Network Mapping (NMAP)

List of Content:

1. ARP: ARP (Address Resolution Protocol) is a network protocol used to map an IP address (Layer 3) to a MAC address (Layer 2) within a local network (LAN).

Works:

Sending ARP Request:

- The ARP Ping tool sends an ARP request to a specific IP address.
- This request asks: "Who has IP 192.168.1.104? Tell me your MAC address."

Receiving ARP Reply:

- If the target device is active, it replies with its MAC address.
- If the target device is offline, there will be no response.

Command for ARP ping

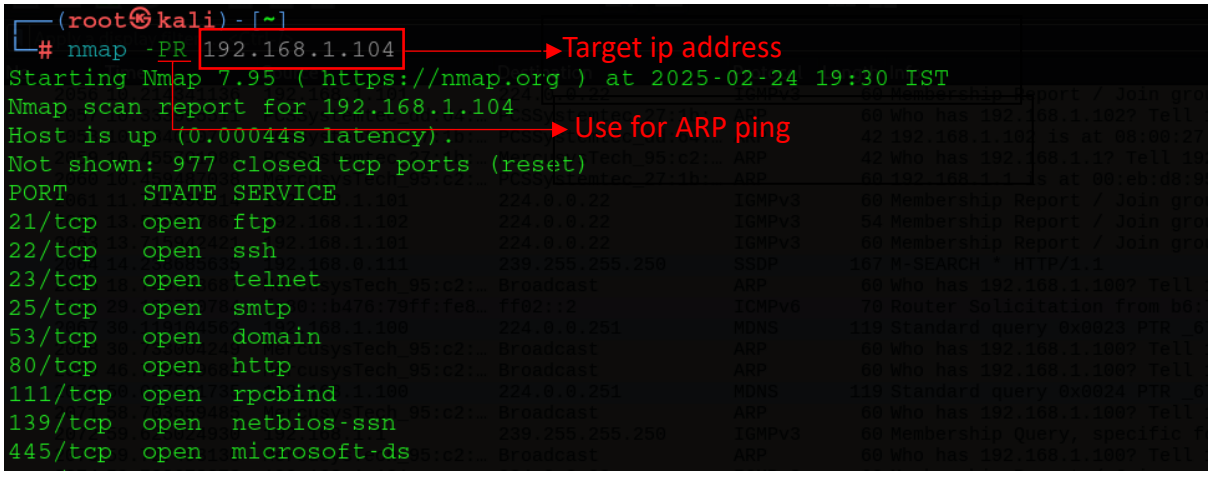
nmap -PR 192.168.1.104

where, nmap denotes network mapping

PR denotes **ARP Ping** (Address Resolution Protocol) to check if the target is alive.

192.168.1.104 is the target ip address.

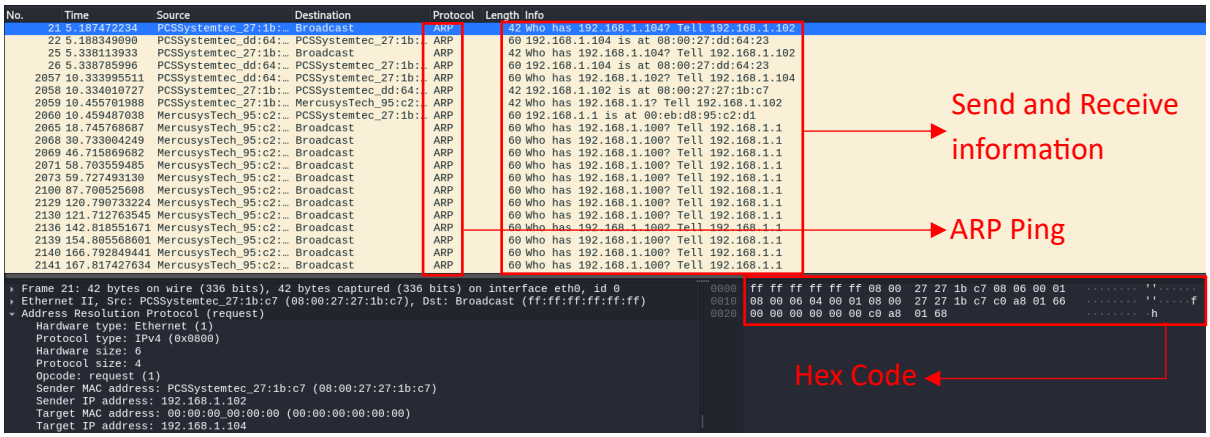
Example:




```
┌──(root㉿kali)-[~]
└─# nmap -PR 192.168.1.104
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-24 19:30 IST
Nmap scan report for 192.168.1.104
Host is up (0.00044s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
```

```
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:DD:64:23 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.73 seconds
```

Result:



2. ICMP Address Mask Ping

ICMP (Internet Control Message Protocol) operates at Layer 3 (Network Layer) of the OSI model and is primarily used for network troubleshooting and communication.

ICMP Address Mask Ping (ICMP Type 17 & 18)

ICMP “Address Mask Request” (Type 17) asks a router for its subnet mask. If allowed, the router replies with “Address Mask Reply” (Type 18) containing the subnet mask.

How it Works?

1 Host sends an ICMP Type 17 request (Address Mask Request).

2 If the router allows it, it replies with ICMP Type 18 (Address Mask Reply) containing the subnet mask (e.g., 255.255.255.0).

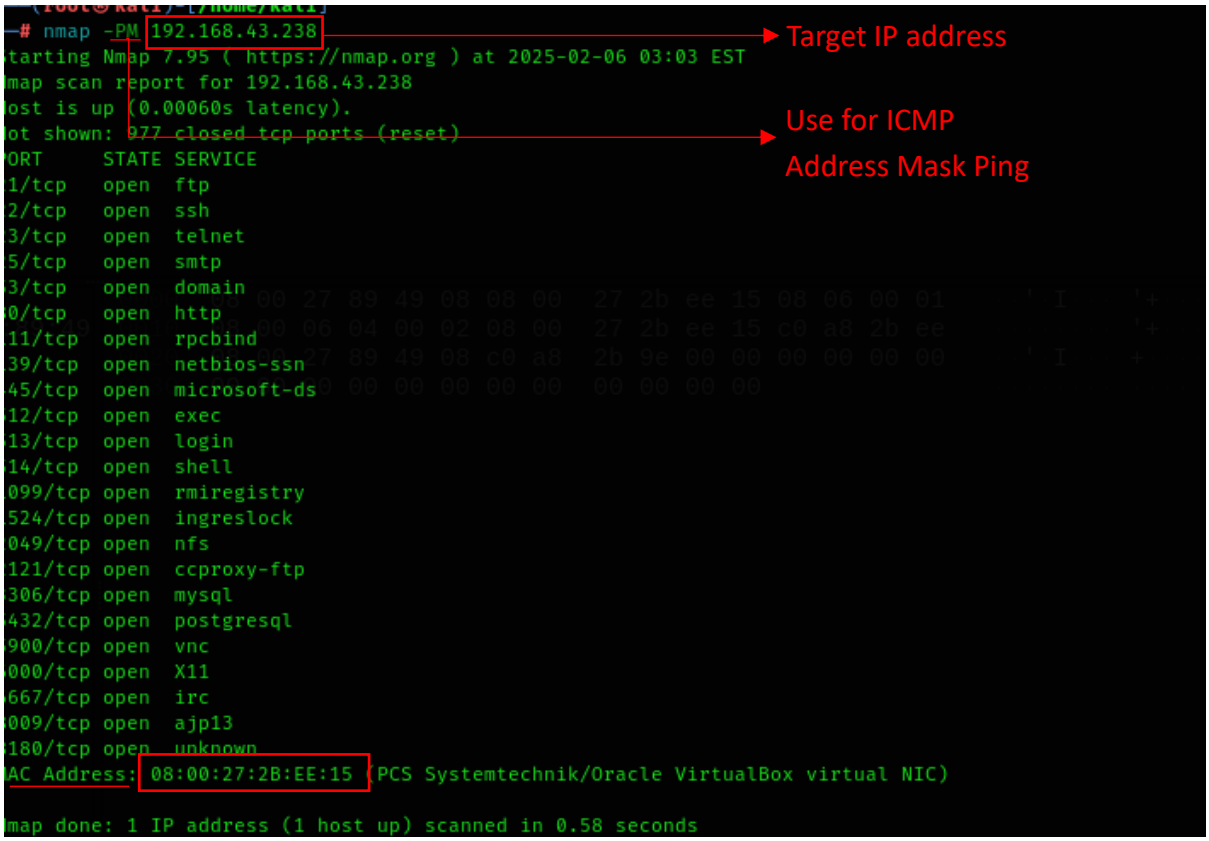
Command in Linux:

nmap -PM 192.168.1.1

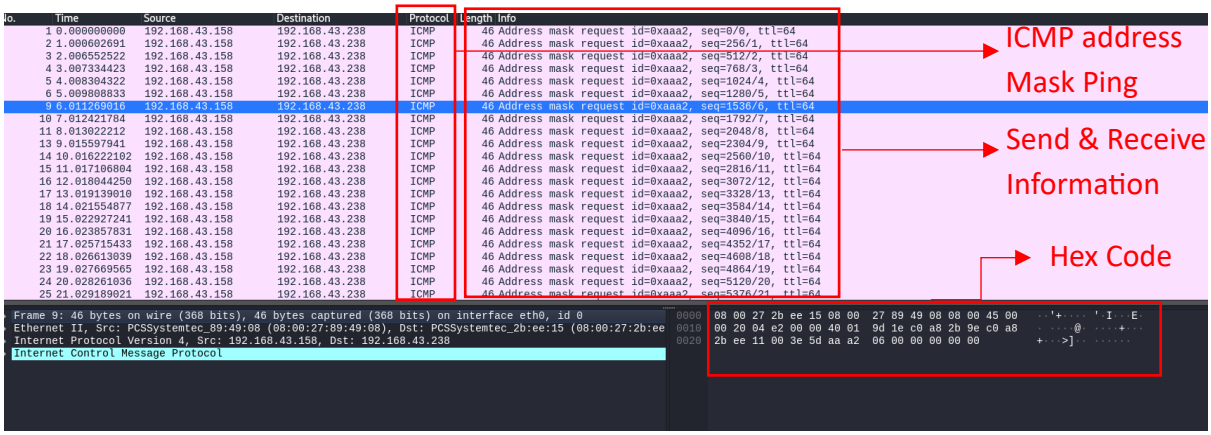
Where, nmap is network mapping.

-PM stands for ICMP Address Mask Ping.

Example:



Result:



3. ICMP Address Echo Ping:

Purpose: Checks if a device is online and measures response time.

How It Works:

1 Sender sends ICMP Echo Request (Type 8) to the target.

2Target replies with ICMP Echo Reply (Type 0) if it's reachable.

3Round-Trip Time (RTT) is measured for latency analysis.

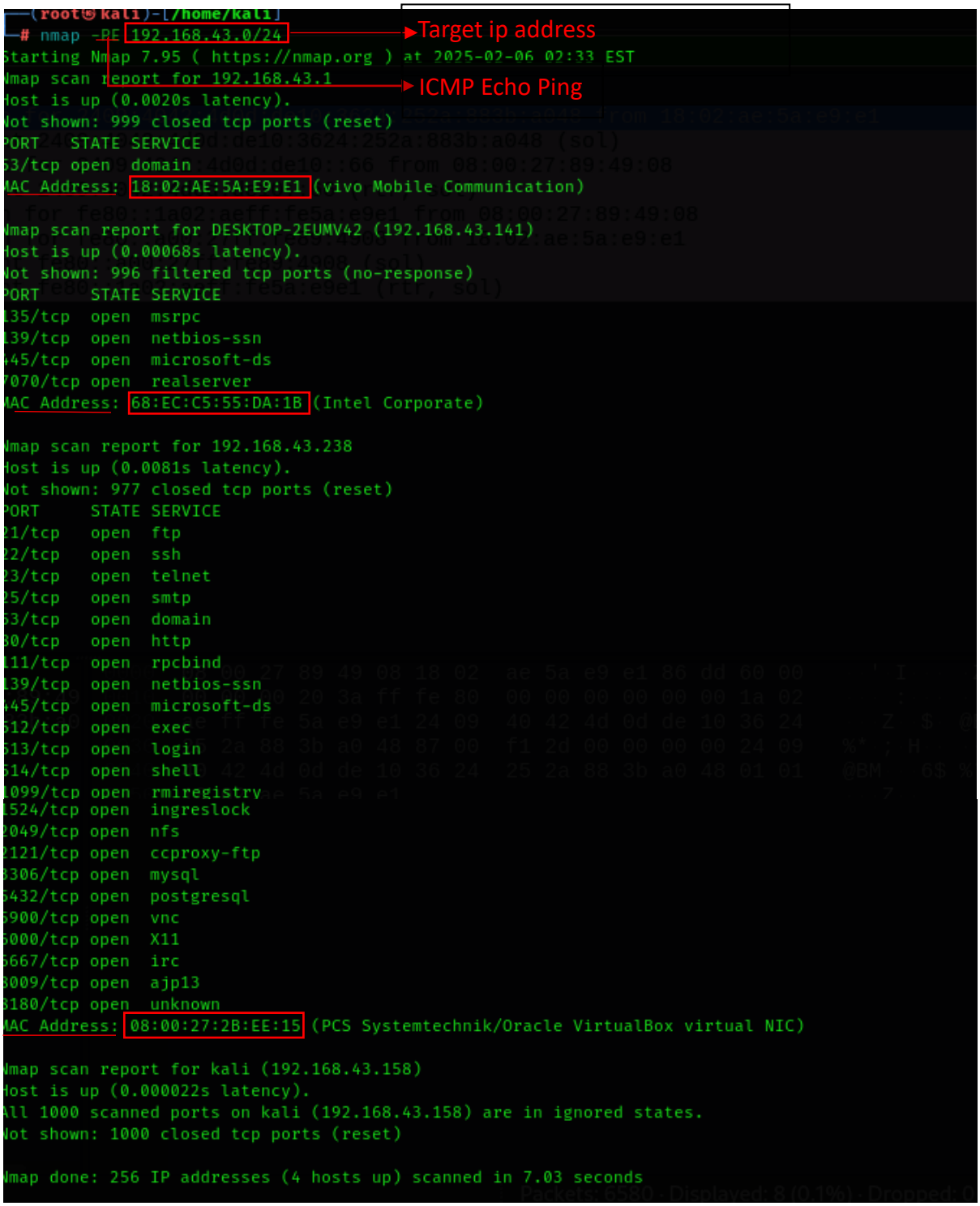
Command in Kali Linux:

nmap -PE 192.168.43.0

Where, nmap is network mapping.

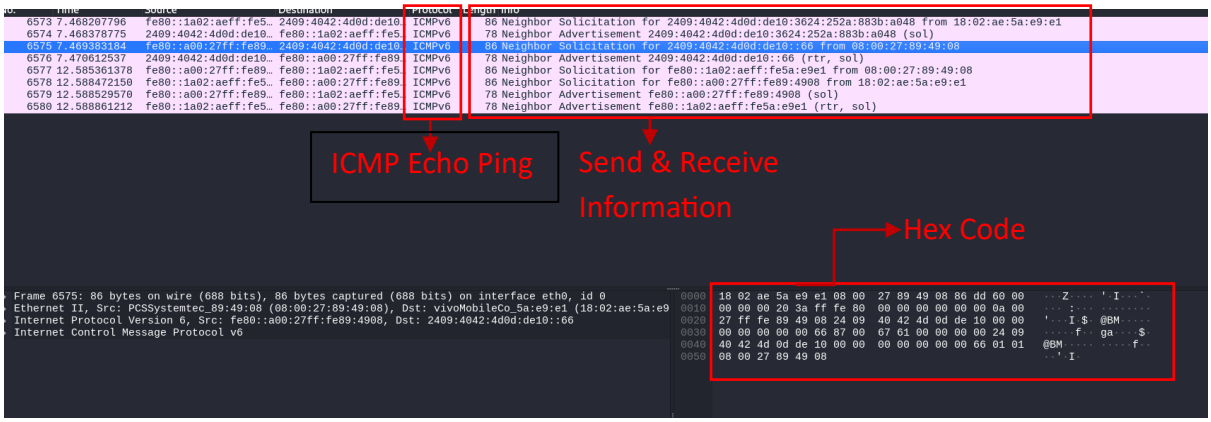
-PE stands for ICMP echo ping.

192.168.43.0 is a targeted ip address.




```
┌──(root㉿kali)-[/home/kali]
└─# nmap -PE 192.168.43.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-06 02:33 EST
Nmap scan report for 192.168.43.1
Host is up (0.0020s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 18:02:AE:5A:E9:E1 (vivo Mobile Communication)

Nmap scan report for DESKTOP-2EUMV42 (192.168.43.141)
Host is up (0.00068s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
7070/tcp open  realserver
MAC Address: 68:EC:C5:55:DA:1B (Intel Corporate)

Nmap scan report for 192.168.43.238
Host is up (0.0081s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:2B:EE:15 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for kali (192.168.43.158)
Host is up (0.000022s latency).
All 1000 scanned ports on kali (192.168.43.158) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 7.03 seconds
```

Result:



4. ICMP Timestamp Ping:

ICMP Timestamp Request (Type 13) asks a device for the current time. If allowed, the device responds with Type 14 (Timestamp Reply) containing the time in milliseconds since midnight UTC.

How it Works?

1 Host sends an ICMP Type 13 request (Timestamp Request).

2 If the target allows it, it replies with ICMP Type 14 (Timestamp Reply) containing the system timestamp.

Command in Kali Linux:

nmap -PP 192.168.43.0

where, nmap is network mapping.

-PP stands for Timestamp Ping.

192.168.43.0 is targeted ip address.

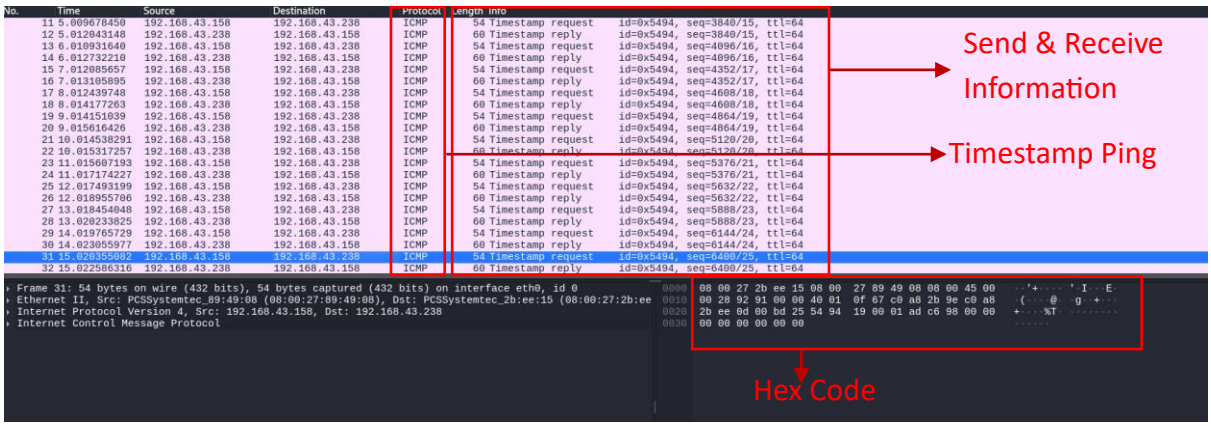
Example:

```
—# nmap -PP 192.168.43.0/24
tarting Nmap 7.95 ( https://nmap.org ) at 2025-02-06 02:42 EST
lmap scan report for 192.168.43.1
lost is up (0.0019s latency).
lot shown: 999 closed tcp ports (reset)
ORT   STATE SERVICE
3/tcp open  domain
AC Address: 18:02:AE:5A:E9:E1 (vivo Mobile Communication)

lmap scan report for DESKTOP-2EUMV42 (192.168.43.141)
lost is up (0.0011s latency).
lot shown: 996 filtered tcp ports (no-response)
ORT   STATE SERVICE
35/tcp  open  msrpc
39/tcp  open  netbios-ssn
45/tcp  open  microsoft-ds
070/tcp open  realserver
AC Address: 68:EC:C5:55:DA:1B (Intel Corporate)

lmap scan report for 192.168.43.238
lost is up (0.0015s latency).
lot shown: 977 closed tcp ports (reset)
ORT   STATE SERVICE
1/tcp   open  ftp
2/tcp   open  ssh
3/tcp   open  telnet
5/tcp   open  smtp
3/tcp   open  domain
0/tcp   open  http
11/tcp  open  rpcbind
39/tcp  open  netbios-ssn
45/tcp  open  microsoft-ds
12/tcp  open  exec
13/tcp  open  login
14/tcp  open  shell
099/tcp open  rmiregistry
524/tcp open  ingreslock
049/tcp open  nfs
121/tcp open  ccproxy-ftp
306/tcp open  mysql
432/tcp open  postgresql
900/tcp open  vnc
000/tcp open  X11
667/tcp open  irc
009/tcp open  ajp13
180/tcp open  unknown
AC Address: 08:00:27:2B:EE:15 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

lmap scan report for kali (192.168.43.158)
lost is up (0.000071s latency).
ll 1000 scanned ports on kali (192.168.43.158) are in ignored states.
lot shown: 1000 closed tcp ports (reset)
```

Target ip address

Timestamp Ping

Result:



5. Perform a Ping Scan Only:

A ping scan is used to find live (online) hosts in a network without scanning ports.

Works:

1 Sends ICMP Echo Requests (Ping) to target hosts.

2 Waits for ICMP Echo Replies from active devices.

3 Lists only live hosts (ignores unresponsive ones).

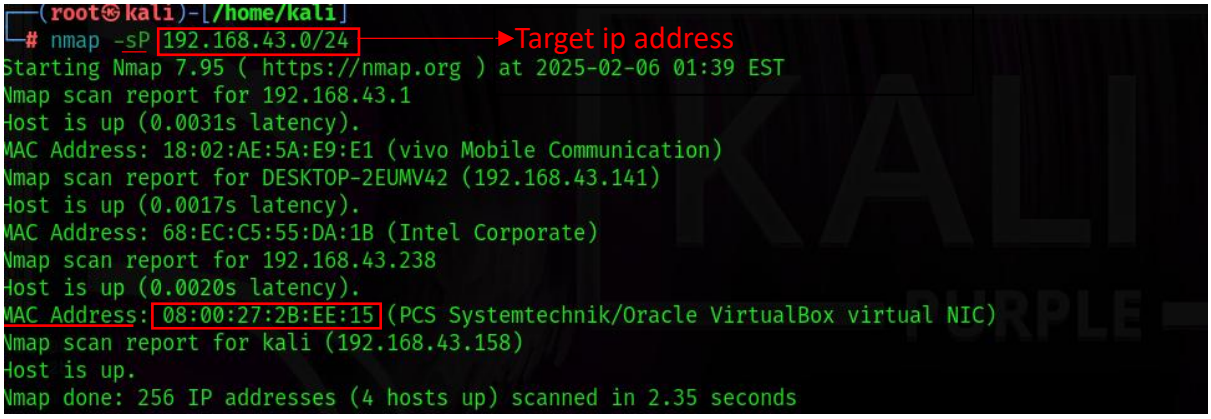
Command in Kali Linux:

nmap -sP 192.168.43.0

where, nmap is network mapping.

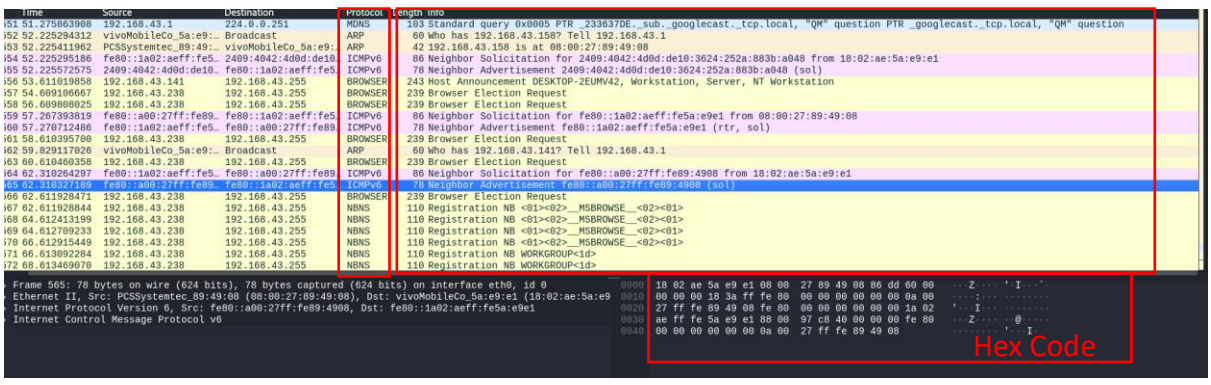
-sP stands for Pin Scan.

192.168.43.0 is a targeted ip address.**Example:**




```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sP 192.168.43.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-06 01:39 EST
Nmap scan report for 192.168.43.1
Host is up (0.0031s latency).
MAC Address: 18:02:AE:5A:E9:E1 (vivo Mobile Communication)
Nmap scan report for DESKTOP-2EUMV42 (192.168.43.141)
Host is up (0.0017s latency).
MAC Address: 68:EC:C5:55:DA:1B (Intel Corporate)
Nmap scan report for 192.168.43.238
Host is up (0.0020s latency).
MAC Address: 08:00:27:2B:EE:15 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for kali (192.168.43.158)
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.35 seconds
```

Result:



6. TCP ACK Ping:

TCP ACK Ping (-PA) is a technique used by Nmap to detect live hosts by sending TCP ACK packets instead of ICMP Echo Requests.

Works:

- Nmap sends a TCP ACK packet to the target.
- If the target is alive, it responds with TCP RST (Reset) (since no connection exists).
- If no response, the target is either offline or blocking packets.
- Bypasses ICMP filtering, useful when ICMP ping is blocked by firewalls.

Command in Kali Linux:

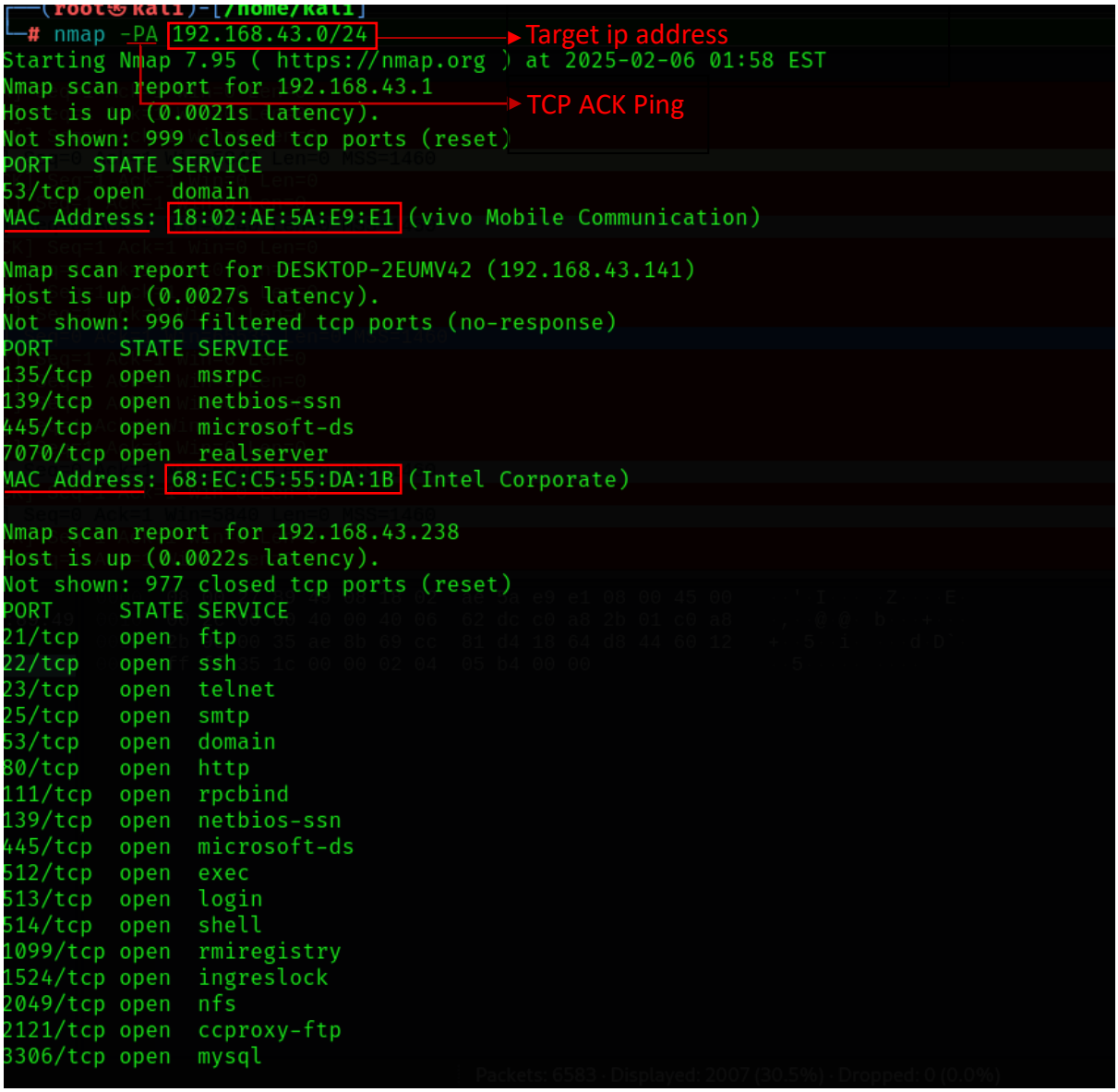
nmap -PA 192.168.43.0/24

Where, nmap is network mapping

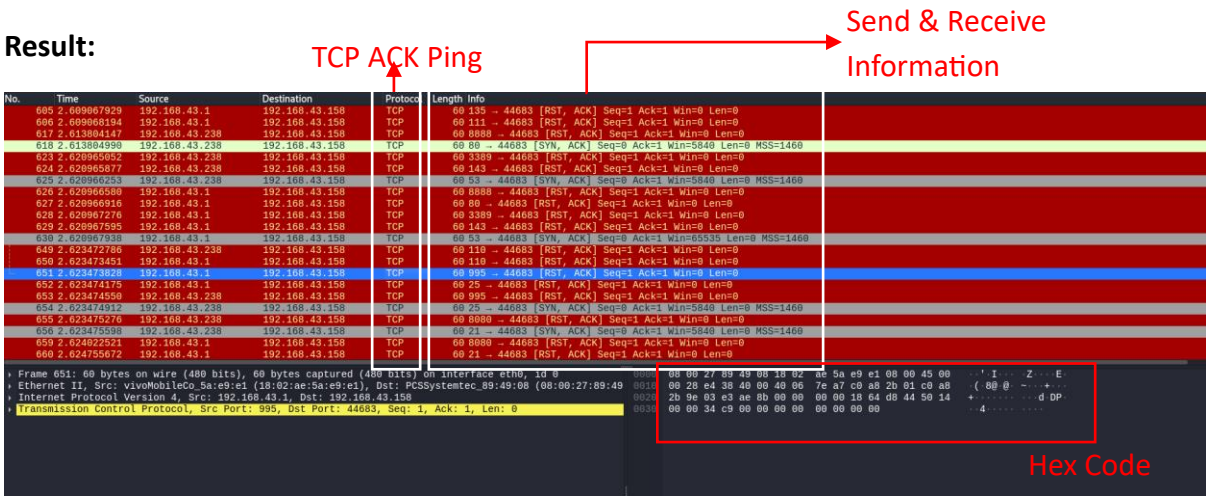
-PA stands for TCP ACK Ping.

Here 192.168.43.0 is a target ip address.

Example:



Result:



7. TCP SYN Ping:

TCP SYN Ping (-PS) is a host discovery technique used by Nmap to check if a system is alive by sending TCP SYN packets instead of ICMP pings.

Works:

Works:

Sends a TCP SYN Packet: Nmap sends a SYN packet to a target port.

Receives a Response: SYN-ACK: Indicates the port is open and the host is alive.

RST (Reset): Indicates the port is closed, but the host is still up.

No Response: May mean the host is down or blocking the probe.

Command I Kali Linux:

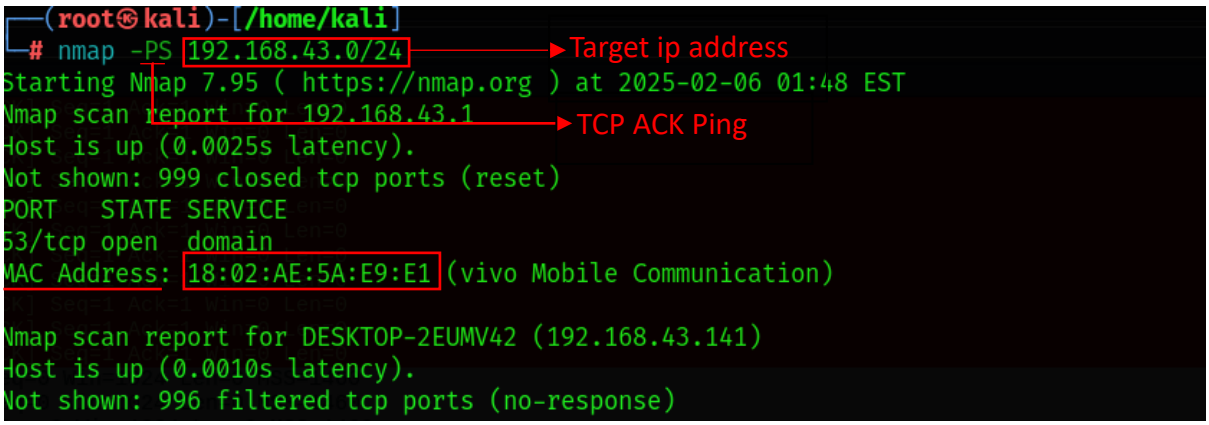
nmap -PS 192.168.43.0

Where, nmap is network mapping.

-PS stands for TCP ACK Ping.

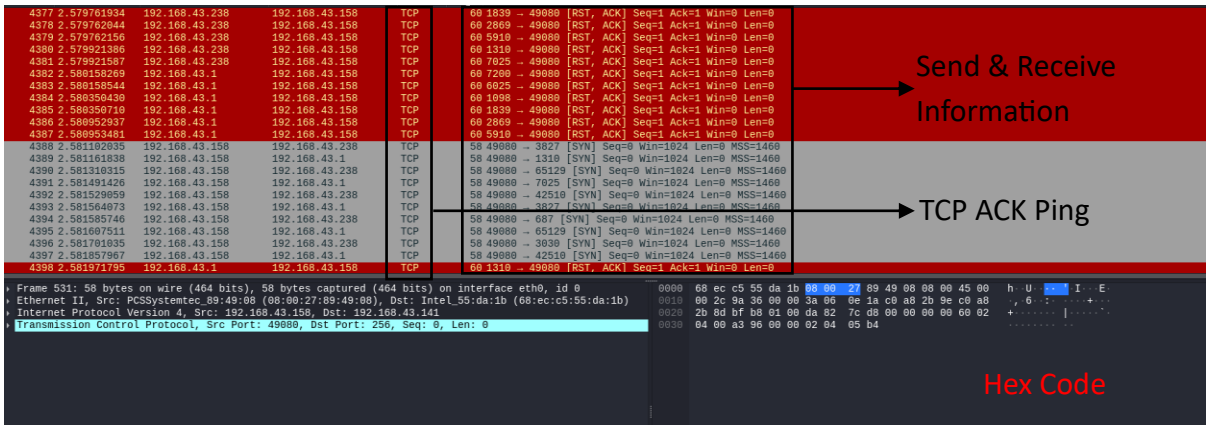
Here 192.168.43.0 is a target ip address.

Example:



```
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
7070/tcp open  realserver
MAC Address: 68:EC:C5:55:DA:1B (Intel Corporate)

Nmap scan report for 192.168.43.238
Host is up (0.0018s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
```

Result:



8. UDP Ping:

UDP Ping is a network scanning technique used to determine if a host is online by sending UDP packets to a target port.

Works:

Sends a UDP Packet: A UDP packet is sent to a specific port on the target host.

Response Received: ICMP "Port Unreachable" reply indicates the host is up if the port is closed.

No Response: Could mean the port is open/filtered or the host is down.

Command in Kali Linux:

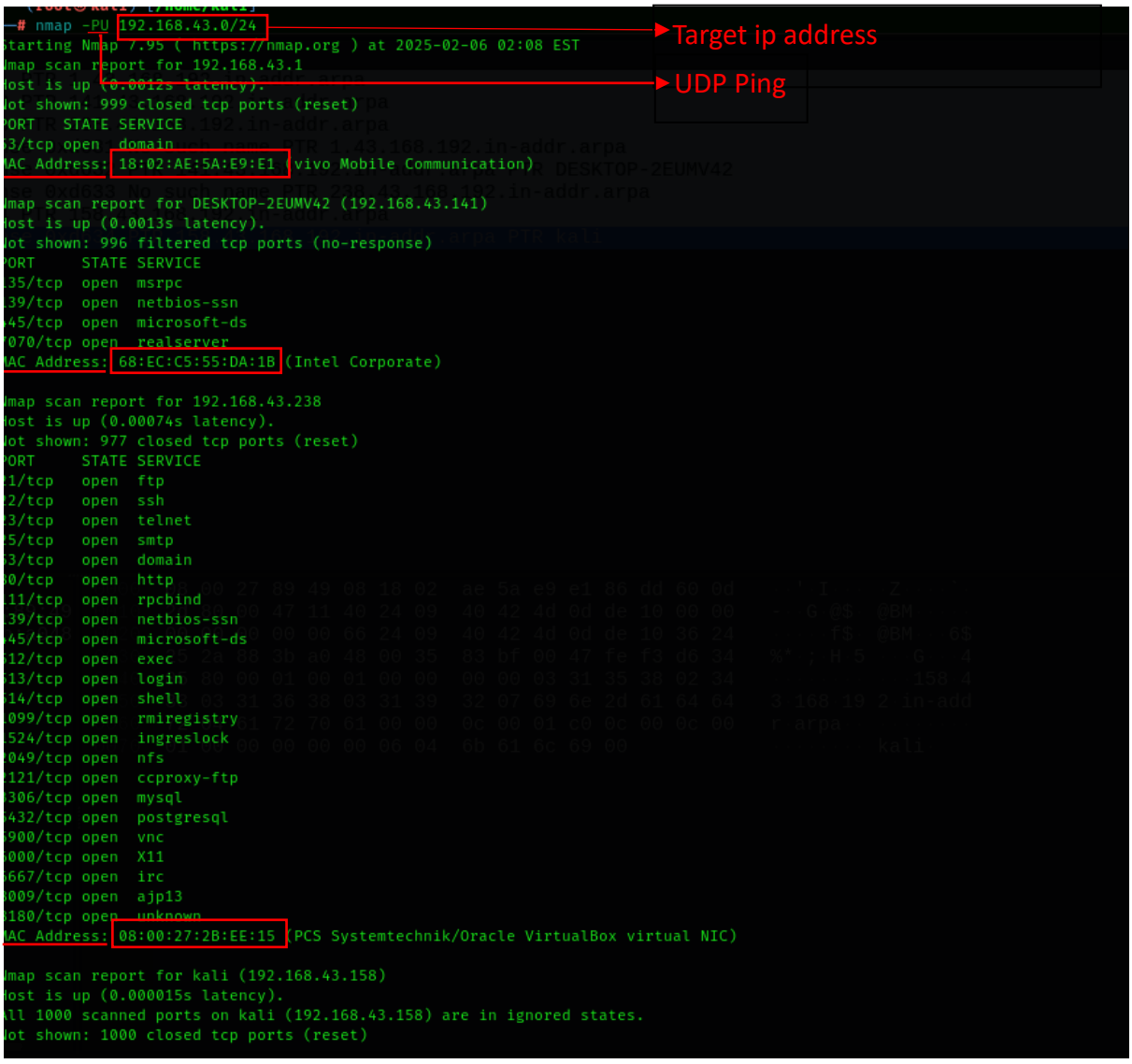
Nmap -PU 192.168.43.0

Where, nmap is network mapping

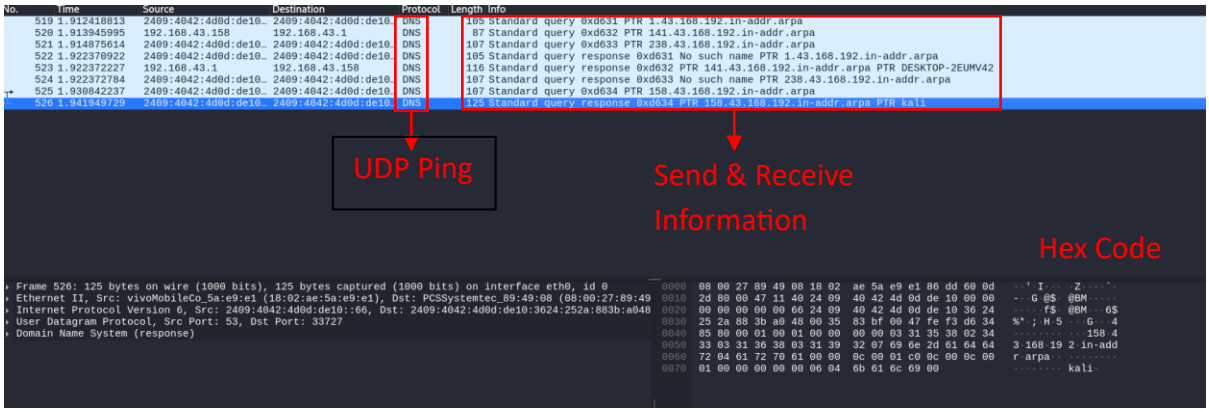
-PU stand for UDP Ping.

192.168.43.0 is a target ip address.

Example:



Result:


No. Time Source Destination Protocol Length Info
519 1.912418813 2409:4042:4d0d:de10… 2409:4042:4d0d:de10… DNS 105 Standard query 0xd631 PTR 1.43.168.192.in-addr.arpa
520 1.913945995 192.168.43.158 192.168.43.1 DNS 87 Standard query 0xd632 PTR 141.43.168.192.in-addr.arpa
521 1.914875614 2409:4042:4d0d:de10… 2409:4042:4d0d:de10… DNS 107 Standard query 0xd633 PTR 238.43.168.192.in-addr.arpa
522 1.922370922 2409:4042:4d0d:de10… 2409:4042:4d0d:de10… DNS 105 Standard query response 0xd631 No such name PTR 1.43.168.192.in-addr.arpa
523 1.922372227 192.168.43.1 192.168.43.158 DNS 116 Standard query response 0xd632 PTR 141.43.168.192.in-addr.arpa PTR DESKTOP-2EUMV42
524 1.922372784 2409:4042:4d0d:de10… 2409:4042:4d0d:de10… DNS 107 Standard query response 0xd633 No such name PTR 238.43.168.192.in-addr.arpa
525 1.930842237 2409:4042:4d0d:de10… 2409:4042:4d0d:de10… DNS 107 Standard query 0xd634 PTR 158.43.168.192.in-addr.arpa
526 1.941949729 2409:4042:4d0d:de10… 2409:4042:4d0d:de10… DNS 125 Standard query response 0xd634 PTR 158.43.168.192.in-addr.arpa PTR kali
UDP Ping
Send & Receive Information
Hex Code
Frame 526: 125 bytes on wire (1000 bits), 125 bytes captured (1000 bits) on interface eth0, id 0
Ethernet II, Src: vivoMobileCo_5a:e9:e1 (18:02:ae:5a:e9:e1), Dst: PCSSystemtec_89:49:08 (08:00:27:89:49
Internet Protocol Version 6, Src: 2409:4042:4d0d:de10::66, Dst: 2409:4042:4d0d:de10:3624:252a:883b:a048
User Datagram Protocol, Src Port: 53, Dst Port: 33727
Domain Name System (response)
0000 08 00 27 89 49 08 18 02 ae 5a e9 e1 86 dd 60 0d
0010 2d 80 00 47 11 40 24 09 40 42 4d 0d de 10 00 00
0020 00 00 00 00 00 66 24 09 40 42 4d 0d de 10 36 24
0030 25 2a 88 3b a0 48 00 35 83 bf 00 47 fe f3 d6 34
0040 85 80 00 01 00 01 00 00 00 00 03 31 35 38 02 34
0050 33 03 31 36 38 03 31 39 32 07 69 6e 2d 61 64 64
0060 72 04 61 72 70 61 00 00 0c 00 01 c0 0c 00 0c 00
0070 01 00 00 00 00 00 06 04 6b 61 6c 69 00