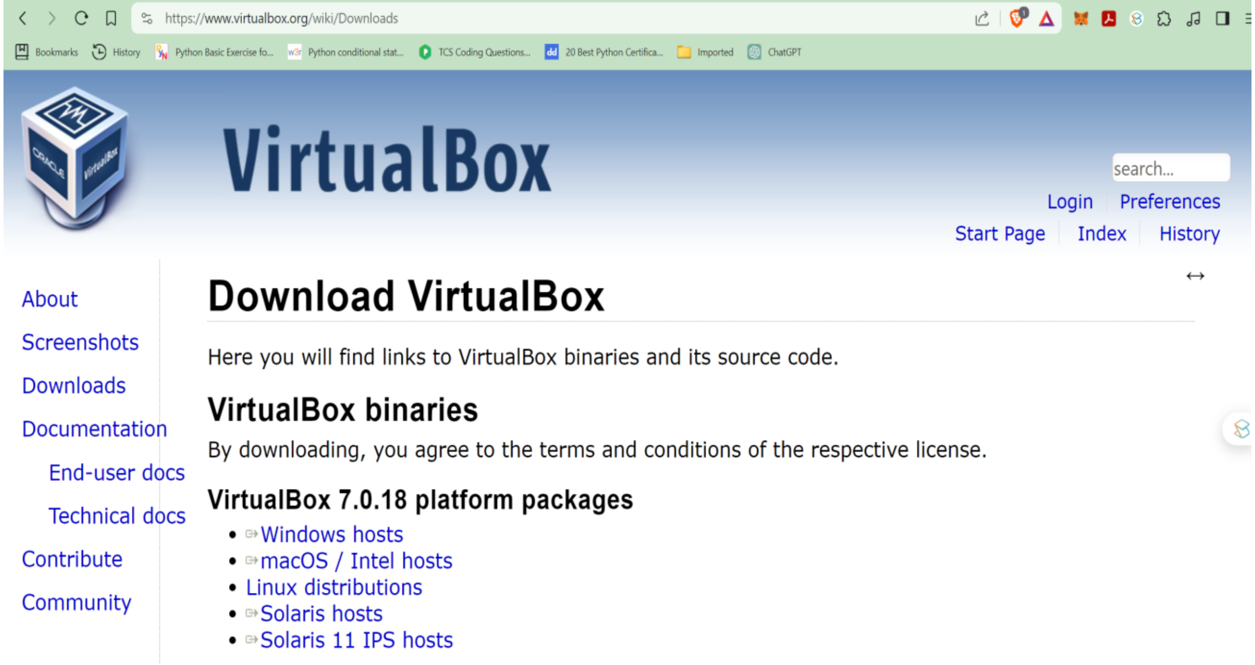
Experiment 5

Objective: ARP Poisoning Attack: Set up an ARP poisoning attack using tools like Ettercap. Analyze the captured packets to understand how the attack can lead to a Man-in-the-Middle scenario.

Install Virtual Box Manager on Windows



Download VirtualBox

Here you will find links to VirtualBox binaries and its source code.

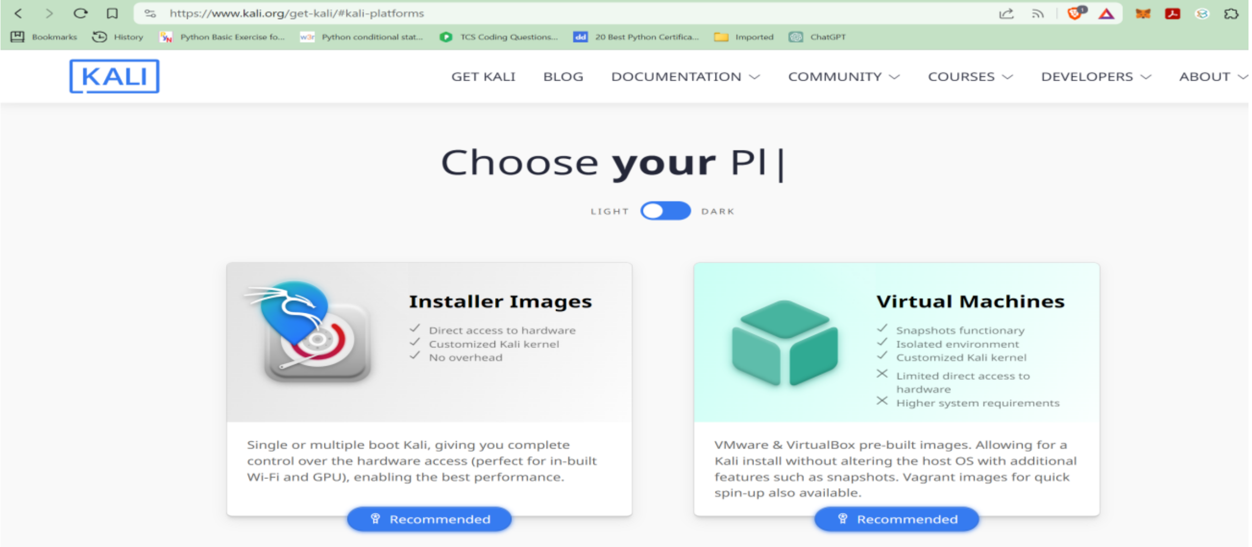
VirtualBox binaries

By downloading, you agree to the terms and conditions of the respective license.

VirtualBox 7.0.18 platform packages

- Windows hosts
- macOS / Intel hosts
- Linux distributions
- Solaris hosts
- Solaris 11 IPS hosts

Install Kali Linux through Virtual Box



Choose **your** Pl|

Installer Images

✓ Direct access to hardware
✓ Customized Kali kernel
✓ No overhead

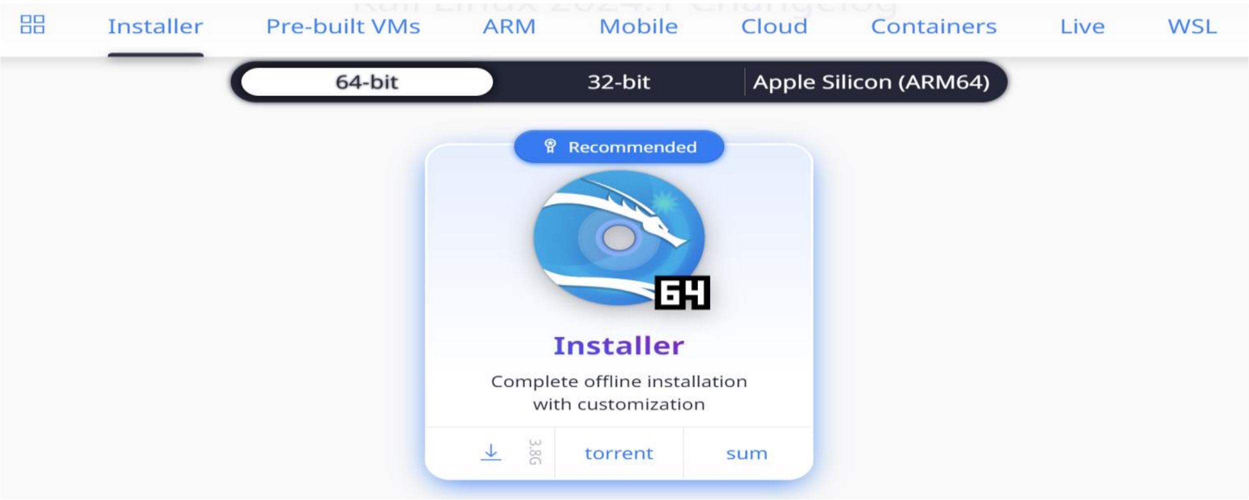
Single or multiple boot Kali, giving you complete control over the hardware access (perfect for in-built Wi-Fi and GPU), enabling the best performance.

Virtual Machines

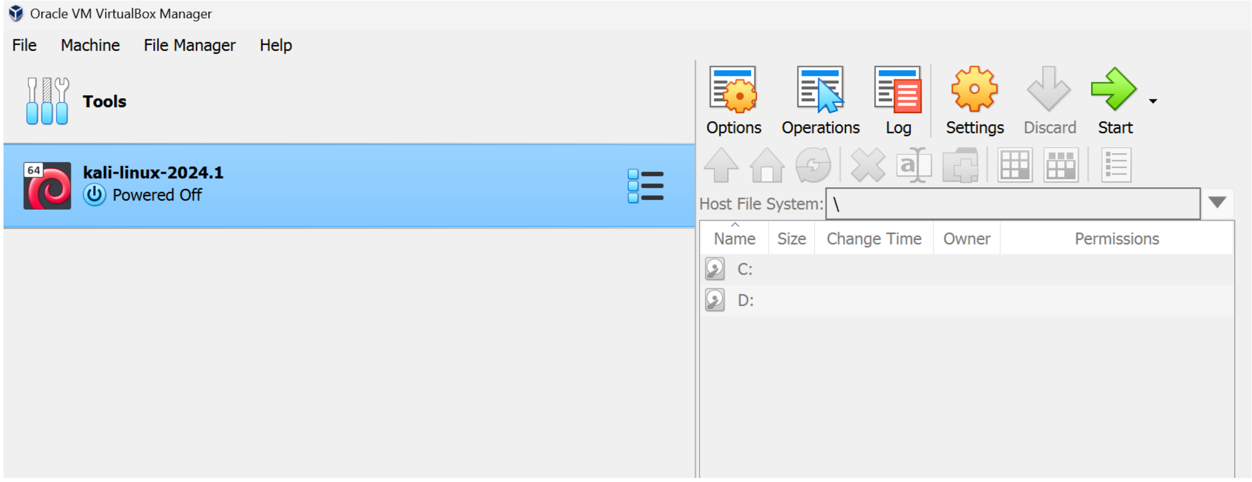
✓ Snapshots functionary
✓ Isolated environment
✓ Customized Kali kernel
✕ Limited direct access to hardware
✕ Higher system requirements

VMware & VirtualBox pre-built images. Allowing for a Kali install without altering the host OS with additional features such as snapshots. Vagrant images for quick spin-up also available.

Choose Installer Image



Complete offline installation with customization

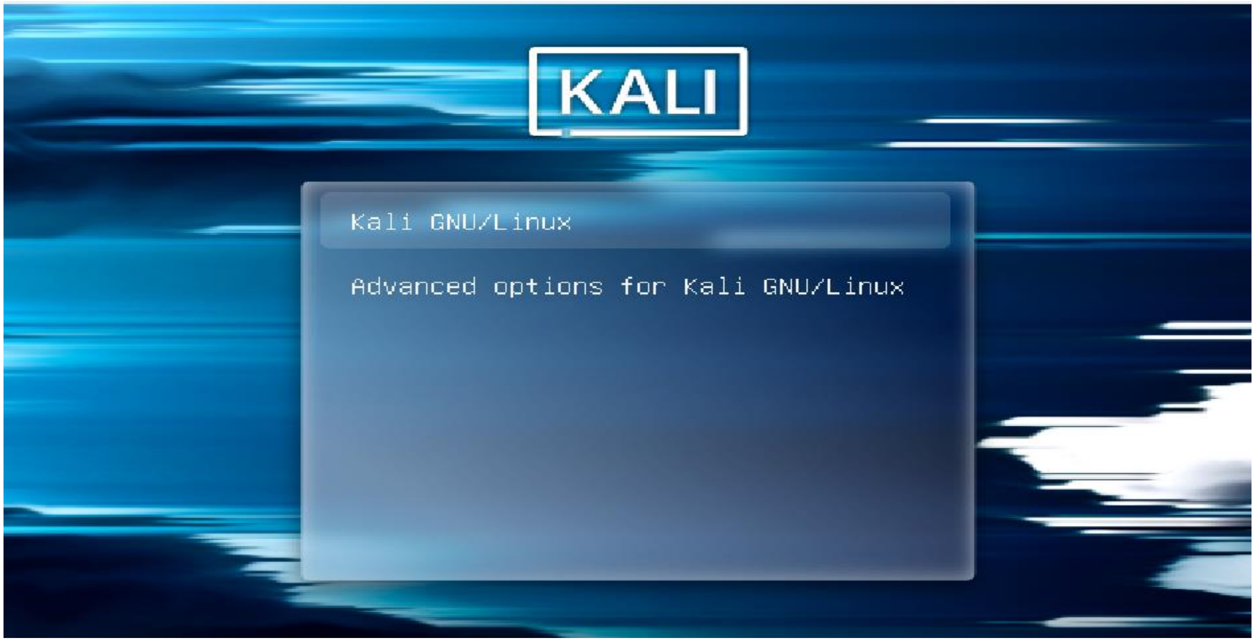


kali-linux-2024.1
Powered Off

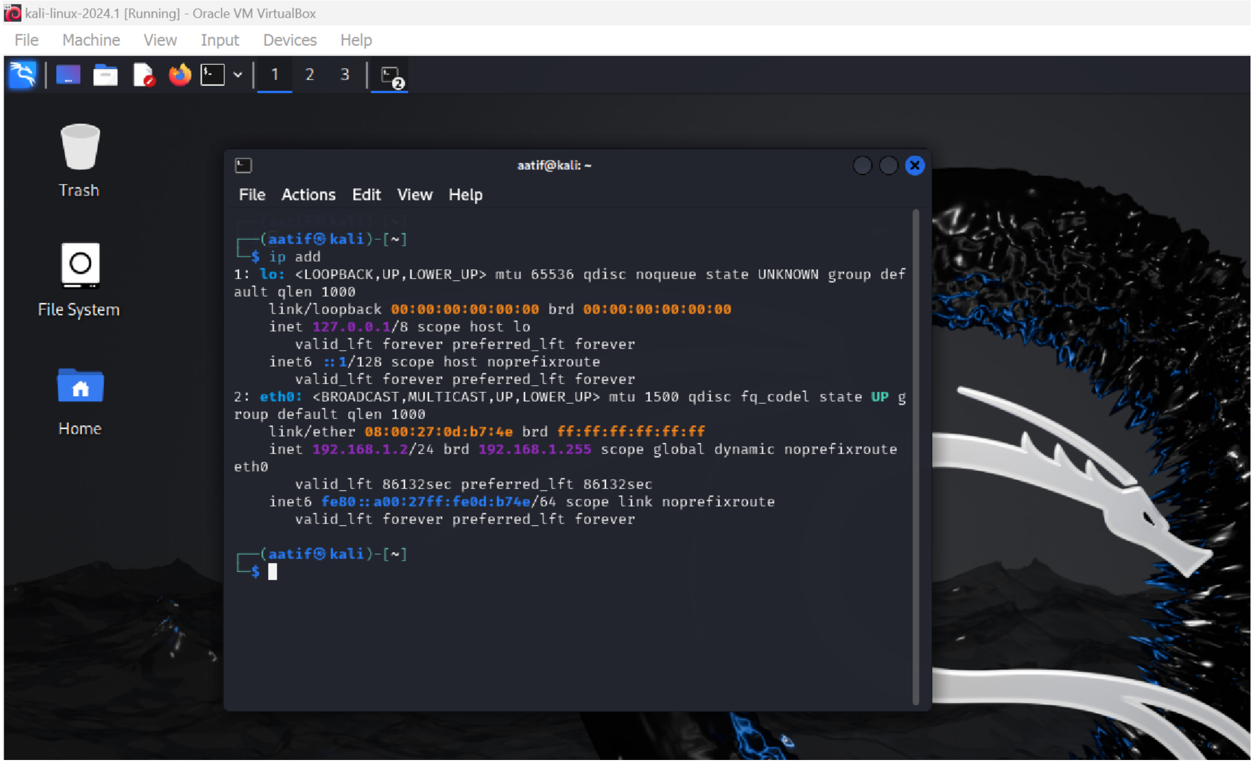
Host File System: \

Name	Size	Change Time	Owner	Permissions
C:				
D:				

Start Kali Linux:

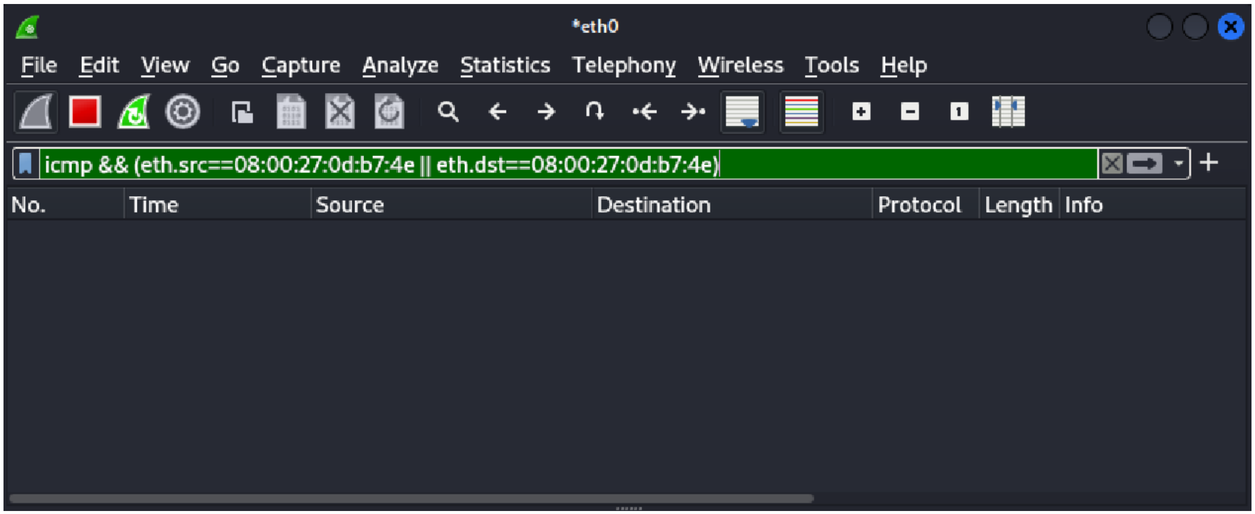


Open Terminal and write command: ***ip add***


kali-linux-2024.1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
aatif@kali: ~
File Actions Edit View Help

```
┌──(aatif㉿kali)-[~]
└─$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault 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: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:0d:b7:4e brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.2/24 brd 192.168.1.255 scope global dynamic noprefixroute
eth0
       valid_lft 86132sec preferred_lft 86132sec
    inet6 fe80::a00:27ff:fe0d:b74e/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(aatif㉿kali)-[~]
└─$
```

Copy MAC address from above and run command in wireshark @kali

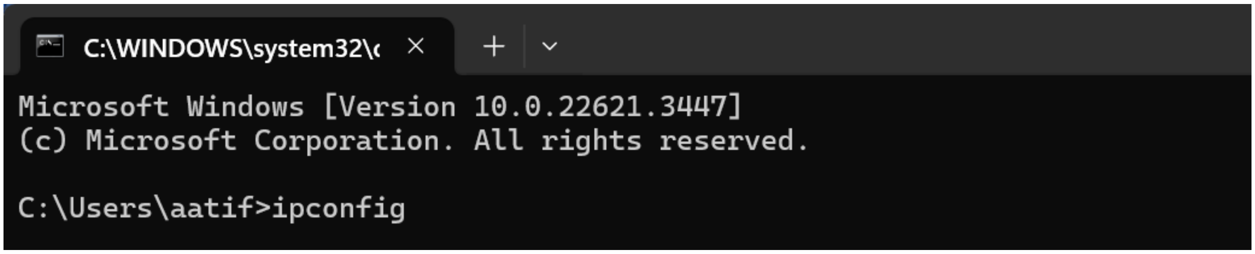

*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info

```
icmp && (eth.src==08:00:27:0d:b7:4e || eth.dst==08:00:27:0d:b7:4e)
```

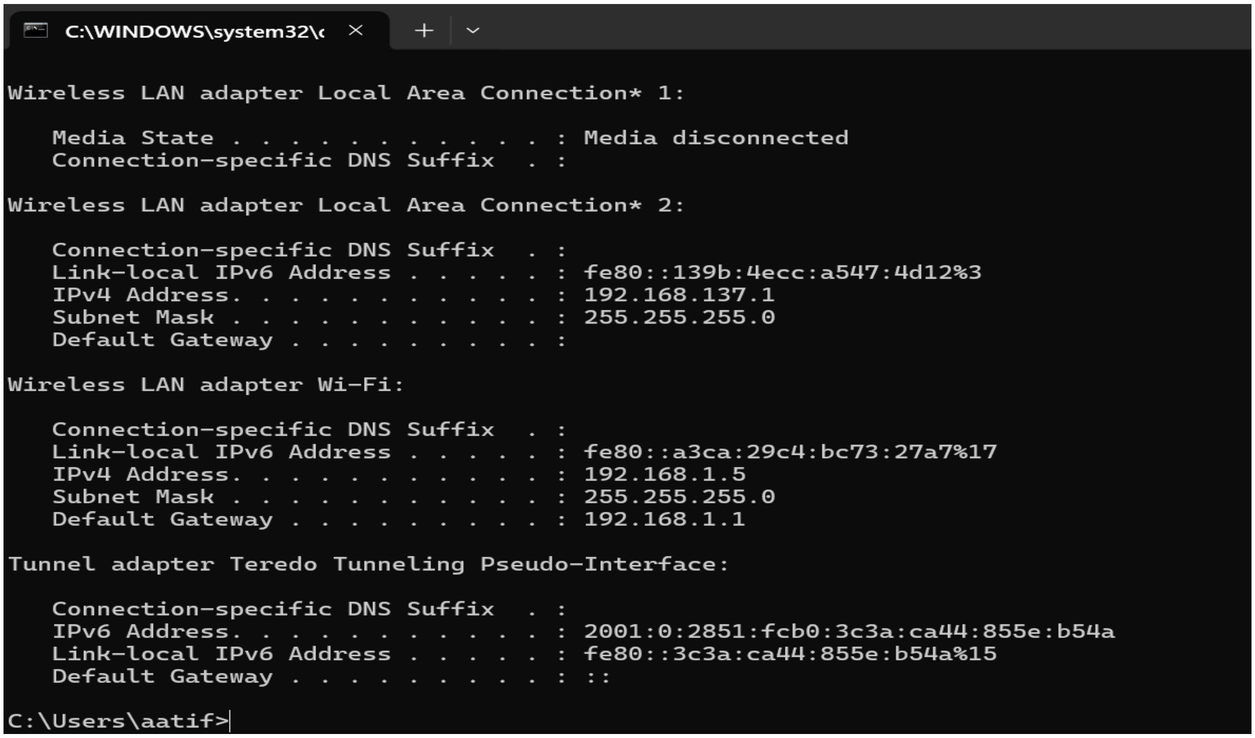
We observe: No traffic is being captured

Aim is to capture the traffic between Target and default gate way on same line.

So we go to Target Device (Windows) and find IP address and default gateway.



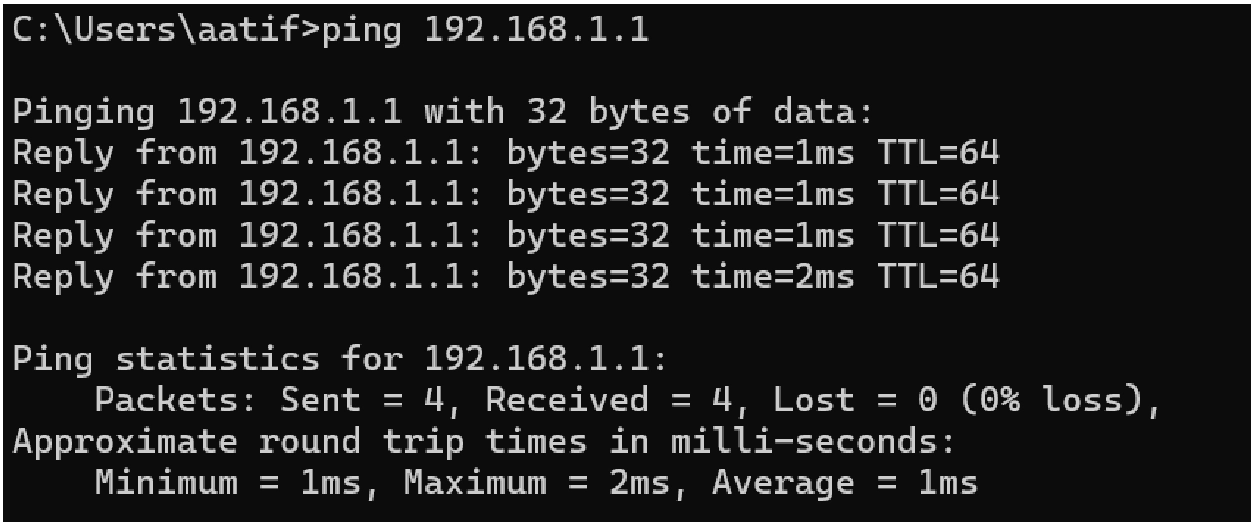
```
Microsoft Windows [Version 10.0.22621.3447]
(c) Microsoft Corporation. All rights reserved.

C:\Users\aatif>ipconfig
```



```
Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::139b:4ecc:a547:4d12%3
   IPv4 Address. . . . . . . . . . . : 192.168.137.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a3ca:29c4:bc73:27a7%17
   IPv4 Address. . . . . . . . . . . : 192.168.1.5
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:2851:fcb0:3c3a:ca44:855e:b54a
   Link-local IPv6 Address . . . . . : fe80::3c3a:ca44:855e:b54a%15
   Default Gateway . . . . . . . . . : ::

C:\Users\aatif>
```

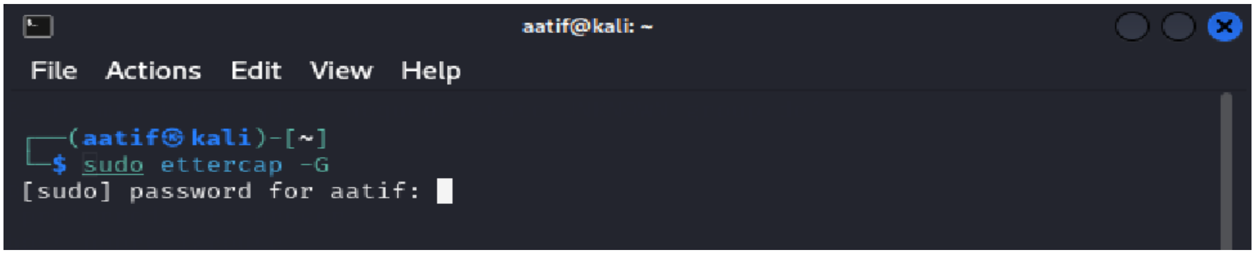
IPv4 Address. . . . . : **192.168.1.5**

Default Gateway . . . . : **192.168.1.1**



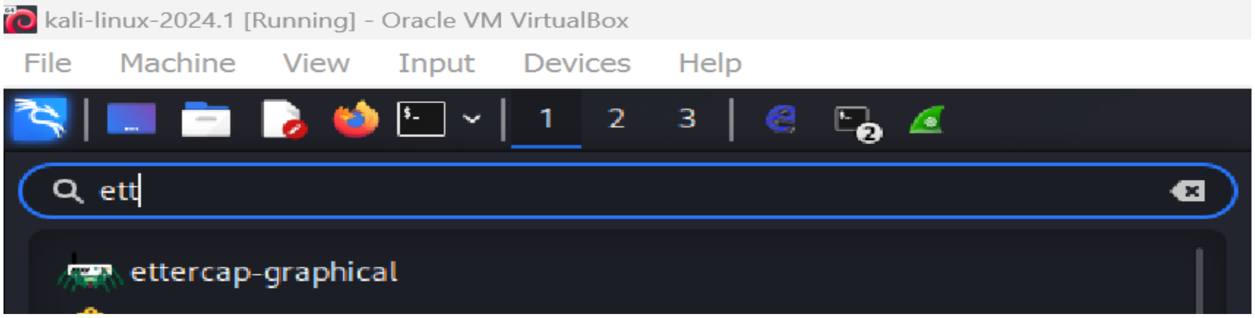
```
C:\Users\aatif>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

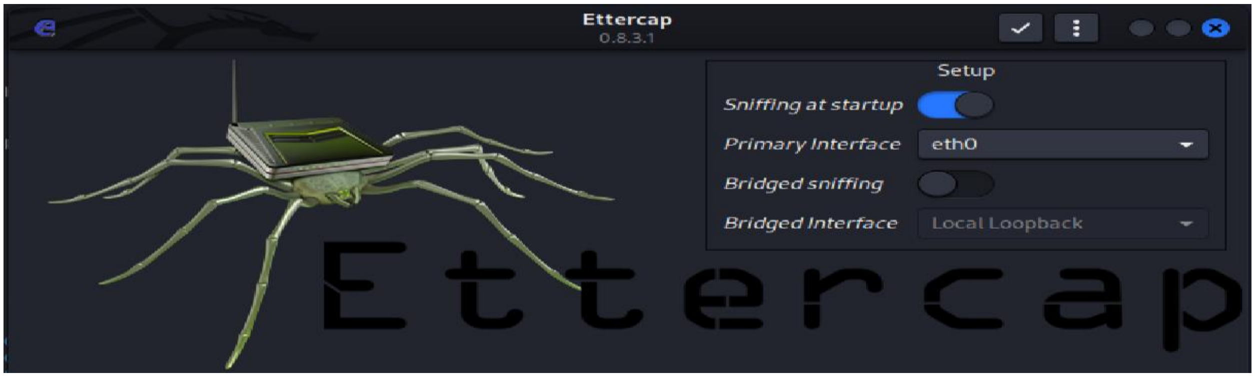
We are going to sniff traffic once we enable ARP poising using Tool Ettercap



```
┌──(aatif㉿kali)-[~]
└─$ sudo ettercap -G
[sudo] password for aatif: 
```

OR





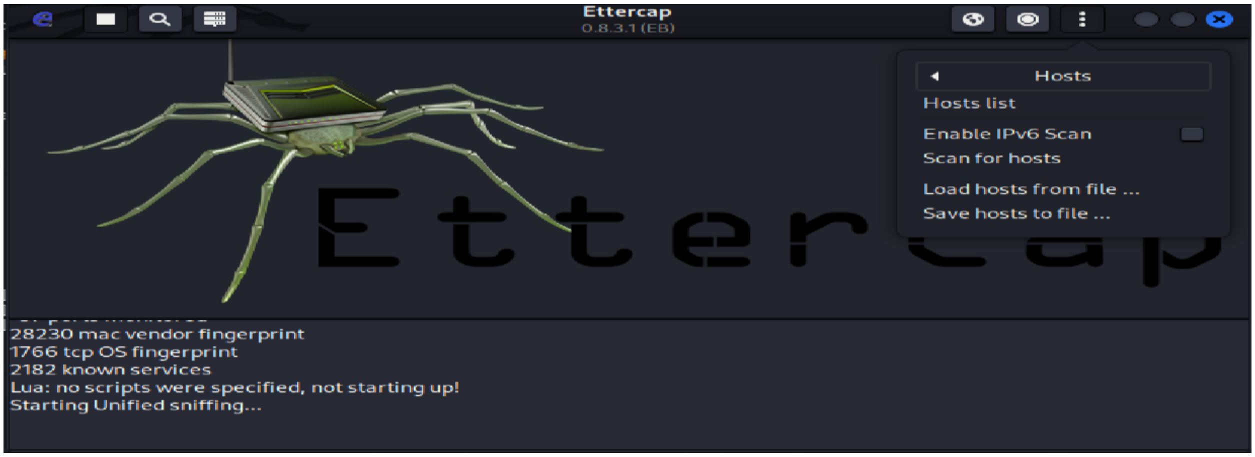
Sniffing at startup ●

Primary Interface: eth0

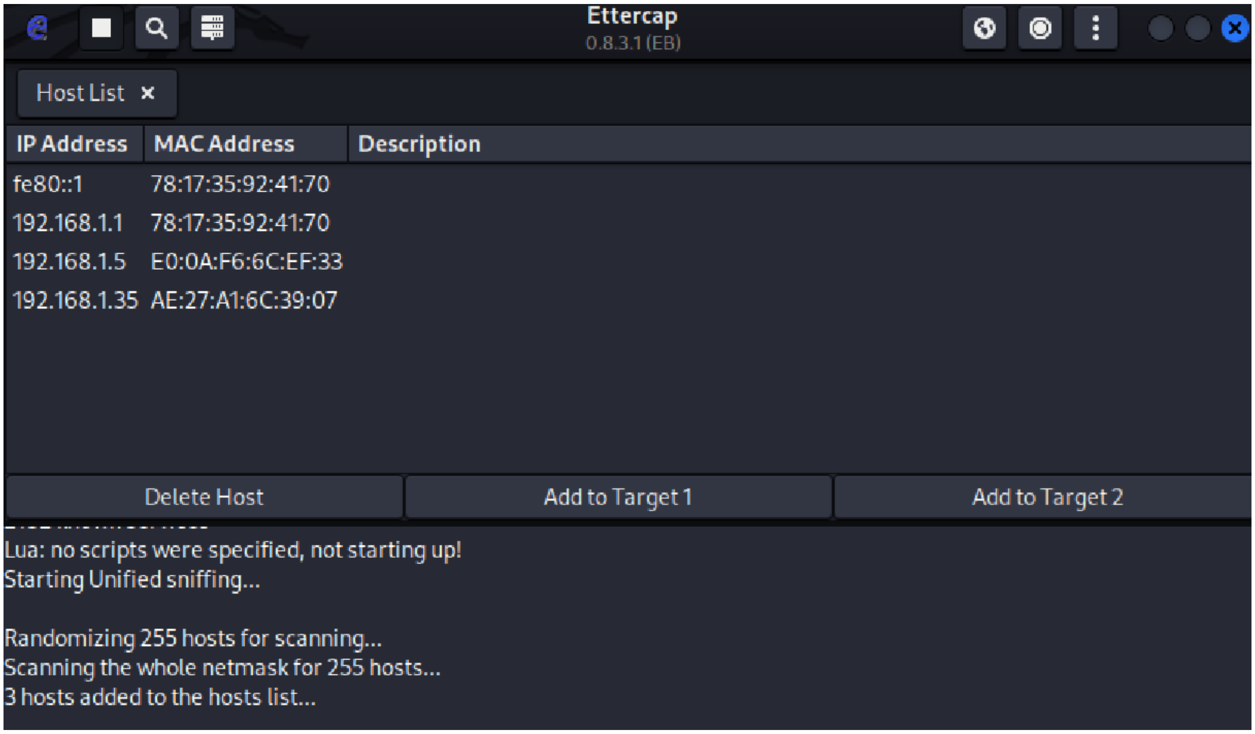
Bridged sniffing ○

Bridged Interface: Local Loopback

Click on three dots and scan for hosts



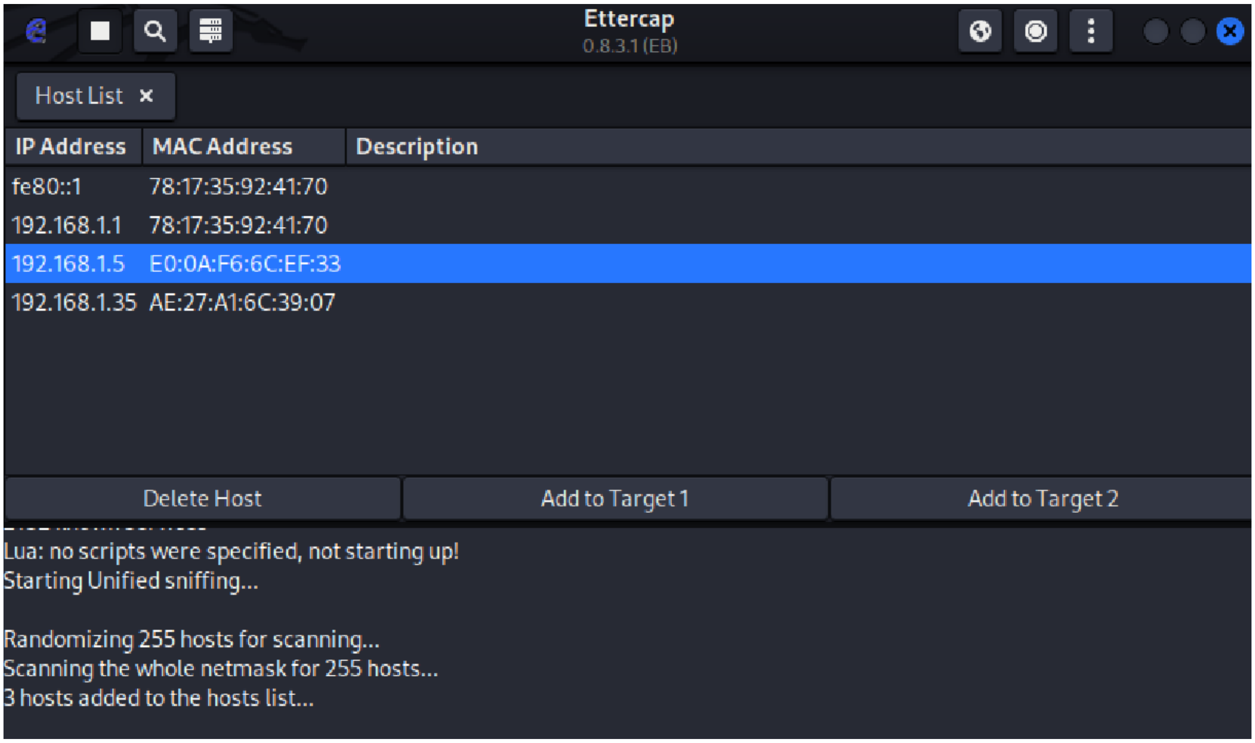
```
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
```



IP Address	MAC Address	Description
fe80::1	78:17:35:92:41:70	
192.168.1.1	78:17:35:92:41:70	
192.168.1.5	E0:0A:F6:6C:EF:33	
192.168.1.35	AE:27:A1:6C:39:07	

```
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...
```

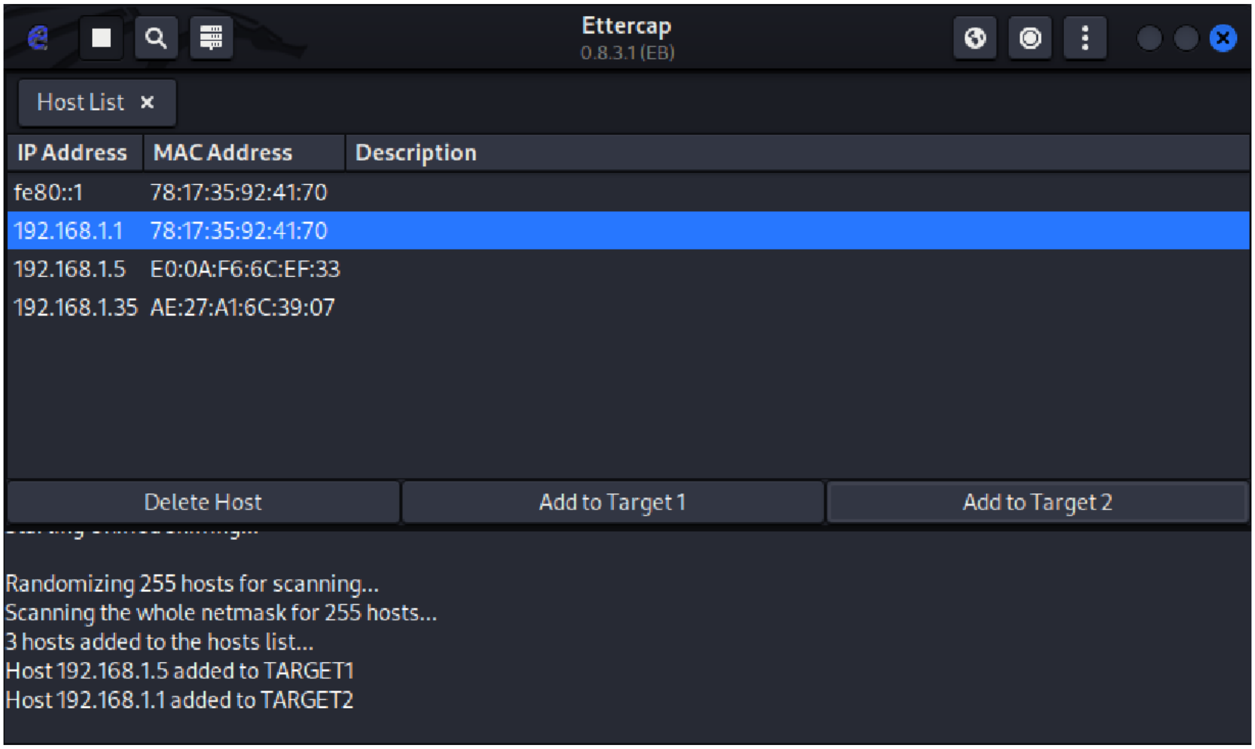
Select Ip Address and Add to Target 1



IP Address	MAC Address	Description
fe80::1	78:17:35:92:41:70	
192.168.1.1	78:17:35:92:41:70	
192.168.1.5	E0:0A:F6:6C:EF:33	
192.168.1.35	AE:27:A1:6C:39:07	

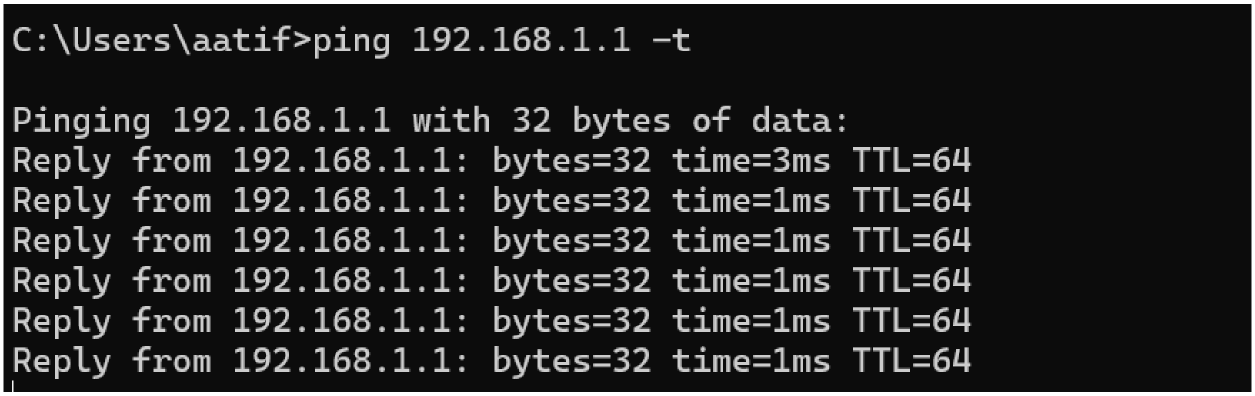
```
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...
```

Select Default Gateway and Add to Target 2



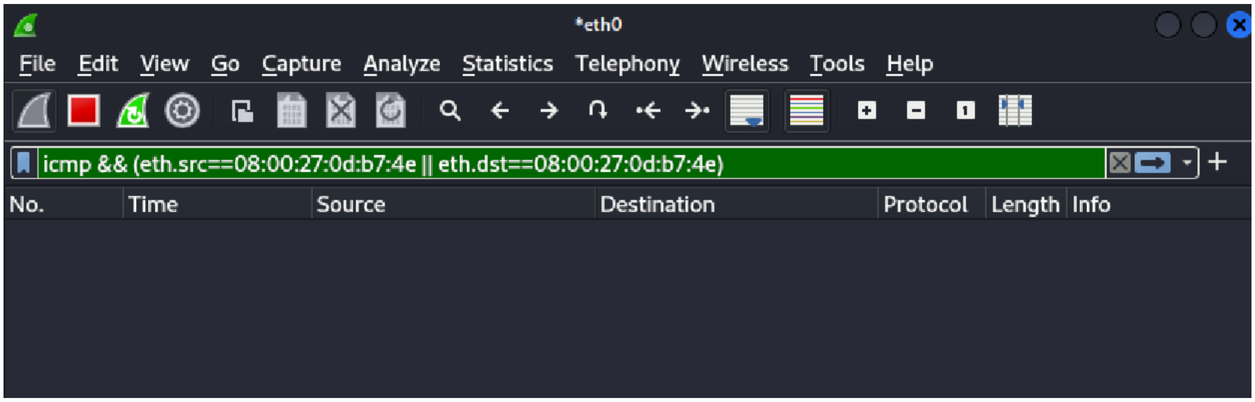
IP Address	MAC Address	Description
fe80::1	78:17:35:92:41:70	
192.168.1.1	78:17:35:92:41:70	
192.168.1.5	E0:0A:F6:6C:EF:33	
192.168.1.35	AE:27:A1:6C:39:07	

```
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...
Host 192.168.1.5 added to TARGET1
Host 192.168.1.1 added to TARGET2
```



```
C:\Users\aatif>ping 192.168.1.1 -t

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=3ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
```

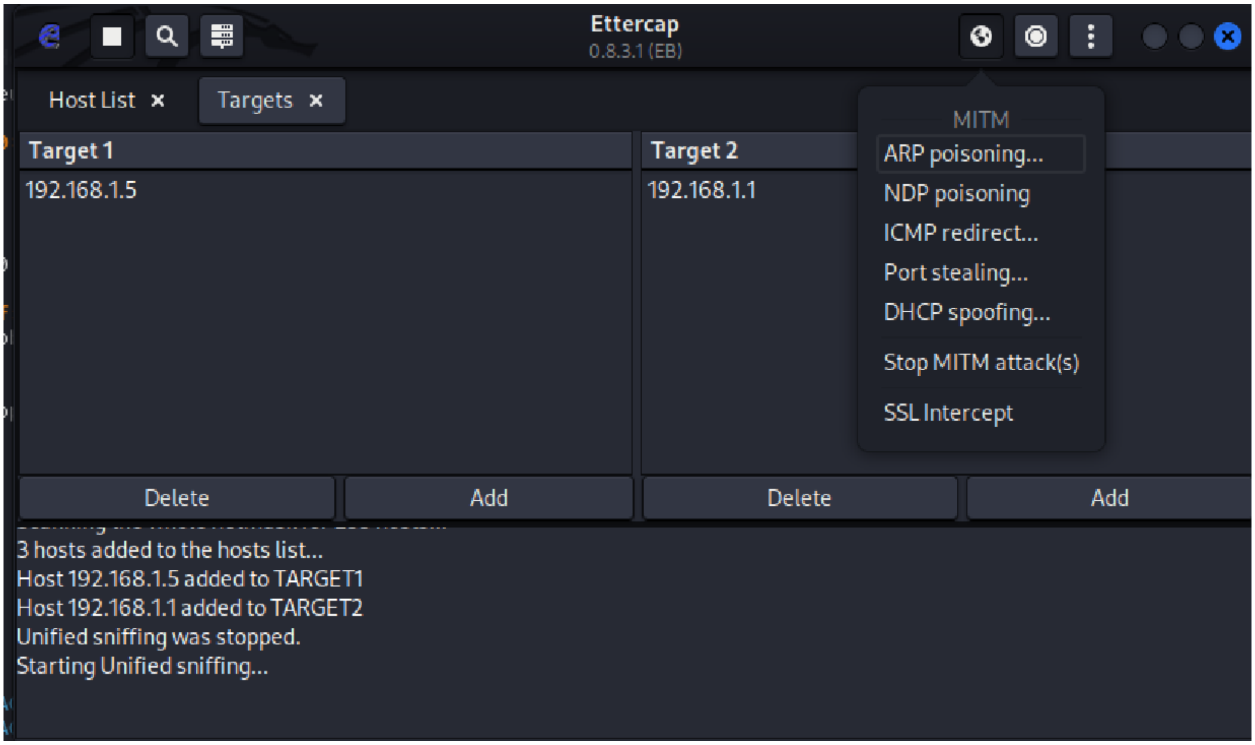
Still Nothing is capturing



```
icmp && (eth.src==08:00:27:0d:b7:4e || eth.dst==08:00:27:0d:b7:4e)
```

No.	Time	Source	Destination	Protocol	Length	Info

Select Current Targets

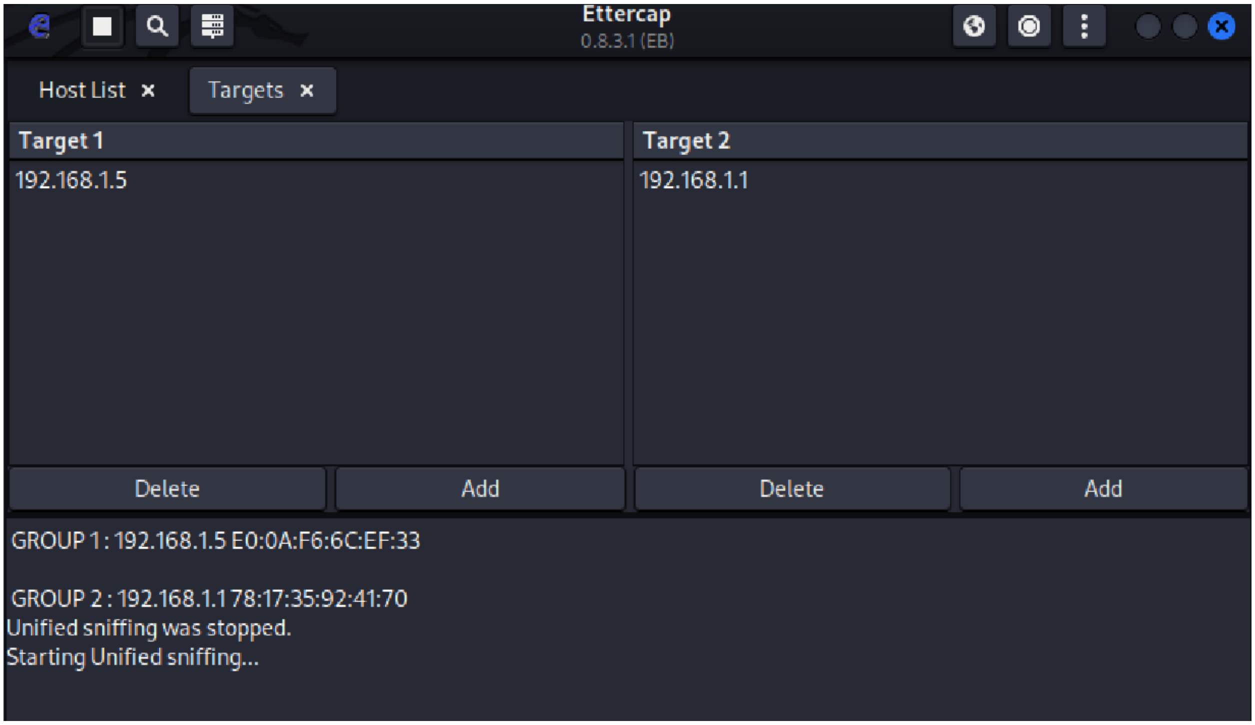


Target 1: 192.168.1.5

Target 2: 192.168.1.1

```
3 hosts added to the hosts list...
Host 192.168.1.5 added to TARGET1
Host 192.168.1.1 added to TARGET2
Unified sniffing was stopped.
Starting Unified sniffing...
```

Click ARP Poisoning and start sniffing

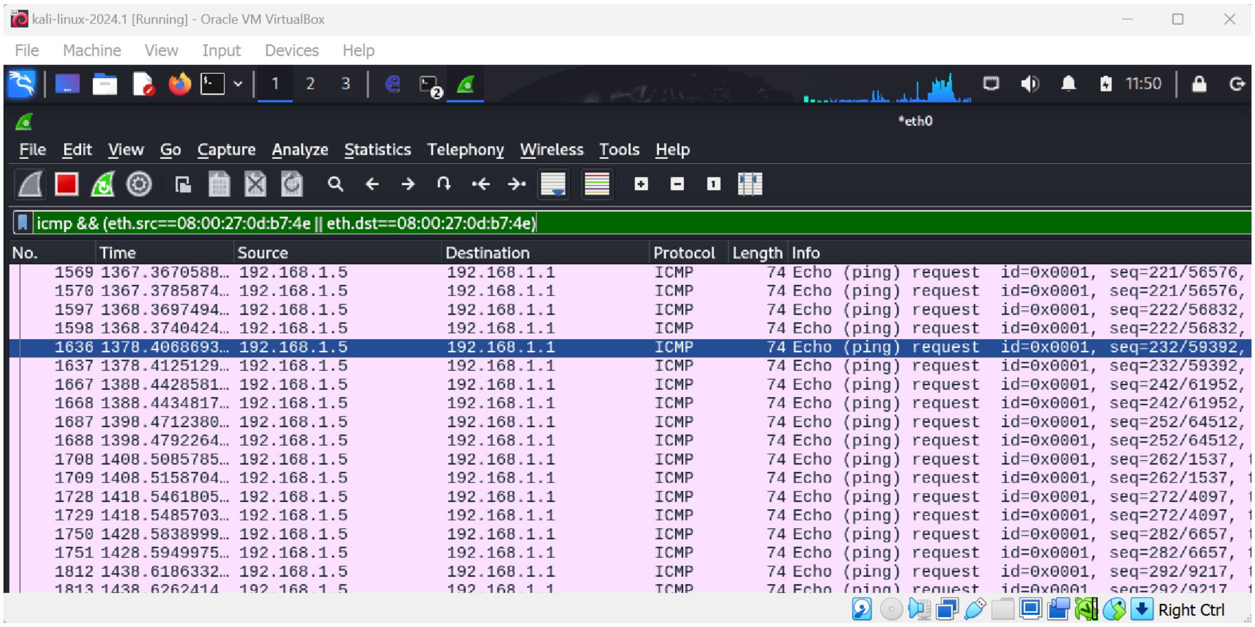


Target 1: 192.168.1.5

Target 2: 192.168.1.1

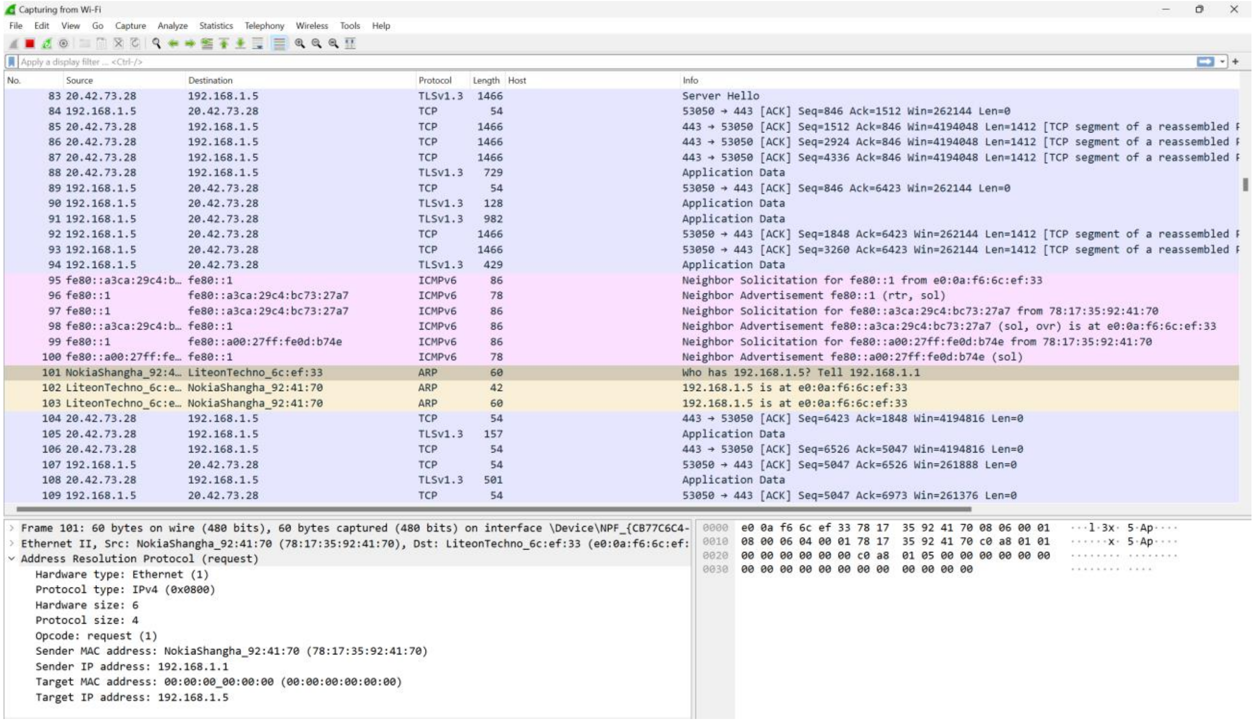
```
 GROUP 1 : 192.168.1.5 E0:0A:F6:6C:EF:33

 GROUP 2 : 192.168.1.1 78:17:35:92:41:70
Unified sniffing was stopped.
Starting Unified sniffing...
```

Now we can see, packets are being captured


kali-linux-2024.1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3
11:50
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Right Ctrl

```
icmp && (eth.src==08:00:27:0d:b7:4e || eth.dst==08:00:27:0d:b7:4e)

No.   Time            Source        Destination   Protocol  Length Info
 1569 1367.3670588…  192.168.1.5   192.168.1.1   ICMP        74 Echo (ping) request  id=0x0001, seq=221/56576,
 1570 1367.3785874…  192.168.1.5   192.168.1.1   ICMP        74 Echo (ping) request  id=0x0001, seq=221/56576,
 1597 1368.3697494…  192.168.1.5   192.168.1.1   ICMP        74 Echo (ping) request  id=0x0001, seq=222/56832,
 1598 1368.3740424…  192.168.1.5   192.168.1.1   ICMP        74 Echo (ping) request  id=0x0001, seq=222/56832,
 1636 1378.4068693…  192.168.1.5   192.168.1.1   ICMP        74 Echo (ping) request  id=0x0001, seq=232/59392,
 1637 1378.4125129…  192.168.1.5   192.168.1.1   ICMP        74 Echo (ping) request  id=0x0001, seq=232/59392,
 1667 1388.4428581…  192.168.1.5   192.168.1.1   ICMP        74 Echo (ping) request  id=0x0001, seq=242/61952,
 1668 1388.4434817…  192.168.1.5   192.168.1.1   ICMP        74 Echo (ping) request  id=0x0001, seq=242/61952,
 1687 1398.4712380…  192.168.1.5   192.168.1.1   ICMP        74 Echo (ping) request  id=0x0001, seq=252/64512,
 1688 1398.4792264…  192.168.1.5   192.168.1.1   ICMP        74 Echo (ping) request  id=0x0001, seq=252/64512,
 1708 1408.5085785…  192.168.1.5   192.168.1.1   ICMP        74 Echo (ping) request  id=0x0001, seq=262/1537, t
 1709 1408.5158704…  192.168.1.5   192.168.1.1   ICMP        74 Echo (ping) request  id=0x0001, seq=262/1537, t
 1728 1418.5461805…  192.168.1.5   192.168.1.1   ICMP        74 Echo (ping) request  id=0x0001, seq=272/4097, t
 1729 1418.5485703…  192.168.1.5   192.168.1.1   ICMP        74 Echo (ping) request  id=0x0001, seq=272/4097, t
 1750 1428.5838999…  192.168.1.5   192.168.1.1   ICMP        74 Echo (ping) request  id=0x0001, seq=282/6657, t
 1751 1428.5949975…  192.168.1.5   192.168.1.1   ICMP        74 Echo (ping) request  id=0x0001, seq=282/6657, t
 1812 1438.6186332…  192.168.1.5   192.168.1.1   ICMP        74 Echo (ping) request  id=0x0001, seq=292/9217, t
 1813 1438.6262414…  192.168.1.5   192.168.1.1   ICMP        74 Echo (ping) request  id=0x0001, seq=292/9217, t
```

Open Wireshark on target Machine and check ARP Poisoning


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Source              Destination                Protocol Length Host  Info
  83 20.42.73.28         192.168.1.5                TLSv1.3  1466         Server Hello
  84 192.168.1.5         20.42.73.28                TCP        54         53050 → 443 [ACK] Seq=846 Ack=1512 Win=262144 Len=0
  85 20.42.73.28         192.168.1.5                TCP      1466         443 → 53050 [ACK] Seq=1512 Ack=846 Win=4194048 Len=1412 [TCP segment of a reassembled P
  86 20.42.73.28         192.168.1.5                TCP      1466         443 → 53050 [ACK] Seq=2924 Ack=846 Win=4194048 Len=1412 [TCP segment of a reassembled P
  87 20.42.73.28         192.168.1.5                TCP      1466         443 → 53050 [ACK] Seq=4336 Ack=846 Win=4194048 Len=1412 [TCP segment of a reassembled P
  88 20.42.73.28         192.168.1.5                TLSv1.3   729         Application Data
  89 192.168.1.5         20.42.73.28                TCP        54         53050 → 443 [ACK] Seq=846 Ack=6423 Win=262144 Len=0
  90 192.168.1.5         20.42.73.28                TLSv1.3   128         Application Data
  91 192.168.1.5         20.42.73.28                TLSv1.3   982         Application Data
  92 192.168.1.5         20.42.73.28                TCP      1466         53050 → 443 [ACK] Seq=1848 Ack=6423 Win=262144 Len=1412 [TCP segment of a reassembled P
  93 192.168.1.5         20.42.73.28                TCP      1466         53050 → 443 [ACK] Seq=3260 Ack=6423 Win=262144 Len=1412 [TCP segment of a reassembled P
  94 192.168.1.5         20.42.73.28                TLSv1.3   429         Application Data
  95 fe80::a3ca:29c4:b…  fe80::1                    ICMPv6     86         Neighbor Solicitation for fe80::1 from e0:0a:f6:6c:ef:33
  96 fe80::1             fe80::a3ca:29c4:bc73:27a7  ICMPv6     78         Neighbor Advertisement fe80::1 (rtr, sol)
  97 fe80::1             fe80::a3ca:29c4:bc73:27a7  ICMPv6     86         Neighbor Solicitation for fe80::a3ca:29c4:bc73:27a7 from 78:17:35:92:41:70
  98 fe80::a3ca:29c4:b…  fe80::1                    ICMPv6     86         Neighbor Advertisement fe80::a3ca:29c4:bc73:27a7 (sol, ovr) is at e0:0a:f6:6c:ef:33
  99 fe80::1             fe80::a00:27ff:fe0d:b74e   ICMPv6     86         Neighbor Solicitation for fe80::a00:27ff:fe0d:b74e from 78:17:35:92:41:70
 100 fe80::a00:27ff:fe…  fe80::1                    ICMPv6     78         Neighbor Advertisement fe80::a00:27ff:fe0d:b74e (sol)
 101 NokiaShangha_92:4…  LiteonTechno_6c:ef:33      ARP        60         Who has 192.168.1.5? Tell 192.168.1.1
 102 LiteonTechno_6c:e…  NokiaShangha_92:41:70      ARP        42         192.168.1.5 is at e0:0a:f6:6c:ef:33
 103 LiteonTechno_6c:e…  NokiaShangha_92:41:70      ARP        60         192.168.1.5 is at e0:0a:f6:6c:ef:33
 104 20.42.73.28         192.168.1.5                TCP        54         443 → 53050 [ACK] Seq=6423 Ack=1848 Win=4194816 Len=0
 105 20.42.73.28         192.168.1.5                TLSv1.3   157         Application Data
 106 20.42.73.28         192.168.1.5                TCP        54         443 → 53050 [ACK] Seq=6526 Ack=5047 Win=4194816 Len=0
 107 192.168.1.5         20.42.73.28                TCP        54         53050 → 443 [ACK] Seq=5047 Ack=6526 Win=261888 Len=0
 108 20.42.73.28         192.168.1.5                TLSv1.3   501         Application Data
 109 192.168.1.5         20.42.73.28                TCP        54         53050 → 443 [ACK] Seq=5047 Ack=6973 Win=261376 Len=0
```

```
> Frame 101: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{CB77C6C4-
> Ethernet II, Src: NokiaShangha_92:41:70 (78:17:35:92:41:70), Dst: LiteonTechno_6c:ef:33 (e0:0a:f6:6c:ef:
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: NokiaShangha_92:41:70 (78:17:35:92:41:70)
    Sender IP address: 192.168.1.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.5
```

```
0000  e0 0a f6 6c ef 33 78 17  35 92 41 70 08 06 00 01   ···l·3x· 5·Ap····
0010  08 00 06 04 00 01 78 17  35 92 41 70 c0 a8 01 01   ······x· 5·Ap····
0020  00 00 00 00 00 00 c0 a8  01 05 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```