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 captu	ring traffic: "Ca	apture/Interface	s"					
000		🛛 The Wireshar	rk Network	Analyzer				
<u>File</u> <u>E</u> dit <u>V</u> iew	v <u>G</u> o <u>C</u> apture <u>A</u> naly	ze <u>S</u> tatistics <u>H</u> elp			_			
			🤏 春	<u> </u>	7 •		- 🕰 🗹	-
🗹 <u>F</u> ilter:		▼ 4	<u>Express</u>	ion 🔒 <u>C</u>	lear 🍕 🛆	pply		
	000	🗴 Wireshark: Cap	ture Interfa	ces				
	Device Description	IP	Packets	Packets/s		Stop		
	🛒 en0	unknown	0	0	<mark>∭</mark> _Start	<u>الله O</u> ptions		
	🛒 en 1	fe80::223:6cff:fe8c:4ad8	29	0	<mark>∭</mark> _Start	<u>الله O</u> ptions		
	io0 €	::1	840	0	<mark>≧≴</mark> £art	<u>الله O</u> ptions		-
	🔀 <u>H</u> elp					XClose		
							1.	
Ready to load o	r capture					I N	lo Packets	··· //

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 <u>www.umass.edu</u>

Step 5:

Stop capturing.

0 0	🖲 🔿 🔿 📉 (Untitled) - Wireshark					
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>C</u>	<u>G</u> o <u>C</u> apture <u>A</u> nalyze	<u>S</u> tatistics <u>H</u> elp				
Bi 🕷 🚳 🚳	🏟 🖿 🗔 🗶 😂		🗼 🥺 猜		0, 🖭 🍑 🔟 📑 🛛 🔹	
₩ <u>F</u> ilter:			▼ 🕈 <u>E</u> xpressi	on <u> C</u> lear <i> A</i> pply		
No Time	Source	Destination	Protoco	Info	*	
37 1.120606	128.119.91.230	192.168.1.197	TLSv1	Application Data		
38 1.120647	192.168.1.197	128.119.91.230	TCP	63987 > imaps [ACK] Seq=	=91 Ack=107 Win=33277 Len=0 T	
39 1.537944	128.119.91.200	192.168.1.197	TCP	https > 65158 [FIN, ACK]	Seq=1 Ack=1 Win=3173 Len=0	
40 1.537999	192.168.1.197	128.119.91.200	TCP	65158 > https [ACK] Seq=	=1 Ack=2 Win=33304 Len=0 TSV=	
41 2.248131	72.14.204.18	192.168.1.5	TCP	https > 57021 [ACK] Seq=	=1 Ack=1 Win=194 Len=0 TSV=11	
42 2.248161	72.14.204.18	192.168.1.5	TCP	https > 57021 [ACK] Seq=	=1 Ack=29 Win=194 Len=0 TSV=1	
43 2.248379	72.14.204.18	192.168.1.5	TCP	https > 57021 [FIN, ACK]	Seq=1 Ack=29 Win=194 Len=0	
44 2.248660	192.168.1.5	72.14.204.18	TCP	57021 > https [ACK] Seq=	=29 Ack=2 Win=65535 Len=0 TSV	
45 2.668387	63.245.209.93	192.168.1.197	TCP	http > 65155 [FIN, ACK]	Seq=1 Ack=1 Win=6432 Len=0	
46 2.668427	192.168.1.197	63.245.209.93	TCP	65155 > http [ACK] Seq=1	. Ack=2 Win=65535 Len=0	
47 2.668900	63.245.209.93	192.168.1.197	TCP	http > 65154 [FIN, ACK]	Seq=1 Ack=1 Win=6516 Len=0	
48 2.668915	192.168.1.197	63.245.209.93	TCP	65154 > http [ACK] Seq=1	. Ack=2 Win=65535 Len=0 🛛 🐺	
▲						
▷ Frame 38 (66 bvt	es on wire. 66 bytes ca	aptured)				
Ethernet II Src	· Apple 8c·4a·d8 (00·2	3.6c.8c.4a.d8)	Dst. 00.26.f2.f	9.84.ac (00.26.f2.f9.84.a	ic)	
A Internet Brotoco	- Apple_001 14100 (0012)	(102 169 1 107)	Det. 120 110 0			
Thermet Protoco	teal Destand Car Dest	(192.100.1.197),	Dat Dast das	(128.119.91.230)	07 1	
P Transmission Con	ITFOL PROTOCOL, SFC PORT	: 63987 (63987)	, DST Port: ima	ps (993), Sed: 91, Ack: 1	.07, Len: 0	
0000 00 26 f2 f9 8	34 ac 00 23 6c 8c 4a d	8 08 00 45 00	.&#l.J</td><td>E.</td><td><u> </u></td></tr><tr><td>0010 00 34 0a 59 4</td><td>40 00 40 06 91 a0 c0 a</td><td>B 01 c5 80 77</td><td>.4.Y@.@</td><td>W</td><td></td></tr><tr><td>0020 5b e6 f9 f3 0</td><td>03 e1 42 28 cc 92 ad 3</td><td>0 8c a7 80 10</td><td>LB(0.</td><td>••</td><td></td></tr><tr><td>0030 81 fd 07 18 0</td><td>00 00 01 01 08 0a 28 1</td><td>4 32 87 1† 7b</td><td></td><td></td><td></td></tr><tr><td>0040 8e 5e</td><td></td><td></td><td>•</td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td colspan=7>File: "/var/tmp/etherQOix6rsJhM" 6229 Bytes 00:00:02 Packets: 48 Displa</td></tr></tbody></table>			

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?

000	🔿 🔿 🔿 🔯 (Untitled) - Wireshark					
<u>File Edit View Go Capture Analyze Statistics H</u> elp						
🗐 🕷 🚳 🕷	🍬 🖿 🗔 🗙 😂	8 9 4) 🔶 🐳 🛧 🛃 🔲 💽 ! Q, Q, Q, 🖭 🕁 🕅 📑 🔹			
🗹 Filter: http && ip.addr==128.119.103.13 💌 🕈 Expression 🚢 Clear 🎺 Apply						
No Time	Source	Destination	Protocol Info			
7 1.396168	192.168.1.197	128.119.103.13	B 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	B 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	HIP CONTINUATION OF NON-HIP TRATTIC			
01 2 649126	128.119.103.13	192.168.1.19/	HTTP Continuation or non-HTTP traffic			
101 2 6703/9	128 119 103 13	192.160.1.19/	HTTP Continuation of 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			
4						
▶ Frame 7 (837 byt	es on wire. 837 bytes	captured)				
▶ Ethernet II. Sro	: Apple 8c:4a:d8 (00:2	3:6c:8c:4a:d8)	Dst: 00:26:f2:f9:84:ac (00:26:f2:f9:84:ac)			
D Internet Protoco	1 Src 192 168 1 197	(192 168 1 197)	Dst. 128 119 103 13 (128 119 103 13)			
A Transmission Con	trol Protocol Src Por	t. 65222 (65222)) Det Port: http (80) Seg: 1 Ack: 1 Lep: 783			
A Hypertext Transf	ier Protocol	C. 05222 (05222)	, bat for t. http (00), bed. 1, Ack. 1, Ech. 705			
v Hypertext Halist	er Frotocot					
0000 00 26 f2 f9 8	34 ac 00 23 6c 8c 4a d	8 08 00 45 00	.&# 1.JE.</td></tr><tr><td>0010 03 3/ 9t 32 4</td><td>40 00 40 06 ee 9c c0 a</td><td>8 01 c5 80 //</td><td>./.2@.@W</td></tr><tr><td>0020 67 00 Te C6 0</td><td>00 00 00 00 00 02 87 De 1</td><td>D 20 EE 00 18</td><td>9P.\</td></tr><tr><td>0040 65 2f 63 6d 7</td><td>73 2f 6d 65 64 69 61 2</td><td>f 69 6d 61 67</td><td>e/cms/me_dia/imag</td></tr><tr><td>0050 65 73 2f 31 3</td><td>32 33 39 2e 6a 70 67 2</td><td>0 48 54 54 50</td><td>es/1239. jpg HTTP</td></tr><tr><td>File: "/var/tmp/eth</td><td>herT40cavIOCo" 289 KR</td><td>00.00.03</td><td>Packets: 765 Displ</td></tr><tr><td>Junes /var/unp/eu</td><td>1011100g/1000 200 Kb</td><td>00.00.00</td><td>1 acres. 705 Dispi j</td></tr></tbody></table>			

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