

## Introduction to Computer Networks

**Project #1** 15 points

**Due:** October 15, 10:00am

**Hand in:** answers to Part A questions 1 – 3, answers to Part B questions 1 – 18

**Submit: (1)** a hardcopy in class

Note: You are expected to submit a well-organized hardcopy report in class. The report should include

- your names, the project number, date, and etc.;
- the original questions and your answers right under the questions. Remember to include supporting materials for your answers. You have to explain how you get each answer by showing diagrams/screenshots (0.5pts) when appropriate and highlighting the related fields (0.5pts).
- **60% of the points count for answering each question, and 40% of the points count for printing out the right supporting material.**
- A sample document is listed at the end of this document.
- This is a group project, and two students a group.

### Part A

Wireshark Lab: Getting Started

Version: 2.0 © 2007 J.F. Kurose, K.W. Ross. All Rights Reserved

One's understanding of network protocols can often be greatly deepened by "seeing protocols in action" and by "playing around with protocols" – observing the sequence of messages exchanged between two protocol entities, delving down into the details of protocol operation, and causing protocols to perform certain actions and then observing these actions and their consequences. In the Wireshark labs<sup>1</sup>, you'll be running various network applications in different scenarios using a computer on your desk, at home, or in a lab. You'll observe the network protocols in your computer "in action," interacting and exchanging messages with protocol entities executing elsewhere in the Internet.

The basic tool for observing the messages exchanged between executing protocol entities is called a packet sniffer. As the name suggests, a packet sniffer captures ("sniffs") messages being sent/received from/by your computer; it will also typically store and/or display the contents of the various protocol fields in these captured messages. A packet sniffer itself is passive. It observes messages being sent and received by applications and protocols running on your computer, but never sends packets itself. Similarly, received packets are never explicitly addressed to the packet sniffer. Instead, a packet sniffer receives a copy of packets that are sent/received from/by application and protocols executing on your machine.

Figure 1 shows the structure of a packet sniffer. At the right of Figure 1 are the protocols (in this case, Internet protocols) and applications (such as a web browser or ftp client) that normally run on your computer. The packet sniffer, shown within the dashed rectangle in Figure 1 is an addition to the usual software in your computer, and consists of two parts. The packet capture library receives a copy of every link-layer frame that is sent from or received by your computer. Recall from the discussion from section 1.5 in the text (Figure 1.20<sup>2</sup>) that messages exchanged by higher layer protocols such as HTTP, FTP, TCP, UDP, DNS, or IP all are eventually encapsulated in link-layer frames that are transmitted over physical media such as an Ethernet cable. In Figure 1, the assumed physical media is an Ethernet, and so all upper layer protocols are eventually encapsulated within an Ethernet frame. Capturing all link-layer frames thus gives you all messages sent/received from/by all protocols and applications executing in your computer.

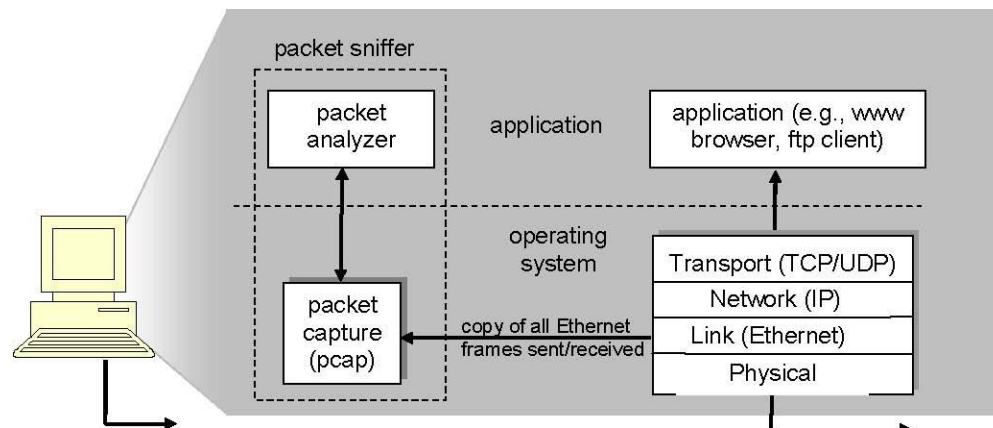
The second component of a packet sniffer is the packet analyzer, which displays the contents of all

---

<sup>1</sup> Earlier versions of these labs used the Ethereal packet analyzer. In May 2006, the developer of Ethereal joined a new company, and had to leave the Ethereal® trademarks behind. He then created the Wireshark network protocol analyzer, a successor to Ethereal®. Since Ethereal® is no longer being actively maintained or developed, we have thus switched these labs over to Wireshark with the 4<sup>th</sup> edition of our text.

<sup>2</sup> Figure numbers refer to figures in the 4<sup>th</sup> edition of our text.

fields within a protocol message. In order to do so, the packet analyzer must “understand” the structure of all messages exchanged by protocols. For example, suppose we are interested in displaying the various fields in messages exchanged by the HTTP protocol in Figure 1. The packet analyzer understands the format of Ethernet frames, and so can identify the IP datagram within an Ethernet frame. It also understands the IP datagram format, so that it can extract the TCP segment within the IP datagram. Finally, it understands the TCP segment structure, so it can extract the HTTP message contained in the TCP segment. Finally, it understands the HTTP protocol and so, for example, knows that the first bytes of an HTTP message will contain the string “GET,” “POST,” or “HEAD,” as shown in Figure 2.8 in the text.



**Figure 1:** Packet sniffer structure

We will be using the Wireshark packet sniffer (<http://www.wireshark.org/>) for these labs, allowing us to display the contents of messages being sent/received from/by protocols at different levels of the protocol stack. (Technically speaking, Wireshark is a packet analyzer that uses a packet capture library in your computer). Wireshark is a free network protocol analyzer that runs on Windows, Linux/Unix, and Mac computers. It’s an ideal packet analyzer for our labs – it is stable, has a large user base and well-documented support that includes:

- a user-guide ([http://www.wireshark.org/docs/wsug\\_html\\_chunked/](http://www.wireshark.org/docs/wsug_html_chunked/))
- man pages (<http://www.wireshark.org/docs/man-pages/>)
- a detailed FAQ (<http://www.wireshark.org/faq.html>)

### Getting Wireshark

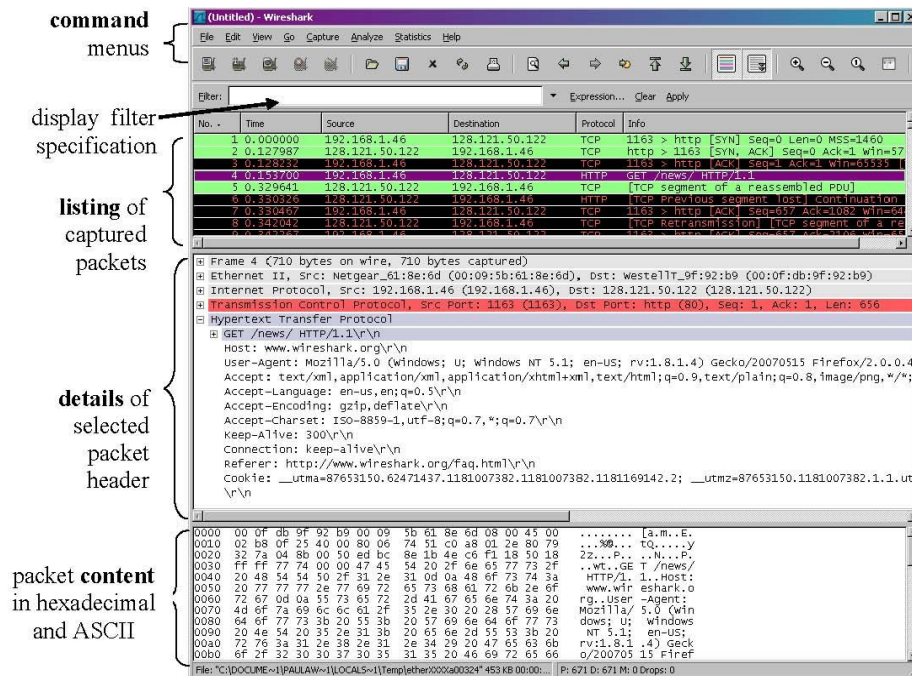
1. Wireshark has been installed in all machines in Jiao-2 104

2. Alternatively, you can install Wireshark on your own computer, See <http://www.wireshark.org/download.html> for a list of supported operating systems and download sites. Download and install the Wireshark software:

- Go to <http://www.wireshark.org/download.html> and download and install the Wireshark binary for your computer.
- Download the Wireshark user guide. The Wireshark FAQ has a number of helpful hints and interesting tidbits of information, particularly if you have trouble installing or running Wireshark.

### Running Wireshark

When you run the Wireshark program, the Wireshark graphical user interface shown in Figure 2 will be displayed. Initially, no data will be displayed in the various windows.



**Figure 2: Wireshark Graphical User Interface**

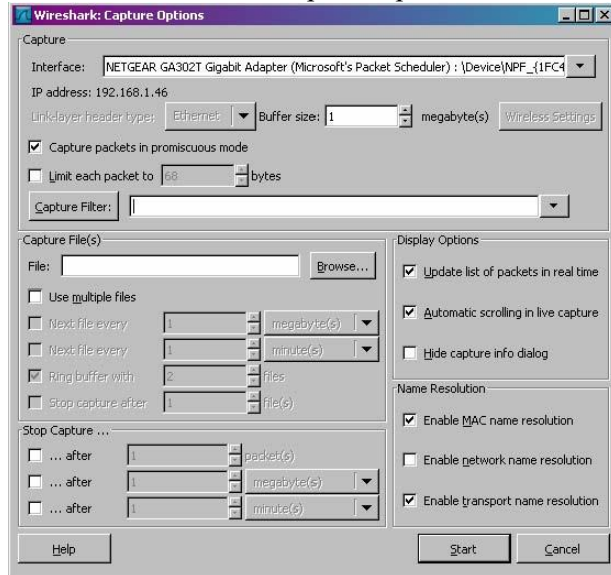
The Wireshark interface has five major components:

- The command menus are standard pulldown menus located at the top of the window. Of interest to us now are the File and Capture menus. The File menu allows you to save captured packet data or open a file containing previously captured packet data, and exit the Wireshark application. The Capture menu allows you to begin packet capture.
- The packet-listing window displays a one-line summary for each packet captured, including the packet number (assigned by Wireshark; this is not a packet number contained in any protocol's header), the time at which the packet was captured, the packet's source and destination addresses, the protocol type, and protocol-specific information contained in the packet. The packet listing can be sorted according to any of these categories by clicking on a column name. The protocol type field lists the highest level protocol that sent or received this packet, i.e., the protocol that is the source or ultimate sink for this packet.
- The packet-header details window provides details about the packet selected (highlighted) in the packet listing window. (To select a packet in the packet listing window, place the cursor over the packet's one-line summary in the packet listing window and click with the left mouse button.). These details include information about the Ethernet frame (assuming the packet was sent/received over an Ethernet interface) and IP datagram that contains this packet. The amount of Ethernet and IP-layer detail displayed can be expanded or minimized by clicking on the plus-or-minus boxes to the left of the Ethernet frame or IP datagram line in the packet details window. If the packet has been carried over TCP or UDP, TCP or UDP details will also be displayed, which can similarly be expanded or minimized. Finally, details about the highest level protocol that sent or received this packet are also provided.
- The packet-contents window displays the entire contents of the captured frame, in both ASCII and hexadecimal format.
- Towards the top of the Wireshark graphical user interface, is the packet display filter field, into which a protocol name or other information can be entered in order to filter the information displayed in the packet-listing window (and hence the packet-header and packet-contents windows). In the example below, we'll use the packet-display filter field to have Wireshark hide (not display) packets except those that correspond to HTTP messages.

### Taking Wireshark for a Test Run

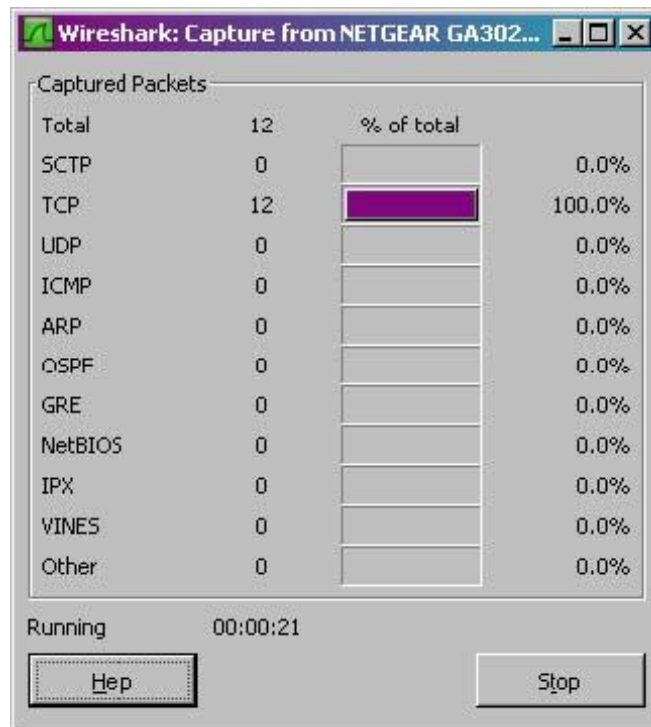
The best way to learn about any new piece of software is to try it out! We'll assume that your computer is connected to the Internet via a wired Ethernet interface. Do the following

- Step 1: Start up your favorite web browser, which will display your selected homepage.
- Step 2: Start up the Wireshark software. You will initially see a window similar to that shown in Figure 2, except that no packet data will be displayed in the packet-listing, packet-header, or packet-contents window, since Wireshark has not yet begun capturing packets.
- Step 3: To begin packet capture, select the Capture pull down menu and select Options. This will cause the “Wireshark: Capture Options” window to be displayed, as shown in Figure 3.



**Figure 3:** Wireshark Capture Options Window

- Step 4: You can use most of the default values in this window, but uncheck “Hide capture info dialog” under Display Options. The network interfaces (i.e., the physical connections) that your computer has to the network will be shown in the Interface pull down menu at the top of the Capture Options window. In case your computer has more than one active network interface (e.g., if you have both a wireless and a wired Ethernet connection), you will need to select an interface that is being used to send and receive packets (mostly likely the wired interface). After selecting the network interface (or using the default interface chosen by Wireshark), click Start. Packet capture will now begin - all packets being sent/received from/by your computer are now being captured by Wireshark!
- Step 5: Once you begin packet capture, a packet capture summary window will appear, as shown in Figure 4. This window summarizes the number of packets of various types that are being captured, and (importantly!) contains the Stop button that will allow you to stop packet capture. Don't stop packet capture yet.



**Figure 4:** Wireshark Packet Capture Window

- Step 6: While Wireshark is running, enter the URL:

<http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>

and have that page displayed in your browser. In order to display this page, your browser will contact the HTTP server at [gaia.cs.umass.edu](http://gaia.cs.umass.edu) and exchange HTTP messages with the server in order to download this page, as discussed in section 2.2 of the text. The Ethernet frames containing these HTTP messages will be captured by Wireshark.

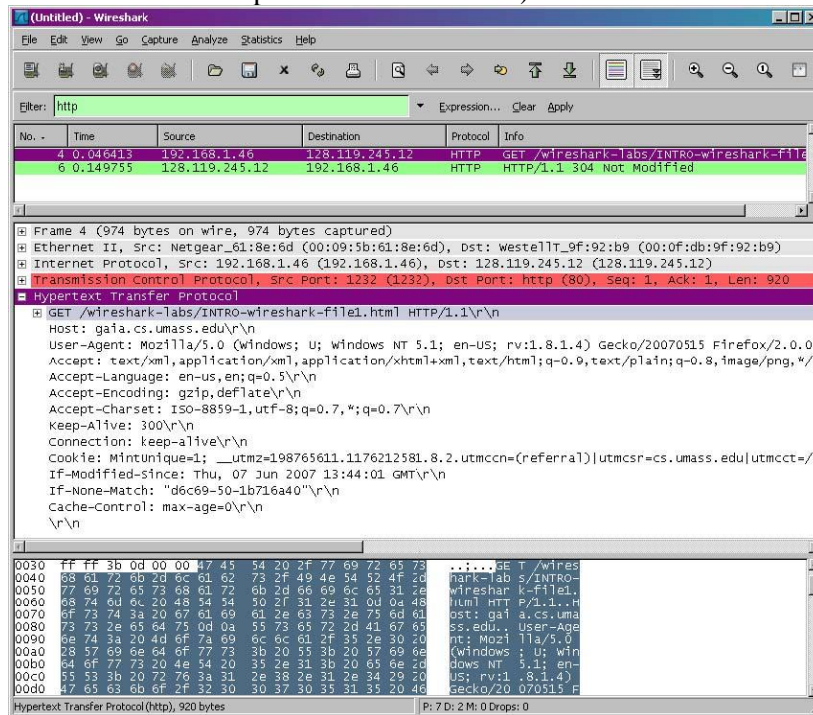
- Step 7: After your browser has displayed the `INTRO-wireshark-file1.html` page, stop Wireshark packet capture by selecting stop in the Wireshark capture window. This will cause the Wireshark capture window to disappear and the main Wireshark window to display all packets captured since you began packet capture. The main Wireshark window should now look similar to Figure 2. You now have live packet data that contains all protocol messages exchanged between your computer and other network entities! The HTTP message exchanges with the [gaia.cs.umass.edu](http://gaia.cs.umass.edu) web server should appear somewhere in the listing of packets captured. But there will be many other types of packets displayed as well (see, e.g., the many different protocol types shown in the Protocol column in Figure 2).

Even though the only action you took was to download a web page, there were evidently many other protocols running on your computer that are unseen by the user. We'll learn much more about these protocols as we progress through the text! For now, you should just be aware that there is often much more going on than "meet's the eye"!

- Step 8: Type in "http" (without the quotes, and in lower case – all protocol names are in lower case in Wireshark) into the display filter specification window at the top of the main Wireshark window. Then select Apply (to the right of where you entered "http"). This will cause only HTTP message to be displayed in the packet-listing window.
- Step 9: Select the first http message shown in the packet-listing window. This should be the HTTP GET message that was sent from your computer to the [gaia.cs.umass.edu](http://gaia.cs.umass.edu) HTTP server. When you select the HTTP GET message, the Ethernet frame, IP datagram, TCP segment, and



HTTP message header information will be displayed in the packet-header window<sup>3</sup>. By clicking plus-and-minus boxes to the left side of the packet details window, minimize the amount of Frame, Ethernet, Internet Protocol, and Transmission Control Protocol information displayed. Maximize the amount information displayed about the HTTP protocol. Your Wireshark display should now look roughly as shown in Figure 5. (Note, in particular, the minimized amount of protocol information for all protocols except HTTP, and the maximized amount of protocol information for HTTP in the packet-header window).



**Figure 5:** Wireshark display after step 9

- Exit Wireshark

The goal of the first part of this lab was primarily to introduce you to Wireshark. The following questions will demonstrate that you've been able to get Wireshark up and running, and have explored some of its capabilities. Based on your Wireshark experimentation, answer the following **Questions**:

1. (0.5 pts) List **up to** 10 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.
2. (1 pt) How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)
3. (1 pt) Print the two HTTP messages displayed above. To do so, select Print from the Wireshark File command menu, and select "Selected Packet Only" and "Print as displayed" and select "output to a file", and then click OK. Copy the text to your final PDF document for submission.

## Part B

### Wireshark Lab: HTTP

<sup>3</sup> Recall that the HTTP GET message that is sent to the gaia.cs.umass.edu web server is contained within a TCP segment, which is contained (encapsulated) in an IP datagram, which is encapsulated in an Ethernet frame. If this process of encapsulation isn't quite clear yet, review section 1.5 in the text

Having gotten our feet wet with the Wireshark packet sniffer in the introductory lab, we're now ready to use Wireshark to investigate protocols in operation. In this lab, we'll explore several aspects of the HTTP protocol: the basic GET/response interaction, HTTP message formats, retrieving large HTML files, retrieving HTML files with embedded objects, and HTTP authentication and security. Before beginning these labs, you might want to review Section 2.2 of the text.

## 1. The Basic HTTP GET/response interaction

Let's begin our exploration of HTTP by downloading a very simple HTML file - one that is very short, and contains no embedded objects. Do the following:

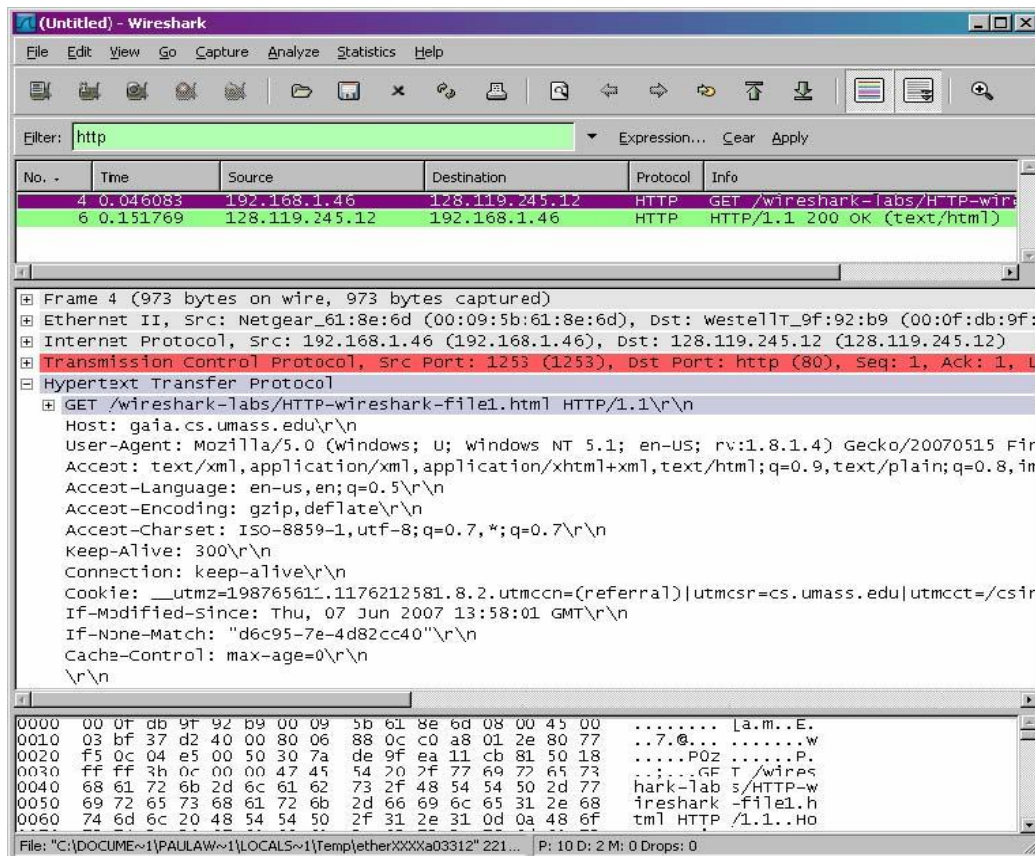
- Start up your web browser.
- Start up the Wireshark packet sniffer, as described in the Introductory lab (but don't yet begin packet capture). Enter "http" (just the letters, not the quotation marks) in the display-filter-specification window, so that only captured HTTP messages will be displayed later 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 (we'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>  
Your browser should display the very simple, one-line HTML file.
- Stop Wireshark packet capture.

Your Wireshark window should look similar to the window shown in Figure 1. 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.<sup>4</sup>

The example in Figure 1 shows in the packet-listing window that two HTTP messages were captured: the GET message (from your browser to the gaia.cs.umass.edu web server) and the response message from the server to your browser. The packet-contents window shows details of the selected message (in this case the HTTP GET message, which is highlighted in the packet-listing window). Recall that since the HTTP message was carried inside a TCP segment, which was carried inside an IP datagram, which was carried within an Ethernet frame, Wireshark displays the Frame, Ethernet, IP, and TCP packet information as well. We want to minimize the amount of non-HTTP data displayed (we're interested in HTTP here, and will be investigating these other protocols in later labs), so make sure the boxes at the far left of the Frame, Ethernet, IP and TCP information have a plus sign (which means there is hidden, undisplayed information), and the HTTP line has a minus sign (which means that all information about the HTTP message is displayed).

---

<sup>4</sup> Download the zip file <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip> and extract the file `http-ethereal-trace-1`. The traces in this zip file were collected by Wireshark running on one of the author's computers, while performing the steps indicated in the Wireshark lab. 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-1` trace file. The resulting display should look just like Figure 1.



**Figure 1:** Wireshark Display after [http://gaia.cs.umass.edu/wireshark-labs/ HTTP-wireshark-file1.html](http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html) has been retrieved by your browser

(Note: You should ignore any HTTP GET and response for favicon.ico. If you see a reference to this file, it is your browser automatically asking the server if it (the server) has a small icon file that should be displayed next to the displayed URL in your browser. We'll ignore references to this pesky file in this lab.)

By looking at the information in the HTTP GET and response messages, answer the following questions. When answering these questions, you should print out the GET and response messages (you can use the "Print Screen" button to copy the messages) and indicate where in the message you found the information that answers the following Questions:

1. (1pt) Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
2. (0.5pts) What languages (if any) does your browser indicate that it can accept to the server?
3. (1 pt) What is the IP address of your computer? Of the gaia.cs.umass.edu server?
4. (0.5pt) What is the status code returned from the server to your browser?
5. (0.5pt) When was the HTML file that you are retrieving last modified at the server?
6. (0.5pt) How many bytes of content are being returned to your browser?

In your answer to question 5 above, you might have been surprised to find that the document you just retrieved was last modified within a minute before you downloaded the document. That's because (for this particular file), the gaia.cs.umass.edu server is setting the file's last-modified time to be the current time, and is doing so once per minute. Thus, if you wait a minute between accesses, the file will appear to have been recently modified, and hence your browser will download a "new" copy of the document.



## 2. The HTTP CONDITIONAL GET/response interaction

Recall from Section 2.2.6 of the text, that 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 Netscape 7.0, select *Edit->Preferences->Advanced->Cache* and clear the memory and disk cache. For 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; see footnote 4. This trace file was gathered while performing the steps above on one of the author's computers.)

Answer the following Questions:

7. (0.5pts) 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. (1pt) Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
9. (0.5pts) 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. (1pt) 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.

## 3. Retrieving Long Documents

In our examples thus far, the documents retrieved have been simple and short HTML files. Let's next see what happens when we download a long HTML file. 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-file3.html>  
Your browser should display the rather 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.

(Note: If you are unable to run Wireshark on a live network connection, you can use the http-ethereal-trace-3 packet trace to answer the questions below; see footnote 4. This trace file was gathered while performing the steps above on one of the author's computers.)

In the packet-listing window, you should see your HTTP GET message, followed by a multiple-packet response to your HTTP GET request. This multiple-packet response deserves a bit of explanation. Recall from Section 2.2 (see Figure 2.9 in the text) that the HTTP response message consists of a status line, followed by header lines, followed by a blank line, followed by the entity body. In the case of our HTTP GET, the entity body in the response is the entire requested HTML file.

In our case here, the HTML file is rather long, and at 4500 bytes is too large to fit in one TCP packet. The single HTTP response message is thus broken into several pieces by TCP, with each piece being contained within a separate TCP segment (see Figure 1.20 in the text). Each TCP segment is recorded as a separate packet by Wireshark, and the fact that the single HTTP response was fragmented across multiple TCP packets is indicated by the “Continuation” phrase displayed by Wireshark. We stress here that there is no “Continuation” message in HTTP!

Answer the following Questions:

- 11.**(0.5pts) How many HTTP GET request messages were sent by your browser?
- 12.**(0.5pts) How many data-containing TCP segments were needed to carry the single HTTP response?
- 13.**(0.5pts) What is the status code and phrase associated with the response to the HTTP GET request?
- 14.**(0.5pts) Are there any HTTP status lines in the transmitted data associated with a TCP-induced “Continuation”?

#### 4. HTML Documents with Embedded Objects

Now that we’ve seen how Wireshark displays the captured packet traffic for large HTML files, we can look at what happens when your browser downloads a file with embedded objects, i.e., a file that includes other objects (in the example below, image files) that are stored on another server(s).

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-file4.html>

Your browser should display a short HTML file with two images. These two images are referenced in the base HTML file. That is, the images themselves are not contained in the HTML; instead the URLs for the images are contained in the downloaded HTML file. As discussed in the textbook, your browser will have to retrieve these logos from the indicated web sites. Our publisher’s logo is retrieved from the www.aw-bc.com web site. The image of our book’s cover is stored at the manic.cs.umass.edu server.

- Stop Wireshark packet capture, and enter “http” in the display-filter-specification window, so that only captured HTTP messages will be displayed.

(Note: If you are unable to run Wireshark on a live network connection, you can use the http-ethereal-trace-4 packet trace to answer the questions below; see footnote 4. This trace file was gathered while performing the steps above on one of the author’s computers.)

Answer the following Questions:

- 15.**(1pt) How many HTTP GET request messages were sent by your browser? To which Internet addresses (IP addresses) were these GET requests sent?
- 16.**(0.5pt) Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

#### 5 HTTP Authentication

Finally, let’s try visiting a web site that is password-protected and examine the sequence of HTTP message exchanged for such a site. The URL

[http://gaia.cs.umass.edu/wireshark-labs/protected\\_pages/HTTP-wireshark-file5.html](http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html)

is password protected. The username is “wireshark-students” (without the quotes), and the password is “network” (again, without the quotes). So let’s access this “secure” password-protected site. Do the following:

Make sure your browser’s cache is cleared, as discussed above, and close down your browser. Then,

start up your browser

- Start up the Wireshark packet sniffer
  - Enter the following URL into your browser  
[http://gaia.cs.umass.edu/wireshark-labs/protected\\_pages/HTTP-wiresharkfile5.html](http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharkfile5.html)
  - Type the requested user name and password into the pop up box.
  - 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-5 packet trace to answer the questions below; see footnote 1. This trace file was gathered while performing the steps above on one of the author’s computers.)

Now let’s examine the Wireshark output. You might want to first read up on HTTP authentication by reviewing the easy-to-read material on “HTTP Access Authentication Framework” at [http://frontier.userland.com/stories/storyReader\\$2159](http://frontier.userland.com/stories/storyReader$2159)

Answer the following **Questions**:

- 17.**(0.5pts) What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?
- 18.**(0.5pts)When your browser’s sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

The username (wireshark-students) and password (network) that you entered are encoded in the string of characters (d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcm0=) following the “Authorization: Basic” header in the client’s HTTP GET message. While it may appear that your username and password are encrypted, they are simply encoded in a format known as Base64 format. The username and password are not encrypted! To see this, go to <http://base64-encoder-online.waraxe.us/> and enter the base64-encoded string **d2lyZXNoYXJrLXN0dWRlbnRz** and press decode. Voila! You have translated from Base64 encoding to ASCII encoding, and thus should see your username! To view the password, enter the remainder of the string **Om5ldHdvcm0=** and press decode. Since anyone can download a tool like Wireshark and sniff packets (not just their own) passing by their network adaptor, and anyone can translate from Base64 to ASCII (you just did it!), it should be clear to you that simple passwords on WWW sites are not secure unless additional measures are taken.

Fear not! As we will see in Chapter 8, there are ways to make WWW access more secure. However, we’ll clearly need something that goes beyond the basic HTTP authentication framework!

**Sample solution:** (60% for answering each question, and 40% for printing out the right packets)

## Part 1. Capturing and analyzing Ethernet frames

```
⊕ Frame 36 (873 bytes on wire, 873 bytes captured)
⊖ Ethernet II, Src: Wistron_c1:15:71 (00:16:d3:c1:15:71), Dst: All-HSRP-routers_0b (00:00:0c:07:ac:0b)
  ⊖ Destination: All-HSRP-routers_0b (00:00:0c:07:ac:0b)
    Address: All-HSRP-routers_0b (00:00:0c:07:ac:0b)
    ....0 .... = IG bit: Individual address (unicast)
    ....0 .... = LG bit: Globally unique address (factory default)
  ⊖ Source: Wistron_c1:15:71 (00:16:d3:c1:15:71)
    Address: Wistron_c1:15:71 (00:16:d3:c1:15:71)
    ....0 .... = IG bit: Individual address (unicast)
    ....0 .... = LG bit: Globally unique address (factory default)
  Type: IP (0x0800)
⊕ Internet Protocol, Src: 129.252.11.215 (129.252.11.215), Dst: 74.125.65.113 (74.125.65.113)
⊕ Transmission Control Protocol, Src Port: fji1c1-tep-b (1902), Dst Port: http (80), Seq: 1, Ack: 1, Len: 819
⊖ Hypertext Transfer Protocol
  ⊕ GET /complete/search?client=chrome&hl=en-US&q=http%3A%2F%2Fgaia.cs.umass.edu%2Fwireshark-labs%2FHTTP-ethe
    Host: clients1.google.com\r\n
    Connection: keep-alive\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/530.5 (KHTML, like Gecko) Chrome/.
    Accept-Encoding: gzip, deflate, sdch\r\n
    [truncated] Cookie: PREF=ID=2c9e21f6cd5626b6:U=ec4ed60f223a32fd:TM=1251857472:LM=1252613451:GM=1:IG=3:S=5
    Accept-Language: en-US,en;q=0.8\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3\r\n
    \r\n
```

**1. (0.2pt) What is the 48-bit Ethernet address of your computer?**

00:16:d3:c1:15:71

**2. What is the 48-bit destination address in the Ethernet frame?**

00:00:0c:07:ac:0b

**Is this the Ethernet address of `gaia.cs.umass.edu`? (Hint: the answer is *no*). What device has this as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong. Re-read pages 468-469 in the text and make sure you understand the answer here.]**

It is the router/gateway on this Ethernet.

**3. Give the hexadecimal value for the two-byte Frame type field. What do the bit(s) whose value is 1 mean within the flag field?**

0x0800. It means the payload is IP datagram

**4. (0.5pt) How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?**

55<sup>th</sup> byte is G, there are 54 bytes in front of ‘G’.