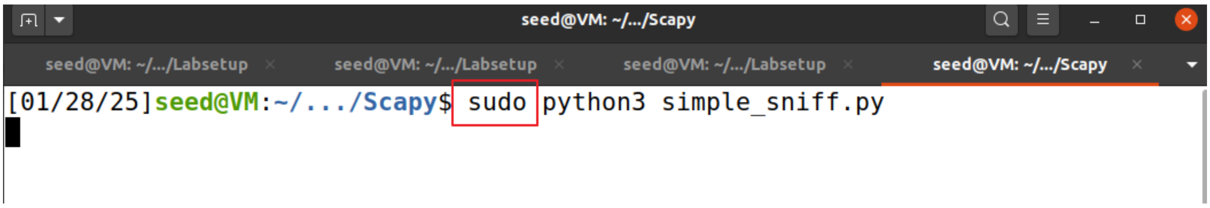
Task 1.1 Sniffing Packets

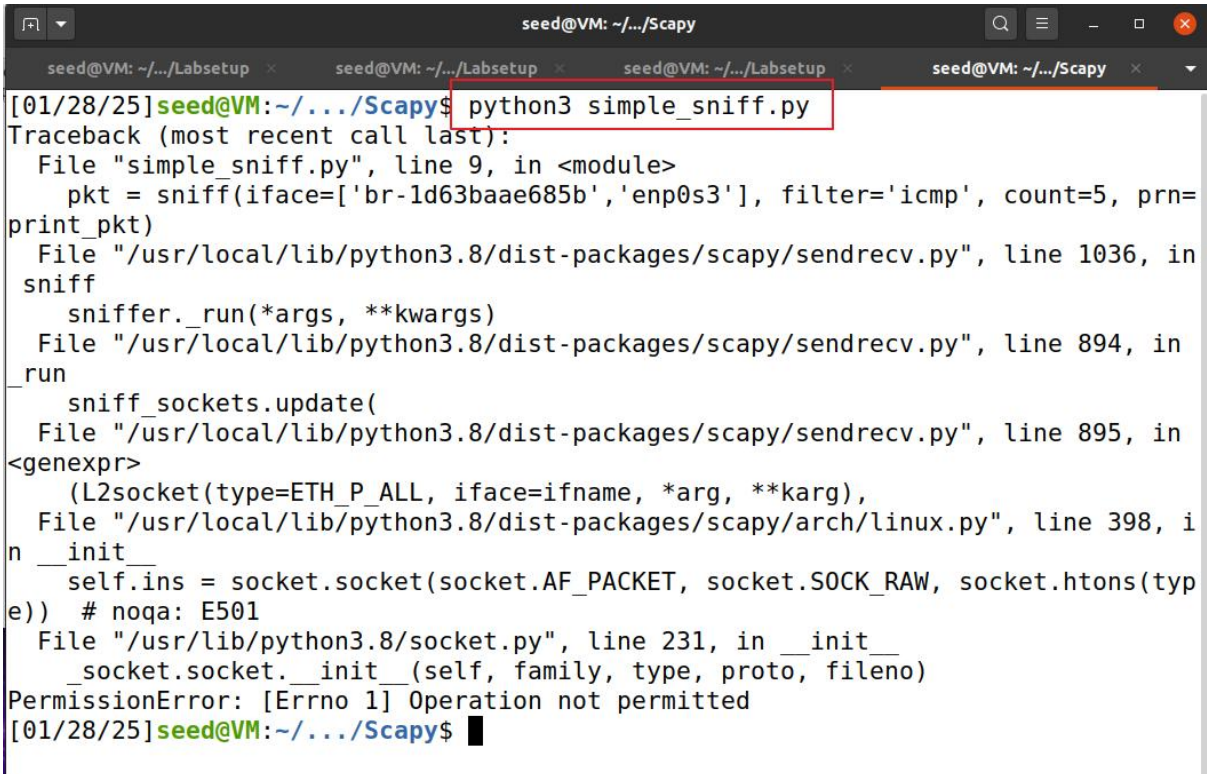
Task 1.1A

Run program simple_sniff.py โดยใช้คำสั่ง sudo มีผลทำให้โปรแกรมสามารถทำงานได้



```
[01/28/25]seed@VM:~/.../Scapy$ sudo python3 simple_sniff.py
█
```

Run program simple_sniff.py โดยไม่มีคำสั่ง sudo โปรแกรมมีการฟ้อง PermissionError

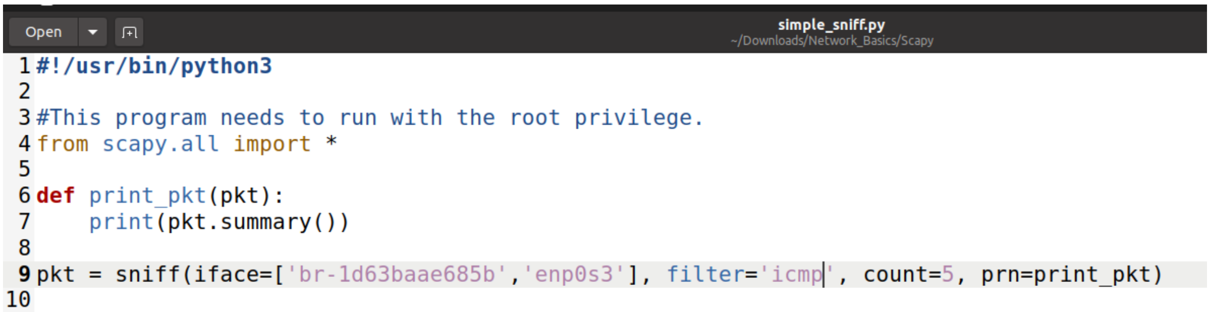


```
[01/28/25]seed@VM:~/.../Scapy$ python3 simple_sniff.py
Traceback (most recent call last):
  File "simple_sniff.py", line 9, in <module>
    pkt = sniff(iface=['br-1d63baae685b','enp0s3'], filter='icmp', count=5, prn=
print_pkt)
  File "/usr/local/lib/python3.8/dist-packages/scapy/sendrecv.py", line 1036, in
 sniff
    sniffer._run(*args, **kwargs)
  File "/usr/local/lib/python3.8/dist-packages/scapy/sendrecv.py", line 894, in
_run
    sniff_sockets.update(
  File "/usr/local/lib/python3.8/dist-packages/scapy/sendrecv.py", line 895, in
<genexpr>
    (L2socket(type=ETH_P_ALL, iface=ifname, *arg, **karg),
  File "/usr/local/lib/python3.8/dist-packages/scapy/arch/linux.py", line 398, i
n __init__
    self.ins = socket.socket(socket.AF_PACKET, socket.SOCK_RAW, socket.htons(typ
e))  # noqa: E501
  File "/usr/lib/python3.8/socket.py", line 231, in __init__
    _socket.socket.__init__(self, family, type, proto, fileno)
PermissionError: [Errno 1] Operation not permitted
[01/28/25]seed@VM:~/.../Scapy$ █
```

Task 1.1B

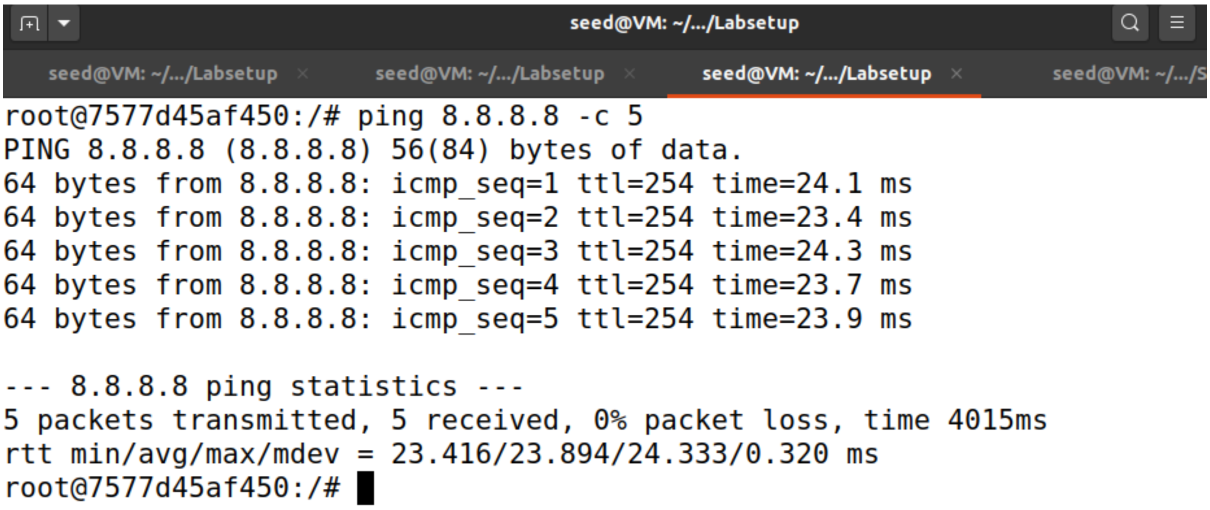
- Capture only the ICMP packet

Code ที่ใช้



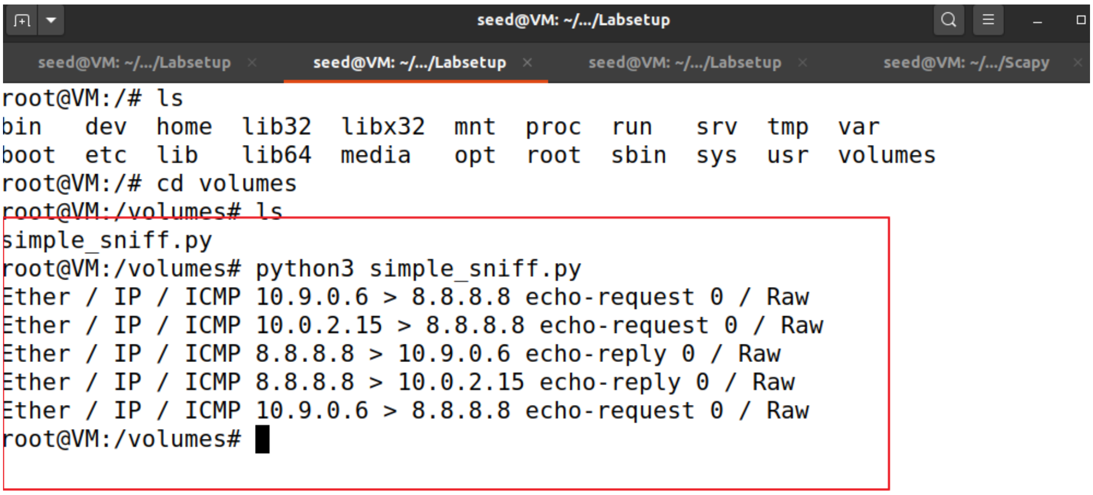
```
#!/usr/bin/python3

#This program needs to run with the root privilege.
from scapy.all import *

def print_pkt(pkt):
    print(pkt.summary())

pkt = sniff(iface=['br-1d63baae685b','enp0s3'], filter='icmp', count=5, prn=print_pkt)
```

ฝั่งผู้ถูกโจรกรรม



```
root@7577d45af450:/# ping 8.8.8.8 -c 5
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=254 time=24.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=254 time=23.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=254 time=24.3 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=254 time=23.7 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=254 time=23.9 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4015ms
rtt min/avg/max/mdev = 23.416/23.894/24.333/0.320 ms
root@7577d45af450:/#
```

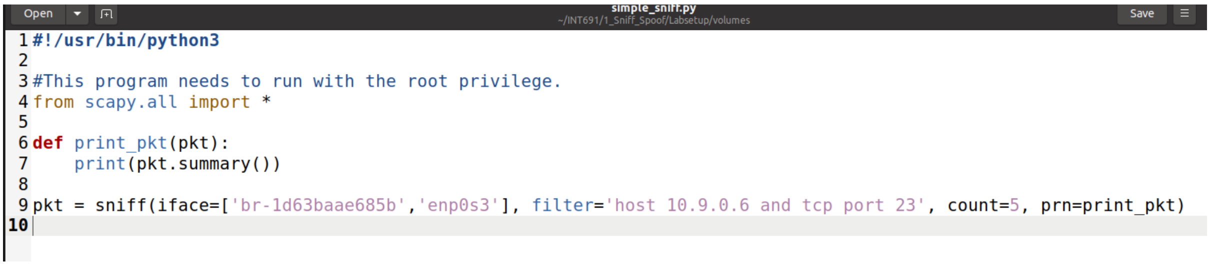
ฝั่ง Attacker



```
root@VM:/# ls
bin   dev  home  lib32  libx32  mnt  proc  run   srv  tmp  var
boot  etc  lib   lib64  media   opt  root  sbin  sys  usr  volumes
root@VM:/# cd volumes
root@VM:/volumes# ls
simple_sniff.py
root@VM:/volumes# python3 simple_sniff.py
Ether / IP / ICMP 10.9.0.6 > 8.8.8.8 echo-request 0 / Raw
Ether / IP / ICMP 10.0.2.15 > 8.8.8.8 echo-request 0 / Raw
Ether / IP / ICMP 8.8.8.8 > 10.9.0.6 echo-reply 0 / Raw
Ether / IP / ICMP 8.8.8.8 > 10.0.2.15 echo-reply 0 / Raw
Ether / IP / ICMP 10.9.0.6 > 8.8.8.8 echo-request 0 / Raw
root@VM:/volumes#
```

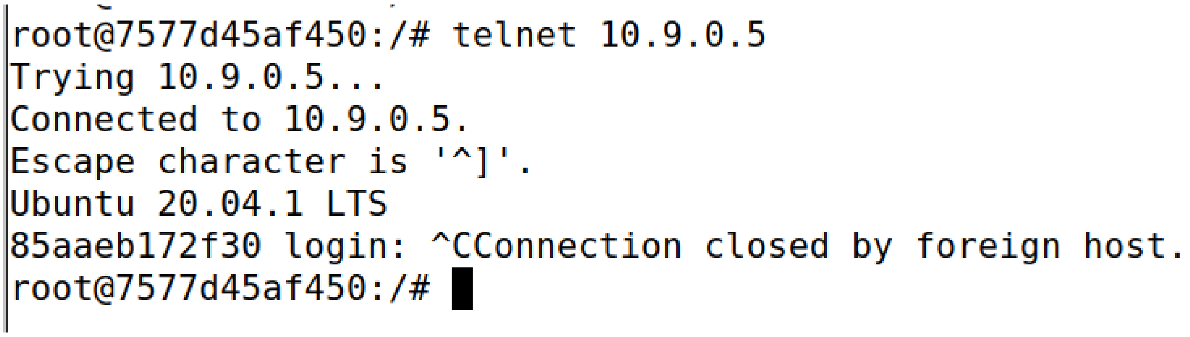
- Capture any TCP packet that comes from a particular IP and with a destination port number 23

Code ที่ใช้



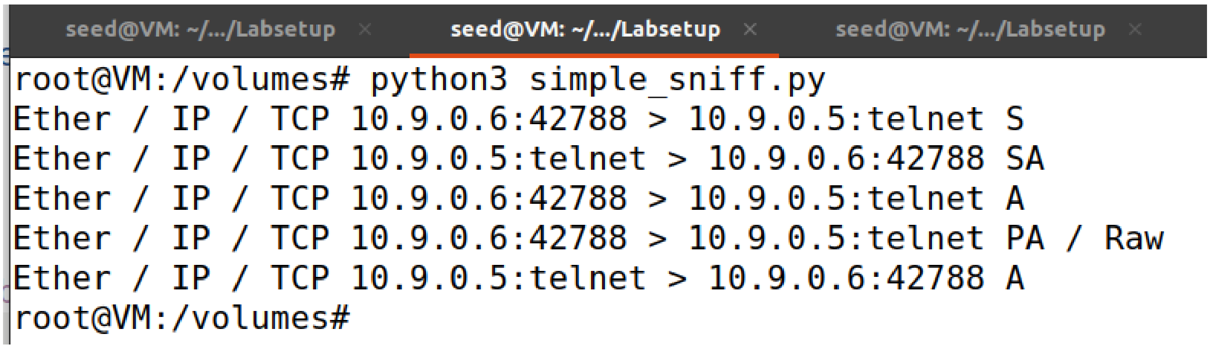
```
#!/usr/bin/python3

#This program needs to run with the root privilege.
from scapy.all import *

def print_pkt(pkt):
    print(pkt.summary())

pkt = sniff(iface=['br-1d63baae685b','enp0s3'], filter='host 10.9.0.6 and tcp port 23', count=5, prn=print_pkt)
```

ฝั่งผู้ถูกโจรกรรม



```
root@7577d45af450:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
85aaeb172f30 login: ^CConnection closed by foreign host.
root@7577d45af450:/# 
```

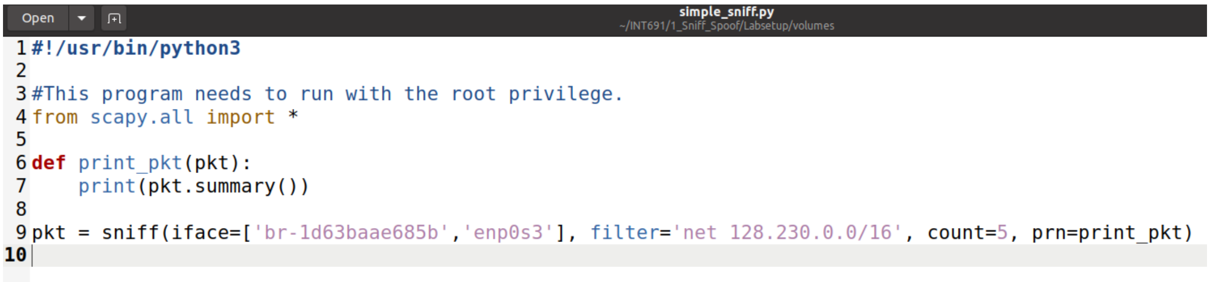
ฝั่ง Attacker



```
root@VM:/volumes# python3 simple_sniff.py
Ether / IP / TCP 10.9.0.6:42788 > 10.9.0.5:telnet S
Ether / IP / TCP 10.9.0.5:telnet > 10.9.0.6:42788 SA
Ether / IP / TCP 10.9.0.6:42788 > 10.9.0.5:telnet A
Ether / IP / TCP 10.9.0.6:42788 > 10.9.0.5:telnet PA / Raw
Ether / IP / TCP 10.9.0.5:telnet > 10.9.0.6:42788 A
root@VM:/volumes#
```

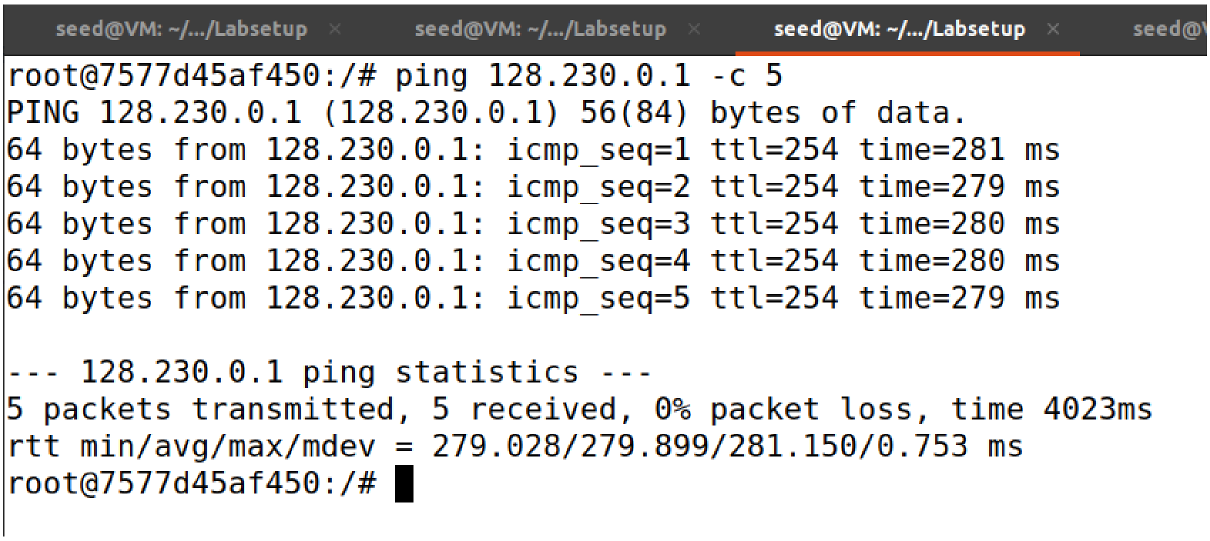
- Capture packets comes from or to go to a particular subnet. You can pick any subnet, such as 128.230.0.0/16; you should not pick the subnet that your VM is attached to.

Code ที่ใช้



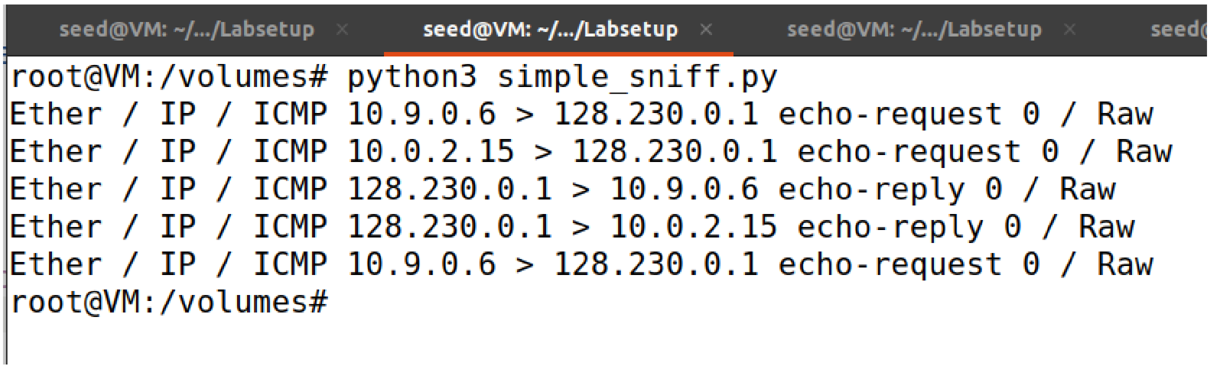
```
#!/usr/bin/python3

#This program needs to run with the root privilege.
from scapy.all import *

def print_pkt(pkt):
    print(pkt.summary())

pkt = sniff(iface=['br-1d63baae685b','enp0s3'], filter='net 128.230.0.0/16', count=5, prn=print_pkt)

```

ฝั่งที่ถูกโจรกรรม



```
root@7577d45af450:/# ping 128.230.0.1 -c 5
PING 128.230.0.1 (128.230.0.1) 56(84) bytes of data.
64 bytes from 128.230.0.1: icmp_seq=1 ttl=254 time=281 ms
64 bytes from 128.230.0.1: icmp_seq=2 ttl=254 time=279 ms
64 bytes from 128.230.0.1: icmp_seq=3 ttl=254 time=280 ms
64 bytes from 128.230.0.1: icmp_seq=4 ttl=254 time=280 ms
64 bytes from 128.230.0.1: icmp_seq=5 ttl=254 time=279 ms

--- 128.230.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4023ms
rtt min/avg/max/mdev = 279.028/279.899/281.150/0.753 ms
root@7577d45af450:/# 
```

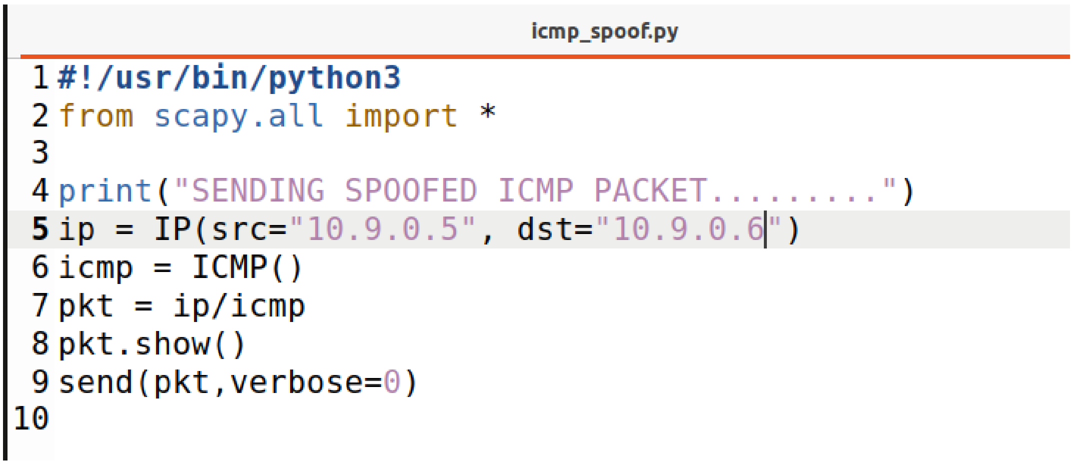
ฝั่ง Attacker



```
root@VM:/volumes# python3 simple_sniff.py
Ether / IP / ICMP 10.9.0.6 > 128.230.0.1 echo-request 0 / Raw
Ether / IP / ICMP 10.0.2.15 > 128.230.0.1 echo-request 0 / Raw
Ether / IP / ICMP 128.230.0.1 > 10.9.0.6 echo-reply 0 / Raw
Ether / IP / ICMP 128.230.0.1 > 10.0.2.15 echo-reply 0 / Raw
Ether / IP / ICMP 10.9.0.6 > 128.230.0.1 echo-request 0 / Raw
root@VM:/volumes#
```

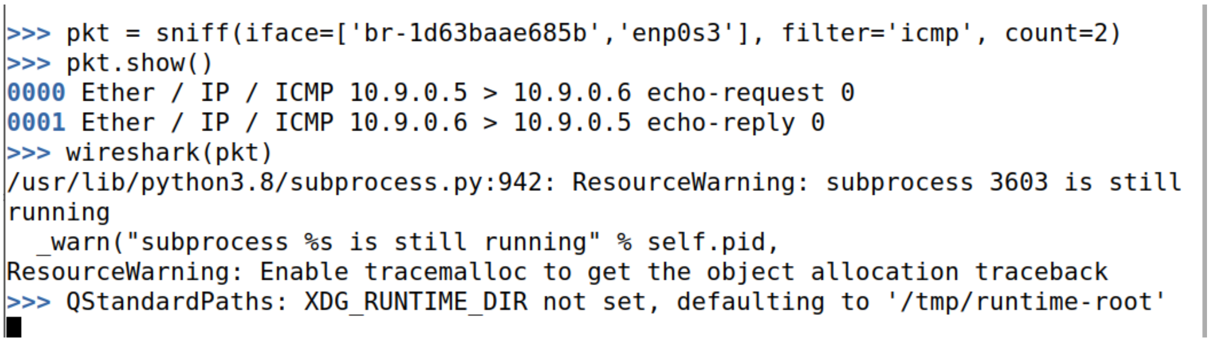
Task 1.2: Spoofing ICMP Packets

Code ที่ใช้ทำ Spoof



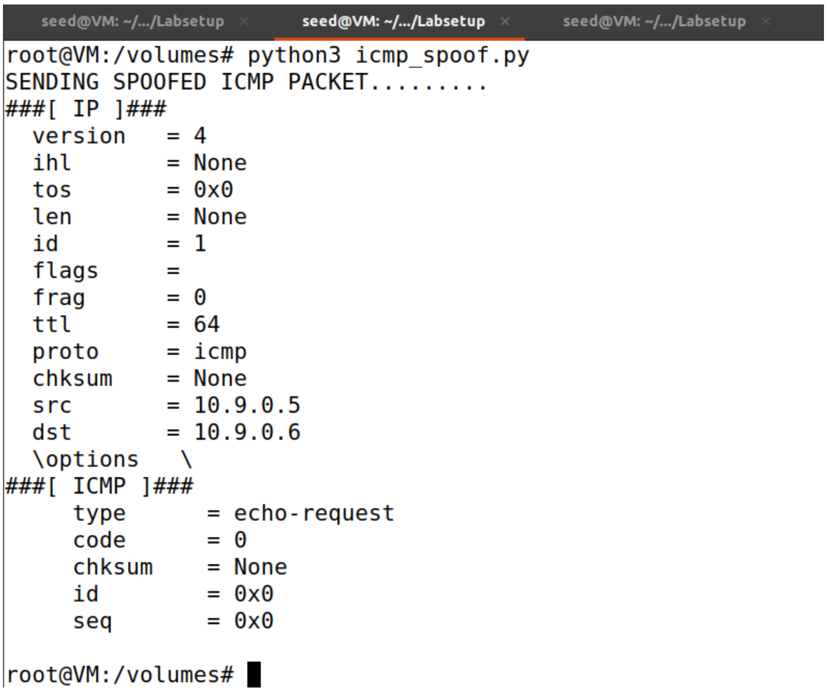
```
#!/usr/bin/python3
from scapy.all import *

print("SENDING SPOOFED ICMP PACKET.........")
ip = IP(src="10.9.0.5", dst="10.9.0.6")
icmp = ICMP()
pkt = ip/icmp
pkt.show()
send(pkt,verbose=0)

```

Code ที่ใช้ทำ Sniff



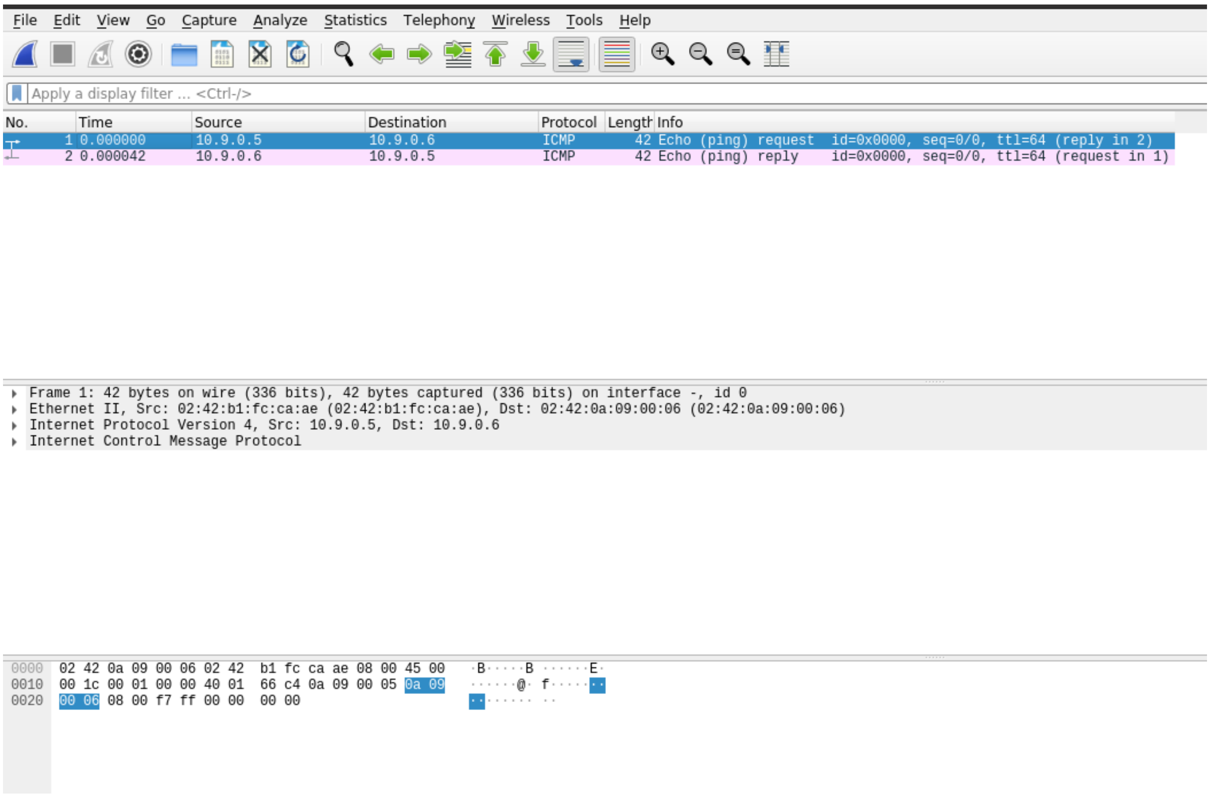
```
>>> pkt = sniff(iface=['br-1d63baae685b','enp0s3'], filter='icmp', count=2)
>>> pkt.show()
0000 Ether / IP / ICMP 10.9.0.5 > 10.9.0.6 echo-request 0
0001 Ether / IP / ICMP 10.9.0.6 > 10.9.0.5 echo-reply 0
>>> wireshark(pkt)
/usr/lib/python3.8/subprocess.py:942: ResourceWarning: subprocess 3603 is still
running
  _warn("subprocess %s is still running" % self.pid,
ResourceWarning: Enable tracemalloc to get the object allocation traceback
>>> QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
█
```

ผลการทำ Spoof



```
root@VM:/volumes# python3 icmp_spoof.py
SENDING SPOOFED ICMP PACKET.........
###[ IP ]###
  version   = 4
  ihl       = None
  tos       = 0x0
  len       = None
  id        = 1
  flags     =
  frag      = 0
  ttl       = 64
  proto     = icmp
  chksum    = None
  src       = 10.9.0.5
  dst       = 10.9.0.6
  \options   \
###[ ICMP ]###
     type      = echo-request
     code      = 0
     chksum    = None
     id        = 0x0
     seq       = 0x0

root@VM:/volumes# █
```

ผลการทำ Sniff แล้วเปิดด้วย wireshark



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

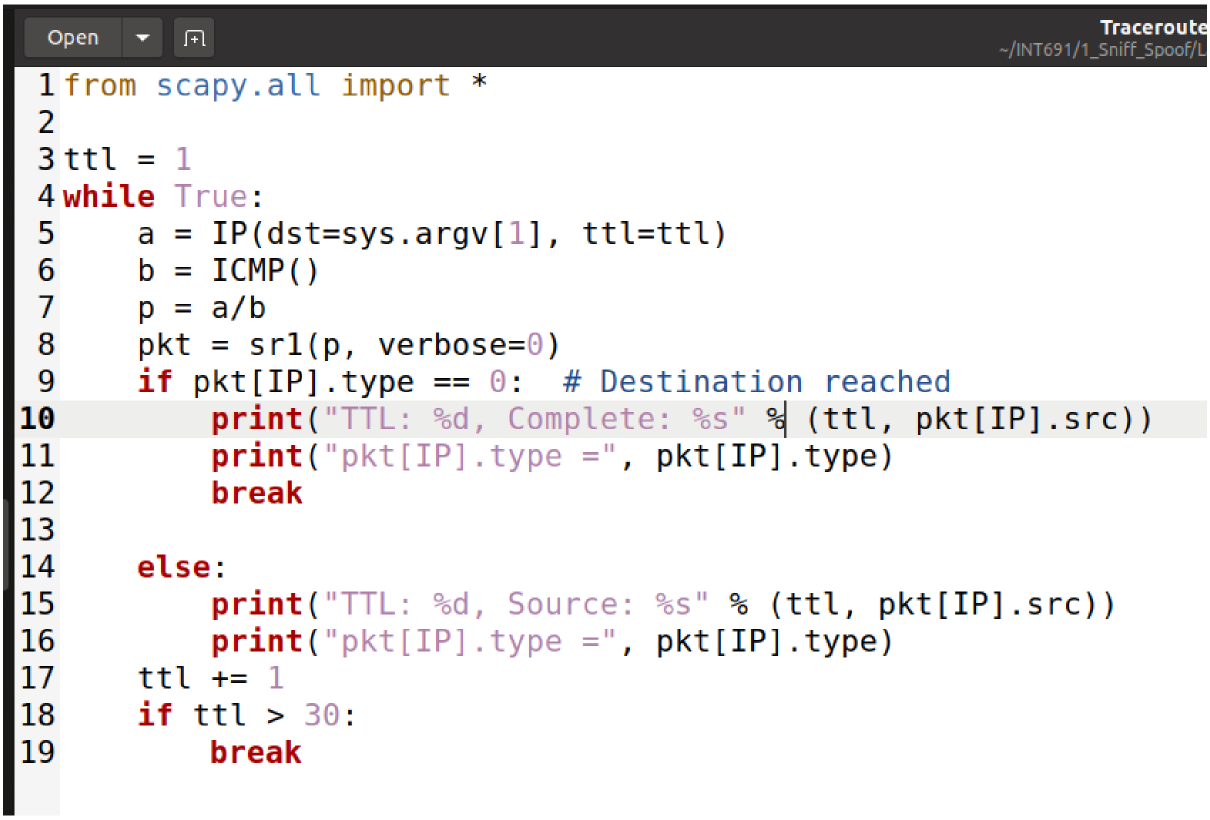
```
No.   Time       Source       Destination   Protocol Length Info
    1 0.000000   10.9.0.5     10.9.0.6      ICMP         42 Echo (ping) request  id=0x0000, seq=0/0, ttl=64 (reply in 2)
    2 0.000042   10.9.0.6     10.9.0.5      ICMP         42 Echo (ping) reply    id=0x0000, seq=0/0, ttl=64 (request in 1)
```

```
▸ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface -, id 0
▸ Ethernet II, Src: 02:42:b1:fc:ca:ae (02:42:b1:fc:ca:ae), Dst: 02:42:0a:09:00:06 (02:42:0a:09:00:06)
▸ Internet Protocol Version 4, Src: 10.9.0.5, Dst: 10.9.0.6
▸ Internet Control Message Protocol
```

```
0000  02 42 0a 09 00 06 02 42  b1 fc ca ae 08 00 45 00   ·B····B ······E·
0010  00 1c 00 01 00 00 40 01  66 c4 0a 09 00 05 0a 09   ······@· f·····••
0020  00 06 08 00 f7 ff 00 00  00 00                     ••······ ··
```

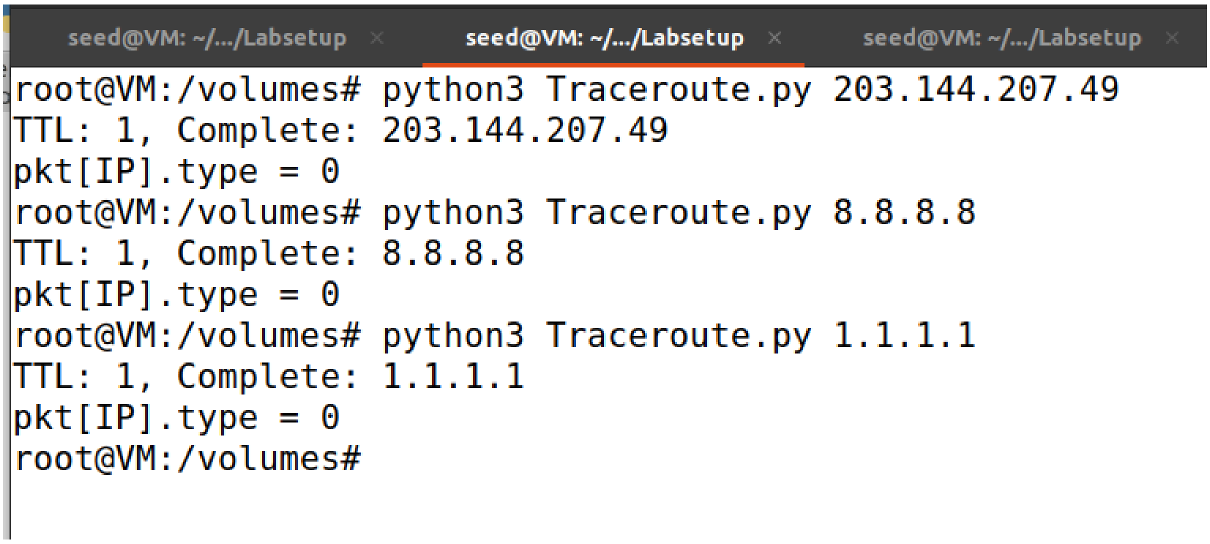
Task 1.3: Traceroute

Code ที่ใช้



```
from scapy.all import *

ttl = 1
while True:
    a = IP(dst=sys.argv[1], ttl=ttl)
    b = ICMP()
    p = a/b
    pkt = sr1(p, verbose=0)
    if pkt[IP].type == 0:  # Destination reached
        print("TTL: %d, Complete: %s" % (ttl, pkt[IP].src))
        print("pkt[IP].type =", pkt[IP].type)
        break

    else:
        print("TTL: %d, Source: %s" % (ttl, pkt[IP].src))
        print("pkt[IP].type =", pkt[IP].type)
    ttl += 1
    if ttl > 30:
        break
```

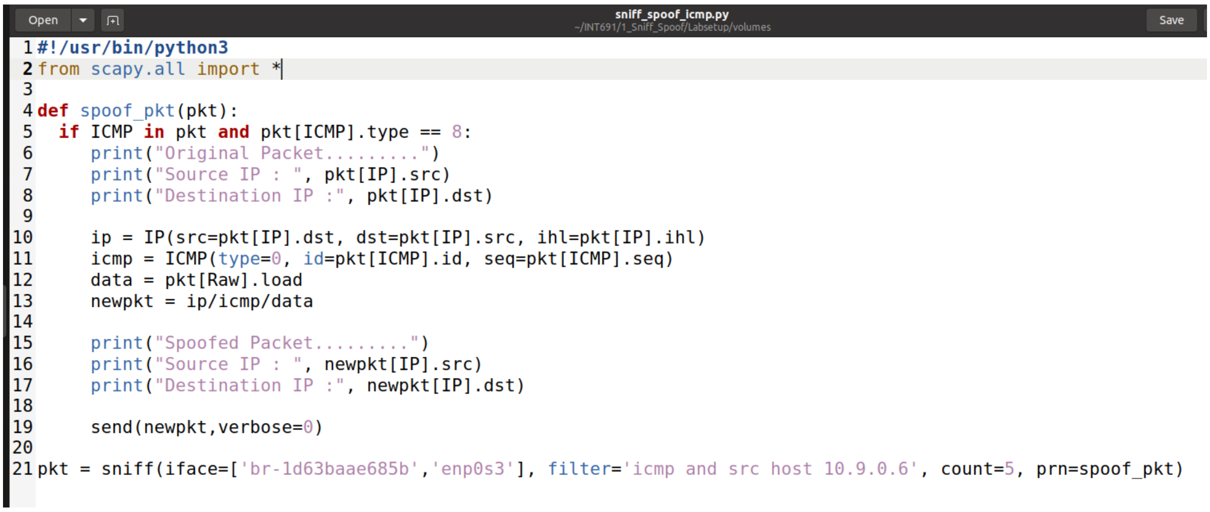
ผลลัพท์ที่ได้



```
root@VM:/volumes# python3 Traceroute.py 203.144.207.49
TTL: 1, Complete: 203.144.207.49
pkt[IP].type = 0
root@VM:/volumes# python3 Traceroute.py 8.8.8.8
TTL: 1, Complete: 8.8.8.8
pkt[IP].type = 0
root@VM:/volumes# python3 Traceroute.py 1.1.1.1
TTL: 1, Complete: 1.1.1.1
pkt[IP].type = 0
root@VM:/volumes#
```

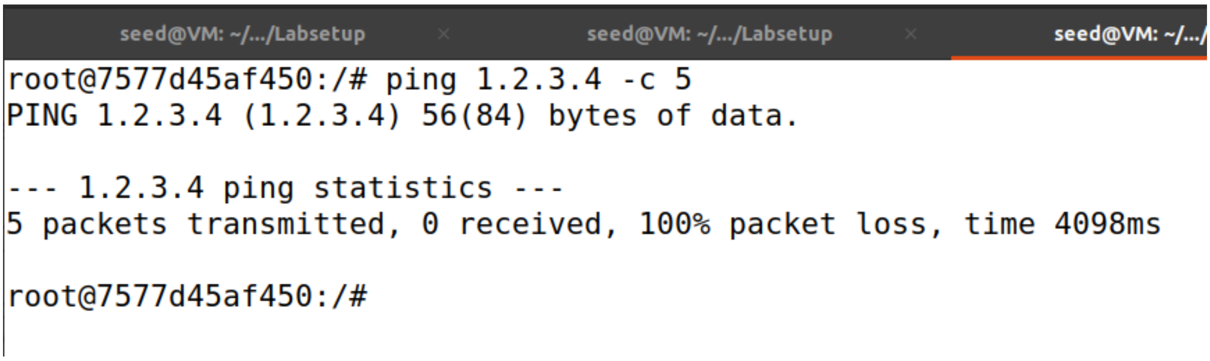
Task 1.4: Sniffing and-then Spoofing

Code ที่ใช้



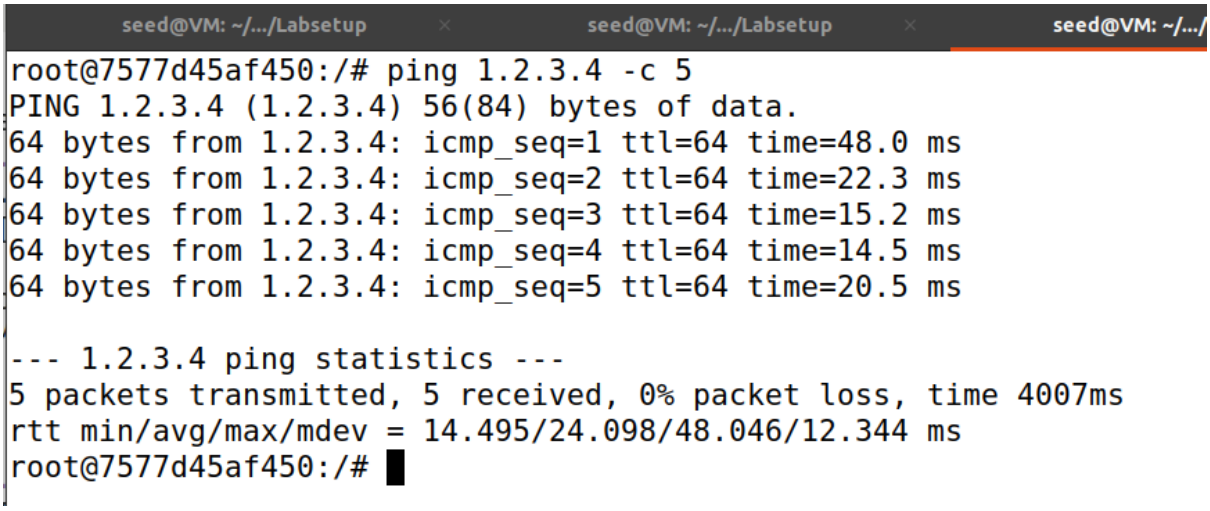
```python
#!/usr/bin/python3
from scapy.all import *

def spoof_pkt(pkt):
  if ICMP in pkt and pkt[ICMP].type == 8:
     print("Original Packet.........")
     print("Source IP : ", pkt[IP].src)
     print("Destination IP :", pkt[IP].dst)

     ip = IP(src=pkt[IP].dst, dst=pkt[IP].src, ihl=pkt[IP].ihl)
     icmp = ICMP(type=0, id=pkt[ICMP].id, seq=pkt[ICMP].seq)
     data = pkt[Raw].load
     newpkt = ip/icmp/data

     print("Spoofed Packet.........")
     print("Source IP : ", newpkt[IP].src)
     print("Destination IP :", newpkt[IP].dst)

     send(newpkt,verbose=0)

pkt = sniff(iface=['br-1d63baae685b','enp0s3'], filter='icmp and src host 10.9.0.6', count=5, prn=spoof_pkt)
```

ping 1.2.3.4 โดยที่ยังไม่ได้ทำ sniff & spoof จะ packet loss 100%



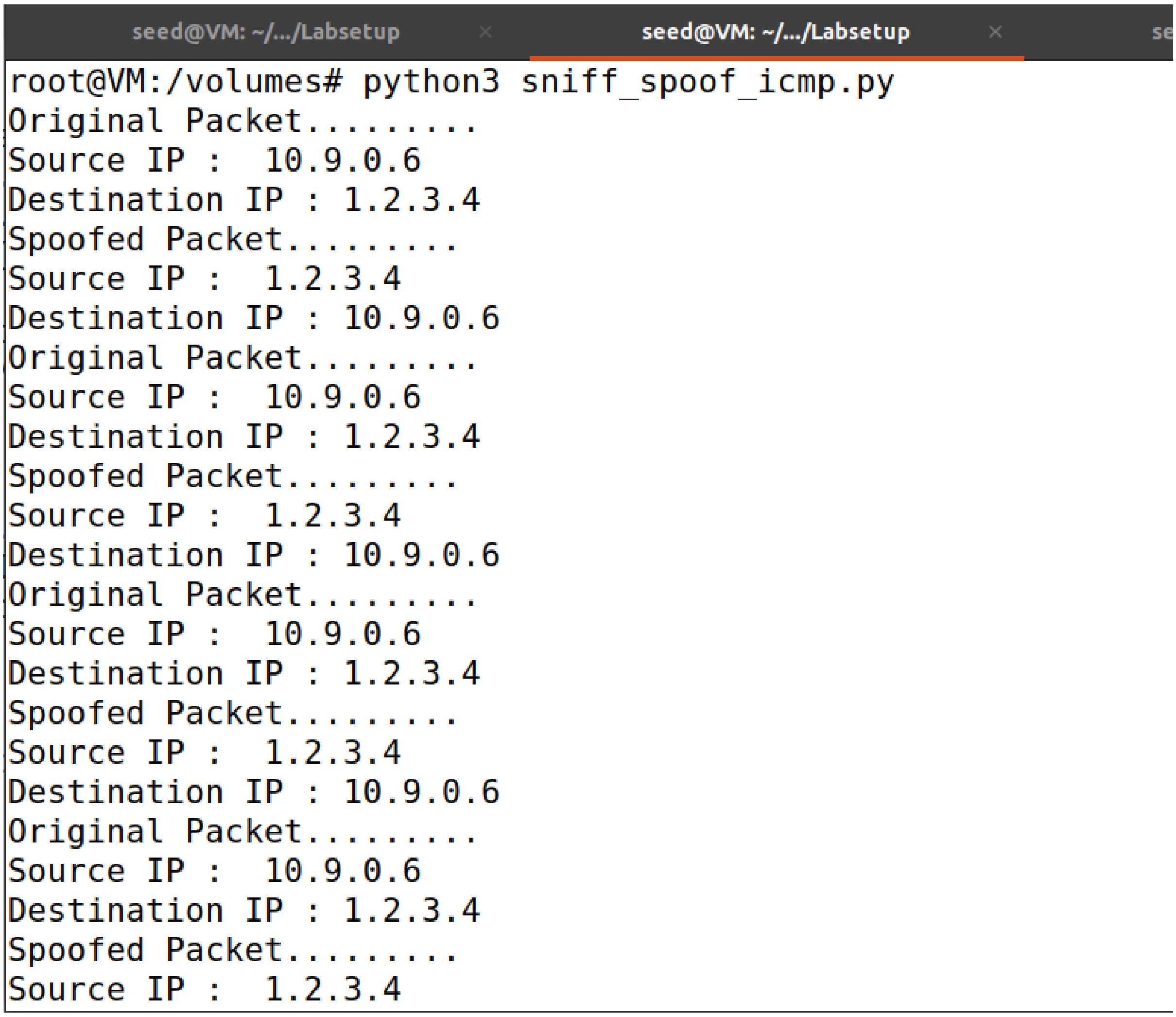
```
root@7577d45af450:/# ping 1.2.3.4 -c 5
PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data.

--- 1.2.3.4 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4098ms

root@7577d45af450:/#
```

หลังจากเปิดใช้ sniff & spoof ฝ่ายที่ ping 1.2.3.4 จะโดน packet ปลอมหลอกว่ามี receive กลับมา



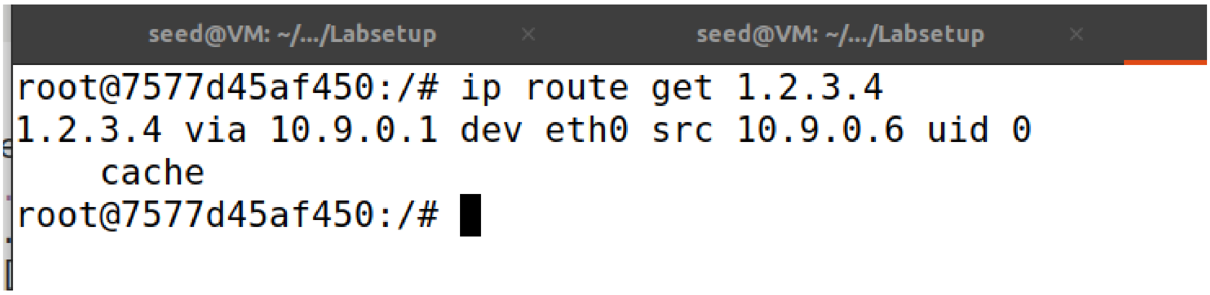
```
root@7577d45af450:/# ping 1.2.3.4 -c 5
PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data.
64 bytes from 1.2.3.4: icmp_seq=1 ttl=64 time=48.0 ms
64 bytes from 1.2.3.4: icmp_seq=2 ttl=64 time=22.3 ms
64 bytes from 1.2.3.4: icmp_seq=3 ttl=64 time=15.2 ms
64 bytes from 1.2.3.4: icmp_seq=4 ttl=64 time=14.5 ms
64 bytes from 1.2.3.4: icmp_seq=5 ttl=64 time=20.5 ms

--- 1.2.3.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 14.495/24.098/48.046/12.344 ms
root@7577d45af450:/#
```

หน้าจอฝ่าย sniff & spoof จะแสดงดังนี้



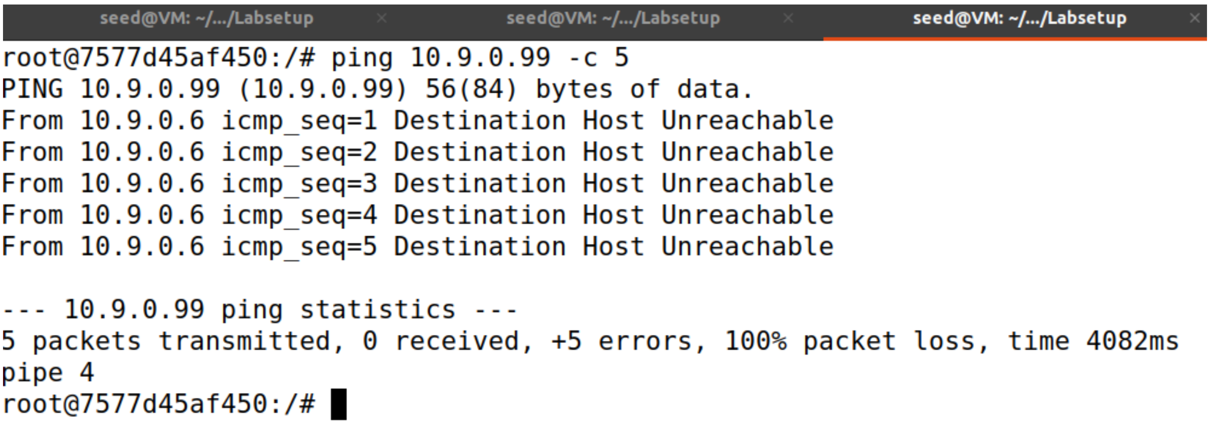
```
root@VM:/volumes# python3 sniff_spoof_icmp.py
Original Packet.........
Source IP :  10.9.0.6
Destination IP : 1.2.3.4
Spoofed Packet.........
Source IP :  1.2.3.4
Destination IP : 10.9.0.6
Original Packet.........
Source IP :  10.9.0.6
Destination IP : 1.2.3.4
Spoofed Packet.........
Source IP :  1.2.3.4
Destination IP : 10.9.0.6
Original Packet.........
Source IP :  10.9.0.6
Destination IP : 1.2.3.4
Spoofed Packet.........
Source IP :  1.2.3.4
Destination IP : 10.9.0.6
Original Packet.........
Source IP :  10.9.0.6
Destination IP : 1.2.3.4
Spoofed Packet.........
Source IP :  1.2.3.4
```

สาเหตุที่สามารถ spoof ได้เนื่องจาก 1.2.3.4 มีการรู้จัก route ผ่านทาง router 10.9.0.1



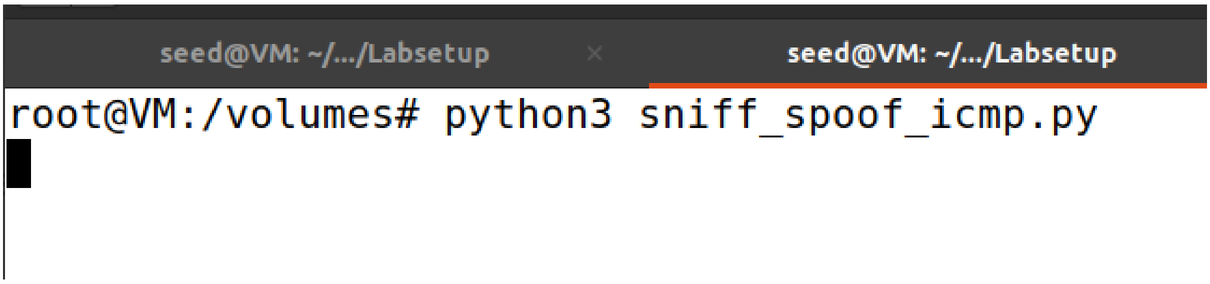
```
root@7577d45af450:/# ip route get 1.2.3.4
1.2.3.4 via 10.9.0.1 dev eth0 src 10.9.0.6 uid 0
    cache
root@7577d45af450:/# 
```

ping 10.9.0.99 จะไม่ว่าจะมีการทำ sniff & spoof หรือไม่ก็จะขึ้นว่า Destinatiom host unreachable



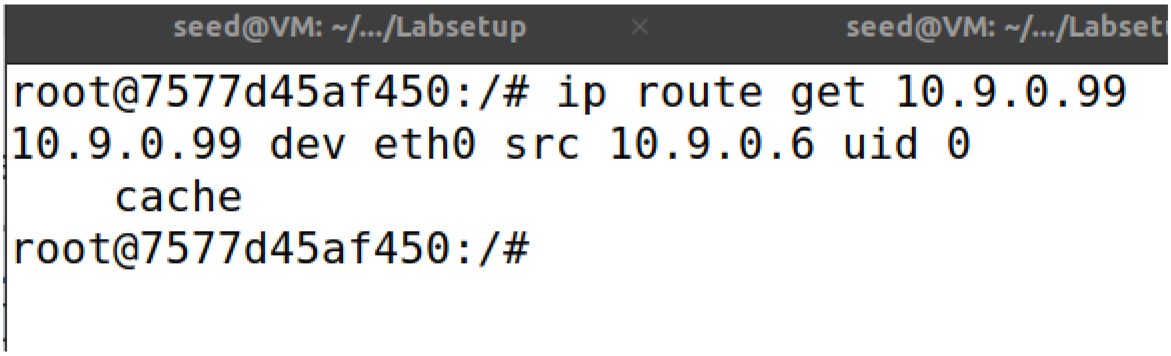
```
root@7577d45af450:/# ping 10.9.0.99 -c 5
PING 10.9.0.99 (10.9.0.99) 56(84) bytes of data.
From 10.9.0.6 icmp_seq=1 Destination Host Unreachable
From 10.9.0.6 icmp_seq=2 Destination Host Unreachable
From 10.9.0.6 icmp_seq=3 Destination Host Unreachable
From 10.9.0.6 icmp_seq=4 Destination Host Unreachable
From 10.9.0.6 icmp_seq=5 Destination Host Unreachable

--- 10.9.0.99 ping statistics ---
5 packets transmitted, 0 received, +5 errors, 100% packet loss, time 4082ms
pipe 4
root@7577d45af450:/# 
```

ส่วนฝั่งที่ทำ sniff & spoof จะไม่มีอะไรเกิดขึ้น เนื่องจากดักจับไม่ได้



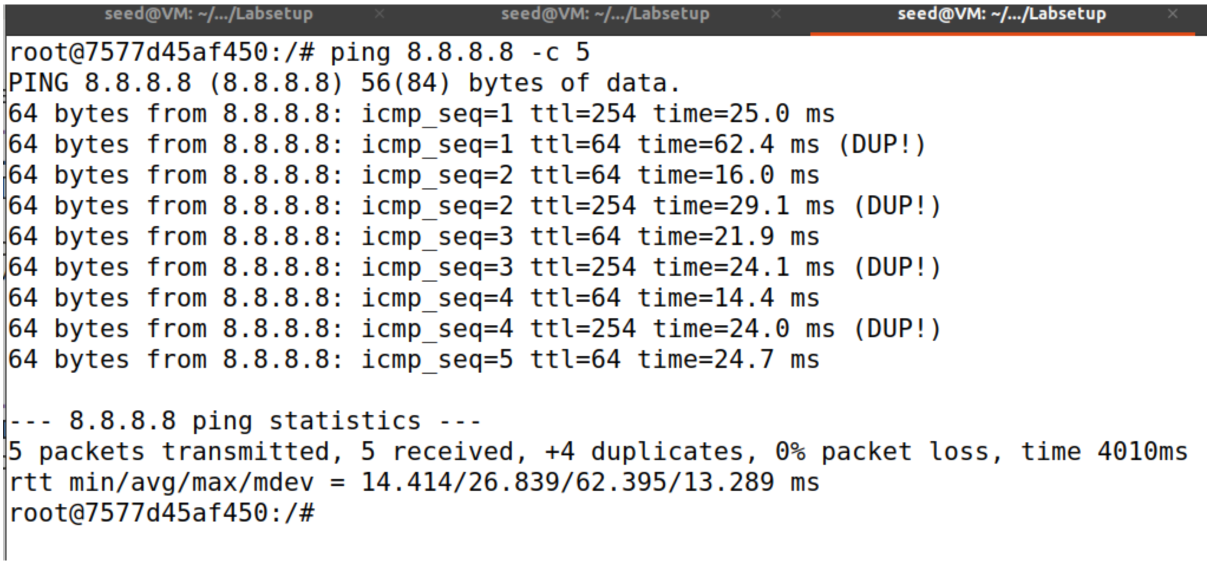
```
root@VM:/volumes# python3 sniff_spoof_icmp.py
```

สาเหตุเนื่องจาก 10.9.0.99 ไม่ถูกรู้จักจาก route ใดเลย



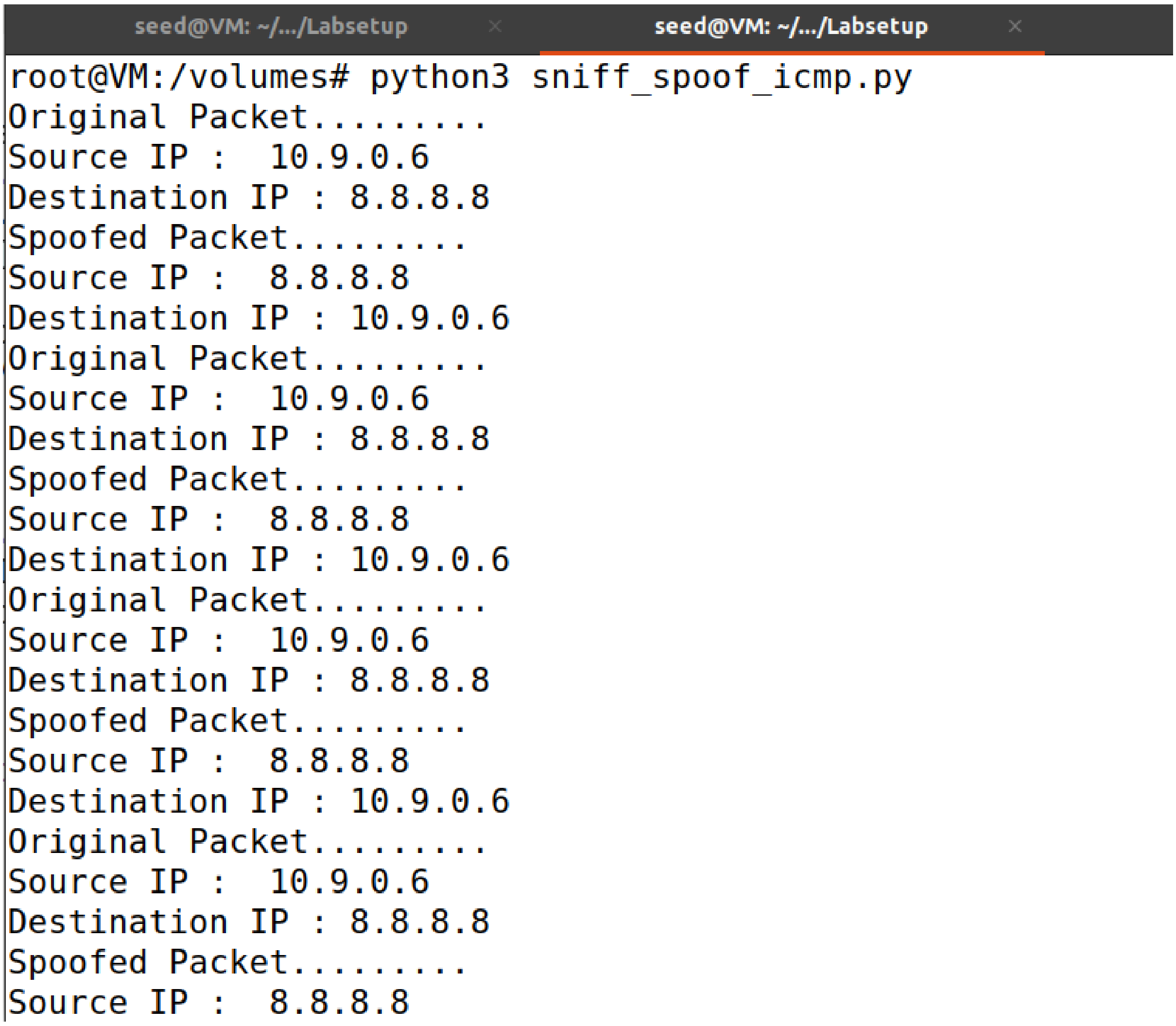
```
root@7577d45af450:/# ip route get 10.9.0.99
10.9.0.99 dev eth0 src 10.9.0.6 uid 0
    cache
root@7577d45af450:/#
```

ping 8.8.8.8 หลังจากมีการทำ sniff & spoof ได้จะพบว่ามี DUP เนื่องจาก 8.8.8.8 เป็นปลายทางที่มีอยู่จริงจริงทำให้ได้รับ reply จาก 8.8.8.8 และ จากการ spoof จึงทำให้เกิด DUP



```
root@7577d45af450:/# ping 8.8.8.8 -c 5
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=254 time=25.0 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=64 time=62.4 ms (DUP!)
64 bytes from 8.8.8.8: icmp_seq=2 ttl=64 time=16.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=254 time=29.1 ms (DUP!)
64 bytes from 8.8.8.8: icmp_seq=3 ttl=64 time=21.9 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=254 time=24.1 ms (DUP!)
64 bytes from 8.8.8.8: icmp_seq=4 ttl=64 time=14.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=254 time=24.0 ms (DUP!)
64 bytes from 8.8.8.8: icmp_seq=5 ttl=64 time=24.7 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, +4 duplicates, 0% packet loss, time 4010ms
rtt min/avg/max/mdev = 14.414/26.839/62.395/13.289 ms
root@7577d45af450:/#
```

หน้าจอฝั่ง spoof



```
root@VM:/volumes# python3 sniff_spoof_icmp.py
Original Packet.........
Source IP :  10.9.0.6
Destination IP : 8.8.8.8
Spoofed Packet.........
Source IP :  8.8.8.8
Destination IP : 10.9.0.6
Original Packet.........
Source IP :  10.9.0.6
Destination IP : 8.8.8.8
Spoofed Packet.........
Source IP :  8.8.8.8
Destination IP : 10.9.0.6
Original Packet.........
Source IP :  10.9.0.6
Destination IP : 8.8.8.8
Spoofed Packet.........
Source IP :  8.8.8.8
Destination IP : 10.9.0.6
Original Packet.........
Source IP :  10.9.0.6
Destination IP : 8.8.8.8
Spoofed Packet.........
Source IP :  8.8.8.8
```