# CINF 3331: Business Data Communications

# Assignment 1: HTTP and E-mail

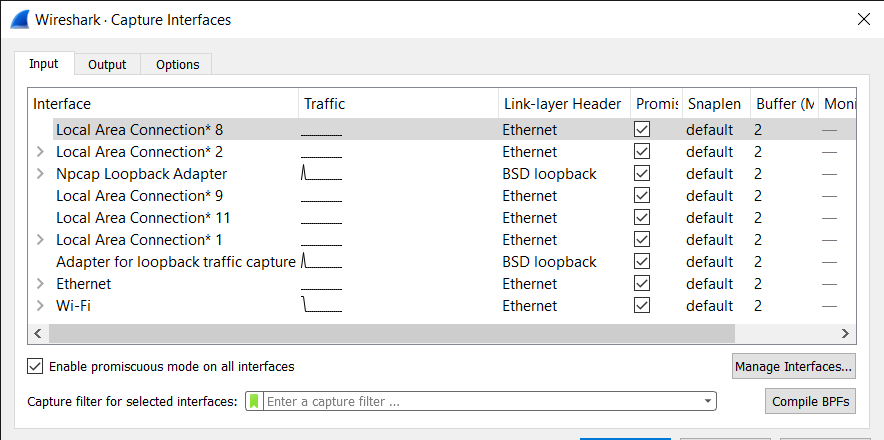
Type your answers and paste your screenshots directly in this file in the indicated spots. Save this file with a filename in this format – *First Name\_Last Name\_Assignment 1*.docx. **Please save your Wireshark capture file using the same name and submit with this Word file together.**

You will need the following software installed on your PC or use the computer in our classroom to complete this homework assignment.

1. Wireshark (available at wireshark.org). I recommend using the latest Stable Release.
2. A web browser that you are comfortable using. You will need to clear your cache.
3. A few files for analysis, which are posted next to this assignment on BB.

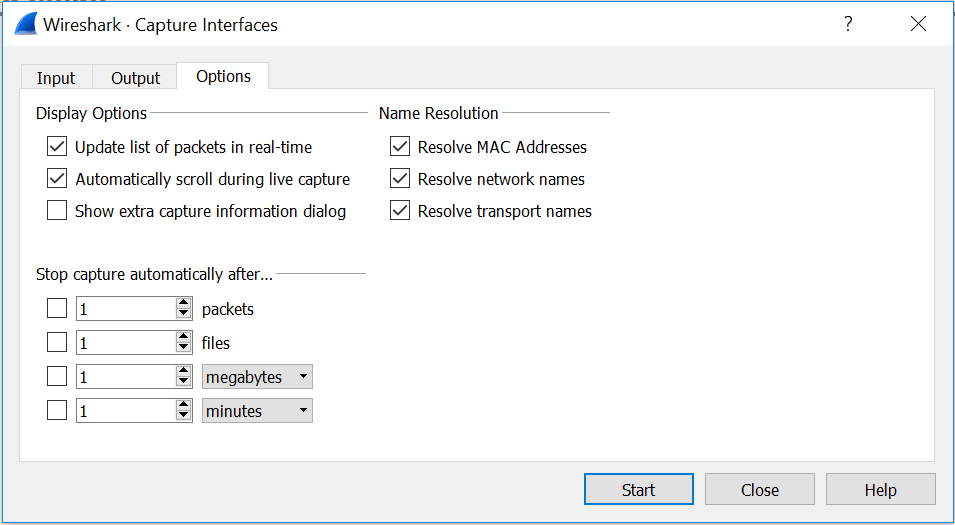
# Introducing Wireshark & HTTP

1. Clear the browsing history and cache in your browser and close all existing browser sessions (If you don’t know how to do this, use google for instructions). Or you can use the private window in Firefox or incognito window in Google Chrome.
2. Start Wireshark and select the **Capture 🡪 Options** to open the Capture Interfaces window – which contains a list of all the interfaces available on your PC. Pick the appropriate interface to capture from the list of available devices (the interface that sees some activity under “**Traffic**” in terms of packets sent / packets received is the one you should choose).

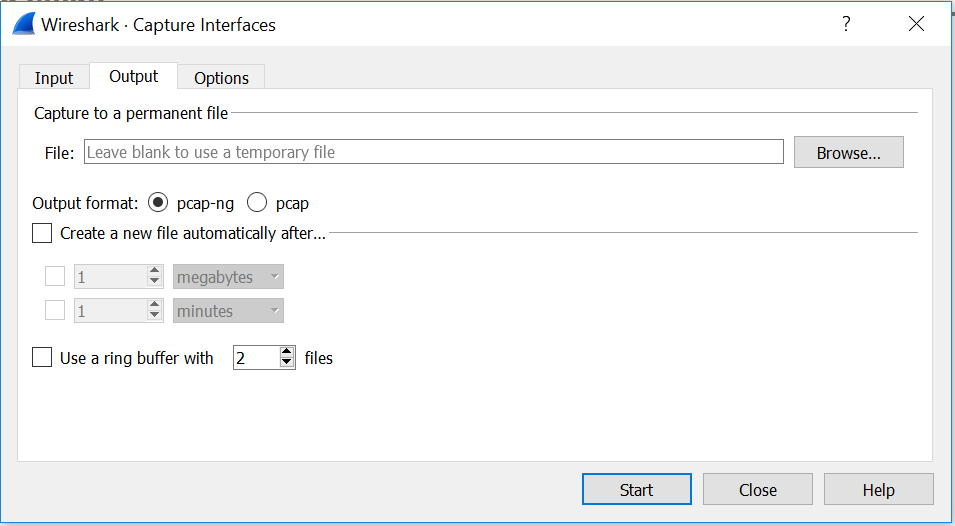


1. Select the **options** button and set the following parameters.

(Read the Wireshark user guide for information about each individual options)



1. To save the capture session you are about to start, use the ‘Capture to a permanent file’ section in the Output tab and set a file name and location for saving your capture to your local drive.



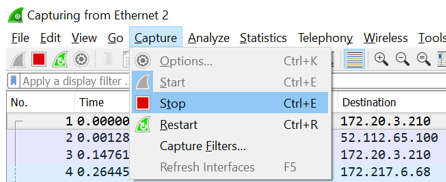
1. After setting all the parameters and checkboxes as shown in the screenshots, press ‘Start’ to capture the traffic.

NOTE: Your network data will be captured from this instant.

1. Use your **web browser** to go to [www.washington.edu](http://www.washington.edu). You can try to click the link directly or copy and paste it to your browser to visit. To make sure your website visit is valid to complete this assignment. You need to be able to see the following “Not Secure” sign in your address bar.



1. Stop the capture after the website has completely loaded. Press the ‘Stop’ menu item in ‘Capture’ menu to do this action. Or the Stop icon (a red box) on the tool bar.



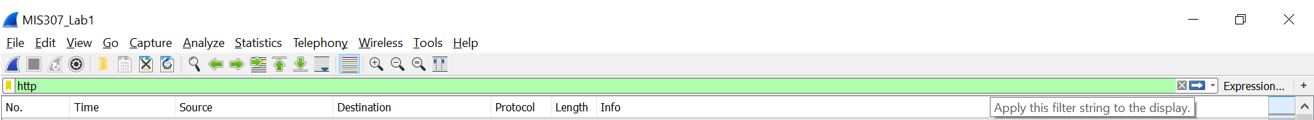
1. Ensure that the session is saved (File🡪Save, if necessary, and check the folder you saved the capture file to).
2. Verify the packet list details in Wireshark for all the captured data and note down your initial observations.
3. Check the packet details and the packet bytes for the packets that were captured in this session.
4. Observe the protocol hierarchy statistics by navigating to **‘Statistics 🡪 Protocol hierarchy’** menu item.

Graphical user interface, application, table

Description automatically generated

1. You’ve probably captured a lot of information. To make it more readable, apply a filter so that only the HTTP data is shown:

Type HTTP in the blank which indicates “Apply a display filter … <Ctrl-/>”. Then press Enter to get the result.



Your screen should look similar to the one below, with only HTTP related data packets shown in the list.

Graphical user interface, application

Description automatically generated

1. Observe the protocol hierarchy statistics for the HTTP packets by following the same procedure as in step 11 on the applied filter for HTTP packets. You should be able to see a similar screen with the corresponding percentages

Graphical user interface, table

Description automatically generated

1. Repeat 12 for the filter of TCP (Filter TCP packets)

Graphical user interface

Description automatically generated with medium confidence

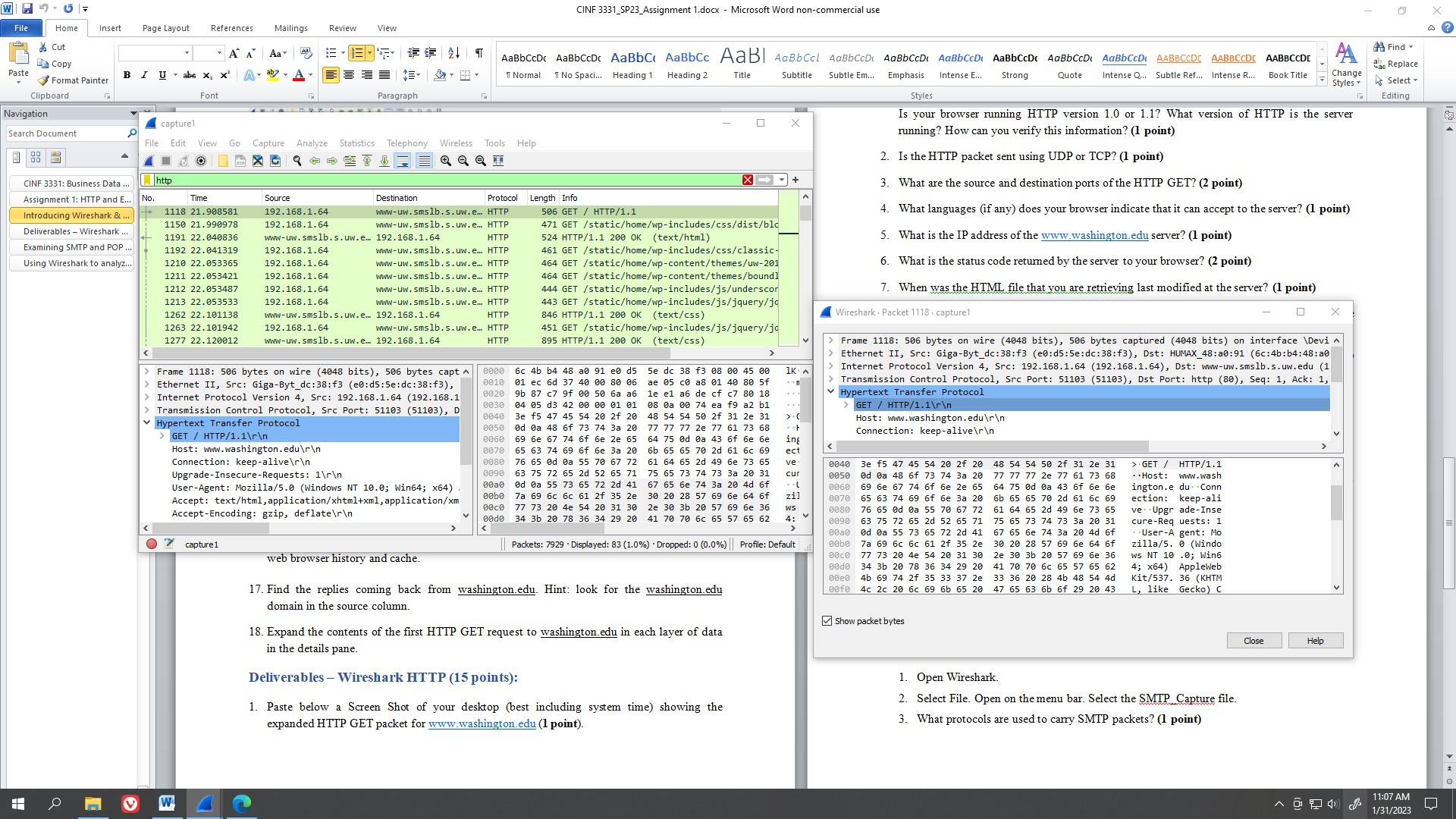
1. Observe the protocol hierarchy statistics for the TCP packets by following the same procedure as in step 11 on the applied filter for TCP packets. You should be able to see a similar screen with the corresponding percentages

A screenshot of a computer

Description automatically generated with medium confidence

1. Find the initial HTTP GET request for washington.edu. Hint: look for the first item that has washington.edu domain as the destination. If you only see IP Addresses in the Destination column, you didn’t turn on all the right options for your capture in step 3. If you don’t see any packets going to the washington.edu domain, you may not have properly cleared your web browser history and cache.
2. Find the replies coming back from washington.edu. Hint: look for the washington.edu domain in the source column.
3. Expand the contents of the first HTTP GET request to washington.edu in each layer of data in the details pane.

# Deliverables – Wireshark HTTP (15 points):

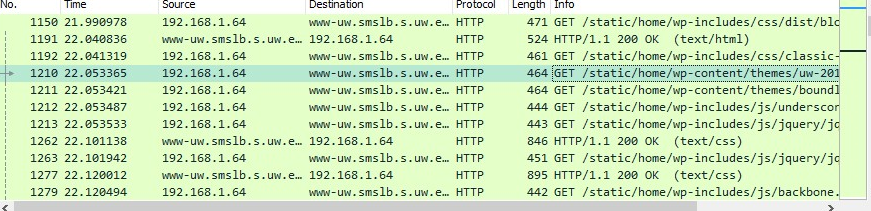
1. Paste below a Screen Shot of your desktop (best including system time) showing the expanded HTTP GET packet for [www.washington.edu](http://www.washington.edu) (**1 point**). 

Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running? How can you verify this information? **(1 point)**

**HTTP 1.1 is used by client. The HTTP version is stated to be 1.1 in the request header. HTTP 1.1 is used by the server. The HTTP version is stated to be 1.1 in the response header.**

1. Is the HTTP packet sent using UDP or TCP? **(1 point) The HTTP packets are using TCP**
2. What are the source and destination ports of the HTTP GET? **(2 point)** **The source port 51103, destination port 80.**
3. What languages (if any) does your browser indicate that it can accept to the server? **(1 point) The accept-language is: en-US,en;q=0.9. US English with a weight preference of 0.9.**
4. What is the IP address of the [www.washington.edu](http://www.washington.edu) server? **(1 point) www-uw.smslb.s.uw.edu (128.95.155.135)**
5. What is the status code returned by the server to your browser? **(2 point) Status Code is 200**
6. When was the HTML file that you are retrieving last modified at the server? **(1 point) Tue, 31 Jan 2023 01:09:08 GMT**
7. How many bytes of content are being returned to your browser? You need to add up all the HTTP response bytes. **(1 point) 1518567 bytes**
8. **(2 point)** Approximately how many HTTP GET request messages did your browser send to Washington.edu? 37

Show a screen shot below.



Why did your client have to send several HTTP requests? It is requesting website data in parts. Some parts are JPEG data, some parts are CSS style sheet data. Some are raw HTML data. etc.

1. What type of web server is used? **(1 point)** Apache/2.2.24 (Unix) mod\_ssl/2.2.24 OpenSSL/1.0.1e-fips PHP/7.2.23 mod\_pubcookie/3.3.4a mod\_uwa/3.2.1
2. Some companies do not advertise the type of web server they use. Why do you think they do this? **(1 point)** Security reasons. Knowing the framework of a server can lead to finding vulnerabilities.

# Examining SMTP and POP Protocols

# Using Wireshark to analyze SMTP and POP data (10 points).

To do the exercises you will need to download the two packet files *(****Files****: SMTP\_Capture.pcap, and POP3\_Capture.pcap)* posted on BB.

**Exercise 1: Viewing an SMTP Session**

1. Open Wireshark.
2. Select File. Open on the menu bar. Select the SMTP\_Capture file.
3. What protocols are used to carry SMTP packets? **(1 point) Protocols used are TCP, SMTP, and SMTP/IMF** ****
4. Observe the SMTP header in Packet **#**18. Find the information for every field of the header of this SMTP packet: **(1 point)**
   1. From: "Student" <student@starfish.eller.arizona.edu>
   2. To: <teacher@starfish.eller.arizona.edu>
   3. Date: Sat, 27 Nov 2010 18:00:52 -0700
   4. Subject: Class information
   5. Message ID #: <00a801cb8e97$b41ebbb0$1c5c3310$@eller.arizona.edu>
5. The first three frames are the three steps of the TCP startup. Frames 4 to 24, 26 contain the e-mail process and the e-mail message. Frames 25, 27-29 describe TCP shutdown. **(1 point)**
   1. What port number is used by the client? How do you know?
   2. What port number is used on the server? How do you know?

Transmission Control Protocol, Src Port: 55012 (55012), Dst Port: smtp (25), Seq: 4380, Ack: 222, Len: 6

Port 55012 for Client. Port 25 for Server.

In packets, a source port and destination port can be found.

Packet 24 describes a “C” client sending a QU IT command to the server. Packet 26 describes an “S” server sending a 221 code.

1. Locate packet 18 and click on it. Look inside the packet and expand the Internet Message Format tab (expand as many levels as needed). Answer the following questions from the email message **(1 point)**:
   1. What is the name of the person sending the email message? Pat Green
   2. When was she born? DOB: Feb 10 1980
   3. What is her SSN? SSN: 123-44-3211
   4. Which part of the SMTP packed did you find this information in? SMTP, under IMF, under MIME Multipart Media Encapsulation, under either Encapsulated multipart part: (text/plain) OR Encapsulated multipart part: (text/html)
   5. In viewing this message, would you be concerned about email security? How could the security be improved? Security can be improved by improving the protocol used, or using a different protocol. The vulnerability is that the raw html text is saved and sent. Instead, the raw text must be hidden somehow while still being sent. One way to accomplish this is text encryption.
2. Locate frames 14 and 15. What is the purpose of these 2 frames? **(1 points) Packet 14 and 5 are DATA Fragments. Packet 14 houses plain text. Packet 15 houses the message style sheet. Both are reassembled into Packet 18.**

**Exercise 2: Viewing a POP3 Session**

1. Open Wireshark.
2. Select File. Open on the menu bar. Select the POP3\_Capture file.
3. What protocols are used to transmit POP3 packets? **(1 point) Protocols used are TCP and POP.**
4. The first three frames are the three steps of the TCP startup. Frames 4 - 30 contain the e-mail process and the e-mail message. The last four packets are the TCP shutdown. **(1 point)**
   1. What port number is used by the client? Why?
   2. What port number is used on the server? Why?

Transmission Control Protocol, Src Port: 53200 (53200), Dst Port: pop3 (110), Seq: 75, Ack: 5229, Len: 6

Port 53200 for Client. Port 110 for Server.

In packets, a source port and destination port can be found.

Packet 29 describes a “C” client sending a QU IT command to the server. Packet 30 describes an “S” server sending a +OK response, as well as logging out and deleting messages.

1. Locate frames 5-11. These frames are used to process the user ID and password required by the SPA (Secure Password Authentication) security process.
   1. From what you see, can you determine the user ID and password of the user? **(1 point) C: USER teacher AND C: PASS just4teacher**
2. Look in packet 19. Open the POP part of the display. Can you read the entire contents of the message? If not where is the rest of it?  **Hint:** Right click and the packet and select **Follow TCP Stream (1 point)** Packet 19 delivers the first part of the mail. The following packet, Packet 20, holds the rest of the text mail.
3. What are Frames 26 and 27 used for? **(1 point) Frame 26 is a command from Client to delete a message. Frame 27 is a response from Server stating that the message is marked for deletion.**