HTTP Minilab

Ver 2.0

Let's begin the exploration of HTTP by downloading a very simple HTML file; one that is very short, and contains no embedded objects.

Do the following:

- Start up your web browser.
- Start up the Wireshark packet capture, as described in the introductory lab (but don't yet begin packet capture). Enter the string "http" in the Filter-field, then press the button Apply so that only captured HTTP messages will be displayed later in the packet-listing window. (We are only interested in the HTTP protocol here, and don't want to see the clutter of all captured packets).
- Start Wireshark packet capture.
- Enter the following to your browser: http://tech-uofm.info/TECH3812a.html. Your browser should display the very simple, two-line HTML file as follows:

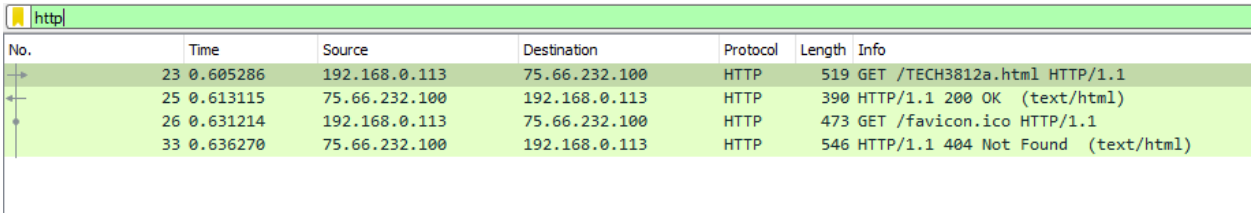
Lab 1

This is a very simple webpage

- Stop Wireshark packet capture.

Note: if you need to repeat the capture, you will need to clear your short term cache or you will not get the correct packets, but instead get a "304 Not Modified" instead of "200 OK" message.

You should have something like the following:



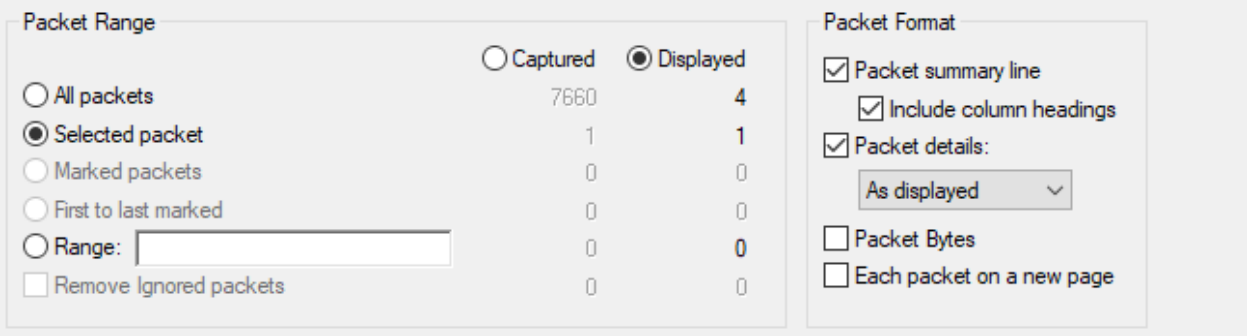
You can ignore the packets "GET /favicon.ico" and the "404 Not found". The first is requesting an icon to display on the tab (if defined) and the 2nd says it does not exist.

The first packet "GET /TECH3812a.html HTTP/1.1" is your computer requesting the website, the "HTTP/1.1 200 OK" packet is the response from the server including the web page itself.

Select the "GET /TECH3812a.html HTTP/1.1" and then, in the center window, click on the ">" next to the line that says "Hypertext Transfer Protocol". This shows the actual data sent to the server to retrieve the website.

If you look at the first two lines withing that section, you will see the command to retrieve the website, and on what HOST that website is located on.

Stop the capture and do a File | Export Packet Dissections | As Plain Text. A new window will appear….on the bottom of the screen, select the values as show:



And then save the file to a know location and name.

Open the text file you saved. You should have something similar to this:

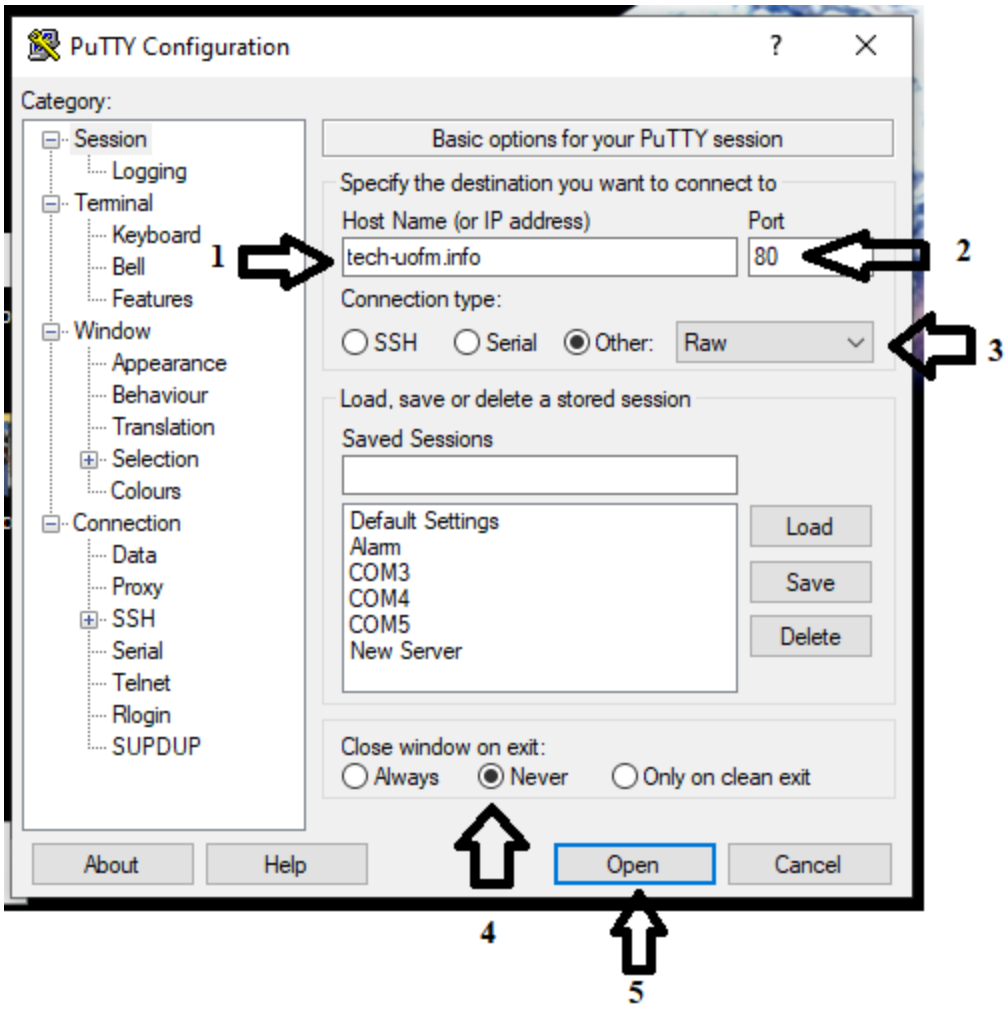
```
No.     Time           Source                Destination           Protocol Length Info
     23 0.605286       192.168.0.113         75.66.232.100         HTTP     519    GET /TECH3812a.html HTTP/1.1

Frame 23: 519 bytes on wire (4152 bits), 519 bytes captured (4152 bits) on interface \Device\NPF_{6A3C51E9-B582-4FBA-BEC3-1A85FCB3FC0E},
Ethernet II, Src: Dell_d8:9c:76 (f8:b1:56:d8:9c:76), Dst: HonHaiPr_8c:ef:f6 (90:4c:e5:8c:ef:f6)
Internet Protocol Version 4, Src: 192.168.0.113, Dst: 75.66.232.100
Transmission Control Protocol, Src Port: 51530, Dst Port: 80, Seq: 1, Ack: 1, Len: 465
Hypertext Transfer Protocol
    GET /TECH3812a.html HTTP/1.1\r\n
    Host: tech-uofm.info\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Cookie: _dd_s=logs=1&id=ce551296-68d4-410a-9c9c-4471a534d3c8&created=1649211116712&expire=1649213225789\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://tech-uofm.info/TECH3812a.html]
    [HTTP request 1/2]
    [Response in frame: 25]
    [Next request in frame: 26]
```

Copy and paste the two highlighted lines shown above into another Notepad or Notepad++ file and edit these lines, removing the leading spaces and the \n\r at the end of the line. Copy these edited lines to the clipboard. [note that these lines might be separated by other text in newer versions of Wireshark]

The other lines, give the server more information about your computer and how to send the website, but the two lines you have copied are critical lines to request a website.

Now we are going to trick the server into serving the webpage, but this time using PUTTY.

Open putty and set it up as follows:



Once the putty terminal window opens, do a right click to paste the previously copied text into the window and follow it with two ENTERs.

You should get a similar response to the 2nd wire shark packet's Hypertext Transfer Protocol and Line-based text data.

This shows that as long as you can send simple text via the network, you can retrieve a website.

Using what you have learned above. Try to do the same procedure with the website: http://tech-uofm.info/TECH3812b.html. Show the instructor when you have successfully retrieved the website in putty.

Now, without using wireshark to give you the lines of text….try to retrieve the website: http://dankohn.info/projects/galileo.html. Show the instructor when you have successfully retrieved the website in putty.

Lastly, with wireshark capturing turned on, try retrieving the 1st website using https://tech-uofm.info/TECH3812a.html. What was different? Could you use the same method using putty to

retrieve an https:// website? (hints: 1. There is NO filter for https. 2. Look for a DNS packets for https://tech-uofm.info, those packets will be right before the website packets.