Jakub Szpunar
CS4480
WS Lab 2

1) Both the browser and server are running HTTP v1.1 (See red highlights in packets).
2) Browser indicates it can accept US English and regular English (See orange highlights)
3) My computer's IP is 192.168.11.41. The server's ip is 128.119.245.12. (See violet highlight)
4) Status code 200 (OK). (See yellow highlight).
5) The file was last modified 01/17/2013 (See green highlight).
6) 128 bytes of content are being returned (See blue highlight).
7) Looking through the raw data, I don't see anything that wireshark did not sniff out automatically.

No. Time Source Destination Protocol Length Info
12 1.086094000 **192.168.11.41** **128.119.245.12** HTTP 443 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

Frame 12: 443 bytes on wire (3544 bits), 443 bytes captured (3544 bits) on interface 0
Ethernet II, Src: AsustekC_40:d8:45 (f4:6d:04:40:d8:45), Dst: Buffalo_b3:f7:46 (00:24:a5:b3:f7:46)
Internet Protocol Version 4, Src: 192.168.11.41 (192.168.11.41), Dst: 128.119.245.12 (128.119.245.12)
Transmission Control Protocol, Src Port: 46560 (46560), Dst Port: http (80), Seq: 1, Ack: 1, Len: 389
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
User-Agent: Opera/9.80 (Windows NT 6.2; WOW64) Presto/2.12.388 Version/12.12\r\n
Host: gaia.cs.umass.edu\r\n
Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/webp, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1\r\n
Accept-Language: en-US,en;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]

No. Time Source Destination Protocol Length Info
15 1.160651000 128.119.245.12 192.168.11.41 HTTP 482 HTTP/1.1 200 OK (text/html)

Frame 15: 482 bytes on wire (3856 bits), 482 bytes captured (3856 bits) on interface 0

Ethernet II, Src: Buffalo_b3:f7:46 (00:24:a5:b3:f7:46), Dst: AsustekC_40:d8:45 (f4:6d:04:40:d8:45)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.11.41 (192.168.11.41)
Transmission Control Protocol, Src Port: http (80), Dst Port: 46560 (46560), Seq: 1, Ack: 390, Len: 428
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
Request Version: HTTP/1.1
Status Code: 200
Response Phrase: OK
Date: Thu, 17 Jan 2013 02:16:14 GMT\r\n
Server: Apache/2.2.3 (CentOS)\r\n
Last-Modified: Thu, 17 Jan 2013 02:16:01 GMT\r\n
ETag: "8734d-80-937cba40"\r\n
Accept-Ranges: bytes\r\n
Content-Length: **128\r\n**
Keep-Alive: timeout=10, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
Line-based text data: text/html
<html>\n
Congratulations. You've downloaded the file \n
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
</html>\n

8) I don’t see any if-modified-since line.

9) The server explicitly returned the file; under line based data it is seen. (Red highlight)

10) I don’t see that line. My browser added a cache-control line though. (Green highlight)

11) Result was explicitly returned, no caching occurred. (Blue highlight)

No. Time Source Destination Protocol Length Info
14 1.426211000 192.168.11.41 128.119.245.12 HTTP 443 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1

Frame 14: 443 bytes on wire (3544 bits), 443 bytes captured (3544 bits) on interface 0
Ethernet II, Src: AsustekC_40:d8:45 (f4:6d:04:40:d8:45), Dst: Buffalo_b3:f7:46 (00:24:a5:b3:f7:46)
Internet Protocol Version 4, Src: 192.168.11.41 (192.168.11.41), Dst: 128.119.245.12 (128.119.245.12)
Transmission Control Protocol, Src Port: 46934 (46934), Dst Port: http (80), Seq: 1, Ack: 1, Len: 389
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
Request Method: GET
Request URI: /wireshark-labs/HTTP-wireshark-file2.html
Request Version: HTTP/1.1
User-Agent: Opera/9.80 (Windows NT 6.2; WOW64) Presto/2.12.388 Version/12.12\r\n
Host: gaia.cs.umass.edu\r\n
Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/webp, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1\r\n
Accept-Language: en-US,en;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

No. Time Source Destination Protocol Length Info
17 1.518710000 128.119.245.12 192.168.11.41 HTTP 726 HTTP/1.1 200 OK (text/html)

Frame 17: 726 bytes on wire (5808 bits), 726 bytes captured (5808 bits) on interface 0
Ethernet II, Src: Buffalo_b3:f7:46 (00:24:a5:b3:f7:46), Dst: AsustekC_40:d8:45 (f4:6d:04:40:d8:45)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.11.41 (192.168.11.41)
Transmission Control Protocol, Src Port: http (80), Dst Port: 46934 (46934), Seq: 1, Ack: 390, Len: 672
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
Request Version: HTTP/1.1
Status Code: 200
Response Phrase: OK
Date: Thu, 17 Jan 2013 02:42:29 GMT\r\n

Server: Apache/2.2.3 (CentOS)\r\n
Last-Modified: Thu, 17 Jan 2013 02:42:01 GMT\r\n
ETag: "d6c96-173-f0787040"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 371\r\n
Keep-Alive: timeout=10, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n

Line-based text data: text/html

\n
<html>\n
\n
**Congratulations again! Now you've downloaded the file lab2-2.html.
\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
\n**
**will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE
\n**
field in your browser's HTTP GET request to the server.\n
\n
</html>\n

No.	Time	Source	Destination	Protocol	Length	Info
22	2.864772000	192.168.11.41	128.119.245.12	HTTP	468	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1

Frame 22: 468 bytes on wire (3744 bits), 468 bytes captured (3744 bits) on interface 0
Ethernet II, Src: AsustekC_40:d8:45 (f4:6d:04:40:d8:45), Dst: Buffalo_b3:f7:46 (00:24:a5:b3:f7:46)
Internet Protocol Version 4, Src: 192.168.11.41 (192.168.11.41), Dst: 128.119.245.12 (128.119.245.12)
Transmission Control Protocol, Src Port: 46934 (46934), Dst Port: http (80), Seq: 826, Ack: 1183, Len: 414
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
Request Method: GET
Request URI: /wireshark-labs/HTTP-wireshark-file2.html
Request Version: HTTP/1.1
User-Agent: Opera/9.80 (Windows NT 6.2; WOW64) Presto/2.12.388 Version/12.12\r\n
Host: gaia.cs.umass.edu\r\n
Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/webp, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1\r\n
Accept-Language: en-US,en;q=0.9\r\n

Accept-Encoding: gzip, deflate\r\n
Cache-Control: no-cache\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

No. Time Source Destination Protocol Length Info
23 2.938714000 128.119.245.12 192.168.11.41 HTTP 725 HTTP/1.1 200 OK (text/html)

Frame 23: 725 bytes on wire (5800 bits), 725 bytes captured (5800 bits) on interface 0
Ethernet II, Src: Buffalo_b3:f7:46 (00:24:a5:b3:f7:46), Dst: AsustekC_40:d8:45 (f4:6d:04:40:d8:45)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.11.41 (192.168.11.41)
Transmission Control Protocol, Src Port: http (80), Dst Port: 46934 (46934), Seq: 1183, Ack: 1240, Len: 671
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
Request Version: HTTP/1.1
Status Code: 200
Response Phrase: OK
Date: Thu, 17 Jan 2013 02:42:30 GMT\r\n
Server: Apache/2.2.3 (CentOS)\r\n
Last-Modified: Thu, 17 Jan 2013 02:42:01 GMT\r\n
ETag: "d6c96-173-f0787040"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 371\r\n
Keep-Alive: timeout=10, max=98\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
Line-based text data: text/html
\n
<html>\n
\n
**Congratulations again! Now you've downloaded the file lab2-2.html.
\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
\n**
**will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE
\n**
field in your browser's HTTP GET request to the server.\n
\n

</html>\n

12) It looks like only one GET request was sent. Packet number 8, the only packet, had the request.
13) In the response, the first packet contained the status code/response. This was packet 10 in wireshark.
14) Status code and response is 200 OK.
15) Four TCP segments were needed to carry all of the data back to the browser.

No. Time Source Destination Protocol Length Info
8 0.200961000 192.168.11.41 128.119.245.12 HTTP 443 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1

Frame 8: 443 bytes on wire (3544 bits), 443 bytes captured (3544 bits) on interface 0
Ethernet II, Src: AsustekC_40:d8:45 (f4:6d:04:40:d8:45), Dst: Buffalo_b3:f7:46 (00:24:a5:b3:f7:46)
Internet Protocol Version 4, Src: 192.168.11.41 (192.168.11.41), Dst: 128.119.245.12 (128.119.245.12)
Transmission Control Protocol, Src Port: 47209 (47209), Dst Port: http (80), Seq: 1, Ack: 1, Len: 389
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
[Message: GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /wireshark-labs/HTTP-wireshark-file3.html
Request Version: HTTP/1.1
User-Agent: Opera/9.80 (Windows NT 6.2; WOW64) Presto/2.12.388 Version/12.12\r\n
Host: gaia.cs.umass.edu\r\n
Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/webp, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1\r\n
Accept-Language: en-US,en;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]

No. Time Source Destination Protocol Length Info
17 0.415770000 128.119.245.12 192.168.11.41 HTTP 477 HTTP/1.1 200 OK (text/html)

Frame 17: 477 bytes on wire (3816 bits), 477 bytes captured (3816 bits) on interface 0
Ethernet II, Src: Buffalo_b3:f7:46 (00:24:a5:b3:f7:46), Dst: AsustekC_40:d8:45 (f4:6d:04:40:d8:45)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.11.41 (192.168.11.41)
Transmission Control Protocol, Src Port: http (80), Dst Port: 47209 (47209), Seq: 4381, Ack: 390, Len: 423
[4 Reassembled TCP Segments (4803 bytes): #10(1460), #12(1460), #16(1460), #17(423)]
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
[Message: HTTP/1.1 200 OK\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Version: HTTP/1.1
Status Code: 200
Response Phrase: OK
Date: Thu, 17 Jan 2013 02:53:50 GMT\r\n
Server: Apache/2.2.3 (CentOS)\r\n
Last-Modified: Thu, 17 Jan 2013 02:53:01 GMT\r\n
ETag: "d6c97-1194-17cf3d40"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 4500\r\n
Keep-Alive: timeout=10, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
Line-based text data: text/html

16) 3 Total GET requests. First for the text set to 128.119.245.12, second for the cover of the book sent to 128.119.240.90, third for the Pearson logo to 165.193.140.14.

17) They look to have been downloaded in parallel as the browser asks for both images before it receives a response from either image. Additionally, the responses come out of order form the get requests. (These packets not in this document for space considerations).

18) 401 Authorization Required

19) There is an authorization field sent with credentials as plain text.