School of Electrical and Electronic of Enginnering
EEE 4474-01 : Experiments on Communication Networks
2조 2016142096 **조윤신**, 2017142043 **김재민**

Result Report Week 1

wireshark(1) : Getting Started HTTP DNS

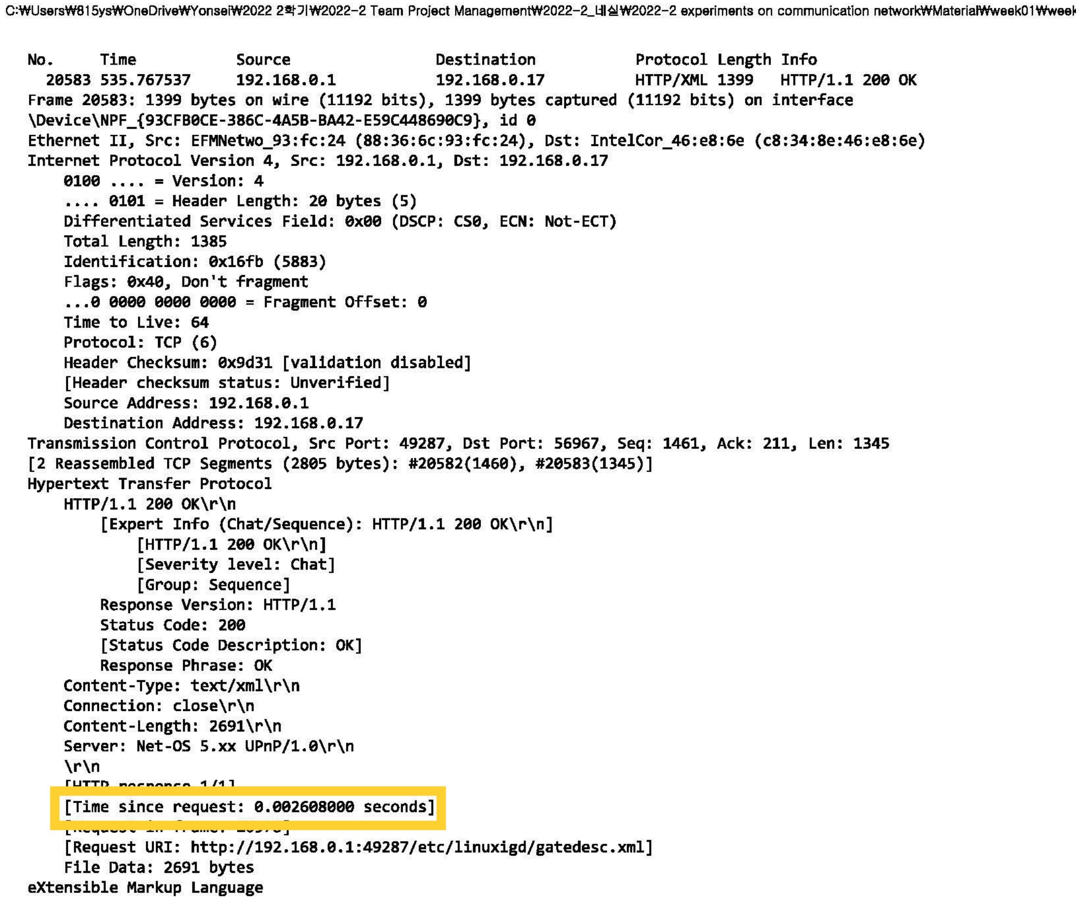
1 Experiment 1 : Getting Started

1.a Running Wireshark

Problems

Problem 1: List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.
Answer TCP, DNS, TLSV ... etc

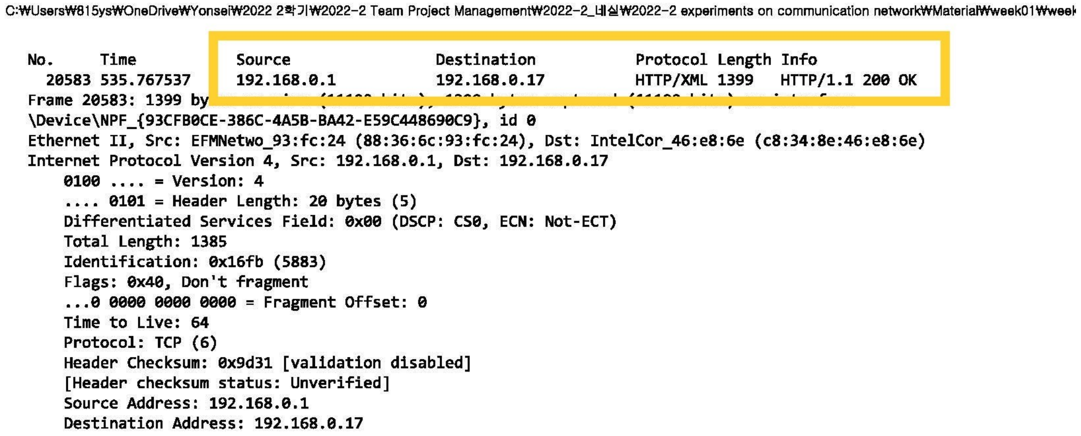
Problem 2: How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)
Answer It tooks 0.002608 (sec)



```
C:₩Users₩815ys₩OneDrive₩Yonsei₩2022 2학기₩2022-2 Team Project Management₩2022-2_네실₩2022-2 experiments on communication network₩Material₩week01₩week

No.     Time           Source                Destination           Protocol Length Info
  20583 535.767537     192.168.0.1           192.168.0.17          HTTP/XML 1399   HTTP/1.1 200 OK
Frame 20583: 1399 bytes on wire (11192 bits), 1399 bytes captured (11192 bits) on interface
\Device\NPF_{93CFB0CE-386C-4A5B-BA42-E59C448690C9}, id 0
Ethernet II, Src: EFMNetwo_93:fc:24 (88:36:6c:93:fc:24), Dst: IntelCor_46:e8:6e (c8:34:8e:46:e8:6e)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.17
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1385
    Identification: 0x16fb (5883)
    Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x9d31 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.1
    Destination Address: 192.168.0.17
Transmission Control Protocol, Src Port: 49287, Dst Port: 56967, Seq: 1461, Ack: 211, Len: 1345
[2 Reassembled TCP Segments (2805 bytes): #20582(1460), #20583(1345)]
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: text/xml\r\n
    Connection: close\r\n
    Content-Length: 2691\r\n
    Server: Net-OS 5.xx UPnP/1.0\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.002608000 seconds]
    [Request in frame: [illegible]]
    [Request URI: http://192.168.0.1:49287/etc/linuxigd/gatedesc.xml]
    File Data: 2691 bytes
eXtensible Markup Language
```

Figure 1: Problem 1-2's screenshot : Packet-HTTP/1.1 200 OK

Problem 3: What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)? What is the Internet address of your computer?
Answer Since the packet I print out is the replied message from gaia.cs.umass.edu. The source adr that value of 192.168.0.1 is the gaia.cs.umass.edu 's adr, and the destination adr, 192.168.0.17 is the internet adr of my computer.

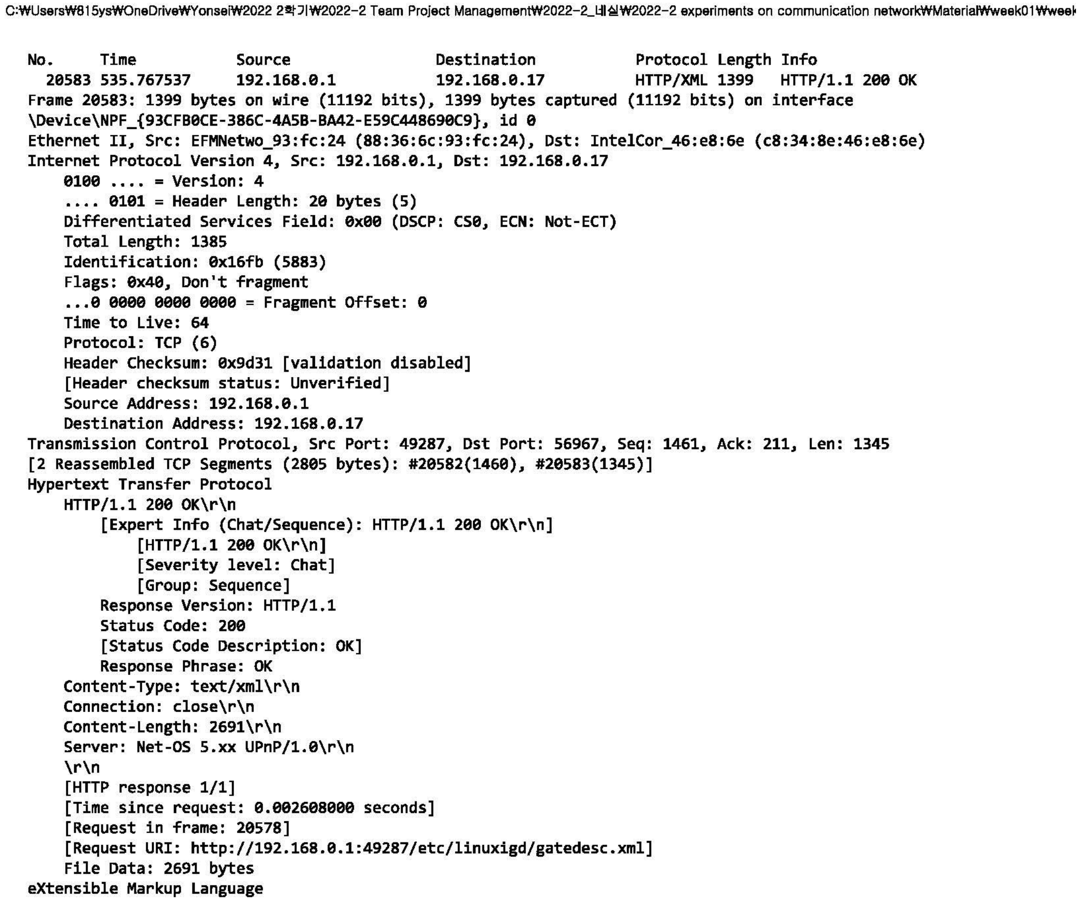


```
C:₩Users₩815ys₩OneDrive₩Yonsei₩2022 2학기₩2022-2 Team Project Management₩2022-2_네실₩2022-2 experiments on communication network₩Material₩week01₩week

No.     Time           Source                Destination           Protocol Length Info
  20583 535.767537     192.168.0.1           192.168.0.17          HTTP/XML 1399   HTTP/1.1 200 OK
Frame 20583: 1399 by
\Device\NPF_{93CFB0CE-386C-4A5B-BA42-E59C448690C9}, id 0
Ethernet II, Src: EFMNetwo_93:fc:24 (88:36:6c:93:fc:24), Dst: IntelCor_46:e8:6e (c8:34:8e:46:e8:6e)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.17
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1385
    Identification: 0x16fb (5883)
    Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x9d31 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.1
    Destination Address: 192.168.0.17
```

Figure 2: Problem 1-3's screenshot : Packet-HTTP/1.1 200 OK

Problem 4: Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the "Selected Packet Only" and "Print as displayed" radial buttons, and then click OK.

Answer



```
C:₩Users₩815ys₩OneDrive₩Yonsei₩2022 2학기₩2022-2 Team Project Management₩2022-2_네실₩2022-2 experiments on communication network₩Material₩week01₩week

No.     Time           Source                Destination           Protocol Length Info
  20583 535.767537     192.168.0.1           192.168.0.17          HTTP/XML 1399   HTTP/1.1 200 OK
Frame 20583: 1399 bytes on wire (11192 bits), 1399 bytes captured (11192 bits) on interface
\Device\NPF_{93CFB0CE-386C-4A5B-BA42-E59C448690C9}, id 0
Ethernet II, Src: EFMNetwo_93:fc:24 (88:36:6c:93:fc:24), Dst: IntelCor_46:e8:6e (c8:34:8e:46:e8:6e)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.17
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1385
    Identification: 0x16fb (5883)
    Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x9d31 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.1
    Destination Address: 192.168.0.17
Transmission Control Protocol, Src Port: 49287, Dst Port: 56967, Seq: 1461, Ack: 211, Len: 1345
[2 Reassembled TCP Segments (2805 bytes): #20582(1460), #20583(1345)]
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: text/xml\r\n
    Connection: close\r\n
    Content-Length: 2691\r\n
    Server: Net-OS 5.xx UPnP/1.0\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.002608000 seconds]
    [Request in frame: 20578]
    [Request URI: http://192.168.0.1:49287/etc/linuxigd/gatedesc.xml]
    File Data: 2691 bytes
eXtensible Markup Language
```

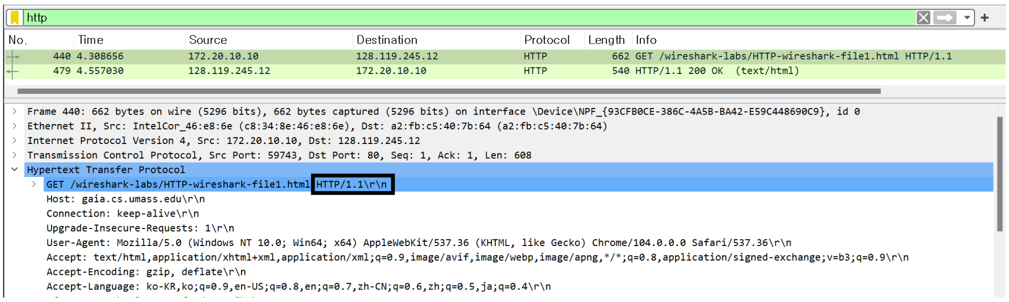
Figure 3: Problem 1-4's screenshot : Packet-HTTP/1.1 200 OK

2 Experiment 2 : HTTP

2.a HTTP : The Basic HTTP GET/response interaction

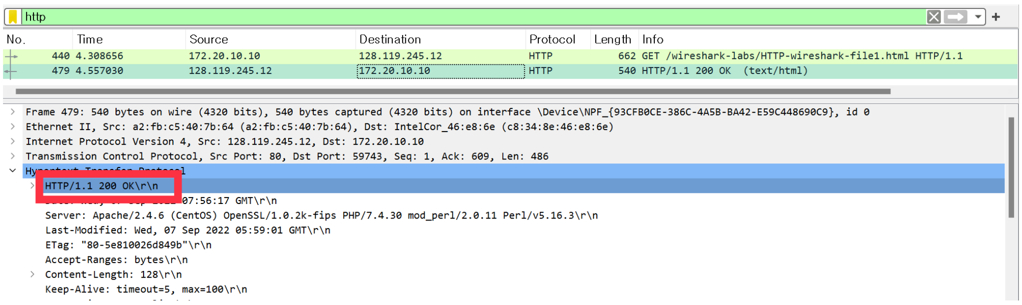
Problems

Problem 1: Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
Answer My browser's HTTP version : 1.1 / The server's HTTP version : 1.1



```
http
No.    Time        Source          Destination     Protocol  Length  Info
  440  4.308656    172.20.10.10    128.119.245.12  HTTP         662  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  479  4.557030    128.119.245.12  172.20.10.10    HTTP         540  HTTP/1.1 200 OK  (text/html)

> Frame 440: 662 bytes on wire (5296 bits), 662 bytes captured (5296 bits) on interface \Device\NPF_{93CFB0CE-386C-4A5B-BA42-E59C448690C9}, id 0
> Ethernet II, Src: IntelCor_46:e8:6e (c8:34:8e:46:e8:6e), Dst: a2:fb:c5:40:7b:64 (a2:fb:c5:40:7b:64)
> Internet Protocol Version 4, Src: 172.20.10.10, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 59743, Dst Port: 80, Seq: 1, Ack: 1, Len: 608
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7,zh-CN;q=0.6,zh;q=0.5,ja;q=0.4\r\n
```

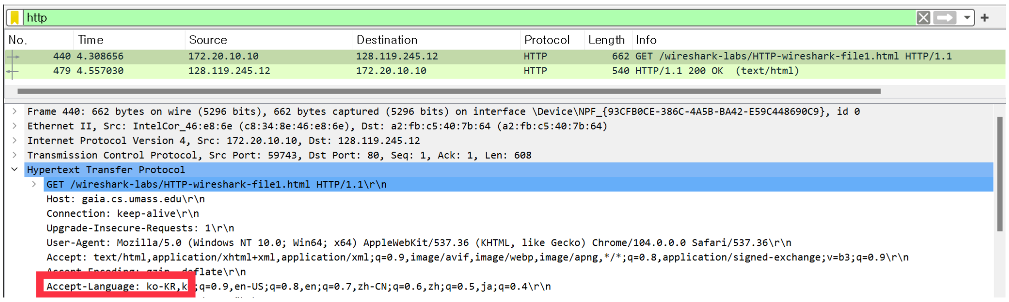
Figure 4: Problem 2-1-1's screenshot : Packet-GET / wireshark-file1.html HTTP/1.1



```
http
No.    Time        Source          Destination     Protocol  Length  Info
  440  4.308656    172.20.10.10    128.119.245.12  HTTP         662  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  479  4.557030    128.119.245.12  172.20.10.10    HTTP         540  HTTP/1.1 200 OK  (text/html)

> Frame 479: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{93CFB0CE-386C-4A5B-BA42-E59C448690C9}, id 0
> Ethernet II, Src: a2:fb:c5:40:7b:64 (a2:fb:c5:40:7b:64), Dst: IntelCor_46:e8:6e (c8:34:8e:46:e8:6e)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.20.10.10
> Transmission Control Protocol, Src Port: 80, Dst Port: 59743, Seq: 1, Ack: 609, Len: 486
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Wed, 07 Sep 2022 07:56:17 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 07 Sep 2022 05:59:01 GMT\r\n
    ETag: "80-5e810026d849b"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
```

Figure 5: Problem 2-1-2's screenshot : Packet-HTTP/1.1 200 OK

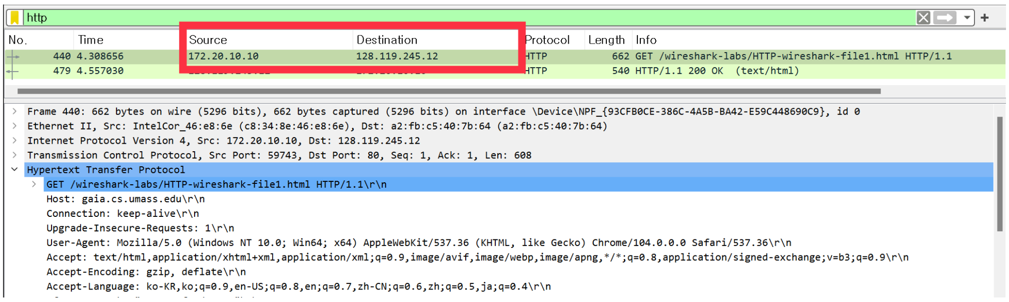
Problem 2: What languages (if any) does your browser indicate that it can accept to the server?
Answer Accept-Language : ko-kr



```
http
No.    Time        Source          Destination     Protocol  Length  Info
  440  4.308656    172.20.10.10    128.119.245.12  HTTP         662  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  479  4.557030    128.119.245.12  172.20.10.10    HTTP         540  HTTP/1.1 200 OK  (text/html)

> Frame 440: 662 bytes on wire (5296 bits), 662 bytes captured (5296 bits) on interface \Device\NPF_{93CFB0CE-386C-4A5B-BA42-E59C448690C9}, id 0
> Ethernet II, Src: IntelCor_46:e8:6e (c8:34:8e:46:e8:6e), Dst: a2:fb:c5:40:7b:64 (a2:fb:c5:40:7b:64)
> Internet Protocol Version 4, Src: 172.20.10.10, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 59743, Dst Port: 80, Seq: 1, Ack: 1, Len: 608
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7,zh-CN;q=0.6,zh;q=0.5,ja;q=0.4\r\n
```

Figure 6: Problem 2-2's screenshot : Packet-GET / wireshark-file1.html HTTP/1.1

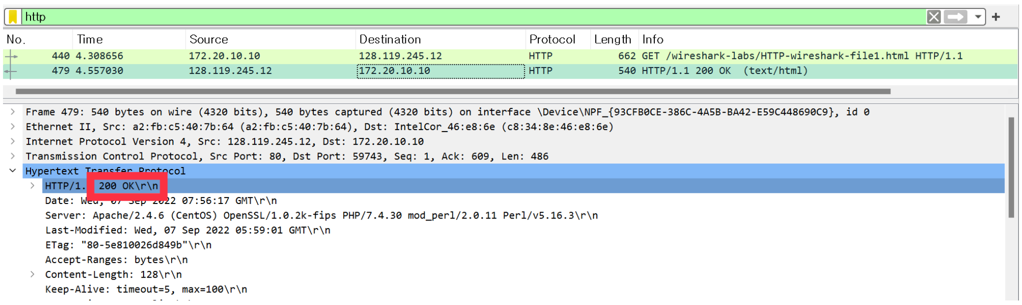
Problem 3: What is the IP address of your computer? Of the gaia.cs.umass.edu server?
Answer My computer : 172.20.10.10 / gaia.cd.umass.edu : 128.119.245.12



```
http
No.    Time        Source          Destination     Protocol  Length  Info
  440  4.308656    172.20.10.10    128.119.245.12  HTTP         662  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  479  4.557030    128.119.245.12  172.20.10.10    HTTP         540  HTTP/1.1 200 OK  (text/html)

> Frame 440: 662 bytes on wire (5296 bits), 662 bytes captured (5296 bits) on interface \Device\NPF_{93CFB0CE-386C-4A5B-BA42-E59C448690C9}, id 0
> Ethernet II, Src: IntelCor_46:e8:6e (c8:34:8e:46:e8:6e), Dst: a2:fb:c5:40:7b:64 (a2:fb:c5:40:7b:64)
> Internet Protocol Version 4, Src: 172.20.10.10, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 59743, Dst Port: 80, Seq: 1, Ack: 1, Len: 608
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7,zh-CN;q=0.6,zh;q=0.5,ja;q=0.4\r\n
```

Figure 7: Problem 2-3's screenshot : Packet-GET / wireshark-file1.html HTTP/1.1

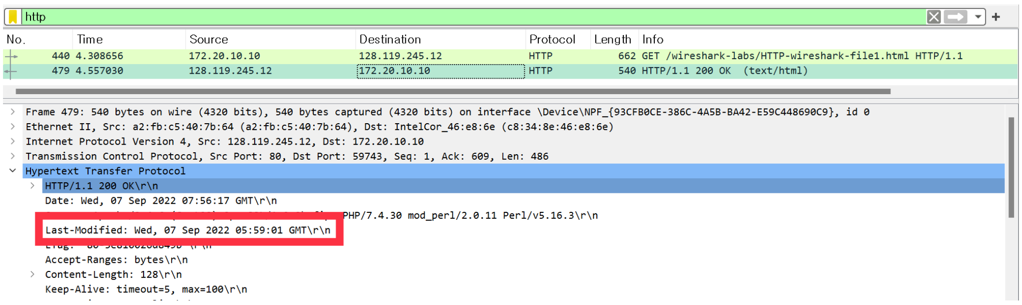
Problem 4: What is the status code returned from the server to your browser?
Answer status code : 200 OK



```
http

No.   Time       Source          Destination     Protocol  Length  Info
  440 4.308656   172.20.10.10    128.119.245.12  HTTP         662  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  479 4.557030   128.119.245.12  172.20.10.10    HTTP         540  HTTP/1.1 200 OK  (text/html)

> Frame 479: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{93CFB0CE-386C-4A5B-BA42-E59C448690C9}, id 0
> Ethernet II, Src: a2:fb:c5:40:7b:64 (a2:fb:c5:40:7b:64), Dst: IntelCor_46:e8:6e (c8:34:8e:46:e8:6e)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.20.10.10
> Transmission Control Protocol, Src Port: 80, Dst Port: 59743, Seq: 1, Ack: 609, Len: 486
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Wed, 07 Sep 2022 07:56:17 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 07 Sep 2022 05:59:01 GMT\r\n
    ETag: "80-5e810026d849b"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
```

Figure 8: Problem 2-4's screenshot : Packet-HTTP/1.1 200 OK

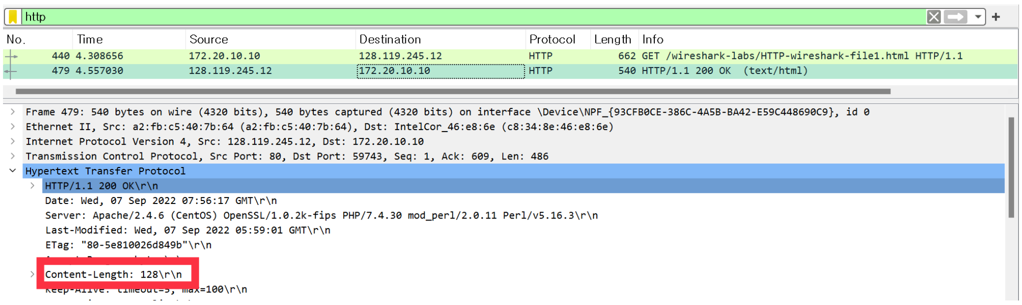
Problem 5: When was the HTML file that you are retrieving last modified at the server?
Answer Last-Modified : Wed, 07 Sep 2022 05:59:01 GMT



```
http

No.   Time       Source          Destination     Protocol  Length  Info
  440 4.308656   172.20.10.10    128.119.245.12  HTTP         662  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  479 4.557030   128.119.245.12  172.20.10.10    HTTP         540  HTTP/1.1 200 OK  (text/html)

> Frame 479: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{93CFB0CE-386C-4A5B-BA42-E59C448690C9}, id 0
> Ethernet II, Src: a2:fb:c5:40:7b:64 (a2:fb:c5:40:7b:64), Dst: IntelCor_46:e8:6e (c8:34:8e:46:e8:6e)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.20.10.10
> Transmission Control Protocol, Src Port: 80, Dst Port: 59743, Seq: 1, Ack: 609, Len: 486
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Wed, 07 Sep 2022 07:56:17 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 07 Sep 2022 05:59:01 GMT\r\n
    ETag: "80-5e810026d849b"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
```

Figure 9: Problem 2-5's screenshot : Packet-HTTP/1.1 200 OK

Problem 6: How many bytes of content are being returned to your browser?
Answer 128 bytes



```
http

No.   Time       Source          Destination     Protocol  Length  Info
  440 4.308656   172.20.10.10    128.119.245.12  HTTP         662  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  479 4.557030   128.119.245.12  172.20.10.10    HTTP         540  HTTP/1.1 200 OK  (text/html)

> Frame 479: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{93CFB0CE-386C-4A5B-BA42-E59C448690C9}, id 0
> Ethernet II, Src: a2:fb:c5:40:7b:64 (a2:fb:c5:40:7b:64), Dst: IntelCor_46:e8:6e (c8:34:8e:46:e8:6e)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.20.10.10
> Transmission Control Protocol, Src Port: 80, Dst Port: 59743, Seq: 1, Ack: 609, Len: 486
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Wed, 07 Sep 2022 07:56:17 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 07 Sep 2022 05:59:01 GMT\r\n
    ETag: "80-5e810026d849b"\r\n
  > Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
```

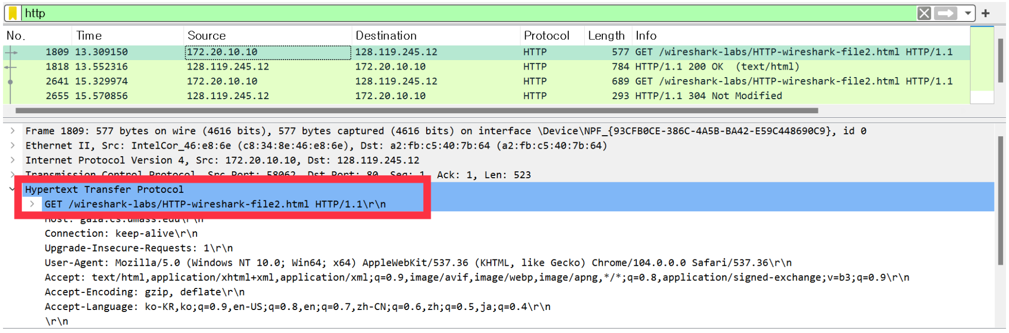
Figure 10: Problem 2-6's screenshot : Packet-HTTP/1.1 200 OK

Problem 7: By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.
Answer No, There are no headers in the HTTP Message below.

2.b HTTP : The HTTP CONDITIONAL GET/response interaction

Problems

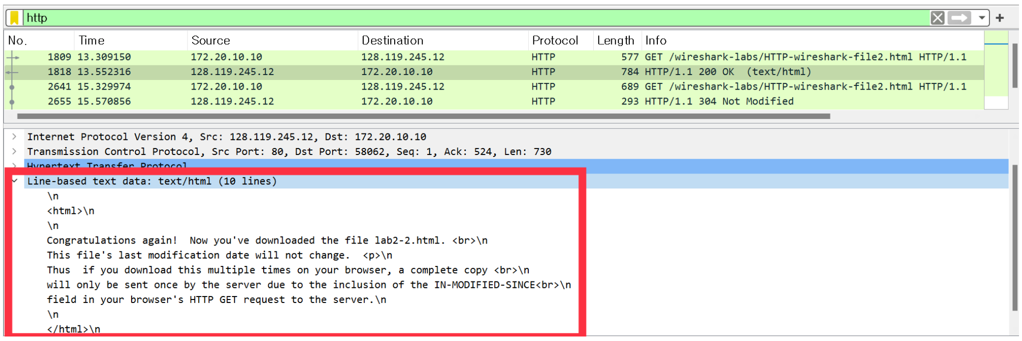
Problem 8: Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?
Answer There is no "IF-MODIFIED-SINCE" in the first GET packet.



```
http
No.     Time        Source          Destination     Protocol  Length  Info
  1809 13.309150   172.20.10.10    128.119.245.12  HTTP         577 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  1818 13.552316   128.119.245.12  172.20.10.10    HTTP         784 HTTP/1.1 200 OK  (text/html)
  2641 15.329974   172.20.10.10    128.119.245.12  HTTP         689 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  2655 15.570856   128.119.245.12  172.20.10.10    HTTP         293 HTTP/1.1 304 Not Modified

> Frame 1809: 577 bytes on wire (4616 bits), 577 bytes captured (4616 bits) on interface \Device\NPF_{93CFB0CE-386C-4A5B-BA42-E59C448690C9}, id 0
> Ethernet II, Src: IntelCor_46:e8:6e (c8:34:8e:46:e8:6e), Dst: a2:fb:c5:40:7b:64 (a2:fb:c5:40:7b:64)
> Internet Protocol Version 4, Src: 172.20.10.10, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 58062, Dst Port: 80, Seq: 1, Ack: 1, Len: 523
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7,zh-CN;q=0.6,zh;q=0.5,ja;q=0.4\r\n
    \r\n
```

Figure 11: Problem 2-8's screenshot : Packet-GET / wireshark-file2.html HTTP/1.1

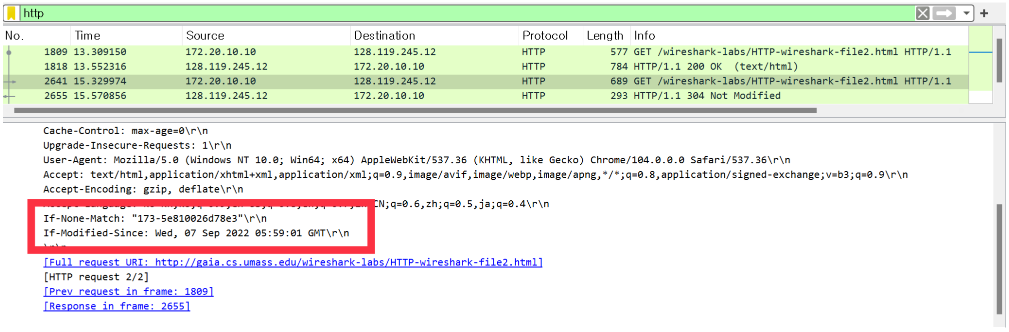
Problem 9: Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
Answer Yes. The server explictly returned the contents of the html file.



```
http
No.     Time        Source          Destination     Protocol  Length  Info
  1809 13.309150   172.20.10.10    128.119.245.12  HTTP         577 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  1818 13.552316   128.119.245.12  172.20.10.10    HTTP         784 HTTP/1.1 200 OK  (text/html)
  2641 15.329974   172.20.10.10    128.119.245.12  HTTP         689 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  2655 15.570856   128.119.245.12  172.20.10.10    HTTP         293 HTTP/1.1 304 Not Modified

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.20.10.10
> Transmission Control Protocol, Src Port: 80, Dst Port: 58062, Seq: 1, Ack: 524, Len: 730
> Hypertext Transfer Protocol
v Line-based text data: text/html (10 lines)
    \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
```

Figure 12: Problem 2-9's screenshot : Packet-HTTP/1.1 200 OK

Problem 10: Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? If so, what information follows the "IF-MODIFIED-SINCE:" header?
Answer Yes. The information followed as 'wed, 07 sep 2022 05:59:01 GMT'

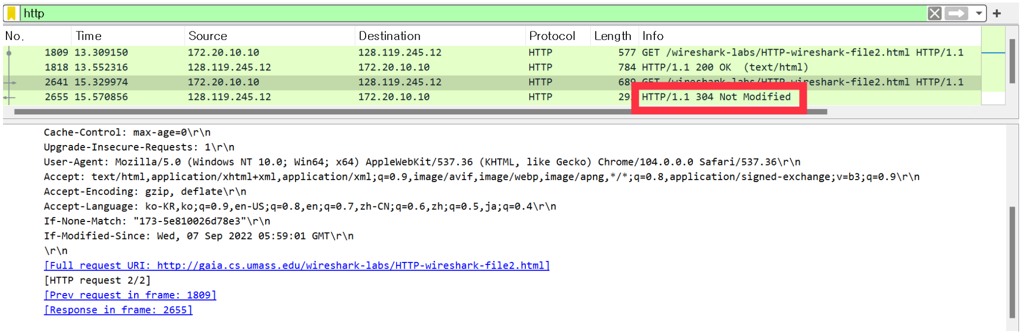


```
http
No.     Time        Source          Destination     Protocol  Length  Info
  1809 13.309150   172.20.10.10    128.119.245.12  HTTP         577 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  1818 13.552316   128.119.245.12  172.20.10.10    HTTP         784 HTTP/1.1 200 OK  (text/html)
  2641 15.329974   172.20.10.10    128.119.245.12  HTTP         689 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  2655 15.570856   128.119.245.12  172.20.10.10    HTTP         293 HTTP/1.1 304 Not Modified

    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7,zh-CN;q=0.6,zh;q=0.5,ja;q=0.4\r\n
    If-None-Match: "173-5e810026d78e3"\r\n
    If-Modified-Since: Wed, 07 Sep 2022 05:59:01 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 2/2]
    [Prev request in frame: 1809]
    [Response in frame: 2655]
```

Figure 13: Problem 2-10's screenshot : Packet-GET / wireshark-file2.html HTTP/1.1

Problem 11: What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.
Answer The status code and phrase returned from the server is 'HTTP/1.1 Note Modified'.
Since the browser loaded the file data from the browser's cache[1], the server not returned the file contents.

[1] That, file hasnt's been modified



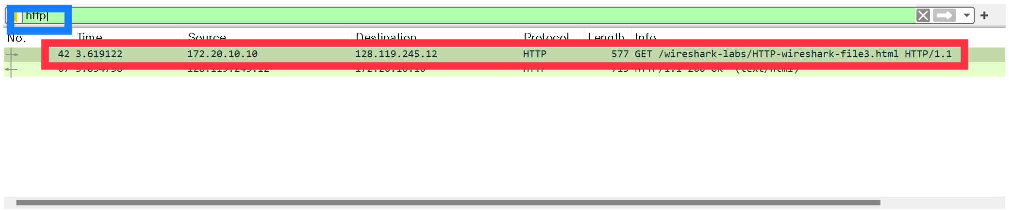
```
http
No.    Time       Source           Destination      Protocol  Length Info
  1809 13.309150  172.20.10.10     128.119.245.12   HTTP      577 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  1818 13.552316  128.119.245.12   172.20.10.10     HTTP      784 HTTP/1.1 200 OK  (text/html)
  2641 15.329974  172.20.10.10     128.119.245.12   HTTP      689 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  2655 15.570856  128.119.245.12   172.20.10.10     HTTP      29  HTTP/1.1 304 Not Modified

    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7,zh-CN;q=0.6,zh;q=0.5,ja;q=0.4\r\n
    If-None-Match: "173-5e810026d78e3"\r\n
    If-Modified-Since: Wed, 07 Sep 2022 05:59:01 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 2/2]
    [Prev request in frame: 1809]
    [Response in frame: 2655]
```

Figure 14: Problem 2-11's screenshot : Packet-HTTP/1.1 304 Not Modified

2.c HTTP : Retrieving Long Documents

Problems

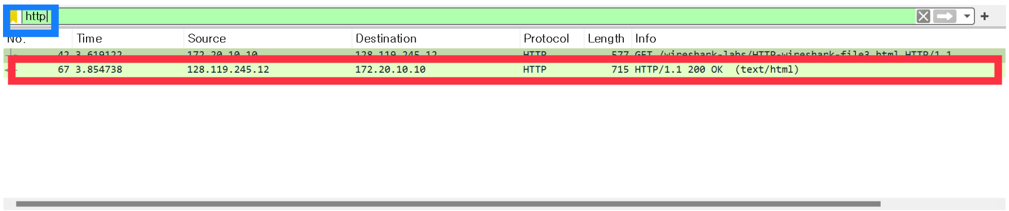
Problem 12: How many HTTP GET request messages did your browser send?
Answer 1 times / Packet no.42



```
http|
No.    Time       Source           Destination      Protocol  Length Info
    42 3.619122   172.20.10.10     128.119.245.12   HTTP      577 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
```

Figure 15: Problem 2-12's screenshot : Captured packet lists filterd by keyword 'http' getting file3

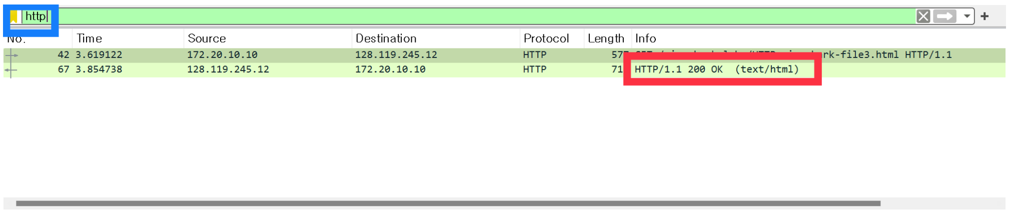
Problem 13: Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
Answer Packet no.67



```
http|
No.    Time       Source           Destination      Protocol  Length Info
    67 3.854738   128.119.245.12   172.20.10.10     HTTP      715 HTTP/1.1 200 OK  (text/html)
```

Figure 16: Problem 2-13's screenshot : Captured packet lists filterd by keyword 'http' getting file3

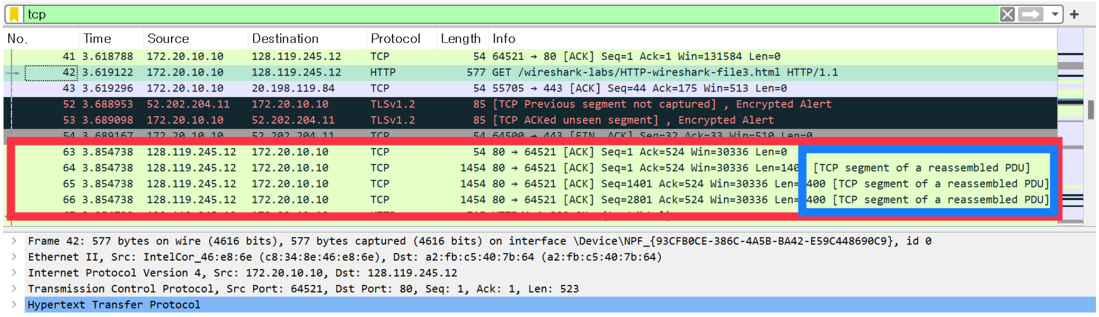
Problem 14: What is the status code and phrase in the response?
Answer Status code : 200 / Phrase : OK



```
http|
No.    Time       Source           Destination      Protocol  Length Info
    42 3.619122   172.20.10.10     128.119.245.12   HTTP      57                           rk-file3.html HTTP/1.1
    67 3.854738   128.119.245.12   172.20.10.10     HTTP      71  HTTP/1.1 200 OK  (text/html)
```

Figure 17: Problem 2-14's screenshot : Captured packet lists filterd by keyword 'http' getting file3

Problem 15: How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?
Answer
Three packets. There are three data-containing TCP segments needed to transport the single HTTP response and the text in the bill of Rights in wireshark-lab file3.



```
tcp

No.   Time      Source          Destination     Protocol  Length Info
   41 3.618788  172.20.10.10    128.119.245.12  TCP           54 64521 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
   42 3.619122  172.20.10.10    128.119.245.12  HTTP         577 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
   43 3.619296  172.20.10.10    20.198.119.84   TCP           54 55705 → 443 [ACK] Seq=44 Ack=175 Win=513 Len=0
   52 3.688953  52.202.204.11   172.20.10.10    TLSv1.2       85 [TCP Previous segment not captured] , Encrypted Alert
   53 3.689098  172.20.10.10    52.202.204.11   TLSv1.2       85 [TCP ACKed unseen segment] , Encrypted Alert
   54 3.689167  172.20.10.10    52.202.204.11   TCP           54 64500 → 443 [FIN, ACK] Seq=32 Ack=33 Win=510 Len=0
   63 3.854738  128.119.245.12  172.20.10.10    TCP           54 80 → 64521 [ACK] Seq=1 Ack=524 Win=30336 Len=0
   64 3.854738  128.119.245.12  172.20.10.10    TCP         1454 80 → 64521 [ACK] Seq=1 Ack=524 Win=30336 Len=140  [TCP segment of a reassembled PDU]
   65 3.854738  128.119.245.12  172.20.10.10    TCP         1454 80 → 64521 [ACK] Seq=1401 Ack=524 Win=30336 Len=400 [TCP segment of a reassembled PDU]
   66 3.854738  128.119.245.12  172.20.10.10    TCP         1454 80 → 64521 [ACK] Seq=2801 Ack=524 Win=30336 Len=400 [TCP segment of a reassembled PDU]

> Frame 42: 577 bytes on wire (4616 bits), 577 bytes captured (4616 bits) on interface \Device\NPF_{93CFB0CE-386C-4A5B-BA42-E59C448690C9}, id 0
> Ethernet II, Src: IntelCor_46:e8:6e (c8:34:8e:46:e8:6e), Dst: a2:fb:c5:40:7b:64 (a2:fb:c5:40:7b:64)
> Internet Protocol Version 4, Src: 172.20.10.10, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 64521, Dst Port: 80, Seq: 1, Ack: 1, Len: 523
> Hypertext Transfer Protocol
```

Figure 18: Problem 2-15's screenshot : Captured packet lists filterd by keyword 'TCP'