

70_71.60Bat_Cmd_Rundll_Reg

Emilio Cabo Gomis

Indice

Introducción.....	3
601 Tlist.....	1
603 TkillPID.....	3
741_wsatFormal.....	5
741 WsatFeatures.....	6
736_administradorDispositivos.....	7
733 RDLLConectarUDRed.....	8
733_BorrarHistorial.....	9
735 RDLLFirewall.....	10
731 RDLLUninstall.....	11
732 RDLLRed.....	12
724_habilitarConfRed.....	13
726_MostrarDirGW.....	14
729_PuertosHabilitados.....	15
721_reinstalarTCPIP.....	16
722_ConfActualTCP.....	17

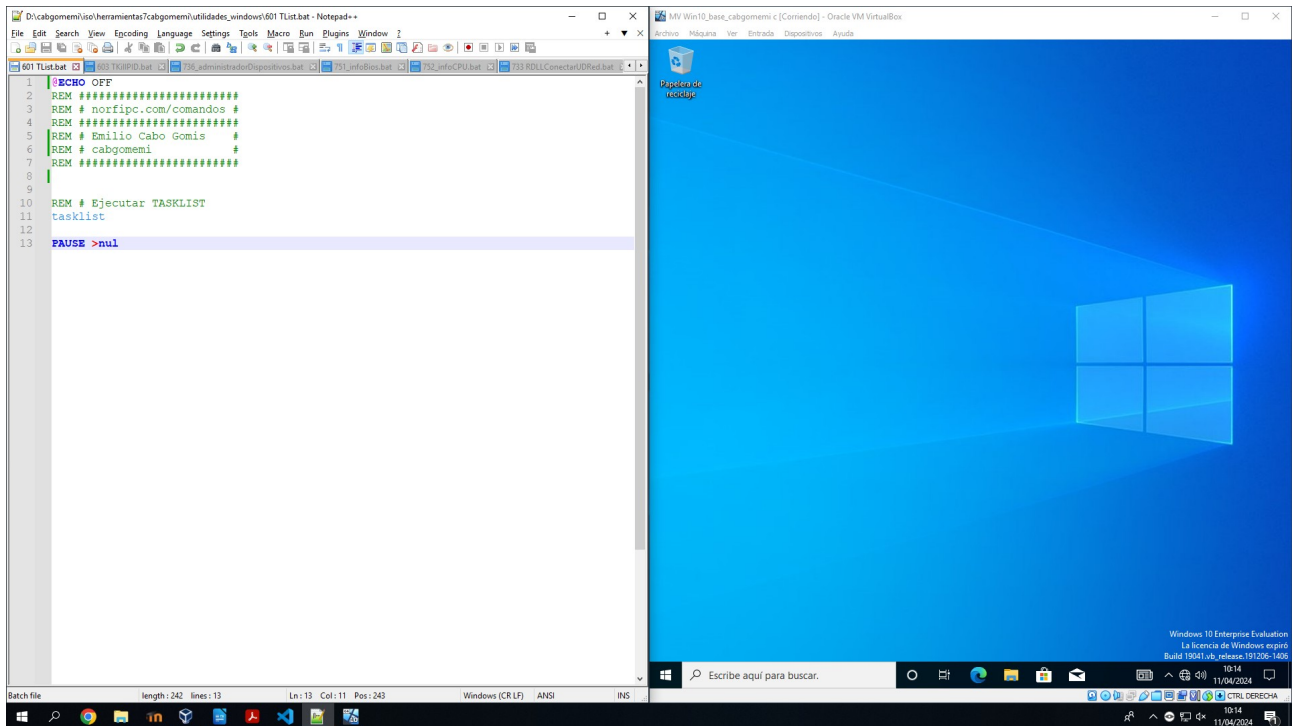
Introducción

En este ejercicio realizaremos 15 ejercicios en los que ejecutaremos una serie de scripts con las extensiones. **bat**, **Cmd** e **Rundll32**

Para ello utilizaremos un clon enlazado de una máquina **Windows 10** creada previamente.

601 Tlist

Este es el contenido del script



The screenshot shows a Windows 10 desktop environment. On the left, a Notepad++ window is open, displaying a batch script named '601 Tlist.bat'. The script contains the following lines:

```
1 ECHO OFF
2 REM #####
3 REM # noifipc.com/comandos #
4 REM #####
5 REM # Emilio Cabo Gomis #
6 REM # cabgomemi #
7 REM #####
8
9
10 REM # Ejecutar TASKLIST
11 tasklist
12
13 PAUSE >nul
```

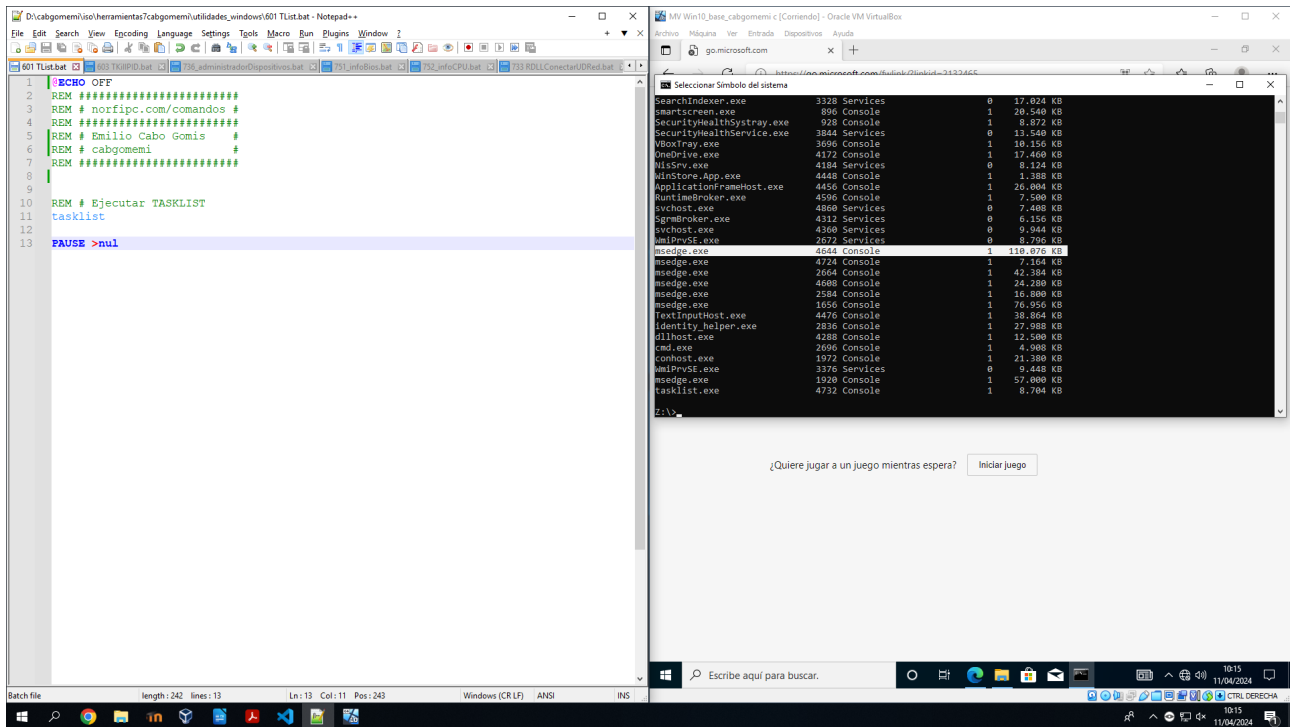
On the right, a VirtualBox window is open, showing a Windows 10 desktop. The desktop background is blue with the Windows logo. The taskbar at the bottom shows the search bar and several application icons. The system tray in the bottom right corner displays the date and time as 10:14 on 11/04/2024.

Realizamos una acción para que nos salga una nueva tarea.

Ejecutamos el script.

Vemos la tarea que nos ha salido según el PID **4644**

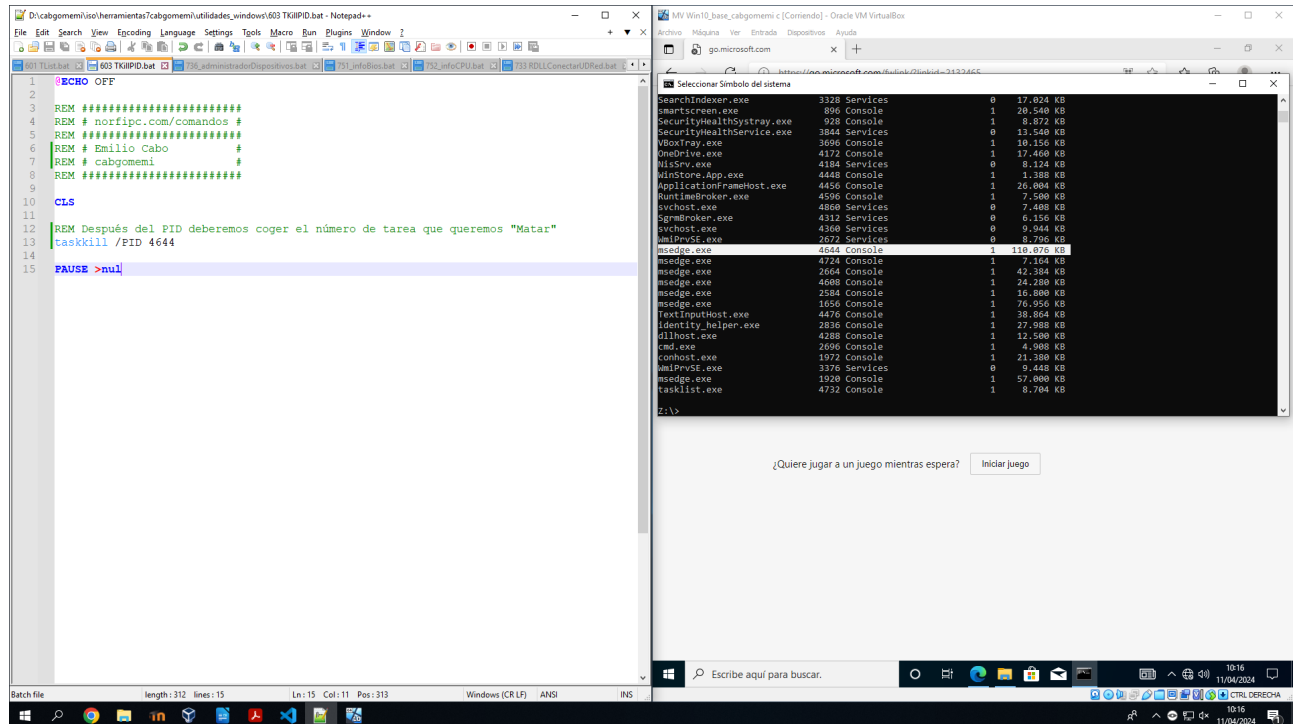
70_71.60Bat_Cmd_Rundll_Reg



603 TkilIPID

La tarea que abrimos antes (En nuestro caso internet explorer) según el PID que captamos en el anterior comando.

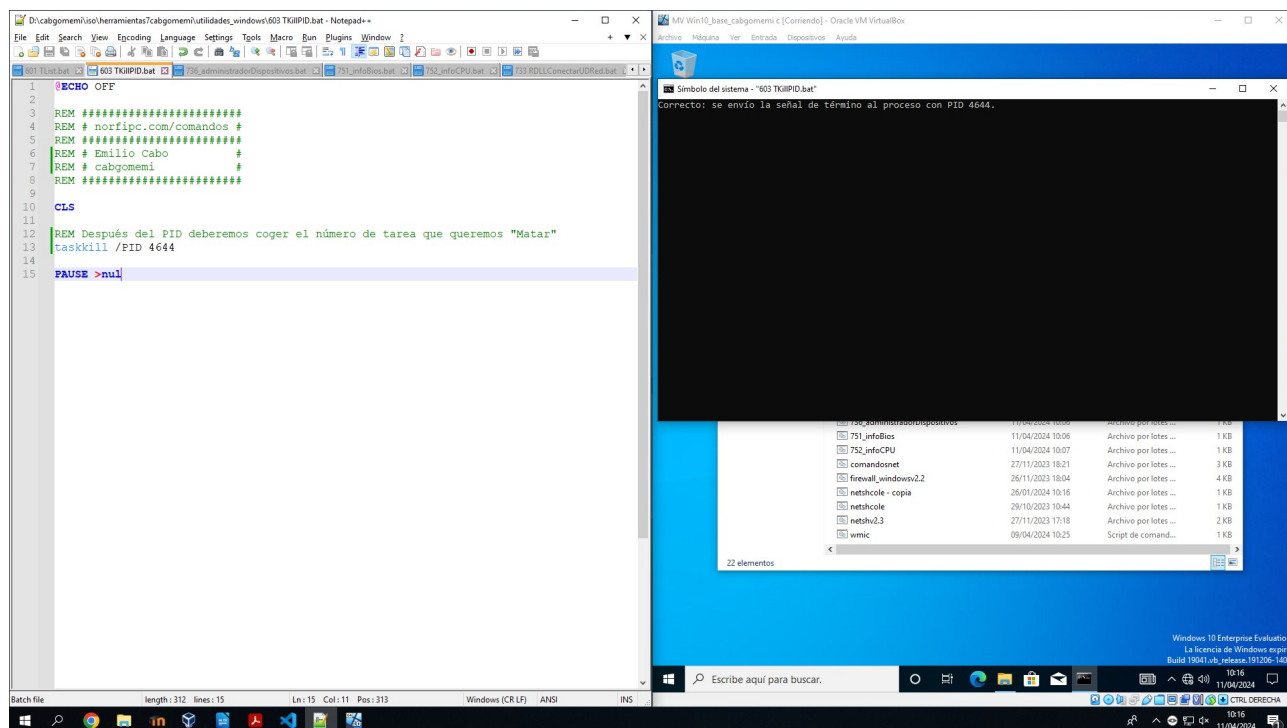
Editamos el script adecuadamente.



Ejecutamos el script.

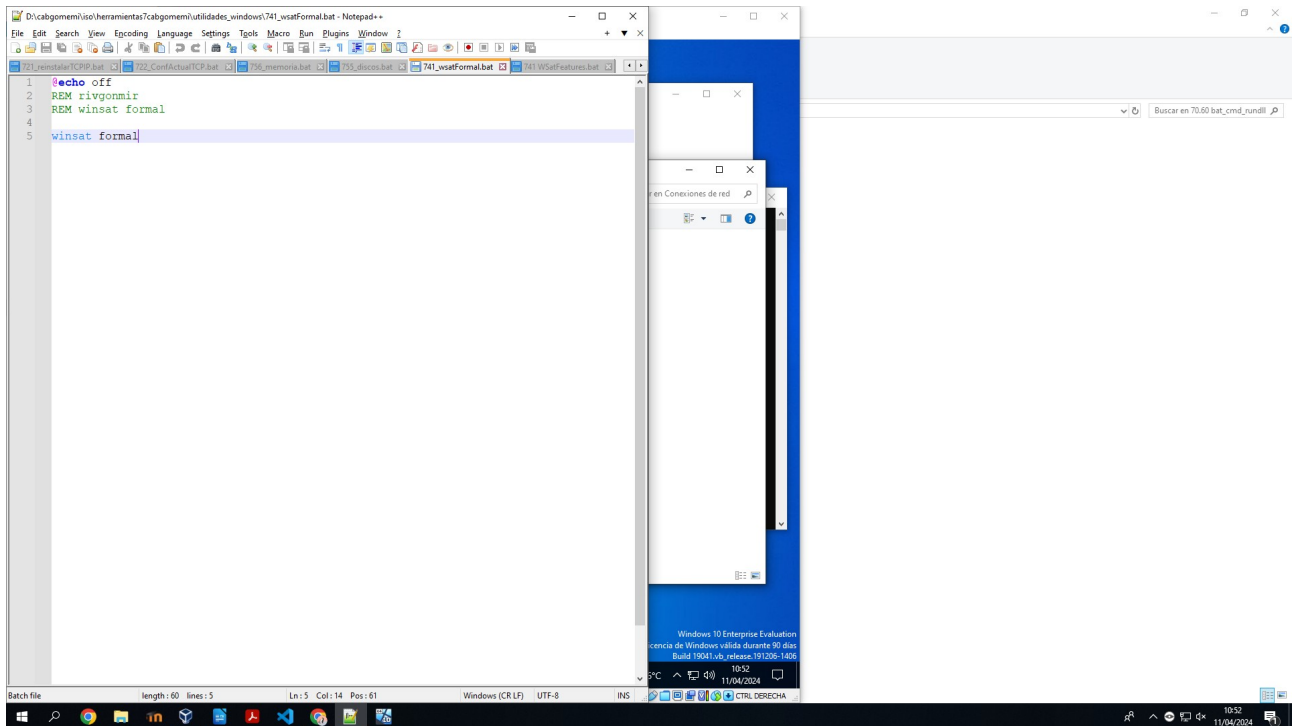
Finalizará la ejecución de edge.

70_71.60Bat_Cmd_Rundll_Reg

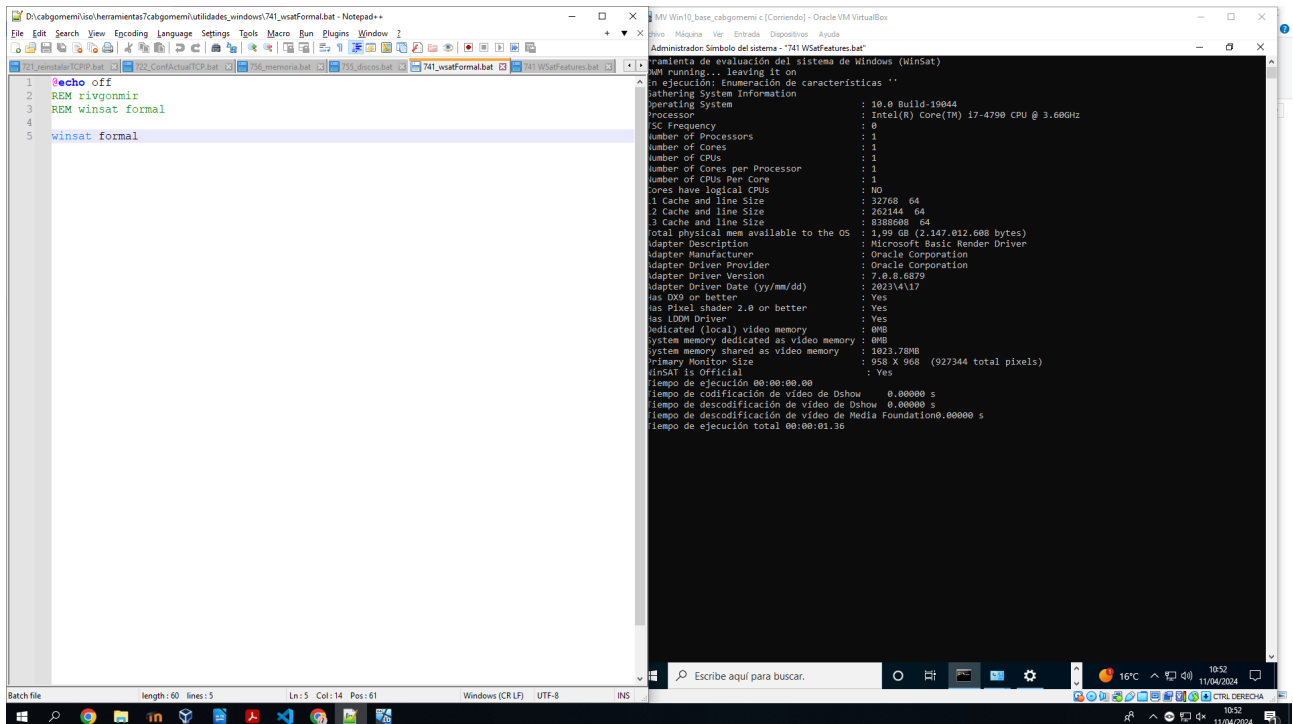


741_wsafFormal

Editamos el script adecuadamente.

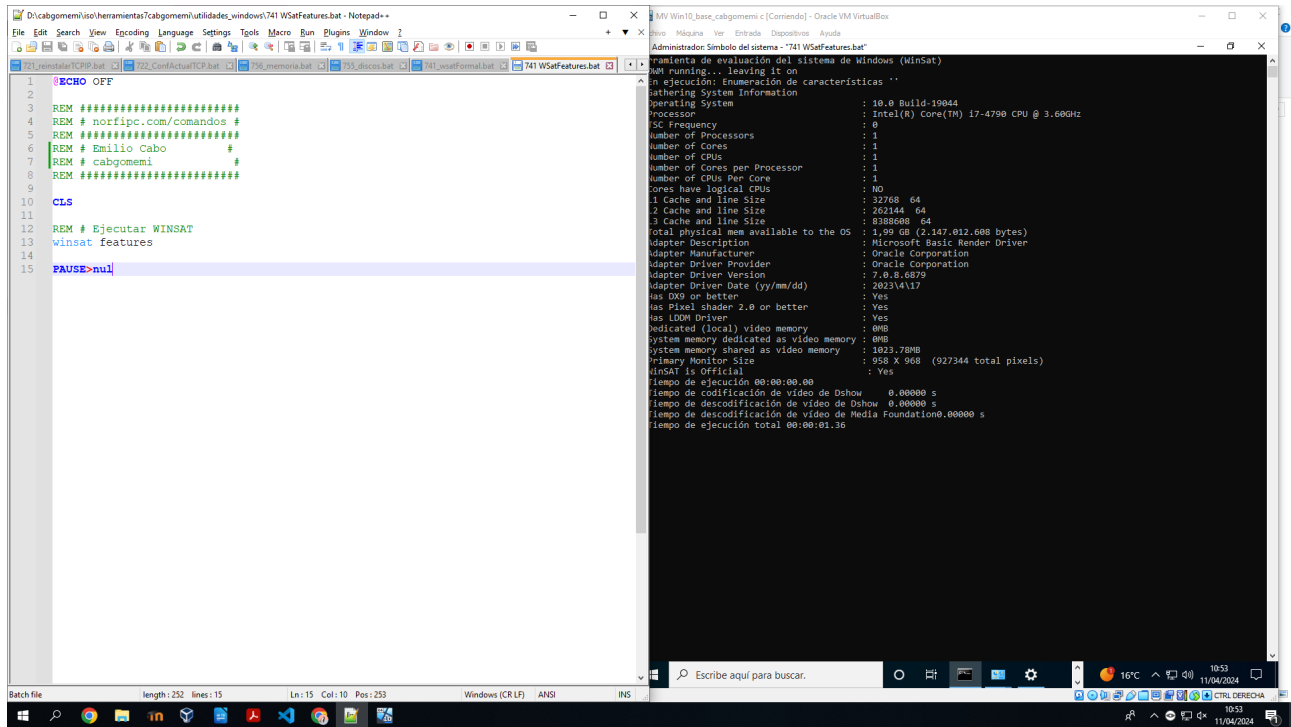


Ejecutamos el script.



741 WsatFeatures

Editamos el script adecuadamente.



```
1 @ECHO OFF
2 REM #####
3 REM # norfipc.com/comandos #
4 REM # #####
5 REM # Emilio Cabo #
6 REM # cabgomemi #
7 REM # #####
8
9
10 CLS
11
12 REM # Ejecutar WINSAT
13 winsat features
14
15 PAUSE>nu|
```

Administrador: Símbolo del sistema - "741 WsatFeatures.bat"

Administrador: Evaluación del sistema de Windows (WinSAT)

WinSAT running... Leaving it on in ejecución: Enumeración de características "

Gathering System Information

Operating System : 10.0 Build-19044

Processor : Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz

SC Frequency : 0

Number of Processors : 1

Number of Cores : 1

Number of CPUs : 1

Number of Cores per Processor : 1

Number of CPUs Per Core : 1

Cores have logical CPUs : NO

1 Cache and line Size : 32768 64

2 Cache and line Size : 262144 64

3 Cache and line Size : 8388608 64

total physical mem available to the OS : 1.99 GB (2.147.012.688 bytes)

Adapter Description : Microsoft Basic Render Driver

Adapter Manufacturer : Oracle Corporation

Adapter Driver Provider : Oracle Corporation

Adapter Driver Version : 7.0.8.6879

Adapter Driver Date (yy/mm/dd) : 2023/4/17

Has DX9 or better : Yes

Has Pixel shader 2.0 or better : Yes

Has LDM Driver : Yes

Dedicated (local) video memory : 0MB

System memory dedicated as video memory : 0MB

System memory shared as video memory : 1023.78MB

Primary Monitor Size : 958 X 968 (927344 total pixels)

WinSAT is Official : Yes

tiempo de ejecución 00:00:00.00

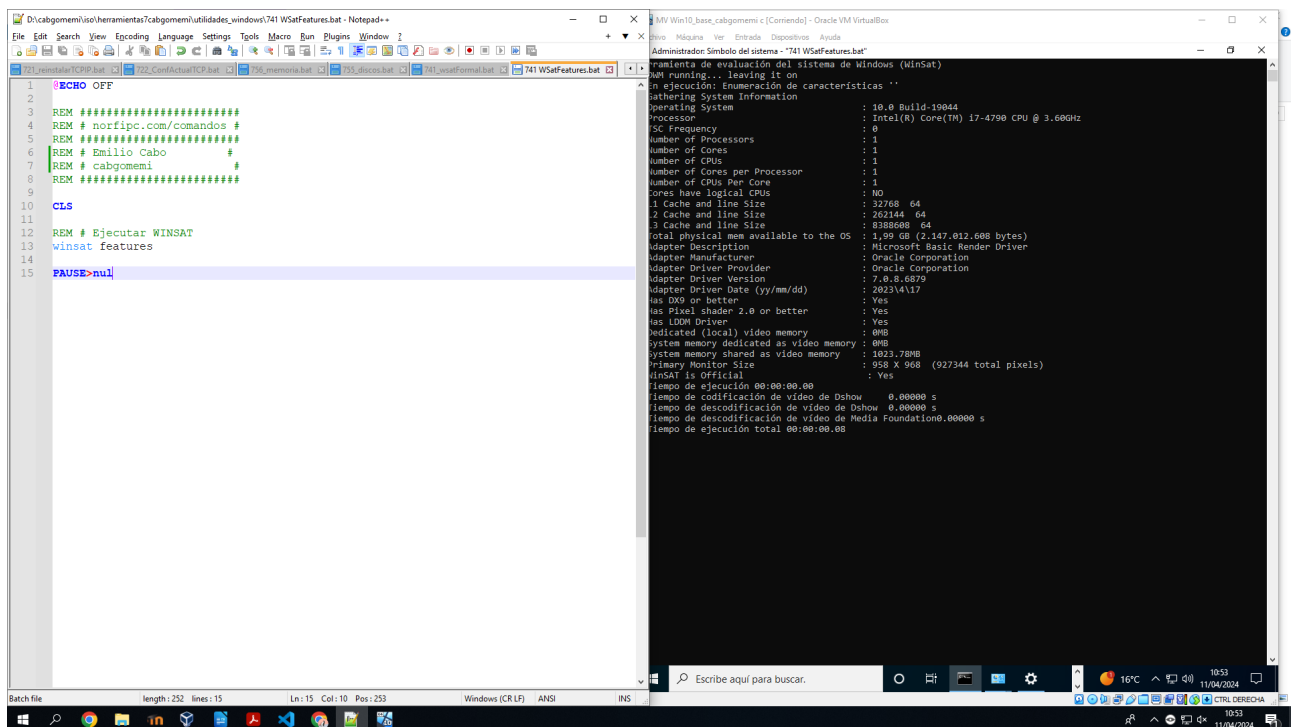
tiempo de codificación de vídeo de Dshow 0.00000 s

tiempo de decodificación de vídeo de Dshow 0.00000 s

tiempo de decodificación de vídeo de Media Foundation 0.00000 s

tiempo de ejecución total 00:00:01.36

Ejecutamos el script.



```
1 @ECHO OFF
2 REM #####
3 REM # norfipc.com/comandos #
4 REM # #####
5 REM # Emilio Cabo #
6 REM # cabgomemi #
7 REM # #####
8
9
10 CLS
11
12 REM # Ejecutar WINSAT
13 winsat features
14
15 PAUSE>nu|
```

Administrador: Símbolo del sistema - "741 WsatFeatures.bat"

Administrador: Evaluación del sistema de Windows (WinSAT)

WinSAT running... Leaving it on in ejecución: Enumeración de características "

Gathering System Information

Operating System : 10.0 Build-19044

Processor : Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz

SC Frequency : 0

Number of Processors : 1

Number of Cores : 1

Number of CPUs : 1

Number of Cores per Processor : 1

Number of CPUs Per Core : 1

Cores have logical CPUs : NO

1 Cache and line Size : 32768 64

2 Cache and line Size : 262144 64

3 Cache and line Size : 8388608 64

total physical mem available to the OS : 1.99 GB (2.147.012.688 bytes)

Adapter Description : Microsoft Basic Render Driver

Adapter Manufacturer : Oracle Corporation

Adapter Driver Provider : Oracle Corporation

Adapter Driver Version : 7.0.8.6879

Adapter Driver Date (yy/mm/dd) : 2023/4/17

Has DX9 or better : Yes

Has Pixel shader 2.0 or better : Yes

Has LDM Driver : Yes

Dedicated (local) video memory : 0MB

System memory dedicated as video memory : 0MB

System memory shared as video memory : 1023.78MB

Primary Monitor Size : 958 X 968 (927344 total pixels)

WinSAT is Official : Yes

tiempo de ejecución 00:00:00.00

tiempo de codificación de vídeo de Dshow 0.00000 s

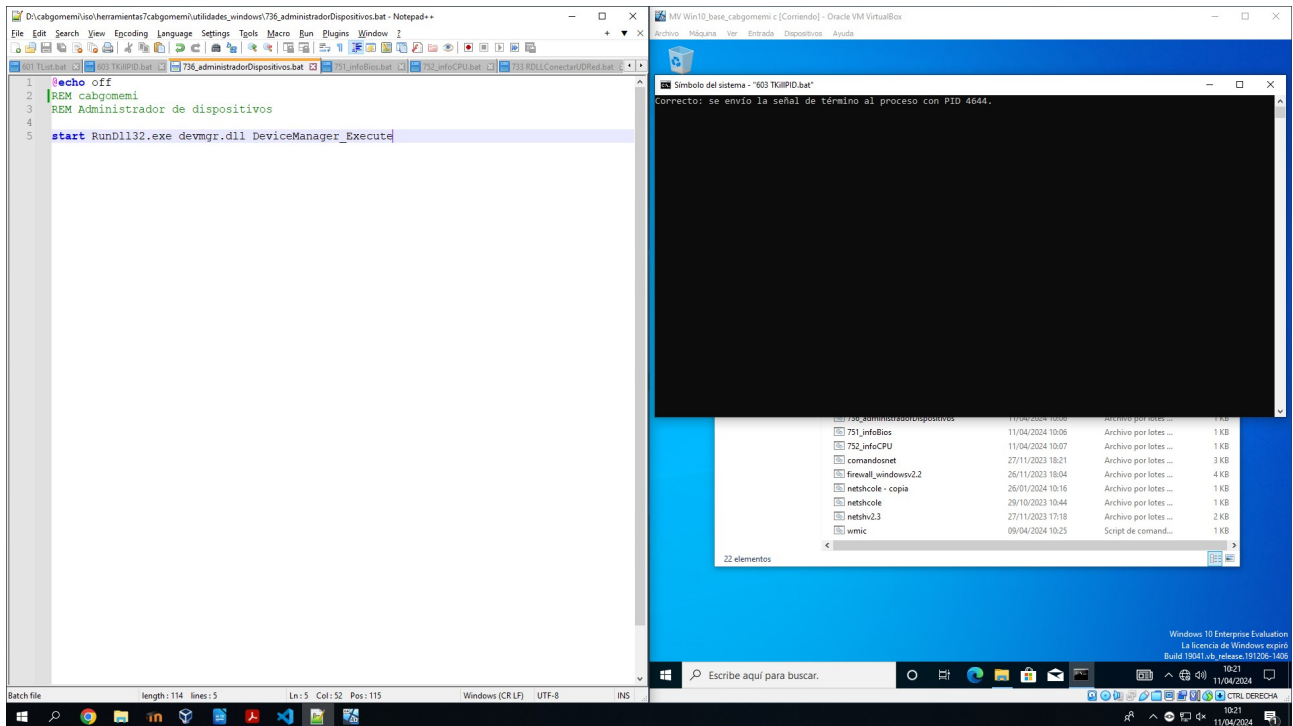
tiempo de decodificación de vídeo de Dshow 0.00000 s

tiempo de decodificación de vídeo de Media Foundation 0.00000 s

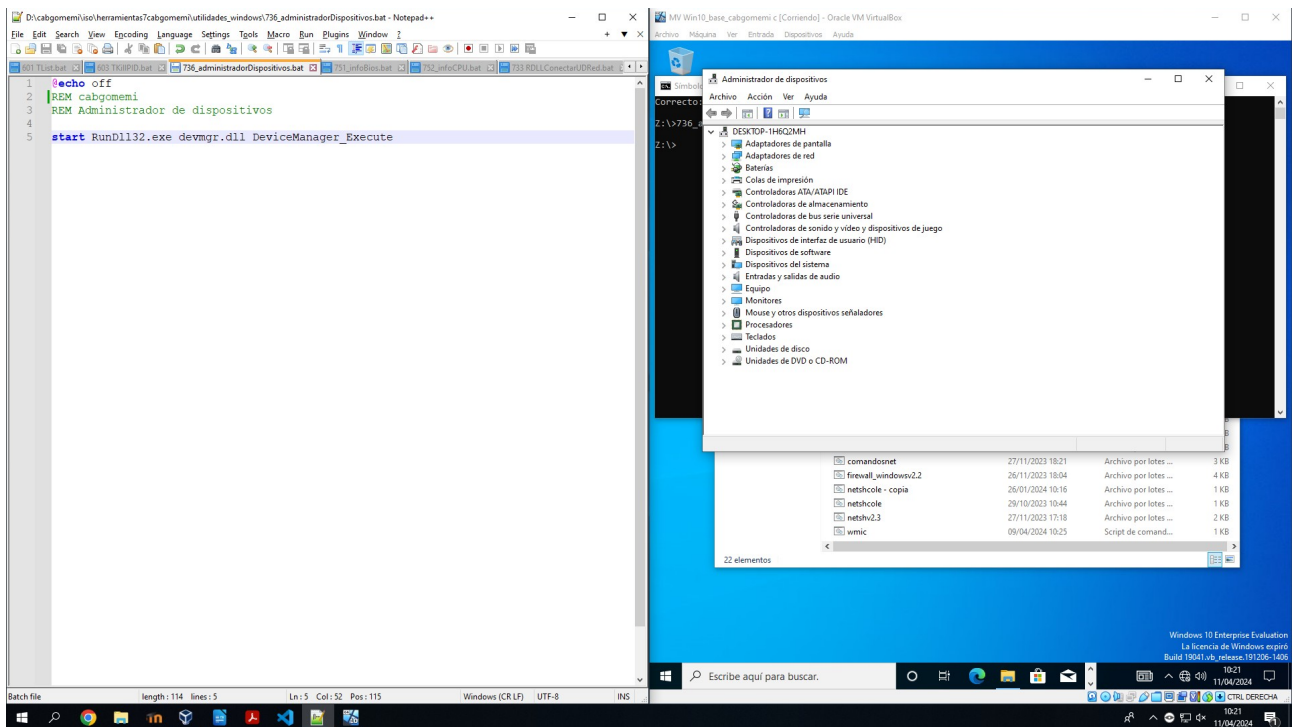
tiempo de ejecución total 00:00:00.00

736_administradorDispositivos

Editamos el script adecuadamente.

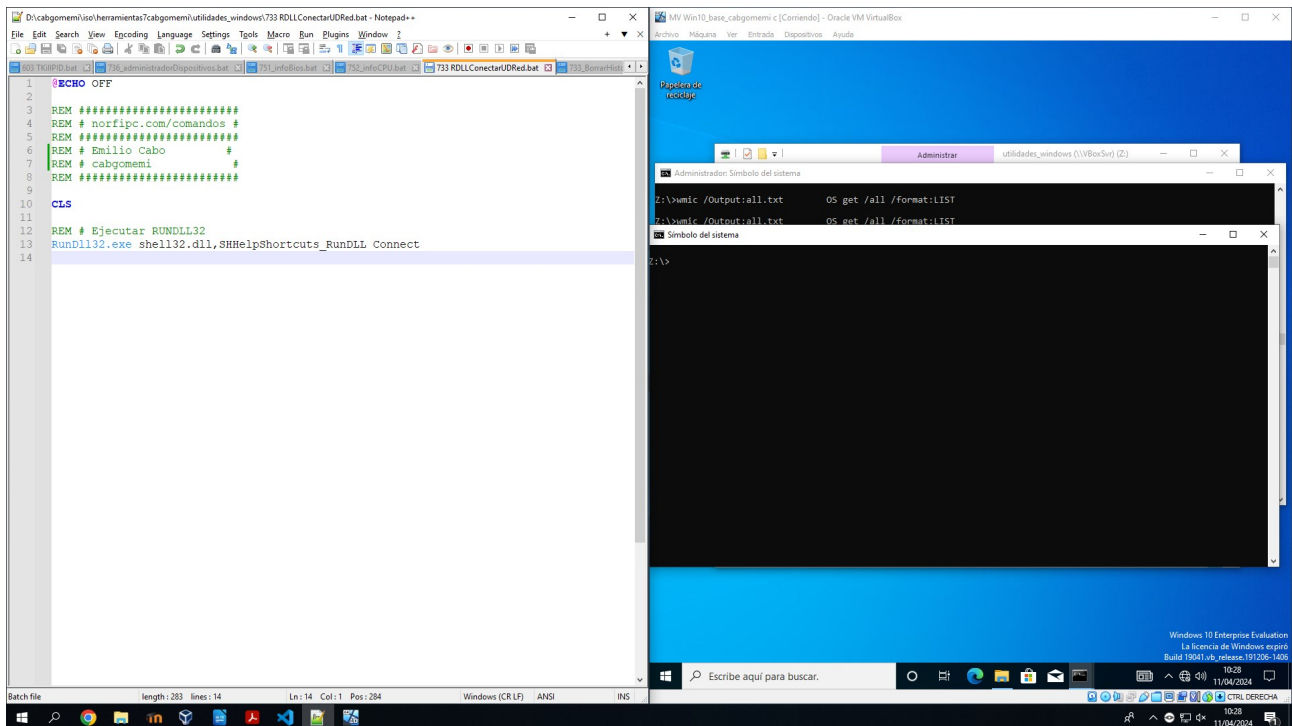


Ejecutamos el script.

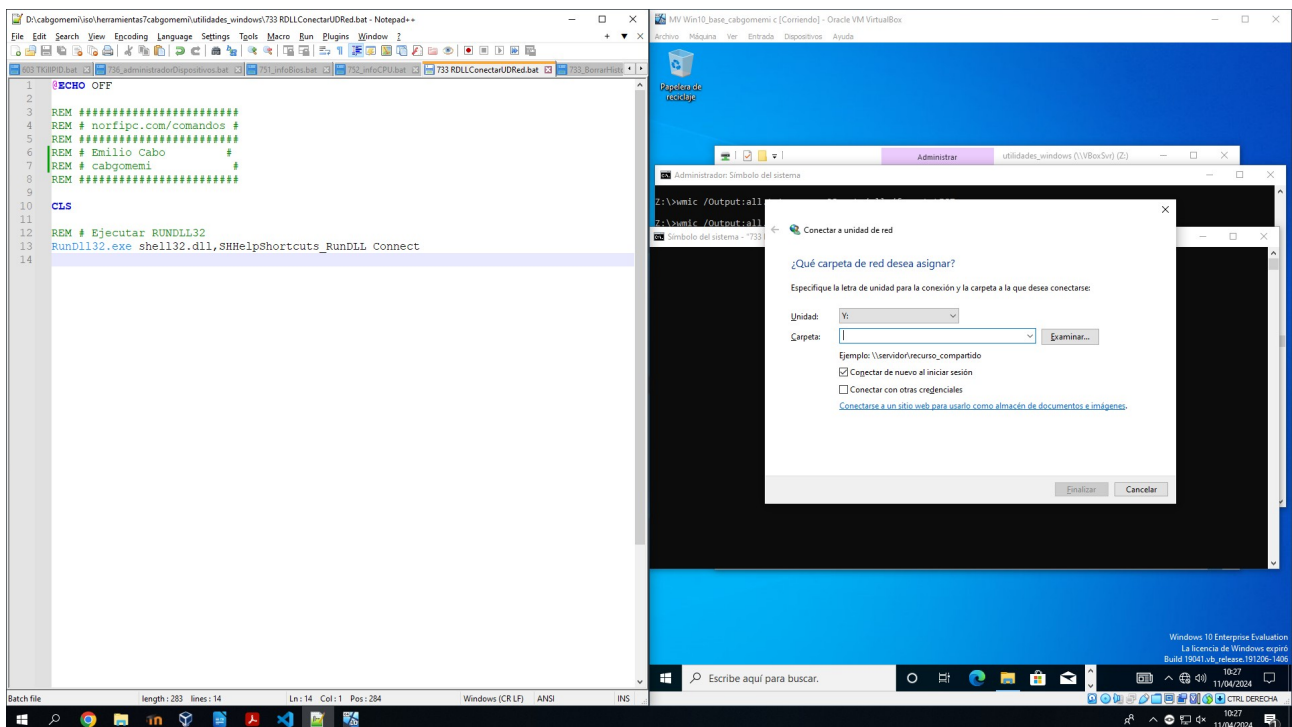


733 RDLLConectarUDRed

Editamos el script adecuadamente.

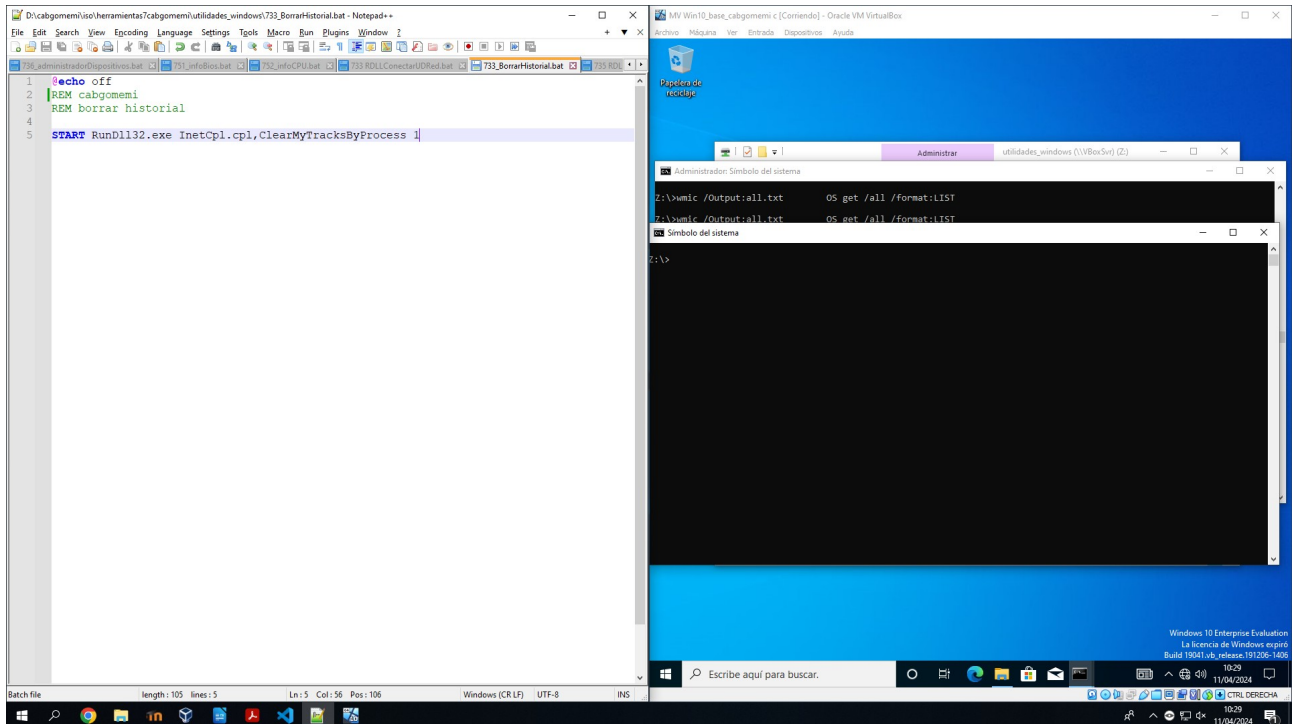


Ejecutamos el script.

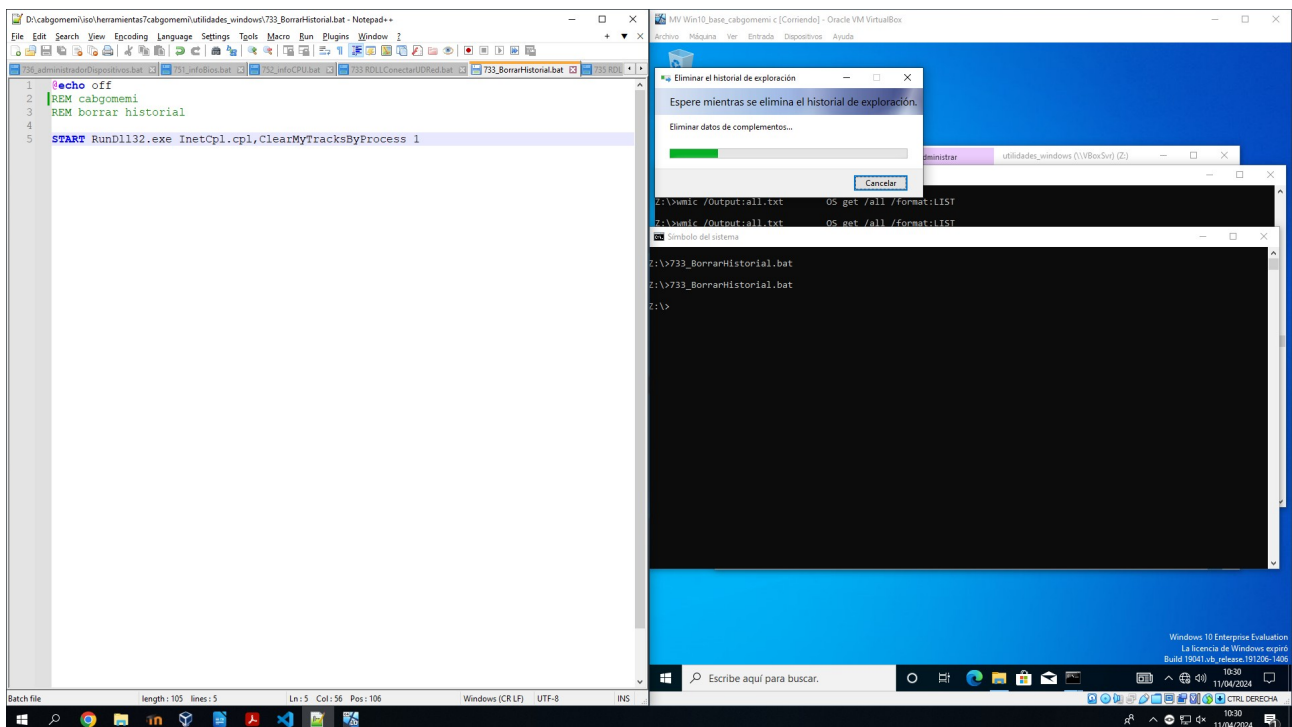


733_BorrarHistorial

Editamos el script adecuadamente.

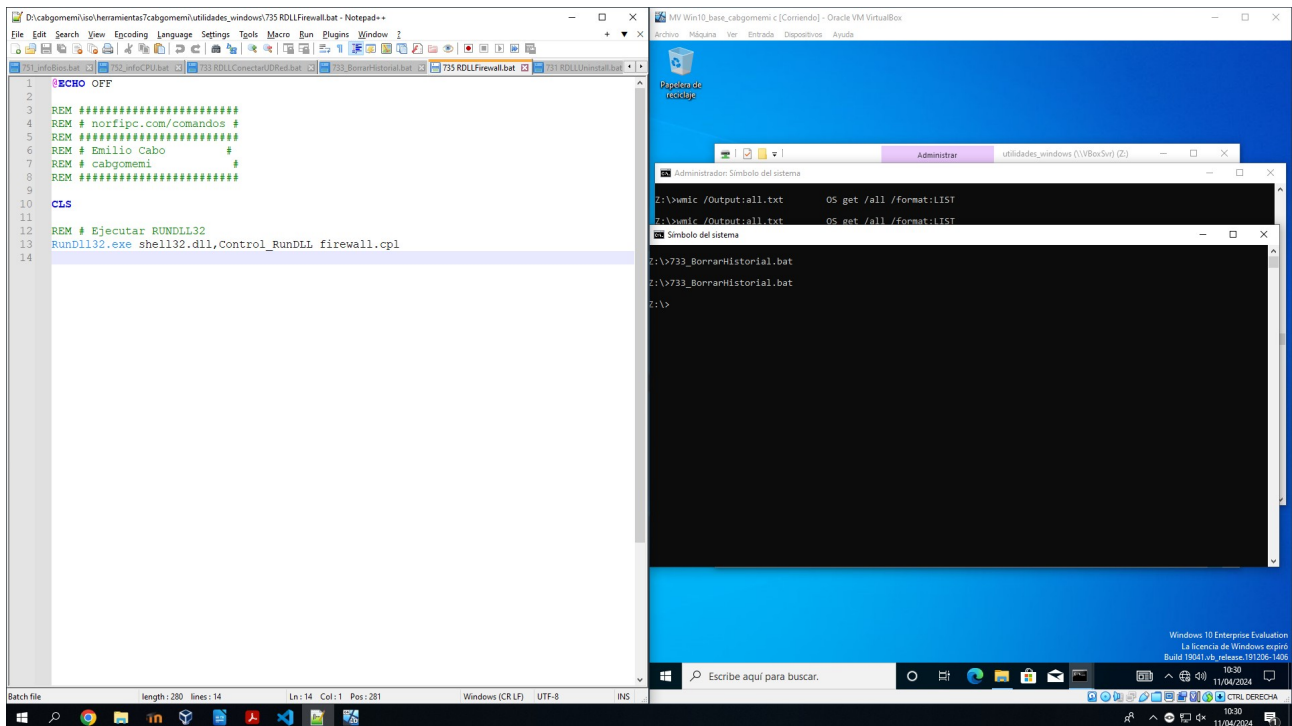


Ejecutamos el script.

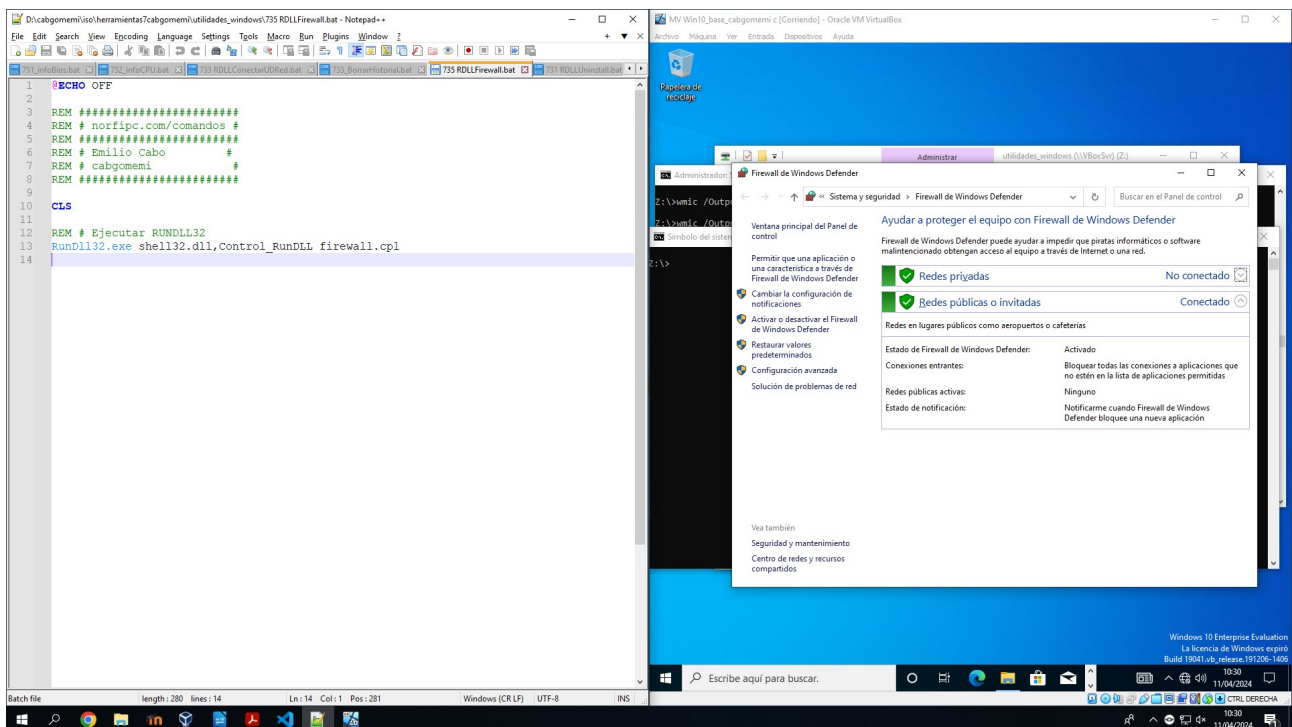


735 RDLLFirewall

Editamos el script adecuadamente.

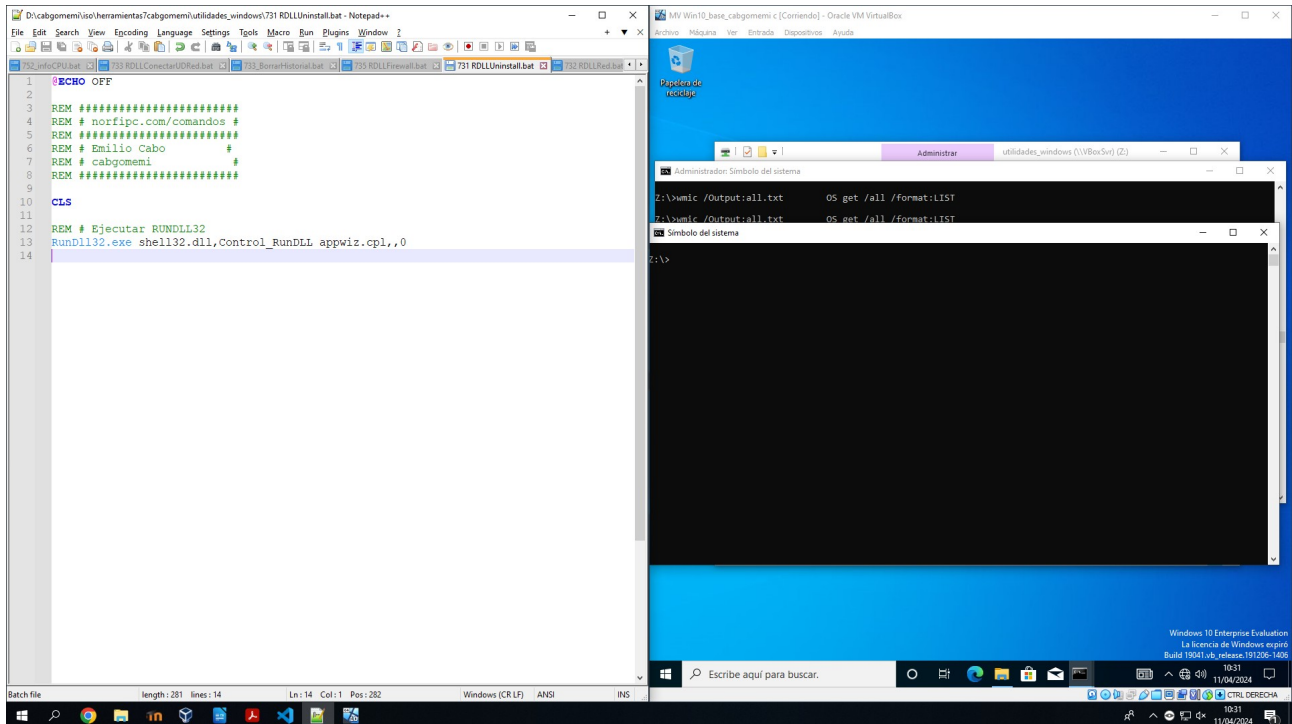


Ejecutamos el script.

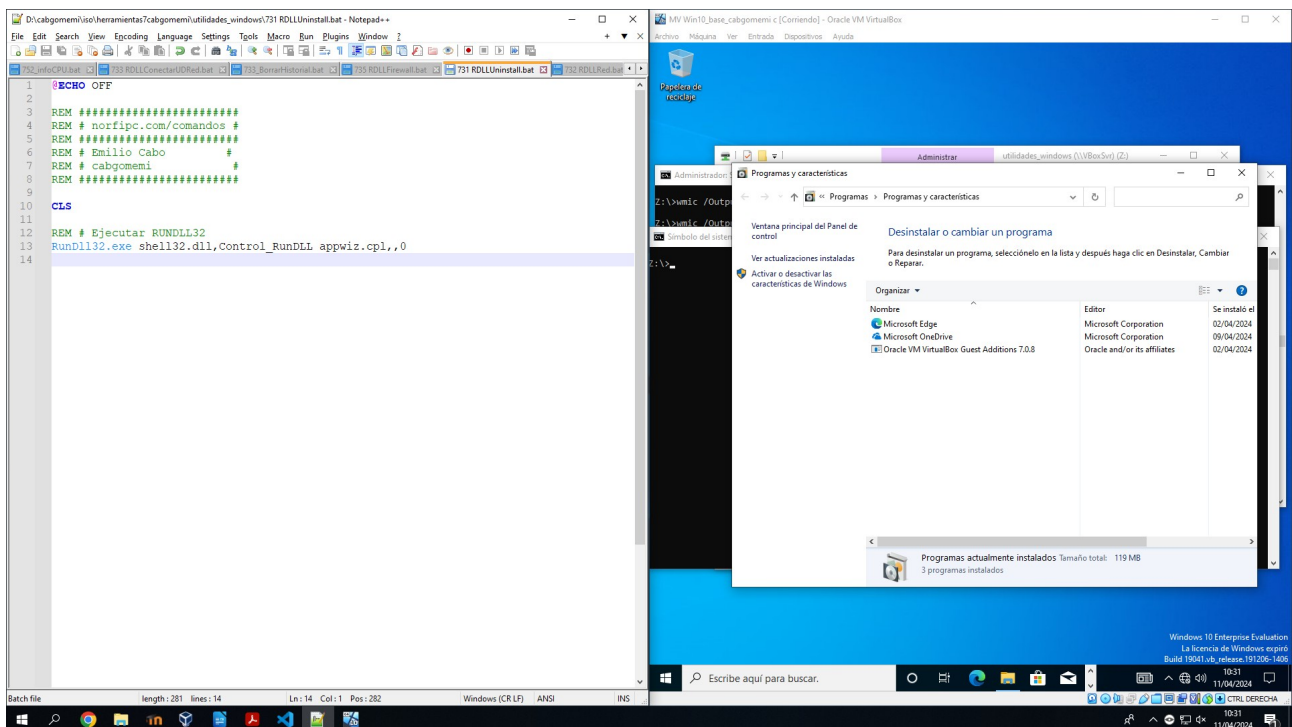


731 RDLLUninstall

Editamos el script adecuadamente.

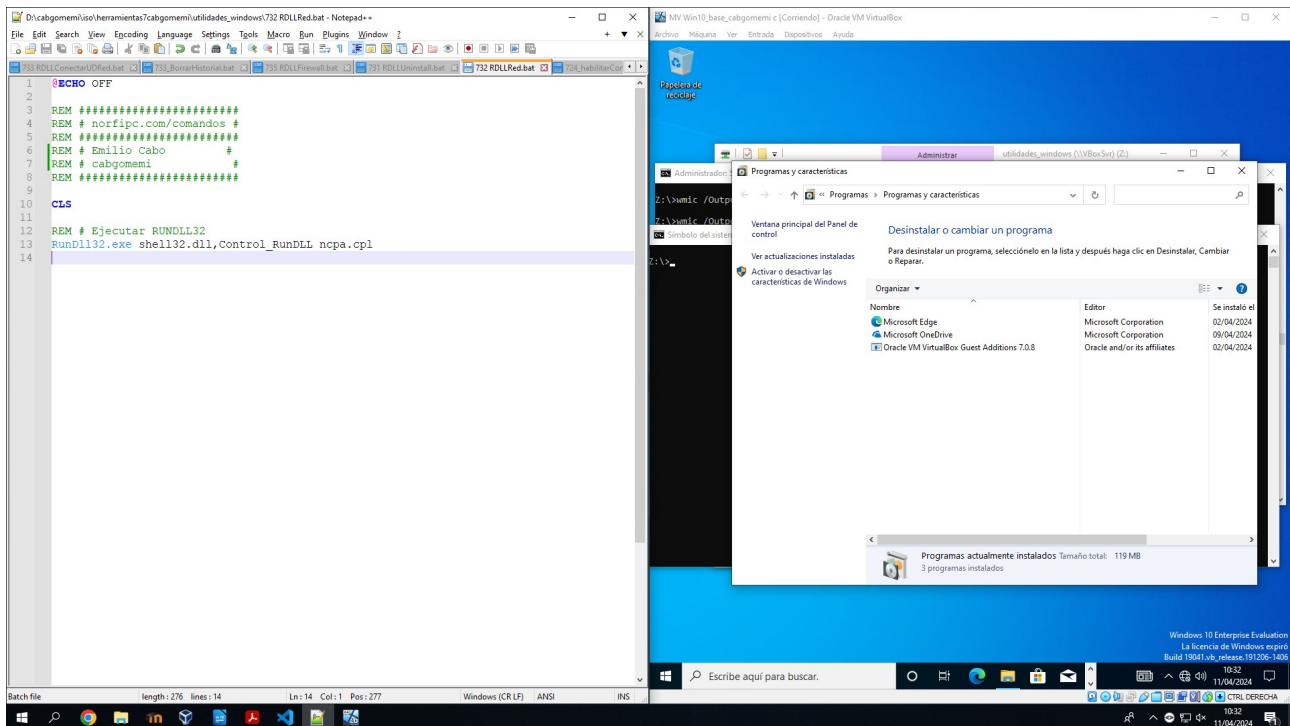


Ejecutamos el script.

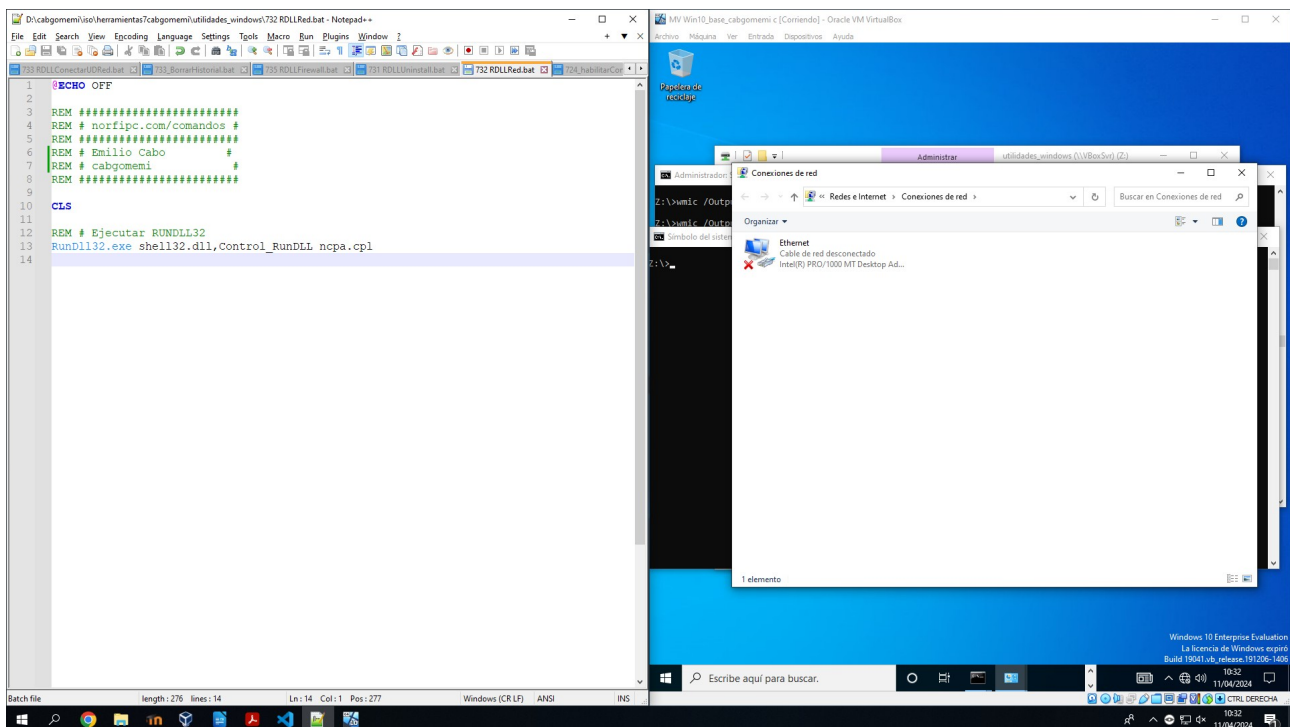


732 RDLLRed

Editamos el script adecuadamente.

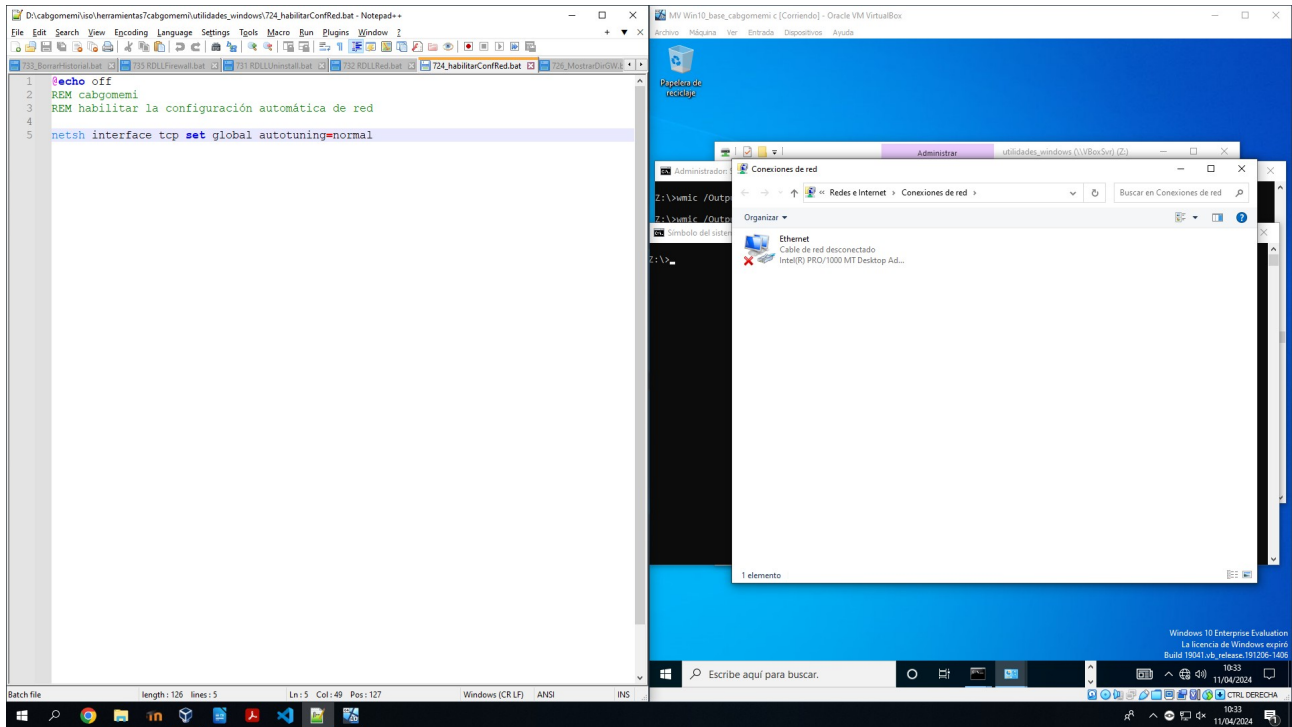


Ejecutamos el script.

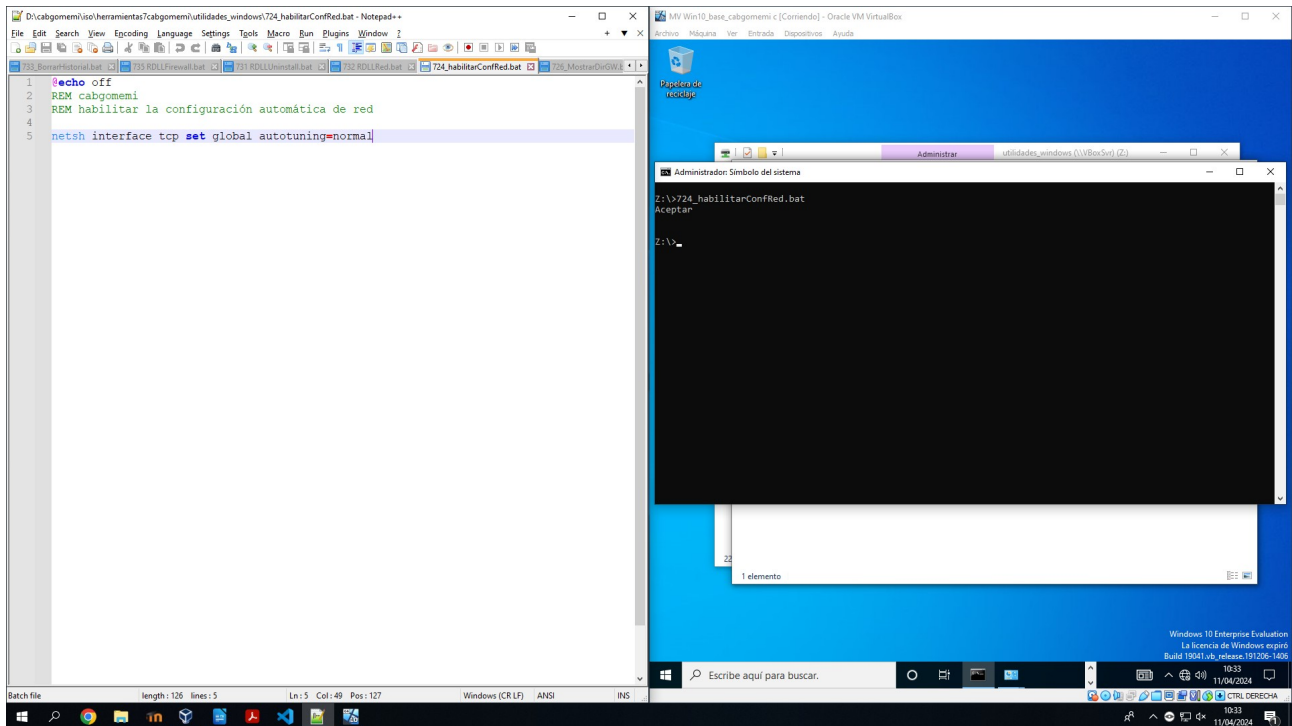


724_habilitaConfRed

Editamos el script adecuadamente.

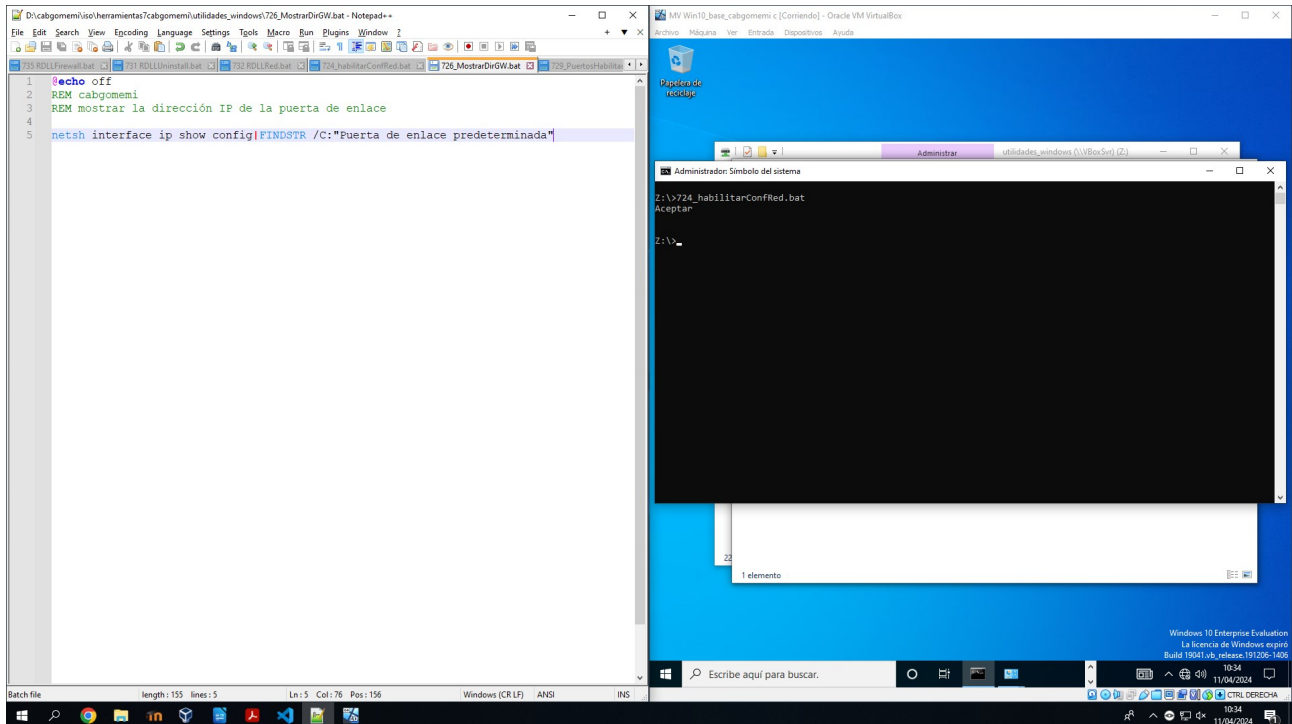


Ejecutamos el script.

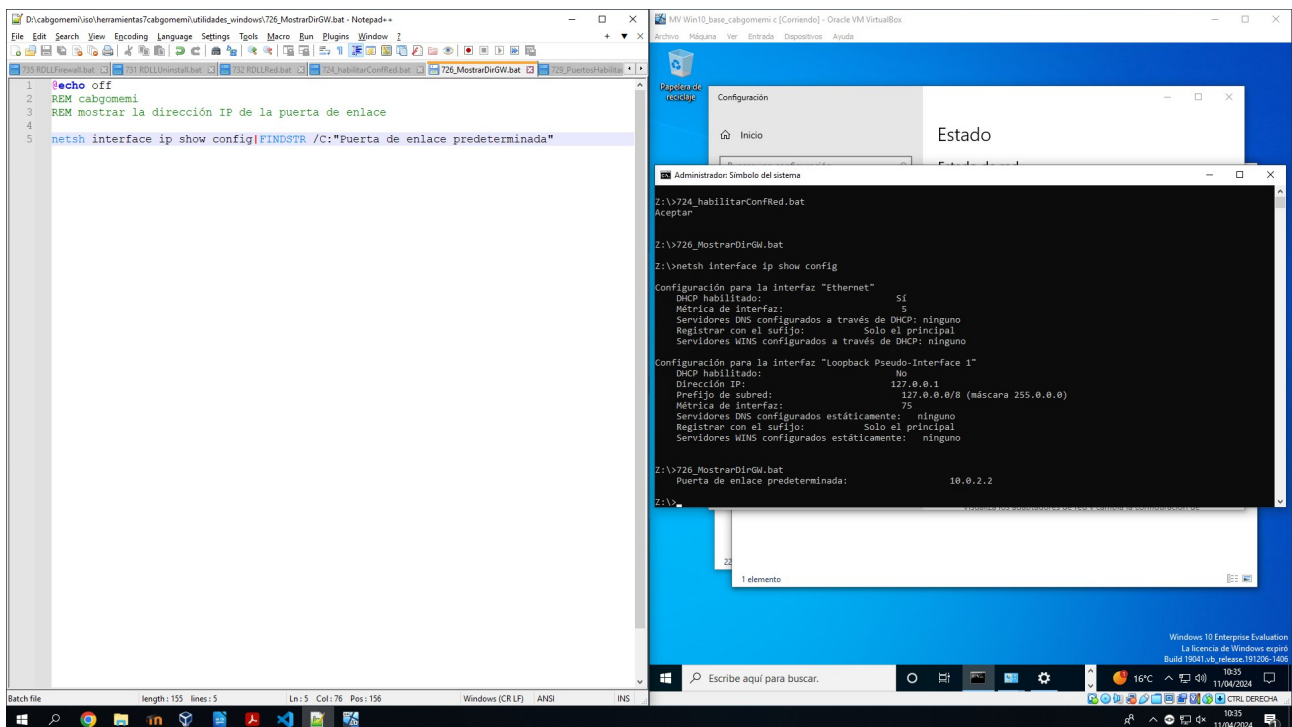


726_MostrarDirGW

Editamos el script adecuadamente.

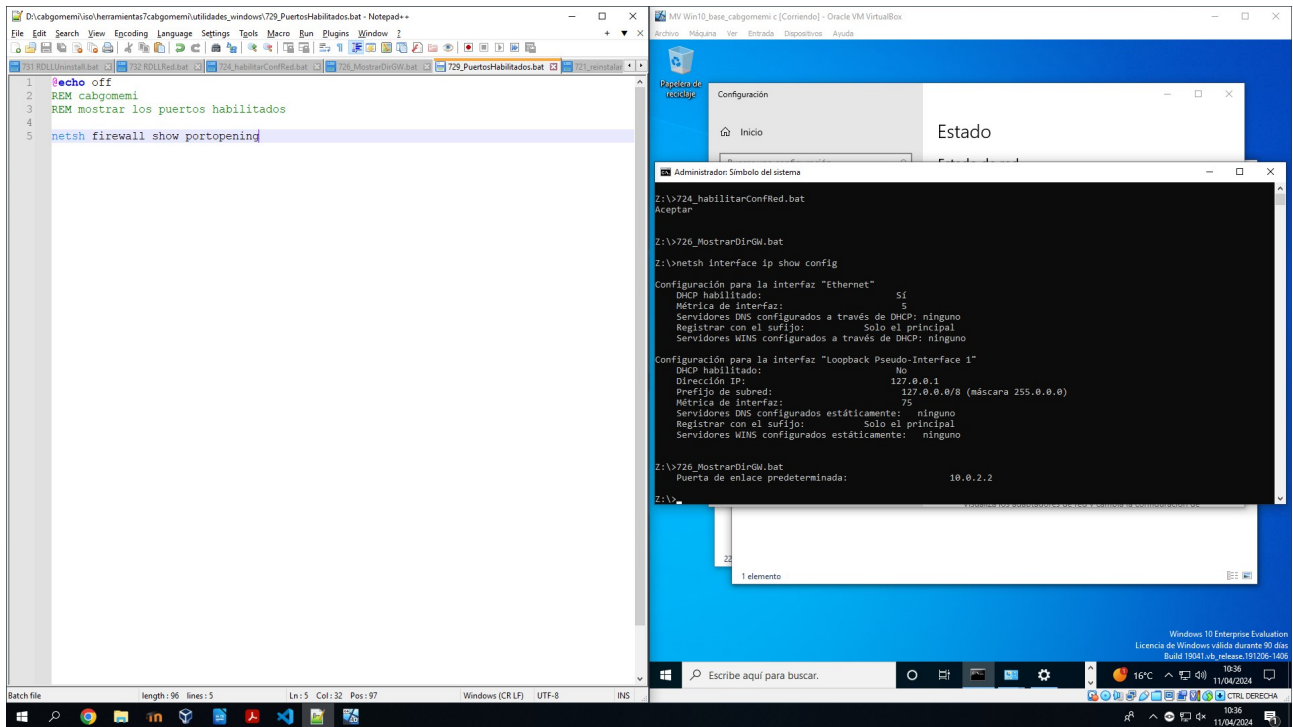


Ejecutamos el script.

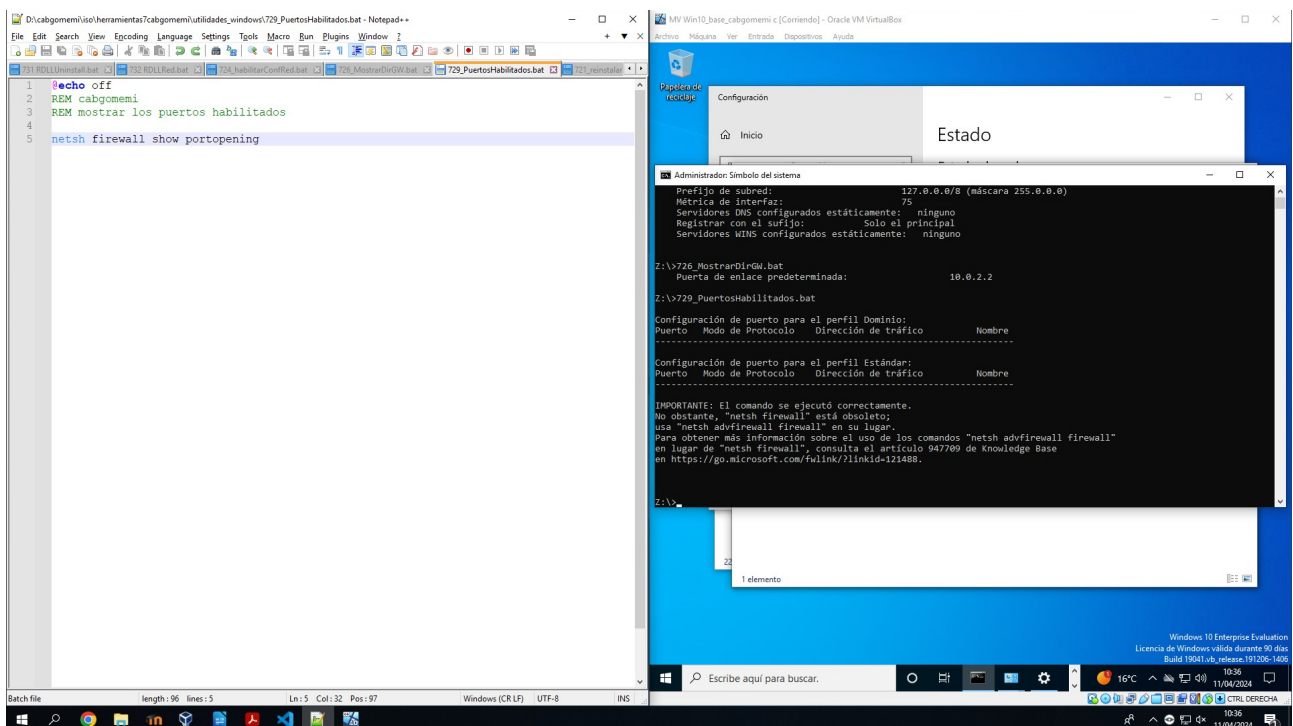


729_PuertosHabilitados

Editamos el script adecuadamente.

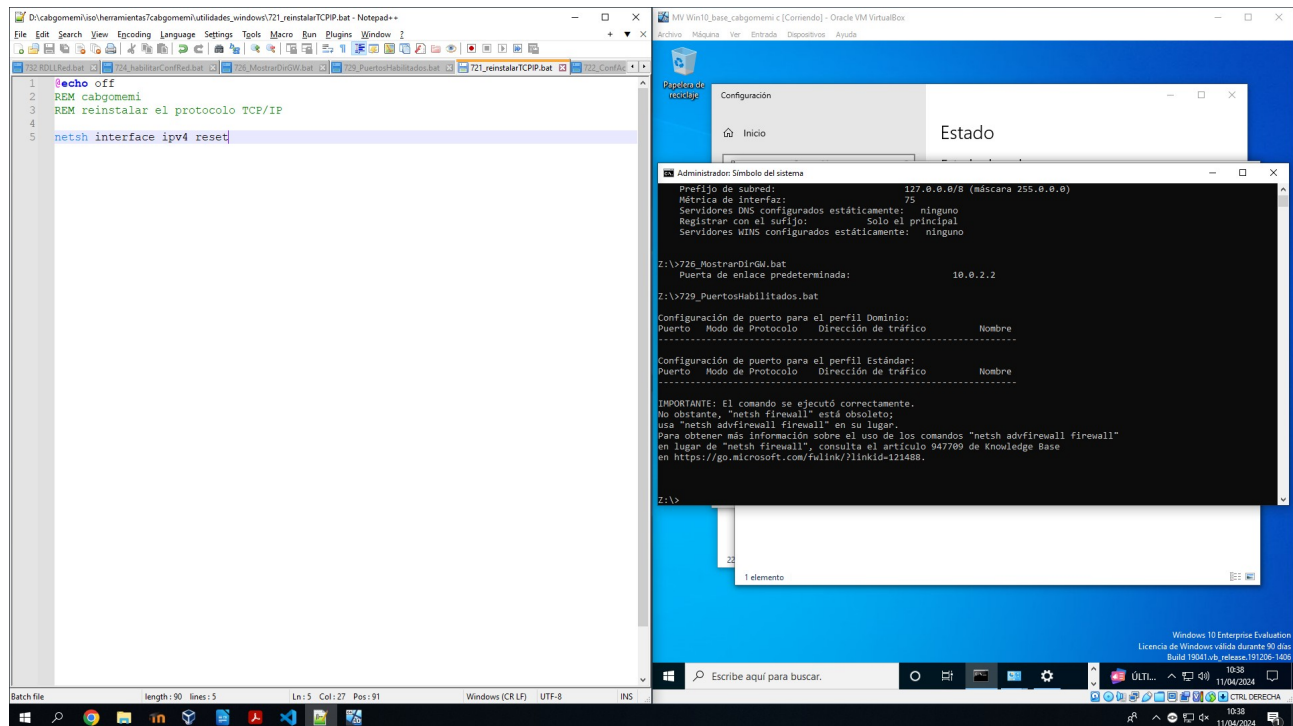


Ejecutamos el script.

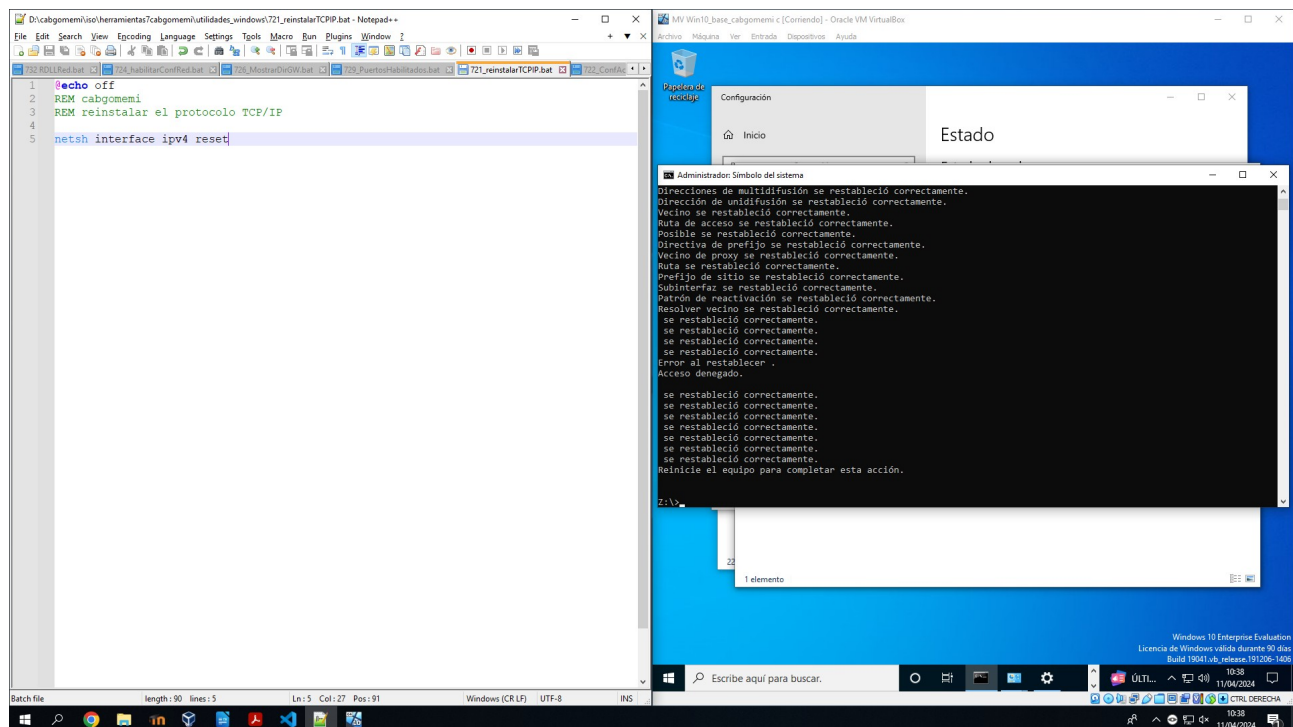


721_reinstalarTCP/IP

Editamos el script adecuadamente.

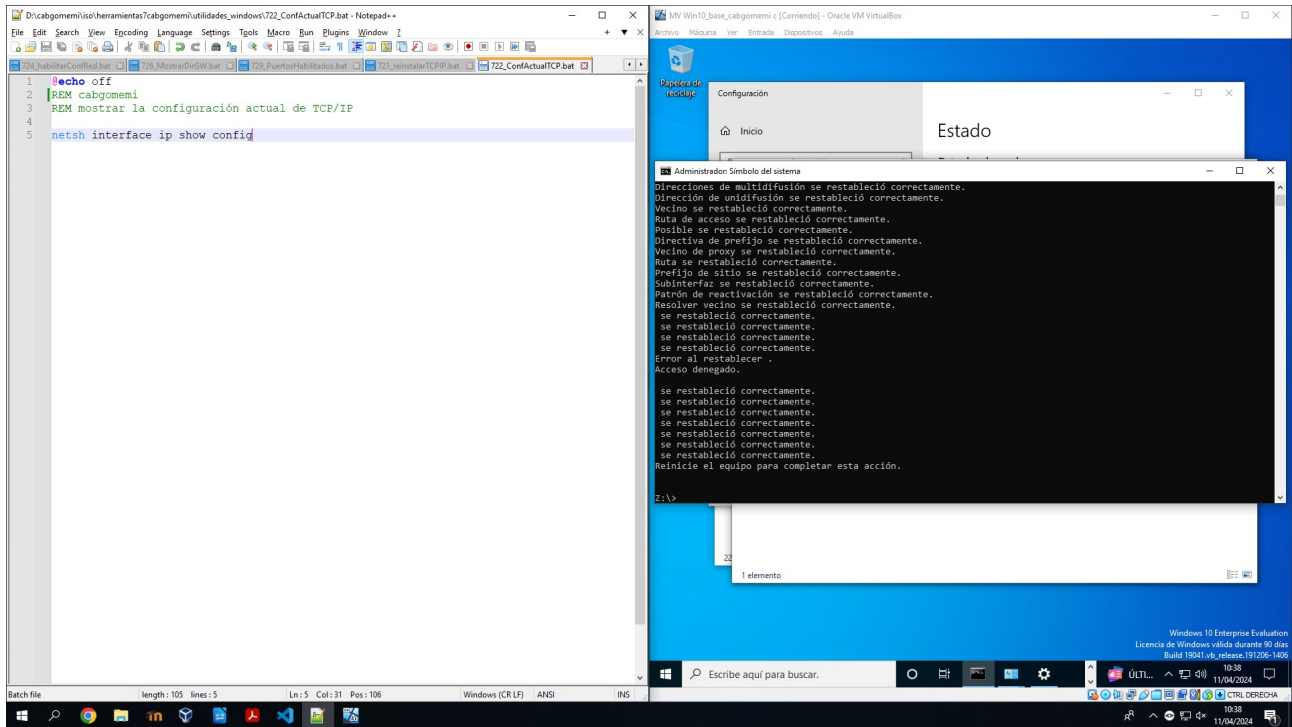


Ejecutamos el script.



722_ConfActualTCP

Editamos el script adecuadamente.



Ejecutamos el script.

