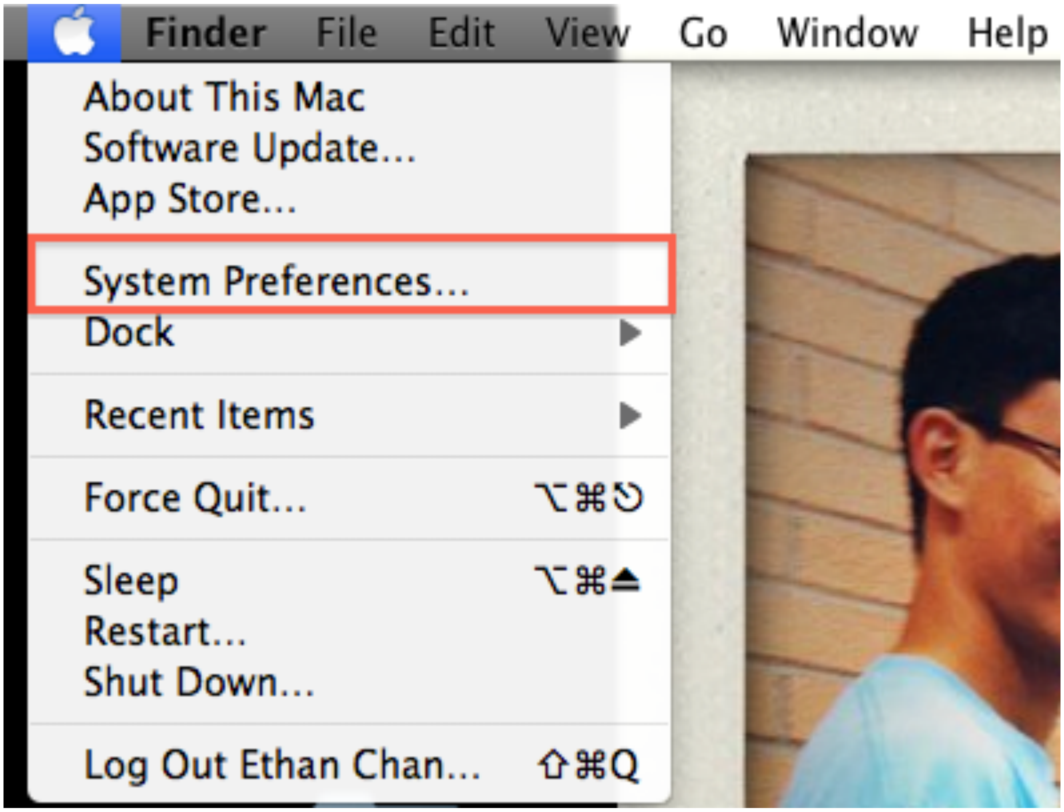
Ethan Chan
2:00pm-3:30pm
EE450

LAB 2: Wireshark

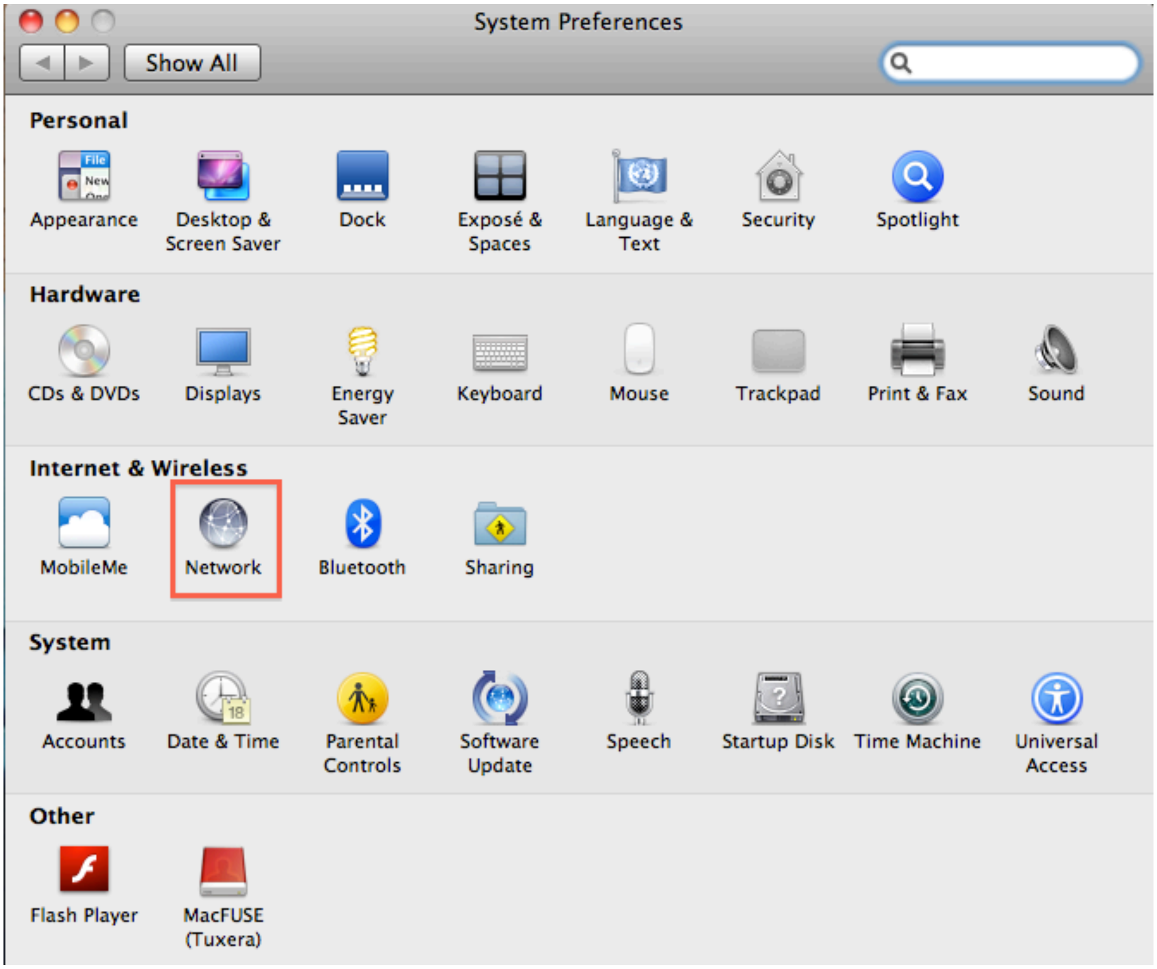
Part I

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

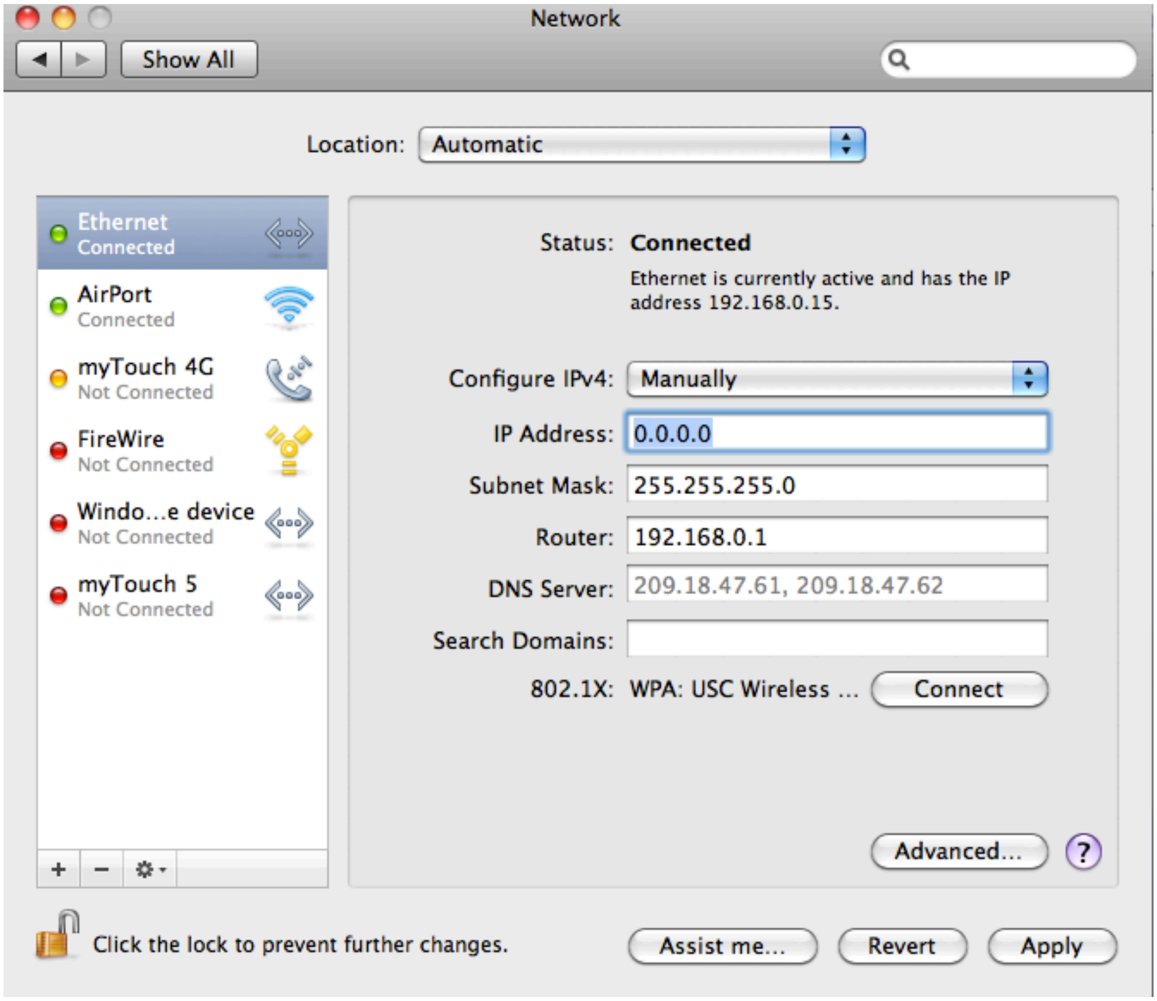
1) Click the Apple located at the top left hand corner of the desktop and select "System Preferences…"



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.



Location: Automatic

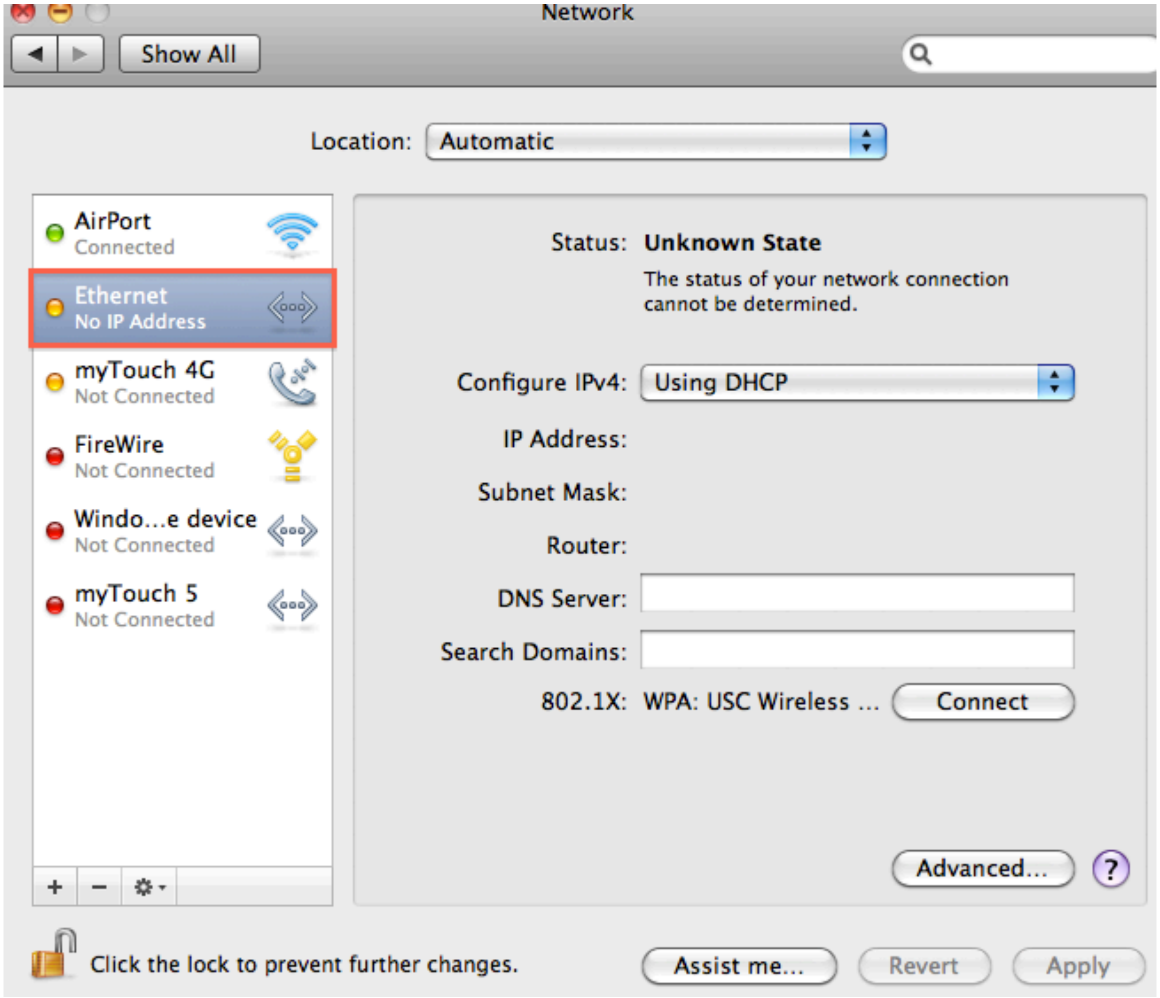
Ethernet Connected
AirPort Connected
myTouch 4G Not Connected
FireWire Not Connected
Windo…e device Not Connected
myTouch 5 Not Connected

Status: **Connected**
Ethernet is currently active and has the IP address 192.168.0.15.

Configure IPv4: Manually
IP Address: 0.0.0.0
Subnet Mask: 255.255.255.0
Router: 192.168.0.1
DNS Server: 209.18.47.61, 209.18.47.62
Search Domains:
802.1X: WPA: USC Wireless …

Click the lock to prevent further changes.

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



Location: Automatic

AirPort
Connected

Ethernet
No IP Address

myTouch 4G
Not Connected

FireWire
Not Connected

Windo...e device
Not Connected

myTouch 5
Not Connected

Status: **Unknown State**

The status of your network connection cannot be determined.

Configure IPv4: Using DHCP

IP Address:

Subnet Mask:

Router:

DNS Server:

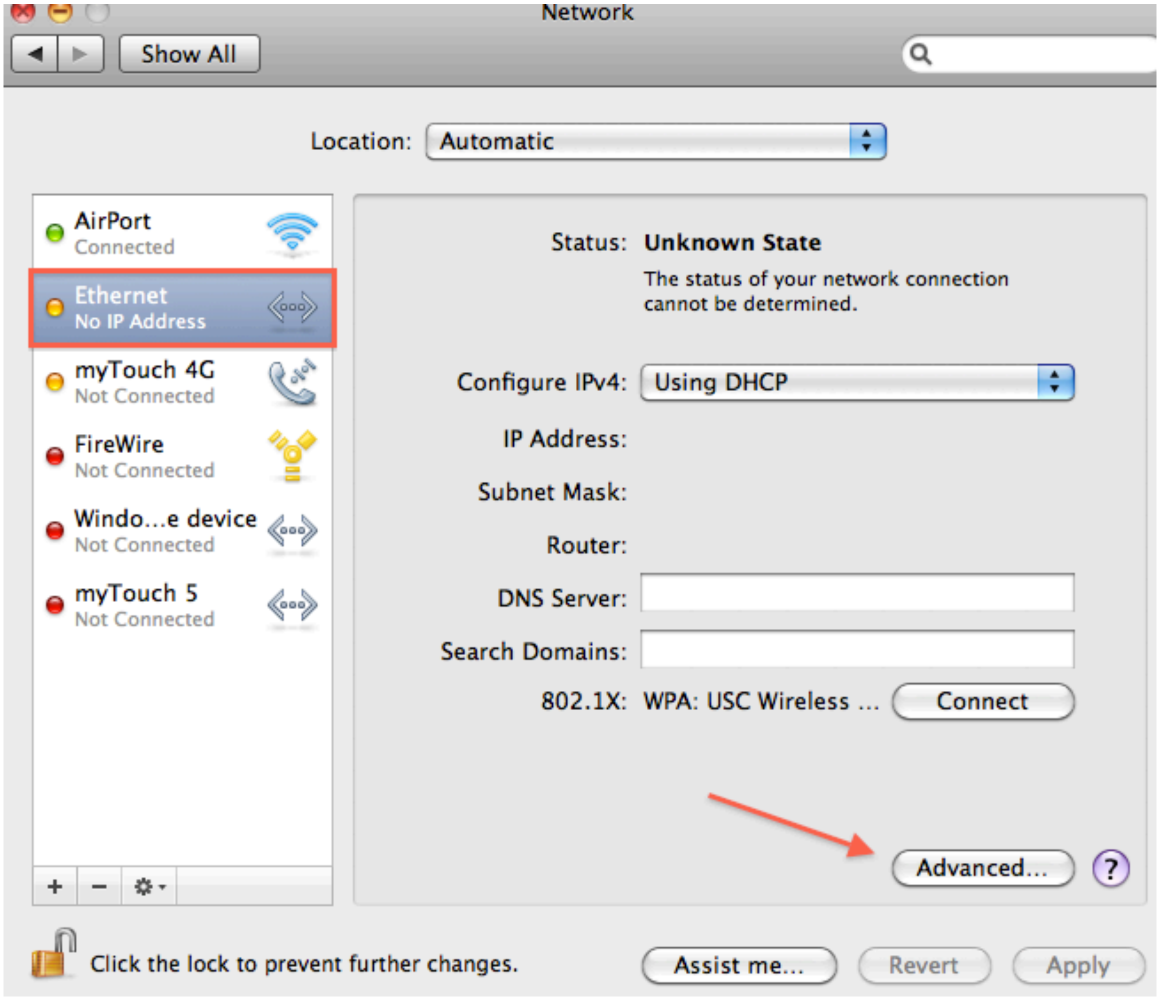
Search Domains:

802.1X: WPA: USC Wireless ...

Click the lock to prevent further changes.

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

a) Click the “Advanced” option



Network

Location: Automatic

AirPort
Connected

Ethernet
No IP Address

myTouch 4G
Not Connected

FireWire
Not Connected

Windo…e device
Not Connected

myTouch 5
Not Connected

Status: **Unknown State**

The status of your network connection cannot be determined.

Configure IPv4: Using DHCP

IP Address:

Subnet Mask:

Router:

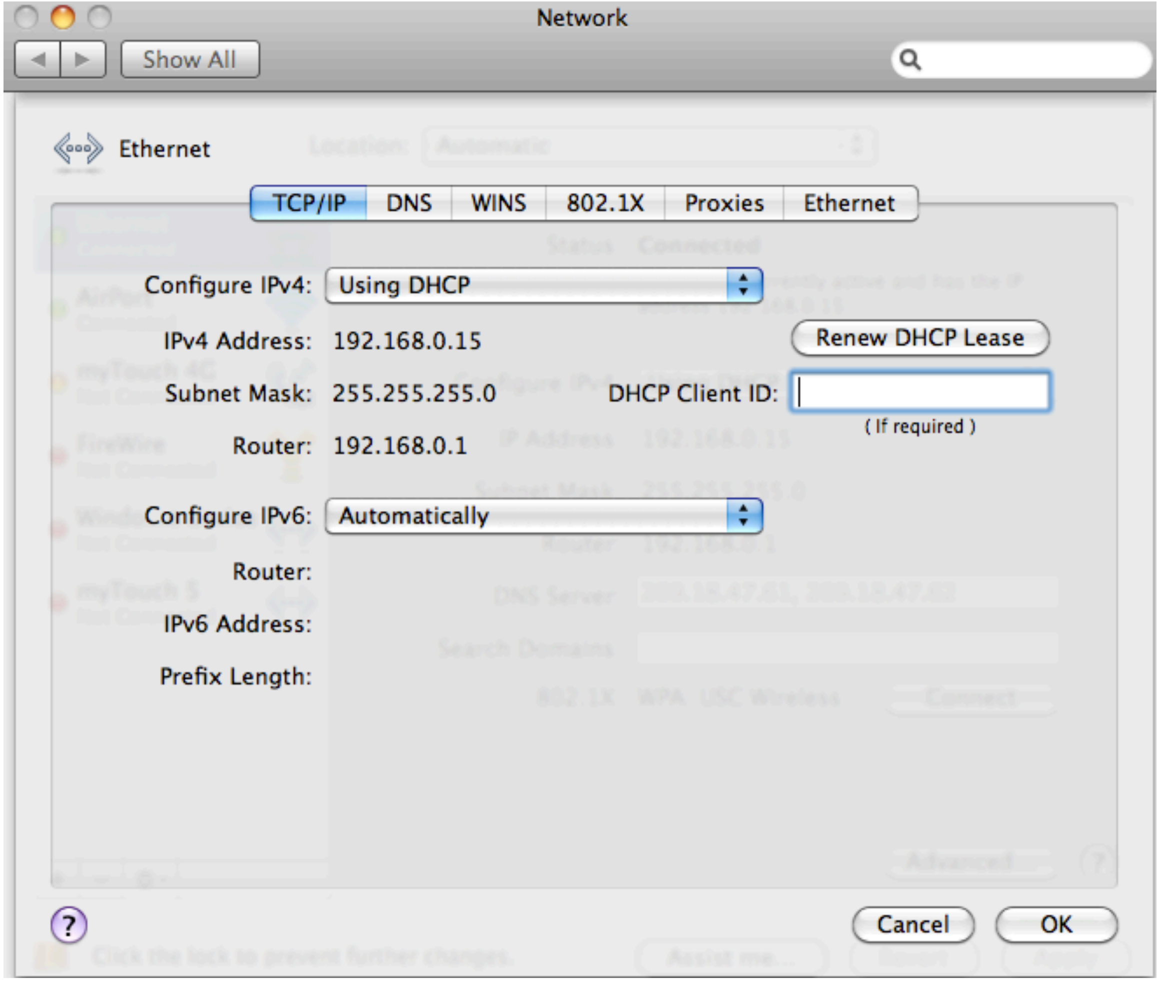
DNS Server:

Search Domains:

802.1X: WPA: USC Wireless …

Click the lock to prevent further changes.

b) Click “Renew DHCP Lease”



Configure IPv4: Using DHCP

IPv4 Address: 192.168.0.15

Subnet Mask: 255.255.255.0

Router: 192.168.0.1

DHCP Client ID:
(If required)

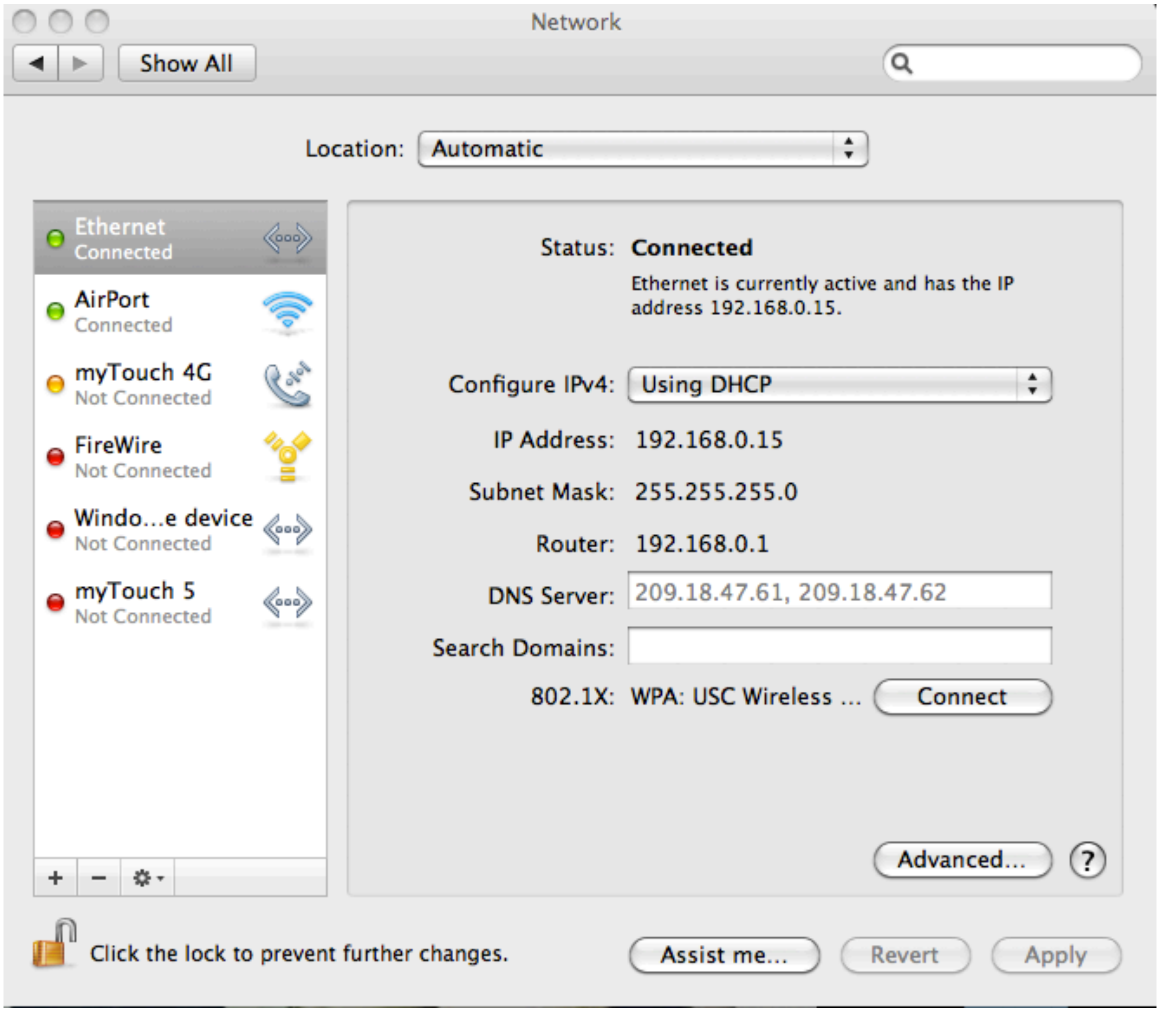
Configure IPv6: Automatically

Router:

IPv6 Address:

Prefix Length:

6) DHCP renews your IP address!



Location: Automatic

Status: Connected

Ethernet is currently active and has the IP address 192.168.0.15.

Configure IPv4: Using DHCP

IP Address: 192.168.0.15

Subnet Mask: 255.255.255.0

Router: 192.168.0.1

DNS Server: 209.18.47.61, 209.18.47.62

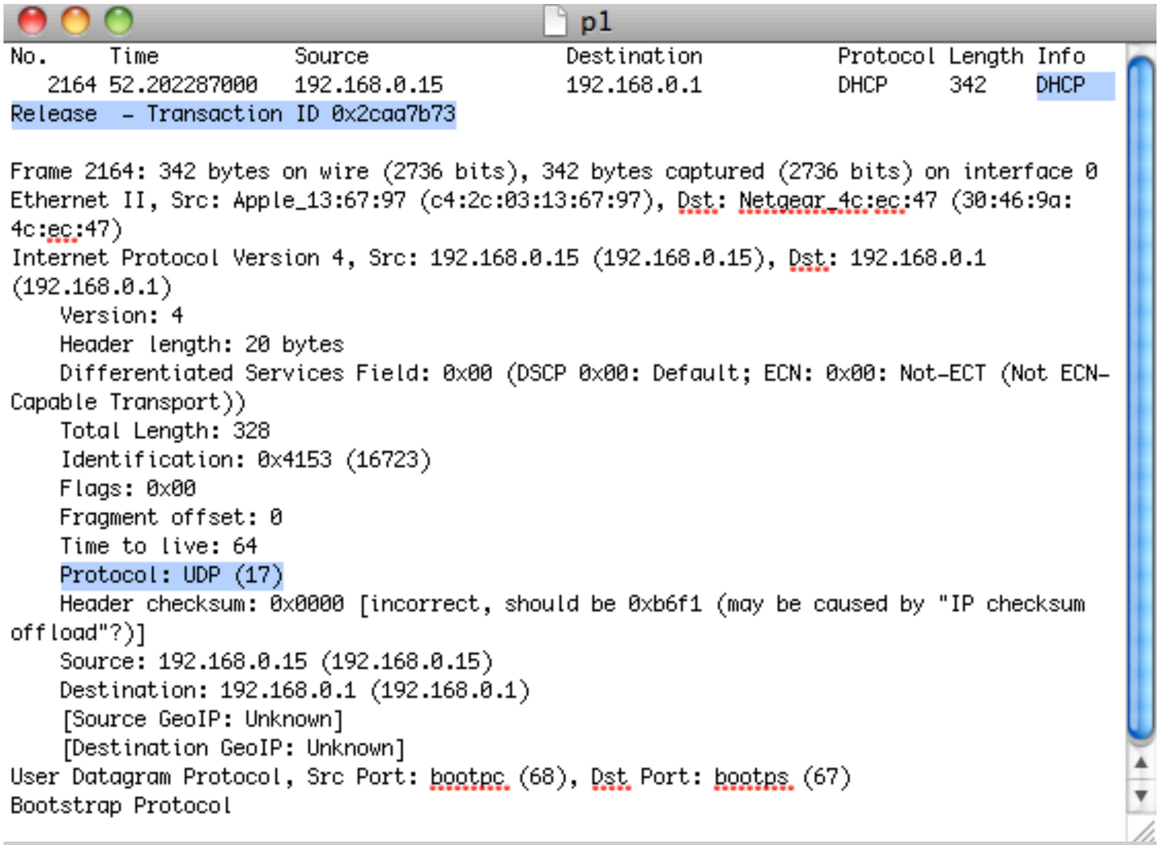
Search Domains:

802.1X: WPA: USC Wireless ...

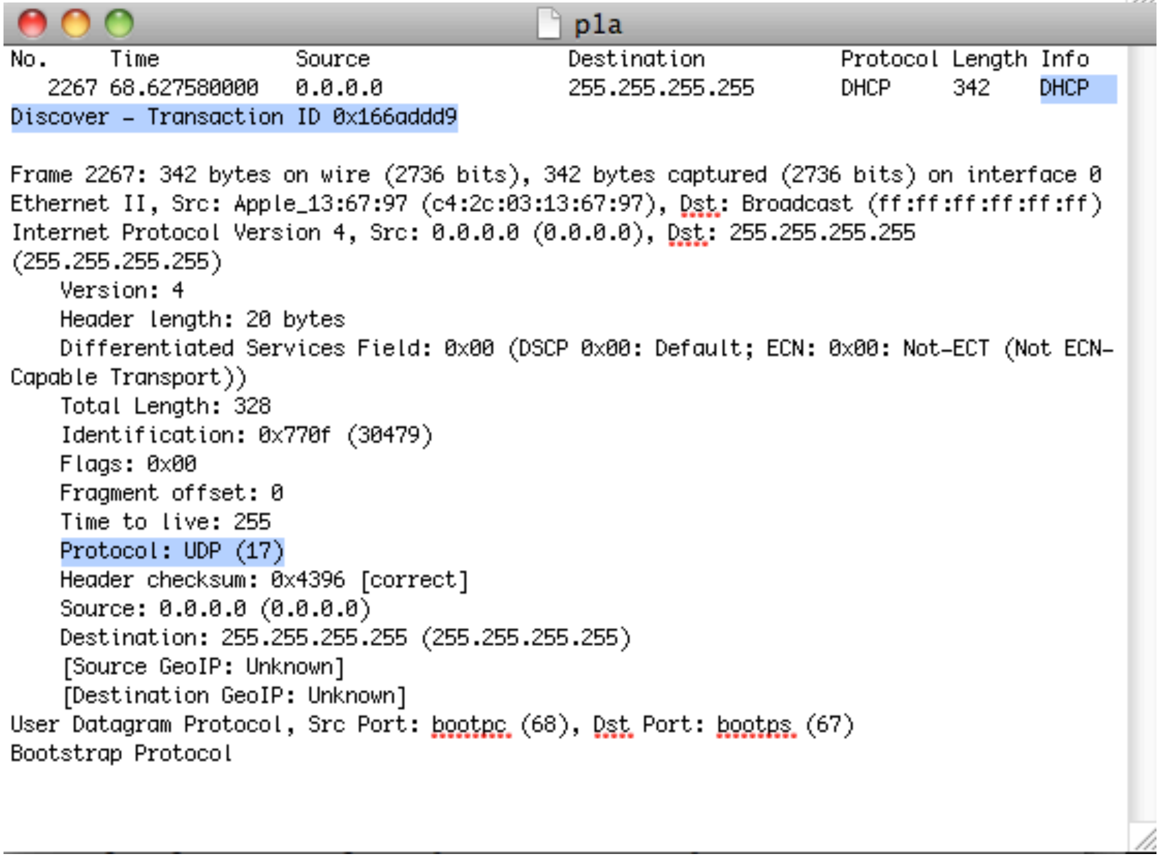
Click the lock to prevent further changes.

DHCP Questions:

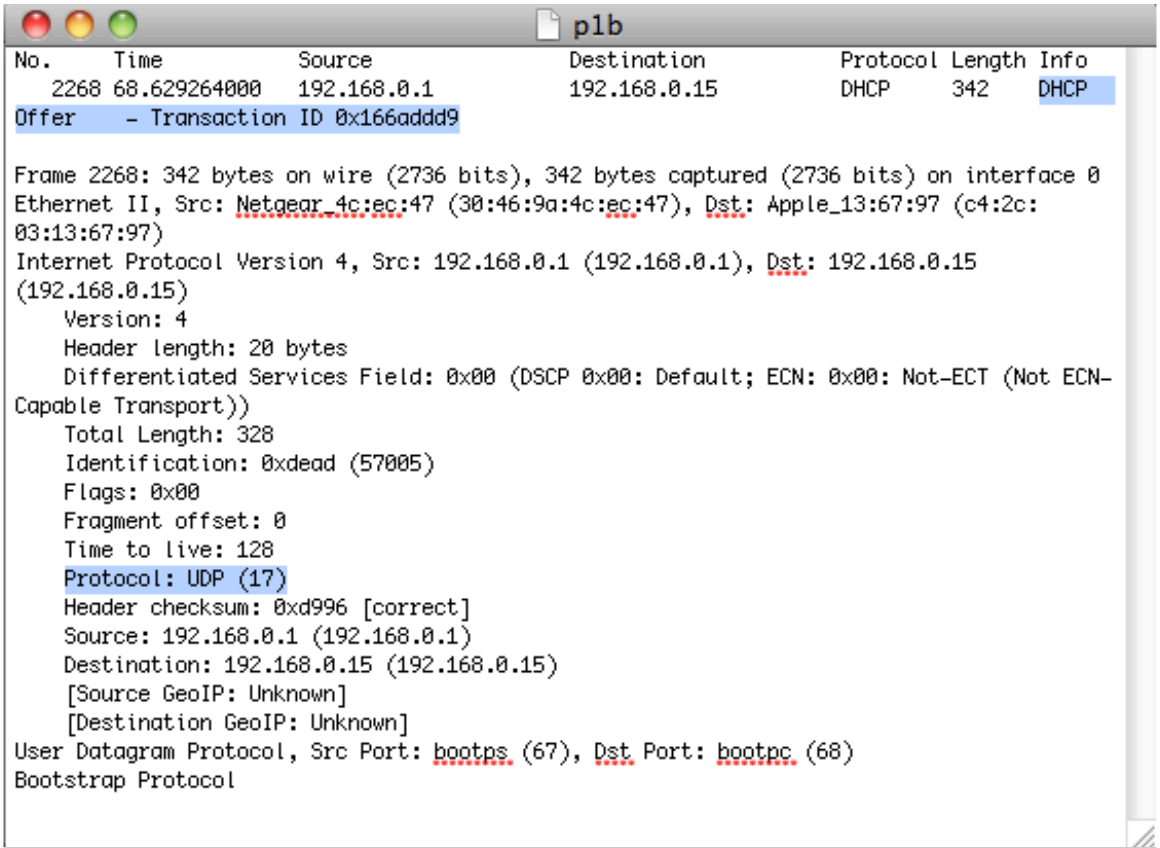
1) The DHCP messages are NOT sent over TCP but rather through UDP
Looking at the all the DHCP messages and we can see that they all use UDP protocol



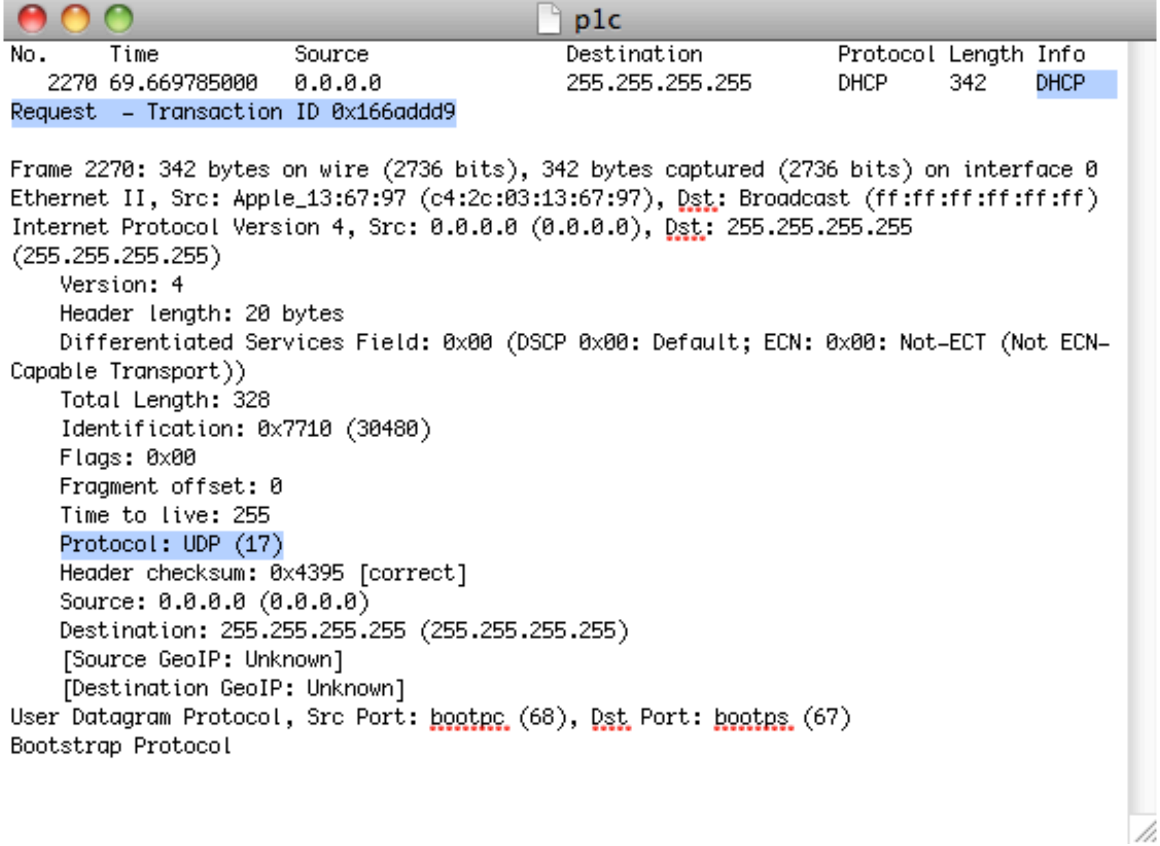
```
No.     Time           Source              Destination           Protocol Length  Info
   2164 52.202287000   192.168.0.15        192.168.0.1           DHCP     342     DHCP
Release  - Transaction ID 0x2caa7b73

Frame 2164: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: Apple_13:67:97 (c4:2c:03:13:67:97), Dst: Netgear_4c:ec:47 (30:46:9a:
4c:ec:47)
Internet Protocol Version 4, Src: 192.168.0.15 (192.168.0.15), Dst: 192.168.0.1
(192.168.0.1)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-
Capable Transport))
    Total Length: 328
    Identification: 0x4153 (16723)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0x0000 [incorrect, should be 0xb6f1 (may be caused by "IP checksum
offload"?)]
    Source: 192.168.0.15 (192.168.0.15)
    Destination: 192.168.0.1 (192.168.0.1)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
Bootstrap Protocol
```



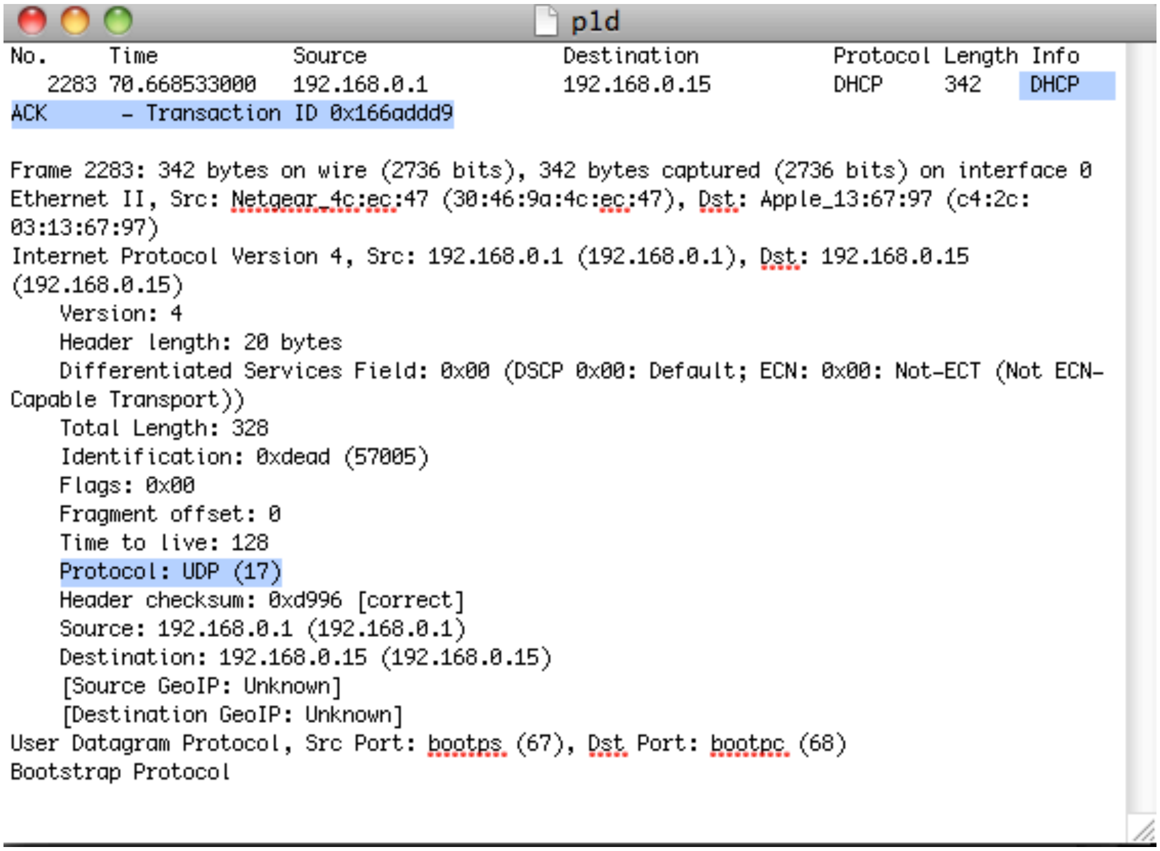
```
No.     Time           Source              Destination           Protocol Length  Info
   2267 68.627580000   0.0.0.0             255.255.255.255       DHCP     342     DHCP
Discover - Transaction ID 0x166addd9

Frame 2267: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: Apple_13:67:97 (c4:2c:03:13:67:97), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255
(255.255.255.255)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-
Capable Transport))
    Total Length: 328
    Identification: 0x770f (30479)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: UDP (17)
    Header checksum: 0x4396 [correct]
    Source: 0.0.0.0 (0.0.0.0)
    Destination: 255.255.255.255 (255.255.255.255)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
Bootstrap Protocol
```



```
No.     Time           Source                Destination           Protocol Length Info
   2268 68.629264000   192.168.0.1           192.168.0.15          DHCP     342    DHCP
Offer     - Transaction ID 0x166addd9

Frame 2268: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: Netgear_4c:ec:47 (30:46:9a:4c:ec:47), Dst: Apple_13:67:97 (c4:2c:
03:13:67:97)
Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.15
(192.168.0.15)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-
Capable Transport))
    Total Length: 328
    Identification: 0xdead (57005)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0xd996 [correct]
    Source: 192.168.0.1 (192.168.0.1)
    Destination: 192.168.0.15 (192.168.0.15)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
Bootstrap Protocol
```

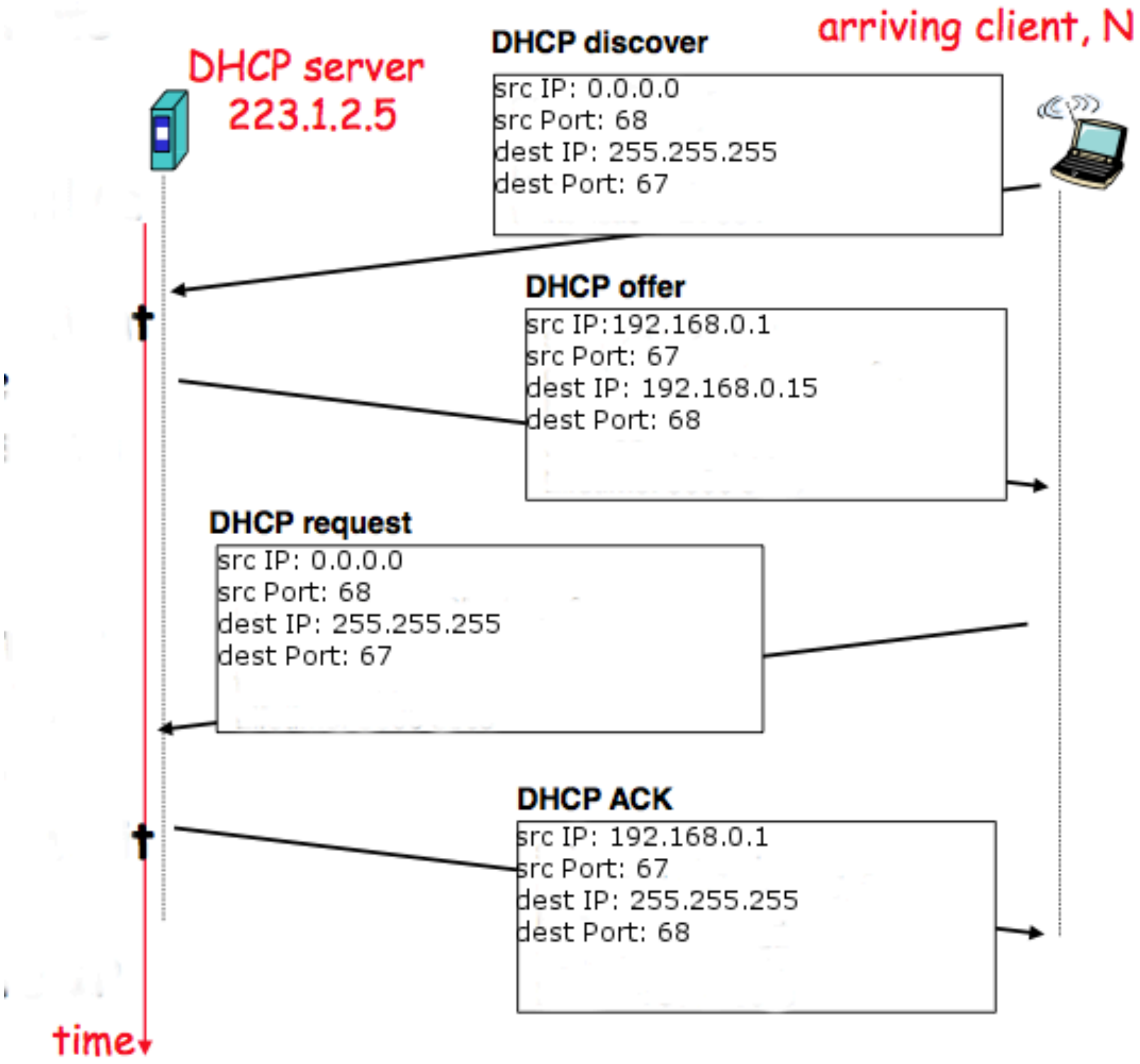


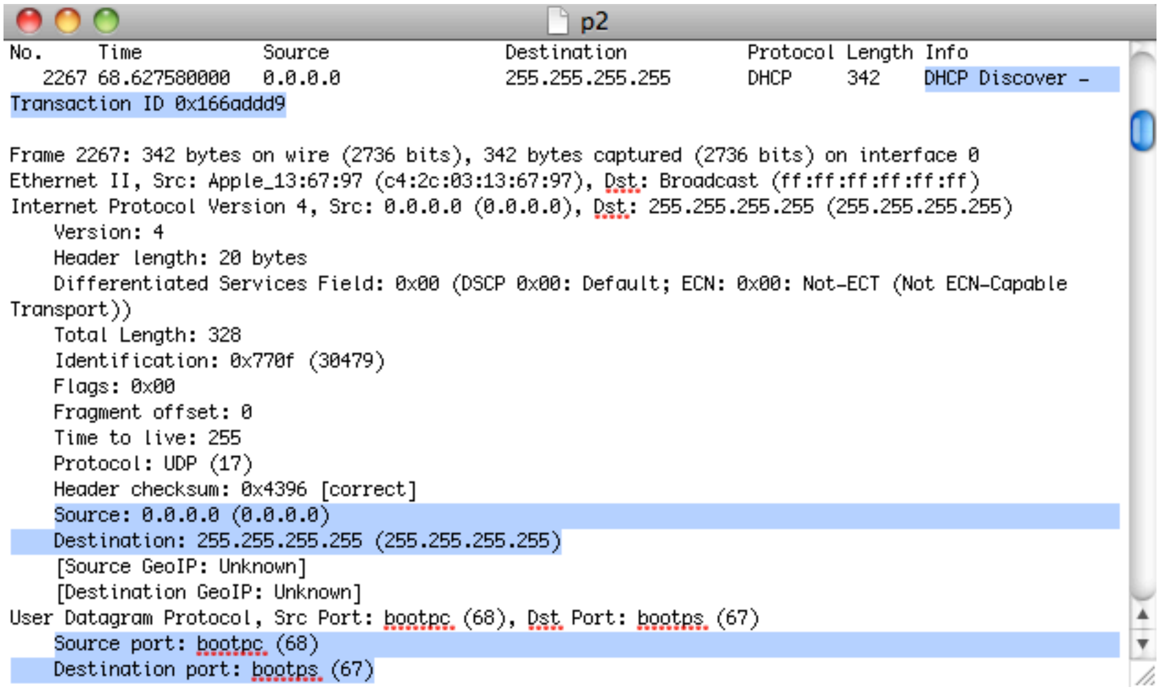
```
No.     Time           Source                Destination           Protocol Length Info
   2270 69.669785000   0.0.0.0               255.255.255.255       DHCP     342    DHCP
Request   - Transaction ID 0x166addd9

Frame 2270: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: Apple_13:67:97 (c4:2c:03:13:67:97), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255
(255.255.255.255)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-
Capable Transport))
    Total Length: 328
    Identification: 0x7710 (30480)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: UDP (17)
    Header checksum: 0x4395 [correct]
    Source: 0.0.0.0 (0.0.0.0)
    Destination: 255.255.255.255 (255.255.255.255)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
Bootstrap Protocol
```



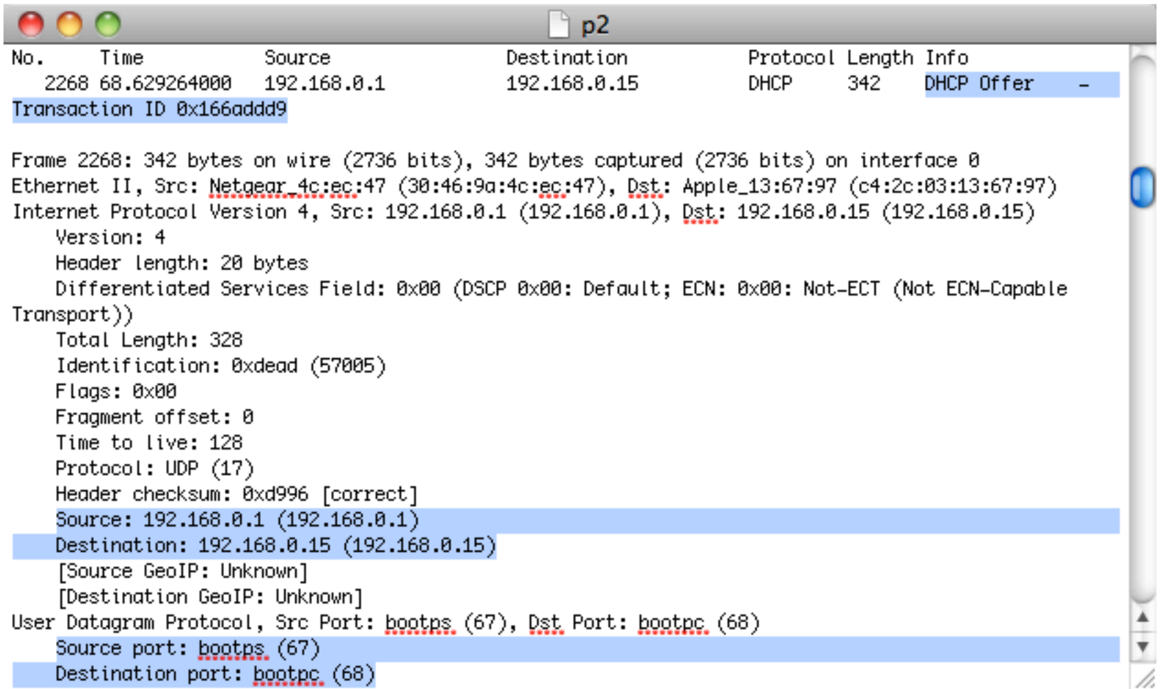
```
No.     Time           Source                Destination           Protocol Length Info
   2283 70.668533000   192.168.0.1           192.168.0.15          DHCP     342    DHCP
ACK         - Transaction ID 0x166addd9

Frame 2283: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: Netgear_4c:ec:47 (30:46:9a:4c:ec:47), Dst: Apple_13:67:97 (c4:2c:
03:13:67:97)
Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.15
(192.168.0.15)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-
Capable Transport))
    Total Length: 328
    Identification: 0xdead (57005)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0xd996 [correct]
    Source: 192.168.0.1 (192.168.0.1)
    Destination: 192.168.0.15 (192.168.0.15)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
Bootstrap Protocol
```

2)

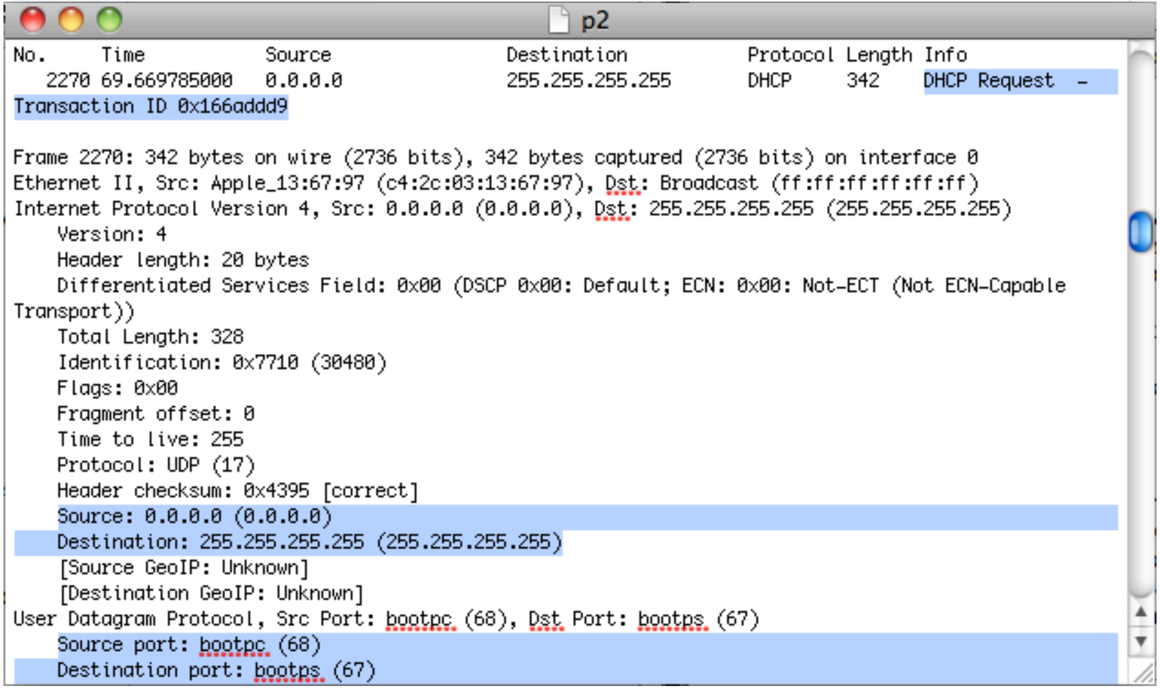




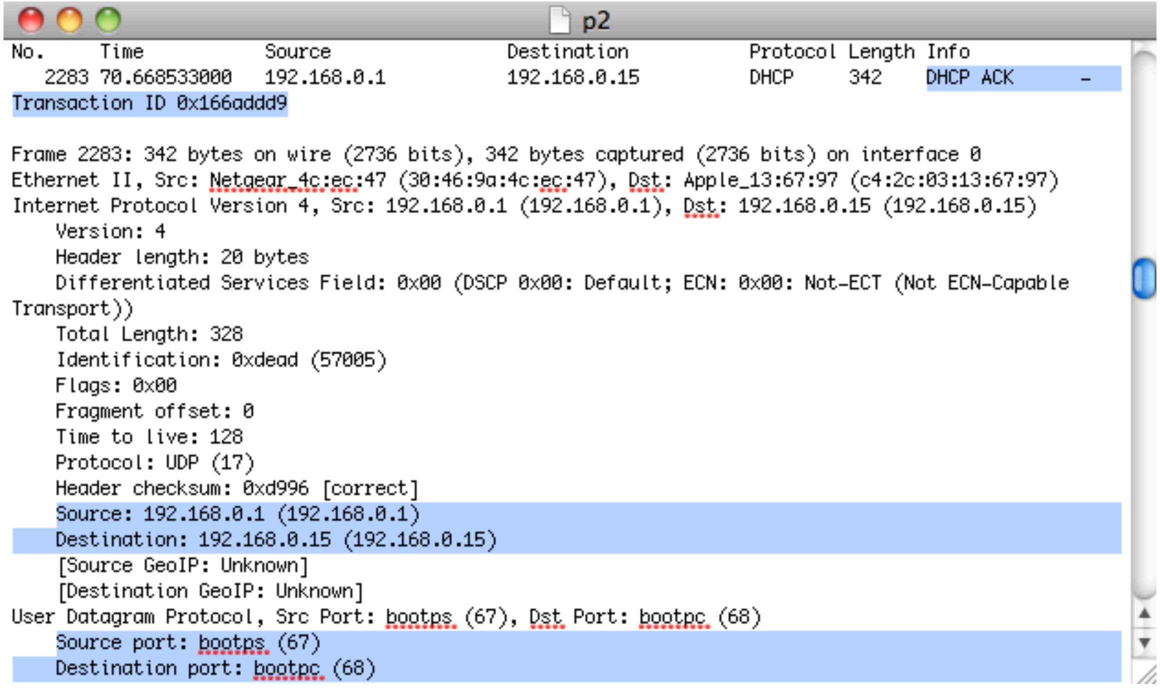
```
No.     Time            Source                Destination           Protocol Length Info
   2267 68.627580000    0.0.0.0               255.255.255.255       DHCP     342    DHCP Discover -
Transaction ID 0x166addd9

Frame 2267: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: Apple_13:67:97 (c4:2c:03:13:67:97), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable
Transport))
    Total Length: 328
    Identification: 0x770f (30479)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: UDP (17)
    Header checksum: 0x4396 [correct]
    Source: 0.0.0.0 (0.0.0.0)
    Destination: 255.255.255.255 (255.255.255.255)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
    Source port: bootpc (68)
    Destination port: bootps (67)
```



```
No.     Time            Source              Destination         Protocol Length Info
   2268 68.629264000    192.168.0.1         192.168.0.15        DHCP     342    DHCP Offer    -
Transaction ID 0x166addd9

Frame 2268: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: Netgear_4c:ec:47 (30:46:9a:4c:ec:47), Dst: Apple_13:67:97 (c4:2c:03:13:67:97)
Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.15 (192.168.0.15)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable
Transport))
    Total Length: 328
    Identification: 0xdead (57005)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0xd996 [correct]
    Source: 192.168.0.1 (192.168.0.1)
    Destination: 192.168.0.15 (192.168.0.15)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
    Source port: bootps (67)
    Destination port: bootpc (68)
```



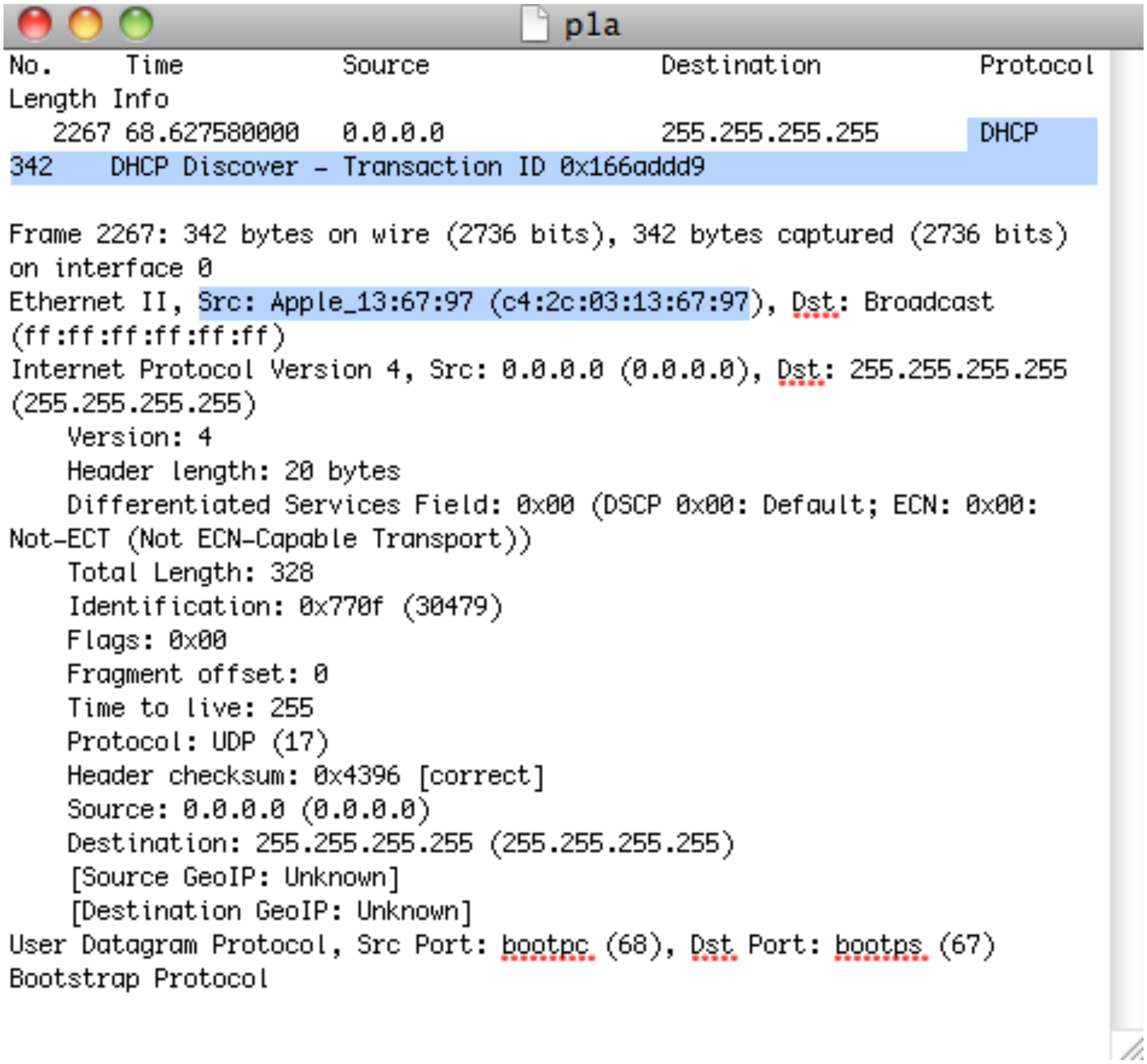
```
No.     Time            Source              Destination         Protocol Length Info
   2270 69.669785000    0.0.0.0             255.255.255.255     DHCP     342    DHCP Request  -
Transaction ID 0x166addd9

Frame 2270: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: Apple_13:67:97 (c4:2c:03:13:67:97), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable
Transport))
    Total Length: 328
    Identification: 0x7710 (30480)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: UDP (17)
    Header checksum: 0x4395 [correct]
    Source: 0.0.0.0 (0.0.0.0)
    Destination: 255.255.255.255 (255.255.255.255)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
    Source port: bootpc (68)
    Destination port: bootps (67)
```



```
No.      Time            Source              Destination         Protocol Length Info
   2283 70.668533000  192.168.0.1         192.168.0.15        DHCP     342    DHCP ACK      -
Transaction ID 0x166addd9

Frame 2283: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: Netgear_4c:ec:47 (30:46:9a:4c:ec:47), Dst: Apple_13:67:97 (c4:2c:03:13:67:97)
Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.15 (192.168.0.15)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable
Transport))
    Total Length: 328
    Identification: 0xdead (57005)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0xd996 [correct]
    Source: 192.168.0.1 (192.168.0.1)
    Destination: 192.168.0.15 (192.168.0.15)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
    Source port: bootps (67)
    Destination port: bootpc (68)
```

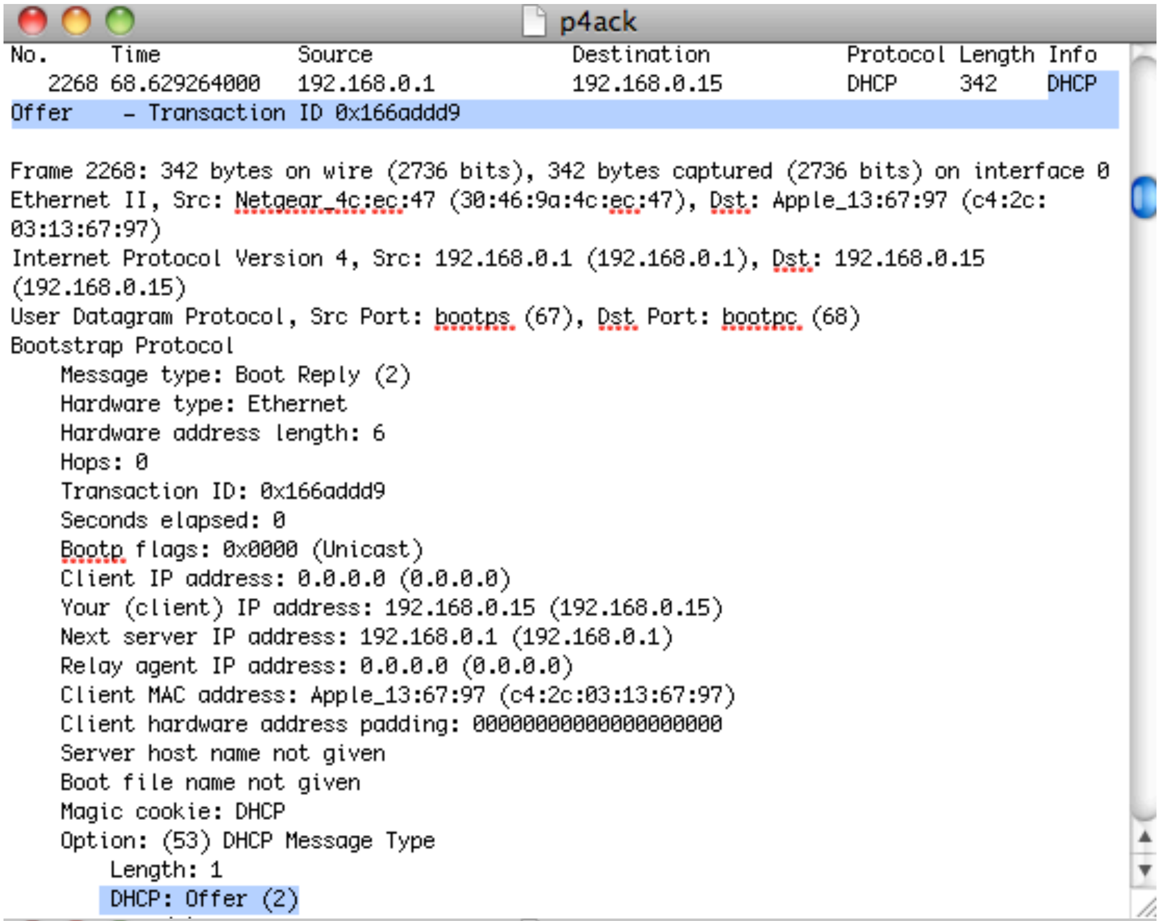
The port numbers 67 and 68 used in my DHCP message protocolsare the same port numbers used in example in the lab assignment.

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.

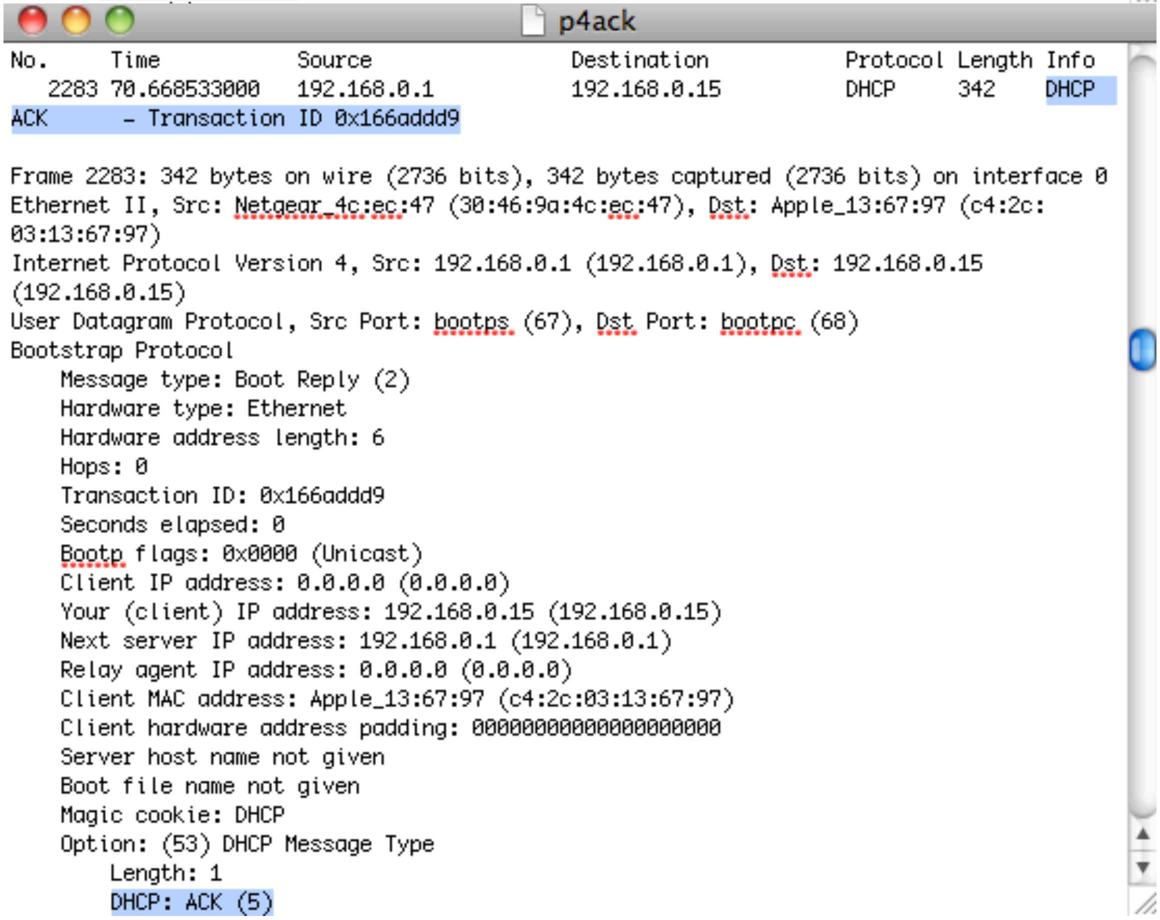


```
No.      Time            Source              Destination         Protocol
Length Info
   2267 68.627580000  0.0.0.0             255.255.255.255     DHCP
342    DHCP Discover - Transaction ID 0x166addd9

Frame 2267: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
on interface 0
Ethernet II, Src: Apple_13:67:97 (c4:2c:03:13:67:97), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255
(255.255.255.255)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00:
Not-ECT (Not ECN-Capable Transport))
    Total Length: 328
    Identification: 0x770f (30479)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: UDP (17)
    Header checksum: 0x4396 [correct]
    Source: 0.0.0.0 (0.0.0.0)
    Destination: 255.255.255.255 (255.255.255.255)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
Bootstrap Protocol
```

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.

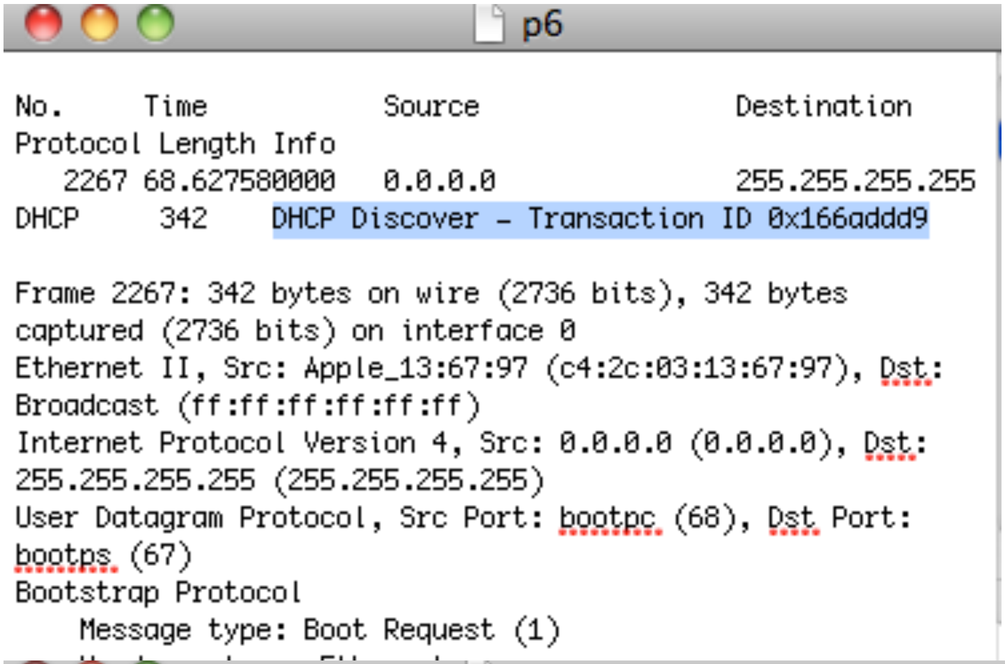


```
No.     Time            Source              Destination         Protocol Length Info
   2268 68.629264000    192.168.0.1         192.168.0.15        DHCP     342    DHCP
Offer    - Transaction ID 0x166addd9

Frame 2268: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: Netgear_4c:ec:47 (30:46:9a:4c:ec:47), Dst: Apple_13:67:97 (c4:2c:
03:13:67:97)
Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.15
(192.168.0.15)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x166addd9
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 192.168.0.15 (192.168.0.15)
    Next server IP address: 192.168.0.1 (192.168.0.1)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: Apple_13:67:97 (c4:2c:03:13:67:97)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    Option: (53) DHCP Message Type
        Length: 1
        DHCP: Offer (2)
```

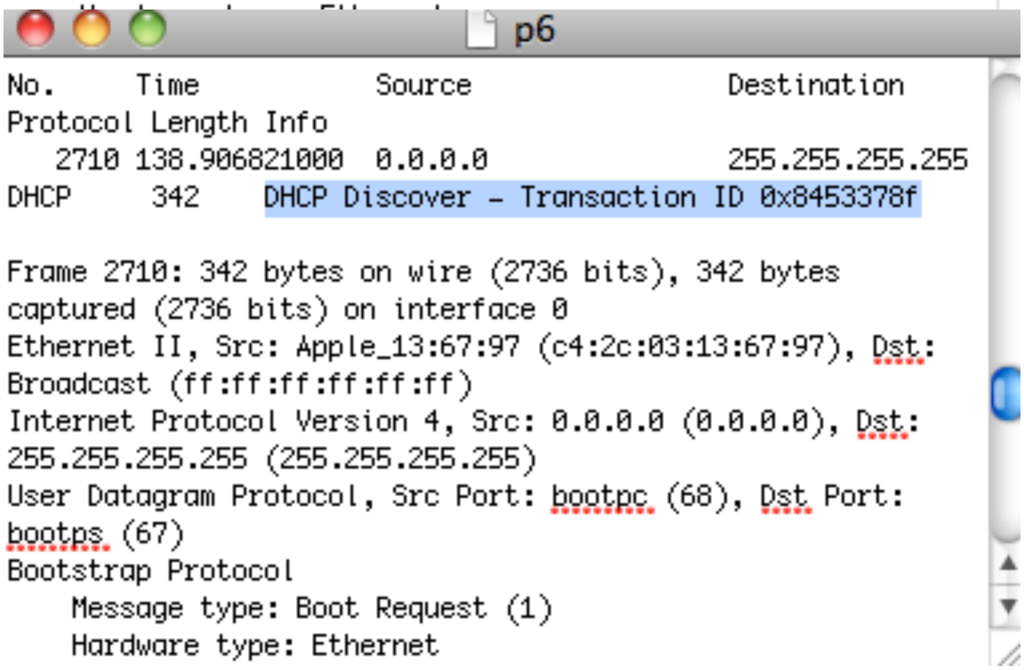


```
No.     Time            Source              Destination         Protocol Length Info
   2283 70.668533000    192.168.0.1         192.168.0.15        DHCP     342    DHCP
ACK      - Transaction ID 0x166addd9

Frame 2283: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: Netgear_4c:ec:47 (30:46:9a:4c:ec:47), Dst: Apple_13:67:97 (c4:2c:
03:13:67:97)
Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.15
(192.168.0.15)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x166addd9
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 192.168.0.15 (192.168.0.15)
    Next server IP address: 192.168.0.1 (192.168.0.1)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: Apple_13:67:97 (c4:2c:03:13:67:97)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    Option: (53) DHCP Message Type
        Length: 1
        DHCP: ACK (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.

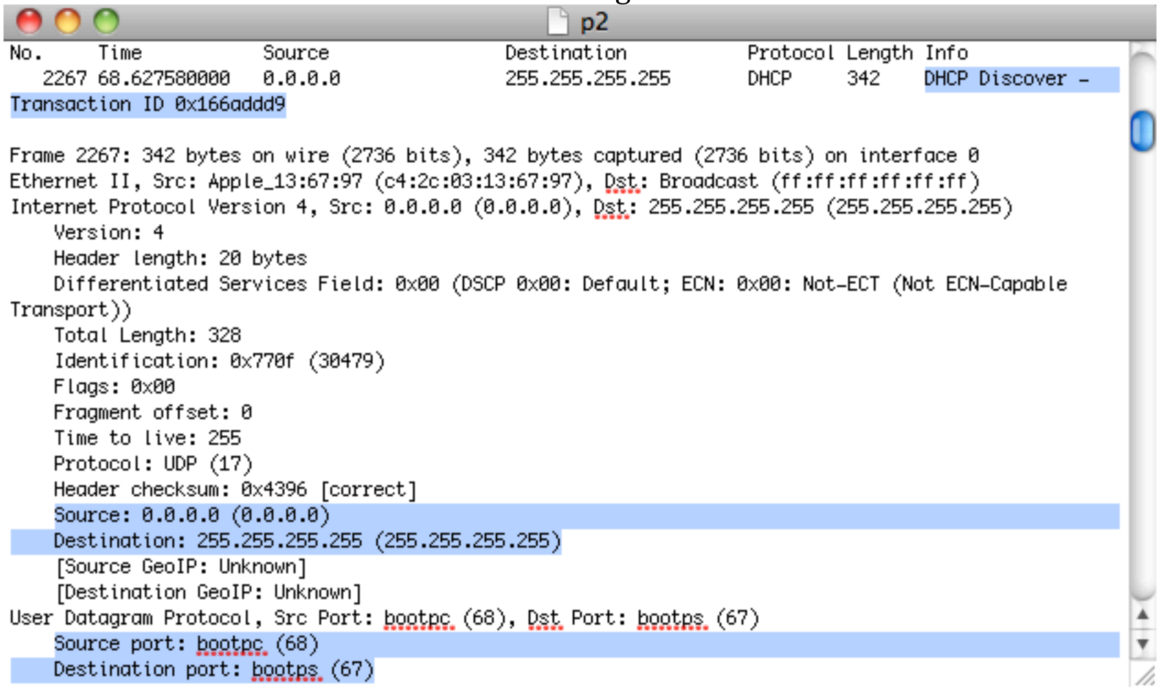


```
No.     Time            Source                Destination
Protocol Length Info
   2267 68.627580000   0.0.0.0               255.255.255.255
DHCP     342     DHCP Discover - Transaction ID 0x166addd9

Frame 2267: 342 bytes on wire (2736 bits), 342 bytes
captured (2736 bits) on interface 0
Ethernet II, Src: Apple_13:67:97 (c4:2c:03:13:67:97), Dst:
Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst:
255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootpc (68), Dst Port:
bootps (67)
Bootstrap Protocol
    Message type: Boot Request (1)
```



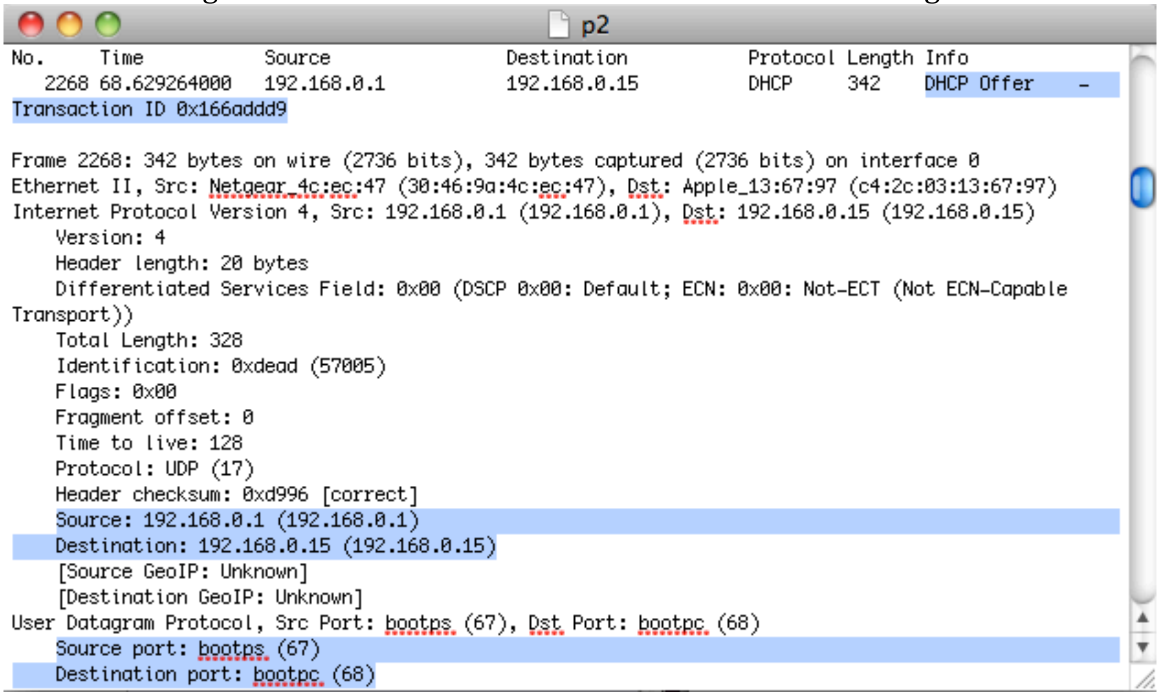
```
No.     Time            Source                Destination
Protocol Length Info
   2710 138.906821000  0.0.0.0               255.255.255.255
DHCP     342     DHCP Discover - Transaction ID 0x8453378f

Frame 2710: 342 bytes on wire (2736 bits), 342 bytes
captured (2736 bits) on interface 0
Ethernet II, Src: Apple_13:67:97 (c4:2c:03:13:67:97), Dst:
Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst:
255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootpc (68), Dst Port:
bootps (67)
Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
```

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.



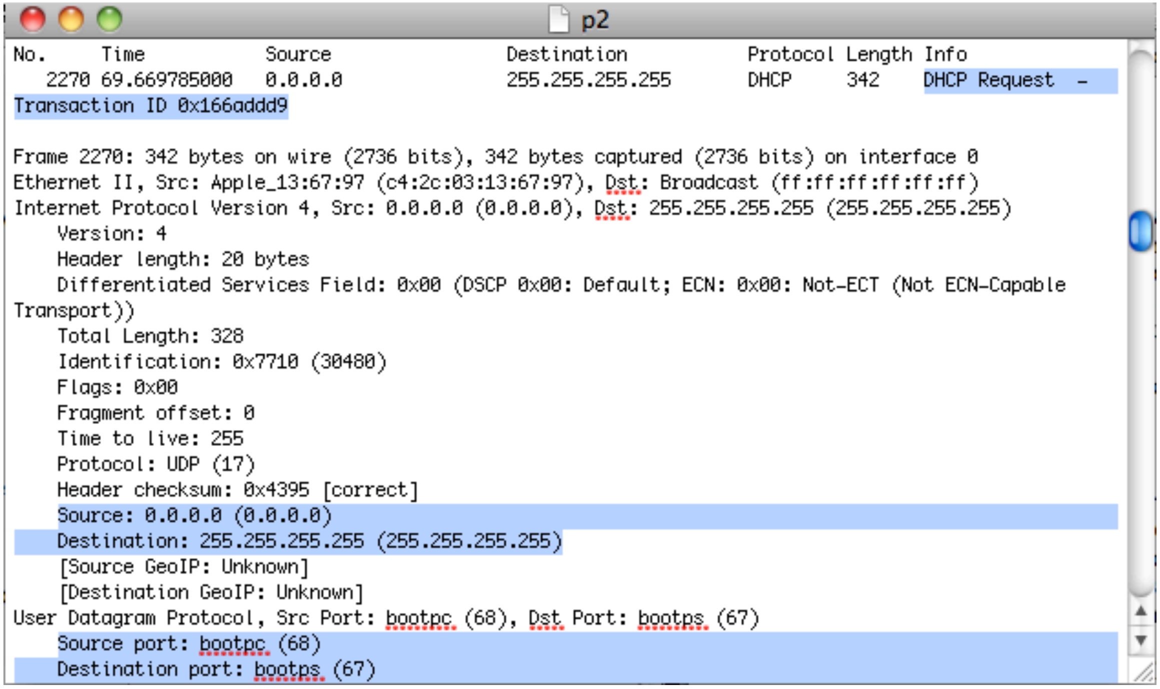
```
No.     Time           Source                Destination           Protocol Length Info
   2267 68.627580000   0.0.0.0               255.255.255.255       DHCP     342    DHCP Discover -
Transaction ID 0x166addd9

Frame 2267: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: Apple_13:67:97 (c4:2c:03:13:67:97), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable
Transport))
    Total Length: 328
    Identification: 0x770f (30479)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: UDP (17)
    Header checksum: 0x4396 [correct]
    Source: 0.0.0.0 (0.0.0.0)
    Destination: 255.255.255.255 (255.255.255.255)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
    Source port: bootpc (68)
    Destination port: bootps (67)
```

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.



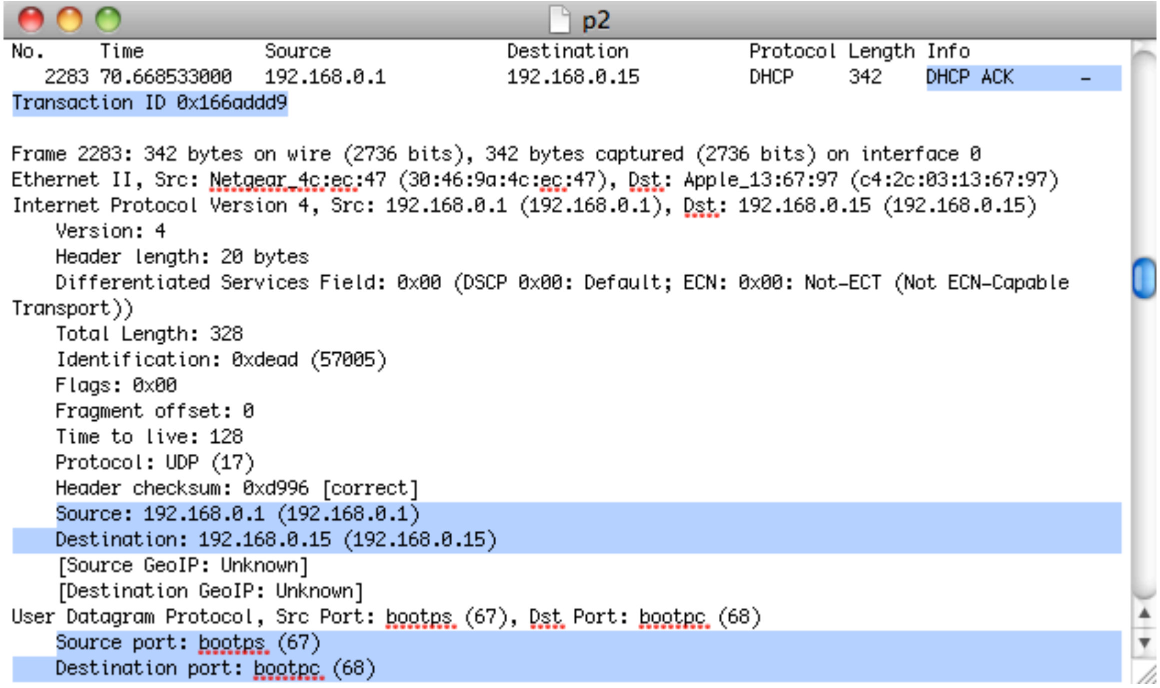
```
No.     Time           Source                Destination           Protocol Length Info
   2268 68.629264000   192.168.0.1           192.168.0.15          DHCP     342    DHCP Offer    -
Transaction ID 0x166addd9

Frame 2268: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: Netgear_4c:ec:47 (30:46:9a:4c:ec:47), Dst: Apple_13:67:97 (c4:2c:03:13:67:97)
Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.15 (192.168.0.15)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable
Transport))
    Total Length: 328
    Identification: 0xdead (57005)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0xd996 [correct]
    Source: 192.168.0.1 (192.168.0.1)
    Destination: 192.168.0.15 (192.168.0.15)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
    Source port: bootps (67)
    Destination port: bootpc (68)
```

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.



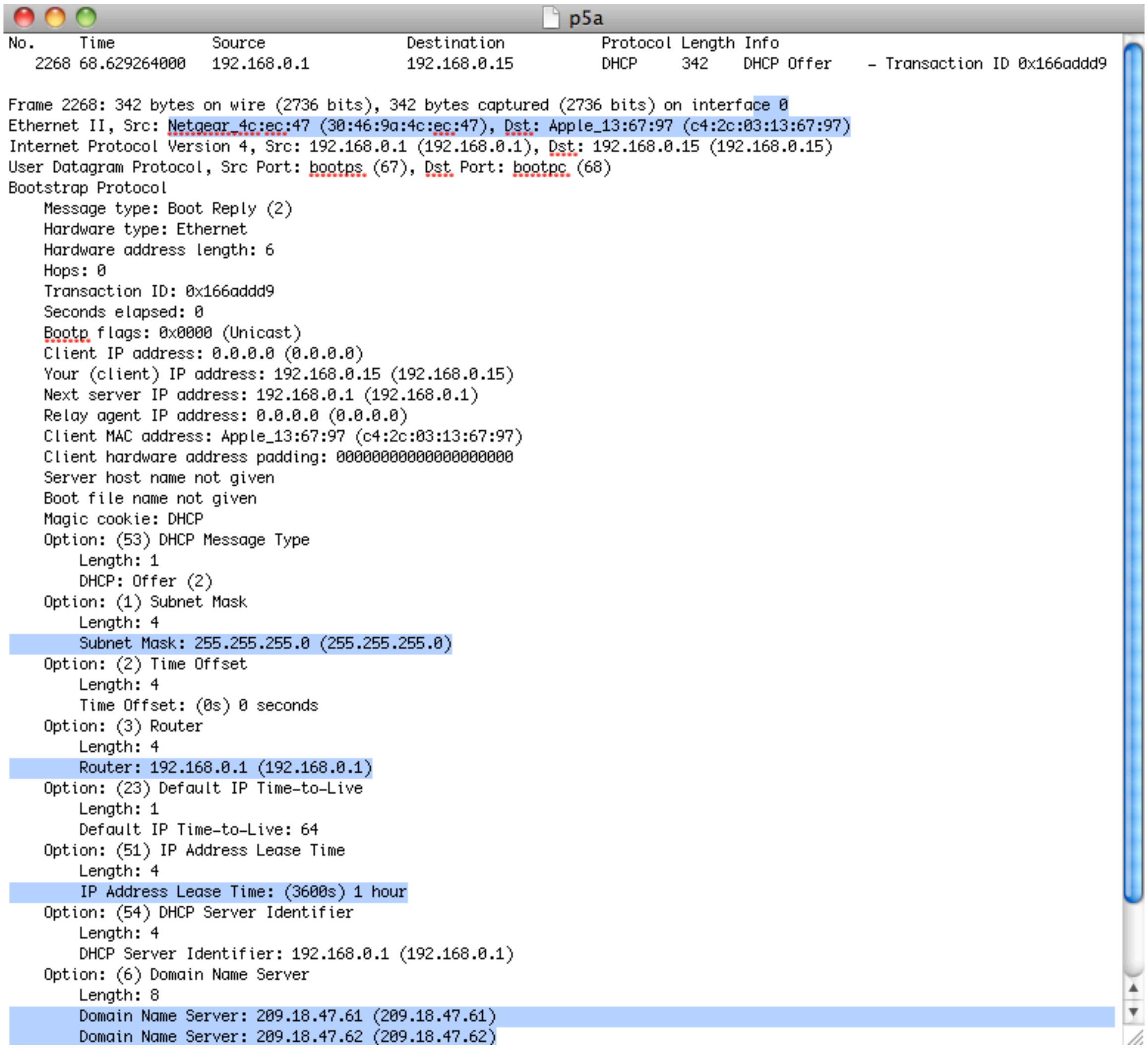
```
No.     Time             Source              Destination         Protocol Length Info
   2270 69.669785000    0.0.0.0             255.255.255.255     DHCP     342    DHCP Request  -
Transaction ID 0x166addd9

Frame 2270: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: Apple_13:67:97 (c4:2c:03:13:67:97), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable
Transport))
    Total Length: 328
    Identification: 0x7710 (30480)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: UDP (17)
    Header checksum: 0x4395 [correct]
    Source: 0.0.0.0 (0.0.0.0)
    Destination: 255.255.255.255 (255.255.255.255)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
    Source port: bootpc (68)
    Destination port: bootps (67)
```

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.



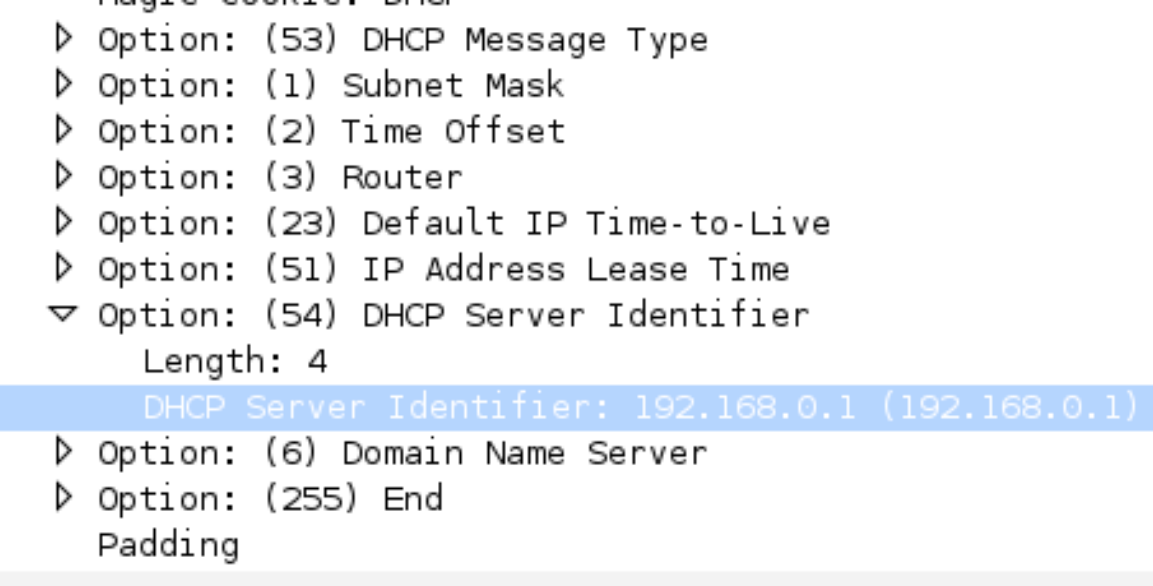
```
No.     Time             Source              Destination         Protocol Length Info
   2283 70.668533000    192.168.0.1         192.168.0.15        DHCP     342    DHCP ACK      -
Transaction ID 0x166addd9

Frame 2283: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: Netgear_4c:ec:47 (30:46:9a:4c:ec:47), Dst: Apple_13:67:97 (c4:2c:03:13:67:97)
Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.15 (192.168.0.15)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable
Transport))
    Total Length: 328
    Identification: 0xdead (57005)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0xd996 [correct]
    Source: 192.168.0.1 (192.168.0.1)
    Destination: 192.168.0.15 (192.168.0.15)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
    Source port: bootps (67)
    Destination port: bootpc (68)
```

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.



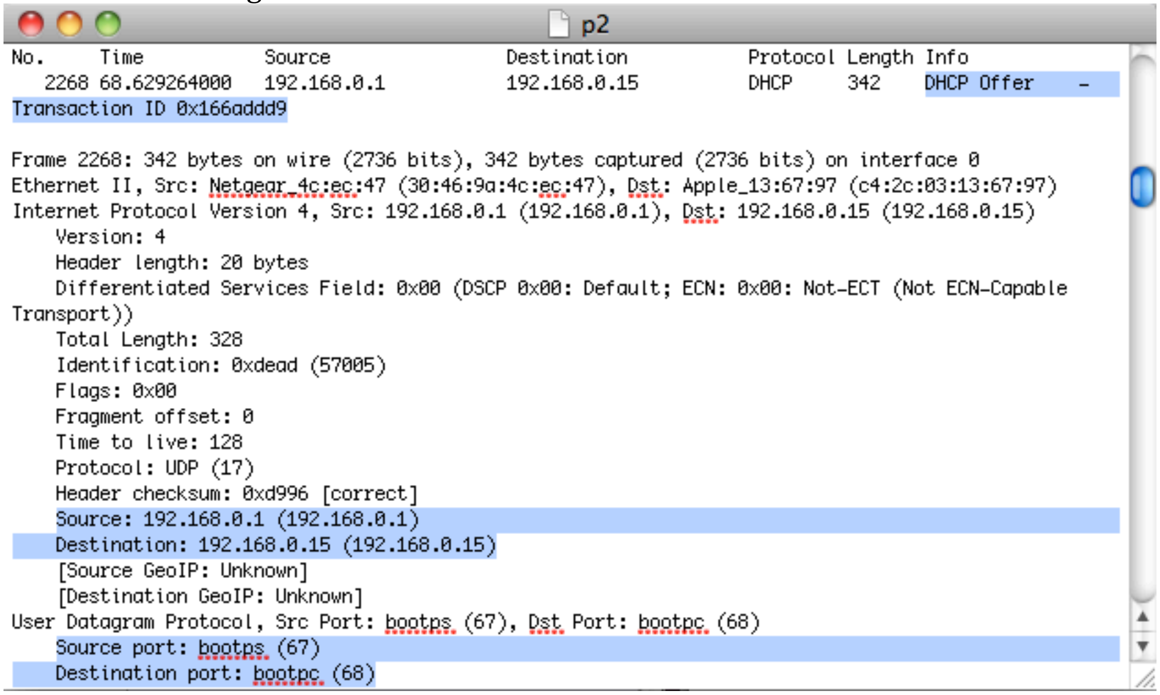
```
No.     Time              Source               Destination          Protocol Length Info
   2268 68.629264000    192.168.0.1          192.168.0.15         DHCP      342    DHCP Offer    - Transaction ID 0x166addd9

Frame 2268: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: Netgear_4c:ec:47 (30:46:9a:4c:ec:47), Dst: Apple_13:67:97 (c4:2c:03:13:67:97)
Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.15 (192.168.0.15)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x166addd9
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 192.168.0.15 (192.168.0.15)
    Next server IP address: 192.168.0.1 (192.168.0.1)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: Apple_13:67:97 (c4:2c:03:13:67:97)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    Option: (53) DHCP Message Type
        Length: 1
        DHCP: Offer (2)
    Option: (1) Subnet Mask
        Length: 4
        Subnet Mask: 255.255.255.0 (255.255.255.0)
    Option: (2) Time Offset
        Length: 4
        Time Offset: (0s) 0 seconds
    Option: (3) Router
        Length: 4
        Router: 192.168.0.1 (192.168.0.1)
    Option: (23) Default IP Time-to-Live
        Length: 1
        Default IP Time-to-Live: 64
    Option: (51) IP Address Lease Time
        Length: 4
        IP Address Lease Time: (3600s) 1 hour
    Option: (54) DHCP Server Identifier
        Length: 4
        DHCP Server Identifier: 192.168.0.1 (192.168.0.1)
    Option: (6) Domain Name Server
        Length: 8
        Domain Name Server: 209.18.47.61 (209.18.47.61)
        Domain Name Server: 209.18.47.62 (209.18.47.62)
```

7) The IP address of my DHCP server is 192.168.0.1



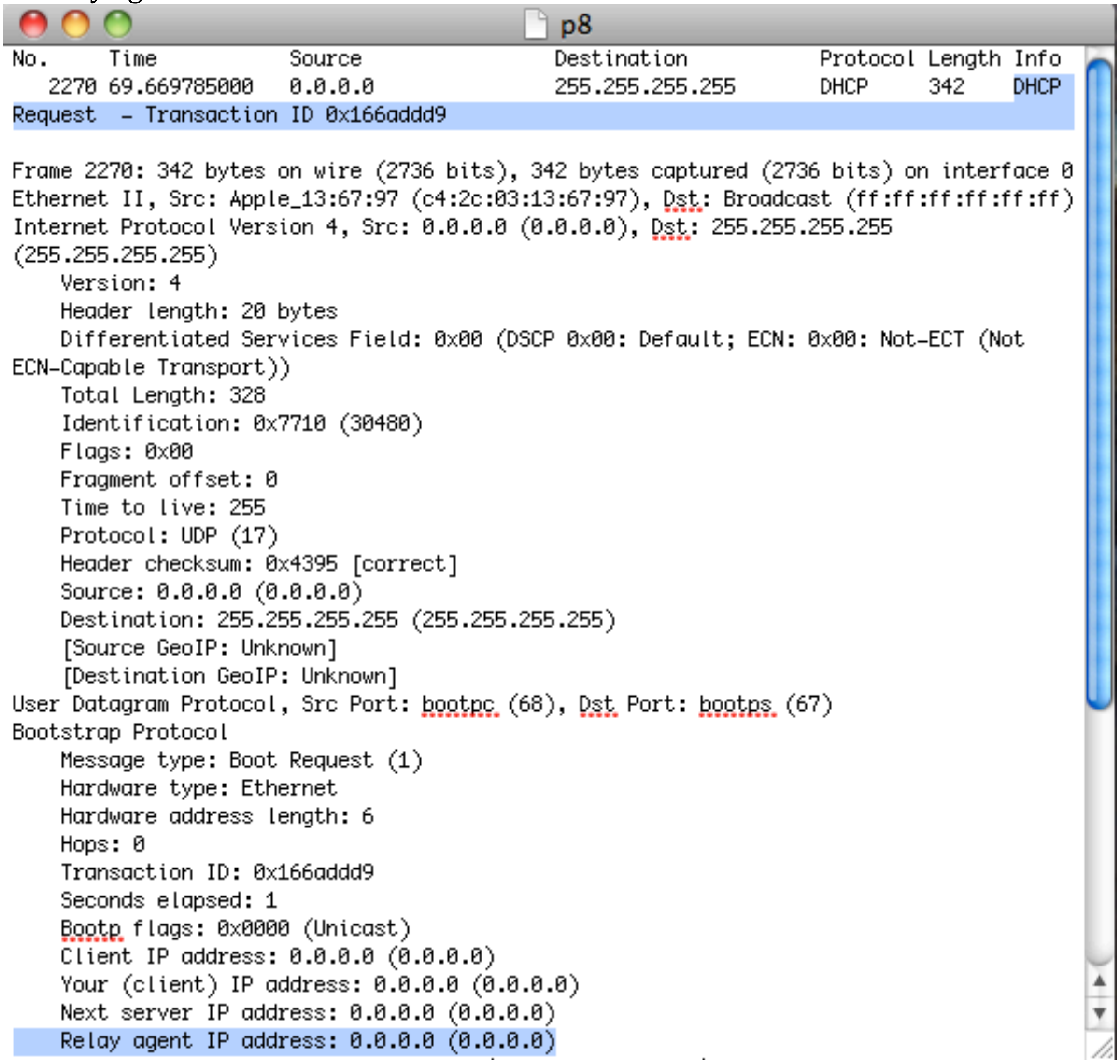
```
▷ Option: (53) DHCP Message Type
▷ Option: (1) Subnet Mask
▷ Option: (2) Time Offset
▷ Option: (3) Router
▷ Option: (23) Default IP Time-to-Live
▷ Option: (51) IP Address Lease Time
▽ Option: (54) DHCP Server Identifier
    Length: 4
    DHCP Server Identifier: 192.168.0.1 (192.168.0.1)
▷ Option: (6) Domain Name Server
▷ Option: (255) End
  Padding
```

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



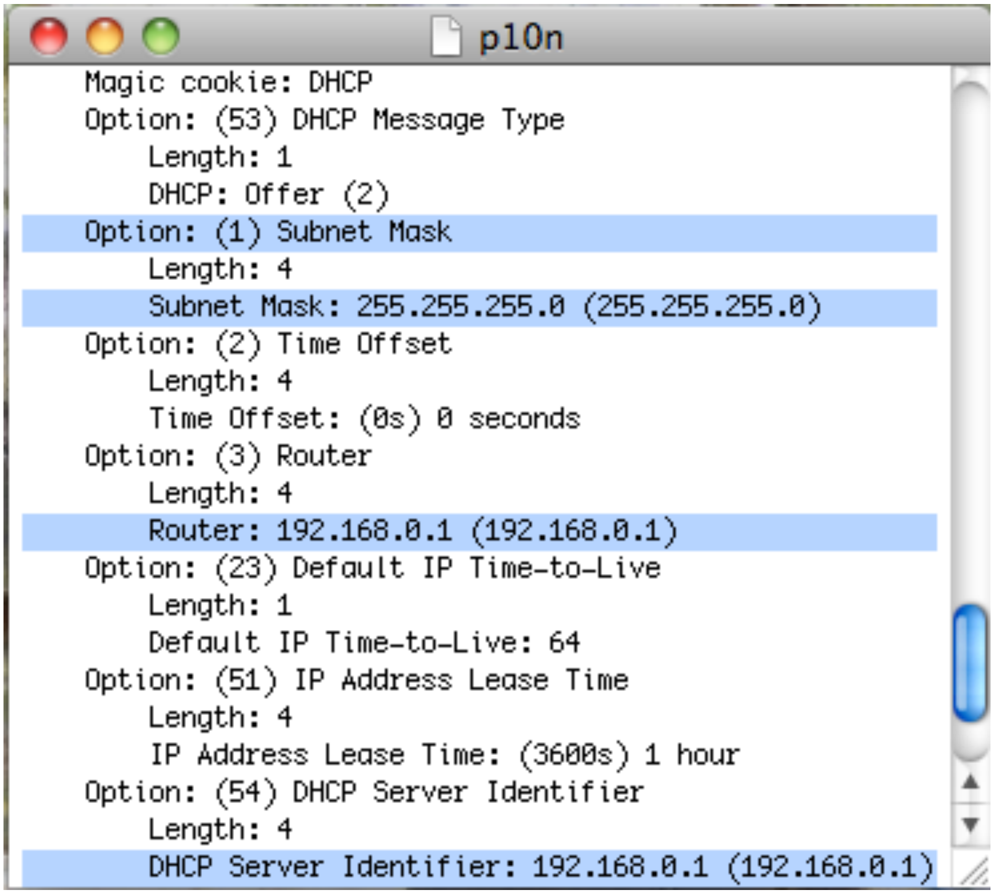
```
No.     Time            Source              Destination         Protocol Length Info
   2268 68.629264000    192.168.0.1         192.168.0.15        DHCP     342    DHCP Offer    -
Transaction ID 0x166addd9

Frame 2268: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: Netgear_4c:ec:47 (30:46:9a:4c:ec:47), Dst: Apple_13:67:97 (c4:2c:03:13:67:97)
Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.15 (192.168.0.15)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable
Transport))
    Total Length: 328
    Identification: 0xdead (57005)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0xd996 [correct]
    Source: 192.168.0.1 (192.168.0.1)
    Destination: 192.168.0.15 (192.168.0.15)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
    Source port: bootps (67)
    Destination port: bootpc (68)
```

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



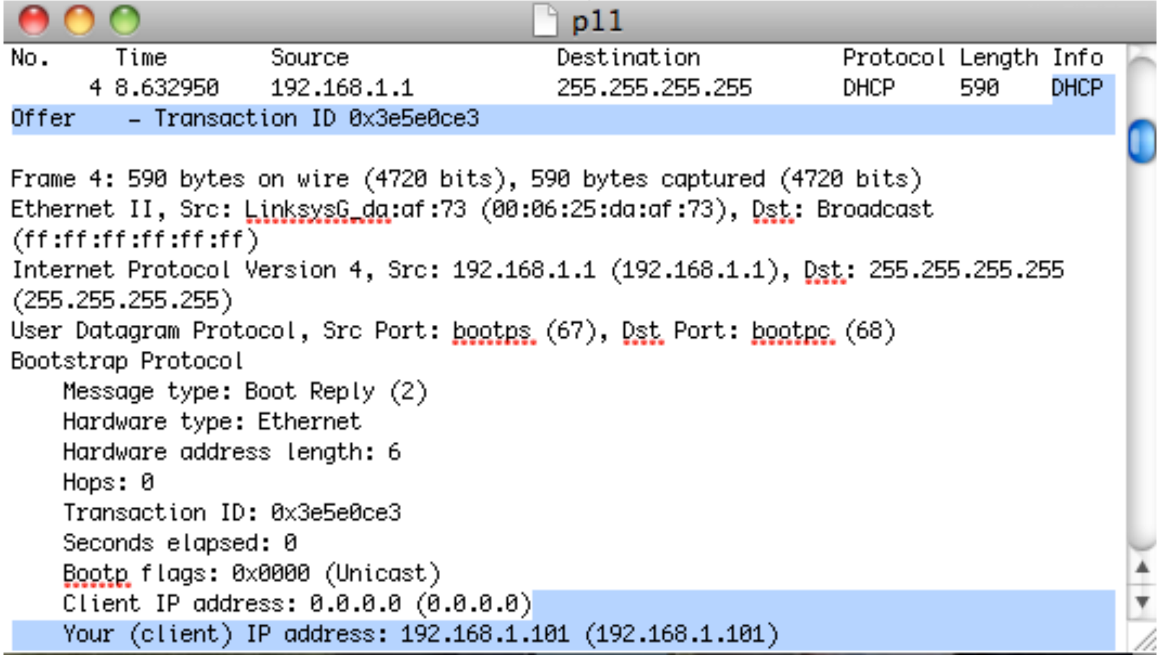
```
No.     Time           Source                Destination           Protocol Length Info
   2270 69.669785000   0.0.0.0               255.255.255.255       DHCP     342    DHCP
Request  - Transaction ID 0x166addd9

Frame 2270: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: Apple_13:67:97 (c4:2c:03:13:67:97), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255
(255.255.255.255)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not
ECN-Capable Transport))
    Total Length: 328
    Identification: 0x7710 (30480)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: UDP (17)
    Header checksum: 0x4395 [correct]
    Source: 0.0.0.0 (0.0.0.0)
    Destination: 255.255.255.255 (255.255.255.255)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x166addd9
    Seconds elapsed: 1
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
```

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.

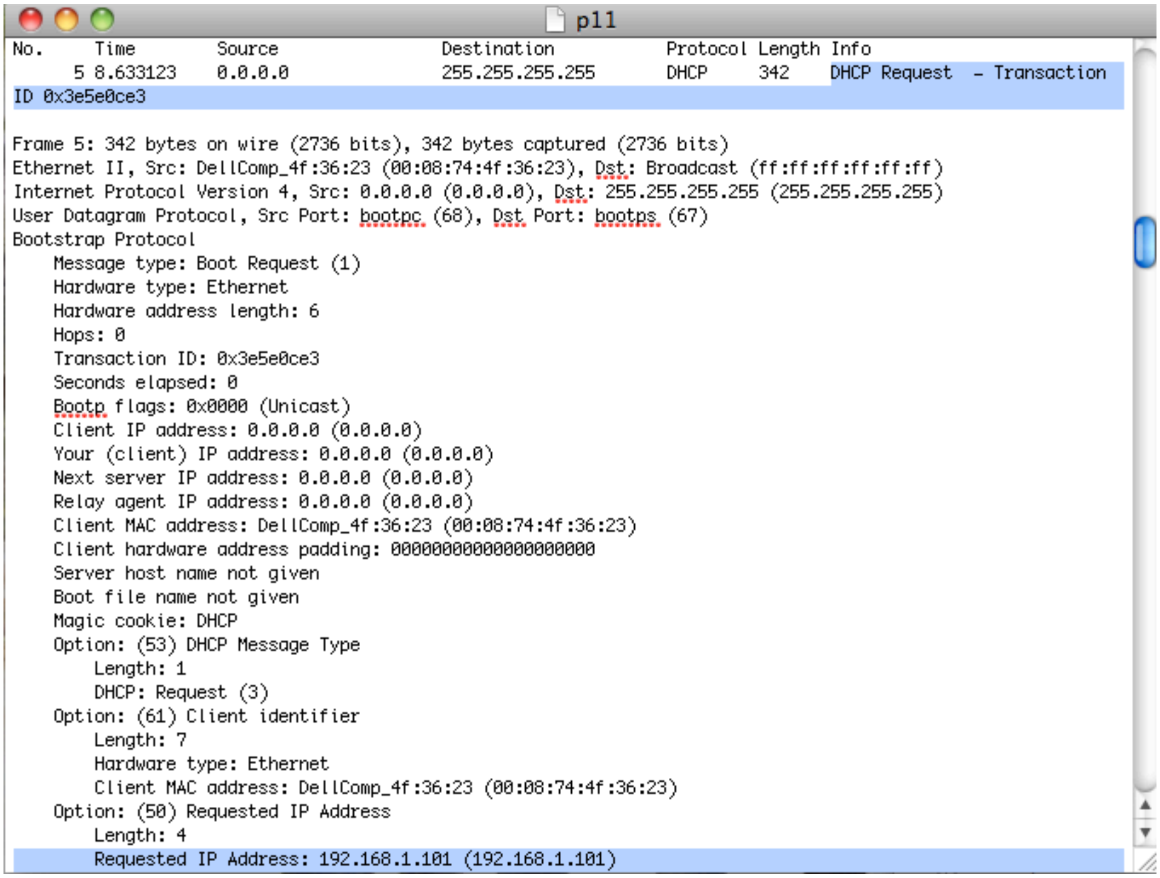


```
    Magic cookie: DHCP
    Option: (53) DHCP Message Type
        Length: 1
        DHCP: Offer (2)
    Option: (1) Subnet Mask
        Length: 4
        Subnet Mask: 255.255.255.0 (255.255.255.0)
    Option: (2) Time Offset
        Length: 4
        Time Offset: (0s) 0 seconds
    Option: (3) Router
        Length: 4
        Router: 192.168.0.1 (192.168.0.1)
    Option: (23) Default IP Time-to-Live
        Length: 1
        Default IP Time-to-Live: 64
    Option: (51) IP Address Lease Time
        Length: 4
        IP Address Lease Time: (3600s) 1 hour
    Option: (54) DHCP Server Identifier
        Length: 4
        DHCP Server Identifier: 192.168.0.1 (192.168.0.1)
```

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

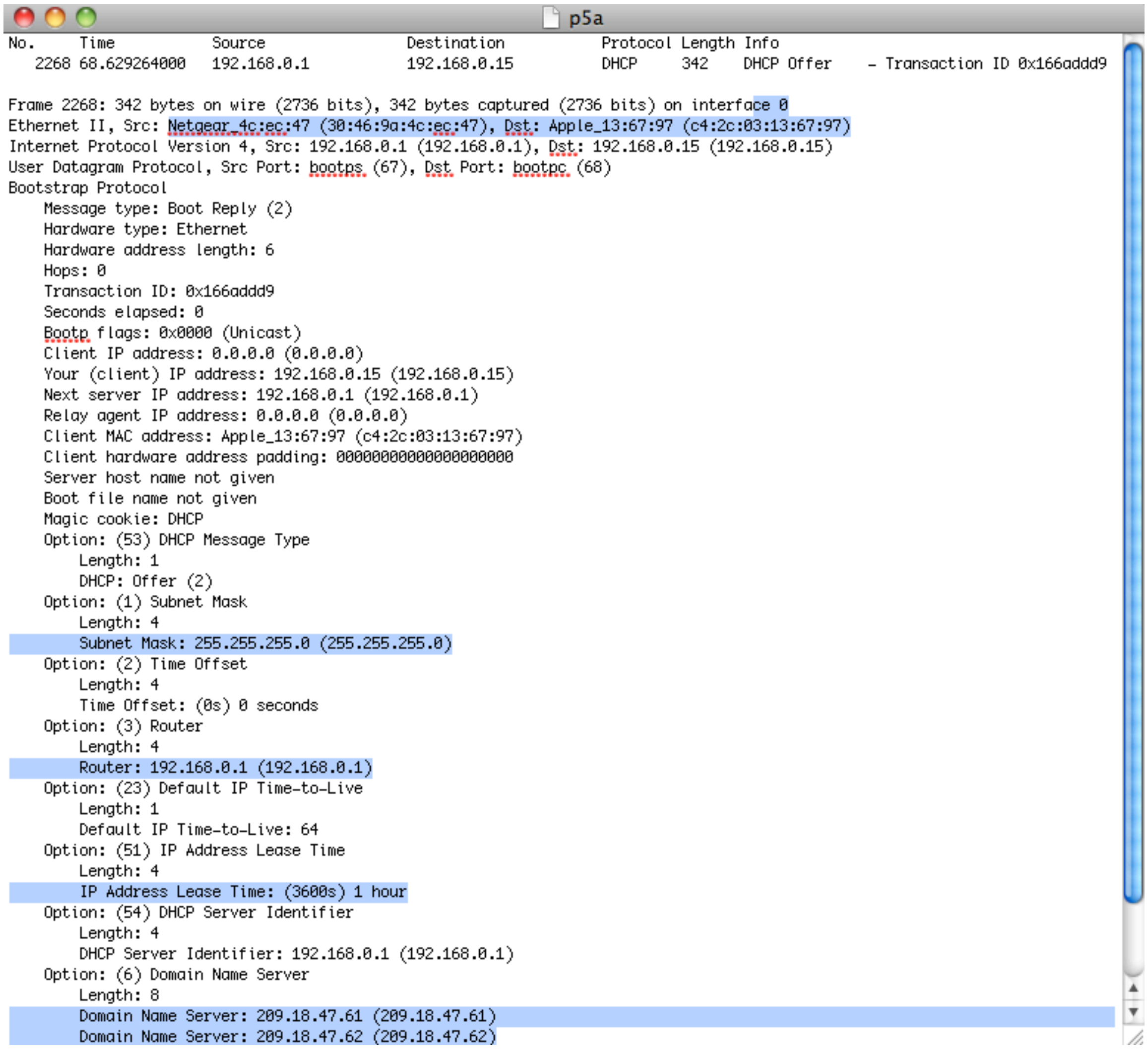


```
No.     Time        Source              Destination         Protocol Length Info
      4 8.632950    192.168.1.1         255.255.255.255     DHCP     590    DHCP
Offer    - Transaction ID 0x3e5e0ce3

Frame 4: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits)
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 255.255.255.255
(255.255.255.255)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x3e5e0ce3
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 192.168.1.101 (192.168.1.101)
```



```
No.     Time        Source                Destination           Protocol Length Info
      5 8.633123    0.0.0.0               255.255.255.255       DHCP     342    DHCP Request  - Transaction
ID 0x3e5e0ce3

Frame 5: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
Ethernet II, Src: DellComp_4f:36:23 (00:08:74:4f:36:23), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x3e5e0ce3
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: DellComp_4f:36:23 (00:08:74:4f:36:23)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    Option: (53) DHCP Message Type
        Length: 1
        DHCP: Request (3)
    Option: (61) Client identifier
        Length: 7
        Hardware type: Ethernet
        Client MAC address: DellComp_4f:36:23 (00:08:74:4f:36:23)
    Option: (50) Requested IP Address
        Length: 4
        Requested IP Address: 192.168.1.101 (192.168.1.101)
```

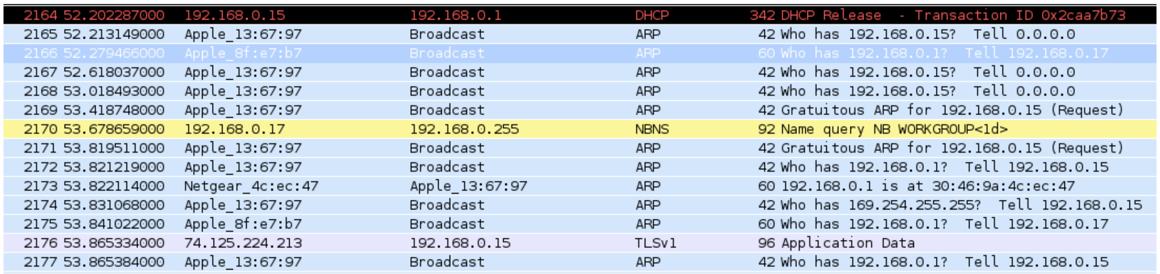
12) The purpose of the lease time is so as to not dedicate a path for a host because there are limited connections to be offered. The lease time is 1 hour.



```
No.      Time             Source              Destination         Protocol Length Info
   2268 68.629264000    192.168.0.1         192.168.0.15        DHCP     342    DHCP Offer    - Transaction ID 0x166addd9

Frame 2268: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: Netgear_4c:ec:47 (30:46:9a:4c:ec:47), Dst: Apple_13:67:97 (c4:2c:03:13:67:97)
Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.15 (192.168.0.15)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x166addd9
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 192.168.0.15 (192.168.0.15)
    Next server IP address: 192.168.0.1 (192.168.0.1)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: Apple_13:67:97 (c4:2c:03:13:67:97)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    Option: (53) DHCP Message Type
        Length: 1
        DHCP: Offer (2)
    Option: (1) Subnet Mask
        Length: 4
        Subnet Mask: 255.255.255.0 (255.255.255.0)
    Option: (2) Time Offset
        Length: 4
        Time Offset: (0s) 0 seconds
    Option: (3) Router
        Length: 4
        Router: 192.168.0.1 (192.168.0.1)
    Option: (23) Default IP Time-to-Live
        Length: 1
        Default IP Time-to-Live: 64
    Option: (51) IP Address Lease Time
        Length: 4
        IP Address Lease Time: (3600s) 1 hour
    Option: (54) DHCP Server Identifier
        Length: 4
        DHCP Server Identifier: 192.168.0.1 (192.168.0.1)
    Option: (6) Domain Name Server
        Length: 8
        Domain Name Server: 209.18.47.61 (209.18.47.61)
        Domain Name Server: 209.18.47.62 (209.18.47.62)
```

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.

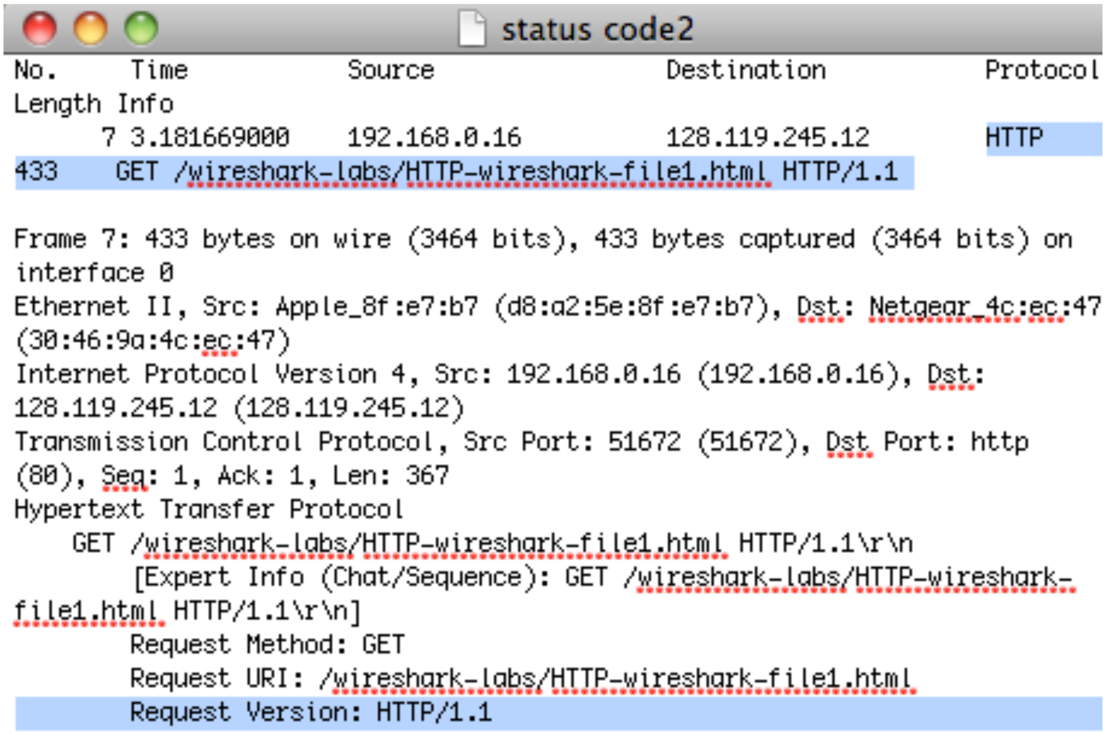
14) Yes there were ARP packets sent. These packets are used to navigate from router to router to reach the DHCP server and back to the host because although source and destination IP addresses do not change during transmission, the physical addresses do especially if it takes multiple hops to reach the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



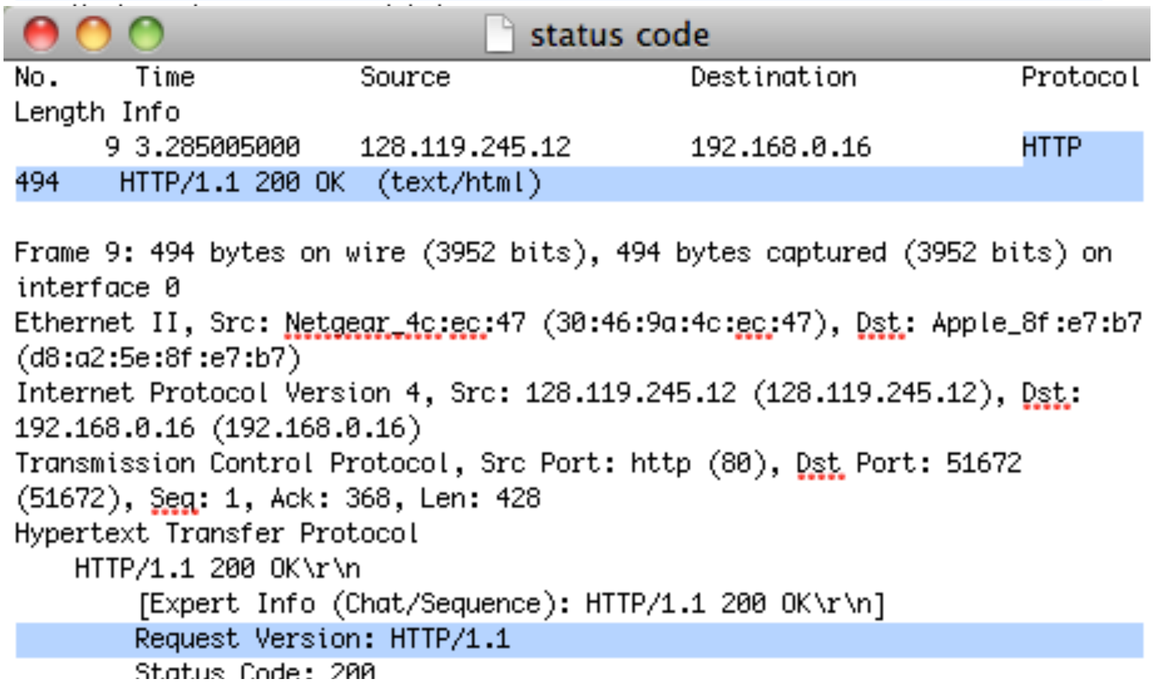
```
2164 52.202287000  192.168.0.15      192.168.0.1     DHCP   342 DHCP Release  - Transaction ID 0x2caa7b73
2165 52.213149000  Apple_13:67:97    Broadcast       ARP     42 Who has 192.168.0.15?  Tell 0.0.0.0
2166 52.279466000  Apple_8f:e7:b7    Broadcast       ARP     60 Who has 192.168.0.1?  Tell 192.168.0.17
2167 52.618037000  Apple_13:67:97    Broadcast       ARP     42 Who has 192.168.0.15?  Tell 0.0.0.0
2168 53.018493000  Apple_13:67:97    Broadcast       ARP     42 Who has 192.168.0.15?  Tell 0.0.0.0
2169 53.418748000  Apple_13:67:97    Broadcast       ARP     42 Gratuitous ARP for 192.168.0.15 (Request)
2170 53.678659000  192.168.0.17      192.168.0.255   NBNS    92 Name query NB WORKGROUP<1d>
2171 53.819511000  Apple_13:67:97    Broadcast       ARP     42 Gratuitous ARP for 192.168.0.15 (Request)
2172 53.821219000  Apple_13:67:97    Broadcast       ARP     42 Who has 192.168.0.1?  Tell 192.168.0.15
2173 53.822114000  Netgear_4c:ec:47  Apple_13:67:97  ARP     60 192.168.0.1 is at 30:46:9a:4c:ec:47
2174 53.831068000  Apple_13:67:97    Broadcast       ARP     42 Who has 169.254.255.255?  Tell 192.168.0.15
2175 53.841022000  Apple_8f:e7:b7    Broadcast       ARP     60 Who has 192.168.0.1?  Tell 192.168.0.17
2176 53.865334000  74.125.224.213    192.168.0.15    TLSv1   96 Application Data
2177 53.865384000  Apple_13:67:97    Broadcast       ARP     42 Who has 192.168.0.1?  Tell 192.168.0.15
```

Part II

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

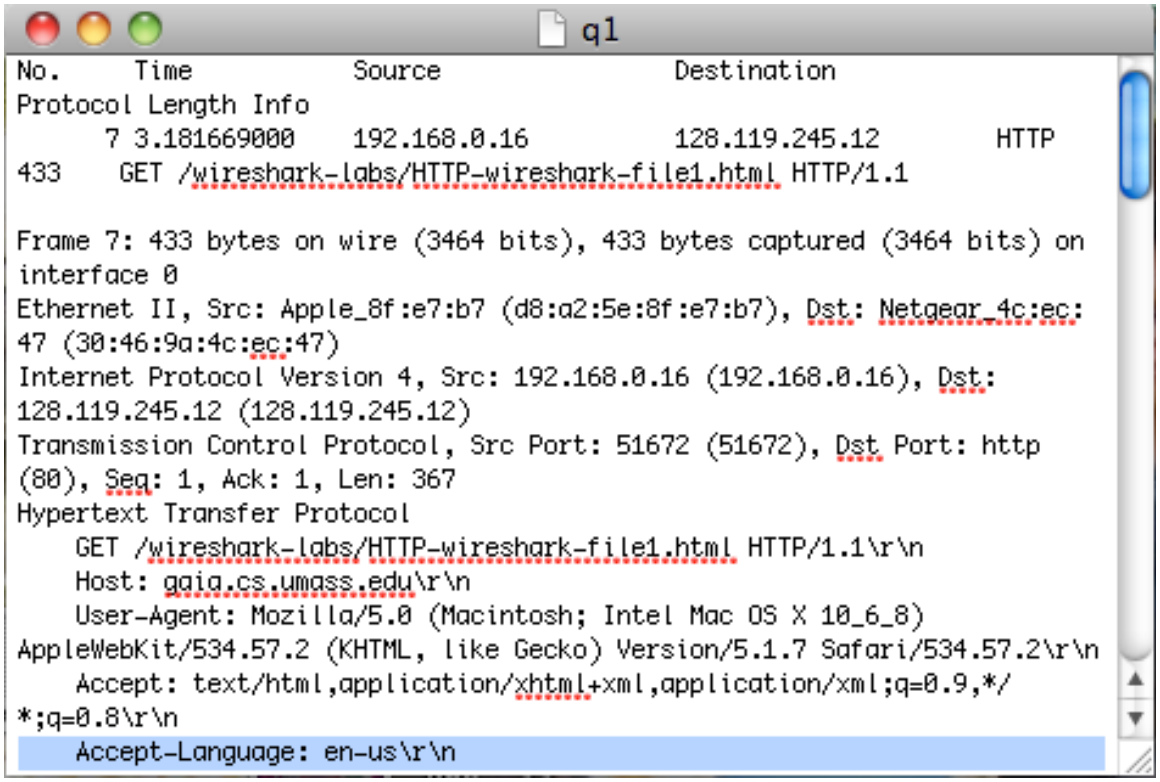


```
No.      Time              Source                Destination           Protocol
Length Info
      7 3.181669000     192.168.0.16          128.119.245.12        HTTP
433     GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

Frame 7: 433 bytes on wire (3464 bits), 433 bytes captured (3464 bits) on
interface 0
Ethernet II, Src: Apple_8f:e7:b7 (d8:a2:5e:8f:e7:b7), Dst: Netgear_4c:ec:47
(30:46:9a:4c:ec:47)
Internet Protocol Version 4, Src: 192.168.0.16 (192.168.0.16), Dst:
128.119.245.12 (128.119.245.12)
Transmission Control Protocol, Src Port: 51672 (51672), Dst Port: http
(80), Seq: 1, Ack: 1, Len: 367
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-
file1.html HTTP/1.1\r\n]
        Request Method: GET
        Request URI: /wireshark-labs/HTTP-wireshark-file1.html
        Request Version: HTTP/1.1
```



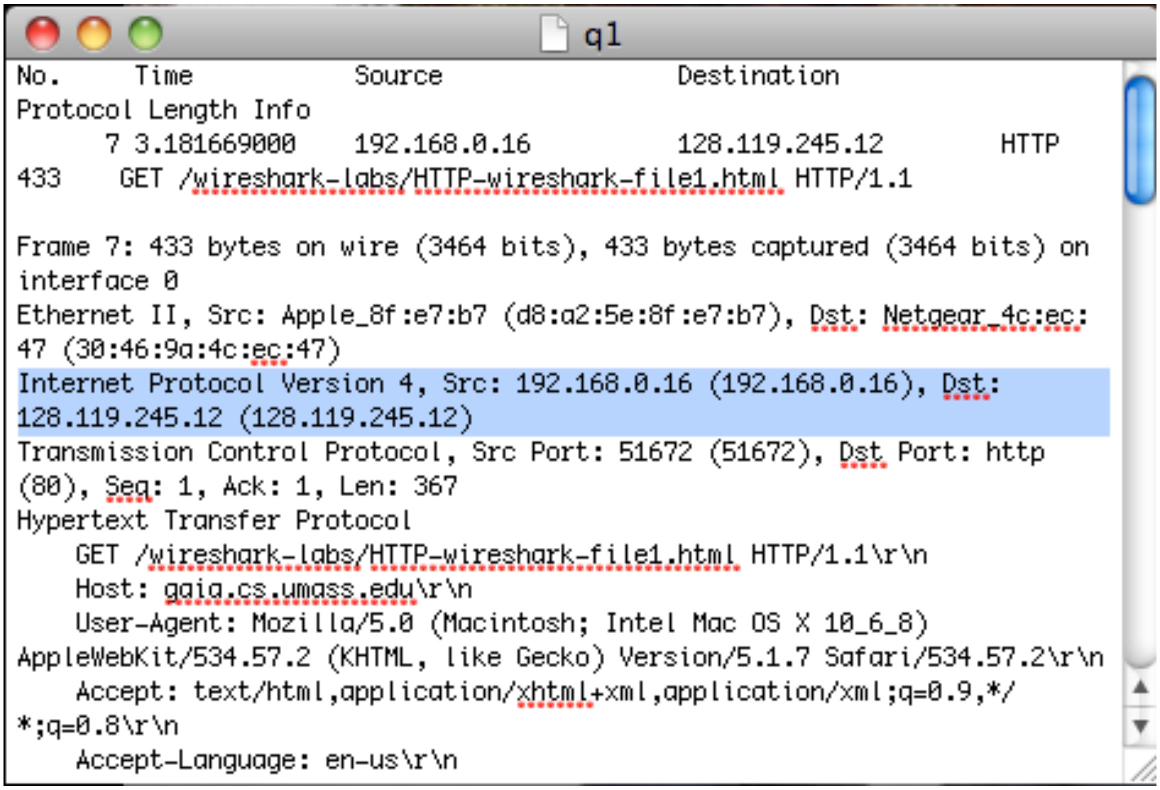
```
No.      Time              Source                Destination           Protocol
Length Info
      9 3.285005000     128.119.245.12        192.168.0.16          HTTP
494     HTTP/1.1 200 OK  (text/html)

Frame 9: 494 bytes on wire (3952 bits), 494 bytes captured (3952 bits) on
interface 0
Ethernet II, Src: Netgear_4c:ec:47 (30:46:9a:4c:ec:47), Dst: Apple_8f:e7:b7
(d8:a2:5e:8f:e7:b7)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst:
192.168.0.16 (192.168.0.16)
Transmission Control Protocol, Src Port: http (80), Dst Port: 51672
(51672), Seq: 1, Ack: 368, Len: 428
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        Request Version: HTTP/1.1
        Status Code: 200
```

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



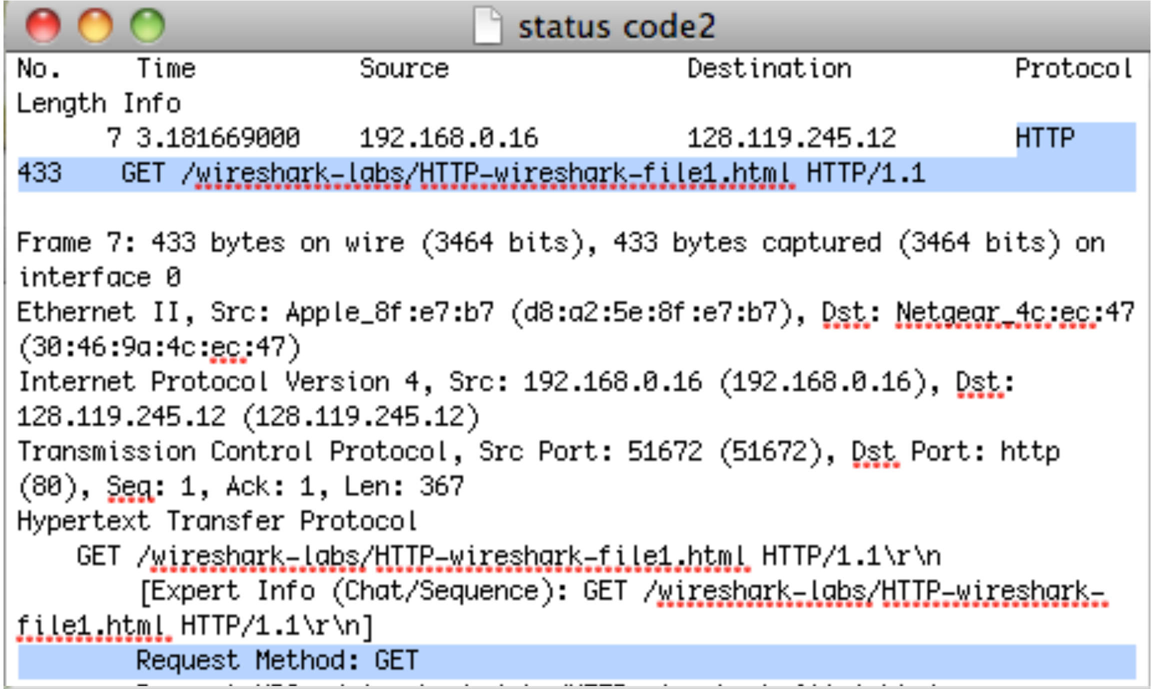
```
No.     Time           Source                Destination
Protocol Length Info
      7 3.181669000    192.168.0.16          128.119.245.12        HTTP
433    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

Frame 7: 433 bytes on wire (3464 bits), 433 bytes captured (3464 bits) on
interface 0
Ethernet II, Src: Apple_8f:e7:b7 (d8:a2:5e:8f:e7:b7), Dst: Netgear_4c:ec:
47 (30:46:9a:4c:ec:47)
Internet Protocol Version 4, Src: 192.168.0.16 (192.168.0.16), Dst:
128.119.245.12 (128.119.245.12)
Transmission Control Protocol, Src Port: 51672 (51672), Dst Port: http
(80), Seq: 1, Ack: 1, Len: 367
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8)
AppleWebKit/534.57.2 (KHTML, like Gecko) Version/5.1.7 Safari/534.57.2\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/
*;q=0.8\r\n
    Accept-Language: en-us\r\n
```

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

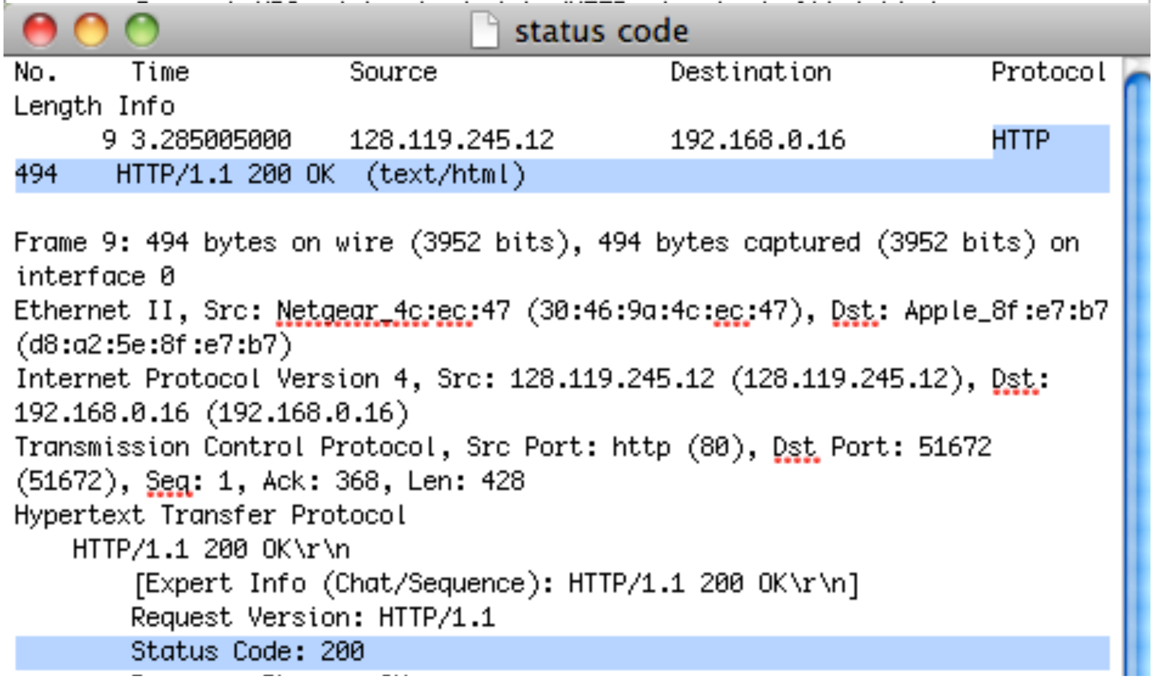


```
No.     Time           Source                Destination
Protocol Length Info
      7 3.181669000    192.168.0.16          128.119.245.12        HTTP
433    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

Frame 7: 433 bytes on wire (3464 bits), 433 bytes captured (3464 bits) on
interface 0
Ethernet II, Src: Apple_8f:e7:b7 (d8:a2:5e:8f:e7:b7), Dst: Netgear_4c:ec:
47 (30:46:9a:4c:ec:47)
Internet Protocol Version 4, Src: 192.168.0.16 (192.168.0.16), Dst:
128.119.245.12 (128.119.245.12)
Transmission Control Protocol, Src Port: 51672 (51672), Dst Port: http
(80), Seq: 1, Ack: 1, Len: 367
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8)
AppleWebKit/534.57.2 (KHTML, like Gecko) Version/5.1.7 Safari/534.57.2\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/
*;q=0.8\r\n
    Accept-Language: en-us\r\n
```

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

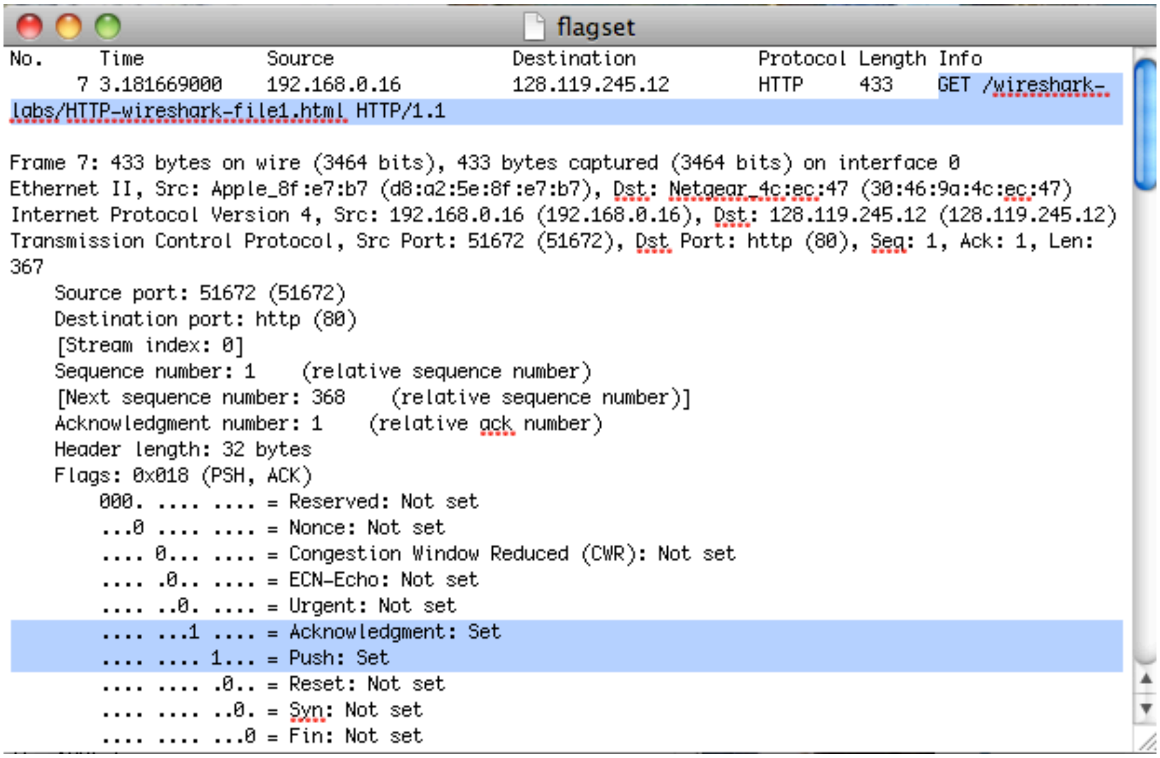


```
No.     Time            Source                Destination           Protocol
Length Info
      7 3.181669000     192.168.0.16          128.119.245.12        HTTP
433     GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

Frame 7: 433 bytes on wire (3464 bits), 433 bytes captured (3464 bits) on
interface 0
Ethernet II, Src: Apple_8f:e7:b7 (d8:a2:5e:8f:e7:b7), Dst: Netgear_4c:ec:47
(30:46:9a:4c:ec:47)
Internet Protocol Version 4, Src: 192.168.0.16 (192.168.0.16), Dst:
128.119.245.12 (128.119.245.12)
Transmission Control Protocol, Src Port: 51672 (51672), Dst Port: http
(80), Seq: 1, Ack: 1, Len: 367
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-
file1.html HTTP/1.1\r\n]
        Request Method: GET
```



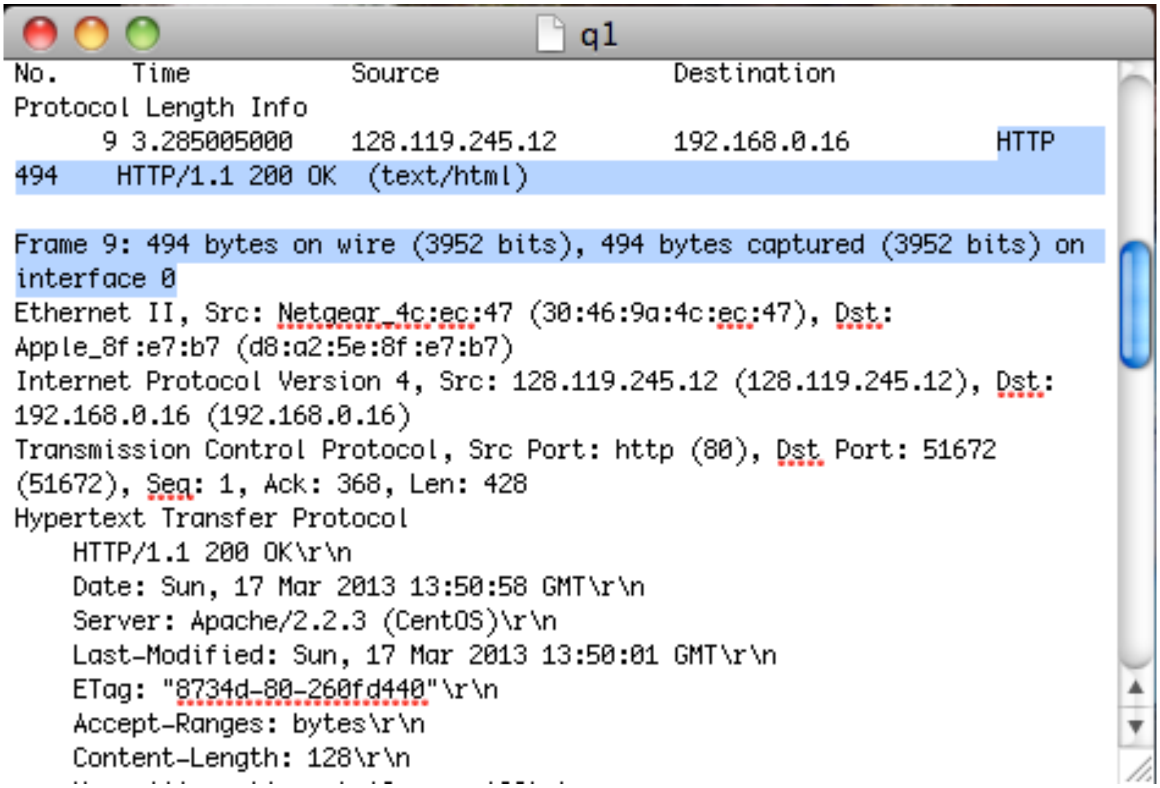
```
No.     Time            Source                Destination           Protocol
Length Info
      9 3.285005000     128.119.245.12        192.168.0.16          HTTP
494     HTTP/1.1 200 OK  (text/html)

Frame 9: 494 bytes on wire (3952 bits), 494 bytes captured (3952 bits) on
interface 0
Ethernet II, Src: Netgear_4c:ec:47 (30:46:9a:4c:ec:47), Dst: Apple_8f:e7:b7
(d8:a2:5e:8f:e7:b7)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst:
192.168.0.16 (192.168.0.16)
Transmission Control Protocol, Src Port: http (80), Dst Port: 51672
(51672), Seq: 1, Ack: 368, Len: 428
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        Request Version: HTTP/1.1
        Status Code: 200
```

5. The Acknowledgment and Push flags were set.



```
No.     Time           Source                Destination           Protocol Length Info
      7 3.181669000    192.168.0.16          128.119.245.12        HTTP     433    GET /wireshark-
labs/HTTP-wireshark-file1.html HTTP/1.1

Frame 7: 433 bytes on wire (3464 bits), 433 bytes captured (3464 bits) on interface 0
Ethernet II, Src: Apple_8f:e7:b7 (d8:a2:5e:8f:e7:b7), Dst: Netgear_4c:ec:47 (30:46:9a:4c:ec:47)
Internet Protocol Version 4, Src: 192.168.0.16 (192.168.0.16), Dst: 128.119.245.12 (128.119.245.12)
Transmission Control Protocol, Src Port: 51672 (51672), Dst Port: http (80), Seq: 1, Ack: 1, Len:
367
    Source port: 51672 (51672)
    Destination port: http (80)
    [Stream index: 0]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 368    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Header length: 32 bytes
    Flags: 0x018 (PSH, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Nonce: Not set
        .... 0... .... = Congestion Window Reduced (CWR): Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 1... = Push: Set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
```

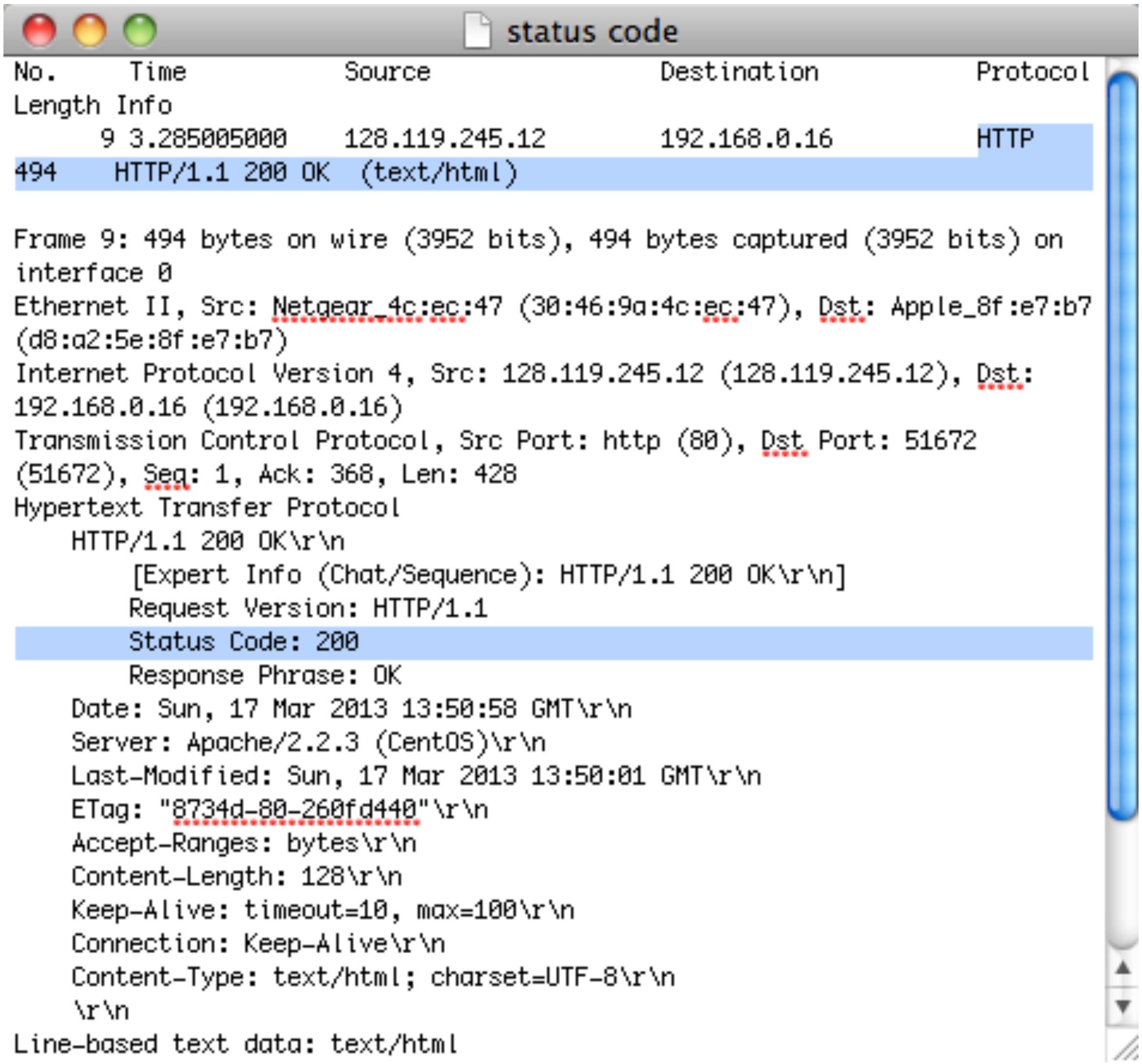
6. 494 bytes are returned to my browser.



```
No.     Time           Source                Destination
Protocol Length Info
      9 3.285005000    128.119.245.12        192.168.0.16          HTTP
494    HTTP/1.1 200 OK  (text/html)

Frame 9: 494 bytes on wire (3952 bits), 494 bytes captured (3952 bits) on
interface 0
Ethernet II, Src: Netgear_4c:ec:47 (30:46:9a:4c:ec:47), Dst:
Apple_8f:e7:b7 (d8:a2:5e:8f:e7:b7)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst:
192.168.0.16 (192.168.0.16)
Transmission Control Protocol, Src Port: http (80), Dst Port: 51672
(51672), Seq: 1, Ack: 368, Len: 428
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Sun, 17 Mar 2013 13:50:58 GMT\r\n
    Server: Apache/2.2.3 (CentOS)\r\n
    Last-Modified: Sun, 17 Mar 2013 13:50:01 GMT\r\n
    ETag: "8734d-80-260fd440"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 128\r\n
```

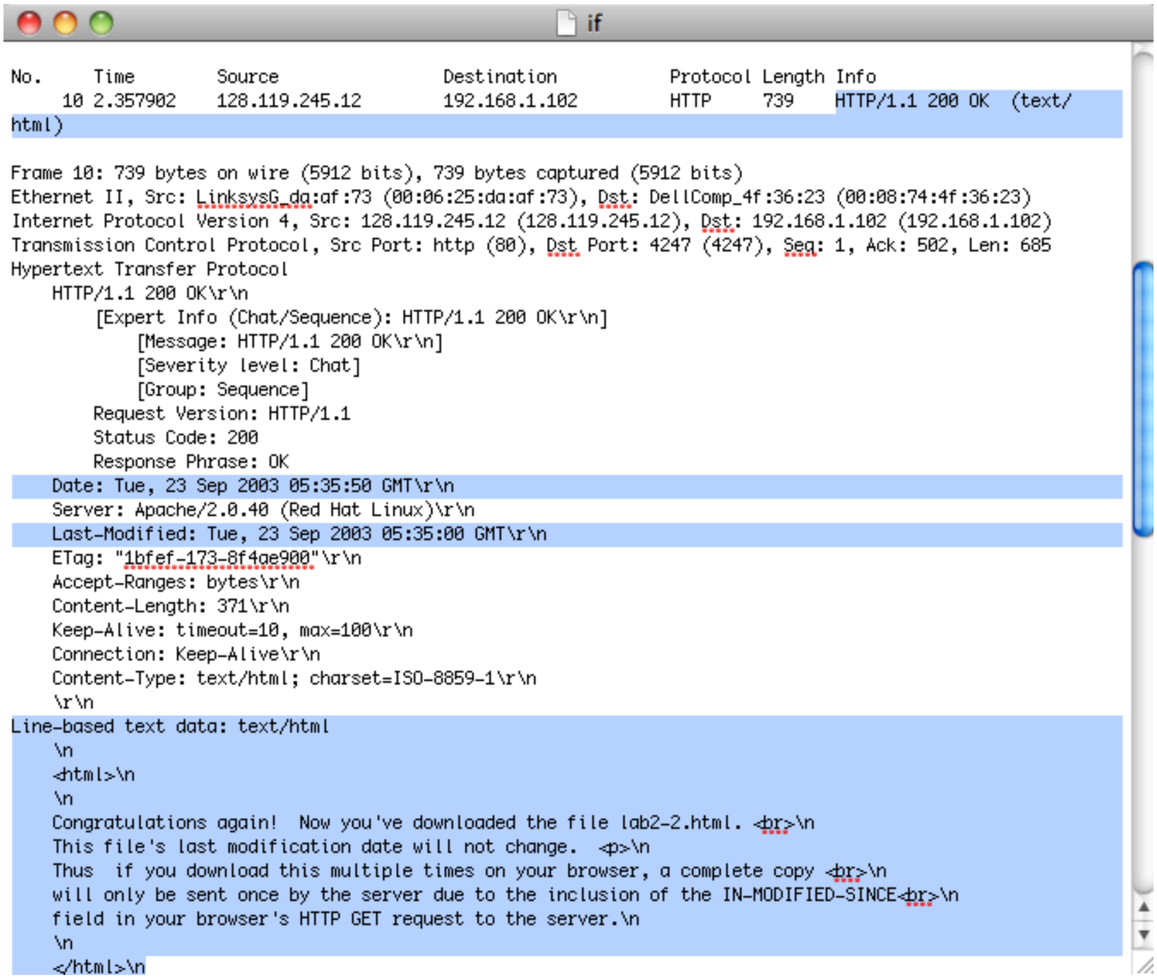
7. Upon inspection, there does not seem to be any headers within the physical data that was not displayed in the packet listing window.

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



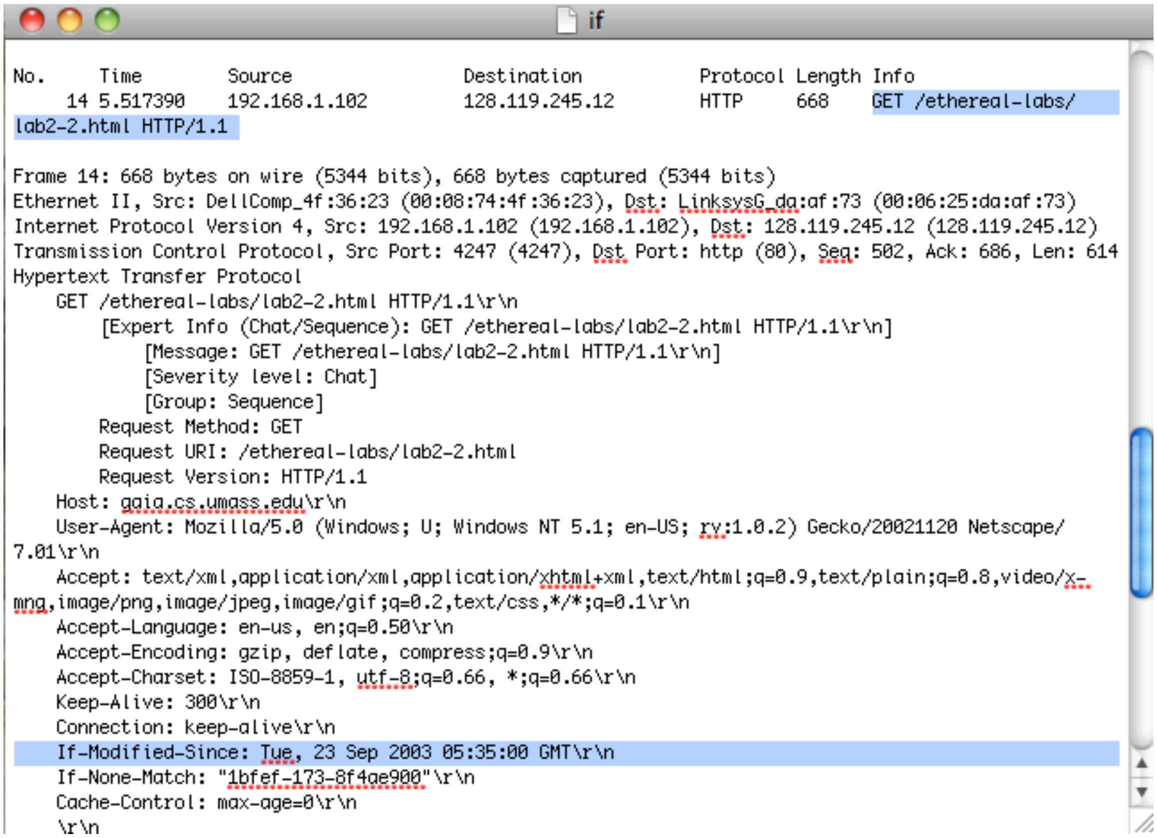
```
No.     Time              Source                Destination           Protocol
Length Info
      9 3.285005000    128.119.245.12        192.168.0.16          HTTP
494    HTTP/1.1 200 OK  (text/html)

Frame 9: 494 bytes on wire (3952 bits), 494 bytes captured (3952 bits) on
interface 0
Ethernet II, Src: Netgear_4c:ec:47 (30:46:9a:4c:ec:47), Dst: Apple_8f:e7:b7
(d8:a2:5e:8f:e7:b7)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst:
192.168.0.16 (192.168.0.16)
Transmission Control Protocol, Src Port: http (80), Dst Port: 51672
(51672), Seq: 1, Ack: 368, Len: 428
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        Request Version: HTTP/1.1
        Status Code: 200
        Response Phrase: OK
    Date: Sun, 17 Mar 2013 13:50:58 GMT\r\n
    Server: Apache/2.2.3 (CentOS)\r\n
    Last-Modified: Sun, 17 Mar 2013 13:50:01 GMT\r\n
    ETag: "8734d-80-260fd440"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 128\r\n
    Keep-Alive: timeout=10, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
Line-based text data: text/html
```

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.



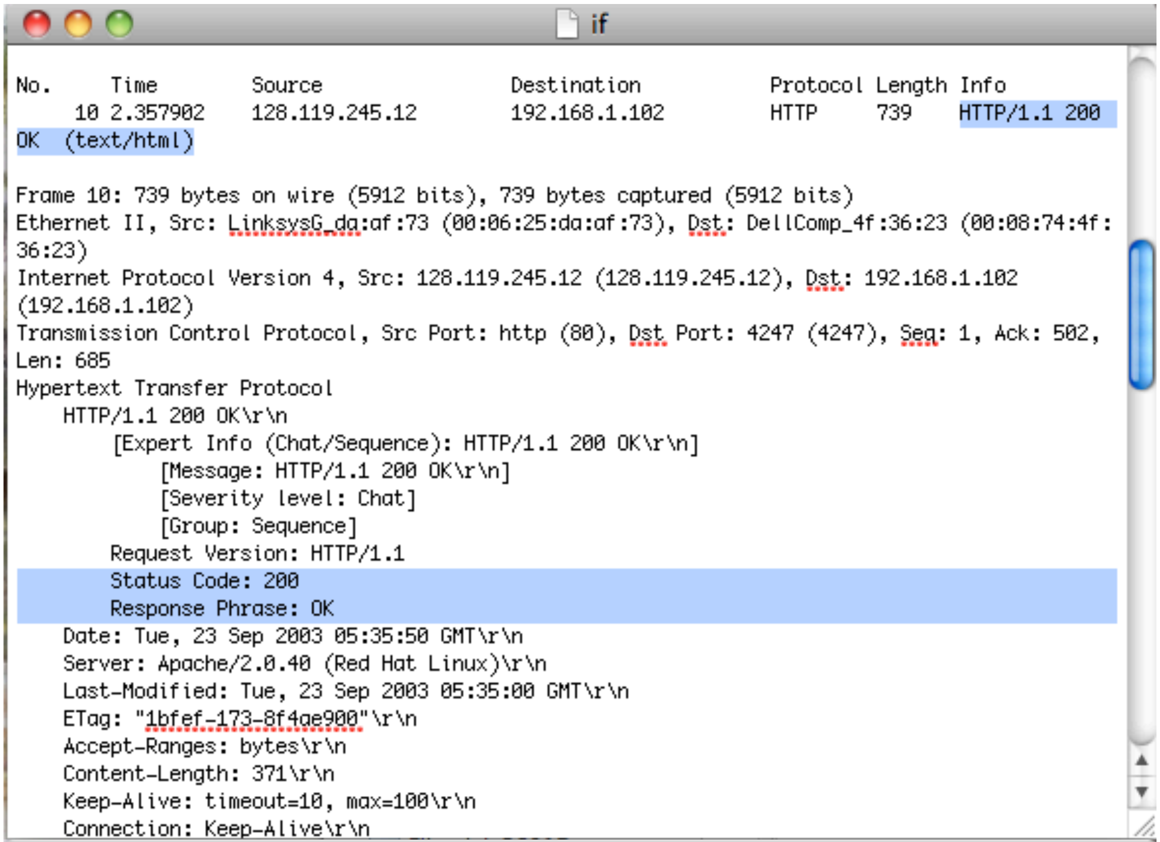
```
No.     Time        Source                Destination           Protocol Length Info
     10 2.357902    128.119.245.12        192.168.1.102         HTTP     739    HTTP/1.1 200 OK  (text/
html)

Frame 10: 739 bytes on wire (5912 bits), 739 bytes captured (5912 bits)
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: DellComp_4f:36:23 (00:08:74:4f:36:23)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.102 (192.168.1.102)
Transmission Control Protocol, Src Port: http (80), Dst Port: 4247 (4247), Seq: 1, Ack: 502, Len: 685
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
            [Message: HTTP/1.1 200 OK\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Version: HTTP/1.1
        Status Code: 200
        Response Phrase: OK
    Date: Tue, 23 Sep 2003 05:35:50 GMT\r\n
    Server: Apache/2.0.40 (Red Hat Linux)\r\n
    Last-Modified: Tue, 23 Sep 2003 05:35:00 GMT\r\n
    ETag: "1bfef-173-8f4ae900"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 371\r\n
    Keep-Alive: timeout=10, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=ISO-8859-1\r\n
    \r\n
Line-based text data: text/html
    \n
    <html>\n
    \n
    Congratulations again!  Now you've downloaded the file lab2-2.html. <br>\n
    This file's last modification date will not change.  <p>\n
    Thus  if you download this multiple times on your browser, a complete copy <br>\n
    will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
    field in your browser's HTTP GET request to the server.\n
    \n
    </html>\n
```

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.

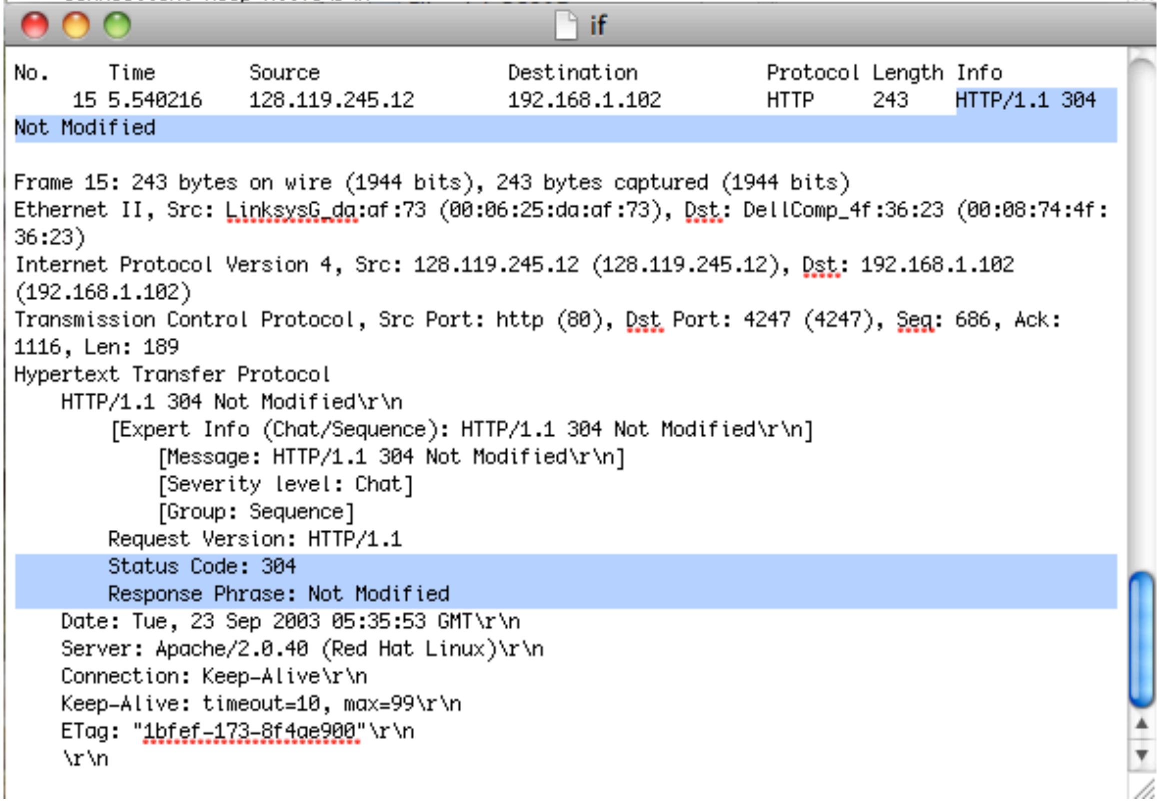


```
No.     Time        Source                Destination           Protocol Length Info
     14 5.517390    192.168.1.102         128.119.245.12        HTTP     668    GET /ethereal-labs/
lab2-2.html HTTP/1.1

Frame 14: 668 bytes on wire (5344 bits), 668 bytes captured (5344 bits)
Ethernet II, Src: DellComp_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: 128.119.245.12 (128.119.245.12)
Transmission Control Protocol, Src Port: 4247 (4247), Dst Port: http (80), Seq: 502, Ack: 686, Len: 614
Hypertext Transfer Protocol
    GET /ethereal-labs/lab2-2.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /ethereal-labs/lab2-2.html HTTP/1.1\r\n]
            [Message: GET /ethereal-labs/lab2-2.html HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
        Request URI: /ethereal-labs/lab2-2.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/
7.01\r\n
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-
mng,image/png,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1\r\n
    Accept-Language: en-us, en;q=0.50\r\n
    Accept-Encoding: gzip, deflate, compress;q=0.9\r\n
    Accept-Charset: ISO-8859-1, utf-8;q=0.66, *;q=0.66\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    If-Modified-Since: Tue, 23 Sep 2003 05:35:00 GMT\r\n
    If-None-Match: "1bfef-173-8f4ae900"\r\n
    Cache-Control: max-age=0\r\n
    \r\n
```

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.

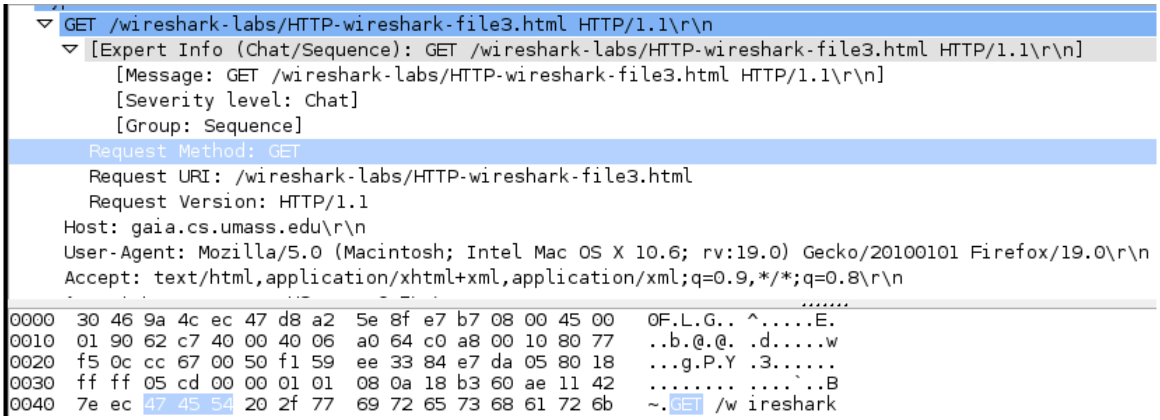


```
No.     Time           Source                Destination           Protocol Length Info
     10 2.357902       128.119.245.12        192.168.1.102         HTTP     739    HTTP/1.1 200
OK  (text/html)

Frame 10: 739 bytes on wire (5912 bits), 739 bytes captured (5912 bits)
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: DellComp_4f:36:23 (00:08:74:4f:
36:23)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.102
(192.168.1.102)
Transmission Control Protocol, Src Port: http (80), Dst Port: 4247 (4247), Seq: 1, Ack: 502,
Len: 685
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
            [Message: HTTP/1.1 200 OK\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Version: HTTP/1.1
        Status Code: 200
        Response Phrase: OK
    Date: Tue, 23 Sep 2003 05:35:50 GMT\r\n
    Server: Apache/2.0.40 (Red Hat Linux)\r\n
    Last-Modified: Tue, 23 Sep 2003 05:35:00 GMT\r\n
    ETag: "1bfef-173-8f4ae900"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 371\r\n
    Keep-Alive: timeout=10, max=100\r\n
    Connection: Keep-Alive\r\n
```



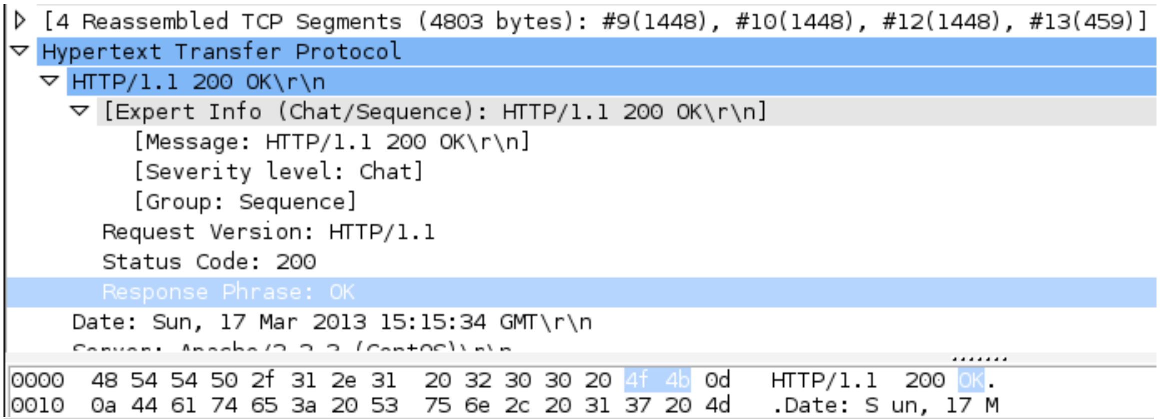
```
No.     Time           Source                Destination           Protocol Length Info
     15 5.540216       128.119.245.12        192.168.1.102         HTTP     243    HTTP/1.1 304
Not Modified

Frame 15: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits)
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: DellComp_4f:36:23 (00:08:74:4f:
36:23)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.102
(192.168.1.102)
Transmission Control Protocol, Src Port: http (80), Dst Port: 4247 (4247), Seq: 686, Ack:
1116, Len: 189
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
            [Message: HTTP/1.1 304 Not Modified\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Version: HTTP/1.1
        Status Code: 304
        Response Phrase: Not Modified
    Date: Tue, 23 Sep 2003 05:35:53 GMT\r\n
    Server: Apache/2.0.40 (Red Hat Linux)\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=10, max=99\r\n
    ETag: "1bfef-173-8f4ae900"\r\n
    \r\n
```

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

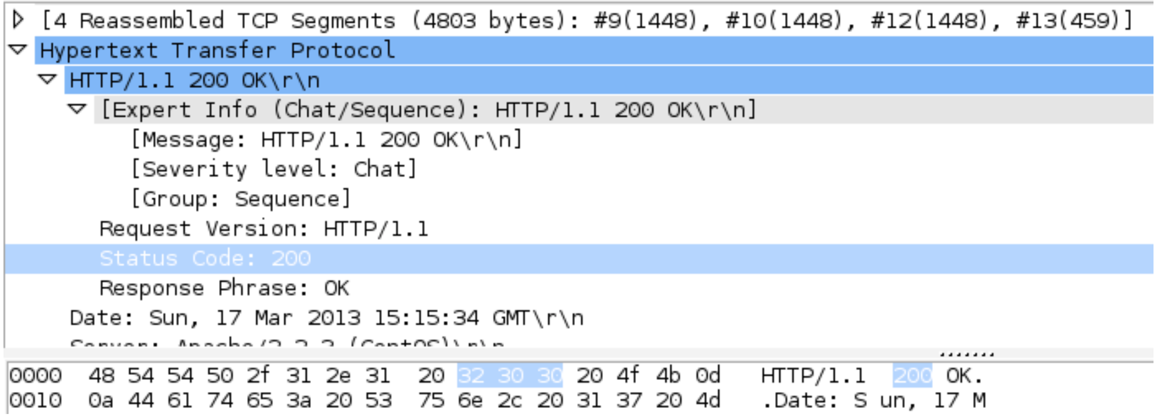


```
 ▽ GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
   ▽ [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
       [Message: GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
       [Severity level: Chat]
       [Group: Sequence]
     Request Method: GET
     Request URI: /wireshark-labs/HTTP-wireshark-file3.html
     Request Version: HTTP/1.1
   Host: gaia.cs.umass.edu\r\n
   User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.6; rv:19.0) Gecko/20100101 Firefox/19.0\r\n
   Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
0000  30 46 9a 4c ec 47 d8 a2  5e 8f e7 b7 08 00 45 00   0F.L.G.. ^.....E.
0010  01 90 62 c7 40 00 40 06  a0 64 c0 a8 00 10 80 77   ..b.@.@. .d.....w
0020  f5 0c cc 67 00 50 f1 59  ee 33 84 e7 da 05 80 18   ...g.P.Y .3......
0030  ff ff 05 cd 00 00 01 01  08 0a 18 b3 60 ae 11 42   ........ ....`..B
0040  7e ec 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   ~.GET /w ireshark
```

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

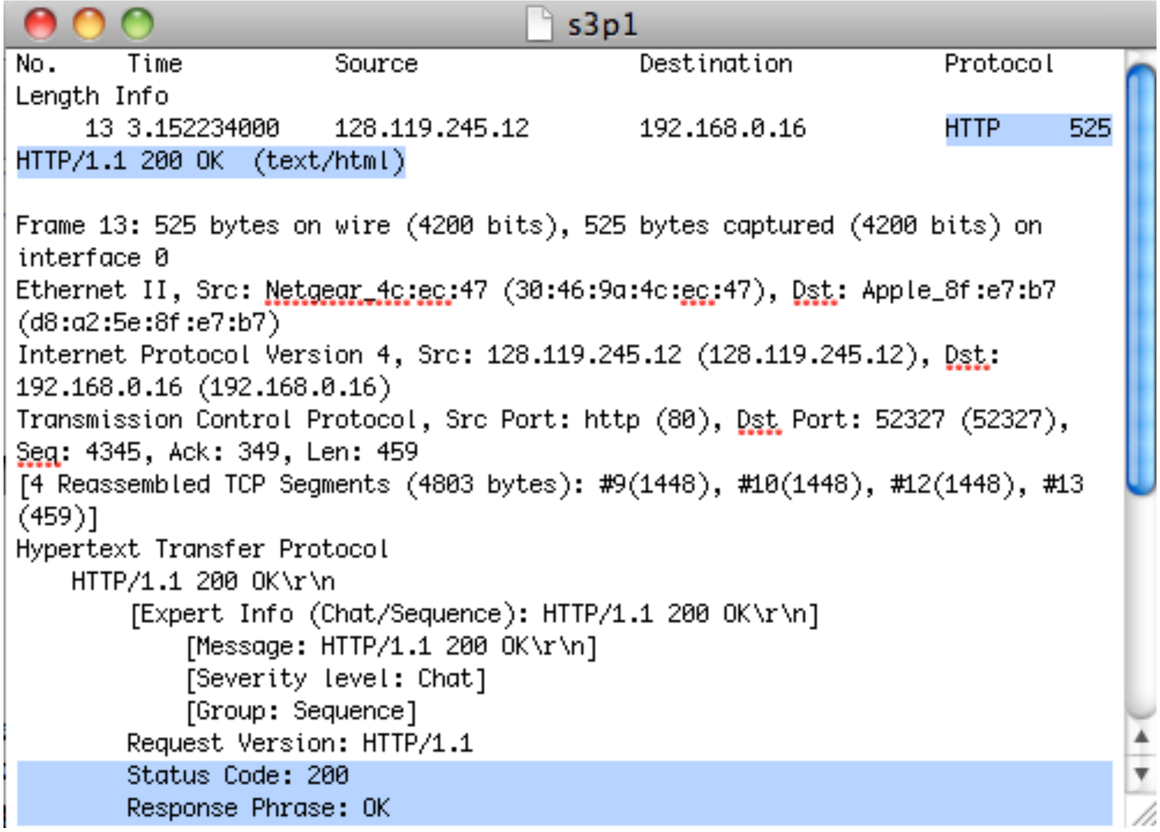


```
▷ [4 Reassembled TCP Segments (4803 bytes): #9(1448), #10(1448), #12(1448), #13(459)]
▽ Hypertext Transfer Protocol
  ▽ HTTP/1.1 200 OK\r\n
    ▽ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [Message: HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Version: HTTP/1.1
      Status Code: 200
      Response Phrase: OK
    Date: Sun, 17 Mar 2013 15:15:34 GMT\r\n
    Server: Apache/2.2.3 (CentOS)\r\n
0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK.
0010  0a 44 61 74 65 3a 20 53  75 6e 2c 20 31 37 20 4d   .Date: S un, 17 M
```



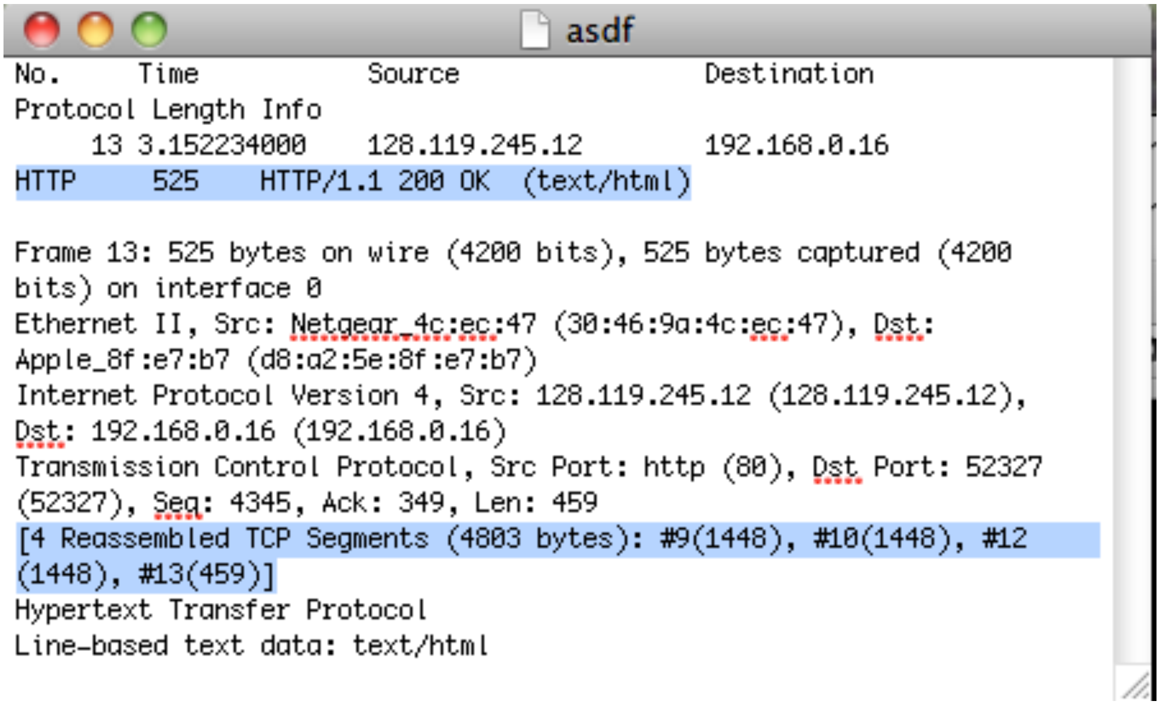
```
▷ [4 Reassembled TCP Segments (4803 bytes): #9(1448), #10(1448), #12(1448), #13(459)]
▽ Hypertext Transfer Protocol
  ▽ HTTP/1.1 200 OK\r\n
    ▽ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [Message: HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Version: HTTP/1.1
      Status Code: 200
      Response Phrase: OK
    Date: Sun, 17 Mar 2013 15:15:34 GMT\r\n
    Server: Apache/2.2.3 (CentOS)\r\n
0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK.
0010  0a 44 61 74 65 3a 20 53  75 6e 2c 20 31 37 20 4d   .Date: S un, 17 M
```

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



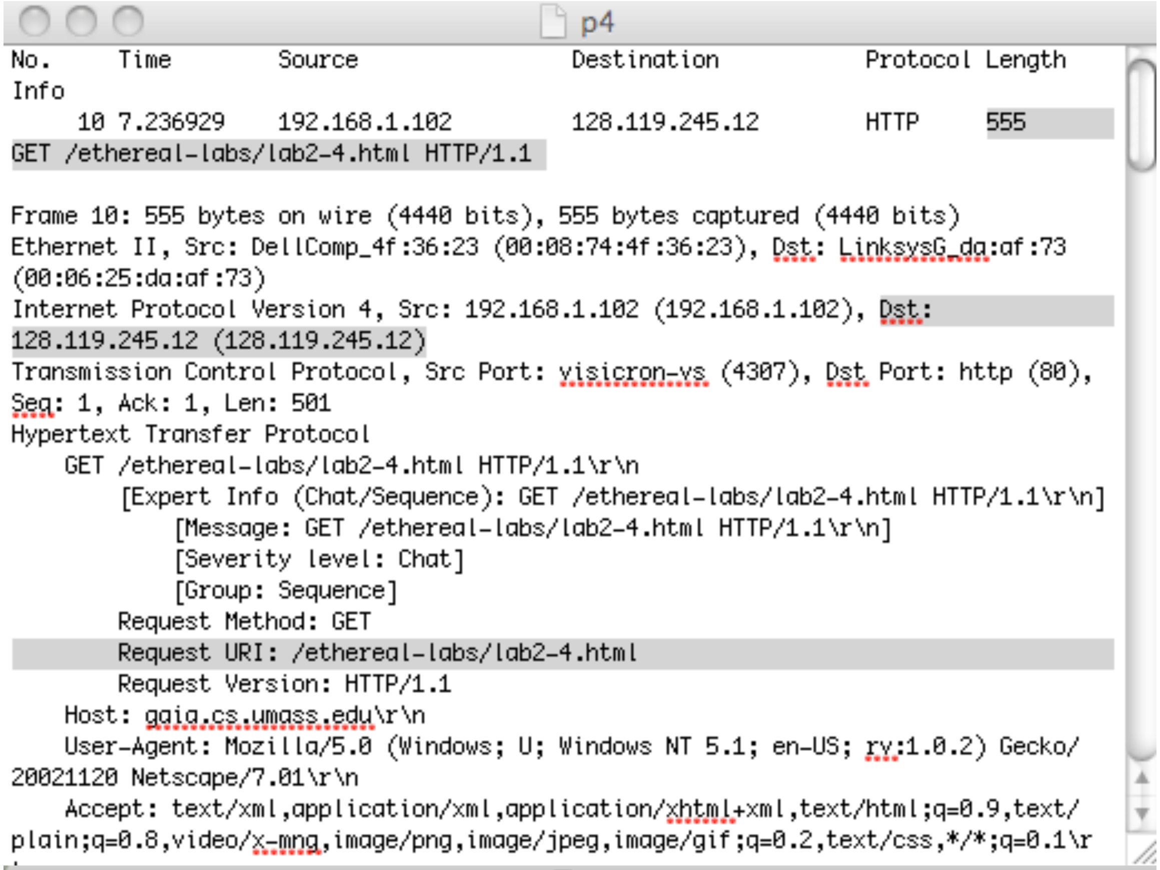
```
No.     Time            Source                Destination           Protocol
Length Info
     13 3.152234000     128.119.245.12        192.168.0.16          HTTP     525
HTTP/1.1 200 OK  (text/html)

Frame 13: 525 bytes on wire (4200 bits), 525 bytes captured (4200 bits) on
interface 0
Ethernet II, Src: Netgear_4c:ec:47 (30:46:9a:4c:ec:47), Dst: Apple_8f:e7:b7
(d8:a2:5e:8f:e7:b7)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst:
192.168.0.16 (192.168.0.16)
Transmission Control Protocol, Src Port: http (80), Dst Port: 52327 (52327),
Seq: 4345, Ack: 349, Len: 459
[4 Reassembled TCP Segments (4803 bytes): #9(1448), #10(1448), #12(1448), #13
(459)]
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
            [Message: HTTP/1.1 200 OK\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Version: HTTP/1.1
        Status Code: 200
        Response Phrase: OK
```

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

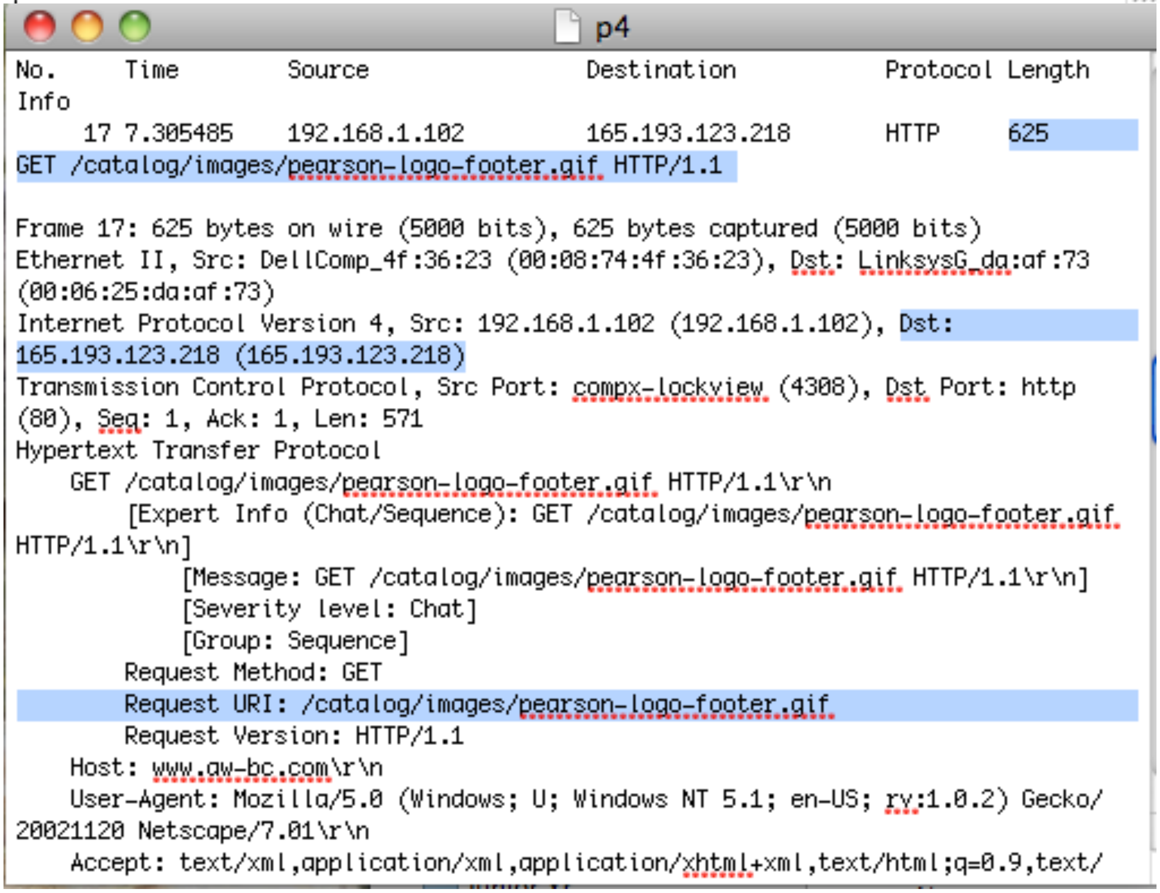


```
No.     Time            Source                Destination
Protocol Length Info
     13 3.152234000     128.119.245.12        192.168.0.16
HTTP     525    HTTP/1.1 200 OK  (text/html)

Frame 13: 525 bytes on wire (4200 bits), 525 bytes captured (4200
bits) on interface 0
Ethernet II, Src: Netgear_4c:ec:47 (30:46:9a:4c:ec:47), Dst:
Apple_8f:e7:b7 (d8:a2:5e:8f:e7:b7)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12),
Dst: 192.168.0.16 (192.168.0.16)
Transmission Control Protocol, Src Port: http (80), Dst Port: 52327
(52327), Seq: 4345, Ack: 349, Len: 459
[4 Reassembled TCP Segments (4803 bytes): #9(1448), #10(1448), #12
(1448), #13(459)]
Hypertext Transfer Protocol
Line-based text data: text/html
```

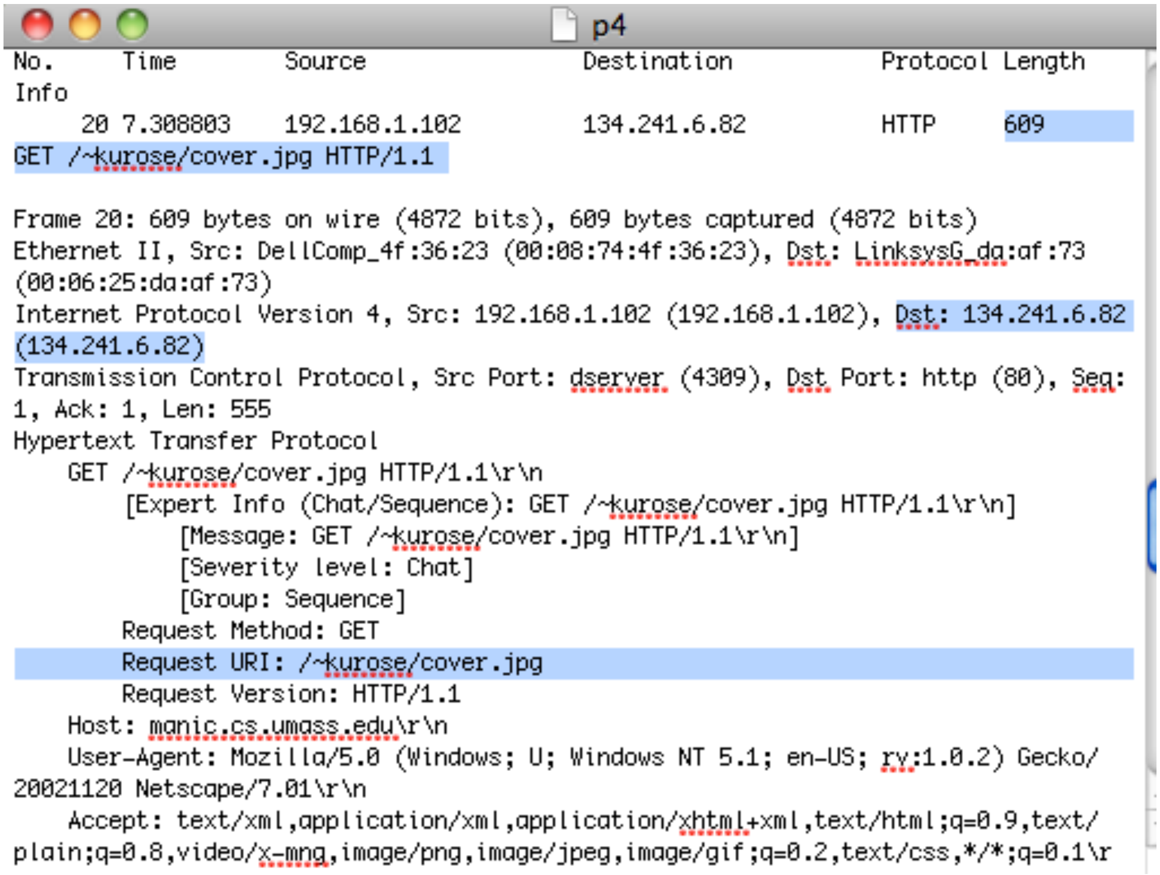
16. There are three HTTP GET request messages sent. The three internet address with their corresponding IP address are: /ethereal-labs/lab2-4.html (128.119.245.12), /catalog/images/pearson-logo-footer.gif (165.193.123.218), and /~kurose/cover.jpg (134.241.6.82).



```
No.     Time          Source              Destination          Protocol Length
Info
     10 7.236929      192.168.1.102       128.119.245.12       HTTP     555
GET /ethereal-labs/lab2-4.html HTTP/1.1

Frame 10: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits)
Ethernet II, Src: DellComp_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73
(00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst:
128.119.245.12 (128.119.245.12)
Transmission Control Protocol, Src Port: visicron-vs (4307), Dst Port: http (80),
Seq: 1, Ack: 1, Len: 501
Hypertext Transfer Protocol
    GET /ethereal-labs/lab2-4.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /ethereal-labs/lab2-4.html HTTP/1.1\r\n]
            [Message: GET /ethereal-labs/lab2-4.html HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
        Request URI: /ethereal-labs/lab2-4.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/
20021120 Netscape/7.01\r\n
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/
plain;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1\r
```

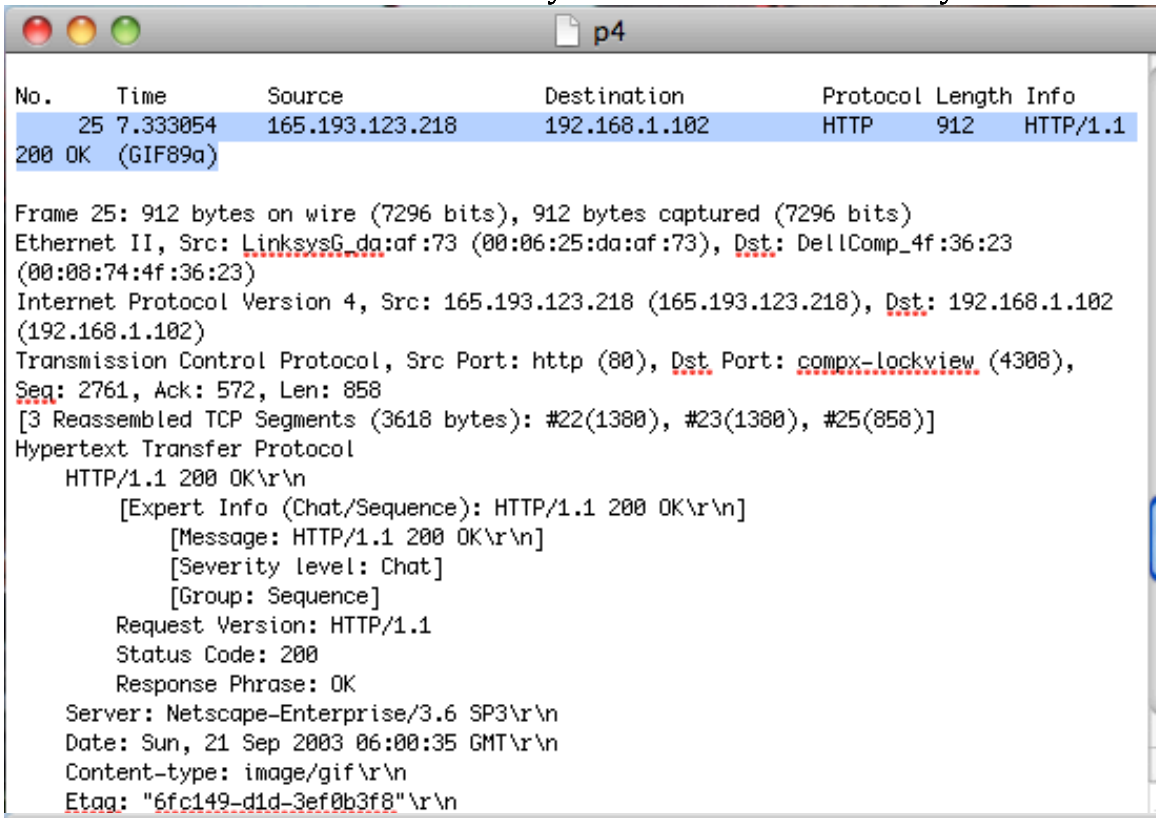


```
No.     Time          Source              Destination          Protocol Length
Info
     17 7.305485      192.168.1.102       165.193.123.218      HTTP     625
GET /catalog/images/pearson-logo-footer.gif HTTP/1.1

Frame 17: 625 bytes on wire (5000 bits), 625 bytes captured (5000 bits)
Ethernet II, Src: DellComp_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73
(00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst:
165.193.123.218 (165.193.123.218)
Transmission Control Protocol, Src Port: compx-lockview (4308), Dst Port: http
(80), Seq: 1, Ack: 1, Len: 571
Hypertext Transfer Protocol
    GET /catalog/images/pearson-logo-footer.gif HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /catalog/images/pearson-logo-footer.gif
HTTP/1.1\r\n]
            [Message: GET /catalog/images/pearson-logo-footer.gif HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
        Request URI: /catalog/images/pearson-logo-footer.gif
        Request Version: HTTP/1.1
    Host: www.aw-bc.com\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/
20021120 Netscape/7.01\r\n
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/
```

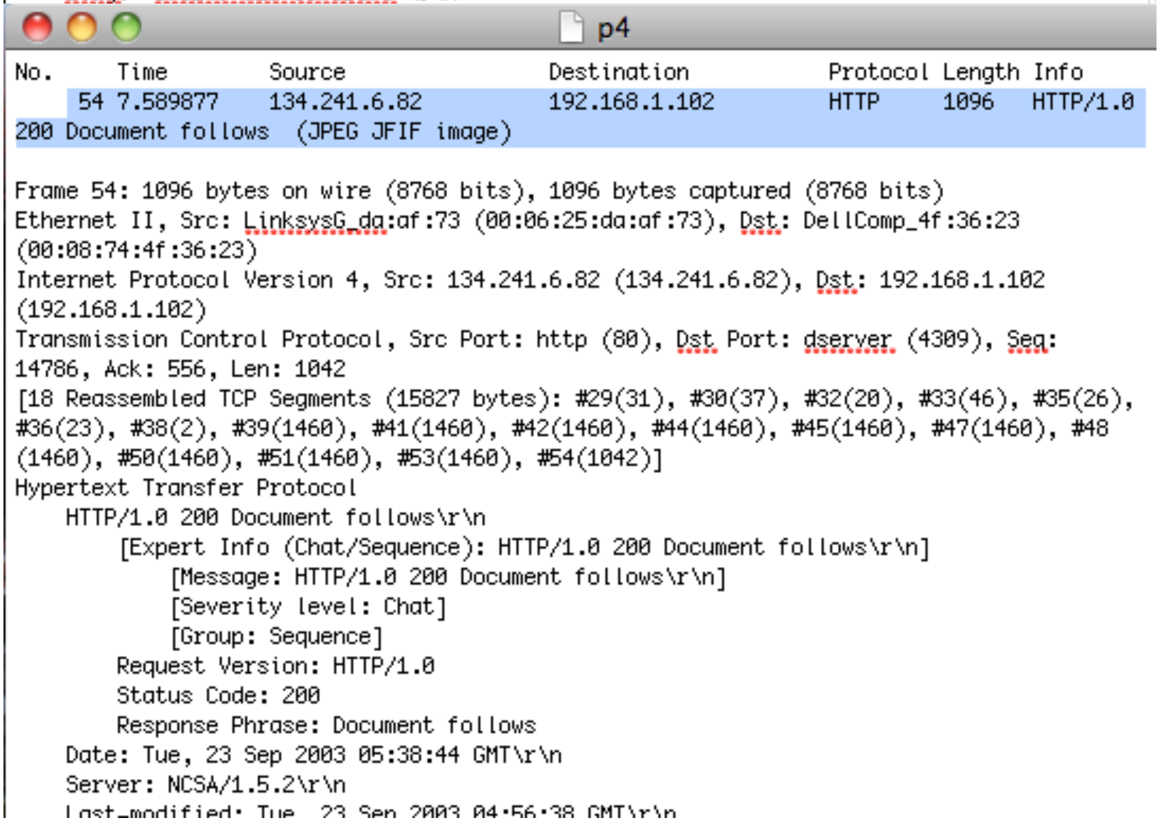


```
No.     Time           Source                Destination           Protocol Length
Info
     20 7.308803       192.168.1.102         134.241.6.82          HTTP     609
GET /~kurose/cover.jpg HTTP/1.1

Frame 20: 609 bytes on wire (4872 bits), 609 bytes captured (4872 bits)
Ethernet II, Src: DellComp_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73
(00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: 134.241.6.82
(134.241.6.82)
Transmission Control Protocol, Src Port: dserver (4309), Dst Port: http (80), Seq:
1, Ack: 1, Len: 555
Hypertext Transfer Protocol
    GET /~kurose/cover.jpg HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /~kurose/cover.jpg HTTP/1.1\r\n]
            [Message: GET /~kurose/cover.jpg HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
        Request URI: /~kurose/cover.jpg
        Request Version: HTTP/1.1
    Host: manic.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/
20021120 Netscape/7.01\r\n
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/
plain;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1\r
```

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.

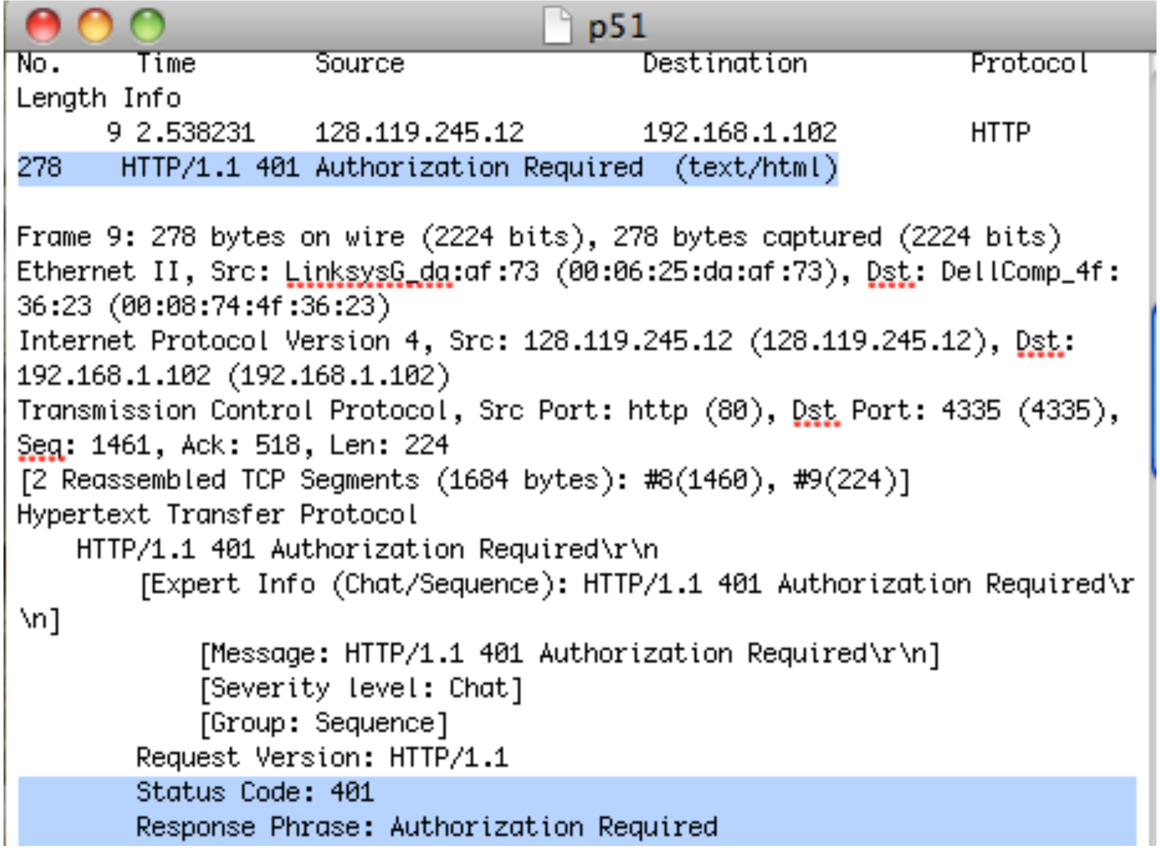


```
No.     Time          Source                Destination           Protocol Length Info
     25 7.333054      165.193.123.218       192.168.1.102         HTTP     912    HTTP/1.1
200 OK  (GIF89a)

Frame 25: 912 bytes on wire (7296 bits), 912 bytes captured (7296 bits)
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: DellComp_4f:36:23
(00:08:74:4f:36:23)
Internet Protocol Version 4, Src: 165.193.123.218 (165.193.123.218), Dst: 192.168.1.102
(192.168.1.102)
Transmission Control Protocol, Src Port: http (80), Dst Port: compx-lockview (4308),
Seq: 2761, Ack: 572, Len: 858
[3 Reassembled TCP Segments (3618 bytes): #22(1380), #23(1380), #25(858)]
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
            [Message: HTTP/1.1 200 OK\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Version: HTTP/1.1
        Status Code: 200
        Response Phrase: OK
    Server: Netscape-Enterprise/3.6 SP3\r\n
    Date: Sun, 21 Sep 2003 06:00:35 GMT\r\n
    Content-type: image/gif\r\n
    Etag: "6fc149-d1d-3ef0b3f8"\r\n
```



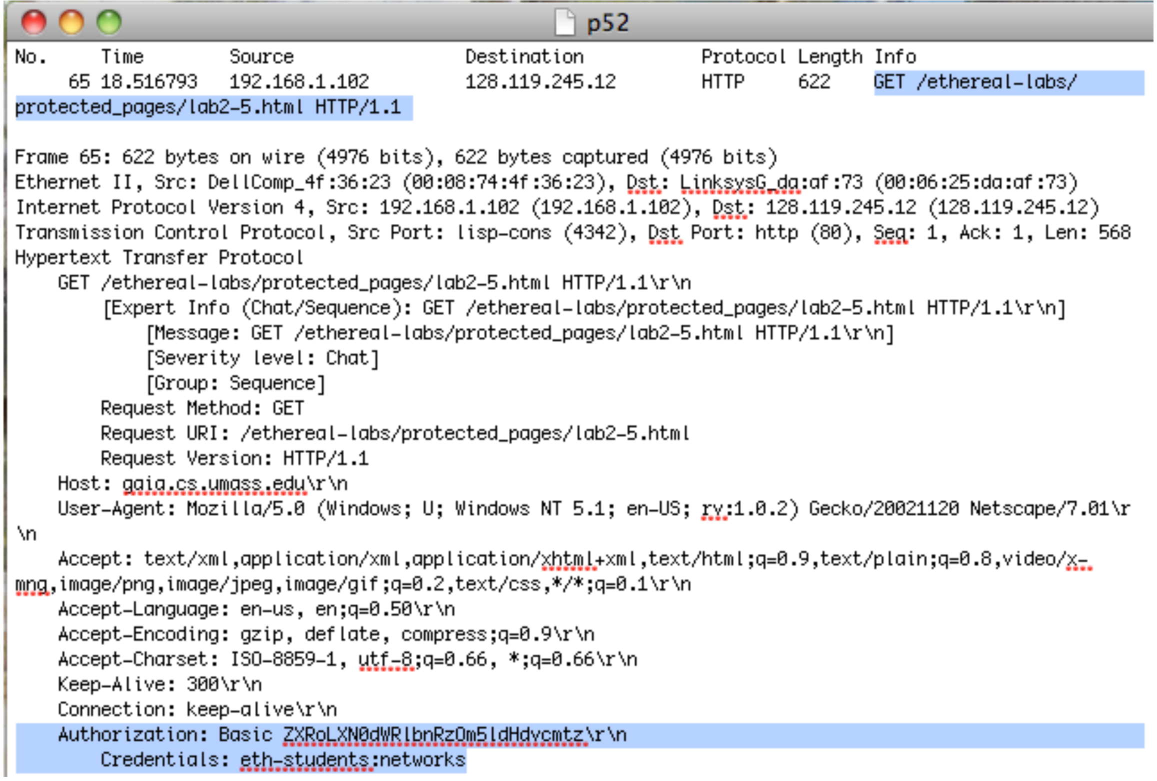
```
No.     Time          Source                Destination           Protocol Length Info
     54 7.589877      134.241.6.82          192.168.1.102         HTTP     1096   HTTP/1.0
200 Document follows  (JPEG JFIF image)

Frame 54: 1096 bytes on wire (8768 bits), 1096 bytes captured (8768 bits)
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: DellComp_4f:36:23
(00:08:74:4f:36:23)
Internet Protocol Version 4, Src: 134.241.6.82 (134.241.6.82), Dst: 192.168.1.102
(192.168.1.102)
Transmission Control Protocol, Src Port: http (80), Dst Port: dserver (4309), Seq:
14786, Ack: 556, Len: 1042
[18 Reassembled TCP Segments (15827 bytes): #29(31), #30(37), #32(20), #33(46), #35(26),
#36(23), #38(2), #39(1460), #41(1460), #42(1460), #44(1460), #45(1460), #47(1460), #48
(1460), #50(1460), #51(1460), #53(1460), #54(1042)]
Hypertext Transfer Protocol
    HTTP/1.0 200 Document follows\r\n
        [Expert Info (Chat/Sequence): HTTP/1.0 200 Document follows\r\n]
            [Message: HTTP/1.0 200 Document follows\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Version: HTTP/1.0
        Status Code: 200
        Response Phrase: Document follows
    Date: Tue, 23 Sep 2003 05:38:44 GMT\r\n
    Server: NCSA/1.5.2\r\n
    Last-modified: Tue, 23 Sep 2003 04:56:38 GMT\r\n
```

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.



```
No.     Time        Source              Destination           Protocol
Length Info
      9 2.538231    128.119.245.12      192.168.1.102         HTTP
278    HTTP/1.1 401 Authorization Required  (text/html)

Frame 9: 278 bytes on wire (2224 bits), 278 bytes captured (2224 bits)
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: DellComp_4f:
36:23 (00:08:74:4f:36:23)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst:
192.168.1.102 (192.168.1.102)
Transmission Control Protocol, Src Port: http (80), Dst Port: 4335 (4335),
Seq: 1461, Ack: 518, Len: 224
[2 Reassembled TCP Segments (1684 bytes): #8(1460), #9(224)]
Hypertext Transfer Protocol
    HTTP/1.1 401 Authorization Required\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 401 Authorization Required\r
\n]
            [Message: HTTP/1.1 401 Authorization Required\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Version: HTTP/1.1
        Status Code: 401
        Response Phrase: Authorization Required
```

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.



```
No.     Time        Source              Destination         Protocol Length Info
     65 18.516793   192.168.1.102       128.119.245.12      HTTP     622    GET /ethereal-labs/
protected_pages/lab2-5.html HTTP/1.1

Frame 65: 622 bytes on wire (4976 bits), 622 bytes captured (4976 bits)
Ethernet II, Src: DellComp_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: 128.119.245.12 (128.119.245.12)
Transmission Control Protocol, Src Port: lisp-cons (4342), Dst Port: http (80), Seq: 1, Ack: 1, Len: 568
Hypertext Transfer Protocol
    GET /ethereal-labs/protected_pages/lab2-5.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /ethereal-labs/protected_pages/lab2-5.html HTTP/1.1\r\n]
            [Message: GET /ethereal-labs/protected_pages/lab2-5.html HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
        Request URI: /ethereal-labs/protected_pages/lab2-5.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/7.01\r
\n
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-
mng,image/png,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1\r\n
    Accept-Language: en-us, en;q=0.50\r\n
    Accept-Encoding: gzip, deflate, compress;q=0.9\r\n
    Accept-Charset: ISO-8859-1, utf-8;q=0.66, *;q=0.66\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    Authorization: Basic ZXRoLXN0dWRlbnRzOm5ldHdvcmtz\r\n
        Credentials: eth-students:networks
```