

CPS 706 - Wireshark HTTP

| No. | Time | Source | Destination | Protocol |
|-----|--------------------|----------------|----------------|----------|
| 39 | 14:24:04.347319464 | 10.0.2.5 | 128.119.245.12 | HTTP |
| 64 | 14:24:04.728409779 | 128.119.245.12 | 10.0.2.5 | HTTP |
| 69 | 14:24:05.159475936 | 10.0.2.5 | 128.119.245.12 | HTTP |
| 74 | 14:24:05.282867457 | 128.119.245.12 | 10.0.2.5 | HTTP |

Linux cooked capture
 Internet Protocol Version 4, Src: 10.0.2.5, Dst: 128.119.245.12
 Transmission Control Protocol, Src Port: 54420, Dst Port: 80, Seq: 857206604, Ac
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 i686; rv:60.0) Gecko/20100101 Fire
 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
 \r\n
 [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file
 HTTP request 1/11

0030 50 18 72 10 83 0e 00 00 47 45 54 20 2f 77 69 72 P.r.... GET /wir
 0040 65 73 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 eshark-l abs/HTT
 0050 2d 77 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 -wiresha rk-file1
 0060 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a .html HT TP/1.1..
 0070 48 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d Host: ga ia.cs.um

- Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
 - HTTP Version 1.1
- What languages (if any) does your browser indicate that it can accept to the server?
 - En-us (US English)
- What is the IP address of your computer? Of the gaia.cs.umass.edu server?
 - Computer IP address: 10.0.2.5
 - Gaia.cs.umass.edu server: 128.119.245.12

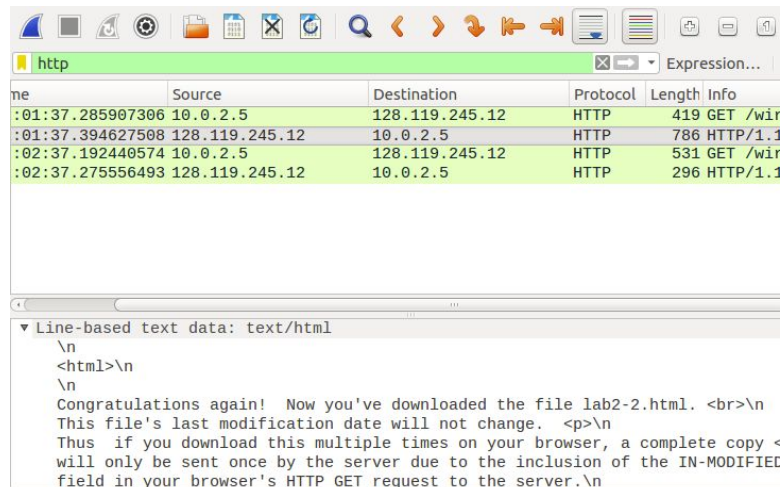
| No. | Time | Source | Destination | Protocol |
|-----|--------------------|----------------|-------------|----------|
| 190 | 14:27:00.326816489 | 128.119.245.12 | 10.0.2.5 | HTTP |
| 193 | 14:27:00.343055284 | 128.119.245.12 | 10.0.2.5 | OCSP |
| 199 | 14:27:00.343055284 | 128.119.245.12 | 10.0.2.5 | OCSP |

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.5
 Transmission Control Protocol, Src Port: 80, Dst Port: 54420, Seq: 1262
Hypertext Transfer Protocol
 HTTP/1.1 200 OK\r\n
 Date: Tue, 21 Jan 2020 19:24:06 GMT\r\n
 Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl
 Last-Modified: Tue, 21 Jan 2020 06:59:04 GMT\r\n
 ETag: "80-59ca0f1814470"\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 1/11

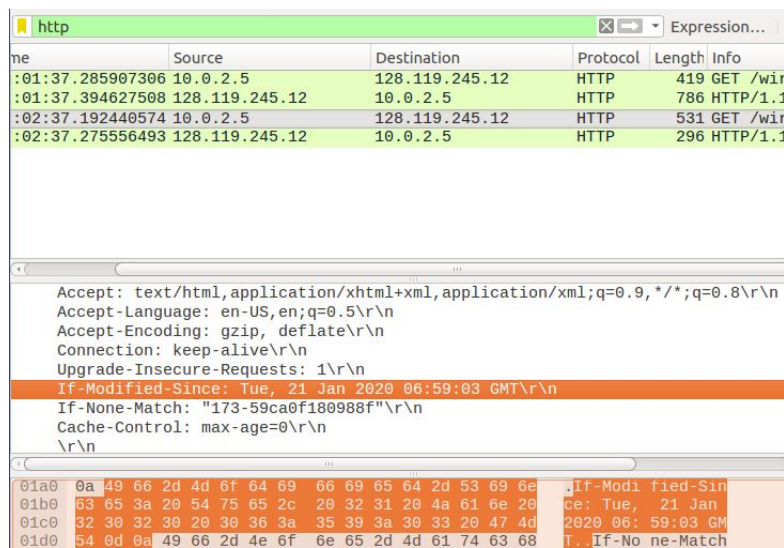
0030 50 18 7e 95 f1 2a 00 00 48 54 54 50 2f 31 2e 31 P... HTTP/1.
 0040 20 32 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 200 OK. .Date:

- What is the status code returned from the server to your browser?
 - 200 OK

5. *When was the HTML file that you are retrieving last modified at the server?*
 - Last-modified: Tue, 21 Jan 2020 06:59:04
6. *How many bytes of content are being returned to our browser?*
 - Content-length: 128 bytes
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 packet-listing window? If so, name one*
 - No. All the raw data are also displayed in the packet-listing window



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?*
 - No
9. *Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?*
 - Yes, it provided the line-based text data (the HTML file)



10. 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?

- Yes. The information that follows the header includes the last modification date
- If-Modified-Since: Tue, 21 Jan 2020 06:50:03 GMT

| Time | Source | Destination | Protocol | Length | Info |
|-----------------|----------------|----------------|----------|--------|----------|
| 01:37.285907306 | 10.0.2.5 | 128.119.245.12 | HTTP | 419 | GET /wir |
| 01:37.394627508 | 128.119.245.12 | 10.0.2.5 | HTTP | 786 | HTTP/1.1 |
| 02:37.192440574 | 10.0.2.5 | 128.119.245.12 | HTTP | 531 | GET /wir |
| 02:37.275556493 | 128.119.245.12 | 10.0.2.5 | HTTP | 296 | HTTP/1.1 |

| |
|--|
| Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.5 |
| Transmission Control Protocol, Src Port: 80, Dst Port: 39306, Seq: 65720, Ack: |
| Hypertext Transfer Protocol |
| HTTP/1.1 304 Not Modified\r\n |
| Date: Wed, 22 Jan 2020 03:02:38 GMT\r\n |
| Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 |
| Connection: Keep-Alive\r\n |
| Keep-Alive: timeout=5, max=100\r\n |
| ETag: "173-59ca0f180988f"\r\n |

| | | | |
|------|-------------------------|-------------------------|-------------------|
| 0030 | 50 18 7e 25 6f b4 00 00 | 48 54 54 50 2f 31 2e 31 | P.~%o... HTTP/1.1 |
| 0040 | 20 33 30 34 20 4e 6f 74 | 20 4d 6f 64 69 66 69 65 | 304 Not Modifie |
| 0050 | 64 0d 0a 44 61 74 65 3a | 20 57 65 64 2c 20 32 32 | d..Date: Wed, 22 |
| 0060 | 20 4a 61 6e 20 32 30 32 | 30 20 30 33 3a 30 32 3a | Jan 2020 03:02: |
| 0070 | 33 38 20 47 4d 54 0d 0a | 53 65 72 76 65 72 3a 20 | 38 GMT.. Server: |
| 0080 | 41 70 61 63 68 65 2f 32 | 2e 34 2e 36 20 28 43 65 | Apache/2.4.6 (Ce |

11. 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.

- 304 Not Modified
- No, the server did not return the contents of the file which can be seen based on the difference in content-length between the first and second HTTP reply
- It is not being sent again because of the inclusion of the “If-Modified-Since” field in the second HTTP GET

| No. | Time | Source | Destination | Protocol |
|-----|--------------------|-----------------|-----------------|----------|
| 15 | 22:47:29.866830305 | 10.0.2.5 | 128.119.245.12 | HTTP |
| 16 | 22:47:29.868291034 | 207.164.234.129 | 10.0.2.5 | DNS |
| 17 | 22:47:29.868319965 | 10.0.2.5 | 207.164.234.129 | ICMP |
| 18 | 22:47:29.912944556 | 192.168.2.1 | 10.0.2.5 | DNS |
| 19 | 22:47:29.913053423 | 127.0.1.1 | 127.0.0.1 | DNS |
| 20 | 22:47:30.046326640 | 128.119.245.12 | 10.0.2.5 | TCP |
| 21 | 22:47:30.046358219 | 10.0.2.5 | 128.119.245.12 | TCP |
| 22 | 22:47:30.046599293 | 128.119.245.12 | 10.0.2.5 | TCP |
| 23 | 22:47:30.046606670 | 10.0.2.5 | 128.119.245.12 | TCP |

| | | | | |
|---|--|--|--|--|
| Transmission Control Protocol, Src Port: 80, Dst Port: 39360, Seq: 139160, Ack: 39360 | | | | |
| [3 Reassembled TCP Segments (4861 bytes): #20(2920), #22(1460), #24(481)] | | | | |
| [Frame: 20, payload: 0-2919 (2920 bytes)] | | | | |
| [Frame: 22, payload: 2920-4379 (1460 bytes)] | | | | |
| [Frame: 24, payload: 4380-4860 (481 bytes)] | | | | |
| [Segment count: 3] | | | | |
| [Reassembled TCP length: 4861] | | | | |
| [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2057...] | | | | |
| Hypertext Transfer Protocol | | | | |
| HTTP/1.1 200 OK\r\n | | | | |

| | | |
|------|---|-------------------------------------|
| 0000 | 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d | HTTP/1.1 200 OK. |
| 0010 | 0a 44 61 74 65 3a 20 57 65 64 2c 20 32 32 20 4a | .Date: Wed, 22 Jun 2020 03:47:29 |
| 0020 | 61 6e 20 32 30 32 30 20 30 33 3a 34 37 3a 32 39 | GMT. Server: Apache/2.4.18 (Ubuntu) |
| 0030 | 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70 | |

12. How many HTTP GET request messages were sent by your browser?
 - One HTTP GET request
13. How many data-containing TCP segments were needed to carry the single HTTP response?
 - 3 TCP segments were needed
14. What is the status code and phrase associated with the response to the HTTP GET request?
 - 200 OK
15. Are there any HTTP status lines in the transmitted data associated with a TCP-induced "Continuation"?
 - No

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------------|----------------|----------------|----------|--------|----------------|
| 7 | 22:44:10.292374245 | 10.0.2.5 | 128.119.245.12 | HTTP | 417 | GET / HTTP/1.1 |
| 14 | 22:44:10.562757281 | 128.119.245.12 | 10.0.2.5 | HTTP | 1127 | 200 OK |
| 18 | 22:44:10.661713300 | 10.0.2.5 | 128.119.245.12 | HTTP | 374 | GET / HTTP/1.1 |
| 23 | 22:44:10.668531099 | 10.0.2.5 | 128.119.245.12 | HTTP | 388 | GET / HTTP/1.1 |
| 32 | 22:44:10.820207879 | 128.119.245.12 | 10.0.2.5 | HTTP | 745 | 200 OK |
| 72 | 22:44:16.621991560 | 128.119.245.12 | 10.0.2.5 | HTTP | 5240 | 200 OK |

| | | | | | | |
|--|--|--|--|--|--|--|
| Transmission Control Protocol, Src Port: 37228, Dst Port: 80, Seq: 1201450752, Ack: 39360 | | | | | | |
| Hypertext Transfer Protocol | | | | | | |
| GET /pearson.png HTTP/1.1\r\n | | | | | | |
| Host: gaia.cs.umass.edu\r\n | | | | | | |
| User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0\r\n | | | | | | |
| Accept: */*\r\n | | | | | | |
| Accept-Language: en-US,en;q=0.5\r\n | | | | | | |
| Accept-Encoding: gzip, deflate\r\n | | | | | | |
| Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html\r\n | | | | | | |

16. How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent?
 - 3 HTTP GET request messages were sent
 - Internet address: 128.119.245.12

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.

- The browser downloaded the 2 images serially because the HTTP responses were received at different times (one came after the other).
- First response at 22:44:10
- Second response at 22:44:16

| | Source | Destination | Protocol | Length | Info |
|----------------|----------------|----------------|----------|--------|--------------|
| 3:47.811868757 | 10.0.2.5 | 128.119.245.12 | HTTP | 433 | GET /wire... |
| 3:48.115012237 | 128.119.245.12 | 10.0.2.5 | HTTP | 771 | HTTP/1.1 ... |
| 4:15.537369866 | 10.0.2.5 | 128.119.245.12 | HTTP | 492 | GET /wire... |
| 4:15.674423802 | 128.119.245.12 | 10.0.2.5 | HTTP | 544 | HTTP/1.1 ... |
| 4:16.412465302 | 10.0.2.5 | 128.119.245.12 | HTTP | 358 | GET /favi... |
| 4:16.466903999 | 128.119.245.12 | 10.0.2.5 | HTTP | 538 | HTTP/1.1 ... |
| 4:16.489314627 | 10.0.2.5 | 128.119.245.12 | HTTP | 298 | GET /favi... |
| 4:16.533527451 | 128.119.245.12 | 10.0.2.5 | HTTP | 538 | HTTP/1.1 ... |

▶ Frame 51: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface
 ▶ Ethernet II, Src: RealtekU_12:35:00 (52:54:00:12:35:00), Dst: PcsCompu_24:f1:88 (08:00:27:24:f1:88)
 ▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.5
 ▶ Transmission Control Protocol, Src Port: 80, Dst Port: 44296, Seq: 10943, Ack: 4268
 ▶ Hypertext Transfer Protocol
 ▶ HTTP/1.1 401 Unauthorized\r\n
 Date: Fri, 31 Jan 2020 20:13:48 GMT\r\n
 Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/5.10.1
 WWW-Authenticate: Basic realm="wireshark-students only"\r\n
 Content-Length: 304\r\n

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

- 401 Unauthorized

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

- Authorization Field
Authorization: Basic d2lyZXNoYXJrLXN0dWRIbnRzOm5ldHdvcm5z=\r\n
Credentials: wireshark-students:network