Lab 4: UDP & its content

Book: Section 3.3, 3.3.1, 3.3.2.

Part 1. Theory and structure of UDP.

1) What is the local IP address of your laptop/PC given to you by the DHCP server?
2) What's your laptop/PC's mac address?
3) What is the default gateway address on your laptop/PC?
4) What is the DNS address on your laptop/PC?

Questions 1, 2, 3, and 4 must be answered with a single screenshot ***P1-4*** which contains proof of all 4 points above. These questions don't give you any points and the absence of answers for these questions will nullify your lab 4 grade.

5) How many fields are in the UDP datagram?
6) Name those fields:

Questions 5 and 6 must be answered with a single screenshot P5-6, where the screenshot must contain proof either from the book or from one of those websites: https://www.rfc-editor.org or https://www.ietf.org or https://datatracker.ietf.org

7) Which of those fields are required and which are optional?

You may include the answer for question 7 in ***P5-6*** or make it separate as ***P7*** and the screenshot must contain proof either from the book or any website, which you think is "reliable". Hint: 3 websites shown above are reliable.

8) What is a UDP payload? The screenshot must contain the structure of the UDP header, plus your own explanation on the screenshot, which is at least 1 sentence long.
9) How UDP payload's size is determined from the "length" field? Say, you know the value of length, and you are asked to find a UDP payload's size. How do you do that? Explain it on the same screenshot.
10) How many bytes is the size of the destination port? BUT HOW DID YOU FIND OUT?

Questions 8, 9, and 10 must be answered on screenshot ***P8-10***.

Part 2. Practice. Is youtube really UDP? Or TCP?

11) What is the transport layer protocol used by youtube?

12) Has Google implemented it inside the company or have they bought it from another company?

Questions 11 and 12 must be answered on screenshot ***P11-12***. The screenshot must contain proof from a reliable website.

13) Is it constructed by the principles of TCP or UDP?

Question 13 must be answered on screenshot ***P13***. The screenshot must contain proof and your summary, which is 1-3 sentences long.

14) What are the advantages of that protocol?

Question 14 must be answered on screenshot ***P14***. The screenshot must contain proof and your summary, which is 1-3 sentences long.

Now try to prove that your answer to Q11 is correct. Capture packets of that protocol in Wireshark, save your wireshark file as "*L4_youtube*" for submission. Make a screenshot ***P15*** where you pick a packet of 'protocol from Q11', annotate its name in the packet list window on Wireshark.

15) What port number does that protocol use? The screenshot must contain details from your wireshark file. The port number must be annotated in the packet details window. Put the answer on screenshot ***P15***.

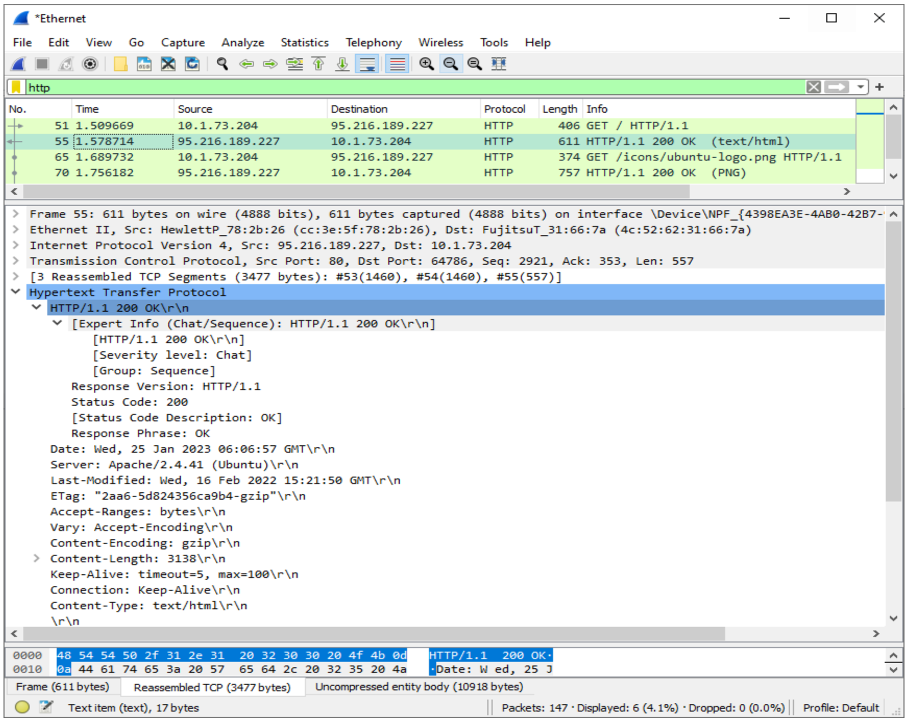
16) On screenshot ***P15***, make visible "***Protocol_name IETF***" section from the packet details window. The content of that section must be visible and annotated.

Submit: (screenshots are *jpg* or *png*, wireshark file is *pcapng*)
P1-4 **-** screenshot of from terminal (0 for the lab, if not uploaded)
P5-6 - screenshot of UDP datagram fields
P7 - screenshot optional and required fields of UDP
P8-10 **-** screenshots for UDP payload, destination port field.
P11-12 - screenshot of youtube's protocol
P13 **-** screenshot of youtube's protocol's transport methods.
P14 - screenshot of youtube's protocol's advantages
P15 - screenshots for the last part, from wireshark.
L4_youtube - wireshark capture file for the last part.

!Attention! Using wrong filename for screenshots or wireshark files will lead to loss of points.
If you don't submit a screenshot or a wireshark file for a particular part, that part will be graded as 0.

IMPORTANT! How to annotate a screenshot as a correct proof to your answer.
Incorrect proof doesn't give any points.

1) Incorrect proof:


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

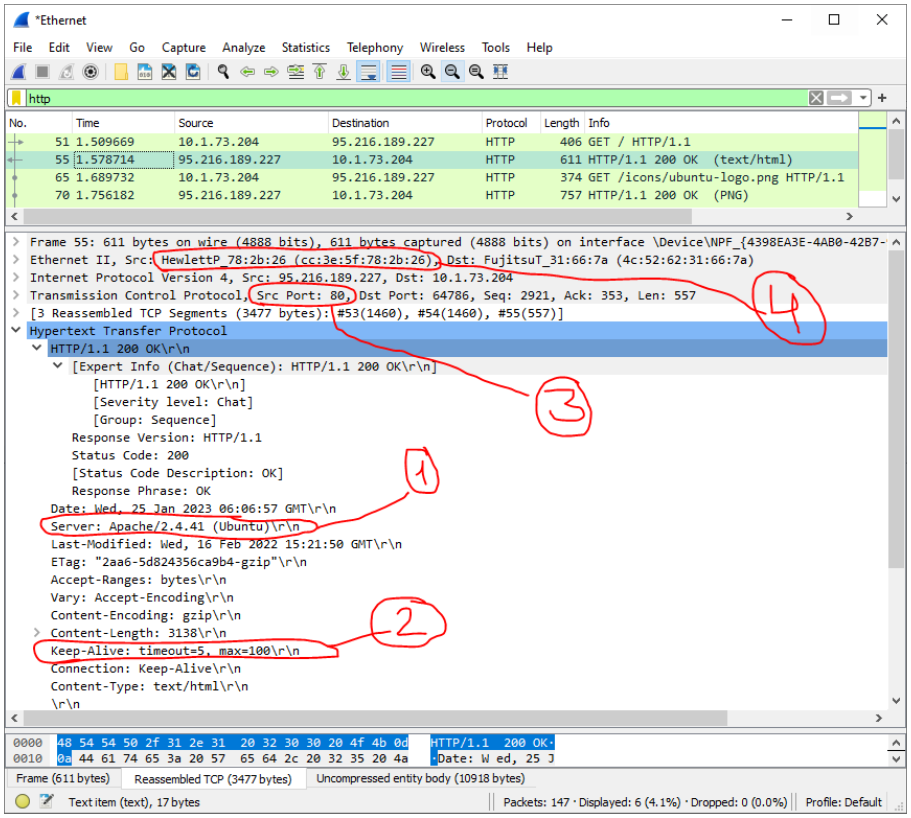
```
No.   Time       Source          Destination     Protocol  Length Info
   51 1.509669   10.1.73.204     95.216.189.227  HTTP       406 GET / HTTP/1.1
   55 1.578714   95.216.189.227  10.1.73.204     HTTP       611 HTTP/1.1 200 OK  (text/html)
   65 1.689732   10.1.73.204     95.216.189.227  HTTP       374 GET /icons/ubuntu-logo.png HTTP/1.1
   70 1.756182   95.216.189.227  10.1.73.204     HTTP       757 HTTP/1.1 200 OK  (PNG)
```

```
> Frame 55: 611 bytes on wire (4888 bits), 611 bytes captured (4888 bits) on interface \Device\NPF_{4398EA3E-4AB0-42B7-
> Ethernet II, Src: HewlettP_78:2b:26 (cc:3e:5f:78:2b:26), Dst: FujitsuT_31:66:7a (4c:52:62:31:66:7a)
> Internet Protocol Version 4, Src: 95.216.189.227, Dst: 10.1.73.204
> Transmission Control Protocol, Src Port: 80, Dst Port: 64786, Seq: 2921, Ack: 353, Len: 557
> [3 Reassembled TCP Segments (3477 bytes): #53(1460), #54(1460), #55(557)]
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    v [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: Wed, 25 Jan 2023 06:06:57 GMT\r\n
    Server: Apache/2.4.41 (Ubuntu)\r\n
    Last-Modified: Wed, 16 Feb 2022 15:21:50 GMT\r\n
    ETag: "2aa6-5d824356ca9b4-gzip"\r\n
    Accept-Ranges: bytes\r\n
    Vary: Accept-Encoding\r\n
    Content-Encoding: gzip\r\n
  > Content-Length: 3138\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html\r\n
    \r\n
```

```
0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1 200 OK·
0010  0a 44 61 74 65 3a 20 57  65 64 2c 20 32 35 20 4a   ·Date: W ed, 25 J
```

Figure 10: incorrect proof. No annotations.

2) Correct proof:


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
4
3
1
2

```
No.   Time       Source          Destination     Protocol  Length Info
   51 1.509669   10.1.73.204     95.216.189.227  HTTP       406 GET / HTTP/1.1
   55 1.578714   95.216.189.227  10.1.73.204     HTTP       611 HTTP/1.1 200 OK  (text/html)
   65 1.689732   10.1.73.204     95.216.189.227  HTTP       374 GET /icons/ubuntu-logo.png HTTP/1.1
   70 1.756182   95.216.189.227  10.1.73.204     HTTP       757 HTTP/1.1 200 OK  (PNG)
```

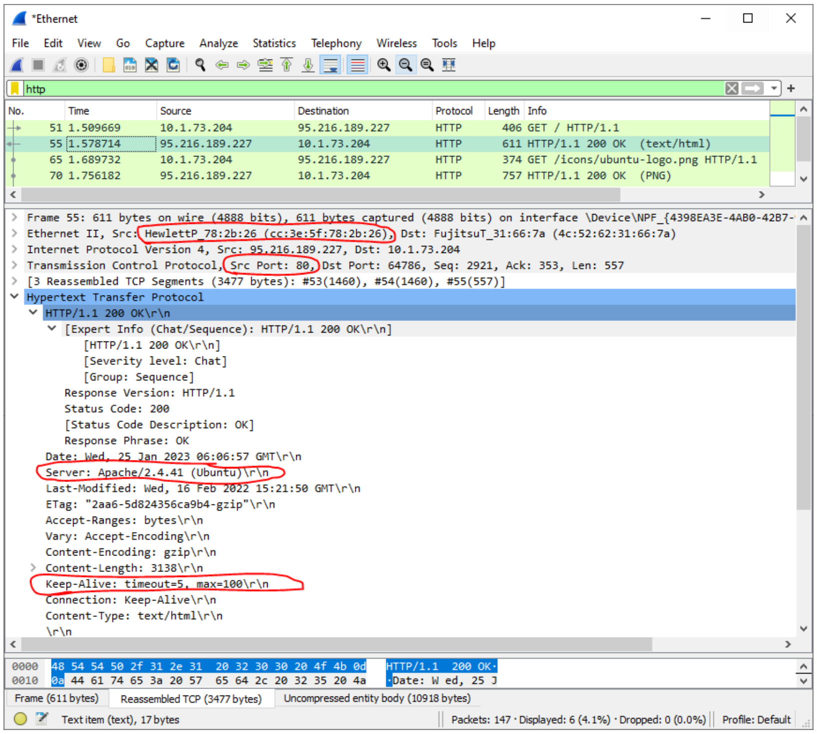
```
> Frame 55: 611 bytes on wire (4888 bits), 611 bytes captured (4888 bits) on interface \Device\NPF_{4398EA3E-4AB0-42B7-
> Ethernet II, Src: HewlettP_78:2b:26 (cc:3e:5f:78:2b:26), Dst: FujitsuT_31:66:7a (4c:52:62:31:66:7a)
> Internet Protocol Version 4, Src: 95.216.189.227, Dst: 10.1.73.204
> Transmission Control Protocol, Src Port: 80, Dst Port: 64786, Seq: 2921, Ack: 353, Len: 557
> [3 Reassembled TCP Segments (3477 bytes): #53(1460), #54(1460), #55(557)]
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    v [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: Wed, 25 Jan 2023 06:06:57 GMT\r\n
    Server: Apache/2.4.41 (Ubuntu)\r\n
    Last-Modified: Wed, 16 Feb 2022 15:21:50 GMT\r\n
    ETag: "2aa6-5d824356ca9b4-gzip"\r\n
    Accept-Ranges: bytes\r\n
    Vary: Accept-Encoding\r\n
    Content-Encoding: gzip\r\n
  > Content-Length: 3138\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html\r\n
    \r\n
```

```
0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1 200 OK·
0010  0a 44 61 74 65 3a 20 57  65 64 2c 20 32 35 20 4a   ·Date: W ed, 25 J
```

Frame (611 bytes)
Reassembled TCP (3477 bytes)
Uncompressed entity body (10918 bytes)
Text item (text), 17 bytes
Packets: 147 · Displayed: 6 (4.1%) · Dropped: 0 (0.0%)
Profile: Default

Figure 11: correct proof. Red annotations with question numbers shown.

3) Incorrect proof:



*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time        Source          Destination     Protocol Length Info
   51 1.509669    10.1.73.204     95.216.189.227  HTTP     406 GET / HTTP/1.1
   55 1.578714    95.216.189.227  10.1.73.204     HTTP     611 HTTP/1.1 200 OK  (text/html)
   65 1.689732    10.1.73.204     95.216.189.227  HTTP     374 GET /icons/ubuntu-logo.png HTTP/1.1
   70 1.756182    95.216.189.227  10.1.73.204     HTTP     757 HTTP/1.1 200 OK  (PNG)
```

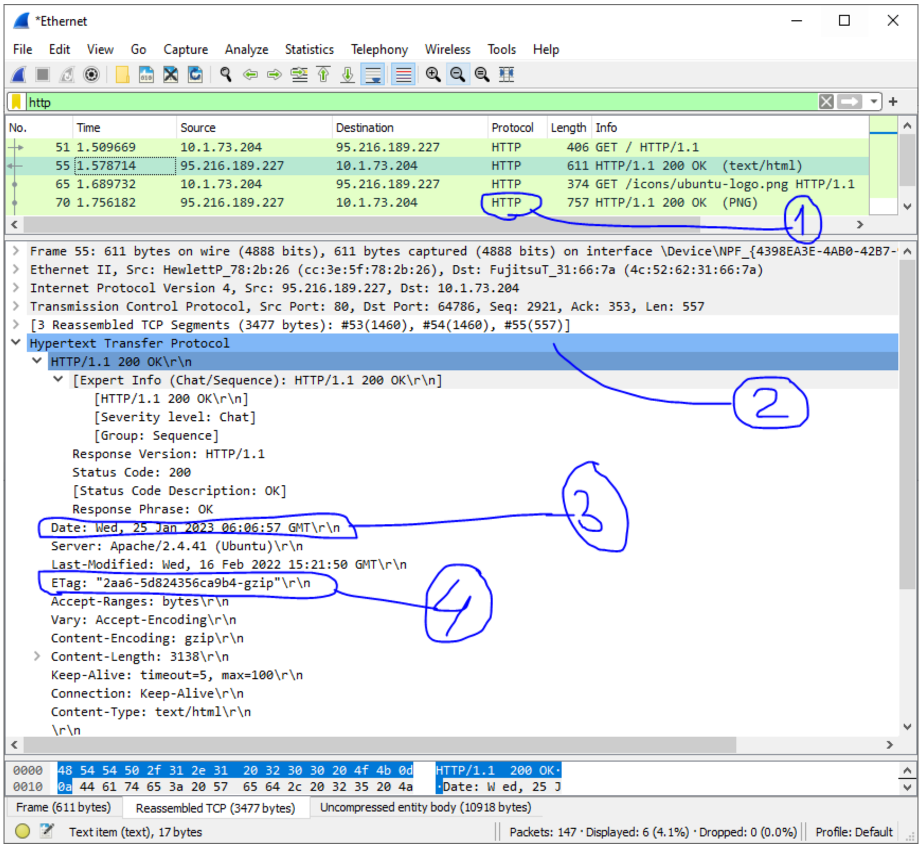
```
> Frame 55: 611 bytes on wire (4888 bits), 611 bytes captured (4888 bits) on interface \Device\NPF_{4398EA3E-4AB0-42B7-
> Ethernet II, Src: HewlettP_78:2b:26 (cc:3e:5f:78:2b:26), Dst: FujitsuT_31:66:7a (4c:52:62:31:66:7a)
> Internet Protocol Version 4, Src: 95.216.189.227, Dst: 10.1.73.204
> Transmission Control Protocol, Src Port: 80, Dst Port: 64786, Seq: 2921, Ack: 353, Len: 557
> [3 Reassembled TCP Segments (3477 bytes): #53(1460), #54(1460), #55(557)]
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    v [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: Wed, 25 Jan 2023 06:06:57 GMT\r\n
    Server: Apache/2.4.41 (Ubuntu)\r\n
    Last-Modified: Wed, 16 Feb 2022 15:21:50 GMT\r\n
    ETag: "2aa6-5d824356ca9b4-gzip"\r\n
    Accept-Ranges: bytes\r\n
    Vary: Accept-Encoding\r\n
    Content-Encoding: gzip\r\n
  > Content-Length: 3138\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html\r\n
    \r\n

0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK·
0010  0a 44 61 74 65 3a 20 57  65 64 2c 20 32 35 20 4a   ·Date: W ed, 25 J
```

Frame (611 bytes)
Reassembled TCP (3477 bytes)
Uncompressed entity body (10918 bytes)
Text item (text), 17 bytes
Packets: 147 · Displayed: 6 (4.1%) · Dropped: 0 (0.0%)
Profile: Default

Figure 12: incorrect proof. Annotations without the question numbers.

4) Incorrect proof:



*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
1
2
3
4

```
No.   Time        Source          Destination     Protocol Length Info
   51 1.509669    10.1.73.204     95.216.189.227  HTTP     406 GET / HTTP/1.1
   55 1.578714    95.216.189.227  10.1.73.204     HTTP     611 HTTP/1.1 200 OK  (text/html)
   65 1.689732    10.1.73.204     95.216.189.227  HTTP     374 GET /icons/ubuntu-logo.png HTTP/1.1
   70 1.756182    95.216.189.227  10.1.73.204     HTTP     757 HTTP/1.1 200 OK  (PNG)
```

```
> Frame 55: 611 bytes on wire (4888 bits), 611 bytes captured (4888 bits) on interface \Device\NPF_{4398EA3E-4AB0-42B7-
> Ethernet II, Src: HewlettP_78:2b:26 (cc:3e:5f:78:2b:26), Dst: FujitsuT_31:66:7a (4c:52:62:31:66:7a)
> Internet Protocol Version 4, Src: 95.216.189.227, Dst: 10.1.73.204
> Transmission Control Protocol, Src Port: 80, Dst Port: 64786, Seq: 2921, Ack: 353, Len: 557
> [3 Reassembled TCP Segments (3477 bytes): #53(1460), #54(1460), #55(557)]
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    v [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: Wed, 25 Jan 2023 06:06:57 GMT\r\n
    Server: Apache/2.4.41 (Ubuntu)\r\n
    Last-Modified: Wed, 16 Feb 2022 15:21:50 GMT\r\n
    ETag: "2aa6-5d824356ca9b4-gzip"\r\n
    Accept-Ranges: bytes\r\n
    Vary: Accept-Encoding\r\n
    Content-Encoding: gzip\r\n
  > Content-Length: 3138\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html\r\n
    \r\n

0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK·
0010  0a 44 61 74 65 3a 20 57  65 64 2c 20 32 35 20 4a   ·Date: W ed, 25 J
```

Frame (611 bytes)
Reassembled TCP (3477 bytes)
Uncompressed entity body (10918 bytes)
Text item (text), 17 bytes
Packets: 147 · Displayed: 6 (4.1%) · Dropped: 0 (0.0%)
Profile: Default

Figure 13: incorrect proof. Annotations are not red.