208

MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL

DIRECCIÓN DE INVESTIGACIÓN CRIMINAL E INTERPOL

Bogotá, D.C. 01 de septiembre de 2010

No. 004883 / **GRIDI – ADEPE**

ASUNTO : Dictamen en Informática Forense

AL : Doctora
Fiscal 18 Delegada Especializada
Unidad Nacional para la Extinción de Dominio y el Lavado de Activos
Ciudad.

Proceso No. 9477

De conformidad con lo solicitado en el oficio de la referencia, me permito enviar el resultado del análisis practicado.

1. ELEMENTOS DE ESTUDIO

1.1 Disco duro marca Samsung serie S20BJ9CZ509485 de 500 GB.
1.2 Disco duro marca Samsung serie S20BJ9CZ509480 de 500 GB.
1.3 Disco duro marca Samsung serie S20BJ9CZ509706 de 500 GB.
1.4 Disco duro marca Samsung serie S20BJ9CZ509487 de 500 GB.
1.5 Disco duro marca Samsung serie S20BJ9CZ509488 de 500 GB.
1.6 Disco duro marca Samsung serie S20BJ9CZ509475 de 500 GB.
1.7 Disco duro marca Samsung serie S20BJ9CZ509490 de 500 GB.
1.8 Disco duro marca Samsung serie S23CJ9CZ508484 de 500 GB.
1.9 Disco duro marca Samsung serie S23CJ9CZ508415 de 500 GB.
1.10 Disco duro marca Samsung serie S20BJ9CZ509484 de 500 GB.
1.11 Disco duro marca Samsung serie S20BJ9CZ509481 de 500 GB.
1.12 Disco duro marca Samsung serie S20BJ9CZ509486 de 500 GB.
1.13 Disco duro marca Samsung serie S20BJ9CZ509696 de 500 GB.
1.14 Disco duro marca Samsung serie S20BJ9CZ509479 de 500 GB.
1.15 Disco duro marca Samsung serie S20BJ9CZ509476 de 500 GB.
1.16 Disco duro marca Samsung serie S20BJ9CZ509707 de 500 GB.
1.17 Disco duro marca Samsung serie S23CJ9CZ508420 de 500 GB.
1.18 Disco duro marca Toshiba serie 20K7C9ZQT.
1.19 Disco duro marca Hitachi serie 080325BB0F00WDHSGKTC de 250 GB.
1.20 Disco duro marca Hitachi serie SJH82MLE de 160 GB.
1.21 Un computador portátil marca Acer serie LUS050B2289122A02C2547.
1.22 Disco duro marca Western Digital serie WMAMF1836956 de 40 GB.
1.23 Un computador de mesa marca Hasse modelo JXQ513365 No. Inventario 337.
1.24 Disco duro marca Seagate serie 5LY3VJ56 de 80 GB.
1.25 Disco duro marca Maxtor serie 6PS3HJJ4 de 80 GB.
1.26 Un computador de mesa marca Hasse modelo JXQ513365 No. Inventario 145.
1.27 Disco duro marca Seagate serie 5JXK7X8A de 40 GB.
1.28 Disco duro marca Hitachi serie 080521BB6F00WDJAVZMG de 250 GB.
1.29 Un computador portátil marca Sony Vaio modelo PCG-5PZP Service TAG C600P6ME.
1.30 Disco duro marca Samsung serie S10MJ9DQ507672 de 320 GB.
1.31 Disco duro marca Samsung serie S00JJ40X902005 de 38 GB.

209

2. ANALISIS SOLICITADO

Se transcribe lo solicitado por la Fiscalía General de la Nación mediante oficio 9793 de fecha 21/06/2010 bajo la coordinación de la Fiscalía 18 Delegada Especializada así:

1. De las imágenes recolectadas en el allanamiento se duplica dichas imágenes y se tomen dos imágenes de los discos duros físicos entregados

2. Extraer la información contenida en estas imágenes a información legible, entendible a cualquier persona.

3. Extracción de usuarios y paswords de la información contenida en las bases de datos (software contable y otros).

4. Se haga exportación de la información contenida en las bases de datos (software contable o motores de bases de datos) a paquetes de Microsoft office (archivos de Excel, Word, Powerpoint).

5. Aportar por escrito y por cada imagen y discos analizados, los respectivos usuarios y claves.

3. MEDIOS TECNICOS UTILIZADOS

3.1 Equipo de cómputo FRED SR.

3.2 Tableau USB forensic Bridge.

3.3 Programa "FTK Imager Versión 2.5.1" de la suite Access Data, con el cual se realizó la imagen del disco duro, programa utilizado para realizar la imagen forense de los dispositivos en formato E01 con una compresión de 9.

3.4 Programa para análisis forense – Encase Law versión 6.13; se trata de una herramienta forense que ayuda a la captura y análisis de imágenes y dispositivos de almacenamiento (discos duros, discos externos, memorias, discos compactos, disquetes y dispositivos móviles), en general sistemas de almacenamiento de información digital, especializado para la recuperación y análisis de información, esta versión es exclusiva para las autoridades dedicadas a la informática forense.

3.5 Juego de herramientas forense para computador, bloqueadores de escritura y conectores.

3.6 Software Microsoft Windows XP Profesional, Versión 2002 y Microsoft Office 2003 actualizados.

4. ANALISIS PRACTICADOS Y RESULTADOS OBTENIDOS

4.1 Fijación fotográfica de los elementos objeto de análisis, así:

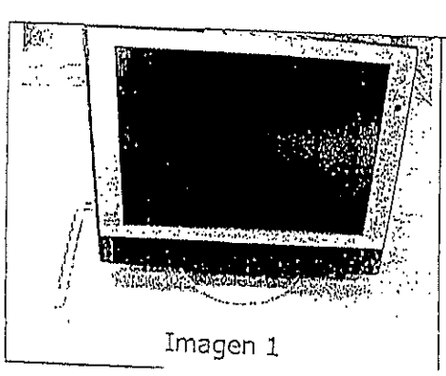

Imagen 1

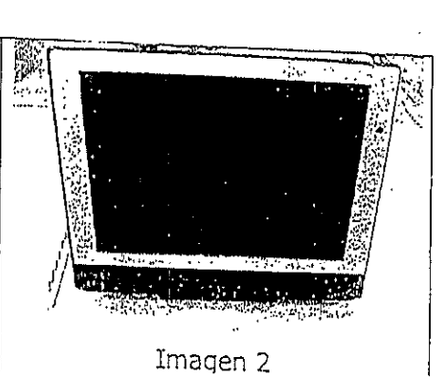

Imagen 2

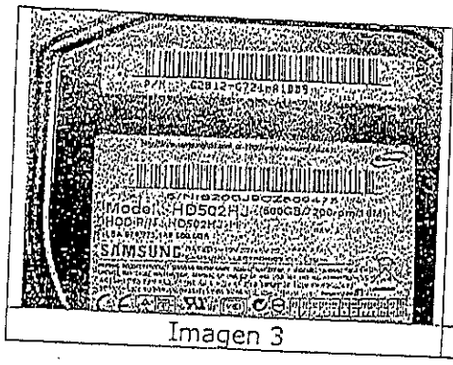

Imagen 3

Imagen 4

Imagen 5

Imagen 6

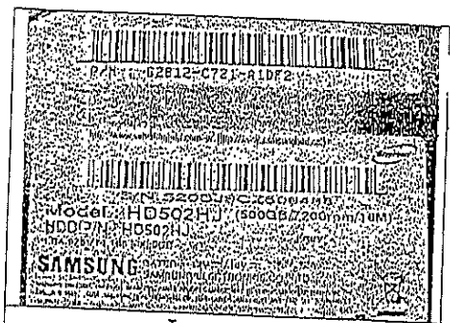

Imagen 7

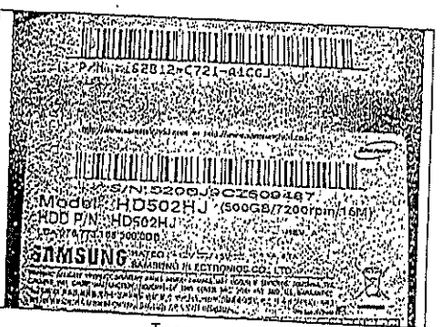

Imagen 8

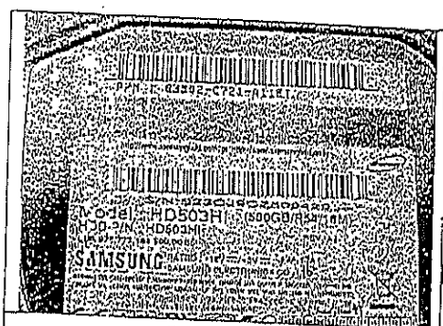

Imagen 9

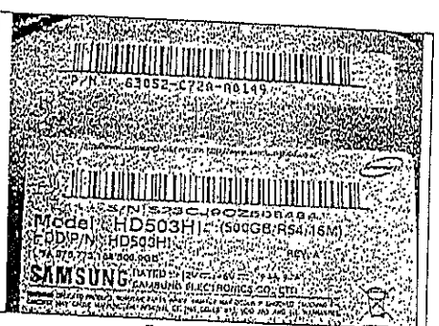

Imagen 10

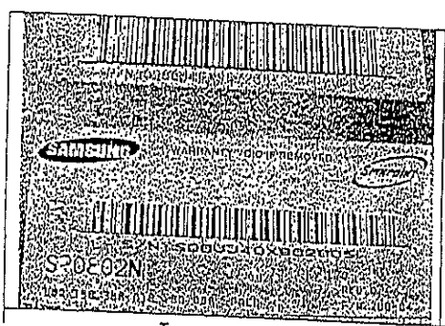

Imagen 11

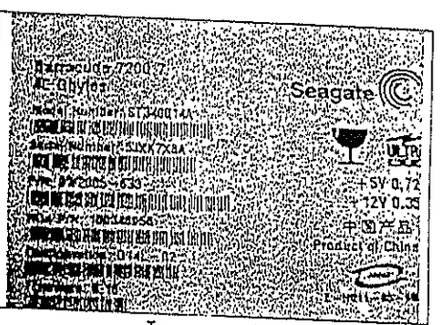

Imagen 12

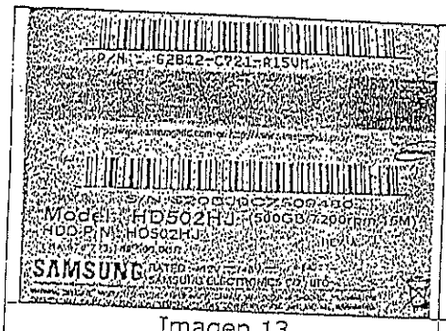

Imagen 13

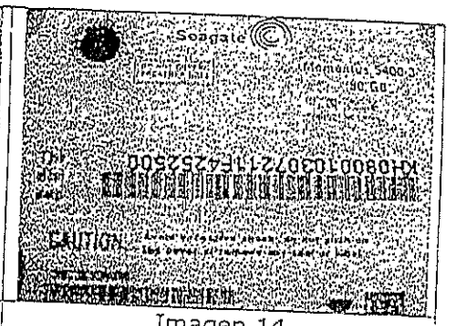

Imagen 14

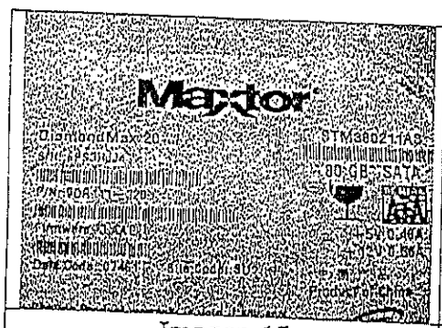

Imagen 15

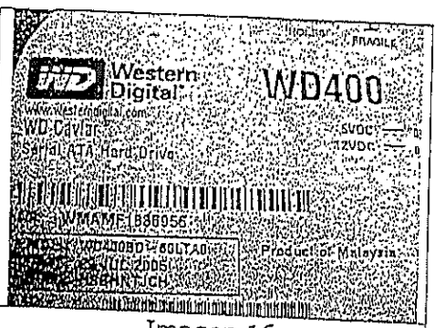

Imagen 16

Imagen 17

Imagen 18

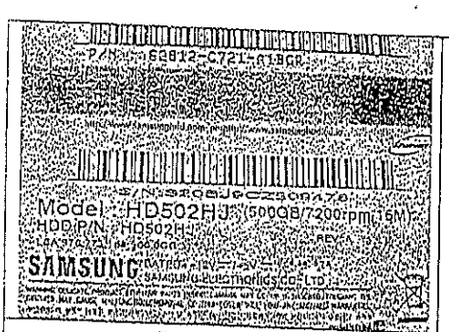

Imagen 19

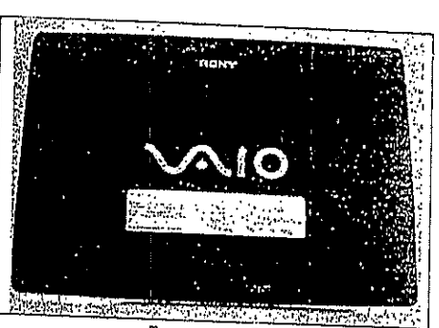

Imagen 20

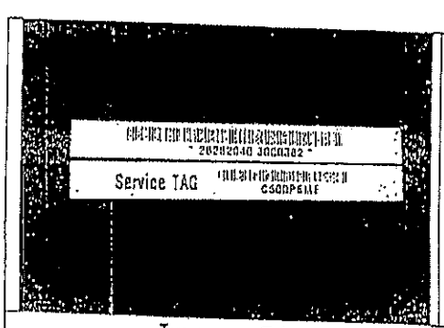

Imagen 21

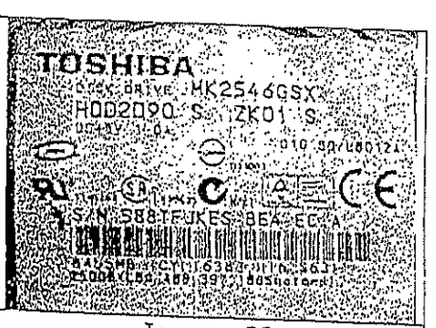

Imagen 22

212

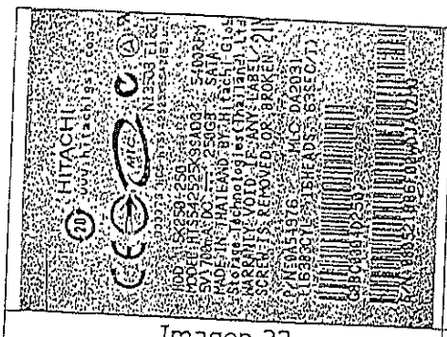

Imagen 23

Imagen 24

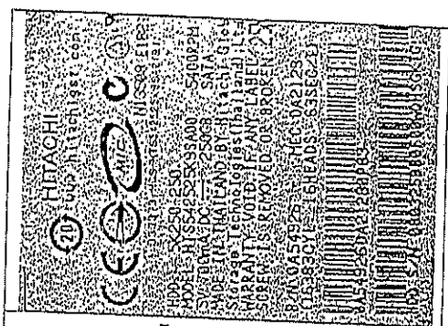

Imagen 25

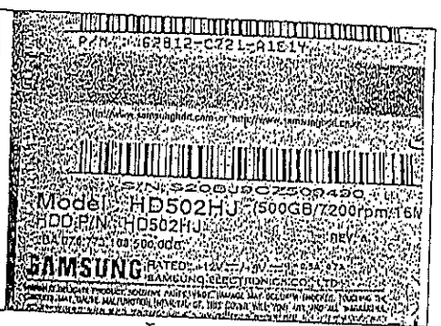

Imagen 26

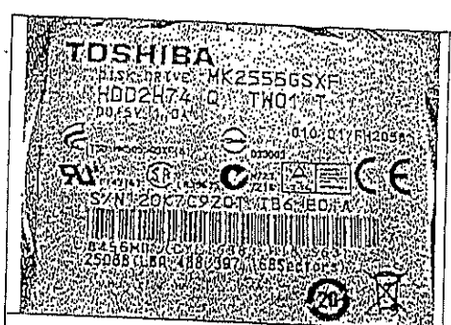

Imagen 27

Imagen 28

Imagen 29

Imagen 30

Imagen 31

Imagen 32

213

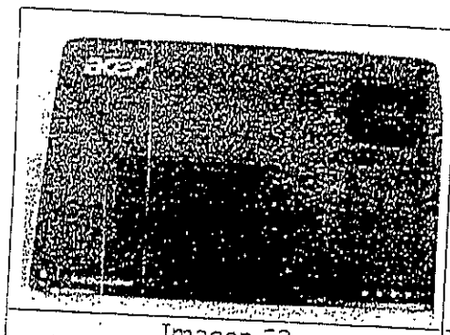

Imagen 33

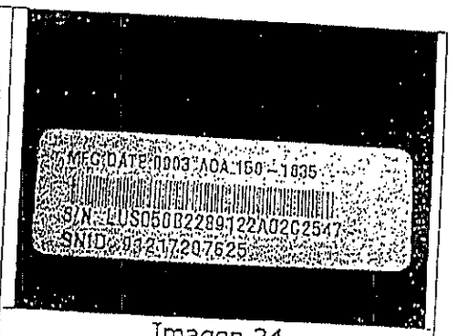

Imagen 34

4.2 Para los dispositivos relacionados en el ítem No. 1.18 al 1.31 se conectan a la computadora forense en la bahía de lectura para discos IDE y SATA, la cual se encuentra protegida contra escritura y mediante el empleo del software Forensic ToolKit se realizan las imágenes forenses.

4.3 Para cada una de las imágenes forenses se extrae la suma de verificación MD5 y SHA1, que se encuentra en el archivo con extensión TXT generado al momento de la creación de la imagen autenticándose cada una de las ellas con las siguientes sumas de verificación:

Computador de mesa No. inventario 145

MD5: 73ee6074fb7ae1ff5aa2c3d39f5cd756
SHA1: 686af60f0f49a9944acf899690e98f69811d9b35

Computador de mesa No. inventario 337

MD5: 659225a4eb3f0ebe9e37654bd2cea926
SHA1: aa753ef4cc5798e8819629b5b6e014cbb03a877e

Disco Duro marca Seagate SN 5JXK7X8A 8.7

MD5: 195686744867be2663f8d6be4d1ce97b
SHA1: b58130f34f69f3f3da311e6b42dd500e27bd60a3

Disco Duro marca Hitachi serial SJH82MLE 160GB

MD5: 0d3d4e28fd66cab5de13371a84704458
SHA1: b3b23c858b384582cd394d5e0fca922b46a9d99b

Disco Duro marca Toshiba serial 20K7C9ZQTIB6ECA 250GB

MD5: 306ae0bcda6ed0a8ee022f394b4e1d79
SHA1: 911b7a02581c7aea3afc7b3d0592814e1a926063

Disco Duro marca Maxtor SN 6853HJJ4 80GB

MD5: 07c976eb08441a88953951d4c531e94c
SHA1: 6f76cf3cadbdba775ce02d72d018231427f1582e

Disco Duro marca Maxtor, de 160 GB, SN 6RABAZ25

MD5: f240f00116f8acc0f1ee5cd4157af4bb
SHA1: 8630602b93a81b7f748d4aeb3870e208eb8e3c0d

Memoria marca Team, color azul, de 1 GB

MD5: 7a91c5e4d8c4e6884dca36a5150202b4
SHA1: 8caf6049d7f69d754c030c762417ce52532ab106

Disco duro marca Seagate, S/N 6RX2HHZS, de 160 GB.

MD5: a1196d70236bfda3b74ef4efd7a87298
SHA1: 42f229f02de2eb39bbfcfa7d849ad5fea4f93453

Disco duro serial No. 6PS30VPZ

MD5: 2449849962d49ae9c543650dc935702a
SHA1: 00d97b24f24ba13b88fa362fff348298316da288

Disco duro serial No. WCADK447322

MD5: 4650e2e70298030dcc22eed568c85fb3
SHA1: f107584d6b0cea99586a5d308137d2f889dcd4b3

Disco duro serial No. 5FB4WXQH

MD5: 6fcded95e922eb5761f151003affe1d2
SHA1: 6a697dcca6dfea1714a108b96eb98b00104b61c3

Disco duro serial 3797 Servidor Buildercon

MD5: cd9957757edad15033a712c2d75dbe14
SHA1: 22eca2364330fd2c620de5c06024d754f753b366

Disco duro serial No. X0H2054R

MD5: f55511e6d7ff9ef7debc91b06d2a1049
SHA1: 677d586002414fd5c3d2cf14c82e5ad28a0a2ffe

Disco duro marca Western Digital, serial WMAMF1836956

MD5: 77c1454cf0d1c192c98263d2484b544d
SHA1: 45bf220c2b8abf21c8c084e3f9ece33427453962

Disco duro marca Hitachi S/N 080521BB6F00WDJAVZMG de 250 GB.

MD5: 40df43b9779b52187472b288fb14c369
SHA1: eb40ec9d097b029e6500a56456169771295275a5

Disco duro marca Western Digital de 40GB

MD5: 22fe3a869fb93c4b10d70076da519b39
SHA1: bdab27febae204935cfeb3b3b03a03b399827db8

Disco duro marca Fujitsu de 250 GB S/N K41LT852FJ1L

MD5: 1b140eef33dcdd38cb2cf27fa3872935
SHA1: babe78e3cca94f495f89c85c07c5ed2ce80b733f

Disco duro marca Hitachi, de 80 GB, SNS6RRSZZM

MD5: 802143263ee154cd3392e8417ff6cfaf
SHA1: 2d7989546c77dbeda100859b3caddcdc46b886fa

Disco duro marca Samsung, 500 GB, S/N 520BJDWS947233

MD5: 8128cea08217726bd2405493077f6bb7
SHA1: f01f179d2fec2b65bb34da3bfd0c9652a8855443

Disco duro marca Maxtor de 80 GB. S/N L242YP5G

MD5: 62cbe5ea923e41ba537b6438f4609fcb
SHA1: 35796c20db44df68e4c7a2c3919d91b81a56e071

Disco duro marca Samsung de 160 GB. S/N S0V3J9CS201487

MD5: a440bc36f642be2d7677442c809dc33d
SHA1: 501d57f18c66bc0da842c126a438b161abc1cad5

Disco duro marca Hitachi de 164 GB. S/N Z2S7HBRJ

MD5: 953d9ed9f5e88697ea2f368f39156c3b
SHA1: 8bd8b3d75e647e566f55cf9b000dbe00214c95e8

Disco duro marca Hitachi de 164 GB. S/N Z2S7DBRJ

MD5: 05b4c70b8ed10e704b2c716c529cc0e2
SHA1: a9969b5cd91dd0915d5589e042bf3d235c2ddb7a

Disco duro contadora ciudad Cartagena

MD5: 928754c817ab599330da4a542c34f859
SHA1: 50cba12ba03f3359982f489edf1ce2d67e3f695a

Disco duro marca western digital de 40 GB de almacenamiento 5

MD5: 22fe3a869fb93c4b10d70076da519b39
SHA1: bdab27febae204935cfeb3b3b03a03b399827db8

Disco duro marca Fujitsu de 250 GB serial numero K41LT852FJ1L 5

MD5: 1b140eef33dcdd38cb2cf27fa3872935
SHA1: babe78e3cca94f495f89c85c07c5ed2ce80b733f

Marca Excelstor, S/N Q5A65QB, modelo j8080, capacidad 80 GB 13

MD5: e4bab43ea1f46362b5897d48abe3751e
SHA1: acda42211b0c7777bb4bfd95d7c25db530bddb28

Marca Maxtor, S/N R2V2XDWE, mod 4r080l06210p1, cap 80 GB 13

MD5: c2c7eee3d93128242a729e5306fe37ae
SHA1: f460edbe9550987a613b72c837aeef24e77bae69

Disco duro marca Hitachi SN 080325BB0F00WDHSGKTC 250 GB 5.2

MD5: 4e72c43911c546d4ff9c4f7437884f06
SHA1: ac65f55f9754a13c78a84ebad9111512728dcec1

Disco duro marca Western Digital SN WCAPW5107524 OBJ 2

MD5: f338eed4f20e764190d8cf162250491e
SHA1: 4a6249f39a981c06d46e065299c5b6216713a0d0

Disco duro marca Toshiba DE 100 GB S/N 25234274S APOSUCRE 14.1

MD5: ec78efad7fe913df5bf05ca758705260
SHA1: 9f0fbe6ff029107d3c62fb46a8fdc25b5248a32d

Disco duro marca Seagate de 40 GB. S/N 5JXBP0N1 14.2

MD5: 5cb8abccf735a17dea42ff57967b4dfa
SHA1: 6cd643ed08e6b9f74b412d90ea2a0f5a09eb8d6b

Zoocriadero No. 2 Oficina Administrador Seagate de 320 GB. 13

MD5: 73b9f7e0298cba35a7405ba1ae9b5fe1
SHA1: 8641a340bec97e53b6e86f02e9b30699be7aac5f

Servidor marca DELL POWEREDGER200, serie No. 8N726H1

MD5: 7ccef51058e2cdadb4032eae87a0f242
SHA1: 29392b56c8446e068231f55040e953e5965700f4

216

Disco duro marca Seagate de 80 GB. S/N 5LY3VJ56

MD5: ee0d321735f87bca67aba718164aa133
SHA1: 45b79182a66419db73d1fee0de8e603287ecd960

Disco duro marca Samsung de 320GB. S/N S10MJ9DQ507672

MD5: 34f00f194de98e63480b0ebdc1f12f17
SHA1: b5416699300a74c6889254c5f8dba2fd7719b4fe

4.4 Se crea un archivo de caso para cada imagen, verificando la integridad de la misma mediante la suma de verificación MD5 y SHA1, generándose error para las siguientes imágenes:

- **Disco duro marca Samsung de 500 GB. S/N S20BJ9CZ509485 – Magangue:** Se encuentran almacenadas 02 imágenes forenses las cuales presentan daño, siendo imposible la extracción de la información.

- **Disco duro marca Samsung S/N S20BJ9CZ509707 – Uniapuestas Valledupar:** Se encuentran almacenadas 03 imágenes forenses, de las cuales 02 se encuentran dañadas.

4.5 Se procede a recuperar carpetas y archivos borrados.

4.6 Se calcula el MD5 de cada uno de los archivos aportados.

4.7 Se realiza filtrado de archivos por las extensiones doc, xls, mdb, csv, jpg, avi, mpg, pdf, txt, ppt, zip, rar, htm, entre otras.

4.8 Se extraen los archivos y se almacenan en tres (03) discos duros (Anexo No. 1).

5. INFORMACIÓN QUE APORTA A LA INVESTIGACIÓN

Como resultado de la exportación de la información se aportan las siguientes cantidades de archivos, especificados por extensión, así:

	DOC	XLS	BD	PPT	PDF	JPG	AVI	MPG	TXT	ZIP-RAR	HTM
Barranquilla	13.944	11.854	210	81	4.732	4.069	0	0	84	871	2.636
Santa Marta	4.276	3.045	0	242	761	613	0	8	0	0	0
Cartagena	151	588	13	26	12	1.758	38	0	0	0	0
Valledupar	02	02	0	0	0	0	0	0	0	0	0
Sincelejo	0	0	0	0	0	4.166	99	13	0	0	0
Magangue	1.656	1.524	349	19	332	61	0	0	0	282	49

ANEXO No. 1: Dos (02) discos duros marca Seagate de 20 GB cada uno, seriales No. 3HT3JYW7, 3HT2W6KQ y un (01) disco duro marca Western Digital de 40 GB serial No. WCAMA4166244, los cuales contienen la información extraída a las imágenes forenses objeto de análisis y los valores Hash de los archivos aportados.

6. CONCLUSIONES

➢ Los siguientes discos duros presentan daño físico y no es posible su lectura:

- **Disco duro marca Samsung de 500 GB. S/N S20BJ9CZ509475 – Santa Marta:** Se encuentran almacenadas 05 imágenes forenses. Inicialmente se pudo extraer la información pero una vez terminado el procedimiento presentó un daño físico lo que impide su lectura.

217

- **Disco duro marca Samsung S/N S20BJ9CZ509486 – Uniapuestas Barranquilla:** Dicho disco duro presenta daño físico siendo imposible la extracción de información.

- **Disco duro marca Samsung S/N S00JJ40X902005 de 80 GB. – Bogotá:** Dicho disco duro se encuentra con un hueco en la parte posterior siendo expuesto al medio ambiente lo cual daña el dispositivo.

➢ Los siguientes discos duros presentan imágenes forenses realizadas en campo pero que al momento de montarlas en el software forense del laboratorio no presentan ningún tipo de información para exportar, así:

- **Disco Duro marca Toshiba Serial Número 588TFJKES de 250GB, extraído del Computador portátil marca Sony Vaio modelo PCG5PZP Service TAG C600 PEME - Bogotá:** No tiene información.

- **Disco duro marca Toshiba S/N 20K7C9ZQT – Uniproducciones Barranquilla:** No tiene información.

- **Disco duro marca Maxtor S/N 6P53HJJ4 – Seguridad 911 – Barranquilla:** No tiene información.

- **Disco duro marca Samsung S/N S20BJ9CZ509479 – Zoocriadero Barranquilla:** Las imágenes forenses almacenadas en este disco corresponden al computador del perito y no a los discos duros objetivo de la diligencia, (error del perito que realizó las imágenes).

- **Disco duro marca Samsung S/N S10MJ9DQ507672 de 320 GB. – Barranquilla:** No tiene información.

- **Un computador portátil marca Acer serie LUZ050B2289122A02C2547 – Barranquilla:** No tiene información.

Dando cumplimiento al requerimiento, los peritos dan por terminado el presente dictamen el cual deberá ser remitido a la autoridad que originó dicha solicitud, junto con los elementos objeto de análisis debidamente embalados, rotulados y con las respectivas cadenas de custodia.

Subintendente **JOSE ANDRES ALDANA MONTENEGRO**
Perito Grupo Investigaciones Tecnológicas DIJIN

Patrullero **EDWIN ALEXANDER LOGATTO CUADROS**
Perito Grupo Investigaciones Tecnológicas DIJIN

Patrullero **GEINER TARAZONA GUERRERO**
Perito Grupo Investigaciones Tecnológicas DIJIN

Patrullera **SANDRA PATRICIA SISA SEQUERA**
Perito Grupo Investigaciones Tecnológicas DIJIN