**Network Mapping (NMAP)**

List of Content:

1. ARP Ping
2. ICMP Address Mask Ping
3. ICMP Echo Ping
4. ICMP Timestamp Ping
5. Ping Scan
6. TCP ACK Ping
7. TCP SYN Ping
8. UDP Ping

**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.

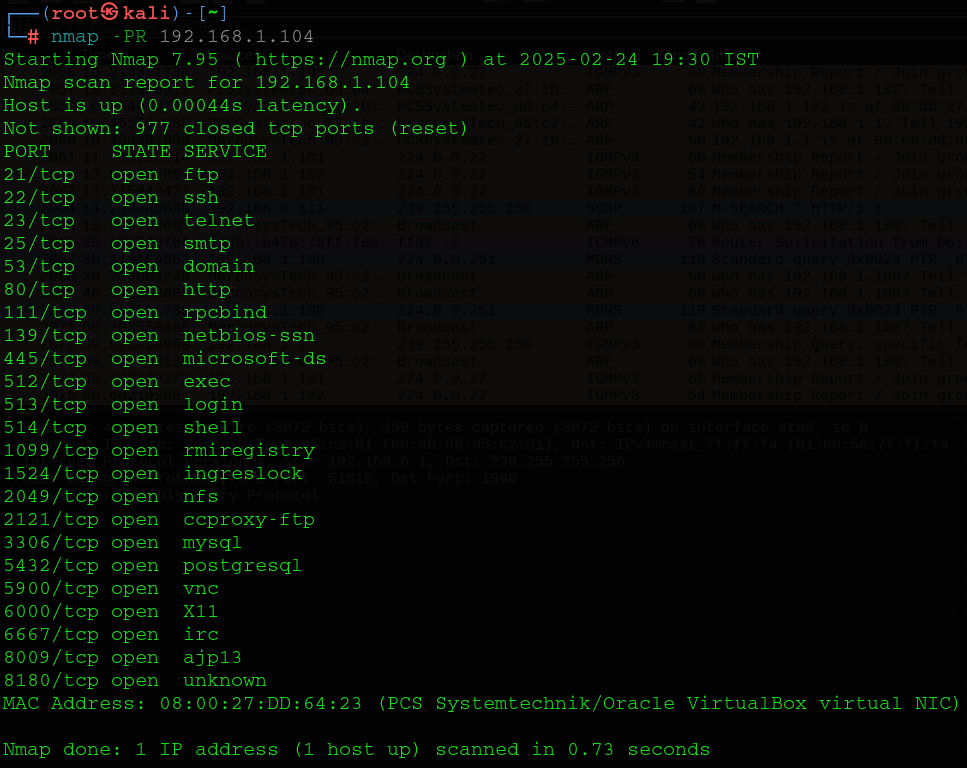
**Command for ARP ping**

nmap -PR 192.168.1.104

where, nmap denotes network mapping

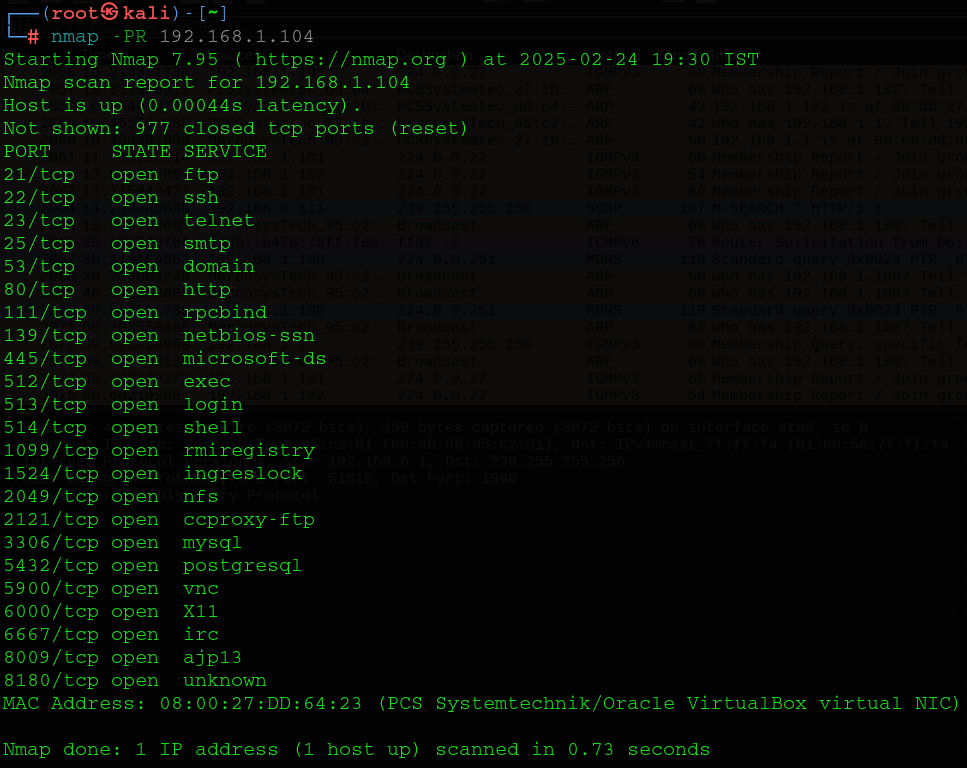
PR denotes **ARP Ping** (Address Resolution Protocol) to check if the target is alive.

192.168.1.104 is the target ip address.

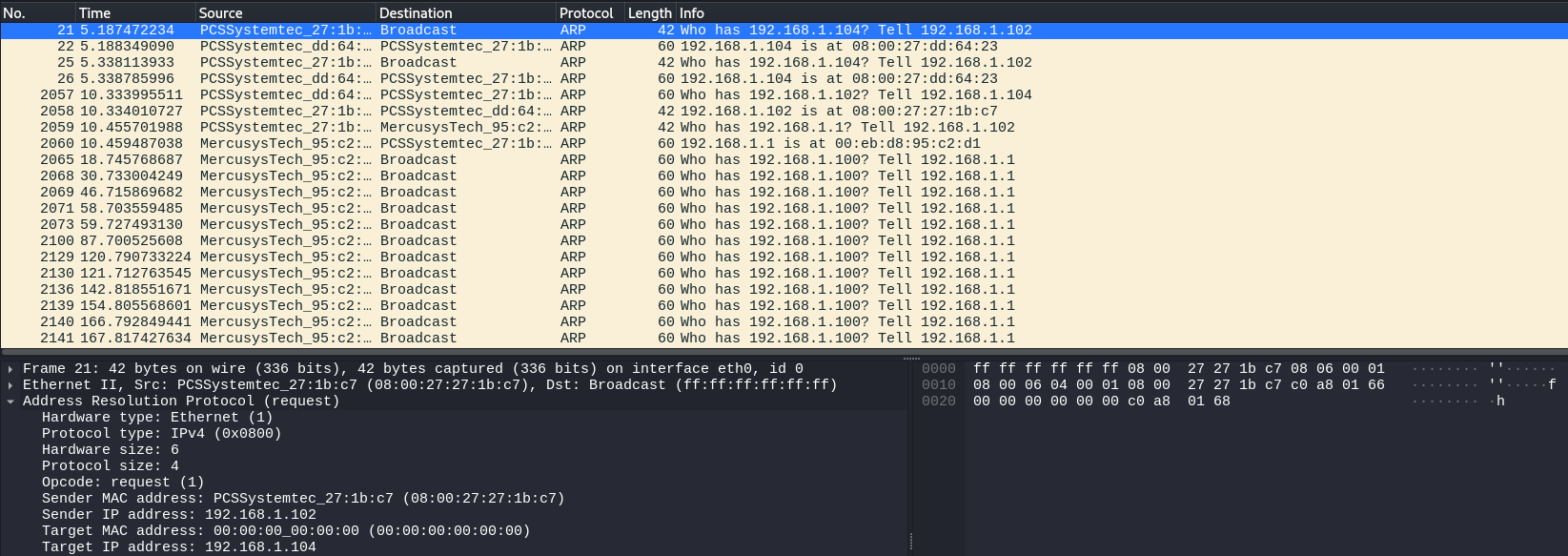
**Example:**

Target ip address

Use for ARP ping

****

**Result:**



Send and Receive information

ARP Ping

Hex Code

**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?**

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

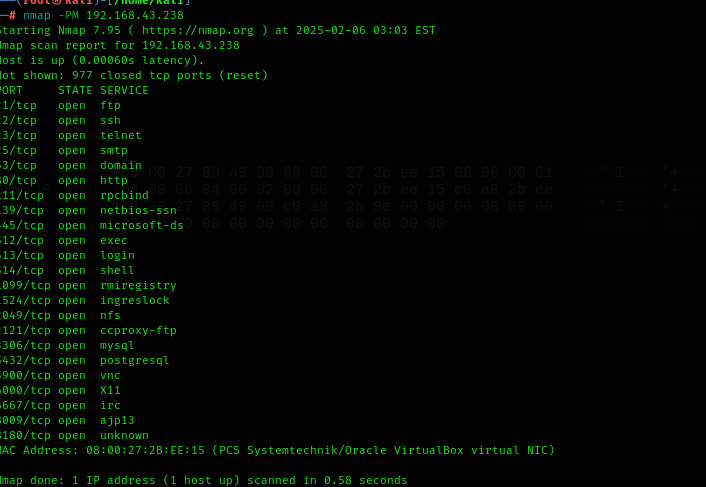
2️ If the router allows it, it replies with ICMP Type 18 (Address Mask Reply) containing the subnet mask (e.g., 255.255.255.0).

**Command in Linux:**

nmap -PM 192.168.1.1

Where, nmap is network mapping.

-PM stands for ICMP Address Mask Ping.

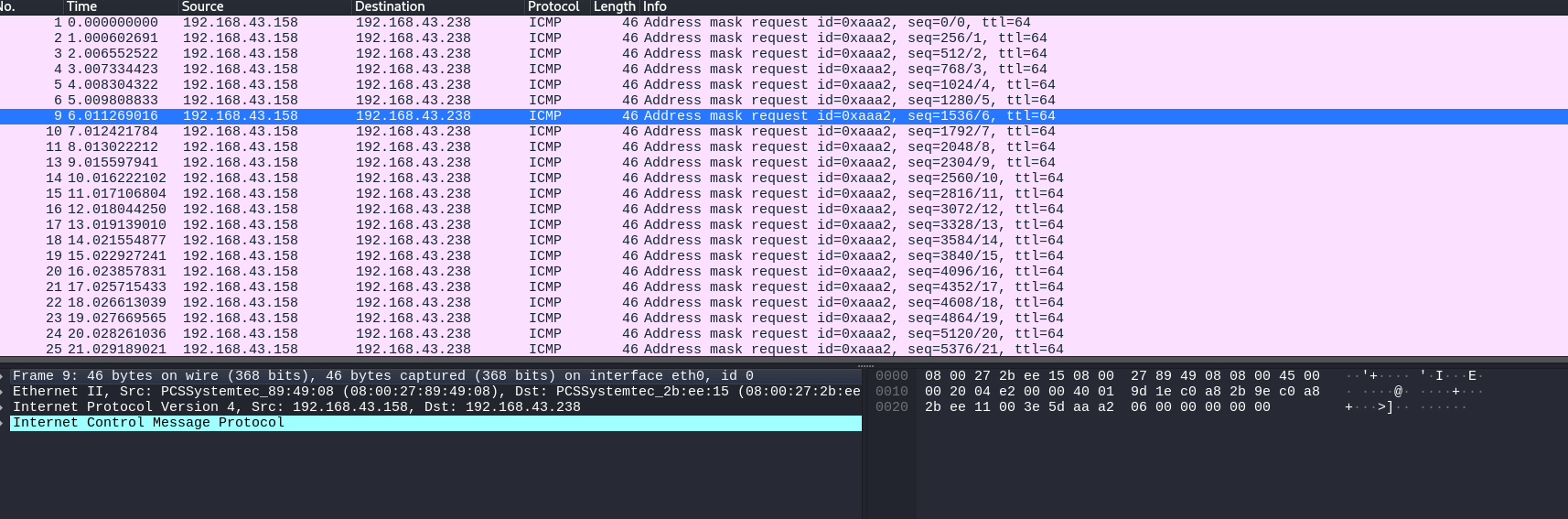
Example:

Target IP address

Use for ICMP Address Mask Ping

**Result:**

ICMP address Mask Ping

****

Send & Receive Information

Hex Code

**3. ICMP Address Echo Ping:**

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

How It Works:

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

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

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

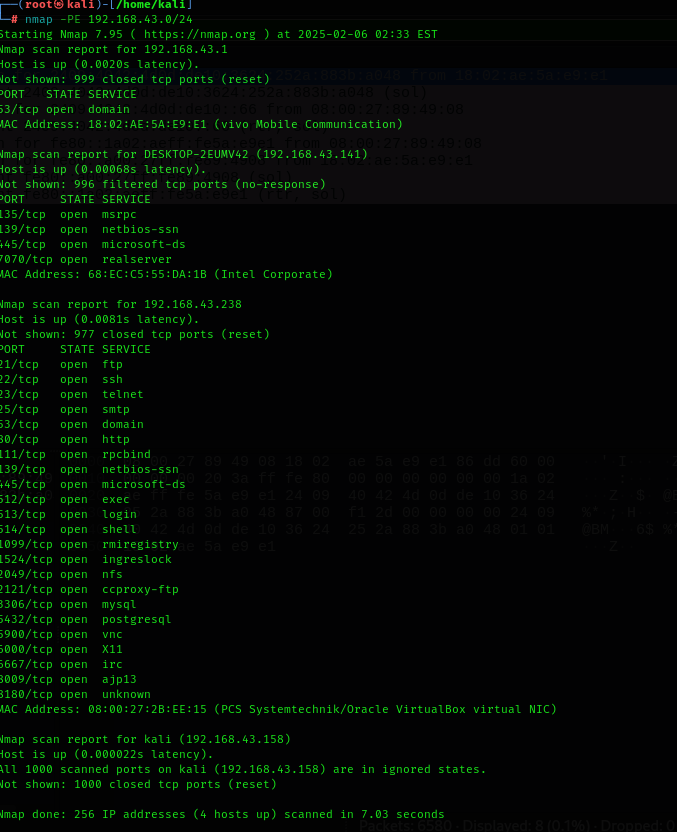
**Command in Kali Linux:**

nmap -PE 192.168.43.0

Where, nmap is network mapping.

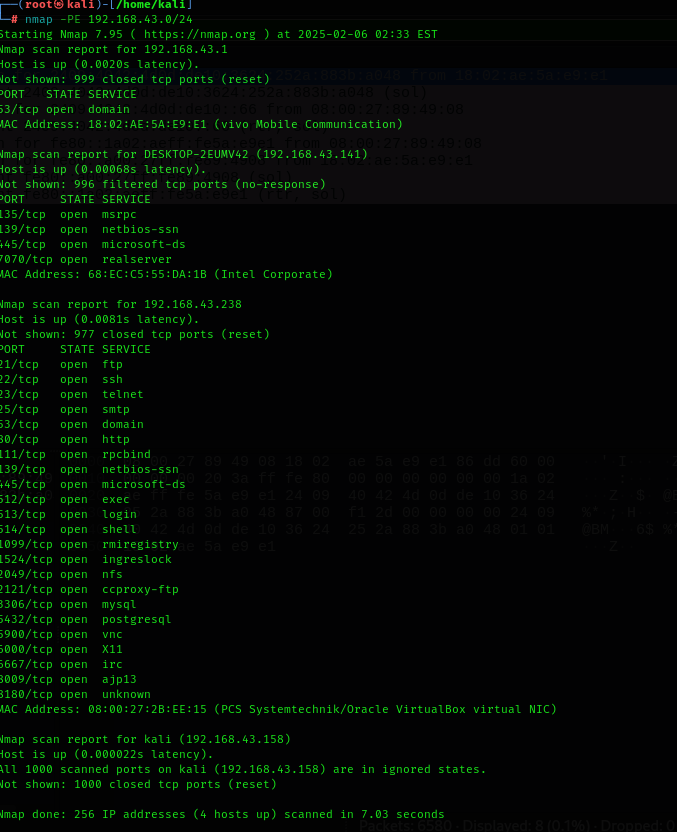
-PE stands for ICMP echo ping.

192.168.43.0 is a targeted ip address.

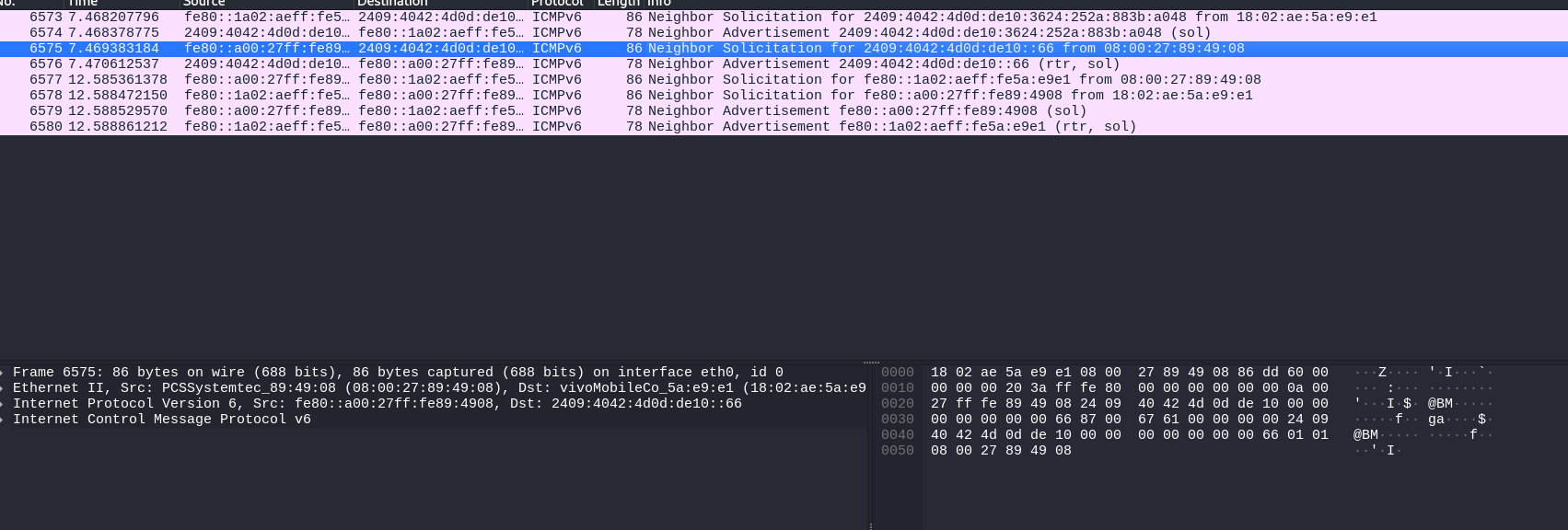


Target ip address

ICMP Echo Ping



**Result:**



ICMP Echo Ping

Send & Receive Information

Hex Code

**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?**

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

2️ 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

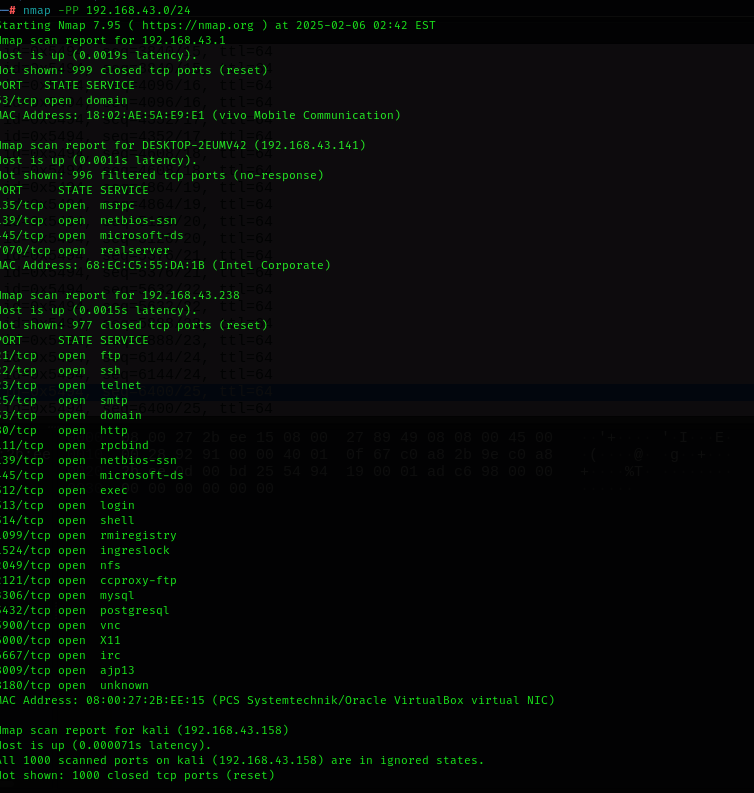
where, nmap is network mapping.

-PP stands for Timestamp Ping.

192.168.43.0 is targeted ip address.

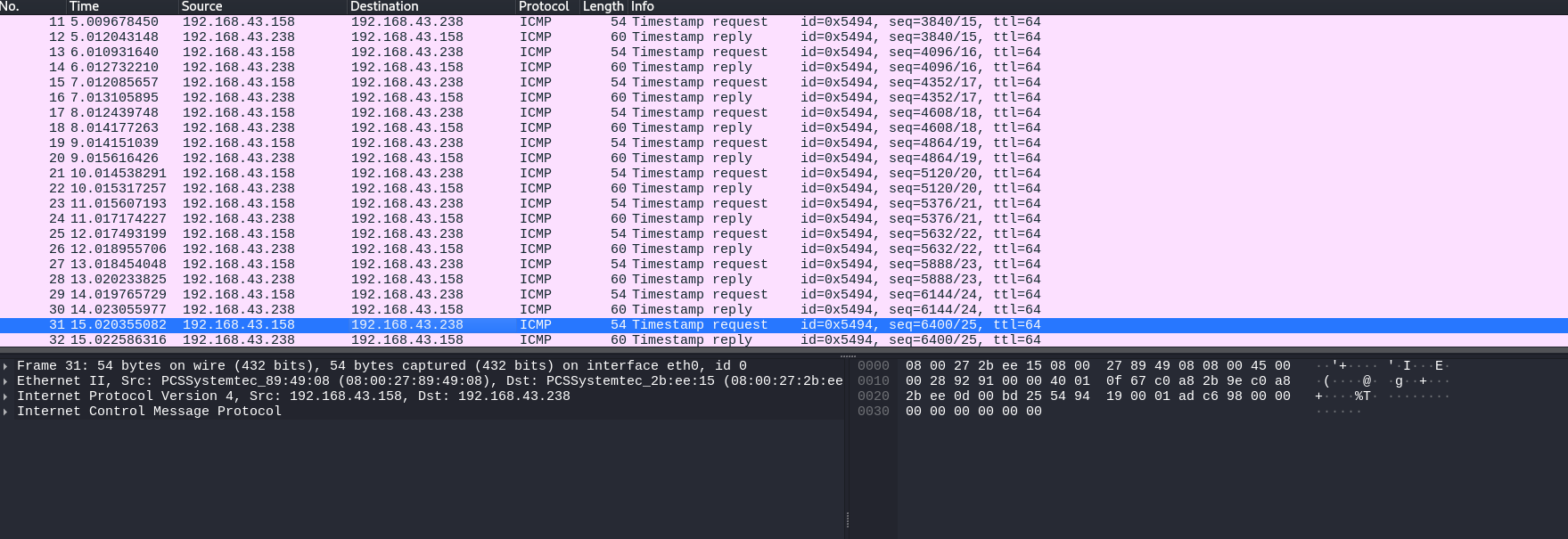
**Example:**

Target ip address



Timestamp Ping

**Result:**

****

Send & Receive Information

Timestamp Ping

Hex Code

**5. Perform a Ping Scan Only:**

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

**Works:**

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

2️ Waits for ICMP Echo Replies from active devices.

3️ Lists only live hosts (ignores unresponsive ones).

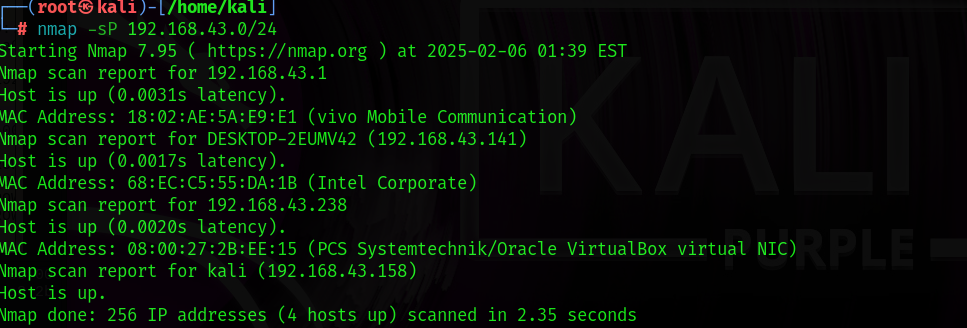
**Command in Kali Linux:**

nmap -sP 192.168.43.0

where, nmap is network mapping.

-sP stands for Pin Scan.

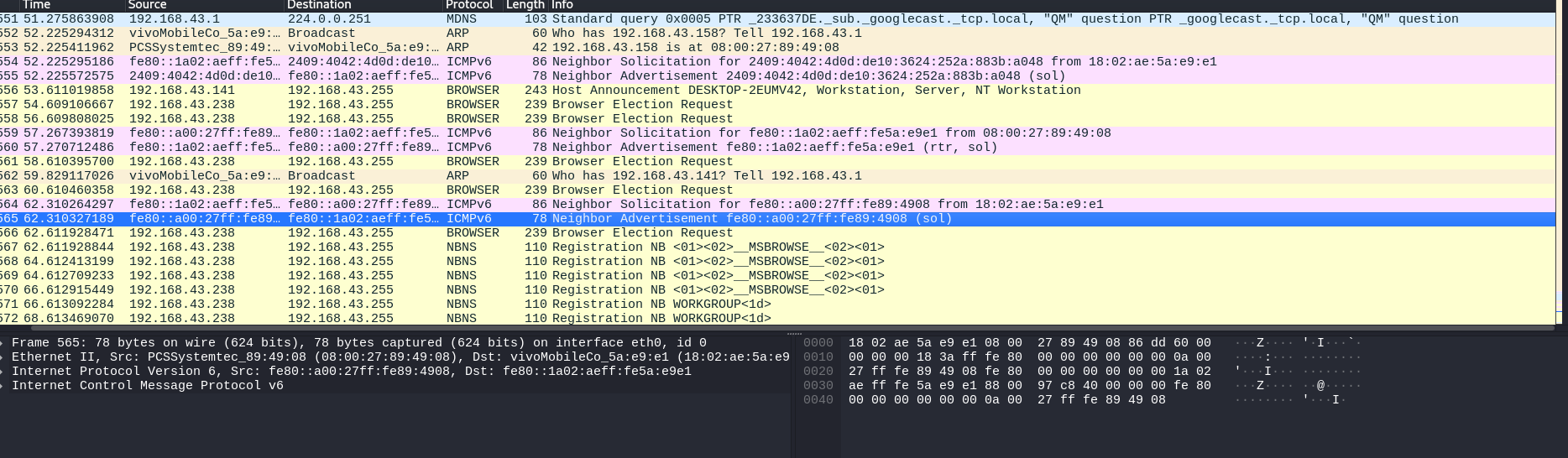
192.168.43.0 is a targeted ip address.**Example:**



Target ip address

Send & Receive Information

**Result:**

****

Hex Code

**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.

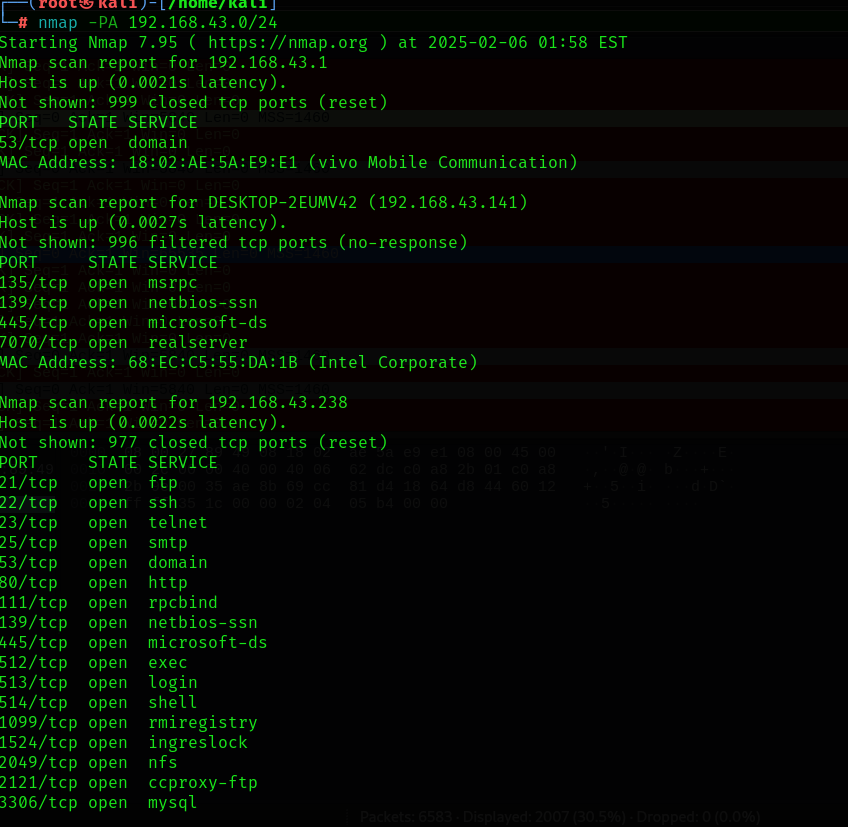
**Command in Kali Linux:**

nmap -PA 192.168.43.0/24

Where, nmap is network mapping

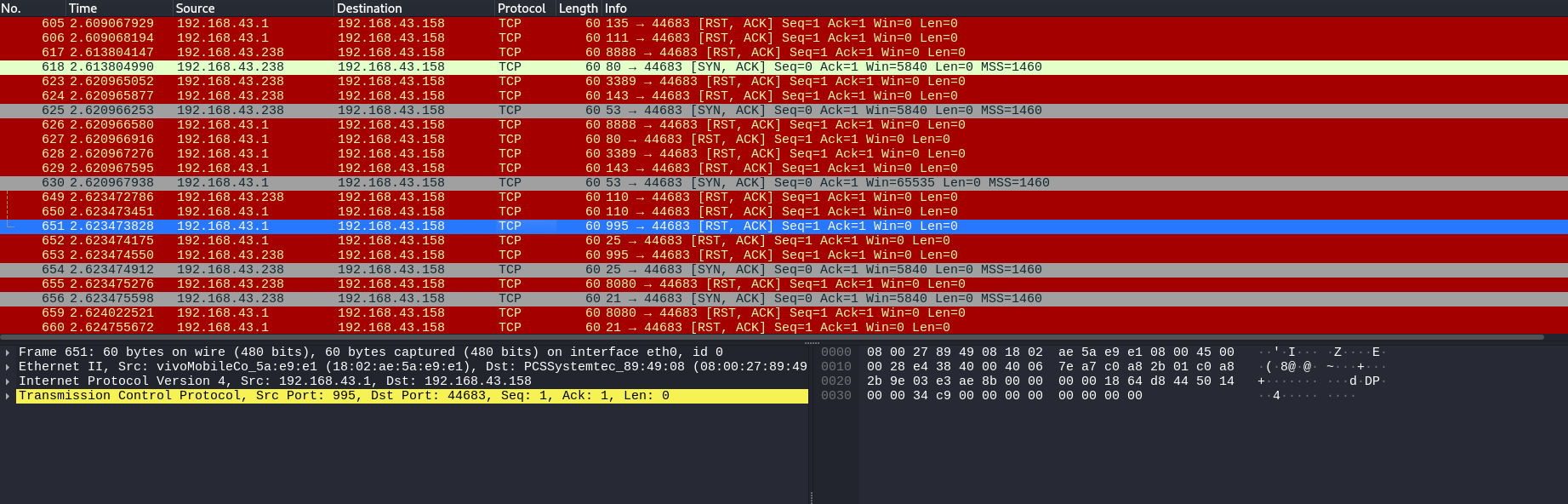
-PA stands for TCP ACK Ping.

Here 192.168.43.0 is a target ip address.

**Example:**

Target ip address

TCP ACK Ping

**Result:**

TCP ACK Ping

Send & Receive Information

Hex Code

**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:**

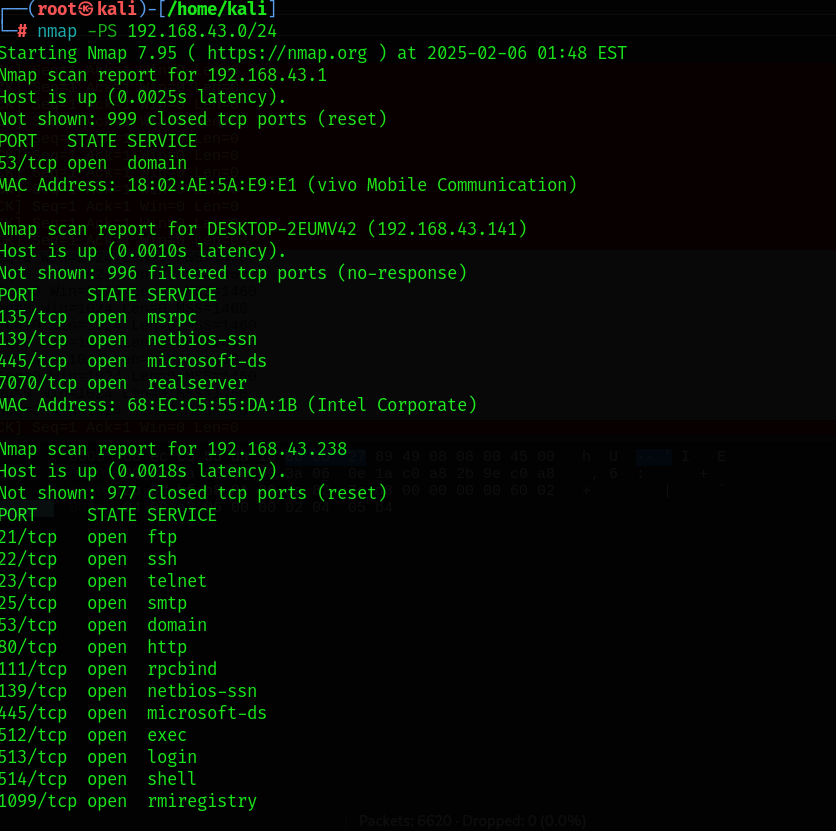
nmap -PS 192.168.43.0

Where, nmap is network mapping.

-PS stands for TCP ACK Ping.

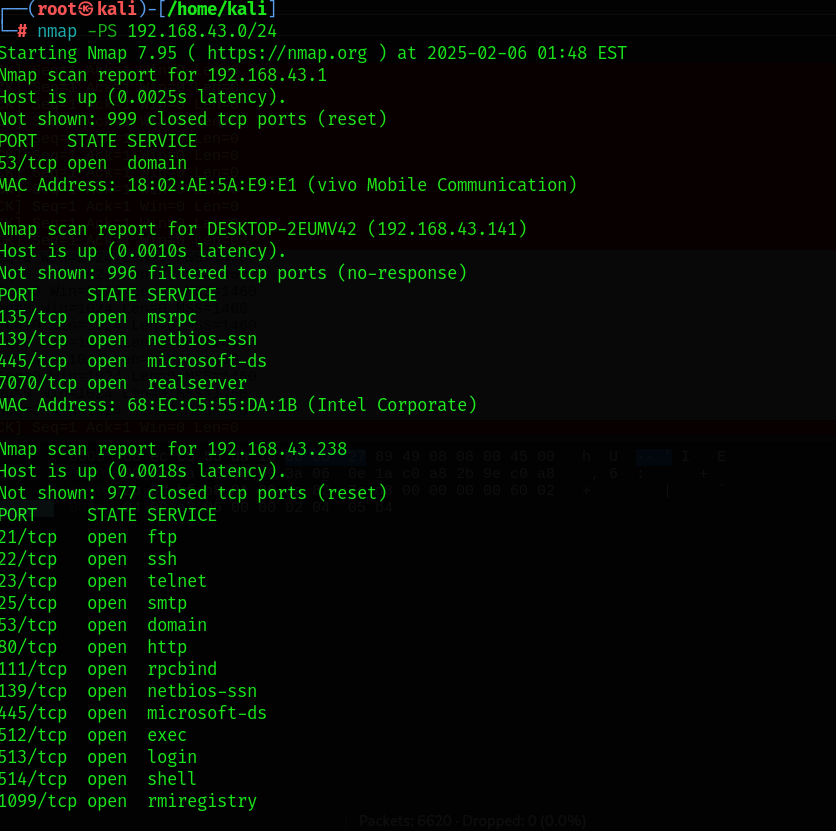
Here 192.168.43.0 is a target ip address.

**Example:**

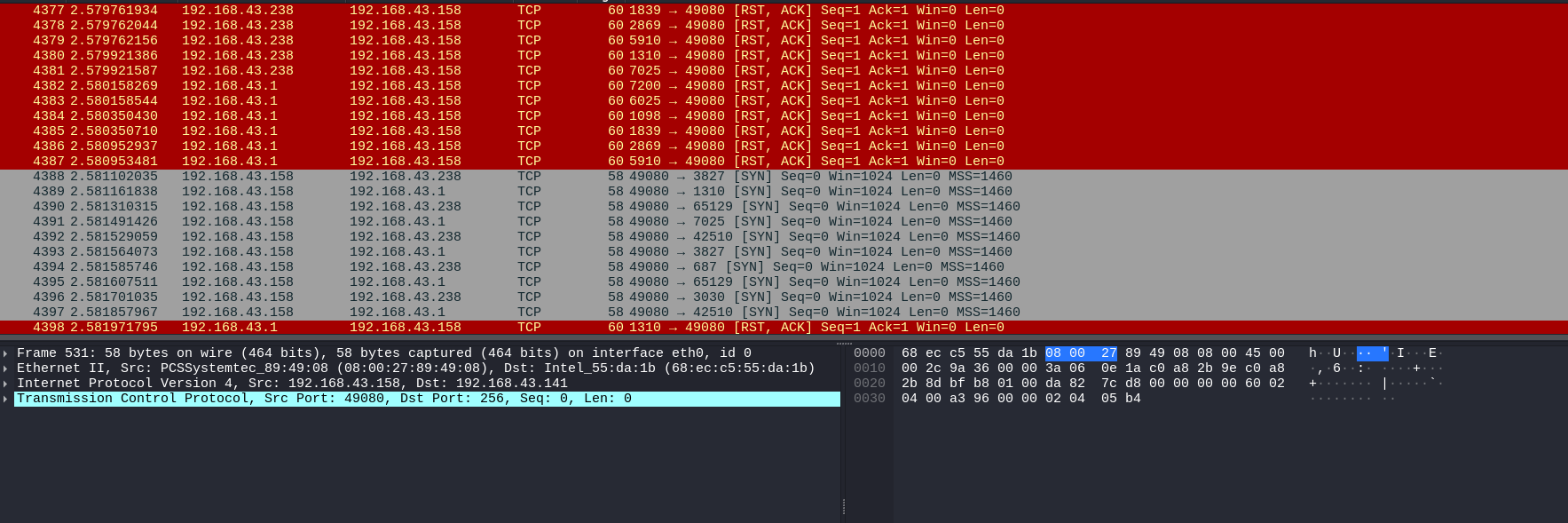


Target ip address

TCP ACK Ping



**Result:**



TCP ACK Ping

Send & Receive Information

Hex Code

**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.

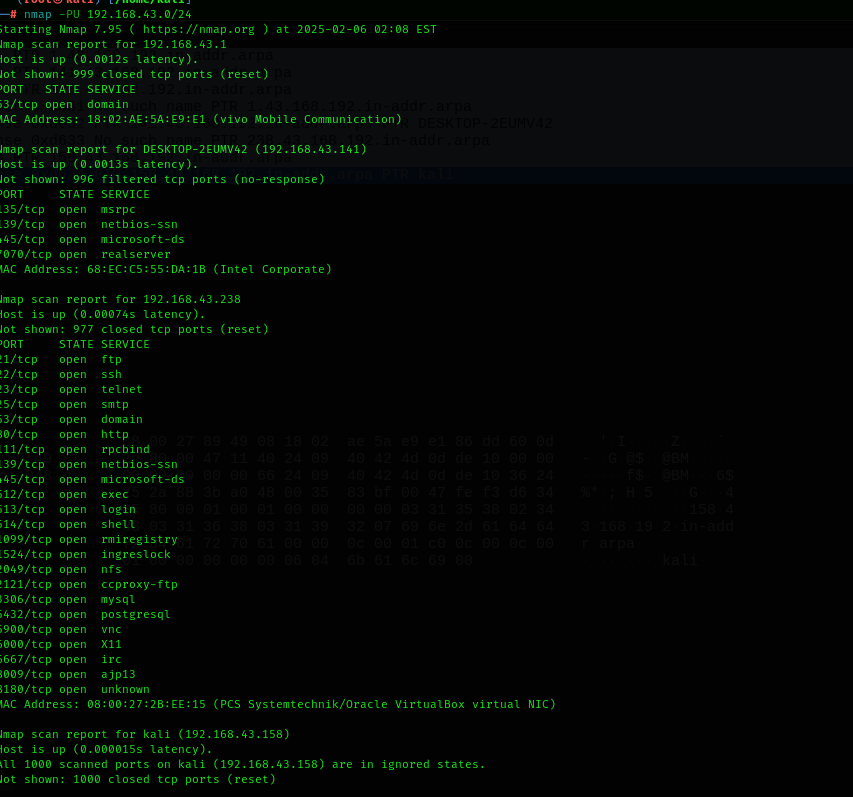
**Command in Kali Linux:**

Nmap -PU 192.168.43.0

Where, nmap is network mapping

-PU stand for UDP Ping.

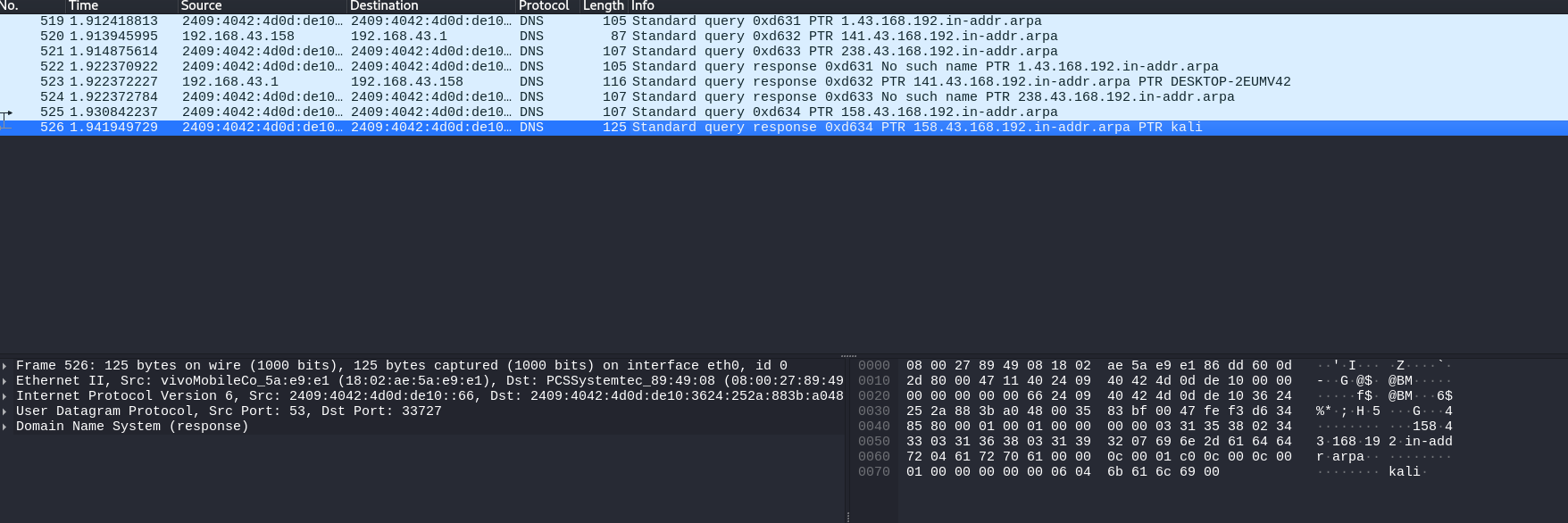
192.168.43.0 is a target ip address.

**Example:**

Target ip address

UDP Ping

**Result:**

****

UDP Ping

Send & Receive Information

Hex Code