CS352-Summer 2019

Instructor: Murtadha Aldeer

Teaching Assistant: Yujie Ren

Project 2-Wireshark

The aim of this lab is to use Wireshark for packet sniffing. Wireshark is an open source software tool that allows you to examine packets captured by any network interface on your machine. We recommend that you first install this software on your personal machine.

Please work through each of the tasks discussed below. Each task will specify material you are required to hand in. You will need to cut several snapshots and put them into a document and convert that document (is possible) to a PDF file. For submission please submit the PDF file (with you NetID as its name) via Sakai.

Installation

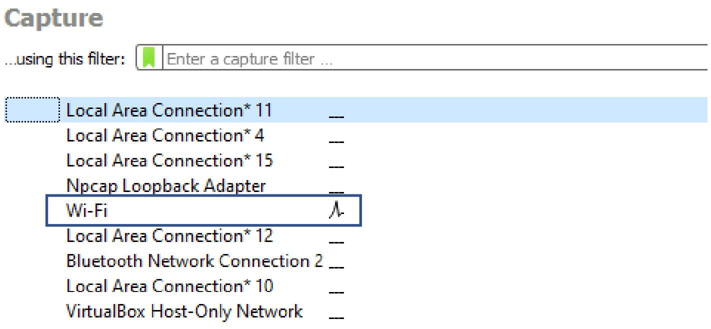
See the slides titles **CS352-Summer2019-Wireshark**

Note 1: This assignment/project is based on the fact that you will use your personal laptop to run Wireshark. Also, the laptop in use is connected to the Internet through a Wi-Fi router (Access point), at home or somewhere else.

Note 2: Make sure to clear your web browser's cache

OK, lets start with Wireshark!

1) Start a capture session using Wireshark. From the main screen of Wireshark, you need to select the interface you are using to connection to the Internet, example: Wi-Fi, see below screenshot



Capture

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

Local Area Connection* 11
Local Area Connection* 4
Local Area Connection* 15
Npcap Loopback Adapter
Wi-Fi
Local Area Connection* 12
Bluetooth Network Connection 2
Local Area Connection* 10
VirtualBox Host-Only Network

Capture traffic when you are opening a web page in your browser. Open the web page http://www.ox.ac.uk Please save the trace you use in the lab and submit it with your answers. To save go to “File” and select save file (e.g., call it NetID (which is your NetID)).

2) Stop capturing and examine the trace and find the exchange of packets between your machine and the web server (the host providing the web pages to your machine). In the trace you can see many protocols listed. Some of these protocols are called transport protocols. Answer the following:

   a- Which transport protocol is used between your machine and the web server?
   b- You will see that other protocols are captured in your trace. One such protocol is HTTP. What is the relationship between the transport protocol you identified and HTTP?
   c- Type in “http” (without the quotes, and in lower case – all protocol names are in lower case in Wireshark) into the display filter specification window at the top of the main Wireshark window. Then select Apply (to the right of where you entered “http”). This will cause only HTTP messages to be displayed in the packet-listing window. To see the exchange of HTTP messages with the web server, click statistics → flow graph → then check the “limit to display filter” box. Take a snapshot or copy/paste the packets displayed on the monitor (no need to scroll down and copy all).

3) In the trace you will find IP addresses within the packets. Answer the following:

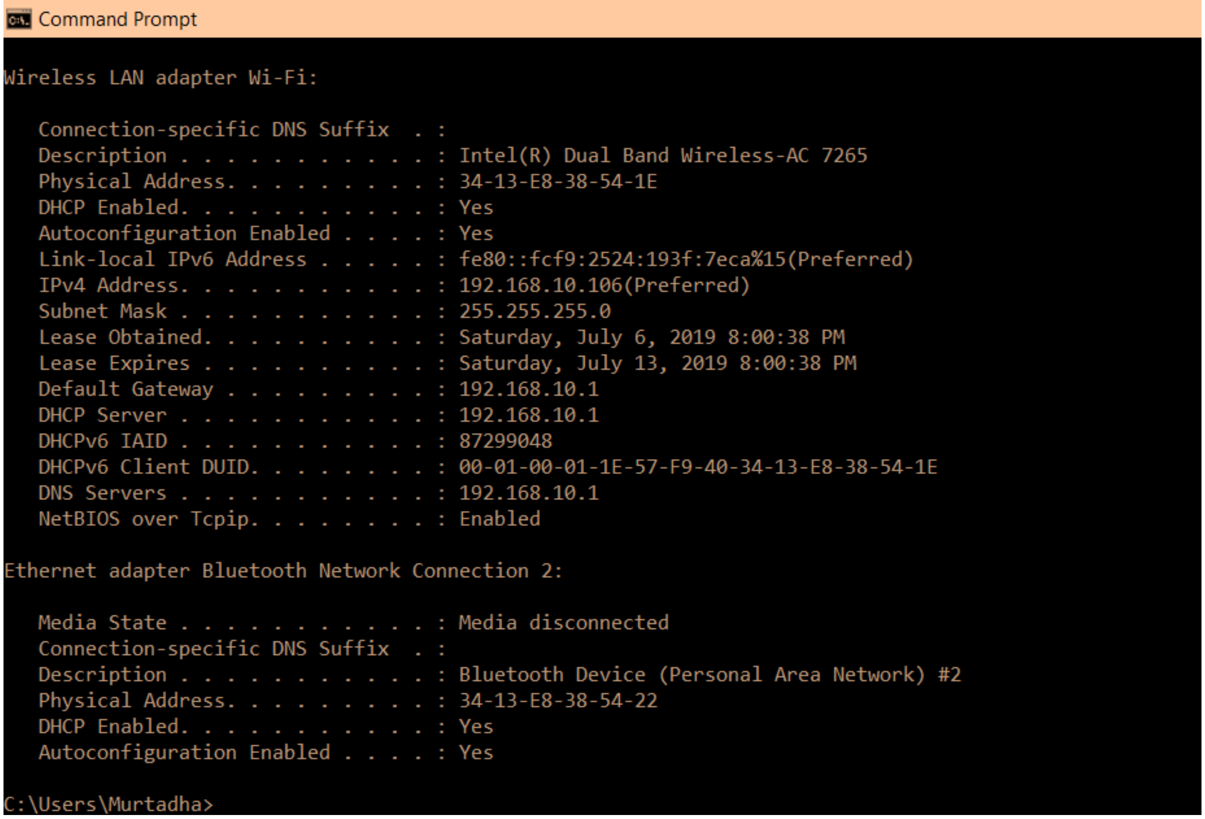
   a- Find an example packet in the trace where the IP address associated with your machine is present. Provide this example packet with your submission (take a screen dump or cut and paste the packet).
   b- We discussed protocol layers in class. Which layer is the IP associated with? Which layer is the transport protocol you identified in sec. 2 a is associated with? Which layer is the HTTP protocol associated with?

   Make sure to provide you answer in the required sequence. You may use a table like this to answer this section:

Layer	Protocol

4)

   a- We discussed the MAC (medium access control) address in class. You can find the MAC address of your machine using ifconfig /all a on unix, Linux, windows, and OSX machines - at the command line. If you are using the WLAN, look for **Physical Address** under **Wireless LAN adapter Wi-Fi**. Take a snapshot for this part, the output should be like this:



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 7265
   Physical Address. . . . . . . . . : 34-13-E8-38-54-1E
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::fcf9:2524:193f:7eca%15(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.10.106(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Saturday, July 6, 2019 8:00:38 PM
   Lease Expires . . . . . . . . . . : Saturday, July 13, 2019 8:00:38 PM
   Default Gateway . . . . . . . . . : 192.168.10.1
   DHCP Server . . . . . . . . . . . : 192.168.10.1
   DHCPv6 IAID . . . . . . . . . . . : 87299048
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1E-57-F9-40-34-13-E8-38-54-1E
   DNS Servers . . . . . . . . . . . : 192.168.10.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network) #2
   Physical Address. . . . . . . . . : 34-13-E8-38-54-22
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

C:\Users\Murtadha>
```

b- Can you find the MAC address for your machine in the trace?. What is the MAC address of your machine? Hint: you should click on a message originated from your machine and then click on Ethernet II in the packet details pane to see the MAC address (shown as Src address). (take a screen dump for the Ethernet II details that show this).

c- What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of www.ox.ac.uk ? (Hint: the answer is no).

What device has this as its Ethernet address (MAC address)? Based on the answer you will provide, why this the address of this device and not that of the web server that is hosting ox.ac.uk?

5) Answer the following:

a- Before doing this part, start capturing a new trace (make sure that you save the previous trace file).

Now, at the command line on your machine, type ping www.ox.ac.uk. Did you get 4 replies? Is so, stop capturing via Wireshark. Take a snapshot for the output of ping command.

What does the **time** (in *ms*) given there (at the command line) refer to? Hence it is related to the delay components we covered in the 1st lecture. FYI, you can see the packets resulted from typing ping, captured by the Wireshark. To see these, type ICMP in the filter field. Take a screen dump or cut and paste the packet that shows these packets. They should be 8 packets.

b- Repeat part a for www.lincoln.ac.nz

For this part, include screen dumps or cut and paste packets as in a.
Why the time in *ms* is greater as compared to that in part a? what do you think? You may use a simple equation and one line of description to answer this question.

In case you use any reference or online resource, make sure to provide citation.