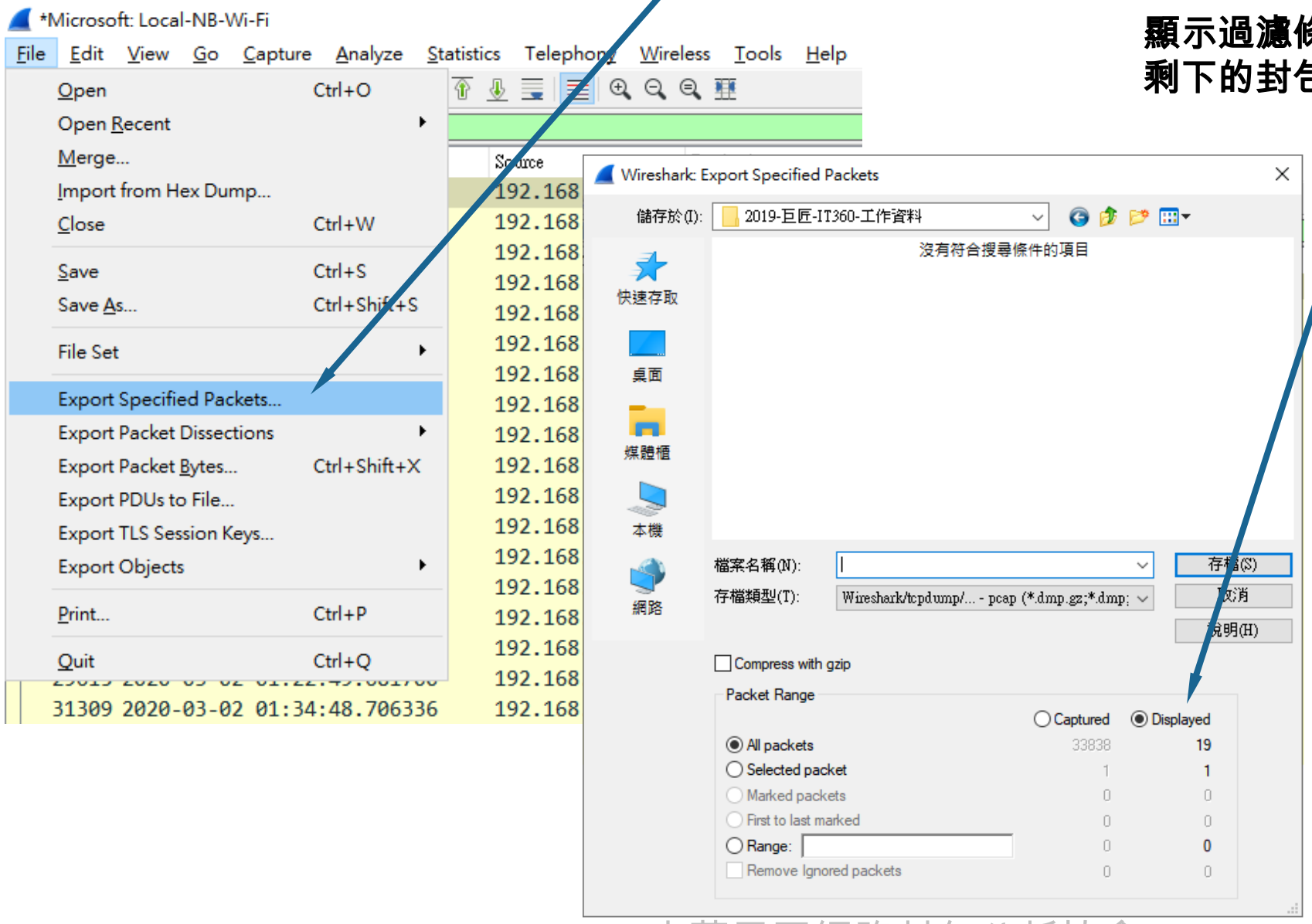
找出資安問題封包的方式，除了自動化機制之外，剩下的方式就是:

- **顯示過濾條件 (Display Filter)**
- **特定行為模式 (Network Behavior)**
- **豐富判讀經驗 (Skills and Experience)**



在功能選單，選取 File 的 Export Specified Packets 項目，會出現這個對話視窗

顯示過濾條件 Display Filter
剩下的封包數量



匯出網路通訊的封包資料檔案

準備錄製網路封包

先關閉所有通訊程式，包括遊戲程式、網頁瀏覽器、電郵程式、與任何已知通訊程式。

準備DOS程式介面，預備執行命令列

這個動作，是為方便執行 PING 指令，產生封包

在 Wireshark 選擇適當網路卡

應該是 有線網路卡 或是 Wifi 無線卡

設定顯示過濾條件

在顯示過濾條件(Display Filter) 設定 icmp 過濾條件

匯出特定(過濾後)網路封包檔案

我們為了確定Wireshark 在電腦錄製正確的網路封包，
可以透過先前的DOS介面，輸入PING 168.95.1.1

如果網路有接通，則Wireshark應該會錄製到自己電腦與168.95.1.1的ICMP封包。
接著，我們可以直接設定 顯示過濾條件(Display Filter) 不必停止錄封包，就可以顯示封包內容有ICMP的網路活動。停止網錄錄製後，便可以直接匯出過濾後的網錄封包。

匯出連線微軟的網路封包

錄製 ping www.microsoft.com 封包，並且根據微軟的機構代碼(ORG ID) 為 8068與8075，設定顯示過濾條件，同時過濾(顯示)本機對微軟機構的通訊封包。

匯出ARP封包 (內網活動)

長時間紀錄ARP封包行為，可以取得網卡位址資料。同時，也能夠取得，同一個Switch的網路設備清單，藉此可以瞭解內網設備。

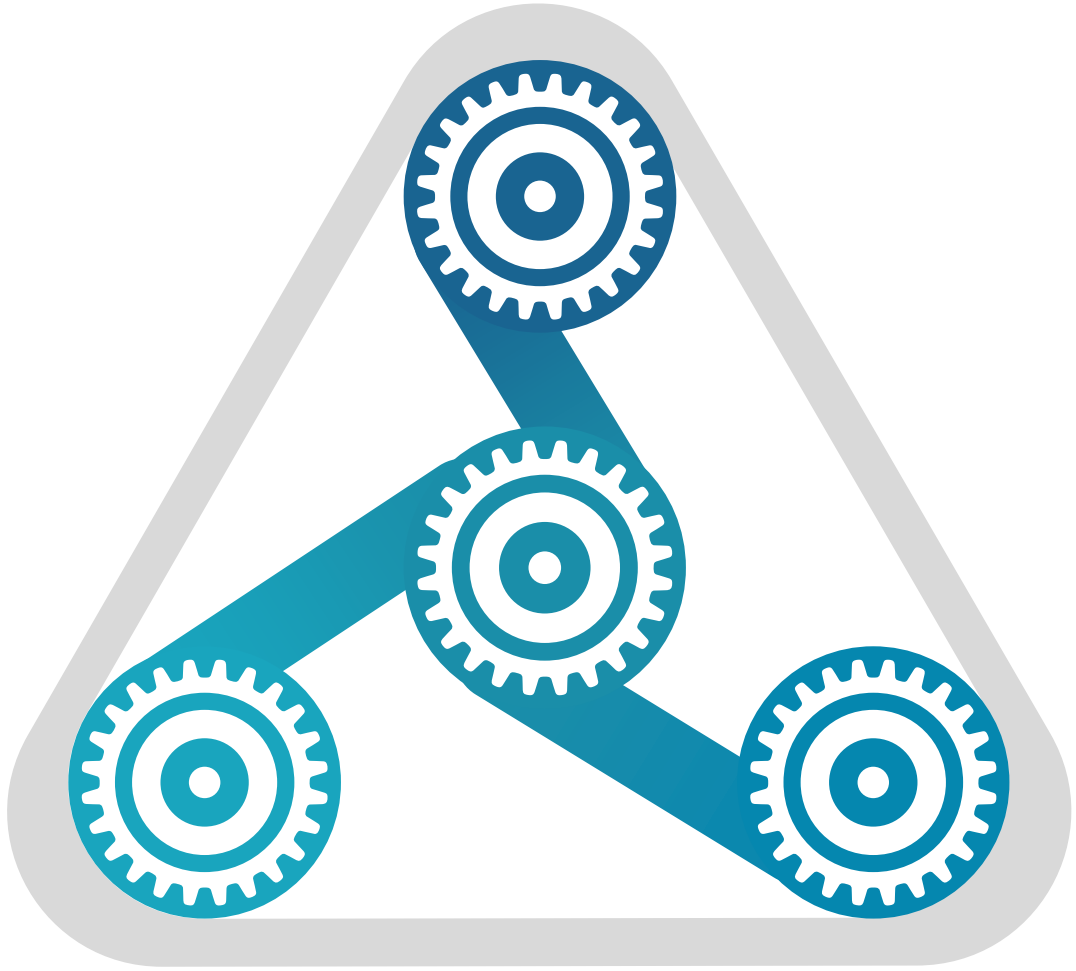
匯出非台灣的網路封包

請設定顯示過濾條件，將不是台灣的外網通訊，全部顯示出來。

特別注意，只要**對外部網路的通訊封包**，要忽略內部網路互傳的通訊封包。

實作題目 (範例操作)

命令列模式的封包分析



(1) Wireshark　(2) TShark　(3) Python

適合大量分析作業的方式

一般來說，不論使用哪種方式，要注意三個關鍵，作為命令列操作的參數。
特別注意參數大小寫字母的差異!!

-r　輸入封包檔案資料

這個參數，告訴 Wireshark/Tshark 要讀取的 PCAP 封包檔案名稱

-R 或 –Y　顯示過濾條件

如同GUI介面，適當的顯示過濾條件可以用來快速篩選我們要的封包資料，而 -R 是 Wireshark 使用, -Y 是 Tshark 使用。條件字串可以使用 “ 與 “ 框列起來。

-w　重新儲存檔案名稱

針對 Tshark 來說，將符合過濾條件的封包資料，另外儲存成為新封包檔案, 適合作為大量封包分析的批次作業方式，動作類似GUI介面的Wireshark的Export Special Packets 匯出特殊封包功能。

常見的正常網路封包範例

請同學開啟各個正常範例封包檔案，確定能夠顯示正常網路通訊封包的檔案目錄。

NSPA Skills – Web Browse Behavior-連接(瀏覽)網站網頁(加密)

Apply a display filter ··· <Ctrl-/> Expression···

No.	Time	Source	Destination	Protocol	Length	Info
4676	2019-08-07 16:23:58.119542	192.168.201.59	168.95.192.1	DNS	78	Standard query 0xce12 A outlook.office.com
4677	2019-08-07 16:23:58.123029	168.95.192.1	192.168.201.59	DNS	236	Standard query response 0xce12 A outlook.office.com CNA
4678	2019-08-07 16:23:58.124517	192.168.201.59	13.107.18.11	TCP	66	52416 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256
4679	2019-08-07 16:23:58.127015	13.107.18.11	192.168.201.59	TCP	66	443 → 52416 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=
4680	2019-08-07 16:23:58.127134	192.168.201.59	13.107.18.11	TCP	54	52416 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
4681	2019-08-07 16:23:58.127957	192.168.201.59	13.107.18.11	TLSv1.2	261	Client Hello
4682	2019-08-07 16:23:58.130199	13.107.18.11	192.168.201.59	TCP	60	443 → 52416 [ACK] Seq=1 Ack=208 Win=2102272 Len=0
4683	2019-08-07 16:23:58.156719	13.107.18.11	192.168.201.59	TCP	1506	443 → 52416 [ACK] Seq=1 Ack=208 Win=2102272 Len=1452 [T
4684	2019-08-07 16:23:58.156724	13.107.18.11	192.168.201.59	TCP	1506	443 → 52416 [ACK] Seq=1453 Ack=208 Win=2102272 Len=1452
4685	2019-08-07 16:23:58.156828	192.168.201.59	13.107.18.11	TCP	54	52416 → 443 [ACK] Seq=208 Ack=2905 Win=262144 Len=0
4686	2019-08-07 16:23:58.156980	13.107.18.11	192.168.201.59	TLSv1.2	1483	Server Hello, Certificate, Certificate Status, Server K
4687	2019-08-07 16:23:58.157040	192.168.201.59	13.107.18.11	TCP	54	52416 → 443 [ACK] Seq=208 Ack=4334 Win=260608 Len=0
4688	2019-08-07 16:23:58.167333	192.168.201.59	13.107.18.11	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Hand
4689	2019-08-07 16:23:58.170257	13.107.18.11	192.168.201.59	TCP	60	443 → 52416 [ACK] Seq=4334 Ack=301 Win=2102272 Len=0
4690	2019-08-07 16:23:58.170729	13.107.18.11	192.168.201.59	TLSv1.2	380	New Session Ticket, Change Cipher Spec, Encrypted Hands
4691	2019-08-07 16:23:58.170733	13.107.18.11	192.168.201.59	TLSv1.2	123	Application Data
4692	2019-08-07 16:23:58.170870	192.168.201.59	13.107.18.11	TCP	54	52416 → 443 [ACK] Seq=301 Ack=4729 Win=262144 Len=0
4693	2019-08-07 16:23:58.172397	192.168.201.59	13.107.18.11	TLSv1.2	141	Application Data
4694	2019-08-07 16:23:58.172682	192.168.201.59	13.107.18.11	TLSv1.2	92	Application Data
4695	2019-08-07 16:23:58.172875	192.168.201.59	13.107.18.11	TLSv1.2	1404	Application Data
4696	2019-08-07 16:23:58.173160	192.168.201.59	13.107.18.11	TLSv1.2	876	Application Data
4697	2019-08-07 16:23:58.173332	192.168.201.59	13.107.18.11	TLSv1.2	92	Application Data
4698	2019-08-07 16:23:58.174877	13.107.18.11	192.168.201.59	TCP	60	443 → 52416 [ACK] Seq=4729 Ack=426 Win=2102272 Len=0
4699	2019-08-07 16:23:58.174879	13.107.18.11	192.168.201.59	TLSv1.2	92	Application Data
4700	2019-08-07 16:23:58.174986	192.168.201.59	13.107.18.11	TCP	54	52416 → 443 [ACK] Seq=2636 Ack=4767 Win=261888 Len=0

NSPA Skills – Web Browse Behavior-連接(瀏覽)網站網頁(明碼)

Apply a display filter ··· <Ctrl-/> Expression···

No.	Time	Source	Destination	Protocol	Length	Info
257	2019-08-07 16:17:05.951506	192.168.201.59	168.95.192.1	DNS	88	Standard query 0xd1a1 A cdn.content.prod.cms.msn.com
258	2019-08-07 16:17:05.951511	192.168.201.59	168.95.192.1	DNS	94	Standard query 0x712c A tile-service.weather.microsoft.
259	2019-08-07 16:17:05.954258	168.95.192.1	192.168.201.59	DNS	195	Standard query response 0xd1a1 A cdn.content.prod.cms.m
260	2019-08-07 16:17:05.954259	168.95.192.1	192.168.201.59	DNS	200	Standard query response 0x712c A tile-service.weather.m
261	2019-08-07 16:17:05.966760	192.168.201.59	173.222.181.250	TCP	66	52299 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
262	2019-08-07 16:17:05.967015	192.168.201.59	96.17.1.251	TCP	66	52300 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
263	2019-08-07 16:17:05.968189	192.168.201.59	173.222.181.250	TCP	66	52301 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
264	2019-08-07 16:17:05.969983	52.229.207.60	192.168.201.59	TCP	60	443 → 52298 [ACK] Seq=5864 Ack=419 Win=262400 Len=0
265	2019-08-07 16:17:05.969985	96.17.1.251	192.168.201.59	TCP	66	80 → 52300 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1
266	2019-08-07 16:17:05.970128	192.168.201.59	96.17.1.251	TCP	54	52300 → 80 [ACK] Seq=1 Ack=1 Win=66560 Len=0
267	2019-08-07 16:17:05.970323	192.168.201.59	96.17.1.251	HTTP	267	GET /zh-TW/livetile/preinstall?region=TW&appid=C98EA5B0
268	2019-08-07 16:17:05.972979	173.222.181.250	192.168.201.59	TCP	66	80 → 52299 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1
269	2019-08-07 16:17:05.972980	96.17.1.251	192.168.201.59	TCP	60	80 → 52300 [ACK] Seq=1 Ack=214 Win=30336 Len=0
270	2019-08-07 16:17:05.973094	192.168.201.59	173.222.181.250	TCP	54	52299 → 80 [ACK] Seq=1 Ack=1 Win=66560 Len=0
271	2019-08-07 16:17:05.973249	192.168.201.59	173.222.181.250	HTTP	269	GET /singletile/summary/alias/experiencebyname/today?ma
272	2019-08-07 16:17:05.973984	96.17.1.251	192.168.201.59	TCP	1506	80 → 52300 [ACK] Seq=1 Ack=214 Win=30336 Len=1452 [TCP
273	2019-08-07 16:17:05.973988	96.17.1.251	192.168.201.59	TCP	1506	80 → 52300 [ACK] Seq=1453 Ack=214 Win=30336 Len=1452 [T
274	2019-08-07 16:17:05.973990	173.222.181.250	192.168.201.59	TCP	66	80 → 52301 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1
275	2019-08-07 16:17:05.973991	96.17.1.251	192.168.201.59	TCP	1506	80 → 52300 [ACK] Seq=2905 Ack=214 Win=30336 Len=1452 [T
276	2019-08-07 16:17:05.973992	96.17.1.251	192.168.201.59	HTTP/X…	312	HTTP/1.1 200 OK
277	2019-08-07 16:17:05.974037	192.168.201.59	96.17.1.251	TCP	54	52300 → 80 [ACK] Seq=214 Ack=2905 Win=66560 Len=0
278	2019-08-07 16:17:05.974133	192.168.201.59	173.222.181.250	TCP	54	52301 → 80 [ACK] Seq=1 Ack=1 Win=66560 Len=0
279	2019-08-07 16:17:05.974147	192.168.201.59	96.17.1.251	TCP	54	52300 → 80 [ACK] Seq=214 Ack=4615 Win=66560 Len=0
280	2019-08-07 16:17:05.974263	192.168.201.59	173.222.181.250	HTTP	272	GET /singletile/summary/alias/experiencebyname/today?ma
281	2019-08-07 16:17:05.978320	173.222.181.250	192.168.201.59	TCP	60	80 → 52299 [ACK] Seq=1 Ack=216 Win=30336 Len=0

NSPA Skills – Web Browse Behavior-網頁檔案擷取完成-1

Apply a display filter ··· <Ctrl-/> Expression···

No.	Time	Source	Destination	Protocol	Length	Info
75	2019-08-19 14:09:31.504401	192.168.201.59	117.18.237.29	TCP	54	49841 → 80 [FIN, ACK] Seq=1 Ack=1 Win=260 Len=0
76	2019-08-19 14:09:31.504512	192.168.201.59	117.18.237.29	TCP	54	49803 → 80 [FIN, ACK] Seq=1 Ack=1 Win=257 Len=0
77	2019-08-19 14:09:31.504584	192.168.201.59	117.18.237.29	TCP	54	49827 → 80 [FIN, ACK] Seq=1 Ack=1 Win=260 Len=0
78	2019-08-19 14:09:31.504680	192.168.201.59	203.69.81.43	TCP	54	49970 → 80 [FIN, ACK] Seq=1 Ack=1 Win=257 Len=0
79	2019-08-19 14:09:31.504767	192.168.201.59	104.18.20.226	TCP	54	49842 → 80 [FIN, ACK] Seq=1 Ack=1 Win=260 Len=0
80	2019-08-19 14:09:31.504837	192.168.201.59	104.18.20.226	TCP	54	49843 → 80 [FIN, ACK] Seq=1 Ack=1 Win=260 Len=0
81	2019-08-19 14:09:31.504928	192.168.201.59	104.18.20.226	TCP	54	50079 → 80 [FIN, ACK] Seq=1 Ack=1 Win=260 Len=0
82	2019-08-19 14:09:31.505023	192.168.201.59	13.35.11.139	TCP	54	49777 → 80 [FIN, ACK] Seq=1 Ack=1 Win=260 Len=0
83	2019-08-19 14:09:31.507155	203.69.81.43	192.168.201.59	TCP	60	80 → 49970 [FIN, ACK] Seq=1 Ack=2 Win=245 Len=0
84	2019-08-19 14:09:31.507156	13.35.11.139	192.168.201.59	TCP	60	80 → 49777 [FIN, ACK] Seq=1 Ack=2 Win=119 Len=0
85	2019-08-19 14:09:31.507257	192.168.201.59	203.69.81.43	TCP	54	49970 → 80 [ACK] Seq=2 Ack=2 Win=257 Len=0
86	2019-08-19 14:09:31.507309	192.168.201.59	13.35.11.139	TCP	54	49777 → 80 [ACK] Seq=2 Ack=2 Win=260 Len=0
87	2019-08-19 14:09:31.507594	104.18.20.226	192.168.201.59	TCP	60	80 → 49843 [FIN, ACK] Seq=1 Ack=2 Win=34 Len=0
88	2019-08-19 14:09:31.507595	104.18.20.226	192.168.201.59	TCP	60	80 → 50079 [FIN, ACK] Seq=1 Ack=2 Win=30 Len=0
89	2019-08-19 14:09:31.507596	104.18.20.226	192.168.201.59	TCP	60	80 → 49842 [FIN, ACK] Seq=1 Ack=2 Win=34 Len=0
90	2019-08-19 14:09:31.507669	192.168.201.59	104.18.20.226	TCP	54	49843 → 80 [ACK] Seq=2 Ack=2 Win=260 Len=0
91	2019-08-19 14:09:31.507712	192.168.201.59	104.18.20.226	TCP	54	50079 → 80 [ACK] Seq=2 Ack=2 Win=260 Len=0
92	2019-08-19 14:09:31.507738	192.168.201.59	104.18.20.226	TCP	54	49842 → 80 [ACK] Seq=2 Ack=2 Win=260 Len=0
93	2019-08-19 14:09:31.540441	117.18.237.29	192.168.201.59	TCP	60	80 → 49827 [FIN, ACK] Seq=1 Ack=2 Win=296 Len=0
94	2019-08-19 14:09:31.540528	192.168.201.59	117.18.237.29	TCP	54	49827 → 80 [ACK] Seq=2 Ack=2 Win=260 Len=0
95	2019-08-19 14:09:31.547406	117.18.237.29	192.168.201.59	TCP	60	80 → 49841 [FIN, ACK] Seq=1 Ack=2 Win=294 Len=0
96	2019-08-19 14:09:31.547460	192.168.201.59	117.18.237.29	TCP	54	49841 → 80 [ACK] Seq=2 Ack=2 Win=260 Len=0
97	2019-08-19 14:09:31.547933	117.18.237.29	192.168.201.59	TCP	60	80 → 49803 [FIN, ACK] Seq=1 Ack=2 Win=296 Len=0
98	2019-08-19 14:09:31.547985	192.168.201.59	117.18.237.29	TCP	54	49803 → 80 [ACK] Seq=2 Ack=2 Win=257 Len=0

NSPA Skills – Web Behavior – Windows 擷取天氣資訊

Apply a display filter ··· <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
90883	2020-04-18 17:43:05.099099	10.0.1.2	203.69.81.80	TCP	66	51521 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
90884	2020-04-18 17:43:05.099477	203.69.81.80	10.0.1.2	TCP	66	80 → 51520 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=1 SACK_PER
90885	2020-04-18 17:43:05.099481	203.69.81.80	10.0.1.2	TCP	66	80 → 51521 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=1 SACK_PER
90886	2020-04-18 17:43:05.099519	10.0.1.2	203.69.81.80	TCP	54	51521 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
90887	2020-04-18 17:43:05.099521	10.0.1.2	203.69.81.80	TCP	54	51520 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
90888	2020-04-18 17:43:05.099577	10.0.1.2	203.69.81.80	HTTP	356	GET /weatherservice.svc/livetile?city=%E5%AD%9F%E8%B2%B7&lat=18.927&long
90889	2020-04-18 17:43:05.099579	10.0.1.2	203.69.81.80	HTTP	355	GET /weatherservice.svc/livetile?city=%E5%B7%B4%E9%BB%8E&lat=48.857&long
90890	2020-04-18 17:43:05.103037	203.69.81.80	10.0.1.2	HTTP	291	HTTP/1.1 404 Not Found (text/html)
90891	2020-04-18 17:43:05.103146	203.69.81.80	10.0.1.2	HTTP	291	HTTP/1.1 404 Not Found (text/html)
90892	2020-04-18 17:43:05.152557	10.0.1.2	203.69.81.80	TCP	54	51521 → 80 [ACK] Seq=303 Ack=238 Win=261888 Len=0
90893	2020-04-18 17:43:05.155813	10.0.1.2	203.69.81.80	TCP	54	51520 → 80 [ACK] Seq=302 Ack=238 Win=261888 Len=0
90894	2020-04-18 17:43:05.204491	137.117.209.30	10.0.1.2	TCP	60	80 → 51519 [ACK] Seq=819 Ack=574 Win=64962 Len=0
90895	2020-04-18 17:43:05.204669	137.117.209.30	10.0.1.2	TCP	60	80 → 51518 [ACK] Seq=821 Ack=573 Win=64963 Len=0
90896	2020-04-18 17:43:05.259423	137.117.209.30	10.0.1.2	HTTP	878	HTTP/1.1 302 Redirect (text/html)
90897	2020-04-18 17:43:05.259601	10.0.1.2	203.69.81.80	HTTP	358	GET /weatherservice.svc/livetile?city=%E9%9B%AA%E9%BB%8E&lat=-33.870&lon
90898	2020-04-18 17:43:05.259603	10.0.1.2	137.117.209.30	HTTP	350	GET /WeatherService.svc/LiveTile?city=%E7%B4%90%E7%B4%84%E5%B8%82&lat=40
90899	2020-04-18 17:43:05.260040	137.117.209.30	10.0.1.2	HTTP	874	HTTP/1.1 302 Redirect (text/html)
90900	2020-04-18 17:43:05.260172	10.0.1.2	203.69.81.80	HTTP	356	GET /weatherservice.svc/livetile?city=%E5%80%AB%E6%95%A6&lat=51.506&long
90901	2020-04-18 17:43:05.262753	203.69.81.80	10.0.1.2	HTTP	291	HTTP/1.1 404 Not Found (text/html)
90902	2020-04-18 17:43:05.263260	203.69.81.80	10.0.1.2	HTTP	291	HTTP/1.1 404 Not Found (text/html)
90903	2020-04-18 17:43:05.310823	10.0.1.2	203.69.81.80	TCP	54	51521 → 80 [ACK] Seq=605 Ack=475 Win=261632 Len=0
90904	2020-04-18 17:43:05.310840	10.0.1.2	137.117.209.30	TCP	54	51518 → 80 [ACK] Seq=573 Ack=1641 Win=262144 Len=0
90905	2020-04-18 17:43:05.311989	10.0.1.2	203.69.81.80	TCP	54	51520 → 80 [ACK] Seq=606 Ack=475 Win=261632 Len=0
90906	2020-04-18 17:43:05.423329	137.117.209.30	10.0.1.2	TCP	60	80 → 51519 [ACK] Seq=1643 Ack=870 Win=64666 Len=0
90907	2020-04-18 17:43:05.467711	137.117.209.30	10.0.1.2	HTTP	894	HTTP/1.1 302 Redirect (text/html)
90908	2020-04-18 17:43:05.467890	10.0.1.2	203.69.81.80	HTTP	366	GET /weatherservice.svc/livetile?city=%E7%B4%90%E7%B4%84%E5%B8%82&lat=40
90909	2020-04-18 17:43:05.472205	203.69.81.80	10.0.1.2	HTTP	291	HTTP/1.1 404 Not Found (text/html)
90910	2020-04-18 17:43:05.511251	10.0.1.2	137.117.209.30	TCP	54	51519 → 80 [ACK] Seq=870 Ack=2483 Win=261120 Len=0
90911	2020-04-18 17:43:05.521252	10.0.1.2	203.69.81.80	TCP	54	51521 → 80 [ACK] Seq=917 Ack=712 Win=261376 Len=0

NSPA Skills – Web Browse Behavior-網頁檔案擷取完成-2

Apply a display filter ··· <Ctrl-/> Expression···

No.	Time	Source	Destination	Protocol	Length	Info
175	2019-08-19 14:09:47.259877	192.168.201.76	255.255.255.255	DB-LSP…	200	Dropbox LAN sync Discovery Protocol
176	2019-08-19 14:09:47.261881	192.168.201.76	192.168.201.255	DB-LSP…	200	Dropbox LAN sync Discovery Protocol
177	2019-08-19 14:09:47.261967	192.168.201.76	255.255.255.255	DB-LSP…	200	Dropbox LAN sync Discovery Protocol
178	2019-08-19 14:09:47.262072	192.168.201.76	255.255.255.255	DB-LSP…	200	Dropbox LAN sync Discovery Protocol
179	2019-08-19 14:09:47.262074	192.168.201.76	255.255.255.255	DB-LSP…	200	Dropbox LAN sync Discovery Protocol
180	2019-08-19 14:09:49.118949	JuniperN_05:27:e2	Spanning-tree-(for…	STP	60	RST. Root = 32768/0/28:8a:1c:05:27:c1 Cost = 0 Port =
181	2019-08-19 14:09:49.209640	JuniperN_05:27:e2	LLDP_Multicast	LLDP	229	TTL = 120 SysDesc = Juniper Networks, Inc. ex2200-48t-4
182	2019-08-19 14:09:49.255752	192.168.201.59	119.161.16.12	TCP	54	53987 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1020 Len=0
183	2019-08-19 14:09:49.255951	192.168.201.59	119.161.16.12	TCP	54	53988 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1022 Len=0
184	2019-08-19 14:09:49.256105	192.168.201.59	216.58.200.42	TCP	54	49716 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1019 Len=0
185	2019-08-19 14:09:49.256219	192.168.201.59	216.58.200.227	TCP	54	53981 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1019 Len=0
186	2019-08-19 14:09:49.256343	192.168.201.59	216.58.200.227	TCP	54	53982 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1023 Len=0
187	2019-08-19 14:09:49.256437	192.168.201.59	216.58.200.227	TCP	54	53983 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1023 Len=0
188	2019-08-19 14:09:49.256544	192.168.201.59	216.58.200.227	TCP	54	53984 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1023 Len=0
189	2019-08-19 14:09:49.256619	192.168.201.59	216.58.200.227	TCP	54	53985 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1023 Len=0
190	2019-08-19 14:09:49.256729	192.168.201.59	216.58.200.227	TCP	54	53986 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1023 Len=0
191	2019-08-19 14:09:49.256923	192.168.201.59	216.58.200.38	TCP	54	53974 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1024 Len=0
192	2019-08-19 14:09:49.257062	192.168.201.59	216.58.200.34	TCP	54	49774 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1024 Len=0
193	2019-08-19 14:09:49.257179	192.168.201.59	172.217.160.98	TCP	54	53980 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1022 Len=0
194	2019-08-19 14:09:49.257561	192.168.201.59	52.200.14.132	TLSv1.2	1588	Application Data
195	2019-08-19 14:09:49.258646	119.161.16.12	192.168.201.59	TCP	60	443 → 53987 [FIN, ACK] Seq=1 Ack=2 Win=126 Len=0
196	2019-08-19 14:09:49.258738	192.168.201.59	119.161.16.12	TCP	54	53987 → 443 [ACK] Seq=2 Ack=2 Win=1020 Len=0
197	2019-08-19 14:09:49.258819	216.58.200.42	192.168.201.59	TCP	60	443 → 49716 [FIN, ACK] Seq=1 Ack=2 Win=266 Len=0
198	2019-08-19 14:09:49.258821	119.161.16.12	192.168.201.59	TCP	60	443 → 53988 [FIN, ACK] Seq=1 Ack=2 Win=119 Len=0

NSPA Skills – Web Browse Behavior-網頁檔案連續擷取

Apply a display filter ··· <Ctrl-/> Expression···

No.	Time	Source	Destination	Protocol	Length	Info
2241	2019-08-07 16:17:40.541618	192.168.201.59	203.104.150.4	TLSv1.2	1038	Application Data
2242	2019-08-07 16:17:40.546398	203.104.150.4	192.168.201.59	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypted Hands
2243	2019-08-07 16:17:40.548323	192.168.201.59	203.104.150.4	TLSv1.2	1038	Application Data
2244	2019-08-07 16:17:40.548904	203.104.150.4	192.168.201.59	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypted Hands
2245	2019-08-07 16:17:40.551002	192.168.201.59	203.104.150.4	TLSv1.2	1038	Application Data
2246	2019-08-07 16:17:40.557237	52.229.207.60	192.168.201.59	TCP	66	443 → 52345 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1
2247	2019-08-07 16:17:40.557398	192.168.201.59	52.229.207.60	TCP	54	52345 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
2248	2019-08-07 16:17:40.575074	192.168.201.59	52.229.207.60	TLSv1.2	254	Client Hello
2249	2019-08-07 16:17:40.580450	203.104.150.4	192.168.201.59	TLSv1.2	179	Application Data
2250	2019-08-07 16:17:40.580452	203.104.150.4	192.168.201.59	TCP	60	443 → 52343 [FIN, ACK] Seq=3676 Ack=1628 Win=17920 Len=
2251	2019-08-07 16:17:40.580645	192.168.201.59	203.104.150.4	TCP	54	52343 → 443 [ACK] Seq=1628 Ack=3677 Win=66304 Len=0
2252	2019-08-07 16:17:40.582085	203.104.150.4	192.168.201.59	TLSv1.2	179	Application Data
2253	2019-08-07 16:17:40.582329	203.104.150.4	192.168.201.59	TCP	60	443 → 52344 [FIN, ACK] Seq=3676 Ack=1628 Win=17920 Len=
2254	2019-08-07 16:17:40.582393	192.168.201.59	203.104.150.4	TCP	54	52344 → 443 [ACK] Seq=1628 Ack=3677 Win=66304 Len=0
2255	2019-08-07 16:17:40.583992	192.168.201.59	203.104.150.4	TCP	54	52343 → 443 [FIN, ACK] Seq=1628 Ack=3677 Win=66304 Len=
2256	2019-08-07 16:17:40.585266	192.168.201.59	203.104.150.4	TCP	54	52344 → 443 [FIN, ACK] Seq=1628 Ack=3677 Win=66304 Len=
2257	2019-08-07 16:17:40.588045	203.104.150.4	192.168.201.59	TLSv1.2	179	Application Data
2258	2019-08-07 16:17:40.591251	203.104.150.4	192.168.201.59	TCP	60	443 → 52341 [FIN, ACK] Seq=3676 Ack=1628 Win=17920 Len=
2259	2019-08-07 16:17:40.591370	192.168.201.59	203.104.150.4	TCP	54	52341 → 443 [ACK] Seq=1628 Ack=3677 Win=66304 Len=0
2260	2019-08-07 16:17:40.592751	192.168.201.59	203.104.150.4	TCP	54	52341 → 443 [FIN, ACK] Seq=1628 Ack=3677 Win=66304 Len=
2261	2019-08-07 16:17:40.593551	203.104.150.4	192.168.201.59	TLSv1.2	179	Application Data
2262	2019-08-07 16:17:40.593553	203.104.150.4	192.168.201.59	TCP	60	443 → 52342 [FIN, ACK] Seq=3676 Ack=1628 Win=17920 Len=
2263	2019-08-07 16:17:40.593708	192.168.201.59	203.104.150.4	TCP	54	52342 → 443 [ACK] Seq=1628 Ack=3677 Win=66304 Len=0
2264	2019-08-07 16:17:40.597542	192.168.201.59	203.104.150.4	TCP	54	52342 → 443 [FIN, ACK] Seq=1628 Ack=3677 Win=66304 Len=
2265	2019-08-07 16:17:40.609799	52.229.207.60	192.168.201.59	TCP	1506	443 → 52345 [ACK] Seq=1 Ack=201 Win=262656 Len=1452 [TC

NSPA Skills – Web Browse Behavior-網頁檔案擷取完成(斷線)

Apply a display filter ··· <Ctrl-/> Expression···

No.	Time	Source	Destination	Protocol	Length	Info
37254	2019-08-07 16:40:18.861046	13.107.21.200	192.168.201.59	TCP	1506	443 → 52583 [ACK] Seq=552046 Ack=13898 Win=2101504 Len=
37255	2019-08-07 16:40:18.861048	13.107.21.200	192.168.201.59	TCP	1506	443 → 52583 [ACK] Seq=553498 Ack=13898 Win=2101504 Len=
37256	2019-08-07 16:40:18.861050	13.107.21.200	192.168.201.59	TLSv1.2	1227	Application Data
37257	2019-08-07 16:40:18.861052	13.107.21.200	192.168.201.59	TLSv1.2	92	Application Data
37258	2019-08-07 16:40:18.861115	192.168.201.59	13.107.21.200	TCP	54	52583 → 443 [ACK] Seq=13898 Ack=556161 Win=262144 Len=0
37259	2019-08-07 16:40:29.070191	192.168.201.59	172.217.160.82	TCP	54	52582 → 443 [RST, ACK] Seq=480 Ack=3105 Win=0 Len=0
37260	2019-08-07 16:40:29.071108	192.168.201.59	31.13.87.1	TCP	54	52480 → 443 [RST, ACK] Seq=9726 Ack=6254 Win=0 Len=0
37261	2019-08-07 16:40:29.071189	192.168.201.59	31.13.87.36	TCP	54	52506 → 443 [RST, ACK] Seq=512850 Ack=2324056 Win=0 Len
37262	2019-08-07 16:40:29.071373	192.168.201.59	172.217.160.66	TCP	54	52580 → 443 [RST, ACK] Seq=1524 Ack=585 Win=0 Len=0
37263	2019-08-07 16:40:29.072111	192.168.201.59	203.74.69.145	TCP	54	52575 → 443 [RST, ACK] Seq=1710 Ack=38402 Win=0 Len=0
37264	2019-08-07 16:40:29.072713	192.168.201.59	172.217.24.18	TCP	54	52581 → 443 [RST, ACK] Seq=480 Ack=3105 Win=0 Len=0
37265	2019-08-07 16:40:29.072846	192.168.201.59	203.74.69.209	TCP	54	52564 → 443 [RST, ACK] Seq=3281 Ack=107856 Win=0 Len=0
37266	2019-08-07 16:40:29.073204	192.168.201.59	203.74.69.81	TCP	54	52559 → 443 [RST, ACK] Seq=3479 Ack=205312 Win=0 Len=0
37267	2019-08-07 16:40:29.073351	192.168.201.59	203.74.69.81	TCP	54	52579 → 443 [RST, ACK] Seq=620 Ack=238 Win=0 Len=0
37268	2019-08-07 16:40:29.073418	192.168.201.59	172.217.160.100	TCP	54	52578 → 443 [RST, ACK] Seq=598 Ack=232 Win=0 Len=0
37269	2019-08-07 16:40:29.073493	192.168.201.59	31.13.87.36	TCP	54	52568 → 443 [RST, ACK] Seq=1043 Ack=1499 Win=0 Len=0
37270	2019-08-07 16:40:29.073555	192.168.201.59	203.74.69.145	TCP	54	52574 → 443 [RST, ACK] Seq=620 Ack=238 Win=0 Len=0
37271	2019-08-07 16:40:29.073629	192.168.201.59	31.13.87.5	TCP	54	52557 → 443 [RST, ACK] Seq=1516 Ack=76653 Win=0 Len=0
37272	2019-08-07 16:40:29.073745	192.168.201.59	203.74.69.17	TCP	54	52561 → 443 [RST, ACK] Seq=3295 Ack=292291 Win=0 Len=0
37273	2019-08-07 16:40:29.073805	192.168.201.59	216.58.200.35	TCP	54	52577 → 443 [RST, ACK] Seq=5623 Ack=2962 Win=0 Len=0
37274	2019-08-07 16:40:29.073863	192.168.201.59	172.217.24.2	TCP	54	52576 → 443 [RST, ACK] Seq=611 Ack=232 Win=0 Len=0
37275	2019-08-07 16:40:29.393415	192.168.201.59	52.114.158.50	TCP	54	52586 → 443 [RST, ACK] Seq=1625 Ack=6601 Win=0 Len=0
37276	2019-08-07 16:40:29.394634	192.168.201.59	13.107.21.200	TCP	54	52584 → 443 [RST, ACK] Seq=670 Ack=258 Win=0 Len=0
37277	2019-08-07 16:40:29.396205	192.168.201.59	13.107.21.200	TCP	54	52583 → 443 [RST, ACK] Seq=13898 Ack=556161 Win=0 Len=0
37278	2019-08-07 16:40:49.156342	192.168.201.152	192.168.201.59	UDP	70	54898 → 2054 Len=28

NSPA Skills – Web Browse Behavior-網頁檔案擷取完成(斷線)

Apply a display filter ··· <Ctrl-/> Expression···

No.	Time	Source	Destination	Protocol	Length	Info
53489	2019-08-07 16:51:30.879852	192.168.201.59	63.251.109.133	TCP	54	52867 → 443 [RST, ACK] Seq=1993 Ack=8521 Win=0 Len=0
53490	2019-08-07 16:51:30.880123	192.168.201.59	63.251.109.133	TCP	54	52866 → 443 [FIN, ACK] Seq=339 Ack=5204 Win=260864 Len=
53491	2019-08-07 16:51:30.880179	192.168.201.59	63.251.109.133	TCP	54	52866 → 443 [RST, ACK] Seq=340 Ack=5204 Win=0 Len=0
53492	2019-08-07 16:51:30.880458	192.168.201.59	63.251.109.143	TCP	54	52843 → 443 [FIN, ACK] Seq=1660 Ack=6285 Win=260608 Len
53493	2019-08-07 16:51:30.880512	192.168.201.59	63.251.109.143	TCP	54	52843 → 443 [RST, ACK] Seq=1661 Ack=6285 Win=0 Len=0
53494	2019-08-07 16:51:30.880776	192.168.201.59	63.251.109.143	TCP	54	52844 → 443 [FIN, ACK] Seq=337 Ack=5204 Win=260864 Len=
53495	2019-08-07 16:51:30.880849	192.168.201.59	63.251.109.143	TCP	54	52844 → 443 [RST, ACK] Seq=338 Ack=5204 Win=0 Len=0
53496	2019-08-07 16:51:30.881136	192.168.201.59	50.116.239.135	TCP	54	52840 → 443 [FIN, ACK] Seq=8829 Ack=5044 Win=65535 Len=
53497	2019-08-07 16:51:30.881191	192.168.201.59	50.116.239.135	TCP	54	52840 → 443 [RST, ACK] Seq=8830 Ack=5044 Win=0 Len=0
53498	2019-08-07 16:51:30.881317	192.168.201.59	50.116.239.135	TCP	54	52852 → 80 [FIN, ACK] Seq=2526 Ack=571 Win=65535 Len=0
53499	2019-08-07 16:51:30.881635	192.168.201.59	50.116.239.135	TCP	54	52841 → 443 [FIN, ACK] Seq=542 Ack=3418 Win=65535 Len=0
53500	2019-08-07 16:51:30.881724	192.168.201.59	50.116.239.135	TCP	54	52841 → 443 [RST, ACK] Seq=543 Ack=3418 Win=0 Len=0
53501	2019-08-07 16:51:30.882149	192.168.201.59	96.7.252.75	TCP	54	52850 → 443 [FIN, ACK] Seq=337 Ack=3085 Win=261632 Len=
53502	2019-08-07 16:51:30.882225	192.168.201.59	96.7.252.75	TCP	54	52850 → 443 [RST, ACK] Seq=338 Ack=3085 Win=0 Len=0
53503	2019-08-07 16:51:30.882614	192.168.201.59	50.116.239.135	TCP	54	52807 → 443 [FIN, ACK] Seq=3235 Ack=3498 Win=65535 Len=
53504	2019-08-07 16:51:30.882680	192.168.201.59	50.116.239.135	TCP	54	52807 → 443 [RST, ACK] Seq=3236 Ack=3498 Win=0 Len=0
53505	2019-08-07 16:51:30.883027	192.168.201.59	50.116.239.135	TCP	54	52808 → 443 [FIN, ACK] Seq=542 Ack=3418 Win=65535 Len=0
53506	2019-08-07 16:51:30.883111	192.168.201.59	50.116.239.135	TCP	54	52808 → 443 [RST, ACK] Seq=543 Ack=3418 Win=0 Len=0
53507	2019-08-07 16:51:30.883611	192.168.201.59	18.136.128.217	TCP	54	52792 → 443 [FIN, ACK] Seq=334 Ack=5654 Win=65535 Len=0
53508	2019-08-07 16:51:30.883672	192.168.201.59	18.136.128.217	TCP	54	52792 → 443 [RST, ACK] Seq=335 Ack=5654 Win=0 Len=0
53509	2019-08-07 16:51:30.884109	192.168.201.59	52.88.201.222	TCP	54	52819 → 443 [FIN, ACK] Seq=333 Ack=3509 Win=65535 Len=0
53510	2019-08-07 16:51:30.884181	192.168.201.59	52.88.201.222	TCP	54	52819 → 443 [RST, ACK] Seq=334 Ack=3509 Win=0 Len=0
53511	2019-08-07 16:51:30.884562	192.168.201.59	67.226.210.15	TCP	54	52803 → 443 [FIN, ACK] Seq=1110 Ack=6165 Win=261120 Len
53512	2019-08-07 16:51:30.884631	192.168.201.59	67.226.210.15	TCP	54	52803 → 443 [RST, ACK] Seq=1111 Ack=6165 Win=0 Len=0
53513	2019-08-07 16:51:30.884999	192.168.201.59	67.226.210.15	TCP	54	52806 → 443 [FIN, ACK] Seq=330 Ack=5445 Win=261632 Len=

NSPA Skills – FTP Behavior – FTP 匿名登入

Apply a display filter ··· <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
34	2014-12-08 18:20:47.517000	192.168.1.188	125.227.239.179	TCP	66	49199 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
35	2014-12-08 18:20:47.517000	125.227.239.179	192.168.1.188	TCP	66	21 → 49199 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1452 WS=1 SACK
36	2014-12-08 18:20:47.517000	192.168.1.188	125.227.239.179	TCP	54	49199 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0
37	2014-12-08 18:20:47.595000	125.227.239.179	192.168.1.188	FTP	89	Response: 220 PCMan's FTP Server 2.0 Ready.
38	2014-12-08 18:20:47.595000	192.168.1.188	125.227.239.179	FTP	70	Request: USER anonymous
39	2014-12-08 18:20:47.595000	125.227.239.179	192.168.1.188	FTP	90	Response: 331 User name okay, need password.
40	2014-12-08 18:20:47.611000	192.168.1.188	125.227.239.179	FTP	73	Request: PASS user@user-PC
41	2014-12-08 18:20:47.611000	125.227.239.179	192.168.1.188	FTP	74	Response: 530 Not logged in.
42	2014-12-08 18:20:47.626000	125.227.239.179	192.168.1.188	TCP	60	21 → 49199 [FIN, ACK] Seq=92 Ack=36 Win=64205 Len=0
43	2014-12-08 18:20:47.626000	192.168.1.188	125.227.239.179	TCP	54	49199 → 21 [ACK] Seq=36 Ack=93 Win=8100 Len=0
44	2014-12-08 18:20:47.642000	192.168.1.188	125.227.239.179	TCP	54	49199 → 21 [FIN, ACK] Seq=36 Ack=93 Win=8100 Len=0
45	2014-12-08 18:20:47.642000	125.227.239.179	192.168.1.188	TCP	60	21 → 49199 [ACK] Seq=93 Ack=37 Win=64205 Len=0
46	2014-12-08 18:20:48.531000	192.168.1.188	125.227.239.179	TCP	66	49200 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
47	2014-12-08 18:20:48.531000	125.227.239.179	192.168.1.188	TCP	66	21 → 49200 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1452 WS=1 SACK
48	2014-12-08 18:20:48.531000	192.168.1.188	125.227.239.179	TCP	54	49200 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0
49	2014-12-08 18:20:48.594000	125.227.239.179	192.168.1.188	FTP	89	Response: 220 PCMan's FTP Server 2.0 Ready.
50	2014-12-08 18:20:48.594000	192.168.1.188	125.227.239.179	FTP	70	Request: USER anonymous
51	2014-12-08 18:20:48.594000	125.227.239.179	192.168.1.188	FTP	90	Response: 331 User name okay, need password.
52	2014-12-08 18:20:48.594000	192.168.1.188	125.227.239.179	FTP	73	Request: PASS user@user-PC
53	2014-12-08 18:20:48.672000	125.227.239.179	192.168.1.188	FTP	74	Response: 530 Not logged in.
54	2014-12-08 18:20:48.672000	125.227.239.179	192.168.1.188	TCP	60	21 → 49200 [FIN, ACK] Seq=92 Ack=36 Win=64205 Len=0
55	2014-12-08 18:20:48.672000	192.168.1.188	125.227.239.179	TCP	54	49200 → 21 [ACK] Seq=36 Ack=93 Win=8100 Len=0
56	2014-12-08 18:20:48.672000	192.168.1.188	125.227.239.179	TCP	54	49200 → 21 [FIN, ACK] Seq=36 Ack=93 Win=8100 Len=0
57	2014-12-08 18:20:48.672000	125.227.239.179	192.168.1.188	TCP	60	21 → 49200 [ACK] Seq=93 Ack=37 Win=64205 Len=0
58	2014-12-08 18:20:49.436000	61.92.206.20	192.168.1.27	TCP	74	[TCP Retransmission] 4058 → 23 [SYN] Seq=0 Win=5840 Len=0 MSS=1452 S
59	2014-12-08 18:20:50.684000	192.168.1.188	125.227.239.179	TCP	66	49201 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
60	2014-12-08 18:20:50.684000	125.227.239.179	192.168.1.188	TCP	66	21 → 49201 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1452 WS=1 SACK
61	2014-12-08 18:20:50.684000	192.168.1.188	125.227.239.179	TCP	54	49201 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0
62	2014-12-08 18:20:50.700000	125.227.239.179	192.168.1.188	FTP	89	Response: 220 PCMan's FTP Server 2.0 Ready.

NSPA Skills – Telnet Behavior

Apply a display filter ··· <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
14	2015-06-10 19:37:07.819000	10.10.1.108	10.10.1.10	TCP	54	23 → 49241 [ACK] Seq=300 Ack=133 Win=65536 Len=0
15	2015-06-10 19:37:07.827000	10.10.1.10	10.10.1.108	TELNET	543	Telnet Data ...
16	2015-06-10 19:37:07.838000	10.10.1.108	10.10.1.10	TELNET	245	Telnet Data ...
17	2015-06-10 19:37:08.046000	10.10.1.10	10.10.1.108	TCP	54	49241 → 23 [ACK] Seq=622 Ack=491 Win=65024 Len=0
18	2015-06-10 19:37:12.055000	10.10.1.10	10.10.1.108	TELNET	55	Telnet Data ...
19	2015-06-10 19:37:12.065000	10.10.1.108	10.10.1.10	TELNET	55	Telnet Data ...
20	2015-06-10 19:37:12.276000	10.10.1.10	10.10.1.108	TCP	54	49241 → 23 [ACK] Seq=623 Ack=492 Win=65024 Len=0
21	2015-06-10 19:37:12.396000	10.10.1.10	10.10.1.108	TELNET	55	Telnet Data ...
22	2015-06-10 19:37:12.406000	10.10.1.108	10.10.1.10	TELNET	55	Telnet Data ...
23	2015-06-10 19:37:12.566000	10.10.1.10	10.10.1.108	TELNET	55	Telnet Data ...
24	2015-06-10 19:37:12.583000	10.10.1.108	10.10.1.10	TELNET	55	Telnet Data ...
25	2015-06-10 19:37:12.747000	10.10.1.10	10.10.1.108	TELNET	55	Telnet Data ...
26	2015-06-10 19:37:12.757000	10.10.1.108	10.10.1.10	TELNET	55	Telnet Data ...
27	2015-06-10 19:37:12.967000	10.10.1.10	10.10.1.108	TCP	54	49241 → 23 [ACK] Seq=626 Ack=495 Win=65024 Len=0
28	2015-06-10 19:37:14.674000	10.10.1.10	10.10.1.108	TELNET	56	Telnet Data ...
29	2015-06-10 19:37:14.683000	10.10.1.108	10.10.1.10	TELNET	66	Telnet Data ...
30	2015-06-10 19:37:14.893000	10.10.1.10	10.10.1.108	TCP	54	49241 → 23 [ACK] Seq=628 Ack=507 Win=65024 Len=0
31	2015-06-10 19:37:15.554000	10.10.1.10	10.10.1.108	TELNET	55	Telnet Data ...
32	2015-06-10 19:37:15.618000	10.10.1.108	10.10.1.10	TCP	54	23 → 49241 [ACK] Seq=507 Ack=629 Win=65024 Len=0
33	2015-06-10 19:37:15.720000	10.10.1.10	10.10.1.108	TELNET	55	Telnet Data ...
34	2015-06-10 19:37:15.774000	10.10.1.108	10.10.1.10	TCP	54	23 → 49241 [ACK] Seq=507 Ack=630 Win=65024 Len=0
35	2015-06-10 19:37:15.977000	10.10.1.10	10.10.1.108	TELNET	55	Telnet Data ...
36	2015-06-10 19:37:16.029000	10.10.1.108	10.10.1.10	TCP	54	23 → 49241 [ACK] Seq=507 Ack=631 Win=65024 Len=0
37	2015-06-10 19:37:16.131000	10.10.1.10	10.10.1.108	TELNET	55	Telnet Data ...
38	2015-06-10 19:37:16.183000	10.10.1.108	10.10.1.10	TCP	54	23 → 49241 [ACK] Seq=507 Ack=632 Win=65024 Len=0
39	2015-06-10 19:37:16.335000	10.10.1.10	10.10.1.108	TELNET	56	Telnet Data ...
40	2015-06-10 19:37:16.337000	10.10.1.108	10.10.1.10	TELNET	97	Telnet Data ...
41	2015-06-10 19:37:16.539000	10.10.1.10	10.10.1.108	TCP	54	49241 → 23 [ACK] Seq=634 Ack=550 Win=65024 Len=0

NSPA Skills – SMB/CIFS - Activity

not arp

No.	Time	Source	Destination	Protocol	Length	Info
365	2020-06-19 11:53:26.784932	10.0.1.4	10.0.1.15	TCP	66	49201 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
367	2020-06-19 11:53:26.785337	10.0.1.15	10.0.1.4	TCP	66	445 → 49201 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK
368	2020-06-19 11:53:26.785676	10.0.1.4	10.0.1.15	TCP	60	49201 → 445 [ACK] Seq=1 Ack=1 Win=65536 Len=0
369	2020-06-19 11:53:26.785678	10.0.1.4	10.0.1.15	SMB	213	Negotiate Protocol Request
370	2020-06-19 11:53:26.787460	10.0.1.15	10.0.1.4	SMB2	463	Negotiate Protocol Response
371	2020-06-19 11:53:26.787842	10.0.1.4	10.0.1.15	SMB2	164	Negotiate Protocol Request
372	2020-06-19 11:53:26.789689	10.0.1.15	10.0.1.4	SMB2	463	Negotiate Protocol Response
373	2020-06-19 11:53:26.790622	10.0.1.4	10.0.1.15	SMB2	220	Session Setup Request, NTLMSSP_NEGOTIATE
374	2020-06-19 11:53:26.790939	10.0.1.15	10.0.1.4	SMB2	299	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSS
375	2020-06-19 11:53:26.791564	10.0.1.4	10.0.1.15	SMB2	581	Session Setup Request, NTLMSSP_AUTH, User: NSPA3\Admin
376	2020-06-19 11:53:26.792422	10.0.1.15	10.0.1.4	SMB2	159	Session Setup Response
377	2020-06-19 11:53:26.792902	10.0.1.4	10.0.1.15	SMB2	162	Tree Connect Request Tree: \\10.0.1.15\IPC$
378	2020-06-19 11:53:26.792996	10.0.1.15	10.0.1.4	SMB2	138	Tree Connect Response
379	2020-06-19 11:53:26.793361	10.0.1.4	10.0.1.15	SMB2	210	Ioctl Request FSCTL_VALIDATE_NEGOTIATE_INFO
380	2020-06-19 11:53:26.793437	10.0.1.15	10.0.1.4	SMB2	194	Ioctl Response FSCTL_VALIDATE_NEGOTIATE_INFO
381	2020-06-19 11:53:26.793813	10.0.1.4	10.0.1.15	SMB2	178	Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
382	2020-06-19 11:53:26.793815	10.0.1.4	10.0.1.15	SMB2	190	Create Request File: wkssvc
383	2020-06-19 11:53:26.793846	10.0.1.15	10.0.1.4	TCP	54	445 → 49201 [ACK] Seq=1393 Ack=1487 Win=64256 Len=0
384	2020-06-19 11:53:26.793887	10.0.1.15	10.0.1.4	SMB2	778	Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
385	2020-06-19 11:53:26.793979	10.0.1.15	10.0.1.4	SMB2	210	Create Response File: wkssvc
386	2020-06-19 11:53:26.794257	10.0.1.4	10.0.1.15	TCP	60	49201 → 445 [ACK] Seq=1487 Ack=2273 Win=65536 Len=0
387	2020-06-19 11:53:26.794259	10.0.1.4	10.0.1.15	SMB2	162	GetInfo Request FILE_INFO/SMB2_FILE_STANDARD_INFO File: wkssvc
388	2020-06-19 11:53:26.794325	10.0.1.15	10.0.1.4	SMB2	154	GetInfo Response
389	2020-06-19 11:53:26.794697	10.0.1.4	10.0.1.15	DCERPC	330	Bind: call_id: 2, Fragment: Single, 3 context items: WKSSVC V1.0 (32b
390	2020-06-19 11:53:26.794774	10.0.1.15	10.0.1.4	SMB2	138	Write Response
391	2020-06-19 11:53:26.795132	10.0.1.4	10.0.1.15	SMB2	171	Read Request Len:1024 Off:0 File: wkssvc
392	2020-06-19 11:53:26.795185	10.0.1.15	10.0.1.4	DCERPC	254	Bind_ack: call_id: 2, Fragment: Single, max_xmit: 4280 max_recv: 4280
393	2020-06-19 11:53:26.795559	10.0.1.4	10.0.1.15	WKSSVC	262	NetWkstaGetInfo request Level:100
394	2020-06-19 11:53:26.795737	10.0.1.15	10.0.1.4	WKSSVC	330	NetWkstaGetInfo response

NSPA Skills – SMTP

Apply a display filter ··· <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
107	2006-08-14 13:39:05.531000	61.221.67.43	61.218.77.115	SMTP	148	S: 220 mail.diamondinfotech.com.tw ESMTP Sendmail 8.11.2/8.8.7; Mor
108	2006-08-14 13:39:05.984000	61.218.77.115	61.221.67.43	SMTP	76	C: EHLO imss.fmt.com.tw
109	2006-08-14 13:39:05.984000	61.221.67.43	61.218.77.115	TCP	60	25 → 2145 [ACK] Seq=95 Ack=23 Win=31944 Len=0
110	2006-08-14 13:39:05.984000	61.221.67.43	61.218.77.115	SMTP	264	S: 250-mail.diamondinfotech.com.tw Hello dns1.fmt.com.tw [61.218.77
111	2006-08-14 13:39:06.453000	61.218.77.115	61.221.67.43	SMTP	96	C: MAIL FROM:<schsiao@fmt.com.tw> SIZE=1834
112	2006-08-14 13:39:06.453000	61.221.67.43	59.120.215.162	DNS	70	Standard query 0x4dc0 ANY fmt.com.tw
113	2006-08-14 13:39:06.453000	61.221.67.43	61.218.77.115	TCP	60	25 → 2145 [ACK] Seq=305 Ack=65 Win=31944 Len=0
114	2006-08-14 13:39:06.562000	59.120.215.162	61.221.67.43	DNS	162	Standard query response 0x4dc0 ANY fmt.com.tw A 61.30.78.226 A 61.2
115	2006-08-14 13:39:06.562000	61.221.67.43	61.218.77.115	SMTP	99	S: 250 2.1.0 <schsiao@fmt.com.tw>... Sender ok
116	2006-08-14 13:39:06.718000	61.221.67.43	59.120.215.162	DNS	77	Standard query 0x4dc0 A rs590.ndmc.edu.tw
117	2006-08-14 13:39:06.875000	61.218.77.115	61.221.67.43	SMTP	113	C: RCPT TO:<gloria@mail.diamondinfotech.com.tw> NOTIFY=NEVER
118	2006-08-14 13:39:06.875000	61.221.67.43	59.120.215.162	DNS	87	Standard query 0x4dc1 ANY mail.diamondinfotech.com.tw
119	2006-08-14 13:39:06.875000	61.221.67.43	61.218.77.115	TCP	60	25 → 2145 [ACK] Seq=350 Ack=124 Win=31944 Len=0
120	2006-08-14 13:39:06.921000	59.120.215.162	61.221.67.43	DNS	131	Standard query response 0x4dc1 ANY mail.diamondinfotech.com.tw A 61
121	2006-08-14 13:39:06.921000	61.221.67.43	61.218.77.115	SMTP	118	S: 250 2.1.5 <gloria@mail.diamondinfotech.com.tw>... Recipient ok
122	2006-08-14 13:39:07.234000	61.218.77.115	61.221.67.43	SMTP	60	C: DATA
123	2006-08-14 13:39:07.234000	61.221.67.43	61.218.77.115	SMTP	104	S: 354 Enter mail, end with "." on a line by itself
124	2006-08-14 13:39:07.296000	59.120.215.162	61.221.67.43	DNS	77	Standard query response 0x4dd0 Server failure A mail.vanko.com.tw
125	2006-08-14 13:39:07.437000	61.218.77.115	61.221.67.43	SMTP	132	C: DATA fragment, 78 bytes
126	2006-08-14 13:39:07.437000	61.221.67.43	61.218.77.115	TCP	60	25 → 2145 [ACK] Seq=464 Ack=208 Win=31944 Len=0
127	2006-08-14 13:39:07.453000	61.218.77.115	61.221.67.43	SMTP	1434	C: DATA fragment, 1380 bytes
128	2006-08-14 13:39:07.453000	61.218.77.115	61.221.67.43	SMTP	97	C: DATA fragment, 43 bytes
129	2006-08-14 13:39:07.453000	61.218.77.115	61.221.67.43	SMTP	97	C: DATA fragment, 43 bytes
130	2006-08-14 13:39:07.453000	61.221.67.43	61.218.77.115	TCP	60	25 → 2145 [ACK] Seq=464 Ack=1674 Win=31944 Len=0
131	2006-08-14 13:39:07.875000	61.218.77.115	61.221.67.43	SMTP/IMF	347	subject: =?big5?B?xaqo+jogoW23c6pprOyn3qFuOC8yOatls/imV8B1tGYgIC0g1
132	2006-08-14 13:39:07.875000	61.221.67.43	61.218.77.115	SMTP	108	S: 250 2.0.0 k7E5c6x04690 Message accepted for delivery
133	2006-08-14 13:39:08.375000	61.218.77.115	61.221.67.43	SMTP	60	C: QUIT
134	2006-08-14 13:39:08.375000	61.221.67.43	61.218.77.115	SMTP	112	S: 221 2.0.0 mail.diamondinfotech.com.tw closing connection
135	2006-08-14 13:39:08.390000	61.221.67.43	61.218.77.115	TCP	60	25 → 2145 [FIN, ACK] Seq=576 Ack=1973 Win=31944 Len=0

NSPA Skills – Windows VPN - Initialize

Apply a display filter ··· <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	2020-04-21 00:12:11.512107	192.168.0.7	219.100.37.137	ISAKMP	450	Identity Protection (Main Mode)
2	2020-04-21 00:12:11.561101	219.100.37.137	192.168.0.7	ISAKMP	246	Identity Protection (Main Mode)
3	2020-04-21 00:12:11.581946	192.168.0.7	219.100.37.137	ISAKMP	430	Identity Protection (Main Mode)
4	2020-04-21 00:12:11.644488	219.100.37.137	192.168.0.7	ISAKMP	398	Identity Protection (Main Mode)
5	2020-04-21 00:12:11.664715	192.168.0.7	219.100.37.137	ISAKMP	122	Identity Protection (Main Mode)
6	2020-04-21 00:12:11.711092	219.100.37.137	192.168.0.7	ISAKMP	122	Identity Protection (Main Mode)
7	2020-04-21 00:12:11.713658	192.168.0.7	219.100.37.137	ISAKMP	490	Quick Mode
8	2020-04-21 00:12:11.761515	219.100.37.137	192.168.0.7	ISAKMP	234	Quick Mode
9	2020-04-21 00:12:11.763168	192.168.0.7	219.100.37.137	ISAKMP	106	Quick Mode
10	2020-04-21 00:12:11.764467	192.168.0.7	219.100.37.137	ESP	190	ESP (SPI=0xd521c2c6)
11	2020-04-21 00:12:12.765439	192.168.0.7	219.100.37.137	ESP	190	ESP (SPI=0xd521c2c6)
12	2020-04-21 00:12:14.766713	192.168.0.7	219.100.37.137	ESP	190	ESP (SPI=0xd521c2c6)
13	2020-04-21 00:12:18.768127	192.168.0.7	219.100.37.137	ESP	190	ESP (SPI=0xd521c2c6)
14	2020-04-21 00:12:26.773484	192.168.0.7	219.100.37.137	ESP	190	ESP (SPI=0xd521c2c6)
15	2020-04-21 00:12:30.713701	192.168.0.7	219.100.37.137	UDPENCAP	43	NAT-keepalive
16	2020-04-21 00:12:36.773810	192.168.0.7	219.100.37.137	ESP	190	ESP (SPI=0xd521c2c6)
17	2020-04-21 00:12:46.790334	192.168.0.7	219.100.37.137	ISAKMP	122	Informational
18	2020-04-21 00:12:46.792013	192.168.0.7	219.100.37.137	ISAKMP	138	Informational
19	2020-04-21 00:12:46.840987	219.100.37.137	192.168.0.7	ISAKMP	122	Informational
20	2020-04-21 00:12:46.840989	219.100.37.137	192.168.0.7	ISAKMP	234	Quick Mode
21	2020-04-21 00:12:46.840990	219.100.37.137	192.168.0.7	ISAKMP	138	Informational
22	2020-04-21 00:12:46.840991	219.100.37.137	192.168.0.7	ISAKMP	122	Informational
23	2020-04-21 00:12:46.841728	219.100.37.137	192.168.0.7	ISAKMP	122	Informational

Smart Phone 網路封包範例

以下是智慧手機的範例封包，由於各種作業系統的網路行為不同，再加上不同版本的手機型號，自行修改原生系統的程式內容。同時，多樣的手機應用程式App版本，也影響其網路封包活動。

我們觀察的重點，可以聚焦在以下的主要項目：

01 **目標通訊的IP位址與國家資訊**

可以先忽略Google的IP位址, 以減少負擔。

02 **出現目標IP位址的次序**

這些次序僅左為執行Process的參考，而非絕對。

03 **反覆出現的通訊行為**

特別是不明目標位址的週期反覆行為，與連線失敗通訊的嘗試行為，都屬於異常的網路行為模式。

04 **特殊通訊服務 與 無App操作的背景通訊**

使用者沒有操作App, 確有相關通訊會傳送出去，這是需要特別注意的網路活動之一。

NSPA Skills – Smart Phone – Android(Galaxy-8)

ip

No.	Time	Source	Destination	Protocol	Length	Info
30	2019-12-26 23:48:31.464023	0.0.0.0	255.255.255.255	DHCP	354	DHCP Request - Transaction ID 0xb0c24f4d
31	2019-12-26 23:48:31.466660	192.168.123.1	255.255.255.255	DHCP	353	DHCP ACK - Transaction ID 0xb0c24f4d
32	2019-12-26 23:48:31.479985	192.168.123.1	255.255.255.255	DHCP	353	DHCP ACK - Transaction ID 0xb0c24f4d
37	2019-12-26 23:48:31.708313	192.168.123.7	192.168.123.1	DNS	89	Standard query 0xb5cf A connectivitycheck.gstatic.com
38	2019-12-26 23:48:31.708765	192.168.123.7	192.168.123.1	DNS	76	Standard query 0xb37c A time.android.com
39	2019-12-26 23:48:31.721760	192.168.123.1	192.168.123.7	DNS	105	Standard query response 0xb5cf A connectivitycheck.gstatic.com A 216.58.200.35
40	2019-12-26 23:48:31.725431	192.168.123.1	192.168.123.7	DNS	140	Standard query response 0xb37c A time.android.com A 216.239.35.4 A 216.239.35.8
41	2019-12-26 23:48:31.742579	192.168.123.7	216.239.35.4	NTP	90	NTP Version 3, client
42	2019-12-26 23:48:31.765954	216.239.35.4	192.168.123.7	NTP	90	NTP Version 3, server
43	2019-12-26 23:48:31.874376	192.168.123.7	192.168.123.1	DNS	74	Standard query 0xd1e6 A www.google.com
44	2019-12-26 23:48:31.887820	192.168.123.1	192.168.123.7	DNS	90	Standard query response 0xd1e6 A www.google.com A 172.217.27.132
45	2019-12-26 23:48:31.888979	192.168.123.7	216.58.200.35	TCP	74	43406 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 TSval=4294899633 TSe
47	2019-12-26 23:48:31.892377	192.168.123.7	172.217.27.132	TCP	74	59570 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 TSval=4294899633 TS
48	2019-12-26 23:48:31.902197	216.58.200.35	192.168.123.7	TCP	74	80 → 43406 [SYN, ACK] Seq=0 Ack=1 Win=60192 Len=0 MSS=1380 SACK_PERM=1 TSval=309
49	2019-12-26 23:48:31.904315	192.168.123.7	216.58.200.35	TCP	66	43406 → 80 [ACK] Seq=1 Ack=1 Win=87680 Len=0 TSval=4294899636 TSecr=3093963103
50	2019-12-26 23:48:31.904901	192.168.123.7	216.58.200.35	HTTP	293	GET /generate_204 HTTP/1.1
51	2019-12-26 23:48:31.908269	172.217.27.132	192.168.123.7	TCP	74	443 → 59570 [SYN, ACK] Seq=0 Ack=1 Win=60192 Len=0 MSS=1380 SACK_PERM=1 TSval=14
52	2019-12-26 23:48:31.910992	192.168.123.7	172.217.27.132	TCP	66	59570 → 443 [ACK] Seq=1 Ack=1 Win=87680 Len=0 TSval=4294899638 TSecr=1486017278
53	2019-12-26 23:48:31.919815	216.58.200.35	192.168.123.7	TCP	66	80 → 43406 [ACK] Seq=1 Ack=228 Win=61440 Len=0 TSval=3093963122 TSecr=4294899637
54	2019-12-26 23:48:31.921463	216.58.200.35	192.168.123.7	HTTP	168	HTTP/1.1 204 No Content
55	2019-12-26 23:48:31.922039	216.58.200.35	192.168.123.7	TCP	66	80 → 43406 [FIN, ACK] Seq=103 Ack=228 Win=61440 Len=0 TSval=3093963122 TSecr=429
56	2019-12-26 23:48:31.924455	192.168.123.7	216.58.200.35	TCP	66	43406 → 80 [ACK] Seq=228 Ack=103 Win=87680 Len=0 TSval=4294899641 TSecr=30939631
57	2019-12-26 23:48:31.929365	192.168.123.7	216.58.200.35	TCP	66	43406 → 80 [FIN, ACK] Seq=228 Ack=104 Win=87680 Len=0 TSval=4294899642 TSecr=309
58	2019-12-26 23:48:31.932589	192.168.123.7	172.217.27.132	TLSv1…	246	Client Hello
59	2019-12-26 23:48:31.941335	216.58.200.35	192.168.123.7	TCP	66	80 → 43406 [ACK] Seq=104 Ack=229 Win=61440 Len=0 TSval=3093963143 TSecr=42948996
60	2019-12-26 23:48:31.947098	172.217.27.132	192.168.123.7	TCP	66	443 → 59570 [ACK] Seq=1 Ack=181 Win=61440 Len=0 TSval=1486017316 TSecr=429489964
61	2019-12-26 23:48:31.950119	172.217.27.132	192.168.123.7	TLSv1…	1484	Server Hello
62	2019-12-26 23:48:31.950941	172.217.27.132	192.168.123.7	TLSv1…	1201	Certificate, Server Key Exchange, Server Hello Done
63	2019-12-26 23:48:31.952456	192.168.123.7	172.217.27.132	TCP	66	59570 → 443 [ACK] Seq=181 Ack=1419 Win=90496 Len=0 TSval=4294899649 TSecr=148601

NSPA Skills – Smart Phone – Android(Galaxy-10)

ip

No.	Time	Source	Destination	Protocol	Length	Info
18	2020-06-10 18:33:06.262004	0.0.0.0	255.255.255.255	DHCP	356	DHCP Request - Transaction ID 0x30c90cab
19	2020-06-10 18:33:06.267006	192.168.137.1	192.168.137.222	DHCP	344	DHCP ACK - Transaction ID 0x30c90cab
22	2020-06-10 18:33:06.535894	192.168.137.222	192.168.137.1	DNS	89	Standard query 0xb107 A connectivitycheck.gstatic.com
23	2020-06-10 18:33:06.659855	192.168.137.1	192.168.137.222	DNS	105	Standard query response 0xb107 A connectivitycheck.gstatic.com A 172.217.160.67
27	2020-06-10 18:33:07.536791	192.168.137.222	192.168.137.1	DNS	76	Standard query 0x33c6 A time.android.com
28	2020-06-10 18:33:07.576406	192.168.137.1	192.168.137.222	DNS	140	Standard query response 0x33c6 A time.android.com A 216.239.35.0 A 216.239.35.4
29	2020-06-10 18:33:07.581223	192.168.137.222	216.239.35.0	NTP	90	NTP Version 3, client
30	2020-06-10 18:33:07.591510	192.168.137.222	192.168.137.1	DNS	74	Standard query 0x46da A www.google.com
31	2020-06-10 18:33:07.612170	192.168.137.1	192.168.137.222	DNS	90	Standard query response 0x46da A www.google.com A 216.58.200.228
32	2020-06-10 18:33:07.657838	192.168.137.222	216.58.200.228	TCP	74	34066 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 TSval=435677218 TSe
33	2020-06-10 18:33:07.670366	192.168.137.222	172.217.160.67	TCP	74	44344 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 TSval=2305400020 TSe
34	2020-06-10 18:33:07.683281	216.58.200.228	192.168.137.222	TCP	74	443 → 34066 [SYN, ACK] Seq=0 Ack=1 Win=60192 Len=0 MSS=1380 SACK_PERM=1 TSval=23
35	2020-06-10 18:33:07.685637	192.168.137.222	216.58.200.228	TCP	66	34066 → 443 [ACK] Seq=1 Ack=1 Win=88064 Len=0 TSval=435677246 TSecr=2398965685
36	2020-06-10 18:33:07.692214	172.217.160.67	192.168.137.222	TCP	74	80 → 44344 [SYN, ACK] Seq=0 Ack=1 Win=60192 Len=0 MSS=1380 SACK_PERM=1 TSval=250
37	2020-06-10 18:33:07.703158	192.168.137.222	172.217.160.67	TCP	66	44344 → 80 [ACK] Seq=1 Ack=1 Win=88064 Len=0 TSval=2305400044 TSecr=2508557644
38	2020-06-10 18:33:07.703158	192.168.137.222	172.217.160.67	HTTP	293	GET /generate_204 HTTP/1.1
39	2020-06-10 18:33:07.724180	216.239.35.0	192.168.137.222	NTP	90	NTP Version 3, server
40	2020-06-10 18:33:07.740197	172.217.160.67	192.168.137.222	TCP	66	80 → 44344 [ACK] Seq=1 Ack=228 Win=61440 Len=0 TSval=2508557691 TSecr=2305400044
41	2020-06-10 18:33:07.740251	172.217.160.67	192.168.137.222	HTTP	168	HTTP/1.1 204 No Content
42	2020-06-10 18:33:07.740395	172.217.160.67	192.168.137.222	TCP	66	80 → 44344 [FIN, ACK] Seq=103 Ack=228 Win=61440 Len=0 TSval=2508557692 TSecr=230
43	2020-06-10 18:33:07.749064	192.168.137.222	192.168.137.1	DNS	86	Standard query 0xd411 A android.clients.google.com
44	2020-06-10 18:33:07.749064	192.168.137.222	216.58.200.228	TLSv1…	583	Client Hello
45	2020-06-10 18:33:07.752546	192.168.137.222	172.217.160.67	TCP	66	44344 → 80 [ACK] Seq=228 Ack=103 Win=88064 Len=0 TSval=2305400100 TSecr=25085576
46	2020-06-10 18:33:07.752547	192.168.137.222	172.217.160.67	TCP	66	44344 → 80 [FIN, ACK] Seq=228 Ack=104 Win=88064 Len=0 TSval=2305400102 TSecr=250
48	2020-06-10 18:33:07.772144	172.217.160.67	192.168.137.222	TCP	66	80 → 44344 [ACK] Seq=104 Ack=229 Win=61440 Len=0 TSval=2508557724 TSecr=23054001
49	2020-06-10 18:33:07.780204	192.168.137.1	192.168.137.222	DNS	206	Standard query response 0xd411 A android.clients.google.com CNAME android.l.goog
50	2020-06-10 18:33:07.783462	216.58.200.228	192.168.137.222	TCP	66	443 → 34066 [ACK] Seq=1 Ack=518 Win=61440 Len=0 TSval=2398965782 TSecr=435677304
51	2020-06-10 18:33:07.792397	216.58.200.228	192.168.137.222	TLSv1…	1448	Server Hello, Change Cipher Spec
52	2020-06-10 18:33:07.792571	216.58.200.228	192.168.137.222	TLSv1…	1315	Application Data

NSPA Skills – Smart Phone – Android(Sugar)

ip

No.	Time	Source	Destination	Protocol	Length	Info
7	2019-12-27 01:14:24.460862	0.0.0.0	255.255.255.255	DHCP	334	DHCP Request - Transaction ID 0x1e2bcef4
8	2019-12-27 01:14:24.463302	192.168.123.1	255.255.255.255	DHCP	353	DHCP ACK - Transaction ID 0x1e2bcef4
10	2019-12-27 01:14:24.480676	192.168.123.1	255.255.255.255	DHCP	353	DHCP ACK - Transaction ID 0x1e2bcef4
13	2019-12-27 01:14:24.823638	192.168.123.33	192.168.123.1	DNS	77	Standard query 0xfd0f A captive.apple.com
14	2019-12-27 01:14:24.837564	192.168.123.1	192.168.123.33	DNS	221	Standard query response 0xfd0f A captive.apple.com CNAME captive-cidr.origin-app
15	2019-12-27 01:14:24.922695	192.168.123.33	17.253.117.203	TCP	74	47436 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 TSval=4294885003 TSe
16	2019-12-27 01:14:24.927536	192.168.123.33	192.168.123.1	DNS	76	Standard query 0xf946 A time.android.com
17	2019-12-27 01:14:24.936771	17.253.117.203	192.168.123.33	TCP	74	80 → 47436 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=358
18	2019-12-27 01:14:24.939539	192.168.123.33	17.253.117.203	TCP	66	47436 → 80 [ACK] Seq=1 Ack=1 Win=87808 Len=0 TSval=4294885008 TSecr=3580618466
19	2019-12-27 01:14:24.943101	192.168.123.1	192.168.123.33	DNS	140	Standard query response 0xf946 A time.android.com A 216.239.35.0 A 216.239.35.4
20	2019-12-27 01:14:24.950033	192.168.123.33	17.253.117.203	HTTP	269	GET / HTTP/1.1
21	2019-12-27 01:14:24.964570	17.253.117.203	192.168.123.33	TCP	66	80 → 47436 [ACK] Seq=1 Ack=204 Win=30208 Len=0 TSval=3580618495 TSecr=4294885010
22	2019-12-27 01:14:24.966615	17.253.117.203	192.168.123.33	HTTP	781	HTTP/1.1 200 OK (text/html)
23	2019-12-27 01:14:24.966667	17.253.117.203	192.168.123.33	TCP	66	80 → 47436 [FIN, ACK] Seq=716 Ack=204 Win=30208 Len=0 TSval=3580618498 TSecr=429
24	2019-12-27 01:14:24.969386	192.168.123.33	17.253.117.203	TCP	66	47436 → 80 [ACK] Seq=204 Ack=716 Win=90112 Len=0 TSval=4294885017 TSecr=35806184
25	2019-12-27 01:14:24.983018	192.168.123.33	216.239.35.0	NTP	90	NTP Version 3, client
26	2019-12-27 01:14:24.996478	192.168.123.33	17.253.117.203	TCP	66	47436 → 80 [FIN, ACK] Seq=204 Ack=717 Win=90112 Len=0 TSval=4294885025 TSecr=358
27	2019-12-27 01:14:24.998880	216.239.35.0	192.168.123.33	NTP	90	NTP Version 3, server
28	2019-12-27 01:14:25.009682	17.253.117.203	192.168.123.33	TCP	66	80 → 47436 [ACK] Seq=717 Ack=205 Win=30208 Len=0 TSval=3580618540 TSecr=42948850
36	2019-12-27 01:14:30.615123	192.168.123.33	192.168.123.1	DNS	76	Standard query 0x843b A mtalk.google.com
37	2019-12-27 01:14:30.629041	192.168.123.1	192.168.123.33	DNS	121	Standard query response 0x843b A mtalk.google.com CNAME mobile-gtalk.l.google.co
38	2019-12-27 01:14:30.629325	192.168.123.1	192.168.123.33	DNS	121	Standard query response 0x843b A mtalk.google.com CNAME mobile-gtalk.l.google.co
39	2019-12-27 01:14:30.634485	192.168.123.33	192.168.123.1	ICMP	149	Destination unreachable (Port unreachable)
40	2019-12-27 01:14:30.698365	192.168.123.33	108.177.125.188	TCP	74	51688 → 5228 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 TSval=4294886735 T
41	2019-12-27 01:14:30.716136	108.177.125.188	192.168.123.33	TCP	74	5228 → 51688 [SYN, ACK] Seq=0 Ack=1 Win=62392 Len=0 MSS=1430 SACK_PERM=1 TSval=3
42	2019-12-27 01:14:30.718244	192.168.123.33	108.177.125.188	TCP	66	51688 → 5228 [ACK] Seq=1 Ack=1 Win=87808 Len=0 TSval=4294886741 TSecr=3331733654
43	2019-12-27 01:14:30.730005	192.168.123.33	108.177.125.188	TLSv1…	583	Client Hello
44	2019-12-27 01:14:30.743982	108.177.125.188	192.168.123.33	TCP	66	5228 → 51688 [ACK] Seq=1 Ack=518 Win=63488 Len=0 TSval=3331733682 TSecr=42948867
45	2019-12-27 01:14:30.745558	108.177.125.188	192.168.123.33	TLSv1…	1484	Server Hello, Change Cipher Spec

常見的異常網路封包範例

請同學開啟各個異常範例封包檔案，確定能夠顯示異常網路通訊封包的檔案目錄。

NSPA Skills – Cycle Period Connection – 固定時間循環行為-1

Apply a display filter ··· <Ctrl-/> Expression···

No.	Time	Source	Destination	Protocol	Length	Info
27	2018-11-06 15:36:09.461619	172.20.10.2	199.191.50.188	TCP	66	1698 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P
28	2018-11-06 15:36:09.729293	199.191.50.188	172.20.10.2	TCP	54	443 → 1698 [RST, ACK] Seq=1 Ack=1 Win=8212 Len=0
29	2018-11-06 15:36:10.231177	172.20.10.2	199.191.50.188	TCP	66	[TCP Retransmission] 1698 → 443 [SYN] Seq=0 Win=64240 Len=0 M
30	2018-11-06 15:36:10.691748	199.191.50.188	172.20.10.2	TCP	54	443 → 1698 [RST, ACK] Seq=1 Ack=1 Win=8212 Len=0
31	2018-11-06 15:36:11.199973	172.20.10.2	199.191.50.188	TCP	66	[TCP Retransmission] 1698 → 443 [SYN] Seq=0 Win=64240 Len=0 M
32	2018-11-06 15:36:11.490750	199.191.50.188	172.20.10.2	TCP	54	443 → 1698 [RST, ACK] Seq=1 Ack=1 Win=8212 Len=0
33	2018-11-06 15:36:11.496633	172.20.10.2	199.191.50.188	TCP	66	1699 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P
34	2018-11-06 15:36:11.719107	199.191.50.188	172.20.10.2	TCP	54	443 → 1699 [RST, ACK] Seq=1 Ack=1 Win=8212 Len=0
35	2018-11-06 15:36:12.231320	172.20.10.2	199.191.50.188	TCP	66	[TCP Retransmission] 1699 → 443 [SYN] Seq=0 Win=64240 Len=0 M
36	2018-11-06 15:36:12.604784	199.191.50.188	172.20.10.2	TCP	54	443 → 1699 [RST, ACK] Seq=1 Ack=1 Win=8212 Len=0
37	2018-11-06 15:36:13.106420	172.20.10.2	199.191.50.188	TCP	66	[TCP Retransmission] 1699 → 443 [SYN] Seq=0 Win=64240 Len=0 M
38	2018-11-06 15:36:13.347364	199.191.50.188	172.20.10.2	TCP	54	443 → 1699 [RST, ACK] Seq=1 Ack=1 Win=8212 Len=0
39	2018-11-06 15:36:14.369177	172.20.10.2	199.191.50.188	TCP	66	1700 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P
40	2018-11-06 15:36:14.586107	199.191.50.188	172.20.10.2	TCP	54	443 → 1700 [RST, ACK] Seq=1 Ack=1 Win=8212 Len=0
41	2018-11-06 15:36:15.090981	172.20.10.2	199.191.50.188	TCP	66	[TCP Retransmission] 1700 → 443 [SYN] Seq=0 Win=64240 Len=0 M
42	2018-11-06 15:36:15.320910	199.191.50.188	172.20.10.2	TCP	54	443 → 1700 [RST, ACK] Seq=1 Ack=1 Win=8212 Len=0
43	2018-11-06 15:36:15.825510	172.20.10.2	199.191.50.188	TCP	66	[TCP Retransmission] 1700 → 443 [SYN] Seq=0 Win=64240 Len=0 M
44	2018-11-06 15:36:16.117045	199.191.50.188	172.20.10.2	TCP	54	443 → 1700 [RST, ACK] Seq=1 Ack=1 Win=8212 Len=0
45	2018-11-06 15:36:16.122993	172.20.10.2	199.191.50.188	TCP	66	1701 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P
46	2018-11-06 15:36:16.336733	199.191.50.188	172.20.10.2	TCP	54	443 → 1701 [RST, ACK] Seq=1 Ack=1 Win=8212 Len=0
47	2018-11-06 15:36:16.841254	172.20.10.2	199.191.50.188	TCP	66	[TCP Retransmission] 1701 → 443 [SYN] Seq=0 Win=64240 Len=0 M
48	2018-11-06 15:36:17.087251	199.191.50.188	172.20.10.2	TCP	54	443 → 1701 [RST, ACK] Seq=1 Ack=1 Win=8212 Len=0
49	2018-11-06 15:36:17.591412	172.20.10.2	199.191.50.188	TCP	66	[TCP Retransmission] 1701 → 443 [SYN] Seq=0 Win=64240 Len=0 M
50	2018-11-06 15:36:17.839690	199.191.50.188	172.20.10.2	TCP	54	443 → 1701 [RST, ACK] Seq=1 Ack=1 Win=8212 Len=0
51	2018-11-06 15:36:18.874739	172.20.10.2	199.191.50.188	TCP	66	1702 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P

NSPA Skills – Mass SYN Connection – Port Scan

Apply a display filter ··· <Ctrl-/> Expression···

No.	Time	Source	Destination	Protocol	Length	Info
611	2019-08-19 15:36:43.809608	192.168.201.59	192.168.201.51	TCP	66	58630 → 542 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
612	2019-08-19 15:36:43.825107	192.168.201.59	192.168.201.51	TCP	66	58631 → 543 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
613	2019-08-19 15:36:43.840527	192.168.201.59	192.168.201.51	TCP	66	58632 → 544 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
614	2019-08-19 15:36:43.856262	192.168.201.59	192.168.201.51	TCP	66	58633 → 545 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
615	2019-08-19 15:36:43.871676	192.168.201.59	192.168.201.51	TCP	66	58634 → 546 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
616	2019-08-19 15:36:43.887381	192.168.201.59	192.168.201.51	TCP	66	58635 → 547 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
617	2019-08-19 15:36:43.902939	192.168.201.59	192.168.201.51	TCP	66	58636 → 548 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
618	2019-08-19 15:36:43.919056	192.168.201.59	192.168.201.51	TCP	66	58637 → 549 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
619	2019-08-19 15:36:44.199965	192.168.201.59	192.168.201.51	TCP	66	58638 → 550 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
620	2019-08-19 15:36:44.215972	192.168.201.59	192.168.201.51	TCP	66	58639 → 551 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
621	2019-08-19 15:36:44.231758	192.168.201.59	192.168.201.51	TCP	66	58640 → 552 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
622	2019-08-19 15:36:44.247466	192.168.201.59	192.168.201.51	TCP	66	58641 → 553 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
623	2019-08-19 15:36:44.262549	192.168.201.59	192.168.201.51	TCP	66	58642 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
624	2019-08-19 15:36:44.278098	192.168.201.59	192.168.201.51	TCP	66	58643 → 555 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
625	2019-08-19 15:36:44.293955	192.168.201.59	192.168.201.51	TCP	66	58644 → 556 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
626	2019-08-19 15:36:44.309340	192.168.201.59	192.168.201.51	TCP	66	58645 → 557 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
627	2019-08-19 15:36:44.325053	192.168.201.59	192.168.201.51	TCP	66	58646 → 558 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
628	2019-08-19 15:36:44.340585	192.168.201.59	192.168.201.51	TCP	66	58647 → 559 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
629	2019-08-19 15:36:44.357002	192.168.201.59	192.168.201.51	TCP	66	58648 → 560 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
630	2019-08-19 15:36:44.371813	192.168.201.59	192.168.201.51	TCP	66	58649 → 561 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
631	2019-08-19 15:36:44.387511	192.168.201.59	192.168.201.51	TCP	66	58650 → 562 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
632	2019-08-19 15:36:44.403201	192.168.201.59	192.168.201.51	TCP	66	58651 → 563 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
633	2019-08-19 15:36:44.419531	192.168.201.59	192.168.201.51	TCP	66	58652 → 564 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
634	2019-08-19 15:36:44.434129	192.168.201.59	192.168.201.51	TCP	66	58653 → 565 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
635	2019-08-19 15:36:45.699878	192.168.201.59	192.168.201.51	TCP	66	58654 → 566 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256

NSPA Skills – Mass SYN Connection – Port Scan

Apply a display filter ··· <Ctrl-/> Expression···

No.	Time	Source	Destination	Protocol	Length	Info
378	2019-08-19 15:42:36.237565	192.168.201.59	61.222.173.42	TCP	66	61677 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
379	2019-08-19 15:42:36.253124	192.168.201.59	61.222.173.42	TCP	66	61678 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
380	2019-08-19 15:42:36.269173	192.168.201.59	61.222.173.42	TCP	66	61679 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
381	2019-08-19 15:42:36.284358	192.168.201.59	61.222.173.42	TCP	66	61680 → 119 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
382	2019-08-19 15:42:36.300486	192.168.201.59	61.222.173.42	TCP	66	61681 → 6588 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=25
383	2019-08-19 15:42:36.332256	192.168.201.59	61.222.173.43	TCP	66	61682 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
384	2019-08-19 15:42:36.346936	192.168.201.59	61.222.173.43	TCP	66	61683 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
385	2019-08-19 15:42:36.362402	192.168.201.59	61.222.173.43	TCP	66	61684 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
386	2019-08-19 15:42:36.378165	192.168.201.59	61.222.173.43	TCP	66	61685 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
387	2019-08-19 15:42:36.394072	192.168.201.59	61.222.173.43	TCP	66	61686 → 119 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
388	2019-08-19 15:42:36.412268	192.168.201.59	61.222.173.43	TCP	66	61687 → 6588 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=25
389	2019-08-19 15:42:36.707545	192.168.201.59	61.222.173.44	TCP	66	61688 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
390	2019-08-19 15:42:36.721848	192.168.201.59	61.222.173.44	TCP	66	61689 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
391	2019-08-19 15:42:36.737497	192.168.201.59	61.222.173.44	TCP	66	61690 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
392	2019-08-19 15:42:36.753524	192.168.201.59	61.222.173.44	TCP	66	61691 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
393	2019-08-19 15:42:36.769133	192.168.201.59	61.222.173.44	TCP	66	61692 → 119 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
394	2019-08-19 15:42:36.785066	192.168.201.59	61.222.173.44	TCP	66	61693 → 6588 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=25
395	2019-08-19 15:42:36.816311	192.168.201.59	61.222.173.45	TCP	66	61694 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
396	2019-08-19 15:42:36.832942	192.168.201.59	61.222.173.45	TCP	66	61695 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
397	2019-08-19 15:42:36.849462	192.168.201.59	61.222.173.45	TCP	66	61696 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
398	2019-08-19 15:42:36.862587	192.168.201.59	61.222.173.45	TCP	66	61697 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
399	2019-08-19 15:42:36.877814	192.168.201.59	61.222.173.45	TCP	66	61698 → 119 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
400	2019-08-19 15:42:36.894338	192.168.201.59	61.222.173.45	TCP	66	61699 → 6588 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=25
401	2019-08-19 15:42:36.926402	192.168.201.59	61.222.173.46	TCP	66	61700 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
402	2019-08-19 15:42:36.940445	192.168.201.59	61.222.173.46	TCP	66	61701 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256

NSPA Skills – Mass SYN Connection – Malware Infection

Apply a display filter ··· <Ctrl-/> Expression···

No.	Time	Source	Destination	Protocol	Length	Info
117	2017-11-10 12:28:56.414841	10.0.1.10	10.50.57.161	TCP	66	50198 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
118	2017-11-10 12:28:56.414841	10.0.1.10	10.50.77.52	TCP	66	50197 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
119	2017-11-10 12:28:56.414841	10.0.1.10	10.48.101.26	TCP	66	50199 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
120	2017-11-10 12:28:56.414841	10.0.1.10	10.49.139.33	TCP	66	50200 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
121	2017-11-10 12:28:56.414994	10.0.1.10	10.48.12.17	TCP	66	50201 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
122	2017-11-10 12:28:56.414994	10.0.1.10	10.51.15.35	TCP	66	50202 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
123	2017-11-10 12:28:56.414999	10.0.1.10	10.49.173.57	TCP	66	50203 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
124	2017-11-10 12:28:56.414999	10.0.1.10	10.50.135.45	TCP	66	50204 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
125	2017-11-10 12:28:56.415115	10.0.1.10	10.48.16.90	TCP	66	50205 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
126	2017-11-10 12:28:57.428854	10.0.1.10	10.50.137.23	TCP	66	50207 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
127	2017-11-10 12:28:57.428854	10.0.1.10	10.49.212.192	TCP	66	50206 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
128	2017-11-10 12:28:57.428923	10.0.1.10	10.49.166.22	TCP	66	50210 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
129	2017-11-10 12:28:57.428923	10.0.1.10	10.50.129.54	TCP	66	50209 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
130	2017-11-10 12:28:57.428924	10.0.1.10	10.49.141.91	TCP	66	50208 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
131	2017-11-10 12:28:57.428988	10.0.1.10	10.49.210.130	TCP	66	50211 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
132	2017-11-10 12:28:57.429033	10.0.1.10	10.49.165.133	TCP	66	50212 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
133	2017-11-10 12:28:57.429050	10.0.1.10	10.49.175.187	TCP	66	50214 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
134	2017-11-10 12:28:57.429050	10.0.1.10	10.48.16.215	TCP	66	50213 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
135	2017-11-10 12:28:58.442851	10.0.1.10	10.49.67.100	TCP	66	50216 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
136	2017-11-10 12:28:58.442850	10.0.1.10	10.49.212.69	TCP	66	50215 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
137	2017-11-10 12:28:58.442851	10.0.1.10	10.50.63.72	TCP	66	50218 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
138	2017-11-10 12:28:58.442851	10.0.1.10	10.59.4.34	TCP	66	50217 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
139	2017-11-10 12:28:58.442967	10.0.1.10	10.50.21.46	TCP	66	50219 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
140	2017-11-10 12:28:58.442967	10.0.1.10	10.49.166.62	TCP	66	50220 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
141	2017-11-10 12:28:58.442992	10.0.1.10	10.49.173.31	TCP	66	50222 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1

NSPA Skills – Mass SYN Connection – P2P Initialize

Apply a display filter ··· <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
27	2006-08-19 17:42:10.593000	218.167.20.84	219.73.7.23	TCP	70	4050 → 2582 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM=1
28	2006-08-19 17:42:10.609000	218.167.20.84	124.155.137.252	TCP	70	4051 → 4383 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM=1
29	2006-08-19 17:42:10.609000	218.167.20.84	59.117.66.95	TCP	70	4052 → 17956 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM=1
30	2006-08-19 17:42:10.625000	218.167.20.84	61.229.218.59	TCP	70	4053 → 3554 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM=1
31	2006-08-19 17:42:10.625000	218.167.20.84	203.218.107.146	TCP	70	4054 → 12183 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM=1
32	2006-08-19 17:42:10.640000	218.167.20.84	218.175.183.174	TCP	70	4055 → 20383 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM=1
33	2006-08-19 17:42:10.640000	218.167.20.84	61.64.117.27	TCP	70	4056 → 24314 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM=1
34	2006-08-19 17:42:10.656000	218.167.20.84	59.113.189.155	TCP	70	4057 → 15801 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM=1
35	2006-08-19 17:42:10.656000	218.167.20.84	60.198.135.231	TCP	70	4058 → 10476 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM=1
36	2006-08-19 17:42:10.656000	218.167.20.84	222.94.246.62	TCP	70	4059 → 16327 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM=1
37	2006-08-19 17:42:10.656000	218.167.20.84	59.112.234.144	TCP	70	4060 → 6156 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM=1
38	2006-08-19 17:42:10.671000	218.167.20.84	219.79.231.252	TCP	70	4061 → 14695 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM=1
39	2006-08-19 17:42:10.671000	218.167.20.84	219.79.164.70	TCP	70	4062 → 11687 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM=1
40	2006-08-19 17:42:10.671000	218.167.20.84	61.244.129.6	TCP	70	4063 → 22702 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM=1
41	2006-08-19 17:42:10.687000	218.167.20.84	203.218.201.106	TCP	70	4064 → 14340 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM=1
42	2006-08-19 17:42:10.687000	218.167.20.84	218.253.151.111	TCP	70	4065 → 7238 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM=1
43	2006-08-19 17:42:10.687000	218.167.20.84	218.167.184.197	TCP	70	4066 → 3439 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM=1
44	2006-08-19 17:42:10.687000	218.167.20.84	220.131.165.216	TCP	70	4067 → 14540 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM=1
45	2006-08-19 17:42:10.703000	218.167.20.84	218.102.175.105	TCP	70	4068 → 5258 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM=1
46	2006-08-19 17:42:10.703000	218.167.20.84	218.161.97.178	TCP	70	4069 → 5100 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM=1
47	2006-08-19 17:42:10.703000	218.167.20.84	203.218.190.59	TCP	70	4070 → 5192 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM=1
48	2006-08-19 17:42:10.703000	218.167.20.84	210.242.221.204	TCP	70	4071 → 12161 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM=1
49	2006-08-19 17:42:10.718000	218.167.20.84	218.170.195.162	TCP	70	4072 → 5472 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM=1
50	2006-08-19 17:42:10.718000	218.167.20.84	125.232.0.213	TCP	70	4073 → 5100 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM=1
51	2006-08-19 17:42:10.718000	218.167.20.84	218.162.93.96	TCP	70	4074 → 10041 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM=1
52	2006-08-19 17:42:10.734000	218.167.20.84	218.160.158.25	TCP	70	4075 → 7371 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM=1
53	2006-08-19 17:42:10.734000	218.167.20.84	220.142.193.67	TCP	70	4076 → 8359 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM=1
54	2006-08-19 17:42:10.734000	218.167.20.84	219.84.74.98	TCP	70	4077 → 10962 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM=1
55	2006-08-19 17:42:10.734000	218.167.20.84	218.167.205.234	TCP	70	4078 → 3615 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM=1

NSPA Skills – Mass RST ACK – Port Scan (Firewall Rejected)

Apply a display filter ··· <Ctrl-/> Expression···

No.	Time	Source	Destination	Protocol	Length	Info
1132	2019-08-19 15:43:27.037682	61.222.173.87	192.168.201.59	TCP	60	21 → 61946 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1133	2019-08-19 15:43:27.037924	61.222.173.86	192.168.201.59	TCP	60	6588 → 61945 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1134	2019-08-19 15:43:27.037925	61.222.173.87	192.168.201.59	TCP	60	110 → 61949 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1135	2019-08-19 15:43:27.037926	61.222.173.87	192.168.201.59	TCP	60	25 → 61947 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1136	2019-08-19 15:43:27.037927	61.222.173.87	192.168.201.59	TCP	60	80 → 61948 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1137	2019-08-19 15:43:27.037928	61.222.173.87	192.168.201.59	TCP	60	119 → 61950 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1138	2019-08-19 15:43:27.037929	61.222.173.88	192.168.201.59	TCP	60	6588 → 61957 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1139	2019-08-19 15:43:27.037930	61.222.173.88	192.168.201.59	TCP	60	25 → 61953 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1140	2019-08-19 15:43:27.037931	61.222.173.88	192.168.201.59	TCP	60	21 → 61952 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1141	2019-08-19 15:43:27.038153	61.222.173.87	192.168.201.59	TCP	60	6588 → 61951 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1142	2019-08-19 15:43:27.038155	61.222.173.88	192.168.201.59	TCP	60	80 → 61954 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1143	2019-08-19 15:43:27.038155	61.222.173.88	192.168.201.59	TCP	60	119 → 61956 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1144	2019-08-19 15:43:27.038157	61.222.173.88	192.168.201.59	TCP	60	110 → 61955 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1145	2019-08-19 15:43:27.574551	61.222.173.89	192.168.201.59	TCP	60	21 → 61958 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1146	2019-08-19 15:43:27.574553	61.222.173.89	192.168.201.59	TCP	60	80 → 61960 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1147	2019-08-19 15:43:27.574554	61.222.173.89	192.168.201.59	TCP	60	25 → 61959 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1148	2019-08-19 15:43:27.574724	61.222.173.89	192.168.201.59	TCP	60	119 → 61962 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1149	2019-08-19 15:43:27.574726	61.222.173.89	192.168.201.59	TCP	60	110 → 61961 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1150	2019-08-19 15:43:28.648254	61.222.173.89	192.168.201.59	TCP	60	6588 → 61963 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1151	2019-08-19 15:43:28.648391	61.222.173.90	192.168.201.59	TCP	60	21 → 61964 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1152	2019-08-19 15:43:28.648393	61.222.173.90	192.168.201.59	TCP	60	25 → 61965 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1153	2019-08-19 15:43:29.185136	61.222.173.90	192.168.201.59	TCP	60	110 → 61967 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1154	2019-08-19 15:43:29.185137	61.222.173.90	192.168.201.59	TCP	60	80 → 61966 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1155	2019-08-19 15:43:29.185273	61.222.173.90	192.168.201.59	TCP	60	6588 → 61969 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1156	2019-08-19 15:43:29.185274	61.222.173.90	192.168.201.59	TCP	60	119 → 61968 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

NSPA Skills – Download Malware – 偽裝於HTTP的惡意下載過程

Apply a display filter ··· <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
249	2019-01-11 13:55:29.589441	192.168.1.14	168.95.1.1	DNS	76	Standard query 0xb425 A lipertekstil.com
250	2019-01-11 13:55:29.621930	QnoTechn_00:61:cf	Broadcast	ARP	60	192.168.1.1 is at 00:17:16:00:61:cf
251	2019-01-11 13:55:29.927133	168.95.1.1	192.168.1.14	DNS	92	Standard query response 0xb425 A lipertekstil.com A 94.73.146.142
252	2019-01-11 13:55:29.945409	192.168.1.14	94.73.146.142	TCP	66	50098 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
253	2019-01-11 13:55:30.003265	ZyxelCom_07:61:f1	IPv4mcast_7f:ff:…	LOOP	64	No valid function found
254	2019-01-11 13:55:30.023017	ZyxelCom_07:61:f1	IPv4mcast_7f:ff:…	LOOP	64	No valid function found
255	2019-01-11 13:55:30.122020	QnoTechn_00:61:cf	Broadcast	ARP	60	192.168.1.1 is at 00:17:16:00:61:cf
256	2019-01-11 13:55:30.300331	94.73.146.142	192.168.1.14	TCP	66	80 → 50098 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1460 WS=16 SA
257	2019-01-11 13:55:30.300451	192.168.1.14	94.73.146.142	TCP	54	50098 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
258	2019-01-11 13:55:30.329641	192.168.1.14	94.73.146.142	HTTP	403	GET /imza/sserv.jpg HTTP/1.1
259	2019-01-11 13:55:30.621973	QnoTechn_00:61:cf	Broadcast	ARP	60	192.168.1.1 is at 00:17:16:00:61:cf
260	2019-01-11 13:55:30.685621	94.73.146.142	192.168.1.14	TCP	60	80 → 50098 [ACK] Seq=1 Ack=350 Win=30336 Len=0
261	2019-01-11 13:55:30.687010	94.73.146.142	192.168.1.14	HTTP	1029	HTTP/1.1 404 Not Found (text/html)
262	2019-01-11 13:55:30.699543	192.168.1.14	168.95.1.1	DNS	83	Standard query 0x7591 A drseymacelikgulecol.com
263	2019-01-11 13:55:30.887461	192.168.1.14	94.73.146.142	TCP	54	50098 → 80 [ACK] Seq=350 Ack=976 Win=64724 Len=0
264	2019-01-11 13:55:30.899546	168.95.1.1	192.168.1.14	DNS	99	Standard query response 0x7591 A drseymacelikgulecol.com A 94.73.1
265	2019-01-11 13:55:30.902729	192.168.1.14	94.73.144.214	TCP	66	50099 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
266	2019-01-11 13:55:31.023874	ZyxelCom_07:61:f1	IPv4mcast_7f:ff:…	LOOP	64	No valid function found
267	2019-01-11 13:55:31.025585	ZyxelCom_07:61:f1	IPv4mcast_7f:ff:…	LOOP	64	No valid function found
268	2019-01-11 13:55:31.122104	QnoTechn_00:61:cf	Broadcast	ARP	60	192.168.1.1 is at 00:17:16:00:61:cf
269	2019-01-11 13:55:31.208331	94.73.144.214	192.168.1.14	TCP	66	80 → 50099 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1460 WS=16 SA
270	2019-01-11 13:55:31.208441	192.168.1.14	94.73.144.214	TCP	54	50099 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
271	2019-01-11 13:55:31.208613	192.168.1.14	94.73.144.214	HTTP	448	GET /wp-content/themes/better-health/assets/css/sserv.jpg HTTP/1.1
272	2019-01-11 13:55:31.406598	5.135.104.98	192.168.1.14	TCP	60	80 → 50096 [FIN, ACK] Seq=197 Ack=454 Win=65664 Len=0
273	2019-01-11 13:55:31.406683	192.168.1.14	5.135.104.98	TCP	54	50096 → 80 [ACK] Seq=454 Ack=198 Win=65504 Len=0
274	2019-01-11 13:55:31.513372	94.73.144.214	192.168.1.14	TCP	60	80 → 50099 [ACK] Seq=1 Ack=395 Win=30336 Len=0
275	2019-01-11 13:55:31.516140	94.73.144.214	192.168.1.14	TCP	351	80 → 50099 [PSH, ACK] Seq=1 Ack=395 Win=30336 Len=297 [TCP segment
276	2019-01-11 13:55:31.525777	94.73.144.214	192.168.1.14	TCP	1514	80 → 50099 [ACK] Seq=298 Ack=395 Win=30336 Len=1460 [TCP segment o
277	2019-01-11 13:55:31.525836	192.168.1.14	94.73.144.214	TCP	54	50099 → 80 [ACK] Seq=395 Ack=1758 Win=65700 Len=0

NSPA Skills – Web Behavior – Web CGI Scanning

Apply a display filter ··· <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
571	2006-08-16 10:11:44.554000	172.16.1.184	59.120.215.160	TCP	62	3277 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
572	2006-08-16 10:11:44.634000	172.16.1.184	59.120.215.160	TCP	54	3277 → 80 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
573	2006-08-16 10:11:44.705000	172.16.1.184	59.120.215.160	TCP	62	3278 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
574	2006-08-16 10:11:44.735000	59.120.215.160	172.16.1.184	TCP	60	80 → 3277 [ACK] Seq=1 Ack=2 Win=17520 Len=0
575	2006-08-16 10:11:44.755000	59.120.215.160	172.16.1.184	TCP	60	80 → 3277 [FIN, ACK] Seq=1 Ack=2 Win=17520 Len=0
576	2006-08-16 10:11:44.825000	59.120.215.160	172.16.1.184	TCP	62	80 → 3278 [SYN, ACK] Seq=0 Ack=1 Win=17520 Len=0 MSS=1460 SACK_PER
577	2006-08-16 10:11:44.845000	172.16.1.184	59.120.215.160	HTTP	117	GET ///modules.php?name=Members_List&&sql_debug=1 HTTP/1.0
578	2006-08-16 10:11:44.915000	59.120.215.160	172.16.1.184	TCP	1514	80 → 3278 [ACK] Seq=1 Ack=64 Win=17457 Len=1460 [TCP segment of a
579	2006-08-16 10:11:45.125000	59.120.215.160	172.16.1.184	TCP	1514	80 → 3278 [ACK] Seq=1461 Ack=64 Win=17457 Len=1460 [TCP segment of
580	2006-08-16 10:11:45.165000	172.16.1.184	59.120.215.160	TCP	54	3278 → 80 [FIN, ACK] Seq=64 Ack=2921 Win=65535 Len=0
581	2006-08-16 10:11:45.185000	59.120.215.160	172.16.1.184	HTTP	1104	HTTP/1.1 404 Object Not Found (text/html)
582	2006-08-16 10:11:45.265000	172.16.1.184	59.120.215.160	TCP	62	3279 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
583	2006-08-16 10:11:45.335000	59.120.215.160	172.16.1.184	TCP	62	80 → 3279 [SYN, ACK] Seq=0 Ack=1 Win=17520 Len=0 MSS=1460 SACK_PER
584	2006-08-16 10:11:45.355000	172.16.1.184	59.120.215.160	HTTP	182	GET ///quote.html?filename=../../../../../../../../../../../../../
585	2006-08-16 10:11:45.426000	59.120.215.160	172.16.1.184	TCP	1514	80 → 3279 [ACK] Seq=1 Ack=129 Win=17392 Len=1460 [TCP segment of a
586	2006-08-16 10:11:45.456000	59.120.215.160	172.16.1.184	TCP	1514	80 → 3279 [ACK] Seq=1461 Ack=129 Win=17392 Len=1460 [TCP segment o
587	2006-08-16 10:11:45.526000	172.16.1.184	59.120.215.160	TCP	54	3279 → 80 [FIN, ACK] Seq=129 Ack=2921 Win=65535 Len=0
588	2006-08-16 10:11:45.546000	59.120.215.160	172.16.1.184	HTTP	1104	HTTP/1.1 404 Object Not Found (text/html)
589	2006-08-16 10:11:45.566000	172.16.1.184	59.120.215.160	TCP	62	3280 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
590	2006-08-16 10:11:45.646000	59.120.215.160	172.16.1.184	TCP	60	80 → 3279 [ACK] Seq=3972 Ack=130 Win=17392 Len=0
591	2006-08-16 10:11:45.666000	59.120.215.160	172.16.1.184	TCP	62	80 → 3280 [SYN, ACK] Seq=0 Ack=1 Win=17520 Len=0 MSS=1460 SACK_PER
592	2006-08-16 10:11:45.686000	172.16.1.184	59.120.215.160	HTTP	80	HEAD /ROADS/ HTTP/1.0
593	2006-08-16 10:11:45.756000	59.120.215.160	172.16.1.184	HTTP	198	HTTP/1.1 404 Object Not Found
594	2006-08-16 10:11:45.786000	172.16.1.184	59.120.215.160	TCP	54	[TCP ACKed unseen segment] 3280 → 80 [FIN, ACK] Seq=27 Ack=146 Win
595	2006-08-16 10:11:45.856000	59.120.215.160	172.16.1.184	TCP	60	[TCP Previous segment not captured] 80 → 3280 [ACK] Seq=146 Ack=28
596	2006-08-16 10:11:45.876000	172.16.1.184	59.120.215.160	TCP	62	3281 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
597	2006-08-16 10:11:45.956000	59.120.215.160	172.16.1.184	TCP	62	80 → 3281 [SYN, ACK] Seq=0 Ack=1 Win=17520 Len=0 MSS=1460 SACK_PER
598	2006-08-16 10:11:45.976000	172.16.1.184	59.120.215.160	HTTP	98	GET ///php/php.exe?c:\boot.ini HTTP/1.0
599	2006-08-16 10:11:46.046000	59.120.215.160	172.16.1.184	TCP	1514	80 → 3281 [ACK] Seq=1 Ack=45 Win=17476 Len=1460 [TCP segment of a

NSPA Skills – Web Behavior – SQL Injection

Apply a display filter ··· <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
8	2015-05-25 10:15:43.932000	10.10.1.50	10.10.1.100	HTTP	266	GET /EmployeesY.asp?City=London'%20%20And%20char(94)%2Bdb_name()%2B
9	2015-05-25 10:15:43.934000	10.10.1.100	10.10.1.50	HTTP	1170	HTTP/1.1 500 Internal Server Error (text/html)
10	2015-05-25 10:15:43.936000	10.10.1.100	10.10.1.50	HTTP	1181	HTTP/1.1 500 Internal Server Error (text/html)
11	2015-05-25 10:15:44.038000	10.10.1.50	10.10.1.100	HTTP	241	HEAD /EmployeesY.asp?City=London';declare%20@a%20int-- HTTP/1.1
12	2015-05-25 10:15:44.038000	10.10.1.100	10.10.1.50	HTTP	297	HTTP/1.1 200 OK
13	2015-05-25 10:15:57.659000	10.10.1.50	10.10.1.100	HTTP	270	HEAD /EmployeesY.asp?City=London;create%20table%20t_jiaozhu(jiaozhu
14	2015-05-25 10:15:57.660000	10.10.1.100	10.10.1.50	HTTP	297	HTTP/1.1 200 OK
15	2015-05-25 10:15:58.168000	10.10.1.50	10.10.1.100	HTTP	257	GET /EmployeesY.asp?City=London'%20and(char(94)%2Buser%2Bchar(94))>
16	2015-05-25 10:15:58.169000	10.10.1.100	10.10.1.50	HTTP	1170	HTTP/1.1 500 Internal Server Error (text/html)
17	2015-05-25 10:15:58.221000	10.10.1.50	10.10.1.100	HTTP	311	GET /EmployeesY.asp?City=London'%20%20And%20(char(94)%2Bcast(IS_SRV
18	2015-05-25 10:15:58.222000	10.10.1.50	10.10.1.100	HTTP	261	GET /EmployeesY.asp?City=London'%20%20And%20char(94)%2Buser%2Bchar(
19	2015-05-25 10:15:58.229000	10.10.1.100	10.10.1.50	HTTP	1213	HTTP/1.1 500 Internal Server Error (text/html)
20	2015-05-25 10:15:58.231000	10.10.1.50	10.10.1.100	HTTP	266	GET /EmployeesY.asp?City=London'%20%20And%20char(94)%2Bdb_name()%2B
21	2015-05-25 10:15:58.233000	10.10.1.100	10.10.1.50	HTTP	1170	HTTP/1.1 500 Internal Server Error (text/html)
22	2015-05-25 10:15:58.234000	10.10.1.100	10.10.1.50	HTTP	1181	HTTP/1.1 500 Internal Server Error (text/html)
23	2015-05-25 10:15:58.386000	10.10.1.50	10.10.1.100	HTTP	241	HEAD /EmployeesY.asp?City=London';declare%20@a%20int-- HTTP/1.1
24	2015-05-25 10:15:58.388000	10.10.1.100	10.10.1.50	HTTP	297	HTTP/1.1 200 OK
25	2015-05-25 10:16:09.201000	10.10.1.50	10.10.1.100	HTTP	270	HEAD /EmployeesY.asp?City=London;create%20table%20t_jiaozhu(jiaozhu
26	2015-05-25 10:16:09.202000	10.10.1.100	10.10.1.50	HTTP	297	HTTP/1.1 200 OK
27	2015-05-25 10:16:09.757000	10.10.1.50	10.10.1.100	HTTP	257	GET /EmployeesY.asp?City=London'%20and(char(94)%2Buser%2Bchar(94))>
28	2015-05-25 10:16:09.758000	10.10.1.100	10.10.1.50	HTTP	1170	HTTP/1.1 500 Internal Server Error (text/html)
29	2015-05-25 10:16:09.809000	10.10.1.50	10.10.1.100	HTTP	311	GET /EmployeesY.asp?City=London'%20%20And%20(char(94)%2Bcast(IS_SRV
30	2015-05-25 10:16:09.810000	10.10.1.50	10.10.1.100	HTTP	261	GET /EmployeesY.asp?City=London'%20%20And%20char(94)%2Buser%2Bchar(
31	2015-05-25 10:16:09.813000	10.10.1.100	10.10.1.50	HTTP	1213	HTTP/1.1 500 Internal Server Error (text/html)
32	2015-05-25 10:16:09.814000	10.10.1.50	10.10.1.100	HTTP	266	GET /EmployeesY.asp?City=London'%20%20And%20char(94)%2Bdb_name()%2B
33	2015-05-25 10:16:09.815000	10.10.1.100	10.10.1.50	HTTP	1170	HTTP/1.1 500 Internal Server Error (text/html)
34	2015-05-25 10:16:09.816000	10.10.1.100	10.10.1.50	HTTP	1181	HTTP/1.1 500 Internal Server Error (text/html)
35	2015-05-25 10:16:09.919000	10.10.1.50	10.10.1.100	HTTP	241	HEAD /EmployeesY.asp?City=London';declare%20@a%20int-- HTTP/1.1
36	2015-05-25 10:16:09.920000	10.10.1.100	10.10.1.50	HTTP	297	HTTP/1.1 200 OK

NSPA Skills – Malware Infected – 連接C&C Host 的失敗-1

Apply a display filter ··· <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
280	2019-08-09 21:57:20.641787	192.168.0.2	224.0.0.251	MDNS	168	Standard query 0x0016 PTR _%9E5E7C8F47989526C9BCD95D24084F6F0E
281	2019-08-09 21:57:20.664172	192.168.0.3	224.0.0.251	MDNS	420	Standard query response 0x0000 PTR Google-Home-bd921514bdaca0
282	2019-08-09 21:57:20.664174	192.168.0.3	224.0.0.251	MDNS	405	Standard query response 0x0000 PTR Google-Home-bd921514bdaca0
283	2019-08-09 21:57:28.545063	192.168.0.5	95.168.185.183	TCP	66	55523 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P
284	2019-08-09 21:57:28.823864	95.168.185.183	192.168.0.5	TCP	54	80 → 55523 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
285	2019-08-09 21:57:29.325107	192.168.0.5	95.168.185.183	TCP	66	[TCP Retransmission] 55523 → 80 [SYN] Seq=0 Win=64240 Len=0 M
286	2019-08-09 21:57:29.622992	95.168.185.183	192.168.0.5	TCP	54	80 → 55523 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
287	2019-08-09 21:57:30.123068	192.168.0.5	95.168.185.183	TCP	66	[TCP Retransmission] 55523 → 80 [SYN] Seq=0 Win=64240 Len=0 M
288	2019-08-09 21:57:30.402982	95.168.185.183	192.168.0.5	TCP	54	80 → 55523 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
289	2019-08-09 21:57:33.319340	LiteonTe_44:e0:15	D-LinkIn_e2:73:a2	ARP	42	Who has 192.168.0.1? Tell 192.168.0.5
290	2019-08-09 21:57:33.321207	D-LinkIn_e2:73:a2	LiteonTe_44:e0:15	ARP	42	192.168.0.1 is at 74:da:da:e2:73:a2
291	2019-08-09 21:57:40.472591	192.168.0.2	224.0.0.251	MDNS	168	Standard query 0x0017 PTR _%9E5E7C8F47989526C9BCD95D24084F6F0E
292	2019-08-09 21:57:40.475193	192.168.0.3	224.0.0.251	MDNS	420	Standard query response 0x0000 PTR Google-Home-bd921514bdaca0
293	2019-08-09 21:57:40.475194	192.168.0.3	224.0.0.251	MDNS	405	Standard query response 0x0000 PTR Google-Home-bd921514bdaca0
294	2019-08-09 21:58:00.484919	192.168.0.2	224.0.0.251	MDNS	168	Standard query 0x0018 PTR _%9E5E7C8F47989526C9BCD95D24084F6F0E
295	2019-08-09 21:58:00.487706	192.168.0.3	224.0.0.251	MDNS	420	Standard query response 0x0000 PTR Google-Home-bd921514bdaca0
296	2019-08-09 21:58:00.487717	192.168.0.3	224.0.0.251	MDNS	405	Standard query response 0x0000 PTR Google-Home-bd921514bdaca0
297	2019-08-09 21:58:00.888122	192.168.0.5	203.104.150.2	TLSv1.2	95	Application Data
298	2019-08-09 21:58:00.930023	203.104.150.2	192.168.0.5	TLSv1.2	95	Application Data
299	2019-08-09 21:58:00.970585	192.168.0.5	203.104.150.2	TCP	54	54242 → 443 [ACK] Seq=370 Ack=370 Win=253 Len=0
300	2019-08-09 21:58:04.492390	192.168.0.1	224.0.0.1	IGMPv2	46	Membership Query, general
301	2019-08-09 21:58:05.819663	LiteonTe_44:e0:15	D-LinkIn_e2:73:a2	ARP	42	Who has 192.168.0.1? Tell 192.168.0.5
302	2019-08-09 21:58:05.821447	D-LinkIn_e2:73:a2	LiteonTe_44:e0:15	ARP	42	192.168.0.1 is at 74:da:da:e2:73:a2
303	2019-08-09 21:58:20.481887	192.168.0.2	224.0.0.251	MDNS	168	Standard query 0x0019 PTR _%9E5E7C8F47989526C9BCD95D24084F6F0E
304	2019-08-09 21:58:20.483847	192.168.0.3	224.0.0.251	MDNS	420	Standard query response 0x0000 PTR Google-Home-bd921514bdaca0
305	2019-08-09 21:58:20.484841	192.168.0.3	224.0.0.251	MDNS	405	Standard query response 0x0000 PTR Google-Home-bd921514bdaca0
306	2019-08-09 21:58:22.818135	192.168.0.3	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlezone._tcp.local, "QM" questi
307	2019-08-09 21:58:22.819493	192.168.0.3	224.0.0.251	MDNS	119	Standard query 0x0000 SRV bd921514-bdac-a02f-8264-50026f5f7c3
308	2019-08-09 21:58:22.828232	192.168.0.3	224.0.0.251	MDNS	268	Standard query response 0x0000 PTR bd921514-bdac-a02f-8264-50

NSPA Skills – Malware Infected – 連接C&C Host 的失敗-2

ip.addr==95.168.185.183

No.	Time	Source	Destination	Protocol	Length	Info
283	2019-08-09 21:57:28.545063	192.168.0.5	95.168.185.183	TCP	66	55523 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PI
284	2019-08-09 21:57:28.823864	95.168.185.183	192.168.0.5	TCP	54	80 → 55523 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
285	2019-08-09 21:57:29.325107	192.168.0.5	95.168.185.183	TCP	66	[TCP Retransmission] 55523 → 80 [SYN] Seq=0 Win=64240 Len=0 MS
286	2019-08-09 21:57:29.622992	95.168.185.183	192.168.0.5	TCP	54	80 → 55523 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
287	2019-08-09 21:57:30.123068	192.168.0.5	95.168.185.183	TCP	66	[TCP Retransmission] 55523 → 80 [SYN] Seq=0 Win=64240 Len=0 MS
288	2019-08-09 21:57:30.402982	95.168.185.183	192.168.0.5	TCP	54	80 → 55523 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
557	2019-08-09 22:07:30.673819	192.168.0.5	95.168.185.183	TCP	66	55526 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PI
558	2019-08-09 22:07:30.970299	95.168.185.183	192.168.0.5	TCP	54	80 → 55526 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
559	2019-08-09 22:07:31.470383	192.168.0.5	95.168.185.183	TCP	66	[TCP Retransmission] 55526 → 80 [SYN] Seq=0 Win=64240 Len=0 MS
560	2019-08-09 22:07:31.753458	95.168.185.183	192.168.0.5	TCP	54	80 → 55526 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
561	2019-08-09 22:07:32.254449	192.168.0.5	95.168.185.183	TCP	66	[TCP Retransmission] 55526 → 80 [SYN] Seq=0 Win=64240 Len=0 MS
562	2019-08-09 22:07:32.537367	95.168.185.183	192.168.0.5	TCP	54	80 → 55526 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
768	2019-08-09 22:17:32.608711	192.168.0.5	95.168.185.183	TCP	66	55529 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PI
769	2019-08-09 22:17:32.902212	95.168.185.183	192.168.0.5	TCP	54	80 → 55529 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
770	2019-08-09 22:17:33.401952	192.168.0.5	95.168.185.183	TCP	66	[TCP Retransmission] 55529 → 80 [SYN] Seq=0 Win=64240 Len=0 MS
771	2019-08-09 22:17:33.680769	95.168.185.183	192.168.0.5	TCP	54	80 → 55529 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
772	2019-08-09 22:17:34.181476	192.168.0.5	95.168.185.183	TCP	66	[TCP Retransmission] 55529 → 80 [SYN] Seq=0 Win=64240 Len=0 MS
773	2019-08-09 22:17:34.457313	95.168.185.183	192.168.0.5	TCP	54	80 → 55529 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
977	2019-08-09 22:27:34.499229	192.168.0.5	95.168.185.183	TCP	66	55534 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PI
978	2019-08-09 22:27:34.780720	95.168.185.183	192.168.0.5	TCP	54	80 → 55534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
982	2019-08-09 22:27:35.282515	192.168.0.5	95.168.185.183	TCP	66	[TCP Retransmission] 55534 → 80 [SYN] Seq=0 Win=64240 Len=0 MS
983	2019-08-09 22:27:35.560085	95.168.185.183	192.168.0.5	TCP	54	80 → 55534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
987	2019-08-09 22:27:36.061127	192.168.0.5	95.168.185.183	TCP	66	[TCP Retransmission] 55534 → 80 [SYN] Seq=0 Win=64240 Len=0 MS
988	2019-08-09 22:27:36.346226	95.168.185.183	192.168.0.5	TCP	54	80 → 55534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1254	2019-08-09 22:37:36.399208	192.168.0.5	95.168.185.183	TCP	66	55538 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PI
1255	2019-08-09 22:37:36.690739	95.168.185.183	192.168.0.5	TCP	54	80 → 55538 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1256	2019-08-09 22:37:37.191631	192.168.0.5	95.168.185.183	TCP	66	[TCP Retransmission] 55538 → 80 [SYN] Seq=0 Win=64240 Len=0 MS
1257	2019-08-09 22:37:37.471689	95.168.185.183	192.168.0.5	TCP	54	80 → 55538 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1258	2019-08-09 22:37:37.971902	192.168.0.5	95.168.185.183	TCP	66	[TCP Retransmission] 55538 → 80 [SYN] Seq=0 Win=64240 Len=0 MS

NSPA Skills – Relay Behavior – 連接C&C Host

tcp.len>=40 and (ip.addr in {210.208.82.85 222.78.71.91})

No.	Time	Source	Destination	Protocol	Length	Info
109	2007-01-12 14:10:34.328000	210.208.82.85	140.112.180.171	TCP	758	2000 → 1356 [PSH, ACK] Seq=1 Ack=1 Win=65453 Len=704
302	2007-01-12 14:10:34.812000	210.208.82.85	140.112.180.171	TCP	744	2000 → 1262 [PSH, ACK] Seq=1 Ack=1 Win=64941 Len=690
306	2007-01-12 14:10:34.828000	140.112.180.171	222.78.71.91	TCP	744	5202 → 1056 [PSH, ACK] Seq=1465 Ack=1 Win=16802 Len=690
516	2007-01-12 14:10:35.343000	210.208.82.85	140.112.180.171	TCP	660	2000 → 1356 [PSH, ACK] Seq=705 Ack=1 Win=65453 Len=606
721	2007-01-12 14:10:35.859000	210.208.82.85	140.112.180.171	TCP	460	2000 → 1262 [PSH, ACK] Seq=691 Ack=1 Win=64941 Len=406
848	2007-01-12 14:10:36.156000	140.112.180.171	222.78.71.91	TCP	460	5202 → 1056 [PSH, ACK] Seq=2155 Ack=1 Win=16802 Len=406
1140	2007-01-12 14:10:36.875000	210.208.82.85	140.112.180.171	TCP	984	2000 → 1262 [PSH, ACK] Seq=1097 Ack=1 Win=64941 Len=930
1387	2007-01-12 14:10:37.500000	210.208.82.85	140.112.180.171	TCP	586	[TCP Previous segment not captured] 2000 → 1356 [PSH, ACK] Se
1394	2007-01-12 14:10:37.515000	140.112.180.171	222.78.71.91	TCP	1282	5202 → 1103 [PSH, ACK] Seq=1 Ack=1 Win=17314 Len=1228
1644	2007-01-12 14:10:38.125000	140.112.180.171	222.78.71.91	TCP	984	5202 → 1056 [PSH, ACK] Seq=2561 Ack=1 Win=16802 Len=930
1649	2007-01-12 14:10:38.140000	210.208.82.85	140.112.180.171	TCP	792	2000 → 1262 [PSH, ACK] Seq=2027 Ack=1 Win=64941 Len=738
1784	2007-01-12 14:10:38.500000	210.208.82.85	140.112.180.171	TCP	1116	2000 → 1356 [PSH, ACK] Seq=2539 Ack=1 Win=65453 Len=1062
2033	2007-01-12 14:10:39.125000	210.208.82.85	140.112.180.171	TCP	892	2000 → 1262 [PSH, ACK] Seq=2765 Ack=1 Win=64941 Len=838
2088	2007-01-12 14:10:39.250000	140.112.180.171	222.78.71.91	TCP	1116	5202 → 1103 [PSH, ACK] Seq=1229 Ack=1 Win=17314 Len=1062
2241	2007-01-12 14:10:39.625000	210.208.82.85	140.112.180.171	TCP	900	2000 → 1356 [PSH, ACK] Seq=3601 Ack=1 Win=65453 Len=846
2473	2007-01-12 14:10:40.203000	210.208.82.85	140.112.180.171	TCP	1046	2000 → 1262 [PSH, ACK] Seq=3603 Ack=1 Win=64941 Len=992
2667	2007-01-12 14:10:40.687000	210.208.82.85	140.112.180.171	TCP	978	2000 → 1356 [PSH, ACK] Seq=4447 Ack=1 Win=65453 Len=924
2671	2007-01-12 14:10:40.703000	140.112.180.171	222.78.71.91	TCP	1506	5202 → 1103 [PSH, ACK] Seq=2291 Ack=1 Win=17314 Len=1452
2857	2007-01-12 14:10:41.218000	210.208.82.85	140.112.180.171	TCP	842	2000 → 1262 [PSH, ACK] Seq=4595 Ack=1 Win=64941 Len=788
3113	2007-01-12 14:10:41.890000	210.208.82.85	140.112.180.171	TCP	838	2000 → 1356 [PSH, ACK] Seq=5371 Ack=1 Win=65453 Len=784
3264	2007-01-12 14:10:42.265000	140.112.180.171	222.78.71.91	TCP	842	[TCP Previous segment not captured] 5202 → 1056 [PSH, ACK] Se
3309	2007-01-12 14:10:42.375000	210.208.82.85	140.112.180.171	TCP	828	2000 → 1262 [PSH, ACK] Seq=5383 Ack=1 Win=64941 Len=774
3517	2007-01-12 14:10:42.875000	210.208.82.85	140.112.180.171	TCP	552	2000 → 1356 [PSH, ACK] Seq=6155 Ack=1 Win=65453 Len=498
3730	2007-01-12 14:10:43.390000	140.112.180.171	222.78.71.91	TCP	552	[TCP Previous segment not captured] 5202 → 1103 [PSH, ACK] Se
3984	2007-01-12 14:10:44.015000	210.208.82.85	140.112.180.171	TCP	594	2000 → 1356 [PSH, ACK] Seq=6653 Ack=1 Win=65453 Len=540
4176	2007-01-12 14:10:44.546000	210.208.82.85	140.112.180.171	TCP	722	2000 → 1262 [PSH, ACK] Seq=6389 Ack=1 Win=64941 Len=668
4382	2007-01-12 14:10:45.031000	210.208.82.85	140.112.180.171	TCP	1174	2000 → 1356 [PSH, ACK] Seq=7193 Ack=1 Win=65453 Len=1120
4592	2007-01-12 14:10:45.578000	210.208.82.85	140.112.180.171	TCP	1514	2000 → 1262 [ACK] Seq=7057 Ack=1 Win=64941 Len=1460
4609	2007-01-12 14:10:45.609000	140.112.180.171	222.78.71.91	TCP	1506	[TCP Previous segment not captured] 5202 → 1056 [PSH, ACK] Se

NSPA Skills – DNS Spoofing – DNS 異常行為

Apply a display filter ··· <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	2016-05-07 09:04:14.775345	192.168.88.135	8.8.8.8	DNS	76	Standard query 0x1e8a A www.facebook.com
2	2016-05-07 09:04:14.813184	8.8.8.8	192.168.88.135	DNS	121	Standard query response 0x1e8a A www.facebook.com CNAME star-mini.c1
3	2016-05-07 09:04:15.426011	8.8.8.8	192.168.88.135	DNS	108	Standard query response 0x1e8a A www.facebook.com A 127.0.1.1
4	2016-05-07 09:04:22.479347	192.168.88.135	192.168.88.2	DNS	74	Standard query 0x6f7f A www.google.com
5	2016-05-07 09:04:22.483885	192.168.88.2	192.168.88.135	DNS	90	Standard query response 0x6f7f A www.google.com A 172.217.3.4
6	2016-05-07 09:04:22.495643	192.168.88.2	192.168.88.135	DNS	104	Standard query response 0x6f7f A www.google.com A 127.0.1.1
7	2016-05-07 09:04:25.788691	192.168.88.135	8.8.8.8	DNS	76	Standard query 0x7476 A www.facebook.com
8	2016-05-07 09:04:25.797088	8.8.8.8	192.168.88.135	DNS	108	Standard query response 0x7476 A www.facebook.com A 127.0.1.1
9	2016-05-07 09:04:25.813851	8.8.8.8	192.168.88.135	DNS	121	Standard query response 0x7476 A www.facebook.com CNAME star-mini.c1
10	2016-05-07 09:04:27.833273	192.168.88.135	8.8.8.8	DNS	76	Standard query 0xf53e A www.facebook.com
11	2016-05-07 09:04:27.843966	8.8.8.8	192.168.88.135	DNS	108	Standard query response 0xf53e A www.facebook.com A 127.0.1.1
12	2016-05-07 09:04:27.852573	8.8.8.8	192.168.88.135	DNS	121	Standard query response 0xf53e A www.facebook.com CNAME star-mini.c1
13	2016-05-07 09:04:30.756865	192.168.88.135	8.8.8.8	DNS	76	Standard query 0xde1f A www.facebook.com
14	2016-05-07 09:04:30.766237	8.8.8.8	192.168.88.135	DNS	108	Standard query response 0xde1f A www.facebook.com A 127.0.1.1
15	2016-05-07 09:04:30.775929	8.8.8.8	192.168.88.135	DNS	121	Standard query response 0xde1f A www.facebook.com CNAME star-mini.c1
16	2016-05-07 09:04:35.247504	192.168.88.135	8.8.8.8	DNS	74	Standard query 0x91b8 A www.google.com
17	2016-05-07 09:04:35.259520	8.8.8.8	192.168.88.135	DNS	104	Standard query response 0x91b8 A www.google.com A 127.0.1.1
18	2016-05-07 09:04:35.267679	8.8.8.8	192.168.88.135	DNS	90	Standard query response 0x91b8 A www.google.com A 172.217.2.4
19	2016-05-07 09:04:38.417313	192.168.88.135	8.8.8.8	DNS	74	Standard query 0x5f98 A www.google.com
20	2016-05-07 09:04:38.427344	8.8.8.8	192.168.88.135	DNS	104	Standard query response 0x5f98 A www.google.com A 127.0.1.1
21	2016-05-07 09:04:38.436135	8.8.8.8	192.168.88.135	DNS	90	Standard query response 0x5f98 A www.google.com A 172.217.0.36
22	2016-05-07 09:04:46.003791	192.168.88.135	8.8.8.8	DNS	70	Standard query 0x17b4 A www.qq.com
23	2016-05-07 09:04:46.013684	8.8.8.8	192.168.88.135	DNS	96	Standard query response 0x17b4 A www.qq.com A 127.0.1.1
24	2016-05-07 09:04:46.099796	8.8.8.8	192.168.88.135	DNS	165	Standard query response 0x17b4 A www.qq.com CNAME qq.com.edgesuite.r
25	2016-05-07 09:04:52.980289	192.168.88.135	8.8.8.8	DNS	72	Standard query 0x19ee A www.sita.com
26	2016-05-07 09:04:52.992002	8.8.8.8	192.168.88.135	DNS	100	Standard query response 0x19ee A www.sita.com A 127.0.1.1
27	2016-05-07 09:04:53.023532	8.8.8.8	192.168.88.135	DNS	88	Standard query response 0x19ee A www.sita.com A 88.86.109.120
28	2016-05-07 09:05:05.236493	192.168.88.135	192.168.88.2	DNS	72	Standard query 0x4d21 A www.yaho.com
29	2016-05-07 09:05:05.246190	192.168.88.2	192.168.88.135	DNS	100	Standard query response 0x4d21 A www.yaho.com A 127.0.1.1

NSPA Skills – ARP Spoofing – 網路竊聽竊密行為

Apply a display filter ··· <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	2006-08-21 20:02:23.250000	172.16.1.100	61.220.15.125	TCP	62	1091 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
2	2006-08-21 20:02:23.250000	172.16.1.100	61.220.15.125	TCP	62	[TCP Out-Of-Order] 1091 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 S
3	2006-08-21 20:02:23.250000	61.220.15.125	172.16.1.100	TCP	62	80 → 1091 [SYN, ACK] Seq=0 Ack=1 Win=49640 Len=0 MSS=1460 SACK_PERM
4	2006-08-21 20:02:23.250000	61.220.15.125	172.16.1.100	TCP	62	[TCP Out-Of-Order] 80 → 1091 [SYN, ACK] Seq=0 Ack=1 Win=49640 Len=0
5	2006-08-21 20:02:23.265000	172.16.1.100	61.220.15.125	TCP	60	1091 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
6	2006-08-21 20:02:23.312000	172.16.1.100	61.220.15.125	HTTP	966	POST /login.do HTTP/1.1 (application/x-www-form-urlencoded)
7	2006-08-21 20:02:23.312000	172.16.1.100	61.220.15.125	TCP	966	[TCP Retransmission] 1091 → 80 [PSH, ACK] Seq=1 Ack=1 Win=17520 Len
8	2006-08-21 20:02:23.375000	61.220.15.125	172.16.1.100	TCP	60	80 → 1091 [ACK] Seq=1 Ack=913 Win=48728 Len=0
9	2006-08-21 20:02:23.421000	61.220.15.125	172.16.1.100	HTTP	410	HTTP/1.1 302 Moved Temporarily
10	2006-08-21 20:02:23.421000	61.220.15.125	172.16.1.100	TCP	410	[TCP Retransmission] 80 → 1091 [PSH, ACK] Seq=1 Ack=913 Win=48728 L
11	2006-08-21 20:02:23.421000	172.16.1.100	61.220.15.125	HTTP	865	GET /index.html?form=personal&errcode=01022 HTTP/1.1
12	2006-08-21 20:02:23.437000	172.16.1.100	61.220.15.125	TCP	865	[TCP Retransmission] 1091 → 80 [PSH, ACK] Seq=913 Ack=357 Win=17164
13	2006-08-21 20:02:23.437000	61.220.15.125	172.16.1.100	TCP	60	80 → 1091 [ACK] Seq=357 Ack=1724 Win=47917 Len=0
14	2006-08-21 20:02:23.437000	61.220.15.125	172.16.1.100	TCP	1514	80 → 1091 [ACK] Seq=357 Ack=1724 Win=49640 Len=1460 [TCP segment of
15	2006-08-21 20:02:23.453000	61.220.15.125	172.16.1.100	TCP	1514	[TCP Retransmission] 80 → 1091 [ACK] Seq=357 Ack=1724 Win=49640 Len
16	2006-08-21 20:02:23.453000	61.220.15.125	172.16.1.100	TCP	1514	[TCP Previous segment not captured] 80 → 1091 [ACK] Seq=3277 Ack=17
17	2006-08-21 20:02:23.500000	61.220.15.125	172.16.1.100	TCP	1514	[TCP Previous segment not captured] 80 → 1091 [ACK] Seq=6197 Ack=17
18	2006-08-21 20:02:23.500000	61.220.15.125	172.16.1.100	TCP	1514	[TCP Retransmission] 80 → 1091 [ACK] Seq=6197 Ack=1724 Win=49640 Le
19	2006-08-21 20:02:23.515000	61.220.15.125	172.16.1.100	TCP	1514	80 → 1091 [ACK] Seq=7657 Ack=1724 Win=49640 Len=1460 [TCP segment o
20	2006-08-21 20:02:23.515000	61.220.15.125	172.16.1.100	TCP	1514	80 → 1091 [PSH, ACK] Seq=9117 Ack=1724 Win=49640 Len=1460 [TCP segme
21	2006-08-21 20:02:23.515000	61.220.15.125	172.16.1.100	TCP	1514	[TCP Out-Of-Order] 80 → 1091 [ACK] Seq=7657 Ack=1724 Win=49640 Len=
22	2006-08-21 20:02:23.531000	61.220.15.125	172.16.1.100	TCP	1514	80 → 1091 [ACK] Seq=10577 Ack=1724 Win=49640 Len=1460 [TCP segment
23	2006-08-21 20:02:23.531000	61.220.15.125	172.16.1.100	TCP	1514	80 → 1091 [ACK] Seq=12037 Ack=1724 Win=49640 Len=1460 [TCP segment
24	2006-08-21 20:02:23.531000	61.220.15.125	172.16.1.100	TCP	1514	[TCP Out-Of-Order] 80 → 1091 [PSH, ACK] Seq=9117 Ack=1724 Win=49640
25	2006-08-21 20:02:23.531000	61.220.15.125	172.16.1.100	TCP	1514	80 → 1091 [PSH, ACK] Seq=13497 Ack=1724 Win=49640 Len=1460 [TCP segr
26	2006-08-21 20:02:23.546000	61.220.15.125	172.16.1.100	TCP	1514	[TCP Retransmission] 80 → 1091 [ACK] Seq=10577 Ack=1724 Win=49640 L
27	2006-08-21 20:02:23.546000	61.220.15.125	172.16.1.100	TCP	1514	[TCP Retransmission] 80 → 1091 [ACK] Seq=12037 Ack=1724 Win=49640 L
28	2006-08-21 20:02:23.546000	172.16.1.100	61.220.15.125	TCP	60	[TCP ACKed unseen segment] 1091 → 80 [ACK] Seq=1724 Ack=9117 Win=17
29	2006-08-21 20:02:23.546000	61.220.15.125	172.16.1.100	TCP	1514	[TCP Retransmission] 80 → 1091 [PSH, ACK] Seq=13497 Ack=1724 Win=49

NSPA Skills – SMB Malware – 透過網路芳鄰的惡意程式感染

Apply a display filter ··· <Ctrl-/>

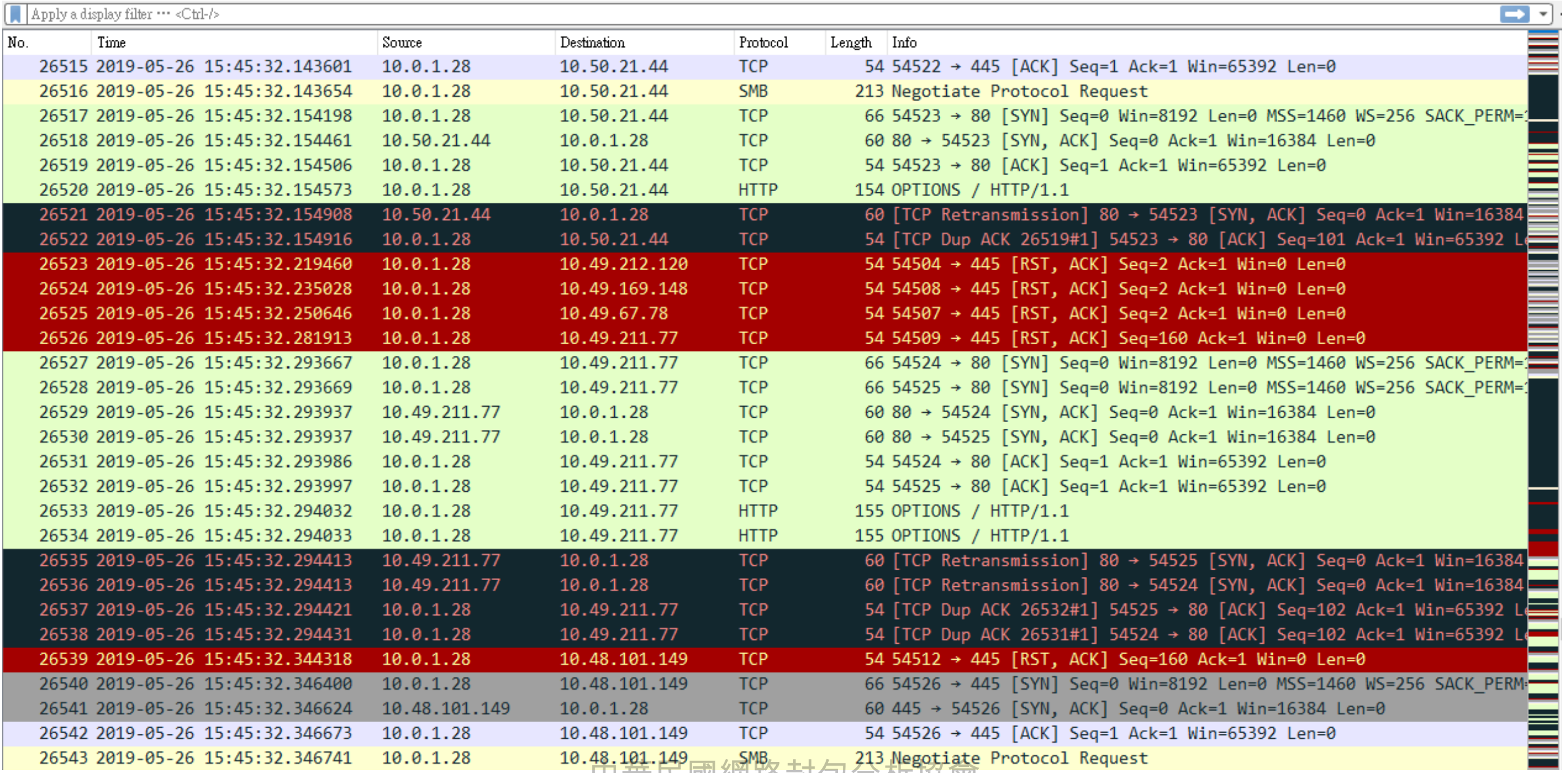
No.	Time	Source	Destination	Protocol	Length	Info
305	2014-08-10 08:18:25.362000	fe80::e504:…	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
306	2014-08-10 08:18:29.364000	fe80::e504:…	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
307	2014-08-10 08:18:32.367000	fe80::e504:…	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
308	2014-08-10 08:18:35.370000	fe80::e504:…	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
309	2014-08-10 08:18:38.172000	PcsCompu_3a…	AzureWav_52:90:99	ARP	60	192.168.0.8 is at 08:00:27:3a:c3:40
310	2014-08-10 08:18:38.173000	192.168.0.6	192.168.0.8	NBNS	110	Name query response NB 192.168.11.25
311	2014-08-10 08:18:38.175000	192.168.0.8	192.168.0.6	ICMP	74	Echo (ping) request id=0x0200, seq=6400/25, ttl=32 (reply in 312)
312	2014-08-10 08:18:38.176000	192.168.0.6	192.168.0.8	ICMP	74	Echo (ping) reply id=0x0200, seq=6400/25, ttl=128 (request in 311)
313	2014-08-10 08:18:38.178000	192.168.0.8	192.168.0.6	TCP	62	1065 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
314	2014-08-10 08:18:38.179000	192.168.0.6	192.168.0.8	TCP	62	139 → 1065 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM=1
315	2014-08-10 08:18:38.180000	192.168.0.8	192.168.0.6	NBSS	126	Session request, to USER-PC<20> from SECULAB-WINXP<00>
316	2014-08-10 08:18:38.181000	192.168.0.6	192.168.0.8	NBSS	58	Positive session response
317	2014-08-10 08:18:38.233000	192.168.0.8	192.168.0.6	SMB	191	Negotiate Protocol Request
318	2014-08-10 08:18:38.235000	192.168.0.6	192.168.0.8	SMB	420	Negotiate Protocol Response
319	2014-08-10 08:18:38.239000	192.168.0.8	192.168.0.6	SMB	278	Session Setup AndX Request, NTLMSSP_NEGOTIATE
320	2014-08-10 08:18:38.242000	192.168.0.6	192.168.0.8	SMB	430	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PRO
321	2014-08-10 08:18:38.245000	192.168.0.8	192.168.0.6	SMB	304	Session Setup AndX Request, NTLMSSP_AUTH, User: \
322	2014-08-10 08:18:38.249000	192.168.0.6	192.168.0.8	SMB	250	Session Setup AndX Response
323	2014-08-10 08:18:38.251000	192.168.0.8	192.168.0.6	SMB	138	Tree Connect AndX Request, Path: \\USER-PC\IPC$
324	2014-08-10 08:18:38.255000	192.168.0.6	192.168.0.8	SMB	114	Tree Connect AndX Response
325	2014-08-10 08:18:38.258000	192.168.0.8	192.168.0.6	LANMAN	176	NetServerEnum2 Request, Workstation, Server, SQL Server, Domain Contro
326	2014-08-10 08:18:38.260000	192.168.0.6	192.168.0.8	LANMAN	186	NetServerEnum2 Response
327	2014-08-10 08:18:38.262000	192.168.0.8	192.168.0.6	SMB	97	Logoff AndX Request
328	2014-08-10 08:18:38.263000	192.168.0.6	192.168.0.8	SMB	97	Logoff AndX Response
329	2014-08-10 08:18:38.265000	192.168.0.8	192.168.0.6	SMB	93	Tree Disconnect Request
330	2014-08-10 08:18:38.266000	192.168.0.6	192.168.0.8	SMB	93	Tree Disconnect Response
331	2014-08-10 08:18:38.267000	192.168.0.8	192.168.0.6	SMB	278	Session Setup AndX Request, NTLMSSP_NEGOTIATE
332	2014-08-10 08:18:38.269000	192.168.0.6	192.168.0.8	SMB	430	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PRO
333	2014-08-10 08:18:38.270000	192.168.0.8	192.168.0.6	SMB	304	Session Setup AndX Request, NTLMSSP_AUTH, User: \

NSPA Skills – SMB Malware – 透過網路芳鄰的惡意程式感染

Apply a display filter ··· <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
30287	2019-05-26 15:49:52.381406	10.0.1.28	10.59.42.15	TCP	66	54896 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=
30288	2019-05-26 15:49:52.381698	10.59.42.15	10.0.1.28	TCP	60	445 → 54896 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0
30289	2019-05-26 15:49:52.381747	10.0.1.28	10.59.42.15	TCP	54	54896 → 445 [ACK] Seq=1 Ack=1 Win=65392 Len=0
30290	2019-05-26 15:49:52.381807	10.0.1.28	10.59.42.15	SMB	213	Negotiate Protocol Request
30291	2019-05-26 15:49:52.433077	10.50.3.54	10.0.1.28	TCP	60	80 → 54893 [ACK] Seq=1 Ack=100 Win=65436 Len=0
30292	2019-05-26 15:49:52.503801	10.0.1.28	10.48.2.225	TCP	66	54897 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=
30293	2019-05-26 15:49:52.504123	10.48.2.225	10.0.1.28	TCP	60	445 → 54897 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0
30294	2019-05-26 15:49:52.504158	10.0.1.28	10.48.2.225	TCP	54	54897 → 445 [ACK] Seq=1 Ack=1 Win=65392 Len=0
30295	2019-05-26 15:49:52.519204	10.0.1.28	10.48.2.225	TCP	54	54897 → 445 [FIN, ACK] Seq=1 Ack=1 Win=65392 Len=0
30296	2019-05-26 15:49:52.542545	10.49.196.13	10.0.1.28	TCP	60	80 → 54894 [ACK] Seq=1 Ack=102 Win=65434 Len=0
30297	2019-05-26 15:49:52.567605	10.0.1.28	10.48.2.225	TCP	66	54898 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=
30298	2019-05-26 15:49:52.567914	10.48.2.225	10.0.1.28	TCP	60	445 → 54898 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0
30299	2019-05-26 15:49:52.567954	10.0.1.28	10.48.2.225	TCP	54	54898 → 445 [ACK] Seq=1 Ack=1 Win=65392 Len=0
30300	2019-05-26 15:49:52.567972	10.0.1.28	10.48.2.225	SMB	213	Negotiate Protocol Request
30301	2019-05-26 15:49:52.582592	10.0.1.28	10.50.3.33	TCP	66	54899 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=
30302	2019-05-26 15:49:52.582922	10.50.3.33	10.0.1.28	TCP	60	445 → 54899 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0
30303	2019-05-26 15:49:52.582956	10.0.1.28	10.50.3.33	TCP	54	54899 → 445 [ACK] Seq=1 Ack=1 Win=65392 Len=0
30304	2019-05-26 15:49:52.597986	10.0.1.28	10.50.3.33	TCP	54	54899 → 445 [FIN, ACK] Seq=1 Ack=1 Win=65392 Len=0
30305	2019-05-26 15:49:52.629104	10.0.1.28	10.59.42.15	TCP	54	[TCP Retransmission] 54895 → 445 [FIN, ACK] Seq=1 Ack=1 Win=6539
30306	2019-05-26 15:49:52.646745	10.0.1.28	10.50.3.33	TCP	66	54900 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=
30307	2019-05-26 15:49:52.647039	10.50.3.33	10.0.1.28	TCP	60	445 → 54900 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0
30308	2019-05-26 15:49:52.647088	10.0.1.28	10.50.3.33	TCP	54	54900 → 445 [ACK] Seq=1 Ack=1 Win=65392 Len=0
30309	2019-05-26 15:49:52.647125	10.0.1.28	10.50.3.33	SMB	213	Negotiate Protocol Request
30310	2019-05-26 15:49:52.738442	10.0.1.28	10.48.16.104	TCP	54	54880 → 445 [RST, ACK] Seq=160 Ack=1 Win=0 Len=0
30311	2019-05-26 15:49:52.738534	10.0.1.28	10.59.42.15	TCP	213	[TCP Retransmission] 54896 → 445 [PSH, ACK] Seq=1 Ack=1 Win=6539
30312	2019-05-26 15:49:52.739894	10.0.1.28	10.48.16.104	TCP	66	54901 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=
30313	2019-05-26 15:49:52.740123	10.48.16.104	10.0.1.28	TCP	60	445 → 54901 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0
30314	2019-05-26 15:49:52.740175	10.0.1.28	10.48.16.104	TCP	54	54901 → 445 [ACK] Seq=1 Ack=1 Win=65392 Len=0
30315	2019-05-26 15:49:52.740215	10.0.1.28	10.48.16.104	SMB	213	Negotiate Protocol Request

NSPA Skills – SMB Malware – 透過網路芳鄰的惡意程式感染



Apply a display filter ··· <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
26515	2019-05-26 15:45:32.143601	10.0.1.28	10.50.21.44	TCP	54	54522 → 445 [ACK] Seq=1 Ack=1 Win=65392 Len=0
26516	2019-05-26 15:45:32.143654	10.0.1.28	10.50.21.44	SMB	213	Negotiate Protocol Request
26517	2019-05-26 15:45:32.154198	10.0.1.28	10.50.21.44	TCP	66	54523 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=
26518	2019-05-26 15:45:32.154461	10.50.21.44	10.0.1.28	TCP	60	80 → 54523 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0
26519	2019-05-26 15:45:32.154506	10.0.1.28	10.50.21.44	TCP	54	54523 → 80 [ACK] Seq=1 Ack=1 Win=65392 Len=0
26520	2019-05-26 15:45:32.154573	10.0.1.28	10.50.21.44	HTTP	154	OPTIONS / HTTP/1.1
26521	2019-05-26 15:45:32.154908	10.50.21.44	10.0.1.28	TCP	60	[TCP Retransmission] 80 → 54523 [SYN, ACK] Seq=0 Ack=1 Win=16384
26522	2019-05-26 15:45:32.154916	10.0.1.28	10.50.21.44	TCP	54	[TCP Dup ACK 26519#1] 54523 → 80 [ACK] Seq=101 Ack=1 Win=65392 L
26523	2019-05-26 15:45:32.219460	10.0.1.28	10.49.212.120	TCP	54	54504 → 445 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
26524	2019-05-26 15:45:32.235028	10.0.1.28	10.49.169.148	TCP	54	54508 → 445 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
26525	2019-05-26 15:45:32.250646	10.0.1.28	10.49.67.78	TCP	54	54507 → 445 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
26526	2019-05-26 15:45:32.281913	10.0.1.28	10.49.211.77	TCP	54	54509 → 445 [RST, ACK] Seq=160 Ack=1 Win=0 Len=0
26527	2019-05-26 15:45:32.293667	10.0.1.28	10.49.211.77	TCP	66	54524 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=
26528	2019-05-26 15:45:32.293669	10.0.1.28	10.49.211.77	TCP	66	54525 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=
26529	2019-05-26 15:45:32.293937	10.49.211.77	10.0.1.28	TCP	60	80 → 54524 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0
26530	2019-05-26 15:45:32.293937	10.49.211.77	10.0.1.28	TCP	60	80 → 54525 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0
26531	2019-05-26 15:45:32.293986	10.0.1.28	10.49.211.77	TCP	54	54524 → 80 [ACK] Seq=1 Ack=1 Win=65392 Len=0
26532	2019-05-26 15:45:32.293997	10.0.1.28	10.49.211.77	TCP	54	54525 → 80 [ACK] Seq=1 Ack=1 Win=65392 Len=0
26533	2019-05-26 15:45:32.294032	10.0.1.28	10.49.211.77	HTTP	155	OPTIONS / HTTP/1.1
26534	2019-05-26 15:45:32.294033	10.0.1.28	10.49.211.77	HTTP	155	OPTIONS / HTTP/1.1
26535	2019-05-26 15:45:32.294413	10.49.211.77	10.0.1.28	TCP	60	[TCP Retransmission] 80 → 54525 [SYN, ACK] Seq=0 Ack=1 Win=16384
26536	2019-05-26 15:45:32.294413	10.49.211.77	10.0.1.28	TCP	60	[TCP Retransmission] 80 → 54524 [SYN, ACK] Seq=0 Ack=1 Win=16384
26537	2019-05-26 15:45:32.294421	10.0.1.28	10.49.211.77	TCP	54	[TCP Dup ACK 26532#1] 54525 → 80 [ACK] Seq=102 Ack=1 Win=65392 L
26538	2019-05-26 15:45:32.294431	10.0.1.28	10.49.211.77	TCP	54	[TCP Dup ACK 26531#1] 54524 → 80 [ACK] Seq=102 Ack=1 Win=65392 L
26539	2019-05-26 15:45:32.344318	10.0.1.28	10.48.101.149	TCP	54	54512 → 445 [RST, ACK] Seq=160 Ack=1 Win=0 Len=0
26540	2019-05-26 15:45:32.346400	10.0.1.28	10.48.101.149	TCP	66	54526 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=
26541	2019-05-26 15:45:32.346624	10.48.101.149	10.0.1.28	TCP	60	445 → 54526 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0
26542	2019-05-26 15:45:32.346673	10.0.1.28	10.48.101.149	TCP	54	54526 → 445 [ACK] Seq=1 Ack=1 Win=65392 Len=0
26543	2019-05-26 15:45:32.346741	10.0.1.28	10.48.101.149	SMB	213	Negotiate Protocol Request

NSPA Skills – SMB Abnormal – 透過網路芳鄰的異常網路行為

Apply a display filter ··· <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
73	2020-06-19 11:52:48.688280	18.163.170.109	10.0.1.15	TLSv1.2	131	Application Data
74	2020-06-19 11:52:48.698516	10.0.1.15	18.163.170.109	TLSv1.2	85	Application Data
75	2020-06-19 11:52:48.714078	10.0.1.15	178.185.66.227	TCP	66	49253 → 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
76	2020-06-19 11:52:48.729453	18.163.170.109	10.0.1.15	TCP	60	443 → 49192 [ACK] Seq=1166 Ack=2173 Win=16 Len=0
77	2020-06-19 11:52:48.855255	178.185.66.227	10.0.1.15	TCP	66	445 → 49253 [SYN, ACK] Seq=0 Ack=1 Win=14520 Len=0 MSS=1452 SACK_PERM=
78	2020-06-19 11:52:48.855355	10.0.1.15	178.185.66.227	TCP	54	49253 → 445 [ACK] Seq=1 Ack=1 Win=66560 Len=0
79	2020-06-19 11:52:48.855438	10.0.1.15	178.185.66.227	SMB	213	Negotiate Protocol Request
80	2020-06-19 11:52:48.915604	10.0.1.15	18.163.170.109	TLSv1.2	439	Application Data
81	2020-06-19 11:52:48.950714	18.163.170.109	10.0.1.15	TCP	60	443 → 49192 [ACK] Seq=1166 Ack=2558 Win=16 Len=0
82	2020-06-19 11:52:48.952643	18.163.170.109	10.0.1.15	TLSv1.2	85	Application Data
83	2020-06-19 11:52:48.987418	178.185.66.227	10.0.1.15	TCP	60	445 → 49253 [ACK] Seq=1 Ack=160 Win=15592 Len=0
84	2020-06-19 11:52:48.996295	178.185.66.227	10.0.1.15	SMB	185	Negotiate Protocol Response
85	2020-06-19 11:52:48.996933	10.0.1.15	178.185.66.227	SMB	196	Session Setup AndX Request, NTLMSSP_NEGOTIATE
86	2020-06-19 11:52:49.002453	10.0.1.15	18.163.170.109	TCP	54	49192 → 443 [ACK] Seq=2558 Ack=1197 Win=255 Len=0
87	2020-06-19 11:52:49.130927	178.185.66.227	10.0.1.15	SMB	346	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PRO
88	2020-06-19 11:52:49.131324	10.0.1.15	178.185.66.227	SMB	538	Session Setup AndX Request, NTLMSSP_AUTH, User: NSPA3\Admin
89	2020-06-19 11:52:49.266921	178.185.66.227	10.0.1.15	SMB	166	Session Setup AndX Response
90	2020-06-19 11:52:49.267254	10.0.1.15	178.185.66.227	SMB	152	Tree Connect AndX Request, Path: \\178.185.66.227\IPC$
91	2020-06-19 11:52:49.402847	178.185.66.227	10.0.1.15	SMB	114	Tree Connect AndX Response
92	2020-06-19 11:52:49.402998	10.0.1.15	178.185.66.227	SMB	174	Trans2 Request, GET_DFS_REFERRAL, File: \178.185.66.227\public
93	2020-06-19 11:52:49.534912	178.185.66.227	10.0.1.15	SMB	93	Trans2 Response, GET_DFS_REFERRAL, Error: STATUS_NOT_FOUND
94	2020-06-19 11:52:49.535572	10.0.1.15	178.185.66.227	SMB	156	Tree Connect AndX Request, Path: \\178.185.66.227\PUBLIC
95	2020-06-19 11:52:49.666935	178.185.66.227	10.0.1.15	SMB	93	Tree Connect AndX Response, Error: STATUS_ACCESS_DENIED
96	2020-06-19 11:52:49.718828	10.0.1.15	178.185.66.227	TCP	54	49253 → 445 [ACK] Seq=1106 Ack=674 Win=66048 Len=0
97	2020-06-19 11:52:49.748250	10.0.1.15	172.67.75.154	TCP	55	49250 → 443 [ACK] Seq=1 Ack=1 Win=256 Len=1 [TCP segment of a reassemb
98	2020-06-19 11:52:49.899419	18.163.170.109	10.0.1.15	TLSv1.2	131	Application Data
99	2020-06-19 11:52:49.909413	10.0.1.15	18.163.170.109	TLSv1.2	85	Application Data
100	2020-06-19 11:52:49.913051	172.67.75.154	10.0.1.15	TCP	66	443 → 49250 [ACK] Seq=1 Ack=2 Win=67 Len=0 SLE=1 SRE=2
101	2020-06-19 11:52:49.979569	18.163.170.109	10.0.1.15	TCP	60	443 → 49192 [ACK] Seq=1274 Ack=2589 Win=16 Len=0

NSPA Skills – SMB Abnormal – 透過網路芳鄰的異常網路行為

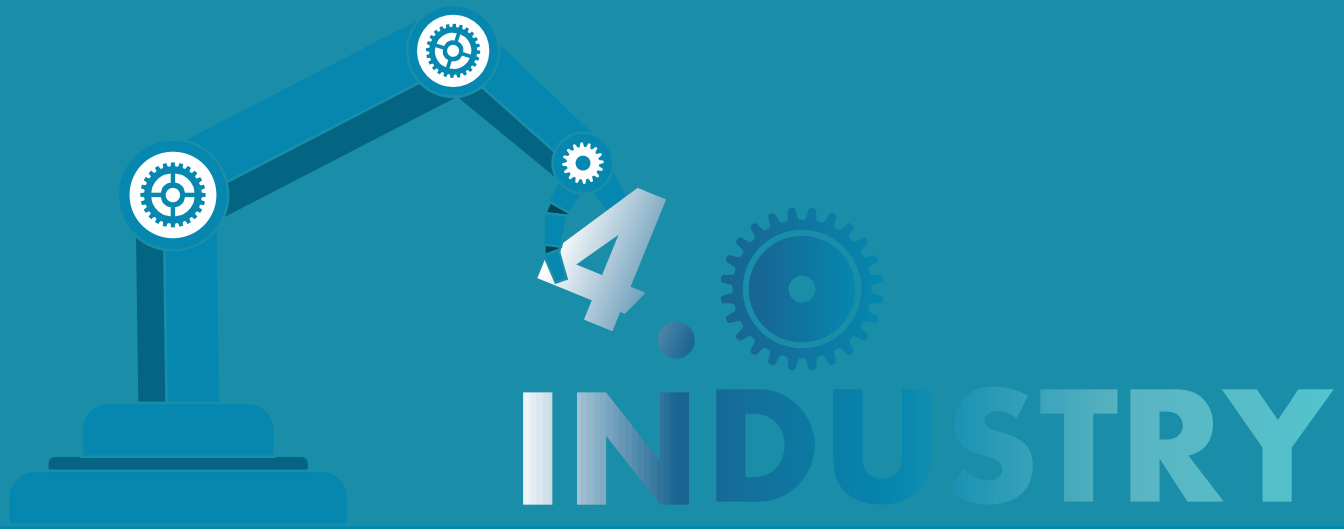
Apply a display filter ··· <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
52	2008-01-24 17:50:47.906000	61.215.254.251	61.216.7.46	TCP	70	2754 → 445 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
53	2008-01-24 17:50:47.906000	61.216.7.46	61.215.254.251	TCP	70	445 → 2754 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 SACK_PERM=1
54	2008-01-24 17:50:48.015000	61.215.254.251	61.216.7.46	TCP	62	2754 → 445 [ACK] Seq=1 Ack=1 Win=17280 Len=0
55	2008-01-24 17:50:48.015000	61.215.254.251	61.216.7.46	SMB	199	Negotiate Protocol Request
56	2008-01-24 17:50:48.015000	61.216.7.46	61.215.254.251	SMB	151	Negotiate Protocol Response
57	2008-01-24 17:50:48.109000	61.215.254.251	61.216.7.46	SMB	238	Session Setup AndX Request, NTLMSSP_NEGOTIATE
58	2008-01-24 17:50:48.109000	61.216.7.46	61.215.254.251	SMB	337	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PRO
59	2008-01-24 17:50:48.218000	61.215.254.251	61.216.7.46	SMB	368	Session Setup AndX Request, NTLMSSP_AUTH, User: HOKUTO\admin
60	2008-01-24 17:50:48.218000	61.216.7.46	61.215.254.251	SMB	183	Session Setup AndX Response
61	2008-01-24 17:50:48.328000	61.215.254.251	61.216.7.46	SMB	154	Tree Connect AndX Request, Path: \\61.216.7.46\IPC$
62	2008-01-24 17:50:48.375000	61.216.7.46	61.215.254.251	SMB	122	Tree Connect AndX Response
63	2008-01-24 17:50:48.484000	61.215.254.251	61.216.7.46	SMB	158	Tree Connect AndX Request, Path: \\61.216.7.46\ADMIN$
64	2008-01-24 17:50:48.484000	61.216.7.46	61.215.254.251	SMB	101	Tree Connect AndX Response, Error: STATUS_BAD_NETWORK_NAME
65	2008-01-24 17:50:48.531000	61.215.254.251	61.216.7.46	SMB	158	Tree Connect AndX Request, Path: \\61.216.7.46\ADMIN$
66	2008-01-24 17:50:48.531000	61.216.7.46	61.215.254.251	SMB	101	Tree Connect AndX Response, Error: STATUS_BAD_NETWORK_NAME
67	2008-01-24 17:50:48.640000	61.215.254.251	61.216.7.46	SMB	158	Tree Connect AndX Request, Path: \\61.216.7.46\ADMIN$
68	2008-01-24 17:50:48.640000	61.216.7.46	61.215.254.251	SMB	101	Tree Connect AndX Response, Error: STATUS_BAD_NETWORK_NAME
69	2008-01-24 17:50:48.734000	61.215.254.251	61.216.7.46	SMB	158	Tree Connect AndX Request, Path: \\61.216.7.46\ADMIN$
70	2008-01-24 17:50:48.750000	61.216.7.46	61.215.254.251	SMB	101	Tree Connect AndX Response, Error: STATUS_BAD_NETWORK_NAME
71	2008-01-24 17:50:48.843000	61.215.254.251	61.216.7.46	SMB	252	Session Setup AndX Request, NTLMSSP_NEGOTIATE
72	2008-01-24 17:50:48.843000	61.216.7.46	61.215.254.251	SMB	337	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PRO
73	2008-01-24 17:50:48.953000	61.215.254.251	61.216.7.46	SMB	298	Session Setup AndX Request, NTLMSSP_AUTH, User: \
74	2008-01-24 17:50:48.953000	61.216.7.46	61.215.254.251	SMB	183	Session Setup AndX Response
75	2008-01-24 17:50:49.062000	61.215.254.251	61.216.7.46	SMB	154	Tree Connect AndX Request, Path: \\61.216.7.46\IPC$
76	2008-01-24 17:50:49.062000	61.216.7.46	61.215.254.251	SMB	122	Tree Connect AndX Response
77	2008-01-24 17:50:49.109000	61.215.254.251	61.216.7.46	SMB	150	Tree Connect AndX Request, Path: \\61.216.7.46\C$
78	2008-01-24 17:50:49.109000	61.216.7.46	61.215.254.251	SMB	101	Tree Connect AndX Response, Error: STATUS_BAD_NETWORK_NAME
79	2008-01-24 17:50:49.218000	61.215.254.251	61.216.7.46	SMB	150	Tree Connect AndX Request, Path: \\61.216.7.46\C$
80	2008-01-24 17:50:49.218000	61.216.7.46	61.215.254.251	SMB	101	Tree Connect AndX Response, Error: STATUS_BAD_NETWORK_NAME

NSPA Skills – SMB Abnormal – 透過網路芳鄰的密碼攻擊

Apply a display filter ··· <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
382	2015-07-13 14:59:09.749000	10.10.1.102	10.10.1.10	TCP	62	1863 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
383	2015-07-13 14:59:09.751000	10.10.1.10	10.10.1.102	TCP	62	445 → 1863 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM
384	2015-07-13 14:59:09.753000	10.10.1.102	10.10.1.10	TCP	60	1863 → 445 [ACK] Seq=1 Ack=1 Win=64240 Len=0
385	2015-07-13 14:59:09.755000	10.10.1.102	10.10.1.10	SMB	191	Negotiate Protocol Request
386	2015-07-13 14:59:09.758000	10.10.1.10	10.10.1.102	SMB	463	Negotiate Protocol Response
387	2015-07-13 14:59:09.762000	10.10.1.102	10.10.1.10	SMB	294	Session Setup AndX Request, NTLMSSP_NEGOTIATE
388	2015-07-13 14:59:09.765000	10.10.1.10	10.10.1.102	SMB	430	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_
389	2015-07-13 14:59:09.769000	10.10.1.102	10.10.1.10	SMB	436	Session Setup AndX Request, NTLMSSP_AUTH, User: TEST-KOLIBRIWEB\Tes
390	2015-07-13 14:59:09.773000	10.10.1.10	10.10.1.102	SMB	93	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
391	2015-07-13 14:59:09.777000	10.10.1.102	10.10.1.10	TCP	60	1863 → 445 [FIN, ACK] Seq=760 Ack=825 Win=63416 Len=0
392	2015-07-13 14:59:09.781000	10.10.1.10	10.10.1.102	TCP	54	445 → 1863 [ACK] Seq=825 Ack=761 Win=63618 Len=0
393	2015-07-13 14:59:09.785000	10.10.1.10	10.10.1.102	TCP	54	445 → 1863 [RST, ACK] Seq=825 Ack=761 Win=0 Len=0
394	2015-07-13 14:59:09.789000	10.10.1.102	10.10.1.10	TCP	62	1865 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
395	2015-07-13 14:59:09.792000	10.10.1.10	10.10.1.102	TCP	62	445 → 1865 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM
396	2015-07-13 14:59:09.794000	10.10.1.102	10.10.1.10	TCP	62	1866 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
397	2015-07-13 14:59:09.797000	10.10.1.10	10.10.1.102	TCP	62	139 → 1866 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM
398	2015-07-13 14:59:09.799000	10.10.1.102	10.10.1.10	TCP	60	1865 → 445 [ACK] Seq=1 Ack=1 Win=64240 Len=0
399	2015-07-13 14:59:09.801000	10.10.1.102	10.10.1.10	TCP	60	1866 → 139 [RST] Seq=1 Win=0 Len=0
400	2015-07-13 14:59:09.803000	10.10.1.102	10.10.1.10	SMB	191	Negotiate Protocol Request
401	2015-07-13 14:59:09.806000	10.10.1.10	10.10.1.102	SMB	463	Negotiate Protocol Response
402	2015-07-13 14:59:09.810000	10.10.1.102	10.10.1.10	SMB	294	Session Setup AndX Request, NTLMSSP_NEGOTIATE
403	2015-07-13 14:59:09.814000	10.10.1.10	10.10.1.102	SMB	430	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_
404	2015-07-13 14:59:09.817000	10.10.1.102	10.10.1.10	SMB	436	Session Setup AndX Request, NTLMSSP_AUTH, User: TEST-KOLIBRIWEB\Tes
405	2015-07-13 14:59:09.821000	10.10.1.10	10.10.1.102	SMB	93	Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
406	2015-07-13 14:59:09.825000	10.10.1.102	10.10.1.10	TCP	60	1865 → 445 [FIN, ACK] Seq=760 Ack=825 Win=63416 Len=0
407	2015-07-13 14:59:09.829000	10.10.1.10	10.10.1.102	TCP	54	445 → 1865 [ACK] Seq=825 Ack=761 Win=63618 Len=0
408	2015-07-13 14:59:09.834000	10.10.1.10	10.10.1.102	TCP	54	445 → 1865 [RST, ACK] Seq=825 Ack=761 Win=0 Len=0
409	2015-07-13 14:59:09.838000	10.10.1.102	10.10.1.10	TCP	62	1867 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
410	2015-07-13 14:59:09.843000	10.10.1.10	10.10.1.102	TCP	62	445 → 1867 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM



評量與討論

中華民國 網路封包分析協會
NSPA/NTPA

http://www.nspacert.org

http://www.ntpa.org.tw

http://www.nspa-cert-tw.org

http://www.huge-diamond.net


THANK YOU
中華民國 網路封包分析協會 NSPA/NTPA
中華民國網路封包分析協會