Lab 8.3.2 Conducting a Network Capture with Wireshark

Objectives

- Perform a network traffic capture with Wireshark to become familiar with the Wireshark interface and environment.
- Analyze traffic to a web server
- Create a filter to limit the network capture to ICMP packets.
- Ping a remote host to observe how the ICMP packet filter operates during the network capture.

Background / Preparation

In this lab, you will install Wireshark, a well-known network protocol analyzer and monitoring tool. Wireshark captures all packets sent or received by the computer NIC. It can be installed either in the lab or on a PC at home. You will use it to trace and view various types of network protocols and traffic. Wireshark was formerly known as Ethereal.

Wireshark software is freeware and is available from www.wireshark.org. The software installer, wireshark-setup-0.99.5.exe, should be available on the local Networking Academy server.

You can perform this lab individually, in pairs, or in teams.

The following resources are required:

- A Windows XP-based PC with an Ethernet network and at least two hosts
- Wireshark Version 0.99.5 software (or most current version)
- Internet connectivity (optional but desirable)
- Access to the PC command prompt
- Access to PC network TCP/IP configuration
Step 1: Install and launch Wireshark

If Wireshark has been loaded on the PC previously, go to the Wireshark program folder Start > All Programs > Wireshark > Wireshark and click the application icon.

If Wireshark has not been installed, follow these steps:

a. Given the local network path to the Wireshark software installer, wireshark-setup-0.99.5.exe, download the installer to the PC desktop.

b. Double-click the installer and follow the installation prompts, accepting the defaults.
1) **Click I Agree.**

![Wireshark 0.99.5 Setup]

**License Agreement**
Please review the license terms before installing Wireshark 0.99.5.

Press Page Down to see the rest of the agreement.

**GNU GENERAL PUBLIC LICENSE**
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
Everyone is permitted to copy and distribute verbatim copies of
this license document, but changing it is not allowed.

Preamble
The licenses for most software are designed to take away your
freedom to share and change it. Wireshark, being open source
software, is most erect about preserving user freedom. It is
licensed under the terms of the GNU General Public License.

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Wireshark 0.99.5.

![Nullsoft: Install System v2.17]

2) **Make sure to install WinPcap on the PC.** WinPcap includes a driver to support packet capture. Wireshark uses this library to capture live network data with Windows.

![Wireshark 0.99.5 Setup]

**Install WinPcap?**
WinPcap is required to capture live network data. Should WinPcap be installed?

- Currently installed WinPcap version
  WinPcap 4.0

- **Install**
  - **✔** Install WinPcap 4.0
    - If selected, the currently installed WinPcap 4.0 will be uninstalled first.

- **Services**
  - **☐** Start WinPcap service "NPF" at startup
    - (so users without Administrator privileges can capture)

- What is WinPcap?

![Nullsoft: Install System v2.17]
c. Click **Install** and follow the remaining prompts to the end of the installation process.

d. After the software is installed, click the checkbox to launch Wireshark.

**Step 2: Select an interface to use for capturing packets**

a. Start the Wireshark application.

b. From the **Capture** menu, click **Interfaces**.

![Wireshark Network Analyzer](image)

3) Click the **Start** button for the Ethernet interface (NIC) that you want to use to capture network traffic.

![Wireshark Capture Interfaces](image)

**Step 3: Start a network capture**

a. Scroll through the menus and view the toolbar on the Wireshark startup Interface.

b. Click the **New Live Capture** button and observe the information gathered by Wireshark. Allow the capture to continue for a few minutes so that you can observe the different types of traffic on the network.

![Wireshark Network Analyzer](image)
Step 4: Analyze Web traffic information (optional)

a. If Internet connectivity is available, open a browser and go to www.google.com. Minimize the Google window and return to Wireshark. You should see captured traffic similar to that shown below. Locate the Source, Destination, and Protocol columns on the Wireshark display screen.

```
4) The connection to the Google server will start with a query to the DNS server to look up the server IP address. The destination server IP address will most likely start with 64.x.x.x. What is the source and destination of the first packet sent to the Google server?

b. Open another browser window and go to the ARIN Whois database http://www.arin.net/whois/ or use another whois lookup tool and enter the IP address of the destination server. To what organization is this IP address assigned?

c. What are the protocols used to establish the connection to the web server and deliver the web page to your local host?

d. What is the color used to highlight the traffic between your host and the Google web server?

Step 5: Filter a network capture

a. Open a command prompt window by clicking Start > All Programs > Run and typing cmd. Alternatively, click Start > All Programs > Accessories and select Command Prompt.

b. Ping a host IP address on your local network and observe the Wireshark capture window. Scroll up and down the window in which the traffic is displayed. What types of protocols are in use?
c. In the Filter text box, type icmp and click Apply. Internet Control Message Protocol (ICMP) is the protocol that ping uses to test network connectivity to another host.

d. When icmp is typed in the Filter text box, what kind of traffic is was displayed?

_______________________________________________________________________________

e. Click the Filter: Expression button on the Wireshark window. Scroll down the list and view the filter possibilities there. Are TCP, HTTP, ARP and other protocols listed? 

Step 6: Reflection

a. There are hundreds of filters listed in the Filter: Expression option. It may be possible that, in a large network, there would be enormous amounts and many different types of traffic. Which three filters in the long list do you think might be most useful to a network administrator?

_______________________________________________________________________________

b. Is Wireshark a tool for out-of-band or in-band network monitoring? ______________ Explain your answer.

_______________________________________________________________________________