Assignment 2: Use Wireshark to View Network Traffic

By Philiphine Cheptanui

Introduction

This assignment required the use of Wireshark to sniff packets. Wireshark is a valuable tool in networking because it is used to troubleshoot networks, analyze network traffic, develop Software and protocols, and educate network enthusiasts. As traffic is transmitted over the network, Wireshark captures each Protocol Data Unit (PDU) and can decode and analyze its content. The assignment, thus, was to use Wireshark to capture ICMP traffic, IP address, and Ethernet MAC address and compare the process and experience of obtaining MAC addresses in the local subnets and remote network.

Discussion

Part 1: Capture and Analyse local ICMP data in Wireshark

In this section, I pinged the IP address of my internet-enabled mobile device, since it is on the same WLAN as my PC. The aim was to analyze the traffic and learn the MAC address on my mobile device, and how packet headers are used to transport data to the target destination. Wireshark captures all traffic in real-time, and to narrow down the results of the activity, I applied the ICMP filter since I was only interested in observing this type of traffic.

Step 3

B. Does the source MAC merge with your PC Interface?

Yes, it does. Before starting Wireshark, I used ipconfig /all to obtain the IP and MAC address of my PC (192.168.100.7; 7A.E3.76.0F.89.20). After pinging my mobile device (My pc and my mobile device are on the same WLAN), I analyzed one packet, and sure enough, the source MAC address matches the one I had recorded earlier. See Fig. 1.

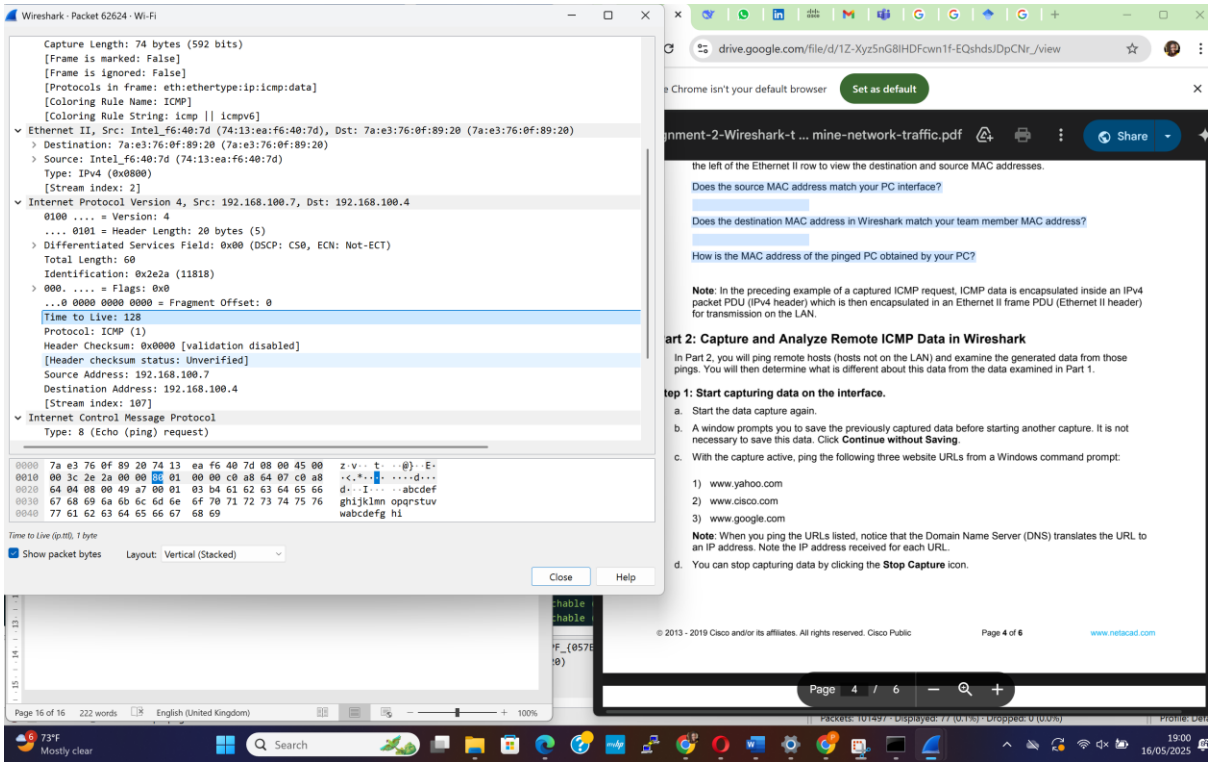

Figure 1. Source (Learner)

Does the destination MAC address in Wireshark match your team member's MAC Address?

Yes, it does. See Fig. 1

How is the MAC address of the pinged PC obtained by your PC?

When my PC pings the IP address of my colleague in the same network, my PC will need the MAC of the target device to send the ICMP request (ping). Ping initiates an ICMP request, and my PC uses the subnet mask to check if the destination IP is in the same subnet as the target PC (which is true). To send traffic to another PC on the same subnet, the target PC's MAC address is needed (Weissman, 2021). Thus, my PC will check the ARP table to see if it already knows the MAC of the target IP address. If the PC finds the MAC address associated with the target IP, the ping proceeds. If not, my PC will broadcast an ARP request (FF:FF:FF:FF:FF), asking who has 192.168.100.4 and requests the owner to tell 192.168.100.7. My colleague's PC will respond by sending a unicast ARP reply to 192.169.100.7. The reply contains its MAC and IP address. Upon receipt of the MAC address, my PC will encapsulate the ICMP ping with the source MAC and destination MAC, and then transmit it.

Part 2: Capture and Analyse Remote ICMP data in Wireshark

In part 2, I pinged three remote hosts (yahoo.com, cisco.com, and google.com). I then observed the MAC addresses and IP addresses as the packet was transmitted. In this activity, I only learned the IP addresses of these three hosts, but not their MAC addresses. However, I noted that packets in each of the three hosts had a similar MAC address encapsulated. Further research indicates that this MAC address is associated with the last hop router, which acts as the default gateway.

IP Address for www.yahoo.com: 69.147.82.60 *(See Fig.2)*

MAC address for www.yahoo.com: The remote host does not show the MAC address. It mirrors EC. 79. F2. D4.43.CB, which is the router's MAC (default gateway).

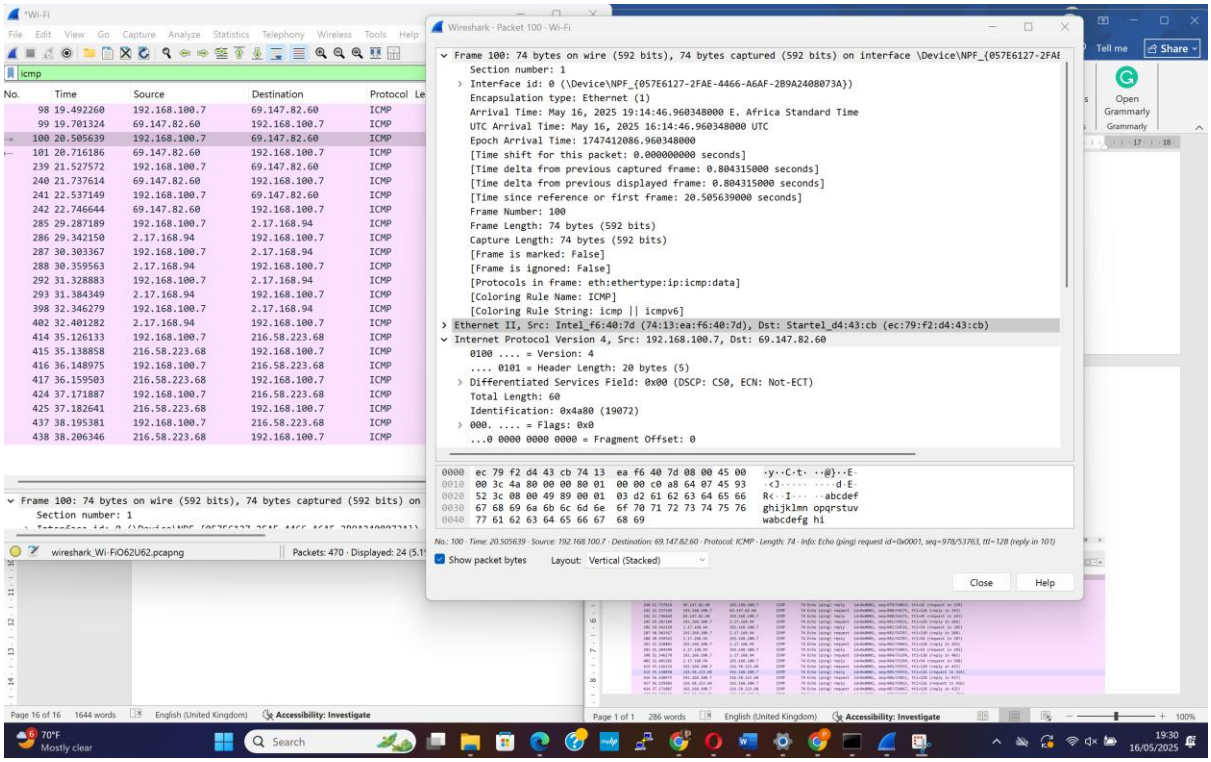

Figure 2. Source (Learner)

IP Address for www.cisco.com *2.17.168.94 (See Fig.3)*

MAC address for www.cisco.com. *The remote host does not show the MAC address. It mirrors EC. 79. F2. D4.43.CB, which is the router's MAC (default gateway).*

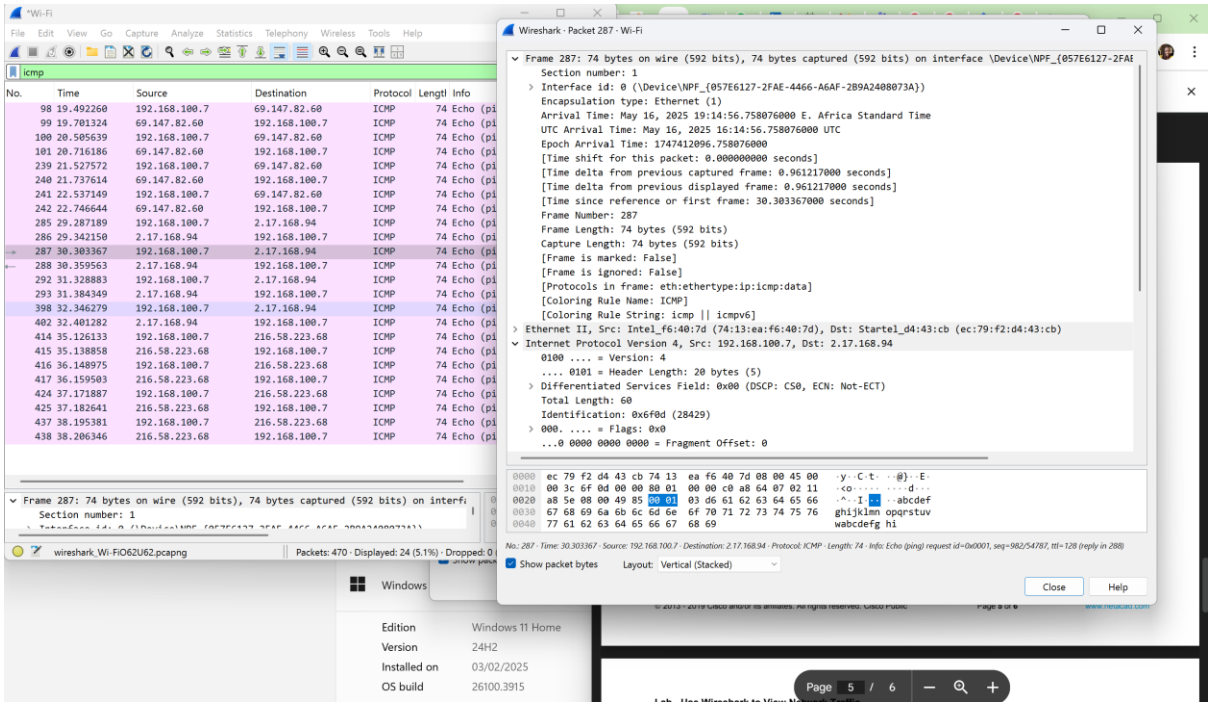

Figure 3. Source (Learner)

IP Address for www.google.com : *216.58.223.68 (See Fig.4)*

MAC address for www.google.com. *The remote host does not show the MAC address. It mirrors EC. 79. F2. D4.43.CB, which is the router's MAC (default gateway).*

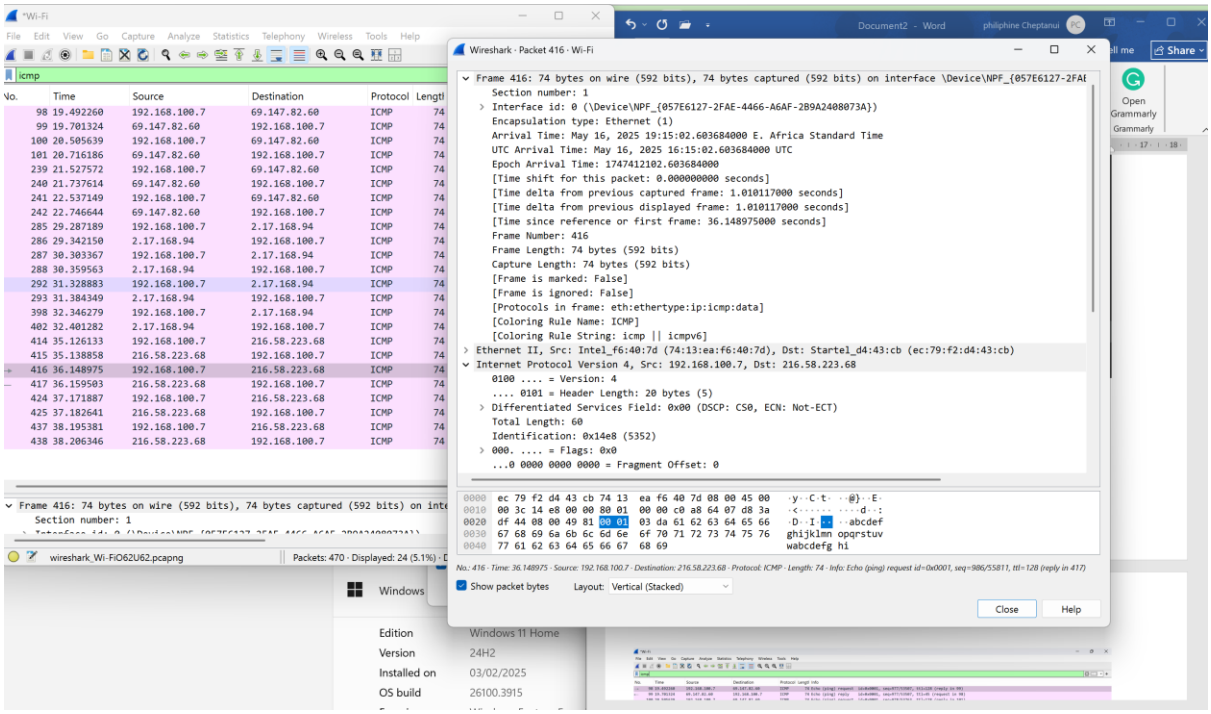

Figure 4. Source (Learner)

What is significant about this information?

The fact that I cannot see the MAC address of the target hosts is significant information worth noting. I cannot obtain the MAC addresses of the remote hosts using Wireshark or ping. Burke and Partsenidis (2024), MAC addresses are used for communication in layer 2 within the local network. When my PC pings a remote host, the packet is sent through a router (default gateway). The router forwards the packet through multiple routers, and at each router, the MAC address is rewritten to mirror the MAC address of that router (Sandip & Aibin, 2024; Ferreira Filho, & Pictet, 2021). Thus, the final MAC address becomes the final Router's MAC and NOT the destination's MAC. Hiding the MAC address is a security measure since hackers can use it to track down the hardware device globally. This, therefore, explains why ARP broadcasts are not routed beyond the local subnet. Meanwhile, the IP address of the destination host is used to forward packets. This is because the IP address is global and allows end-to-end routing.

How does this information differ from the local ping information you received in part 1?

The remote ping information differs from the local ping information in that, in the former, no MAC address was obtained for each of the three remote hosts. Remote ping relies on Layer 3 IP routing that allows the router to strip off the source MAC address and encapsulate it with its own MAC. The MAC address keeps changing from one hop to the other, as the router encapsulates the packet with new MAC addresses (Sandip & Aibin, 2024;

Ferreira Filho, & Pictet, 2021). In the latter, the MAC address is revealed because the local subnet allows for ARP ping to get the destination MAC address.

Conclusion

This Wireshark activity was a thought-provoking hands-on activity that any network enthusiast would enjoy. Local and remote pings were observed, with a close analysis of how PCs obtain MAC addresses when IP addresses are provided. It is worth noting that MAC addresses can only be obtained for devices within the local subnet and not for devices on the remote network. From the activity, I learned that PCs use a MAC address to communicate with hosts within the local subnet and use an IP address to communicate with hosts in a remote network. Pinging initiates an ICPM request, and the PC uses the subnet mask to check if the destination IP is in the same subnet as the target PC. The PC will broadcast an ARP request, and the target PC responds with a unicast ARP reply that contains its MAC and IP address. If the host is in a remote network, the ICMP request is forwarded to the router that uses the IP address of the destination host to forward packets. In a remote connection, the MAC address is not revealed because of security. This explains why a router does not forward ARP requests, and its interface acts as the end of a broadcast domain.

References

Burke J., & Partsenidis, C. (2024, July). MAC address vs. IP address: What's the difference? Search Networking. https://www.techtarget.com/searchnetworking/answer/What-is-the-difference-between-an-IP-address-and-a-physical-address.

Ferreira Filho, W., & Pictet, R. (2021). *Computer Science Unleashed: Harness the Power of Computational Systems*. Code Energy.

Sandip R., & Aibin M. (2024). Do Routers Change the MAC Address of Packets When Forwarding? Baelddung. https://www.baeldung.com/cs/routers-forwarding-mac-address.

Weissman, J. S. (2021). Principles of computer security: CompTIA Security+ and beyond lab manual (Exam SY0-601). McGraw-Hill Education.