

**Computer Networks Lab**

**Report**

**Name:** Donia Ghazy, Mohammed abuelwafa

**ID:** 900172124, 900172603

The goal of this project is to capture and analyze RTP and RTCP packets during a real-time conference session over a wireless network.

**Difference between RTP and RTCP:**

**RTP:**

* Real Time Protocol (RTP) is a real-time end-to-end transport protocol. It is mostly used upon UDP, which is also considered as a transport protocol. RTP is very closely coupled to the application it carries. So, RTP is best protocol that applications can use to implement a new single protocol.
* RTP doesn't guarantee timely delivery of packets, nor does it keep the packets in sequence.
* RTP gives the responsibility for recovering lost segments and resequencing of the packets for the application layer.
* **What RTP provides is:**

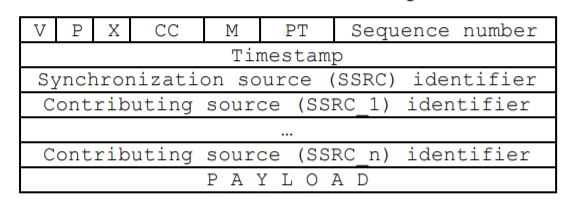
• Payload type identification

• Source identification

• Sequence numbering

• Timestamping

* **RTP packet format:**



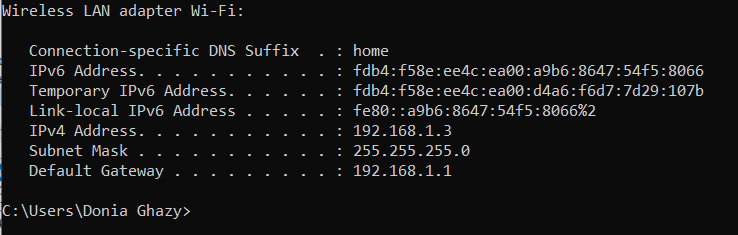
* **The version number (V)** is currently 2.
* **The padding bit (P)** indicates if there is padding octets inserted at the end of this packet. Padding may be required by some applications with fixed length packet sizes.
* **The extension (X)** bit indicates if there is an experimental extension after the fixed header.
* **The count field (CC)** tells the number of contributing source identifiers (CSRC) following the fixed header.
* **The marker bit (M)** may be used as general marker, f.g. indicating the beginning of a speech burst.
* **The payload type (PT)** field identifies the payload format, which are discussed in the chapter 2.2.
* **The sequence number** is an incrementing counter which is started by a source from a random number.
* **The timestamp** corresponds to the generation instant of the first octet in the payload.
* **The synchronization source identifier (SSRC)** is a randomly generated value that uniquely identifies the source within a session.
* **One or more contributing source identifiers** which are supplied by the mixer and the payload.

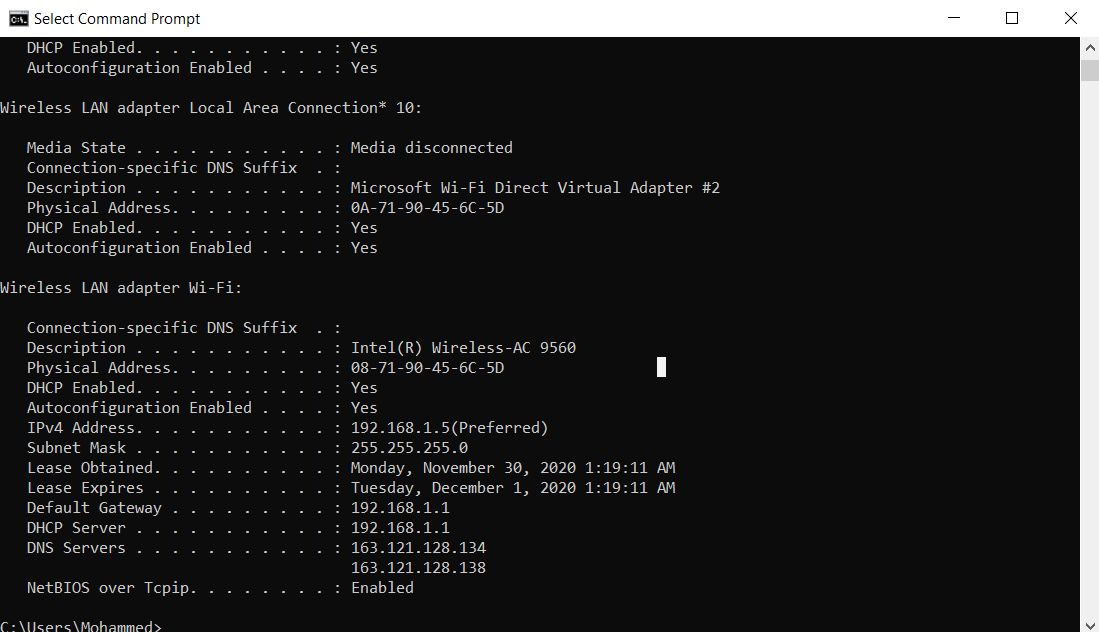
**RTCP:**

* Real Time Control Protocol (RTCP) provides the RTP session participants feedback on the quality of the data distribution.
* The underlying protocol must provide multiplexing of the data and control packets, with UDP this is usually implemented using separate port numbers.
* The format of the RTCP packets is fairly similar to RTP packets, e.g. the type indication is at the same location.
* It is responsible for QoS monitoring and congestion control, identification, and session size estimation and scaling.
* The RTCP packets carry also a transport-level identifier (called a canonical name) for a RTP source, which is used to keep track of each participant.
* **Its drawbacks are**
* Congestion due to floods of RTCP packets in highly dynamic groups.
* Large delays between receipt of RTCP packets from a single user
* Large size of the group membership tables
* **RTCP packet format:** Each RTCP packet starts with a header similar to that of the RTP data packets. The payload type field identifies the type of the packet. There are five RTCP payload types defined as follows:
* Sender Report (SR) takes a value of 200
* Receiver Report (RR) takes a value of 201
* Source Description (SDES) takes a value of 202
* Goodbye (BYE) takes a value of 203
* Application-defined packet (APP) takes a value of 204

1. **Part I: Real Network Implementation:**

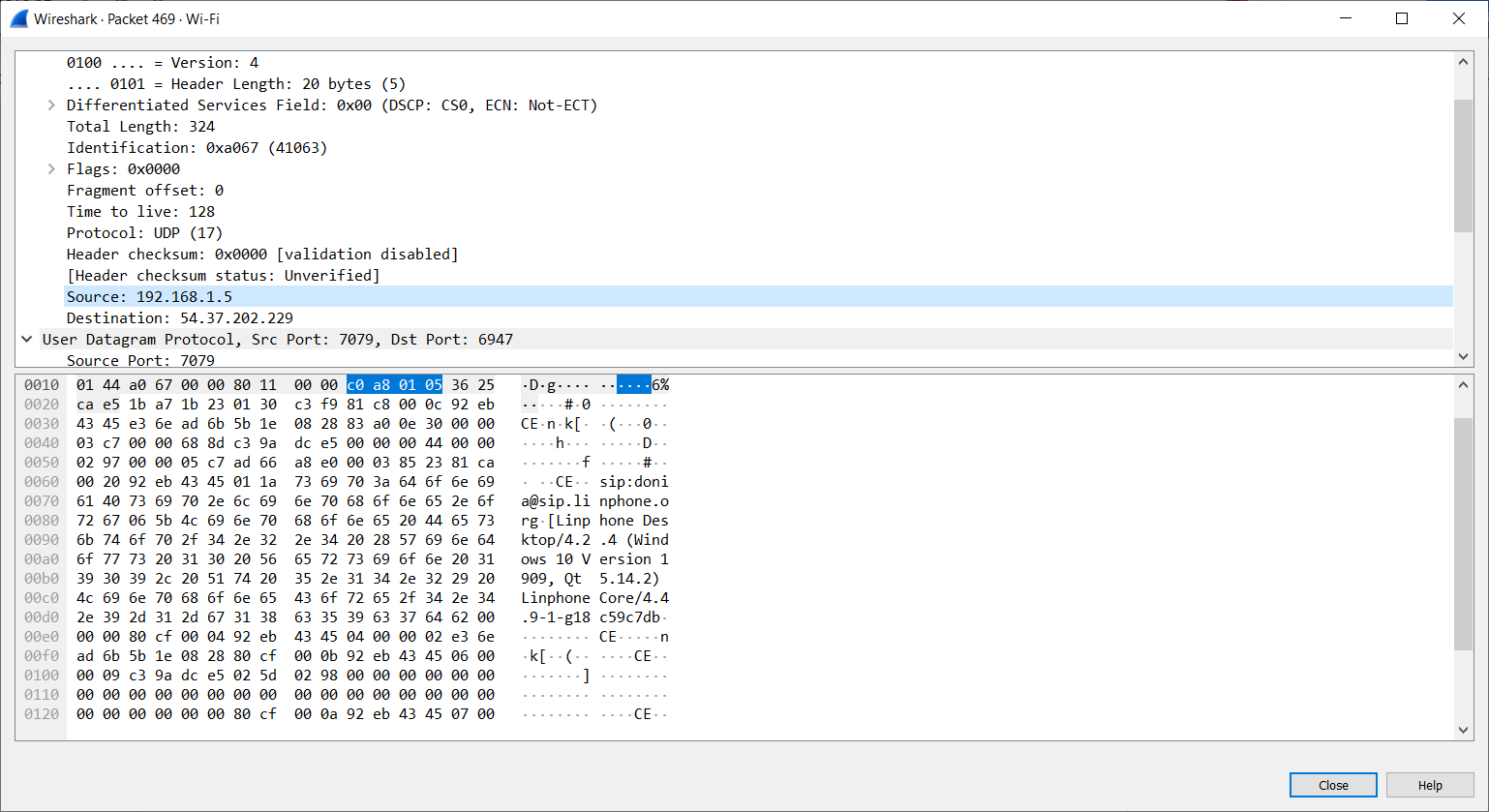
* Machine’s IPs:

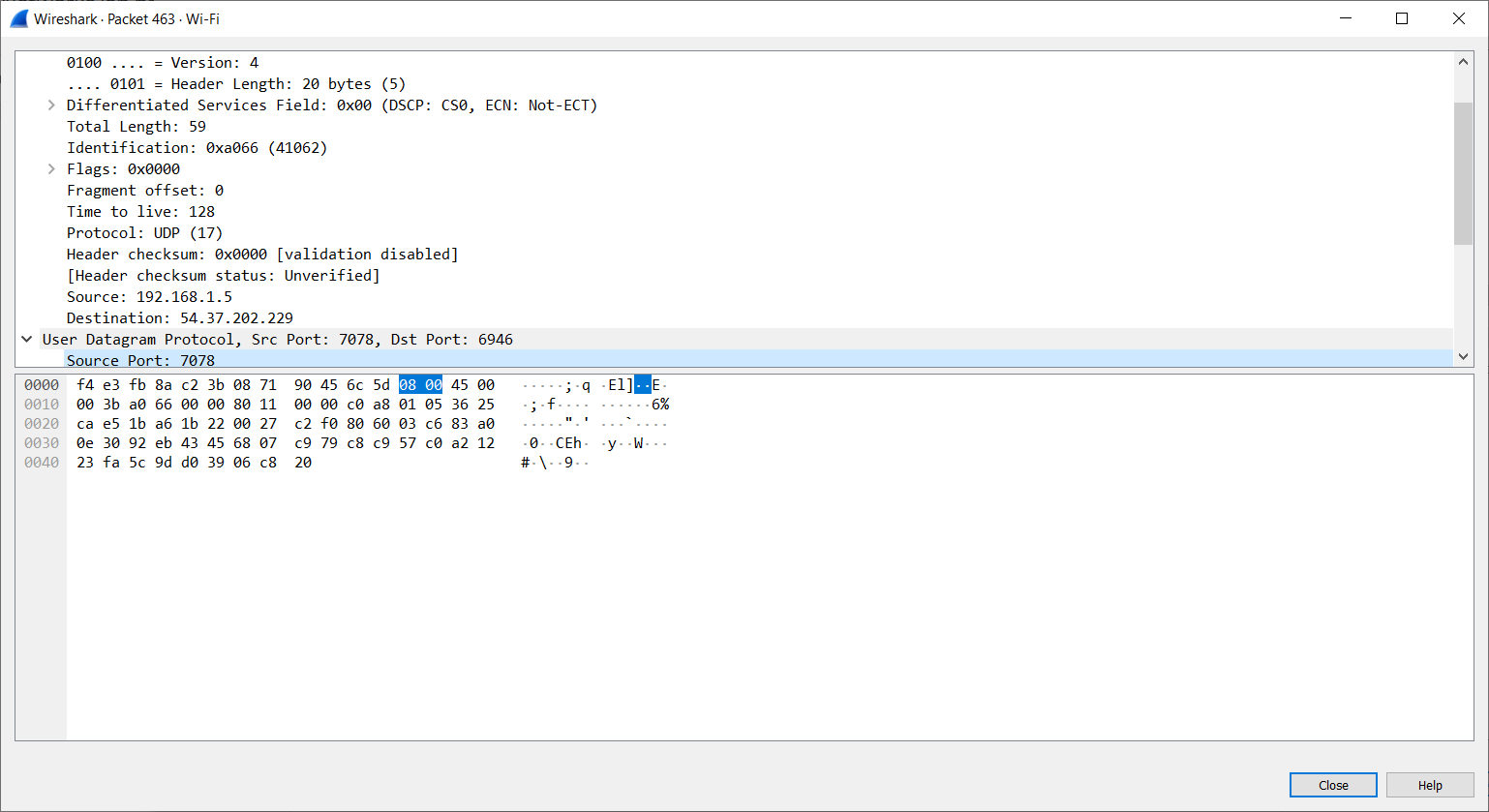


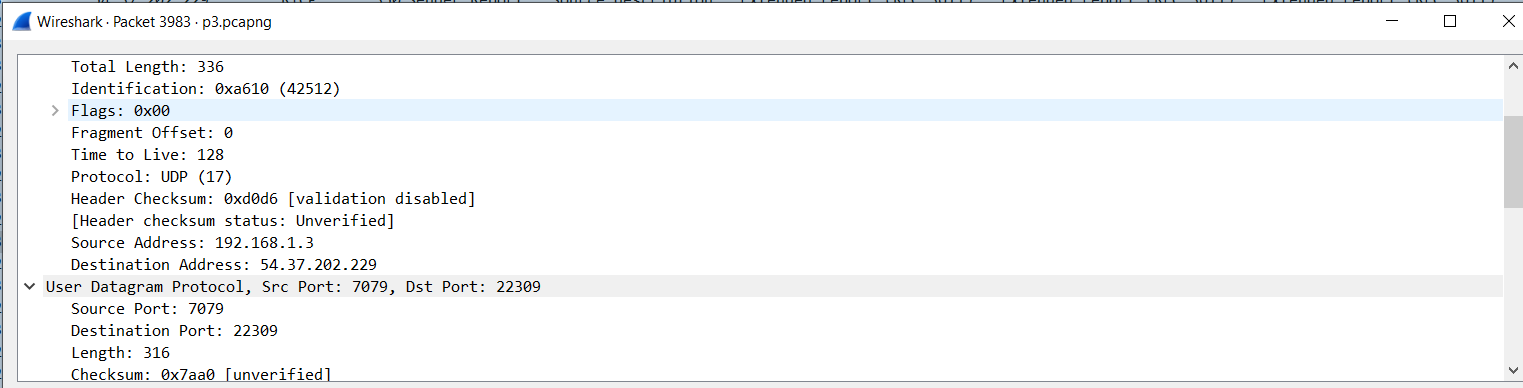


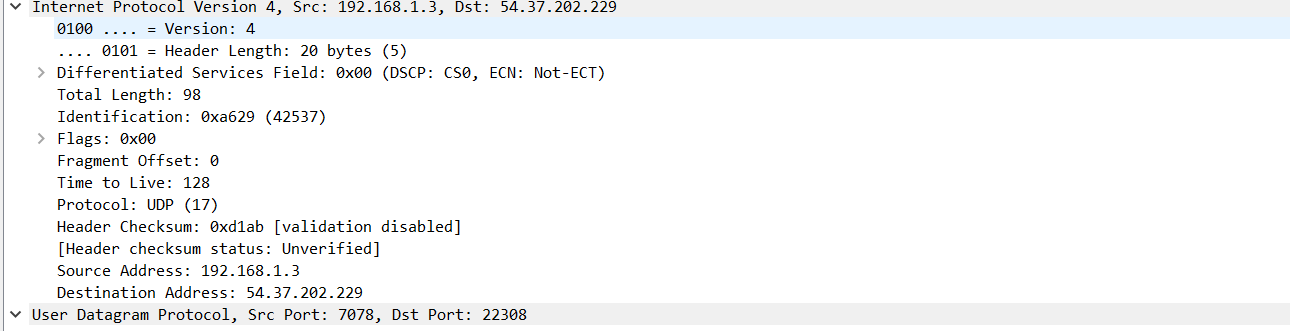
* Requirement 1:

Some RTP and RTCP headers as follows:









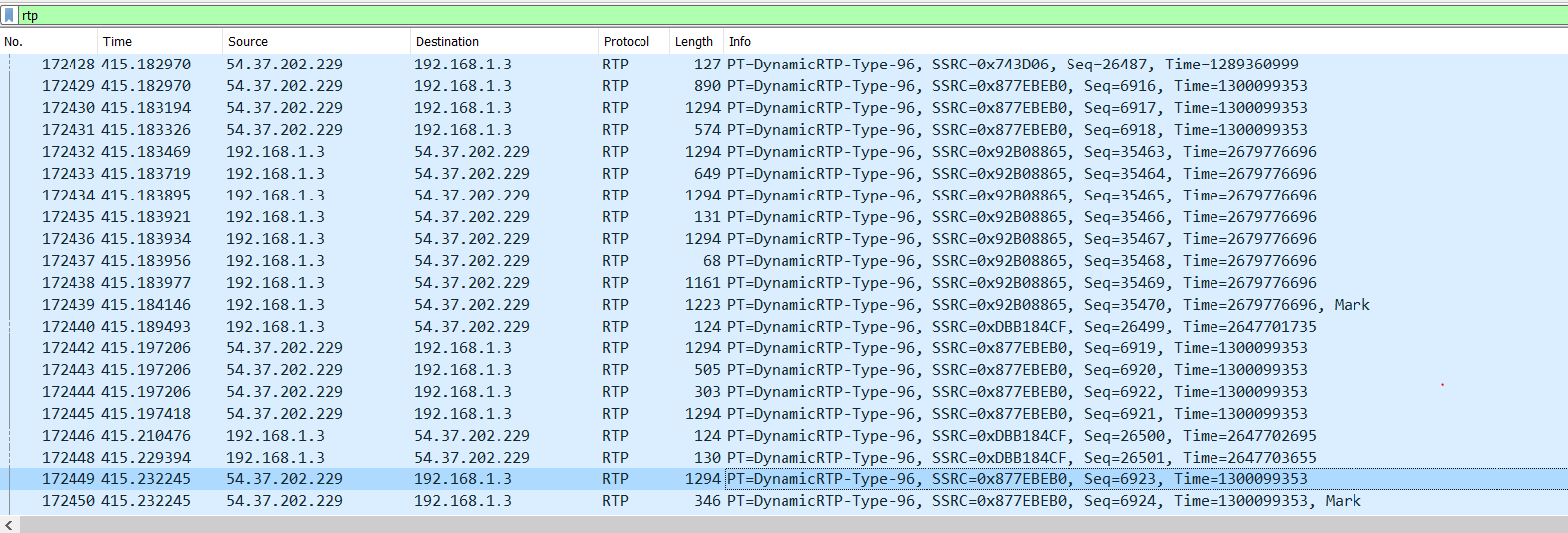
There are some techniques and filters that we used to separate these packets. They are explained as follows:

1. From Wireshark itself, we can choose Analyze, Enabled Protocols, enable rtp-udp: this will show the RTP and RTCP protocols separately from each other.
2. From the header itself, we can notice that RTCP destination port is always greater than RTP destination port by value of one as RTCP is always an odd number, while RTP is always an even number.

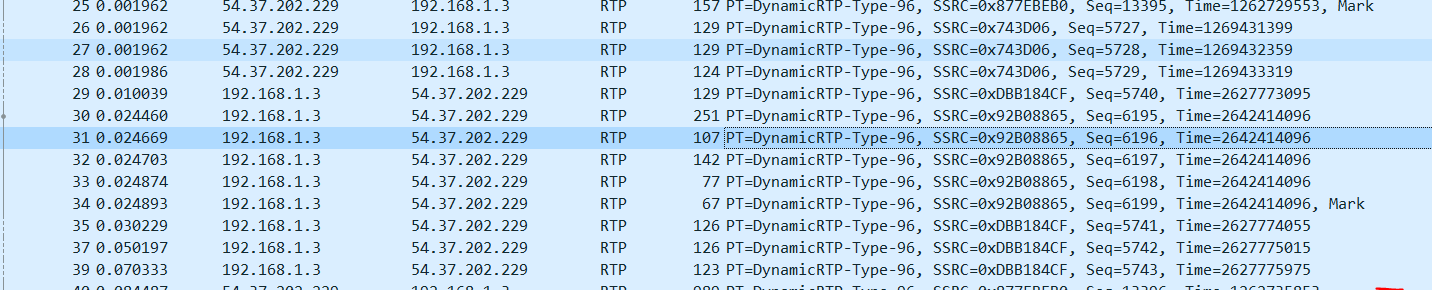
* Requirement 2:

Some filter results for the audio and video payloads as follows:

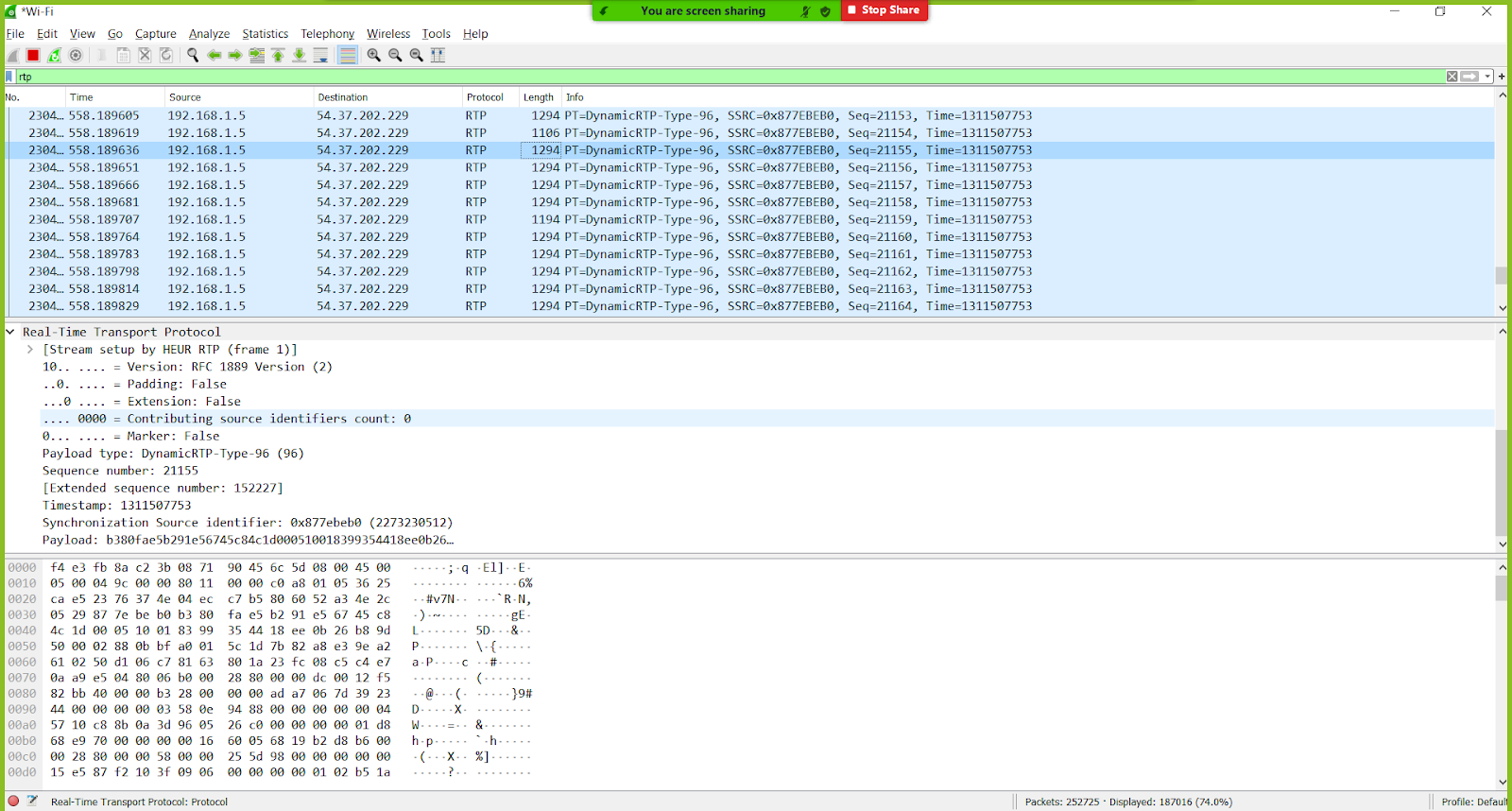
**For both video and audio together:**



**For audio alone:**



**For video alone:**

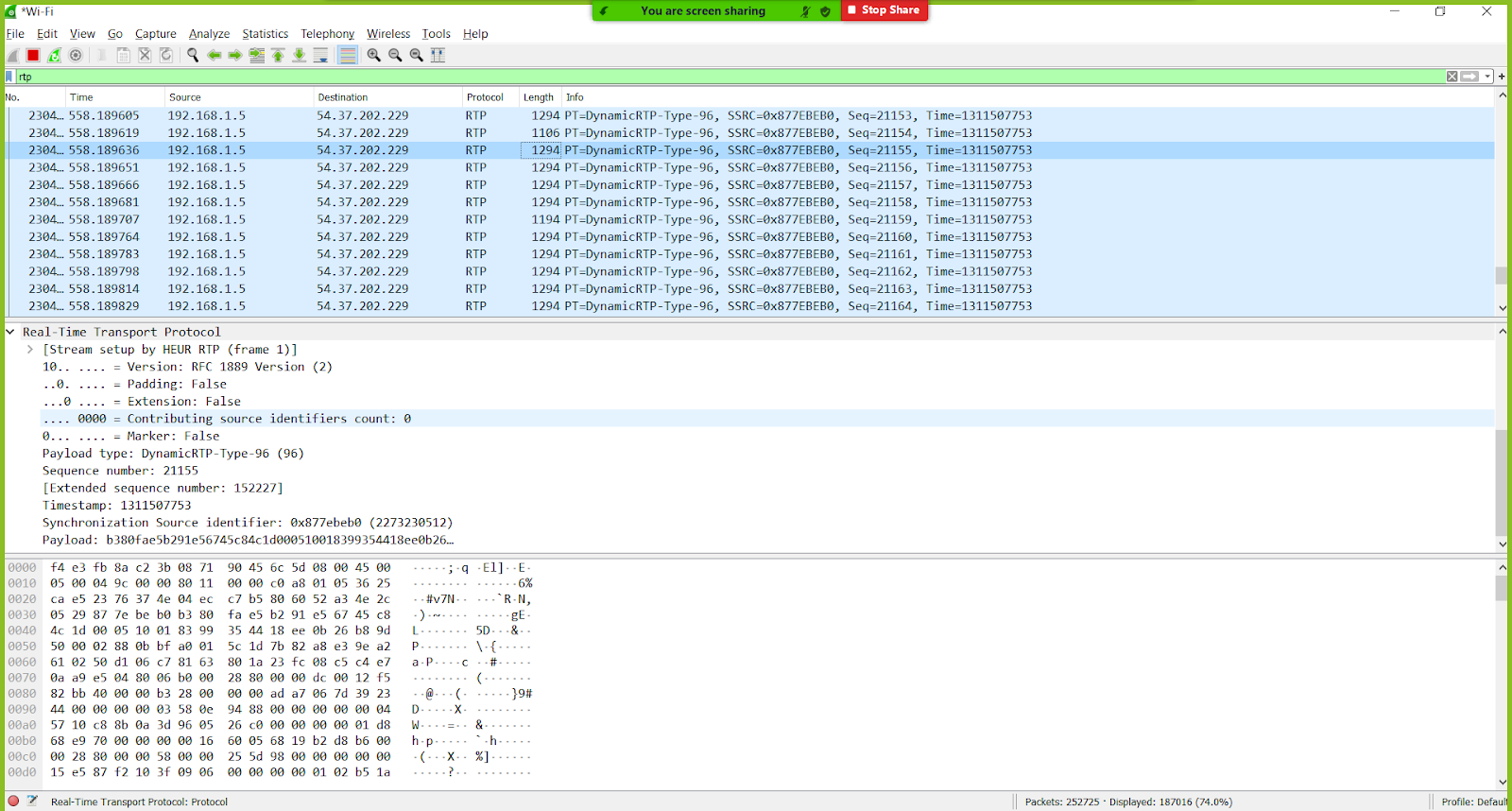


There are some techniques we used to extract the payload types. We used three different methods and explained farther as follows:

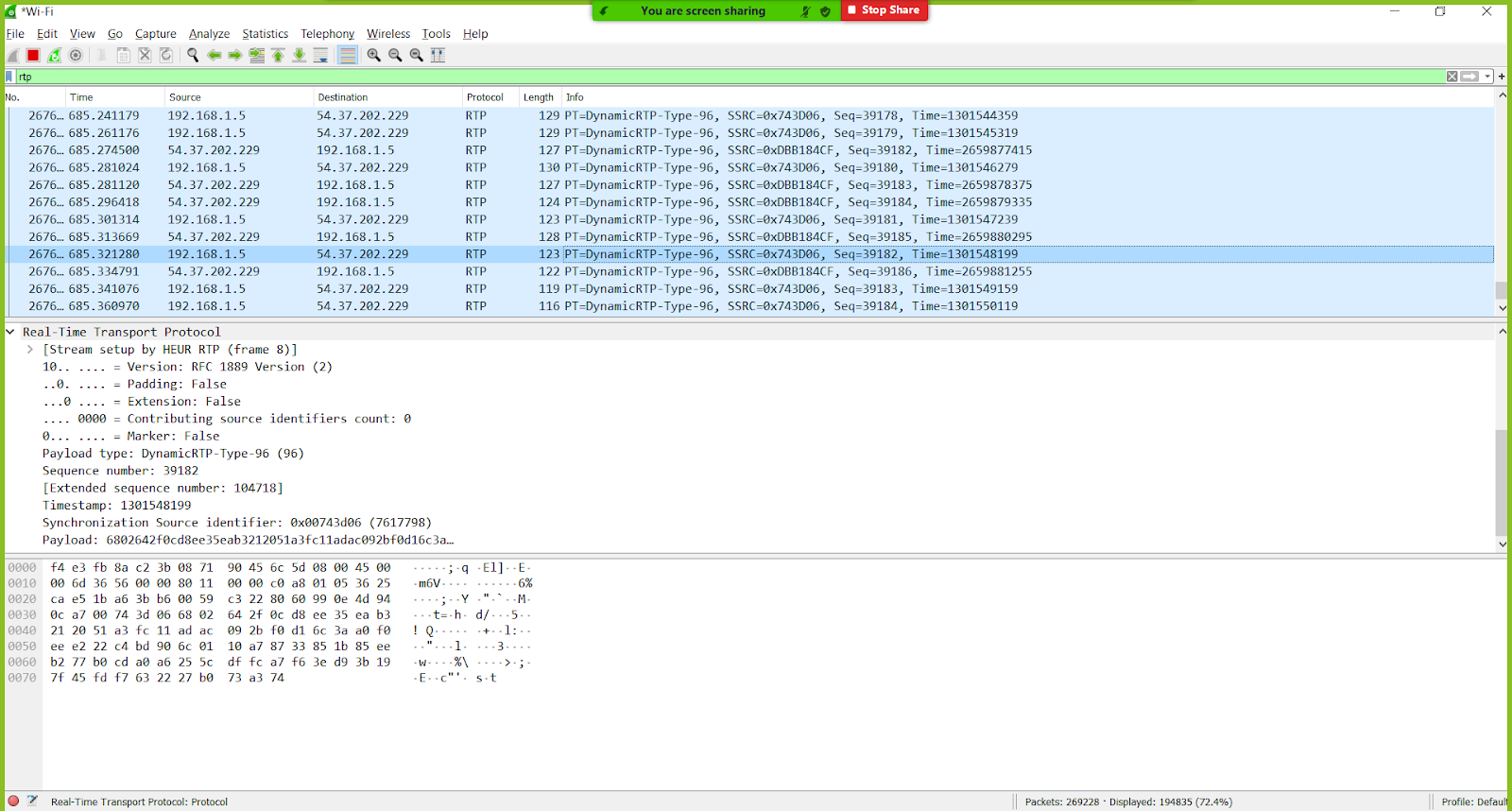
1. **Method no. 1:**

We managed to differentiate between the audio and video packets by observing the length of the packets, the video packets have more data than the audio packets as video packets have a length of 1294 bytes, while audio packets have a length of 116-130 bytes. This could be verified as follows:

RTP video payload:



RTP audio payload:

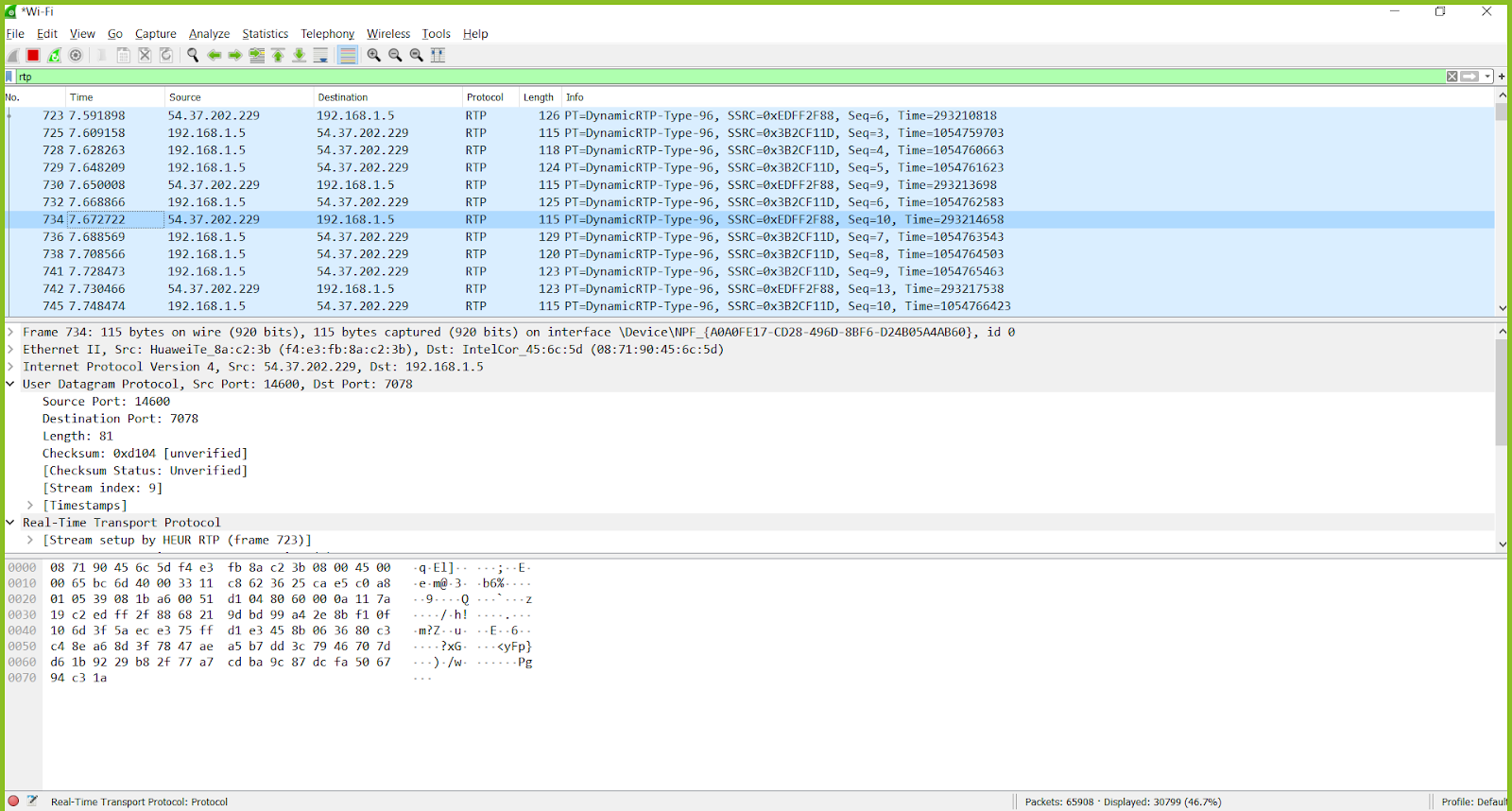


1. **Method no. 2:**

We managed to differentiate between them analytically by calculating the sampling rate between two consecutive packets. For example, by taking sequence 10 and 9, we can find that:

T = = = 42.266 KHz

From the result, we can conclude that these packets are audio packets due to the sampling rate. Similarly, by calculating the sampling rate of two video consecutive packets. It was around 90 KHz.



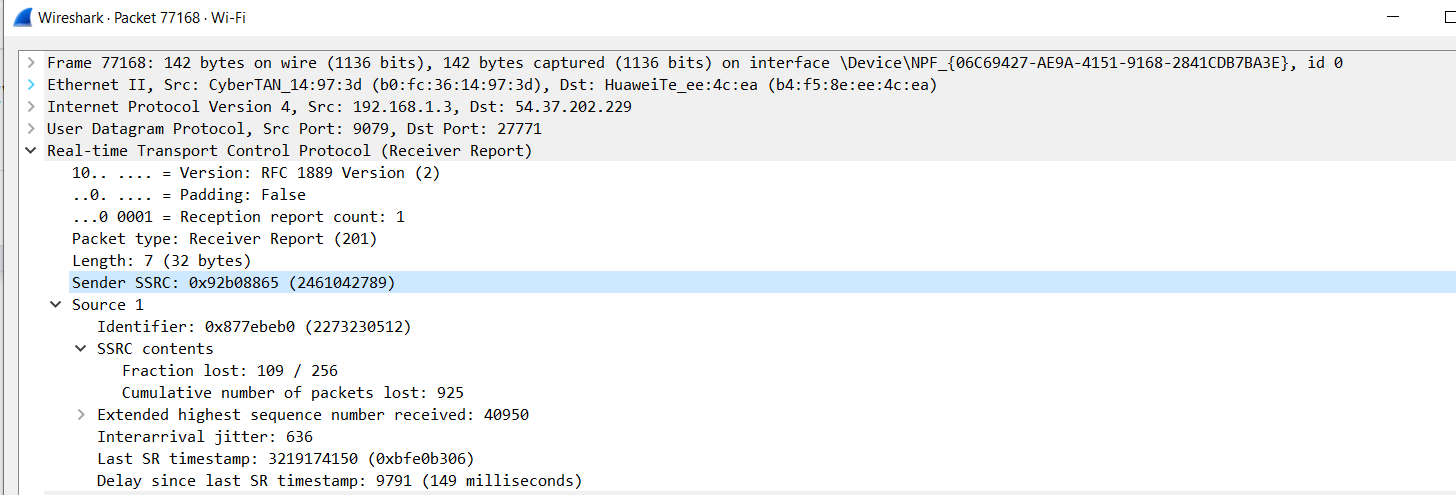
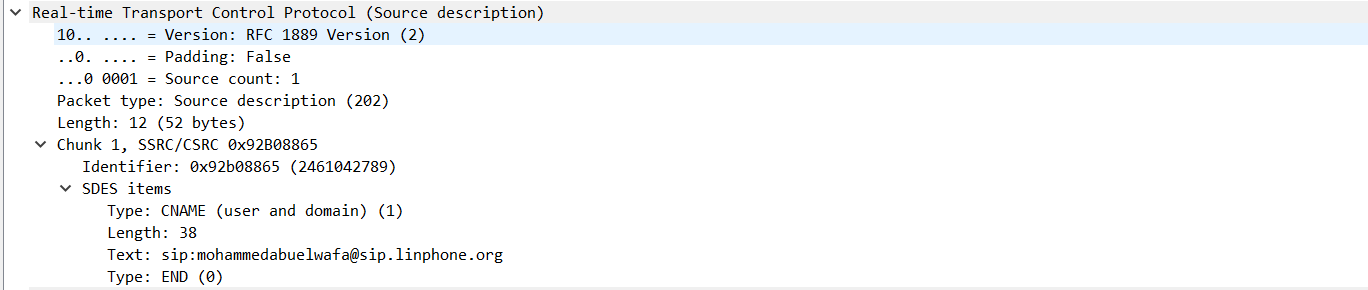
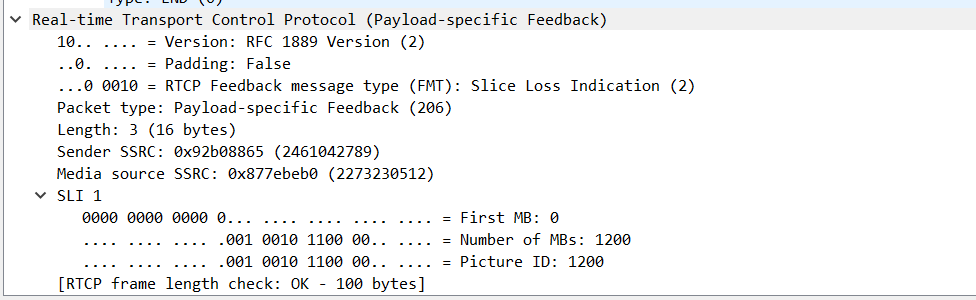
1. **Method no. 3:**

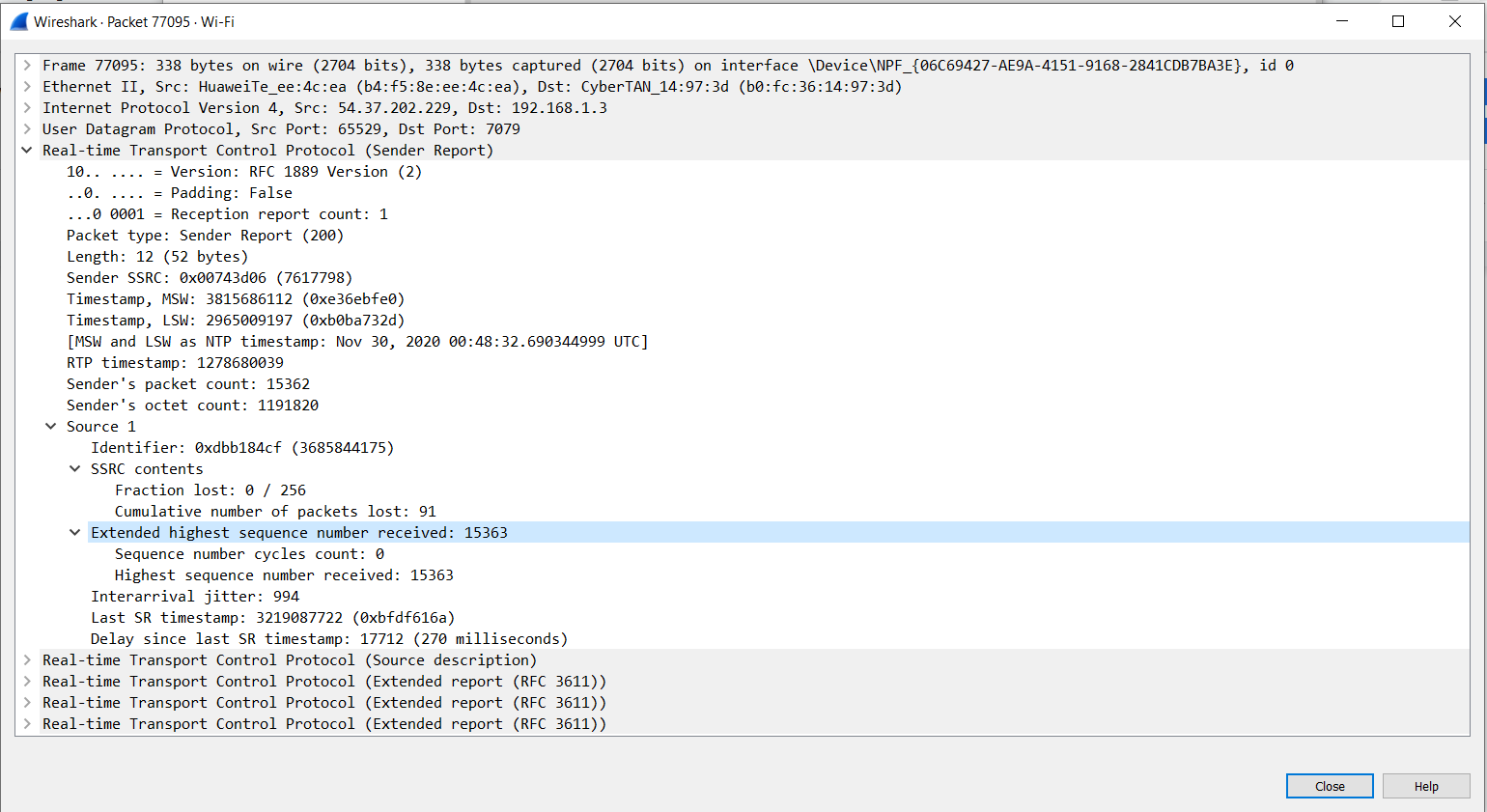
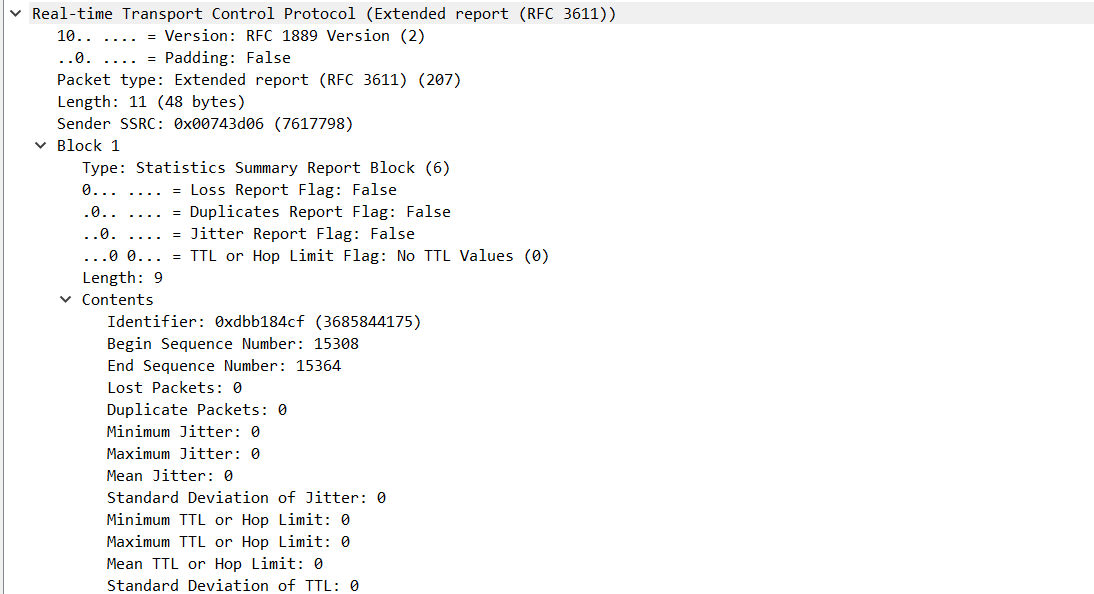
We can differentiate between them by monitoring the sequence numbers. We can easily find that the sequence number of the audio payload has a different order than the video payload. The range of video sequence are around 700-800ish, while the range of audio sequence are around 33000ish.



* Requirement three:

We managed to find three reports that were mentioned explicitly to get such as receiver, sender, and source description reports. Additionally, we found other additional reports such as payload-specific feedback and extended reports. The following screenshots display the headers of each.





|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Source port no. | No. of packets | Packet type | SSRC | No. of packet loss |
| 65529 | 15362 | Sender report 200 | 0x00743d06 | 91 |
| 9079 | 40949 | Receiver report 201 | 0x92b08865 | 925 |

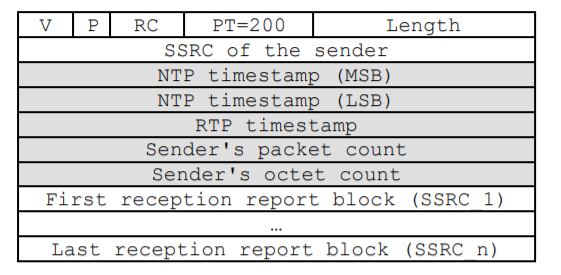
Incoming and outgoing packets for participant 1:

The usage of each report can be explained as follows:

The sender reports (SR) and receiver reports (RR) exchange information on packet losses, delay and delay jitter. This information may be used to implement a TCP like flow control mechanism upon UDP at the application level using adaptive encodings.

**Sender report**: in the conference call, it shows the information for the outgoing packets. It contains the number of packets sent but it does not guarantee that all of these packets will be transmitted as some packets might be lost. In addition, it contains the packet type which is sender type and has the value of 200. In addition, it has the sender SSRC.

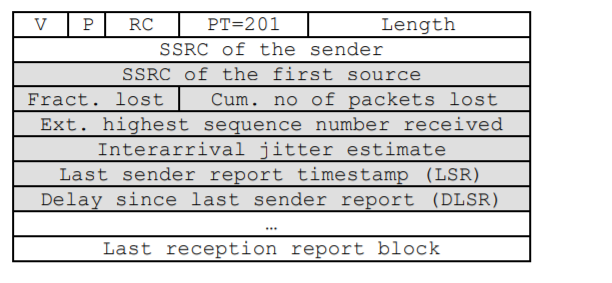
**Format of sender report is as follows:**



* **The version number (V).**
* **Padding field (P)** are the same as in RTP packet.
* **The reception report count (RC)** indicates the number of receiver reports attached to this packet. The maximum number of receiver reports is 32.
* **The payload type (PT)** for sender report is 200.
* **SSRC of the sender.**
* **The high part** of the 64-bit NTP (Network Time Protocol) timestamp.
* **The low part** of the 64-bit NTP (Network Time Protocol) timestamp.
* **The RTP timestamp** indicates the relative sending time of this packet.

**Receiver report**: in the conference call, it shows the information for the ingoing packets. It contains the number of packets sent but it does not guarantee that all of these packets will be transmitted as some packets might be lost. In addition, it contains the packet type which is sender type and has the value of 201. In addition, it has the receiver SSRC.

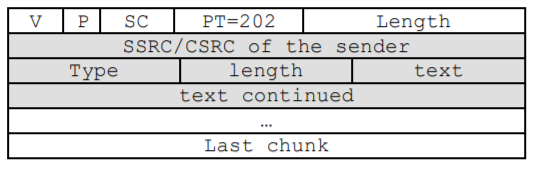
**Format of receiver report is as follows:**



* **SSRC** of the source.
* **The fraction lost** field indicates the number of packets lost divided by the number of packets expected since last receiver report.

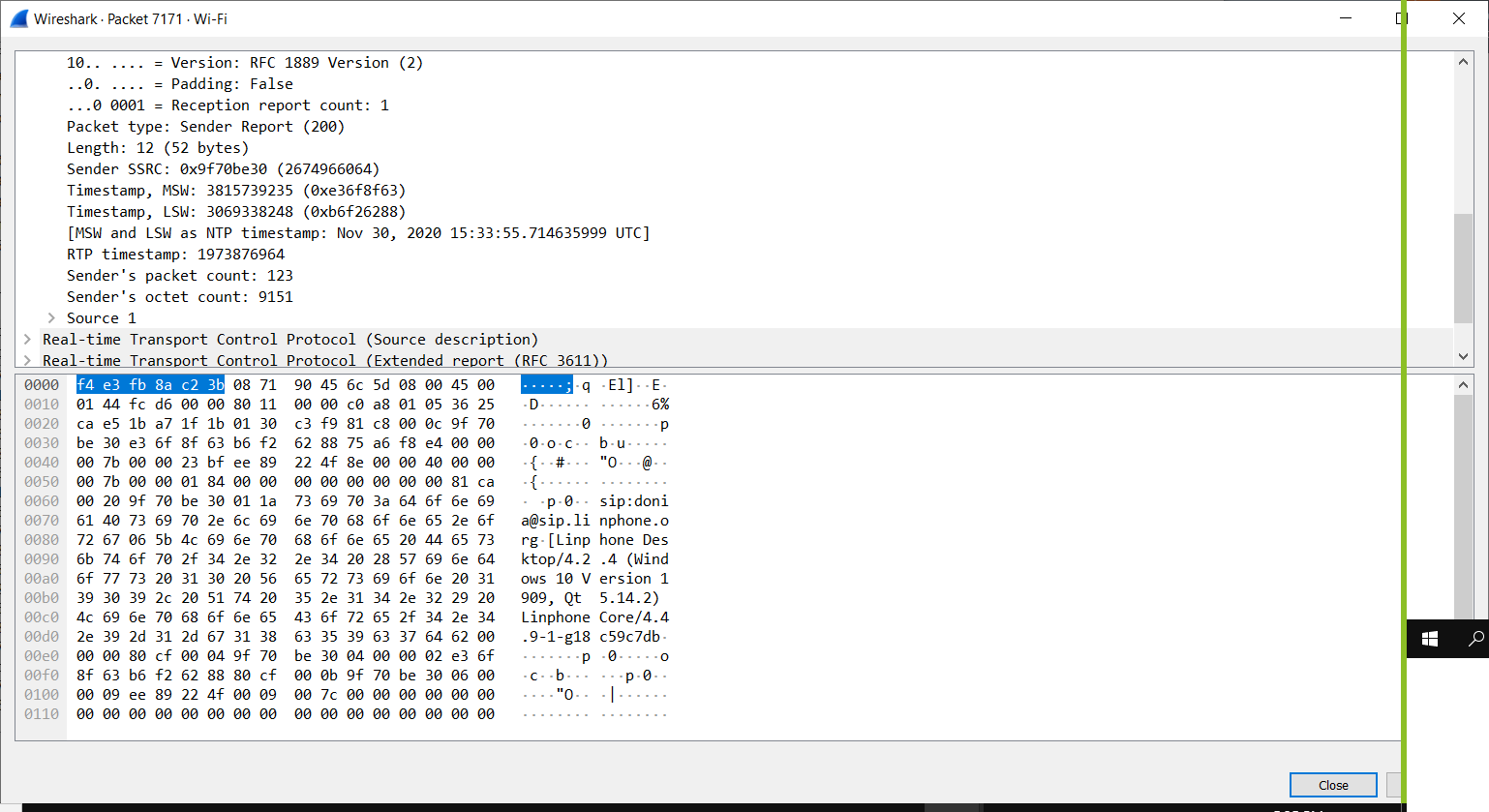
**Source description**: it contains a description of the packet type which is source description and has the value of 202. In addition, it holds SDEE items such as its name and type.

**Format of source description is as follows**:

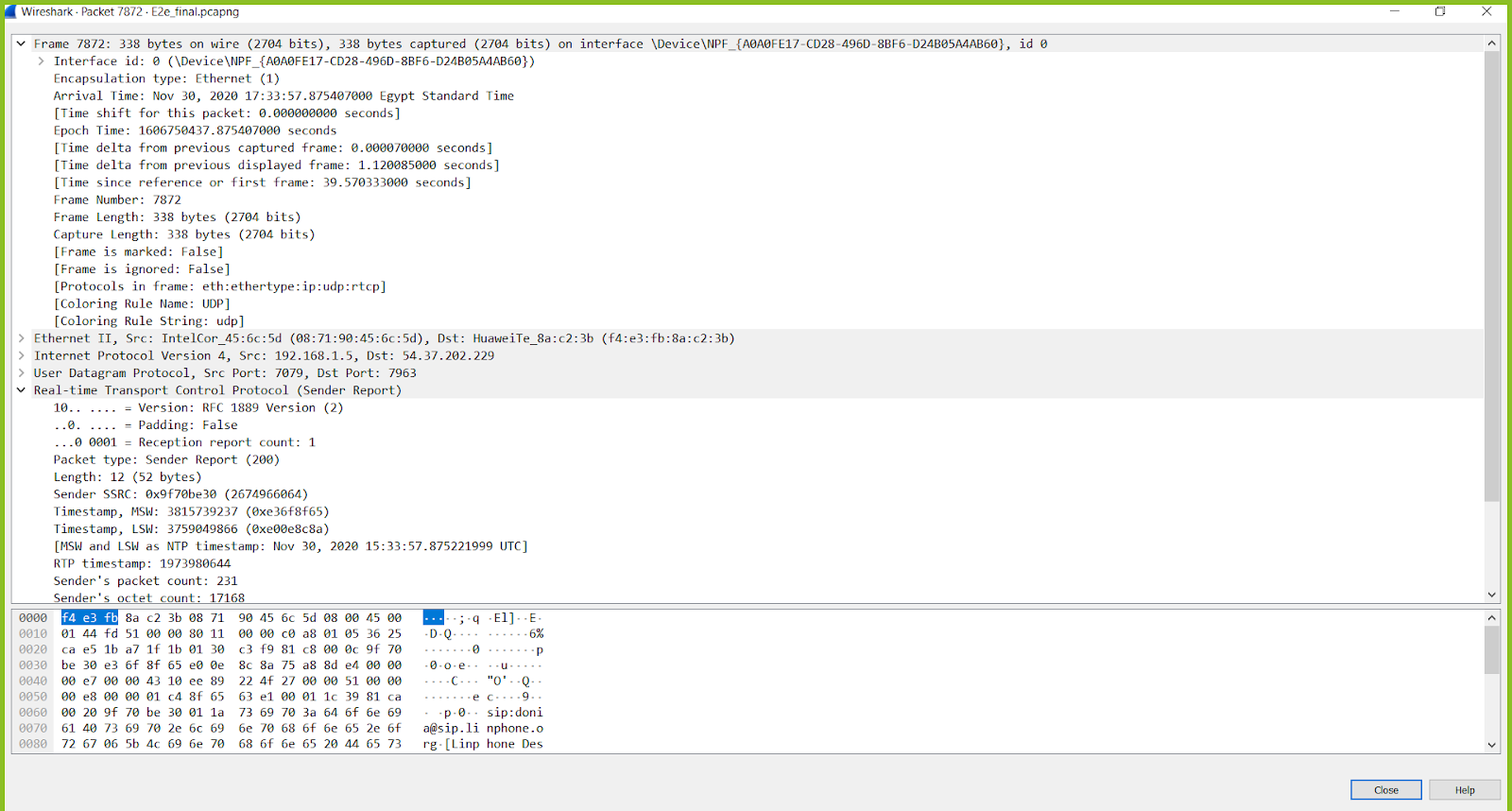


* It is a three-level structure composed of a header and zero or more chunks
* It describes the source identified in that particular chunk.
* Each SDES item starts with an 8-bit type field followed by an 8-bit octet count, which identifies the length of the following text field.
* Requirement 4:

Taking two RTCP packets x, x+1 as examples for calculating the E2E delay.



Packet x



Packet x+1

For packet X:

**NTP**: Nov 30, 2020 15:33:55.714635999 UTC

**RTP timestamp**: 1973876964

**RTP data audio sampling rate**: 48 KHz (from line phone page)

For packet X+1:

**NTP timestamp**: Nov 30, 2020 15:33:57.875221999 UTC

**RTP** **timestamp**: 1973980644

* **Incremental difference in Number of units**:
* Packetx Timestamp –Packetx+1 Timestamp= 1973980644 -1973876964= 103680 unit
* **Time difference**: = = 2.16 s

This time difference can also be verified using the difference in NTP timestamp as follows:

57.875221999 - 55.714635999 = 2.16 s

* **Wall clock time**: NTP time : Nov 30, 2020 17:33:57.875407000 Egypt Standard Time

In order to convert RTP time to NTP time for a packet:

Packetx (NTP) = packet0 (NTP) + (Packetx (RTP) - packet0 (RTP))/ 48000)

In order to calculate the E2E delay for the following

* **Arrival Time**: Nov 30, 2020 17:33:58.165097000 Egypt Standard Time
* **Timestamp**: 1973995044

Using the first RTCP packet as reference (Packet0)

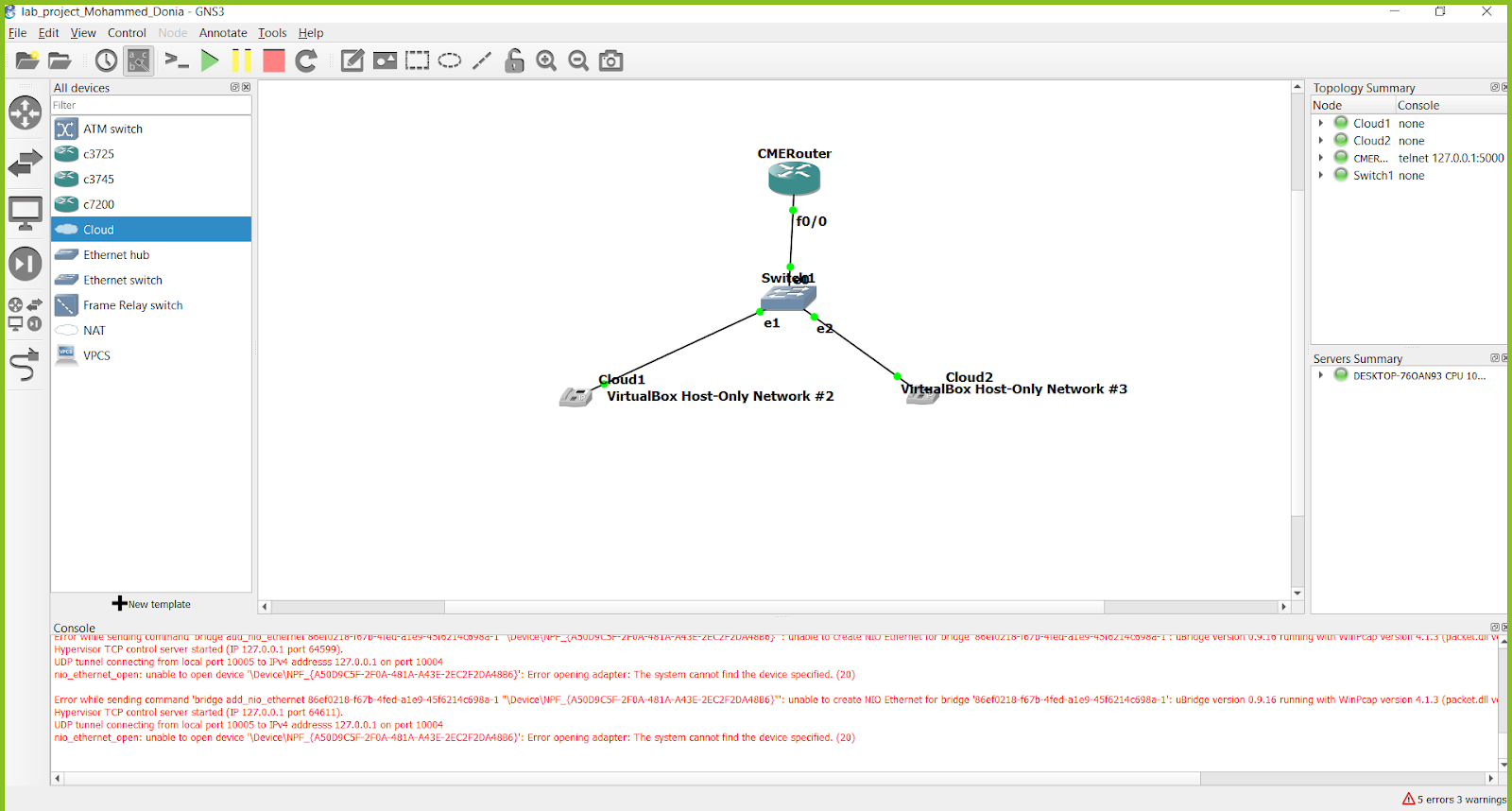
* **NTP for this RTP** = = 59.08
* **E2E delay** = arrival time - NTP (RTP timestamp) =

58.165097000 - 59.08= -0.009 s

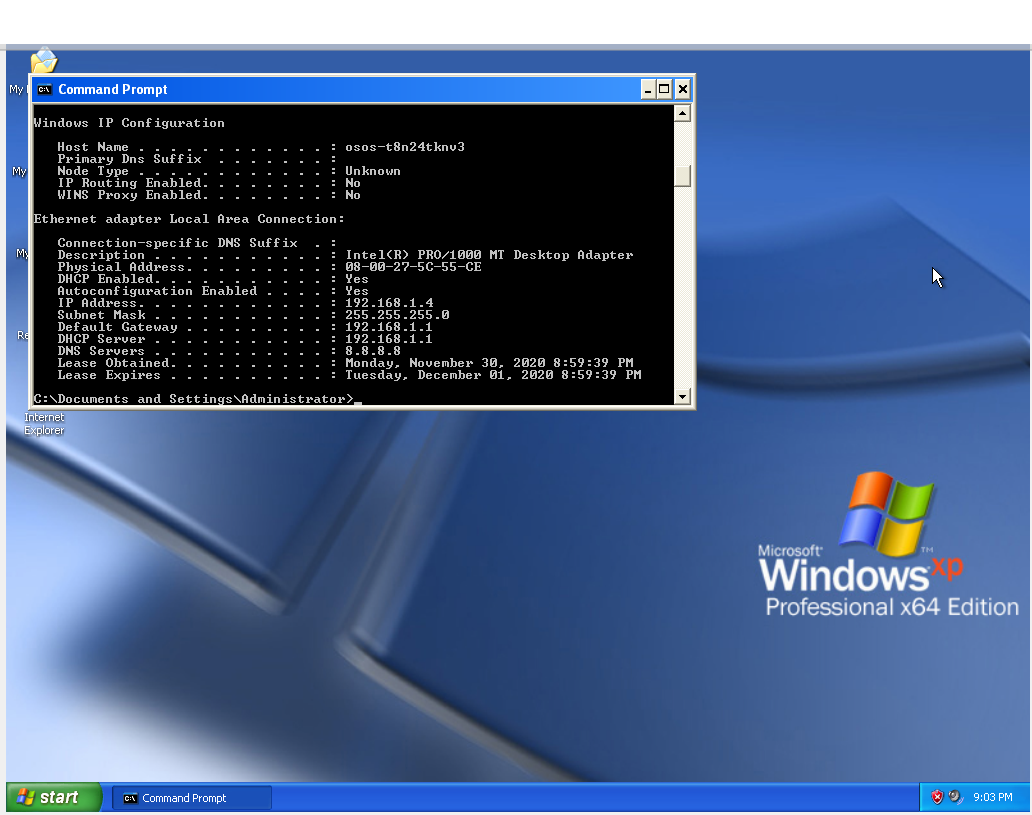
Taking the absolute value of it so basically the delay value is 0.009 s.

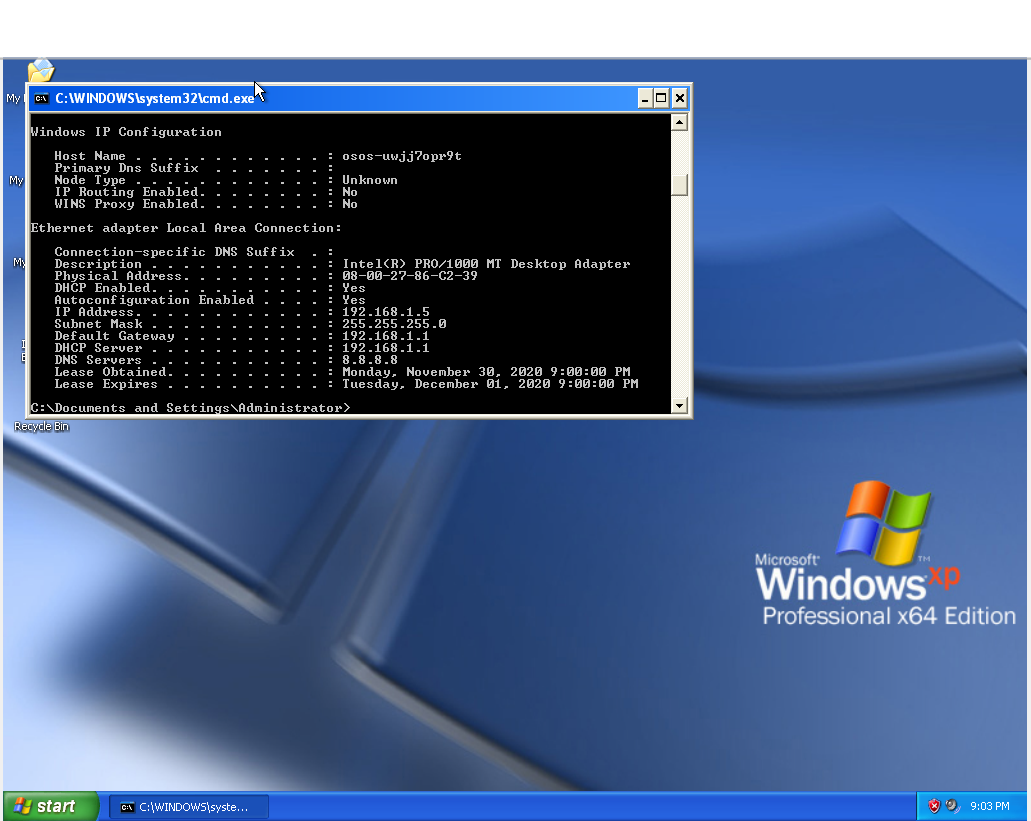
1. **Part II: GNS3 Network Implementation**

We have designed the topology of the network in GNS3 and configured each component separately and defined the router as a DHCP server to dynamically assign each cloud (VM) an IP. The following screenshot shows the topology of the network.

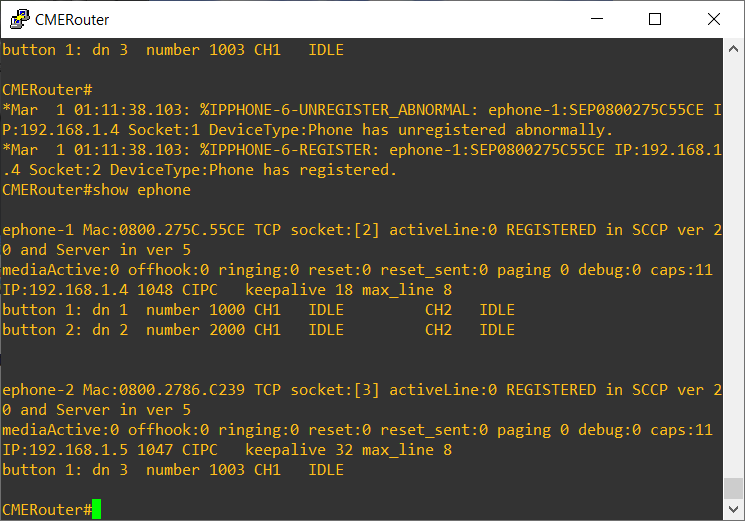


Dynamic configuration of the two VMs:

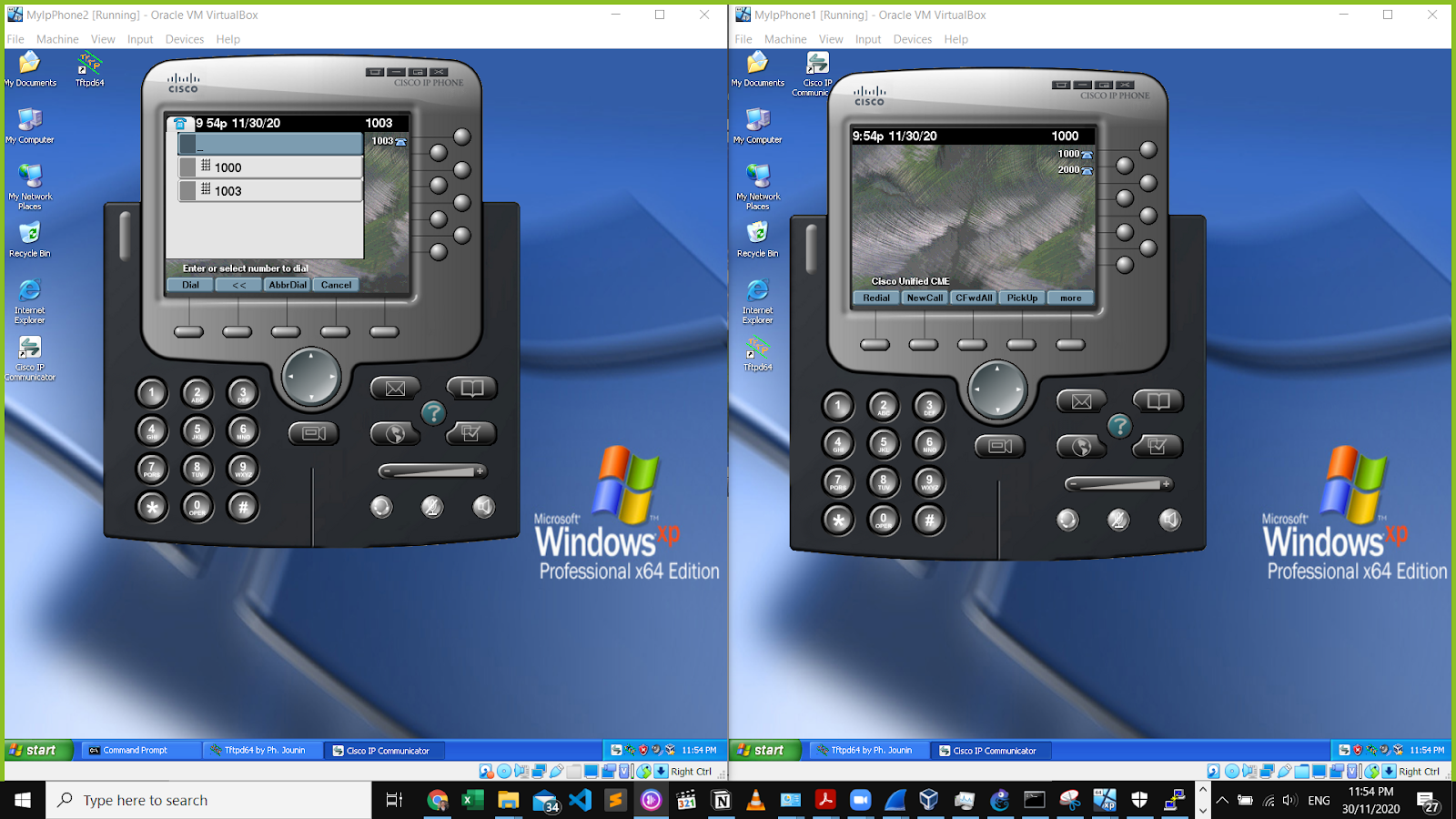




We have implemented all the steps successfully and were able to make a voice call from one VM to another and vice. These are the verification commands that we did in order to testify the correctness of the results.



After applying the previous commands, we started the two communicators and we found that each one of the VMs could dial the number of the other VM and we can hear our voices clearly. The following screenshot shows the final setup for our environment.



**References:**

[1] Ehsan MaiqaniEhsan Maiqani 9011010 silver badges1515 bronze badges, & AymericMAymericM 1. (1969, May 01). Linphone opus codec sampling rate. Retrieved November 30, 2020, from <https://stackoverflow.com/questions/60580526/linphone-opus-codec-sampling-rate>

[2] Koistinen, T. (n.d.). Protocol overview: RTP and RTCP. Nokia Telecommunications.  Retrieved November 30, 2020, from<https://www.netlab.tkk.fi/opetus/s38130/k99/presentations/4.pdf>

[3] Network Time Protocol (Version 3) Specification, Implementation and Analysis. (n.d.). Retrieved November 30, 2020, from <https://tools.ietf.org/html/rfc1305>

[4] Project 3:  Analysis of RTP and RTCP Packets. (n.d.). Retrieved November 30, 2020, from <https://www.ece.rutgers.edu/~marsic/books/CN/projects/wireshark/ws-project-3.html>

[5] RTCP. (n.d.). Retrieved November 30, 2020, from <https://wiki.wireshark.org/RTCP>

[6] RTP. (n.d.). Retrieved November 30, 2020, from <https://wiki.wireshark.org/RTP>

[7] RTP. (n.d.). Retrieved November 30, 2020, from <https://wiki.wireshark.org/RTP>

[8] What is RTCP (Real Time Control Transport Protocol)? (2020, November 09). Retrieved November 30, 2020, from <https://www.3cx.com/pbx/rtcp/>