Ethan Chan

2:00pm-3:30pm

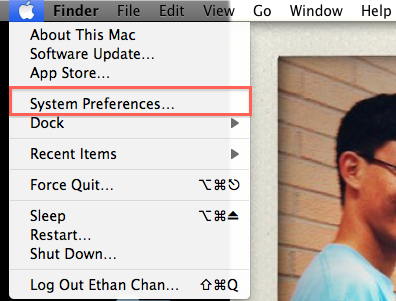
EE450

**LAB 2: Wireshark**

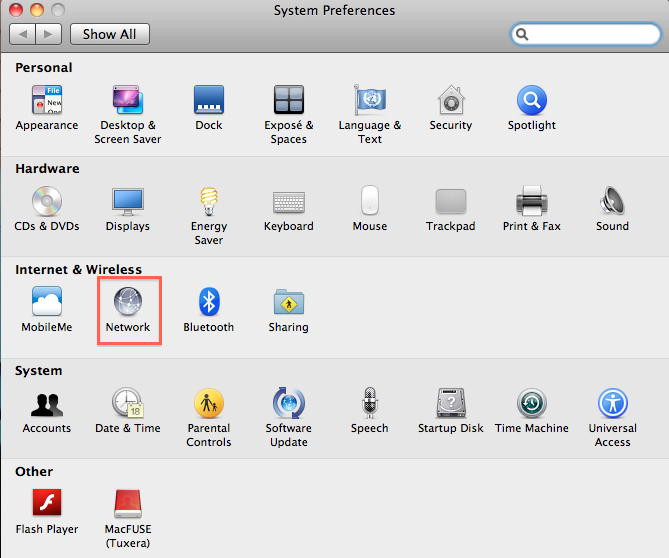
**Part I**

To release and renew a host IP address for a Mac computer one must:

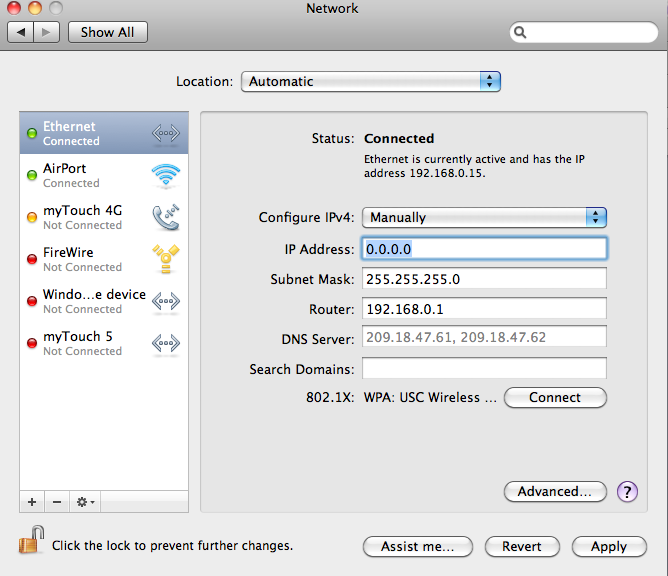
1) Click the Apple located at the top left hand corner of the desktop and select “System Preferences…"



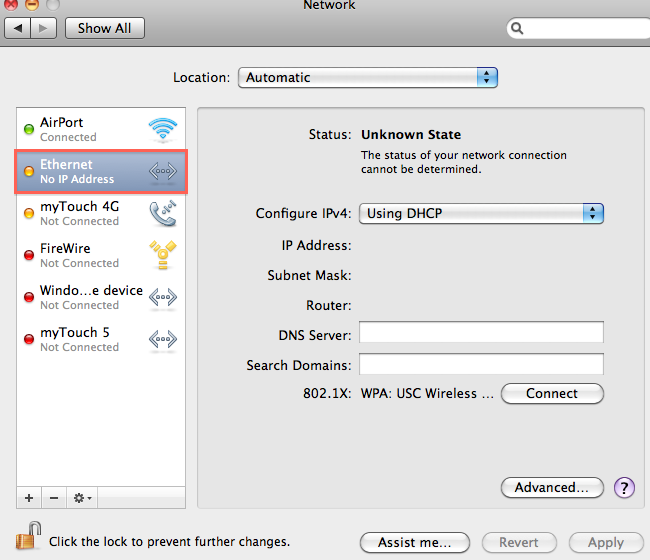
2) In the System Preferences Window select the “Network” icon



3) The equivalent of “ipconfig/release” command in the Command Window Prompt is to select “Configure IPv4”, setting it “Manually”, and setting the IP Address as 0.0.0.0.

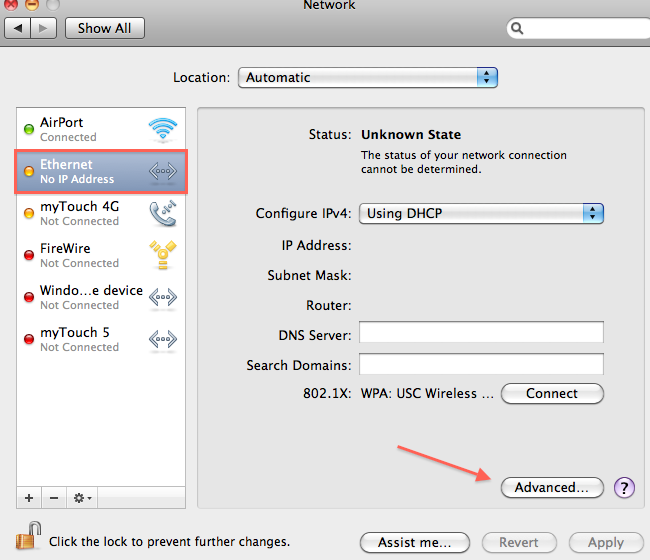


4) And this leads the Ethernet port on the left column to read “No IP address”

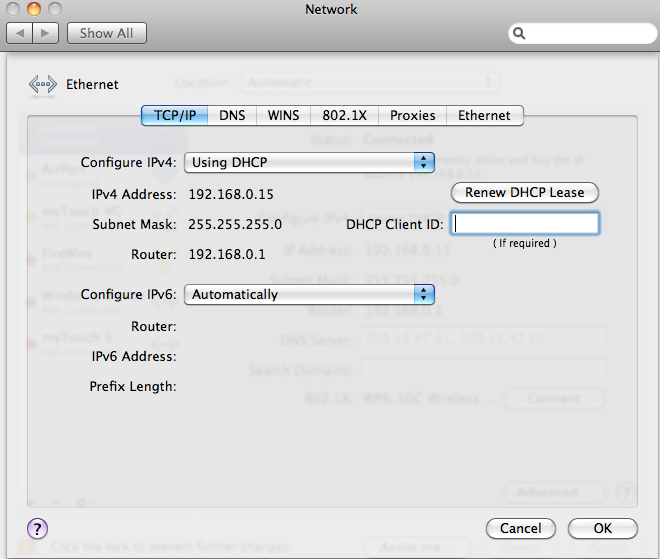


5) The equivalent to “ipconfig/renew” is a two step process:

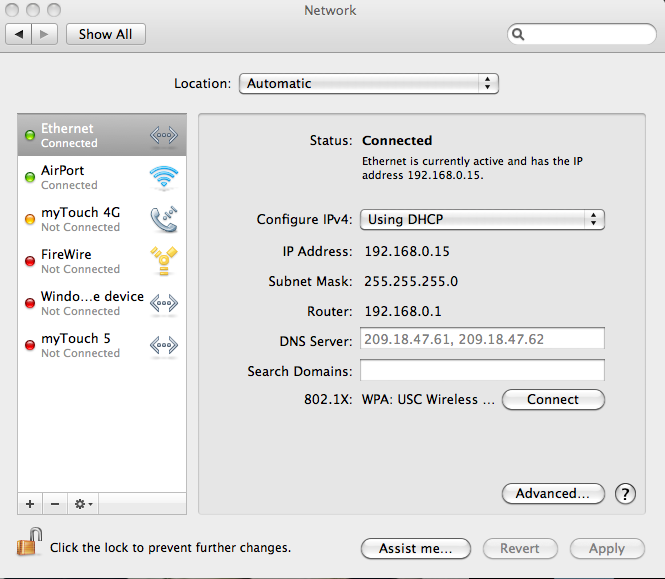
a) Click the “Advanced” option



b) Click “Renew DHCP Lease”



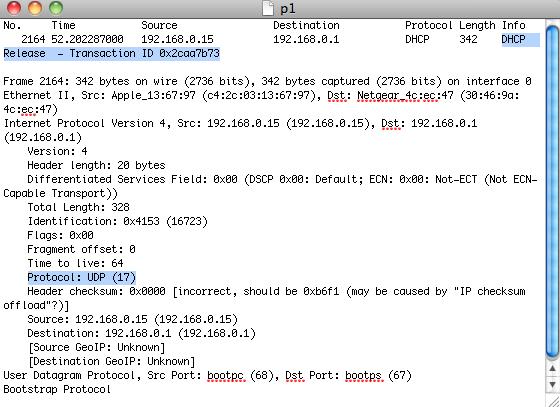
6) DHCP renews your IP address!

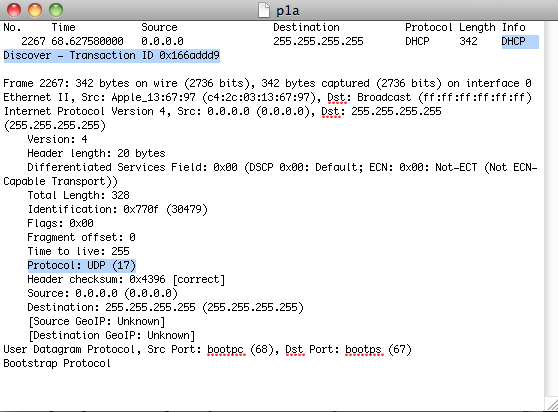


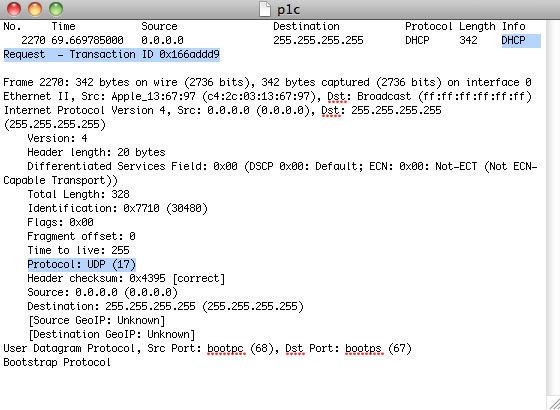
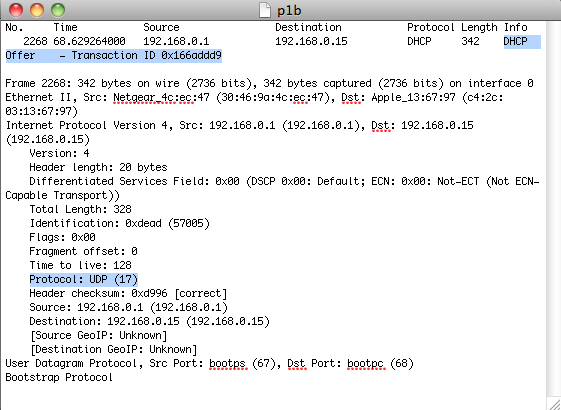
DHCP Questions:

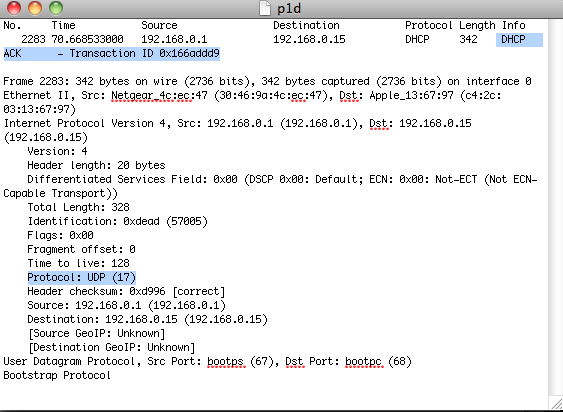
1) The DHCP messages are NOT sent over TCP but rather through UDP

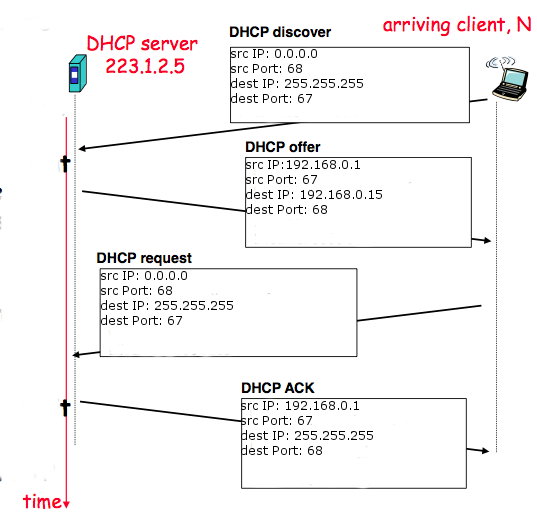
Looking at the all the DHCP messages and we can see that they all use UDP protocol

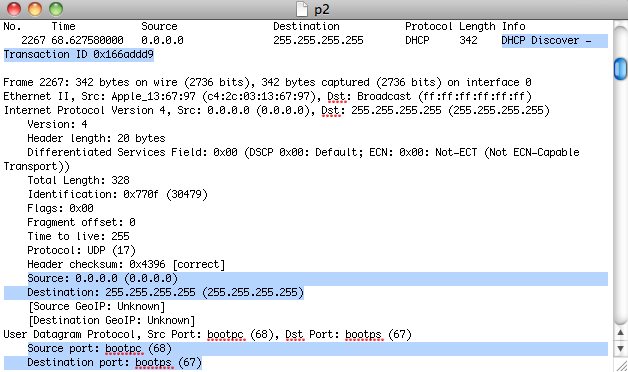


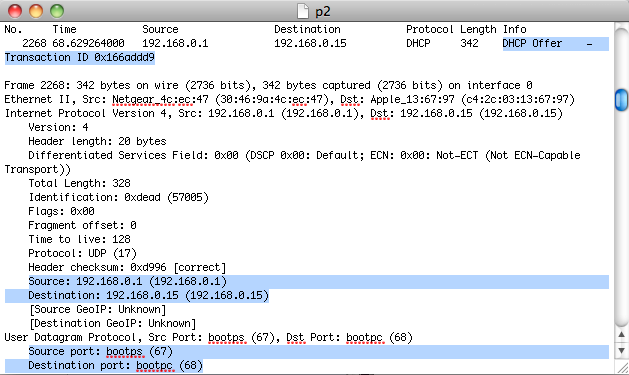


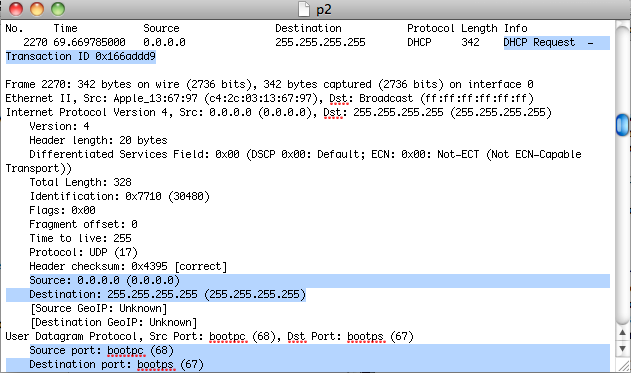


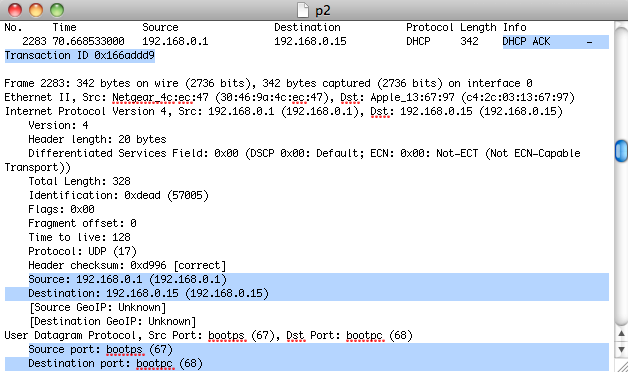


2) 



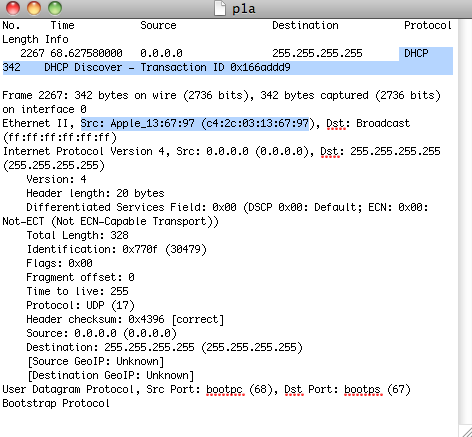




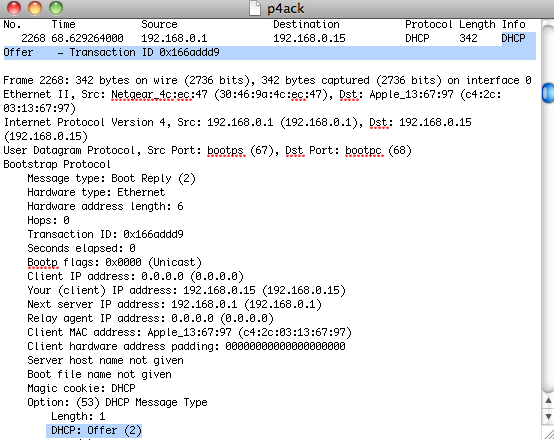


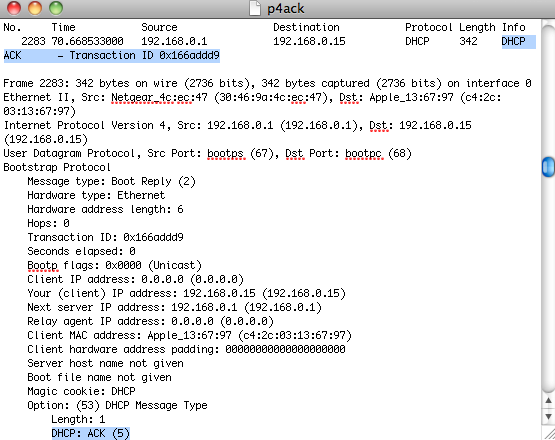
The port numbers 67 and 68 used in my DHCP message protocolsare the same port numbers used in example in the lab assignment.

3) The link-layer address of my host in numeric and hex format is Apple\_13:69:97 and c4:2c:03:13:69:97 respectively.

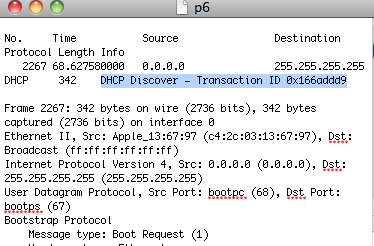


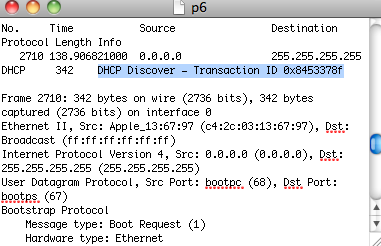
4) The differing values between DHCP Offer messages and DHCP ACD messages is the DHCP Message type. For DHCP Offer the value is 2 and for DHCP ACK the value is 5.



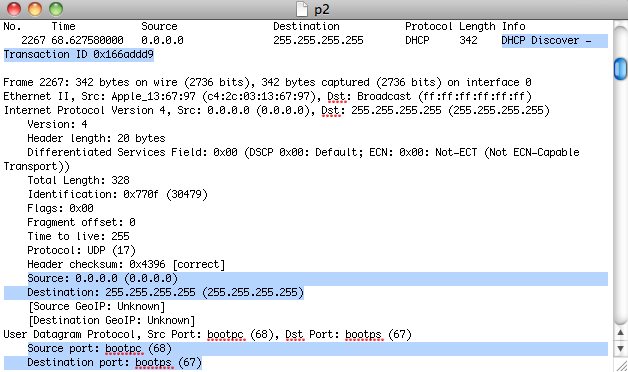


5) The Transaction-Ids were “0x166add9” and “0x8453378f” for the first and second messages respectively. We need Transaction-ID field to distinguish between the different DHCP transactions from the different hosts that are trying to obtain IP addresses.

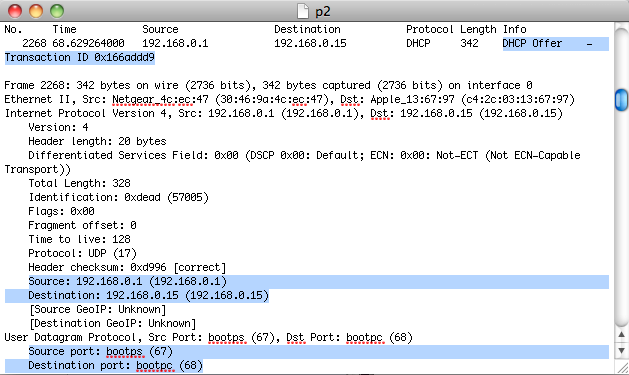




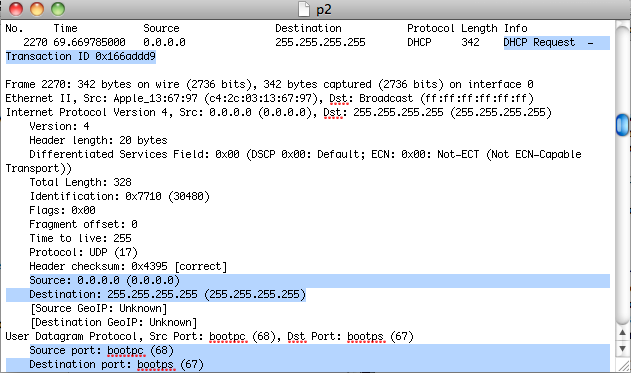
6) Initially the host has no IP address so it sets its own source IP address to be 0.0.0.0, which indicates that it needs an IP address. The source wants to communicate with the DHCP server but it does not know the IP address of the DHCP server. The discover message broadcasts its signal. The destination IP address is set as 255.255.255.255 which is a broadcasted signal.



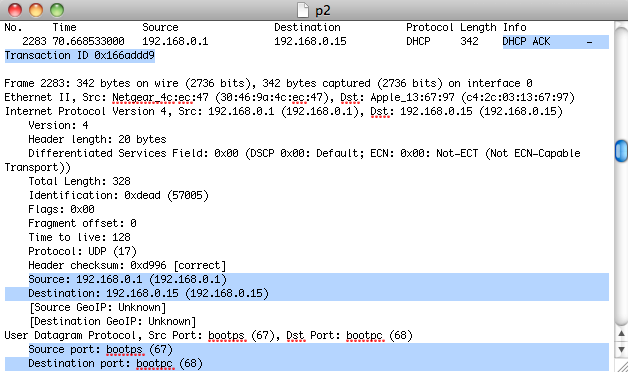
The DHCP discover message is picked up by only the DHCP server and dropped by all the rest. The DHCP server responds with a DHCP offer message that offers an IP address. The source IP address is that of the DHCP server and the destination IP address is usually broadcasted with 255.255.255.255. In this case the destination IP address is being set to the IP address that the DHCP server is offering to the host.



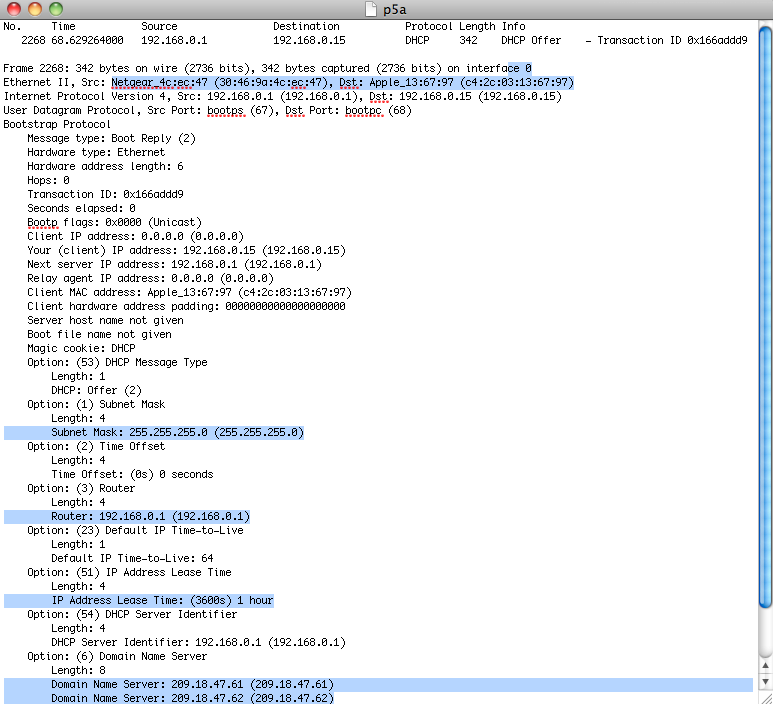
The host node receives the offer and decides to request for it. The DHCP request message still has a source IP address as 0.0.0.0 because the IP address has yet to be assigned to that host yet and the destination IP address is once again broadcasted. Since the DHCP IP address is known now, the Destination IP address can be unicasted, however in this case it is broadcasted.



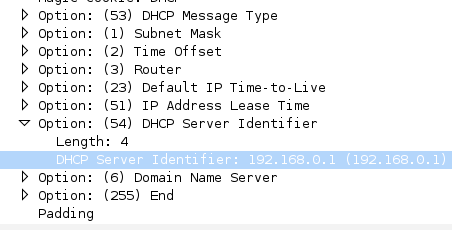
The DHCP server then responds to the request with an ACK message. The DHCP server sets its source IP address as its own IP address and the destination IP address is set as the address that the server is acknowledging that it is giving over to the host.



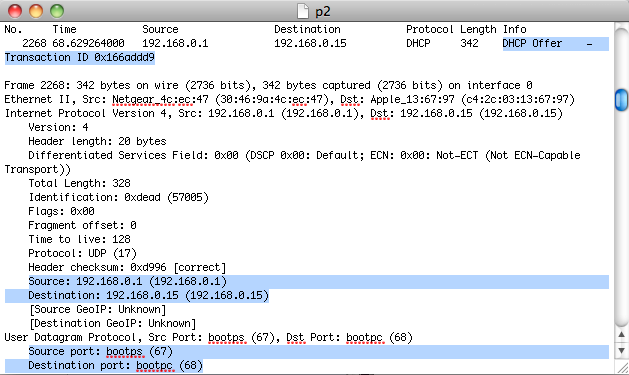
Other information: The DHCP server also lets the host know the MAC address and IP address of the DHCP server, the subnet mask, the default router, the IP address lease time, and the local DNS server’s IP address.



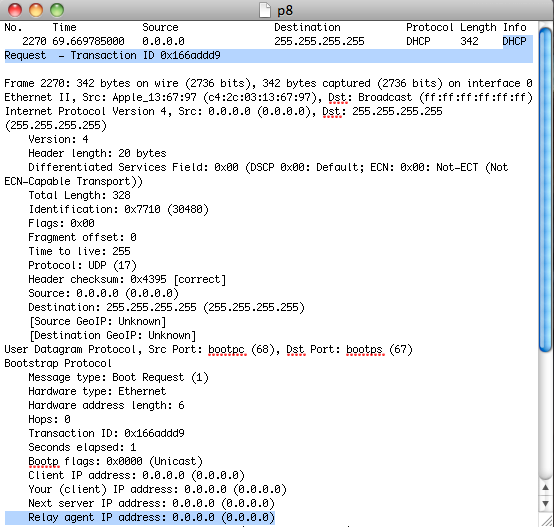
7) The IP address of my DHCP server is 192.168.0.1



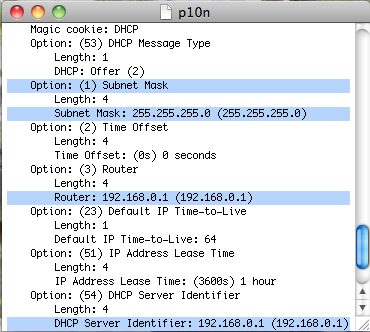
8) The DHCP server offers the IP address “192.168.0.1” to the host through the DHCP Offer message



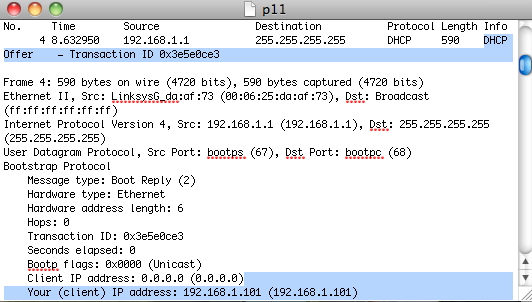
9) The values 0.0.0.0 indicate the absence of a relay agent. In my experiment there is no relay agent.

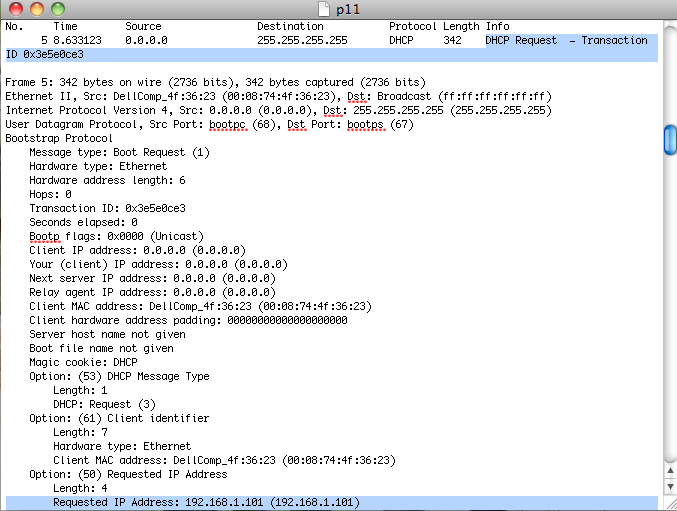


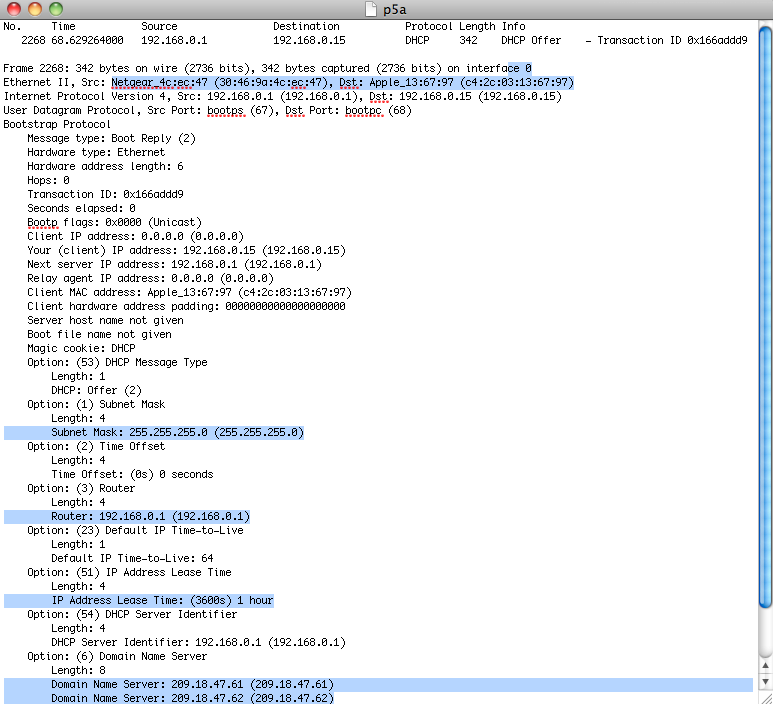
10) The purpose of the subnet mask is to compare the destination and source IP addresses to see if they are of the same local network. If they are not of the same local network the local router will be needed to see if it is connected to another local network that has a DHCP server. The IP address of the default gateway is 192.168.0.1 and the subnet Mask is 255.255.255.0. It looks like my router might include DHCP services as well.



11) By looking at the Offer and Request messages, it looks like the client accepted the IP address offered in the offered message.

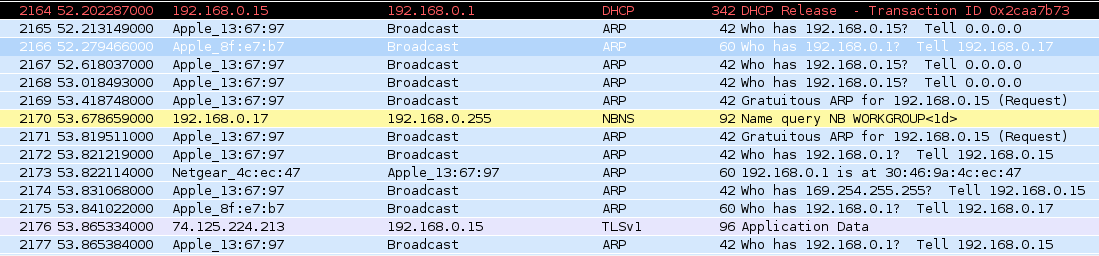




12) The purpose of the lease time is so as to not dedicate a path for a host because there are limited connections to be offered. The lease time is 1 hour.

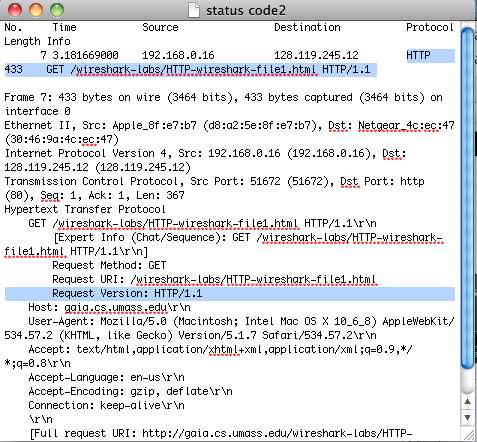
13) The purpose of the DHCP release message is to give up it (release) its dynamically allocated IP address. The DHCP server does not issue an acknowledgement of receiving the DHCP’s release message. If the release message were lost, there an IP address would be dedicated to one host and could lead to congestion of the network unless the DHCP automatically releases that IP address after the lease time is up.

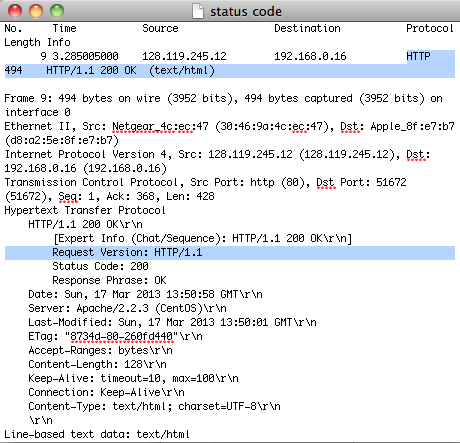
14) Yes there were ARP packets sent. These packets are used to navigate from router to router to reach the DHCP server and back to the host because although source and destination IP addresses do not change during transmission, the physical addresses do especially if it takes multiple hops to reach the final destination.



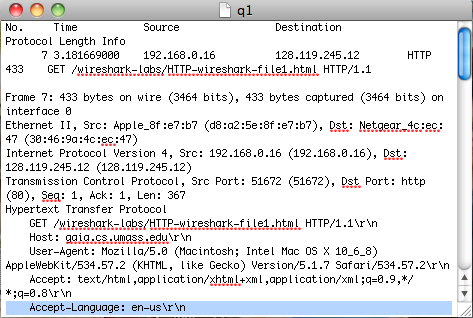
**Part II**

1. Both the server and the browser are running on HTTP version 1.1

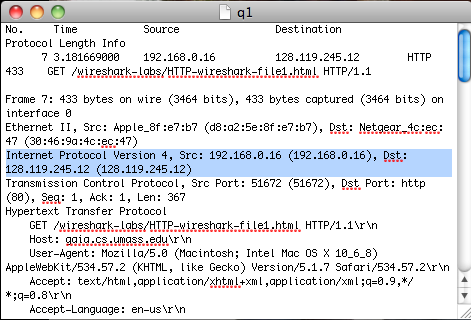




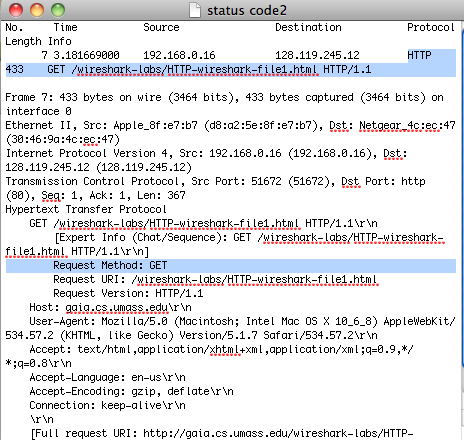
2. My browser indicates that it can accept English (“en-us\r\n”) to the server.

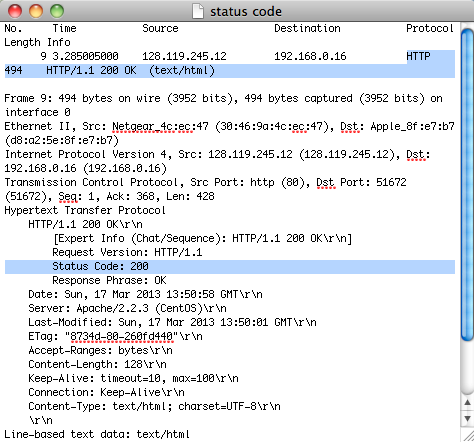


3. The IP address of my computer is 192.168.0.16 and the IP address of giao.cs.umass.edu server is 128.119.245.12

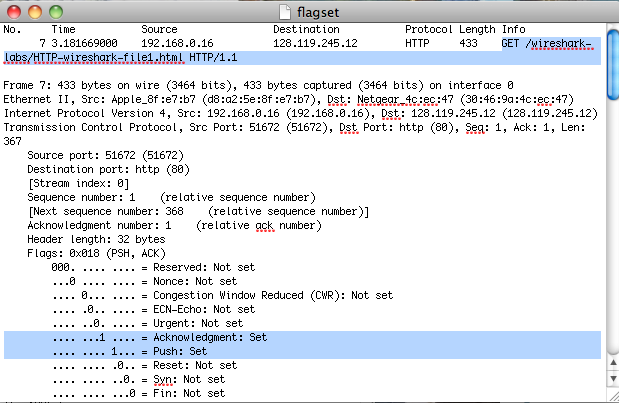


4. Status code sent from browser to server is “GET” and status code returned from server to browser is 200. Responding with “OK”

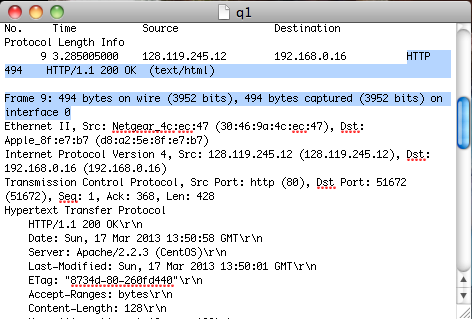




5. The Acknowledgment and Push flags were set.

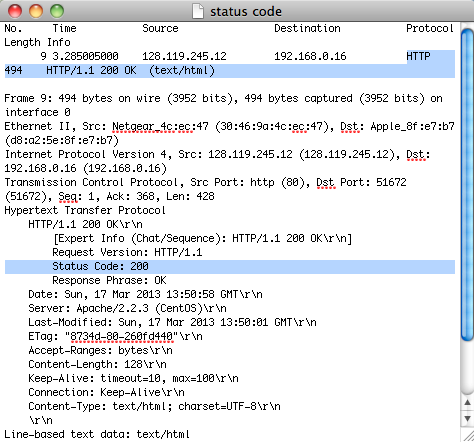


6. 494 bytes are returned to my browser.

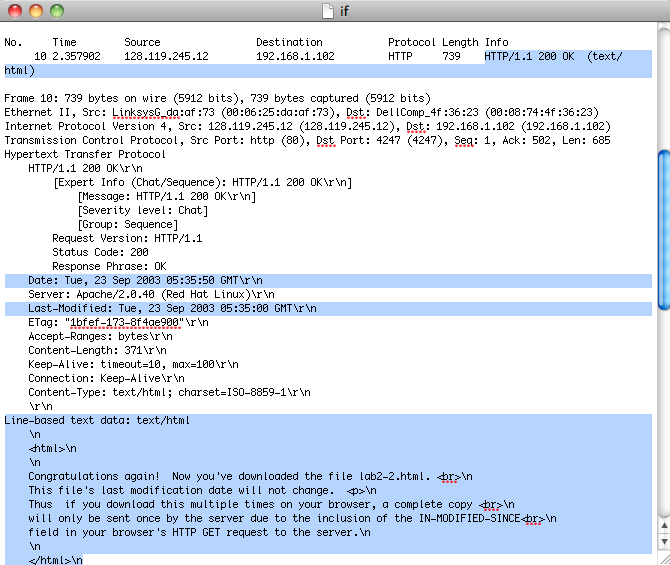


7. Upon inspection, there does not seem to be any headers within the physical data that was not displayed in the packet listing window.

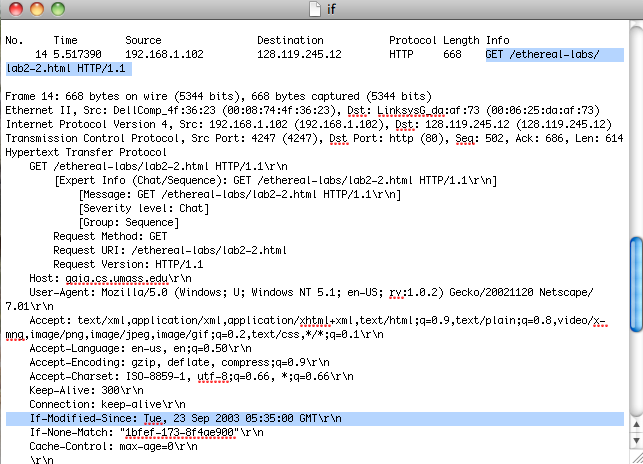
8. There is no IF-MODIFIED-SINCE header.



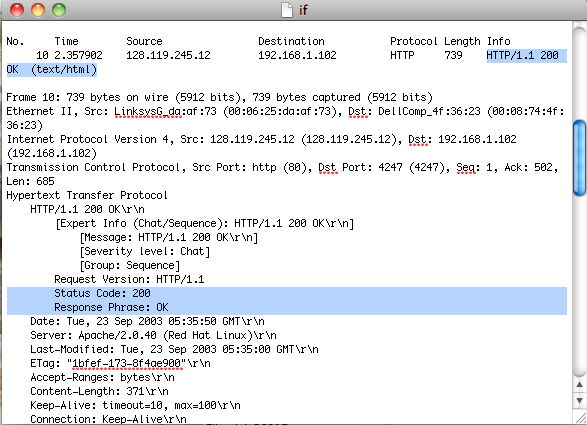
9. Yes the server explicitly returned the contents of the file which is seen clearly by the date that was modified which was the same date that the HTTP file was accessed. The content that was sent is in the highlighted section of the “Line-based” data.

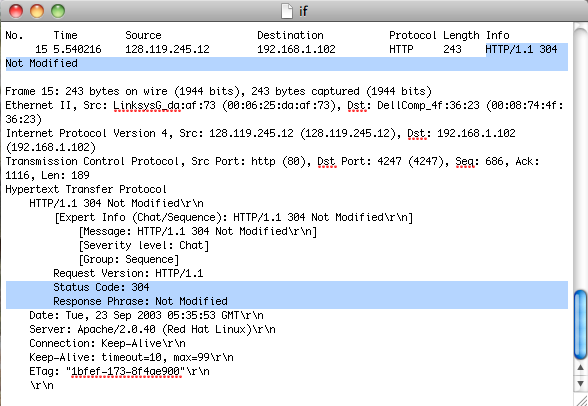


10. Yes there is an “IF-MODIFIED-SINCE” line in the second HTTP GET. The date “Tue, 23 Sep 2003 05:35:00 GMT\r\n” (which is the date that the HTTP file was accessed) follows the IF-MODIFIED-SINCE header.

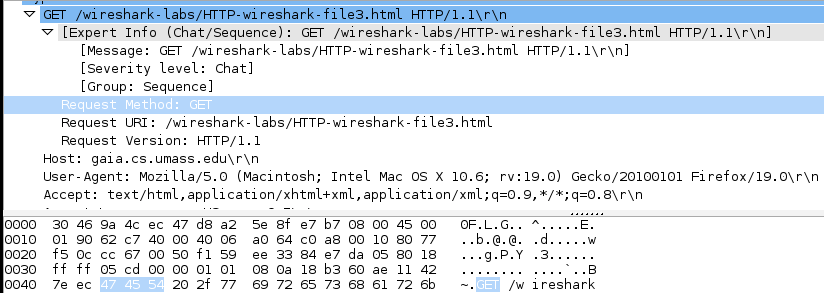


11. The status code and phrase returned by the server in the response to the second HTTP GET is different from the first response to the first HTTP GET. The status codes were 200 and 384 for the first and second respectively and the phrases were OK and Not Modified for the first and second respectively.

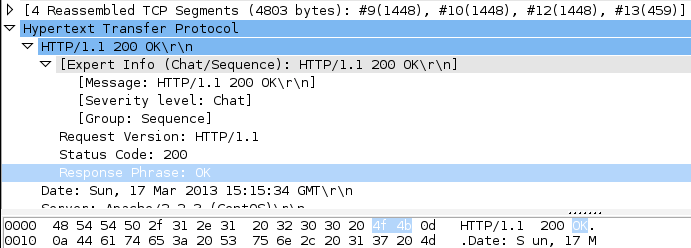


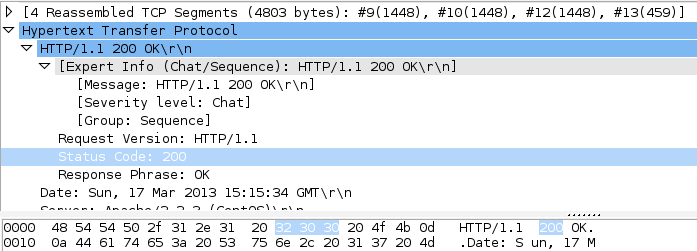


12. Only one HTTP GET request messages was sent by my browser. Packet number 40 in the trace contains the GET message for the Bill of Rights

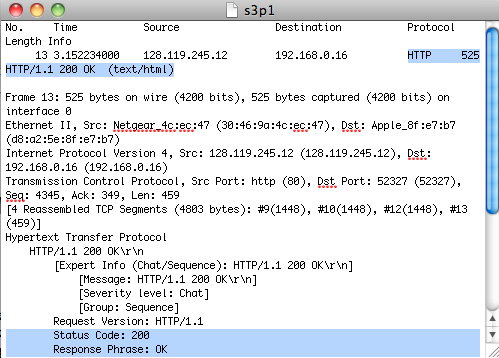


13. Packet number 0000 contains the status code and phrase associated with the response to the HTTP GET request.

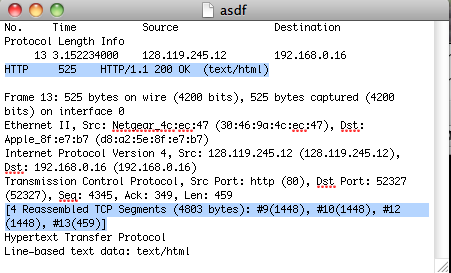




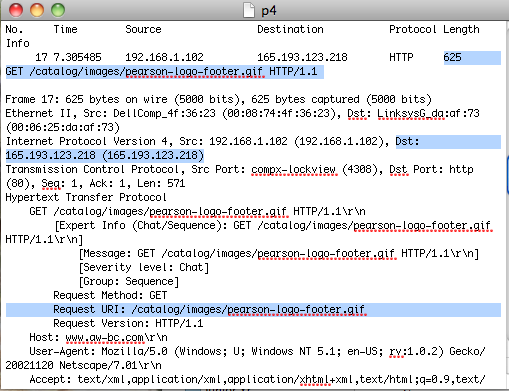
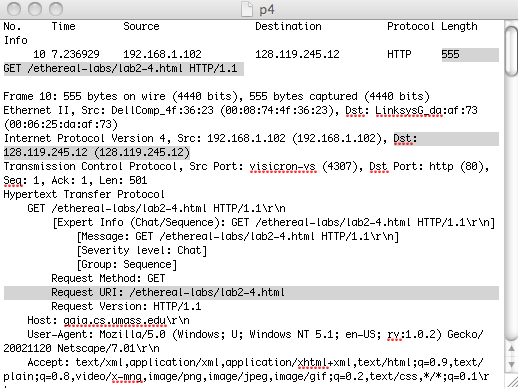
14. The status code is 200 and the response phrase is “OK”

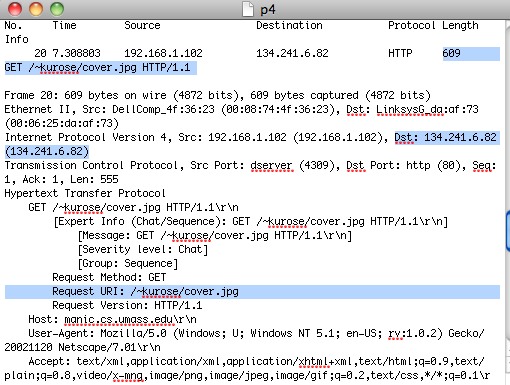


15. 4 TCP segments are needed to carry the single http response and the text of the Bill of Rights

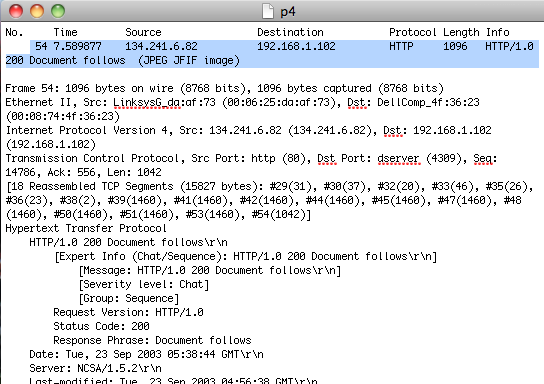
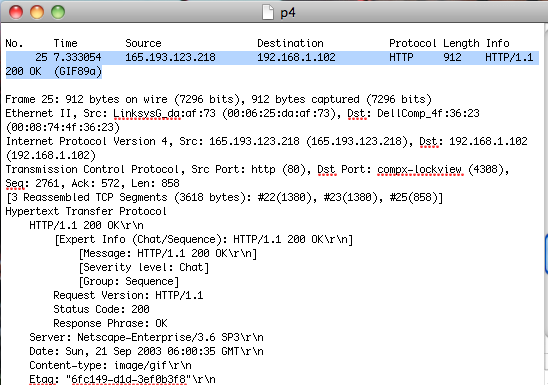


16. There are three HTTP GET request messages sent. The three internet address with their corresponding IP address are: /ethereal-labs/lab2-4.html (128.119.245.12), /catalog/images/pearson-logo-footer.gif (165.193.123.218), and /~kurose/cover.jpg (134.241.6.82).

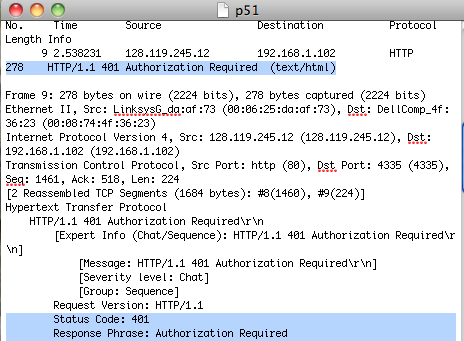




17. The browser downloaded the two images serially because we can see that the two responses to the two HTTP GET messages are not executed at the same time. We know that the two following snapshots are messages sent two the two images because the destination IP addresses match the IP address of the server that the two images are stored on. We can also see that they are downloaded serially.



18. The server’s response to the initial HTTP GET message is an Authorization Required message. This is the response because a username and password is required to load this HTTP file.



19. The new field that is included in the HTTP GET message is the “Authorization” header which includes the username and password that the user inputs to unlock the HTTP file.

