COSC 4377 – Networking - Kevin B Long

# interlocking-uh-m-186.eps

See Teams Assignment for Due Date

Multiple submissions accepted.

100 pts possible

1. Do the Wireshark lab on DNS, and answer the questions below.During lecture I told you that you might have to copy and paste in the document. I think instead I’ve captured all the lab’s questions below, so hopefully this is much easier.

1. Run nslookup to obtain the IP address of the web server for the Indian Institute of Technology in Bombay, India: www.iitb.ac.in. What is the IP address of www.iitb.ac.in 103.21.124.10
2. What is the IP address of the DNS server that provided the answer to your nslookup command in question 1 above? 103.21.127.129
3. Did the answer to your nslookup command in question 1 above come from an authoritative or non-authoritative server? It is an authoritative server
4. Use the nslookup command to determine the name of the authoritative name server for the iit.ac.in domain. What is that name? (If there are more than one authoritative servers, what is the name of the first authoritative server returned by nslookup)? If you had to find the IP address of that authoritative name server, how would you do so?The name of the first authoritative server is dns1.iitb.ac.in. To find the IP address of the server, I can use "nslookup dns1.iitb.ac.in".

Tracing DNS with Wireshark

1. Locate the first DNS query message resolving the name gaia.cs.umass.edu. What is the packet number[[1]](#footnote-2) in the trace for the DNS query message? Is this query message sent over UDP or TCP? The first packet number in the trace for the DNS query message is 15. The query message is sent over UDP.
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? The corresponding DNS packet number is 17. It is also sent over UDP.
3. What is the destination port for the DNS query message? What is the source port of the DNS response message? Since the destination port for the query message is the same as the source port of the response message, the port is 53.
4. To what IP address is the DNS query message sent?  75.75.75.75
5. Examine the DNS query message. How many “questions” does this DNS message contain? How many “answers” answers does it contain? 1 question, 0 answer
6. Examine the DNS response message to the initial query message. How many “questions” does this DNS message contain? How many “answers” answers does it contain?1 question, 1 answer
7. 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/>? 22   
   What is the packet number in the trace of the DNS query made to resolve gaia.cs.umass.edu so that this initial HTTP request can be sent to the gaia.cs.umass.edu IP address? 15??  
   What is the packet number in the trace of the received DNS response? 155  
   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>?205  
   What is the packet number in the DNS query made to resolve gaia.cs.umass.edu so that this second HTTP request can be sent to the gaia.cs.umass.edu IP address?        
   Discuss how DNS caching affects the answer to this last question.

Playing with nslookup

1. What is the destination port for the DNS query message? What is the source port of the DNS response message? The destination port for the query message is the same as the source port of the response message which is 53
2. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? The IP address of the DNS query is to the IP address of the local DNS server
3. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”? It is a Type A Class IN query message. The query message does not contain any "answers"
4. Examine the DNS response message to the query message. How many “questions” does this DNS response message contain? How many “answers”?1 query and 1 answer

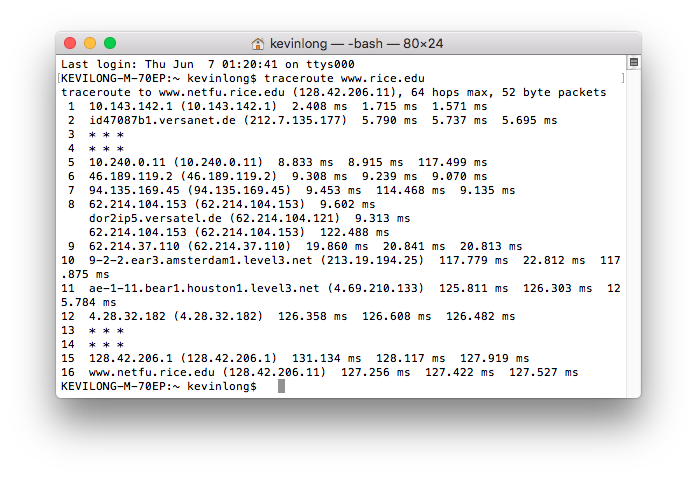
Use nslookup to issue a command that will return a type NS DNS record

1. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? The IP address of the DNS query is to the IP address of the local DNS server
2. Examine the DNS query message. How many questions does the query have? Does the query message contain any “answers”?The query message contains 1 question and 0 answer.
3. Examine the DNS response message. How many answers does the response have? What information is contained in the answers? How many additional resource records are returned? What additional information is included in these additional resource records? The response message contains 1 answer, which includes name of the host, class, data length, and Type.
4. Traceroute #1

This problem will require a bit of experimentation.

From a terminal/command window, traceroute a route to a major university web site, such as [www.rice.edu](http://www.rice.edu), [www.uh.edu](http://www.uh.edu), [www.itesm.mx](http://www.itesm.mx), [www.stanford.edu](http://www.stanford.edu), etc. from a terminal or command window on your computer. Make sure it starts with www. You may have to try different destinations and try from different places to find one that will give you a good traceroute. A good traceroute can have rows of asterisks, but needs to finish with a final row showing data and numbers.

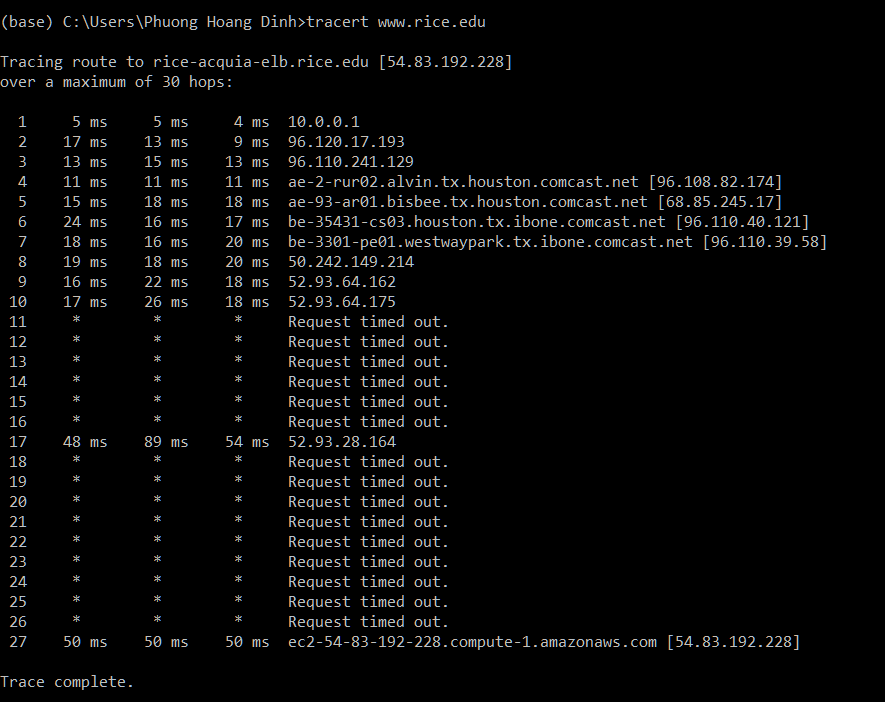
For example, here’s one I did from Germany to rice.edu back in the good old days (3 years ago):



If you can’t get a good tracereoute from home, get one from school. I got nowhere trying to get to sites from behind my AT&T fiber service at home, but had more luck at school. When your traceroute finishes, use it to answer the questions below.

1. Paste a picture of your traceroute below:

**<replace this line with a snapshot of your traceroute from your machine, or from the traceroute web site you used>**

****

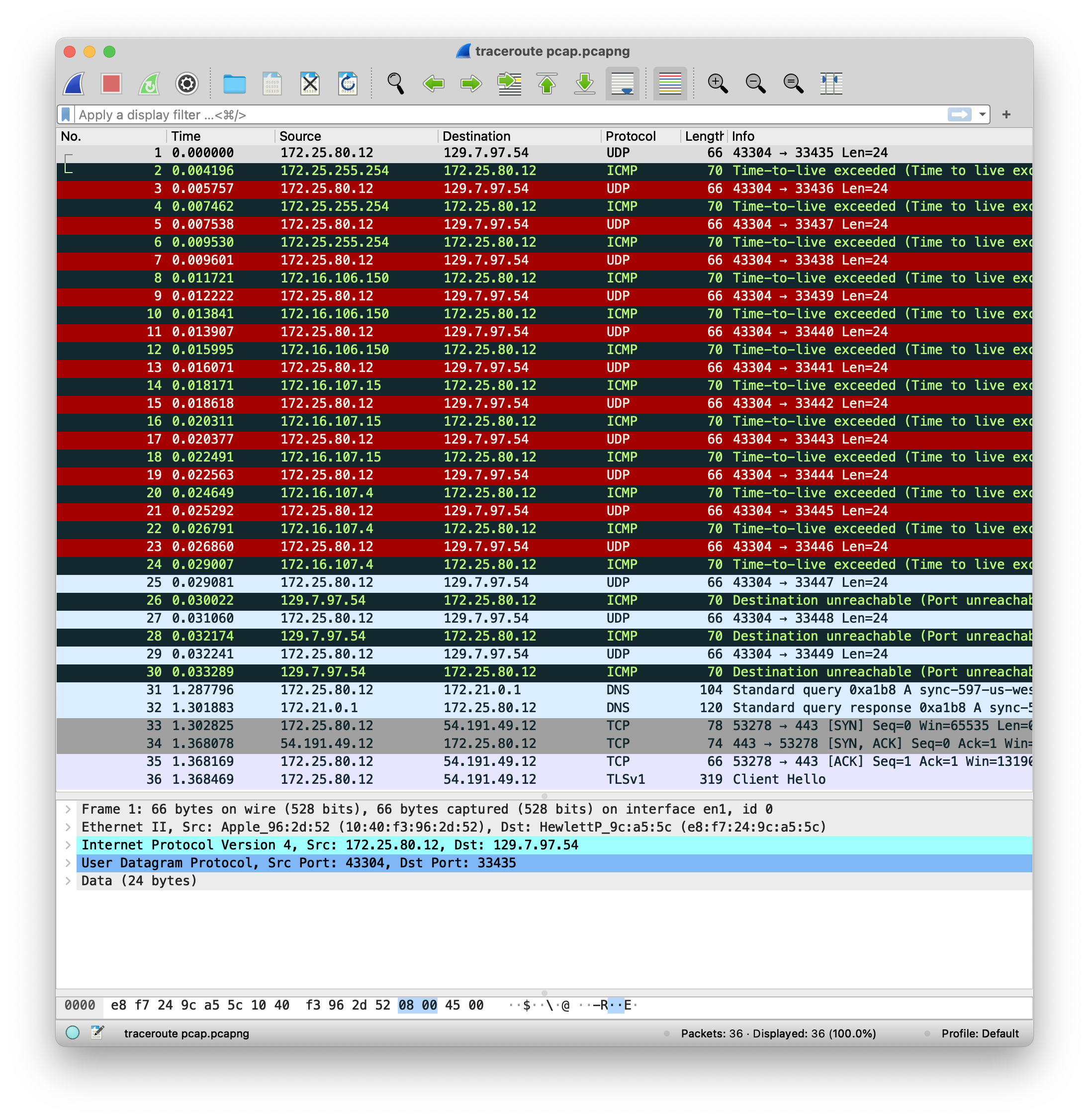
1. Start Wireshark and begin a capture. From your command window or terminal window, traceroute to the same site you used in (a). It doesn’t matter if all you get are asterisks. Let it finish/give up, and then stop the capture.
2. Which row numbers in the traceroute are not routers? All of them are routers.
3. If you are really lucky, your trace may include an example of route divergence, where a different router handles one of the three packets that make up the test of a hop. Mine are in step 8. How many different routers handled the hop #8?

3 different routers

1. How many total packets were sent from my computer as part of this traceroute example? Hint: it’s the same as the number of measurements made. There are 3 packets per hop, for 16 hops => 16\*3 = 48 packets.
2. Go to <https://tools.keycdn.com/traceroute> and trace to [www.microsoft.com](http://www.microsoft.com) from several different countries. I believe keycdn automatically uses 10 countries for you. Even though all of them are tracerouting to the same domain name, they don’t all end at the same IP address. What’s going on? There are multiple reasons why this is the case, one is the domain uses multiple servers to handle incoming traffic to prevent overloading. Another reason is that the shortest path to a destination server influences the traceroute path. Thus, a call from Germany might be directed to a load handling server that is closer to Germany than in the U.S.
3. Each numbered row has three numbers followed by “ms”. What do these represent? Choose the best answer: 2
4. The elapsed time from sending the three packets from my computer to arriving at the desired destination. When the error packet is returned, I calculate the time it took to arrive at the router and that is what is shown.
5. The elapsed time from sending the three packets to the other router plus the time to send the response back, but not the time spent processing the packet or building the reponse.
6. The elapsed time for the combined propagation delays in both directions.
7. The elapsed time from when I sent each of the three packets towards the desired destination, which a router intercepted, processed, built an error packet, queued it in a buffer back towards me, and returned it to me. That total time is what is displayed.
8. The minimum, average, and maximum response times for the three packets.
9. Several rows of my traceroute show times that are smaller than a later row. What’s happening?1
10. The earlier router included queueing time when it reports an error, but its queueing time is omitted when on the next stage the packet is simply routed on through without error. So if the later router has a smaller queueing delay, then that is what is included in the total, and thus the number is smaller.
11. The earlier router’s queueing delay is always included. The reason why an earlier router has a greater time than a later router is purely chance. The packet being measured simply encountered a longer delay as did all packets then. A few seconds later, things changed.
12. The earlier router gives a low priority to traceroute packets and thus the packet and the processing of the error message was much longer than just routing the packet. On the subsequent step when the packet did not die in that router but in a later one, the time was less since the delay was less. How do we know? The router doesn’t tell us it’s slowing down traceroutes, but we can infer it when the next router appears to be faster.
13. Pure random chance; run the traceroute again, and the situation may be reversed. If the router’s queue is always full, it will always have longer queueing delay than a subsequent router with less in its queue. You’re likely seeing a router at one step that’s always busy and therefore reports a large total time, and the one beyond it is not busy, and thus a lower time.
14. In my trace, and maybe in yours, there are rows of just asterisks. Sometimes there is a row with a combination of asterisks and times. What do the asterisks represent?2
15. The router is using encrypted packet streams
16. The router “rate limits” how often it responds to these messages or may explicitly prohibit them and dropped/ignored it.
17. That hop is not a router
18. The router’s buffer is full and it dropped your packet
19. The time exceeded the average up to that point, and traceroute reported an asterisk.
20. Second traceroute problem. Consult the first 5 or so minutes of Lecture 10 from 20 Feb 2023 for important help on this problem.

Open the traceroute pcap file in the homework using wireshark or something similar.

Here’s a snapshot of it. Hopefully this is all you must have, but you will for sure find additional helpful hints in the pcap file that might make it easier to understand what’s going on.



1. Over how many IP subnets or LANs does Wireshark show you passed through to reach the destination? Include the destination in your count because it represents the only device on the last network you’ll see.
2. Open one of the ICMP packets early in the trace. What does ICMP stand for? You can find it in the middle detail section of the Wireshark window.

ICMP: Internet Control Message Protocol

1. What is the type number and what is the code number of this ICMP message, and what do they mean? A small snapshot is fine, or you can type it out.

There are two ICMP mentioned in the previous snapshot. The first is Type 13 Code number 0 => Time-to-live exceeded. The send message is Type 3 Code 3 => Destination unreachable

1. What about the type and number of the very last packet sent as part of this traceroute to your intended destination?

The last message is Type 3 Code 3 => Destination unreachable

1. What is the IP address of the host the traceroute is really trying to reach?

54.191.49.12

1. Go to <https://mxtoolbox.com/NetworkTools.aspx>. Search for the “ping” field, and type in that destination IP address. To what organization is this IP address assigned? The tool shows you in the IP Address column below the address.

The IP address is assigned to University of Houston.

1. **Cookies**

Choose your favorite browser. Pick a retail store you have not visited before and are OK if you never do (we’re going to mess things up a little). Don’t open its web page yet.

Find and open the cookie manager for your browser. You may have to search the help pages.

In Chrome, I used: <https://support.google.com/chrome/answer/95647?hl=en-419>

In Firefox, I navigated to this site by entering it in the URL field:

about:preferences#privacy

1. So what’s the site you chose? https://www.nordstromrack.com/

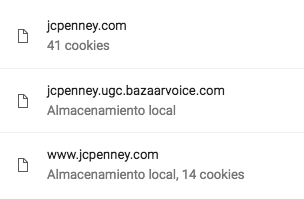
I chose [www.jcpenney.com](http://www.jcpenney.com).

Find and clear any cookies that have the name of the site. Leave the cookie manager open.

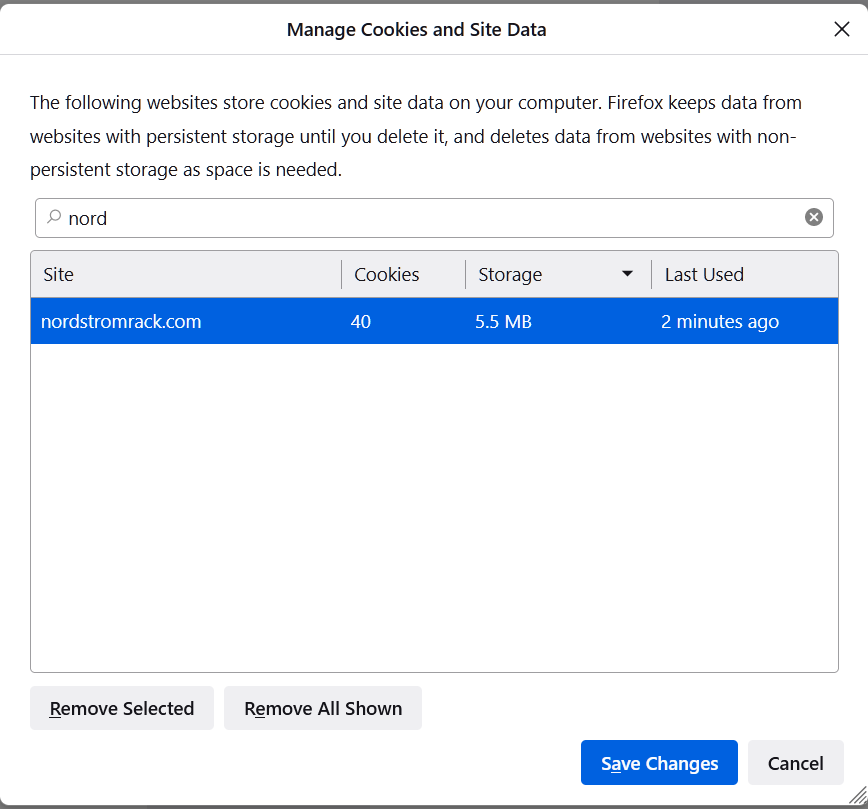
1. Go to the site’s home page. Consult the cookie manager again in your browser and search again for cookies for this site.

Were cookies created by just opening their home page? Yes  
How many? 40

Include a snapshot of what the cookie manager shows. For example, here’s what Chrome showed me:



<< replace this with your snapshot>>



1. Click on a product on the web page. Observe the URL in your browser after you have clicked on the product. Paste it here. Here’s the one I got for jcpenney.com:

<https://www.jcpenney.com/p/arizona-long-sleeve-thermal-top/ppr5007324806?pTmplType=regular&rrec=true&rrplacementtype=norecs>

Your URL: https://www.nordstromrack.com/s/gucci-mens-rubber-strap-wrist-watch-46mm/6163468?origin=category-personalizedsort&breadcrumb=Home%2FEvents%2FDesigner%20Watches%20for%20All%20Feat.%20Versace%20%26%20Fendi&eventId=1014459&color=000

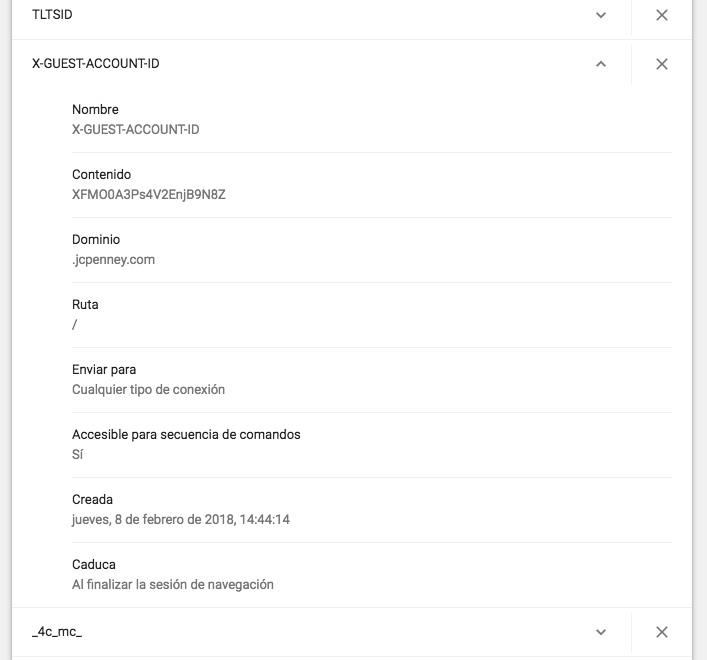
Do you see a pattern of variables and values encoded in the URL? For example, separated by ampersand symbols (&’s)? If you do, type one out here:

color =000

If you’re not sure what that looks like, remember the Amazon URLs we explored in lecture. They use that a lot, and you can see it if you navigate around even a little.

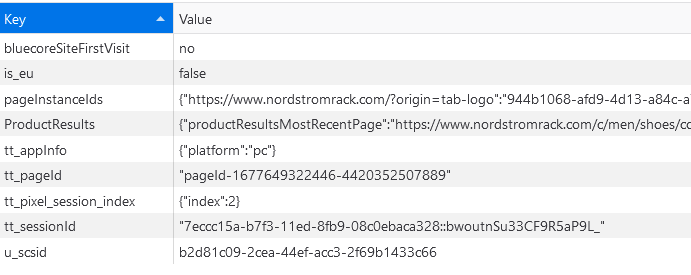
1. Examine one of the cookies. If navigating did not produce a cookie, check your settings (to make sure they’re not restricted), try another browser, or another site. Choose a cookie that looks like it has something that identifies you – you can get a good hint by looking at the name of the cookie – good candidates include a session ID, or a guest ID. Inspect the cookie with your browser (most provide a cookie inspector tool), and paste a snapshot of the details your browser provides. .

Here was the one I chose:



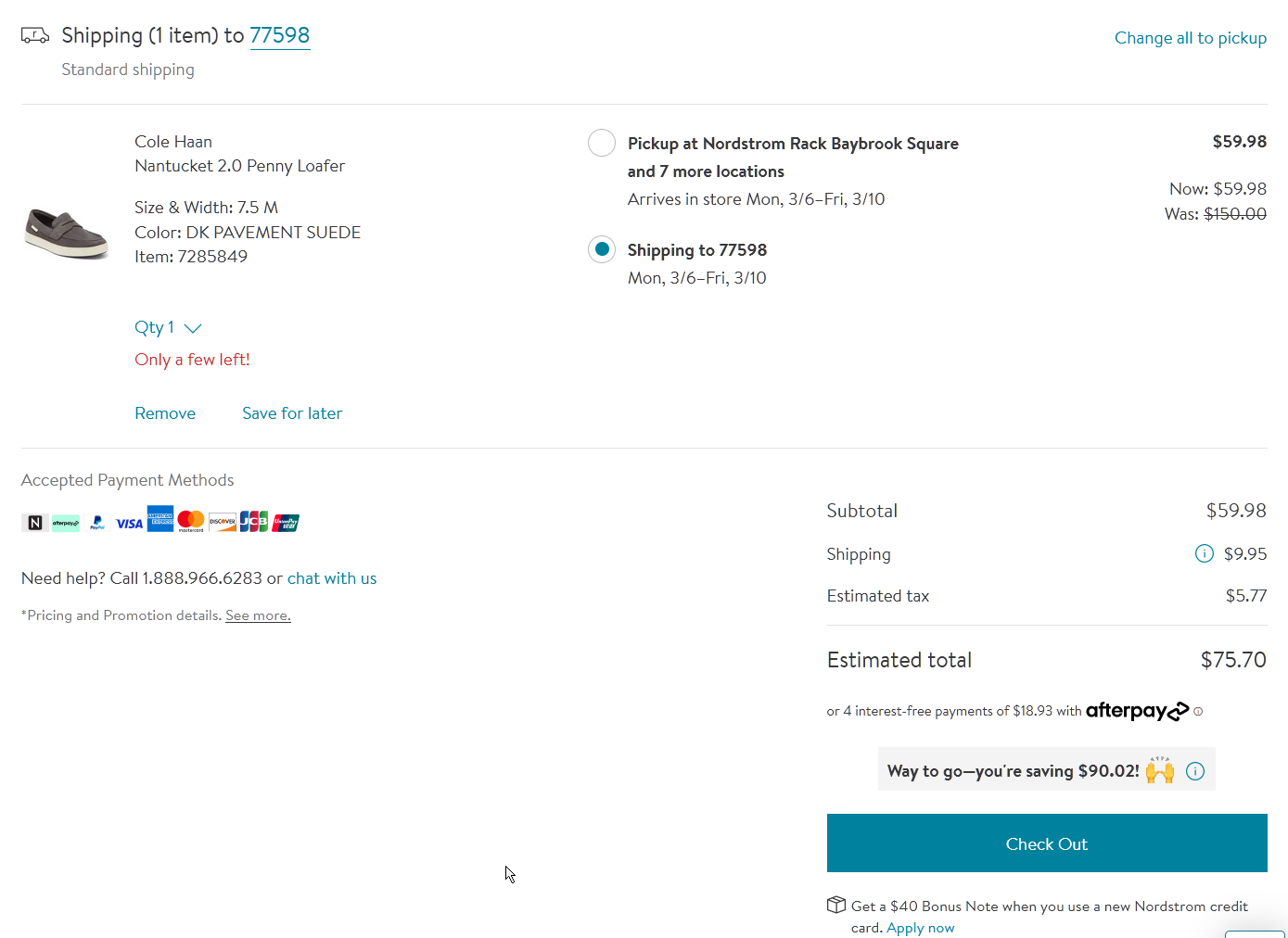
Although most of the fields were readable and had a variable-value combination, the guest account ID looks encrypted or at the least very random: XFM00A3Ps4V2EnjB9N8Z.

<<Include a snapshot of your cookie here>>



1. Add the product you were browsing above to your cart. Include a snapshot of the cart so we know what you added here:

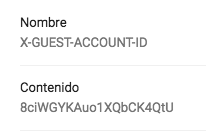
<<include cart snapshot here>>



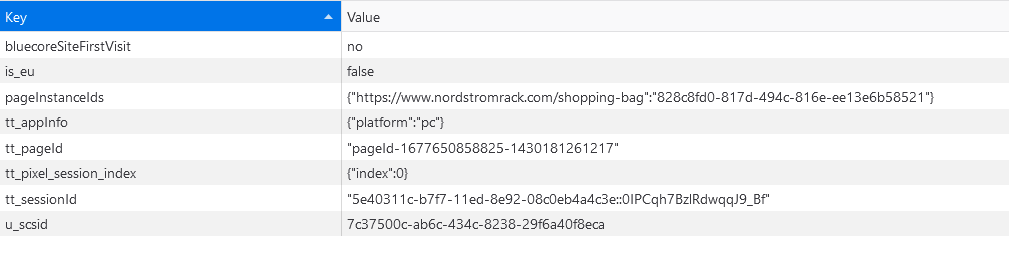
While that cart page is still open, clear the cache again for the domain (you might have to do that from a different window). Now refresh the page. Is the item still in the cart?

No, the item got removed.

1. Examine the cookies again. Look for the same cookie from (d). Was it replaced? Does it still have the same unique identifier as before? Mine changed:

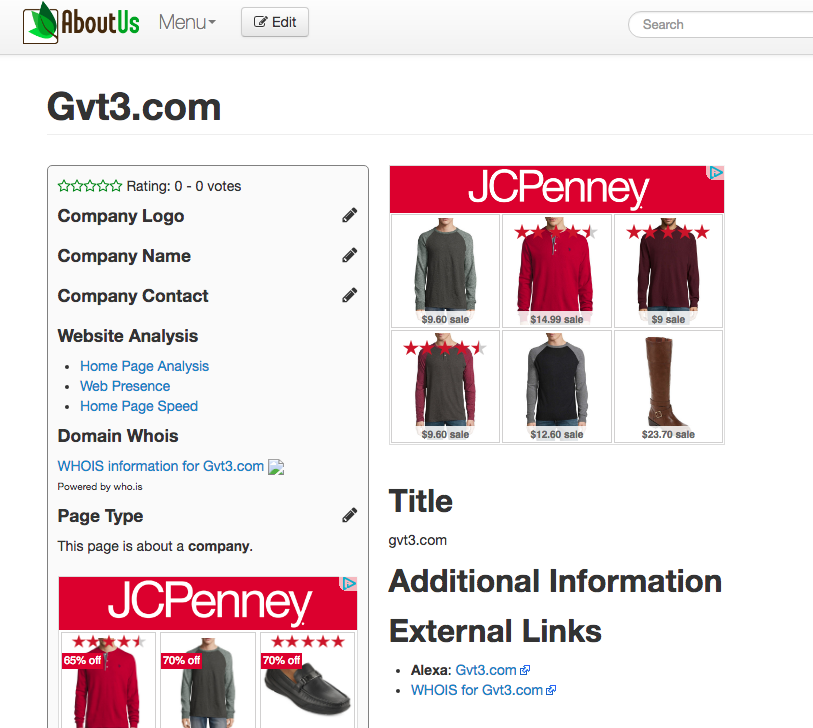


<<Include a snapshot of the cookie here.>>



The cookie got replaced, it now have a different unique identifier.

1. Wait a few minutes and go to a site with google ads, like nytimes.com. Did you see your cart item in one of the ads? I happened to need to go to aboutus.com/Gvt3.com (sort of random site) and look what ads I got! Lol. My browser might not remember what I put in my cart, but Google did!



<<Include a snapshot of a web page with ads that you visited to see if your cart item showed up>>

1. This is all about maintaining state. In summary, check/highlight/include which your chosen site uses to maintain state:

cookies

URL variables

Some use both, some use neither!

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.

<< 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 a contractor considering digging a trench for a new irrigation line, who do you call before you dig? I need to call 811. Specifically in Texas, it is Texas811.

The remainder of this homework is given as a quiz so that it may be graded immediately. Check for a companion assignment for homework #1.

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-2)