University of Victoria

Department of Electrical and Computer and Engineering
ECE 458

Laboratory BO 1

Experiment #1
Introduction to WireShark and Layered Protocol

Feb 14, 2021

Report submitted on Feb 15, 2020

Gucheng Wang
V00942654

Introduction:

In this lab, students are asked to follow the procedure to get familiar with the Wireshark software which is one of the most widely used network protocol analyzers. It passively sniffs packets that are sent from or received by a designated network interface, but never sends packets itself. It receives a copy of sent packets from or received by applications and protocols executing on end systems.

Procedure:

Installation:

In this step, students downloaded the wireshark on the website for free and installed it.
Getting familiar with WireShark:
In this step, students started the wireshark and made sure all sets are set well and know what parameters in the column stand for, then students are asked to capture a trace using wget command. After that students close the browser to stop the unnecessary web content.

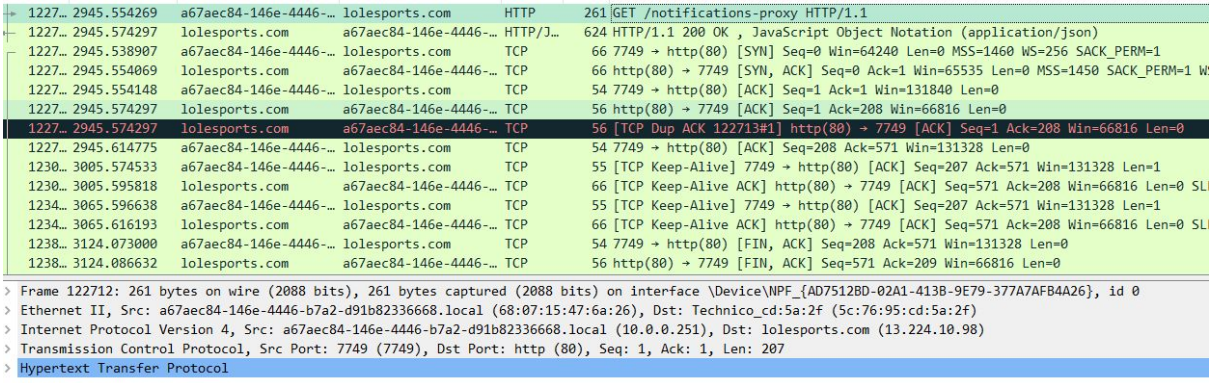
After that students launch WireShark and choose a network interface that we would like to capture the packets on. Select the interface we are using. Uncheck “Capture packets in promiscuous mode”. And use the capture filter “tcp port 80”, then it will capture the trace successfully.

Layered Protocol:

In this step, students were asked to analyze the detailed information of different layers of the protocol in http get packet, we can use the packet provided or captured.

Discussion Questions:

1. Capture a trace without any filters.
122712 2945.554269 a67aec84-146e-4446-b7a2-d91b82336668.local lolesports.com HTTP 261 GET /notifications-proxy HTTP/1.1

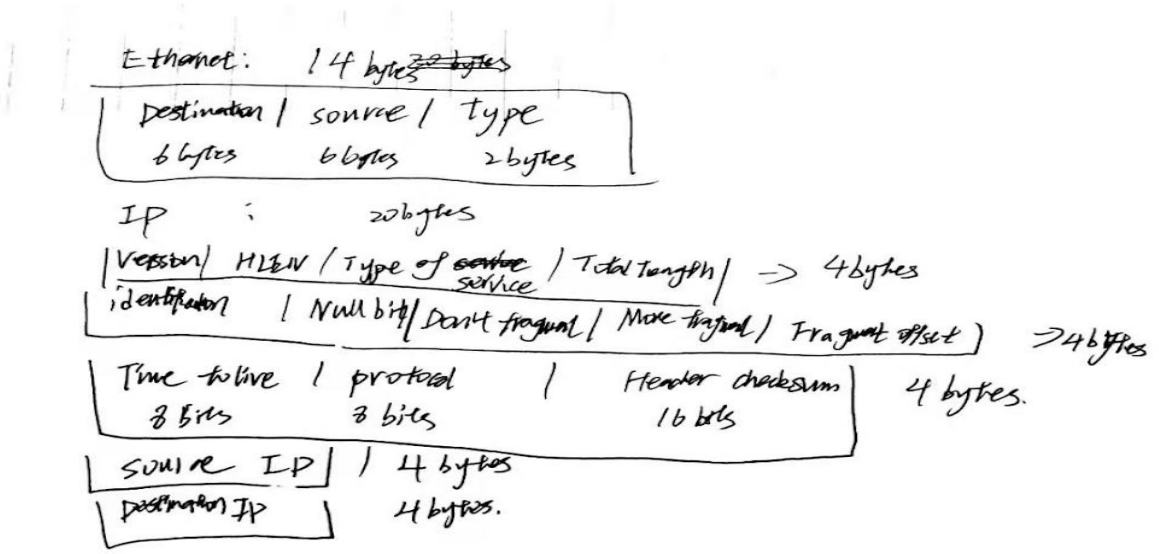


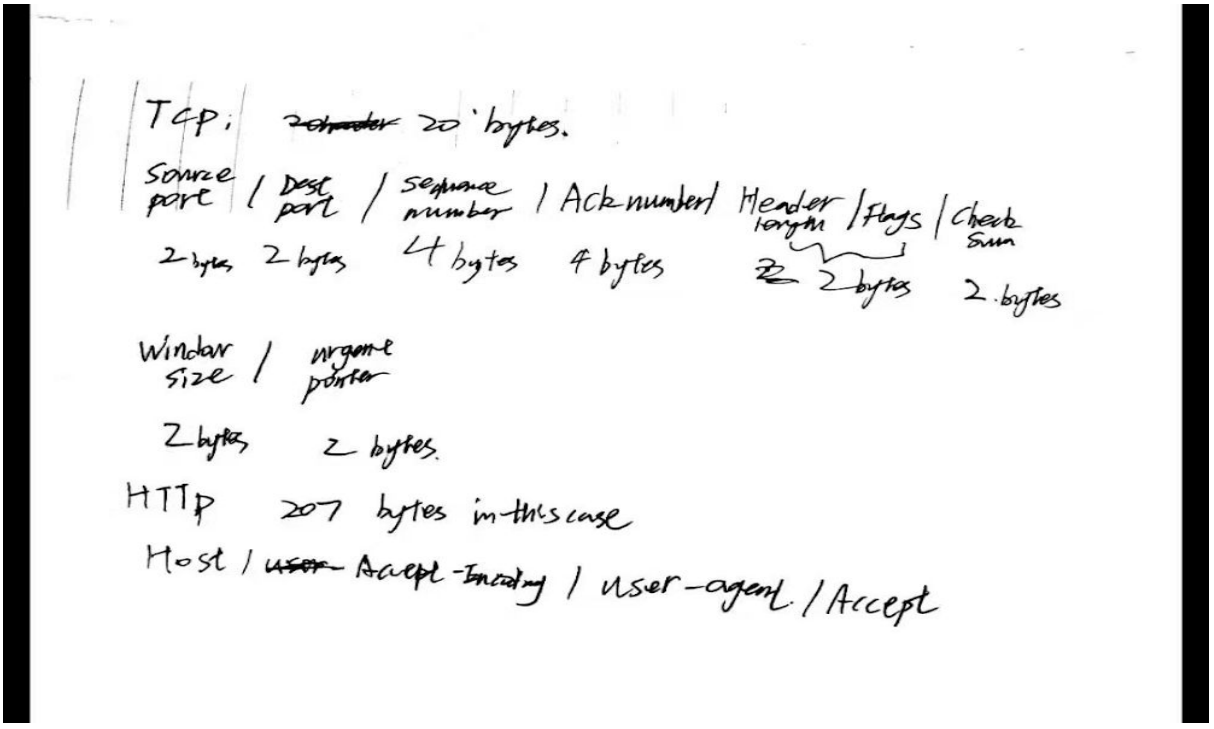
2. List at least 3 different protocols that appear in the protocol column of the unfiltered packet-listing window.

1,Ethernet II, Src: a67aec84-146e-4446-b7a2-d91b82336668.local (68:07:15:47:6a:26), Dst: Technico_cd:5a:2f (5c:76:95:cd:5a:2f)
2,(IP)Internet Protocol Version 4, Src: a67aec84-146e-4446-b7a2-d91b82336668.local (10.0.0.251), Dst: lolesports.com (13.224.10.98)
3,(TCP)Transmission Control Protocol, Src Port: 7749 (7749), Dst Port: http (80), Seq: 1, Ack: 1, Len: 207

3. How long did it take from the HTTP GET message being sent to the HTTP OK reply being received?
In this case it takes 0.020028s(2945.574297-2955.554269).

1. Draw the structure of an HTTP GET packet.





2. In the provided trace (lab1-wget-trace.pacp), calculate the average overhead of all of the packets from the server to the client (in percentage). (Hint: For a packet, the overhead is the size of all headers over the packet's total size. The average overhead is the ratio of the sum of the headers' size over the sum of the packets' size).
Header length:2*(40+20)+24*(32+20)=1368
packet length:2*74+13*66+7*1484+177+1362+164+216=13313
overhead=1368/13313=0.1028.

3. Which bytes in the Ethernet header field tell that the next higher layer protocol is IP? What is its hexadecimal value?
Bytes 13,14(type) tell the next higher layer is IP. Hexadecimal value is 0x0800

4. Which bytes in the IP header field tell that the next higher layer protocol is TCP? What is its hexadecimal value?
Bytes 10(protocol) tells the next higher layer is TCP, its hexadecimal value is 6.

1. How many Ethernet interfaces are in your computer, and how to determine it?
There are 4 ethernet interfaces in my computer, to determine this value in console add command ifconfig and it will show the ethernets on your computer.
2. How to turn down/up an Ethernet interface?
command: ifdown/ifup plus the name of the interface you want to turn up or down, eg ifdown eth0.
3. Ping 10 packets to two websites. Compare the statistic results (i.e., the packet loss rate and average round-trip time).
ping -c 5 google.ca
packets: sent = 5, received = 5, loss = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum= 13ms, Maximum = 17ms, Average = 15ms

ping -c 5 baidu.com
packets: sent = 5, received = 5, loss = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum= 252ms, Maximum = 255ms, Average = 253ms

Compared results: all packets are sent successfully without any loss, however the rrt is not the same which is caused by different location of server.

Conclusion:

In this lab, students are asked to capture a Http get packet and analyze its structure. This lets students be familiar with the instructions of using wireshark and how the packets are sent and received between source and destination. Students also learned different commands ,like wget , ifconfig and ping to manage the ethernet and send packets to websites. Overall this lab introduces students how wireshark works and how to use it to capture various packets.

Reference:

1,
ECE458. (2021). Ece458Lab.https://studentweb.uvic.ca/%7Ewenjunyang/ECE458/notes.html
2,
Andrew Tanenbaum and David Wetherall, Computer Networks 5/E, Prentice Hall, Oct. 2010
3,
James F. Kurose and Keith W. Ross. 2009. Computer Networking: A Top-Down Approach (5th ed.). Addison-Wesley Publishing Company, USA.

Feedback:

It is very necessary to let students have a chance to ask what they are confused about, for that it is remotely done in the lab, students find it very hard to ask questions.