

HTTP

A. The Basic HTTP GET/RESPONSE interaction

No.	Source	Destination	Protocol	Length	Info
51	10.8.0.8	128.119.245.12	HTTP	460	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
55	128.119.245.12	10.8.0.8	HTTP	538	HTTP/1.1 200 OK (text/html)

▶	Frame 51: 460 bytes on wire (3680 bits), 460 bytes captured (3680 bits) on interface 0
▶	Raw packet data
▶	Internet Protocol Version 4, Src: 10.8.0.8, Dst: 128.119.245.12
▶	Transmission Control Protocol, Src Port: 46516, Dst Port: 80, Seq: 1, Ack: 1, Len: 408
▼	Hypertext Transfer Protocol
▶	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
	Host: gaia.cs.umass.edu\r\n
	User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:58.0) Gecko/20100101 Firefox/58.0\r\n
	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
	Accept-Language: en-US,en;q=0.5\r\n
	Accept-Encoding: gzip, deflate\r\n
	Connection: keep-alive\r\n
	Upgrade-Insecure-Requests: 1\r\n
	Pragma: no-cache\r\n
	Cache-Control: no-cache\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: 55]

Figure 1: HTTP GET request to <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
What languages (if any) does your browser indicate that it can accept to the server?

Answer : Both browser and server are running **HTTP version 1.1**. The languages accepted by browser are **en-us** and **en**.

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

Answer : My IP address is **10.8.0.8** and the server's is **128.119.245.12**.

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

Answer : HTTP/1.1 200 OK (text/html).

No.	Source	Destination	Protocol	Length	Info
51	10.8.0.8	128.119.245.12	HTTP	460	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
55	128.119.245.12	10.8.0.8	HTTP	538	HTTP/1.1 200 OK (text/html)

▶	Frame 55: 538 bytes on wire (4304 bits), 538 bytes captured (4304 bits) on interface 0
▶	Raw packet data
▶	Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.8.0.8
▶	Transmission Control Protocol, Src Port: 80, Dst Port: 46516, Seq: 1, Ack: 409, Len: 486
▼	Hypertext Transfer Protocol
▶	HTTP/1.1 200 OK\r\n
	Date: Sun, 18 Feb 2018 12:28:13 GMT\r\n
	Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
	Last-Modified: Sun, 18 Feb 2018 06:59:01 GMT\r\n
	Etag: "80-56571cc69bee"\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: 0.393884918 seconds]
	[Request in frame: 51]
	File Data: 128 bytes
▶	Line-based text data: text/html

Figure 2: HTTP response from <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>

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

Answer : Last-Modified: Sun, 18 Feb Jun 2018 06:59:01 GMT

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

Answer : Content-Length: 128

B. The HTTP CONDITIONAL GET/RESPONSE interaction

http					
No.	Source	Destination	Protocol	Length	Info
+	21 10.8.0.8	128.119.245.12	HTTP	460	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
+	25 128.119.245.12	10.8.0.8	HTTP	782	HTTP/1.1 200 OK (text/html)
+	75 10.8.0.8	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
+	84 128.119.245.12	10.8.0.8	HTTP	291	HTTP/1.1 304 Not Modified

▶ Frame 21: 460 bytes on wire (3680 bits), 460 bytes captured (3680 bits) on interface 0

Raw packet data

▶ Internet Protocol Version 4, Src: 10.8.0.8, Dst: 128.119.245.12

▶ Transmission Control Protocol, Src Port: 54378, Dst Port: 80, Seq: 1, Ack: 1, Len: 408

▼ Hypertext Transfer Protocol

▶ GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n

Host: gaia.cs.umass.edu\r\n

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:58.0) Gecko/20100101 Firefox/58.0\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n

Accept-Language: en-US,en;q=0.5\r\n

Accept-Encoding: gzip, deflate\r\n

Connection: keep-alive\r\n

Upgrade-Insecure-Requests: 1\r\n

Pragma: no-cache\r\n

Cache-Control: no-cache\r\n

\r\n

Figure 3: Contents of the first HTTP GET request to <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>

7. 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?

Answer : No

http					
No.	Source	Destination	Protocol	Length	Info
21	10.8.0.8	128.119.245.12	HTTP	460	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
25	128.119.245.12	10.8.0.8	HTTP	782	HTTP/1.1 200 OK (text/html)
75	10.8.0.8	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
84	128.119.245.12	10.8.0.8	HTTP	291	HTTP/1.1 304 Not Modified

▶ Frame 25: 782 bytes on wire (6256 bits), 782 bytes captured (6256 bits) on interface 0

Raw packet data

▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.8.0.8

▶ Transmission Control Protocol, Src Port: 80, Dst Port: 54378, Seq: 1, Ack: 409, Len: 730

▶ Hypertext Transfer Protocol

▼ Line-based text data: text/html

```
\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
```

Figure 4: Response message of the first HTTP GET request from <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>

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

Answer : Yes because we can see the contents in the **Line-based text data** field.

http					
No.	Source	Destination	Protocol	Length	Info
21	10.8.0.8	128.119.245.12	HTTP	460	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
25	128.119.245.12	10.8.0.8	HTTP	782	HTTP/1.1 200 OK (text/html)
75	10.8.0.8	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
84	128.119.245.12	10.8.0.8	HTTP	291	HTTP/1.1 304 Not Modified
Frame 75: 529 bytes on wire (4232 bits), 529 bytes captured (4232 bits) on interface 0					
Raw packet data					
Internet Protocol Version 4, Src: 10.8.0.8, Dst: 128.119.245.12					
Transmission Control Protocol, Src Port: 54378, Dst Port: 80, Seq: 409, Ack: 731, Len: 477					
Hypertext Transfer Protocol					
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n					
Host: gaia.cs.umass.edu\r\n					
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:58.0) Gecko/20100101 Firefox/58.0\r\n					
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n					
Accept-Language: en-US,en;q=0.5\r\n					
Accept-Encoding: gzip, deflate\r\n					
Connection: keep-alive\r\n					
Upgrade-Insecure-Requests: 1\r\n					
If-Modified-Since: Sun, 25 Feb 2018 06:59:02 GMT\r\n					
If-None-Match: "173-56603edad1986"\r\n					
Cache-Control: max-age=0\r\n					
\r\n					

Figure 5: Contents of the second HTTP GET request to <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>

9. 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? If so, what information follows the “IF-MODIFIED-SINCE:” header?

Answer : Yes. The information following the "IF-MODIFIED-SINCE:" header is: Sun, 25 Feb 2018 6:59:02 GMT which is the date of the last modification of the file from the previous get request.

http					
No.	Source	Destination	Protocol	Length	Info
21	10.8.0.8	128.119.245.12	HTTP	460	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
25	128.119.245.12	10.8.0.8	HTTP	782	HTTP/1.1 200 OK (text/html)
75	10.8.0.8	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
84	128.119.245.12	10.8.0.8	HTTP	291	HTTP/1.1 304 Not Modified
Frame 84: 291 bytes on wire (2328 bits), 291 bytes captured (2328 bits) on interface 0					
Raw packet data					
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.8.0.8					
Transmission Control Protocol, Src Port: 80, Dst Port: 54378, Seq: 731, Ack: 886, Len: 239					
Hypertext Transfer Protocol					
HTTP/1.1 304 Not Modified\r\n					
Date: Mon, 26 Feb 2018 02:18:04 GMT\r\n					
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n					
Connection: Keep-Alive\r\n					
Keep-Alive: timeout=5, max=99\r\n					
ETag: "173-56603edad1986"\r\n					
\r\n					
[HTTP response 2/2]					
[Time since request: 0.543567003 seconds]					
[Proxy request is: GET / 200]					

Figure 6: Response message of the second HTTP GET request from <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>

10. 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 contents of the file? Explain.

Answer : The status code and phrase returned from the server is **HTTP/1.1 304 Not Modified**. The server didn't return the contents of the file since the browser loaded it from its cache.