CS 315: Computer Networks Lab
Spring 2022-23, IIT Dharwad
Assignment-2
Getting started with Wireshark
January 10, 2023

Lab Instructions

- Please leave your bags on the Iron shelf near the SP16 entrance.
- Login to the Ubuntu OS on your machine. The login credentials are as follows:
    - Username: user
    - Password: 123456
- Mark your attendance in the attendance sheet before leaving the lab.
- Handle the lab resources with utmost care.
- Please go through the following exercises in today's lab.
- It is recommended that you complete all the following exercises during the lab slot itself.
- If you face any difficulties, please feel free to seek help online or from your peers or TAs.
- After finishing all exercises, please carry your solutions with you (via email/pen drive) for future reference, and delete the files from the desktop.

Wireshark

Objective: The objective of this assignment is to get familiarize with the Wireshark interface

Part-1

Open wireshark and browser, start capturing wireshark packet capture, in the browser enter the url http://iitdh.ac.in. After your browser has displayed the website page, stop Wireshark packet capture by selecting stop in the Wireshark capture window. This will cause the Wireshark capture window to disappear and the main Wireshark window to display all packets captured since you began packet capture. Color Coding: You will see packets highlighted in green, blue, and black. Wireshark uses colors to help you identify the types of traffic at a glance. By default, green is TCP traffic, dark blue is DNS traffic, light blue is UDP traffic, and black identifies TCP packets with problems - for example, they could have been delivered out-of-order. You now have live packet data that contains all protocol messages exchanged between your computer and other network entities! However, as you will notice the http messages are not clearly shown because there are many other packets included in the packet capture. Even though the only action you took was to open your browser, there are many other programs in your computer that communicate via the network in the background. To filter the connections to the ones we want to focus on, we have to use the filtering functionality of Wireshark by typing http in the filtering field. Notice that we now view only the packets that are of protocol http. However, we also still do not have the exact

communication we want to focus on because using http as a filter is not descriptive enough to allow us to find our connection to http://iitdh.ac.in.
We need to be more precise if we want to capture the correct set of packets. To further filter packets in Wireshark, we need to use a more precise filter. By setting the http.host==iitdh.ac.in, we are restricting the view to packets that have as an http host the http://iitdh.ac.in website. Now, we can try another protocol. Let's use the Domain Name System (DNS) protocol as an example here. Let's try now to find out what are those packets following one of the conversations (also called network flows), select one of the packets and press the right mouse button. Click on Follow UDP Stream.

Answer the following:

1. If a packet is highlighted by black, what does it mean for the packet?
2. What is the filter command for listing all outgoing http traffic?
3. Why does DNS use Follow UDP Stream while http use Follow TCP Stream?

Part-2

In this assignment, you will be tested for your familiarity in using Wireshark for packet capture and analysis. Start packet capture in wireshark application and then open your web browser(Firefox) and type in an URL of website of your choice (http://iitdh.ac.in, http://www.amazon.in, http://youtube.com etc.).

Answer the following questions, based on your experimentation:

1. List the different protocols that appear in the protocol column in the unfiltered packet-listing window in wireshark GUI?
2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received for the web page you visited in your web browser? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)
3. What is the Internet (IP) address of the URL you visited and what is the Internet address of your computer?
4. Print the two HTTP messages displayed in wireshark GUI after you had visited the above URL through your web browser. To do so, select Print from the Wireshark File command menu, and select “Selected Packet Only” and then click Print.
5. Execute the above steps on Google Chrome, Safari or any other browsers also, check whether you will be able to see http protocol. Write down your analysis with screenshots.

Submission Details

- Write your answers in a single doc/tex file, and submit its PDF named after your IIT Dharwad roll number**,** which contains the answers (screenshots if necessary) for all the questions of Part-1 and Part-2.