Lab Assignment 1 for ECE671

Posted: 02/02/2021

Due: 02/09/2021

Step 1:
Download and install wireshark on your laptop/desktop from here:

http://www.wireshark.org/

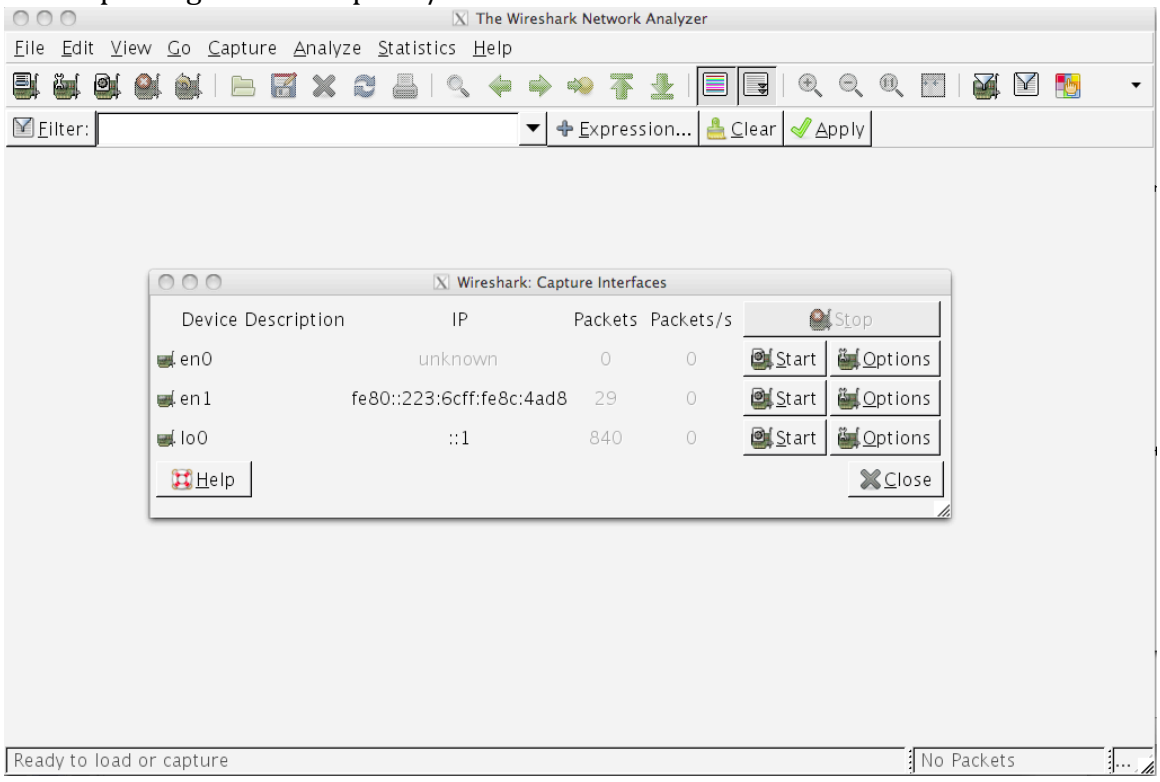
Step 2:
Read the following page to make sure you have *capture privileges:*
http://wiki.wireshark.org/CaptureSetup/CapturePrivileges

Run wireshark

*Tip for MacOS: "*sudo /Applications/Wireshark.app/Contents/MacOS/Wireshark"

Step 3:

Start capturing traffic: "Capture/Interfaces"



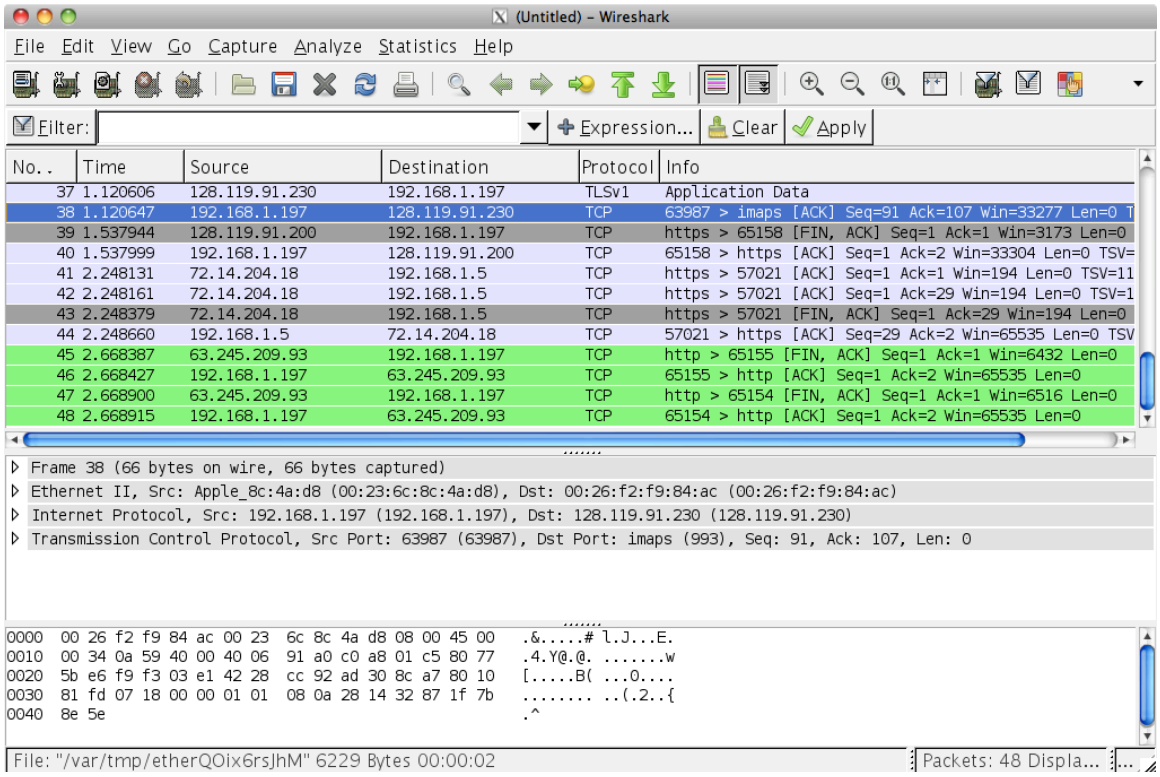
Hit "Start" on the respective interface. (In the example above it would be "en1".)

Step 4:

While continuing to capture traffic start your browser and direct it to www.ece.umass.edu

Step 5:

Stop capturing.



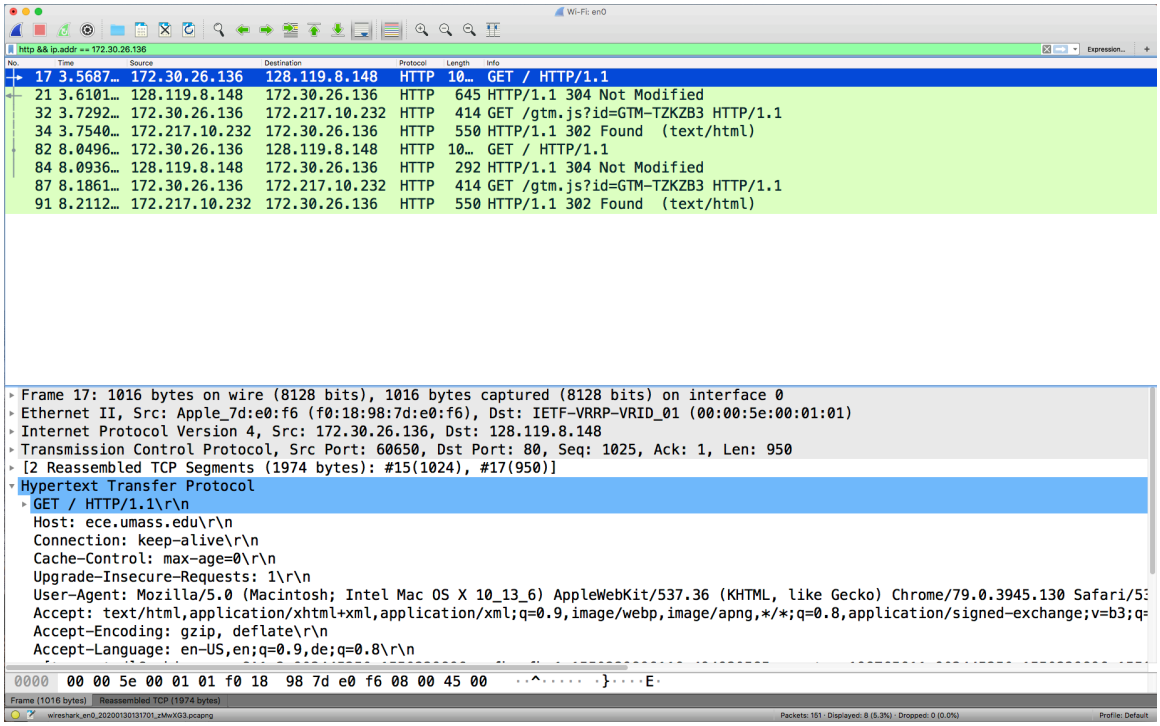
Step 6:

Filter the packets that belong to the http session between your host and the UMass web server.

Enter “http && ip.addr == 172.30.26.136” in the “Filter” field of wireshark as shown below.

Step 7:

Take a screenshot of this result. How many packets were transmitted from the UMass web server to your client in this session?


Wi-Fi: en0
http && ip.addr == 172.30.26.136
No. Time Source Destination Protocol Length Info
17 3.5687… 172.30.26.136 128.119.8.148 HTTP 10… GET / HTTP/1.1
21 3.6101… 128.119.8.148 172.30.26.136 HTTP 645 HTTP/1.1 304 Not Modified
32 3.7292… 172.30.26.136 172.217.10.232 HTTP 414 GET /gtm.js?id=GTM-TZKZB3 HTTP/1.1
34 3.7540… 172.217.10.232 172.30.26.136 HTTP 550 HTTP/1.1 302 Found (text/html)
82 8.0496… 172.30.26.136 128.119.8.148 HTTP 10… GET / HTTP/1.1
84 8.0936… 128.119.8.148 172.30.26.136 HTTP 292 HTTP/1.1 304 Not Modified
87 8.1861… 172.30.26.136 172.217.10.232 HTTP 414 GET /gtm.js?id=GTM-TZKZB3 HTTP/1.1
91 8.2112… 172.217.10.232 172.30.26.136 HTTP 550 HTTP/1.1 302 Found (text/html)
Frame 17: 1016 bytes on wire (8128 bits), 1016 bytes captured (8128 bits) on interface 0
Ethernet II, Src: Apple_7d:e0:f6 (f0:18:98:7d:e0:f6), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
Internet Protocol Version 4, Src: 172.30.26.136, Dst: 128.119.8.148
Transmission Control Protocol, Src Port: 60650, Dst Port: 80, Seq: 1025, Ack: 1, Len: 950
[2 Reassembled TCP Segments (1974 bytes): #15(1024), #17(950)]
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
Host: ece.umass.edu\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9,de;q=0.8\r\n
0000 00 00 5e 00 01 01 f0 18 98 7d e0 f6 08 00 45 00
Frame (1016 bytes) Reassembled TCP (1974 bytes)
wireshark_en0_20200130131701_zMwXG3.pcapng
Packets: 151 · Displayed: 8 (5.3%) · Dropped: 0 (0.0%)
Profile: Default