



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

**CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA
(TECNOLOGÍAS DE LA INFORMACIÓN)**

**TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO
DE INGENIERO EN SISTEMAS E INFORMÁTICA**

**TEMA: ESTUDIO COMPARATIVO DE TÉCNICAS FILE CARVING
PARA LA RECUPERACIÓN DE INFORMACIÓN PERDIDA POR DAÑOS
DE IMPACTO Y HUMEDAD EN DISPOSITIVOS DE
ALMACENAMIENTO SSD**

AUTOR: PÉREZ GAVILANES, CAROLINA ESTEFANÍA

DIRECTOR: ING. NINAHUALPA QUIÑA, GEOVANNI Mgtr

SANGOLQUÍ

2018



**DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA**

CERTIFICACIÓN

Certifico que el trabajo de titulación "ESTUDIO COMPARATIVO DE TÉCNICAS FILE CARVING PARA LA RECUPERACIÓN DE INFORMACIÓN PERDIDA POR DAÑOS DE IMPACTO Y HUMEDAD EN DISPOSITIVOS DE ALMACENAMIENTO SSD" realizado por la señorita **CAROLINA ESTEFANÍA PÉREZ GAVILANES**, ha sido revisado en su totalidad y analizado por software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de las Fuerzas Armadas-ESPE, por lo tanto me permito acreditarlo públicamente y autorizar a la señorita **CAROLINA ESTEFANÍA PÉREZ GAVILANES** para que lo sustente públicamente.

Sangolquí, 23 de febrero del 2017

Ing. Geovanni Ninahualpa Mgtr.

DIRECTOR



DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

AUTORÍA DE RESPONSABILIDAD

Yo, CAROLINA ESTEFANÍA PÉREZ GAVILANES con cédula de identidad N° 172173405-9, declaro que este trabajo de titulación "ESTUDIO COMPARATIVO DE TÉCNICAS FILE CARVING PARA LA RECUPERACIÓN DE INFORMACIÓN PERDIDA POR DAÑOS DE IMPACTO Y HUMEDAD EN DISPOSITIVOS DE ALMACENAMIENTO SSD" ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaro que este trabajo es de mi autoría, en virtud de ello me declaro responsable del contenido, veracidad y alcance de la investigación mencionada.

Sangolquí, 21 de febrero del 2018

A handwritten signature in blue ink, appearing to read 'Carolina', is positioned above a horizontal line.

CAROLINA ESTEFANÍA PÉREZ GAVILANES

CC. 1721734059



DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

AUTORIZACIÓN

Yo, CAROLINA ESTEFANÍA PÉREZ GAVILANES autorizo a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca virtual de la institución el presente trabajo de titulación "ESTUDIO COMPARATIVO DE TÉCNICAS FILE CARVING PARA LA RECUPERACIÓN DE INFORMACIÓN PERDIDA POR DAÑOS DE IMPACTO Y HUMEDAD EN DISPOSITIVOS DE ALMACENAMIENTO SSD", cuyo contenido, ideas y criterios es de mi autoría y responsabilidad.

Sangolquí, 21 de febrero del 2018



CAROLINA ESTEFANÍA PÉREZ GAVILANES

CC. 1721734059

DEDICATORIA

A mi familia quienes han estado apoyándome en cada paso de mi vida y han hecho posible la culminación de esta grandiosa etapa.

Carolina

AGRADECIMIENTO

Agradezco a mis padres y hermano quienes con su paciencia y amor han sido mi soporte, ejemplo y guía, al brindarme todo su amor incondicional.

A mis amigos quienes han estado junto a mí durante esta larga etapa de la vida, que me han brindado su mano en todo momento y he tenido grandes experiencias durante el recorrido por la universidad.

También, agradezco a la Universidad de las Fuerzas Armadas-ESPE por permitirme conocer a grandes seres humanos y profesionales que han sido ejemplo y motivación para continuar y superarme día a día. Al equipo del Laboratorio de Seguridad de la Información por su conocimiento y experiencia en el tema de esta investigación, en especial a mi director de proyecto Ing. Geovanni Ninahualpa Mgtr. Quien me ha guiado con paciencia y dedicación hasta culminar esta etapa.

Muchas gracias a todos.

Carolina

TABLA DE CONTENIDOS

CERTIFICADO	i
AUTORÍA DE RESPONSABILIDAD.....	ii
AUTORIZACIÓN.....	iii
DEDICATORIA.....	iv
AGRADECIMIENTO.....	v
TABLA DE CONTENIDOS.....	vi
ÍNDICE DE TABLAS	xiv
ÍNDICE DE FIGURAS	xxi
RESUMEN.....	xxviii
ABSTRACT	xxix
CAPÍTULO I.....	1
INTRODUCCIÓN	1
1.1 Antecedentes.....	1
1.2 Planteamiento del problema	3
1.3 Descripción resumida del proyecto	6
1.4 Justificación e importancia	7

1.5	Objetivos.....	9
1.5.1	Objetivo General	9
1.5.2	Objetivos Específicos.....	9
CAPÍTULO II		10
MARCO TEÓRICO.....		10
2.1	Almacenamiento de Información	10
2.2	Dispositivos de almacenamiento	11
2.2.1	Tipos de dispositivos de almacenamiento.....	11
2.3	Dispositivos de almacenamiento SSD	13
2.3.1	Geometría del dispositivo SSD	14
2.3.2	Arquitectura lógica.....	16
2.3.3	Subsistencia electrónica; cantidad de carga	18
2.3.5	Comparación disco SSD vs HDD	19
2.4	Recuperación de datos	20
2.4.1	Técnicas de recuperación de datos.....	21

2.5	Técnicas de recuperación File Carving	21
2.5.1	Basadas en la estructura interna de los archivos sin información del filesystem	22
2.5.2	Basadas en archivos fragmentados sin información del filesystem.....	22
2.6	Técnicas Semantic Carving & Fragment Recovery Carving.....	23
2.7	Herramientas de recuperación de datos	23
2.7.1	Herramientas de recuperación de datos para Linux	23
2.7.2	Herramientas de recuperación de datos para Windows	26
CAPÍTULO III		31
METODOLOGÍA DE RECUPERACIÓN DE INFORMACIÓN		31
3.1	Análisis físico	33
3.1.1	Inspección Visual.....	33
3.1.2	Verificación de la fuente de potencia.....	33
3.1.3	Detección en el BIOS (Sistema básico de entrada/ salida)	35
3.2	Reparación física temporal	35
3.2.1	Identificación de la gravedad y tipo de daño	36

3.2.2	Identificación de la posible solución.....	36
3.2.3	Ejecución de la solución	36
3.2.4	Verificación del resultado de la solución.....	37
3.3	Obtención de imagen	37
3.3.1	Preparación del dispositivo SSD de destino	37
3.3.2	Creación de la imagen.....	38
3.3.3	Verificación de la imagen	38
3.4	Análisis lógico	38
3.5	Recuperación de datos	39
3.5.1	Ejecución de software especializado File Carving	40
3.5.2	Revisión de archivos recuperados.....	40
CAPÍTULO VI.....		42
DESARROLLO DEL PROYECTO.....		42
4.1	Aplicación de encuesta	42
4.1.1	Selección del tamaño del segmento	42

4.1.2	Determinación de la muestra.....	43
4.1.3	Determinación de la pregunta de la prueba piloto	43
4.1.4	Tabulación de los resultados	44
4.1.5	Procesamiento de datos.....	45
4.2	Selección de los escenarios.....	55
4.2.1	Caída por descuido.....	55
4.2.2	Escenario: Caída de forma intencional	56
4.2.3	Escenario: Golpe con objeto contundente de forma intencional.....	56
4.2.4	Escenario: Aplastamientos de forma intencional.....	56
4.2.5	Escenario: Humedecimiento	59
4.3	Preparación de los escenarios	60
4.3.1	Laboratorio de ensayo de materiales / Dpt. Ciencias de la Tierra y Construcción ..	60
4.3.2	Laboratorio de materiales / Dpt. Energía y Mecánica	61
4.3.3	Laboratorio de informática forense / Dpt. de Ciencias de la Computación.....	62
4.4	Ejecutar la experimentación	63

4.4.1	Escenario 1: Caída por descuido menor a 1 metro	64
4.3.2	Escenario 2: Caída por descuido entre 1 y 2 metros	73
4.3.3	Escenario 3: Caída intencional en investigaciones forenses digitales con altura mayor a 2 metros	82
4.3.4	Escenario 4: Aplastamiento de forma intencional en investigaciones forenses digitales con una fuerza de 4,02 KN	101
4.3.5	Escenario 5: Aplastamiento de forma intencional en investigaciones forenses digitales con una fuerza de 4,75 kilo newtons	106
4.3.6	Escenario 6: Aplastamiento de forma intencional en investigaciones forenses digitales con una fuerza de 11,62 KN	112
4.3.7	Escenario 7: Golpe con objeto contundente.....	117
4.3.8	Escenario 8: Humedecimiento	123
CAPÍTULO V		137
RESULTADOS		137
5.1	Análisis de resultados	137
5.1.1	Escenario 1 Caída por descuido menor a 1 metro fuerza de 2,275 N	137

5.1.2	Escenario 2 Caída por descuido entre 1 y 2 metros con fuerza de 6,48 N.....	140
5.1.3	Escenario 3 Caída intencional en investigaciones forenses digitales con altura mayor a 2 metros.....	142
5.1.4	Escenario 4 Aplastamiento de forma intencional en investigaciones forenses digitales con una fuerza de 4,02 KN.....	149
5.1.5	Escenario 5 Aplastamiento de forma intencional en investigaciones forenses digitales con una fuerza de 4,75 KN.....	151
5.1.6	Escenario 6 Aplastamiento de forma intencional en investigaciones forenses digitales con una fuerza de 11,62 KN.....	153
5.1.7	Escenario 7 Golpe con objeto contundente.....	155
5.1.8	Escenario 8 Humedecimiento.....	155
5.2	Evaluar métricas de File Carving.....	160
5.3	Discusión de resultados.....	183
CAPÍTULO VI.....		186
CONCLUSIONES Y LÍNEAS DE TRABAJO FUTURO.....		186
6.1	Conclusiones.....	186

6.2	Recomendaciones	187
6.3	Líneas de trabajos futuros.....	187
BIBLIOGRAFÍA.....		188

ÍNDICE DE TABLAS

Tabla 1 <i>Tipos de unidades de almacenamiento de estado sólido</i>	13
Tabla 2 <i>Lectura/Escritura dispositivos SSD</i>	14
Tabla 3 <i>Consumo de energía dispositivos SSD</i>	18
Tabla 4 <i>Duración de los datos en dispositivos SSD</i>	19
Tabla 5 <i>Diferencias discos SSD Y HDD</i>	19
Tabla 6 <i>Técnica basada en la estructura interna de los archivos sin información del filesystem</i>	22
Tabla 7 <i>Técnicas basadas en archivos fragmentados sin información del filesystem</i>	22
Tabla 8 <i>Técnicas Semantic Carving & Fragment Recovery Carving</i>	23
Tabla 9 <i>Descripción de pines dispositivo SATA</i>	34
Tabla 10 <i>Síntomas de daños físicos</i>	35
Tabla 11 <i>Principales daños lógicos</i>	39
Tabla 12 <i>Métricas de las técnicas File Carving</i>	41
Tabla 13 <i>Tamaño del segmento meta</i>	42
Tabla 14 <i>Tamaño de la muestra</i>	43
Tabla 15 <i>Resultados de la prueba piloto</i>	45
Tabla 16 <i>Valores para calcular el tamaño de la muestra</i>	45

Tabla 17 <i>Escenarios caídas por descuido</i>	56
Tabla 18 <i>Escenarios forma intencional por aplastamiento</i>	61
Tabla 19 <i>Hardware utilizado</i>	62
Tabla 20 <i>Software especializado</i>	63
Tabla 21 <i>Características del dispositivo SSD para el escenario 1</i>	67
Tabla 22 <i>Resultado análisis físico del SSD para el escenario 1</i>	69
Tabla 23 <i>Resultado obtención imagen SSD para el escenario 1</i>	70
Tabla 24 <i>Características del dispositivo SSD para el escenario 2</i>	76
Tabla 25 <i>Resultado análisis físico SSD para el escenario 2</i>	78
Tabla 26 <i>Resultado obtención imagen SSD para el escenario 2</i>	79
Tabla 27 <i>Características del dispositivo SSD2</i>	84
Tabla 28 <i>Características del dispositivo SSD</i>	89
Tabla 29 <i>Características del dispositivo SSD escenario cuarto piso</i>	96
Tabla 30 <i>Resultado análisis físico SSD para el escenario cuarto piso</i>	98
Tabla 31 <i>Resultado obtención imagen SSD para el escenario cuarto piso</i>	98
Tabla 32 <i>Resultado análisis físico para el escenario 4</i>	103
Tabla 33 <i>Resultado obtención de imagen escenario 4</i>	103

Tabla 34 <i>Resultado análisis físico para el escenario 5</i>	108
Tabla 35 <i>Resultado obtención imagen SSD para el escenario 5</i>	109
Tabla 36 <i>Resultado análisis físico para el escenario 6</i>	113
Tabla 37 <i>Resultado obtención imagen SSD para el escenario 6</i>	114
Tabla 38 <i>Resultado análisis físico para el escenario 7</i>	121
Tabla 39 <i>Resultado análisis físico para el escenario 8</i>	125
Tabla 40 <i>Resultado obtención de imagen escenario 8</i>	127
Tabla 41 <i>Total, de archivos recuperados herramienta Foremost escenario 1</i>	137
Tabla 42 <i>Total, de archivos recuperados herramienta Scalpel escenario 1</i>	138
Tabla 43 <i>Total, de archivos recuperados herramienta Adroit Photo Recovery escenario 1</i>	138
Tabla 44 <i>Total, de archivos recuperados herramienta PhotoRec escenario 1</i>	139
Tabla 45 <i>Total, de archivos recuperados herramienta Foremost escenario 2</i>	140
Tabla 46 <i>Total, de archivos recuperados herramienta Scalpel escenario 2</i>	141
Tabla 47 <i>Total, de archivos recuperados herramienta Adroit Photo Recovery escenario 2</i>	141
Tabla 48 <i>Total, de archivos recuperados herramienta PhotoRec escenario 2</i>	142
Tabla 49 <i>Archivos recuperados herramienta Foremost escenario 3-caída segundo piso</i>	143
Tabla 50 <i>Archivos recuperados herramienta Scalpel escenario 3- caída segundo piso</i>	143

Tabla 51 Archivos recuperados herramienta Adroit Photo Recovery escenario 3- 2do piso.....	144
Tabla 52 Archivos recuperados herramienta PhotoRec escenario 3- caída 2do piso	144
Tabla 53 Archivos recuperados herramienta Foremost escenario 3- caída 3er piso.....	145
Tabla 54 Archivos recuperados herramienta Scalpel escenario 3- caída 3er piso.	145
Tabla 55 Archivos recuperados herramienta Adroit Photo Recovery escenario 3- 3er piso. ...	146
Tabla 56 Archivos recuperados herramienta PhotoRec escenario 3- 3er piso.	146
Tabla 57 Archivos recuperados herramienta Foremost escenario 3- 4to piso.....	147
Tabla 58 Archivos recuperados herramienta Scalpel escenario 3- 4to piso	147
Tabla 59 Archivos recuperados herramienta Adroit Photo Recovery.....	148
Tabla 60 Archivos recuperados herramienta PhotoRec escenario 3- 4to piso.....	148
Tabla 61 Archivos recuperados herramienta Foremost escenario 4 - vehículo pequeño.....	149
Tabla 62 Archivos recuperados herramienta Scalpel escenario 4 - vehículo pequeño	149
Tabla 63 Archivos recuperados herramienta Adroit escenario 4 - vehículo pequeño.....	150
Tabla 64 Archivos recuperados herramienta PhotoRec escenario 4 - vehículo pequeño	150
Tabla 65 Archivos recuperados herramienta Foremost escenario 5 - vehículo mediano	151
Tabla 66 Archivos recuperados herramienta Scalpel escenario 5 - vehículo mediano.....	151
Tabla 67 Archivos recuperados herramienta Adroit escenario 5 - vehículo mediano.	152

Tabla 68	<i>Archivos recuperados herramienta PhotoRec escenario 5 - vehículo mediano</i>	152
Tabla 69	<i>Archivos recuperados herramienta Foremost escenario 6 - vehículo pesado.....</i>	153
Tabla 70	<i>Archivos recuperados herramienta Scalpel escenario 6 - vehículo pesado.</i>	153
Tabla 71	<i>Archivos recuperados herramienta Adroit escenario 6 - vehículo pesado.</i>	154
Tabla 72	<i>Archivos recuperados herramienta PhotoRec escenario 6 - vehículo pesado.....</i>	154
Tabla 73	<i>Archivos recuperados herramienta Foremost escenario 8 – tiempo 10 segundos</i>	155
Tabla 74	<i>Archivos recuperados herramienta Scalpel escenario 8 – tiempo 10 segundos.....</i>	155
Tabla 75	<i>Archivos recuperados herramienta Adroit escenario 8 – tiempo 10 segundos</i>	156
Tabla 76	<i>Archivos recuperados herramienta PhotoRec escenario 8 – tiempo 10 segundos.</i>	156
Tabla 77	<i>Archivos recuperados herramienta Foremost escenario 8 – tiempo 30 segundos.</i>	157
Tabla 78	<i>Archivos recuperados herramienta Scalpel escenario 8 – tiempo 30 segundos.....</i>	157
Tabla 79	<i>Archivos recuperados herramienta PhotoRec escenario 8 – tiempo 30 segundos</i>	158
Tabla 80	<i>Archivos recuperados herramienta Adroit escenario 8 – tiempo 30 segundos</i>	158
Tabla 81	<i>Archivos recuperados herramienta Foremost escenario 8 – tiempo 65 segundos</i>	159
Tabla 82	<i>Archivos recuperados herramienta Scalpel escenario 8 – tiempo 65 segundos.....</i>	159
Tabla 83	<i>Archivos recuperados herramienta PhotoRec escenario 8 – tiempo 65 segundos</i>	160
Tabla 84	<i>Archivos recuperados herramienta Adroit escenario 8 – tiempo 65 segundos</i>	160

Tabla 85 <i>Cantidad de archivos iniciales</i>	161
Tabla 86 <i>Análisis, caídas utilizando Foremost en archivos de ofimática</i>	162
Tabla 87 <i>Comparación de archivos ofimática, fuerza 2,275 Newtons con foremost</i>	162
Tabla 88 <i>Análisis, caídas utilizando Scalpel en archivos de ofimática</i>	163
Tabla 89 <i>Comparación de archivos ofimática, fuerza 2,275 Newtons con scalpel</i>	163
Tabla 90 <i>Análisis, caídas utilizando PhotoRec en archivos de ofimática</i>	164
Tabla 91 <i>Comparación de archivos ofimática, fuerza 2,275 Newtons con photorec</i>	164
Tabla 92 <i>Análisis, caídas utilizando Foremost en archivos multimedia</i>	165
Tabla 93 <i>Comparación de archivos multimedia, fuerza 2,275 Newtons con foremost</i>	166
Tabla 94 <i>Análisis caídas utilizando Scalpel en archivos multimedia</i>	166
Tabla 95 <i>Comparación de archivos multimedia, fuerza 15,367 Newtons con scapel</i>	167
Tabla 96 <i>Análisis caídas utilizando PhotoRec en archivos multimedia</i>	167
Tabla 97 <i>Comparación de archivos multimedia, fuerza 15,367 Newtons con photorec</i>	168
Tabla 98 <i>Análisis caídas utilizando Adroit Photo Recovery en archivos multimedia</i>	168
Tabla 99 <i>Comparación de archivos multimedia, fuerza 6,480 Newtons con adroit</i>	169
Tabla 100 <i>Análisis caídas utilizando Foremost en archivos de ofimática</i>	169
Tabla 101 <i>Comparación de archivos ofimática, fuerza 6,480 Kilo Newtons con foremost</i>	170

Tabla 102 <i>Análisis aplastamiento utilizando Scalpel en archivos de ofimática</i>	170
Tabla 103 <i>Comparación de archivos ofimática, fuerza 4,020 Kilo Newtons con scapel.....</i>	171
Tabla 104 <i>Análisis aplastamiento utilizando PhotoRec en archivos de ofimática</i>	171
Tabla 105 <i>Comparación de archivos ofimática, fuerza 4,750 Kilo Newtons con photorec.....</i>	172
Tabla 106 <i>Análisis aplastamiento utilizando Foremost en archivos multimedia</i>	172
Tabla 107 <i>Comparación de archivos multimedia, fuerza 4,020 Kilo Newtons con foremost</i>	173
Tabla 108 <i>Análisis aplastamiento utilizando Scalpel en archivos multimedia</i>	173
Tabla 109 <i>Comparación de archivos multimedia, fuerza 4,020 Kilo Newtons con scalpel.....</i>	174
Tabla 110 <i>Análisis aplastamiento utilizando PhotoRec en archivos multimedia</i>	174
Tabla 111 <i>Comparación de archivos multimedia, fuerza 4,020 Kilo Newtons con photorec....</i>	175
Tabla 112 <i>Análisis aplastamiento utilizando Adroit Photo Recovery en archivos multimedia .</i>	175
Tabla 113 <i>Comparación de archivos multimedia, fuerza 4,020 Kilo Newtons con adroit</i>	176
Tabla 114 <i>Análisis humedecimiento utilizando Foremost en archivos de ofimática</i>	176
Tabla 115 <i>Comparación de archivos ofimática, tiempo 10 segundos con foremost.....</i>	177
Tabla 116 <i>Análisis humedecimiento utilizando Scalpel en archivos de ofimática.....</i>	177
Tabla 117 <i>Comparación de archivos ofimática, tiempo 10 segundos con scalpel</i>	178
Tabla 118 <i>Análisis humedecimiento utilizando PhotoRec en archivos de ofimática.....</i>	178

Tabla 119 <i>Comparación de archivos ofimática, tiempo 10 segundos con photorec</i>	179
Tabla 120 <i>Análisis humedecimiento utilizando Foremost en archivos multimedia</i>	179
Tabla 121 <i>Comparación de archivos multimedia, tiempo 10 segundos con foremost</i>	180
Tabla 122 <i>Análisis humedecimiento utilizando Scalpel en archivos multimedia</i>	180
Tabla 123 <i>Comparación de archivos multimedia, tiempo 10 segundos con scalpel</i>	181
Tabla 124 <i>Análisis humedecimiento utilizando PhotoRec en archivos multimedia</i>	181
Tabla 125 <i>Comparación de archivos multimedia, tiempo 30 segundos con photorec</i>	182
Tabla 126 <i>Análisis humedecimiento utilizando Adroit en archivos multimedia</i>	182
Tabla 127 <i>Comparación de archivos multimedia, tiempo 10 segundos con photorec</i>	183
Tabla 128 <i>Archivos válidos recuperados ofimática</i>	183
Tabla 129 <i>Archivos válidos recuperados multimedia</i>	184

ÍNDICE DE FIGURAS

Figura 1 Principales causas de pérdida de datos	4
Figura 2 Geometría de dispositivos SSD	15
Figura 3 Arquitectura NAND Flash.....	17
Figura 4 Arquitectura SSD propuesta	18
Figura 5 Causas de pérdida de información.....	20

Figura 6 Configuración Scalpel	24
Figura 7 PhotoRec reconocimiento del dispositivo	27
Figura 8 Partición del dispositivo seleccionado.....	27
Figura 9 Selección de tipos de archivos a recuperar	28
Figura 10 Directorio de salida.....	29
Figura 11 Adroit Photo Recovery selección de dispositivo	30
Figura 12 PhotoRec ejecución de software	30
Figura 13 Metodología de recuperación de.....	31
Figura 14 Metodología para recuperar información	32
Figura 15 Fases de análisis físico.....	33
Figura 16 Distribución de pines de un disco duro-SATA.....	34
Figura 17 Fases de la reparación física temporal	36
Figura 18 Fases de la obtención de imagen	37
Figura 19 Fases de la recuperación de datos	40
Figura 20 Tabulación prueba piloto	44
Figura 21 Encuesta, pregunta 1	46
Figura 22 Encuesta, pregunta 2	47

Figura 23 Encuesta, pregunta 3.....	48
Figura 24 Encuesta, pregunta 4.....	49
Figura 25 Encuesta, pregunta 5.....	50
Figura 26 Encuesta, pregunta 6.....	51
Figura 27 Encuesta, pregunta 7.....	52
Figura 28 Encuesta, pregunta 8.....	53
Figura 29 Encuesta, pregunta 9.....	54
Figura 30 Encuesta, pregunta 10.....	55
Figura 31 Dimensiones vehículo liviano.....	57
Figura 32 Vehículo mediano de referencia.....	58
Figura 33 Vehículo pesado de referencia.....	59
Figura 34 Máquina de compresión simple.....	60
Figura 35 Máquina de impacto.....	61
Figura 36 Fórmulas para cálculo de fuerza de impacto.....	63
Figura 37 Estado inicial del SSD para el escenario 1.....	65
Figura 38 Altura de escritorio.....	66
Figura 39 Altura de rebote.....	67

Figura 40 Hash md5 para el escenario 1	70
Figura 41 Resultados foremost SSD para el escenario 1	71
Figura 42 Resultados PhotoRec SSD para el escenario 1	72
Figura 43 Estado Inicial SSD para el escenario 2	74
Figura 44 Altura para el escenario 2	75
Figura 45 Altura de rebote escenario 2	76
Figura 46 Hash md5 para el escenario 2	79
Figura 47 Resultados foremost escenario 2	80
Figura 48 Resultado PhotoRec escenario 2.....	81
Figura 49 Altura segundo piso	82
Figura 50 Altura de rebote segundo piso	83
Figura 51 Resultado foremost caída segundo piso.....	86
Figura 52 Resultado Adroit PhotoRecovery caída segundo piso.....	87
Figura 53 Resultado PhotoRec caída segundo piso	87
Figura 54 Altura tercer piso	88
Figura 55 Altura de rebote tercer piso.....	89
Figura 56 Resultado foremost caída tercer piso	91

Figura 57 Resultado Adroit PhotoRecovery caída tercer piso	92
Figura 58 Resultado PhotoRec caída tercer piso.....	92
Figura 59 Estado inicial escenario cuarto piso.....	93
Figura 60 Altura para el escenario cuarto piso.....	94
Figura 61 Altura de rebote cuarto piso.....	95
Figura 62 Hash md5 para el escenario 3	99
Figura 63 Resultado Foremost caída cuarto piso	100
Figura 64 Resultado Adroit PhotoRecovery caída cuarto piso	101
Figura 65 Resultado PhotoRec caída cuarto piso.....	101
Figura 66 Fuerza ejercida del vehículo liviano sobre el dispositivo SSD.....	102
Figura 67 Hash para el escenario 4	104
Figura 68 Resultado foremost escenario 4	105
Figura 69 Resultados PhotoRec escenario 4	106
Figura 70 Resultados Adroit Photo Recovery escenario 4.....	106
Figura 71 Vehículo Ford sport track	107
Figura 72 Aplastamiento al dispositivo SSD por el vehículo mediano	107
Figura 73 Hash para el escenario 5	109

Figura 74 Resultados foremost escenario 5	110
Figura 75 Resultados PhotoRec escenario 5	111
Figura 76 Resultados Adroit Photo Recovery escenario 5.....	111
Figura 77 Fuerza de aplastamiento del vehículo pesado.....	112
Figura 78 Hash para el escenario 6	114
Figura 79 Resultados foremost escenario 6	115
Figura 80 Resultados Adroit photo recovery escenario 6	116
Figura 81 Resultados PhotoRec escenario 6	117
Figura 82 Distancia recorrida objeto contundente	118
Figura 83 Altura desde el centro de gravedad del objeto contundente	118
Figura 84 Fuerza de golpe con objeto contundente	120
Figura 85 Identificación de la solución	122
Figura 86 Limpieza de contactos de dispositivo SSD.....	123
Figura 87 SSD sometido en agua durante 10 segundos	124
Figura 88 SSD daño físico por agua durante 10 segundos.....	125
Figura 89 SSD reparación física temporal debido a agua	126
Figura 90 Hash para el SSD daño físico por agua durante 10 segundos.....	128

Figura 91 Resultado Foremost SSD en agua durante 10 segundos.....	129
Figura 92 Resultados Adroit photo recovery SSD en agua durante 10 segundos.....	130
Figura 93 Resultados PhotoRec SSD en agua durante 10 segundos.....	130
Figura 94 SSD sometido en agua durante 30 segundos	131
Figura 95 Resultado foremost SSD en agua durante 30 segundos.....	132
Figura 96 Resultados PhotoRec SSD en agua durante 30 segundos.....	133
Figura 97 Resultados Adroit Photo Recovery SSD en agua durante 30 segundos	133
Figura 98 SSD sometido en agua durante 65 segundos	134
Figura 99 Resultados Foremost SSD en agua durante 65 segundos	135
Figura 100 Resultado PhotoRec SSD en agua durante 65 segundos	136
Figura 101 Resultado Adroit Photo Recovery SSD en agua durante 65 segundos.....	136
Figura 102 Archivos válidos recuperados ofimática.....	184
Figura 103 Archivos válidos recuperados ofimática.....	185

RESUMEN

En el presente trabajo se realiza un análisis comparativo de dos técnicas File Carving utilizadas en las investigaciones forenses digitales aplicadas a dispositivos de almacenamiento SSD. Su principal objetivo es determinar la técnica que permita recuperar la mayor cantidad de información de forma íntegra. La primera parte de esta investigación se encuentra contenida en los capítulos 1 y 2, que presentan el marco teórico y el estado del arte acerca de los dispositivos de almacenamiento, técnicas de recuperación de datos y su funcionamiento. El capítulo 3 detalla la metodología a seguir para la recuperación de datos, la parte fundamental del proyecto se detalla en el capítulo 4, donde, se realiza la selección, preparación y aplicación de los escenarios en que los dispositivos de almacenamiento SSD han sufrido daños físicos como golpes, aplastamiento o humedad. A continuación, en el capítulo 5 se presenta los resultados del análisis de datos recopilados durante el capítulo anterior, finalmente en el capítulo 6 se detalla las conclusiones, recomendaciones y trabajo futuro.

PALABRAS CLAVE:

- **DISPOSITIVOS SSD**
- **TALLADO DE ARCHIVOS**
- **TALLADO SEMÁNTICO**
- **TALLADO DE RECUPERACIÓN DE FRAGMENTOS**

ABSTRACT

In this work, a comparative analysis of two File Carving techniques used in digital forensic investigations applied to SSD storage devices is performed. Its main objective is to determine the technique that allows to recover the greatest amount of information in its entirety. The first part of this research is contained in chapters 1 and 2, which present the theoretical framework and the state of the art about storage devices, data recovery techniques and their operation. Chapter 3 details the methodology to follow for data recovery, the fundamental part of the project is detailed in chapter 4, where the selection, preparation and application of the scenarios in which the SSD storage devices have suffered physical damage is made like bumps, crushing or humidity. Then, in chapter 5 the results of the analysis of data collected during the previous chapter are presented, finally in chapter 6 the conclusions, recommendations and future work are detailed.

KEYWORDS:

- **SSD DEVICES**
- **FILE CARVING**
- **SEMANTIC CARVING**
- **FRAGMENT RECOVERY CARVING**

ESTUDIO COMPARATIVO DE TÉCNICAS FILE CARVING PARA LA RECUPERACIÓN DE INFORMACIÓN PERDIDA POR DAÑOS DE IMPACTO Y HUMEDAD EN DISPOSITIVOS DE ALMACENAMIENTO SSD

CAPÍTULO I

INTRODUCCIÓN

1.1 Antecedentes

Durante las últimas décadas, el valor de la información ha cobrado mucha importancia, según lo menciona (Poisel, Tjoa, & Tavolato, 2011), el término "sociedad de la información" se ha introducido para referirse a la sociedad actual. La creación, manipulación, distribución y uso de la información se han convertido en actividades fundamentales en todos los ámbitos como la economía, política, cultura, entre otras, esta información se encuentra en distintos dispositivos de almacenamiento como memorias flash (USB), tarjetas micro SD, discos duros sólidos, discos duros electromecánicos, entre otros.

Según (Thing, et.al, 2011) la creciente dependencia de dispositivos de almacenamiento digital como discos electromecánicos y de estado sólido, para almacenar datos privados importantes e información altamente confidencial, ha dado lugar a que, durante la investigación forense digital, exista una mayor necesidad de recuperación de datos eficiente y precisa de archivos borrados.

Existe un índice de los años 2008-2009 (Kovačić, et.al, 2016) que revelan el comienzo del uso comercial masivo de discos duros basados en la tecnología de estado sólido (SSD), que ahora están reemplazando rápidamente los discos duros electromecánicos, compuestos de componentes mecánicos y electrónicos (HD). La tecnología de disco de estado sólido utiliza la misma interfaz electrónica que las unidades de disco duro para comunicarse con el resto del equipo, lo que facilita la instalación del disco de estado sólido y la sustitución de unidades de almacenamiento

electromecánicas. Los discos duros contruidos en tecnología de estado sólido tienen un controlador de memoria y una memoria flash de los que depende principalmente el rendimiento del dispositivo.

El daño, deterioro o destrucción intencional de los dispositivos de almacenamiento, son factores clave que dificultan en gran medida a la posible recuperación de datos y mitigación de este riesgo, (Ninahualpa, Diaz, & Gunn, 2017) indican que en el marco de los procedimientos, metodologías y técnicas a aplicar es necesario concientizar el vínculo que existe entre los factores que han producido la pérdida de información como son:

- Tipo de Fallo o mal Funcionamiento
- Tipo de Archivo a Restaurar
- Motivación Humana

Existen diferentes técnicas de recuperación de información, como son las técnicas de File Carving, éstas permiten la recuperación de archivos sin un conocimiento previo sobre el tipo de archivo que se va a recuperar, según (Poisel & Tjoa, 2013) debido a los avances en la investigación, el File Carving se ha convertido en una técnica esencial tanto para la recuperación de datos generales como para las investigaciones forenses digitales.

Ésta técnica consta de 3 pasos necesarios para la recuperación y se detallan a continuación:

- Recuperación de datos basados en metadatos: se basa en el sistema de archivos que se está utilizando, ya que los datos borrados y el orden de bloques de datos pueden ser preservados durante el proceso de eliminación de archivos. Los metadatos del sistema de archivos contienen información sobre el tamaño de bloque utilizado.

- Clasificación de fragmentos de archivos: Después del paso de pre procesamiento, los bloques restantes que no se pueden asociar con un archivo se envían al proceso de clasificación de fragmentos de archivo.
- Reensamblaje de fragmentos: Los bloques que han sido clasificados de acuerdo a su tipo se reensamblan en el orden correcto. El resultado de este paso es el archivo original o, en el caso de piezas faltantes, un archivo parcialmente ensamblado.

1.2 Planteamiento del problema

Actualmente, la información en la sociedad cumple un papel muy importante en todos los entornos: educativo, empresarial, personal, entre otros, que son almacenados en diferentes tipos de dispositivos o unidades como lo son los discos duros. Hoy en día los discos duros en estado sólido SSD¹ están teniendo una gran acogida, pero que como cualquier dispositivo de almacenamiento es vulnerable a sufrir algún tipo de daño y la información que contiene podría verse afectada o perderse de forma definitiva.

En la conferencia realizada por la empresa (IRecovery, 2017)), se presentó la estadística de daños en los dispositivos de almacenamiento con un alto porcentaje de daños en dispositivos de almacenamiento por factores físicos como caídas y golpes como se muestra en la Figura 1, siendo este un valor significativo se ha visto la necesidad de conocer que técnicas permiten la recuperación de datos bajo estas circunstancias.

¹ Los dispositivos de almacenamiento SSD son discos duros que utilizan una tecnología basada en memorias flash nand, y no contienen partes móviles como los discos duros tradicionales.

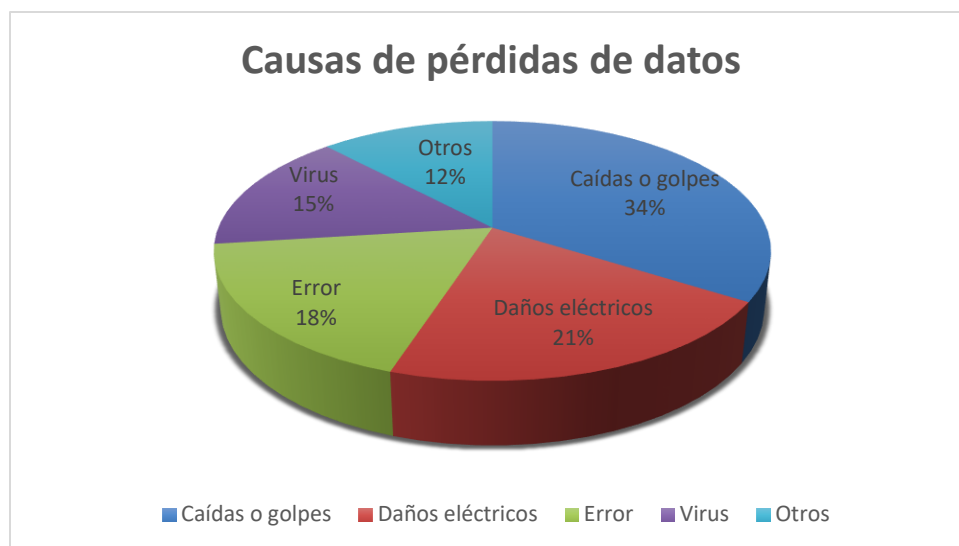


Figura 1 Principales causas de pérdida de datos
Fuente: (IRecovery, 2017)

Otro de los factores que causan daños en los dispositivos de almacenamiento son a causa de líquidos, existen varios casos en los que las computadoras portátiles y dispositivos de almacenamiento se caen al inodoro, a la bañera o a la piscina siendo estos los más comunes. (Nuncic, Michael;, 2017).

Según informes de peritaje informático, más del 60% de los casos presentados de pérdida de datos en las empresas o instituciones son a causa de sabotaje a los sistemas de información como robo o destrucción de los dispositivos de almacenamiento que en la mayoría de los casos es causado por los mismos empleados, siendo esta información valiosa para la empresa ya que podría contener registros contables, bases de datos de clientes entre otros, pudiendo afectar la supervivencia de las mismas (RecoveryLabs, 2017).

Los hospitales, instituciones educativas, viviendas, construcciones comerciales entre otras que cuentan con recursos tecnológicos como: computadoras, dispositivos de almacenamiento, internet, teléfonos inteligentes, servidores, sistemas de comunicación, etc., utilizados para su correcto funcionamiento y el desarrollo de sus actividades cotidianas, que durante los fuertes sismos

ocurridos en los últimos años han sido afectados causando destrucción parcial o total en los recursos mencionados.

La información que se ha perdido por las causas mencionadas anteriormente requiere un proceso de recuperación para poder acceder a la misma, pero las investigaciones sobre este tema únicamente tratan sobre la recuperación de datos a causa de daños de virus o malware, fallos en el sistema de archivos, entre otros daños lógicos, sin darle mayor importancia a la recuperación de datos perdidos por factores físicos y ambientales que también son otras causantes principales como los detallados a continuación:

- Golpes o impacto
- Incineración / Fuego
- Humedecimiento / Derrame de líquido
- Electrocuación / Sobrecarga eléctrica
- Magnetización

Conociendo estos factores causantes de la pérdida de datos, es necesario realizar un análisis de la información que se podría recuperar si hay un dispositivo de almacenamiento SSD que ha sido afectado por alguno de estos factores. Para esto es indispensable conocer que técnica resulta más eficiente utilizar mediante un análisis comparativo entre las herramientas que implementan estas técnicas de File Carving. Tener dicho análisis sería de gran ayuda para los investigadores forenses digitales que diariamente se ven confrontados con grandes cantidades de datos que tienen que ser procesados en cortos períodos de tiempo, es por esta razón que mientras exista una tabla comparativa que permita conocer la técnica más eficiente se acortará el tiempo de este proceso de recuperación según el caso.

Algunas técnicas de recuperación de datos como las basadas en firmas presentan varios inconvenientes sin poder recuperar: metadatos, archivos fragmentados, la estructura del directorio, mientras que las técnicas como File Carving dan solución a estos problemas haciendo el proceso de recuperación de datos más rápido y utilizando menor cantidad de espacio (Constanzo & Waimann, 2012).

1.3 Descripción resumida del proyecto

Este proyecto de investigación presentará un análisis de la información a ser recuperada de los dispositivos de almacenamiento SSD utilizando técnicas de File Carving que han sido evaluados en 2 escenarios siendo estos: golpes/impacto y humedad/derrame de líquido detallados a continuación:

Impacto: al momento que un dispositivo de almacenamiento SSD es golpeado con diferente intensidad de fuerza/ impacto.

Humedad: al momento que un dispositivo de almacenamiento SSD es dañado al ser sometido en agua en diferentes intervalos de tiempo.

Un ejemplo claro de estos escenarios se puede identificar cuando se presenta un delito y un dispositivo de almacenamiento que contiene evidencia incriminatoria se intenta eliminar o desaparecer, y estos dispositivos son golpeados o sometidos en agua hasta su destrucción total o parcial.

Las técnicas a utilizar son las siguientes:

Semantic Carving (Constanzo & Waimann, 2012), es utilizada para recuperar archivos de texto, donde se identifica el idioma en un bloque y los relaciona con bloques con el mismo idioma hasta reconstruir un texto de forma coherente.

Fragment Recovery Carving (Constanzo & Waimann, 2012), es utilizada para unir dos o mas fragmentos de un archivo, descartando los bloques intermedios que no pertenecen a los fragmentos.

Una vez elaborada la recopilación de la información, se empleará cuadros comparativos donde se va a analizar los resultados obtenidos aplicando las dos técnicas definidas sobre las siguientes métricas:

- Cantidad de archivos recuperados: es la cantidad total de archivos recuperados sean válidos, parcialmente válidos o falsos positivos.
- Cantidad de archivos válidos recuperados: son los archivos que se recuperaron de forma íntegra.
- Cantidad de falsos positivos o parcialmente recuperados: archivos que recuperan, pero no son accesibles en el caso de ofimática y archivos que se encuentran visibles, pero están incompletos como los archivos multimedia.

1.4 Justificación e importancia

Actualmente, la información dentro de las empresas y compañías cumple un rol vital para el correcto funcionamiento del negocio y la realización normal de sus actividades y al verse expuesta a situaciones de pérdida de sus datos tendría consecuencias graves provocando incluso el quiebre del negocio. Estos datos valiosos, por lo general se encuentran almacenados en los distintos tipos de dispositivos de almacenamiento como los de estado sólido o SSD que se encuentran dentro de computadoras de escritorio, portátiles o de uso externo siendo propensos a los diferentes tipos de daños tanto físicos como lógicos.

Para (B&S Recuperación de datos, 2017) no sólo las empresas tienen riesgo de pérdida de datos, debido a que los datos se encuentran en todo tipo de ambiente y clases sociales, que van desde las instituciones gubernamentales, pequeñas y grandes empresas hasta los usuarios comunes.

Los usuarios comunes utilizan los medios de almacenamiento para grabar y guardar fotografías de eventos especiales como vacaciones, datos personales, correos electrónicos o cuentas personales.

En casos de investigación forense digital, los dispositivos de almacenamiento son los más requeridos para la recopilación de evidencias, debido a que los involucrados intentan eliminar la información incriminatoria de los dispositivos de almacenamiento. Entre las formas más comunes para la destrucción de dichos dispositivos en este caso son los daños físicos como golpes o siendo sumergidos en agua.

En cuanto a los daños físicos, los más comunes son golpes/impacto o humedad/derrame de líquido que son producidos en distintos tipos de escenarios y pueden ser intencionales o no intencionales.

Golpes: Cuando un dispositivo de almacenamiento SSD sufre una caída o es aplastado con diferente intensidad de fuerza/impacto que varía dependiendo de la altura de la caída o si es lanzado con una fuerza inicial.

Humedad: Cuando un dispositivo de almacenamiento SSD ha sido afectado por derrame de un líquido o es sometido en agua en diferentes intervalos de tiempo a causa de algún accidente, descuido o de forma intencional al tener cerca de nuestro ordenador agua, café o algún tipo de líquido.

Estos dispositivos luego de sufrir estos daños son dados de baja sin intentar recuperar la información, y no se conocen estadísticas de cuanta información podría recuperarse en caso de utilizar diferentes técnicas.

Con el proyecto se puede apoyar a las aplicaciones de File Carving y realizar un análisis comparativo de dos técnicas en diferentes escenarios para una predicción de las métricas de cantidad de archivos recuperados, válidos recuperados y falsos positivos.

Esta investigación se realizará para comparar dos técnicas file carving con la identificación de una metodología que permita la recuperación de información donde los metadatos del sistema de archivos no se encuentren disponibles por daños en el dispositivo de almacenamiento sean estos lógicos o físicos.

1.5 Objetivos

1.5.1 Objetivo General

Realizar un estudio comparativo de dos técnicas File Carving para la recuperación de información perdida por daños de impacto y humedad en dispositivos de almacenamiento SSD.

1.5.2 Objetivos Específicos

- Determinar la metodología de recuperación de información.
- Preparar los escenarios de aplicación: caída, aplastamiento, golpe o impacto y humedad.
- Aplicar la metodología de recuperación de datos para cada escenario utilizando dos técnicas File Carving.
- Recolectar los datos recuperados de los dispositivos de almacenamiento SSD.
- Analizar y comparar las dos técnicas File Carving aplicadas utilizando cuadros comparativos.
- Evaluar y exponer resultados sobre las métricas del File Carving.

CAPÍTULO II

MARCO TEÓRICO

El capítulo tiene como objetivo el dar a conocer varios conceptos con referencia al tema de investigación como son los diferentes tipos de dispositivos de almacenamiento, escenarios más comunes de daños en los dispositivos de almacenamiento, técnicas y herramientas de recuperación de datos.

2.1 Almacenamiento de Información

La información cumple un papel muy importante en nuestro día a día, tanto para personas como empresas, y la forma de almacenar información en la nube o de forma electrónica para mantener la información de forma permanente es tendencia durante los últimos años. (Seguridad Digital INAP, s.f.).

Gracias al uso de internet que incrementa en todo el mundo diariamente se procesan grandes cantidades de datos, y por cada sesenta segundos se genera la siguiente información:

YouTube:	500 horas de video
E-mails:	150.000 mails
Facebook:	3.300.000 posts
Google:	65.972 búsquedas
Instagram:	65.972 fotos
Twitter:	448.000 tuits
WordPress:	1.440 posts
WhatsApp:	29.000.000 mensajes

Toda esta gran cantidad de información ha obligado a las empresas a que cambien la infraestructura y la tecnología para la recopilación de la información, descartando el uso de dispositivos de almacenamiento como cintas, discos magnéticos o memorias flash. Exigiendo que las empresas elijan formas óptimas de almacenamiento, como la empresa Hewlett Packard Enterprise (HPE) que ofrece una tecnología que son las cabinas All Flash Array (AFA) que utiliza discos de estado sólido SSD teniendo una mayor velocidad, tanto en escritura como lectura y mayor duración para un mejor rendimiento (Eleconomista.es, 2017).

2.2 Dispositivos de almacenamiento

Actualmente, las computadoras tanto portátiles como de escritorio necesitan dispositivos de almacenamiento para guardar los datos de forma definitiva al momento que la corriente eléctrica es interrumpida, y no solo el almacenamiento temporal de la memoria principal (Rebollo Pedruelo, 2011).

Además, los sistemas de almacenamiento están constituidos por uno o varios discos duros que constituyen en sí mismos un elemento delicado necesitando ciertas condiciones mínimas para su correcto funcionamiento, pero si son excedidos podría provocar averías físicas evitando que se pueda acceder a la información contenida (Ruiz, 2005).

2.2.1 Tipos de dispositivos de almacenamiento

2.2.1.1 Dispositivos magnéticos

Unidad de cinta magnética: Es un dispositivo que permite el almacenamiento utilizando una cinta en un carrete abierto como un cartucho, siendo esta una opción para almacenamiento de grandes cantidades de información de forma práctica (Papiewski, John;, s.f.).

Unidad de disco flexible o disquetera: El disquete es un disco removible magnético cuya capacidad de almacenamiento va desde 79,6 KB - 240 MB y se ha vuelto insuficiente para las necesidades y requerimientos actuales (Osteguna, 2005).


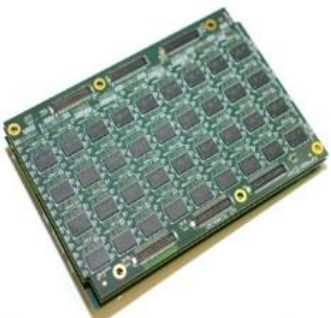
Unidad de disco rígido o disco duro: A nivel mundial existe un alto índice del uso de discos duros con un 80% de computadoras tanto de escritorio como portátiles. Los componentes principales son cabezales, platos y motor (IRecovery, 2017).

2.2.1.2 Dispositivos de estado sólido

Son dispositivos de almacenamiento mejor conocidos como Solid-State Drive (SSD) que según (IRecovery, 2017) son el futuro de los sistemas de almacenamiento. Estos tipos de discos son más rápidos que los tradicionales HDD y permiten que los sistemas operativos puedan tener un inicio más rápido. Los soportes SSD no contienen partes mecánicas y están constituidos principalmente de 2 elementos que son tarjeta electrónica y chip de memoria.

Para (Crisros, 2013) existen dos tipos de unidades de almacenamiento de estado sólido detallados en la tabla 1. Además, los dispositivos de almacenamiento de estado sólido o SSD según su uso son internos (discos duros de estado sólido) y externos (Memoria USB, Memoria Flash o Micro SD).

Tabla 1*Tipos de unidades de almacenamiento de estado sólido*

Tipo	Características
<p>SSD basados en memoria volátil SDRAM</p>  <p>Fuente: (Diffen)</p>	<p>Rápido acceso a datos, menos de 0.01 milisegundos.</p> <p>Usados para acelerar aplicaciones instaladas en el ordenador.</p>
<p>SSD basados en DRAM</p>  <p>Fuente: (Beeler, Brian;, 2012)</p>	<p>Incorpora una batería interna para asegurar la persistencia de datos, además de contar con un sistema de respaldo de disco.</p> <p>Si la potencia se detiene, la batería mantiene el dispositivo encendido el suficiente tiempo como para copiar todos los datos de la memoria RAM al disco de respaldo.</p> <p>Después de la restauración de energía, los datos se vuelven a copiar desde el disco de respaldo a la RAM y el SSD continua su operación normalmente.</p>

Fuente: (Crisros, 2013)

2.3 Dispositivos de almacenamiento SSD

Según (IBM, 2017), los SSD son dispositivos de almacenamiento que utilizan memoria de estado sólido no volátil (memoria flash), y el tiempo de acceso a los datos almacenados reduce notablemente ya que las operaciones de lectura son más rápidas que las operaciones de escritura. Un SSD funciona de igual forma que la unidad de disco duro o hard disk drive (HDD), pero los datos son almacenados de forma distinta utilizando chips con memorias flash interconectadas que son capaces de mantener la información aun cuando la potencia se ha perdido. (pcmag.com, 2017).

Según lo indica (Pérez Romero, V;, 2016) los discos SSD son más resistentes a golpes o impactos físicos que los dispositivos HDD. Estas nuevas unidades de almacenamiento no cuentan

con partes móviles ya que intercambian los platos giratorios por chips de memoria flash con gran capacidad haciendo que tengan un tamaño físico menor y mayor capacidad de almacenamiento. Las principales características de los SSD en cuanto a la lectura y escritura de datos se presentan en la tabla 2.

Tabla 2

Lectura/Escritura dispositivos SSD

Pruebas Sintéticas	Dispositivo SSD
Lectura secuencial	240 MB/s
Escritura secuencial	78 MB/s
Lectura aleatoria 512k	203 MB/s
Escritura aleatoria 512k	66 MB/s
Lectura aleatoria 4k	14 MB/s
Escritura aleatoria 4k	10 MB/s
Tiempo de acceso lectura/escritura	0,2 ms / 0,2 ms

Fuente: (Maturana, 2014)

2.3.1 Geometría del dispositivo SSD

La geometría del disco de estado sólido según (EcuRed, 2012) viene dado por las partes indicadas en la Figura 2:

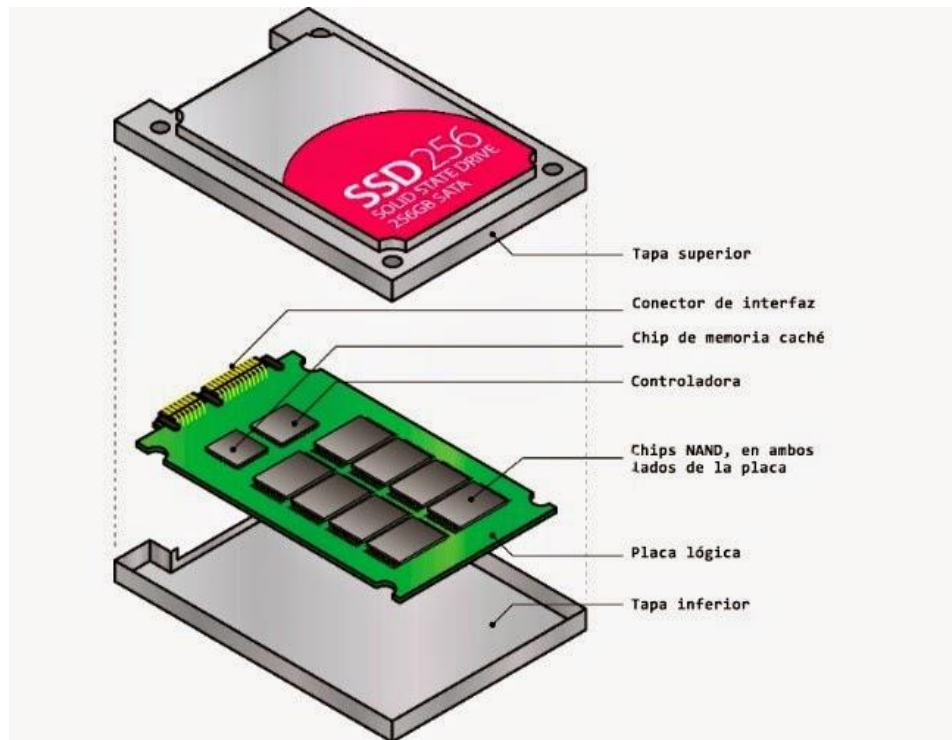


Figura 2 Geometría de dispositivos SSD
Fuente: (Maturana, 2014)

Descripción de los componentes

- Las tapas superior e inferior están encargadas de proteger los circuitos internos que contiene el SSD.
- Consta de 2 conectores SATA uno de 15 terminales que permite la alimentación del SSD, y otro de 7 terminales que permite la transmisión de datos entre la tarjeta madre y el dispositivo.
- Chip de memoria utiliza un pequeño dispositivo de memoria DRAM similar al caché de los discos duros. El directorio de la colocación de bloques y el desgaste de nivelación de datos también se mantiene en la memoria caché mientras la unidad está operativa.

- La controladora es un procesador electrónico que administra, gestiona y une los módulos de memoria con los conectores de entrada y salida. Las principales funciones que realiza son: Corrección de errores (ECC), use nivelación, bad bloque de asignación, leer y escribir el almacenamiento en caché, recolección de basura, cifrado.
- Módulos de memoria consisten en chips NAND Flash conectados en paralelo los cuales se encargan de almacenar los datos.
- Placa lógica es la que contiene los circuitos impresos para la conexión con los demás componentes del dispositivo SSD.

2.3.2 Arquitectura lógica

(Yan, Wang, & Yu, 2014) En su publicación sobre “Diseño e implementación de una arquitectura SSD basada en flash eficiente”, presenta la arquitectura lógica como se aprecia en la Figura 3, basada en memorias NAND flash que es la utilizada en los discos duros en estado sólido. La operación de lectura/programa puede solamente acceder al nivel de página, mientras que la operación de borrado puede solamente acceder al nivel de bloque.

La escritura se realiza mediante una operación de programa, que debe ir precedida de una operación de borrado que establece todos los bits en el bloque físico de destino en 1. Estas operaciones muestran una velocidad de asimetría. La operación de programa es más larga que la operación de lectura, pero relativamente más rápida que la operación de borrado.

A medida que avanza la tecnología de fabricación, la matriz flash NAND contiene cada vez más células lógicas en un solo paquete. Como se muestra en la Figura 3, la memoria flash NAND MT29F256G08KCAB de Micrón contiene dos buses independientes, que admiten la transferencia de datos DDR asíncrona y síncrona. Este chip flash NAND tiene dos objetivos por paquete, dos datos por objetivo y dos planos por dado.

Cada plano contiene su propio conjunto de registros de datos / caché. Esta arquitectura permite que el dispositivo flash realice operaciones de caché, copia de seguridad, múltiples matrices y multiplano.

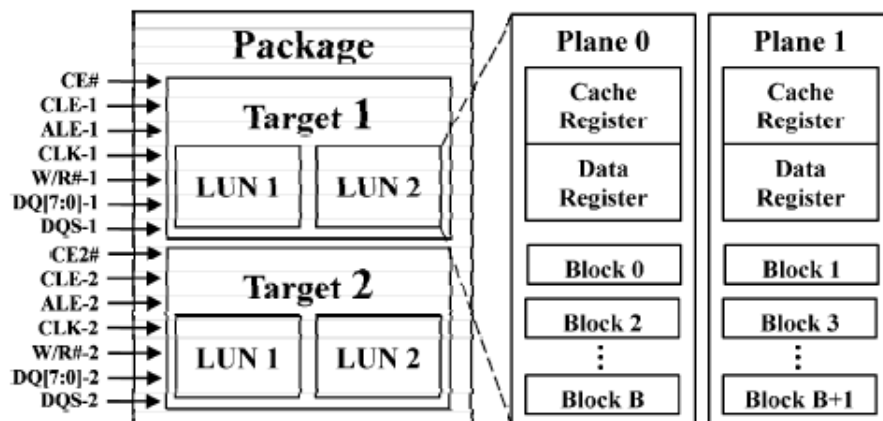


Figura 3 Arquitectura NAND Flash

Fuente: (Yan, Wang, & Yu, 2014)

(Takeuchi , 2012) presenta la arquitectura lógica de un dispositivo SSD como se muestra en la Figura 4 y cuyo funcionamiento se explica a continuación:

Durante la escritura, los datos se almacenan primero en la memoria de la clase de almacenamiento (SCM) a 10 Gbps. Luego los datos en SCM se transfieren a la memoria flash NAND con la velocidad de escritura sostenida de 2,69 Gbps, finalmente durante la lectura, la salida de lectura de datos de la memoria flash NAND al controlador pasa por SCM.

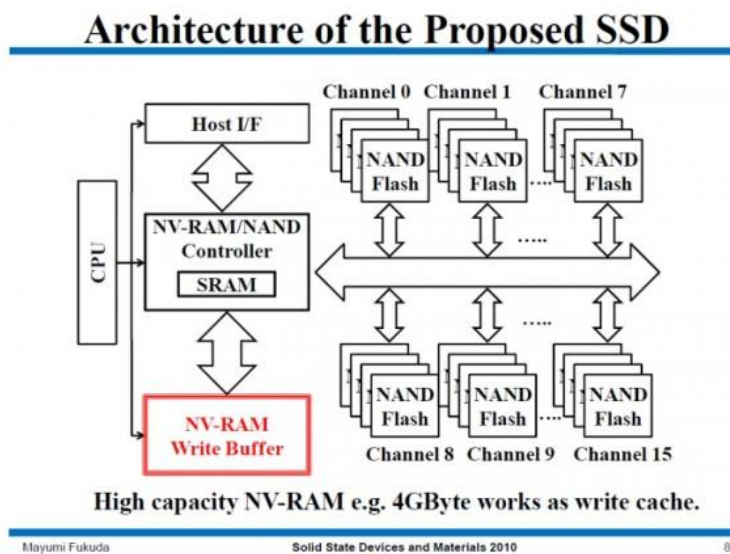


Figura 4 Arquitectura SSD propuesta
Fuente: (Takeuchi , 2012)

2.3.3 Subsistencia electrónica; cantidad de carga

(García, Alberto;, 2017) indica que los dispositivos SSD consumen energía dependiendo de la diferencia de capacidad de almacenamiento, así como la tecnología de este como se puede ver en la tabla 3.

Tabla 3

Consumo de energía dispositivos SSD

Marca	Capacidad de almacenamiento	Consumo de energía
Seagate Barracuda	1 TB	5.3 vatios
Seagate Barracuda	2 TB / 3 TB	8 vatios
Samsung 580 EVO	250 GB	0.025 vatios

Fuente: (García, Alberto;, 2017)

(Mayoraz, Guillermo;, 2016) habla sobre cuánto dura la información en un dispositivo SSD, afirmando que dichos dispositivos de uso personal y profesional están diseñados para guardar datos a 25°C durante 2 años. (Cox, 2011) en su investigación demuestra que al aumentar la temperatura el tiempo de retención de datos baja considerablemente en una relación inversamente proporcional.

En caso de los dispositivos SSD de uso empresarial al pasar de una temperatura de 25° a 30° el tiempo de los datos contenidos baja de 20 semanas a tan solo 10. Esta información se aprecia mejor en la tabla 4.

Tabla 4

Duración de los datos en dispositivos SSD

Carga de trabajo	Uso activo (encendido)	Uso de retención (apagado)	Fracaso funcional Rqmt (FFR)
Cliente	40°C 8 horas/día	30 °C 1 año	<=3%
Empresa	55 °C 24 horas/día	40 °C 3 meses	<=3%

Fuente: (Cox, 2011)

2.3.5 Comparación disco SSD vs HDD

Los dispositivos de almacenamiento SSD y HDD son las unidades más utilizadas para guardar información, pero tienen grandes diferencias que se detallan en la tabla 5:

Tabla 5

Diferencias discos SSD Y HDD

Características	SSD	HDD
Capacidad	256 GB a 16 TB	1 TB a 10 TB
Consumo	Menor	Mayor
Coste	Precio elevado	Más económico
Calor, electricidad, ruido	Como no hay rotación en un SSD, utiliza menos energía y no generan ruido o calor.	Utilizan más electricidad para girar los platos, generando ruido y calor.
Fragmentación	No tiene	Puede darse
Durabilidad	Sus celdas pueden reescribirse un número limitado de veces	Las partes mecánicas que pueden dañarse con movimientos bruscos
Tiempo de arranque del Sistema Operativo	7 segundos	16 segundos
Transferencia de datos	200 a 550 MB/s	50 a 150 MB/s

Fuente: (Yubal;, 2017)

2.4 Recuperación de datos

Los dispositivos de almacenamiento pueden sufrir daños como:

- Fallo de hardware: es causado por incendio, daños por inundaciones o golpes.
- Falla lógica: cuando es formateada accidentalmente, tiene corrupción en el firmware o falla en los semiconductores que afectan los datos contenidos.

Por esta razón se hace necesario el proceso de recuperación de datos, ya que la información contenida es de gran valor ya sea para empresas o de forma personal.

Actualmente existen diferentes formas de recuperación de datos por distintos medios digitales utilizando software básico, pero sobrescribiendo sobre el dispositivo de almacenamiento, siendo esta opción la no recomendable ya que los archivos recuperados pueden podrían estar dañados y causar mayor número de falsos positivos.

Los factores causantes de pérdida de información según (IRecovery, 2017) se detallan en la Figura 5:

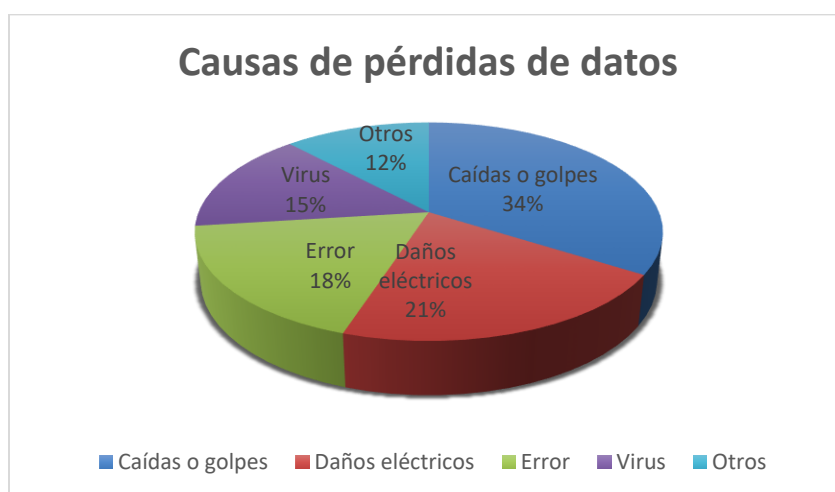


Figura 5 Causas de pérdida de información
Fuente: (IRecovery, 2017)

2.4.1 Técnicas de recuperación de datos

Técnica Signature Search (Búsqueda de firmas): Ésta técnica se utiliza cuando los archivos se pueden reconocer, pero no por completo, como por ejemplo los archivos *.jpg son fácilmente reconocibles, mientras que los archivos más complejos no se pueden reconocer causando una gran desventaja. La herramienta IsoBuster es la que implementa esta técnica que contiene una lista basada en todos los tipos de 'firmas' reconocibles. Esta lista contiene todos los posibles archivos reconocidos por este método, hasta que encuentra la siguiente firma reconocible (IsoBuster, 2017).

Técnica basada en el reemplazo del hardware: Ésta técnica es la más utilizada en los discos HDD por su estructura física que permite el cambio de sus partes dañadas reemplazando con nuevas que cumplan las mismas características para que el disco duro pueda funcionar nuevamente y la información sea extraída.

Técnicas Talla de Archivos (File Carving): Ésta es una técnica poderosa para recuperar archivos y fragmentos de archivos cuando las entradas de directorio están dañadas o faltan. El bloque de datos es buscado bloque por bloque para datos residuales que coinciden con los valores de encabezado y pie de página específicos del tipo de archivo. Tallar es especialmente útil en casos criminales donde el uso de esta técnica puede recuperar evidencia.

2.5 Técnicas de recuperación File Carving

File Carving o talla de datos (Christiaan Beek, s.f.) es el proceso de extraer una colección de datos de un conjunto de datos más grande. Las técnicas de File Carving con frecuencia se producen durante una investigación digital cuando se analiza el espacio del sistema de archivos no asignado para extraer archivos. Los archivos se "tallan" en el espacio no asignado utilizando valores de encabezado y pie de página específicos del tipo de archivo.

Según (Constanzo & Waimann, 2012) y (Ninahualpa, Diaz, & Gunn, 2017) las técnicas File Carving se clasifican de la siguiente manera:

2.5.1 Basadas en la estructura interna de los archivos sin información del filesystem

Tabla 6

Técnica basada en la estructura interna de los archivos sin información del filesystem

Técnica	Características
Header-Footer File	Basa su funcionalidad en dos identificadores “Encabezado” y “Pie/Fin”, pues cuando este se encuentra presente se conoce el inicio y el final, de modo que los bloques útiles ocupados son considerados como el archivo a restaurar (Esra’a Alshammary, 2016).
File Structure and Block Content	Basa su funcionalidad en dos partes, la estructura del archivo a restaurar y los bloques útiles contenidos en él (Alherbawi, Shukur, & Sulaiman, 2016).
File Structure Based Carving	Analiza las estructuras internas del tipo de archivo, además de las que se encuentran en la cabecera (Constanzo & Waimann, 2012).
Semantic Carving	Identifica el idioma utilizado en un bloque, y lo relaciona con bloques en el mismo idioma de forma coherente para reconstruir un texto (Constanzo & Waimann, 2012).

2.5.2 Basadas en archivos fragmentados sin información del filesystem

Tabla 7

Técnicas basadas en archivos fragmentados sin información del filesystem

Técnica	Características
Fragmentation Issue	Se emplean con el fin de restaurar un archivo que se encuentra fragmentado en el dispositivo de almacenamiento. En este sentido estas técnicas no cuentan con: identificadores o cadenas de secuencia para reconocer en los fragmentos (Esra’a Alshammary, 2016).
Predictive File	Fundamenta su acción en la creación de nueva metadata que referencie a los bloques de almacenamiento válidos, utilizando un sistema de archivos (Filesystem) virtual como forma de predicción y acceso a los mismos (Alherbawi, Shukur, & Sulaiman, 2016).
Fragment Recovery Carving	Es utilizada al describir cualquier método de carving en el que dos o más fragmentos se reensamblan para formar el archivo u objeto original (Simson, 2007).
Statistical Carving	Se calcula en función matemática de los bloques buscando similitudes entre ellos para reconstruir los archivos. Algunas variantes usan funciones estadísticas, hashes, y/o signatures, entre otras (Constanzo & Waimann, 2012).

2.6 Técnicas Semantic Carving & Fragment Recovery Carving

Tabla 8

Técnicas Semantic Carving & Fragment Recovery Carving

Semantic Carving	Fragment Recovery Carving
Es una técnica para recuperar archivos basados en un análisis lingüístico del contenido del archivo. Por cada bloque se identifica el idioma utilizado y lo relaciona con todos los bloques que se encuentren con el mismo idioma de forma coherente. Es una técnica muy útil para los formatos de archivos de texto.	Esta técnica de recuperación es especialmente útil para la recuperación de archivos que se encuentren fragmentados, donde encuentra dos o más fragmentos de un archivo, y separa los bloques de fragmentos que no corresponden al archivo (Poisel, Tjoa, & Tavolato, 2011).
Existe un prototipo que implementa esta técnica que fue presentado por S. Garfinkel llamado S2 que es escrito en C++ (Forensics II, 2016).	Existen varias herramientas específicas para este proceso como lo es Scalpel para el sistema operativo Kali Linux y Adroit Photo Recovery en el sistema operativo Windows
La técnica Content based Carving también implementa Semantic Carving y una herramienta que la utiliza para el análisis interno de la estructura de los archivos es Foremost en el sistema operativo Kali Linux y PhotoRec en el sistema operativo Windows	

2.7 Herramientas de recuperación de datos

Las herramientas presentadas a continuación son basadas en las técnicas mencionadas en la sección 2.6, sus características y funcionamiento se indica a continuación.

2.7.1 Herramientas de recuperación de datos para Linux

Scalpel (Tecmint, 2013), esta herramienta implementa la técnica fragment recovery carving, que permite ensamblar los archivos fragmentados, es de código abierto para sistemas operativos Linux y Mac. Es también utilizada para investigaciones forense digital.

2.7.1.1 Proceso de recuperación de datos utilizando Scalpel en el sistema operativo Kali Linux

La herramienta Scalpel se encuentra instalada por defecto en el sistema operativo, pero debe ser configurada como se presenta a continuación:

A. Configurar el archivo scalpel.conf

Con la siguiente línea de comandos se accede al archivo de configuración scalpel.conf.

```
$ leafpad /etc/scalpel/scalpel.conf
```

A continuación, descomentar las extensiones de archivos que se desea recuperar como se muestra en la figura 6.



```
scalpel.conf x
82 # art y 150000 \x4a\x47\x03\xe0 \xd0\xcb\x00\x00
83 #
84 # GIF and JPG files (very common)
85 # gif y 5000000 \x47\x49\x46\x38\x37\x61 \x00\x3b
86 # gif y 5000000 \x47\x49\x46\x38\x39\x61 \x00\x3b
87 # jpg y 200000000 \xff\xd8\xff\xe0\x00\x10 \xff\xd9
88 #
89 #
90 # PNG
91 # png y 20000000 \x50\xe4\x47 \xff\xfc\xfd\xfe
92 #
93 #
94 # BMP (used by MSWindows, use only if you have reason to think there are
95 # BMP files worth digging for. This often kicks back a lot of false
96 # positives
97 #
98 # bmp y 100000 BM??\x00\x00\x00
99 #
100 # TIFF
```

Figura 6 Configuración Scalpel

Fuente: (Hausser, Tann, 2013)

B. Seleccionar dispositivo a recuperar

Se debe seleccionar el dispositivo del cual se realizará el proceso de recuperación de información y la ubicación de destino donde se guardará los datos recuperados

```
$ scalpel 'nombre de partición o carpeta a recuperar' -o 'directorio de salida'
```

Finalmente se debe esperar que el proceso termine y se verifica en el directorio de salida los archivos recuperados.

Foremost (Kali Tools. , 2014), esta herramienta es utilizada para el algoritmo Semantic carving, para recuperar archivos perdidos basados en sus encabezados, pies de página y estructuras de datos internas, foremost puede trabajar en archivos de imagen o directamente en una unidad.

2.7.1.2 Proceso de recuperación de datos utilizando Foremost en el sistema operativo Kali Linux

La herramienta Foremost se encuentra instalada por defecto en el sistema operativo, y permite seleccionar un tipo de extensión de archivo a recuperar o todos como se presenta a continuación:

A. Seleccionar tipo de archivo

La opción -t indica el tipo de archivo a recuperar, se debe especificar la extensión (jpg, png, doc, pdf, etc.), o en el caso de requerir todos los archivos especificar con la opción all.

```
-t all
```

B. Ejecutar la recuperación

Ejecutar el siguiente comando:

```
$ foremost -v -t all -i 'nombre de partición' -o 'directorio de salida'
```

Dónde:

- v: opción para visualizar el proceso de recuperación de datos (se puede omitir)
- i: opción para seleccionar el nombre de partición o carpeta a recuperar
- o: opción para seleccionar el directorio de salida

2.7.2 Herramientas de recuperación de datos para Windows

PhotoRec (Tannhausser, 2014), está diseñado para recuperar archivos, de todo tipo de extensión ya sea de multimedia o de texto, archivos de discos duros, memorias flash, CD-ROM, o incluso imágenes borradas de las tarjetas de memorias de cámaras digitales. PhotoRec ignora el sistema de archivos, y hace una búsqueda profunda de los datos basado en la estructura interna de los archivos, funcionando incluso si el sistema de archivos tiene graves daños o ha sido formateado.

2.7.2.1 Proceso de recuperación de datos utilizando PhotoRec en el sistema operativo Windows 7

A. Seleccionar la partición del dispositivo a recuperar

En la figura 7 se presenta como la herramienta reconoce los dispositivos de almacenamiento.


```

C:\Users\carop\Desktop\PhotoRec\testdisk-7.1-WIP\photorec_win.exe
PhotoRec 7.1-WIP, Data Recovery Utility, January 2018
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

PhotoRec is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys, then press Enter):
Disk /dev/sda - 750 GB / 698 GiB (RO) - TOSHIBA MK7575GSX
>Disk /dev/sdb - 7807 MB / 7446 MiB (RO) - Kingston DataTraveler 2.0

>[Proceed ] [ Quit ]

Note:
Disk capacity must be correctly detected for a successful recovery.
If a disk listed above has an incorrect size, check HD jumper settings and BIOS
detection, and install the latest OS patches and disk drivers.

```

Figura 7 PhotoRec reconocimiento del dispositivo

B. Seleccionar el sistema de archivos

Identificar el sistema de archivos como se muestra en la figura 8.

```

C:\Users\carop\Desktop\PhotoRec\testdisk-7.1-WIP\photorec_win.exe
PhotoRec 7.1-WIP, Data Recovery Utility, January 2018
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk /dev/sdb - 7807 MB / 7446 MiB (RO) - Kingston DataTraveler 2.0

Partition          Start      End      Size in sectors
No partition       0  0  1  949  59  6  15249408 [Whole disk]
> 1 P HPFS - NTFS  0 128  1  949  59  6  15241344 [CAROP]

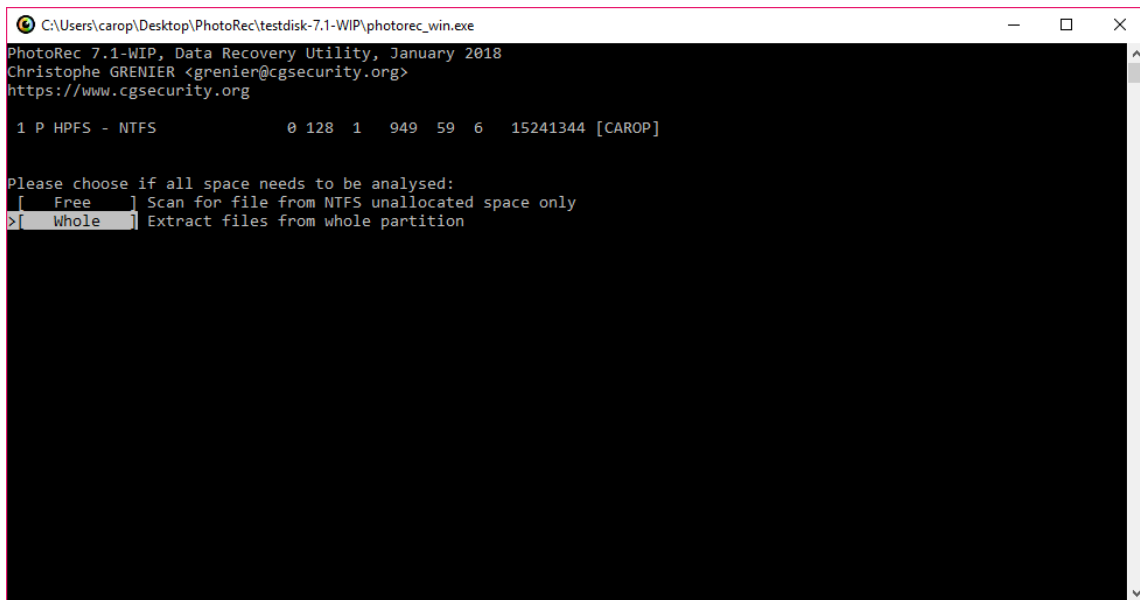
>[ Search ] [Options] [File Opt] [ Quit ]
Start file recovery

```

Figura 8 Partición del dispositivo seleccionado

C. Seleccionar el tipo de recuperación

Seleccionar la opción whole que se refiere a todos los formatos de archivos que se aprecia en la figura 9.



```
C:\Users\carop\Desktop\PhotoRec\testdisk-7.1-WIP\photorec_win.exe
PhotoRec 7.1-WIP, Data Recovery Utility, January 2018
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

1 P HPFS - NTFS          0 128 1  949 59 6  15241344 [CAROP]

Please choose if all space needs to be analysed:
[ _ Free _ ] Scan for file from NTFS unallocated space only
> [ Whole ] Extract files from whole partition
```

Figura 9 Selección de tipos de archivos a recuperar

D. Seleccionar la ubicación de salida

Finalmente seleccionar el directorio de salida y continuar como se presenta en la figura 10.

```

C:\Users\carop\Desktop\PhotoRec\testdisk-7.1-WIP\photorec_win.exe
PhotoRec 7.1-WIP, Data Recovery Utility, January 2018

Please select a destination to save the recovered files to.
Do not choose to write the files to the same partition they were stored on.
Keys: Arrow keys to select another directory
      C when the destination is correct
      Q to quit
Directory C:\Users\carop\Desktop\PhotoRec\testdisk-7.1-WIP
>drwx----- 197609 197609      0 21-Feb-2018 00:36 .
drwx----- 197609 197609      0 21-Jan-2018 23:42 ..
drwx----- 197609 197609      0 2-Feb-2018 00:25 63
drwx----- 197609 197609      0 21-Jan-2018 23:44 platforms
-rwx----- 197609 197609     220 8-Jan-2018 19:20 AUTHORS.txt
-rwx----- 197609 197609    18326 8-Jan-2018 19:20 COPYING.txt
-rwx----- 197609 197609     117 24-Dec-2017 15:21 INFO
-rwx----- 197609 197609    19026 8-Jan-2018 19:20 NEWS.txt
-rwx----- 197609 197609   5004393 29-Nov-2017 00:21 Qt5Core.dll
-rwx----- 197609 197609   4512524 29-Nov-2017 00:21 Qt5Gui.dll
-rwx----- 197609 197609   5855185 29-Nov-2017 00:21 Qt5Widgets.dll
-rwx----- 197609 197609     350 8-Jan-2018 19:20 THANKS.txt
-rwx----- 197609 197609      38 8-Jan-2018 19:20 VERSION.txt
-rwx----- 197609 197609   4460160 25-Nov-2016 07:20 cygwf-2.dll
-rwx----- 197609 197609   1089410 5-Dec-2017 01:01 cyggcc_s-seh-1.dll
-rwx----- 197609 197609   1411628 5-Dec-2017 07:18 cygiconv-2.dll
-rwx----- 197609 197609   414751 25-Nov-2016 07:19 cygjpeg-8.dll
-rwx----- 197609 197609   3397952 5-Dec-2017 08:03 cygncursesw-10.dll
-rwx----- 197609 197609   116053 5-Dec-2017 01:01 cygssp-0.dll
-rwx----- 197609 197609   3150128 5-Dec-2017 06:01 cygwin1.dll
-rwx----- 197609 197609    351821 5-Dec-2017 07:12 cygz.dll

Next

```

Figura 10 Directorio de salida

Adroit photo Recovery: Es una herramienta para recuperar imágenes de diferentes formatos que han sido fragmentadas y se basa en la técnica fragment recovery carving. La aplicación permite seleccionar la unidad a escanear y ver información sobre ella, como unidad, tipo, tamaño, nombres de volumen, sistema de archivos y tiempo estimado (Humphries, Suzanne;, 2017).

2.7.2.2 Proceso de recuperación de datos utilizando Adroit Photo Recovery en el sistema operativo Windows 7

A. Seleccionar el dispositivo a recuperar

En la figura 11 se presentan los dispositivos reconocidos para el análisis.

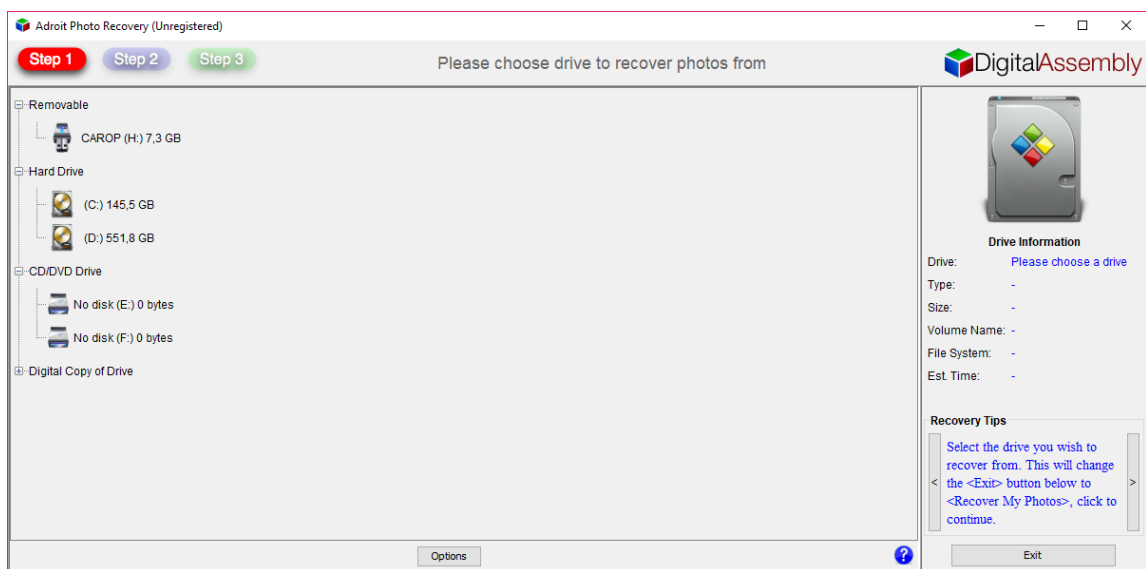


Figura 11 Adroit Photo Recovery selección de dispositivo

B. Iniciar el análisis del dispositivo

Como se presenta en la figura 12 el análisis está en proceso, y se debe esperar su finalización.

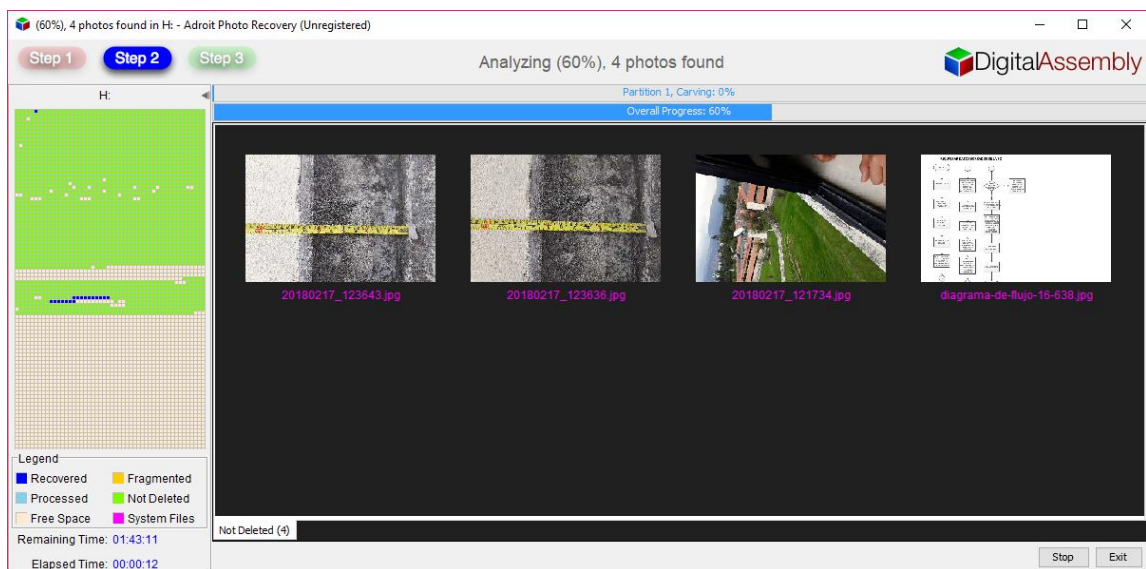


Figura 12 PhotoRec ejecución de software

CAPÍTULO III

METODOLOGÍA DE RECUPERACIÓN DE INFORMACIÓN

Actualmente, no existe definida una metodología o estándar para el proceso de recuperación de información ya sea de forma personal o en pericia. El principal objetivo es recuperar mayor cantidad de información de forma íntegra. (Pérez García, 2011) realizó una propuesta de metodología aplicada a los dispositivos de almacenamiento HDD y consta de 7 etapas como se aprecia en la figura 13.

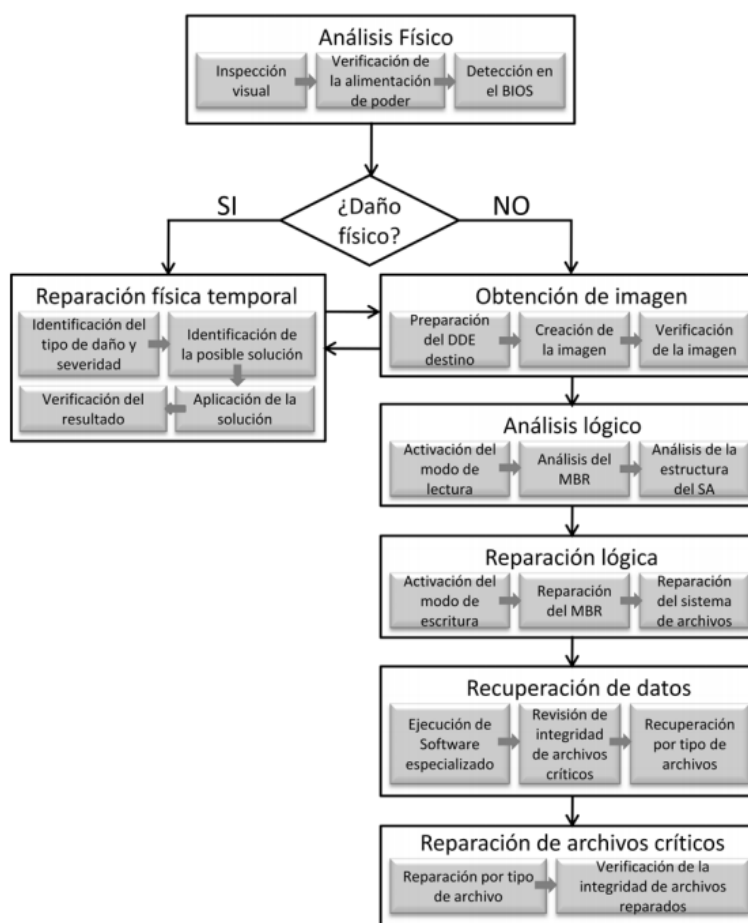


Figura 13 Metodología de recuperación de información para dispositivos HDD

Fuente: (Pérez García, 2011)

Esta investigación se basará en la metodología propuesta y será adaptada a los dispositivos de almacenamiento SSD, basándose en las mejores prácticas que utilizan las grandes y reconocidas empresas especializadas en la recuperación de información.

La metodología propuesta para los dispositivos SSD está compuesta por 5 etapas con diferentes fases cada una, cómo se puede apreciar en la Figura 14, que parte del análisis físico y pasa por la recuperación física temporal en caso de existir daño físico, luego se obtiene la imagen y se verifica si existe daño lógico, finalizando con el proceso de recuperación de datos con software específico sobre la imagen del dispositivo SSD a ser recuperado.

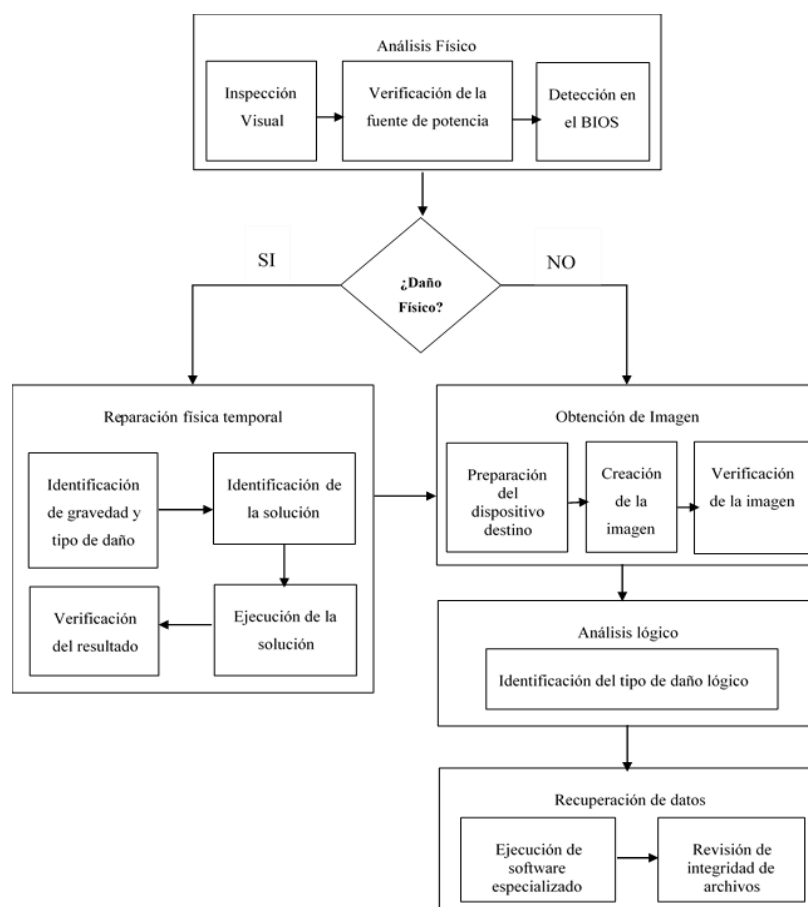


Figura 14 Metodología para recuperar información
Fuente: (Pérez García, 2011)

A continuación, se detallan cada una de las etapas y fases que conforman la metodología seleccionada.

3.1 Análisis físico

En esta etapa se realiza una inspección física del dispositivo SSD con el objetivo de evitar un mayor daño y cuenta con 3 fases que se indican en la Figura 15.

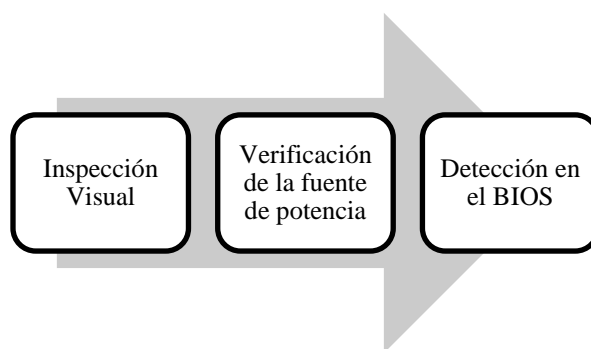


Figura 15 Fases de análisis físico
Fuente: (Pérez García, 2011)

3.1.1 Inspección Visual

En la primera fase se realiza una inspección visual de los componentes para verificar la existencia o no de un daño en los mismos. Se recomienda separar las tapas del dispositivo SSD con su tarjeta lógica para tener un mejor visón de los circuitos integrados, ya que podrían encontrarse desoldados, rotos, mojados o con quemaduras.

3.1.2 Verificación de la fuente de potencia

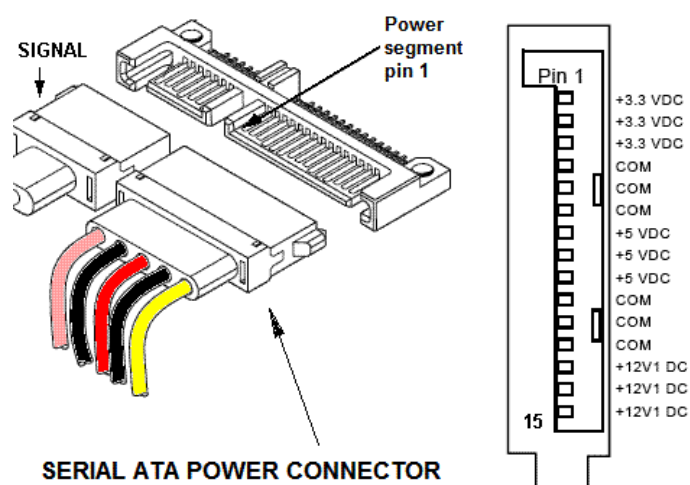
La segunda fase de esta etapa es verificar que la alimentación de poder sea la correcta para cada pin del dispositivo SSD de tipo SATA que se indica en la tabla 9, con la ayuda de un multímetro.

Tabla 9*Descripción de pines dispositivo SATA*

# PIN	FUNCIÓN-
1	3.3 V
2	3.3 V
3	3.3 V
4	Tierra
5	Tierra
6	Tierra
7	5 V
8	5 V
9	5 V
10	Tierra
11	Giro / Dispositivos IDE
12	Tierra
13	12 V
14	12 V
15	12 V

Fuente: (Pérez García, 2011)

Para conocer si el voltaje sobre el dispositivo SSD es el correcto se mide desde el pin con voltaje 3.3 V que son el pin 1,2 y 3, como se aprecia en la Figura 16.

**Figura 16** Distribución de pines de un disco duro-SATA

Fuente: (Nimlotx, 2013)

3.1.3 Detección en el BIOS (Sistema básico de entrada/ salida)

Los dispositivos SSD con sus características; modelo, capacidad y marca, deben ser reconocidos en el BIOS de los ordenadores, que están destinados a la recuperación de información. En la tabla 10 se presentan los síntomas que indican la presencia de daños físicos:

Tabla 10

Síntomas de daños físicos

Síntomas de daños físicos
Componente con un daño visible
Tiene variaciones de voltaje o es nulo
No se reconoce en el BIOS
Arranque es intermitente (lectura/escritura)
Existen sectores defectuosos o dañados.
Algunos de los componentes se sobrecalientan

Fuente: (Pérez García, 2011)

En caso de que el dispositivo SSD no presente ninguno de los daños físicos presentados, se continúa en la etapa 3 (Obtención de imagen).

3.2 Reparación física temporal

Las reparaciones aplicadas a los dispositivos SSD son de forma temporal, ya que con la manipulación se podría alterar las condiciones de funcionamiento. En la Figura 17 se puede apreciar las fases de esta etapa, que son las encargadas de planear los procedimientos para una reparación temporal, acorde al tipo de daño identificado y su gravedad.

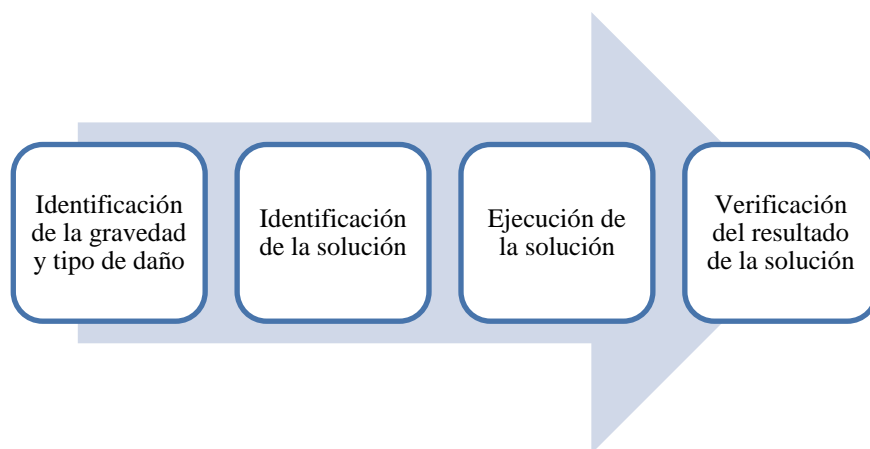


Figura 17 Fases de la reparación física temporal
Fuente: (Pérez García, 2011)

3.2.1 Identificación de la gravedad y tipo de daño

En esta fase se toman en cuenta los síntomas que presenta el dispositivo de almacenamiento SSD detallados en la tabla 10, estos síntomas podrían afectar a un elemento y este causar daños más severos a otros elementos.

3.2.2 Identificación de la posible solución

Basándose en el daño encontrado en el dispositivo SSD, se debe realizar un plan de la posible o posibles soluciones, considerando tanto herramientas físicas como de software que se requieran.

3.2.3 Ejecución de la solución

En esta fase se aplica la solución definida anteriormente, las soluciones se deben probar hasta que el dispositivo SSD funcione y sea reconocido en el BIOS, luego de la aplicación de la solución los dispositivos ya no son confiables para su uso.

3.2.4 Verificación del resultado de la solución

Al finalizar la reparación temporal del dispositivo SSD, se debe conectar al ordenador disponible para las pruebas y se pasa a la siguiente etapa que es la obtención de la imagen. En el caso de que no se tenga acceso al dispositivo SSD se determina que no es posible recuperar la información, finalizando la metodología en esta etapa.

3.3 Obtención de imagen

La etapa de obtención de imagen del dispositivo SSD es necesaria para disminuir la pérdida de datos, ya que los dispositivos reparados es posible que el SSD se ejecute una sola vez más sin que la información haya sido recuperada o extraída. Es necesario obtener al menos 2 imágenes y almacenarlas en dispositivos que previamente se haya verificado su correcto funcionamiento, la primera imagen obtenida corresponde al SSD original y la segunda imagen obtenida se realiza de la imagen obtenida. Esta etapa consta de 3 fases detalladas en la Figura 18.

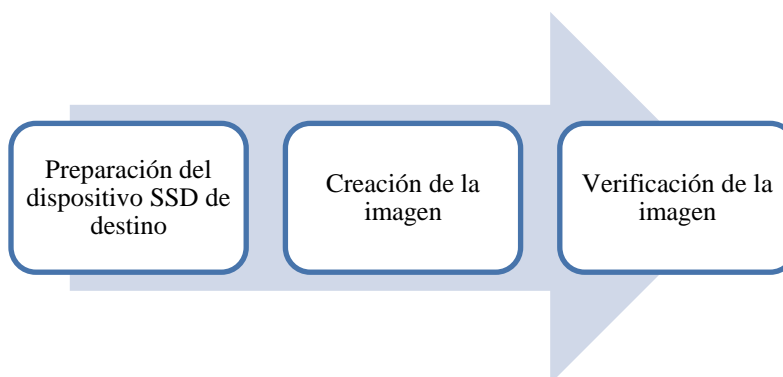


Figura 18 Fases de la obtención de imagen

Fuente: (Pérez García, 2011)

3.3.1 Preparación del dispositivo SSD de destino

El dispositivo SSD de destino debe tener al menos la misma capacidad o mayor que el dispositivo SSD dañado y luego debe ser sanitizado, este proceso consiste en llenar todos los sectores del SSD con código 0x00 para evitar mezclar la información se sobrescriba en el

dispositivo. Existe una herramienta en Windows que permite realizar este proceso y es WinHex, y en Kali Linux se tiene la herramienta de administración de discos, es necesario tener las precauciones suficientes para evitar más daños en el dispositivo original.

3.3.2 Creación de la imagen

Existen diversas herramientas para este proceso que se pueden utilizar como lo es WinHex, Clonezilla, ByteBack, FTK Imager, entre otras.

3.3.3 Verificación de la imagen

Al finalizar la creación de la imagen se debe obtener un código hash que es un algoritmo matemático que toma cualquier bloque de datos en este caso la imagen obtenida y lo transforma en una nueva serie de caracteres con una longitud fija (Kaspersky, 2017).

Si al generar un hash de la imagen del dispositivo SSD, y si algún archivo o tan solo un byte han sido alterados, cambiados o eliminados, el hash obtenido ya no será el mismo que el hash generado inicialmente. Existen varias herramientas que permiten realizar este proceso que son: WinMD5, MD5sum.

3.4 Análisis lógico

Para determinar si el dispositivo tiene algún tipo de daño lógico se procede a identificar en la tabla 11 los principales daños lógicos que podrían llegar a tener los dispositivos de almacenamiento SSD.

Tabla 11*Principales daños lógicos*

Daño	Síntoma
Estructura del MBR/EBR corrupta	El SO no inicia
Sistema de archivos corruptos	La unidad lógica no es reconocida por el SO propio o por ningún SO externo. Pantalla azul con mensaje de error
Archivos corruptos	
Borrado de archivos	Archivos faltantes
Formateo	La unidad lógica se visualiza como nueva
Reparticionamiento	
Sobreescritura parcial/total	El SO no inicia o los archivos no pueden ser abiertos conteniendo código parcialmente o totalmente ilegible

Fuente: (Pérez García, 2011)

Una vez identificado el tipo de daño lógico que tiene el dispositivo SSD se continúa con la siguiente etapa que es la recuperación de datos tomando en cuenta el software necesario.

3.5 Recuperación de datos

En esta etapa se procede a la recuperación de información utilizando el software especializado para cada archivo, en esta investigación se utilizarán herramientas de las técnicas File Carving que cuenta con las fases indicadas en la Figura 19.

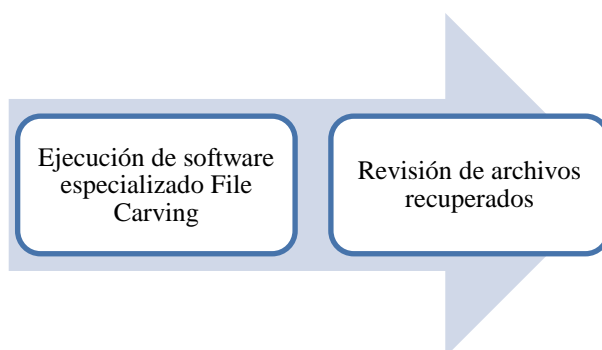


Figura 19 Fases de la recuperación de datos

Fuente: (Pérez García, 2011)

3.5.1 Ejecución de software especializado File Carving

Existen diferentes herramientas que utilizan técnicas File Carving que harán posible el desarrollo de esta fase que pueden ser herramientas de recuperación de datos para todos los archivos como Foremost y Scalpel, que recuperan los archivos de cualquier extensión, mientras que existen otras herramientas que son especializadas para cada tipo de archivo como lo son PhotoRec, Adroit Photo Recovery que son utilizadas únicamente en la recuperación de imágenes de cualquier extensión.

3.5.2 Revisión de archivos recuperados

En esta fase se revisa que por cada herramienta utilizada se haya recuperado información y se debe llenar un cuadro identificando las métricas que indica la recuperación de datos utilizando las técnicas File Carving como se muestra en la tabla 12.

Tabla 12*Métricas de las técnicas File Carving*

Métrica	Descripción
Cantidad de archivos recuperados	Cantidad total de archivos recuperados sean válidos, parcialmente válidos y falsos positivos
Cantidad de archivos válidos recuperados	Son los archivos que se recuperaron de forma íntegra.
Cantidad de falsos o negativos (Ofimática) o parcialmente recuperados(Multimedia)	Archivos que han sido recuperados, pero no se abren o se encuentran parcialmente recuperados.

Fuente: (Constanzo & Waimann, 2012)

Finalizando esta etapa se debe generar un reporte por cada dispositivo que se vea sometido a una recuperación de datos para conocer a detalle lo sucedido durante este proceso y tomar las acciones necesarias.

CAPÍTULO VI

DESARROLLO DEL PROYECTO

4.1 Aplicación de encuesta

Para preparar los escenarios en los cuales se realizará la experimentación se debe determinar una selección de las causas más comunes por los cuales se daña un dispositivo de almacenamiento cuya información se ha visto afectada. Se ha podido preparar los escenarios luego de aplicar una encuesta (Anexo 1) cuyo proceso se detalla a continuación:

4.1.1 Selección del tamaño del segmento

El tamaño de segmento servirá como universo de estudio para realizar el levantamiento de la información para conocer los factores más comunes de los daños en disco duros.

En la tabla 13 se detalla la selección del tamaño de segmento de personas a las que se aplicará la encuesta.

Tabla 13

Tamaño del segmento meta

DESCRIPCIÓN	TAMAÑO DEL SEGMENTO
Estudiantes de la Universidad de las Fuerzas Armadas ESPE	20.200
Estudiantes de la Universidad de las Fuerzas Armadas ESPE Pregrado	19.000
Estudiantes del departamento de Ciencias de la Computación de la Universidad de las Fuerzas Armadas ESPE	500
Estudiantes del departamento de Ciencias de la Computación de la Universidad de las Fuerzas Armadas ESPE de 5to a 9no nivel	138
Tamaño del Segmento Meta	138

Fuente:

Universidad de las Fuerzas Armadas ESPE

4.1.2 Determinación de la muestra

Para la determinación del tamaño de la muestra es necesario cumplir la siguiente fórmula cuyos valores serán descritos en la tabla 14.

$$n = \frac{z^2 * P * Q * N}{e^2 (N - 1) + z^2 * P * Q}$$

Tabla 14

Tamaño de la muestra

n	Tamaño de la muestra
Z	Margen de confiabilidad (equivale a un nivel de confianza, aproximado del 96%)
P (Por calcular)	Probabilidad de aceptación sobre conocer los factores más comunes causantes de daños en los discos duros o dispositivos de almacenamiento.
Q (Por calcular)	Probabilidad de no aceptación sobre conocer los factores más comunes causantes de daños en los discos duros o dispositivos de almacenamiento.
E	Error de muestreo (5%)
N	Tamaño del segmento meta
N-1	Factor, población menos 1

Los valores P y Q al ser la probabilidad de éxito y fracaso en la investigación se determinan para asegurar la confiabilidad de los datos recolectados con la muestra, donde se realizó una prueba piloto que consta de una sola pregunta encuestando al 20% de la población y el procedimiento es el siguiente:

4.1.3 Determinación de la pregunta de la prueba piloto

¿Le gustaría conocer cuáles son los factores más comunes por los que se daña un disco duro o dispositivo de almacenamiento?

SI_____

NO_____

4.1.4 Tabulación de los resultados

La prueba piloto se realizó a 21 personas y los resultados obtenidos son los que se muestran en la Figura 20:



Figura 20 Tabulación prueba piloto

Los valores de probabilidad de éxito y fracaso se obtienen como se indica en la tabla 15, considerando los resultados positivos de la frecuencia relativa como el valor de P y a los resultados negativos como el valor de Q.

Tabla 15*Resultados de la prueba piloto*

	Frecuencia	Frecuencia Relativa
SI	19	0.9048
NO	2	0.0952
Total	21	1

En la tabla 16 se presentan los valores que serán utilizados en la fórmula anterior y se procede al cálculo de la muestra:

Tabla 16*Valores para calcular el tamaño de la muestra*

n	Valor
Z	1.96
P	0.9048
Q	0.0952
E	0.05
N	138
N-1	137

$$n = \frac{z^2 * P * Q * N}{e^2 (N - 1) + z^2 * P * Q} \quad ; \quad n = \frac{1.96^2 * 0.9048 * 0.0952 * 138}{0.5^2 * 137 + 1.96^2 * 0.9048 * 0.0952}$$

$$n = \frac{45.665}{0.673} \quad ; \quad n = 68$$

El valor de la muestra da como resultado 68 personas, que son el número de encuestas a ser aplicadas entre los estudiantes de 5to a 9no nivel del departamento de Ciencias de la Computación de la Universidad de las Fuerzas Armadas ESPE.

4.1.5 Procesamiento de datos

En esta fase se presentan los resultados que se obtuvieron luego de realizada la encuesta (Anexo 2) para la investigación: “Estudio comparativo de técnicas File Carving para la recuperación de

información perdida por daños de impacto y humedad en dispositivos de almacenamiento SSD”, a continuación, para obtener una mejor comprensión de los resultados de la encuesta describiremos cada pregunta con su resultado y el gráfico respectivo.

PREGUNTA N° 1

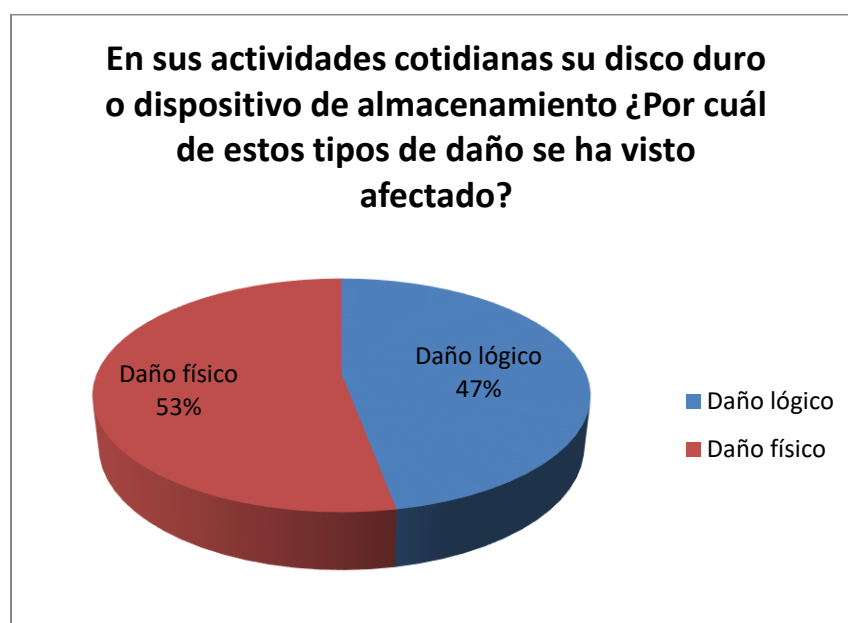


Figura 21 Encuesta, pregunta 1

Los resultados de la pregunta 1, nos permite conocer el porcentaje de estudiantes que se han visto afectados por daño en su disco duro o dispositivo de almacenamiento de los cuales el 53 % se han visto afectados por daños físicos mientras que el 47 % se han visto afectados por daños lógicos, por lo que se puede apreciar que no existe una diferencia marcada entre los daños físicos y lógicos sin embargo prevalecen los daños físicos.

PREGUNTA N° 2

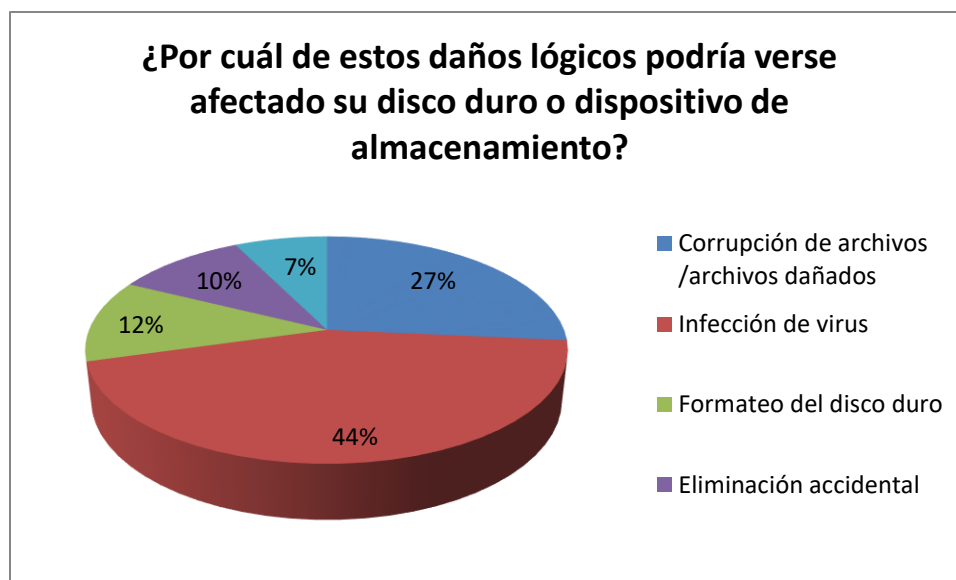


Figura 22 Encuesta, pregunta 2

Los resultados que se obtuvieron en esta pregunta nos permiten identificar que el mayor daño lógico que ha afectado a los discos duros o dispositivos de almacenamiento son los causados por Infección de virus con un 44% de los estudiantes encuestados, siguiendo en el porcentaje con un 27% la corrupción o archivos dañados, además el 12% se han visto afectados por los formateos del disco duro, el 10% se han visto afectados por eliminación accidental de sus datos, finalmente el 7% de los estudiantes ha manifestado que han tenido un mal funcionamiento del sistema operativo.

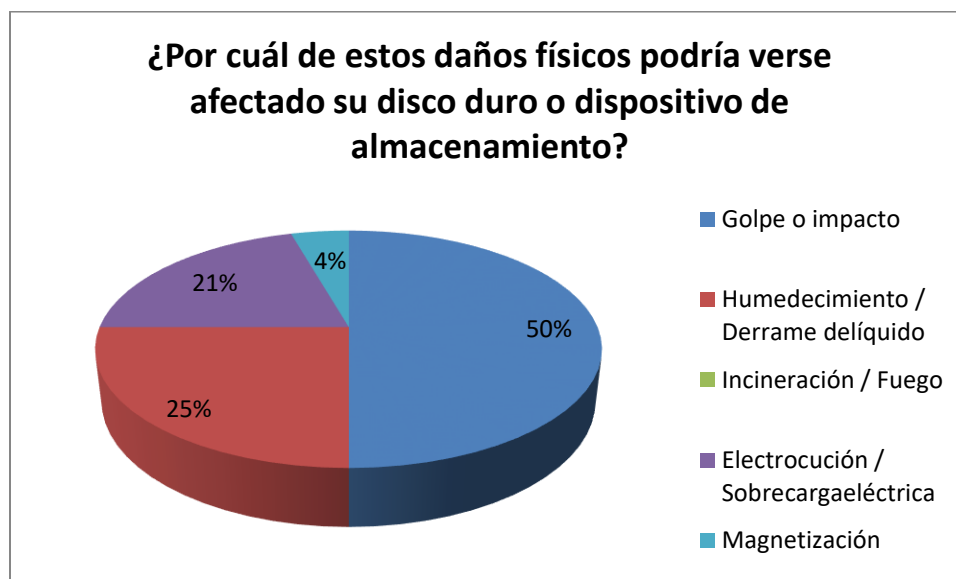
PREGUNTA N° 3

Figura 23 Encuesta, pregunta 3

Dentro de la afectación física de los discos duros o dispositivos de almacenamiento podemos observar que el 50% de los encuestados han sufrido estos daños a causa de golpes o impactos, mientras que el 25% han sufrido daños por humedecimiento o derrame de líquidos siendo esta la segunda causa con porcentajes altos de daños. Otro porcentaje considerable de daño físico es el de electrocuación o sobrecarga eléctrica con un 21%, finalmente e 4,4% de los estudiantes sufrieron daños por magnetización. En la encuesta realizada los estudiantes no han manifestado que sus discos duros o dispositivos de almacenamiento han sufrido daños físicos por incineración o fuego.

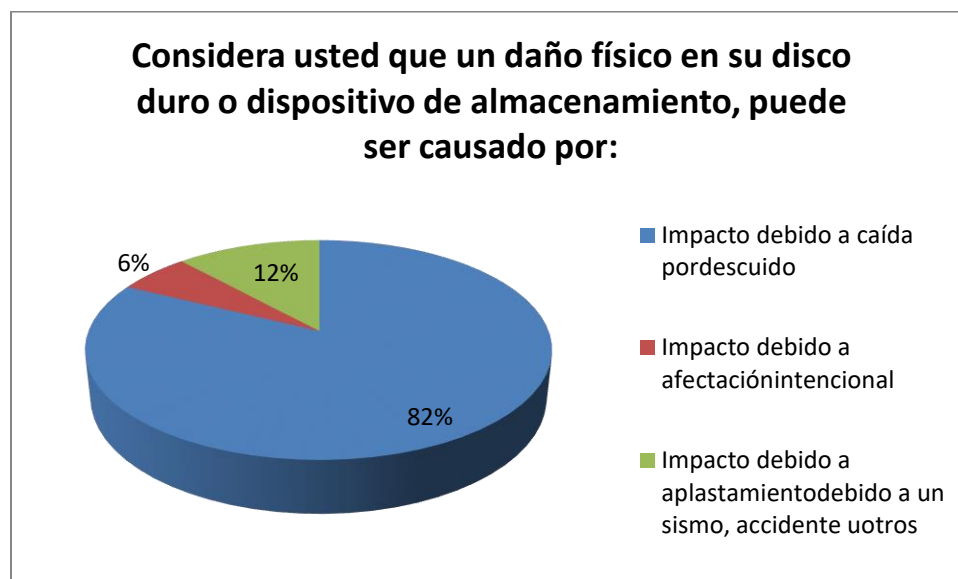
PREGUNTA N° 4

Figura 24 Encuesta, pregunta 4

Es evidente identificar que el 82% de los estudiantes encuestados han sufrido daños en sus discos duros por caídas a causa de un descuido, siendo este factor como el más común de las causas de los daños físicos. El 12% de encuestados considera que los daños físicos en sus discos duros son causados por impacto debido a aplastamiento debido a sismo, accidente u otros. Finalmente, el 6% de estudiantes manifiesta que los daños físicos en sus discos duro o dispositivos de almacenamiento a causa de impacto debido a afectación intencional, es decir para tratar de desaparecer evidencia comprometedoras o de algún delito no ha sido un factor por el cual se han visto afectados en gran medida.

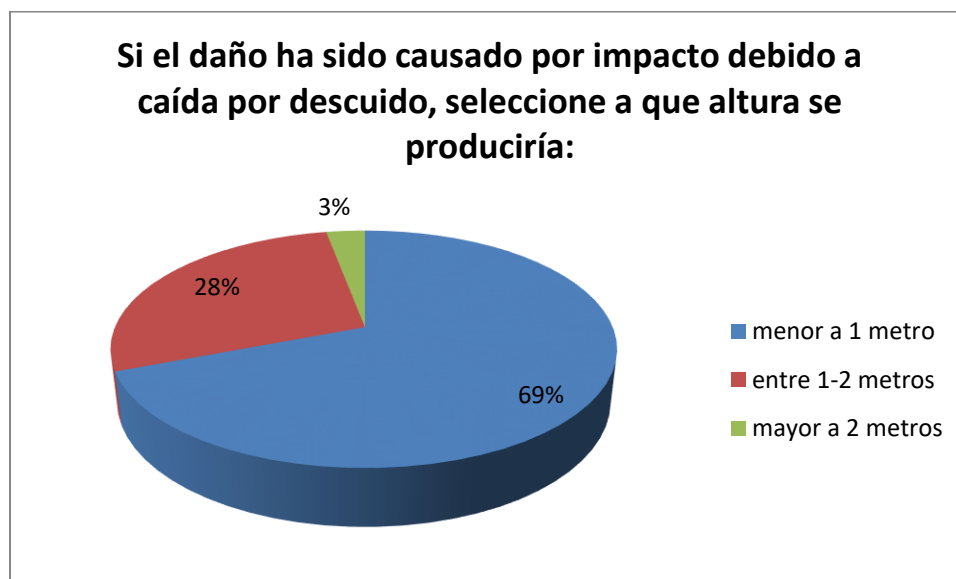
PREGUNTA N° 5

Figura 25 Encuesta, pregunta 5

Los resultados obtenidos en la pregunta 5 presenta un alto porcentaje de 69% de daños causados por impacto por descuido cuya altura de caída menor a un metro que representa la caída de un escritorio, mesa, mueble, entre otros. El 28% considera que los daños causados por descuido pueden haber sido a una altura de entre 1 a 2 a causa de caída de un archivador o librero. Finalmente, el 3% de daños a causa de una caída mayor que 2 metros es decir una caída desde una planta superior de algún tipo de edificación o de escaleras.

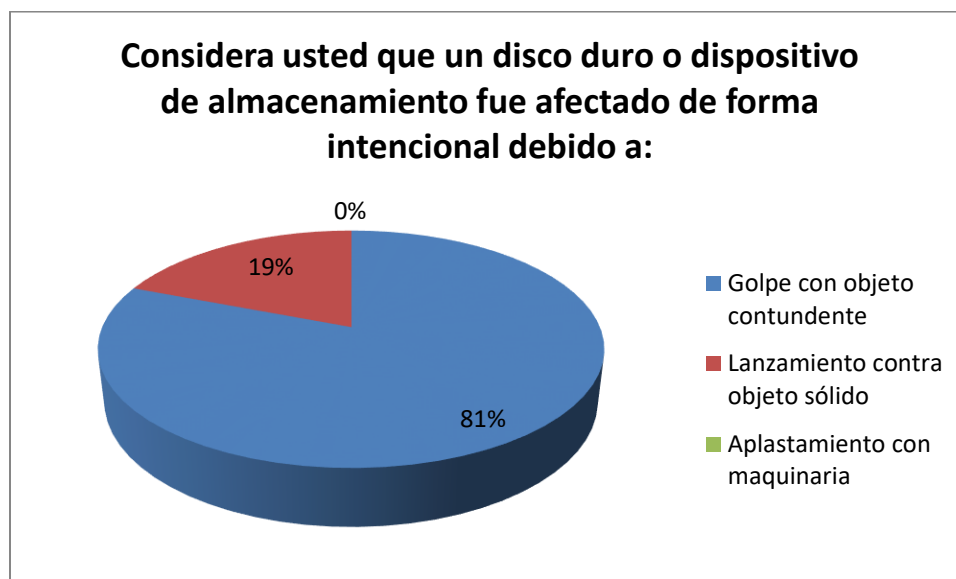
PREGUNTA N° 6

Figura 26 Encuesta, pregunta 6

En los resultados de la pregunta 6 se brinda una perspectiva que los daños de un disco duro o dispositivo de almacenamiento han sido causados por golpe con objeto contundente como martillo, palo, piedra, entre otros, con un porcentaje de 81%, y apenas el 19% considera que los daños en discos duros de forma intencional son provocados con lanzamiento contra objetos sólidos, mientras que los discos duros de los estudiantes encuestados no se han visto afectados por aplastamientos con maquinaria.

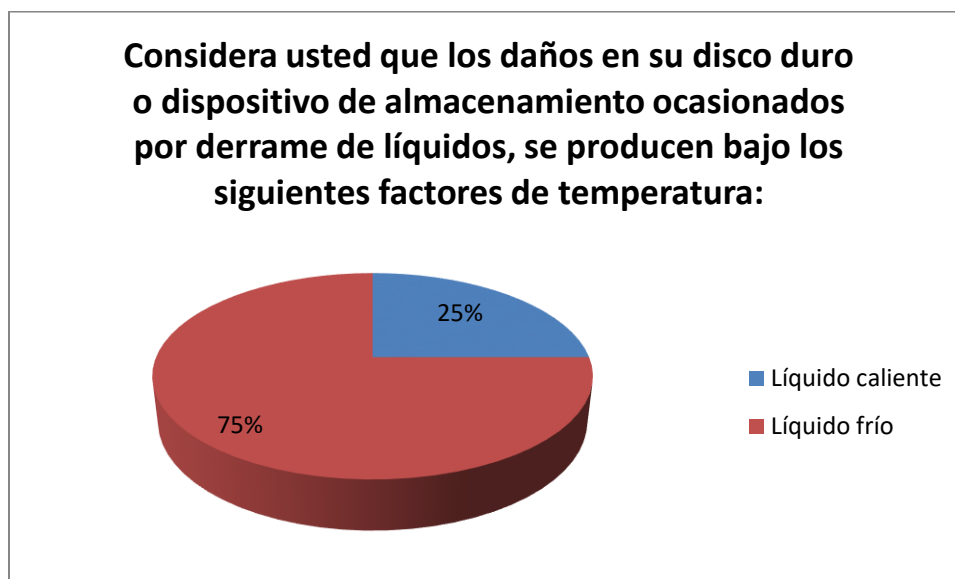
PREGUNTA N° 7

Figura 27 Encuesta, pregunta 7

Al analizar la pregunta 7, donde se considera que los daños en los discos duros o dispositivos de almacenamiento causados por derrame líquidos se producen en condiciones de líquidos fríos en un 75%, mientras que el 25% se producen en condiciones de líquidos calientes.

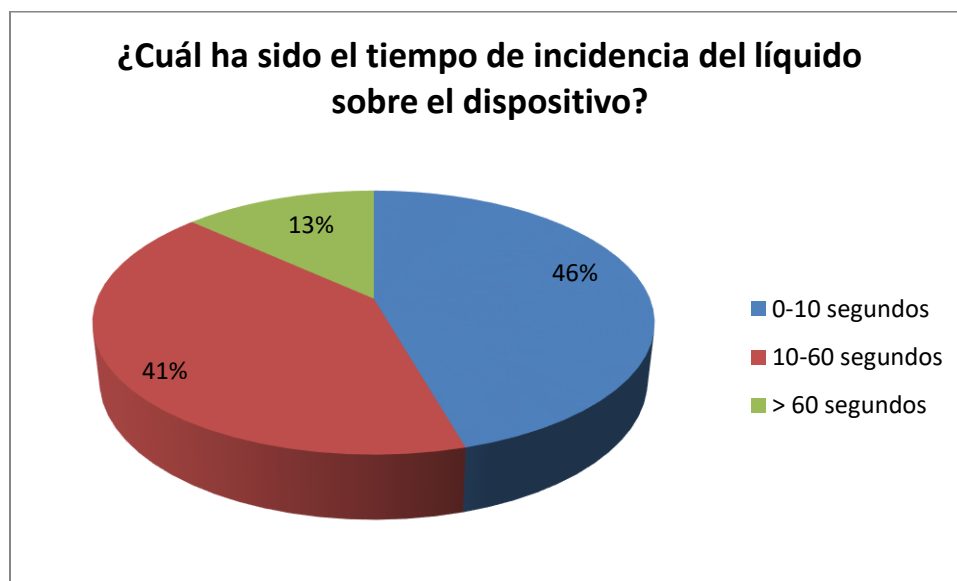
PREGUNTA N° 8

Figura 28 Encuesta, pregunta 8

Los resultados de la pregunta 8 señalan que el 46% de encuestados indican que el tiempo de incidencia del líquido sobre el dispositivo ha sido entre 0 y 10 segundos. El 41% indica que se ha visto afectado entre 10 y 60 segundos, finalmente el 13% se ha visto afectado por incidencia del líquido por más de 60 segundos.

PREGUNTA N° 9

Figura 29 Encuesta, pregunta 9

De los resultados de esta pregunta podemos observar que el 55% de los dispositivos de almacenamiento de los estudiantes que han sido encuestados han podido recuperar la información de forma parcial, después de que sus dispositivos han sufrido algún golpe o impacto, seguido de un 35% que ha podido recuperar la información mínimamente y apenas el 10% ha recuperado la información por completo.

PREGUNTA N° 10

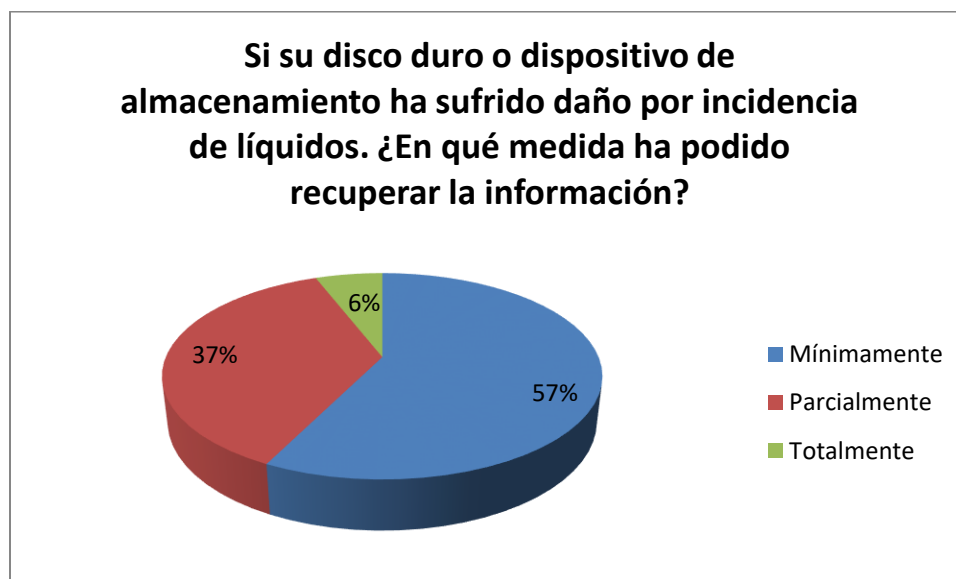


Figura 30 Encuesta, pregunta 10

De los resultados de esta pregunta podemos observar que el 57% de discos duros que han sufrido daño por incidencia de líquidos han podido recuperar la información de forma mínima, seguido de un 37% que ha podido recuperar la información parcialmente y apenas el 6% ha recuperado la información por completo.

Al finalizar esta encuesta se ha determinado los escenarios en los que los dispositivos de almacenamiento se han visto afectados que son:

4.2 Selección de los escenarios

4.2.1 Caída por descuido

Caída por descuido con un 82%, donde se toma en cuenta la altura de caída más frecuente por la que se ven más afectados que son las indicadas en la tabla 17:

Tabla 17*Escenarios caídas por descuido*

Altura	Escenario
Menor a 1 metro	Desde un escritorio o mesa que tiene un estándar de altura según (Uncomo, s.f.) de 70 a 74 cm
Entre 1 a 2 metros	(Plazola Cisneros, 2017) Indica que un stand o librero tiene un estándar de altura de 1.60 a 2.00 metros.

4.2.2 Escenario: Caída de forma intencional

Caída de forma intencional desde una altura superior a 2 metros que se presenta en las investigaciones forenses para destruir el dispositivo de almacenamiento y no tener acceso a la información.

4.2.3 Escenario: Golpe con objeto contundente de forma intencional

Según el estudio realizado, los golpes con objeto contundente han tenido una gran cantidad de casos con el 81%, que sucede en los casos de delitos informáticos al tratar de destruir un dispositivo de almacenamiento, hasta no tener acceso a la información, por lo que se debe medir la fuerza con la que el dispositivo sufre dichos daños.

4.2.4 Escenario: Aplastamientos de forma intencional

En el caso de investigaciones forenses los dispositivos de almacenamiento son destruidos de forma intencional al ser aplastados por vehículos, y el nivel de daño dependerá del tipo de vehículo por lo que se han considerado 3 tipos de vehículos que son livianos, medianos y pesados.

En la categoría livianos se tomó en cuenta al vehículo Aveo Family de 1.365 kg (Chevrolet, 2017) como se muestra en la Figura 31, cuyo motor y tracción se encuentran ubicados en la parte delantera del vehículo, en este caso se considera que la distribución del peso es de 60% para la parte delantera y 40% en la parte trasera obteniendo un peso por cada llanta delantera de 409,50 kg. La fuerza ejercida por una de las llantas delanteras se obtiene con la siguiente fórmula.

$$F = m * g$$

$$F = 409,50 \text{ kg} * 9,80665 \frac{\text{m}}{\text{s}^2}$$

$$F = 4.015,82 \text{ N}$$



Figura 31 Dimensiones vehículo liviano

Fuente: (Chevrolet, 2017)

En la categoría medianos se consideró al vehículo Ford Sport Track (Tecnoautos, 2017) con un peso de 1.939 kg como se muestra en la Figura 32, cuyo motor se encuentra ubicado en la parte delantera y la tracción en la parte trasera por lo que el peso total será distribuido 50% en la parte delantera y 50% en la parte trasera. De esta forma por cada llanta se tiene un peso de 484,75 kg. La fuerza ejercida por una de las llantas delanteras se obtiene con la siguiente fórmula.

$$F = m * g$$

$$F = 484,75 \text{ kg} * 9,80665 \frac{\text{m}}{\text{s}^2}$$

$$F = 4.753,77 \text{ N}$$



Figura 32 Vehículo mediano de referencia

Fuente: (Tecnoautos, 2017)

En la categoría de pesados se consideró a un camión FSR34N (Chevrolet-Trucks, 2017) con un peso de 3.815 kg, cuyo eje delantero tiene un peso de 2.370 kg como se aprecia en la figura 33, por lo que cada llanta delantera tendrá un peso de 1.185 kg. Donde la fuerza ejercida por una de las llantas delanteras se obtiene con la siguiente fórmula.

$$F = m * g$$

$$F = 1.185 \text{ kg} * 9,80665 \frac{\text{m}}{\text{s}^2}$$

$$F = 11.620,88 \text{ N}$$



Figura 33 Vehículo pesado de referencia
Fuente: (Chevrolet-Trucks, 2017)

4.2.5 Escenario: Humedecimiento

Los daños en los dispositivos de almacenamiento a causa del derrame de un líquido por agua fría han tenido mayor incidencia con un 75% que puede llegar a darse a causa de agua derramada sobre el ordenador ya sea de forma intencional o accidental con una temperatura promedio que va desde los 10°C y 22°C según (FlacsoAndes, 2012) que corresponde a la Ciudad de Quito, el tiempo de incidencia se considera el rango de:

- 0-10 segundos.
- 10-60 segundos.
- Más de 60 segundos.

4.3 Preparación de los escenarios

Para la preparación de los escenarios se ha utilizado 3 laboratorios en los que se realizará la experimentación, los laboratorios utilizados y sus materiales se detallan a continuación:

4.3.1 Laboratorio de ensayo de materiales / Dpt. Ciencias de la Tierra y Construcción

En este laboratorio se va a preparar el escenario en el caso de que un dispositivo de almacenamiento SSD se encuentre afectado de forma intencional a causa de aplastamiento de un vehículo de 3 tipos como se indicó en la sección 4.1.4. Para lo cual se necesita simular la fuerza de aplastamiento que los vehículos aplican sobre el dispositivo hasta destruirlos y que su información no pueda ser recuperada, utilizando la máquina de compresión simple cuyas unidades de fuerza se encuentran en Kilo Newtons y se aprecia en la Figura 34.



Figura 34 Máquina de compresión simple

Debido a que esta máquina utiliza medidas de Kilo Newtons se transformó las fuerzas de aplastamiento de referencia encontradas en cada categoría como se indica en a tabla 18.

Tabla 18

Escenarios forma intencional por aplastamiento

Vehículo	Fuerza de un eje Newton	Fuerza de un eje Kilo newton
Liviano	4.015,82 N	4,02 KN
Mediano	4.753,77 N	4,75 KN
Pesado	11.620,88 N	11,62 KN

4.3.2 Laboratorio de materiales / Dpt. Energía y Mecánica

En este laboratorio se va a utilizar la máquina de impacto como se aprecia en la Figura 35, para simular y determinar la fuerza de impacto con la que un dispositivo SSD se afecta de forma intencional con golpe con objeto contundente.



Figura 35 Máquina de impacto

4.3.3 Laboratorio de informática forense / Dpt. de Ciencias de la Computación

El siguiente escenario se ha obtenido de la encuesta realizada anteriormente donde se presenta un alto nivel de daños en dispositivos de almacenamiento de forma accidental por derrame de un líquido en agua fría.

Para el escenario más común determinado que es por caída accidental desde diferentes alturas se utilizará un flexómetro y los escritorios y libreros del laboratorio que cumplen con los estándares de altura para los muebles.

Finalmente, luego de realizar la experimentación para cada escenario descrito, en este laboratorio se procede a utilizar las herramientas y software necesario para la recuperación de información.

En cuanto al hardware a utilizar se cuenta con 3 computadoras con la información presentada en la tabla 19:

Tabla 19

Hardware utilizado

Código	Marca	Procesador	Memoria	Bios	Sistema Operativo	Capacidad
PC01	Maxtor STM325031	Intel Core i7	4 GB	DPP3510J.8 6A.0572.200 9.0715.2346	Windows 7/ Kali Linux	250 GB
PC02	WesternDigital/ WD- WMAT22342312	Intel Core i7	4 GB	R01-B3L	Kali Linux	160 GB
PC03	WesternDigital/ ABPKT- 75PK4T0	Intel Core i7	4 GB	A17	Windows 7/ Kali Linux	500 GB

El software utilizado se detalla en la tabla 20 conjuntamente a su versión.

Tabla 20

Software especializado

Software	Compatibilidad	Versión
Foremost	Kali Linux	V 1.5.7
Scalpel	Kali Linux	V 1.6
PhotoRec	Windows	V 7.1
Adroit Photo Recovery	Windows	V 27
CrystalDiskInfo	Windows	V 7.1.0
Clonezilla-Live	Kali-Linux	V 1.2.12
WinMD5	Windows	V 1.20
WinHex	Windows	V 18.1

4.4 Ejecutar la experimentación

En el caso de caída por descuido se debe considerar los datos y fórmulas de la Figura 36 que corresponden a la caída libre de objetos en física.

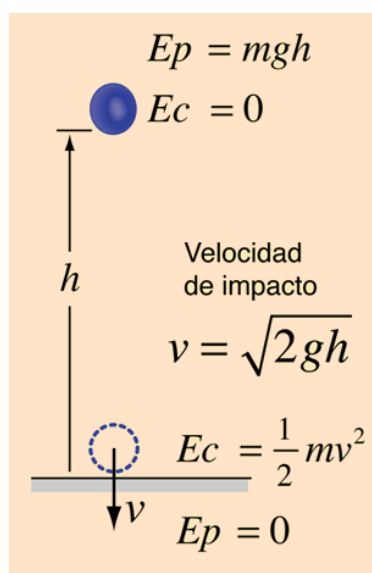


Figura 36 Fórmulas para cálculo de fuerza de impacto

Fuente: (Hyperphysics, 2017)

Energía potencial: es la energía capaz de generar un trabajo como consecuencia de la posición de un cuerpo.

$$Ep = m * g * h$$

Para el punto inicial la energía cinética es igual a 0, debido a que es la energía que posee por su movimiento, pero se encuentra en reposo.

Velocidad de impacto: Es la velocidad adquirida del objeto hasta el momento del impacto.

$$v = \sqrt{2gh}$$

En este punto la energía cinética y la energía potencial serán iguales para obtener la aceleración alcanzada utilizando una altura de rebote que es la distancia que viajó el objeto después del impacto.

$$Ep = Ec$$

$$m * a * h_r = \frac{1}{2} * m * v^2$$

$$a = \frac{v^2}{2h_r}$$

La fórmula para calcular la fuerza de impacto es: $F = m * a$

4.4.1 Escenario 1: Caída por descuido menor a 1 metro

A. Verificar la integridad del dispositivo SSD

Utilizando la herramienta CrystalDiskInfo como se observa en la Figura 37, el dispositivo SSD tiene un correcto rendimiento.

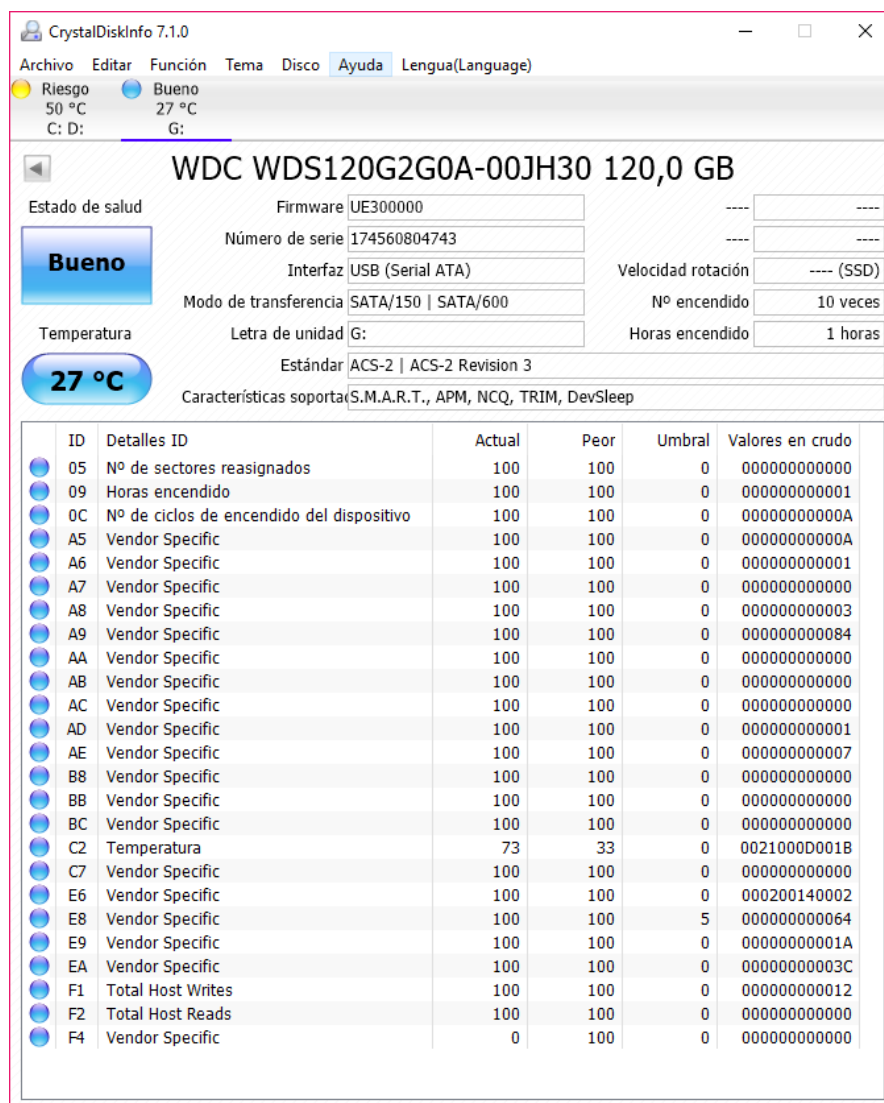


Figura 37 Estado inicial del SSD para el escenario 1

B. Pesar el dispositivo de almacenamiento SSD

Se coloca el dispositivo SSD sobre una balanza obteniendo un peso de 32 gramos.

C. Determinar la altura de caída

Se ubica al dispositivo de almacenamiento sobre un escritorio con una altura de 72.5 cm como se observa en la Figura 38.



Figura 38 Altura de escritorio

D. Dejar caer el dispositivo de almacenamiento SSD

Desde el borde del escritorio se deja caer al dispositivo sin velocidad inicial

E. Calcular la altura de rebote

Para los cálculos requeridos un valor importante a considerar es la altura de rebote que permitirá calcular la aceleración del objeto en este caso el dispositivo SSD con un valor de 10 cm como se aprecia en la Figura 39.

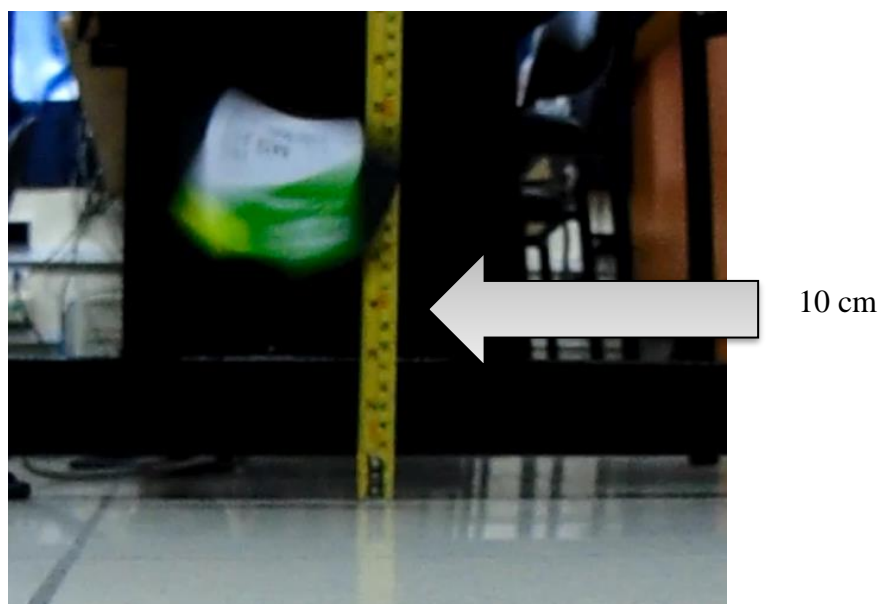


Figura 39 Altura de rebote

F. Calcular fuerza de impacto

En la tabla 21 se aprecian los valores necesarios para la aplicación de la fórmula de caída libre de un SSD: masa del objeto y la altura de caída, mientras que la gravedad se mantiene como un valor constante.

Tabla 21

Características del dispositivo SSD para el escenario 1

DATOS	UNIDADES	VALOR
Masa / m	kg	0,032
Altura / h	m	0,725
Gravedad / g	m/s ²	9,81

Energía Potencial

$$E_p = m * g * h$$

$$E_p = 0,032 \text{ kg} * 9,81 \frac{\text{m}}{\text{s}^2} * 0,725 \text{ m}$$

$$E_p = 0,23 \text{ N m}$$

Velocidad de Impacto

$$v = \sqrt{2gh}$$

$$v = \sqrt{2 * 9,81 \frac{\text{m}}{\text{s}^2} * 0,725 \text{ m}}$$

$$v = \sqrt{14,22 \frac{\text{m}^2}{\text{s}^2}}$$

$$v = 3,77 \frac{\text{m}}{\text{s}}$$

Aceleración

$$a = \frac{v^2}{2h_r}$$

$$a = \frac{(3,77 \frac{\text{m}}{\text{s}})^2}{2 * (0,1 \text{ m})}$$

$$a = 71,06 \frac{\text{m}^2}{\text{s}^2}$$

Fuerza de impacto

$$F = m * a$$

$$F = 0.032 \text{ kg} * 71,06 \frac{\text{m}^2}{\text{s}^2}$$

$$F = 2,27512 \text{ N}$$

Luego de conocer la fuerza de impacto del dispositivo SSD se procede a la recuperación de información siguiendo la metodología descrita en el capítulo 3 como se detalla a continuación:

4.4.1.1 Aplicación de la metodología para el escenario 1 con F= 2, 27512 Newtons

Capacidad de almacenamiento: 120 GB

Espacio utilizado: 19 GB

ETAPA 1: Análisis físico

En esta etapa inicia con la revisión de la estructura física del disco duro, para identificar los daños físicos visibles. Los resultados se visualizan en la tabla 22.

Tabla 22

Resultado análisis físico del SSD para el escenario 1

FASES	RESULTADO
Inspección visual	No se encontró indicios de golpes o abolladuras en el SSD, ni en sus componentes.
Verificación de la alimentación de poder	La energía eléctrica que debe recibir el dispositivo SSD es la correcta, sin generar problemas en la alimentación de poder.
Detección en el BIOS	El BIOS de la PC01 detectó al SSD con sus características correctas de marca y capacidad.

Al terminar esta etapa, se puede concluir que el dispositivo SSD no presenta ningún tipo de daño físico, pasando directamente a la etapa 3 que es la obtención de imagen.

ETAPA 3: Obtención de imagen

Se obtuvo una imagen completa del dispositivo SSD como se presenta en la tabla 23, donde se detalla las fases cumplidas.

Tabla 23

Resultado obtención imagen SSD para el escenario 1

FASES	RESULTADO
Preparación del SSD de destino	El dispositivo de destino cumple las mismas características del SSD que es marca WesternDigital de 120GB de almacenamiento.
Creación de la imagen	Se utilizó el software Clonezilla-Live que permitió hacer la copia completa del dispositivo SSD1
Verificación de la imagen	Se generó el hash MD5 para la imagen obtenida como se presenta en la Figura 40.

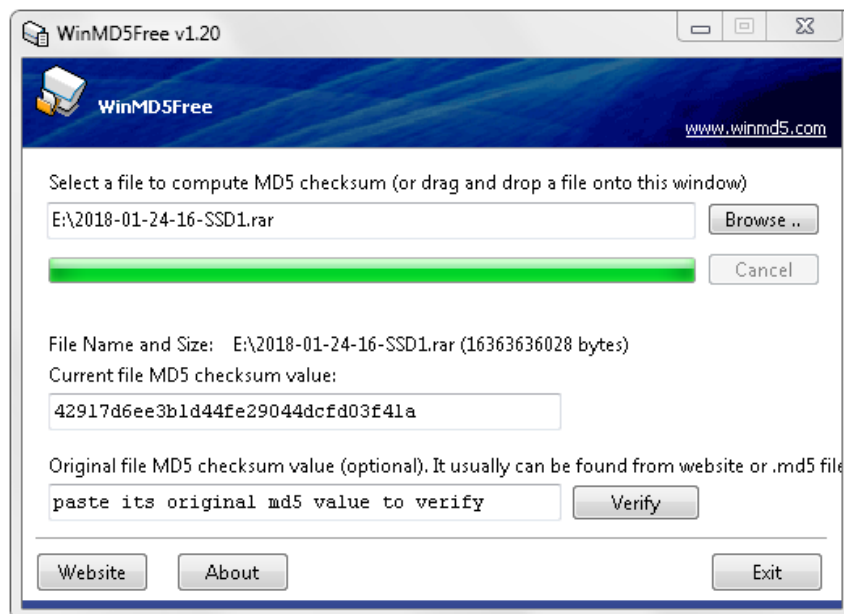


Figura 40 Hash md5 para el escenario 1

ETAPA 4: Análisis lógico

En la fase de verificación del tipo de daño lógico se basó en la tabla 11, y no se identificó ningún tipo de daño lógico por lo que se procede a continuar en la etapa 5 que es la recuperación de datos del dispositivo a pesar de que no presente ningún tipo de daño ni lógico ni físico.

ETAPA 5: Recuperación de datos

Para la recuperación de datos se utilizó 4 herramientas que son: Foremost/Scalpel para Linux y PhotoRec/Adroit Photo Recovery para Windows. Obteniendo los siguientes resultados para cada herramienta.

Foremost, recuperó un total de 24.647 archivos y se obtuvo la siguiente información por tipo de archivo como se indica en la Figura 41.

```
24647 FILES EXTRACTED

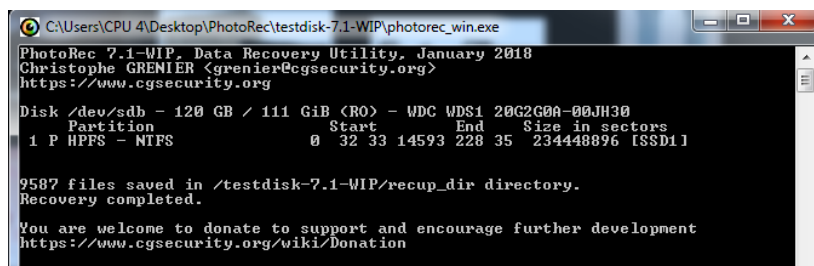
jpg:= 18363
gif:= 120
bmp:= 4
wmv:= 10
mov:= 13
rif:= 3
htm:= 19
ole:= 491
zip:= 1657
rar:= 70
exe:= 6
png:= 3718
pdf:= 173
```

Figura 41 Resultados foremost SSD para el escenario 1

Scalpel, recupero un total de 787 archivos y se obtuvo la siguiente información por tipo de archivo:

- Png: 178
- Jpg: 5
- Gif: 9
- Bmp: 2
- Mov: 393
- Htm: 52
- Zip: 92
- Mpg: 26
- Wpc: 4
- Doc: 9
- Avi: 10
- Art: 5
- Fws: 2

PhotoRec, ha recuperado un total de 9.587 archivos como se muestra en la Figura 42 y son detallados a continuación:



```
CAUsers\CPU 4\Desktop\PhotoRec\testdisk-7.1-WIP\photorec_win.exe
PhotoRec 7.1-WIP, Data Recovery Utility, January 2018
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk /dev/sdb - 120 GB / 111 GiB <RO> - WDC WDS1 20G2G0A-00JH30
Partition          Start          End      Size in sectors
 1 P HPFS - NTFS      0 32 33 14593 228 35 234448896 [SSD1]

9587 files saved in /testdisk-7.1-WIP/recup_dir directory.
Recovery completed.

You are welcome to donate to support and encourage further development
https://www.cgsecurity.org/wiki/Donation
```

Figura 42 Resultados PhotoRec SSD para el escenario 1

- Exe: 17
- Jar: 5
- Zip: 60
- Doc: 163
- Txt: 2.000
- Xml: 3
- Jpg: 7009
- Ppt: 5
- Html: 45
- Gif: 8
- Png: 1183
- Csv: 9
- Xlsx: 259

Adroit photo recovery, recupero un total de 37.375 imágenes de los cuales:

- Jpg: 31.274
- Bpm: 10
- Gif: 245
- Png: 5.846

4.3.2 Escenario 2: Caída por descuido entre 1 y 2 metros

A. Verificar la integridad del dispositivo SSD

Utilizando la herramienta CrystalDiskInfo como se observa en la Figura 43, el dispositivo SSD tiene un correcto rendimiento.

CrystalDiskInfo 7.1.0

Archivo Editar Función Tema Disco Ayuda Lengua(Language)

Riesgo 44 °C Buena 30 °C
C: D: G:

WDC WDS120G2G0A-00JH30 120,0 GB

Estado de salud **Bueno**

Firmware UE300000
Número de serie 174560805763
Interfaz USB (Serial ATA) Velocidad rotación ---- (SSD)
Modo de transferencia SATA/150 | SATA/600 Nº encendido 2 veces
Temperatura 30 °C Letra de unidad G: Horas encendido 2 horas
Estándar ACS-2 | ACS-2 Revision 3
Características soportadas S.M.A.R.T., APM, NCQ, TRIM, DevSleep

ID	Detalles ID	Actual	Peor	Umbral	Valores en crudo
05	Nº de sectores reasignados	100	100	0	000000000000
09	Horas encendido	100	100	0	000000000002
0C	Nº de ciclos de encendido del dispositivo	100	100	0	000000000002
A5	Vendor Specific	100	100	0	000000000006
A6	Vendor Specific	100	100	0	000000000001
A7	Vendor Specific	100	100	0	000000000000
A8	Vendor Specific	100	100	0	000000000000
A9	Vendor Specific	100	100	0	000000000056
AA	Vendor Specific	100	100	0	000000000000
AB	Vendor Specific	100	100	0	000000000000
AC	Vendor Specific	100	100	0	000000000000
AD	Vendor Specific	100	100	0	000000000001
AE	Vendor Specific	100	100	0	000000000000
B8	Vendor Specific	100	100	0	000000000000
BB	Vendor Specific	100	100	0	000000000000
BC	Vendor Specific	100	100	0	000000000000
C2	Temperatura	70	49	0	00310010001E
C7	Vendor Specific	100	100	0	000000000000
E6	Vendor Specific	100	100	0	000100140001
E8	Vendor Specific	100	100	5	000000000064
E9	Vendor Specific	100	100	0	00000000000F
EA	Vendor Specific	100	100	0	000000000025
F1	Total Host Writes	100	100	0	000000000012
F2	Total Host Reads	100	100	0	000000000000
F4	Vendor Specific	0	100	0	000000000000

Figura 43 Estado Inicial SSD para el escenario 2

B. Pesar el dispositivo de almacenamiento SSD

Se coloca el dispositivo SSD sobre una balanza obteniendo un peso de 32 gramos.

C. Determinar la altura de caída

Se ubica al dispositivo de almacenamiento sobre un estante con una altura de 1,65 m como se observa en la Figura 44.



Figura 44 Altura para el escenario 2

D. Dejar caer el dispositivo de almacenamiento SSD

Desde el borde de un estante y se deja caer al dispositivo sin velocidad inicial.

E. Calcular la altura de rebote

Para los cálculos requeridos un valor importante a considerar es la altura de rebote que permitirá calcular la aceleración del objeto en este caso el dispositivo SSD con un valor de 8 cm como se aprecia en la Figura 45.

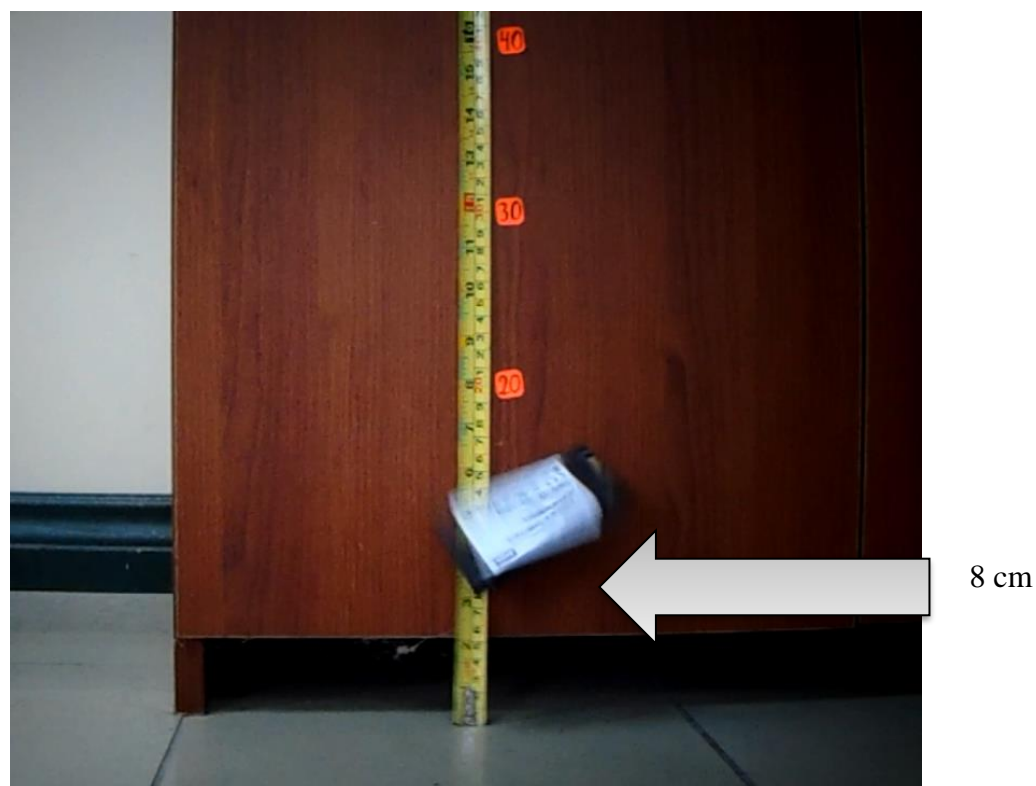


Figura 45 Altura de rebote escenario 2

F. Calcular fuerza de impacto

En la tabla 24 se aprecian los valores necesarios para la aplicación de la fórmula de caída libre de un SSD, tanto como la masa del objeto y la altura de caída, mientras que la gravedad se mantiene como un valor constante.

Tabla 24

Características del dispositivo SSD para el escenario 2

DATOS	UNIDADES	VALOR
Masa / m	kg	0,032
Altura / h	m	1,65
Gravedad / g	m/s ²	9,81

Energía Potencial

$$E_p = m * g * h$$

$$E_p = 0,032 \text{ kg} * 9,81 \frac{\text{m}}{\text{s}^2} * 1,65 \text{ m}$$

$$E_p = 0,52 \text{ N m}$$

Velocidad de Impacto

$$v = \sqrt{2gh}$$

$$v = \sqrt{2 * 9,81 \frac{\text{m}}{\text{s}^2} * 1,65 \text{ m}}$$

$$v = \sqrt{32,37 \frac{\text{m}^2}{\text{s}^2}}$$

$$v = 5,69 \frac{\text{m}}{\text{s}}$$

Aceleración

$$a = \frac{v^2}{2h_r}$$

$$a = \frac{(5,69 \frac{\text{m}}{\text{s}})^2}{2 * (0,08 \text{ m})}$$

$$a = 202,35 \frac{\text{m}^2}{\text{s}^2}$$

Fuerza de impacto

$$F = m * a$$

$$F = 0,032 \text{ kg} * 202,35 \frac{\text{m}^2}{\text{s}^2}$$

$$F = 6,48 \text{ N}$$

Luego de conocer la fuerza de impacto del dispositivo SSD se procede a la recuperación de información siguiendo la metodología descrita en capítulo 3 como se detalla a continuación:

4.3.2.1 Aplicación de la metodología para el escenario 2 con $F = 6,48$ Newtons

Capacidad de almacenamiento: 120 GB

Espacio utilizado: 17,9 GB

ETAPA 1: Análisis físico

En esta etapa inicia con la revisión de la estructura física del disco duro, para identificar los daños físicos visibles. Los resultados se visualizan en la tabla 25.

Tabla 25

Resultado análisis físico SSD para el escenario 2

FASES	RESULTADO
Inspección visual	No se encontró indicios de golpes o abolladuras en el SSD, ni en sus componentes.
Verificación de la alimentación de poder	La energía eléctrica que debe recibir el dispositivo SSD es la correcta, sin generar problemas en la alimentación de poder.
Detección en el BIOS	El BIOS de la PC01 detectó al SSD con sus características correctas de marca y capacidad.

Al terminar esta etapa, se puede concluir que el dispositivo SSD no presenta ningún tipo de daño físico, pasando directamente a la etapa 3 que es la obtención de imagen.

ETAPA 3: Obtención de imagen

Se obtuvo una imagen completa del dispositivo SSD, para continuar con la etapa 4 que es análisis lógico, en la tabla 26 se detalla las fases cumplidas.

Tabla 26

Resultado obtención imagen SSD para el escenario 2

FASES	RESULTADO
Preparación del SSD de destino	El dispositivo de destino cumple las mismas características del SSD que es marca WesternDigital de 120GB de almacenamiento.
Creación de la imagen	Se utilizó el software Clonezilla-Live que permitió hacer la copia completa del dispositivo SSD.
Verificación de la imagen	Se generó el hash MD5 para la imagen obtenida como se presenta en la Figura 46.

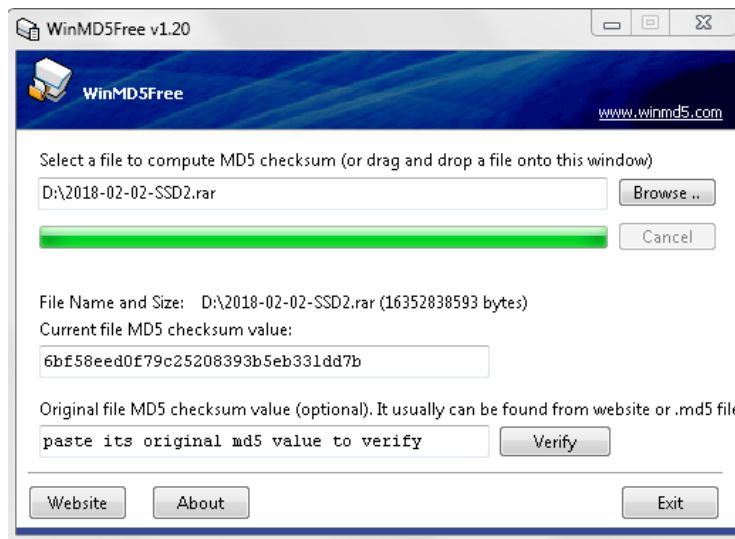


Figura 46 Hash md5 para el escenario 2

ETAPA 4: Análisis lógico

En la fase de verificación del tipo de daño lógico se basó en la tabla 11, y no se identificó ningún tipo de daño lógico por lo que se procede con la etapa 5 que es la recuperación de datos del dispositivo a pesar de que no presente ningún tipo de daño ni lógico ni físico.

ETAPA 5: Recuperación de datos

Para la recuperación de datos se utilizó 4 herramientas que son: Foremost/Scalpel para Linux y PhotoRec/Adroit Photo Recovery para Windows. Obteniendo los siguientes resultados para cada herramienta.

Foremost, recuperó un total de 24.661 archivos y se obtuvo la siguiente información por tipo de archivo como se indica en la Figura 47.

```
24661 FILES EXTRACTED
jpg:= 18363
gif:= 120
bmp:= 4
wmv:= 10
mov:= 13
rif:= 3
htm:= 19
ole:= 492
zip:= 1654
rar:= 86
exe:= 6
png:= 3718
pdf:= 173
```

Figura 47 Resultados foremost escenario 2

Scalpel, recupero un total de 22.881 archivos y se obtuvo la siguiente información por tipo de archivo:

- Avi: 0
- Bmp: 10
- Doc: 450
- Gif: 115
- Htm: 39
- Jpg: 9651
- Mov: 1426
- Mpg: 11190

Adroit Photo Recovery, recupero un total de 13.395 imágenes y se obtuvo la siguiente información:

- Completas: 13.125
- Dañadas: 14
- Falsos positivos: 256

Photo Rec, recupero un total de 16240 archivos como se aprecia en la Figura 48.

```
PhotoRec 7.1-WIP, Data Recovery Utility, January 2018
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk /dev/sdb - 120 GB / 111 GiB (RO) - WDC WDS1 20G2G0A-00JH30
Partition      Start      End      Size in sectors
 1 P HPFS - NTFS      0 32 33 14593 228 35 234448896 [SSD2]

Destination /testdisk-7.1-WIP/recup_dir

Pass 4 - Reading sector 34518656/234448896, 16240 files found
Elapsed time 1h29m18s - Estimated time to completion 8h37m13
jpg: 11618 recovered
png: 1964 recovered
zip: 1344 recovered
doc: 509 recovered
pdf: 168 recovered
apple: 152 recovered
mpg: 145 recovered
gif: 116 recovered
rar: 64 recovered
others: 160 recovered
```

Figura 48 Resultado PhotoRec escenario 2

4.3.3 Escenario 3: Caída intencional en investigaciones forenses digitales con altura mayor a 2 metros

Para la ejecución de este escenario se ha tomado diferentes alturas del edificio del departamento de Ciencias de la Computación que son:

SEGUNDO PISO

A. Determinar la altura de caída

Se ubica al dispositivo de almacenamiento al filo de la ventana del edificio con una altura de 4,90 m como se observa en la Figura 49.



Figura 49 Altura segundo piso

B. Calcular altura de rebote

Para los cálculos requeridos un valor importante a considerar es la altura de rebote que permitirá calcular la aceleración del objeto en este caso el dispositivo SSD con un valor de referencia de 18 centímetros como se observa en la Figura 50.

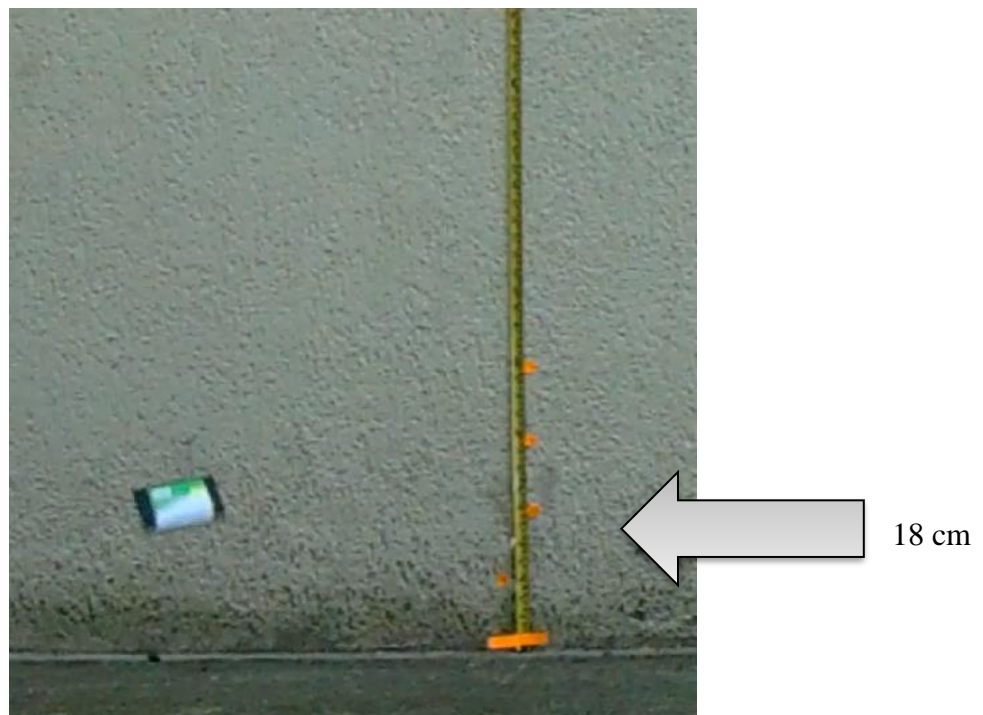


Figura 50 Altura de rebote segundo piso

C. Calcular fuerza de impacto

En la tabla 27 se aprecian los valores necesarios para la aplicación de la fórmula de caída libre de un SSD, tanto como la masa del objeto y la altura de caída, mientras que la gravedad se mantiene como un valor constante.

Tabla 27*Características del dispositivo SSD2*

DATOS	UNIDADES	VALOR
Masa / m	kg	0,032
Altura / h	m	4,90
Gravedad / g	m/s ²	9,81

Energía Potencial

$$E_p = m * g * h$$

$$E_p = 0,032 \text{ kg} * 9,81 \frac{\text{m}}{\text{s}^2} * 8,12 \text{ m}$$

$$E_p = 2,55 \text{ N m}$$

Velocidad de Impacto

$$v = \sqrt{2gh}$$

$$v = \sqrt{2 * 9,81 \frac{\text{m}}{\text{s}^2} * 8,12 \text{ m}}$$

$$v = \sqrt{159,31 \frac{\text{m}^2}{\text{s}^2}}$$

$$v = 12,62 \frac{\text{m}}{\text{s}}$$

Aceleración

$$a = \frac{v^2}{2h_r}$$

$$a = \frac{(12,62 \frac{m}{s})^2}{2 * (0,18 m)}$$

$$a = 442,40 \frac{m^2}{s^2}$$

Fuerza de impacto

$$F = m * a$$

$$F = 0,032 kg * 442,40 \frac{m^2}{s^2}$$

$$F = 14,16 N$$

D. Recuperación de datos

Para la recuperación de datos se utilizó 4 herramientas que son: Foremost/Scalpel para Linux y PhotoRec/Adroit Photo Recovery para Windows. Obteniendo los siguientes resultados para cada herramienta.

Foremost, recuperó un total de 22.992 archivos y se obtuvo la siguiente información por tipo de archivo como se indica en la Figura 51.

```
22992 FILES EXTRACTED

jpg:= 16712
gif:= 120
bmp:= 4
wmv:= 9
mov:= 12
htm:= 19
ole:= 487
zip:= 1652
rar:= 86
exe:= 6
png:= 3712
pdf:= 173
-----
```

Figura 51 Resultado foremost caída segundo piso

Scalpel, recuperó un total de 26.689 archivos como se detalla a continuación:

- Bmp 11
- Doc 900
- Gif 115
- Htm 39
- Jpg 9.651
- Mov 26
- Mpg 15417
- Pdf 33
- Png 351

Adroit Photo Recovery, recuperó un total de 13.278 como se indica en la Figura 52.

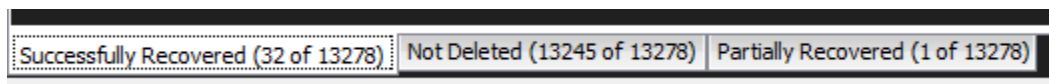


Figura 52 Resultado Adroit PhotoRecovery caída segundo piso

Photo Recovery, recuperó un total de 17.447 como se indica en la Figura 53.

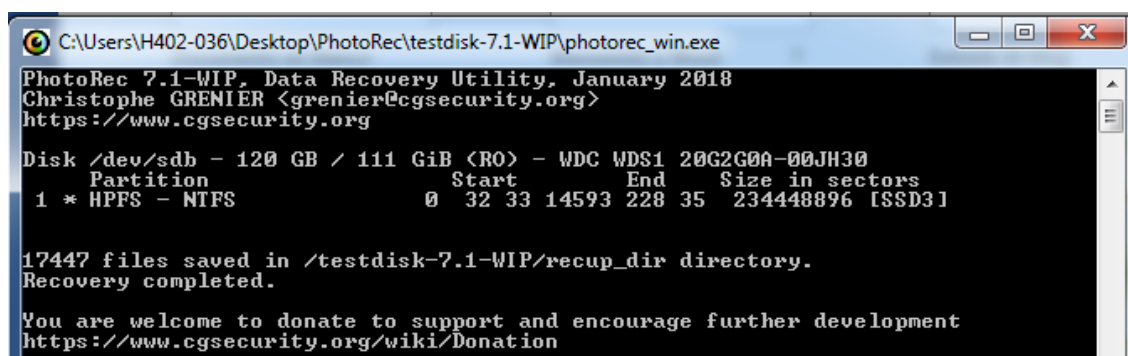


Figura 53 Resultado PhotoRec caída segundo piso

TERCER PISO

A. Determinar la altura de caída

Se ubica al dispositivo de almacenamiento al filo de la ventana del edificio con una altura de 8,12 m como se observa en la Figura 54.



Figura 54 Altura tercer piso

B. Calcular altura de rebote

Para los cálculos requeridos un valor importante a considerar es la altura de rebote que permitirá calcular la aceleración del objeto en este caso el dispositivo SSD con un valor de referencia de 10 centímetros como se observa en la Figura 55.

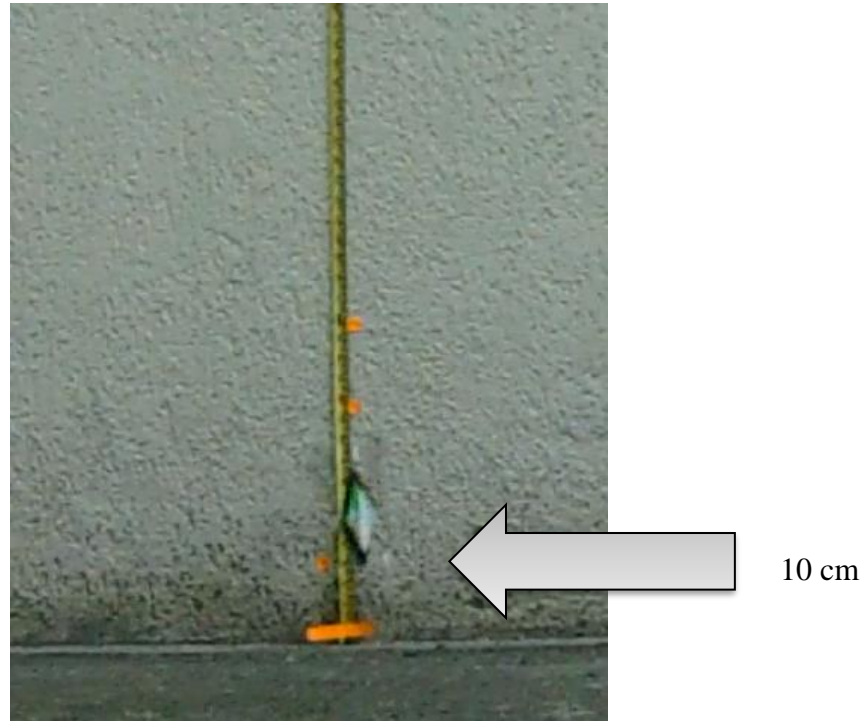


Figura 55 Altura de rebote tercer piso

C. Calcular fuerza de impacto

En la tabla 28 se aprecian los valores necesarios para la aplicación de la fórmula de caída libre de un SSD, tanto como la masa del objeto y la altura de caída, mientras que la gravedad se mantiene como un valor constante.

Tabla 28

Características del dispositivo SSD

DATOS	UNIDADES	VALOR
Masa / m	kg	0,032
Altura / h	m	8,12
Gravedad / g	m/s ²	9,81

Energía Potencial

$$E_p = m * g * h$$

$$E_p = 0,032 \text{ kg} * 9,81 \frac{\text{m}}{\text{s}^2} * 4,90 \text{ m}$$

$$E_p = 1,54 \text{ N m}$$

Velocidad de Impacto

$$v = \sqrt{2gh}$$

$$v = \sqrt{2 * 9,81 \frac{\text{m}}{\text{s}^2} * 4,90 \text{ m}}$$

$$v = \sqrt{96,14 \frac{\text{m}^2}{\text{s}^2}}$$

$$v = 9,80 \frac{\text{m}}{\text{s}}$$

Aceleración

$$a = \frac{v^2}{2h_r}$$

$$a = \frac{(9,80 \frac{\text{m}}{\text{s}})^2}{2 * (0,10 \text{ m})}$$

$$a = 480,20 \frac{\text{m}^2}{\text{s}^2}$$

Fuerza de impacto

$$F = m * a$$

$$F = 0,032 \text{ kg} * 480,20 \frac{\text{m}^2}{\text{s}^2}$$

$$F = 15,37 \text{ N}$$

Para la recuperación de datos se utilizó 4 herramientas que son: Foremost/Scalpel para Linux y PhotoRec/Adroit Photo Recovery para Windows. Obteniendo los siguientes resultados para cada herramienta.

Foremost, recuperó un total de 22.971 archivos y se obtuvo la siguiente información por tipo de archivo como se indica en la Figura 56.

```
22971 FILES EXTRACTED

jpg:= 16680
gif:= 120
bmp:= 4
wmv:= 9
mov:= 13
htm:= 19
ole:= 488
zip:= 1653
rar:= 88
exe:= 6
png:= 3718
pdf:= 173
-----
```

Figura 56 Resultado foremost caída tercer piso

Scalpel, recuperó un total de 25.994 archivos como se detalla a continuación:

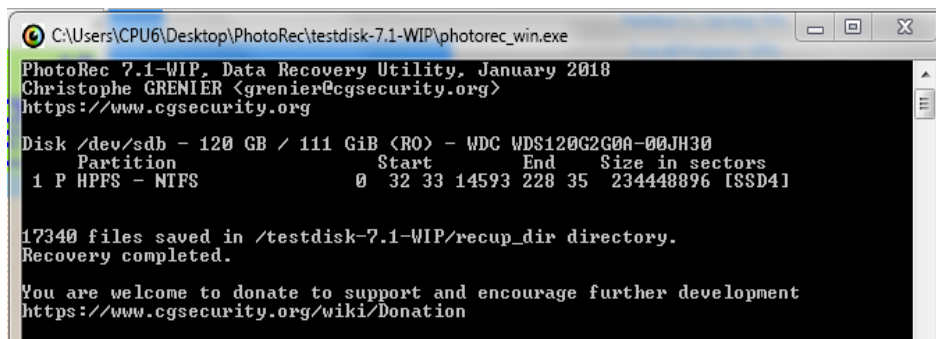
- Bmp 11
- Doc 900
- Gif 115
- Htm 39
- Jpg 9.300
- Mov 26
- Mpg 15.215
- Pdf 33
- Png 355

Adroit Photo Recovery, recuperó un total de 13.246 como se indica en la Figura 57.

Not Deleted (13246 of 13246)

Figura 57 Resultado Adroit PhotoRecovery caída tercer piso

PhotoRec, recuperó un total de 17.340 como se indica en la Figura 58.



```
C:\Users\CPU6\Desktop\PhotoRec\testdisk-7.1-WIP\photorec_win.exe
PhotoRec 7.1-WIP, Data Recovery Utility, January 2018
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk /dev/sdb - 120 GB / 111 GiB (RO) - WDC WDS120G2G0A-00JH30
Partition      Start          End      Size in sectors
1 P HPFS - NTFS      0 32 33 14593 228 35 234448896 [SSD4]

17340 files saved in /testdisk-7.1-WIP/recup_dir directory.
Recovery completed.

You are welcome to donate to support and encourage further development
https://www.cgsecurity.org/wiki/Donation
```

Figura 58 Resultado PhotoRec caída tercer piso

CUARTO PISO

A. Verificar la integridad del dispositivo SSD

Utilizando la herramienta CrystalDiskInfo como se observa en la Figura 59, el dispositivo SSD tiene un correcto rendimiento.

CrystalDiskInfo 7.1.0

Archivo Editar Función Tema Disco Ayuda Lengua(Language)

Riesgo: Bueno
44 °C 30 °C
C: D: G:

WDC WDS120G2G0A-00JH30 120,0 GB

Estado de salud: **Bueno**

Firmware: UE300000
Número de serie: 174560805763
Interfaz: USB (Serial ATA) Velocidad rotación: ---- (SSD)
Modo de transferencia: SATA/150 | SATA/600 Nº encendido: 2 veces
Temperatura: **30 °C** Letra de unidad: G: Horas encendido: 2 horas
Estándar: ACS-2 | ACS-2 Revision 3
Características soportadas: S.M.A.R.T., APM, NCQ, TRIM, DevSleep

ID	Detalles ID	Actual	Peor	Umbral	Valores en crudo
05	Nº de sectores reasignados	100	100	0	000000000000
09	Horas encendido	100	100	0	000000000002
0C	Nº de ciclos de encendido del dispositivo	100	100	0	000000000002
A5	Vendor Specific	100	100	0	000000000006
A6	Vendor Specific	100	100	0	000000000001
A7	Vendor Specific	100	100	0	000000000000
A8	Vendor Specific	100	100	0	000000000000
A9	Vendor Specific	100	100	0	000000000056
AA	Vendor Specific	100	100	0	000000000000
AB	Vendor Specific	100	100	0	000000000000
AC	Vendor Specific	100	100	0	000000000000
AD	Vendor Specific	100	100	0	000000000001
AE	Vendor Specific	100	100	0	000000000000
B8	Vendor Specific	100	100	0	000000000000
BB	Vendor Specific	100	100	0	000000000000
BC	Vendor Specific	100	100	0	000000000000
C2	Temperatura	70	49	0	00310010001E
C7	Vendor Specific	100	100	0	000000000000
E6	Vendor Specific	100	100	0	000100140001
E8	Vendor Specific	100	100	5	000000000064
E9	Vendor Specific	100	100	0	00000000000F
EA	Vendor Specific	100	100	0	000000000025
F1	Total Host Writes	100	100	0	000000000012
F2	Total Host Reads	100	100	0	000000000000
F4	Vendor Specific	0	100	0	000000000000

Figura 59 Estado inicial escenario cuarto piso

B. Pesar el dispositivo de almacenamiento SSD

Se coloca el dispositivo SSD sobre una balanza obteniendo un peso de 32 gramos.

C. Determinar la altura de caída

Se ubica al dispositivo de almacenamiento al filo de la ventana del edificio de 11.34 m como se observa en la Figura 60.



Figura 60 Altura para el escenario cuarto piso

D. Calcular altura de rebote

Para los cálculos requeridos un valor importante a considerar es la altura de rebote que permitirá calcular la aceleración del objeto en este caso el dispositivo SSD con un valor de referencia de 23 centímetros como se observa en la Figura 61.

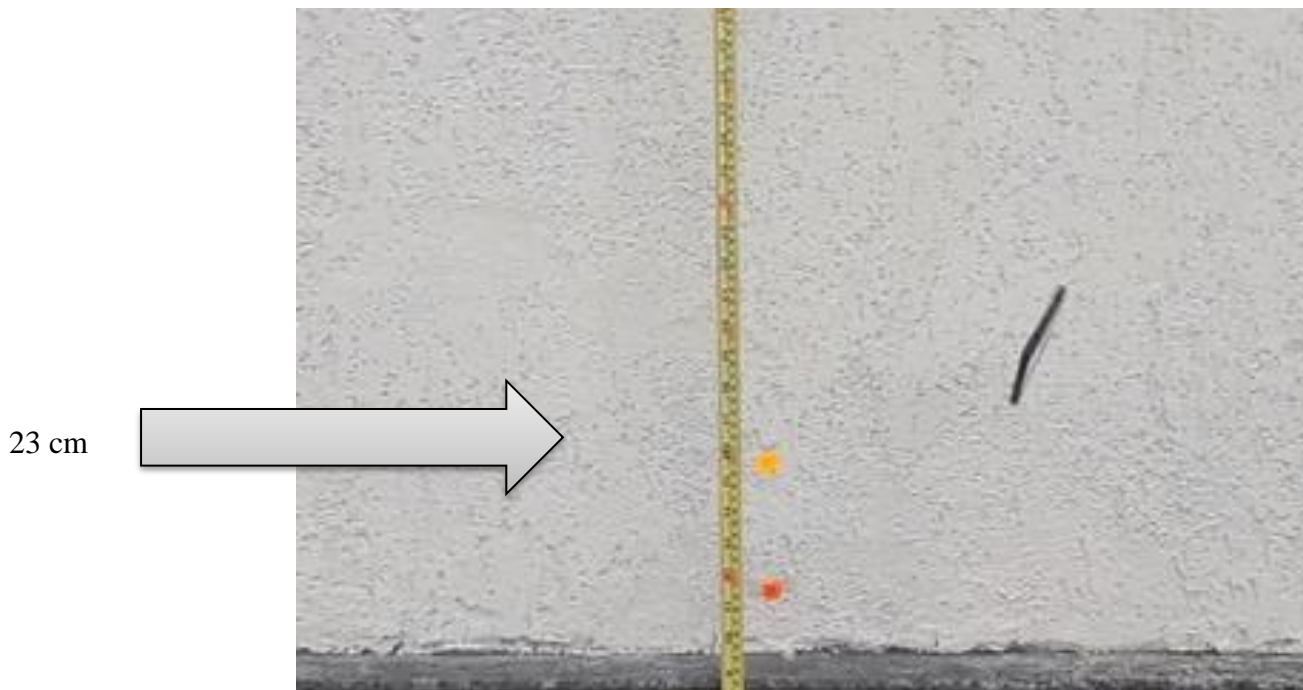


Figura 61 Altura de rebote cuarto piso

E. Calcular la fuerza de impacto

En la tabla 29 se aprecian los valores necesarios para la aplicación de la fórmula de caída libre de un SSD, tanto como la masa del objeto y la altura de caída, mientras que la gravedad se mantiene como un valor constante.

Tabla 29*Características del dispositivo SSD escenario cuarto piso*

DATOS	UNIDADES	VALOR
Masa / m	kg	0,032
Altura / h	m	11,34
Gravedad / g	m/s ²	9,81

Energía Potencial

$$E_p = m * g * h$$

$$E_p = 0,032 \text{ kg} * 9,81 \frac{\text{m}}{\text{s}^2} * 11,34 \text{ m}$$

$$E_p = 11,65 \text{ N m}$$

Velocidad de Impacto

$$v = \sqrt{2gh}$$

$$v = \sqrt{2 * 9,81 \frac{\text{m}}{\text{s}^2} * 11,34 \text{ m}}$$

$$v = \sqrt{222,49 \frac{\text{m}^2}{\text{s}^2}}$$

$$v = 14,92 \frac{\text{m}}{\text{s}}$$

Aceleración

$$a = \frac{v^2}{2h_r}$$

$$a = \frac{(14,92 \frac{m}{s})^2}{2 * (0,23 m)}$$

$$a = 483,93 \frac{m^2}{s^2}$$

Fuerza de impacto

$$F = m * a$$

$$F = 0,032 kg * 483,93 \frac{m^2}{s^2}$$

$$F = 15,49 N$$

Luego de conocer la fuerza de impacto del dispositivo SSD se procede a la recuperación de información siguiendo la metodología descrita en el capítulo 3 como se detalla a continuación:

4.3.3.1 Aplicación de la metodología para el escenario 3

Capacidad de almacenamiento: 120 GB

Espacio utilizado: 17,9 GB

ETAPA 1: Análisis físico

En esta etapa inicia con la revisión de la estructura física del disco duro, para identificar los daños físicos visibles. Los resultados se visualizan en la tabla 30.

Tabla 30

Resultado análisis físico SSD para el escenario cuarto piso

FASES	RESULTADO
Inspección visual	No se encontró indicios de golpes o abolladuras en el SSD, ni en sus componentes.
Verificación de la alimentación de poder	La energía eléctrica que debe recibir el dispositivo SSD es la correcta, sin generar problemas en la alimentación de poder.
Detección en el BIOS	El BIOS de la PC01 detectó al SSD con sus características correctas de marca y capacidad.

Al terminar esta etapa, se puede concluir que el dispositivo SSD no presenta ningún tipo de daño físico, pasando directamente a la etapa 3 que es la obtención de imagen.

ETAPA 3: Obtención de imagen

Se obtuvo una imagen completa del dispositivo SSD para continuar con la etapa 4 que es análisis lógico, en la tabla 31 se detalla las fases cumplidas de la etapa 3.

Tabla 31

Resultado obtención imagen SSD para el escenario cuarto piso

FASES	RESULTADO
Preparación del SSD de destino	El dispositivo de destino cumple las mismas características del SSD que es marca WesternDigital de 120GB de almacenamiento.
Creación de la imagen	Se utilizó el software Clonezilla-Live que permitió hacer la copia completa del dispositivo SSD.
Verificación de la imagen	Se generó el hash MD5 para la imagen obtenida como se presenta en la Figura 62.

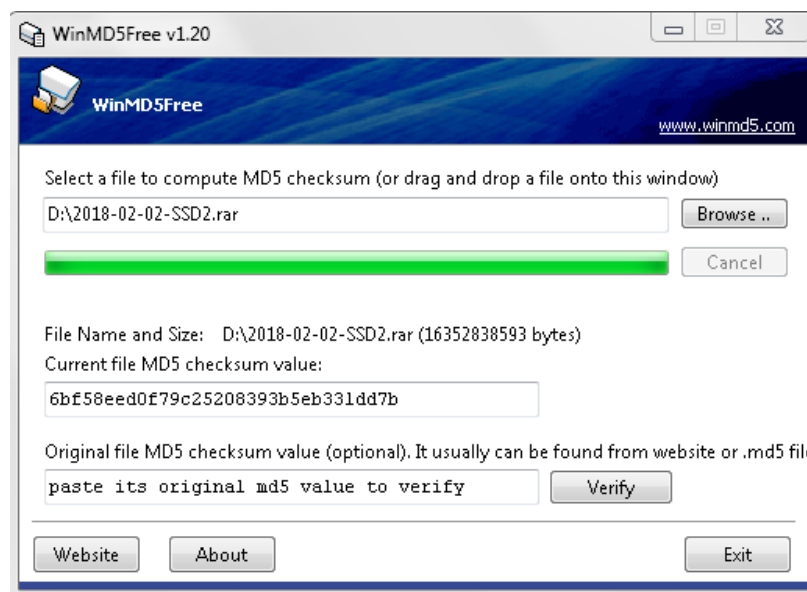


Figura 62 Hash md5 para el escenario 3

ETAPA 4: Análisis lógico

En la fase de verificación del tipo de daño lógico se basó en la tabla 11, y no se identificó ningún tipo de daño lógico por lo que se procede con la etapa 5 que es la recuperación de datos del dispositivo a pesar de que no presente ningún tipo de daño ni lógico ni físico.

ETAPA 5: Recuperación de datos

Para la recuperación de datos se utilizó 4 herramientas que son: Foremost/Scalpel para Linux y PhotoRec/Adroit Photo Recovery para Windows. Obteniendo los siguientes resultados para cada herramienta.

Foremost, recuperó un total de 20.396 archivos y se obtuvo la siguiente información por tipo de archivo como se indica en la Figura 63.

```
20396 FILES EXTRACTED

jpg:= 14509
gif:= 120
bmp:= 4
wmv:= 10
mov:= 13
htm:= 19
ole:= 437
zip:= 1598
rar:= 62
exe:= 6
png:= 3451
pdf:= 167
-----
```

Figura 63 Resultado Foremost caída cuarto piso

Scalpel, recuperó un total de 19.143 archivos como se detalla a continuación:

- Bmp 7
- Doc 665
- Gif 64
- Htm 39
- Jpg 7.173
- Mov 26
- Mpg 10.781
- Pdf 33
- Png 355

Adroit Photo Recovery, recuperó un total de 14.947 como se indica en la Figura 64.

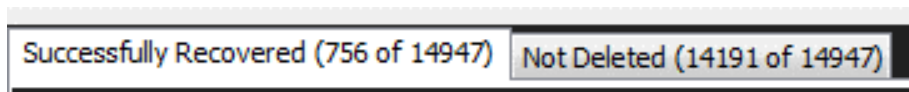


Figura 64 Resultado Adroit PhotoRecovery caída cuarto piso

Photo Recovery, recuperó un total de 17.340 como se indica en la Figura 65.

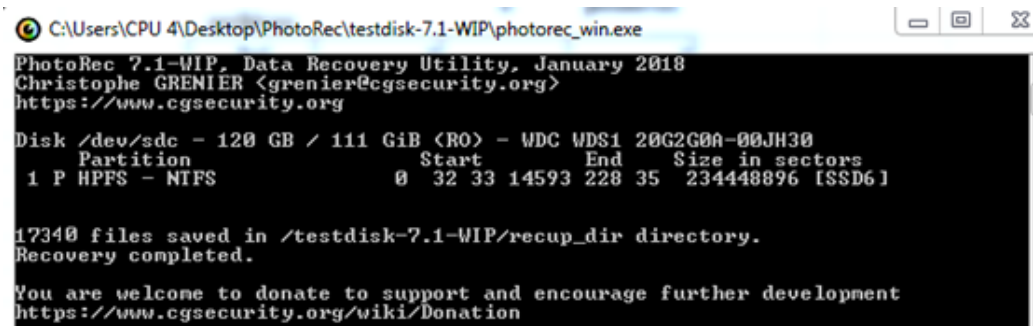


Figura 65 Resultado PhotoRec caída cuarto piso

4.3.4 Escenario 4: Aplastamiento de forma intencional en investigaciones forenses digitales con una fuerza de 4,02 KN

A. Seleccionar la fuerza de aplastamiento

La fuerza es de 4,02 KN que corresponde al vehículo liviano Aveo Family

B. Aplicar fuerza de aplastamiento

En el laboratorio de materiales del departamento de ciencias de la tierra, utilizando la máquina de compresión se aplicó una fuerza de 4,0 KN como se presenta en la Figura 66.

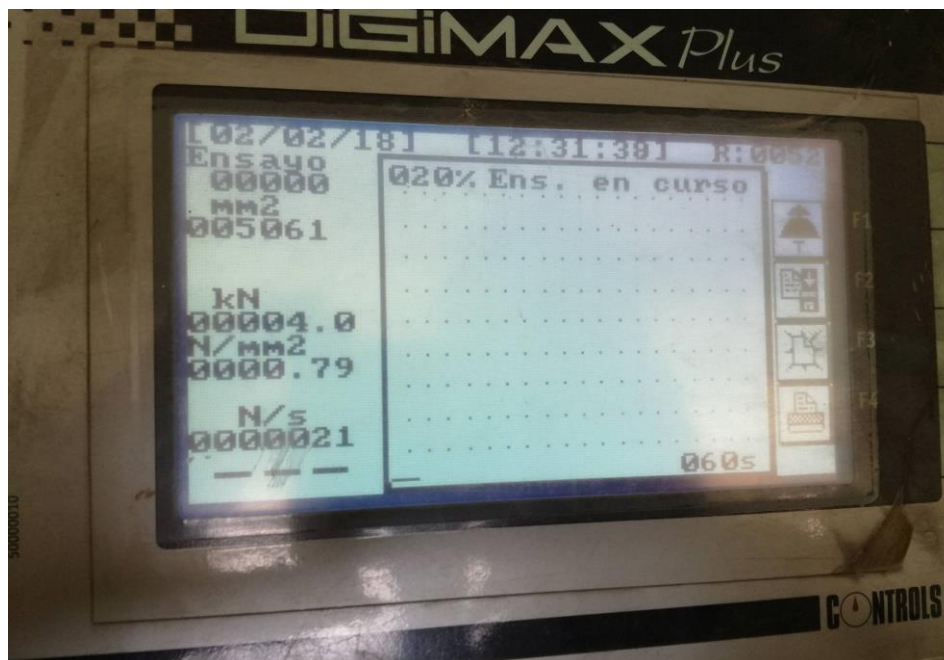


Figura 66 Fuerza ejercida del vehículo liviano sobre el dispositivo SSD

C. Recuperar información

Luego de haber aplicado la fuerza de aplastamiento del vehículo liviano al dispositivo SSD se procede a la recuperación de información siguiendo la metodología descrita en el capítulo 3 como se detalla a continuación:

4.3.4.1 Aplicación de la metodología para el escenario 4

Capacidad de almacenamiento: 120 GB

Espacio utilizado: 17,9 GB

ETAPA 1: Análisis físico

En esta etapa inicia con la revisión de la estructura física del disco duro, para identificar los daños físicos visibles. Los resultados se visualizan en la tabla 32.

Tabla 32*Resultado análisis físico para el escenario 4*

FASES	RESULTADO
Inspección visual	El dispositivo SSD no tienen ningún tipo de daño físico visible en su estructura o componentes
Verificación de la alimentación de poder	La energía eléctrica que debe recibir el dispositivo SSD es la correcta, sin generar problemas en la alimentación de poder.
Detección en el BIOS	El BIOS de la PC01 detectó al SSD con sus características correctas de marca y capacidad.

Al terminar esta etapa, se puede concluir que el dispositivo SSD no presenta ningún tipo de daño físico, pasando directamente a la etapa 3 que es la obtención de imagen.

ETAPA 3: Obtención de imagen

Se obtuvo una imagen completa del dispositivo SSD, para continuar con la etapa 4 que es análisis lógico, en la tabla 33 se detalla las fases cumplidas.

Tabla 33*Resultado obtención de imagen escenario 4*

FASES	RESULTADO
Preparación del SSD de destino	El dispositivo de destino cumple las mismas características del SSD que es marca WesternDigital de 120GB de almacenamiento.
Creación de la imagen	Se utilizó el software Clonezilla-Live que permitió hacer la copia completa del dispositivo SSD.
Verificación de la imagen	Se generó el hash MD5 para la imagen obtenida como se presenta en la Figura 67.

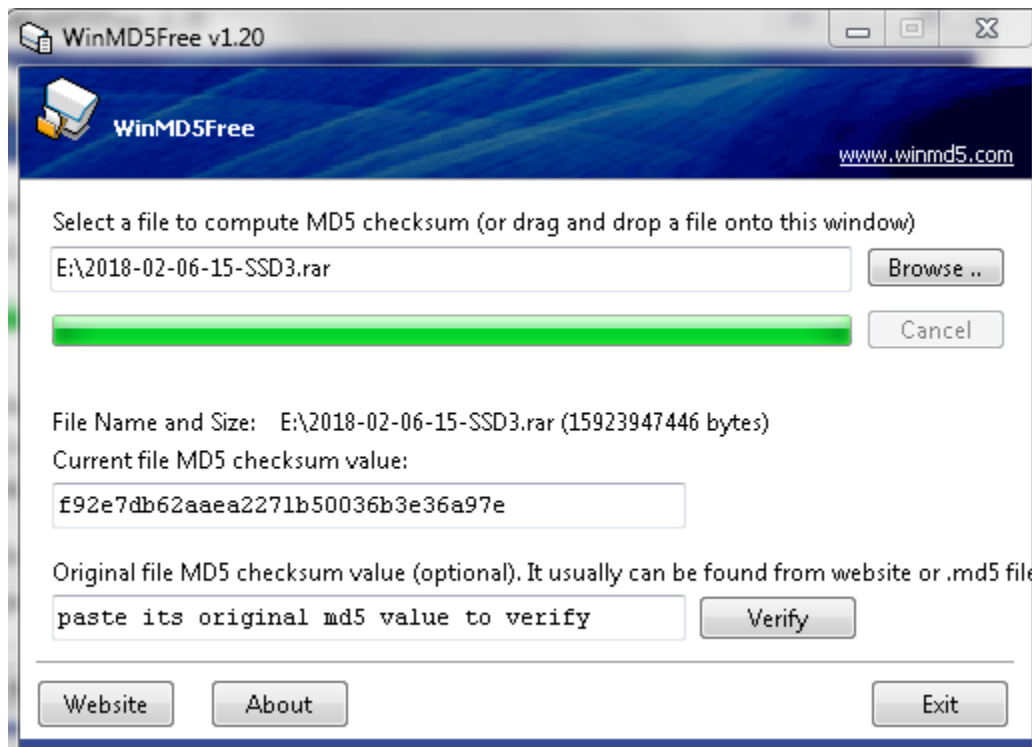


Figura 67 Hash para el escenario 4

ETAPA 4: Análisis lógico

En la fase de verificación del tipo de daño lógico se basó en la tabla 11, y no se identificó ningún tipo de daño lógico por lo que se procede con la etapa 5 que es la recuperación de datos del dispositivo a pesar de que no presente ningún tipo de daño ni lógico ni físico.

ETAPA 5: Recuperación de datos

Para la recuperación de datos se utilizó 4 herramientas que son: Foremost/Scalpel para Linux y PhotoRec/Adroit Photo Recovery para Windows. Obteniendo los siguientes resultados para cada herramienta.

Foremost, recupero un total de 22.992 archivos como se presenta en la Figura 68.

```
22992 FILES EXTRACTED

jpg:= 16712
gif:= 120
bmp:= 4
wmv:= 9
mov:= 12
htm:= 19
ole:= 487
zip:= 1652
rar:= 86
exe:= 6
png:= 3712
pdf:= 173
```

Figura 68 Resultado foremost escenario 4

Scalpel, ha recuperado un total de 26.689 archivos como se presenta a continuación:

- Bmp 11
- Doc 900
- Gif 115
- Htm 39
- Jpg 9.724
- Mov 26
- Mpg 15490
- Pdf 33
- Png 351

PhotoRec, recupero un total de 17.452 archivos como se presenta en la Figura 69.

```
PhotoRec 7.1-WIP, Data Recovery Utility, January 2018
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk /dev/sdb - 120 GB / 111 GiB (RO) - WDC WDS1 20G2G0A-00JH30
Partition      Start      End      Size in sectors
1 * HPFS - NTFS    0 32 33 14593 228 35 234448896 [SSD3]

17452 files saved in /testdisk-7.1-WIP/recup_dir directory.
Recovery completed.

You are welcome to donate to support and encourage further development
https://www.cgsecurity.org/wiki/Donation
```

Figura 69 Resultados PhotoRec escenario 4

AdroitPhoto Recovery, recupero un total de 14.980 imágenes como se presenta en la Figura 70.

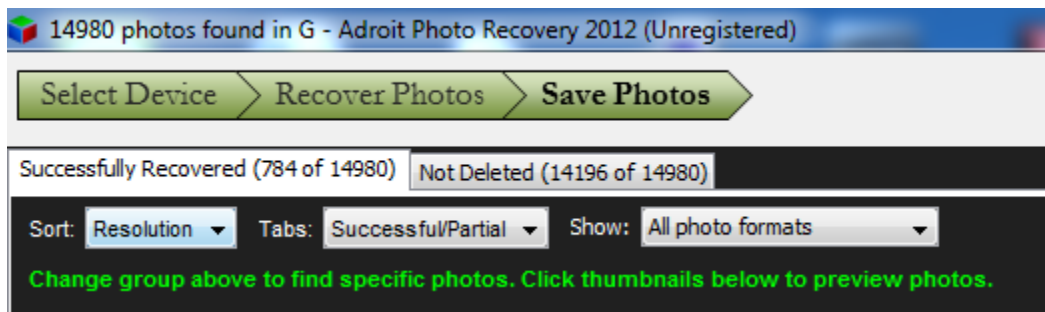


Figura 70 Resultados Adroit Photo Recovery escenario 4

4.3.5 Escenario 5: Aplastamiento de forma intencional en investigaciones forenses digitales con una fuerza de 4,75 kilo newtons

A. Seleccionar la fuerza de aplastamiento

La fuerza es de 4,75 KN que corresponde al vehículo mediano Ford sport track

B. Aplicar fuerza de aplastamiento

El dispositivo SSD se sometió a la fuerza de aplastamiento real del vehículo mediano Ford sport track que tiene una fuerza de 4,75 KN como se aprecia en la Figura 71 y 72.



Figura 71 Vehículo Ford sport track

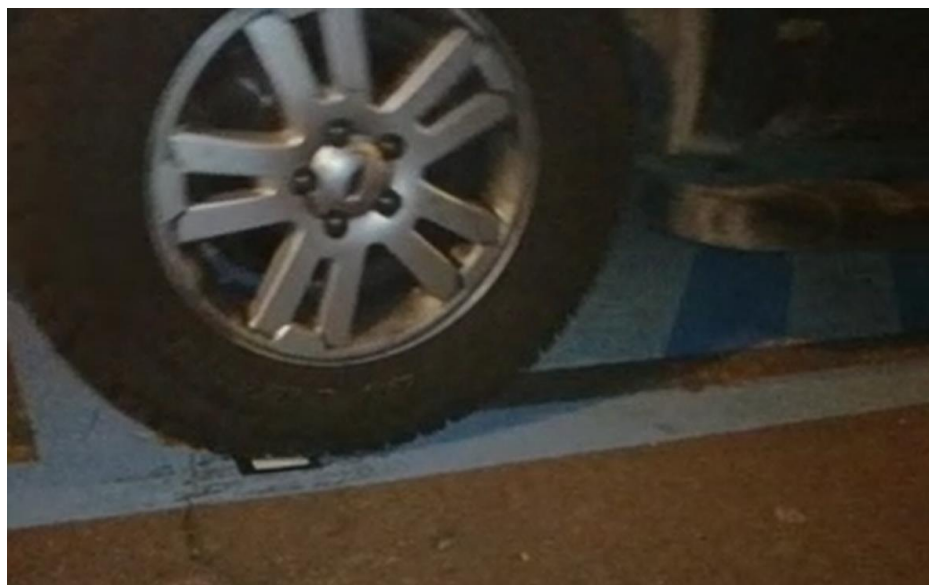


Figura 72 Aplastamiento al dispositivo SSD por el vehículo mediano

C. Recuperar información

Luego de haber aplicado la fuerza de aplastamiento del vehículo mediano al dispositivo SSD se procede a la recuperación de información siguiendo la metodología descrita en el capítulo 3 como se detalla a continuación:

4.3.5.1 Aplicación de la metodología para el escenario 5

Capacidad de almacenamiento: 120 GB

Espacio utilizado: 17,9 GB

ETAPA 1: Análisis físico

En esta etapa inicia con la revisión de la estructura física del disco duro, para identificar los daños físicos visibles. Los resultados se visualizan en la tabla 34.

Tabla 34

Resultado análisis físico para el escenario 5

FASES	RESULTADO
Inspección visual	El dispositivo SSD no tienen ningún tipo de daño físico visible en su estructura o componentes
Verificación de la alimentación de poder	La energía eléctrica que debe recibir el dispositivo SSD es la correcta, sin generar problemas en la alimentación de poder.
Detección en el BIOS	El BIOS de la PC01 detectó al SSD con sus características correctas de marca y capacidad.

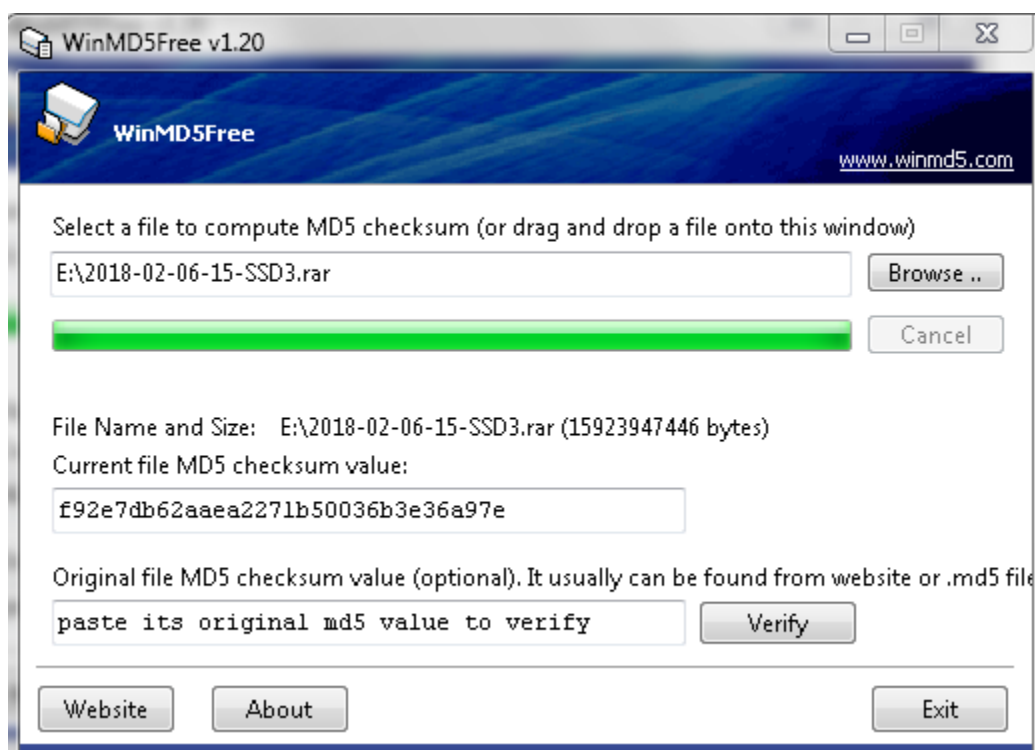
Al terminar esta etapa, se puede concluir que el dispositivo SSD no presenta ningún tipo de daño físico, pasando directamente a la etapa 3 que es la obtención de imagen.

ETAPA 3: Obtención de imagen

Se obtuvo una imagen completa del dispositivo SSD, para continuar con la etapa 4 que es análisis lógico, en la tabla 35 se detalla las fases cumplidas.

Tabla 35*Resultado obtención imagen SSD para el escenario 5*

FASES	RESULTADO
Preparación del SSD de destino	El dispositivo de destino cumple las mismas características del SSD que es marca WesternDigital de 120GB de almacenamiento.
Creación de la imagen	Se utilizó el software Clonezilla-Live que permitió hacer la copia completa del dispositivo SSD.
Verificación de la imagen	Se generó el hash MD5 para la imagen obtenida como se presenta en la Figura 73.

**Figura 73** Hash para el escenario 5

ETAPA 4: Análisis lógico

En la fase de verificación del tipo de daño lógico se basó en la tabla 11, y no se identificó ningún tipo de daño lógico por lo que se procede con la etapa 5 que es la recuperación de datos del dispositivo a pesar de que no presente ningún tipo de daño ni lógico ni físico.

ETAPA 5: Recuperación de datos

Para la recuperación de datos se utilizó 4 herramientas que son: Foremost/Scalpel para Linux y PhotoRec/Adroit Photo Recovery para Windows. Obteniendo los siguientes resultados para cada herramienta.

Foremost, recupero un total de 22.992 archivos como se presenta en la Figura 74.

```
22992 FILES EXTRACTED
jpg:= 16712
gif:= 120
bmp:= 4
wmv:= 9
mov:= 12
htm:= 19
ole:= 487
zip:= 1652
rar:= 86
exe:= 6
png:= 3712
pdf:= 173
```

Figura 74 Resultados foremost escenario 5

Scalpel, ha recuperado un total de 26.689 archivos como se presenta a continuación:

- Bmp 11
- Doc 900
- Gif 115

- Htm 39
- Jpg 9.724
- Mov 26
- Mpg 15490
- Pdf 33
- Png 351

PhotoRec, recupero un total de 17.452 archivos como se presenta en la Figura 75.

```
PhotoRec 7.1-WIP, Data Recovery Utility, January 2018
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk /dev/sdb - 120 GB / 111 GiB (RO) - WDC WDS1 20G2G0A-00JH30
  Partition      Start      End      Size in sectors
  1 * HPFS - NTFS 0 32 33 14593 228 35 234448896 [SSD3]

17452 files saved in /testdisk-7.1-WIP/recup_dir directory.
Recovery completed.

You are welcome to donate to support and encourage further development
https://www.cgsecurity.org/wiki/Donation
```

Figura 75 Resultados PhotoRec escenario 5

AdroitPhoto Recovery, recupero un total de 14.980 imágenes como se presenta en la Figura 76.



Figura 76 Resultados Adroit Photo Recovery escenario 5

4.3.6 Escenario 6: Aplastamiento de forma intencional en investigaciones forenses digitales con una fuerza de 11,62 KN

A. Seleccionar la fuerza de aplastamiento

La fuerza es de 11,62 KN que corresponde al vehículo pesado, en este caso un camión FSR 34N

B. Aplicar fuerza de aplastamiento

En el laboratorio de materiales del departamento de ciencias de la tierra, utilizando la máquina de compresión se aplicó una fuerza de 11,8 KN como se presenta en la Figura 77.

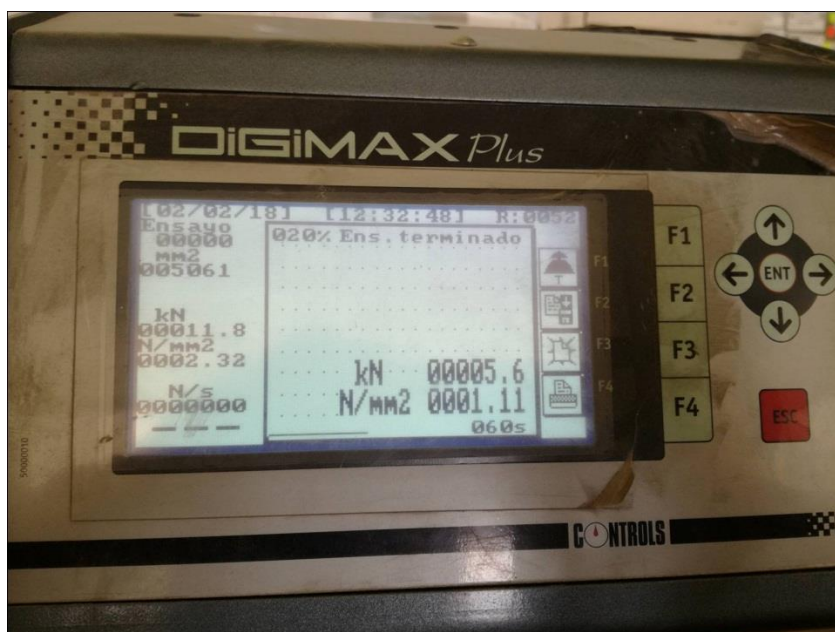


Figura 77 Fuerza de aplastamiento del vehículo pesado

C. Recuperar información

Luego de haber aplicado la fuerza de aplastamiento del vehículo pesado al dispositivo SSD se procede a la recuperación de información siguiendo la metodología descrita en el capítulo 3 como se detalla a continuación:

4.3.6.1 Aplicación de la metodología para el escenario 6

Capacidad de almacenamiento: 120 GB

Espacio utilizado: 17,9 GB

ETAPA 1: Análisis físico

Esta etapa inicia con la revisión de la estructura física del disco duro, para identificar los daños físicos visibles. Los resultados se visualizan en la tabla 36.

Tabla 36

Resultado análisis físico para el escenario 6

FASES	RESULTADO
Inspección visual	El dispositivo SSD no tienen ningún tipo de daño físico visible en su estructura o componentes
Verificación de la alimentación de poder	La energía eléctrica que debe recibir el dispositivo SSD es la correcta, sin generar problemas en la alimentación de poder.
Detección en el BIOS	El BIOS de la PC01 detectó al SSD con sus características correctas de marca y capacidad.

Al terminar esta etapa, se puede concluir que el dispositivo SSD no presenta ningún tipo de daño físico, pasando directamente a la etapa 3 que es la obtención de imagen.

ETAPA 3: Obtención de imagen

Se obtuvo una imagen completa del dispositivo SSD, para continuar con la etapa 4 que es análisis lógico, en la tabla 37 se detalla las fases cumplidas.

Tabla 37

Resultado obtención imagen SSD para el escenario 6

<i>FASES</i>	<i>RESULTADO</i>
<i>Preparación del SSD de destino</i>	El dispositivo de destino cumple las mismas características del SSD que es marca WesternDigital de 120GB de almacenamiento.
<i>Creación de la imagen</i>	Se utilizó el software Clonezilla-Live que permitió hacer la copia completa del dispositivo SSD.
<i>Verificación de la imagen</i>	Se generó el hash MD5 para la imagen obtenida como se presenta en la Figura 78.

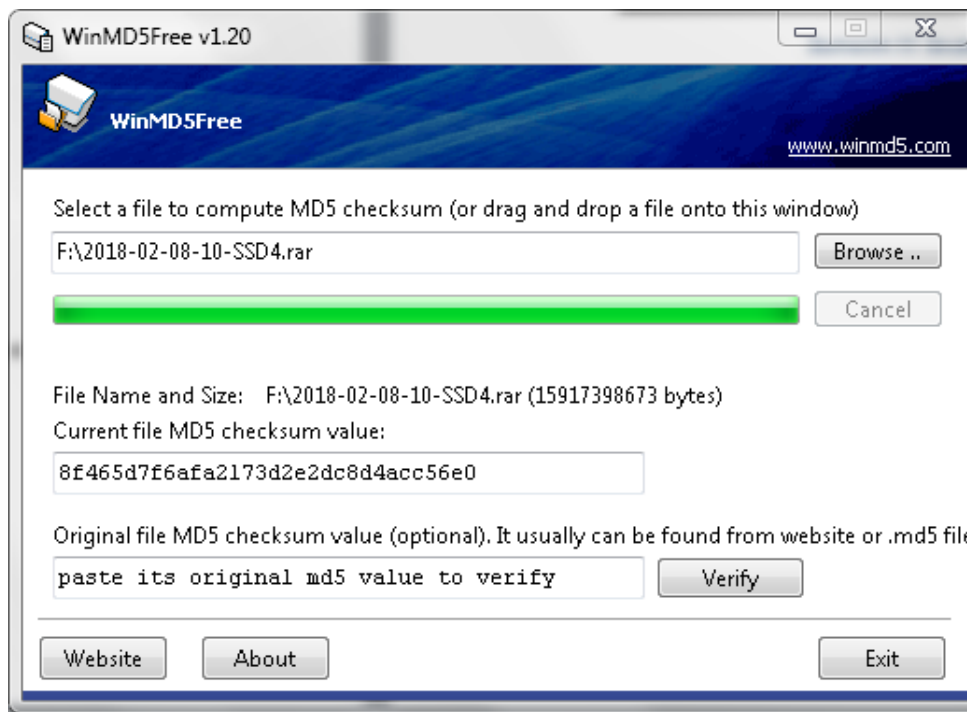


Figura 78 Hash para el escenario 6

De la imagen obtenida en esta etapa se procede a la etapa 4 donde se realiza el análisis lógico del dispositivo para determinar el tipo de daño.

ETAPA 4: Análisis lógico

En la fase de verificación del tipo de daño lógico se basó en la tabla 11, y no se identificó ningún tipo de daño lógico por lo que se procede con la etapa 5 que es la recuperación de datos del dispositivo a pesar de que no presente ningún tipo de daño ni lógico ni físico.

ETAPA 5: Recuperación de datos

Para la recuperación de datos se utilizó 4 herramientas que son: Foremost/Scalpel para Linux y PhotoRec/Adroit Photo Recovery para Windows. Obteniendo los siguientes resultados para cada herramienta.

Foremost, recuperó un total de 22.971 archivos como se presenta en la Figura 79.

```
22971 FILES EXTRACTED

jpg:= 16680
gif:= 120
bmp:= 4
wmv:= 9
mov:= 13
htm:= 19
ole:= 488
zip:= 1653
rar:= 88
exe:= 6
png:= 3718
pdf:= 173
-----
```

Figura 79 Resultados foremost escenario 6

Scalpel, recuperó un total de 26.689 archivos como se detalla a continuación:

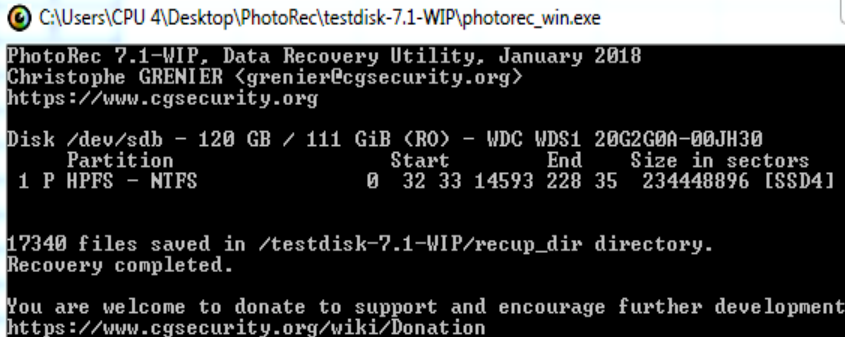
- Bmp 11
- Doc 900
- Gif 115
- Htm 39
- Jpg 9.724
- Mov 26
- Mpg 15490
- Pdf 33
- Png 351

Adroit Photo Recovery, recuperó un total de 14.948 imágenes como se aprecia en la Figura 80.



Figura 80 Resultados Adroit photo recovery escenario 6

PhotoRec, recuperó un total de 17.340 archivos como se presenta en la Figura 81.



```
C:\Users\CPU 4\Desktop\PhotoRec\testdisk-7.1-WIP\photorec_win.exe
PhotoRec 7.1-WIP, Data Recovery Utility, January 2018
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk /dev/sdb - 120 GB / 111 GiB (RO) - WDC WDS1 20G2G0A-00JH30
Partition      Start      End      Size in sectors
1 P HPFS - NTFS    0 32 33 14593 228 35 234448896 [SSD41]

17340 files saved in /testdisk-7.1-WIP/recup_dir directory.
Recovery completed.

You are welcome to donate to support and encourage further development
https://www.cgsecurity.org/wiki/Donation
```

Figura 81 Resultados PhotoRec escenario 6

4.3.7 Escenario 7: Golpe con objeto contundente

A. Identificar la masa del objeto contundente

Para este escenario se ha utilizado la fuerza aplicada sobre el dispositivo al ser golpeado con un objeto de masa 17,512 kg.

B. Determinar la altura recorrida

La distancia recorrida es de 0,022 metros como se presenta en la Figura 82, y la altura hacia el centro de gravedad es de 0,043 metros como se indica en la Figura 83.



Figura 82 Distancia recorrida objeto contundente



Figura 83 Altura desde el centro de gravedad del objeto contundente

C. Calcular la fuerza de impacto

Para este proceso se calculó la fuerza ejercida sobre el dispositivo tomado en cuenta el teorema de conservación de la energía (Universidad de Sevilla, 2010) que indica que el trabajo en este caso la energía potencial es igual a la fuerza por distancia, teniendo lo siguiente:

Cálculo de la energía potencial

$$Ep = m * g * h$$

$$Ep = 17,512 \text{ kg} * 9,80665 \frac{\text{m}}{\text{s}^2} * 0.043 \text{ m}$$

$$Ep = 7,38 \text{ N m}$$

Cálculo de la fuerza

$$Ep = F * distancia$$

$$F = \frac{Ep}{distancia}$$

$$F = \frac{7,38 \text{ N}}{0,022 \text{ m}}$$

$$F = \frac{7,38 \frac{\text{Kg} * \text{m}}{\text{s}^2}}{0,022 \text{ m}}$$

$$F = 335,455 \text{ N}$$

En la Figura 84 se presenta el dispositivo SSD que ha sido afectado por la fuerza calculada anteriormente.

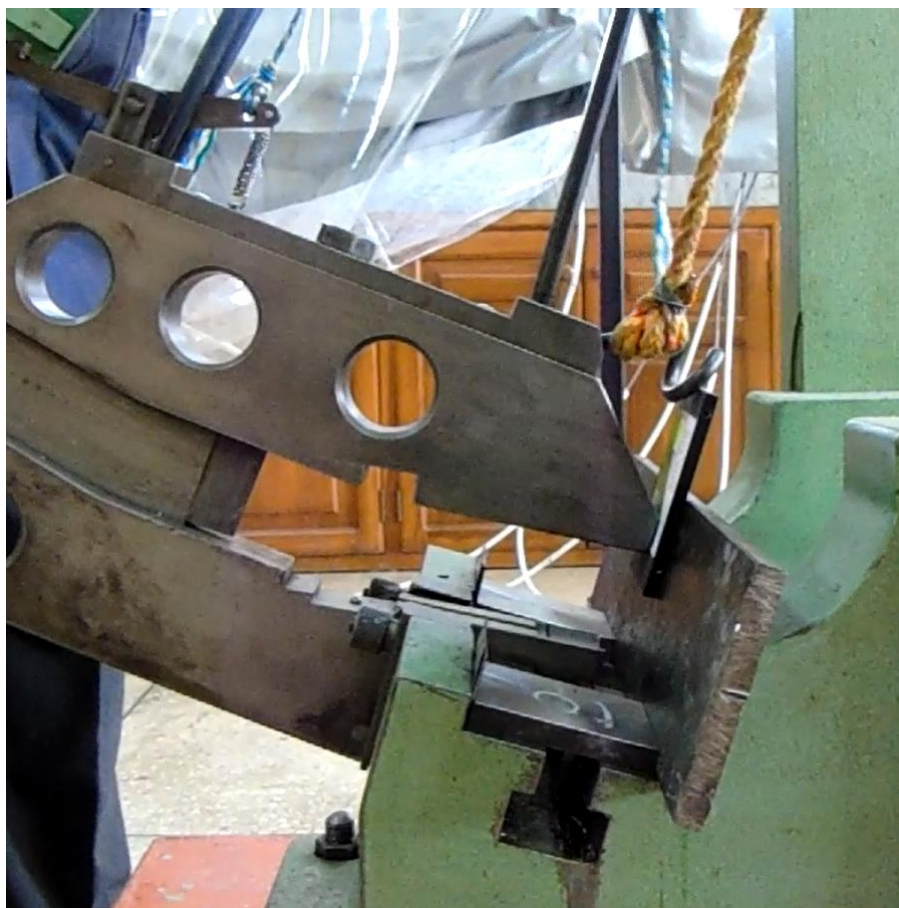


Figura 84 Fuerza de golpe con objeto contundente

4.3.7.1 Aplicación de la metodología para el escenario 7

Capacidad de almacenamiento: 120 GB

Espacio utilizado: 17,9 GB

ETAPA 1: Análisis físico

En esta etapa inicia con la revisión de la estructura física del disco duro, para identificar los daños físicos visibles. Los resultados se visualizan en la tabla 38.

Tabla 38

Resultado análisis físico para el escenario 7

FASES	RESULTADO
Inspección visual	El dispositivo SSD no tiene ningún tipo de daño físico visible en su estructura o componentes.
Verificación de la alimentación de poder	La energía eléctrica que debe recibir el dispositivo SSD es la correcta, sin generar problemas en la alimentación de poder.
Detección en el BIOS	El BIOS de la PC01, PC02, PC03 no detectó al SSD.

Al finalizar esta etapa se puede identificar un daño físico ya que el dispositivo SSD no ha sido reconocido por ninguna de las computadoras.

ETAPA 2: Reparación física temporal

Como el dispositivo SSD tenía un daño físico se procedió a ejecutar cada una de las fases de esta etapa como se detalla a continuación.

Identificación de la gravedad y tipo de daño

Basándose en los síntomas de daños físicos identificados en la tabla 10, se puede determinar que el dispositivo SSD no es reconocido por el BIOS.

Se procedió a abrir la carcasa del dispositivo verificando que los componentes se encuentren en su lugar y correctamente conectados, pero a pesar de que no tenía un daño físico visible se encuentra afectado.

Identificación de la solución

Como se aprecia el dispositivo SSD en la Figura 85, sus componentes se encuentran conectados de forma correcta, es posible que se requiera un limpiador de contactos para eliminar la estática existente.



Figura 85 Identificación de la solución

Ejecución de la solución

Se ha realizado el proceso de limpiar contactos como se presenta en la Figura 86 sin obtener que el dispositivo SSD sea reconocido en alguna de las computadoras disponibles.

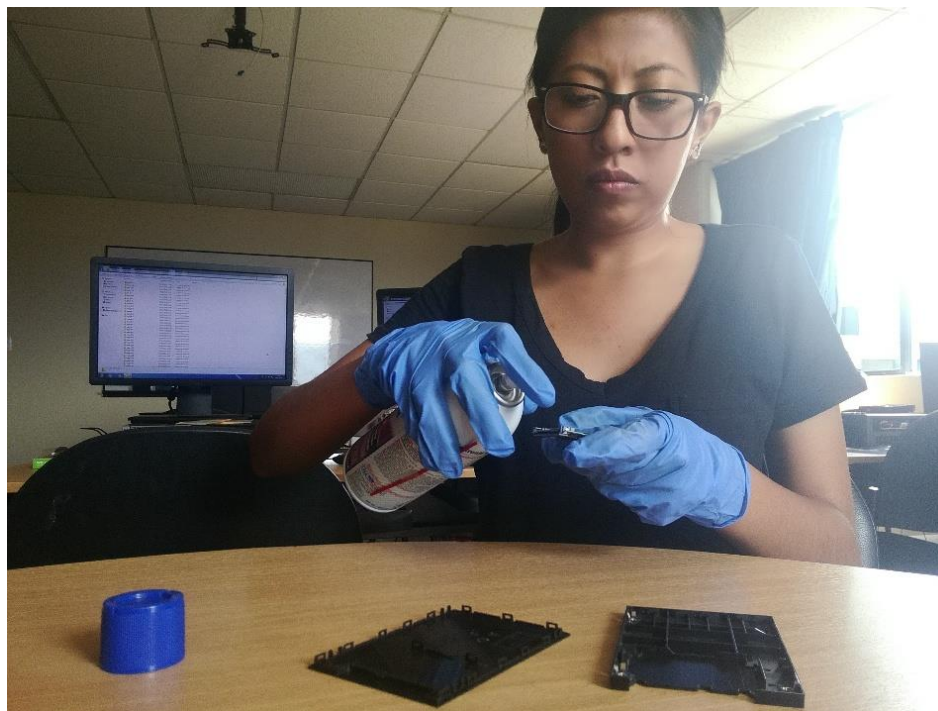


Figura 86 Limpieza de contactos de dispositivo SSD

Verificación de la solución aplicada

Para verificar que se ha obtenido éxito en este proceso el dispositivo debe ser reconocido en el BIOS de las computadoras PC01, PC02 y PC03, pero no se ha conseguido el objetivo.

4.3.8 Escenario 8: Humedecimiento

Para este escenario se han considerado varios tiempos en los que un dispositivo de almacenamiento SSD ha sido sometido a agua para lo cual se conoce que el tiempo de incidencia es:

TIEMPO DE 0-10 SEGUNDOS

A. Tomar la temperatura del agua

Con un termómetro de ambiente sumergir en agua y medir la temperatura, teniendo 19°C.

B. Sumergir el dispositivo de almacenamiento SSD

Sumergir el dispositivo de almacenamiento SSD durante 10 segundos, como se presenta en la Figura 87.

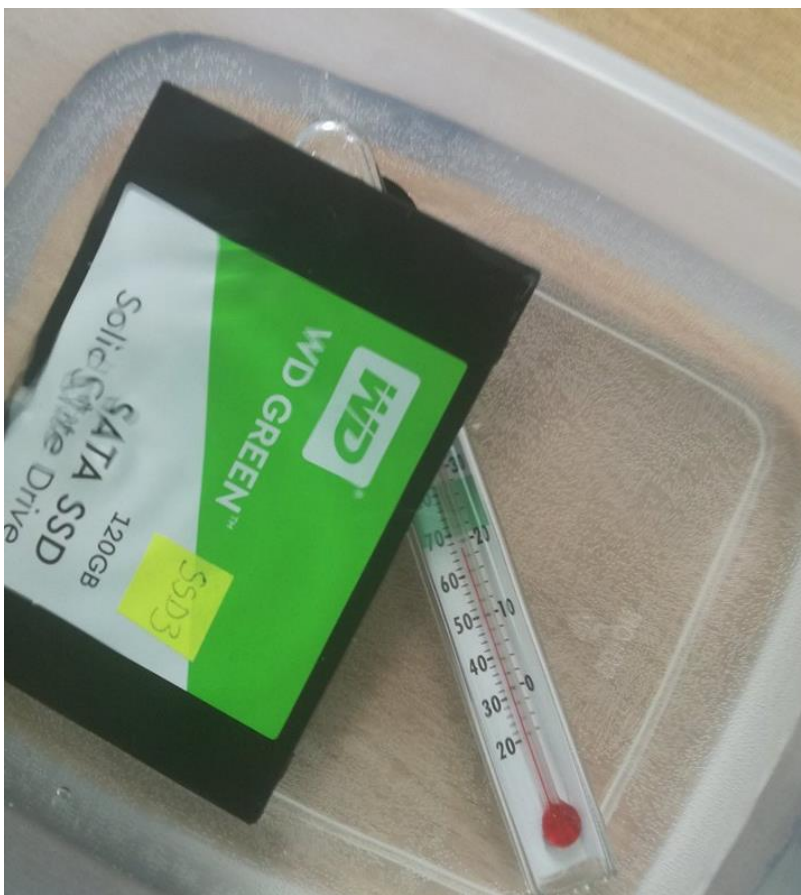


Figura 87 SSD sometido en agua durante 10 segundos

4.3.8.1 Aplicación de la metodología para el escenario 8

Capacidad de almacenamiento: 120 GB

Espacio utilizado: 17,9 GB

ETAPA 1: Análisis físico

Esta etapa inicia con la revisión de la estructura física del disco duro, para identificar los daños físicos visibles. Los resultados se visualizan en la tabla 39.

Tabla 39

Resultado análisis físico para el escenario 8

FASES	RESULTADO
Inspección visual	El dispositivo SSD se encuentra mojado, tanto su carcasa como sus componentes y se puede apreciar en la Figura 88 sin poder conectar al ningún equipo.
Verificación de la alimentación de poder	No se puede probar que la energía eléctrica sea la correcta, debido a que se encuentra mojado.
Detección en el BIOS	No se puede probar el reconocimiento por parte del BIOS, debido a que se encuentra mojado.



Figura 88 SSD daño físico por agua durante 10 segundos

Al finalizar esta etapa se puede concluir que el dispositivo SSD ha sufrido un daño físico, por lo que se procede a la segunda etapa que es la reparación física temporal.

ETAPA 2: Reparación física temporal

Identificación de la gravedad y tipo de daño

Basándose en el tipo de daño físico se procedió a abrir la carcasa del dispositivo, y como se muestra en la Figura 89 se observa parcialmente mojado.



Figura 89 SSD reparación física temporal debido a agua

Ejecución de la solución

La solución en este caso es secar inmediatamente y aplicar el limpiador de contactos que tiene un secado rápido y dejando reposar unos minutos.

Verificación de la solución

Al finalizar esta fase se debe conseguir la correcta identificación del SSD en el BIOS, teniendo éxito para este caso donde el dispositivo SSD se ha reconocido de forma correcta.

ETAPA 3: Obtención de imagen

Se obtuvo una imagen completa del dispositivo SSD, para continuar con la etapa 4 que es análisis lógico, en la tabla 40 se detalla las fases cumplidas.

Tabla 40

Resultado obtención de imagen escenario 8

FASES	RESULTADO
Preparación del SSD de destino	El dispositivo de destino cumple las mismas características del SSD que es marca WesternDigital de 120GB de almacenamiento.
Creación de la imagen	Se utilizó el software Clonezilla-Live que permitió hacer la copia completa del dispositivo SSD
Verificación de la imagen	Se generó el hash MD5 para la imagen obtenida como se presenta en la Figura 90.

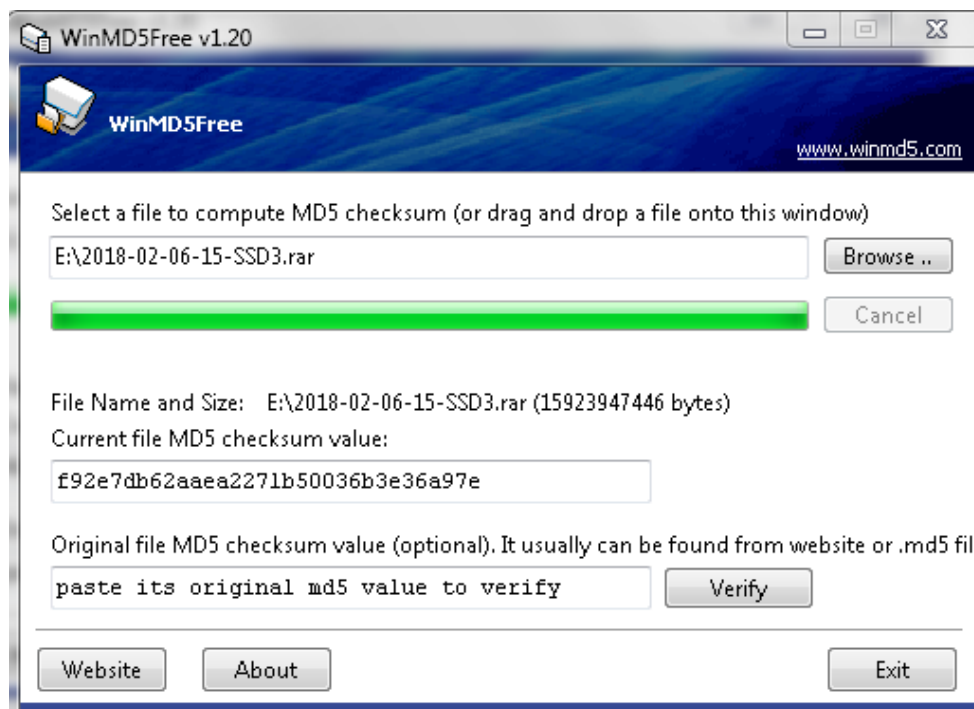


Figura 90 Hash para el SSD daño físico por agua durante 10 segundos

ETAPA 4: Análisis lógico

En la fase de verificación del tipo de daño lógico se basó en la tabla 11, y no se identificó ningún tipo de daño lógico por lo que se procede con la etapa 5 que es la recuperación de datos del dispositivo a pesar de que no presente ningún tipo de daño ni lógico ni físico.

ETAPA 5: Recuperación de datos

Para la recuperación de datos se utilizó 4 herramientas que son: Foremost/Scalpel para Linux y PhotoRec/Adroit Photo Recovery para Windows. Obteniendo los siguientes resultados para cada herramienta.

Foremost, recupero un total de 22.992 archivos como se presenta en la Figura 91.


```
22992 FILES EXTRACTED

jpg:= 16712
gif:= 120
bmp:= 4
wmv:= 9
mov:= 12
htm:= 19
ole:= 487
zip:= 1652
rar:= 86
exe:= 6
png:= 3712
pdf:= 173
-----
-
```

Figura 91 Resultado Foremost SSD en agua durante 10 segundos

Scalpel, recuperó un total de 26.689 archivos como se detalla a continuación:

- Bmp 11
- Doc 900
- Gif 115
- Htm 39
- Jpg 9.724
- Mov 26
- Mpg 15490
- Pdf 33
- Png 351

Adroit Photo Recovery, recuperó un total de 13.278 imágenes como se aprecia en la Figura 92.

Successfully Recovered (32 of 13278)	Not Deleted (13245 of 13278)	Partially Recovered (1 of 13278)
--------------------------------------	------------------------------	----------------------------------

Figura 92 Resultados Adroit photo recovery SSD en agua durante 10 segundos

PhotoRec, recuperó un total de 19.340 archivos como se presenta en la Figura 93.

```

C:\Users\CPU 4\Desktop\PhotoRec\testdisk-7.1-WIP\photorec_win.exe
PhotoRec 7.1-WIP, Data Recovery Utility, January 2018
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk /dev/sdb - 120 GB / 111 GiB <RO> - WDC WDS1 20G2G0A-00JH30
Partition      Start      End      Size in sectors
 1 P HPFS - NTFS      0 32 33 14593 228 35 234448896 [SSD41]

19340 files saved in /testdisk-7.1-WIP/recup_dir directory.
Recovery completed.

```

Figura 93 Resultados PhotoRec SSD en agua durante 10 segundos

TIEMPO DE 10-60 SEGUNDOS

A. Tomar la temperatura del agua

Con un termómetro de ambiente sumergir en agua y medir la temperatura, teniendo 21 °C.

B. Sumergir el dispositivo de almacenamiento SSD

Sumergir el dispositivo de almacenamiento SSD durante 30 segundos, como se presenta en la Figura 94.



Figura 94 SSD sometido en agua durante 30 segundos

C. Recuperar información

Para la recuperación de datos se utilizó 4 herramientas que son: Foremost/Scalpel para Linux y PhotoRec/Adroit Photo Recovery para Windows. Obteniendo los siguientes resultados para cada herramienta.

Foremost, recupero un total de 22.992 archivos como se presenta en la Figura 95.

```
22971 FILES EXTRACTED

jpg:= 16680
gif:= 120
bmp:= 4
wmv:= 9
mov:= 13
htm:= 19
ole:= 488
zip:= 1653
rar:= 88
exe:= 6
png:= 3718
pdf:= 173
-----
-
```

Figura 95 Resultado foremost SSD en agua durante 30 segundos

Scalpel, ha recuperado un total de 26.687 archivos como se presenta a continuación:

- Bmp 11
- Gif 115
- Jpg 9.723
- Mov 26
- Mpg 15490
- Png 351
- Doc 900
- Htm 39
- Pdf 32

PhotoRec, recupero un total de 19.321 imágenes como se presenta en la Figura 96.

```
PhotoRec 7.1-WIP, Data Recovery Utility, January 2018
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk /dev/sdb - 120 GB / 111 GiB (RO) - WDC WDS1 20G2G0A-00JH30
Partition      Start      End      Size in sectors
1 * HPFS - NTFS    0 32 33 14593 228 35 234448896 [SSD3]

19321 files saved in /testdisk-7.1-WIP/recup_dir directory.
Recovery completed.

You are welcome to donate to support and encourage further development
https://www.cgsecurity.org/wiki/Donation
```

Figura 96 Resultados PhotoRec SSD en agua durante 30 segundos

AdroitPhoto Recovery, recupero un total de 13.246 imágenes como se presenta en la Figura 97.

Not Deleted (13246 of 13246)

Figura 97 Resultados Adroit Photo Recovery SSD en agua durante 30 segundos

TIEMPO MÁS DE 60 SEGUNDOS

A. Tomar la temperatura del agua

Con un termómetro de ambiente sumergir en agua y medir la temperatura, teniendo 21 °C.

B. Sumergir el dispositivo de almacenamiento SSD

Sumergir el dispositivo de almacenamiento SSD durante 65 segundos, como se presenta en la Figura 98.



Figura 98 SSD sometido en agua durante 65 segundos

C. Recuperar información

Para la recuperación de datos se utilizó 4 herramientas que son: Foremost/Scalpel para Linux y PhotoRec/Adroit Photo Recovery para Windows. Obteniendo los siguientes resultados para cada herramienta.

Foremost, recupero un total de 22.992 archivos como se presenta en la Figura 99.

```
22992 FILES EXTRACTED

jpg:= 16712
gif:= 120
bmp:= 4
wmv:= 9
mov:= 12
htm:= 19
ole:= 487
zip:= 1652
rar:= 86
exe:= 6
png:= 3712
pdf:= 173
-----
```

Figura 99 Resultados Foremost SSD en agua durante 65 segundos

Scalpel, ha recuperado un total de 26.680 archivos como se presenta a continuación:

- Bmp 11
- Gif 113
- Jpg 9.721
- Mov 26
- Mpg 15490
- Png 351
- Doc 900
- Htm 35
- Pdf 33

PhotoRec, recupero un total de 19.325 archivos como se presenta en la Figura 100.

```
PhotoRec 7.1-WIP, Data Recovery Utility, January 2018
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk /dev/sdb - 120 GB / 111 GiB (RO) - WDC WDS1 20G2G0A-00JH30
Partition      Start      End      Size in sectors
1 * HPFS - NTFS    0 32 33 14593 228 35 234448896 [SSD3]

19325 files saved in /testdisk-7.1-WIP/recup_dir directory.
Recovery completed.

You are welcome to donate to support and encourage further development
https://www.cgsecurity.org/wiki/Donation
```

Figura 100 Resultado PhotoRec SSD en agua durante 65 segundos

Adroit Photo Recovery, recupero un total de 13.278 archivos como se presenta en la Figura 101.

Successfully Recovered (32 of 13278)	Not Deleted (13245 of 13278)	Partially Recovered (1 of 13278)
--------------------------------------	------------------------------	----------------------------------

Figura 101 Resultado Adroit Photo Recovery SSD en agua durante 65 segundos

CAPÍTULO V

RESULTADOS

5.1 Análisis de resultados

5.1.1 Escenario 1 Caída por descuido menor a 1 metro fuerza de 2,275 N

Tabla 41

Total, de archivos recuperados herramienta Foremost escenario 1

Formato de archivos	Total, Recuperados	Válidos recuperados	Falsos positivos
Avi	3	3	0
Bmp	4	4	0
Doc	156	156	0
Exe	6	0	6
Gif	120	0	120
Htm	19	19	0
Jar	1	1	0
Jpg	18363	18117	246
Mov	13	0	13
Pdf	173	173	0
Png	3718	3718	0
Ppt	1	1	0
Rar	70	70	0
Wmv	10	7	3
Xlsx	1142	1142	0
Zip	358	0	358
Total	24.157	23.411	746

Tabla 42*Total, de archivos recuperados herramienta Scalpel escenario 1*

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Bmp	10	0	10
Doc	900	0	900
Gif	123	1	122
Htm	66	56	10
Jpg	9.100	8.175	925
Mov	57	0	57
Mpg	13.104	0	13.104
Pdf	33	31	2
Png	350	0	350
Total	23.743	8.263	15.480

Tabla 43*Total, de archivos recuperados herramienta Adroit Photo Recovery escenario 1*

Formato de imagen	Válidos recuperados	No recuperado
Jpg	30.776	498
Bmp	6	4
Gif	127	118
Png	5.288	558
Total	36.197	1.178

Tabla 44*Total, de archivos recuperados herramienta PhotoRec escenario 1*

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Exe	17	0	17
Jar	5	5	0
Zip	60	60	0
Doc	163	156	7
Txt	2.000	2.000	0
Xml	3	1	2
Jpg	7009	7009	0
Ppt	5	0	5
Html	45	7	38
Gif	8	8	0
Png	1183	1183	0
Csv	9	9	0
Xlsx	259	259	0
Total	10.766	10.697	69

5.1.2 Escenario 2 Caída por descuido entre 1 y 2 metros con fuerza de 6,48 N

Tabla 45

Total, de archivos recuperados herramienta Foremost escenario 2

Formato de archivos	Total, Recuperados	Válidos recuperados	Falsos positivos
Avi	3	3	0
Bmp	4	4	0
Doc	156	156	0
Exe	6	2	4
Gif	120	2	118
Htm	19	18	1
Jar	1	0	1
Jpg	18085	16176	1909
Mov	13	0	13
Pdf	173	173	0
Png	3718	3718	0
Ppt	1	1	0
Rar	86	86	0
Wmv	10	8	2
Xlsx	1139	1139	0
Total	23.534	21.486	2.048

Tabla 46*Total, de archivos recuperados herramienta Scalpel escenario 2*

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Avi	0	0	0
Bmp	10	0	10
Doc	450	0	450
Gif	115	2	115
Pdf	33	31	2
Htm	39	38	1
Jpg	9641	8590	1051
Mov	1426	0	1426
Mpg	11190	0	11190
Png	347	0	347
Total	23.251	8.661	14.592

Tabla 47*Total, de archivos recuperados herramienta Adroit Photo Recovery escenario 2*

Formato de imagen	Total, Recuperado	No recuperado
Jpg	12859	243
Bmp	6	6
Gif	116	1
Png	2117	148
Total	15.098	398

Tabla 48

Total, de archivos recuperados herramienta PhotoRec escenario 2

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Pdf	168	168	0
Exe	3	2	1
Bmp	6	6	0
Jpg	14628	14628	0
Png	1680	1680	0
Wmv	6	2	4
Xls	1306	1306	0
Doc	272	122	144
html	28	28	0
rar	54	54	0
Gif	115	115	0
Avi	9	0	8
Mp4	5	4	1
Ppt	4	1	3
Mov	3	3	0
Mpg	145	111	34
Mp3	4	4	0
Flv	19	19	0
Total	18.455	18.253	195

5.1.3 Escenario 3 Caída intencional en investigaciones forenses digitales con altura mayor a 2 metros

SEGUNDO PISO: ALTURA DE 4,90 METROS (14,16 N)

Tabla 49*Archivos recuperados herramienta Foremost escenario 3-caída segundo piso*

Formato de archivos	Total, Recuperados	Válidos recuperados	Falsos positivos
Avi	0	0	0
Bmp	4	4	0
Gif	120	2	118
Jpg	16.712	16.397	315
Mov	12	0	12
Png	3.712	3.712	0
Wmv	9	8	1
Doc	156	156	0
Pdf	173	173	0
Xlsx	1.139	1.139	0
Ppt	1	1	0
Exe	6	2	4
Htm	20	20	0
Total	22.064	21.614	450

Tabla 50*Archivos recuperados herramienta Scalpel escenario 3- caída segundo piso*

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Bmp	11	0	11
Doc	900	0	900
Gif	115	2	113
Htm	39	39	0
Jpg	9.861	8.838	1.023
Mov	26	0	26
Mpg	15490	0	15490
Pdf	33	33	0
Png	372	0	372
Total	26.847	8.912	17.935

Tabla 51*Archivos recuperados herramienta Adroit Photo Recovery escenario 3- 2do piso*

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Jpg	11.983	11.752	231
Bmp	6	6	0
Gif	104	104	0
Png	1.185	1.077	108
Total	13.278	12.939	339

Tabla 52*Archivos recuperados herramienta PhotoRec escenario 3- caída 2do piso*

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Rar	69	69	0
Mpg	145	140	5
Doc	316	185	131
Jpg	12673	12673	0
Pdf	192	192	0
Wma	6	6	0
Wmv	7	7	0
Avi	9	1	8
Flv	19	19	0
Ppt	15	1	14
Mp3	30	25	5
Xlsx	1190	1189	1
Mp4	27	25	2
Png	1965	1965	0
Exe	5	3	2
Bmp	6	6	0
Html	28	28	0
Gif	116	115	1
Total	16.818	16.649	169

TERCER PISO: ALTURA DE 8,12 METROS (15,37 N)**Tabla 53***Archivos recuperados herramienta Foremost escenario 3- caída 3er piso.*

Formato de archivos	Total	Válidos recuperados	Falsos positivos
Avi	0	0	0
Bmp	4	4	0
Gif	120	2	118
Jpg	16.680	16.373	307
Mov	13	0	13
Png	3.718	3.309	409
Wmv	9	8	1
Doc	156	156	0
Pdf	173	173	0
Xlsx	1.139	1.139	0
Ppt	1	1	0
Total	22.013	21.165	848

Tabla 54*Archivos recuperados herramienta Scalpel escenario 3- caída 3er piso.*

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Bmp	11	0	11
Doc	900	0	900
Gif	115	2	113
Htm	39	39	0
Jpg	9.300	8.277	1.023
Mov	26	0	26
Mpg	15.215	0	15490
Pdf	33	33	0
Png	355	0	355
Total	25.994	8.351	17.918

Tabla 55

Archivos recuperados herramienta Adroit Photo Recovery escenario 3- 3er piso.

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Jpg	11.958	11.719	239
Bmp	6	6	0
Gif	99	99	0
Png	1.183	1.071	112
Total	13.246	12.895	351

Tabla 56

Archivos recuperados herramienta PhotoRec escenario 3- 3er piso.

Formato de archivos	Total, Recuperados	Válidos recuperados	Falsos positivos
Avi	9	1	8
Bmp	6	6	0
Gif	116	115	1
Jpg	16.471	16.471	0
Mov	4	4	0
Png	1.965	1.965	0
Wmv	181	181	0
Doc	317	167	150
Pdf	188	188	0
Xlsx	1.526	1.214	312
Ppt	2	1	1
Total	20.785	20.313	472

CUARTO PISO: ALTURA DE 11,34 METROS (15,49)**Tabla 57***Archivos recuperados herramienta Foremost escenario 3- 4to piso.*

Formato de archivos	Total, Recuperados	Válidos recuperados	Falsos positivos
Avi	0	0	0
Bmp	4	4	0
Gif	120	2	118
Jpg	16.671	16.360	311
Mov	13	0	13
Png	3.718	3.309	409
Wmv	9	8	1
Doc	156	156	0
Pdf	173	173	0
Xlsx	1.122	1.122	0
Ppt	1	1	0
Total	21.987	21.135	852

Tabla 58*Archivos recuperados herramienta Scalpel escenario 3- 4to piso*

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Bmp	7	7	0
Doc	665	0	665
Gif	64	7	57
Htm	39	39	0
Jpg	7.173	6.305	868
Mov	26	0	26
Mpg	10.781	0	10.781
Pdf	33	33	0
Png	355	0	355
Total	19.143	6.391	12.752

Tabla 59

Archivos recuperados herramienta Adroit Photo Recovery

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Jpg	12.931	12.678	253
Bmp	6	6	0
Gif	101	99	2
Png	1.909	1.788	121
Total	14.947	14.571	376

Tabla 60

Archivos recuperados herramienta PhotoRec escenario 3- 4to piso

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Rar	69	69	0
Mpg	145	140	5
Doc	301	181	120
Jpg	12661	12661	0
Pdf	137	137	0
Wma	6	6	0
Wmv	7	7	0
Avi	9	1	8
Ppt	15	1	14
Mp3	30	25	5
Xlsx	1190	1189	1
Mp4	0	0	0
Png	1965	1965	0
Exe	5	3	2
Bmp	6	6	0
Html	28	28	0
Gif	116	115	1
Total	16.690	16.534	156

5.1.4 Escenario 4 Aplastamiento de forma intencional en investigaciones forenses digitales con una fuerza de 4,02 KN

Tabla 61

Archivos recuperados herramienta Foremost escenario 4 - vehículo pequeño

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Bmp	4	4	0
Docx	162	162	0
Exe	6	2	4
Gif	120	2	118
Htm	20	20	0
Jar	1	1	0
Jpg	16932	16677	255
Mov	12	0	12
Pdf	173	173	0
Png	3726	3726	0
Ppt	1	0	1
Wmv	9	9	0
Xls	1139	1139	0
Total	22.305	21.915	390

Tabla 62

Archivos recuperados herramienta Scalpel escenario 4 - vehículo pequeño

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Bmp	11	0	11
Doc	900	0	900
Gif	115	2	113
Htm	39	39	0
Jpg	9.724	8.677	1047
Mov	26	0	26
Mpg	15490	0	15490
Pdf	33	33	0
Png	351	0	351
Total	26.689	8.751	17.938

Tabla 63*Archivos recuperados herramienta Adroit escenario 4 - vehículo pequeño*

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Jpg	12822	12591	231
Bmp	6	6	0
Gif	116	115	1
Png	2128	2016	112
Total	15.072	14.728	344

Tabla 64*Archivos recuperados herramienta PhotoRec escenario 4 - vehículo pequeño*

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Rar	68	68	0
Mpg	145	140	5
Doc	307	172	135
Jpg	15826	15826	0
Pdf	172	172	0
Wma	6	6	0
Wmw	7	7	0
Avi	9	1	8
Flv	19	19	0
Ppt	1	1	0
Mp3	30	25	5
Xls	1513	1511	2
Mp4	26	26	0
Png	1301	1301	0
Exe	4	2	2
Bmp	5	5	0
Html	33	33	0
Gif	113	112	1
Ppt	14	0	14
Total	19.599	19.427	172

5.1.5 Escenario 5 Aplastamiento de forma intencional en investigaciones forenses digitales con una fuerza de 4,75 KN

Tabla 65

Archivos recuperados herramienta Foremost escenario 5 - vehículo mediano

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Bmp	4	4	0
Docx	156	156	0
Exe	6	2	4
Gif	120	2	118
Htm	19	19	0
Jar	1	1	0
Jpg	16712	16379	333
Mov	12	0	12
Pdf	173	173	0
Png	3712	3712	0
Ppt	1	0	1
Rar	86	85	1
Wmv	9	9	0
Xls	1139	1139	0
Total	22.150	21.681	469

Tabla 66

Archivos recuperados herramienta Scalpel escenario 5 - vehículo mediano.

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Avi	11	0	11
Bmp	0	0	0
Doc	6	0	6
Jpg	339	66	273
Mpg	17.000	25	16975
Pdf	33	33	0
Total	17.389	124	17.265

Tabla 67

Archivos recuperados herramienta Adroit escenario 5 - vehículo mediano.

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Jpg	12742	12492	250
Bmp	6	6	0
Gif	116	115	1
Png	2116	1968	148
Total	14.980	14.581	399

Tabla 68

Archivos recuperados herramienta PhotoRec escenario 5 - vehículo mediano

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Rar	68	68	0
Mpg	145	140	5
Doc	307	172	135
Jpg	15637	15637	0
Pdf	166	166	0
Wma	6	6	0
Wmw	7	7	0
Avi	9	1	8
Flv	19	19	0
Ppt	1	1	0
Mp3	30	25	5
Xls	1513	1509	4
Mp4	26	25	1
Png	1297	1297	0
Exe	4	2	2
Bmp	5	5	0
Html	33	33	0
Gif	113	112	1
Ppt	14	0	14
Total	19.400	19.225	175

5.1.6 Escenario 6 Aplastamiento de forma intencional en investigaciones forenses digitales con una fuerza de 11,62 KN

Tabla 69

Archivos recuperados herramienta Foremost escenario 6 - vehículo pesado.

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Bmp	4	4	0
Docx	156	156	0
Exe	4	1	3
Gif	120	2	118
Htm	19	19	0
Rar	88	76	12
Jpg	16680	16334	346
Mov	13	0	13
Pdf	173	0	173
Png	3718	3717	1
Ppt	1	1	0
Wmv	9	9	0
Xlsx	1139	1139	0
Total	22.124	21.458	666

Tabla 70

Archivos recuperados herramienta Scalpel escenario 6 - vehículo pesado.

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Avi	0	0	0
Bmp	0	0	0
Doc	6	0	6
Jpg	339	66	273
Mpg	17.000	17	16.983
Total	17.345	83	17.262

Tabla 71

Archivos recuperados herramienta Adroit escenario 6 - vehículo pesado.

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Jpg	12710	12492	218
Bmp	6	6	0
Gif	116	116	0
Png	2116	1968	148
Total	14.948	14.582	366

Tabla 72

Archivos recuperados herramienta PhotoRec escenario 6 - vehículo pesado.

Formato de archivo	Total, Recuperados	Recuperados	Falsos positivos
Pdf	172	172	0
Exe	3	3	1
Doc	317	235	82
Xlsx	1233	1233	0
Bmp	6	6	0
Jpg	16602	16602	0
Png	635	635	0
Rar	68	68	0
Htm	27	27	0
Gif	115	115	0
Mp4	27	26	1
Ppt	4	1	3
Mpeg	145	145	0
Avi	6	0	6
Mp3	30	30	0
Wmv	6	6	0
Total	19.396	19.304	93

5.1.7 Escenario 7 Golpe con objeto contundente

No se ha podido recuperar debido al daño que tiene el dispositivo SSD

5.1.8 Escenario 8 Humedecimiento

TIEMPO 0 - 10 SEGUNDOS

Tabla 73

Archivos recuperados herramienta Foremost escenario 8 – tiempo 10 segundos

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Bmp	4	4	0
Gif	120	2	18
Jpg	16.680	16630	350
Mov	13	0	13
Png	3718	3310	408
Wmv	9	9	0
Htm	19	19	0
Pdf	173	173	0
Doc	156	156	0
Ppt	1	1	0
Xls	1139	1139	0
Total	22.032	21.443	789

Tabla 74

Archivos recuperados herramienta Scalpel escenario 8 – tiempo 10 segundos

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Bmp	11	0	11
Gif	115	2	113
Jpg	9.724	8677	1047
Mov	26	0	26
Mpg	15490	0	15490
Png	351	0	351
Doc	900	0	900
Htm	39	39	0
Pdf	33	33	0
Wmv	972	72	900
Total	27.661	8.823	18.838

Tabla 75

Archivos recuperados herramienta Adroit escenario 8 – tiempo 10 segundos

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Jpg	11710	11506	204
Bmp	6	6	0
Gif	48	48	0
Png	1514	1394	120
Total	13.278	12.954	324

Tabla 76

Archivos recuperados herramienta PhotoRec escenario 8 – tiempo 10 segundos.

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Pdf	173	173	0
Htm	33	33	0
Doc	315	241	74
Xlsx	1234	1234	0
Ppt	4	2	2
Bmp	6	6	0
Jpg	16605	16605	0
Png	635	635	0
Gif	115	115	0
Mp4	27	26	1
Mpeg	145	145	0
Avi	6	0	6
Mp3	21	21	0
Wmv	6	6	0
Total	19.325	19.242	83

TIEMPO 10 -60 SEGUNDOS

Tabla 77

Archivos recuperados herramienta Foremost escenario 8 – tiempo 30 segundos.

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Bmp	4	4	0
Gif	120	102	18
Jpg	16.678	16327	351
Mov	13	0	13
Png	3718	3310	408
Wmv	9	9	0
Htm	19	19	0
Pdf	173	173	0
Doc	156	156	0
Ppt	1	1	0
Xls	1137	1137	0
Total	22.028	21.238	790

Tabla 78

Archivos recuperados herramienta Scalpel escenario 8 – tiempo 30 segundos

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Bmp	11	0	11
Gif	115	2	113
Jpg	9.723	8676	1047
Mov	26	0	26
Mpg	15490	0	15490
Png	351	0	351
Doc	900	0	900
Htm	39	39	0
Pdf	32	32	0
Total	26.687	8.749	17.938

Tabla 79*Archivos recuperados herramienta PhotoRec escenario 8 – tiempo 30 segundos*

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Pdf	172	172	0
Htm	31	31	0
Doc	317	235	82
Xlsx	1233	1233	0
Ppt	4	1	3
Bmp	6	6	0
Jpg	16602	16602	0
Png	635	635	0
Gif	115	115	0
Mp4	27	26	1
Mpeg	145	145	0
Avi	6	0	6
Mp3	30	30	0
Wmv	6	6	0
Total	19.329	19.237	92

Tabla 80*Archivos recuperados herramienta Adroit escenario 8 – tiempo 30 segundos*

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Jpg	11691	11487	204
Bmp	6	6	0
Gif	39	39	0
Png	1510	1390	120
Total	13.246	12.922	324

MÁS DE 60 SEGUNDOS

Tabla 81*Archivos recuperados herramienta Foremost escenario 8 – tiempo 65 segundos*

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Bmp	4	4	0
Gif	120	102	18
Jpg	16.679	16330	349
Mov	13	0	13
Png	3713	3302	411
Wmv	9	9	0
Htm	19	19	0
Pdf	173	173	0
Doc	156	156	0
Ppt	1	1	0
Xls	1136	1136	0
Total	22.023	21.232	791

Tabla 82*Archivos recuperados herramienta Scalpel escenario 8 – tiempo 65 segundos*

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Bmp	11	0	11
Gif	113	4	109
Jpg	9.721	8669	1052
Mov	26	0	26
Mpg	15490	0	15490
Png	351	0	351
Doc	900	0	900
Htm	35	35	0
Pdf	33	33	0
Total	26.680	8.741	17.939

Tabla 83

Archivos recuperados herramienta PhotoRec escenario 8 – tiempo 65 segundos

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Pdf	172	172	0
Htm	27	27	0
Doc	317	224	93
Xlsx	1231	1231	0
Ppt	4	1	3
Bmp	6	6	0
Jpg	16600	16600	0
Png	635	635	0
Gif	115	115	0
Mp4	27	22	5
Mpeg	145	145	0
Avi	6	0	6
Mp3	30	30	0
Wmv	6	6	0
Total	19.321	19.214	107

Tabla 84

Archivos recuperados herramienta Adroit escenario 8 – tiempo 65 segundos

Formato de archivo	Total, Recuperados	Válidos recuperados	Falsos positivos
Jpg	11710	11489	221
Bmp	6	6	0
Gif	48	46	2
Png	1514	1392	122
Total	13.278	12.933	345

5.2 Evaluar métricas de File Carving

Se realizó un análisis comparativo en tanto a los formatos de archivos que son ofimática y multimedia considerando las siguientes métricas.

- **ART:** Total de archivos recuperados
- **AVR:** Archivos válidos recuperados
- **AFP:** Falsos positivos (Ofimática)
- **APR:** Archivos parcialmente recuperados (Multimedia)

En la tabla 85 se detalla la cantidad de archivos iniciales del dispositivo de almacenamiento SSD.

Tabla 85

Cantidad de archivos iniciales

Tipo de archivo	Cantidad
Pdf	157
Avi	1
Bmp	2
Xls	1090
Gif	50
Html	22
Jpg	7385
Mov	2
Mp3	27
Mp4	24
Png	617
Wmv	14
Doc	158
Xml	7
Flv	19

La evaluación inicia con el análisis del escenario de caídas.

ESCENARIO CAÍDAS PARA ARCHIVOS DE OFIMÁTICA

En la tabla 86 se puede identificar las métricas de File Carving por cada fuerza que se ha aplicado con la herramienta **Foremost** que implementa **Semantic Carving**, donde se puede

observar que los falsos positivos no existen al utilizar esta herramienta, teniendo apenas un falso positivo con la fuerza de 6,480 Newtons, mientras que las fuerzas de los otros escenarios han sido recuperadas de forma exitosa.

Tabla 86

Análisis, caídas utilizando Foremost en archivos de ofimática

Técnicas	Cantidad de archivos iniciales	ART	AVR	AFP	Fuerza
Semantic Carving	1.453	1.491	1.491	0	2,275
		1.488	1.487	1	6,480
		1.489	1.489	0	14,160
		1.469	1.469	0	15,370
		1.452	1.452	0	15,490

El promedio de archivos válidos recuperados con las fuerzas que van de 2,275 a 15,49 Newtons es de **1.478 archivos**.

Con la fuerza de 2,275 Newtons, la herramienta foremost ha recuperado mayor cantidad de información con un total de 1.491 archivos, y en este caso se analizó la información por tipo de archivo como se presenta en la tabla 87. Se puede observar que el número de archivos recuperados es mayor a la cantidad de archivos iniciales.

Tabla 87

Comparación de archivos ofimática, fuerza 2,275 Newtons con foremost

ARCHIVOS INICIALES		ARCHIVOS RECUPERADOS		
Tipo de archivo	Cantidad	Total, Recuperados	Válidos recuperados	Falsos positivos
Pdf	157	173	173	0
Xls	1.090	1.142	1.142	0
Html	22	19	19	0
Doc	158	156	156	0

En la tabla 88 se analiza los archivos recuperados utilizando herramienta **Scalpel** que implementa la técnica **Fragment Recovery Carving**, donde se puede observar que los falsos

positivos son mayores que los válidos recuperados en todas las fuerzas, lo que indica que no tiene una buena recuperación para archivos de tipo ofimática.

Tabla 88

Análisis, caídas utilizando Scalpel en archivos de ofimática

Técnicas	Cantidad de archivos	ART	AVR	AFP	Fuerza
Fragment recovery carving	1.453	999	87	912	2,275
		522	69	453	6,480
		511	66	445	14,160
		972	72	900	15,370
		737	72	665	15,490

El promedio de archivos válidos recuperados con las fuerzas que van de 2,275 a 15,49 Newtons es de **73 archivos**.

Con la fuerza de 2,275 Newtons, la herramienta scalpel ha recuperado mayor cantidad de información con un total de 999 archivos, y en este caso se analizó la información por tipo de archivo como se presenta en la tabla 89. Se puede observar que el número de archivos recuperados es menor a la cantidad de archivos iniciales a diferencia del tipo de archivo doc donde existe un alto índice de archivos duplicados.

Tabla 89

Comparación de archivos ofimática, fuerza 2,275 Newtons con scalpel

ARCHIVOS INICIALES		ARCHIVOS RECUPERADOS		
Tipo de archivo	Cantidad	Total, Recuperados	Válidos recuperados	Falsos positivos
Pdf	157	33	31	2
Html	22	66	56	10
Doc	158	900	0	900

En la tabla 90 se analiza los archivos utilizando herramienta **PhotoRec** que implementa **Semantic Carving**, donde se puede observar que los falsos positivos son menores que los válidos

recuperados en todas las fuerzas lo que indica que tiene una buena recuperación para archivos de tipo ofimática.

Tabla 90

Análisis, caídas utilizando PhotoRec en archivos de ofimática

Técnicas	Cantidad de archivos	ART	AVR	AFP	Fuerza
Semantic Carving	1.453	2.479	2.432	47	2,275
		1.778	1.625	147	6,480
		1.741	1.595	146	14,160
		2.033	1.570	463	15,370
		1.671	1.536	135	15,490

El promedio de archivos válidos recuperados con las fuerzas que van de 2,275 a 15,49 Newtons es de **1.752 archivos**.

Con la fuerza de 2,275 Newtons, la herramienta photorec ha recuperado mayor cantidad de información con un total de 2.479 archivos, y en este caso se analizó la información por tipo de archivo como se presenta en la tabla 91. El número de archivos recuperados es menor a los archivos iniciales como los de tipo xls que de 1.090 apenas se han recuperado 268 archivos.

Tabla 91

Comparación de archivos ofimática, fuerza 2,275 Newtons con photorec

ARCHIVOS INICIALES		ARCHIVOS RECUPERADOS		
Tipo de archivo	Cantidad	Total, Recuperados	Válidos recuperados	Falsos positivos
Xls	1.090	268	268	0
Html	22	4	7	38
Doc	158	163	156	7
Xml	7	3	1	2

ESCENARIO CAÍDAS PARA ARCHIVOS DE MULTIMEDIA

En la tabla 92 se analiza los archivos utilizando herramienta **Foremost** que implementa **Semantic Carving**, donde se puede observar que los archivos parcialmente recuperados son

menores que los válidos recuperados en cada caso de las fuerzas aplicadas, pero aun así son valores representativos que podría contener información valiosa.

Tabla 92

Análisis, caídas utilizando Foremost en archivos multimedia

Técnicas	Cantidad de archivos	ART	AVR	APR	Fuerza
Semantic Carving	8.122	22.231	21.849	382	2,275
		21.953	19.911	2042	6,480
		20.569	20.123	446	14,160
		20.544	19.696	848	15,367
		20.535	19.683	852	15,490

El promedio de archivos válidos recuperados con las fuerzas que van de 2,275 a 15,49 Newtons es de **20.252 archivos**.

Con la fuerza de 2,275 Newtons, la herramienta foremost ha recuperado mayor cantidad de información con un total de 22.231 archivos, y en este caso se analizó la información por tipo de archivo como se presenta en la tabla 93. Se puede observar que el número de archivos recuperados es mayor a los archivos iniciales, teniendo los archivos de tipo jpg con una diferencia de 10.978 que indica que existen archivos recuperados repetidos una o varias veces.

Tabla 93

Comparación de archivos multimedia, fuerza 2,275 Newtons con foremost

ARCHIVOS INICIALES		ARCHIVOS RECUPERADOS		
Tipo de archivo	Cantidad	Total, Recuperados	Válidos recuperados	Falsos positivos
Avi	1	3	3	0
Bmp	2	4	4	0
Gif	50	120	0	120
Jpg	7.385	18.363	18.117	246
Mov	2	13	0	13
Png	617	3.718	3.718	0
Wmv	14	10	7	3

En la tabla 94 se analiza los archivos utilizando herramienta **Scalpel** que implementa **Fragment Recovery Carving**, donde se puede observar que los archivos parcialmente recuperados son mayores que los válidos recuperados en cada caso de las fuerzas aplicadas, por lo que se está perdiendo gran cantidad de información.

Tabla 94

Análisis caídas utilizando Scalpel en archivos multimedia

Técnicas	Cantidad de archivos	ART	AVR	APR	Fuerza
Fragment recovery carving	8.122	22.744	8.176	14.568	2,275
		22.741	8.602	14.139	6,480
		22.729	8.590	14.139	14,160
		25.022	8.297	17.018	15,367
		18.406	6.319	12087	15,490

El promedio de archivos válidos recuperados con las fuerzas que van de 2,275 a 15,49 Newtons es de **8.105 archivos**.

Con la fuerza de 15,367 Newtons, la herramienta scapel ha recuperado mayor cantidad de información con un total de 25.022 archivos, y en este caso se analizó la información por tipo de archivo como se presenta en la tabla 95. Se puede observar que el número de archivos recuperados

es mayor a los archivos iniciales, teniendo los archivos de tipo jpg con una diferencia de 10.978 que indica que existen archivos recuperados repetidos una o varias veces.

Tabla 95

Comparación de archivos multimedia, fuerza 15,367 Newtons con scapel

ARCHIVOS INICIALES		ARCHIVOS RECUPERADOS		
Tipo de archivo	Cantidad	Total, Recuperados	Válidos recuperados	Falsos positivos
Bmp	2	11	0	11
Gif	50	115	2	113
Jpg	7.385	9.300	8.277	1.023
Mov	2	26	0	26
Mpg	24	15.215	0	15.490
Png	617	355	0	355

En la tabla 96 se analiza los archivos utilizando herramienta **PhotoRec** que implementa **Semantic Carving**, donde se puede observar que los archivos parcialmente recuperados son menores que los válidos recuperados en cada caso de las fuerzas aplicadas, y los válidos recuperados tienen una gran cantidad de información que podría recuperarse de forma íntegra.

Tabla 96

Análisis caídas utilizando PhotoRec en archivos multimedia

Técnicas	Cantidad de archivos	ART	AVR	APR	Fuerza
Semantic Carving	8.122	8.205	8.200	5	2,275
		16.620	16.573	47	6,480
		15.003	14.982	21	14,160
		18.752	18.743	9	15,367
		14.945	14.926	19	15,490

El promedio de archivos válidos recuperados con las fuerzas que van de 2,275 a 15,49 Newtons es de **14.685 archivos**.

Con la fuerza de 15,367 Newtons, la herramienta photorec ha recuperado mayor cantidad de información con un total de 18.752 archivos, y en este caso se analizó la información por tipo de

archivo como se presenta en la tabla 97. Se puede observar que el número de archivos recuperados es mayor a los archivos iniciales en cada caso.

Tabla 97

Comparación de archivos multimedia, fuerza 15,367 Newtons con photorec

ARCHIVOS INICIALES		ARCHIVOS RECUPERADOS		
Tipo de archivo	Cantidad	Total, Recuperados	Válidos recuperados	Falsos positivos
Avi	1	9	1	8
Bmp	2	6	6	0
Gif	50	116	115	1
Jpg	7.385	16.471	16.471	0
Mov	2	4	4	0
Png	617	1.965	1.965	0
Wmv	14	181	181	0

En la tabla 98 se analiza los archivos utilizando herramienta **Adroit Photo Recovery** que es especial para archivos de imágenes y que implementa **Fragment Recovery Carving**, donde se puede observar que los archivos parcialmente recuperados son menores que los válidos recuperados en cada caso de las fuerzas aplicadas, y aun así tienen un valor elevado donde podría perderse información valiosa.

Tabla 98

Análisis caídas utilizando Adroit Photo Recovery en archivos multimedia

Técnicas	Cantidad de archivos	ART	AVR	APR	Fuerza
Fragment recovery carving	8.122	37.375	36.197	1.178	2,275
		15.098	14.700	398	6,480
		13.278	12.939	339	14,160
		13.246	12.895	351	15,367
		14.947	14.571	376	15,490

El promedio de archivos válidos recuperados con las fuerzas que van de 2,275 a 15,49 Newtons es de **18.260 archivos**.

Con la fuerza de 6,480 Newtons, la herramienta *adroit photo recovery* ha recuperado mayor cantidad de información con un total de 15.098 archivos, y en este caso se analizó la información por tipo de archivo como se presenta en la tabla 99. Se puede observar que el número de archivos recuperados es mayor a los archivos iniciales en cada caso con varios archivos repetidos.

Tabla 99

Comparación de archivos multimedia, fuerza 6,480 Newtons con adroit

ARCHIVOS INICIALES		ARCHIVOS RECUPERADOS		
Tipo de archivo	Cantidad	Total, Recuperados	Válidos recuperados	Falsos positivos
Bmp	2	6	0	6
Gif	50	116	115	1
Jpg	7.385	12.859	12.616	243
Png	617	2.117	1.969	148

La siguiente evaluación para cada escenario de aplastamiento se detalla a continuación en tanto archivos de tipo ofimática como multimedia.

ESCENARIO APLASTAMIENTO PARA ARCHIVOS DE OFIMÁTICA

En la tabla 100 se analiza los archivos utilizando herramienta **Foremost**, donde se puede observar que los falsos positivos son menores que los válidos recuperados en todas las fuerzas de aplastamiento excepto cuando el dispositivo SSD ha tenido una fuerza de aplastamiento grande de 11,62 KN.

Tabla 100

Análisis caídas utilizando Foremost en archivos de ofimática

Técnicas	Cantidad de archivos	ART	AVR	AFP	Fuerza
Semantic Carving	1.453	1.495	1.494	1	4,020
		1.488	1.487	1	4,750
		1.488	1.315	173	11,620

El promedio de archivos válidos recuperados con las fuerzas que van de 4,020 a 11,620 Kilo Newtons es de **1.432 archivos**.

Con la fuerza de 4,750 y 11,620 Kilo Newtons, la herramienta foremost ha recuperado mayor cantidad de información con un total de 1.488 archivos, pero en el caso de la fuerza mayor el número de falsos positivos es de 173, por lo que se toma la fuerza de 4,750 que ha tenido mayor cantidad de válidos recuperados. En este caso se analizó la información por tipo de archivo como se presenta en la tabla 101. Se puede observar que el número de archivos recuperados teniendo una mayor precisión con los archivos de tipo html.

Tabla 101

Comparación de archivos ofimática, fuerza 6,480 Kilo Newtons con foremost

ARCHIVOS INICIALES		ARCHIVOS RECUPERADOS		
Tipo de archivo	Cantidad	Total, Recuperados	Válidos recuperados	Falsos positivos
Pdf	157	173	173	0
Xls	1.090	1.139	1.139	0
Html	22	19	19	0
Doc	158	156	156	0
Ppt	1	1	0	1

En la tabla 102 se analiza los archivos utilizando herramienta **Scalpel**, donde se puede observar que los falsos positivos en el caso de una fuerza de aplastamiento pequeña de 4,020 kilo newtons es mayor que los válidos recuperados, mientras que el resto de las fuerzas tienen han recuperado de forma mínima este tipo de archivos.

Tabla 102

Análisis aplastamiento utilizando Scalpel en archivos de ofimática

Técnicas	Cantidad de archivos	ART	AVR	AFP	Fuerza
Fragment Recovery	1.453	972	72	900	4,020
Carving		39	33	6	4,750
		6	0	6	11,620

El promedio de archivos válidos recuperados con las fuerzas que van de 4,020 a 11,620 Kilo Newtons es de apenas **35 archivos**.

Con la fuerza de 4,020 Kilo Newtons, la herramienta scalpel ha recuperado mayor cantidad de información con un total de 972 archivos, y en este caso se analizó la información por tipo de archivo como se presenta en la tabla 103. Se puede observar que en el caso de documentos word hay un valor alto de archivos recuperados que son falsos positivos y los pdf tienen una mayor precisión.

Tabla 103

Comparación de archivos ofimática, fuerza 4,020 Kilo Newtons con scalpel

ARCHIVOS INICIALES		ARCHIVOS RECUPERADOS		
Tipo de archivo	Cantidad	Total, Recuperados	Válidos recuperados	Falsos positivos
Pdf	157	33	33	0
Html	22	39	39	0
Doc	158	900	0	900

En la tabla 104 se analiza los archivos utilizando la herramienta **PhotoRec**, donde se puede observar que los falsos positivos son menores que los válidos recuperados, teniendo un valor aceptable de válidos recuperados.

Tabla 104

Análisis aplastamiento utilizando PhotoRec en archivos de ofimática

Técnicas	Cantidad de archivos	ART	AVR	AFP	Fuerza
Semantic Carving	1.453	1.733	1.717	16	4,020
		2.034	1.881	153	4,750
		1.753	1.668	85	11,620

El promedio de archivos válidos recuperados con las fuerzas que van de 4,020 a 11,620 Kilo Newtons es de **1.755 archivos**.

Con la fuerza de 4,750 Kilo Newtons, la herramienta photorec ha recuperado mayor cantidad de información con un total de 2.034 archivos, y en este caso se analizó la información por tipo de archivo como se presenta en la tabla 105. Se puede observar que existe gran cantidad de duplicados en los archivos xlsx.

Tabla 105

Comparación de archivos ofimática, fuerza 4,750 Kilo Newtons con photorec

ARCHIVOS INICIALES		ARCHIVOS RECUPERADOS		
Tipo de archivo	Cantidad	Total, Recuperados	Válidos recuperados	Falsos positivos
Pdf	157	166	166	0
Xls	1.090	1.513	1.509	4
Html	22	33	33	0
Doc	158	307	172	135
Ppt	1	15	1	14

ESCENARIO APLASTAMIENTO PARA ARCHIVOS MULTIMEDIA

En la tabla 106 se analiza los archivos recuperados utilizando la herramienta **Foremost**, donde se puede observar que los archivos parcialmente recuperados son menores que los válidos recuperados, teniendo un valor aceptable de válidos recuperados.

Tabla 106

Análisis aplastamiento utilizando Foremost en archivos multimedia

Técnicas	Cantidad de archivos	ART	AVR	APR	Fuerza
Semantic Carving	8.122	20.803	20.418	385	4,020
		20.569	20.106	463	4,750
		20.544	20.066	478	11,620

El promedio de archivos válidos recuperados con las fuerzas que van de 4,020 a 11,620 Kilo Newtons es de **20.197 archivos**.

Con la fuerza de 4,020 Kilo Newtons, la herramienta foremost ha recuperado mayor cantidad de información con un total de 20.803 archivos, y en este caso se analizó la información por tipo

de archivo como se presenta en la tabla 107. Se puede observar que existe gran cantidad de duplicados en los archivos en todos los tipos.

Tabla 107

Comparación de archivos multimedia, fuerza 4,020 Kilo Newtons con foremost

ARCHIVOS INICIALES		ARCHIVOS RECUPERADOS		
Tipo de archivo	Cantidad	Total, Recuperados	Válidos recuperados	Falsos positivos
Bmp	2	4	4	0
Gif	50	120	2	118
Jpg	7.385	16.932	16.677	255
Mov	2	12	0	12
Png	617	3.726	3.726	0
Wmv	14	9	9	0

En la tabla 108 se analiza los archivos utilizando la herramienta **Scalpel**, donde se puede observar que los archivos parcialmente recuperados son mayores casi en totalidad de todos los archivos recuperados, sin tener gran cantidad de datos íntegros.

Tabla 108

Análisis aplastamiento utilizando Scalpel en archivos multimedia

Técnicas	Cantidad de archivos	ART	AVR	APR	Fuerza
Fragment	8.122	25.717	8.679	17.038	4,020
Recovery		17.350	91	17.259	4,750
Carving		17.339	83	17.256	11,620

El promedio de archivos válidos recuperados con las fuerzas que van de 4,020 a 11,620 Kilo Newtons es de **2.951 archivos**.

Con la fuerza de 4,020 Kilo Newtons, la herramienta scalpel ha recuperado mayor cantidad de información con un total de 25.717 archivos, y en este caso se analizó la información por tipo de archivo como se presenta en la tabla 109. Se puede observar que existe gran cantidad de duplicados en los archivos en todos los tipos en especial en los de archivos de tipo Mpg.

Tabla 109

Comparación de archivos multimedia, fuerza 4,020 Kilo Newtons con scalpel

ARCHIVOS INICIALES		ARCHIVOS RECUPERADOS		
Tipo de archivo	Cantidad	Total, Recuperados	Válidos recuperados	Falsos positivos
Bmp	2	11	0	11
Gif	50	115	2	113
Jpg	7.385	9.724	8.677	1.047
Mov	2	26	0	26
Mpg	24	15.490	0	15.490
Png	617	351	0	351

En la tabla 110 se analiza los archivos utilizando la herramienta **PhotoRec**, donde se puede observar que los archivos parcialmente recuperados son mínimos, lo que indica que se tendrá la mayor cantidad de datos de forma íntegra.

Tabla 110

Análisis aplastamiento utilizando PhotoRec en archivos multimedia

Técnicas	Cantidad de archivos	ART	AVR	APR	Fuerza
Semantic Carving	8.122	17.487	17.468	19	4,020
		17.294	17.274	20	4,750
		17.272	17.265	7	11,620

El promedio de archivos válidos recuperados con las fuerzas que van de 4,020 a 11,620 Kilo Newtons es de **17.336 archivos**.

Con la fuerza de 4,020 Kilo Newtons, la herramienta photorec ha recuperado mayor cantidad de información con un total de 17.487 archivos, y en este caso se analizó la información por tipo de archivo como se presenta en la tabla 111. Se puede observar que existe gran cantidad de duplicados en los archivos en todos los tipos en especial en los de archivos de tipo Jpg, Png y Mpg.

Tabla 111

Comparación de archivos multimedia, fuerza 4,020 Kilo Newtons con photorec

ARCHIVOS INICIALES		ARCHIVOS RECUPERADOS		
Tipo de archivo	Cantidad	Total, Recuperados	Válidos recuperados	Falsos positivos
Avi	1	9	1	8
Bmp	2	5	5	0
Gif	50	113	112	1
Jpg	7.385	15.826	15.826	0
Mp3	27	30	25	5
Mp4	24	26	26	0
Png	617	1.301	1.301	0
Wmv	14	7	7	0
Flv	19	19	19	0
Mpg	0	145	140	5
Wma	0	6	6	0

En la tabla 112 se analiza los archivos utilizando la herramienta **Adroit Photo Recovery**, donde se puede observar que los archivos parcialmente recuperados son menores que los válidos a pesar de que sea un valor representativo donde podría perderse información valiosa.

Tabla 112

Análisis aplastamiento utilizando Adroit Photo Recovery en archivos multimedia

Técnicas	Cantidad de archivos	ART	AVR	APR	Fuerza
Fragment Recovery	8.122	15.072	14.728	344	4,020
Carving		14.980	14.581	399	4,750
		14.948	14.582	366	11,620

El promedio de archivos válidos recuperados con las fuerzas que van de 4,020 a 11,620 Kilo Newtons es de **14.630 archivos**.

Con la fuerza de 4,020 Kilo Newtons, la herramienta adroit photo recovery, ha recuperado mayor cantidad de información con un total de 15.072 archivos, y en este caso se analizó la información por tipo de archivo como se presenta en la tabla 113. Se puede observar que existe un alto número de archivos duplicados para todos los casos.

Tabla 113

Comparación de archivos multimedia, fuerza 4,020 Kilo Newtons con adroit

ARCHIVOS INICIALES		ARCHIVOS RECUPERADOS		
Tipo de archivo	Cantidad	Total, Recuperados	Válidos recuperados	Falsos positivos
Bmp	2	6	6	0
Gif	50	116	115	1
Jpg	7.385	12.822	12.591	231
Png	617	2.128	2.016	112

Finalmente, la evaluación se realiza para los escenarios de humedecimiento tanto para archivos de ofimática como archivos multimedia.

ESCENARIO HUMEDECIMIENTO PARA ARCHIVOS OFIMÁTICA

En la tabla 114 se analiza los archivos utilizando la herramienta **Foremost**, donde se puede observar que no tiene falsos positivos, lo que significa que la información recuperada ha sido de forma íntegra.

Tabla 114

Análisis humedecimiento utilizando Foremost en archivos de ofimática

Técnicas	Cantidad de archivos	ART	AVR	AFP	Tiempo segundo
Semantic Carving	1.453	1.488	1.488	0	10,000
		1.486	1.486	0	30,000
		1.485	1.485	0	65,000

El promedio de archivos válidos recuperados de dispositivos SSD que han estado sumergidos en agua, que van desde 10 segundos a 65 segundos es de **1.486 archivos**.

Con el tiempo de 10 segundos, la herramienta foremost, ha recuperado mayor cantidad de información con un total de 1.488 archivos, y en este caso se analizó la información por tipo de archivo como se presenta en la tabla 115. Se puede observar que en los tipos de archivos word es quien tiene una mayor precisión.

Tabla 115

Comparación de archivos ofimática, tiempo 10 segundos con foremost

ARCHIVOS INICIALES		ARCHIVOS RECUPERADOS		
Tipo de archivo	Cantidad	Total, Recuperados	Válidos recuperados	Falsos positivos
Pdf	157	173	173	0
Xls	1.090	1.139	1.139	0
Html	22	19	19	0
Doc	158	156	156	0
Ppt	1	1	1	0

En la tabla 116 se analiza los archivos utilizando la herramienta **Scalpel**, donde se puede observar que tiene una gran cantidad de falsos positivos, donde se pierde la información de los archivos de ofimática.

Tabla 116

Análisis humedecimiento utilizando Scalpel en archivos de ofimática

Técnicas	Cantidad de archivos	ART	AVR	AFP	Tiempo segundo
Fragment	1.453	972	72	900	10,000
Recovery		971	71	900	30,000
Carving		968	68	900	65,000

El promedio de archivos válidos recuperados de dispositivos SSD que han estado sumergidos en agua, que van desde 10 segundos a 65 segundos es de **70 archivos**.

Con el tiempo de 10 segundos, la herramienta scalpel, ha recuperado mayor cantidad de información con un total de 972 archivos, y en este caso se analizó la información por tipo de archivo como se presenta en la tabla 117. Se puede observar que en los tipos de archivos word es quien tiene una mayor precisión.

Tabla 117

Comparación de archivos ofimática, tiempo 10 segundos con scalpel

ARCHIVOS INICIALES		ARCHIVOS RECUPERADOS		
Tipo de archivo	Cantidad	Total, Recuperados	Válidos recuperados	Falsos positivos
Pdf	157	33	33	0
Html	22	39	39	0
Doc	158	900	0	900

En la tabla 118 se analiza los archivos utilizando la herramienta **PhotoRec**, donde se puede observar que los falsos positivos son menores que los válidos recuperados, pero no deja de ser un valor representativo.

Tabla 118

Análisis humedecimiento utilizando PhotoRec en archivos de ofimática

Técnicas	Cantidad de archivos	ART	AVR	AFP	Tiempo segundo
Semantic Carving	1.453	1.759	1.683	76	10,000
		1.757	1.672	85	30,000
		1.751	1.655	96	65,000

El promedio de archivos válidos recuperados de dispositivos SSD que han estado sumergidos en agua, que van desde 10 segundos a 65 segundos es de **1.670 archivos**.

Con el tiempo de 10 segundos, la herramienta photorec, ha recuperado mayor cantidad de información con un total de 1.759 archivos, y en este caso se analizó la información por tipo de archivo como se presenta en la tabla 119. Se puede observar que los archivos recuperados de tipo pdf y htm tienen menor número de duplicados.

Tabla 119

Comparación de archivos ofimática, tiempo 10 segundos con photorec

ARCHIVOS INICIALES		ARCHIVOS RECUPERADOS		
Tipo de archivo	Cantidad	Total, Recuperados	Válidos recuperados	Falsos positivos
Pdf	157	173	173	0
Xls	1.090	1.234	1.234	0
Html	22	33	33	0
Doc	158	315	241	74
Ppt	1	4	2	2

ESCENARIO HUMEDECIMIENTO PARA ARCHIVOS MULTIMEDIA

En la tabla 120 se analiza los archivos utilizando la herramienta **Foremost**, donde se puede observar que los archivos parcialmente recuperados son representativos ya que podrían tener gran cantidad de información.

Tabla 120

Análisis humedecimiento utilizando Foremost en archivos multimedia

Técnicas	Cantidad de archivos	ART	AVR	APR	Tiempo segundo
Semantic Carving	8.122	20.544	19.955	789	10,000
		20.542	19.752	790	30,000
		20.538	19.747	791	65,000

El promedio de archivos válidos recuperados de dispositivos SSD que han estado sumergidos en agua, que van desde 10 segundos a 65 segundos es de **19.818 archivos**.

Con el tiempo de 10 segundos, la herramienta foremost, ha recuperado mayor cantidad de información con un total de 20.544 archivos, y en este caso se analizó la información por tipo de archivo como se presenta en la tabla 121. Se puede observar la mayor cantidad de archivos recuperados de tipo jpg y png tiene varios duplicados.

Tabla 121

Comparación de archivos multimedia, tiempo 10 segundos con foremost

ARCHIVOS INICIALES		ARCHIVOS RECUPERADOS		
Tipo de archivo	Cantidad	Total, Recuperados	Válidos recuperados	Falsos positivos
Bmp	2	4	4	0
Gif	50	120	2	18
Jpg	7.385	16.680	16.630	350
Mov	2	13	0	13
Png	617	3.718	3.310	408
Wmv	14	9	9	0

En la tabla 122 se analiza los archivos utilizando la herramienta **Scapel**, donde se puede observar que los archivos parcialmente recuperados superan a los válidos recuperados.

Tabla 122

Análisis humedecimiento utilizando Scalpel en archivos multimedia

Técnicas	Cantidad de archivos	ART	AVR	APR	Tiempo segundo
Fragment Recovery Carving	8.122	25.717	8.679	17.038	10,000
		25.716	8.678	17.038	30,000
		25.712	8.673	17.039	65,000

El promedio de archivos válidos recuperados de dispositivos SSD que han estado sumergidos en agua, que van desde 10 segundos a 65 segundos es **de 8.676 archivos**.

Con el tiempo de 10 segundos, la herramienta scalpel, ha recuperado mayor cantidad de información con un total de 25.717 archivos, y en este caso se analizó la información por tipo de archivo como se presenta en la tabla 123. Se puede observar que en todos los casos existen duplicados.

Tabla 123

Comparación de archivos multimedia, tiempo 10 segundos con scalpel

ARCHIVOS INICIALES		ARCHIVOS RECUPERADOS		
Tipo de archivo	Cantidad	Total, Recuperados	Válidos recuperados	Falsos positivos
Bmp	2	11	0	11
Gif	50	115	2	113
Jpg	7.385	9.724	8.677	1.047
Mov	2	26	0	26
Mpg	24	15.490	0	15.490
Png	617	351	0	351

En la tabla 124 se analiza los archivos utilizando la herramienta **PhotoRec**, donde se puede observar que no los archivos parcialmente recuperados para cada caso son mínimos por lo que la mayoría de los archivos multimedia que son recuperados son íntegros.

Tabla 124

Análisis humedecimiento utilizando PhotoRec en archivos multimedia

Técnicas	Cantidad de archivos	ART	AVR	APR	Tiempo segundo
Semantic Carving	8.122	17.566	17.559	7	10,000
		17.572	17.565	7	30,000
		17.570	17.559	11	65,000

El promedio de archivos válidos recuperados de dispositivos SSD que han estado sumergidos en agua, que van desde 10 segundos a 65 segundos es de **17.561 archivos**.

Con el tiempo de 30 segundos, la herramienta photorec, ha recuperado mayor cantidad de información con un total de 17.572 archivos, y en este caso se analizó la información por tipo de archivo como se presenta en la tabla 125. Se puede observar que en todos los casos existen duplicados, donde el tipo de archivo Wmv es el más preciso.

Tabla 125

Comparación de archivos multimedia, tiempo 30 segundos con photorec

ARCHIVOS INICIALES		ARCHIVOS RECUPERADOS		
Tipo de archivo	Cantidad	Total, Recuperados	Válidos recuperados	Falsos positivos
Avi	1	6	0	6
Bmp	2	6	6	0
Gif	50	115	115	0
Jpg	7.385	16.602	16.602	0
Mp3	27	30	30	0
Mp4	24	27	26	1
Png	617	635	635	0
Wmv	14	6	6	0
Mpg	0	145	145	0

En la tabla 126 se analiza los archivos utilizando la herramienta **Adroit Photo Recovery**, donde se puede observar que no los archivos parcialmente recuperados para cada caso son menos que los válidos recuperados y son un número representativo que no asegura la integridad en la recuperación de datos.

Tabla 126

Análisis humedecimiento utilizando Adroit en archivos multimedia

Técnicas	Cantidad de archivos	ART	AVR	APR	Tiempo segundo
Fragment Recovery Carving	8.122	13.278	12.954	324	10,000
		13.246	12.922	324	30,000
		13.278	12.933	345	65,000

El promedio de archivos válidos recuperados de dispositivos SSD que han estado sumergidos en agua, que van desde 10 segundos a 65 segundos es de **12.936 archivos**.

Con el tiempo de 10 y 65 segundos, la herramienta adroit photo recovery, ha recuperado mayor cantidad de información con un total de 13.278 archivos, y en este caso se analizó la información por tipo de archivo como se presenta en la tabla 127 considerando el tiempo de 10 segundos ya que tiene menor cantidad de falsos positivos. Se puede observar que en todos los casos existen duplicados en especial el tipo de archivo jpg con un alto índice.

Tabla 127

Comparación de archivos multimedia, tiempo 10 segundos con photorec

ARCHIVOS INICIALES		ARCHIVOS RECUPERADOS		
Tipo de archivo	Cantidad	Total, Recuperados	Válidos recuperados	Falsos positivos
Bmp	2	6	6	0
Gif	50	48	48	0
Jpg	7.385	11.710	11.506	204
Png	617	1.514	1.394	120

5.3 Discusión de resultados

A partir del promedio obtenido de los archivos válidos recuperados en cada escenario se presenta la tabla 128 de resumen para el caso de los archivos de tipo ofimática.

Tabla 128

Archivos válidos recuperados ofimática

Herramienta	Caídas	Aplastamiento	Humedecimiento
Foremost	1478	1432	1486
Scalpel	73	35	70
PhotoRec	1752	1755	1670

En la figura 102 se puede apreciar que la herramienta Scalpel que implementa fragment recovery carving, ha tenido el menor promedio de recuperación de datos como mínimo es 35 archivos, seguido de Foremost que implementa semantic carving para el sistema operativo Kali Linux, finalmente le sigue PhotoRec para Windows tiene un promedio de recuperación alto para todos los escenarios con 1.755 archivos en el caso de aplastamiento.

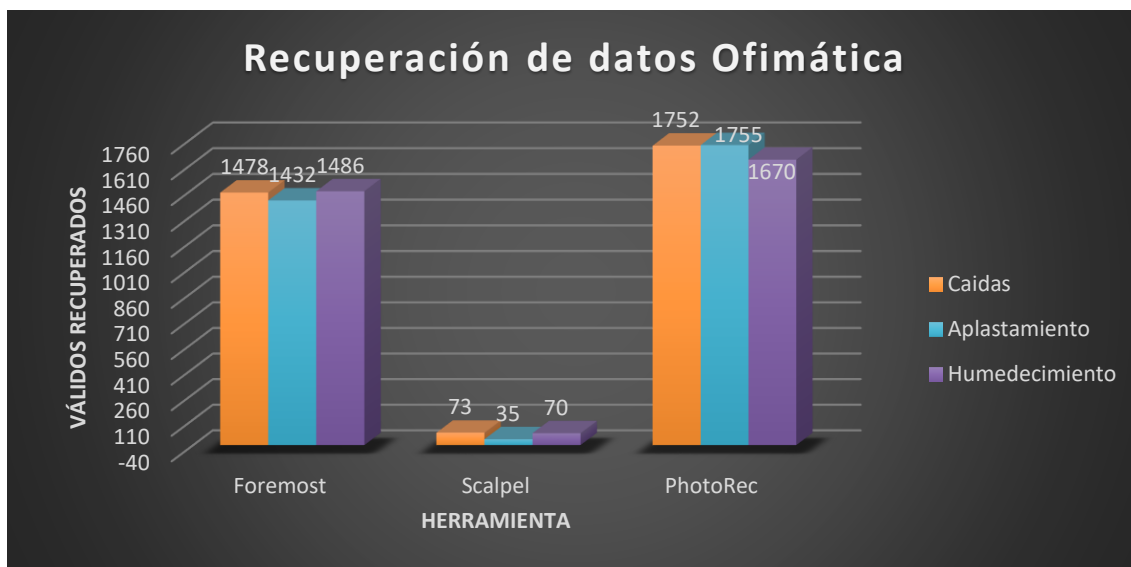


Figura 102 Archivos válidos recuperados ofimática

Se presenta la tabla 129 de resumen para el caso de los archivos de tipo multimedia

Tabla 129

Archivos válidos recuperados multimedia

Herramienta	Caídas	Aplastamiento	Humedecimiento
Foremost	20252	20197	19818
Scalpel	8105	2951	8676
PhotoRec	14685	17336	17561
Adroit Photo Recovery	18340	14630	12936

En la figura 103 se puede apreciar que la herramienta Scalpel que implementa fragment recovery carving para los archivos multimedia, tiene válidos recuperados en menor cantidad que el resto de las herramientas, siendo Foremost quien lidera la lista y es la mejor herramienta y técnica al recuperar archivos multimedia con mayor cantidad de datos íntegros.

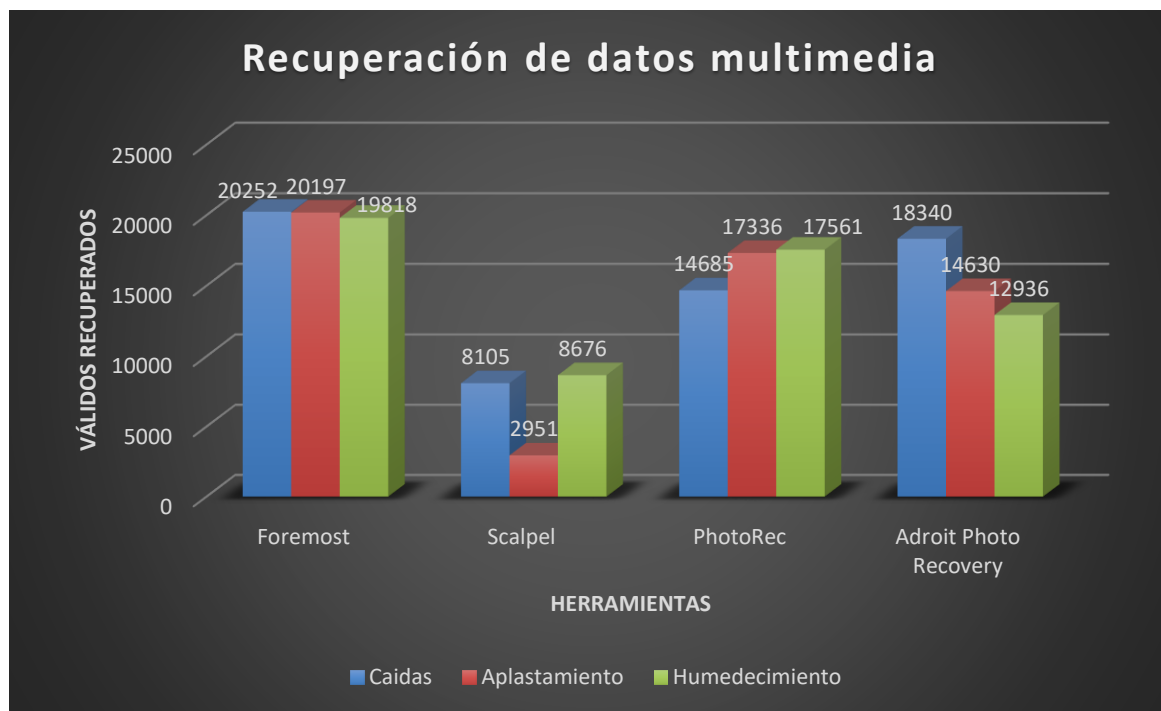


Figura 103 Archivos válidos recuperados ofimática

CAPÍTULO VI

CONCLUSIONES Y LÍNEAS DE TRABAJO FUTURO

6.1 Conclusiones

- Se elabora una propuesta metodológica para recuperación de información en dispositivos de almacenamiento SSD, en base de una investigación experimental que considera varios escenarios de afectación por condiciones ambientales o antrópicas como: caída, aplastamiento, golpe con objeto contundente y humedad.
- La herramienta Foremost que utiliza la técnica Semantic Carving, es una de las que permiten recuperar la mayor cantidad de archivos válidos tanto para formatos de ofimática como de multimedia, además permite recuperar íntegramente documentos de ofimática y en forma parcial los archivos de multimedia.
- La herramienta PhotoRec que utiliza también la técnica Semantic Carving, es otra de las que permiten recuperar la mayor cantidad de archivos válidos, tanto para formatos de ofimática como de multimedia. A pesar de ser la herramienta con los mejores resultados, presenta un mayor número de falsos positivos que Foremost en archivos .doc y los archivos de otro formato no tienen problema para ser recuperados.
- Los dispositivos de estado sólido SSD son muy resistentes al daño por caída mayor a 11 metros, pero en cambio al sufrir un golpe con objeto contundente superior a 335,455 Newtons el daño es significativo y no se puede recuperar la información.

6.2 Recomendaciones

- Elaborar un modelo matemático para predecir la cantidad de información a ser recuperada, de acuerdo a cada escenario, en el que se realice un número de experimentos que permitan tener confiabilidad en el modelo.
- Hacer conocer a los constructores de las herramientas de carving: Foremost y PhotoRec, los resultados de esta experimentación, con el objeto de que realicen un análisis de sus productos, a fin de determinar la razón de estos resultados y los procesos de mejora que podrían tener en nuevas versiones.
- En el caso de que un dispositivo de almacenamiento SSD no sea reconocido bajo ningún concepto se recomienda utilizar herramientas otras interfaces que son utilizadas en sitios especializados de recuperación de datos.

6.3 Líneas de trabajos futuros

Como un trabajo futuro sobre esta investigación se propone la estandarización de una metodología de recuperación de datos y la elaboración de un modelo predictivo de cantidad de información que puede ser recuperada bajo los escenarios propuestos.

BIBLIOGRAFÍA

- Aldaej, A., Gulam, M., & Yousuf, M. (2017). Solid state drive data recovery in open source environment. *IEEE Xplore*, 228 - 231.
- Alherbawi, N., Shukur, Z., & Sulaiman, R. (2016). A Survey on Data Carving in Digital Forensic. *Asian Journal of Information Technology*, 15(24), 5137-5144.
- Aljumah, A., Yousuf Uddin, M., & Gulam Ahamad, M. (2014). Comparison between File Carving from Disk Drive and Disk Image in Open Source Environment. *IEEE Xplore*, 1-4.
- Allauto*. (2016). Obtenido de Allauto: <http://allauto.biz/car/skoda/octavia/1-9-tdi-dsg-105/photos/>
- Arnoldo. (20 de 09 de 2014). *MySite*. Obtenido de MySite: <http://ex-sheffield.org/soloparaingenierosnet/2014/09/20/terremotos-y-computadoras/>
- Automovilescolombia*. (2017). Obtenido de Automovilescolombia: https://automovilescolombia.com/vehiculos/land_rover/range_rover_evoque/fichatecnica/medidas-capacidades
- AutomovilesColombia*. (2017). Obtenido de AutomovilesColombia: <https://automovilescolombia.com/vehiculos/suzuki/grand-vitara/fichatecnica/medidas-capacidades>
- B&S Recuperación de datos. (2017). *B&S Recuperación de datos*. Obtenido de B&S Recuperación de datos: http://www.bs.com.pe/datos/recuperacion_de_datos_que_es.php
- Beeler, Brian;. (8 de 01 de 2012). *StorageReview*. Obtenido de StorageReview: http://www.storagereview.com/ocz_enterprise_ssds_on_display_storage_visions_2012

Cao, T., Vaz Salles, M., & Sowell, B. (2011). Fast Checkpoint Recovery Algorithms for Frequently Consistent Applications. *ACM*, 265-276.

CGSECURITY. (18 de 04 de 2015). Obtenido de *CGSECURITY*:
http://www.cgsecurity.org/wiki/PhotoRec_ES

CGSecurity-TestDisk. (18 de 04 de 2015). Obtenido de *CGSecurity-TestDisk*:
<http://www.cgsecurity.org/wiki/TestDisk>

Chevrolet. (2017). Obtenido de *Chevrolet*: <http://www.chevrolet.com.ec/aveo-family-auto-economico/especificaciones.html>

Chevrolet. (2017). Obtenido de *Chevrolet*:
http://www.chevrolet.com.ec/content/dam/Chevrolet/lat-am/Ecuador/nscwebsite/es/Home/Cars/Aveo_Family/Model_Overview/02_pdf/Hoja_t%C3%A9cnica_Aveo_Family.pdf

Chevrolet-Trucks. (2017). Obtenido de *Chevrolet-Trucks*:
http://www.chevrolet.com.ec/content/dam/Chevrolet/lat-am/Ecuador/nscwebsite/es/Home/Trucks/FSR/02_PDF/C_FSR34N-2.pdf

Christiaan Beek. (s.f.). *McAfee*. Obtenido de *McAfee*:
<https://pdfs.semanticscholar.org/0438/28f3a1e8809e67dd8d6047ad3fa763dde312.pdf>

Cohen, M. I. (2008). Advanced Jpeg Carving. *ACM*, 16.

Constanzo, B., & Waimann, J. (2012). El estado actual de las Técnicas de File Carving y la necesidad de Nuevas Tecnologías que implementen Carving Inteligente. *Journal CADI*.

Cox, A. (10 de 08 de 2011). *Flash Memory summit*. Obtenido de Flash Memory summit: https://www.flashmemorysummit.com/English/Collaterals/Proceedings/2011/20110810_T1B_Cox.pdf

Crisros. (25 de 05 de 2013). *Arquitectura de Computadoras*. Recuperado el 24 de 10 de 2017, de *Arquitectura de Computadoras*: <https://arquitecturadecomputadora.wordpress.com/category/metodos-de-almacenamiento/>

DARNOWSKI, F., & CHOJNACKI, A. (2015). Selected Methods of File Carving and Analysis of Digital Storage Media in Computer Forensics. *Przełąd Teleinformatyczny*, 25-40.

Di Iorio, A. H., Castellote, M., Podestá, A., Greco, F., Constanzo, B., & Waimann, J. (2013). El framework CIRA, un aporte a las técnicas de file carving. *Google Scholar*.

Diffen. (s.f.). Obtenido de Diffen: <http://www.diffen.com/difference/Image:SDRAM.jpg>

Digital Inteliigence. (2017). Obtenido de Digital Inteliigence: <https://www.digitalintelligence.com/software/accessdata/forensic toolkit/>

EcuRed. (17 de 11 de 2012). Obtenido de EcuRed: <http://www.ecured.cu/index.php/SSD>

Eleconomista.es. (21 de 11 de 2017). Obtenido de Eleconomista.es: <http://www.eleconomista.es/tecnologia/noticias/8758290/11/17/La-importancia-del-almacenamiento-de-datos-en-el-nuevo-entorno-digital.html>

Esra'a Alshammary, A. H. (2016). Reviewing and Evaluating Existing File Carving. 2016 Cybersecurity and Cyberforensics Conference (págs. 55-59). Jordan: IEEE. *IEEE Xplore*, 55-59.

FlacsoAndes. (2012). Recuperado el 2018, de FlacsoAndes: <http://www.flacsoandes.edu.ec/biblio/catalog/resGet.php?resId=17830>

Forensics II. (2016). Recuperado el 20 de 02 de 2018, de Forensics II: http://users.du.se/~hjo/cs/dt2016/presentation/extra_carving_w4.pdf

Forensicswiki. (10 de 06 de 2015). Obtenido de Forensicswiki: http://www.forensicswiki.org/wiki/Bulk_extractor

García, Alberto;. (19 de 05 de 2017). *ADSLZONE*. Obtenido de ADSLZONE: <https://www.adslzone.net/2017/05/19/cuanto-consume-cada-componente-del-ordenador/>

GNU. (21 de 02 de 2017). Obtenido de GNU: <https://www.gnu.org/software/ddrescue/>

Guo, Y. (2010). Data recovery function testing for digital forensic tools. *SpringerLink*, 297-311.

Hausser, Tann;. (2013). *GNU/Linux y cultura Geek*. Obtenido de GNU/Linux y cultura Geek: <https://lamiradadelreplicante.com/2013/12/09/recuperar-archivos-borrados-con-scalpel/>

Humphries, Suzanne;. (2017). *TopTenReviews*. Obtenido de <http://www.toptenreviews.com/software/multimedia/best-photo-recovery-software/adroit-photo-recovery-review/>

Hyperphysics. (2017). Recuperado el 21 de 02 de 2018, de Hyperphysics: <http://hyperphysics.phy-astr.gsu.edu/hbasees/flobi.html>

IBM. (24 de 05 de 2017). *IBM*. Recuperado el 13 de 09 de 2017, de IBM: <https://www.ibm.com/support/knowledgecenter/en/POWER8/p8ebj/arebjsolidstatedrives.htm>

IRcovery. (25 de 09 de 2017). Curso intensivo / Conviértete en data specialist en recuperación de datos y análisis forense. Bogotá.

- IsoBuster*. (2017). Obtenido de IsoBuster:
https://www.isobuster.com/es/help/configuraciones_de_recuperacion_de_datos
- Jacecuador*. (2015). Obtenido de Jacecuador: <http://www.jacecuador.com/en/jac-sunray-carga/>
- Jiménez, Ángel;. (02 de 11 de 2011). *El Mundo*. Obtenido de El Mundo:
<http://www.elmundo.es/blogs/elmundo/el-gadgetoblog/2011/11/02/la-crisis-del-disco-duro.html>
- Kali Tools*. . (18 de 02 de 2014). Obtenido de Kali Tools. : <http://tools.kali.org/forensics/foremost>
- Kaspersky*. (10 de 04 de 2017). Recuperado el 24 de 01 de 2017, de Kaspersky:
<https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/>
- MacKenzie, R., & Scorell, M. (2008). Recovery of Circumstantial Digital Evidence Leading to an Anton Piller Order: A Case Study. *ACM*, 20.
- Maturana, J. (23 de 01 de 2014). *Xataka*. Obtenido de Xataka:
<https://www.xataka.com/componentes/instala-un-ssd-en-tu-portatil-y-dale-una-nueva-vida>
- Mayoraz, Guillermo;. (06 de 06 de 2016). *Tecnovortex*. Obtenido de
<https://tecnovortex.com/cuanto-dura-la-informacion-en-un-ssd/>
- Nimlotx. (29 de 05 de 2013). *Electrónica fácil*. Obtenido de Electrónica fácil:
<https://arquitecturaumg.wordpress.com/2013/05/29/discos-duros-con-interfaz-sata/>
- Ninahualpa, G., Diaz, J., & Gunn, S. (2017). Data Restoration and File Carving. *IEEE Xplore*, 1-5.

Noelia Hernández. (16 de 10 de 2013). *Computerhoy*. Obtenido de Computerhoy: <http://computerhoy.com/noticias/hardware/como-funcionan-sistemas-recuperacion-datos-6768>

Nuncic, Michael;. (03 de 04 de 2017). *KrollOntrack*. Obtenido de KrollOntrack: <https://www.ontrackdatarecovery.es/blog/cual-es-la-principal-causa-mundial-de-perdidas-de-datos-de-2016/>

Osteguna. (2005). *Gobierno de España*. Obtenido de Gobierno de España: <http://recursostic.educacion.es/observatorio/web/eu/equipamiento-tecnologico/hardware/250-eduardo-quiroya-gomez>

Oyanedel, Juan Pablo. (18 de 06 de 2013). *Fayerwayer*. Obtenido de Fayerwayer: <https://www.fayerwayer.com/2013/06/todo-lo-que-debes-saber-sobre-las-unidades-de-estado-solido-ssd/>

Papiewski, John;. (s.f.). *Techlandia*. Obtenido de Techlandia: https://techlandia.com/unidad-cinta-magnetica-hechos_393321/

pcmag.com. (05 de 07 de 2017). *pcmag.com*. Recuperado el 13 de 09 de 2017, de pcmag.com: <http://latam.pcmag.com/dispositivos-almacen-reviews-comparativos/123/feature/ssd-vs-hdd-cual-es-la-diferencia>

Penalva, Javier;. (11 de 02 de 2017). *Xataka*. Obtenido de Xataka: <https://www.xataka.com/especiales/ssd-contra-disco-duro-asi-mejora-el-rendimiento-un-portatil-de-mas-de-7-anos-con-un-ssd-de-50-euros>

Pérez García, M. (2011). *Recuperación de información en discos duros electromecánicos a nivel físico y lógico para su análisis forense informático*. México D.F.

Pérez Romero, V;. (02 de 06 de 2016). *ComputerHoy*. Obtenido de ComputerHoy:
<http://computerhoy.com/noticias/hardware/fiabilidad-discos-ssd-mito-realidad-45914>

Plazola Cisneros, A. (2017). *Enciclopedia de Arquitectura Plazola*. Obtenido de
<https://es.scribd.com/document/365138885/plazola-arquitectura-habitacional-iii-pdf>

Poisel, R., Tjoa, S., & Tavolato, P. (2011). Advanced file carving approaches for multimedia files. *JoWUA*, 42-58. Obtenido de Researchgate.

Raj Kumar, A. R., & Renju Mathew, A. (2016). A Method for Carving Fragmented Document and Image Files. *Ieee Xplore*, 1-6.

Rebollo Pedruelo, M. (29 de 11 de 2011). *Universidad Politécnica de Valencia*. Recuperado el 19 de 10 de 2017, de Universidad Politécnica de Valencia: <http://hdl.handle.net/10251/13706>

RecoveryLabs. (04 de 2017). Recuperado el 20 de 01 de 2018, de RecoveryLabs:
<http://www.recoverylabs.com/sala-de-prensa/mas-del-60-de-casos-de-peritaje-informatico-se-deben-sabotaje-en-las-empresas-segun-recovery-labs/>

Ruiz, Christopher;. (04 de 10 de 2012). *Slideshare*. Obtenido de Slideshare:
<https://es.slideshare.net/vincent250miles/modelos-de-cargas-para-puentes>

Ruiz, M. (11 de 2005). *Recovery Labs*. Obtenido de Recovery Labs:
<http://www.recoverylabs.com/sala-de-prensa/la-importancia-de-los-datos/>

RuSolut. (s.f.). Obtenido de RuSolut: <https://rusolut.com/analysis-of-bit-errors-in-nand/>

Seguridad Digital INAP. (s.f.). Obtenido de
https://seguridad.inap.es/almacenamiento_de_la_informacion.html

Simson, G. (2007). Carving contiguous and fragmented files with fast object validation. *ScienceDirect*, S2-S12.

Takeuchi, K. (2012). Highly reliable low power Solid-State Drives (SSDs). *IEEE Xplore*, 1-2.

Tannhausser. (28 de 06 de 2014). *La mirada del replicante*. Obtenido de La mirada del replicante: <http://lamiradadelreplicante.com/2014/06/28/los-mejores-programas-para-la-recuperacion-de-archivos-en-gnulinux/>

Tecmint. (07 de 06 de 2013). Obtenido de Tecmint : <https://www.tecmint.com/install-scalpel-a-filesystem-recovery-tool-to-recover-deleted-filesfolders-in-linux/>

Tecnoautos. (2017). Obtenido de Tecnoautos: <https://tecnoautos.com/automoviles/fichas-tecnicas/ficha-tecnica-del-ford-explorer-sport-track-ensamblado-en-2003/>

Todocoche. (2017). Obtenido de Todocoche: <http://www.todocoche.com/coche/minicooper/austinmini/austinmini>

Tong-Wei, C., & Ming-Lee, C. (2011). Design of a Digital Forensics Evidence Reconstruction System for Complex and Obscure Fragmented File Carving. *IEEE Xplore*, 793-797.

Uncomo. (s.f.). Recuperado el 25 de 01 de 2018, de Uncomo: <https://hogar.uncomo.com/articulo/cuales-son-las-medidas-adecuadas-para-la-mesa-de-trabajo-47200.html>

Universidad de Sevilla. (19 de 02 de 2010). Obtenido de Universidad de Sevilla: http://laplace.us.es/wiki/index.php/Teorema_de_conservaci3n_de_la_energ3a_mec3nica

Windows Forensics. (s.f.). Obtenido de Windows Forensics: https://www.packtpub.com/mapt/book/networking_and_servers/9781784390495/7/ch07lv11sec44/event-log-recovery-with-evtxtract

Xways. (27 de 11 de 2017). Obtenido de Xways: <https://www.x-ways.net/winhex/>

Yan, W., Wang, X., & Yu, X. (2014). Design and implementation of an efficient flash-based SSD architecture. *IEEE Xplore*, 79-83.

Yubal;. (02 de 10 de 2017). *Xataka*. Obtenido de Xataka: <https://www.xataka.com/basics/hdd-vs-ssd>