WORKING WITH WIRESHARK

Student Handout

Duration: 1 hour

Objectives:

At the end of this lab students will be able to:

a) Set up wireshark
b) Capture packets using wireshark
c) Observe packet headers and details via wireshark
d) Calculate delay

Summary:

Wireshark is a network packet analyzer also called a packet sniffer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible.

You could think of a network packet analyzer as a measuring device used to examine what's going on inside a network cable, just like a voltmeter is used by an electrician to examine what's going on inside an electric cable (but at a higher level, of course).

In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, all that has changed. Wireshark is perhaps one of the best open source packet analyzers available today.

Here are some examples people use Wireshark for:

- network administrators use it to troubleshoot network problems
- network security engineers use it to examine security problems
- developers use it to debug protocol implementations
- people use it to learn network protocol internals

In this first Wireshark lab, you'll obtain and install a copy of Wireshark, access a Web site, and capture and examine the protocol messages being exchanged between your Web browser and the Web server.

Procedure

Part (a): Setting up Wireshark

1. For installation in your home computer, download Wireshark 1.10.7 from their main site to suit your OS specifications. http://www.wireshark.org/download.html
2. Once download run the installation file. During the installation you will be prompted to install WinPCap, click Yes to install this. WinPCap is necessary for Wireshark to work.

WinPcap is software that allows your network interface card to (NIC) operate in "promiscuous" mode. Normally if a NIC sees traffic addressed to another NIC on the network, it ignores it. If you are running a network sniffer application, you may have a need to capture that traffic for inspection. Putting a NIC in promiscuous mode allows your NIC to capture traffic addressed to another machine and pass it to the sniffer application.

3. Once all installations are done, you can now use Wireshark. Refer to Figure 1 and Figure 2 of the Appendix for a general layout of the Wireshark application.

Part (b): Capture packets using Wireshark

1. Now you will begin capturing packets. Choose the required interface, in this lab you will choose Ethernet, then press Start. This will begin a capture session
2. Observe packets being captured.
3. Next, open your browser and go to wireshark.org
4. Switch back to Wireshark and observe the packets being captured.

Part (c): Observe packet details

1. Now you will go further into observing the packet details.
2. To observe the conversation between your PC and wireshark.org
3. Click on capture as shown in Figure 3.
4. To view the entire conversation between your PC and wireshark.org. Right click on a captured packet -> Follow TCP Stream. Refer to Figure 4.

Part (d): Calculate delay

Consider a packet of length 100 bytes which begins at source host A and travels over two link to a destination host B. The links have a propagation speed of 2.8 x 10^8 m/s, a transmission rate of 1 Mbps in Link 1 and 2 Mbps in Link 2. Link 1 is 1000m and Link 2 is 200 km. What is the total end-to-end delay for the packet?

Appendix

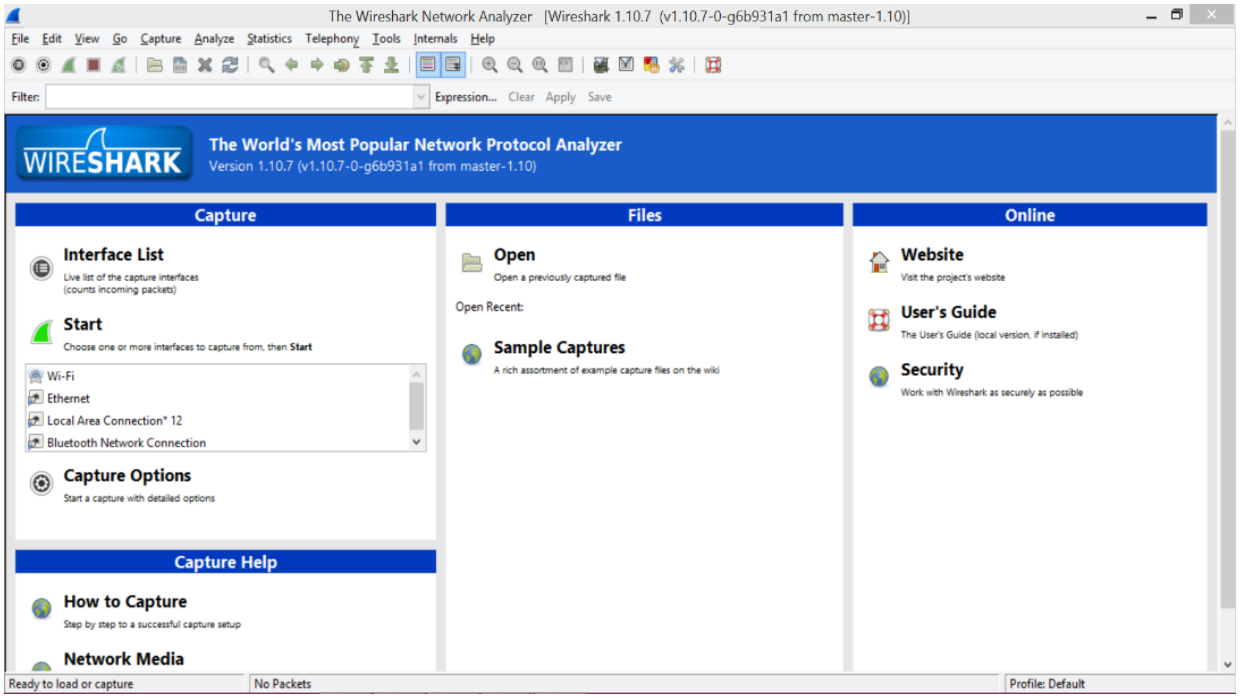

Figure 1 showing startup screen of Wireshark

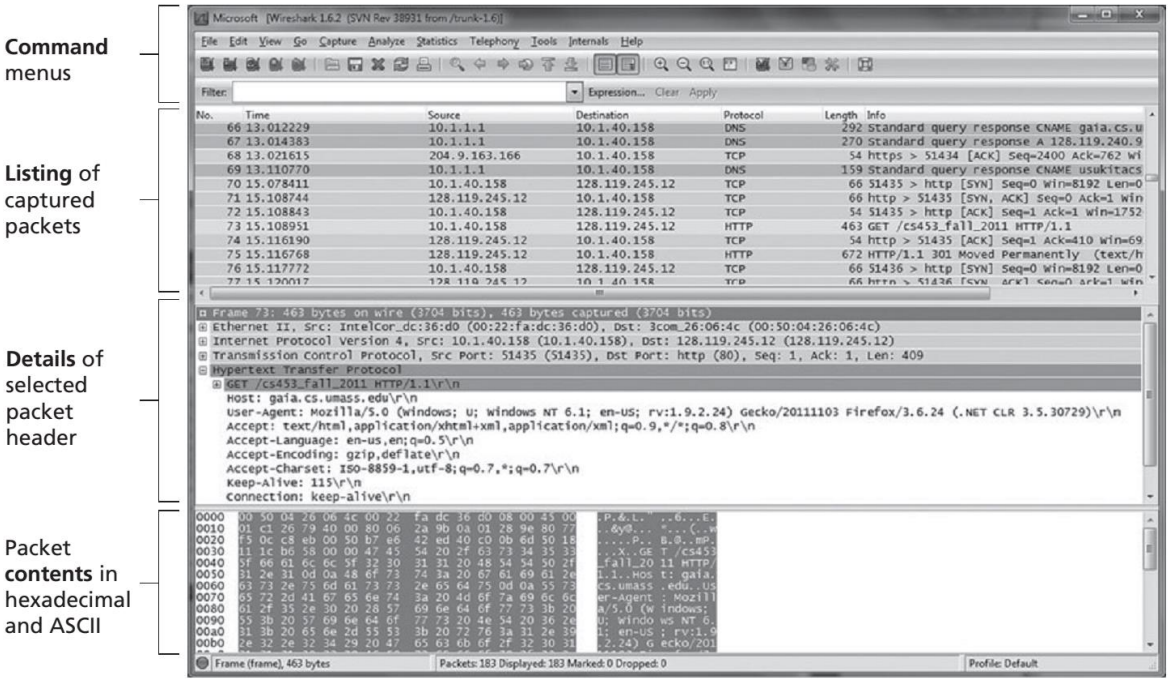

Figure 2 showing screenshot of Wireshark application

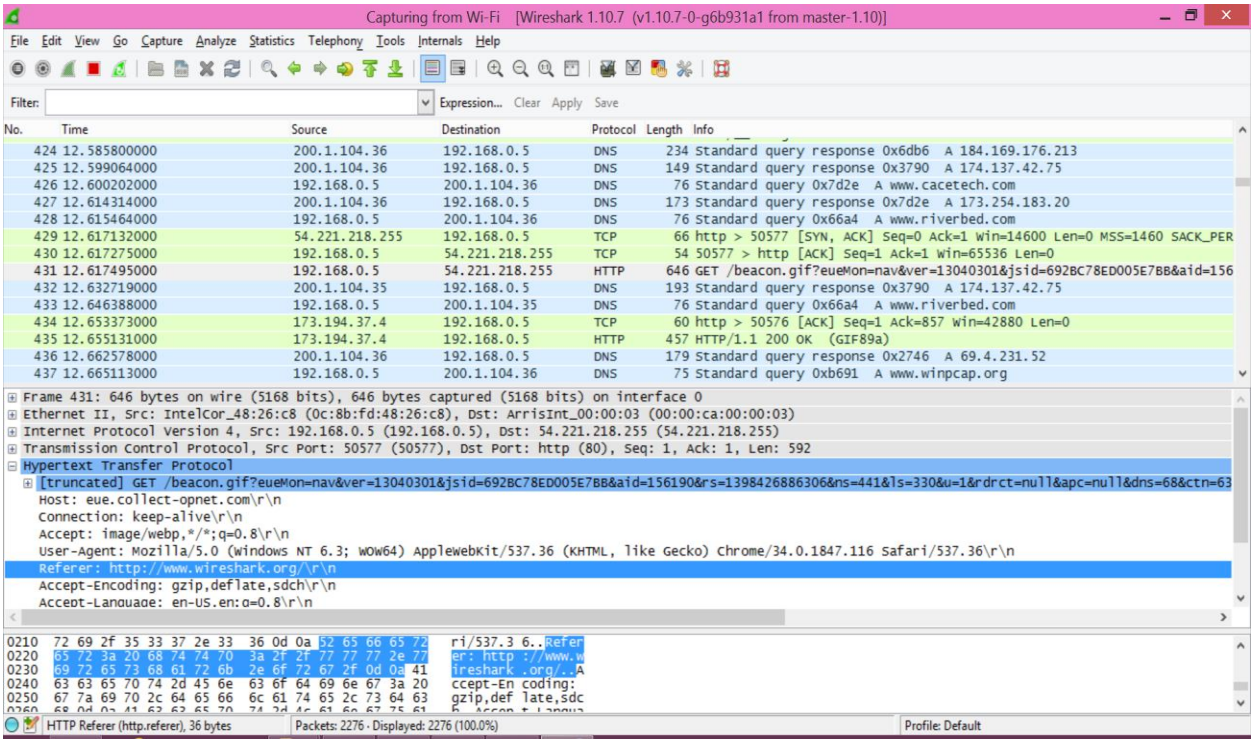

Figure 3 showing selection of HTTP packet

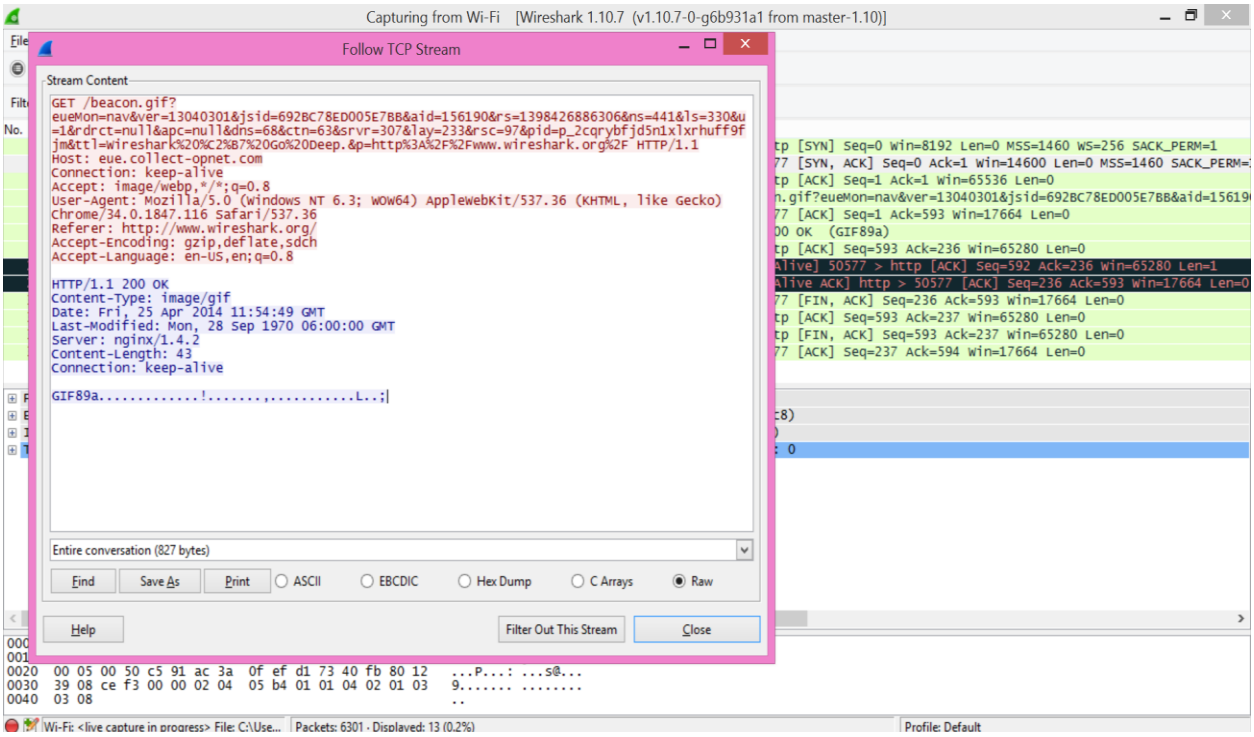

Figure 4 showing conversation between PC and wireshark.org