

# Packet Analysis- Wireshark

## A Practical Exercise

Name: \_\_\_\_\_

---

- I. Equipment:** Laptop w/ Wireshark program, wireless NIC, and PE20dumpfile located on syllabus webpage.
- II. Wireshark.** The key to network management is to understand what is being sent across a network and how the individual devices on a network are communicating with each other. The easiest way to do this is to capture a snapshot of all packets moving through the network for a period of time and analyze them. *Wireshark* is a tool that will capture and decode packets. Wireshark uses the NIC as a sort of video camera, taking pictures of every packet that passes by on the network and saving these images to a local file, called a “dump file” or “capture.” After the initial period of capturing the dump, Wireshark analyzes each packet, determines its protocol type, and displays its contents in a readable form.
- III. Using Wireshark to Examine a Previous Capture.** In this section you will use Wireshark in its analysis capabilities to examine a previously captured dump file. Special attention will be focused on the types of protocols used and the contents of certain individual packets.
- a. Download the file “Wireshark\_dumpfile” from EE302 website onto your Desktop
  - b. Double click on the “Wireshark” icon on the Desktop
  - c. Once open, Wireshark should appear, with blank view fields and a message at the bottom reading “Ready to load or capture”
  - d. Click “File’ →”Open...” → And open “Wireshark\_dumpfile” on your Desktop. After several seconds of processing the file, the view fields should contain a list of source and destination and source IP addresses, protocol names, and information about each packet.
  - e. Click on the column title “Protocol” to sort the captured packets by protocol type. The first listed packet should be No. 184 and will have a destination of “Broadcast.” What is Broadcast and what does it mean?  
\_\_\_\_\_  
\_\_\_\_\_
  - f. The first protocol group listed is “ARP.” ARP stands for “Address Resolution Protocol. This is the protocol used to connect the assignment of an IP address to the physical address of the NIC (MAC address). Click on packet No.430 .
    - i. What is the Source MAC address? \_\_\_\_\_
    - ii. What IP is the packet looking for? \_\_\_\_\_
  - g. Scroll down the packet listing window until packets using the “DNS” protocol are viewable. DNS stands for “Domain Name Server.” This protocol is used to make a request to a DNS for the numeric IP address associated with the name of a host or network, an example would be [www.espn.com](http://www.espn.com) or [www.google.com](http://www.google.com).

- h. Click on packet No.13 . The computer with the source IP of 131.122.194.2 is requesting the IP address of a host from the DNS Server (131.122.220.1). Under "Info" you can see "Standard Query A www.weather.com" This is what is being asked of the DNS by the source IP. The bottom window in Wireshark contains the actual contents of the selected packet, in both hexadecimal and ASCII text. Can you find [www.weather.com](http://www.weather.com) in the actual contents of the packet? \_\_\_\_\_
- i. Click on packet No.14 . Note this is the next packet captured and is from the DNS back to 131.122.194.2. What do you think this packet will contain?  
\_\_\_\_\_
- j. Note the IP contained in packet 421's "Info." Minimize Wireshark and open Internet Explorer. Enter the noted IP into Internet Explorer and press enter. What website are you taken to?  
\_\_\_\_\_
- k. How many sites were visited in this capture session, use the HTTP protocol to show them and pick out the recognizable ones and list them here. \_\_\_\_\_  
\_\_\_\_\_

**IV. Using Wireshark as a Real-Time Capture/Monitoring Application.** We will now use Wireshark to capture images of packets from the network in real-time and examine what traffic is being originated from systems on the network and what the traffic contains.

- a. Click "File"→"Close" to close the previously captured dump file. Click "Capture"→"Interfaces" then choose an active interface ( Carts A-D ( Dell Wireless), Carts 5-8 ( Netgear HA501 Wireless Adapter or Linksys Dual Band), and Carts 9-10 ( Intel/Pro). You should see packet activity.
- b. Click on "Details" to view the Characteristics of your interface and the MAC address. \_\_\_\_\_
- c. Click on "Options" write down your IP address. \_\_\_\_\_
- d. Make sure that the Packet Limit is not selected.
- e. Make sure to select Stop Capture, and enter in 1 minute.
- f. Make sure that MAC Name Resolution is selected.
- g. Make sure that Network Name Resolution is selected.
- h. All other fields should be left in the default mode.
- i. Click "Start", open internet explorer and go to [www.tlca.org](http://www.tlca.org). Let it finish loading then go to [www.cnn.com](http://www.cnn.com) and let it finish loading. Observe the number of packets captured by Wireshark progressing. Wireshark is using the laptop's NIC like a video camera recording everything that goes by.
- j. If the Wireshark capture window is still open, click "Stop."
- k. Wireshark will analyze and sort the captured packets and return you to the main Wireshark window. Notice the large number of packets captured in that short amount of time.

- l. Click on “Protocol” to sort the captured packets by protocol, and scroll to the HTTP group of packets. Note the large number of HTTP packets. If you only went to two websites why aren’t there only a few packets for each page? (Hint: How much data can each packet contain?)
- 
- 

- m. Look through the DNS section of packets and see if you can find the requests for the two websites you visited.

- V. Further Exploration. There are a multitude of protocols employed on institutional networks, including the Naval Academy Data Network. Here are a list of the most commonly used Protocols and their purpose, some of these protocols were seen in the captures during this PE.
- a. AIM: AOL Instant Messenger Protocol. Uses plain text as transport language, for messages, as well as passwords and other sensitive information.
  - b. ARP: Address Resolution Protocol. Used to pair IP addresses with MAC addresses.
  - c. DHCP: Dynamic Host Configuration Protocol, used to request IP addresses for a host system from a central (DHCP) server
  - d. HTTP: Hypertext Transfer Protocol. These are the rules used for exchanging text, images, multimedia, etc on the World Wide Web (WWW).
  - e. TCP: Transmission Control Protocol. TCP keeps track of the individual packets that data is divided into for transmission through the Internet.

VI. Questions.

- a. Could *Wireshark* be employed on a network to determine if someone was trying to communicate with a system that they were not supposed to have access to? How?

- b. With *Wireshark*, How could one determine which users and protocols require the most bandwidth?

- VII. What is the IP of www.usna.edu?