HTTP & Wireshark

Eng: Rasha Khillo

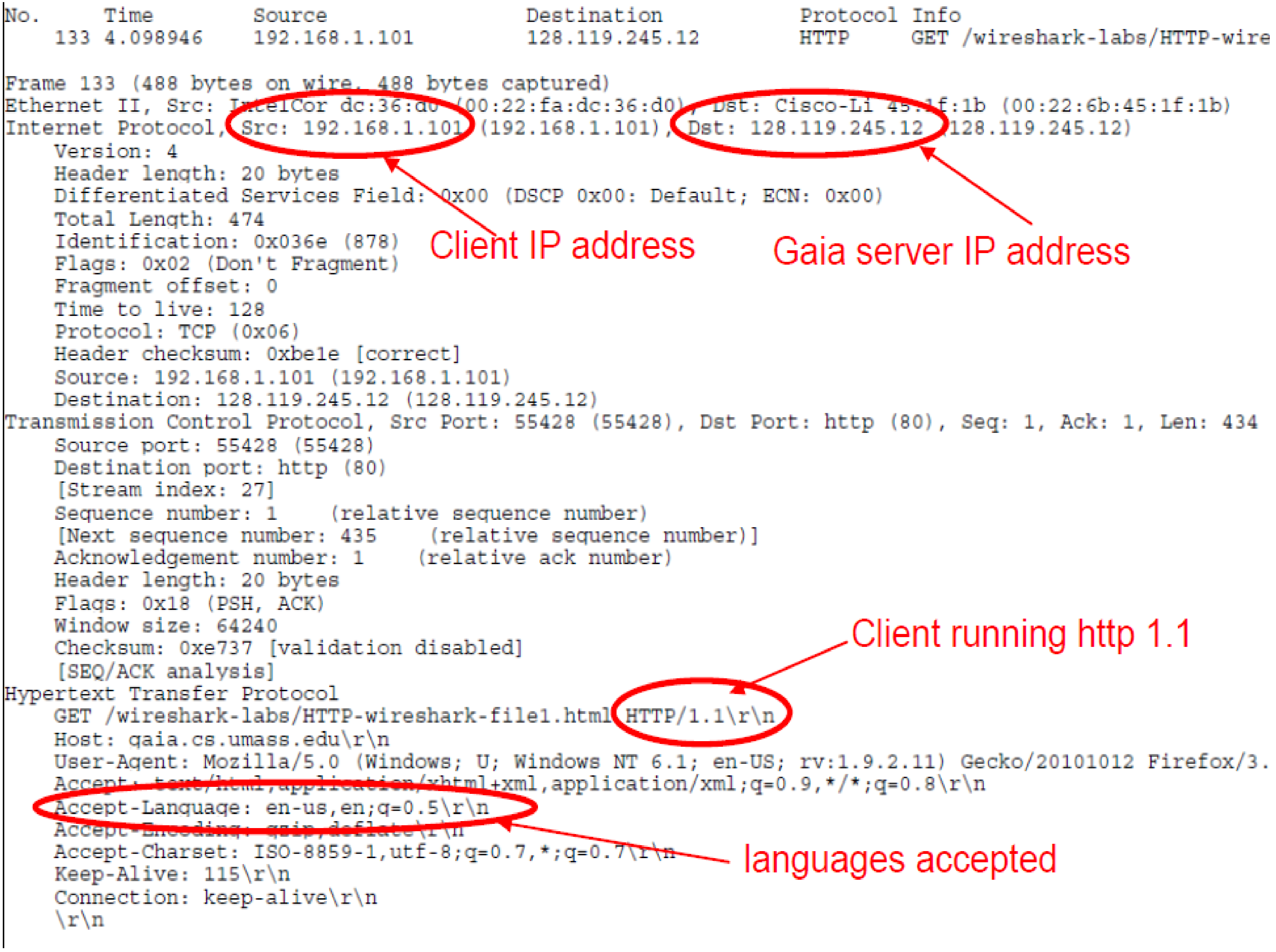
WiresharkLab:HTTP
The Basic HTTP GET/response interaction

- Enter “http” (just the letters, not the quotation marks) in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window.
- Begin Wireshark packet capture.
- Enter the following to your browser
  http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html
- Your browser should display the very simple, one-line HTML file.
- Stop Wireshark packet capture.

Exercise 1: The Basic HTTP GET/response interaction

- By looking at the information in the HTTP GET and response messages, answer the following questions:

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
2. What languages (if any) does your browser indicate that it can accept to the server?
3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
4. What is the status code returned from the server to your browser?
5. When was the HTML file that you are retrieving last modified at the server?
6. How many bytes of content are being returned to your browser?



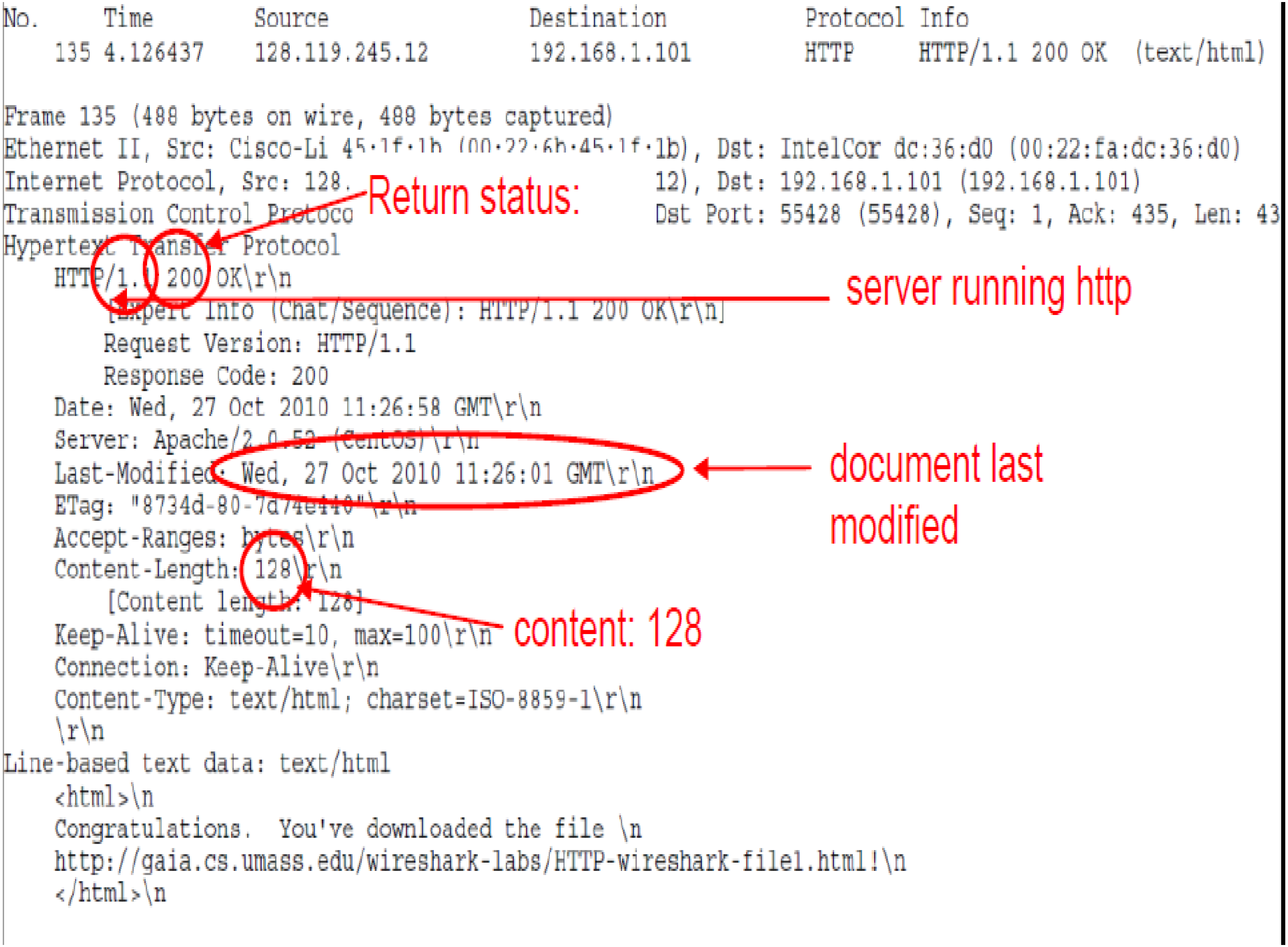
```
No.     Time        Source                Destination           Protocol Info
    133 4.098946    192.168.1.101         128.119.245.12        HTTP     GET /wireshark-labs/HTTP-wire

Frame 133 (488 bytes on wire, 488 bytes captured)
Ethernet II, Src: IntelCor dc:36:d0 (00:22:fa:dc:36:d0), Dst: Cisco-Li 45:1f:1b (00:22:6b:45:1f:1b)
Internet Protocol, Src: 192.168.1.101 (192.168.1.101), Dst: 128.119.245.12 (128.119.245.12)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 474
    Identification: 0x036e (878)
    Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (0x06)
    Header checksum: 0xbe1e [correct]
    Source: 192.168.1.101 (192.168.1.101)
    Destination: 128.119.245.12 (128.119.245.12)
Transmission Control Protocol, Src Port: 55428 (55428), Dst Port: http (80), Seq: 1, Ack: 1, Len: 434
    Source port: 55428 (55428)
    Destination port: http (80)
    [Stream index: 27]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 435    (relative sequence number)]
    Acknowledgement number: 1    (relative ack number)
    Header length: 20 bytes
    Flags: 0x18 (PSH, ACK)
    Window size: 64240
    Checksum: 0xe737 [validation disabled]
    [SEQ/ACK analysis]
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 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.11) Gecko/20101012 Firefox/3.
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 115\r\n
    Connection: keep-alive\r\n
    \r\n
```

Client IP address

Gaia server IP address

Client running http 1.1

languages accepted



```
No.     Time        Source                Destination           Protocol Info
    135 4.126437    128.119.245.12        192.168.1.101         HTTP     HTTP/1.1 200 OK  (text/html)

Frame 135 (488 bytes on wire, 488 bytes captured)
Ethernet II, Src: Cisco-Li 45:1f:1b (00:22:6b:45:1f:1b), Dst: IntelCor dc:36:d0 (00:22:fa:dc:36:d0)
Internet Protocol, Src: 128.                          12), Dst: 192.168.1.101 (192.168.1.101)
Transmission Control Protoco                          Dst Port: 55428 (55428), Seq: 1, Ack: 435, Len: 43
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
        Response Code: 200
    Date: Wed, 27 Oct 2010 11:26:58 GMT\r\n
    Server: Apache/2.0.52 (CentOS)\r\n
    Last-Modified: Wed, 27 Oct 2010 11:26:01 GMT\r\n
    ETag: "8734d-80-7d74e440"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 128\r\n
        [Content length: 128]
    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
    <html>\n
    Congratulations.  You've downloaded the file \n
    http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
    </html>\n
```

Return status:

server running http

document last modified

content: 128

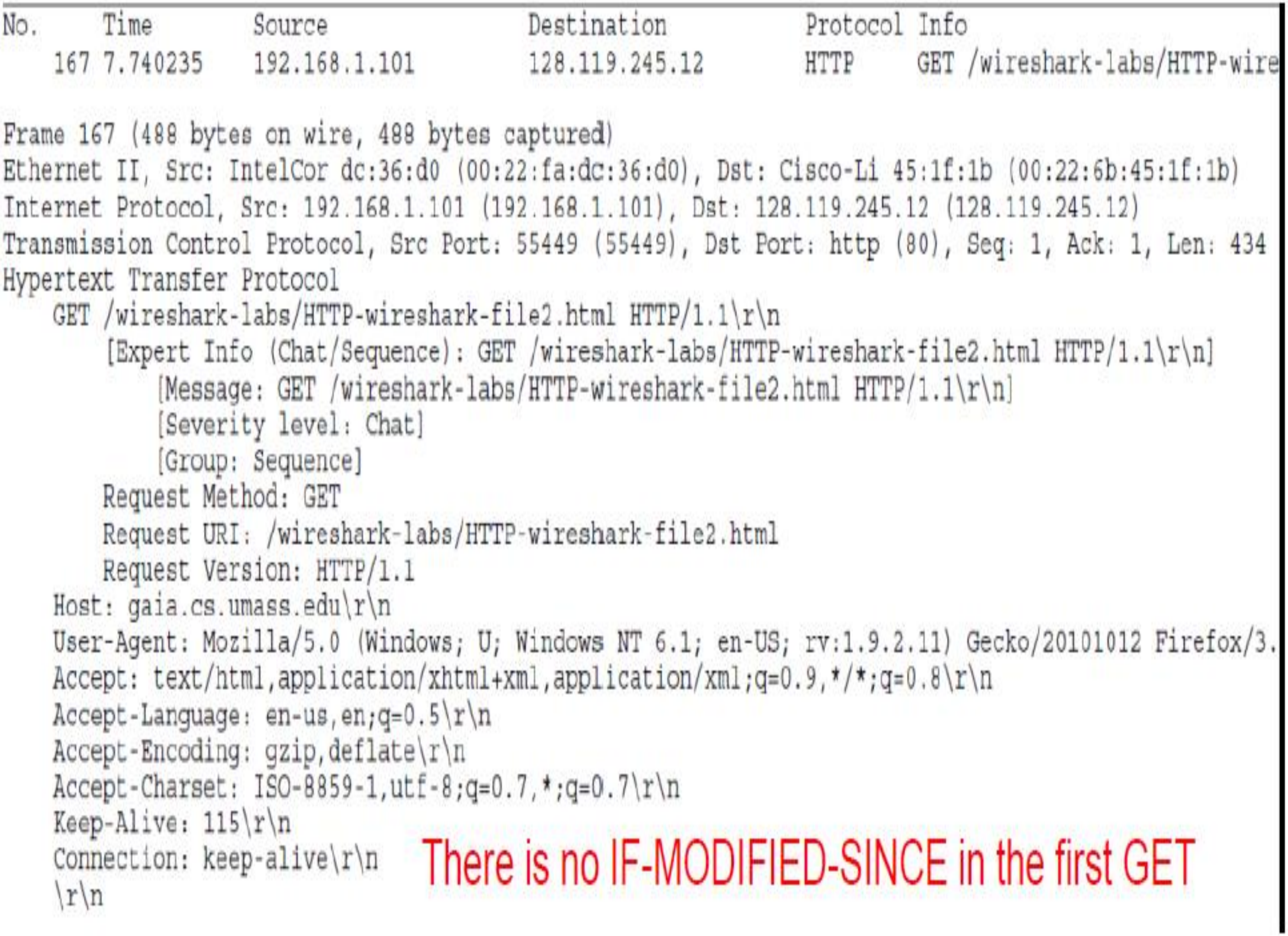
The HTTP CONDITIONAL GET/response interaction

- Most web browsers perform object caching and thus perform a conditional GET when retrieving an HTTP object.
- Make sure your browser's cache is empty.
- Now do the following:
- Start up your web browser, and make sure your browser's cache is cleared.
- Start up the Wireshark packet sniffer
- Enter the following URL into your browser http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html
  Your browser should display a very simple five-line HTML file.
- Quickly enter the same URL into your browser again (or simply select the refresh button on your browser)
- Stop Wireshark packet capture, and enter "http" in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window.

Exercise 2: The HTTP CONDITIONAL GET/response interaction

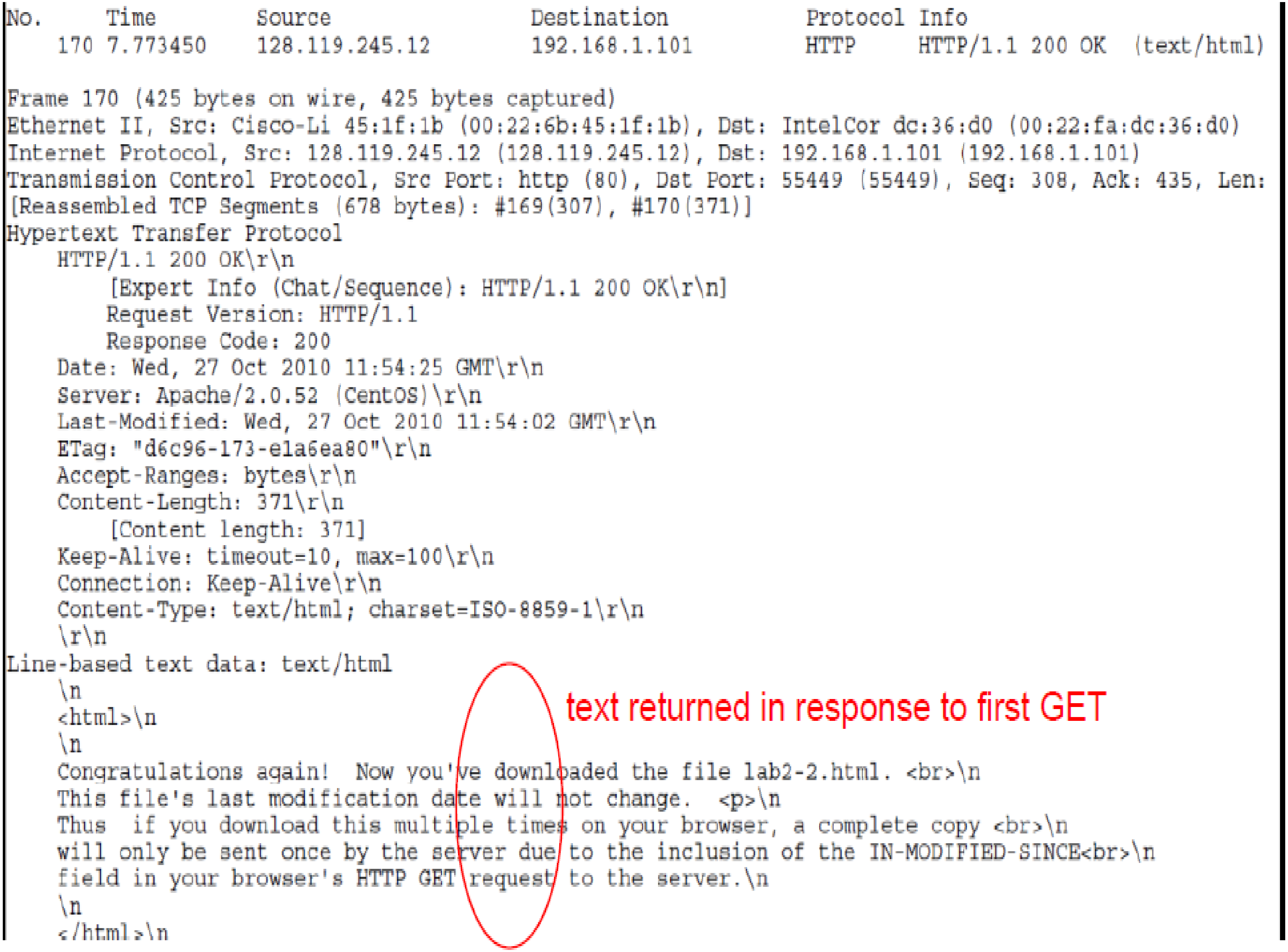
- Answer the following questions:

1. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?
2. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
3. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? If so, what information follows the "IF-MODIFIED-SINCE:" header?
4. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.



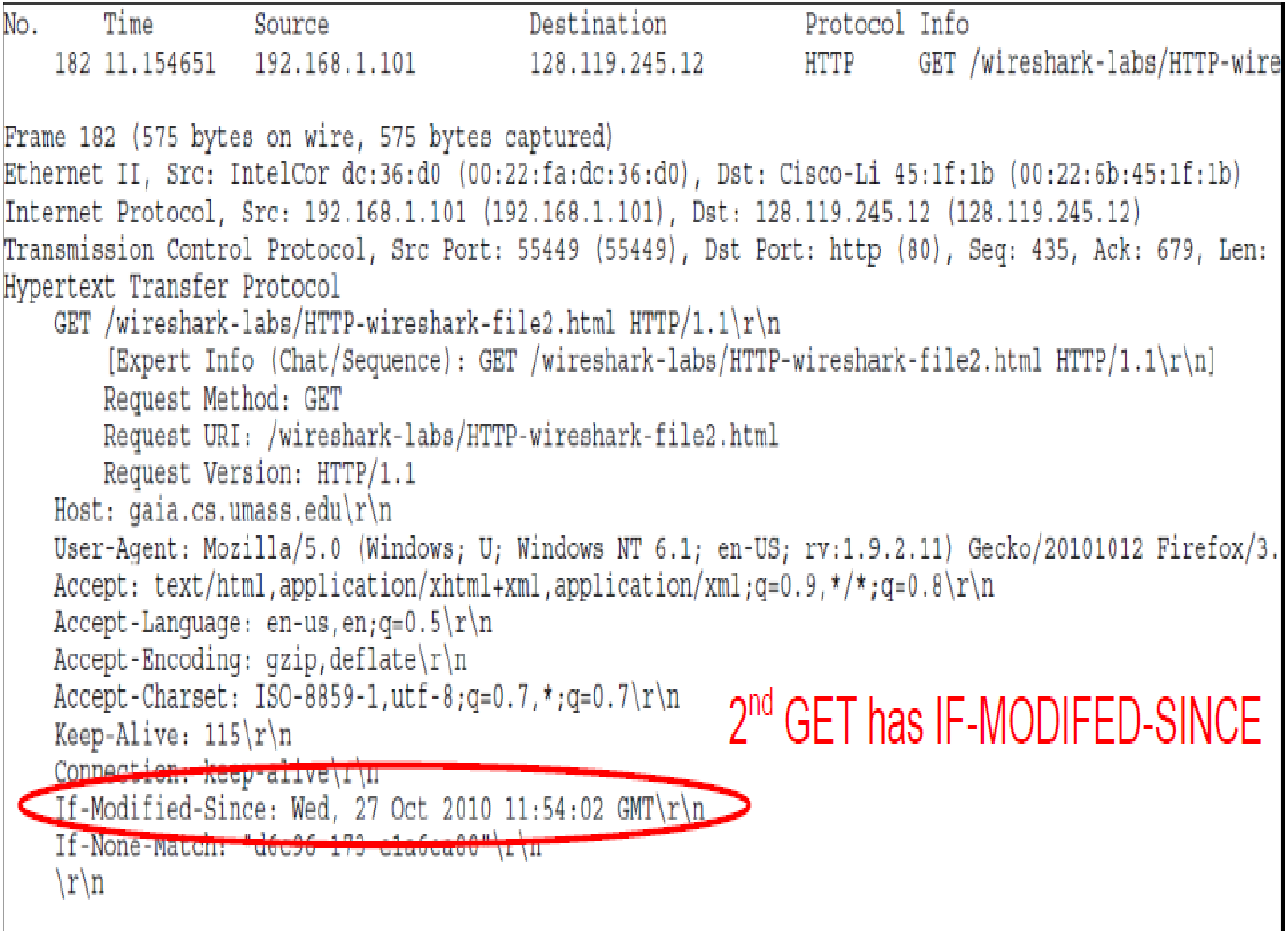
```
No.     Time         Source                 Destination            Protocol Info
    167 7.740235     192.168.1.101          128.119.245.12         HTTP     GET /wireshark-labs/HTTP-wire

Frame 167 (488 bytes on wire, 488 bytes captured)
Ethernet II, Src: IntelCor dc:36:d0 (00:22:fa:dc:36:d0), Dst: Cisco-Li 45:1f:1b (00:22:6b:45:1f:1b)
Internet Protocol, Src: 192.168.1.101 (192.168.1.101), Dst: 128.119.245.12 (128.119.245.12)
Transmission Control Protocol, Src Port: 55449 (55449), Dst Port: http (80), Seq: 1, Ack: 1, Len: 434
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
            [Message: GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
        Request URI: /wireshark-labs/HTTP-wireshark-file2.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.11) Gecko/20101012 Firefox/3.
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 115\r\n
    Connection: keep-alive\r\n
    \r\n
```

There is no IF-MODIFIED-SINCE in the first GET



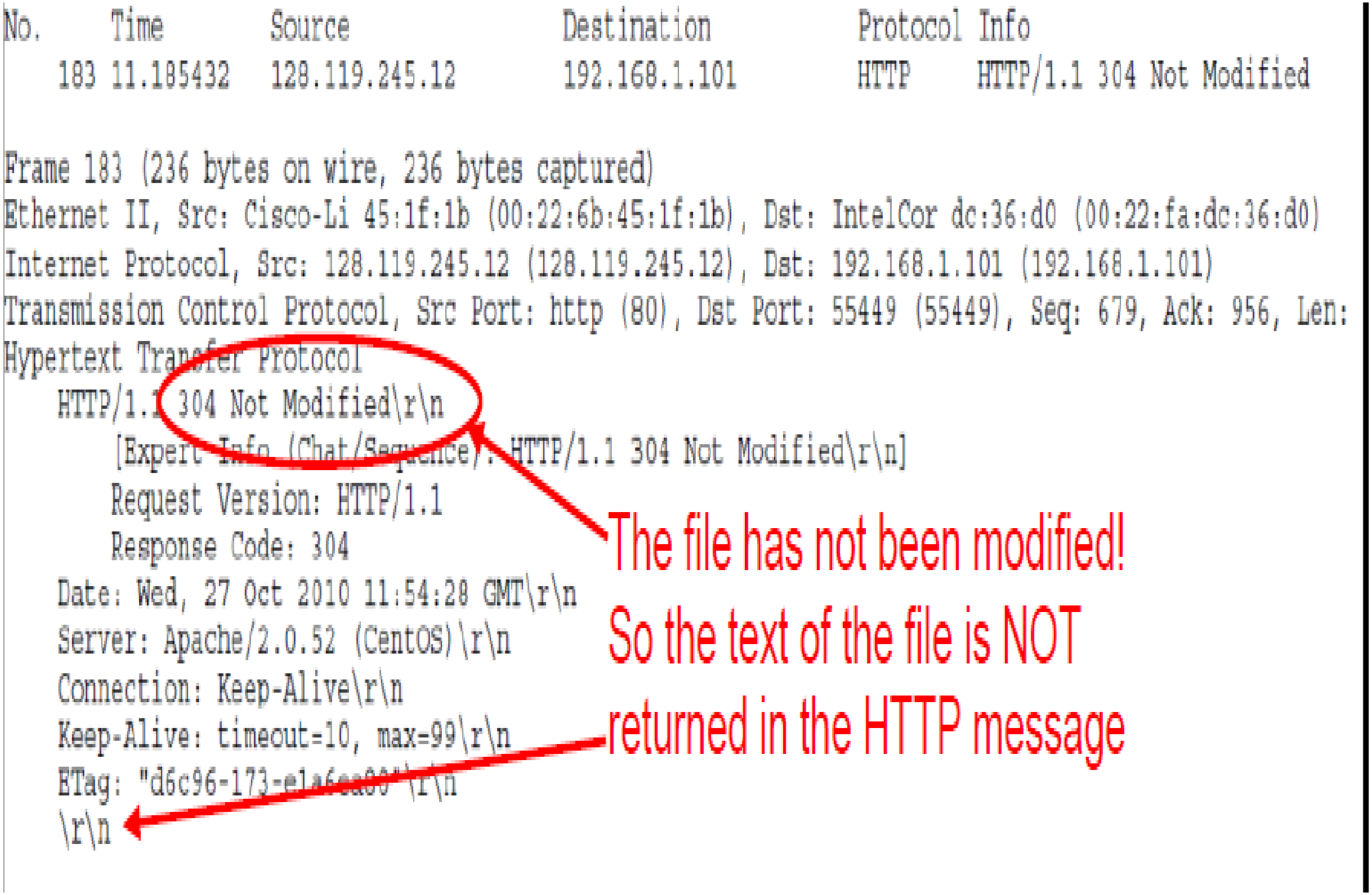
```
No.     Time        Source                Destination           Protocol Info
    170 7.773450    128.119.245.12        192.168.1.101         HTTP     HTTP/1.1 200 OK  (text/html)

Frame 170 (425 bytes on wire, 425 bytes captured)
Ethernet II, Src: Cisco-Li 45:1f:1b (00:22:6b:45:1f:1b), Dst: IntelCor dc:36:d0 (00:22:fa:dc:36:d0)
Internet Protocol, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.101 (192.168.1.101)
Transmission Control Protocol, Src Port: http (80), Dst Port: 55449 (55449), Seq: 308, Ack: 435, Len:
[Reassembled TCP Segments (678 bytes): #169(307), #170(371)]
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
        Response Code: 200
    Date: Wed, 27 Oct 2010 11:54:25 GMT\r\n
    Server: Apache/2.0.52 (CentOS)\r\n
    Last-Modified: Wed, 27 Oct 2010 11:54:02 GMT\r\n
    ETag: "d6c96-173-e1a6ea80"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 371\r\n
        [Content length: 371]
    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
```

text returned in response to first GET



```
No.     Time        Source                Destination           Protocol Info
    182 11.154651   192.168.1.101         128.119.245.12        HTTP     GET /wireshark-labs/HTTP-wire

Frame 182 (575 bytes on wire, 575 bytes captured)
Ethernet II, Src: IntelCor dc:36:d0 (00:22:fa:dc:36:d0), Dst: Cisco-Li 45:1f:1b (00:22:6b:45:1f:1b)
Internet Protocol, Src: 192.168.1.101 (192.168.1.101), Dst: 128.119.245.12 (128.119.245.12)
Transmission Control Protocol, Src Port: 55449 (55449), Dst Port: http (80), Seq: 435, Ack: 679, Len:
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
        Request Method: GET
        Request URI: /wireshark-labs/HTTP-wireshark-file2.html
        Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.11) Gecko/20101012 Firefox/3.
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 115\r\n
    Connection: keep-alive\r\n
    If-Modified-Since: Wed, 27 Oct 2010 11:54:02 GMT\r\n
    If-None-Match: "d6c96-173-c1a6ca00"\r\n
    \r\n
```

2nd GET has IF-MODIFED-SINCE



```
No.     Time        Source                Destination           Protocol Info
    183 11.185432   128.119.245.12        192.168.1.101         HTTP     HTTP/1.1 304 Not Modified

Frame 183 (236 bytes on wire, 236 bytes captured)
Ethernet II, Src: Cisco-Li 45:1f:1b (00:22:6b:45:1f:1b), Dst: IntelCor dc:36:d0 (00:22:fa:dc:36:d0)
Internet Protocol, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.101 (192.168.1.101)
Transmission Control Protocol, Src Port: http (80), Dst Port: 55449 (55449), Seq: 679, Ack: 956, Len:
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
        Request Version: HTTP/1.1
        Response Code: 304
    Date: Wed, 27 Oct 2010 11:54:28 GMT\r\n
    Server: Apache/2.0.52 (CentOS)\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=10, max=99\r\n
    ETag: "d6c96-173-e1a6ea80"\r\n
    \r\n
```

The file has not been modified!

So the text of the file is NOT returned in the HTTP message

Conditional GET

- This conditional GET is telling the server to send the object only if the object has been modified since the specified date.
- The cache performs an up-to-date check by issuing a conditional GET.

HTML Documents with Embedded Objects

- Now we can look at what happens when your browser downloads a file with embedded objects, i.e., a file that includes other objects (in the example below, image files) that are stored on another server(s).
- Do the following:
- Start up your web browser, and make sure your browser's cache is cleared, as discussed above.
- Start up the Wireshark packet sniffer
- Enter the following URL into your browser
- http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html
  your browser should display a short HTML file with two images.
- Stop Wireshark packet capture.

Exercise 3: HTML Documents with Embedded Objects (Quiz)

- Answer the following questions:

1. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent? Use the following table to arrange your answer.

Packet Number in the trace	Internet address the packet was sent to	The reason to send get message

Exercise 3: HTML Documents with Embedded Objects (Quiz)

2. What is the server's response (status code and phrase) in response to each HTTP GET message from your browser? Use the following table to arrange your answer:

Packet Number in the trace	Status code and phrase

3. When your browser's sends the HTTP GET message for the second time how many HTTP GET request messages did your browser send? What is the server's response (status code and phrase) in response to the HTTP GET?