Gurwinder Singh

CSC 138-03

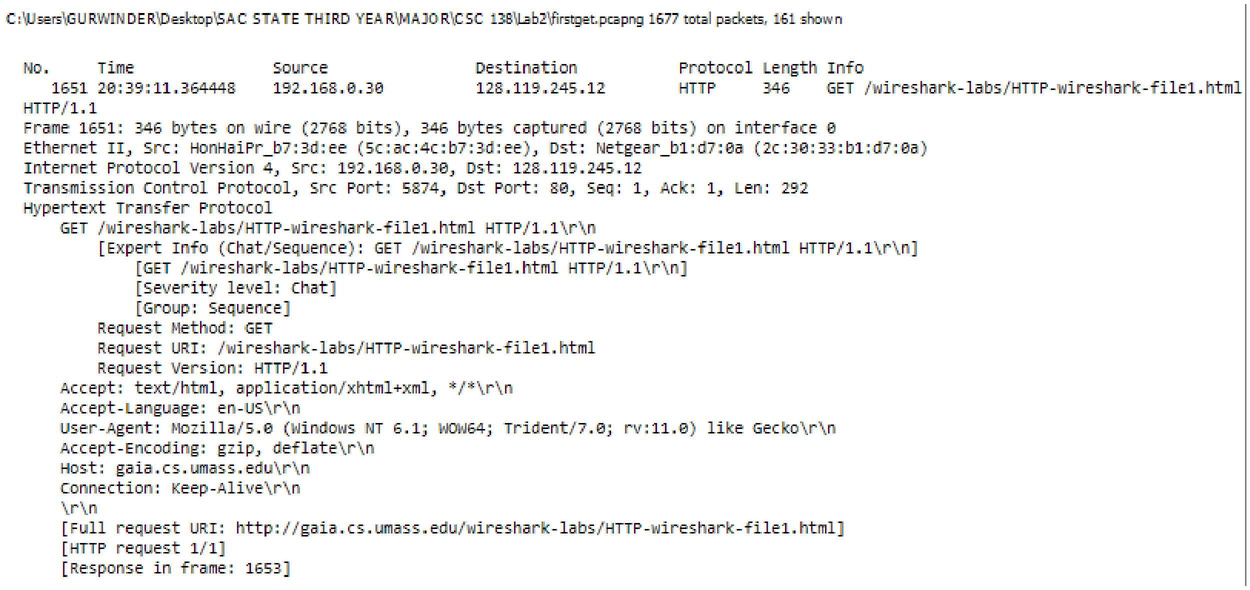
2/25/2019

Lab 2

(Section 1)

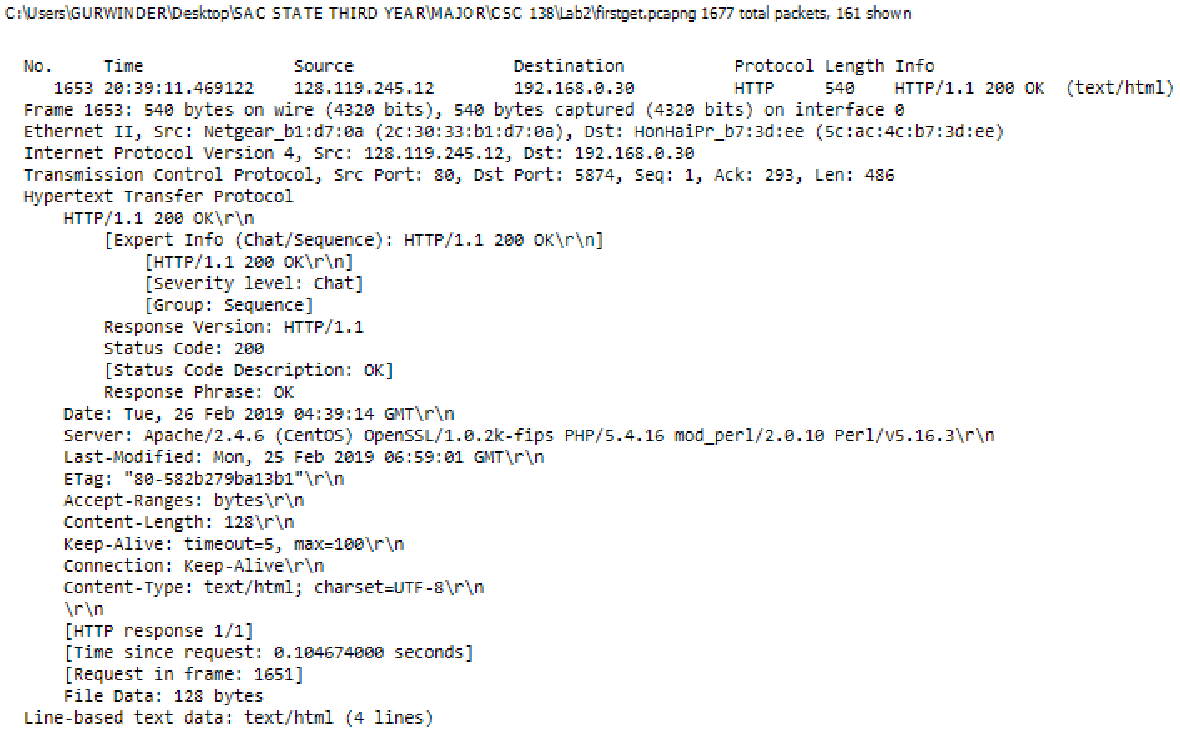
1) My browser is running HTTP version 1.1. Server is also running 1.1 .
2) Accept-Language : en-US\r\n
3) Internet address of gaia.cs.umass.edu : 128.119.245.12
   Internet address of my computer: 192.168.0.30
4) Status Code: 200
5) Last-Modified: Mon, 25 Feb 2019 06:59:01 GMT
6) 128 bytes of content are being returned to my browser.
7) No there are no headers.

GET MESSAGE



```
C:\Users\GURWINDER\Desktop\SAC STATE THIRD YEAR\MAJOR\CSC 138\Lab2\firstget.pcapng 1677 total packets, 161 shown

No.     Time               Source                Destination           Protocol Length Info
   1651 20:39:11.364448    192.168.0.30          128.119.245.12        HTTP     346    GET /wireshark-labs/HTTP-wireshark-file1.html
HTTP/1.1
Frame 1651: 346 bytes on wire (2768 bits), 346 bytes captured (2768 bits) on interface 0
Ethernet II, Src: HonHaiPr_b7:3d:ee (5c:ac:4c:b7:3d:ee), Dst: Netgear_b1:d7:0a (2c:30:33:b1:d7:0a)
Internet Protocol Version 4, Src: 192.168.0.30, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 5874, Dst Port: 80, Seq: 1, Ack: 1, Len: 292
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]
            [GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
        Request URI: /wireshark-labs/HTTP-wireshark-file1.html
        Request Version: HTTP/1.1
    Accept: text/html, application/xhtml+xml, */*\r\n
    Accept-Language: en-US\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
    Accept-Encoding: gzip, deflate\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 1653]
```

RESPONSE Message



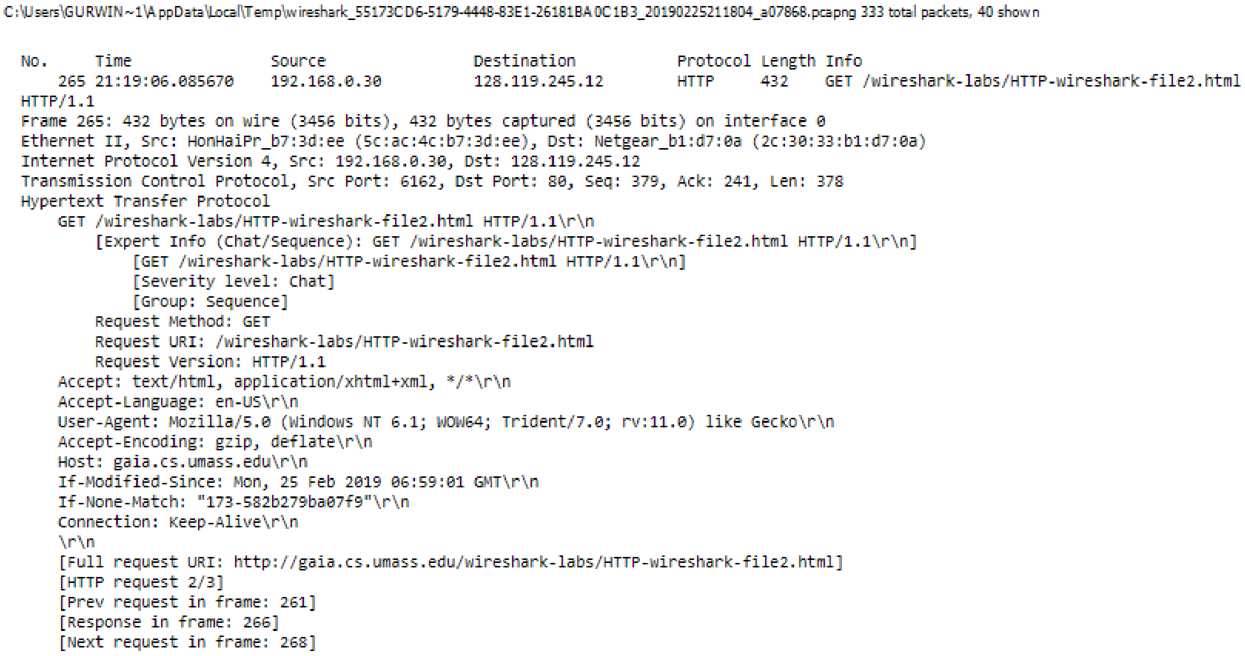
C:\Users\GURWINDER\Desktop\SAC STATE THIRD YEAR\MAJOR\CSC 138\Lab2\firstget.pcapng 1677 total packets, 161 shown

```
No.     Time               Source             Destination        Protocol Length Info
   1653 20:39:11.469122    128.119.245.12     192.168.0.30       HTTP     540    HTTP/1.1 200 OK  (text/html)
Frame 1653: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
Ethernet II, Src: Netgear_b1:d7:0a (2c:30:33:b1:d7:0a), Dst: HonHaiPr_b7:3d:ee (5c:ac:4c:b7:3d:ee)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.30
Transmission Control Protocol, Src Port: 80, Dst Port: 5874, Seq: 1, Ack: 293, Len: 486
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
            [HTTP/1.1 200 OK\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Tue, 26 Feb 2019 04:39:14 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Mon, 25 Feb 2019 06:59:01 GMT\r\n
    ETag: "80-582b279ba13b1"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.104674000 seconds]
    [Request in frame: 1651]
    File Data: 128 bytes
Line-based text data: text/html (4 lines)
```

(Section 2)

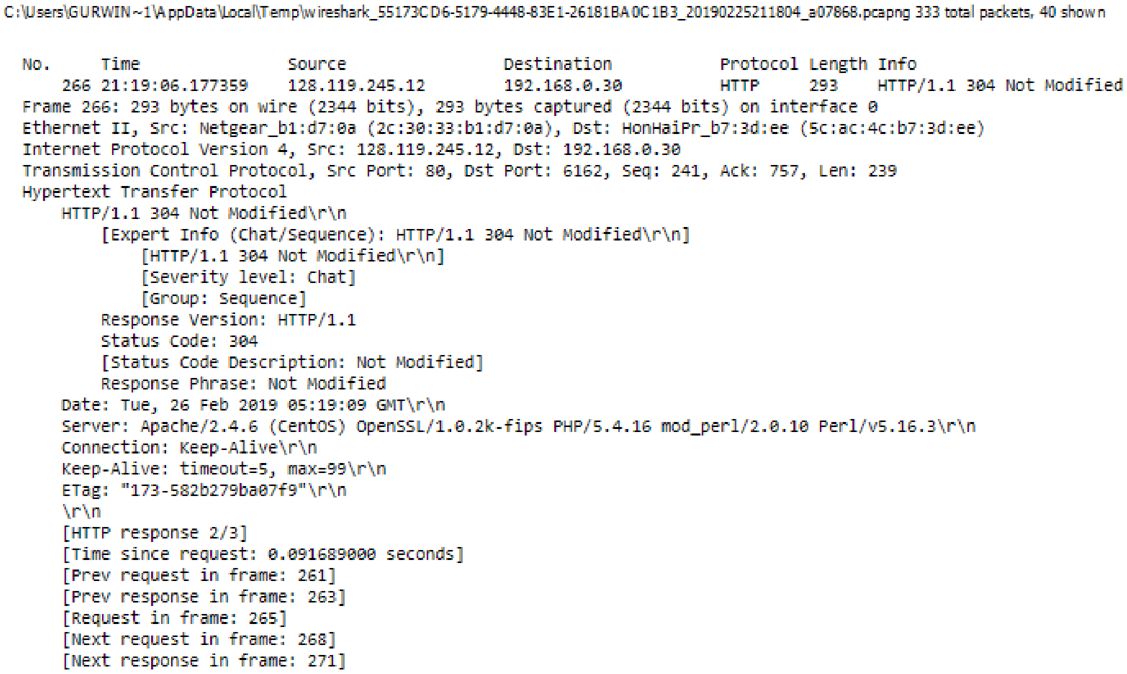
8) Yes I do see IF-MODIFIED- SINCE line
    a. If-Modified-Since: Mon, 25 Feb 2019 06:59:01 GMT.
9) Yes, the server explicitly return the contents of the file because time since request is 0.091689000
10) Yes I do see IF-MODIFIED-SINCE and it is same as last one
    a. If-Modified-Since: Mon, 25 Feb 2019 06:59:01 GMT
11) Status Code : 304 and phrase returned : Not Modified, Yes because it only took 0.091689000 seconds. It took the same time as the first one did.

GET MESSAGE



```
C:\Users\GURWIN~1\AppData\Local\Temp\wireshark_55173CD6-5179-4448-83E1-26181BA0C1B3_20190225211804_a07868.pcapng 333 total packets, 40 shown

No.     Time               Source                Destination           Protocol Length Info
    265 21:19:06.085670    192.168.0.30          128.119.245.12        HTTP     432    GET /wireshark-labs/HTTP-wireshark-file2.html 
HTTP/1.1 
Frame 265: 432 bytes on wire (3456 bits), 432 bytes captured (3456 bits) on interface 0
Ethernet II, Src: HonHaiPr_b7:3d:ee (5c:ac:4c:b7:3d:ee), Dst: Netgear_b1:d7:0a (2c:30:33:b1:d7:0a)
Internet Protocol Version 4, Src: 192.168.0.30, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 6162, Dst Port: 80, Seq: 379, Ack: 241, Len: 378
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]
            [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
    Accept: text/html, application/xhtml+xml, */*\r\n
    Accept-Language: en-US\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
    Accept-Encoding: gzip, deflate\r\n
    Host: gaia.cs.umass.edu\r\n
    If-Modified-Since: Mon, 25 Feb 2019 06:59:01 GMT\r\n
    If-None-Match: "173-582b279ba07f9"\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 2/3]
    [Prev request in frame: 261]
    [Response in frame: 266]
    [Next request in frame: 268]
```

RESPONSE Message



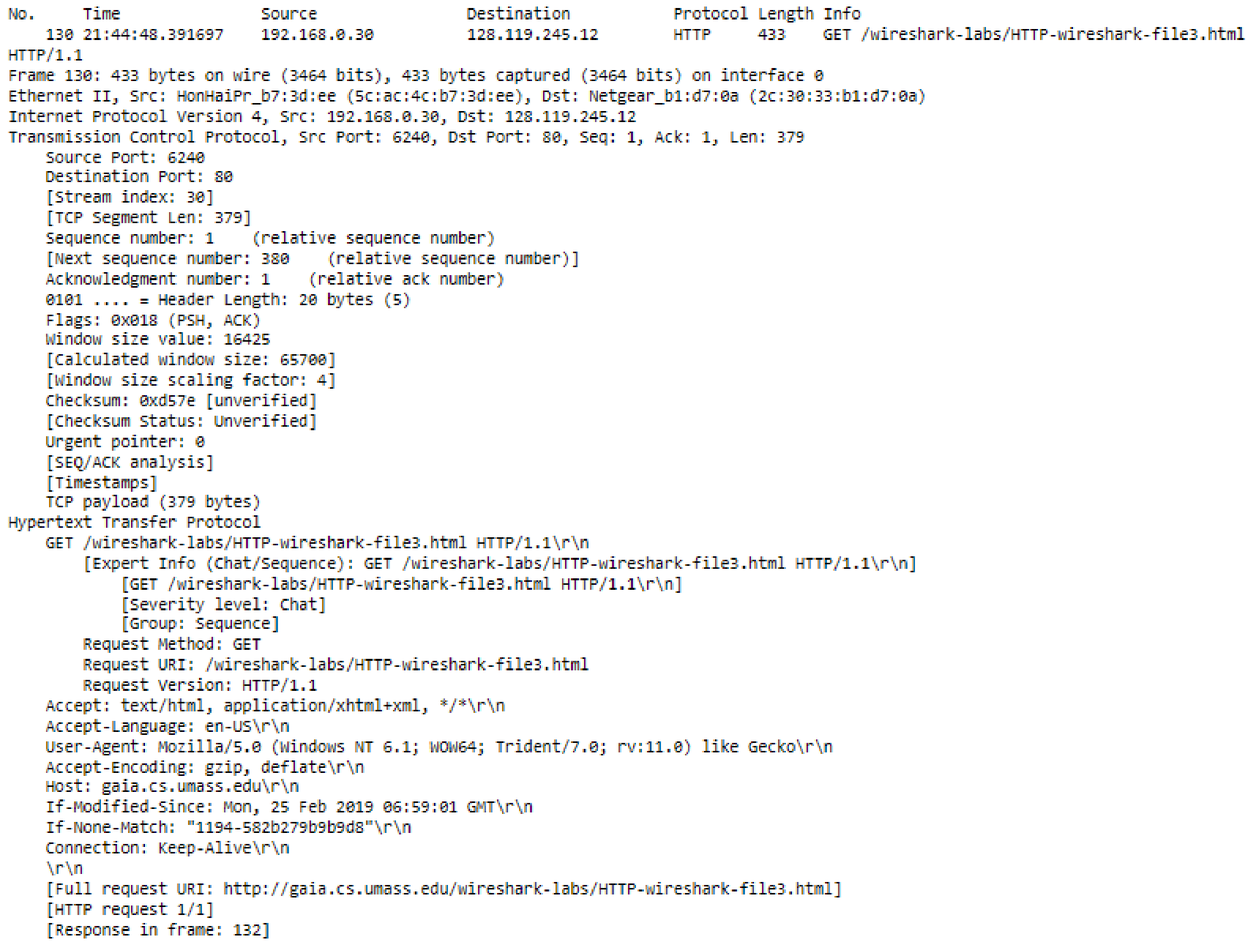
```
C:\Users\GURWIN~1\AppData\Local\Temp\wireshark_55173CD6-5179-4448-83E1-26181BA0C1B3_20190225211804_a07868.pcapng 333 total packets, 40 shown

No.     Time               Source                Destination           Protocol Length Info
    266 21:19:06.177359    128.119.245.12        192.168.0.30          HTTP     293    HTTP/1.1 304 Not Modified 
Frame 266: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface 0
Ethernet II, Src: Netgear_b1:d7:0a (2c:30:33:b1:d7:0a), Dst: HonHaiPr_b7:3d:ee (5c:ac:4c:b7:3d:ee)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.30
Transmission Control Protocol, Src Port: 80, Dst Port: 6162, Seq: 241, Ack: 757, Len: 239
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
            [HTTP/1.1 304 Not Modified\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Response Version: HTTP/1.1
        Status Code: 304
        [Status Code Description: Not Modified]
        Response Phrase: Not Modified
    Date: Tue, 26 Feb 2019 05:19:09 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=99\r\n
    ETag: "173-582b279ba07f9"\r\n
    \r\n
    [HTTP response 2/3]
    [Time since request: 0.091689000 seconds]
    [Prev request in frame: 261]
    [Prev response in frame: 263]
    [Request in frame: 265]
    [Next request in frame: 268]
    [Next response in frame: 271]
```

(Section 3)

12) Only 1 Http get request messages my browser sent. Packet 130.

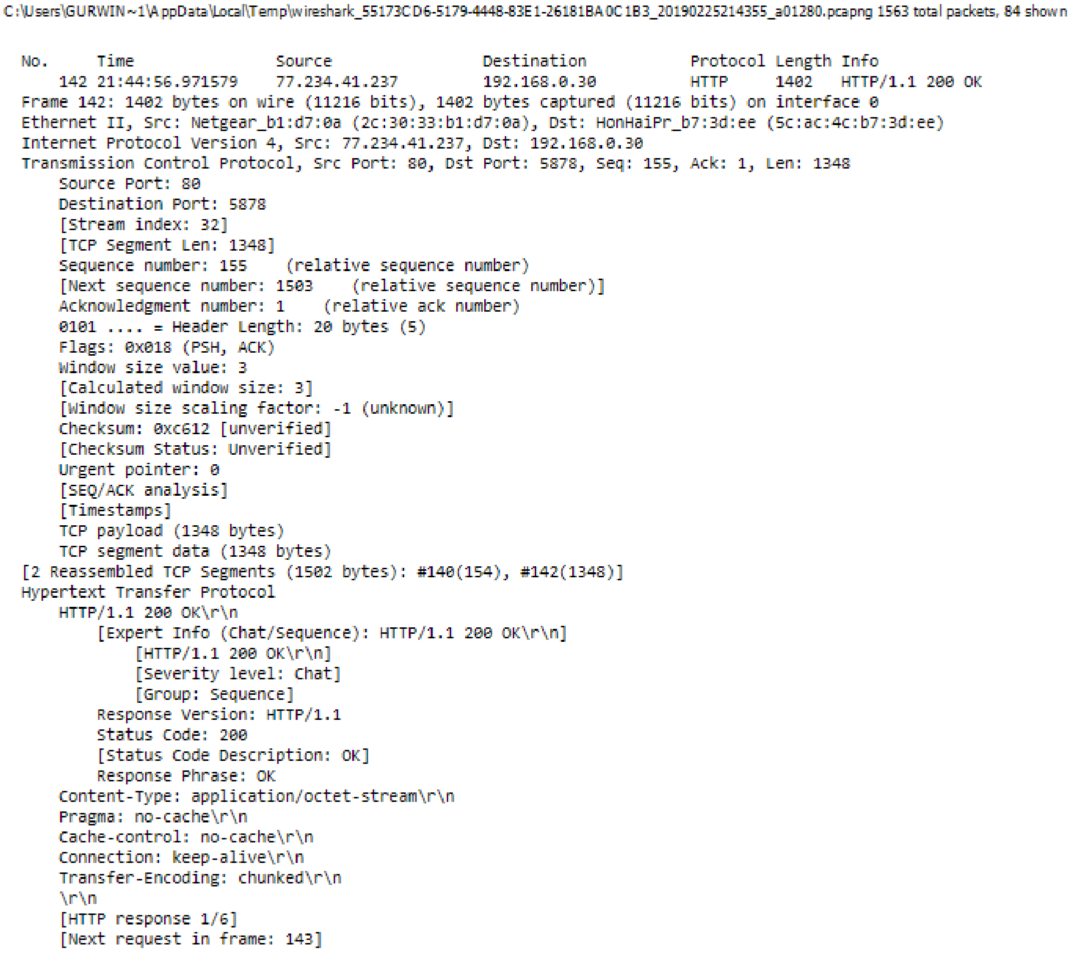
13) Packet 142 contains status code and phrase associated with HTTP GET request.
14) Status code: 200 and phrase: OK.
15) 5 TCP segments

GET MESSAGE



```
No.     Time               Source                Destination           Protocol Length Info
    130 21:44:48.391697    192.168.0.30          128.119.245.12        HTTP     433    GET /wireshark-labs/HTTP-wireshark-file3.html
HTTP/1.1
Frame 130: 433 bytes on wire (3464 bits), 433 bytes captured (3464 bits) on interface 0
Ethernet II, Src: HonHaiPr_b7:3d:ee (5c:ac:4c:b7:3d:ee), Dst: Netgear_b1:d7:0a (2c:30:33:b1:d7:0a)
Internet Protocol Version 4, Src: 192.168.0.30, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 6240, Dst Port: 80, Seq: 1, Ack: 1, Len: 379
    Source Port: 6240
    Destination Port: 80
    [Stream index: 30]
    [TCP Segment Len: 379]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 380    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window size value: 16425
    [Calculated window size: 65700]
    [Window size scaling factor: 4]
    Checksum: 0xd57e [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
    [Timestamps]
    TCP payload (379 bytes)
Hypertext Transfer Protocol
    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]
            [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
    Accept: text/html, application/xhtml+xml, */*\r\n
    Accept-Language: en-US\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
    Accept-Encoding: gzip, deflate\r\n
    Host: gaia.cs.umass.edu\r\n
    If-Modified-Since: Mon, 25 Feb 2019 06:59:01 GMT\r\n
    If-None-Match: "1194-582b279b9b9d8"\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
    [HTTP request 1/1]
    [Response in frame: 132]
```

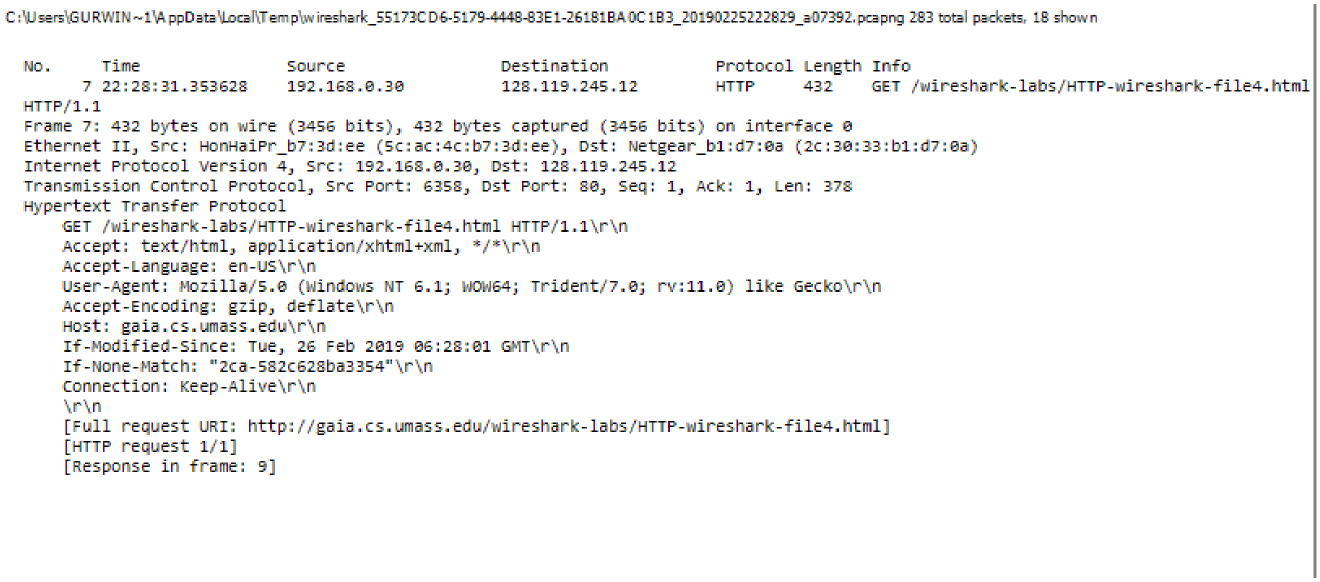
RESPONSE MESSAGE



```
C:\Users\GURWIN~1\AppData\Local\Temp\wireshark_55173CD6-5179-4448-83E1-26181BA0C1B3_20190225214355_a01280.pcapng 1563 total packets, 84 shown

No.     Time               Source                Destination           Protocol Length Info
    142 21:44:56.971579    77.234.41.237         192.168.0.30          HTTP     1402   HTTP/1.1 200 OK
Frame 142: 1402 bytes on wire (11216 bits), 1402 bytes captured (11216 bits) on interface 0
Ethernet II, Src: Netgear_b1:d7:0a (2c:30:33:b1:d7:0a), Dst: HonHaiPr_b7:3d:ee (5c:ac:4c:b7:3d:ee)
Internet Protocol Version 4, Src: 77.234.41.237, Dst: 192.168.0.30
Transmission Control Protocol, Src Port: 80, Dst Port: 5878, Seq: 155, Ack: 1, Len: 1348
    Source Port: 80
    Destination Port: 5878
    [Stream index: 32]
    [TCP Segment Len: 1348]
    Sequence number: 155    (relative sequence number)
    [Next sequence number: 1503    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window size value: 3
    [Calculated window size: 3]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0xc612 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    [SEQ/ACK analysis]
    [Timestamps]
    TCP payload (1348 bytes)
    TCP segment data (1348 bytes)
[2 Reassembled TCP Segments (1502 bytes): #140(154), #142(1348)]
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
            [HTTP/1.1 200 OK\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Content-Type: application/octet-stream\r\n
    Pragma: no-cache\r\n
    Cache-control: no-cache\r\n
    Connection: keep-alive\r\n
    Transfer-Encoding: chunked\r\n
    \r\n
    [HTTP response 1/6]
    [Next request in frame: 143]
```

(Section 4)

16) My browser sent 3 Http GET request messages,
    a. http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html
    b. http://manic.cs.umass.edu/~kurose/cover_5th_ed.jpg
    c. http://gaia.cs.umass.edu/pearson.png
17) They are download serially because one image time since request is 0.095335000, and other is 0.341225000



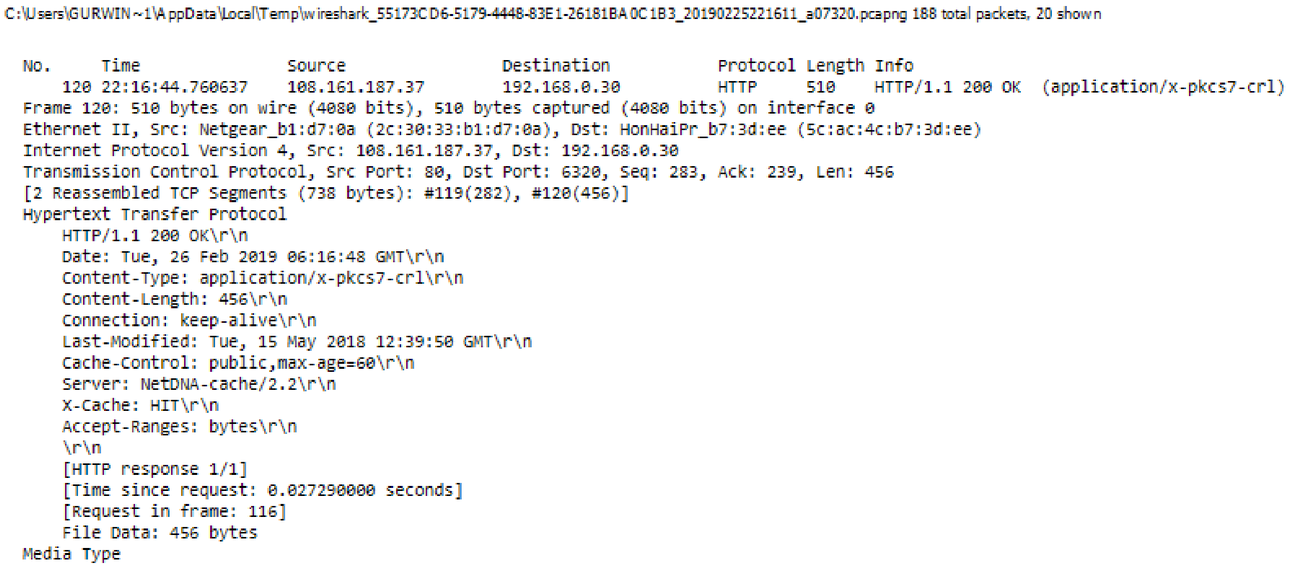
C:\Users\GURWIN~1\AppData\Local\Temp\wireshark_55173CD6-5179-4448-83E1-26181BA0C1B3_20190225222829_a07392.pcapng 283 total packets, 18 shown

```
No.     Time               Source                Destination           Protocol Length Info
      7 22:28:31.353628    192.168.0.30          128.119.245.12        HTTP     432    GET /wireshark-labs/HTTP-wireshark-file4.html
HTTP/1.1
Frame 7: 432 bytes on wire (3456 bits), 432 bytes captured (3456 bits) on interface 0
Ethernet II, Src: HonHaiPr_b7:3d:ee (5c:ac:4c:b7:3d:ee), Dst: Netgear_b1:d7:0a (2c:30:33:b1:d7:0a)
Internet Protocol Version 4, Src: 192.168.0.30, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 6358, Dst Port: 80, Seq: 1, Ack: 1, Len: 378
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n
    Accept: text/html, application/xhtml+xml, */*\r\n
    Accept-Language: en-US\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
    Accept-Encoding: gzip, deflate\r\n
    Host: gaia.cs.umass.edu\r\n
    If-Modified-Since: Tue, 26 Feb 2019 06:28:01 GMT\r\n
    If-None-Match: "2ca-582c628ba3354"\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]
    [HTTP request 1/1]
    [Response in frame: 9]
```

(Section 5)

18) The Server response is 401 Unauthorized.

19) Autorization:Basic



C:\Users\GURWIN~1\AppData\Local\Temp\wireshark_55173CD6-5179-4448-83E1-26181BA0C1B3_20190225221611_a07320.pcapng 188 total packets, 20 shown

```
No.     Time               Source                Destination           Protocol Length Info
    120 22:16:44.760637    108.161.187.37        192.168.0.30          HTTP     510    HTTP/1.1 200 OK  (application/x-pkcs7-crl)
Frame 120: 510 bytes on wire (4080 bits), 510 bytes captured (4080 bits) on interface 0
Ethernet II, Src: Netgear_b1:d7:0a (2c:30:33:b1:d7:0a), Dst: HonHaiPr_b7:3d:ee (5c:ac:4c:b7:3d:ee)
Internet Protocol Version 4, Src: 108.161.187.37, Dst: 192.168.0.30
Transmission Control Protocol, Src Port: 80, Dst Port: 6320, Seq: 283, Ack: 239, Len: 456
[2 Reassembled TCP Segments (738 bytes): #119(282), #120(456)]
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Tue, 26 Feb 2019 06:16:48 GMT\r\n
    Content-Type: application/x-pkcs7-crl\r\n
    Content-Length: 456\r\n
    Connection: keep-alive\r\n
    Last-Modified: Tue, 15 May 2018 12:39:50 GMT\r\n
    Cache-Control: public,max-age=60\r\n
    Server: NetDNA-cache/2.2\r\n
    X-Cache: HIT\r\n
    Accept-Ranges: bytes\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.027290000 seconds]
    [Request in frame: 116]
    File Data: 456 bytes
Media Type
```