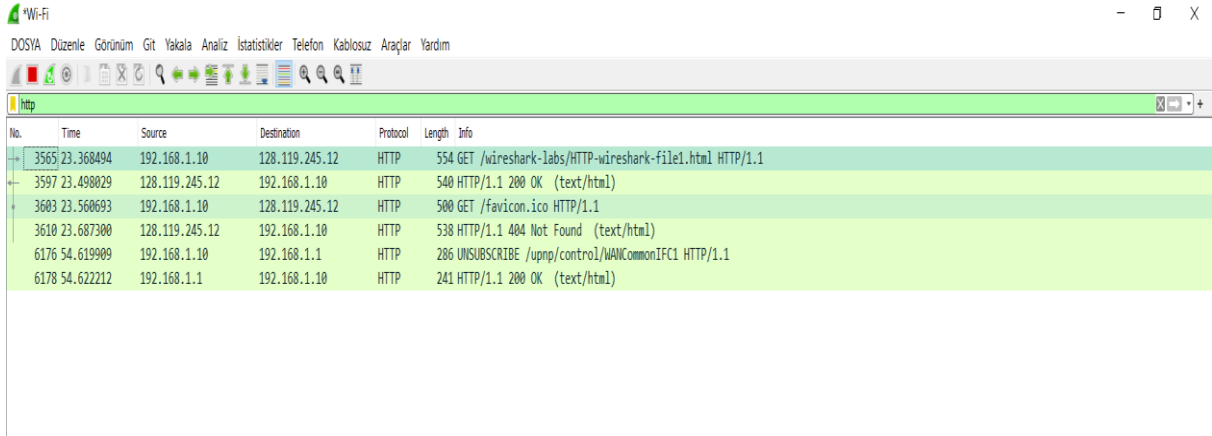


HASAN MERT YALÇIN - 150119647

1. The Basic HTTP GET/response interaction

Q1)

HTTP version is http/1.1

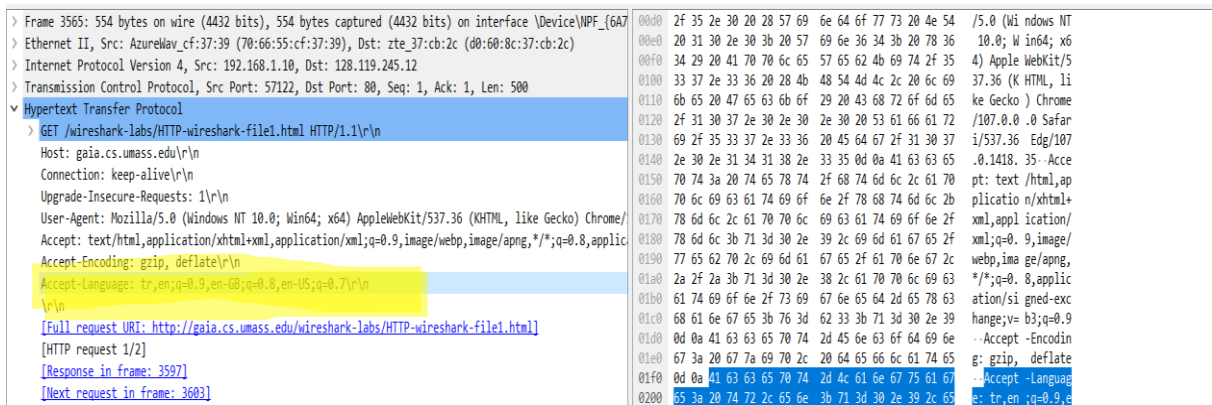


The image shows a Wireshark packet capture window. The top bar indicates the capture is on the 'Wi-Fi' interface. The packet list pane shows several HTTP packets. The selected packet is packet 3565, which is a GET request for '/wireshark-labs/HTTP-wireshark-file1.html' from 192.168.1.10 to 128.119.245.12. The packet details pane shows the HTTP structure, including the status line 'HTTP/1.1 200 OK (text/html)'.

No.	Time	Source	Destination	Protocol	Length	Info
3565	23.368494	192.168.1.10	128.119.245.12	HTTP	554	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
3597	23.498029	128.119.245.12	192.168.1.10	HTTP	540	HTTP/1.1 200 OK (text/html)
3603	23.560693	192.168.1.10	128.119.245.12	HTTP	500	GET /favicon.ico HTTP/1.1
3610	23.687300	128.119.245.12	192.168.1.10	HTTP	538	HTTP/1.1 404 Not Found (text/html)
6176	54.619909	192.168.1.10	192.168.1.1	HTTP	286	UNSUBSCRIBE /unnp/control/WANCommonIFC1 HTTP/1.1
6178	54.622212	192.168.1.1	192.168.1.10	HTTP	241	HTTP/1.1 200 OK (text/html)

Q2)

Accept language is Turkish : tr,en;q=0.9,en-GB;q=0.8,en-US;q=0.7\r\n

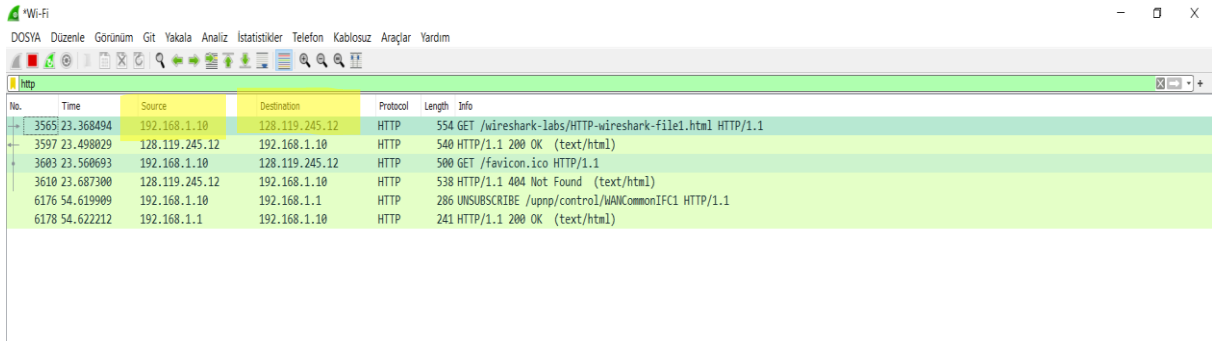


The image shows the packet details pane for the selected HTTP GET request. The pane is expanded to show the 'Hypertext Transfer Protocol' section. The 'Accept-Language' header is highlighted in yellow, showing the value 'tr,en;q=0.9,en-GB;q=0.8,en-US;q=0.7\r\n'. The 'Full request URI' is also visible, showing 'http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html'.

Frame 3565: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface \\Device\\NPF_{6A7...}	00d0 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 /5.0 (Windows NT
> Ethernet II, Src: AzureWav_cf:37:39 (70:66:55:cf:37:39), Dst: zte_37:cb:2c (d0:60:8c:37:cb:2c)	00e0 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 10.0; Win64; x6
> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 128.119.245.12	00f0 34 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 4) AppleWebKit/5
> Transmission Control Protocol, Src Port: 57122, Dst Port: 80, Seq: 1, Ack: 1, Len: 500	0100 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 37.36 (KHTML, li
> Hypertext Transfer Protocol	0110 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 ke Gecko) Chrome
> GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n	0120 2f 31 30 37 2e 30 2e 30 2e 30 20 53 61 66 61 72 /107.0.0.0 Safari
Host: gaia.cs.umass.edu\r\n	0130 69 2f 35 33 37 2e 33 36 20 45 64 67 2f 31 30 37 i/537.36 Edge/107
Connection: keep-alive\r\n	0140 2e 30 2e 31 34 31 38 2e 33 35 0d 0a 41 63 63 65 .0.1418. 35 -Acce
Upgrade-Insecure-Requests: 1\r\n	0150 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 pt: text/html,ap
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/	0160 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b plicatio n/html+
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/	0170 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f xml,appl ication/
Accept-Encoding: gzip, deflate\r\n	0180 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f xml;q=0. 9,image/
Accept-Language: tr,en;q=0.9,en-GB;q=0.8,en-US;q=0.7\r\n	0190 77 65 62 70 2c 69 6d 61 67 65 2f 61 70 6e 67 2c webp,ima ge/apng,
\r\n	01a0 2a 2f 2a 3b 71 3d 30 2e 38 2c 61 70 70 6c 69 63 */*;q=0. 8,applic
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]	01b0 61 74 69 6f 6e 2f 73 69 67 6e 65 64 2d 65 78 63 ation/si gned-exc
[HTTP request 1/2]	01c0 68 61 6e 67 65 3b 76 3d 62 33 3b 71 3d 30 2e 39 hange;v= b3;q=0.9
[Response in frame: 3597]	01d0 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e - -Accept -Encodin
[Next request in frame: 3603]	01e0 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 g: gzip, deflate
	01f0 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 - -Accept -Languag
	0200 65 3a 20 74 72 2c 65 6e 3b 71 3d 30 2e 39 2c 65 e: tr,en ;q=0.9,e

Q3)

My IP address is 192.168.1.10 and
gaia.cs.umass.edu server is 128.119.245.12

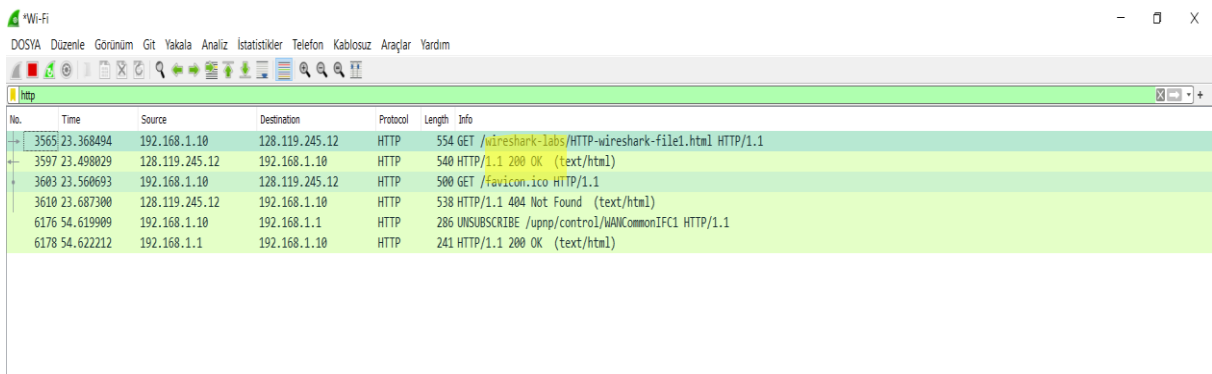


Wireshark packet capture showing HTTP traffic. The table below represents the data visible in the packet list pane.

No.	Time	Source	Destination	Protocol	Length	Info
3565	23.368494	192.168.1.10	128.119.245.12	HTTP	554	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
3597	23.498029	128.119.245.12	192.168.1.10	HTTP	540	HTTP/1.1 200 OK (text/html)
3603	23.560693	192.168.1.10	128.119.245.12	HTTP	500	GET /favicon.ico HTTP/1.1
3610	23.687300	128.119.245.12	192.168.1.10	HTTP	538	HTTP/1.1 404 Not Found (text/html)
6176	54.619909	192.168.1.10	192.168.1.1	HTTP	286	UNSUBSCRIBE /upnp/control/WANCommonIFC1 HTTP/1.1
6178	54.622212	192.168.1.1	192.168.1.10	HTTP	241	HTTP/1.1 200 OK (text/html)

Q4)

Status code is 200 OK



Wireshark packet capture showing HTTP traffic. The table below represents the data visible in the packet list pane.

No.	Time	Source	Destination	Protocol	Length	Info
3565	23.368494	192.168.1.10	128.119.245.12	HTTP	554	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
3597	23.498029	128.119.245.12	192.168.1.10	HTTP	540	HTTP/1.1 200 OK (text/html)
3603	23.560693	192.168.1.10	128.119.245.12	HTTP	500	GET /favicon.ico HTTP/1.1
3610	23.687300	128.119.245.12	192.168.1.10	HTTP	538	HTTP/1.1 404 Not Found (text/html)
6176	54.619909	192.168.1.10	192.168.1.1	HTTP	286	UNSUBSCRIBE /upnp/control/WANCommonIFC1 HTTP/1.1
6178	54.622212	192.168.1.1	192.168.1.10	HTTP	241	HTTP/1.1 200 OK (text/html)

Q5)

The last modified date is : Wed, 09 Nov 2022 06:59:01 GMT\r\n

```
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Wed, 09 Nov 2022 21:30:54 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, 09 Nov 2022 06:59:01 GMT\r\n
    ETag: "80-5ed043103b344"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
```

Q6)

Content length 128 bytes, Content-Length : 128\r\n [Content Length : 23709]

```
▼ HTTP/1.1 200 OK\r\n
  Date: Wed, 09 Nov 2022 21:30:54 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, 09 Nov 2022 06:59:01 GMT\r\n
  ETag: "80-5ed043103b344"\r\n
  Accept-Ranges: bytes\r\n
  > Content-Length: 128\r\n
    [Content length: 128]
  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: 0.129535000 seconds]
```

Q7)

No, I do not see any headers that are not displayed in the packet window.

2.The HTTP CONDITIONAL GET/response interaction

Q8)

No, there is no IF-MODIFIED-SINCE line.

Q9)

Yes, the server explicitly returned the contents of the file.

```
[Time since request: 0.137312000 seconds]
[Request in frame: 1397]
[Next request in frame: 1442]
[Next response in frame: 1452]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
File Data: 371 bytes
▼ 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
```

Q10)

Yes I saw. If-Modified-Since : Wed, 09 Nov 2022 06:59:01 GMT\R\n

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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: tr,en;q=0.9,en-GB;q=0.8,en-US;q=0.7\r\n
If-None-Match: "173-5ed043103ab73"\r\n
If-Modified-Since: Wed, 09 Nov 2022 06:59:01 GMT\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: 1452]
```

Q11)

The status code: 304 and status code description: Not modified.
No, the server does not explicitly return the contents of the file.

```
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.10
> Transmission Control Protocol, Src Port: 80, Dst Port: 57559, Seq: 1, Ack: 613, 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
    Date: Wed, 09 Nov 2022 21:51:58 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
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "173-5ed043103ab73"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.141496000 seconds]
    [Request in frame: 1623]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

3. Retrieving Long Documents

Q12)

My browser sent 2 http GET request to the server.

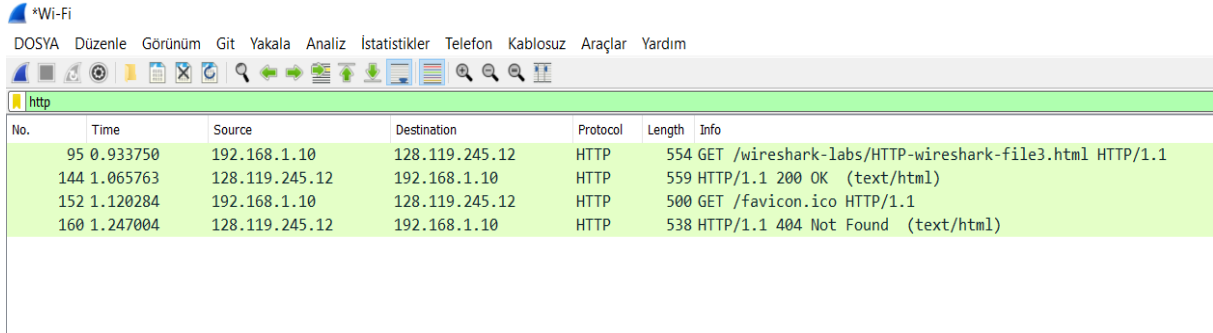
*Wi-Fi

DOSYA Düzenle Görünüm Git Yakala Analiz İstatistikler Telefon Kablosuz Araçlar Yardım

No.	Time	Source	Destination	Protocol	Length	Info
95	0.933750	192.168.1.10	128.119.245.12	HTTP	554	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
144	1.065763	128.119.245.12	192.168.1.10	HTTP	559	HTTP/1.1 200 OK (text/html)
152	1.120284	192.168.1.10	128.119.245.12	HTTP	500	GET /favicon.ico HTTP/1.1
160	1.247004	128.119.245.12	192.168.1.10	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Q13)

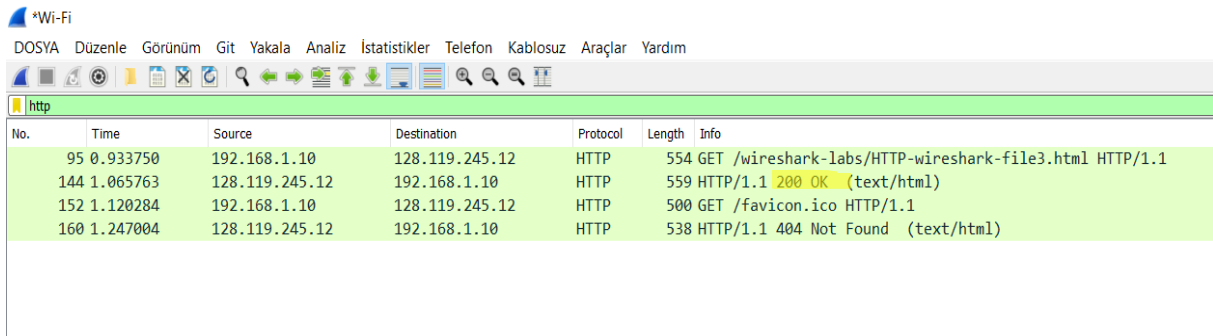
The packet 144 contains the status code and phrase associated with response to the http GET request.



No.	Time	Source	Destination	Protocol	Length	Info
95	0.933750	192.168.1.10	128.119.245.12	HTTP	554	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
144	1.065763	128.119.245.12	192.168.1.10	HTTP	559	HTTP/1.1 200 OK (text/html)
152	1.120284	192.168.1.10	128.119.245.12	HTTP	500	GET /favicon.ico HTTP/1.1
160	1.247004	128.119.245.12	192.168.1.10	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Q14)

The status of code and phrase in the response 200 OK.



No.	Time	Source	Destination	Protocol	Length	Info
95	0.933750	192.168.1.10	128.119.245.12	HTTP	554	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
144	1.065763	128.119.245.12	192.168.1.10	HTTP	559	HTTP/1.1 200 OK (text/html)
152	1.120284	192.168.1.10	128.119.245.12	HTTP	500	GET /favicon.ico HTTP/1.1
160	1.247004	128.119.245.12	192.168.1.10	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Q15)

The data sent in 4 reassembled TCP Segments.

```

> Frame 144: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface \Device\NPF_{6F ^
> Ethernet II, Src: zte_37:cb:2c (d0:60:8c:37:cb:2c), Dst: AzureWav_cf:37:39 (70:66:55:cf:37:39)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.10
> Transmission Control Protocol, Src Port: 80, Dst Port: 57709, Seq: 4357, Ack: 501, Len: 505
> [4 Reassembled TCP Segments (4861 bytes): #140(1452), #141(1452), #143(1452), #144(505)]
> Hypertext Transfer Protocol
  Line-based text data: text/html (98 lines)
    <html><head> \n
    <title>Historical Documents:THE BILL OF RIGHTS</title></head>\n
    \n
    \n
    <body bgcolor="#ffffff" link="#330000" vlink="#666633">\n
    <p><br>\n
    </p>\n
    <p><center><b>THE BILL OF RIGHTS</b><br>\n
    <em>Amendments 1-10 of the Constitution</em>\n
    </center>\n
    \n
    <p>The Conventions of a number of the States having, at the time of adopting\n
    the Constitution, expressed a desire, in order to prevent misconstruction\n

```

4. HTML Documents with Embedded Objects

Q16)

4 HTTP GET request messages sent.

No.	Time	Source	Destination	Protocol	Length	Info
3416	19.007661	192.168.1.10	128.119.245.12	HTTP	554	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
3435	19.141789	128.119.245.12	192.168.1.10	HTTP	1355	HTTP/1.1 200 OK (text/html)
3436	19.152535	192.168.1.10	128.119.245.12	HTTP	500	GET /pearson.png HTTP/1.1
3448	19.231336	192.168.1.10	178.79.137.164	HTTP	467	GET /8E_cover_small.jpg HTTP/1.1
3453	19.287156	128.119.245.12	192.168.1.10	HTTP	761	HTTP/1.1 200 OK (PNG)
3455	19.290172	178.79.137.164	192.168.1.10	HTTP	225	HTTP/1.1 301 Moved Permanently
4081	20.069057	192.168.1.10	128.119.245.12	HTTP	500	GET /favicon.ico HTTP/1.1
4082	20.201234	128.119.245.12	192.168.1.10	HTTP	538	HTTP/1.1 404 Not Found (text/html)

The internet addresses:

\r\n

[Full request URI: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>]

[HTTP request 1/3]

\r\n

[Full request URI: <http://gaia.cs.umass.edu/pearson.png>]

[HTTP request 2/3]

\r\n

[Full request URI: http://kurose.cslash.net/8E_cover_small.jpg]

[HTTP request 1/1]

[Full request URI: <http://gaia.cs.umass.edu/favicon.ico>]

[HTTP request 3/3]

Q17)

There is two different images and different servers. So, there is different relations.

5 HTTP Authentication

Q18)

```
> Frame 1769: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF_{66^
> Ethernet II, Src: zte_37:cb:2c (d0:60:8c:37:cb:2c), Dst: AzureWav_cf:37:39 (70:66:55:cf:37:39)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.10
> Transmission Control Protocol, Src Port: 80, Dst Port: 58146, Seq: 1, Ack: 517, Len: 717
v Hypertext Transfer Protocol
  v HTTP/1.1 401 Unauthorized\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
      Response Version: HTTP/1.1
      Status Code: 401
      [Status Code Description: Unauthorized]
      Response Phrase: Unauthorized
      Date: Wed, 09 Nov 2022 22:38:45 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
      WWW-Authenticate: Basic realm="wireshark-students only"\r\n
  v Content-Length: 381\r\n
    [Content length: 381]
    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
```


Q19)

```

  ▾ GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1]
      Request Method: GET
      Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
      Request Version: HTTP/1.1
      Host: gaia.cs.umass.edu\r\n
      Connection: keep-alive\r\n
      Cache-Control: max-age=0\r\n
      ▾ Authorization: Basic aGFzYW46MTIzNGFzZA==\r\n
        Credentials: hasan:1234asd
      Upgrade-Insecure-Requests: 1\r\n
      User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\n
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: tr,en;q=0.9,en-GB;q=0.8,en-US;q=0.7\r\n
      \r\n
      [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
      [HTTP request 1/1]
      [Response in frame: 3134]

```