## **NSCAP Homework #1**

Author: 0816146 韋詠祥

## 實驗內容

利用 C++ 的 libpcap 函式庫,撰寫可以指定介面卡、過濾類型、攔截數量的指令介面程式,支援 TCP、UDP 及 ICMP 協議基本解析。

## 實驗截圖

```
+ hw1 git:(master) x ./main --interface ens160
- c 4 --filter icmp
Transport type: ICMP
Source IP: 140.113.168.192
ICMP type value: 8

Transport type: ICMP
Source IP: 140.113.168.192
ICMP type value: 8

Transport type: ICMP
Source IP: 140.113.168.192
ICMP type value: 8

Transport type: ICMP
Source IP: 140.113.168.192
ICMP type value: 8

Transport type: ICMP
Source IP: 140.113.168.192
ICMP type value: 8

Transport type: ICMP
Source IP: 140.113.168.192
ICMP type value: 0

Transport type: ICMP
Source IP: 140.113.168.160
ICMP type value: 0

Transport type: ICMP
Source IP: 140.113.168.160
ICMP type value: 0

Transport type: ICMP
Source IP: 140.113.168.160
ICMP type value: 0

Transport type: ICMP
Source IP: 140.113.168.160
Destination IP: 140.113.168.160
ICMP type value: 0

Transport type: ICMP
Source IP: 140.113.168.160

Experiment 1: ICMP

Source IP: 140.113.168.160

Experiment 1: ICMP

Final diameter in the properties of data.

* hw1 git:(master) x

Experiment 1: ICMP

Inscapl 0:zsh* 1:man-

"cs.sean.cat" 11:22 21-Feb-23
```

圖 1:可正常顯示來源及目的地,並印出 ICMP 類型編號

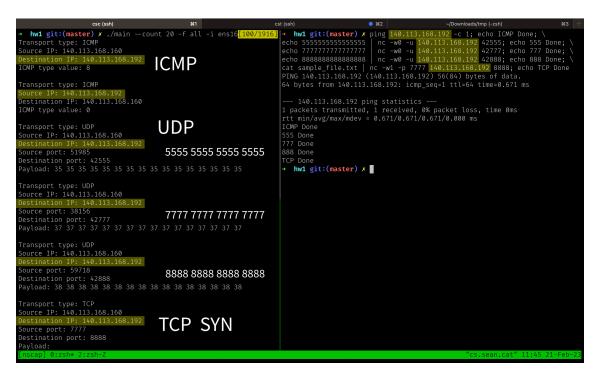


圖 2:成功解析出 UDP 傳輸內容(前 16 位元組)

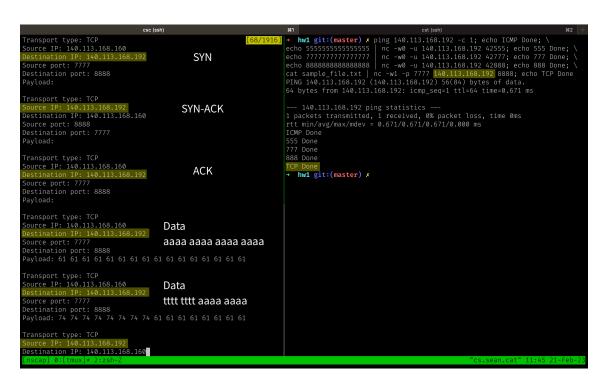


圖 3: 攔截到 TCP 封包,透過順序可以推斷三向交握過程,並顯示出部分傳輸資料