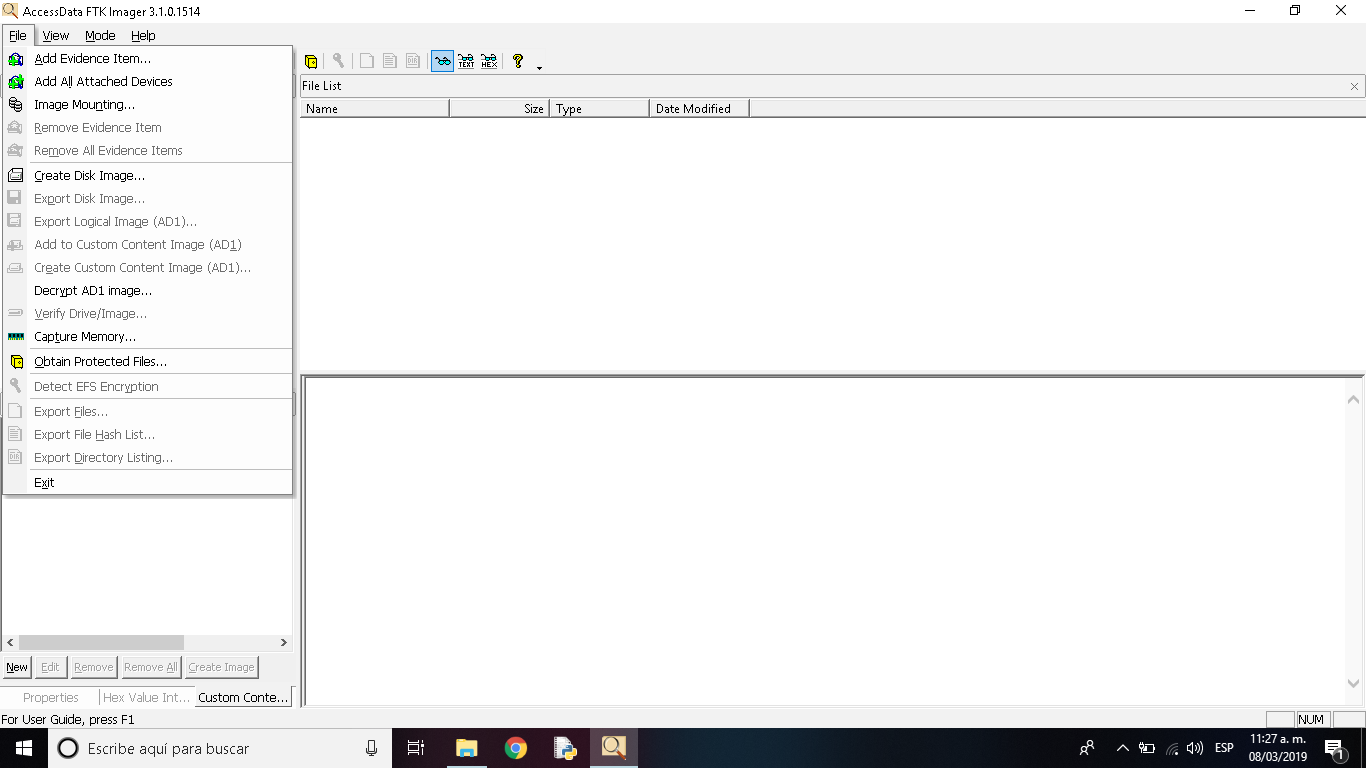
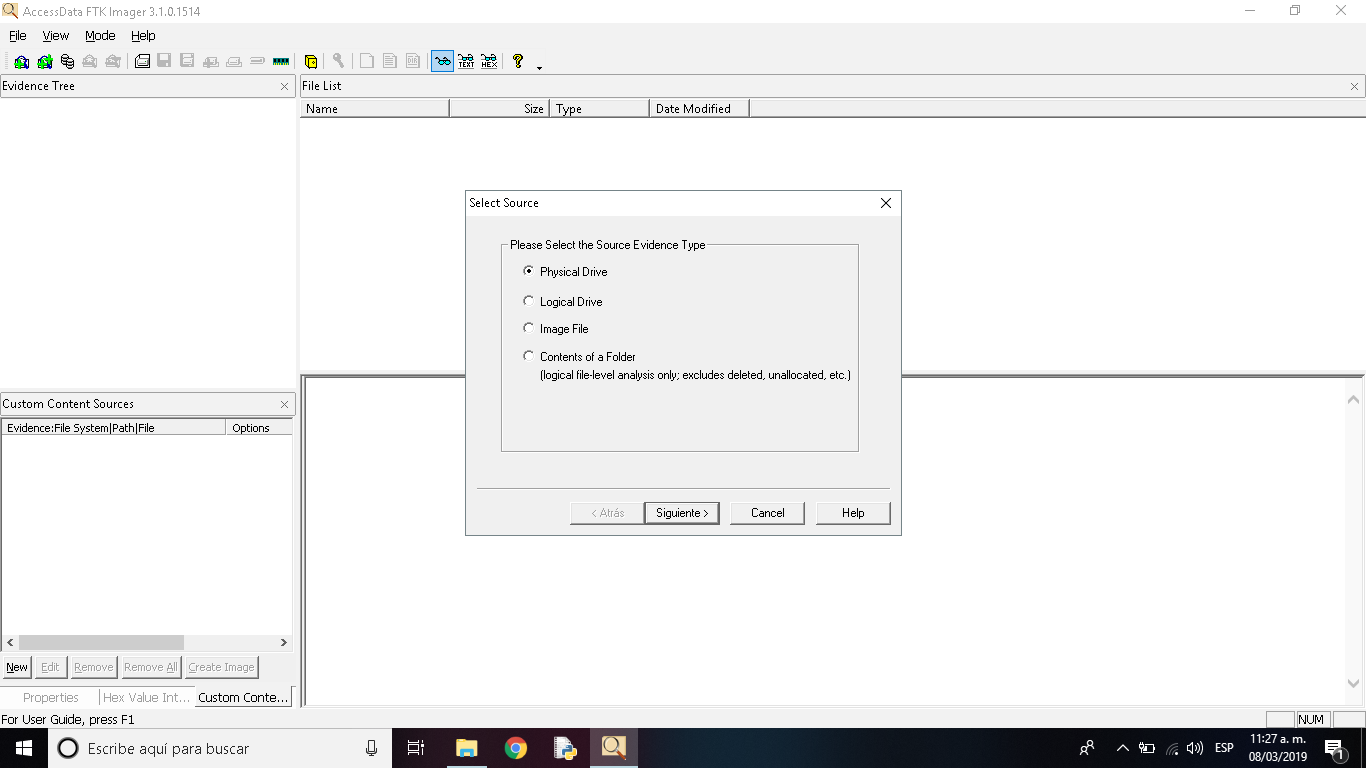
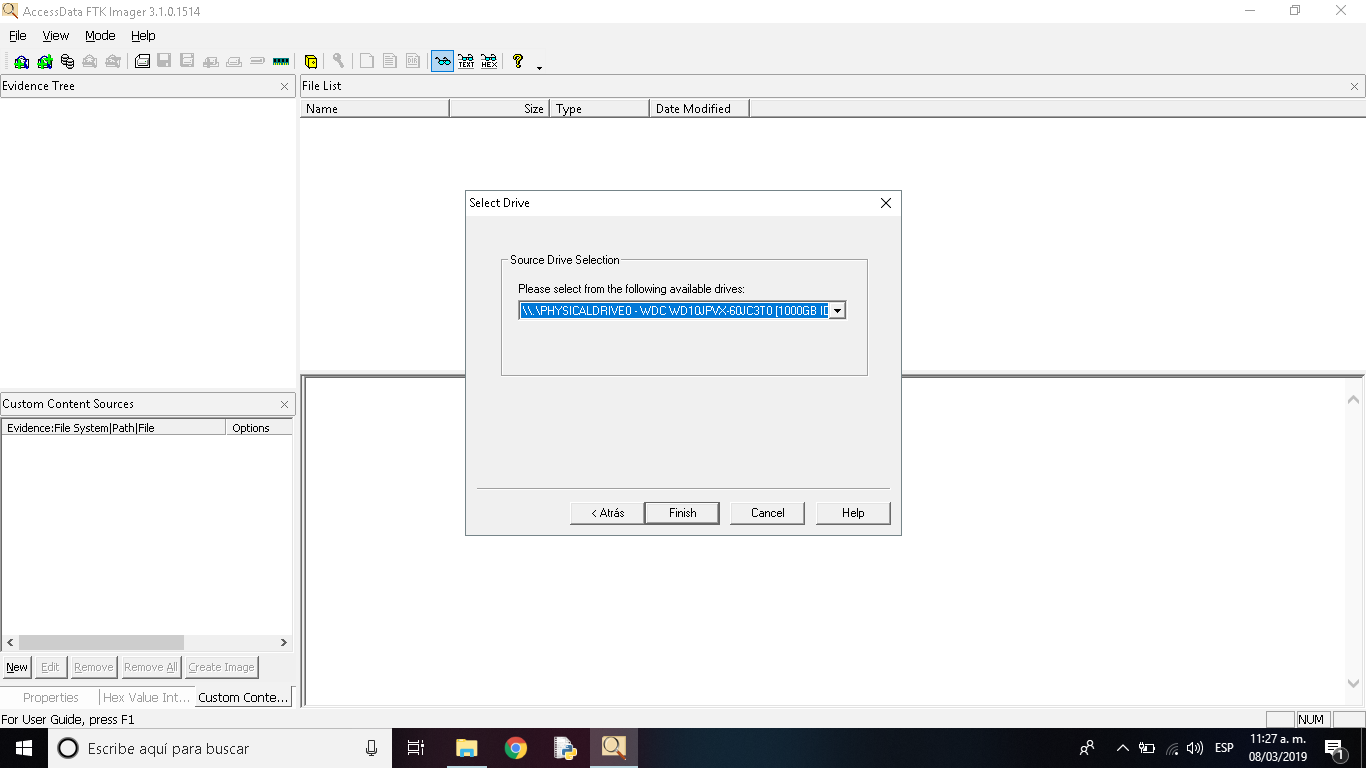
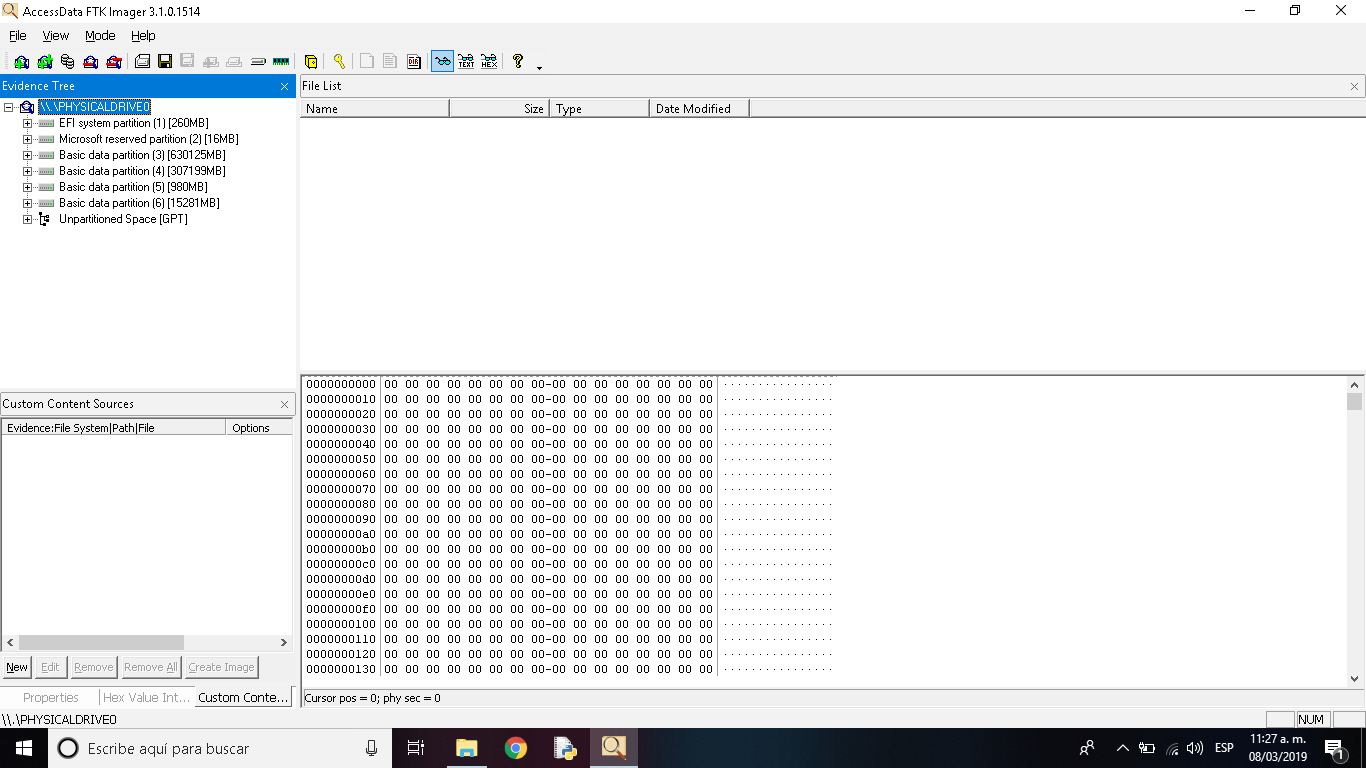
Iniciamos con el programa AccessData FTK para extraer una copia de los archivos



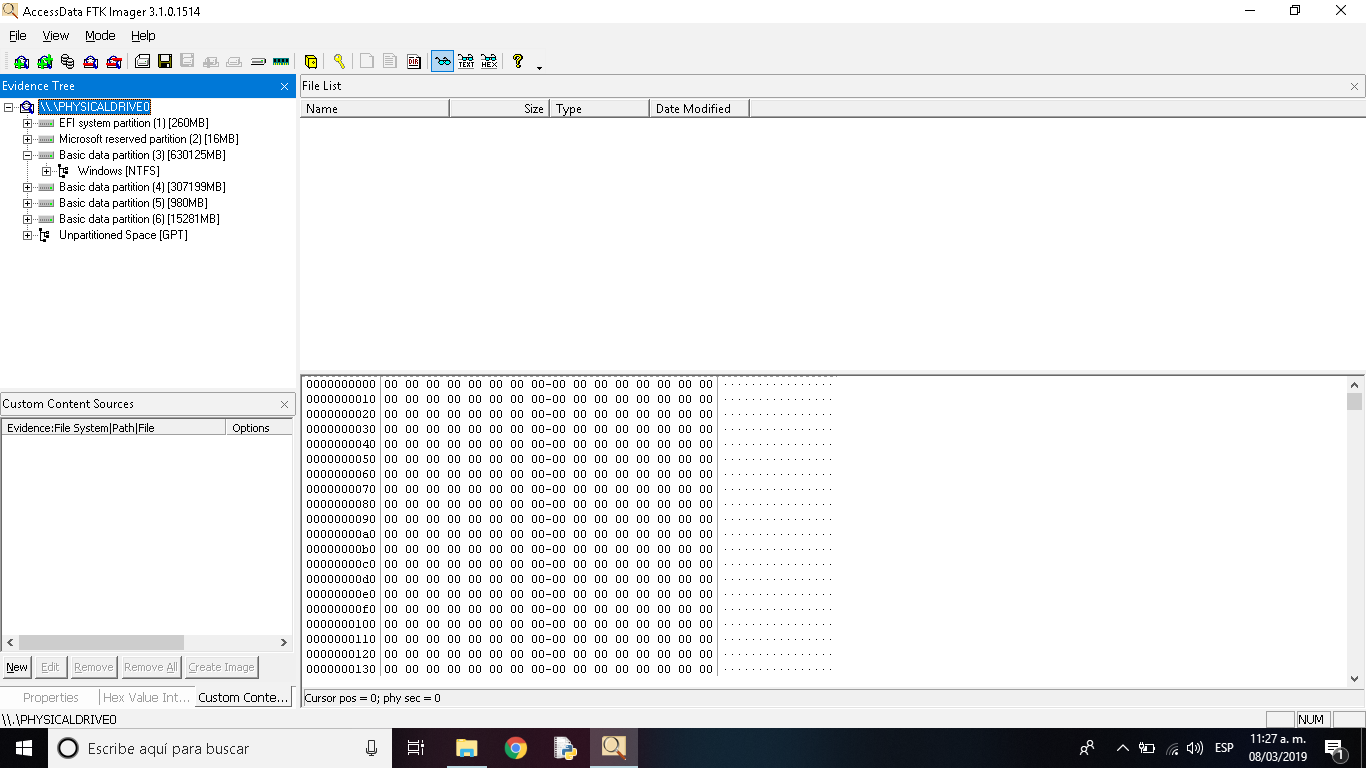
Vamos agregar la evidencia del equipo



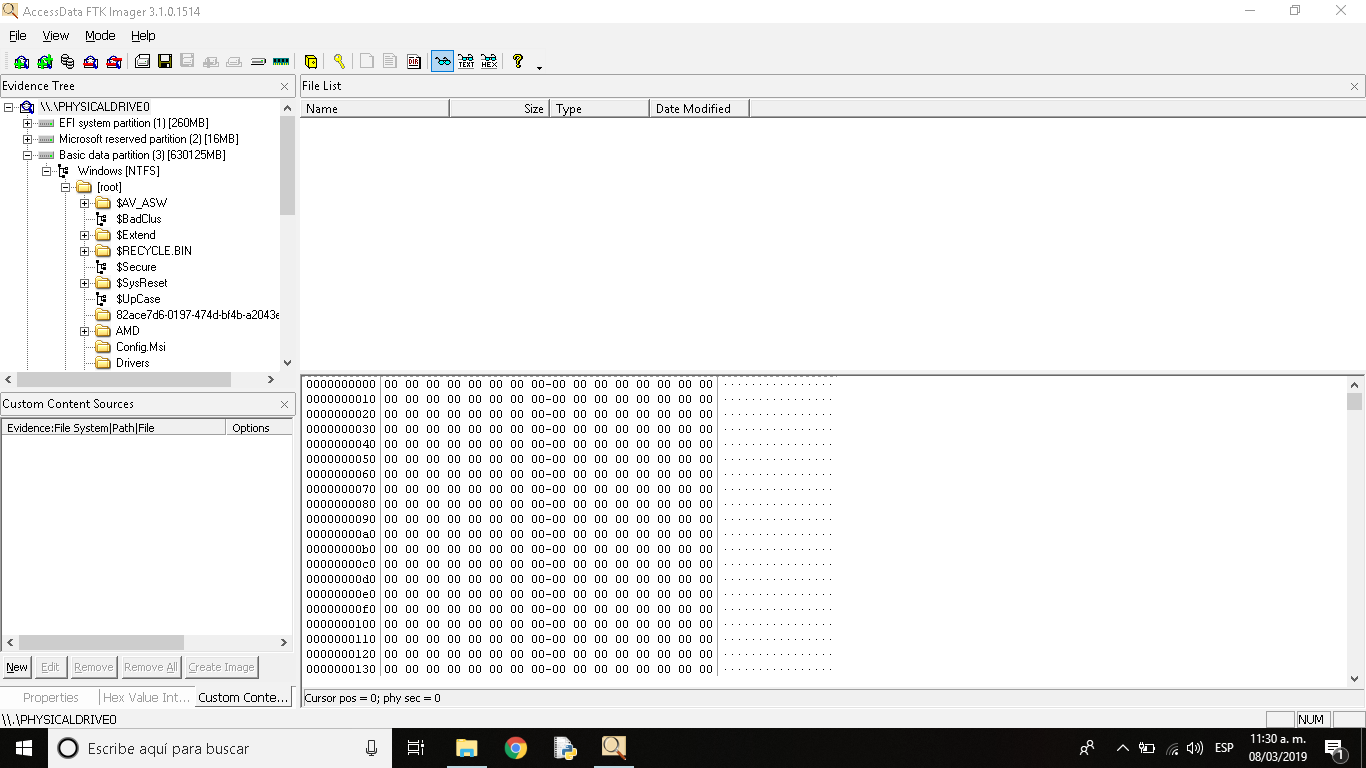
Establecemos que sea la fisica

Le damos en finish.

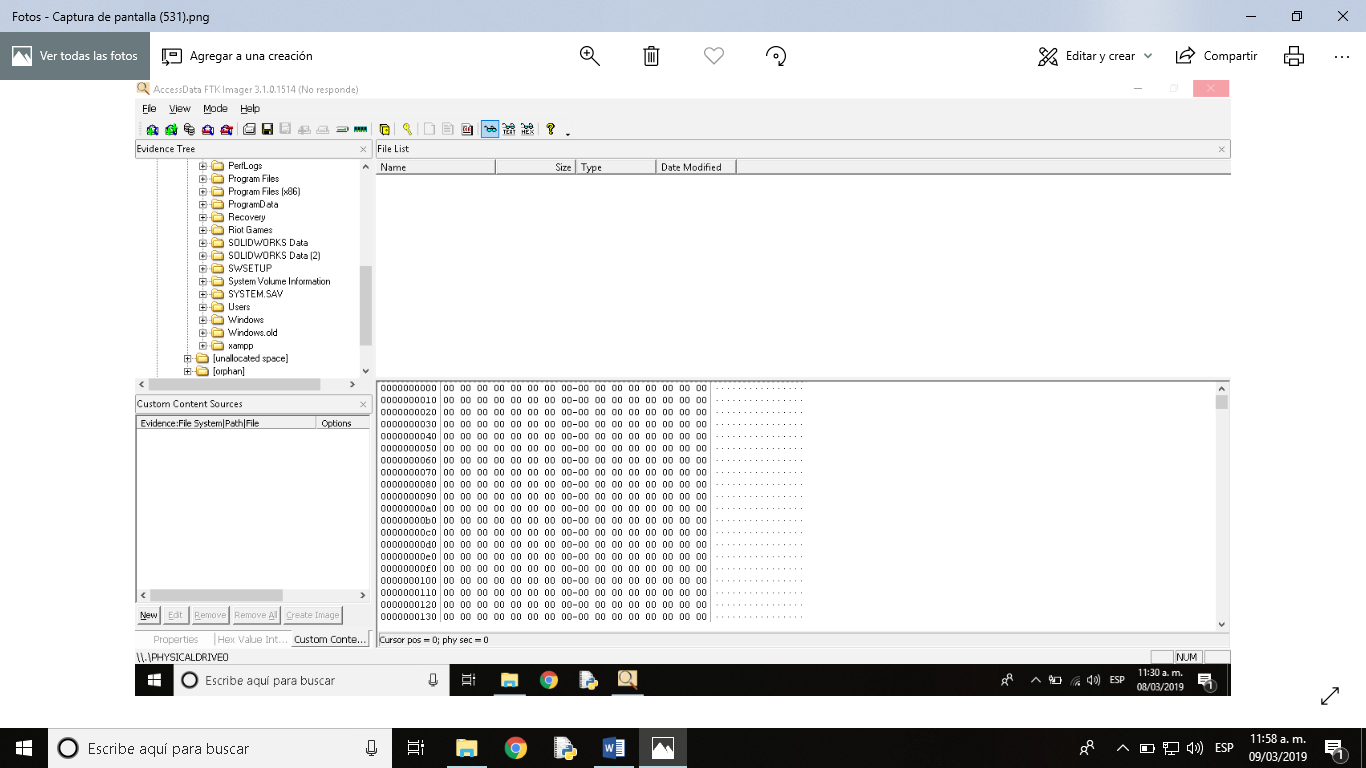
Vamos a desplegar las opciones de PHYSICALDRIVE0



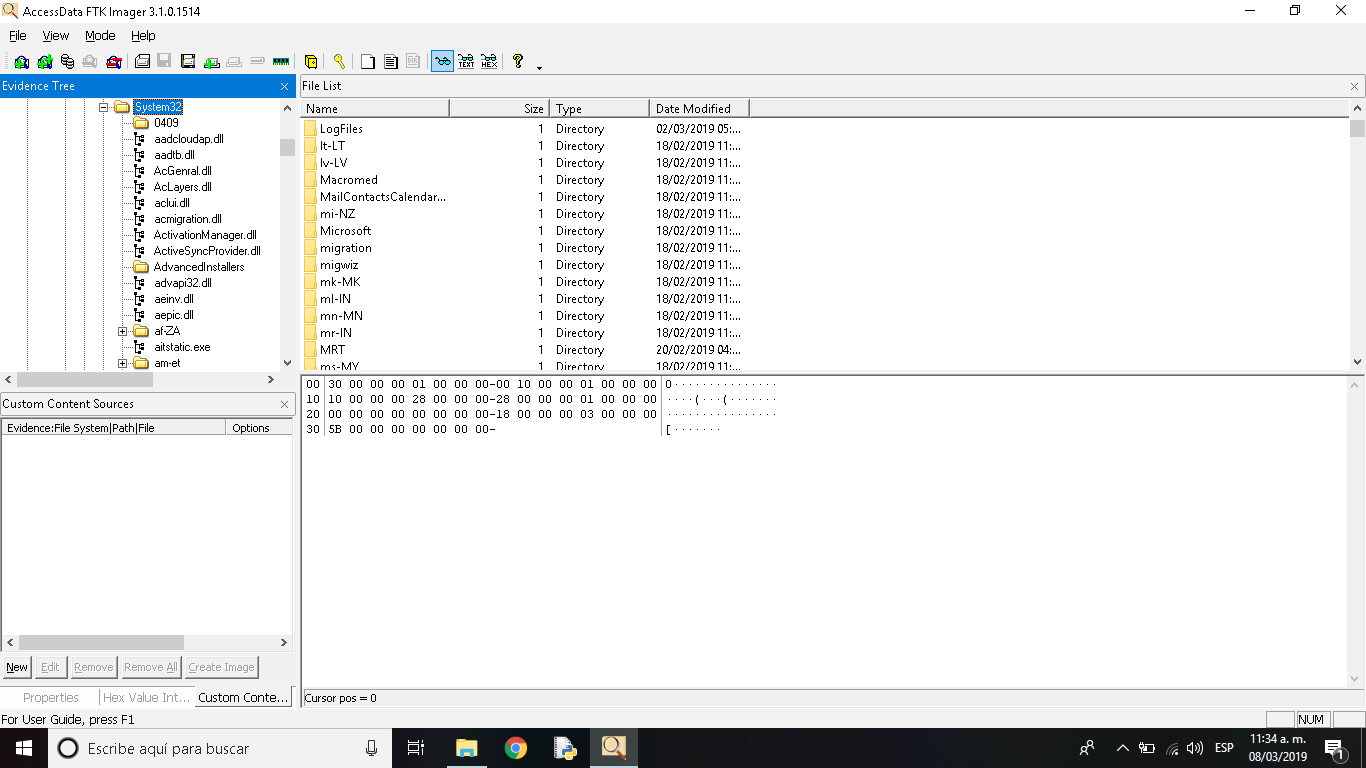
Vamos a desplegar la que tenga mas espacio en MB.



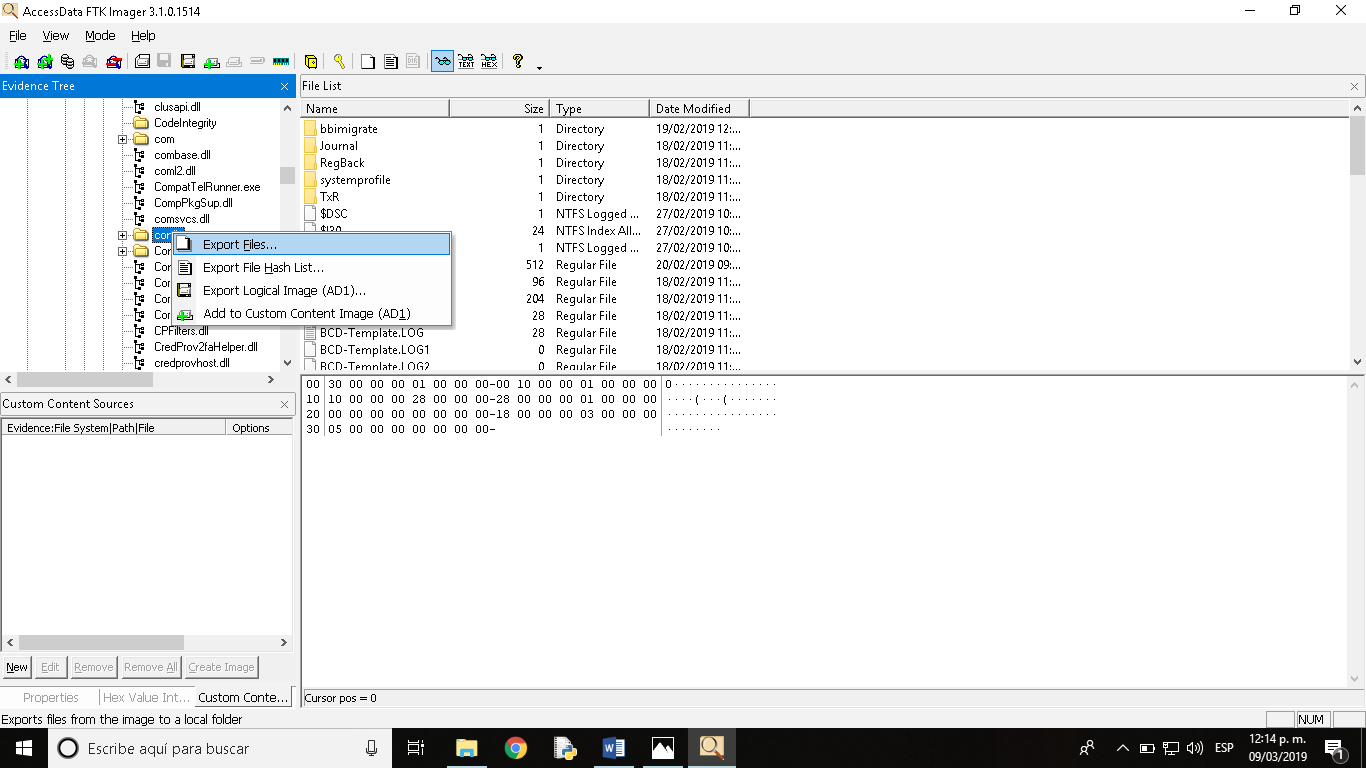
Desplegamos ahora todas las opciones de Windows y dentro de esta la de root.



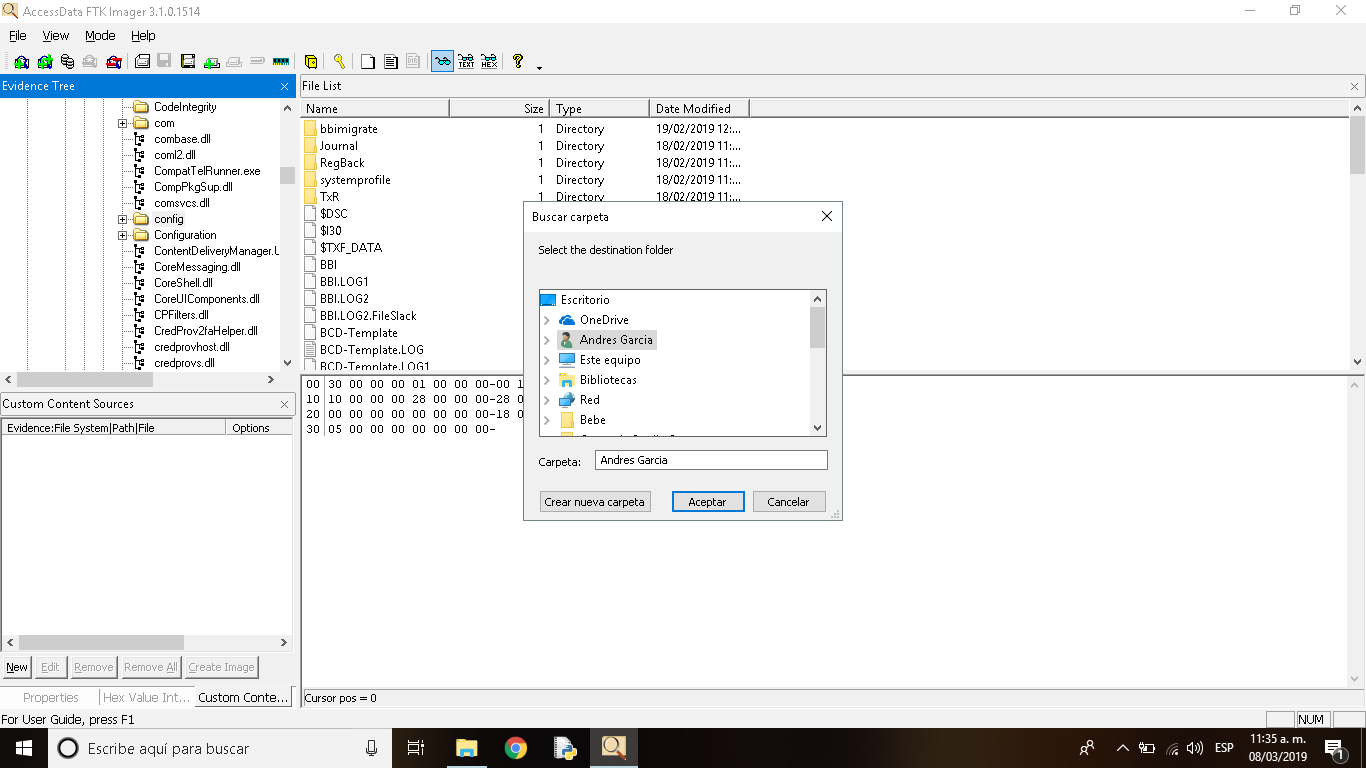
Ahora vamos a desplegar las opciones de Windows.



Ahora desplegamos la opción de System32.

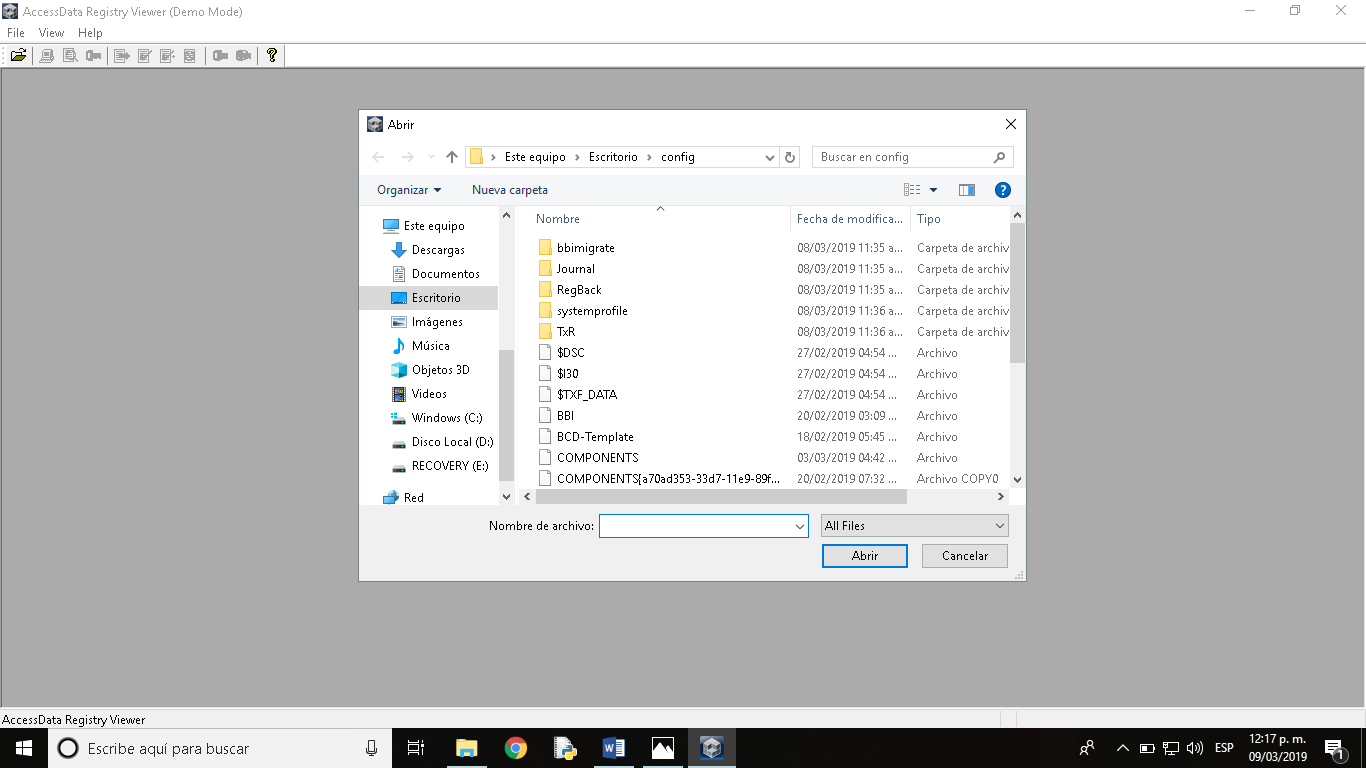


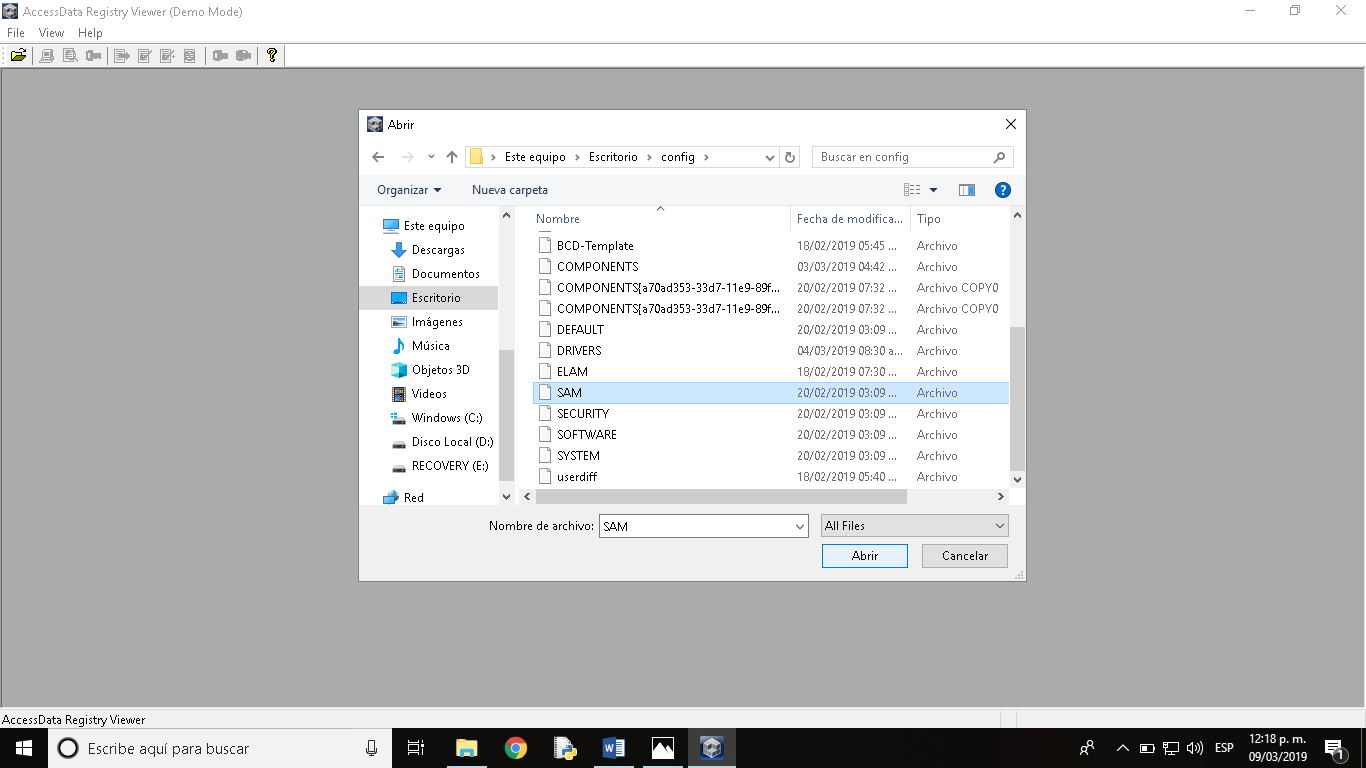
Buscamos la carpeta config y le damos clic derecho. Despues Export Files.



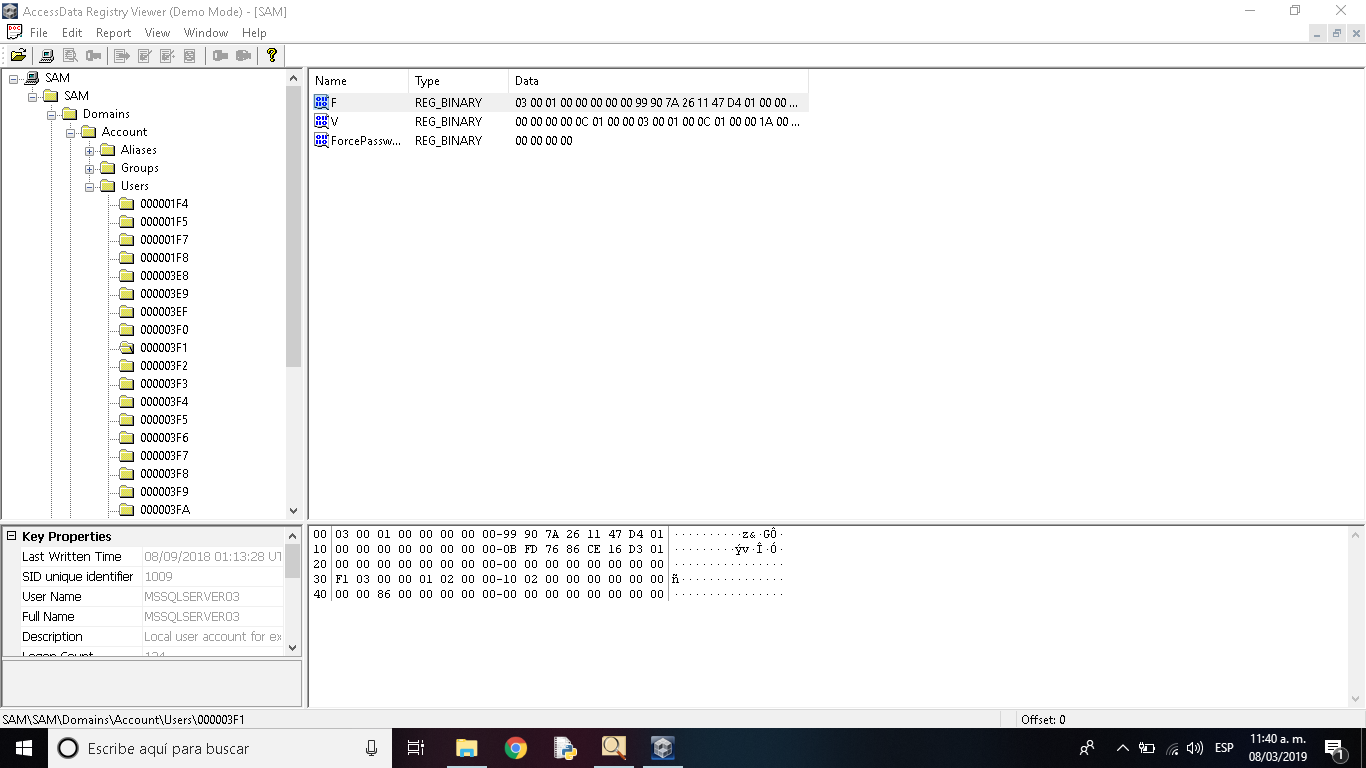
Ahora vamos a elegir una ruta donde se va a guardar nuestra carpeta con la información del sistema y le damos aceptar.

Abrimos el programa AccessData Resgistry Viewer para poder ver la información que extrajimos con el programa anterior.



Vamos a presionar la carpeta de la izquierda, para poder abrir la que exportamos anteriormente. 

Seleccionamos el archivo SAM, para poder ver la información de los usuarios.



Se va a desplegar cada una de las carpetas en el siguiente orden, esto es para poder llegar a usuarios:

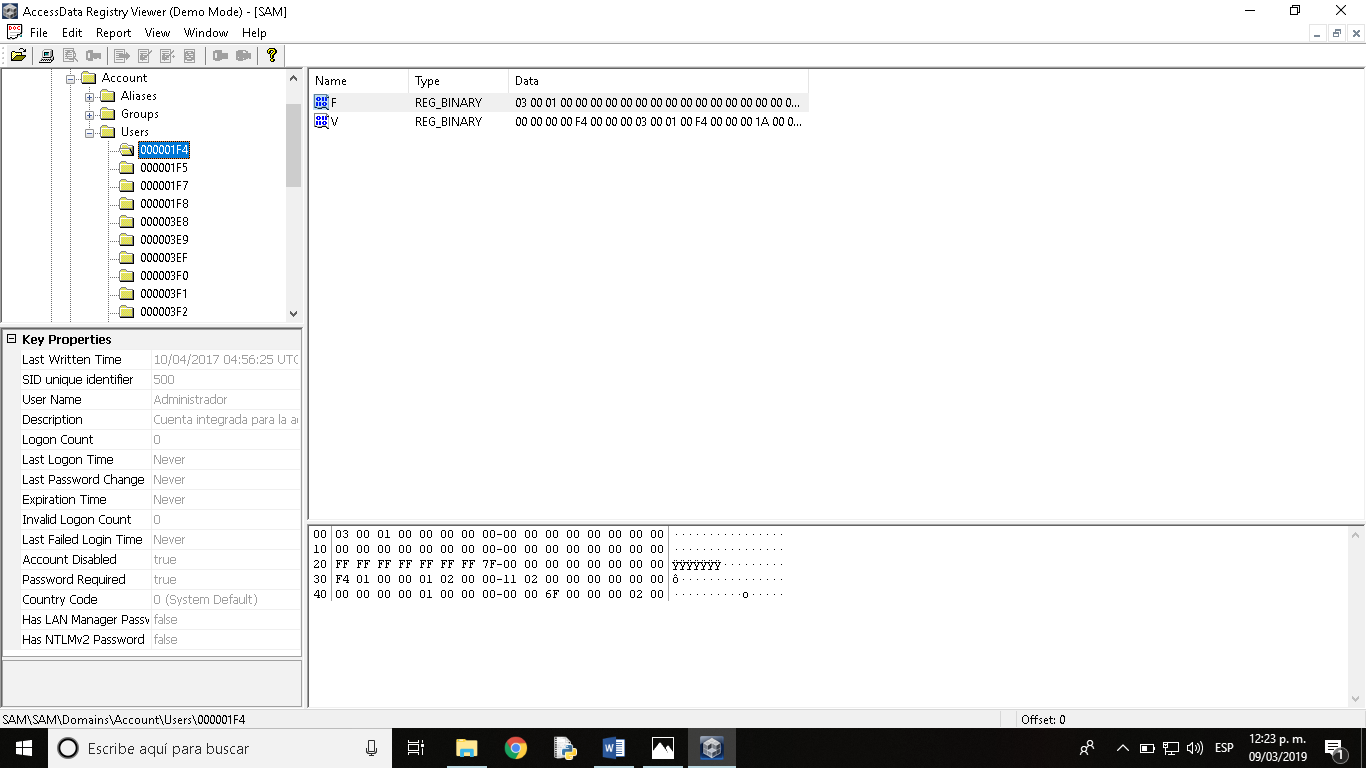
1.- Sam

2.-Domains

3.-Account

4.-Users

Como podemos observar todos los usuarios que tenemos y como observación la mayoría de los usuarios son creados por varias máquinas virtuales y no desde la nativa.



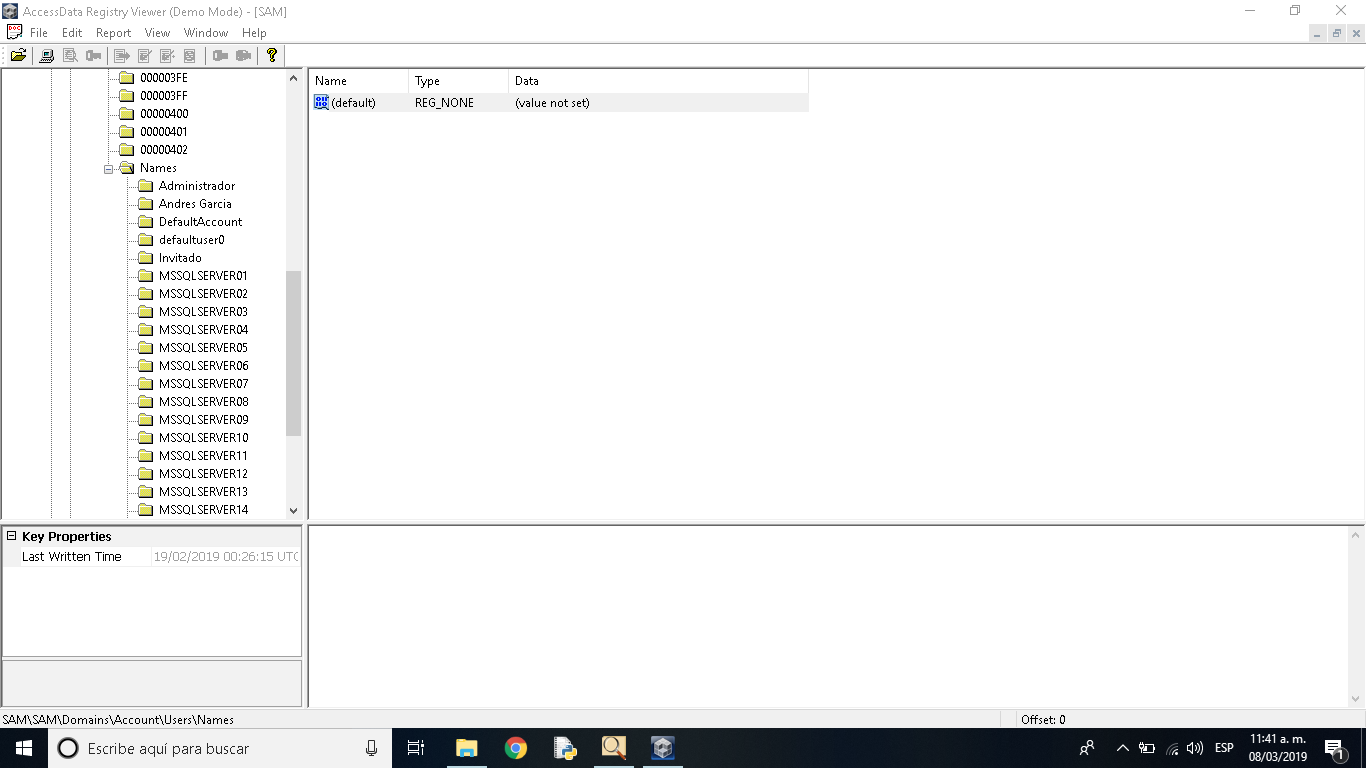
Presionando alguno con clic izquierdo vamos a poder observar algunos de los datos del usuario, como:

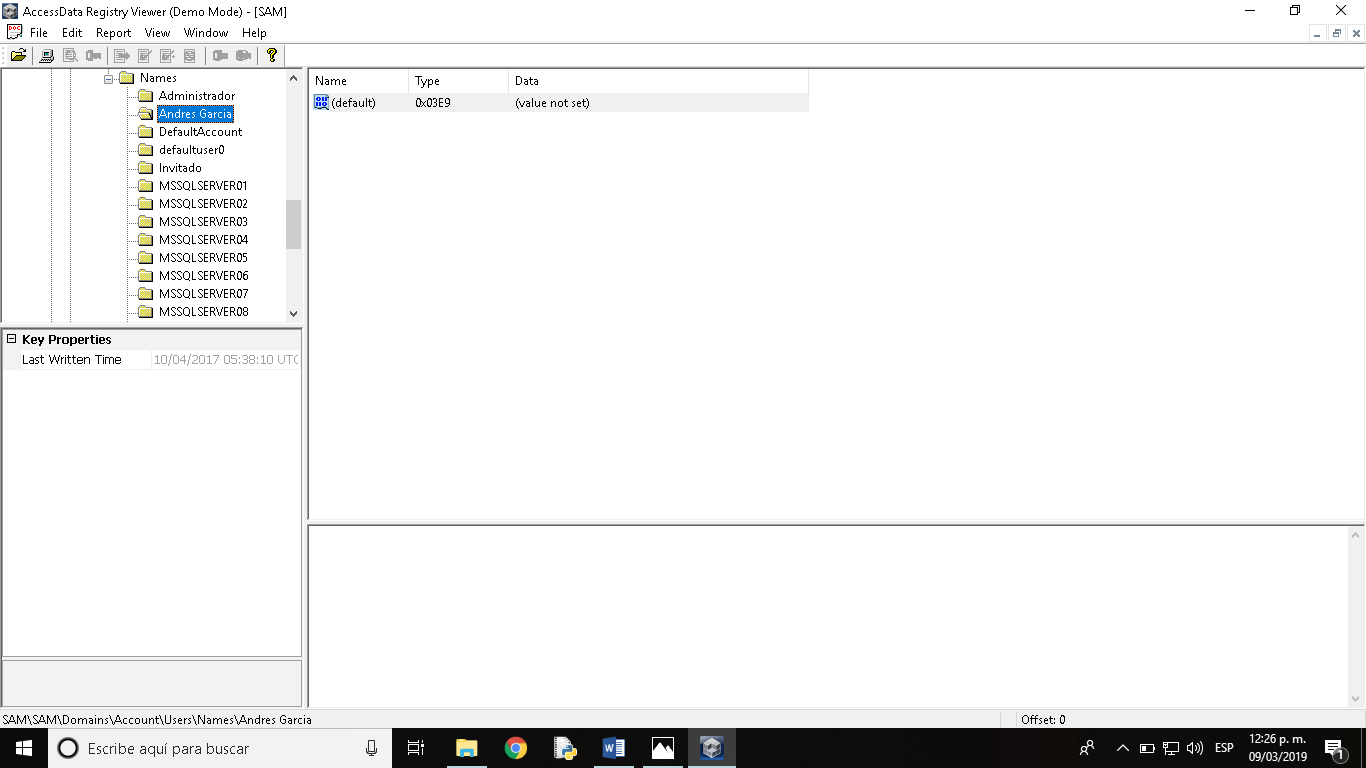
\*Fecha de creación

\*Tipo de usuario

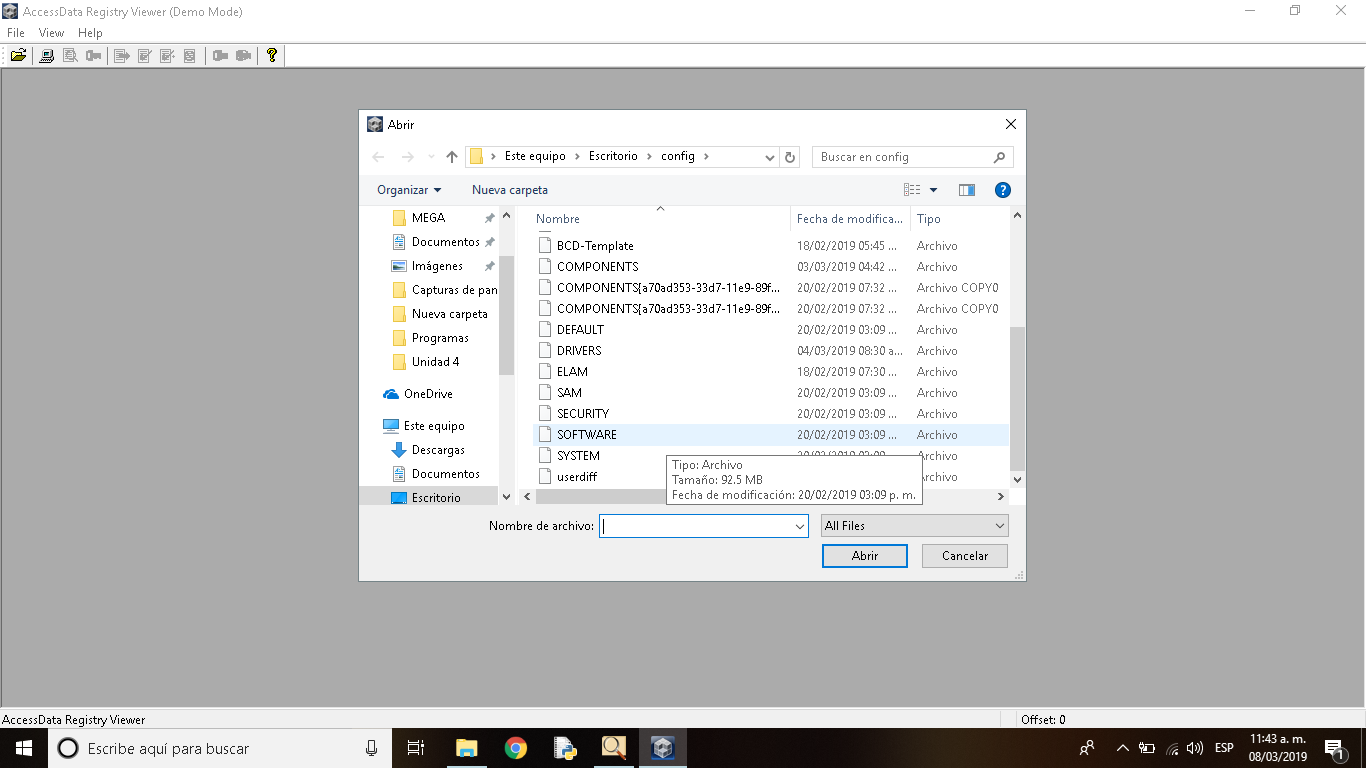
\*La cantidad de veces que ha accedido con la cuenta.

\*Si tiene contraseña, entre otros datos.

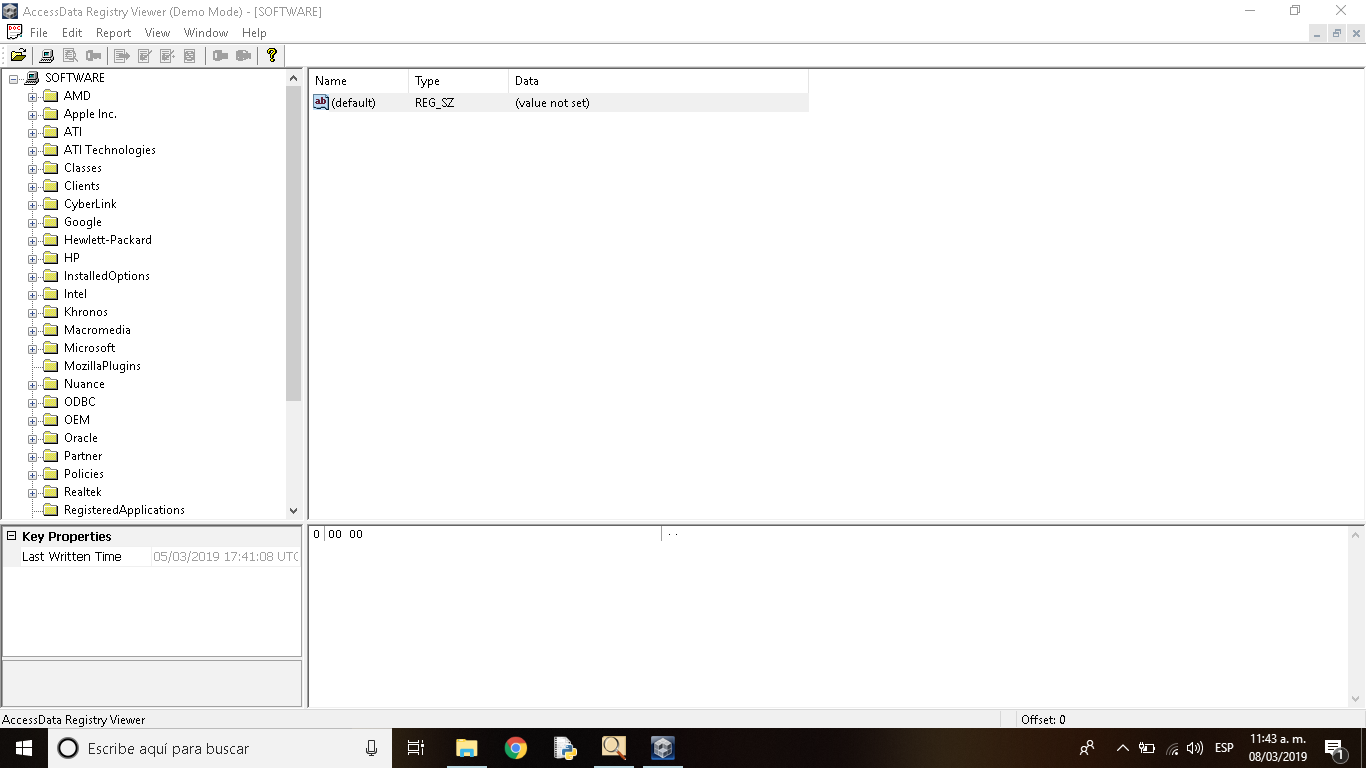


Mas abajo podemos ver la opción de Names, para ver descripción del usuario. 

Podemos observar que nos muestra el nombre de usuario y la mayoria son de maquinas virtuales.



Seleccionamos el archivo SOFTWARE, para poder ver la información de los programas instalados en algun momento.



Vamos a desplegar el contenido de SOFTWARE y podemos observar todos los programas que se hayan instalado en algún momento.