

- Capture and Analyze Network Traffic Using Wireshark

```

File Machine View Input Devices Help
Capturing from eth0 root@kali: /home/kali

Applications
root@kali ~# ping -c 10 google.com

PING google.com (216.58.200.174) 56(84) bytes of data:
64 bytes from del11s06-in-f14.1e100.net (216.58.200.174): icmp_seq=1 ttl=111 time=32.7 ms
64 bytes from del11s06-in-f14.1e100.net (216.58.200.174): icmp_seq=2 ttl=111 time=34.7 ms
64 bytes from del11s06-in-f14.1e100.net (216.58.200.174): icmp_seq=3 ttl=111 time=33.1 ms
64 bytes from del11s06-in-f14.1e100.net (216.58.200.174): icmp_seq=4 ttl=111 time=45.5 ms
64 bytes from del11s06-in-f14.1e100.net (216.58.200.174): icmp_seq=5 ttl=111 time=31.7 ms
64 bytes from del11s06-in-f14.1e100.net (216.58.200.174): icmp_seq=6 ttl=111 time=33.1 ms
64 bytes from del11s06-in-f14.1e100.net (216.58.200.174): icmp_seq=7 ttl=111 time=35.7 ms
64 bytes from del11s06-in-f14.1e100.net (216.58.200.174): icmp_seq=8 ttl=111 time=33.4 ms
64 bytes from del11s06-in-f14.1e100.net (216.58.200.174): icmp_seq=9 ttl=111 time=31.9 ms
64 bytes from del11s06-in-f14.1e100.net (216.58.200.174): icmp_seq=10 ttl=111 time=35.1 ms

— google.com ping statistics —
10 packets transmitted, 10 received, 0% packet loss, time 9004ms
rtt min/avg/max/mdev = 31.651/34.671/45.463/3.811 ms

```

Filter :DNS

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|--------------|--------------|----------|--------|----------------------------|
| 9 | 52.548150609 | 10.0.2.15 | 192.168.29.1 | DNS | 70 | Standard query 0xc67 A go |
| 10 | 52.548194387 | 10.0.2.15 | 192.168.29.1 | DNS | 70 | Standard query 0xc165 AAAA |
| 11 | 52.552319408 | 192.168.29.1 | 10.0.2.15 | DNS | 86 | Standard query response 0x |
| 12 | 52.569152403 | 192.168.29.1 | 10.0.2.15 | DNS | 98 | Standard query response 0x |
| 15 | 52.603191130 | 10.0.2.15 | 192.168.29.1 | DNS | 87 | Standard query 0xcdc8 PTR |
| 16 | 52.622738480 | 192.168.29.1 | 10.0.2.15 | DNS | 157 | Standard query response 0x |

Filter : ICMP

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|----------------|----------------|----------|--------|---------------------|
| 13 | 52.569928271 | 10.0.2.15 | 216.58.200.174 | ICMP | 98 | Echo (ping) request |
| 14 | 52.602623113 | 216.58.200.174 | 10.0.2.15 | ICMP | 98 | Echo (ping) reply |
| 17 | 53.571079992 | 10.0.2.15 | 216.58.200.174 | ICMP | 98 | Echo (ping) request |
| 18 | 53.605723267 | 216.58.200.174 | 10.0.2.15 | ICMP | 98 | Echo (ping) reply |
| 19 | 54.571721856 | 10.0.2.15 | 216.58.200.174 | ICMP | 98 | Echo (ping) request |
| 20 | 54.604714750 | 216.58.200.174 | 10.0.2.15 | ICMP | 98 | Echo (ping) reply |
| 21 | 55.573713914 | 10.0.2.15 | 216.58.200.174 | ICMP | 98 | Echo (ping) request |
| 22 | 55.619114079 | 216.58.200.174 | 10.0.2.15 | ICMP | 98 | Echo (ping) reply |
| 23 | 56.575002193 | 10.0.2.15 | 216.58.200.174 | ICMP | 98 | Echo (ping) request |
| 24 | 56.606592266 | 216.58.200.174 | 10.0.2.15 | ICMP | 98 | Echo (ping) reply |
| 25 | 57.576424123 | 10.0.2.15 | 216.58.200.174 | ICMP | 98 | Echo (ping) request |
| 26 | 57.609479264 | 216.58.200.174 | 10.0.2.15 | ICMP | 98 | Echo (ping) reply |
| 27 | 58.577633232 | 10.0.2.15 | 216.58.200.174 | ICMP | 98 | Echo (ping) request |

Filter : DHCP

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|----------|-----------------|----------|--------|-----------------------------|
| 1 | 0.000000000 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Discover - Transaction |
| 2 | 0.000939647 | 10.0.2.3 | 255.255.255.255 | DHCP | 590 | DHCP Offer - Transaction |
| 3 | 0.001019969 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Request - Transaction |
| 4 | 1.759995432 | 10.0.2.3 | 255.255.255.255 | DHCP | 590 | DHCP ACK - Transaction |
| 5 | 37.545346953 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 | DHCP Request - Transaction |
| 6 | 38.220688651 | 10.0.2.3 | 255.255.255.255 | DHCP | 590 | DHCP ACK - Transaction |

Protocols Identified

1. DHCP (Dynamic Host Configuration Protocol)

- **Packets:** 1–6
- **Purpose:** Assigns IP addresses to the VM.
- **Key Details:**
 - DHCP Discover, Offer, Request, ACK sequence captured.
 - Client IP was assigned via DHCP from **10.0.2.3**.

2. DNS (Domain Name System)

- **Packets:** 9–12, 15–16
- **Purpose:** Resolves domain names like **google.com** to IP addresses.
- **Key Details:**
 - Standard A and AAAA queries to **192.168.29.1**.
 - Reverse lookup (PTR query) for IP **216.58.200.174**.

3. ICMP (Internet Control Message Protocol)

- **Packets:** 13–14, 17–34
- **Purpose:** Used by the **ping** command to test connectivity.
- **Key Details:**
 - 10 Echo Request–Reply pairs to IP **216.58.200.174** (Google server).
 - Consistent round-trip times, no packet loss.

4. ARP (Address Resolution Protocol)

- **Packets:** 7–8
- Purpose:** Resolves IP address **10.0.2.1** to its MAC address.
- **Key Details:**
 - Request made by **PCSSystemtec_0e:34:8d**.
 - Response: MAC **52:54:00:12:35:00**.