CS 315: Computer Networks Lab
Spring 2024-25, IIT Dharwad
Assignment-2
Getting started with Wireshark
Jan 13, 2025

Lab Instructions

- Please leave your bags near the 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 familiarize oneself with the Wireshark interface.

Part-1

Open wireshark and browser, start capturing wireshark packet capture, in the browser enter the the following urls: https://iitdh.ac.in, https://amazon.in, and https://youtube.com - wait till each of the webpage loads completely and then fetch the next url. After your browser has displayed the webpages, stop Wireshark packet capture by selecting stop in the Wireshark capture window. Save the Wireshark trace locally.

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!

To view the packets belonging to a particular set of protocol, we need to use the filter field in Wireshark and enter the corresponding protocol. For example, 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 filter 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`, **or** use `frame contains "iitdh"` 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

Start packet capture in the Wireshark application and then open your web browser (Firefox or Microsoft edge) and type the following URLs (https://iitdh.ac.in, https://www.amazon.in, and https://youtube.com) one after other and wait till each of these webpages load.

Answer the following questions

1. List any 5 protocols you observe inside the entire trace file.
2. Use the following filters in the display filter field of Wireshark and answer with the count of the total number of displayed packets for each of the filters.
    a. frame contains “iitdh”
    b. http.request.method==GET
    c. http.request.method==POST
    d. tcp
    e. tls
    f. tcp and tls
3. a) Analyze the network traffic for requests to the following domains: iitdh, Amazon, and YouTube. For iitdh and Amazon, identify the ClientHello packet, and for YouTube, identify the first standard HTTPS packet. Fill in the table below with the Domain, Source IP, and Destination IP for each case:

Domain	Source IP	Destination IP
iitdh.ac.in		

amazon.in		
youtube.com		

b) For the observed packets in Q3.a), find the source and destination port numbers and fill the following table

Domain	Source Port	Destination Port
iitdh.ac.in		
amazon.in		
youtube.com		

Hint: In the filter field, type tcp.port==sourceport and press enter to observe all the traces, such as handshakes or replies between your system and the requested domain names.

c) Determine the time taken to complete the TCP handshake (SYN, SYNACK and ACK) for all the above-requested domain names.

d) Use the filter: tcp.port==DEST_PORT inside the display filter of the Wireshark, where DEST_PORT is the port number for the iitdh.ac.in domain. Now goto **Statistics->Flow Graph** and observe the entire communication between your system and the iitdh.ac.in server. Take a screenshot and add it into your answer.

4. In the request trace for the domain name "iitdh.ac.in", look for the first HTTP packet and answer the following questions:
    a) What is the HTTP request type
    b) What is the version of the HTTP?
    c) What is the response status code for the above GET request packet?
    d) What is the time taken to receive the response (200 OK) for the above GET request packet? (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.)
    e) Does the IP address of the domains you visited above same as you get their result using the command `host iitdh.ac.in` (change the domain in this command and check for other domains).
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.