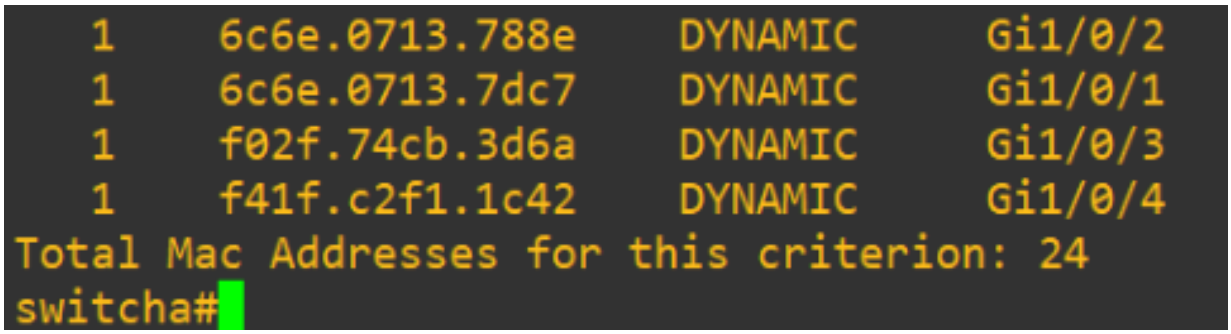
# You Poisoned my ARP

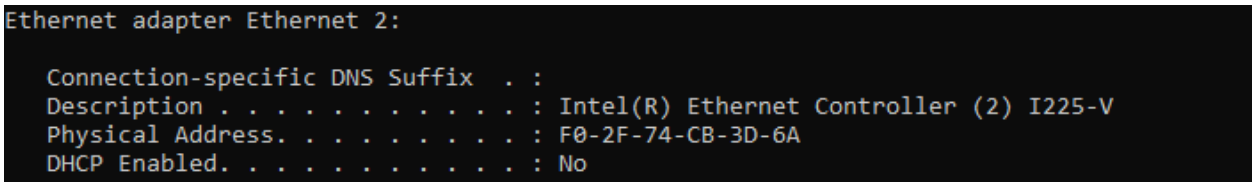
**Objective:** In this at-home lab Ettercap was used to carry out an ARP poisoning attack to intercept traffic between two devices on the same network. The purpose of this lab was to understand how ARP spoofing works and how it can be used in man-in-the-middle attacks. In order to prevent this attack, DHCP snooping and Dynamic ARP Inspection (DAI) were configured on the switch. DHCP snooping builds a list of trusted IP-to-MAC address bindings, and DAI uses that list to check ARP packets and block any that didn't match.

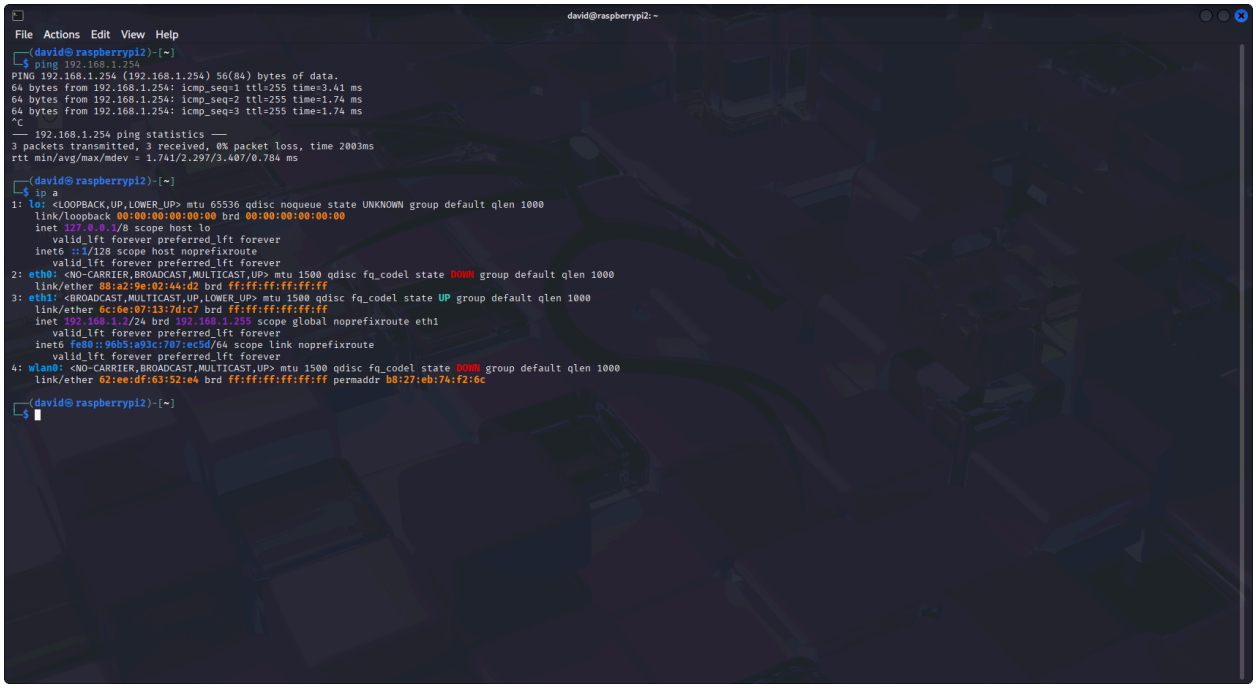
**Equipment:** Kali Linux, PC, Mac, Ettercap, 2811 router, and 3560 switch

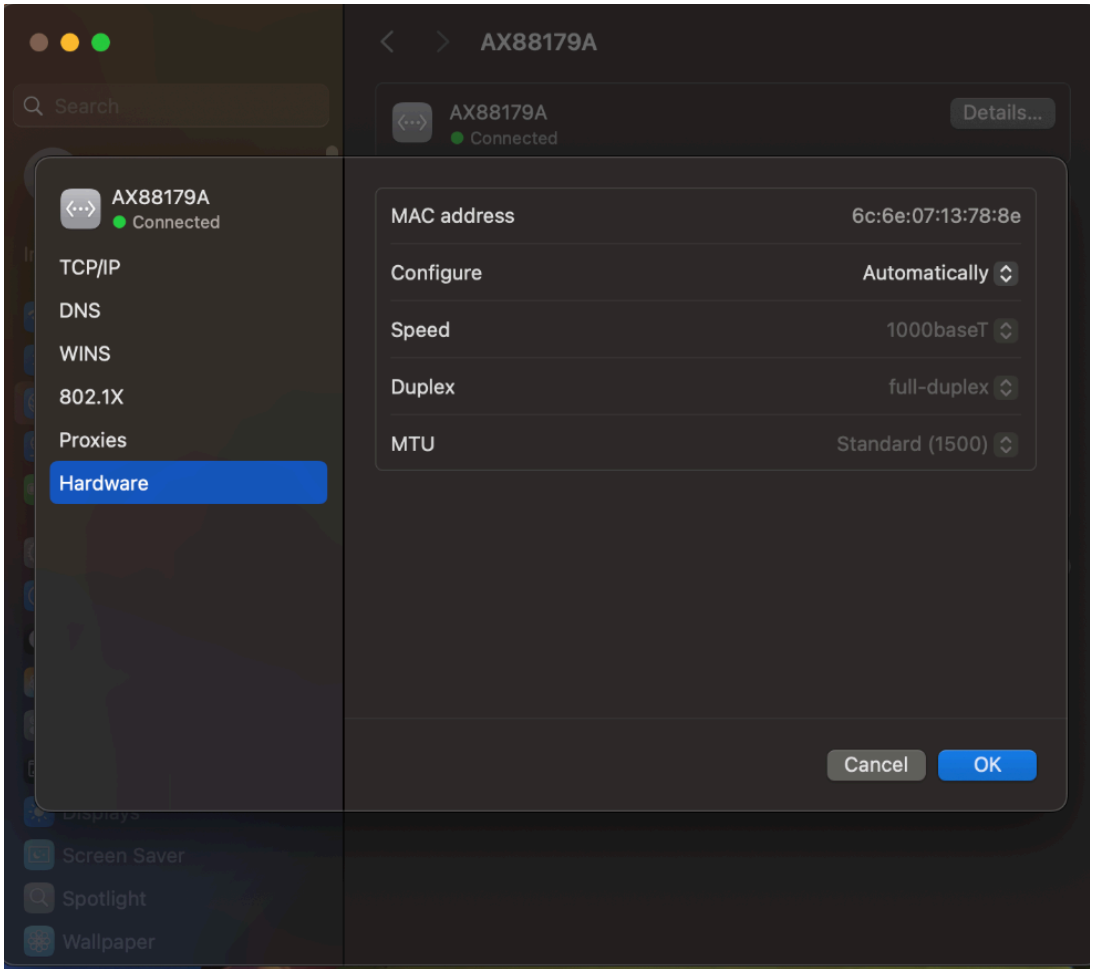
**Steps:**

1. Verify that the Mac Addresses register on the switches table

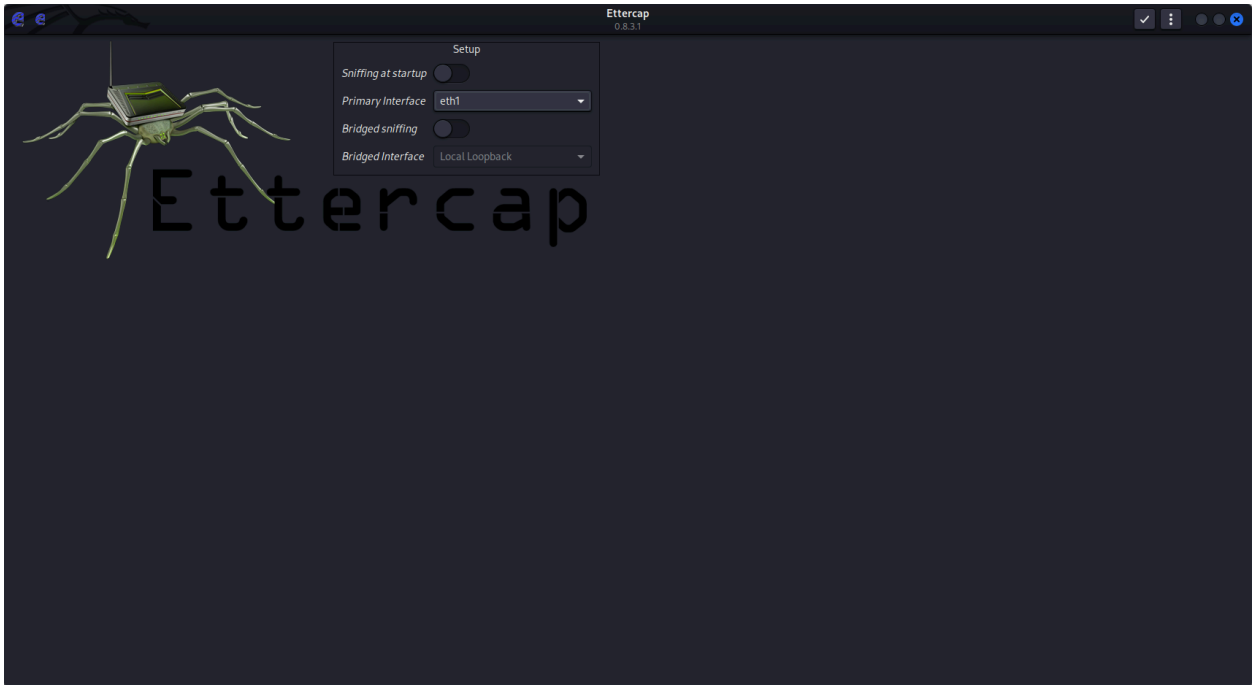


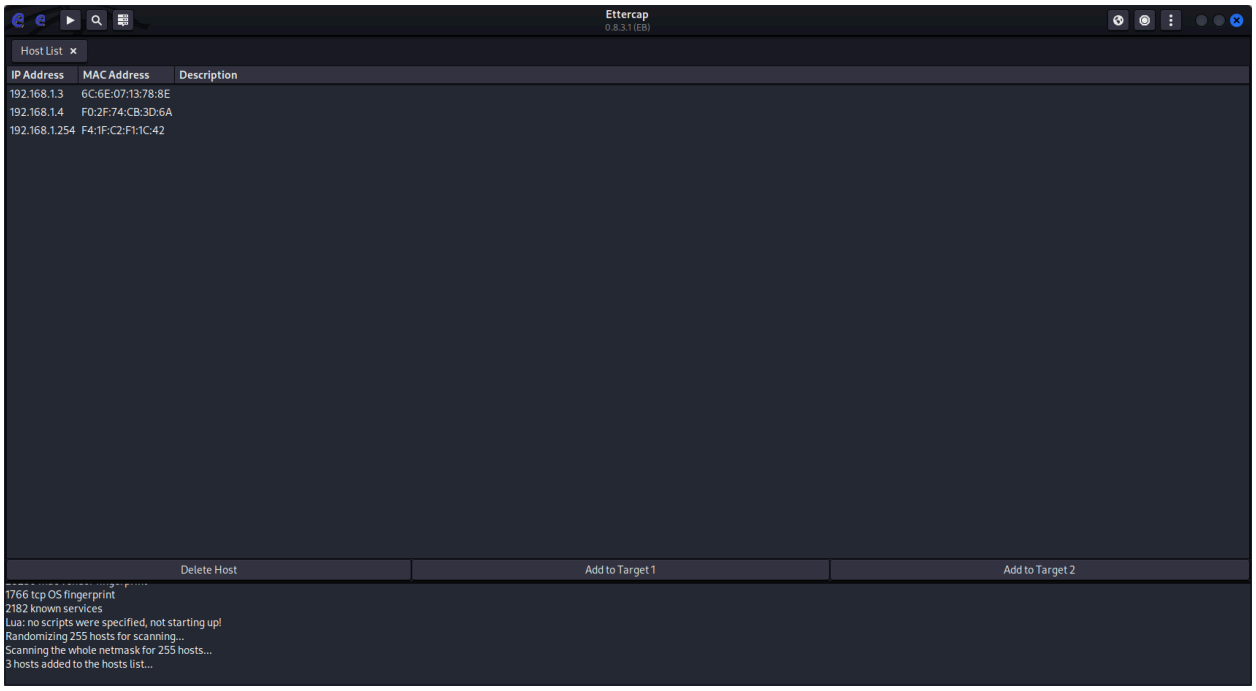

david@raspberrypi2: ~
File Actions Edit View Help
(david㉿raspberrypi2)-[~]
$ ping 192.168.1.254
PING 192.168.1.254 (192.168.1.254) 56(84) bytes of data.
64 bytes from 192.168.1.254: icmp_seq=1 ttl=255 time=3.41 ms
64 bytes from 192.168.1.254: icmp_seq=2 ttl=255 time=1.74 ms
64 bytes from 192.168.1.254: icmp_seq=3 ttl=255 time=1.74 ms
^C
— 192.168.1.254 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.741/2.297/3.407/0.784 ms
(david㉿raspberrypi2)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
link/ether 88:a2:9e:02:44:d2 brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 6c:6e:07:13:7d:c7 brd ff:ff:ff:ff:ff:ff
inet 192.168.1.2/24 brd 192.168.1.255 scope global noprefixroute eth1
valid_lft forever preferred_lft forever
inet6 fe80::96b5:a93c:707:ec5d/64 scope link noprefixroute
valid_lft forever preferred_lft forever
4: wlan0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
link/ether 62:ee:df:63:52:e4 brd ff:ff:ff:ff:ff:ff permaddr b8:27:eb:74:f2:6c
(david㉿raspberrypi2)-[~]
$


AX88179A
Search
AX88179A
Connected
Details...
AX88179A
Connected
TCP/IP
DNS
WINS
802.1X
Proxies
Hardware
MAC address
6c:6e:07:13:78:8e
Configure
Automatically
Speed
1000baseT
Duplex
full-duplex
MTU
Standard (1500)
Cancel
OK
Screen Saver
Spotlight
Wallpaper

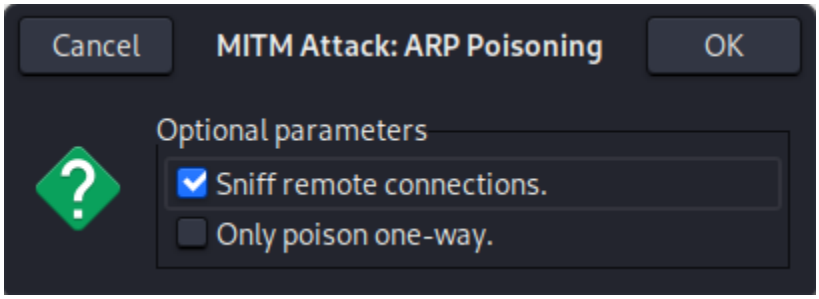
2. Setup Ettercap



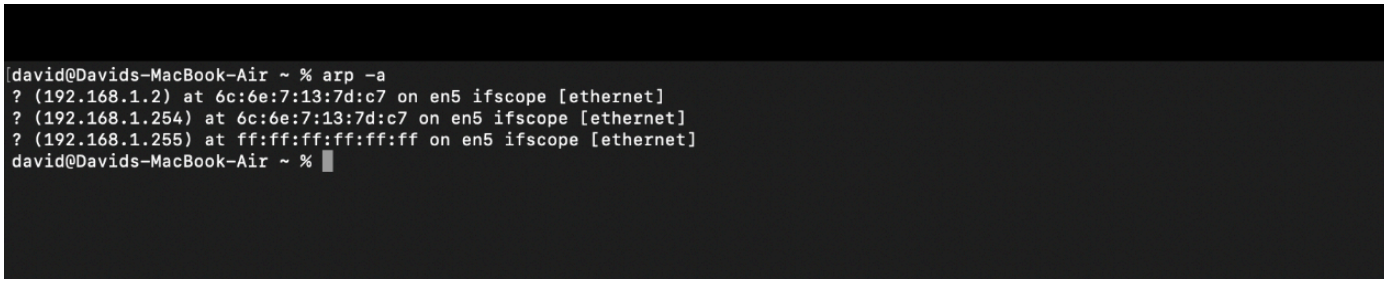

3. Scan for host within the subnet



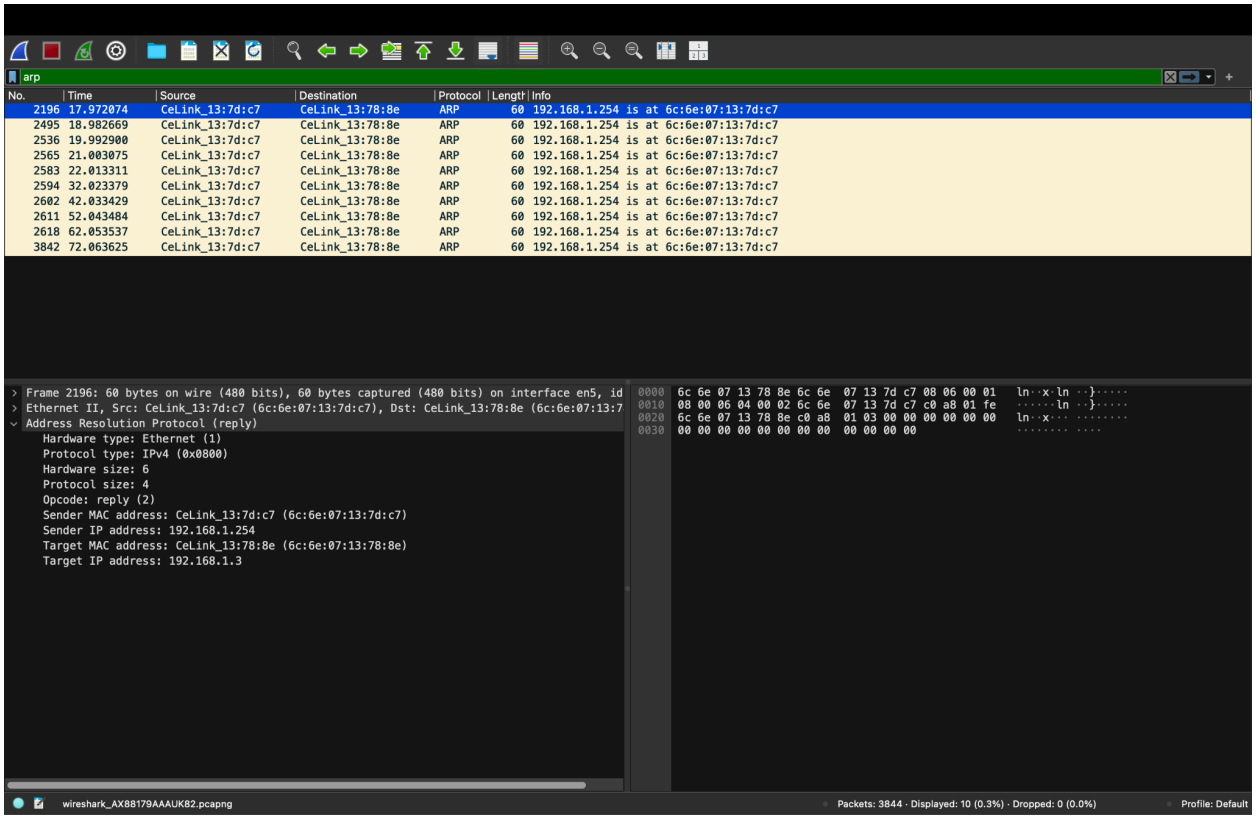
4. Add my Mac on target 1 which ends with 8E and the router interface that ends with 42




5. I verify that the ARP attack is working by checking my arp table on my Mac



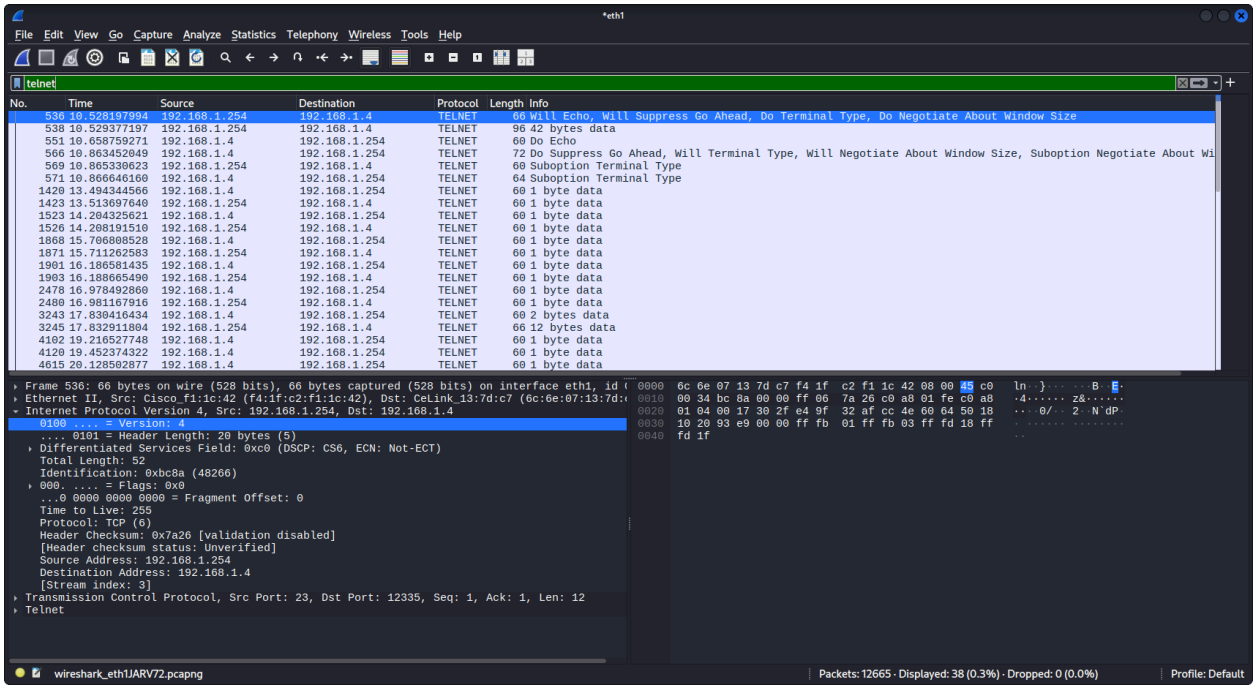

6. I look at the ARP traffic attack with wireshark

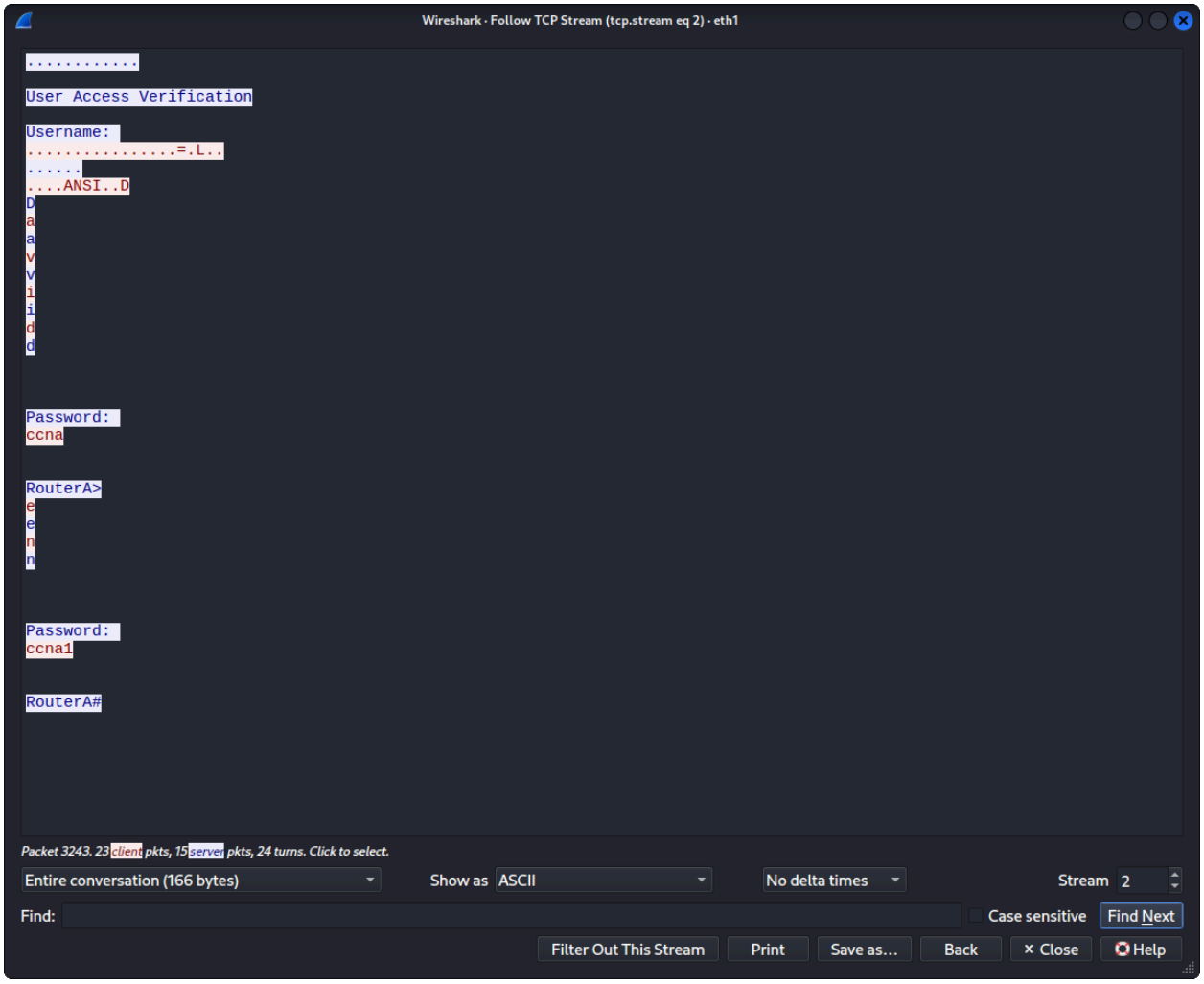


7. As you can see the MAC address does not match what the router has

```
RouterA#sh int g0/1
GigabitEthernet0/1 is up, line protocol is up (connected)
  Hardware is Gigabit Ethernet, address is f41f.c2f1.1c42 (bia f41f.c2f1.1c42)
  Internet address is 192.168.1.254/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not set
  Full-duplex, 1000Mb/s, link type is auto, media type is 10/100/1000BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:32, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     7382 packets input, 2696841 bytes, 0 no buffer
     Received 2929 broadcasts (100 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 2526 multicast, 0 pause input
     0 input packets with dribble condition detected
 --More--
```

8. On my Kali Linux machine I intercepted a telnet session to obtain sensitive information






9. To stop this attack I made a DHCP pool with IP DHCP snooping and ARP inspection as well

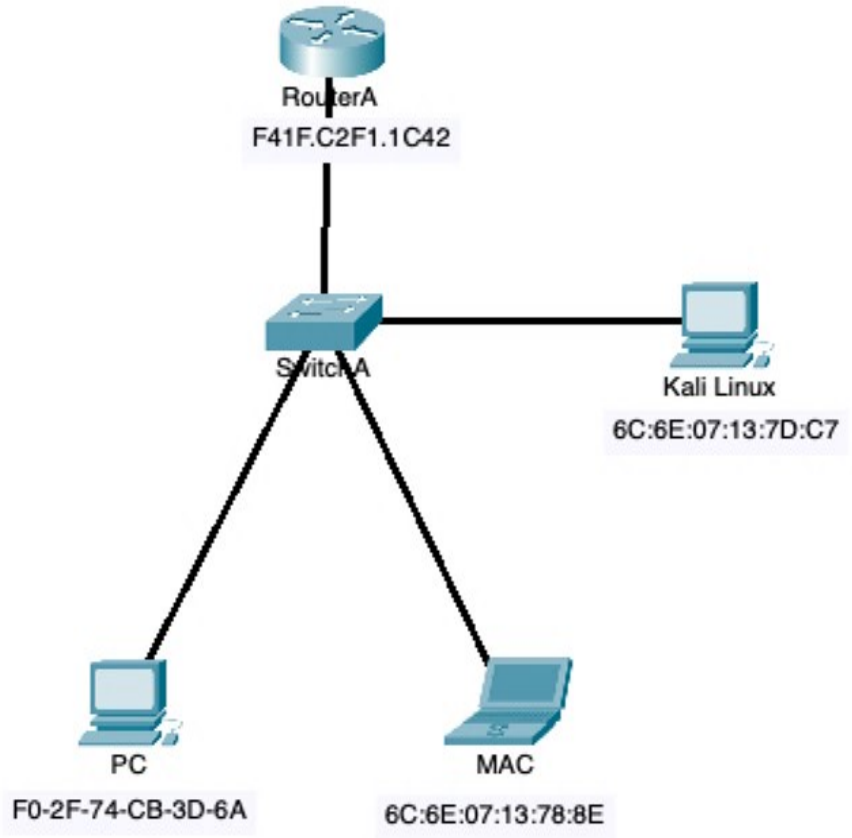
```
ip dhcp excluded-address 192.168.1.254
!
ip dhcp pool Home
   network 192.168.1.0 255.255.255.0
   default-router 192.168.1.254
!
!
!
```

10. I verify that it's working

```
RouterA#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.168.1.2         016c.6e07.137d.c7       Mar 02 1993 12:48 AM    Automatic
RouterA#
```

11. Lastly I enable ARP inspection

```
switcha>en
switcha#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
switcha(config)#ip arp inspection vlan 1
switcha(config)#
```


RouterA
F41F.C2F1.1C42
Switch A
Kali Linux
6C:6E:07:13:7D:C7
PC
F0-2F-74-CB-3D-6A
MAC
6C:6E:07:13:78:8E