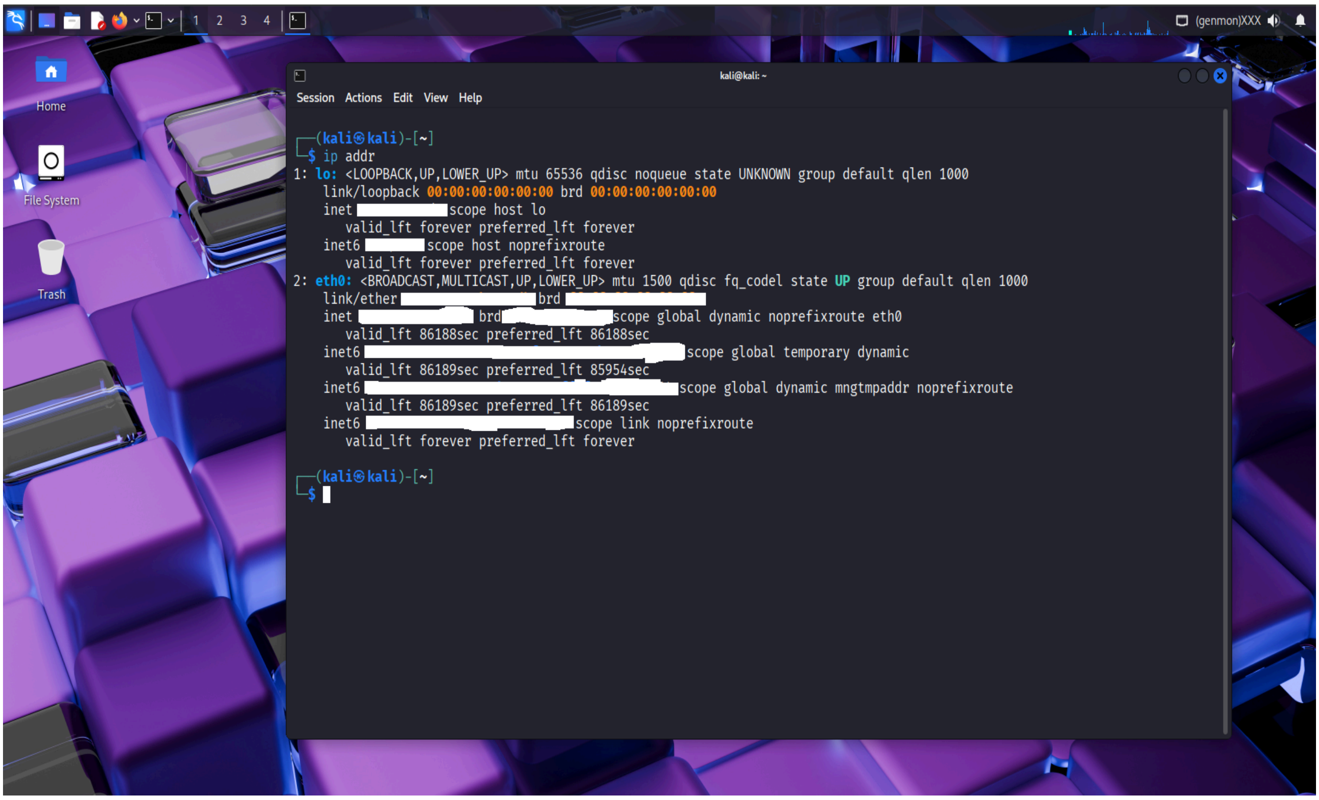
Network Footprinting



```
┌──(kali㉿kali)-[~]
└─$ ip addr
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 [redacted] scope host lo
       valid_lft forever preferred_lft forever
    inet6 [redacted] scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether [redacted] brd [redacted]
    inet [redacted] brd [redacted] scope global dynamic noprefixroute eth0
       valid_lft 86188sec preferred_lft 86188sec
    inet6 [redacted] scope global temporary dynamic
       valid_lft 86189sec preferred_lft 85954sec
    inet6 [redacted] scope global dynamic mngtmpaddr noprefixroute
       valid_lft 86189sec preferred_lft 86189sec
    inet6 [redacted] scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ 
```

The `ip addr` command (also commonly shortened to `ip a`) is a fundamental Linux utility used to display and manipulate routing, network devices, interfaces, and tunnels. When executed without any additional options, it provides a detailed overview of all network interfaces on the system.

Here's a breakdown of the information typically shown:

Loopback Interface (lo)

This is a special virtual interface that acts as a local connection, allowing the machine to communicate with itself. It's often assigned the IPv4 address `127.0.0.1` and the IPv6 address `::1`.

Ethernet/Wireless Interfaces (e.g., eth0, wlan0)

These are your primary network interfaces for connecting to a local area network (LAN) or wireless network.

Key Information Displayed:

- **Interface Name:** e.g., `eth0`, `wlan0`, `enp0s3`.
- **Link Status:** Indicates if the interface is `UP` (active) or `DOWN` (inactive).
- **MAC Address (link/ether):** The hardware address of the network card.
- **IPv4 Address (inet):** The IP address assigned to the interface within an IPv4 network. This will also show the subnet mask (e.g., `/24` or `255.255.255.0`). The

Network Footprinting

"IP Local range" typically refers to the private IP address range assigned to your machine, which falls within these `inet` addresses.

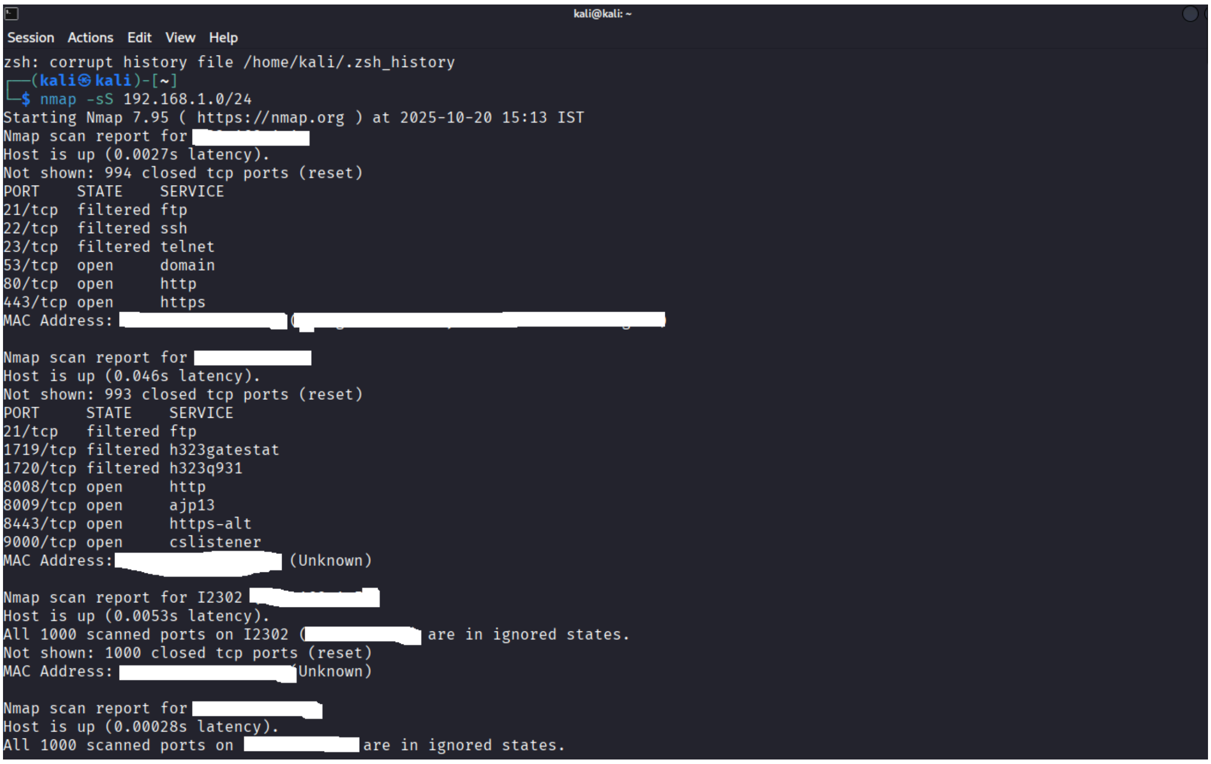
- **IPv6 Address (inet6):** The IP address assigned to the interface within an IPv6 network. This might include link-local addresses (`fe80::...`) and global unicast addresses.
- **Broadcast Address (brd):** The address used to send data to all devices on the same subnet.
- **Scope:** Indicates the scope of the IP address, such as `global` (routable on the internet), `link` (local to the network segment), or `host` (only accessible from the local machine).

Subnets

The subnet information is directly embedded within the IPv4 and IPv6 address entries. For IPv4, it's usually represented in CIDR notation (e.g., `192.168.1.10/24`), where `/24` indicates a subnet mask that allows for a specific range of IP addresses within that network.

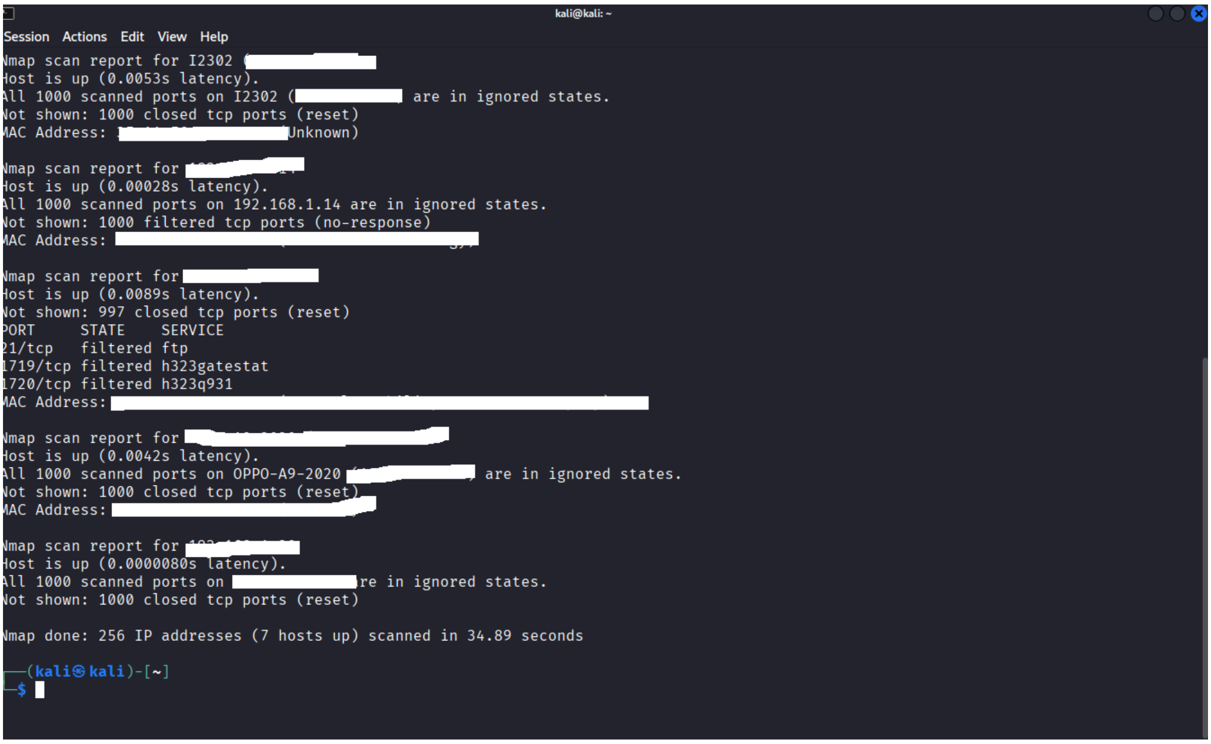
The `ip addr` command is an essential tool for network troubleshooting, configuration, and understanding your machine's network connectivity.

Show the IP address of the machine ,local host ,Subnets,Ipv6,Ipv4 also the IP Local range
Command >> $ ip addr



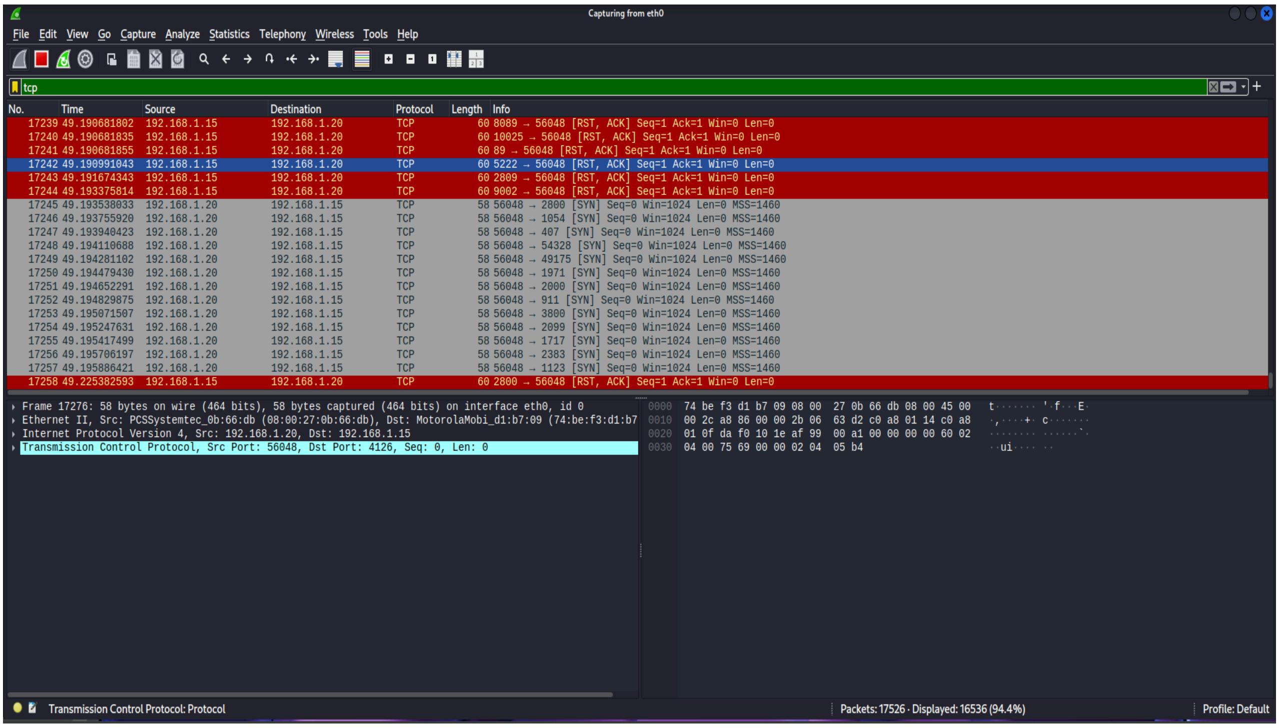
```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-20 15:13 IST
Nmap scan report for [redacted]
Host is up (0.0027s latency).
Not shown: 994 closed tcp ports (reset)
PORT    STATE    SERVICE
21/tcp  filtered ftp
22/tcp  filtered ssh
23/tcp  filtered telnet
53/tcp  open     domain
80/tcp  open     http
443/tcp open     https
MAC Address: [redacted] ([redacted]

Nmap scan report for [redacted]
Host is up (0.046s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   filtered ftp
1719/tcp filtered h323gatestat
1720/tcp filtered h323q931
8008/tcp open     http
8009/tcp open     ajp13
8443/tcp open     https-alt
9000/tcp open     cslistener
MAC Address:[redacted] (Unknown)

Nmap scan report for I2302 [redacted]
Host is up (0.0053s latency).
All 1000 scanned ports on I2302 ([redacted] are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: [redacted](Unknown)

Nmap scan report for [redacted]
Host is up (0.00028s latency).
All 1000 scanned ports on [redacted] are in ignored states.
```

Network Footprinting



```
Nmap scan report for I2302 [redacted]
Host is up (0.0053s latency).
All 1000 scanned ports on I2302 ([redacted] are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: [redacted]Unknown)

Nmap scan report for [redacted]
Host is up (0.00028s latency).
All 1000 scanned ports on 192.168.1.14 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: [redacted]

Nmap scan report for [redacted]
Host is up (0.0089s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   filtered ftp
1719/tcp filtered h323gatestat
1720/tcp filtered h323q931
MAC Address: [redacted]

Nmap scan report for [redacted]
Host is up (0.0042s latency).
All 1000 scanned ports on OPPO-A9-2020 [redacted] are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: [redacted]

Nmap scan report for [redacted]
Host is up (0.0000080s latency).
All 1000 scanned ports on [redacted]re in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (7 hosts up) scanned in 34.89 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Nmap Scan of The Local Range Ip address
Cmd >> $ nmap -sS <ip> -oN scan_results.txt



Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp

No.   Time         Source        Destination   Protocol Length Info
17239 49.190681802 192.168.1.15  192.168.1.20  TCP      60 8089 → 56048 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17240 49.190681835 192.168.1.15  192.168.1.20  TCP      60 10025 → 56048 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17241 49.190681855 192.168.1.15  192.168.1.20  TCP      60 89 → 56048 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17242 49.190991043 192.168.1.15  192.168.1.20  TCP      60 5222 → 56048 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17243 49.191674343 192.168.1.15  192.168.1.20  TCP      60 2809 → 56048 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17244 49.193375814 192.168.1.15  192.168.1.20  TCP      60 9002 → 56048 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17245 49.193538033 192.168.1.20  192.168.1.15  TCP      58 56048 → 2800 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17246 49.193755920 192.168.1.20  192.168.1.15  TCP      58 56048 → 1054 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17247 49.193940423 192.168.1.20  192.168.1.15  TCP      58 56048 → 407 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17248 49.194110688 192.168.1.20  192.168.1.15  TCP      58 56048 → 54328 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17249 49.194281102 192.168.1.20  192.168.1.15  TCP      58 56048 → 49175 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17250 49.194479430 192.168.1.20  192.168.1.15  TCP      58 56048 → 1971 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17251 49.194652291 192.168.1.20  192.168.1.15  TCP      58 56048 → 2000 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17252 49.194829875 192.168.1.20  192.168.1.15  TCP      58 56048 → 911 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17253 49.195071507 192.168.1.20  192.168.1.15  TCP      58 56048 → 3800 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17254 49.195247631 192.168.1.20  192.168.1.15  TCP      58 56048 → 2099 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17255 49.195417499 192.168.1.20  192.168.1.15  TCP      58 56048 → 1717 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17256 49.195706197 192.168.1.20  192.168.1.15  TCP      58 56048 → 2383 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17257 49.195886421 192.168.1.20  192.168.1.15  TCP      58 56048 → 1123 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17258 49.225382593 192.168.1.15  192.168.1.20  TCP      60 2800 → 56048 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

› Frame 17276: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface eth0, id 0
› Ethernet II, Src: PCSSystemtec_0b:66:db (08:00:27:0b:66:db), Dst: MotorolaMobi_d1:b7:09 (74:be:f3:d1:b7
› Internet Protocol Version 4, Src: 192.168.1.20, Dst: 192.168.1.15
› Transmission Control Protocol, Src Port: 56048, Dst Port: 4126, Seq: 0, Len: 0

0000  74 be f3 d1 b7 09 08 00  27 0b 66 db 08 00 45 00   t······· '·f···E·
0010  00 2c a8 86 00 00 2b 06  63 d2 c0 a8 01 14 c0 a8   ·,····+· c·······
0020  01 0f da f0 10 1e af 99  00 a1 00 00 00 00 60 02   ········ ······`·
0030  04 00 75 69 00 00 02 04  05 b4                     ··ui···· ··

Transmission Control Protocol: Protocol          Packets: 17526 · Displayed: 16536 (94.4%)          Profile: Default
```

The TCP handshake capture of Wireshark network Analysis
Tool: WireShark