

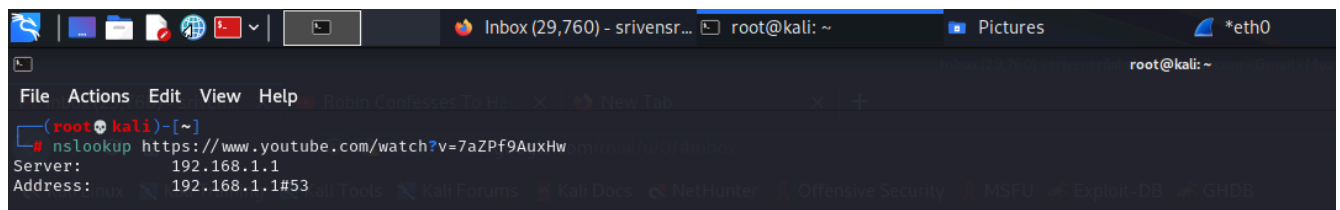
Objective:

To understand session-like behavior in UDP, despite it being a connectionless protocol, by examining a simple communication between a client and a server.

Choose a UDP-Based Application:

1. **DNS Query:** Use a tool like **nslookup** to perform a DNS lookup.
2. **Streaming Service:** Play a short video clip on a platform that uses UDP for streaming.
3. Run the **nslookup** command to resolve a domain name, such as

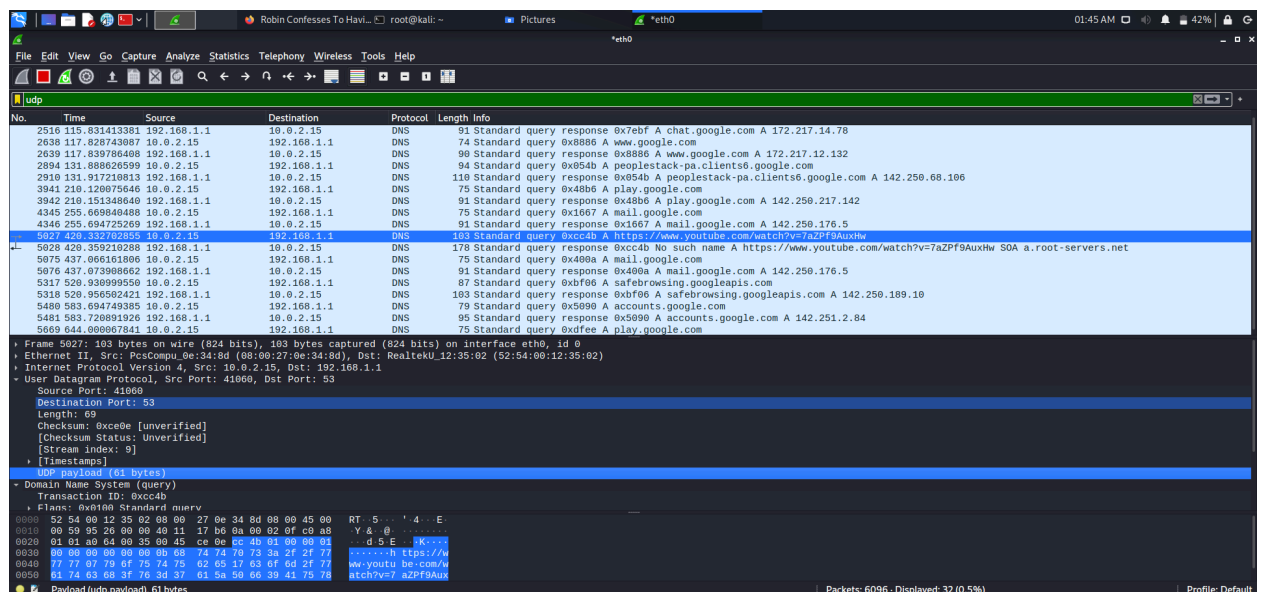
nslookup youtube.com/watch?v=7aZPf9AuxHw



```
File Actions Edit View Help
(root@kali)~[~]
# nslookup https://www.youtube.com/watch?v=7aZPf9AuxHw
Server:      192.168.1.1
Address:     192.168.1.1#53
```

Scroll through the captured UDP packets to find those related to your **nslookup** query or streaming activity, we see that the server address 192.168.1.1

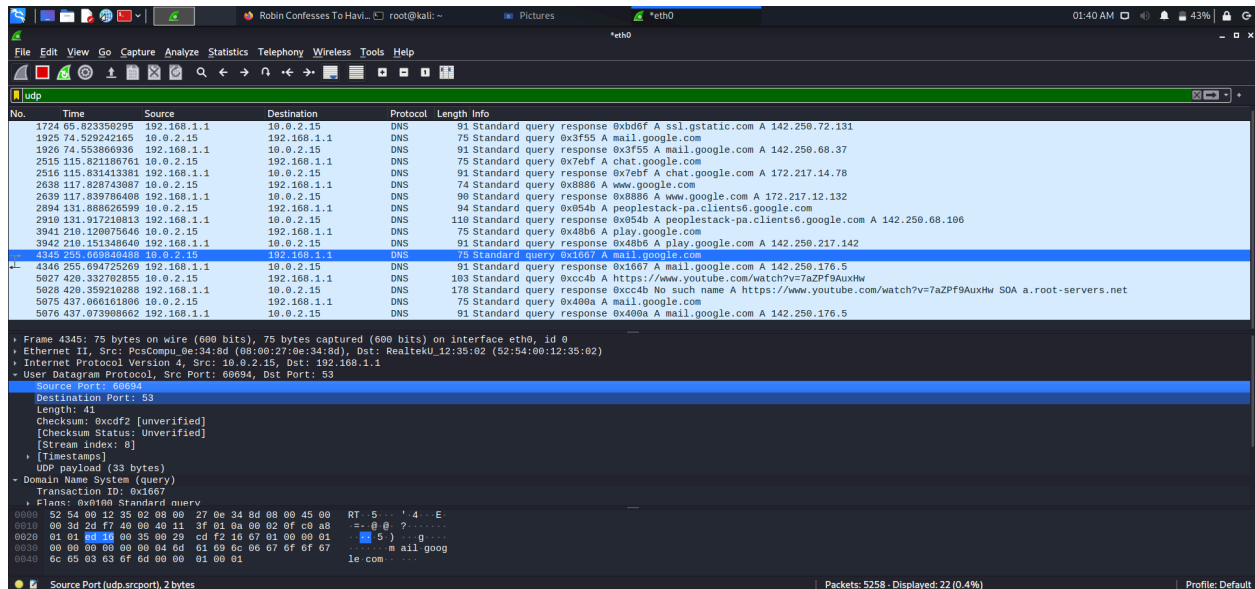
Identify packets by checking the source and destination IP addresses and ports. DNS traffic used port 53, while streaming might use different ports.



The screenshot shows a Wireshark packet capture on the 'eth0' interface. The packet list pane displays several DNS queries and responses. The selected packet (No. 5027) is a DNS query from 192.168.1.1 to 192.168.1.1. The packet details pane shows the following information:

- Frame 5027: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface eth0, id 0
- Ethernet II, Src: PcsCompu_0e:34:8d (08:00:27:0e:34:8d), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
- Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.1
- User Datagram Protocol, Src Port: 41060, Dst Port: 53
- Source Port: 41060
- Destination Port: 53
- Length: 60
- Checksum: 0xc0e0 [unverified]
- [Checksum Status: Unverified]
- [Stream index: 9]
- [Timestamps]
- UDP payload (61 bytes)
- Domain Name System (query)
- Transaction ID: 0xc04b
- Flags: 0x0100 Standard query
- 52 54 00 12 35 02 08 00 27 0e 34 8d 08 00 45 00 RT: 5...4...E
- 60 59 95 20 08 00 4b 11 17 b0 8a 08 02 0f c0 a8 Y& .0.
- 01 01 00 04 00 35 00 45 ce 0e c0 4b 01 00 00 00 d 5 E K...
- 00 00 00 00 00 00 00 00 74 74 76 73 3a 2f 2f 77h https://w
- 77 77 07 79 6f 75 74 75 62 65 17 63 6f 6d 2f 77 ww.youtu.be.com/w
- 63 74 65 3f 74 74 2f 61 5a 58 66 39 43 75 78 tch?v=7 aZPf9Aux

The packet bytes pane shows the raw data of the selected packet.

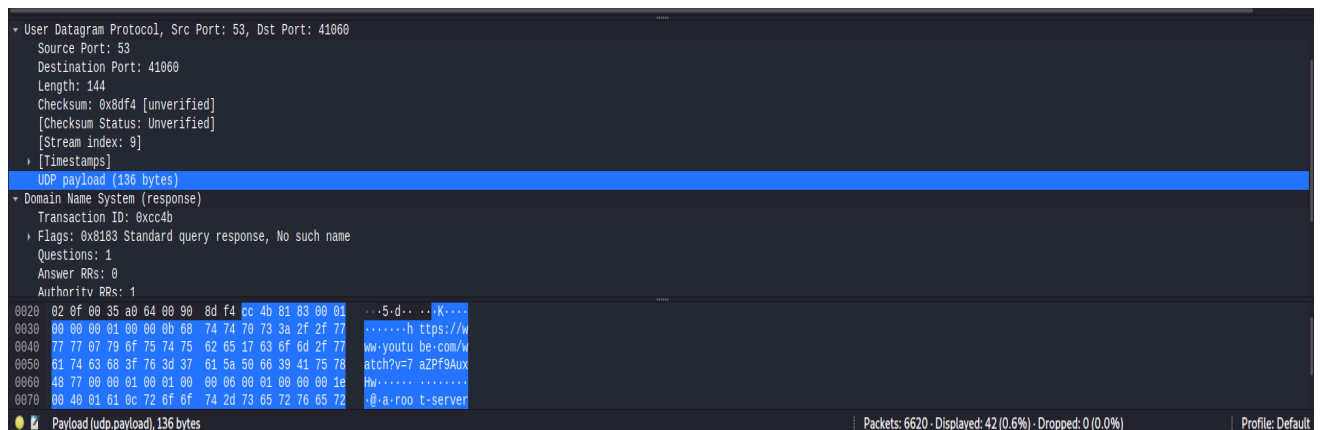


Source IP Address: The IP address of the client which our computer 10.0.2.15

Destination IP Address: The IP address of the server - 192.168.1.1

Source Port: A dynamically allocated port used by your machine - 60694

Destination Port: Port 53 for DNS queries, or a different port for streaming services.



Discuss how UDP handles data transmission without establishing a session.

1. UDP does not require a handshake like SYN, SYN-ACK, ACK to establish a connection before data transmission.
2. Stateless communication, each UDP packet is independent, meaning there is no inherent ordering or guarantee of delivery. This is evident in the lack of acknowledgement packets.
3. UDP has session like behavior through application layer mechanisms

Comparison with TCP session Creation

1. **TCP:** Establishes a connection using a three-way handshake SYN, SYN-ACK, ACK, maintains state, and ensures ordered and reliable delivery of packets.
2. **UDP:** Does not establish a connection, does not maintain state, and does not guarantee packet order or delivery.