Assignment 5 (Macro Assignment 3)

Section 3.1:

```
subbu@subbu-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::5b8:ca6e:14e6:19c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:de:cf:29  txqueuelen 1000  (Ethernet)
        RX packets 100  bytes 17333 (17.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 153  bytes 16355 (16.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
subbu@subbu-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::d224:d969:68ca:76e1  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:29:64:67  txqueuelen 1000  (Ethernet)
        RX packets 98  bytes 17456 (17.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 159  bytes 17187 (17.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

1. In this assignment, I used 2 linux (Ubuntu) virtual machines on my windows os
2. Above screenshots are system specifications - IP of PS1 is 10.0.2.15 and PS2 is 10.0.2.4

Section 3.2:

1. First two are of ping and sniff from ps1 to ps2 and the next two are the same from ps2 to ps1

```
>>> ps1_pckt = IP(dst="10.0.2.4")/ICMP()
>>> send(ps1_pckt,count=5)
.....
Sent 5 packets.
>>>
```

```
>>> rec_pckt = sniff(filter="icmp",count=10)
>>> rec_pckt.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
>>> 
```

```
>>> ps2_pckt = IP(dst="10.0.2.15")/ICMP()
>>> send(ps2_pckt,count=5)
.....
Sent 5 packets.
>>> 
```

```
>>> recv_pckt = sniff(filter="icmp",count=10)
>>> recv_pckt.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
>>>
```

Section 3.3:

1. The reply is sent by a sniff response function in the second and fourth screenshots
2. Custom reply has a payload to differentiate it from system generated
3. My payload is 00050005 (byte format)
4. Normal text is converted into bytes in wireshark captures hence I sent this

```
>>> ps1_pckt = IP(dst="10.0.2.4")/ICMP()
>>> send(ps1_pckt,count=5)
.....
Sent 5 packets.
```

```
>>> def icmp_reply(p):
...     dstn = p[IP].src
...     if (p[ICMP].type == 8) :
...             print("Detected and Sending reply")
...             rep = IP(dst=dstn)/ICMP(type="echo-reply")/"\0\5\0\5"
...             send(rep)
...
>>> sniff(filter="icmp",prn=icmp_reply)
Detected and Sending reply
.
Sent 1 packets.
Detected and Sending reply
.
Sent 1 packets.
Detected and Sending reply
.
Sent 1 packets.
Detected and Sending reply
.
Sent 1 packets.
Detected and Sending reply
.
Sent 1 packets.
^C<Sniffed: TCP:0 UDP:0 ICMP:15 Other:0>
>>>
```

```
>>> ps2_pck = IP(dst="10.0.2.15")/ICMP()
>>> send(ps2_pck,count=5)
.....
Sent 5 packets.
>>>
```

```
>>> def icmp_reply(p):
...     dstn = p[IP].src
...     if (p[ICMP].type == 8) :
...             print("Detected and Sending reply")
...             rep = IP(dst=dstn)/ICMP(type="echo-reply")/"\0\5\0\5"
...             send(rep)
...
>>> sniff(filter="icmp",prn=icmp_reply)
Detected and Sending reply
.
Sent 1 packets.
Detected and Sending reply
.
Sent 1 packets.
Detected and Sending reply
.
Sent 1 packets.
Detected and Sending reply
.
Sent 1 packets.
Detected and Sending reply
.
Sent 1 packets.
^C<Sniffed: TCP:0 UDP:0 ICMP:15 Other:0>
>>>
```

Section 3.4:

1. DNS replies are served by custom_dns_serv function in the 3rd screenshot
2. This function pings standard 8.8.8.8 server to get response
3. Now new DNS query reply is constructed from the scratch using the information

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

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.67.68
Name:   www.google.com
Address: 2404:6800:4007:805::2004
```

```
>>>
>>> query = DNSQR(qname="www.google.com")
>>> dns_req = IP(dst="10.0.2.4")/UDP(dport=53)/DNS(rd=1,qd=query)
>>> reply = sr1(dns_req)
Begin emission:
.Finished sending 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
>>>
```

```
>>> def custom_dns_serv(p):
...     print("Started")
...     dstn = p[IP].src
...     qsn = p[DNSQR].qname
...     print(qsn)
...     query = DNSQR(qname=qsn)
...     ans_pkt = sr1(IP(dst="8.8.8.8")/UDP(dport=53)/
...             DNS(rd=1,qd=query))
...     ans = ans_pkt[DNSRR].rdata
...     print("Recieved and Sending back")
...     print(ans)
...     send(IP(dst=dstn)/UDP(dport=53)/
...             DNS(id=p[DNS].id,qr=1,rd=1,ra=1,qdcount=1,ancount=1,
...             qd=DNSQR(qname=qsn),an=DNSRR(rrname=qsn,
...             type=ans_pkt[DNSRR].type,rclass=ans_pkt[DNSRR].rclass,
...             rdata=ans)))
...     print("Done")
...
...
>>> sniff(filter="udp and port 53",count=1,prn=custom_dns_serv)
Started
b'www.google.com.'
Begin emission:
.Finished sending 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
Recieved and Sending back
172.217.167.36
.
Sent 1 packets.
Done
<Sniffed: TCP:0 UDP:1 ICMP:0 Other:0>
>>>
```

```
subbu@subbu-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
```

```
>>> query = DNSQR(qname="www.cse.iitm.ac.in")
>>> dns_req_pc2 = IP(dst="10.0.2.15")/UDP(dport=53)/DNS(rd=1,qd=query)
>>> reply = sr1(dns_req_pc2)
Begin emission:
.Finished sending 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
```

```
>>> def custom_dns_serv(p):
...     print("Started")
...     dstn = p[IP].src
...     qsn = p[DNSQR].qname
...     print(qsn)
...     query = DNSQR(qname=qsn)
...     ans_pkt = sr1(IP(dst="8.8.8.8")/UDP(dport=53)/
...             DNS(rd=1,qd=query))
...     ans = ans_pkt[DNSRR].rdata
...     print("Recieved and Sending back")
...     print(ans)
...     send(IP(dst=dstn)/UDP(dport=53)/
...             DNS(id=p[DNS].id,qr=1,rd=1,ra=1,qdcount=1,ancount=1,
...             qd=DNSQR(qname=qsn),an=DNSRR(rrname=qsn,
...             type=ans_pkt[DNSRR].type,rclass=ans_pkt[DNSRR].rclass,
...             rdata=ans)))
...     print("Done")
...
>>> sniff(filter="udp and port 53",count=1,prn=custom_dns_serv)
Started
b'www.cse.iitm.ac.in.'
Begin emission:
.Finished sending 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
Recieved and Sending back
b'cse.iitm.ac.in.'
.
Sent 1 packets.
Done
<Sniffed: TCP:0 UDP:1 ICMP:0 Other:0>
>>>
```

Section 3.5:

1. Here, for first connection the transfer of 200 bytes of data is shown but the programs transfers 2000 as asked, this is just to reduce the length of screenshot and it makes almost no difference in the code
2. Ports used are 5005 and 5034
3. The information and captures are provided for both the sets making it 4 screenshots and 2 captures

```
subbu@subbu-VirtualBox:~$ sudo python3 server.py
Started...
.
Sent 1 packets.
Connected to :
10.0.2.4 5005
Recieved Sequence:1
.
Sent 1 packets.
Acked Sequence:1
Recieved Sequence:2
.
Sent 1 packets.
Acked Sequence:2
.
Sent 1 packets.
.
Sent 1 packets.
[b'hihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihi
hihihihihihihihihihihihi', b'bybybybybybybybybybybybybybybybybybybybybybybybybybyby
bybybybybybybybybybybybybybybybybybybybybybybybybybybyby']
Connection closed
Ended
subbu@subbu-VirtualBox:~$
```

```
subbu@subbu-VirtualBox:~$ sudo python3 client.py
.
Sent 1 packets.
.
Sent 1 packets.
Connected to Server
.
Sent 1 packets.
Acked-Sequence:1
.
Sent 1 packets.
Acked-Sequence:2
Data Sent Sucessfully
.
Sent 1 packets.
Acked-Sequence:0
Acked-Finish
.
Sent 1 packets.
```

```
subbu@subbu-VirtualBox:~$ sudo python3 server.py
Started...
.
Sent 1 packets.
Connected to :
10.0.2.15 5005
Recieved Sequence:1
.
Sent 1 packets.
Acked Sequence:1
Recieved Sequence:2
.
Sent 1 packets.
Acked Sequence:2
.
Sent 1 packets.
.
Sent 1 packets.
[b'hihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihih
ihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihih
ihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihih
ihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihih
ihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihih
ihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihih
ihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihih
ihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihih
ihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihih
ihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihihi', b'bybybybybyby
bybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybyby
bybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybyby
bybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybyby
bybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybyby
bybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybybyby
```

```
subbu@subbu-VirtualBox:~$ sudo python3 client.py
.
Sent 1 packets.
.
Sent 1 packets.
Connected to Server
.
Sent 1 packets.
Acked-Sequence:1
.
Sent 1 packets.
Acked-Sequence:2
Data Sent Sucessfully
.
Sent 1 packets.
Acked-Sequence:0
Acked-Finish
.
Sent 1 packets.
```