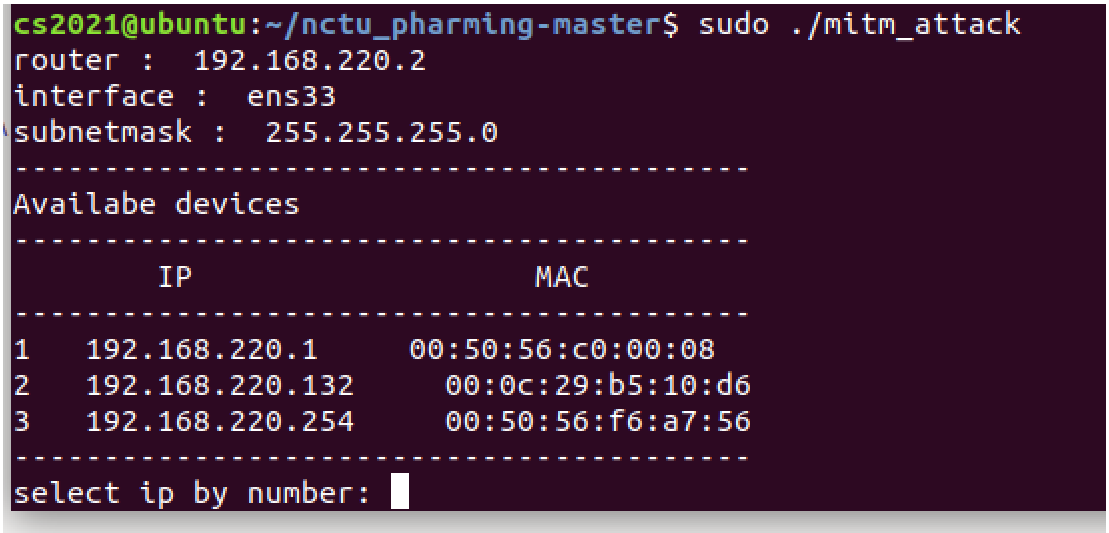
Item 1:please give evidence that you have finished the MITM attack

Scenario2

Task I:

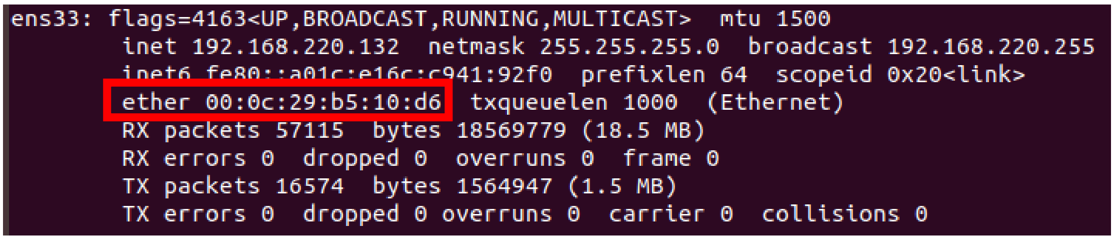
Device Address Information Collection



```
cs2021@ubuntu:~/nctu_pharming-master$ sudo ./mitm_attack
router :  192.168.220.2
interface :  ens33
subnetmask :  255.255.255.0
-----------------------------------------
Availabe devices
-----------------------------------------
        IP                     MAC
-----------------------------------------
1   192.168.220.1      00:50:56:c0:00:08
2   192.168.220.132      00:0c:29:b5:10:d6
3   192.168.220.254      00:50:56:f6:a7:56
-----------------------------------------
select ip by number: 
```

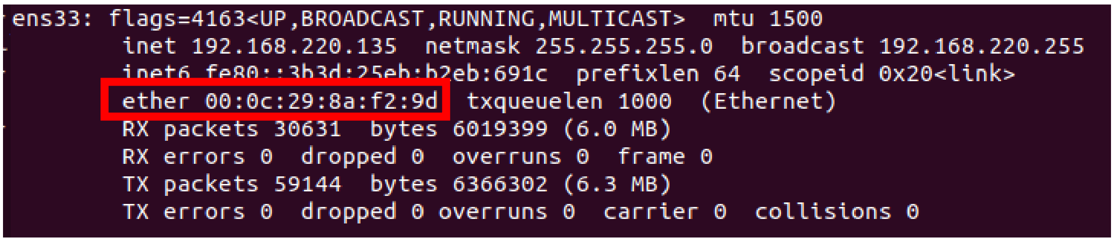
Task II: ARP Spoofing

Victim



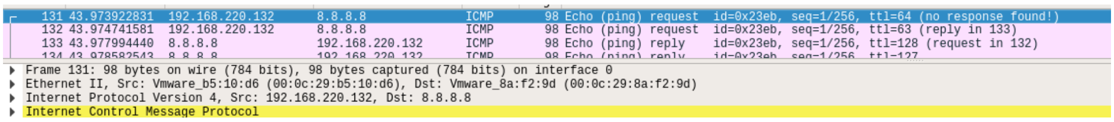
```
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.220.132  netmask 255.255.255.0  broadcast 192.168.220.255
        inet6 fe80::a01c:e16c:c941:92f0  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:b5:10:d6  txqueuelen 1000  (Ethernet)
        RX packets 57115  bytes 18569779 (18.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16574  bytes 1564947 (1.5 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Attacker



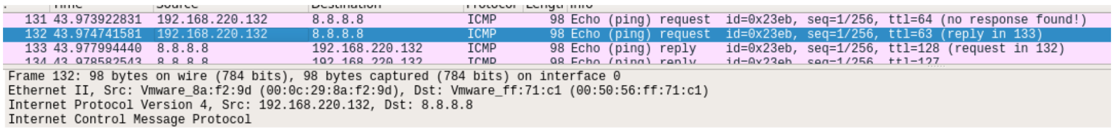
```
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.220.135  netmask 255.255.255.0  broadcast 192.168.220.255
        inet6 fe80::3b3d:25eb:b2eb:691c  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:8a:f2:9d  txqueuelen 1000  (Ethernet)
        RX packets 30631  bytes 6019399 (6.0 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 59144  bytes 6366302 (6.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Victim->Attacker



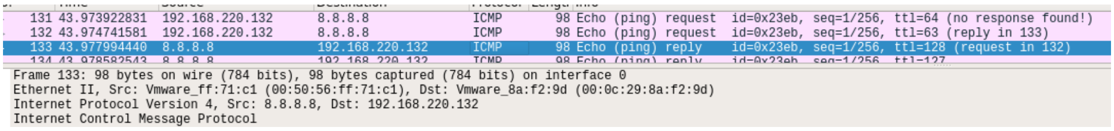
```
131 43.973922831  192.168.220.132  8.8.8.8          ICMP   98 Echo (ping) request  id=0x23eb, seq=1/256, ttl=64 (no response found!)
132 43.974741581  192.168.220.132  8.8.8.8          ICMP   98 Echo (ping) request  id=0x23eb, seq=1/256, ttl=63 (reply in 133)
133 43.977994440  8.8.8.8          192.168.220.132  ICMP   98 Echo (ping) reply    id=0x23eb, seq=1/256, ttl=128 (request in 132)
134 43.978582543  8.8.8.8          192.168.220.132  ICMP   98 Echo (ping) reply    id=0x23eb, seq=1/256, ttl=127
▸ Frame 131: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▸ Ethernet II, Src: Vmware_b5:10:d6 (00:0c:29:b5:10:d6), Dst: Vmware_8a:f2:9d (00:0c:29:8a:f2:9d)
▸ Internet Protocol Version 4, Src: 192.168.220.132, Dst: 8.8.8.8
▸ Internet Control Message Protocol
```

Attacker->AP



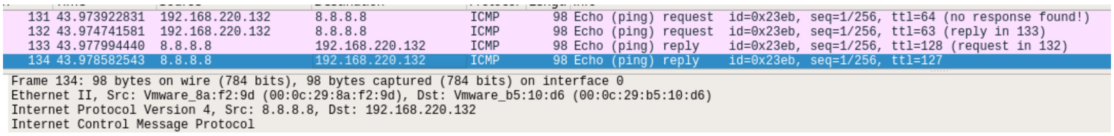
```
    Time          Source           Destination      Protocol Length Info
131 43.973922831  192.168.220.132  8.8.8.8          ICMP     98 Echo (ping) request  id=0x23eb, seq=1/256, ttl=64 (no response found!)
132 43.974741581  192.168.220.132  8.8.8.8          ICMP     98 Echo (ping) request  id=0x23eb, seq=1/256, ttl=63 (reply in 133)
133 43.977994440  8.8.8.8          192.168.220.132  ICMP     98 Echo (ping) reply    id=0x23eb, seq=1/256, ttl=128 (request in 132)
134 43.978582543  8.8.8.8          192.168.220.132  ICMP     98 Echo (ping) reply    id=0x23eb, seq=1/256, ttl=127
Frame 132: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: Vmware_8a:f2:9d (00:0c:29:8a:f2:9d), Dst: Vmware_ff:71:c1 (00:50:56:ff:71:c1)
Internet Protocol Version 4, Src: 192.168.220.132, Dst: 8.8.8.8
Internet Control Message Protocol
```

AP->Attacker



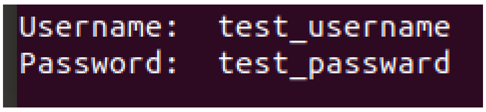
```
 131 43.973922831  192.168.220.132   8.8.8.8           ICMP      98 Echo (ping) request  id=0x23eb, seq=1/256, ttl=64 (no response found!)
 132 43.974741581  192.168.220.132   8.8.8.8           ICMP      98 Echo (ping) request  id=0x23eb, seq=1/256, ttl=63 (reply in 133)
 133 43.977994440  8.8.8.8           192.168.220.132   ICMP      98 Echo (ping) reply    id=0x23eb, seq=1/256, ttl=128 (request in 132)
 134 43.978582543  8.8.8.8           192.168.220.132   ICMP      98 Echo (ping) reply    id=0x23eb, seq=1/256, ttl=127
Frame 133: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: Vmware_ff:71:c1 (00:50:56:ff:71:c1), Dst: Vmware_8a:f2:9d (00:0c:29:8a:f2:9d)
Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.220.132
Internet Control Message Protocol
```

Attacker->Victim



```
 131 43.973922831  192.168.220.132   8.8.8.8           ICMP      98 Echo (ping) request  id=0x23eb, seq=1/256, ttl=64 (no response found!)
 132 43.974741581  192.168.220.132   8.8.8.8           ICMP      98 Echo (ping) request  id=0x23eb, seq=1/256, ttl=63 (reply in 133)
 133 43.977994440  8.8.8.8           192.168.220.132   ICMP      98 Echo (ping) reply    id=0x23eb, seq=1/256, ttl=128 (request in 132)
 134 43.978582543  8.8.8.8           192.168.220.132   ICMP      98 Echo (ping) reply    id=0x23eb, seq=1/256, ttl=127
Frame 134: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: Vmware_8a:f2:9d (00:0c:29:8a:f2:9d), Dst: Vmware_b5:10:d6 (00:0c:29:b5:10:d6)
Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.220.132
Internet Control Message Protocol
```

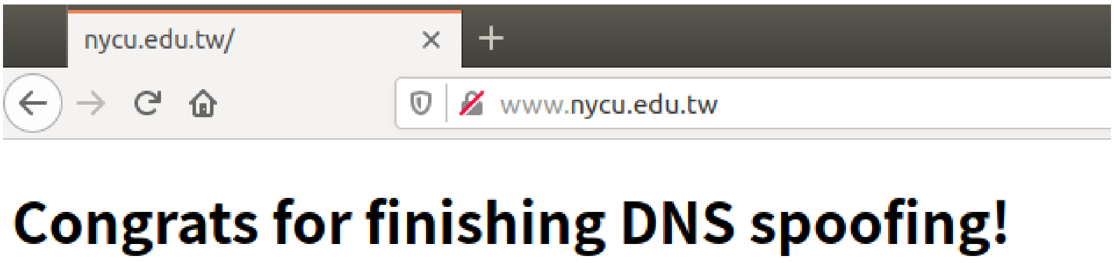
Task III:SSL Split on Encrypted SSL/TLS Connections



```
Username:  test_username
Password:  test_passward
```

Item 2 : please give evidence that you have finished the pharming attack

Scenario2



Congrats for finishing DNS spoofing!

Item 3 (10%): please propose a solution that can defend against the ARP spoofing attack

Ans:

1. Use static ARP: The ARP protocol lets us define a static ARP entry for an IP address, and prevent devices from listening on ARP responses for that address. For example, if a workstation always connects to the same router, we can define a static ARP entry for that router, preventing an attack.
2. Use packet filtering: Packet filtering solutions can identify poisoned ARP packets by seeing that they contain conflicting source information, and stop them before reaching devices on our network.

3. Use VPN: VPN allows devices to connect to the Internet through an encrypted tunnel. This makes all communication encrypted, and worthless for the ARP spoofing attacker.