HomeGroup Windows

Student Name: David Saldaña Castaño

# Date of delivery: 15/02/2018

521-David-PARP401C-Sniffers-CapturaWINdocx

# Objetives

In this exercise, We are going to learn how to create a Homegroup.

How to do basic network configurations.

How to add a system into the Homegroup.

# Loot and material needed

VMWare Workstation or another virtualization tools, in my case: VMWare.

Cutting tool.

Microsoft Word.

ISOS of Windows 7 and Windows 10.

PDF sent by the teacher as guide.

Content

[Date of delivery: 15/02/2018 1](#_Toc506464976)

[Objetives 1](#_Toc506464977)

[Loot and material needed 1](#_Toc506464978)

[SETUP 3](#_Toc506464979)

[We are going to sniff the network with the netsh command. 3](#_Toc506464980)

[Capturing the network 4](#_Toc506464981)

[Now, we are going to see the results in the .etl file 4](#_Toc506464982)

[In the SYSADMIT folder we can see two files: .cab and .etl 5](#_Toc506464983)

[Inside of the .cab file, we can see a .html report that we can open by our browser. 5](#_Toc506464984)

[This is the report of the capture. 6](#_Toc506464985)

[To open the .etl file we need the programm: Microsoft message analyzer, so let’s download it! 6](#_Toc506464986)

[Once it is installed we can open the file .cab and see the capture. 7](#_Toc506464987)

[Adding new parameters to the command. 8](#_Toc506464988)

[Stopping the new capture. 8](#_Toc506464989)

[In the same folder that before, we save the generated files by the capture. 9](#_Toc506464990)

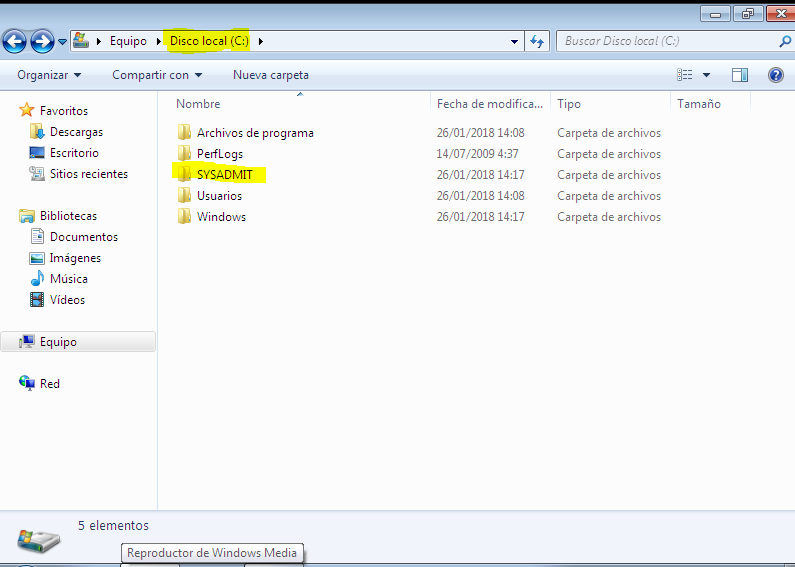
[We put the IP address that we have used in the capture as a fiter and we see the results. 9](#_Toc506464991)

[FINAL CONSIDERATION AND METACOGNITION 9](#_Toc506464992)

# SETUP

# We are going to sniff the network with the netsh command.

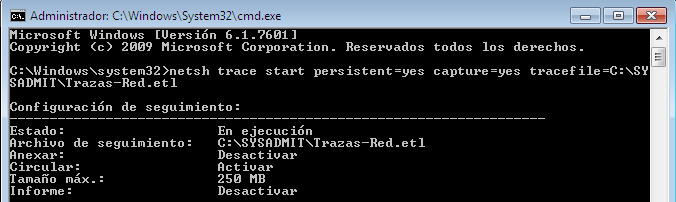
First of all we are going to create the folder where the network sniff is going to be captured.



# Capturing the network

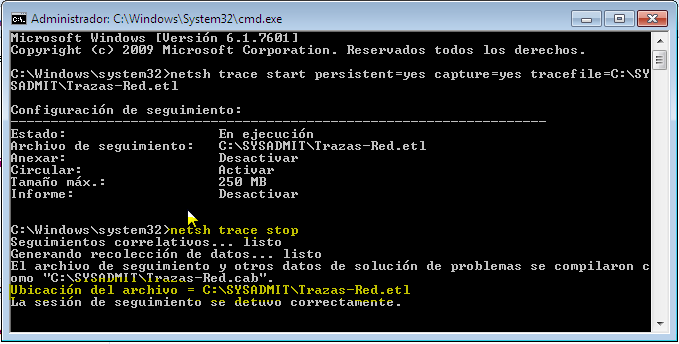
With the command **“netsh trace start persistent=yes capture=yes tracefile=C:\SYSADMIT\Trazas-Red.etl”** we are sniffing our network and the capture file is going to be saved in the folder that we have created before.

Persistent=yes: It means that if we restart the computer, it continues sniffing.

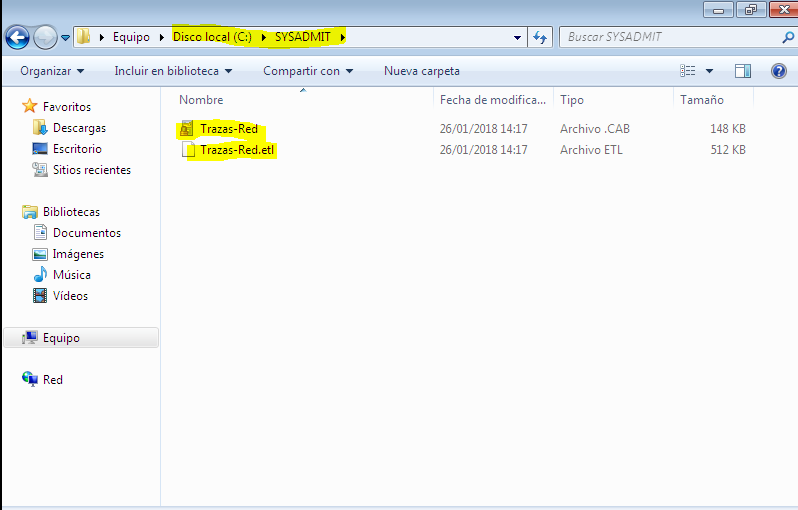


# Now, we are going to see the results in the .etl file

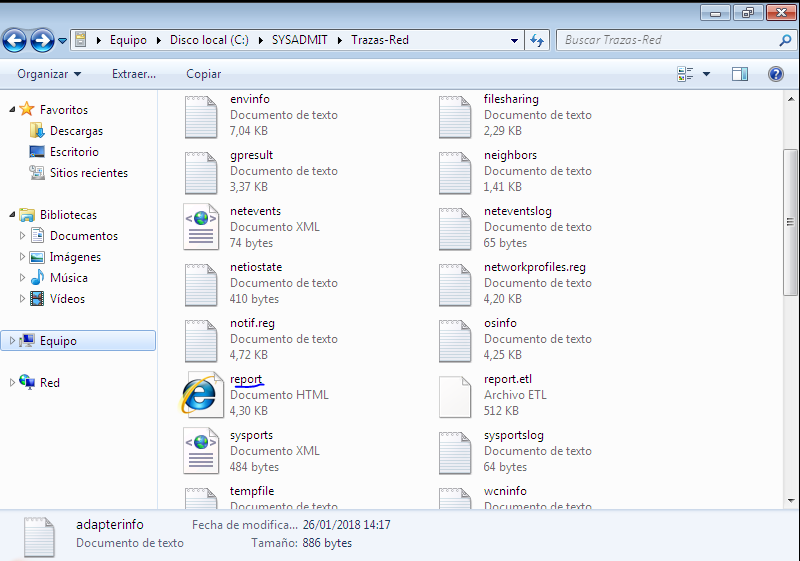
With the command **“netsh trace stop”** we stop the capture and if there is no issues, the capture is going to be saved where we have especified before.



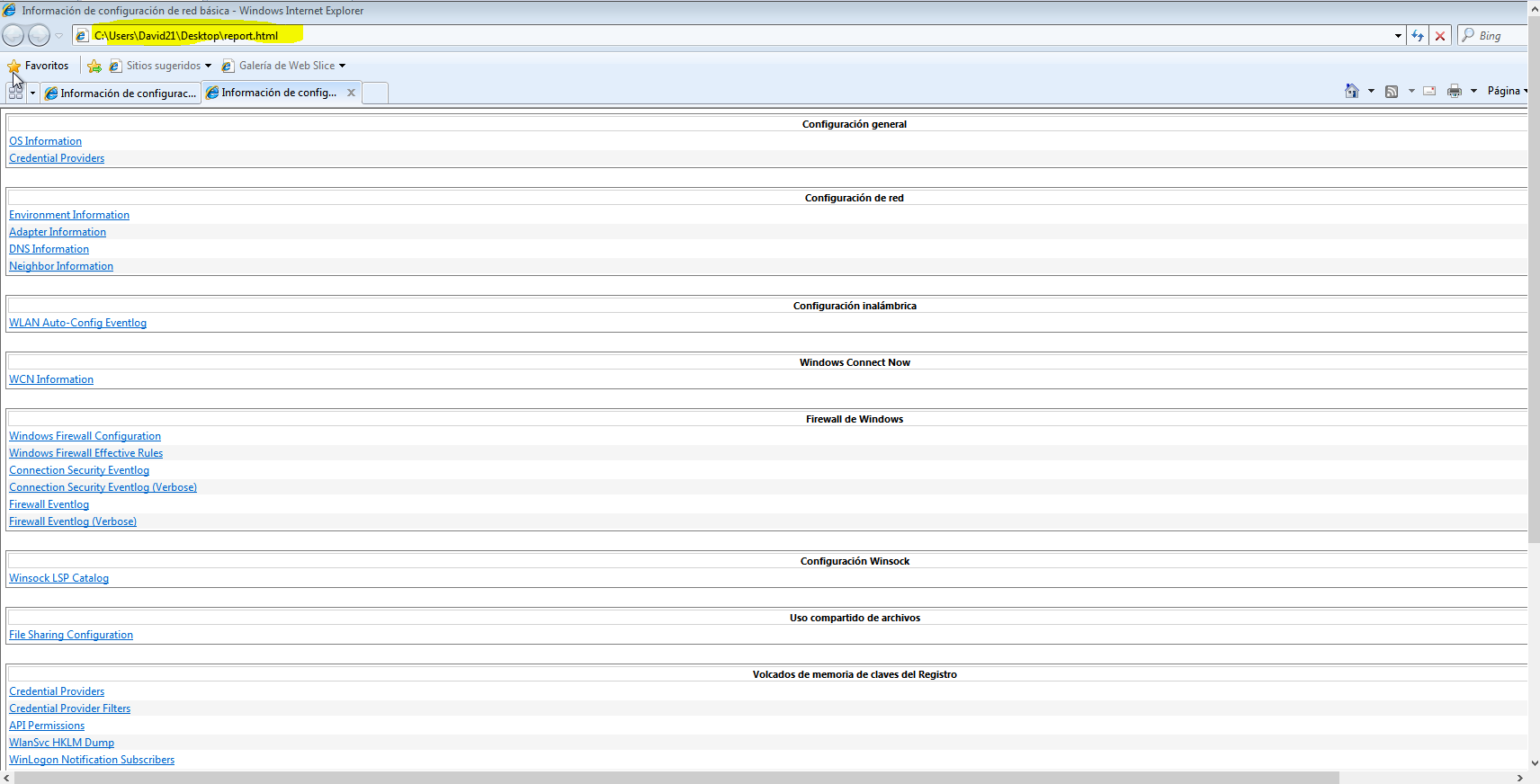
# In the SYSADMIT folder we can see two files: .cab and .etl



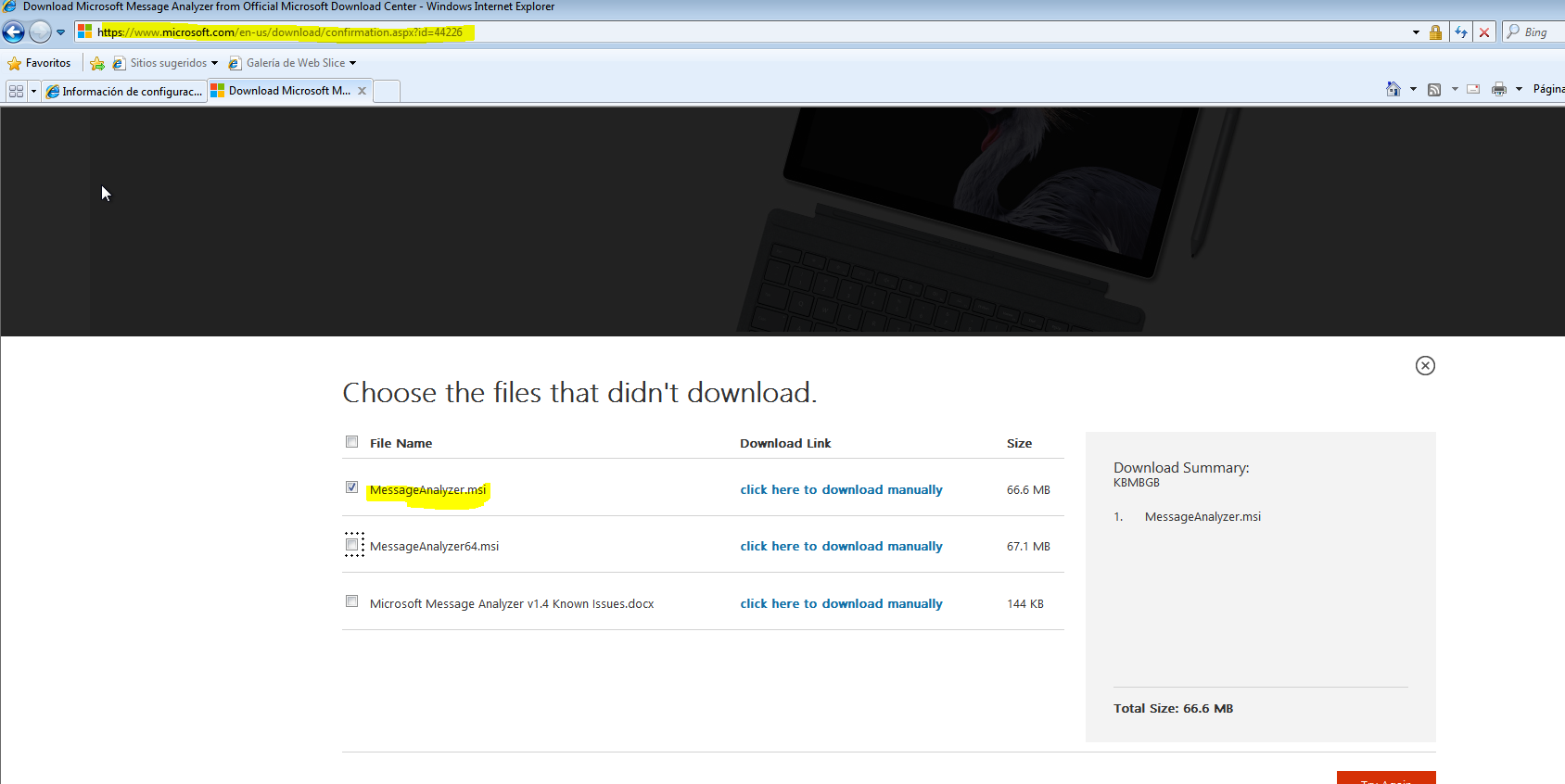
# Inside of the .cab file, we can see a .html report that we can open by our browser.

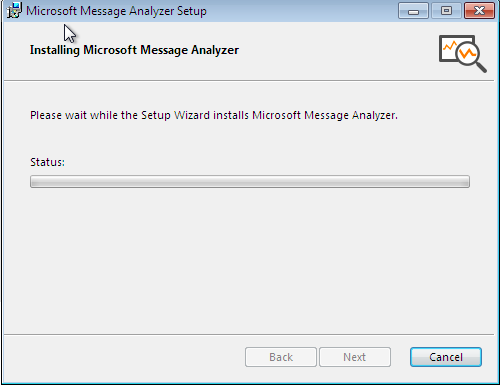


# This is the report of the capture.

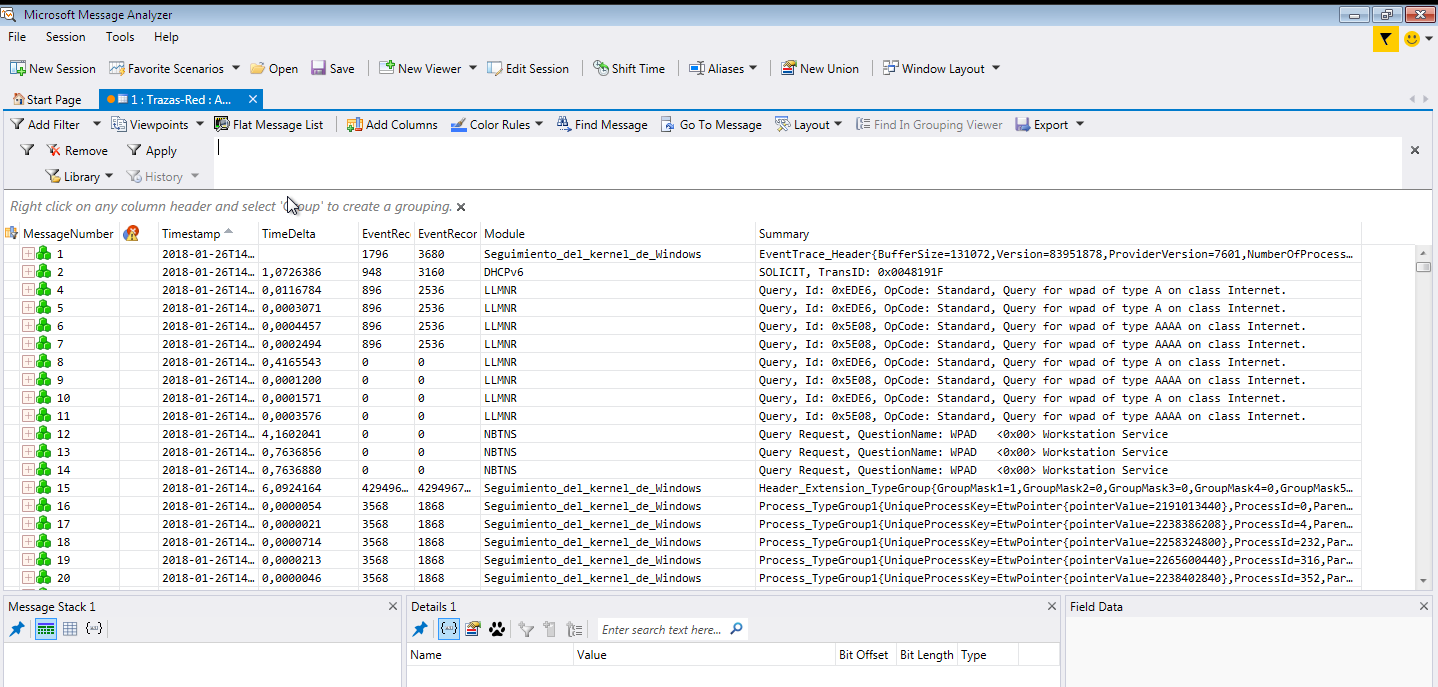


# To open the .etl file we need the programm: Microsoft message analyzer, so let’s download it!



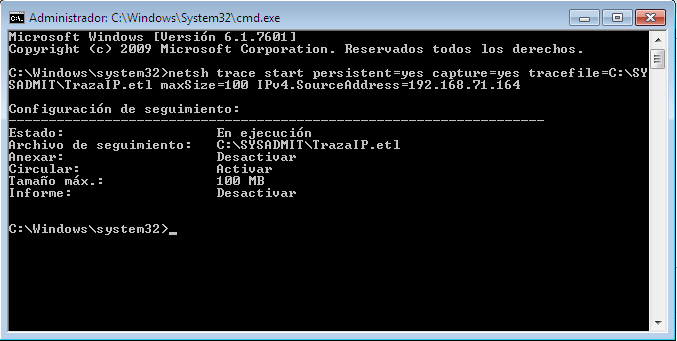


# Once it is installed we can open the file .cab and see the capture.

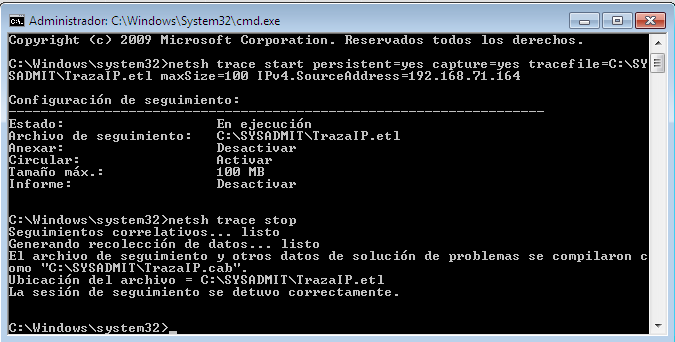


# Adding new parameters to the command.

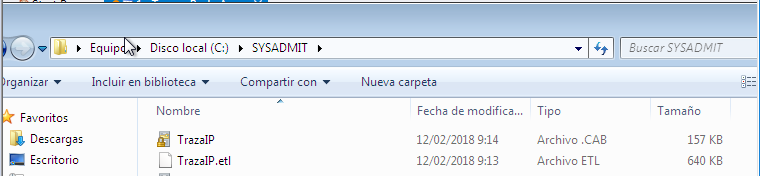
With the parameter maxsize= we configure the size of the generated file.



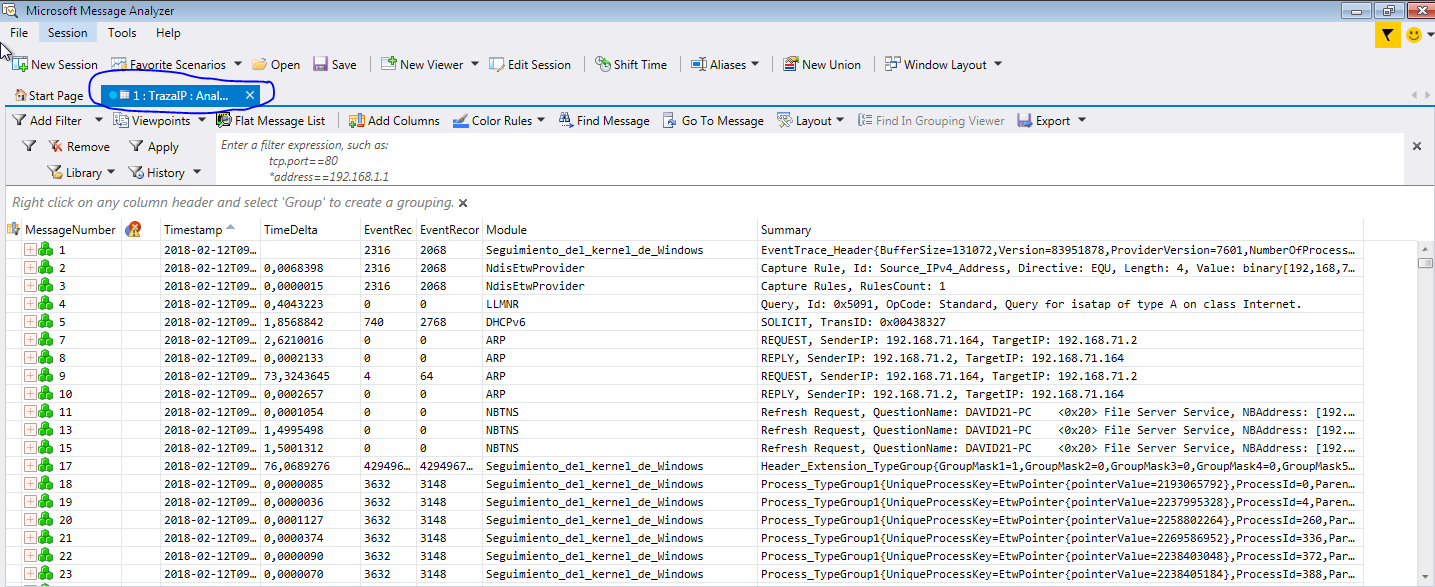
# Stopping the new capture.



# In the same folder that before, we save the generated files by the capture.



# We put the IP address that we have used in the capture as a fiter and we see the results.



# FINAL CONSIDERATION AND METACOGNITION

On the one hand, I have learnt another tool to sniff the network and I have tos ay that this tool is very flexible, you can do so many things with it.

To sum up, the practice has been interesting and I am looking forward to do the next one.