Dharmin Tank Task 5

Capture and Analyze Network Traffic Using Wireshark

```
File Machine View Input Devices Help

Applications

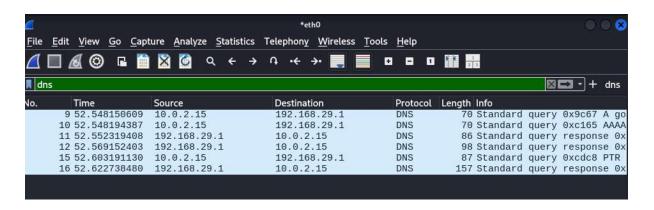
(root@ lali)-[/home/kali]

ping -c 10 google.com

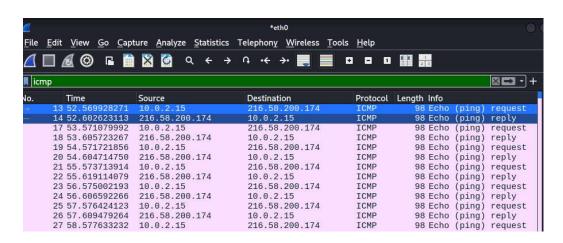
PTNG google.com (216.58.200.174) 56(84) bytes of data.
64 bytes from dellis06-in-f14.le100.net (216.58.200.174): icmp_seq=1 ttl=111 time=32.7 ms
64 bytes from dellis06-in-f14.le100.net (216.58.200.174): icmp_seq=2 ttl=111 time=34.7 ms
64 bytes from dellis06-in-f14.le100.net (216.58.200.174): icmp_seq=2 ttl=111 time=34.7 ms
64 bytes from dellis06-in-f14.le100.net (216.58.200.174): icmp_seq=3 ttl=111 time=35.5 ms
64 bytes from dellis06-in-f14.le100.net (216.58.200.174): icmp_seq=5 ttl=111 time=31.7 ms
64 bytes from dellis06-in-f14.le100.net (216.58.200.174): icmp_seq=6 ttl=111 time=31.7 ms
64 bytes from dellis06-in-f14.le100.net (216.58.200.174): icmp_seq=6 ttl=111 time=35.7 ms
64 bytes from dellis06-in-f14.le100.net (216.58.200.174): icmp_seq=7 ttl=111 time=35.7 ms
64 bytes from dellis06-in-f14.le100.net (216.58.200.174): icmp_seq=9 ttl=111 time=35.7 ms
64 bytes from dellis06-in-f14.le100.net (216.58.200.174): icmp_seq=9 ttl=111 time=35.7 ms
64 bytes from dellis06-in-f14.le100.net (216.58.200.174): icmp_seq=9 ttl=111 time=35.7 ms
64 bytes from dellis06-in-f14.le100.net (216.58.200.174): icmp_seq=9 ttl=111 time=35.7 ms
64 bytes from dellis06-in-f14.le100.net (216.58.200.174): icmp_seq=9 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

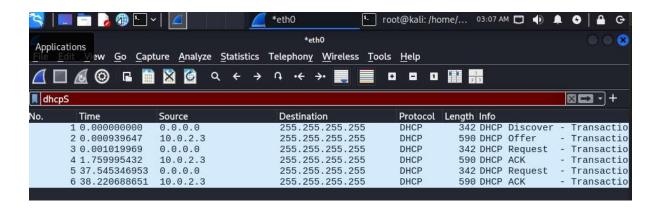


Filter: ICMP



Dharmin Tank Task 5

Filter: DHCP



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)

o 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)

o 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.