Trojan.Congur 事件說明

林宜進

簡介

- TACERT 陳老師在12/12日信中問有關於Congur資安事件相關問題，為以下這三點:
  1. 此類資安事件的偵測規則之特徵內容為何?
  2. 是APP本身權限問題嗎?
  3. 有其他偵測的特徵嗎?(信中舉的範例是IP位置)

IPS上的規則

- 內對外連線 (dst port 是 6280)
- **封包內容包含以下特徵(共五個)**
  1. /collect
  2. ts=
  3. ver=
  4. diff=
  5. hash=

廠商的確認回覆

4

Dear 宜進,

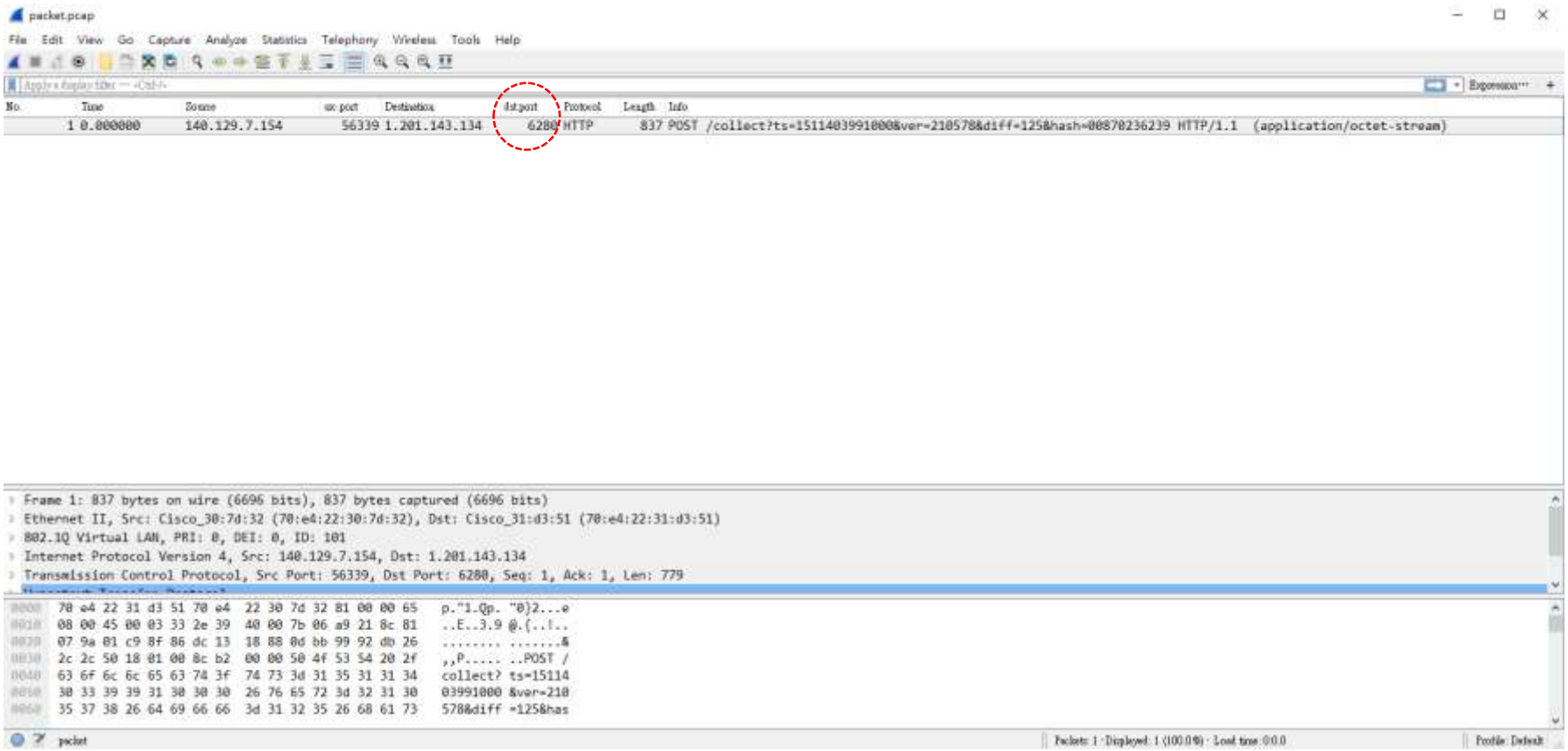
1. IP問題，從IPS上看，這些觸發事件的目標IP會連到韓國和大陸的IP，這個事件的規則是否和目標IP無關?
   此事件規則與目標IP無關
2. 封包特徵，從IPS上看到的規則是要符合5個特徵才會觸發，請問這些特徵的內容是甚麼?
   依照snort rule，只要符合下列5個特徵即會觸發告警

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 6280 (msg:"MALWARE-CNC Andr.Trojan.Congur variant outbound connection detected"; flow:to_server,established;
content:"/collect"; fast_pattern:only; content:"ts="; nocase; content:"ver="; nocase; content:"diff="; nocase; content:"hash="; nocase; metadata:impact_flag
red, policy balanced-ips drop, policy security-ips drop, service http;
reference:url,virustotal.com/en/file/cd050a2868646f231c544c566ba3cc34538e63a5125a2c7ad1f4bbd41d5e8cdd/analysis/; classtype:trojan-activity; sid:44554;
rev:1; )
```

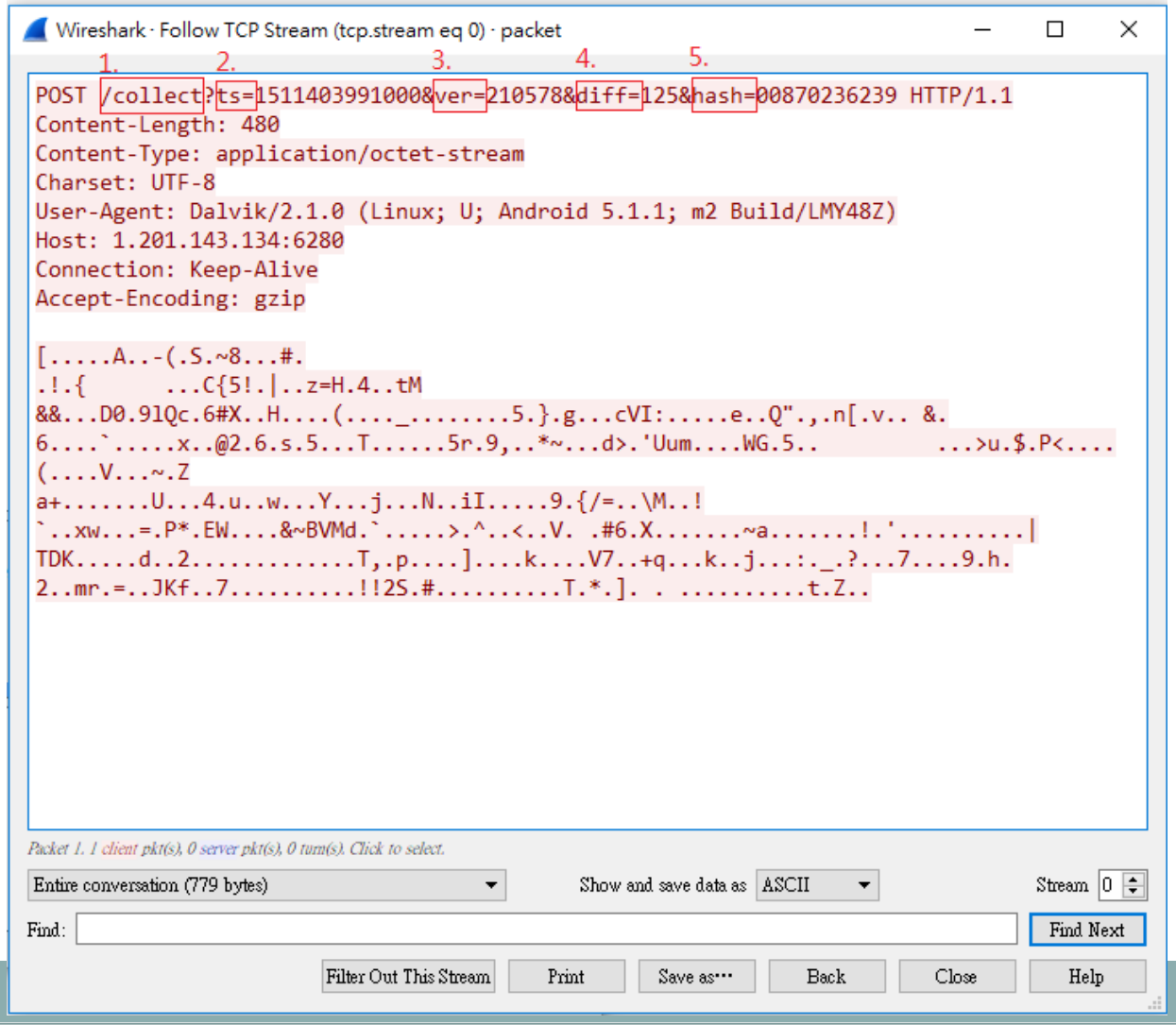
```
POST /collect?ts=1459318632000&ver=25483557&diff=1989&hash=00850463526 HTTP/1.1
Content-Length: 480
Content-Type: application/octet-stream
Charset: UTF-8
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0.1; Redmi Note 3 MIUI/V8.1.1.0.MHOMIDI)
Host: 123.56.205.151:6280
Connection: Keep-Alive
Accept-Encoding: gzip

...i.      .3..M69N{..x..R.._.......#..C..n:...     ...a......-.b>.-..>(..$..][...
9.!.......:0.6.^;.|,.Qe.V...N...E.:.YL.....A......-.ef...If....f.!G....C3o.6..B.]'. 7_.
$;.#.D.....y..%.0)...3Y..P..<#...~.B...D.....8..w....^[-...>cT.\.. -..z}Hi..).....)2.
:t......,.|d?.gr......7....Z.
1..u..)OA.Oe.n3..-..xR{^P..N.&..R]1..q.Y.f.n.l...&F).S/..FJ.XD...
#...S..q738.|2..Q.M...EKD..Z......F....u.....R*.....b...&T..
2.h...F4."P.tS..x..h.^.o..R.R.Mf...\1.k.F....~...m...9@.$.
.@|.%....!S....<$_.?
```

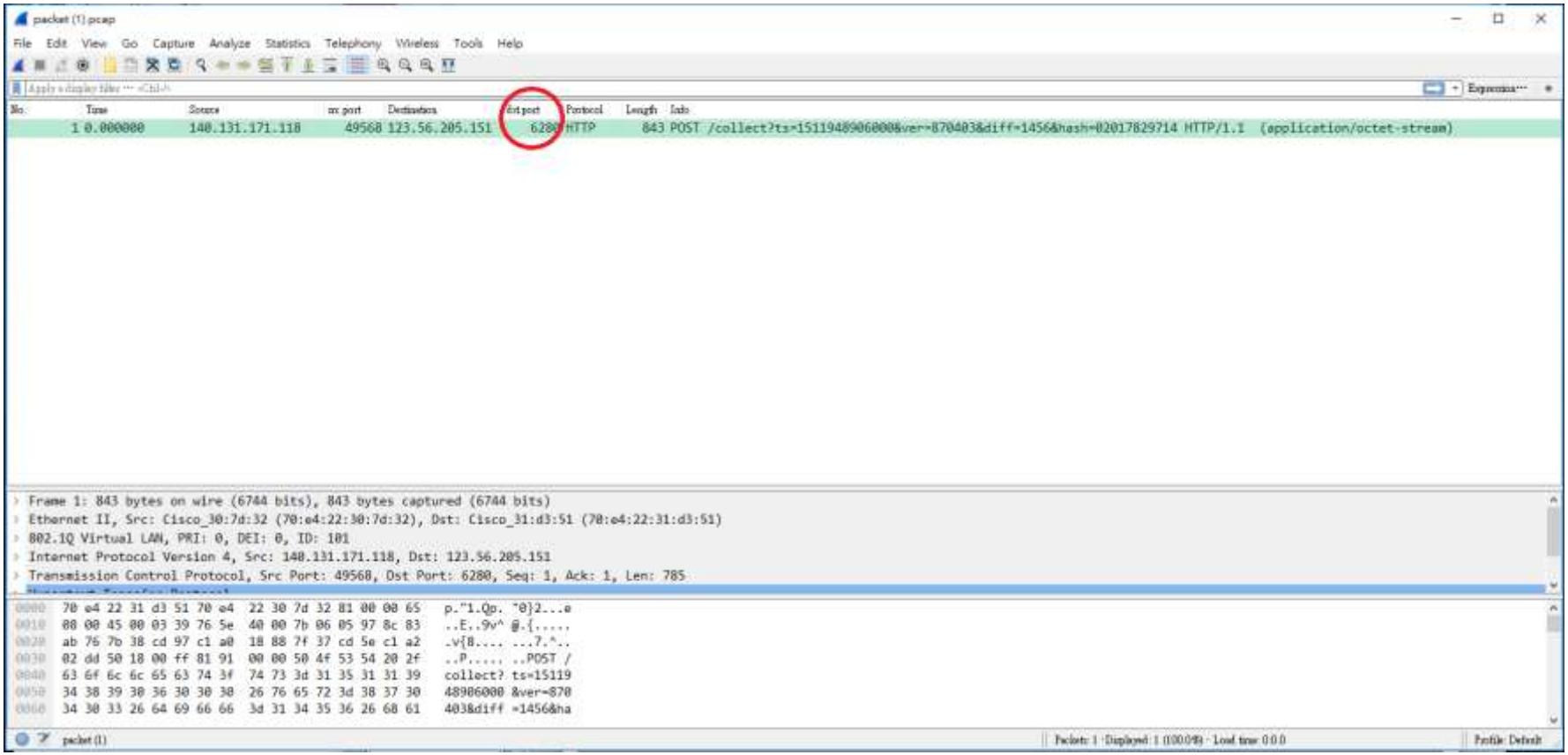
IPS上的封包範例-1 (dst port 6280)



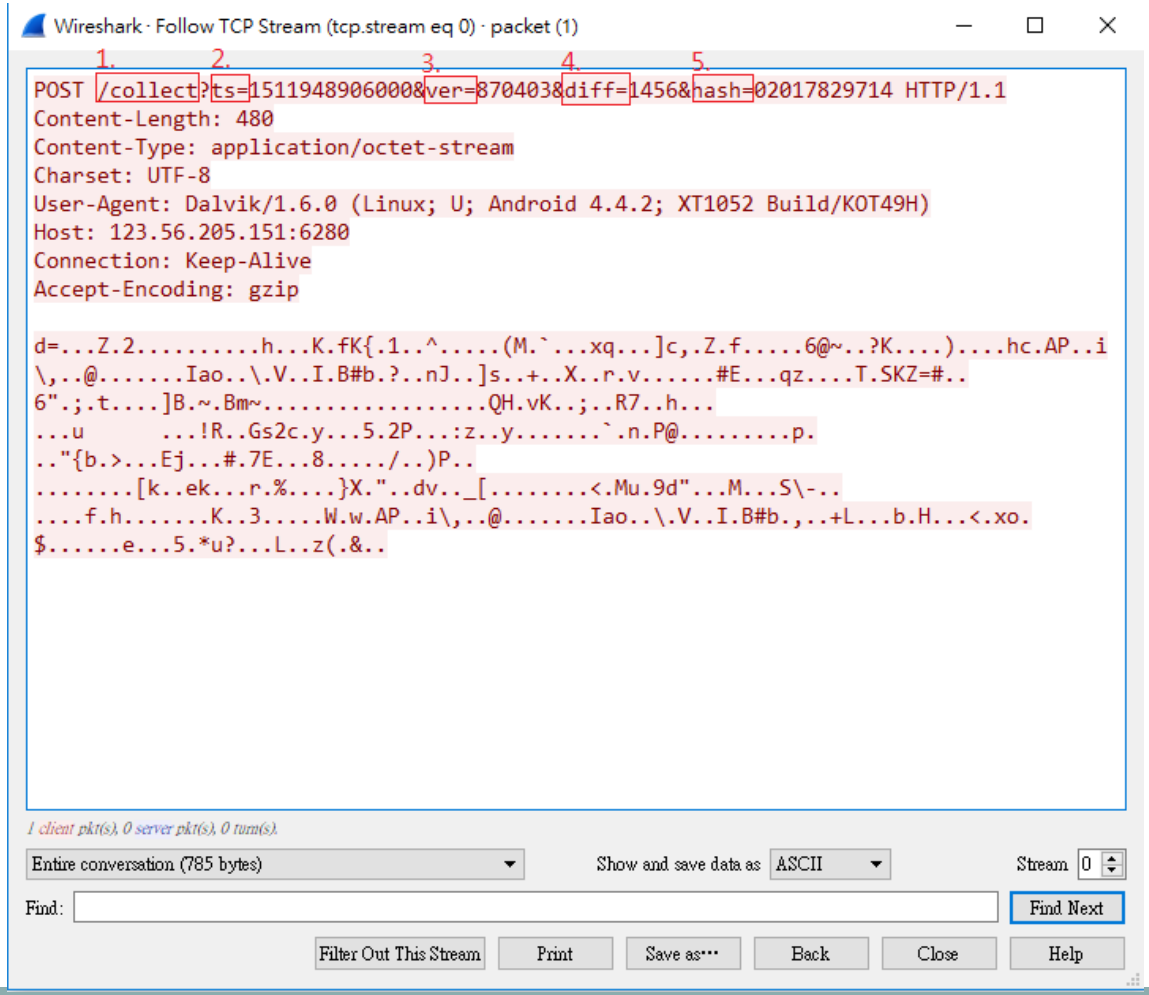
IPS上的封包範例-1 (符合特徵)



IPS上的封包範例-2 (dst port 6280)



IPS上的封包範例-2 (符合特徵)



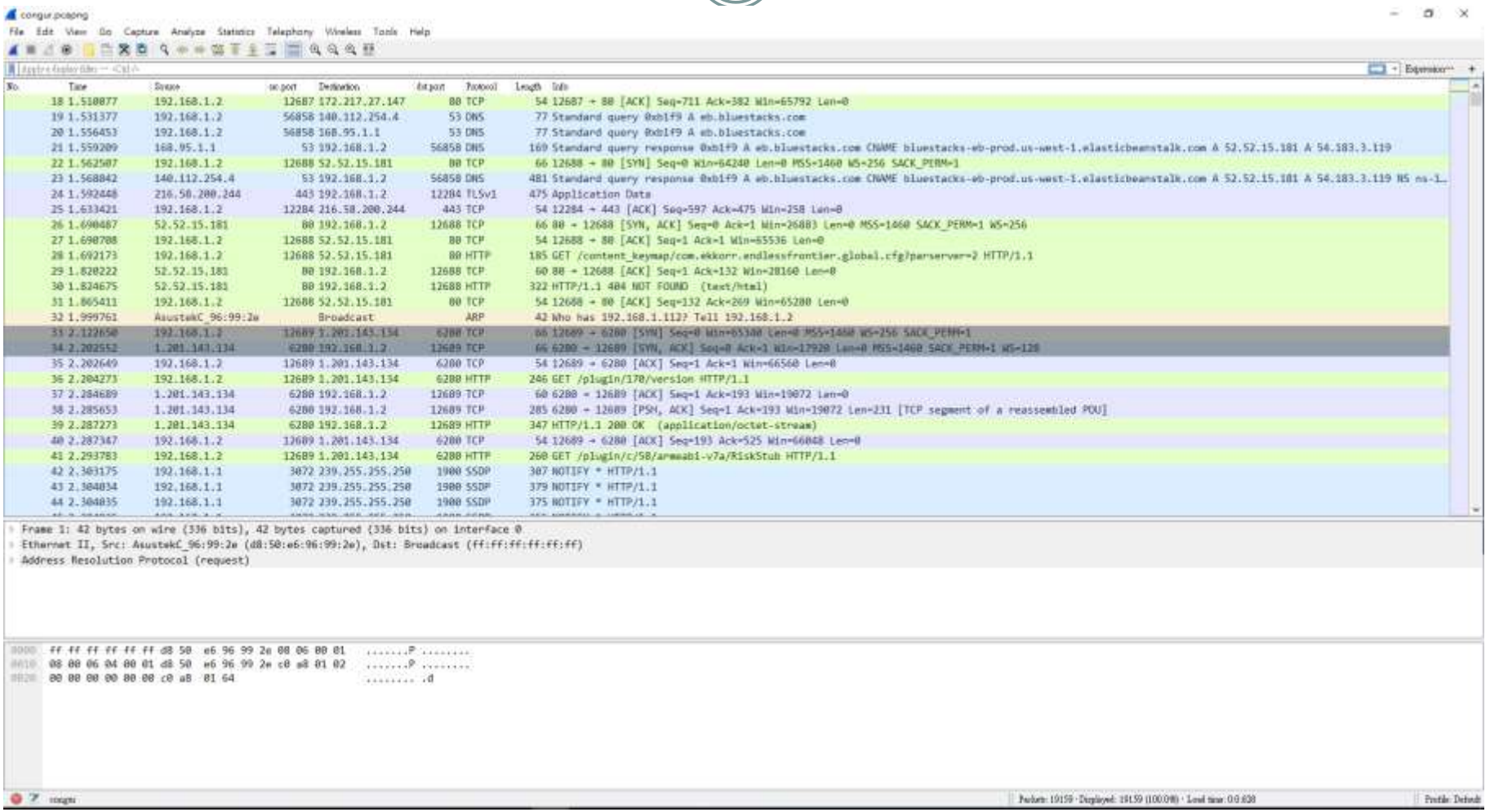
結論

- 此次Congur資安事件是符合IPS上的規則而開單；從IPS上調閱的封包，經過檢查後也都符合IPS的規則
- 似乎跟目標IP沒有太大的相關性(從該規則中只提到目標port)
- IPS無法檢查該APP權限的問題。

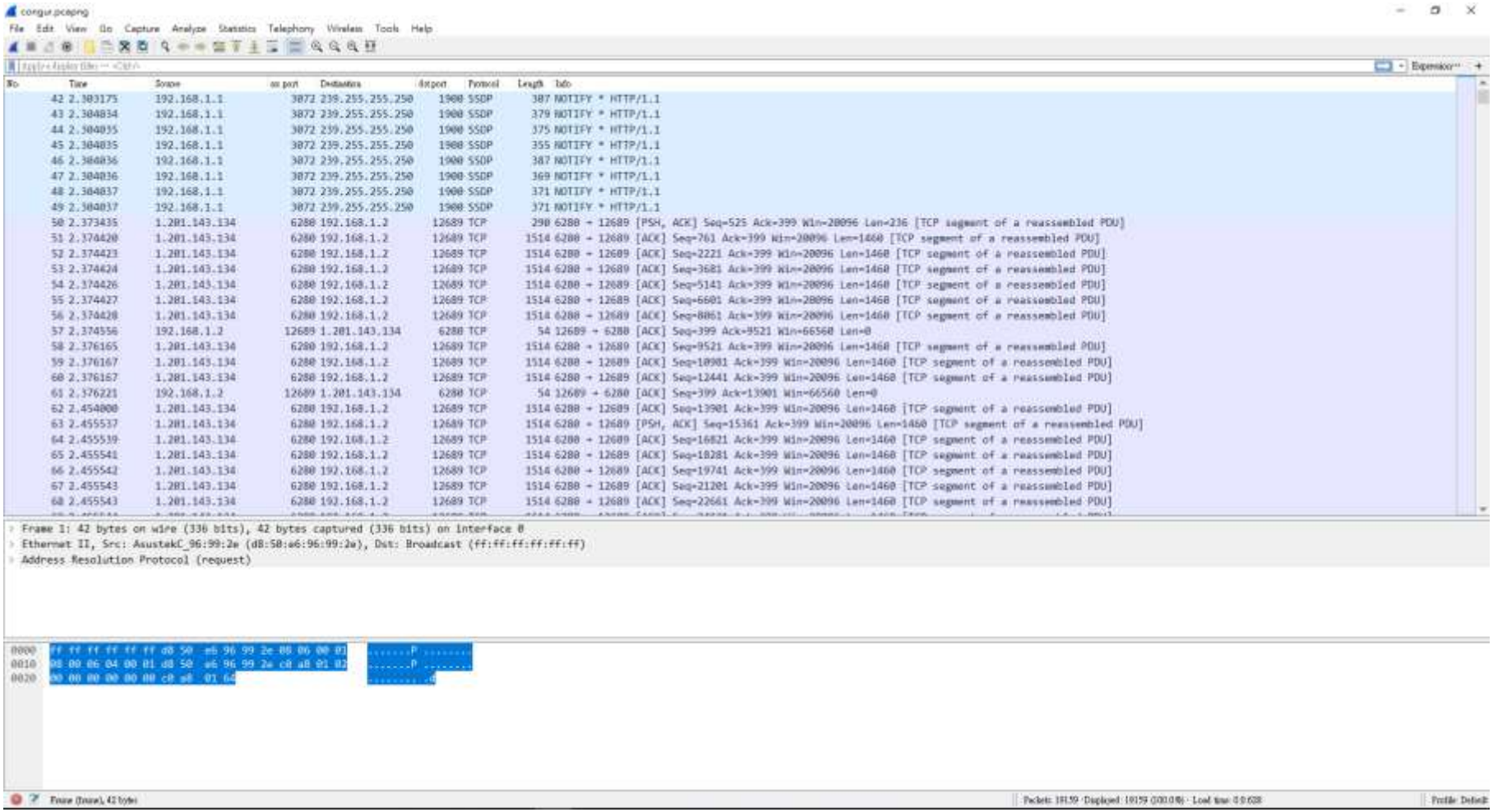
實測環境

- OS: Windows 10 Pro (1703版)
- Android模擬器: BlueStacks 3
- 測試遊戲:無盡的邊疆 1.8.9 (非LINE版本)
- 測試時間:約5分鐘
- 測試時的IP: 192.168.1.2 (筆電接網路線到AP，AP接出去的IP為140.112.3.250)

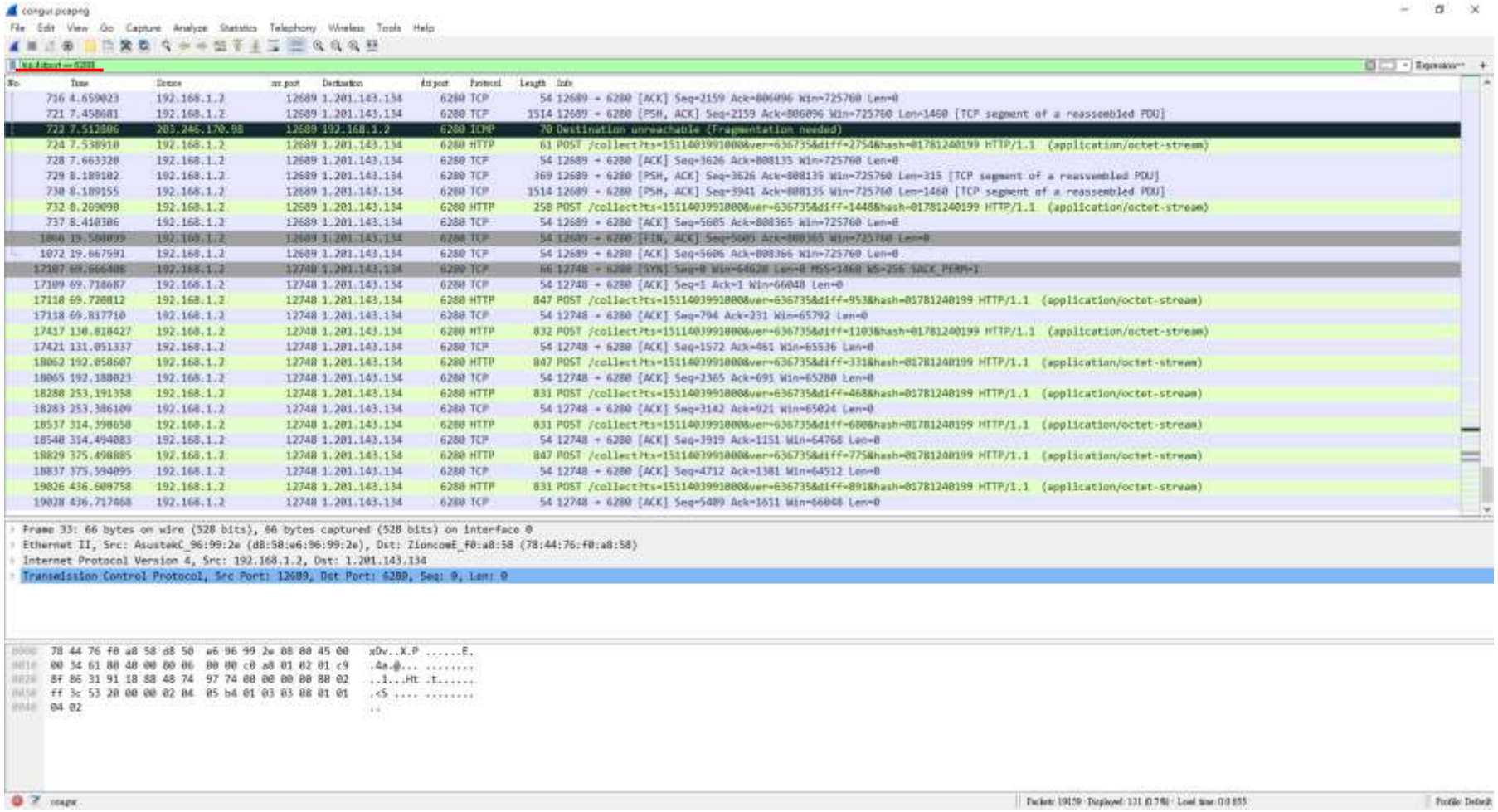
實測封包-1(無使用Filter)



實測封包-2(無使用Filter)

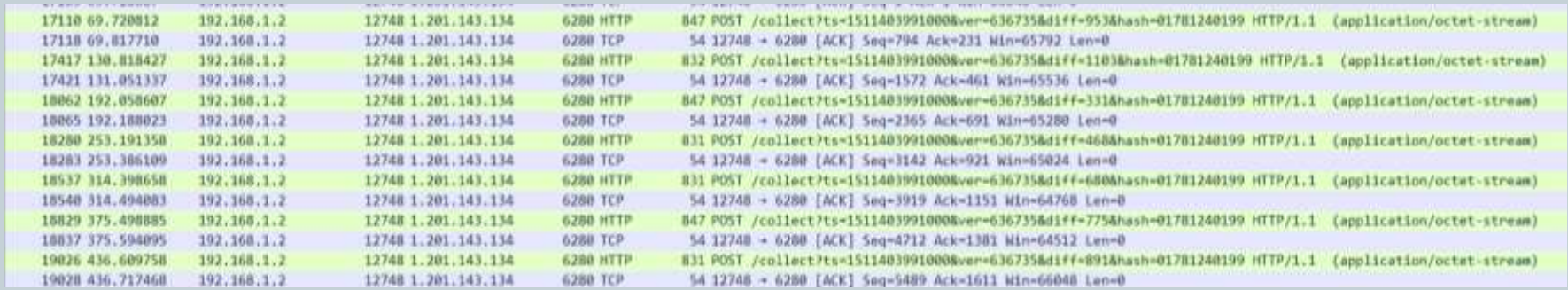


實測封包-3(設filter)



觀察的結果

- 已知在遊玩遊戲時，平均1分鐘會丟出觸發資安事件的封包內容(如下圖，不論是沒有動作或是點擊遊戲內的icon)
- 目前有請廠商和原廠確認此規則的判斷細節，再另行回覆通知我們ASOC。



```
17110 69.720812   192.168.1.2   12748 1.201.143.134   6280 HTTP   847 POST /collect?ts=1511403991000&ver=636735&diff=953&hash=01781240199 HTTP/1.1  (application/octet-stream)
17118 69.817710   192.168.1.2   12748 1.201.143.134   6280 TCP     54 12748 → 6280 [ACK] Seq=794 Ack=231 Win=65792 Len=0
17417 130.818427  192.168.1.2   12748 1.201.143.134   6280 HTTP   832 POST /collect?ts=1511403991000&ver=636735&diff=1103&hash=01781240199 HTTP/1.1  (application/octet-stream)
17421 131.051337  192.168.1.2   12748 1.201.143.134   6280 TCP     54 12748 → 6280 [ACK] Seq=1572 Ack=461 Win=65536 Len=0
18062 192.058607  192.168.1.2   12748 1.201.143.134   6280 HTTP   847 POST /collect?ts=1511403991000&ver=636735&diff=331&hash=01781240199 HTTP/1.1  (application/octet-stream)
18065 192.188023  192.168.1.2   12748 1.201.143.134   6280 TCP     54 12748 → 6280 [ACK] Seq=2365 Ack=691 Win=65280 Len=0
18280 253.191358  192.168.1.2   12748 1.201.143.134   6280 HTTP   831 POST /collect?ts=1511403991000&ver=636735&diff=468&hash=01781240199 HTTP/1.1  (application/octet-stream)
18283 253.386109  192.168.1.2   12748 1.201.143.134   6280 TCP     54 12748 → 6280 [ACK] Seq=3142 Ack=921 Win=65024 Len=0
18537 314.398658  192.168.1.2   12748 1.201.143.134   6280 HTTP   831 POST /collect?ts=1511403991000&ver=636735&diff=680&hash=01781240199 HTTP/1.1  (application/octet-stream)
18540 314.494083  192.168.1.2   12748 1.201.143.134   6280 TCP     54 12748 → 6280 [ACK] Seq=3919 Ack=1151 Win=64768 Len=0
18829 375.498885  192.168.1.2   12748 1.201.143.134   6280 HTTP   847 POST /collect?ts=1511403991000&ver=636735&diff=775&hash=01781240199 HTTP/1.1  (application/octet-stream)
18837 375.594095  192.168.1.2   12748 1.201.143.134   6280 TCP     54 12748 → 6280 [ACK] Seq=4712 Ack=1381 Win=64512 Len=0
19026 436.609758  192.168.1.2   12748 1.201.143.134   6280 HTTP   831 POST /collect?ts=1511403991000&ver=636735&diff=891&hash=01781240199 HTTP/1.1  (application/octet-stream)
19028 436.717468  192.168.1.2   12748 1.201.143.134   6280 TCP     54 12748 → 6280 [ACK] Seq=5489 Ack=1611 Win=66048 Len=0
```