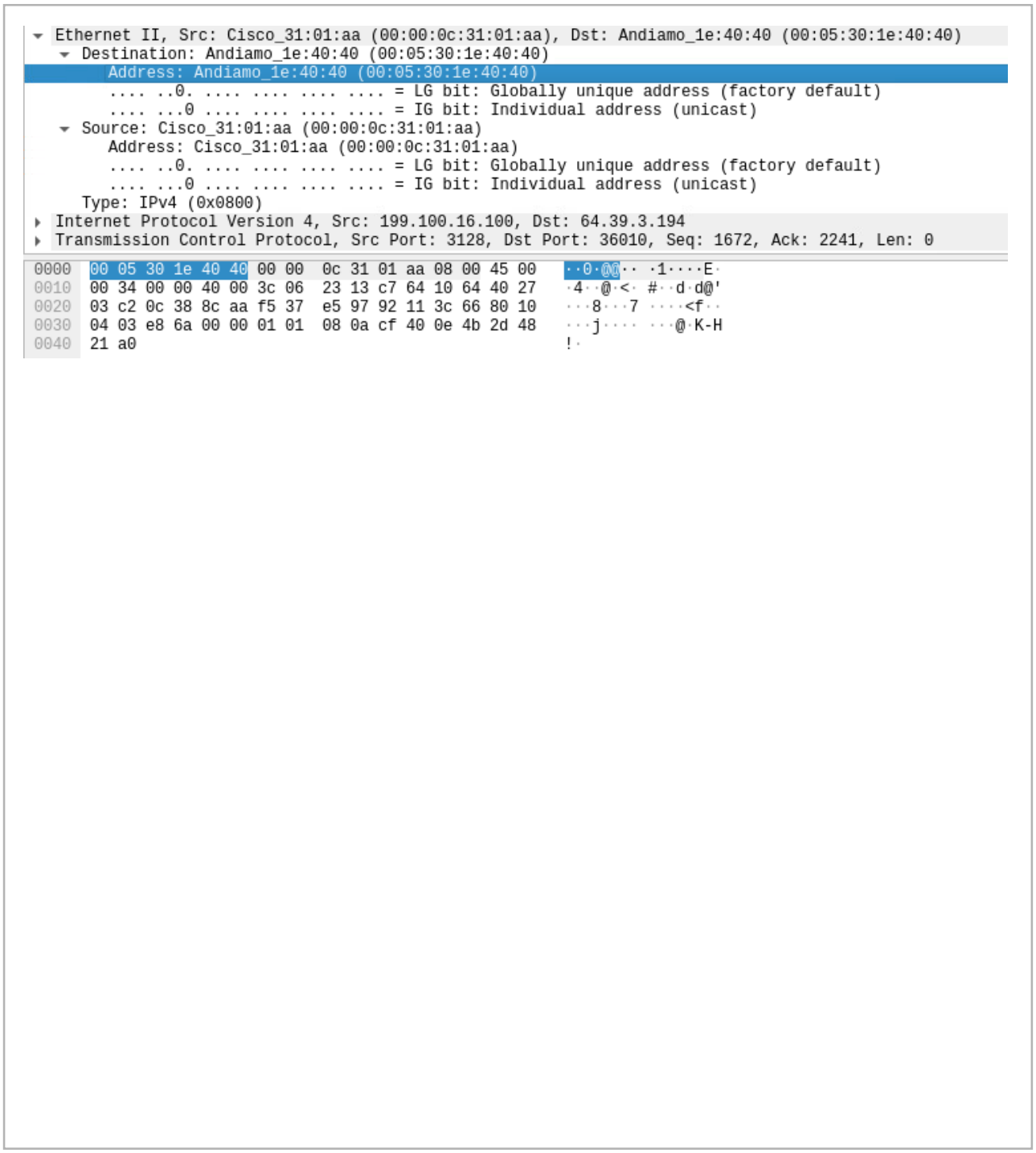
430/530 – Wireshark Lab

Name: Jacob Boicken

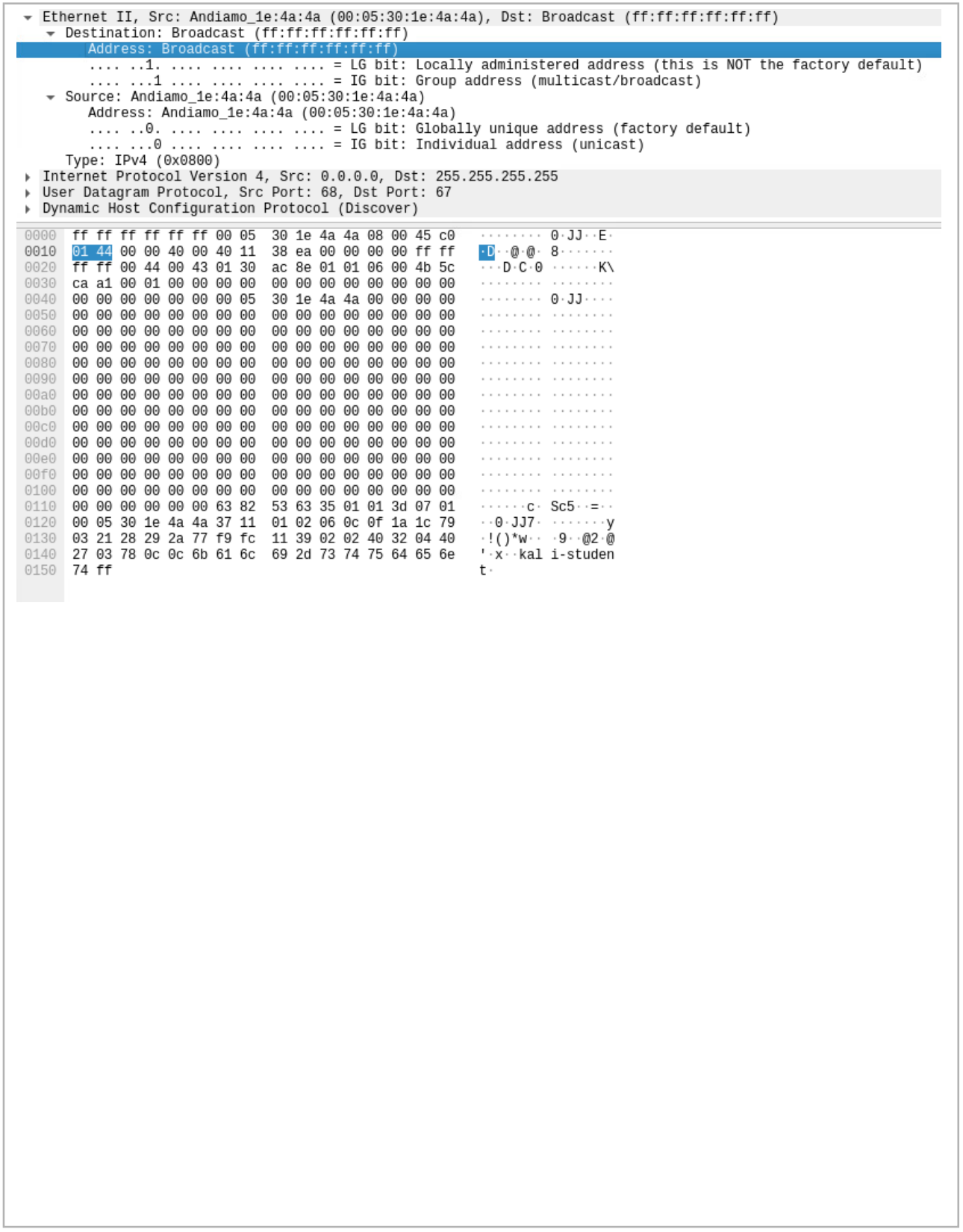
Please review the lab directions and example screen capture provided in Canvas for exactly what is expected for each packet header image submission.

Ethernet Header Screen Capture



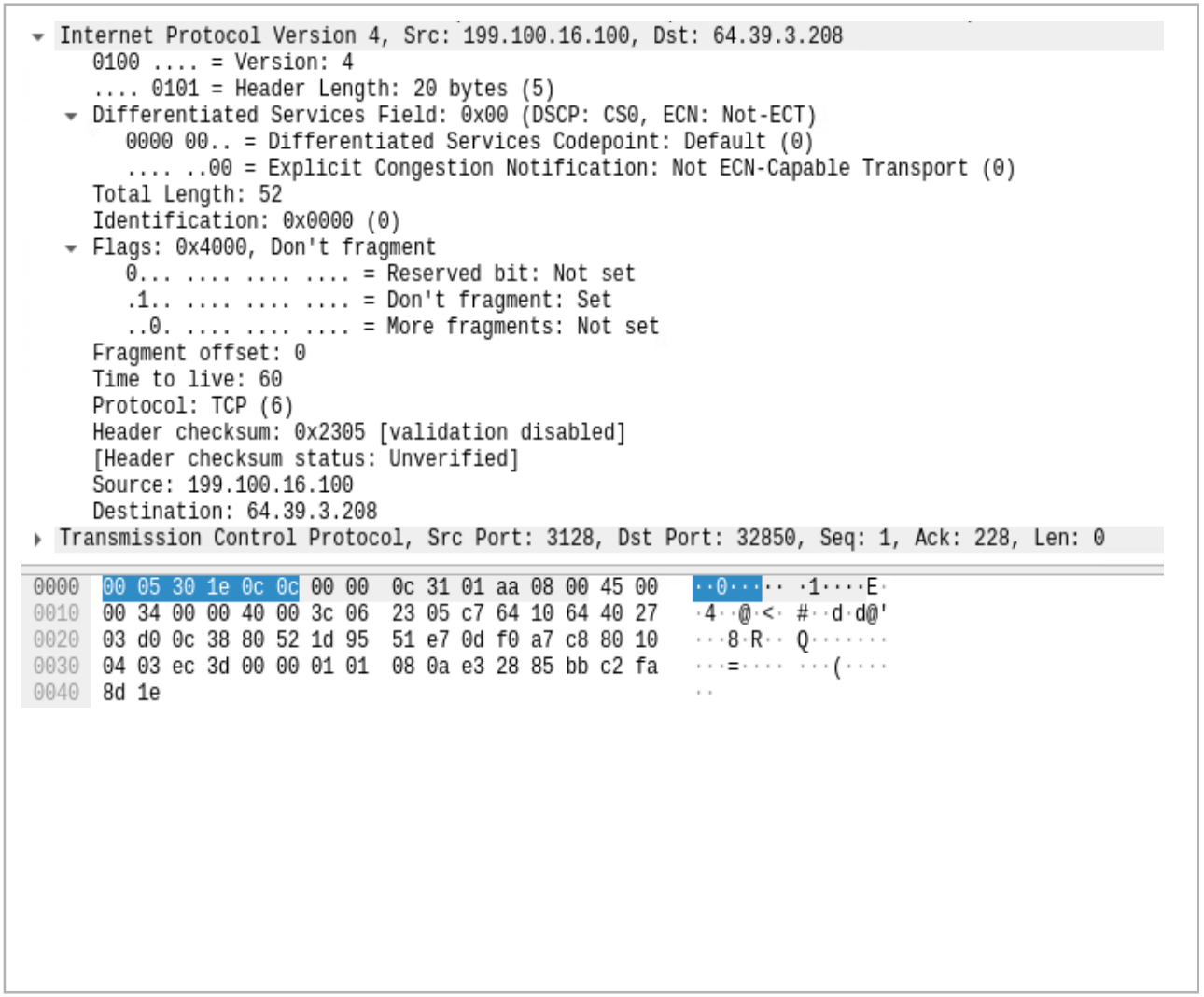
Ethernet Header – Broadcast Packet Screen Capture

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.



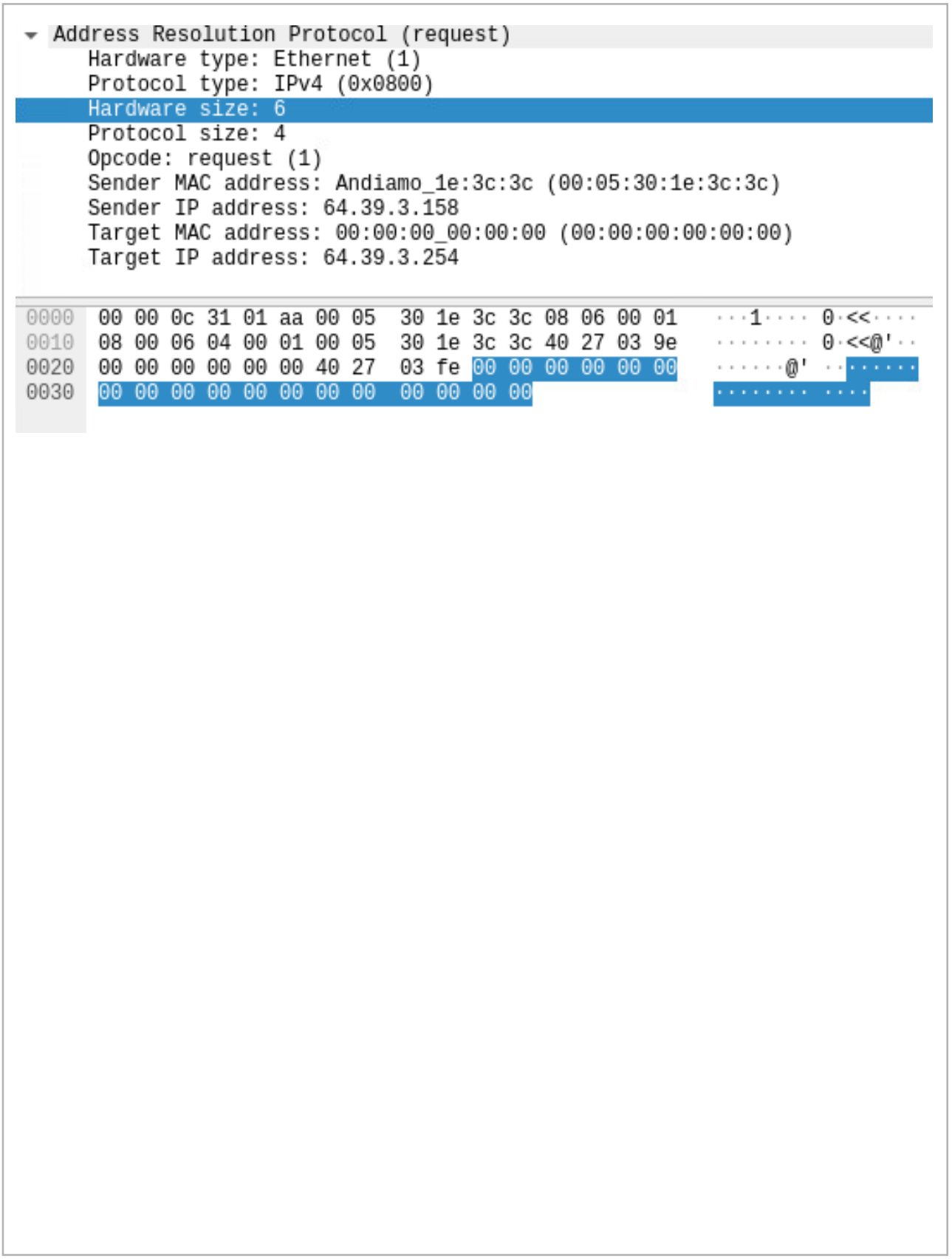
IP Header with Kali IP Screen Capture

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).

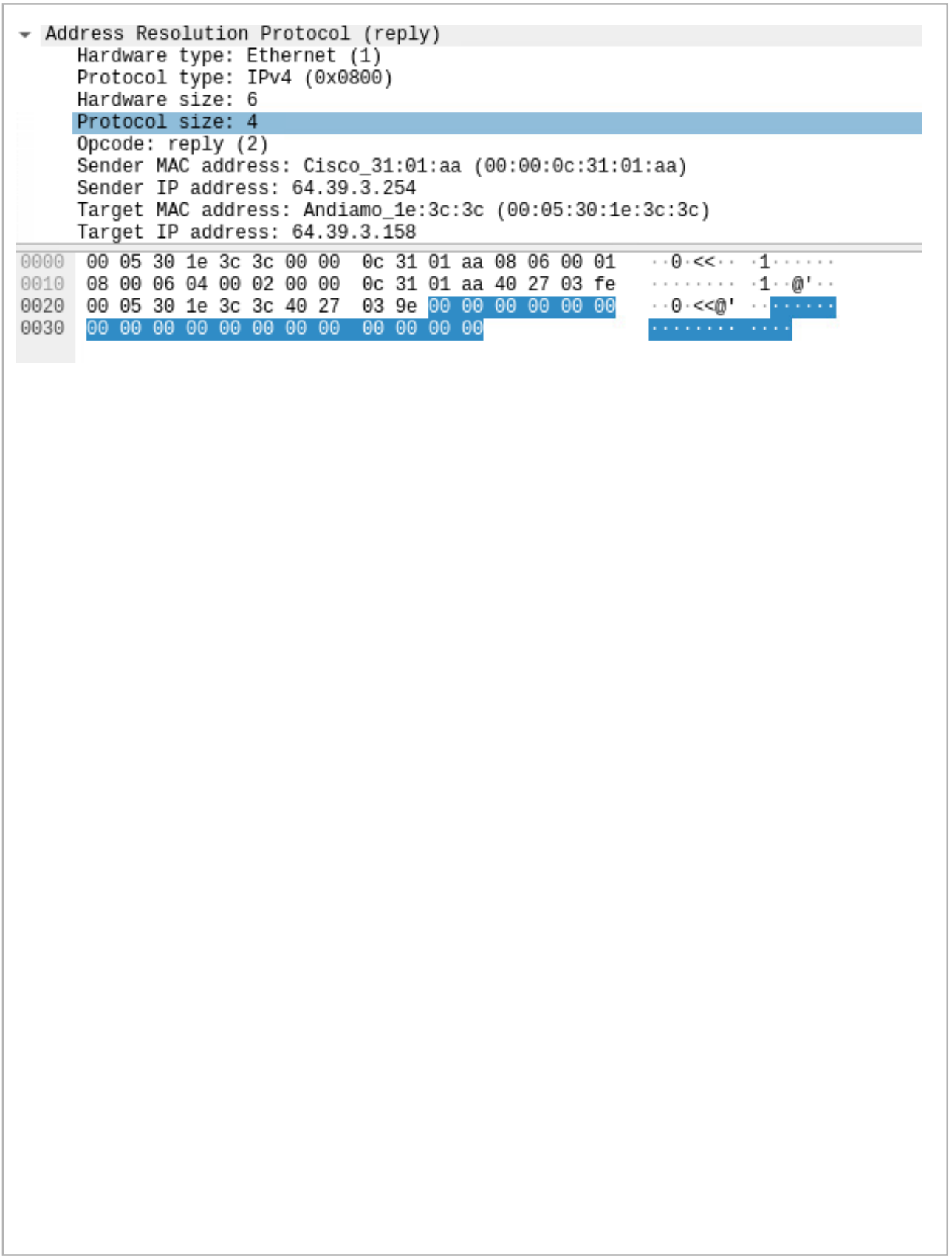


Kali IP Address Screen Capture

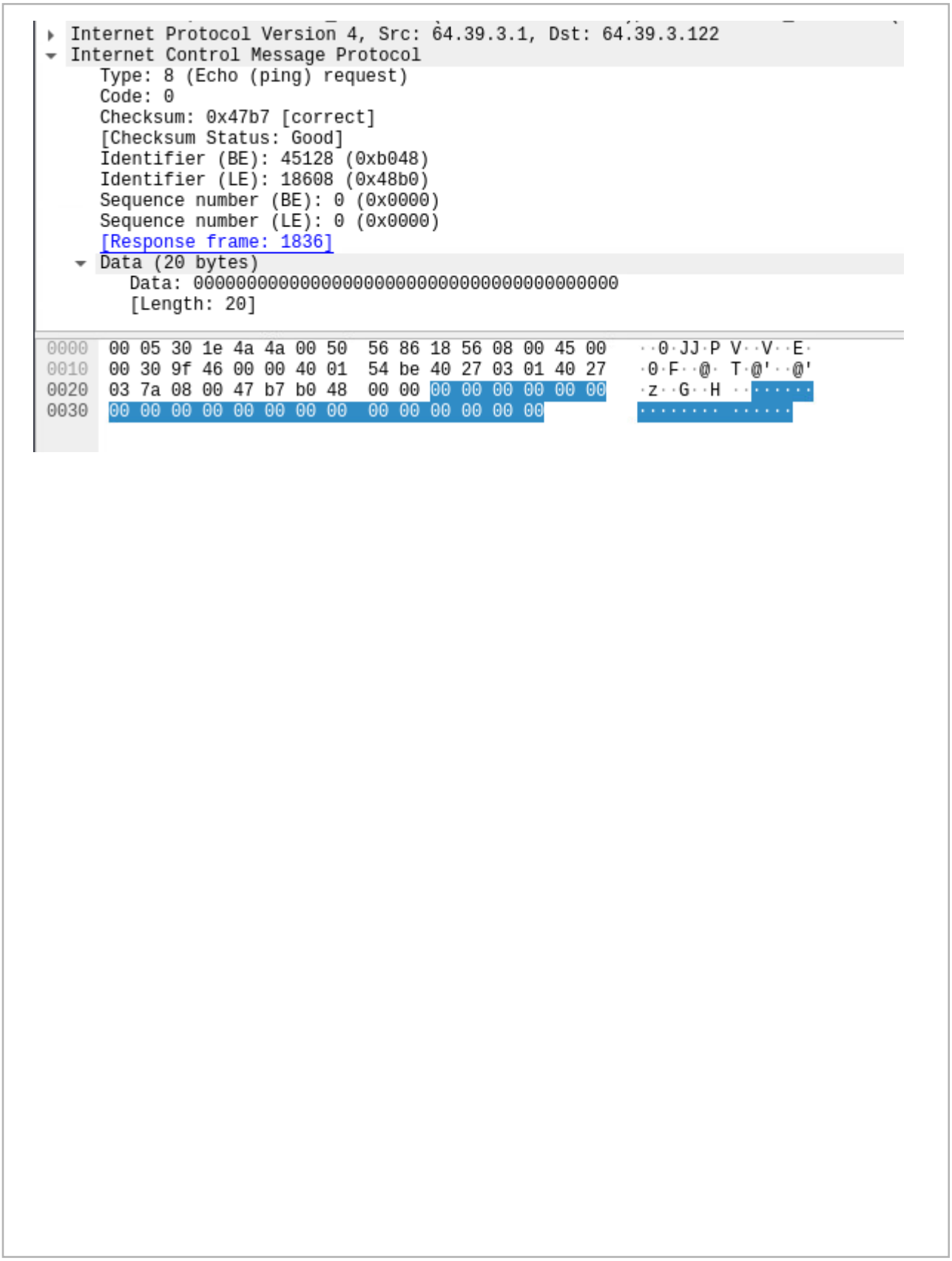
ARP Header – Request Packet Screen Capture



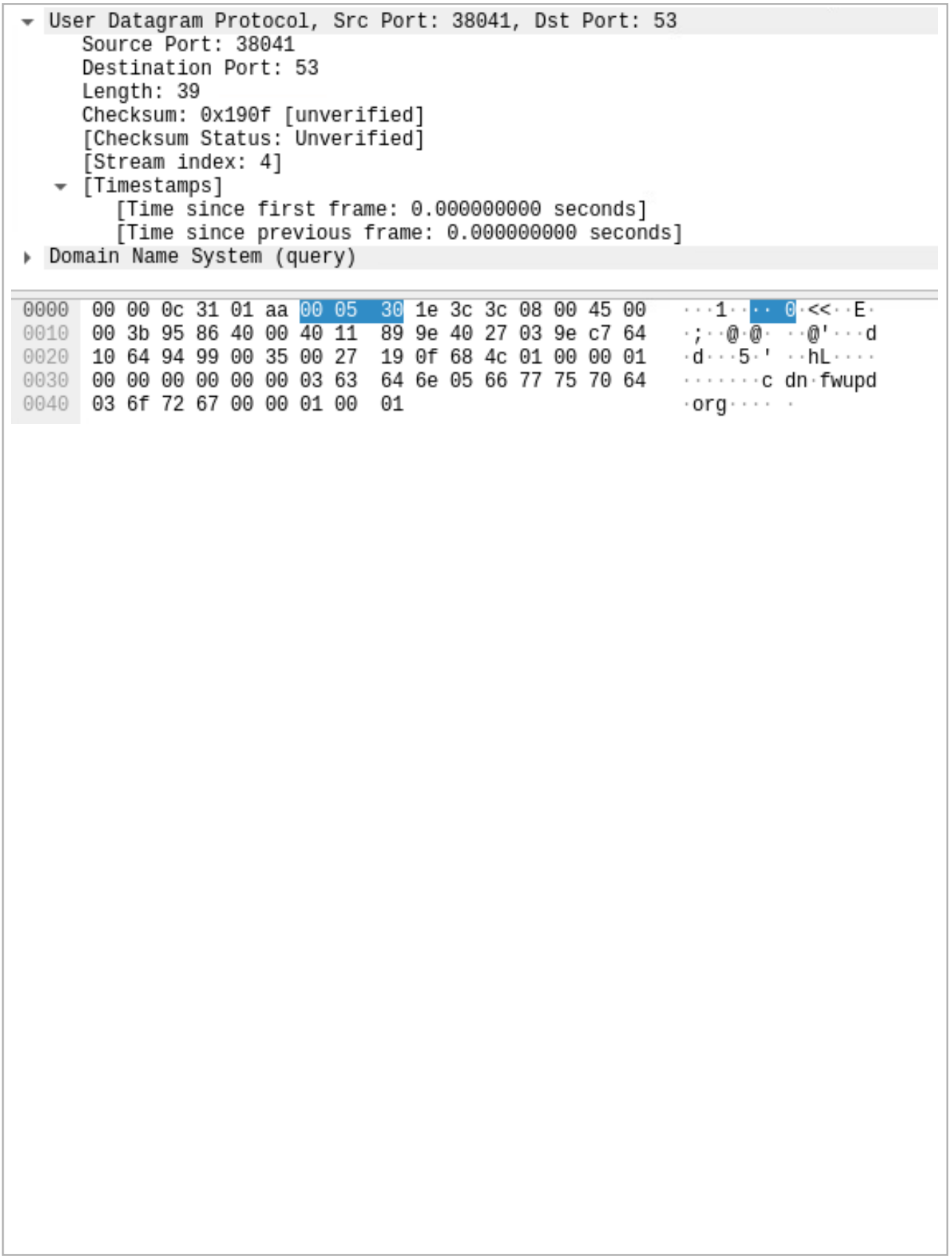
ARP Header – Reply Packet Screen Capture



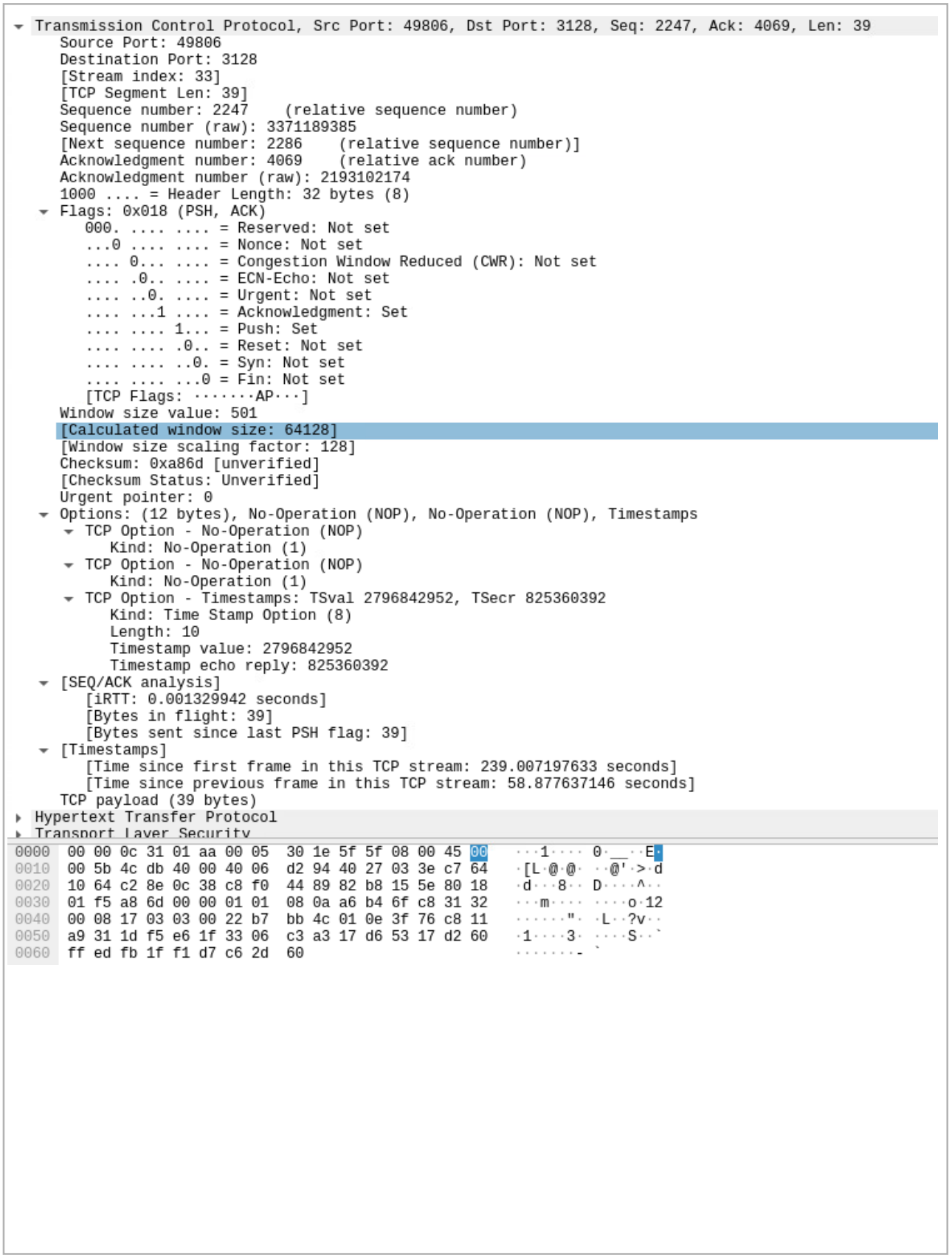
ICMP Header Screen Capture



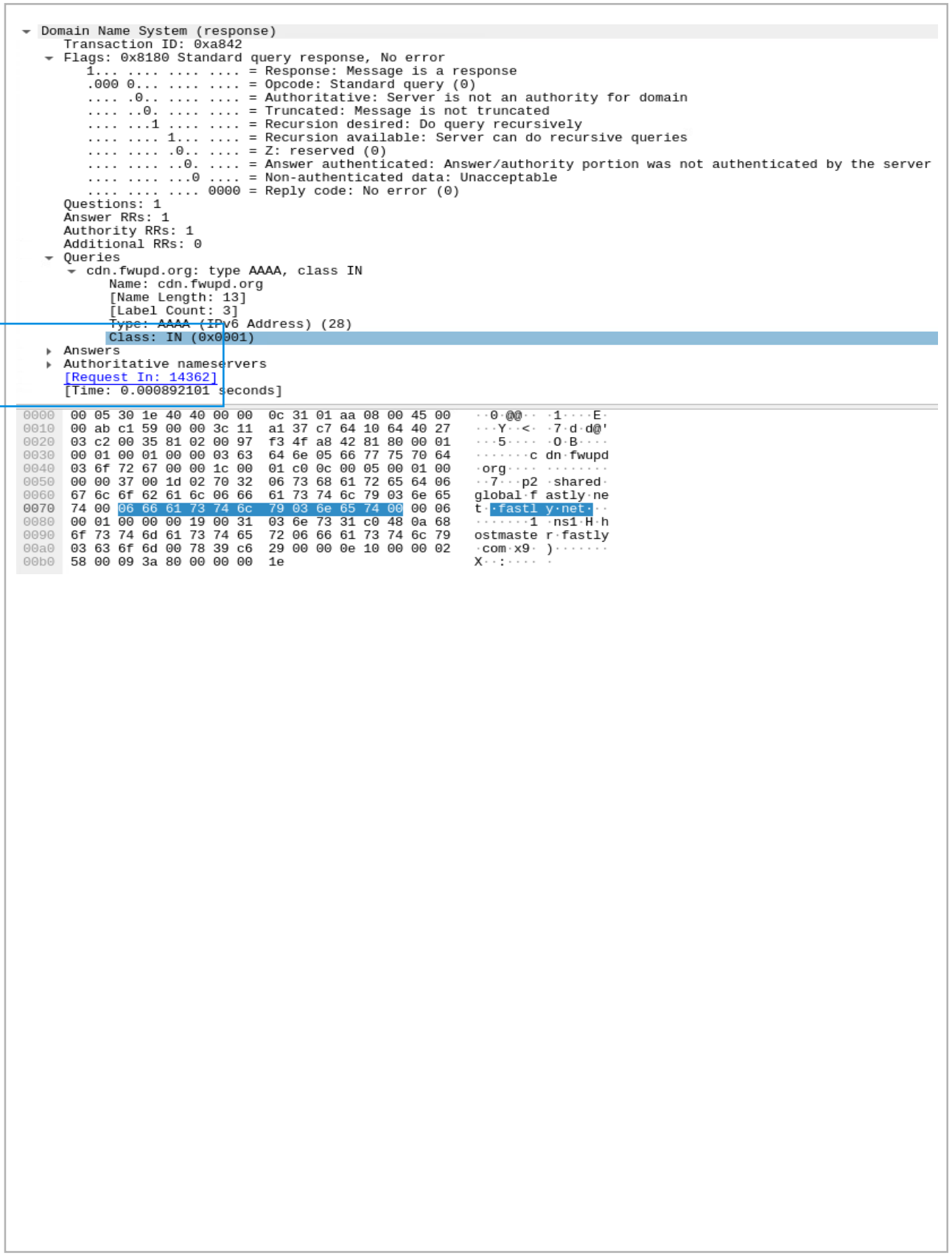
UDP Header Screen Capture



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?

A good actor, like a network admin or myself on a Saturday night trying to fix network issues, could use wireshark to view their network to diagnose where in the network connection issues are. Such as my laptop not being able to reach my web proxy, I can use wireshark to see if packets are generated to my web proxy or not to then determine if it say my host firewall blocking out bound or proxy settings not being set up.

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?

A bad actor / attacker could use wireshark for internal network reconnaissance or eavesdropping. They learn what devices talk to each other, the protocols/ports used, and any unencrypted traffic. This gives them a map of the network and can build attack points from there. Unencrypted traffic could hold information like password, auth/api tokens, or other sensitive pieces of information that is allow since it is internal, which an attacker could use.

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

Countermeasures to malicous wireshark usage would first be internal encryption anywhere possible. From then on it depends on the network design/implementation. The computer can only read what is sent to its network device, so if the device is directly behind a switch it should only be able see traffic addressed to itself. The same goes for encrypted wireless. Hubs/buses and other network designs can allow for a single client to see more traffic than want it is meant to read.

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?

From the lectures, we hear Dr. Jacobson talk about network devices operating in promiscuous mode. Wireshark shows us what that mode is able to pick up and what sniffing looks like (in scale). For the amount of information that wireshark picks up, its simply copying what the network device on the computer holds, so we get the headers/data of Ethernet, IP, TCP/UDP, and etc. This matches up with what we have seen in the hw/quizzes as well.

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 have used wireshark somewhat before. However, since I don't know the filters very well, I ended up trying to use "!=" as a not equals. This didn't work. Rather, you have to do !(ip.addr == x.x.x.x). As well, looking at the drop down list when typing in a filter, I found interesting searches you can do like looking up by geoip/location or selecting usb or usbaudio which are interfaces. You can then filter by usb/audio fields. I did not know wireshark can be used for all sorts of devices.