In this task, we will see how to read information about HTTP messages received and sent by your computer using **Wireshark**.

1. Open your browser.
2. Before performing the steps below, make sure the cache of your browser is empty.

   To remove cached files from Google **Chrome**, select Settings, and then click Clear browsing data, as shown in Figures 1 and 2.

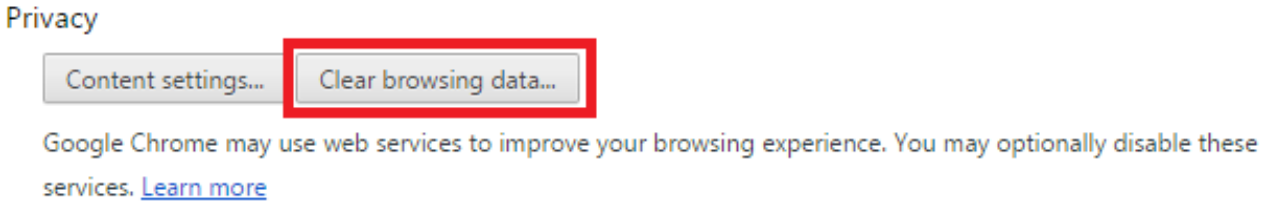


Figure 1

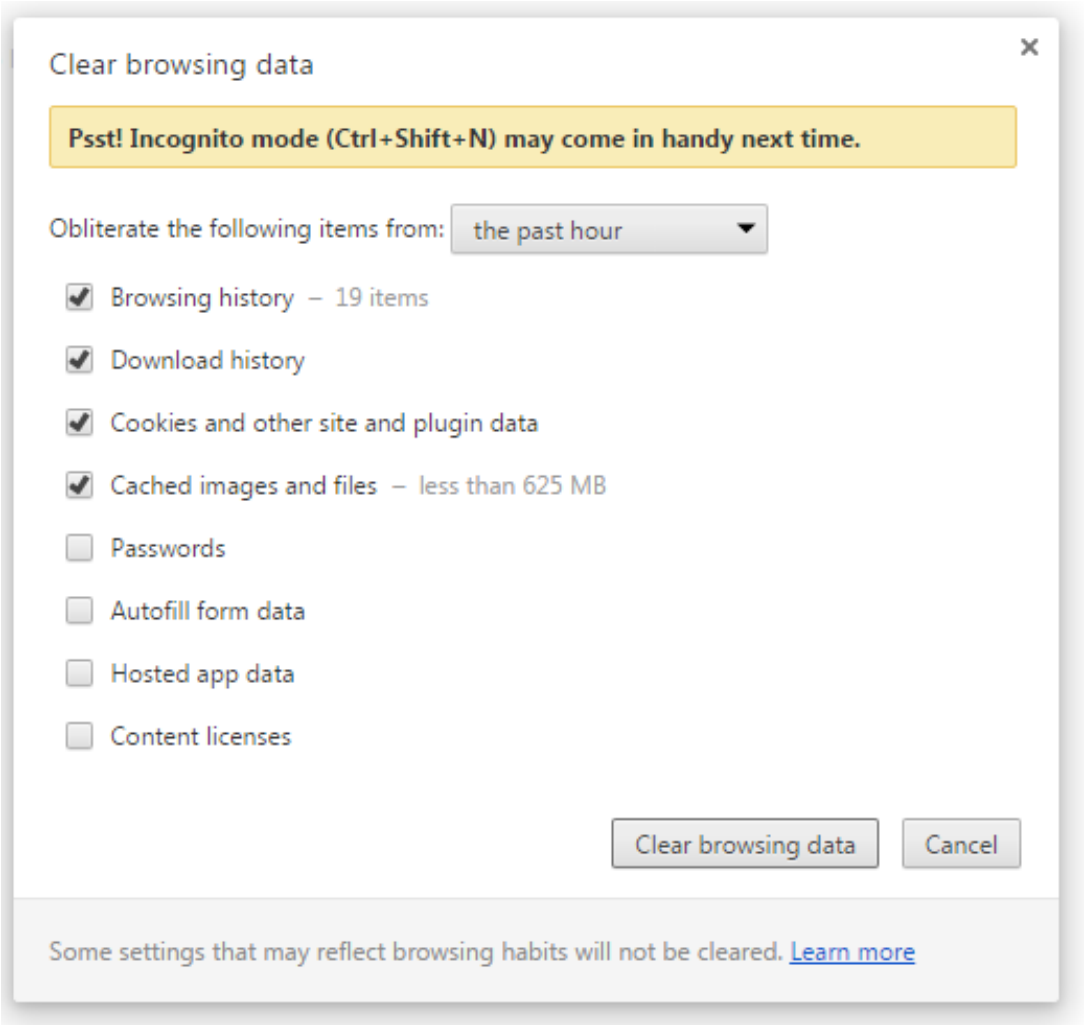


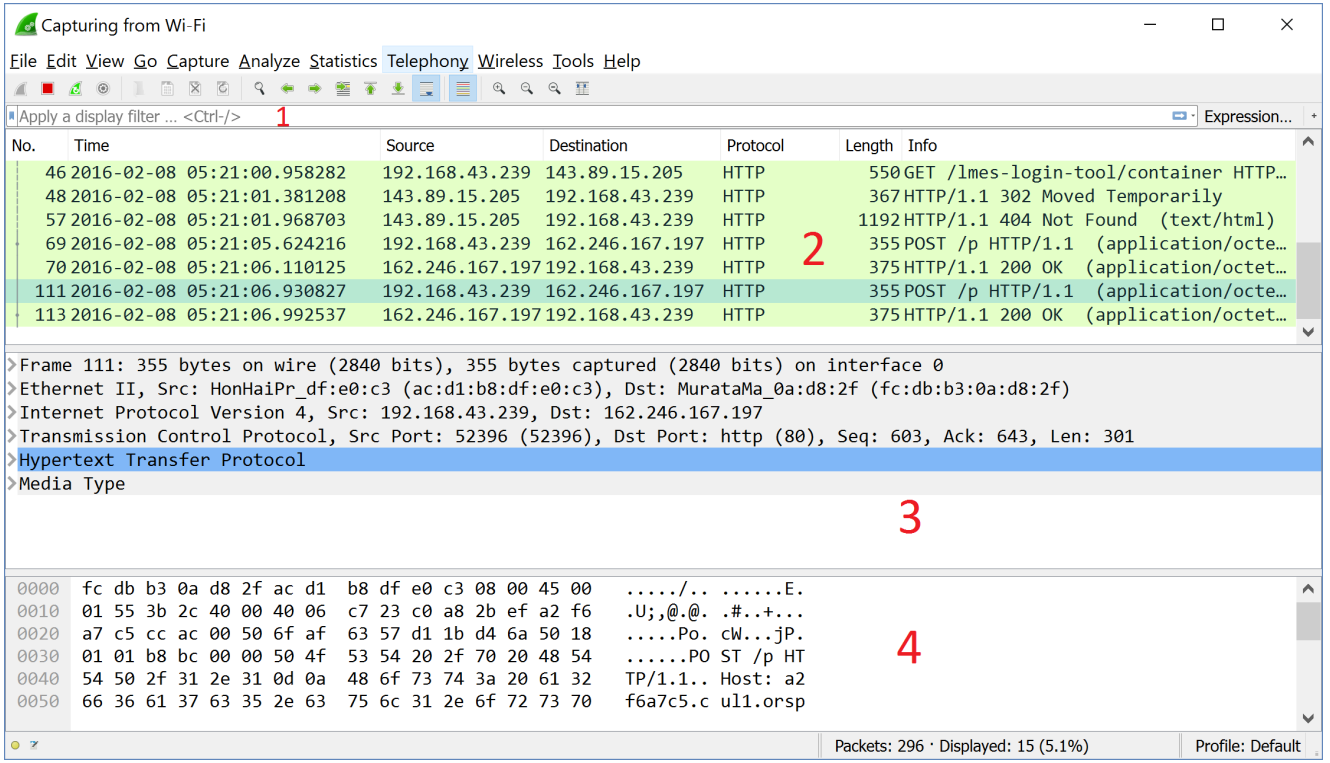
Figure 2

To remove cached files from **Firefox**, as shown in Figure 3, select *Edit => Preferences => Advanced => Network => Clear Now.*

Figure 3: Clear the cache in Firefox

3. Set up Wireshark so that it is capturing packets, as described on the previous pages.
4. Enter the URL: http://course.ee.ust.hk/elec1200/. In order to display this page, your browser will contact the HTTP server course.ee.ust.hk and exchange HTTP messages with it in order to download the files required to display this page. The Ethernet frames containing these HTTP messages will be captured by Wireshark.
5. After your browser has displayed the page, stop Wireshark packet capture by

selecting “Stop” in the Wireshark capture window. The Wireshark window should now look similar to that of the figure shown below. You now have all protocol messages exchanged between your computer and other network entities!



6. The HTTP message exchanges between your computer and the course.ee.ust.hk web server should appear somewhere in the listing of packets captured. However, there will be many other types of packets displayed as well. Even though the only action you took was to download a web page, there are many other protocols running on your computer that are unseen by the user.

7. In order to see only those packets sent and received by your web browser, enter “http” (without the quotes and in lower case) into the display filter specification sub-window (**1**) at the top of the window. Most messages, except HTTP messages, will be

suppressed in the packet-listing sub-window (**2**). You may see SSDP messages on the display, feel free to ignore them.

8. Select the "GET /elec1200/" message that was sent from your computer to the course.ee.ust.hk web server. When you select the HTTP GET message, the Ethernet frame, IP datagram, TCP segment, and HTTP message header information will be displayed in the packet-header sub-window (**3**). By clicking on the ">" icons in the packet details window, you can see more details about these.
9. The response from the server to your browser should be one of the next HTTP packets after the GET request. You can check that it is the correct response by looking at the source and destination fields, which should be the reverse of the GET request.
10. Use the information in the packet-listing (**2**) and packet-header (**3**) sub-windows to answer the questions below.

LAB 4 TASK 1 QUESTION 1

(1/1 point)

What is the version of HTTP that the server using??

1.1 ▾ ✔ **Answer:** 1.1

You have used 1 of 2 submissions

LAB 4 TASK 1 QUESTION 2

(1/1 point)

What is the IP address of the http://course.ee.ust.hk/elec1200/ web server?

143.89.44.246 ▾ ✔ **Answer:** 143.89.44.246

You have used 1 of 2 submissions

Lab 4 Task 1 Question 3

(1/1 point)

What is the number of bytes of content is being returned to your browser?

5039 ✔ **Answer:** 5039

5039

Hint: Check the Content-Length field under the detailed Hypertext Transfer Protocol information about the packet.

You have used 1 of 3 submissions