430/530 – Wireshark Lab

Name: Youwon Song

Please review the lab directions and example screen capture provided in Canvas for exactly what is expected for each packet header image submission.

Ethernet Header Screen Capture

Ethernet Header – Broadcast Packet Screen Capture

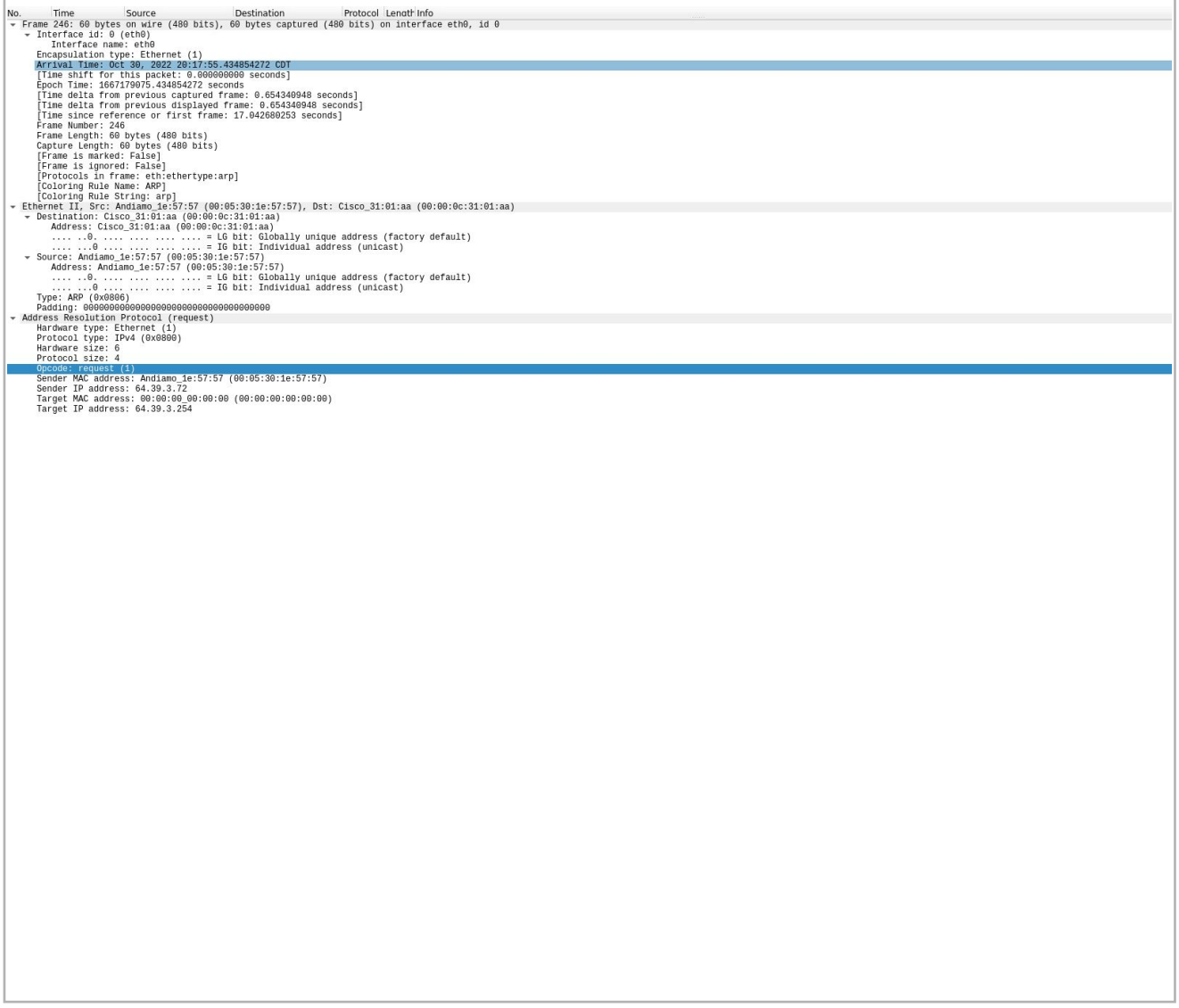
Find an Ethernet packet that is a broadcast packet. This capture should be a different packet from the **Ethernet Header Screen Capture** on the previous page.

IP Header with Kali IP Screen Capture

Most specifically, find an IP packet where the IP address matches the IP address of your Kali box. In addition to a screen capture of the IP header, include a screen capture of how you determined the IP address of your Kali box (circle the IP address on the capture, if necessary).

Kali IP Address Screen Capture

ARP Header – Request Packet Screen Capture



ARP Header – Reply Packet Screen Capture

ICMP Header Screen Capture

UDP Header Screen Capture

TCP Header Screen Capture

DNS Header Screen Capture

Lab Reflection

Answer the following reflection questions using complete sentences - use details and be specific to avoid vague answers. All responses should be *at least* three sentences. Please spend time thinking of thoughtful responses.

a) Why would a "good actor" want to use a network packet analyzer program like Wireshark?

Because it can check every details of the network packet that can be used to analyze, trace network connection, check the contents of suspect network transactions, troubleshooting networks that have some issues in performance. it would be useful for good actor.

b) Why would a "bad actor" want to use a program like Wireshark? How could they use Wireshark to their advantage? What information could potentially be gained by using a program like Wireshark?

Since it is a open-source, free program that can be used to capture network traffic in real time, it can be used by bad actor very easily. Bad actor can view data going in and out through the network. They can also sniff the packet from the network by using Wireshark.

c) Are there any countermeasures that could decrease the impact of the information a bad actor could obtain when using a program like Wireshark?

To decrease the impact of the information against a bad actor is using virtual private network called VPN. It can't prevent every impact, but it can decrease the impact of information a bad actor could obtain.

d) What connection do you see between the book's materials, lectures, and assignments and what is presented in Wireshark? What are your reactions to the amount of information Wireshark provides about each packet?

I could see some connection between the book's material, lectures, and assignments that everything i learned through them is presented in Wireshark. I could see a plenty of packets with different types of protocol with different ip addresses. I could also see lots of packets with hex values that we decoded through assignments. I was pretty surprised since each packets offer lots of information specifically that i've learned in this course, which made me spend lots of time to understand a single packet.

e) If you're new to Wireshark, what did you find most interesting about Wireshark? Be specific. If you're already familiar with Wireshark, seek out some new information, such as a different way to use filters, and share what you have learned.

I was new to Wireshark. The most interesting about Wireshark that i found is that i can filter the packet types that i want to focus on. it made me easy to check and find packets that i want. One interesting thing i've found by working this lab is that i can make a filter by myself to find something specific packets.