

1. 解釋標準

- 甲、RFC 7540: Hypertext Transfer Protocol Version 2 (HTTP/2)，是個可以向下相容於 HTTP/1.1 的新標準。他可以更有效率的使用網路資源、可以多工的處理 requests 和 responses 來加快網頁讀取速度等等。<https://tools.ietf.org/html/rfc7540>
- 乙、RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2，是個定義 1.2 版 Transport Layer Security (TLS) 的文件，這個協定可以防通訊被竊聽等等的問題，也對 handshake 等等進行優化。<https://tools.ietf.org/html/rfc5246>
- 丙、IEEE 802.15.4: 定義了 low-rate wireless personal area networks (LR-WPANs) 通訊協定，是個針對短距離、低功率、低速度的無線通訊所訂定的標準
https://en.wikipedia.org/wiki/IEEE_802.15.4

2. 分析 unknown.pcap

- 甲、Source: 10.18.119.44
Destination: 10.18.116.221

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.18.119.44	10.18.116.221	KRB5	357	AS-REQ

乙、8 bytes

- 丙、Kerberos，是一種計算機網路授權協議，用來在非安全網路中，對個人通信以安全的手段進行身份認證，客戶端和伺服器端均可對對方進行身份認證。可以用於防止竊聽、防止重放攻擊、保護數據完整性等場合。

```
> Frame 1: 357 bytes on wire (2856 bits), 357 bytes captured (2856 bits)
> Ethernet II, Src: Alcatel-4c:10:05 (00:d0:95:4c:10:05), Dst: HewlettP_ce:ba
> Internet Protocol Version 4, Src: 10.18.119.44, Dst: 10.18.116.221
▼ User Datagram Protocol, Src Port: 2694, Dst Port: 88
    Source Port: 2694
    Destination Port: 88
    Length: 323
    Checksum: 0x54d1 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
▼ Kerberos
    > as-req
```

0020	74 dd 0a 86 00 58 01 43 54 d1 6a 82 01 37 30 82	t...X.C T.j..70.
0030	01 33 a1 03 02 01 05 a2 03 02 01 0a a3 67 30 65	.3..... ..g0e
0040	30 50 a1 03 02 01 02 a2 49 04 47 30 45 a0 03 02	0P..... I.G0E...
0050	01 17 a1 06 02 04 00 b4 e6 30 a2 36 04 34 b9 190.6.4..
0060	37 af d2 66 aa 16 ed 15 4f 6e ad 12 8f b4 7a f4	7..f.... On....z.
0070	eb 28 8d 5e 97 67 00 2b fd 0a 7d be bd 6e 02 42	.(.^.g.+ ..}.n.B
0080	1a da 36 70 01 a1 84 a4 28 b7 73 95 53 94 d5 21	..6p.... (.s.S..!
0090	69 38 30 11 a1 04 02 02 00 80 a2 09 04 07 30 05	i80..... ..0.
00a0	a0 03 01 01 ff a4 81 bd 30 81 ba a0 07 03 05 00 0.....
00b0	40 81 00 10 a1 1d 30 1b a0 03 02 01 01 a1 14 30	@.....0.0
00c0	12 1b 10 e5 8b 95 e5 93 a1 e7 a7 91 e7 a7 91 e9
00d0	95 b7 24 a2 0d 1b 0b 41 42 43 44 2e 43 4f 4d 2e	..\$....A BCD.COM.
00e0	54 57 a3 20 30 1e a0 03 02 01 02 a1 17 30 15 1b	TW. 0... ..0..
00f0	06 6b 72 62 74 67 74 1b 0b 41 42 43 44 2e 43 4f	.krbtgt. .ABCD.CO
0100	4d 2e 54 57 a5 11 18 0f 32 30 33 37 30 39 31 33	M.TW.... 20370913
0110	30 32 34 38 30 35 a6 11 18 0f 32 30 33 37 30	024805Z. ...20370

User Datagram Protocol (udp), 8 bytes

3. 測速

本次網路速度測試結果如下：

本測試資料僅供參考

來賓IP：	210.66.250.63
測試檔案大小(1MB=1024x1024x8bits)	4 MB
本次花費時間	1.121 秒
本次測試速度	31.038 Mbps
平均測試速度 (共 1 次測試)	---

請選擇要測的檔案大小：

甲、早上 8 點

4MB ▼

再次測試

本次網路速度測試結果如下：

本測試資料僅供參考

來賓IP：	210.66.250.63
測試檔案大小(1MB=1024x1024x8bits)	64 MB
本次花費時間	18.074 秒
本次測試速度	30.802 Mbps
平均測試速度 (共 2 次測試)	---

請選擇要測的檔案大小：

乙、中午 12 點

64MB ▼

再次測試

丙、晚上 8 點

本次網路速度測試結果如下：

本測試資料僅供參考

來賓IP：	140.123.101.248
測試檔案大小(1MB=1024x1024x8bits)	4 MB
本次花費時間	0.684 秒
本次測試速度	30.678 Mbps
平均測試速度 (共 1 次測試)	---

請選擇要測的檔案大小：

4MB



再次測試

丁、與網卡速度是否有差異：有 (100 Mbps vs 30 Mbps 左右)

原因：宿舍區絕對不會是只有我一人在使用網路，所以頻寬被共享掉後我不會得到全部的網路速度(頻寬)！

```
命令提示字元
Microsoft Windows [版本 10.0.14393]
(c) 2016 Microsoft Corporation. 著作權所有，並保留一切權利。

C:\Users\UsHome4045>tracert www.cs.ccu.edu.tw

在 30 個跳點上
追蹤 www.cs.ccu.edu.tw [140.123.101.3] 的路由:

  1  9 ms  5 ms  1 ms  192.168.216.1
  2  1 ms  1 ms  1 ms  h63-210-66-250.seed.net.tw [210.66.250.63]
  3  12 ms  5 ms  1 ms  h126-210-66-250.seed.net.tw [210.66.250.126]
  4  *      *      *      要求等候逾時。
  5  3 ms  4 ms  3 ms  192.72.113.129
  6  7 ms  8 ms  6 ms  140.123.231.250
  7  6 ms  6 ms  6 ms  140.130.252.250
  8  6 ms  6 ms  6 ms  140.123.9.238
  9  6 ms  7 ms  6 ms  www.cs.ccu.edu.tw [140.123.101.3]

追蹤完成。

C:\Users\UsHome4045>
```

4.

5. 四種 packet delay

- 甲、Nodal processing: 進行 bit error checking, 還有從 packet's header 決定出 packet 要送去哪裡的時間
- 乙、Queueing delay: 在 router queue 中等待被傳輸的時間
- 丙、Transmission delay: 送資料進入 link 的時間（取決於頻寬）
- 丁、Propagation delay: 資料在網路線中跑的時間

```
C:\Users\UsHome4045>nslookup www.cs.ccu.edu.tw
伺服器: UnKnown
Address: 192.168.2.1

未經授權的回答:
名稱: www.cs.ccu.edu.tw
Address: 140.123.101.3

C:\Users\UsHome4045>nslookup www.ccu.edu.tw
伺服器: UnKnown
Address: 192.168.2.1

未經授權的回答:
名稱: herol.ccu.edu.tw
Addresses: 2001:288:6001:5::5
140.123.5.5
Aliases: www.ccu.edu.tw
```

6.

7. 這題太有意思了，記得大一的時候我們的比賽隊名 581DDOS 就是因為這個事件而命名的呀。

- 甲、Github 遭受到攻擊
<https://zh.wikipedia.org/wiki/%E5%AF%B9Git%EF%9A%84%E5%AE%A1%E6%9F%A5%E5%92%8C%E5%B0%81%E9%94%81>
- 乙、大陸有長城防火牆，所以有一些國外的新聞網站是無法看到的，因此有些人把某些新聞網掛在 Github 上面(畢竟長城防火牆沒有擋下 Github)，像是 CN-NYTimes。
中國政府希望透過 DDOS 手段讓 Github 認知到這件事情，希望可以達成讓這些 repo 下架的目的。
- 丙、Wiki 上面有提及四大手法，其中之一是利用中國大陸以外的網友與翻牆的網友瀏覽被劫持的百度 JavaScript 檔案，讓他們每 2 秒向 GitHub 上的 GreatFire 或紐約時報中文網 發出 request。
這招後來被 GitHub 暫時禁止使用彈窗警告攔住。

8. 指令說明

甲、Ping: 對基地網址傳送 ICMP 封包，測試看看與輸入的 IP 目前的連線狀況是否是通暢的

```
C:\Users\UsHome4045>ping 8.8.8.8

Ping 8.8.8.8 (使用 32 位元組的資料):
回覆自 8.8.8.8: 位元組=32 時間=14ms TTL=41
回覆自 8.8.8.8: 位元組=32 時間=13ms TTL=41
回覆自 8.8.8.8: 位元組=32 時間=14ms TTL=41
回覆自 8.8.8.8: 位元組=32 時間=14ms TTL=41

8.8.8.8 的 Ping 統計資料:
    封包: 已傳送 = 4, 已收到 = 4, 已遺失 = 0 (0% 遺失),
    大約的來回時間 (毫秒):
        最小值 = 13ms, 最大值 = 14ms, 平均 = 13ms
```

乙、Tcpcmdump: 封包分析工具 (在 linux 上執行)

```
Nodejs gti:(master) sudo tcpdump -l ens33
[sudo] password for henrybear327:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), capture size 262144 bytes
17:39:46.392271 IP tsa03s01-in-f238.1e100.net.https > 192.168.100.131.54354: Flags [P.], seq 1456502353:1456502416, ack 2910206492, win 64240, length 63
17:39:46.392302 IP 192.168.100.131.54354 > tsa03s01-in-f238.1e100.net.https: Flags [.] , ack 63, win 30016, length 0
17:39:46.393118 IP tsa03s01-in-f238.1e100.net.https > 192.168.100.131.54354: Flags [P.], seq 63, ack 1, win 64240, length 0
17:39:46.393990 IP 192.168.100.131.54354 > tsa03s01-in-f238.1e100.net.https: Flags [F.], seq 1, ack 64, win 30016, length 0
17:39:46.395679 IP tsa03s01-in-f238.1e100.net.https > 192.168.100.131.54354: Flags [.] , ack 2, win 64239, length 0
17:39:46.408368 IP 192.168.100.131.38213 > 192.168.100.2.domain: 38605+ PTR? 131.100.168.192.in-addr.arpa. (46)
17:39:46.427420 IP 192.168.100.2.domain > 192.168.100.131.38213: 38605 NXDomain 0/0/0 (46)
17:39:46.440196 IP 192.168.100.131.38213 > 192.168.100.2.domain: 41663+ PTR? 2.100.168.192.in-addr.arpa. (44)
17:39:46.448531 IP 192.168.100.2.domain > 192.168.100.131.38213: 41663 NXDomain 0/0/0 (44)
17:39:47.801160 IP 192.168.100.131.51037 > tl-in-f189.1e100.net.https: UDP, length 23
17:39:47.802267 IP 192.168.100.131.38213 > 192.168.100.2.domain: 32290+ PTR? 189.189.233.64.in-addr.arpa. (45)
17:39:47.817591 IP 192.168.100.2.domain > 192.168.100.131.38213: 32290 1/0/0 PTR tl-in-f189.1e100.net. (79)
17:39:47.840827 IP tl-in-f189.1e100.net.https > 192.168.100.131.51037: UDP, length 31
17:39:48.228069 IP 192.168.100.131.38213 > 192.168.100.2.domain: 2235+ A? chikuu.tw. (27)
17:39:48.236430 IP 192.168.100.131.38213 > 192.168.100.2.domain: 33165+ A? stats.hosting24.com. (37)
17:39:48.237148 IP 192.168.100.131.38213 > 192.168.100.2.domain: 52202+ A? www.google-analytics.com. (42)
17:39:48.238109 IP 192.168.100.131.38213 > 192.168.100.2.domain: 19767+ A? fonts.googleapis.com. (38)
17:39:48.246405 IP 192.168.100.2.domain > 192.168.100.131.38213: 52202 2/0/0 CNAME www-google-analytics.l.google.com., A 216.58.200.238 (102)
17:39:48.246441 IP 192.168.100.2.domain > 192.168.100.131.38213: 19767 2/0/0 CNAME googleadapis.l.google.com., A 64.233.189.95 (90)
17:39:48.255879 IP 192.168.100.2.domain > 192.168.100.131.38213: 33165 1/0/0 A 31.170.100.65 (53)
17:39:48.257680 IP 192.168.100.131.36644 > 31.170.100.65.http: Flags [S], seq 174037566, win 29200, options [mss 1460,sackOK,TS val 33744850 ecr 0,nop,wscale 7], length 0
17:39:48.259070 IP 192.168.100.131.38213 > 192.168.100.2.domain: 6590+ PTR? 65.160.170.31.in-addr.arpa. (44)
17:39:48.261688 IP 192.168.100.131.36646 > 31.170.100.65.http: Flags [S], seq 3900605736, win 29200, options [mss 1460,sackOK,TS val 33744851 ecr 0,nop,wscale 7], length 0
17:39:48.280327 IP 192.168.100.131.47602 > tsa03s01-in-f238.1e100.net.https: UDP, length 1350
17:39:48.287298 IP 192.168.100.131.47093 > tl-in-f95.1e100.net.https: UDP, length 1350
17:39:48.290186 IP tsa03s01-in-f238.1e100.net.https > 192.168.100.131.47602: UDP, length 1350
17:39:48.296213 IP tsa03s01-in-f238.1e100.net.https > 192.168.100.131.47602: UDP, length 31
17:39:48.546648 IP 192.168.100.131.38213 > 192.168.100.2.domain: 9326+ PTR? 95.189.233.64.in-addr.arpa. (44)
17:39:48.570231 IP 192.168.100.2.domain > 192.168.100.131.38213: 9326 1/0/0 PTR tl-in-f95.1e100.net. (77)
17:39:48.717689 IP 31.170.161.90.http > 192.168.100.131.55682: Flags [S.], seq 2118925469, ack 941866631, win 64240, options [mss 1460], length 0
17:39:48.717955 IP 192.168.100.131.38213 > 192.168.100.2.domain: 32219+ PTR? 90.161.170.31.in-addr.arpa. (44)
17:39:48.718252 IP 192.168.100.131.55682 > 31.170.161.90.http: Flags [.] , ack 1, win 29200, length 0
17:39:48.718755 IP 31.170.161.90.http > 192.168.100.131.55684: Flags [S.], seq 937392357, ack 1720400765, win 64240, options [mss 1460], length 0
17:39:48.718782 IP 192.168.100.131.55682 > 31.170.161.90.http: Flags [P.], seq 1:509, ack 1, win 29200, length 508: HTTP: GET /android-x-firebase-03-KE8NB3K87KE6K96K99KE6K9FA5KE8KA9KA2/ HT
```

丙、Ipconfig: 列出這台電腦的所有網路卡相關資訊

```
命令提示字元
'ipconfig' 不是內部或外部命令、可執行的程式或批次檔。

C:\Users\UsHome4045>ipconfig

Windows IP 設定

乙太網路卡 乙太網路 2:

    連線特定 DNS 尾碼 . . . . . : 
    連結-本機 IPv6 位址 . . . . . : fe80::b0ef:b037:a636:f010%8
    IPv4 位址 . . . . . : 192.168.2.100
    子網路遮罩 . . . . . : 255.255.255.0
    預設閘道 . . . . . : 192.168.2.1

乙太網路卡 VMware Network Adapter VMnet1:

    連線特定 DNS 尾碼 . . . . . : 
    連結-本機 IPv6 位址 . . . . . : fe80::10b2:c175:eb75:17b5%21
    IPv4 位址 . . . . . : 192.168.20.1
    子網路遮罩 . . . . . : 255.255.255.0
    預設閘道 . . . . . : 

乙太網路卡 VMware Network Adapter VMnet8:

    連線特定 DNS 尾碼 . . . . . : 
    連結-本機 IPv6 位址 . . . . . : fe80::4096:991:5161:ebde%6
    IPv4 位址 . . . . . : 192.168.100.1
    子網路遮罩 . . . . . : 255.255.255.0
    預設閘道 . . . . . :
```