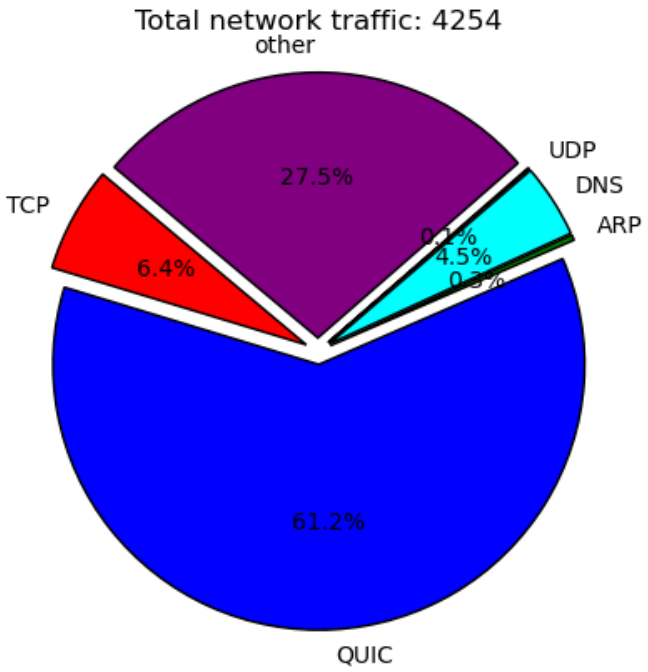
PCAP Analysis report

This report analyzes the PCAP file: today.pcap. It will determine whether a DDoS attack is detected. Some types of attacks we will search for include: SYN flooding, UDP flooding, ICMP flooding, and HTTP-GET flooding.



TCP: 273 TCP packets with a AVG packet size of: 463.18, packet ra
13.73

QUIC: 2604 QUIC packets with a AVG packet size of: 728.52, packe
rate: 144.53

ARP: 14 ARP packets with a AVG packet size of: 57.43, packet rate

DNS: 191 DNS packets with a AVG packet size of: 136.82, packet ra
10.57

UDP: 4 UDP packets with a AVG packet size of: 127.50, packet rate

Other: 1168 Other packets with a AVG packet size of: 915.06, packe
rate: 55.44

After thoroughly analyzing the pcap file, we have found no evidence of suspicious traffic indicative of a Distributed Denial-of-Service (DDoS) attack. The network traffic patterns appear consistent with normal activity, with no abnormal spikes in packet rates, unusual connection attempts, or high-volume requests targeting a specific host. Additionally, there are no signs of SYN floods, UDP floods and ICMP floods that would typically characterize a DDoS event. Based on this assessment, we conclude that the observed traffic does not exhibit malicious intent or behavior associated with a coordinated attack.

Results of the PCAP analysis:

- No evidence of a SYN flood attack has been detected. Only 0.37% of TCP handshakes remain incomplete, which is within the expected threshold for normal network fluctuations. Additionally, there are no abnormal spikes in SYN packet rates or signs of bursty traffic behavior that would indicate a volumetric attack.
- No evidence of a UDP flood attack has been detected.
- No evidence of an ICMP flood attack has been detected.