Wireshark
Exercises

A Project Using the Wireshark Packet Analyzer

November 2011

Table of Contents

I) Exercise One

Open "Wireshark", then use the "File" menu and the "Open" command to open the file "Exercise One.pcap". You should see 26 packets listed.

This set of packets describes a 'conversation' between a user's client and a central server. This entire conversation happens automatically, after a user types something and hits enter. Look at the packets to answer the following questions in relation to this conversation.

In answering the following questions, use brief descriptions. For example, "In frame X, the client requests a web page, and in frame Y, the server delivers the content of the page."

a) What is the IP address of the client that initiates the conversation?
a) Use the first two packets to identify the server that is going to be contacted. List the common name, and three IP addresses that can be used for the server.
b) What is happening in frames 3, 4, and 5?
c) What is happening in frames 6 and 7?
d) Ignore frame eight. However, for your information, frame eight is used to manage flow control.
e) What is happening in frames nine and ten? How are these two frames related?
f) What happens in packet 11?
g) After the initial set of packets is received, the client sends out a new request in packet 12. This occurs automatically without any action by the user. Why does this occur? See the first "hint" to the left.
h) What is occurring in packets 13 through 22?
i) Explain what happens in packets 23 through 26. See the second "hint" to the left.
j) In one sentence describe what the user was doing (Reading email? Accessing a web page? FTP? Other?).

Hint: See the accompanying document titled the "QuickStart Guide" – Look under the appendix describing "Hits Versus Page Views".

Hint: a favicon.ico is a small graphic that can be used as an icon to identify a web page. In the following graphic the colorful "G" to the left is a favicon.ico.

Review: The TCP/IP network does not know how to route using names, such as www.yahoo.com. It only knows how to route using IP addresses. Therefore, a common name (CNAME), such as www.yahoo.com must be translated to an IP address, like 216.109.117.106 before your computer can request a web page.

Your computer uses a DNS request to lookup a CNAME and it gets back a set of IP addresses (a primary address and one or more backup addresses) that can be used to contact the server.

Hint: See the accompanying document titled the "QuickStart Guide" – Look under the appendix describing "Hits Versus Page Views".

II) Exercise Two

Open "Wireshark", then use the "File" menu and the "Open" command to open the file "Exercise Two.pcap". You should see 176 packets listed.

a) In the first few packets, the client machine is looking up the common name (cname) of a web site to find its IP address. What is the cname of this web site? Give two IP addresses for this web site.
b) How many packets/frames does it take to receive the web page (the answer to the first http get request only)?
c) Does this web site use gzip to compress its data for sending? Does it write cookies? In order to answer these questions, look under the payload for the reassembled packet that represents the web page. This will be the last packet from question b above. Look to see if it has "Content-Encoding" set to gzip, and to see if it has a "Set-Cookie" to write a cookie.
d) What is happening in packets 26 and 27? Does every component of a web page have to come from the same server? See the Hint to the left.
e) In packet 37 we see another DNS query, this time for us.i1.yimg.com. Why does the client need to ask for this IP address? Didn't we just get this address in packet 26? (This is a trick question; carefully compare the two common names in packet 26 and 37.)
f) In packet 42 we see a HTTP "Get" statement, and in packet 48 a new HTTP "Get" statement. Why didn't the system need another DNS request before the second get statement? Click on packet 42 and look in the middle window. Expand the line titled "Hypertext Transfer Protocol" and read the "Host:" line. Compare that line to the "Host:" line for packet 48.
g) Examine packet 139. It is one segment of a PDU that is reassembled with several other segments in packet 160. Look at packets 141, 142, and 143. Are these three packets also part of packet 160? What happens if a set of packets that are supposed to be reassembled do not arrive in a continuous stream or do not arrive in the proper order?
h) Return to examine frames 141 and 142. Both of these are graphics (GIF files) from the same source IP address. How does the client know which graphic to match up to each get statement? Hint: Click on each

and look in the middle window for the heading line that starts with “Transmission Control Protocol”. What difference do you see in the heading lines for the two files? Return to the original “Get” statements. Can you see the same difference in the “Get” statements?

III) Exercise Three

Open "Wireshark", then use the "File" menu and the "Open" command to open the file "Exercise Three.pcap". You should see 22 packets listed.

These packets represent two different requests for web pages. Packets 1-7 involve the request for the web page www.yahoo.com. Packets 8-22 involve the request for the web page my.usf.edu.

a) Compare the destination port in the TCP packet in frame 3 with the destination port in the TCP packet in frame 12. What difference do you see? What does this tell you about the difference in the two requests?

The following table compares the two requests for web pages. For example, row i) shows that frames 1-2 and frames 8-9 represent the DNS lookups for each of the web requests.

Row	www.yahoo.com frames	my.usf.com frames	Brief Explanation of Activity
i)	1-2	8-9	DNS Request to find IP address for common name & DNS Response
ii)	3-5	10-12	Three-way handshake
iii)	--	13-20	
iv)	6	21	"Get" request for web page
v)	7	22	First packet from web server with web page content.

b) Explain what is happening in row "iii" above. Why are there no frames listed for yahoo in row "iii"?

c) Look at the "Info" column on frame 6. It says: "GET / HTTP / 1.1. What is the corresponding Info field for the my.usf.com web request (frame 21)? Why doesn't it read the same as in frame 6?

IV) Exercise Four

In this exercise, you are going to capture live traffic from your computer. Open up Wireshark and use the "Capture" menu to save live traffic. The Wireshark "QuickStart" guide distributed with these exercises contains more instructions on using Wireshark.

Start capturing data, visit a live web site using your standard Internet browser, and stop capturing data.

If you have a large amount of network traffic, the relevant data may be hidden among a lot of broadcast messages. To focus on just the key frames, you can set a display filter like this.

For the IP number enter the IP number of your client machine. Type it as shown (ip.addr==your.ip.address) in the graphic above. Then click on "Apply".

Using an approach similar to the approach in Exercise One, describe the set of frames that you captured.

- For this description think of this as a conversation – every discussion starts with a question and follows with an answer.
- For example, two of the frames will contain the DNS request for an IP address for the web site, and the DNS answer with the IP number.
- Remember that some answers may take several frames if they need to be reassembled from segmented packets.

First, you must decide on a web site to visit. Pick a web site, such as www.yahoo.com, or www.cnn.com that you haven't visited yet today.

If you pick one that you recently visited, your system may not need to send out a DNS request, since the IP address may be cached (saved temporarily) on your machine. For this exercise, we would prefer to have a DNS request as part of the detail of transactions.