ARP SPOOF POISONING

SUBJECT NAME: Cryptography and Network Security
SUBJECT CODE: CS6008
MODULE: 04

NAME: R.Aadharsh
REG.NO.: 2019103604
DATE: 06/06/2022

AIM:

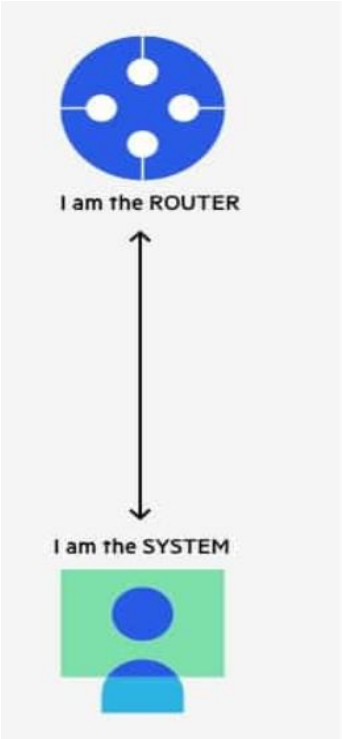
Using arpspoof to poison network and detect using Wireshark

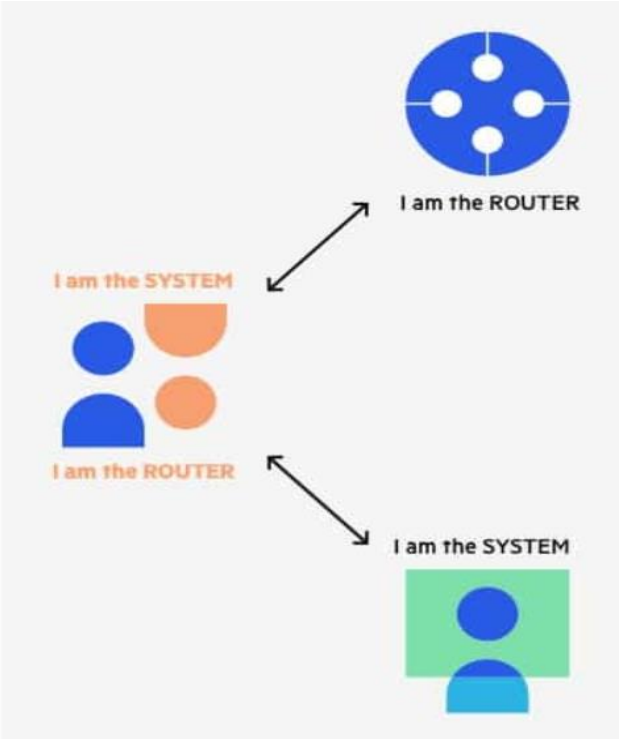
TOOLS INVOLVED:

ETTERCAP
VISUAL STUDIO CODE
KALI LINUX TERMINAL (WSL)
WINDOWS (OPERATION SYSTEM)

PROBLEM DESCRIPTION:

Address Resolution Protocol (ARP) is a protocol that enables network communications to reach a specific device on the network. ARP translates Internet Protocol (IP) addresses to a Media Access Control (MAC) address, and vice versa. Most commonly, devices use ARP to contact the router or gateway that enables them to connect to the Internet.





Once the attacker succeeds in an ARP spoofing attack, they can:

Continue routing the communications as-is—the attacker can sniff the packets and steal data, except if it is transferred over an encrypted channel like HTTPS.

Perform session hijacking—if the attacker obtains a session ID, they can gain access to accounts the user is currently logged into.

Alter communication—for example pushing a malicious file or website to the workstation.

Distributed Denial of Service (DDoS)—the attackers can provide the MAC address of a server they wish to attack with DDoS, instead of their own machine. If they do this for a large number of IPs, the target server will be bombarded with traffic.

Having a Kali linux box and a windows 10 machine(Target Machine). We are going to intercept the traffic entering and exiting the windows 10 machine by using ARC poisoning attack and Man in the middle attack from the kali linux machine. Here both the machines are guest virtual machines but this attack is

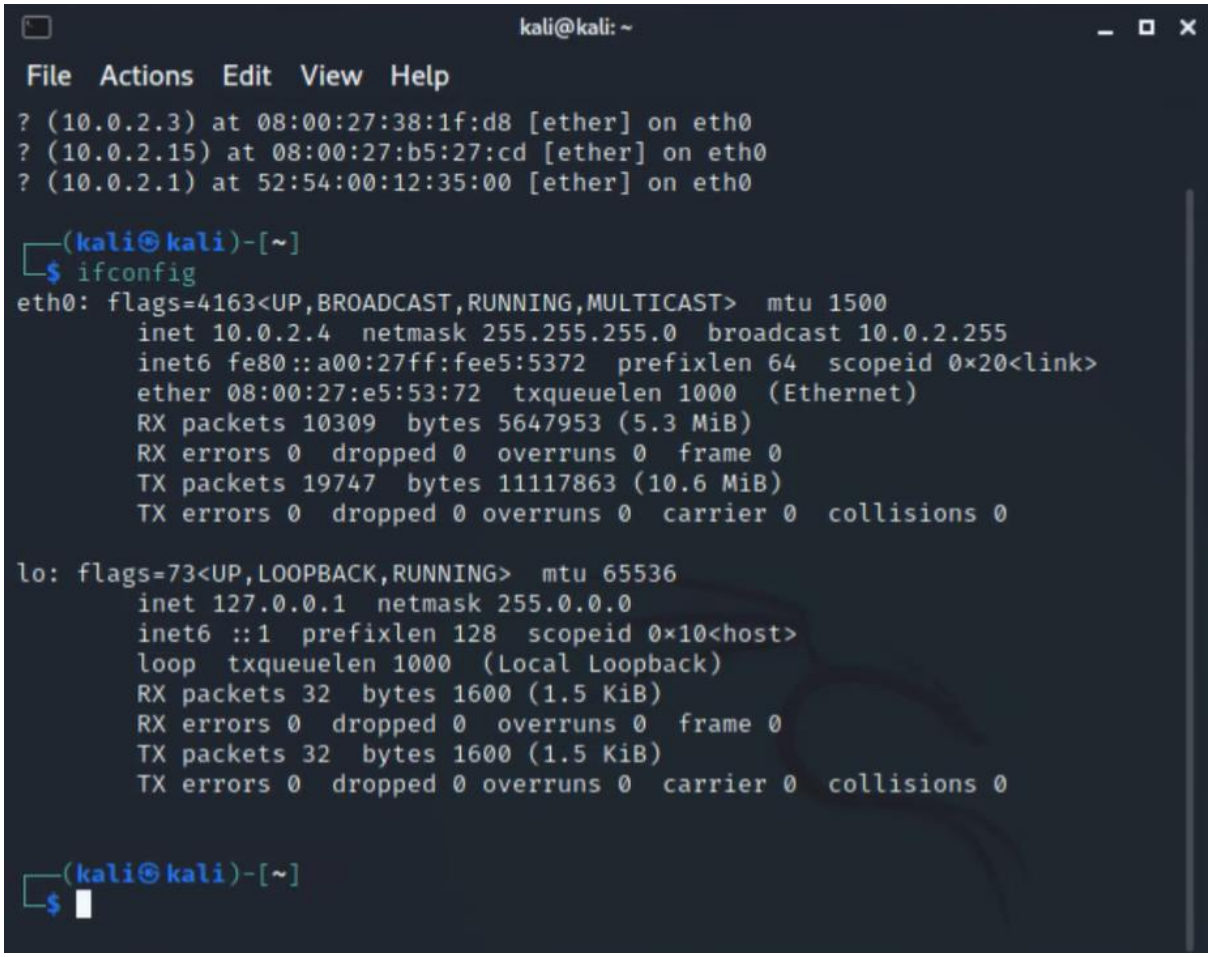
performed in cable connected machines similarly also.

OUTPUT:

Intercepting the traffic entering and exiting the machine using ARP poisioning attack.

SCREENSHOTS:

Kali Linux machine:



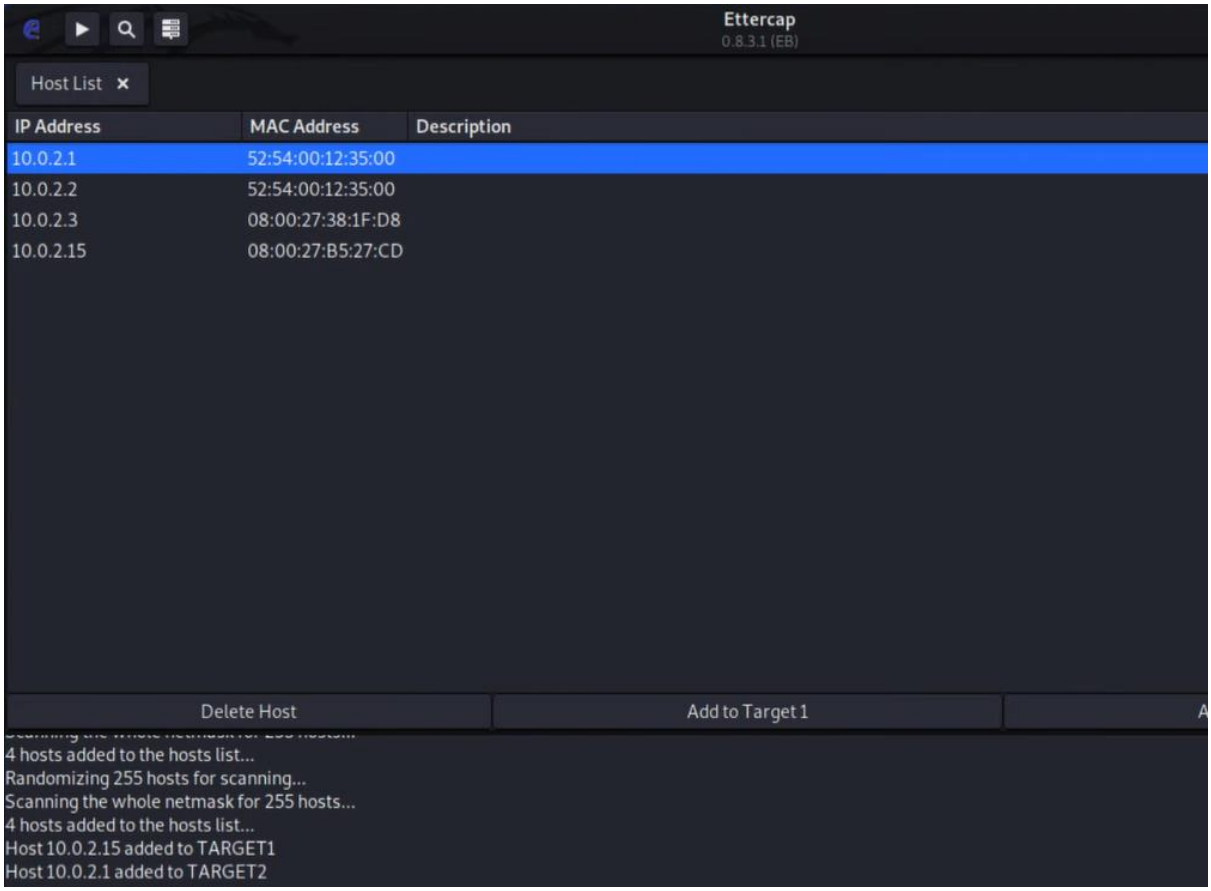
Windows 10 Machine:

```
Command Prompt
(c) Microsoft Corporation. All rights reserved.

C:\Users\tyler>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::74d1:898d:cee3:2748%6
   IPv4 Address. . . . . . . . . . . : 10.0.2.15
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.1

C:\Users\tyler>arp -a

Interface: 10.0.2.15 --- 0x6
  Internet Address      Physical Address      Type
  10.0.2.1              52-54-00-12-35-00     dynamic
  10.0.2.3              08-00-27-38-1f-d8     dynamic
  10.0.2.4              08-00-27-e5-53-72     dynamic
  10.0.2.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

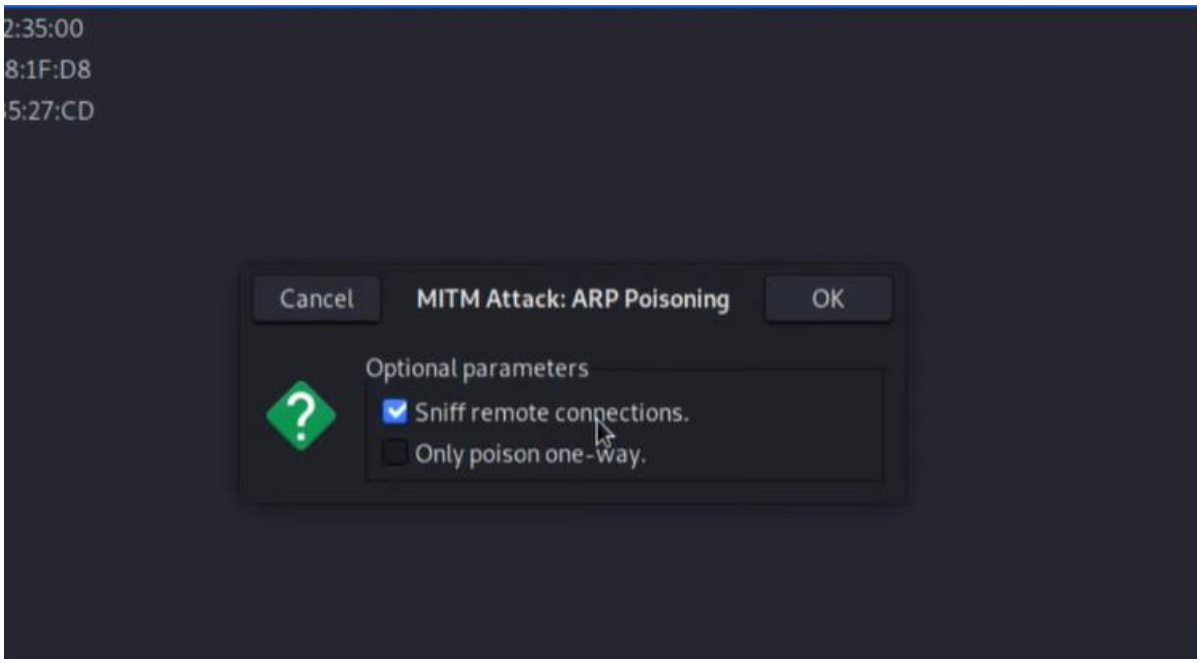
Using Ettercap tool to perform ARP poisoning.And before that forwarding traffic to gateway and start wireshark to know how the attack changes.

```
┌──(kali㉿kali)-[~]
└─$ sysctl net.ipv4.ip_forward=1
```

In Ettercap , search for the available machine Ips
The search creates a bunch of ARPs and they send signals to the machines to find out the machines that respond to it to find out the active systems.
After finding out the machines, we set out targets



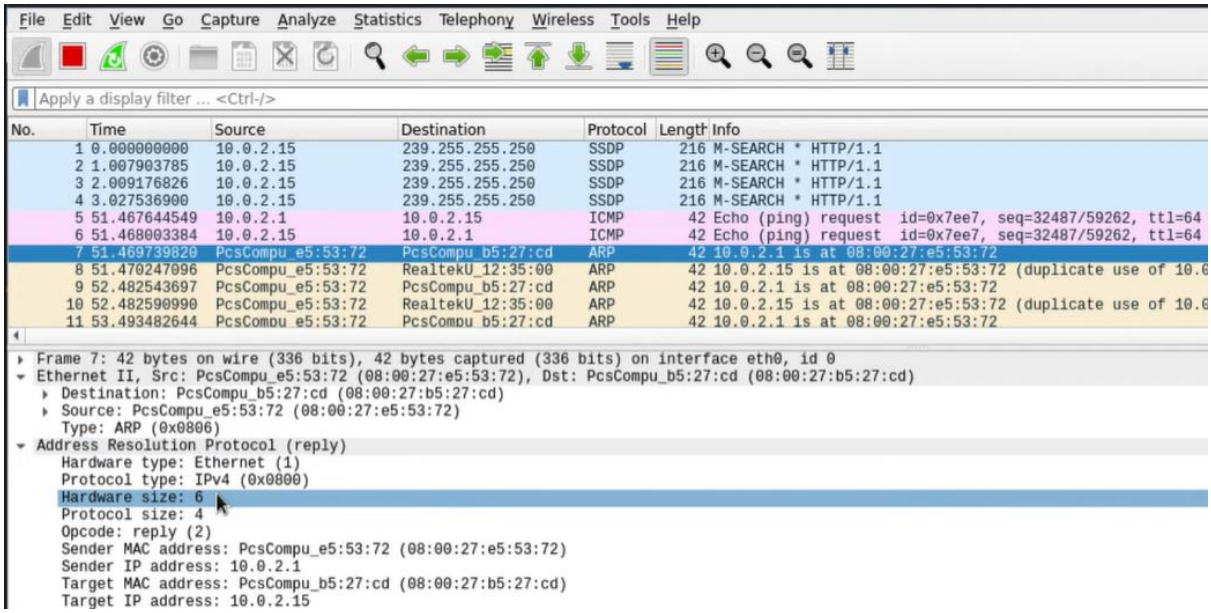
Initiating the ARP poisioning attack



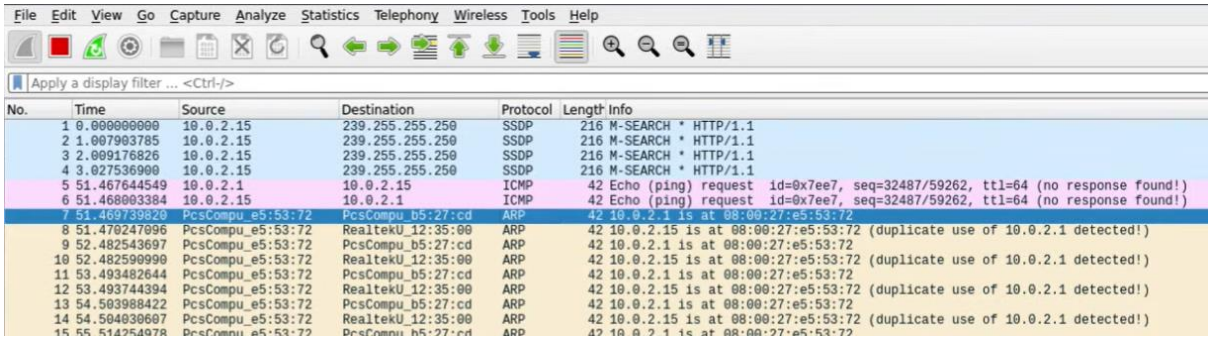
Now its attacked so the windows thinks that the Ettercap box is the gateway

```
Interface: 10.0.2.15 --- 0x6
  Internet Address      Physical Address      Type
  10.0.2.1              08-00-27-e5-53-72     dynamic
  10.0.2.3              08-00-27-38-1f-d      dynamic
  10.0.2.4              08-00-27-e5-53-72     dynamic
  10.0.2.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

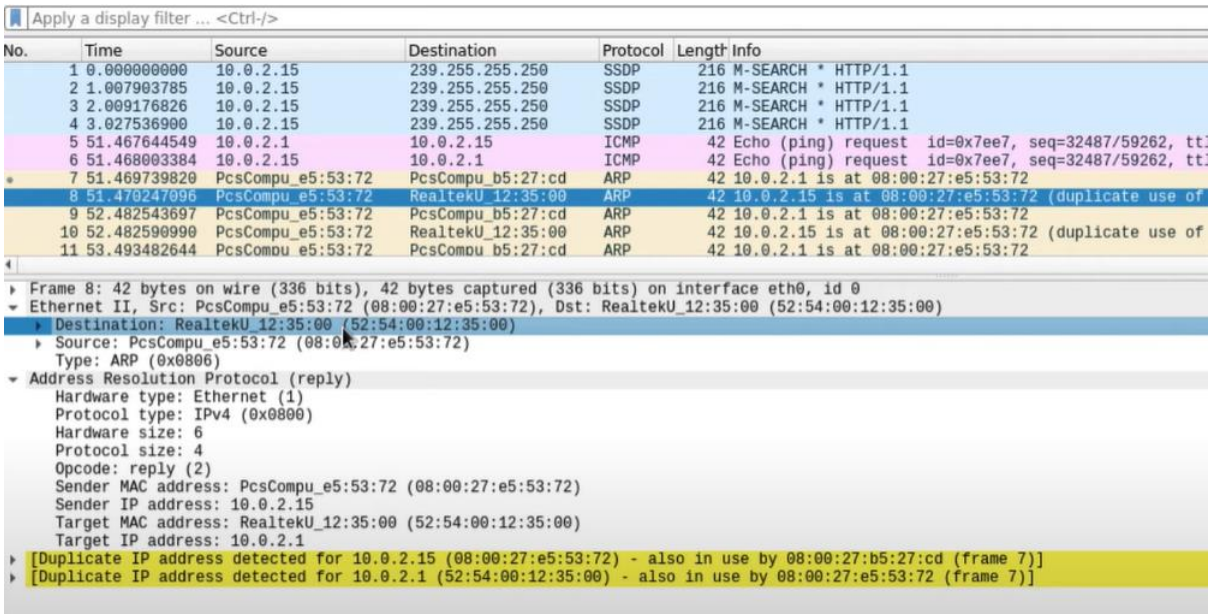
Checking the packets in wireshark

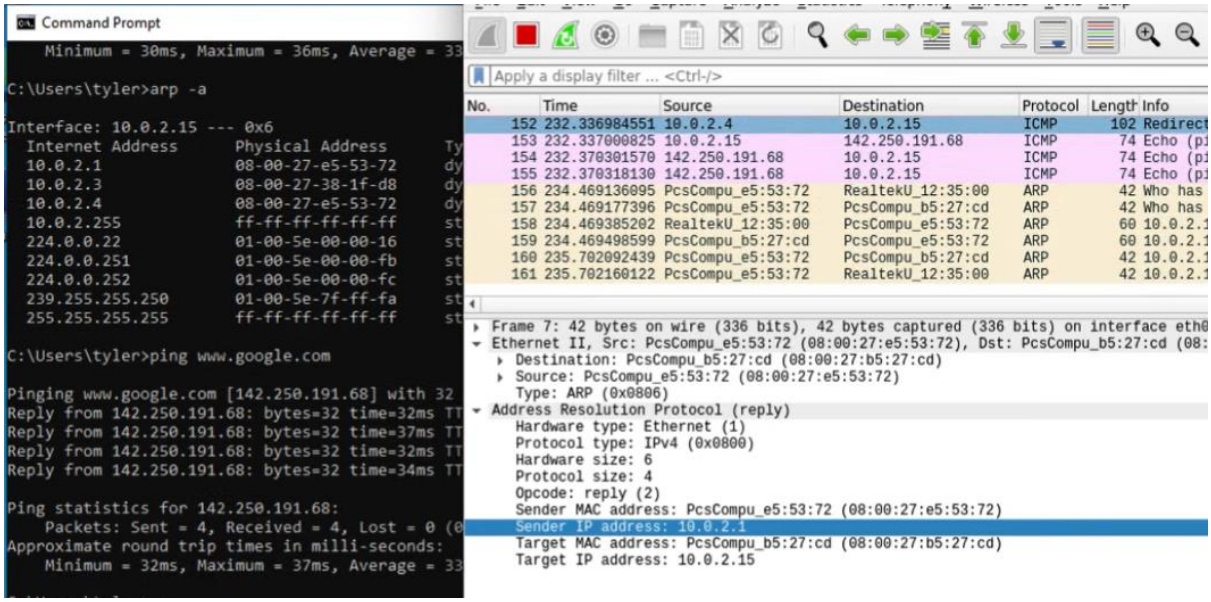


Here the Ettercap machine pretends to be the kali linux to the windows machine and as the windows machine to the kali linux box. So basically it impersonates the sender and the receiver and performs the man in the middle attack .



Here wireshark finds out duplicates also.

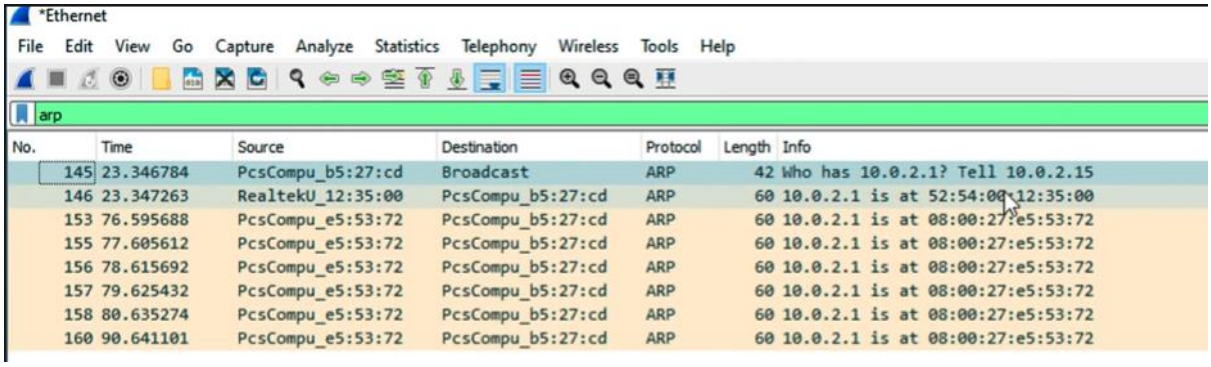




Packets being transferred from sender to man in the middle and then to the receiver.

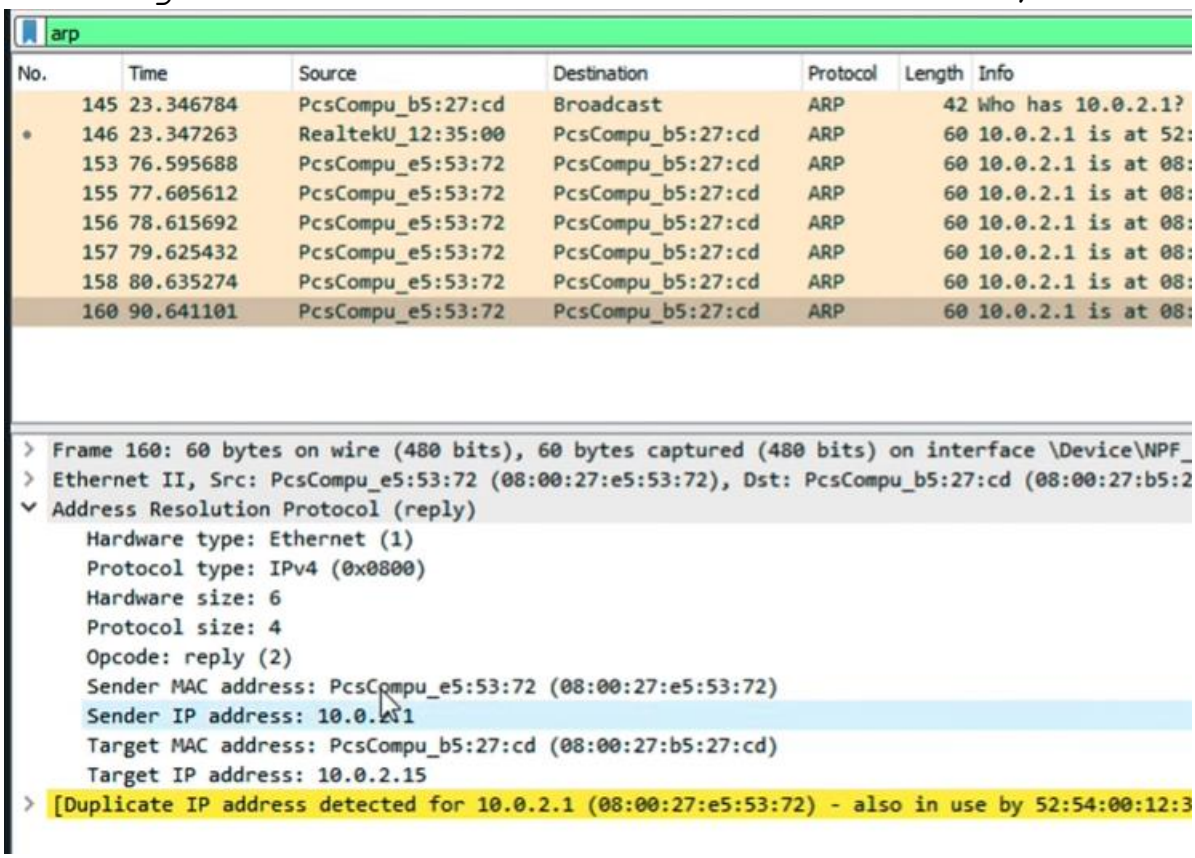
Here we are able to capture the information but the information is encrypted so it is pretty hard to decrypt the information to get the actual information .

In wireshack



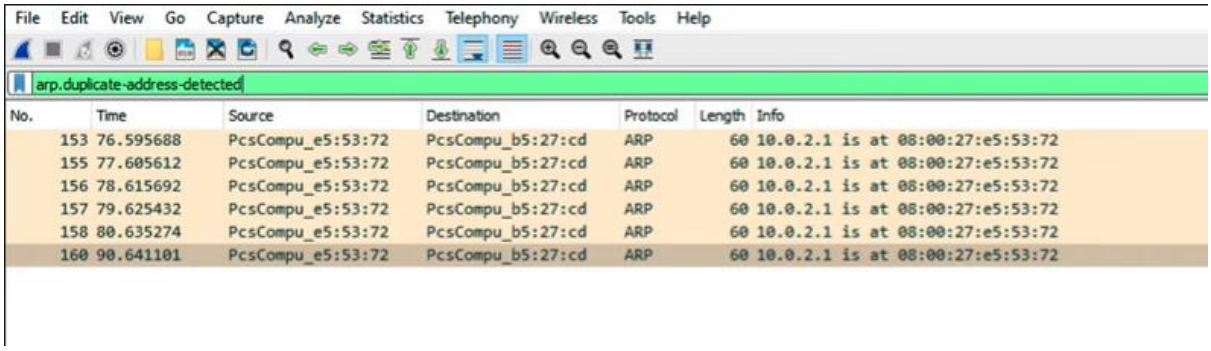
We initially have the legitimate Ips but following it we have a series of random ARPs generated.

Having a more detailed look over it,



Wireshark tells that there is a duplicate ip configured.

So we can use this as a filter and find out all the bad ARPs .



This is how we use wireshark to detect the ARP poisoning attack .