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.

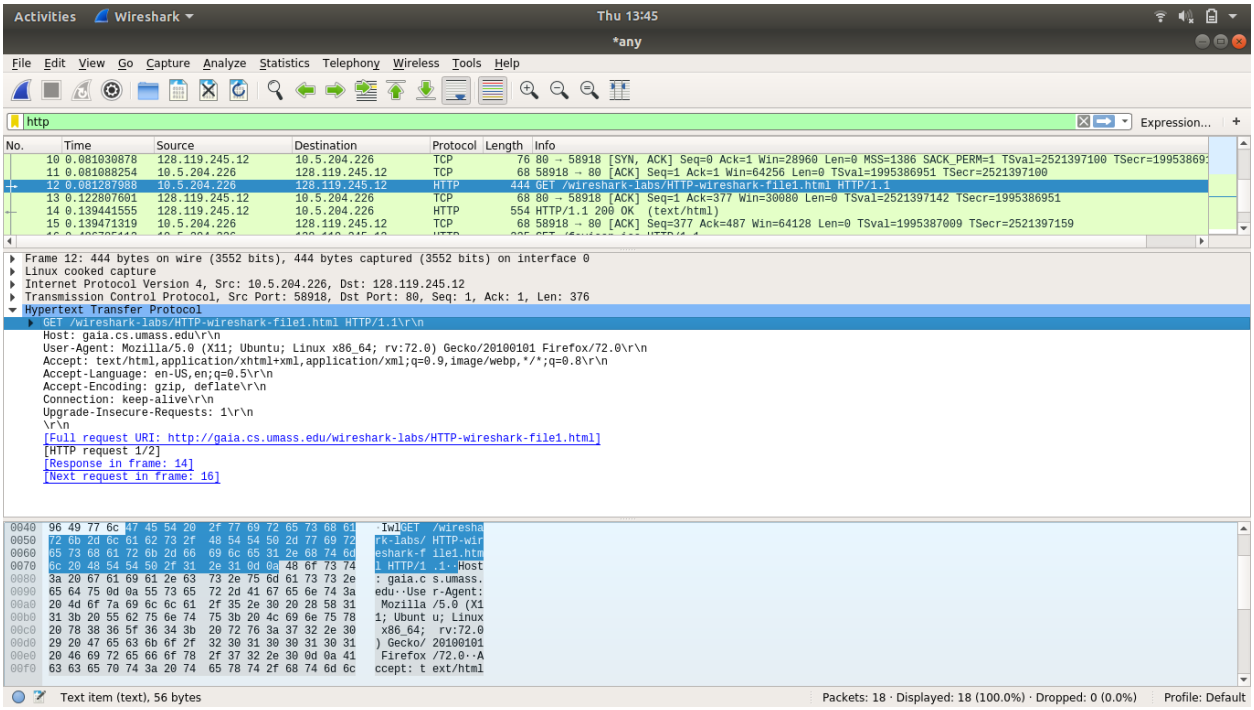

Image 1

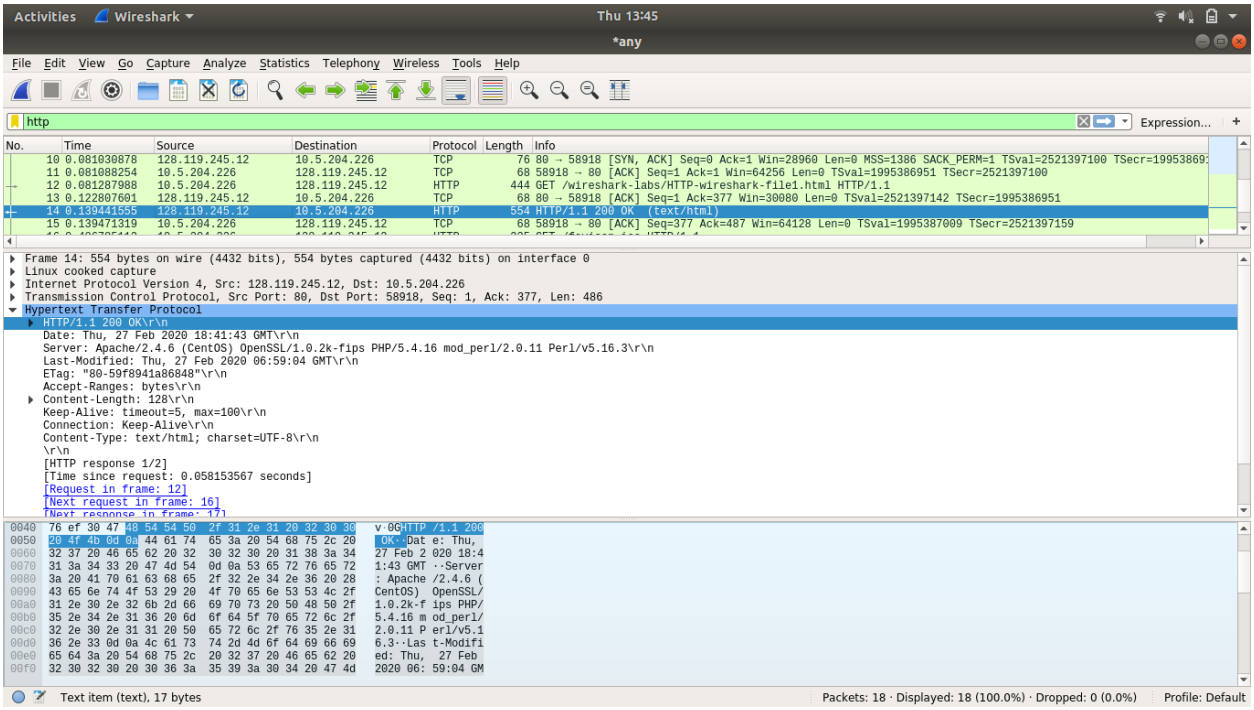

Image 2

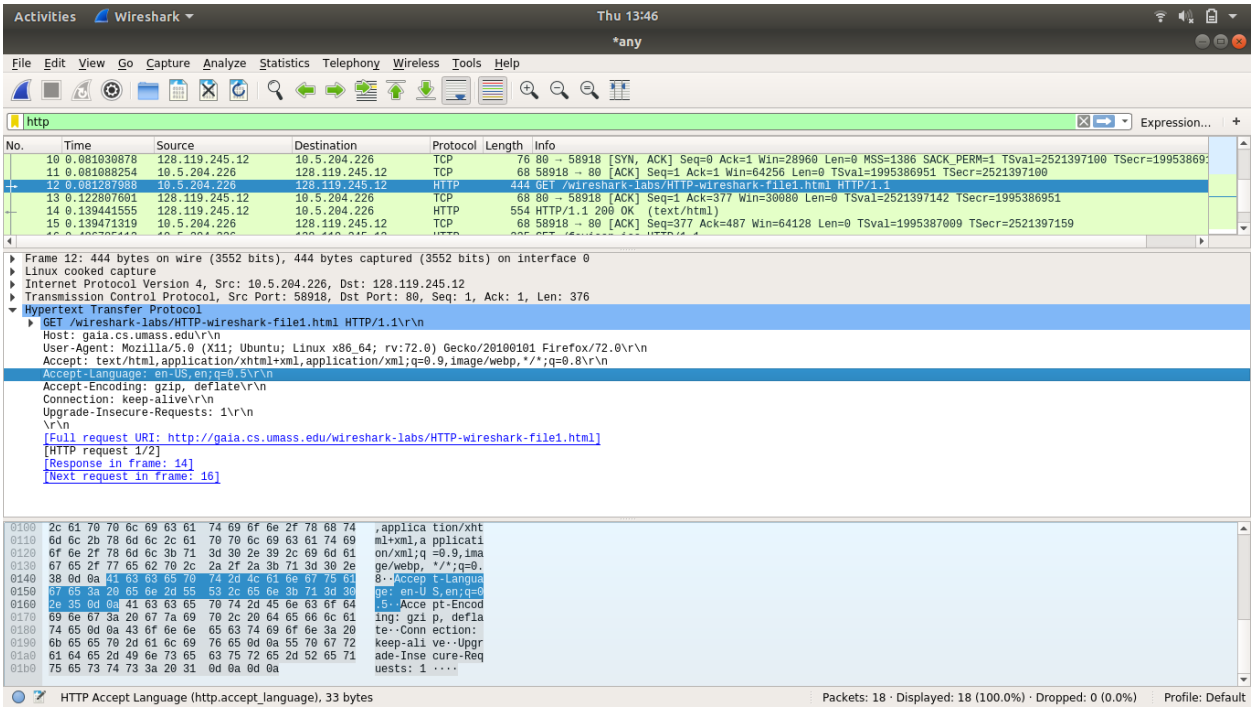

Image 3

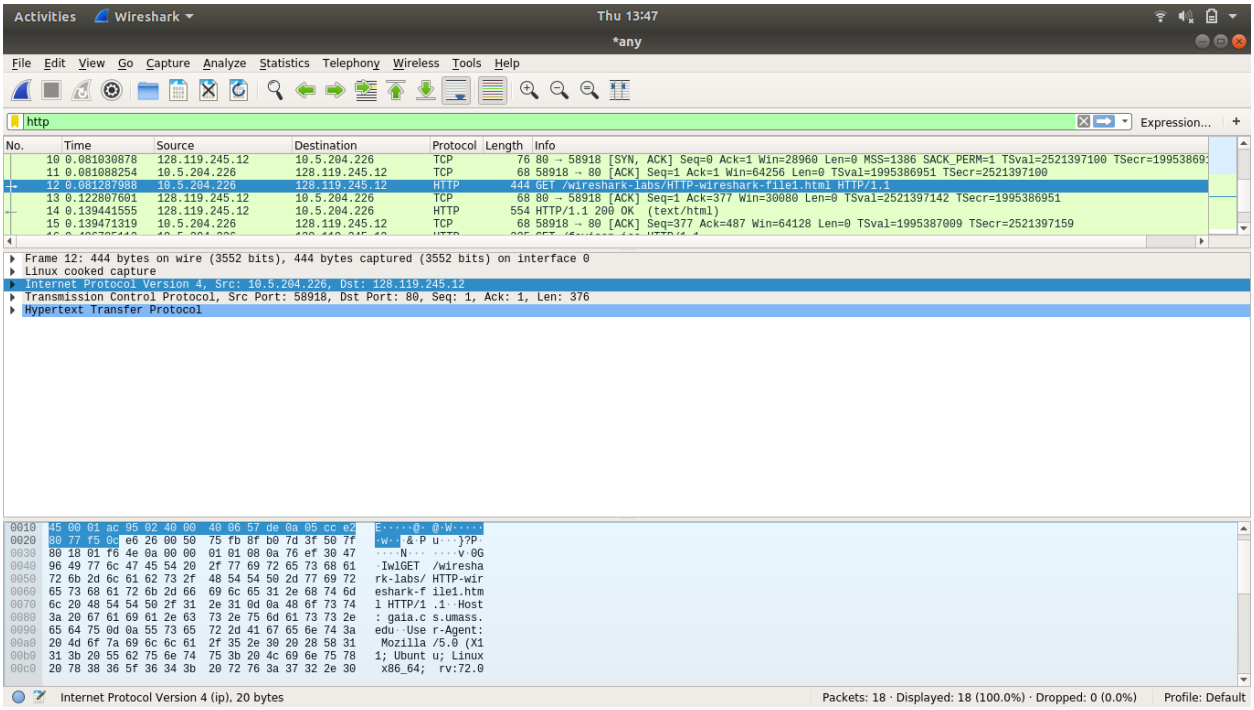

Image 4

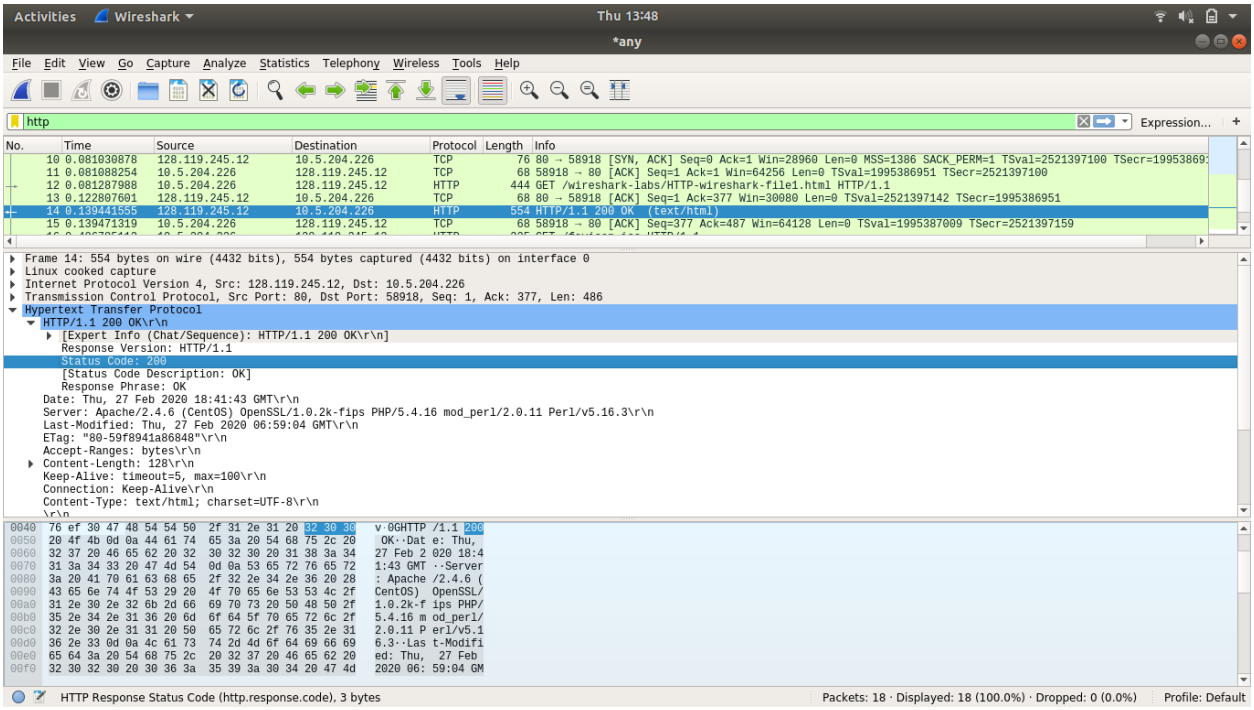

Image 5

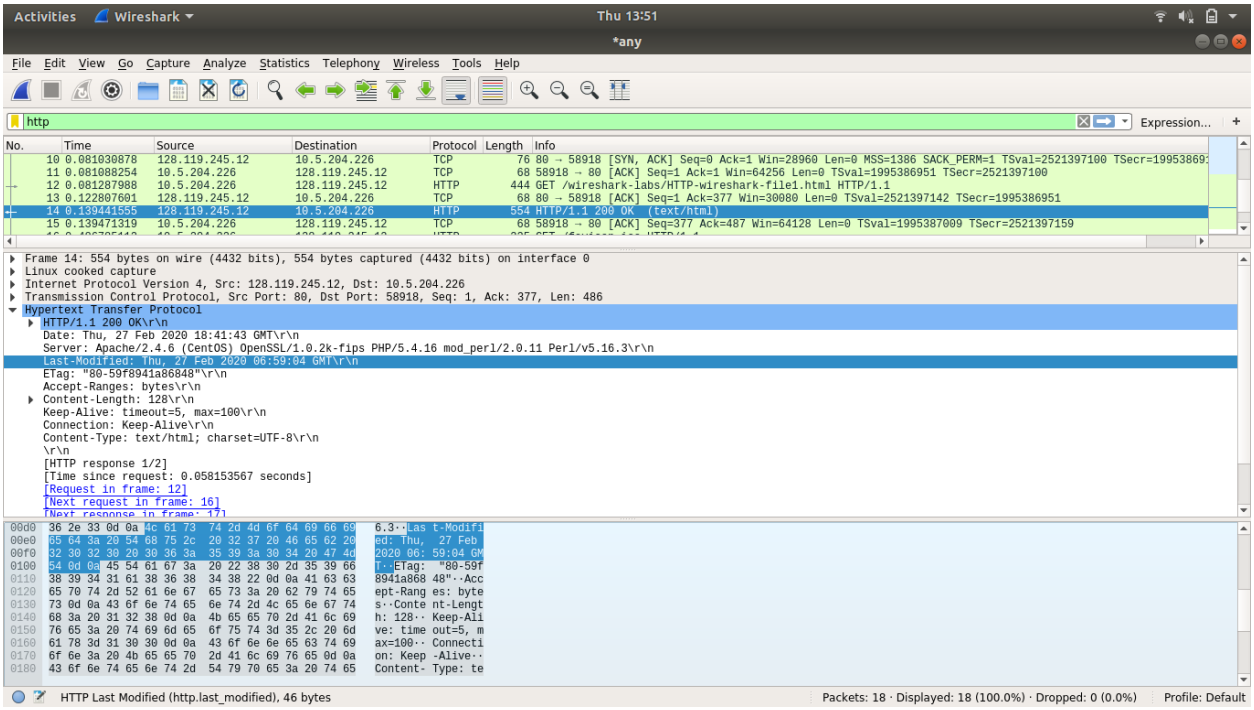

Image 6

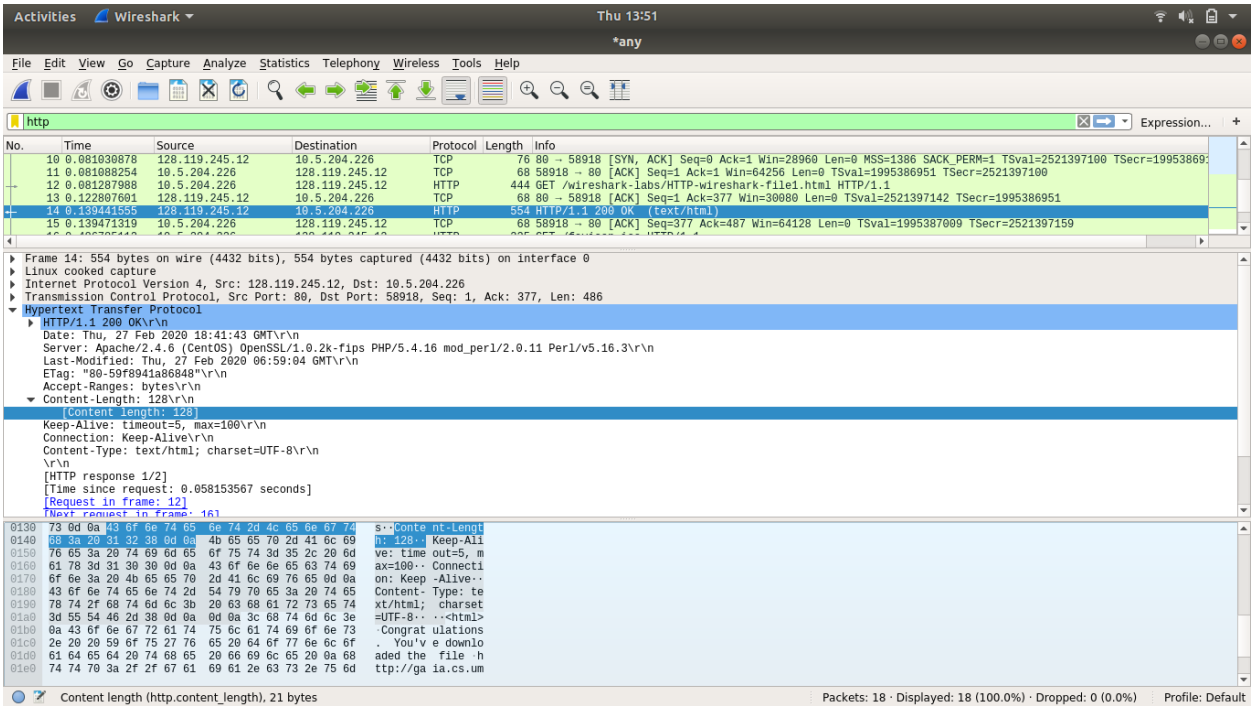
Activities
Wireshark
Thu 13:51
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
No. Time Source Destination Protocol Length Info
10 0.081030878 128.119.245.12 10.5.204.226 TCP 76 80 → 58918 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1386 SACK_PERM=1 TSval=2521397100 TSecr=19953869
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
[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 1/2]
[Time since request: 0.058153567 seconds]
[Request in frame: 12]
0130 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 s··Conte nt-Lengt
0140 68 3a 20 31 32 38 0d 0a 4b 65 65 70 2d 41 6c 69 h: 128·· Keep-Ali
0150 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c 20 6d ve: time out=5, m
0160 61 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63 74 69 ax=100·· Connecti
0170 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a on: Keep -Alive··
0180 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 Content- Type: te
0190 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 xt/html; charset
01a0 3d 55 54 46 2d 38 0d 0a 0d 0a 3c 68 74 6d 6c 3e =UTF-8·· ··<html>
01b0 0a 43 6f 6e 67 72 61 74 75 6c 61 74 69 6f 6e 73 ·Congrat ulations
01c0 2e 20 20 59 6f 75 27 76 65 20 64 6f 77 6e 6c 6f . You'v e downlo
01d0 61 64 65 64 20 74 68 65 20 66 69 6c 65 20 0a 68 aded the file ·h
01e0 74 74 70 3a 2f 2f 67 61 69 61 2e 63 73 2e 75 6d ttp://ga ia.cs.um
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.

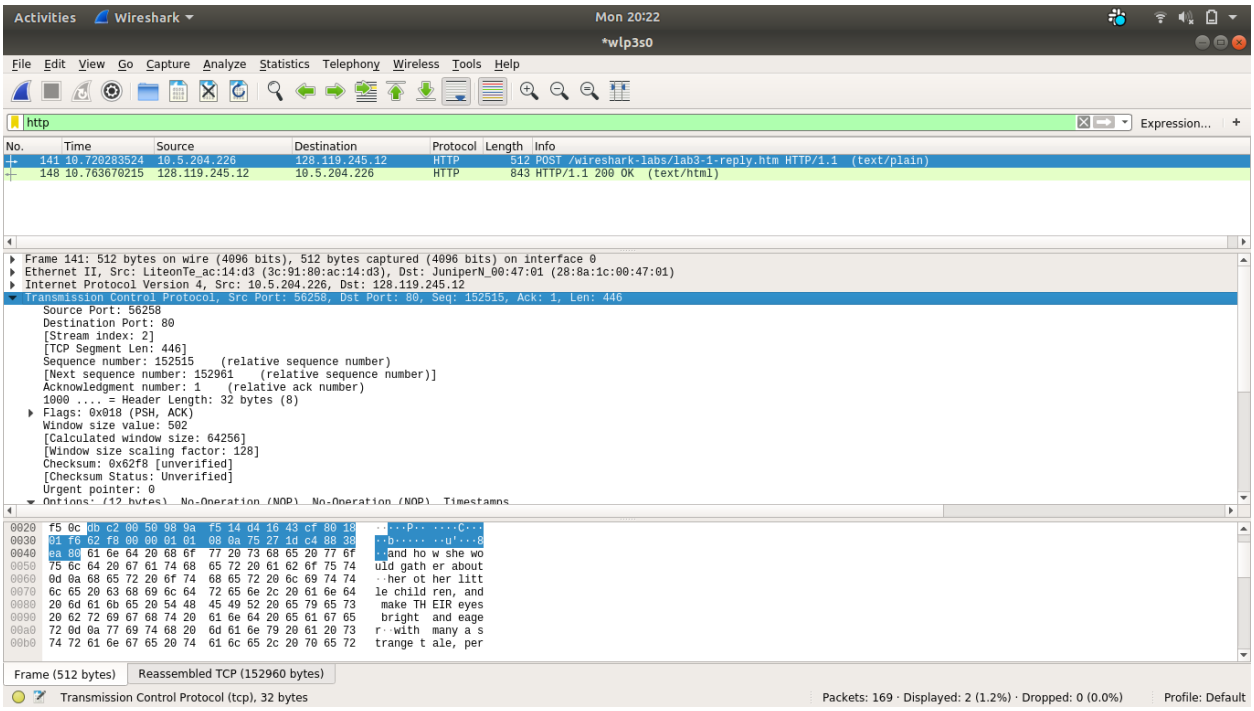

Image 1

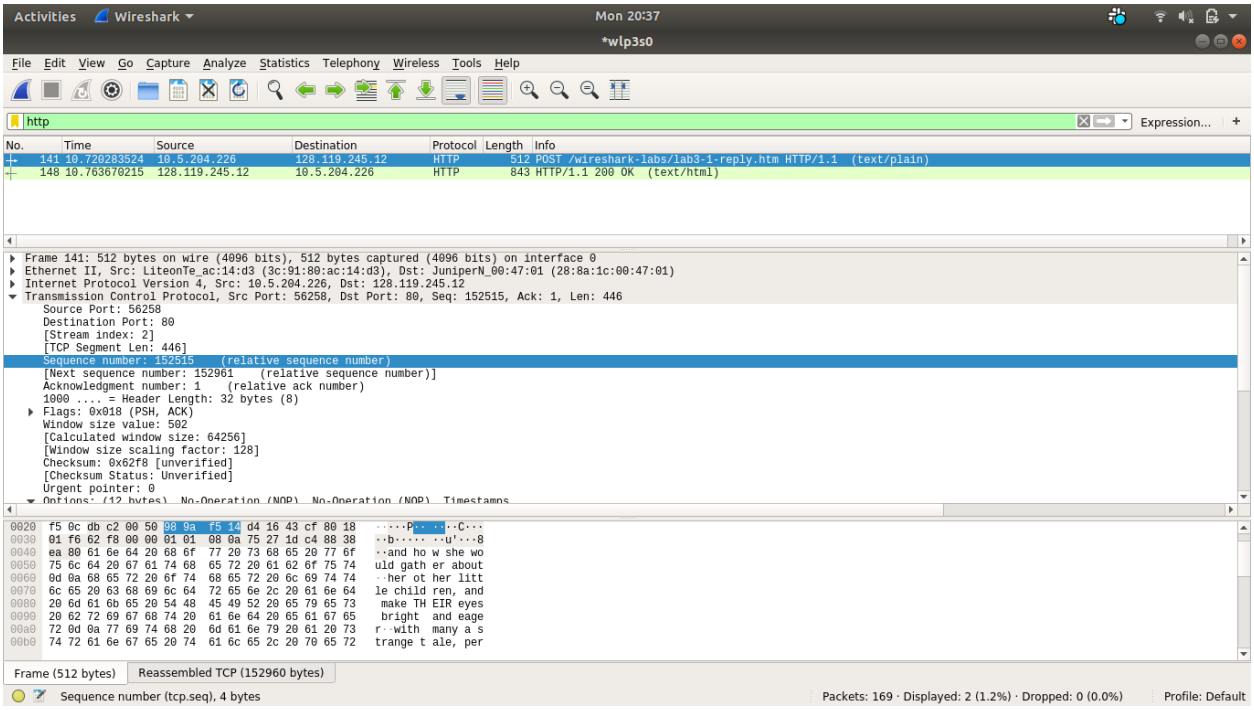

Image 2

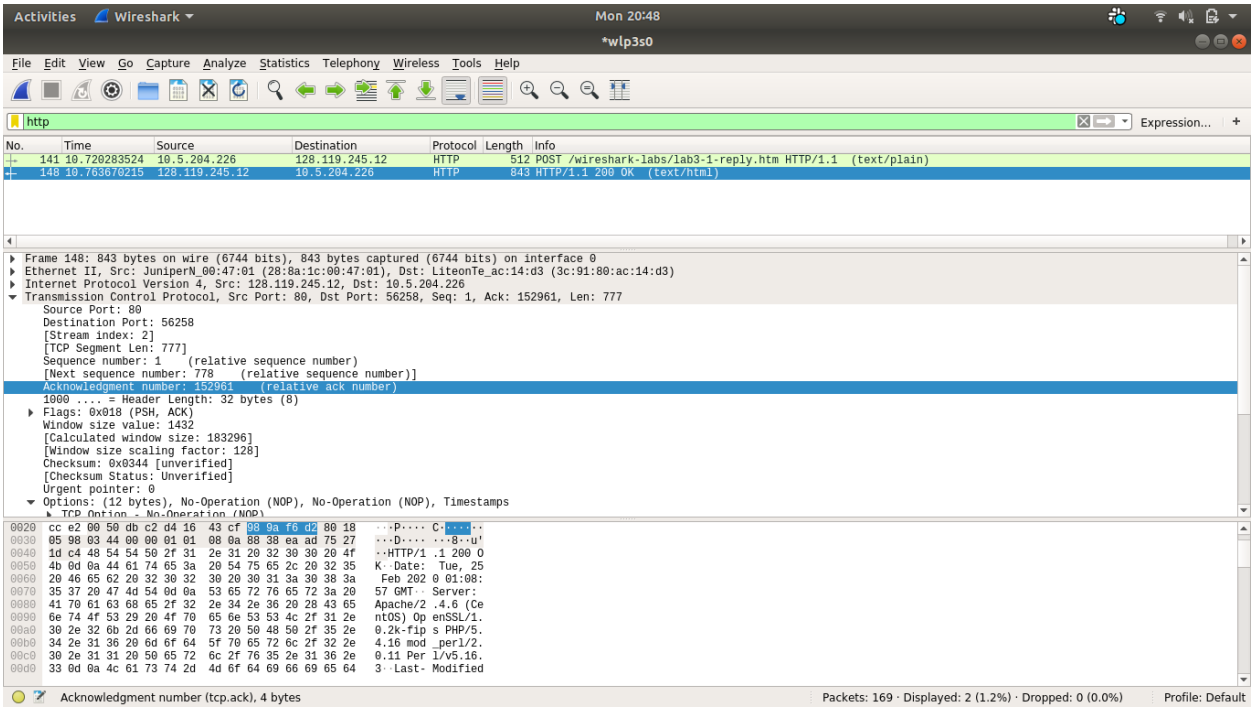
Activities
Wireshark
Mon 20:48
*wlp3s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
No. Time Source Destination Protocol Length Info
141 10.720283524 10.5.204.226 128.119.245.12 HTTP 512 POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
148 10.763670215 128.119.245.12 10.5.204.226 HTTP 843 HTTP/1.1 200 OK (text/html)
Frame 148: 843 bytes on wire (6744 bits), 843 bytes captured (6744 bits) on interface 0
Ethernet II, Src: JuniperN_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: 10.5.204.226
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)
1000 .... = Header Length: 32 bytes (8)
Flags: 0x018 (PSH, ACK)
Window size value: 1432
[Calculated window size: 183296]
[Window size scaling factor: 128]
Checksum: 0x0344 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
TCP Option - No-Operation (NOP)
0020 cc e2 00 50 db c2 d4 16 43 cf 98 9a f6 d2 80 18
0030 05 98 03 44 00 00 01 01 08 0a 88 38 ea ad 75 27
0040 1d c4 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f
0050 4b 0d 0a 44 61 74 65 3a 20 54 75 65 2c 20 32 35
0060 20 46 65 62 20 32 30 32 30 20 30 31 3a 30 38 3a
0070 35 37 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20
0080 41 70 61 63 68 65 2f 32 2e 34 2e 36 20 28 43 65
0090 6e 74 4f 53 29 20 4f 70 65 6e 53 53 4c 2f 31 2e
00a0 30 2e 32 6b 2d 66 69 70 73 20 50 48 50 2f 35 2e
00b0 34 2e 31 36 20 6d 6f 64 5f 70 65 72 6c 2f 32 2e
00c0 30 2e 31 31 20 50 65 72 6c 2f 76 35 2e 31 36 2e
00d0 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64
Acknowledgment number (tcp.ack), 4 bytes
Packets: 169 · Displayed: 2 (1.2%) · Dropped: 0 (0.0%)
Profile: Default

Image 3