

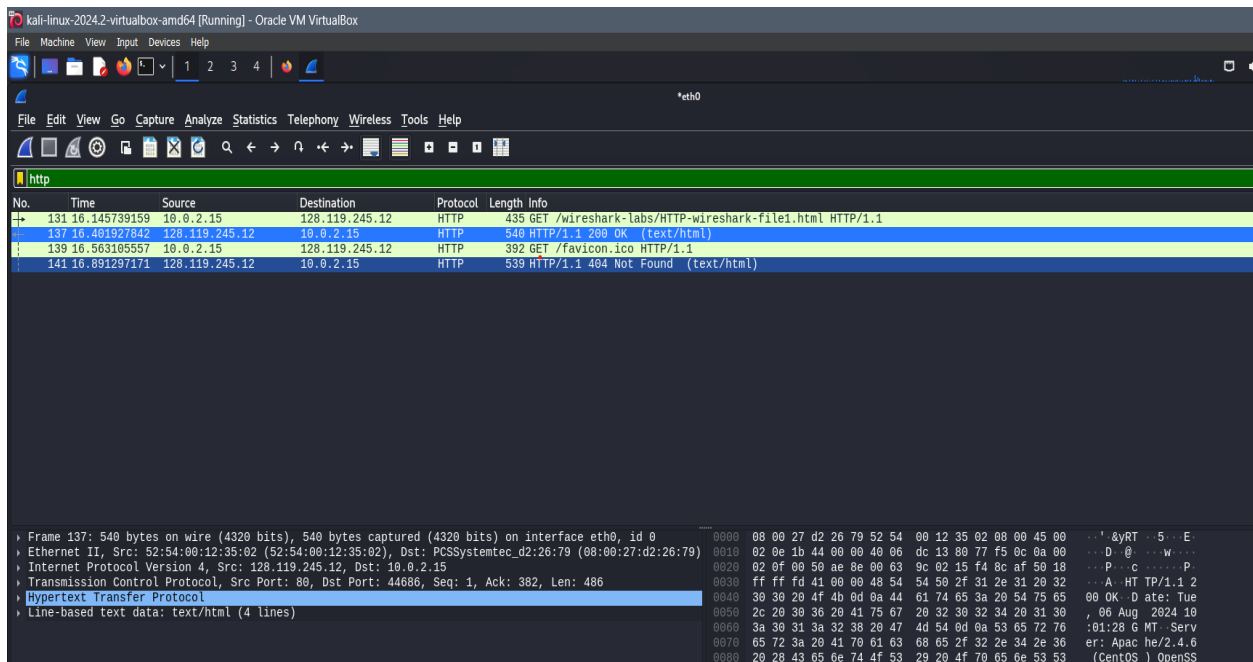
## IP LAB EXPERIMENT-3

NAME : T.PAVAN KUMAR

ROLL NO: CB.SC.P2CYS24018

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

-- HTTP version 1.1



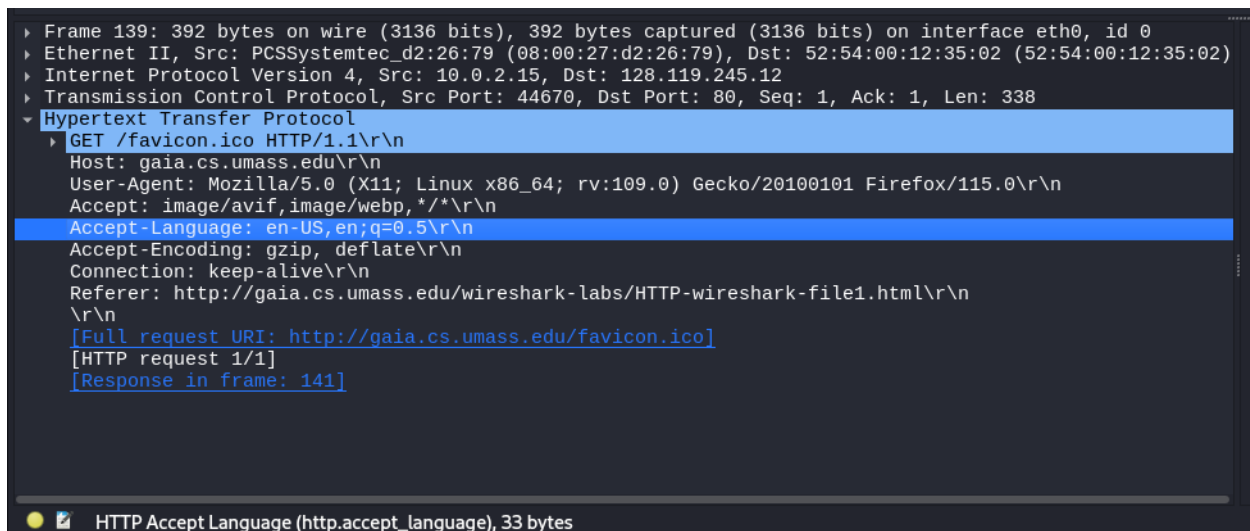
The image shows a Wireshark capture of HTTP traffic. The packet list pane on the left shows four packets. The selected packet (No. 137) is an HTTP GET request for /wireshark-labs/HTTP-wireshark-file1.html. The packet details pane on the right shows the structure of the HTTP message, including the request line, status line, and various headers. The status line indicates a 200 OK response. The packet bytes pane at the bottom shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
131	16.145739159	10.0.2.15	128.119.245.12	HTTP	435	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
137	16.461927842	128.119.245.12	10.0.2.15	HTTP	540	HTTP/1.1 200 OK (text/html)
139	16.563165557	10.0.2.15	128.119.245.12	HTTP	392	GET /favicon.ico HTTP/1.1
141	16.891297171	128.119.245.12	10.0.2.15	HTTP	539	HTTP/1.1 404 Not Found (text/html)

Frame 137: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface eth0, id 0  
Ethernet II, Src: 52:54:00:12:35:02 (52:54:00:12:35:02), Dst: PCSystemtec\_d2:26:79 (08:00:27:d2:26:79)  
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.15  
Transmission Control Protocol, Src Port: 80, Dst Port: 44686, Seq: 1, Ack: 382, Len: 486  
Hypertext Transfer Protocol  
Line-based text data: text/html (4 lines)

```
0000 08 00 27 d2 26 79 52 54 08 12 35 02 00 00 45 00  ...&yRT...5...E-
0010 02 0e 1b 44 00 00 40 06 dc 13 80 77 f5 0c 0a 00  ...D...w...
0020 02 0f 00 50 ae 8e 00 63 9c 02 15 f4 8c af 50 18  ...P...C...P...
0030 ff ff fd 41 00 00 48 54 54 50 2f 31 20 31 20 32  ...A...HT...TP/1.1 2
0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 75 65 00 OK Date: Tue
0050 2c 20 30 36 20 41 75 67 20 32 30 32 34 20 31 30 , 06 Aug 2024 10
0060 3a 30 31 3a 32 38 20 47 4d 54 0d 0a 53 65 72 76 :01:28 G MT Serv
0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 er: Apac he/2.4.6
0080 20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 (CentOS ) OpenSS
```

2. What languages (if any) do your browser indicate that it can accept to the server?



```

Frame 139: 392 bytes on wire (3136 bits), 392 bytes captured (3136 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_d2:26:79 (08:00:27:d2:26:79), Dst: 52:54:00:12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 44670, Dst Port: 80, Seq: 1, Ack: 1, Len: 338
Hypertext Transfer Protocol
  GET /favicon.ico HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0\r\n
  Accept: image/avif,image/webp,*/*\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Connection: keep-alive\r\n
  Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/favicon.ico]
  [HTTP request 1/1]
  [Response in frame: 141]

```

HTTP Accept Language (http.accept\_language), 33 bytes

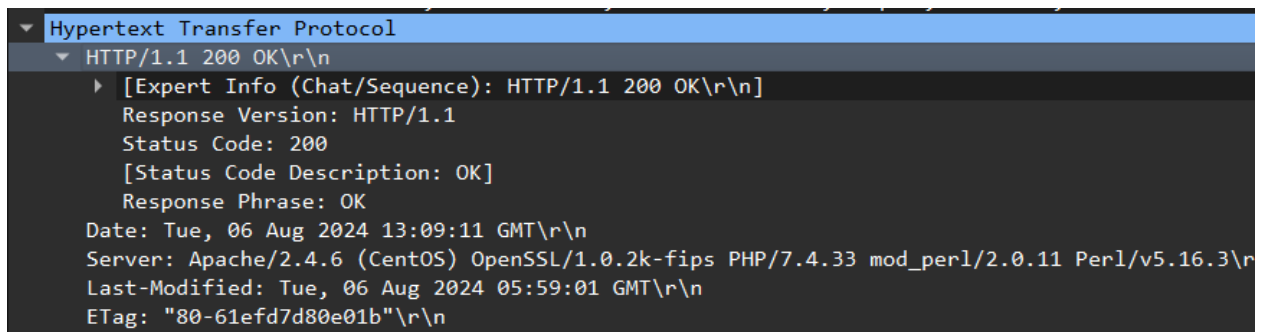
3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

IP Address of My computer- 10.11.132.192

Destination Address - 128.119.245.12

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

-- 200



```

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: Tue, 06 Aug 2024 13:09:11 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
  Last-Modified: Tue, 06 Aug 2024 05:59:01 GMT\r\n
  ETag: "80-61efd7d80e01b"\r\n

```

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

-- Tuesday, 06 August 2024 13:09:11

```
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: Tue, 06 Aug 2024 13:09:11 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/
    Last-Modified: Tue, 06 Aug 2024 05:59:01 GMT\r\n
```

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

-- 128 bytes

```
Accept-Ranges: none\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 1/2]
[Time since request: 0.264179000 seconds]
```

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.

-- No

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?

-- The first time I have requested the resource, there is no cached data to compare against. Because I cleared all the cache. In such cases, the browser will send a normal GET request without the If-Modified-Since header.

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

```
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/2]
[Time since request: 0.264179000 seconds]
[Request in frame: 6284]
[Next request in frame: 6337]
[Next response in frame: 6367]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
File Data: 128 bytes
▼ Line-based text data: text/html (4 lines)
<html>\n
Congratulations. You've downloaded the file \n
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
</html>\n
```

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? What information follows the “IFMODIFIED-SINCE:” header?

```
Upgrade-Insecure-Requests: 1\r\n
If-Modified-Since: Tue, 06 Aug 2024 05:59:01 GMT\r\n
If-None-Match: "173-61efd7d80d84b"\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 1/1]
[Response in frame: 298]
```

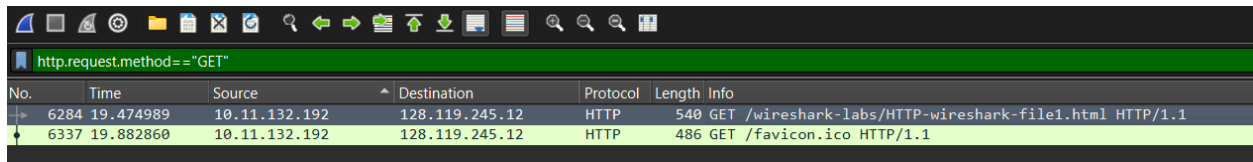
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the file’s contents?

```
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.15
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 38206, Seq: 1, Ack: 468, Len: 240
  ▼ Hypertext Transfer Protocol
    ▼ HTTP/1.1 304 Not Modified\r\n
      [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
      Response Version: HTTP/1.1
      Status Code: 304
      [Status Code Description: Not Modified]
      Response Phrase: Not Modified
```

12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

-- 2 http get requests were sent.

The packet number in the trace is 6284.



A screenshot of the Wireshark interface showing a packet capture. The top toolbar includes icons for file operations, network analysis, and search. Below the toolbar, a green filter bar contains the text 'http.request.method==\"GET\"'. The main packet list table shows two packets:

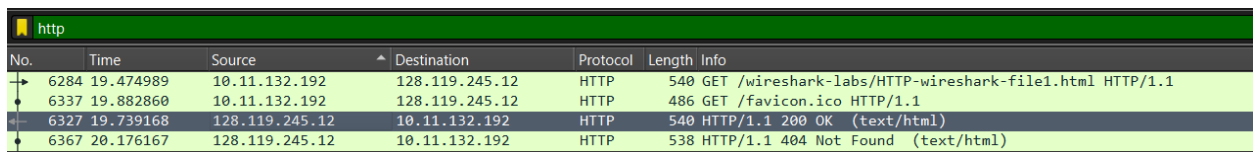
No.	Time	Source	Destination	Protocol	Length	Info
6284	19.474989	10.11.132.192	128.119.245.12	HTTP	540	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
6337	19.882860	10.11.132.192	128.119.245.12	HTTP	486	GET /favicon.ico HTTP/1.1

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

-- The packet number in the trace is 6327.

Status code is 200.

Phrase associated with the response is OK .



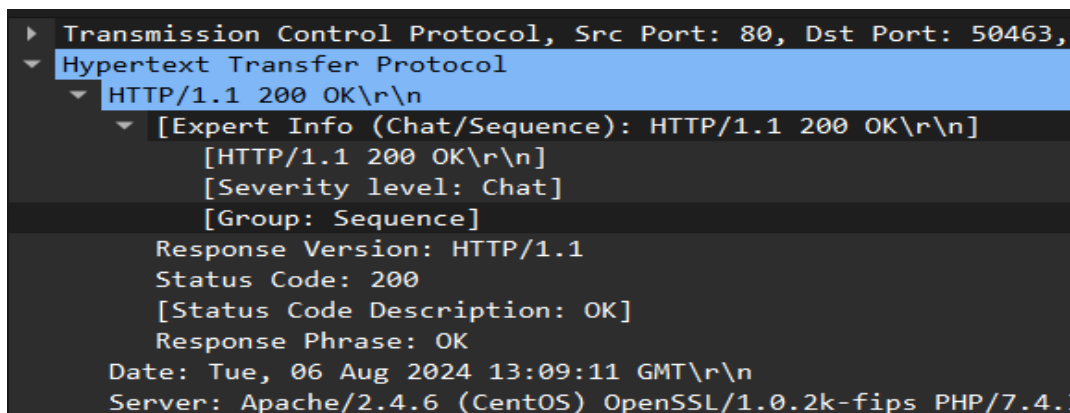
A screenshot of the Wireshark interface showing a packet capture. The top toolbar is visible. Below it, a green filter bar contains the text 'http'. The main packet list table shows four packets:

No.	Time	Source	Destination	Protocol	Length	Info
6284	19.474989	10.11.132.192	128.119.245.12	HTTP	540	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
6337	19.882860	10.11.132.192	128.119.245.12	HTTP	486	GET /favicon.ico HTTP/1.1
6327	19.739168	128.119.245.12	10.11.132.192	HTTP	540	HTTP/1.1 200 OK (text/html)
6367	20.176167	128.119.245.12	10.11.132.192	HTTP	538	HTTP/1.1 404 Not Found (text/html)

14. What is the status code and phrase in the response?

-- Status code is 200.

Phrase associated with the response is OK.



A screenshot of the Wireshark packet details pane. The left pane shows a tree view with 'Transmission Control Protocol, Src Port: 80, Dst Port: 50463', 'Hypertext Transfer Protocol', and 'HTTP/1.1 200 OK\r\n' selected. The right pane shows the expanded details for the selected packet:

Field	Value
[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, 06 Aug 2024 13:09:11 GMT\r\n
Server:	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.3

15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

--- 3 TCP Segments were needed.

13	5.457158106	10.0.2.15	128.119.245.12	TCP	54 53112 → 80 [ACK] Seq=1 Ack=1 Win=32120 Len=0
14	5.458349796	10.0.2.15	128.119.245.12	HTTP	435 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
15	5.459089162	128.119.245.12	10.0.2.15	TCP	60 80 → 53112 [ACK] Seq=1 Ack=382 Win=65535 Len=0
20	5.840651479	128.119.245.12	10.0.2.15	TCP	2974 80 → 53112 [ACK] Seq=1 Ack=382 Win=65535 Len=2920 [TCP segment of a reassembled PDU]
21	5.840768618	10.0.2.15	128.119.245.12	TCP	54 53112 → 80 [ACK] Seq=382 Ack=2921 Win=30660 Len=0
22	5.841367465	128.119.245.12	10.0.2.15	HTTP	1995 HTTP/1.1 200 OK (text/html)
23	5.841442958	10.0.2.15	128.119.245.12	TCP	54 53112 → 80 [ACK] Seq=382 Ack=4862 Win=30660 Len=0

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

```
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 404 Not Found\r\n
    ▶ [Expert Info (Chat/Sequence): HTTP/1.1 404 Not Found\r\n]
      Response Version: HTTP/1.1
      Status Code: 404
      [Status Code Description: Not Found]
      Response Phrase: Not Found
      Date: Wed, 07 Aug 2024 13:55:37 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
      ▶ Content-Length: 253\r\n
      Keep-Alive: timeout=5, max=100\r\n
      Connection: Keep-Alive\r\n
      Content-Type: text/html; charset=iso-8859-1\r\n
      \r\n
      [HTTP response 1/1]
      [Time since request: 0.339479193 seconds]
      [Request in frame: 56]
      [Request URI: http://gaia.cs.umass.edu/wiresharklabs/protected_pages/HTTP-wireshark-file5.html]
      File Data: 253 bytes
  ▼ Line-based text data: text/html (7 lines)
    <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
    <html><head>\n
```

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

```
▶ Frame 70: 539 bytes on wire (4312 bits), 539 bytes captured (4312 bits) on interface eth0, id 0
▶ Ethernet II, Src: 52:54:00:12:35:02 (52:54:00:12:35:02), Dst: PCSSystemtec_d2:26:79 (08:00:27:d2:26:79)
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.15
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 40042, Seq: 1, Ack: 354, Len: 485
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 404 Not Found\r\n
    ▶ [Expert Info (Chat/Sequence): HTTP/1.1 404 Not Found\r\n]
      Response Version: HTTP/1.1
      Status Code: 404
      [Status Code Description: Not Found]
      Response Phrase: Not Found
      Date: Wed, 07 Aug 2024 13:55:38 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
      ▶ Content-Length: 209\r\n
      Keep-Alive: timeout=5, max=100\r\n
      Connection: Keep-Alive\r\n
      Content-Type: text/html; charset=iso-8859-1\r\n
      \r\n
      [HTTP response 1/1]
      [Time since request: 0.350158990 seconds]
      [Request in frame: 68]
      [Request URI: http://gaia.cs.umass.edu/favicon.ico]
  ▼ Expert Info (_ws.expert)
```