

Lab 1: HTTP

1. The Basic HTTP GET/response interaction

1. My browser running HTTP version 1.1. The server is running version 4.

The screenshot shows a Wireshark capture of an HTTP interaction. The packet list pane displays several packets, with packet 8158 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The Hypertext Transfer Protocol section is expanded, showing the request method (GET), request URI, request version (HTTP/1.1), and host (gaia.cs.umass.edu). The packet bytes pane shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
8158	33.393131	192.168.0.26	128.119.245.12	HTTP	611	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
8170	33.484746	128.119.245.12	192.168.0.26	HTTP	540	HTTP/1.1 200 OK (text/html)
8186	33.791250	192.168.0.26	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
8203	33.881682	128.119.245.12	192.168.0.26	HTTP	538	HTTP/1.1 404 Not Found (text/html)
8278	34.293479	2601:206:4200:1870::...	2600:1406:3c:392::3...	HTTP	264	GET /pkiops/certs/Microsoft%20Azure%20TLS%20Issuing...

Frame 8158: 611 bytes on wire (4888 bits), 611 bytes captured (4888 bits) on interface \Device\NPF_{45498BDF-190F-4733-AD59-08C706C} Ethernet II, Src: IntelCor_fb:80:83 (f0:77:c3:fb:80:83), Dst: Netgear_fc:76:1e (94:a6:7e:fc:76:1e)
Internet Protocol Version 4, Src: 192.168.0.26, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 49510, Dst Port: 80, Seq: 1, Ack: 1, Len: 557
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]
Request Method: GET
Request URI: /wireshark-labs/HTTP-wireshark-file1.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n

0000 94 a6 7e fc 76 1e f0 77 c3 fb 80 83 08 00 45 00 ...V..WE.
0010 02 55 8f df 40 00 80 06 00 00 c0 a8 00 1a 80 77 ..U..@...

Internet Protocol Version 4 (ip), 20 bytes | Packets: 10806 · Displayed: 6 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

2. Accept-Language: en-US, en;q=0.9\r\n

The screenshot shows a Wireshark capture of an HTTP interaction. The packet list pane displays several packets, with packet 8158 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The Hypertext Transfer Protocol section is expanded, showing the request method (GET), request URI, request version (HTTP/1.1), host (gaia.cs.umass.edu), connection (keep-alive), upgrade-insecure-requests (1), user-agent (Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36), accept (text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch), accept-encoding (gzip, deflate), accept-language (en-US,en;q=0.9), and if-none-match (80-5e9a2574beed8). The packet bytes pane shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
8158	33.393131	192.168.0.26	128.119.245.12	HTTP	611	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
8170	33.484746	128.119.245.12	192.168.0.26	HTTP	540	HTTP/1.1 200 OK (text/html)
8186	33.791250	192.168.0.26	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
8203	33.881682	128.119.245.12	192.168.0.26	HTTP	538	HTTP/1.1 404 Not Found (text/html)
8278	34.293479	2601:206:4200:1870::...	2600:1406:3c:392::3...	HTTP	264	GET /pkiops/certs/Microsoft%20Azure%20TLS%20Issuing...

Request Method: GET
Request URI: /wireshark-labs/HTTP-wireshark-file1.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9\r\nIf-None-Match: "80-5e9a2574beed8"\r\n

0000 94 a6 7e fc 76 1e f0 77 c3 fb 80 83 08 00 45 00 ...V..WE.
0010 02 55 8f df 40 00 80 06 00 00 c0 a8 00 1a 80 77 ..U..@...

Internet Protocol Version 4 (ip), 20 bytes | Packets: 10806 · Displayed: 6 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

3. My computer: 192.168.0.26

The gaia.cs.umass.edu server: 128.119.245.12

The screenshot shows the Wireshark interface with a packet capture of an HTTP GET request. The packet list pane shows several packets, with packet 8170 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The Hypertext Transfer Protocol section is expanded, showing the request method (GET), request URI, request version, host, and connection.

No.	Time	Source	Destination	Protocol	Length	Info
8150	33.393131	192.168.0.26	128.119.245.12	HTTP	611	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
8170	33.484746	128.119.245.12	192.168.0.26	HTTP	540	HTTP/1.1 200 OK (text/html)
8186	33.791250	192.168.0.26	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
8203	33.881682	128.119.245.12	192.168.0.26	HTTP	538	HTTP/1.1 404 Not Found (text/html)
8278	34.293479	2601:206:4200:1870::...	2600:1406:3c:392::3...	HTTP	264	GET /pkips/certs/Microsoft%20Azure%20TLS%20Issuing...

Packet 8170 details:

- Ethernet II, Src: IntelCor_fb:80:83 (f0:77:c3:fb:80:83), Dst: Netgear_fc:76:1e (94:a6:7e:fc:76:1e)
- Internet Protocol Version 4, Src: 192.168.0.26, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 49510, Dst Port: 80, Seq: 1, Ack: 1, Len: 557
- 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]
 - 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

Packet 8170 hex dump:

```
0060 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f  tml HTTP /1.1..Ho
0070 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73  st: gaia .cs.umas
```

HTTP Host (http.host), 25 bytes

Packets: 10806 · Displayed: 6 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

4. Status Code: 200

The screenshot shows the Wireshark interface with a packet capture of an HTTP 200 OK response. The packet list pane shows several packets, with packet 8170 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The Hypertext Transfer Protocol section is expanded, showing the response version, status code, status code description, response phrase, date, server, last-modified, and etag.

No.	Time	Source	Destination	Protocol	Length	Info
8150	33.393131	192.168.0.26	128.119.245.12	HTTP	611	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
8170	33.484746	128.119.245.12	192.168.0.26	HTTP	540	HTTP/1.1 200 OK (text/html)
8186	33.791250	192.168.0.26	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
8203	33.881682	128.119.245.12	192.168.0.26	HTTP	538	HTTP/1.1 404 Not Found (text/html)
8278	34.293479	2601:206:4200:1870::...	2600:1406:3c:392::3...	HTTP	264	GET /pkips/certs/Microsoft%20Azure%20TLS%20Issuing...

Packet 8170 details:

- Ethernet II, Src: IntelCor_fb:80:83 (f0:77:c3:fb:80:83), Dst: Netgear_fc:76:1e (94:a6:7e:fc:76:1e)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.26
- Transmission Control Protocol, Src Port: 80, Dst Port: 49510, Seq: 1, Ack: 1, Len: 557
- 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: Fri, 30 Sep 2022 21:39:33 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: Fri, 30 Sep 2022 05:59:01 GMT\r\n
 - ETag: "80-5e9deb0cb58ce"\r\n

Packet 8170 hex dump:

```
0000 f0 77 c3 fb 80 83 94 a6 7e fc 76 1e 08 00 45 20  .w.....~v...E
0010 02 0e 3d 52 40 00 1d 06 e8 31 80 77 f5 0c c0 a8  ..=R@...~1.w....
```

wireshark_Wi-Fi3BP1S1.pcapng

Packets: 10806 · Displayed: 6 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

5. File last modified on server: Fri, 30 sep 2022 05:59:01 GMT\r\n

Wireshark packet capture showing an HTTP 200 OK response. The packet list shows a GET request for /wireshark-labs/HTTP-wireshark-file1.html. The packet details pane shows the response structure, including the 'Last-Modified' header highlighted in yellow.

No.	Time	Source	Destination	Protocol	Length	Info
8158	33.393131	192.168.0.26	128.119.245.12	HTTP	611	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
8170	33.484746	128.119.245.12	192.168.0.26	HTTP	540	HTTP/1.1 200 OK (text/html)
8186	33.791250	192.168.0.26	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
8203	33.881682	128.119.245.12	192.168.0.26	HTTP	538	HTTP/1.1 404 Not Found (text/html)
8278	34.293479	2601:206:4200:1870::...	2600:1406:3c:392::3...	HTTP	264	GET /pkips/certs/Microsoft%20Azure%20TLS%20Issuing...

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: Fri, 30 Sep 2022 21:39:33 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: Fri, 30 Sep 2022 05:59:01 GMT\r\n
 - ETag: "80-5e9deb0cb58ce"\r\n

00c0 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 .16.3..L ast-Modi
00d0 66 69 65 64 3a 20 46 72 69 2c 20 33 30 20 53 65 fied: Fr i, 30 Se

HTTP Last Modified (http.last_modified), 46 bytes

Packets: 10806 · Displayed: 6 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

6. Content length: 128

Wireshark packet capture showing an HTTP 200 OK response. The packet details pane shows the response structure, including the 'Content-Length' header highlighted in yellow.

No.	Time	Source	Destination	Protocol	Length	Info
8158	33.393131	192.168.0.26	128.119.245.12	HTTP	611	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
8170	33.484746	128.119.245.12	192.168.0.26	HTTP	540	HTTP/1.1 200 OK (text/html)
8186	33.791250	192.168.0.26	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
8203	33.881682	128.119.245.12	192.168.0.26	HTTP	538	HTTP/1.1 404 Not Found (text/html)
8278	34.293479	2601:206:4200:1870::...	2600:1406:3c:392::3...	HTTP	264	GET /pkips/certs/Microsoft%20Azure%20TLS%20Issuing...

Response Phrase: OK

Date: Fri, 30 Sep 2022 21:39:33 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: Fri, 30 Sep 2022 05:59:01 GMT\r\n

ETag: "80-5e9deb0cb58ce"\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

00c0 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 .16.3..L ast-Modi
00d0 66 69 65 64 3a 20 46 72 69 2c 20 33 30 20 53 65 fied: Fr i, 30 Se

HTTP Last Modified (http.last_modified), 46 bytes

Packets: 10806 · Displayed: 6 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

7. No, I do not see any headers within the data that are not displayed in the packet-listing window.

2. The HTTP CONDITIONAL GET/response interaction

8. No, I do not see an “IF-MODIFIED-SINCE” line in the HTTP GET.

The screenshot shows a Wireshark capture of an HTTP GET request. The packet list pane displays four packets. Packet 892 is a GET request for /wireshark-labs/HTTP-wireshark-file2.html. Packet 898 is the response, which is a 200 OK (text/html). The packet details pane shows the full request URI and the response status. The packet bytes pane shows the raw data of the request and response.

No.	Time	Source	Destination	Protocol	Length	Info
892	12.111523	192.168.0.26	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
898	12.204728	128.119.245.12	192.168.0.26	HTTP	784	HTTP/1.1 200 OK (text/html)
1268	22.108577	192.168.0.26	128.119.245.12	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1273	22.203784	128.119.245.12	192.168.0.26	HTTP	294	HTTP/1.1 304 Not Modified

Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9\r\n\r\n[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

0000 94 a6 7e fc 76 1e f0 77 c3 fb 80 83 08 00 45 00 ...V..wE.
0010 02 00 90 64 40 00 80 06 00 00 c0 a8 00 1a 80 77 ...d@...w

Hypertext Transfer Protocol: Protocol | Packets: 1298 · Displayed: 4 (0.3%) · Dropped: 0 (0.0%) | Profile: Default

9. Yes, the server explicitly returns the contents of the file. As shown in the screenshot.

The screenshot shows a Wireshark capture of an HTTP GET request. The packet list pane displays four packets. Packet 892 is a GET request for /wireshark-labs/HTTP-wireshark-file2.html. Packet 898 is the response, which is a 200 OK (text/html). The packet details pane shows the full request URI and the response status. The packet bytes pane shows the raw data of the request and response.

No.	Time	Source	Destination	Protocol	Length	Info
892	12.111523	192.168.0.26	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
898	12.204728	128.119.245.12	192.168.0.26	HTTP	784	HTTP/1.1 200 OK (text/html)
1268	22.108577	192.168.0.26	128.119.245.12	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1273	22.203784	128.119.245.12	192.168.0.26	HTTP	294	HTTP/1.1 304 Not Modified

Line-based text data: text/html (10 lines)
\n<html>\n\nCongratulations again! Now you've downloaded the file lab2-2.html.
\nThis file's last modification date will not change. <p>\nThus if you download this multiple times on your browser, a complete copy
\nwill only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE
\nfield in your browser's HTTP GET request to the server.\n\n</html>\n

0000 f0 77 c3 fb 80 83 94 a6 7e fc 76 1e 08 00 45 20 ...W.....~V...E
0010 03 02 02 4e 40 00 1c 06 23 42 80 77 f5 0c c0 a8 ...N@... #B..w....

Hypertext Transfer Protocol: Protocol | Packets: 1298 · Displayed: 4 (0.3%) · Dropped: 0 (0.0%) | Profile: Default

10. Yes, I see an “IF-MODIFIED-SINCE” line in the second HTTP GET and the header contains Fri, 30 Sep 2022 05:59:01 GMT\r\n

The screenshot shows a Wireshark packet capture window titled "*Wi-Fi". The packet list pane displays four packets. Packet 1273 is selected, showing an HTTP GET request for "/wireshark-labs/HTTP-wireshark-file2.html" with a status of 304 Not Modified. The packet details pane shows the request headers, including "If-Modified-Since: Fri, 30 Sep 2022 05:59:01 GMT\r\n". The packet bytes pane shows the raw data of the request line.

No.	Time	Source	Destination	Protocol	Length	Info
892	12.111523	192.168.0.26	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
898	12.204728	128.119.245.12	192.168.0.26	HTTP	784	HTTP/1.1 200 OK (text/html)
1268	22.108577	192.168.0.26	128.119.245.12	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1273	22.203784	128.119.245.12	192.168.0.26	HTTP	294	HTTP/1.1 304 Not Modified

Upgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9\r\nIf-None-Match: "173-5e9deb0cb4d16"\r\nIf-Modified-Since: Fri, 30 Sep 2022 05:59:01 GMT\r\n\r\n[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]\r\n[HTTP request 1/1]\r\n[Response in frame: 1273]

0240 30 63 62 34 64 31 36 22 0d 0a 49 66 2d 4d 6f 64 0cb4d16" ..If-Mod\r\n0250 69 66 69 65 64 2d 53 69 6e 63 65 3a 20 46 72 69 ified-Si nce: Fri

Request line (http.request.line), 50 bytes | Packets: 1298 · Displayed: 4 (0.3%) · Dropped: 0 (0.0%) | Profile: Default

11. Status Code: 304 and phrase returned: Not Modified. No, the server does not explicitly return the contents of the file.

The screenshot shows a Wireshark packet capture window titled "*Wi-Fi". The packet list pane displays four packets. Packet 1273 is selected, showing an HTTP 304 Not Modified response. The packet details pane shows the response headers, including "Status Code: 304" and "Response Phrase: Not Modified". The packet bytes pane shows the raw data of the response.

No.	Time	Source	Destination	Protocol	Length	Info
892	12.111523	192.168.0.26	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
898	12.204728	128.119.245.12	192.168.0.26	HTTP	784	HTTP/1.1 200 OK (text/html)
1268	22.108577	192.168.0.26	128.119.245.12	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1273	22.203784	128.119.245.12	192.168.0.26	HTTP	294	HTTP/1.1 304 Not Modified

Hypertext Transfer Protocol

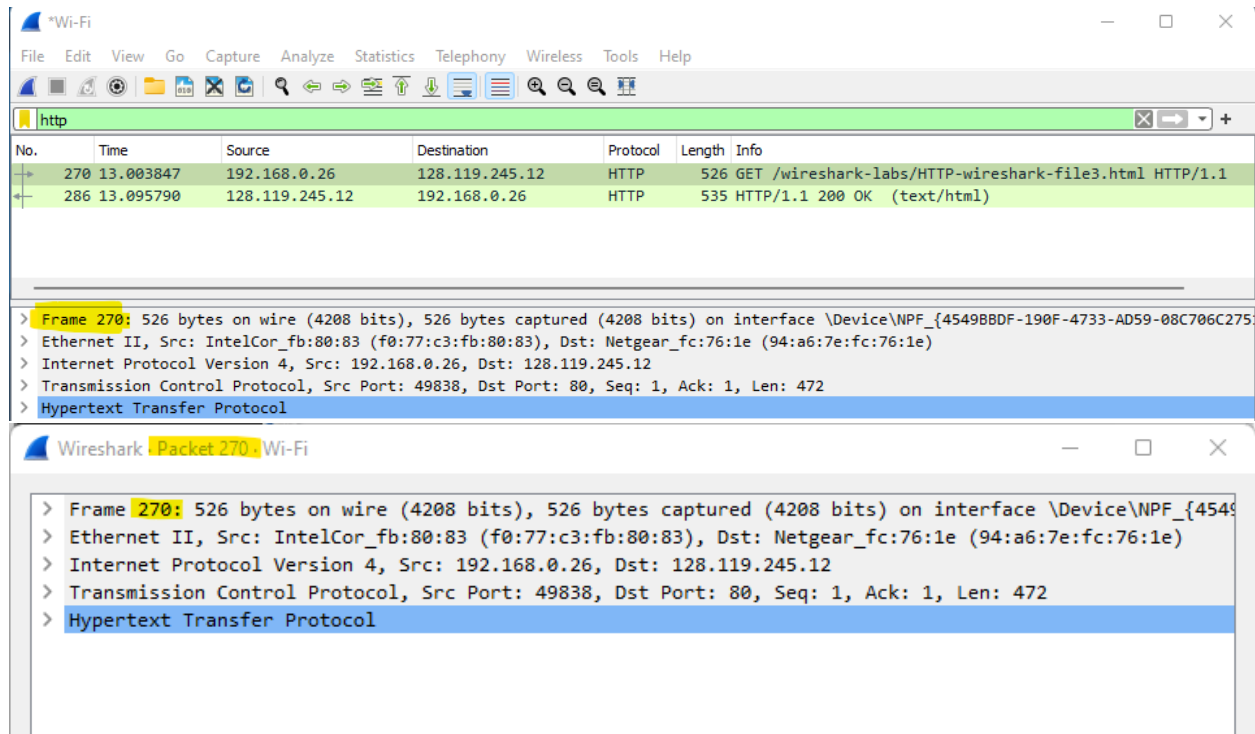
- HTTP/1.1 304 Not Modified\r\n
 - [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
 - Response Version: HTTP/1.1
 - Status Code: 304
 - [Status Code Description: Not Modified]
 - Response Phrase: Not Modified
 - Date: Fri, 30 Sep 2022 22:34:11 GMT\r\n
 - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips 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

0000 f0 77 c3 fb 80 83 94 a6 7e fc 76 1e 08 00 45 20 ..W.....~V...E\r\n0010 01 18 9b ba 40 00 1d 06 8a bf 80 77 f5 0c c0 a8 ...@... ..W....

Hypertext Transfer Protocol: Protocol | Packets: 1298 · Displayed: 4 (0.3%) · Dropped: 0 (0.0%) | Profile: Default

3. Retrieving Long Documents

12. One HTTP GET request message my browser sent. Packet number: 270

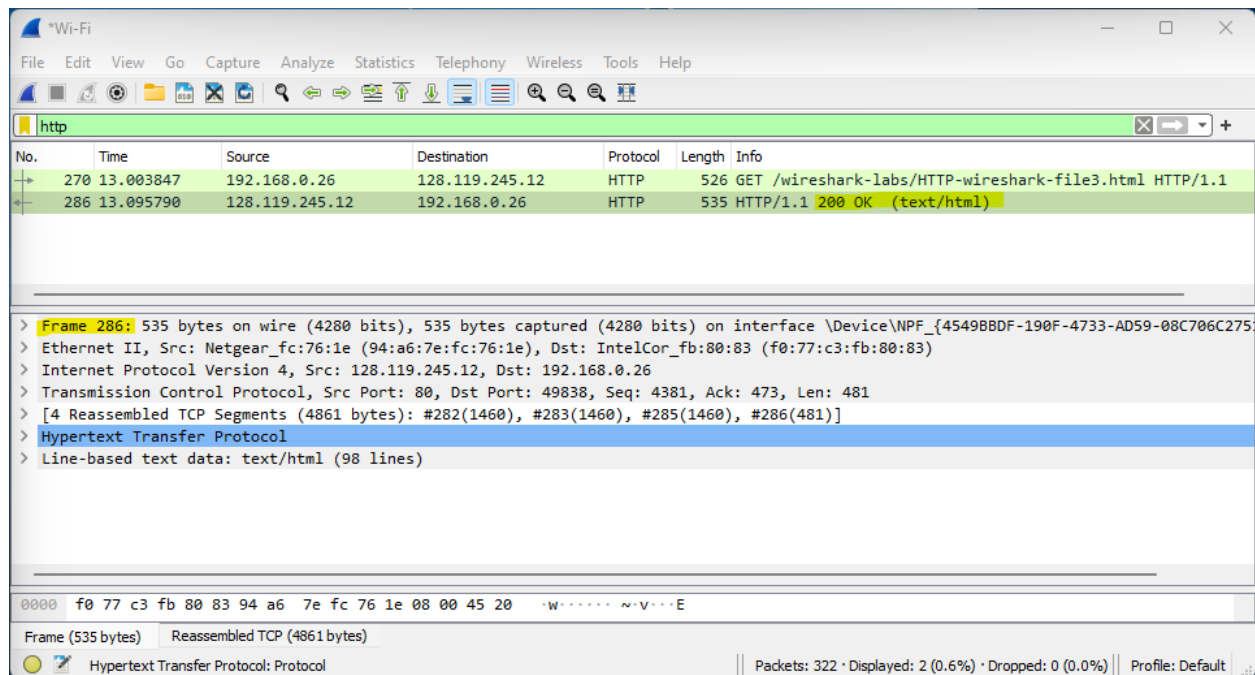


The image shows two screenshots of the Wireshark network protocol analyzer. The top screenshot displays a packet list with two entries: packet 270 (13.003847) and packet 286 (13.095790). Packet 270 is an HTTP GET request to /wireshark-labs/HTTP-wireshark-file3.html. Packet 286 is an HTTP 200 OK response. The bottom screenshot shows the detailed view of packet 270, highlighting the Hypertext Transfer Protocol section.

No.	Time	Source	Destination	Protocol	Length	Info
270	13.003847	192.168.0.26	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
286	13.095790	128.119.245.12	192.168.0.26	HTTP	535	HTTP/1.1 200 OK (text/html)

Frame 270: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface \Device\NPF_{45498BDF-190F-4733-AD59-08C706C275} Ethernet II, Src: IntelCor_fb:80:83 (f0:77:c3:fb:80:83), Dst: Netgear_fc:76:1e (94:a6:7e:fc:76:1e) Internet Protocol Version 4, Src: 192.168.0.26, Dst: 128.119.245.12 Transmission Control Protocol, Src Port: 49838, Dst Port: 80, Seq: 1, Ack: 1, Len: 472 Hypertext Transfer Protocol

13. Packet number: 286 contains the status code and phrase associated with the response.



The image shows two screenshots of the Wireshark network protocol analyzer. The top screenshot displays a packet list with two entries: packet 270 (13.003847) and packet 286 (13.095790). Packet 286 is an HTTP 200 OK response. The bottom screenshot shows the detailed view of packet 286, highlighting the Hypertext Transfer Protocol section and the line-based text data.

No.	Time	Source	Destination	Protocol	Length	Info
270	13.003847	192.168.0.26	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
286	13.095790	128.119.245.12	192.168.0.26	HTTP	535	HTTP/1.1 200 OK (text/html)

Frame 286: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{45498BDF-190F-4733-AD59-08C706C275} Ethernet II, Src: Netgear_fc:76:1e (94:a6:7e:fc:76:1e), Dst: IntelCor_fb:80:83 (f0:77:c3:fb:80:83) Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.26 Transmission Control Protocol, Src Port: 80, Dst Port: 49838, Seq: 4381, Ack: 473, Len: 481 [4 Reassembled TCP Segments (4861 bytes): #282(1460), #283(1460), #285(1460), #286(481)] Hypertext Transfer Protocol Line-based text data: text/html (98 lines)

0000 f0 77 c3 fb 80 83 94 a6 7e fc 76 1e 08 00 45 20 -W.....~V...E

Frame (535 bytes) Reassembled TCP (4861 bytes)

Hypertext Transfer Protocol: Protocol

Packets: 322 · Displayed: 2 (0.6%) · Dropped: 0 (0.0%) Profile: Default

14. Status Code: 200 and Response Phrase: OK

The screenshot shows a Wireshark capture of an HTTP transaction. The packet list at the top shows two packets: a GET request (No. 270) and a 200 OK response (No. 286). The response packet is selected, and the packet details pane shows the following information:

- 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: Fri, 30 Sep 2022 22:52:05 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: Fri, 30 Sep 2022 05:59:01 GMT\r\n
 - Etag: "1194-5e9deb0cafef5"\r\n

The packet bytes pane shows the raw data of the response, and the packet summary pane shows the frame and reassembled TCP segments.

15. 4 TCP segments

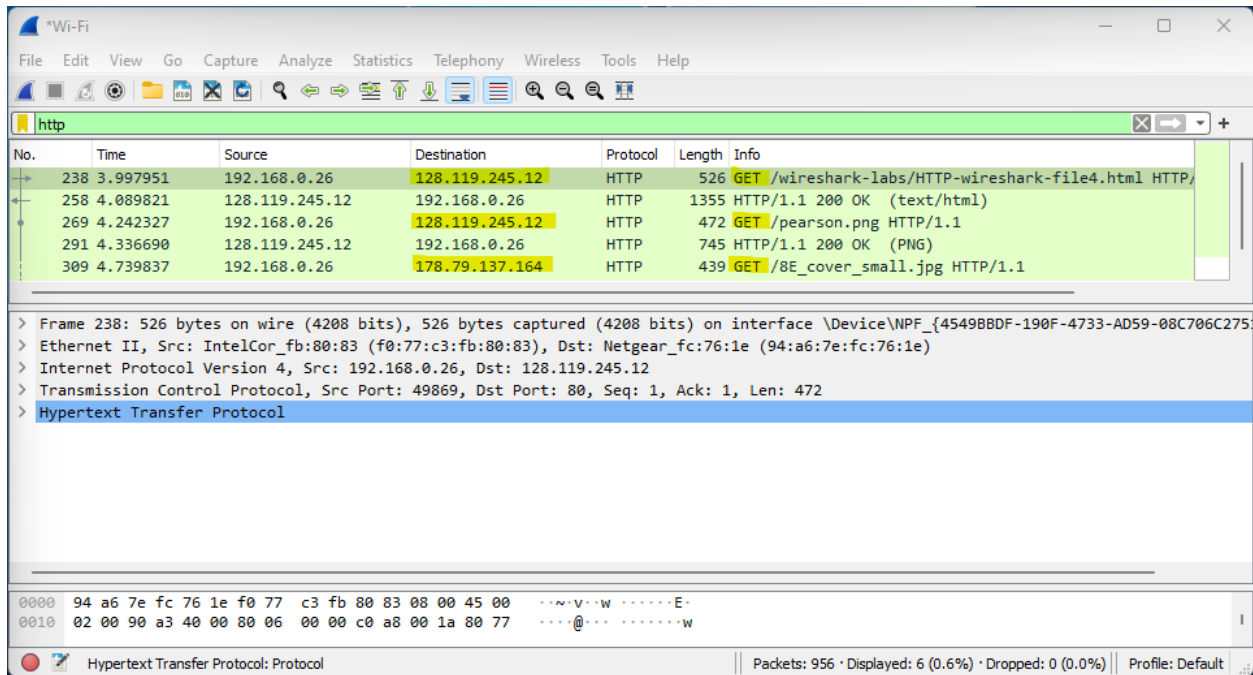
The screenshot shows a Wireshark capture of an HTTP transaction. The packet list at the top shows two packets: a GET request (No. 270) and a 200 OK response (No. 286). The response packet is selected, and the packet details pane shows the following information:

- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.26**
- Transmission Control Protocol, Src Port: 80, Dst Port: 49838, Seq: 4381, Ack: 473, Len: 481**
- [4 Reassembled TCP Segments] (4861 bytes): #282(1460), #283(1460), #285(1460), #286(481)]**
 - [Frame: 282, payload: 0-1459 (1460 bytes)]
 - [Frame: 283, payload: 1460-2919 (1460 bytes)]
 - [Frame: 285, payload: 2920-4379 (1460 bytes)]
 - [Frame: 286, payload: 4380-4860 (481 bytes)]
 - [Segment count: 4]
 - [Reassembled TCP length: 4861]
 - [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a204672692c203330205365702032...]
- Hypertext Transfer Protocol**

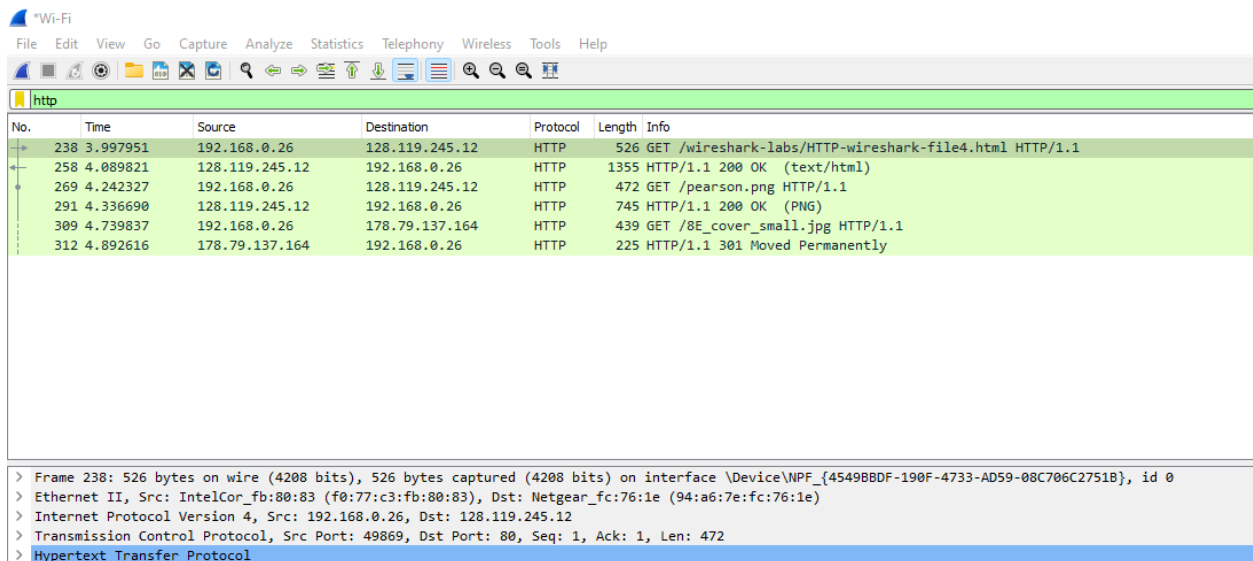
The packet bytes pane shows the raw data of the response, and the packet summary pane shows the frame and reassembled TCP segments.

4. HTML Documents with Embedded Objects

16. 3 HTTP GET requests messages my browser sent. The internet addresses where GET requests were sent are highlighted in the screenshot below.

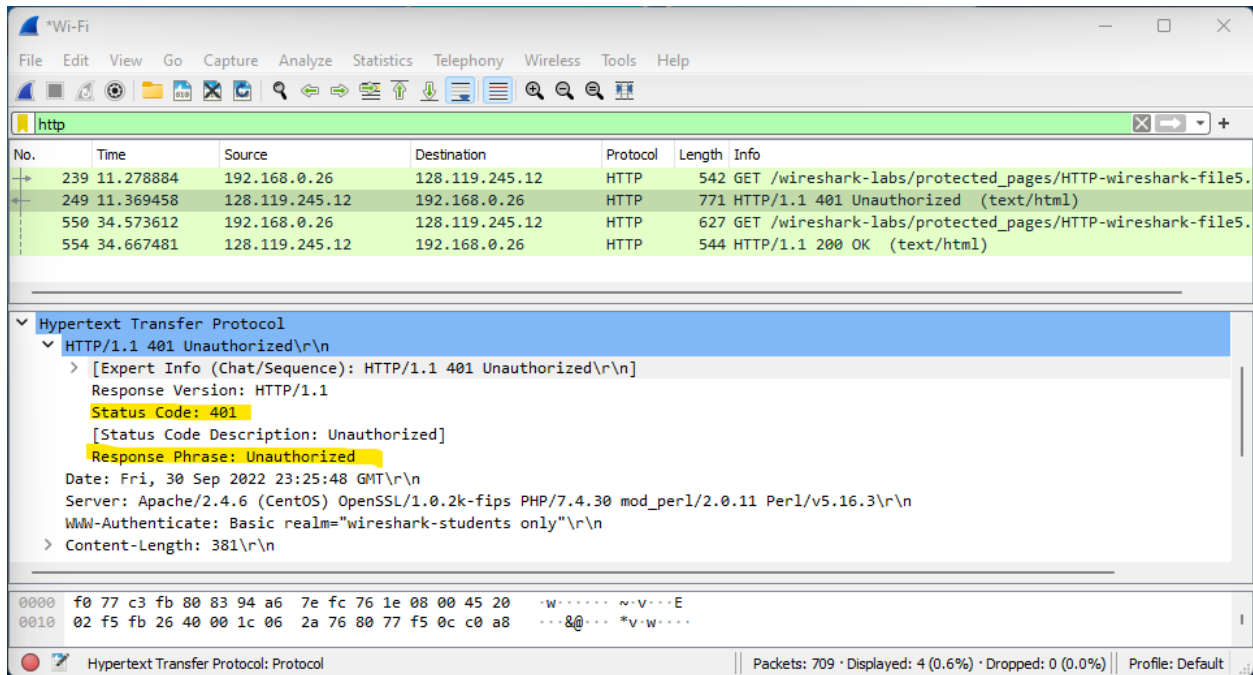


17. The browser downloaded the two images in serially. I believe this to be the case because the first image was requested and sent before the second image was requested by the browser. Had they been running in parallel, both files would have been requested then would have returned in the same time period. In this case however, the second image was only requested after the first image came back.



5. HTTP Authentication

18. Response to the initial HTTP GET message is status code: 401 and Response Phrase: Unauthorized



19. New field is Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcm5=\r\n Credentials: wireshark-students:network. The image below shows it.

