IMELCF

INSTITUTO DE MEDICINA LEGAL Y CIENCIAS FORENSES

Licdo. Fernando A. Sánchez R.
Perito de Informática Forense
fernando.sanchez.rios@imelcf.gob.pa

2023

¿Informática Forense?

Disciplina encargada del estudio de métodos, procesos, técnicas y desarrollo, tanto a nivel de hardware como software, del trato que se da a la información digital.

Perteneciente o relativo al foro.

Lugar en el cual los tribunales escuchan y definen causas.

Definición de evidencia digital

- Según el sitio web https://www.sanchezgarridoabogados.com/ “La evidencia digital es cualquier información de valor probatorio que se almacena o transmite en forma digital (datos en binario a bajo nivel).”

- Según el Manual de Procedimiento del Sistema de Cadena de Custodia del IMELCF, “EVIDENCIA DIGITAL: Se refiere a todos los datos, información, programas almacenados y mensajes transmitidos utilizando un sistema informático.”


Canal St
S Halsted St
GARMIN
MAGELLAN
GARMIN


NOKIA
ZonaTop5.com


32GB


HYPER
HYPER
SAMSUNG


SIM
Micro SD
OPEN YOUR EYES


htc
nexus


LTE 4G
4G LTE


NOKIA
desmotivaciones.es
Vendo Celular
Incluye cámara de vídeo, reproductor MP3, Bluetooth y Memoria

Gmail

Yahoo!

Outlook

Peritaje - Perito

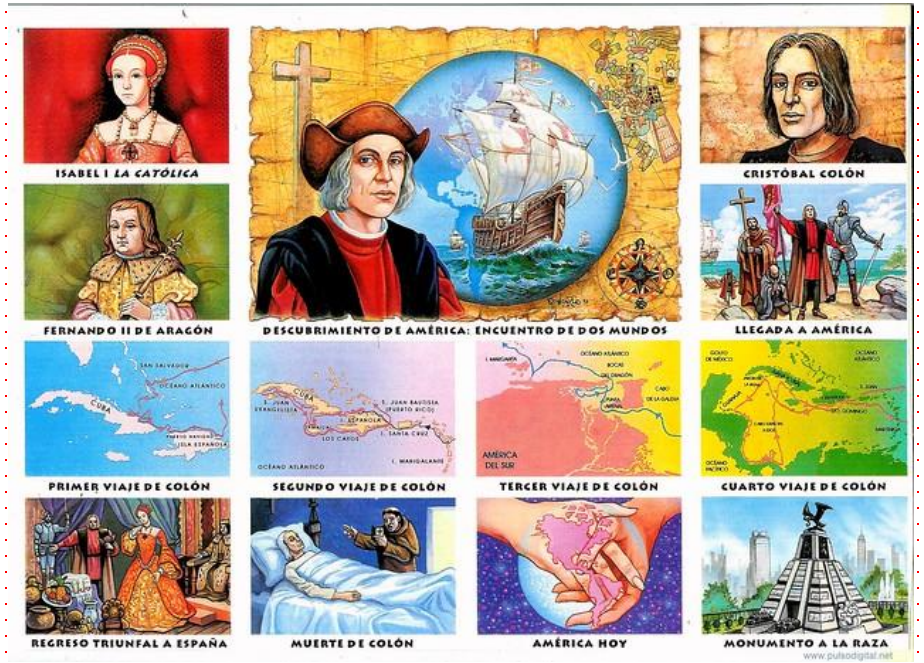
CPP de la República de Panamá dice:

"Artículo 406. Procedencia. Puede practicarse un peritaje cuando sea necesario poseer conocimientos especiales en alguna ciencia, arte o técnica para descubrir o valorar un elemento de prueba. La prueba pericial debe ser practicada por expertos imparciales, objetivos e independientes.

Solo podrá fungir como perito la **persona natural que acredite mediante el respectivo certificado o diploma su idoneidad para la materia sometida a su experticia o dictamen**. Se exceptúan los casos prácticos para los cuales no se requiere diploma o certificado de idoneidad, en cuyo caso deberá acreditarse la experiencia."

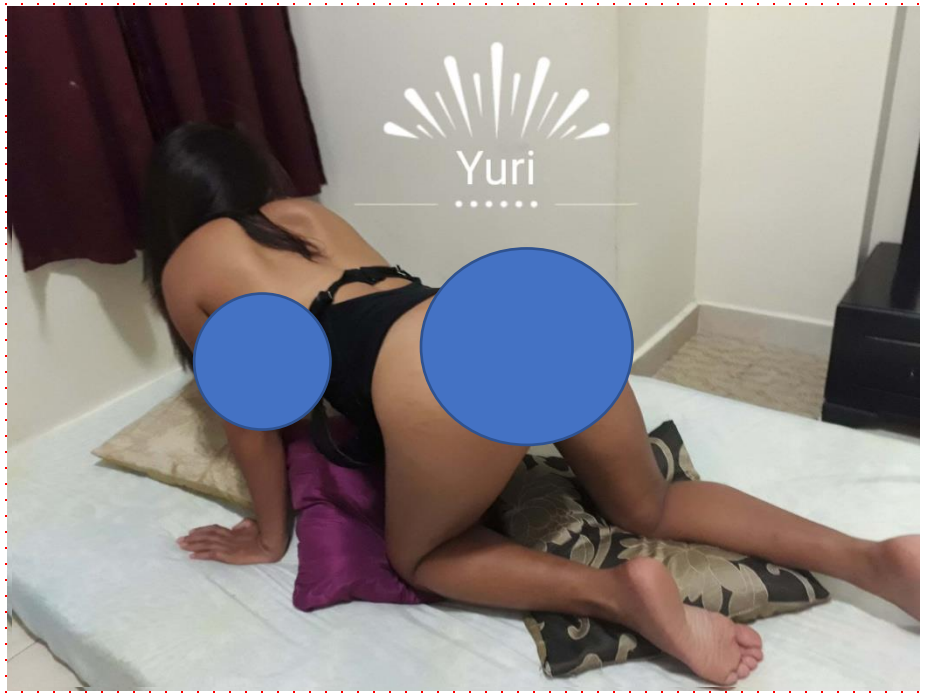
Metadatos

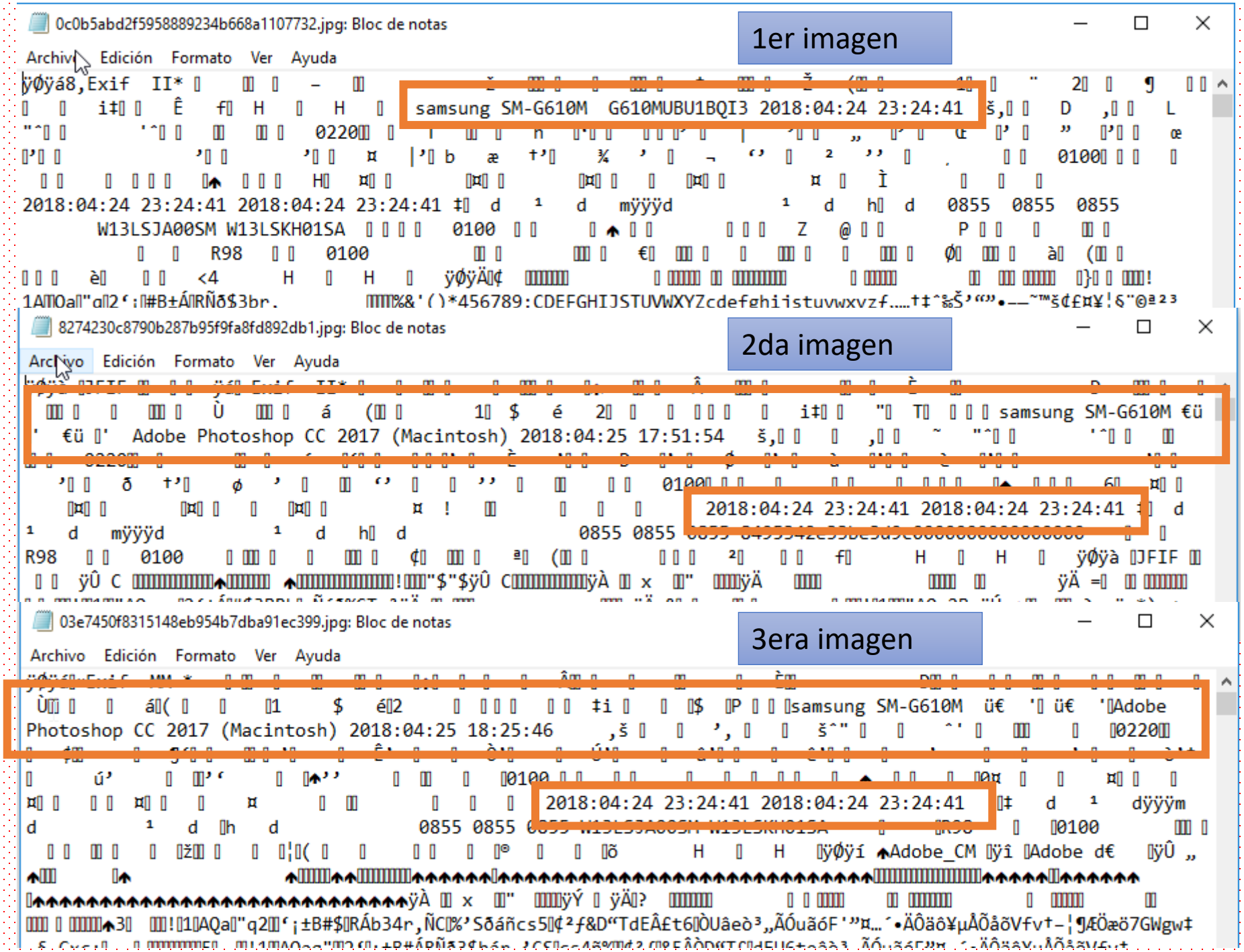
- Datos que describen a un archivo (leyenda de un archivo)
  - Nombre del archivo
  - Tamaño
  - Ubicación
  - Desde que dispositivo se generó
  - Coordenadas
  - Fecha de creación
  - Fecha de modificación
  - Fecha de ultimo acceso
  - Ruta del archivo



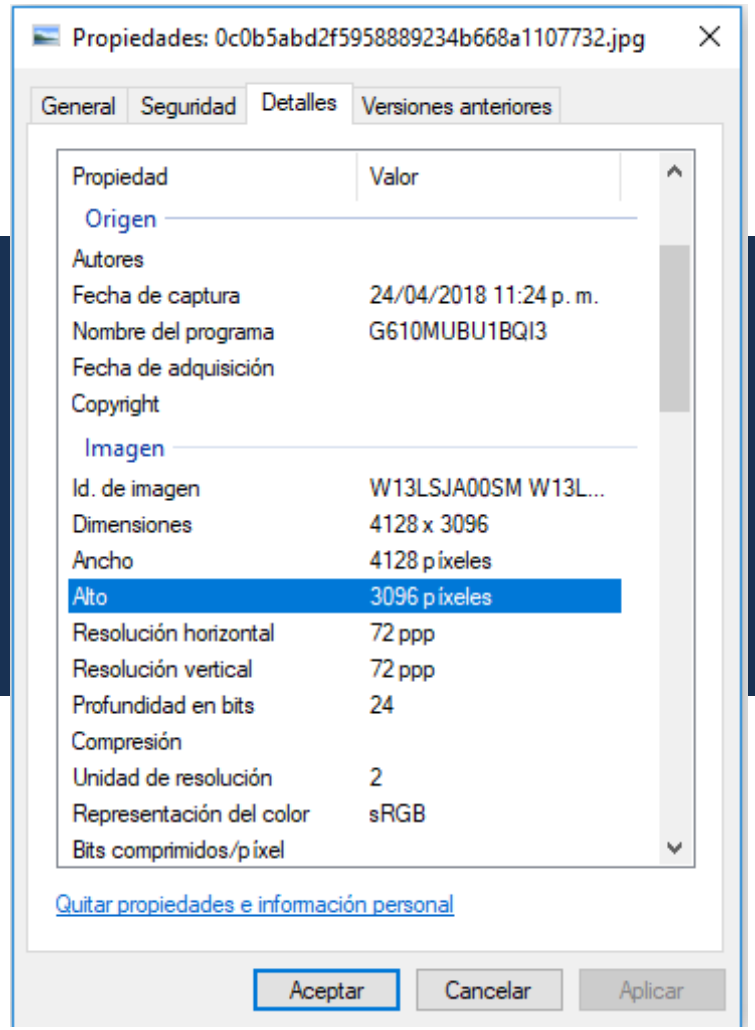
Type	Value
Latitude	8.902222222222223
Longitude	-79.58138888888888
Device Model	GT-I8200L
Device Make	SAMSUNG
Source File Path	/LogicalFileSet1/IMG_20170912_163935.jpg
Artifact ID	-9223372036854775807

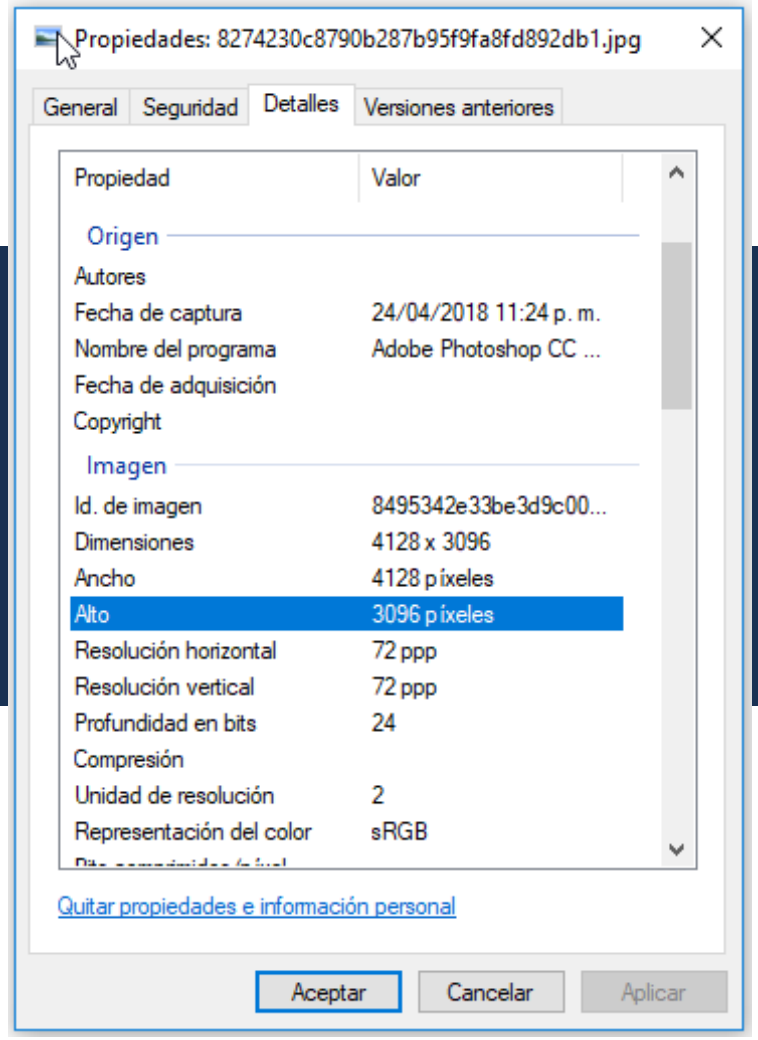
Imágenes ejemplo…

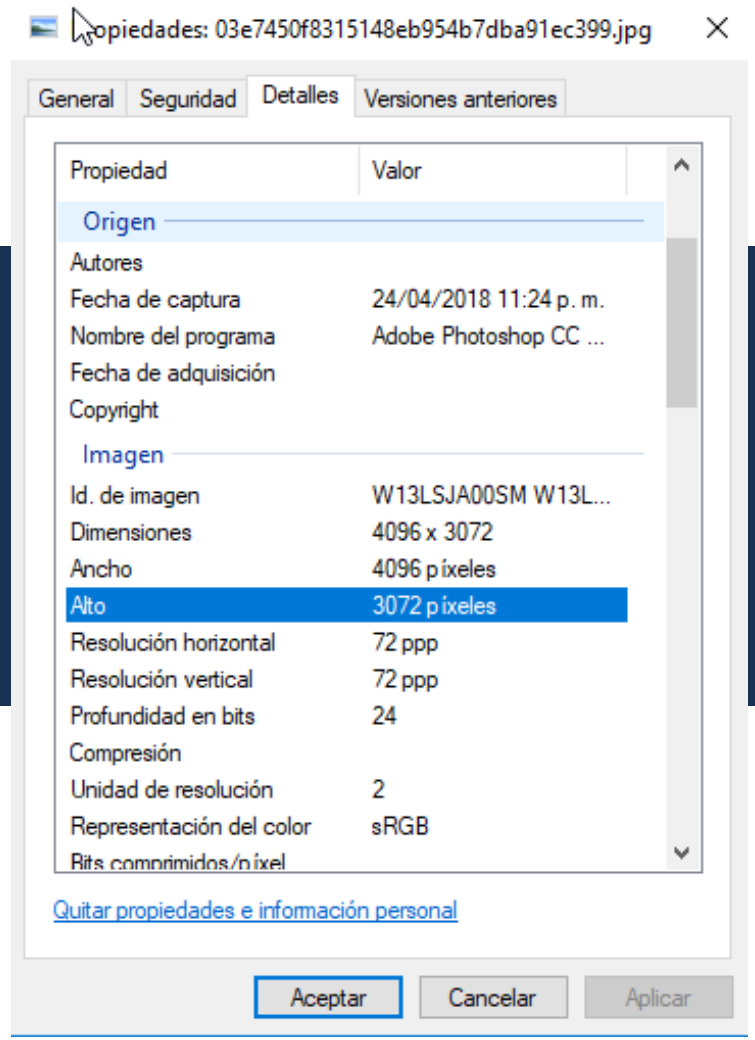



0c0b5abd2f5958889234b668a1107732.jpg: Bloc de notas
Archivo Edición Formato Ver Ayuda
1er imagen
samsung SM-G610M G610MUBU1BQI3 2018:04:24 23:24:41
2018:04:24 23:24:41 2018:04:24 23:24:41
W13LSJA00SM W13LSKH01SA
8274230c8790b287b95f9fa8fd892db1.jpg: Bloc de notas
Archivo Edición Formato Ver Ayuda
2da imagen
samsung SM-G610M
Adobe Photoshop CC 2017 (Macintosh) 2018:04:25 17:51:54
2018:04:24 23:24:41 2018:04:24 23:24:41
03e7450f8315148eb954b7dba91ec399.jpg: Bloc de notas
Archivo Edición Formato Ver Ayuda
3era imagen
samsung SM-G610M
Adobe Photoshop CC 2017 (Macintosh) 2018:04:25 18:25:46
2018:04:24 23:24:41 2018:04:24 23:24:41
Adobe_CM
Adobe

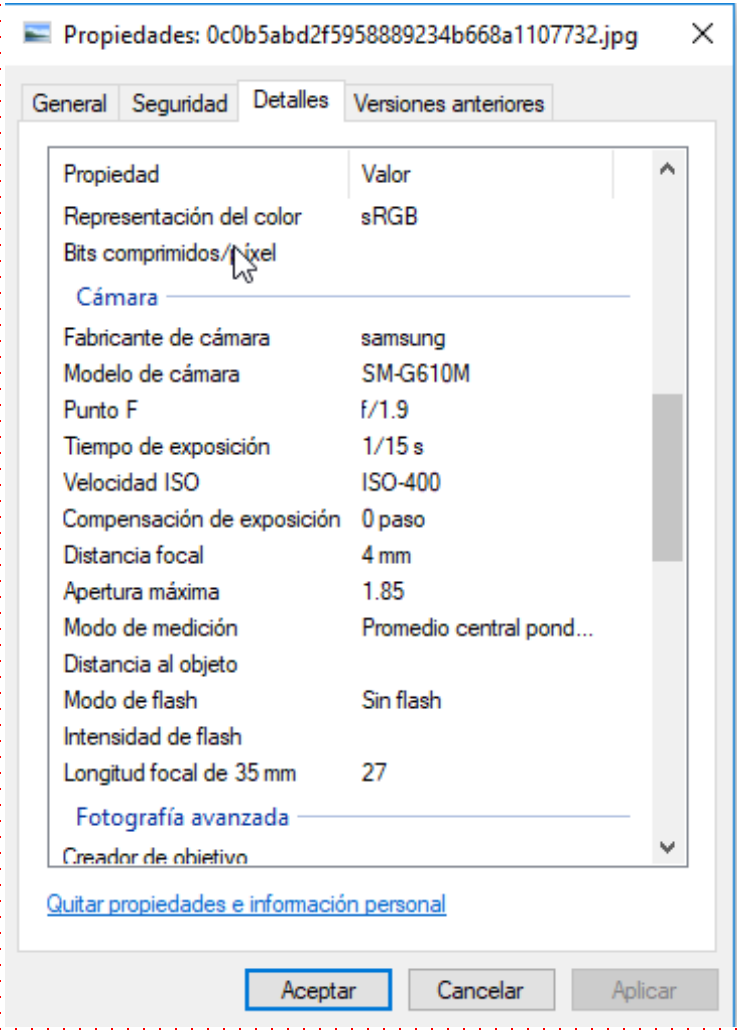
Propiedades: Origen

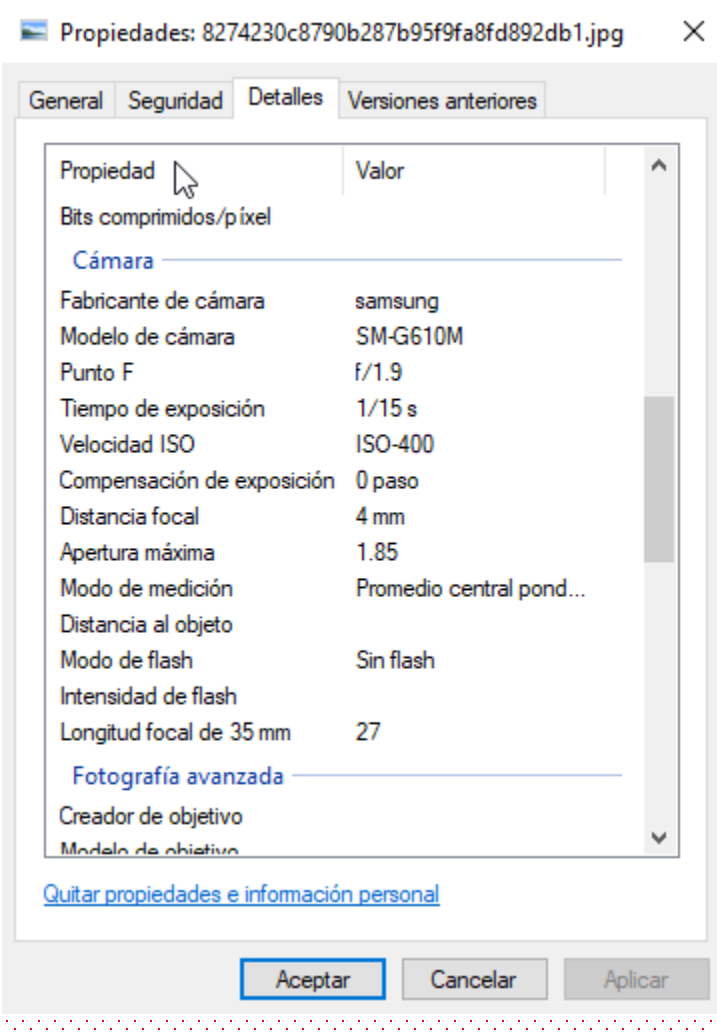


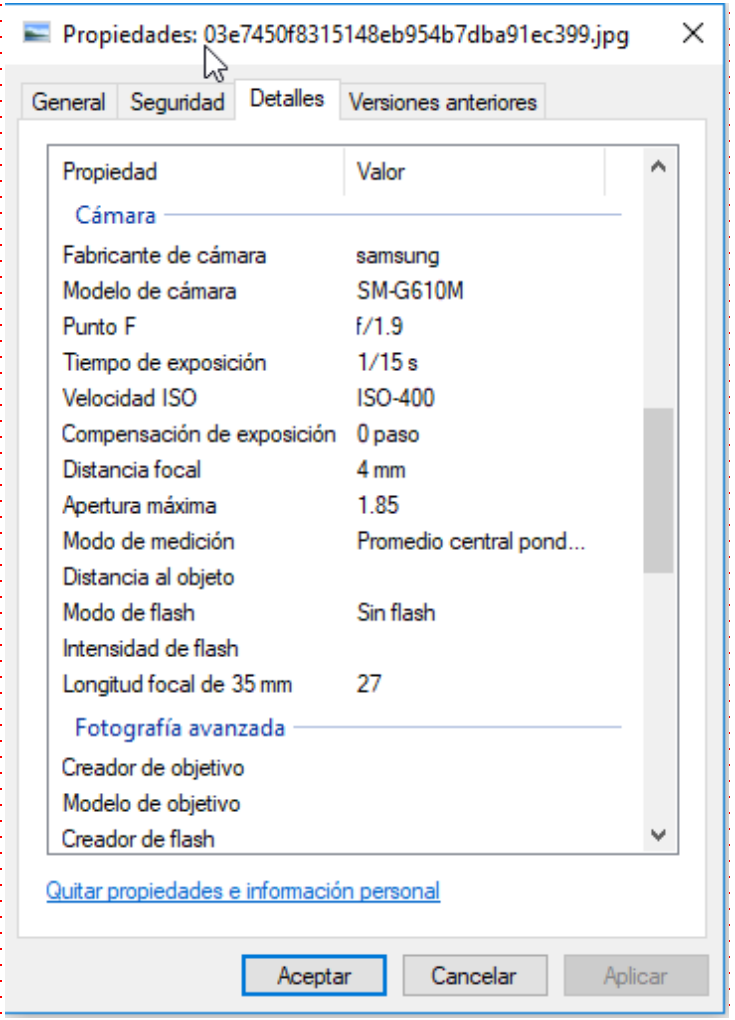




Propiedades: Cámara







Archivo Caché

Área de almacenamiento dedicada a la recuperación a gran velocidad de los datos usados o solicitados con más frecuencia.

Ej: estados de Whatsapp, Paginas web, documentos

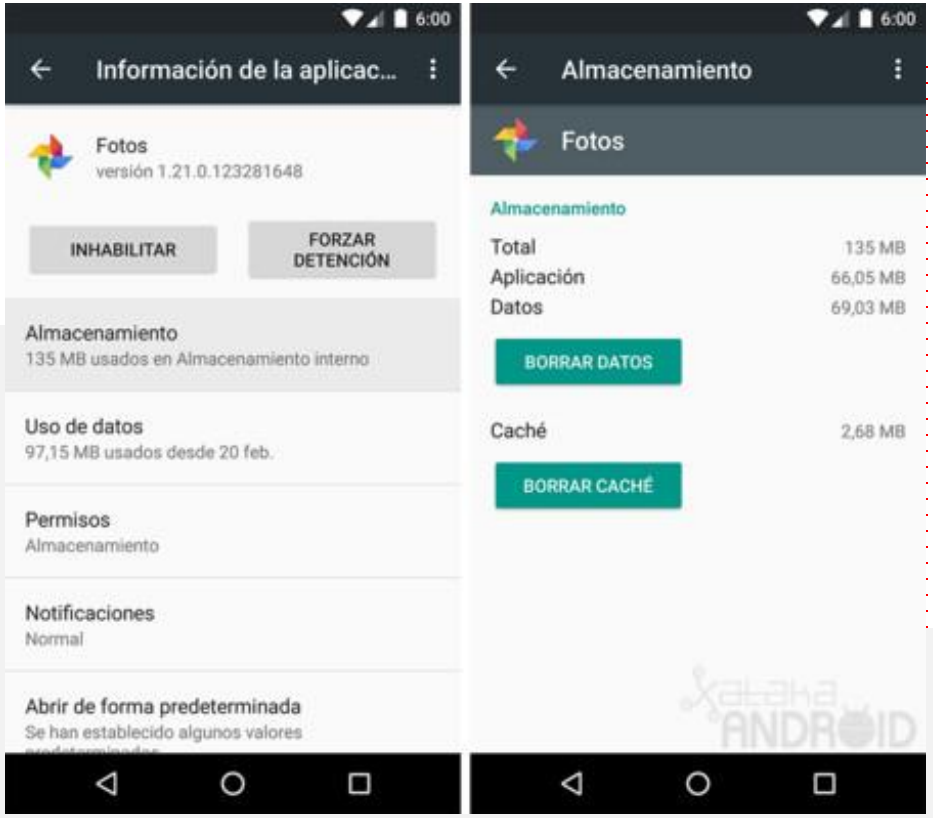
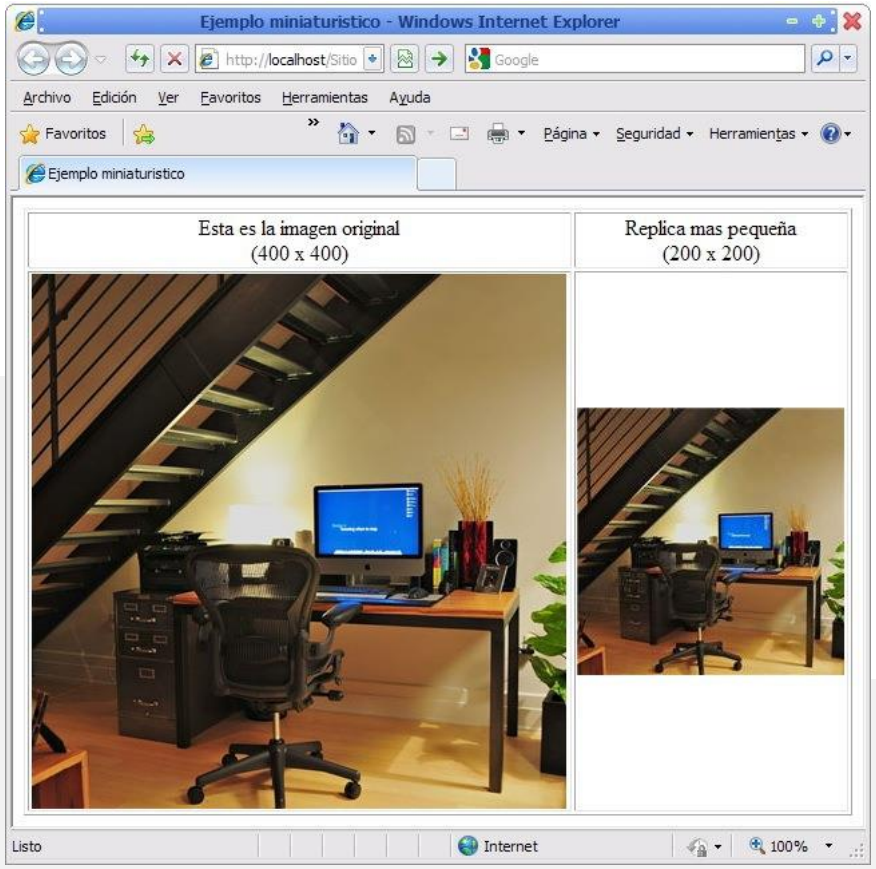


Imagen Thumbnail

Versión reducida de una imagen, para que sea más fácil su carga, renderizado e identificación.

Ej: Galería de fotos



VS

Luis Adolfo Chavez Salazar

Digitally signed by Luis Adolfo Chavez Salazar
DN: ou=Terms of use at www.e-sign.cl/rpa C(04), ou=Authenticated by E-Sign S.A., ou=Member, VeriSign Trust Network, ou=Digital ID Class 2, ou=RUT - 16474110-9, cn=Luis Adolfo Chavez Salazar, email=lchavez@e-sign.cl
Date: 2012.01.03 12:31:00 -03'00'

Niveles de la información digital

Valor binario = 1 o 0

Conjuntos de 1 y 0 = letra/símbolo/número

Cadena = Dato

Conjunto de datos = Registro

Registro = Información

Valor HASH

Valor iniciar **2**

Seguir los siguientes pasos:

1. Sumar 4
2. Dividir entre 2
3. Multiplicar por 5

¿Cuál es el resultado?

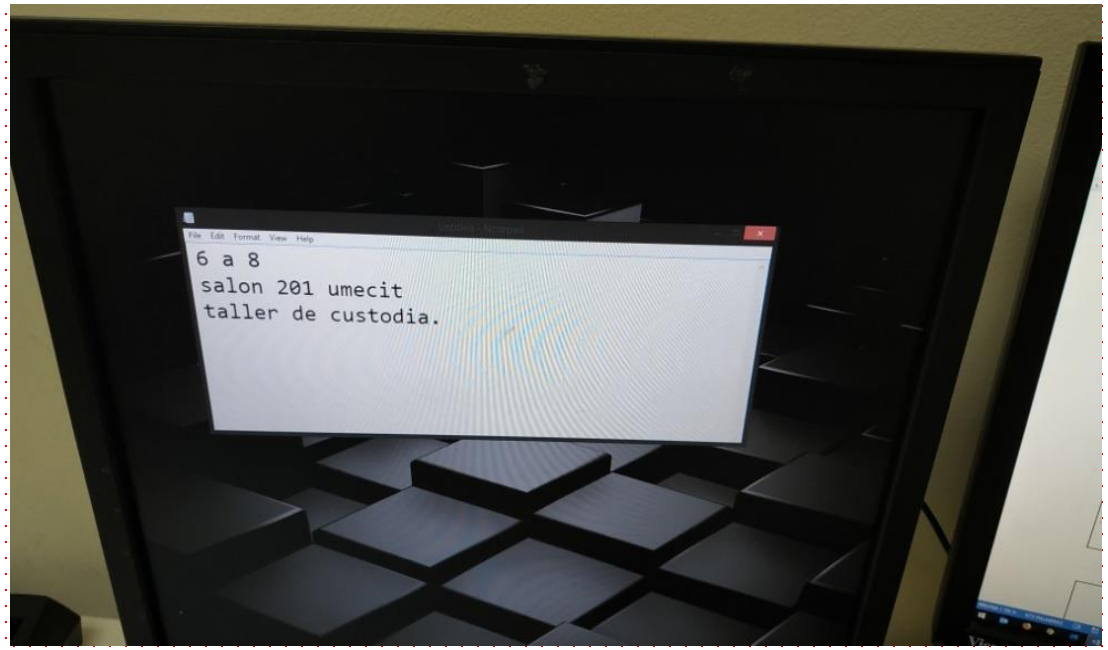
- Resultado único obtenido de la secuencia de instrucciones matemáticas (cálculos y operaciones algebraicas) realizadas sobre determinado valor inicial.
- El resultado es una cadena alfanumérica.
- A la secuencia de instrucciones se les conoce como Algoritmo.
- Ejemplo de Algoritmos: MD5, SHA-1, SHA-256.
- La longitud de la cadena depende del algoritmo utilizado.

palabra	Valor HASH MD5	Valor Hash SHA-1
Panama	6bec347f256837d3539ad619bd489de7	1e36b31e788231fba03577144de1d23b04a5d324
panama	a0420c052acb3a75b05456fabf9093dc	04e211be7c0964a2686badec91c70403a08a703d
Panamá	ab3a984364b4a1c99eec99df56c87edf	88329bdf2ef0365c57b4268d0df26f9588afa8d3
panamá	109557d4a746a623c8a34ef919345700	17e09bcc4636221212aaa919c2e0b2469be23518

https://hash.online-convert.com/es/generador-md5

Ejemplo de valor HASH…

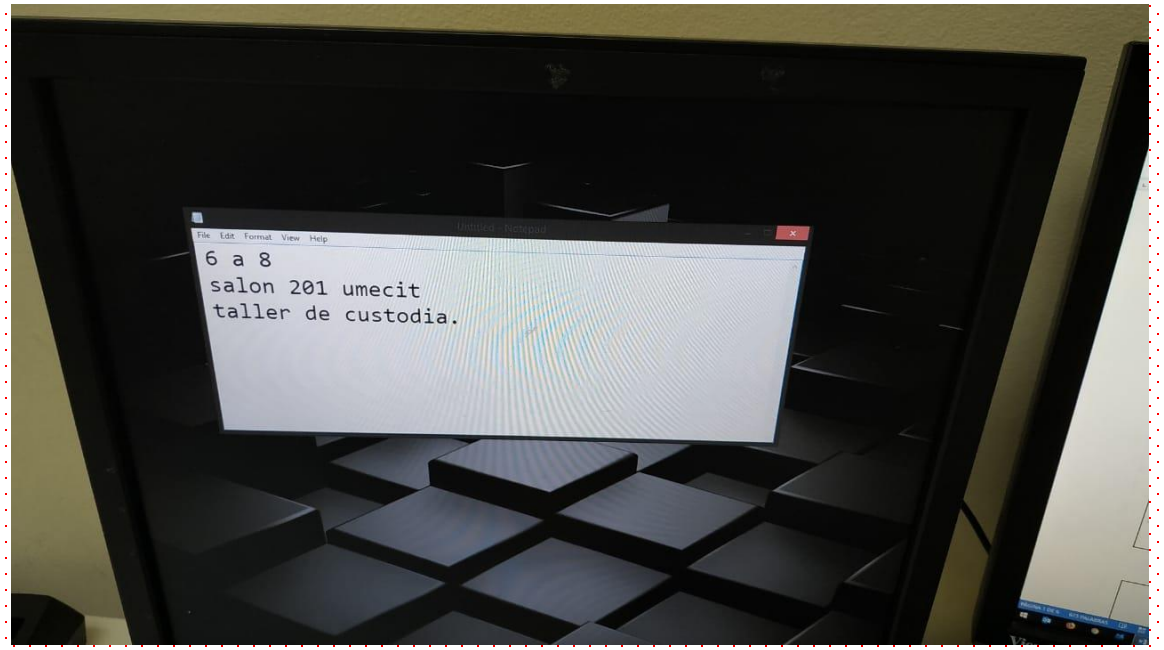
Imagen 1



IMG_20190401_142144.jpg
MD5: BBE7103317EE827B3FC817071077151F
SHA-1: D838DD2CB5FDE877910EAFF5CD022DC144D8D171

Tomada con la Cámara

Imagen 2



IMG-20190405-WA0000.jpg
MD5: 78C1A3DD0E955E0D744A88BB404D658F
SHA-1: 77BFD670E46C4CFE976D9C3CD65084689155AF78

Enviada por Whatsapp

Cadena de custodia y descripción de indicios

Identidad

Integridad y autenticidad

Preservación

Seguridad

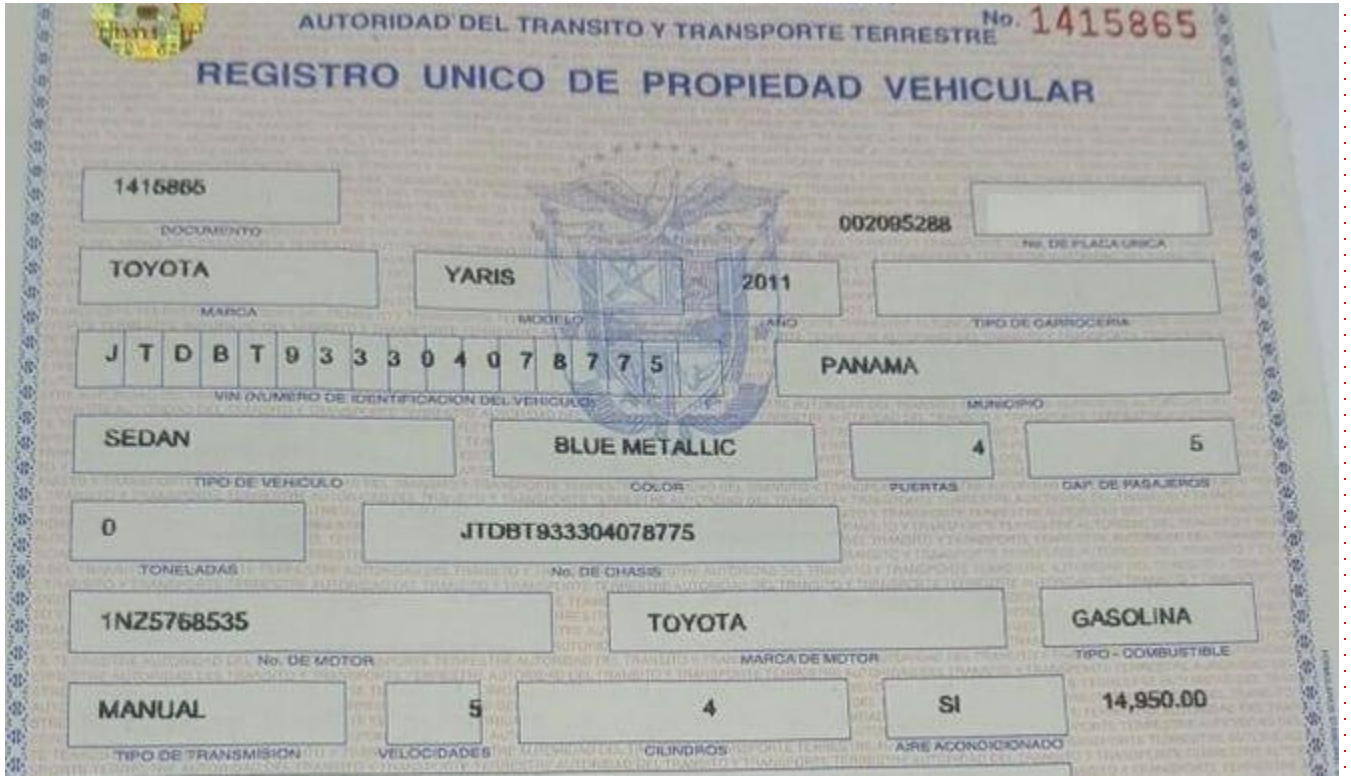
Almacenamiento

Continuidad

Mismidad

Principios

Identidad: Entendida como la individualización del indicio y/o evidencia, mediante la descripción completa de sus características específicas y condiciones físicas.


AUTORIDAD DEL TRANSITO Y TRANSPORTE TERRESTRE

No. 1415865

REGISTRO UNICO DE PROPIEDAD VEHICULAR

1415865 (DOCUMENTO)

002095288 (No. DE PLACA UNICA)

TOYOTA (MARCA) | YARIS (MODELO) | 2011 (AÑO) | (TIPO DE CARROCERIA)

J T D B T 9 3 3 3 0 4 0 7 8 7 7 5 (VIN (NUMERO DE IDENTIFICACION DEL VEHICULO))

PANAMA (MUNICIPIO)

SEDAN (TIPO DE VEHICULO) | BLUE METALLIC (COLOR) | 4 (PUERTAS) | 5 (CAP. DE PASAJEROS)

0 (TONELADAS) | JTDBT933304078775 (No. DE CHASIS)

1NZ5768535 (No. DE MOTOR) | TOYOTA (MARCA DE MOTOR) | GASOLINA (TIPO - COMBUSTIBLE)

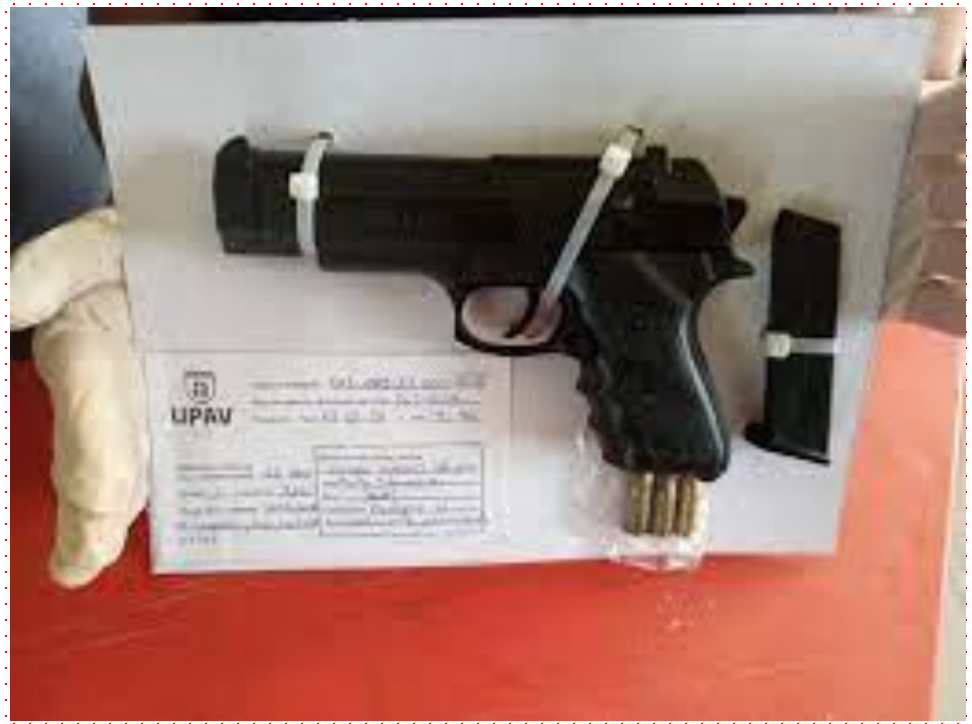
MANUAL (TIPO DE TRANSMISION) | 5 (VELOCIDADES) | 4 (CILINDROS) | SI (AIRE ACONDICIONADO) | 14,950.00

Principios

Integridad y autenticidad: Determina que el indicio y/o evidencia que se encontró y recolectó, o se incorporó conforme al debido proceso, está completo y es el mismo que se está utilizando para tomar una decisión judicial y que sus características no han cambiado, salvo en aquellos casos en que por la misma naturaleza del indicio y/o evidencia se produzcan transformaciones inevitables o se hayan realizado modificaciones durante la práctica de alguna prueba, de lo cual se deberá dejar constancia escrita.

Preservación: Es el mantenimiento y resguardo del indicio y/o evidencia en condiciones adecuadas que aseguren su conservación e inalterabilidad de acuerdo con su clase y naturaleza.

Seguridad: Son todas aquellas actividades encaminadas a mantener los indicios y/o evidencias en un lugar seguro, libres y exentos de todo riesgo, asegurando la certeza de su origen y destino. Esta misma protección y vigilancia se ejercerán sobre los documentos que formen parte del sistema de cadena de custodia.



Principios

Almacenamiento: Es la acción de guardar el indicio y/o evidencia bajo las condiciones adecuadas, de acuerdo con los procedimientos técnicos y científicos de cada especialidad, manteniendo su preservación y seguridad.

Continuidad: Se refiere al traslado y traspaso del indicio y/o evidencia en secuencia ininterrumpida, desde su ubicación en el lugar de los hechos investigados o donde se descubran y recolecten, hasta su disposición final.

Principios

Mismidad: Hace referencia a la capacidad de probar que se trata del “mismo indicio y/o evidencia”, en el “mismo estado” y con la “misma relación” y en el “mismo momento” del hecho, salvo en aquellos casos en que por la misma naturaleza del indicio y/o evidencia se produzcan transformaciones inevitables o se hayan realizado modificaciones durante la práctica de alguna prueba, de lo cual se deberá dejar constancia escrita.

Cadena de custodia y descripción de indicios

Número IMEI:

- Número de serie (15 valores) que identifica al terminal físicamente
- Se encuentra en la parte trasera del dispositivo, en el porta SIM, o detrás de la batería

Cadena de custodia y descripción de indicios

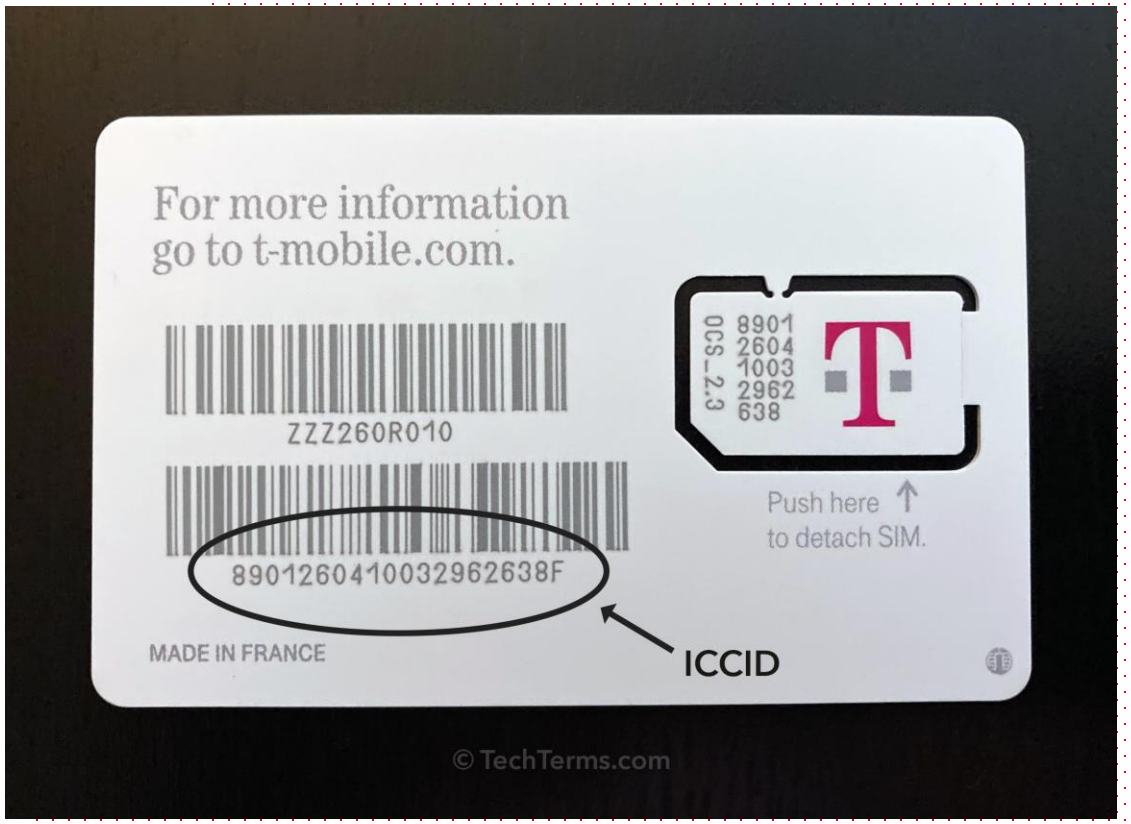
Número ICCID:

- número gravado en la SIM de nuestro teléfono 20 dígitos

- Comienza con 89

- MCC: Código de País Móvil

- MNC: Código de Red Móvil




SIM2
microSD
SIM1
TELEFONO CELULAR
/ CELLULAR PHONE
NOM


SAMSUNG
NOM

Cadena de custodia y descripción de indicios

Número de serie/Service Tag:

- Identificación única de cada computador o CPU para computadoras Dell, Lenovo y HP

Cadena de custodia y descripción de indicios

Presentación de la evidencia

Presentación de la evidencia digital

Documentos/archivos nativos digitales:

- Tiene metadatos propios, es sustentable su origen, nunca se a impreso.
- Es fácil de replicable y verificable.
- Reportes de sistemas de información, registros extraídos de una base de datos, documentos PDF firmados electrónicamente, sonido, imagen.

Documentos/archivos migrados a un medio digital:

- No tiene metadatos propios, difícil sustentar su origen, ya existe en el mundo presencial.
- Fácil de replicar, no es tan fácil verificar.
- Imagen escaneada, foto de un documento de identidad

Captura de pantalla:

- Intenta ilustrar un determinado contenido en un determinado instante-momento.
- Difícilmente replicable, fácil de verificar.

Presentación de la evidencia digital

Principios	Contexto	Finalidad	Utilidad
Relevancia	Condición jurídica que contempla elementos analizados bajo la pertinencia de los que mismos respecto del caso.	Probar o no la hipótesis planteada a partir de la exclusión del material que resulte irrelevante.	Si se encuentran elementos que no cumplan esta condición deben ser excluidos.
Confiabilidad	Permite desde la parte técnica facilitar la contradicción.	Validar la repetibilidad y auditabilidad del proceso aplicado para la obtención de evidencia.	Si un tercero (Contraparte) sigue el mismo proceso debe obtener los mismos resultados.
Suficiencia	Permite entender la experiencia y formalidad del perito.	Validar si las evidencias recolectadas y analizadas tienen elementos suficientes para sustentar los hallazgos.	Analiza la completitud de las pruebas.

Fuente:
https://www.unodc.org/documents/ropan/2021/PANZ41/Aspectos_basicos_de_la_investigacion_que_involucra_prueba_digital.pdf

Presentación de la evidencia digital

Fuente:
https://www.unodc.org/documents/ropan/2021/PANZ41/Aspectos_basicos_de_la_investigacion_que_involucra_prueba_digital.pdf

Gracias

“Ciencia y Tecnología al Servicio de la Verdad y la Justicia”