

## Lab Assignment 1 for ECE374

Posted: 01/26/15

Due: 02/02/15

### 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*:

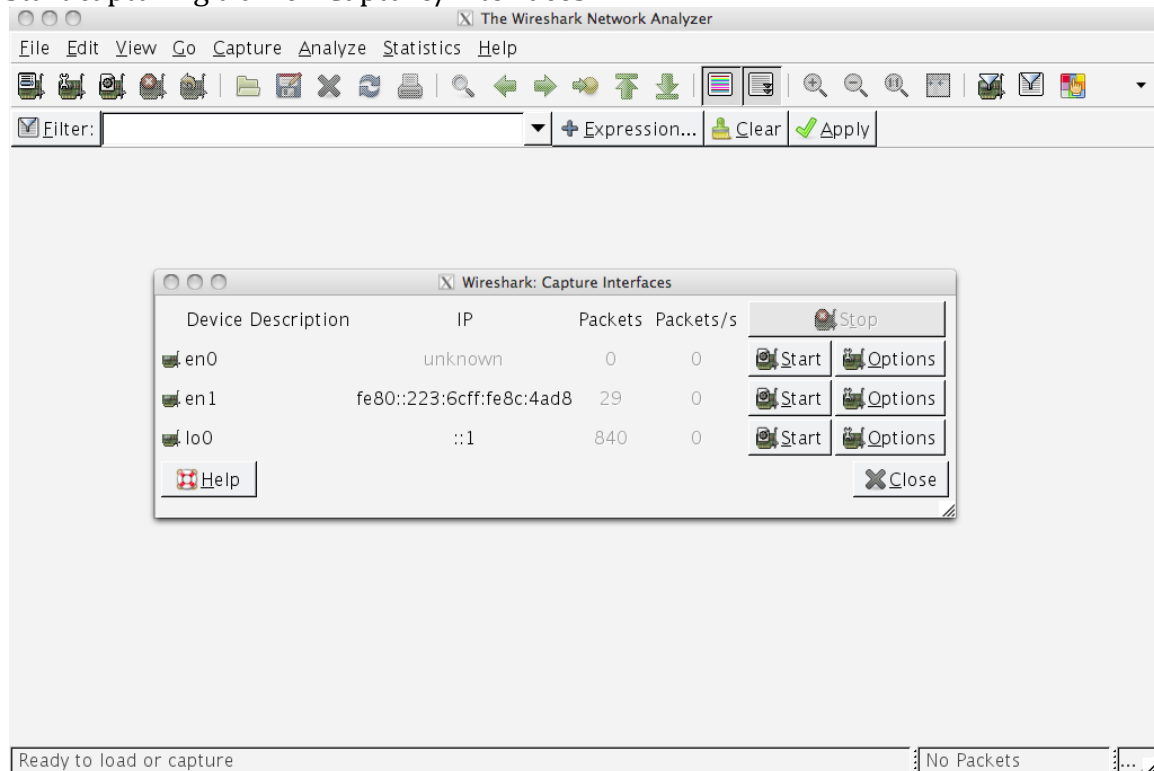
<http://wiki.wireshark.org/CaptureSetup/CapturePrivileges>

Run wireshark

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

### Step 3:

Start capturing traffic: “Capture/Interfaces”



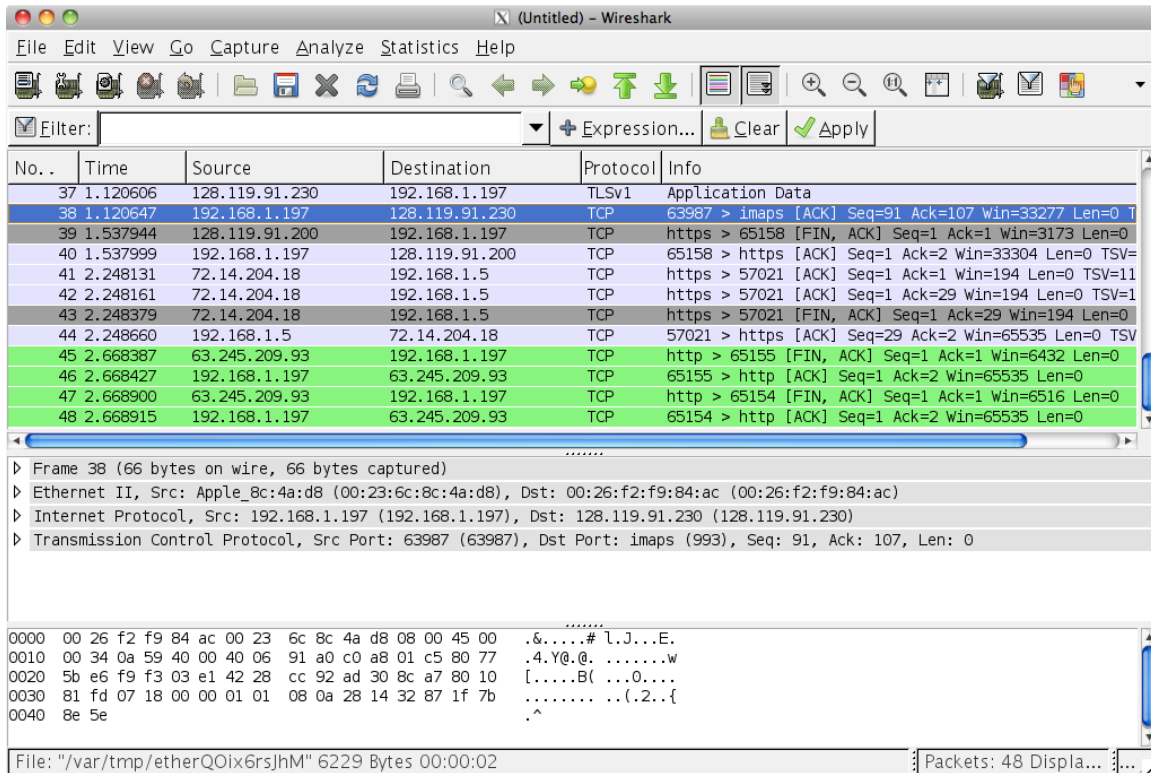
Hit “Start” on the respective interface. (In the example above it would be “en1”.)

#### Step 4:

While continuing to capture traffic start your browser and direct it to [www.umass.edu](http://www.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==128.119.103.148" 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?

The screenshot shows the Wireshark interface with a packet capture filter set to `http && ip.addr==128.119.103.13`. The packet list displays several HTTP packets. Packet 7 is selected, showing a GET request for `/umhome/cms/media/images/1239.jpg` from `192.168.1.197` to `128.119.103.13`. The packet details pane shows the layers: Ethernet II, Internet Protocol, Transmission Control Protocol, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Info
7	1.396168	192.168.1.197	128.119.103.13	HTTP	GET /umhome/cms/media/images/1239.jpg HTTP/1.1
66	1.475848	128.119.103.13	192.168.1.197	HTTP	HTTP/1.1 200 OK (JPEG JFIF image)
81	2.596633	192.168.1.197	128.119.103.13	HTTP	GET / HTTP/1.1
85	2.628658	128.119.103.13	192.168.1.197	HTTP	Continuation or non-HTTP traffic
87	2.630593	128.119.103.13	192.168.1.197	HTTP	Continuation or non-HTTP traffic
89	2.647664	128.119.103.13	192.168.1.197	HTTP	Continuation or non-HTTP traffic
91	2.648126	128.119.103.13	192.168.1.197	HTTP	Continuation or non-HTTP traffic
101	2.670349	128.119.103.13	192.168.1.197	HTTP	Continuation or non-HTTP traffic
102	2.670618	128.119.103.13	192.168.1.197	HTTP	Continuation or non-HTTP traffic
104	2.671349	128.119.103.13	192.168.1.197	HTTP	Continuation or non-HTTP traffic
106	2.679028	128.119.103.13	192.168.1.197	HTTP	Continuation or non-HTTP traffic
107	2.680281	128.119.103.13	192.168.1.197	HTTP	Continuation or non-HTTP traffic

Frame 7 (837 bytes on wire, 837 bytes captured)

- Ethernet II, Src: Apple\_8c:4a:d8 (00:23:6c:8c:4a:d8), Dst: 00:26:f2:f9:84:ac (00:26:f2:f9:84:ac)
- Internet Protocol, Src: 192.168.1.197 (192.168.1.197), Dst: 128.119.103.13 (128.119.103.13)
- Transmission Control Protocol, Src Port: 65222 (65222), Dst Port: http (80), Seq: 1, Ack: 1, Len: 783
- Hypertext Transfer Protocol

0000 00 26 f2 f9 84 ac 00 23 6c 8c 4a d8 08 00 45 00 .&....# \.J...E.  
0010 03 37 9f 32 40 00 40 06 ee 9c c0 a8 01 c5 80 77 .7.2@.@. ....w  
0020 67 0d fe c6 00 50 0b 5c d2 87 be fb 25 ee 50 18 g....P.\ ....%.P.  
0030 ff ff d4 31 00 00 47 45 54 20 2f 75 6d 68 6f 6d ...1..GE T /umhom  
0040 65 2f 63 6d 73 2f 6d 65 64 69 61 2f 69 6d 61 67 e/cms/me dia/imag  
0050 65 73 2f 31 32 33 39 2e 6a 70 67 20 48 54 54 50 es/1239. jpg HTTP

File: "/var/tmp/etherT40cgvIOCo" 289 KB 00:00:03 Packets: 765 Displ...

Submit the screenshot and the answer to the question in step 7 in moodle!!