Investigación criminal

# Cibercrimen y evidencia digital

Del rastro informático a la identificación del autor



01

# La evidencia digital

Por qué no se trata como la prueba física

RASGOS PROPIOS

# ¿Qué la hace tan especial?

### Alterable

Puede modificarse con facilidad, incluso de manera involuntaria al acceder a ella.

### Duplicable

Admite copias idénticas al original, verificables bit a bit.

### Fácil de destruir

Se pierde o elimina en segundos si no se la resguarda a tiempo.

### Contundente

Si está bien preservada, su valor probatorio es muy alto.

**Elemento diferenciador: no se peritia como un arma; se trabaja sobre un copiado forense**

INTEGRIDAD DE LA PRUEBA

# Copia forense y función hash

## Copiado forense

- Se trabaja sobre una **copia bit a bit** del soporte original.
- Se utilizan **duplicadores forenses** y **bloqueadores de escritura** para no alterar el original.
- El análisis se hace sobre la copia, no sobre el dispositivo secuestrado.

## La huella digital del archivo

Al aplicar una función criptográfica a un documento, por ejemplo **SHA-256**, se obtiene un código de 64 caracteres hexadecimales: el **hash**. Funciona como su huella digital: cualquier cambio en el archivo produce un hash distinto.



02

# Del hecho al autor

El recorrido de una investigación por ciberdelitos

PRIMER ABORDAJE

# Denuncia, resguardo y requerimientos

## Resguardo inmediato

- Imágenes, videos y mensajes mediante el sistema **UFED**.
- También publicaciones en redes, correos electrónicos, capturas de sitios web, chats y audios.

## ¿A quién se pide información?

- A las empresas que prestan el servicio: Google, Microsoft, Yahoo, Meta (Facebook, WhatsApp), X (Twitter).
- Vía principal: **portales para fuerzas de seguridad**, ágiles, rápidos y seguros.

## Cooperación internacional

- **MLAT**: tratado de cooperación jurídica internacional en materia penal.
- En la práctica, una vía **lenta e ineficaz** para la urgencia de estos casos.

**Posibles infracciones: arts. 128, 131, 149 bis y 183, 2.º párrafo, CP. Los fraudes tienen un abordaje particular**

CIRCUITO DE TRABAJO

# De los datos de conexión al domicilio

| | | |
|---|---|---|
| 1 | **Respuesta de la empresa** | **Datos de registración** (nombre, edad, sexo, fecha de nacimiento, nombre de usuario, cuenta asociada) y **registros de creación y conexión** (IP, fecha, hora y huso horario). |
| 2 | **Conversión horaria** | Los datos de conexión se convierten al **huso horario local**. |
| 3 | **Consulta a los ISP** | Se requiere a las empresas proveedoras de internet qué cliente usaba cada IP en ese momento. |
| 4 | **Domicilio** | Del estudio de los logueos surge el domicilio o los domicilios del usuario; se ordenan medidas de constatación. |
| 5 | **Allanamiento** | Lo realizan **cuerpos especializados** y capacitados en el manejo de evidencia digital. |
| 6 | **Análisis forense** | Con software forense se analiza el material secuestrado, se individualiza la prueba y se determina la **identidad del autor**. |

FUENTES DE LA INVESTIGACIÓN

# Líneas de investigación

Víctima

## Evidencia que aporta la víctima

- Correos electrónicos, páginas web y chats.
- Extracción forense de sus dispositivos (UFED / Cellebrite Reader) y cálculo de hash del material.

Organismo

## Evidencia que aporta un organismo

- Reportes del **National Center for Missing and Exploited Children** (NCMEC).
- ¿Cómo es un informe? ¿Qué medidas permite tomar?

Fraudes

## Preservaciones en fraudes

- Declaración de personal especializado.
- Resguardo técnico de la evidencia.



03

# Pautas para investigar en entornos digitales

Identificadores, direcciones IP, husos horarios y registros de conexión

EL PRIMER DATO

# ¿Cómo identifico a un usuario?

El nombre visible puede cambiar o repetirse; lo que individualiza la cuenta es su identificador.

## Red social

- La URL del perfil contiene un **ID numérico** único (profile.php?id=...).
- Existen herramientas en línea que permiten obtener ese ID.

## Mensajería y correo

- Distinguir el **nombre visible** del **ID de la cuenta**.
- Ejemplo de ID: live:usuario.

## WhatsApp

- El ID de usuario es el **número telefónico** completo.
- Prefijo internacional (+54), 9, código de área (11) y número de abonado.

CONCEPTOS BÁSICOS

# ¿Qué es una dirección IP?

Es un conjunto de números que identifica, de manera lógica y jerárquica, una conexión a internet.

- La empresa proveedora del servicio de internet (Cablevisión, Telefónica, Telered, Telecentro, Claro, etc.) **asigna a cada cliente una dirección IP** para que tenga conectividad.
- Esa IP puede ser **fija o dinámica**, y **pública o privada**.
- Ejemplo IPv4: **192.168.255.254**
- Ejemplo IPv6: **2001:0db8:85a3:0000:1319:8a2e:0370:7344**

CLASIFICACIÓN

# Tipos de dirección IP

## IP pública

Identifica de forma única una conexión a internet.

## IP privada

Se utiliza exclusivamente en redes de área local; no sale a navegar por internet.

## IP fija o estática

El cliente se conecta siempre con la misma dirección IP.

## IP dinámica

Cada conexión usa una IP distinta. Los proveedores la emplean porque tienen más clientes que direcciones disponibles.

UN OBSTÁCULO FRECUENTE

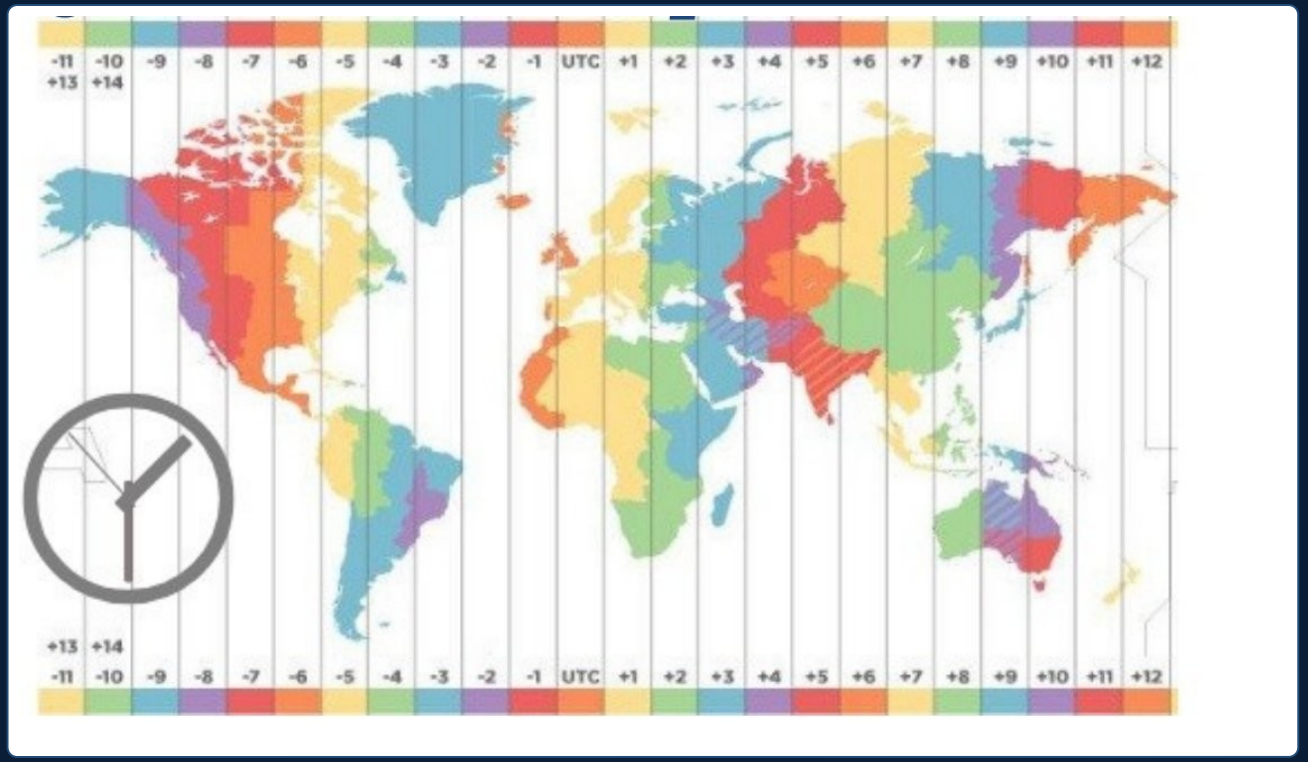
# El nateo de IP

## Una sola IP pública da conectividad a muchos usuarios mediante IP privadas, y las empresas no suelen guardar la asignación histórica

Es la modalidad que usan en gran medida las prestadoras de internet móvil, y no hay normativa que las obligue a conservar esos datos.

CONVERSIÓN HORARIA

# ¿Por qué importa el huso horario?

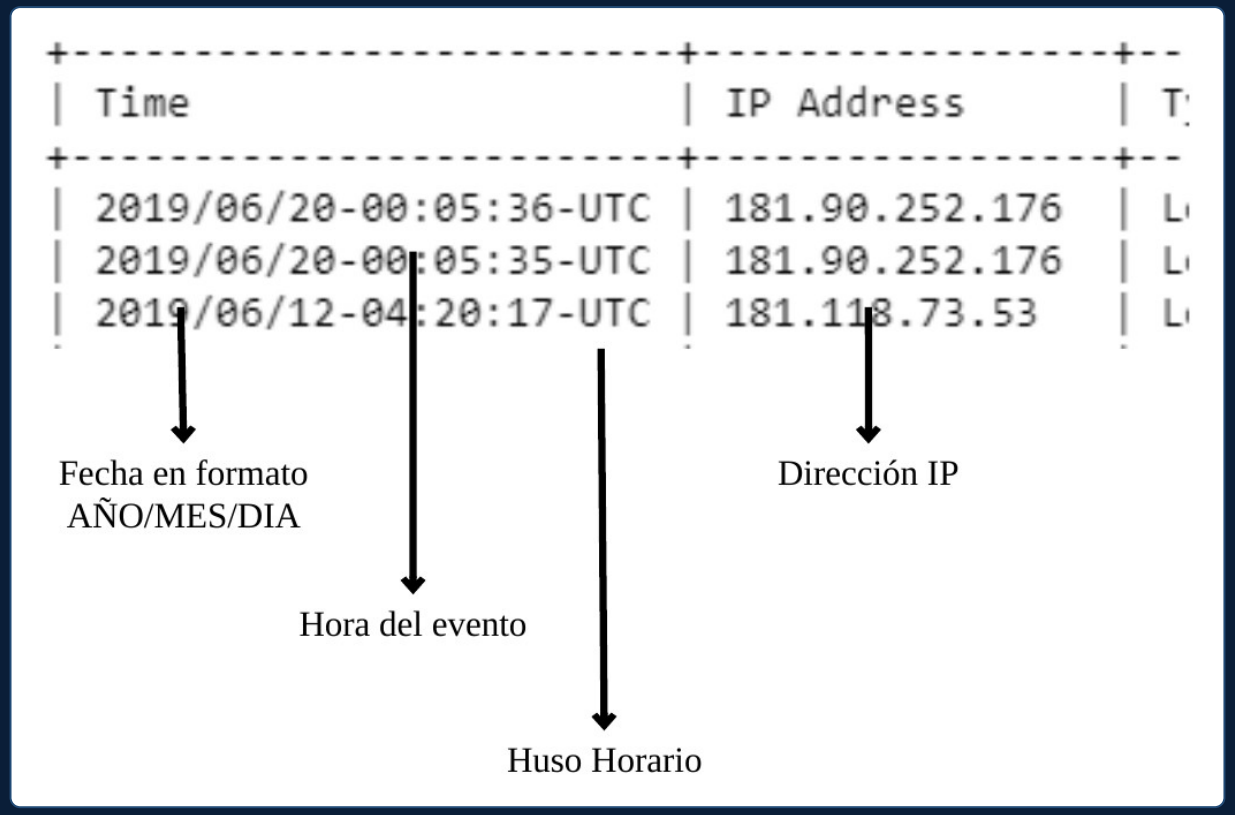



CLAVES

- Las empresas informan los eventos en un huso determinado, en general **UTC**.
- Sin convertirlo a la hora local, la consulta al ISP apunta a otro momento y otro usuario.
- Herramienta de apoyo: **worldtimebuddy.com**.

REGISTRO DE CONEXIÓN

# ¿Qué es un log y cómo se compone?

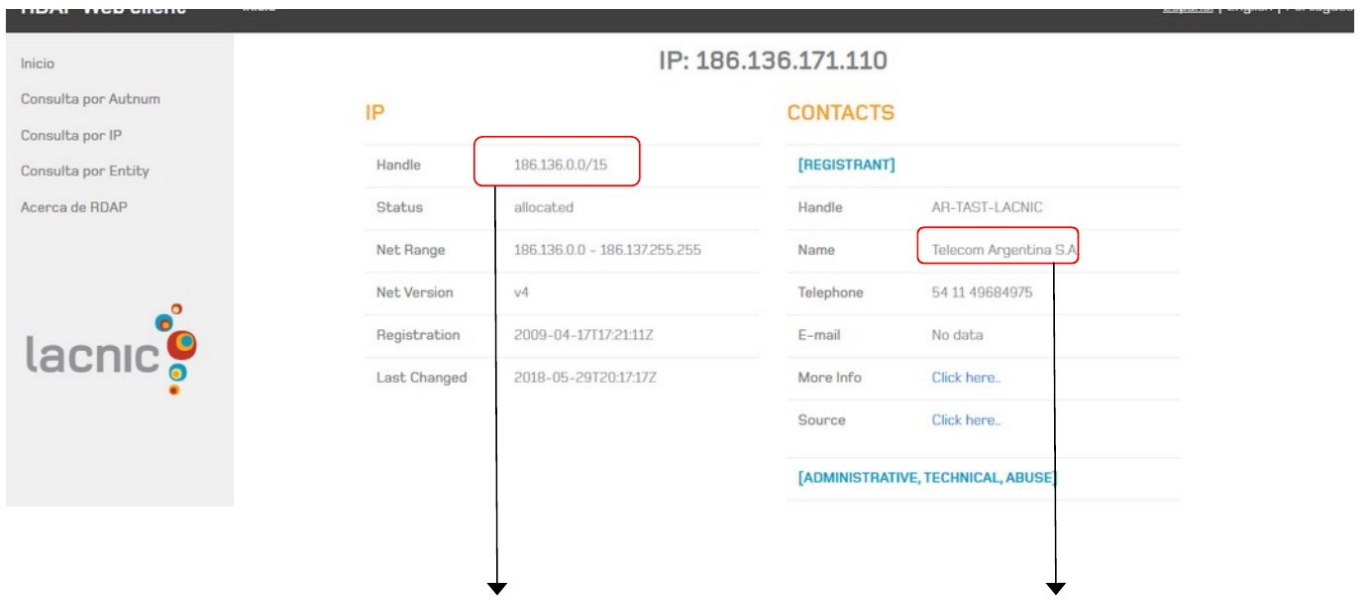



COMPONENTES

- **Fecha** en formato año/mes/día.
- **Hora** del evento.
- **Huso horario** en que se informa.
- **Dirección IP**.
- Es evidencia del comportamiento: permite determinar el sitio y el momento exacto del evento.

CONSULTA DE IP

# ¿Qué empresa administra la IP?




En el panel de búsqueda de se deberá consignar la IP que se desea consultar. Se pueden consultar interfaces del tipo IPv4 o IPv6

El dato de mayor interés en la consulta es la ISP (Internet Service Provider) en donde se consigna qué empresa es la que administra la IP consultada.

CÓMO SE CONSULTA

- En **iplocation.net** o en el cliente RDAP de **LACNIC** se ingresa la IP (IPv4 o IPv6).
- El dato de mayor interés es el **ISP** (Internet Service Provider): la empresa que administra la IP.
- Listado de ISP locales: icannlac.org.



04

# La información en poder de las empresas

Qué guardan los proveedores y cómo se obtiene, en el país y en el extranjero

TRES NIVELES DE INFORMACIÓN

# A mayor intromisión, mayores recaudos

Los recaudos vienen dados por los canales y requisitos que exige cada tipo de información.

| | |
|---|---|
| **Básica o de suscripción** | Nombre, país, dirección, teléfonos, edad, género, fecha de nacimiento, correo o teléfono asociado, tarjeta de crédito, fecha e IP de creación de la cuenta. Se entrega por los **portales para agentes de la ley y fuerzas de seguridad**. |
| **Transaccional** | Remitente y receptor, IP involucradas, días y horas de las comunicaciones, volumen de datos, sitios visitados y **registros de log in y log out**. Requiere **intervención judicial**. |
| **De contenido** | Texto y adjuntos de correos y mensajes, publicaciones restringidas, historial de localización y archivos en la nube. Debe requerirse por **exhorto internacional** (MLAT). |

INFORMACIÓN TRANSACCIONAL

# Cómo se obtiene

## Intervención judicial

- Todo pedido de esta índole debe materializarse con la intervención judicial que garantice los derechos del investigado.
- Las empresas exigen la **firma del juez** del caso.

## Canales

- Algunas empresas reciben el pedido por sus **portales** o por correo electrónico.
- Otras exigen un **exhorto internacional**, con intervención de autoridades judiciales del país extranjero.

MODELO DE PEDIDO

# Solicitud a Meta de registración y logueos

| | |
|---|---|
| **Firma y fecha** | Oficio con **fecha actual**, firmado por el juez. |
| **Sello** | Sello oval, medalla o sello de la dependencia que emite la solicitud. |
| **Destinatario** | Meta Platforms, Inc., 1601 Willow Road, Menlo Park, CA 94025. |
| **Delito** | Descripción o transcripción del **delito investigado**, que permita conocer el objeto de la investigación; puede adjuntarse documentación respaldatoria. |
| **Diligenciamiento** | Aunque lo libra el juez, puede diligenciarlo el propio juzgado, la fiscalía o la fuerza policial interviniente. |

MODELO DE PEDIDO

# Consulta a la ISP

*Que informe a qué usuario de su compañía se hallaba asignada la dirección IP 183.136.171.110 el día 16/06/2016 a las 10:16 hora local, debiendo precisar la fecha de alta y estado actual del servicio del cliente, como así también domicilio de instalación, facturación y datos de contacto del cliente.*

**Ejemplo de requerimiento a la empresa proveedora de internet**

RECAUDOS

- La hora debe estar **convertida al huso local**.
- Una IP sin fecha y hora exactas no identifica a nadie, salvo que sea fija.

ROL DE NAVEGACIÓN

# La secuencia completa del caso

| | | |
|---|---|---|
| 1 | **Identificación de perfiles** | URL, ID y cuentas asociadas del perfil investigado. |
| 2 | **Preservación y conservación** | Preservación de la evidencia de la víctima y conservación de los datos del imputado. |
| 3 | **Solicitud a la empresa** | Registración y logueos del perfil (p. ej., a Meta). |
| 4 | **Rol de navegación** | Con la respuesta: consulta de IP (LACNIC), conversión horaria (worldtimebuddy) e identificación del ISP local. |
| 5 | **Solicitud a la ISP** | Titular, domicilio de instalación y datos de contacto. |
| 6 | **Allanamiento y análisis integral** | Secuestro del material y cruce de toda la información obtenida. |

MEDIDAS URGENTES

# Conservación y casos de emergencia

## Conservación de información

- Procedimiento sencillo de **naturaleza cautelar**, no probatoria.
- Conserva la información **90 días** hasta la petición formal.
- Requiere elementos objetivos que hagan sospechar una actividad ilícita vinculada a esa información, y **peligro en la demora**.

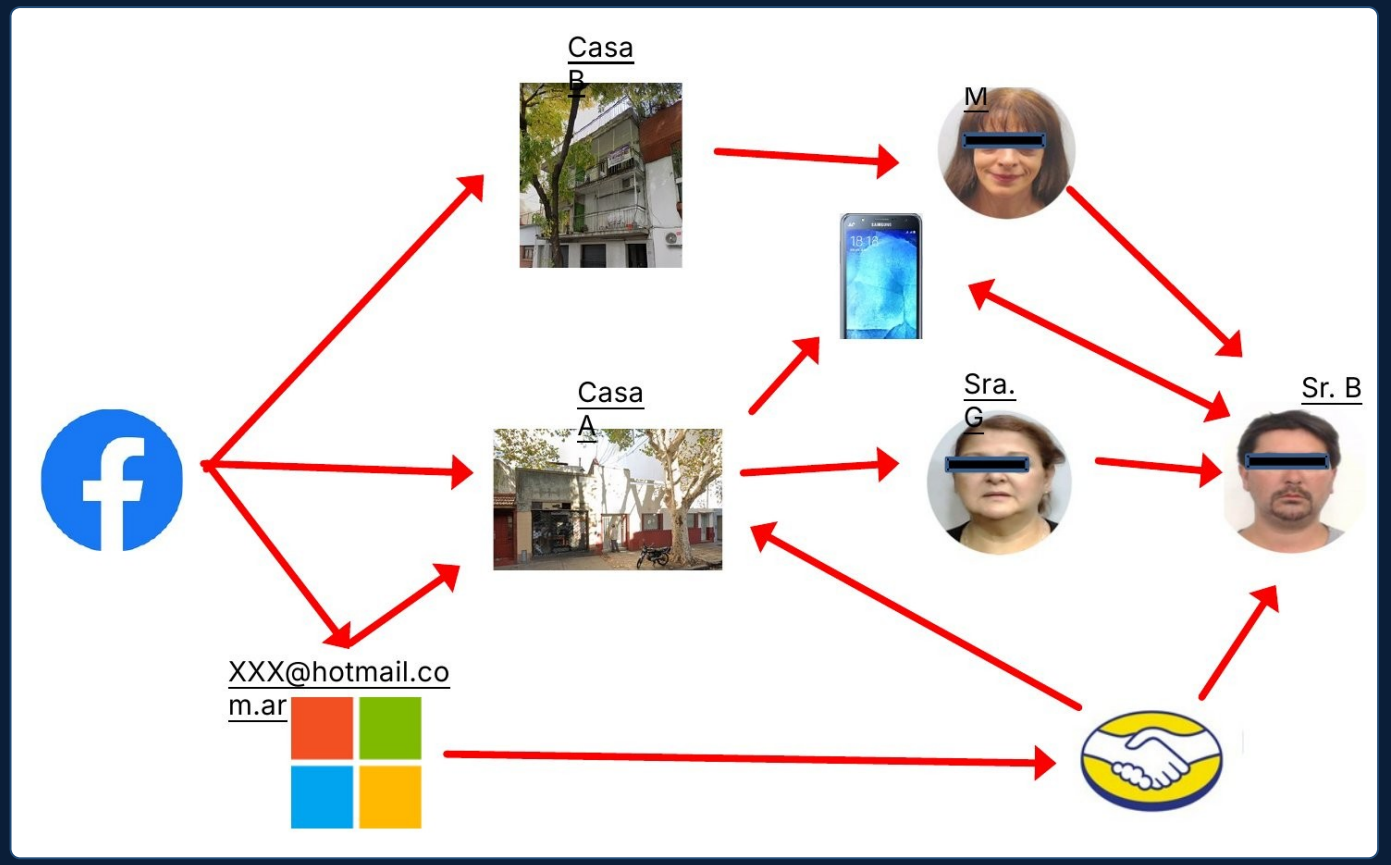
## Casos de emergencia

- Riesgo inmediato de muerte o de seria afectación a la integridad física.
- Las empresas pueden entregar **voluntariamente** información básica, transaccional o de contenido sin exhorto.
- Hay que fundar detalladamente la urgencia; cada empresa tiene canales específicos.

# ¿Cómo se diligencia un exhorto internacional?

| | | |
|---|---|---|
| 1 | **Pedido local** | El fiscal solicita la medida al juez local. |
| 2 | **Traducción** | Obtenido el oficio, se traduce al inglés. |
| 3 | **Cancillería local** | Se diligencia por la cancillería o el ministerio de relaciones exteriores del país oficiante. |
| 4 | **Cancillería extranjera** | Interviene la cancillería del país oficiado. |
| 5 | **Juez extranjero** | Evalúa la viabilidad del pedido y si existe causa razonable. |
| 6 | **Fiscal extranjero** | Interviene para cumplir la medida. |
| 7 | **Empresa prestataria** | Coopera entregando la información requerida. |

# Vincular cuentas, domicilios y personas




QUÉ SE CRUZA

- Los logueos de distintas cuentas (red social, correo, plataformas de pago) conducen a **domicilios**.
- En cada domicilio se identifican **personas y dispositivos**.
- Las **fuentes abiertas** completan el mapa de vínculos antes del allanamiento.

05

# Allanamiento, secuestro y análisis

Llegamos a este punto de la investigación: ¿cómo seguimos?

MEDIDAS POSIBLES

# Las herramientas del momento

### Allanamiento

Físico o remoto.

### Secuestro y análisis

En el laboratorio o en el lugar (triage).

### Requisa

Del imputado y de otros sospechosos.

### Plain view

Hallazgo de evidencia a simple vista durante la medida.

ANTES DE ENTRAR

# ¿Qué es lo que vamos a buscar?

No es lo mismo recolectar evidencia digital que secuestrar prueba física: cambian la incautación, la preservación, el riesgo de alteración y la presentación.

- **Principio de libertad probatoria**: medidas de conservación rápida (*quick freeze*).
- ¿Es admisible la utilización analógica de las normas ya existentes?
- Marco de referencia: **arts. 16 a 21 del Convenio de Budapest**.

PROBLEMAS Y SOLUCIONES

# Cuando los datos no están en el lugar

## Desafíos

- Las órdenes judiciales se limitan a lugares físicos (el hogar del sospechoso).
- Los datos pueden estar en un **servidor externo** al que se accede por internet.
- Almacenamiento en la **nube**.
- Sistemas informáticos en el **extranjero**.
- Comunicaciones anónimas: **TOR** o terminales públicas.

## Soluciones

- Órdenes de registro con **cierta flexibilidad**.
- Ante esas situaciones, los operadores deben poder **extender el registro** a ese sistema.
- Es fundamental poder extenderlo **rápidamente** cuando haya motivos para creer que los datos están en otro sistema.

PEDIDO AL JUEZ

# Allanamiento extensivo a los datos

El fiscal pide al juez el allanamiento y el secuestro del material y la evidencia digital, extensivo a:

### Computadoras

Portátiles o de escritorio.

### Memoria RAM

Solo disponible con el equipo encendido.

### Soportes

Discos, CD, DVD, pendrives, memorias, tablets.

### Celulares

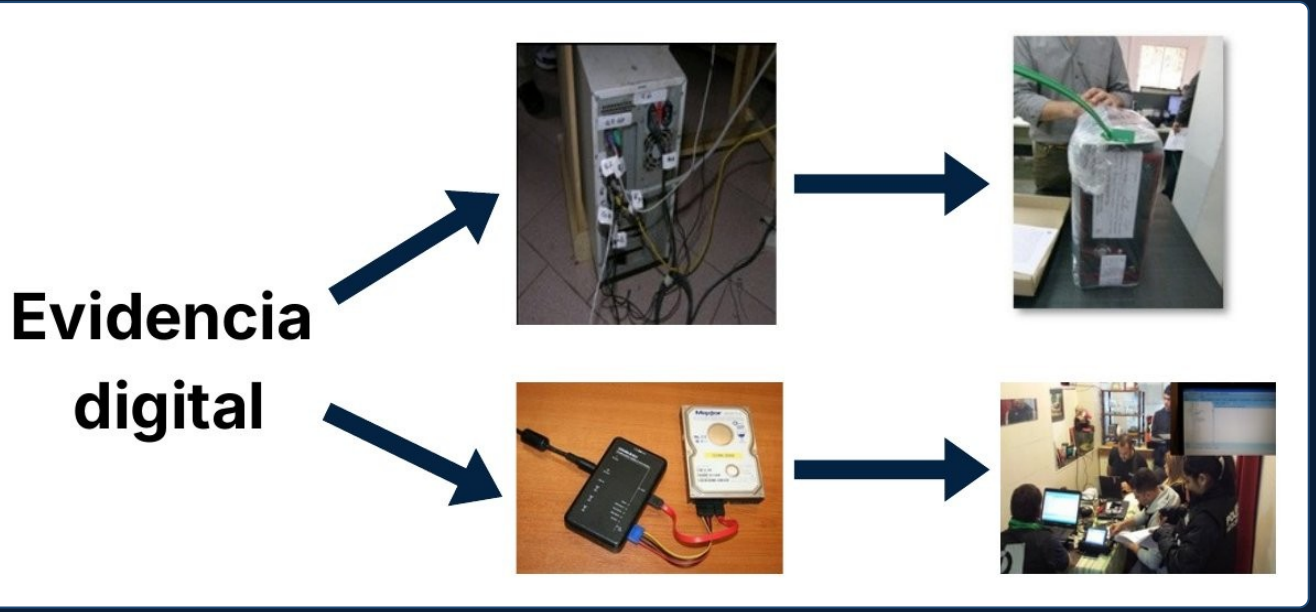
Teléfonos móviles.

### Álbumes de fotos

Archivos fotográficos.

DOS CAMINOS

# Laboratorio o análisis en el lugar (triage)




TRIAGE

- Búsqueda rápida en el lugar: hay que definir **por qué, cuándo y cómo**.
- Interactúa con el dispositivo: no es contaminación, pero debe ser **controlada**.
- El análisis en laboratorio permite la pericia completa.

BUENAS PRÁCTICAS

# Desafíos al tratar la evidencia digital

| | |
|---|---|
| **Copia** | Copia bit a bit con **duplicador forense** o **bloqueador de escritura**. |
| **Software** | Software específico para analizar el material (p. ej., Cellebrite Reader). |
| **Investigación en vivo** | Triage: búsqueda rápida con interacción controlada sobre el dispositivo. |
| **Protocolo** | Protocolo de buenas prácticas en todo el circuito. |
| **Laboratorio** | Pericia conjunta o por separado, tiempos de análisis y **rol de la defensa**. |



06

# Casos de fraude

Tipologías de maniobras: phishing y SIM swap

INFORMACIÓN BANCARIA

# El sistema financiero como fuente

## Tipologías

- **Phishing**: engaño para obtener credenciales de la víctima.
- **SIM swap**: toma de control de la línea telefónica para recibir los códigos de validación.

## Preguntas clave

- ¿Qué entidades conviven hoy en el sistema bancario y financiero?
- ¿Qué información resguardan?
- ¿Qué recaudos exige obtenerla? Ley 21.526 de Entidades Financieras y Comunicación "A" 7711 BCRA (06/03/2023).
- ¿Cuál es la situación en el Poder Judicial de la Ciudad?

CASO REAL, DATOS RESERVADOS

# Mecánica de un SIM swap con fraude

1

## Toma de la línea

Un tercero activa una **SIM nueva** mediante la autogestión de la operadora, en otro equipo (IMEI) y con impacto en una antena identificada.

2

## Acceso al home banking

Con la línea en su poder, recibe los **códigos token** que el banco envía por SMS desde un número corto.

3

## Transferencias

Desde el perfil de la víctima se realizan transferencias a cuentas de terceros.

# ¿Cómo investigarlo?

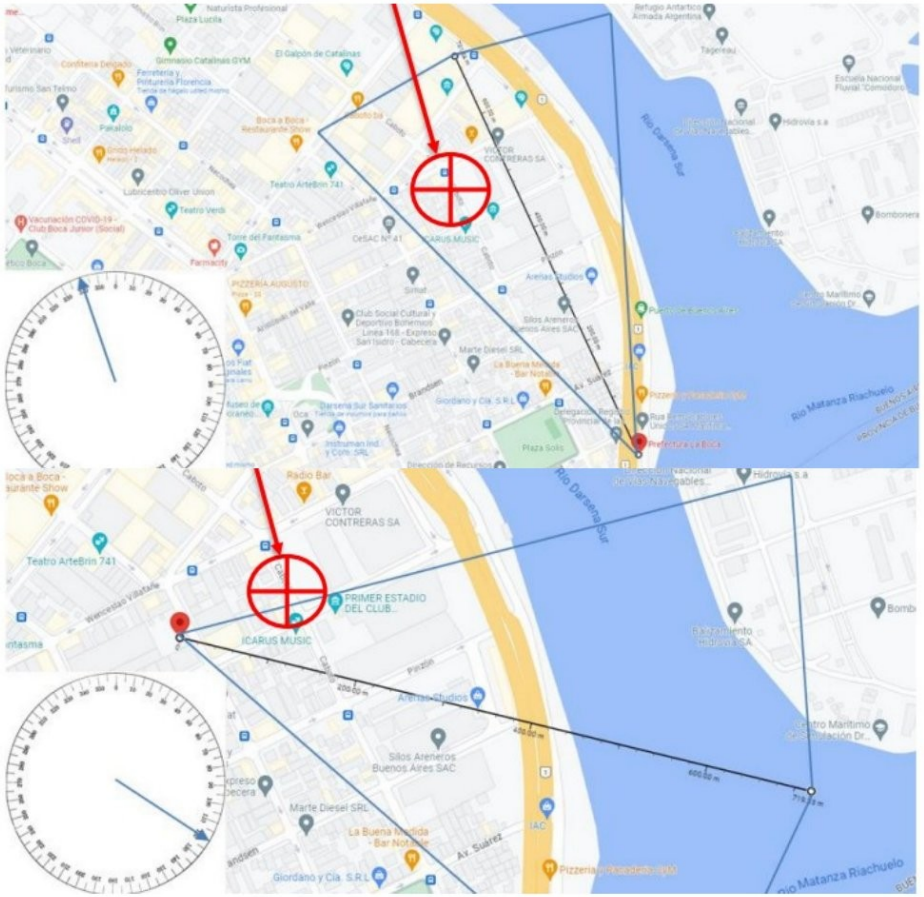



DATOS DE LA OPERADORA

- Momento exacto del cambio de SIM.
- **IMEI** del equipo anterior y del nuevo.
- **Números cortos** desde los que llegaron los SMS.
- **Celdas** (antenas) con impacto de cada equipo.

ANÁLISIS DE CELDAS

# Ubicar el equipo por su antena




DATOS DE CADA ANTENA

- Latitud y longitud.
- Radio de cobertura.
- Azimut.
- Apertura vertical y horizontal.
- Con esos datos se proyecta el sector de cobertura sobre el mapa y se acota la zona donde operaba el equipo.

FUENTES COMPLEMENTARIAS

# Bases para identificar a los responsables

## Registro Nacional de las Personas

Datos de identidad de las personas vinculadas al hecho.

## Bases comerciales

Informes de bases como Nosis o SudamericaData para vincular personas, domicilios y actividad.

## Registros de la operadora

Constancias del proceso de validación de identidad del cliente al gestionar la línea.

# Muchas gracias

Cibercrimen y evidencia digital