

**Lab - 04**  
**Trace File Analysis**  
**Computer Networks**

**Program: MScIT Sem-2**  
**Group ID : 28**

**Student Name**

**Student ID**

Dev Adnani

202212012

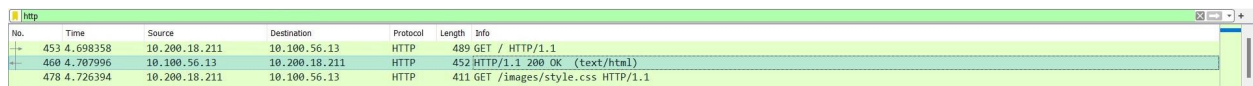
Saif Saiyed

202212083

# 202212083

## 2.2.1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

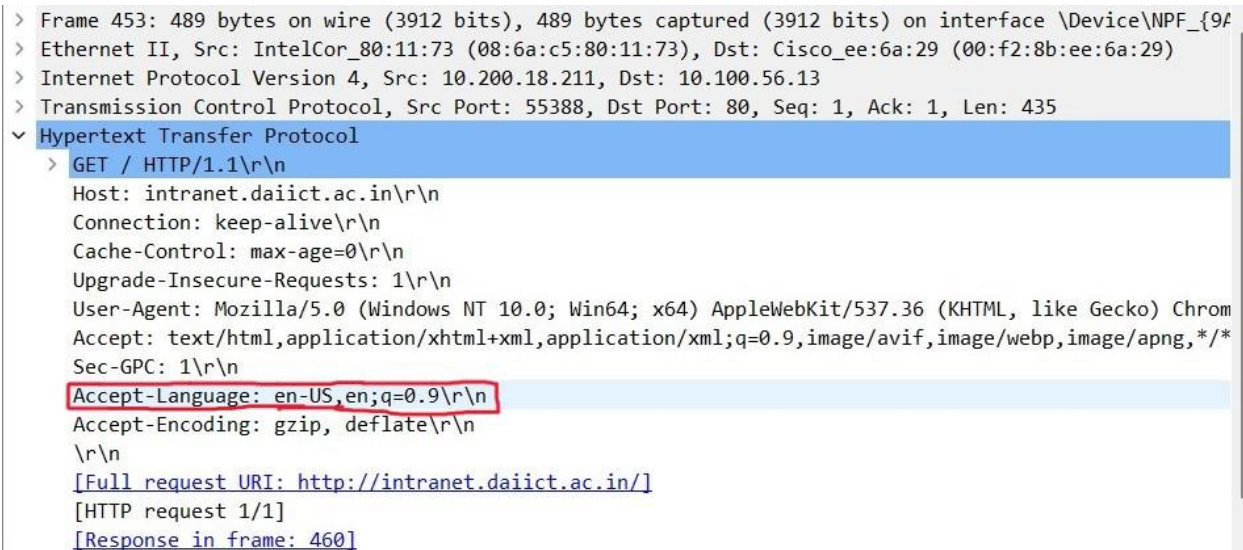
Ans : Both browser and server are running HTTP version of 1.1



No.	Time	Source	Destination	Protocol	Length	Info
453	4.698358	10.200.18.211	10.100.56.13	HTTP	489	GET / HTTP/1.1
460	4.797996	10.100.56.13	10.200.18.211	HTTP	452	HTTP/1.1 200 OK (text/html)
478	4.726394	10.200.18.211	10.100.56.13	HTTP	411	GET /images/style.css HTTP/1.1

## 2.2.2. What languages (if any) does your browser indicate that it can accept to the server?

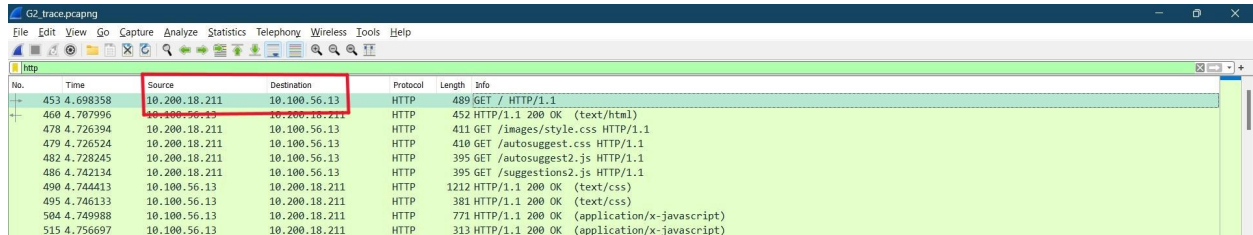
Ans : The browser indicates that it will accept en-US language to the server.



```
> Frame 453: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits) on interface \Device\NPF_{9A...}
> Ethernet II, Src: IntelCor_80:11:73 (08:6a:c5:80:11:73), Dst: Cisco_ee:6a:29 (00:f2:8b:ee:6a:29)
> Internet Protocol Version 4, Src: 10.200.18.211, Dst: 10.100.56.13
> Transmission Control Protocol, Src Port: 55388, Dst Port: 80, Seq: 1, Ack: 1, Len: 435
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: intranet.daiict.ac.in\r\n
    Connection: keep-alive\r\n
    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) Chrom
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
    Sec-GPC: 1\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    \r\n
    [Full request URI: http://intranet.daiict.ac.in/]
    [HTTP request 1/1]
    [Response in frame: 460]
```

### 2.2.3. What is the IP address of your computer?

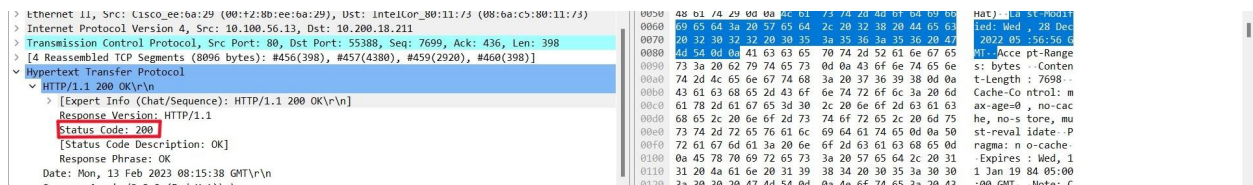
Ans : Source IP - 10.200.18.211  
Destination IP - 10.100.56.13



No.	Time	Source	Destination	Protocol	Length	Info
453	4.698358	10.200.18.211	10.100.56.13	HTTP	489	GET / HTTP/1.1
460	4.707996	10.100.56.13	10.200.18.211	HTTP	452	HTTP/1.1 200 OK (text/html)
478	4.726394	10.200.18.211	10.100.56.13	HTTP	411	GET /images/style.css HTTP/1.1
479	4.726524	10.200.18.211	10.100.56.13	HTTP	410	GET /autosuggest.css HTTP/1.1
482	4.728245	10.200.18.211	10.100.56.13	HTTP	395	GET /autosuggest2.js HTTP/1.1
486	4.742134	10.200.18.211	10.100.56.13	HTTP	395	GET /suggestions2.js HTTP/1.1
490	4.744413	10.100.56.13	10.200.18.211	HTTP	1212	HTTP/1.1 200 OK (text/css)
495	4.746133	10.100.56.13	10.200.18.211	HTTP	381	HTTP/1.1 200 OK (text/css)
504	4.749988	10.100.56.13	10.200.18.211	HTTP	771	HTTP/1.1 200 OK (application/x-javascript)
515	4.756697	10.100.56.13	10.200.18.211	HTTP	313	HTTP/1.1 200 OK (application/x-javascript)

### 2.2.4. What is the status code returned from the server to your browser?

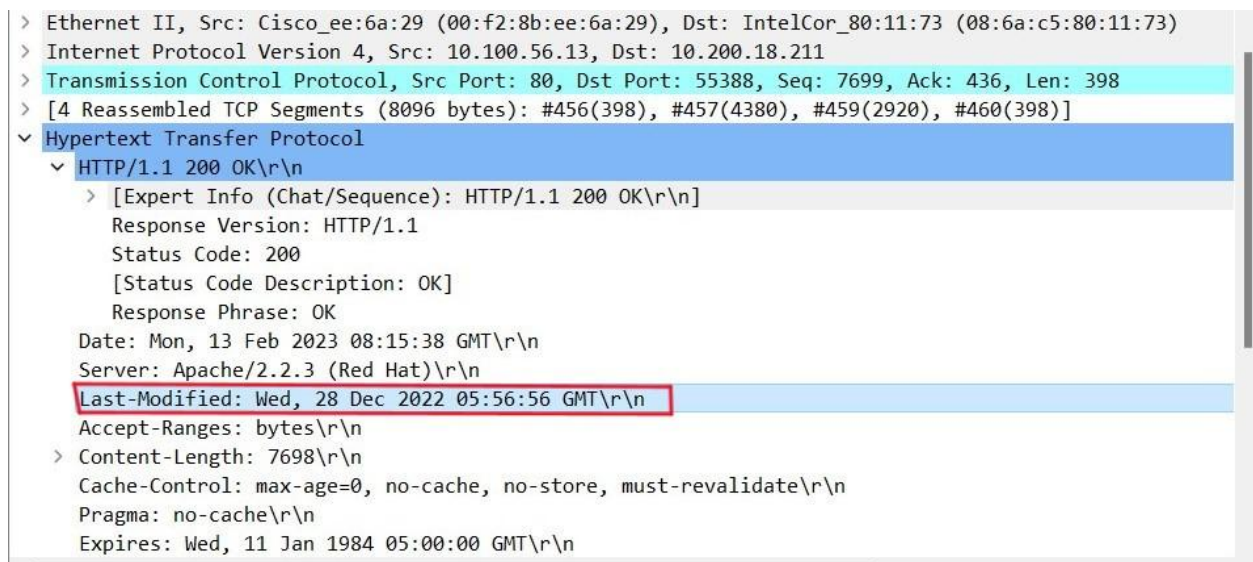
Ans : The status code returned was 200 OK.



Packet	Details
460	Ethernet II, Src: Cisco_ee:6a:29 (00:f2:8b:ee:6a:29), Dst: IntelCor_80:11:73 (08:6a:c5:80:11:73)
	Internet Protocol Version 4, Src: 10.100.56.13, Dst: 10.200.18.211
	Transmission Control Protocol, Src Port: 80, Dst Port: 55388, Seq: 7699, Ack: 436, Len: 398
	[4 Reassembled TCP Segments (8096 bytes): #456(398), #457(4380), #459(2920), #460(398)]
	Hypertext Transfer Protocol
	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: Mon, 13 Feb 2023 08:15:38 GMT\r\n

### 2.2.5. When was the HTML file that you are retrieving last modified at the server?

Ans : Last-Modified: Wed, 28 Dec 2022 05:56:56 GMT\r\n



Packet	Details
460	Ethernet II, Src: Cisco_ee:6a:29 (00:f2:8b:ee:6a:29), Dst: IntelCor_80:11:73 (08:6a:c5:80:11:73)
	Internet Protocol Version 4, Src: 10.100.56.13, Dst: 10.200.18.211
	Transmission Control Protocol, Src Port: 80, Dst Port: 55388, Seq: 7699, Ack: 436, Len: 398
	[4 Reassembled TCP Segments (8096 bytes): #456(398), #457(4380), #459(2920), #460(398)]
	Hypertext Transfer Protocol
	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: Mon, 13 Feb 2023 08:15:38 GMT\r\n
	Server: Apache/2.2.3 (Red Hat)\r\n
	Last-Modified: Wed, 28 Dec 2022 05:56:56 GMT\r\n
	Accept-Ranges: bytes\r\n
	Content-Length: 7698\r\n
	Cache-Control: max-age=0, no-cache, no-store, must-revalidate\r\n
	Pragma: no-cache\r\n
	Expires: Wed, 11 Jan 1984 05:00:00 GMT\r\n

## 2.2.6. How many bytes of content are being returned to your browser?

Ans : 7698 bytes.

```
> Internet Protocol Version 4, Src: 10.100.56.13, Dst: 10.200.18.211
> Transmission Control Protocol, Src Port: 80, Dst Port: 55388, Seq: 7699, Ack: 436, Len: 398
> [4 Reassembled TCP Segments (8096 bytes): #456(398), #457(4380), #459(2920), #460(398)]
√ Hypertext Transfer Protocol
  √ 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: Mon, 13 Feb 2023 08:15:38 GMT\r\n
      Server: Apache/2.2.3 (Red Hat)\r\n
      Last-Modified: Wed, 28 Dec 2022 05:56:56 GMT\r\n
      Accept-Ranges: bytes\r\n
      √ Content-Length: 7698\r\n
        [Content length: 7698]
      Cache-Control: max-age=0, no-cache, no-store, must-revalidate\r\n
      Pragma: no-cache\r\n
      Expires: Wed, 11 Jan 1984 05:00:00 GMT\r\n
```

**3.2.1. 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?**

Ans : No, we can't see an “IF-MODIFIED-SINCE” line in the HTTP GET.

**3.2.2. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?**

Ans : The server returned the contents of the file. We can see it through the Line Based Text Data.

The screenshot shows the Wireshark interface with a packet capture of an HTTP transaction. The packet list on the left shows a GET request (No. 453) and its response (No. 460). The packet details pane on the right shows the response structure, including the status bar '200 OK' and the 'Content-Type' header 'text/html'. The packet bytes pane on the right shows the raw data of the response, which is an HTML document. The HTML content is visible in the packet bytes pane, showing a document with a title 'AIICCT Intranet' and a body containing a script and a link to 'autosuggest2.js'.

**3.3.3. 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?**

Ans : No, cant find IF-MODIFIED-SINCE.

**3.3.4. 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.**

Ans : 200 OK and yes the server explicitly returned the contents of the file because of line based text data.



### 4.2.1. How many HTTP GET request messages did your browser send?

Ans : 36 GET requests.

The image shows a Wireshark capture of network traffic. The top pane displays a list of 36 GET requests. The middle pane shows the details of the first request (Frame 453), including the HTTP GET method, Host, and various headers. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
453	4.698358	10.200.18.211	10.100.56.13	HTTP	489	GET / HTTP/1.1
478	4.726394	10.200.18.211	10.100.56.13	HTTP	411	GET /images/style.css HTTP/1.1
479	4.726524	10.200.18.211	10.100.56.13	HTTP	410	GET /autosuggest.css HTTP/1.1
482	4.728245	10.200.18.211	10.100.56.13	HTTP	395	GET /autosuggest2.js HTTP/1.1
486	4.742134	10.200.18.211	10.100.56.13	HTTP	395	GET /suggestions2.js HTTP/1.1
1575	18.564116	10.200.18.211	10.100.56.13	HTTP	515	GET /p_majumder/ HTTP/1.1
1860	22.326157	10.200.18.211	168.235.65.201	HTTP	498	GET / HTTP/1.1
1939	23.447965	10.200.18.211	168.235.65.201	HTTP	512	GET /fire/2022/home HTTP/1.1
2023	24.253391	10.200.18.211	168.235.65.201	HTTP	803	GET /assets/application-bf308f1f0ad4fd4336fde5cb742d54500756e6cc4efa038d95d5ca6be011833.css HTTP/1.1
2024	24.253578	10.200.18.211	168.235.65.201	HTTP	787	GET /assets/application-9eab7f75266923c82793f4e6a5878932b356a1b8ce5ef065bf4532073eda328.js HTTP/1.1
2333	26.014491	10.200.18.211	168.235.65.201	HTTP	800	GET /assets/title_logos/title_left-2022.png HTTP/1.1
4771	46.411192	10.200.18.211	10.100.56.13	HTTP	463	GET / HTTP/1.1
4794	46.451419	10.200.18.211	10.100.56.13	HTTP	411	GET /images/style.css HTTP/1.1
4795	46.451561	10.200.18.211	10.100.56.13	HTTP	410	GET /autosuggest.css HTTP/1.1
4796	46.451690	10.200.18.211	10.100.56.13	HTTP	395	GET /autosuggest2.js HTTP/1.1
4797	46.451795	10.200.18.211	10.100.56.13	HTTP	395	GET /suggestions2.js HTTP/1.1
5533	53.805941	10.200.18.211	10.100.56.13	HTTP	515	GET /p_majumder/ HTTP/1.1
6092	57.703079	10.200.18.211	168.235.65.201	HTTP	497	GET / HTTP/1.1
6172	58.252876	10.200.18.211	168.235.65.201	HTTP	815	GET / HTTP/1.1

### 4.2.2. How many data-containing TCP segments were needed to carry the single HTTP response?

Ans : 4 data-containing TCP segments were needed to carry the single HTTP response.

The image shows a Wireshark capture of network traffic. The top pane displays a list of 4 data-containing TCP segments. The middle pane shows the details of the first segment (Frame 453), including the TCP segment data and the HTTP response. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
453	4.698358	10.200.18.211	10.100.56.13	HTTP	489	GET / HTTP/1.1
478	4.726394	10.200.18.211	10.100.56.13	HTTP	411	GET /images/style.css HTTP/1.1
479	4.726524	10.200.18.211	10.100.56.13	HTTP	410	GET /autosuggest.css HTTP/1.1
482	4.728245	10.200.18.211	10.100.56.13	HTTP	395	GET /autosuggest2.js HTTP/1.1
486	4.742134	10.200.18.211	10.100.56.13	HTTP	395	GET /suggestions2.js HTTP/1.1
1575	18.564116	10.200.18.211	10.100.56.13	HTTP	515	GET /p_majumder/ HTTP/1.1
1860	22.326157	10.200.18.211	168.235.65.201	HTTP	498	GET / HTTP/1.1
1939	23.447965	10.200.18.211	168.235.65.201	HTTP	512	GET /fire/2022/home HTTP/1.1
2023	24.253391	10.200.18.211	168.235.65.201	HTTP	803	GET /assets/application-bf308f1f0ad4fd4336fde5cb742d54500756e6cc4efa038d95d5ca6be011833.css HTTP/1.1
2024	24.253578	10.200.18.211	168.235.65.201	HTTP	787	GET /assets/application-9eab7f75266923c82793f4e6a5878932b356a1b8ce5ef065bf4532073eda328.js HTTP/1.1
2333	26.014491	10.200.18.211	168.235.65.201	HTTP	800	GET /assets/title_logos/title_left-2022.png HTTP/1.1
4771	46.411192	10.200.18.211	10.100.56.13	HTTP	463	GET / HTTP/1.1
4794	46.451419	10.200.18.211	10.100.56.13	HTTP	411	GET /images/style.css HTTP/1.1
4795	46.451561	10.200.18.211	10.100.56.13	HTTP	410	GET /autosuggest.css HTTP/1.1
4796	46.451690	10.200.18.211	10.100.56.13	HTTP	395	GET /autosuggest2.js HTTP/1.1
4797	46.451795	10.200.18.211	10.100.56.13	HTTP	395	GET /suggestions2.js HTTP/1.1
5533	53.805941	10.200.18.211	10.100.56.13	HTTP	515	GET /p_majumder/ HTTP/1.1
6092	57.703079	10.200.18.211	168.235.65.201	HTTP	497	GET / HTTP/1.1
6172	58.252876	10.200.18.211	168.235.65.201	HTTP	815	GET / HTTP/1.1

### 4.2.3. What is the status code and phrase associated with the response to the HTTP GET request?

Ans : The status code returned was 200 OK.

The image shows a Wireshark capture of network traffic. The top pane displays a list of 4 data-containing TCP segments. The middle pane shows the details of the first segment (Frame 453), including the TCP segment data and the HTTP response. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
453	4.698358	10.200.18.211	10.100.56.13	HTTP	489	GET / HTTP/1.1
478	4.726394	10.200.18.211	10.100.56.13	HTTP	411	GET /images/style.css HTTP/1.1
479	4.726524	10.200.18.211	10.100.56.13	HTTP	410	GET /autosuggest.css HTTP/1.1
482	4.728245	10.200.18.211	10.100.56.13	HTTP	395	GET /autosuggest2.js HTTP/1.1
486	4.742134	10.200.18.211	10.100.56.13	HTTP	395	GET /suggestions2.js HTTP/1.1
1575	18.564116	10.200.18.211	10.100.56.13	HTTP	515	GET /p_majumder/ HTTP/1.1
1860	22.326157	10.200.18.211	168.235.65.201	HTTP	498	GET / HTTP/1.1
1939	23.447965	10.200.18.211	168.235.65.201	HTTP	512	GET /fire/2022/home HTTP/1.1
2023	24.253391	10.200.18.211	168.235.65.201	HTTP	803	GET /assets/application-bf308f1f0ad4fd4336fde5cb742d54500756e6cc4efa038d95d5ca6be011833.css HTTP/1.1
2024	24.253578	10.200.18.211	168.235.65.201	HTTP	787	GET /assets/application-9eab7f75266923c82793f4e6a5878932b356a1b8ce5ef065bf4532073eda328.js HTTP/1.1
2333	26.014491	10.200.18.211	168.235.65.201	HTTP	800	GET /assets/title_logos/title_left-2022.png HTTP/1.1
4771	46.411192	10.200.18.211	10.100.56.13	HTTP	463	GET / HTTP/1.1
4794	46.451419	10.200.18.211	10.100.56.13	HTTP	411	GET /images/style.css HTTP/1.1
4795	46.451561	10.200.18.211	10.100.56.13	HTTP	410	GET /autosuggest.css HTTP/1.1
4796	46.451690	10.200.18.211	10.100.56.13	HTTP	395	GET /autosuggest2.js HTTP/1.1
4797	46.451795	10.200.18.211	10.100.56.13	HTTP	395	GET /suggestions2.js HTTP/1.1
5533	53.805941	10.200.18.211	10.100.56.13	HTTP	515	GET /p_majumder/ HTTP/1.1
6092	57.703079	10.200.18.211	168.235.65.201	HTTP	497	GET / HTTP/1.1
6172	58.252876	10.200.18.211	168.235.65.201	HTTP	815	GET / HTTP/1.1

### 5.2.1. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

Ans : 36 GET requests. They were sent to 10.100.56.13, 168.235.65.201.

### 5.2.2. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two websites in parallel? Explain.

Ans : No, the browser didn't download the two images serially.

The image shows a Wireshark packet capture of an HTTP session. The top pane displays a list of 36 GET requests. The middle pane shows the details of the selected packet (No. 411), which is a GET request for /images/style.css. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
453	4.698358	10.200.18.211	10.100.56.13	HTTP	489	GET / HTTP/1.1
478	4.726394	10.200.18.211	10.100.56.13	HTTP	411	GET /images/style.css HTTP/1.1
479	4.726524	10.200.18.211	10.100.56.13	HTTP	410	GET /autosuggest.css HTTP/1.1
482	4.728245	10.200.18.211	10.100.56.13	HTTP	395	GET /autosuggest2.js HTTP/1.1
486	4.742134	10.200.18.211	10.100.56.13	HTTP	395	GET /suggestions2.js HTTP/1.1
1575	18.564116	10.200.18.211	10.100.56.13	HTTP	515	GET /~p_majumder/ HTTP/1.1
1860	22.326157	10.200.18.211	168.235.65.201	HTTP	498	GET / HTTP/1.1
1939	23.447965	10.200.18.211	168.235.65.201	HTTP	512	GET /fire/2022/home HTTP/1.1
2023	24.253391	10.200.18.211	168.235.65.201	HTTP	803	GET /assets/application-bf308f1f0ad4f443336fde5cb742d54500756e6ccdefa038d95d5ca0be011833.css HTTP/1.1
2024	24.253578	10.200.18.211	168.235.65.201	HTTP	787	GET /assets/application-9eab7f75266923c82793f4e66a5878932b356a1b8ce5ef065bf4532073eda328.js HTTP/1.1
2333	26.014491	10.200.18.211	168.235.65.201	HTTP	800	GET /assets/title_logos/title_left-2022.png HTTP/1.1
4771	46.411192	10.200.18.211	10.100.56.13	HTTP	463	GET / HTTP/1.1
4794	46.451419	10.200.18.211	10.100.56.13	HTTP	411	GET /images/style.css HTTP/1.1
4795	46.451561	10.200.18.211	10.100.56.13	HTTP	410	GET /autosuggest.css HTTP/1.1
4796	46.451690	10.200.18.211	10.100.56.13	HTTP	395	GET /autosuggest2.js HTTP/1.1
4797	46.451795	10.200.18.211	10.100.56.13	HTTP	395	GET /suggestions2.js HTTP/1.1
5533	53.805041	10.200.18.211	10.100.56.13	HTTP	515	GET /~p_majumder/ HTTP/1.1
6092	57.703079	10.200.18.211	168.235.65.201	HTTP	497	GET / HTTP/1.1
6172	58.252876	10.200.18.211	168.235.65.201	HTTP	815	GET / HTTP/1.1

Frame 478: 411 bytes on wire (3288 bits), 411 bytes captured (3288 bits) on interface \Device\NPF...  
Ethernet II, Src: IntelCor\_80:11:73:08:6a:c5:80:11:73, Dst: Cisco\_ee:6a:29:00:f2:8b:ee:6a:29  
Internet Protocol Version 4, Src: 10.200.18.211, Dst: 10.100.56.13  
Transmission Control Protocol, Src Port: 55389, Dst Port: 80, Seq: 1, Ack: 1, Len: 357  
Hypertext Transfer Protocol  
GET /images/style.css HTTP/1.1  
[Expert Info (Chat/Sequence): GET /images/style.css HTTP/1.1  
Request Method: GET  
Request URI: /images/style.css  
Request Version: HTTP/1.1  
Host: intranet.daiict.ac.in  
Connection: keep-alive  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36  
Accept: text/css,\*/\*;q=0.1  
Sec-GPC: 1  
Accept-Language: en-US,en;q=0.9  
Referer: http://intranet.daiict.ac.in/  
Accept-Encoding: gzip, deflate  
\\n\\n

0030 02 01 61 8b 00 00 47 45 54 20 f4 69 6d 61 67 65 - a GE T /image  
0040 72 7f 73 74 79 6c 65 2c 63 73 73 20 48 54 54 50 - /style.css HTTP  
0050 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 69 6e 74 72 - /1.1-Host: intr  
0060 61 6e 65 74 2e 64 61 69 69 63 74 2e 61 63 2e 69 - anet.dai ict.ac.i  
0070 6e 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b - n-Connec tion: k  
0080 65 65 70 2d 61 6c 69 76 65 0d 0a 55 73 65 72 2d - eep-alliv e-User-  
0090 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6e 61 2f 35 - Agent: M ozilla/5  
00a0 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 - .0 (Wind ows NT 1  
00b0 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 34 29 - 0.0; Win 64; x64)  
00c0 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 33 37 - AppleWe bKit/537  
00d0 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 66 65 - .36 (KHT ML, like  
00e0 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 2f 31 - Gecko) Chrome/1  
00f0 31 30 2e 30 2e 30 2e 30 20 53 61 66 61 72 69 2f - 10.0.0.0 Safari/  
0100 35 33 37 2e 33 36 0d 0a 41 63 63 65 70 74 3a 20 - 537.36- Accept:  
0110 74 65 78 74 2f 63 73 73 2c 2a 2f 2a 3b 71 3d 30 - text/css ,/\*;q=0  
0120 2e 31 0d 0a 53 65 63 2d 47 50 43 3a 20 31 0d 0a - .1-Sec- GPC: 1-  
0130 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a - Accept-L anguage:  
0140 20 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e 39 0d - en-US,e n;q=0.9-  
0150 0a 52 65 66 65 72 65 72 3a 20 68 74 74 70 3a 2f - .Referer : http/  
0160 2f 69 6e 74 72 61 6e 65 74 2e 64 61 69 69 63 74 - /intran e .daiict  
0170 2e 61 63 2e 69 6e 2f 0d 0a 41 63 63 65 70 74 2d - .ac.in/. -Accept-

## 6.2.1. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

Ans : Status Code - 200; Phrase - OK.

```
> Ethernet II, Src: Cisco_ee:6a:29 (00:f2:8b:ee:6a:29), Dst: IntelCor_80:11:73 (08:6a:c5:80:11:73)
> Internet Protocol Version 4, Src: 10.100.56.13, Dst: 10.200.18.211
> Transmission Control Protocol, Src Port: 80, Dst Port: 55388, Seq: 7699, Ack: 436, Len: 398
> [4 Reassembled TCP Segments (8096 bytes): #456(398), #457(4380), #459(2920), #460(398)]
  Hypertext Transfer Protocol
    [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: Mon, 13 Feb 2023 08:15:38 GMT\r\n
```

## 6.2.2. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

Ans : Nothing is included in the HTTP GET message for the second time. Just the referer is changed to http://intranet.daiict.ac.in.

```
G2_trace.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request.method == "GET"

No. Time Source Destination Protocol Length Info
453 4.698358 10.200.18.211 10.100.56.13 HTTP 489 GET / HTTP/1.1
478 4.726394 10.200.18.211 10.100.56.13 HTTP 411 GET /images/style.css HTTP/1.1
479 4.726524 10.200.18.211 10.100.56.13 HTTP 410 GET /autosuggest.css HTTP/1.1
482 4.728245 10.200.18.211 10.100.56.13 HTTP 395 GET /autosuggest2.js HTTP/1.1
486 4.742134 10.200.18.211 10.100.56.13 HTTP 395 GET /suggestions2.js HTTP/1.1
1575 18.564116 10.200.18.211 10.100.56.13 HTTP 515 GET /p_majumder/ HTTP/1.1
1860 22.326157 10.200.18.211 168.235.65.201 HTTP 498 GET / HTTP/1.1
1939 23.447965 10.200.18.211 168.235.65.201 HTTP 512 GET /fire/2022/home HTTP/1.1
2023 24.25391 10.200.18.211 168.235.65.201 HTTP 803 GET /assets/application-bf308f1f0ad4fd43336fde5cb742d54500756e6cc4efa038d95d5ca6be011833.css HTTP/1.1
2024 24.253578 10.200.18.211 168.235.65.201 HTTP 787 GET /assets/application-9eab7f75266923c82793f4e66a5878932b356a1b8ce5ef065bf4532073eda328.js HTTP/1.1
2333 26.014491 10.200.18.211 168.235.65.201 HTTP 800 GET /assets/title_logos/title_left-2022.png HTTP/1.1
4771 46.411192 10.200.18.211 10.100.56.13 HTTP 463 GET / HTTP/1.1
4794 46.451419 10.200.18.211 10.100.56.13 HTTP 411 GET /images/style.css HTTP/1.1
4795 46.451561 10.200.18.211 10.100.56.13 HTTP 410 GET /autosuggest.css HTTP/1.1
4796 46.451690 10.200.18.211 10.100.56.13 HTTP 395 GET /autosuggest2.js HTTP/1.1
4797 46.451795 10.200.18.211 10.100.56.13 HTTP 395 GET /suggestions2.js HTTP/1.1
5533 53.805041 10.200.18.211 10.100.56.13 HTTP 515 GET /p_majumder/ HTTP/1.1
6092 57.703079 10.200.18.211 168.235.65.201 HTTP 497 GET / HTTP/1.1
6172 58.252876 10.200.18.211 168.235.65.201 HTTP 815 GET / HTTP/1.1

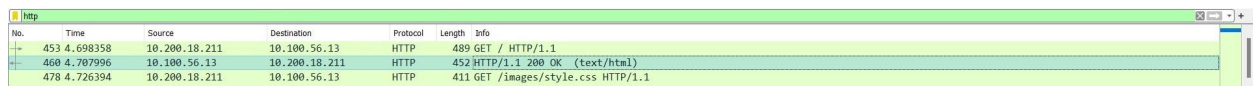
> Frame 478: 411 bytes on wire (3288 bits), 411 bytes captured (3288 bits) on interface \Device\NPF_{09...}
> Ethernet II, Src: IntelCor_80:11:73 (08:6a:c5:80:11:73), Dst: Cisco_ee:6a:29 (00:f2:8b:ee:6a:29)
> Internet Protocol Version 4, Src: 10.200.18.211, Dst: 10.100.56.13
> Transmission Control Protocol, Src Port: 55389, Dst Port: 80, Seq: 1, Ack: 1, Len: 357
  Hypertext Transfer Protocol
    GET /images/style.css HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /images/style.css HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /images/style.css
      Request Version: HTTP/1.1
      Host: intranet.daiict.ac.in\r\n
      Connection: keep-alive\r\n
      User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36\r\n
      Accept: text/css,*/*;q=0.9\r\n
      Accept-Language: en-US,en;q=0.9\r\n
      Referer: http://intranet.daiict.ac.in/\r\n
      Accept-Encoding: gzip, deflate\r\n
      \r\n
```



# 202212012

## 2.2.1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

Ans : Both browser and server are running HTTP version of 1.1

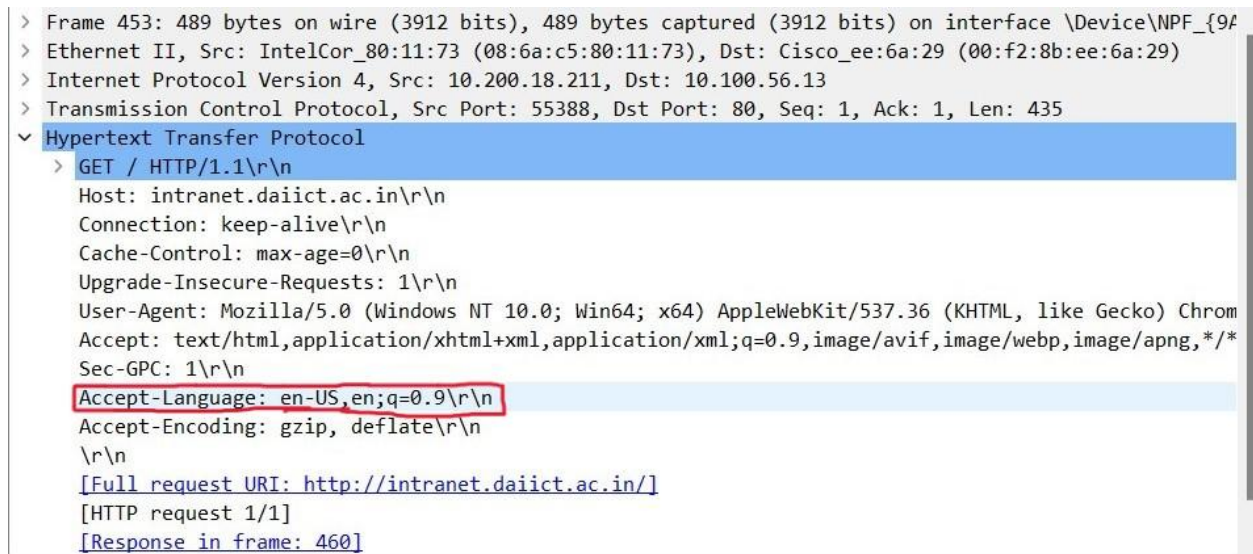


A screenshot of a Wireshark packet capture window. The top bar shows 'http'. The packet list on the left shows three packets: 453 (GET / HTTP/1.1), 460 (HTTP/1.1 200 OK (text/html)), and 478 (GET /images/style.css HTTP/1.1). The packet details pane on the right shows the selected packet (460) with its structure: HTTP, 452, HTTP/1.1 200 OK (text/html).

No.	Time	Source	Destination	Protocol	Length	Info
453	4.698358	10.200.18.211	10.100.56.13	HTTP	489	GET / HTTP/1.1
460	4.797996	10.100.56.13	10.200.18.211	HTTP	452	HTTP/1.1 200 OK (text/html)
478	4.726394	10.200.18.211	10.100.56.13	HTTP	411	GET /images/style.css HTTP/1.1

## 2.2.2. What languages (if any) does your browser indicate that it can accept to the server?

Ans : The browser indicates that it will accept en-US language to the server.



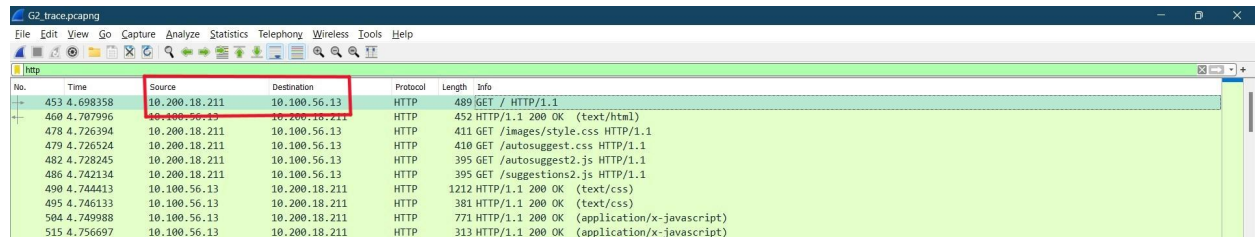
A screenshot of a Wireshark packet capture window showing the details of a Hypertext Transfer Protocol (HTTP) request. The packet list on the left shows three packets: 453 (GET / HTTP/1.1), 460 (HTTP/1.1 200 OK (text/html)), and 478 (GET /images/style.css HTTP/1.1). The packet details pane on the right shows the selected packet (460) with its structure: Hypertext Transfer Protocol, GET / HTTP/1.1\r\n, Host: intranet.daiict.ac.in\r\n, Connection: keep-alive\r\n, 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) Chrom, Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/,\*, Accept-Encoding: gzip, deflate\r\n, \r\n, [Full request URI: http://intranet.daiict.ac.in/], [HTTP request 1/1], [Response in frame: 460].

No.	Time	Source	Destination	Protocol	Length	Info
453	4.698358	10.200.18.211	10.100.56.13	HTTP	489	GET / HTTP/1.1
460	4.797996	10.100.56.13	10.200.18.211	HTTP	452	HTTP/1.1 200 OK (text/html)
478	4.726394	10.200.18.211	10.100.56.13	HTTP	411	GET /images/style.css HTTP/1.1

```
> Frame 453: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits) on interface \Device\NPF_{9A...}
> Ethernet II, Src: IntelCor_80:11:73 (08:6a:c5:80:11:73), Dst: Cisco_ee:6a:29 (00:f2:8b:ee:6a:29)
> Internet Protocol Version 4, Src: 10.200.18.211, Dst: 10.100.56.13
> Transmission Control Protocol, Src Port: 55388, Dst Port: 80, Seq: 1, Ack: 1, Len: 435
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: intranet.daiict.ac.in\r\n
    Connection: keep-alive\r\n
    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) Chrom
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
    Sec-GPC: 1\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    \r\n
    [Full request URI: http://intranet.daiict.ac.in/]
    [HTTP request 1/1]
    [Response in frame: 460]
```

### 2.2.3. What is the IP address of your computer?

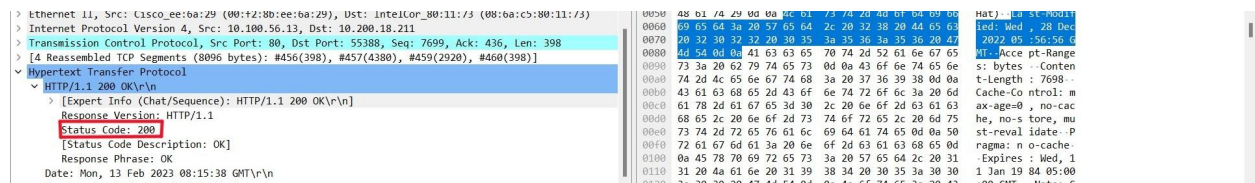
Ans : Source IP - 10.200.18.211  
Destination IP - 10.100.56.13



No.	Time	Source	Destination	Protocol	Length	Info
453	4.698358	10.200.18.211	10.100.56.13	HTTP	489	GET / HTTP/1.1
460	4.707996	10.100.56.13	10.200.18.211	HTTP	452	HTTP/1.1 200 OK (text/html)
478	4.726394	10.200.18.211	10.100.56.13	HTTP	411	GET /images/style.css HTTP/1.1
479	4.726524	10.200.18.211	10.100.56.13	HTTP	410	GET /autosuggest.css HTTP/1.1
482	4.728245	10.200.18.211	10.100.56.13	HTTP	395	GET /autosuggest2.js HTTP/1.1
486	4.742134	10.200.18.211	10.100.56.13	HTTP	395	GET /suggestions2.js HTTP/1.1
490	4.744413	10.100.56.13	10.200.18.211	HTTP	1212	HTTP/1.1 200 OK (text/css)
495	4.746133	10.100.56.13	10.200.18.211	HTTP	381	HTTP/1.1 200 OK (text/css)
504	4.749988	10.100.56.13	10.200.18.211	HTTP	771	HTTP/1.1 200 OK (application/x-javascript)
515	4.756697	10.100.56.13	10.200.18.211	HTTP	313	HTTP/1.1 200 OK (application/x-javascript)

### 2.2.4. What is the status code returned from the server to your browser?

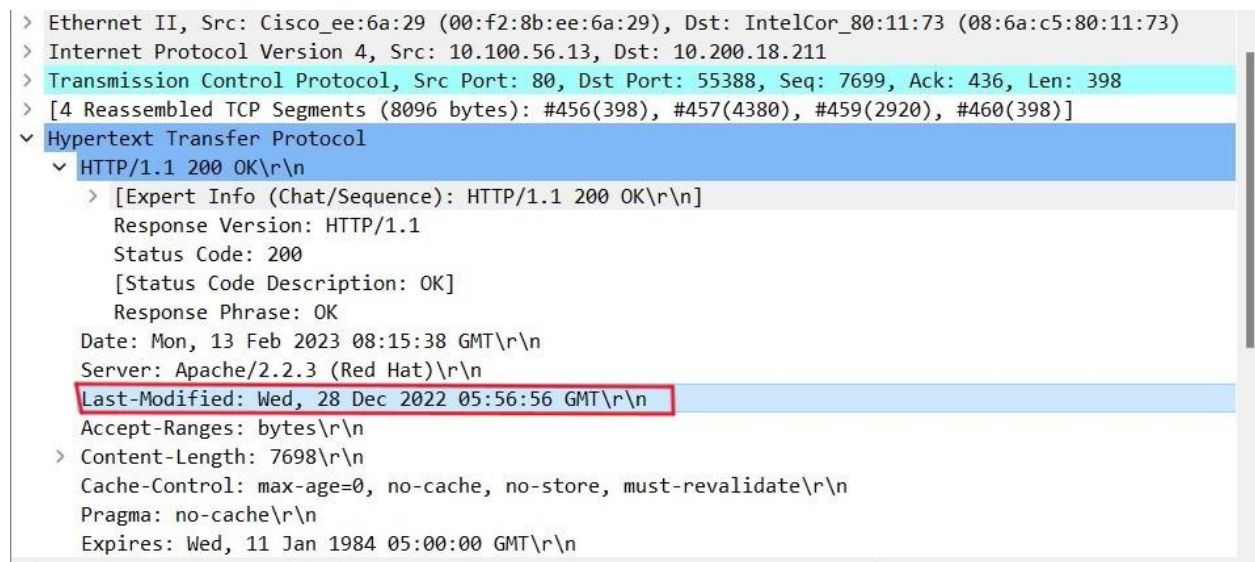
Ans : The status code returned was 200 OK.



Packet	Details
460	Ethernet II, Src: Cisco_ee:6a:29 (00:f2:8b:ee:6a:29), Dst: IntelCor_80:11:73 (08:6a:c5:80:11:73)
	Internet Protocol Version 4, Src: 10.100.56.13, Dst: 10.200.18.211
	Transmission Control Protocol, Src Port: 80, Dst Port: 55388, Seq: 7699, Ack: 436, Len: 398
	[4 Reassembled TCP Segments (8096 bytes): #456(398), #457(4380), #459(2920), #460(398)]
	Hypertext Transfer Protocol
	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: Mon, 13 Feb 2023 08:15:38 GMT\r\n

### 2.2.5. When was the HTML file that you are retrieving last modified at the server?

Ans : Last-Modified: Wed, 28 Dec 2022 05:56:56 GMT\r\n



Packet	Details
460	Ethernet II, Src: Cisco_ee:6a:29 (00:f2:8b:ee:6a:29), Dst: IntelCor_80:11:73 (08:6a:c5:80:11:73)
	Internet Protocol Version 4, Src: 10.100.56.13, Dst: 10.200.18.211
	Transmission Control Protocol, Src Port: 80, Dst Port: 55388, Seq: 7699, Ack: 436, Len: 398
	[4 Reassembled TCP Segments (8096 bytes): #456(398), #457(4380), #459(2920), #460(398)]
	Hypertext Transfer Protocol
	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: Mon, 13 Feb 2023 08:15:38 GMT\r\n
	Server: Apache/2.2.3 (Red Hat)\r\n
	Last-Modified: Wed, 28 Dec 2022 05:56:56 GMT\r\n
	Accept-Ranges: bytes\r\n
	Content-Length: 7698\r\n
	Cache-Control: max-age=0, no-cache, no-store, must-revalidate\r\n
	Pragma: no-cache\r\n
	Expires: Wed, 11 Jan 1984 05:00:00 GMT\r\n

## 2.2.6. How many bytes of content are being returned to your browser?

Ans : 7698 bytes.

```
> Internet Protocol Version 4, Src: 10.100.56.13, Dst: 10.200.18.211
> Transmission Control Protocol, Src Port: 80, Dst Port: 55388, Seq: 7699, Ack: 436, Len: 398
> [4 Reassembled TCP Segments (8096 bytes): #456(398), #457(4380), #459(2920), #460(398)]
√ Hypertext Transfer Protocol
  √ 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: Mon, 13 Feb 2023 08:15:38 GMT\r\n
      Server: Apache/2.2.3 (Red Hat)\r\n
      Last-Modified: Wed, 28 Dec 2022 05:56:56 GMT\r\n
      Accept-Ranges: bytes\r\n
      √ Content-Length: 7698\r\n
        [Content length: 7698]
      Cache-Control: max-age=0, no-cache, no-store, must-revalidate\r\n
      Pragma: no-cache\r\n
      Expires: Wed, 11 Jan 1984 05:00:00 GMT\r\n
```

**3.2.1. 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?**

Ans : No, we can't see an “IF-MODIFIED-SINCE” line in the HTTP GET.

**3.2.2. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?**

Ans : The server returned the contents of the file. We can see it through the Line Based Text Data.

The screenshot shows the Wireshark interface with a packet capture of an HTTP transaction. The packet list on the left shows a GET request (No. 453) and its response (No. 460). The packet details pane on the left shows the structure of the response, including the status bar (200 OK) and the content type (text/html). The packet bytes pane on the right shows the raw data of the response, which is the HTML content of the file.

No.	Time	Source	Destination	Protocol	Length	Info
453	4.698358	10.200.18.211	10.100.56.13	HTTP	489	GET / HTTP/1.1
460	4.707996	10.100.56.13	10.200.18.211	HTTP	452	HTTP/1.1 200 OK (text/html)

Line-based text data: text/html (146 lines)

```
<html xmlns="http://www.w3.org/1999/xhtml">\n<head>\n<meta http-equiv="content-type" content="text/html; charset=iso-8859-1" />\n<link rel="stylesheet" href="images/style.css" type="text/css" />\n<title>OAIIC Intranet</title>\n<script type="text/javascript" src="autosuggest2.js"></script>\n<script type="text/javascript" src="suggestions2.js"></script>\n<link rel="stylesheet" type="text/css" href="autosuggest.css" />\n<script type="text/javascript">\n  window.onload = function () {\n    var oTextbox = new AutoSuggestControl(document.getElementById("txt1"), new StateS\n  }\n</script>\n</head>\n<body>\n<div class="content">\n<div class="header">\n  <a href="campus.html" target="_blank"><img src="images/bg1.jpg" width="780" height="24
```

**3.3.3. 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?**

Ans : No, cant find IF-MODIFIED-SINCE.

**3.3.4. 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.**

Ans : 200 OK and yes the server explicitly returned the contents of the file because of line based text data.



### 4.2.1. How many HTTP GET request messages did your browser send?

Ans : 36 GET requests.

The image shows a Wireshark capture of network traffic. The top pane displays a list of 36 GET requests. The middle pane shows the details of the first GET request (Frame 453), including the HTTP request line, headers, and body. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Frame 453: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits) on interface \Device\NPF... (92...)

Ethernet II, Src: IntelCor, 80:11:73 (08:6a:c5:80:11:73), Dst: Cisco\_ee:6a:29 (00:f2:8b:ee:6a:29)

Internet Protocol Version 4, Src: 10.200.18.211, Dst: 10.100.56.13

Transmission Control Protocol, Src Port: 55388, Dst Port: 80, Seq: 1, Ack: 1, Len: 435

Hypertext Transfer Protocol

GET / HTTP/1.1

Request Method: GET

Request URI: /

Request Version: HTTP/1.1

Host: intranet.daiict.ac.in

Connection: keep-alive

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.0.0 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8

Accept-Language: en-US,en;q=0.9

Accept-Encoding: gzip, deflate

### 4.2.2. How many data-containing TCP segments were needed to carry the single HTTP response?

Ans : 4 data-containing TCP segments were needed to carry the single HTTP response.

The image shows a Wireshark capture of network traffic. The top pane displays a list of 4 data-containing TCP segments. The middle pane shows the details of the first TCP segment (Frame 454), including the TCP header, payload, and body. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Frame 454: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits) on interface \Device\NPF... (92...)

Ethernet II, Src: IntelCor, 80:11:73 (08:6a:c5:80:11:73), Dst: Cisco\_ee:6a:29 (00:f2:8b:ee:6a:29)

Internet Protocol Version 4, Src: 10.100.56.13, Dst: 10.200.18.211

Transmission Control Protocol, Src Port: 80, Dst Port: 55388, Seq: 7699, Ack: 436, Len: 398

[4 Reassembled TCP Segments (8096 bytes): #456(398), #457(4380), #459(2920), #460(398)]

Hypertext Transfer Protocol

HTTP/1.1 200 OK

Response Version: HTTP/1.1

Status Code: 200

Status Code Description: OK

Response Phrases: OK

Date: Mon, 13 Feb 2023 08:15:38 GMT

### 4.2.3. What is the status code and phrase associated with the response to the HTTP GET request?

Ans : The status code returned was 200 OK.

The image shows a Wireshark capture of network traffic. The top pane displays a list of 4 data-containing TCP segments. The middle pane shows the details of the first TCP segment (Frame 454), including the TCP header, payload, and body. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Frame 454: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits) on interface \Device\NPF... (92...)

Ethernet II, Src: IntelCor, 80:11:73 (08:6a:c5:80:11:73), Dst: Cisco\_ee:6a:29 (00:f2:8b:ee:6a:29)

Internet Protocol Version 4, Src: 10.100.56.13, Dst: 10.200.18.211

Transmission Control Protocol, Src Port: 80, Dst Port: 55388, Seq: 7699, Ack: 436, Len: 398

[4 Reassembled TCP Segments (8096 bytes): #456(398), #457(4380), #459(2920), #460(398)]

Hypertext Transfer Protocol

HTTP/1.1 200 OK

Response Version: HTTP/1.1

Status Code: 200

Status Code Description: OK

Response Phrases: OK

Date: Mon, 13 Feb 2023 08:15:38 GMT

### 5.2.1. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

Ans : 36 GET requests. They were sent to 10.100.56.13, 168.235.65.201.

### 5.2.2. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two websites in parallel? Explain.

Ans : No, the browser didn't download the two images serially.

The image shows a Wireshark packet capture of an HTTP session. The top pane displays a list of 36 GET requests. The middle pane shows the details of the selected packet (No. 411), which is a GET request for /images/style.css. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
453	4.698358	10.200.18.211	10.100.56.13	HTTP	489	GET / HTTP/1.1
478	4.726394	10.200.18.211	10.100.56.13	HTTP	411	GET /images/style.css HTTP/1.1
479	4.726524	10.200.18.211	10.100.56.13	HTTP	410	GET /autosuggest.css HTTP/1.1
482	4.728245	10.200.18.211	10.100.56.13	HTTP	395	GET /autosuggest2.js HTTP/1.1
486	4.742134	10.200.18.211	10.100.56.13	HTTP	395	GET /suggestions2.js HTTP/1.1
1575	18.564116	10.200.18.211	10.100.56.13	HTTP	515	GET /~p_majumder/ HTTP/1.1
1860	22.326157	10.200.18.211	168.235.65.201	HTTP	498	GET / HTTP/1.1
1939	23.447965	10.200.18.211	168.235.65.201	HTTP	512	GET /fire/2022/home HTTP/1.1
2023	24.253391	10.200.18.211	168.235.65.201	HTTP	803	GET /assets/application-bf308f1f0ad4f443336fde5cb742d54500756e6ccdefa038d95d5ca0be011833.css HTTP/1.1
2024	24.253578	10.200.18.211	168.235.65.201	HTTP	787	GET /assets/application-9eab7f75266923c82793f4e66a5878932b356a1b8ce5ef065bf4532073eda328.js HTTP/1.1
2333	26.014491	10.200.18.211	168.235.65.201	HTTP	800	GET /assets/title_logos/title_left-2022.png HTTP/1.1
4771	46.411192	10.200.18.211	10.100.56.13	HTTP	463	GET / HTTP/1.1
4794	46.451419	10.200.18.211	10.100.56.13	HTTP	411	GET /images/style.css HTTP/1.1
4795	46.451561	10.200.18.211	10.100.56.13	HTTP	410	GET /autosuggest.css HTTP/1.1
4796	46.451690	10.200.18.211	10.100.56.13	HTTP	395	GET /autosuggest2.js HTTP/1.1
4797	46.451795	10.200.18.211	10.100.56.13	HTTP	395	GET /suggestions2.js HTTP/1.1
5533	53.805041	10.200.18.211	10.100.56.13	HTTP	515	GET /~p_majumder/ HTTP/1.1
6092	57.703079	10.200.18.211	168.235.65.201	HTTP	497	GET / HTTP/1.1
6172	58.252876	10.200.18.211	168.235.65.201	HTTP	815	GET / HTTP/1.1

Frame 478: 411 bytes on wire (3288 bits), 411 bytes captured (3288 bits) on interface \Device\NPF\_{9f...} Ethernet II, Src: IntelCor\_80:11:73:08:6a:c5:80:11:73, Dst: Cisco\_ee:6a:29:00:f2:8b:ee:6a:29  
Internet Protocol Version 4, Src: 10.200.18.211, Dst: 10.100.56.13  
Transmission Control Protocol, Src Port: 55389, Dst Port: 80, Seq: 1, Ack: 1, Len: 357  
Hypertext Transfer Protocol  
GET /images/style.css HTTP/1.1  
[Expert Info (Chat/Sequence): GET /images/style.css HTTP/1.1  
Request Method: GET  
Request URI: /images/style.css  
Request Version: HTTP/1.1  
Host: intranet.daiict.ac.in  
Connection: keep-alive  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36  
Accept: text/css,\*/\*;q=0.1  
Sec-GPC: 1  
Accept-Language: en-US,en;q=0.9  
Referer: http://intranet.daiict.ac.in/  
Accept-Encoding: gzip, deflate  
\\n

0000 02 01 61 8b 00 00 47 45 54 20 f2 8b ee 6a 29 - a GE T /image  
0040 f2 8b ee 6a 29 02 01 61 8b 00 00 47 45 54 20 - /style.css HTTP  
0080 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 69 6e 74 72 - /1.1-Host: intr  
00c0 61 6e 65 74 2e 64 61 69 69 63 74 2e 61 63 2e 69 - anet.dai ict.ac.i  
0100 6e 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b - n-Connec tion: k  
0140 65 65 70 2d 61 6c 69 76 65 0d 0a 55 73 65 72 2d - eep-alliv e--User-  
0180 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6e 61 2f 35 - Agent: M ozilla/5  
0200 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 - .0 (Wind ows NT 1  
0240 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 34 29 - 0.0; Win 64; x64)  
0280 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 33 37 - AppleWe bKit/537  
0300 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 66 65 - .36 (KHT ML, like  
0340 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 2f 31 - Gecko) Chrome/1  
0380 31 30 2e 30 2e 30 2e 30 20 53 61 66 61 72 69 2f - 10.0.0.0 Safari/  
0400 35 33 37 2e 33 36 0d 0a 41 63 63 65 70 74 3a 20 - 537.36- Accept:  
0440 74 65 78 74 2f 63 73 73 2c 2a 2f 2a 3b 71 3d 30 - text/css ,/\*;q=0  
0480 2e 31 0d 0a 53 65 63 2d 47 50 43 3a 20 31 0d 0a - .1-Sec- GPC: 1-  
0500 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a - Accept-L anguage:  
0540 20 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e 39 0d - en-US,e n;q=0.9-  
0580 0a 52 65 66 65 72 65 72 3a 20 68 74 74 70 3a 2f - .Referer : http/  
0600 2f 69 6e 74 72 61 6e 65 74 2e 64 61 69 69 63 74 - /intranet .daiict-  
0640 2e 61 63 2e 69 6e 2f 0d 0a 41 63 63 65 70 74 2d - .ac.in/. -Accept-

### 6.2.1. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

Ans : Status Code - 200; Phrase - OK.

[illegible]

### 6.2.2. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

Ans : Nothing is included in the HTTP GET message for the second time. Just the referer is changed to <http://intranet.daiict.ac.in>.

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, and Help. Below the menu is a toolbar with icons for common actions like opening files, saving, and zooming.

The main window is divided into three panes:

- Packet List:** Shows a list of captured packets. The selected packet is #478, an HTTP GET request to `/images/style.css` from `10.200.18.211` to `10.100.56.13`.
- Packet Details:** Provides a hierarchical view of the selected packet's structure. It shows the Ethernet II frame, Internet Protocol Version 4 header, and the Hypertext Transfer Protocol (HTTP) request. The HTTP request details include the method (GET), request URI (`/images/style.css`), and various headers:
  - `Host: intranet.dalict.ac.in/vr/n`
  - `Connection: keep-alive/vr/n`
  - `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.0.0 Safari/...`
  - `Accept: text/css,*/*;q=0.1/vr/n`
  - `Accept-Language: en-US,en;q=0.9/vr/n`
  - `Referer: http://intranet.dalict.ac.in/vr/n` (highlighted with a red box)
  - `Accept-Encoding: gzip, deflate/vr/n`
- Packet Bytes:** Displays the raw data of the selected packet in hexadecimal and ASCII format.

The status bar at the bottom indicates the current packet is 18718 bytes in size, with a display filter of `http.request.method == "GET"`.