|  |  |
| --- | --- |
| **ACTA- N°** | **[***Número asignado***]** |

**SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

**OFICINA DE TECNOLOGÍA E INFORMÁTICA**

**GRUPO DE TRABAJO DE INFORMÁTICA FORENSE Y SEGURIDAD DIGITAL**

**RADICADO [*EN NÚMERO EL RADICADO*]**

En la ciudad de Bogotá, el [*Día en letras*] ([*Día en números*]) del mes de [*Mes en letras*] de [*Año en letras*] ([*Año en números*]), el Grupo de Trabajo de Informática Forense y Seguridad Digital (en adelante “GTIFSD”) de la Superintendencia de Industria y Comercio (en adelante “SIC”), recibe por parte del [*Grupo que realiza la solicitud*] el expediente con radicado N° [*En números el número de radicado*] con el fin de realizar la depuración de los mensajes de datos de [*Número en letras*] ([*valor numerico*]) dispositivo(s) contenedor(es) de evidencia digital (CD/DVD/BLURAY/USB/DD). El objetivo de esta depuración de mensajes de datos es [*escribir objetivo de la actividad a realizar*].

1. **DESCRIPCIÓN DEL REQUERIMIENTO**

[*Nombre de la persona que hace la solicitud*], [*Cargo*], [*Grupo de trabajo y Delegatura*] solicita al GTIFSD el día [*Día en letras*] ([*Día en números*]) del mes de [*Mes en letras*] de [*Año en letras*] ([*Año en números*]) depuración de mensajes de datos de [*Número en texto*] ([*Valor numerico*]) dispositivos contenedores de evidencia digital ([*Especificar los tipos de dispositivos*])**,** que se encuentran en el expediente con número de radicado N° [*En números el número de radicado*] **–** [*NOMBRE DEL CASO EN MAYUSCULA SOSTENIDA*]. Al finalizar la depuración se solicita al GTIFSD todos los mensajes de datos almacenados en los dispositivos de origen revisados en ([*Identificar los tipos de dispositivo de destino*]), esto con el fin de [*escribir objetivo de la actividad a realizar*].

1. **HERRAMIENTAS DE SOFTWARE Y HARDWARE UTILIZADAS**

A continuación se relacionan las herramientas de software y hardware utilizadas para realizar la actividad de identificación y copia de [*Numero en letras*] ([*Valor numerico*]) dispositivos contenedores de evidencia digital ([*Identificar los tipos de dispositivo*]):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SOFTWARE/HARDWARE** | **PROPÓSITO** | **NOMBRE** | **VERSIÓN** | **FABRICANTE** |
| [*Identificar si es Software o Hardware*] | [*Identificar el propósito u objetivo de la herramienta empleada*] | [*Identificar el nombre del software o la placa SIC del hardware*] | [*Identificar versión o modelo de la herramienta empleada*] | [*Identificar el fabricante o la marca de la herramienta*] |
| [*Identificar si es Software o Hardware*] | [*Identificar el propósito u objetivo de la herramienta empleada*] | [*Identificar el nombre del software o la placa SIC del hardware*] | [*Identificar versión o modelo de la herramienta empleada*] | [*Identificar el fabricante o la marca de la herramienta*] |

Tabla 1 Relación de herramientas de software y hardware utilizadas en la actividad.

1. **DESCRIPCIÓN GENERAL DE LA ACTIVIDAD**

Se realiza la actividad de depuración de mensajes de datos [*Numero en letras*] ([*valor numérico*]) dispositivos contenedores de evidencia digital ([*describir los tipos de dispositivos copiados*]) en [*Numero en letras*] etapas así:

1. **(SI APLICA)** Registro fotográfico de dispositivos de origen: Se capturan 4 tipos de fotografías: (i) embalaje, (ii) vista frontal, (iii) vista posterior y (iv) serial físico del dispositivo, esto para identificar visualmente el estado físico y otros elementos de identificación únicos del contenedor, es decir, el serial físico, etiqueta y otros, para esta etapa son utilizados las herramientas de hardware [*Listar las diferentes herramientas de hardware empeladas durante esta etapa separadas por comas*].
2. Análisis técnico de dispositivos de origen: Se realiza la identificación de los dispositivos de origen mediante dos análisis: (i) análisis físico, en donde se identifican las características físicas del contenedor de evidencia digital, es decir, su ubicación exacta en el expediente, el tipo de dispositivo, marca, serial físico y estado, y (ii) análisis lógico, en donde se identifican las características lógicas del dispositivo contenedor de evidencia digital, es decir, la capacidad del dispositivo contenedor, el peso de la información digital, el serial lógico, numero de archivos, carpetas e imágenes forenses y el estado. Para esta etapa son utilizadas las herramientas de software [*Listar las herramientasde software empleadas en esta etapa separadas por comas*], así como la herramienta de hardware [*Listar las diferentes herramientas de hardware empeladas durante esta etapa separadas por comas*].
3. Búsqueda de mensajes de datos: Esta actividad se realiza por medio del software FTK Lab, licenciado para el uso de la SIC, que se conecta a los servidores del GTIFSD por medio de conexión privada y segura; adicionalmente se utilizan filtros y opciones de búsqueda y dtSearch, opciones de uso que incluye las herramientas de informática forense utilizadas.
4. Extracción de imagen forense derivada: Una vez seleccionados y exportados los mensajes de datos con el software FTK Lab, se realiza una nueva imagen forense, denominada imagen forense derivada, en la cual los mensajes de datos conservan su integridad y validez probatoria ya que no son modificados o alterados, lo anterior debido al software forense especializado para realizar este tipo de actividades.
5. Copia de los mensajes de datos[[1]](#footnote-1): Se realiza la copia de la totalidad de los mensajes de datos que contienen los dispositivos identificados anteriormente usando el software [*Listar las herramientasde software empleadas en esta etapa separadas por comas*], a un contenedor de evidencia digital de destino [*Identificar el tipo de dispositivo de almacenamiento del contenedor temporal o final*].
6. Análisis técnico de dispositivo de destino: Se realiza la identificación el dispositivo contenedor de evidencia digital final, en el cual reposara la compilación de los dispositivos de origen anteriormente identificados y copiados. En esta etapa se realizan dos análisis: (i) análisis físico, en donde se identifican las características físicas del contenedor de evidencia digital, es decir, el tipo de dispositivo, marca, capacidad, embalaje, serial físico y estado físico, y (ii) análisis lógico, en donde se identifican las características lógicas del dispositivo contenedor de evidencia digital, es decir, la capacidad del dispositivo contenedor, el serial lógico, número de archivos, carpetas e imágenes forenses y el estado lógico. Para esta etapa son utilizados las herramientas de software [*Listar las herramientasde software empleadas en esta etapa separadas por comas*], así como la herramienta de hardware [*Listar las diferentes herramientas de hardware empeladas durante esta etapa separadas por comas*].
7. **(SI APLICA) REGISTRO FOTOGRÁFICO DE DISPOSITIVOS DE ORIGEN**

Para realizar la identificación física y visual del tipo de embalaje, el estado del dispositivo se realiza 4 tipos de fotografías (i) embalaje, (ii) vista frontal, (iii) vista posterior y (iv) serial físico del dispositivo, con una cámara fotografías propiedad del GTIFSD con las siguientes características técnicas:

|  |  |
| --- | --- |
| **CARACTERÍSTICA** | **VALOR** |
| Dimensión | [*Identificar las dimensiones de la fotografia*] |
| Resolución | [*Identificar la resolución de la fotografía*] |

Tabla 2 Características técnicas de las fotografías tomadas.

Estas fotografías se anexan a la presente acta *(Ver Anexo* [*Identificar si es físico o digital*][*Numero secuencial de anexo*]*)* en las que pueden ser identificadas de acuerdo al folio asignado al dispositivo por parte de [*Identificar grupo que solicito la actividad*].

1. **ANÁLISIS TÉCNICO DE DISPOSITIVOS DE ORIGEN**

[*Identificar el grupo que solicito la actividad*] entrega un total de [*Numero en texto*] ([*Valor numerico*]) dispositivos contenedores de evidencia digital ([*Describir los tipos de dispositivos copiados*]) correspondientes al caso N° [*En número el radicado*].

A continuación se adjunta un cuadro resumen de los cuadernos del expediente en donde se encuentran los dispositivos contenedores de evidencia digital:

|  |  |  |
| --- | --- | --- |
| **N° TOTAL DE DISPOSITIVOS POR CUADERNO** | **NOMBRE DE CUADERNO PUBLICO** | **NOMBRE DE CUADERNO RESERVADO** |
| [*Escriba valor numérico*] | [*Identificar el cuaderno*] | [*Identificar el cuaderno*] |
| [*Escriba valor numérico*] | [*Identificar el cuaderno*] | [*Identificar el cuaderno*] |

Tabla 3 Resumen de cuadernos con dispositivos.

Se identifican [*Numero en texto*] ([*Valor numérico*]) dispositivos contenedores de evidencia digital ([*Describir los tipos de dispositivos copiados*]), el detalle de los mismos se anexan a la presente acta *(Ver Anexo* [*Identificar si es físico o digital*][*Numero secuencial de anexo*]*)* con la siguiente información por cada dispositivo de origen identificado:

1. NÚMERO DEL DISPOSITIVO
2. ANÁLISIS FÍSICO:
   * Radicado del caso al que pertenece.
   * Ubicación exacta (cuaderno y folio) en el que reside el dispositivo.
   * Tipo de dispositivo.
   * Marca.
   * Serial físico.
   * Estado físico.
3. ANÁLISIS LÓGICO:
   * Capacidad total del dispositivo (tamaño).
   * Espacio utilizado o peso.
   * Numero de archivos que contiene el dispositivo.
   * Numero de carpetas que se encuentran en el dispositivo.
   * Serial lógico.
   * Estado lógico.

**(SI APLICA)** Los soportes técnicos de verificación lógica y física del estado de los archivos digitales y la capa física de cada uno de los dispositivos se anexan a la presente acta *(Ver Anexo* [*Identificar si es físico o digital*][*Numero secuencial de anexo*]*)*.

1. **IDENTIFICACIÓN DE IMÁGENES FORENSES ORIGINALES**

De acuerdo a la tarea de depuración y posterior adquisición de imagen forense derivada, se relaciona las huellas Hash de las imágenes parciales obtenidas en la visita administrativa identificadas como imágenes primarias incluidas en [*Numero en texto*] ([*Valor numérico*]) dispositivos contenedores de evidencia digital (*[Describir los tipos de dispositivos copiados]*) de la siguiente manera:

* **Imagen parcial [*Identificar el nombre de la imagen parcial*]**

Esta imagen parcial contiene los archivos en formato -.AD1- de la información del material probatorio, se verifica con éxito y se compone de (i) un archivo digital de imagen forense - .AD1-, (ii) un archivo digital en formato de archivo de texto -.TXT- y (iii) Un archivo digital en formato de separación por comas -.CSV-.

|  |
| --- |
| [*En este recuadro plasmar el log de adquisición de la imagen forense identificada*] |

Log de Adquisición 1 Contenido de hash de la imagen parcial [Nombre de la imagen parcial]

1. **BÚSQUEDA DE LOS MENSAJES DE DATOS**

La tarea de depuración de mensajes de datos se realiza para las evidencia digitales [*Listar separadas por comas las evidencias*], situados dentro de las diferentes imágenes forenses adquiridas, incluidas en [*Numero en texto*] ([*Valor numérico*]) dispositivos contenedores de evidencia digital ([*Describir los tipos de dispositivos copiados*]), el detalle del mismo se anexa a la presente acta *(Ver Anexo* [*Identificar si es físico o digital*][*Numero secuencial de anexo*]*)*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **N°** | **ASUNTO** | **DE:** | **PARA:** | **FECHA DE ENVIO** | **FECHA DE RECEPCION** | **TAMAÑO** | **CANTIDAD DE ADJUNTOS** | **CARPETA ASOCIADA** |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

Tabla 4 Estructura para depuración de mesajes de datos

1. **ADQUISICIÓN DE IMAGEN FORENSE DERIVADA**

Al finalizar la identificación de los mensjaes de datos a depurar, se procede a realizar la imagen forense derivada de los mensajes de datos almacenada en el servidor utilizando el software FTK Lab. El proceso de creación de la imagen forense comienza el día [*Día en letras*] ([*Valor numérico*]) de mes [*Identificar el mes*] a las [*Horas*]:[*Minutos*] [*en formato militar*] y finaliza el [*Día en letras*] ([*Valor numérico*]) de mes [*Identificar el mes*] en texto de [*Año en letras*] [*Valor numerico*] a las [*Horas*]:[*Minutos*] [*en formato militar*] a continuación se cita el informe de las adquisiciones de la herramienta forense:

* **Imagen parcial [*Identificar el nombre de la imagen parcial*]**

Esta imagen parcial contiene los archivos en formato -.AD1- de la información del material probatorio, se verifica con éxito y se compone de (i) un archivo digital de imagen forense - .AD1-, (ii) un archivo digital en formato de archivo de texto -.TXT- y (iii) Un archivo digital en formato de separación por comas -.CSV-.

|  |
| --- |
| [*En este recuadro plasmar el log de adquisición de la imagen forense identificada*] |

Log de Adquisición 2 Contenido de hash de la imagen parcial [Nombre de la imagen parcial]

1. **DISPOSITIVO DE DESTINO**

Finalmente se procederá a realizar el borrado de las imágenes forenses parciales adquiridas en la visita administrativa, y se incluyen las nuevas imágenes forenses derivadas como resultado de la depuración de los mensajes de datos.

El resultado de la depuracion realizada en la etapa anterior se almacena en [*Numero en letras*] ([*Valor numérico*]) dispositivo contenedor de evidencia digital ([*Describir los tipos de dispositivos de destino*]), **APLICA ÚNICAMENTE SI EL DESTINO ES UN DISCO DURO** debidamente esterilizado, el detalle del dispositivo de destino se adjunta a continuación:

**APLICA UNICAMENTE SI HAY UN SOLO DISPOSITIVO DESTINO**

| **CARACTERISTICA** | **DESCRIPCION DE DISPOSITIVO DESTINO** |
| --- | --- |
| Tipo de Dispositivo | [*Identificar tipo de dispositivo*] |
| Marca | [*Identificar marca del dispositivo*] |
| Serial Físico | [*Describir el serial físico*] |
| Estado Físico | [*Describir el estado fisico*] |
| Capacidad total | [*Describir la capacidad del dispositivo*] |
| Espacio utilizado o Peso | [*Describir espacio usado* (Xinorbis)] |
| Número Archivos | [*Describir número de archivos total* (Xinorbis)] |
| Número Carpetas | [*Describir número de carpetas total* (Xinorbis)] |
| Serial Lógico | [*Describir serial lógico*] |
| Estado Lógico | [*Describir estado lógico*] |

Tabla 5 Caracteristicas técnicas de contenedor de evidencia digital de destino.

El resultado final del proceso se encuentra en el contenedor de evidencia digital anteriormente nombrado. Este contenedor tiene su correspondiente cadena de custodia que reposan en el expediente del caso. La información mantiene su integridad y validez probatoria mediante las imágenes forenses y huellas hash según lo indica el Articulo 11 de la Ley 527 de 1999.

**APLICA UNICAMENTE SI HAY MAS DE UN DISPOSITIVO DESTINO**

El detalle de los [*Numero en texto*] ([*Valor numérico*]) dispositivos contenedores de evidencia digital ([*Describir los tipos de dispositivos copiados*]), de destino se anexan a la presente acta *(Ver Anexo* [*Identificar si es físico o digital*][*Numero secuencial de anexo*]*)*. con la siguiente información por cada dispositivo:

1. ANALISIS FISICO:
   * Radicado del caso al que pertenece.
   * Tipo de dispositivo.
   * Marca.
   * Serial físico.
   * Estado físico.
2. ANALISIS LOGICO:
   * Capacidad total del dispositivo.
   * Espacio utilizado o Peso.
   * Numero de archivos que contiene el dispositivo.
   * Numero de carpetas que se encuentra en el dispositivo.
   * Serial lógico.
   * Estado lógico.

Se verifica el correcto funcionamiento de [*Identificar los contenedores de evidencia digital*] de evidencia digital con el software [*Identificar las herramientas de software empleadas*]. La información mantiene su integridad y validez probatoria mediante las imágenes forenses y huellas hash según lo indica el Articulo 11 de la Ley 527 de 1999.

1. **OBSERVACIONES**
2. **ANEXOS**

De acuerdo a las actividades realizadas anteriormente y el volumen de información, los anexos de la presente acta se entrega un dispositivo ([*Describir los tipos de dispositivos*]) con las siguientes características técnicas:

|  |  |
| --- | --- |
| **DESCRIPCIÓN** | **INFORMACIÓN** |
| Marca | [*Describa marca*] |
| Capacidad | [*Describa capacidad*] |
| Serial Físico | [*Describa serial físico*] |
| Serial Lógico | [*Describa serial lógico*] |
| Número de carpetas | [*Dscriba numero de carpetas*] |
| Número de archivos | [*Describa numero de archivos*] |

Tabla 6 Características técnicas del dispositivo anexo al acta.

El cual contiene los siguientes anexos:

| **IDENTIFICADOR** | **DESCRIPCIÓN** | **CANTIDAD DE FOLIOS *(Anexo fisico)*** | **RUTA *(Anexo Digital)*** |
| --- | --- | --- | --- |
| [*Numero secuencial si aplica*] | Identificación y análisis de dispositivos [*Valor numérico*] contenedores de evidencia digital de origen | [*Si aplica en valor numérico la cantidad de folios*] | [DESCRIBIR TIPO DE DISPOSITIVO]:\ANEXO [*Valor numérico*] - IDENTIFICACION |
| [*Numero secuencial si aplica*] | Cuadros resumen de identificación y copia de dispositivos de origen y destino | [*Si aplica en valor numérico la cantidad de folios*] | DESCRIBIR TIPO DE DISPOSITIVO]:\ANEXO [*Valor numérico*] – RESUMEN COPIA |
| [*Numero secuencial si aplica*] | Paquete de informe de copia de [*Valor numérico*] contenedores de evidencia digital   * + - 1. **(SI APLICA)** Informe de copia ejecutivo       2. **(SI APLICA)** Informe de inspección del dispositivo de origen       3. **(SI APLICA)** Informe de funcionamiento del dispositivo de origen       4. **(SI APLICA)** Informe de inspeccion del dispositivo de destino       5. **(SI APLICA)** Informe de funcionamiento del dispositivo de destino       6. **(SI APLICA)** Informe de copia técnico | [*Si aplica en valor numérico la cantidad de folios*] | DESCRIBIR TIPO DE DISPOSITIVO]:\ANEXO [*Valor numérico*] – INFORMES DE COPIA |
| **TOTAL DE FOLIOS** | | **[*En numero totalizar los folios de los anexos*]** | **NO APLICA** |

Tabla 7 Cuadro resumen de anexos del acta.

La actividad termina el [*Día en letras*] ([*Valor* numérico]) de mes [*Identificar el mes*] del [*Año en letras*] ([*Valor numérico*]) a las [*Horas*]:[*Minutos*] [*en formato militar*], firman los encargados de las actividades técnicas mencionadas y la revisión de la presente acta por parte del GTIFSD,

|  |  |
| --- | --- |
| **Realizado por:**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **[*NOMBRE DE QUIEN REALIZA LA ACTIVIDAD*]**  C.C [*CEDULA*] [*CIUDAD*]  [*Identificar si es servidor o contratista*]  ACE Accessdata Certified Examiner | **Revisado por:**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **[*NOMBRE DE QUIEN REVISA LA ACTIVIDAD*]**  C.C [*CEDULA*] de [*CIUDAD*]  [*Identificar si es servidor o contratista*]  ACE Accessdata Certified Examiner |

**ANEXO [*Numero de anexo*]**

|  |  |
| --- | --- |
| **DESCRIPCIÓN** | **CANTIDAD FOLIOS** |
| Cuadros resumen de identificación y copia de dispositivos de origen y destino | [*Escribir número de folios sin incluir la página de presentación*] |

1. **DISPOSITIVO N° 1.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **TIPO DE ANALISIS** | **CARACTERISTICA** | | **DESCRIPCION**  **DISPOSITIVO ORIGEN** | **DESCRIPCION DE DISPOSITIVO DESTINO** |
| **ANÁLISIS FÍSICO** | Radicado | | [*Indicar el numero de radicado*] | [*Indicar el numero de radicado*] **(SI APLICA)** |
| Ubicación | Cuaderno | [*Identificar si es publico o reservado*] | [*Identificar si es publico o reservado*] **(SI APLICA)** |
| Folio | [*Identificar folio*] | [*Identificar folio*] **(SI APLICA)** |
| Tipo de Dispositivo | | [*Identificar tipo de dispositivo*] | [*Identificar tipo de dispositivo*] |
| Marca | | [*Identificar marca*] | [*Identificar marca*] |
| Serial Físico | | [*Identificar serial fisico*] | [*Identificar serial fisico*] |
| Estado Físico | | [*Identificar el estado físico del dispositivo*] | [*Identificar el estado físico del dispositivo*] |
| **ANÁLISIS LÓGICO** | Capacidad total | | [*Identificar en GB la capacidad del dispositivo*] | [*Identificar en GB la capacidad del dispositivo*] |
| Espacio utilizado o Peso | | [*Identificar en GB el espacio utilizada en el dispositivo*] | [*Identificar en GB el espacio utilizada en el dispositivo*] |
| Número Archivos | | [*Cantidad de archivos*] | [*Cantidad de archivos*] |
| Número Carpetas | | [*Cantidadde carpetas*] | [*Cantidadde carpetas*] |
| Serial Lógico | | [*Identificar serial logico*] | [*Identificar serial logico*] |
| Estado Lógico | | [*Identificar el estado lógico* (Optimo, malo)] | [*Identificar el estado lógico* (Optimo, malo)] |

**ANEXO [*Numero de anexo*]**

|  |  |
| --- | --- |
| **DESCRIPCIÓN** | **CANTIDAD FOLIOS** |
| Paquete de informe de copia de [*Valor numérico*] contenedores de evidencia digital | [*Escribir número de folios sin incluir la página de presentación*] |

**DISPOSITIVO 1**

1. **INFORME DE COPIA EJECUTIVO**

**INCLUIR INFORME DE COPIA EJECUTIVO**

1. **(SI APLICA) INFORME DE INSPECCIÓN DEL DISPOSITIVO DE ORIGEN**

|  |
| --- |
| [*Incluir el informe de funcionamiento*] |

1. **(SI APLICA) INFORME DE FUNCIONAMIENTO DEL DISPOSITIVO DE ORIGEN**

|  |
| --- |
| [*Incluir el informe de funcionamiento*] |

1. **(SI APLICA) INFORME DE INSPECCIÓN DEL DISPOSITIVO DE DESTINO**

|  |
| --- |
| [*Incluir el informe de funcionamiento*] |

1. **(SI APLICA) INFORME DE INSPECCIÓN DEL DISPOSITIVO DE DESTINO**

|  |
| --- |
| [*Incluir el informe de funcionamiento*] |

1. **(SI APLICA) INFORME TÉCNICO DE COPIA DEL DISPOSITIVO DE ORIGEN AL DESTINO**

|  |
| --- |
| [*Incluir el informe de funcionamiento*] |

1. Mensaje de Datos: “información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax” Ley 527 de 1999. [↑](#footnote-ref-1)