

RECOPILOCIÓN DE EVIDENCIAS VOLÁTILES EN WINDOWS



ERIC SERRANO MARÍN

ANÁLISIS FORENSE DE CIBERSEGURIDAD INFORMÁTICA I.E.S MARTINEZ MONTAÑES

INDICE

1. Indique, paso a paso, cómo realizaría una copia forense de los archivos volátiles de un sistema operativo Windows:	2
FTK Imager.....	2
Magnet RAM Capture.....	3
DumpIt.....	6
WinPmem.....	7
2. De una de las memorias RAM, guarde todas las palabras sacadas con el comando (strings (Linux) o strings.exe (Windows)) en un archivo llamado "archivoRAM.txt". De este archivo muestre todos los correos electrónicos existentes en la memoria RAM.	8
3. Mediante FTK Imager, capture las siguientes evidencias volátiles:	10
Ficheros del sistema: hiberful.sys, swapfile.sys, pagefile.sys	12
Ficheros de usuarios del sistema: NTUSER.DAT y UserClass.dat	12
Ficheros de logs del sistema operativo.....	13
Ficheros SAM, SECURITY, SOFTWARE y SYSTEM.....	14
Fichero \$MFT	15
Explicación de cada archivo/fichero:	16

1. INDIQUE, PASO A PASO, CÓMO REALIZARÍA UNA COPIA FORENSE DE LOS ARCHIVOS VOLÁTILES DE UN SISTEMA OPERATIVO WINDOWS:

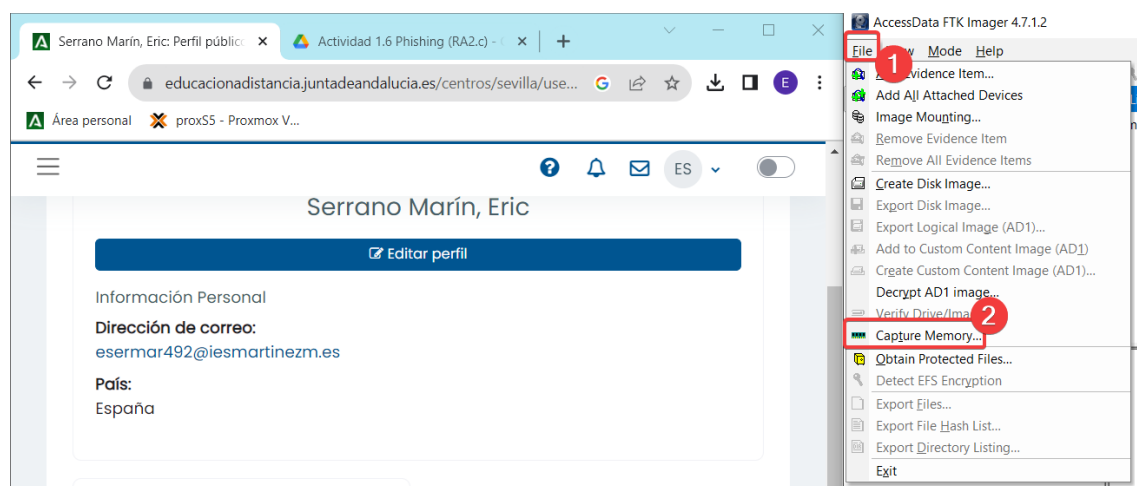
Memoria RAM (con 4 herramientas: FTK Imager, Magnet RAM Capture, DumpIt y alguna adicional)

FTK IMAGER.

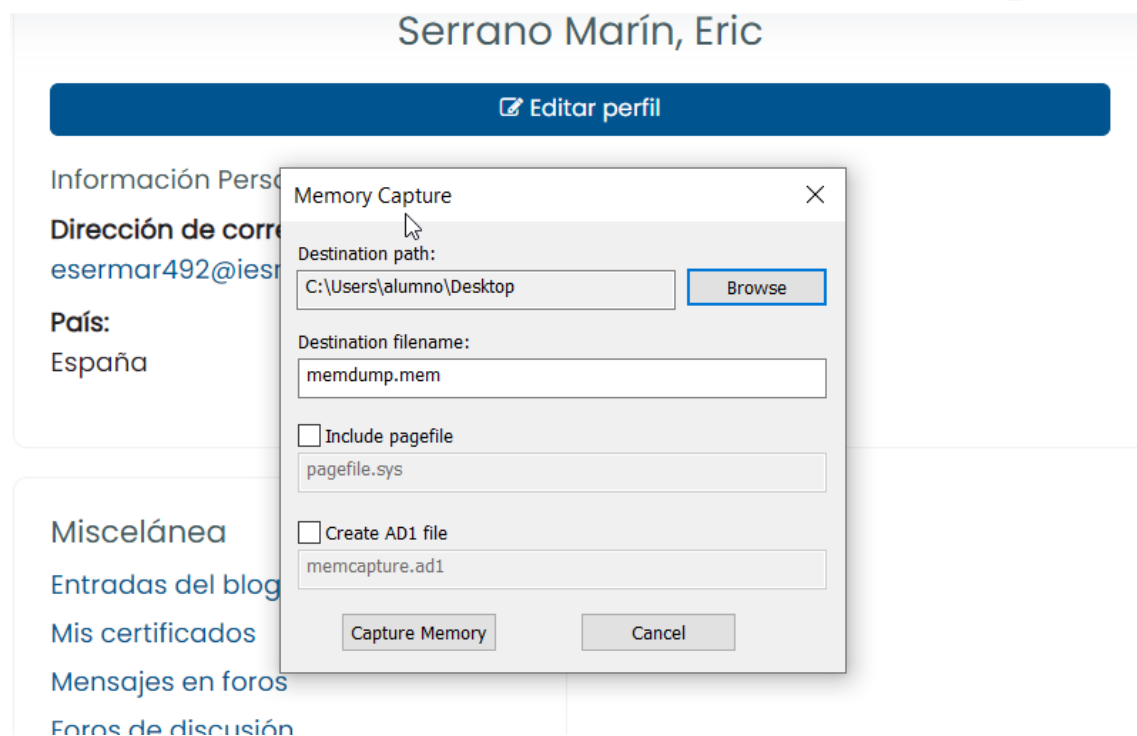
Instalaremos FTK Imager, no voy a poner el proceso, porque es todo siguiente, siguiente.

<https://www.exterro.com/ftk-imager>

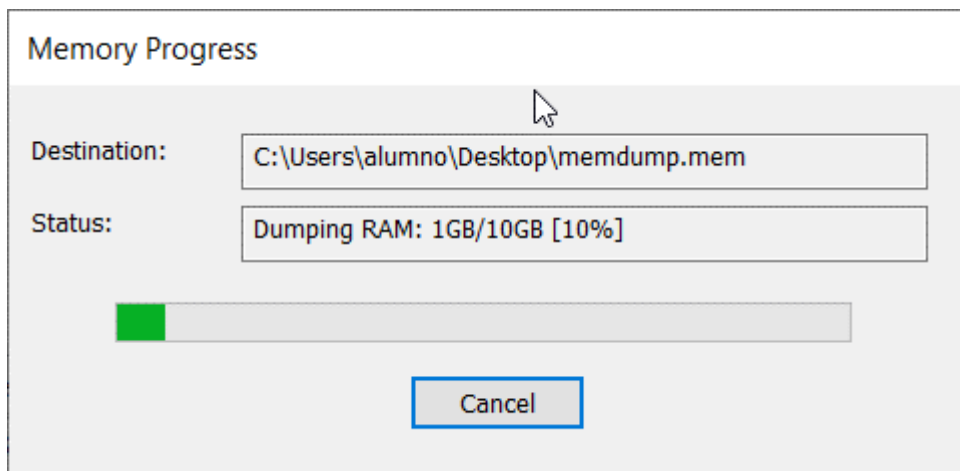
File -> Capture Memory.



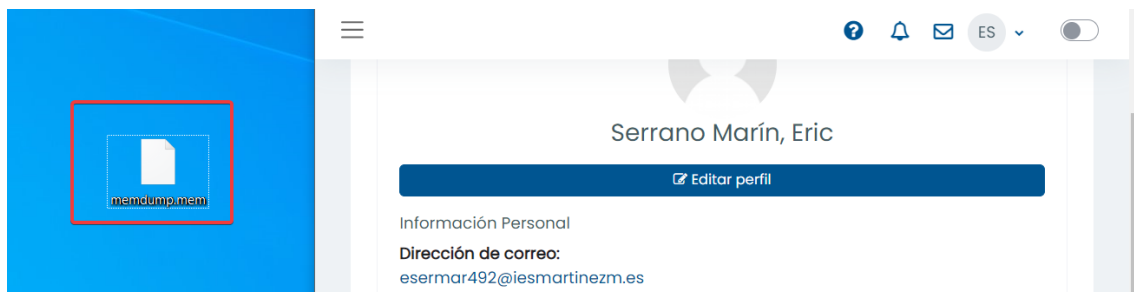
Vamos a decir que queremos que se nos guarde en el escritorio.



Y empezará el proceso.



Aquí podemos ver el archivo en la ruta que hemos seleccionado (Desktop).

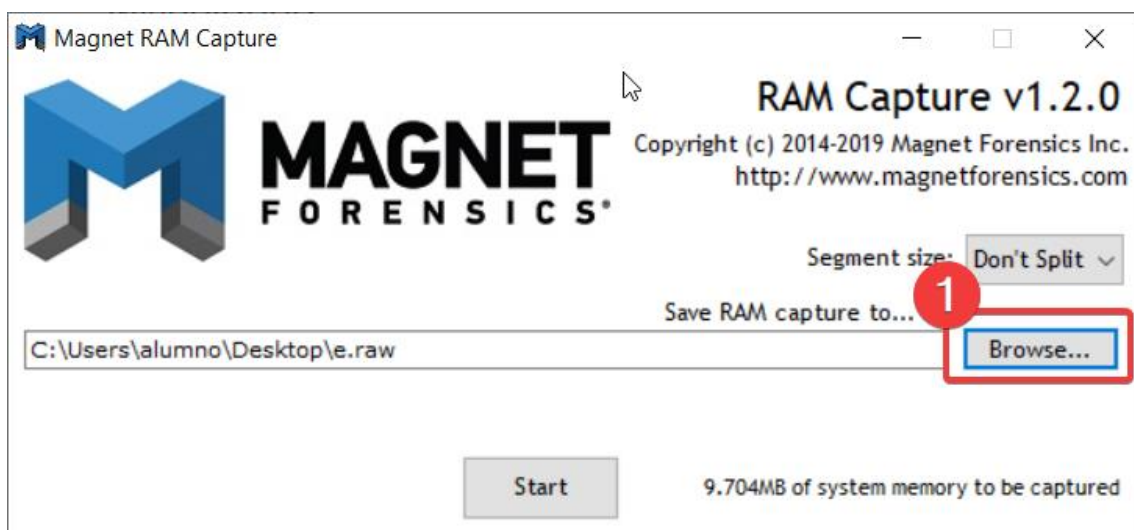


MAGNET RAM CAPTURE.

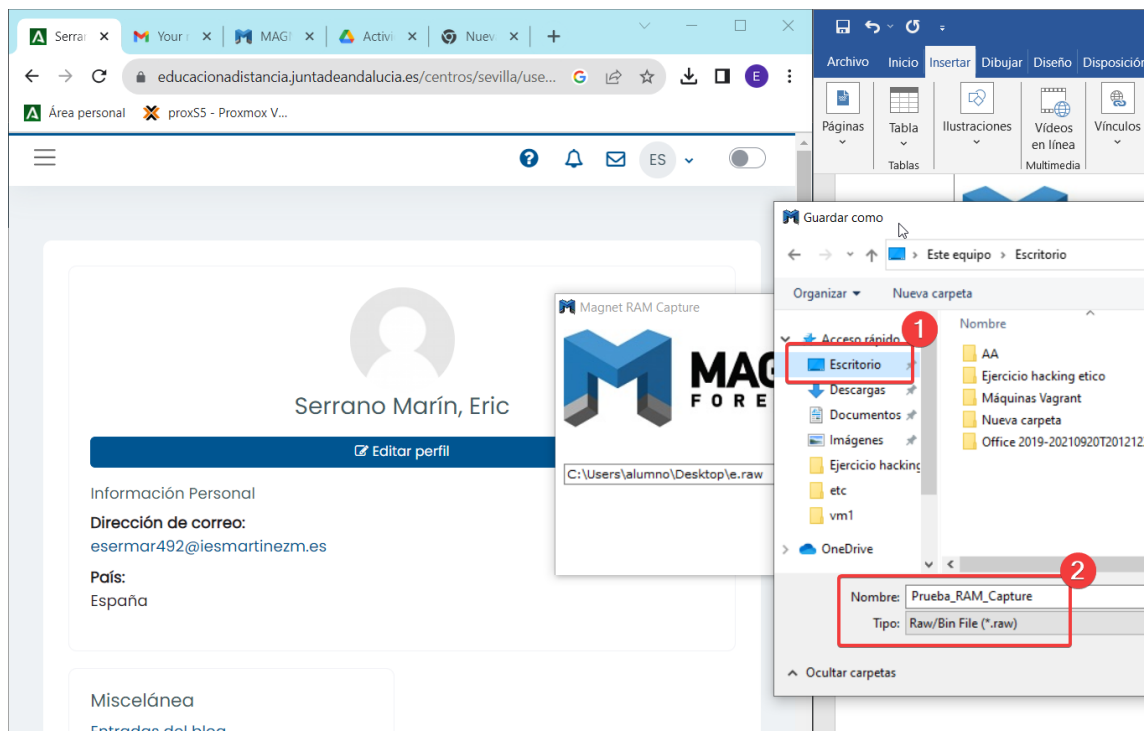
Para poder descargar el archivo hay que poner tu correo electrónico y te lo mandan. No hay nada raro al hacer la instalación, todo es muy fácil, así que no voy a poder capturas.

<https://www.magnetforensics.com/resources/magnet-ram-capture/>

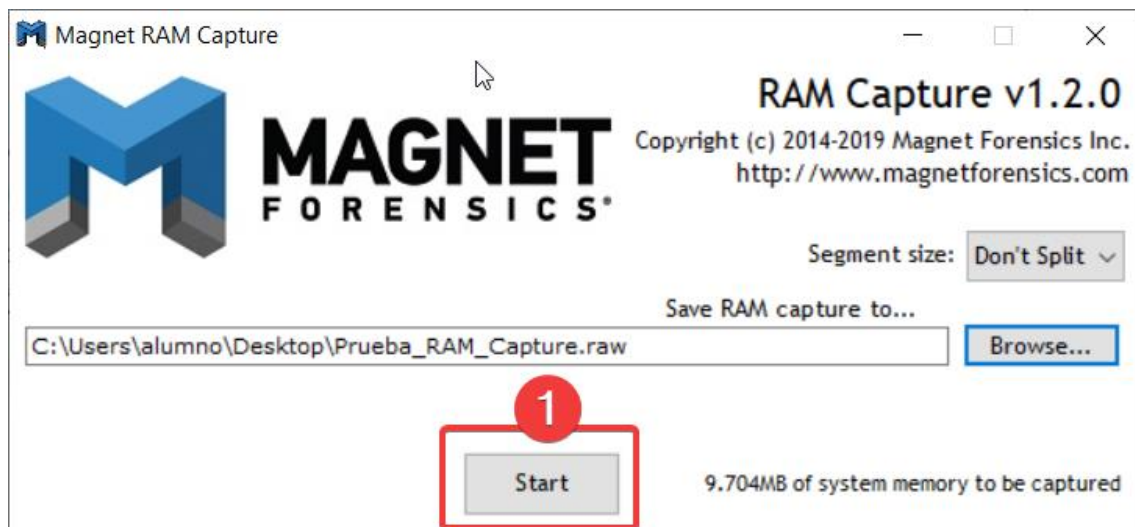
Una vez descargado y ejecutado, haremos clic en Browse, para elegir donde queremos que se nos guarde el archivo.



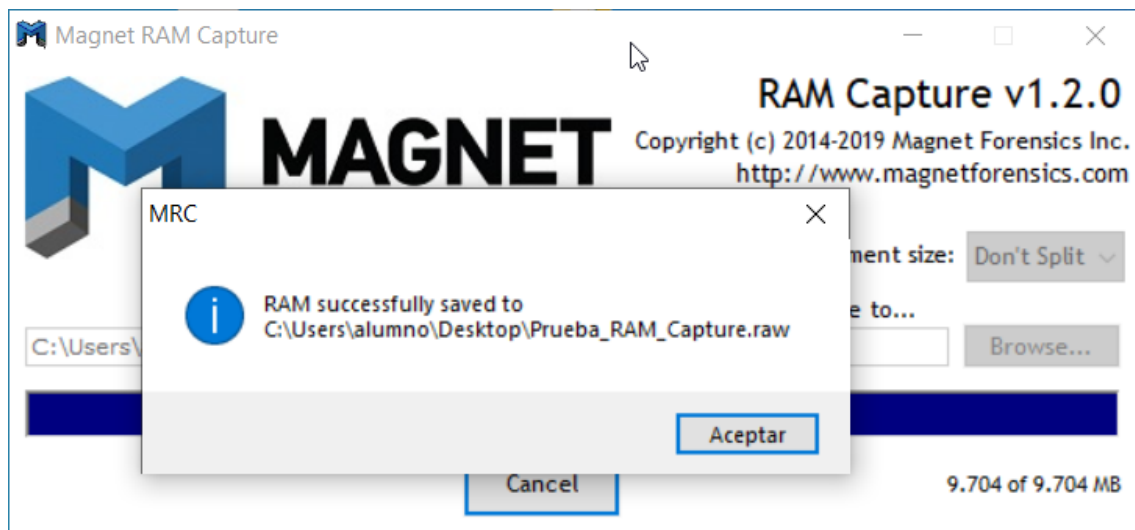
Ahora pondremos el nombre que queremos que tenga.



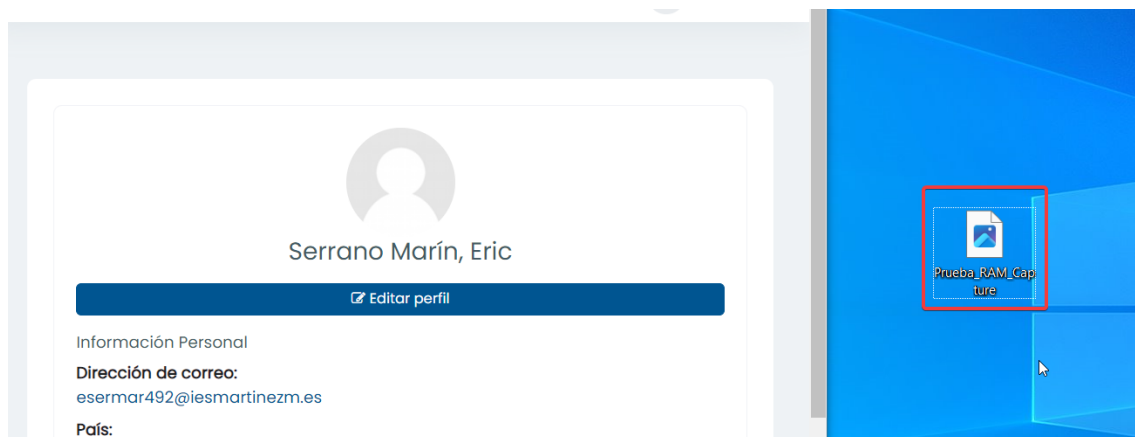
Y pulsaremos en Start.



Como podemos observar, ya ha acabado.



Y ya tenemos nuestro archivo en el escritorio.

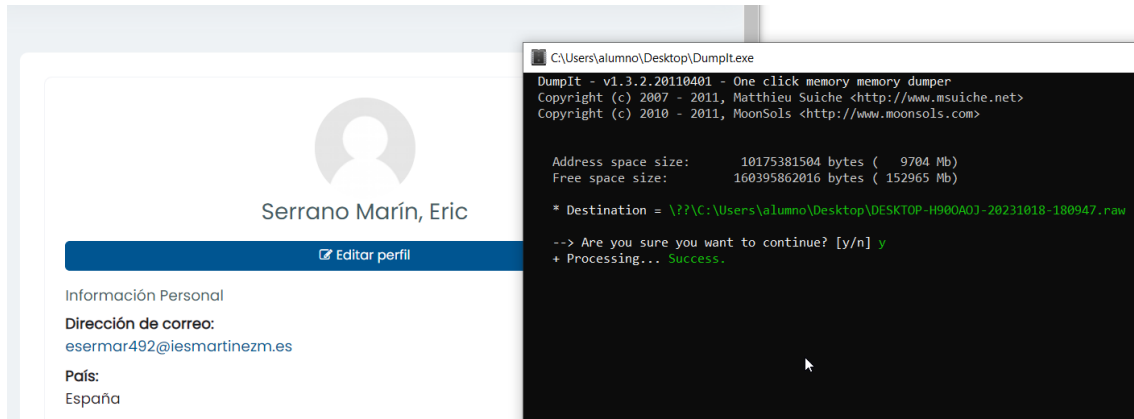


DUMPIT.

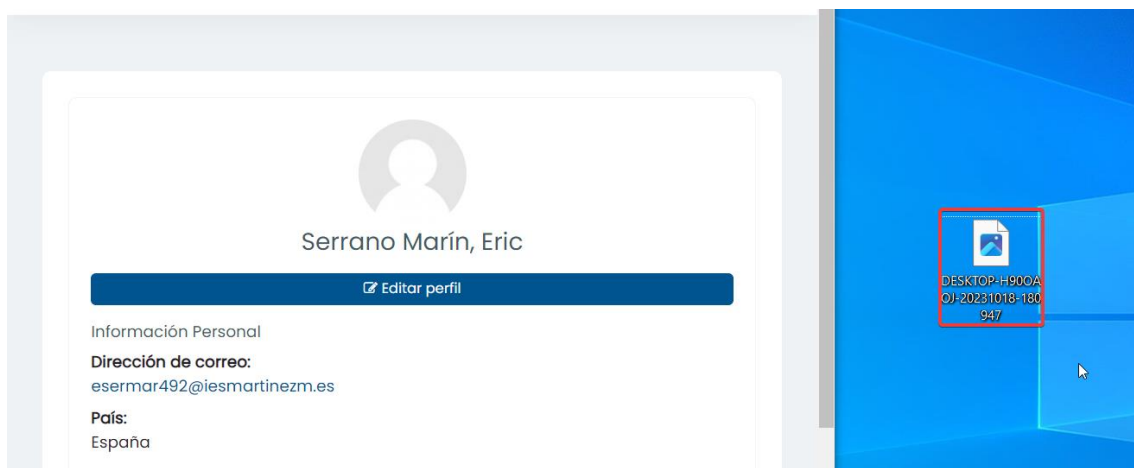
<https://www.toolwar.com/2014/01/dumpit-memory-dump-tools.html>

Solo tenemos que descargar el archivo, ejecutarlo y se nos abrirá la cmd.

Solo tendremos que decirle “y”, el archivo se nos guardará al lado de donde esté el ejecutable, en este caso en el escritorio.



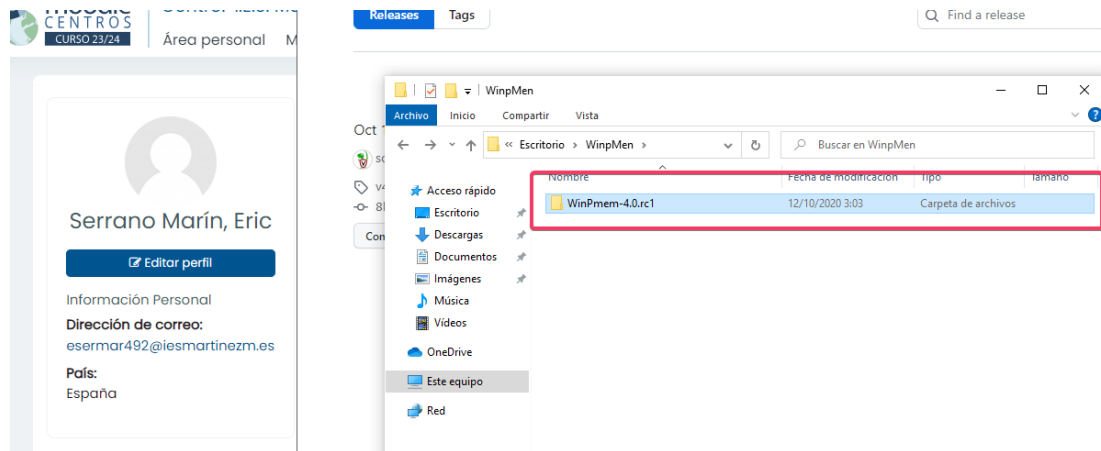
Aquí tenemos el archivo en el escritorio.



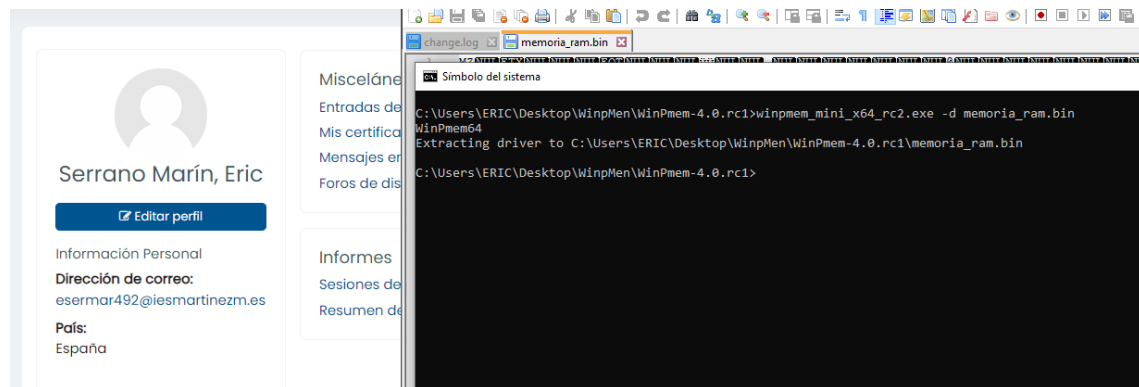
WINPMEM.

Descargaremos de github y descomprimiremos el archivo.

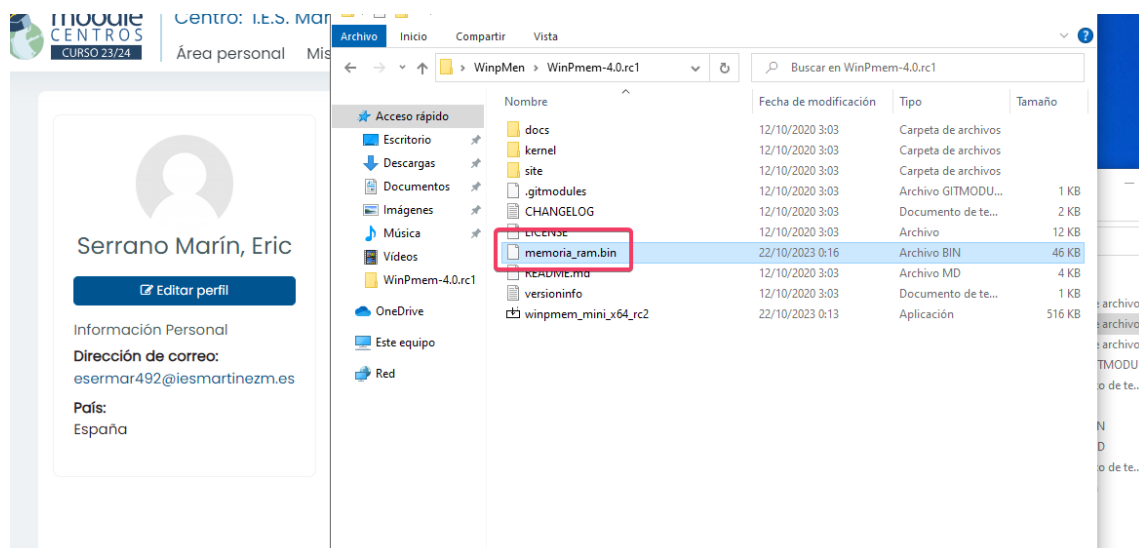
<https://github.com/Velocidex/WinPmem/releases>



Entraremos en la carpeta donde hemos hecho la extracción y pondremos lo siguiente.



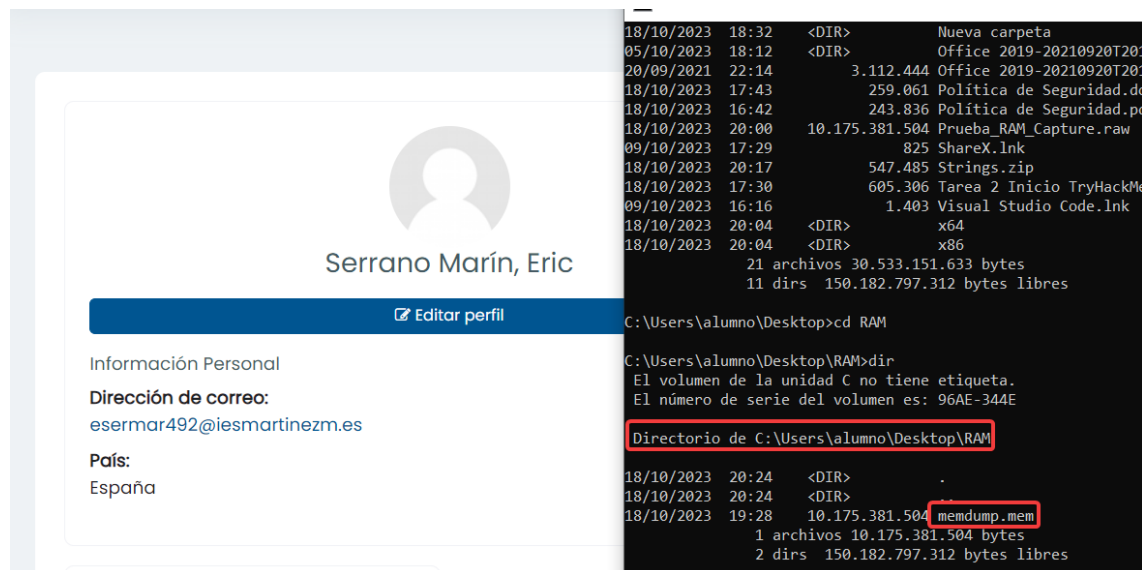
Aquí podemos encontrar el archivo.



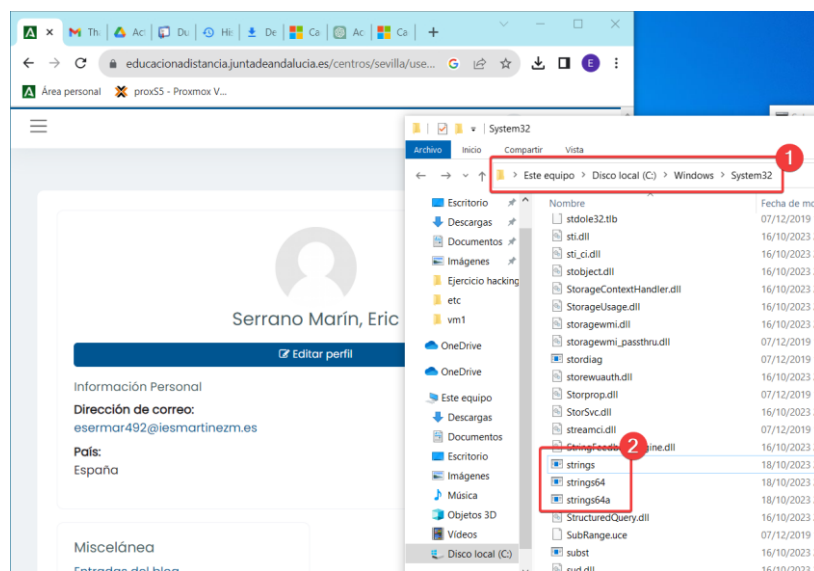
2. DE UNA DE LAS MEMORIAS RAM, GUARDE TODAS LAS PALABRAS SACADAS CON EL COMANDO (STRINGS (LINUX) O STRINGS.EXE (WINDOWS)) EN UN ARCHIVO LLAMADO "ARCHIVORAM.TXT". DE ESTE ARCHIVO MUESTRE TODOS LOS CORREOS ELECTRÓNICOS EXISTENTES EN LA MEMORIA RAM.

He descargado strings.exe en el siguiente enlace: <https://learn.microsoft.com/es-es/sysinternals/downloads/strings>.

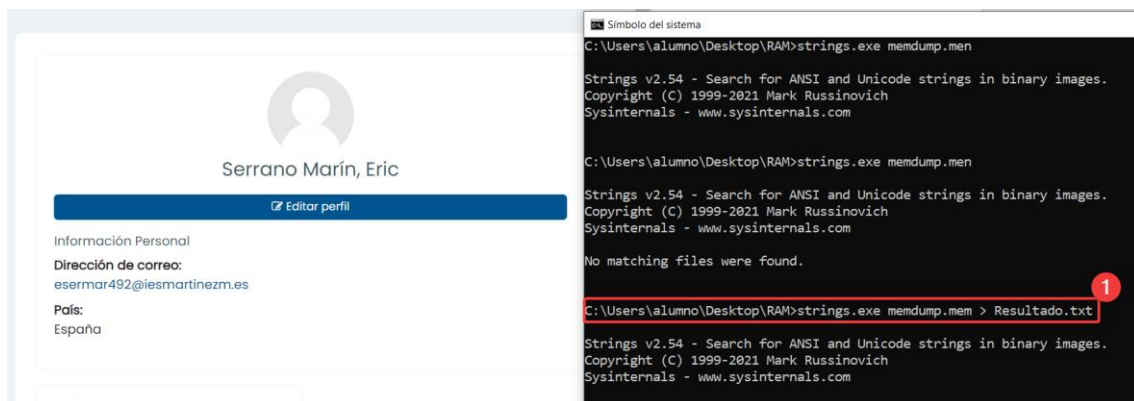
Vamos a entrar a la cmd y vamos a ir a la ruta donde tenemos el archivo RAM (en mi caso C:\Users\alumno\Desktop\RAM).



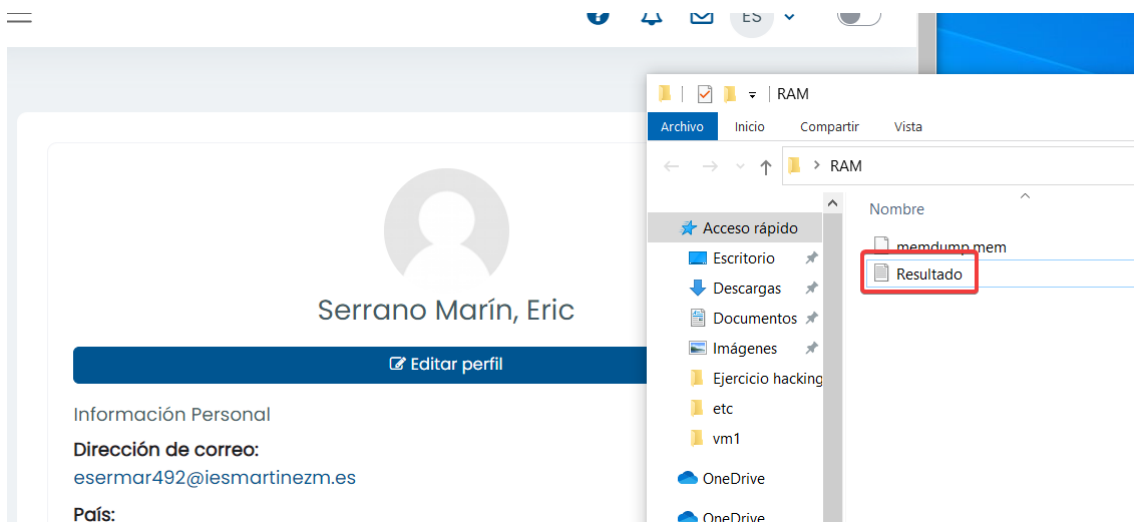
He descomprimido strings.exe en system32 con se puede observar en la captura.



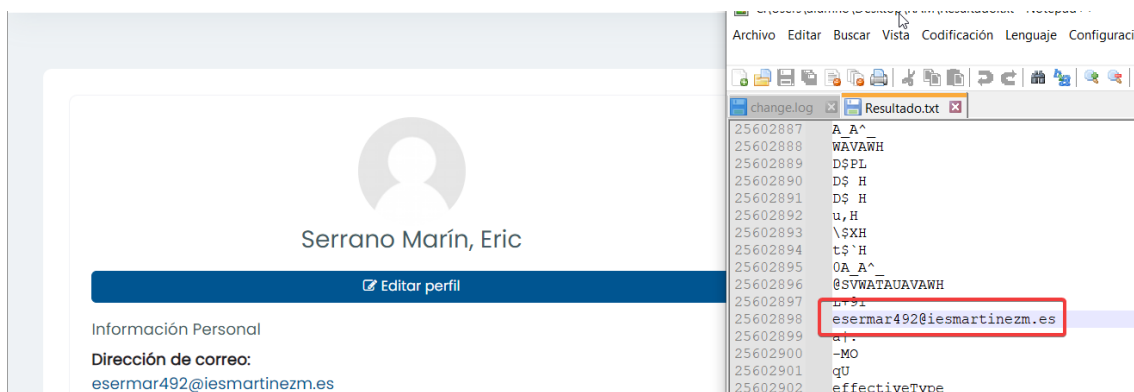
Ahora ejecutaremos el siguiente comando (strings.exe + [nombre_archivo_memoria] + > [futuro_nombre_archivo.txt])



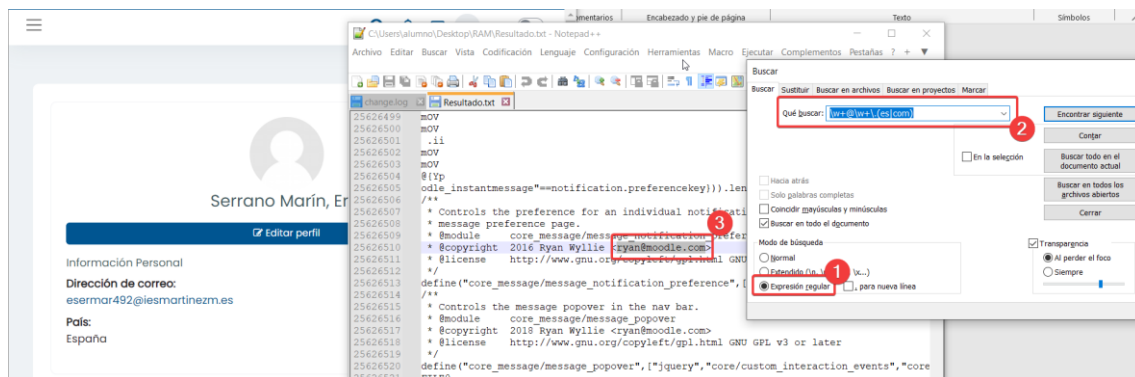
Ya nos ha creado el .txt.



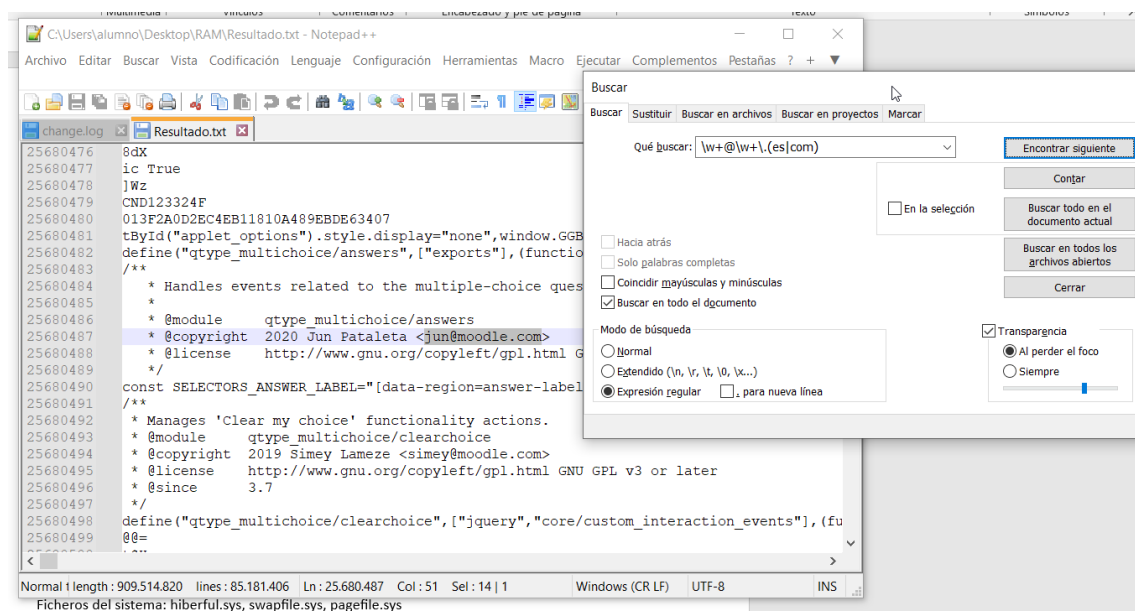
Vamos a entrar con el Notepad++, y vamos a buscar @ies pulsando Ctr+F. Obviamente busco @ies porque sé que es mi correo y va a aparecer.



Ahora estoy buscando usando expresiones regulares, he encontrado lo siguiente.

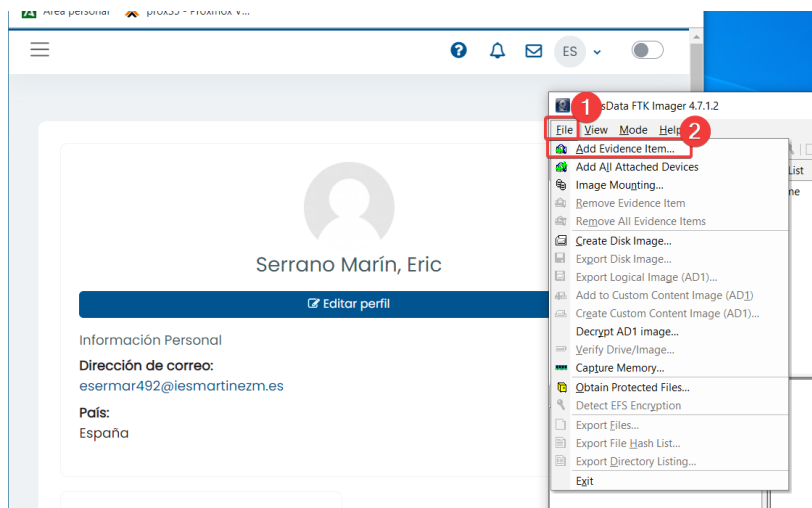


Aquí tenemos otro más.

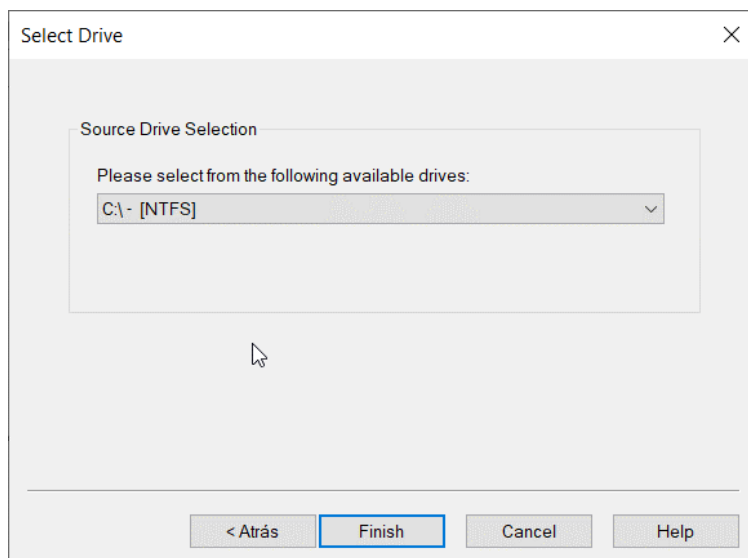
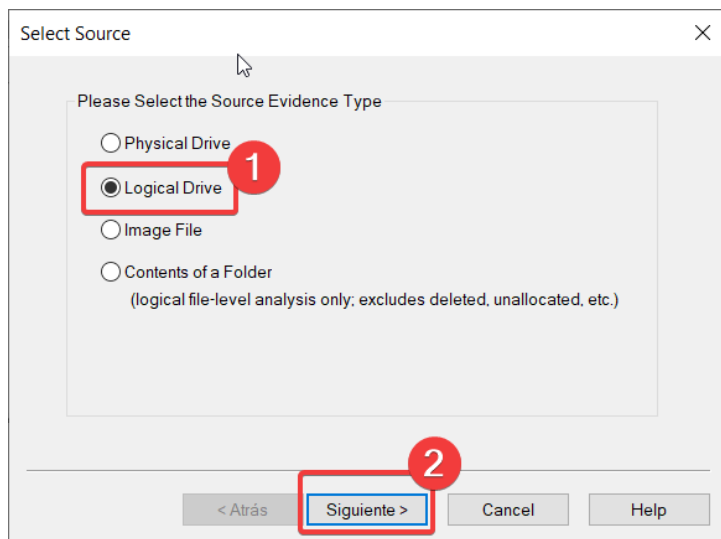


3. MEDIANTE FTK IMAGER, CAPTURA LAS SIGUIENTES EVIDENCIAS VOLÁTILES:

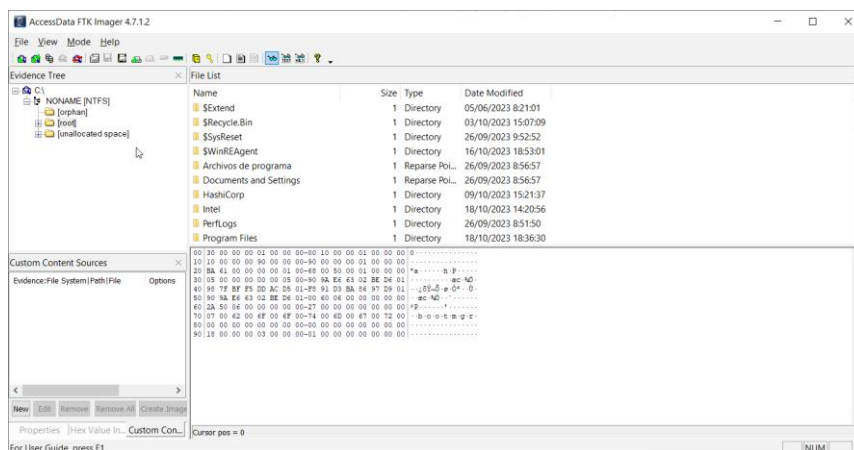
File -> Add Evidente Item..



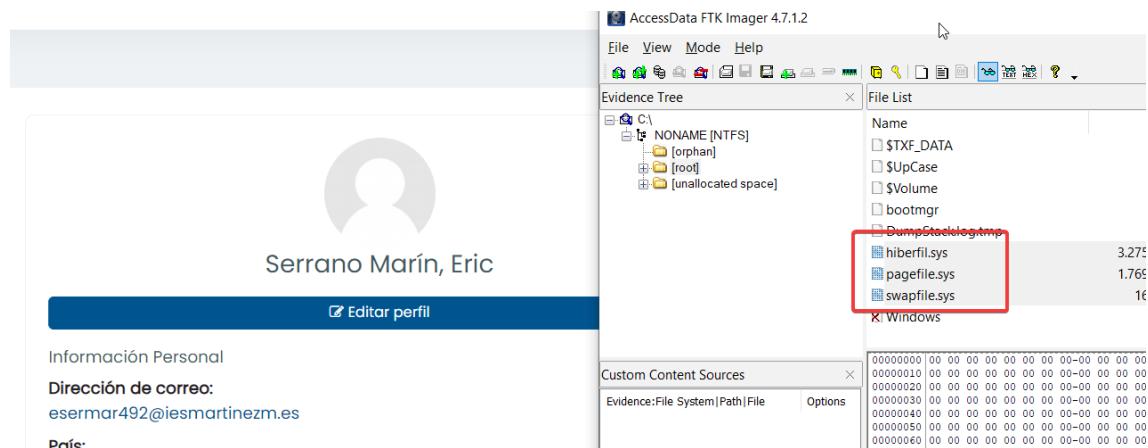
Seleccionaremos Logical Drive, ya que queremos solo C:\



Y ahora ya podemos empezar a buscar.



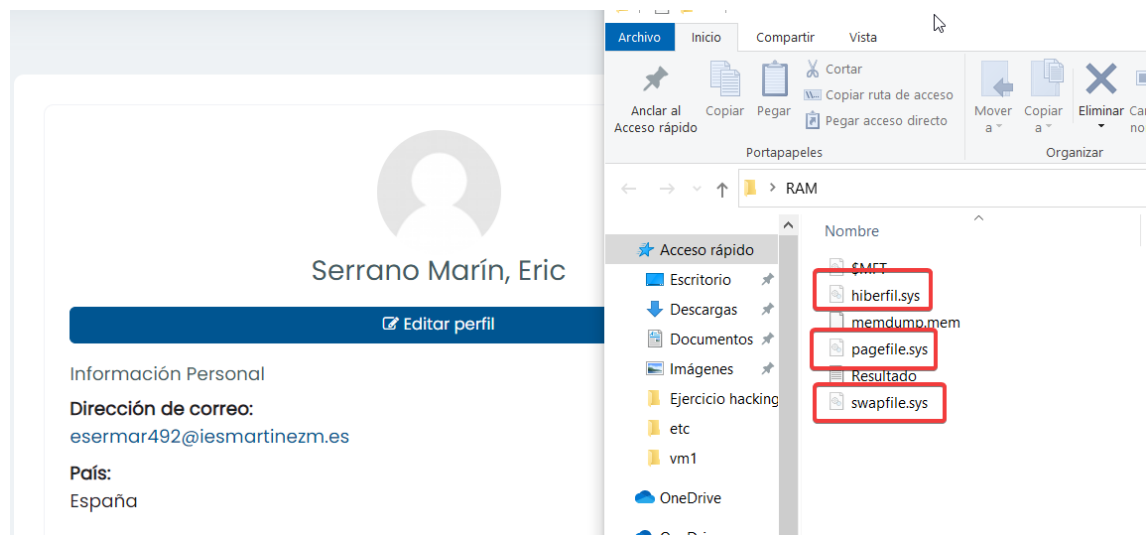
FICHEROS DEL SISTEMA: HIBERFUL.SYS, SWAPFILE.SYS, PAGEFILE.SYS



The image shows a user profile for Eric Serrano Marín on the left and the AccessData FTK Imager 4.7.1.2 interface on the right. The FTK Imager shows a file list with the following entries:

Name	Size
\$TXF_DATA	
\$UpCase	
\$Volume	
bootmgr	
DumpStacklog.tmp	
hiberfil.sys	3.275
pagefile.sys	1.769
swapfile.sys	16

The files hiberfil.sys, pagefile.sys, and swapfile.sys are highlighted with a red box.

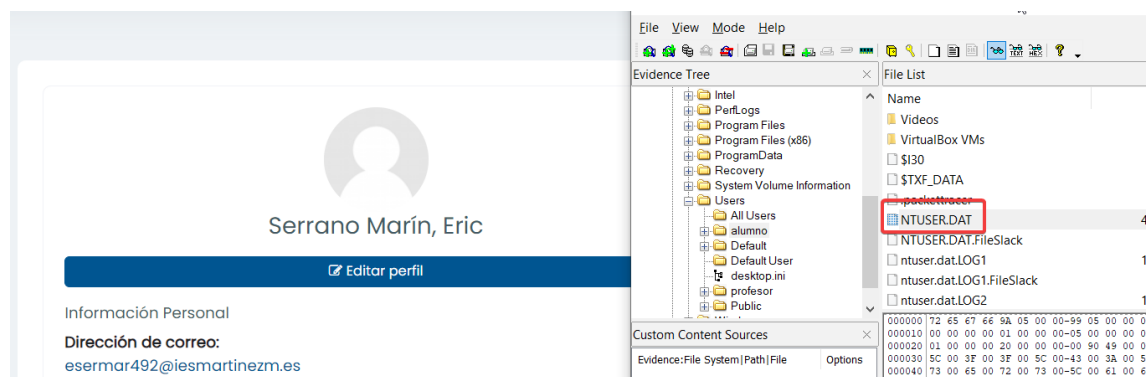


The image shows a user profile for Eric Serrano Marín on the left and a Windows File Explorer window on the right. The File Explorer shows the contents of the RAM drive, with the following files listed:

Nombre
\$MFT
hiberfil.sys
memdump.mem
pagefile.sys
Resultado
swapfile.sys

The files hiberfil.sys, pagefile.sys, and swapfile.sys are highlighted with a red box.

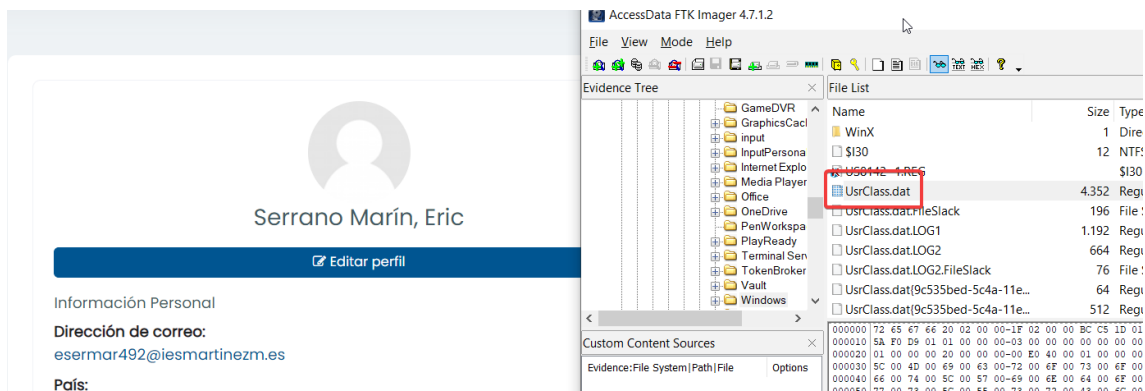
FICHEROS DE USUARIOS DEL SISTEMA: NTUSER.DAT Y USRCLASS.DAT



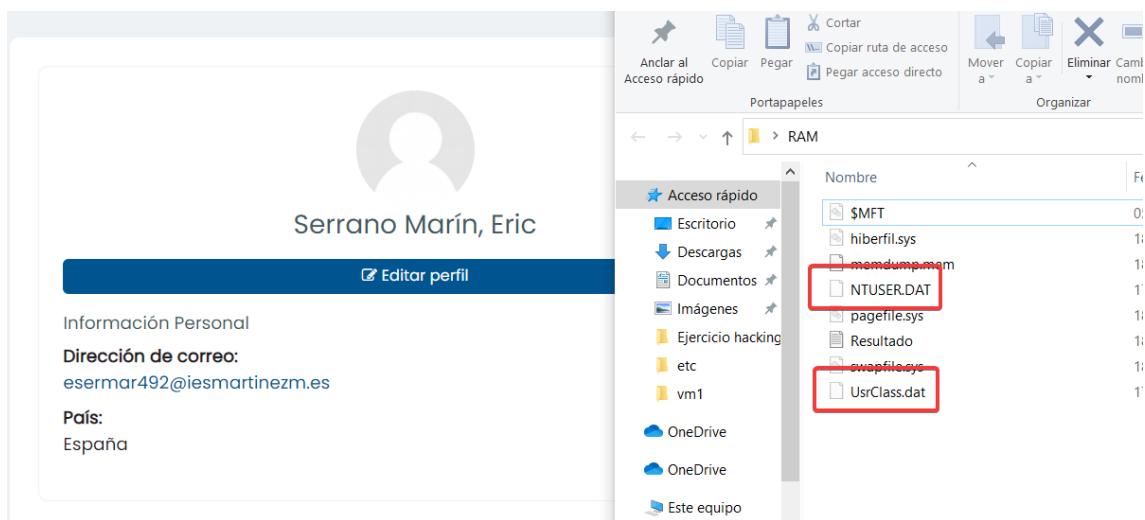
The image shows a user profile for Eric Serrano Marín on the left and the AccessData FTK Imager 4.7.1.2 interface on the right. The FTK Imager shows a file list with the following entries:

Name	Size
Videos	
VirtualBox VMs	
\$130	
\$TXF_DATA	
hiberfil.sys	
NTUSER.DAT	4
NTUSER.DAT.FileSlack	
ntuser.dat.LOG1	1
ntuser.dat.LOG1.FileSlack	
ntuser.dat.LOG2	1

The file NTUSER.DAT is highlighted with a red box.

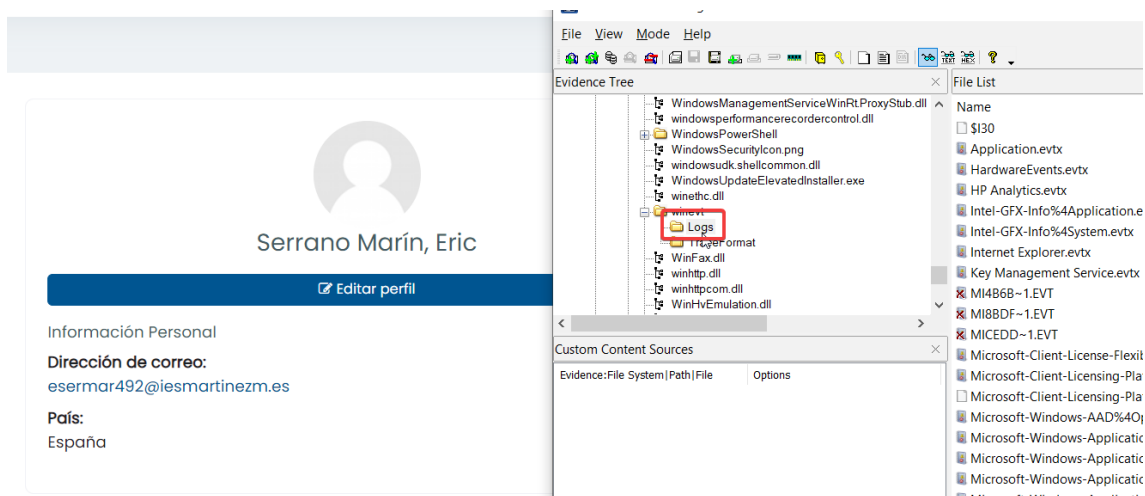


Aquí tenemos ambos archivos

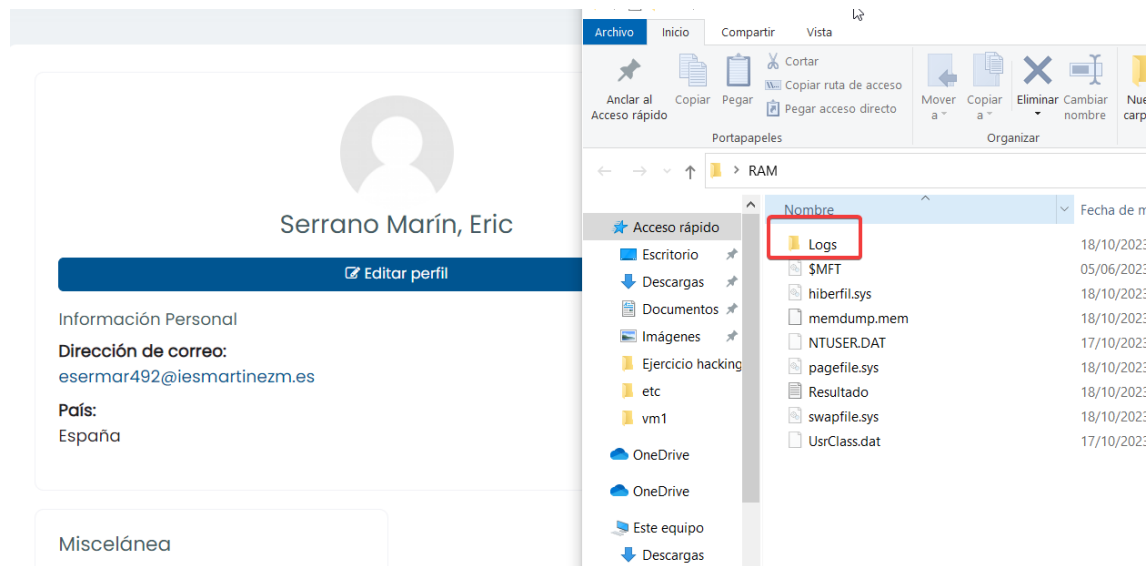


FICHEROS DE LOGS DEL SISTEMA OPERATIVO.

Ubicación: C:\Windows\System32\winevt\Logs

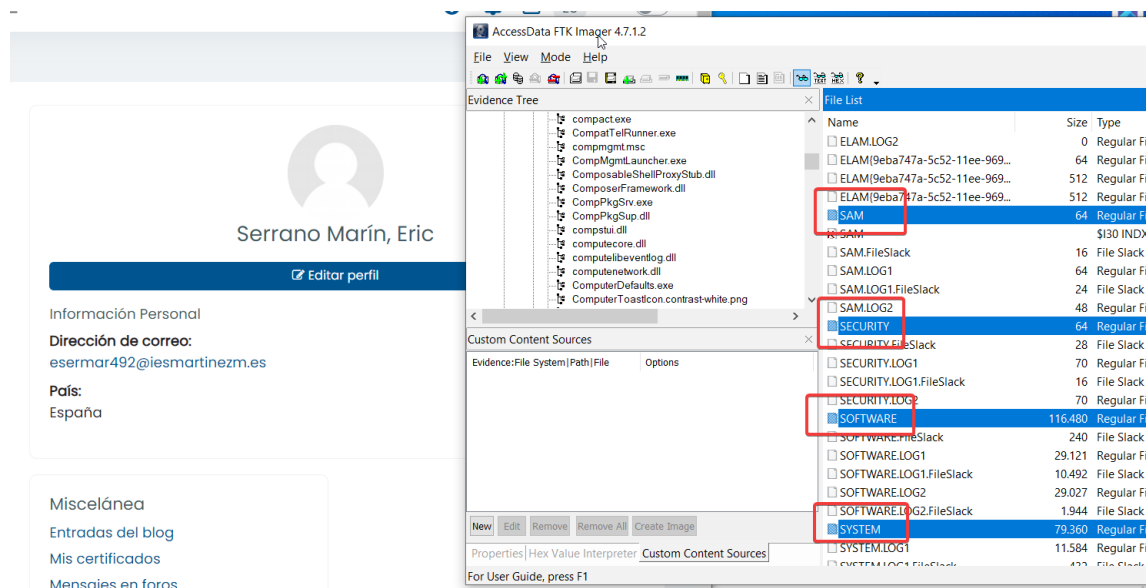


Ya tenemos Logs exportado en la carpeta.

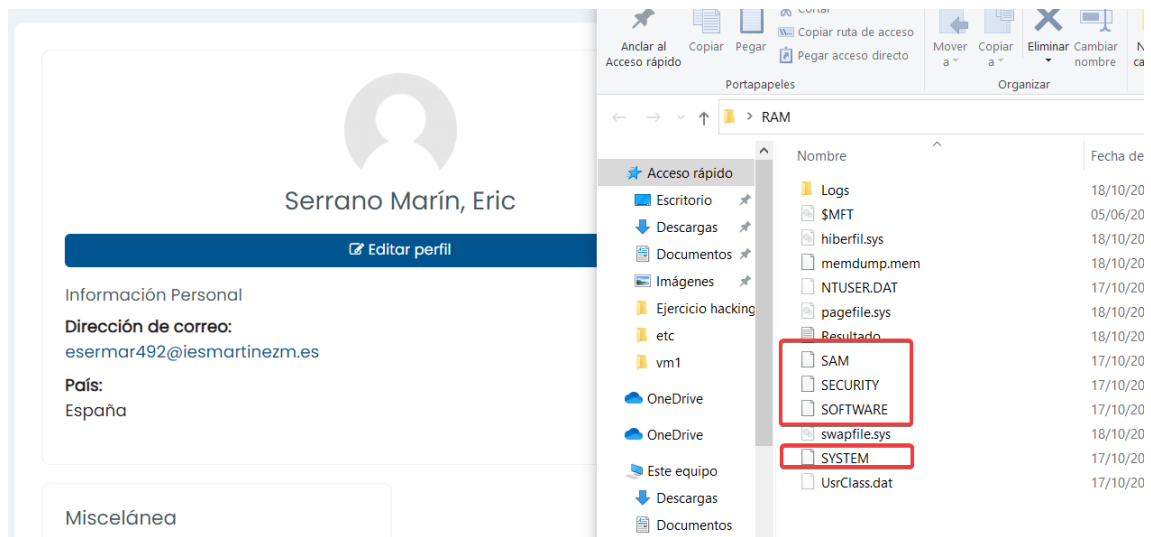


FICHEROS SAM, SECURITY, SOFTWARE Y SYSTEM

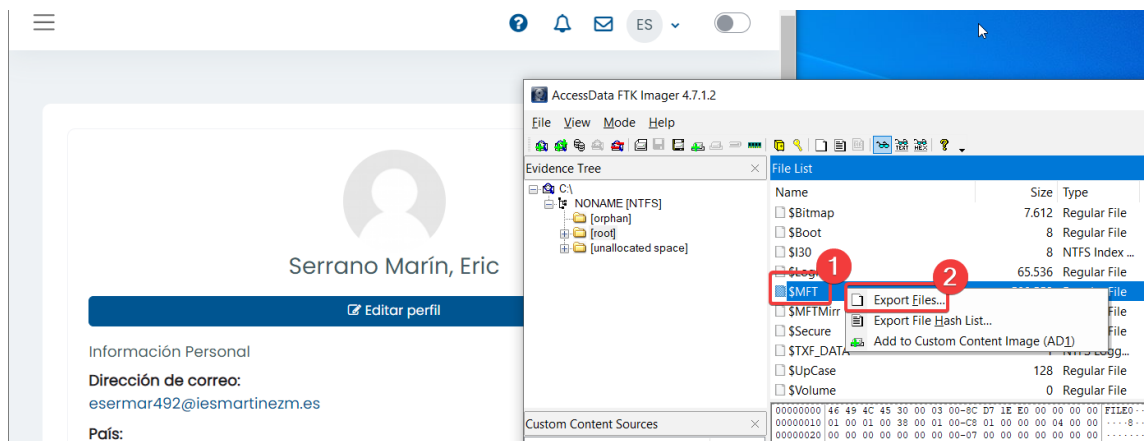
- SAM: %SystemRoot%\system32\config\SAM
- SECURITY: %SystemRoot%\system32\config\SECURITY
- SOFTWARE: %SystemRoot%\system32\config\SOFTWARE
- SYSTEM: %SystemRoot%\system32\config\SYSTEM



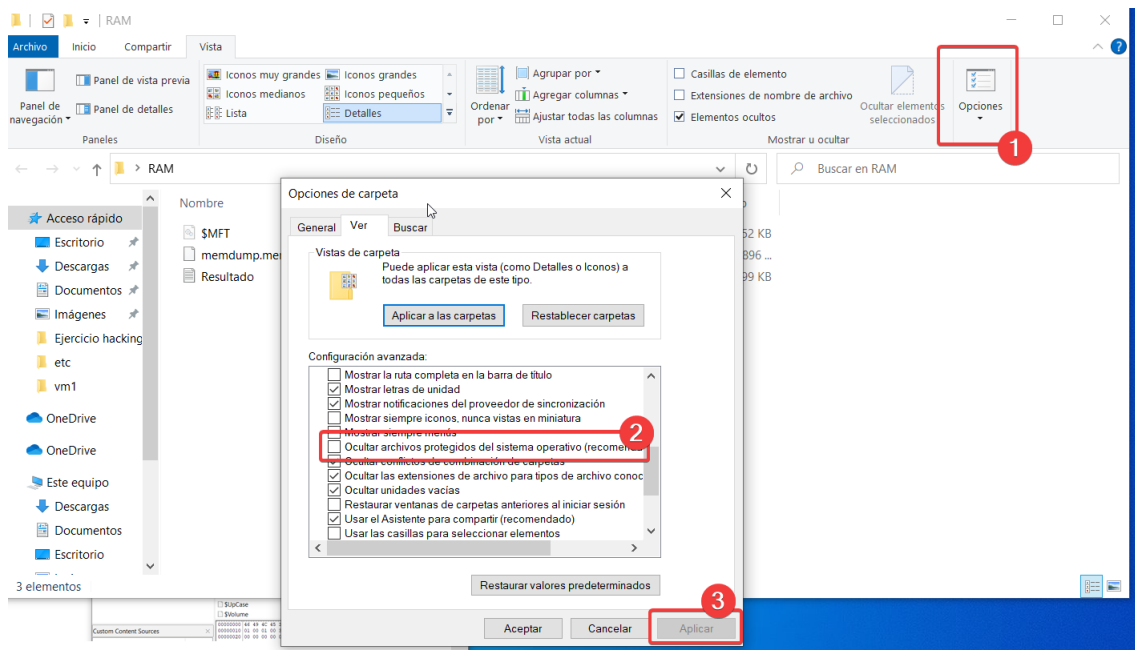
Aquí tenemos los archivos exportados.



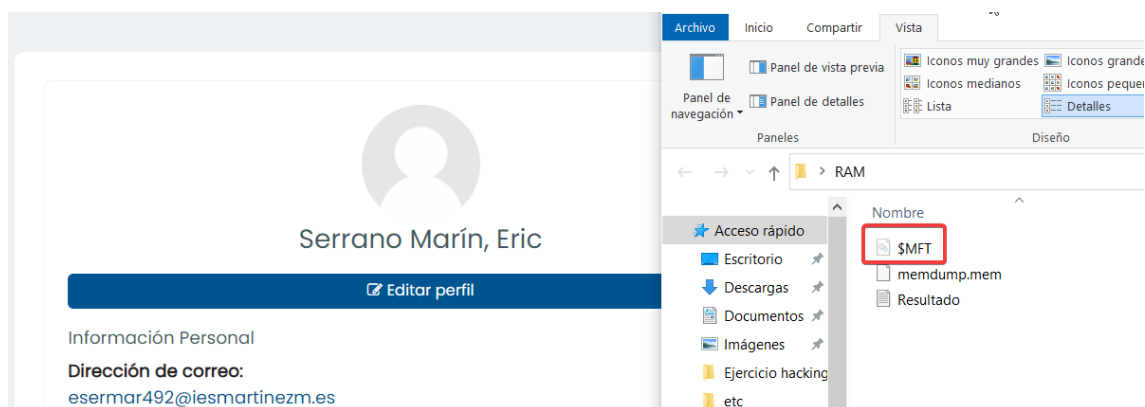
FICHERO \$MFT



Para poder ver el archivo que hemos guardado (lo he guardado en la carpeta RAM, que he estado usando durante toda la práctica)



Ya podemos ver el archivo.



EXPLICACIÓN DE CADA ARCHIVO/FICHERO:

Ntuser.dat y **usrclass.dat**: **ntuser.dat** contiene la configuración específica del registro para el usuario, y **usrclass.dat** almacena configuraciones relacionadas con las clases de objetos y extensiones de Shell.

SAM (Security Account Manager): Contiene información sobre cuentas de usuario y contraseñas en un sistema Windows. Es crucial para la autenticación de usuarios.

SECURITY: Almacena la información de políticas de seguridad, como permisos y políticas de auditoría, utilizada para controlar el acceso a recursos del sistema.

SOFTWARE: Contiene configuraciones de software y aplicaciones instaladas en el sistema, incluyendo información del registro y ajustes específicos de programas.

SYSTEM: Almacena la configuración y la información del registro relacionada con el hardware y controladores del sistema. Es esencial para el funcionamiento adecuado del sistema operativo.

\$MFT: Es parte de la estructura del sistema de archivos NTFS y contiene información sobre todos los archivos y directorios en una unidad, incluyendo su ubicación en el disco y metadatos esenciales.