NEHAL JHAJHARIA (U20CS093)

COMPUTER NETWORKS

ASSIGNMENT 04

1. Give brief details about HTTP. What is the difference between HTTP and HTTPS?

HTTP is an acronym for Hypertext Transfer Protocol. This protocol is used to transmit hypertext or data over the web in the format of plain text. It makes use of Transmission Control Protocol (TCP), which uses port number 80. However, http:// is not a secured protocol. Though comparatively less secure, it is still used for browsing, video conferencing or playing video games, and so on.

HTTPS is HTTP with encryption and verification. The only difference between the two protocols is that HTTPS uses TLS (SSL) to encrypt normal HTTP requests and responses. As a result, HTTPS is far more secure than HTTP. HTTP runs at the application layer while HTTPS runs at the transport layer. HTTP runs by default on port number 80 while HTTPS runs on port number 443. HTTP is fast compared to HTTPS. Computation power is consumed by

HTTPS to encrypt the communication channel, so it is slow.

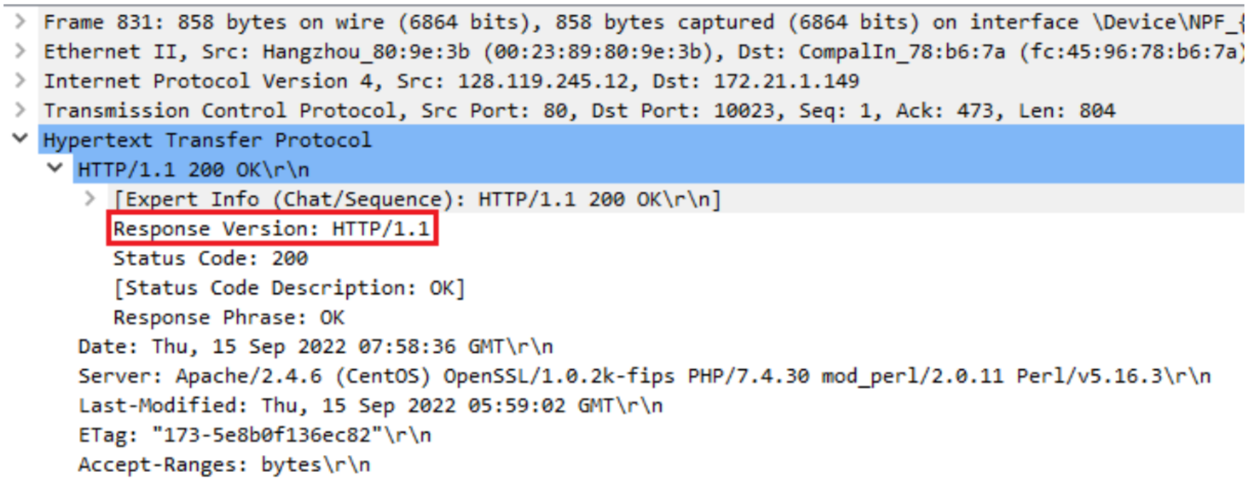
2. Write down the steps to capture HTTP request packets for the following URL. URL: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html

Step1: Start up the Wireshark packet sniffer

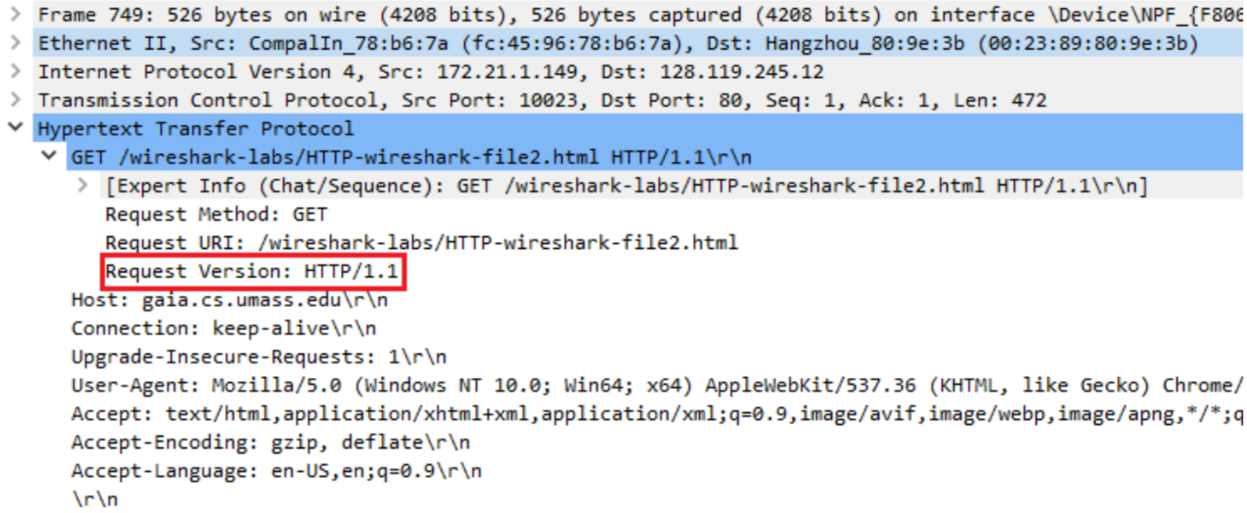
Step 2: Enter the following URL into your browser http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html

Step 3: Now select the package where noise is present. It will open the package. Step 4: Now type http in the filter section and capture your packet.

3. Answer the following questions for the above URL request. a) Which version your browser and server are running on?



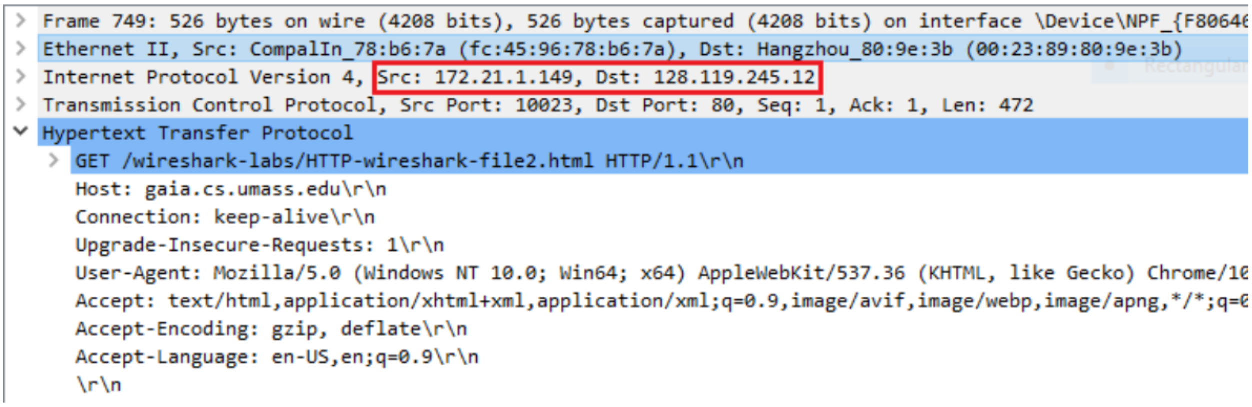
```
> Frame 831: 858 bytes on wire (6864 bits), 858 bytes captured (6864 bits) on interface \Device\NPF_{
> Ethernet II, Src: Hangzhou_80:9e:3b (00:23:89:80:9e:3b), Dst: CompalIn_78:b6:7a (fc:45:96:78:b6:7a)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.21.1.149
> Transmission Control Protocol, Src Port: 80, Dst Port: 10023, Seq: 1, Ack: 473, Len: 804
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Thu, 15 Sep 2022 07:58:36 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: Thu, 15 Sep 2022 05:59:02 GMT\r\n
    ETag: "173-5e8b0f136ec82"\r\n
    Accept-Ranges: bytes\r\n
```



```
> Frame 749: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface \Device\NPF_{F806
> Ethernet II, Src: CompalIn_78:b6:7a (fc:45:96:78:b6:7a), Dst: Hangzhou_80:9e:3b (00:23:89:80:9e:3b)
> Internet Protocol Version 4, Src: 172.21.1.149, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 10023, Dst Port: 80, Seq: 1, Ack: 1, Len: 472
v Hypertext Transfer Protocol
  v 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
    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/
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
```

Both browser and server running on HTTP/1.1 server

b) What is the IP address of your host machine and server?

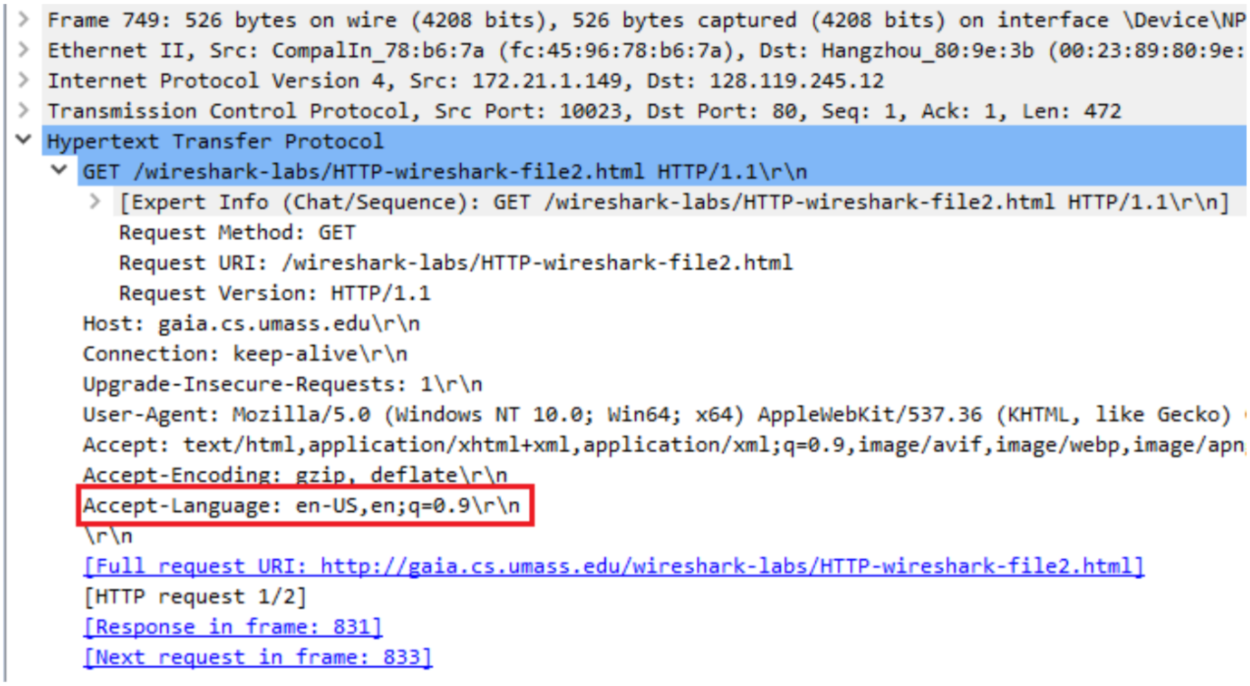


```
> Frame 749: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface \Device\NPF_{F80646
> Ethernet II, Src: CompalIn_78:b6:7a (fc:45:96:78:b6:7a), Dst: Hangzhou_80:9e:3b (00:23:89:80:9e:3b)
> Internet Protocol Version 4, Src: 172.21.1.149, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 10023, Dst Port: 80, Seq: 1, Ack: 1, Len: 472
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/10
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
```

Address of my machine is: 172.21.1.149

Address of server is: 128.119.245.12

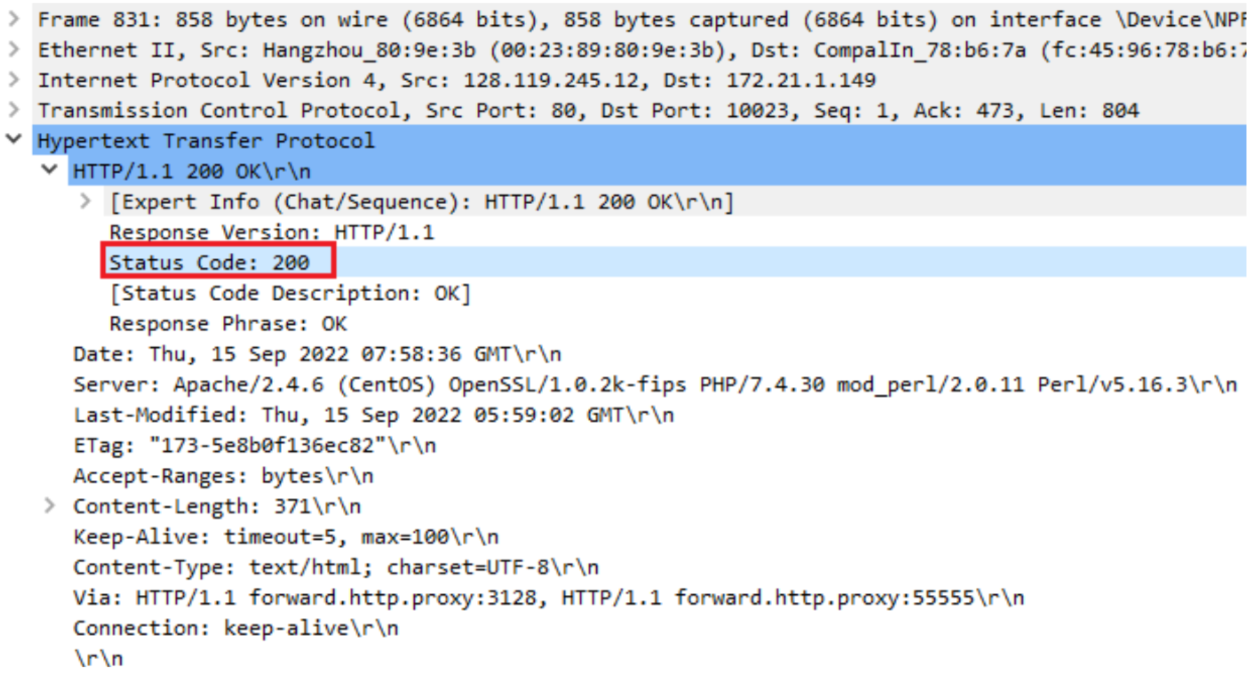
c) List out the languages accepted by your browsers.



```
> Frame 749: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface \Device\NP
> Ethernet II, Src: CompalIn_78:b6:7a (fc:45:96:78:b6:7a), Dst: Hangzhou_80:9e:3b (00:23:89:80:9e:
> Internet Protocol Version 4, Src: 172.21.1.149, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 10023, Dst Port: 80, Seq: 1, Ack: 1, Len: 472
v Hypertext Transfer Protocol
  v 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
    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)
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/2]
    [Response in frame: 831]
    [Next request in frame: 833]
```

Languages accepted by browser are: en-Us,en

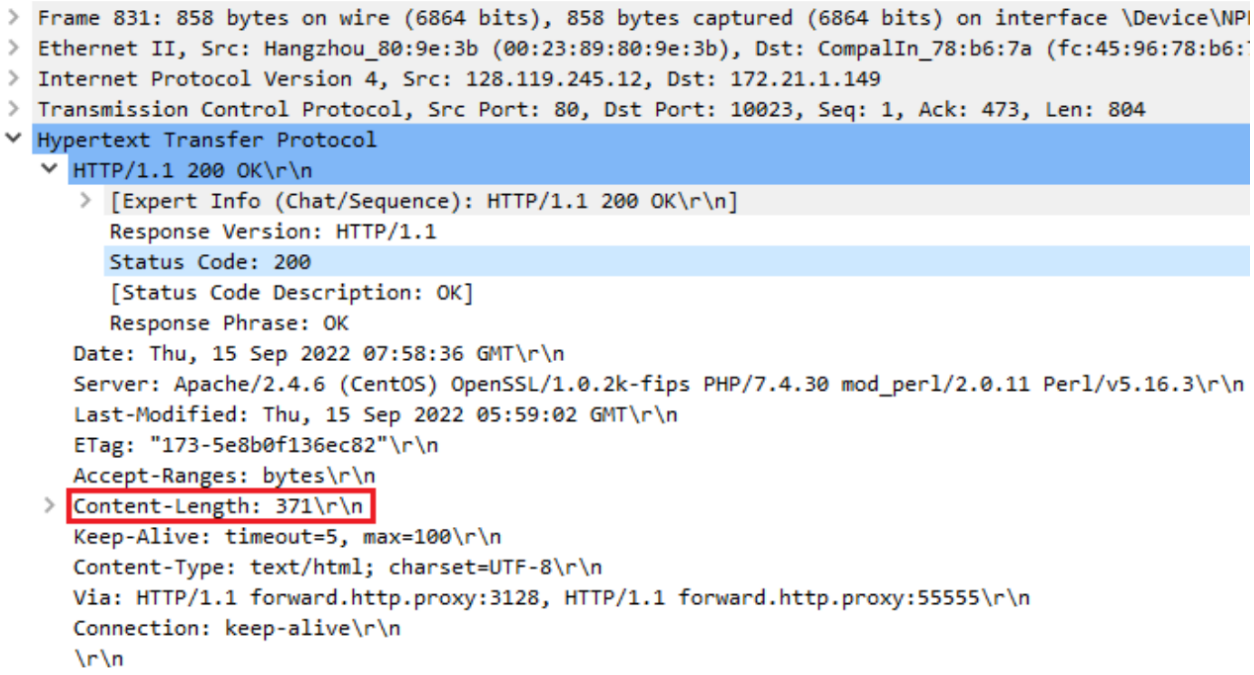
d) What is the status code returned from the server to your browser?



```
> Frame 831: 858 bytes on wire (6864 bits), 858 bytes captured (6864 bits) on interface \Device\NPF
> Ethernet II, Src: Hangzhou_80:9e:3b (00:23:89:80:9e:3b), Dst: CompalIn_78:b6:7a (fc:45:96:78:b6:7
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.21.1.149
> Transmission Control Protocol, Src Port: 80, Dst Port: 10023, Seq: 1, Ack: 473, Len: 804
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Thu, 15 Sep 2022 07:58:36 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: Thu, 15 Sep 2022 05:59:02 GMT\r\n
    ETag: "173-5e8b0f136ec82"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 371\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    Via: HTTP/1.1 forward.http.proxy:3128, HTTP/1.1 forward.http.proxy:55555\r\n
    Connection: keep-alive\r\n
    \r\n
```

Server returns 200 as status code

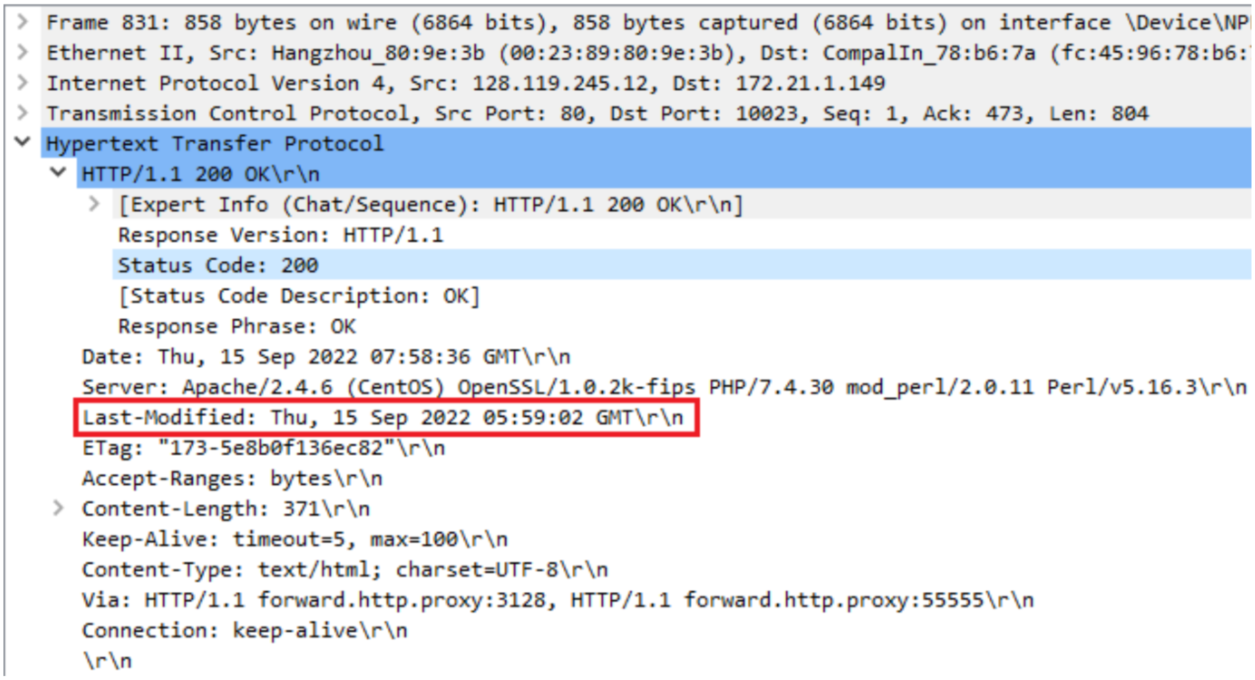
e) What is the size of the content received from the server?



```
> Frame 831: 858 bytes on wire (6864 bits), 858 bytes captured (6864 bits) on interface \Device\NPF
> Ethernet II, Src: Hangzhou_80:9e:3b (00:23:89:80:9e:3b), Dst: CompalIn_78:b6:7a (fc:45:96:78:b6:7
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.21.1.149
> Transmission Control Protocol, Src Port: 80, Dst Port: 10023, Seq: 1, Ack: 473, Len: 804
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Thu, 15 Sep 2022 07:58:36 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: Thu, 15 Sep 2022 05:59:02 GMT\r\n
    ETag: "173-5e8b0f136ec82"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 371\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    Via: HTTP/1.1 forward.http.proxy:3128, HTTP/1.1 forward.http.proxy:55555\r\n
    Connection: keep-alive\r\n
    \r\n
```

Size of content received from the server: 371

f) Check the last modification date of the retrieved HTML file.



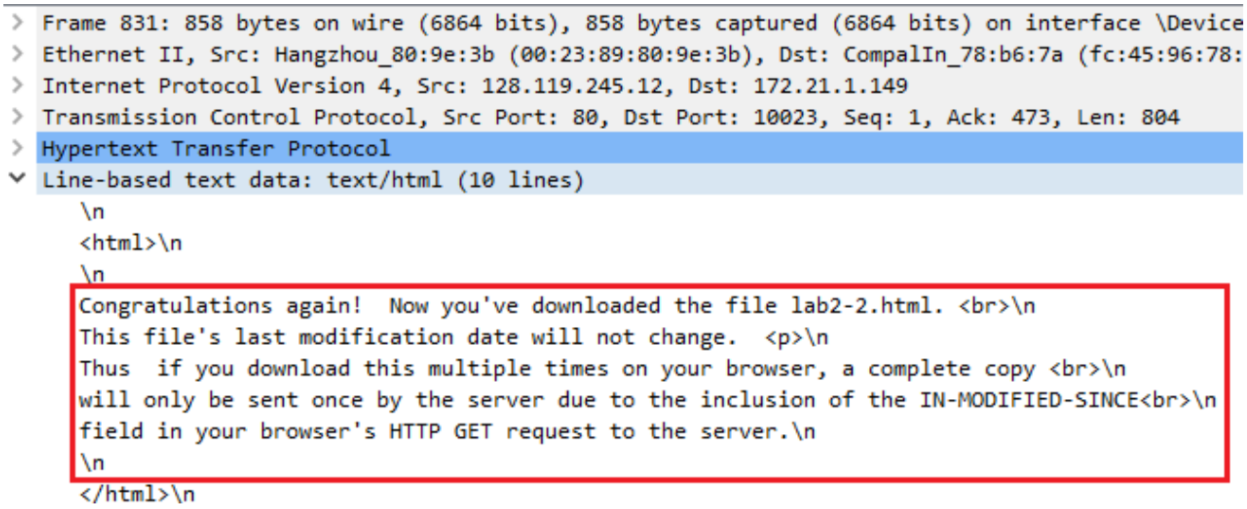
```
> Frame 831: 858 bytes on wire (6864 bits), 858 bytes captured (6864 bits) on interface \Device\NP
> Ethernet II, Src: Hangzhou_80:9e:3b (00:23:89:80:9e:3b), Dst: CompalIn_78:b6:7a (fc:45:96:78:b6:
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.21.1.149
> Transmission Control Protocol, Src Port: 80, Dst Port: 10023, Seq: 1, Ack: 473, Len: 804
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Thu, 15 Sep 2022 07:58:36 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: Thu, 15 Sep 2022 05:59:02 GMT\r\n
    ETag: "173-5e8b0f136ec82"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 371\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    Via: HTTP/1.1 forward.http.proxy:3128, HTTP/1.1 forward.http.proxy:55555\r\n
    Connection: keep-alive\r\n
    \r\n
```

Last modification date of retrieved HTML file is Thu, 15 Sep 2022

g) Did you receive the content of the file as a response?

Yes

h) Did you receive the content of the file if you requested the same HTML file?



```
> Frame 831: 858 bytes on wire (6864 bits), 858 bytes captured (6864 bits) on interface \Device
> Ethernet II, Src: Hangzhou_80:9e:3b (00:23:89:80:9e:3b), Dst: CompalIn_78:b6:7a (fc:45:96:78:
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.21.1.149
> Transmission Control Protocol, Src Port: 80, Dst Port: 10023, Seq: 1, Ack: 473, Len: 804
> 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
```

DNS

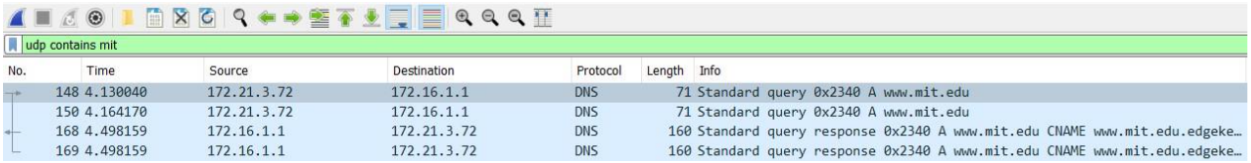
DNS

Apply nslookup on the following URL and answer the following questions related to the DNS.

URL: www.mit.edu

1. Are DNS queries sent and received using TCP or UDP?

DNS queries are send over UDP



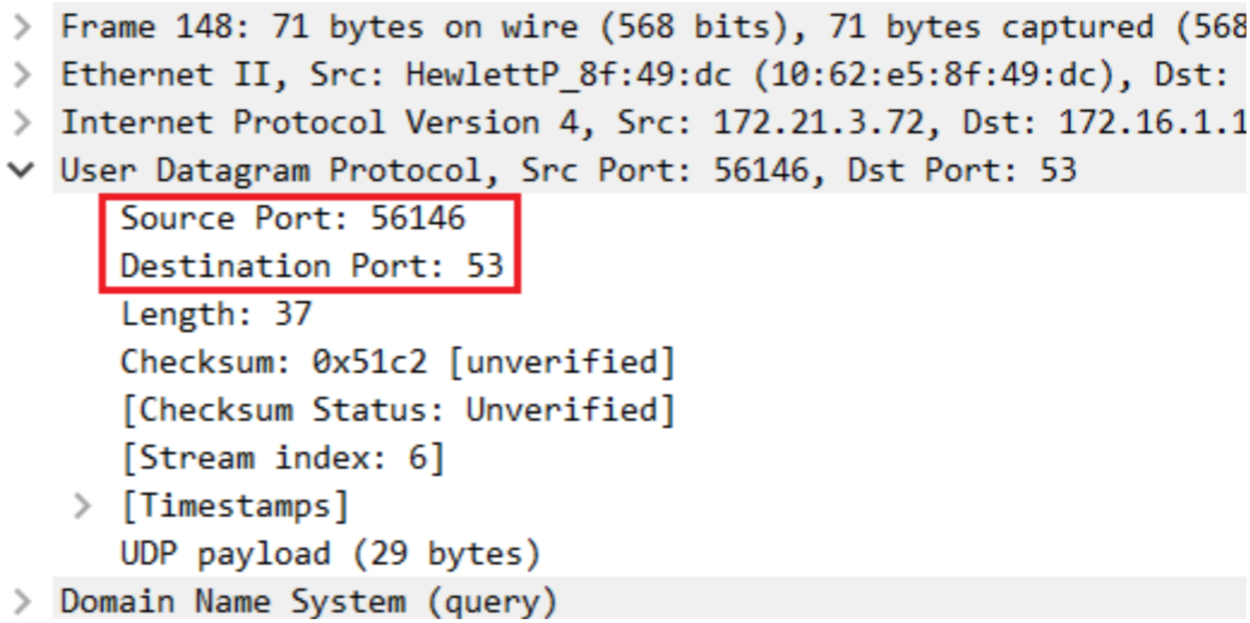
udp contains mit

No.	Time	Source	Destination	Protocol	Length	Info
148	4.130040	172.21.3.72	172.16.1.1	DNS	71	Standard query 0x2340 A www.mit.edu
150	4.164170	172.21.3.72	172.16.1.1	DNS	71	Standard query 0x2340 A www.mit.edu
168	4.498159	172.16.1.1	172.21.3.72	DNS	160	Standard query response 0x2340 A www.mit.edu CNAME www.mit.edu.edgeke…
169	4.498159	172.16.1.1	172.21.3.72	DNS	160	Standard query response 0x2340 A www.mit.edu CNAME www.mit.edu.edgeke…

2. What is the destination port of the DNS query and source port of the DNS response?

Source Port number is 56146

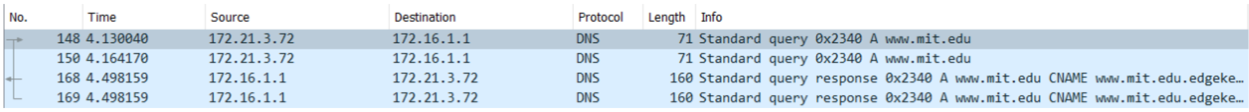
Destination Port number is 53



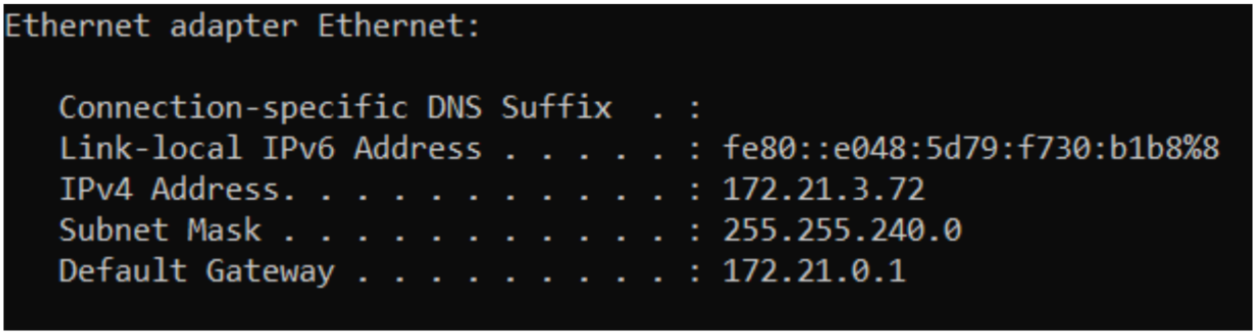
```
> Frame 148: 71 bytes on wire (568 bits), 71 bytes captured (568
> Ethernet II, Src: HewlettP_8f:49:dc (10:62:e5:8f:49:dc), Dst:
> Internet Protocol Version 4, Src: 172.21.3.72, Dst: 172.16.1.1
v User Datagram Protocol, Src Port: 56146, Dst Port: 53
    Source Port: 56146
    Destination Port: 53
    Length: 37
    Checksum: 0x51c2 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 6]
  > [Timestamps]
    UDP payload (29 bytes)
> Domain Name System (query)
```

3. What is the IP address of the DNS query message? Verify the IP address of the local

DNS server using ipconfig.



```
No.     Time       Source        Destination   Protocol  Length  Info
    148 4.130040   172.21.3.72   172.16.1.1    DNS           71 Standard query 0x2340 A www.mit.edu
    150 4.164170   172.21.3.72   172.16.1.1    DNS           71 Standard query 0x2340 A www.mit.edu
    168 4.498159   172.16.1.1    172.21.3.72   DNS          160 Standard query response 0x2340 A www.mit.edu CNAME www.mit.edu.edgeke…
    169 4.498159   172.16.1.1    172.21.3.72   DNS          160 Standard query response 0x2340 A www.mit.edu CNAME www.mit.edu.edgeke…
```

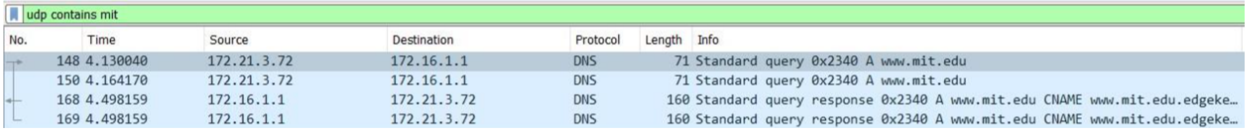


```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e048:5d79:f730:b1b8%8
   IPv4 Address. . . . . . . . . . . : 172.21.3.72
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 172.21.0.1
```

IP address of local DNS server is 172.21.3.72

4. What is the “Type” of the DNS query sent?



```
udp contains mit
No.     Time       Source        Destination   Protocol  Length  Info
    148 4.130040   172.21.3.72   172.16.1.1    DNS           71 Standard query 0x2340 A www.mit.edu
    150 4.164170   172.21.3.72   172.16.1.1    DNS           71 Standard query 0x2340 A www.mit.edu
    168 4.498159   172.16.1.1    172.21.3.72   DNS          160 Standard query response 0x2340 A www.mit.edu CNAME www.mit.edu.edgeke…
    169 4.498159   172.16.1.1    172.21.3.72   DNS          160 Standard query response 0x2340 A www.mit.edu CNAME www.mit.edu.edgeke…
```

It’s a type A Standard Query