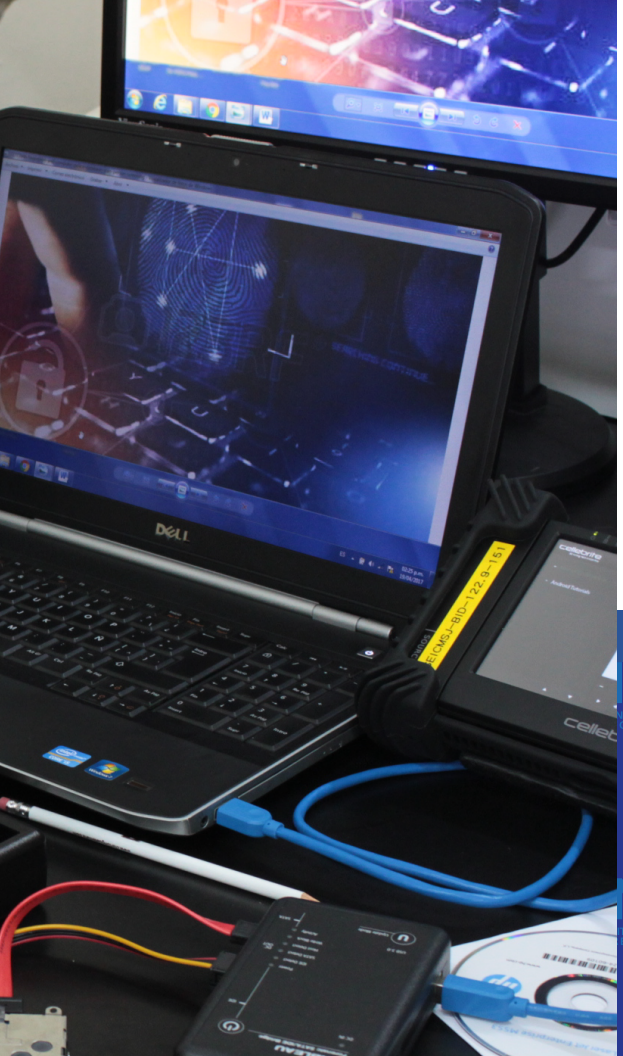


INACIF
INSTITUTO NACIONAL DE CIENCIAS FORENSES DE GUATEMALA

VERDAD Y JUSTICIA,
NUESTRO COMPROMISO

Laboratorio de Informática Forense

Dra. Ingrid Johana Romero Escribá. Administración 2022-2027

OTD-DTC-LAB-064 Versión 01

Esta guía será de utilidad para autoridad competente con el fin de realizar las solicitudes de análisis y remisión de indicios conforme a los servicios que presta la institución actualmente.

La información de este documento se basa en la guía identificada como OTD-DTC-LAB-064 versión 01.

Laboratorio de Informática Forense

Índice

	Presentación	7
1.	Informática Forense	9
2.	Laboratorio De Informática Forense	9
3.	Servicios que ofrece el laboratorio	9
3.1.	Descargas de seguridad de plataformas que prestan servicios en internet	9
3.2.	Análisis de dispositivos móviles	9
3.3.	Análisis de computadoras y dispositivos de almacenamiento	10
3.4.	Indicios que se analizan en el Laboratorio de Informática Forense de INACIF	10
4.	Análisis que no realiza el laboratorio	10
5.	Requisitos para solicitar servicios (indicios y solicitud de análisis)	11
5.1.	Recomendaciones para el embalaje	11
5.2.	Recomendaciones generales	11
5.3.	¿Cómo solicitar los análisis?	11
6.	Tiempo de análisis	11
7.	Glosario	12

Presentación

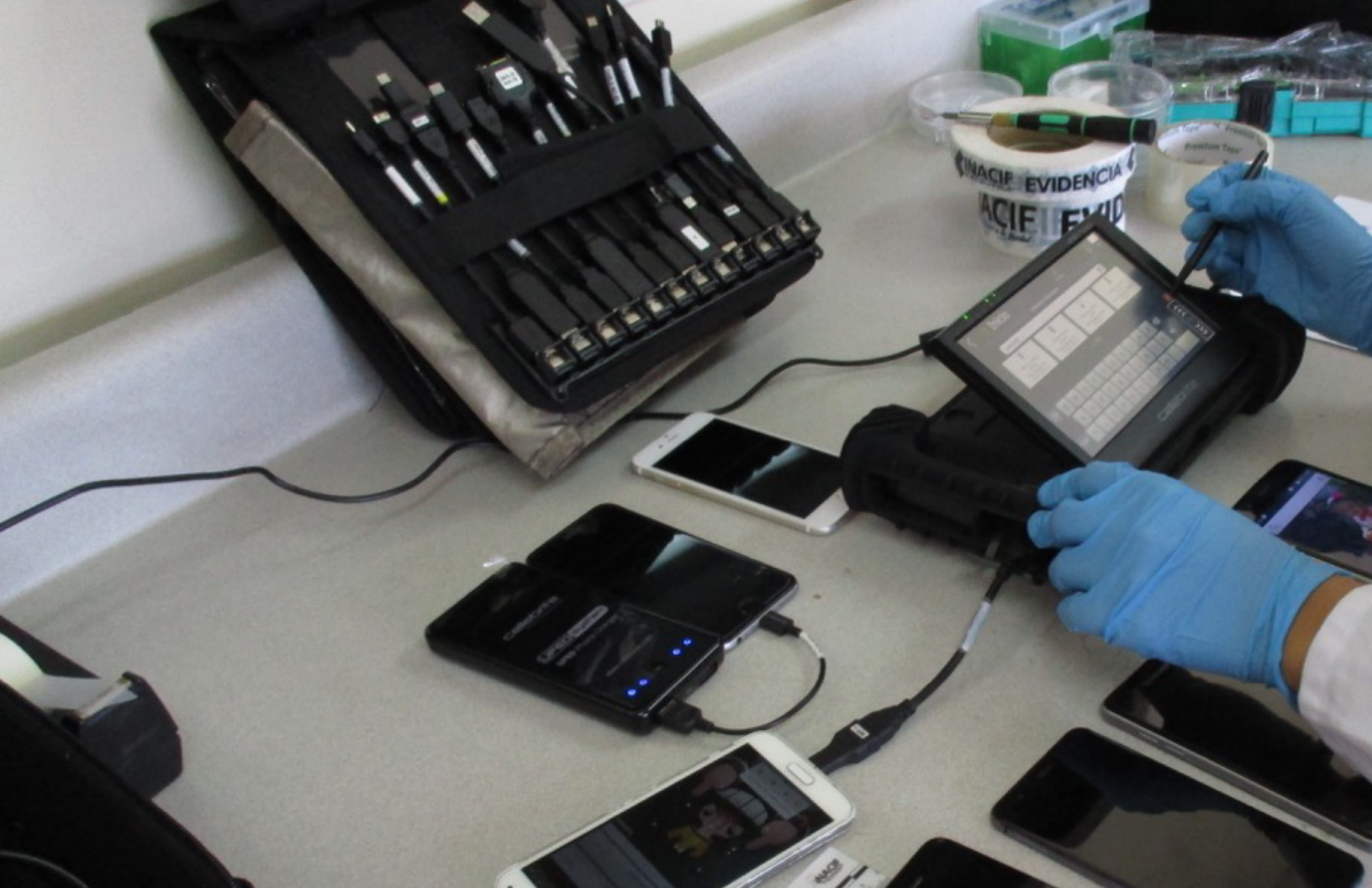
El Instituto Nacional de Ciencias Forenses de Guatemala -INACIF- presenta esta versión actualizada de la *Guía de Servicios del Laboratorio de Informática Forense*, como una herramienta útil a la autoridad competente que realiza requerimientos a dicho laboratorio, en el marco de una investigación penal.

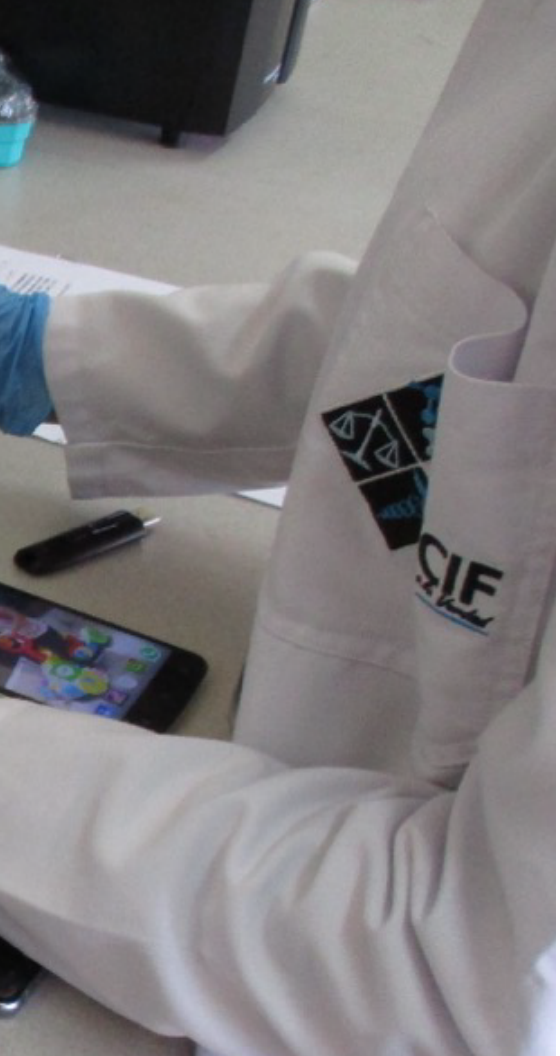
Asimismo, esta versión incluye los servicios de análisis informático forense relacionados a: descargas de seguridad de plataformas que prestan servicios en internet (redes sociales, correos electrónicos con credenciales de acceso); análisis de dispositivos móviles (celulares, tablets, tarjetas SIM) y análisis de computadoras y dispositivos de almacenamiento.

Uno de los servicios que actualmente presta el Laboratorio de Informática Forense (Análisis de dispositivos móviles (tarjetas SIM)) cuenta con una metodología acreditada bajo la Norma de Calidad Internacional ISO/IEC 17025:2017. Esta acreditación demuestra la estandarización de los procedimientos analíticos para la obtención de los resultados y evidencia la competencia técnica y operativa del área.

Adicionalmente, la presente guía es útil como fuente de información para personas individuales y entidades afines, que deseen conocer la gama de servicios con la que cuenta el Laboratorio de Informática Forense del INACIF y que evidencia el compromiso de la institución de poner a disposición del Sector Justicia, investigación científico forense de calidad internacional.

Es importante tomar en cuenta que el trabajo conjunto entre Organismo Judicial, Ministerio Público, INACIF y demás instituciones del sector justicia, es determinante para generar un sistema oportuno y adecuado a las necesidades del país. En ese sentido, es básico el intercambio de información y la generación de guías y otros documentos que permitan establecer las directrices y los requisitos idóneos para su funcionamiento.


EVIDENCIA



1. INFORMÁTICA FORENSE

Según Buró Federal de Investigaciones -FBI por sus siglas en inglés-, la Informática Forense es la ciencia que permite adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y almacenados en un medio computacional.

2. LABORATORIO DE INFORMÁTICA FORENSE

Los análisis correspondientes al Laboratorio de Informática Forense del INACIF, por su función, son análisis denominados post-mortem, debido a que no se asiste a la escena del crimen para realizar imágenes forenses en el lugar o para extraer datos en sistemas activos.

3. SERVICIOS QUE OFRECE EL LABORATORIO

Los servicios que presta el laboratorio son aplicables a todos los hechos en donde se hayan utilizado dispositivos de almacenamiento digital o las Tecnologías de Información y Comunicación (TICs), como medio o fin para cometer un delito.

3.1. Descargas de seguridad de plataformas que prestan servicios en internet (Redes sociales, correos electrónicos con credenciales de acceso)

- Análisis de perfiles de redes sociales con credenciales de acceso (voluntario)
  - ✓ Facebook
  - ✓ Google takeout (servicios asociados a Google)
  - ✓ Twitter
  - ✓ Snapchat
  - ✓ Instagram
  - ✓ WhatsApp (conversaciones)

3.2 Análisis de dispositivos móviles (celulares, tablets, tarjetas SIM)

- Registro de llamadas
- Registro de chats
- Registro de mensajes
- Registro de contactos

- Registro de imágenes
- Registro de videos
- Registro de audios
- Registro de correos electrónicos
- Timeline de actividad del dispositivo
- Redes inalámbricas a las que se hubiera conectado el dispositivo
- Desbloqueo de patrones y contraseñas
- Cuentas asociadas al dispositivo
- Existencia de aplicaciones instaladas
- Determinar el proveedor de servicio
- Historial de navegación
- Eventos en el calendario
- Análisis de correspondencia de IMEI

3.3 Análisis de computadoras y dispositivos de almacenamiento

- Búsqueda, restauración y extracción de archivos de:
  - ✓ Imagen
  - ✓ Audio
  - ✓ Video
  - ✓ Documentos
  - ✓ Correos electrónicos
  - ✓ Historial de internet
  - ✓ Archivos comprimidos
  - ✓ Archivos ejecutables
- Recuperación de datos y archivos en espacio no asignado
- Localización y análisis de máquinas virtuales
- Determinar línea de tiempos de creación, modificación y ultimo acceso de archivos
- Determinar hora del último inicio de sesión
- Análisis de registros de la computadora
- Redes inalámbricas a las que se hubiera conectado una computadora portátil
- Análisis de firmas de los archivos contenidos
- Búsquedas en el historial de navegación
- Recuperación de contraseñas almacenadas en los navegadores de internet
- Determinar registros de los dispositivos USB conectados a la computadora
- Existencia de programas instalados
- Usuarios del sistema
- Análisis de contenedores de correos electrónicos

3.4 Indicios que se analizan en el Laboratorio de Informática Forense del INACIF

- Computadoras
- Discos duros
- Discos ópticos (CD, DVD, BLURAY)
- Tarjetas de memoria (SD, Micro SD, etc.)
- DVR (bajo ciertos criterios)
- Memorias USB
- Teléfonos celulares
- Tablets
- Tarjetas SIM
- Cajas y dongles de flasheo
- Cámaras fotográficas y/o de video

4. ANÁLISIS QUE NO REALIZA EL LABORATORIO

- Rastreos de direcciones IP en la web
- Mejoramiento y análisis de video
- Mejoramiento y análisis de imágenes

- Mejoramiento y análisis de audio
- Análisis de funcionamiento, verificación o identificación de características de *routers*, moduladores, radiotransmisores.
- Dispositivos que no tienen almacenamiento local

5. REQUISITOS PARA SOLICITAR SERVICIOS (INDICIOS Y SOLICITUD DE ANÁLISIS)

5.1 Recomendaciones para el embalaje

- Las computadoras y discos duros se deben embalar en cajas de cartón, procurando que queden fijos a esta, haciendo uso de sujetadores plásticos con el fin de evitar que sufran golpes o vibraciones que puedan dañar los dispositivos.
- Los discos ópticos, tarjetas de memoria y memorias USB pueden ser embalados en sobres de papel manila y evitar la exposición a los rayos solares.
- Los dispositivos móviles como teléfonos celulares y tablets pueden ser embalados en sobres de papel manila, bolsas Faraday o cajas de cartón, evitando que sufran golpes que puedan dañen componentes electrónicos internos.

  De ser posible, se debe colocar el dispositivo en modo avión y deshabilitar las conexiones Wifi, Bluetooth y de transmisión de datos.

  Si al dispositivo no es posible deshabilitarle las opciones descritas, o no se puede apagar, se recomienda trasladar en bolsas Faraday o bien cubrirlo con cinco o más capas de papel aluminio.

  Se recomienda, que, de ser posible, se solicite al dueño del dispositivo, el pin, código, contraseña o el patrón de desbloqueo.

5.2 Recomendaciones generales

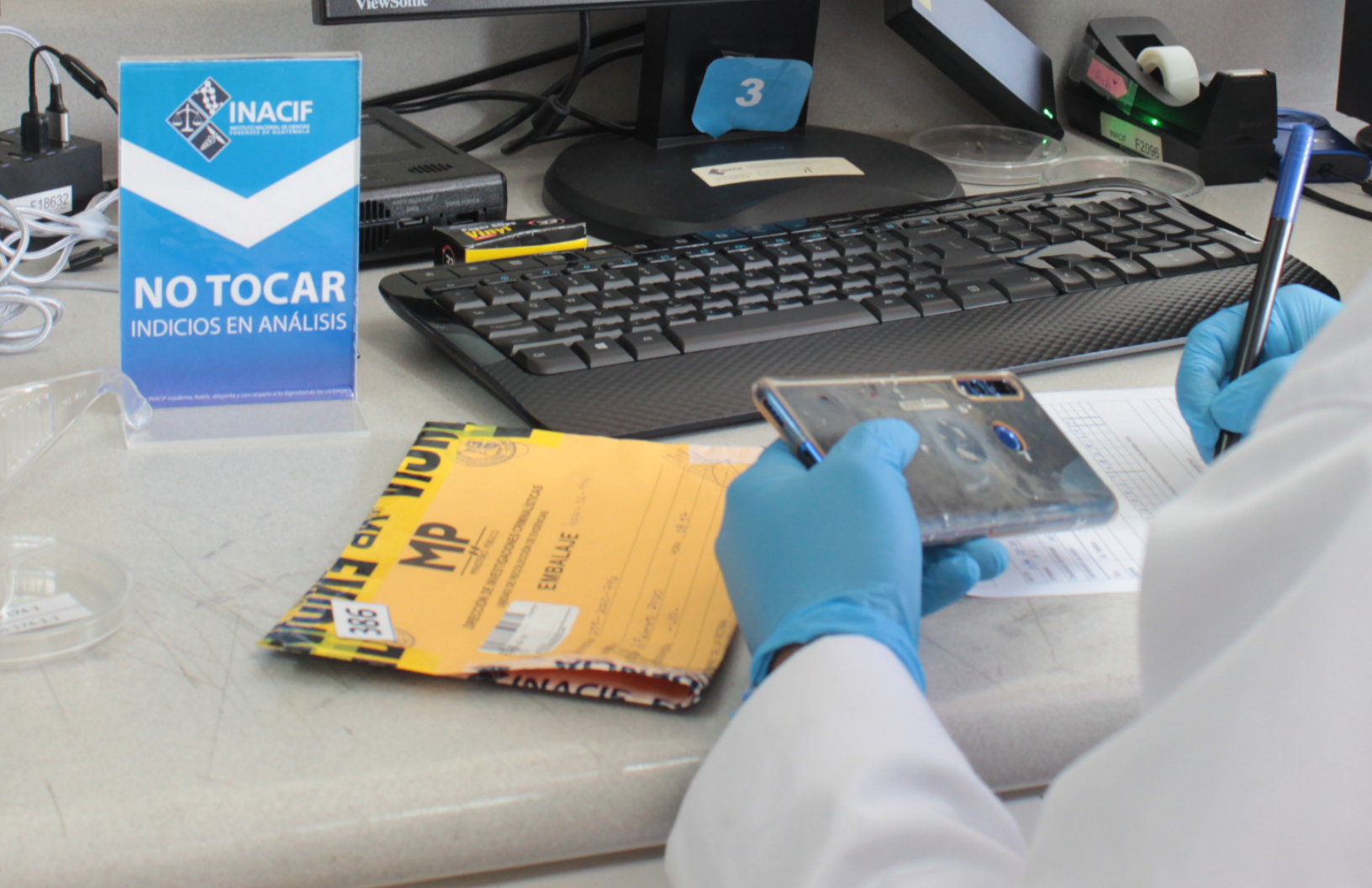
- Manipular los equipos adecuadamente.
- No someter a vibraciones.
- No exponer los dispositivos a altas o bajas temperaturas.
- Alejar fuentes electromagnéticas.
- Realizar una adecuada descripción de los indicios.
- No colocar en la descripción del indicio, datos que no son visibles o que se consultan en el sistema, como, por ejemplo, el IMEI lógico; esto es motivo de rechazo.

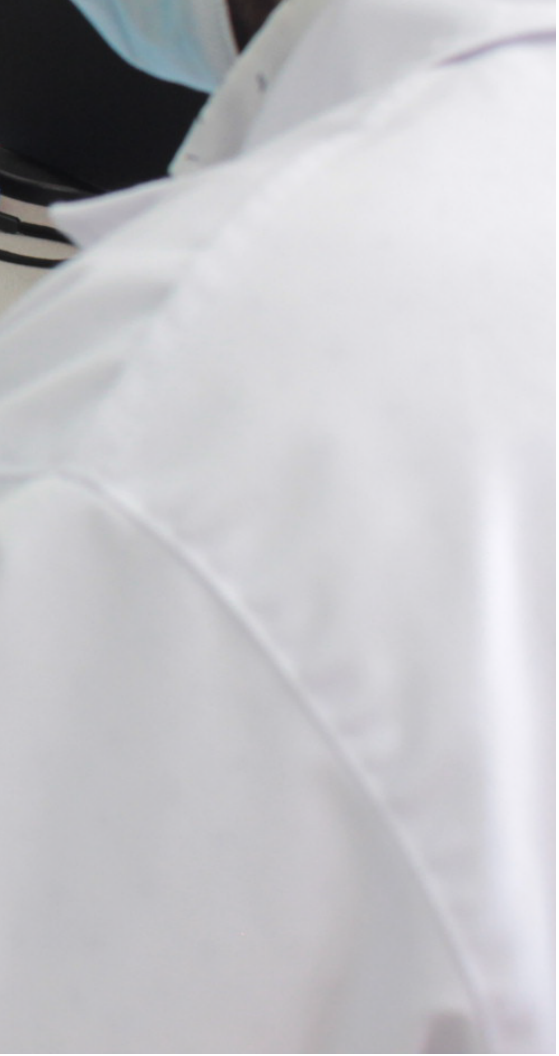
5.3 ¿Cómo solicitar los análisis?

Es necesario que el documento de cadena de custodia contenga lo siguiente:

- ✓ Referencia MP.
- ✓ Tipo de dispositivo.
- ✓ Fecha de recolección.
- ✓ Marca, modelo, serie, capacidad de almacenamiento, descripción física.
- ✓ Lugar de recolección.
- ✓ Solicitud específica.

- Si es un DVR, en la solicitud se debe colocar la fecha y hora (específicas) del suceso que se investiga, o de lo contrario la fiscalía debe adjuntar un disco duro de la misma capacidad para grabar el resultado de la extracción.
- Debe adjuntarse un oficio o describir en la cadena de custodia una **breve reseña** del hecho, con el fin de orientar la búsqueda de archivos y datos.
- La solicitud debe indicar qué es lo que se necesita, debido a que se rechazará si únicamente indica **"informática forense o guarda y custodia".**


INACIF
NO TOCAR
INDICIOS EN ANÁLISIS
MP
EMBALAJE
3



6. TIEMPO DE ANÁLISIS

El tiempo requerido para emitir un dictamen por el Laboratorio de Informática Forense es de 30 días aproximadamente, a partir de que el caso sea asignado al perito correspondiente.

7. GLOSARIO

Archivo Electrónico: conjunto de información que se almacena para consultarse o utilizarse posteriormente.

Código Hash: algoritmo matemático que se utiliza para hacer una comprobación criptográfica o un código de integridad de la evidencia informática o de comunicaciones.

Copia de seguridad: es un duplicado de la información importante, que se realiza para salvaguardar los archivos, por si ocurriese algún problema que impida acceder a los archivos originales almacenados.

Disco óptico: es un disco en el que los datos se graban y se leen a través de rayos láser.

Imagen Forense: proceso que se requiere para generar una copia "bit-a-bit" de todo el medio de almacenamiento, lo que permitirá recuperar en el siguiente paso, toda la información contenida y borrada del disco duro.

IMEI (International Mobile Equipment): el identificador internacional de equipos móviles, permite identificar teléfonos móviles GSM, su longitud típica es de 15 dígitos.

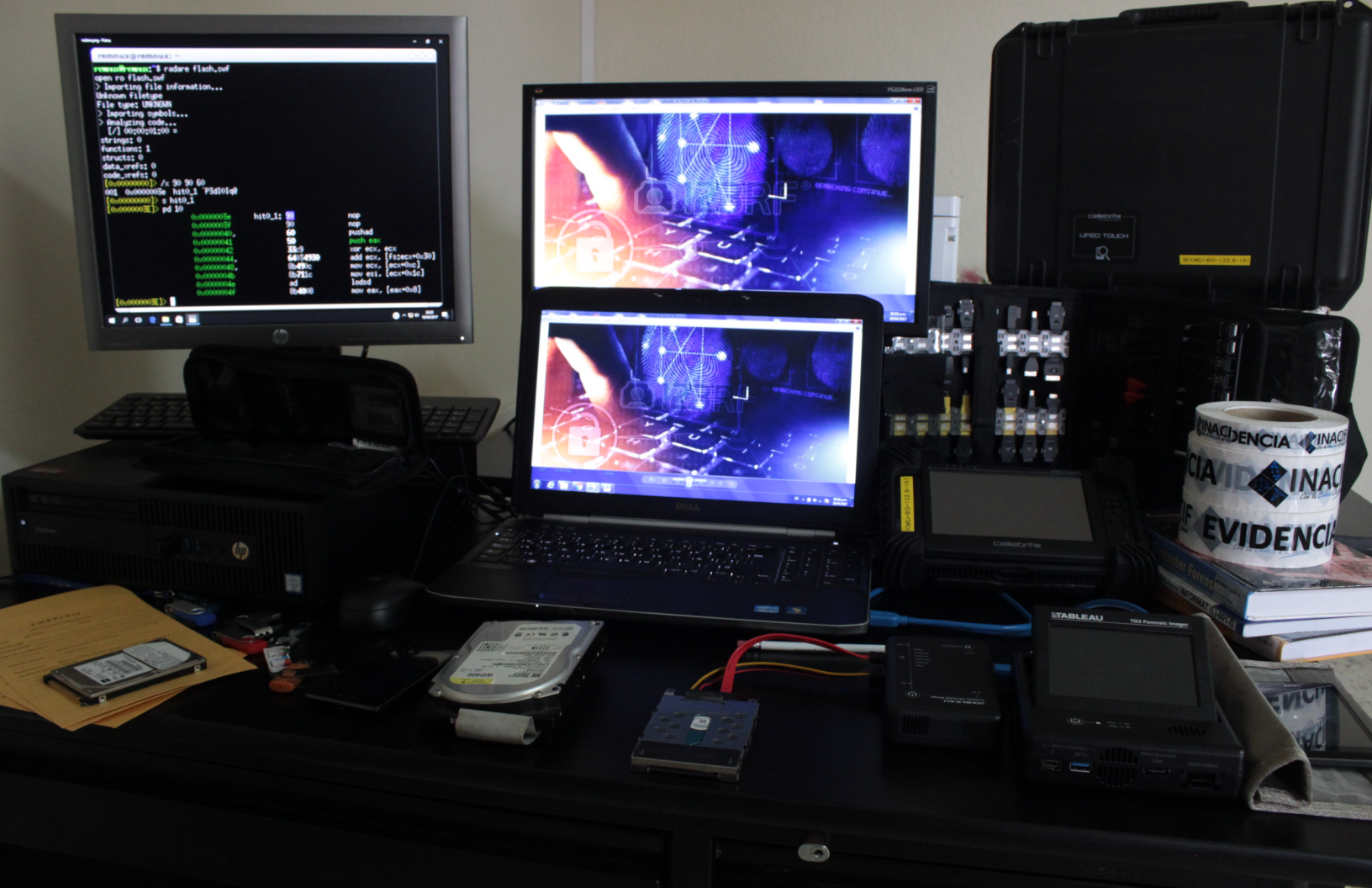
Memoria Flash: tipo de memoria que puede ser borrada y reprogramada en unidades de memoria llamadas "bloques".

Metadatos: es información que caracteriza o describe el contenido, calidad, condiciones, historia, disponibilidad y otras características de los datos o archivos.

SIM (Subscriber Identity Module/Módulo de Identidad del Suscriptor): es una tarjeta inteligente que guarda importantes datos en red necesarios para realizar una conexión con el proveedor de la red celular.

Tarjeta de memoria micro SD: es una tarjeta de memoria micro SD, es un formato para tarjetas de memoria flash para el almacenamiento de archivos digitales en dispositivos electrónicos. Es especialmente usado en teléfonos móviles, dispositivos GPS portátiles, reproductores de MP3, consolas de videojuegos, entre otros.

Teléfono móvil: dispositivo de comunicación que realiza una serie de funciones que van desde un simple organizador digital a una computadora personal de bajo nivel. Su tamaño es regularmente compacto, con batería y peso ligero. Estos dispositivos se conectan a una red de comunicaciones inalámbricas a través de transmisiones de ondas de radio o satélites.


remnux@remnux: ~
remnux@remnux:~$ radare flash.swf
open ro flash.swf
> Importing file information...
Unknown filetype
File type: UNKNOWN
> Importing symbols...
> Analyzing code...
[/] 00:00:01:00 =
strings: 0
functions: 1
structs: 0
data_refs: 0
code_refs: 0
[0x00000000]> /x 90 90 60
001 0x0000005e hit0_1 'PSdl0lq@
[0x00000000]> s hit0_1
[0x0000005E]> pd 10
hit0_1:
nop
nop
pushad
push eax
xor ecx, ecx
add ecx, [fs:ecx+0x30]
mov ecx, [ecx+0xc]
mov esi, [ecx+0x1c]
lodsd
mov eax, [eax+0x8]
SEARCHING CONTINUE...
celebrite
UFED TOUCH
INACIDENCIA
EVIDENCIA
TABLEAU
TD3 Forensic Imager

SÍGUENOS EN NUESTRAS REDES

14 Calle 5-49 zona 1 Edificio Nasa
PBX: 2327-3100
Correo electrónico : inacif@inacif.gob.gt
www.inacif.gob.gt