Name: Shubhan Singh

Class: SE Comps B

Roll no.: 2022300118

**CCN Experiment 7**

Packet Crafting

**Aim:** Packet Crafting using Scapy

**Objectives**:

1. Gain hands-on experience with Scapy, a Python-based packet manipulation tool.
2. Understand the functionality and significance of protocols at the Application and Transport Layers.
3. Analyze and dissect packets to comprehend the structure and contents of different protocols.
4. Investigate the interaction between Application and Transport Layer protocols.
5. Develop skills in crafting custom packets for specific networking scenarios.

**Problem Statement:**

Kindly craft the following packets. Take a screenshot of results. Also take screenshots of the crafted packet you send.

**1. Ping (ICMP Echo Request)**:

* Craft an ICMP Echo Request packet using Scapy.
* Send the packet to a target IP address.
* Expect an ICMP Echo Reply packet in response from the target.

**Code:**

from scapy.all import \*

def ping(ip):

    icmp\_request = IP(dst=ip) / ICMP()

    icmp\_response = sr1(icmp\_request, timeout=1)

    if icmp\_response:

        print(f"Received reply from {ip}")

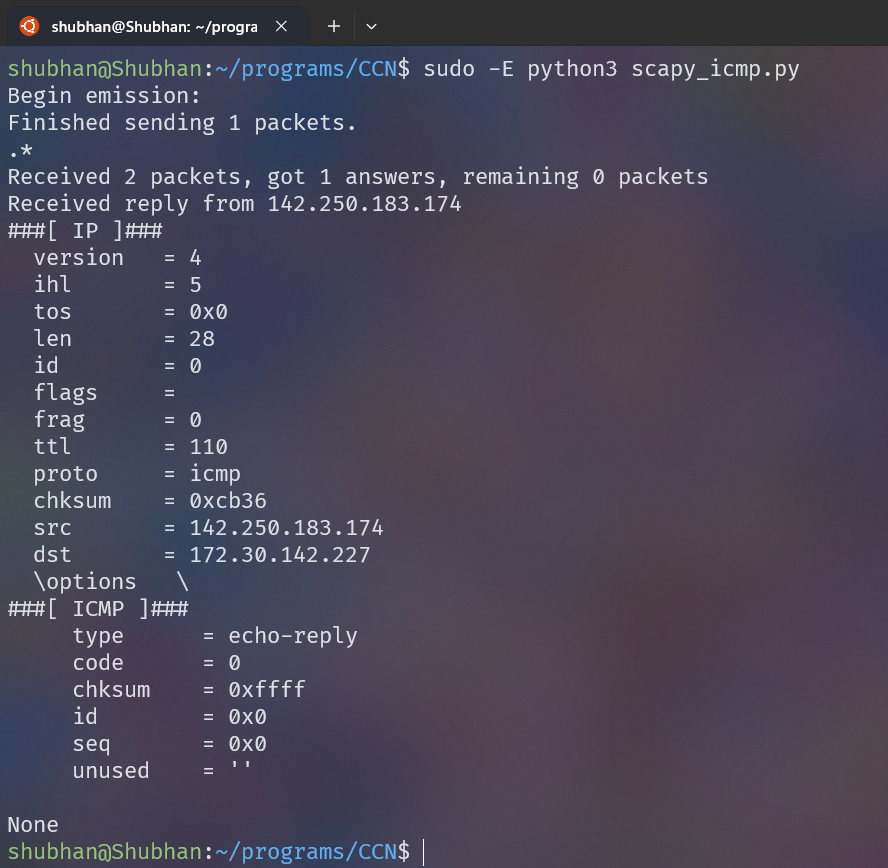
        print(icmp\_response.show())

    else:

        print(f"No reply from {ip}")

ping('142.250.183.174')

**Output:**



**2. UDP Datagram**:

* Craft a UDP packet with custom payload using Scapy.
* Send the UDP packet to a target listening on a specific UDP port.
* Expect a response from the target if the port is open and reachable.

**Code:**

from scapy.all import IP, UDP, sr1

def send\_udp\_packet(ip, port, payload):

    udp\_packet = IP(dst=ip) / UDP(dport=port) / payload

    udp\_response = sr1(udp\_packet, timeout=1)

    if udp\_response:

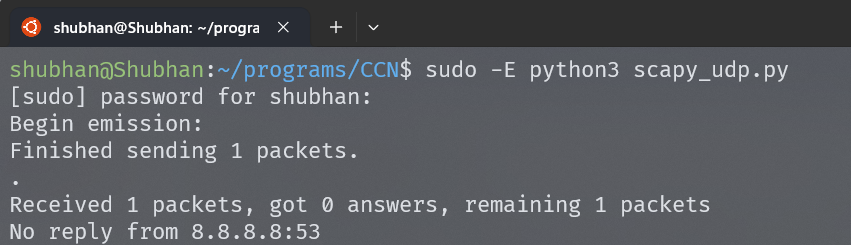
        print(f"Received reply from {ip}:{port}: {udp\_response.show()}")

    else:

        print(f"No reply from {ip}:{port}")

send\_udp\_packet('8.8.8.8', 53, 'My message')

**Output:**

****

(No response was received from server)

**3. DNS Query**:

* Craft a DNS query packet using Scapy to query a DNS server for a specific domain.
* Send the DNS query packet to the DNS server.
* Expect a DNS response containing the IP address associated with the queried domain.

**Code:**

from scapy.all import \*

ip='8.8.8.8'

icmp\_request = IP(dst=ip) / UDP(dport=53) / DNS(rd=1,qd=DNSQR(qname='www.google.com'))

icmp\_response = sr1(icmp\_request, verbose=0)

if icmp\_response:

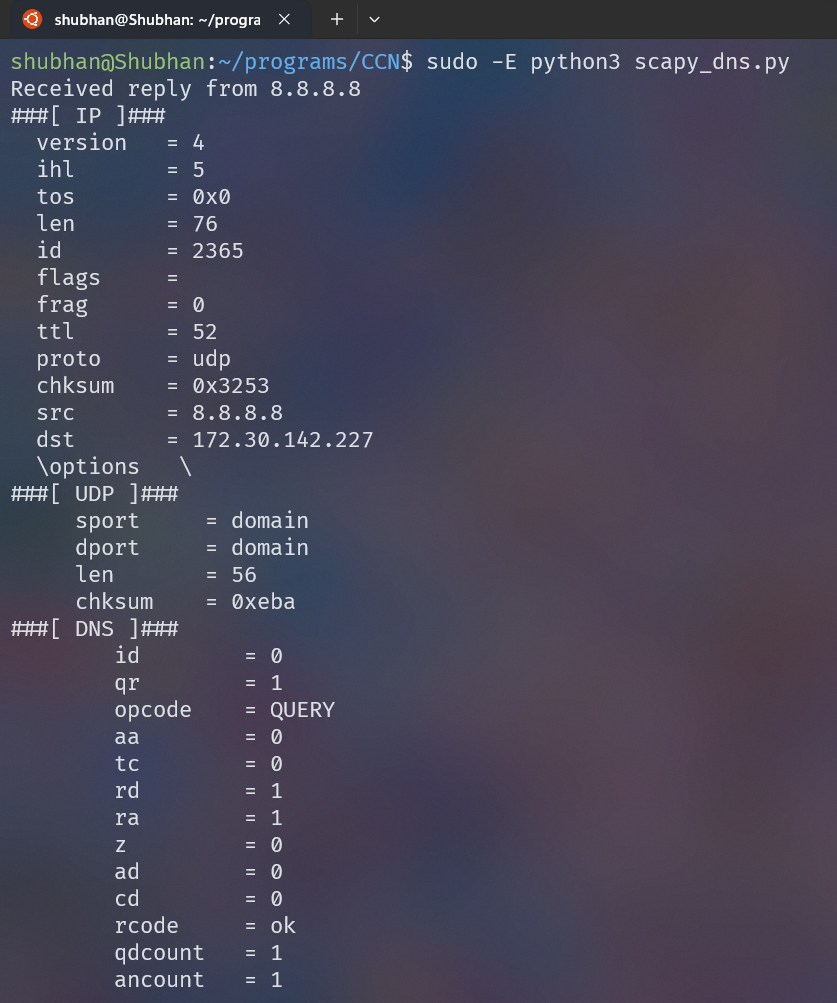
    print(f"Received reply from {ip}")

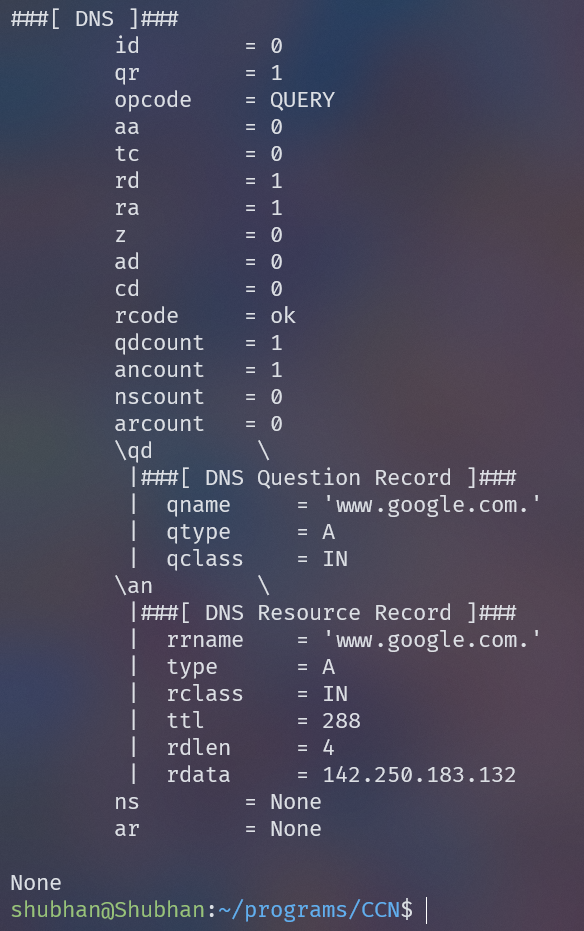
    print(icmp\_response.show())

else:

    print(f"No reply from {ip}")

**Output: (On next page)**





**4. HTTP GET Request**:

* Craft an HTTP GET request packet using Scapy to retrieve a specific web page from a web server.
* Send the HTTP GET request to the web server.
* Expect an HTTP response containing the requested web page content.

**5 . Traceroute**

* Craft UDP packets with increasing TTL (Time-to-Live) values using Scapy.
* Send these packets towards a destination IP address.
* Observe the ICMP Time Exceeded messages returned by intermediate routers to map the network path to the destination.