CIT 223: Data Communication and Computer Network Lab
Assignment #04
Introduction to WireShark

Anup Adhikari
anup.adhikari@gandakiuniversity.edu.np
Gandaki University

Published Date: June 4, 2024, Deadline Date: **June 11, 2024**

1 Introduction

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.

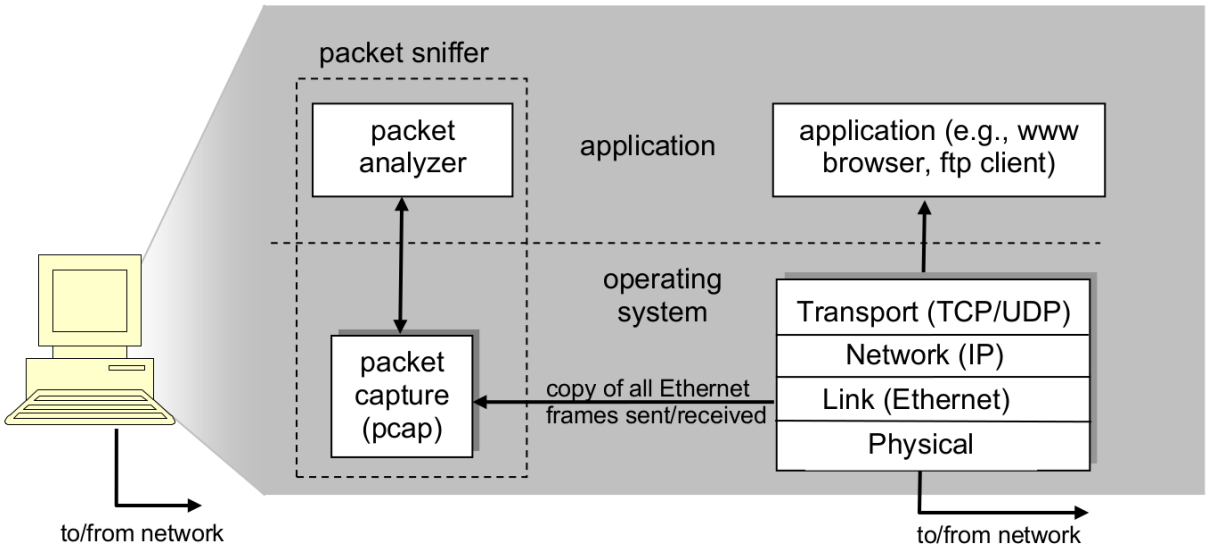

Figure 1: Packet Sniffer Structure

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 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.

2 Objectives

The objectives of the lab are:

1. to look into encapsulation at different layers using WireShark.

3 Instructions

1. Download and install Wireshark software from `http://www.wireshark.org/download.html`.
2. Open Wireshark

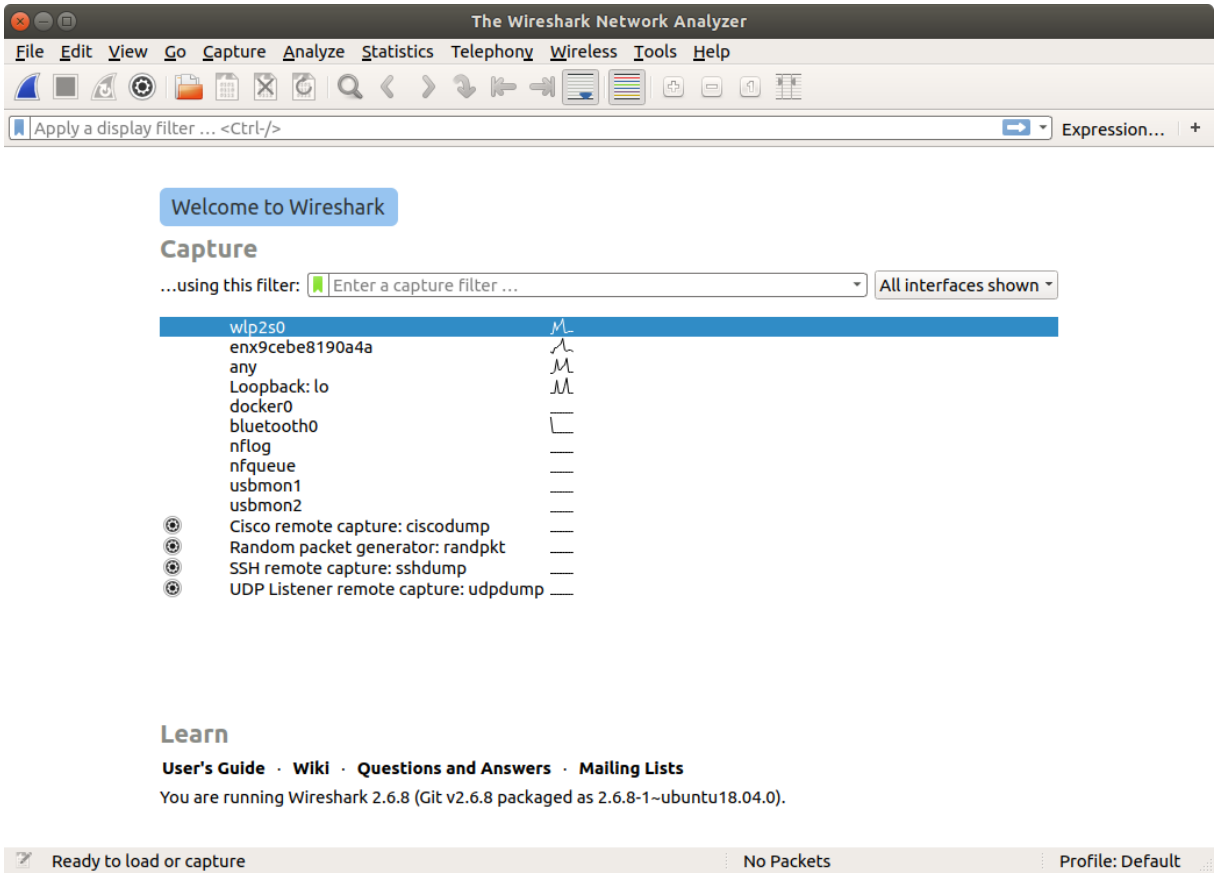

Figure 2: Initial Wireshark Screen

3. Note that under the Capture section, there is a list of so-called interfaces.
4. Click on the interfaces to view the packets being sent received by the network host.

5. Now analyze different packets. See Figure 3

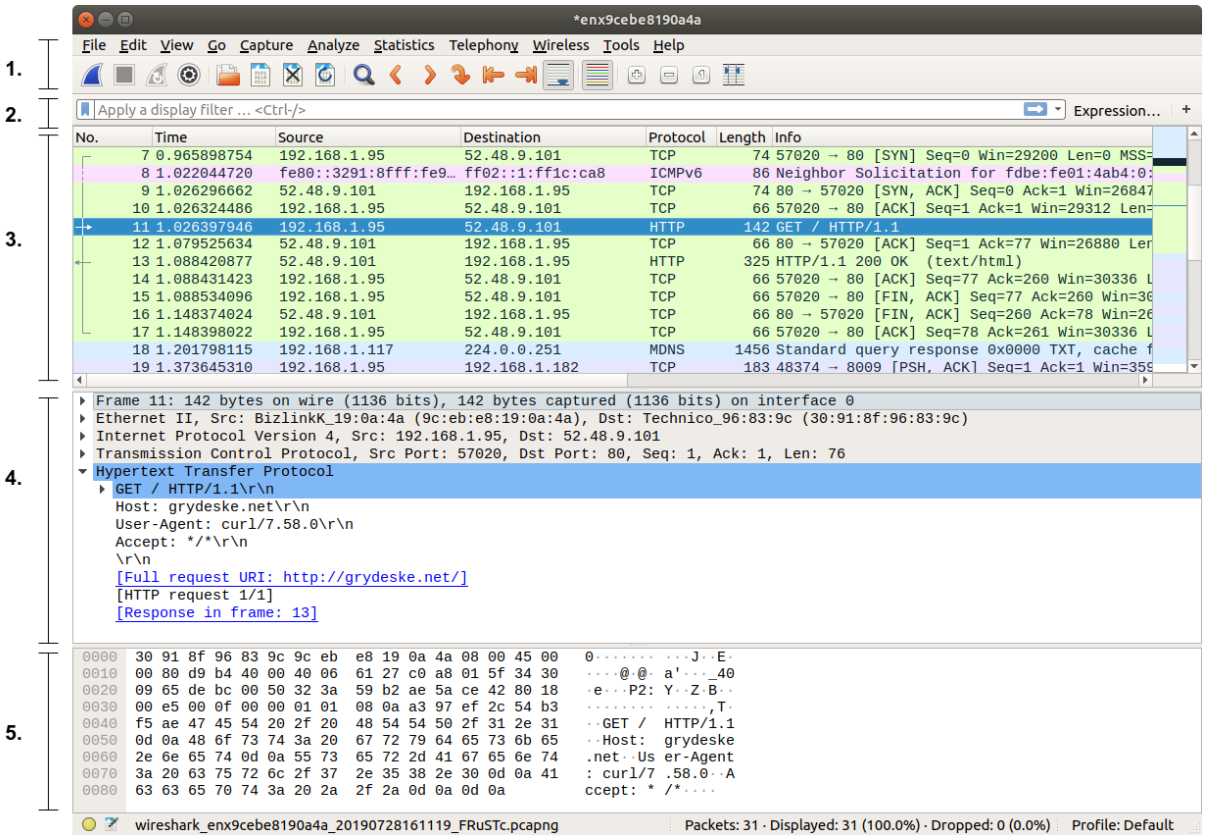

Figure 3: Capture and Analysis

4 Lab Tasks

Question 1

Complete all the exercises from `https://imada.sdu.dk/u/jamik/dm557-19/wireshark/wireshark-intro.html`.

Question 2

Write a socket client program using UDP in one computer and another socket server program using UDP in other computer. Observe the packets in Wireshark.

Question 3

Write a socket client program using TCP in one computer and another socket server program using TCP in other computer. Observe the packets in Wireshark.