Wireshark Lab 1 - Intro

IT 520-A – Enterprise Infrastructure & Networks
Instruction: Scroll to the bottom of the page, for in-class deliverables.

In this first lab, you'll get acquainted with Wireshark, and make some simple packet captures and observations.

We will be using the Wireshark packet sniffer [http://www.wireshark.org/] for this and subsequent 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, Mac, and Linux/Unix computer. 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/), man pages (http://www.wireshark.org/docs/man-pages/), and a detailed FAQ (http://www.wireshark.org/faq.html), rich functionality that includes the capability to analyze hundreds of protocols, and a well-designed user interface. It operates in computers using Ethernet, serial (PPP and SLIP), 802.11 wireless LANs, and many other link-layer technologies (if the OS on which it's running allows Wireshark to do so).

Getting and Installing Wireshark

In order to run Wireshark, you will need to have access to a computer that supports both Wireshark and the *libpcap* or *WinPCap* packet capture library. The *libpcap* software will be installed for you, if it is not installed within your operating system, when you install Wireshark. 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. The Wireshark FAQ has a number of helpful hints and interesting tidbits of information, particularly if you have trouble installing or running Wireshark.

Hint: There are a lot of videos on YouTube showing how to install Wireshark.

Running Wireshark

When you run the Wireshark program, you'll get a startup screen that looks something like the Figure 1 below. Different versions of Wireshark will have different startup screens – so don't panic if yours doesn't look exactly like the screen below! Wireshark runs on many different platforms with many different window managers, different styles applied and

there are different versions of the underlying GUI toolkit used, your screen might look different from the provided screenshots. But as there are no real differences in functionality, these screenshots should still be well understandable.
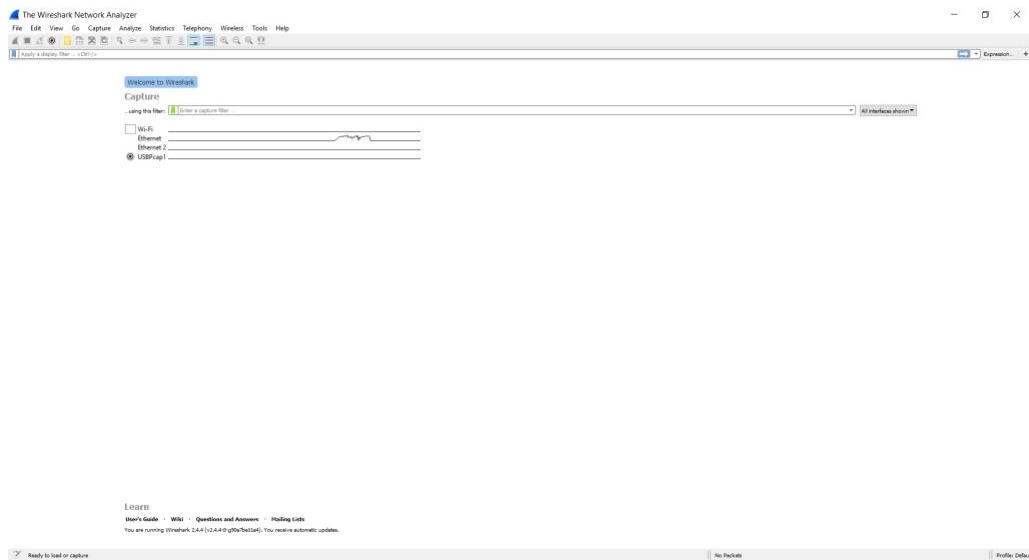

Figure 1: Initial Wireshark Screen

There's not much interesting on this screen. But note that under the Capture section, there is a list of so-called interfaces. The computer we're taking these screenshots from has three real interfaces – "Wi-Fi, Ethernet and Ethernet 2". Yours might look different. Wi-Fi is the interface for Wi-Fi access. Ethernet and Ethernet 2 are the interface for Ethernet ports. All packets to/from this computer will pass through either the Wi-Fi or Ethernet interface, so it's here where we want to capture packets. Double click the interface through which you are getting Internet connectivity.

If you are getting internet access via wireless then select WiFi. If via cable, select Ethernet.

Let's take Wireshark out for a spin! If you click on your connected interface to start packet capture (i.e., for Wireshark to begin capturing all packets being sent to/from that interface), a screen like Figure 2 will be displayed, showing information about the packets being captured. Once you start packet capture, you can stop it by using the stop option on the menu.
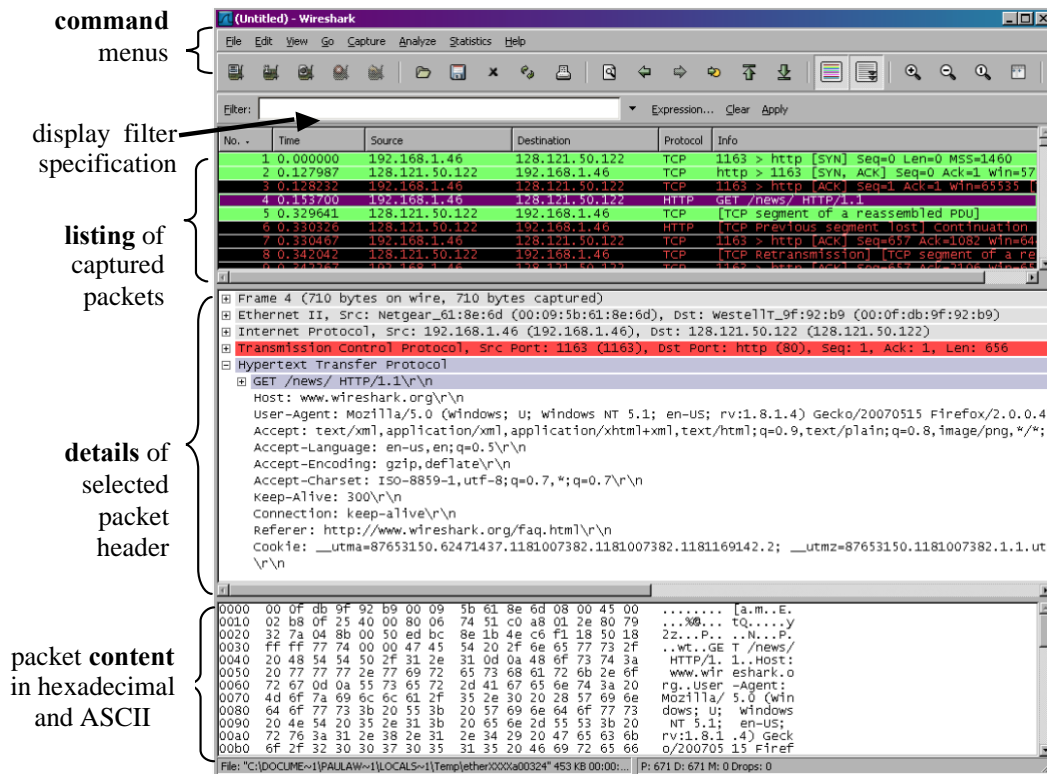
command
menus

display filter
specification

listing of
captured
packets

details of
selected
packet
header

packet content
in hexadecimal
and ASCII

Figure 2: Wireshark Graphical User Interface, during packet capture and analysis

This looks more interesting! 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 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. (Don't worry, same steps apply to Wireless connection). Close the Wireshark application, and all your browsers before starting 1 below:

1. Start up your favorite web browser, which will display your selected homepage.

2. Start up the Wireshark software. You will initially see a window like that shown in Figure 1. Wireshark has not yet begun capturing packets.

3. Double click on your interface to start capturing packets. Wireshark is now capturing all packets being sent/received from/by your computer! Your screen should look like figure 3 below. You can always stop by selecting "Stop capturing packets" from the menu. But don't stop packet capture yet. Let's capture some interesting packets first. To do so, we'll need to generate some network traffic. Let's do so using a web browser, which will use the HTTP protocol that we will study in detail in class to download content from a website.
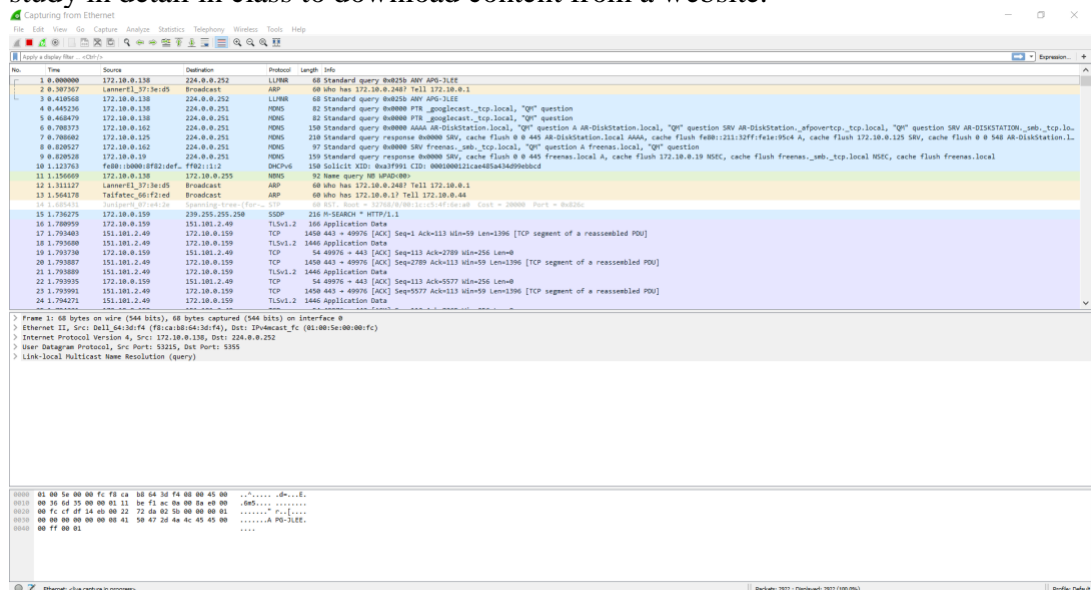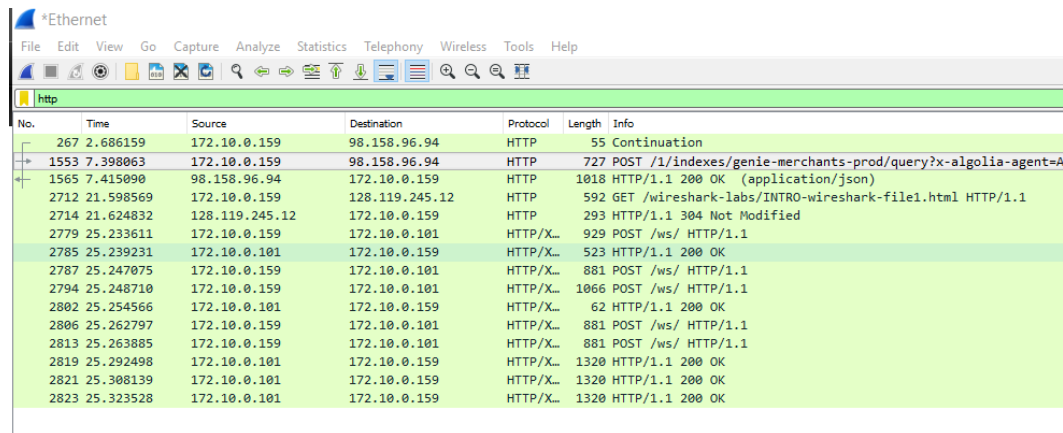

Figure 3: Wireshark Capture

4. 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.

5. After your browser has displayed the INTRO-wireshark-file1.html page (it is a simple one line of congratulations), stop Wireshark packet capture by selecting stop in the Wireshark capture window. The main Wireshark window should now look similar to Figure 3.

6. 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 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 3). 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"!

7. 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 like figure 4 below:

Figure 4: Wireshark HTTP Filter.

8. Find the HTTP GET message that was sent from your computer to the gaia.cs.umass.edu HTTP server. (Look for an HTTP GET message in the "listing of captured packets" portion of the Wireshark window (see Figure 4 – the 4th among the list) that shows "GET" followed by the gaia.cs.umass.edu URL that you entered. 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[1]. By clicking on '+' and '-' right-pointing and down-pointing arrowheads 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.
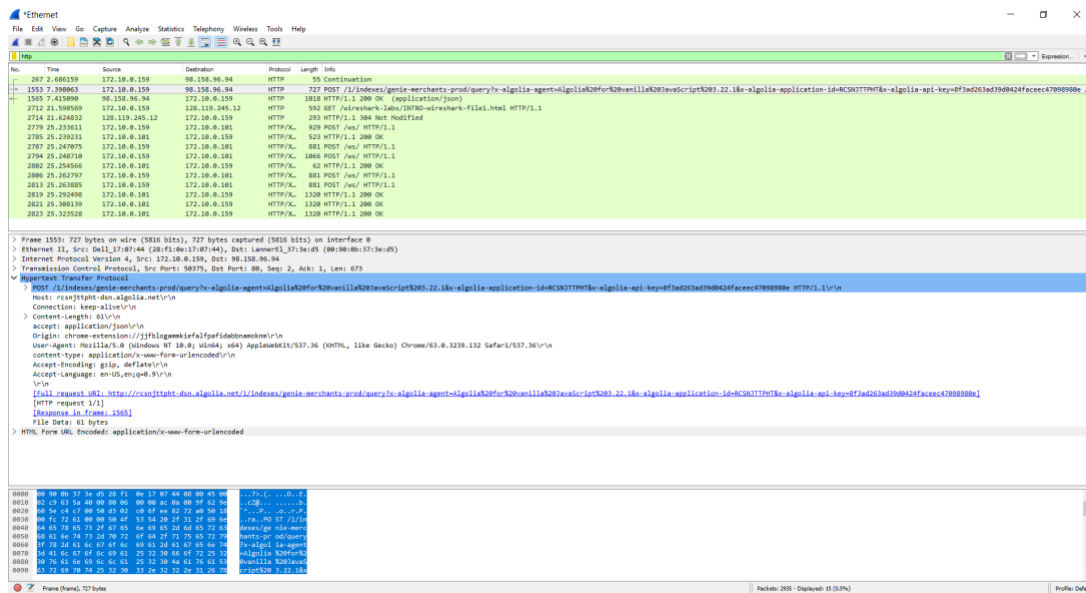
9. Save the file and Exit Wireshark

Figure 5: Wireshark window after step 8

Class deliverable in the next page!!!

What to hand in

For each of these question, take a screen shot and add attach it to your answer. Also, save your Wireshark lab file. We would use it later in the class.

The goal of this first 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. Answer the following questions, based on your Wireshark experimentation:

- (*For each of these questions, take a screenshot of Wireshark, and attach it to your answer*) - Questions without Full Screenshot will not be graded. A lab submission template is available on canvas. Your screenshot should indicate the time and date on your computer.
- Include a terminal screenshot showing computer IP address on the front page before Question 1, and a full PRINT of the HTTP OK message as the last page.

Labs will NOT be graded if either of these two is missing.

Questions:

1. What is the Internet address of your computer?
2. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.
3. 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*.)
4. What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)?
5. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select *Print* from the Wireshark *File* command menu, and select the "*Selected Packet Only*" and *"Print as displayed"* radial buttons, and then click OK.

Don't forget to save your Wireshark Lab file.