

網路行為異常偵測

TANET2017論文 - 與北區 ASOC 共同發表

傳統網路分析之瓶頸與限制

Netflow

- * Layer 2 mac address Level: 無法觀察
 - * 無法偵測 broadcast storm, arp spoofing
- * Layer 3 IP Level
 - * 無法偵測同網段之網路連線行為
 - * 無法即時反應網路連線資訊、僅能提供連線 Summary 結果
 - * 路由器 Netflow Active Time 預設 30 分鐘: 一個持續檔案傳輸之連線需 30 分鐘後才會匯出 Summary 傳輸結果資料
 - * 無法觀察 TTL(Time to Live) 變化
- * Layer 4 TCP Level: 有限分析
 - * 無法觀察 TCP Sessions、TCP retransmission、Out of order、Duplicate ack ...
- * Layer 7 Application Level: 無法分析

傳統網路分析之瓶頸與限制

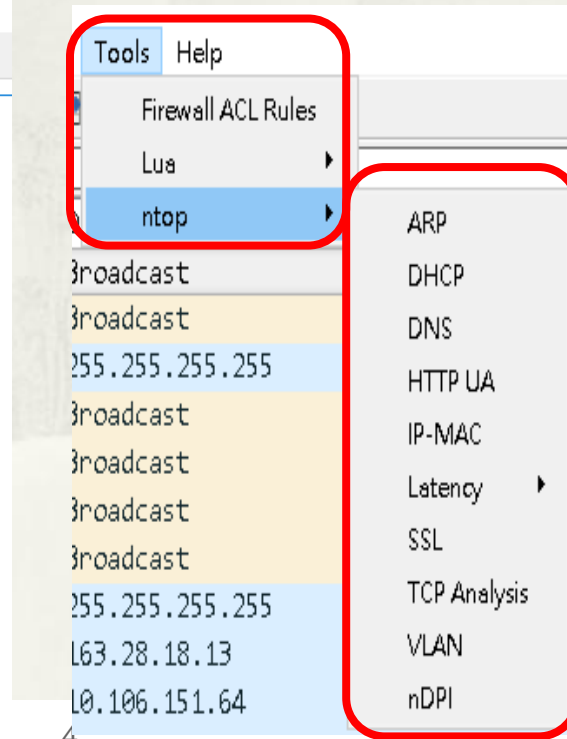
Wireshark

- * 見樹不見林:
 - * 可詳細觀察每個封包所有欄位資訊，但缺乏整體統計與分析。
- * 針對高速網路 10Gbps,100Gbps 側錄有困難
- * 無法針對 Layer7 應用層分析與過濾
 - * “filter all Skype” traffic is not possible

Network Overview based on packet level

Wireshark + ntop plugin

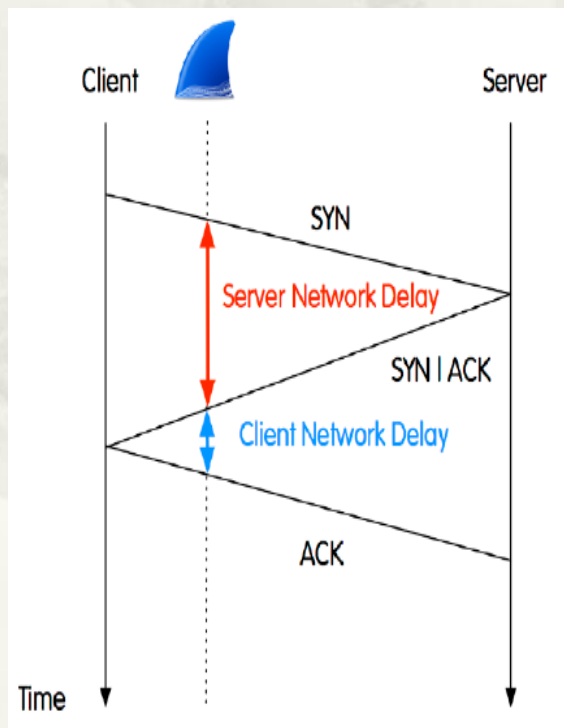
- * ntop plugin (sharkfest 2017)
 - * Lua script for wireshark (Open Source)
 - * <https://github.com/ntop/nDPI/tree/dev/wireshark>



分析案例一

網路很慢 vs. 網站很慢

- * 使用者抱怨反應
 - * 網路很慢 vs. 網站很慢
 - * Network Delay vs. Application Delay

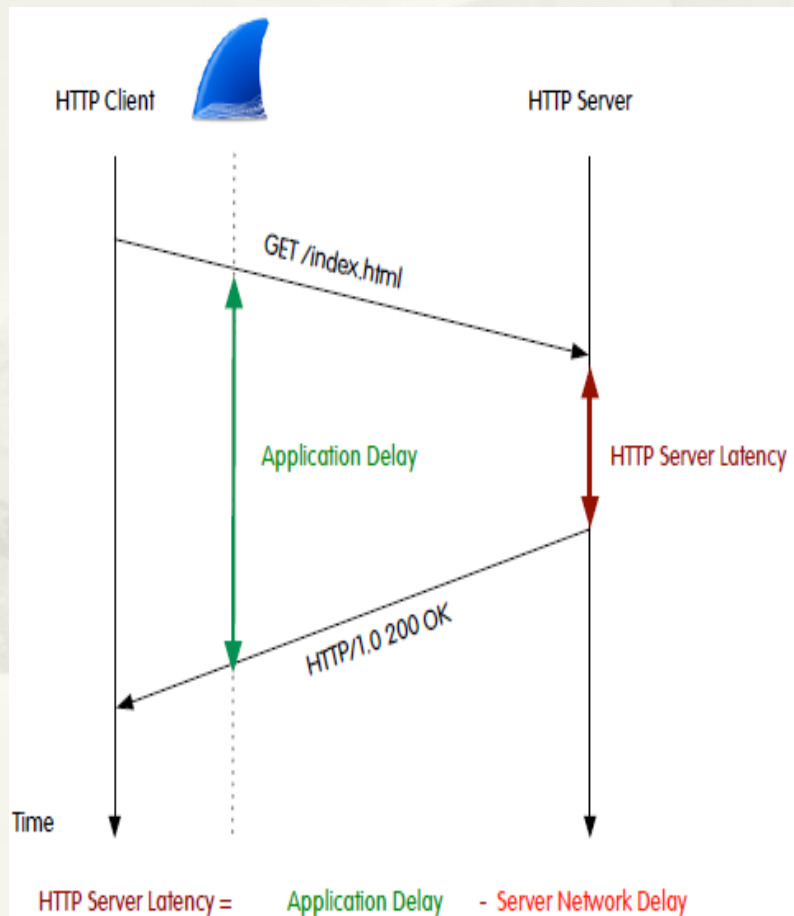


Wireshark · Network Latency	
Client	Min/Max RTT
172.16.0.2	0.038 / 0.117 msec
Server	Min RTT
54.194.226.6	296.570 / 296.570 msec
72.251.245.181	286.275 / 286.275 msec
37.139.11.123	281.332 / 281.332 msec
34.224.135.40	197.057 / 197.057 msec
34.239.56.165	196.941 / 196.941 msec
205.180.86.172	142.621 / 142.621 msec
64.38.119.27	141.538 / 141.538 msec
103.243.221.109	108.627 / 108.627 msec
106.10.193.33	82.442 / 82.442 msec
103.67.200.188	74.881 / 74.881 msec
50.116.239.135	57.246 / 57.246 msec

分析案例一

網路很慢 vs. 網站很慢

* Application Delay



Wireshark · Application Latency	
Server	Min Application RTT
103.243.221.109	1429.770 / 1429.770 msec
204.11.109.68	432.199 / 432.199 msec
63.251.252.12	222.961 / 222.961 msec
204.2.197.204	220.601 / 220.601 msec
34.224.135.40	202.335 / 202.335 msec
54.172.137.57	202.254 / 202.254 msec
69.20.20.10	177.324 / 177.324 msec
64.38.119.27	145.299 / 145.299 msec
52.9.175.175	132.866 / 132.866 msec
38.106.10.133	131.861 / 131.861 msec
103.67.200.188	85.984 / 85.984 msec

分析案例二

SYN Flood

- * 統計 TCP flag 比例偵測異常行為。
- * 自行新增 Lua script 程式碼

The screenshot displays the Wireshark interface for TCP Packets Analysis. The left pane shows a list of packets, with several SYN packets highlighted in green. The right pane shows the packet details for a selected SYN packet, including the 'Abnormal Packets Percentage' (38.4%) and 'SYN Packets Percentage' (85.6%), which is highlighted with a red box. Below these statistics, the 'Total Retransmissions' is 1827, and the 'Total Out-of-Order' is 1. The 'Total Lost Segment' is 46. The bottom pane shows the packet bytes and the ACK field details.

Info
125 Continuation Data
125 443 → 53917 [ACK] Seq=...
125 65197 → 80 [SYN] Seq=...
125 65198 → 80 [SYN] Seq=...
125 65199 → 80 [SYN] Seq=...
125 65200 → 80 [SYN] Seq=...
125 65204 → 80 [SYN] Seq=...
125 65205 → 80 [SYN] Seq=...
125 65206 → 80 [SYN] Seq=...
125 65207 → 80 [SYN] Seq=...
125 65208 → 80 [SYN] Seq=...
125 65209 → 80 [SYN] Seq=...
125 65210 → 80 [SYN] Seq=...
125 65211 → 80 [SYN] Seq=...
125 65212 → 80 [SYN] Seq=...
125 65213 → 80 [SYN] Seq=...
125 65214 → 80 [SYN] Seq=...

Abnormal Packets Percentage : 38.4 %
SYN Packets Percentage : 85.6 %
Total Retransmissions : 1827

140.112.39.85:443 -> 222.255.251.22:2910 6
140.112.39.85:13281 -> 220.161.204.250:2161 5
140.112.39.85:443 -> 222.255.251.22:2871 4
140.112.39.85:65485 -> 174.132.175.69:443 2
49.98.162.99:34294 -> 140.112.39.85:13281 2
140.112.39.85:49516 -> 210.73.221.250:80 1
140.112.39.85:49515 -> 210.73.221.250:80 1
140.112.39.85:49519 -> 210.73.221.250:80 1
140.112.39.85:49517 -> 210.73.221.250:80 1
140.112.39.85:49521 -> 210.73.221.250:80 1
140.112.39.85:49518 -> 210.73.221.250:80 1

Total Out-of-Order : 1

113.161.128.120:42762 -> 140.112.39.85:443 1

Total Lost Segment : 46

140.112.39.85:443 -> 113.161.128.120:42762 9

分析案例三

實體網路線異常

- * 臺大校內某系所網頁首頁 Web Server
- * 新增統計 TCP 封包異常比例，Lua script 程式碼

```
label = label .. "Abnormal Packets  
Percentage : " ..  
formatPctg((num_tcp_retrans +  
num_tcp_ooo +  
num_tcp_lost_segment +  
num_tcp_duplicate_ack) /  
last_processed_packet_number *  
100) .. "\n"
```

Wireshark · TCP Packets Analysis

Abnormal Packets Percentage : 22.7 %

Total Retransmissions : 150

140.112.23.234:795	->	140.112.23.144:2049	125
140.112.23.234:80	->	180.76.15.10:39838	12
140.112.23.234:80	->	106.120.173.135:62793	7
64.233.188.188:5228	->	140.112.23.190:47072	6

Total Out-of-Order : 49

140.112.23.234:795	->	140.112.23.144:2049	46
140.112.23.234:80	->	180.76.15.10:39838	2
5.185.95.203:59030	->	140.112.23.89:23	1

Total Lost Segment : 1

140.112.23.234:795	->	140.112.23.144:2049	1
--------------------	----	---------------------	---

Total Duplicate Ack : 224

140.112.23.144:2049	->	140.112.23.234:795	192
180.76.15.10:39838	->	140.112.23.234:80	23
106.120.173.135:62793	->	140.112.23.234:80	9

分析案例四

IPS 誤擋

- * 連線臺大首頁
www.ntu.edu.tw 封包
遭 IPS 誤擋
- * 新增統計 TCP 封包異常比例，Lua script 程式碼(同前頁)

Wireshark · TCP Packets Analysis

Abnormal Packets Percentage : 24.1 %

Total Retransmissions : 1395

140.112.8.116:80	>	140.112.114.183:56217	358
140.112.8.116:80	>	140.112.114.183:56214	329
140.112.8.116:80	>	140.112.114.183:56211	224
140.112.8.116:80	>	140.112.114.183:56213	184
140.112.8.116:80	>	140.112.114.183:56215	130
140.112.8.116:80	>	140.112.114.183:56210	125
140.112.8.116:80	>	140.112.114.183:56207	23
140.112.8.116:80	>	140.112.114.183:56218	19
108.177.97.157:443	->	140.112.114.183:56201	3

Total Out-of-Order : 35

140.112.8.116:80	>	140.112.114.183:56213	17
140.112.8.116:80	>	140.112.114.183:56218	16
140.112.8.116:80	>	140.112.114.183:56211	1
140.112.8.116:80	>	140.112.114.183:56215	1

Total Lost Segment : 68

140.112.8.116:80	->	140.112.114.183:56218	22
140.112.8.116:80	->	140.112.114.183:56217	11
140.112.8.116:80	->	140.112.114.183:56213	10
140.112.8.116:80	->	140.112.114.183:56214	8
140.112.8.116:80	->	140.112.114.183:56211	4
140.112.8.116:80	->	140.112.114.183:56215	4

分析案例五

重複嘗試登入

- * 不尋常的重複嘗試登入，可能被入侵的徵兆
 - * 傳統偵測方式：需於應用程式 Access Log 進行分析
- SSH login failed**

```
Last failed login: Mon Nov 20 08:59:19 CST 2017 from 223.68.134.29 on ssh:notty
There were 4770 failed login attempts since the last successful login.
Last login: Mon Oct 30 20:59:47 2017 from davisyoupc.cc.ntu.edu.tw
```

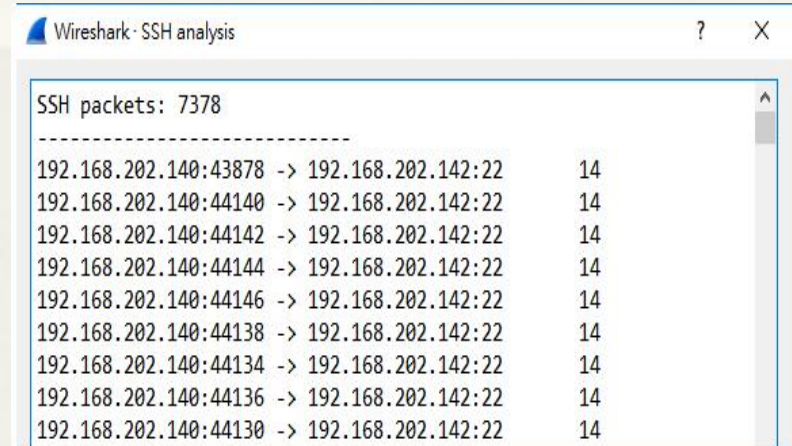
RDP login failed

等級	日期和時間	來源	事件識別碼	工作類別
資訊	2017/10/25 下午 04:06:51	TerminalServices-RemoteConnectionMana...	1149	無
資訊	2017/10/25 下午 04:06:51	TerminalServices-RemoteConnectionMana...	261	無
資訊	2017/10/25 下午 04:06:51	TerminalServices-RemoteConnectionMana...	261	無
資訊	2017/10/25 下午 04:06:45	TerminalServices-RemoteConnectionMana...	261	無
資訊	2017/10/25 下午 04:06:42	TerminalServices-RemoteConnectionMana...	261	無
資訊	2017/10/25 下午 04:06:38	TerminalServices-RemoteConnectionMana...	261	無
資訊	2017/10/25 下午 04:06:34	TerminalServices-RemoteConnectionMana...	261	無
資訊	2017/10/25 下午 04:06:31	TerminalServices-RemoteConnectionMana...	261	無
資訊	2017/10/25 下午 04:06:25	TerminalServices-RemoteConnectionMana...	261	無
資訊	2017/10/25 下午 03:53:32	TerminalServices-RemoteConnectionMana...	1149	無
資訊	2017/10/25 下午 03:53:32	TerminalServices-RemoteConnectionMana...	261	無
資訊	2017/10/25 下午 03:53:32	TerminalServices-RemoteConnectionMana...	261	無
資訊	2017/10/25 下午 03:05:11	TerminalServices-RemoteConnectionMana...	1149	無
資訊	2017/10/25 下午 03:05:10	TerminalServices-RemoteConnectionMana...	261	無
資訊	2017/10/25 下午 03:05:09	TerminalServices-RemoteConnectionMana...	261	無

分析案例五

重複嘗試登入...

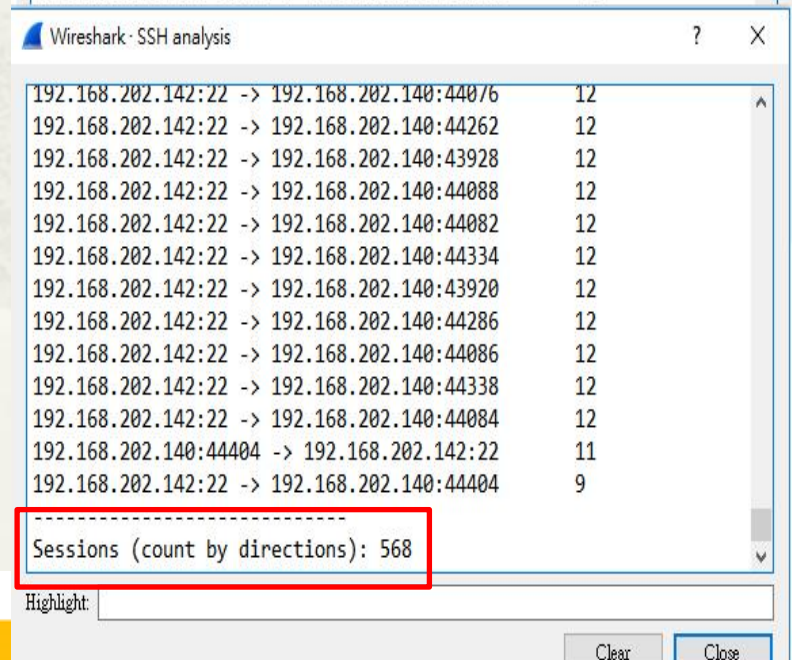
- * 分析連入 Server 封包，相同 Client IP 在短時間內不斷建立不同 tcp.stream，即可能是嘗試登入行為
- * 自行新增 Lua script 程式碼



Wireshark - SSH analysis

SSH packets: 7378

Source IP:Port	Destination IP:Port	Count
192.168.202.140:43878	192.168.202.142:22	14
192.168.202.140:44140	192.168.202.142:22	14
192.168.202.140:44142	192.168.202.142:22	14
192.168.202.140:44144	192.168.202.142:22	14
192.168.202.140:44146	192.168.202.142:22	14
192.168.202.140:44138	192.168.202.142:22	14
192.168.202.140:44134	192.168.202.142:22	14
192.168.202.140:44136	192.168.202.142:22	14
192.168.202.140:44130	192.168.202.142:22	14



Wireshark - SSH analysis

192.168.202.142:22	192.168.202.140:44076	12
192.168.202.142:22	192.168.202.140:44262	12
192.168.202.142:22	192.168.202.140:43928	12
192.168.202.142:22	192.168.202.140:44088	12
192.168.202.142:22	192.168.202.140:44082	12
192.168.202.142:22	192.168.202.140:44334	12
192.168.202.142:22	192.168.202.140:43920	12
192.168.202.142:22	192.168.202.140:44286	12
192.168.202.142:22	192.168.202.140:44086	12
192.168.202.142:22	192.168.202.140:44338	12
192.168.202.142:22	192.168.202.140:44084	12
192.168.202.140:44404	192.168.202.142:22	11
192.168.202.142:22	192.168.202.140:44404	9

Sessions (count by directions): 568

Highlight:

Clear Close



LAYER 7 網路行為分析

Layer 7 分析-傳統方式

* 傳統分析方式

* 21 ftp

* 22 ssh

* 23 telnet

* 80 http

* 443 https

* ...

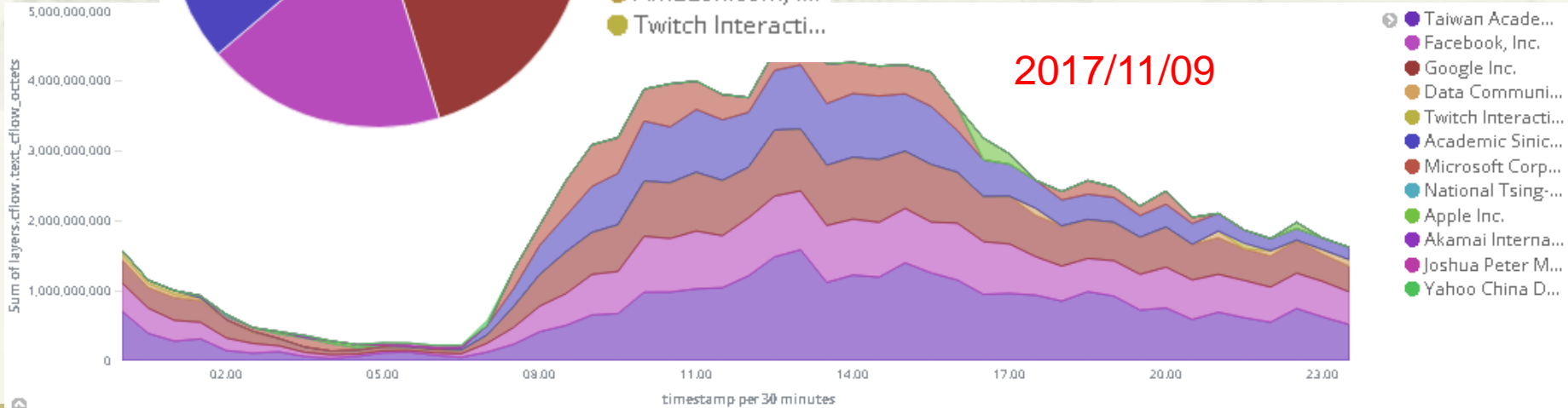
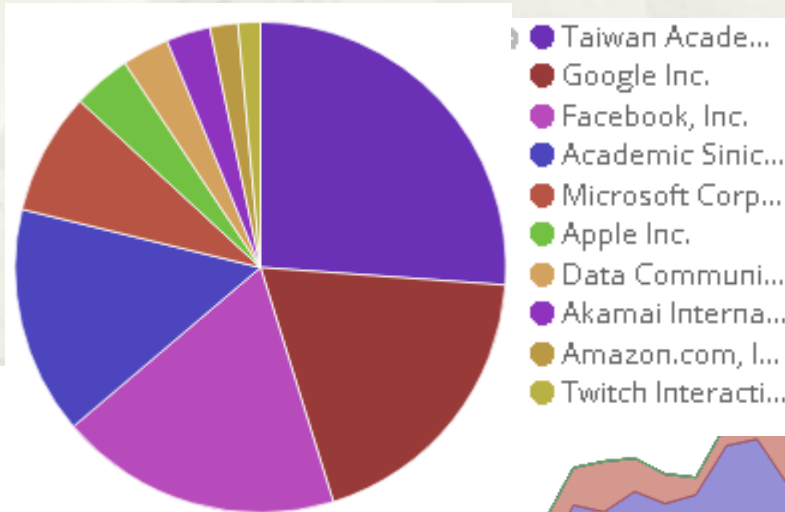


Layer 7 分析-ASN

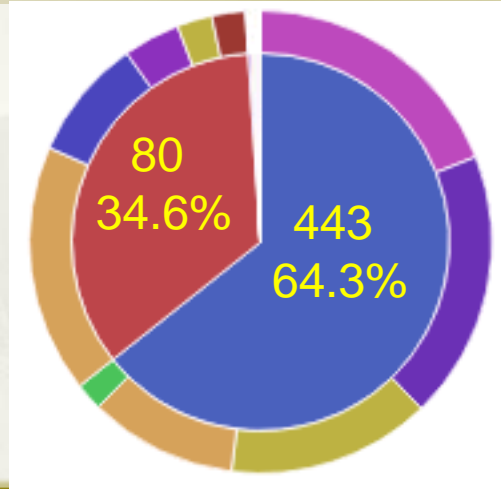
- * 使用 Geoip 查詢 IP 所屬 Autonomous System Number(ASN)
 - * 優點: 現有 IP 就可分析，可套用於現成 Netflow 分析工具
 - * 缺點: 僅能大略分析網路行為，無法辨識如 P2P 等 Protocol

Layer 7 分析-ASN

- * 區網 TAnet 100G Top 10 ASN 分析結果
- * netflow + ELK Stack



Layer 7 分析-ASN



port	Source ASN	%
443	Facebook, Inc.	26%
443	Google Inc.	25%
443	Academic Sinica Network	19%
443	Taiwan Academic Network (TANet) Information Center	14%
443	Data Communication Business Group	3%
80	Taiwan Academic Network (TANet) Information Center	50%
80	Microsoft Corporation	25%
80	Apple Inc.	11%
80	Academic Sinica Network	8%
80	Akamai International B.V.	6%

Layer 7 分析-DPI

- * 使用 DPI (Deep Packet Inspection) 分析
 - * 商業硬體設備
 - * Proprietary protocol pattern 非公開
 - * 倚賴廠商不斷更新 pattern
 - * Open Source DPI Library
 - * nDPI, Support 186+ application protocols
 - * <https://github.com/ntop/nDPI/tree/dev/example>
 - * 網路社群力量大

nDPI Support 186+ Protocols

FTP POP SMTP IMAP DNS IPP HTTP MDNS NTP NETBIOS NFS SSDP BGP SNMP
XDMCP SMB SYSLOG DHCP PostgreSQL MySQL TDS DirectDownloadLink I23V5
AppleJuice DirectConnect Socrates WinMX VMware PANDO Filetopia iMESH Kontiki
OpenFT Kazaa/Fasttrack Gnutella eDonkey Bittorrent OFF AVI Flash OGG MPEG
QuickTime RealMedia Windowsmedia MMS XBOX QQ MOVE RTSP Feidian Icecast PPLive
PPStream Zattoo SHOUTCast SopCast TVAnts TVUplayer VeohTV QQLive
Thunder/Webthunder Souseek GaduGadu IRC Popo Jabber MSN Oscar Yahoo Battlefield
Quake VRRP Steam Halflife2 World of Warcraft Telnet STUN IPSEC GRE ICMP IGMP EGP
SCTP OSPF IP in IP RTP RDP VNC PCAnywhere SSL SSH USENET MGCP IAX TFTP AFP
StealthNet Aimini SIP Truphone ICMPv6 DHCPv6 Armagetron CrossFire Dofus Fiesta
Florensia Guildwars HTTP Application Activesync Kerberos LDAP MapleStory msSQL PPTP
WARCRAFT3 World of Kung Fu MEEBO FaceBook Twitter DropBox Gmail Google Maps
YouTube Skype Google DCE RPC NetFlow_IPFIX sFlow HTTP Connect (SSL over HTTP)
HTTP Proxy Netflix Citrix CitrixOnline/GotoMeeting Apple (iMessage, FaceTime...) Webex
WhatsApp Apple iCloud Viber Apple iTunes Radius WindowsUpdate TeamViewer Tuenti
LotusNotes SAP GTP UPnP LLMNR RemoteScan Spotify H323 OpenVPN NOE CiscoVPN
TeamSpeak Tor CiscoSkinny RTCP RSYNC Oracle Corba UbuntuONE CNN Wikipedia
Whois-DAS Collectd Redis ZeroMQ Megaco QUIC WhatsApp Voice Stracraft Teredo
Snapchat Simet OpenSignal 99Taxi GloboTV Deezer Instagram Microsoft cloud services
Twitch KakaoTalk Voice and Chat HotspotShield VPN

Install nDPI with Wireshark

* Wireshark Extcap plugin

Wireshark Authors Folders Plugins Keyboard Shortcuts License

Name	Location	Typical Files
"File" dialogs	D:\	capture files
Temp	C:\WiresharkPortable\Data\Temp	untitled capture files
Personal configuration	C:\WiresharkPortable\Data\	d/filters, preferences, ethers, ...
Global configuration	C:\WiresharkPortable\App\Wireshark	d/filters, preferences, manu/f, ...
System	C:\WiresharkPortable\App\Wireshark	ethers, ipxnets
Program	C:\WiresharkPortable\App\Wireshark	program files
Personal Plugins	C:\WiresharkPortable\Data\plugins	dissector plugins
Global Plugins	C:\WiresharkPortable\App\Wireshark\plugins	dissector plugins
Extcap path	C:\WiresharkPortable\App\Wireshark\extcap	Extcap Plugins search path

Capture

..using this filter:


- utun1
- Loopback: lo0
- Wi-Fi: en1
- gif0
- stf0
- FireWire: fw0
- p2p0
- Cisco remote capture: cisco
- nDPI interface: ndpi
- Random packet generator: randpkt
- SSH remote capture: ssh
- UDP Listener remote capture: udpdump

nDPI Layer 7 protocol 分析

Src port	Destination	Dest port	Protocol	Length	info
443	140.112.41.76	2242	SSL.Facebook	1492	[TCP segment of a reassembled PDUI]
443	140.112.41.76	2242	SSL.Facebook	1492	[TCP segment of a reassembled PDUI]
443	140.112.41.76	2242	SSL.Facebook	1458	App
443	140.112.41.76	2242	SSL.Facebook	1492	[TCP segment of a reassembled PDUI]
2461	216.58.200.46	443	SSL.Google	135	App
2461	216.58.200.46	443	SSL.Google	138	App
2461	216.58.200.46	443	SSL.Google	124	App
443	140.112.41.76	2461	SSL.Google	151	App
2461	216.58.200.46	443	SSL.Google	120	App
443	140.112.41.76	2461	SSL.Google	88	443
443	140.112.41.76	2461	SSL.Google	120	App
443	140.112.41.76	2461	SSL.Google	88	443
2461	216.58.200.46	443	TCP	82	2461
2393	111.221.29.193	443	TCP	82	2393
2394	111.221.29.194	443	TCP	82	2394
443	140.112.41.76	1808	SSL.Dropbox	339	App
1808	162.125.34.129	443	SSL.Dropbox	1091	App
443	140.112.41.76	1808	SSL.Dropbox	88	443
443	140.112.41.76	1808	SSL.Dropbox	437	App
1808	162.125.34.129	443	SSL.Dropbox	817	App

Protocol	Size	Percentage
SSL	2.5 MB	[60.5 %]
QUIC.GMail	725.97 KB	[17.2 %]
SSL.Facebook	438.13 KB	[10.4 %]
QUIC.Google	334.06 KB	[7.9 %]
Unknown	51.76 KB	[1.2 %]
SSL.Google	35.27 KB	[< 1 %]
QUIC	16.23 KB	[< 1 %]
QUIC.YouTube	10.63 KB	[< 1 %]
BitTorrent	10.42 KB	[< 1 %]
SSL.Amazon	7.78 KB	[< 1 %]
DNS	7.44 KB	[< 1 %]

Flow	Size	Percentage
203.66.159.1 / 140.112.41.128 [SSL]	2.26 MB	[54.7 %]
172.217.24.5 / 140.112.41.128 [QUIC.GMail]	650.83 KB	[15.4 %]
31.13.87.36 / 140.112.41.128 [SSL.Facebook]	238.69 KB	[5.6 %]
31.13.87.5 / 140.112.41.128 [SSL.Facebook]	174.31 KB	[4.1 %]
202.39.235.195 / 140.112.41.128 [SSL]	145.76 KB	[3.4 %]
140.112.41.128 / 172.217.24.5 [QUIC.GMail]	72.36 KB	[1.7 %]
216.58.200.238 / 140.112.41.128 [QUIC.Google]	49.51 KB	[1.2 %]
74.125.204.189 / 140.112.41.128 [QUIC.Google]	49.01 KB	[1.2 %]
74.125.23.189 / 140.112.41.128 [QUIC.Google]	49.01 KB	[1.2 %]
172.217.24.14 / 140.112.41.128 [QUIC.Google]	44.96 KB	[1.1 %]
140.112.41.128 / 172.217.24.14 [QUIC.Google]	38.91 KB	[< 1 %]



簡報完畢
謝謝