Atharva Yadav

Roll No. 127

Batch : S23

Network Lab

Assignment: TCPDUMP

Theory: 1. TCP (Transmission Control Protocol):

• TCP headers contain essential information for reliable, connection-oriented communication.

• Fields include source and destination ports, sequence and acknowledgment numbers, window size, and flags like SYN, ACK, and FIN.

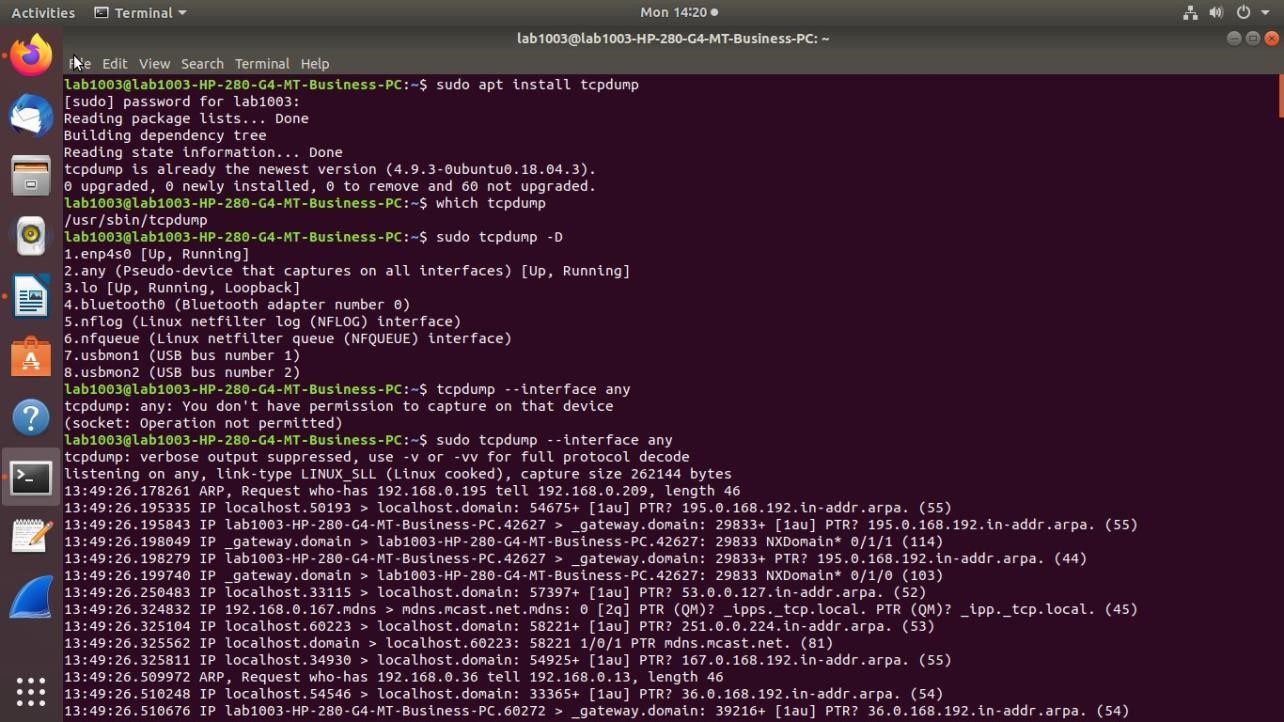
• Analysis of TCP headers helps in monitoring connection establishment, data transfer, and connection termination. 2. IP (Internet Protocol): • IP headers encapsulate data packets and facilitate routing across network devices.

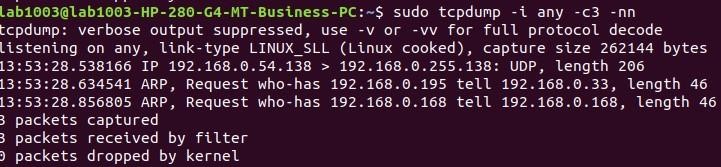
• Fields include source and destination IP addresses, version, header length, protocol, and checksum.

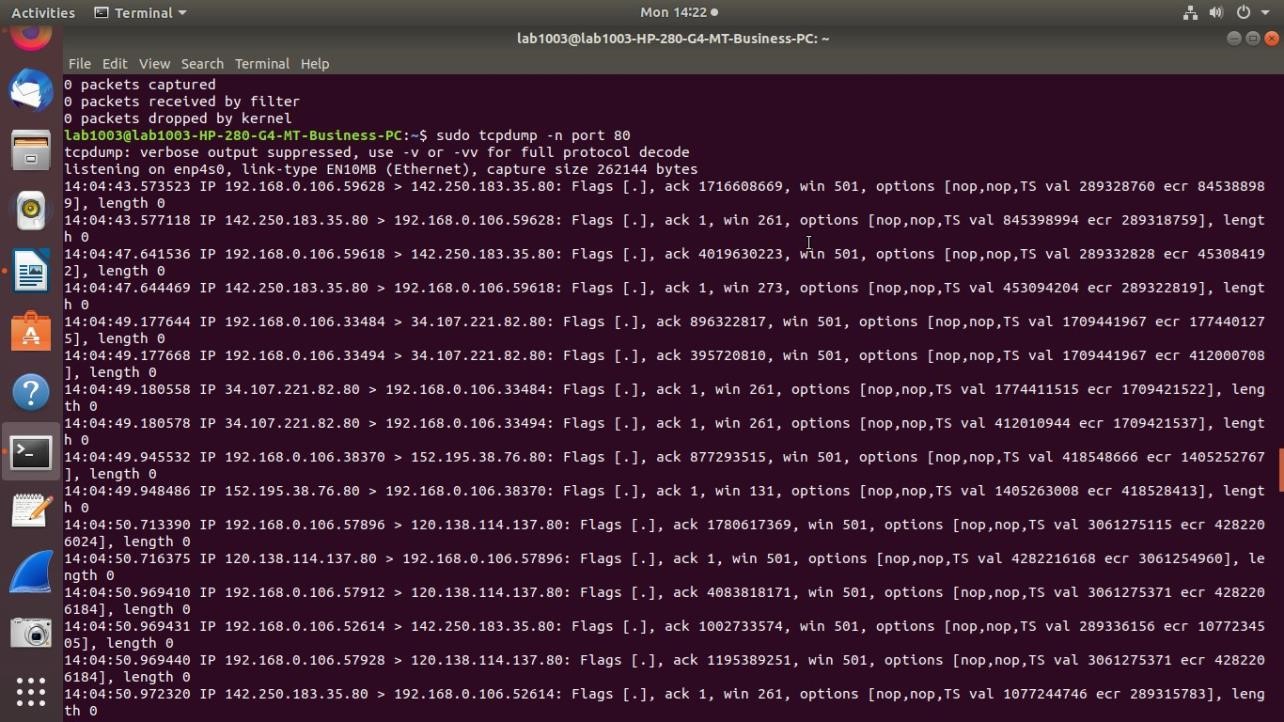
• Analysis of IP headers provides insights into packet routing, network addressing, and protocol version used for communication. 3. UDP (User Datagram Protocol):

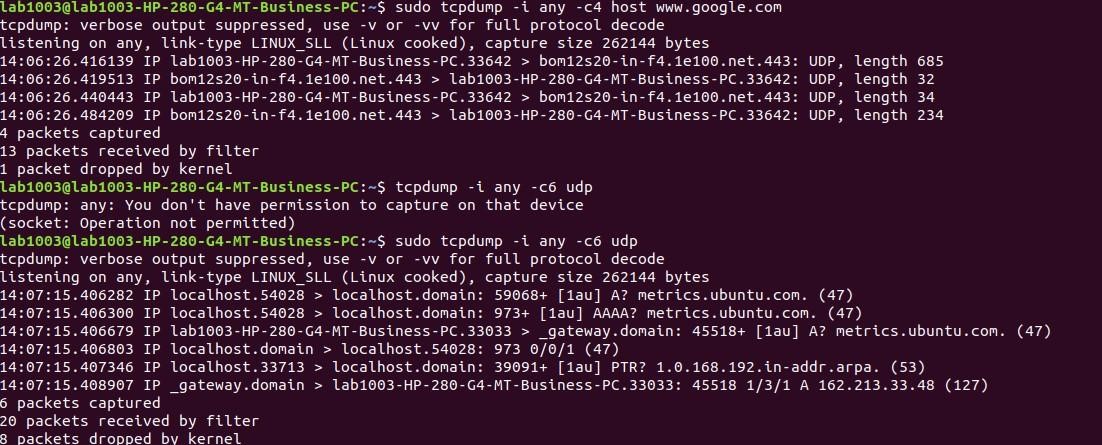
• UDP headers support connectionless, unreliable communication, ideal for realtime applications.

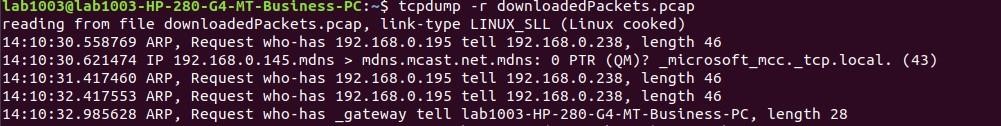
• Fields include source and destination ports, length, and checksum. • Analysis of UDP headers helps in understanding datagram transmission and reception without the overhead of connection establishment and acknowledgment.

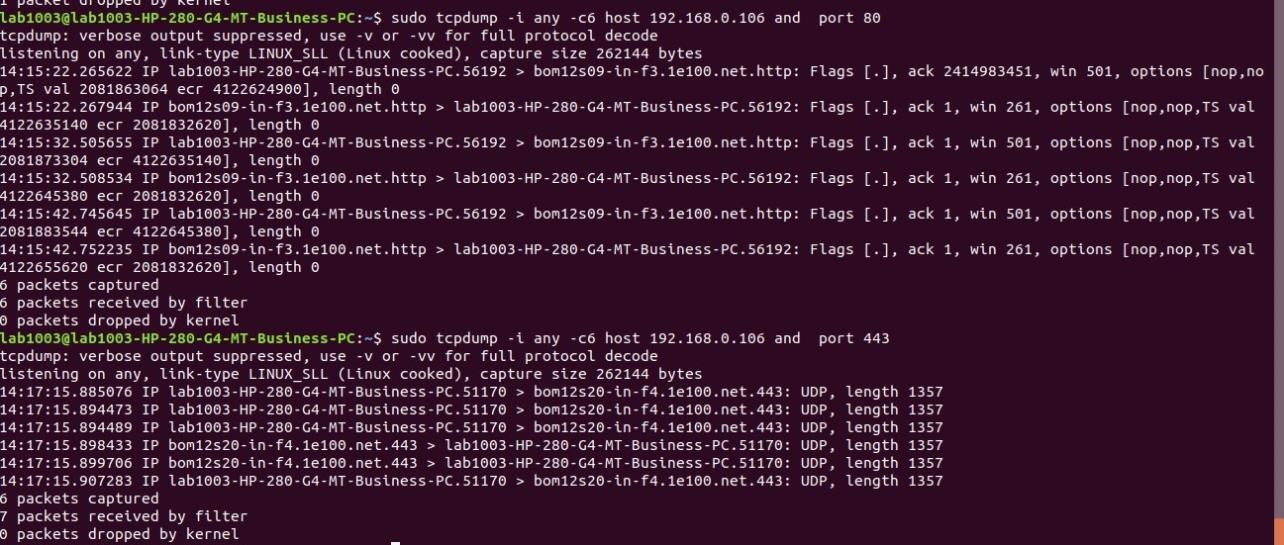












Conclusions:

TCPDUMP enables detailed examination of packet headers, facilitating network troubleshooting, performance monitoring, and security analysis.

• By analyzing TCP headers, network administrators can diagnose connection issues, monitor traffic flow, and detect potential security threats.

• Examination of IP headers aids in understanding packet routing, identifying network congestion points, and ensuring proper addressing. • Analysis of UDP headers helps in optimizing real-time applications, diagnosing packet loss, and ensuring efficient data transmission. Overall, TCPDUMP provides valuable insights into network traffic behavior and protocol usage, empowering administrators to maintain and optimize network performance and security.