שמות המגישים

יבגני אודינצוב -328667217

טלי טבלין - 206999195

דניאל דהן – 208906909

Project Cyber Risk Assessment sniffer

We built project that works in network protocols. Which includes:

Adversary:

Arp poisoning and packet sniffer to influence the flow of data.

Client:

Uses self-built pseudoTCP to send data to Server.

Server:

Uses self-built pseudoTCP to receive data .

pseudoTCP:

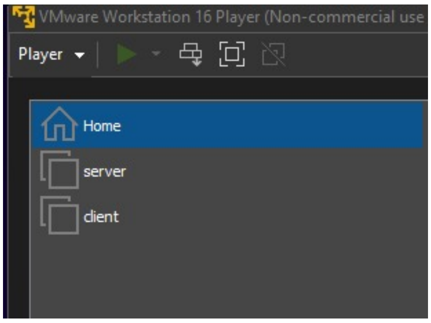
Application layer that simulates a real TCP behavior over UDP raw socket.

The demonstration starts on the next page

Settings:

Real PC – Adversary (Windows 11)

Client and server are Virtual machines (Linux OS)



VMware Workstation 16 Player (Non-commercial use

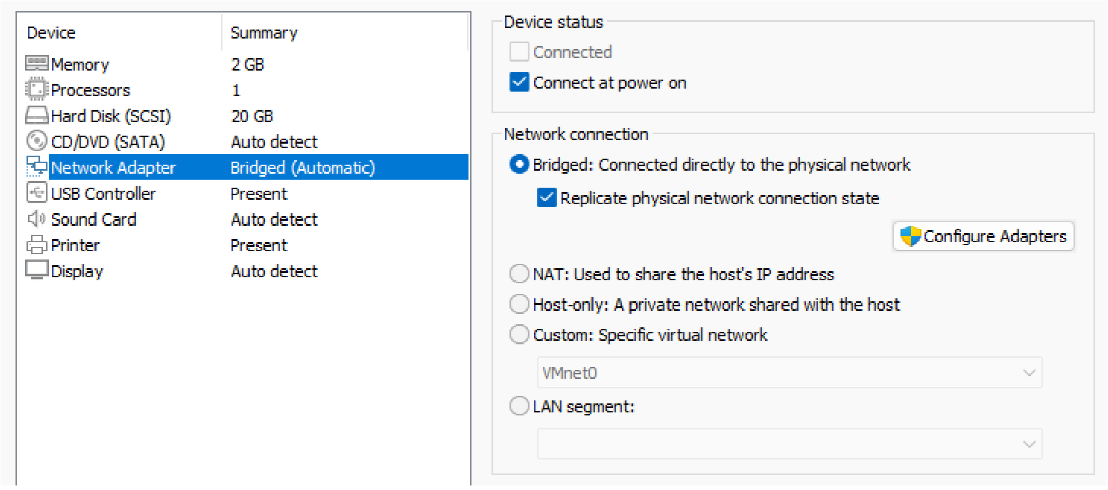
Player

Home

server

client

Which has bridged connection



Device	Summary
Memory	2 GB
Processors	1
Hard Disk (SCSI)	20 GB
CD/DVD (SATA)	Auto detect
Network Adapter	Bridged (Automatic)
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

□ Connected

☑ Connect at power on

Network connection

● Bridged: Connected directly to the physical network

☑ Replicate physical network connection state

Configure Adapters

○ NAT: Used to share the host's IP address

○ Host-only: A private network shared with the host

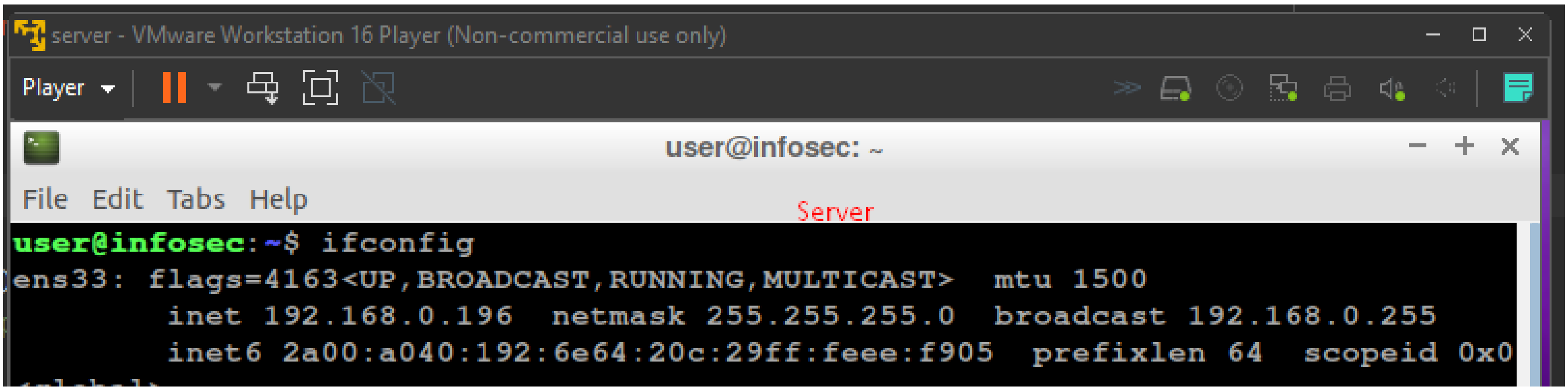
○ Custom: Specific virtual network

VMnet0

○ LAN segment:

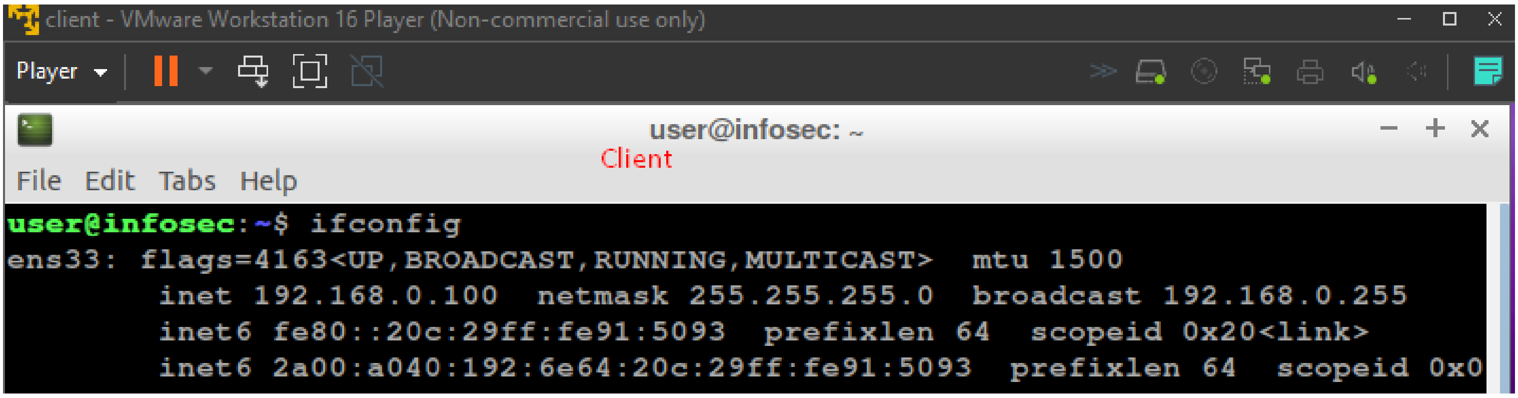
Configurations:

Server: 192.168.0.196


server - VMware Workstation 16 Player (Non-commercial use only)
Player
user@infosec: ~
File Edit Tabs Help
Server

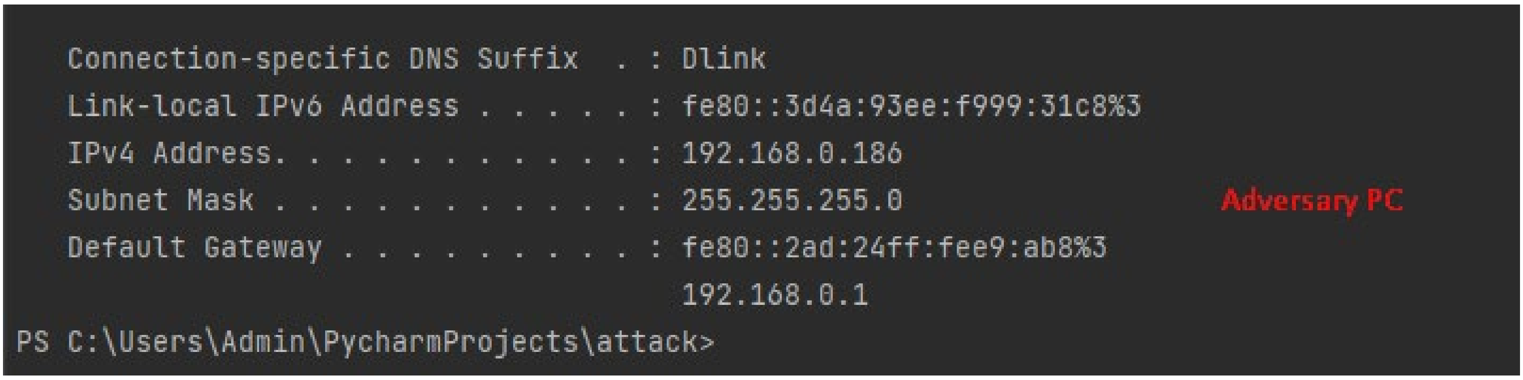
```
user@infosec:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.196  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 2a00:a040:192:6e64:20c:29ff:feee:f905  prefixlen 64  scopeid 0x0
```

Client: 192.168.0.100


client - VMware Workstation 16 Player (Non-commercial use only)
Player
user@infosec: ~
Client
File Edit Tabs Help

```
user@infosec:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.100  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::20c:29ff:fe91:5093  prefixlen 64  scopeid 0x20<link>
        inet6 2a00:a040:192:6e64:20c:29ff:fe91:5093  prefixlen 64  scopeid 0x0
```

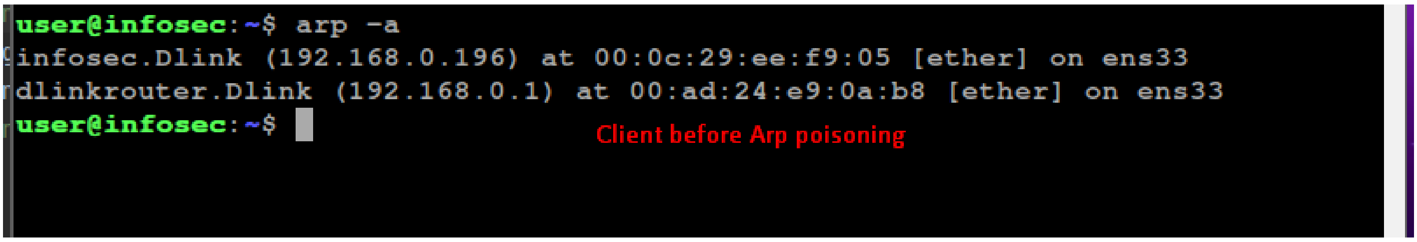
Adversary: 192.168.0.186



```
   Connection-specific DNS Suffix  . : Dlink
   Link-local IPv6 Address . . . . . : fe80::3d4a:93ee:f999:31c8%3
   IPv4 Address. . . . . . . . . . . : 192.168.0.186
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::2ad:24ff:fee9:ab8%3
                                       192.168.0.1
PS C:\Users\Admin\PycharmProjects\attack>
```

Client & Server communications without MiTM:

Clients ARP Table:



```
user@infosec:~$ arp -a
infosec.Dlink (192.168.0.196) at 00:0c:29:ee:f9:05 [ether] on ens33
dlinkrouter.Dlink (192.168.0.1) at 00:ad:24:e9:0a:b8 [ether] on ens33
user@infosec:~$
```

Client before Arp poisoning

When we launch the server and client , the traffic works as usual and without packet loss, next few screenshots demonstrate the communication between the client and server. The client willing to send a really long text message, the text message divided into chunks with length of 100 , 33 chunks overall.

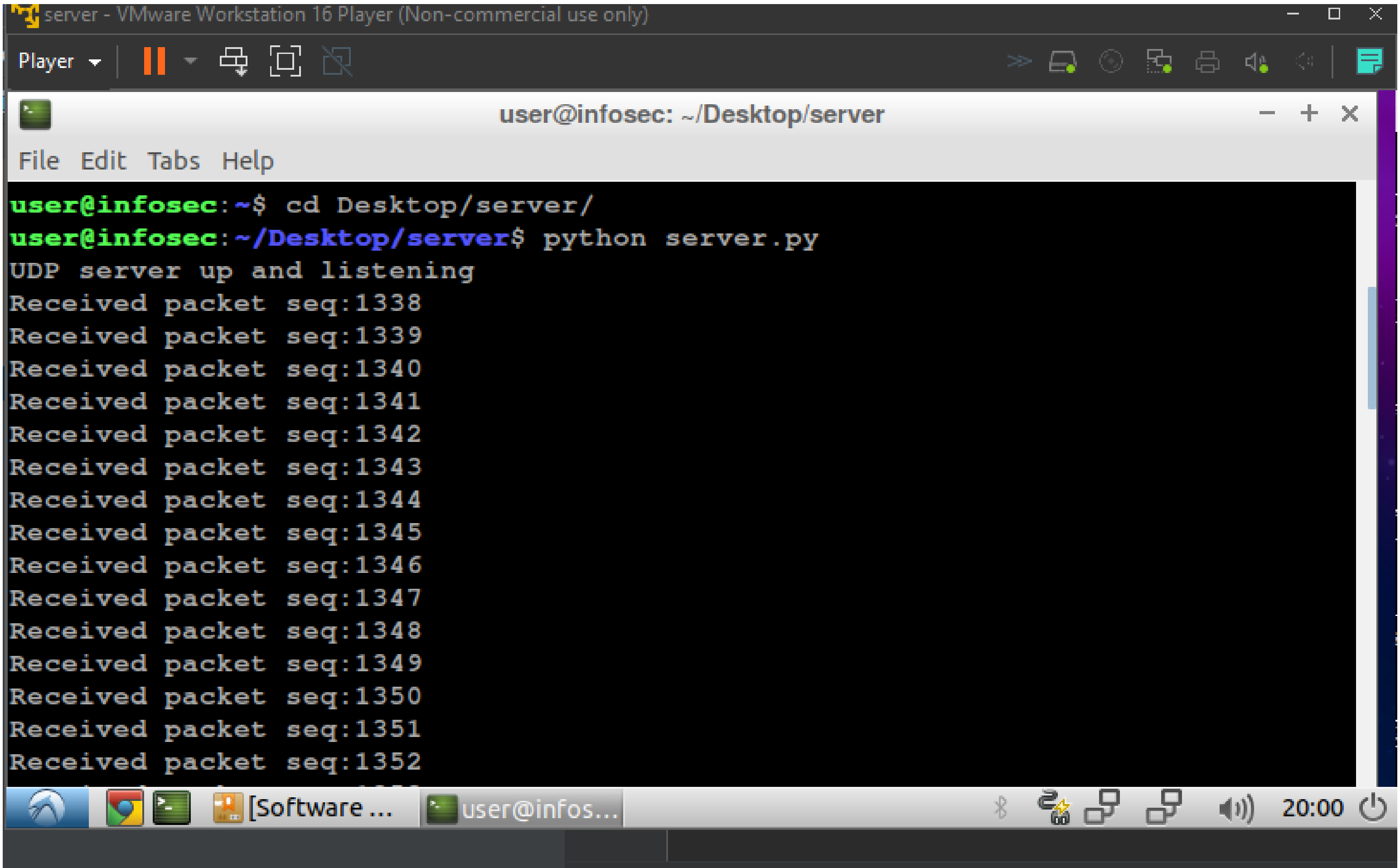
Server:

Prints the sequence number of received packet then responds with ACK number.

At the end when all chunks received - server calculates checksum from all 33 chunks then compare with the client's one. Finally closes the connection then printing packets info.

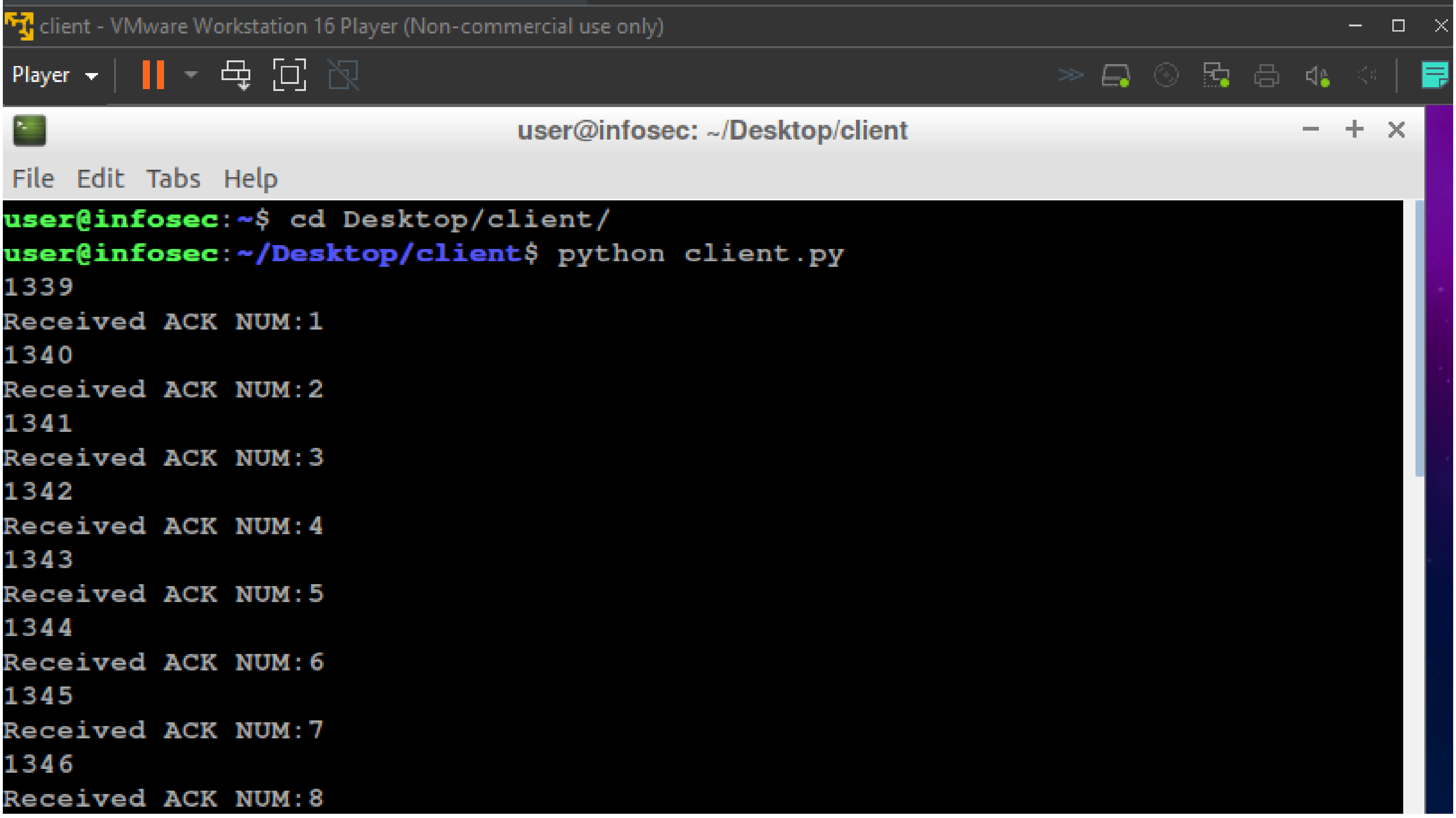
Client:

Dividing the message into chunks, sending them one by one. At the end when server received everything connection closed.



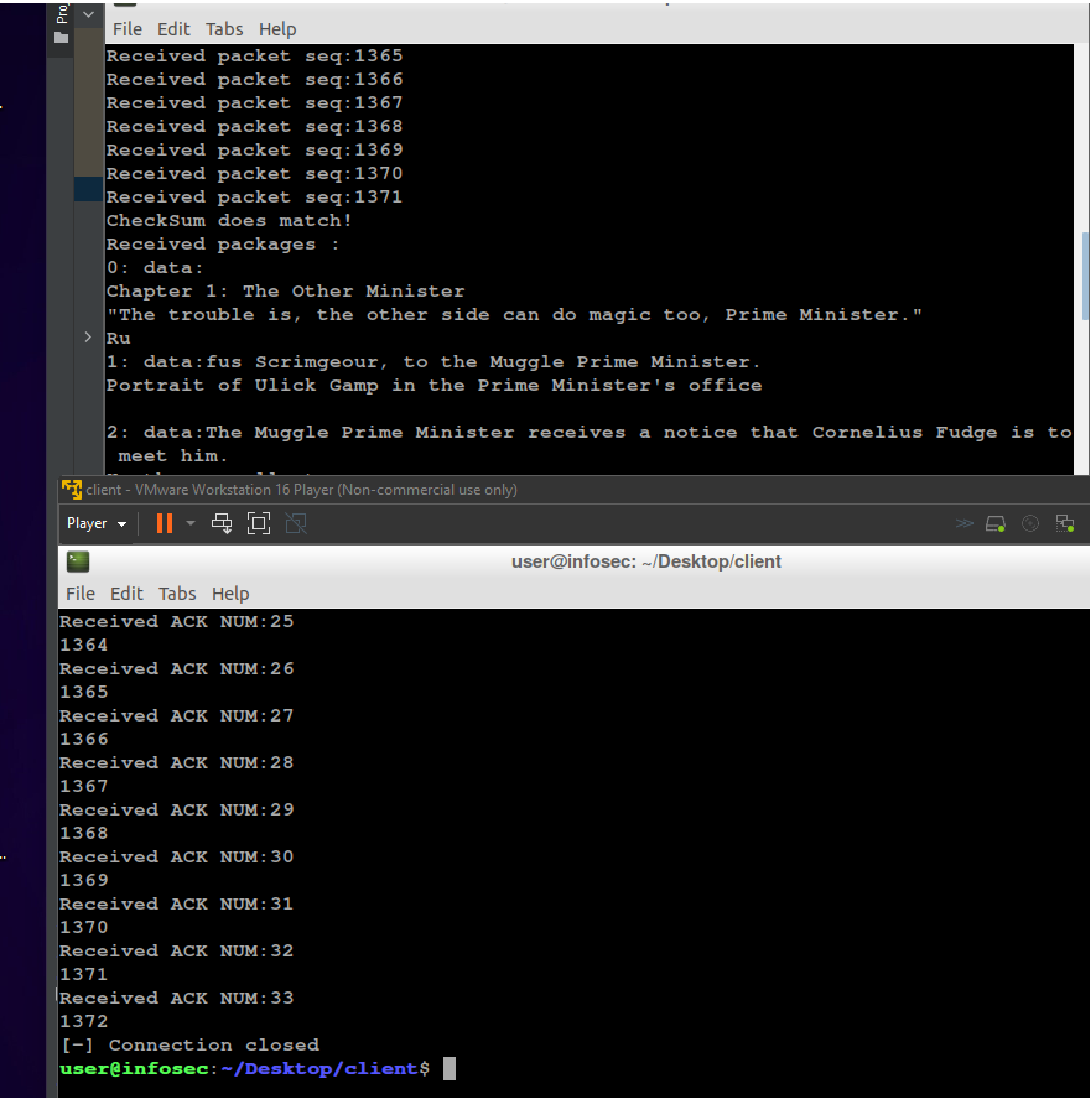
server - VMware Workstation 16 Player (Non-commercial use only)
Player
user@infosec: ~/Desktop/server
File Edit Tabs Help
[Software ...
user@infos...
20:00

```
user@infosec:~$ cd Desktop/server/
user@infosec:~/Desktop/server$ python server.py
UDP server up and listening
Received packet seq:1338
Received packet seq:1339
Received packet seq:1340
Received packet seq:1341
Received packet seq:1342
Received packet seq:1343
Received packet seq:1344
Received packet seq:1345
Received packet seq:1346
Received packet seq:1347
Received packet seq:1348
Received packet seq:1349
Received packet seq:1350
Received packet seq:1351
Received packet seq:1352
```



client - VMware Workstation 16 Player (Non-commercial use only)
Player
user@infosec: ~/Desktop/client
File Edit Tabs Help

```
user@infosec:~$ cd Desktop/client/
user@infosec:~/Desktop/client$ python client.py
1339
Received ACK NUM:1
1340
Received ACK NUM:2
1341
Received ACK NUM:3
1342
Received ACK NUM:4
1343
Received ACK NUM:5
1344
Received ACK NUM:6
1345
Received ACK NUM:7
1346
Received ACK NUM:8
```



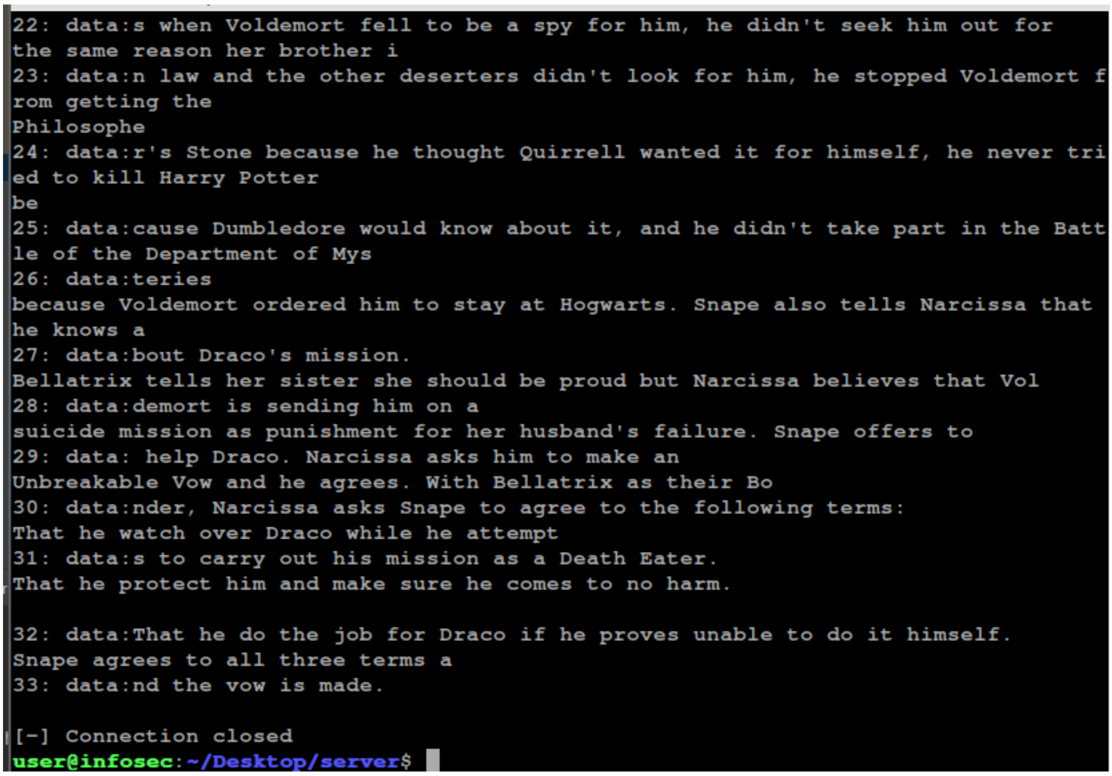
File Edit Tabs Help
client - VMware Workstation 16 Player (Non-commercial use only)
Player
user@infosec: ~/Desktop/client
File Edit Tabs Help

```
Received packet seq:1365
Received packet seq:1366
Received packet seq:1367
Received packet seq:1368
Received packet seq:1369
Received packet seq:1370
Received packet seq:1371
CheckSum does match!
Received packages :
0: data:
Chapter 1: The Other Minister
"The trouble is, the other side can do magic too, Prime Minister."
Ru
1: data:fus Scrimgeour, to the Muggle Prime Minister.
Portrait of Ulick Gamp in the Prime Minister's office

2: data:The Muggle Prime Minister receives a notice that Cornelius Fudge is to
 meet him.
```

```
Received ACK NUM:25
1364
Received ACK NUM:26
1365
Received ACK NUM:27
1366
Received ACK NUM:28
1367
Received ACK NUM:29
1368
Received ACK NUM:30
1369
Received ACK NUM:31
1370
Received ACK NUM:32
1371
Received ACK NUM:33
1372
[-] Connection closed
user@infosec:~/Desktop/client$
```

Server



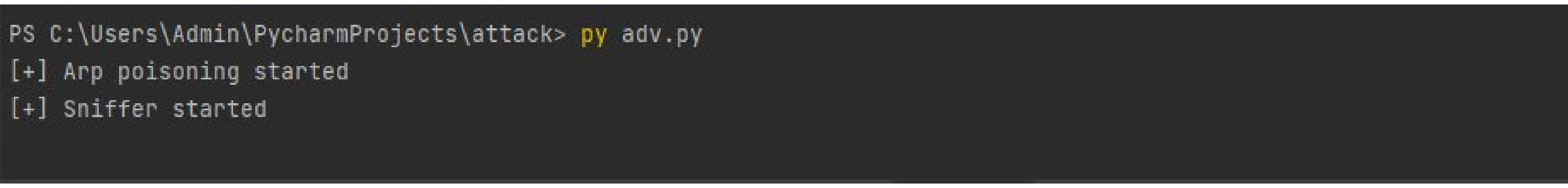
```
22: data:s when Voldemort fell to be a spy for him, he didn't seek him out for
the same reason her brother i
23: data:n law and the other deserters didn't look for him, he stopped Voldemort f
rom getting the
Philosophe
24: data:r's Stone because he thought Quirrell wanted it for himself, he never tri
ed to kill Harry Potter
be
25: data:cause Dumbledore would know about it, and he didn't take part in the Batt
le of the Department of Mys
26: data:teries
because Voldemort ordered him to stay at Hogwarts. Snape also tells Narcissa that
he knows a
27: data:bout Draco's mission.
Bellatrix tells her sister she should be proud but Narcissa believes that Vol
28: data:demort is sending him on a
suicide mission as punishment for her husband's failure. Snape offers to
29: data: help Draco. Narcissa asks him to make an
Unbreakable Vow and he agrees. With Bellatrix as their Bo
30: data:nder, Narcissa asks Snape to agree to the following terms:
That he watch over Draco while he attempt
31: data:s to carry out his mission as a Death Eater.
That he protect him and make sure he comes to no harm.

32: data:That he do the job for Draco if he proves unable to do it himself.
Snape agrees to all three terms a
33: data:nd the vow is made.

[-] Connection closed
user@infosec:~/Desktop/server$ 
```

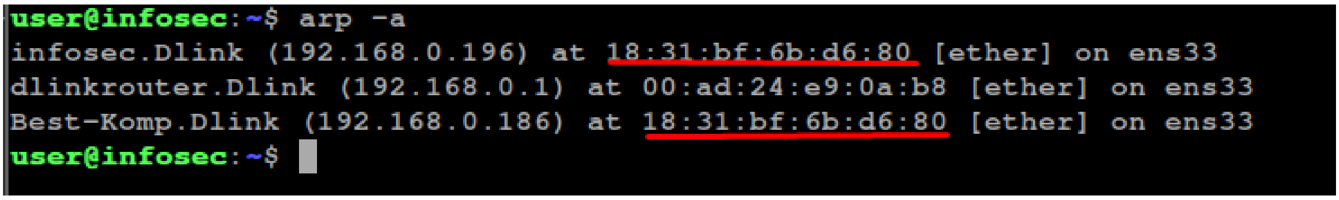
Client & Server communications with MiTM:

Adversary launched the script:



```
PS C:\Users\Admin\PycharmProjects\attack> py adv.py
[+] Arp poisoning started
[+] Sniffer started
```

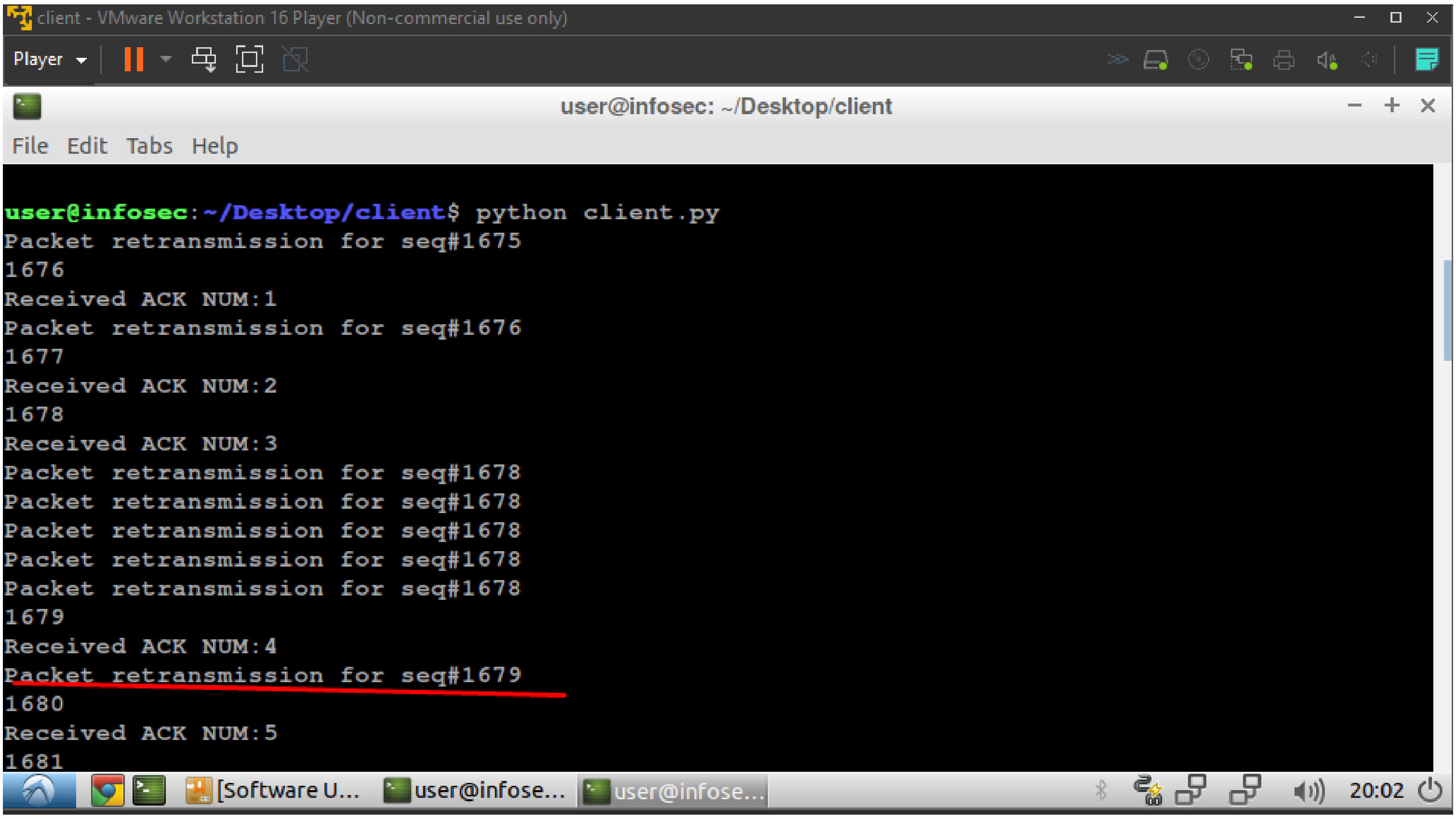
Client's arp table after:



```
user@infosec:~$ arp -a
infosec.Dlink (192.168.0.196) at 18:31:bf:6b:d6:80 [ether] on ens33
dlinkrouter.Dlink (192.168.0.1) at 00:ad:24:e9:0a:b8 [ether] on ens33
Best-Komp.Dlink (192.168.0.186) at 18:31:bf:6b:d6:80 [ether] on ens33
user@infosec:~$ 
```

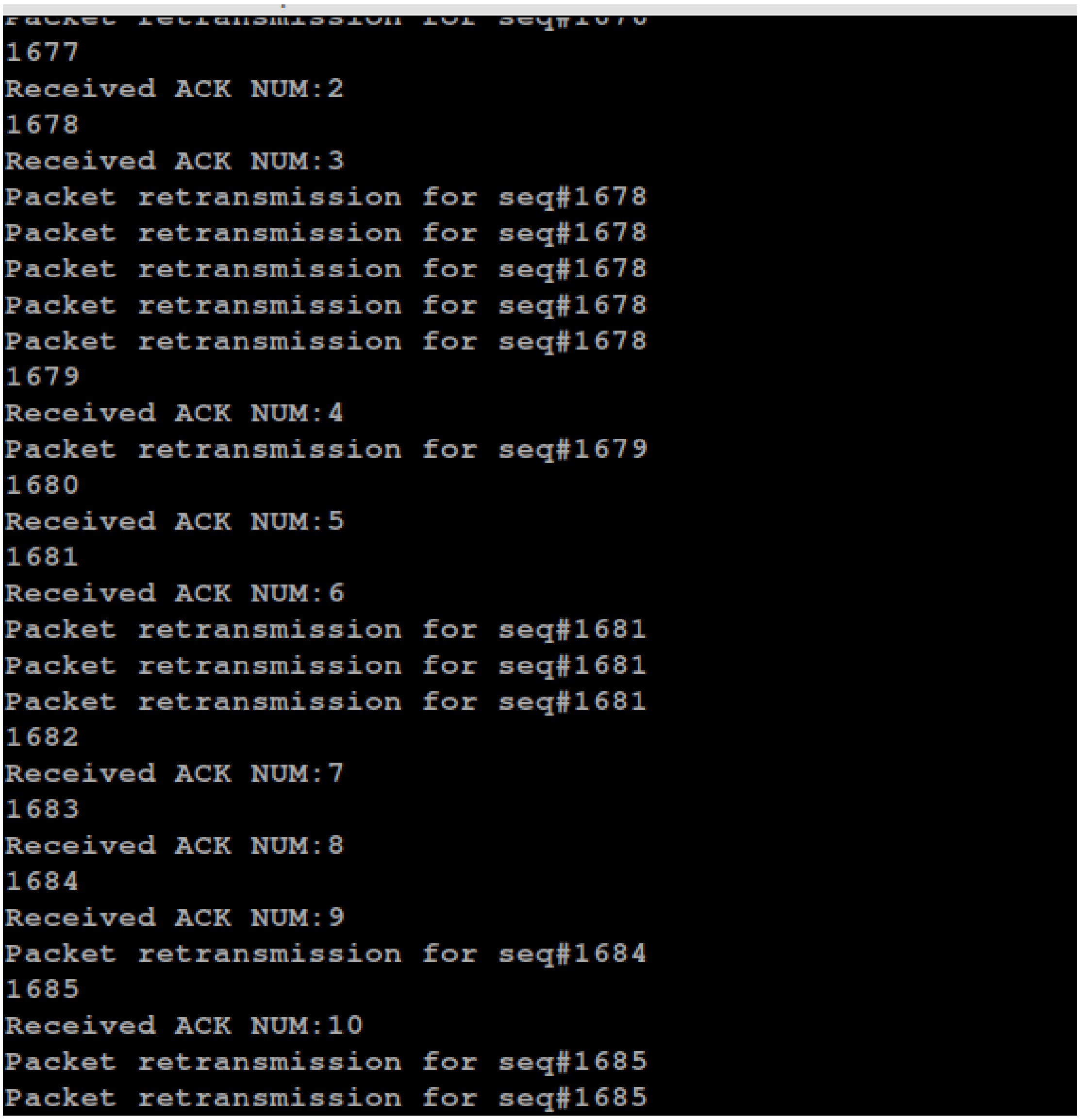
This time adversary dropping the packets so client making retransmissions, the rest behavior the same as regular communication so not every log screenshot included.

Client:



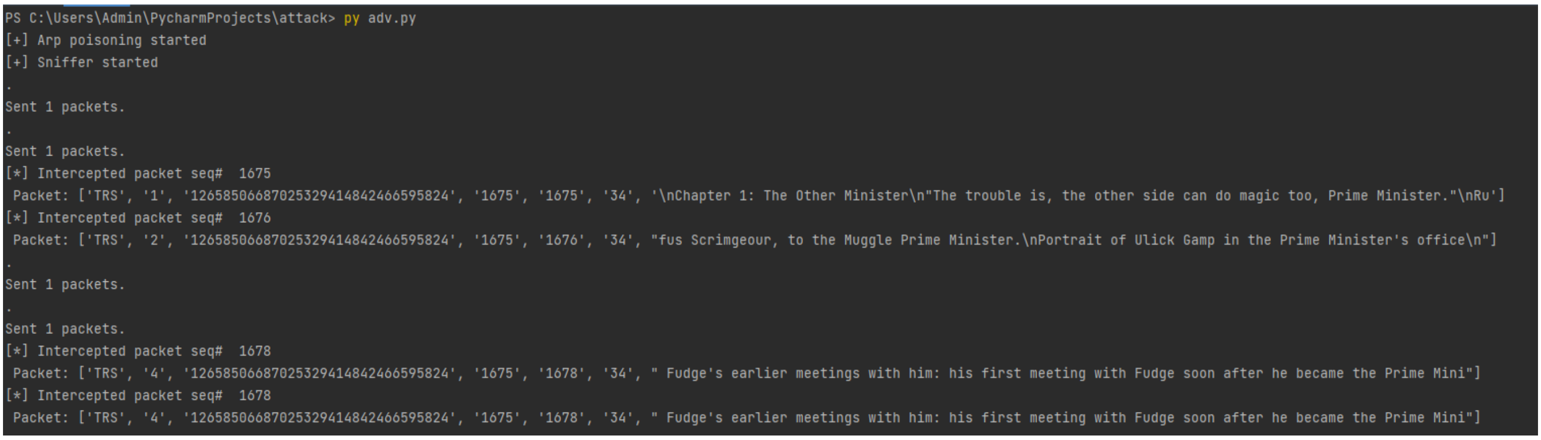
client - VMware Workstation 16 Player (Non-commercial use only)
Player
user@infosec: ~/Desktop/client
File Edit Tabs Help
[Software U...
user@infose...
user@infose...
20:02

```
user@infosec:~/Desktop/client$ python client.py
Packet retransmission for seq#1675
1676
Received ACK NUM:1
Packet retransmission for seq#1676
1677
Received ACK NUM:2
1678
Received ACK NUM:3
Packet retransmission for seq#1678
Packet retransmission for seq#1678
Packet retransmission for seq#1678
Packet retransmission for seq#1678
Packet retransmission for seq#1678
1679
Received ACK NUM:4
Packet retransmission for seq#1679
1680
Received ACK NUM:5
1681
```

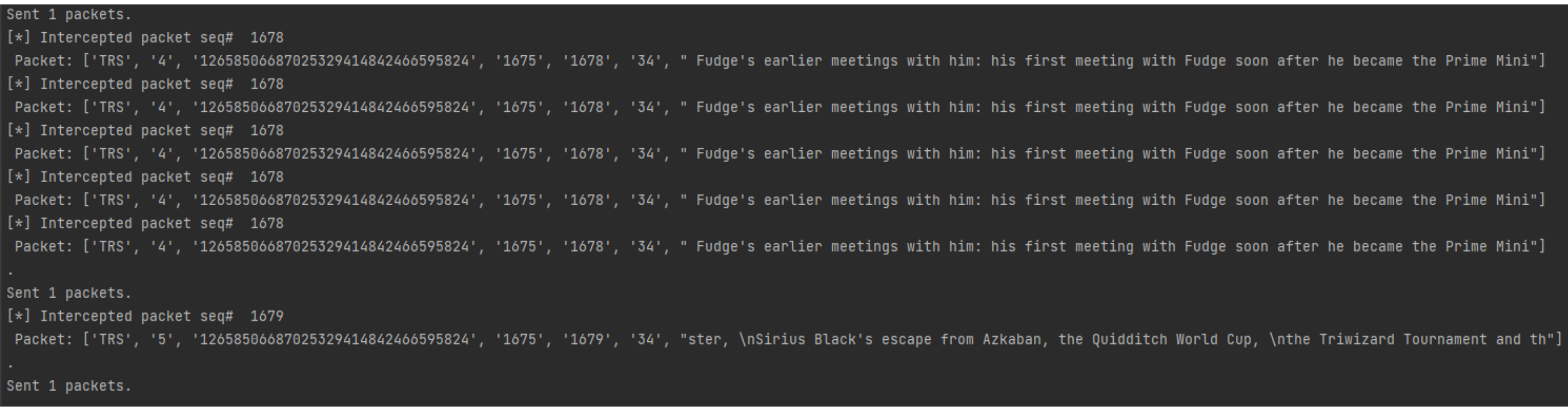


```
Packet retransmission for seq#1676
1677
Received ACK NUM:2
1678
Received ACK NUM:3
Packet retransmission for seq#1678
Packet retransmission for seq#1678
Packet retransmission for seq#1678
Packet retransmission for seq#1678
Packet retransmission for seq#1678
1679
Received ACK NUM:4
Packet retransmission for seq#1679
1680
Received ACK NUM:5
1681
Received ACK NUM:6
Packet retransmission for seq#1681
Packet retransmission for seq#1681
Packet retransmission for seq#1681
1682
Received ACK NUM:7
1683
Received ACK NUM:8
1684
Received ACK NUM:9
Packet retransmission for seq#1684
1685
Received ACK NUM:10
Packet retransmission for seq#1685
Packet retransmission for seq#1685
```

Adversary:

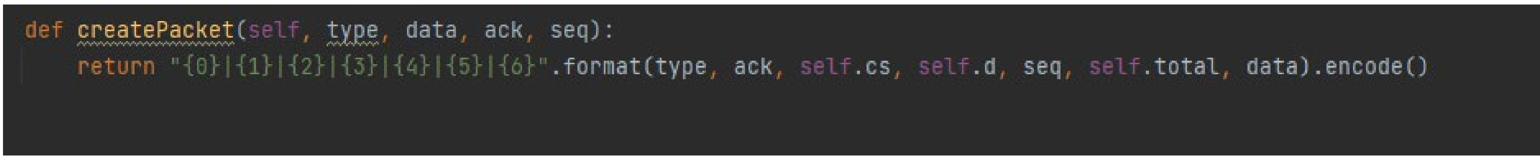


```
PS C:\Users\Admin\PycharmProjects\attack> py adv.py
[+] Arp poisoning started
[+] Sniffer started
.
Sent 1 packets.
.
Sent 1 packets.
[*] Intercepted packet seq#  1675
 Packet: ['TRS', '1', '12658506687025329414842466595824', '1675', '1675', '34', '\nChapter 1: The Other Minister\n"The trouble is, the other side can do magic too, Prime Minister."\nRu']
[*] Intercepted packet seq#  1676
 Packet: ['TRS', '2', '12658506687025329414842466595824', '1675', '1676', '34', "fus Scrimgeour, to the Muggle Prime Minister.\nPortrait of Ulick Gamp in the Prime Minister's office\n"]
.
Sent 1 packets.
.
Sent 1 packets.
[*] Intercepted packet seq#  1678
 Packet: ['TRS', '4', '12658506687025329414842466595824', '1675', '1678', '34', " Fudge's earlier meetings with him: his first meeting with Fudge soon after he became the Prime Mini"]
[*] Intercepted packet seq#  1678
 Packet: ['TRS', '4', '12658506687025329414842466595824', '1675', '1678', '34', " Fudge's earlier meetings with him: his first meeting with Fudge soon after he became the Prime Mini"]
```



```
Sent 1 packets.
[*] Intercepted packet seq#  1678
 Packet: ['TRS', '4', '126585066870253294148424665958 24', '1675', '1678', '34', " Fudge's earlier meetings with him: his first meeting with Fudge soon after he became the Prime Mini"]
[*] Intercepted packet seq#  1678
 Packet: ['TRS', '4', '12658506687025329414842466595824', '1675', '1678', '34', " Fudge's earlier meetings with him: his first meeting with Fudge soon after he became the Prime Mini"]
[*] Intercepted packet seq#  1678
 Packet: ['TRS', '4', '12658506687025329414842466595824', '1675', '1678', '34', " Fudge's earlier meetings with him: his first meeting with Fudge soon after he became the Prime Mini"]
[*] Intercepted packet seq#  1678
 Packet: ['TRS', '4', '12658506687025329414842466595824', '1675', '1678', '34', " Fudge's earlier meetings with him: his first meeting with Fudge soon after he became the Prime Mini"]
[*] Intercepted packet seq#  1678
 Packet: ['TRS', '4', '12658506687025329414842466595824', '1675', '1678', '34', " Fudge's earlier meetings with him: his first meeting with Fudge soon after he became the Prime Mini"]
.
Sent 1 packets.
[*] Intercepted packet seq#  1679
 Packet: ['TRS', '5', '12658506687025329414842466595824', '1675', '1679', '34', "ster, \nSirius Black's escape from Azkaban, the Quidditch World Cup, \nthe Triwizard Tournament and th"]
.
Sent 1 packets.
```

We can see here that adversary printing info about dropped packet, to understand the header lets see the header constructor:



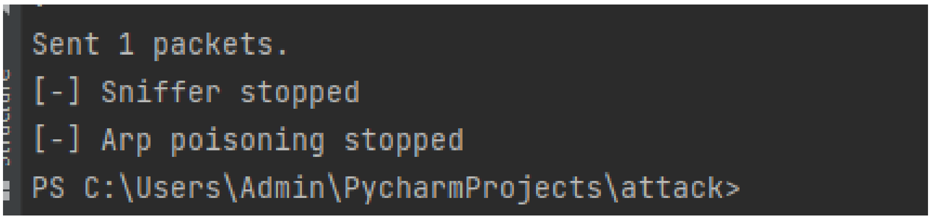
```
def createPacket(self, type, data, ack, seq):
    return "{0}|{1}|{2}|{3}|{4}|{5}|{6}".format(type, ack, self.cs, self.d, seq, self.total, data).encode()
```

So the header looks like:

Packet Type | ACK#| Checksum | d| Seq# | Total packets expected | Data

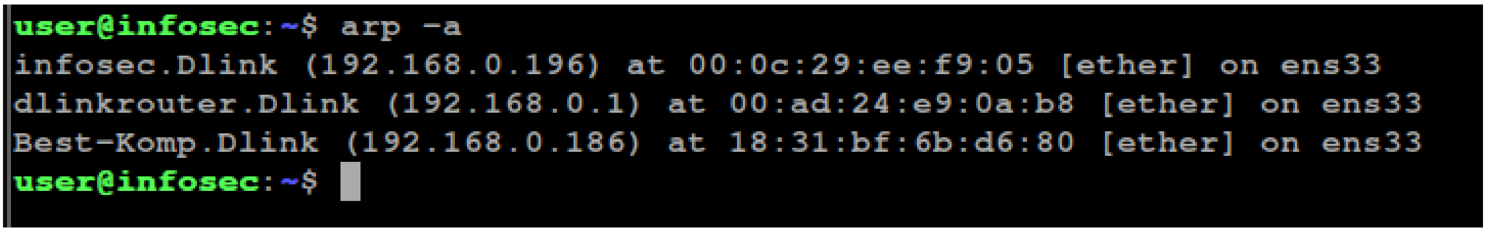
As we can see the same packet that adversary dropped , client retransmitted.

Adversary stopped the script (Cntrl + C)



```
Sent 1 packets.
[-] Sniffer stopped
[-] Arp poisoning stopped
PS C:\Users\Admin\PycharmProjects\attack>
```

Clients arp table is not poisoned anymore



```
user@infosec:~$ arp -a
infosec.Dlink (192.168.0.196) at 00:0c:29:ee:f9:05 [ether] on ens33
dlinkrouter.Dlink (192.168.0.1) at 00:ad:24:e9:0a:b8 [ether] on ens33
Best-Komp.Dlink (192.168.0.186) at 18:31:bf:6b:d6:80 [ether] on ens33
user@infosec:~$
```