

CSP334 : Computer Networks
Lab Assignment No 4
Assignment on HTTP

Sahil
2016UCS0008

September 26, 2018

1 The Basic HTTP GET/ Response Interaction:

File: *simple1.html*

1.1 HTTP Version of browser and server:

206	14:15:5...	10.10.41.88	145.14.144.38	HTTP	524	GET /simple1.html HTTP/1.1
218	14:15:5...	145.14.144.38	10.10.41.88	HTTP	86	HTTP/1.1 200 OK (text/html)

IPA of computer IPA of server

Frame 206: 524 bytes on wire (4192 bits), 524 bytes captured (4192 bits) on interface 0
Ethernet II, Src: Apple_24:e0:94 (f0:79:60:24:e0:94), Dst: Cisco_af:0c:64 (a0:3d:6f:af:0c:64)
Internet Protocol Version 4, Src: 10.10.41.88, Dst: 145.14.144.38
Transmission Control Protocol, Src Port: 50508, Dst Port: 80, Seq: 693037869, Ack: 393313500:
Hypertext Transfer Protocol
GET /simple1.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /simple1.html HTTP/1.1\r\n]
Request Method: GET
Request URI: /simple1.html
Request Version: HTTP/1.1 HTTP Version of browser
Host: cncourse.000webhostapp.com\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, li
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://cncourse.000webhostapp.com/\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n Languages accepted by browser
\r\n
[Full request URI: http://cncourse.000webhostapp.com/simple1.html]
HTTP/1.1 200 OK

As highlighted, version 1.1 is used by both browser and server.

1.2 Languages accepted by the browser:

As shown above, English language is accepted.

1.3 IPA of computer and *cncourse* web server:

IPA of computer is 10.10.41.88 and that of server is 145.14.144.38.

1.4 Status code returned from server to the browser: 200

Time	Source	Destination	Protocol	Length	Info
206	14:15:5...	10.10.41.88	145.14.144.38	HTTP	524 GET /simple1.html HTTP/1.1
218	14:15:5...	145.14.144.38	10.10.41.88	HTTP	86 HTTP/1.1 200 OK (text/html)

Frame 218: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
Ethernet II, Src: Cisco_af:0c:64 (a0:3d:6f:af:0c:64), Dst: Apple_24:e0:94 (f0:79:60:24:e0:94)
Internet Protocol Version 4, Src: 145.14.144.38, Dst: 10.10.41.88
Transmission Control Protocol, Src Port: 80, Dst Port: 50508, Seq: 3933135792, Ack: 6930383
[4 Reassembled TCP Segments (809 bytes): #215(372), #216(71), #217(346), #218(20)]
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

1.5 HTML file last modified at the server:

There is no *last-modified* header in the HTTP packet.

1.6 Bytes of content returned to the browser:

```
Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
Date: Wed, 26 Sep 2018 09:46:57 GMT\r\n
Content-Type: text/html; charset=UTF-8\r\n
Transfer-Encoding: chunked\r\n
Connection: keep-alive\r\n
Server: awex\r\n
X-Xss-Protection: 1; mode=block\r\n
X-Content-Type-Options: nosniff\r\n
X-Request-ID: e2c87efa9ac876853f80920d8c936d69\r\n
Content-Encoding: gzip\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.284845000 seconds]
[Request in frame: 241]
> HTTP chunked response Bytes of content returned to browser
Content-encoded entity body (gzip): 480 bytes -> 680 bytes
File Data: 680 bytes
Line-based text data: text/html (10 lines) Packet content window
40 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d HTTP/1.1 200 OK
10 0a 44 61 74 65 3a 20 57 65 64 2c 20 32 36 20 53 Date: Wed, 26 S
20 65 70 20 32 30 31 38 20 30 39 3a 34 36 3a 35 37 ep 2018 09:46:57
30 20 47 2d 54 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 GMT Co ntent-Ty
40 70 65 3a 20 74 65 78 74 2f 68 74 6d 6c 3b 20 63 pe: text /html; c
50 68 61 72 73 65 74 3d 55 54 46 2d 38 0d 0a 54 72 harset=U TF-8 Tr
60 61 6e 73 66 65 72 2d 45 6e 63 6f 64 69 6e 67 3a ansfer-E ncoding:
70 20 63 68 75 6e 6b 65 64 0d 0a 43 6f 6e 6e 65 63 chunked Conne
80 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 tion: ke ep-alive
90 0d 0a 53 65 72 76 65 72 3a 20 61 77 65 78 0d 0a Server : awex
a0 58 2d 58 73 73 2d 50 72 6f 74 65 63 74 69 6f 6e X-Xss-Pr otection
b0 3a 20 31 3b 20 6d 6f 64 65 3d 62 6c 6f 63 6b 0d : 1; mod e=block
c0 0a 58 2d 43 6f 6e 74 65 6e 74 2d 54 79 70 65 2d X-Conte nt-Type-
d0 4f 70 74 69 6f 6e 73 3a 20 6e 6f 73 6e 69 66 66 Options: nosniff
e0 0d 0a 58 2d 52 65 71 75 65 73 74 2d 49 44 3a 20 X-Requ est-ID:
f0 65 32 63 38 37 65 66 61 39 61 63 38 37 36 38 35 e2c87efa 9ac87685
10 33 66 38 30 39 32 30 64 38 63 39 33 36 64 36 39 3f80920d 8c936d69
20 0d 0a 43 6f 6e 74 65 6e 74 2d 45 6e 63 6f 64 69 Content-Encodi
30 1f 8b 08 00 00 00 00 00 00 03 b2 c9 28 c9 cd b1 ng: gzip 42
40 e3 e5 b2 c9 48 4d 4c 01 d2 9c 36 25 99 25 39 a9 HML 6% 9
50 76 0a c1 99 b9 05 39 a9 0a 86 56 0a fe 79 39 95 v 9 V y9
60 0a 21 a9 15 25 0a 36 fa 10 49 5e 2e 00 00 00 00 ! 6 I
70 ff ff 0d 0a 34 31 0d 0a b2 d1 87 aa b7 49 ca 4f 41 I 0
80 a9 04 eb 37 b4 73 ce cf 2d 28 2d 49 2d 52 f0 4b 7 s -(I-R-K
```

As highlighted, 480 bytes are returned to browser in *gzip* format which is then uncompressed to 680 bytes by the browser.

1.7 Headers not displayed in the packet-listing window:

As seen in the packet content window, all the headers shown in the packet-listing window are only displayed, so there is NO additional header present.

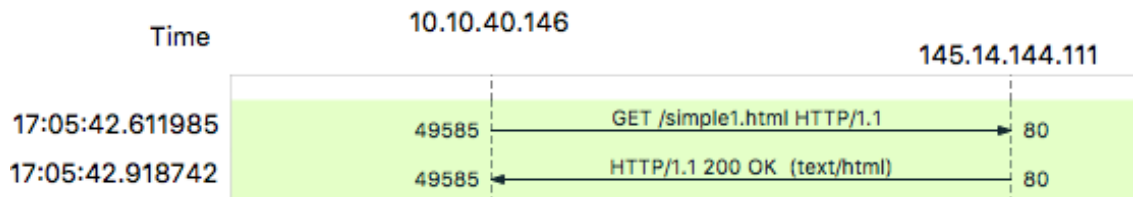
1.8 No. of request sent by browser and responded by server:

Topic / Item	Count	Rate (ms)	Percent	Burst rate	Burst start
▼ HTTP Requests by HTTP Host	1	0.0035	100%	0.0100	5.839
▼ cncourse.000webhostapp.com	1	0.0035	100.00%	0.0100	5.839
/simple1.html	1	0.0035	100.00%	0.0100	5.839

There is one request sent by the browser to the *simple1.html* file on the server, and same is responded back by the server.

1.9 HTTP traffic flow graph showing the packet exchanges between the client and the server:

The *HTTP traffic flow* graph is obtained from the **Statistics - Flow Graph** option and then checking the option *Limit to display filter* as the filter chosen is HTTP.



1.10 File *simple2.html*:

Last modified information is not available for the *html* file but for the *GIF* image loaded along with this html, it is displayed below.

```
Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
  Server: nginx/1.12.2\r\n
  Date: Wed, 26 Sep 2018 09:17:53 GMT\r\n
  Content-Type: image/gif\r\n
  Content-Length: 9601\r\n
  Last-Modified: Fri, 03 Jun 2016 13:32:18 GMT\r\n
  Connection: keep-alive\r\n
  ETag: "575186e2-2581"\r\n
  Expires: Thu, 26 Sep 2019 09:17:53 GMT\r\n
  Cache-Control: max-age=31536000\r\n
  Accept-Ranges: bytes\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.411436000 seconds]
[Request in frame: 323]
File Data: 9601 bytes
Compuserve GIF, Version: GIF89a
```

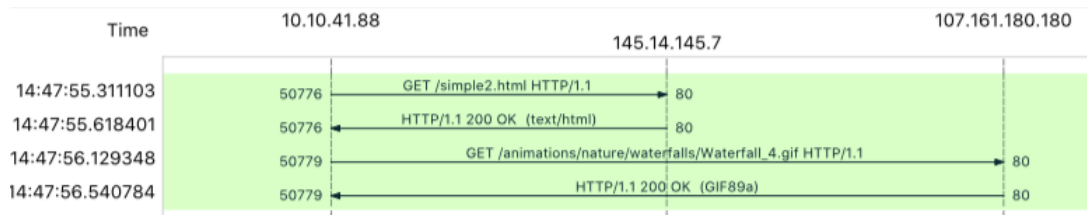
Bytes of content returned for the HTML file is 572 bytes. That for the GIF is 9601 bytes.

```
Hypertext Transfer Protocol
▶ HTTP/1.1 200 OK\r\n
  Date: Wed, 26 Sep 2018 09:17:52 GMT\r\n
  Content-Type: text/html; charset=UTF-8\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  Server: awex\r\n
  X-Xss-Protection: 1; mode=block\r\n
  X-Content-Type-Options: nosniff\r\n
  X-Request-ID: a370cb879592100b6ea0221a42134a4e\r\n
  Content-Encoding: gzip\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.307298000 seconds]
  [Request in frame: 295]
▶ HTTP chunked response
  Content-encoded entity body (gzip): 572 bytes -> 868 bytes
  File Data: 868 bytes
  Line-based text data: text/html (13 lines)
```

No. of requests sent by the browser and responded by the server are both 2, as shown below.

Topic / Item	Count	Rate (ms)	Percent	Burst rate	Burst start
▼ HTTP Requests by HTTP Host	2	0.0016	100%	0.0100	3.791
▼ cncourse.000webhostapp.com	1	0.0008	50.00%	0.0100	3.791
/simple2.html	1	0.0008	100.00%	0.0100	3.791
▼ gifgifs.com	1	0.0008	50.00%	0.0100	4.609
/animations/nature/waterfalls/Waterfall_4.gif	1	0.0008	100.00%	0.0100	4.609

HTTP Traffic Flow graph:



1.11 File *simple3.html*:

Last modified information is not available for the *simple3.html* file.

	Time	Source	Destination	Protocol	Length	Info
93	14:48:20...	10.10.41.88	145.14.145.7	HTTP	565	GET /simple3.html HTTP/1.1
103	14:48:20...	145.14.145.7	10.10.41.88	HTTP	86	HTTP/1.1 200 OK (text/html)
108	14:48:20...	10.10.41.88	145.14.145.7	HTTP	577	GET /simple1.html HTTP/1.1
109	14:48:20...	10.10.41.88	145.14.145.7	HTTP	577	GET /simple2.html HTTP/1.1
128	14:48:20...	145.14.145.7	10.10.41.88	HTTP	86	HTTP/1.1 200 OK (text/html)
137	14:48:20...	145.14.145.7	10.10.41.88	HTTP	86	HTTP/1.1 200 OK (text/html)

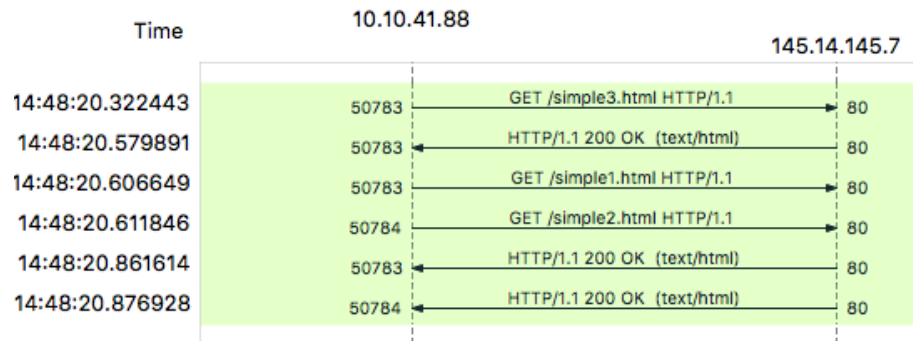
Bytes of content returned for the HTML file is 138 bytes for *simple3.html*. It also loads *simple1.html* and *simple2.html* whose sizes were mentioned earlier.

```
Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
Date: Wed, 26 Sep 2018 09:18:17 GMT\r\n
Content-Type: text/html; charset=UTF-8\r\n
Transfer-Encoding: chunked\r\n
Connection: keep-alive\r\n
Server: awex\r\n
X-Xss-Protection: 1; mode=block\r\n
X-Content-Type-Options: nosniff\r\n
X-Request-ID: 37e26d841c1af140b506268b5a254bee\r\n
Content-Encoding: gzip\r\n
\r\n
[HTTP response 1/2]
[Time since request: 0.257448000 seconds]
[Request in frame: 93]
[Next request in frame: 108]
[Next response in frame: 128]
> HTTP chunked response
Content-encoded entity body (gzip): 138 bytes -> 174 bytes
File Data: 174 bytes
Line-based text data: text/html (10 lines)
```

No. of requests sent by the browser and responded by the server are both 3, as shown below.

Topic / Item	Count	Rate (ms)	Percent	Burst rate	Burst start
▼ HTTP Requests by HTTP Host	3	0.0054	100%	0.0200	4.409
▼ cncourse.000webhostapp.com	3	0.0054	100.00%	0.0200	4.409
/simple1.html	1	0.0018	33.33%	0.0100	4.409
/simple2.html	1	0.0018	33.33%	0.0100	4.415
/simple3.html	1	0.0018	33.33%	0.0100	4.125

HTTP Traffic Flow graph:



1.12 File *simple4.html*:

```
Hypertext Transfer Protocol
▶ HTTP/1.1 200 OK\r\n
  Date: Wed, 26 Sep 2018 09:18:35 GMT\r\n
  Content-Type: image/jpeg\r\n
  Content-Length: 5193\r\n
  Connection: keep-alive\r\n
  Last-Modified: Tue, 11 Sep 2018 06:26:03 GMT\r\n
  Accept-Ranges: bytes\r\n
  Server: awex\r\n
  X-Xss-Protection: 1; mode=block\r\n
  X-Content-Type-Options: nosniff\r\n
  X-Request-ID: b77178a9b38c9f67e9cce17f8894e439\r\n
  \r\n
[HTTP response 1/2]
[Time since request: 0.277401000 seconds]
```

Last modified information is not available for the *simple4.html* file but its present for the JPEG image files loaded from another server, as shown above for one such image.

Bytes of content returned for the HTML file is 535 bytes for *simple4.html*. It also loads 10 other image files.

```
Hypertext Transfer Protocol
▶ HTTP/1.1 200 OK\r\n
  Date: Wed, 26 Sep 2018 09:18:35 GMT\r\n
  Content-Type: text/html; charset=UTF-8\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  Server: awex\r\n
  X-Xss-Protection: 1; mode=block\r\n
  X-Content-Type-Options: nosniff\r\n
  X-Request-ID: 8e7e8025b405c3b23e26b06746e7b4ec\r\n
  Content-Encoding: gzip\r\n
  \r\n
[HTTP response 1/3]
[Time since request: 0.296096000 seconds]
[Request in frame: 188]
[Next request in frame: 203]
[Next response in frame: 238]
▶ HTTP chunked response
  Content-encoded entity body (gzip): 535 bytes -> 1043 bytes
  File Data: 1043 bytes
```

No. of requests sent by the browser and responded by the server are both 11, as shown below.

Topic / Item	Count	Rate (ms)	Percent	Burst rate	Burst start
▼ HTTP Requests by HTTP Host	11	0.0089	100%	0.0600	8.509
▼ cncourse.000webhostapp.com	11	0.0089	100.00%	0.0600	8.509
/simple4.html	1	0.0008	9.09%	0.0100	7.930
/9.jpg	1	0.0008	9.09%	0.0100	8.509
/8.jpg	1	0.0008	9.09%	0.0100	8.259
/7.jpg	1	0.0008	9.09%	0.0100	8.256
/6.jpg	1	0.0008	9.09%	0.0100	8.517
/5.jpg	1	0.0008	9.09%	0.0100	8.516
/4.jpg	1	0.0008	9.09%	0.0100	8.509
/3.jpg	1	0.0008	9.09%	0.0100	8.528
/2.jpg	1	0.0008	9.09%	0.0100	8.856
/1.jpg	1	0.0008	9.09%	0.0100	8.541
/0.jpg	1	0.0008	9.09%	0.0100	8.860

HTTP Traffic Flow graph:



Whether images downloaded serially or parallelly:

The image downloads occurred *parallelly*. We can say so since in the above traffic flow graph, its clearly visible that the requests for the images 7.jpg, 8.jpg,

9.jpg, ..., all were made in a single go without waiting for response of either of the image to be available. The first response is available after 6 images were already requested.

1.13 Time required to access the pdf file:

	Time	Source	Destination	Protocol	Length	Info
139	15:18:09.780182	10.10.41.88	145.14.144.2...	HTTP	571	GET /Sec377judgment.pdf HTTP/1.1
3263	15:18:17.659664	145.14.144.2...	10.10.41.88	HTTP	1354	HTTP/1.1 200 OK (application/pdf)

Frame 3263: 1354 bytes on wire (10832 bits), 1354 bytes captured (10832 bits) on interface 0 Ethernet II, Src: Cisco_af:0c:64 (a0:3d:6f:af:0c:64), Dst: Apple_24:e0:94 (f0:79:60:24:e0:94) Internet Protocol Version 4, Src: 145.14.144.210, Dst: 10.10.41.88 Transmission Control Protocol, Src Port: 80, Dst Port: 50885, Seq: 1318341303, Ack: 2932179289, Len: 1280 [1932 Reassembled TCP Segments (2795005 bytes): #150(1448), #151(1448), #153(1317), #155(1448), #156(1448)]
Hypertext Transfer Protocol
▶ HTTP/1.1 200 OK\r\n
Date: Wed, 26 Sep 2018 09:48:06 GMT\r\n
Content-Type: application/pdf\r\n
▶ Content-Length: 2794673\r\n
Connection: keep-alive\r\n
Last-Modified: Sun, 23 Sep 2018 19:35:27 GMT\r\n
Accept-Ranges: bytes\r\n
Server: awex\r\n
X-Xss-Protection: 1; mode=block\r\n
X-Content-Type-Options: nosniff\r\n
X-Request-ID: ccc944971ee0a76d92a52876d4ff92e1\r\n
\r\n
[HTTP response 1/1]
[Time since request: 7.879482000 seconds]

The time required as highlighted = 7.88 seconds.

1.14 Table for time required to access each of the files:

S.No	File Name	Time Required to access the file (in seconds)
1.	simple1.html	0.284
2.	simple2.html	0.307
3.	simple3.html	0.257
4.	PDF file	7.88
5.	Large Text file	1.167

2 The HTTP CONDITIONAL GET/Response Interaction:

The 4 requests were captured as shown below:

Source	Destination	Protocol	Length	Info
10.10.41.88	13.75.89.224	HTTP	470	GET / HTTP/1.1
13.75.89.224	10.10.41.88	HTTP	839	HTTP/1.1 200 OK (text/html)
10.10.41.88	13.75.89.224	HTTP	668	GET / HTTP/1.1
13.75.89.224	10.10.41.88	HTTP	232	HTTP/1.1 304 Not Modified

2.1 First HTTP GET request from the browser to the server:

Time	Source	Destination	Protocol	Length	Info
1226	13:3...	10.10.41.88	13.75.89.224	HTTP	470 GET / HTTP/1.1
1345	13:3...	13.75.89.224	10.10.41.88	HTTP	839 HTTP/1.1 200 OK (text/html)
4414	13:3...	10.10.41.88	13.75.89.224	HTTP	668 GET / HTTP/1.1
4444	13:3...	13.75.89.224	10.10.41.88	HTTP	232 HTTP/1.1 304 Not Modified

Frame 1226: 470 bytes on wire (3760 bits), 470 bytes captured (3760 bits) on interface 0
Ethernet II, Src: Apple_24:e0:94 (f0:79:60:24:e0:94), Dst: Cisco_af:0c:64 (a0:3d:6f:af:0c:64)
Internet Protocol Version 4, Src: 10.10.41.88, Dst: 13.75.89.224
Transmission Control Protocol, Src Port: 50297, Dst Port: 80, Seq: 873883957, Ack: 60751268
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
Request Method: GET
Request URI: /
Request Version: HTTP/1.1
Host: sahilbansal.azurewebsites.net\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
\r\n
[Full request URI: http://sahilbansal.azurewebsites.net/]
[HTTP request 1/2]
[Response in frame: 1345]
[Next request in frame: 4414]

There is no **IF-MODIFIED-SINCE** header in this GET request.

2.2 Contents of the server response:

```
▼ 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
  ▼ Content-Length: 995\r\n
    [Content length: 995]
    Content-Type: text/html\r\n
    Content-Encoding: gzip\r\n
    Last-Modified: Wed, 16 Mar 2016 05:07:30 GMT\r\n
    Accept-Ranges: bytes\r\n
    ETag: "1d9aa2bd417fd11:0"\r\n
    Vary: Accept-Encoding\r\n
    Server: Microsoft-IIS/10.0\r\n
    X-Powered-By: ASP.NET\r\n
    Set-Cookie: ARRAffinity=51eab1e7238eef604414d12e63646b052a35a5889c1ff734327cfc
    Date: Wed, 26 Sep 2018 08:01:19 GMT\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.169716000 seconds]
    [Request in frame: 1226]
    [Next request in frame: 4414]
    [Next response in frame: 4444]
    Content-encoded entity body (gzip): 995 bytes -> 2476 bytes
    File Data: 2476 bytes
  ▼ Line-based text data: text/html (33 lines)
    \357\273\277<!DOCTYPE html>\r\n
    <HTML>\r\n
    <HEAD>\r\n
      <TITLE>\r\n
      SAHIL BANSAL\r\n
      </TITLE>\r\n
    </HEAD>\r\n
    <BODY BGCOLOR="LIGHTGREY">\r\n
      <hr color="green" size="5" /></hr>\r\n
      <center>\r\n
```

Yes, the server has explicitly responded with the content of the file since the *content length* has a positive value and also the HTML file is visible as shown.

2.3 Second HTTP GET request from the browser to the server:

```
Hypertext Transfer Protocol
▼ GET / HTTP/1.1\r\n
  ▶ [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /
    Request Version: HTTP/1.1
    Host: sahilbansal.azurewebsites.net\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 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    Cookie: ARRAffinity=51eab1e7238eef604414d12e63646b052a35a5889c1ff734327cfd28e7f
      Cookie pair: ARRAffinity=51eab1e7238eef604414d12e63646b052a35a5889c1ff734327
    If-None-Match: "1d9aa2bd417fd11:0"\r\n
  If-Modified-Since: Wed, 16 Mar 2016 05:07:30 GMT\r\n
  \r\n
  [Full request URI: http://sahilbansal.azurewebsites.net/]
  [HTTP request 2/2]
  [Prev request in frame: 1226]
  [Response in frame: 4444]
```

Yes, now we can see an **IF-MODIFIED-SINCE** header in the HTTP GET request. The value of the header is the date when the file was last modified on the server side. It shows *Wed, Mar 16, 2016* as the last modified date.

2.4 HTTP status code and phrase returned from the server in response to 2nd HTTP GET:

```
Transmission Control Protocol, Src Port: 80, Dst Port: 8027, Seq: 607
▼ 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
      Accept-Ranges: bytes\r\n
      ETag: "1d9aa2bd417fd11:0"\r\n
      Server: Microsoft-IIS/10.0\r\n
      X-Powered-By: ASP.NET\r\n
      Date: Wed, 26 Sep 2018 08:01:24 GMT\r\n
    \r\n
    [HTTP response 2/2]
    [Time since request: 0.145110000 seconds]
    [Prev request in frame: 1226]
    [Prev response in frame: 1345]
    [Request in frame: 4414]
```

The status code is **304** and the response phrase is **Not Modified** in response to the 2nd HTTP GET request. The server did not explicitly return the content of the file this time since there is no content length header visible, as well as no content visible after two cr-lf present after the Date Header.

This happens because the client sent an IF-MODIFIED GET request, in which the server responds with the content only when the file has been modified on the server after the date of previous entry of the file in the cache accessible by client. Otherwise, it just sends a 304-Not Modified response.

3 Retrieving Long Documents:

3.1 HTTP GET request messages sent by the browser:

624	05:33:14.818792	10.10.41.88	145.14.144.188	HTTP	526	GET /largeText.html HTTP/1.1
637	05:33:15.082354	145.14.144.188	10.10.41.88	HTTP	77	[TCP Previous segment not captured] Continuation
641	05:33:15.082761	145.14.144.188	10.10.41.88	HTTP	1275	Continuation
642	05:33:15.082768	145.14.144.188	10.10.41.88	HTTP	960	Continuation
645	05:33:15.083051	145.14.144.188	10.10.41.88	HTTP	616	Continuation
646	05:33:15.083058	145.14.144.188	10.10.41.88	HTTP	555	Continuation
647	05:33:15.083145	145.14.144.188	10.10.41.88	HTTP	491	Continuation
648	05:33:15.083148	145.14.144.188	10.10.41.88	HTTP	456	Continuation
649	05:33:15.083149	145.14.144.188	10.10.41.88	HTTP	457	Continuation
672	05:33:15.329014	145.14.144.188	10.10.41.88	HTTP	1514	Continuation
673	05:33:15.329019	145.14.144.188	10.10.41.88	HTTP	1514	Continuation
677	05:33:15.339258	145.14.144.188	10.10.41.88	HTTP	1514	Continuation
678	05:33:15.339444	145.14.144.188	10.10.41.88	HTTP	1514	Continuation
680	05:33:15.339723	145.14.144.188	10.10.41.88	HTTP	1514	Continuation
682	05:33:15.339887	145.14.144.188	10.10.41.88	HTTP	1514	Continuation
683	05:33:15.340203	145.14.144.188	10.10.41.88	HTTP	1514	Continuation
685	05:33:15.340403	145.14.144.188	10.10.41.88	HTTP	1514	Continuation
687	05:33:15.340682	145.14.144.188	10.10.41.88	HTTP	1514	Continuation
688	05:33:15.340882	145.14.144.188	10.10.41.88	HTTP	1514	Continuation
692	05:33:15.341645	145.14.144.188	10.10.41.88	HTTP	1514	Continuation
694	05:33:15.343412	145.14.144.188	10.10.41.88	HTTP	1514	Continuation
695	05:33:15.343649	145.14.144.188	10.10.41.88	HTTP	1514	Continuation
696	05:33:15.343653	145.14.144.188	10.10.41.88	HTTP	1514	Continuation
699	05:33:15.343822	145.14.144.188	10.10.41.88	HTTP	1514	Continuation

1066	05:33:15.892655	145.14.144.188	10.10.41.88	HTTP	1514	Continuation
1070	05:33:15.892837	145.14.144.188	10.10.41.88	HTTP	1514	Continuation
1071	05:33:15.893104	145.14.144.188	10.10.41.88	HTTP	1514	Continuation
1072	05:33:15.893108	145.14.144.188	10.10.41.88	HTTP	1514	Continuation
1073	05:33:15.893110	145.14.144.188	10.10.41.88	HTTP	1514	Continuation
1074	05:33:15.893111	145.14.144.188	10.10.41.88	HTTP	1514	Continuation
1075	05:33:15.893113	145.14.144.188	10.10.41.88	HTTP	1514	Continuation
1079	05:33:15.893344	145.14.144.188	10.10.41.88	HTTP	1514	Continuation
1080	05:33:15.893347	145.14.144.188	10.10.41.88	HTTP	1032	Continuation
4001	05:35:35.987440	10.10.41.88	145.14.145.72	HTTP	530	GET /Sec377judgment.pdf HTTP/1.1
7342	05:35:43.070363	145.14.145.72	10.10.41.88	HTTP	1058	HTTP/1.1 200 OK (application/pdf)

The browser sent 2 HTTP GET requests, one for the pdf file and other for the large text file since both requests were made in the same wireshark session. Both the requests are highlighted above. The packet numbers 624 and 4001 in the trace contain the HTTP GET message.

3.2 Packet no in trace containing the status code and phrase associated with the response to the HTTP GET request:

We receive *TCP Continuation* message for the large text file requested, as shown by packet no. 637 highlighted in black above. A **200 OK** response is received for the pdf file requested as shown below. The response is the packet no. 4001 in the above trace.

```
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: Wed, 26 Sep 2018 00:05:33 GMT\r\n
    Content-Type: application/pdf\r\n
    Content-Length: 2794673\r\n
    Connection: keep-alive\r\n
    Last-Modified: Sun, 23 Sep 2018 19:35:27 GMT\r\n
    Accept-Ranges: bytes\r\n
    Server: awex\r\n
    X-Xss-Protection: 1; mode=block\r\n
    X-Content-Type-Options: nosniff\r\n
    X-Request-ID: cad96c56148459f5d3772708bc2b4db2\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 7.082923000 seconds]
    [Request in frame: 4001]
    File Data: 2794673 bytes
  Media Type
    Media type: application/pdf (2794673 bytes)
```

3.3 Status code and phrase in the response:

The status code is **200** and the response phrase is **OK**.

3.4 No. of data-containing TCP segments needed to carry the single HTTP response and the text of the file:

145.14.144.188	10.10.41.88	HTTP	1514	Continuation
145.14.144.188	10.10.41.88	HTTP	1514	Continuation
145.14.144.188	10.10.41.88	HTTP	1514	Continuation
145.14.144.188	10.10.41.88	HTTP	1514	Continuation
145.14.144.188	10.10.41.88	HTTP	1514	Continuation
145.14.144.188	10.10.41.88	HTTP	1514	Continuation
145.14.144.188	10.10.41.88	HTTP	1514	Continuation
145.14.144.188	10.10.41.88	HTTP	1514	Continuation
145.14.144.188	10.10.41.88	HTTP	1514	Continuation
145.14.144.188	10.10.41.88	HTTP	1514	Continuation
145.14.144.188	10.10.41.88	HTTP	1514	Continuation
145.14.144.188	10.10.41.88	HTTP	1514	Continuation
145.14.144.188	10.10.41.88	HTTP	1514	Continuation
145.14.144.188	10.10.41.88	HTTP	1514	Continuation
145.14.144.188	10.10.41.88	HTTP	1514	Continuation
145.14.144.188	10.10.41.88	HTTP	1514	Continuation
10.10.41.88	145.14.145.72	HTTP	530	GET /Sec377judgment.pdf HTTP/1.1
145.14.145.72	10.10.41.88	HTTP	1058	HTTP/1.1 200 OK (application/pdf)

16 bits), 77 bytes captured (616 bits) on interface 0
54 (a0:3d:6f:af:0c:64), Dst: Apple_24:e0:94 (f0:79:60:24:e0:94)
rc: 145.14.144.188, Dst: 10.10.41.88
af 0c 64 08 00 45 20 :y\$::: = o d ·· E
e7 91 0e 90 bc 0a 0a ? · @ * · · · · · · · ·

ugVGTe.pcapng

Total HTTP packets count

Packets: 13303 · Displayed: 131 (1.0%)

In total, there are 131 HTTP packets were displayed, as shown in bottom right corner here, out of which 2 packets are for the pdf file, whereas in the remaining 129 packets, 1 is for the GET request and 1 is for the HTTP response, so, in total 127 data containing TCP segments were needed to carry the text of the file.

4 HTML Documents with CGI Script:

Source	Destination	Protocol	Length	Info
10.10.40.146	145.14.144.70	HTTP	503	GET /simple5.php HTTP/1.1
145.14.144.70	10.10.40.146	HTTP	86	HTTP/1.1 200 OK (text/html)
10.10.40.146	145.14.144.70	HTTP	457	GET /favicon.ico HTTP/1.1
145.14.144.70	10.10.40.146	HTTP	132	[TCP Previous segment not captured] Continuation
145.14.144.70	10.10.40.146	HTTP	516	Continuation
145.14.144.70	10.10.40.146	HTTP	173	[TCP Previous segment not captured] Continuation
145.14.144.70	10.10.40.146	HTTP	319	Continuation
145.14.144.70	10.10.40.146	HTTP	86	Continuation
10.10.40.146	145.14.144.70	HTTP	747	POST /simple5.php HTTP/1.1 (application/x-www-form-urlencoded)
145.14.144.70	10.10.40.146	HTTP	86	HTTP/1.1 200 OK (text/html)

4.1 Method used in the HTTP message:

GET method is used to get the simple5.php file whereas POST method is also used to send the input taken from user to the server.

4.2 No. of HTTP request messages sent by the browser:

Total 3 HTTP request messages are sent by the browser.

4.3 IPA to which the requests are sent:

The IPA to which the requests are sent is 145.14.144.70.

5 HTTP Authentication:

114	17:42:51.695865	10.10.40.146	203.109.74.71	HTTP	444	GET / HTTP/1.1
118	17:42:51.746722	203.109.74.71	10.10.40.146	HTTP	317	HTTP/1.1 302 Found
120	17:42:51.750355	10.10.40.146	203.109.74.71	HTTP	457	GET /src/login.php HTTP/1.1
128	17:42:51.845991	203.109.74.71	10.10.40.146	HTTP	1201	HTTP/1.1 200 OK (text/html)
139	17:42:51.875091	10.10.40.146	203.109.74.71	HTTP	483	GET /images/logo.jpg HTTP/1.1
196	17:42:52.024471	203.109.74.71	10.10.40.146	HTTP	614	HTTP/1.1 200 OK (JPEG JFIF image)
199	17:42:52.118840	10.10.40.146	203.109.74.71	HTTP	479	GET /favicon.ico HTTP/1.1
200	17:42:52.168985	203.109.74.71	10.10.40.146	HTTP	564	HTTP/1.1 404 Not Found (text/html)
763	17:43:24.538250	10.10.40.146	203.109.74.71	HTTP	785	POST /src/redirect.php HTTP/1.1 (a
771	17:43:24.688737	203.109.74.71	10.10.40.146	HTTP	656	HTTP/1.1 302 Found
773	17:43:24.697245	10.10.40.146	203.109.74.71	HTTP	628	GET /src/webmail.php HTTP/1.1
777	17:43:24.818452	203.109.74.71	10.10.40.146	HTTP	999	HTTP/1.1 200 OK (text/html)
781	17:43:24.851816	10.10.40.146	203.109.74.71	HTTP	608	GET /src/left_main.php HTTP/1.1
782	17:43:24.853179	10.10.40.146	203.109.74.71	HTTP	609	GET /src/right_main.php HTTP/1.1
791	17:43:25.094894	203.109.74.71	10.10.40.146	HTTP	562	HTTP/1.1 200 OK (text/html)
800	17:43:25.198865	203.109.74.71	10.10.40.146	HTTP	1100	HTTP/1.1 200 OK (text/html)
803	17:43:25.212602	10.10.40.146	203.109.74.71	HTTP	538	GET /images/sort_none.png HTTP/1.1
807	17:43:25.265041	203.109.74.71	10.10.40.146	HTTP	636	HTTP/1.1 200 OK (PNG)

5.1 Server response to the initial HTTP GET message:

```
Hypertext Transfer Protocol
▼ GET / HTTP/1.1\r\n
  ► [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /
    Request Version: HTTP/1.1
    Host: mail.svnit.ac.in\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (I
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/a
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    . . . . .
```

The status code is 302 and the response phrase is **Found**, in response to the initial GET message which is shown above.

5.2 New field included in HTTP GET message when browser sends request for 2nd time:

```
Hypertext Transfer Protocol
▼ GET /src/login.php HTTP/1.1\r\n
  ► [Expert Info (Chat/Sequence): GET /src/login.php HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /src/login.php
    Request Version: HTTP/1.1
  Host: mail.svnit.ac.in\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9\r\n
  \r\n
```

Considering the 2nd GET request sent by browser and comparing the HTTP message with previous one, we find that no new field is included.

5.3 Content of packet in wireshark where password is displayed:

```
Hypertext Transfer Protocol
  POST /src/redirect.php HTTP/1.1\r\n
  Host: mail.svnit.ac.in\r\n
  Connection: keep-alive\r\n
  Content-Length: 96\r\n
  Cache-Control: max-age=0\r\n
  Origin: http://mail.svnit.ac.in\r\n
  Upgrade-Insecure-Requests: 1\r\n
  Content-Type: application/x-www-form-urlencoded\r\n
  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,ima
  Referer: http://mail.svnit.ac.in/src/login.php\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9\r\n
  Cookie: SQMSESSID=bf64554412b1cdad1691cf0909f243a4\r\n
  \r\n
  [Full request URI: http://mail.svnit.ac.in/src/redirect.php]
  [HTTP request 1/3]
  [Response in frame: 771]
  [Next request in frame: 773]
  File Data: 96 bytes
  HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "login_username" = "dcja@coed.svnit.ac.in"
  Form item: "secretkey" = "dcj123"
    Key: secretkey
    Value: dcj123
  Form item: "is_autodetect_results" = "1"
200 2f 2a 3b 71 3d 30 2e 38 0d 0a 52 65 66 65 72 65 /*;q=0.8 ..Refere
210 72 3a 20 68 74 74 70 3a 2f 2f 6d 61 69 6c 2e 73 r: http: //mail.s
220 76 6e 69 74 2e 61 63 2e 69 6e 2f 73 72 63 2f 6c vnit.ac. in/src/l
230 6f 67 69 6e 2e 70 68 70 0d 0a 41 63 63 65 70 74 ogin.php ..Accept
240 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c -Encodin g: gzip,
250 20 64 65 66 6c 61 74 65 0d 0a 41 63 63 65 70 74 deflate ..Accept
260 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 55 53 -Languag e: en-US
270 2c 65 6e 3b 71 3d 30 2e 39 0d 0a 43 6f 6f 6b 69 ,en;q=0. 9...Cooki
280 65 3a 20 53 51 4d 53 45 53 53 49 44 3d 62 66 36 e: SQMSE SSID=bf6
290 34 35 35 34 34 31 32 62 31 63 64 61 64 31 36 39 4554412b 1cdad169
2a0 31 63 66 30 39 30 39 66 32 34 33 61 34 0d 0a 0d 1cf0909f 243a4...
2b0 0a 6c 6f 67 69 6e 5f 75 73 65 72 6e 61 6d 65 3d .login_u sername=
2c0 64 63 6a 61 25 34 30 63 6f 65 64 2e 73 76 6e 69 dcja%40c oed.svni
2d0 74 2e 61 63 2e 69 6e 26 73 65 63 72 65 74 6b 65 t.ac.in& secretke
2e0 79 3d 64 63 6a 31 32 33 26 6a 73 5f 61 75 74 6f y=dcj123 &js_auto
2f0 64 65 74 65 63 74 5f 72 65 73 75 6c 74 73 3d 31 detect_r esults=1
300 26 6a 75 73 74 5f 6c 6f 67 67 65 64 5f 69 6e 3d &just_lo gged_in=
310 31 1
```

The password is highlighted in the packet content window with light blue color.