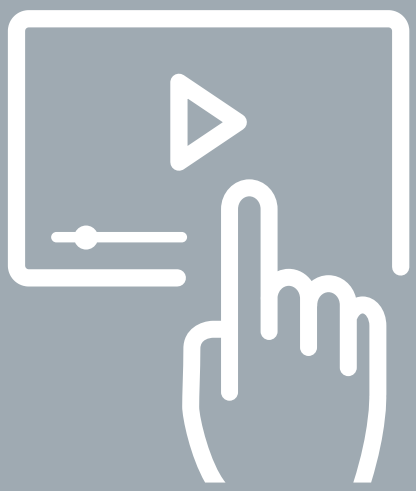
Guía

para la valoración judicial
de la prueba pericial
en materia de

ANÁLISIS DE VIDEO DIGITAL

DR. VICENTE **TORRES ZUÑIGA**



Para obtener la versión digital de esta guía escanea el QR.

ÍNDICE

PRELUDIO GENERAL

La presente guía es un instrumento de apoyo para realizar la valoración judicial de las distintas pruebas periciales, en especial de aquellas consideradas científicas y técnicas; está constituida por cuatro subguías en donde se describen los criterios generales que deben ser considerados para la valoración de la prueba, así como los errores que podrían presentarse en la prueba pericial y que pueden ser tomados en cuenta para su valoración; además de los criterios mínimos, es decir, los grados de tolerancia permisible asociados a cada etapa por la que transita la prueba y que se reflejan en fallas o circunstancias frecuentes.

La Subguía 1 ha sido pensada para señalar aquellos presupuestos mínimos, tanto para la prueba como para el indicio, desde el punto de vista de la ciencia forense; no establece criterios completamente jurídicos pero sí busca reflejar la indivisible relación entre el Derecho y la Ciencia. Por su parte, las Subguías 2, 3 y 4 contienen los elementos de obtención, análisis y presentación del indicio para cada área científica y técnica. Finalmente, se ha desarrollado un glosario compuesto por dos secciones: una parte general que contiene términos comunes a la ciencia forense y un segmento específico con conceptos propios de cada área forense.

Para facilitar su comprensión y evitar ambigüedades e interpretaciones que se alejen del objetivo del presente instrumento, se incluyen apéndices con conceptos, ideas, ejemplos y aclaraciones pertinentes que complementan los criterios descritos en las subguías.

Los criterios técnicos que se enuncian a lo largo de la presente guía se desarrollan de forma general para realizar una intervención en la especialidad de análisis de video digital. Lo anterior es pertinente, en particular para el caso de los métodos que forman parte de la Subguía 3 – Etapa de análisis, pues si bien declaran las etapas que integran dicho análisis, puede percibirse profuso para la acción de valoración de la prueba. Sin embargo, es crucial que el juzgador cuente con el bagaje técnico-científico necesario a fin de evitar sesgos e interpretaciones erróneas. Resulta pertinente aclarar que la terminología empleada en las presentes guías no se acota a una estricta acepción procesal. Tal es el caso de los términos “prueba” e “indicio”, que se utilizan en sentido amplio. De forma general, podemos asumir que, para fines del presente documento, el término “prueba” se considera como sinónimo de peritaje o actividad pericial; y para el término “indicio” se asume como todo objeto material sobre el que se versa la prueba.

Con respecto al término “método”, se advierte una definición amplia aplicable a las diversas especialidades, alcance de la presente guía, con ciertas consideraciones específicas que se precisarán en su momento. Se adopta, entonces, el concepto de Jonker y Pennink (2010) quienes lo definen como “la secuencia de acciones a seguir para conseguir un determinado fin, y que deben ejecutarse en un orden riguroso e invariable”. Con el objetivo de completar lo anterior, y a efecto de reducir la posible confusión con el término “técnica”, a continuación la definición que precisan los mismos autores y que corresponde a “materiales, herramientas o instrumentos específicos con los cuales se ejecuta un método”.

Independientemente de la función específica que realice, la actuación del personal pericial oficial que interviene en la investigación de los delitos debe observar en todo momento, además de los estándares técnicos que garanticen la integridad del trabajo forense, los derechos humanos de las personas involucradas. Para esto, se debe considerar el enfoque diferenciado para la niñez, la orientación sexual, las personas con discapacidad, las personas adultas mayores, las personas pertenecientes a comunidades indígenas, las personas migrantes, así como la perspectiva de género, tomando en cuenta las necesidades específicas que manifieste cada persona con la que deben interactuar en el ejercicio de sus funciones.

En coordinación y comunicación con la Fiscalía, deben articularse con las autoridades correspondientes en todas las etapas del procedimiento, observando los requisitos procesales que para su función establece el Código Nacional de Procedimientos Penales (CNPP) en lo que se refiere a los actos de investigación,[1] y desarrollando sus intervenciones bajo los principios de legalidad, objetividad, eficiencia, profesionalismo, honradez, lealtad y respeto a los derechos humanos reconocidos en la Constitución Política de los Estados Unidos Mexicanos (CPEUM) y en los instrumentos internacionales, en el propio Código y demás aplicables.

[1] Numerales 266 a 303.

NOTA METODOLÓGICA

La guía tiene como sustento dos vertientes principales: a nivel nacional se apoya en guías, manuales, acuerdos y protocolos que regulan el quehacer técnico-científico de las entidades de procuración y administración de justicia; en el ámbito internacional, se refuerza con artículos, manuales y guías publicados por grupos de personas expertas peritos en análisis de video digital, como el *Global guidelines for digital forensics laboratories* de la Organización Internacional de Policía Criminal o Policía Internacional (INTERPOL, por sus siglas en inglés), el *Best practice manual for forensic Image and video enhancement* del European Network of Forensic Science Institutes (ENFSI), el *Video evidence, a law enforcement guide to resources and best practices* del Bureau of Justice Assistance (BJA) del Departamento de Justicia de los Estados Unidos de América, entre otros textos especializados que se pueden encontrar en la sección de referencias (pág. 177).

Esta guía responde principalmente al cuestionamiento sobre si un video es falso. Así, las precauciones y análisis que realizará la persona experta se centran en los elementos que lo constituyen: sus imágenes, objeto de estudio en cuestión. Las examinaciones digitales forenses que aquí se plantean son útiles para encontrar algún signo de falsificación en el video. En caso de no encontrar alguna señal o indicación de engaño en el video, debe interpretarse como la falta de huellas de posible falsificación, es decir, no prueba que las imágenes sean reales, solo se demuestra que, por los recursos técnicos utilizados, no hay razón para considerar falso el video.

Este documento se limita al análisis de videos digitales, los cuales, debido al estado tecnológico actual, son los que más se requieren. La examinación de las imágenes de videos para lograr la identificación de personas u objetos, o bien, el análisis de videos analógicos, quedan fuera del alcance de esta guía.

En el apartado técnico-científico, la identificación de videos falsos se sustenta en métodos matemáticos que se apoyan en algún tipo de herramienta o interfaz. Por ello, se espera que la persona experta domine los conceptos, fundamentos y alcances de varias técnicas; desde el análisis de metadatos, el estudio de tablas de cuantificación, el estudio de artefactos, hasta la ejecución de algoritmos adversariales para reconocer videos ultrafalsos, como se ilustra en el Apéndice 5 (pág. 169 de esta guía). Así, debemos considerar que el avance tecnológico favorece la construcción de videos falsos cada vez más sofisticados, pero también el desarrollo de procedimientos novedosos para descubrir su engaño; por lo que se sugiere estar atento a sucesivas actualizaciones de esta guía.

CRITERIOS GENERALES DE PERTINENCIA PERICIAL DE LA PRUEBA

Subguía 1

		✓
1.1. Presupuestos mínimos para la realización de la prueba		
1	La solicitud del acto de investigación es pertinente jurídicamente.[a]	
2	La solicitud del acto de investigación puede ser ejecutada materialmente.[b]	
3	La solicitud de la autoridad ministerial detalla de manera clara las acciones requeridas para la intervención pericial.[c]	
4	El Registro de Cadena de Custodia (RCC) detalla de manera clara las acciones realizadas por la persona experta al momento de recabar, embalar y trasladar los indicios; asimismo, asegura la trazabilidad del indicio para un buen seguimiento.[d]	
5	La persona experta que realiza el análisis de video cuenta con la formación requerida para asegurar su calidad.[e]	
6	El indicio fue proporcionado por alguna de las personas participantes,[f] se obtuvo sin violación a las comunicaciones privadas al existir una resolución judicial que autorizó recabarlo que no constituya una afectación a los derechos humanos ni esté relacionada con materias legalmente excluidas.[g]	
1.2. Criterios mínimos de pertinencia pericial del indicio para ser procesado		
1	El medio de almacenamiento contiene un archivo de video con imágenes que pueden ser analizadas.	
2	Por su estructura, las imágenes conforman un conjunto al que se le puede llamar video.	

[a] La solicitud debe contar con todos los elementos contemplados en el art. 292 del Código Nacional de Procedimientos Penales (CNPP).

[b] Por ejemplo, si se entrega un medio de almacenamiento (como puede ser una unidad USB) para examinar un video, el archivo de video debe existir y ser apto para el análisis. De otro modo, la acción de análisis no se puede realizar.

[c] Para ello, el o los elementos de estudio se encuentran debidamente embalados, requisitados y/o preservados como lo marca el CNPP o las guías técnicas aplicables a la legislación vigente.

[d] Para mayor detalle revisar el Acuerdo A/009/2015 de la entonces Procuraduría General de la República (PGR), publicado en el *Diario Oficial de la Federación* el 12 de febrero de 2015.

[e] La identificación de videos falsos se basa en métodos matemáticos, al ser parte de un algoritmo, y este de un método de investigación. Por ello, se espera que la persona experta que analiza el video domine conceptos, fundamentos y alcances de las técnicas. Por ejemplo, el estudio de metadatos, el análisis ELA e incluso el uso de redes neuronales, como se sugiere en el Apéndice 5 (pág. 169).

[f] Si son aportados por la víctima, ofendido, testigo, o bien, por la persona sujeta a investigación, porque se trata de su videograbadora o *smartphone*, entonces debe de existir un consentimiento en la Carpeta de Investigación, según el art. 276 del CNPP.

[g] Arts. 16 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM); 252, 291, 292, 293 y 294 del CNPP; 189 al 190 Bis de la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR) y 8, 11 Bis 1, 16 al 28 de la Ley Federal Contra la Delincuencia Organizada (LFCDO).

CRITERIOS GENERALES DE PERTINENCIA PERICIAL DE LA PRUEBA

Apéndice 1

En el presente apéndice se describen los criterios generales para considerar la pertinencia científica de la prueba al no cumplir con aspectos técnicos indispensables para su aceptación, desde el punto de vista científico.

1.1. Presupuestos mínimos para la realización de la prueba

1.1.1. La redacción clara y detallada de la solicitud evita errores de interpretación. En ocasiones las solicitudes se redactan sin suficiente precisión respecto al análisis solicitado, lo que dificulta la correcta atención de la misma. Por ello, se recomienda que durante la valoración se confirme la pertinencia de la solicitud con respecto al indicio con el que se cuenta.

1.1.2. Se debe confirmar si la solicitud y el acto de investigación pueden ser ejecutados materialmente respecto del indicio con el que se cuenta. Es decir, se debe contar con un medio de almacenamiento y los datos a analizar. Por ejemplo, un teléfono celular (como medio de almacenamiento) cuenta con un video para analizar (datos).

1.1.3. El uso de términos generales sin un detalle claro sobre la acción concreta que se requiere realizar impide que la persona experta aplique el análisis, por lo que puede incumplir con lo que el solicitante espera obtener. Si la solicitud es imprecisa, está mal dirigida u omite el tipo de examinación a realizar, se obstaculiza que la persona experta pueda continuar con el análisis del indicio. En concreto, para esta guía nos referimos a que se debe solicitar la búsqueda de algún elemento indicativo de que el video es falso. O bien, se solicite una mejora en la calidad del video con fines de auxilio para otra prueba pericial, como la identificación de personas, vehículos u objetos.

1.1.4. La Cadena de Custodia es el sistema de control e inventario aplicado al indicio desde su localización, descubrimiento o aportación, en el lugar de intervención, hasta que la autoridad competente ordene su conclusión.[2] El Registro de Cadena de Custodia (RCC) es el documento en el que se inscriben los indicios o elementos materiales probatorios y las personas que intervienen.

1.1.5. La persona experta que efectúe el análisis de imágenes digitales debe contar con una capacitación específica, —comprobable en cualquier etapa del procedimiento penal—, para tratar con el indicio electrónico-digital, analizarlo y realizar el dictamen correspondiente. Además, debe acreditar que posee los conocimientos y habilidades para analizar imágenes digitales

[2] Artículo 227 del Código Nacional de Procedimientos Penales (CNPP).

en video o fotografía digital. Las personas aptas para trabajar estos indicios son licenciados o egresados de posgrados o diplomados en las áreas de físico-matemáticas e ingenierías o tecnologías de la información. Además, deben presenta certificaciones oficiales de programas de cómputo relacionados con el procesamiento digital de imágenes.

1.2. Criterios mínimos de pertinencia pericial del indicio para ser procesado

1.2.1. Los medios de almacenamiento deben contener imágenes que puedan ser extraídas para su análisis; entre los más comunes se encuentran los discos ópticos (por ejemplo, CD, DVD, Blu-ray, etc.), dispositivos de almacenamiento USB, unidades de estado sólido, tarjetas SD, entre otras tecnologías. Es posible que el medio de almacenamiento del video se encuentre en un estado tal que imposibilite su análisis; como puede ser por efecto del fuego o de una encriptación.

1.2.2. El concepto de "video" se describe en el documento "Definiciones, Recomendaciones y Directrices para el Uso de Procesamiento de Video Forense en el Sistema de Justicia Penal" del Grupo Científico de Trabajo Sobre Tecnologías de la Imagen (SWGIT, por sus siglas en inglés). Así, un video se define como la representación electrónica de un conjunto de imágenes que muestra escenas fijas o en movimiento, abarca diversas tecnologías de grabación, procesamiento, almacenamiento, transmisión de imágenes y reconstrucción por medios electrónicos digitales o analógicos de secuencias de imágenes. La tecnología actual permite incorporar audio al video, pero para los fines de esta guía no se considera la componente sonora.

ETAPA DE RECOLECCIÓN Y ALMACENAMIENTO (PROCESAMIENTO) DEL VIDEO DIGITAL

Subguía 2

		✓
2.1. Obtención de archivos		
1	Se identificó el archivo con el video a analizar a partir del medio de almacenamiento.[a]	
2.2. Recolección de archivos		
1	Se describió[b] el medio de almacenamiento,[c] fuente en la que se encontraba la muestra de video, como pueden ser: USB, teléfono móvil, computadora portátil, computadora de escritorio, disco óptico, sitio *web* en Internet, entre otros.	
2	Se describieron los medios técnicos para obtener el video.[d]	
3	Se describieron las características de la grabación en el archivo por analizar,[e] por ejemplo, los fotogramas por segundo (*frame rate*).	
4	Se registró quién entrego el archivo de video a la autoridad.[f]	
5	Se consideraron las condiciones específicas para asegurar la conservación, protección y la no alteración de la información contenida en el medio de almacenamiento, entre las que se encuentran el registro del nombre del archivo de interés y el HASH correspondiente (consúltese el glosario de esta guía, pág. 170).	
2.3. Traslado y cadena de custodia		
1	Se realizó el registro completo de todas las personas intervinientes durante el traslado del medio de almacenamiento que contiene el video, hasta la recepción del indicio en el laboratorio, o bien, en bodega temporal de indicios.[g]	
2	Durante el traslado del medio de almacenamiento del video se aplicaron las medidas de protección correspondientes al tipo de empaque-embalaje y su respectivo inventario,[h] con la finalidad de que no se altere su fidelidad, autenticidad y contenido.	
3	El traslado se realizó sin demora para asegurar la conservación física del medio de almacenamiento del video y así evitar su pérdida o alteración.	
2.4. Almacenamiento del video digital		
1	En la recepción del indicio electrónico se verificó la correspondencia de datos en el RCC,[i] en el caso de que el video digital se encuentre almacenado en un dispositivo electrónico.	
2	Durante el almacenamiento del indicio electrónico, en la bodega temporal o de indicios se aplicaron las medidas de protección correspondientes, en el caso de que el video digital se encuentre almacenado en un dispositivo electrónico.	
2.5. Errores que descartan el procesamiento del video digital		
1	El video digital se obtuvo sin considerar los criterios mínimos de calidad —como los señalados en la sección 1.2.1 y 1.2.2 de la Subguía 1 (pág. 152)— para realizar su estudio. De modo que no es posible su carga o reproducción en el sistema de análisis.	

		✓
2.6. Fallas y/o circunstancias tolerables en el procesamiento del video digital		
1	Grabaciones de video muy largas que hayan sido segmentadas para facilitar el procesamiento y análisis, sin alterar su contenido.	
2	Falta de concordancia entre los datos contenidos en alguno de los siguientes elementos: oficio de petición, el RCC y en el embalaje; respecto de los datos de carpeta de investigación: nombre de las víctimas, inculpados, testigos y otros, así como en el número y descripción de los indicios.[j]	
3	En el caso de que el video se encuentre almacenado en un dispositivo electrónico, se presente ruptura de la trazabilidad del indicio electrónico durante el procesamiento (recolección, documentación fotográfica y embalaje) y traslado.	
4	En el caso de que la muestra de video se encuentre almacenada en un dispositivo electrónico, existe un uso inadecuado del RCC al dejarlo incompleto, no registrar a todos los intervinientes o no acompañar en todo momento al indicio.	

[a] Como primera etapa antes del análisis, el medio de almacenamiento debe contener el archivo de interés.

[b] Toda esta información debe ser coherente con el Registro de la Cadena de Custodia (RCC).

[c] De acuerdo con lo señalado en el art. 291 del Código Nacional de Procedimientos Penales (CNPP) "la intervención de comunicaciones abarca todo sistema de comunicación, o programas que sean resultado de la evolución tecnológica, que permita el intercambio de datos, informaciones, audio, video, mensajes, así como archivos electrónicos que graben, conserven el contenido de las conversaciones o registren datos que identifiquen la comunicación, los cuales se pueden presentar en tiempo real [...] información, documentos, archivos de texto, audio, imagen o video contenidos en cualquier dispositivo, accesorio, aparato electrónico, equipo informático, aparato. También se requerirá autorización judicial en los casos de extracción de información, la cual consiste en la obtención de comunicaciones privadas, datos de identificación de las comunicaciones; así como la de almacenamiento y todo aquello que pueda contener información, incluyendo la almacenada en las plataformas o centros de datos remotos vinculados con éstos".

[d] Se debe aclarar si se extrajo directamente el video del medio de almacenamiento, realizando una copia fiel de la fuente, o bien, si se extrajeron por completo las imágenes del medio de almacenamiento. También puede ocurrir que se grabe el video original, lo que sucede cuando se usa un teléfono celular para grabar la pantalla de una computadora.

[e] Se debe mencionar si se trata de un video en tiempo real o un video por lapsos (*time lapse*); pues será determinante en las consideraciones del análisis y en el dictamen.

[f] De acuerdo con lo señalado por el art. 276 del CNPP, el archivo multimedia pudo haber sido entregado por un testigo o por alguno de los participantes en la escena (por ejemplo, la persona imputada) o bien, la autoridad accedió al medio de almacenamiento (como un *smartphone*). Es posible que el video se encontrara en un medio público (una red social digital), o bien, la autoridad solicitara a una empresa la entrega del material, en caso de que esta cuente con cámaras de seguridad de circuito cerrado.

[g] El registro de los intervinientes relacionados con un indicio se realiza mediante el formato de RCC.

[h] Art. 298 del CNPP.

[i] Algunos ejemplos de datos que deben corresponder en el RCC son: los actores que participaron desde el inicio del RCC hasta la entrega en bodega o laboratorio, la coincidencia entre la descripción en el RCC y la registrada en la etiqueta del embalaje, la trazabilidad de los elementos procesados en el RCC y en físico.

[j] La falta de concordancia de estos datos puede ser un error tolerable siempre y cuando no comprometa su identidad, trazabilidad de la evidencia, el reconocimiento de sus características originales o su eficacia para acreditar el hecho o circunstancia de que se trate. De lo contrario, la posibilidad de descartar ese indicio será valorada y determinada por el órgano jurisdiccional.

ETAPA DE RECOLECCIÓN Y ALMACENAMIENTO (PROCESAMIENTO) DEL VIDEO DIGITAL

Apéndice 2

2.1. Obtención de archivos

2.1.1. Se debe asegurar por medio del Registro de la Cadena de Custodia (RCC) que el video a estudiar provenga del correspondiente medio de almacenamiento. Por otro lado, es posible que, además del video a analizar, el medio de almacenamiento cuente con muchos más archivos digitales; por lo que se deben indicar las rutas de carpetas y el nombre específico del archivo de video a analizar. Se recomienda la revisión de las normas NMX-I-27037-NYCE-2015, que versa sobre "ingeniera del *software*, requisitos de calidad y evaluación de productos del *software* (SQuaRE), requisitos de calidad" y la norma NMX-I-289-NYCE-2016, que versa sobre "metodología de análisis forense de datos y guías de ejecución", ambas publicadas en el *Diario Oficial de la Federación,* con fechas del 8 enero del 2016 y 17 de junio del 2016, respectivamente.

2.2. Recolección

2.2.1. La presente se centra en el estudio de videos digitales, los cuales siempre requieren de un medio de almacenamiento que debe ser descrito, pues implica los alcances tecnológicos que debe considerar la prueba pericial. Por ejemplo, un medio obsoleto de almacenamiento puede dificultar la tarea de extraer el video.

2.2.2. Cuando el video analizado fue obtenido de un sitio web, se deberá seguir un protocolo para el procesamiento de evidencia digital. Por ejemplo, documentar una reconstrucción de eventos digitales, registrando datos como la URL de donde se obtuvo el archivo, su calidad y formato, así como la versión de la aplicación de descarga, o bien el *software* responsable de obtener los archivos, entre otros (Horsman, 2020, Partes 1 y 2).

2.2.3. Es importante describir las características del video, pues implican qué datos se grabaron. Tal vez solo se registró el movimiento de los objetos o se encuentra acelerada la sucesión de imágenes. Esta información es relevante, ya que afecta la etapa de análisis.

2.2.4. Debe ser clara la descripción de cómo se obtuvo el video. Es posible que el propietario lo entregara a la autoridad, o bien, el testigo que registró el hecho, uno de los participantes del video o el representante legal de alguna persona, institución o empresa.

2.2.5. Dependiendo de la tecnología utilizada se aplicarán diferentes medidas. En general, los dispositivos electrónicos deben contar con precintos que aseguren la clausura de entradas o salidas de datos: telecomunicaciones (por ejemplo, Internet por cable o WiFi, puertos de impresoras, USB, discos ópticos, entre otros). Además, deben embalarse en contenedores de aislamiento de señales electromagnéticas, denominados jaulas de Faraday.

La información digital es susceptible de ser modificada o eliminada tanto por medios locales como de forma remota (acciones directas o a distancia) que también incluyen la negación de servicios, por ejemplo, mediante la encriptación de discos duros. Por ello se requiere que los medios de almacenamiento, especialmente los encontrados en el lugar de interés, cuenten con precintos, que son medios físicos que impiden el intercambio de señales electromagnéticas entre dispositivos.

2.3. Traslado y cadena de custodia

2.3.1. Se debe documentar quiénes fueron las personas que tuvieron contacto con el medio de almacenamiento donde se encuentra el video digital, con el fin de registrar la trazabilidad de los cambios que pudo sufrir el video digital.

2.3.2. En general, las precauciones para la protección de medios de almacenamiento electrónico con embalaje o empacados son:

- uso de materiales metálicos que aíslen el dispositivo de cualquier comunicación electromagnética, tales como bolsas de papel aluminio, bolsas antiestáticas o jaulas de Faraday, ya que pueden provocar la pérdida o alteración de la información contenida en el dispositivo;
- uso de materiales como el hule espuma para reprimir efectos por vibración o impactos;
- evitar que los sobres de papel o plástico sean doblados o maltratados y
- no escribir directamente sobre el embalaje. Por ejemplo, un disco óptico es propenso a rayaduras que pueden dañar los datos grabados en este medio de almacenamiento.

2.3.3. A diferencia de las muestras biológicas, el video digital no es perecedero por naturaleza; sin embargo, es deseable que el tiempo de traslado sea corto, pues es una precaución de la integridad del video digital. De lo contrario, se puede generar suspicacia sobre una posible alteración del video correspondiente.

2.4. Almacenamiento

2.4.1. Cuando la persona experta acceda al archivo de video digital, deberá generar un identificador compuesto por caracteres (letras y números); esta cadena alfanumérica autentifica y ayuda a la trazabilidad. Aunque existen muchos protocolos, por lo general se utiliza un protocolo tipo SHA-256 para obtener lo que se le llama HASH.[3] La verificación de la correspondencia de datos puede incluir la correspondencia con el HASH.

2.4.2. Es indispensable en cualquier bodega de almacenamiento de indicios, ya sea temporal, de transición o por tiempo indefinido,[4] realizar la correcta clasificación para el acomodo y alma-

[3] Un HASH es el resultado de una función matemática. El HASH es un identificador único e irrepetible a partir de los datos del archivo estudiado. El HASH es una pieza clave en la cadena de custodia del video digital.

[4] Excepto en los casos que señala el art. 300 del Código Nacional de Procedimientos Penales (CNPP).

cenamiento de estos, a fin de evitar confusiones posteriores, principalmente entre los indicios procesados y no procesados.

Para indicios electrónicos, algunas medidas de protección que deben considerarse durante el almacenamiento en una bodega temporal o en una bodega de indicios son:

- conservar a temperatura ambiente;
- mantener en un espacio ventilado y
- evitar la humedad y la exposición directa al sol.

2.5. Errores que descartan el procesamiento

2.5.1. Es posible que el video digital provenga de la grabación de un monitor. Es el equivalente a realizar la captura de pantalla en imagen desplegada en la computadora, o bien, tomar una fotografía de otra foto. De modo que el análisis se aplica a este segundo registro y no sobre el original. El análisis no apoyará la autenticidad de las imágenes, pues se efectúa en un medio secundario que no es fiel a la fuente de los datos, es decir, la imagen o imágenes originales. También es posible que el video digital se malogre durante una etapa previa al análisis por la acción de una encriptación, daños en el medio de almacenamiento, entre otros.

2.6. Fallas y/o circunstancias tolerables en el procesamiento

2.6.1. Es posible que el registro del hecho sea parte de un video muy extenso. Mientras más grande sea el video más recursos puede exigir a la computadora. El análisis de archivos de video requiere de un alto desempeño de la tarjeta gráfica y memoria, además de capacidad de almacenamiento para guardar los resultados en el equipo. En tal caso, el video completo puede ser cargado en el sistema de análisis (*software*) y luego, para optimizar el estudio, concentrar el análisis en una sección específica. Mediante la documentación técnica y el Registro de Cadena de Custodia (por ejemplo, utilizando los "hashes") se puede asegurar que los datos analizados provienen del archivo fuente. Los archivos editados (por compresión, recorte u otra acción) tienen hashes diferentes a los del archivo fuente.

ETAPA DE ANÁLISIS

Subguía 3

		✓
3.1. Trabajo preliminar al análisis del video digital		
1	La persona experta accedió al video de interés contenido en el medio de almacenamiento.	
2	En el caso de los videos digitales grabados en dispositivos removibles para CD, DVD o memorias flash, la persona experta realizó una copia verificada por HASH del video de interés en otro dispositivo de almacenamiento.[a]	
3.2. Fuente del video digital		
1	La persona experta buscó digitalmente en Internet la posible fuente del video o antecedentes de su publicación.	
2	Se realizó un análisis de metadatos con el fin de identificar el autor, dispositivo de grabación o edición, fecha y lugar donde se generó el video.	
3.3. Análisis de información de la imagen digital[b]		
1	Se realizó un análisis de metadatos para asegurar su coherencia con las imágenes.	
2	Se analizó la estructura binaria del archivo.[c]	
3	Se analizaron tablas de cuantificación entre los fotogramas.	
4	Se realizó una búsqueda de artefactos por efectos de lentes.[d]	
5	Se realizó un análisis de niveles de error (*Error Level Analysis*, ELA) entre los fotogramas.	
6	Se hizo un análisis del estado de los píxeles en la estructura de las imágenes.	
7	Se realizó un análisis para identificar objetos clonados entre fotogramas.	
8	Se estudió la coherencia de luces y sombras en escena de la imagen.	
9	Se realizó un estudio para calcular la hora solar y geolocalización.	
10	Se realizó un análisis fotogramétrico de los objetos de referencia y las personas.	
11	Se realizó un estudio de la integridad de los fotogramas por convolución.	
12	Se revisó la integridad del video mediante un sistema tipo red neuronal.	

		✓
3.4. Errores que descartan el análisis del video digital		
1	Realizar análisis sin documentar su proceso, de modo que resulte imposible repetir las operaciones por otra persona experta.	
2	Falta de documentación sobre las tasas de incertidumbre y tasas de confiabilidad de las técnicas utilizadas en los análisis específicos.	
3.5. Fallas y/o circunstancias tolerables en el análisis del video digital		
1	Utilización de *software* sin certificación o que provenga de una empresa o compañía privada o institución pública.	
2	Se carece del tiempo preciso de grabación (que incluye a la hora solar) y ubicación exacta de la grabación del video.	

[a] Es posible que alguna de las partes solicite una certificación ante notario público de las copias de archivos o sus impresiones. Desde el punto de vista técnico, tales certificaciones son insuficientes para asegurar que la información de ambos archivos sea la misma. Por ello se necesitan las certificaciones matemáticas tipo HASH.

[b] Todas esta técnicas y métodos son esenciales para revelar si un video es falso. Así, de faltar alguna prueba, aumentará la posibilidad de que el video sea falso. Si bien recomendamos que se realicen todos estos exámenes, es posible que un video manipulado repruebe solamente uno y que sea suficiente y evidente para acreditar su naturaleza falsa. Aprobar todos los exámenes solo revela que no se acredita la falsedad en el archivo digital.

[c] Ya que esta guía se centra en el estudio de imágenes en video digital, es necesario considerar que la esencia de la imagen digital es una tabla de valores, de modo que se puede analizar su conformación para encontrar incoherencias en la estructura. Por ejemplo, en los estampados de hora de cámaras de seguridad, los añadidos de logos o marcas de agua.

[d] Pueden ser aberraciones, secciones del sensor óptico que dejaron de funcionar (llamados "píxeles muertos" o *hot spots*) u otros tipos de artefactos.

ETAPA DE ANÁLISIS

Apéndice 3

3.1. Trabajo preliminar al análisis

3.1.1. En caso de no obtenerse el video digital, no es posible realizar el análisis de video. Esta guía se centra en el estudio de esta clase de archivos.

3.1.2. Con el fin de preservar el estado original del indicio, se debe asegurar que los análisis a los videos digitales se realicen en una copia fiel (copia bit a bit) del archivo original. Existen programas de cómputo (por ejemplo, basados en sistemas ejecutables en MATLAB o ImageJ, o en lenguajes de programación como Python) que lo garantizan y que pueden emitir un certificado de identificación que lo asegura, conocido como HASH. Los archivos digitales son susceptibles a ser copiados de forma exacta y comprobable. Algoritmos tipo HASH permiten certificar la copia bit a bit entre archivos; de modo que, si se observa una alteración en el video analizado, también se encuentra tal alteración en el archivo original. Así, para la prueba pericial de análisis de video digital, los certificados HASH complementan al registro de cadena de custodia.

3.2. Fuente del video

3.2.1. La búsqueda se debe realizar en Internet, especialmente en redes sociales. Ya que el análisis versa sobre encontrar elementos que indiquen que el video es falso; es recomendable ejecutar esta exploración, incluso si se presupone la fuente del video. Por ejemplo, es posible que un particular entregara un video a la Fiscalía, pero estas imágenes ya se encontraban en Internet desde hace tiempo. La inconsistencia entre las imágenes de diferentes fuentes puede ser un indicador de que el video cuestionado sea falso; de otro modo, la exploración en Internet aporta información al estudio del caso. A través de herramientas digitales es posible identificar antecedentes de publicación de tales imágenes; entre las herramientas de búsqueda inversa de imágenes se encuentran TinEye, Google images, Shutterstock, TECXIPIO y sus equivalentes de video: Duplichecker, Berify, entre otras.

3.2.2. Los dispositivos generadores de imágenes digitales (por ejemplo, videocámaras, *scanners* o *smartphones*), además de producir los datos del video también pueden generar datos complementarios a las imágenes (metadatos). Los metadatos pueden perderse después de una edición del video o compresión. Así, algunos archivos de video contienen información sobre el fabricante, el autor, elementos fotométricos (distancia focal, exposición, etc.), imágenes miniatura, datos del dispositivo de generación, la fecha, la localización geográfica e incluso más datos relevantes; sin embargo, hay archivos de video que carecen de estos. Para completar la prueba pericial se necesita documentar el análisis de los metadatos del video.

3.3. Análisis de la información

3.3.1. Los metadatos contienen información relevante para determinar si un archivo de video digital es falso; sin embargo, en algunos casos, como en formatos comprimidos o editados, se pierde. Con todo, es importante revisar si existen metadatos que describan la hora y fecha en que se generó el video, el dispositivo de videograbación, la geolocalización y cualquier otra información relevante para el estudio forense.

3.3.2. La estructura primordial de los archivos digitales de video es binaria. Por ello se debe garantizar la realización de al menos un estudio de muestreos locales sobre la calidad de estos datos. Los resultados de este estudio son matemáticos, por lo que deben presentar su incertidumbre.

3.3.3. Las tablas de cuantificación son una técnica de análisis para archivos comprimidos tanto en imágenes como en videos digitales. Ejemplos y detalles de su uso se encuentran en (Kornblum, 2008). En esencia, las tablas de cuantificación son tablas numéricas de varios renglones y columnas, una imagen o video de referencia crea una tabla estándar, mientras que un archivo cuestionado forma una tabla de comparación. Al contrastar estos arreglos numéricos es posible identificar imágenes procesadas por *software*; además de ser un auxiliar para reconocer el tipo y modelo de cámara.

3.3.4. Todos los sistemas de videograbación que utilizan sistemas ópticos (conjuntos de lentes) presentan cierta distorsión en la imagen, a veces imperceptible al ojo humano, pero que se revela por medio de algoritmos. Existen más de 50 tipos diferentes de artefactos, entre los que podemos mencionar píxeles que siempre son blancos y píxeles que siempre son negros, efectos de aberración óptica, entre otros. Es posible que la mayor parte del video digital muestre ciertos grados en los artefactos, pero en algunos segmentos se encuentren otros niveles en los artefactos, lo que puede ser un indicativo de alteración. Además, esta exploración de artefactos es útil para caracterizar el medio de videograbación, lo que puede autentificar a un dispositivo con una serie de videos o imágenes.

3.3.5. Por las siglas en inglés de *Error Level Analysis,* ELA es una técnica popular para identificar imágenes falsas por inconsistencias de compresión entre objetos y los alrededores de la imagen. Esta técnica también se puede aplicar en fotogramas **o imágenes individuales**.

3.3.6. Se refiere a píxeles dañados (que siempre están en blanco o negro) que caracterizan a los sistemas de video. Es posible también que el video cuente con canales de píxeles ocultos, que los editores de imágenes suelen denominar “capas”, como sucede con las imágenes de formato tipo PNG.

3.3.7. Existen muchos algoritmos para realizar una búsqueda (automática y supervisada) de objetos clonados en imágenes y videos. Una lista esencial de algoritmos ejemplificados se puede consultar en los trabajos de Wang, W. (2009) y Kaur, H. & Jindal, N. (2020). En todo caso, se debe documentar cómo se procedió en este análisis.

3.3.8. Reflejos, sombras y variaciones de iluminación son producto de la posición y geometría de las superficies; su estudio permite encontrar incoherencias que revelen un video o imágenes falsas. Un ejemplo didáctico se puede consultar en el artículo "Exhibiendo adulteración fotográfica vía inconsistencia física de sombras" (Ramírez-Ornelas, Torres-Zúñiga, 2020). En tal comunicación se muestra que para algunos casos solo basta con trazar líneas rectas entre puntos estratégicos de los objetos y sus sombras producidas por una fuente de luz; la imagen será falsa si las líneas convergen en más de un punto.

3.3.9. Se debe tratar de calcular la hora solar y la geolocalización buscando coherencia entre los metadatos y lo observado en la imagen. Es posible que el dispositivo cuente con tales datos o no estén calibrados, también es posible que el video se haya grabado en ausencia de luz natural, situación que no invalida el video o las imágenes, pero se debe documentar.

3.3.10. Se deben documentar mediciones de objetos, personas y distancias entre puntos clave observados en el video. La falta de coherencia entre estas mediciones realizadas en campo puede ser clave para identificar un video falso; además de que es información útil para otras periciales: identificación de personas, reconstrucción de hechos mecánicos, por mencionar algunas.

3.3.11. La técnica de convolución es un algoritmo matemático que puede ser parte de un sistema forense de análisis de imágenes. Es una técnica auxiliar para identificar imágenes y videos falsos.

3.3.12. Se puede exponer mejor la manipulación de videos de tipo ultrafalsos (*deepfake*) por medio de sistemas de *deep learning*, por lo que se requiere un *software* tipo red neuronal para realizar la tarea. Los videos ultrafalsos son construcciones de redes neuronales adversariales y es esta misma perspectiva la que se aprovecha para encontrar la falsedad de tales videos.

3.4. Errores que descartan el análisis del video digital

3.4.1. Si se carece de la documentación que permita la revisión de cálculos, técnicas y procedimientos en los análisis, entonces resulta imposible verificar las acciones por otra persona experta, lo cual es un error en la documentación que invalida el estudio.

3.4.2. En esencia, todos los análisis de video son cuantificables, por lo que se pueden establecer tasas de incertidumbre en los estudios forenses. De modo que los análisis deben contar con la documentación sobre la confiabilidad de la técnica y del estudio realizado.

3.5. Fallas y/o circunstancias tolerables en el análisis del video digital

3.5.1. Es posible que se utilicen diferentes herramientas de distintos proveedores o desarrolladores para llevar a cabo los análisis. No es una exigencia utilizar una determinada marca o tecnología, pero sí es requisito documentar las acciones realizadas en el estudio con fines de verificación y repetición.

3.5.2. Si bien existen medios de investigación y es deseable determinar el tiempo en que se realizó la grabación (incluyendo la hora solar) y ubicación, en esta etapa no es un tema esencial contar con estos dos datos de tiempo y espacio. Es posible que se carezca del tiempo y localización debido a la naturaleza de la grabación; por ejemplo, en una habitación cerrada con iluminación artificial y por la ausencia de los metadatos correspondientes, pero esto no invalida el estudio del video.

ETAPA DE PRESENTACIÓN DE RESULTADOS

Subguía 4

		✓
4.1. Resultados		
1	Se reporta el origen fuente del archivo.	
2	Se reporta el medio de almacenamiento que recibió la persona experta.	
3	Se reporta que se tomaron las medidas de preservación del video original.	
4	Se reporta el identificador HASH del video digital analizado.	
5	Se reporta el formato o tipo de grabación del archivo de video.	
6	Se reportan los intervalos entre fotogramas (*frames*) analizados y se enfatiza sobre los fotogramas que presentaron indicios de manipulación.	
7	Se reportan los fotogramas y zonas de la imagen donde se realizó un proceso de amplificación (*zoom*).	
8	El reporte se complementa con capturas de pantalla indicando el tiempo de reproducción y al fotograma correspondiente al video.	
9	En caso de requerir impresiones de las imágenes del video de interés, se consideró la relación entre aspecto y tamaño.	
10	El reporte detalla las herramientas de análisis utilizados, los algoritmos empleados y los comandos ejecutados en cada etapa del proceso de estudio.	
11	Se indican los análisis realizados y, en su caso, que el video analizado reprobó.	
12	Se reportan las tasas de incertidumbre o confiabilidad de las técnicas realizadas.	
4.2. Errores que descartan los resultados		
1	Falta de documentación de las tasas de incertidumbre y tazas de confiabilidad de las técnicas utilizadas en los análisis específicos.	
2	Falta de figuras, imágenes o capturas de pantalla que resuman o ejemplifiquen que el video es falso.	
3	Si el HASH reportado no es trazable en el Registro de Cadena de Custodia (RCC) del video digital que se debía de estudiar.	
4.3. Fallas y/o circunstancias tolerables en los resultados		
1	Variaciones en el formato de presentación de los resultados en cuanto al orden y detalles del contenido.[(a)]	

[(a)] Diferentes expertos pueden variar en la presentación del orden y detalles del contenido. Aunque no existe un criterio universal de presentación del reporte de resultados, sí se espera que los procedimientos sean reportados de modo tal que otra persona experta pueda obtener los mismos resultados.

ETAPA DE PRESENTACIÓN DE RESULTADOS

Apéndice 4

4.1. Resultados

4.1.1. Independientemente de la vía por la que se obtuvo el video, se requiere explorar digitalmente cuál es el origen del video, para lo cual se puede examinar los metadatos, las redes sociales, las escenas del video o usar otro medio.

4.1.2. Es recomendable que en la sección de resultados se enfatice el tipo de medio de almacenamiento que recibió la persona experta.

4.1.3. Es recomendable mencionar, en los resultados, que se llevaron a cabo las medidas de preservación del video.

4.1.4. Se reporta en los resultados el HASH como modo de identificar el video analizado.

4.1.5. Se debe realizar el reporte del formato o tipo de archivo de video, con el fin de aclarar el detalle de tipo de archivo digital analizado.

4.1.6. Sin importar si se trata de un video extenso o corto, se deben reportar entre qué fotogramas se han realizado estudios y en cuáles se encontró una indicación de alteración. La alteración de un fotograma puede comprometer un video completo.

4.1.7. Es común que se realicen acercamientos dentro de fotogramas, por lo general requieren que se mejore la imagen, lo que implica un procesamiento digital; por ello, es doblemente importante su reporte. En caso de no realizarse, entonces se debe reportar la razón para no realizarlo u otra causa para su omisión.

4.1.8. El reporte puede presentar figuras clave donde se muestre un detalle que la persona experta desea resaltar.

4.1.9. Algunos sistemas de video alteran el aspecto, por ello se debe verificar si se sigue algún estándar de codificación de televisión digital como el ITU-601 u otro.[5] De otro modo, se deben corregir las imágenes para que la representación impresa sea más fiel a la realidad.

[5] ITU-601 es el primer estándar sobre televisión digital de la hoy llamada Unión Internacional de Telecomunicaciones, la recomendación se refiere al muestreo de señales de audio y video. La norma ha evolucionado, por lo que se debe conocer la relación de aspecto (por ejemplo, 3:3 o 16:9 u otro) hasta el submuestreo de componentes de color. Se puede encontrar más información en el documento de referencia de la Unión Internacional de Telecomunicaciones de 2020.

4.1.10. Con fines de transparencia, se debe detallar el proceso para que, si es requerido, otra persona experta verifique o refute los resultados.

4.1.11. Se enlistan los análisis realizados y aquellos en los cuales se muestra que el video fue manipulado.

4.1.12. Es esencial reportar las tasas de incertidumbre o confiabilidad de cada técnica realizada.

4.2. Errores que descartan los resultados

4.2.1. De acuerdo con estándares internacionales sobre la valoración de la prueba científica (por ejemplo, el estándar Daubert), se debe reportar cuantitativamente el grado de confiabilidad del análisis que muestra la falsedad de un video digital.

4.2.2. El reporte debe contener los resultados visuales, en particular si se dictamina que el video es falso.

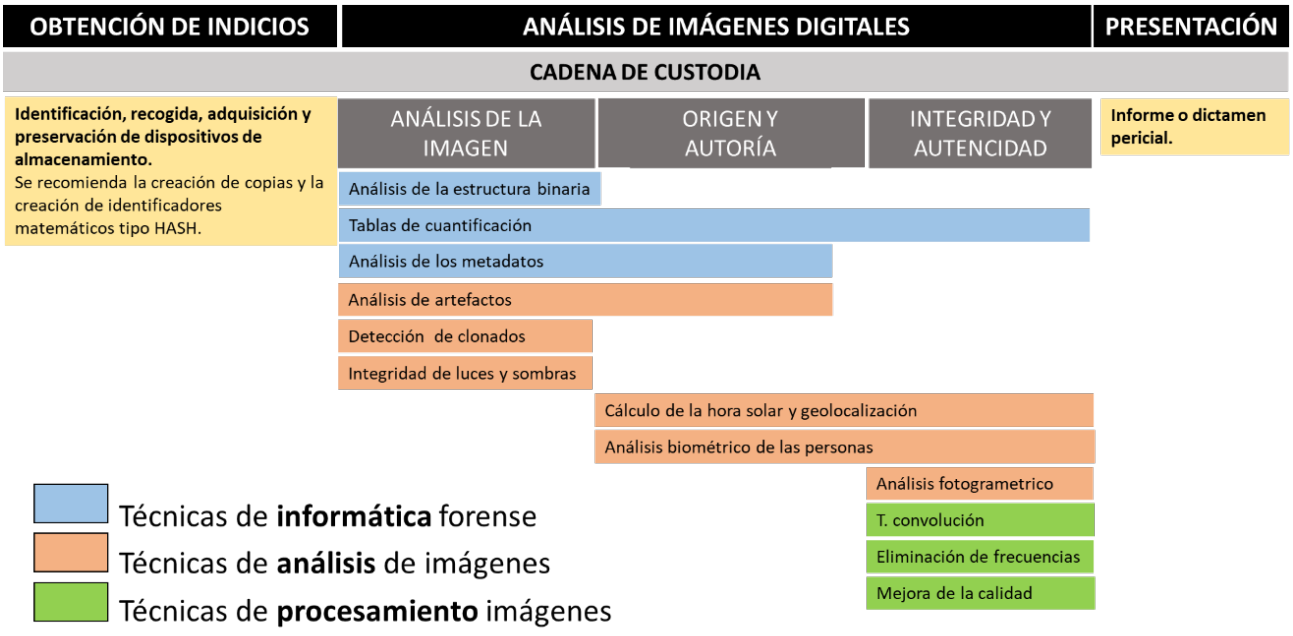
4.2.3. El HASH representa la identificación digital del archivo digital, siempre debe estar presente en la documentación sobre el video a estudiar, en particular en el reporte de sus análisis. Si el HASH en el reporte es diferente al de la fuente original, se debe documentar la razón de este cambio y debe ser trazable en el Registro de Cadena de Custodia (RCC).

4.3. Fallas y/o circunstancias tolerables en los resultados

4.3.1. Existen diversas formas de reportar los resultados de un estudio de video digital, las cuales deben ser toleradas. Es de esperar que varíe el orden al presentar datos, análisis y resultados; además de que algunos dictámenes mostrarán más imágenes o tablas comparativas que otros. En todo caso, deben ser claros los procedimientos para que otra persona experta repita cada etapa y alcance los mismos resultados.

ESQUEMA DEL FLUJO DE TRABAJO DEL ANÁLISIS FORENSE DE IMÁGENES PARA IDENTIFICAR SI UN VIDEO DIGITAL ES FALSO

Apéndice 5



Adaptado de Alejandro Maestre
https://imagencientifica.es/servicios/analisis-forense-de-imagen.html

El análisis de las imágenes con fines forenses tiene como uno de sus objetivos identificar si un video digital es falso. El análisis de imágenes se apoya en varias técnicas informáticas, analíticas y de procesamiento que pueden ser útiles para establecer la integridad y autenticidad de la información. El esquema muestra que en todo momento se debe mantener la cadena de custodia.

GLOSARIO

Glosario básico

Aberración óptica: todos los sistemas de lentes producen un grado de desviación defectuosa que se plasma en la fotografía como una pérdida de nitidez o alteración. Las aberraciones más comunes son: esférica, coma, astigmatismo, curvatura de campo (de barril o cojín), distorsión y cromática. Su presencia puede ser útil con fines de autenticación de la imagen o identificación de la cámara.

Almacenamiento: acto de preservar una imagen.

Algoritmo adversarial: consiste en dos redes neuronales, una generadora y otra discriminatoria. La primera produce una salida que es evaluada por la segunda; esta información retroalimenta a la red generadora, por lo que cambia su siguiente salida para obtener una mejorar evaluación de la red discriminatoria. La dinámica entre estas dos redes le permite al sistema de cómputo producir resultados de alta calidad.

Análisis ELA: tipo de estudio que calcula el nivel de compresión entre píxeles vecinos. Los objetos sobrepuestos en una fotografía digital suelen contar con un nivel de compresión diferente al resto del archivo. Para resaltar esta diferencia, se produce una imagen de salida donde el objeto sobrepuesto presenta bordes resaltados en el color o tono.

Análisis fotogramétrico: estudio para conocer datos precisos de la forma, dimensiones y posición espacial de un objeto utilizando mediciones realizadas en una o varias imágenes del mismo.

Análisis de imágenes digitales: es la extracción de información (cualitativa o cuantitativa) derivada de los sensores electrópticos representada en dos o tres dimensiones. Abarca las imágenes en escala de grises y a color. En lo que concierne a esta guía, puede englobar desde el ultravioleta hasta el infrarrojo cercano del espectro electromagnético.

Archivar: almacenamiento de datos digitales por un periodo prolongado.

Artefactos: es una distorsión, adición o error que altera la calidad y fidelidad de la imagen, de modo que no tiene correlato con el objeto real.

Codec: algoritmo codificador y decodificador (compresor y descompresor) para imágenes digitales y datos en video utilizado para reducir la cantidad de datos de transmisión o almacenamiento. Si bien no es un formato de almacenamiento, es indispensable para interpretar los datos almacenados en un video.

Compresión: un proceso para reducir el tamaño de un archivo de datos preservando el significado semántico original.

Conversión: cambiar la representación (codificación o formato de archivo o ambos) de imágenes digitales o datos de video. Si la codificación de las imágenes se modifica mediante la conversión, puede producirse una pérdida de calidad de la imagen. La conversión también puede influir en la cantidad o tipo de metadatos codificados. El resultado de un paso de conversión se denomina "imagen convertida" o "video convertido".

Copia bit a bit: una copia 1:1 (idéntica bit a bit) de una imagen digital o archivo de video. Si una etapa de verificación ha confirmado que la copia de los datos es idéntica, se denomina "copia verificada".

Copia de trabajo: copia (verificada) de una imagen de la primera copia o un video de la primera copia que puede estar sujeto a procesamiento.

Copia verificada: una copia 1:1 (idéntica en cada bit) de un archivo de imagen o video que ha pasado con éxito una etapa de verificación para demostrar que el original y la copia de los datos son idénticos.

Copiar: acción de reproducir información con cierto nivel de precisión. Dependiendo del proceso, pueden perderse datos o no.

Compresión con pérdida: el proceso de cambiar el método de codificación para reducir el tamaño de los datos a través de una pérdida de información, es decir, la información no se puede recuperar en su forma original.

Compresión sin pérdida: el proceso de cambiar el método de codificación para reducir el tamaño de los datos sin pérdida de información, es decir, la información original aún se puede recuperar en su forma original.

Datos: información en forma analógica o digital que se puede transmitir o procesar.

***Deep learning*:** el aprendizaje profundo es un conjunto de algoritmos de aprendizaje automático que intenta modelar abstracciones de alto nivel utilizando funciones matemáticas e iteración de datos.

Dictamen pericial: es la emisión de la opinión en un problema concreto que ha sido planteado por parte de una persona experta, llegando a puntos específicos con base en las investigaciones efectuadas, procedimientos y fundamentos técnico-científicos.

Disco óptico: medio de almacenamiento de datos. Consiste en un disco circular donde por medios ópticos (por lo general un láser) se registra y se lee información que se ha grabado como surcos microscópicos sobre una de las caras del medio. Entre las tecnologías de discos ópticos se encuentran las denominadas: CD, DVD, Blu ray, UMD (*Universal Media Disc*) entre otras.

Formato de archivo: estructura con la cual se organiza un archivo de datos para ser observado en un dispositivo.

Formato nativo: el formato de codificación y archivo de la primera versión almacenada permanentemente de una imagen o video.

Fotografía: la mezcla de técnica y ciencia para registrar imágenes en una superficie sensible a la luz.

Fotogramas: también llamado *frame*, es cada una de las imágenes que conforman un video. Se expresan en hercios (Hz) o *frames per second* (fps).

Fotogrametría: es una técnica que utiliza varias fotografías o videos para obtener medidas fiables de objetos físicos y su entorno. Esta técnica de medición de coordenadas tridimensionales utiliza imágenes con el fin de conseguir las dimensiones, forma y posición espacial de los objetos.

***Frame rate*:** traducido como "fotogramas por segundo", "tasa de fotogramas" o "cuadros por segundo", es la frecuencia a la cual un dispositivo despliega imágenes. Sus siglas pueden ser "fps" o f/s. El término se aplica tanto para películas, videos, gráficos por computadora u otros sistemas similares.

Imagen: en este documento se utiliza como abreviatura de imagen digital.

Imagen digital: datos digitales que representan una matriz de valores de brillo o color y en ocasiones metadatos.

Imagen de primera copia: la primera copia (verificada) generada por el laboratorio del material de imagen digital enviado.

Imagen procesada: una imagen resultado de un proceso. Es la salida de realizar una serie de operaciones. Ver "procesamiento de imágenes".

Interfaz: se trata de la conexión física y funcional establecida entre dos aparatos, dispositivos o sistemas que funcionan independientemente uno del otro. En este sentido, la comunicación entre un ser humano y una computadora se realiza por medio de una interfaz.

HASH: función que recibe de entrada una cadena de datos (archivo) de tipo y tamaño variable y su salida es una cadena alfanumérica de longitud fija. De modo que es una representación compacta de la cadena de entrada. Existen algoritmos como sha256, cuyo funcionamiento es adecuado en el área forense; pues son sensibles a cambios de un solo bit o carácter dentro del archivo. De tal modo que, dados dos hashes diferentes, implica que los archivos fuente son diferentes.

Medios de almacenamiento: cualquier elemento físico que permite almacenar datos digitales.

Mejora de la imagen: cualquier proceso destinado a optimizar la apariencia de un detalle específico dentro de una imagen o video digital con respecto a un propósito y uso previstos.

Metadatos: son datos que describen información sobre otros más. Los archivos digitales cuentan con una serie de datos que describen características adicionales del archivo, una parte de estos datos se genera automáticamente por los dispositivos o programas de edición. Así, en los archivos multimedia, como los de foto y video, los datos pueden ser características de la exposición de la imagen, datos personales, del fabricante o modelo de cámara, entre otros.

Nube: es como se denomina coloquialmente a la tecnología que permite el acceso remoto (desde cualquier ubicación y momento) a programas de almacenamiento de archivo y procesamiento de datos a través de Internet, sin la necesidad de conectarse a una computadora personal o un servidor local.

Objetos clonados: en procesamiento digital de imágenes, un clon es un conjunto de elementos replicados y sobrepuestos sobre otra zona.

Operación de imagen: función de procesamiento de imagen.

Píxel: (acrónimo del inglés *picture element*) es la menor unidad homogénea en color que forma parte de una imagen digital.

Precinto: se trata de una ligadura o señal con la que se cierran los accesos a instrumentos o sitios con el fin de mantenerlos aislados de interferencia, excepto cuando son consultados por un responsable legal.

Primera copia de video: la primera copia generada (verificada) en el laboratorio del material de video digital enviado.

Procesamiento de imágenes: cualquier actividad que utilice imágenes digitales o datos de video (entrada, fuente) para calcular una nueva imagen digital o datos de video (salida, resultado).

Procesamiento dentro del cuadro: cuadros de salida o resultados calculados a partir de datos extraídos del cuadro de entrada correspondiente original.

Procesamiento entre cuadros: cuadros de salida o resultados calculados a partir de datos extraídos de varios cuadros de entrada.

Redes neuronales: sistema computacional que consiste en módulos (llamados de "entrada", "oculto" y de "salida") que se trasmiten información. Los datos de entrada atraviesan la red neuronal mediante operaciones matemáticas ejecutadas en cada módulo, produciendo al final valores de salida. En lugar de ser programados de modo explícito, estos sistemas se adaptan, por lo que en una etapa inicial (el entrenamiento) son alimentados con datos predefinidos y se evalúa su salida. El entrenamiento termina cuando las salidas son aceptables respecto a los datos de entrada.

Registro de procesamiento de imágenes: un registro de etapas realizadas en el procesamiento de imágenes.

Relación de aspecto: la relación entre el ancho y la altura de un rectángulo, como una imagen de 39 píxeles o un fotograma de video activo.

Región de interés: parte de una imagen que se selecciona o elige para un examen o procesamiento adicional, en inglés *region of interest* (ROI).

Redes sociales: estructuras formadas en Internet por organizaciones o personas al conectarse a partir de intereses comunes. A través de ellas se puede compartir información en texto, imagen y audio.

Secuencia de bits duplicada: en informática forense, una reproducción exacta bit a bit de los datos que es independiente del medio físico de almacenamiento de datos.

Tasa de un coeficiente: valor que expresa la relación entre la cantidad y la frecuencia de un fenómeno. Se utiliza para indicar la presencia de un fenómeno medido indirectamente. La incertidumbre es un parámetro asociado al resultado de una medida, que caracteriza la dispersión de los valores que podrían razonablemente ser atribuidos al mensurando. En este documento nos referimos a la tasa de incertidumbre como una cuantificación de la relación de la medida y su precisión; en caso de contar con un valor estándar esta medida se puede relacionar con la exactitud. Por tanto, la tasa de incertidumbre se puede expresar como el porcentaje del error asociado dividido por la medición.

Video: en este documento se utiliza como abreviatura de video digital.

Videoanálisis: examen técnico que implica la comparación o evaluación de video.

Videos analógicos: señales de video registradas, trasmitidas y almacenadas como un voltaje de variación continua, en lugar de como una estructura de bits como en el video digital. Por lo anterior, su análisis es diferente al de los videos digitales, requiriendo otras herramientas y con alcances diferentes.

Video digital: datos digitales que representan una secuencia de imágenes digitales grabadas del mismo tamaño de píxel y metadatos; puede incluir datos de audio.

Videos ultrafalsos: son videos digitales manipulados, extremadamente realistas, que se construyeron mediante técnicas de inteligencia artificial. También son conocidos como *deepfake*.

Glosario general

Almacenamiento de indicios: colocar los objetos recolectados en áreas que cumplan con ciertas especificaciones de acuerdo con su tipo.

Base de datos: colección o conjunto de datos organizados bajo criterios que permiten la búsqueda de información.

Bodega de indicios: lugar con características específicas que tiene como finalidad el resguardo de indicios para garantizar su integridad.

Consentimiento informado: acto por el cual se otorga autorización para efectuar un procedimiento de orden jurídico, médico o científico que implique la invasión de la persona en su cuerpo, integridad o en su información personal. Este acto debe contemplar una fase explicativa de los procedimientos a llevar a cabo, las opciones con las que se cuenta paralelas a la opción propuesta, los efectos secundarios, entre otros; y una fase de concordancia que se expresa por medio de la firma del documento de consentimiento informado de las personas autorizadas para ello por la ley. Debe contener, al menos, los siguientes datos: 1. Nombre de la institución; 2. Nombre o razón social del establecimiento; 3. Título del documento; 4. Lugar y fecha; 5. Acto autorizado; 6. Señalamiento de los riesgos y beneficios; 7. Autorización al personal; 8. Nombre y firma de la persona que otorga la autorización; 9. Nombre completo y firma de quien realiza el acto autorizado.

Conservación: se refiere al estado en que permanecen los indicios y evidencias a fin de evitar su pérdida o degradación natural.

Cotejar: observación de dos o más elementos para determinar la existencia de discrepancias o similitudes.

Documentación fotográfica: es la impresión o captura de una imagen sobre un medio sensible a la luz (análoga o digital), para registrar y preservar las características de la misma, con el fin de reproducirla cuando se requiera. Existen diferentes tomas:

- Plano general. Toma que abarca una visión general del indicio dentro del lugar de la investigación.
- Plano medio. Toma que relaciona al indicio con el plano general.
- Plano de acercamiento. Toma que resalta alguna característica del indicio con referencia de un testigo métrico.
- Gran acercamiento. Toma que abarca el detalle del indicio.

Embalaje: conjunto de materiales que envuelven, soportan y protegen al indicio o elemento material probatorio con la finalidad de identificarlo, garantizar su mismidad y reconocer el acceso no autorizado durante su traslado y almacenamiento. Cuando los indicios sean embalados en bolsas de plástico o de papel, estas deben ser del tamaño adecuado para las dimensiones del indicio.

Intervención: etapa en el proceso penal en donde el personal ministerial, pericial y policial investiga en el lugar de los hechos, hallazgo o enlace. Dicho personal puede realizar acciones encaminadas a la toma de muestras (huellas dactilares, sangre, saliva, muestras de voz) a víctimas, testigos o presuntos responsables.

Mismidad: relacionado a la autenticidad. Describe una propiedad con la que debe cumplir el indicio. Se refiere a la forma de acreditar la identidad verdadera de algo. La manera de garantizar la autenticidad del indicio es a través del procedimiento de cadena de custodia.

Procesamiento: conjunto de acciones para buscar, documentar, identificar, revelar, recolectar, embalar, trasladar y registrar en el Registro de Cadena de Custodia (RCC) los indicios hallados en el lugar de investigación.

Recolección: proceso realizado por una persona capacitada en el manejo del indicio, en el que el elemento o fragmento a analizar es localizado y después trasladado de una forma apropiada para poder realizar una comparación y/o análisis.

Registro de Cadena de Custodia (RCC): se refiere al procedimiento de control que se aplica al indicio desde la localización por parte de una autoridad, policía o agente de Ministerio Público, hasta que la autoridad competente ordene su conclusión. Su objetivo general es garantizar la mismidad y autenticidad de los indicios mediante actividades de control y elaboración de registros que demuestren la continuidad y trazabilidad de la cadena de custodia, con el fin de incorporarlos como medio de prueba en el proceso penal.

Señalización-identificación: asignación individual de un indicativo numérico o alfabético, o su combinación, único y consecutivo para cada indicio. Dicha asignación le corresponderá durante todo el procedimiento penal con el fin de asegurar su mismidad y trazabilidad durante las diferentes etapas del proceso.

Solicitud de prueba: actos de investigación que se consideren pertinentes y útiles para el esclarecimiento de los hechos, de acuerdo con los artículos 129, 131, 149, 217, 251 y 252 del Código Nacional de Procedimientos Penales (CNPP).

Testigo métrico: material de apoyo que contiene una escala métrica. Se debe incluir durante la documentación fotográfica para tener referencia de las dimensiones del indicio.

Traslado: envío del indicio a la bodega de indicios y/o al laboratorio para análisis. Se deben establecer las condiciones para el manejo del indicio, destino, condiciones ambientales y el tipo de transporte que se debe emplear.

Trazabilidad: principio con el que se garantiza el seguimiento del o los estudios realizados al indicio.

REFERENCIAS

Al-Athamneh, M. K. (2016). Video Authentication Based on Statistical Local Information. *Proceedings - 9th IEEE/ACM International Conference on Utility and Cloud Computing, UCC 2016*, 388-391.

Christian, A., & Sheth, R. (2016). Digital Video Forgery Detection and Authentication Technique - A Review. *IJSRST, 2*(5), 138-143.

ENFSI. (2018). *Best Practice Manual for Forensic Image and Video Enhancement*. European Network of Forensic Science Institutes.

Horsman, G. (2020). Part 1:-quality assurance mechanisms for digital forensic investigations: Introducing the Verification of Digital Evidence (VODE) framework. *Forensic Science International*, 100038.

Horsman, G. (2020). Part 2:-Quality assurance mechanisms for digital forensic investigations: knowledge sharing and the Capsule of Digital Evidence (CODE). *Forensic Science International*, 100035.

INTERPOL. (2019). *Global guidelines for digital forensics laboratories*. INTERPOL.

Jonker, J., & Pennink, B. (2010). *The Essence of Research Methodology: A Concise Guide for Master and PhD Students in Management Science*. Springer.

Kacprzyk, J. (2020). *Digital image forensics, Theory and Implementation*. Springer.

Kaur, H., & Jindal, N. (2020). Image and Video Forensics: A Critical Survey. *Wireless Pers Commun, 112*, 1281-1302.

Kävrestad, J. (2020). *Fundamentals of Digital Forensics*. Springer.

Kornblum, J. D. (2008). Using JPEG quantization tables to identify imagery processed by software. *Digital Investigation*, S21-S25.

Maras, M. H., & Alexandrou, A. (2019). Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos. *The International Journal of Evidence & Proof, 23*(3), 255-262.

María Elena Darahuge, L. E. (2014). *Manual de Informática forense II*. Errepar.

Mezaris, V. N. (2019). *Video verification in the fake news era*. Springer.

NFSTC. (09 de 2013). *A Simplified Guide to Crime Scene Investigation*. Recuperado el 4 de 09 de 2020, de National Forensic Science Technology Center. http://www.forensicsciencesimplified.org/av/

Norma mexicana NMX-I-25030-NYCE-2015: Tecnologías de la información-ingeniera del software-requisitos de calidad y evaluación de productos del software (SQuaRE)-requisitos de calidad. (8 de enero de 2016). *Diario Oficial de la Federación*.

Norma mexicana NMX-I-289-NYCE-2016: Tecnologías de la información - Metodología de análisis forense de datos y guías de ejecución (Cancela a la NMX-I-289-NYCE-2013). (17 de junio de 2016). *Diario Oficial de la Federación*.

OSAC, V. T. (2020). *Standard Practice for Data Retrieval from Digital CCTV Systems.* NIST.

OSAC, V. T. (2020). *Training Guidelines for Video Analysis, Image Analysis and Photography*. NIST.

Pandey, R. S. (2016). Passive forensics in image and video using noise features: A review. *Digital Investigation*(19), 1-28.

Ramírez-Ornelas & Torres-Zúñiga. (2020). Exhibiendo adulteración fotográfica vía inconsistencia física de sombras. *Revista del Instituto Federal de Defensoría Pública*, *29,* 111-122.

Sadeghi, S. D. (2018). State of the art in passive digital image forgery detection: copy-move image forgery. *Pattern Analysis and Applications, 21*(2), 291-306.

Scientific Working Group on Digital Evidence. (2018). *SWGDE Best Practices for Digital Forensic Video Analysis*. SWGDE.

Seckiner, D. M. (2018). Forensic image analysis – CCTV distortion and artefacts. *Forensic Science International*(285), 77-85.

Shahraki, A. S., H., S., Amril, M. H., & Nikmaram, M. (2013). Survey: video forensic tools. *Journal of Theoretical and Applied Information Technology, 47*(1), 98-107.

Singh, R. A. (2018). Video content authentication techniques: a comprehensive survey. *Multimedia Systems, 24*(2), 211-240.

Sitara, K. M. (2016). Digital video tampering detection: An overview of passive techniques. *Digital Investigation*(18), 8-22.

Sitara, K. M. (2018). Detection of inter-frame forgeries in digital videos. *Forensic Science International*(289), 186-206.

The Forensic Science Regulator. (2014). *Appendix: Digital Forensics - Video Analysis.* The Forensic Science Regulator.

The Forensic Science Regulator. (2016). *Forensic Image Comparison and Interpretation Evidence: Guidance for Prosecutors and Investigators.* The Forensic Science Regulator.

Unión Internacional de Telecomunicaciones. (20 de 09 de 2020). *BT.601: Parámetros de codificación de televisión digital para estudios con formatos de imagen normal 4:3 y de pantalla ancha 16:9*. https://www.itu.int/rec/R-REC-BT.601/es [acceso: 20/septiembre/2020]: https://www.itu.int/rec/R-REC-BT.601/es

Verolme, E. M. (2017). Application of forensic image analysis in accident investigations. *Forensic Science International*(278), 137-147.

Video Evidence, A Law Enforcement Guide to Resources and Best Practices. (2014). Bureau of Justice Assistance U.S. Department of Justice.

WALES, G. S. (2019). *Proposed framework for digital video authentication*. University of Colorado.

Wang, W. (2009). *Digital Video Forensics*. Hanover, New Hampshire. Tesis doctoral en Ciencias de la Computación, Dartmouth College.

Zhang, Y. D. (2019). Face Spoofing Video Detection Using Spatio-Temporal Statistical Binary Pattern. *IEEE Region 10 Annual International Conference, Proceedings/TENCON*, 209-314.