Mariam Adegbindin

CIDM 6340 Network Management & InfoSec

Managing my Network

**What did I do?**

I installed Wireshark on my computer, which is connected to the network. I tweaked its settings so that my computer's network card captures all the network traffic, not just the messages sent directly to it. Using Wireshark, I started recording the network traffic, capturing details of each message such as its timing, destination, and transmission path.

Wireshark is adept at identifying various types of internet traffic and displays the nature of the exchanges—whether they involve a web page request, email communication, or video streaming. I let the recording run until I've gathered sufficient data.

Once the recording is stopped, I comb through the collected data with Wireshark's assistance. It offers handy tools to help organize and interpret the mass of information, like isolating messages from a particular device or pinpointing disruptions in communication. Additionally, Wireshark enables the creation of graphs and summaries, aiding in the visualization and clarification of any patterns or issues within the network traffic.

**What were the results?**

The traffic comprises many protocols including QUIC, UDP, ARP, and ICMPv6. QUIC is the primary protocol commonly utilized for secure communications in contemporary online applications, especially by Google services.

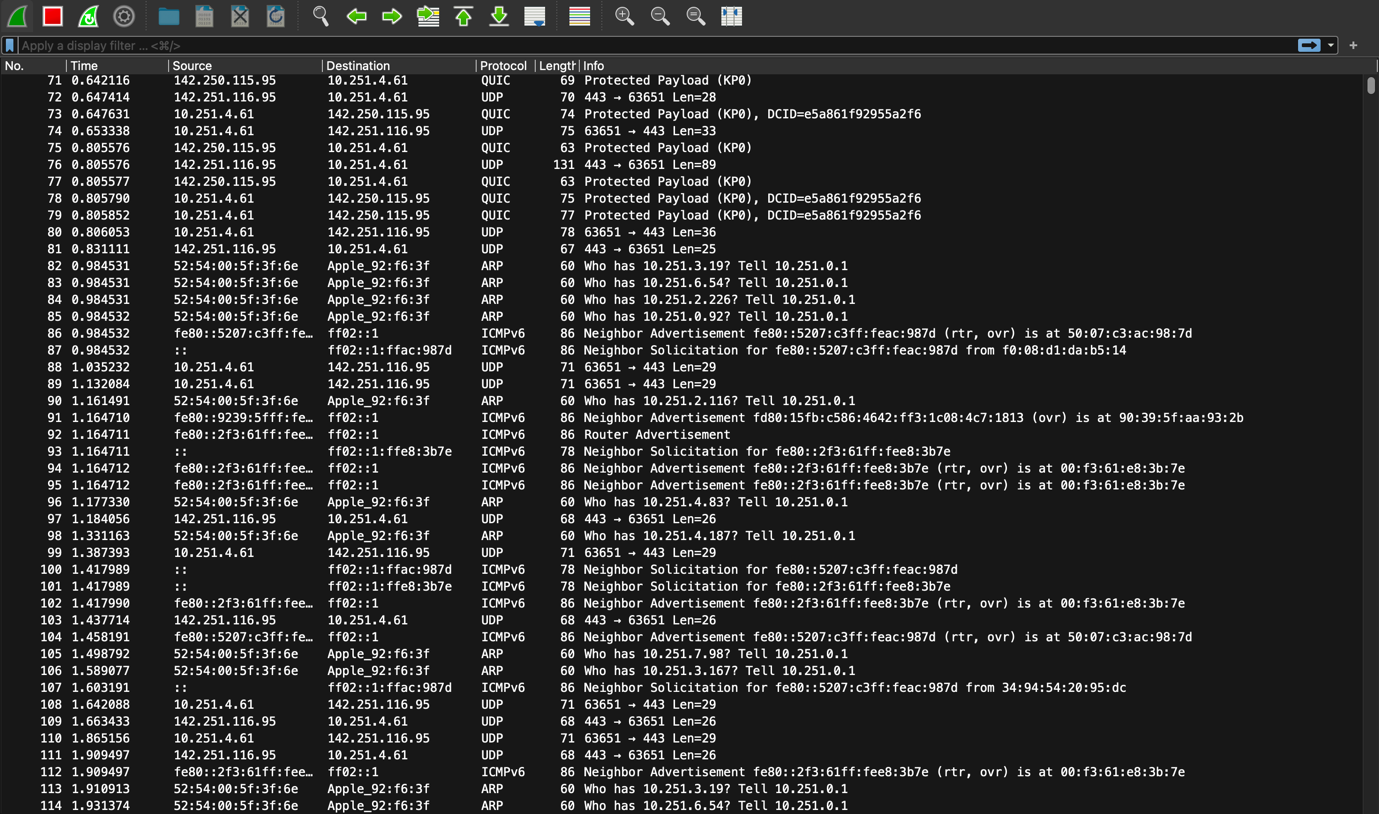
A constant communication occurs between an internal IP address (10.251.4.61) and an external IP address (142.250.115.95), mostly using QUIC protocol. This implies engaging in conversation, maybe with an online service. The port numbers used (443 and 63561) suggest a secure online connection to a server most likely handling HTTPS traffic.

Packets for common services like DNS on port 53 and HTTP/S traffic on ports 80 and 443 are seen, which are commonplace for networks interacting with the internet or internal web services. When QUIC protocol is present, it suggests the utilization of Google services, as Google commonly employs QUIC for rapid and secure web connections. ARP queries are often apparent during network operations when devices associate IP addresses with physical MAC addresses. IPv6 traffic, such as Neighbour Solicitation messages, is a component of the Neighbour Discovery Protocol (NDP) for IPv6, like ARP for IPv4.

**A screenshot of a computer

Description automatically generated**

No visible packets show immediate indicators of a cyber-attack. Indicators of an attack may include several unsuccessful connection attempts (TCP SYN floods), high levels of traffic to a specific port (indicative of a Denial-of-Service attack), or abnormal outbound connections that might imply data theft. The attack surface of a network encompasses all potential entry points for unauthorized users to gain access or take data. Open ports like 80 and 443 in this grab might be used as entry points for attacks if the corresponding web services contain weaknesses. Utilizing protocols such as QUIC implies encrypted transmission, which decreases the vulnerability to attacks by making it challenging for attackers to intercept or manipulate encrypted communications.

****

**What Did You Learn?**

Network packets are little data units sent over a network. When transmitting data via a network, it is divided into smaller units called packets. The packets include both the data being transferred and the essential headers including source and destination details, as well as routing and error-checking information.

Wireshark is a network protocol analyser, commonly referred to as a network sniffer. The tool collects packets in real-time and enables users to view the specifics of the network traffic. This is highly beneficial for jobs like diagnosing network problems, monitoring network performance, auditing network security, and doing forensic investigation following security events. Wireshark can intercept packets sent to and from a particular machine on the network. Analysts may examine the packet contents to detect malicious activities or illegal data transfers.

I have developed a sophisticated comprehension of digital networks, the complexities of packet transport, and the notion of an attack surface. By monitoring data transmission throughout the network, analyzing its division into packets, and subsequent reassembly, a comprehensive understanding of network communication in operation was obtained. This procedure emphasized the significance of the metadata of each packet, which is crucial for network diagnosis and optimization.  
  
Comprehending the attack surface, which refers to all possible areas of security vulnerability on a network, was quite instructive. Understanding this information is crucial for strengthening network security through the detection and reduction of risks like open ports or obsolete services. Utilizing this information in upcoming situations will be extremely beneficial; observing network activity helps swiftly identify and resolve security concerns, a crucial element in preserving strong network integrity.  
  
The insights obtained from this experience are highly beneficial for any firm. Proactively monitoring, analyzing, and responding to network activity can help avoid data breaches, therefore safeguarding the firm from substantial financial and reputational harm. Optimizing network performance according to traffic patterns can improve productivity and save operating expenses.  
  
Packet analysis provides practical expertise that goes beyond academic study and is essential for cybersecurity defense and network performance. This competence is crucial in the current digital environment, where proactive cybersecurity measures are not just advantageous but necessary for corporate resilience and success.