

Lab 4_Wireshark

Part 1

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

- Our browser and the server are running version 1.1 of HTTP.
(Image 1 and 2: Highlighted in Packet Details Pane)

2. What languages (if any) does your browser indicate that it can accept to the server?

- en-US and en (US English and Standard English)
(Image 3: Accept-Language in Packet Details Pane)

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

- Computer: 10.5.204.226 (Image 4: Src in Packet Details Pane)
- Server: 128.119.245.12 (Image 4: Dst in Packet Details Pane)

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

- 200 (Image 5: Status Code in Packet Details Pane)

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

- Thurs, 27 February 2020 06:59:04 GMT (Image 6: Last-Modified in Packet Details Pane)

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

- 128 bytes (Image 7: Content length in Packet Details Pane)

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 headers are there.

Activities Wireshark Thu 13:45

*any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
10	0.081030878	128.119.245.12	10.5.204.226	TCP	76	80 → 58918 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1386 SACK_PERM=1 TSval=2521397100 TSecr=1995386951
11	0.081088254	10.5.204.226	128.119.245.12	TCP	68	58918 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1995386951 TSecr=2521397100
12	0.081287988	10.5.204.226	128.119.245.12	HTTP	444	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
13	0.122807601	128.119.245.12	10.5.204.226	TCP	68	80 → 58918 [ACK] Seq=1 Ack=377 Win=30080 Len=0 TSval=2521397142 TSecr=1995386951
14	0.139441555	128.119.245.12	10.5.204.226	HTTP	554	HTTP/1.1 200 OK (text/html)
15	0.139471319	10.5.204.226	128.119.245.12	TCP	68	58918 → 80 [ACK] Seq=377 Ack=487 Win=64128 Len=0 TSval=1995387009 TSecr=2521397159

Frame 12: 444 bytes on wire (3552 bits), 444 bytes captured (3552 bits) on interface 0

- Linux cooked capture
- Internet Protocol Version 4, Src: 10.5.204.226, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 58918, Dst Port: 80, Seq: 1, Ack: 1, Len: 376
- 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:72.0) Gecko/20100101 Firefox/72.0\r\n
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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-file1.html]
 - [HTTP request 1/2]
 - [Response in frame: 14]
 - [Next request in frame: 16]

0040 96 49 77 6c 37 45 54 20 2f 7f 69 72 65 73 68 6d .l.w|GET /wiresha
0050 f2 08 20 c0 01 62 73 2f 48 54 54 50 2d 77 69 72 k|s/labs/ HTTP-wi
0060 85 73 69 61 72 6b 2d 69 69 6c 65 31 2e 68 74 6d shark-f ile1.htm
0070 8c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 l HTTP/1 .1: Host
0080 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 73 2e : gaia.c s.umass.
0090 65 64 75 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a edu ·Use r-Agent:
00a0 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 50 31 Mozilla /5.0 (X1
00b0 31 3b 20 55 62 75 6e 74 75 3b 20 4c 69 6e 75 78 1; Ubunt u; Linux
00c0 20 78 38 36 5f 36 34 3b 20 72 76 3a 37 32 2e 30 x86_64; rv:72.0
00d0 20 20 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31) Gecko/ 20100101
00e0 20 46 69 72 65 6e 6f 78 2f 37 32 2e 30 0d 0a 41 Firefox /72.0 ·A
00f0 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c ccept: t ext/html

Text item (text), 56 bytes

Packets: 18 · Displayed: 18 (100.0%) · Dropped: 0 (0.0%) Profile: Default

Image 1

Activities Wireshark Thu 13:45

*any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
10	0.081030878	128.119.245.12	10.5.204.226	TCP	76	80 → 58918 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1386 SACK_PERM=1 TSval=2521397100 TSecr=1995386951
11	0.081088254	10.5.204.226	128.119.245.12	TCP	68	58918 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1995386951 TSecr=2521397100
12	0.081287988	10.5.204.226	128.119.245.12	HTTP	444	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
13	0.122807601	128.119.245.12	10.5.204.226	TCP	68	80 → 58918 [ACK] Seq=1 Ack=377 Win=30080 Len=0 TSval=2521397142 TSecr=1995386951
14	0.139441555	128.119.245.12	10.5.204.226	HTTP	554	HTTP/1.1 200 OK (text/html)
15	0.139471319	10.5.204.226	128.119.245.12	TCP	68	58918 → 80 [ACK] Seq=377 Ack=487 Win=64128 Len=0 TSval=1995387009 TSecr=2521397159

Frame 14: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface 0

- Linux cooked capture
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.5.204.226
- Transmission Control Protocol, Src Port: 80, Dst Port: 58918, Seq: 1, Ack: 377, Len: 486
- Hypertext Transfer Protocol
 - HTTP/1.1 200 OK\r\n
 - Date: Thu, 27 Feb 2020 18:41:43 GMT\r\n
 - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
 - Last-Modified: Thu, 27 Feb 2020 06:59:04 GMT\r\n
 - ETag: "80-59f8941a86848"\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 1/2]
 - [Time since request: 0.058153567 seconds]
 - [Request in frame: 12]
 - [Next request in frame: 16]
 - [Next response in frame: 17]

0040 76 ef 39 47 48 54 54 50 2f 31 2e 31 20 32 30 30 v.0GHTTP /1.1 200
0050 20 4f 4b 0d 0e 44 61 74 65 3a 20 54 68 75 2c 20 OK Date: Thu,
0060 32 37 20 4b 65 62 20 32 30 32 30 20 31 38 3a 34 27 Feb 2 020 18:4
0070 31 3a 3a 33 29 47 4d 54 0d 0a 53 65 72 76 65 72 1:43 GMT ·Server
0080 3a 20 41 70 61 63 68 65 2f 32 2e 3a 2e 36 20 28 : Apache /2.4.6 (C
0090 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 4c 2f CentOS) OpenSSL/
00a0 31 2e 30 2e 32 6b 2d 6e 69 70 73 20 50 48 50 2f 1.0.2k-f ips PHP/
00b0 35 2e 34 2e 31 36 20 6d 6f 64 5f 70 65 72 6c 2f 5.4.16 m od perl/
00c0 32 2e 30 2e 31 31 20 50 65 72 6c 2f 76 35 2e 31 2.0.11 P erl/v5.1
00d0 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 6.3 ·Las t-Modifi
00e0 65 64 3a 20 54 68 75 2c 20 32 37 20 46 65 62 20 ed: Thu, 27 Feb
00f0 32 30 32 30 20 30 36 3a 35 39 3a 30 30 20 47 4d 2020 06: 59:04 GM

Text item (text), 17 bytes

Packets: 18 · Displayed: 18 (100.0%) · Dropped: 0 (0.0%) Profile: Default

Image 2

Activities Wireshark Thu 13:46 *any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
10	0.081030878	128.119.245.12	10.5.204.226	TCP	76	80 → 58918 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1386 SACK_PERM=1 TSval=2521397100 TSecr=1995386951
11	0.081088254	10.5.204.226	128.119.245.12	TCP	68	58918 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1995386951 TSecr=2521397100
12	0.081287988	10.5.204.226	128.119.245.12	HTTP	444	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
13	0.122807691	128.119.245.12	10.5.204.226	TCP	68	80 → 58918 [ACK] Seq=1 Ack=377 Win=30080 Len=0 TSval=2521397142 TSecr=1995386951
14	0.139441555	128.119.245.12	10.5.204.226	HTTP	554	HTTP/1.1 200 OK (text/html)
15	0.139471319	10.5.204.226	128.119.245.12	TCP	68	58918 → 80 [ACK] Seq=377 Ack=487 Win=64128 Len=0 TSval=1995387009 TSecr=2521397159

Frame 12: 444 bytes on wire (3552 bits), 444 bytes captured (3552 bits) on interface 0

- Linux cooked capture
- Internet Protocol Version 4, Src: 10.5.204.226, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 58918, Dst Port: 80, Seq: 1, Ack: 1, Len: 376
- 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:72.0) Gecko/20100101 Firefox/72.0\r\n
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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-file1.html]
 - [HTTP request 1/2]
 - [Response in frame: 14]
 - [Next request in frame: 16]

00100 2c 61 70 70 6c 69 63 61 74 69 6f 6a 2f 78 68 74 ,application/xht
 00110 6d 6c 2b 78 6d 6c 61 70 70 6c 69 63 61 74 69 ml+xml, applicati
 00120 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 on/xml;q =0.9, ima
 00130 67 65 2f 77 65 62 70 2c 2a 2f 2a 3b 71 3d 30 2e ge/webp, /*;q=0.
 00140 38 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 8-Accept-Langua
 00150 67 65 3a 20 65 6e 2d 65 63 2e 65 6a 2b 71 2d 68 ge: en-US,en;q=0
 00160 2e 25 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 5-Accept-Encod
 00170 69 6e 67 3a 20 67 7a 69 70 2c 2d 64 65 66 6c 61 ing: gzip, defla
 00180 74 65 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 te-Connec tion:
 00190 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 67 72 keep-alive- Upgr
 001a0 61 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 ade-Inse cure-Req
 001b0 75 65 73 74 73 3a 20 31 0d 0a 0d 0a uests: 1

HTTTP Accept Language (http.accept_language), 33 bytes

Packets: 18 · Displayed: 18 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

Image 3

Activities Wireshark Thu 13:47 *any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
10	0.081030878	128.119.245.12	10.5.204.226	TCP	76	80 → 58918 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1386 SACK_PERM=1 TSval=2521397100 TSecr=1995386951
11	0.081088254	10.5.204.226	128.119.245.12	TCP	68	58918 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1995386951 TSecr=2521397100
12	0.081287988	10.5.204.226	128.119.245.12	HTTP	444	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
13	0.122807691	128.119.245.12	10.5.204.226	TCP	68	80 → 58918 [ACK] Seq=1 Ack=377 Win=30080 Len=0 TSval=2521397142 TSecr=1995386951
14	0.139441555	128.119.245.12	10.5.204.226	HTTP	554	HTTP/1.1 200 OK (text/html)
15	0.139471319	10.5.204.226	128.119.245.12	TCP	68	58918 → 80 [ACK] Seq=377 Ack=487 Win=64128 Len=0 TSval=1995387009 TSecr=2521397159

Frame 12: 444 bytes on wire (3552 bits), 444 bytes captured (3552 bits) on interface 0

- Linux cooked capture
- Internet Protocol Version 4, Src: 10.5.204.226, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 58918, Dst Port: 80, Seq: 1, Ack: 1, Len: 376
- Hypertext Transfer Protocol

00100 45 00 01 ac 95 02 40 00 40 06 57 de 0a 05 cc e2 E-----@.0-W-----
 00200 80 77 f5 04 e6 26 00 50 75 fb 8f b0 7d 3f 50 7f [w.f&P u...}P
 00300 09 10 01 f6 4e 0a 00 00 01 01 00 0a 76 ef 30 47 --N...v.00
 00400 96 49 77 6c 47 45 54 20 2f 77 69 72 65 73 68 61 :lwGET /wiresha
 00500 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 69 72 rk-labs/ HTTP-wir
 00600 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68 74 6d eshark-f ile1.htm
 00700 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 1 HTTP/1.1: Host
 00800 3a 20 67 69 61 2e 63 73 2e 75 6d 61 73 73 2e : gaia.c s.umass.
 00900 65 64 75 0d 0a 55 73 65 72 2d 41 6f 65 6e 74 3a edu Use r-Agent:
 00a00 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 Mozilla /5.0 (X1
 00b00 31 3b 20 55 62 75 6e 74 75 3b 20 4c 69 6e 75 78 i; Ubuntu; Linux
 00c00 20 78 38 36 5f 36 34 3b 20 72 76 3a 37 32 2e 30 x86_64; rv:72.0

Internet Protocol Version 4 (ip), 20 bytes

Packets: 18 · Displayed: 18 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

Image 4

Activities Wireshark Thu 13:48 *any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
10	0.081930878	128.119.245.12	10.5.204.226	TCP	76	80 → 58918 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1386 SACK_PERM=1 TSval=2521397100 TSecr=1995386951
11	0.081988254	10.5.204.226	128.119.245.12	TCP	68	58918 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1995386951 TSecr=2521397100
12	0.081287988	10.5.204.226	128.119.245.12	HTTP	444	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
13	0.122807691	128.119.245.12	10.5.204.226	TCP	68	80 → 58918 [ACK] Seq=1 Ack=377 Win=30080 Len=0 TSval=2521397142 TSecr=1995386951
14	0.139441555	128.119.245.12	10.5.204.226	HTTP	554	HTTP/1.1 200 OK (text/html)
15	0.139471319	10.5.204.226	128.119.245.12	TCP	68	58918 → 80 [ACK] Seq=377 Ack=487 Win=64128 Len=0 TSval=1995387009 TSecr=2521397159

Frame 14: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface 0

Linux cooked capture

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.5.204.226

Transmission Control Protocol, Src Port: 80, Dst Port: 58918, Seq: 1, Ack: 377, Len: 486

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: Thu, 27 Feb 2020 18:41:43 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n

Last-Modified: Thu, 27 Feb 2020 06:59:04 GMT\r\n

ETag: "80-59f8941a86848"\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

0000 76 ef 30 47 48 54 54 50 2f 31 2e 34 20 02 20 30 v.0GHTTP /1.1 200

0001 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 68 75 2c 20 OK - Dat e: Thu,

0002 32 37 20 46 65 62 20 32 30 32 30 20 31 38 3a 34 27 Feb 2 020 18:4

0003 31 3a 34 33 20 47 4d 54 0d 0a 53 65 72 76 65 72 1:43 GMT -Server

0004 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 20 28 : Apache /2.4.6 (

0005 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 4c 2f CentOS) OpenSSL/

0006 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48 50 2f 1.0.2k-f ips PHP/

0007 35 2e 34 2e 31 36 20 6d 6f 64 5f 70 65 72 6c 2f 5.4.16 m od_perl/

0008 32 2e 30 2e 31 31 20 50 65 72 6c 2f 76 35 2e 31 2.0.11 P erl/v5.1

0009 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 6.3- Las t-Modifi

000a 65 64 3a 20 54 68 75 2c 20 32 37 20 46 65 62 20 ed: Thu, 27 Feb

000b 32 30 32 30 20 30 36 3a 35 39 3a 30 34 20 47 4d 2020 06: 59:04 GM

HTTP Response Status Code (http.response.code), 3 bytes

Packets: 18 · Displayed: 18 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

Image 5

Activities Wireshark Thu 13:51 *any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
10	0.081930878	128.119.245.12	10.5.204.226	TCP	76	80 → 58918 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1386 SACK_PERM=1 TSval=2521397100 TSecr=1995386951
11	0.081988254	10.5.204.226	128.119.245.12	TCP	68	58918 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1995386951 TSecr=2521397100
12	0.081287988	10.5.204.226	128.119.245.12	HTTP	444	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
13	0.122807691	128.119.245.12	10.5.204.226	TCP	68	80 → 58918 [ACK] Seq=1 Ack=377 Win=30080 Len=0 TSval=2521397142 TSecr=1995386951
14	0.139441555	128.119.245.12	10.5.204.226	HTTP	554	HTTP/1.1 200 OK (text/html)
15	0.139471319	10.5.204.226	128.119.245.12	TCP	68	58918 → 80 [ACK] Seq=377 Ack=487 Win=64128 Len=0 TSval=1995387009 TSecr=2521397159

Frame 14: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface 0

Linux cooked capture

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.5.204.226

Transmission Control Protocol, Src Port: 80, Dst Port: 58918, Seq: 1, Ack: 377, Len: 486

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Thu, 27 Feb 2020 18:41:43 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n

Last-Modified: Thu, 27 Feb 2020 06:59:04 GMT\r\n

ETag: "80-59f8941a86848"\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

0000 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 6.3- Las t-Modifi

0001 65 64 3a 20 54 68 75 2c 20 32 37 20 46 65 62 20 ed: Thu, 27 Feb

0002 32 30 32 30 20 30 36 3a 35 39 3a 30 34 20 47 4d 2020 06: 59:04 GM

0003 64 0d 0a 45 54 61 67 3a 20 22 38 30 2d 35 39 66 74 ETag: "80-59f

0004 38 39 34 31 61 38 36 38 34 38 2d 0d 0a 41 63 63 8941a868 48"-Acc

0005 65 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 74 65 ept-Rang es: byte

0006 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 s-Conte nt-Lengt

0007 40 68 3a 20 31 32 38 0d 0a 4b 65 65 70 2d 41 6c 69 h: 128- Keep-All

0008 76 65 3a 20 74 69 6d 65 6f 75 74 30 35 2c 20 6d ve: time out=5, m

0009 61 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63 74 69 ax=100- Connecti

000a 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a on: Keep -Alive-

000b 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 Content- Type: te

HTTP Last Modified (http.last_modified), 46 bytes

Packets: 18 · Displayed: 18 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

Image 6

Activities Wireshark Thu 13:51 *any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
10	0.081030878	128.119.245.12	10.5.204.226	TCP	76	80 → 58918 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1386 SACK_PERM=1 TSval=2521397100 TSecr=1995386951
11	0.081088254	10.5.204.226	128.119.245.12	TCP	68	58918 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1995386951 TSecr=2521397100
12	0.081287988	10.5.204.226	128.119.245.12	HTTP	444	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
13	0.122807691	128.119.245.12	10.5.204.226	TCP	68	80 → 58918 [ACK] Seq=1 Ack=377 Win=30080 Len=0 TSval=2521397142 TSecr=1995386951
14	0.139441555	128.119.245.12	10.5.204.226	HTTP	554	HTTP/1.1 200 OK (text/html)
15	0.139471319	10.5.204.226	128.119.245.12	TCP	68	58918 → 80 [ACK] Seq=377 Ack=487 Win=64128 Len=0 TSval=1995387009 TSecr=2521397159

Frame 14: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface 0

- Linux cooked capture
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.5.204.226
- Transmission Control Protocol, Src Port: 80, Dst Port: 58918, Seq: 1, Ack: 377, Len: 486
- Hypertext Transfer Protocol
 - HTTP/1.1 200 OK\r\n
 - Date: Thu, 27 Feb 2020 18:41:43 GMT\r\n
 - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
 - Last-Modified: Thu, 27 Feb 2020 06:59:04 GMT\r\n
 - ETag: "80-59f8941a86848"\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 1/2]
 - [Time since request: 0.058153567 seconds]
 - [Request in frame: 12]
 - [Next request in frame: 161]

Content length (http.content_length), 21 bytes

Packets: 18 · Displayed: 18 (100.0%) · Dropped: 0 (0.0%) Profile: Default

Image 7

Part 2

1. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu? To answer this question, it's probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the "details of the selected packet header window" (refer to Figure 2 in the "Getting Started with Wireshark" Lab if you're uncertain about the Wireshark windows.

- Client IP: 10.5.204.226 (Image 1: Source in Packet List Pane)
- Client Port: 56258 (Image 1: Src Port in Packet Details Pane)

2. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?

- Gaia IP: 128.119.245.12 (Image 1: Destination in Packet List Pane)
- Gaia Port: 80 (Image 1: Dst Port in Packet Details Pane)

3. What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu?

- Client IP: 10.5.204.226 (Image 2: Source in Packet List Pane)
- Client Port: 56258 (Image 2: Source Port in Packet Details Pane)

4. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?

- Sequence Number: 152515 (Image 2: Sequence Number in Packet Details Pane)
- There is a specific bit in the sequence that acts as a flag specifying the segment as a SYN segment.

5. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment.

- Sequence Number: 1 (Image 3: Sequence Number in Packet Details Pane)
- Ack: 152961 (Image 3: Acknowledgement Number in Packet Details Pane)
- The SYN value of 1 indicates that gaia.cs.edu successfully received the request. The ACK number comes from our original SYN number and adding the segment length (446) to it.
- There is a specific bit in the sequence that acts as a flag specifying the segment as a SYNACK segment.

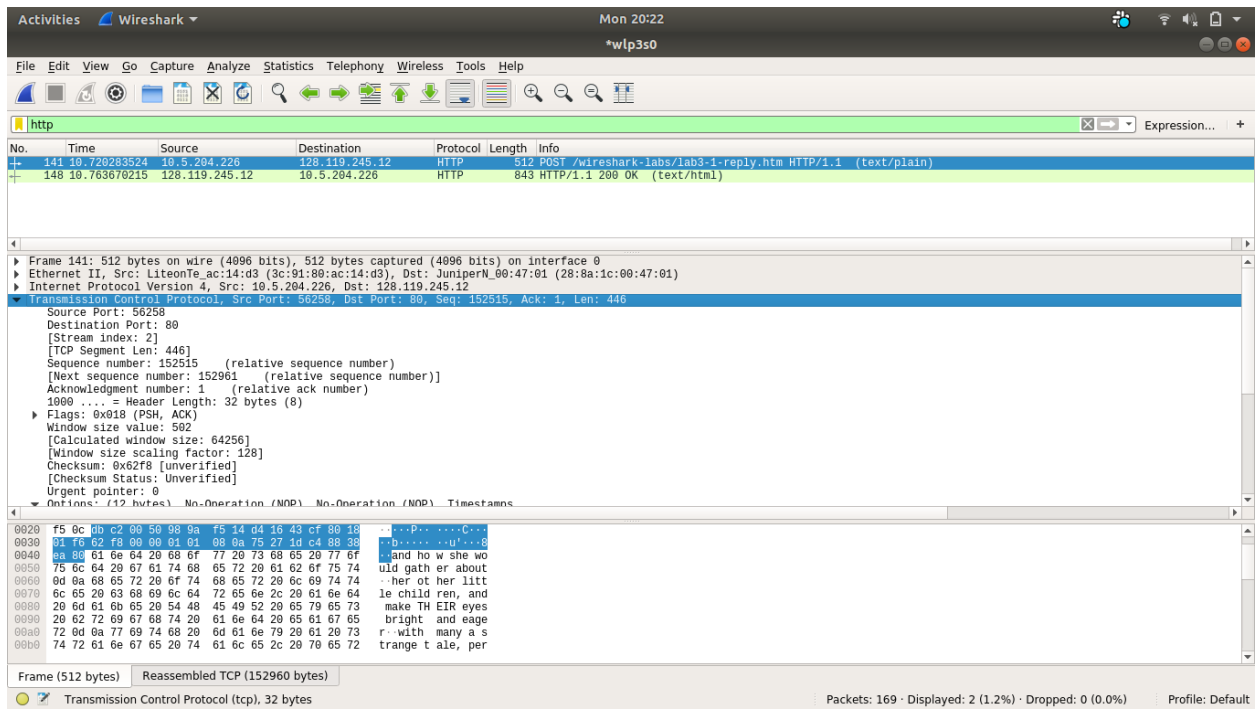


Image 1

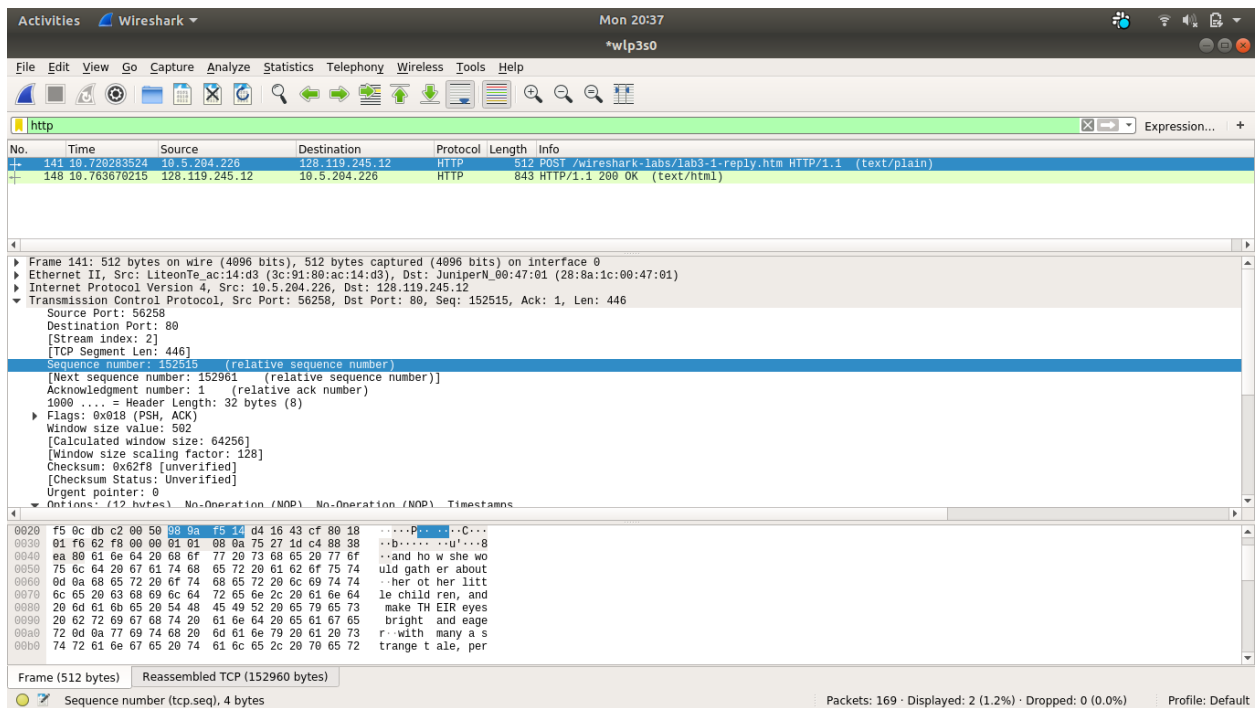


Image 2

The image shows a Wireshark capture of network traffic on the interface *wlp3s0. The top pane shows a list of packets, with packet 148 selected. The middle pane shows the details of the selected packet, which is an HTTP POST request. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Packets:

No.	Time	Source	Destination	Protocol	Length	Info
141	10.729283524	19.5.204.226	128.119.245.12	HTTP	512	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
148	10.763670215	128.119.245.12	19.5.204.226	HTTP	843	HTTP/1.1 200 OK (text/html)

Packet 148 Details:

- Frame 148: 843 bytes on wire (6744 bits), 843 bytes captured (6744 bits) on interface 0
- Ethernet II, Src: JuniperM_00:47:01 (28:8a:1c:00:47:01), Dst: LiteonTe_ac:14:d3 (3c:91:80:ac:14:d3)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 19.5.204.226
- Transmission Control Protocol, Src Port: 80, Dst Port: 56258, Seq: 1, Ack: 152961, Len: 777
 - Source Port: 80
 - Destination Port: 56258
 - [Stream Index: 2]
 - [TCP Segment Len: 777]
 - Sequence number: 1 (relative sequence number)
 - [Next sequence number: 778 (relative sequence number)]
 - Acknowledgment number: 152961 (relative ack number)
 - 1980 = Header Length: 32 bytes (8)
 - Flags: 0x018 (PSH, ACK)
 - Window size value: 1432
 - [Calculated window size: 183296]
 - [Window size scaling factor: 128]
 - Checksum: 0x8344 [unverified]
 - [Checksum Status: Unverified]
 - Urgent pointer: 0
 - Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps

Raw Packet Data (Hex/ASCII):

```

0020 cc e2 00 50 db c2 d4 16 43 cf 80 9a f6 d2 80 18 ...P....C-...
0030 05 98 03 44 00 00 01 01 08 0a 89 38 ea ad 75 27 ...D....8..u'
0040 1d c4 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f ...HTTP/1.1 200 O
0050 4b 0d 0a 44 61 74 65 3a 20 54 75 65 2c 20 32 35 K..Date: Tue, 25
0060 20 46 05 62 20 32 30 32 30 20 30 31 3a 30 30 3a Feb 202 0 01:08:
0070 35 37 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 57 GMT..Server:
0080 41 70 61 63 68 65 2f 32 2e 3a 2e 36 20 28 43 65 Apache/2.4.6 (Ce
0090 6e 74 4f 53 29 20 4f 70 65 6e 53 53 4c 2f 31 2e ntOS) Op enSSL/1.
00a0 30 2e 32 60 2d 66 69 70 73 20 50 48 50 2f 35 2e 0.2k-fip s PHP/5.
00b0 34 2e 31 30 20 60 6f 64 5f 70 65 72 6c 2f 32 2e 4.16 mod_perl/2.
00c0 30 2e 31 31 20 50 65 72 6c 2f 76 35 2e 31 36 2e 0.11 Per l/v5.16.
00d0 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64 3..Last-Modified
  
```

Status Bar: Acknowledgment number (tcp.ack), 4 bytes | Packets: 169 · Displayed: 2 (1.2%) · Dropped: 0 (0.0%) | Profile: Default

Image 3