Exercise 1

1

UDP, HTTP og TCP

2

It took approximately 0.2 seconds to receive the HTTP OK reply was received after sending the GET request.

3

I interpret "internet address" as IP address, which in that case the IP address is 128.119.245.12.

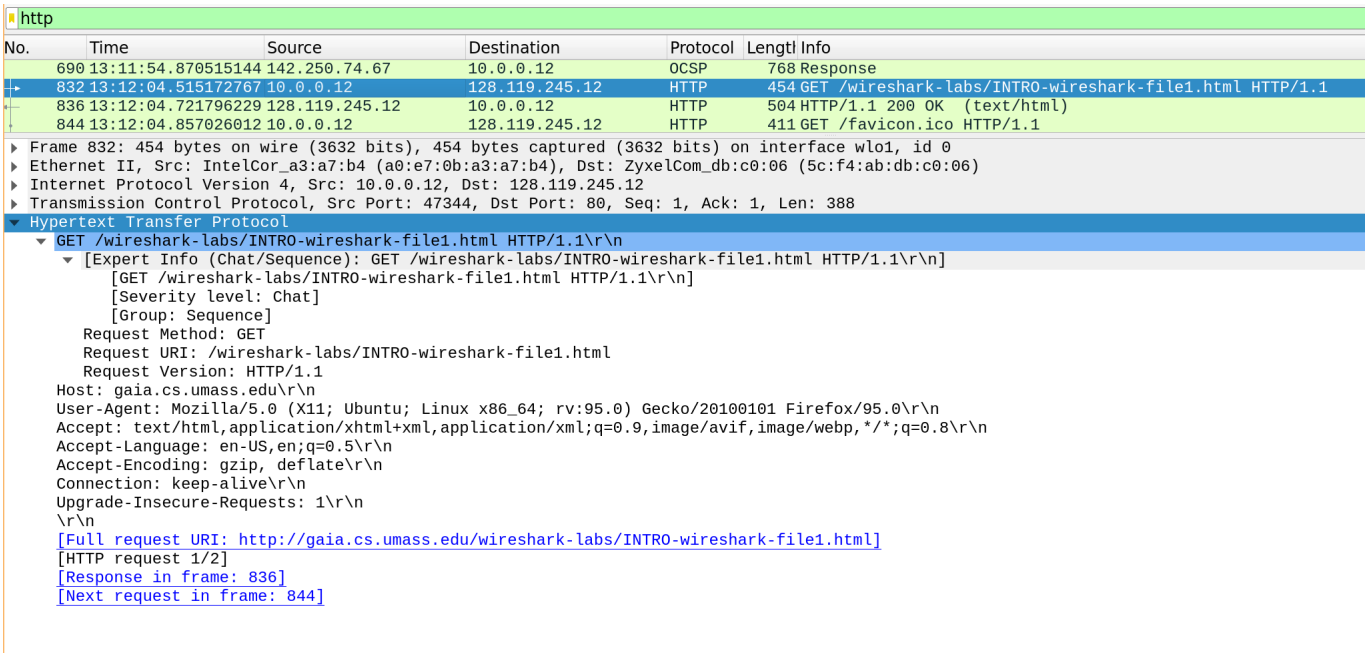
My computers IP address is 10.0.0.12.

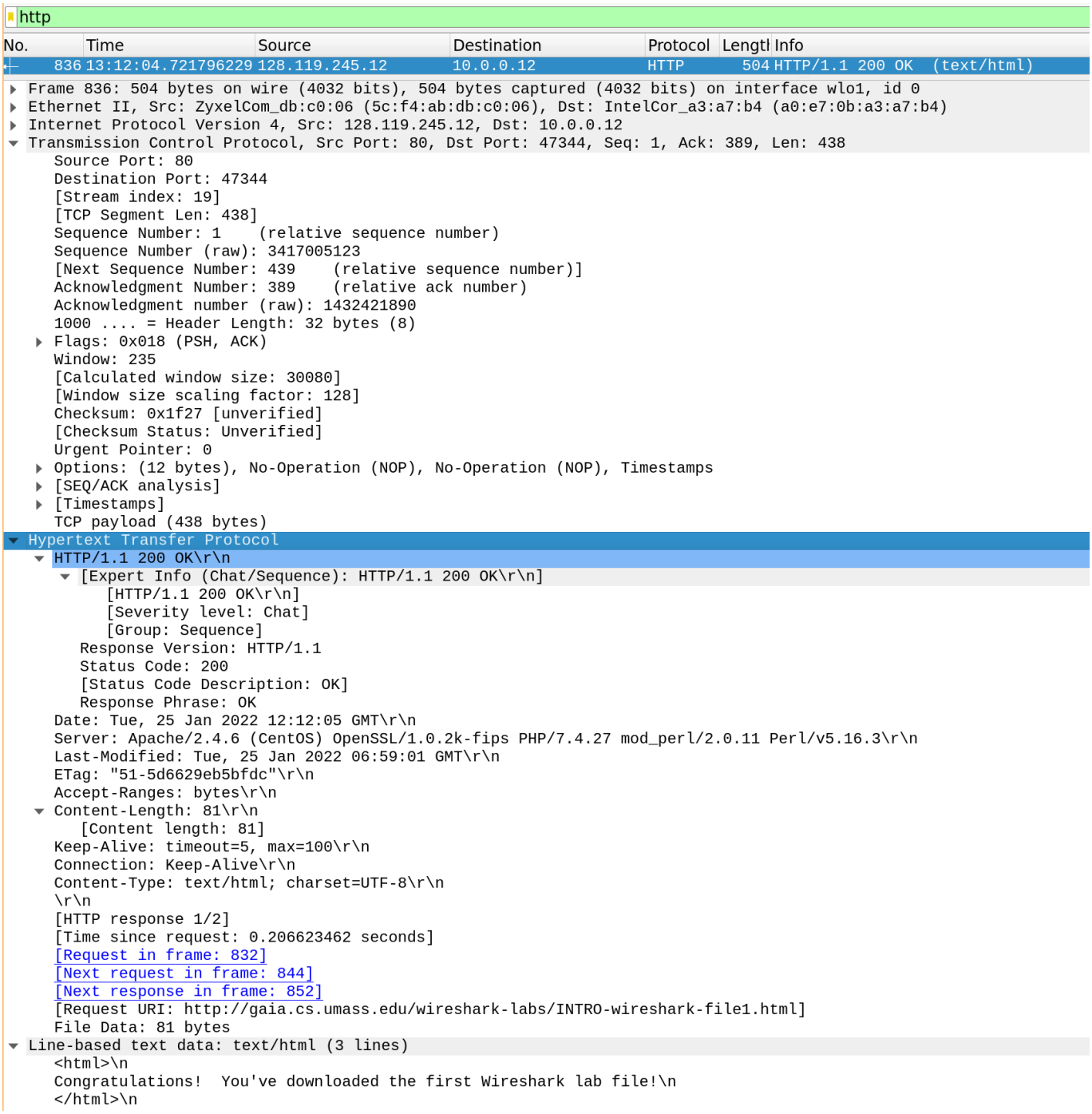
4

It depends on what is meant, the total length of the packet captured is 504 bytes, while the TCP payload is 438 bytes.

The HTML file size is 81 bytes.

5


http
No. Time Source Destination Protocol Lengt Info
690 13:11:54.870515144 142.250.74.67 10.0.0.12 OCSP 768 Response
832 13:12:04.515172767 10.0.0.12 128.119.245.12 HTTP 454 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
836 13:12:04.721796229 128.119.245.12 10.0.0.12 HTTP 504 HTTP/1.1 200 OK (text/html)
844 13:12:04.857026012 10.0.0.12 128.119.245.12 HTTP 411 GET /favicon.ico HTTP/1.1
Frame 832: 454 bytes on wire (3632 bits), 454 bytes captured (3632 bits) on interface wlo1, id 0
Ethernet II, Src: IntelCor_a3:a7:b4 (a0:e7:0b:a3:a7:b4), Dst: ZyxelCom_db:c0:06 (5c:f4:ab:db:c0:06)
Internet Protocol Version 4, Src: 10.0.0.12, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 47344, Dst Port: 80, Seq: 1, Ack: 1, Len: 388
Hypertext Transfer Protocol
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
[GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /wireshark-labs/INTRO-wireshark-file1.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:95.0) Gecko/20100101 Firefox/95.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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/INTRO-wireshark-file1.html]
[HTTP request 1/2]
[Response in frame: 836]
[Next request in frame: 844]


http
No. Time Source Destination Protocol Lengt Info
836 13:12:04.721796229 128.119.245.12 10.0.0.12 HTTP 504 HTTP/1.1 200 OK (text/html)
Frame 836: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits) on interface wlo1, id 0
Ethernet II, Src: ZyxelCom_db:c0:06 (5c:f4:ab:db:c0:06), Dst: IntelCor_a3:a7:b4 (a0:e7:0b:a3:a7:b4)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.12
Transmission Control Protocol, Src Port: 80, Dst Port: 47344, Seq: 1, Ack: 389, Len: 438
Source Port: 80
Destination Port: 47344
[Stream index: 19]
[TCP Segment Len: 438]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 3417005123
[Next Sequence Number: 439 (relative sequence number)]
Acknowledgment Number: 389 (relative ack number)
Acknowledgment number (raw): 1432421890
1000 .... = Header Length: 32 bytes (8)
Flags: 0x018 (PSH, ACK)
Window: 235
[Calculated window size: 30080]
[Window size scaling factor: 128]
Checksum: 0x1f27 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[SEQ/ACK analysis]
[Timestamps]
TCP payload (438 bytes)
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
[HTTP/1.1 200 OK\r\n]
[Severity level: Chat]
[Group: Sequence]
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Tue, 25 Jan 2022 12:12:05 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.27 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Tue, 25 Jan 2022 06:59:01 GMT\r\n
ETag: "51-5d6629eb5bfdc"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 81\r\n
[Content length: 81]
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: 0.206623462 seconds]
[Request in frame: 832]
[Next request in frame: 844]
[Next response in frame: 852]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
File Data: 81 bytes
Line-based text data: text/html (3 lines)
<html>\n
Congratulations! You've downloaded the first Wireshark lab file!\n
</html>\n