COSC 4377 – Networking - Kevin B Long

# interlocking-uh-m-186.eps

Homework #2

Due 11:59am, Monday, 10 June 2019

Multiple submissions accepted.

**Name: De Vo**

**Peoplesoft ID: 1080326**

1. (15 pts) Socket Programming

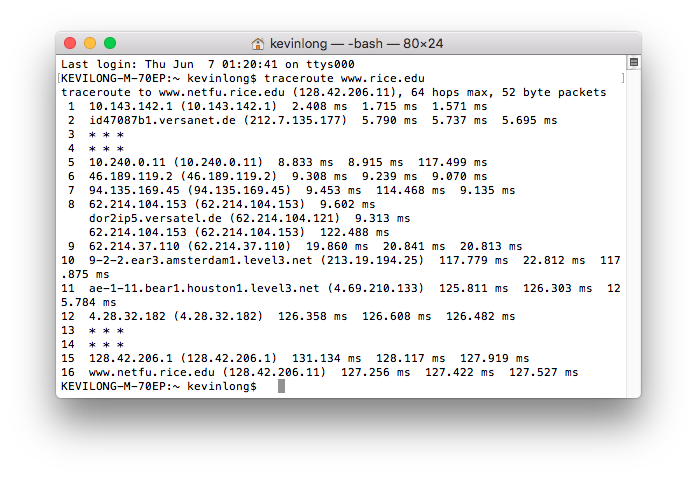
Please see server.py file submission

1. (10 pts) Complete the third Wireshark lab on SSL. SSL is more or less defunct, replaced by TLS. So you will probably need the pcap file to complete this lab.
2. (30 pts, 15x3) Traceroute

This problem will require a bit of experimentation.

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. 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. That means a traceroute that may have some rows of asterisks, but the last row must not.

For example, here’s one I did from Germany to rice.edu:



1. Paste your traceroute below:

**<paste your traceroute here>**

1. How many steps did your traceroute require? \_\_\_\_\_\_\_\_\_\_\_
2. What type of device is responding (or not) in each row? \_\_\_\_\_\_\_\_\_\_\_\_\_
3. Each numbered row has three numbers followed by “ms”. What exactly are these?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Why are there 3? Why do they differ in some rows?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Were there rows of just asterisks? If so, what does that represent? \_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Why do you think you can have asterisks and yet still reach your destination?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Were there some rows whose times were greater than the times of later rows? How can this be? For an example, see the last two rows of the last rice traceroute. Note how in row 15 it’s reported to require 131.134 to reach that row in one instance, and 127.256 to reach the destination which is one step further away.



\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. What is the average time to reach your destination and how did you calculate that value?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Quickly (not later in the day) traceroute from the same place to just [the](http://itesm.mx/) domain name (remove www).

1. Ignoring any change in the values at the end of each row, are the traceroutes the same?

\_\_\_\_\_\_\_\_(Yes or No). Why do you think this is the case?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Second traceroute.

Repeat the first traceroute above from a different network. The more diverse (further away) the starting location the better. You can try this second traceroute from school, a restaurant, home, etc. You can also try finding a remote web-based traceroute server at <http://traceroute.org>. You can also get a friend to traceroute for you and send the results back as long as you are directing the work and not taking someone else’s results. Sometimes just tracerouting from work or home is very different but for greater diversity try finding a place in a very different location geographically. Include your traceroute snapshot (or copy and paste the text). Here are two rice.edu examples. You should include only one:

From lg.uar.net (on the list for Turkey at traceroute.org):

1 87.245.237.81 [AS 9002] 1.041 ms 4.573 ms 5.273 ms

2 87.245.232.245 [AS 9002] 34.721 ms 87.245.232.234 [AS 9002] 33.660 ms 33.433 ms

3 213.198.77.213 [AS 2914] 32.840 ms 33.532 ms 33.127 ms

4 129.250.7.54 [AS 2914] 33.853 ms 34.063 ms 37.482 ms

MPLS Label=337632 CoS=0 TTL=1 S=1

5 129.250.4.96 [AS 2914] 118.526 ms 117.813 ms 131.261 ms

MPLS Label=405328 CoS=0 TTL=1 S=0

MPLS Label=299984 CoS=0 TTL=1 S=1

6 129.250.5.12 [AS 2914] 165.128 ms 167.765 ms 161.715 ms

MPLS Label=318688 CoS=0 TTL=1 S=0

MPLS Label=299984 CoS=0 TTL=2 S=1

7 129.250.5.21 [AS 2914] 163.418 ms 160.814 ms 158.023 ms

MPLS Label=299984 CoS=0 TTL=1 S=1

8 129.250.5.226 [AS 2914] 165.888 ms 165.728 ms 166.336 ms

9 128.241.2.166 [AS 2914] 154.248 ms 159.282 ms 155.208 ms

10 \* \* \*

11 \* \* \*

12 128.42.206.1 [AS 8] 161.622 ms 159.292 ms 154.703 ms

13 128.42.206.11 [AS 8] 154.973 ms 155.224 ms 160.062 ms

From rwth-aachen.de:

Last login: Thu Jun 7 10:10:25 on console

KEVILONG-M-70EP:~ kevinlong$ traceroute www.rice.edu

traceroute to www.netfu.rice.edu (128.42.206.11), 64 hops max, 52 byte packets

1 mops-gw-vl700.mops.rwth-aachen.de (134.61.32.1) 1.793 ms 1.262 ms 1.314 ms

2 c4k-ww10-1-vl122.noc.rwth-aachen.de (137.226.39.241) 1.953 ms 2.059 ms 2.342 ms

3 n7k-ww10-1-et8-27.noc.rwth-aachen.de (137.226.34.1) 1.702 ms 1.656 ms 1.815 ms

4 fw-xwin-2-vl158.noc.rwth-aachen.de (134.130.3.253) 1.516 ms 1.442 ms 1.571 ms

5 n7k-ww10-1-xwin-vl106.noc.rwth-aachen.de (134.130.3.227) 2.198 ms 2.232 ms 2.070 ms

6 n7k-lssnord-1-xwin-po101-1.noc.rwth-aachen.de (134.130.9.130) 2.179 ms 2.359 ms 2.493 ms

7 cr-fra2-be8-3006.x-win.dfn.de (188.1.242.109) 5.652 ms 6.249 ms 6.134 ms

8 dfn.mx1.fra.de.geant.net (62.40.124.217) 5.420 ms 5.914 ms 5.922 ms

9 ae1.mx1.ams.nl.geant.net (62.40.98.129) 13.714 ms 12.542 ms 12.499 ms

10 ae2.mx1.lon.uk.geant.net (62.40.98.80) 20.499 ms 19.546 ms 19.539 ms

11 internet2-gw.mx1.lon.uk.geant.net (62.40.124.45) 94.337 ms 94.502 ms 94.639 ms

12 ae-1.4079.rtsw.atla.net.internet2.edu (198.71.45.6) 107.374 ms 107.407 ms 107.212 ms

13 et-7-0-0.4079.rtsw.jcsn.net.internet2.edu (162.252.70.47) 122.165 ms 121.556 ms 121.968 ms

14 et-8-3-0.4079.rtsw.houh.net.internet2.edu (162.252.70.44) 130.927 ms 129.812 ms 130.637 ms

15 74.200.187.54 (74.200.187.54) 129.998 ms 130.186 ms 129.916 ms

16 74.200.187.46 (74.200.187.46) 130.230 ms 130.297 ms 130.148 ms

17 rice-i2-1.setg.net (198.32.229.138) 130.359 ms 130.937 ms 130.155 ms

18 \* \* \*

19 \* \* \*

20 128.42.206.1 (128.42.206.1) 310.143 ms 244.981 ms 164.185 ms

21 www.netfu.rice.edu (128.42.206.11) 164.014 ms 164.127 ms 165.028 ms

KEVILONG-M-70EP:~ kevinlong$

1. Paste your screen dump below:

**<paste your traceroute here>**

1. How many steps did your traceroute require? \_\_\_\_\_\_\_\_\_\_\_
2. Examine the routes in the two traceroutes. Do they ever converge? To converge means to share the path from that point on to the destination. Don’t assume they do – they may not even converge at the end. What is the row number in each traceroute where they converge?

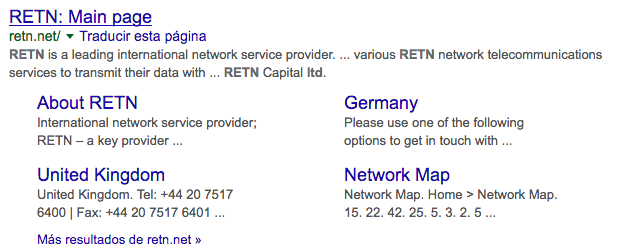
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Looking up IP addresses

In one of my traceroutes, the one from uar.net (shown above), all I got were IP addresses and ASN numbers – no names. I went to a site to help determine to whom the addresses were assigned, <https://mxtoolbox.com/NetworkTools.aspx>. In the ping tool, I entered the IP address from my first row of my traceroute, 87.245.237.81, and saw it was assigned to the organization RETN Limited. Ping doesn’t include this, but the site looks it up as part of ping.



I googled the name I highlighted above:



That’s an ISP. So in my case, the very first hop in my traceroute was from an ISP, which makes sense, because I was in a hotel with no internal network of its own).

1. Use the tools and methods shown above to determine the first ISP in sequence handling your traceroute to your destination. Provide the domain name or the name of the organization to whom the IP is assigned, not the IP address. Your own internal organization is not an ISP.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Who is the ISP at the end of the path for each traceroute (or from the last line with information in it)?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and (if different) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **(10 pts, 2x5) Layers**

When you pass a packet through a router (letting it do its normal job), at which of the five TCP/IP layers is the software running that makes the routing/forwarding decisions? Give the number and name. Names are Physical, Data Link, Network, Transport and Application.

#:\_\_\_\_\_ Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. So when you run a traceroute, and you are receiving responses from the device on row 5, is the software you mentioned in (a) what is running in hops 2, 3, and 4?

Y/N:\_\_\_\_\_\_ Explain: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Suppose the device in row 5 had a small web server used to configure the router remotely, protected of course with a password. At what layer is the software running in that device that interacts with our browser? Remember, if you don’t know what layer it’s at, we discussed what answer you should assume is correct.

#:\_\_\_\_\_ Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Defend this answer: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. (24 pts, 8x3) Cookies

Choose your favorite browser. Pick a commercial site (a company that sells products that’s large enough to have a cool web site) that you don’t visit and don’t care if you have to log in again (we’re going to mess things up a little).

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

In google, here’s what 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:

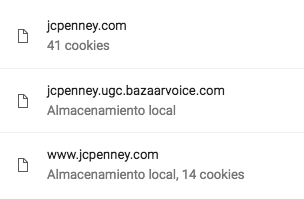
about:preferences#privacy

1. So what’s the site you’re chose? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

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

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



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:

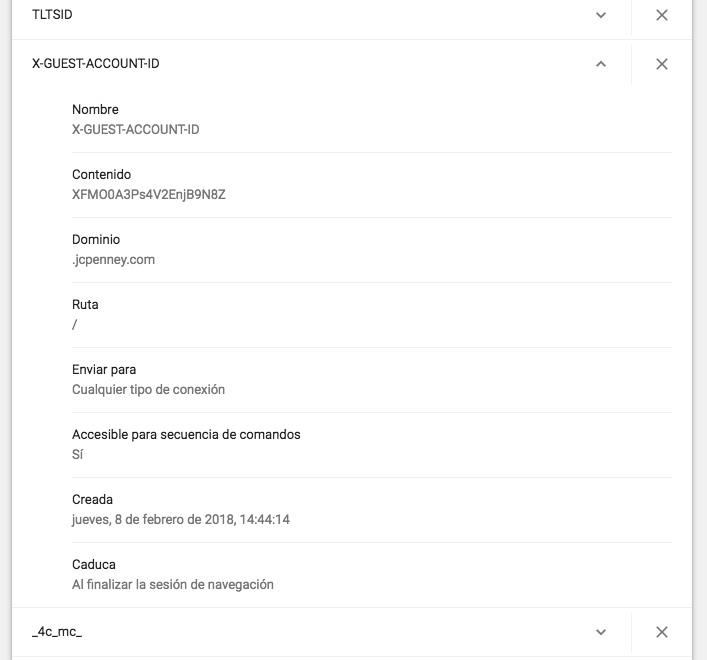
<https://www.jcpenney.com/p/arizona-long-sleeve-thermal-top/ppr5007324806?pTmplType=regular&rrec=true&rrplacementtype=norecs>

Your URL:

Do you see a pattern of variables and values encoded in the URL? For example, separated by ampersand symbols (&’s)?

1. Examine one of the cookies. If navigating did not produce a cookie, check your settings, 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. .

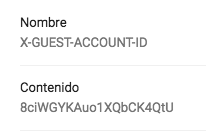
Here was the one I chose:



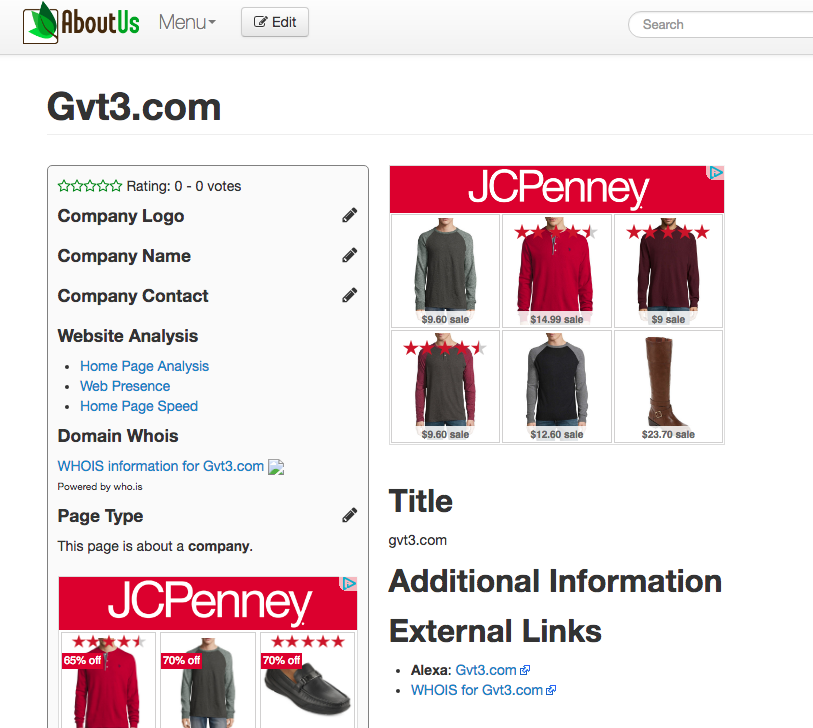
Although most of the fields were readable and had a variable-value combination, the guest account ID looks encrypted or at the least very random: XFM00A3Ps4V2EnjB9N8Z.

What about the value of the cookie you chose to inspect?

1. Add the product you were browsing above to your cart, and then clear the cache again for the domain while that web page is still displayed and the item is still in your cart. Now refresh the page. Is the item still in the cart? \_\_\_\_\_\_
2. 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:



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!



1. Does the site you chose use custom URLs or cookies or both or neither to maintain state?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_