My computer’s Execution environment for assignment

1. HW information

* processor: Intel(R) Core(TM) i5-10210U CPU @ 1.60GHz (8 CPUs), 2.1GHz
* memory : 8192MB RAM

1. System information

* OS: Windows 10 Enterprise 64비트 (10.0, 빌드 19041)
  + Windows 사양
    - edition: Windows 10 Enterprise
    - version : 2004
    - OS build : 19041.388
* language : Korean
* system model 17ZD995-VX50K
* BIOS : C1ZE0110 X64

Wireshark version : <Wireshark 3.4.9 stable> version

Wi-Fi

SSID: WUNIST\_AAA

protocol: Wi-Fi 5(802.11ac)

링크-로컬 IPv6 주소: fe80::e00c:a3ea:d344:f65a%23

IPv4 address: 10.64.131.140

IPv4 DNS server: 10.4.1.151

10.4.1.152

Web

I analyze NAVER which has host name ‘[www.naver.com](http://www.naver.com)’ and 223.130.200.104 is one of it’s address

HTTP Request Message is like below

GET / HTTP/1.1 // request line

Host: 223.130.200.104 /\* header lines which is naver’s address

Connection: keep-alive //

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9

Accept-Encoding: gzip, deflate

Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7

And HTTP Response Message is like below

HTTP/1.1 302 Moved Temporarily

Server: NWS

Date: Sat, 16 Oct 2021 12:46:13 GMT

Content-Type: text/html

Transfer-Encoding: chunked

Connection: keep-alive

Location: https://www.naver.com/

Vary: Accept-Encoding,User-Agent

8a

<html>

<head><title>302 Found</title></head>

<body>

<center><h1>302 Found</h1></center>

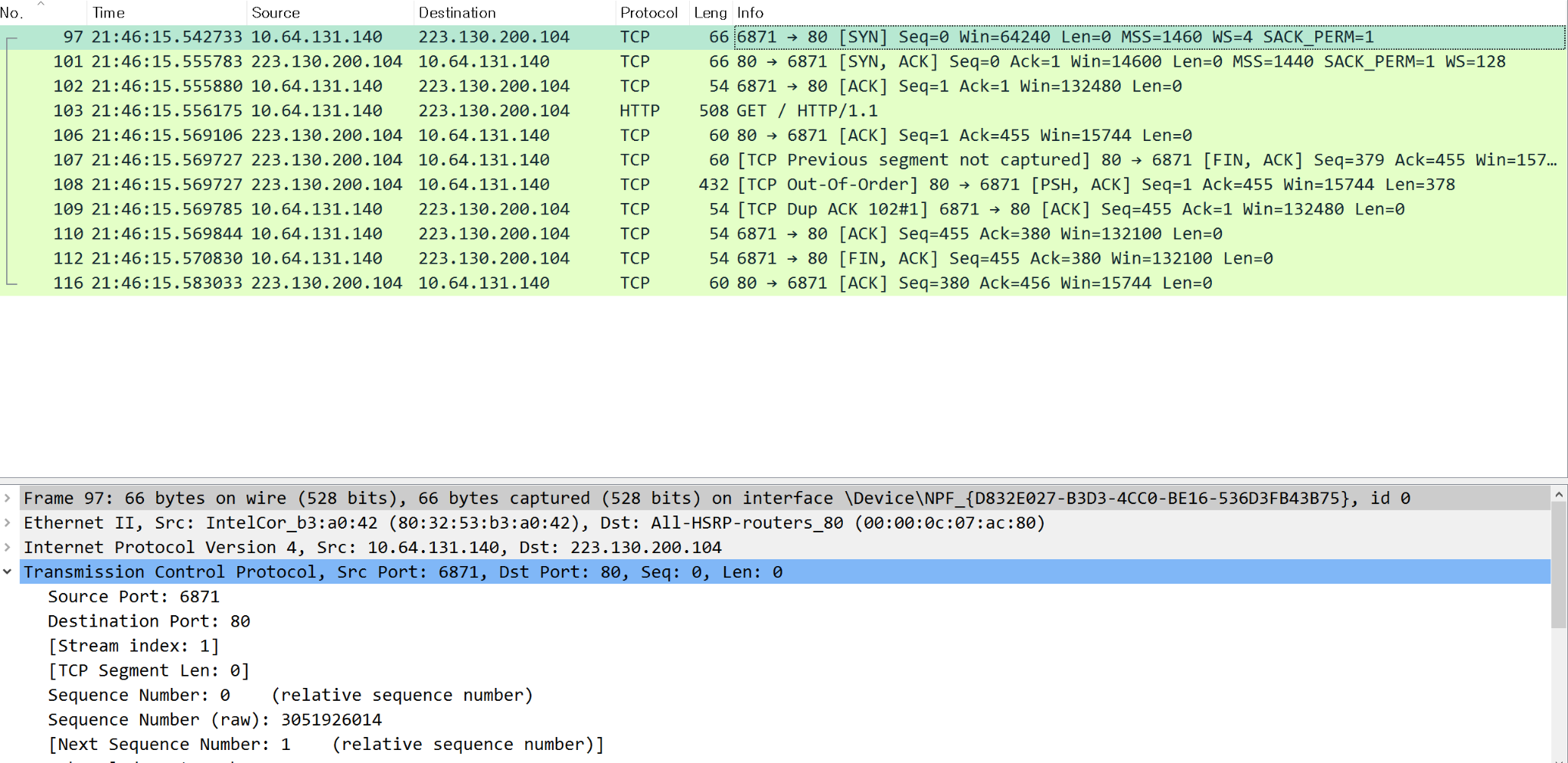
<hr><center> NWS </center>

</body>

</html>

0

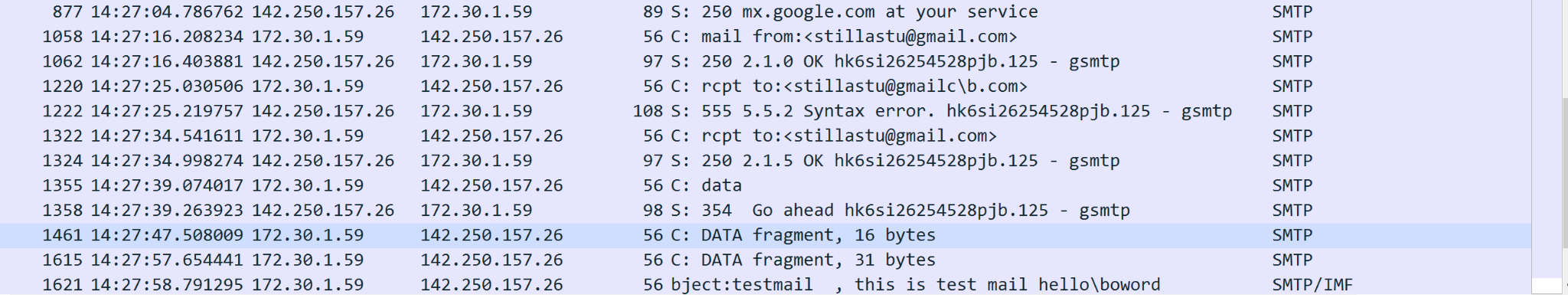
HTTP uses TCP so See below captured picture.



From the contents, we know that it is a non-persistent connection. And the RTT is known from  which in the [Seq/ACK analysis] part. And the length of each packet length.

e-mail

I send email using cmd with telnet commands as below.



It uses SMTP protocol.

And below is the stream.

220 mx.google.com ESMTP hk6si26254528pjb.125 - gsmtp

helo google.com

250 mx.google.com at your service

mail from:<stillastu@gmail.com>

250 2.1.0 OK hk6si26254528pjb.125 - gsmtp

rcpt to:<stillastu@gmailc..com>

555 5.5.2 Syntax error. hk6si26254528pjb.125 - gsmtp

rcpt to:<stillastu@gmail.com>

250 2.1.5 OK hk6si26254528pjb.125 - gsmtp

data

354 Go ahead hk6si26254528pjb.125 - gsmtp

subject:testmail

this is test mail hello.oword

.

421-4.7.0 [115.22.114.231 15] Our system has detected that this message is

421-4.7.0 suspicious due to the very low reputation of the sending IP address.

421-4.7.0 To protect our users from spam, mail sent from your IP address has

421-4.7.0 been temporarily rate limited. Please visit

421 4.7.0 https://support.google.com/mail/answer/188131 for more information. hk6si26254528pjb.125 - gsmtp

I can find several things in it.

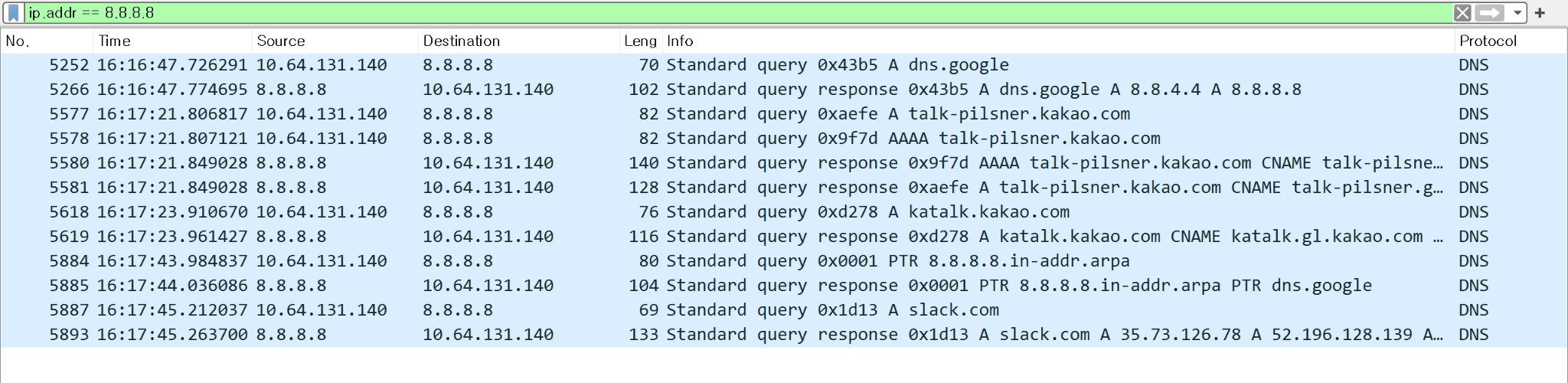
1. packet length
2. Client ip and Server ip
3. Client and Server name
4. Who send the email
5. Who receive the email
6. what is the subject
7. what is the content

And I find that Google protects email from messages.

DNS

In my DNS analysis, it uses the DNS protocol.

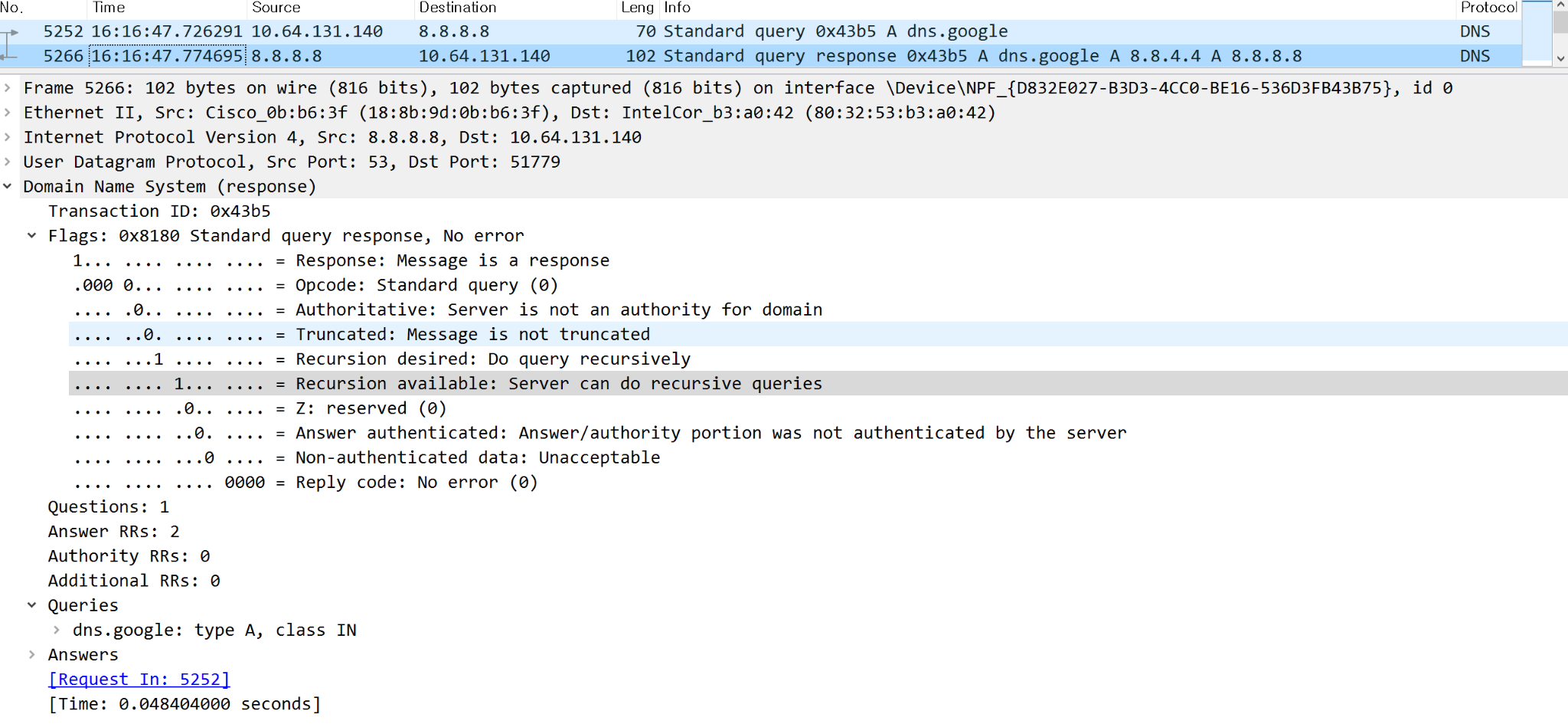
And first, Send DNS Query Message which has information from 10.64.131.140(My local computer) to 8.8.8.8

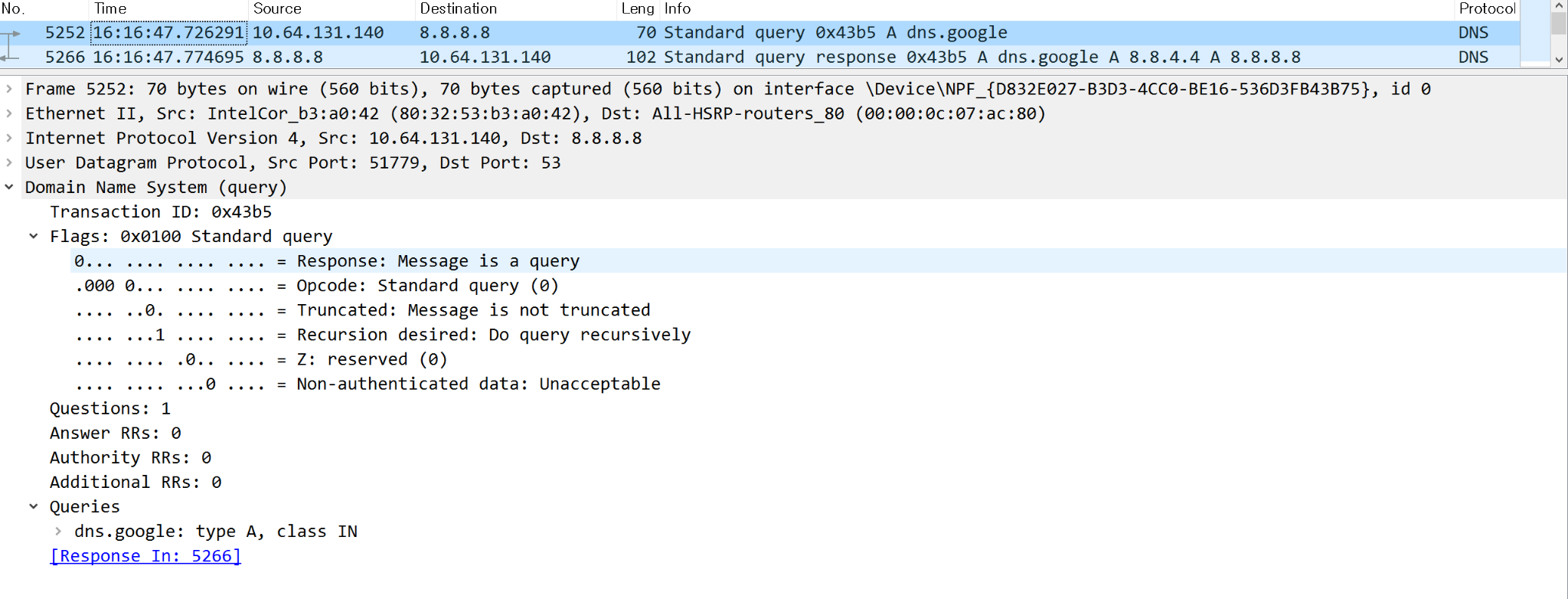
****

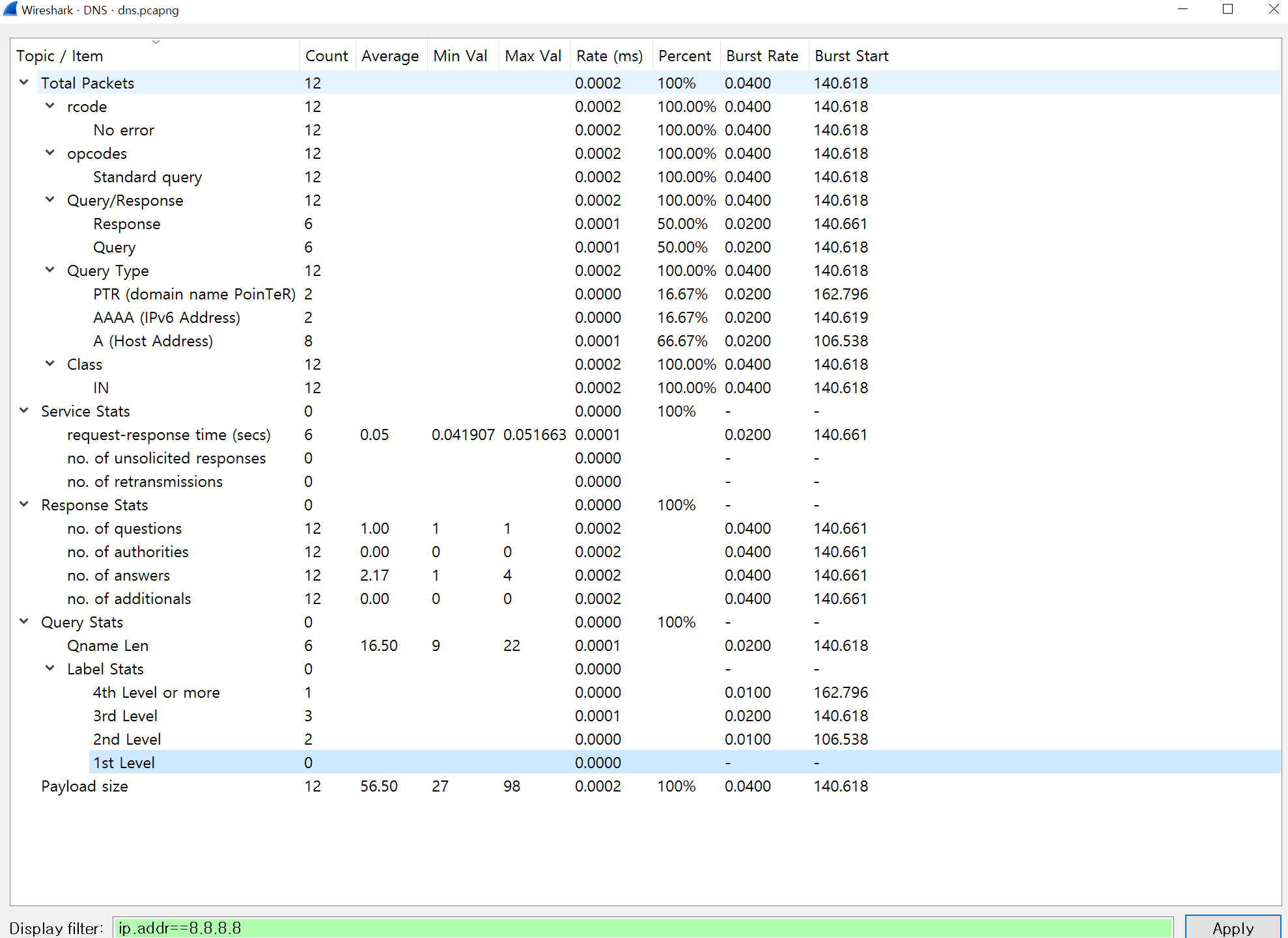
We know that RR has the 4th tuple.(Name, Value, Type, TTL)

And Type is A. So Name is hostname and Value is IP address about hostname.

and query responses like below.

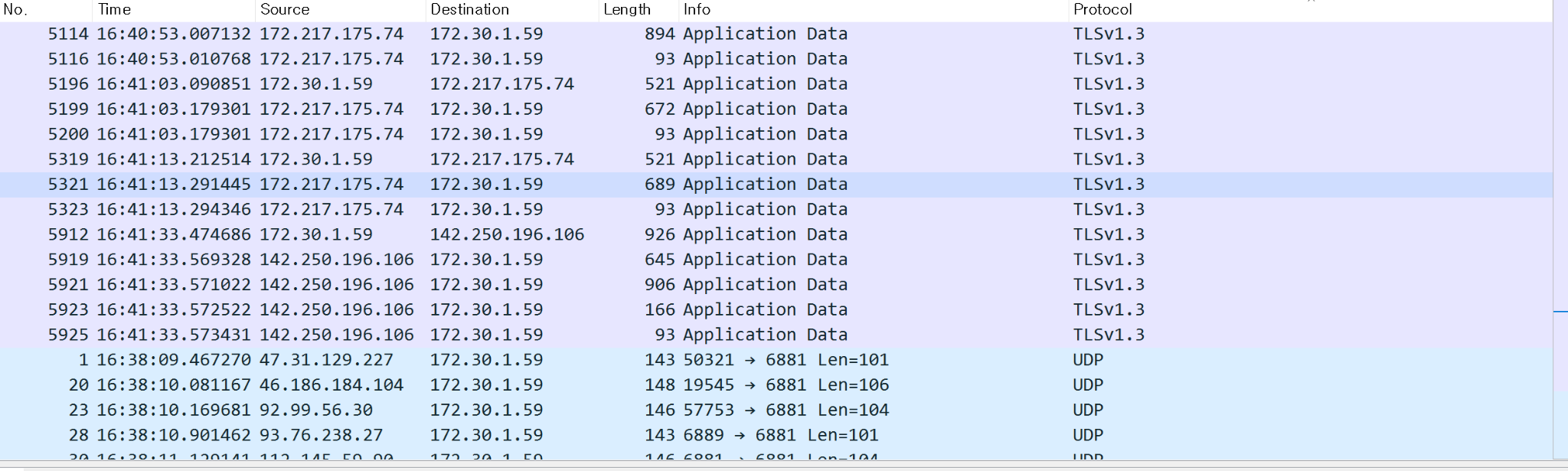






network games

To analyze network games with wireshark, I download amongus with BlueStacks.



There are two kinds of protocol.

One is the UDP protocol and the other is the TLSv1.3 protocol which was not learned.

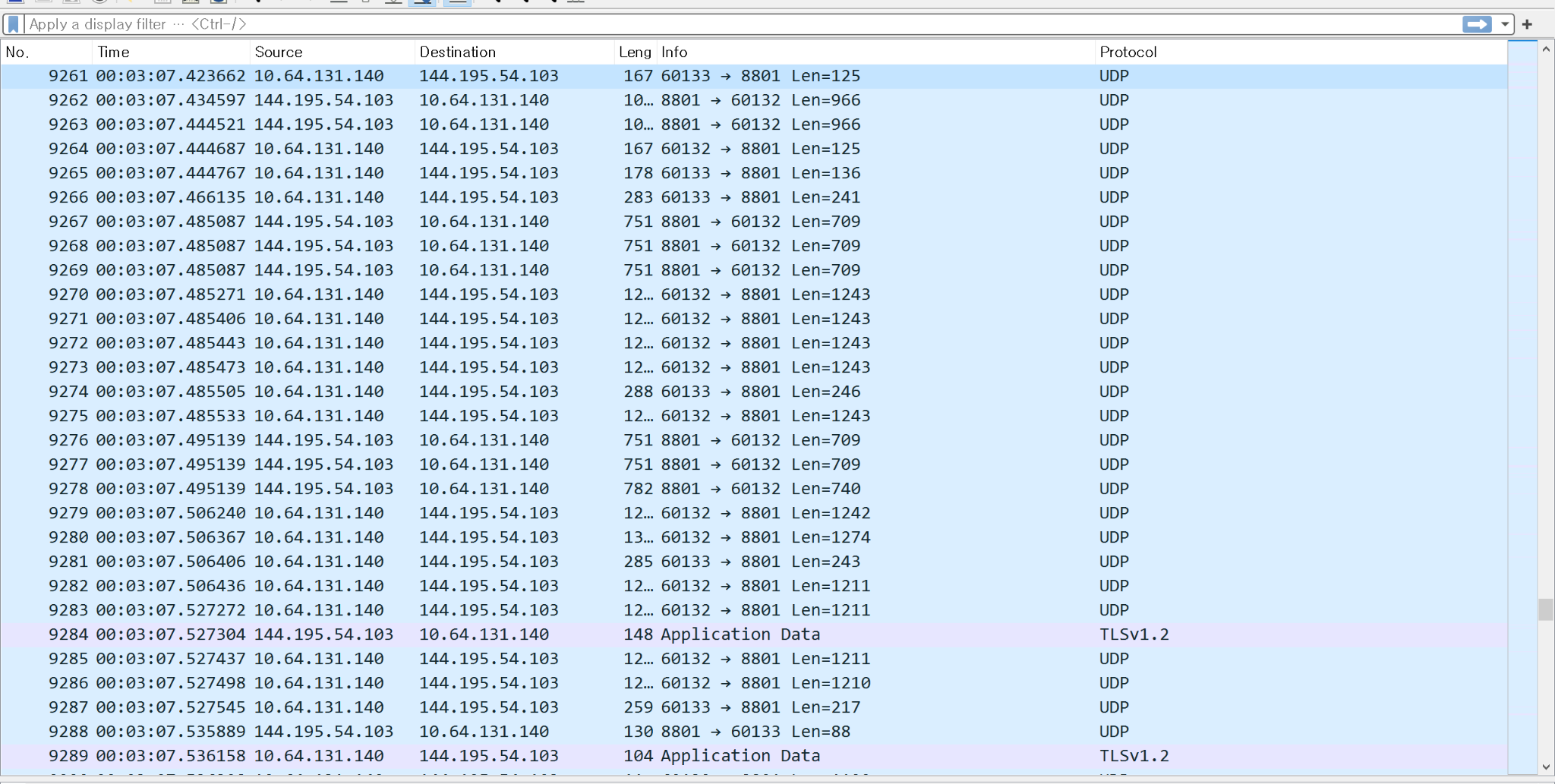
At the end of the TLSv1.3 protocol, UDP protocols are invoked.

So I analyze it as TLSv1.3 for entering the program, and UDP for a faster game.

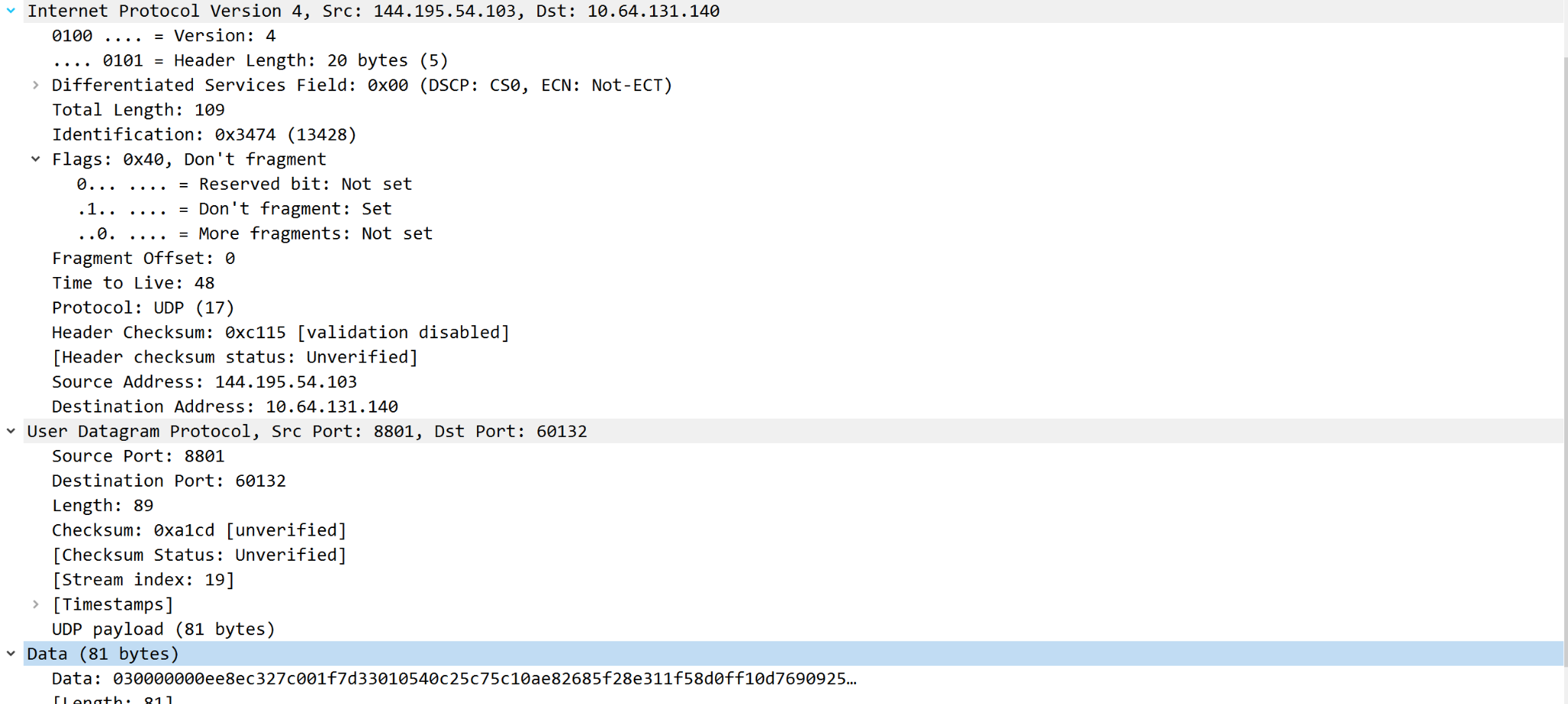
video conferencing

For my video conferencing analysis, I use zoom. And it uses UDP protocol like below.

As we learned, it uses UDP protocol.



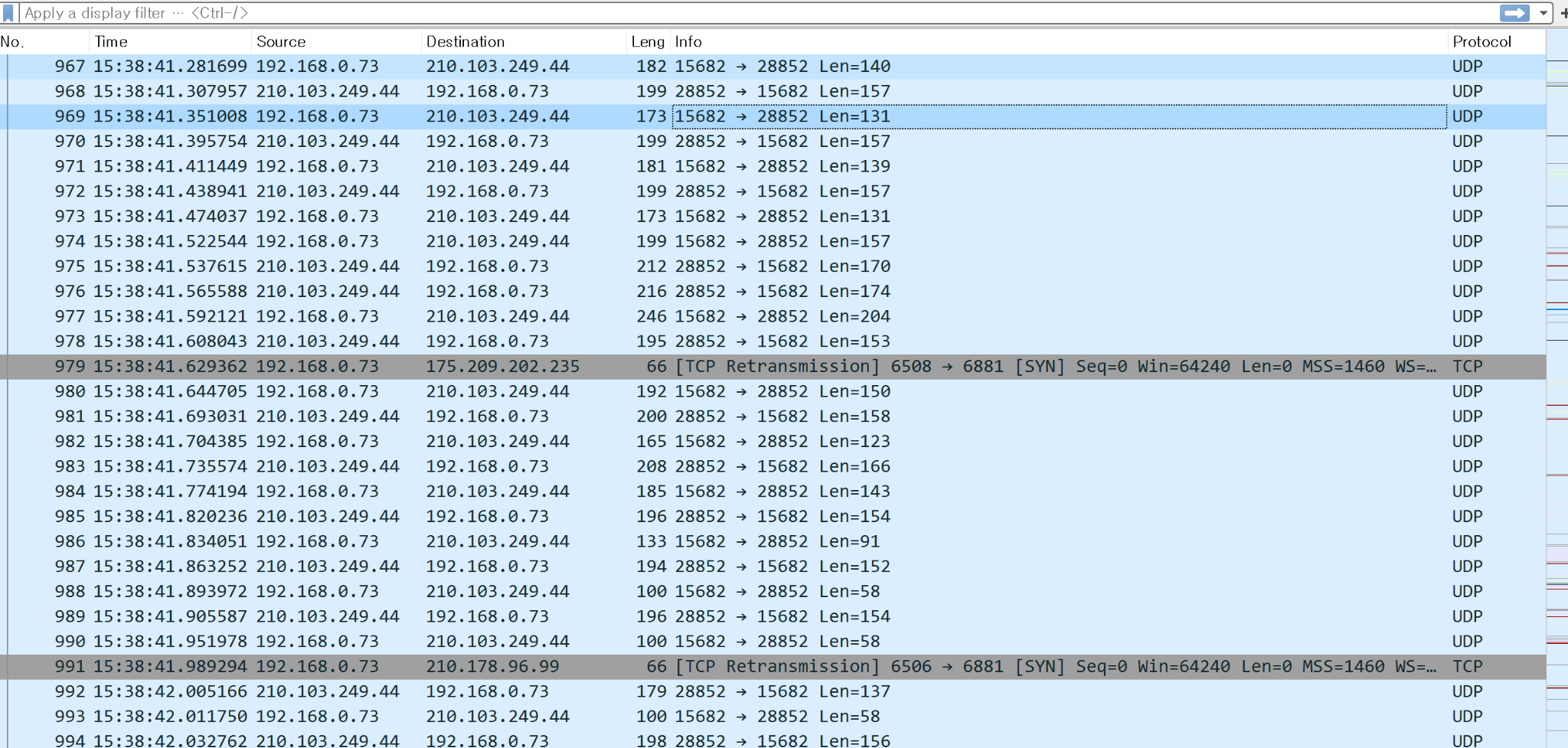
And what is in the packet from below. And as follow stream I saw that ..Zoom Video Communications, Inc.1.0...U... which is seen i use zoom video communications.



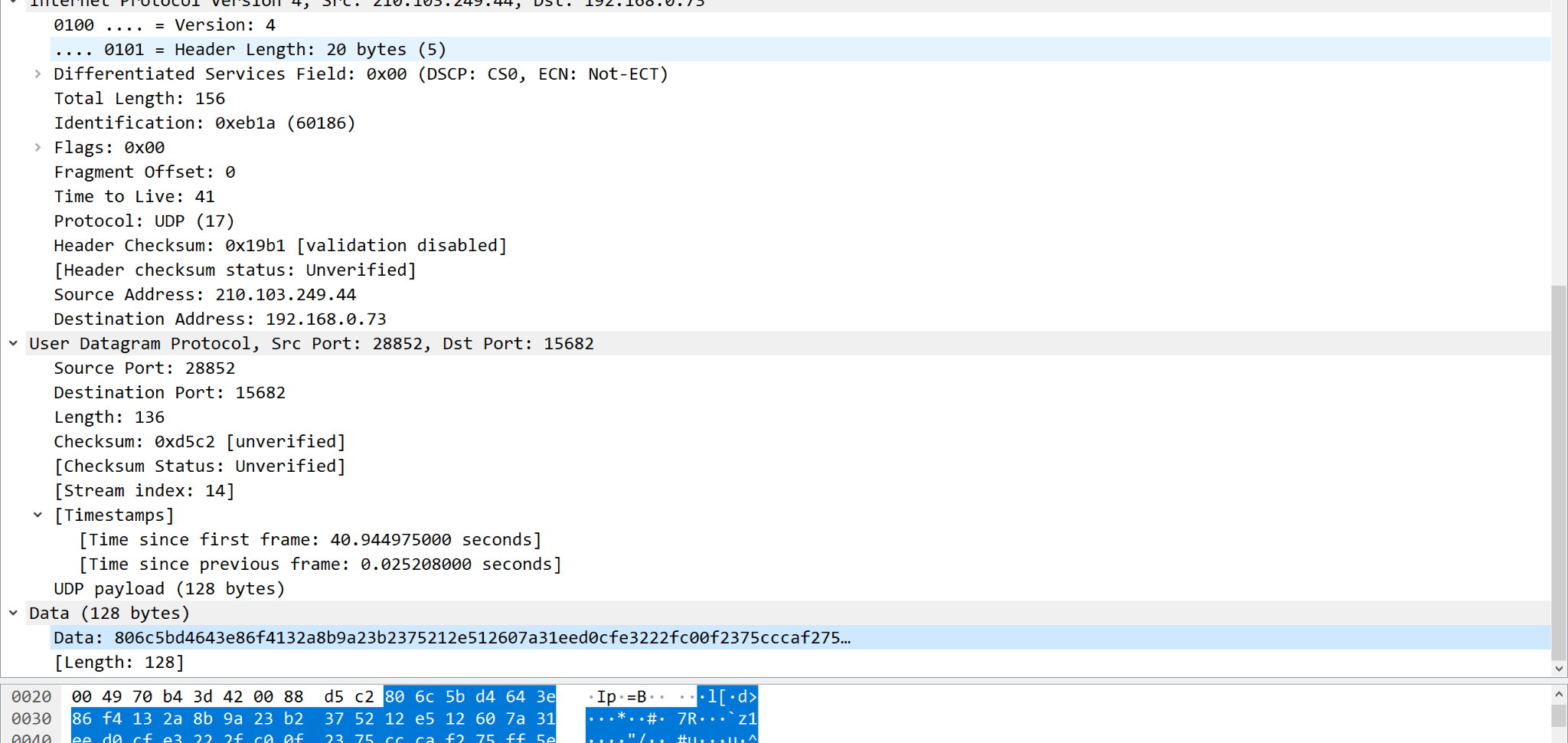
voice over IP

For my voice over ip analysis, I use kakao voice talk. And it uses UDP protocol like below.

As we learned, it uses UDP protocol.



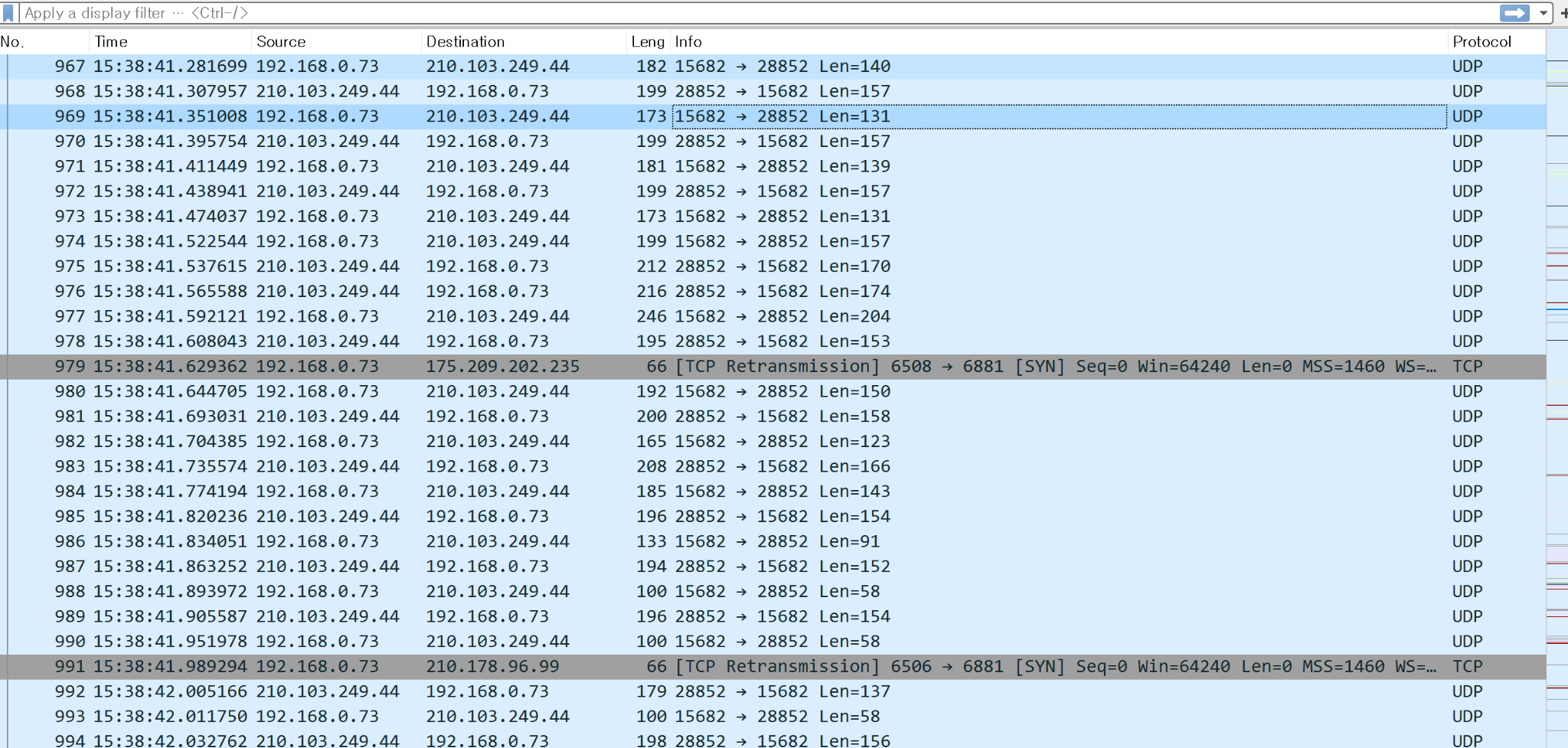
And what is in the packet from below.

****

video streaming

For my video streaming analysis, I use Youtube streaming.

First, because I have access to Youtube. There is a TCP protocol which looks like a Web application and after starting to see streaming video. it uses UDP protocol like below. As we learned, it usually uses UDP protocol.



And what is in the packet from below.

