COSC 4377 – Networking - Kevin B Long

# interlocking-uh-m-186.eps

Homework #1

Summer 2023

Your name:

Your Student ID:

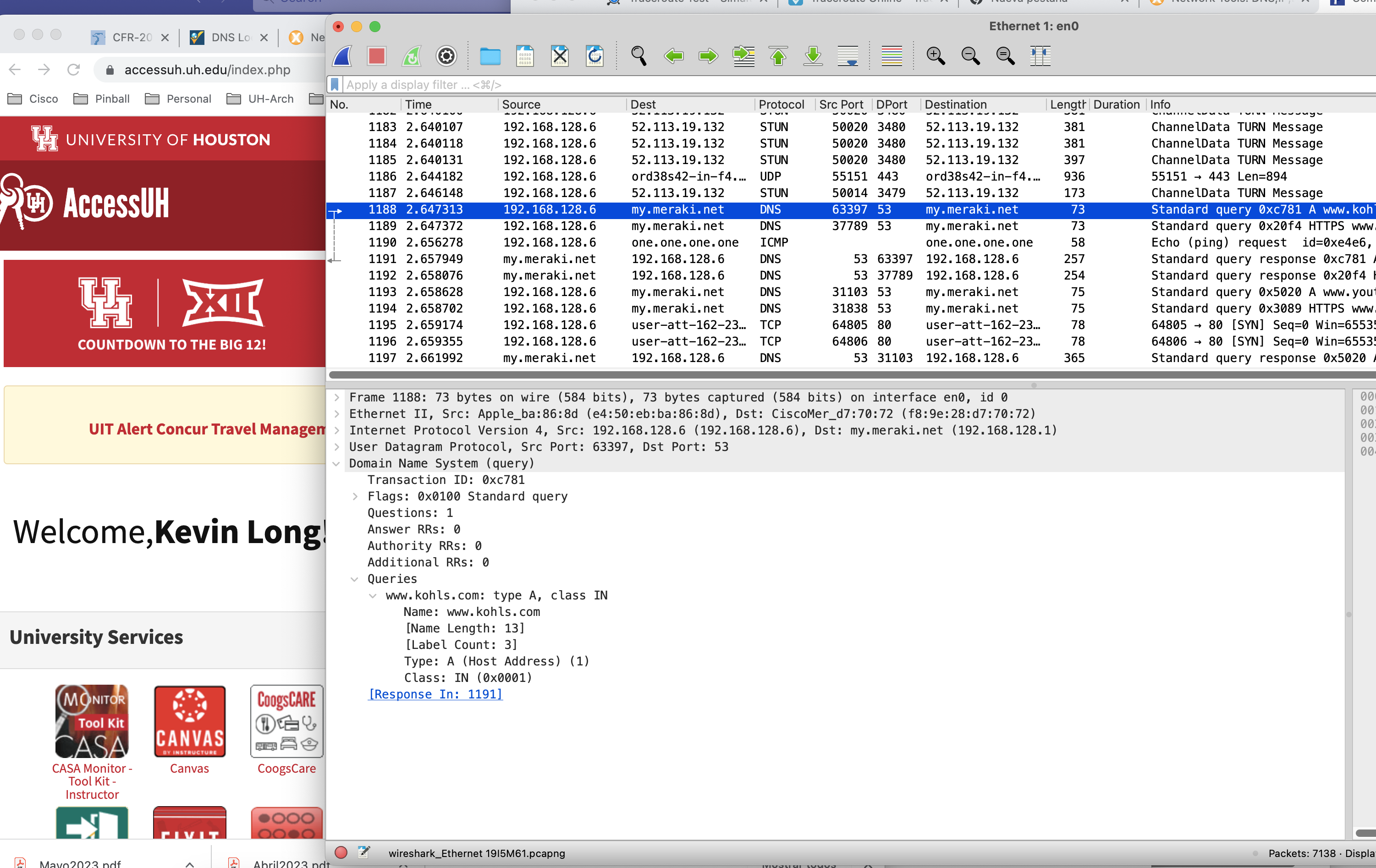
Tip: Make sure you review the first part of the lecture 6 recording to learn how to do this homework. There are some helpful tips in that which will make this easier to understand.

1. Open the Intro to Wireshark lab. You’ll find the lab in the Teams General channel under Files, Class Materials, Wireshark labs.

Don’t insert your answers into the Wireshark document you download there. Instead, fill them out here. Just so you know, my questions do not follow the lab’s questions.

First, include a snapshot of your wireshark window showing the various answers for each question. Have some UH window open behind it with enough showing to let us see your name.

For example, here’s an image I might include:



You’ll see a spot to include a snapshot each time I ask for one.

* 1. Which of the following protocols are shown as appearing (i.e., are listed in the Wireshark “protocol” column) in your trace file: TCP, QUIC, HTTP, DNS, UDP, TLSv1.2?

Your answer:

Include a snapshot showing some of the protocols you just listed.

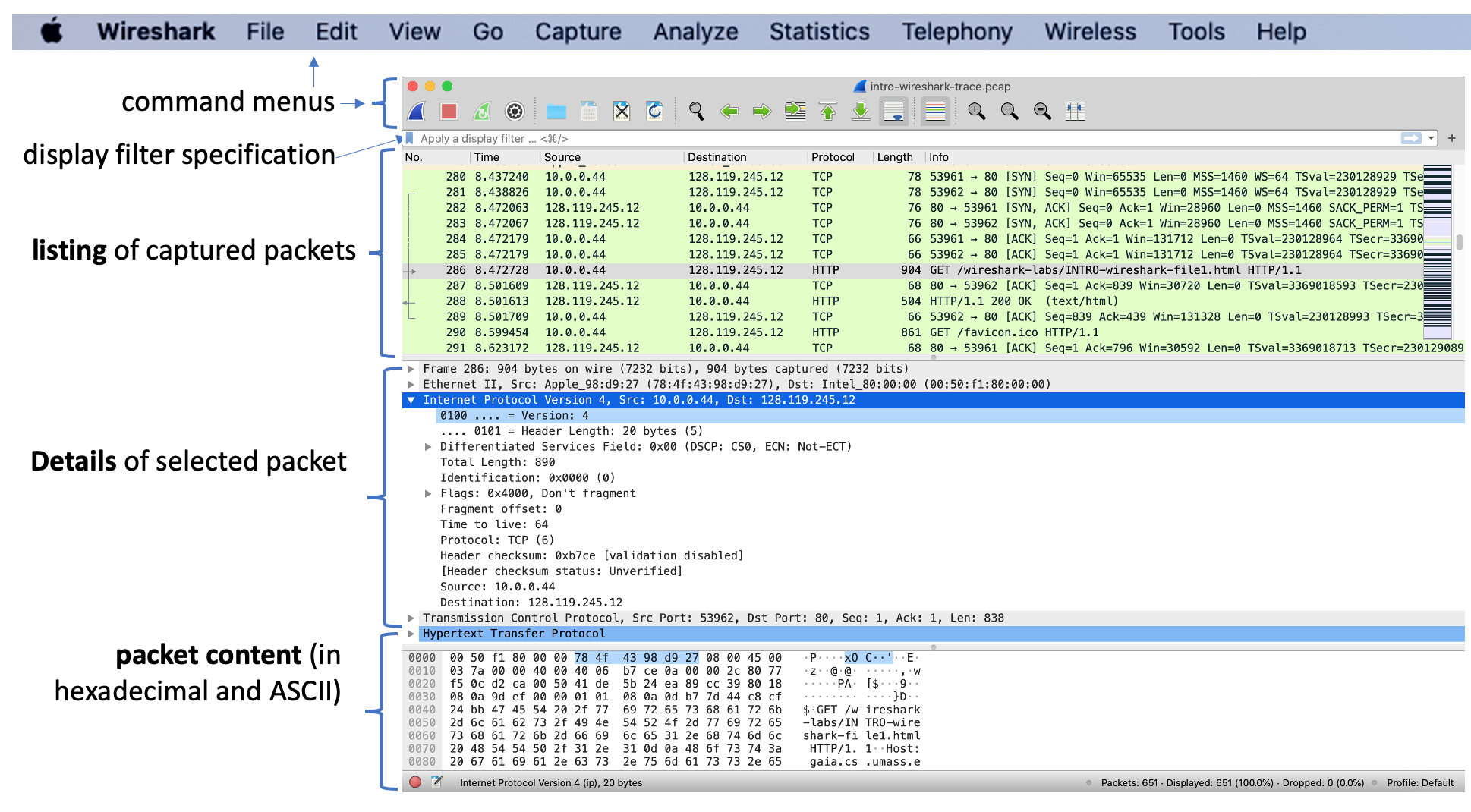
<replace this with your screen capture>

* 1. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received
  2. Find a packet from or to gaia.cs.umass.edu. What’s its (IP) address?
  3. What’s the IP address of the computer that sent the HTTP GET message (your computer)?

Include another screen snapshot if needed to show the data you used for this answer and the previous two answers – they should all be on the same page, I think.

<optionally replace this with your screen capture>

Note: some of you may find that you have been assigned an IPv6 (IP version 6) address by your router instead of an IPv4 address. They look very different, but Wireshark can handle them. Don’t be concerned if your address has this format:   
“2001:0db8:85a3:0000:0000:8a2e:0370:7334.”

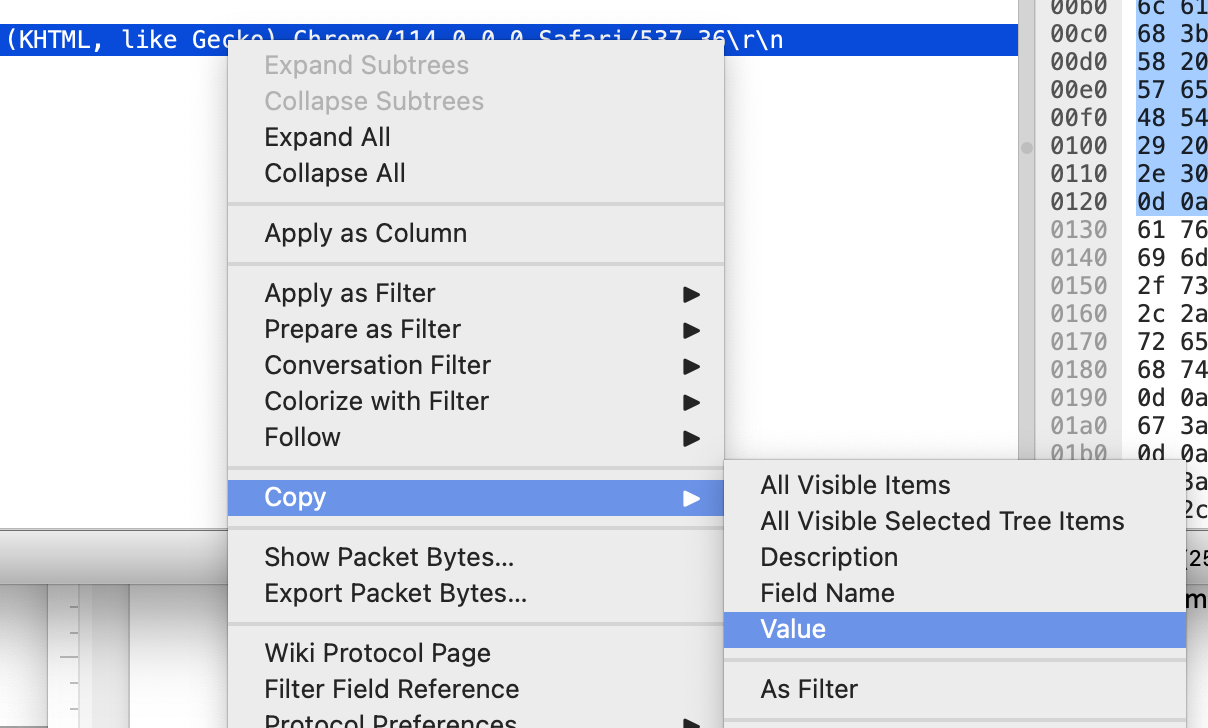
* 1. Expand the information on the HTTP message in Wireshark’s “Details of selected packet” window so you can see the fields in the HTTP GET request message. Here’s the example from the lab:

What type of Web browser issued the HTTP request?

The answer is shown following the “User-Agent:” field. This field value in the HTTP message is how a web server learns what type of browser you are using. You may remember from class that most of the time the browser reports the type of HTML formatting with which it is compatible, which is usually more than one. We figured out by process of elimination in lecture that Chrome on a Mac reports that it’s compatible with and can process HTML code sent according to four HTML browser specifications: Mozilla, AppleWebKit, Chrome, and Safari (see the dark blue line in the image).



For your answer, copy and paste in the entire field value from Wireshark by right-clicking or command-clicking on the User-Agent line that has the answer and selecting Copy->Value (see image below). Then you can just paste it in the field above. Make sure it’s from the browser, not the web server – look at which IP is the source and which is the destination if you get confused.



* 1. Expand the information on the Transmission Control Protocol for this packet so you can see the fields in the TCP segment carrying the HTTP message. What is the destination port number (the number following “Dest Port:” for the TCP segment containing the HTTP request) to which this HTTP request is being sent?

From our discussion in class, is this a “well-known” port number? Y. N

What’s the port number your operating system appears to have assigned your browser?

From our discussion in class, is this source port number likely a “well-known port?”

Y N

If your prior image(s) did not show the TCP port numbers, include one here.

<replace this with your screen capture>

1. Let’s continue with questions about the Wireshark lab that are just for our class.
   1. Is your IP address really your IP address? You can see your source address in Wireshark, but very often that address is changed at the edge of your network (for reasons we’ll discuss soon).

Go to <https://www.lookip.net/ip>, and first let’s enter the IP address Wireshark says you have. LookIP will tell you if your IP address is part of a block owned by an organization or that is is a private address. Which does it say?

Owned by an organization or  A private IP

* 1. Now go to a different page at the same site: <https://www.lookip.net/what-is/my-ip>. This causes a bunch of packets to be sent from your browser to their web server as happens with any page you are trying to load. We know that those packets began at your computer and we know your IP address. But what IP address does LookIP state is yours?

Is it the same as the one Wireshark is reporting?

Y N

If it is not, it is likely that Network Address Translation is changing it. We will learn more about that later.

That’s it for the Intro Wireshark lab.

1. Turn your attention to a different Wireshark lab, the one on DNS. You’ll find it in the same folder as you did the Intro lab. Don’t answer the questions in that Word doc. Instead, do the lab, but answer the questions presented here:

Divide your student ID # by 500. Write the remainder (between 0 and 499) here:

Find that number in the file whose name starts with “500 hosts” in the General->Files->Class Materials folder on Teams. What host name are you being assigned to investigate?

1. Run nslookup for that host by opening a terminal or command window and typing

nslookup <host>

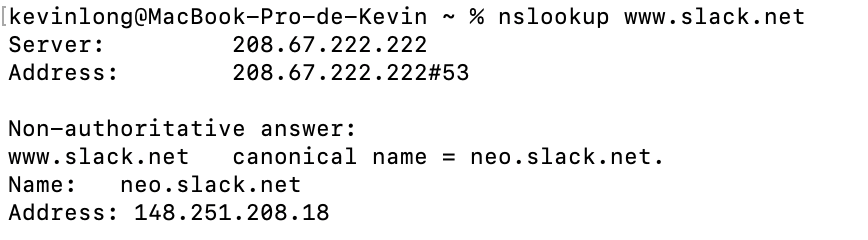
where <host> is the assigned host from the spreadsheet. You will get a block of text back.

Does nslookup provide you with a “canonical” name? This indicates that the host name you were assigned is an alias for the real host, but not the primary name of the host in DNS records. If you are given a canonical name, list it here:

If you are shown more than one IP address for your assigned host, you are seeing DNS’s attempt to balance the load on servers by using a “round robin” technique to cycle among the IPs. You won’t be able to tell the one you’re using from this. To figure it out, **ping** the host from a terminal window. The particular IP it is using, which it learned from DNS, is shown.

According to DNS and possibly your ping test, what’s the target host’s IP address?

Include a screen snapshot of your nslookup command and results like this:



<optionally replace this with your screen capture>

1. What is the IP address of the DNS server that provided the answer about your assigned host? For my nslookup, the DNS server was 208.67.222.222. What’s yours?

Does it appear that this might be the default local DNS server? You can tell by whether the IP address starts the same and mostly matches your own IP address.

1. Did the answer to your nslookup command come from an authoritative or non-authoritative server?  Authoritative  Non-authoritative

An authoritative server is the DNS server for the domain name with the official DNS records. A non-authoritative server is any other source between the authoritative server and your computer that has a copy cached that’s still within its time-to-live.

Tracing DNS with Wireshark

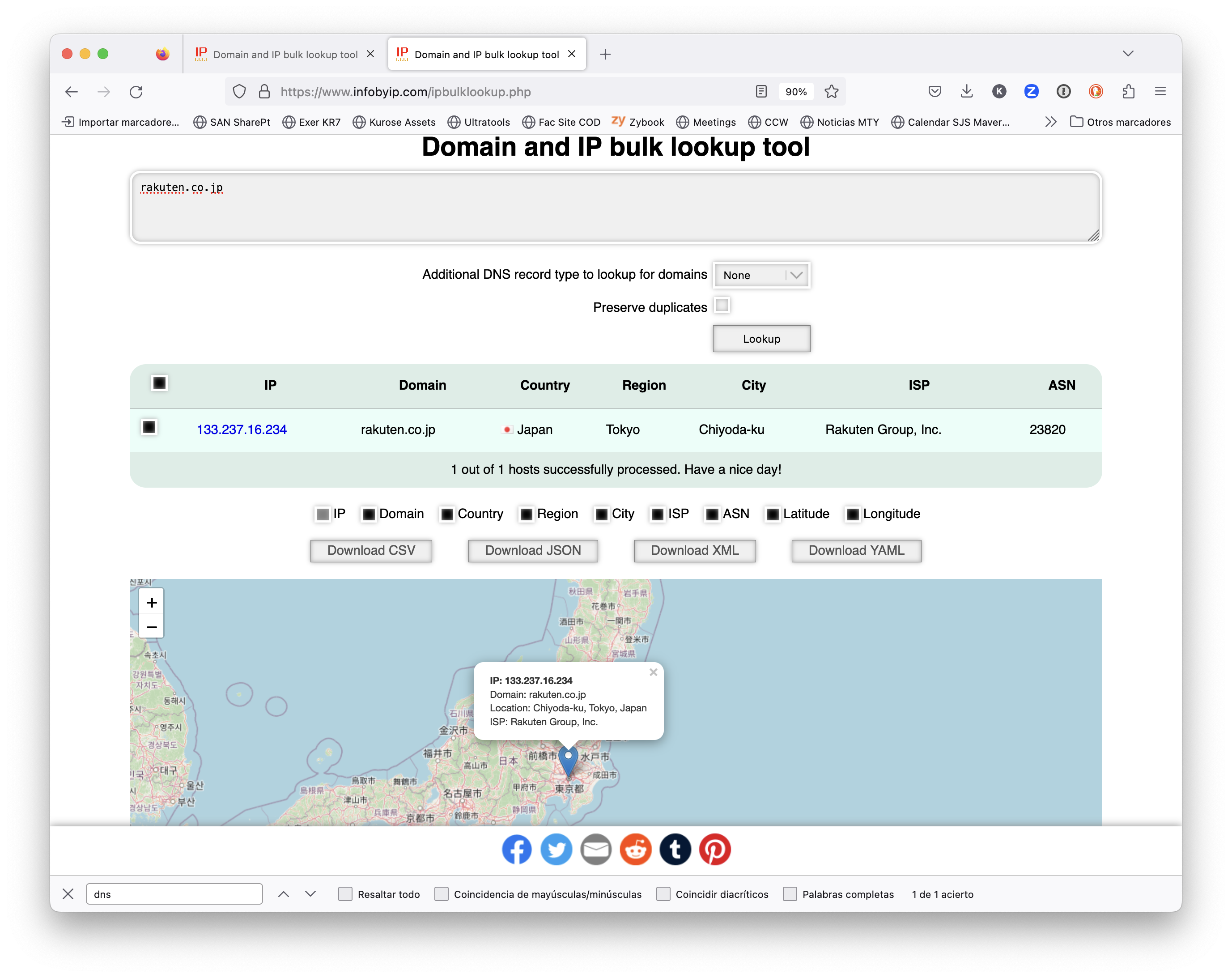
1. Locate the first DNS query message resolving the name of your host. What is the packet number[[1]](#footnote-1) in the trace for the DNS query message? Is this query message sent over UDP or TCP?
2. Now locate the corresponding DNS response to the initial DNS query. What is the packet number in the trace for the DNS response message? Is this response message received via UDP or TCP?
3. What is the destination port for the DNS query message?

What is the source port of the DNS response message?

1. Examine the DNS query message. How many “questions” does this DNS message contain?

How many “answers” does it contain?

1. The web page for the base file <http://gaia.cs.umass.edu/kurose_ross/> references the image object <http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E_2.jpg>, which, like the base webpage, is on gaia.cs.umass.edu.   
   What is the packet number in the trace for the initial HTTP GET request for the base file <http://gaia.cs.umass.edu/kurose_ross/>?         
   What is the packet number in the trace for the HTTP GET request for the image object <http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E2.jpg>?
2. Go to <https://www.infobyip.com/ipbulklookup.php> and type in your assigned host’s name (the one from the spreadsheet earlier). You are looking to get something back like this:

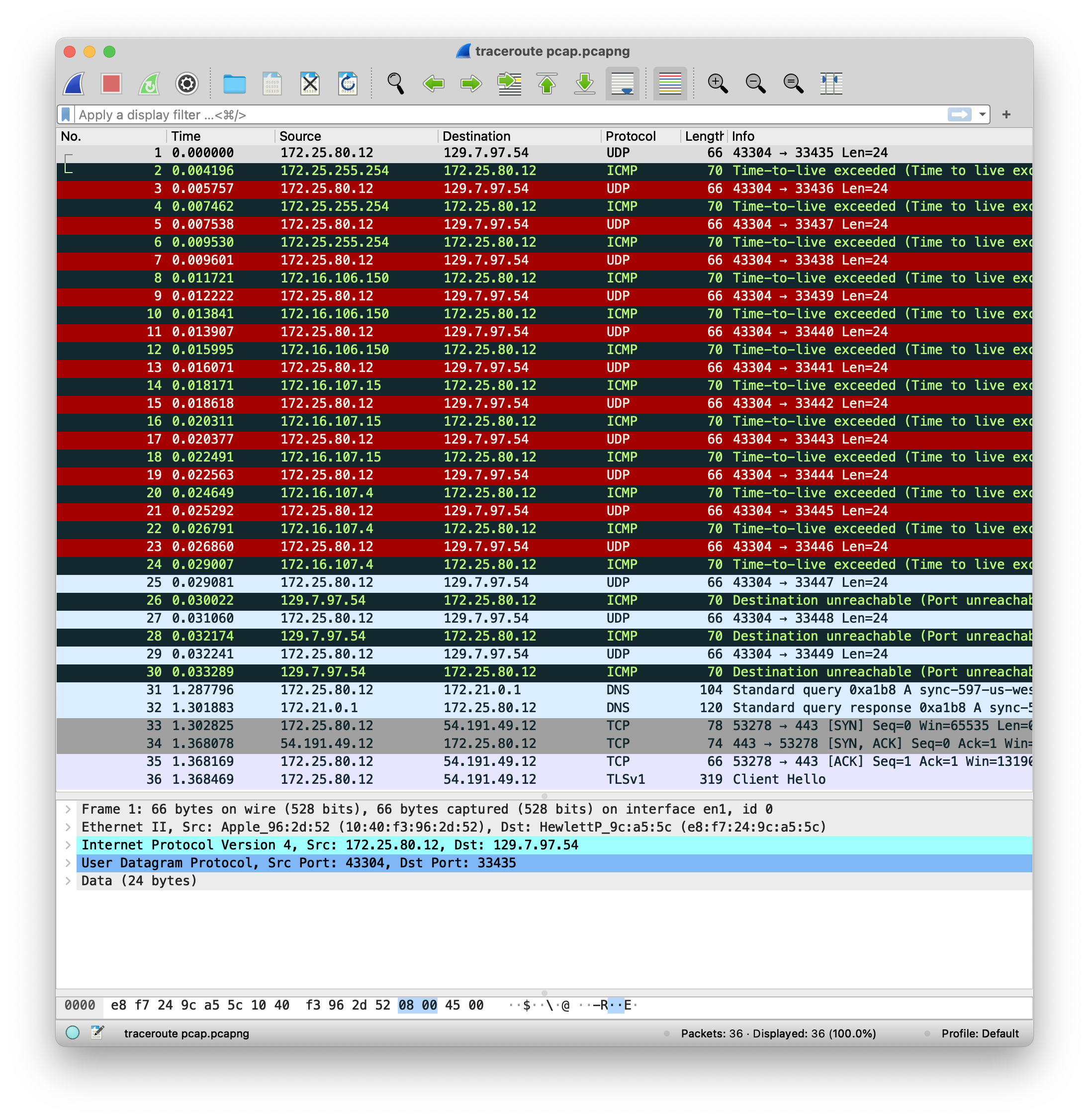


Paste in your screen snapshot.

<replace this with your screen capture>

1. Traceroute.

In the class materials folder on Teams, there’s a Wireshark folder. Open the “traceroute.pcap” file. It should look like this:



This is a \*very\* scrubbed pcap file – almost all unneeded packets are removed. If you play with traceroute yourself you’ll undoubtedly have tons of irrelevant packets littering your trace.

1. We don’t actually see “Traceroute” as the protocol being used here. That’s because it’s not a protocol. Systems accomplish their task of discovering the routers by sending packets in one of two methods: UDP probes, and ICMP queries. Examine the packets being send from our host (which by the way is on the UH campus). Which method appears to be used?  UDP Probe ICMP query
2. Where are the packets being sent? To what IP address or host name?

Our of the 30 packets being sent, how many arrive at the intended destination?

1. What’s the number of routers we discovered along the way?
2. What field are we intentionally manipulating to force the receiving routers to reject our packet and identify themselves?
3. In what layer does this field live? Answer 1-5 for Physical-1 (like the cable), Data Link-2 (Ethernet or WiFi), Network-3 (IP), Transport-4 (UDP or TCP) or Application-5 (could be anything).
4. What is the Type and Code number for the ICMP errors we’re getting back from the routers?
5. What is the type of error that the intermediate routers are showing us? Copy the text from Wireshark for one of the early response packets.
6. What’s the first packet number in this trace that makes it past all the routers and to the intended host?
7. Is the problem we cause once we reach the host the same that we caused at the intermediate routers along the way? Explain:       We ll look at your answer for a yes/no, a statement of the type of error that is, and what exactly is the reason behind the error.
8. What is the protocol and layer involved in giving us the error from the host? As before, answer with the layer name or number plus the name of the protocol Wireshark is showing us.
9. Cookies

The University of Houston’s FM radio station, 88.7 KUHF, is an affiliate of National Public Radio. A Saturday morning show I usually catch is Planet Money. Last fall, and again this weekend, they aired a story about the origin of the computer cookie. The story is located [here](https://www.npr.org/2022/11/18/1137657496/third-party-cookie-data-tracking-internet-user-privacy).

There’s also a very good (and a bit more serious) story about his invention [here](https://hiddenheroes.netguru.com/lou-montulli?utm_source=pocket_saves). There is a transcript for the radio article. You will need to read both to answer the questions. I expect your explanations, when asked, to be unique.

* 1. Who is the father of cookies?
  2. Would you guess that he lives in a home or in an apartment? Explain:
  3. Where did he attend college?
  4. Where did he work when he developed the code for cookies?
  5. What company figured out how to pervert the intended privacy of cookies to become a $1B advertising industry?
  6. Which two key elections in the West have outcomes which are attributed to targeted advertising made possible by cookies?
  7. What is the term we used in lecture to describe what web browsers are missing that cookies help to address?
  8. Into which browser was the cookie technology initially placed?
  9. Once he discovered how cookies were being successfully used for ad tracking, do the host/authors believe he could have killed them? Why?
  10. What was discovered that led him to decide against eliminating cookies?

1. **Locator markings**

Paste in the photo of the locator markings you took as discussed in lecture. There should be at least 2 different colors of markings. It can be a direct photo or one from a google satellite image, etc. It should be different than everyone else’s photo, and it must come from the town where you live. If you’re desperate, try looking for markings around IAH’s terminal C or along Cullen Blvd at UH. I think those projects have gone on long enough to have been captured in Google satellite images. It is far preferable for you to come across and take a photo of your own.

.

<< replace this line with your photo or screen capture>>

Now ID the utilities identified in the markings using the APWA color code found here: <https://www2.apwa.net/documents/About/TechSvcs/One-Call/COLORCC.PDF>

Proposed excavation

Temporrary survey markings

Electrical power lines, cables, conduit and lighting cables

Gas, oil, steam, petroleum or gaseous materials

Communication, alarm or signal lines, cables or conduit

Potable water

Reclaimed water

Sewers and drain lines

If you are going to excavate earth anywhere in Texas, including for a tree in your back yard, who does state law compel you to contact? What telephone number must you call before you dig?

1. Remember that this “packet number” is assigned by Wireshark for listing purposes only; it is NOT a packet number contained in any real packet header. [↑](#footnote-ref-1)