Assignment 3

Wireshark

Part 1 (HTTP)

A. The Basic HTTP GET/RESPONSE interaction

Download a very simple HTML file - one that is very short, and contains no embedded objects. Do the following:

- Start up your web browser
- Start up the Wireshark packet sniffer (but don't yet begin packet capture). Enter "http" (just the letters, not the quotation marks) in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window. (We're only interested in the HTTP protocol here, and don't want to see the clutter of all captured packets).
- Wait a bit more than one minute (you'll see why shortly), and then begin Wireshark packet capture.
- Enter the following to your browser http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html
- Stop Wireshark packet capture.

If you are unable to run Wireshark on a live network connection, you can download a packet trace that was created when the steps above were followed
By looking at the information in the HTTP GET and response messages, answer the following questions. When answering the following questions, you should print out the GET and response messages and indicate where in the message you've found the information that answers the following questions.

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running? What languages (if any) does your browser indicate that it can accept to the server?
2. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
3. What is the status code returned from the server to your browser?
4. When was the HTML file that you are retrieving last modified at the server?
5. How many bytes of content are being returned to your browser?

B. The HTTP CONDITIONAL GET/response interaction

Most web browsers perform object caching and thus perform a conditional GET when retrieving an HTTP object. Before performing the steps below, make sure your browser's cache is empty. (To do this under Firefox, select Tools->Clear Private Data, or for Internet Explorer, select Tools->Internet Options->Delete File; these actions will remove cached files from your browser's cache.)
Now do the following :

- Start up your web browser, and make sure your browser's cache is cleared, as discussed above.
- Start up the Wireshark packet sniffer
- Enter the following URL into your browser
  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, and enter "http" in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window.

(*Note: If you are unable to run Wireshark on a live network connection, you can use the http-ethereal-trace-2 packet trace to answer the questions below)*

7. 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?
8. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
9. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? If so, what information follows the "IF-MODIFIED-SINCE:" header?
10. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

Part 2(DNS)

A. **Tracing DNS with Wireshark**
First you need to capture the DNS packets that are generated by ordinary Web-surfing activity.

- Use ipconfig(Windows)/ifconfig(linux) to empty the DNS cache in your host.
- Open your browser and empty your browser cache. (With Internet Explorer, go to Tools menu and select Internet Options; then in the General tab select Delete Files.)
- Open Wireshark and enter “ip.addr == your_IP_address” into the filter, where you obtain your_IP_address (the IP address for the computer on which you are running Wireshark) 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.

Answer the following questions :

1. Locate the DNS query and response messages. Are they sent over UDP or TCP?
2. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?
3. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?
4. This web page contains images. Before retrieving each image, does your host issue new DNS queries?
5. Sort the queries according to their DNS response time. Attach screenshot along with it.

   Now do the following:
   - Start packet capture.
   - Do an nslookup on www.mit.edu
   - Stop packet capture.

6. What is the destination port for the DNS query message? What is the source port of DNS response message?
7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”? If yes, then how many “answers” are provided? What does each of these answers contain?
8. Examine the DNS response message. What “Type” of DNS query is it? Does the response message contain any “answers”? If yes, then how many “answers” are provided? What does each of these answers contain?

Now do the following

- Start packet capture.
- Do nslookup –type=NS mit.edu
- Stop packet capture.

9. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
10. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
11. Examine the DNS response message. What MIT name servers does the response message provide? Does this response message also provide the IP addresses of the MIT name servers?

Part 3 (TCP)

Download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the file *tcpethereal-trace-1.* 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 *tcp-ethereal-trace-1* trace file.

Whenever possible, when answering a question you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. Annotate the printout 3 to explain your answer. To print a packet, use File->Print, choose Selected packet only, choose Packet summary line, and select the minimum amount of packet detail that you need to answer the question.

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? To answer this question, it's probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the "details of the selected packet header window".
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?

Change Wireshark's "listing of captured packets" window so that it shows information about the TCP segments containing the HTTP or other messages, rather than about the HTTP or other messages. To have Wireshark do this, select Analyze->Enabled Protocols. Then uncheck the HTTP box (if checked) and select OK.

We will use the packet trace to analyze TCP behavior *tcpethereal-trace-1* in http://gaia.cs.umass.edu/wireshark-labs/wiresharktraces.zip. Answer the following questions for the TCP segments:

1. 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?
2. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did *gaia.cs.umass.edu* determine that value? What is it in the segment that identifies the segment as a SYNACK segment?
3. 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.
4. What is the length of each of the first six TCP segments?
5. What is the minimum amount of available buffer space advertised at the received for the entire trace? Does the lack of receiver buffer space ever throttle the sender?
6. Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?

Part 4 (UDP)

Start capturing packets in Wireshark and then do something that will cause your host to send and receive several UDP packets. (One way to do this would be to use the nslookup command) 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.
Whenever possible, when answering a question you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. Annotate the printout to explain your answer.
To print a packet, use File->Print, choose Selected packet only, choose Packet summary line, and select the minimum amount of packet detail that you need to answer the question.

1. Select one packet. From this packet, determine how many fields are there in the UDP header. Name these fields
2. The value in the length field is the length of what? Verify your claim with the captured UDP packet.
3. Observe the source address. Verify that the source address is your IP address.
4. Observe the destination address.
5. What is the maximum number of bytes that can be included in a UDP payload?
6. What is the largest possible port number?
7. What is the protocol number for UDP?(Hint : You will need to look into the IP header)
8. Search “UDP” on google and determine the fields on which the UDP checksum is calculated.
9. Examine a pair of UDP packets in which the first packet is sent by your host and the second packet is a reply to the first packet. Describe the relationship between the port numbers in the two packets.