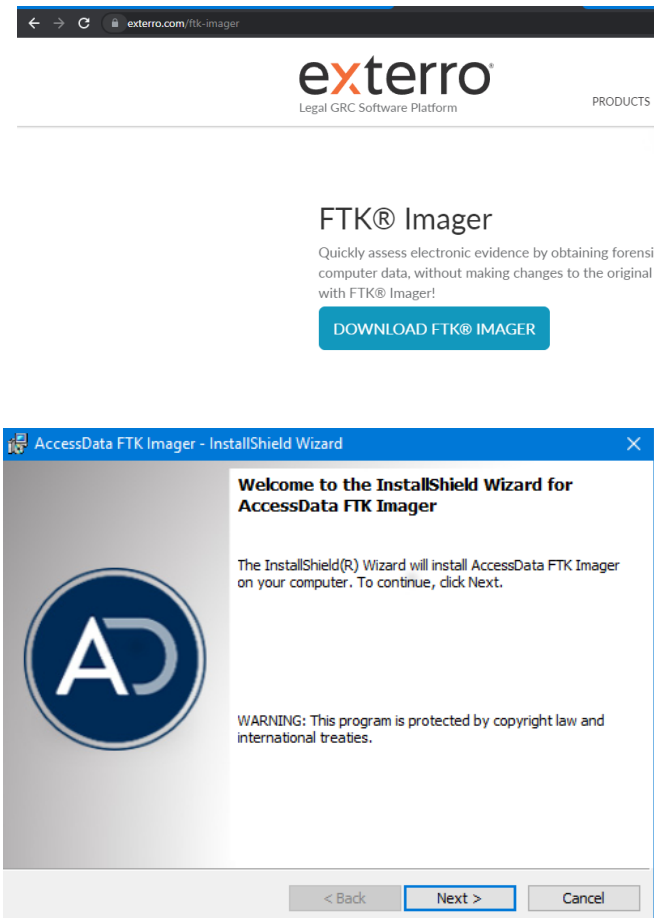
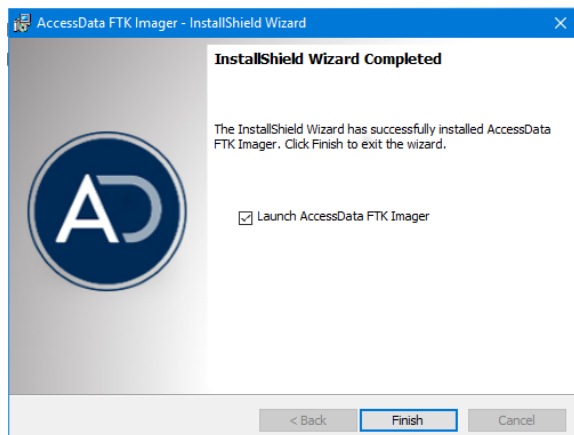
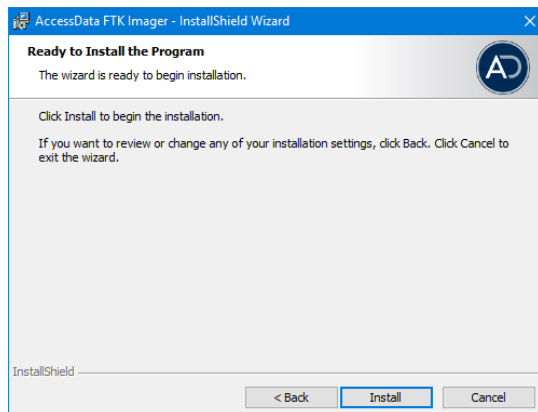
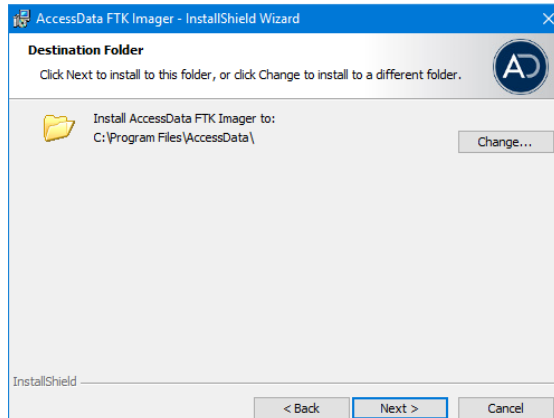
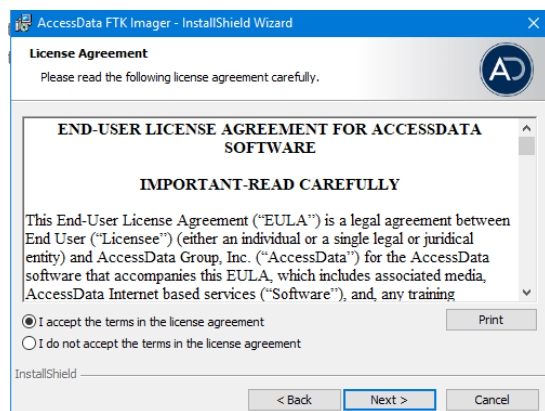


 	INGENIERÍA DE SISTEMAS		 INICIAL APELLIDO APTERNO
	AUDITORIA DE SISTEMAS		
PRIMER PARCIAL			
NOMBRES	APELLIDO PATERNO	APELLIDO MATERNO	
EDSON JAVIER	PACO	LIMACHI	
CI.	CEL.	FECHA	
5972576	73734591	2/4/2023	

DESARROLLO:

CAPTURA DE PANTALLA	DESARROLLO/EXPLICACIÓN
	<ol style="list-style-type: none"> 1. Para realizar el examen es necesario emplear aplicación o software que debemos descargar y lo explicamos paso a paso a continuación 2. Primeramente, realizamos la descarga de la aplicación llamada FTK Imager de la pagina oficial que es exterro el siguiente link redireccionara a la página directamente Link https://www.exterro.com/ftk-imager FTK IMAGER. - Para la descarga nos saldrá un pequeño formulario se debe llenar y aceptar los términos y condiciones Seguido dar clic a enviar Y se procese el comienzo de la descarga de manera automática} 3. Ir a la carpeta descargada y dar clic al ejecutable 4. Seguido nos aparece la siguiente pantalla 5. Le damos a <i>NEXT</i> para continuar con la instalación

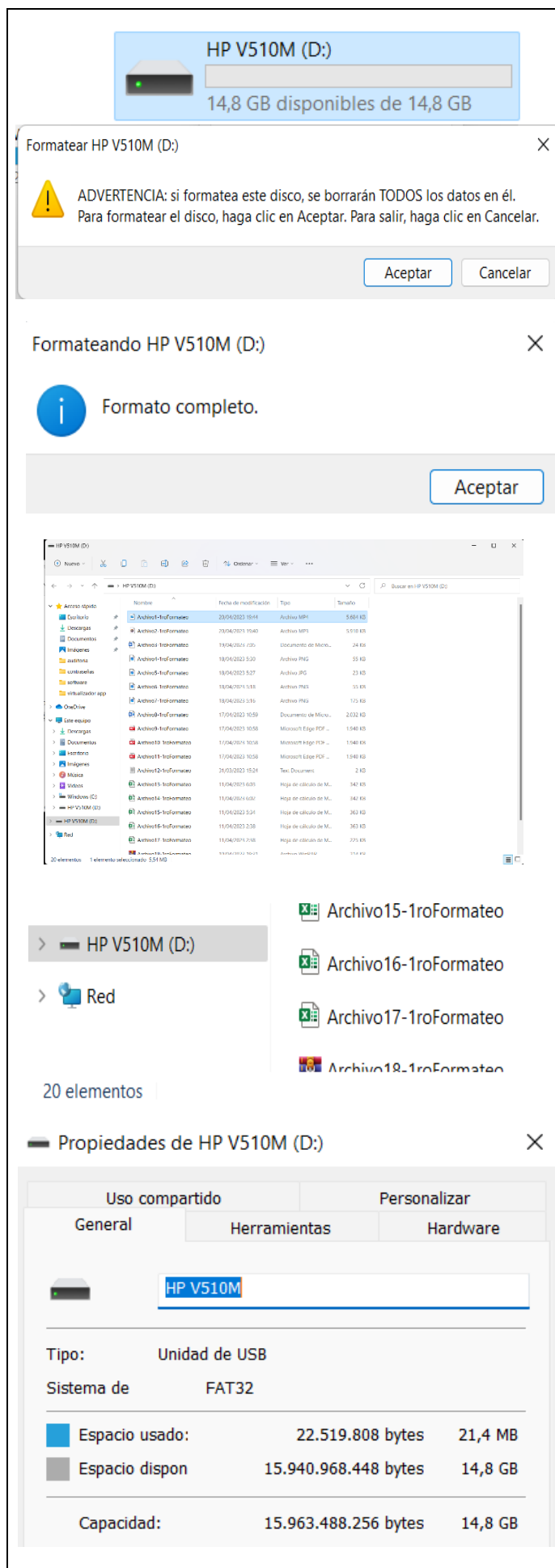


6. Nos dará la siguiente ventana
7. Le damos a la opción de aceptar términos y condiciones
8. Es recomendable realizar una pequeña lectura a los términos y condiciones para informarnos
9. Seguimiento de NEXT

10. Seleccionamos la ruta de donde se instalará los paquetes
11. Ya viene una ruta por defecto se puede dejar ahí o
12. Le damos a NEXT

13. Una vez completada los demás pasos damos a opción INSTALL

14. El proceso de instalación se realizará
15. Cuando se finalice damos a la opción FINISH



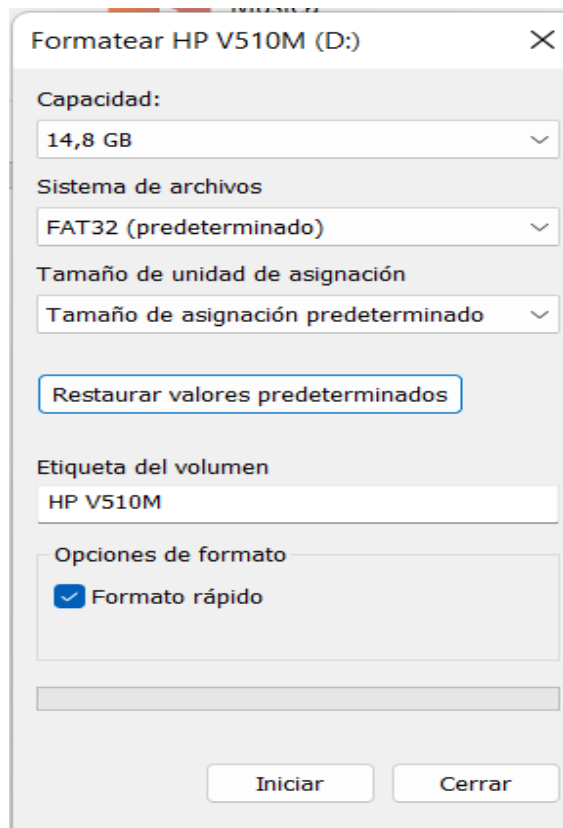
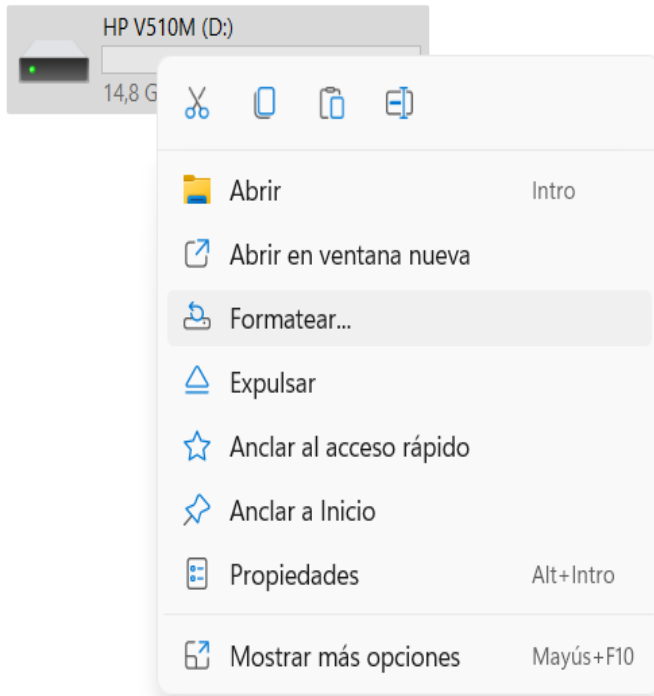
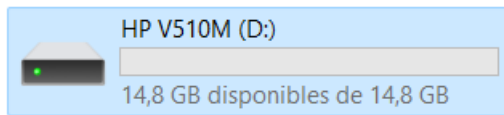
PRIMER FORMATEO

16. Podemos apreciar la unidad extraíble USB
17. Como indica el laboratorio realizamos un primer formateo a la unidad para que se verifique que la unidad esta vacía esto nos simulara una unidad nueva
18. Podemos ver que al momento de realizar el formateo nos da las advertencias
19. Le damos aceptar y el proceso se inicia
20. Esperamos a que se finalice el formateo y nos de un mensaje como el que podemos apreciar

SEGUNDO FORMATEO

21. Una vez realizado el proceso nos procedemos a llenar de diferentes archivos la unidad USB para el primer formateo
22. Como manda la guía primero realizamos la inserción de 20 archivos con el respectivo nombre "Archivo1-1roFormateo"
23. En la imagen que apreciamos podemos ver la cantidad de elementos que se inserto
24. Cabe destacar que son diferentes tipos de archivos los ingresados a la memoria USB
25. Podemos apreciar en la imagen en el contador de documentos
26. Nos muestra 20 elementos en la unidad USB
27. Cumpliendo la condición del laboratorio

28. En la imagen podemos ver una muestra las propiedades de la unidad de almacenamiento
29. Apreciamos que se tiene ocupado 21.4 Mb del espacio total
30. Cabe destacar que no es muy grande porque los archivos ingresados no tienen ocupan mucho espacio
31. Esto se realizo para acelerar el proceso de recuperación



32. Ya que a mas datos que analizar y mas memoria de la unidad será más demoroso el proceso de análisis

33. En la imagen podemos ver la unidad

34. Siguiendo la condición del laboratorio procedemos a formatear la unidad USB

35. Por lo cual nos vamos a la unidad le damos clic derecho

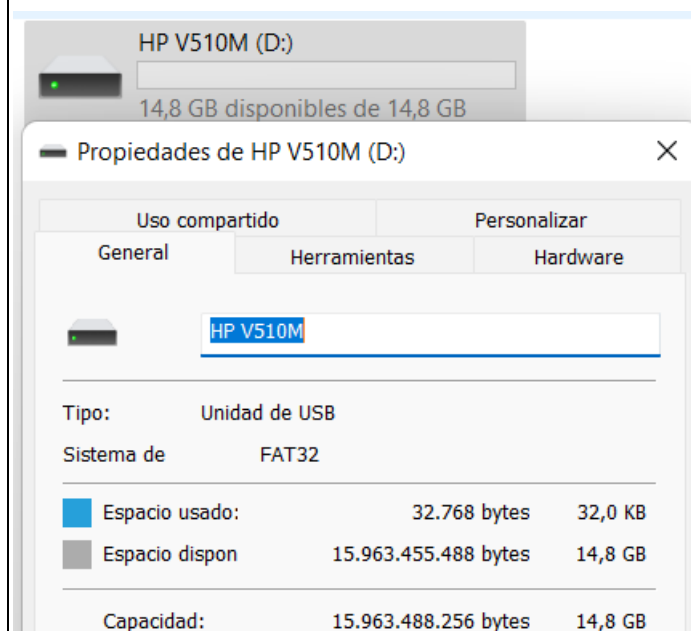
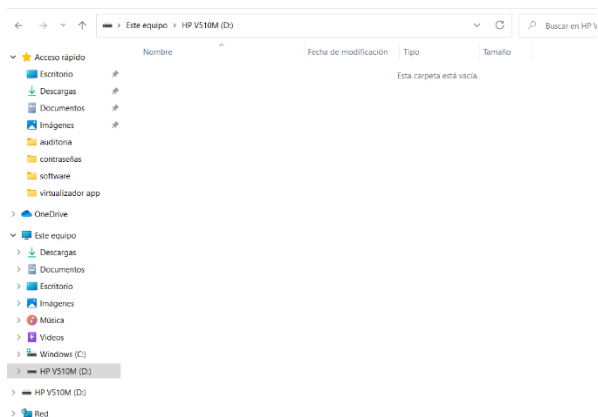
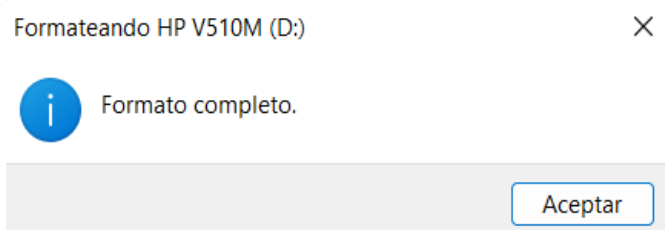
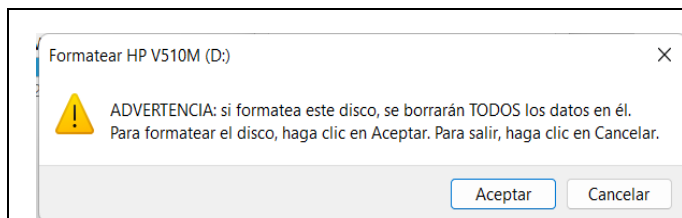
36. No vamos a la opción de formatear

37. Al realizar le paso 36 nos despliega esta ventana por lo siguiente

38. Nos mostrara la configuración de la unidad

39. Para que realiza el proceso de formateo de la unidad

40. Damos a la opción INICIAR



41. Al realizar el paso 40 nos despliega una advertencia
42. Lo cual procedemos a leer y damos ACEPTAR

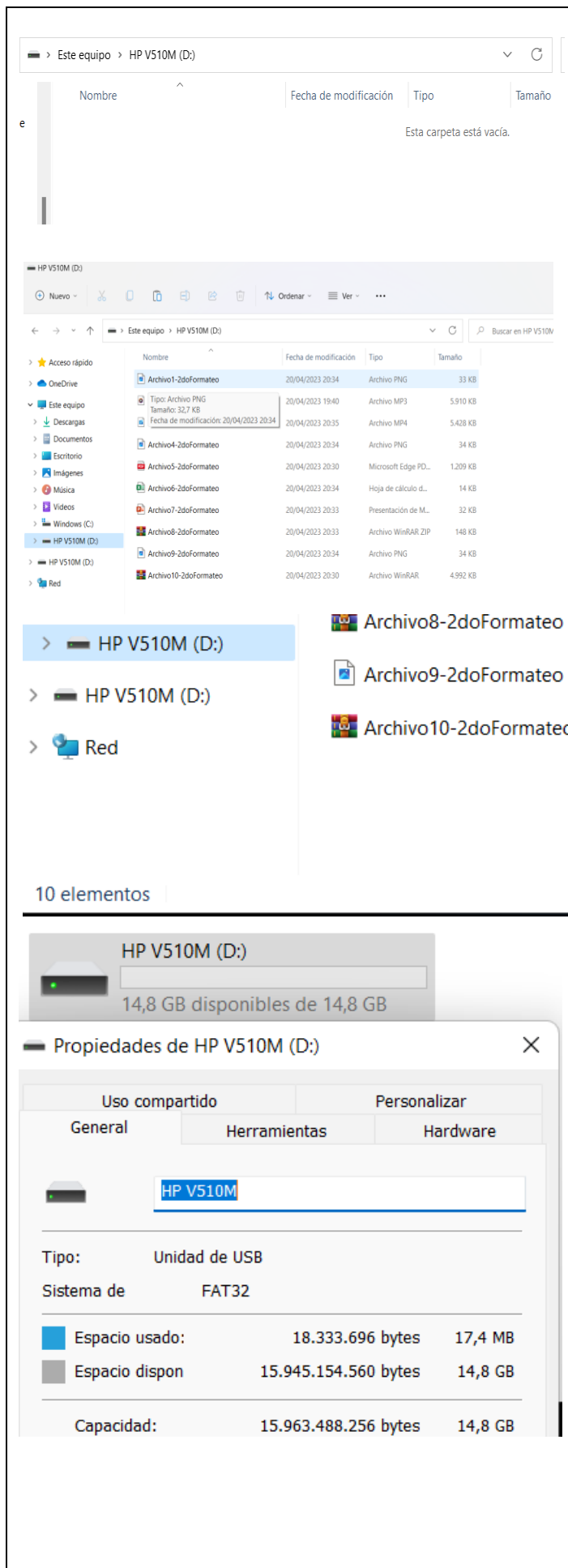
43. Una vez finalizada la operación nos despliega este mensaje de confirmación
44. Le damos aceptar

45. Nos dirigimos a la unidad y podemos ver que no hay ningún archivo y la unidad esta total mente vacío

46. Otra manera de verificar que se realizó el formateo
47. Nos vamos a la opción de propiedades
48. Podemos apreciar que la unidad solo ocupa 32.0kb
49. Este valor esta ocupado por datos almacenados por defectos de fábrica de la unidad de almacenamiento
50. Esto nos indica que no existe ningún archivo y el formateo fue realizado

TERCER FORMATEO

1. Para realizar el segundo formateo solicitado por el laboratorio debemos ingresar datos o archivos lo cual se realizará a continuación
2. Apreciamos que la unidad está completamente vacío debido al primer formateo
3. Procedemos a ingresar los datos pedidos por el laboratorio
4. Como podemos ver en la imagen podemos apreciar que son diferentes archivos y la cantidad de 10 archivos
5. Podemos apreciar que se tiene 10 elementos ingresados en la unidad de almacenamiento analizada en la auditoria
6. Una prueba que podemos realizar para la muestra de que se ingreso los elementos y archivos
7. Nos dirigimos a la unidad
8. Damos clic derecho y damos a propiedades
9. Podemos apreciar que se tiene 17.4Mb empleados
10. Es la cantidad que los archivos ocupan en la unidad de almacenamiento
11. Una ves verificado que se realizó la inserción de los archivos y el tamaño ocupado
12. Procedemos a formatear la unidad de almacenamiento como indica el laboratorio



Este equipo > HP V510M (D:)

Nombre Fecha de modificación Tipo Tamaño

Esta carpeta está vacía.

HP V510M (D:)

Nuevo Ordenar Ver

Este equipo > HP V510M (D:)

Acceso rápido

OneDrive

Este equipo

Descargas

Documentos

Escritorio

Imágenes

Música

Videos

Windows (C:)

HP V510M (D:)

Red

Nombre	Fecha de modificación	Tipo	Tamaño
Archivo1-2doFormateo	20/04/2023 20:34	Archivo PNG	33 KB
Tipo: Archivo PNG Tamaño: 32,7 KB Fecha de modificación: 20/04/2023 20:34	20/04/2023 19:40	Archivo MP3	5,910 KB
Archivo2-2doFormateo	20/04/2023 20:35	Archivo MP4	5,428 KB
Archivo3-2doFormateo	20/04/2023 20:34	Archivo PNG	34 KB
Archivo4-2doFormateo	20/04/2023 20:30	Microsoft Edge PD...	1,209 KB
Archivo5-2doFormateo	20/04/2023 20:34	Hoja de cálculo d...	14 KB
Archivo6-2doFormateo	20/04/2023 20:33	Presentación de M...	32 KB
Archivo7-2doFormateo	20/04/2023 20:33	Archivo WinRAR ZIP	148 KB
Archivo8-2doFormateo	20/04/2023 20:34	Archivo PNG	34 KB
Archivo9-2doFormateo	20/04/2023 20:30	Archivo WinRAR	4,992 KB

Archivo8-2doFormateo

Archivo9-2doFormateo

Archivo10-2doFormateo

10 elementos

HP V510M (D:)

14,8 GB disponibles de 14,8 GB

Propiedades de HP V510M (D:)

Uso compartido Personalizar

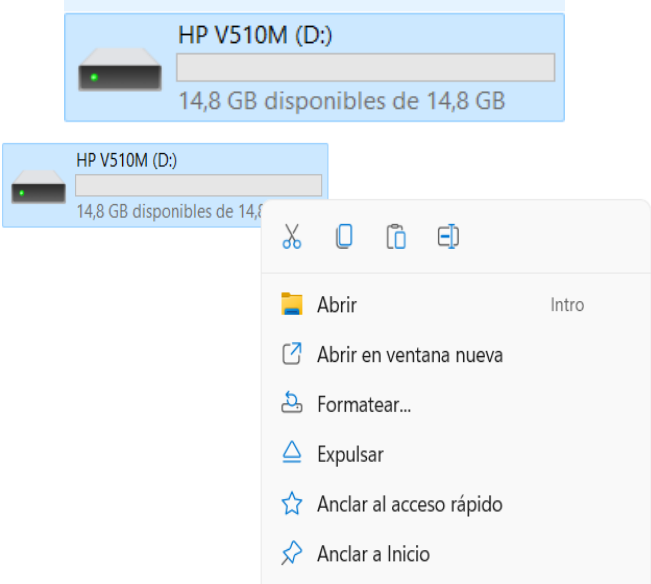
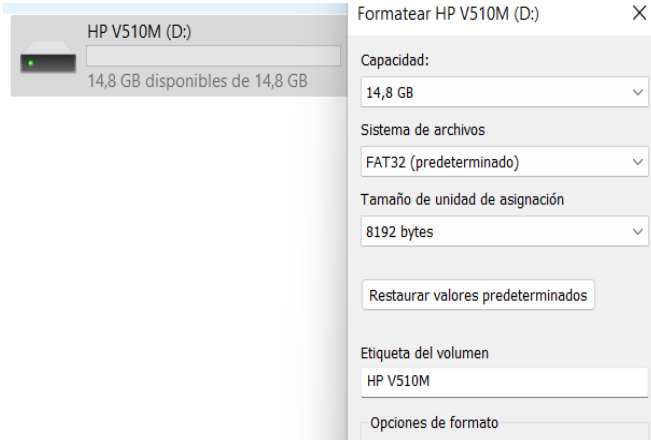
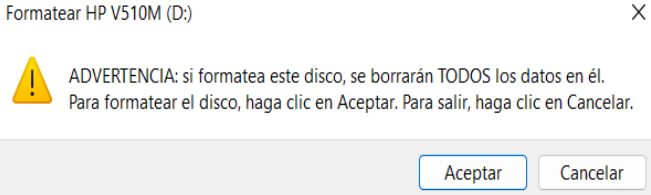
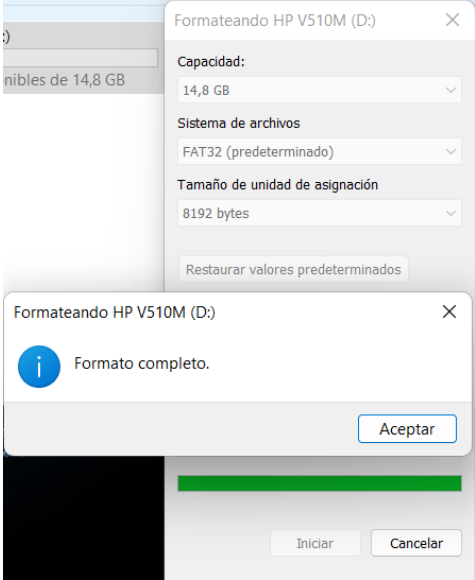
General Herramientas Hardware

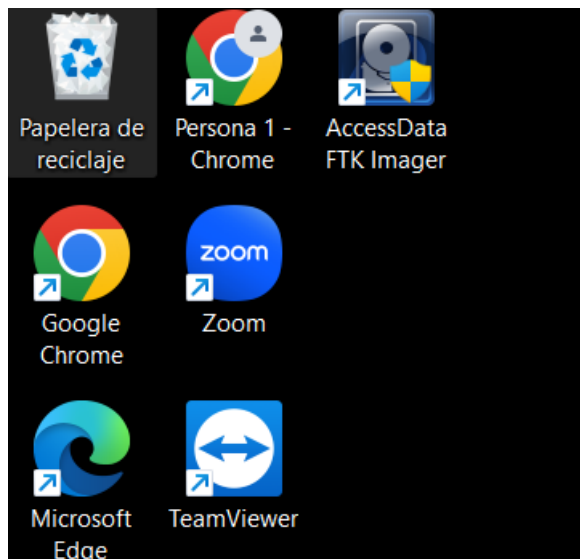
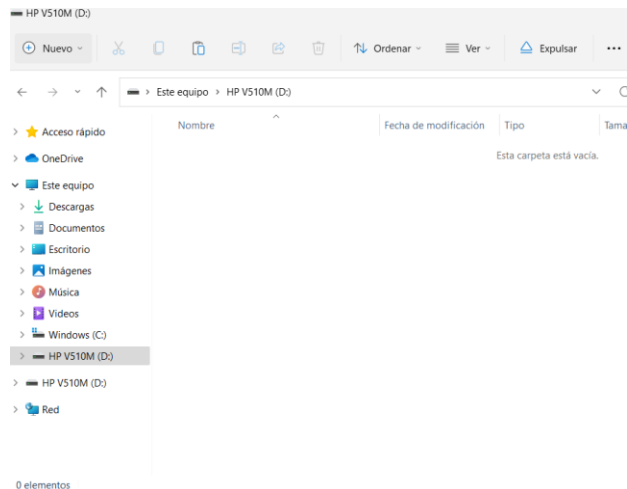
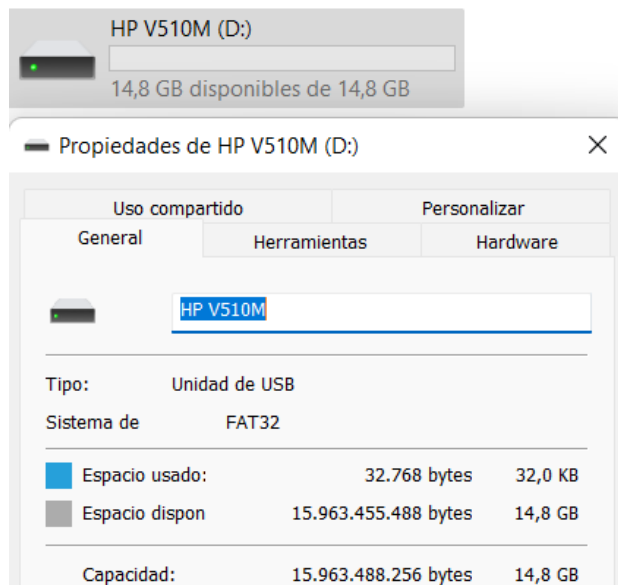
HP V510M

Tipo: Unidad de USB

Sistema de archivos: FAT32

	bytes	MB
Espacio usado:	18.333.696	17,4
Espacio dispon	15.945.154.560	14,8
Capacidad:	15.963.488.256	14,8

   	<p>13. En la imagen podemos ver a la unidad</p> <p>14. Para el proceso de formateo nos vamos la unidad</p> <p>15. Damos clic derecho</p> <p>16. Nos dirigimos a la opción de formatear</p> <p>17. Y nos desplegara una ventana</p> <p>18. Podemos apreciar la ventana desplegada donde nos da la información que lleva de fabrica la unidad de almacenamiento</p> <p>19. Para iniciar el proceso de formateo damos a la opción iniciar</p> <p>20. Nos despliega la siguiente venta de advertencia</p> <p>21. Donde indica que se realizara este proceso y se perderán los datos que se contiene</p> <p>22. Le damos aceptar</p> <p>23. El proceso empezara y esperamos que nos despliegue la ventana de confirmación de que la operación se realizo</p>
--	---



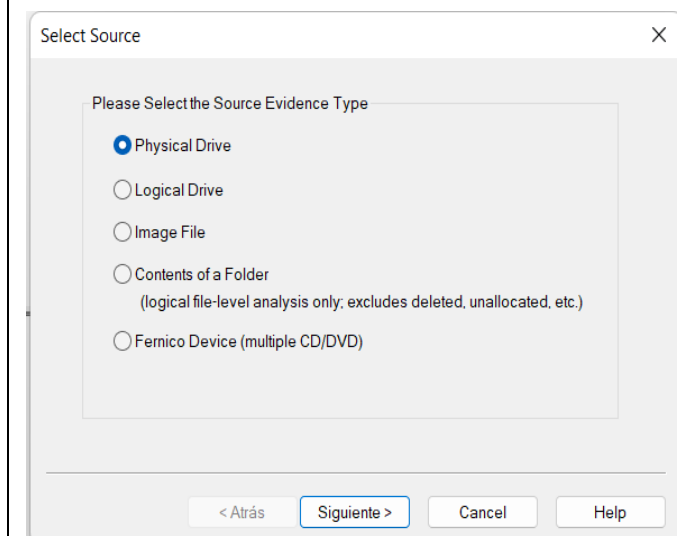
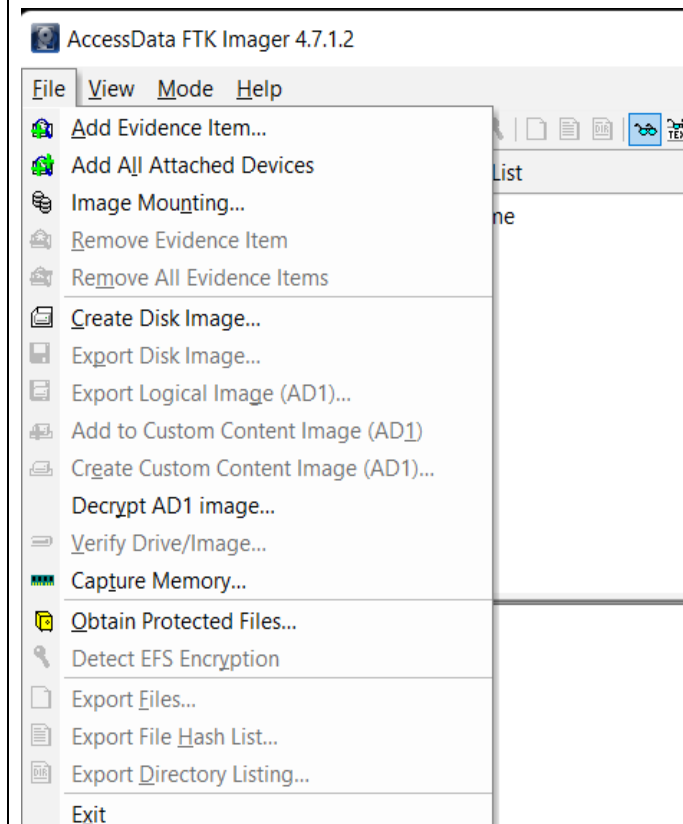
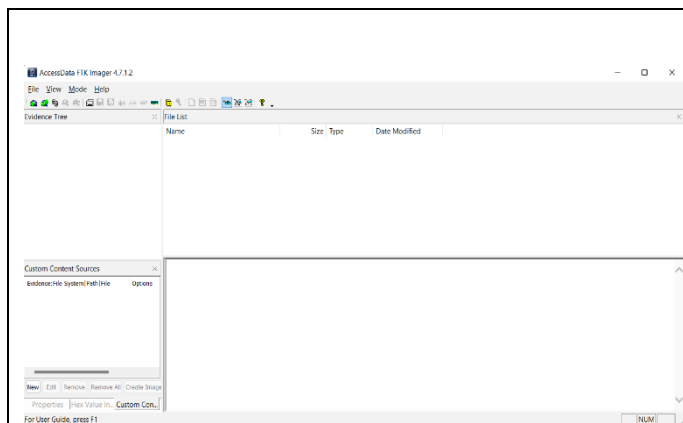
24. Para verificar que se realizó el proceso de formateo correctamente de la unidad de almacenamiento
25. Nos vamos a la unidad y damos clic derecho
26. Nos vamos a la opción de propiedades
27. En la ventana que nos despliega podemos ver que si realizó el proceso

28. Entrando a la unidad de almacenamiento podemos ver que la unidad esta vacío

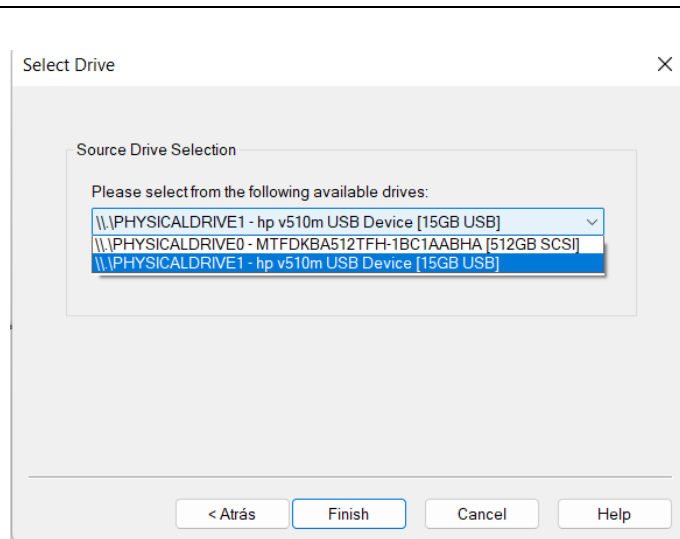
29. Una vez realizada la operación con los documentos nos vamos a trabajar para el proceso de recuperación de datos

TRABAJANDO CON FTK IMAGER

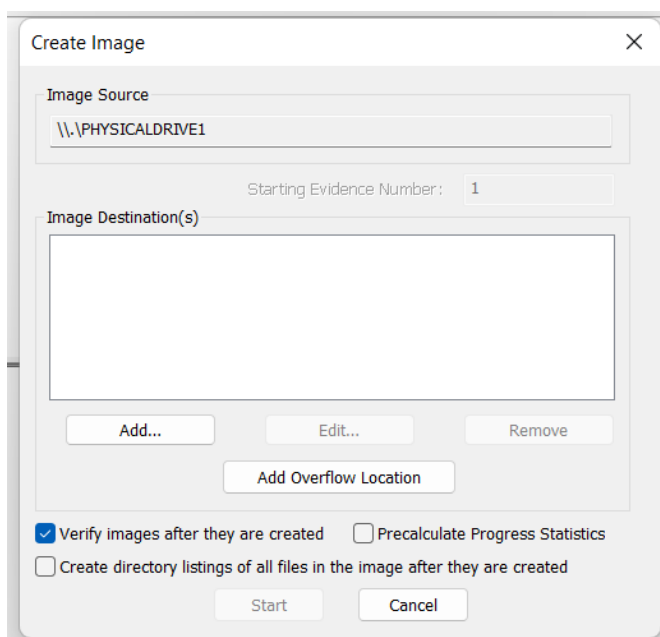
1. Nos vamos al icono que se crea en el escritorio de la aplicación y nos dirigimos para dar doble clic y entrar a la aplicación



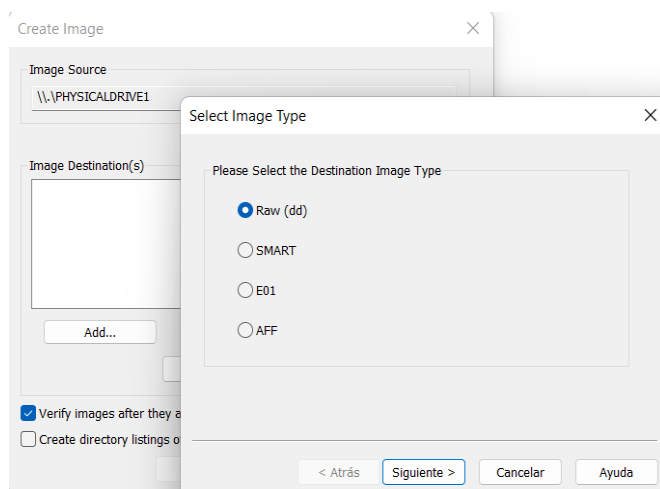
2. En la imagen podemos ver cómo es la aplicación una vez inicia
3. Para empezar a trabajar para la recuperación de datos realizamos el proceso de crear imagen de disco
4. Esto se realiza porque nunca se debe trabajar en la evidencia real y siempre en bueno realizar una imagen de la unidad
5. Para realizar el proceso de creación de imagen de disco
6. Nos dirigimos a la opción de FILE
7. Damos a la opción de CREATE DISK IMAGE
8. Seguidamente nos desplegará la ventana
9. En la imagen podemos apreciar la ventana que nos despliega
10. Elegimos la opción PHYSICAL DRIVE
11. Esta opción es la selección de la unidad de disco que se seleccionará para la creación de la imagen
12. Esto en español nos dice DISCO FISICO
13. Una vez seleccionado la opción damos a siguiente



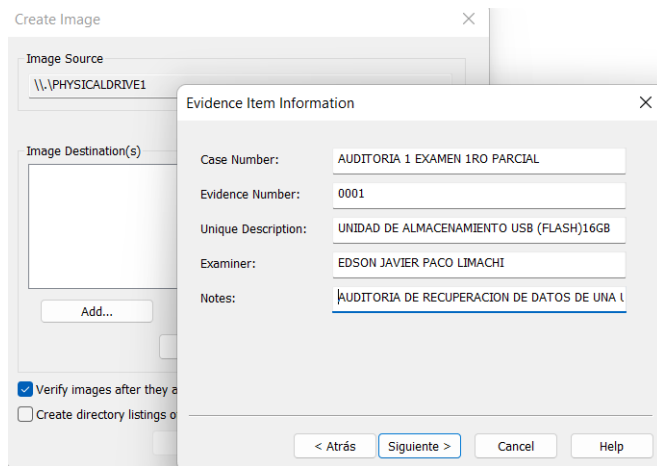
14. En este proceso nos reconoce las unidades de almacenamiento que se tiene en la computadora
15. Lo cual seleccionamos la opción de la USB
16. Una ves seleccionado le damos a FINALIZAR



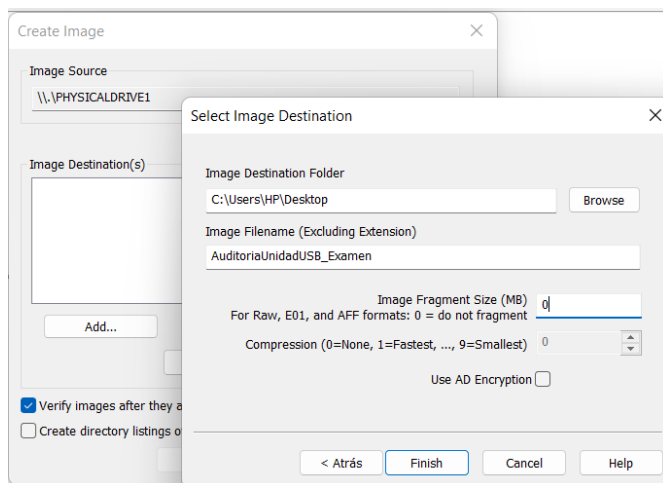
17. Nos desplegara la siguiente ventana y damos a la opción ADD
18. Esta opción nos permitirá seleccionar el tipo de imagen que se va a crear



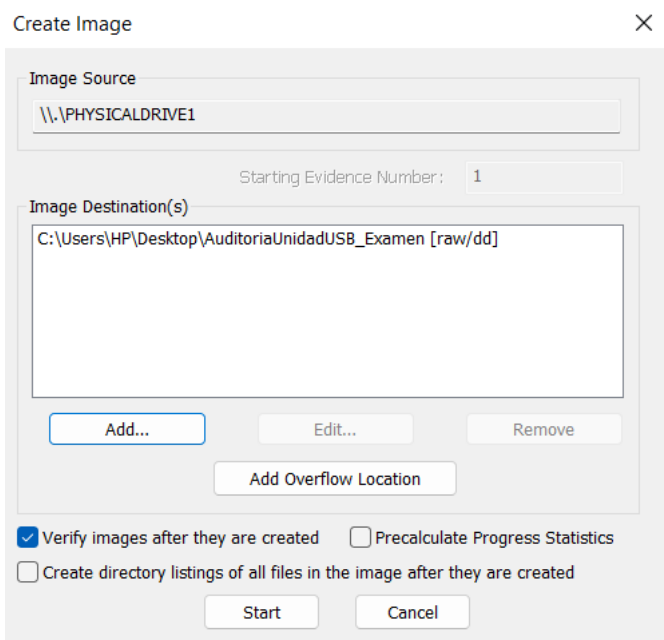
19. Nos da la siguiente ventana y seleccionamos la opción RAW
20. Escogeremos esta opción porque realiza una copia de bit a bit para la creación de la imagen
21. Una ves seleccionado le damos a la opción siguiente



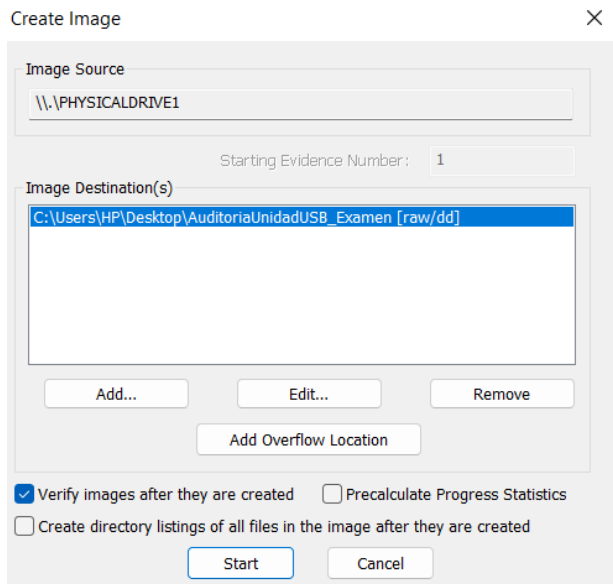
22. Nos despliega la siguiente ventana donde nos pide información para el ítem de la evidencia
23. Donde procedemos llenar la información
24. Una vez realizado el llenado respectivo
25. Damos a la opción SIGUIENTE



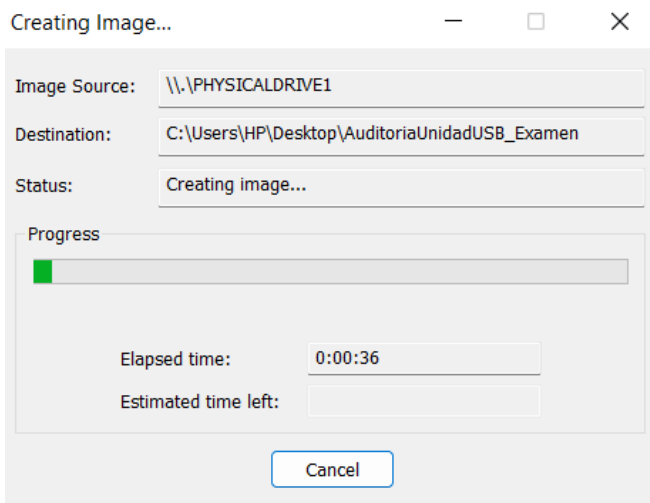
26. Una vez realizado la opción 25 nos despliega esta opción
27. Donde debemos seleccionar la ruta donde se guardará la imagen creada de la unidad USB
28. Nos pide dar el nombre de los archivos que se van a crear
29. La opción donde dice fragmento de imagen lo modificamos a 0
30. Porque analizaremos toda la unidad USB
31. Una vez realizado este paso y llenado de la información solicitada damos a la opción FINISH



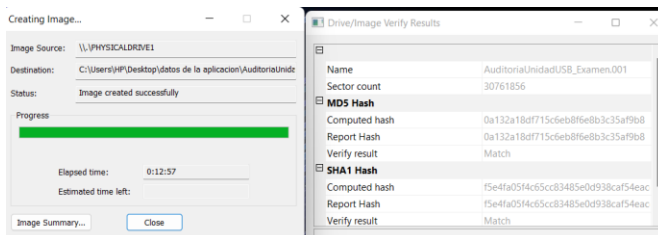
32. Se nos cerrara la ventana y se nos adiciona en la opción
33. Nos debe mostrar de la siguiente manera si todo fue realizado correctamente



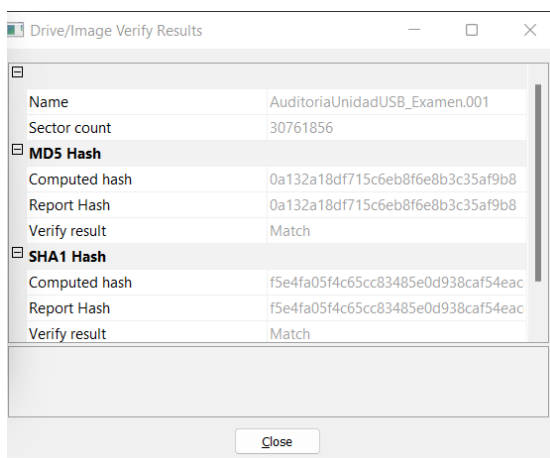
34. En este paso seleccionamos el destino de la imagen adicionada
35. Damos a la opción START



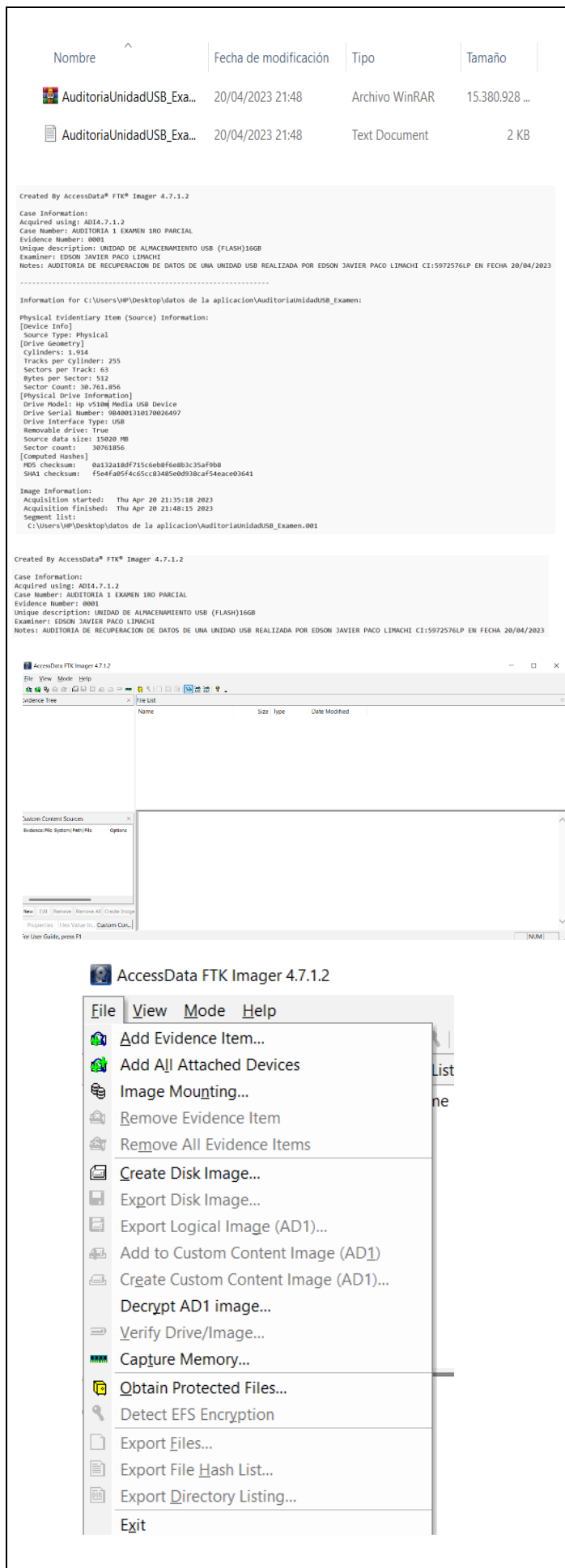
36. E iniciara el proceso de creación de la imagen del disco
37. En este caso la unidad de almacenamiento USB
38. Podemos apreciar la información que nos proporciona
39. Esperamos a que nos finalice la operación
40. Al finalizar la operación se inicia automáticamente el proceso de verificación



41. Una vez realizado la operación de creación nos despliega la venta de información



42. Este proceso nos indica los HASH creados para poder ver que no se realizó ninguna modificación y los archivos son una imagen y no tiene ningún cambio
43. Una vez verificado que HASH están correctos damos a clase

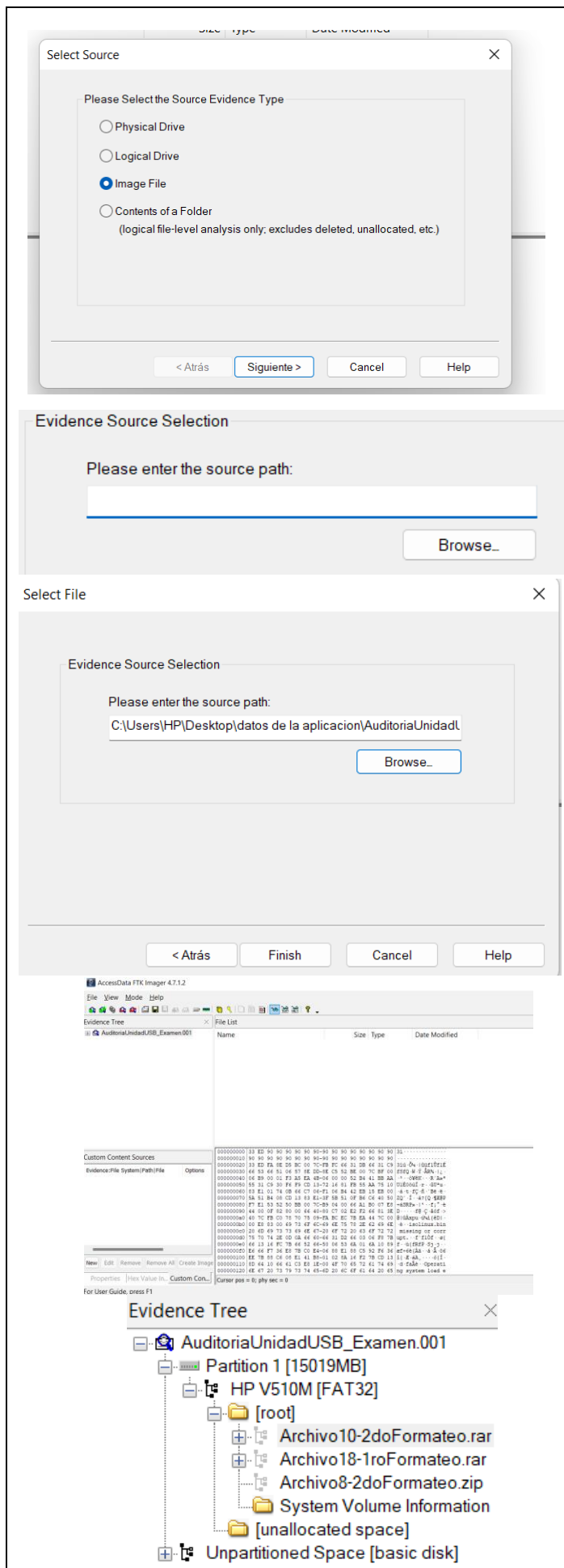


44. En aquí podemos ver los archivos creados
45. El archivo .RAR es la imagen
46. El archivo .txt es la información que nos proporciona la aplicación

47. En aquí podemos apreciar cómo nos indica la información fundamental y características del proceso

TRABAJANDO CON LA IMAGEN

1. Nos dirigimos a la herramienta y procedemos a ingresar la imagen de la unidad de almacenamiento para realizar el análisis y recuperación de datos
2. Para este proceso nos vamos a la opción FILE
3. Damos a la opción ADD EVIDENCE ITEM
4. Esto nos dice adicionar la evidencia



5. Nos da la siguiente opción y debemos seleccionar el tipo de archivo que se va a ingresar para el análisis
6. En este caso sería la opción de IMAGE FILE porque estamos trabajando con una imagen de la unidad creada anteriormente
7. Damos a la opción SIGUIENTE

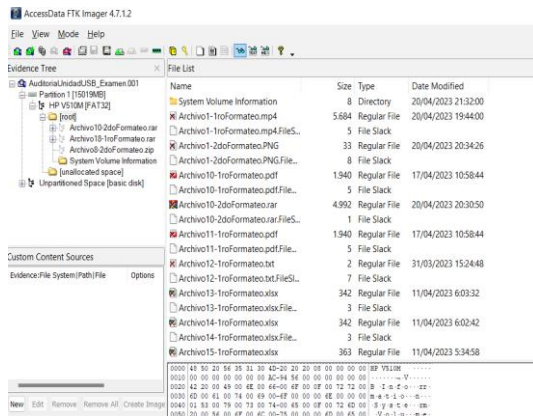
8. Nos despliega esta opción para poder seleccionar el archivo imagen

9. Seleccionamos la carpeta y el archivo de damos a la opción FINISH

10. Una nos importara la herramienta a la imagen de la unidad

11. Nos dirigimos a la sección donde dice EVIDENCE TREE

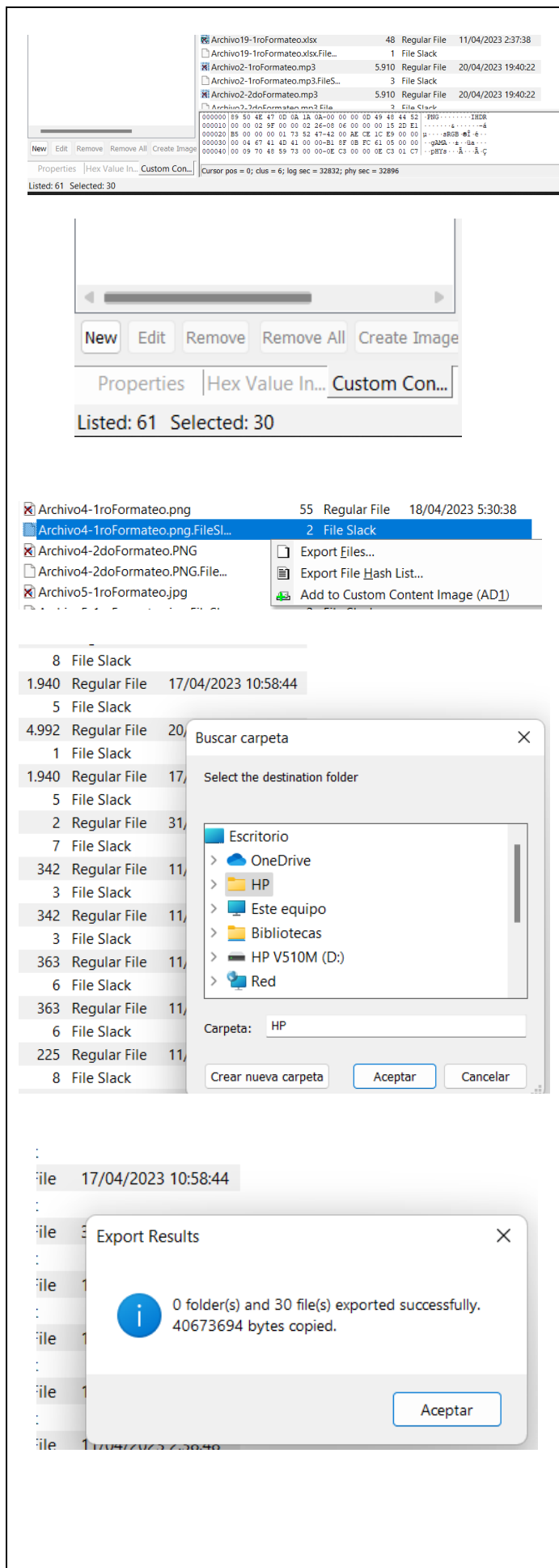
12. Le damos clic a la opción y nos despliega un árbol de opción como se ve en la imagen



Name	Size	Type	Date Modified
System Volume Information	8	Directory	20/04/2023 21:32:00
Archivo1-1roFormateo.mp4	5.684	Regular File	20/04/2023 19:44:00
Archivo1-1roFormateo.mp4.FileS...	5	File Slack	
Archivo1-2doFormateo.PNG	33	Regular File	20/04/2023 20:34:26
Archivo1-2doFormateo.PNG.File...	8	File Slack	
Archivo10-1roFormateo.pdf	1.940	Regular File	17/04/2023 10:58:44
Archivo10-1roFormateo.pdf.File...	5	File Slack	
Archivo10-2doFormateo.rar	4.992	Regular File	20/04/2023 20:30:50
Archivo10-2doFormateo.rar.FileS...	1	File Slack	
Archivo11-1roFormateo.pdf	1.940	Regular File	17/04/2023 10:58:44
Archivo11-1roFormateo.pdf.File...	5	File Slack	
Archivo12-1roFormateo.txt	2	Regular File	31/03/2023 15:24:48
Archivo12-1roFormateo.txt.FileS...	7	File Slack	
Archivo13-1roFormateo.xlsx	342	Regular File	11/04/2023 6:03:32
Archivo13-1roFormateo.xlsx.File...	3	File Slack	
Archivo14-1roFormateo.xlsx	342	Regular File	11/04/2023 6:02:42
Archivo14-1roFormateo.xlsx.File...	3	File Slack	
Archivo15-1roFormateo.xlsx	363	Regular File	11/04/2023 5:34:58
Archivo15-1roFormateo.xlsx.File...	6	File Slack	
Archivo16-1roFormateo.xlsx	363	Regular File	11/04/2023 2:38:48
Archivo16-1roFormateo.xlsx.File...	6	File Slack	
Archivo17-1roFormateo.xlsx	225	Regular File	11/04/2023 2:38:06
Archivo17-1roFormateo.xlsx.File...	8	File Slack	
Archivo18-1roFormateo.rar	214	Regular File	10/04/2023 19:31:56
Archivo18-1roFormateo.rar.FileS...	3	File Slack	
Archivo19-1roFormateo.xlsx	48	Regular File	11/04/2023 2:37:38
Archivo19-1roFormateo.xlsx.File...	1	File Slack	
Archivo2-1roFormateo.mp3	5.910	Regular File	20/04/2023 19:40:22
Archivo2-1roFormateo.mp3.FileS...	3	File Slack	
Archivo2-2doFormateo.mp3	5.910	Regular File	20/04/2023 19:40:22
Archivo2-2doFormateo.mp3	5.910	Regular File	20/04/2023 19:40:22
Archivo2-2doFormateo.mp3.File...	3	File Slack	
Archivo20-1roFormateo.xlsx	225	Regular File	10/04/2023 22:23:24
Archivo20-1roFormateo.xlsx.File...	8	File Slack	
Archivo3-1roFormateo.docx	24	Regular File	19/04/2023 7:05:16
Archivo3-1roFormateo.docx.File...	1	File Slack	
Archivo3-2doFormateo.mp4	5.428	Regular File	20/04/2023 20:35:30
Archivo3-2doFormateo.mp4.File...	5	File Slack	
Archivo4-1roFormateo.png	55	Regular File	18/04/2023 5:30:38
Archivo4-1roFormateo.png.FileS...	2	File Slack	
Archivo4-2doFormateo.PNG	34	Regular File	20/04/2023 20:34:26
Archivo4-2doFormateo.PNG.File...	7	File Slack	
Archivo5-1roFormateo.jpg	23	Regular File	18/04/2023 5:27:40
Archivo5-1roFormateo.jpg.FileS...	2	File Slack	
Archivo5-2doFormateo.pdf	1.209	Regular File	20/04/2023 20:30:00
Archivo5-2doFormateo.pdf.FileS...	8	File Slack	
Archivo6-1roFormateo.png	55	Regular File	18/04/2023 5:18:50
Archivo6-1roFormateo.png.FileS...	2	File Slack	
Archivo6-2doFormateo.xlsx	14	Regular File	20/04/2023 20:34:26

13. Nos vamos a la opción ROOT
14. Y nos despliega todos los archivos que podemos recuperar
15. Para lo cual procedemos a recuperar y buscar los archivos perdidos en el formateo

16. Procedemos a seleccionar los archivos que queremos recuperar

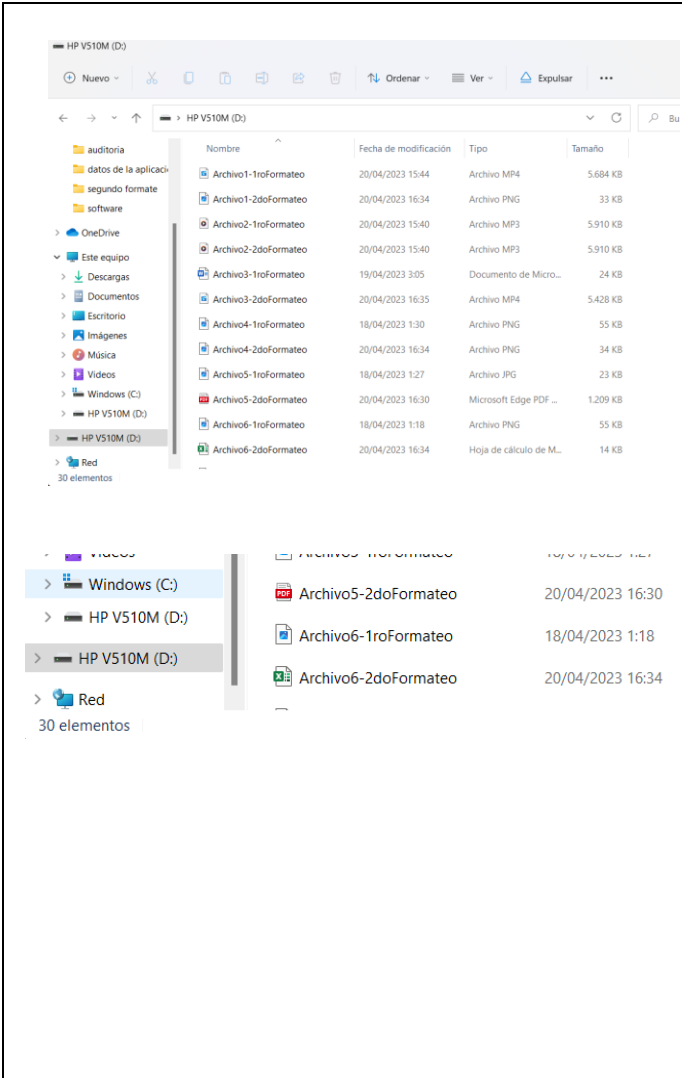


17. En aquí podemos apreciar como seleccionamos los 30 datos perdidos
18. Y recuperaremos todos los archivos

19. Seleccionamos los archivos y damos clic derecho
20. Nos vamos a la opción EXPORT FILES

21. Nos pide seleccionar el destino de exportación de datos

22. Nos da el mensaje de confirmación de la cantidad de archivos recuperados y nos vamos a la unidad



23. Podemos ver aquí que se nos recuperó los archivos

24. Podemos ver la cantidad de archivos que se recuperaron

25. Como conclusión se realizó la recuperación del 100% de datos

26. El total de perdida de datos en los procesos de formateos es de 30 datos

27. Y ahora al finalizar se recuperó 30 datos

REPORTE Y/O CONCLUSIONES

como conclusión tenemos que la herramienta FTK IMAGER nos ayuda a recuperar datos perdidos por diferentes factores
aparte de recuperar los datos nos ayuda a tener una certeza de la confiabilidad y veracidad de los datos con la creación de HASH y con la verificación de datos en el proceso de crear una imagen
cabe resaltar que nos ayuda con la información fundamental proporcionada como ser los datos del hardware analizado como sus seriales fabricante, tamaño de almacenamiento y demás