CSE, VNIT Nagpur

CN Lab Assignment

Instructions:

- Make a brief video (max 10 min) explaining each question on your system. Also make a report of the answers, along with the screenshots, in a pdf format.
- Upload your video (size < 300MB) and answer sheet here in pdf only (can be uploaded only once). Also ensure it has good clarity. Name your files as: <roll no>_<Name>_CNs24_A2.<extension of pdf or video>

HTTP: Assignment

Begin Wireshark packet capture and Enter the following to your browser "http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html" Your browser should display the very simple, one-line HTML file. Now Stop Wireshark packet capture.By looking at the information in the HTTP GET and response messages, answer the following questions:

1. Is your browser running HTTP version 1.0 or 1.1?
2. What languages (if any) does your browser indicate that it can accept to the server?
3. What is the IP address of your computer?
4. What is the status code returned from the server to your browser?

Start up the Wireshark packet sniffer. Enter the following URL into your browser(make sure your browser's cache is empty) http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html . Your browser should display a very simple five-line HTML file.Quickly enter the same URL into your browser again (or simply select the refresh button on your browser).Stop Wireshark packet capture.

Answer the following questions:

5. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?
6. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Start up the Wireshark packet sniffer. Enter the following URL into your browser(make sure your browser’s cache is empty) http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html .Your browser should display the lengthy US Bill of Rights. Stop Wireshark packet capture, and enter “http” in the display-filter-specification window, so that only captured HTTP messages will be displayed.

Answer the following questions:

7. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?
8. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

Start up the Wireshark packet sniffer. Enter the following URL into your browser (make sure your browser’s cache is empty) http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html Your browser should display a short HTML file with two images. Stop Wireshark packet capture.

Answer the following questions:

9. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?
10. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two websites in parallel? Explain

DNS: Assignment

nslookup: nslookup tool allows the host running the tool to query any specified DNS server for a DNS record. The queried DNS server can be a root DNS server, a top-level-domain DNS server, an authoritative DNS server, or an intermediate DNS server.To accomplish this task, nslookup sends a DNS query to the specified DNS server, receives a DNS reply from that same DNS server, and displays the result.

1. Run **'nslookup www.mit.edu'** on your command prompt and what will be the name and IP address of the DNS server that provides the answer?
2. Run **'nslookup –type=NS mit.edu'** on your command prompt and what will be the host names of the authoritative DNS for mit.edu.
3. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?

ipconfig: ipconfig (for Windows) and ifconfig (for Linux/Unix) are among the most useful little utilities in your host, especially for debugging network issues. ipconfig can be used to show your current TCP/IP information, including your address, DNS server addresses, adapter type and so on. For example, you can get all this information about your host simply by entering **'ipconfig \all'** into the Command Prompt.

'ipconfig /displaydns' -->Each entry shows the remaining Time to Live (TTL) in seconds.

To clear the cache, enter **'ipconfig /flushdns'** Flushing the DNS cache clears all entries and reloads the entries from the hosts file.

Now that we are familiar with nslookup and ipconfig, firstly now capture the DNS packets that are generated by ordinary Websurfing activity.

- Use ipconfig to empty the DNS cache in your host.
- Open your browser and empty your browser cache.
- Open Wireshark and enter "ip.addr == <your_IP_address>" into the filter, where you obtain your_IP_address with ipconfig. This filter removes all packets that neither originate nor are destined to your host.
- Start packet capture in Wireshark.
- With your browser, visit the Web page: http://www.ietf.org
- Stop packet capture.

Now answer the following questions:

4. Locate the DNS query and response messages. Are they sent over UDP or TCP?
5. What is the destination port for the DNS query message? What is the source port of the DNS response message?
6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

TCP Assignment

- Start up your web browser. Go the http://gaia.cs.umass.edu/wireshark-labs/alice.txt and retrieve an ASCII copy of *Alice in Wonderland.* Store this file somewhere on your computer.
- Next go to http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html.
- Use the *Browse* button in this form to enter the name of the file (full path name) on your computer containing *Alice in Wonderland* (or do so manually). Don't yet press the "*Upload alice.txt file*" button.
- Now start up Wireshark and begin packet capture *(Capture->Start)* and then press *OK* on the Wireshark Packet Capture Options screen (we'll not need to select any options here).
- Returning to your browser, press the "*Upload alice.txt file*" button to upload the file to the gaia.cs.umass.edu server. Once the file has been uploaded, a short congratulations message will be displayed in your browser window.
- Stop Wireshark packet capture.
- Before analyzing the behavior of the TCP connection in detail, let's take a high level view of the trace. First, filter the packets displayed in the Wireshark window by entering "tcp"

Use the packet trace that you have captured and answer the following questions, by opening the Wireshark captured packet file.

1. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu?
2. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?
3. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?
4. Answer the following:
    a. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN?
    b. What is the value of the Acknowledgement field in the SYNACK segment?
    c. How did gaia.cs.umass.edu determine that value?
    d. What is it in the segment that identifies the segment as a SYNACK segment?

5. What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command; you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.

6. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection:

    a. What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST)?

    b. At what time was each segment sent? And when was the ACK for each segment received?

    c. What is the EstimatedRTT value after the receipt of each ACK? (*Use the EstimatedRTT equation. Assume that the value of the

EstimatedRTT is equal to the measured RTT for the first segment, and then is computed using the EstimatedRTT equation).

d. What is the length of each of the first six TCP segments?

e. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

UDP Assignment

==

Start capturing packets in Wireshark and then do something that will cause your host to send and receive several UDP packets. It's also likely that just by doing nothing (except capturing packets via Wireshark) that some UDP packets sent by others will appear in your trace. After stopping packet capture, set your packet filter so that Wireshark only displays the UDP packets sent and received at your host. Pick one of these UDP packets and expand the UDP fields in the details window.

*Note: If you are unable to find UDP packets or are unable to run Wireshark on a live network connection, you can download a packet trace containing some UDP packets.

(Download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the file http-ethereal-trace-5, which contains some UDP packets carrying SNMP messages. The traces in this zip file were collected by Wireshark running on one of the author's computers. Once you have downloaded the trace, you can load it into Wireshark and view the trace using the *File* pull down menu, choosing *Open*, and then selecting the http-ethereal-trace-5 trace file.)

Use the packet trace that you have captured and answer the following questions, by opening the Wireshark captured packet file.

1. Select *one* UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. Name these fields. (Answer these questions directly from what you observe in the packet trace.)
2. By consulting the displayed information in Wireshark's packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.
3. The value in the Length field is the length of what? (You can consult the text for this answer). Verify your claim with your captured UDP packet.
4. What is the maximum number of bytes that can be included in a UDP payload?
5. What is the largest possible source port number?
6. What is the protocol number for UDP?