

No.	Time	Source	Destination	Protocol	Length	Info
26	4.404770	10.25.2.125	128.119.245.12	HTTP	548	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
47	4.619939	128.119.245.12	10.25.2.125	HTTP	540	HTTP/1.1 200 OK (text/html)

Transmission Control Protocol, Src Port: 52004, Dst Port: 80, Seq: 4, Len: 4, Win: 0

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\r\n]
    - [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: gaia.cs.umass.edu\r\n
  - Connection: keep-alive\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/80.0.3987.87 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;q=0.9\r\n
  - Accept-Encoding: gzip, deflate\r\n
  - Accept-Language: ru,en;q=0.9,ru-RU;q=0.8,en-US;q=0.7,da;q=0.6\r\n
  - \r\n
  - [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
  - [HTTP request 1/1]
  - [Response in frame: 47]

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: Sat, 08 Feb 2020 16:55:24 GMT\r\n
  - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod\_perl/2.0.11 Perl/v5.16.3\r\n
  - Last-Modified: Sat, 08 Feb 2020 06:59:02 GMT\r\n
  - ETag: "80-59e0b0a946492"\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
  - Content-Type: text/html; charset=UTF-8\r\n
  - \r\n
  - [HTTP response 1/1]
  - [Time since request: 0.215169000 seconds]
  - [Request in frame: 26]
  - [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
  - File Data: 128 bytes

1. Both running HTTP 1.1 (info section)
2. English, Russian
3. Computer: 10.25.2.125, Server: 128.119.245.12
4. 200 OK
5. Last-Modified: Sat, 08, Feb 2020 06:59:02 GMT
6. File Data: 128 bytes
7. Content-Length

7229	10.901876	10.25.2.125	128.119.245.12	HTTP	502 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
7241	11.116757	128.119.245.12	10.25.2.125	HTTP	784 HTTP/1.1 200 OK (text/html)
7450	22.850800	10.25.2.125	128.119.245.12	HTTP	614 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
7456	23.064530	128.119.245.12	10.25.2.125	HTTP	294 HTTP/1.1 304 Not Modified
7462	23.316740	10.25.2.125	128.119.245.12	HTTP	328 GET /favicon.ico HTTP/1.1
7467	23.530981	128.119.245.12	10.25.2.125	HTTP	539 HTTP/1.1 404 Not Found (text/html)

#### ▼ Hypertext Transfer Protocol

```
> GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: ru-KZ,ru;q=0.8,en-US;q=0.6,en;q=0.4,kk;q=0.2\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/70.0.3538.102 Safari/537.36 Edge/18.18362\r\n
Accept-Encoding: gzip, deflate\r\n
Host: gaia.cs.umass.edu\r\n
Connection: Keep-Alive\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: 7241]
```

8.No

#### ▼ 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
```

9. Yes, because there is Line-based text data

7229	10.901876	10.25.2.125	128.119.245.12	HTTP	502 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
7241	11.116757	128.119.245.12	10.25.2.125	HTTP	784 HTTP/1.1 200 OK (text/html)
7450	22.850800	10.25.2.125	128.119.245.12	HTTP	614 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
7456	23.064530	128.119.245.12	10.25.2.125	HTTP	294 HTTP/1.1 304 Not Modified
7462	23.316740	10.25.2.125	128.119.245.12	HTTP	328 GET /favicon.ico HTTP/1.1
7467	23.530981	128.119.245.12	10.25.2.125	HTTP	539 HTTP/1.1 404 Not Found (text/html)
7749	78.608738	10.25.2.125	93.184.220.29	HTTP	294 GET /MFEwTzBNMEswSTA3BgUrDgMCGgUAB8TBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHw
7752	78.680044	93.184.220.29	10.25.2.125	OCSP	430 Response

```
> Frame 7450: 614 bytes on wire (4912 bits), 614 bytes captured (4912 bits) on interface \Device\NPF_{8C9091E2-A623-48FA-BC5B-2B16CE9F487D}, id 0
> Ethernet II, Src: ASUSTekC_2e:21:96 (ac:9e:17:2e:21:96), Dst: Cisco_66:73:bf (10:05:ca:66:73:bf)
> Internet Protocol Version 4, Src: 10.25.2.125, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 53032, Dst Port: 80, Seq: 1, Ack: 1, Len: 560
```

#### ▼ Hypertext Transfer Protocol

```
> GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
Cache-Control: max-age=0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: ru-KZ,ru;q=0.8,en-US;q=0.6,en;q=0.4,kk;q=0.2\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/70.0.3538.102 Safari/537.36 Edge/18.18362\r\n
Accept-Encoding: gzip, deflate\r\n
Host: gaia.cs.umass.edu\r\n
If-Modified-Since: Sat, 08 Feb 2020 06:59:02 GMT\r\n
If-None-Match: "173-59e0b0a93bc99"\r\n
\r\n
```

10. Yes, If-Modified-Since value is equal to last one datetime field

7229	10.901876	10.25.2.125	128.119.245.12	HTTP	502	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
7241	11.116757	128.119.245.12	10.25.2.125	HTTP	784	HTTP/1.1 200 OK (text/html)
7450	22.850800	10.25.2.125	128.119.245.12	HTTP	614	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
7456	23.064530	128.119.245.12	10.25.2.125	HTTP	294	HTTP/1.1 304 Not Modified
7462	23.316740	10.25.2.125	128.119.245.12	HTTP	328	GET /favicon.ico HTTP/1.1
7467	23.530981	128.119.245.12	10.25.2.125	HTTP	539	HTTP/1.1 404 Not Found (text/html)
7749	78.608738	10.25.2.125	93.184.220.29	HTTP	294	GET /MFEwTzBNMEswSTAJBgUrDgMCGGUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z
7752	78.680044	93.184.220.29	10.25.2.125	OCSP	430	Response

```
> Frame 7456: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface \Device\NPF_{8C9091E2-A623-48FA-BC5B-2B16CE9F487D}, id 0
> Ethernet II, Src: Cisco_66:73:bf (10:05:ca:66:73:bf), Dst: ASUSTekC_2e:21:96 (ac:9e:17:2e:21:96)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.25.2.125
> Transmission Control Protocol, Src Port: 80, Dst Port: 53032, Seq: 1, Ack: 561, Len: 240
▼ Hypertext Transfer Protocol
  > HTTP/1.1 304 Not Modified\r\n
    Date: Sat, 08 Feb 2020 17:05:52 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
```

## 11. 304 Not Modified. No. Returned body absent

No.	Time	Source	Destination	Protocol	Length	Info
80	2.653225	10.25.2.125	128.119.245.12	HTTP	502	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
89	2.867279	128.119.245.12	10.25.2.125	HTTP	1514	[TCP Previous segment not captured] Continuation
91	2.868142	128.119.245.12	10.25.2.125	HTTP	535	[TCP Previous segment not captured] Continuation

```
> Frame 80: 502 bytes on wire (4016 bits), 502 bytes captured (4016 bits) on interface \Device\NPF_{8C9091E2-A623-48FA-BC5B-2B16CE9F487D}, id 0
> Ethernet II, Src: ASUSTekC_2e:21:96 (ac:9e:17:2e:21:96), Dst: Cisco_66:73:bf (10:05:ca:66:73:bf)
> Internet Protocol Version 4, Src: 10.25.2.125, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 53307, Dst Port: 80, Seq: 1, Ack: 1, Len: 448
▼ Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: ru-KZ,ru;q=0.8,en-US;q=0.6,en;q=0.4,kk;q=0.2\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/70.0.3538.102 Safari/537.36 Edge/18.18362\r\n
    Accept-Encoding: gzip, deflate\r\n
    Host: gaia.cs.umass.edu\r\n
```

12. 1, 80

13. 89

14. 200 OK

15. 2

No.	Time	Source	Destination	Protocol	Length	Info
846	6.066559	10.25.2.125	128.119.245.12	HTTP	502	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
851	6.276902	128.119.245.12	10.25.2.125	HTTP	1127	HTTP/1.1 200 OK (text/html)
853	6.284846	10.25.2.125	128.119.245.12	HTTP	503	GET /pearson.png HTTP/1.1
892	6.496544	128.119.245.12	10.25.2.125	HTTP	745	HTTP/1.1 200 OK (PNG)
896	6.498261	10.25.2.125	128.119.245.12	HTTP	517	GET /~kurose/cover_5th_ed.jpg HTTP/1.1

16. 3 requests were sent: 1-gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html; 2-gaia.cs.umass.edu/pearson.png; 3-manic.cs.umass.edu/~kurose/cover\_5th\_ed.jpg

17. No, sequential; Get HTML, asked for first image, get first image, asked for second image, get second image;

No.	Time	Source	Destination	Protocol	Length	Info
1108	17.274264	10.25.2.125	128.119.245.12	HTTP	563	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
1112	18.003861	128.119.245.12	10.25.2.125	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
1199	40.624319	10.25.2.125	128.119.245.12	HTTP	648	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
1204	40.859932	128.119.245.12	10.25.2.125	HTTP	583	HTTP/1.1 404 Not Found (text/html)
1225	41.628800	10.25.2.125	128.119.245.12	HTTP	538	GET /favicon.ico HTTP/1.1
1226	41.847566	128.119.245.12	10.25.2.125	HTTP	538	HTTP/1.1 404 Not Found (text/html)

  

>	Frame 1199: 648 bytes on wire (5184 bits), 648 bytes captured (5184 bits) on interface \Device\NPF_{8C9091E2-A623-48FA-BC5B-2B16CE9F487D}, id 0
>	Ethernet II, Src: ASUSTekC_2e:21:96 (ac:9e:17:2e:21:96), Dst: Cisco_66:73:bf (10:05:ca:66:73:bf)
>	Internet Protocol Version 4, Src: 10.25.2.125, Dst: 128.119.245.12
>	Transmission Control Protocol, Src Port: 53545, Dst Port: 80, Seq: 1, Ack: 1, Len: 594
>	Hypertext Transfer Protocol
>	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.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
>	Authorization: Basic d2lyZXNoYXJrLXN0dWRLbnRzOm5ldHdvcm0=\r\n

18. 401 Unauthorized

19. Authorization field