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

CONTROL DE CAMBIOS A LA DOCUMENTACIÓN

Versión	Fecha de aprobación	Fecha de revisión	Descripción del cambio	SCD	Solicitado por
01	21/12/2018	03/12/2021	Versión inicial del procedimiento	004-SCD-ISF-2018	RVF
02	03/12/2021	16/09/2022	Corrección lenguaje inclusivo, modos verbales y estructura. Referencias.	006-SCD-ISF-2021	MHC
03	16/09/2022	22/12/2022	Formato nuevo. Inclusión de instrucciones sobre resultados e interpretación. Lenguaje inclusivo.	004-SCD-ISF-2022	MHC
04	22/12/2022	31/07/2023	Agregar indicación de validación	005-SCD-ISF-2022	MHC
05	31/07/2023	-	Ajustes redacción e inclusión textos prerredactados (punto 10).	007-SCD-ISF-2023	MHC

1 Objetivo:

Definir el conjunto de métodos aplicables por parte del personal pericial durante el análisis de autenticidad de imágenes.

2 Alcance:

Aplica para todo el personal pericial que realiza el análisis de autenticidad de imágenes en la sección de Imagen y Sonido Forense del Departamento de Ciencias Forenses.

El análisis de autenticidad pretende establecer si las imágenes presentan indicativos de modificación o rastros de procesos de edición, que sugieran que el indicio ha sido sometido a tratamiento posterior a su momento de toma.

La inspección está dirigida principalmente a examinar la integridad del contenedor, su estructura, método de compresión y particularidades esperadas según su equipo de origen. Por este motivo resulta muy importante la presencia de otras muestras de origen común conocido o el aporte del equipo de origen.

Algunos de los análisis podrían ir dirigidos a confirmar la asociación del material con algún presunto equipo de origen o la confirmación de la presunta hora y fecha registrada en el archivo.

Es importante establecer que un proceso de análisis de autenticidad podría ser muy exhaustivo y sus alcances ser altamente dependientes de la formulación de un cuestionamiento debidamente sustentado sobre los indicios. Es decir -por su complejidad- no se practica "de oficio" sin conocerse antes de parte de la persona solicitante alguna presunta anomalía descrita concretamente para ser evaluada y explicada.

Esta metodología se encuentra validada en el Informe de validación 002-ISF-VAL-2022.

Nota 1: La detección de diferencias con el formato esperado o muestra indubitada de comparación puede sugerir la posibilidad de que el contenido haya sido tratado. No por ello se puede concluir que este procesamiento haya sido dirigido a cambiar con dolo el significado y la interpretación de los eventos registrados. Por este motivo el análisis podría requerir una segunda fase dirigida a evaluar la integridad de la información visual en busca de rastros electrónicos de modificación o remoción de elementos, clonación de áreas o combinación de elementos de diferentes imágenes.

Nota 2: Este análisis requiere que la persona solicitante aporte los discos maestros. Solo en casos debidamente calificados y justificados se realizará este análisis utilizando los discos de copia de trabajo.

3 Referencias:

- Choi, Yun-Seok. Design and Implementation of Video File Structure Analysis Tool for Detecting Manipulated Video Contents. International Journal of Internet, Broadcasting and Communication Vol.10 No.3 128-135 (2018), doi: 10.7236/IJIBC.2018.10.3.128
- Devender Singh, Raahat (2017). Digital Video Forensics: Uncovering the Truth in a World of Distorted Realities. eForensics Magazine, 6 (10), 1-274.
- Gloe, Thomas, et.al. Forensic analysis of video file formats. DFRWS Europe 2014 (2014), doi: 10.1016/j.diin.2014.03.009
- Grigorias, Catalin. Forensic Image Analysis System User's Manual. Versión 6, 2018. Forensic

Media Services. Denver, CO. EEUU.

- Grigoras C., and Smith J.M. (2013) Digital Imaging: Enhancement and Authentication. In: Siegel JA and Saukko PJ (eds.) Encyclopedia of Forensic Sciences, Second Edition, pp. 303-314. Waltham: Academic Press.
- Kashyap, Abhishek, Rajesh Singh Parmar, Megha Agarwal and Hariom Gupta. "An Evaluation of Digital Image Forgery Detection Approaches." Compiting Research Repository (CoRR). Abs/1703.09968. 2017.
- Manual de Instrucciones del SADCF. Departamento de Ciencias Forenses. 2017.
- Procedimiento "Análisis preliminar de muestra de imagen". Sección Imagen y Sonido Forense. Departamento de Ciencias Forenses. Versión vigente.
- Procedimiento "Gestión de indicios de imagen y sonido mediante QuickDME". Sección Imagen y Sonido Forense. Departamento de Ciencias Forenses. Versión vigente.
- Procedimiento "Gestión de Solicitudes y Manejo de Indicios". Departamento de Ciencias Forenses. Versión vigente.
- Quinto Huamán, Carlos, et.al. Authentication and integrity of smartphone videos through multimedia container structure analysis. Future Generation Computer Systems Journal (2020), doi: 10.1016/j.future.2020.02.044
- Ramos López, Raquel, et al. Digital Video Source Identification Based on Container's Structure Analysis. IEEEAccess Journal (2020), doi: 10.1109/ACCESS.2020.2971785
- Rodríguez Santos, Francisco, et.al. Practical implementation of a methodology for digital images authentication using forensics techniques. ACSIJ Advances in Computer Science: an International Journal, Vol. 4, Issue 6, No.18 , November 2015.
- Scientific Working Group on Digital Evidence. SWGDE Best Practices for Image Authentication. Version 1.0, Julio 2018. Consulta Web 14/10/2021. https://www.swgde.org/documents/published
- Scientific Working Group on Digital Evidence. SWGDE Best Practices for Image Content Analysis. Version 1.0, Febrero 2017. Consulta Web 14/10/2021. https://www.swgde.org/documents/published
- Song J, Lee K, Lee WY, Lee H. Integrity verification of the ordered data structures in manipulated video content, Digital Investigation (2016), doi: 10.1016/j.diin.2016.06.001.
- Victor, Simon Jerome. Comparative File Structure Analysis of Video Files Sent and Received via WhatsApp. Tesis M.Sc. University of Colorado. 2020.
- Yang, Pengpeng. Efficient video integrity analysis through container characterization. IEEE Journal of Selected Topics in Signal Processing (2020), doi: 10.1109/JSTSP.2020.3008088
- Xiang, Ziyue, et.al. Forensic Analysis of Video Files Using Metadata. 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2021), doi: 10.1109/CVPRW53098.2021.00115.

4 Equipos y materiales:

4.1 Equipos:

- Computadora con sistema operativo Windows 10 o superior con aplicaciones de ofimática LibreOffice 6.3 o superior, acceso a SADCF (Sistema Automatizado del Departamento de Ciencias Forenses), Acrobat Reader DC , lector de tarjetas "smart card" para firma digital y acceso a Internet.
- Estación de trabajo para análisis de imágenes. Con aplicaciones para la visualización, tratamiento y clarificación, además de un programa para cálculo de SHA1 ó MD5 de archivos, lector hexadecimal y aplicación para inspección de autenticidad similar a Amped Authenticate o FIAS.
- Lector de tarjetas. Deseable solo lectura.
- Dispositivo de memoria USB o equivalente.
- Certificado de firma digital.

4.2 Materiales:

No aplica.

5 Reactivos y materiales de referencia:

No aplica.

6 Condiciones ambientales:

No aplica.

7 Procedimiento:

7.1. Inicio de apertura y descripción de indicios:

7.1.1 Para documentar este proceso utilice la funcionalidad del SADCF "Apertura y descripción de los indicios". Referirse al Procedimiento "Gestión de solicitudes y manejo de indicios".

7.1.2 Describa y otorgue un ID de objeto a cada uno de los dispositivos (discos, cámaras, grabadores o tarjetas) que fueron remitidos como material cuestionado y material de referencia.

7.2. Duplicado de material en servidor de evidencia digital:

7.2.1 Almacene el material remitido para el análisis en el servidor de evidencia digital mediante la aplicación QuickDownloader según se describe en el procedimiento "Gestión de indicios de imagen y sonido mediante QuickDME".

7.2.2 Confeccione un Tag Report mediante AccessDME e incorpore el PDF resultante al legajo como un anexo de tipo "Reporte generado por software" firmándolo digitalmente.

Nota 3: Se podrían eximir de la inclusión en el servidor de evidencia digital aquellos casos en que sea muy alta la capacidad de disco ocupada por el material remitido para el análisis. Como referencia, aquellos que superen los 64 Gb. Dada esta circunstancia realice un cálculo hash del material e incorpórelo al legajo como anexo tipo "Reporte generado por software" firmándolo digitalmente.

7.3. Duplicado de material a unidad de disco de estación de trabajo:

7.3.1 El contenido de cada dispositivo analizado se duplicará en el disco de trabajo de la estación. Se realiza una copia de inmediato y será ésta la que contiene los archivos que serán analizados. La estructura de almacenamiento se muestra en la figura 1.

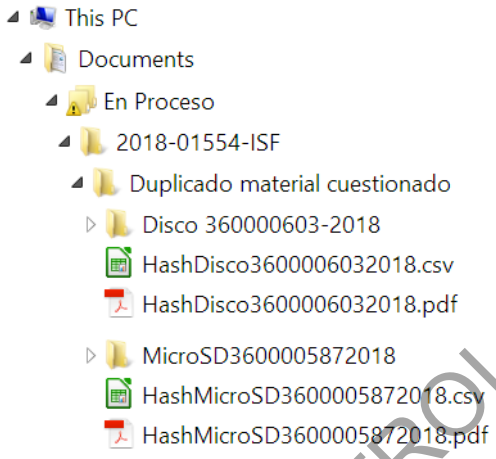

Figura 1: Estructura carpetas de almacenamiento en disco de trabajo.

7.4. Incorporación de reporte de cálculo de hash

7.4.1 Realice el cálculo de los códigos MD5 y/o SHA1 del material presente en aquellos dispositivos cuyo contenido no haya sido descrito durante su inclusión al QuickDME. Realice el cálculo mediante software que genere sus reportes en CSV o TXT. Cada archivo resultante será convertido a PDF mediante el software de elección del analista.

7.4.2 Nombre cada uno de los archivos CSV, TXT y PDF utilizando el número de objeto asignado por el SADCF. Almacénelos en la carpeta nominada "Duplicado de material cuestionado" y su copia correspondiente. Ver figura 1.

7.4.3 Si el material aportado trae un archivo describiendo algún cálculo Hash ejecutado anteriormente cotéjelos con los resultados obtenidos durante la apertura. Reporte en el informe si se encontraron diferencias.

7.4.4 Incorpore al legajo los PDF con los cálculos MD5 y/o SHA1 del contenido de cada uno de los dispositivos de almacenamiento durante el proceso de registro de la apertura de indicios. Para incluirlo incorpórelos al SADCF como anexos tipo "Reporte generado por software" siguiendo las indicaciones en procedimiento "Gestión de solicitudes y manejo de indicios".

7.5 Inspección inicial del hardware de comparación:

7.5.1 Algunos análisis requerirán de la remisión del presunto equipo de origen. Durante el proceso de apertura realice una inspección general de funcionamiento, presencia y contenido de tarjetas de memoria, hora y fecha (tomar nota de desfases).

7.5.2 Si se adjuntan tarjetas de memoria realice una imagen de la misma e incorpórela de la misma manera que se hizo con el material cuestionado según los puntos 7.3 y 7.4.

7.6 Finalización de apertura y destino de indicios:

7.6.1 Revise que haya realizado la inclusión de los reportes Tag del material que haya sido incluido al servidor de evidencia digital mediante QuickDME así como los reportes de cálculo hash que haya sido necesario confeccionar de cualesquiera otros indicios remitidos.

7.6.2 Finalice el proceso de apertura observando la metodología indicada entre los puntos correspondientes del procedimiento "Gestión de solicitudes y manejo de indicios".

7.7 Selección del material de interés:

7.7.1 Basado en la solicitud y descripción de los hechos por parte de la persona solicitante, determine si la cantidad y/o calidad del material tendrá un efecto en la facultad de completar el análisis.

7.7.2 De presentarse insuficiencias determine y gestione la solicitud de material adicional. Si no es posible esto podría impedir la realización del análisis o que sus alcances sean limitados. Estas condiciones deben reportarse en el correspondiente dictamen.

7.7.3 Identifique el material que resulte útil para el análisis de acuerdo a lo indicado por la persona solicitante y la descripción de los hechos. Esta utilidad podría estar dictada por los eventos descritos gráficamente en las imágenes, por las propiedades de los ficheros o ambas.

7.8 Elección de los métodos de análisis que se aplicarán:

7.8.1 Considere que no existe un único método para la autenticación ya que ello dependerá del examen requerido, las particularidades que estén siendo cuestionadas del material, las características de las imágenes y el hardware asociado. Algunos de los métodos se enlistan en los puntos 7.9 y 7.10.

7.9 Inspección de la estructura del archivo de imagen.

7.9.1 Inspeccione la estructura de las imágenes para determinar si hay o no presentes factores que puedan contestar la consulta de la persona solicitante. Los análisis a realizar pueden incluir, entre otros:

- *Análisis del formato de archivo de las imágenes*. Inspección de coherencia entre el material y los tipos de resultados esperados del hardware de origen.
- *Análisis de los metadatos de las imágenes*. Los metadatos pueden ser útiles para identificar la fuente y el historial de procesamiento, pero ellos pueden ser limitados, estar ausentes o sujetos a alteración. Entre los metadatos están: Marca/modelo/serie de la cámara, hora/fecha de creación, ajustes de cámara, resolución y tamaño de imagen, información de geolocalización, nombre de origen, información del lente o flash, frecuencia de cuadros, información de miniaturas asociadas, entre otros.
- *Análisis del contenedor del archivo digital*. podría incluir entre otros: análisis a nivel hexadecimal de cabecera y pie, análisis estructural del EXIF, localización de marcadores de tecnología propietaria, análisis general estructural de componentes del archivo.
- *Análisis de firma de compresión o tablas de cuantificación (Quantization Tables)*. Cotejo de tablas con la intención de encontrar consistencia entre el material cuestionado y muestras de comparación realizadas a la presunta cámara de origen o similares. Se realizará la inspección en busca de las firmas de compresión esperadas de los principales programas de edición catalogados por bases como la de FIAS, Amped Authenticate, JPEG Snoop u otra.

- *Inspección de coherencia de GOP en material de video*: En los casos de material cuestionado de video inspeccionar la coherencia del GOP (Group of Pictures) esperado de las propiedades del equipo de origen y la coherencia entre los artificios presentes en la imagen y los ciclos de cuadros I. Cabe destacar que la detección de cuadros de codificación bidireccional (Cuadros B) no son esperables en un material de un sistema de grabación "al vuelo" como los grabadores de seguridad.

7.10 Inspección del contenido de las imágenes:

7.10.1 Inspeccione el contenido de las imágenes (información visual) para determinar si hay o no presentes factores que puedan contestar la consulta de la persona solicitante. Los análisis a realizar pueden incluir la aplicación de métodos de inspección asistidos por algoritmos como: Análisis de tablas de cuantificación JPEG, histograma DCT (Discrete Cosine Transform), CLA (Compresion Level Analysis), CFA (Color Filter Array Analysis), mapa DCT (Discrete Cosine Transform), mapa CL (Compression Level), mapa CFA (Color Filter Array), mapa diferencial, análisis ELA (Error Level Analysis) en sus diferentes modalidades, mapa de correlación, mapa de probabilidad y bloques, ADJPEG (Aligned Double JPEG), NADJPEG (Nonaligned Double JPEG), análisis de ruido de sensor PRNU (Photo Response Non-Uniformity) o mapa de residuos PRNU entre otros.

7.11 Inspección de elementos confirmatorios de la hora y fecha de toma:

7.11.1 Considere que los valores de hora y fecha de toma registrados en los metadatos de los ficheros, por sí solos, no son concluyentes para determinar el momento de toma pues son susceptibles a imprecisión inadvertida o adulteración dolosa no detectables.

7.11.2 Al observar los datos asociados al material tome en cuenta que hay dos factores que podrían resultar en un dato cronológico desviado de la realidad: a) la hora y fecha que se registran dependen de la precisión en el ajuste del reloj interno del aparato al momento de toma y b) la modificación posterior mediante aplicaciones o rutinas especializadas para la modificación de los metadatos asociados a fecha y hora.

7.11.3 Realice una inspección visual de los eventos registrados en el contenido de las imágenes en busca de algún elemento o evento efímero registrado que resulte útil para confirmar la hora y fecha de toma indicada en las propiedades de los archivos.

8 Criterios de aceptación o rechazo de resultados:

No aplica.

9 Cálculos y evaluación de la incertidumbre:

No aplica.

10 Reporte de análisis y resultados:

10.1 Registro del proceso:

10.1.1 Sin importar los pasos de análisis utilizados es imperativo que cada uno sea documentado. Para ello el personal pericial escogerá entre a) la utilización de herramientas de bitácora en la aplicación elegida, b) mediante un consecutivo de carpetas en que se guarde cada nueva versión con un nombre descriptivo del ajuste aplicado o c) la combinación de ambas.

10.1.2 Si la herramienta cuenta con reportes de bitácora por software los archivos resultantes deben almacenarse en el legajo del caso en el SADCF y en el correspondiente caso dentro de QuickDME. Si permiten la emisión de archivos en PDF éstos deberán firmarse digitalmente.

10.2 Reporte de hallazgos e interpretación:

10.2.1 Por definición es imposible probar de manera contundente la ausencia de manipulación. A pesar de ello es posible determinar si es escasa la posibilidad que el material haya sido adulterado o confeccionado digitalmente mediante la aplicación de un análisis exhaustivo. Por otro lado, si se detectan alteraciones, el analista puede indicar en s interpretación que el material no es auténtico.

10.2.2 La asociación entre el material y la posible cámara de origen podría alcanzarse a partir de la combinación de los métodos mencionados. Sin embargo, la ausencia de suficiente información que apoye esta asociación no excluye la posibilidad de que haya sido obtenida con la cámara en análisis.

10.2.3 La confirmación de una hora y fecha de toma dependerá del registro de eventos efímeros que puedan ser catalogados como indicadores de confirmación o descarte de la veracidad de los indicadores en metadatos. De no hallarse, se debe reportar en el apartado de interpretación la ausencia de ellos y sugerir la incorporación de sustento testimonial.

10.2.4 La formación de una interpretación debe analizar la relevancia de cada característica observada.

10.2.5 El analista deberá formar una interpretación para responder a la pregunta formulada basándose en las características y la investigación realizada sobre el material. Las interpretaciones deben ser debidamente moderadas y mencionar las posibles limitaciones de la metodología y estado de la tecnología.

10.2.6 La interpretación debe ir acompañada del reporte de los hallazgos y no podrán ser sustentadas mediante una escala numérica de probabilidad.

10.2.7 El alcance de las interpretaciones será limitado por la calidad del material, la cantidad de material, la detección de particularidades inconsistentes y la disposición de material pertinente de referencia. Basado en estos factores es posible que el análisis solicitado no se pueda completar. El personal pericial debe ser cuidadoso de no sobredimensionar las conclusiones.

Nota 4: 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.

10.2.8 Utilice la funcionalidad Registro de Datos y Resultados del SADCF para registrar las interpretaciones de los resultados del análisis. El SADCF contempla un conjunto de textos prerredactados para los escenarios más comunes que se muestran a continuación:

- Fotografía o video consistente con original:

  Resultados: *"Tras la inspección del archivo se encontró que la estructura interna del contenedor, los metadatos y los métodos de compresión son consistentes con la muestra indubitada de comparación."*

  Interpretación: *"El material cuestionado es auténtico dado que muestra las propiedades esperadas del material que genera el presunto equipo de origen y no muestra rastros de herramientas de edición."*

- Fotografía o video no consistente con original:

  Resultados: *"Tras la inspección del archivo se encontró que la estructura interna del contenedor, los metadatos y los métodos de compresión no son consistentes con la muestra indubitada de comparación. Se encontraron marcadores y métodos de compresión asociados a herramientas de edición de imagen.*

  Interpretación: *"El material cuestionado ha sido procesado. No proviene directamente de la presunta cámara de origen."*

- Video de DVR consistente con original:

  Resultados: *"Se encontró que el archivo tiene la estructura esperada de un video codificado por el hardware de un sistema de vigilancia. Se encontró que están presentes a través del archivo los marcadores exclusivos de equipos de ese fabricante como los indicadores de formación del GOP propietarios.*

  Interpretación: *"El material no ha sido procesado. Está en formato nativo del fabricante. Proviene directamente de un sistema de vigilancia."*

- Video de DVR no consistente con original:

  Resultados: *"Se encontró que el archivo tiene una estructura distinta al material esperado de un video proveniente de un sistema de vigilancia. Se encontraron residuos asociados a un programa editor de video.*

  Interpretación: *"El material cuestionado ha sido procesado. No proviene directamente de un grabador de un sistema de vigilancia."*

- Cámara de origen, asociación confirmada:

  Resultados*: "Se realizó la inspección de la estructura interna del contenedor, los metadatos y los métodos de compresión de los archivos. Los resultados de los exámenes realizados a la muestra cuestionada y la muestra indubitada de comparación son similares.*

  Interpretación: *"La combinación de las similitudes encontradas sugieren que el material cuestionado fue tomado por el que se aportó como presunto equipo de origen."*

- Cámara de origen, asociación no confirmada:

  Resultados: *"Se realizó la inspección de la estructura interna del contenedor, los metadatos y los métodos de compresión de los archivos. Los resultados de los exámenes realizados a la muestra cuestionada y la muestra indubitada de comparación son distintos.*

  Interpretación: *"La combinación de las diferencias encontradas impiden establecer una asociación entre el material cuestionado y el que se aportó como presunto equipo de origen."*

- Momento de toma consistente con metadatos:

  Resultados: *"Los indicativos en los metadatos del material cuestionado sugieren como posible hora y fecha de toma HH:mm del DD/MM/YYY. Estos datos son consistentes con la información visual registrada.*

  Interpretación: *"La combinación de variables observada en los resultados sugiere que el evento registrado sucedió a la hora y fecha indicada en las propiedades del material cuestionado."*

- Momento de toma en metadatos no concluyente:

  Resultados: *"Los indicativos en los metadatos del material cuestionado sugieren como posible hora y fecha de toma HH:mm del DD/MM/YYY. No se encontraron indicativos en la información visual que ayuden a confirmar o descartar que el evento registrado sucedió a la hora y fecha indicada.*

  Interpretación: *"Los indicativos de hora y fecha en los metadatos, por sí solos, no son parámetros útiles para determinar de manera concluyente el momento de toma pues están sujetos al ajuste del reloj interno del aparato por parte del usuario.*

- Grabación de pantalla:

  Resultados: *"Se muestra la interfaz del sistema operativo de un equipo de vigilancia, y el borde de una pantalla. Hay movimiento observable de elementos que deberían estar fijos en pantalla. Se encontró que el archivo tiene una estructura distinta al material esperado de un video de un sistema de vigilancia y metadatos asociados a un dispositivo de imagen.*

  Interpretación: *El material cuestionado es una grabación de una pantalla realizada con la cámara de un dispositivo de mano. No proviene directamente de una sistema de vigilancia."*

11 Medidas de seguridad y salud ocupacional:

No aplica.

12 Simbología:

CSV: Comma Separated Values.

EXIF: Exchangeable Image File Format.

FIAS: Forensic Image Analysis System.

Gb: Gigabytes.

PDF: Portable Document Format.

SADCF: Sistema Automatizado del Departamento de Ciencias Forenses.

TXT: formato genérico de archivo de texto sin estilo.

13 Terminología:

Autenticación de imagen: la aplicación de las ciencias de la imagen y experticia para discernir si una imagen cuestionada es una representación fiel de los datos originales mediante algún criterio definido, y/o la determinación de la fuente original de una imagen.

Códec: Método y modelo matemático utilizado para codificar y descodificar el video dirigido a reducir espacio de tamaño en el disco y habilitar la posterior interpretación por parte del programa reproductor.

Compresión: Es el proceso de reducir el tamaño de un archivo para ahorrar espacio al almacenarlos.

Códigos MD5 y/o SHA1: secuencias alfanuméricas generadas 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.

Contenedor: Formato de archivo que almacena información de video, audio, metadatos e información de sincronización y corrección de errores siguiendo un patrón preestablecido en su especificación técnica.

Contenido de la imagen: Información visual en una imagen, es decir, los objetos, personas, escenario registrados y todos aquellos deterioros que se muestran visualmente (usualmente resultantes de las limitaciones del método de registro, compresión, almacenamiento y transmisión entre otros).

Estructura del archivo de imagen: Información no visual, asociada al fichero digital de las imágenes; por ejemplo el contenedor, formato, compresor y metadatos necesarios para su gestión y visualización en equipos informáticos.

Formato nativo: Metodología particular que cada modelo de grabador utilizará para almacenar, comprimir y guardar los datos de video una en su banco de información. A menudo portan información propietaria del fabricante.

GOP (Group of Pictures): método para reducir la cantidad de espacio requerido para el almacenamiento de video en que se establece una secuencia de cuadros intra-codificados de referencia (i-Frames) y entre ellos combinaciones de cuadros inter-codificados (cuadros B y cuadros P) que se calculan observando y excluyendo las redundancias encontradas al compararles con sus cuadros vecinos.

Lector hexadecimal: tipo de programa informático que permite al usuario leer o editar los datos binarios fundamentales que componen un archivo de computadora.

Manipulación: Proceso intencional de alterar la apariencia visual de una imagen o particularidades específicas dentro de ésta con el fin de cambiar el significado y su interpretación por parte del observador. Así también se refiere a la modificación de las propiedades de la estructura del archivo de imagen para simular un origen, fecha u hora distinto del verdadero.

QuickDME: Conjunto de aplicaciones forenses para la gestión de evidencia digital, por sus siglas en inglés “Digital Media Evidence”.

14 Anexos

No aplica.