1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running? HTTP 1.1 (see screenshot)

A A A	Win 7Dro22 Davalle	ls Daskton	R. E
*Local Area Connection Wireshark 1.10.6 (vi)	.10.6 from master-1.10)]	is Desktop	
File Edit View Go Canture Analyze Sta	tistics Telephony Tools Interna	ls Help	
			e
	् 🖗 🛸 🌍 ዥ 👱 🔲 🗉	∃ Q, Q, Q, M M ⊠ № %	B
Filter: http	▼ Exp	pression Clear Apply Save	
No. Time Source	Destination Protocol	Length Info	
24 1.786722000 10.211.55.3	130.215.16.168 HTTP	329 GET /wireshark/lab3part1	L.html HTTP/1.1
26 1./89103000 130.215.16.160	130 215 16 168 HTTP	458 HTTP/1.1 200 OK (Text/r 258 GET /favicon ico HTTP/1	1 (1)
36 3.193750000 130.215.16.168	3 10.211.55.3 HTTP	1477 HTTP/1.1 200 OK (text/r	lain)
80 4.911195000 10.211.55.3	70.37.128.164 HTTP	225 GET /pki/mscorp/crl/MSIT	%20Machine%20Aut
81 4.911363000 10.211.55.3	70.37.128.164 HTTP	225 GET /pki/mscorp/crl/MSIT	7%20Machine%20Aut
162 4.955759000 70.37.128.164	10.211.55.3 PKIX-CF	8L 559 Certificate Revocation L	.ist
181 4.957471000 70.37.128.164	10.211.55.3 PKIX-CF	8L 595 Certificate Revocation L	.ist
•	III		+
Frame 24: 329 bytes on wire (26	32 bits). 329 bytes capt	ured (2632 bits) on interface 0	
■ Ethernet II, Src: Parallel_a5:8	6:9d (00:1c:42:a5:86:9d)	, Dst: Parallel_00:00:18 (00:1c:4	42:00:00:18)
Internet Protocol Version 4, Sr ■	c: 10.211.55.3 (10.211.5	5.3), Dst: 130.215.16.168 (130.2)	15.16.168)
	Src Port: 63588 (63588),	Dst Port: http (80), Seq: 1, Ac	k: 1, Len: 275
Hypertext Transfer Protocol			
	HTTP/1.1 r		
Accept: text/ntml, applicatio	n/xntml+xml, */*\r\n		E
User-Agent: Mozilla/5.0 (Wind	lows NT 6.1. Trident/7.0.	rv:11.0 like Gecko r	
Accept-Encoding: gzip. deflat	e\r\n		
Host: spinlab.wpi.edu\r\n			
DNT: 1\r\n			
Connection: Keep-Alive\r\n			
\r\n		-h2	
IFUIL request URL: http://spi	nlap.wp1.edu/w1resnark/l	<u>ab3part1.ntm11</u>	-
<			4
0000 00 1c 42 00 00 18 00 1c 42	a5 86 9d 08 00 45 00	B BE.	*
0010 01 3b 03 7e 40 00 80 06 00	00 0a d3 37 03 82 d7	.;.~@7	
0030 01 00 d6 82 00 00 47 45 54	20 2f 77 69 72 65 73		
0040 68 61 72 6b 2f 6c 61 62 33	70 61 72 74 31 2e 68	hark/lab 3part1.h	-
○ 1/2 Ed. 5c 10 AV 54 54 50 14 Frame (frame), 329 bytes	Packets: 195 · Displayed: 8 (4.1	%) · Dropped: 0 (0 Profile: Default	
📀 🚞 🕸 🌼 I			♦) 1:13 PM 4/3/2014
(U +			4 🔅

- 2. What languages (if any) does your browser indicate that it can accept to the server? en-US (US English) as shown in prior screenshot
- 3. What is the IP address of your computer? Of the spinlab.wpi.edu server? My computer is 10.211.55.3 (this is a virtual IP address assigned by my virtual machine software) and the destination is 130.215.16.168. See prior screenshot.
- 4. What is the status code returned from the server to your browser? 200 OK (see prior screen-shot)
- 5. When was the HTML file that you are retrieving last modified at the server? We can filter messages by http.last_modified and we see that the HTTP response I received for the html

file doesn't show this field. We do have a http.last_modified field in the favicon response however, as shown in the screenshot below. This says the favicon was last modified on Feb 25, 2010.



6. How many bytes of content are being returned to your browser? Content-length = 209 bytes. See screenshot below.

00	💻 Win7Pro32 - Parallels Desktop	
*Local Area Connection [W	[Wireshark 1.10.6 (v1.10.6 from master-1.10)]	
<u>File Edit View Go Capte</u>	pture <u>A</u> nalyze <u>S</u> tatistics Telephony <u>T</u> ools <u>I</u> nternals <u>H</u> elp	
	e 🔚 💥 😂 🔍 🗢 🔿 春 生 🗐 🖬 O. O. O. 🗹 🎬 🗹 畅 %	
Filter: http	 Expression Clear Apply Save 	
No. ▲ Time So 24 1.786722000 1 26 1.789103000 1 33 3.191516000 1 36 3.193750000 1 80 4.911195000 1 81 4.911363000 1 162 4.955759000 7 181 4.957471000 7	Source Destination Protocol Length Info 10.211.55.3 130.215.16.168 HTTP 329 GET /wireshark/lab3part 130.215.16.168 10.211.55.3 HTTP 458 HTTP/1.1 200 OK (text/ 10.211.55.3 130.215.16.168 HTTP 258 GET /favicon.ico HTTP/1 130.215.16.168 10.211.55.3 HTTP 1477 HTTP/1.1 200 OK (text/ 10.211.55.3 70.37.128.164 HTTP 225 GET /pki/mscorp/crl/MS1 10.211.55.3 70.37.128.164 HTTP 225 GET /pki/mscorp/crl/MS1 10.211.55.3 70.37.128.164 HTTP 225 GET /pki/mscorp/crl/MS1 70.37.128.164 10.211.55.3 PKIX-CRL 595 Certificate Revocation 70.37.128.164 10.211.55.3 IM 595 Certificate Revocation <td>t1.html HTTP/1.1 /html) L.1 /plain) IT%20Machine%20Aut List List :42:a5:86:9d) 0.211.55.3)</td>	t1.html HTTP/1.1 /html) L.1 /plain) IT%20Machine%20Aut List List :42:a5:86:9d) 0.211.55.3)
➡ Transmission Contro ➡ Hypertext Transfer ➡ HTTP/1.1 200 OK\r Date: Thu, 03 Apr Server: Apache/2. Accept-Ranges: by ➡ Content-Length: :	rol Protocol, Src Port: http (80), Dst Port: 63588 (63588), Seq: 1, A r Protocol \r\n pr 2014 17:11:01 GMT\r\n 2.2.3 (Red Hat)\r\n bytes\r\n 209\r\n	ck: 276, Len: 4(≡
[Content length Connection: close Content-Type: tex \r\n [HTTP response 1,	th: 209] se\r\n ext/html; charset=I50-8859-1\r\n 1/1] 	
00a0 0d 0a 43 6f 6e 00b0 3a 20 32 30 39 00c0 6e 3a 20 63 6c 00d0 74 2d 54 79 70 00e0 6c 3b 20 63 68 00f0 2e 35 20 2d 31 ○ M Content length (http.cc	e 74 65 6e 74 2d 4c 65 6e 67 74 68 9 0d 0a 43 6f 6e 6e 65 63 74 69 6f c 6f 73 65 0d 0a 43 6f 6e 74 65 6e 0 65 3a 20 74 65 78 74 2f 68 74 6d 6 1 72 73 65 74 3d 49 53 4f 2d 38 1 0d 0a 0d 0a 2c 68 74 6d 6c 2a 2c content_length), 21 byt Packets: 195 · Displayed: 8 (4.1%) · Dropped: 0 (0 Profile: Default	↓ ↓ 1:20 PM
0		4/3/2014

- 7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one. No. The raw data appears to match up exactly with what is shown in the packet-listing window.
- 8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET? No.
- 9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell? See screenshot of response with Alice's Adventures...

00	Win7Pro32 – Parallels Desktop	E K
*Local Area Conr	nection [Wireshark 1.10.6 (v1.10.6 from master-1.10)]	х
<u>File Edit V</u> iew	<u>Go</u> <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics Telephony <u>T</u> ools <u>I</u> nternals <u>H</u> elp	
0 0 🖌 🔳	🔬 😑 🔚 🗶 😂 🍳 🗢 🌳 🛜 👱 🗐 🗐 Đ, Q, Q, 🖻 🌉 🗹 🕵 % 💢	
Filter: http && tcp	p Expression Clear Apply Save	
No. Time	Source Destination Protocol Length Info	
14 0.1193	12000 10.211.55.3 130.215.16.168 HTTP 407 GET /wireshark/alice.txt HTTP/1.1	
138 0.1469	0/000 130.215.16.168 10.211.55.3 HTTP 113/HTTP/1.1 200 0K (text/plain)	
149 2.6427	24000 10.211.51.6.168 10.211.55.3 HTTP 215 HTTP/1.1 304 Not Modified	
•		
[Time sin	ice request: 0.02/595000 seconds]	-
Line-based	text data: text/plain	
	ALICE'S ADVENTURES IN WONDERLAND\r\n	
\r\n		
\r\n	Lewis Carroll\r\n	
\r \r	THE MILLENNIUM FULCRUM EDITION 3.0\r\n	
\r\n		
\r\n		
\r\n \r\n		
\r \r	CHAPTER I\r\n	
\r\n		-
<	III	•
0000 00 1c 4	2 a5 86 9d 00 1c 42 00 00 18 08 00 45 00B BE.	
0010 04 63 9	15 b5 00 00 80 06 cb 8a 82 d7 10 a8 0a d3 .c	
Frame (1137 bytes)	Reassembled TCP (15242/ bytes)	
🔵 💅 🛛 File: "C:\Use	rs\drb\AppData\Local\Temp\wi Packets: 153 · Displayed: 4 (2.6%) · Dropped: 0 (0 Profile: Default	
	- 🗣 🎬 📶 🔽 🧿 🧲	PM 014
<u>ଓ</u>		*

10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? If so, what information follows the "IF-MODIFIED-SINCE:" header? Yes.

If-Modified-Since: Wed, 12 Mar 2014 17:29:08 GMT\r\n.

See screenshot below.



- 11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain. As seen in the previous screenshot, we get a HTTP/1.1 304 Not Modified Response. This is much shorter than the full response packet seen previously which contained all of Alice in Wonderland.
- 12. How many HTTP GET request messages were sent by your browser (again, ignoring requests for favicon.ico)? Just one.
- 13. How many data-containing TCP segments were needed to carry the single HTTP response? From the screenshot below, there are 4 TCP segments.

● ○ ○ ■ Win7Pro32 – Parallels Desktop	- K2
*Local Area Connection [Wireshark 1.10.6 (v1.10.6 from master-1.10)]	o x
<u>File E</u> dit <u>V</u> iew <u>Go</u> <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics Telephony <u>T</u> ools <u>I</u> nternals <u>H</u> elp	
◉ ◉ ∡ ■ ゑ ⊨ ≞ ೫ ₴ < ⇔ ⇔ ₮ ⊻ 目目 € < @ ऌ ₩ № № ₩	
Filter: http && tcp Expression Clear Apply Save	
No. Time Source Destination Protocol Length Info 9 0.005449000 10.211.55.3 130.215.16.168 HTTP 412 GET /wireshark/lab3part3.html H 14 0.008480000 130.215.16.168 10.211.55.3 HTTP 500 HTTP/1.1 200 OK (text/html)	ттр/1.1
< ا	
A Frame 14: 500 bytes on whe (4000 bits), 500 bytes captured (4000 bits) on interface o E thernet II, Src: Parallel_00:00:18 (00:1c:42:00:00:18), Dst: Parallel_a5:86:9d (00:1c:42:a5:86 Internet Protocol Version 4, Src: 130.215.16.168 (130.215.16.168), Dst: 10.211.55.3 (10.211.55. Transmission Control Protocol, Src Port: http (80), Dst Port: 64439 (64439), Seq: 4357, Ack: 35 [4 Reassembled TCP Segments (4802 bytes): #11(1460), #12(1436), #13(1460), #14(446)] [Frame: 11, payload: 0-1459 (1460 bytes)] [Frame: 12, payload: 1460-2895 (1436 bytes)] [Frame: 14, payload: 2896-4355 (1460 bytes)] [Frame: 14, payload: 4356-4801 (446 bytes)] [Segment count: 4] [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2054]	:9d) [3) 9, Len
☐ UTTD (4, 4, 300, 00) w) w	•
0030 40 00 19 63 ee fc 67 3e 3c 68 33 3e 41 6d 65 6e (0cg> <h3>Amen 0040 64 6d 65 67 20 49 58 3c 2f 68 33 3e 3c 2f 66 3a 3e 3c 2f 68 33 3e 3c 2f 66 3a 3e 3c 2f 7a dment IX <h3> 66 7a 3e 3c 7f 3e trong> <h3> ac 7f 3e trong> <h3> >h <h3> fc fc</h3></h3></h3></h3></h3>	E
Frame (500 bytes) Reassembled TCP (4802 bytes)	
⊖ 🛃 File: "C:\Users\drb\AppData\Local\Temp\wi Packets: 26 · Displayed: 2 (7.7%) · Dropped: 0 (0 Profile: Default	
📀 🚞 🕸 🌺 🖭 📶 💽 🥭 🔺 🕨 🗊	5:51 PM 4/3/2014
(Ů •)	 A A

- 14. What is the status code and phrase associated with the response to the HTTP GET request? HTTP/1.1 200 OK (as seen in previous screenshot)
- 15. Are there any HTTP status lines in the transmitted data associated with a TCP- induced "Continuation"? No.
- 16. How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent? Three: 130.215.16.168, 130.215.36.26, 208.122.28.10. See screenshot below.



- 17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain. Based on the timestamps, it appears the images were downloaded serially. Also, the source port is incrementing each time from 64444, 64445, 64446 which means that the images were received serially over separate TCP connections.
- 18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser? HTTP/1.1 401 Authorization Required (see screenshot below)



19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message? Authorization field. See screenshot below.



20. Copy the string of text that appears after "Authorization: Basic", and enter it into the Base64 decoder here - http://www.motobit.com/util/base64-decoder-encoder.asp. Make sure to click on "decode". To what ASCII string does the Base64 string decode to? (Hint: you should see the username and password for the course website embedded in the string). No need since Wireshark has already done the decoding. See the previous screenshot. Our credentials are clearly visible in Wireshark.