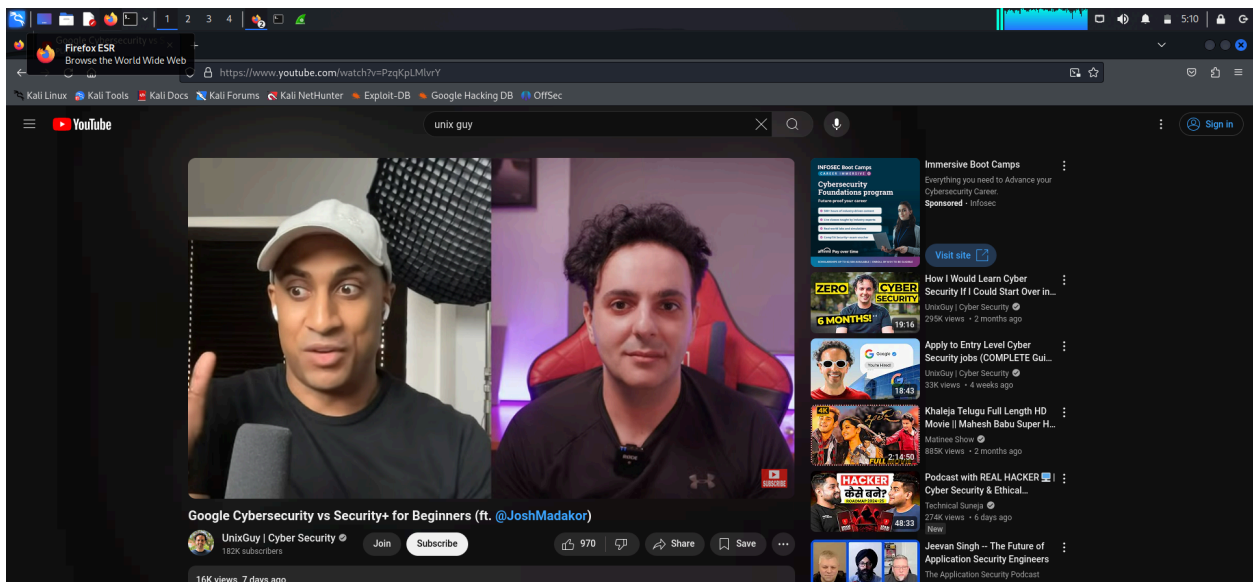
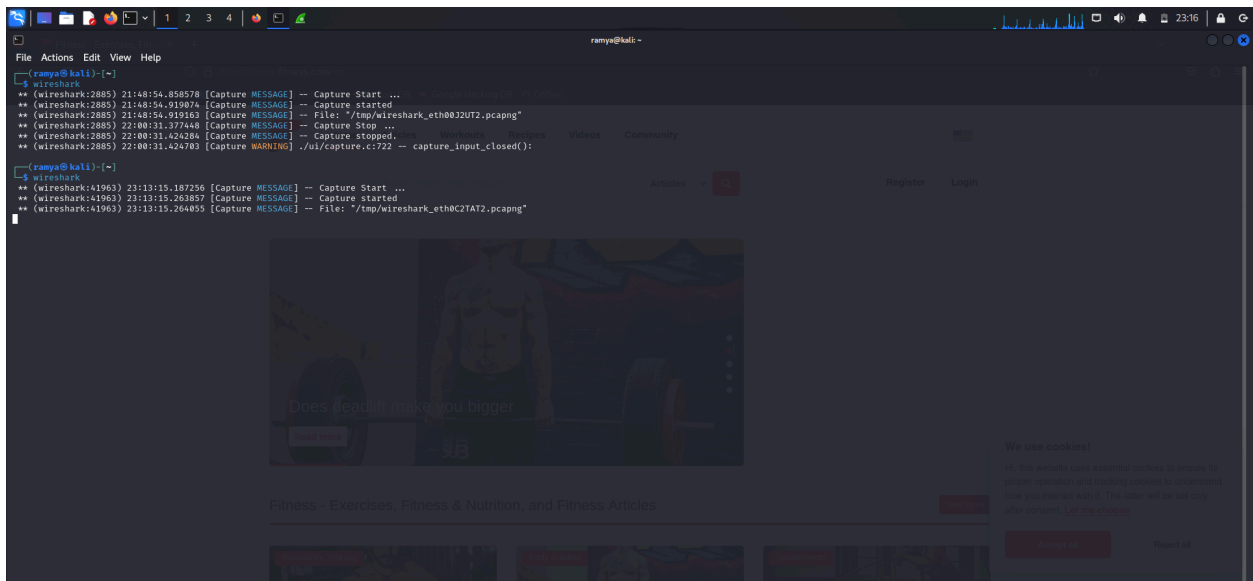


UDP Session Analysis

Bakka Ramyasree

1. Set Up the Environment:

- Use a UDP-based application (e.g., a simple DNS query or streaming service).
- Start capturing traffic in Wireshark.

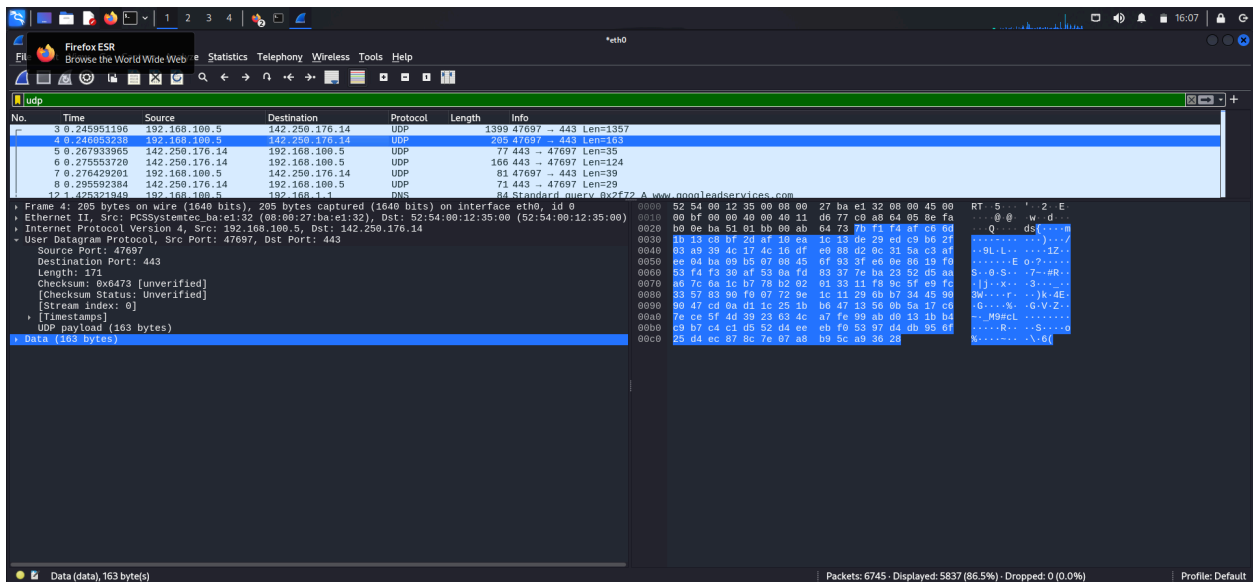
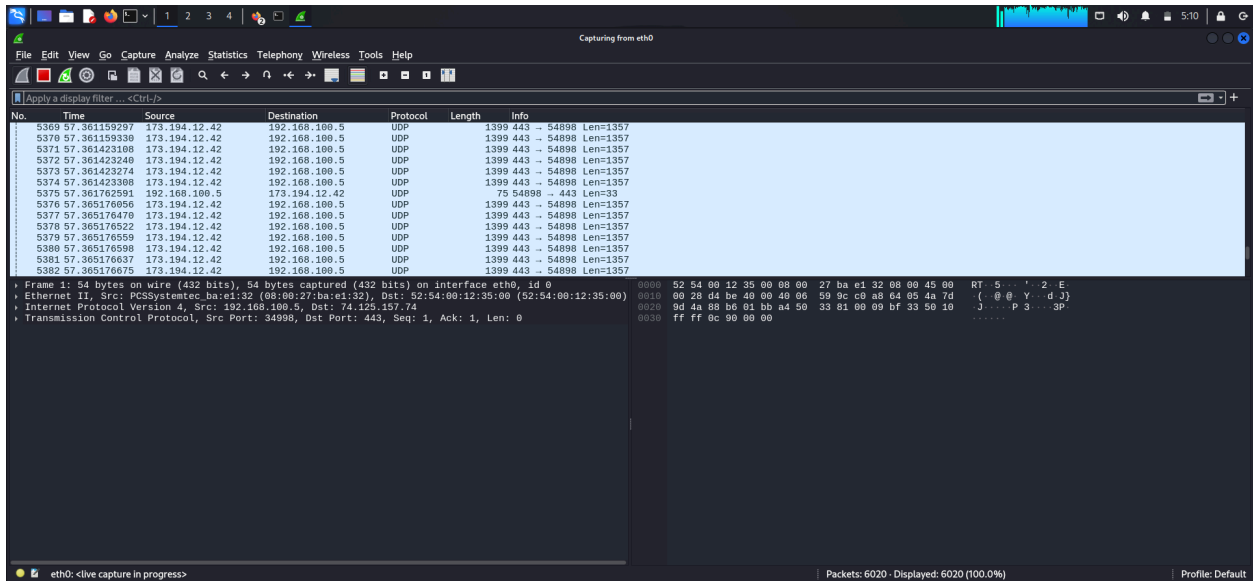


Perform a UDP-Based Task:

- For streaming, play a short video clip. I used firefox to play video on you tube

2. Identify UDP Packets:

- Filter Wireshark traffic using **udp**.
- Locate the packets corresponding to your activity.



Wireshark interface showing a packet capture on interface eth0. The selected packet is a QUIC packet (No. 46) with details expanded to show the QUIC IETF section. The packet is a handshake packet (1399 Initial) with DCID=efa3177fa06a7d6e, SCID=203396, and PKN: 0. The packet length is 1399 bytes. The packet is captured on interface eth0, ID 0.

Frame 46: 1399 bytes on wire (11192 bits), 1399 bytes captured (11192 bits) on interface eth0, ID 0

Ethernet II, Src: PCSysinternat-ba:e1:32 (08:00:27:ba:e1:32), Dst: 52:54:00:12:35:00 (52:54:00:12:35:00)

Internet Protocol Version 4, Src: 192.168.100.5, Dst: 142.250.188.226

User Datagram Protocol, Src Port: 59923, Dst Port: 443

Source Port: 59923

Destination Port: 443

Length: 1365

Checksum: 0x75f1 [unverified]

[Checksum Status: Unverified]

[Stream index: 3]

[Timestamps]

UDP payload (1357 bytes)

QUIC IETF

QUIC IETF

Frame (1399 bytes) Decrypted QUIC (516 bytes)

Packets: 6745 - Displayed: 1011 (15.0%) - Dropped: 0 (0.0%) Profile: Default

Wireshark interface showing a packet capture on interface eth0. The selected packet is a QUIC packet (No. 46) with details expanded to show the QUIC IETF section. The packet is a handshake packet (1399 Initial) with DCID=efa3177fa06a7d6e, SCID=203396, and PKN: 0. The packet length is 1399 bytes. The packet is captured on interface eth0, ID 0.

Frame 46: 1399 bytes on wire (11192 bits), 1399 bytes captured (11192 b

Ethernet II, Src: PCSysinternat-ba:e1:32 (08:00:27:ba:e1:32), Dst: 52:54:00:12:35:00 (52:54:00:12:35:00)

Internet Protocol Version 4, Src: 192.168.100.5, Dst: 142.250.188.226

User Datagram Protocol, Src Port: 59923, Dst Port: 443

Source Port: 59923

Destination Port: 443

Length: 1365

Checksum: 0x75f1 [unverified]

[Checksum Status: Unverified]

[Stream index: 3]

[Timestamps]

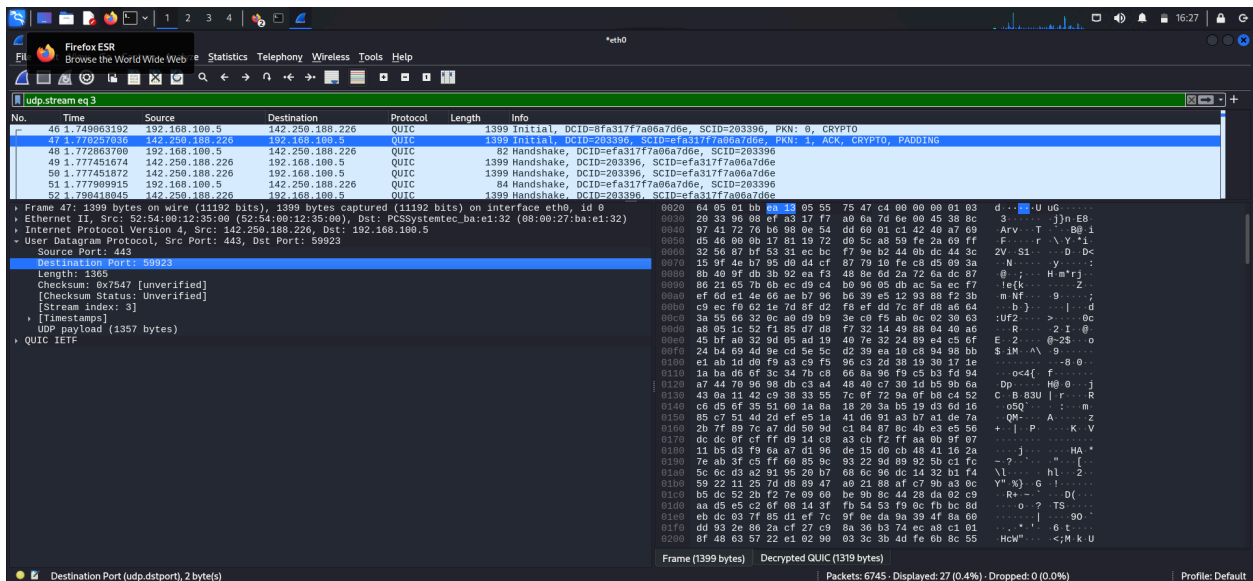
UDP payload (1357 bytes)

QUIC IETF

QUIC IETF

Frame (1399 bytes) Decrypted QUIC (516 bytes)

Packets: 6745 - Displayed: 1011 (15.0%) - Dropped: 0 (0.0%) Profile: Default



Analyze UDP Communication:

Document the source and destination IP addresses, ports, and payload sizes.

ANS: source ip addr is my kali linux :192.168.100.5

And the destination addr is youtube server :142.250.188.256

With source port :59923

Destination port:443 For QUIC, port 443 is common.

Discuss how UDP handles data transmission without establishing a session.

- Data can be sent using UDP (User Datagram Protocol) without establishing a connection between the sender and the recipient.
- No Session Setup: UDP transmits data without first establishing a connection, as opposed to TCP.
- Datagrams are the discrete packets of data that are transmitted. Every packet is transmitted independently and separately.
- Also called as fire and forget protocol it doesn't care about the data receiving or acknowledgement that is why it is faster.

Compare this with TCP session creation.

○

TCP	UDP
Connection oriented protocol	Connectionless protocol
Guarantee the data delivery	No Guarantee
Sets a connection by 3 way handshake	No Handshakes
Reliable	Faster but less reliable

○

Document Findings:

Write a report discussing the nature of UDP communication.

In order to better understand UDP (User Datagram Protocol) communication, this paper analyzes packets from a YouTube video transmitted in real life. Because of its reputation for being connectionless, UDP is frequently utilized for applications needing quick transmission.

- The nature of the connectionless protocol used by UDP communication is that data is sent without first establishing a link. Every datagram, or packet, is sent separately.
- No Handshake: There isn't a handshake procedure, in contrast to TCP. There will be no phases for connection setup or breakdown.
- No Acknowledgments: Error recovery and acknowledgments are not offered by UDP. No assurances are made on the arrival or precise arrangement of packets.

- Efficiency: UDP is speedier and better suited for real-time applications like video streaming because it does not have connection management or error checking.

Observed packets of UDP

- Firstly, packet capture

1. Overview of Packet Capture

- Wireshark was used to record the traffic during a YouTube video broadcast. The following findings were noted:
- Type of Packet: UDP packets
- Procedures QUIC, a system designed to provide faster and more secure data transmission over UDP, is observed.

2. Analysis of Key Packets

- Screenshot 1: QUIC Protocol in a UDP Packet
- 59923 is the source port.
- Port of destination: 443
- Payload 1357 bytes in size
- Details: The packet has a destination port of 443 that is used by QUIC for encrypted communication, and a source port that is characteristic of high-numbered ephemeral ports used by clients.
- Figure 2: An Additional UDP Packet
- 59924 is the source port.
- Port of destination: 443
- Size of Payload: 1357 bytes
- Details: The source port differs somewhat from the first transmission, showing that different ports are used for each packet.