Wireshark Day 1

Download & install wireshark (installation exe included in the resources older for easy reference).

HTTP: Find HTTP packets from <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html> and set wireshark to hide all others (ex: TCP, IP), then give the following information:

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

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? Of the gaia.cs.umass.edu server?

4. What is the status code returned from the server to your browser?

5. When was the HTML file last modified at the server?

6. How many bytes of content are being returned to your browser?

7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

DNS:

1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server? 2. Run nslookup to determine the authoritative DNS servers for a university in Europe.

3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

4. Try out the ipconfig \all, ipconfig \displaydns, and ipconfig \flushdns commands in command prompt. What do they do?

5. Open your browser and empty your browser cache. In wireshark, remove all packets that neither originate nor are destined to your host. Start packet capture in Wireshark and visit <http://www.ietf.org>

* Locate the DNS query and response messages. Are then sent over UDP or TCP?
* What is the destination port for the DNS query message? What is the source port of DNS response message?
* 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?
* Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
* Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?
* Consider the 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?
* This web page contains images. Before retrieving each image, does your host issue new DNS queries?

6. Start packet capture, then do an nslookup on [www.mit.edu](http://www.mit.edu). You’ll find three DNS queries and responses, but for the purpose for the purpose of this lab, just focus on the last query and response message.

* What is the destination port for the DNS query message? What is the source port of DNS response message?
* To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
* Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
* Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

7. Do another capture with nslookup –type=NS mit.edu

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

8. Do another capture with nslookup www.aiit.or.kr bitsy.mit.edu

* To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?
* Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
* Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

TCP:

1. To start off, follow this link <http://gaia.cs.umass.edu/wiresharklabs/alice.txt> and save the file somewhere easily accessible on your computer. Next, go to <http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html> and start a capture. Then click “Upload alice.txt file.” Go ahead and filter out everything that’s not TCP from the capture file.

* 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?
* What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?
* What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu?

2. Change Wireshark’s “listing of captured packets” window so that it shows information about the TCP segments containing the HTTP messages, rather than about the HTTP messages.

* 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 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 sequence number of the TCP segment containing the HTTP POST command?
* What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST)? At what time was each segment sent? When was the ACK for each segment received?
* What is the length of each of the first six TCP segments?
* What is the minimum amount of available buffer space advertised at the received for the entire trace?
* Are there any retransmitted segments in the trace file?
* What is the throughput (bytes transferred per unit time) for the TCP connection?

UDP: Download the wireshark-traces.zip file in the resources folder and extract http-ethereal-trace-5. Open it in wireshark, filter so it only shows UDP packets, and select a random packet to work with.

* Select one UDP packet from the trace. From this packet, determine how many fields there are in the UDP header and name those fields.
* Determine the length (in bytes) of each of the UDP header fields.
* The value in the Length field is the length of what?
* What is the maximum number of bytes that can be included in a UDP payload? (Hint: related to the second part of the problem)
* What is the largest possible source port number?
* What is the protocol number (hexadecimal and decimal notation) for UDP?
* Examine a pair of UDP packets in which the host sent the first UDP packet and the second UDP packet is a reply to this first UDP packet. (Hint: for a second packet to be sent in response to a first packet, the sender of the first packet should be the destination of the second packet). Know the relationship between the port numbers in the two packets.

IP: To begin, simply install pingplotter using the exe file provided in the resources folder.

1. Start a capture, then open up pingplotter and enter the name of a target destination in the “Address to Trace Window.” Enter 3 in the “# of times to Trace” field so that you don’t gather too much data. Find Packet Options and enter a value of 56 in the Packet Size field and then start the trace.

* Select the first ICMP Echo Request message sent by your computer, and expand the IP part of the packet in the packet details window and find your own IP.
* What is the value in the upper layer protocol field?
* How many bytes are in the IP header? How many bytes are in the payload of the IP datagram?
* Has this IP datagram been fragmented?

2. Next, sort the traced packets according to IP source address by clicking on the Source column header. Select the first ICMP Echo Request message sent by your computer, and expand the IP portion in the “details of selected packet header” window. In the “listing of captured packets” window, you should see some ICMP messages.

* Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?
* Which fields stay constant? Which of the fields must stay constant? Which fields must change?
* Can you see a pattern in the values in the Identification field of the IP datagram.

3. With the packets still sorted by source address, find the series of ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router.

* What is the value in the Identification field and the TTL field?
* Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router?

Lab created by Mary Sawyer.