CS3205: Computer Networks

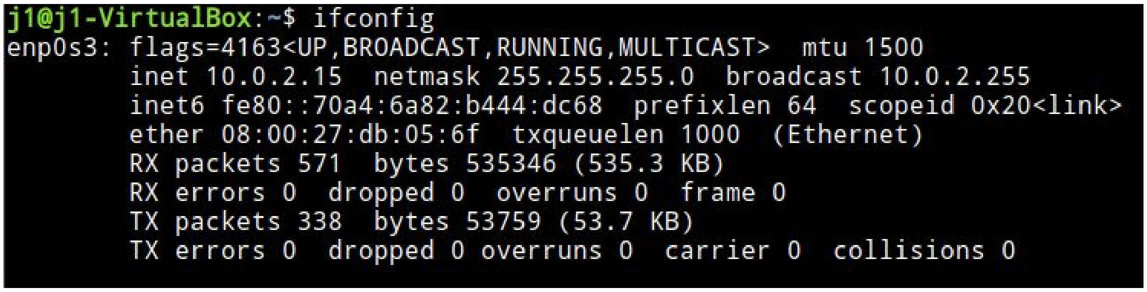
P. JAITESH | CS17B021

Assignment - 5
Playing around Data Packets using Scapy

<u>Section 3.1:</u> (Step-I)

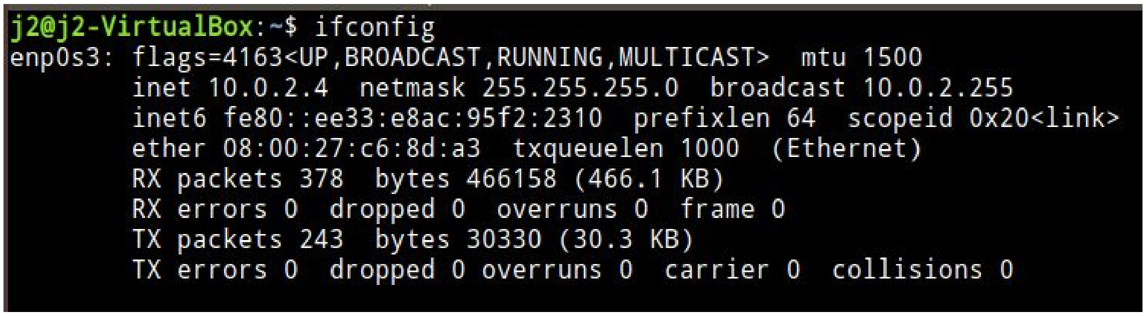
The public Ip addresses of the two systems are

1) IPv4 of First System is **10.0.2.15** and public IPv4 address is **124.123.28.48**



```
j1@j1-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::70a4:6a82:b444:dc68  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:db:05:6f  txqueuelen 1000  (Ethernet)
        RX packets 571  bytes 535346 (535.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 338  bytes 53759 (53.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2) IPv4 of Second System is **10.0.2.4** and public IPv4 address is **124.123.28.48**

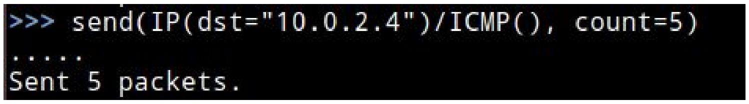


```
j2@j2-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.4  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::ee33:e8ac:95f2:2310  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c6:8d:a3  txqueuelen 1000  (Ethernet)
        RX packets 378  bytes 466158 (466.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 243  bytes 30330 (30.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Section 3.2: (Step-II)

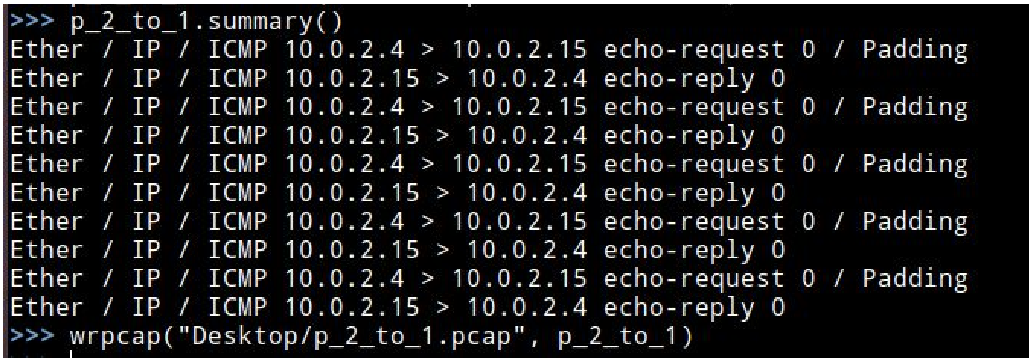
PS1:

1) Command used for sending:(From PS1)



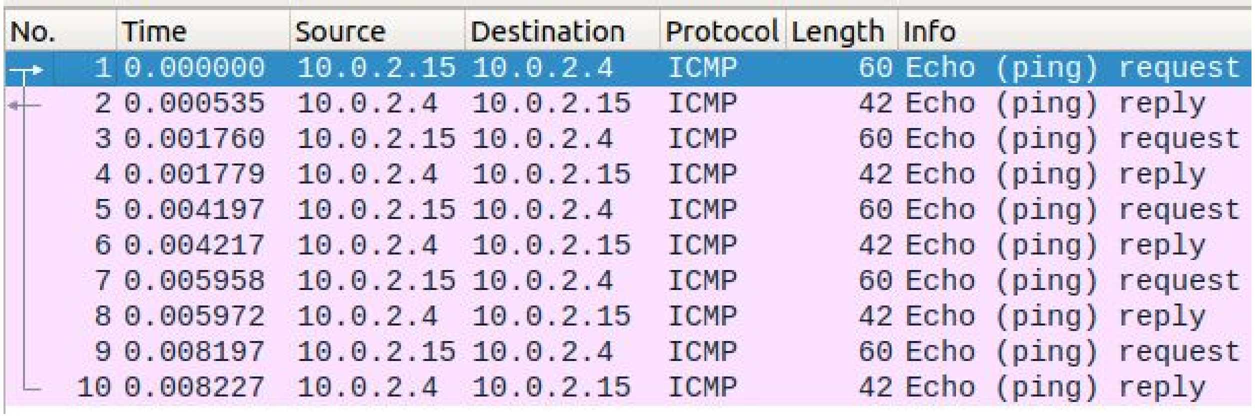
```
>>> send(IP(dst="10.0.2.4")/ICMP(), count=5)
.....
Sent 5 packets.
```

2) Command used for receiving:(At PS2)



```
>>> p_2_to_1.summary()
Ether / IP / ICMP 10.0.2.4 > 10.0.2.15 echo-request 0 / Padding
Ether / IP / ICMP 10.0.2.15 > 10.0.2.4 echo-reply 0
Ether / IP / ICMP 10.0.2.4 > 10.0.2.15 echo-request 0 / Padding
Ether / IP / ICMP 10.0.2.15 > 10.0.2.4 echo-reply 0
Ether / IP / ICMP 10.0.2.4 > 10.0.2.15 echo-request 0 / Padding
Ether / IP / ICMP 10.0.2.15 > 10.0.2.4 echo-reply 0
Ether / IP / ICMP 10.0.2.4 > 10.0.2.15 echo-request 0 / Padding
Ether / IP / ICMP 10.0.2.15 > 10.0.2.4 echo-reply 0
Ether / IP / ICMP 10.0.2.4 > 10.0.2.15 echo-request 0 / Padding
Ether / IP / ICMP 10.0.2.15 > 10.0.2.4 echo-reply 0
>>> wrpcap("Desktop/p_2_to_1.pcap", p_2_to_1)
```

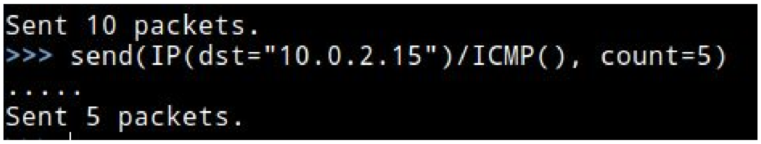
3) Screenshot of PING exchange



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.15	10.0.2.4	ICMP	60	Echo (ping) request
2	0.000535	10.0.2.4	10.0.2.15	ICMP	42	Echo (ping) reply
3	0.001760	10.0.2.15	10.0.2.4	ICMP	60	Echo (ping) request
4	0.001779	10.0.2.4	10.0.2.15	ICMP	42	Echo (ping) reply
5	0.004197	10.0.2.15	10.0.2.4	ICMP	60	Echo (ping) request
6	0.004217	10.0.2.4	10.0.2.15	ICMP	42	Echo (ping) reply
7	0.005958	10.0.2.15	10.0.2.4	ICMP	60	Echo (ping) request
8	0.005972	10.0.2.4	10.0.2.15	ICMP	42	Echo (ping) reply
9	0.008197	10.0.2.15	10.0.2.4	ICMP	60	Echo (ping) request
10	0.008227	10.0.2.4	10.0.2.15	ICMP	42	Echo (ping) reply

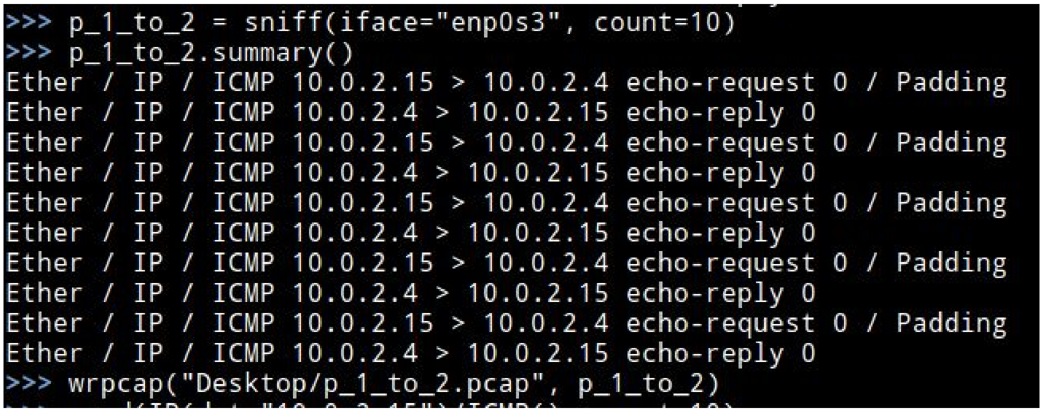
PS2:

4) Command used for sending:(From PS2)



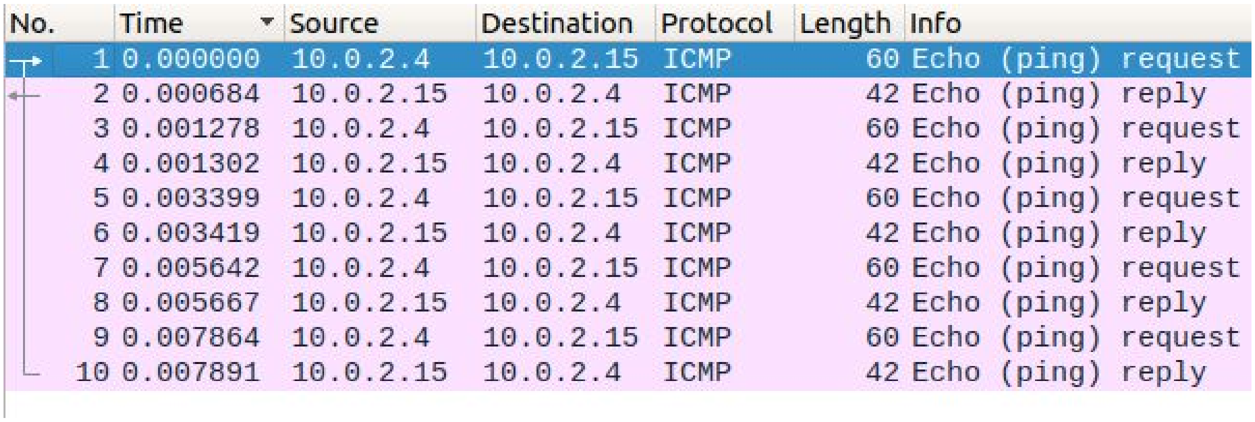
```
Sent 10 packets.
>>> send(IP(dst="10.0.2.15")/ICMP(), count=5)
.....
Sent 5 packets.
```

5) Command used for receiving:(At PS1)



```
>>> p_1_to_2 = sniff(iface="enp0s3", count=10)
>>> p_1_to_2.summary()
Ether / IP / ICMP 10.0.2.15 > 10.0.2.4 echo-request 0 / Padding
Ether / IP / ICMP 10.0.2.4 > 10.0.2.15 echo-reply 0
Ether / IP / ICMP 10.0.2.15 > 10.0.2.4 echo-request 0 / Padding
Ether / IP / ICMP 10.0.2.4 > 10.0.2.15 echo-reply 0
Ether / IP / ICMP 10.0.2.15 > 10.0.2.4 echo-request 0 / Padding
Ether / IP / ICMP 10.0.2.4 > 10.0.2.15 echo-reply 0
Ether / IP / ICMP 10.0.2.15 > 10.0.2.4 echo-request 0 / Padding
Ether / IP / ICMP 10.0.2.4 > 10.0.2.15 echo-reply 0
Ether / IP / ICMP 10.0.2.15 > 10.0.2.4 echo-request 0 / Padding
Ether / IP / ICMP 10.0.2.4 > 10.0.2.15 echo-reply 0
>>> wrpcap("Desktop/p_1_to_2.pcap", p_1_to_2)
```

6) Screenshot of PING exchange

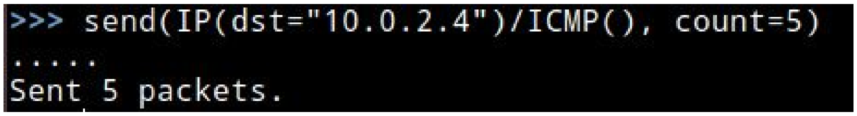


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.4	10.0.2.15	ICMP	60	Echo (ping) request
2	0.000684	10.0.2.15	10.0.2.4	ICMP	42	Echo (ping) reply
3	0.001278	10.0.2.4	10.0.2.15	ICMP	60	Echo (ping) request
4	0.001302	10.0.2.15	10.0.2.4	ICMP	42	Echo (ping) reply
5	0.003399	10.0.2.4	10.0.2.15	ICMP	60	Echo (ping) request
6	0.003419	10.0.2.15	10.0.2.4	ICMP	42	Echo (ping) reply
7	0.005642	10.0.2.4	10.0.2.15	ICMP	60	Echo (ping) request
8	0.005667	10.0.2.15	10.0.2.4	ICMP	42	Echo (ping) reply
9	0.007864	10.0.2.4	10.0.2.15	ICMP	60	Echo (ping) request
10	0.007891	10.0.2.15	10.0.2.4	ICMP	42	Echo (ping) reply

Section 3.3: (Step-III)

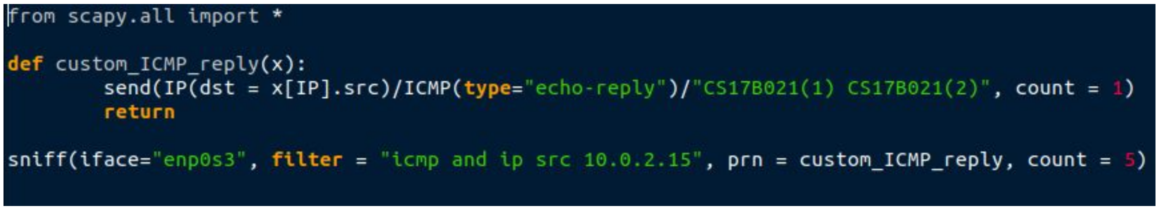
A) Sending ICMP Request from PS1 to PS2

a) PS1 ICMP Request construction command:

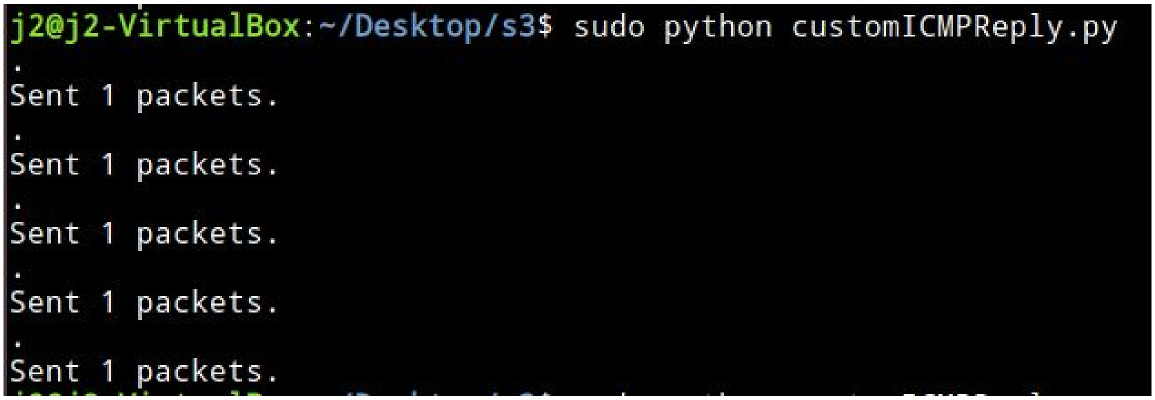


```
>>> send(IP(dst="10.0.2.4")/ICMP(), count=5)
.....
Sent 5 packets.
```

b) PS2 ICMP Custom Response construction program and PING exchange:



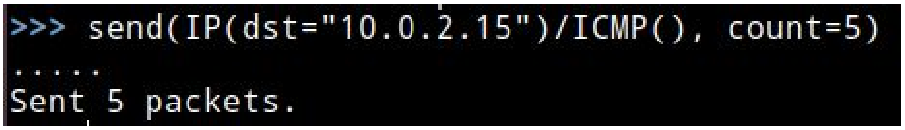
```
from scapy.all import *

def custom_ICMP_reply(x):
        send(IP(dst = x[IP].src)/ICMP(type="echo-reply")/"CS17B021(1) CS17B021(2)", count = 1)
        return

sniff(iface="enp0s3", filter = "icmp and ip src 10.0.2.15", prn = custom_ICMP_reply, count = 5)
```



```
j2@j2-VirtualBox:~/Desktop/s3$ sudo python customICMPReply.py
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
```

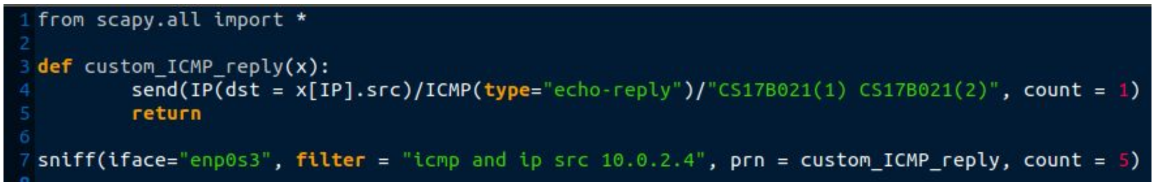
B) Sending ICMP Request from PS2 to PS1

a) PS2 ICMP Request construction command:

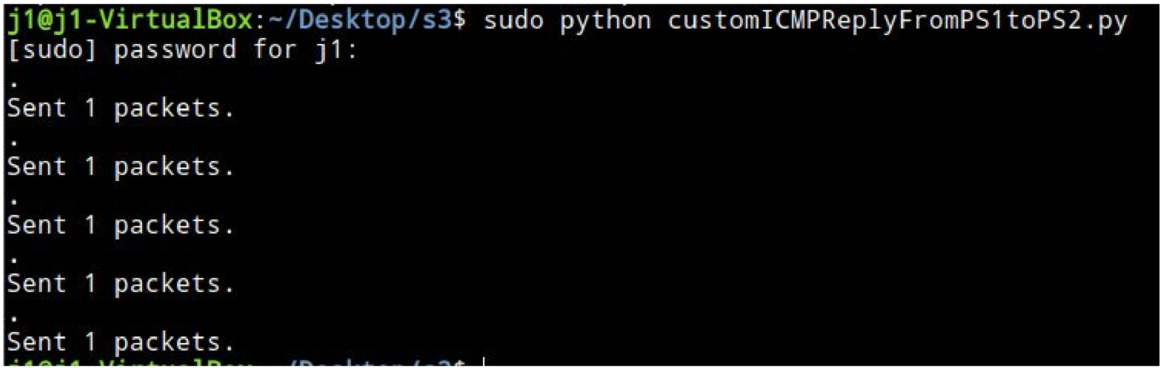


```
>>> send(IP(dst="10.0.2.15")/ICMP(), count=5)
.....
Sent 5 packets.
```

b) PS1 ICMP Custom Response construction program and PING exchange:



```python
from scapy.all import *

def custom_ICMP_reply(x):
        send(IP(dst = x[IP].src)/ICMP(type="echo-reply")/"CS17B021(1) CS17B021(2)", count = 1)
        return

sniff(iface="enp0s3", filter = "icmp and ip src 10.0.2.4", prn = custom_ICMP_reply, count = 5)
```

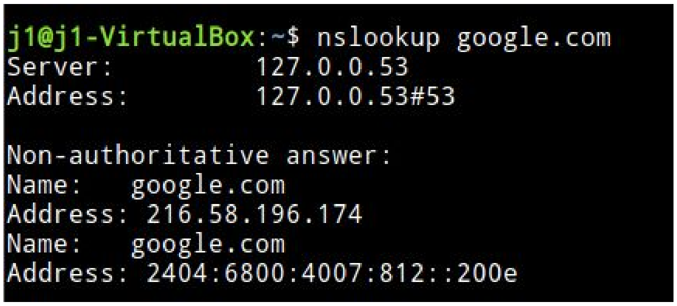


```
j1@j1-VirtualBox:~/Desktop/s3$ sudo python customICMPReplyFromPS1toPS2.py
[sudo] password for j1:
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
j1@j1-VirtualBox:~/Desktop/s3$
```

<u>Section 3.4:</u> (Step-IV)

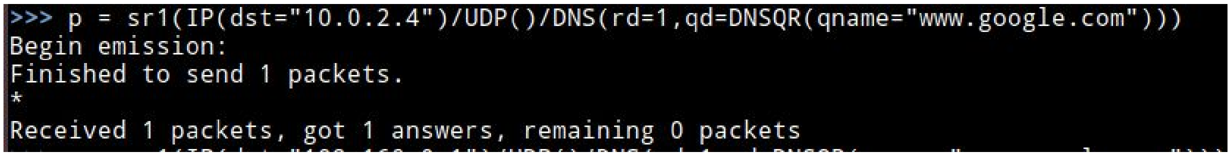
A) <u>Sending DNS request from PS1 to PS2 (www.google.com)</u>

a) PS1 - Screenshot for normal nslookup



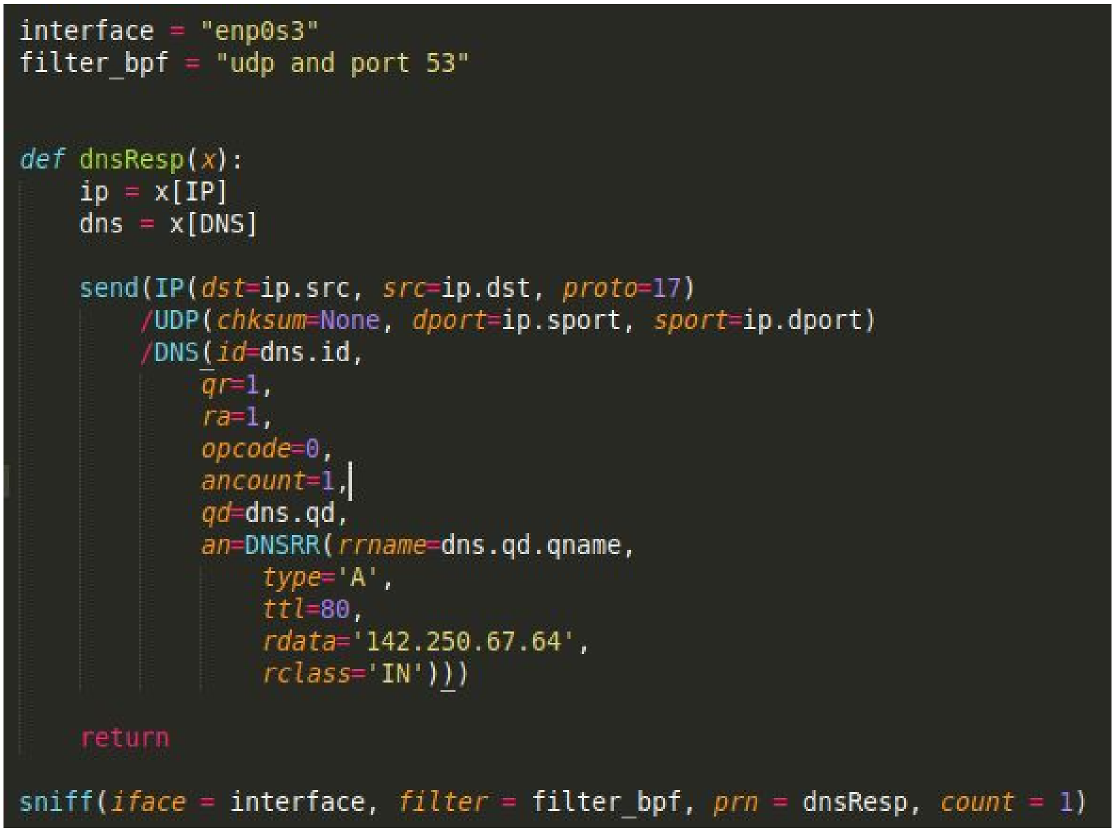
```
j1@j1-VirtualBox:~$ nslookup google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 216.58.196.174
Name:   google.com
Address: 2404:6800:4007:812::200e
```

b) DNS Query Packet Construction at PS1



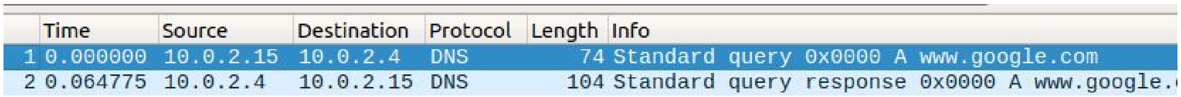
```
>>> p = sr1(IP(dst="10.0.2.4")/UDP()/DNS(rd=1,qd=DNSQR(qname="www.google.com")))
Begin emission:
Finished to send 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
```

c) DNS Query Response Packet construction at PS2



```python
interface = "enp0s3"
filter_bpf = "udp and port 53"


def dnsResp(x):
    ip = x[IP]
    dns = x[DNS]

    send(IP(dst=ip.src, src=ip.dst, proto=17)
        /UDP(chksum=None, dport=ip.sport, sport=ip.dport)
        /DNS(id=dns.id,
            qr=1,
            ra=1,
            opcode=0,
            ancount=1,
            qd=dns.qd,
            an=DNSRR(rrname=dns.qd.qname,
                type='A',
                ttl=80,
                rdata='142.250.67.64',
                rclass='IN')))

    return

sniff(iface = interface, filter = filter_bpf, prn = dnsResp, count = 1)
```

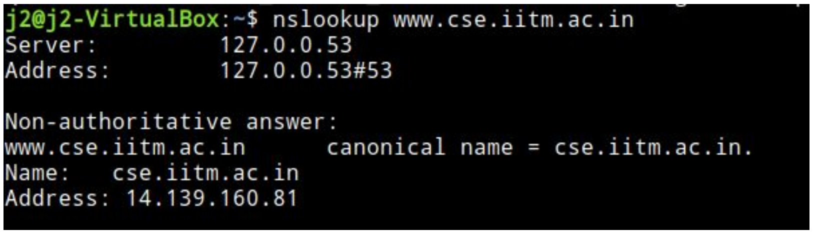
d) PING Exchange (DNS Query and Response)



	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.15	10.0.2.4	DNS	74	Standard query 0x0000 A www.google.com
2	0.064775	10.0.2.4	10.0.2.15	DNS	104	Standard query response 0x0000 A www.google.

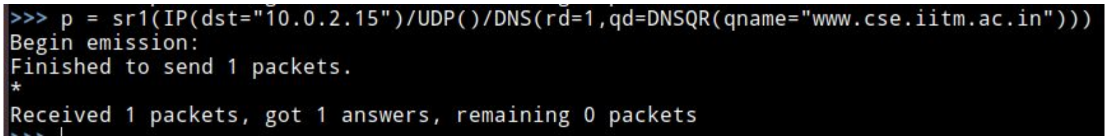
B) Sending DNS request from PS2 to PS1 (www.cse.iitm.ac.in)

a) PS2 - Screenshot for normal nslookup



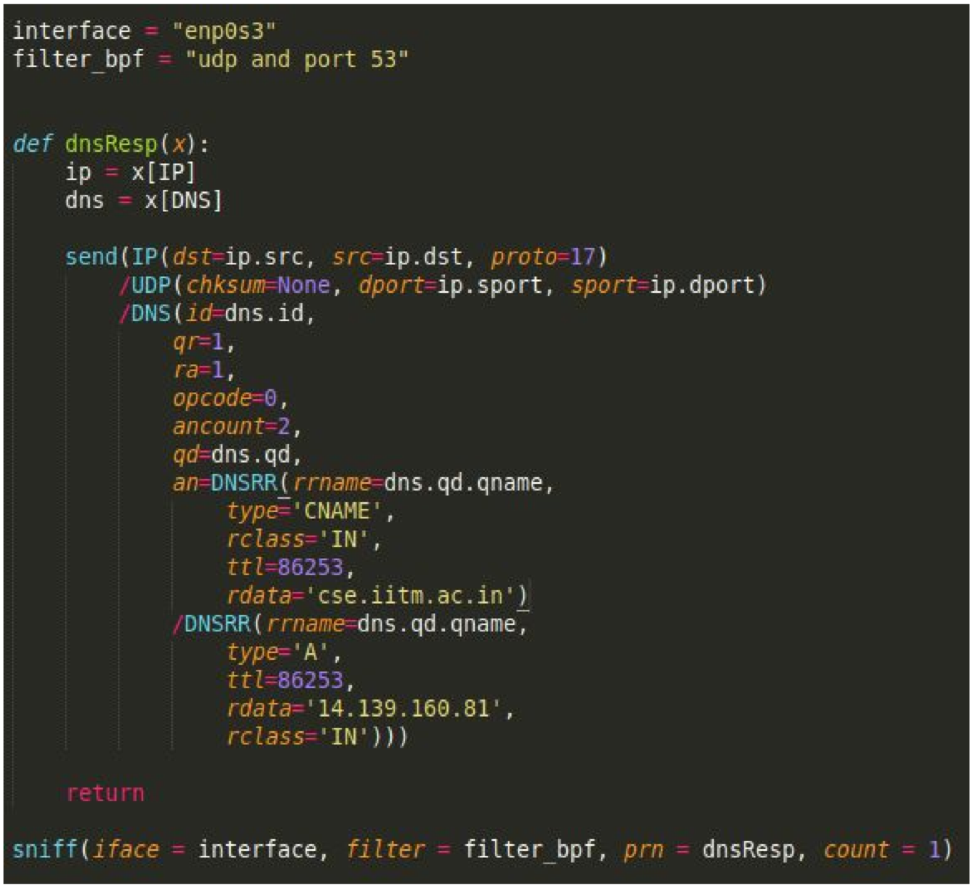
```
j2@j2-VirtualBox:~$ nslookup www.cse.iitm.ac.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
www.cse.iitm.ac.in      canonical name = cse.iitm.ac.in.
Name:   cse.iitm.ac.in
Address: 14.139.160.81
```

b) DNS Query Packet Construction at PS2



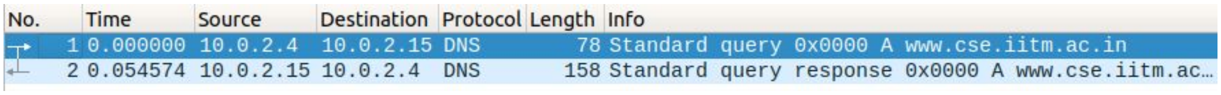
```
>>> p = sr1(IP(dst="10.0.2.15")/UDP()/DNS(rd=1,qd=DNSQR(qname="www.cse.iitm.ac.in")))
Begin emission:
Finished to send 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
```

c) DNS Query Response Packet construction at PS1



```
interface = "enp0s3"
filter_bpf = "udp and port 53"


def dnsResp(x):
    ip = x[IP]
    dns = x[DNS]

    send(IP(dst=ip.src, src=ip.dst, proto=17)
        /UDP(chksum=None, dport=ip.sport, sport=ip.dport)
        /DNS(id=dns.id,
            qr=1,
            ra=1,
            opcode=0,
            ancount=2,
            qd=dns.qd,
            an=DNSRR(rrname=dns.qd.qname,
                type='CNAME',
                rclass='IN',
                ttl=86253,
                rdata='cse.iitm.ac.in')
            /DNSRR(rrname=dns.qd.qname,
                type='A',
                ttl=86253,
                rdata='14.139.160.81',
                rclass='IN')))

    return

sniff(iface = interface, filter = filter_bpf, prn = dnsResp, count = 1)
```

d) PING Exchange (DNS Query and Response)



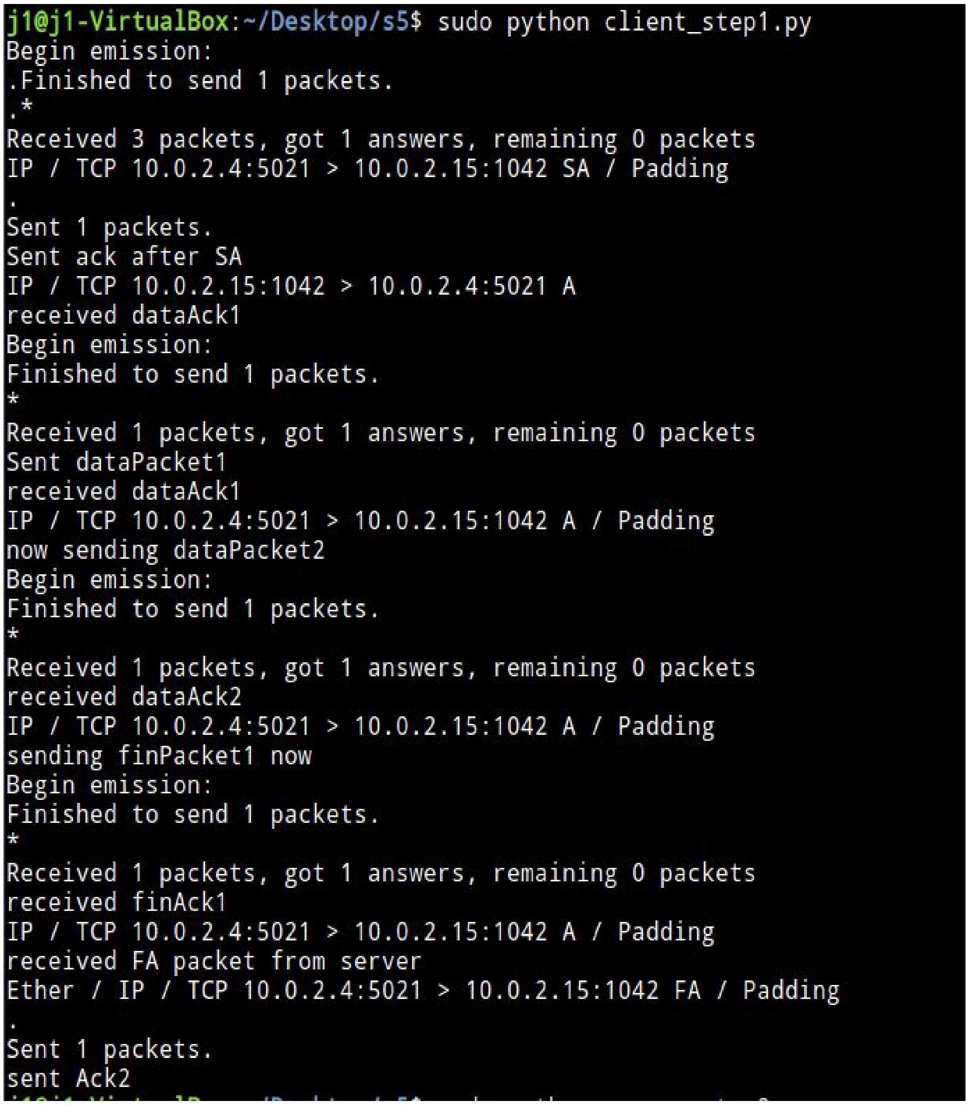
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.4	10.0.2.15	DNS	78	Standard query 0x0000 A www.cse.iitm.ac.in
2	0.054574	10.0.2.15	10.0.2.4	DNS	158	Standard query response 0x0000 A www.cse.iitm.ac…

<u>Section 3.5:</u> (Step-V)

Note: Please execute the command in README.md placed in Step 5 folder at both PS1 and PS2 for python scripts to work.

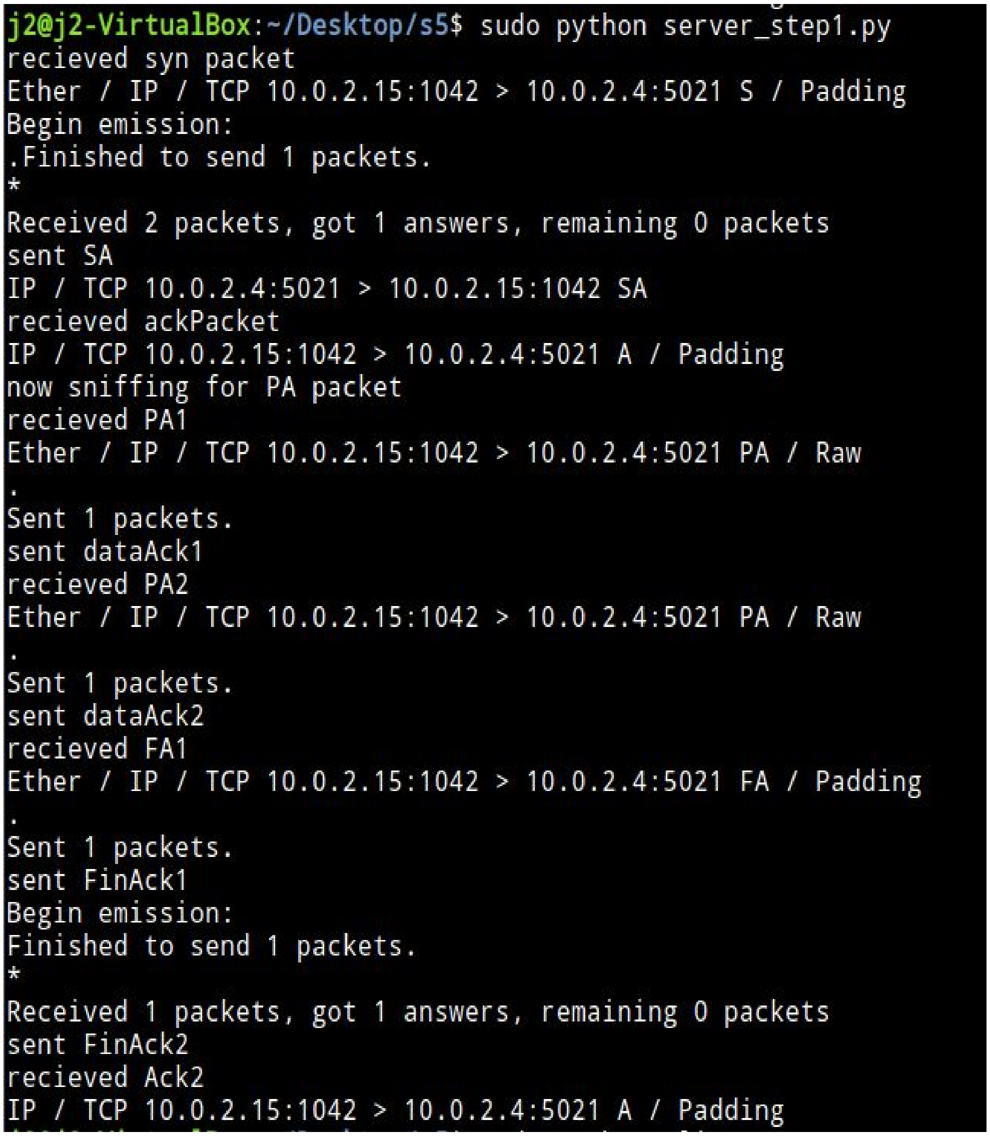
A) PS1 as TCP Client and PS2 as TCP Server

1) Client Side (PS1)



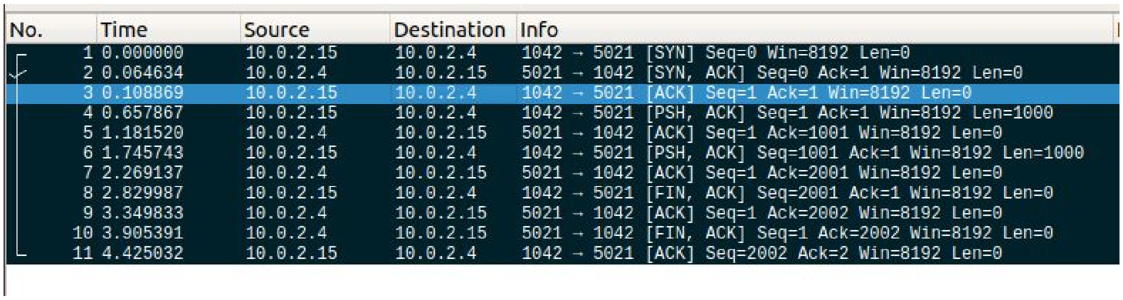
```
j1@j1-VirtualBox:~/Desktop/s5$ sudo python client_step1.py
Begin emission:
.Finished to send 1 packets.
.*
Received 3 packets, got 1 answers, remaining 0 packets
IP / TCP 10.0.2.4:5021 > 10.0.2.15:1042 SA / Padding
.
Sent 1 packets.
Sent ack after SA
IP / TCP 10.0.2.15:1042 > 10.0.2.4:5021 A
received dataAck1
Begin emission:
Finished to send 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
Sent dataPacket1
received dataAck1
IP / TCP 10.0.2.4:5021 > 10.0.2.15:1042 A / Padding
now sending dataPacket2
Begin emission:
Finished to send 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
received dataAck2
IP / TCP 10.0.2.4:5021 > 10.0.2.15:1042 A / Padding
sending finPacket1 now
Begin emission:
Finished to send 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
received finAck1
IP / TCP 10.0.2.4:5021 > 10.0.2.15:1042 A / Padding
received FA packet from server
Ether / IP / TCP 10.0.2.4:5021 > 10.0.2.15:1042 FA / Padding
.
Sent 1 packets.
sent Ack2
```

2) Server Side (PS2)



```
j2@j2-VirtualBox:~/Desktop/s5$ sudo python server_step1.py
recieved syn packet
Ether / IP / TCP 10.0.2.15:1042 > 10.0.2.4:5021 S / Padding
Begin emission:
.Finished to send 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
sent SA
IP / TCP 10.0.2.4:5021 > 10.0.2.15:1042 SA
recieved ackPacket
IP / TCP 10.0.2.15:1042 > 10.0.2.4:5021 A / Padding
now sniffing for PA packet
recieved PA1
Ether / IP / TCP 10.0.2.15:1042 > 10.0.2.4:5021 PA / Raw
.
Sent 1 packets.
sent dataAck1
recieved PA2
Ether / IP / TCP 10.0.2.15:1042 > 10.0.2.4:5021 PA / Raw
.
Sent 1 packets.
sent dataAck2
recieved FA1
Ether / IP / TCP 10.0.2.15:1042 > 10.0.2.4:5021 FA / Padding
.
Sent 1 packets.
sent FinAck1
Begin emission:
Finished to send 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
sent FinAck2
recieved Ack2
IP / TCP 10.0.2.15:1042 > 10.0.2.4:5021 A / Padding
```

3) Wireshark Capture at Client (PS1) showing TCP Packets Exchange

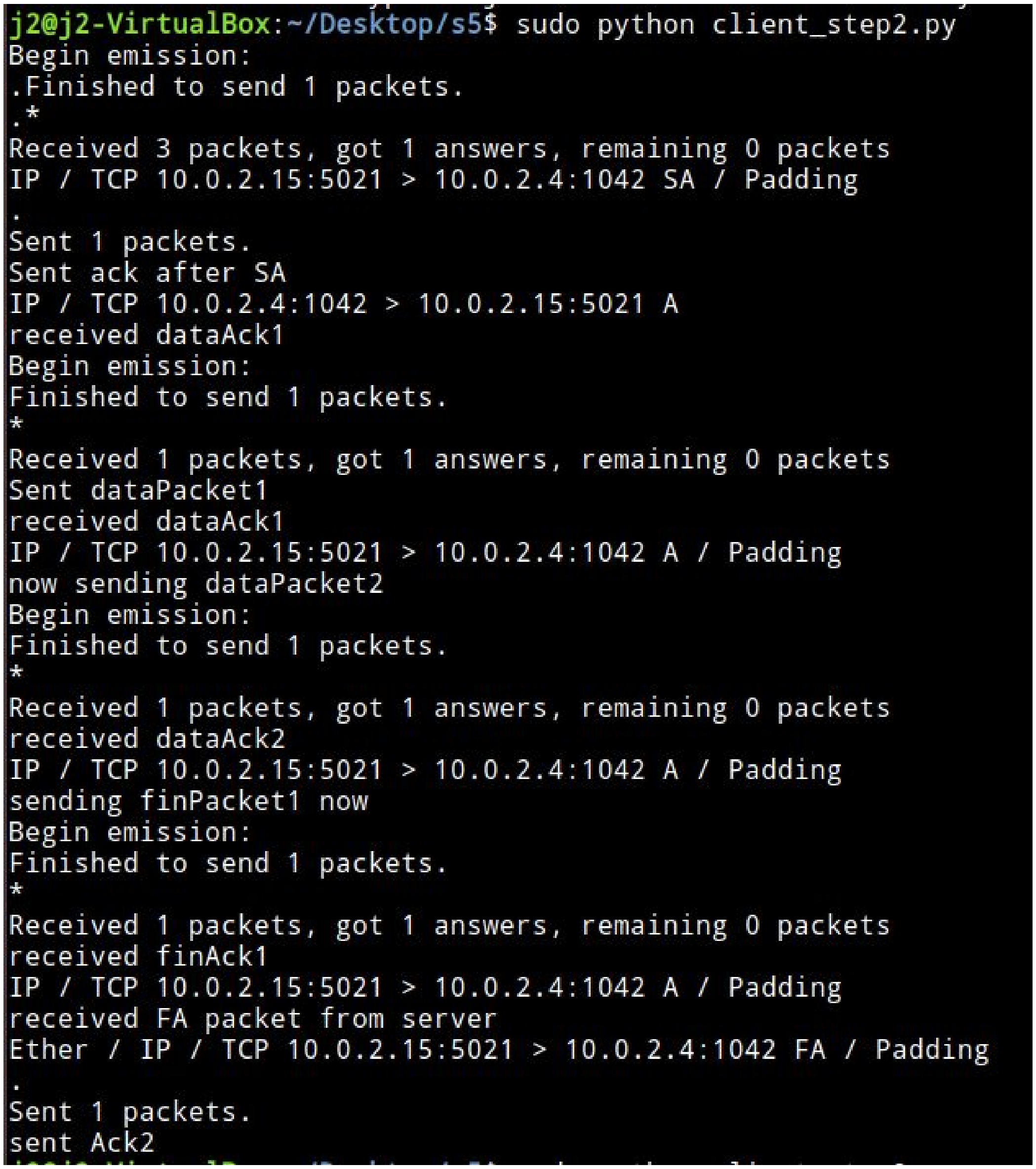


No.	Time	Source	Destination	Info
1	0.000000	10.0.2.15	10.0.2.4	1042 → 5021 [SYN] Seq=0 Win=8192 Len=0
2	0.064634	10.0.2.4	10.0.2.15	5021 → 1042 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
3	0.108869	10.0.2.15	10.0.2.4	1042 → 5021 [ACK] Seq=1 Ack=1 Win=8192 Len=0
4	0.657867	10.0.2.15	10.0.2.4	1042 → 5021 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=1000
5	1.181520	10.0.2.4	10.0.2.15	5021 → 1042 [ACK] Seq=1 Ack=1001 Win=8192 Len=0
6	1.745743	10.0.2.15	10.0.2.4	1042 → 5021 [PSH, ACK] Seq=1001 Ack=1 Win=8192 Len=1000
7	2.269137	10.0.2.4	10.0.2.15	5021 → 1042 [ACK] Seq=1 Ack=2001 Win=8192 Len=0
8	2.829987	10.0.2.15	10.0.2.4	1042 → 5021 [FIN, ACK] Seq=2001 Ack=1 Win=8192 Len=0
9	3.349833	10.0.2.4	10.0.2.15	5021 → 1042 [ACK] Seq=1 Ack=2002 Win=8192 Len=0
10	3.905391	10.0.2.4	10.0.2.15	5021 → 1042 [FIN, ACK] Seq=1 Ack=2002 Win=8192 Len=0
11	4.425032	10.0.2.15	10.0.2.4	1042 → 5021 [ACK] Seq=2002 Ack=2 Win=8192 Len=0

BONUS

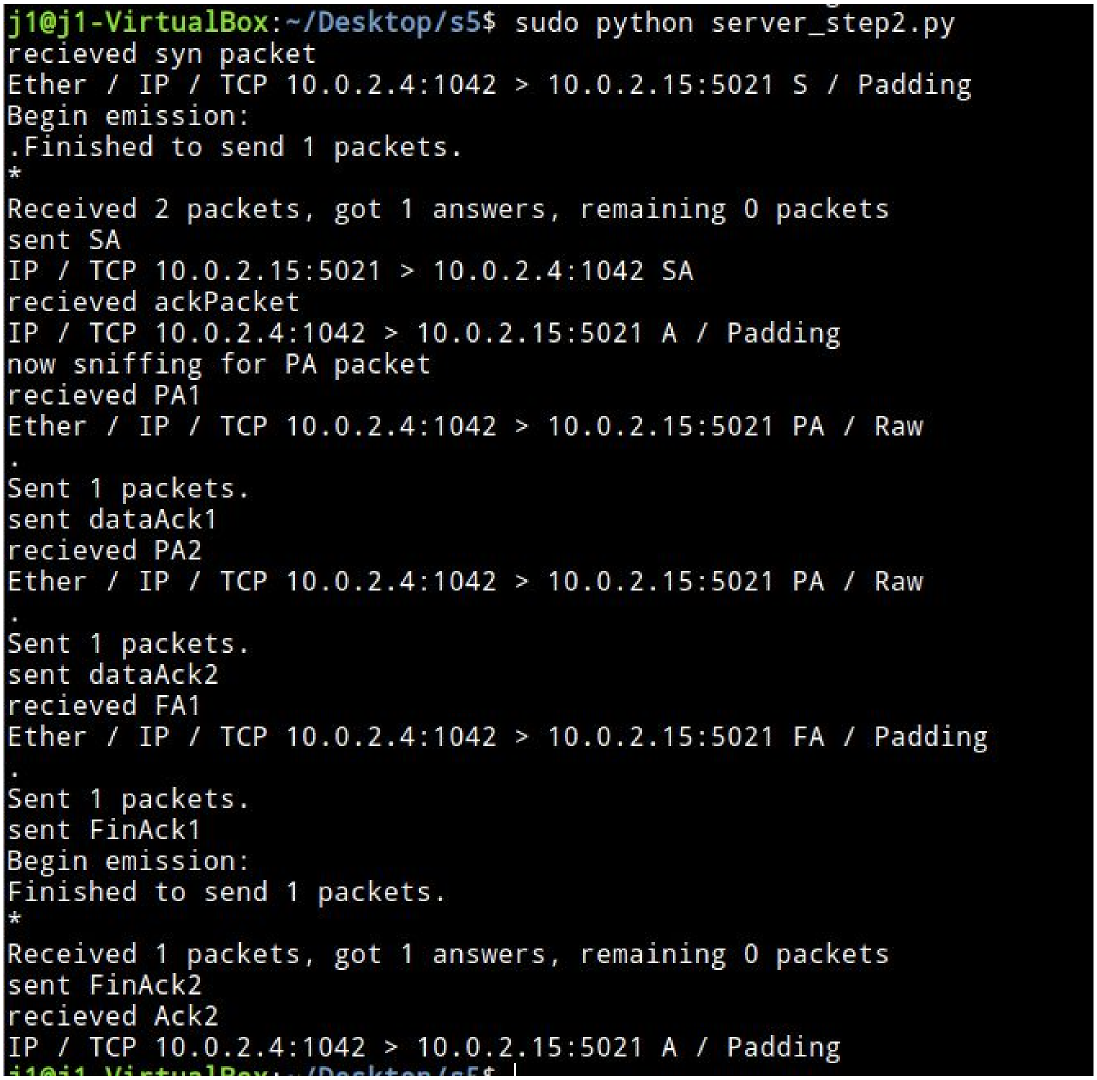
B) PS2 as TCP Client and PS1 as TCP Server

1) **Client Side (PS2)**



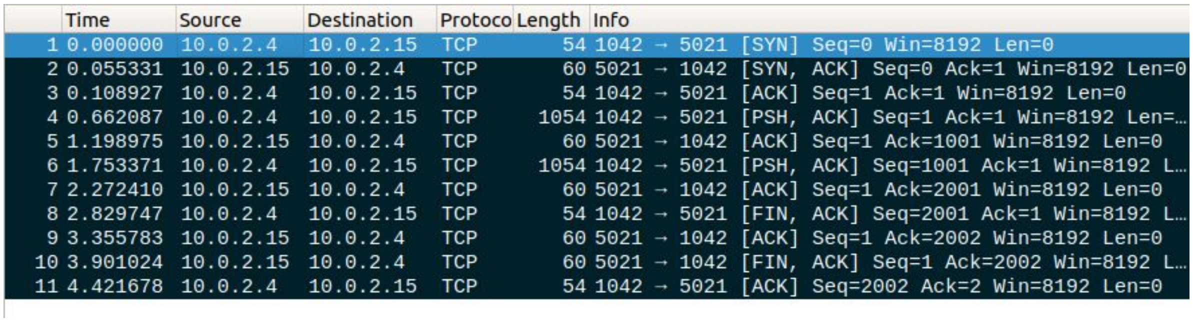
```
j2@j2-VirtualBox:~/Desktop/s5$ sudo python client_step2.py
Begin emission:
.Finished to send 1 packets.
.*
Received 3 packets, got 1 answers, remaining 0 packets
IP / TCP 10.0.2.15:5021 > 10.0.2.4:1042 SA / Padding
.
Sent 1 packets.
Sent ack after SA
IP / TCP 10.0.2.4:1042 > 10.0.2.15:5021 A
received dataAck1
Begin emission:
Finished to send 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
Sent dataPacket1
received dataAck1
IP / TCP 10.0.2.15:5021 > 10.0.2.4:1042 A / Padding
now sending dataPacket2
Begin emission:
Finished to send 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
received dataAck2
IP / TCP 10.0.2.15:5021 > 10.0.2.4:1042 A / Padding
sending finPacket1 now
Begin emission:
Finished to send 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
received finAck1
IP / TCP 10.0.2.15:5021 > 10.0.2.4:1042 A / Padding
received FA packet from server
Ether / IP / TCP 10.0.2.15:5021 > 10.0.2.4:1042 FA / Padding
.
Sent 1 packets.
sent Ack2
```

2) Server Side (PS1)



```
j1@j1-VirtualBox:~/Desktop/s5$ sudo python server_step2.py
recieved syn packet
Ether / IP / TCP 10.0.2.4:1042 > 10.0.2.15:5021 S / Padding
Begin emission:
.Finished to send 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
sent SA
IP / TCP 10.0.2.15:5021 > 10.0.2.4:1042 SA
recieved ackPacket
IP / TCP 10.0.2.4:1042 > 10.0.2.15:5021 A / Padding
now sniffing for PA packet
recieved PA1
Ether / IP / TCP 10.0.2.4:1042 > 10.0.2.15:5021 PA / Raw
.
Sent 1 packets.
sent dataAck1
recieved PA2
Ether / IP / TCP 10.0.2.4:1042 > 10.0.2.15:5021 PA / Raw
.
Sent 1 packets.
sent dataAck2
recieved FA1
Ether / IP / TCP 10.0.2.4:1042 > 10.0.2.15:5021 FA / Padding
.
Sent 1 packets.
sent FinAck1
Begin emission:
Finished to send 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
sent FinAck2
recieved Ack2
IP / TCP 10.0.2.4:1042 > 10.0.2.15:5021 A / Padding
j1@j1-VirtualBox:~/Desktop/s5$
```

3) Wireshark Capture at Client (PS2) showing TCP Packets Exchange



	Time	Source	Destination	Protoco	Length	Info
1	0.000000	10.0.2.4	10.0.2.15	TCP	54	1042 → 5021 [SYN] Seq=0 Win=8192 Len=0
2	0.055331	10.0.2.15	10.0.2.4	TCP	60	5021 → 1042 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
3	0.108927	10.0.2.4	10.0.2.15	TCP	54	1042 → 5021 [ACK] Seq=1 Ack=1 Win=8192 Len=0
4	0.662087	10.0.2.4	10.0.2.15	TCP	1054	1042 → 5021 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=…
5	1.198975	10.0.2.15	10.0.2.4	TCP	60	5021 → 1042 [ACK] Seq=1 Ack=1001 Win=8192 Len=0
6	1.753371	10.0.2.4	10.0.2.15	TCP	1054	1042 → 5021 [PSH, ACK] Seq=1001 Ack=1 Win=8192 L…
7	2.272410	10.0.2.15	10.0.2.4	TCP	60	5021 → 1042 [ACK] Seq=1 Ack=2001 Win=8192 Len=0
8	2.829747	10.0.2.4	10.0.2.15	TCP	54	1042 → 5021 [FIN, ACK] Seq=2001 Ack=1 Win=8192 L…
9	3.355783	10.0.2.15	10.0.2.4	TCP	60	5021 → 1042 [ACK] Seq=1 Ack=2002 Win=8192 Len=0
10	3.901024	10.0.2.15	10.0.2.4	TCP	60	5021 → 1042 [FIN, ACK] Seq=1 Ack=2002 Win=8192 L…
11	4.421678	10.0.2.4	10.0.2.15	TCP	54	1042 → 5021 [ACK] Seq=2002 Ack=2 Win=8192 Len=0