Elaborado o modificado por: **Bach. Federico Sáenz Rodríguez** **Perito en Análisis Forense de Imagen**	**Revisado por Líder Técnico:** **Bach. Federico Sáenz Rodríguez** **Líder Técnico de Sección**
Visto Bueno Encargado de Calidad: **Lic. José Alfonso Rodríguez Arias** **Encargado de Calidad de la Sección Imagen y Sonido Forense**	**Aprobado por:** **Lic. Marco Herrera Charraun** **Jefe, Sección de Imagen y Sonido Forense**

CONTROL DE CAMBIOS A LA DOCUMENTACIÓN

Versión	Fecha de aprobación	Fecha de revisión	Descripción del cambio	SCD	Solicitado por
01	22/12/2020	16/09/2022	Versión inicial del procedimiento	30-SCD-ISF-2020	MHC
02	16/09/2022	31/07/2023	Formato nuevo. Inclusión de instrucciones sobre resultados e interpretación. Lenguaje inclusivo.	004-SCD-ISF-2022	MHC
03	31/07/2023	-	Ajustes redacción e inclusión textos prerredactados (punto 10).	007-SCD-ISF-2023	MHC

1 Objetivo:

Unificar la manera en que se realiza la recuperación de contenido material fotográfico o de video desde artefactos como cámaras fotográficas digitales, dispositivos de memoria extraíbles, discos ópticos y grabadores de sistemas de vigilancia electrónica.

2 Alcance:

Aplica para el personal pericial en análisis forense de imagen de la Sección de Imagen y Sonido Forense del Departamento de Ciencias Forenses que realizan un servicio de recuperación de material de fotografías y videos de dispositivos en condiciones de laboratorio.

La recuperación de datos se entenderá como la inspección pericial de dispositivos de almacenamiento realizado para duplicar las fotografías y videos legibles y que a la vez pretende el rescate del material que ha sido descartado por el usuario o deteriorado por errores lógicos de almacenamiento siendo que esta información podría ser reconstruida combinando herramientas específicas para dicha tarea.

Este procedimiento se refiere a la recuperación de material fotográfico y de video digital de dispositivos como tarjetas de memoria, discos ópticos, cámaras fotográficas, cámaras de video digital, cámaras de acción, cámaras en automóviles (dashcam), grabadores digitales de audio o grabadores de sistemas de vigilancia electrónica (DVR).

Para todo caso de recuperación de datos es importante evaluar el resumen de los hechos y la descripción de las imágenes de interés para la investigación. Para elegir el método de recuperación resulta necesario que el usuario manifieste el objetivo concreto del análisis solicitado o el tipo de contenido de interés.

Contacte a la persona solicitante por correo electrónico o llamada telefónica si el formulario de solicitud de dictamen f083i no brinda información suficiente sobre el instante de interés. Registre estas comunicaciones en el legajo del caso en el SADCF.

Los soportes de almacenamiento de este material incluyen:

- Tarjetas de memoria extraíbles de familias de formatos como Secure Digital Card (SDC, SDHC and SDXC), MicroSD, xD Card (xD), Compact Flash Card (CFC), MicroDrive (MD), Memory Stick Card y entre otros.
- Memoria interna de cámaras (cuando cuentan con ella).
- Recuperación de material no legible en grabadores de sistemas de vigilancia electrónica (DVR) con almacenamiento de video en formato H.264.

Es posible que el método de almacenamiento utilizado por el fabricante impida total o parcialmente la recuperación de estos datos. Este escenario podría ser detectado y reportado tras aplicar los métodos de inspección enlistados en este documento.

El material recuperado de éstos podría requerir procesamiento adicional para mostrar adecuadamente la grabación tales como ajustes de proporción, frecuencia de cuadros por segundo, demultiplexado u otros. De ser necesario acuda al procedimiento "Procesamiento de evidencias de video".

El presente procedimiento excluye la inspección de aparatos telefónicos, tabletas, computadores de escritorio o portátiles. La recuperación de datos de este tipo de indicios es competencia de la Sección Especializada contra el Cibercrimen.

Esta metodología se encuentra validada en el Informe de validación 001-ISF-VAL-2020.

3 Referencias:

[1] Manual de Instrucciones del SADCF. Departamento de Ciencias Forenses. Versión vigente.

[2] Procedimiento "*Gestión de indicios de imagen y sonido mediante QuickDME*". Sección Imagen y Sonido Forense. Departamento de Ciencias Forenses. Versión vigente.

[3] Procedimiento "*Procesamiento de evidencias de video*". Sección Imagen y Sonido Forense. Departamento de Ciencias Forenses. Versión vigente.

[4] Procedimiento "*Gestión de Solicitudes y Manejo de Indicios*". Departamento de Ciencias Forenses. Versión vigente.

[5] Ariffin A, Slay J, Choo KK. *Data recovery from proprietary formatted CCTV hard disks*. In: Advances in Digital Forensics IX. Berlin Heidelberg: Springer; 2013. pp 213-223

[6] City of Madison Police Department. *Digital Forensics*. Consulta web. https://www.cityofmadison.com/police/documents/sop/DigitalForensics.pdf

[7] Fan Yang, Rongrong Li y Chunsheng Wu. Basic Principle and Application of Video Recovery Software for Dahua and Hikvision Brand. General Division of Criminal Investigation, Beijing Public Security Bureau. SHS Web of Conferences. Volume 14, 2015.

[8] Houston Forensic Science Center. *Physical and Logical Imaging Technical Procedure*. https://records.hfscdiscovery.org/Pages/Multimedia.aspx

[9] INTERPOL. *INTERPOL Global Guidelines for Digital Forensics Laboratories*. https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf

[10] Jaehyeok Han, et al. *Analysis of the HIKVISION DVR File System*. Center for Information Security Technologies (CIST), Korea University. Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2015. J.I. James and F. Breitinger (Eds.): ICDF2C 2015, LNICST 157, pp. 189–199, 2015.

[11] Scientific Working Group on Digital Evidence. *SWGDE Proposed Techniques for Advanced Data Recovery from Security DVRs*. Consulta web. https://www.swgde.org/documents

[12] Scientific Working Group on Digital Evidence. *SWGDE Position on the Use of MD5 and SHA1 Hash Algorithms in Digital and Multimedia Forensics*. Consulta web. https://www.swgde.org/documents

[13] Scientific Working Group on Digital Evidence. *SWGDE Best Practices for Computer Forensic Acquisitions*. Consulta web. https://www.swgde.org/documents

[14] Scientific Working Group on Digital Evidence. *SWGDE Best Practices for Maintaining the Integrity of Imagery*. Consulta web. https://www.swgde.org/documents

[15] Tobin Lee, Ahmed Shosha, Pavel Gladyshev. *Reverse engineering a CCTV system, a case study*. Digital Investigation. Volume 11, Issue 3, 2014. Pages 179-186.

[16] U.S. Department of Justice. *Forensic Examination of Digital Evidence: A Guide for Law*

Enforcement. https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

[17] Informe de validación 001-ISF-VAL-2020. Imagen y Sonido Forense. Departamento de Ciencias Forenses. Organismo de Investigación Judicial (OIJ). Poder Judicial de Costa Rica. 2020.

4 Equipos y materiales:

4.1 Equipos:

- Computadora con sistema operativo Windows 10 o superior con aplicaciones de ofimática LibreOffice 6.4 o superior, acceso a SADCF (Sistema Automatizado del Departamento de Ciencias Forenses) Acrobat Reader DC , QuickDME, lector de tarjetas "smart card" para firma digital y acceso a Internet.
- Estación de trabajo para análisis de imágenes. Con aplicaciones para las diferentes etapas del análisis, a saber:
  - Para confección de imágenes forenses y cálculo hash SHA1, SHA2 o MD5 como FTK Imager 4.3 o superior.
  - Para la confección de un reporte S.M.A.R.T. de discos duros como smartctl 7.3
  - Para la visualización e inspección de material fotográfico o de video (como ffmpeg, ffprobe, BsrVideoAnalyzer, MP4 Inspector, VirtualDub 2, MPC-HC o similares)
  - Para recuperación de datos como CnW Forensic o Adroit Photo Forensics.
  - Para inspección de discos de grabadores de seguridad como DVR Examiner
  - Python y el editor IDE de elección (como IDLE, Spyder, Eclipse o similar) para la confección y edición de rutinas de asistencia para la automatización de tareas de recuperación.
  - Software para quemado de discos ópticos.
- Computadora con sistema operativo Linux, con programa para confección de imágenes (como HDDSuperClone o Guymanger), Python 3.8 o superior con software IDE y software para visualización e inspección de material fotográfico (como ffmpeg y VLC o similares).
- Lector de tarjetas forense solo lectura.
- Dispositivo de acceso solo lectura para discos SATA como Tableau Forensic SATA Drive Bay T3iu, Tableau Forensic Universal Bridge T356789iu o Forensic UltraDock Write Blocker.
- Certificado de firma digital.

4.2 Materiales:

N/A

5 Reactivos y materiales de referencia:

N/A

6 Condiciones ambientales:

N/A

7 Procedimiento:

7.1 Preparación del material para análisis:

Nota 1: Es indispensable que se analice cada dispositivo que será sometido a un proceso de recuperación de manera individual. Esto se debe a las significativas diferencias en el método de extracción según las particularidades del hardware y software de origen así como la complejidad a la que suele llegar la descripción del contenido de cada dispositivo. Para ello, cuando resulte oportuno, se debe informar al solicitante que se embalen los indicios por aparte para así conseguir la asignación de un número de orden de trabajo para cada objeto a fin de preservar la legibilidad de los dictámenes emitidos y las herramientas de registro.

7.1.1 Realice la apertura y descripción de indicios documentando este proceso mediante la funcionalidad del SADCF "Apertura y descripción de los indicios" (referirse al Procedimiento Gestión de Solicitudes y Manejo de Indicios punto 7.11). Si al realizar la apertura se encuentran varios dispositivos de almacenamiento asigne un número de indicio, describa y procese cada uno de ellos individualmente.

7.1.2 Inspeccione el indicio en busca de cualquier señal externa de daño (fractura, abolladura, suciedad, indicios de quemaduras, conectores en mal estado u otros). De encontrarse, reporte su hallazgo durante el proceso de apertura y descripción de indicios. Si hay medidas correctivas viables y exitosas consígnelas (por ejemplo, limpieza de conectores u otras tareas menores). Si los defectos visibles podrían comprometer el funcionamiento vaya al punto 7.3.

7.1.3 Cree en el disco de trabajo de la estación de análisis una carpeta nominada de acuerdo al número de caso completo. Cree subcarpetas nombradas en correspondencia al número de indicio. Éstas tendrán a su vez subcarpetas conteniendo los resultados de cada paso. Esas subcarpetas tendrán un nombre compuesto por: *##_DescripciónProcesoRealizado*. De ese modo, el nombre de las subcarpetas describirá la secuencia de procesos aplicados en orden.

7.1.4 Conecte el dispositivo de almacenamiento a la estación de trabajo asegurándose de utilizar un medio que impida la escritura. Para ello utilice el dispositivo forense de conexión solo lectura que corresponda de acuerdo al tipo de indicio remitido.

7.1.5 Confirme que la conexión brinde acceso físico y lógico al dispositivo. Considere que algunos sistemas de archivos propietarios (por ejemplo los de discos de grabadores de vigilancia) impedirían al sistema operativo el acceso lógico a los datos. En tales casos confirme el acceso a nivel de bytes mediante inspector hexadecimal o FTK Imager. Si no se obtiene acceso vaya al punto 7.3.

7.1.6 Confeccione un reporte SMART si el indicio es un disco duro dentro de un grabador y añada el reporte PDF resultante a la carpeta de destino según la estructura señalada en el punto 7.1.3.

Nota 2: Si el indicio es un disco duro dentro de un grabador y el resumen de los hechos insinúa una posible manipulación dolosa del contenido es recomendable usar guantes al acceder al interior del grabador y manipular cuidadosamente los componentes internos ante la posibilidad de que sea conveniente para la investigación la búsqueda de huellas digitales.

7.2 Inspección preliminar de espacio vacío o espacio lleno con patrones de sobrescritura:

Nota 3: La inspección o conteo del espacio vacío podría ayudar a detectar de antemano aquellos dispositivos en que la recuperación no es viable. Un dispositivo completamente ocupado con

valores en cero o patrones de sobrescritura podría reportarse tras esta inspección como un dispositivo sin contenido recuperable. De igual forma podría reportarse aquel dispositivo en el cual el cálculo de espacio disponible que brinda el sistema operativo coincide con el número de bytes en cero o con patrones de sobrescritura.

7.2.1 Realice una inspección preliminar del dispositivo mediante un inspector hexadecimal. Observe la cantidad de espacio con valores en 0 o escritos con patrones de sobreescritura. De ser necesario contabilícelo.

7.2.2 Observe si el monto de espacio de almacenamiento del dispositivo coincide con la cantidad de espacio vacío (alojando ceros o con patrones de desborrado). De ser así, no será posible realizar ninguna recuperación. En tal caso registre este resultado en la funcionalidad de Registro de Datos y Resultados y emita el dictamen indicando esta situación.

7.3 Medidas a tomar si el dispositivo de almacenamiento presenta problemas de acceso por defectos mecánicos o electrónicos que impiden la confección de la imagen:

7.3.1 *Memoria USB o tarjeta de memoria:* Emita un dictamen indicando la imposibilidad de acceso por falta de la tecnología y procedimiento adecuado para el acceso directo a los bancos de memoria.

7.3.2 *Disco duro que manifiesta errores tras alcanzar cierto avance en su proceso de imagen:* Realice la imagen mediante software que permita enumerar y brincar los sectores malos como el HDDSuperClone en una terminal con sistema operativo Linux. Realice la imagen parcial. El reporte del proceso deberá incluirse en el legajo del caso mediante la funcionalidad de Registro de datos y Resultados del SADCF. Una vez finalizado este proceso intente la recuperación del material que no hayan sido afectados por los sectores dañados según se indica en el punto 7.5

7.3.3 *Disco duro de un grabador que manifiesta sonidos de golpes, clicks, fricción, pitidos durante su funcionamiento o no enciende:* Reporte el comportamiento y desperfecto observado. Emita un dictamen indicando la imposibilidad de acceso por falta de la tecnología y procedimiento adecuado para el acceso a discos con desperfectos mecánicos o electrónicos.

7.4 Confección de la imagen del dispositivo de almacenamiento en el disco de trabajo de la estación de análisis:

Nota 4: La confección de una imagen del dispositivo está dirigida a evitar las modificaciones, el desgaste y el riesgo de daños por el uso prolongado del indicio durante su análisis. Existen instancias en que se puede hacer una excepción a la confección de la imagen: a) un dispositivo de gran tamaño (superior a 2TB) que supere las capacidades de almacenamiento para la confección de la imagen o B) si dados el relato e inspección preliminar del equipo se denota de antemano que la recuperación del material de un disco duro es técnicamente rápida y la confección de la imagen sería contraproducente por generar riesgo de desgaste mecánico excesivo sobre dispositivo analizado.

7.4.1 Confeccione la imagen utilizando la aplicación FTK Imager.

7.4.2 Asegúrese de llenar los campos de los datos del caso al confeccionar la imagen porque éstos figurarán y serán pertinentes en el reporte final del FTK Imager.

7.4.3 Seleccione el formato Raw (DD) para para la imagen. Sin fragmentar.

7.4.4 Nomine esta imagen utilizando el ID de objeto que le otorgó el SADCF al indicio.

7.4.5 Habilite la opción de validación que comparará el cálculo del código hash del contenido en el dispositivo de almacenamiento con el cálculo del código hash de la imagen resultante. Si la validación no es exitosa, repita el proceso. Si falla nuevamente reporte un problema de funcionamiento del dispositivo de origen indicando que la inestabilidad en la lectura está usualmente asociada a desperfectos mecánicos o electrónicos.

7.4.6 Elija como carpeta de destino según la estructura señalada en el punto 7.1.2.

7.4.7 Repita los pasos 7.4.1 al 7.4.6 para cada dispositivo de almacenamiento.

7.5 Elección del método o combinación de métodos para recuperación de tarjetas de memoria:

7.5.1 Analice el método o combinación de métodos que mejor se ajuste a esas condiciones considerando que los métodos de almacenamiento de información digital varían y las fuentes de estas diferencias incluyen el hardware, software, sistema operativo, versión de software o el uso alternativo del software o hardware de manera diferente a su diseño original.

7.5.2 Utilice la herramienta de recuperación que mejor se ajuste a la información de interés y las características del material remitido a análisis. Entre algunas podría figurar: Forensic Tool Kit Imager (FTK Imager), CnW Recovery Forensic, Adroit Photo Forensics, HxD entre otras. Refiérase a la funcionalidad de ayuda de cada una de las herramientas.

7.5.3 Explore un duplicado del material recuperado para localizar el material que el solicitante señaló como de interés para la investigación. Si el material se encuentra continúe al punto 7.5.8.

7.5.4 Considere que algunos dispositivos como cámaras de dash o cámaras de acción, a fin de poder almacenar la información al vuelo, utilizan estrategias de almacenamiento diferentes; que guardan los archivos en fragmentos no ordenados. Bajo estas circunstancias los programas de recuperación comerciales forenses suelen fallar en recuperar el material porque los componentes internos que conforman la estructura del formato se encuentran en desorden. De ser así, realice una inspección hexadecimal de la imagen del dispositivo, evalúe la estrategia utilizada y manualmente reconstruya los archivos.

Nota 5: Aunque la recuperación de los escenarios descritos en el punto 7.5.4 puede realizarse manualmente es aconsejable la automatización de la tarea mediante rutinas confeccionadas con lenguajes como Python. Documente los hallazgos combinación de herramientas utilizadas mediante la funcionalidad de Datos y Resultados del SADCF.

7.5.5 Evalúe si el monto de material legible, la cantidad de material recuperado y la cantidad de espacio vacío suman una cantidad similar a la capacidad del dispositivo. Si las cantidades son similares, pero no se encontró el material de interés, se considera una recuperación completa y se puede decir que el material buscado no está presente el el dispositivo remitido para análisis. En tal caso registre este resultado en la funcionalidad de Registro de Datos y Resultados del SADCF y emita el dictamen indicando esta situación.

7.5.6 Evalúe si la cantidad de material desborrado es desproporcionadamente menor que el espacio disponible menos el espacio vacío. Si se cumple esta relación y aún no se encontró el material de interés complemente el proceso de recuperación con otras herramientas de recuperación como las enlistadas en el punto 7.5.3

7.5.7 Repita los pasos descritos en los puntos 7.5.4 al 7.5.6 utilizando otras de las herramientas de recuperación. Si tras ello aun sigue sin recuperarse el material de interés y además persiste un

bloque de datos no interpretables por las herramientas de recuperación registre este resultado mediante la funcionalidad de Registro de Datos del SADCF y Resultados y emita el dictamen indicando la imposibilidad de confirmar la presencia del material de interés.

7.5.8 Compile el material recuperado que coincida con lo indicado en la solicitud y genere su correspondiente cálculo del código hash SHA-256 o superior. Genere un PDF con el listado de archivos y su cálculo hash e incorpórelo firmado digitalmente al legajo digital del caso en el SADCF mediante la funcionalidad de Reporte de Datos y Resultados.

7.6 Métodos de recuperación para discos duros de grabadores de seguridad:

Nota 6: Considere que un desajuste en la hora y fecha del reloj interno de un grabador de seguridad podría haber desviado la asignación de estos valores durante la grabación del evento. Podría ser necesario recabar información de parte de la persona que obtuvo el indicio y sus observaciones sobre estos parámetros al momento del decomiso.

7.6.1 Conecte el disco que se encontraba inserto en el grabador a la estación de análisis mediante bloqueador de lectura.

7.6.2 Confeccione una imagen del disco como se indica en el punto 7.4.

7.6.3 Realice una inspección preliminar mediante DVR Examiner a fin de determinar si es viable la recuperación mediante sus funcionalidades. Evalúe si detecta y recupera adecuadamente el evento de interés señalado por el solicitante. Si el material se encuentra continúe al punto 7.6.11.

7.6.4 Evalúe mediante la inspección con lector hexadecimal si hay contenido en formato H.264. Para ello verifique la presencia frecuente de secuencias hexadecimales de unidades NAL (por ejemplo 0x00000165). Utilice como material de referencia las recomendaciones de marcadores descritos en el documento "*SWGDE Proposed Techniques for Advanced Data Recovery from Security DVRs.*" [11]. Si el encabezado y el material en el disco sugieren una estructura de datos de tecnología Hikvision utilice los marcadores descritos en el documento "*Analysis of the HIKVISION DVR File System*" [10] para la inspección del contenido en el disco.

7.6.5 Evalúe mediante la inspección con lector hexadecimal la estrategia de almacenamiento por bloques que utiliza el grabador. Si el disco no muestra claramente la estructura de almacenamiento que utiliza el grabador será necesario confeccionar una muestra de comparación. Para ello inserte un disco blanqueado en el grabador remitido para análisis, conecte varias cámaras y haga una grabación de referencia. Evalúe el resultado para determinar la forma en que debe explorarse el contenido del disco en análisis.

7.6.6 Tome muestras de la imagen de disco cuestionado para realizar un mapeo de las fechas del material almacenado en el disco. La frecuencia de las muestras dependerá de la configuración del equipo. Se espera que la frecuencia sea tal que hayan al menos cuatro consecutivas asociadas al mismo día. Aunque esta tarea puede realizarse manualmente es aconsejable la automatización de la tarea mediante rutinas confeccionadas con lenguajes como Python, hechas a la medida según los hallazgos del punto 7.6.5.

7.6.7 Almacene cada muestra en el disco de trabajo utilizando como nombre el desplazamiento (offset) del cual fue tomado.

7.6.8 Ejecute una reencapsulación a cada muestra cuando ello sea necesario para su reproducción posterior. De ser así, utilice ffmpeg con alguna fórmula similar a *ffmpeg -i origen.mp4 -c:v copy -c:a copy salida.mkv*.

7.6.9 Reproduzca cada una de las muestras recabadas, observe la hora y fecha mostradas en pantalla y tome nota en una hoja de cálculo o tabla de texto. Tras repetir esto con todas las muestras se obtendrá una tabla que muestra las fechas del material almacenado en el disco y su distribución en el disco de acuerdo a su offset.

7.6.10 Realice duplicados del contenido en las direcciones (offsets) que más se aproximen a las fechas de interés según los resultados de la inspección realizada entre los puntos 7.6.5 y 7.6.7.

7.6.11 Seleccione entre este material aquellos que coinciden con el material solicitado.

7.6.12 Si el formato de origen lo requiere, confeccione copias reencapsuladas o aplique una transcodificación sin pérdida para que el usuario pueda reproducir el material. Opcionalmente, aporte en los resultados el reproductor pertinente para su acceso.

7.6.13 Compile el material recuperado y genere de éste un listado que incluya el cálculo del código hash SHA-256 o superior. Genere un PDF con ese listado e incorpórelo firmado digitalmente al legajo digital del caso en el SADCF mediante la funcionalidad de Reporte de Datos y Resultados.

8 Criterios de aceptación o rechazo de resultados:

No.	Criterio de aceptación	Valor límite	Corrección aplicable
1	Dispositivo en mal estado	N/A	Aplique las medidas en punto 7.3
2	Disco de grabador se seguridad no tiene marcadores de video H264 y el proceso de toma de muestra no sugiere método de recuperación	N/A	Reporte mediante dictamen que el grabador utiliza un método de grabación de tecnología para el cual no se cuentan con herramientas ni método de recuperación.

9 Cálculos y evaluación de la incertidumbre:

N/A

10 Reporte de análisis y resultados:

10.1 Registro del proceso y preparación de material para entrega:

10.1.1 Utilice la funcionalidad de Registro de Datos y Resultados del SADCF, y el grupo de análisis "Recuperación de Datos" para documentar los valores correspondientes a la utilización del espacio de almacenamiento y las cantidades de datos recuperados.

10.1.2 Almacene en el QuickDME las tablas u hojas de cálculo con el listado de las muestras, los listados de archivos resultantes y sus correspondientes cálculos hash, así como los reportes generados por los programas de recuperación pertinentes para el análisis según se detalla en el procedimiento "*Gestión de indicios de imagen y sonido mediante QuickDME*".

10.1.3 Genere un reporte de todo el material que fue incluido en el QuickDME mediante un Tag Report.

10.1.4 Incluya el reporte del material incluido en el QuickDME como dato adjunto al proceso de Registro de Datos y Resultados del Análisis.

10.1.5 Confeccione un disco maestro con el material compilado que haya podido ser recuperado y con reportes los hash que identifican esos ficheros. Según las características del material podría ser conveniente añadir algún reproductor particular para facilitar la visualización al usuario. Genere un indicio derivado mediante la funcionalidad de Datos y Resultados del SADCF para asignar un ID de objeto a este disco maestro. Embale y acompañe de boleta de cadena de custodia para entrega y la custodia posterior por parte del solicitante. Describa este disco en el apartado 6 del dictamen.

10.1.6 Confeccione un segundo disco con el mismo contenido que el que ha sido confeccionado en el punto 10.5. Registre la confección y las características de este disco en el SADCF creando una observación del tipo Productos ISF. Este disco será una copia de trabajo también destinada a la custodia posterior por parte del solicitante. Describa este disco en el apartado 6 del dictamen.

10.1.7 Prepare un dictamen en el que figurará como resultado el listado general con los rangos de fechas detectados en el dispositivo. Si el material de interés se encontró haga referencia al apartado 6 del dictamen donde estará el detalle de los discos confeccionados. Si no se encuentra el material indíquelo explícitamente en el apartado de resultados.

Nota 7: La estación de trabajo y sus discos no son el repositorio final de los indicios recabados. Es posible que el tamaño de los discos en la estación de análisis permita el almacenamiento temporal de la carpeta de algunos casos. Su conservación temporal, en algunas circunstancias, podría simplificar el abordaje de alguna posible ampliación o referencia de otro tipo. Pero es importante considerar que se debe dar prioridad a la existencia de espacio suficiente para el adecuado funcionamiento de la estación de trabajo.

10.2 Reporte de hallazgos e interpretación:

Nota 8: El proceso de recuperación de material de dispositivos corresponde a un reporte de resultados y no requieren la interpretación por parte del analista. La excepción a esto es la recuperación de grabadores imposible debido a la sustitución del disco; en este escenario es viable la interpretación dada la combinación síntomas (ver ejemplo en escenario b, punto 10.2.1).

Nota 9: Los textos prerredactados indicados abajo son un puntos de partida y referencia. En ocasiones podrían requerir la modificación por parte del analista a fin de adaptarlo a la gran variedad de diferentes escenarios posibles

10.2.1 Utilice la funcionalidad Registro de Datos y Resultados para registrar los resultados del análisis. El SADCF contempla un conjunto de textos prerredactados para las condiciones más comunes divididos en dos grupos: a) Recuperación de tarjetas y memoria interna de cámaras y b) Recuperación de grabador de seguridad. Los escenarios contemplados son:

a) Recuperación de tarjetas y memoria interna de cámaras:

- Recuperación estándar:

  "Tras la inspección del dispositivo identificado como tarjeta de memoria objeto ID 360000009-2021 se encontraron:

  - *## fotografías legibles y ## fotografías recuperables,*
  - *## videos legibles y ## videos recuperables.*

  Siguiendo las indicaciones de la persona solicitante se realizó la recuperación del material asociado al evento de interés totalizando ## fotografías y ## videos.

  Todo el material recuperado se entrega en los soportes descritos en el punto 6."

- Dispositivo con espacio disponible en blanco:

"Tras la inspección del dispositivo identificado como tarjeta de memoria objeto ID 360000000-2023 se recuperaron:

- *## fotografías legibles,*
- *## videos legibles.*

El dispositivo tiene en sus áreas disponibles para almacenamiento un valor de 0. Es decir, en ellas no hay contenido borrado, únicamente espacio vacío. Por este motivo no es viable aplicar métodos de recuperación.

Todo el material recuperado se entrega en los discos descritos en el punto 6."

- Dispositivo lleno:

"Tras la inspección del dispositivo identificado como tarjeta de memoria objeto ID 360000009-2021 se encontraron ## fotografías legibles y ## videos legibles.

El dispositivo de almacenamiento se encuentra lleno de material legible. Por este motivo no es viable aplicar métodos de recuperación.

Siguiendo las indicaciones de la persona solicitante se realizó la recuperación del material asociado al evento de interés totalizando ## fotografías y ## videos.

Todo el material recuperado se entrega en los soportes descritos en el punto 6."

- Dispositivo dañado:

"Se intentaron diversos métodos de acceso al contenido y recuperación. No se consiguió ningún tipo de detección de contenido del dispositivo de almacenamiento.

El comportamiento observado sugiere que la tarjeta podría presentar un daño en su firmware, daño físico en tarjeta lógica o en sus bancos de almacenamiento.

Los equipos y metodologías implementadas en nuestra sección no están adecuadas para resolver problemas de carácter físico o electrónico como el presentado por el material remitido para análisis.

Dada la combinación de condiciones antes descritas no es posible realizar la recuperación de los datos solicitada."

b) Recuperación de grabador de seguridad:

- Recuperación estándar:

"El disco dentro del grabador muestra una estructura de datos similar a la utilizada por el sistema de archivos de los equipos de vigilancia marca XXXX.

Tras la inspección del material almacenado en el disco se encontró que su contenido corresponde a:

- *Bloques de video legible que corresponden al plazo entre las HH:mm del DD/MM/YYYY y las HH:mm del DD/MM/YYY.*
- *Bloques de material recuperable correspondiente a fragmentos entre las HH:mm del DD/MM/YYY y las HH:mm del DD/MM/YYY.*
- *Trozos de residuos de material de video parcialmente sobrescrito con marcadores de otras fechas no asociadas al plazo de interés indicado por la persona solicitante.*

Dentro del grabador se encontró información asociada a cuatro cámaras.

Siguiendo las indicaciones de la persona solicitante se logró la recuperación del material asociado al lapso entre las HH:mm y las HH:mm del día DD/MM/YYY.

El material extraído se prepara para su entrega al solicitante en los discos descritos en el punto 6."

- Recuperación imposible por disco de grabador sustituido:

"Tras la inspección del disco identificado como objeto 360000000-2023 se encontró que, según lo indicado en las propiedades de los archivos así como la hora y fecha indicadas en pantalla, el contenido legible corresponde al plazo comprendido entre las HH:mm del DD/MM/YYYY y las HH:mm del día DD/MM/YYYY.

Ese material de video ocupa ### gigabytes de los #### gigabytes de capacidad del disco. El resto del espacio está vacío (cada espacio registra valor de 0). Es decir, no hay otra información para recuperar (desborrar) fuera del rango de video ya mencionado.

Se realizó un examen de la información registrada en el disco por su sistema de control SMART (Self-Monitoring, Analysis, and Reporting Technology). Entre los datos recabados destaca que al momento en que se realiza su inspección en el laboratorio el disco tenía contabilizadas ## horas de funcionamiento. Cabe destacar que las horas de trabajo son similares a las aproximadamente ## horas de registro de video en el disco.

- Interpretación de los resultados:

Todo lo anterior indica que el disco dentro del grabador se instaló nuevo y que la mayoría de sus horas de funcionamiento han sido dedicadas al almacenamiento del material de video del plazo señalado arriba.

Por tanto, el disco dentro del grabador no contiene material asociado al plazo de interés señalado por la persona solicitante

11 Medidas de seguridad y salud ocupacional:

N/A

12 Simbología:

N/A: No aplica.

NAL: del inglés Network Abstraction Layer, es parte del estándar del estándar de codificación de material H264 y HEVC que consiste en subdividir el material de video en cápsulas para favorecer su transmisión por red. Cada cápsula cuenta con un marcador al inicio que describe el tipo de contenido que acarrea. El examen de esos marcadores al inicio de cada cápsula es útil para recuperar material.

SADCF: Sistema Automatizado del Departamento de Ciencias Forenses.

QuickDME: Conjunto base de datos y programas que incluyen el AccessDME, QuickDownloader Evidence Tag y otras herramientas administrativas dirigidas al almacenamiento seguro de evidencia digital.

13 Terminología:

Cálculo Hash: Es un algoritmo matemático que genera una representación alfanumérica que es única e irrepetible para cada archivo digital. El alfanumérico resultante es útil para determinar si la información presente en una instancia es igual a otra.

Capacidad del dispositivo: es el monto de datos que un dispositivo es capaz de almacenar. Usualmente se mide en bytes o algunos de sus múltiplos (como megabytes, gigabytes, terabytes)

Códigos MD5 y/o SHA1: secuencias alfanuméricas generada tras la aplicación de algoritmos que resumen y representan de manera individualizada archivos particulares. El MD5 consta de 32 caracteres y el SHA1 de 40 caracteres.

Disco blanqueado: disco o dispositivo de almacenamiento al que se le ha aplicado un proceso de borrado conocido como "wipe" que consiste en sobrescribir todas la áreas de almacenamiento con valores de cero. Para ello es necesario aplicaciones dedicadas para tal fin.

Espacio disponible: áreas del disco que figuran en el índice como disponibles para alojar nuevos datos. Estas áreas podrían contener datos de archivos que fueron eliminados en combinación con espacio vacío.

Espacio vacío: áreas de almacenamiento con extensas secuencias consecutivas de valor asignado de 0. Esta condición es la esperada en espacios de almacenamiento nunca utilizados o aquellos que han sido sujetos a blanqueo (wipe).

Imagen de un dispositivo: archivo que almacena una copia exacta de cada bit, byte y sector del dispositivo de almacenamiento original.

Lector hexadecimal: Programa informático que permite al usuario leer o editar los datos binarios fundamentales que componen un archivo de computadora en su representación hexadecimal.

Material desborrado: ficheros resultantes de un proceso de recuperación de datos.

Material legible: material que está accesible de manera directa por el sistema operativo porque está descrito en el índice del disco y sus datos están almacenados en buen estado en el disco.

Offset: ubicación de un dato en el dispositivo de almacenamiento; se calcula contando la cantidad de bytes que hay entre éste y el primer byte del dispositivo.

Reencapsular: realizar un traslado de los tracks de un archivo de video a otro contenedor sin transcodificarlos.

SMART (acrónimo de Self-Monitoring, Analysis, and Reporting Technology): sistema de control integrado en las unidades de almacenamiento que recopila datos sobre el estado de la unidad y los notifica al usuario.

Transcodificar: conversión directa (de digital a digital) de un códec a otro. Puede ser con o sin pérdida de calidad, dependiendo del códec usado.

14 Anexos

N/A