

40647027S 陳冠穎

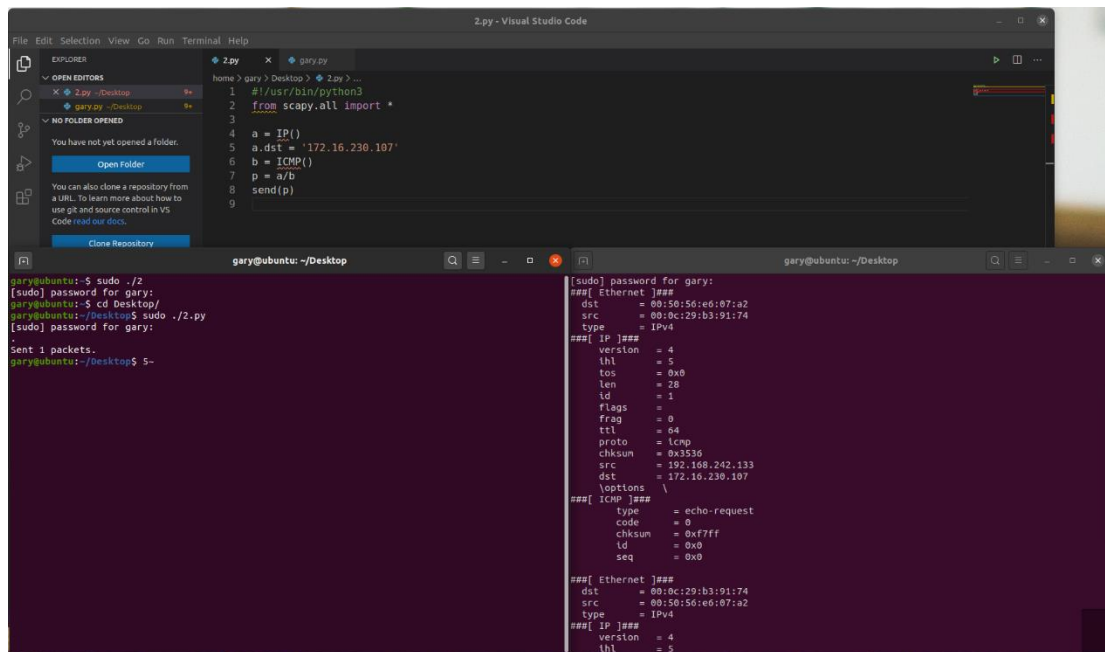
沒使用 `sudo` 執行的話會報錯 `Operation not permitted`。

Task1.1B

1. ICMP: pkt = sniff(filter='icmp',prn=print_pkt)
2. pkt = sniff(filter='port 23 and tcp and src net 192.168',prn=print_pkt)
3. pkt = sniff(filter='src or dst net 172.16',prn=print_pkt)

[illegible]

Task 1.2



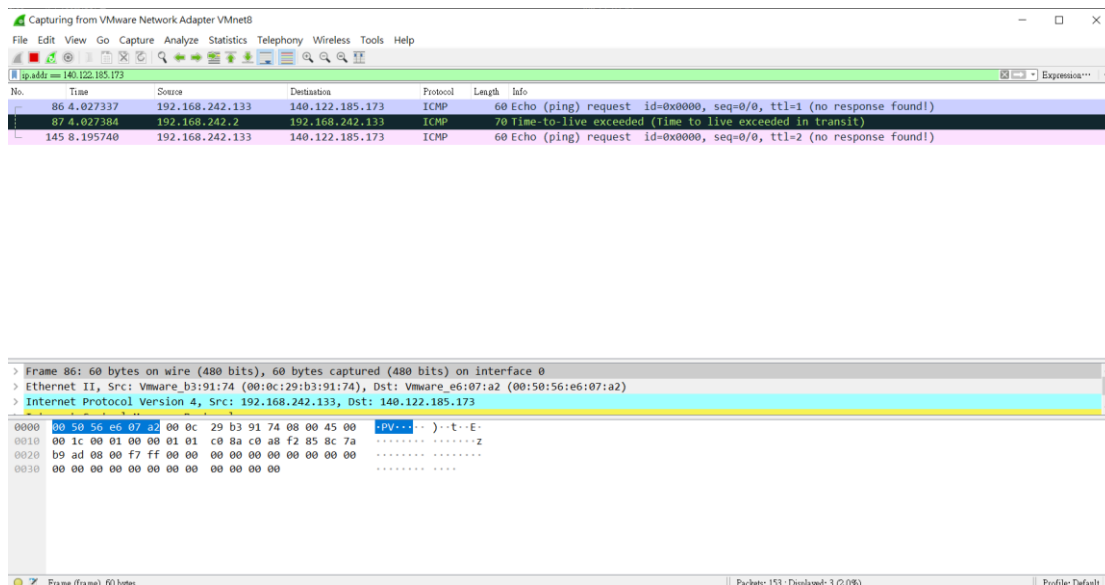
```
2.py
1 #!/usr/bin/python3
2 from scapy.all import *
3
4 a = IP()
5 a.dst = '172.16.230.107'
6 b = ICMP()
7 p = a/b
8 send(p)
9

gary@ubuntu: ~/Desktop
[sudo] password for gary:
[sudo] password for gary:
[sudo] password for gary:
Sent 1 packets.
gary@ubuntu: ~/Desktop$

[sudo] password for gary:
### [ Ethernet ] ###
dst      = 00:50:56:e6:07:a2
src      = 00:0c:29:b3:91:74
type     = IPv4
### [ IP ] ###
version  = 4
ihl      = 5
tos      = 0x0
len      = 28
id       = 1
flags    =
frag     = 0
ttl      = 64
proto    = icmp
chksum   = 0x3536
src      = 192.168.242.133
dst      = 172.16.230.107
\options \
### [ ICMP ] ###
type     = echo-request
code     = 0
chksum   = 0xf7ff
id       = 0x0
seq      = 0x0
### [ Ethernet ] ###
dst      = 00:0c:29:b3:91:74
src      = 00:50:56:e6:07:a2
type     = IPv4
### [ IP ] ###
version  = 4
ihl      = 5
```

Task 1.3

嘗試發送 ICMP 到學校的 IP，TTL 設定為 2 時就能成功。



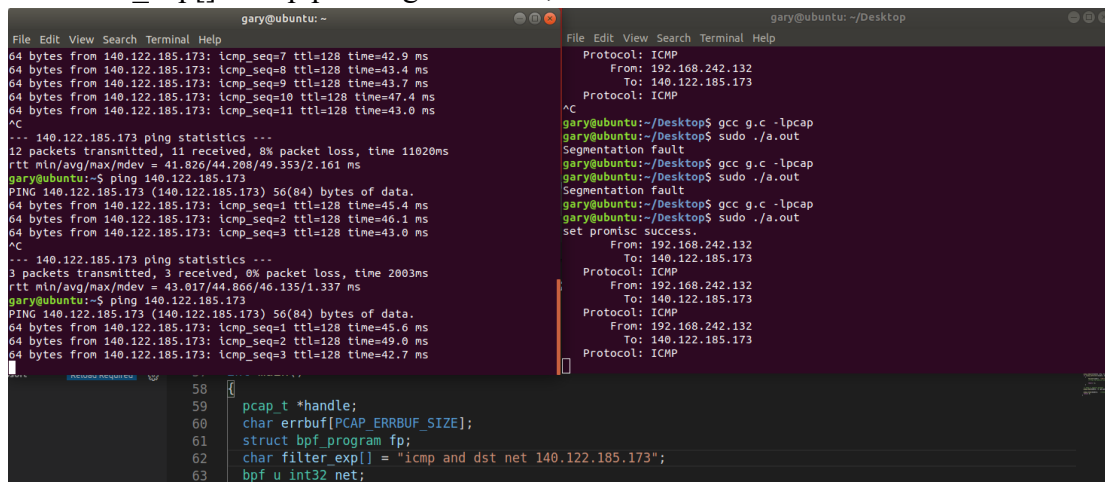
No.	Time	Source	Destination	Protocol	Length	Info
86	4.027337	192.168.242.133	140.122.185.173	ICMP	60	Echo (ping) request id=0x0000, seq=0/0, ttl=1 (no response found!)
87	4.027384	192.168.242.2	192.168.242.133	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
145	8.195740	192.168.242.133	140.122.185.173	ICMP	60	Echo (ping) request id=0x0000, seq=0/0, ttl=2 (no response found!)

> Frame 86: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Vmware_b3:91:74 (00:0c:29:b3:91:74), Dst: Vmware_e6:07:a2 (00:50:56:e6:07:a2)
> Internet Protocol Version 4, Src: 192.168.242.133, Dst: 140.122.185.173

```
0000  00 50 56 e6 07 a2 00 0c 29 b3 91 74 08 00 45 00  -PV...-...-t..E-
0010  00 1c 00 01 00 00 01 01 c0 8a c0 a8 f2 85 8c 7a  .....z
0020  09 ad 00 00 f7 ff 00 00 00 00 00 00 00 00 00 00  .....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```

Task 1.4


```
char filter_exp[] = "tcp portrange 10-100";
```



The image shows two terminal windows from an Ubuntu desktop environment. The left window, titled 'gary@ubuntu: ~', displays the output of several ping commands to the IP address 140.122.185.173. The first ping shows an 8% packet loss, while the second shows 0% loss. The right window, titled 'gary@ubuntu: ~/Desktop', shows the execution of a packet capture program. It displays ICMP traffic from 192.168.242.132 to 140.122.185.173. Below this, it shows the compilation of a program using 'gcc g.c -lpcap' and the execution of './a.out', which successfully sets a promiscuous mode on the interface.

```
gary@ubuntu: ~  
File Edit View Search Terminal Help  
64 bytes from 140.122.185.173: icmp_seq=7 ttl=128 time=42.9 ms  
64 bytes from 140.122.185.173: icmp_seq=8 ttl=128 time=43.4 ms  
64 bytes from 140.122.185.173: icmp_seq=9 ttl=128 time=43.7 ms  
64 bytes from 140.122.185.173: icmp_seq=10 ttl=128 time=47.4 ms  
64 bytes from 140.122.185.173: icmp_seq=11 ttl=128 time=43.0 ms  
^C  
--- 140.122.185.173 ping statistics ---  
12 packets transmitted, 11 received, 8% packet loss, time 11020ms  
rtt min/avg/max/mdev = 41.826/44.208/49.353/2.161 ms  
gary@ubuntu:~$ ping 140.122.185.173  
PING 140.122.185.173 (140.122.185.173) 56(84) bytes of data.  
64 bytes from 140.122.185.173: icmp_seq=1 ttl=128 time=45.4 ms  
64 bytes from 140.122.185.173: icmp_seq=2 ttl=128 time=46.1 ms  
64 bytes from 140.122.185.173: icmp_seq=3 ttl=128 time=43.0 ms  
^C  
--- 140.122.185.173 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2003ms  
rtt min/avg/max/mdev = 43.017/44.866/46.135/1.337 ms  
gary@ubuntu:~$ ping 140.122.185.173  
PING 140.122.185.173 (140.122.185.173) 56(84) bytes of data.  
64 bytes from 140.122.185.173: icmp_seq=1 ttl=128 time=45.6 ms  
64 bytes from 140.122.185.173: icmp_seq=2 ttl=128 time=49.0 ms  
64 bytes from 140.122.185.173: icmp_seq=3 ttl=128 time=42.7 ms
```

```
gary@ubuntu: ~/Desktop  
File Edit View Search Terminal Help  
Protocol: ICMP  
From: 192.168.242.132  
To: 140.122.185.173  
Protocol: ICMP  
^C  
gary@ubuntu:~/Desktop$ gcc g.c -lpcap  
gary@ubuntu:~/Desktop$ sudo ./a.out  
Segmentation fault  
gary@ubuntu:~/Desktop$ gcc g.c -lpcap  
gary@ubuntu:~/Desktop$ sudo ./a.out  
set promisc success.  
From: 192.168.242.132  
To: 140.122.185.173  
Protocol: ICMP  
From: 192.168.242.132  
To: 140.122.185.173  
Protocol: ICMP  
From: 192.168.242.132  
To: 140.122.185.173  
Protocol: ICMP
```

```
58  
59 pcap_t *handle;  
60 char errbuf[PCAP_ERRBUF_SIZE];  
61 struct bpf_program fp;  
62 char filter_exp[] = "icmp and dst net 140.122.185.173";  
63 bpf_u_int32 net;
```