Xueyang (Sean) Wang

XW1154

02/19/2017

CS4793

Homework 02

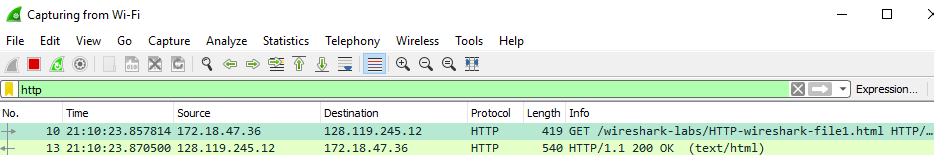


Figure 1. Connection first part

No. Time Source Destination Protocol Length Info

10 21:10:23.857814 172.18.47.36 128.119.245.12 HTTP 419 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

Frame 10: 419 bytes on wire (3352 bits), 419 bytes captured (3352 bits) on interface 0

Ethernet II, Src: IntelCor\_79:6a:e9 (ac:fd:ce:79:6a:e9), Dst: IETF-VRRP-VRID\_53 (00:00:5e:00:01:53)

Internet Protocol Version 4, Src: 172.18.47.36, Dst: 128.119.245.12

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 405

Identification: 0x6a96 (27286)

Flags: 0x02 (Don't Fragment)

Fragment offset: 0

Time to live: 64

Protocol: TCP (6)

Header checksum: 0x7e12 [validation disabled]

[Header checksum status: Unverified]

Source: 172.18.47.36

Destination: 128.119.245.12

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

Transmission Control Protocol, Src Port: 51141, Dst Port: 80, Seq: 1, Ack: 1, Len: 365

Source Port: 51141

Destination Port: 80

[Stream index: 1]

[TCP Segment Len: 365]

Sequence number: 1 (relative sequence number)

[Next sequence number: 366 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

Header Length: 20 bytes

Flags: 0x018 (PSH, ACK)

Window size value: 32768

[Calculated window size: 262144]

[Window size scaling factor: 8]

Checksum: 0x59f0 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

[SEQ/ACK analysis]

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

Accept: text/html, application/xhtml+xml, image/jxr, \*/\*\r\n

Accept-Language: en-US,en;q=0.8,zh-Hans-CN;q=0.7,zh-Hans;q=0.5,es-ES;q=0.3,es;q=0.2\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko\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-file1.html]

[HTTP request 1/1]

[Response in frame: 13]

No. Time Source Destination Protocol Length Info

13 21:10:23.870500 128.119.245.12 172.18.47.36 HTTP 540 HTTP/1.1 200 OK (text/html)

Frame 13: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0

Ethernet II, Src: Cisco\_bf:1e:40 (58:bf:ea:bf:1e:40), Dst: IntelCor\_79:6a:e9 (ac:fd:ce:79:6a:e9)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.18.47.36

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 526

Identification: 0x6933 (26931)

Flags: 0x02 (Don't Fragment)

Fragment offset: 0

Time to live: 51

Protocol: TCP (6)

Header checksum: 0x8bfc [validation disabled]

[Header checksum status: Unverified]

Source: 128.119.245.12

Destination: 172.18.47.36

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

Transmission Control Protocol, Src Port: 80, Dst Port: 51141, Seq: 1, Ack: 366, Len: 486

Source Port: 80

Destination Port: 51141

[Stream index: 1]

[TCP Segment Len: 486]

Sequence number: 1 (relative sequence number)

[Next sequence number: 487 (relative sequence number)]

Acknowledgment number: 366 (relative ack number)

Header Length: 20 bytes

Flags: 0x018 (PSH, ACK)

Window size value: 237

[Calculated window size: 30336]

[Window size scaling factor: 128]

Checksum: 0x0952 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

[SEQ/ACK analysis]

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: Mon, 20 Feb 2017 02:10:24 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod\_perl/2.0.10 Perl/v5.16.3\r\n

Last-Modified: Sun, 19 Feb 2017 06:59:01 GMT\r\n

ETag: "80-548dcae830b68"\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: 0.012686000 seconds]

[Request in frame: 10]

File Data: 128 bytes

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

1. My browser running HTTP version 1.1, the server is running HTTP version 1.1.
2. The list of languages that my browser accepts includes English.
3. The IP address of my computer is 172.18.47.36; The gaia server is 128.119.245.12.
4. The returned status code is “200”
5. Last-Modified: Sun, 19 Feb 2017 06:59:01 GMT
6. The bytes of content is “128” bytes
7. No, I do not see any in the HTTP Message below

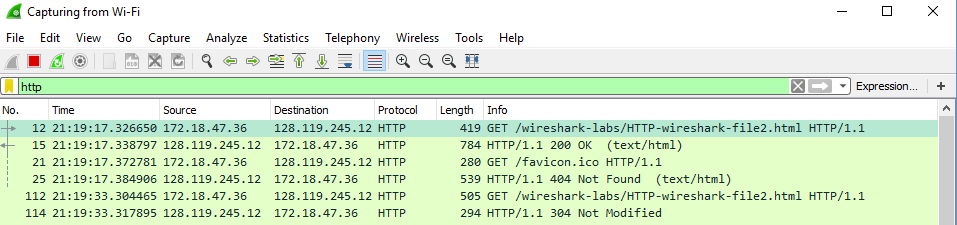


Figure 2. Connection second part

First GET:

No. Time Source Destination Protocol Length Info

12 21:19:17.326650 172.18.47.36 128.119.245.12 HTTP 419 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1

Frame 12: 419 bytes on wire (3352 bits), 419 bytes captured (3352 bits) on interface 0

Ethernet II, Src: IntelCor\_79:6a:e9 (ac:fd:ce:79:6a:e9), Dst: IETF-VRRP-VRID\_53 (00:00:5e:00:01:53)

Internet Protocol Version 4, Src: 172.18.47.36, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 51455, Dst Port: 80, Seq: 1, Ack: 1, Len: 365

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

Accept: text/html, application/xhtml+xml, image/jxr, \*/\*\r\n

Accept-Language: en-US,en;q=0.8,zh-Hans-CN;q=0.7,zh-Hans;q=0.5,es-ES;q=0.3,es;q=0.2\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko\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: 15]

First RETURN:

No. Time Source Destination Protocol Length Info

15 21:19:17.338797 128.119.245.12 172.18.47.36 HTTP 784 HTTP/1.1 200 OK (text/html)

Frame 15: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface 0

Ethernet II, Src: Cisco\_bf:1e:40 (58:bf:ea:bf:1e:40), Dst: IntelCor\_79:6a:e9 (ac:fd:ce:79:6a:e9)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.18.47.36

Transmission Control Protocol, Src Port: 80, Dst Port: 51455, Seq: 1, Ack: 366, Len: 730

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: Mon, 20 Feb 2017 02:19:17 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod\_perl/2.0.10 Perl/v5.16.3\r\n

Last-Modified: Sun, 19 Feb 2017 06:59:01 GMT\r\n

ETag: "173-548dcae830398"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 371\r\n

[Content length: 371]

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: 0.012147000 seconds]

[Request in frame: 12]

File Data: 371 bytes

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

Second GET:

No. Time Source Destination Protocol Length Info

112 21:19:33.304465 172.18.47.36 128.119.245.12 HTTP 505 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1

Frame 112: 505 bytes on wire (4040 bits), 505 bytes captured (4040 bits) on interface 0

Ethernet II, Src: IntelCor\_79:6a:e9 (ac:fd:ce:79:6a:e9), Dst: IETF-VRRP-VRID\_53 (00:00:5e:00:01:53)

Internet Protocol Version 4, Src: 172.18.47.36, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 51461, Dst Port: 80, Seq: 1, Ack: 1, Len: 451

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

Accept: text/html, application/xhtml+xml, image/jxr, \*/\*\r\n

Accept-Language: en-US,en;q=0.8,zh-Hans-CN;q=0.7,zh-Hans;q=0.5,es-ES;q=0.3,es;q=0.2\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n

Accept-Encoding: gzip, deflate\r\n

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

If-Modified-Since: Sun, 19 Feb 2017 06:59:01 GMT\r\n

If-None-Match: "173-548dcae830398"\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: 114]

Second RETURN:

No. Time Source Destination Protocol Length Info

114 21:19:33.317895 128.119.245.12 172.18.47.36 HTTP 294 HTTP/1.1 304 Not Modified

Frame 114: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface 0

Ethernet II, Src: Cisco\_bf:1e:40 (58:bf:ea:bf:1e:40), Dst: IntelCor\_79:6a:e9 (ac:fd:ce:79:6a:e9)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.18.47.36

Transmission Control Protocol, Src Port: 80, Dst Port: 51461, Seq: 1, Ack: 452, Len: 240

Hypertext Transfer Protocol

HTTP/1.1 304 Not Modified\r\n

[Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]

Request Version: HTTP/1.1

Status Code: 304

Response Phrase: Not Modified

Date: Mon, 20 Feb 2017 02:19:33 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-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=100\r\n

ETag: "173-548dcae830398"\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.013430000 seconds]

[Request in frame: 112]

1. No, there is not “IF-MODIFIED-SINCE” line in the first HTTP GET.
2. Yes, the response explicitly return the contents of the file. The text is printed in the file section.
3. Yes, there is “IF-MODIFIED-SINCE” line in the second HTTP GET. The date since last modified.
4. The returned status code is “304 Not Modified.” The server did not explicitly return the contents of the file because it was not modified, so the text of the file is not returned in the HTTP message.

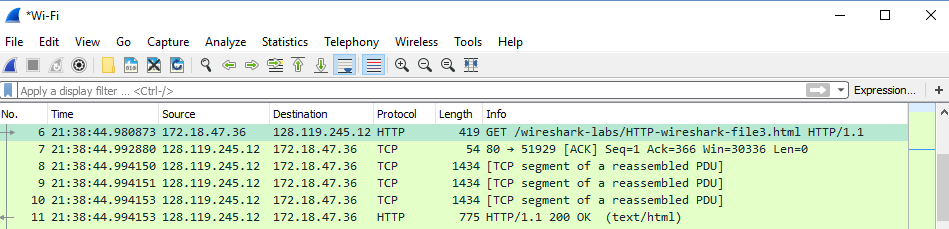


Figure 3. Connection third part

1. There was 1 HTTP GET message. It was packet NO.6.
2. Packet NO.11.
3. The returned state code and Phrase was “200 OK.”
4. 3 packets (8,9,10 in the trace).

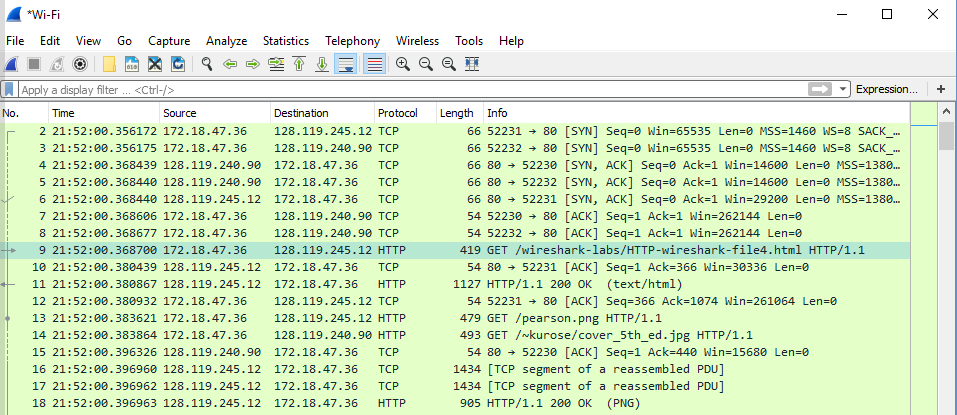


Figure 4. Connection forth part

1. There were 3 HTTP GET messages sent: packet 9 (base file), packet 13(pearson.png), and packet 14 (cover\_5th\_ed.jpg). They were sent to different address: packet 9 was sent to 128.119.245.12; packet 13 was sent to 128.119.235.12; and, packet 14 was sent to 128.119.240.90.
2. The downloads occurred in parallel. The second JPG request (GET message) was sent before completing PNG request(GET message). In the picture, they were actually sent together in parallel.

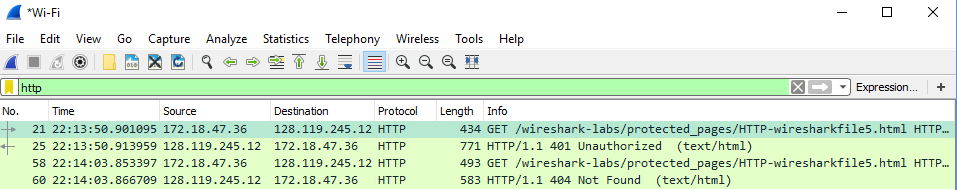


Figure 5. Connecticut fifth part

No. Time Source Destination Protocol Length Info

58 22:14:03.853397 172.18.47.36 128.119.245.12 HTTP 493 GET /wireshark-labs/protected\_pages/HTTP-wiresharkfile5.html HTTP/1.1

Frame 58: 493 bytes on wire (3944 bits), 493 bytes captured (3944 bits) on interface 0

Ethernet II, Src: IntelCor\_79:6a:e9 (ac:fd:ce:79:6a:e9), Dst: IETF-VRRP-VRID\_53 (00:00:5e:00:01:53)

Internet Protocol Version 4, Src: 172.18.47.36, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 52944, Dst Port: 80, Seq: 1, Ack: 1, Len: 439

Hypertext Transfer Protocol

GET /wireshark-labs/protected\_pages/HTTP-wiresharkfile5.html HTTP/1.1\r\n

Accept: text/html, application/xhtml+xml, image/jxr, \*/\*\r\n

Accept-Language: en-US,en;q=0.8,zh-Hans-CN;q=0.7,zh-Hans;q=0.5,es-ES;q=0.3,es;q=0.2\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n

Accept-Encoding: gzip, deflate\r\n

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

Connection: Keep-Alive\r\n

Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n

Credentials: wireshark-students:network

\r\n

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected\_pages/HTTP-wiresharkfile5.html]

[HTTP request 1/1]

[Response in frame: 60]

1. The server’s response was “401 Unauthorized”.
2. The new field included is the Authorization field. This provides the user name and password for a secure website.