INNOVATION

運用PING通道穿透防火牆

指導老師：林淑玲老師

227 13 翁健展、227 11 林秉軒

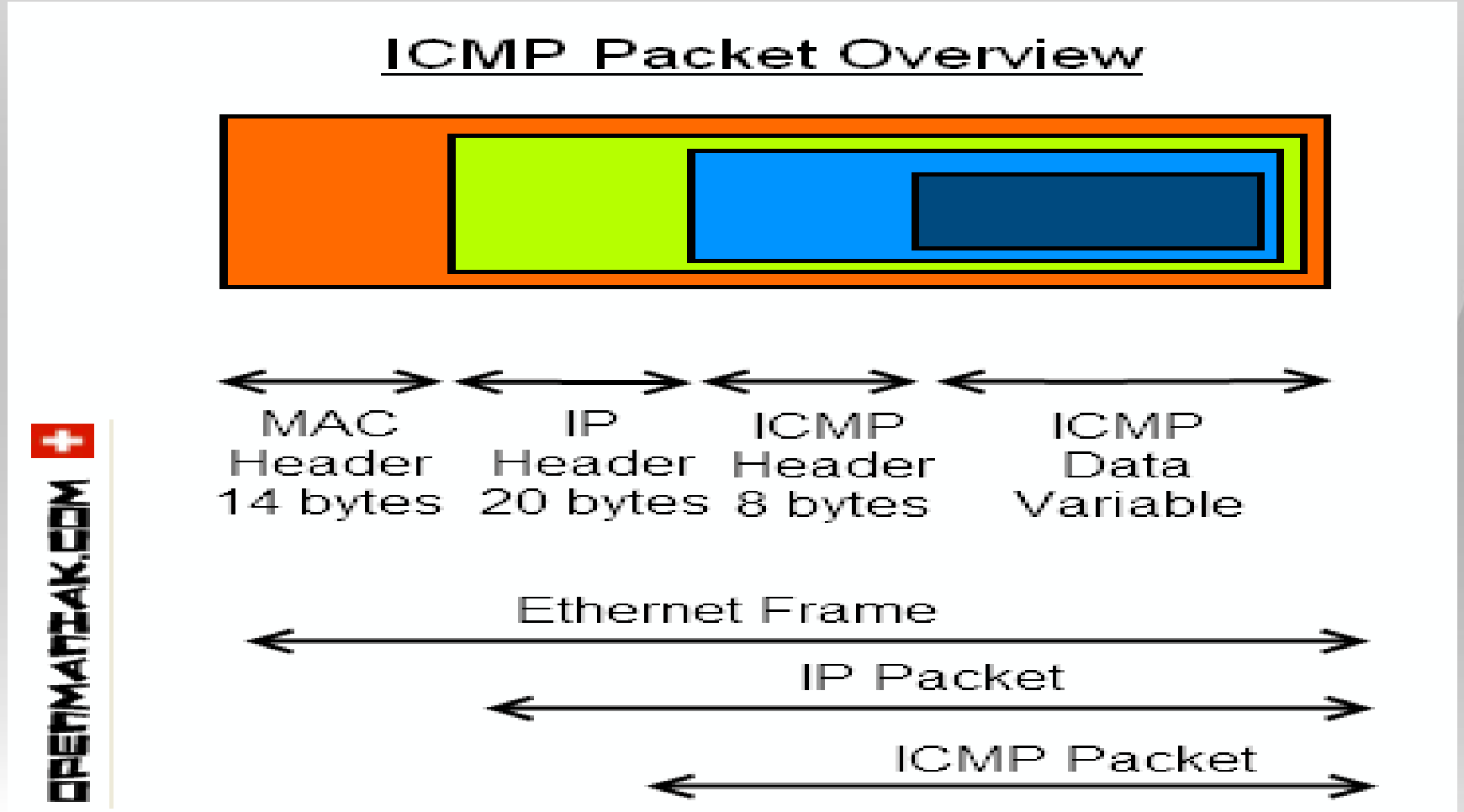
資訊組 INFORMATION

壹、研究動機

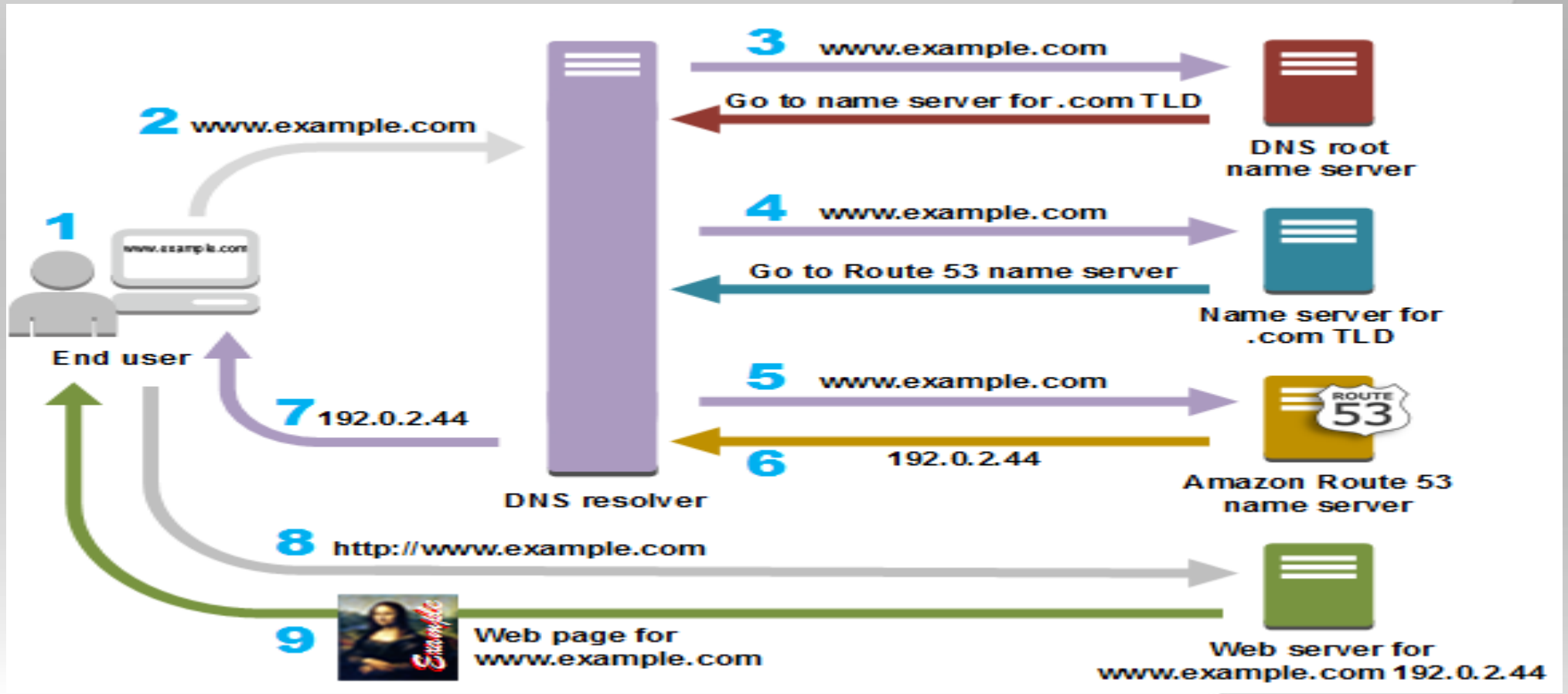
- 大家有聽過X華電信的時間管理員嗎？
- 以前曾經被父母利用電信公司的時間管理員管制上網時間，用到足夠晚之後就會直接無法上網。
- 為了能在晚上上網，我們嘗試找方法能夠繞過電信公司的封鎖。

INNOVATION

背景知識



DNS



INNOVATION

貳、研究工具

COMPUTER

WIRESHARK

SOFTETHER

INNOVATION

參、研究架構

INNOVATION

肆、研究過程

A)PING TUNNEL

一、觀察

二、初步測試

```
C:\Users\shink>tracert google.com

在上限 30 個躍點上
追蹤 google.com [172.217.24.14] 的路由:

  1     2 ms     2 ms     2 ms  192.168.30.1
  2     8 ms     6 ms     6 ms  h254.s98.ts.hinet.net [168.95.98.254]
  3     *        *        *     要求等候逾時。
  4     7 ms     8 ms    11 ms  203-75-90-98.HINET-IP.hinet.net [203.75.90.98]
  5     7 ms    15 ms    11 ms  tpdt-3307.hinet.net [168.95.80.82]
  6     9 ms     8 ms     7 ms  tpdb-3021.hinet.net [220.128.26.94]
  7     7 ms     8 ms     8 ms  pcpd-3211.hinet.net [220.128.26.105]
  8     9 ms     9 ms    10 ms  72.14.218.140
  9    14 ms     8 ms     8 ms  209.85.240.135
 10     6 ms    10 ms     6 ms  209.85.254.233
 11    15 ms     9 ms    10 ms  tsa01s07-in-f14.1e100.net [172.217.24.14]
```

INNOVATION

三、尋找可用軟體

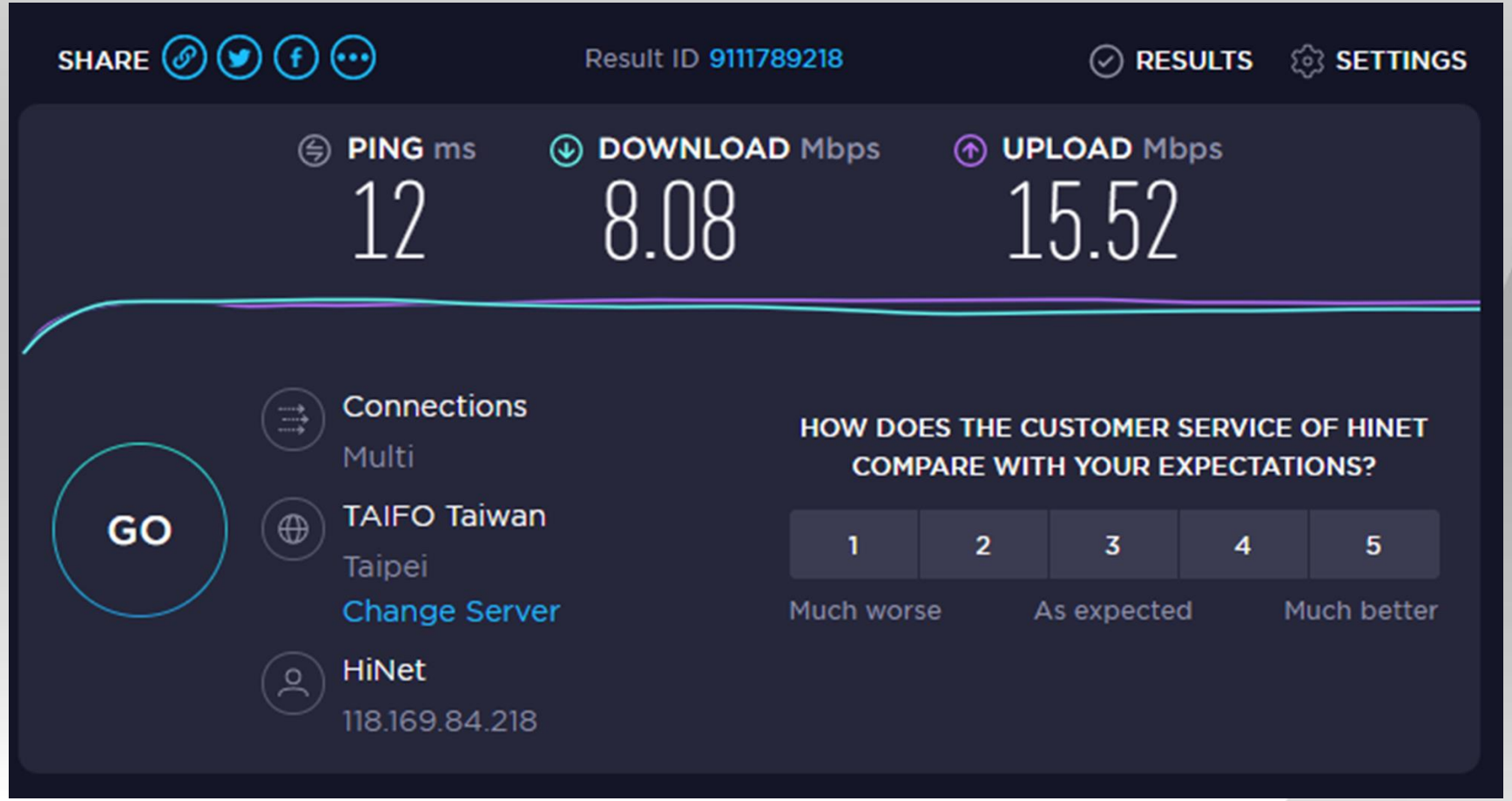
四、架設伺服器

```
user@server:~$ sudo hans -s 192.168.11.0 -p shinkansen -fvr
[sudo] password for user:
hans: opened tunnel device: tun0
hans: unknown client: 235.13.15.94
hans: new client: 1.162.204.36 (192.168.11.100)
hans: sending challenge to: 1.162.204.36
hans: connection established: 1.162.204.36
hans: unknown client: 235.13.15.94
hans: unknown client: 235.13.15.94
```

```
pi@raspberrypi:~ $ sudo hans -c pingshinkansen942.ddns.net -p shinkansen -fv
hans: opened tunnel device: tun0
hans: sending connection request
hans: invalid packet type: 7, state: 1
hans: sending connection request
hans: challenge received
hans: sending challenge response
hans: connection established
```

INNOVATION

五、測試



INNOVATION

肆、研究過程

Ｂ)DNS TUNNEL

INNOVATION

一、觀察

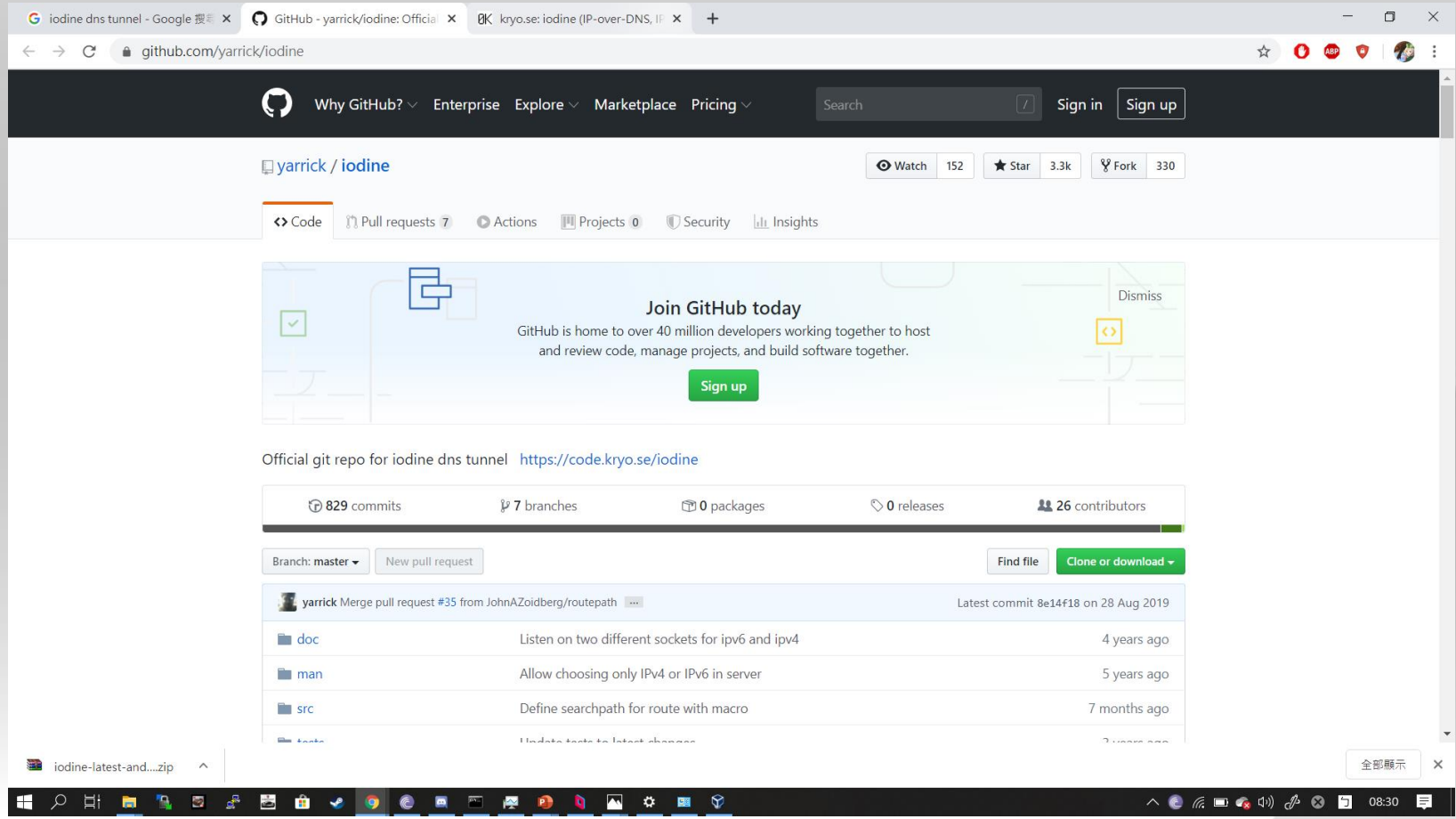
```
C:\Users\shink>tracert google.com

在上限 30 個躍點上
追蹤 google.com [172.217.24.14] 的路由:

  1     2 ms     2 ms     2 ms  192.168.30.1
  2     8 ms     6 ms     6 ms  h254.s98.ts.hinet.net [168.95.98.254]
  3     *        *        *     要求等候逾時。
  4     7 ms     8 ms    11 ms  203-75-90-98.HINET-IP.hinet.net [203.75.90.98]
  5     7 ms    15 ms    11 ms  tpdt-3307.hinet.net [168.95.80.82]
  6     9 ms     8 ms     7 ms  tpdb-3021.hinet.net [220.128.26.94]
  7     7 ms     8 ms     8 ms  pcpd-3211.hinet.net [220.128.26.105]
  8     9 ms     9 ms    10 ms  72.14.218.140
  9    14 ms     8 ms     8 ms  209.85.240.135
 10     6 ms    10 ms     6 ms  209.85.254.233
 11    15 ms     9 ms    10 ms  tsa01s07-in-f14.1e100.net [172.217.24.14]
```

INNOVATION

二、尋找可用軟體



INNOVATION

三、取得網域

- 首先我們需要先取得一個網域，而後我們需要在此網域上建立一個運用ＮＳ解析紀錄的副網域並且將此ＮＳ紀錄指向一個所要用的連線伺服器的網域或位置。

INNOVATION

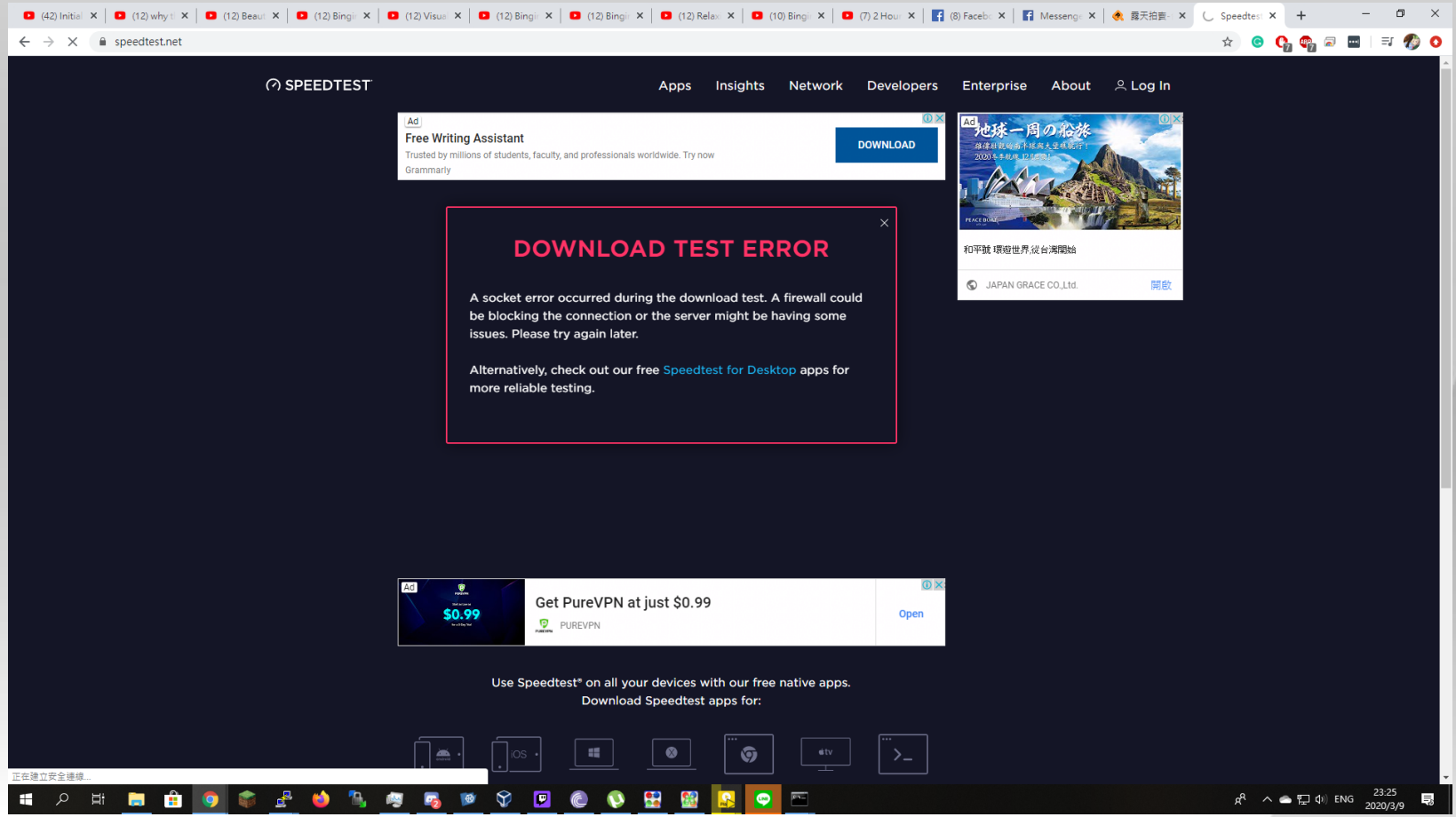
四、架設伺服器

```
user@server:~$ sudo iodined -f -c -P shinkansen 192.168.10.1 t.infor.org &
[2] 3026
user@server:~$ Opened dns0
Setting IP of dns0 to 192.168.10.1
Setting MTU of dns0 to 1130
Opened IPv4 UDP socket
Listening to dns for domain t.infor.org
```

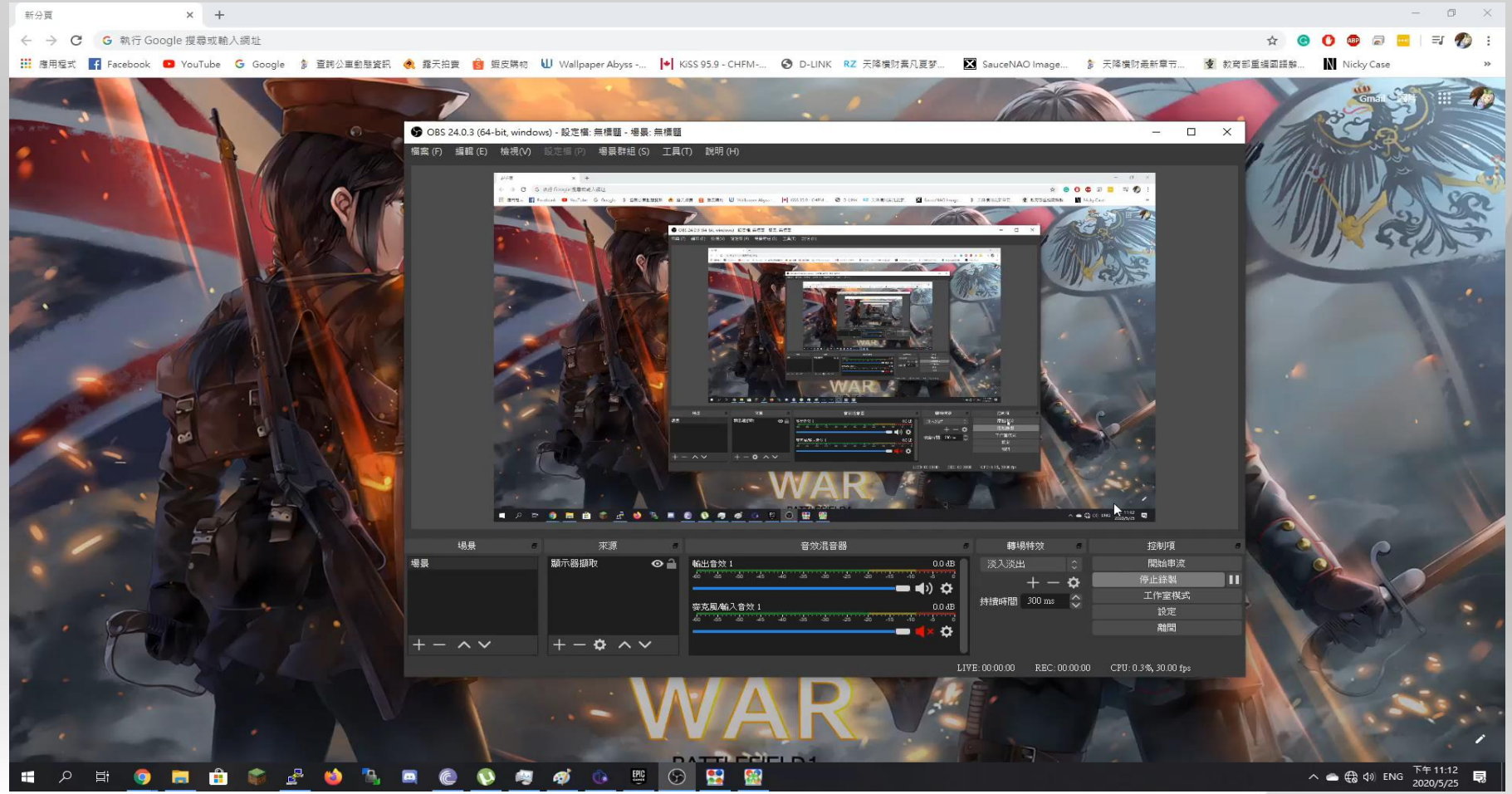
```
pi@raspberrypi:~ $ sudo iodine -f -r -P shinkansen t.infor.org &
[1] 25299
pi@raspberrypi:~ $ Opened dns0
Opened IPv4 UDP socket
Sending DNS queries for t.infor.org to 168.95.192.1
Autodetecting DNS query type (use -T to override).
Using DNS type NULL queries
Version ok, both using protocol v 0x00000502. You are user #0
Setting IP of dns0 to 192.168.10.2
Setting MTU of dns0 to 1130
Server tunnel IP is 192.168.10.1
Skipping raw mode
Using EDNS0 extension
Switching upstream to codec Base128
Server switched upstream to codec Base128
No alternative downstream codec available, using default (Raw)
Switching to lazy mode for low-latency
Server switched to lazy mode
Autoprobing max downstream fragment size... (skip with -m fragsize)
768 ok.. 1152 ok.. ...1344 not ok.. ...1248 not ok.. ...1200 not ok.. 1176 ok.. ...1188 not ok.. will use 1176-2=1174
Setting downstream fragment size to max 1174...
Connection setup complete, transmitting data.
```

INNOVATION

五、測試



INNOVATION


新分頁
執行 Google 搜尋或輸入網址
Facebook
YouTube
Google
Wallpaper Abyss -...
KiSS 95.9 - CHFM-...
D-LINK
SauceNAO Image...
Nicky Case
OBS 24.0.3 (64-bit, windows) - 設定檔: 無標題 - 場景: 無標題
檔案 (F)
編輯 (E)
檢視(V)
場景群組 (S)
工具(T)
說明 (H)
場景
來源
音效混音器
轉場特效
控制項
顯示器擷取
輸出音效 1
麥克風/輸入音效 1
淡入淡出
持續時間
300 ms
開始串流
停止錄製
工作室模式
設定
離開
LIVE: 00:00:00
REC: 00:00:00
CPU: 0.3%, 30.00 fps
WAR
ENG
下午 11:12
2020/5/25

INNOVATION

伍、未來展望

- 我們可發現此通道仍然無法建立與平時同等穩定的連線，故我們希望可尋找其餘方法與協定以求建立更加穩定的連線。
- 我們知道DNS tunnel並非只能以此方式運用，DNS tunnel常用以作為駭入所用之通道，我們希望可在於其他網路中發現此問題並且解決。

INNOVATION

謝謝大家

INNOVATION