Bahria University
Discovering Knowledge

Department of Computer Science

CEL222: Computer Networks

Class: BSCS-4CD

CLO1: Understand the fundamental Building blocks of Computer Networks i.e., Layered approach and protocols that make networking possible

Lab 1: General Introduction to Wireshark and Networking

Time: 11:30 to 02:30

Date: 21,23-02-2023

Lab Instructor: Ms. Nadia Kalsoom

Lab 1: General introduction to Wireshark and Networking

Introduction

The basic purpose of this lab is to introduce you to Wireshark, a popular protocol analyzer. By the end of this lab you will be familiar to its environment and will know how to capture and interactively browse the traffic running on a computer network using it.

Objective

The objective of this lab is to understand basics of Wireshark and Networks.

Tools/Software Requirements

Wireshark

Important Instructions

- Read carefully before starting the lab.
- These exercises are to be done individually.
- You are supposed to provide the answers to the questions listed end of this document and upload this completed document to your course's LMS site.

Description

Introduction to Networking:

A **computer network**, often simply referred to as a network, is a collection of hardware components and computers interconnected by communication channels that allow sharing of resources and information. In the world of computers, networking is the practice of linking two or more computing devices together for the purpose of sharing data. In networking, the communication language used by computer devices is called the protocol. Yet another way to classify computer networks is by the set of protocols they support. Networks often implement multiple protocols to support specific applications.

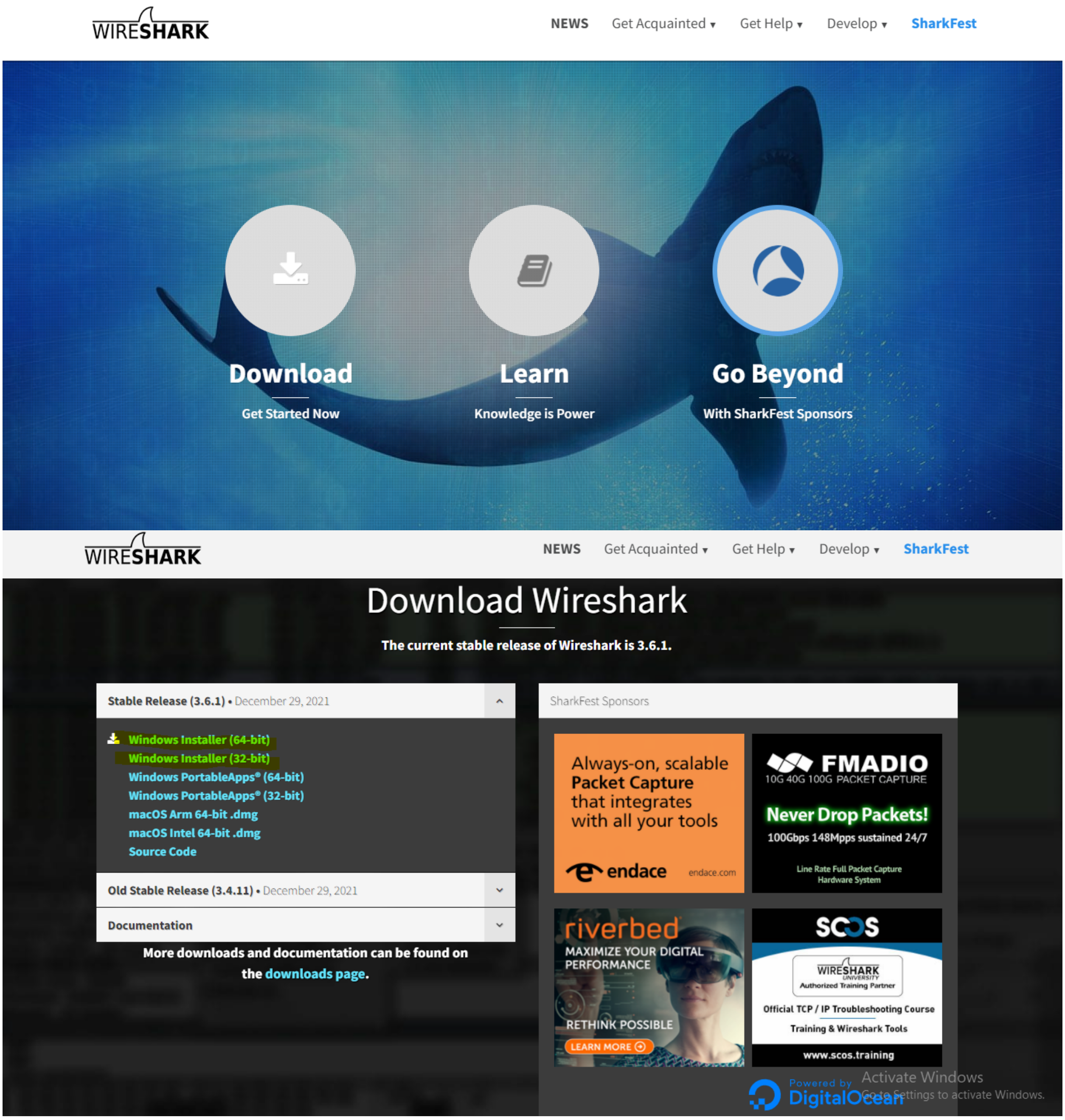
1. **What is a protocol analyzer?**
   Protocol analyzers capture conversations between two or more systems or devices. A protocol analyzer not only captures the traffic, it also decodes (interprets) the traffic. Decoding allows you to view the conversation in English, as opposed to binary language. A sophisticated protocol analyzer will also provide statistics and trend information on the captured traffic. Protocol analyzers provide information about the traffic flow on your local area network (LAN), from which you can view device-specific information.
2. **Introduction to Wireshark**

   Wireshark is a free and open-source packet analyzer, used for network troubleshooting, analysis, software and communications protocol development, and education.

Getting Wireshark

Download and install the Wireshark software:

- Go to http://www.wireshark.org/download.html and download and install the Wireshark binary for your computer. Wireshark can be installed on both Windows and Linux. See the documentation page of Wireshark for more details.



Download Wireshark

The current stable release of Wireshark is 3.6.1.

Stable Release (3.6.1) • December 29, 2021

- Windows Installer (64-bit)
- Windows Installer (32-bit)
- Windows PortableApps® (64-bit)
- Windows PortableApps® (32-bit)
- macOS Arm 64-bit .dmg
- macOS Intel 64-bit .dmg
- Source Code

Old Stable Release (3.4.11) • December 29, 2021

Documentation

More downloads and documentation can be found on the downloads page.

SharkFest Sponsors

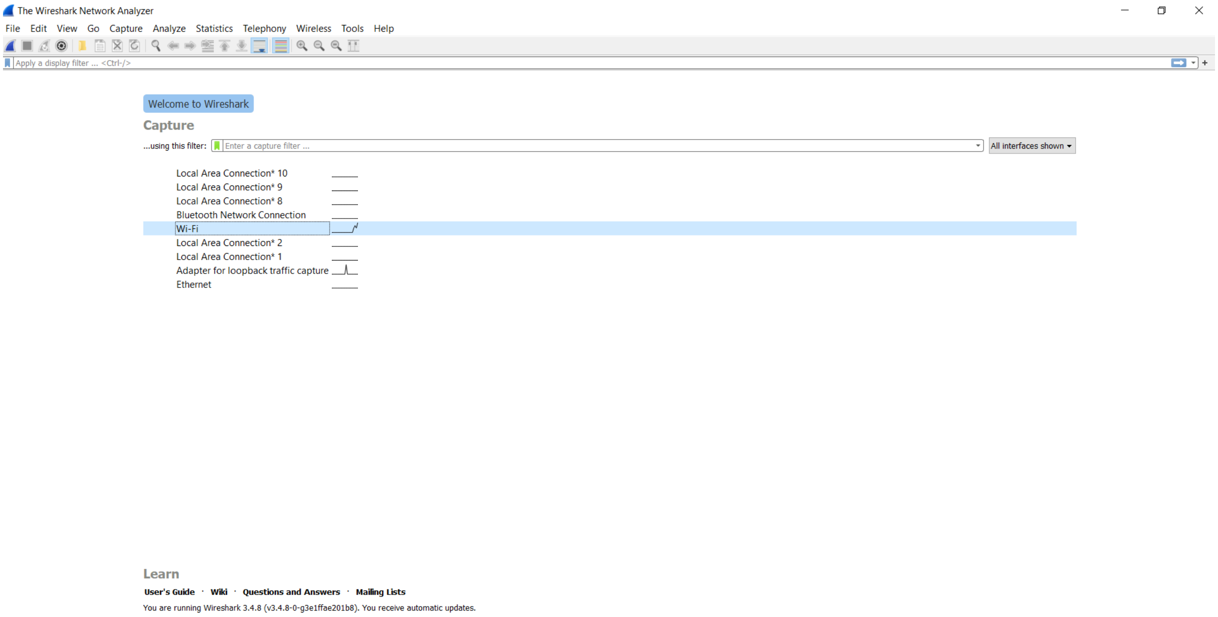
- Download the Wireshark user guide.

The Wireshark FAQ has a number of helpful hints and interesting tidbits of information, particularly if you have trouble installing or running Wireshark.

Running Wireshark

On Windows, you should be able to find the link by clicking on the Start option of the Windows taskbar and thereby finding the wireshark program in All Programs.

On Linux machines, wireshark can be run by typing "wireshark" at the command prompt (in case there is a problem with your path, type "which wireshark" that would show path /usr/bin/wireshark where wireshark is typically installed). When you run the Wireshark program, the Wireshark graphical user interface shown in below fig will be displayed. Initially, no data will be displayed in the various windows.



The Wireshark Network Analyzer

Apply a display filter ... <Ctrl-/>

Capture

...using this filter: Enter a capture filter ...

Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Bluetooth Network Connection
Wi-Fi
Local Area Connection* 2
Local Area Connection* 1
Adapter for loopback traffic capture
Ethernet

You are running Wireshark 3.4.8 (v3.4.8-0-g3e1ffae201b8). You receive automatic updates.

The Wireshark interface has five major components:

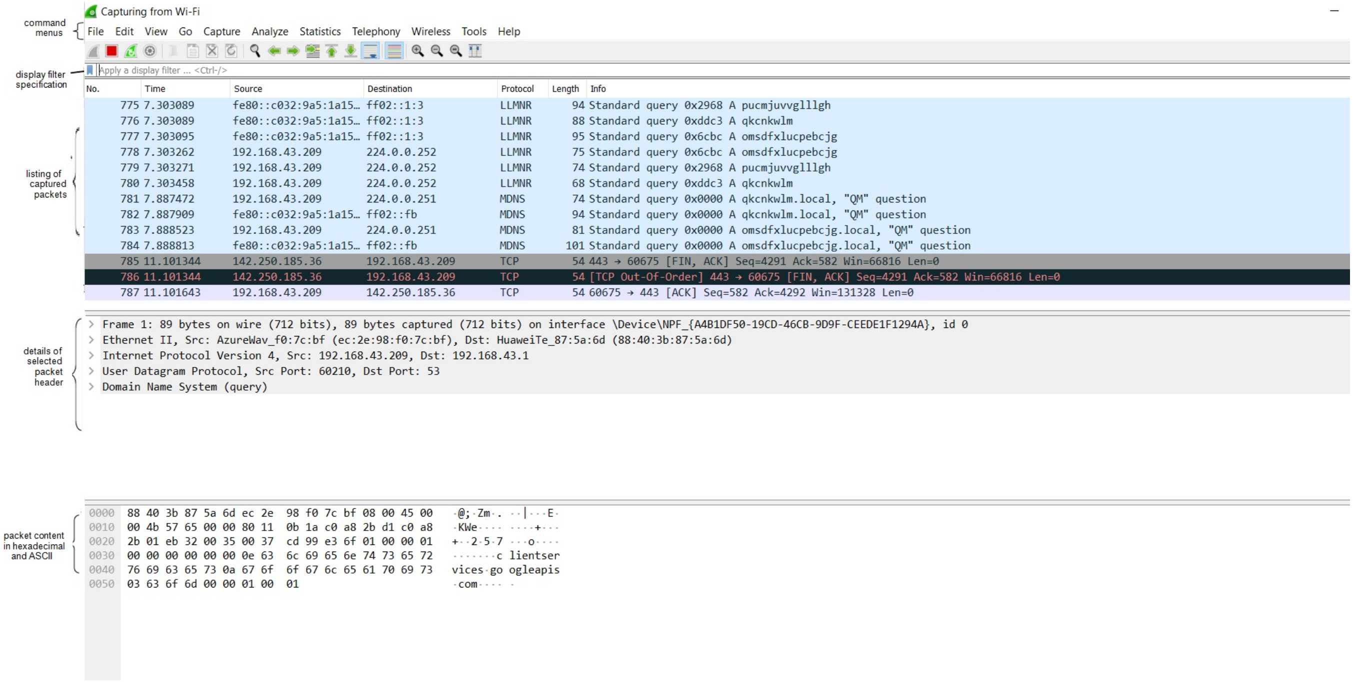
- The **command menus** are standard pull down menus located at the top of the window. Of interest to us is the File and Capture menus. The File menu allows you to save captured packet data or open a file containing previously captured packet data, and exits the Wireshark application. The Capture menu 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 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 right-pointing or down-pointing arrowhead 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.


command menus
display filter specification
listing of captured packets
details of selected packet header
packet content in hexadecimal and ASCII
Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time        Source                 Destination      Protocol  Length  Info
  775 7.303089    fe80::c032:9a5:1a15…   ff02::1:3        LLMNR       94 Standard query 0x2968 A pucmjuvvglllgh
  776 7.303089    fe80::c032:9a5:1a15…   ff02::1:3        LLMNR       88 Standard query 0xddc3 A qkcnkwlm
  777 7.303095    fe80::c032:9a5:1a15…   ff02::1:3        LLMNR       95 Standard query 0x6cbc A omsdfxlucpebcjg
  778 7.303262    192.168.43.209         224.0.0.252      LLMNR       75 Standard query 0x6cbc A omsdfxlucpebcjg
  779 7.303271    192.168.43.209         224.0.0.252      LLMNR       74 Standard query 0x2968 A pucmjuvvglllgh
  780 7.303458    192.168.43.209         224.0.0.252      LLMNR       68 Standard query 0xddc3 A qkcnkwlm
  781 7.887472    192.168.43.209         224.0.0.251      MDNS        74 Standard query 0x0000 A qkcnkwlm.local, "QM" question
  782 7.887909    fe80::c032:9a5:1a15…   ff02::fb         MDNS        94 Standard query 0x0000 A qkcnkwlm.local, "QM" question
  783 7.888523    192.168.43.209         224.0.0.251      MDNS        81 Standard query 0x0000 A omsdfxlucpebcjg.local, "QM" question
  784 7.888813    fe80::c032:9a5:1a15…   ff02::fb         MDNS       101 Standard query 0x0000 A omsdfxlucpebcjg.local, "QM" question
  785 11.101344   142.250.185.36         192.168.43.209   TCP         54 443 → 60675 [FIN, ACK] Seq=4291 Ack=582 Win=66816 Len=0
  786 11.101344   142.250.185.36         192.168.43.209   TCP         54 [TCP Out-Of-Order] 443 → 60675 [FIN, ACK] Seq=4291 Ack=582 Win=66816 Len=0
  787 11.101643   192.168.43.209         142.250.185.36   TCP         54 60675 → 443 [ACK] Seq=582 Ack=4292 Win=131328 Len=0
```

```
> Frame 1: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface \Device\NPF_{A4B1DF50-19CD-46CB-9D9F-CEEDE1F1294A}, id 0
> Ethernet II, Src: AzureWav_f0:7c:bf (ec:2e:98:f0:7c:bf), Dst: HuaweiTe_87:5a:6d (88:40:3b:87:5a:6d)
> Internet Protocol Version 4, Src: 192.168.43.209, Dst: 192.168.43.1
> User Datagram Protocol, Src Port: 60210, Dst Port: 53
> Domain Name System (query)
```

```
0000  88 40 3b 87 5a 6d ec 2e  98 f0 7c bf 08 00 45 00   ·@;·Zm·. ··|···E·
0010  00 4b 57 65 00 00 80 11  0b 1a c0 a8 2b d1 c0 a8   ·KWe···· ····+···
0020  2b 01 eb 32 00 35 00 37  cd 99 e3 6f 01 00 00 01   +··2·5·7 ···o····
0030  00 00 00 00 00 00 0e 63  6c 69 65 6e 74 73 65 72   ·······c lientser
0040  76 69 63 65 73 0a 67 6f  6f 67 6c 65 61 70 69 73   vices·go ogleapis
0050  03 63 6f 6d 00 00 01 00  01                        ·com···· ·
```

Figure 2: Wireshark Graphical User Interface

Steps for performing this lab:

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. Do the following:

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

1. **Start up the Wireshark software.** You will initially see a window similar to that shown in Figure 2, except that no packet data will be displayed in the packet-listing, packet-header, or packet-contents window, since Wireshark has not yet begun capturing packets.