Cancún, Quintana Roo, México 03 de Octubre del 2019

A quien corresponda.

Asunto: Procedimiento de cómo restaurar la copia de seguridad generada por Quick Heal and Seqrite

Quick Heal and **Seqrite Backup and Restore Tool**, le ayuda a restaurar los datos importantes, como documentos, hojas de cálculo, etc. en el caso de Ransomware o cualquier otro malware que los encripte, corrompa o elimine.

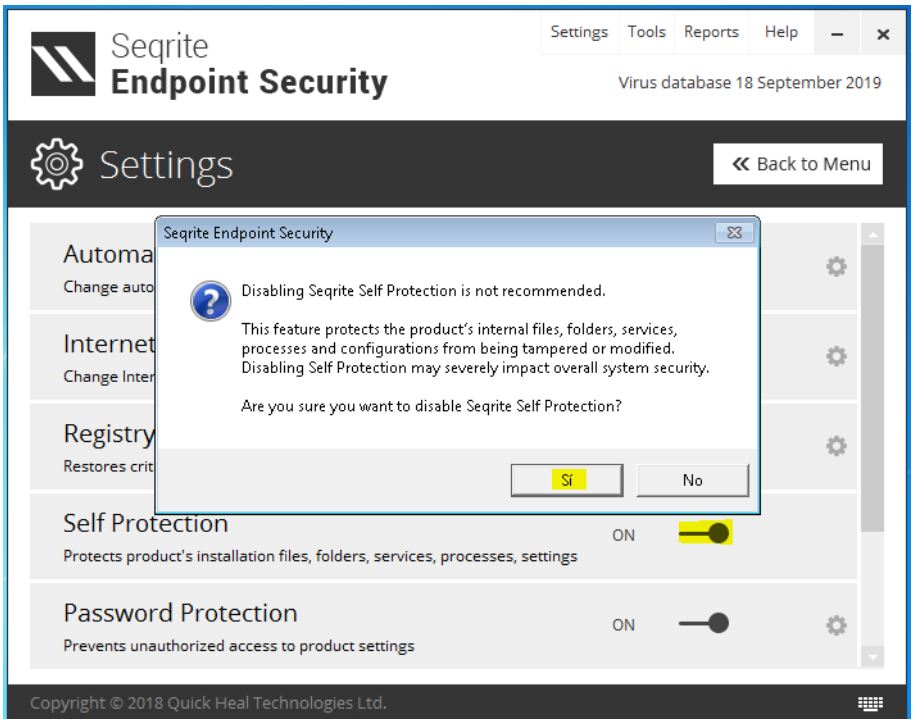
La copia de seguridad se almacena en una unidad donde está disponible la cantidad máxima de espacio libre en disco. La carpeta de respaldo se crea con el nombre aleatorio, por ejemplo: 'cfrbackup-ORALEBLG'

La carpeta de copia de seguridad también está protegida por autoprotección para que los archivos de copia de seguridad permanezcan intactos y no se cifren, corrompan ni eliminen por ninguna actividad de malware.

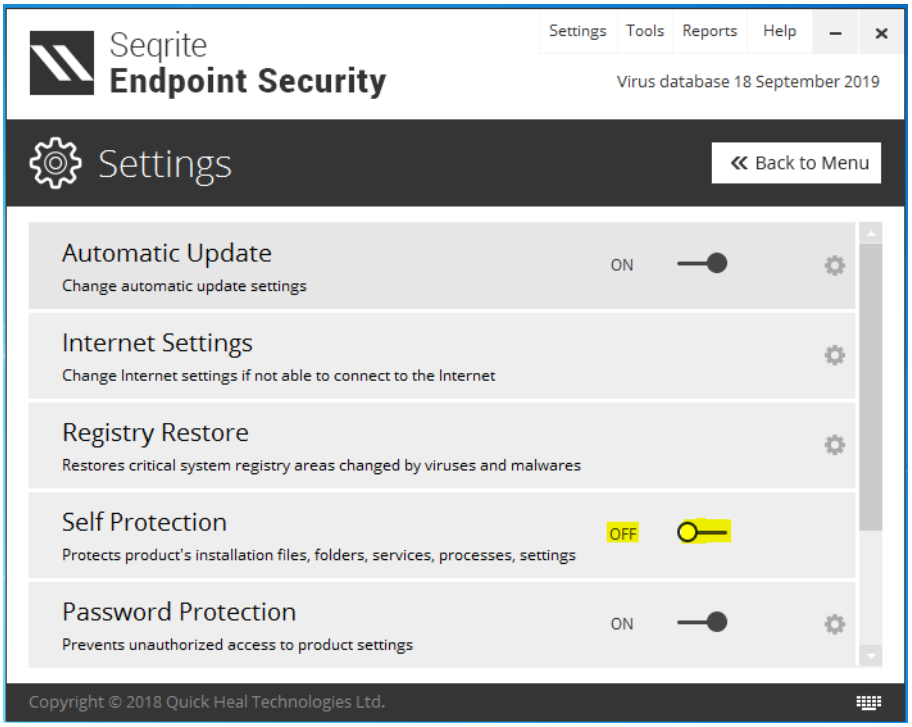
Antes de continuar con la restauración, asegúrese de que:

Quick Heal and **Seqrite** debe estar presente en el sistema antes de que ocurra el incidente del archivo, para que Quick Heal and Seqrite haya hecho una copia de seguridad de esos archivos.
Quick Heal and **Seqrite** debe de estar instalado, actualizado y en funcionamiento.

1. Antes de iniciar con el proceso de restauración, deshabilite la protección de **Quick Heal** o **Seqrite** como se muestra a continuación:



La protección se visualizara de la siguiente manera:



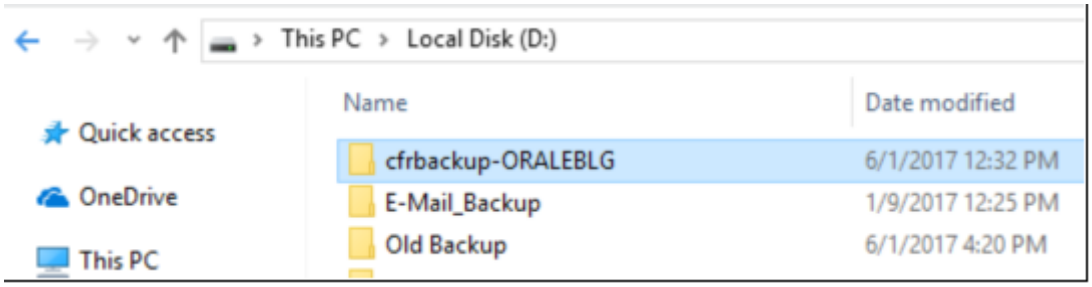
Continuando con el proceso de restauración de datos:

Hay dos formas de restaurar datos:

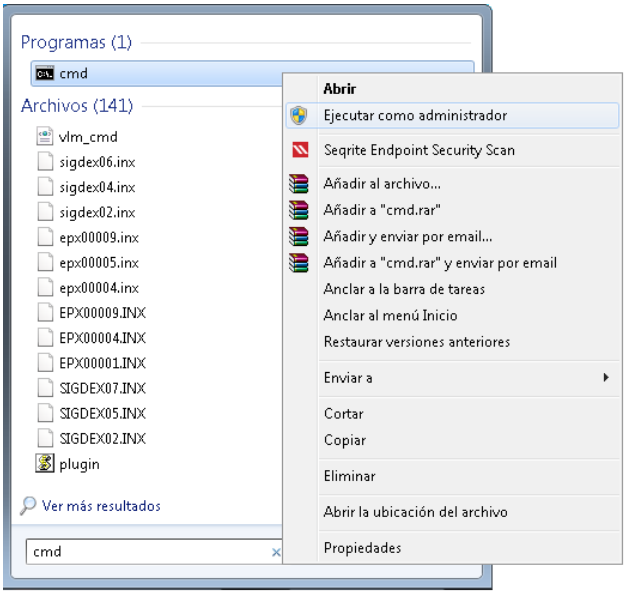
I. Podríamos restaurar la copia de seguridad completa.
II. Podríamos restaurar el archivo único.

Si desea restaurar la copia de seguridad completa, siga los pasos a continuación:

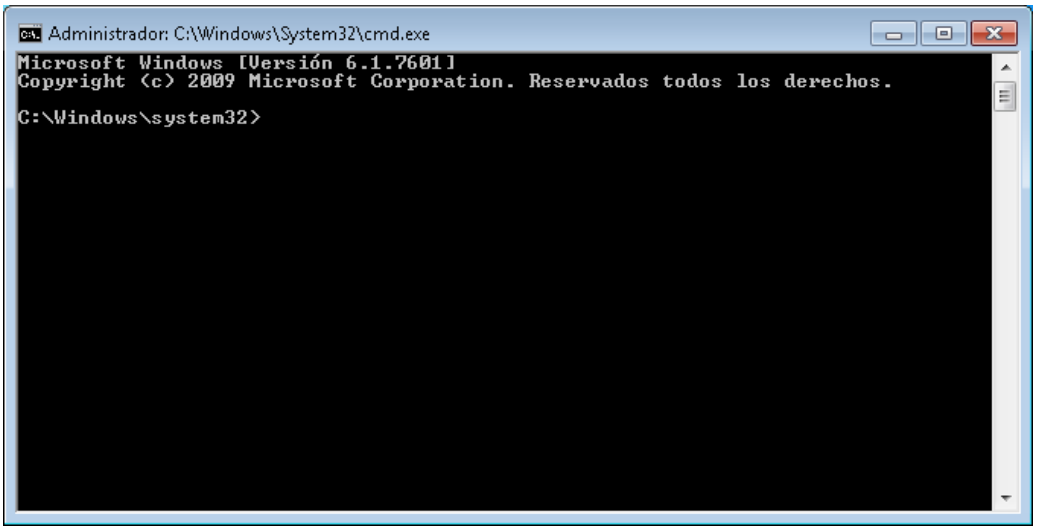
Busque el nombre de la carpeta "cfrbackup - <**random_alpha-numeric string**>" en el disco duro, por ejemplo C: \ cfrbackup-ORALEBLG



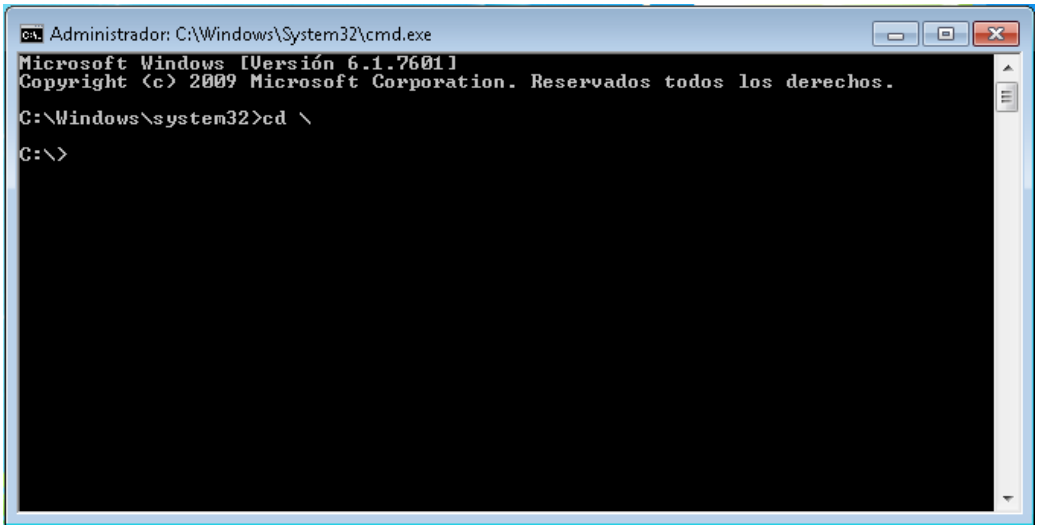
- Haga clic en el menú Inicio de Windows y escriba CMD en las ventanas de búsqueda.



- Haga clic derecho en el resultado de búsqueda para CMD y haga clic en Ejecutar como administrador.
- Obtendrá una ventana de símbolo del sistema negra como se muestra a continuación:

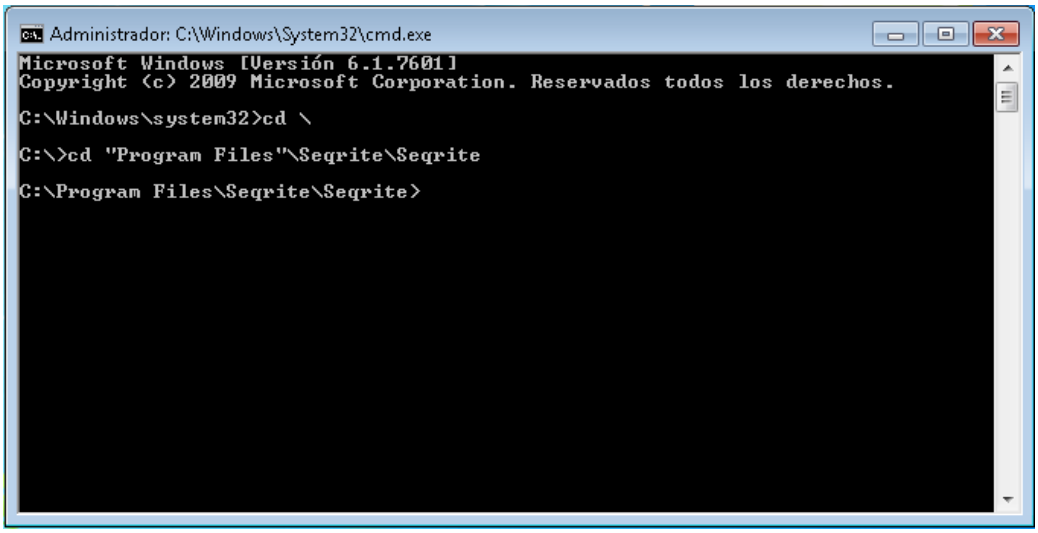


- Escribe 'cd \' y presiona Enter.
- Ahora será redirigido a la raíz de la unidad de la siguiente manera:

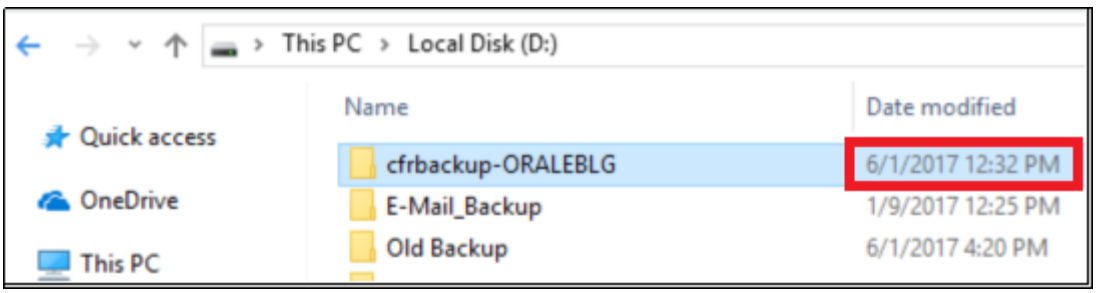


Ahora navegue por el directorio de instalación de Quick Heal o Seqrite.

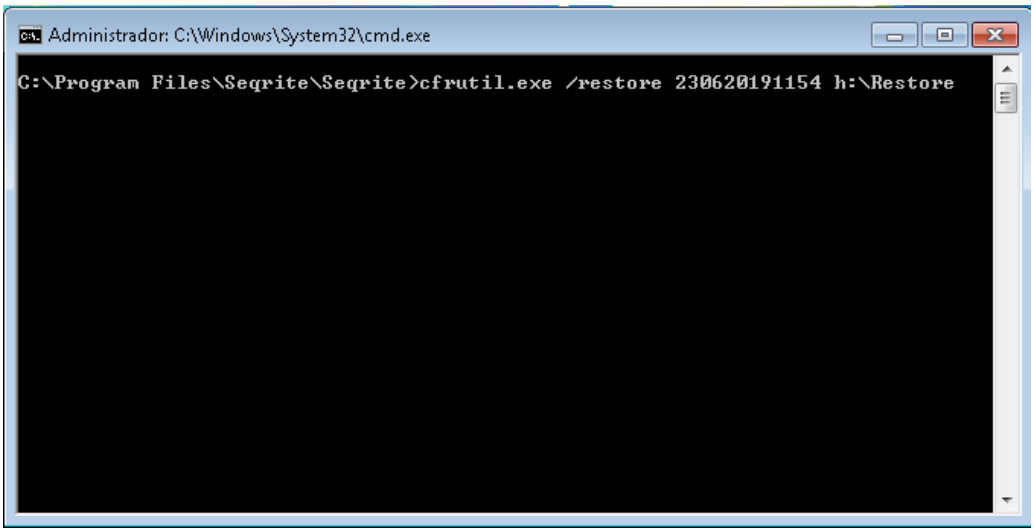
Por ejemplo Si Quick Heal está instalado en “C: \ Archivos de programa \ Seqrite \ Seqrite”, escriba la sintaxis siguiente en la ventana del símbolo del sistema o CMD como se menciona en la siguiente captura de pantalla: "**Cd <espacio> C: \ Archivos de programa \ Seqrite \ Seqrite**"



Fecha de la modificación del archivo:



Escriba **cfrutil.exe / restore** <**fecha de modificación de la carpeta de copia de seguridad**> y la dirección en donde se va a restaurar la información <**Path_to_restore_data**> como se muestra a continuación:



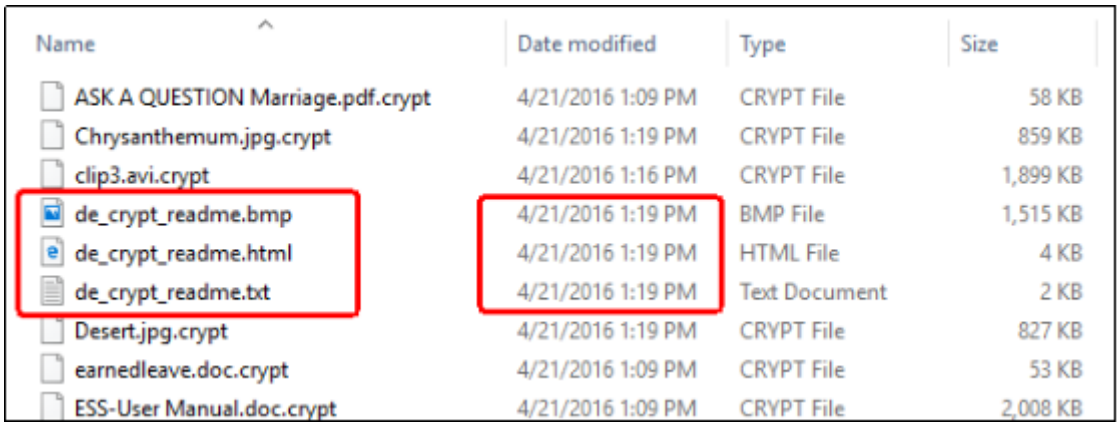
Aquí, la fecha de modificación de la carpeta es el 6/1/2017 12:32 PM, significa 01-junio-2017, 12:32 PM.

También podemos tener la segunda opción para el factor de marcar el tiempo.

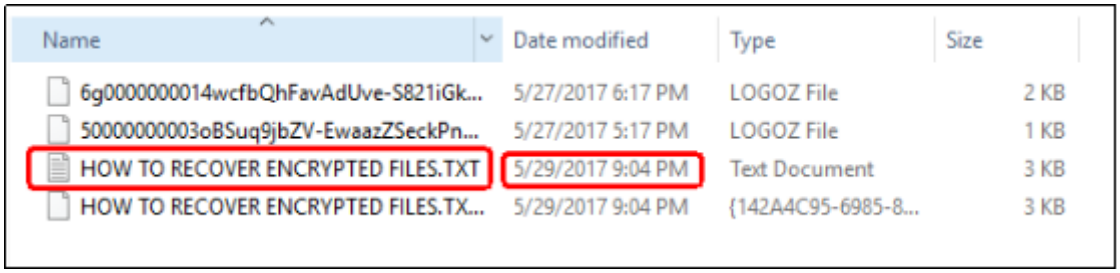
En la mayoría de los casos, Ransomware crea archivos TXT, HTML, BMP de información en la misma ubicación donde ha cifrado los archivos como se menciona en las siguientes capturas de pantalla.

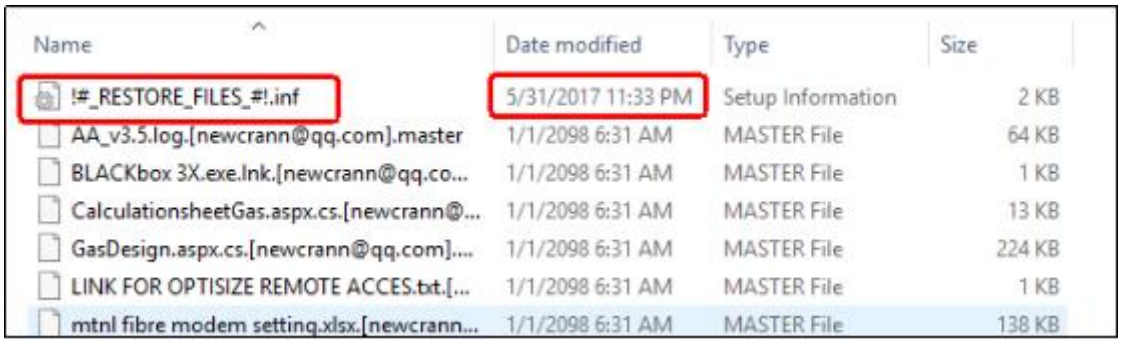
Podemos usar la fecha de modificación de estos archivos para restaurar los datos.

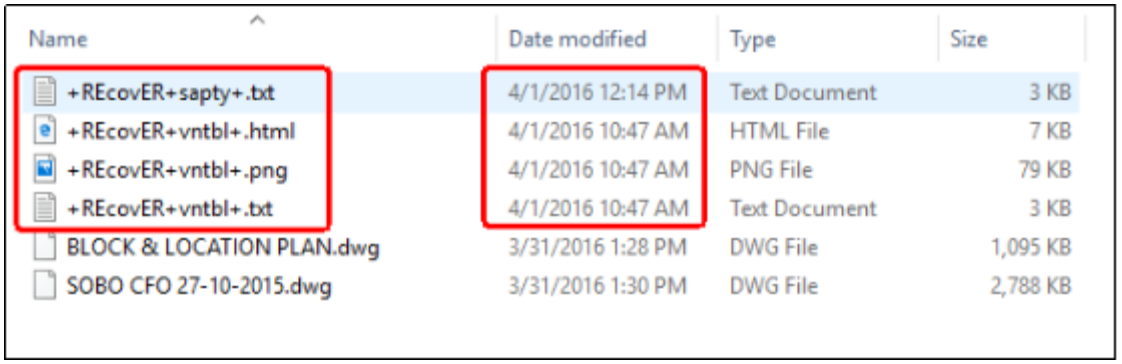
<u>Por ejemplo en un caso de un ataque de Ransomware:</u>

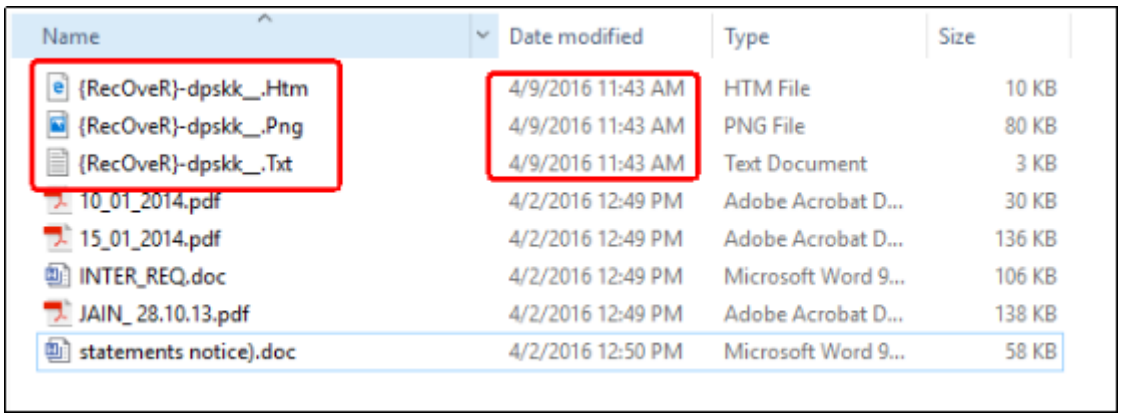


Name	Date modified	Type	Size
ASK A QUESTION Marriage.pdf.crypt	4/21/2016 1:09 PM	CRYPT File	58 KB
Chrysanthemum.jpg.crypt	4/21/2016 1:19 PM	CRYPT File	859 KB
clip3.avi.crypt	4/21/2016 1:16 PM	CRYPT File	1,899 KB
de_crypt_readme.bmp	4/21/2016 1:19 PM	BMP File	1,515 KB
de_crypt_readme.html	4/21/2016 1:19 PM	HTML File	4 KB
de_crypt_readme.txt	4/21/2016 1:19 PM	Text Document	2 KB
Desert.jpg.crypt	4/21/2016 1:19 PM	CRYPT File	827 KB
earnedleave.doc.crypt	4/21/2016 1:09 PM	CRYPT File	53 KB
ESS-User Manual.doc.crypt	4/21/2016 1:09 PM	CRYPT File	2,008 KB









* La entrada de tiempo solo se puede aceptar en formato de 24 horas.

Por ejemplo: Si la fecha de modificación de la carpeta es el 6 de junio de 2017, 3: 20 PM, debe ingresarse como "**060620171520**".

Entonces, la sintaxis del comando para continuar es la siguiente:

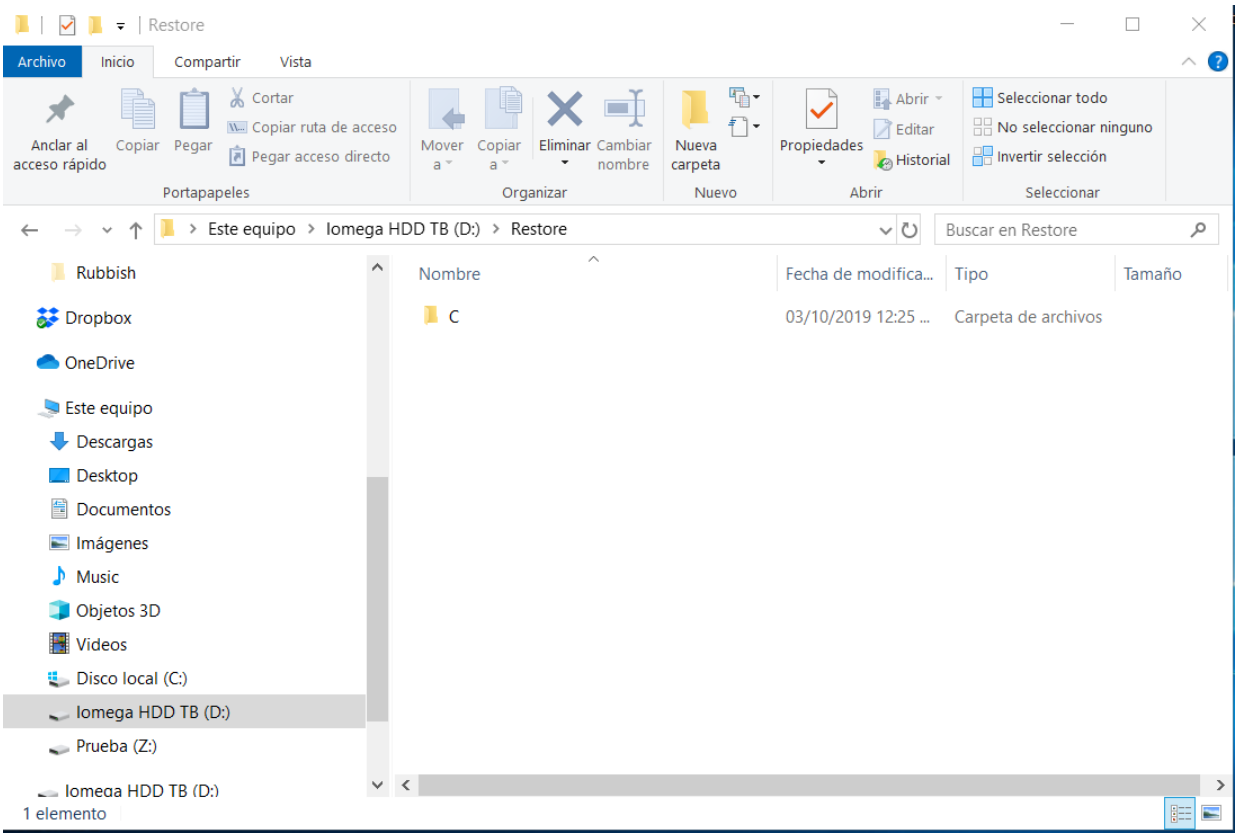
"cfrutil.exe / restore 010620171232 D: \ Restore"

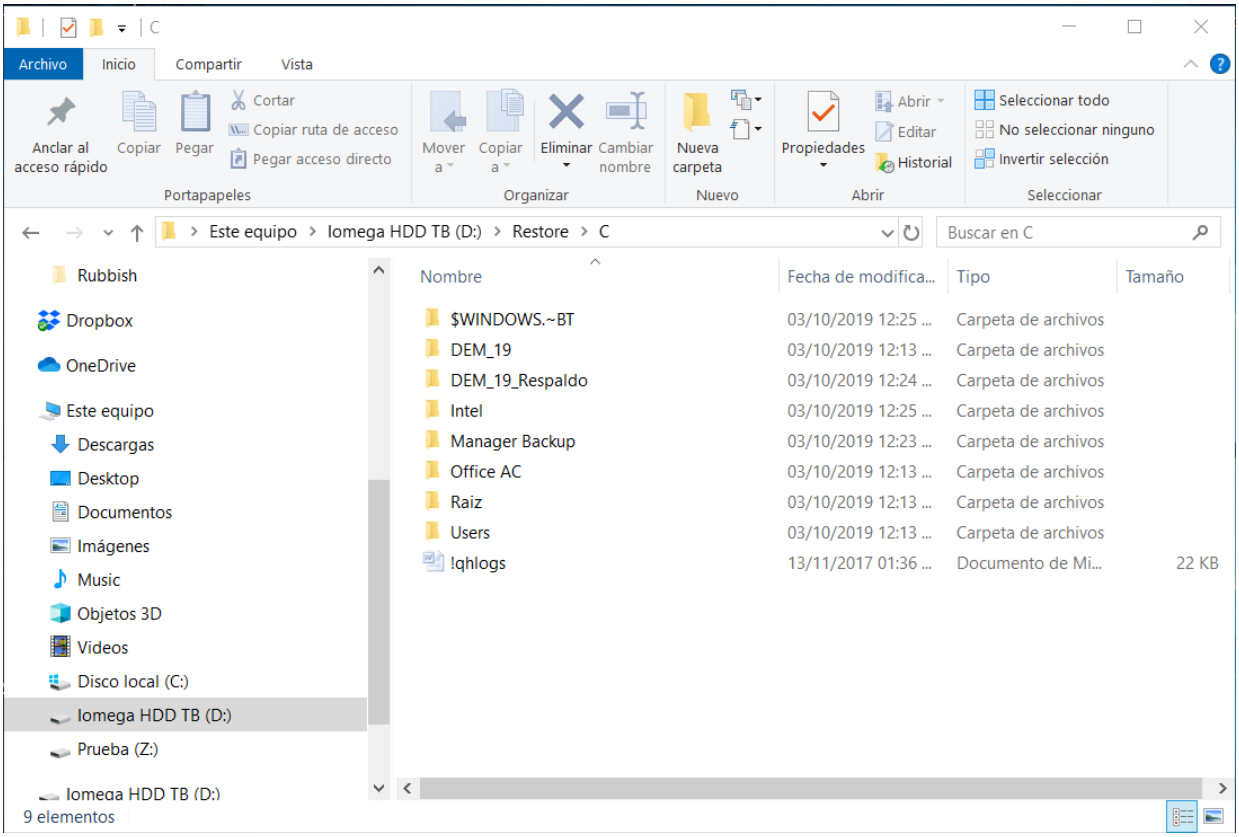
Donde **D: \ Restore** no es más que la ubicación donde se debe restaurar la copia de seguridad.

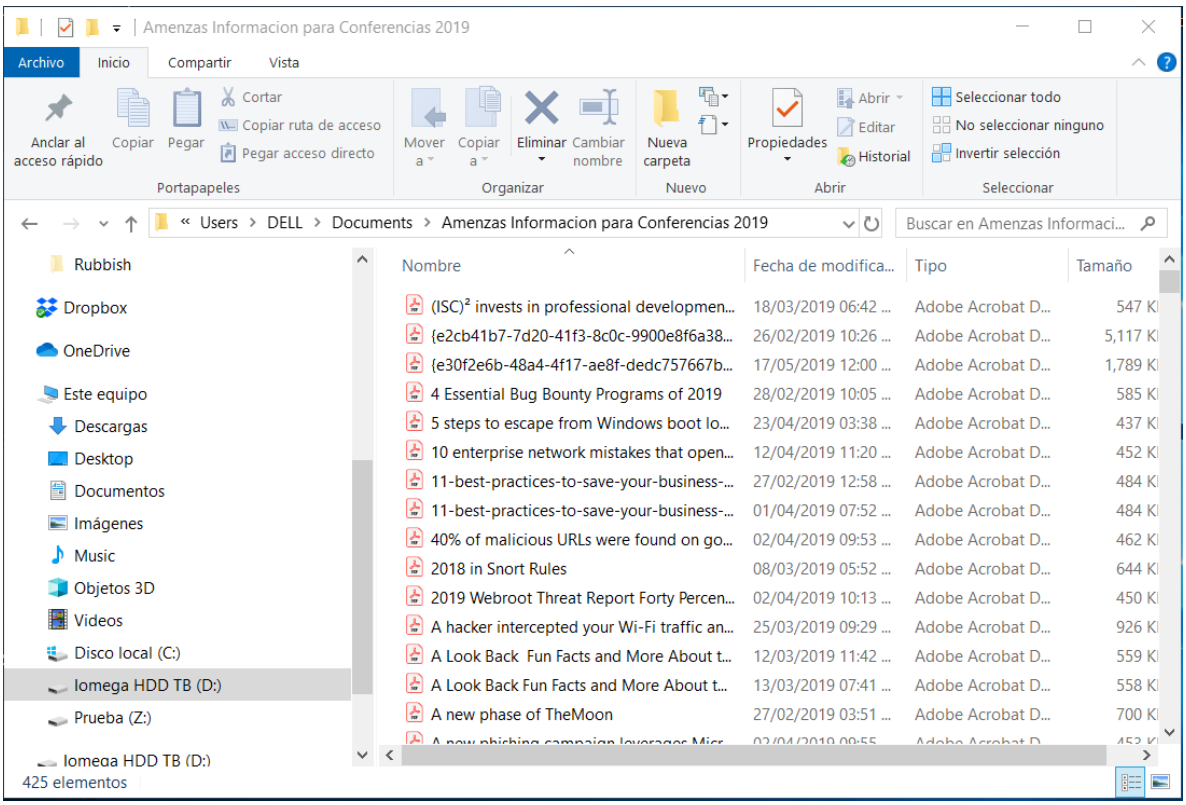
Nota importante: Es imprescindible que el proceso de restauración se lleve a cabo en una unidad diferente a "**C:**" puede realizarse en el mismo disco, en otra partición que contenga suficiente espacio para realizar la restauración de todos los archivos, en caso contrario debe de usarse una unidad de disco duro externo con suficiente espacio para realizar la restauración de los archivos.

Presiona **Enter** y verás que la restauración está en progreso, e indicarla lo siguiente: "**Restaurando copia de seguridad ...**"

Los archivos comenzarán a restaurarse en la carpeta seleccionada con la carpeta de nombre de unidad y las subcarpetas en el formato jerárquico como se muestra a continuación:







Certificaciones:

Oficinas Latinoamérica:

Quick Heal Technologies Limited
Calle Curico No. 34 Mz. 3 Smz. 505, San Geronimo, Cancun, Q. Roo, México 77533
Teléfono: +52 998 989 3157 | ventas-la@quickheal.com | ventas-la@seqrite.com
www.quickheal.com | www.seqrite.com

Si desea restaurar un solo archivo y luego siga los pasos a continuación:

Siga los pasos del 1 al 7 que se realizaron en al anterior procedimiento.

Escriba el comando en la siguiente sintaxis como se menciona a continuación:

cfrutil.exe / restorefile <Ruta_archivo_original> <Path_to_restore_file>

Por ejemplo: **cfrutil.exe / restorefile D: \ ONLINENT \ Onlinent_Final_.rtf D: \ Restore**

Presiona **Enter** y verás que los archivos restaurados se han completado:

Puede ver el archivo restaurado en la ruta seleccionada.