Protocol Analysis: Capturing Packets

This project is intended to be done on your assigned Windows VM on the EiLab Network. This is, in part, because you must do this on a PC that you have administrative rights on because it requires the installation of software. Also it is easier for me to grade it.

Submitting the Assignment for Grading:

All you have to do to submit the assignment is first, complete it, then log into Blackboard and look for the Wireshark assignment and submit that you have completed it. Do not attach anything. Just write a text that says that you completed the assignment, what your student number is, and the name of your computer, i.e. Fall2017-23. If you have trouble with that, then email me these details.

Getting Started

Connect to your assigned VM remotely using Chrome Remote Desktop or some other remote software that you installed on your VM. Otherwise you will need to do the assignment from one of the Thin Client PC's in the EiLab using the Citrix Xen Desktop.

Create a Folder on your Desktop called "**WIRESHARK-Lab"**. You will put all your documents, screen prints, and packet captures in that folder.

Create an RTF (using wordpad) file called **"WIRESHARK-Lab.rtf"** in that folder for taking notes and answering questions. Put your name and student ID at the top and the dates you started and completed the assignment. Copy and paste the questions from below along with your answers there (questions are in red…see below). Also, as you perform each step, i.e. installing Wireshark, installing the FTP program, etc… make a note in this RTF file that you did that and the date you did it. Example:

Jake Messinger

Student ID: 1235456

Started: 11/25/17 @ 9 am

Finished: 11/29/17 at 11:30 am

==========

History

11/15/17

Installed Wireshark

11/17/17

Installed WinSCP

Got familiar with Wireshark Layout.

Filtered out PORT 80 packets... saved PCAP

Lookin for static websites that allow caching:

goodnight.com

etc...

etc...

==========

End of Notes: WIREHSARK-Lab

Objectives

This will introduce you to "packet sniffing," a method by which we can capture packets being sent between computers as they communicate. As a network administrator you can use this method to help evaluate the performance of your network by identifying bottlenecks and slower performing servers or sections of your network. You can also use it to check the security of your network. As a graphic demonstration of this, you will use an FTP client and log into a test FTP server and observe the login packet interchange. You will see that each communication may consist of several packets that are exchanged between the two computers and you will see the potential for security leaks and how to gauge potential abuse of the network by users.

Overview& Prerequisites

You will first install a program called Wireshark on your VM. You should have already installed this by now. This is an open source application freely available on the Internet that allows you to capture packets as they appear at the network adaptor card. This means that you will be able to see all header information on the packet from each of the OSI layers. (Normally these headers are stripped off so that the only portion remaining is the data payload.) You will use the software to view complete packets and locate each layer's header, from the physical layer to the application layer. Doing so will help you to better understand network traffic and identify things that are "out of order." Using this program you will:

1) Analyze simple protocols and learn about the software interface and the information it contains;
2) Observe, analyze and reconstruct specific packet interchanges between a computer and a server; and
3) Monitor the login process to an FTP server. This will include searching for the login information in the Wireshark output.

Procedure

To obtain the software that you will use for this lab, go to www.wireshark.org and download the 64 bit latest version to your VM. Once downloaded, you can install the software. The program includes a program called WinPCap which you must install and tell your VM to load at boot up, which will install after Wireshark is installed. When installing, take all the defaults, except you should tell it to create a Desktop Icon for you. You MUST install the WinPcap

module but you do NOT need to install the USBPcap module. Leave it unchecked. Don't forget to make note of this installation in your RTF file for this assignment.

Part 1: Analyzing simple protocols

After you have installed Wireshark, start the Wireshark program. Make sure you don't have anything else open including any browsers. Depending on the version you have and whether or not you have multiple network connections, \the initial screen will resemble figure 1.

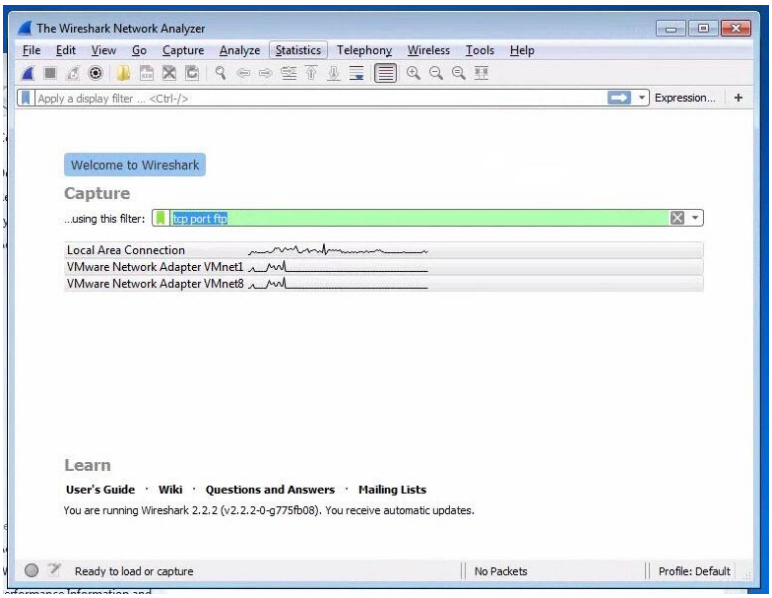

Figure 1: Wireshark Initial Screen

Double click on ***Local Area Connection*** to choose it. You will see a new Screen and an initial packet capture is automatically started. See Figure 2. The capture window is divided into three distinct areas. The top is a listing of all packets received—the packet list pane; the middle provides the details of a packet selected in the packet list pane and is called the packet details pane; and the bottom, called the packet bytes pane, shows the hexadecimal details of the selected packet and will highlight its (selected) fields. You can resize the 3 frames by moving your mouse to the separation line between each frame, clicking and moving it up or down. Figure 2 illustrates this and shows some captured packets.

You can see in figure 2 that some packets are already getting captured. One is selected in the packet list pane. In the packet details pane, you can see the detail of that packet and what type it is. The packet byte pane shows the hexadecimaland ASCII equivalent of each packet at the bottom of the window. Selecting a field in the packet details pane will highlight the hex and ASCII portions of the packet in the packet byte pane.

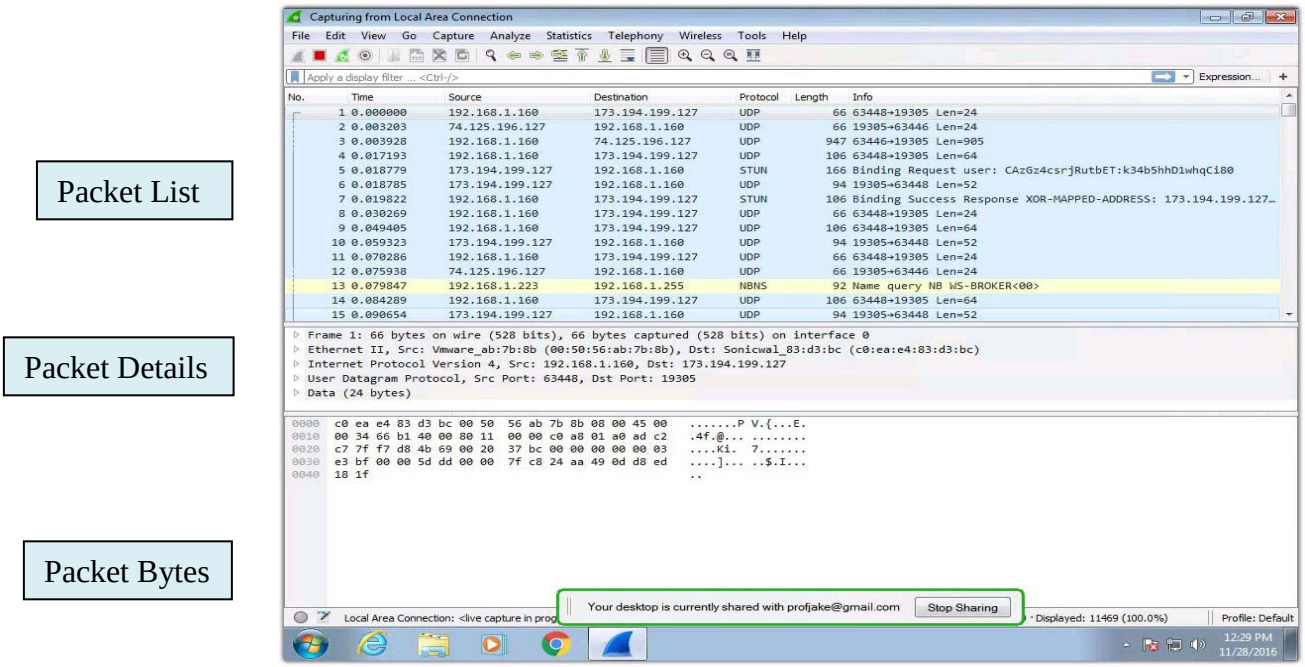

Figure 2: Wireshark

Go ahead and stop the initial packet capture session after receiving a few packets by clicking the red STOP button. The "Blue Fin" is the Start button. If it is greyed out, that means a capture is already in progress. To stop the capture, click the "Red Square." You will probably have already captured hundreds of packets in just a few seconds. Even when you aren't doing anything, your operating system is constantly sending and receiving TCP and UDP packets, especially since you are remote viewing your VM. Don't run captures for too long or your "PCAP" files will get really big. You have the option of filtering just certain types of traffic and saving only what you want to see.

Find a TCP packet in the packet list pane and select it. You can click on the filter line and enter "tcp" to find one quickly. Choose one that has a source IP not on your local network, i.e. not from a 192.168… address. If there aren't any, start a new capture, go open a web browser with your capture running and go to a website. Then come back and stop the capture. In the packet details pane, you should now see all the details of that segment of data. Click on the little right facing triangle next to the word "Frame" to expand the selection. When this part of the packet opens, you will see some summary information that Wireshark logs about every packet that it captures. Now open each subsequent section of the packet beginning with "Ethernet II." You should be able to find the portions of each frame or packet as shown in figures 3a through 3c within the packet details section.

Preamble	Start of Frame	Destination Address	Source Address	Type	Date	FCS	Flag
7 bytes	1 byte	6 bytes	6 bytes	2 bytes	46 - 1500 bytes	4 bytes	8 bytes

Figure 3a: An Ethernet II Frame Layout

Version Number	Header Length	Service Field	Total Length	ID	Flags	Fragment Offset	Time to Live	Next Protocol	Header Checksum	Source IP Address	Destination IP Address	Data
4 bits	4 bits	8 bits	16 bits	16 bits	3 bits	13 bits	8 bits	8 bits	16 bits	32 bits	32 bits	Variable

Figure 3b: The IP Header Layout

Source Port	Destination Port	Sequence Number	ACK Number	Header Length	Flags	Window Size	Header Checksum	Urgent Pointer	Options (Optional)	Data
16 bits	16 bits	32 bits	32 bits	4 bits	8 bits	16 bits	16 bits	16 bits	32 bits	Variable

Figure 3c: The TCP Header Layout

Figure 3a includes 20 bytes that are processed in the hardware and will not be seen in the packet details pane. These are the preamble (7 bytes), the Start of Frame (1 byte), the Frame Check Sequence (FCS, 4 bytes), and the final Flag (8 bytes). This is very helpful in understanding how a frame relates to a packet and segment. You can see where the Frame came from, which should be the router immediately before your PC. Notate in your RTF notes file that you have gotten this far and have a basic understanding of the layout of Wireshark.

Part 2: Finding specific packet sequences

Step 1 Observing a TCP connection

1) Ensure that your capture options are set as before and begin another capture session. Choose to "continue without Saving" to get a new packet capture session.
2) Open a web browser on your workstation and go to a website you think you have never been to before. Allow the web page to finish loading, and then stop the packet capture session.
3) Filter out everything but the web traffic by entering this into the Filter line and clicking the blue Apply button over to the right of the filter line: tcp.port eq 80 or tcp.port==80. Notice that if you don't type the filter in right, it shows in red. You can google for "common wireshark filters" for some good examples. You could also filter for just "http", but that will only show you the contents of the web page and not the set up. Also if you ONLY wanted to see the traffic FROM the server, you could filter for tcp.srcport==80
4) Look at the first three TCP packets in the packet list pane. TCP packets have a green background color (depending on your settings) and are easily recognized.

These three packets should be listed as [SYN], [SYN, ACK] and [ACK]. This 3-packet interchange builds a connection between two computers. You should notice that the destination port for the [SYN] packet is 80, indicating a web request. The second two packets should provide you with a sequence/acknowledgement analysis. Then you will start to see HTTP packets which represent the different files of the web page.

From the Transmission Control Protocol WIKI page:
https://en.wikipedia.org/wiki/Transmission_Control_Protocol

1. **SYN**: The active open is performed by the client sending a SYN to the server. The client sets the segment's sequence number to a random value A.

2. **SYN-ACK**: In response, the server replies with a SYN-ACK. The acknowledgment number is set to one more than the received sequence number i.e. A+1, and the sequence number that the server chooses for the packet is another random number, B.
3. **ACK**: Finally, the client sends an ACK back to the server. The sequence number is set to the received acknowledgement value i.e. A+1, and the acknowledgement number is set to one more than the received sequence number i.e. B+1.

Step 2 Observing a DNS request/response

1) Ensure that your capture options are set as before and begin another capture session. ***Save the previous packet capture to a file called "TCP-CONNECTION" in your WIRESHARK-Lab folder***.
2) Apply a filter to just look at DNS. Type "dns" in the filter box and click the blue apply arrow.
3) In a web browser, go to a random website you have never been to, such as monkees.com or goodlight.com, then go back to Wireshark.
4) Observe the first few DNS entries and note how a "Standard query" is made to your DNS server IP (192.168.1.31 is the primary DNS server on the EiLab Network) for an "A" (address) record of the domain you entered. If a name is found, the next DNS line should contain a response. You can click in the middle pane on the triangle next to "Domain Name Systems (response)" and further look at the detail under "Querries" and then "Answers." You should see an IP address.
5) Note that if you have already been to this website recently, then browser already knows what the IP address is (cached), Wireshark should not show you any additional output. Pay attention to the last packet sequence number. Go back to your browser and hit F5 to refresh. You should see no NEW info as your browser has now learned the IP address of the website you looked up.
6) Go to another random website and observe the behavior again.
7) In some cases, it will retrieve it again anyway, because some websites tell your browser NOT to cache data. Try visiting a website with constantly changing content, such as cnn.com. These days, this is most sites. You should see some significant DNS queries in your Wireshark output every time you reload the web page because it is changing content all the time. If you see none, or just a couple, then this site allows caching OR does not have much dynamic (changing) content. Please ignore references to "googleads," or "doubleclick." These are generated by your Chrome Browser in the background. It makes it harder to find sites that allow caching, but it should be fairly obvious when you go to a site that suppresses caching because you will get just as many responses as you got the first time you went to the site. So again, pay attention to the DNS packet #s and see how many more you are getting that actually pertain to the site you are visiting and not microsft.com or google.com.
8) Notate in your RTF file that you have done the above steps and understand how to see a DNS packet exchange.

ASSIGNMENT DELIVERABLE # 1: Find at least 3 websites that allow caching (this is most static and small company websites with static data, not news sites) and find at least 3 websites that tell your browser NOT to cache and list them. You can tell the "non-cachers" because every time you reload the webpage, you

get just as many packets as the first time. The capture should be saved to a "pcap file…see below. List the 6 sites in you Wordpad rtf file. It may be helpful to complete the following step and look for the "no cache" directive in the actual HTML code in order to determine sites that do not allow caching.

Step 3: Following an HTTP stream

Let's have a closer look at a request/response interchange that requests a web site. Follow these steps to obtain a fresh set of packets:

1) Ensure that your capture options are set as before and begin another capture session. Save the previous one to your Wireshark-Lab folder and call it "DNS".
2) Open Internet Explorer on your workstation, then return to Wireshark and begin a new packet capture session.
3) Type in a URL and after the page loads, return to Wireshark and stop the packet capture.
4) In the filter box, type "http" and click apply, to filter out extra traffic.
5) Find the packet with comments in the "Info" column "GET / HTTP/1.1" and select it. It MIGHT be the first one, But many times, you are redirected to a www.websitename.com and you will see an "HTTP/101. 301 Moved…" packet followed by the NEW site packet and another "GET / HTTP/1.1" entry. Right click this packet and click "Follow" then choose "TCP stream" from the popup menu.
6) A new window will open with the details of the http interchange. The request and acknowledgements from your workstation are in red, and the responses are in blue and should resemble figure 5. This should be a combination of the TCP get commands to get the page along with the HTML data from the page. Scroll through the data and look for important things like "no cache". You will also probably recognize some of the HTML code.

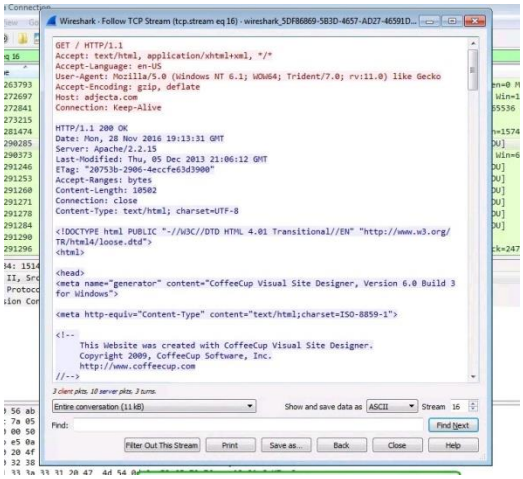

Figure 5: Raw TCP Stream Data

7) At the bottom of this window are some options. Click Close. Make sure the packet capture has been stopped. Select File ► Export Objects ► HTTP. In the resulting window, find the hostname corresponding to the site that contains text/html. Example:

**1842 monkees.com text/html 10kb **

Click the "Save" button. Save the file (with an html extension) To your WIRESHARK-Lab folder as "Following an HTTP stream.html". Then close that window. You can open it in a web browser and it will show you a text version of the webpage with no pictures in it.

8) Minimize all windows and find the file you just saved and open it with a web browser. If the web site is primarily javascript (as many web sites are) or photos, what you see won't be very impressive; however, figure 6 shows http://www.java.com on the left side, while its TCP stream produces the page shown on the right side of the figure. Although you can't see the graphics in the rendered file, you can easily determine its main theme.

Figure 6: Java.com

ASSIGNMENT DELIVERABLE # 1 (continued): Save the output from your websearch to find 3 sites that do NOT cache their main pages along with the above capture. Go to Wireshark, click, File, Save As, then name it "websites") to your WIRESHARK folder.

Part 3: Viewing an FTP transfer

We will now look at the file transfer between an FTP client and an FTP server. You will need a second computer on your network capable of providing file transfer services (an FTP server). I have an FTP server running already for you to use

Server:	192.168.1.34 (in the EiLab)
User:	mis4477
Password:	secret

Step 1: Setting up the FTP program

If you have not already done so, download and install WinSCP from http://winscp.net. Download the "Installation Package" and run it. Notate this in your WIRESHARK notes file.

Run WinSCP and set up a connection. Change the protocol from the default **SFTP** to **FTP** with **no encryption**. (Note: SFTP is not the same as FTPS, which is FTP over TLS/SSL) For the host name, enter "192.168.1.34". Enter "mis4477" for the user and "secret" for the password, then click Save as and save it along with the password so you don't have to type it in again. DO NOT log in yet.

Step 2: Monitor the FTP login exchange

To see the packet interchange between the two computers, perform the following:

1) Open Wireshark on the client, ensure that your capture options are set as before. Clear any previous filter by clicking on Clear. Then type "tcp.port==21" in the apply a display filter box at the top, click the right Apply arrow and begin another capture session. This will show you ONLY the FTP traffic. The FTP service uses port 21.
2) Switch back to the WinSCP FTP program and click Login to establish a connection with the above criteria.
3) If the login was successful, go back to Wireshark and stop the packet capture.

Look for the FTP packets in the Protocol column. In the "Info" column it will say "Request: …" and "Response: …" You should notice that the username and password are displayed for you in this column in readable clear text (also called plaintext). This is shown in figure 8.

If you have never seen a password revealed in a packet sniffer, it can be a real eye opener. Although we know that FTP servers are inherently not secure, this demonstration should make you think about the security of other types of logins. This is how Telnet and FTP worked for years before hacking and security became an issue. We no longer use Telnet (port 23) for remote shell access to a server. We use SSH (port 22). It does the same thing, except it encrypts everything end-to-end.

Try this: Go back to WinSCP and click on Session and New Session, and click on add a new site. This time, choose FTP for the protocol but change the encryption to **FTP over TLS Explicit Encryption**, keep 192.168.1.34 for the host, make sure the port stays at 21, user name and password is the same. Save it as mis4477@192.168.1.34 (secure) . Now switch back to Wireshark and start the packet capture, **first saving your previous packet capture as "FTP unsecure**". Then, go back to Winscp and click Login. First you will note that it asks you to trust this site, click yes. It is sharing a self-signed SSL encryption key. Now go back to Wireshark. What do you see? It should be telling you there are "Encrypted Packets" going back and forth. So, you can be assured that your data is safe. The only thing you can tell from Wireshark is that a TCP connection was made and to where. Save this capture as "FTP Secure".

ASSIGNMENT DELIVERABLE # 2: Save the packet captures to your WIREHSARK folder along with a description in your notes file of what appears to be going on and the difference between ftp and sftp. NOTE, THEY CAN BE VERY LARGE, so redo the FTP and SFTP capture part again but this time, after you filter the FTP and SFTP packets, click File and Export Specified Packets and make sure the "Displayed" button is marked to save just those packets that were filtered out and displayed on your screen. To make sure you did this right, close Wireshark, restart it, and Click File and Open and choose your FTP Unsecure Capture file. If you are unclear about how to do this, google for "How to save only displayed capture wireshark"

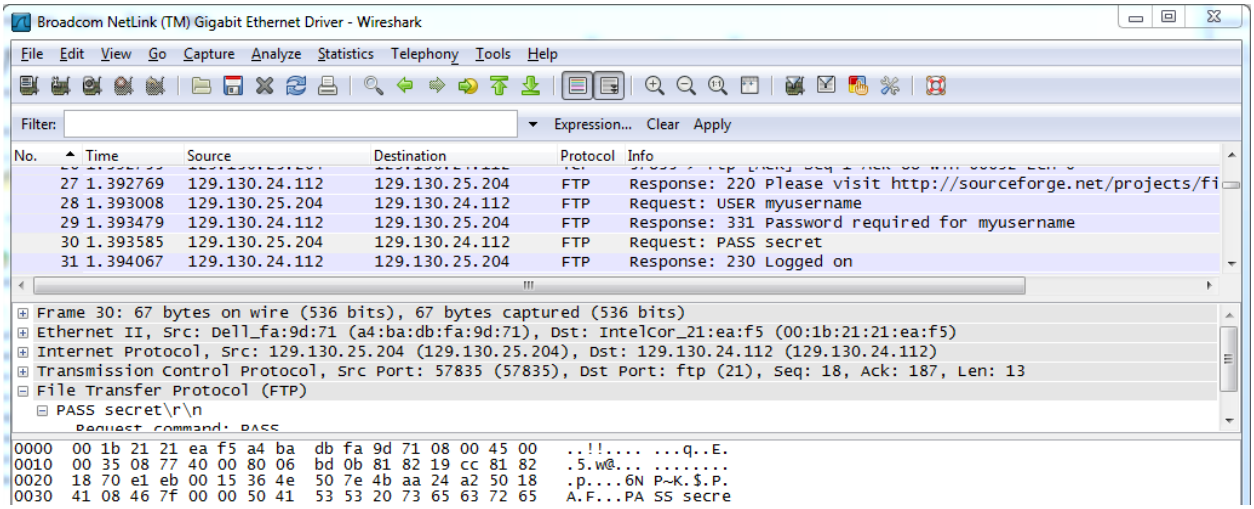

Figure 8: An FTP Login Sequence in Wireshark

(continued on next page)

ASSIGNMENT DELIVERABLE # 3: Answer these short essay questions. Copy and paste them along with your answers in a different color or font into your WIRESHARK-Lab notes file"

1. Packet sniffing can be a controversial subject. Discuss any issues related to ethics that might arise when an organization monitors the electronic activity of its employees, i.e. what sort of issues might arise by sniffing employees' web browsing activity?
2. You looked at packets captured during a web page request. What might this be useful for?
3. Most computers are connected together with switches (rather than hubs). How does this affect the packet capturing process? (hint, can you see traffic from your fellow students?)
4. Discuss how sniffing packets from wireless networks might differ from wired networks. Hint, use google to answer this. Search for wireless packet sniffers and name a couple. Where would be a good place to test out a wireless packet sniffer?

Once you are done with collecting all the data, updating your WIRESHARK-Lab notes and saving your Packet Captures to the WIRESHARK-Lab folder, save and close everything. Disconnect from your VM. DO NOT log off or it will turn it off. Then submit the assignment as mentioned at the top of this instruction.

END OF LAB ASSIGNMENT – THANK YOU ALL!!! Jake