|  |  |  |  |
| --- | --- | --- | --- |
| Casa&Hogar - Home | FacebookC:\Users\Enrique\Pictures\descarga.jpg | **INGENIERÍA DE SISTEMAS** | | **P**  **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** |
|  | 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}   1. Ir a la carpeta descargada y dar clic al ejecutable 2. Seguido nos aparece la siguiente pantalla 3. Le damos a *NEXT* para continuar con la instalación 4. Nos dará la siguiente ventana 5. Le damos a la opción de aceptar términos y condiciones 6. Es recomendable realizar una pequeña lectura a los términos y condiciones para informarnos 7. Seguido de NEXT 8. Seleccionamos la ruta de donde se instalará los paquetes 9. Ya viene una ruta por defecto se puede dejar ahí o 10. Le damos a NEXT 11. Una vez completada los demás pasos damos a opción INSTALL 12. El proceso de instalación se realizará 13. Cuando se finalice damos a la opción FINISH  Primer formateo  1. Podemos apreciar la unidad extraíble USB 2. 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 3. Podemos ver que al momento de realizar el formateo nos da las advertencias 4. Le damos aceptar y el proceso se inicia 5. Esperamos a que se finalice el formateo y nos de un mensaje como el que podemos apreciar  Segundo formateo  1. Una vez realizado el proceso nos procedemos a llenar de diferentes archivos la unidad USB para el primer formateo 2. Como manda la guía primero realizamos la inserción de 20 archivos con el respectivo nombre “Archivo1-1roFormate” 3. En la imagen que apreciamos podemos ver la cantidad de elementos que se inserto 4. Cabe destacar que son diferentes tipos de archivos los ingresados a la memoria USB 5. Podemos apreciar en la imagen en el contador de documentos 6. Nos muestra 20 elementos en la unidad USB 7. Cumpliendo la condición del laboratorio 8. En la imagen podemos ver una muestra las propiedades de la unidad de almacenamiento 9. Apreciamos que se tiene ocupado 21.4 Mb del espacio total 10. Cabe destacar que no es muy grande porque los archivos ingresados no tienen ocupan mucho espacio 11. Esto se realizo para acelerar el proceso de recuperación 12. Ya que a mas datos que analizar y mas memoria de la unidad será más demoroso el proceso de análisis 13. En la imagen podemos ver la unidad 14. Siguiendo la condición del laboratorio procedemos a formatear la unidad USB 15. Por lo cual nos vamos a la unidad le damos clic derecho 16. No vamos a la opción de formatear 17. Al realizar le paso 36 nos despliega esta ventana por lo siguiente 18. Nos mostrara la configuración de la unidad 19. Para que realiza el proceso de formateo de la unidad 20. Damos a la opción INICIAR 21. Al realizar el paso 40 nos despliega una advertencia 22. Lo cual procedemos a leer y damos ACEPTAR 23. Una vez finalizada la operación nos despliega este mensaje de confirmación 24. Le damos aceptar 25. Nos dirigimos a la unidad y podemos ver que no hay ningún archivo y la unidad esta total mente vacío 26. Otra manera de verificar que se realizó el formateo 27. Nos vamos a la opción de propiedades 28. Podemos apreciar que la unidad solo ocupa 32.0kb 29. Este valor esta ocupado por datos almacenados por defectos de fábrica de la unidad de almacenamiento 30. 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 13. En la imagen podemos ver a la unidad 14. Para el proceso de formateo nos vamos la unidad 15. Damos clic derecho 16. Nos dirigimos a la opción de formatear 17. Y nos desplegara una ventana 18. Podemos apreciar la ventana desplegada donde nos da la información que lleva de fabrica la unidad de almacenamiento 19. Para iniciar el proceso de formateo damos a la opción iniciar 20. Nos despliega la siguiente venta de advertencia 21. Donde indica que se realizara este proceso y se perderán los datos que se contiene 22. Le damos aceptar 23. El proceso empezara y esperamos que nos despliegue la ventana de confirmación de que la operación se realizo 24. Para verificar que se realizo 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 realizo 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 ftkimager    1. Nos vamos al icono que ser 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 desplegara 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 seleccionara 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 ves 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 LAIMAGEN  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 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 formarte 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