ANÁLISIS FORENSE PARA LA RECUPERACIÓN DE INFORMACIÓN EN PENDRIVE

Judy Andrea Giraldo Ramírez

Tecnología en Sistemas de Información

Director

Gabriel Taborda Blandón

INSTITUTO TECNOLÓGICO METROPOLITANO

Julio 10 de 2016

RESUMEN

El pendrive, mejor conocido como memoria USB (bus serie universal), es un dispositivo portátil para el almacenamiento, el transporte y la transferencia de información digital, es muy práctico de usar para mantener y leer dicha información. El pendrive es actualmente uno de los dispositivos más utilizado por los usuarios de ordenadores para estos fines; es importante tener en cuenta que el pendrive está expuesto a fallas accidentales o inducidas (físicas o lógicas ambas), que provocan la pérdida de datos. Hay una gran cantidad de software de recuperación de datos para dispositivos de almacenamiento, pero la mayoría de usuarios no lo conocen y este desconocimiento puede generar confusión en los usuarios al momento de definir cuál utilizar. Cuando el dispositivo tiene un daño lógico inducido o accidental, los datos podrán ser recuperados a través de técnicas de software. Hay desinformación acerca de la informática forense, cuando el dispositivo presenta daño inducido se debe hacer el análisis sobre una copia de dicho dispositivo para conservar la evidencia. El objetivo principal de este proyecto es realizar un análisis detallado del software de recuperación de datos y hacer una valoración de las herramientas, proponer una guía metodológica para recuperar total o parcialmente la información contenida en el pendrive o de ser posible la funcionalidad del dispositivo físico.

Palabras claves: Dispositivos digitales, Informática forense, análisis forense, recuperación de información, USB, memoria flash, herramientas, técnicas, métodos, recuperación de datos.

ABSTRACT

The Pen drive, flash drive or USB (Universal Serial Bus) memory, is a portable device used for storing, transporting and transferring digital information, and it is currently one of the most used devices by computer users for these purposes. These devices are constantly exposed to accidental or induced failure, both physical and logical, which causes data losses. There are a lot of software packages for data recovery in damaged storage devices, and this profuse availability causes difficulties at the moment to decide which software to use. When the device has a logical damage, either accidental or induced, data may be recovered through software techniques. There are disinformation about computer forensics, When the device has a premeditated damage the data recovery must be done in a copy of the device to preserve the evidence, The aim of the project is to make a detailed analysis of the data recovery software and to do an evaluation of these, to propose a methodological guide of recovery all or part of the information contained in the pendrive, if possible the functionality of the device.

Key words: *digital devices, computer forensics, forensic analysis, information retrieval, USB, flash memory, tools, techniques, methods, data recovery.*

RECONOCIMIENTOS

Me gustaría que estas líneas sirvieran para expresar mi más profundo y sincero agradecimiento a todas aquellas personas que con su ayuda han colaborado en la realización del presente proyecto, en especial a Gabriel Taborda Blandón, director de esta investigación, por la orientación, el seguimiento y la supervisión continúa de la misma. Especial reconocimiento merece el interés mostrado por mi trabajo y las sugerencias recibidas de Gustavo Varón Beltrán, con el que me encuentro en deuda por el ánimo infundido y la confianza en mí depositada.

Un agradecimiento muy especial merece la comprensión, paciencia y el ánimo recibidos de mi familia y amigos.

A todos ellos, muchas gracias

ACRÓNIMOS

- **APA** American Psychological Association
- **BIOS** Basic Input/Output System
- **CD** Compact Disc
- **CMD** Command Prompt
- **DVD** Disco Versátil Digital
- **ECC** Error correcting code
- **ExFAT** Extended File Allocation Table
- **FAT** File Allocation Table
- **HSPA** High Speed Packet Access
- **IBM** International Business Machines
- **ISO** International Organization for Standardization
- **LBA** Logical Block Addressing
- **LED** light-emitting diode
- **NIP** Número de Identificación Personal
- **NTFS** New Technology File System
- **OS** Operating System
- **PBC** Printed Circuit Board
- **POST** Power On Self Test
- **RAM** Random Access Memory
- **RISC** Reduced Instruction Set Computer
- **ROM** Read Only memory
- **SRAM** Static Random Access Memory
- **URL** Uniform Resource Locator
- **USB** Universal Serial Bus

CONTENIDO

RESUMEN ii

1. INTRODUCCIÓN 1

1.1. Planteamiento del Problema 1

1.2. Objetivo General 2

1.3. Objetivos Específicos 2

1.4. Organización del trabajo 3

2. MEDIOS DE ALMACENAMIENTO DE INFORMACIÓN 4

2.1 Dispositivos de Almacenamiento por Medio Magnético 5

2.1.1 Cinta Magnética 5

2.1.2 Tambor Magnético 5

2.1.3 Disco Duro 5

2.1.4 Disquete o Disco flexible 5

2.2 Dispositivos de Almacenamiento por Medio Óptico: 6

2.2.1 CD-R 7

2.2.2 CD-RW 7

2.2.3 DVD-ROM 7

2.2.4 DVD-RAM 7

2.2.5 Blu-ray 7

2.3 Dispositivos de Almacenamiento por Medio Electrónico-digital: 9

2.3.1 RAM 9

2.3.2 SRAM 9

2.3.3 ROM 9

2.3.6 Tarjeta de memoria digital 10

2.3.8 Disco duro de estado sólido 10

2.3.7 Pendrive 10

2.4 Historia y aspectos técnicos del pendrive 12

2.4.1 Historia del Pendrive 12

2.4.2 Características y funcionamiento del pendrive 14

2.4.3 Memoria Flash 15

2.4.4 Partes físicas del pendrive 21

2.4.5 Estructura lógica del pendrive 23

2.4.6 Usos comunes de un pendrive 25
2.4.7. Pérdida de información 26
2.4.8 Daños o errores comunes del pendrive 29
2.4.9 Avances en el pendrive 30
3. SEGURIDAD INFORMÁTICA, ANÁLISIS FORENSE Y PENDRIVE 33
3.1. Generalidades sobre seguridad informática 33
3.1.1 Una definición de seguridad informática 34
3.1.2 Una definición de Análisis forense o Informática Forense. 36
3.1.3 Análisis en caliente 38
3.1.4. Análisis en frío 39
3.1.5 Evidencia digital 39
3.1.6. Cadena de custodia 40
3.1.7 Captura de Imágenes de un Pendrive 41
3.1.8. Herramientas para informática forense 42
3.1.9. Descripción de algunas herramientas de recuperación de información 43
3.2 Recuperación de datos en dispositivos de almacenamiento 53
3.2.1 Métodos de recuperación en discos duro 54
3.2.2 Métodos para recuperación tanto discos duros como pendrives 66
3.2.3 Métodos para recuperar información en pendrive con daño inducido o accidental 70
4. METODOLOGÍA Y RESULTADOS 82
4.1 Etapa 1: Revisión bibliográfica 82
4.2 Etapa 2: Análisis de la revisión bibliográfica 84
4.3 Etapa 3: Evaluación de herramientas 92
4.4 Etapa 4: Elección de 2 herramientas para pruebas de recuperación de información 98
4.5 Etapa 5: Guía metodológica de recuperación de la información contenida en pendrives 119
5. CONCLUSIONES, RECOMENDACIONES Y TRABAJO FUTURO 124
5.1 Conclusiones 124
5.2 Recomendaciones 126
5.3 Trabajo futuro 129
REFERENCIAS 130

ÍNDICE DE TABLAS

Pág.

Tabla 1: Dispositivos de almacenamiento magnéticos 6

Tabla 2: Dispositivos de almacenamiento ópticos 8

Tabla 3: Dispositivos de almacenamiento electrónico-digitales 11

Tabla 4: Formato predeterminado del sistema de archivos 15

Tabla 5: Usos de las memorias flash NOR y NAND 19

Tabla 6: Componentes internos del pendrive 22

Tabla 7: Tabla de particiones 24

Tabla 8: Herramientas para recuperar información 85

Tabla 9: Métodos para recuperar información en pendrive 91

Tabla 10: Top ten representativo de herramientas 92

Tabla 11: Resultado de la prueba por comunidades profesionales 98

Tabla 12: Sinopsis de las herramientas elegidas para pruebas 99

Tabla 13: Procedimiento inicial de restauración 120

Tabla 14: Casos de daño y herramienta aplicable 122

Tabla 15: Herramientas para proteger y prevenir daños de pendrive 127

ÍNDICE DE IMÁGENES

Pág.

Imagen 1: Memoria flash 16
Imagen 2: Estructura Memoria flash NAND 17
Imagen 3: Memoria flash NOR 18
Imagen 4: Memoria flash NAND 19
Imagen 5: Estructura sector de arranque 23
Imagen 6: Captura iniciación Parted Magic OS 54
Imagen 7: Captura Ejecución TestDisk 55
Imagen 8: Lado Externo de disco duro 56
Imagen 9: Disco duro IDE y SATA 57
Imagen 10: Disco duro PATA (IDE) 57
Imagen 11: Disco duro PATA EIDE 57
Imagen 12: Controlador PCI 57
Imagen 13: Adaptador Externo de disco 58
Imagen 14: Disco duro conectado a otro equipo 58
Imagen 15: Diagrama del primer método 59
Imagen 16: Tarjeta controladora de disco duro 60
Imagen 17: Discos duros del mismo modelo 60
Imagen 18: Tarjeta controladora externa 60
Imagen 19: Tarjeta controladora 61
Imagen 20: Tarjeta controladora conectada 61
Imagen 21: Diagrama del segundo método 63
Imagen 22: Ilustración de una imagen de disco 63
Imagen 23: Captura del comando CHKDSK 63
Imagen 24: Opciones para uso del comando CHKDSK 64
Imagen 25: Diagrama del tercer método 64
Imagen 26: Captura ejecución Photorec 65
Imagen 27: Captura Data Recovery wizard 66
Imagen 28: Captura elección unidad 67
Imagen 29: Captura Pandore Recovery 68

ÍNDICE DE IMÁGENES

Pág.

Imagen 30: Captura ejecución Foremost 69
Imagen 31: Pines del conector del pendrive 72
Imagen 32: Resistencia fusible 73
Imagen 33: Cristal de cuarzo de un pendrive 74
Imagen 34: Captura Ejecución Diskpart 77
Imagen 35: Captura ejecución R-Studio 79
Imagen 36: Iniciación de recuperación con R-Studio 79
Imagen 37: Resultado de la prueba realizada por PcaLab 94
Imagen 38: Pendrive utilizado en la prueba piloto 1 99
Imagen 39: Captura de descarga Recuva 100
Imagen 40: Captura de versión Recuva 100
Imagen 41: Captura de pantalla de inicio de descarga Recuva 100
Imagen 42: Captura de instalación de Recuva 101
Imagen 43: Captura asistente de instalación Recuva 101
Imagen 44: Captura de opciones de instalación Recuva 101
Imagen 45: Captura de progreso de instalación de Recuva 102
Imagen 46: Captura de inicialización asistente de recuperación de archivos 102
Imagen 47: Captura de tipos de archivos a recuperar 102
Imagen 48: Captura de destino de los archivos recuperados 103
Imagen 49: Captura de iniciación de búsqueda de información 103
Imagen 50: Captura de búsqueda de archivos 103
Imagen 51: Captura de pantalla de archivos a recuperar 104
Imagen 52: Captura archivos diferenciados por color identifica posibilidad de recuperación 104
Imagen 53: Captura de pantalla de marcación de archivos 105
Imagen 54: Captura de pantalla de selección de destino para los archivos recuperados 105

Imagen 55: Captura de pantalla de resultados de la prueba con Recuva 105
Imagen 56: Captura de pantalla de visualización de archivos recuperados con Recuva 106
Imagen 57: Captura de visualización de descarga de diskdrill 107
Imagen 58: Captura de inicialización de instalación de disk drill 107
Imagen 59: Captura de progreso de instalación disk drill 107
Imagen 60: Captura elección de unidad a analizar 108
Imagen 61: Captura tipo de escaneo 108
Imagen 62: Captura ubicación destino de los archivos a recuperar 109
Imagen 63: Captura marcación y recuperación de archivos 109
Imagen 64: Captura resultados de la herramienta diskdrill 110
Imagen 65: Captura de archivos recuperados por Diskdrill 110
Imagen 66: Resultado según Recuva 111
Imagen 67: Resultado según DiskDrill 111
Imagen 68: Pendrive utilizado en la prueba piloto 2 111
Imagen 69: Captura de actualización de software de controladores 112
Imagen 70: Captura cambio de letra y ruta de acceso a la unidad 113
Imagen 71: Captura resultados de la herramienta usb Show 114
Imagen 72: Captura ejecución remo recover 114
Imagen 73: Captura prueba realizada con remo recover 115
Imagen 74: Captura destino para archivos a recuperar 115
Imagen 75: Captura resultados de recover 115
Imagen 76: Captura archivos encontrados por diskdrill 116
Imagen 77 Captura marcación de archivos a recuperar 116
Imagen 78 Captura selección de destinos para los archivos a recuperar 117
Imagen 79 Captura resultados de Diskdrill 117

1.INTRODUCCIÓN

La información es considerada como el activo más valioso de toda organización cualesquiera que sean sus objetivos sociales, de tal forma que si se perdiera, su recuperación justifica cualquier esfuerzo. El pendrive o memoria USB, es un dispositivo portátil de almacenamiento y transporte de información, muy cómodo, práctico y fácil de usar, compuesto por una memoria flash, accesible a través de un puerto USB, proporciona comodidad y conveniencia en el manejo de la información, especialmente para aquellas personas de negocios que viajan constantemente, por su manera segura y conveniente de transportar datos y almacenar archivos importantes sin recurrir a la nube, v.gr. servicio Dropbox.

Las ventajas que poseen estos dispositivos son: bajo costo, tamaño reducido, alta capacidad, confiabilidad y facilidad de transporte, entre otras.

Estos dispositivos están expuestos a daños accidentales o inducidos que pueden ocasionar pérdida de datos. No es frecuente un respaldo o copia de ellos. Los afectados comúnmente no recurren a un método formal, la mayoría de usuarios desconocen los mecanismos para recuperar la información almacenada que por incidente alguno se ha perdido; el análisis forense enfocado a la recuperación de información a través de herramientas y procedimientos establecidos, es una alternativa viable.

1.1. Planteamiento del Problema

El pendrive al ser móvil, es susceptible a deteriorarse en el trasporte con mucha facilidad, los daños a que está expuesto son impredecibles y en muchos casos, incontrolables, las causas de la pérdida de información almacenada en dicho dispositivo son muchas y variadas: fallas de software, malware, daño accidental o provocado, este último con

intenciones de destruir o eliminar evidencias. La información puede ser ocultada, eliminada por completo y el dispositivo físico dañado.

Surgen las siguientes preguntas de reflexión sobre el problema.

¿Qué sucedería si se daña el medio donde se almacena la información?

¿Cuándo se daña el pendrive por causas accidentales o no, ocasionando pérdida de información; saben los usuarios qué hacer para recuperarla?

¿Saben los usuarios que mecanismos métodos y herramientas aplicar cuando hay daño lógico, falla en el firmware o en el sistema de archivos o ataques de malwares?

1.2.Objetivo General

Realizar una investigación formativa en el semillero de seguridad informática en la línea de análisis forense para proponer una guía metodológica con las herramientas empleadas para recuperación de información en pendrive, con daño inducido o accidental, que permita la recuperación total o parcial de la información y de ser posible la del dispositivo físico.

1.3.Objetivos Específicos

- Realizar un estado del arte sobre el funcionamiento, la estructura y posibles daños del pendrive.
- Hacer un estado del arte sobre el análisis forense enfocado a la recuperación de información en medios de almacenaje extraíbles, incluido el pendrive.
- Realizar un análisis crítico de los métodos y herramientas para la recuperación de la información en pendrive.
- Efectuar una prueba piloto con 2 herramientas seleccionadas.

- Elaborar criterios generales sobre una guía de recuperación de información en pendrive.

1.4.Organización del trabajo.

El capítulo 1 contiene la definición y planteamiento del problema y su objeto. Se elabora y presenta la problemática que implica la pérdida de información, se formula y analiza el problema planteado y se define el porqué de la investigación y cuál es el objetivo que se pretende alcanzar con la realización de este proyecto.

El capítulo 2 presenta los diferentes medios de almacenamiento de información: magnéticos, ópticos y electrónicos-digital, con referencia especial del pendrive, se presenta de manera detallada el dispositivo, su historia y aspectos técnicos, características, funcionamiento, estructura física y logica, usos, avances y daños.

El capítulo 3 enuncia el aspecto teórico de la seguridad informática, se hace una introducción a los métodos y herramientas comúnmente aplicadas para el proceso de recuperación de información.

En el capítulo 4 se describe y aplica la metodología adoptada para el desarrollo del proyecto, como un resultado, se anexa una tabla resumen de herramientas que se espera sea de gran utilidad, una tabla con las diez más relevantes, de las cuales se escogen dos para pruebas, y para finalizar se propone una metodología.

En el capítulo 5 se presentan las conclusiones, las recomendaciones relacionadas y las orientadas al trabajo futuro a las que se llega con la investigación realizada.

2.MEDIOS DE ALMACENAMIENTO DE INFORMACIÓN

Los dispositivos de almacenamiento de información son "*máquinas o sistemas capaces de desarrollar ciertas acciones como guardar a largo plazo información generada por los usuarios, sin importar el origen u objetivos de tales datos, facilitando así, el transporte de información y la distribución de la misma en distintos equipos. Además de eso, también auxilian como herramientas de almacenamiento seguro de datos, es decir respaldos o backups*". (Peña, 2015), (Hilari, 2006, párr. 6).

La información se puede definir como la "*Comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada. Puede ser privilegiada: que por referirse a hechos o circunstancias que otros desconocen, puede generar ventajas a quien dispone de ella*" (Rae, 2015)

Según Idalberto Chiavenato. (s.f) información es *"un conjunto de datos con un significado, o sea, que reduce la incertidumbre o que aumenta el conocimiento de algo. En verdad, la información es un mensaje con significado en un determinado contexto, disponible para uso inmediato y que proporciona orientación a las acciones por el hecho de reducir el margen de incertidumbre con respecto a nuestras decisiones*"

Existe una gran variedad de dispositivos destinados al almacenamiento de información, tales como magnéticos, ópticos y electrónicos-digital los cuales se clasifican de acuerdo a sus principios de almacenamiento así:

2.1 Dispositivos de Almacenamiento por Medio Magnético

Son los más antiguos y utilizados a gran escala. Los dispositivos magnéticos son aquellos dispositivos de almacenamiento de datos en los que se utilizan propiedades magnéticas para almacenar información digital.

2.1.1 Cinta Magnética

Está formada por una cinta de material plástico recubierta de material ferromagnético, sobre dicha cinta se registran los caracteres en formas de combinaciones de puntos, sobre pistas paralelas al eje longitudinal de la cinta. Estas cintas son soporte de tipo secuencial, esto supone un inconveniente puesto que para acceder a una información determinada se hace necesario leer todas las que le preceden. (Torrez, 2012).

2.1.2 Tambor Magnético

Está formado por cilindros con material magnético capaz de retener información, esta se graba y lee, mediante un cabezal cuyo brazo se mueve en la dirección del eje de giro del tambor. El acceso a la información es directo y no secuencial. (Acosta, 2011).

2.1.3 Disco Duro

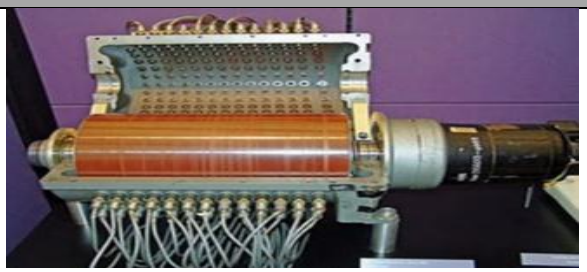
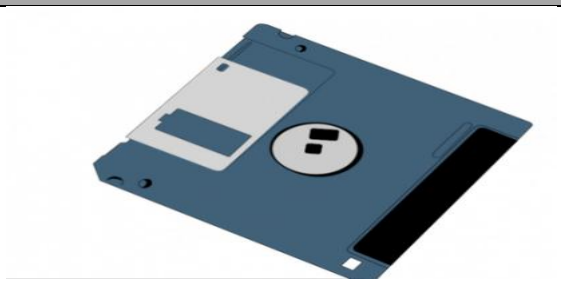
Es un dispositivo de almacenamiento de datos no volátil, que mediante un sistema de grabación magnética almacena datos en formato digital de manera permanente. Está compuesto por uno o más discos magnéticos concéntricos con un cabezal de lectura/escritura que se desplaza hasta la sección concreta del mismo, donde se trabaja con la información en un momento determinado. (Rangel, 2013).

2.1.4 Disquete o Disco flexible

Un disco flexible o también disquete, es un tipo de dispositivo de almacenamiento de datos formado por una pieza circular de un material magnético que permite la grabación y

lectura de datos, encerrado en una carcasa fina cuadrada o rectangular de plástico. (Pelozo, 2013).

Tabla 1: Dispositivos de almacenamiento magnéticos

Dispositivos de Almacenamiento por Medio Magnético	
	
Cinta Magnética imagen tomada de (Torrez, 2012)	**Tambor Magnético imagen tomada de (Acosta, 2011)**
	
Disco flexible imagen tomada de (Pelozo, 2013)	**Disco duro imagen tomada de (Rangel, 2013)**

2.2 Dispositivos de Almacenamiento por Medio Óptico:

Los dispositivos ópticos son aquellos dispositivos de almacenamiento de datos en los que la grabación de los datos es realizada a través de un rayo láser de alta precisión, son bastante utilizados para almacenar archivos multimedia, como música, fotos, videos, programas de computadoras, juegos y aplicaciones comerciales.

2.2.1 CD-R

Es un disco compacto de 650 MB de capacidad que puede ser leído cuantas veces se desee, pero cuyo contenido no puede ser modificado una vez que ya ha sido grabado. Dado que no pueden ser borrados. (Paul, 2012).

2.2.2 CD-RW

Posee la capacidad del CD-R con la diferencia que estos discos son regrabables lo que les da una gran ventaja. (Cárdenas, 2013)

2.2.3 DVD-ROM

Es un disco compacto con capacidad de almacenar 4.7 GB de datos en una cara del disco, un aumento de más de 7 veces con respecto a los CD-R y CD-RW. (Gómez, 2012)

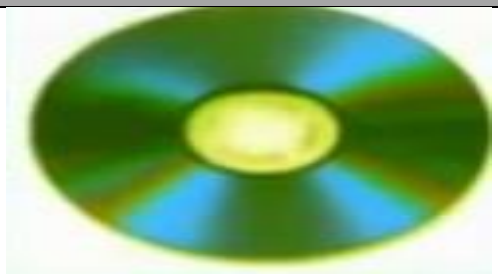
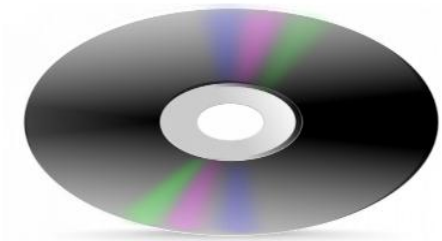
2.2.4 DVD-RAM

Este medio tiene una capacidad de 2.6 GB en una cara del disco y 5.2 GB en un disco de doble cara, son regrabables. (Blanco, 2015)

2.2.5 Blu-ray

El Blu-ray es un avance natural de la tecnología de almacenamiento óptico de datos, que se aprovecha de los últimos avances en las tecnologías láser para poder escribir más datos en menos espacio. En el caso del Blu-ray, la densidad de bits es tal que en un solo disco convencional de una capa, y de 12 mm de diámetro, se pueden escribir hasta 25 GB de datos; es decir, hasta 6 veces más que en el DVD. Este disco también conserva las proporciones y propiedades geométricas que sus antecesores, y supone el triunfo de la compañía Sony frente a Toshiba, que compitió contra el BD con otro formato, ya en desuso, conocido como HD-DVD. (Gutiérrez, 2015)

Tabla 2: Dispositivos de almacenamiento ópticos

Dispositivos de Almacenamiento por Medio óptico	
	
CD-R imagen tomada de (Paul, 2012).	**CD-RW imagen tomada de (Cárdenas, 2013)**
	
DVD-ROM imagen tomada de (Gómez, 2012)	**DVD-RAM imagen tomada de (Blanco, 2015)**
	
Blu-ray imagen tomada de (Gutiérrez, 2015)	

2.3 Dispositivos de Almacenamiento por Medio Electrónico-digital:

Es la más joven y prometedora forma de almacenamiento de información. Utiliza circuitos electrónicos para almacenar la información, los cuales no necesitan moverse para efectuar tal función. Estos dispositivos ganaron fuerza rápidamente en el mercado, su tamaño es muy pequeño y se utilizan masivamente. Son inmunes a los campos magnéticos, mas no a los golpes bruscos, temperatura y humedad, los cuáles pueden producir cambios en el estado lógico de las celdas de memoria o estropearlas definitivamente.

2.3.1 RAM

Siglas de Random Access Memory, un tipo de memoria a la que se puede acceder de forma aleatoria; esto es, se puede acceder a cualquier byte de la memoria sin pasar por los bytes precedentes. Es la memoria desde donde el procesador recibe las instrucciones y guarda los resultados. Es el área de trabajo para la mayor parte del software de un computador. (Informaticamoderna, 2012)

2.3.2 SRAM

Proviene de ("Static Random Access Memory"), lo que traducido significa memoria estática de acceso aleatorio. Se trata de una memoria RAM que tiene la característica de estar construida a base de transistores. La característica más importante de la memoria SRAM es que por las propiedades electrónicas del transistor, este no necesita estarse cargando constantemente de electricidad, tiende a ser sumamente rápida. (Informaticamoderna, 2012)

2.3.3 ROM

Es la sigla de ("Read Only Memory") o memoria de solo lectura. Se trata de un circuito integrado que se encuentra instalado en la tarjeta principal Motherboard, dónde se almacena

información básica referente al equipo, lo que se denomina BIOS que integra un programa llamado POST encargado de reconocer inicialmente los periféricos instalados. (Torrez, 2014)

2.3.6 Tarjeta de memoria digital

Memoria 100% electrónica, basada en el uso de celdas de almacenamiento tipo NAND, permite guardar datos por largos periodos de tiempo sin necesidad de tener alimentación eléctrica, tienen una baja generación de calor, poco desgaste y alta velocidad de transmisión de datos, además tienen la característica de ser memorias portátiles que se pueden utilizar en una gran cantidad de dispositivos. (Informaticamoderna, 2012)

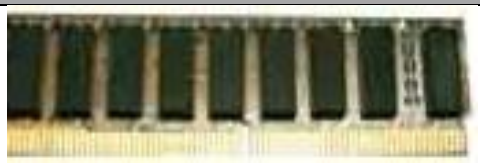
2.3.8 Disco duro de estado sólido

Los discos duros en estado sólido (SSD) son dispositivos de almacenamiento de datos basados en flash para su portátil u ordenador de sobremesa. Un SSD funciona de forma similar que un disco duro tradicional, pero sin la necesidad de incluir piezas móviles. Esta es la diferencia clave entre los dos tipos discos y, como resultado, un SSD es más rápido, silencioso, resistente y eficiente desde el punto de vista energético que su homólogo tradicional. (Verbatim, s.f)

2.3.7 Pendrive

La definición de la Real Academia Española de la lengua es simplemente: "*dispositivo portátil pequeño de almacenamiento de datos*". Un pendrive es "*pequeño dispositivo de bolsillo de almacenamiento de datos, fácil de usar y compatible con todos los sistemas operativos*". (Campos, 2015).

Tabla 3: Dispositivos de almacenamiento electrónico-digital

Dispositivos de Almacenamiento por Medio electrónico-digital	
	
Memorias RAM y SRAM imágenes tomadas de (informaticamoderna, 2012)	
	
Memoria ROM imagen tomada de (Torrez, 2014)	**MMC imagen tomada de (informaticamoderna, 2012)**
	
Disco duro en estado solido imagen tomada de (verbatim, sf)	
	
Pendrive imágenes tomadas de (Centorrino, 2015)	

2.4 Historia y aspectos técnicos del pendrive

En los últimos años, se ha observado un crecimiento importante en la utilización del pendrive, dado que dicho dispositivo permite portar información de forma práctica, fácil y cómoda. Se presenta a continuación sus orígenes y generaciones según Ibarra (2014) y Ricky (2015):

2.4.1 Historia del Pendrive

El pendrive fue inventado en el año 1999, fue lanzado al público en el 2000, según su creador el objetivo era crear un dispositivo que permitiera transportar la información y que fuera fácil de usar. Los primeros modelos de pendrive requerían una batería, los actuales usan la energía eléctrica procedente del puerto USB. Estas memorias son resistentes a los rasguños (externos), al polvo, y algunos hasta al agua, factores que afectaban a las formas previas de almacenamiento portátil, como los disquetes, discos compactos y los DVD. El pendrive durante su existencia ha tenido varias generaciones:

Primera generación

Las empresas Trek Technology e IBM comenzaron a vender las primeras unidades de memoria USB en el año 2000. Trek vendió un modelo bajo el nombre comercial de Thumbdrive e IBM vendió las primeras unidades en Norteamérica bajo la marca DiskOnKey, desarrolladas y fabricadas por la empresa israelí M-Systems en capacidades de 8 MiB, 16 MiB, 32 MiB y 64 MiB. Estos fueron promocionados como los «verdaderos reemplazos del disquete».

Segunda generación

Dentro de esta generación existe conectividad con la norma USB 2.0. Sin embargo, no usan en su totalidad la tasa de transferencia de 480 Mbit/s que soporta la especificación USB 2.0 debido a las limitaciones técnicas de las memorias flash basadas en NAND. Los dispositivos más rápidos de esta generación usan un controlador de doble canal, aunque todavía están muy lejos de la tasa de transferencia posible de un disco duro de la actual generación, o el máximo rendimiento de alta velocidad USB. Las velocidades de transferencia de archivos varían considerablemente. Se afirma que las unidades rápidas típicas leen a velocidades de hasta 480 Mbit/s y escribir a cerca de la mitad de esa velocidad. Esto es aproximadamente 20 veces más rápido que en los dispositivos USB 1.1, que poseen una velocidad máxima de 24 Mbit/s.

Tercera generación

La norma USB 3.0 ofrece tasas de cambio de datos mejoradas enormemente en comparación con su predecesor, además de compatibilidad con los puertos USB 2.0. La norma USB 3.0 fue anunciada a finales de 2008, pero los dispositivos de consumo no estuvieron disponibles hasta principios de 2010. La interfaz USB 3.0 especifica las tasas de transferencia de hasta 4,8 Gbit/s, en comparación con los 480 Mbit/s de USB 2.0. A pesar de que la interfaz USB 3.0 permite velocidades de datos muy altas de transferencia, a partir de 2011 la mayoría de las unidades USB 3.0 Flash no utilizan toda la velocidad de la interfaz USB 3.0 debido a las limitaciones de sus controladores de memoria, aunque algunos controladores de canal de memoria llegan al mercado para resolver este problema. En agosto de 2010, Imation anuncia el lanzamiento al mercado de la nueva línea de USB de seguridad Flash Drive Defender F200, con capacidades de 1 GiB, 2 GiB, 4 GiB, 8 GiB, 16 GiB y 32 GiB. Estas unidades de almacenamiento

cuentan con un sensor biométrico ergonómico basado en un hardware que valida las coincidencias de las huellas dactilares de identificación, antes de permitir el acceso a la información.

El conector USB 3.0. Tiene 9 pines, un lado de 4 pines donde se encuentran 2 pines de transmisión de datos y 2 pines de corriente, pero adicionalmente maneja en el lado contrario 5 pines para la transmisión de datos simultáneos a mayor velocidad, lo que lo hace más rápido que el USB 2.0, el USB 3.0 se le suele diferenciar del USB 2.0 por conector de color azul. USB 3.0 reduce significativamente el tiempo requerido para la transmisión de datos.

2.4.2 Características y funcionamiento del pendrive

Este dispositivo es de almacenamiento no volátil, su naturaleza es de estado sólido, utiliza memoria de tipo flash. Fue pensado para ser utilizado como disco duro externo portátil. Es un medio de almacenamiento muy difundido, de tamaño reducido, alta capacidad, facilidad y confiabilidad en el transporte y almacenamiento de datos, se conecta directamente al ordenador sin necesidad de instalar un software adicional. El conector USB es la puerta de enlace hacia el ordenador, permite procesos simultáneos de lectura/escritura, cuando se conecte se activará el oscilador que es lo que controla el acceso de datos. Cuenta con un alto periodo de duración, teóricamente pueden retener los datos almacenados durante 20 años y reescribirse un millón de veces. (Cortés, 2014).

Su funcionamiento se basa en un circuito que interactúa con el microprocesador del ordenador al que se conecta, funciona como un dispositivo de almacenamiento móvil para los sistemas de computación. Utiliza módulos de memoria flash que contienen datos en una configuración de memoria flash NAND las unidades integradas

que guardan la información en el interior del chip de almacenamiento, lo hacen en forma eléctrica, son condensadores integrados. (Pérez, 2012).

Los pendrive o simplemente USB, tiene varios parámetros determinados por el fabricante. Por ejemplo, las memorias fabricadas por la compañía Kingston tienen por defecto la etiqueta KINGSTON, además, dichas memorias tienen una sola partición y un sistema de archivos FAT32. Los sistemas de archivos, son estructuras y funciones que ayudan al sistema operativo para almacenar y recuperar archivos en un sistema de almacenamiento de manera eficiente, los más utilizados son los sistemas FAT12, FAT16, FAT32 y NTFS para Windows y los sistemas extendidos ext2, ext3 y ext4 para Linux. Cada uno tiene sus ventajas y desventajas. La tabla a continuación muestra en qué sistema de archivos FAT están los dispositivos según su capacidad de almacenamiento.

Tabla 4: Formato predeterminado del sistema de archivos

CAPACIDAD DE ALMACENAMIENTO	FORMATO	CARACTERÍSTICAS
Hasta 2GB	FAT16	Capacidad muy limitada
4GB-32GB	FAT32	Compatible con todos los sistemas operativos y todo tipo de dispositivo.
64GB y superiores	exFAT	Actualización de FAT32.
64GB y superiores	NTFS	Compatible solo con Windows

Tomada de (Informática moderna, 2015)

2.4.3 Memoria Flash

Es una pequeña tarjeta destinada a almacenar información, es denominada no volátil, ya que conserva los datos aun cuando no se encuentra conectada a la corriente eléctrica, está hecha de muchísimas celdas microscópicas que acumulan electrones con

diferentes voltajes a medida que la electricidad pasa a través de ella, creando así un mapa de diferentes cargas eléctricas, de este modo la tarjeta logra guardar la información. La memoria flash de un dispositivo de almacenamiento pendrive puede ser borrada y reprogramada al conectarse a un equipo de cómputo y además permite el borrado bloque a bloque, esta es una característica que facilita su utilización pero que a la vez implica tener un mayor cuidado con la información almacenada en el dispositivo en el momento de borrar archivos. (Cibercentro lalila, 2015).

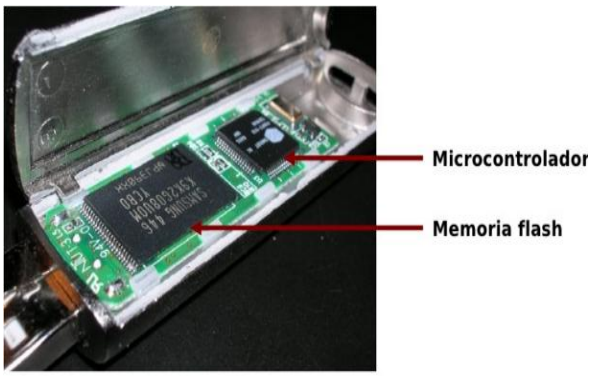


Imagen 1: Memoria flash imagen tomada de (Moreno, 2009)

La memoria flash contiene una matriz de filas y columnas con celdas que tienen dos transistores en cada intersección que tienen como nombres “compuerta flotante” y “compuerta de control”. Dentro de ellos hay millones de celdas que se conectan entre ellas gracias a un elaborado circuito, pueden almacenar más de un bit por celda variando el número de electrones que almacena, para leer, tiene sensores de celda que detectan el contenido de la misma, los dos transistores están separados por una fina capa de óxido ferroso, uno de los transistores recibe el nombre de floating gate, éste está conectado a la fila (wordline) a través del otro transistor, control gate, cuando esta conexión se establece el valor de la celda cambia a 0, pues el valor por defecto es 1 cuando ambos transistores no están unidos. Esto quiere decir que para modificar los valores de las

celdas (borrar o escribir) se le debe aplicar una descarga eléctrica (que va de los 0 a los 13 voltios) que transfiere (0) o (1) electrones, dependiendo del estado de unión de los transistores. (Ortiz, 2013)

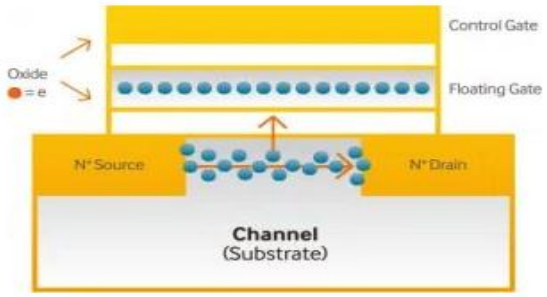


Imagen 2: Estructura Memoria flash NAND imagen tomada de (Palazuelos, 2015)

Existen dos principales tecnologías de memoria Flash: NOR y NAND. Cada tecnología tiene sus puntos fuertes que hacen que resulte ideal para diferentes tipos de aplicaciones.

Memoria Flash NOR

Este tipo de memoria permite una lectura y escritura más lenta que NAND, pero archiva muy rápido las rutas de acceso aleatorias, esto es, tiene tiempos de lectura rápida pero tiempos lentos para borrar y escribir, tiene una densidad baja, para cantidades grandes de almacenamiento, puede requerir múltiples chips. Esto hace que NOR sea más adecuado para la ejecución y almacenamiento de comandos.

Imagen 3: Memoria flash NOR Imagen tomada de (DirectIndustry, 2015)

Memoria Flash NAND

La arquitectura NAND es más indicada para el almacenamiento masivo de datos. Los dispositivos de almacenamiento flash NAND, poseen tiempos de borrado y escritura mucho más rápidos, puede almacenar más datos en un espacio de silicio más pequeño, lo que ahorra el coste por bit, la complejidad del almacenamiento NAND requiere de unos procesos adicionales, incluyendo un gestor de bloques defectuosos, el recolector de basura y el corrector de errores.

Los datos tienen tres sectores, el dato en sí, la dirección y el código de corrección de errores, siempre que se lee un dato el código de corrección verifica que el dato sea correcto es decir que se haya leído correctamente. El código de corrección de errores (ECC) permite un control para verificar los datos en modo de lectura. El controlador genera y almacena una ECC se graba en un bloque y se puede utilizar el código para verificar los datos después de leer el bloque. Los fabricantes de tarjetas de memoria flash pueden poner en práctica protocolos adicionales para ayudar a garantizar la fiabilidad de los datos. Por ejemplo, en condiciones de margen, el controlador en un SanDisk MultiMediaCard lee los datos de vuelta después de escribir para verificar la

operación de escritura. Si un bit es incorrecto, el controlador reemplaza el bit con uno de recambio. El controlador también puede sustituir un bloque incorrecto entero con otro bloque.

Imagen 4: Memoria flash NAND imagen tomada de (DirectIndustry, 2015)

Hay dos formas de clasificar estas memorias flash, según su funcionamiento interno como se resume en la siguiente tabla:

Tabla 5: Usos de las memorias flash NOR y NAND

	Memoria Flash NOR	Memoria Flash NAND
Acceso a alta velocidad	Sí	Sí
Acceso a datos en modo de página	No	Sí
Acceso aleatorio a nivel de byte	Sí	No
Usos típicos	Memoria de dispositivo en red	Almacenamiento industrial

Tomada de (Kingston Technology Corporation, 2015)

Definiciones aclaratorias

Acceso a alta velocidad: capacidad de acceso aleatorio de alta velocidad, para leer y escribir datos en lugares específicos de la memoria sin tener que accederla en modo secuencial, tanto la memoria Flash NOR como la memoria Flash NAD cuentan con esta característica. (Hernández, 2012).

Acceso a datos en modo de página: capacidad de recuperación o escritura de datos como páginas únicas, en modo secuencial, manejando datos en bloques de tamaño pequeño ("páginas"). La memoria Flash NAND puede hacerlo de esta manera, mientras que la memoria Flash NOR puede recuperar bytes individuales (Hernández, 2012).

Acceso aleatorio a nivel de byte: permite la recuperación de datos desde un solo byte. La memoria Flash NOR es excelente en aplicaciones donde los datos se recuperan o se escriben de manera aleatoria. (Hernández, 2012).

Usos típicos: La memoria Flash NOR es excelente en aplicaciones donde los datos se recuperan o se escriben de manera aleatoria. NOR se encuentra más frecuentemente integrada en teléfonos celulares (para almacenar el sistema operativo del teléfono) y Asistentes Digitales Personales; también se utiliza en computadoras para almacenar el programa BIOS que se ejecuta para proporcionar la función de arranque.La memoria Flash NAND se encuentra comúnmente en unidades de disco duro de estado sólido, dispositivos Flash de medios digitales de audio y video, decodificadores de televisión, cámaras digitales, teléfonos celulares (para almacenamiento de datos), y otros dispositivos donde los datos se escriben o leen, generalmente de manera secuencial. (Hernández, 2012).

2.4.4 Partes físicas del pendrive

La exposición relativa, se hace tomando como modelo el pendrive: Kingston DataTraveler 101 rojo, que como protección tiene una cubierta plástica equipada con tapa corrediza para que el conector USB macho no se dañe en el transporte o la manipulación del dispositivo, su parte física está compuesta por un PCB o circuito impreso sobre el cual se encuentran soldados unos componentes electrónicos: Un componente metálico alargado, que es un oscilador de cristal de cuarzo necesario para el funcionamiento de la unidad, produce la señal de reloj principal del dispositivo a 12MHz y controla la salida de datos a través de un bucle de fase cerrado (phase-locked loop), dos circuitos integrados planos ("chips") con muchas terminales. Uno de ellos es un microprocesador RISC (Computadora con Conjunto de Instrucciones Reducidas) que actúa como controlador de almacenamiento implementa el controlador USB y provee la interfaz homogénea y lineal para dispositivos USB seriales orientados a bloques, mientras oculta la complejidad de la orientación a bloques, eliminación de bloques y balance de desgaste. Este controlador posee un pequeño número de circuitos de memoria RAM y ROM, la unidad de almacenamiento de información (Bloque de memoria flash), el interruptor de seguridad contra escrituras encargado de proteger los datos de operaciones de escritura o borrado , el conector USB que es el que provee la interfaz física con el ordenador, permitiendo ser acoplado a él para transferir información, dicho conector maneja 4 pines, 2 para la comunicación o transmisión de datos y 2 de suministro de corriente. El LED indicador de transferencia de datos entre el dispositivo y el ordenador, por último cabe mencionar que se dispone de un espacio disponible para incluir un segundo circuito de memoria flash. (Vargas, 2015)

Tabla 6: Componentes internos del pendrive

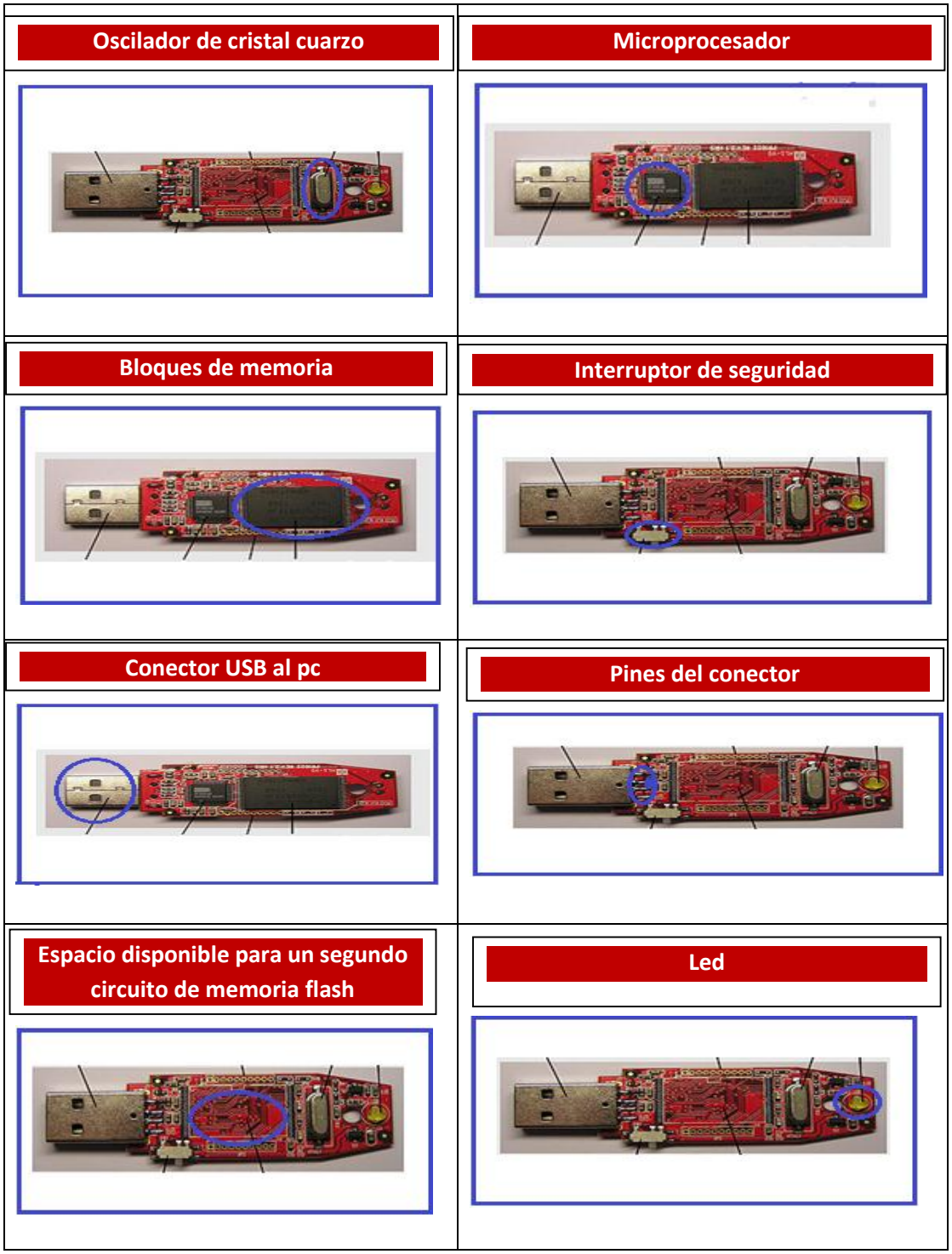


Imagen tomada y modificada de (Vargas, 2015)

2.4.5 Estructura lógica del pendrive

Según Ryckeboer (2010). Las estructuras lógicas referentes al pendrive para almacenar y administrar los datos son:

- **Firmware:** Es un bloque de instrucciones de máquina para propósitos específicos, grabado en el pendrive, normalmente de lectura/escritura, establece la lógica de más bajo nivel que controla los circuitos electrónicos del dispositivo.
- **Boot o sector de arranque**: hace referencia a una sección muy importante de la unidad, en ella se guarda la información esencial sobre las características del dispositivo y se encuentra un programa que permite arrancar el ordenador, contiene 3 ítems: un área para código ejecutable, una tabla de particiones, y una firma de booteo que especifica qué sectores están disponibles para el almacenamiento de directorios y qué sectores contienen las tablas de asignación de archivos.

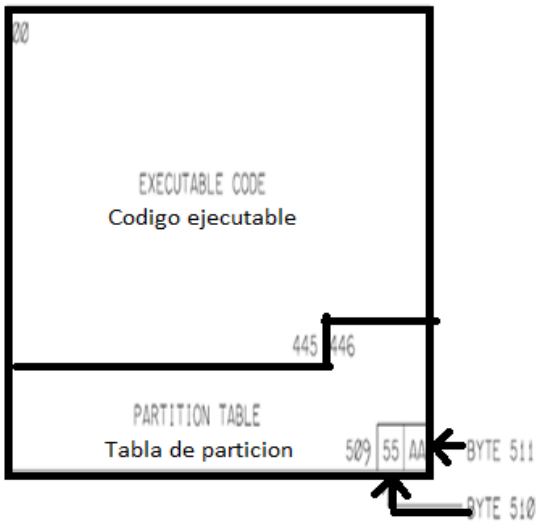


Imagen 5: Estructura sector de arranque tomada de (Ryckeboer, 2010)

- **Tabla de particiones**: permiten definir uno o más volúmenes lógicos o particiones en el dispositivo. En el sector de arranque la tabla de particiones tiene espacio para cuatro entradas de 16 bytes que sirven para especificar a qué partición pertenecen los sectores.

Tabla 7: Tabla de particiones

Registro de arranque maestro
Primera particion primaria
Segunda particion primaria (opcional)
Tercera particion primaria (opcional)
Registro de inicio extendido 1
Particion extendida 1
Registro de inicio extendido 2
Particion extendida 2
Registro de inicio extendido N
Particion extendida N

- **LBA**: proviene de (Logical Block Addressing), que significa direccionamiento de bloque lógico, es un método de acceso usado para identificar la ubicación de los bloques de datos en sistemas de almacenamiento. Con LBA, estos son numerados según un índice, de manera consecutiva siendo el primer bloque LBA 0 (cero), el segundo LBA 1, y así sucesivamente.

  Todos los pendrive soportan direccionamiento de bloque lógico LBA. Los bloques con capacidad de almacenamiento se numeran secuencialmente. Todos los bloques tienen el mismo tamaño, típicamente 512 bytes. La dirección del bloque lógico se refiere a una dirección del sector, ya que el tamaño del bloque es igual a la capacidad de un sector en el dispositivo. Para acceder al pendrive, el software especifica la dirección de bloque lógico de lectura y escritura. El controlador de la unidad traduce cada LBA a un bloque, página y columna de la matriz de memoria. La secuencia de dirección de bloque lógico no tiene porqué corresponder a las ubicaciones físicas de los sectores en una

unidad o en el microprocesador o en la memoria flash, todo lo que importa es que el controlador de medios sepa qué área de almacenamiento corresponde a cada dirección. Con los años, los componentes de software han evolucionado para soportar medios con mayor capacidad de almacenamiento y nuevas características. Algunos de los desarrollos, como el método de direccionamiento de bloque lógico (LBA), simplifican el trabajo de los hosts de los dispositivos de almacenamiento masivo.

- **FAT**: proviene de (File Allocation Table), que significa tabla de localización de archivos, se encarga de asignar espacio a los archivos, administrar el espacio libre y el acceso a los datos resguardados. Estructura la información en la unidad, dicha tabla contiene un mapa de esta, de tal manera que sabe la ubicación de cada uno de los datos almacenados.
- **Sistema de archivos**: estructuras y funciones que ayudan al sistema operativo para almacenar y recuperar archivos de manera eficiente, es un método para el almacenamiento y la organización de los archivos del sistema y los datos que contiene, para facilitar el acceso a los mismos.

2.4.6 Usos comunes de un pendrive

La siguiente clasificación de los usos más comunes del pendrive fue tomada de (Mark_kol, 2011) y (zaniuk, 2012)

- Transportar y almacenar datos: Este es el uso principal de dicho dispositivo, en particular copias de seguridad.
- Reparar equipos: en el campo de reparaciones de equipos sirve como medio para transferir el software de recuperación y antivirus a equipos infectados o dañados.

- Portar aplicaciones y sistemas operativos: sirve para albergar un sistema operativo, permite llevar programas y aplicaciones para usarlos en cualquier equipo y ejecutarlos sin necesidad de instalarlos, esto es posible con una versión portable de dichas aplicaciones y softwares. el pendrive es un medio práctico para cargar con la información de configuración y el software utilizado para el mantenimiento del sistema, solución de problemas y la recuperación, sirve de herramienta a los administradores del sistema.
- Bloquear y desbloquear el equipo: se puede convertir la unidad USB en una "llave" que abre el ordenador mientras está conectado y lo cierra cuando se retira. Si alguien intenta acceder al ordenador sin la clave recibirá un mensaje de "Acceso denegado".
- Instalar y hacer pruebas de manejo de sistema operativo: a través de un pendrive se puede probar un nuevo sistema operativo sin sobrescribir el sistema operativo actual.
- Hacer mantenimiento de sistemas: desde el pendrive instalando el software apropiado puede hacerse procesos de mantenimiento a un sistema.
- Copia de seguridad o respaldo: Existe la opción de hacer cada día una copia de seguridad de los trabajos que se han realizado, usando como medio almacenamiento este dispositivo.

2.4.7. Pérdida de información

De acuerdo con (Seagate, s.f). Generalmente, la pérdida de datos se caracteriza por: la incapacidad de acceder a cualquiera de ellos, la supresión accidental de archivos, sobreescritura de estructuras de control de datos, archivos dañados o con acceso

bloqueado debido al funcionamiento anormal o a la avería del dispositivo, entre otras, se puede producir debido a que este dispositivo móvil de uso muy común, utilizado para almacenar y transportar archivos que contendrán información personal, laboral y educativa, entre otras.

Cada nuevo método de almacenamiento o transferencia de información tiende a introducir muchas más formas nuevas en las que la información en cuestión puede perderse, ser capturada o destruida, debido a causas accidentales o inducidas. Esto puede atribuirse a:

- Errores humanos que incluyen la eliminación intencional o accidental, la sobre escritura de archivos o del sistema.
- Actos de la naturaleza o condiciones adversas del entorno.
- Falla del dispositivo.
- Daño por malwares.
- Errores del software y actualizaciones fallidas.

De estas causas o escenarios las más comunes que conducen a la pérdida de información se listan a continuación:

- **Interrupciones durante la transferencia de datos**: Si algo se torna mal, durante el proceso de transferencia de datos, entonces hay altas probabilidades de perder archivos.
- **Borrado accidental**: La eliminación accidental de los archivos por error o por descuido, es una de las principales razones de pérdida de información.
- **Formateo**: Formateo de una unidad de almacenamiento pendrive con o sin intención se traduce en la pérdida de datos, por lo general el formateo se realiza para liberar espacio o para deshacerse de virus.

- **Oleada de energía eléctrica, magnética**: La escasez o corte de energía mientras la unidad está conectada al sistema o al acceder a los datos desde la unidad, eventualmente causa la pérdida de toda la información que contiene, similarmente un aumento de energía también puede conducir al daño de la unidad.
- **Exposición a la humedad**: La humedad es el agente más peligroso para las tarjetas flash y pendrives porque los pequeños depósitos de agua evaporada pueden entrar en los dispositivos y afectar gravemente sus circuitos, ocasionando daños en su funcionamiento.
- **Errores en el sistema de archivos**: El sistema reconoce el dispositivo y le asigna un nombre pero cuando intenta identificar formato del sistema de archivos encuentra un error. (Sistema de archivos de solo lectura)
- **Extracción inadecuada**: La extracción inadecuada del pendrive mientras se trabaja en algunos de los archivos presentes en el dispositivo se traducirá en la pérdida de los archivos que se han abierto en alguna aplicación. En tales casos, los presentes datos se pierden o se vuelven inaccesibles, además no desconectar el pendrive después de apagar el ordenador hace que algunos archivos se eliminen. Es importante comprobar que todas las operaciones estén completas antes de retirar el dispositivo, recordar que la extracción se debe hacer de forma segura para tener la certeza de que la información queda almacenada correctamente.
- **Infección por virus**: hay casos, en donde el pendrive podría infectarse por virus. Si estos no se analizan y eliminan en el tiempo; se multiplican y la infección se

extendería a la partición de toda unidad flash. Esto hace que la partición de la impulsión del flash sea inaccesible, lo que conduce a la pérdida de datos.

2.4.8 Daños o errores comunes del pendrive

Son muchas y variadas las causas de daños impredecibles de la unidad y en muchos casos, incontrolables por ejemplo: altas temperaturas, golpes o caídas, fallos de software, formateo lógico, daño o avería provocada y malware. Con frecuencia las fallas esconden la información, la eliminan por completo o dañan el dispositivo.

A continuación se listan y describen los daños más frecuentes:

- **Celdas defectuosas en la tarjeta**: Celdas defectuosas que causan el bloqueo de la tarjeta. Por ejemplo, una vez que se accede a la celda defectuosa, todos los intentos de lectura fallan.
- **Falla de inaccesibilidad**: Existen ocasiones en las que un pendrive puede fallar, quedando inaccesible. Esto puede suceder al desconectar el dispositivo de forma abrupta (no se hace el debido proceso de extracción segura), o en otros casos al intentar particionar la unidad flash. (Fabricio Ferri, 2013)
- **Pérdida de formato**: es que aparece una ventana que indica que la unidad no tiene formato, y pregunta si desea formatearla.
- **Falla en la ficha**: En una desconexión repentina cuando se está operando con el dispositivo. Esto la gran mayoría de las veces, se debe a falso contacto por sulfatamiento o deformación de los terminales.
- **Borrado accidental de partición**: Es común, al pretender eliminar la partición del sistema usando las utilidades de gestión de disco, en su lugar por

accidente, eliminar la partición de la impulsión del flash que está conectada al sistema, incluso hay posibilidades de perderla entera.

- **Cambiar el tamaño o formateo**: en casos de redimensionar la partición existente de la unidad flash, si el proceso se interrumpe o no se completa toda ella llegaría a ser corrupta volviendo inaccesibles los datos.

2.4.9 Avances en el pendrive

En la actualidad se pueden equipar a las unidades flash, pendrives, con diversos sistemas de protección tales como: cifrado o biometría, lo que los convierte en una pequeña caja de seguridad para almacenar con total confianza datos de mucho valor.

De acuerdo con Pascual, (2015). Además de aumentar la capacidad de almacenamiento y la velocidad de transferencia de datos, las compañías dedicadas a la fabricación y venta de memorias externas han diseñado también pendrive con características adicionales como los que se muestran a continuación:

USB con teclado numérico para contraseña: este pendrive sólo permite el acceso a la información almacenada en su interior si previamente se marca la contraseña correcta en el pequeño teclado numérico que lleva incorporado.

USB identificación por huella: permite que el usuario tenga acceso a datos protegidos con tan solo escanear su huella digital. La tecnología biométrica del JetFlash 220 hace que sea fácil guardar información y mantenerla protegida.

Pendrive espía: unidad de memoria flash de alta calidad que tiene una cámara espía incrustada en él, está equipada con la avanzada tecnología de detección de movimiento, así como un interruptor de vibración. Es un dispositivo versátil que es capaz de capturar

audio, así como vídeo y que también puede funcionar como una cámara de imagen fija. Su alta capacidad de batería de polímero de litio le permite grabar vídeos de forma continua durante un máximo de 90 minutos.

USB Flash DataTraveler® 2000: ofrece cifrado basado en hardware, así como protección mediante un NIP con acceso a través de un teclado alfanumérico integrado. El cifrado se lleva a cabo en la unidad por lo que no requiere de software ni controladores de hardware. La clave de cifrado y la contraseña se borran después de 10 intentos de ingreso fallidos para impedir intrusiones forzadas. Interfaz: USB 3.1 Gen. 1 (USB 3.0) A prueba de agua/polvo

Flash Drive USB cifrada de Toshiba. En palabras sencillas, un pendrive cifrado mediante hardware. Esta memoria USB incluye algún tipo de chip o circuito (Toshiba lo mantiene en secreto) que cifra por hardware el contenido del pendrive, utilizando el potente algoritmo militar AES de 256 bits, aprobado por el gobierno norteamericano como uno de los sistemas de protección más seguros. El pendrive dispone de una batería recargable para poder llevar a cabo todas estas labores de cifrado y desbloqueo sin tener que estar conectado a un ordenador. Además incorpora un mecanismo de defensa contra la fuerza bruta, que borra todos los datos si alguien intenta introducir el PIN más de diez veces seguidas, puesto que la protección se lleva a cabo a través del hardware, para acceder a los datos del pendrive debe teclearse la contraseña en un teclado incorporado al propio dispositivo.

SanDisk Ultra Dual USB: cuenta con un conector micro USB en un extremo y un conector USB 2.0 en el otro, los cuales permiten transferir archivos con gran facilidad,

y puede almacenar hasta 64 GB de datos. Opción para traspasar archivos del celular hacia el computador o entre celulares.

Pendrive Connect Wireless Stick: pendrive que conecta inalámbricamente el ordenador con el teléfono móvil, permite almacenar en el pendrive lo que se desee y hacer transmisión de ello al Smartphone.

Pendrive que convierte una pantalla con HDMI en un ordenador con Windows 8.1: pequeño dispositivo del tamaño de un pendrive pero con toda la potencia de una computadora portátil. El dispositivo, que permite transformar cualquier pantalla con HDMI en una computadora completa con Windows es compatible con cualquier tipo de mouse y teclado inalámbrico.

Kingston DataTraveler HyperX Predator: pendrive con capacidad de 1 Tb, cuenta con conexión USB 3.0 que garantiza una velocidad de lectura de 240 Mb/s y una velocidad de escritura de 160 Mb/s.

3.SEGURIDAD INFORMÁTICA, ANÁLISIS FORENSE Y PENDRIVE

3.1. Generalidades sobre seguridad informática

Las organizaciones y personas realizan grandes esfuerzos para afrontar la problemática de la seguridad de la información, dados los riesgos que conlleva la pérdida de su confidencialidad, integridad o disponibilidad.

La filtración de la información puede causar pérdidas no solo económicas sino también de imagen, prueba de ello es el llamado "Tsunami panameño" o "papeles de Panamá", ocurrido en el año 2015, o el de gran impacto local dado por los denominados "carteles del papel higiénico y del azúcar" del año 2016, que solo se explican como una falla grave en la seguridad informática de las personas y empresas involucradas. (Guevara, 2016).

De acuerdo con la Norma Técnica Colombiana NTC-ISO/IEC 27002 (2007):

"*La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada. Esto es especialmente importante en el entorno de negocios cada vez más interconectado. Como resultado de esta interconexión creciente, la información se expone a un gran número y variedad de amenazas y vulnerabilidades.*

La información puede existir en diversas formas. Se puede imprimir o escribir en papel, almacenar electrónicamente, transmitir por correo o por medios electrónicos, presentar en películas, o expresarse en la conversación. Cualquiera sea su forma o medio por el cual se comparte o almacena, siempre debería tener protección adecuada.

La seguridad informática es la protección de la información contra una gran variedad de amenazas con el fin de asegurar la continuidad del negocio, minimizar el riesgo para el negocio y maximizar el retorno de inversiones y oportunidades de negocio".

3.1.1 Una definición de seguridad informática

De acuerdo con Barón, (2013) la seguridad informática consiste en "*la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.*"

Según González (2014) el objetivo del proceso de seguridad informática es obtener un nivel aceptable de seguridad, entendiéndose por aceptable un nivel de protección suficiente para que la mayoría de potenciales intrusos interesados en los activos de la organización fracasen en cualquier intento de ataque contra los mismos. De igual forma, se encarga de establecer los mecanismos para registrar cualquier evento fuera del comportamiento normal y tomar las medidas necesarias para establecer las operaciones críticas a la normalidad.

Los aspectos que garantizan la seguridad y fiabilidad de un sistema son:

Confidencialidad: Los componentes del sistema serán accesibles sólo por aquellos usuarios autorizados, los datos solo deben ser conocidos y accedidos por quienes estén debidamente autorizados durante su almacenamiento, procesamiento o transmisión.

En términos de seguridad de la información, la confidencialidad hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos. (González, 2014)

El objetivo de la confidencialidad es, entonces, prevenir la divulgación no autorizada de la información.

Un ejemplo típico de mecanismo que garantice la confidencialidad es la Criptografía, cuyo objetivo es cifrar los datos para que resulten incomprensibles a aquellos usuarios que no disponen de los permisos suficientes, pero, incluso en esta circunstancia, existe un dato sensible que hay que proteger y es la clave de cifrado. Esta clave es necesaria para que el usuario adecuado pueda descifrar la información recibida y en función del tipo de mecanismo de cifrado utilizado, la clave puede/debe viajar por la red, pudiendo ser capturada mediante herramientas diseñadas para ello. Si se produce esta situación, la confidencialidad de la operación realizada (sea bancaria, administrativa o de cualquier tipo) queda comprometida.

Integridad: Los componentes del sistema sólo pueden ser creados y modificados por los usuarios autorizados, los datos solo pueden ser modificados y/o eliminados por quien esté autorizado y los sistemas y aplicaciones solo deben ser operados por dicho personal. (González, 2014)

En términos de seguridad de la información, la integridad hace referencia a la fidelidad de la información o recursos, y normalmente se expresa en lo referente a prevenir el cambio impropio o desautorizado.

El objetivo de la integridad es, prevenir modificaciones no autorizadas de la información.

Disponibilidad: Los usuarios deben tener disponibles todos los componentes del sistema cuando así lo deseen, los sistemas que albergan datos e información deben garantizar su acceso, cuando así se requiera, por quieres tengan derecho a ello (González, 2014). En términos de seguridad de la información, la disponibilidad hace referencia a que la información del sistema debe permanecer accesible a elementos autorizados. El objetivo de la disponibilidad es, entonces, prevenir interrupciones no autorizadas/controladas de los recursos informáticos.

Como resumen de las bases de la seguridad informática que se han comentado puede decirse que la seguridad consiste en mantener el equilibrio adecuado entre estos tres factores, puesto que no tendría sentido conseguir confidencialidad para un archivo a costa de que ni tan siquiera el usuario administrador pueda acceder a él, negando así la disponibilidad.

Al ámbito de la seguridad informática pertenece el área de análisis forense, surgida a raíz del incremento de los diferentes incidentes de seguridad. En el análisis forense se realiza un análisis posterior de los incidentes de seguridad, mediante el cual se trata de reconstruir como se ha penetrado o vulnerado un sistema.

El área de la ciencia forense es la que más ha evolucionado dentro de la seguridad, ya que los incidentes de seguridad han incrementado en los últimos años. Además, los ataques son diferentes y por tanto hay que actualizar las técnicas de análisis en cada momento. (RedIrIs, Red académica de investigación española, S.f).

3.1.2 Una definición de Análisis forense o Informática Forense.

"*La Informática forense es una disciplina dedicada a la recolección de pruebas digitales desde una maquina computacional para fines judiciales mediante la aplicación de técnicas de análisis y de investigación*" (cabrera, 2013), Consiste en la

aplicación de técnicas científicas y analíticas especializadas a estructura tecnológica para adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional. Mediante la selección de criterios que se usan para guiar y asegurar actividades concernientes con el análisis de evidencia digital. Este análisis permite reconstruir lo que ha sucedido en un sistema tras un incidente de seguridad, determinar quién, desde dónde, cómo, cuándo y qué acciones ha llevado a cabo un intruso en los sistemas afectados y encontrar la solución de conflictos tecnológicos relacionados con la seguridad informática y la protección de datos.

Una de las ideas principales de la informática forense, es poder realizar un estudio total de todo tipo de evidencia digital que se encuentre involucrada en un incidente. (es decir, realizar recopilación, preservación, análisis y reportes de la evidencia), con el fin de hacer que esta evidencia cobre un valor legal, y que así mismo, sea admisible a la hora de entablar procesos judiciales en los cuales esta evidencia tenga un carácter determinante en el mismo. (Belloso, 2008), (Sanabria, 2015), (Ocanet, 2015), (Castillo, 2008) y (Juntamay, 2011)

En el campo de la Informática Forense existen diversas etapas que definen la metodología a seguir en una investigación: identificación, preservación o adquisición, análisis y presentación de los resultados. Siguiendo el flujo lógico de actividades, primero se debe identificar las fuentes de datos a analizar y aquello que se desea encontrar, luego se debe adquirir las imágenes forenses de los discos o fuentes de información, posteriormente se realiza el análisis de lo adquirido para extraer

información valiosa y finalmente se ordenan los resultados del análisis y se presentan, de tal modo que resulten útiles. Existen herramientas específicas para cada tarea.

Por lo general cuando se realizan investigaciones los equipos pueden ser hallados en dos formas: vivo o muerto y dependiendo del estado del equipo se realiza el tipo de análisis, es decir en caliente o en frio.

3.1.3 Análisis en caliente

Se realiza un análisis con el ordenador en funcionamiento, obteniendo información que no se podría conseguir en caso de un ataque y el ordenador apagado. Permite ver los procesos, conexiones de red, así como el estado actual de muchos elementos del sistema que son volátiles y se pierden cuando éste se apaga. Puede resultar muy útil en caso de estar sufriendo un ataque en el instante del análisis, pudiendo recopilar información cierta sobre el funcionamiento y origen del mismo. Por otro lado, permite obtener una copia de la memoria RAM del sistema, en la que se puede encontrar mucha información útil. Otra forma en que se suele emplear este análisis es recreando el entorno del sistema e iniciándolo (siempre que se pueda virtualizar, vía una copia exacta del mismo, o bien con el sistema bloqueado contra escritura), siempre y cuando esto no ponga en peligro la evidencia original.

Si el equipo está vivo, lo recomendable es dumpear (volcar) la memoria RAM, extraer la información básica del sistema y luego halar del cable de corriente (práctica recomendada ya que Windows realiza modificaciones y elimina archivos en su proceso normal de apagado).

Luego de ejecutar esta acción, se puede manipular la evidencia como si fuese un entorno muerto.

Se realiza la copia bit a bit (copia exacta) de los medios de almacenamiento, garantizando que el entorno de adquisición no modifica en ningún momento el sistema de archivos (modo solo lectura)

Después de tener la imagen bit a bit, es vital generar inmediatamente su correspondiente HASH en MD5 y SHA-1

Para poder dar fe de la integridad de los datos recién adquiridos y que más adelante no existan inconvenientes. (Lobo, 2014)

3.1.4. Análisis en frío

Se realiza sobre una copia de la evidencia original, que se ha extraído del sistema cuando este se ha detenido o se ha encontrado en ese estado. Permite realizar un análisis más exhaustivo y menos intrusivo con la evidencia original (al trabajar sobre una copia idéntica no se alteran las pruebas originales), pero perdiendo la información volátil si esta no se ha podido extraer antes del sistema a analizar. En ciertos ataques puede ser que no obtengamos toda la información posible debido a la volatilidad de ciertas pruebas, que desaparecen al parar el sistema, pero se puede trabajar más a fondo que en los análisis en caliente, realizando algunas operaciones que no serían posibles de otra forma. (Lobo, 2014)

3.1.5 Evidencia digital

Uno de los pasos a tener en cuenta en toda investigación, sea la que sea, consiste en la captura de las evidencias. Por evidencia se entiende toda información que se pueda procesar en un análisis. Por supuesto que el único fin del análisis de las evidencias es saber con la mayor exactitud qué fue lo que ocurrió.

La evidencia digital puede estar contenida en dispositivos de almacenamiento pendrive, sabiendo esto el principal elemento que se debe proteger en una investigación de cualquier tipo es el dispositivo mismo que contiene la información útil para la investigación. La evidencia digital, debido a su naturaleza, es extremadamente frágil, ésta puede ser alterada, dañada o destruida si no se maneja adecuadamente durante la recogida de los datos, por eso debe recolectarse de tal forma que se garantice su integridad y fiabilidad, para esto están los custodios de la evidencia. (Sanabria, 2015)

Custodios de la evidencia: Son los encargados de proteger toda la evidencia recolectada, que se encuentra en un lugar centralizado. Ellos reciben la evidencia recolectada por los técnicos, se aseguran de que se encuentre propiamente identificada y mantienen una estricta cadena de custodia. (Santander, 2010)

3.1.6. Cadena de custodia

La cadena de custodia tiene como finalidad brindarle soporte veraz a la prueba digital ante el juez, en medio de lo que se conoce como el debido proceso.

Se considera la cadena de custodia como un procedimiento controlado que se aplica a los indicios materiales (prueba indiciaria) relacionados con un hecho delictivo o no, desde su localización hasta su valoración, por parte de los encargados de administrar justicia y que busca asegurar la inocuidad y la esterilidad técnica en el manejo de los mismos, evitando alteraciones, sustituciones, contaminaciones o destrucciones, hasta su disposición definitiva por orden judicial, tiene por objeto asegurar que la prueba ofrecida cumple con los requisitos exigibles procesalmente para la misma. (Arellano, 2012)

3.1.7 Captura de Imágenes de un Pendrive

Para dar inicio al proceso de adquisición de imágenes del dispositivo de almacenamiento Pendrive, se debe preparar un laboratorio de software de análisis con características que permitan obtener, analizar y asegurar la evidencia digital.

Es indispensable contar con software especializado para la realización de esta tarea, teniendo en cuenta que no se podrá realizar modificación alguna ni dejar rastro sobre los datos que sean analizados, que por ningún motivo se modifiquen los tiempos de acceso de los archivos del dispositivo origen.

Es necesario contar con un bloqueador de escritura que permita una conexión segura del dispositivo de almacenamiento origen al equipo forense, evitando de esta manera el riesgo de modificación del estado inicial del medio de almacenamiento sometido al análisis.

Se deben realizar un mínimo de dos imágenes del dispositivo inicial, las dos copias se realizarán desde el dispositivo original, además se hace un hash del dispositivo, para poder dar fe de la integridad de los datos recién adquiridos y que más adelante no existan inconvenientes con su integridad.

Función Hash.

Se define como una operación que se realiza sobre un conjunto de datos de cualquier tamaño de tal forma que se obtiene como resultado, otro conjunto de datos denominado “resumen”, el cual tiene un tamaño fijo e independiente del tamaño original, que además tiene la propiedad de estar asociado unívocamente a los datos iniciales. Esta función se realiza para conservar la evidencia en el dispositivo original y se sigue trabajando sobre la copia.

3.1.8. Herramientas para informática forense

El análisis forense digital permite la identificación y descubrimiento de información relevante en fuentes de datos como pendrive o memorias USB, captura de tráfico de red, o volcado de memoria sin alterar su contenido. Existen muchas herramientas que se pueden utilizar según la tarea específica en las diversas etapas de informática forense y se pueden clasificar en diferentes categorías así:

- Herramientas de disco y de captura de datos
- Herramientas de análisis de archivos
- Herramientas de análisis de registro
- Herramientas de análisis de Internet
- Herramientas de análisis de correo electrónico
- Herramientas de análisis para dispositivos extraíbles
- Herramientas de análisis de sistemas operativos
- Herramientas de análisis de redes
- Herramientas forenses para bases de datos

Esta investigación se centra en las herramientas de análisis para dispositivos extraíbles, dentro de las cuales se encuentran las que permiten extraer y recuperar información, específicamente del pendrive.

Actualmente hay una gran cantidad de herramientas para realizar tareas específicas de recuperación de información y algunas son paquetes de herramientas que permiten realizar varias tareas por ejemplo: EnCase además de escanear el dispositivo permite, crear imágenes de discos para su posterior análisis, recuperar archivos de unidades que hayan sido formateadas, realizar borrado seguro de unidades a bajo nivel,

consultas de archivos por tiempos de creación, último acceso y última escritura, identificación de extensiones de archivos, múltiples soporte de archivos, genera los informes adecuados, además de exportar evidencias. En esta investigación no solo se hace el análisis desde la perspectiva del propósito investigativo donde no se debe alterar el estado del dispositivo, para que sea aceptado como evidencia en los casos de delitos informáticos, sino un enfoque de recuperación de información en términos generales, esto es, análisis forense enfocado a la recuperación de información en el dispositivo de almacenamiento pendrive que han sufrido daño inducido o accidental y por tal razón se ocasionó el borrado o inaccesibilidad a los datos almacenados.

3.1.9. Descripción de algunas herramientas de recuperación de información

A continuación, en términos generales, se hace una descripción de las herramientas más referenciadas, utilizadas para recuperar los datos y/o el dispositivo físico, una vez se ha producido un fallo en el mismo.

Algunas de las herramientas mencionadas en el presente documento se utilizan también para análisis forense, ya que permiten su utilización para búsqueda de ficheros borrados y búsqueda de pruebas en un dispositivo que ha sido manipulado con fines delictivos. En la tabla 8 de este documento, se presenta un resumen sobre estas herramientas y se agregan elementos complementarios para cada una de ellas, como: sistema operativo compatible y tipo de licencia entre otros.

WinHex: Software para informática forense y recuperación de archivos, Editor hexadecimal de Archivos. Apropiado también para peritaje informático, procesamiento de datos de bajo nivel y seguridad informática. Inspecciona archivos binarios, recupera datos borrados o perdidos en unidades dañadas.

Un editor hexadecimal es capaz de mostrar completamente el contenido de cada tipo de archivo. A diferencia de un editor de texto, uno hexadecimal incluso muestra los códigos de control y el código ejecutable, usando un número de dos dígitos basado en el sistema de numeración hexadecimal. . (Almeida, 2014)

Herramienta forense que se especializa en analizar el espacio libre en disco, espacio slack, espacio entre particiones y texto, creando así una descripción detallada de las unidades incluyendo los datos borrados y las secuencias de datos alternativas

- **TestDisk**: Software para recuperar archivos eliminados del pendrive para recuperar las tablas de particiones cuando están dañadas o han sido borradas por error, ayuda a recuperar datos perdidos en particiones y reparar sectores de arranque. TestDisk consulta al sistema operativo para encontrar los dispositivos de almacenamiento. Principalmente problemas causados por software defectuoso, algunos tipos de virus o errores provocados. Puede ser usado en procedimientos de computación forense. Testdisk permite recuperar particiones borradas, Reconstruir tablas de particiones, Reescribir el Master boot record (MBR), Arreglar tablas de arranque de tipo FAT, Reconstruir sectores de arranque NTFS. (cgsecurity, 2015).

- **PhotoRec**: es un software diseñado para recuperar archivos perdidos incluyendo vídeos y documentos, además recupera archivos eliminados de todo tipo, especialmente fotos eliminadas por algún error de las tarjetas de memoria flash, también es capaz de detectar otros ficheros y recuperarlos en caso de necesitarlo. PhotoRec hace una búsqueda profunda de los datos, funcionando incluso si el sistema de archivos está muy dañado o ha sido reformateado, usa un acceso de solo

lectura para manejar la memoria de donde recupera los datos perdidos. (Ecured, 2015), (Tannhausser, 2014).

- **R-Studio**: software de recuperación de datos, que han sido eliminados por ataque de virus o corte de corriente eléctrica; después de haberse reformateado la partición con archivos o aun para distintos sistemas de archivos; cuando la estructura de particiones del dispositivo ha sido cambiada o dañada. Recupera archivos eliminados sin papelera o cuando la papelera ha sido vaciada; Es especialmente útil cuando en el dispositivo aparecen constantemente sectores dañados y hace falta guardar inmediatamente la información que todavía no está dañada. Incluye: Módulo avanzado de reconstrucción de RAID, Editor de texto/hexadecimal con muchas funciones, Módulo avanzado de copia y creación de imágenes de discos en un único programa. Recupera datos de cualquier sistema de disco. (Castellanos, 2012)
- **Scalpel:** Es una utilidad GNU/Linux que utiliza la técnica de File Carving y que es capaz de leer los encabezados, pies de página y estructura interna de los archivos, accediendo a la base de datos de bloques donde están los archivos borrados, siendo capaz de identificar y recuperar al instante todo tipo de archivos: FAT, NFTS, EXT, HFS, entre otros. Es un programa muy útil para el análisis forense de archivos y para efectuar recuperaciones selectivas, ya que editando su configuración podemos seleccionar que tipo de extensiones de archivo, se quiere recuperar. (Tannhausser, 2014)
- **PC Inspector Smart Recovery**: es un software especializado en la recuperación de datos borrados por error de las tarjetas de almacenamiento flash, compact flash y cualquier dispositivo extraíbles. El programa busca archivos borrados y muestra una

vista de solo lectura, por lo que no modificará los archivos almacenados en la tarjeta. Cuando se seleccione el archivo que se quiere recuperar se tendrá que elegir un directorio en el ordenador para copiarlo. (Ranchal, 2015)

- **EnCase Forensics**: es una herramienta utilizada para la informática forense, recolecta datos digitales, realiza análisis, informa sobre descubrimientos y los preserva en un formato válido a efectos legales y validado por los tribunales, produce una duplicación binaria exacta del dispositivo o medio original usando un estándar sin pérdida (loss-less).y luego la verifica generando valores hash MD5 de las imágenes y asignando valores de CRC a los datos. Estas verificaciones revelan cuándo la evidencia ha sido alterada o manipulada indebidamente, ayudando a mantener toda la evidencia digital con validez a efectos legales para su uso en procedimientos judiciales (guidancesoftware, 2013)
- **Digital Forensics** Framework (DFF): es una herramienta de investigación forense digital y una plataforma de desarrollo que le permite recoger, preservar y revelar la evidencia digital. Entre otras, las funciones del DFF incluyen la capacidad de leer RAW, EWF y AFF formatos de archivos forenses, acceder a los dispositivos locales y remotos, analizar los datos del registro, buzón y del sistema de archivos y recuperar archivos ocultos y eliminados. (toolwar, 2014)
- **HELIX3:** es un Live CD basado en Linux que fue construido para ser utilizado en respuesta a incidentes, Informática Forense. Que está lleno de un montón de herramientas de código abierto como editores hexadecimales, carving software, password cracking y más. (Dragonjar, 2015)

  PC Inspector file recovery: Se trata de un programa capaz de recuperar archivos y rescatar datos eliminados, datos perdidos e incluso unidades perdidas. Posee además

la función especial de recuperación, que salva los archivos que no tienen ninguna indicación de directorio. en su listado de formatos, soporta un buen número de ellos, incluyendo los más usados normalmente, como ARJ, AVI, BMP, CDR, DOC, DXF, DBF, XLS, EXE, GIF, HLP, HTML, HTM, JPG, LZH, MID, MOV, MP3, PDF, PNG, RTF, TAR, TIF, WAV o ZIP También ofrece una guía de ayuda y la posibilidad de cambiar el idioma. Reconstruye también los datos en los que no exista posible indicación del directorio al que pertenecen. (Jorge Juan, 2014) (Ranchal, 2015)

- **Foremost:** es una herramienta forense para recuperar archivos borrados y datos en general intenta recuperar los datos borrados aplicando una técnica llamada file carving. La técnica del file carving consiste en recuperar archivos y datos. Foremost escanea la totalidad de contenido del dispositivo de almacenamiento intentando identificar si el contenido escaneado contiene las estructuras hexadecimales típicas de inicio y fin de un determinado tipo de archivo. En el momento que Foremost localice una de estas estructuras (inicio-fin), extraerá la información contenida entre el inicio y el fin recuperando así un archivo que previamente se había borrado.
- **Disk Recovery**: herramienta de gran alcance para recuperar la información perdida. Escanea todos los sectores del disco duro, tarjeta de memoria o cámara digital para asignar la presencia de los archivos perdidos. Incluso si el sistema de archivos está dañado o formateado, se puede reconstruir.(spyware, 2014)
    - **GetDataBack:** herramienta para la recuperación de archivos en dispositivos extraíbles aunque Windows no lo reconozca como unidad, o se haya perdido toda la información de estructura de directorios. Recupera información de memorias

sin formato, todo tipo de datos aunque el borrado se haya realizado hace tiempo. no sin antes saber qué sistema de archivos es NTFS o FAT.(Quituisaca, 2010)

- **Recuva**: Este es un software de recuperación de datos borrados (documentos, video, fotos, música) de discos duros, tarjetas de memoria, pendrive o cualquier medio extraíble

  Para recuperar datos perdidos o borrados con Recuva hay que dejar de usar la unidad que se quiere recuperar lo menos posible ya que cuanto más la usemos más difícil será recuperar los datos. Se debe evitar usar la misma unidad donde están los datos que se quieren recuperar. (Castellanos, 2012).

- **Wise Data Recovery**: es un software de almacenamiento para recuperar archivos eliminados accidentalmente, puede extraer los datos eliminados de cualquier tipo de medio de almacenamiento externo, los cuales incluyen unidades Flash, tarjetas de memoria y reproductores MP3. Recupera los documentos como Word, Excel, TXT, también foto / imagen, como Jpg, Png, Gif, Recupera archivos de correo electrónico, recupera audio, video, y muestra el estado explícito de los datos que deben recuperarse. (Ranchal, 2015)

- **HDDScan:** Es una herramienta muy sofisticada, que permite realizar un chequeo integral del dispositivo en busca de fallas. Similar a TestDisk, la principal ventaja de HDDScan es que trabaja a bajo nivel, que es donde mayor interacción es posible de lograr entre el software y el hardware. Busca en el sistema los dispositivos de almacenamiento que estén instalados, Una vez encontrados, se puede ver la información relativa a cada uno de los dispositivos. (intowindows, 2013)

- **USB Show**: Aplicación que ayuda a poder ver archivos, que por algún virus o persona fueron escondidos. USB Show se puede utilizar en cualquier dispositivo de almacenamiento extraíble. USB Show recuperara todos los archivos ocultos, posiblemente también algún malware es por eso que debe ser usado con mucha precaución. Antes de recuperar sus archivos es recomendable que el sistema donde vaya a realizar esta acción no esté infectada por algún malware.(Ccm, 2015)
- **Micron USB Drive Data Recovery**: es una herramienta para recuperar cualquier archivo que se encuentre en un pendrive o dispositivo de almacenamiento USB que se haya dañado por cualquier motivo, ya sea externo o interno. Tiene la opción de hacer una búsqueda avanzada o estándar. Micron USB Drive Data Recovery es perfectamente compatible con productos de SanDisk, Transcend, Kingston, Lexar, Super Flash, Sony, Super media o Toshiba, entre otros. (Clubic, 2014)
- **Pen Drive Data Doctor Recovery**: software para recuperar datos perdidos del pendrive, recuperación automática y de todo tipo de ficheros, funciona aun en los peores casos de corrupción y daño de unidades USB removibles. Se pueden perder los datos del pen drive por formatear accidentalmente, los archivos pueden estar dañados y diferentes virus pueden eliminar los archivos también. Cualquiera que sea la razón, Pen Drive Data Doctor Recovery puede ayudar a recuperar los datos perdidos y archivos. Hay algunas formas poco comunes que pueden hacer que pierdas el acceso a los datos del pen drive, como la pérdida de la partición. Cuando se produce este problema, se perderán los datos del dispositivo al intentar pasar de un PC a otro. Incluso esta compleja situación puede ser manejada por Pen Drive Data Doctor Recovery. (Software.informer, 2015)

- **Remo Recuperar:** Es una herramienta considerada de las mejores aplicaciones para rescatar información, recuperación de archivos perdidos / borrados. Ha sido diseñada con una opción integrada encontrar, lo que ayuda a encontrar y localizar cualquier archivo en particular sobre la base de diferentes atributos de archivo. Recuperación de archivos perdidos / borrados debido a errores en el sistema de archivos, Se desarrolla con gran variedad de opciones de recuperación para que no sólo rescata los datos del disco duro del ordenador, sino también restaura archivos desde unidades de almacenamiento como tarjetas de memoria flash, unidades USB. Remo Recover es una herramienta ideal para recuperar datos perdidos o eliminados del pendrive, independientemente de la situación de pérdida de datos. Se trata de una herramienta bien construida con algoritmos de recuperación de datos altamente avanzadas para rescatar datos perdidos o eliminados. Es segura y confiable para recuperar datos. Este software funciona con éxito en todo el sistema operativo Windows. (TechGeekShan, 2015).

  Es una utilidad perfecta para recuperar tabla de particiones pérdidas o eliminadas conservando los datos intactos. Realiza una exploración rigurosa para encontrar y localizar la tabla de particiones. A continuación, extrae la tabla de particiones de forma segura y sin causar ningún daño a los datos almacenados en él. Esto a su vez trae todas las particiones de vuelta y por lo tanto sus datos se pueden restaurar de ella fácilmente. Además, esta herramienta también se puede utilizar para recuperar datos de la partición que tiene sectores defectuosos sin esfuerzo con la máxima facilidad. (Remo software, 2013)

- **Partition Wizard**: Es una herramienta de particionado de discos, capaz de reparar todo tipo de unidades de almacenamiento. Recupera particiones perdidas del

pendrive La recuperación de las particiones perdidas solo es posible si el dispositivo es reconocido por el equipo. Un nuevo icono debería aparecer en la lista de unidades del PC. Si la tabla de particiones está dañada, no podrás abrir la memoria con normalidad. En lugar de carpetas, mostrara un aviso similar a "Inserte un disco en Disco extraíble", o bien este otro aviso, "Formatee el disco en la unidad para poder usarlo". El error depende del tipo de problema que tenga el disco, pero el resultado es siempre el mismo: no podrán verse los datos almacenados previamente. Partition Wizard cuenta con dos métodos de escaneo de disco: rápido (Quick Scan) y profundo (Full Scan). El escaneo rápido es la mejor opción para la mayoría de situaciones. Usa el escaneo completo solo si el rápido no encuentra nada.(softonic, 2015)

- **Wondershare Data Recovery**: Es un software efectivo para recuperación de datos en ordenadores y dispositivos de almacenamiento, recupera vídeos, fotos, emails, música y documentos perdidos en el disco duro así como en memorias USB y otros dispositivos de almacenamiento, recupera archivos en más de 550 formatos de forma rápida, segura y completa. (wondershare, 2015)
- **Handy Recovery**: es un software que permite recuperar datos. Está diseñado para restaurar ficheros accidentalmente borrados de los discos duros y pendrive. El programa puede restaurar ficheros dañados por ataque de virus, apagones y errores del software o ficheros de las particiones borradas y formateadas. Si un programa borra los ficheros sin usar la Papelera de Reciclaje, Handy Recovery puede recuperar esos ficheros. También puede recuperar ficheros enviados a la Papelera de Reciclaje después de que esta ha sido vaciada. soporta todos los sistemas de ficheros de Windows para discos duros y pendrive incluso FAT12/16/32,

NTFS/NTFS 5 y recuperación de imágenes de tarjetas Compact Flash, Smart Media. Puede recuperar los ficheros borrados y cifrados en los discos NTFS. (software.informer, 2015)

- **Easy Drive Data Recovery**: es un programa para recuperar datos borrados, dañados o formateados por error, fallas del software o cualquier otro tipo de razones. El programa utiliza algoritmos únicos que permiten recuperar archivos que no están presentes en las entradas del sistema de archivos. Es posible recuperar fotos, imágenes, música, juegos y toda la información. Para recuperar archivos borrados de USB, Easy Drive Data Recovery funciona tanto con almacenamiento externo como interno y admite todo tipo de unidades Flash y USB. El software plantea varios modos de recuperación: Scan Normal, que recupera fácilmente datos normales del pendrive; Scan Deleted, que sin esfuerzo recupera datos borrados del pendrive y Scan Formato, que recupera fácilmente datos con formato pendrive.(munsoft, 2015)

- **Picture Recovery Software for USB Media**, también llamado Digital Picture Recovery, es una herramienta destinada principalmente a encontrar y recuperar imágenes perdidas a causa de cualquier situación que haya podido dañar una unidad de almacenamiento USB. Cuenta con una interfaz muy sencilla, es una aplicación bastante útil y de uso sencillo, realiza escaneo a la unidad y una vez termina, deja opción de elegir las imágenes que se quieren recuperar y a continuación comienza su recuperación. (Cruz, 2011)

- **Flash Memory Recovery** herramienta capaz de recuperar datos almacenados en tarjetas de memoria, dispositivos periféricos, unidades USB y, en definitiva, cualquier dispositivo digital que utilice memoria flash, incluso aunque estos estén

dañados. No importa el tipo de documento ni su formato, Flash Memory Recovery escaneará el dispositivo e intentará encontrar todos los ficheros que puedan ser recuperados. El programa cuenta con una interfaz muy sencilla, en sólo cinco pasos se realizara el proceso de recuperación de los archivos perdidos ya sea por: borrado accidental, archivos dañados, unidades formateadas, documentos borrados por otras aplicaciones, entre otras causas. (Cruz, 2011)

Como se puede apreciar existen muchas herramientas que permiten diagnosticar la causa del fallo y ver el estado de una unidad extraíble, dar solución a los diferentes casos de pérdida de información (accidentalmente, por virus u otras causas) y daños del pendrive (físicos y lógicos), algunas incluso rescatan particiones pérdidas y sectores de arranque, pero desgraciadamente no es garantizada una solución segura al 100% , teniendo en cuenta que en ocasiones la unidad presenta problemas físico que no se pueden resolver con ninguna herramienta, el tratamiento en la mayoría de estos casos es electrónico.

Nota: Cabe indicar que existen herramientas que al momento de recuperar la información perdida mantienen un límite de volumen de información.

3.2 Recuperación de datos en dispositivos de almacenamiento

La recuperación de datos consiste en llevar a cabo un conjunto de acciones para conseguir el acceso a los medios de almacenaje y así poder extraer información perdida o inaccesible contenida en los mismos.

Los usuarios suelen utilizar el pendrive, pero casi nunca hacen una copia de seguridad de la información en él almacenada y a menudo se piensa que los datos en un pendrive que ha sido dañado se pierden para siempre, pero sabiendo la importancia del

valor de la información es necesario y obligatorio recuperarla, no hacerlo en ocasiones trae costos no solo económicos sino también pérdida de confidencialidad y ventaja competitiva.

A continuación se expondrán algunos de los métodos generales reportados en la literatura para recuperar información tanto en discos duros como en pendrives**.**

3.2.1 Métodos de recuperación en discos duro

En esta sección se van a citar algunos de los métodos para la recuperación de discos dañados, ya que en su mayoría también son aplicables al pendrive.

- Moya (s. f.) realiza un método a través de la utilidad Testdisk, vía el sistema operativo Parted Magic OS para recuperar una partición perdida y los archivos contenidos en ella.

  Los pasos sugeridos son:

Paso 1. Se descarga Parted Magic OS: sistema operativo Live diseñado para realizar tareas sobre unidades de disco tales como: recuperar archivos, particionar, clonar, testear, realizar pruebas de rendimiento, borrado seguro, entre otras. Y se graba en un CD o un pendrive como imagen ISO

Paso 2. Se inicia el sistema operativo Parted Magic OS

Imagen 6: Captura iniciación Parted Magic OS tomada de (Moya (s.f.)

Paso 3. Seguir la ruta System Tools/TestDisk a través del icono situado en la esquina inferior izquierda. Se presentarán las especificaciones de testdisk en una ventana. Al seleccionar "créate" mostrará las unidades de almacenamiento físico instaladas así:

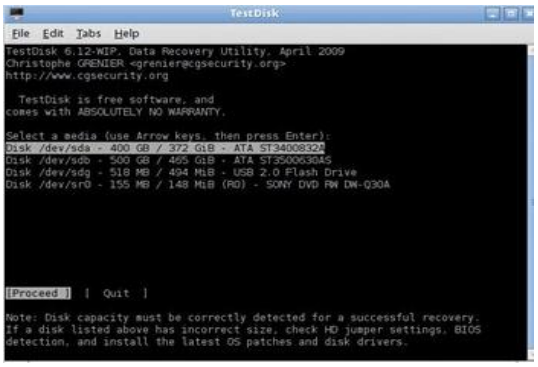


Imagen 7: Captura ejecución TestDisk tomada de (Moya (s.f.)

Paso 4. Elegida la tabla de particiones correspondiente se presentan las siguientes opciones: Analyse, Advenced, Geometry, Options, MBR code, Delete, Quit.

Pulsar sobre Analyse para que estudie la estructura actual de particiones y busque también particiones perdidas.

Paso 5. La nueva pantalla muestra las particiones encontradas en un primer escaneo. La información que ofrece es: Partición (número de partición, tipo de partición - primaria, lógica, bootable- y estructura de archivos), Comienzo (cilindro, cabeza y sector), Final (cilindro, cabeza y sector) y Tamaño en sectores. Además, da la opción de hacer una búsqueda rápida (Quick Search) o realizar una búsqueda en profundidad (Deeper Search), si fuese necesario, esto es, sino se ve la estructura correcta en la tabla mostrada.

Paso 6. Edición de las particiones. En este punto, se encuentra que en la tabla de particiones mostrada hay dos o más que ocupan exactamente el mismo lugar (cilindro, cabeza y sector) o que se superponen, quiere decir que ha encontrado dos particiones

solapadas, una NTFS y otra FAT32, siendo esta última la que verdaderamente se quiere recuperar.

Ubicándose con el cursor sobre la partición y pulsando P, muestra la estructura de directorios de dicha partición, por lo que, ante la duda, se puede averiguar cuál contiene los archivos correctos. Una vez que se decidida qué partición se quiere recuperar y cuál se desea borrar, solo hay que situarse sobre la misma y, con los cursores derecho e izquierdo, dejar en D la que se quiere eliminar y en P, L, o *, según el caso, la que se quiere recuperar.

Una vez realizados estos pasos, solo queda escribir la tabla de particiones correcta pulsando sobre Write. Tras reiniciar el equipo, se deberá haber recuperado la partición perdida y los archivos contenidos en ella.

- Wikihow (s. f.) define los siguientes cuatro métodos para la recuperación del disco:

Primer método: para comprobar el estado del disco duro.

Se realiza mediante los siguientes pasos:

Paso 1. Inspeccionar que el lado externo del disco duro no tenga daños, para esto se debe dejar de utilizar la computadora o el disco duro externo. Apagar la computadora o desconectar el disco externo. Quitar el disco duro de la computadora o el dispositivo. Examinarlo con cuidado para comprobar si tiene puntos calientes u otro daño en la tarjeta controladora externa. Verificar si hay alguna pieza rota.

Imagen 8: lado externo del disco duro tomada de Obando (2015)

Paso 2. Cambiar el cable: Conectar el disco duro con cables nuevos (de alimentación y transferencia de datos) para estar seguro que funcionan bien, y probar de nuevo. Tener en cuenta que si es un disco IDE, se necesitará un cable plano.

Imagen 9:Disco duro IDE y SATA tomada de Auyanet (2013)

Paso 3. Si es un disco PATA (IDE /EIDE), cambiar las configuraciones de los pines. Si estaba en modo "esclavo" o en "selección por cable", colocarlo en la posición "maestro". Conectarlo sin otro dispositivo en ese puerto y probar de nuevo.

Imagen 10: Disco duro PATA (IDE) tomada de Chaparro (2015)

Imagen 11: disco duro PATA EIDE tomada de Chaparro (2015)

Paso 4. Probar con otros IDs y/u otro controlador PCI e intentar determinar si funciona. Si no se tiene otro controlador, una tarjeta PCI que añada puertos a la computadora, simplemente cambia el ID.

Imagen 12: controlador PCI tomada de Hernandez (2015)

Paso 5. Conectar el disco a un adaptador de discos externo o a un alojamiento de disco externo (por ejemplo, un USB), si se tiene. Si no arranca, intentar conectarlo a otra fuente de alimentación (incluye la conexión de datos, ya que algunos discos no funcionan sin ello). Si ninguna de las dos maneras funciona, es probable que la falla esté relacionada con el circuito impreso.

Imagen 13: Adaptador externo de disco tomada de Kirsch (2013)

Paso 6. Conectar el disco a una computadora diferente y probar otra vez. Si enciende, es posible que la placa madre esté dañada, y no el disco duro.

Imagen 14: Disco duro conectado a otro equipo tomada de Araiza (2013)

A continuación se adiciona un diagrama que ilustra en forma esquemática la funcionalidad descrita. La representación pictórica, ayuda a su comprensión y es muy útil para determinar cómo funciona realmente. Describe los pasos del método y como se relacionan entre sí.

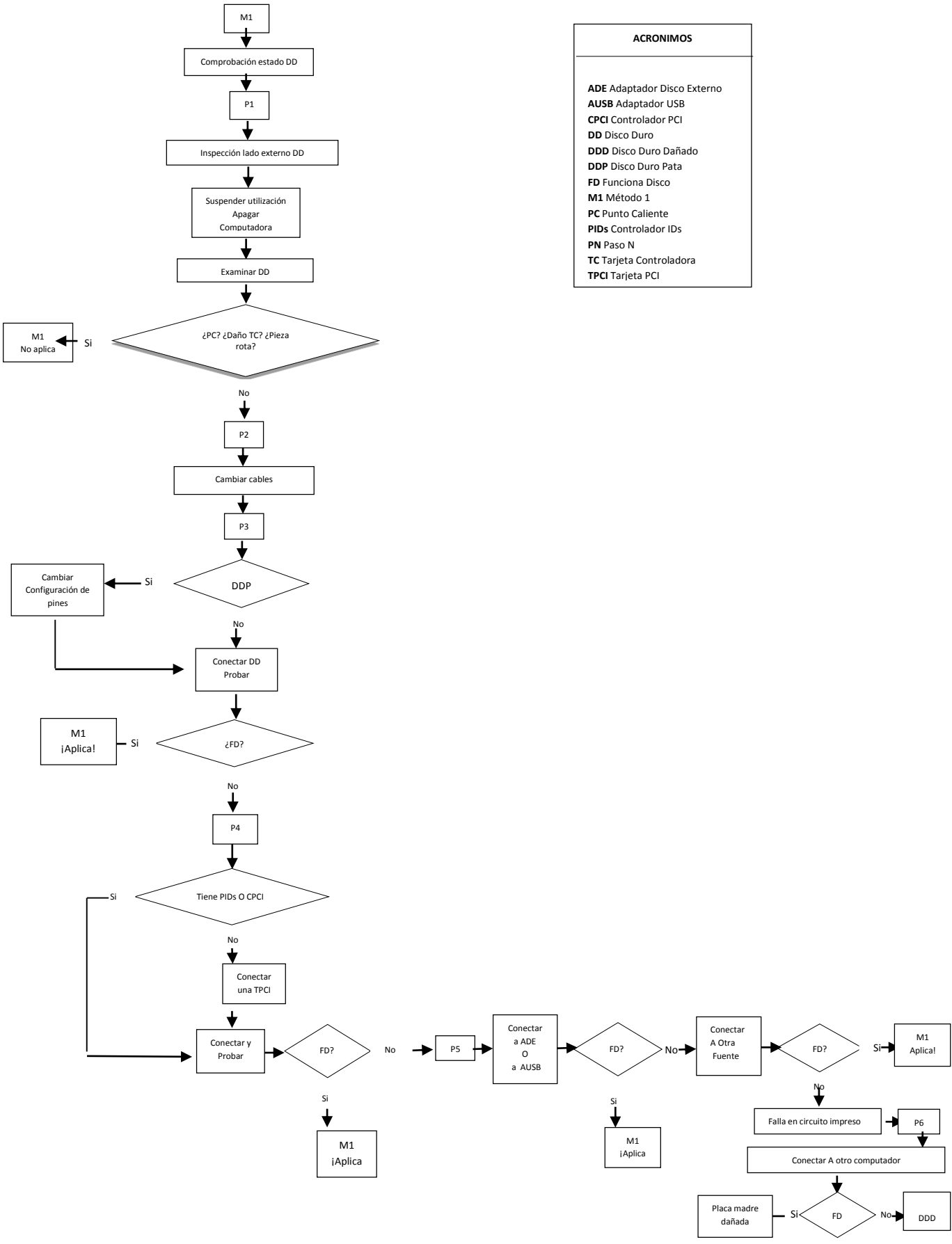


Imagen 15: Diagrama del Primer método

Segundo método: para cambiar la tarjeta controladora del disco duro.

Se realiza siguiendo los pasos a continuación:

Paso 1. Observar la tarjeta controladora y determinar si se puede quitar sin exponer los platos del disco.

Imagen 16: Tarjeta controladora de disco duro tomada de Arangón (2016)

Paso 2. Conseguir un disco duro para experimentar, es muy importante que sea del mismo número de modelo y progresión (es decir, la misma versión de firmware y el mismo número de tarjeta de circuito impreso).

Imagen 17:Discos duros del mismo modelo tomada de Jcristhianp (2008)

Paso 3 .Quitar la tarjeta controladora del disco duro dañado. Quitar con cuidado los tornillos, con el destornillador adecuado. Aprenda cómo está conectada al disco. La mayoría de los discos se conectan con cables planos y filas de pines. Sea cuidadoso y no dobles ni dañes los conectores.

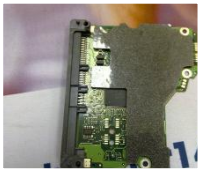


Imagen 18: tarjeta contoladora externa tomada de Auyanet (2011)

Paso 4. Retirar la tarjeta controladora del disco que funciona. También se debe hacer con cuidado.D

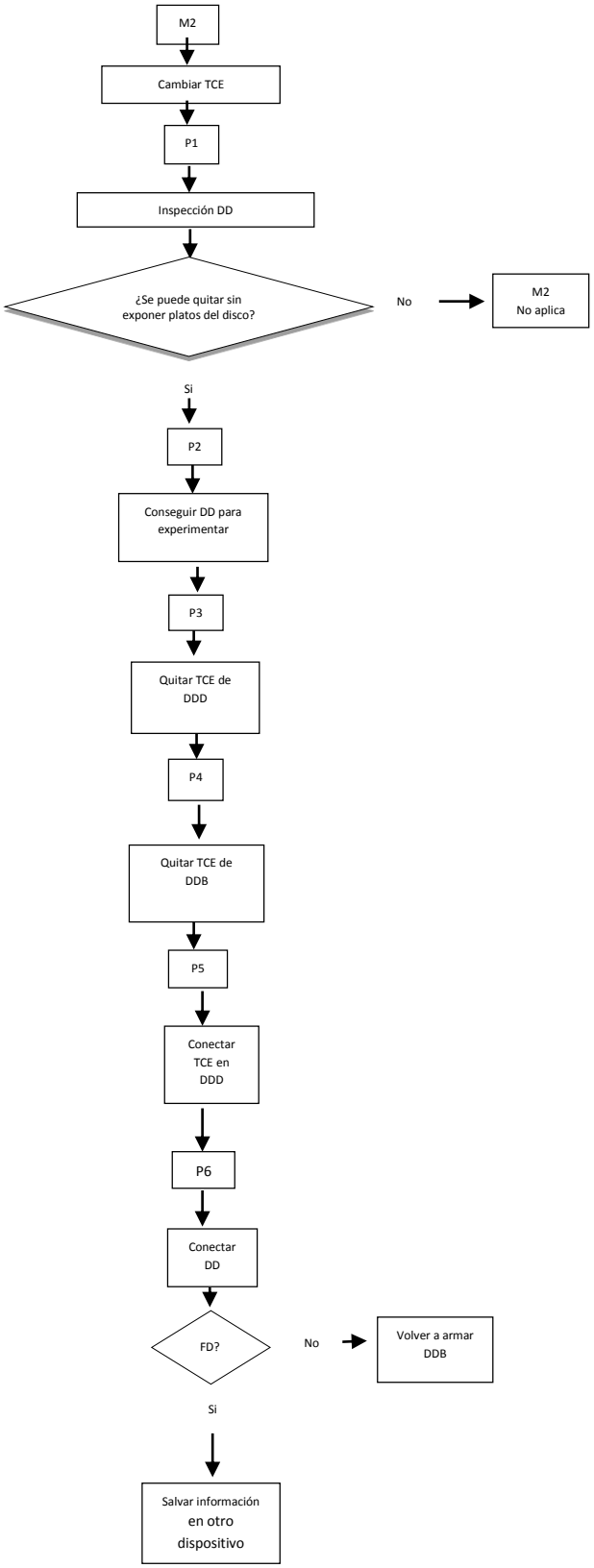
Imagen 19: Tarjeta controladora tomada de Jcristhianp (2008)

Paso 5. Conectar la tarjeta que funciona al disco dañado.

Imagen 20:Tarjeta controladora conectada tomada de Jcristhianp (2008)

Paso 6. Conectar el disco a la computadora o al dispositivo y probarlo. Si funciona, copia inmediatamente los datos en otro disco duro u otro dispositivo. Si no funciona, intenta volver a armar el disco que se compró con la tarjeta controladora que funciona.

A continuación se adiciona un diagrama que ilustra en forma esquemática la funcionalidad descrita. La representación pictórica, ayuda a su comprensión y es muy útil para determinar cómo funciona realmente. Describe los pasos del método y como se relacionan entre sí.



ACRONIMOS

DD Disco Duro
DDB Disco Duro Bueno
DDD Disco Duro Dañado
FD Funciona Disco
M2 Método 2
PN Paso N
TCE Tarjeta Controladora Externa

Imagen 21: Diagrama del Segundo método

Tercer método: para recuperar los datos con las utilidades de reparación del sistema de archivos de Windows.

Muchas veces, cuando Windows no puede detectar el disco duro, se debe a que el sistema de archivos está dañado. En el caso de que haya sucedido esto, lo mejor es tomar una imagen del disco antes de ejecutar algún tipo de utilidad de "reparación del sistema de archivo, con el fin de poder revertir si es necesario al estado original. En Linux, se puede usar el comando DD para crear una imagen del disco duro de forma correcta.

Imagen 22: ilustracion de una imagen de disco tomada de javierkum (2012)

Se puede utilizar un cd de instalación de Windows para encender el equipo y seleccionar el panel de recuperación. Una vez ubicado en la petición de comandos, utilizar "chkdsk" para reparar el sistema de archivos como se ve a continuación.

Imagen 23:Captura del comando CHKDSK tomada de NorfiPC (s.f)

/f - Corrige errores en el disco

/r - Encuentra sectores dañados y recupera la información que sea legible

/l - Realiza una comprobación menos exhaustiva de entradas de índice (Sólo para NTFS)

/c - Omite la comprobación de ciclos dentro de la estructura de carpetas (Sólo para NTFS)
Los dos anteriores reducen la cantidad de tiempo necesario para ejecutar Chkdsk ya que omiten ciertas comprobaciones en el volumen.

/x - Fuerza al volumen a desmontarse primero si es necesario (es necesario usar /f)

/b - Vuelve a evaluar los clústeres incorrectos en el volumen es necesario usar /R (Sólo para NTFS)

/v - Para FAT/FAT32 muestra la ruta completa y el nombre de cada archivo en el disco, si es NTFS muestra mensajes de limpieza si hay.

Imagen 24: Opciones para uso del comando CHKDSK tomada de NorfiPC (s.f)

Cambiar la letra de unidad por la letra del disco respectivo y seguidamente como parámetro /f que indica corrección de errores en el disco

Chkdsk (letra de unidad):/f.

Esta es la manera como Windows intenta recuperar el sistema de archivos.

A continuación se adiciona un diagrama que ilustra en forma esquemática la funcionalidad descrita. La representación pictórica, ayuda a su comprensión y es muy útil para determinar cómo funciona realmente. Describe los pasos del método y como se relacionan entre sí.

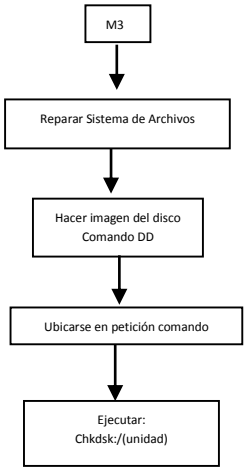


Imagen 25: Diagrama del Tercer método

Cuarto método: para recuperar datos con photorec

Imagen 26: Captura ejecución Photorec tomada de (Zagur, 2013)

Photorec es un software de recuperación de datos/archivos. Este software ignora el sistema de archivos y busca lo que se conoce como cabecera de archivos (la primera parte de cada archivo) y le indica al OS qué tipo de archivo es sin que el sistema tenga que leer la extensión. Este programa se adaptó para buscar también cabeceras que no sean de audio/video. Actualmente, puede buscar hasta 80 tipos de archivos diferentes. Photorec es parte del paquete de Testdisk. Para instalarlo en Linux Distro basado en Debian, se ejecuta el siguiente comando como usuario root.

apt-get install testdisk

Si no se puedes ingresar como root, se agrega al comando anterior "sudo", así:

Sudo apt-get install testdisk

Para usar Photorec en una imagen de archivo en Linux, usa el comando: sudo photorec /log imagefilename -d /some/directory/to-store/recovered/ítems.

Para recuperar archivos directamente desde un dispositivo, ejecutar Photorec sin ningún argumento, se verá un menú de dispositivos disponibles.

sudo photorec /log

Sólo se debe usar esta utilidad si no se puede reparar la partición porque se perderán los nombres de los archivos.

Lo que hace este programa es buscar el disco rígido de los archivos legibles buscando las cabeceras y copiándolas dónde lo indiques con la bandera -d. Como norma general. Muchos tipos de archivos contienen cierta información en la cabecera u otras ubicaciones que permiten recuperar parte del nombre del archivo original, o al menos proporcionar nombres más significativos.

3.2.2 Métodos para recuperación tanto discos duros como pendrives

- Vásquez (2014) define los siguientes dos métodos para recuperar archivos borrados de diferentes medios de almacenamiento donde se incluyen discos duros y pendrives.

Método 1: Recuperación con Data Recovery Wizard

Data Recovery Wizard, es un software libre, Con este se puede recuperar lo que sea, incluso luego de haber formateado.

Paso 1 Descargar el programa e instalarlo.

Paso 2 Ejecutar el programa: se ejecuta y aparecerá lo siguiente:

Imagen 27: Captura Data Recovery wizard tomada de (Vásquez, 2014)

Paso 3 se eligen los tipos de archivos que se quieren recuperar, ya sean fotos, vídeos o todo tipo de archivos y se das clic a "Siguiente".

Nota: La versión gratis de ese programa, tiene como límite de 2GB de archivos a recuperar, si se quieren recuperar más de 2GB de datos es recomendable usar la versión comercial.

Paso 4 elegir en donde se encuentran los archivos que quieres recuperar, si es una memoria USB debe conectarse al ordenador para que aparezca como opción a elegir:

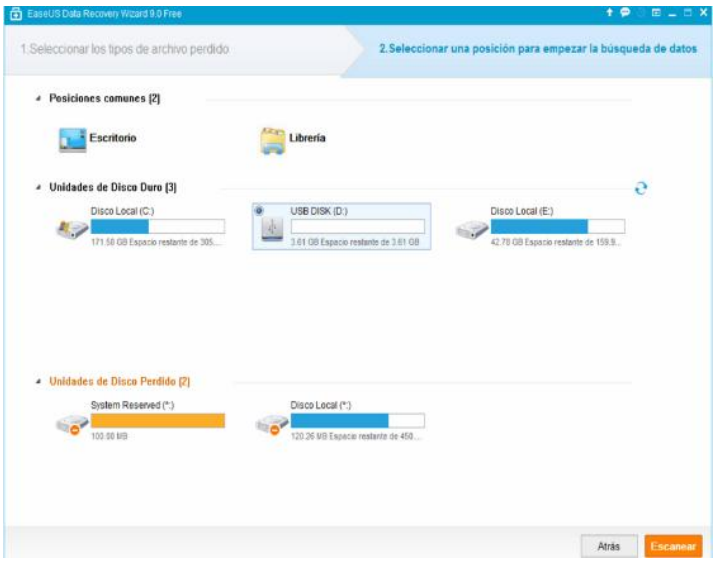


Imagen 28: Captura elección unidad tomado de (Vásquez, 2014)

Paso 5 dar clic al botón que está debajo que dice "Escanear". El programa comenzará a buscar los archivos eliminados de la unidad de almacenamiento elegida.

Paso 6 Después de que termine se pueden elegir los archivos que se quieren recuperar. Es importante saber que el escaneo puede tardar mucho tiempo, ya que se realiza un escaneo profundo.

Método 2 Recuperación con Pandora recovery

Pandora recovery, es un software libre, poco pesado y muy sencillo, que puede recuperar información en todo tipo de unidades incluso luego de haberlas formateado.

Paso 1 descargar el programa.

Paso 2 instalar y ejecutar el programa

A continuación aparecerá lo siguiente ventana:

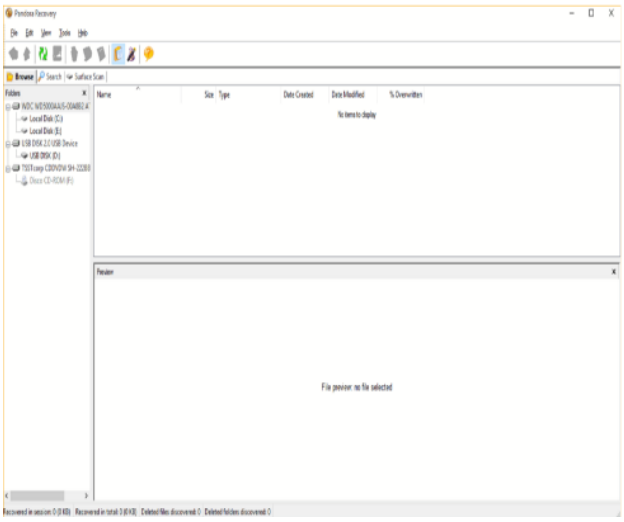


Imagen 29: Captura Pandore Recovery tomada de (Vásquez, 2014)

En la parte izquierda aparecen todas las unidades de almacenamiento conectadas al ordenador.

Paso 3 si se quieren recuperar los archivos de una USB, tarjeta microSD, disco duro externo o dispositivo móvil deberá conectarse para que aparezca ahí y luego de conectarlo

Paso 4 dar clic al botón verde de arriba que tiene el símbolo de  .

Paso 5 Luego dar clic a la unidad de almacenamiento donde están los archivos que se quieren recuperar. El programa de forma inmediata comenzará a escanear esa unidad de almacenamiento en busca de los archivos eliminados para su recuperación.

Paso 6 Luego de que termine de escanear, entonces elegir cuales son las cosas que se quieren restaurar.

- Tannhausser (2014) Propone un método haciendo uso la herramienta foremost de la siguiente manera:

Foremost es una utilidad en línea de comandos que permite recuperar archivos borrados de discos duros, memorias USB, entre otros. Foremost hace uso de una técnica denominada data mining que recupera los archivos basándose en sus encabezados, pies de página y estructura interna de los mismos, lo que le permite recuperar una gran variedad de formatos, ya que permite filtrar el tipo de extensiones que se quieren recuperar.

Instalación de Foremost:

En Ubuntu y derivadas como Linux Mint como sigue:

sudo apt-get install foremost

En Arch Linux y derivadas como Manjaro o Antergos, como sigue:

yaourt -S foremost

La sintaxis típica en línea de comandos para ejecutar el programa es:

Ejecutar como root:

foremost -v -t pdf -i /dev/sdb1 -o /home/jose/datos

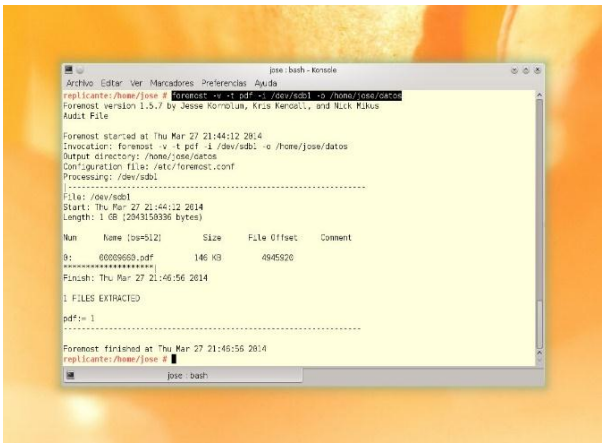


Imagen 30: Captura ejecución Foremost tomada de Tannhausser (2014)

Donde el parámetro -v establece el modo ver José (es opcional, pero nos permite ver cómo transcurre todo el proceso en la consola), -t selecciona el tipo de archivo (en este caso PDF), -i indica la partición o carpeta de la que deseamos recuperar, -o la carpeta destino, que el programa crea automáticamente (en este caso datos)

Si lo que interesa es recuperar todos los datos sin distinguir entre tipos de archivos se hace con el parámetro all. Ejecutando como root lo siguiente:

foremost -v -t all -i /dev/sdb1 -o /home/jose/datos

3.2.3 Métodos para recuperar información en pendrive con daño inducido o accidental

Durante la exposición del proceso de recuperación de la información de un pendrive intervienen los conceptos: Utilidades, programas, aplicaciones, técnicas y herramientas, cuyo estricto significado depende del contexto, esto es, todo aquello que en un momento dado lo rodea, por tanto no se hará aclaración alguna en su uso particular.

En los diferentes métodos empleados para la recuperación de la información contenida en dispositivos de almacenamiento extraíble, los pendrive son un ejemplo, existen técnicas y herramientas que se aplican para recuperar datos perdidos ya sea por daño físico del dispositivo, borrado accidental o premeditado, corrupción del sistema de archivos o ataques de virus, entre otros.

Los sistemas operativos incluyen una serie de comandos, órdenes directas de proceso, que se ejecutan desde la aplicación de escritorio, intérprete de ellos, los hay que detectan el problema cuando la unidad falla y si la información es recuperable ayudan en el proceso. La parte de los sistemas operativos que realiza este tipo de tareas son: en Windows se identifica como CMD y en Linux como Terminal o SHELL.

A continuación se definen los más comunes tipos de daño y sus correspondientes métodos de solución.

Daño físico

Este daño es manifiesto cuando se conecta el pendrive y no es reconocido en ningún puerto por motivo alguno, si tiene led indicador de transferencia, este no parpadea.

Estos fallos pueden ocurrir por:

1. **Forzamiento del dispositivo en el conector USB**: ocasiona averías en alguna pieza móvil o daña la soldadura del pin del conector y por ende el contacto a la placa. Los pendrive tienen una postura única de dirección para insertarse en el puerto conector porque son unidireccionales, sino se inserta en la dirección correcta y se violenta el proceso de conexión podría romperse tanto el dispositivo como el conector.
2. **Cortocircuitos y sobrecarga de energía, recalentamiento, o cargas electroestáticas:** queman cualquier fusible del dispositivo.
3. **Polarización inversa o inserción en puertos USB cruzados o quemados**: quema la resistencia de protección.
4. **Golpes o caídas del dispositivo:** es posible que el cristal de cuarzo se quiebre o se rompan los circuitos.

Según el sitio web Soloelectrónicos, (2014). Los métodos para reparar los daños físicos son:

Caso1.

La unidad flash puede tener el conector roto o hace mal contacto a la placa. Una solución es rearmar el dispositivo de forma temporal, haciéndolo funcionar el tiempo

suficiente para extraer la información que contiene, puentear los contactos del conector USB de la placa flash a un nuevo cable USB.

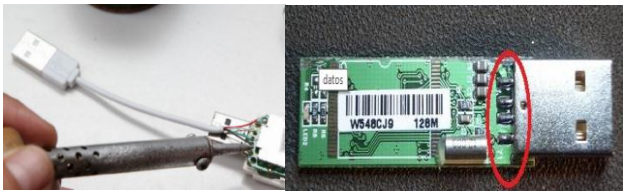


Imagen 31: Pines del conector del pendrive imagen tomada de (solo electrónico, 2014)

Paso 1: Inicialmente debe disponer de las siguientes herramientas: Un soldador de punta fina, un cable USB macho reciclado, un pelacables, un pequeño destornillador de punta plana, una lupa.

Paso 2: Con el destornillador de punta plana, retirar con cuidado la carcasa externa de la unidad flash Utilizar la lupa para inspeccionar la placa de circuito impreso y los puntos de soldadura.

Los puntos de soldadura son los 4 puntos gruesos de que comunican los contactos del conector USB a las líneas de cobre en la tarjeta de circuito. Si el conector se ha desprendido sin causar daños a los puntos de soldadura o a la PCB, puede continuar con el paso siguiente.

Paso 3: Colocar la unidad flash sobre una superficie dura, con los puntos de soldadura hacia arriba.

Paso 4: Cortar el extremo macho del cable USB.

Paso 5: Utilizar el pelacables para exponer aproximadamente 0,6 cm (0,25 pulgadas) de cada uno de los cuatro hilos en el interior del cable.

Paso 6: Soldar cada uno de los cuatro hilos a los cuatro puntos de soldadura: Los colores de izquierda a derecha son negro, verde, blanco y rojo. Se deben adjuntar a los puntos de soldadura en este orden.

Paso 7: Conectar el otro extremo del cable USB a una computadora para verificar si es reconocido el dispositivo, proceda a recuperar la información.

Caso2.

La unidad tiene quemada la resistencia de protección. Una posible solución es reemplazar la pieza siguiendo los siguientes pasos:

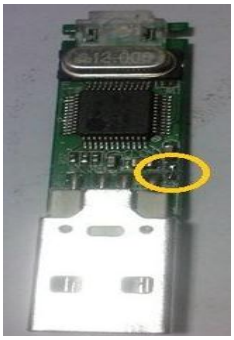


Imagen 32: Resistencia fusible imagen tomada de (solo electrónico, 2014)

Paso 1: determinar cuál es la resistencia a cambiar o puentear siguiéndole el rastro con un multímetro o con una lupa, fijarse en el valor, es el que indica 2R2

Paso 2: reemplazar este componente con otro de la misma resistencia que generalmente es del orden de 1 a 5 ohm.

Nota: La resistencia generalmente está ubicada cerca del puerto conector USB, este componente se puede conseguir en tiendas electrónicas.

Paso 3: una vez reemplazado el componente pase a verificar si es posible recuperar la información.

Caso3.

El cristal de cuarzo se quebró por golpe o caída. Hay que reemplazar dicho componente, buscarlo en otro pendrive o alguna tarjeta electrónica que lo contenga teniendo en cuenta el valor de frecuencia de oscilación que generalmente es de 12 a 24 MHz al reemplazarlo hay que tener precaución de no juntar sus pines.

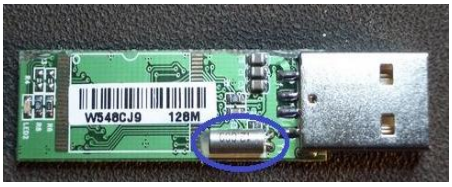


Imagen 33: Cristal de cuarzo del pendrive imagen tomada de (solo electrónico, 2014)

Daño lógico

El término "daño lógico" se refiere a situaciones en las que el error no es un problema en el hardware y el software de nivel requiere de soluciones.

Cuando el dispositivo es reconocido físicamente en el sistema mediante la conexión habitual, pero presenta errores que impiden al sistema operativo el acceso estándar a los datos contenidos, el problema se debe a que algo está mal en el software.

Estos Fallos pueden ocurrir por:

- Golpes o caídas del dispositivo: es posible que se alteren los controladores.
- Operaciones de escritura interrumpidas : pueden dañar la tabla de particiones, impidiendo el acceso al pendrive con normalidad para ver los datos almacenados previamente, al conectarlo muestra un aviso como, “Inserte un disco en Disco extraíble”, o ”Formatee el disco en la unidad para poder usarlo”
- Problema del firmware: causa que el dispositivo informe de capacidad cero, esto hace que el dispositivo resulte inaccesible para cualquier software.
- Errores en el sistema de archivos: El sistema de archivos del dispositivo se corrompe debido a factores como la intrusión de virus, el pendrive sufre ataques de malware esto provoca pérdida y hace que los archivos se oculten, eliminen o el dispositivo se vuelva inaccesible.

- Formateo con algún procedimiento poco estándar a la tabla de particiones: hace que el dispositivo deje de ser reconocido por el sistema operativo. (tabla de partición dañada).

Método para reparar los daños lógicos

Caso 1

Alteración de controladores por la misma causa anterior. Desde administrador de discos: Existen utilidades para la mayoría de componentes del sistema operativo. Uno de los tipos más comunes es la de actualizar controladores del dispositivo.

Pasos:

1. Inicio
2. Panel de control
3. Administrador de dispositivos
4. Controladores de bus serie universal
5. Dispositivos de almacenamiento USB
6. Click derecho
7. Propiedades
8. Controlador
9. Actualizar controlador
10. Busca automática software de controlador actualizado y lo aplica.

Caso 2

La tabla de partición está dañada o formateada con algún sistema de archivos poco estándar.

TestDisk es una herramienta que puede restaurar las tablas de partición dañadas o sobrescritas.

Pasos según Meis (2014)

Paso 1: Descargar testDisk

Paso 2: Ejecutado el programa como administrador se abre una ventana con las siguientes opciones: Create, Append, No Log

Paso 3: seleccione, con las flechas ↑ y ↓ del teclado la opción "Create" y de Enter. Aparecerá por unos segundos "Please wait" y cuando encuentre las unidades de almacenamiento conectadas (pendrive, discos duros externos) aparece una pantalla mostrando los dispositivos conectados identificados por el programa.

Paso 4: De nuevo, con las flechas ↑ y ↓ seleccione el dispositivo que corresponde y con las flechas ← y → la opción "Proceed".

Paso 5: Seleccione el tipo de tabla y de Enter (Elegir "[None] Non partitioned media", de las opciones presentadas)

Paso 6: Cuando de enter, aparecerá una pantalla con varias tareas que el programa puede en principio realizar sobre el dispositivo. Seleccione "Advanced" con las flechas ↑ y ↓ y de enter

Paso 7: A continuación especificará las características del dispositivo. Con las flechas ← y → seleccione la opción "Type" y enter

Paso 8: Con las flechas ↑ y ↓ seleccione "FAT16" y enter

Paso 9: volverá a la pantalla anterior, seleccione con las flechas ← y → la opción "Boot" y enter

Paso 10: seleccione con las flechas ← y → la opción "Rebuild BS" y enter

Paso 11: Comenzará a correr un porcentaje de progreso. Cuando termine, aparece lo que sigue: [Dump] [List] [Quit]

Paso 12: Seleccione “Quit” para cerrar el programa, extrae con seguridad el dispositivo del ordenador y pruebe.

Caso 3

El dispositivo informa de capacidad cero, esto hace que el dispositivo resulte inaccesible para cualquier software.

Pasos según (Soloelectronicos, 2013) Diskpart es un programa que se ejecuta desde CMD en Windows.

1. En el botón de "inicio" click derecho. Seleccionar "Símbolo del Sistema (Administrador)"
2. Una vez dentro de símbolo del sistema escriba el siguiente comando y luego pulse Enter para ejecutarlo: DiskPart
3. A continuación escriba list disk y Enter

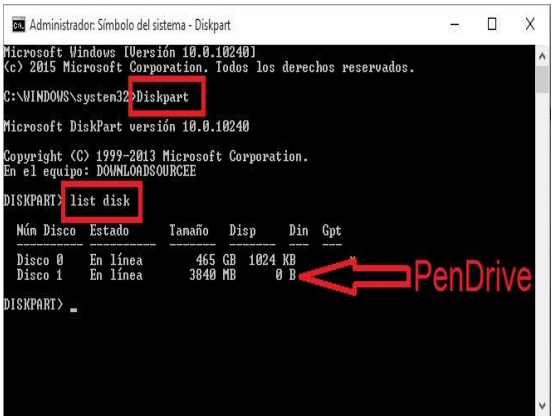


Imagen 34: Captura ejecución DiskPart tomado de (soloelectronicos, 2013)

Se muestra una lista con los discos actualmente conectados en el ordenador. Como es normal se mostrará el disco duro así como la memoria USB externa conectada.

4. El comando que sigue es select disk 1 una vez seleccionado pulsar la tecla Enter.
5. Escribir y ejecutar el comando: clean y Enter. El pendrive ha sido formateado por completo.
6. Crear una partición primaria en dicha memoria USB para lo cual debe introducir el comando: create partition primary y Enter
7. Activarla, para lo cual introducir el comando active
8. Una vez activado, se debe formatear la partición creada, para ello, introducir el comando: format fs=Fat32 o Format fs=NTFS esto dependerá del tipo de formato que quiera dar al pendrive.

Una vez que el proceso de formateado haya terminado, ya se puede utilizar el pendrive de nuevo, se puede utilizar un software de recuperación para intentar recuperar la posible información que aun pueda almacenar el dispositivo tras haber sido formateado.

Caso 4

El pendrive sufre ataques de malwares esto hace que los archivos se oculten, eliminen o el dispositivo se vuelva inaccesible.

- Matheus. (2012) propone el uso de la herramienta: R-Studio.

Los pasos realizados son:

1. Una vez descargado proceder a ejecutar el programa 
2. Seleccionar el dispositivo clic derecho y explorar

Imagen 35: Captura ejecución R-Stidio tomana de (Matheus., 2012)

3. De las siguientes opciones {Simple} {Exhautiva} {ninguna} Selecciona exhaustiva y a continuación la ubicación destino para la información recuperada.
4. Pulsar sobre el botón explorar

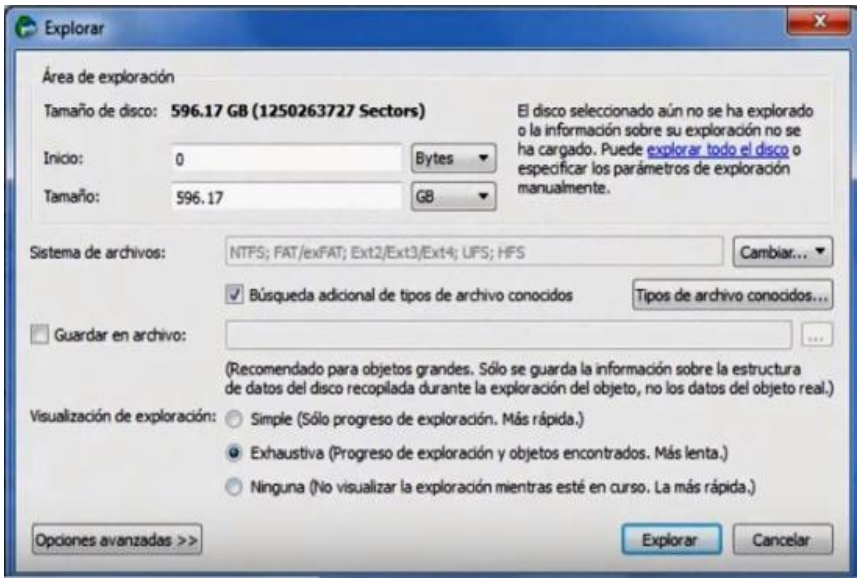


Imagen 36: iniciación de recuperación con R-Studio tomada de (Matheus., 2012)

Automáticamente empieza a buscar los datos a. Una vez encontrados los datos muestra tres tipos, diferenciándolos por un color. Los verdes se recuperarán en su totalidad, los naranja se recuperarán parcialmente y los rojos no se podrán

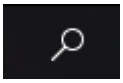
recuperar. Una vez visualizada la información, se seleccionan los archivos y se pulsa sobre recuperar seleccionados.

Se inicia automáticamente la recuperación de datos. Una vez recuperados podrán visualizarse los archivos.

- Bernabé (2011), propone el siguiente método para recuperar carpetas y archivos ocultos en un pendrive.

Nota: El pendrive debe haberse desinfectado de Malwares con anterioridad a este proceso para que surta el efecto esperado

Pasos:

1. Conecte el pendrive, consulte y tome nota de la letra que se le asigno.
2. Realice una la búsqueda en Windows 10.  Escribe cmd en la barra para abrir la consola.
3. con botón derecho del mouse/ejecutar como administrador. Para situarse dentro del dispositivo digite la letra asignada y enter.
4. Una vez dentro de la unidad se ejecuta el siguiente comando:
5. attrib –h –r –s *.* /s /d y Enter.
6. Esto permitirá recuperar las carpetas y archivos almacenados que por algún malware han sido ocultos.

Caso 5

Sistema de archivos dañado o formateado, ocasionó pérdida de información. La herramienta PhotoRec descrita en el apartado anterior es apropiada para resolver este caso. Esta viene incluida con testdisk, se ejecuta bajo línea de comandos.

Según sgSecurity (2016) los pasos a seguir son los siguientes:

1. descargar el programa
2. acceder a la aplicación y escribir la contraseña de administrador
3. seleccionar el dispositivo de la lista presentada y pulsar sobre [proced]
4. Selecciona [search], se presentan dos opciones: [ext2/ext3] ext2/ext3/ext4 filesystem para los sistemas de archivo de Linux y [Other] FAT/NTFS/HFS+/ReiserFS/ para los sistemas de archivos Windows y otros
5. Para este caso pulsar sobre [Other] se presentan 2 opciones: [Free] busca dentro del espacio libre algo específico o [whole] Busca dentro de toda la unidad de almacenamiento
6. para este caso se selecciona [Free] porque lo que se quiere recuperar es algo específico que se borró por error.
7. seleccionar la ubicación donde se guardaran los archivos recuperados, para este caso se seleccionó el escritorio.
8. una vez elegido el destino digite C para confirmar que es correcto

Automáticamente se empieza a gestionar la recuperación de los archivos, durante este proceso se va mostrando en una lista los tipos de archivos que se están recuperando, no conserva los nombres pero sabiendo el tipo de archivo se podrá identificar de forma fácil lo que se desea recuperar solo recupera archivos que no han sido fragmentados (solo los que están guardados completos).

4. METODOLOGÍA Y RESULTADOS

La tecnología actualmente está inmersa en los contextos de la vida humana: familiar, social, académica, laboral, empresarial entre otras, razón por la cual surge la necesidad de conocer los riesgos e impactos en el manejo de la información, más aún cuando se hace uso de dispositivos portátiles de almacenamiento como pendrive, para guardar, transportar y trasferir cantidad diversa de información.

Estos dispositivos están expuestos a daños accidentales y premeditados. Es importante conocer las diferentes formas por las cuales la seguridad física y lógica de un pendrive puede ser vulnerada, provocando la pérdida de información en los mismos. La mayoría de usuarios desconocen el funcionamiento óptimo de estos dispositivos, los riesgos que se generan entorno a la pérdida de información y los mecanismos para recuperarla en caso de incidente.

En este trabajo se explora la recuperación de la información contenida en pendrive, desde el punto de vista del análisis forense y se analizan las herramientas aplicables a dispositivos de almacenamiento. Se aplicó la siguiente metodología:

4.1 Etapa 1: Revisión bibliográfica

En esta etapa se aplican los pasos propuesto por el profesor Edgar Serna, para realizar la revisión a la literatura que consiste en: planificar, realizar y documentar en base a 6 procesos. (Serna, 2013). Descritos a continuación:

a) Definir el área temática

El análisis forense enfocado a la recuperación de información en pendrive

b) Definir las preguntas de investigación

En el análisis se encontró que las preguntas más relevantes para esta investigación son:

¿Qué se entiende por análisis forense para recuperar información?

¿Cuál es el impacto generado por la pérdida de información en personas y organizaciones?

¿Existen alternativas para prevenir el problema de la pérdida de información en dispositivos de almacenamiento?

¿Qué metodologías existen para la recuperación de la información?

¿Qué técnicas, métodos y herramientas son comúnmente aplicados en la recuperación de información en pendrive?

¿Existe alguna relación en la recuperación de información de otros dispositivos de almacenamiento con respecto al pendrive?

c) Definir el proceso de búsqueda

En el proceso de búsqueda se toman en cuenta dos criterios: los Términos o Palabras claves y Las Bases de Datos.

Palabras claves de búsqueda en los exploradores: análisis forense, forensic analysis, recuperación de información, Information recovery, dispositivos de almacenamiento, storage devices, herramientas forenses para recuperación en pendrive, forensic tools for recovery pendrive, metodologías, methodology, técnica, technique, método, method.

Bases de datos consultadas para la búsqueda: IEEE, Scopus, DOAJ, BDCOL, DIALNET, PDF SB, Scielo, Science, E-journal.

d) Definir los criterios de inclusión y exclusión

Para aceptar o excluir referencias bibliográficas se tendrán en cuenta los siguientes criterios:

Fuente de información de acuerdo con (origen, nivel informativo o contenido), fecha con rango entre (2008-2016), trayectoria del autor, metodología, aceptación.

e) Definir la valoración de la calidad

Para valorar si el material sirve y aporta a la revisión bibliográfica del tema los criterios valorados son: Fuente, resultados verificables, aceptación, trayectoria del autor, aplicación.

f) Definir la recopilación de datos

En los artículos que tengan relevancia para esta investigación, se toma en cuenta la referencia bibliográfica tipo APA y si están en internet se adiciona la URL.

4.2 Etapa 2: Análisis de la revisión bibliográfica

El análisis sobre la revisión bibliográfica se encuentra sintetizados en el capítulo 2 y el 3 de este trabajo, así:

En el capítulo Medios de Almacenamiento de Información se expone un estado del arte sobre el pendrive

En el capítulo Seguridad Informática, Análisis Forense y Pendrive se presenta un estado del arte sobre análisis forense enfocado a la recuperación de información pendrive. Dentro de este mismo capítulo se introducen las definiciones y características de algunas herramientas aplicables a la recuperación de información.

Como resultado del análisis de dichas herramientas se construye la siguiente tabla con sus datos más relevantes, a manera de síntesis y para una mejor relación comparativa

Tabla 8: Herramientas para Recuperar Información

HERRAMIENTA	TIPO DE LICENCIA	SISTEMA OPERATIVO COMPATIBLE	APLICACIÓN	DIRECCIÓN UBICACIÓN (URL)
WinHex Ver (pag.43)	Comercial	Windows	Analiza el espacio libre en disco, creando así una descripción detallada de las unidades, inspecciona archivos binarios, recupera datos borrados o perdidos en unidades dañadas. Es un editor hexadecimal capaz de mostrar completamente el contenido de cada tipo de archivo, incluso los códigos de control y el código ejecutable, usando un número de dos dígitos basado en el sistema de numeración hexadecimal	http://www.winhex.com/winhex/index-e.html
TestDisk Ver (pág.44)	software libre	Windows / Linux / Mac	Recupera archivos eliminados, tablas de particiones cuando están dañadas o han sido borradas por error, ayuda a reconstruir sectores de arranque. Usada especialmente para resolver problemas causados por software defectuoso, algunos tipos de virus o errores provocados	http://www.cgsecurity.org/wiki/testDisk_
PhotoRec Ver (pág. 44)	software libre	Windows / Linux / Mac	Recupera archivos perdidos y eliminados de todo tipo. Hace una búsqueda profunda de los datos, funciona incluso si el sistema de archivos está dañado o ha sido reformateado, usa un acceso de solo lectura puede recuperar los datos, aún si la tabla de partición no puede ser recuperada	http://www.cgsecurity.org/wiki/PhotoRec

HERRAMIENTA	TIPO DE LICENCIA	SISTEMA OPERATIVO COMPATIBLE	APLICACIÓN	DIRECCIÓN UBICACIÓN (URL)
R-Studio Ver (pág. 45)	Comercial	Linux, Windows	Recupera datos, que han sido eliminados por ataque de virus o corte de corriente eléctrica; después de haberse reformateado la partición con archivos o aun para distintos sistemas de archivos; cuando la estructura de particiones del dispositivo ha sido cambiada o dañada. Es especialmente útil cuando en el dispositivo aparecen constantemente sectores dañados.incluye, Editor de texto/hexadecimal y de copia y creación de imágenes de discos.	http://www.r-studio.com/
Scalpel Ver (pág. 45)	software libre	Windows	Utiliza la técnica de file carving y es capaz de leer los encabezados, pies de página y estructura interna de los archivos, siendo capaz de identificar y recuperar al instante todo tipo de archivos. Es útil para efectuar recuperaciones selectivas, ya que editando su configuración se puede seleccionar que tipo de extensiones de archivo, se quiere recuperar	http://www.programas.com/descargar_/scalpel-linux/linux
PCInspectorSmart Recovery Ver (pág. 45)	software libre	Windows	Recupera datos borrados por error, busca archivos borrados y muestra una vista de solo lectura, Cuando se seleccione el archivo a recuperar se tendrá que elegir un directorio en el para copiarlo	http://pc-inspector-smart-recovery.softonic.com/
EnCase Forensics Ver (pág. 46)	Comercial	Windows, Linux	Recolecta datos digitales, realiza análisis, produce una duplicación binaria exacta del dispositivo usando un estándar sin pérdida	http://softadvice.informer.com/Download_Encase_Forensic_Software.html

HERRAMIENTA	TIPO DE LICENCIA	SISTEMA OPERATIVO COMPATIBLE	APLICACIÓN	DIRECCIÓN UBICACIÓN (URL)
Digital Forensics Framework Ver (pág. 46)	software libre	Mac, Windows y Linux	Permite recoger, preservar y revelar la evidencia digital, accediendo a los dispositivos locales y remotos, analizando los datos del registro, buzón y del sistema de archivos para recuperar archivos ocultos y eliminados	http://es.softoware.net/apps/download/download-digital-forensics-framework-for-linux.html
PC Inspector file recovery Ver (pág. 46)	software libre	Windows, Linux	Recupera archivos y rescata datos eliminados, perdidos e incluso unidades perdidas. Posee además la función especial de recuperación, que salva los archivos que no tienen ninguna indicación de directorio. En su listado de formatos. También ofrece una guía de ayuda.	http://pc-inspector-file-recovery.softonic.com/
Foremost Ver (pág. 46)	Comercial	Windows	Recupera archivos borrados y datos en general aplicando la técnica del file carving escaneando la totalidad del dispositivo, intenta identificar si el contenido escaneado contiene las estructuras hexadecimales típicas de inicio y fin de un determinado tipo de archivo. Cuando encuentre una de estas estructuras (inicio-fin), extraerá la información contenida entre el inicio y el fin recuperando así un archivo que previamente se había borrado	http://foremost.soft112.com/
Disk Recovery Ver (pág. 47)	software libre	Windows	Recupera la información perdida, reconstruye sistemas de archivos dañados o formateados. Escanea todos los sectores.	http://o-o-diskrecovery.softonic.com/descargar

HERRAMIENTA	TIPO DE LICENCIA	SISTEMA OPERATIVO COMPATIBLE	APLICACIÓN	DIRECCIÓN UBICACIÓN (URL)
GetDataBack Ver (pág. 47)	Comercial	Windows	Recupera todo tipo de datos aunque no sea reconocido el dispositivo o se haya perdido toda la información de estructura de directorios. Aun si se ha realizado un borrado tiempo atrás, no sin antes saber qué sistema de archivos es NTFS o FAT	https://www.runtime.org/data-recovery-software.htm
Recuva Ver (pág. 47)	software libre	Windows	Recupera datos borrados, archivos que han sido suprimidos por errores, accidentes y virus. Indicando la ubicación y el tipo de archivo que se quiere reponer	http://recuva-portable.softonic.com/
Wise Data Recovery Ver (pág. 48)	Comercial	Windows	Recupera archivos eliminados accidentalmente, Recupera los documentos como Word, Excel, TXT, también foto / imagen, como Jpg, Png, Gif, Recupera archivos de correo electrónico, recupera audio, video, y muestra el estado explícito de los datos que deben recuperarse.	http://www.wiseclean er.com/wise-data-recovery.html
HDDScan Ver (pág. 48)	software libre	Windows	Permite realizar un chequeo integral del dispositivo en busca de fallas, busca en el sistema los dispositivos de almacenamiento que estén instalados, Una vez encontrados, se puede ver la información relativa a cada uno de los dispositivos, su principal ventaja de es que trabaja a bajo nivel, que es donde mayor interacción es posible de lograr entre el software y el hardware.	http://www.bestdescargas.com/2010/07/pack-de-aplicaciones-para-reparar.html
USB Show Ver (pág. 48)	software libre	Windows	Permite ver archivos, que por algún virus o persona fueron escondidos, recupera todos los archivos ocultos,	http://www.bestdescargas.com/2010/07/pack-de-aplicaciones-para-reparar.html

HERRAMIENTA	TIPO DE LICENCIA	SISTEMA OPERATIVO COMPATIBLE	APLICACIÓN	DIRECCIÓN UBICACIÓN (URL)
Micron USB Drive Data Recovery Ver (pág. 49)	Comercial	Windows	Rrecupera cualquier archivo que se haya perdido por cualquier motivo, ya sea por daño externo o interno. Tiene la opción de hacer una búsqueda avanzada o estándar.	http://micron-usb-drive-data-recovery.uptodown.com/
Pen Drive Data Doctor Recovery Ver (pág. 49)	software libre	Windows	Recupera todo tipo de ficheros datos perdidos, funciona aun en los peores casos de corrupción y daño. Cualquiera que sea la razón, de pérdida Pen Drive Data Doctor Recovery puede ayudar a recuperar los datos y archivos. El no acceso a los datos del pen drive, por pérdida de partición. También puede ser manejado por Pen Drive Data Doctor Recovery.	http://pen-drive-data-doctor-recovery.archivospc.com/
Remo Recuperar Ver (pág. 49)	Comercial	Windows, Mac, Android	Rescata información, recupera archivos perdidos debido a errores en el sistema de archivos. Tiene una función integrada “encontrar”, lo que ayuda a encontrar y localizar cualquier archivo en particular sobre la base de diferentes atributos de archivo.	http://www.remorecover.com/es/windows/recupere-archivos.html
Partition Wizard Ver (pág. 50)	software libre	Windows	Recupera particiones perdidas solo si el dispositivo es reconocido. Cuenta con dos métodos de escaneo de disco: rápido y profundo, el segundo se usa solo si el primero no da resultado positivo. Si la tabla de particiones está dañada."	http://minitool-partition-wizard.softonic.com
Wondershare Data Recovery Ver (pág. 51)	Comercial	Windows, Mac	Recupera archivos perdidos en más de 550 formatos de forma rápida, segura y completa: vídeos, fotos, emails, música, etc.	http://www.wondershare.es/disk-utility/usb-flash-drive-recovery.html

HERRAMIENTA	TIPO DE LICENCIA	SISTEMA OPERATIVO COMPATIBLE	APLICACIÓN	DIRECCIÓN UBICACIÓN (URL)
Micron USB Drive Data Recovery Ver (pág. 51)	Comercial	Windows	Rrecupera cualquier archivo que se haya perdido por cualquier motivo, ya sea por daño externo o interno. Tiene la opción de hacer una búsqueda avanzada o estándar.	http://micron-usb-drive-data-recovery.uptodown.com/
Pen Drive Data Doctor Recovery Ver (pág. 52)	software libre	Windows	Recupera todo tipo de ficheros datos perdidos, funciona aun en los peores casos de corrupción y daño. Cualquiera que sea la razón, de pérdida Pen Drive Data Doctor Recovery puede ayudar a recuperar los datos y archivos. El no acceso a los datos del pen drive, por pérdida de partición. También puede ser manejado por Pen Drive Data Doctor Recovery.	http://pen-drive-data-doctor-recovery.archivospc.com/
Partition Wizard Ver (pág. 52)	software libre	Windows	Recupera particiones perdidas solo si el dispositivo es reconocido. Cuenta con dos métodos de escaneo de disco: rápido y profundo, el segundo se usa solo si el primero no da resultado positivo. Si la tabla de particiones está dañada."	http://minitool-partition-wizard.softonic.com
Wondershare Data Recovery Ver (pág. 53)	Comercial	Windows, Mac	Recupera archivos perdidos en más de 550 formatos de forma rápida, segura y completa: vídeos, fotos, emails, música, etc.	http://www.wondershare.es/disk-utility/usb-flash-drive-recovery.html

En el capítulo 3 también se exponen algunos métodos de recuperación de información aplicables a pendrive, tanto para daños físicos como lógicos, a continuación, en la tabla 9 se presenta un resumen de los mismos:

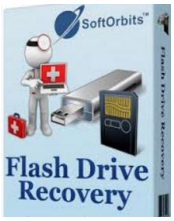
Tabla 9: Métodos para recuperar información en pendrive

AUTOR	DESCRIPCIÓN DEL MÉTODO	TIPO DE DAÑO	QUÉ PROBLEMA RESUELVE	SOLUCIÓN
Solo electrónicos Ver (pág. 68)	Rearmar el dispositivo de forma temporal	Físico	Falla en el conector, mal contacto a la placa	Tratamiento electrónico.
Solo electrónicos Ver (pág. 69)	Reemplazar pieza	Físico	Resistencia de protección quemada	Tratamiento electrónico.
Solo electrónicos Ver (pág. 70)	Reemplazar pieza	Físico	Cristal de cuarzo quebrado	Tratamiento electrónico.
Solo electrónicos Ver (pág. 71)	Actualizar controladores del dispositivo	Lógico	Alteración de controladores	Utilidades propias del sistema operativo. Ej: diskmanager
Meis Ver (pág. 72)	Restaurar tabla de partición	Lógico	Tabla de partición dañada	Herramienta TestDisk
Solo electrónicos Ver (pág. 72)	Particionar dispositivo	Lógico	Capacidad cero informada	Herramienta Diskpart
Matheus Ver (pág. 75)	Desinfectar dispositivo	Lógico	Ataques de malware	Herramienta R-Studio
sgSecurity Ver (pág. 77)	Recuperar algo especifico	Lógico	Sistema de archivos dañado y formateado	Herramienta PhotoRec

4.3 Etapa 3: Evaluación de herramientas

Para clasificar las herramientas más relevantes para la recuperación de la información se tuvieron en cuenta opiniones expresadas en las fuentes encontradas en la revisión bibliográfica y en los top ten que aparecen en Internet. Las fuentes de internet consultadas que sirvieron de base para obtener el siguiente top ten (ver tabla 10) son: Moreno j. (2014), Topdatarecoverysoftware. (s.f), Martínez, R. (2012), ABCarticulos. (2016), Conexión inversa. (2013), Oroxom E. (2015), Cruz N. (2015) Pour, A. (2015), Adriano, J. (2015), fundacionctic. (2012), Cervera. (2015), Noziglia, F. (2011), Cervera. (2015). Para cada herramienta se incluye el enlace oficial desde donde se puede descargar.

Tabla 10: Top ten representativo de herramientas

1. Recuva	2. Pandora Recovery	3. Undelete Plus	4. Disk Drill	5. R-Studio
				
https://www.piriform.com/recuva/download	http://www.portalprogramas.com/pandora-recovery/descargar	http://www.portalprogramas.com/undelete-plus/descargar	http://www.cleverfiles.com/es/	https://www.rstudio.com/products/rstudio/download/
6. PhotoRec	**7.DiskDigger**	**8.TestDisk**	**9.Ease US Data Recovery Wizard**	**10. SoftOrbits Flash Recovery**
				
www.downloadsource.es	http://www.portalprogramas.com/diskdigger/descargar	www.portalprogramas.com	www.easeus.com/partition-manager/epm-free.html	http://softorbits-flash-drive-recovery.softonic.com/

Hay empresas como Masterrecoverylab, Solutekcolombia, It & Data Services S.A, Recovery Labs, Savedata, Cbl Tech, Pca Lab, por mencionar algunas, que se dedican a la recuperación de información y brindan sus servicios tanto a empresas como a personas.

Según Redusers, (2016). El proceso que realizan las empresas es. "Primero se atiende al cliente y se ingresa el equipo para su diagnóstico, El dispositivo pasa a los técnicos, quienes realizan diversos tests para conocer el origen de la falla. Para ello cuentan con software propios para analizar el dispositivo. En caso de que la falla sea física, cuentan con un "área limpia" de partículas, para desarmar los equipos y realizar reparaciones sin que ingrese polvo, las compañías más avanzadas tienen las herramientas para retirar el chip de memoria flash de la tarjeta de circuito con el fin de extraer y descifrar los datos sin procesar almacenados allí. Entre las fallas más comunes se encuentran "la mala manipulación del dispositivo, un factor eléctrico, un problema propio del disco que suma sectores dañados y fallas electrónicas", según Baglivo". Los virus no son los únicos que pueden dañar la información, también hay incidentes "especiales". "casos de sabotaje, de un empleado que se llevó información de la empresa". "una cliente que se estaba separando y quería recuperar los mensajes del celular de su marido para usar como prueba". En este sentido, hay que mencionar que hay empresas que son convocadas para que actúen como peritos en algunos casos judiciales. Con respecto a la privacidad, las empresas firman un pacto de confidencialidad de los datos. La información recuperada se devuelve al usuario de la manera que desee: otro disco duro, pendrives, notebooks o DVD.

PCA Lab realizó una prueba con 8 programas de recuperación. Para las pruebas, creó un set de ficheros con el que trabajar. Este englobaba los archivos tipo más comunes, como imágenes, documentos Word, PDF, TXT, ZIP, entre otros, no se han incluido los ejecutables, ya que estos pueden ser obtenidos nuevamente.

A continuación se presenta la prueba realizada por la empresa PcaLab la cual consiste consiste en tres test:

1. Recuperación de ficheros borrados accidentalmente
2. Recuperación tras formato de disco
3. Recuperación tras escritura.

Estas pruebas se han realizado sobre una partición de dos «gigas», que contenía alrededor de 700 Mbytes de información eliminada. Tener en cuenta que los tiempos aumentarán de forma proporcional a la capacidad del disco, por lo que pueden llegar a ser muy elevados. Otros factores analizados además del porcentaje de éxito en la recuperación de los ficheros, son el tiempo de análisis, la facilidad de uso del programa, la interfaz de usuario o el número de opciones de búsqueda. Aunque se han incluido tanto programas gratuitos como comerciales, se han tratado a ambas bajo los mismos parámetros, ya que las herramientas libres de coste han demostrado estar a la altura de tan delicada empresa.

Resultado de las pruebas efectuadas por PcaLab

	EaseUs Data Recov.	GetData Back	Ontrack EasyRec.	PC Tools File Rec.	DiskDigger	Pandora	PC Inspector	Recuva
Test de borrado accidental								
• Tiempo de análisis (s)	2	1	17,5	4	7	5	39,5	4
• Tiempo de recuperación (s)	7	16	8,6	10,2	24	18,5	11	14,62
• Archivos recuperados (%)	98,7	98,7	100	99,9	99,4	100	98,7	99,5
Test de recuperación tras formato								
• Tiempo de recuperación (s)	63	n.a	1	35	40	11	340	9
• Archivos recuperados (%)	32	n.a.	31,7	30,3	31,2	20,7	8,2	20,8
• Archivos recuperados (nº)	676	n.a.	670	640	659	438	173	440
Test disco sobrescrito								
• Tiempo de análisis (s)	37	1	17,6	13	40	7	7	36
• Tiempo de recuperación (s)	125	108	7	30	130	2	23	11
• Archivos recuperados (%)	3,2	1,6	3,1	2,8	3,2	2,7	2,1	2,8

Imagen 37: Resultados de la prueba de Pca Lab tomado de (Taringa, 2013)

EaseUsDataRecovery: En la recuperación tras un borrado accidental, la cifra se encuentra en la media. Sin embargo, en la recuperación tras darle un formato, nos encontramos ante el líder con un porcentaje de recuperación del 32%, al igual que en la restauración en circunstancias extremas, que, con un 3,2%, empata en el primer puesto con DiskDigger.

El único inconveniente se lo podemos poner en los tiempos de proceso, que se encuentran entre los más altos de la tabla, pero en ningún caso llegando a ser alarmantes. De la interfaz, no hay mucho que decir; si bien nos ofrece ciertas opciones de filtrado para optimizar nuestra búsqueda, su concepción no da lugar a grandes alardes estéticos, ni tampoco lo pretende.

En definitiva, puede definirse como un programa práctico, eficiente y sencillo de usar, para que cualquiera pueda introducirse en el mundo de la recuperación de datos con todas las garantías.

GetDataBack: muestra recobrado un 98,7% de los archivos dañados (cifra dentro de la media). A partir de aquí, las cosas se tuercen. En la prueba realizada con un disco en el que hemos sobrescrito gran parte de los clusteres, solo es capaz de recuperar un 1,6% de los datos perdidos. La cifra más baja de toda la comparativa.

Sin embargo, la sorpresa mayúscula viene en la recuperación tras un formato. Confiados, utilizamos la opción específica disponible para este tipo de desastres. Tras el análisis, nos encontramos con que GetDataBack no ha recuperado ningún archivo, situación que no se ha producido con ningún otro software. Hemos repetido este test con distintas configuraciones y, tras diferentes formatos del disco, desgraciadamente en ningún caso hemos sido capaces de recuperar dato alguno del disco afectado.

Si bien la interfaz resulta correcta, las limitaciones de este programa, tanto en formatos, como en capacidad de reparación, lo convierten en el rival más débil, siendo superado ampliamente por las herramientas gratuitas analizadas en esta comparativa.

Ontrack EasyRecovery D: la interfaz, aun siendo un elemento secundario en esta rama de software, se nos antoja algo desfasada y quizá debería modernizarse para quedar a la altura de la de algunos de sus competidores. Las funciones extra de reparación de archivos resultan muy convenientes, así como el completo informe que nos ofrece al finalizar la recuperación. Algo de lo que deberían aprender el resto de herramientas de la comparativa.

Si bien nos encontramos ante un software de una calidad indudable, que hace muy bien su trabajo, en el 99% de las ocasiones, no necesitaremos realizar un desembolso tan importante que justifique la compra de este programa. Además, si se trata de un caso de máxima necesidad, mejor acudir a un servicio de recuperación especializado, como el de la propia Kroll Ontrack, que ofrece las mejores garantías.

Pandora Recovery 2.1.1: tras dedicar unos minutos a aprender su manejo, descubrimos un 100% de efectividad en ficheros recién eliminados. El resto de pruebas arrojan un 20,7% de acierto en la recuperación tras el formato y un mejorable 2,7% en circunstancias extremas.

La opción de escaneo de superficie resulta especialmente lenta, sin embargo es el camino que tomar cuando la integridad de los datos se encuentre deteriorada o si queremos sacar a relucir un botín que la aplicación no ha sido capaz de divisar tras un análisis rápido.

La opción de instalar la aplicación en una memoria extraíble solo se encuentra disponible adquiriendo el llamado Pandora Power Pack, el cual proporciona la memoria con el

programa ya preinstalado. Además, por el momento, tampoco se comercializa en España, ya que no realizan envíos a Europa. Una lástima que no dispongan de una alternativa descargable que pudiera facilitar su distribución aquí.

PC Tools File Recover 8: muestra buen acabado y notables funciones, permite recuperar documentos de importancia crítica u otros ficheros que se han perdido debido a una eliminación por accidente. Compatible con sistemas de archivos FAT y NTFS

DiskDigger, eficiencia ante situaciones difíciles, este programa no destaca por su velocidad, pero sí por su eficacia en delicadas situaciones. Así se presenta DiskDigger, una herramienta que en su versión más básica se ofrece de forma gratuita

PC Inspector File Recovery 4.0 tiene una baja efectividad, esta aplicación, de fabricación alemana, nos ha resultado complicada de utilizar desde el primer momento. Problemas para reconocer ciertas particiones, menús fragmentados y desestructurados

Recuva 1.30.435 aplicación agradable, la atractiva interfaz, lo sencillo de la navegación por sus menús y la inmediatez de sus resultados, la convierten en un verdadero placer.

Así también "*Diversas comunidades profesionales en el testeo de aplicaciones han probado cinco soluciones gratuitas para Windows con el objetivo de probar dónde llegan este tipo de herramientas en la recuperación de datos, su rapidez y eficacia. La prueba real se realizó sobre un pendrive formateado en el que copiaron 67 archivos en total de todo tipo de formatos (pdf, doc, docx, rtf, epub, azw3 (Kindle eBooks), iso, mp3, jpg, nef, pptx, exe, avi, mp4 , 7z, tar y zip). Los archivos fueron borrados, copiando a continuación 10 nuevos archivos que ocuparan parte del espacio del disco ya que la sobreescritura es un factor que disminuye*

la probabilidad de recuperación de datos. Las soluciones gratuitas utilizadas fueron: Recuva, Disk Drill, PC Inspector File Recovery, Puran File Recovery, Wise Data Recovery. Ninguna fue capaz de recuperar todos los archivos borrados y algunos de los recuperados estaban dañados. También son destacables las diferencias en el tiempo de recuperación". (Gitsinformatica, S.f).

Tabla 11: Resultado de la prueba efectuada por comunidades profesionales

Aplicación	Tiempo de escaneado de archivos borrados	Tiempo de recuperación de archivos	número de archivos recuperados en comparación con los archivos borrados	Archivos recuperados pero corruptos
Piriform Recuva	1 segundo	3 minutos	57/67	10
Puran File Recovery	1 segundo	3 minutos	57/67	10
Wise Data Recovery	1 segundo	6 minutos	57/67	10
Disk Drill	1 segundo	2 minutos	43/67	0
Pc Inspector File Recovery	1 segundo	1 minutos	23/67	2

Resultado de la prueba tabla tomada y modificada de (Gitsinformatica, S.f)

Resultados aceptables en eficacia y en tiempo de recuperación de Recuva y Puran, los dos recomendados.

4.4 Etapa 4: Elección de 2 herramientas para pruebas de recuperación de información

Del top ten de herramientas para recuperación de información construido en esta investigación se eligieron a Recuva **y** Disk Drill para realizar las pruebas piloto. Los criterios que se tomaron en cuenta para la selección son: que en la referencia bibliográfica se recomiendan dada la aplicabilidad y la funcionalidad en diferentes casos de pérdida de información y que son de software libre (ya que este proyecto no cuenta con recursos económicos para adquirir licencias).

Tabla 12: Sinopsis de las herramientas elegidas para pruebas

HERRAMIENTA	DEFINICIÓN	OBJETIVO	MODO DE USO
	Software gratis desarrollado por Piriform, para Microsoft recuperador de información Compatible con las distintas versiones Windows (2000, XP, Vista, 7, 8, 8.1 y 10) adicionalmente al archivo recuperado proporciona el nombre del mismo, la ubicación donde se encontraba y el tamaño. Soporta los formatos FAT, exFAT y NTFS. (Gonzales J., 2015)	Restauración de archivos borrados en forma permanente y que han sido marcados por el sistema operativo como espacio libre. Recuperación de datos eliminados por error Inclusive perdidos como consecuencia de la acción de virus o interrupciones intempestivas.	Fácil de usar y descargar, cuenta con un asistente que facilita el proceso de recuperación. Se deben responder algunas preguntas sobre el tipo de archivos y ubicación de los mismos. El software arrojará los resultados obtenidos y su posibilidad de recuperación, solo se tendrá que seleccionar el documento a salvar, la unidad donde se encontraba, elegir la carpeta donde se guardarán los recuperados y dar clic en la opción 'Recuperar'.
HERRAMIENTA	**DEFINICIÓN**	**OBJETIVO**	**MODO DE USO**
	Software gratis limpio de virus para recuperar datos de pendrive y otros. Compatible con las distintas versiones Windows (Xp, Vista, 7, 8, 8.1 y 10) y con múltiples sistemas de archivos: FAT, exFAT, NTFS y más.	Recuperación de documentos y archivos perdidos tras formateos no deseados, daños de particiones, borrados accidentales, entre otros.	Uso sencillo y fácil descarga sin grandes configuraciones, con solo un clic puede cumplir su objetivo. Bermúdez J. L.,(2016)

Prueba piloto 1

Aplicación de las herramientas Recuva y DiskDrill sobre un pendrive SanDisk cruzer de 2 GB con daño desconocido que fue donado para este proyecto

Imagen 38. Pendrive utilizado en la prueba piloto 1

Pasos para la prueba con recuva:

- Para descargar la herramienta se debe ir al enlace **http://www.piriform.com/recuva**
- Dar click en el botón **Free Download**

Imagen 39 Captura de descarga Recuva

- Se debe ratificar la versión que se va a descargar "Free", pues dicha herramienta también cuenta con una versión profesional con costo.

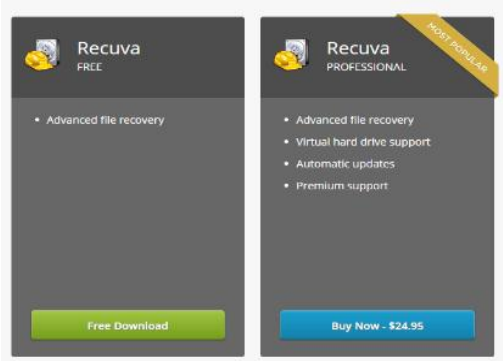


Imagen 40 Captura de versión Recuva

- Dar click en **Piriform.com**

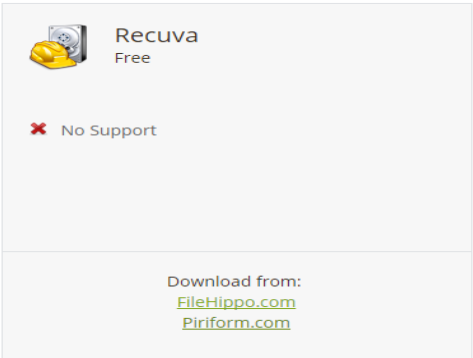


Imagen 41. Captura de pantalla de inicio de descarga Recuva

- Dar click en el botón **Srarted Download,** La descarga es automática.

- Luego se debe ejecutar para instalarlo.

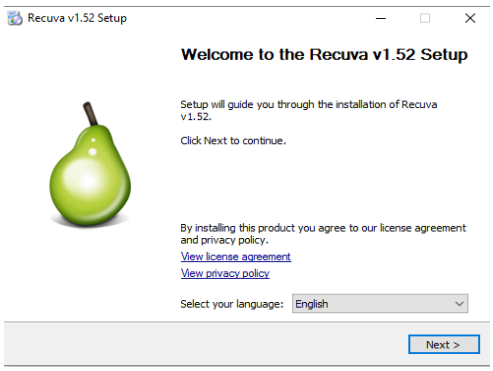


Imagen 42 Captura de instalación de Recuva

- Elegir el idioma y dar click en el botón **Next** para iniciar el asistente de instalación

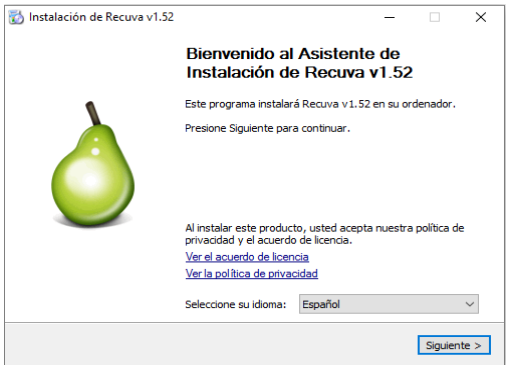


Imagen 43 Captura asistente de instalación Recuva

- Dar click en el botón **Siguiente**
- Se presentan las siguientes opciones de instalación

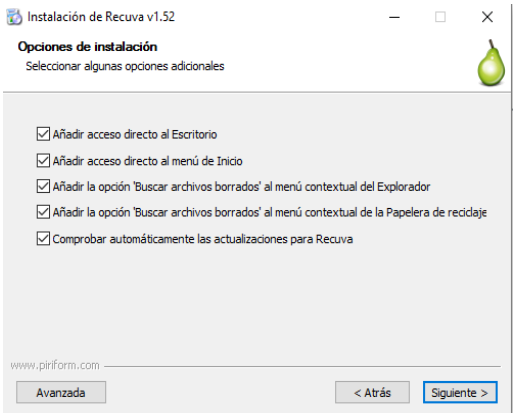


Imagen 44 captura de opciones de instalación Recuva

- Dar click en el botón **Siguiente**
- Muestra el progreso de la instalación

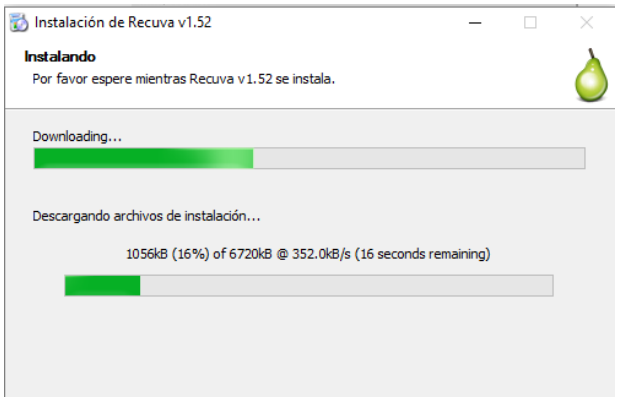


Imagen 45 captura de progreso de instalación de Recuva

- Una vez instalado, dar click en terminar para cerrar el asistente.
  A continuación siguen los pasos para el proceso de recuperación:
- Una vez que se abra el asistente, dar click en el botón Siguiente

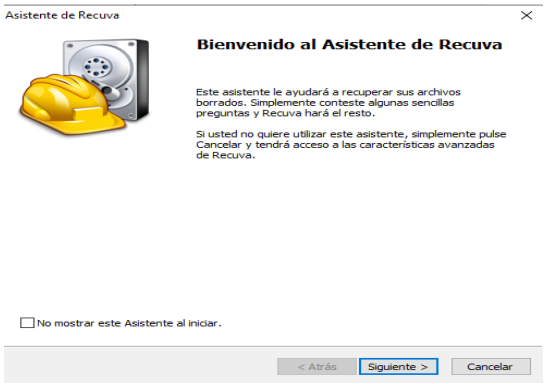


Imagen 46 captura de inicialización del asistente de recuperación de archivos

- En la ventana siguientes se marca **Todos los archivos** como tipo de archivos a recuperar y se da click en **Siguiente**

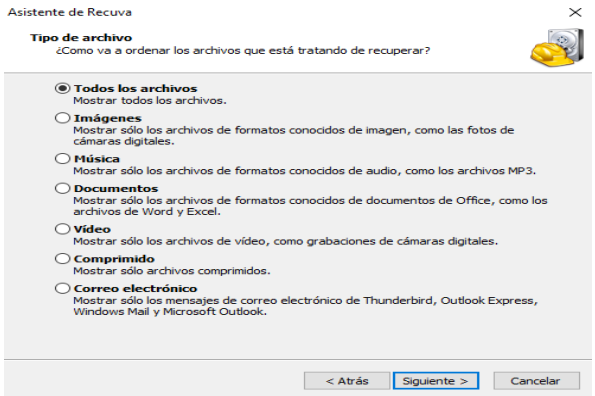


Imagen 47 captura de tipos de archivos a recuperar

- De las siguientes opciones marcar **En una posición específica** para buscar en la ruta del computador el dispositivo donde están los archivos a recuperar, seleccionarlo y presionar el botón **Aceptar**

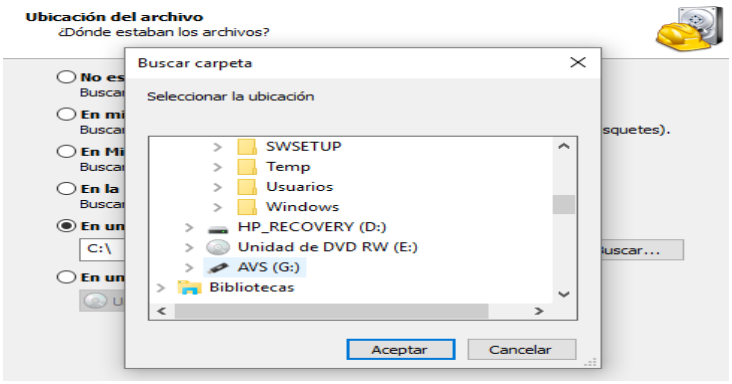


Imagen 48 captura de destino de los archivos recuperados

- Dar click en el botón Siguiente

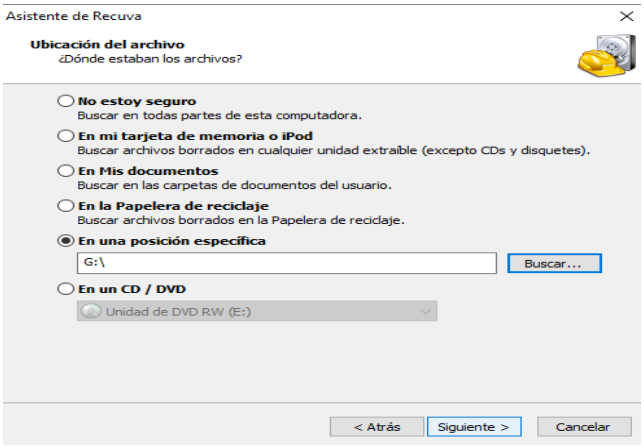


Imagen 49 captura de iniciación de busqueda de información

- Dar click en iniciar para empezar la búsqueda de la información

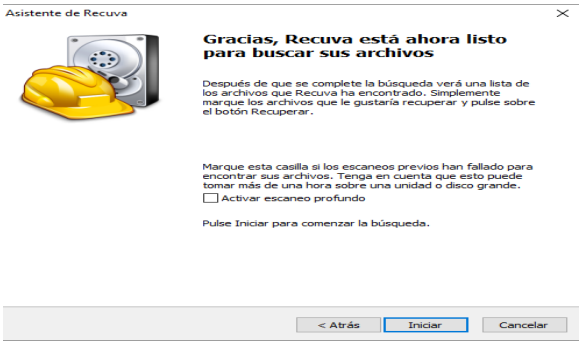


Imagen 50 captura de búsqueda de archivos

- Los archivos marcados con verde son 6 y son los que recuperara totalmente, los marcados con naranja serán parcialmente recuperados y los rojos no se podrán recuperar

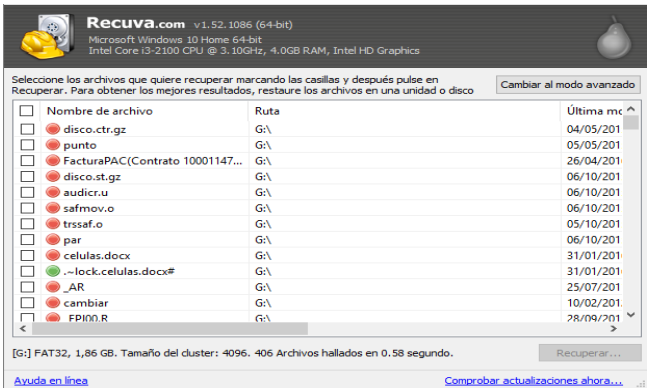


Imagen 51 captura de pantalla de archivos a recuperar

Aclaración

La recuperación de archivos es parcial o total dependiendo de:

- **El tipo de herramienta**: las herramientas son selectivas hay unas, que recuperan archivos completos e integrales y otras que recuperan parte de ellos, estas últimas aplican cuando la recuperación se hace en función de análisis forense judicial porque en una parte de un archivo se puede encontrar una evidencia.
- **El tipo de daño del dispositivo**: si un sector esta físicamente dañado no se podrá recuperar.

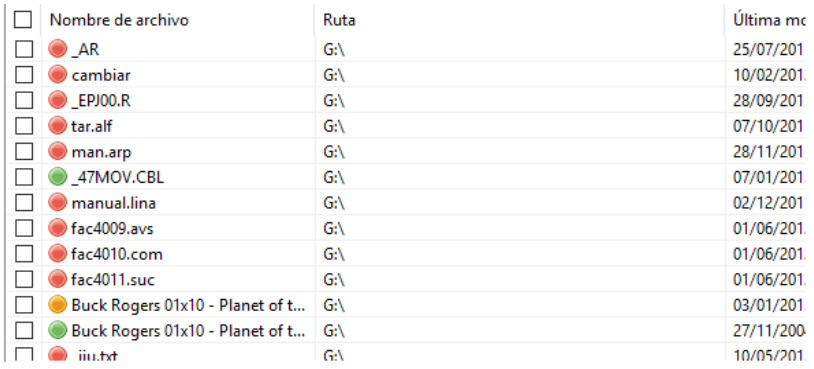


Imagen 52 captura de archivos diferenciados por color que identifica posibilidad de recuperacion

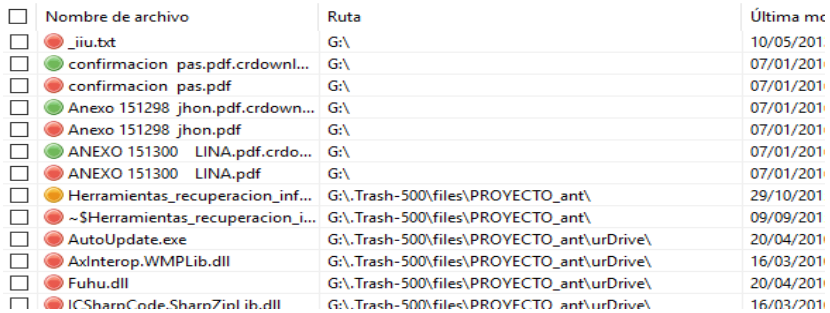


Imagen 53 captura de pantalla de marcación de archivos

- Se deben seleccionar los archivos marcando la casilla respectiva y a continuación dar click en **Recuperar**
- Seleccionar el destino donde se desean ubicar los archivos recuperados y dar click en **aceptar**

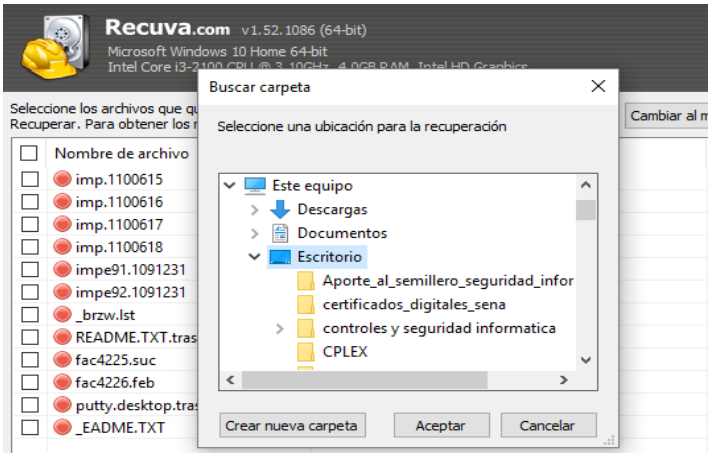


Imagen 54 captura de pantalla de selección de destino para los archivos recuperados

- El resultado es el siguiente

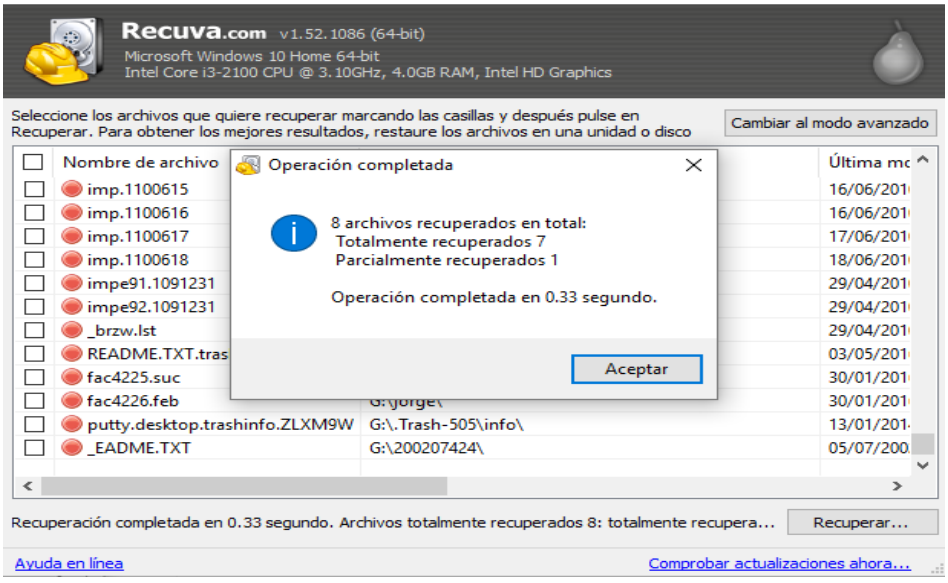


Imagen 55 captura de pantalla de resultados de la prueba con Recuva

- Los archivos recuperados se visualizan en el destino seleccionado anteriormente así:

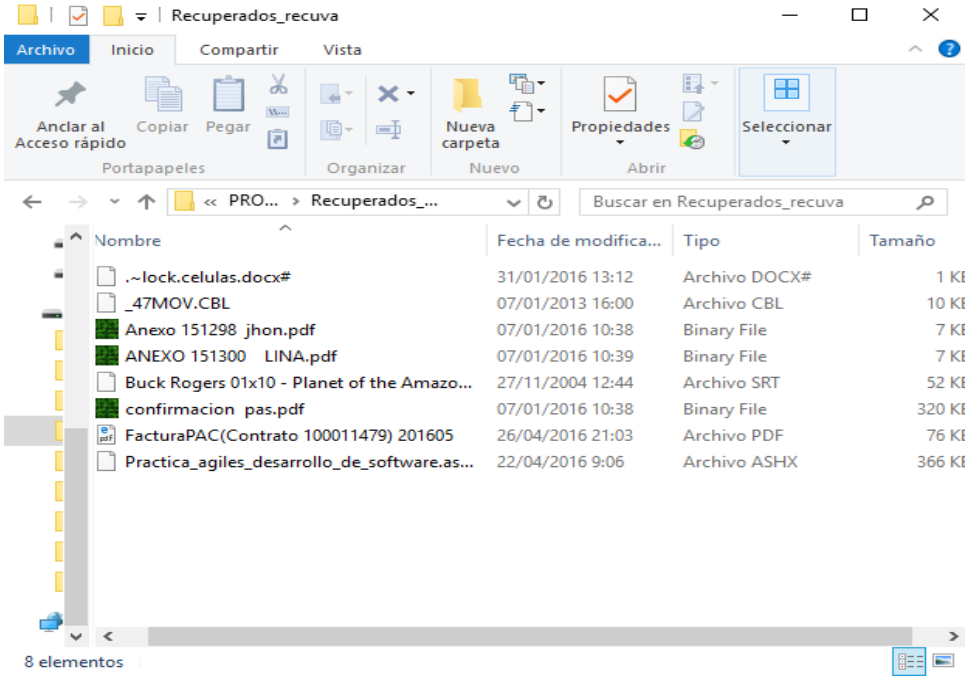


Imagen 56 captura de pantalla de visualización de archivos recuperados con Recuva

Conclusión del resultado de la prueba con Recuva

De los ocho archivos rescatados; seis fueron recuperados correctamente, uno con error (de extensión desconocida) y otro que se considera dañado porque se intentó abrir con varias aplicaciones y no funcionó.

Pasos para la prueba con DiskDrill:

- Para descargar la herramienta se debe ir al enlace **http://www.cleverfiles.com/disk-drill-windows.html**
- Dar click en el siguiente botón 
- Luego se debe ejecutar para instalarlo.

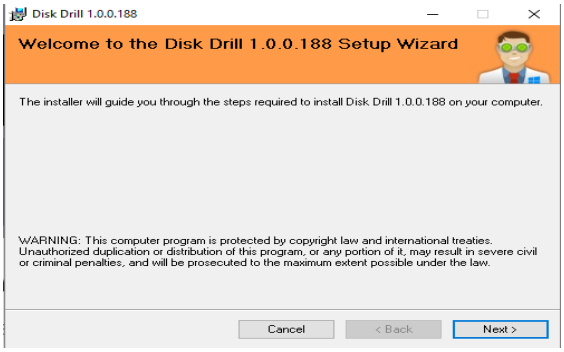


Imagen 57 captura de visualización de descarga de diskdrill

- Dar click en el botón **Next** para iniciar el asistente de instalación

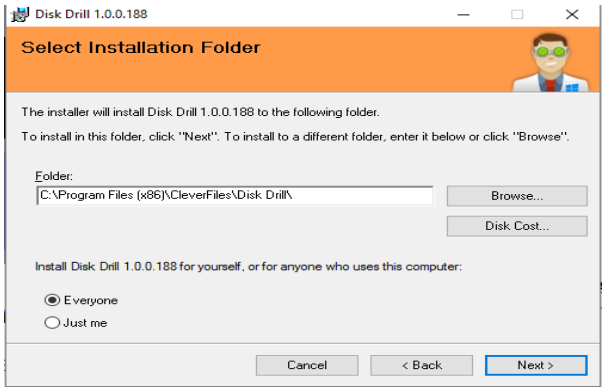


Imagen 58 captura de inicialización de instalación de disk drill

- Elegir la ubicación destino para guardar la instalación
- Se presentan las siguientes opciones de instalación: [Everyone] o [Just me]
- Elegir la opción deseada

- Dar click en el botón **Next** para confirmar e iniciar la instalación

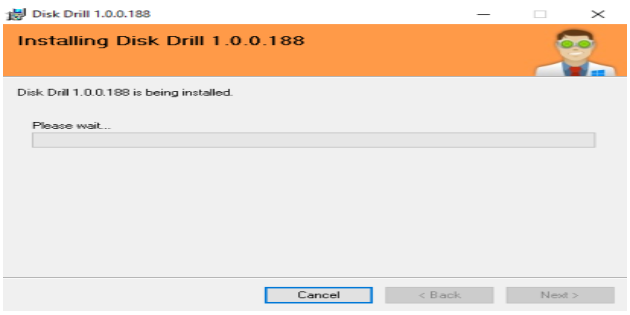


Imagen 59 captura de progreso de instalación disk drill

- Muestra el progreso de la instalación
- Una vez instalado, dar click en Close para cerrar el asistente.

A continuación siguen los pasos para el proceso de recuperación:

- Una vez que se ejecuta el programa, se abre el asistente.
- elegir la unidad o partición a analizar y presionar el botón **Recover**

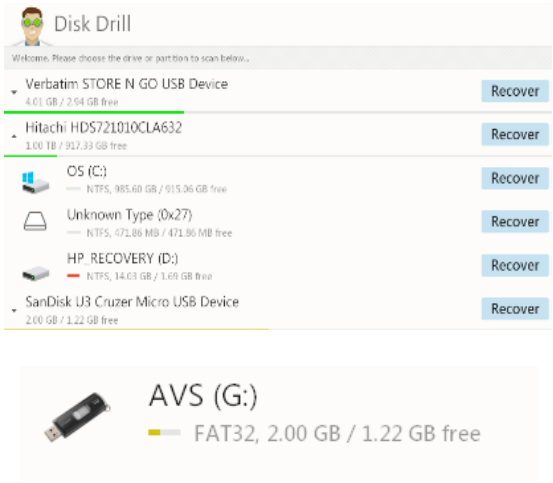


Imagen 60 captura elección de unidad a analizar

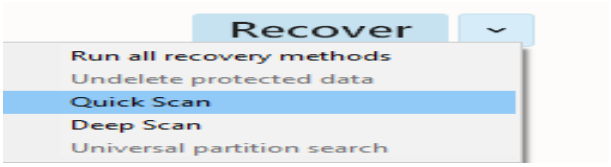


Imagen 61 captura tipo de escaneo

- De las opciones siguientes aparece marcada **Todos los archivos "All files"** como tipo de archivos a recuperar.

- buscar en la ruta del computador, la ubicación destino para los datos a recuperar.

- Dar click en el botón **Aceptar**

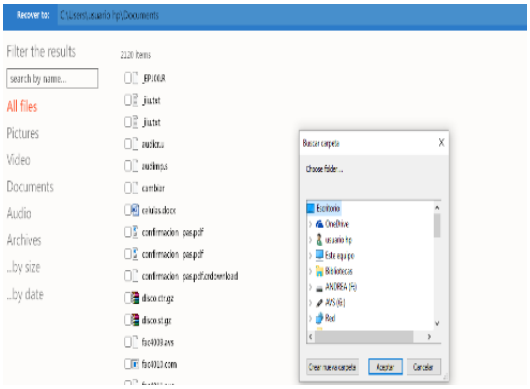


Imagen 62 captura ubicación destino de los archivos a recuperar

- Se deben seleccionar los archivos marcando la casilla respectiva y a continuación dar click en **Recuperar**

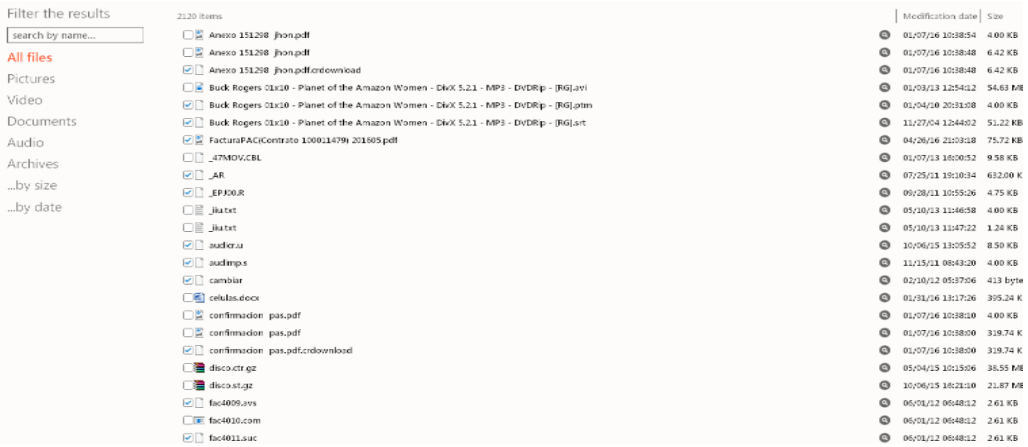


Imagen 63 captura marcación y recuperación de archivos

- El resultado es el siguiente

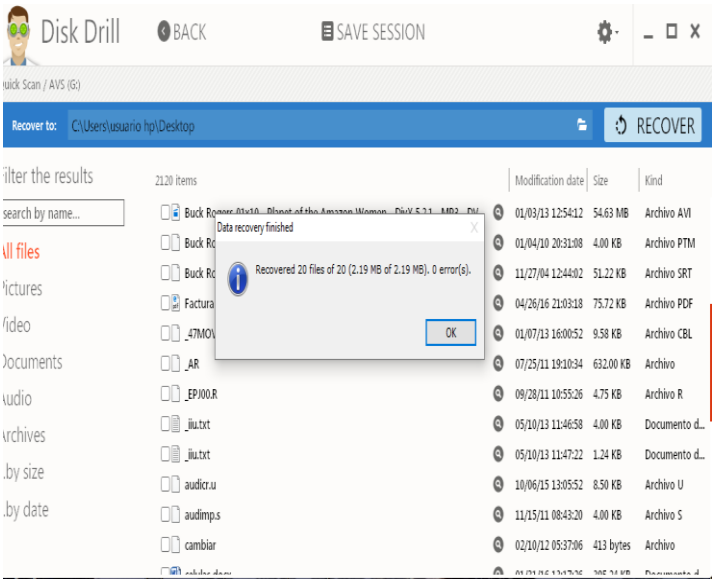
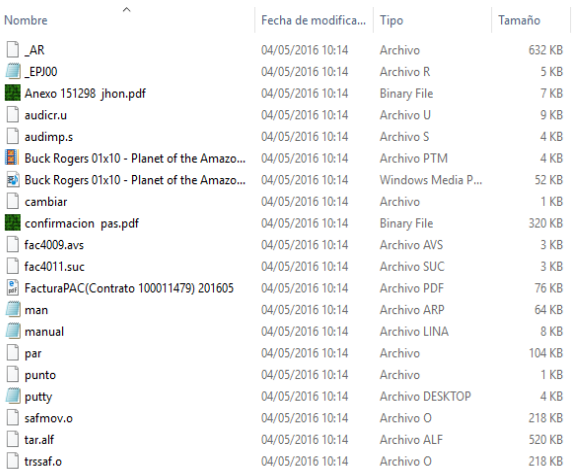


Imagen 64 captura resultados de la herramienta diskdrill

Los archivos recuperados se muestran a continuación



Nombre	Fecha de modifica...	Tipo	Tamaño
_AR	04/05/2016 10:14	Archivo	632 KB
_EPJ00	04/05/2016 10:14	Archivo R	5 KB
Anexo 151298 jhon.pdf	04/05/2016 10:14	Binary File	7 KB
audicr.u	04/05/2016 10:14	Archivo U	9 KB
audimp.s	04/05/2016 10:14	Archivo S	4 KB
Buck Rogers 01x10 - Planet of the Amazo...	04/05/2016 10:14	Archivo PTM	4 KB
Buck Rogers 01x10 - Planet of the Amazo...	04/05/2016 10:14	Windows Media P...	52 KB
cambiar	04/05/2016 10:14	Archivo	1 KB
confirmacion pas.pdf	04/05/2016 10:14	Binary File	320 KB
fac4009.avs	04/05/2016 10:14	Archivo AVS	3 KB
fac4011.suc	04/05/2016 10:14	Archivo SUC	3 KB
FacturaPAC(Contrato 100011479) 201605	04/05/2016 10:14	Archivo PDF	76 KB
man	04/05/2016 10:14	Archivo ARP	64 KB
manual	04/05/2016 10:14	Archivo LINA	8 KB
par	04/05/2016 10:14	Archivo	104 KB
punto	04/05/2016 10:14	Archivo	1 KB
putty	04/05/2016 10:14	Archivo DESKTOP	4 KB
safmov.o	04/05/2016 10:14	Archivo O	218 KB
tar.alf	04/05/2016 10:14	Archivo ALF	520 KB
trssaf.o	04/05/2016 10:14	Archivo O	218 KB

Imagen 65 captura de archivos recuperados

Conclusion del resultado de la prueba con Diskdrill (sobre el mismo pendrive SanDisk cruzer de 2 GB).

De los 20 archivos rescatados 15 fueron correctamente recuperados, 2 con error que por su nombre se identificaron como películas, se probaron 3 reproductores distintos para abrirlos y no funcionó, los otros 3 archivo no cuentan con extensión, no se dejan abrir con ninguna aplicación, también se consideran dañados.

Comparación de resultados, herramientas: Recuva y DiskDrill

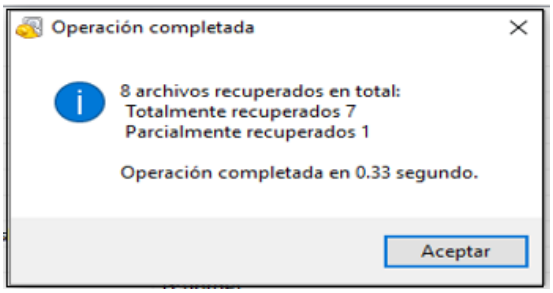


Imagen 66: Resultado según Recuva
(ver pág. 105)

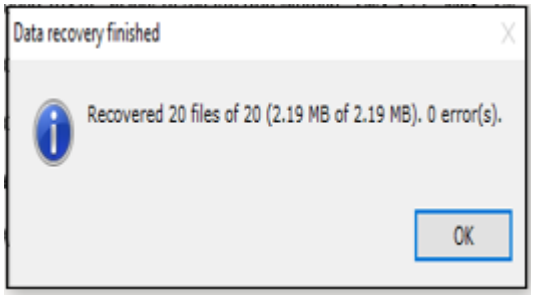


Imagen 67: Resultado según DiskDrill
(ver pág. 110)

Los resultados en eficacia y en tiempo de recuperación de Recuva son aceptables, no obstante, comparando con los arrojados por DiskDrill, es significativa la diferencia en la cantidad de archivos correctamente recuperados.

Se debe tener en cuenta que se trata de versiones gratuitas y es probable que las aplicaciones comerciales sean capaz de ofrecer una mayor eficacia.

Nota: Entre los recuperados con Diskdrill hay 4 que coinciden con los logrados por Recuva.

Prueba piloto 2

Se efectúa a continuación una prueba piloto con utilidades propias del sistema teniendo en cuenta que es un método útil en algunos casos. La prueba está diseñada de la siguiente forma:

Se aplica las utilidades para actualizar controladores y cambiar la letra y ruta de acceso de unidad sobre un pendrive Kingston DTSE9 8 GB no reconocido por ningún equipo con daño desconocido que fue donado para este proyecto.

Imagen 68: Pendrive utilizado en la prueba piloto 2

Pasos para actualizar controladores

- Inicio
- Equipo
- Click derecho
- Administrar
- Administración de dispositivos
- Controladoras de bus serial universal
- Doble click
- Dispositivo de almacenamiento USB
- Click derecho
- Actualizar software de controladores

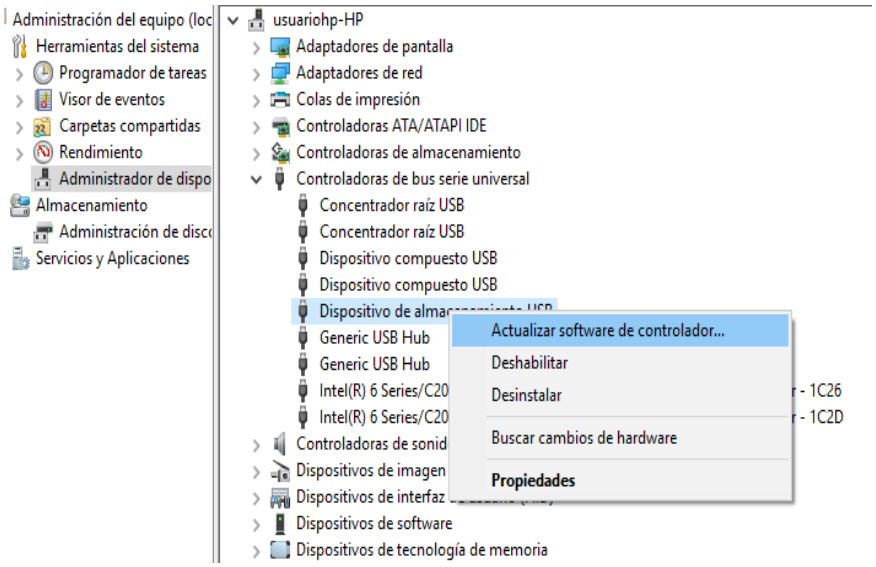


Imagen 69 Captura de actualización de software de controladores

Pasos para cambiar la letra y ruta de acceso de la unidad

- Inicio
- Equipo
- Click derecho
- Administrar
- Administración de discos
- Selecciona la memoria
- Click derecho
- Cambiar letra y ruta de acceso de unidad

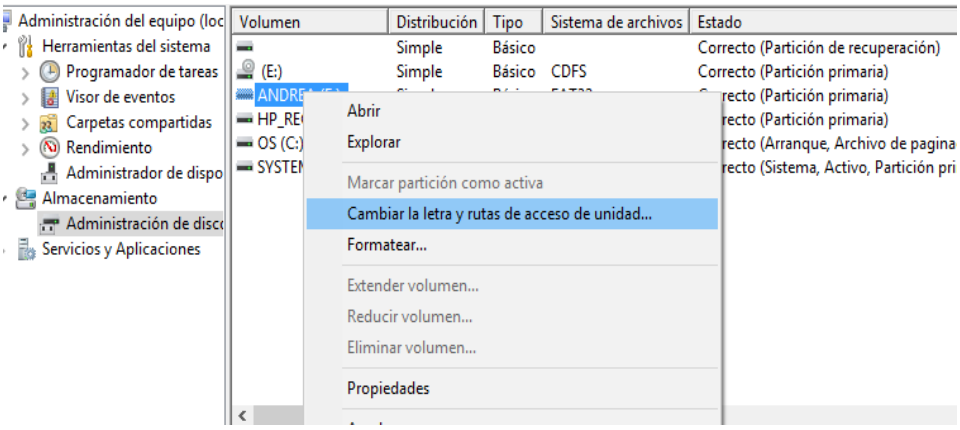


Imagen 70 captura cambio de letra y ruta de acceso a la unidad

Se seleccionó la letra G de las opciones y aceptar.

Esto permitió recuperar la funcionalidad la memoria, pero la muestra vacía. Ahora se procede a aplicar una herramienta de recuperación de datos.

Una vez recuperada la funcionalidad.

Se aplica recuva

Dar click en escanear

No busco los archivos. No da opción de seleccionar archivos a recuperar.

Prueba fallida.

Se Aplicando usb show.

Dar click en recuperar archivos ocultos, seleccionar el dispositivo.

Una vez terminado muestra un mensaje de finalización.

Ir al equipo Abrir el dispositivo

El siguiente fue el resultado

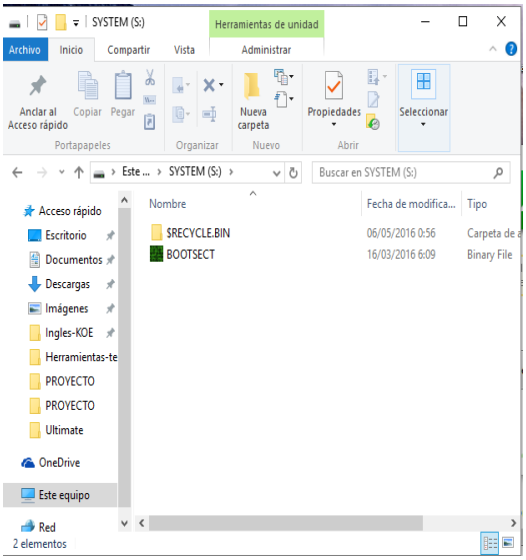


Imagen 71 captura resultados de la herramienta usb Show

El resultado muestra unos archivos recuperados pero se asumen dañados pues no se dejan visualizar se determina prueba fallida.

Se aplica RemoRecover

Pasos para la prueba con RemoRecover:

- Para descargar la herramienta se debe ir al enlace **http://www.remorecover.com/recupere-archivos.html**
- Dar click en el botón **Descargar ahora**
  La descarga se inicia automaticamente.

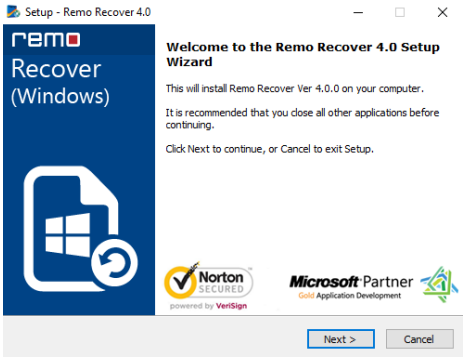


Imagen 72 Captura ejecución remo recover

- Luego se debe ejecutar para instalarlo. Se inicia el asistente anterior
- Dar click en el botón next

- Marcar I accept the agreement para aceptar términos y condiciones y dar click en Next sucesivamente hasta que aparezca el botón instalar

Completada la instalación dar click en finish

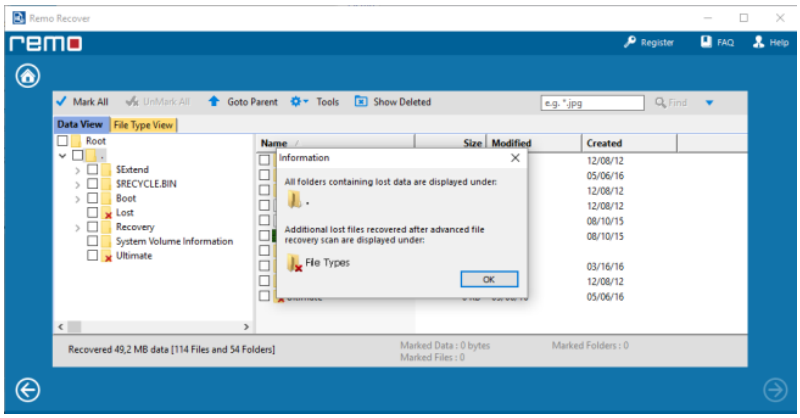


Imagen 73 captura prueba realizada con remo recover

Selecciona la ubicación para los recuperados

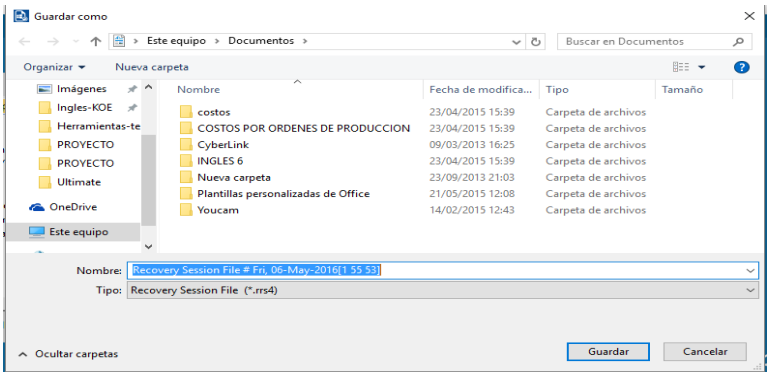


Imagen 74 captura destino para archivos a recuperar

El siguiente es el resultado

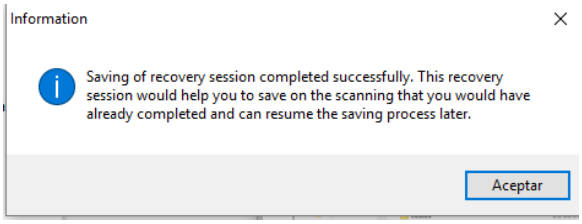


Imagen 75 captura resultados de la herramienta remo recover

RemoRecover no recuperó nada

Se aplica disk dril

Tipo de escaneo profundo

Lo que encontró para recuperar es lo siguiente:

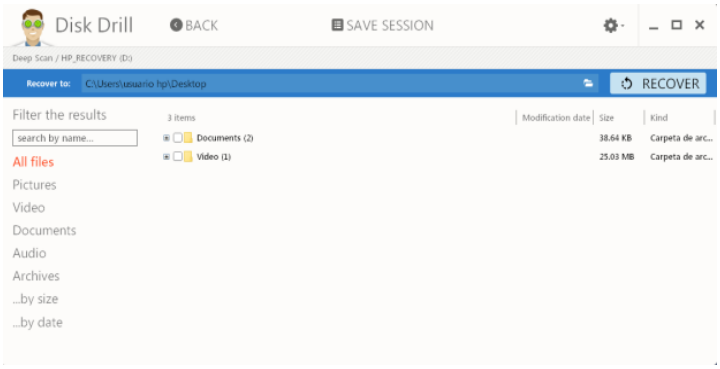


Imagen 76 captura archivos encontrados por diskdrill

Marcar la casilla respectiva y dar click en recover

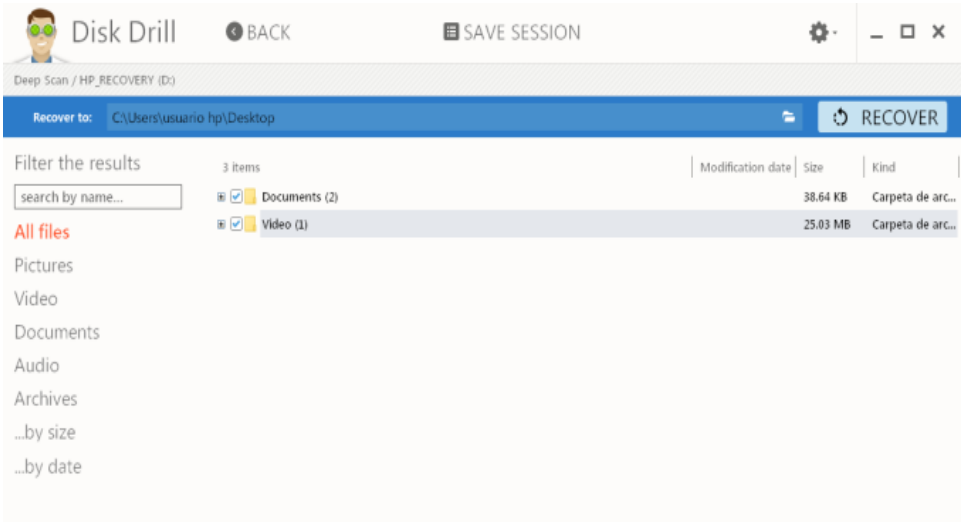


Imagen 77 captura marcación de archivos a recuperar

Seleccionar el destino para ubicar los recuperados

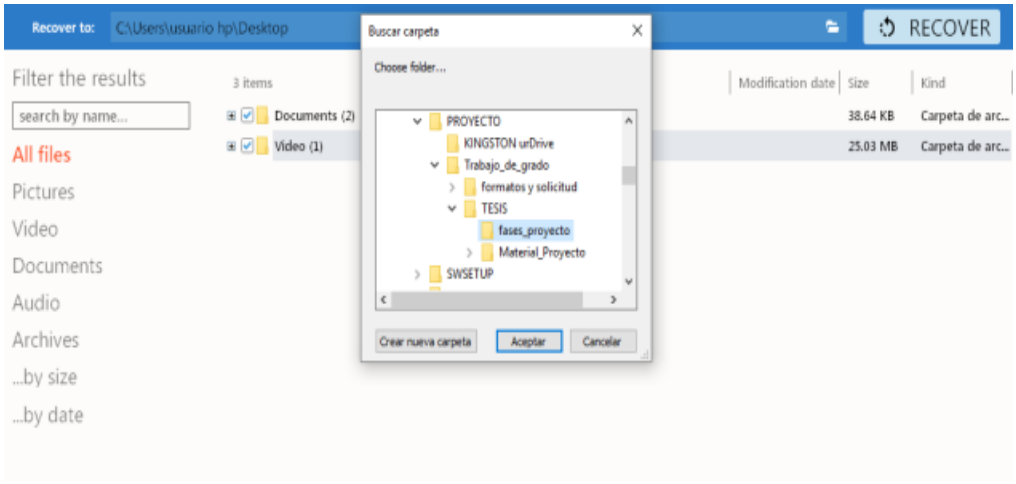


Imagen 78 captura selección de destinos para los archivos a recuperar

El resultado es el siguiente

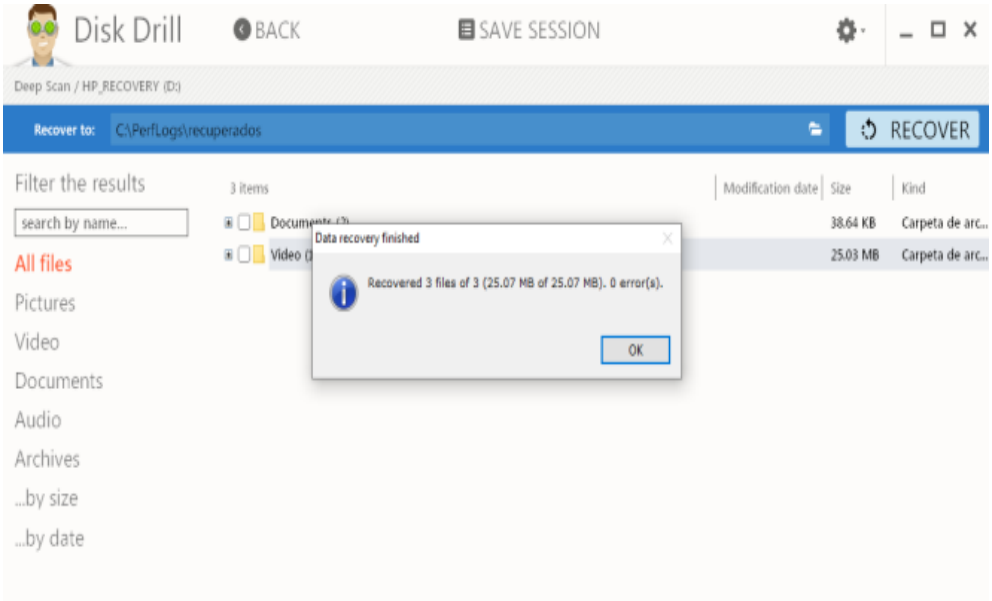


Imagen 79 captura resultados de la herramienta disk drill

Conclusiones del resultado de la prueba con DiskDrill, posterior a la recuperación de funcionalidad del dispositivo físico.

De los 3 archivos recuperados 3 fueron correctamente, 1 video y 2 archivos de Word. Los resultados en eficacia y en tiempo de recuperación son aceptables pero se debe tener en

cuenta que se trata de una versión gratuita y es probable que la aplicación comercial sea capaz de ofrecer una mayor eficacia, teniendo en cuenta que la versión gratuita de Disk Drill analiza los discos y muestra la lista de los archivos eliminados. Después de ver los resultados, pueden activar el programa para recuperarlos. Utilizando la versión gratuita del programa se puede recuperar los datos activando antes, una de las tecnologías de protección y recuperación de archivos: Recovery Vault o Recuperación Garantizada. Dentro de sus características se menciona que es posible recuperar los archivos borrados con sus nombres y estructura originales.

4.5 Etapa 5: Guía metodológica de recuperación de la información contenida en pendrives

Criterios generales

Esta guía pretende ayudarle a mejorar la comprensión y utilización de técnicas de software aplicables para la recuperación de información contenida en pendrives. Su utilidad radica en la posibilidad de brindar una opción factible para una solución óptima; en particular con respecto al daño inducido o accidental de dicho dispositivo.

En función de todo el proceso de análisis y los resultados obtenidos se llega a la conclusión de que la metodología propuesta desde esta investigación para la recuperación de información cuando se presente un daño en un pendrive; dependerá del tipo de daño, es importante contar con información adicional que pueda servir para el diagnóstico y así determinar la causa de la pérdida de los datos para poder seguir correctamente la guía respectiva en el proceso.

Procedimiento para recuperar información de un pendrive.

1. Objetivo

Proponer unos métodos de solución mediante técnicas de software para recuperar información perdida, contenida en pendrives.

2. Definiciones

Recuperación: recuperar archivos perdidos o eliminados de un pendrive por diferentes causas como daño físico del dispositivo de almacenamiento, borrado accidental, fallos del sistema, ataques de virus y hackers, empleando herramientas de recuperación de información.

Medio de almacenamiento masivo: El medio o soporte de almacenamiento es el aparato en donde se escribe o leen datos, permiten el almacenamiento de grandes cantidades de información, tienen la característica de almacenar bloques de bytes, el tipo de acceso viene determinado por la construcción física del medio y la unidad de lectoescritura.

Dispositivo: Equipo que puede manejar los diferentes medios de almacenamiento y pueden ser: magnético, ópticos o electrónicos.

Pendrive: Dispositivo electrónico-digital portátil de almacenamiento de datos que emplea memoria flash NAND.

Información de pendrive: Información ubicada físicamente en una memoria usb, pueden ser archivos personales, información educativa, laboral o de cualquier otro tipo.

Restauración: Volver a poner algo en el estado inicial. La información se restaura en otro dispositivo después de un incidente en el original.

Tabla 13. Procedimiento inicial de restauración.

Paso	Proceso	Especificación
1	Comprobar si verdaderamente la unidad tiene alguna falla, presenta algún error o daño.	La herramienta Check Flash Permite mapear en pantalla el estado del pendrive para saber si tiene daños.
2	Identificar y definir el tipo de daño	Analizar cuál es el tipo de daño que posee el pendrive para poder aplicar determinada herramienta, la más apropiada
3	Verificar si el dispositivo es reconocido y se puede acceder a los archivos almacenados	Si no se puede acceder a los archivos de forma manual proceder a utilizar software de recuperación.

De acuerdo con la experiencia y toda la literatura estudiada sobre las herramientas y métodos para la recuperación de información, teniendo en cuenta que esta investigación se apoya en las herramientas aplicables al pendrive con daño inducido o accidental, se construye

la siguiente tabla que muestra las herramientas propuestas para determinadas fallas del dispositivo.

En la tabla se presenta la mayor cantidad de casos de daño describiendo el problema ocasionado y las diferentes herramientas aplicables en cada caso en particular para la respectiva solución. Esto servirá de iluminación a los usuarios cuando tengan un problema de pérdida de información, cuando el pendrive presente falla.

Tabla 14: Casos de daños y herramienta aplicable

¿Cuándo ocurre el daño?	**¿Qué problema ocasiona?**	**¿Con que herramienta se resuelve?** Herramienta aplicable
El dispositivo sufre ataques de malware	Se ocultan los archivos eliminan o el dispositivo se vuelva inaccesible	• R-Studio • TestDisk • Recuva
No se usa modo seguro para la expulsión del dispositivo	Sistema de archivos corrupto o dañado.	• PhotoRec
Se daña la tabla de particiones o se borra por error, esta formateada con algún sistema de archivos poco estándar.	Deja de funcionar, no es reconocido el pendrive.	• Remo Recover • EaseUS Data Recovery 9.9 • Partition wizard • Utilidad del sistema (Cambiar letra de la unidad)
Se formatea por error el dispositivo	Pérdida de información	• Pen Drive Data Doctor Recovery • NTFS Recovery • DiskDrill
Por motivos desconocidos deja de funcionar correctamente el dispositivo	Inaccesibilidad a la información	• Micron USB Drive Data Recovery, • Partition Wizard
no utilizar la opción de “Quitar Hardware con Seguridad”	Inaccesible	• GetDataBack • HDD Low Level Format Tool (solo para recuperar funcionalidad del dispositivo
Hay celdas defectuosas que causan el bloqueo de la tarjeta. Por ejemplo, una vez que se accede a la celda defectuosa, todos los intentos de lectura fallan.	Sectores dañados	• USB Disk Storage Format Tool **(** posteriormente se puede aplicar herramienta de recuperación de datos**)** • WinHex
Hay interrupción durante transferencia de datos	Pérdida de archivos	• PC Inspector File Recovery
Eliminación accidental por error o por descuido	Pérdida de información	• Wondershare Data Recovery
Oleada de energía eléctrica, magnética	Pérdida de toda la información y daño en la funcionalidad del dispositivo	• Pen Drive Undelete

Errores en el sistema de archivos	Inaccesibilidad, sistema de archivo de solo lectura	• USB Show
Exposición a la humedad	Afecta los circuitos, ocasiona daño del funcionamiento	Flash Memory Recovery

5.CONCLUSIONES, RECOMENDACIONES Y TRABAJO FUTURO

El propósito de esta investigación fue identificar y describir las herramientas destinadas a la recuperación de información y adicionalmente cómo hacerlo. A continuación se presentan las conclusiones, las recomendaciones relacionadas y las orientadas al trabajo futuro.

5.1 Conclusiones

- La guía metodológica para la recuperación de información posibilita que el proceso se desarrolle óptimamente ya que permite identificar la herramienta más apropiada y decidir cuál utilizar según el caso de daño y las necesidades del usuario, no obstante, en algunos casos los resultados de éxito no son garantizados en un 100%, la información se recupera totalmente en la mayoría de ellos pero en ocasiones solo se hace de manera parcial, en forma de ficheros dañados.
- La recuperación de información cuando existe daño físico, se debe realizar solo si el contenido de la unidad es demasiado importante y es estrictamente necesaria y obligatoria su recuperación, si se prueban varias de las herramientas y no se consigue reparar la unidad, se asume que el problema es físico que no se pueden resolver con ninguna técnica de software, se requiere desarmar el equipo y realizar reparación electrónica, existen compañías más avanzadas, especializadas y que disponen de herramientas para retirar el chip de memoria flash NAND de la tarjeta de circuito para poder extraer y descifrar los datos contenidos en la unidad.

- En ocasiones la unidad presenta daños físicos que pueden ser reparados mediante la sustitución de una pieza del dispositivo, sin embargo puede quedar resuelto el daño físico dejando utilizable el pendrive pero persistir el daño lógico, requiriendo una posterior intervención.
- Dependiendo del tipo de herramienta se pueden recuperar multitud de documentos o un número reducido, ya que cada herramienta tiene sus propias especificaciones y requerimientos.
- Cuando el daño del dispositivo es provocado con la intención de ocultar o destruir una evidencia, es necesario que las técnicas de software aplicadas lo sean sobre una imagen del dispositivo.
- El método para recuperar información es un paso a paso de la utilización de las técnicas de software elegidas para cada caso en particular.
- Las herramientas gratuitas son muy útiles y en muchos casos cumplen con el objetivo de recuperación sustituyendo el uso de software costoso.
- Al realizar las pruebas el procedimiento con las dos herramientas fue muy similar:

  Después de descargar e instalar el programa, se selecciona la unidad que tiene problemas y el tipo de escaneo que se quiere hacer (normal, profundo, específico), al finalizar el escaneo, se verá el listado de archivos disponibles para recuperación, se deben marcar y a continuación dar click en el botón recuperar, el programa comenzará a copiar los archivos antes perdidos en la nueva ubicación.
- Para minimizar el riesgo de pérdida de información accidental o inducida se debe disponer de una buena estrategia de backup con el fin de mantener a salvo la información, ya que esta es la técnica que bien implementada asegura un 100% la

eficacia en recuperación de información, actualmente existen varias herramientas que se pueden aplicar para tal fin. (véase tabla 14 pág.122)

5.2 Recomendaciones

- Es recomendable dejar de usar la unidad que se quiere recuperar, ya que cuanto más se use más difícil será recuperar los datos. cuando se escribe sobre el disco las posibilidades de éxito disminuyen de forma considerable, por eso, cuanto antes intentemos recuperar lo que hemos borrado más posibilidades tendremos de que no haya desaparecido para siempre cuando un pendrive falla, o cuando se eliminan o formatean datos en él, por lo general la información no desaparece, se queda en el dispositivo hasta que ese espacio es ocupado con nuevos archivos. Una vez que el espacio ha sido sobre escrito, recuperar los datos es mucho más difícil.
- Iniciar la recuperación inmediatamente se descubra un incidente en la unidad.
- Proteger el pendrive contra escritura (si esto es posible) antes iniciar la recuperación de información.
- No darse por vencido; si un programa no da resultado probar con otros.
- Hacer uso de herramientas que ayuden a prevenir el daño y a minimizar el riesgo. Existen aplicaciones aplicables al pendrive para proteger tanto el dispositivo físico como para salvaguardar la información que contenga y prevenir posibles fallas.

Tabla 15: Herramientas para proteger y prevenir fallas del pendrives

Herramienta	Descripción
USB Disk Ejector	Es una aplicación gratuita para Windows que proporciona una manera fácil de extraer los dispositivos USB de forma segura. No necesita instalación, para extraer un dispositivo USB solo se ejecuta la aplicación y se hace doble clic sobre el dispositivo que se quiere extraer.
USB SoftProtect	Es una aplicación con la que se puede proteger bajo contraseña la memoria USB. Protege la información importante que contiene el pendrive, permite incluir una contraseña adicional que proteja ficheros, cuenta con la opción de cifrar el dispositivo portátil. No tiene límite de peso o capacidad a la hora de realizar el cifrado, por lo que se puede proteger cualquier tamaño de información. Además, el proceso con el que realiza esta acción es de alta velocidad.
USB Rescate	Es una solución a los problemas que los virus ocasionan en las memorias USB, ayudando de este modo a eliminar los archivos que dañan el dispositivo. Entre las diferentes acciones que lleva a cabo el programa se encuentra la opción de eliminar las carpetas y los archivos ocultos que se crean automáticamente por los virus. USB Rescate elimina los virus de raíz del pendrive. Además, no es necesario conocer comandos para eliminar los archivos peligrosos, sino que el programa lo realiza automáticamente, enviando los archivos dañinos a una carpeta llamada 'cuarentena'.(Ericksystem, 2016)
PenSecurity	Es una aplicación que permite manejar con más seguridad el pendrive. La primera función interesante de PenSecurity es la de proteger contra escritura, marcando esta opción se impide que se pueda guardar nueva información en el dispositivo y, por consiguiente, que se pueda borrar nada. También tiene a disposición un cortafuego opcional, que impedirá que la ejecución automática del pendrive se accione directamente. Interesante y útil para prevenir ciertos problemas.

Herramienta	Descripción
USB Doctor	No es un antivirus, sino una herramienta para evitar que infecciones automáticas se extiendan al dispositivo USB y se auto ejecuten. Por lo tanto, es recomendable complementar la actividad de este programa con otro software como antivirus diseñado para garantizar por completo la seguridad del pendrives. Protege el dispositivo de almacenamiento de ser infectado por malware. El programa está basado en el estudio de este tipo de elementos dañinos que utilizan los dispositivos extraíbles para propagarse. Esta utilidad impide la ejecución de virus mediante una vacuna contra malware que se encuentran en el autorun.inf o en las carpetas de reciclaje de los dispositivos de almacenamiento extraíbles, e incluye protección contra nuevas formas de propagación. Es una aplicación fácil de utilizar, con una interfaz agradable, gratuito, y de naturaleza portable.
USB WriteProtect	Utilidad que protege contra escritura los dispositivos de almacenamiento y puertos USB
USB Safeguard	Es una aplicación gratuita para cifrar la unidad, genera una contraseña que se requerirá para acceder a los datos.
USB Utilities	Herramienta para realizar backups y para proteger la seguridad de la unidad, USB Utilities parchea el pendrive para impedir la creación de archivos autoarrancables, usados por algunos virus, y lo escanea en busca de virus. USB Utilities muestra información como el formato del USB, espacio usado y libre, desoculta ficheros y carpetas invisibles.
USB Security Utilities	Es una herramienta que permite proteger el pendrive de infecciones de virus. No requiere instalación, por lo que se puede guardar directamente en el dispositivo y ejecutarla en cualquier momento. Su análisis, puede ser total o de una carpeta en concreto, permite detectar cualquier amenaza que le pueda afectar. Esta herramienta también permite hacer 'backups' de toda la información contenida.

5.3 Trabajo futuro

- Las herramientas de recuperación de información presentadas se podrán aplicar con un enfoque de análisis forense para investigaciones de búsqueda y recolección de evidencias, este sería un trabajo que serviría de base y permitiría aprovechar de mejor forma la utilización de dichas herramientas.
- Actualizar la guía metodológica con nuevas técnicas de software que den solución a la mayoría de los casos de daño del dispositivo, que se podrán ir incluyendo a medida que vayan apareciendo durante los avances de la tecnología.
- Desarrollar un software prototipo para hacer un mapeo bit a bit del pendrive**.**
- Desarrollar una investigación sobre las herramientas de software propietario para recuperación de información y hacer el comparativo con las de software libre que se desarrollaron en esta investigación.

REFERENCIAS

ABCarticulos. (2016). Top 10 Revisión Software Recovery Disk. Recuperado de http://abcarticulos.info/article/top-10-revisin-software-recovery-disk

Adriano, J. (2015). Cómo recuperar archivos eliminados por accidente. Recuperado de http://geekpunto.com/como-recuperar-archivos-eliminados-por-accidente/

Agualimpia, C. (2012). ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES CON SYMBIAN OS, Electrónica, Pontificia Universidad Javeriana. Recuperada de OSfile:///G:/backup/para_referencias_bibliografia/Articulo_Symbian_OS_Forensics_Agualimpia.pdf

Almeida Romo, O.R. (2011). Metodología para la implementación de informática forense en sistemas operativos Windows y Linux. (Tesis de Ingeniero en Sistemas Computacionales). Universidad Técnica del Norte, Ibarra. Recuperada de

Álvarez Murillo M, A. (2016). Análisis Forense de dispositivos móviles iOS y Android. (Tesis de Ingeniería de sistemas). Universitat Oberta de Catalunya. Recuperada de file:///G:/backup/para_referencias_bibliografia/alvarez_2016_analisis_forense_dispositivos_moviles.pdf

Ariza Díaz, A. (2009). Iphorensics: un protocolo de análisis forense para dispositivos móviles. (Tesis de Ingeniería de sistemas). Universidad javeriana, Bogotá. Recuperada de http://pegasus.javeriana.edu.co

Arquillo Cruz J. (2007). Herramienta de apoyo para el análisis forense de computadoras. (Tesis de Ingeniería en informática).Universidad de Jaén, España. Recuperada de http://es.scribd.com

Cabrera, Meza, H.E. (2013). Informática Forense. Recuperado de file:///G:/backup/para_referencias_bibliografia/unad_herramientas%20de%20software%20utilizadasINFORMATICA%20FORENSE.pdf

Calzada Prada, R. (2004). Análisis forense de sistemas, Madrid: RA-MA EDITORIAL

Castañeda, F.J. (2009). Evaluación de herramientas para análisis forense orientada a discos duros. (Tesis de ingeniería en informática). Escuela superior de ingeniería mecánica y eléctrica, Culhuacán. Recuperada de http:// itzamna.bnct.ipn.mx/dspace/1/ESIME%20ANALIS%20FOREN.pdf

Cervera. (2015). Los mejores 10 programas gratuitos para recuperar archivos perdidos. Recuperado de https://www.wondershare.es/eliminar-archivos/gratuitos-para-recuperar-archivos-perdidos.html

Ciberseguridad GITS Informática (2016). Análisis Forense y Peritaje Informático. Recuperado de http://www.gitsinformatica.com/forense.html

Conde, D. (2012). Recuperación de información en dispositivos móviles. Recuperado de file:///G:/backup/para_referencias_bibliografia/Trabajo_final-David_Conde-96085.

Cortés de la Rosa, J.B. (2014). Manejo de evidencia digital en dispositivos de almacenamiento pendrive USB aplicando la norma iso/iec 27037:2012. (Tesis de especialización en seguridad informática). Universidad Nacional Abierta y a Distancia. Pasto, Recuperada http://66.165.175.249/handle/10596/2660Cruz N. (2015). 10 herramientas gratuitas para recuperar archivos borrados. Recuperado de http://www.1000tipsinformaticos.com/2015/04/10-herramientas-gratuitas-para.html

Fundacionctic. (2012). Cinco soluciones para recuperar archivos eliminados. Recuperado de http://www.fundacionctic.org/sat/articulo-cinco-soluciones-para-recuperar-archivos-eliminados

Galán, C. (2012). Organización Computacional. Recuperado de http://www.ecotec.edu.ec/documentacion%5Cinvestigaciones%5Cestudiantes%5Ctrabajos_de_clases/3232_TRECALDE_00000179.pdf

Gobierno de chile departamento de cooperativas. (2010). La información como activo estratégico. Seminario publicado en http: //www.decoop.cl /LinkClick.aspx?fileticket=iOrxDJH%2B%2Fc4%3D&tabid=351

Guevara Jacqueline (2016) Tsunami Panameño. Revista semana edición 1771 pág. 48

Hilari Choquehuanca, S. F. (2006). Dispositivos de almacenamiento, bibliotecología y ciencias de la información, 10(15), 75-81. Recuperado de http://www.ops.org.bo/textocompleto/bvsp/boxp75/revbib/v10n15/v10n15a12.pdf http://repositorio.utn.edu.ec

Icontec. (2013). Fundamentos sistema de gestión seguridad en la información. NTC/ISO 27001:2013.

Luzuriaga, H.A. (2011). Herramientas de análisis forense y recuperación de información en los dispositivos de almacenamiento. (Tesis de maestría en redes y telecomunicaciones). Universidad técnica de Ambato, Ambato – Ecuador. Recuperada de http://repositorio.uta.edu.ec/bitstream/123456789/55/1/t586m.pdf

Martínez Méndez F.J. (2004). *Recuperación de información: modelos, sistemas y evaluación*. Murcia: Kiosko.

Martínez, R. (2012). 10 programas para recuperar archivos borrados en Windows. Recuperado de http://archivo.de10.com.mx/15026.html

Martínez, Romo, J. (2010). Técnicas de recuperación de información. Recuperado de file:///G:/backup/para_referencias_bibliografia/Romo_2010_tecnicas_recuperacion_informacion_web.pdf

Mepal, P. (2016). Las mejores herramientas para recuperar archivos borrados. Recuperado de http://www.omicrono.com/2016/01/las-mejores-herramientas-para-recuperar-archivos-borrados.

Mórelo Madariaga j. (2013). Análisis forense al sistema Android afectado por el malware fakelookout y su solución (Tesis de ingeniería de sistemas). Universidad de san buenaventura. Recuperada de file:///g:/backup/para_referencias_bibliografia/analisis_forense_android_morelo_2013.pdf

Moreno, J. (2014). Programas Excelentes para recuperar archivos borrados. Recuperado de https://jackmoreno.com/2014/07/11/7-programas-excelentes-para-recuperar-archivos-borrados/

Oroxom E. (2015). Recuperando archivos borrados. Recuperado de http://www.milcomos.com/como-recuperar-tus-archivos-borrados-por-error/

Pour, A. (2015). Top 5 de softwares para recuperar datos. Recuperado de https://www.wondershare.com.br/utilitario-de-disco/top5-softwares-recuperar-cartoes-sd.html

Quisbert, M. W. (2012). Herramientas para recuperar datos orientados al usuario. Recuperado de file:///G:/backup/para_referencias_bibliografia/Articulo_Herramientas-para-recuperar-datos-orientadas-al-usuario.pdf

Rebollo, M. (2011). Dispositivos de almacenamiento. Universidad Politécnica de Valencia. Recuperada de file:///G:/backup/para_referencias_bibliografia/Dispositivos_de_almacenamiento_rebollo_2011.pdf

Rivas López J. L. (2009). Análisis forense de sistemas informáticos. Barcelona: Eureca Media. Universidad Nacional Abierta y a Distancia, UNAD. Fundamentos de la Informática Forense. Publicado en http://datateca.unad.edu.co

Santander Peláez, M. (2010) Guía metodológica para la investigación forense en el navegador web Google Chrome. Recuperado de file:///C:/Users/usuario%20hp/Desktop/PROYECTO/Trabajo_de_grado/TESIS/Material_Proyecto/Articulo-GUIA_METODOLOGICA_PARA_LA_INVESTIGACION_FORENSE_EN_EL_NAVEGADOR_WEB_GOOGLE_CHROME.pdf

Serna, e. (2013). ¿Está en crisis la ingeniería en el mundo? Una revisión a la literatura, Rev. Fac. Ing. Univ. Antioquia, (66), 199-208. Recuperado de https://aprendeenlinea.udea.edu.co/revistas/index.php/ingenieria/article/viewFile/15236/13239

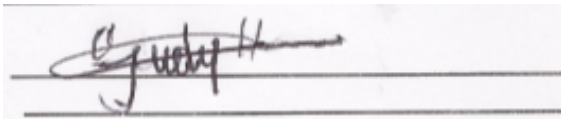
Topdatarecoverysoftware. (S.f). Top 10 programas de recuperación de datos. Recuperado de http://www.topdatarecoverysoftware.org/sr/

Uyana García, M.A. (2014). Diseño de un Área Informática Forense para un Equipo de Respuestas Ante Incidentes de Seguridad Informáticos CSIRT. (Tesis de Maestría en Gerencia de Seguridad y Riesgo). Universidad de las Fuerzas Armadas ESPE, Sangolqui. Recuperada de http://repositorio.espe.edu.ec

Villarrubia, C. (Sin fecha). Seguridad y Alta disponibilidad adopción de pautas de seguridad informática. Recuperado de http://arco.esi.uclm.es/~david.villa/seguridad/pautas.2x4.pdf

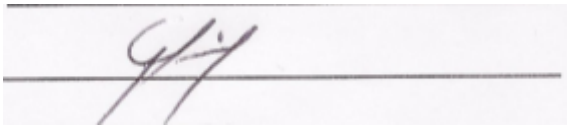
Yopla Mercado, A. (2012). Análisis forense en dispositivos extraíbles. (Tesis de ingeniería de sistemas).Universidad tecnológica del Perú, Lima. Recuperada de http://prezi.com

Yupanqui Chipana, E.R. (2009). Informática Forense. Revista de información tecnología y sociedad. Recuperado de ttp://www.academia.edu/4288731/RITS_3_INFORMATICA_FORENSE

FIRMA ESTUDIANTES 

_____

_____

FIRMA ASESOR 

FECHA ENTREGA: _____

FIRMA COMITÉ TRABAJO DE GRADO DE LA FACULTAD _____

RECHAZADO___ ACEPTADO____ ACEPTADO CON MODIFICACIONES_____

ACTA NO._____

FECHA ENTREGA: _____

FIRMA CONSEJO DE FACULTAD_____

ACTA NO._____

FECHA ENTREGA: _____