電腦網路作業 - Wireshark_HTTP

資工二 S1154041 邱立宇

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

Ans :Browser: 1.1, Server: 1.1

Browser

```
1182 14.168225    192.168.137.163    128.119.245.12    HTTP    540 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1187 14.366654    128.119.245.12     192.168.137.163   HTTP    540 HTTP/1.1 200 OK  (text/html)
```

2. What languages (if any does your brwowser indicate that it can accept to the server? Ans: zh-Tw

```
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
      [GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /wireshark-labs/HTTP-wireshark-file1.html
    Request Version: HTTP/1.1
  Host: www-net.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  DNT: 1\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: zh-TW,zh;q=0.9\r\n
  \r\n
  [Full request URI: http://www-net.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.htm
  [HTTP request 1/1]
  [Response in frame: 1187]
```

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

Ans: My computer IP: 192.168.137.163,

gaia.cs.umass.edu server IP: 128.119.245.12

gaia.cs.umass.edu server IP

```
1182 14.168225    192.168.137.163    128.119.245.12    HTTP    540 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1187 14.366654    128.119.245.12     192.168.137.163   HTTP    540 HTTP/1.1 200 OK  (text/html)
```

My computer IP

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

Ans: 200 OK

```
1182 14.168225    192.168.137.163    128.119.245.12    HTTP    540 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.
1187 14.366654    128.119.245.12     192.168.137.163   HTTP    540 HTTP/1.1 200 OK  (text/html)
```

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

Ans: Fri, 10 Nov 2023 06:59:01

```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [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: Fri, 10 Nov 2023 11:00:58 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
  Last-Modified: Fri, 10 Nov 2023 06:59:01 GMT\r\n
  ETag: "80-609c6daf5e5c2"\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 1/1]
  [Time since request: 0.198429000 seconds]
  [Request in frame: 1182]
```

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

Ans: 128

```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [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: Fri, 10 Nov 2023 11:00:58 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
  Last-Modified: Fri, 10 Nov 2023 06:59:01 GMT\r\n
  ETag: "80-6@c6daf5e5c2"\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 1/1]
  [Time since request: 0.198429000 seconds]
  [Request in frame: 1182]
```

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 pack-listing window? If so, name one.

Ans: No, nothing is not displayed

```
Frame 1187: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface
Ethernet II, Src: TP-Link_6d:aa:c2 (34:60:f9:6d:aa:c2), Dst: IntelCor_6d:4e:e4 (58:ce:2
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.137.163
Transmission Control Protocol, Src Port: 80, Dst Port: 62625, Seq: 1, Ack: 487, Len: 48
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [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: Fri, 10 Nov 2023 11:00:58 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
  Last-Modified: Fri, 10 Nov 2023 06:59:01 GMT\r\n
  ETag: "80-609c6daf5e5c2"\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 1/1]
  [Time since request: 0.198429000 seconds]
  [Request in frame: 1182]
```

```
0030  00 ed e3 9e 00 00 48 54  54 50 2f 31
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a
0050  2c 20 31 30 20 4e 6f 76  20 32 30 32
0060  3a 30 30 3a 35 38 20 47  4d 54 0d 0a
0070  65 72 3a 20 41 70 61 63  68 65 2f 32
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70
0090  4c 2f 31 2e 30 2e 32 6b  2d 66 69 70
00a0  50 2f 37 2e 34 2e 33 33  20 6d 6f 64
00b0  6c 2f 32 2e 30 2e 31 31  20 50 65 72
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d
00d0  66 69 65 64 3a 20 46 72  69 2c 20 31
00e0  76 20 32 30 32 33 20 30  36 3a 35 39
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22
0100  30 39 63 36 64 61 66 35  65 35 63 32
0110  63 63 65 70 74 2d 52 61  6e 67 65 73
0120  74 65 73 0d 0a 43 6f 6e  74 65 6e 74
0130  67 74 68 3a 20 31 32 38  0d 0a 4b 65
0140  6c 69 76 65 3a 20 74 69  6d 65 6f 75
0150  20 6d 61 78 3d 31 30 30  0d 0a 43 6f
0160  74 69 6f 6e 3a 20 4b 65  65 70 2d 41
0170  0d 0a 43 6f 6e 74 65 6e  74 2d 54 79
0180  74 65 78 74 2f 68 74 6d  6c 3b 20 63
0190  65 74 3d 55 54 46 2d 38  0d 0a 0d 0a
01a0  6c 3e 0a 43 6f 6e 67 72  61 74 75 6c
01b0  6e 73 2e 20 20 59 6f 75  27 76 65 20
01c0  6c 6f 61 64 65 64 20 74  68 65 20 66
01d0  0a 68 74 74 70 3a 2f 2f  67 61 69 61
01e0  75 6d 61 73 73 2e 65 64  75 2f 77 69
01f0  61 72 6b 2d 6c 61 62 73  2f 48 54 54
0200  72 65 73 68 61 72 6b 2d  66 69 6c 65
0210  6d 6c 21 0a 3c 2f 68 74  6d 6c 3e 0a
```

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?

Ans: NO, there is no such thing

```
> Frame 1187: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface
> Ethernet II, Src: TP-Link_6d:aa:c2 (34:60:f9:6d:aa:c2), Dst: IntelCor_6d:4e:e4 (58:ce:2
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.137.163
> Transmission Control Protocol, Src Port: 80, Dst Port: 62625, Seq: 1, Ack: 487, Len: 48
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    v [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: Fri, 10 Nov 2023 11:00:58 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
    Last-Modified: Fri, 10 Nov 2023 06:59:01 GMT\r\n
    ETag: "80-609c6daf5e5c2"\r\n
    Accept-Ranges: bytes\r\n
  v 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 1/1]
    [Time since request: 0.198429000 seconds]
    [Request in frame: 1182]
```

9. Inspect the contents of ther server response.

Did the server explicitly return the contents of the file? How can you tell?

Ans: Yes

```
v 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 fof the seond HTTP GET request from your browse 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: 10 Nov 2023 06:59:01

```
> Frame 74: 651 bytes on wire (5208 bits), 651 bytes captured (5208 bits) on interface \Dev
> Ethernet II, Src: IntelCor_6d:4e:e4 (58:ce:2a:6d:4e:e4), Dst: TP-Link_6d:aa:c2 (34:60:f9:
> Internet Protocol Version 4, Src: 192.168.137.163, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 62746, Dst Port: 80, Seq: 487, Ack: 487, Len: 59
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    v [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
        [GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
    Host: www-net.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    DNT: 1\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-TW,zh;q=0.9\r\n
    If-None-Match: "80-609c6daf5e5c2"\r\n
    If-Modified-Since: Fri, 10 Nov 2023 06:59:01 GMT\r\n
    \r\n
    [Full request URI: http://www-net.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.htm
    [HTTP request 2/2]
    [Prev request in frame: 43]
    [Response in frame: 75]
```

11.What is the HTTP status code and phrase returned from the server in response to this second HTTP GET?

Did the serve rexplicitly return the contents of the file? Explain

Ans: It response HTTP/1.1 304 Not Modified. Server didn't return the contents of the file,since it already exist in cache

```
Hypertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
      [HTTP/1.1 304 Not Modified\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Response Version: HTTP/1.1
    Status Code: 304
    [Status Code Description: Not Modified]
    Response Phrase: Not Modified
  Date: Fri, 10 Nov 2023 11:21:28 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.
  Connection: Keep-Alive\r\n
  Keep-Alive: timeout=5, max=99\r\n
  ETag: "80-609c6daf5e5c2"\r\n
  \r\n
  [HTTP response 2/2]
  [Time since request: 0.198621000 seconds]
  [Prev request in frame: 43]
  [Prev response in frame: 45]
  [Request in frame: 74]
  [Request URI: http://www-net.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
```

12.How Manny HTTP GET request messages did your browser send?

Which packet number in the trace contains the GET message for the Bill or Rights?

Ans: 1 request message, packet number is 43

1 request, packet number = 43

43	10.722119	192.168.137.163	128.119.245.12	HTTP	540 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
45	10.920020	128.119.245.12	192.168.137.163	HTTP	540 HTTP/1.1 200 OK (text/html)

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

Ans: 45

43	10.722119	192.168.137.163	128.119.245.12	HTTP	540 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
45	10.920020	128.119.245.12	192.168.137.163	HTTP	540 HTTP/1.1 200 OK (text/html)

packet number = 45

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

Ans: 200 OK

43	10.722119	192.168.137.163	128.119.245.12	HTTP	540 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
45	10.920020	128.119.245.12	192.168.137.163	HTTP	540 HTTP/1.1 200 OK (text/html)

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

Ans: 2

```
[2 Reassembled TCP Segments (4861 bytes): #21(4356), #22(505)]
  [Frame: 21, payload: 0-4355 (4356 bytes)]
  [Frame: 22, payload: 4356-4860 (505 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 4861]
  [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a204672692c203130204e6f762032…]
```

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

To which Internet addresses were these GET requests sent?

Ans: 3 requests

Web Page: 128.119.245.12

Pearson.png: 128.119.245.12

8E Cover small.jpg: 178.79.137.164

No.	Time	Source	Destination	Protocol	Length	Info
372	31.486198	192.168.137.163	128.119.245.12	HTTP	537	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP
376	31.686541	128.119.245.12	192.168.137.163	HTTP	1355	HTTP/1.1 200 OK (text/html)
377	31.713708	192.168.137.163	128.119.245.12	HTTP	483	GET /pearson.png HTTP/1.1
383	31.915308	128.119.245.12	192.168.137.163	HTTP	761	HTTP/1.1 200 OK (PNG)
388	31.993575	192.168.137.163	178.79.137.164	HTTP	450	GET /8E_cover_small.jpg HTTP/1.1
392	32.266206	178.79.137.164	192.168.137.163	HTTP	225	HTTP/1.1 301 Moved Permanently

17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain

Ans:They were serially, since the time response are different, if it's parallel, then it should be returned at the same time

No.	Time	Source	Destination	Protocol	Length	Info
372	31.486198	192.168.137.163	128.119.245.12	HTTP	537	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
376	31.686541	128.119.245.12	192.168.137.163	HTTP	1355	HTTP/1.1 200 OK (text/html)
377	31.713708	192.168.137.163	128.119.245.12	HTTP	483	GET /pearson.png HTTP/1.1
383	31.915308	128.119.245.12	192.168.137.163	HTTP	761	HTTP/1.1 200 OK (PNG)
388	31.993575	192.168.137.163	178.79.137.164	HTTP	450	GET /8E_cover_small.jpg HTTP/1.1
392	32.266206	178.79.137.164	192.168.137.163	HTTP	225	HTTP/1.1 301 Moved Permanently

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

Ans: 401 Unauthorized

No.	Time	Source	Destination	Protocol	Length	Info
552	139.417574	192.168.137.163	128.119.245.12	HTTP	553	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
563	139.618777	128.119.245.12	192.168.137.163	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
595	193.684365	192.168.137.163	128.119.245.12	HTTP	638	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
597	193.885204	128.119.245.12	192.168.137.163	HTTP	544	HTTP/1.1 200 OK (text/html)

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

Ans: Authoriaztion field

No.	Time	Source	Destination	Protocol	Length	Info
25	2.587927	192.168.137.163	128.119.245.12	HTTP	553	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.
29	2.786700	128.119.245.12	192.168.137.163	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
235	17.967326	192.168.137.163	128.119.245.12	HTTP	638	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.
237	18.166750	128.119.245.12	192.168.137.163	HTTP	544	HTTP/1.1 200 OK (text/html)

```
> Frame 235: 638 bytes on wire (5104 bits), 638 bytes captured (5104 bits) on interface \Device\NPF_{C5DD18B5-D207-477E-9
> Ethernet II, Src: IntelCor_6d:4e:e4 (58:ce:2a:6d:4e:e4), Dst: TP-Link_6d:aa:c2 (34:60:f9:6d:aa:c2)
> Internet Protocol Version 4, Src: 192.168.137.163, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 49989, Dst Port: 80, Seq: 1, Ack: 1, Len: 584
v Hypertext Transfer Protocol
  > GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
  v Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
      Credentials: wireshark-students:network
    DNT: 1\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari,
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-excl
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-TW,zh;q=0.9\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: 237]
```