- 2024 -

Recomendaciones sobre manejo de prueba digital 1

—

DATIP | Dirección General de Investigaciones y Apoyo Tecnológico a la Investigación Penal

Laboratorios de Informática Forense y Análisis de Telecomunicaciones

MINISTERIO PÚBLICO
FISCAL
PROCURACIÓN GENERAL DE LA NACIÓN
REPÚBLICA ARGENTINA

Recomendaciones sobre manejo de prueba digital 1

Secuestro en “caliente” de dispositivos móviles con el objeto de facilitar el acceso a la prueba digital utilizando herramientas forenses avanzadas en el marco de causas complejas - Laboratorio de Análisis de Telecomunicaciones de la DATIP - Procesos de recolección de prueba digital en el ámbito de la Justicia Penal Nacional y/o Federal Argentina

---

Elaborado por Dra. M. R. Del Buono - Directora General de DATIP
Ing. N.E. Sanguineti - Jefe de los Laboratorios de Informática Forense y Análisis de Telecomunicaciones

Diseño: Dirección de Comunicación Institucional

Publicación: marzo 2024

- 2024 -

Recomendaciones sobre manejo de prueba digital 1

Secuestro en “caliente” de dispositivos móviles con el objeto de facilitar el acceso a la prueba digital utilizando herramientas forenses avanzadas en el marco de causas complejas - Laboratorio de Análisis de Telecomunicaciones de la DATIP - Procesos de recolección de prueba digital en el ámbito de la Justicia Penal Nacional y/o Federal Argentina

—

DATIP | Dirección General de Investigaciones y Apoyo Tecnológico a la Investigación Penal

Laboratorios de Informática Forense y Análisis de Telecomunicaciones

Índice

I. RESUMEN

Los avances tecnológicos de los últimos años han mejorado notablemente las técnicas de cifrado de la información de usuario presente en los dispositivos móviles. Como contrapartida, las herramientas forenses avanzadas utilizadas en los Laboratorios técnicos permiten la aplicación de distintas tácticas con el objetivo de realizar un desbloqueo exitoso o la adquisición parcial o total de la información, siempre y cuando el modelo de dispositivo esté soportado y las condiciones iniciales respecto al cifrado de la información de usuario así lo permita. El desarrollo de esta recomendación tendrá como objetivo describir someramente los dos modos principales en los cuales puede encontrarse un celular al momento del allanamiento, cuya correcta identificación por parte de los primeros intervinientes y/o los operadores judiciales permitirá ganar eficiencia a la hora del intento de desbloqueo o acceso al dispositivo en los procedimientos periciales.

Palabras clave: Extracción forense de dispositivos móviles. *AFU*. *BFU*. *Brute Force*. Peritaje de dispositivos móviles.

Introducción teórica: antes de comenzar con el desarrollo de estas recomendaciones sobre el manejo de prueba digital es importante conocer, al menos someramente, lo relativo a los tipos de encriptación o cifrado que existen hoy en día en nuestros celulares y la variación en función del estado de bloqueo o desbloqueo de los dispositivos móviles.

Básicamente tenemos dos tipos: cifrado basado en archivos (*File base encprytion-FBE*) y cifrado de disco completo (*Full disk encryption-FDE*).

El cifrado de disco completo es el proceso de codificación de todos los datos del usuario en un dispositivo Android mediante una clave cifrada. Una vez que se cifra un dispositivo, todos los datos creados por el usuario se cifran automáticamente antes de enviarlos al disco y todas las lecturas descifran automáticamente los datos antes de devolverlos al proceso de llamada.
El cifrado de disco completo se introdujo en Android en 4.4, pero Android 5.0 introdujo estas nuevas funciones:

- Creó un cifrado rápido, que solo cifra los bloques usados en la partición de datos para evitar que el primer arranque tarde mucho tiempo. Actualmente, solo los sistemas de archivos ext4 y f2fs admiten el cifrado rápido.

- Se agregó el *forceencrypt fstab* para cifrar en el primer arranque.

- Se agregó soporte para patrones y encriptación sin contraseña.

Se agregó almacenamiento respaldado por hardware de la clave de cifrado mediante la capacidad de firma de *Trusted Execution Environment (TEE)* (como en TrustZone).

El cifrado basado en archivos permite cifrar diferentes archivos con diferentes claves que se pueden desbloquear de forma independiente. A su vez, el cifrado basado en archivos habilita una nueva característica introducida en Android 7.0 llamada *Direct Boot* la cual permite que los dispositivos cifrados arranquen directamente en la pantalla de bloqueo. Anteriormente, en dispositivos encriptados que usaban encriptación de disco completo (FDE), los usuarios debían proporcionar credenciales antes de poder acceder a los datos, lo que impedía que el teléfono realizara todas las operaciones excepto las más básicas. Por ejemplo, las alarmas no podían funcionar, los servicios de accesibilidad no estaban disponibles y los teléfonos no podían recibir llamadas, pero estaban limitados a operaciones básicas de marcación de emergencia.

Con la introducción del cifrado basado en archivos (FBE) y las nuevas API para que las aplicaciones reconozcan el cifrado, es posible que estas aplicaciones operen dentro de un contexto limitado. Esto puede ocurrir antes de que los usuarios hayan proporcionado sus credenciales mientras se sigue protegiendo la información privada del usuario.

En un dispositivo habilitado para FBE, cada usuario del dispositivo tiene dos ubicaciones de almacenamiento disponibles para las aplicaciones:

- Almacenamiento de *Credential Encrypted* (CE), que es la ubicación de almacenamiento predeterminada y solo está disponible después de que el usuario haya desbloqueado el dispositivo.

- Almacenamiento de dispositivo cifrado (DE), que es una ubicación de almacenamiento disponible tanto durante el modo de arranque directo como después de que el usuario haya desbloqueado el dispositivo.

Modo BFU (*Before First Unlock*) – Modo "Frío"

Cuando un dispositivo, ya sea con sistema operativo Android como con iOS se reinicia, algunos datos y servicios pueden estar temporalmente inaccesibles o protegidos hasta que el usuario realice un desbloqueo exitoso. Este enfoque ayuda a garantizar que cierta información sensible no esté disponible hasta que se haya autenticado el usuario. Por ejemplo, en caso de tener configurada una contraseña o un patrón de desbloqueo en un dispositivo, ciertos datos pueden estar cifrados y solo serán accesibles después de que el usuario haya ingresado correctamente la contraseña o patrón después de un reinicio y/o un encendido convencional.

Modo AFU (After First Unlock) – Modo "Caliente"

Se refiere al estado en el que ciertos datos y servicios están disponibles después de que el usuario haya desbloqueado el dispositivo por primera vez luego de un reinicio. Una vez que el usuario ha ingresado su contraseña, PIN o patrón de desbloqueo después de un reinicio, se accede a ciertos datos y servicios que estaban protegidos en el estado "*Before First Unlock*" (BFU).

Cuando el dispositivo se reinicia, algunos datos críticos pueden estar cifrados y protegidos hasta que el usuario autentique su identidad. Una vez que se realiza el desbloqueo después del reinicio, el dispositivo pasa al estado "*After First Unlock*", y los datos y servicios asociados están disponibles y se pueden utilizar.

Este enfoque es una medida de seguridad que ayuda a proteger la información sensible en situaciones en las que el dispositivo se encuentra en manos equivocadas. Al requerir la autenticación del usuario después de un reinicio, se asegura de que solo los usuarios autorizados puedan acceder a ciertos datos.

II. RECOMENDACIONES SOBRE EL MANEJO DE PRUEBA DIGITAL

Secuestro de dispositivos móviles para su posterior adquisición forense: Ahora que ya hemos analizado los distintos estados en los que podemos encontrar un dispositivo móvil respecto al cifrado de su información (AFU y/o BFU) pasaremos a describir las operaciones a llevar a cabo en un Laboratorio forense para lograr la adquisición de la prueba digital contenido en los dispositivos y las implicancias, en cuanto a la eficiencia del desbloqueo y/o la adquisición, respecto al estado inicial del dispositivo a peritar (modo "caliente" Vs modo "frío"); será muy relevante a la hora de intentar desbloqueos utilizando herramientas avanzadas como el UFED PREMIUM[1] de la empresa Cellebrite, entre otras.

Secuestro de dispositivo en "Modo Frío/Cold" – FBE/FDE

Un dispositivo se encuentra en este modo si está apagado o si está encendido pero aún no se ha llevado a cabo la autenticación por parte del usuario introduciendo las credenciales correspondientes, como ya fue explicitado en el apartado introductorio. En caso de estar encendido y tratarse de cifrado del tipo FBE podríamos tener imágenes como las que a continuación se observan, donde luego de finalizar el proceso de inicio (*booteo*) el dispositivo queda a la espera de la autenticación, sin brindar acceso a la cámara ni a las operaciones del tipo "llamada de emergencia".

1. Herramienta avanzada para desbloqueo de dispositivos móviles. Adquirida recientemente por parte del MPF (*OC Nº 56-2023*) para ser utilizada junto al resto del equipamiento tecnológico en el Laboratorio de Análisis de Telecomunicaciones de la DATIP.

Fig.1. Modo Cold Samsung

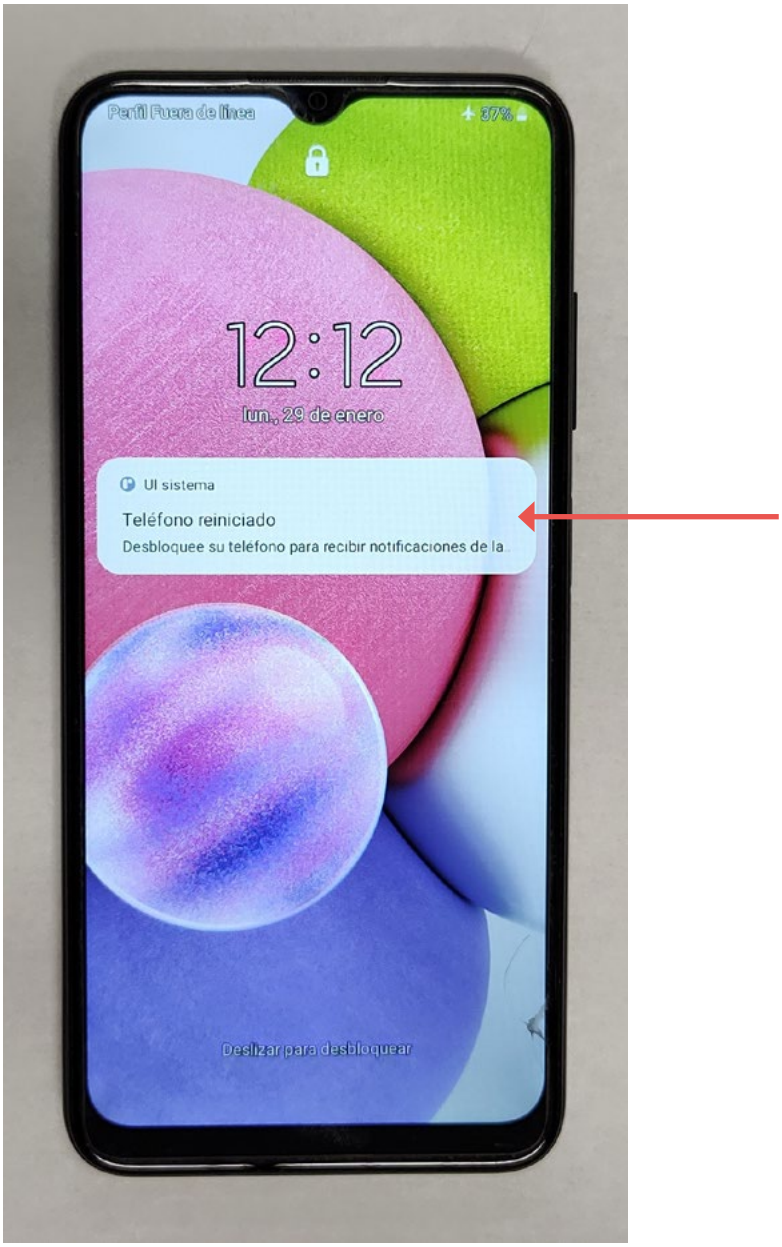

Fig.2. Modo Cold Samsung

Fig. 3. Modo Cold Xiaomi

Para el caso de cifrado del tipo FDE con inicio seguro deberíamos ver, en caso de estar encendido, una pantalla donde se requiera el ingreso de la clave de desbloqueo (en este caso el *booteo* aún no ha finalizado):

Fig. 4

En estos casos, denominados en la práctica forense como "fríos", la única forma de realizar una adquisición de información será a través de mecanismos de fuerza bruta[2] utilizando para ello herramientas específicas o heurísticas propias desarrolladas en el Laboratorio forense con el objeto de

2. Las herramientas comerciales desarrollan distintos *exploits* para intentar obtener ventaja de las distintas vulnerabilidades que existen en los sistemas operativos de dispositivos móviles, logrando en muchas ocasiones la elevación de privilegios o el acceso a zonas no autorizadas dentro de la memoria del dispositivo. En segunda instancia, sobre un universo de dispositivos soportados que varía de versión a versión del software forense, logran ganar permisos para poder llevar a cabo un proceso de prueba y error utilizando combinaciones aleatorias con el objetivo de "descubrir" la clave de bloqueo/cifrado del dispositivo evitando en este proceso la activación de medidas de seguridad defensivas que harían impracticable el ataque (por ejemplo, el *lockout* entre intentos o la activación de factores exponenciales para la reiteración de combinaciones).

obtener, mediante repetición de intentos, la clave, PIN o patrón de bloqueo del dispositivo. Más allá del tiempo que podría llegar a demandar esta técnica, dependiendo en principio de la complejidad de las credenciales del usuario, es importante destacar que no todos los celulares se encontrarán soportados por las herramientas forenses tornando en algunas ocasiones estéril cualquier intento por vulnerar el acceso a la prueba digital.

Respecto al secuestro del PEP digital propiamente dicho en este estado (*frío/cold*) deberá realizarse siguiendo las consideraciones estipuladas en el *Protocolo para la Identificación, Recolección, Preservación, Procesamiento y Presentación de la Evidencia Digital Minseg-MPF 2023*, pero al estar en modo frío no será necesaria su remisión en forma urgente a los laboratorios especializados ni tampoco será necesario (salvo casos excepcionales) proveer alimentación eléctrica al dispositivo para que no pierda su estado de energización, toda vez que la información de usuario se encuentra cifrada, debiendo emplear, como ya se ha dicho, mecanismos de fuerza bruta para intentar la obtención de las claves de bloqueo.

Secuestro de dispositivo en "Modo caliente/Hot" - FBE

Un dispositivo se encuentra en este modo si está encendido y ya se ha realizado la autenticación por parte del usuario introduciendo las credenciales correspondientes, aunque luego proceda a bloquear la pantalla. De esta forma, como ya fue explicitado en el apartado introductorio, la información de usuario permanecerá descifrada (mientras el dispositivo permanezca en este estado *caliente/hot*) y será posible realizar adquisiciones forenses sin necesidad de aplicar técnicas de fuerza bruta, las cuales no suelen estar disponibles para todos los modelos de dispositivos ni aun contando con herramientas especializadas. *Es por ello que la detección de este modo caliente/hot en los dispositivos celulares involucrados en las labores de un allanamiento reviste de vital importancia a la hora de mejorar la eficiencia general de las adquisiciones forenses.* Será determinante el conocimiento por parte de los operadores judiciales para que puedan instruir acabadamente a los primeros intervinientes de las fuerzas de la ley que estén a cargo del allanamiento en cuestión.

En caso de encontrar dispositivos en este modo, el secuestro deberá realizarse siguiendo las consideraciones estipuladas en el *Protocolo para la Identificación, Recolección, Preservación, Procesamiento y Presentación de la Evidencia Digital Minseg-MPF 2023*, intentando en todo momento que el dispositivo sea trasladado a un laboratorio forense especializado completamente aislado de cualquier interacción electromagnética (*modo avión de ser posible/bolsa de Faraday certificada de ser posible/aislación electromagnética mediante múltiples vueltas de papel aluminio o método similar de probada efectividad*) y procurando utilizar los medios idóneos para que no se produzca el apagado del dispositivo por agotamiento de carga; esto produciría la consecuente pérdida del estado *caliente/hot*,

disminuyendo considerablemente las posibilidades de llevar a cabo una adquisición forense exitosa[3]. A continuación se observa una imagen típica de un dispositivo con Sistema Operativo Android el cual se encuentra en modo *caliente/hot*. Podrá observarse que a diferencia del modo *fríо/cold*, aquí se desplegarán las funciones de "llamada de emergencia" y "cámara fotográfica", las cuales se encuentran en la parte inferior de la pantalla del dispositivo.

3. En caso de encontrar el dispositivo al momento del secuestro encendido y desbloqueado, ya sea por la casuística como por una planificación operativa del allanamiento previa con dicho objetivo (fuerzas de la ley y autoridad judicial) será necesario a su vez que el primer interviniente intente, utilizando técnicas conocidas (por ejemplo la ejecución de contenido multimedia), mantener el estado del dispositivo (desbloqueado) para su traslado en forma urgente a un Laboratorio forense, procurando la activación del modo avión y el blindaje del tipo *faraday* de ser posible. Esta tarea debería ser coordinada con los especialistas de los Laboratorios forenses (Por ejemplo con el Laboratorio de Análisis de Telecomunicaciones de la DATIP) para aumentar las posibilidades de éxito, no estando exenta esa tarea de riesgos derivados de las opciones que ofrecen hoy en día los *Smartphone* a sus usuarios con la finalidad de proteger su privacidad, estando disponible la opción de un restablecimiento a fábrica del dispositivo en forma remota; cuestión que será abordada en una próxima recomendación.

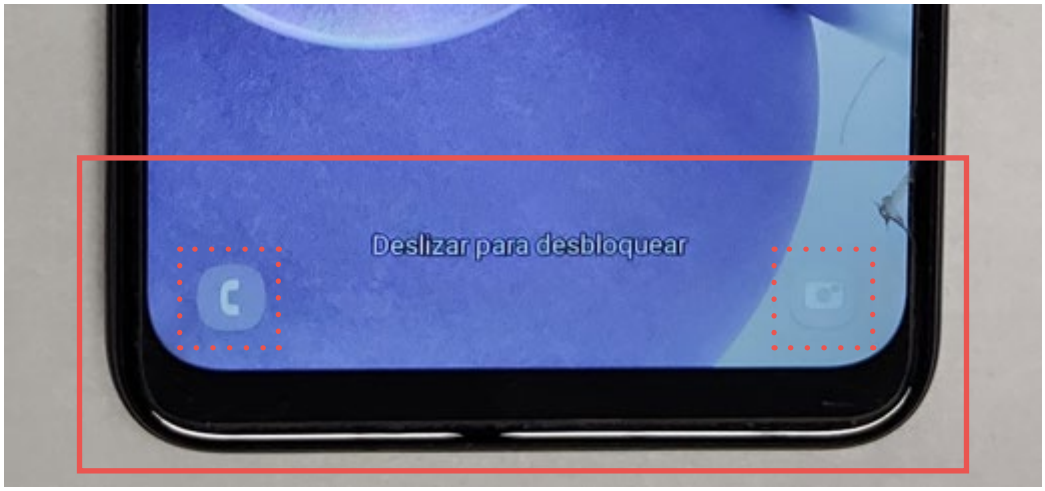

Fig. 5. Modo HOT Samsung

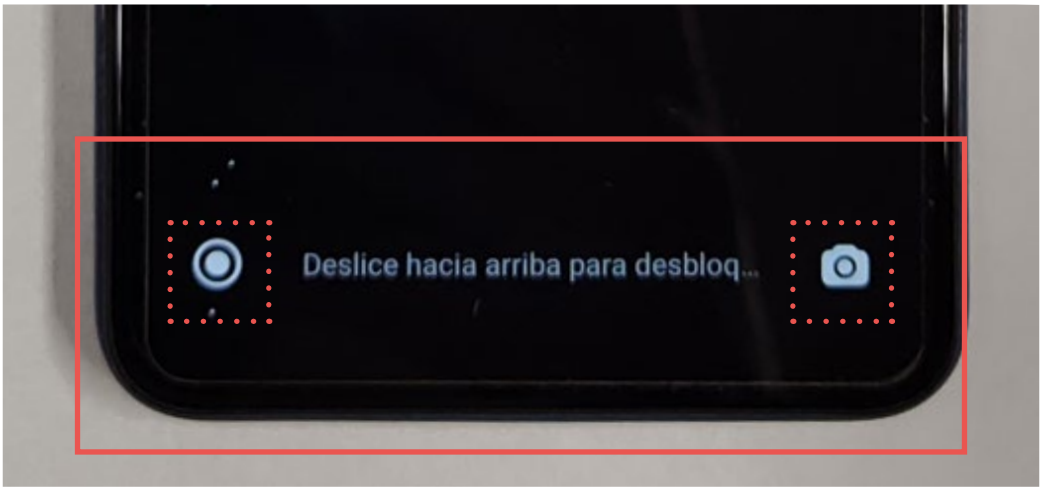

Fig. 6. Modo HOT Xiaomi

III. CONCLUSIÓN

A través del desarrollo de esta recomendación se han explorado algunas particularidades del secuestro de los dispositivos móviles teniendo en cuenta la eficiencia en los peritajes forenses cuando los dispositivos atacados se encuentran en estado caliente, posibilitando de esta forma la obtención de más y mejores resultados en los procedimientos periciales, los cuales redundarán en mejores investigaciones judiciales. El conocimiento por parte de los operadores judiciales de las terminologías, procesos y métodos utilizados en toda la cadena de valor de la informática forense sin lugar a dudas jerarquizarán los procesos investigativos, teniendo esta DATIP y particularmente sus Laboratorios técnicos, como receptores de demandas de todas las jurisdicciones, la obligación de la capacitación permanente a todo el sistema de justicia.

IV. BIBLIOGRAFÍA CONSULTADA

- **[1] IRAM/ISO/IEC 27037 (2018-2022)**
  Guidelines for identification, collection, acquisition and preservation of digital evidence.

- **[2] MPF-MinSeg (2023)**
  Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital.

- **[3] Andrew Hoog (2011)**
  Android Forensics: Investigation, Analysis, and Mobile Security for Google Android

- **[4] Heather Mahalik, Satish Bommisetty, Oleg Skulkin, Rohit Tamma (2018)**
  Practical Mobile Forensics,: A hands-on guide to mastering mobile forensics for the iOS, Android, and the Windows Phone platforms, 3rd Edition

- **[5] Daniela Dupuy, Mariana Kiefer (2017)**
  Cibercrimen. Aspectos de Derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidades de los proveedores de servicios de internet

MINISTERIO PÚBLICO
FISCAL
PROCURACIÓN GENERAL DE LA NACIÓN
REPÚBLICA ARGENTINA

MINISTERIO PÚBLICO
FISCAL
PROCURACIÓN GENERAL DE LA NACIÓN
REPÚBLICA ARGENTINA

MINISTERIO PÚBLICO FISCAL | PROCURACIÓN GENERAL DE LA NACIÓN
Av. de Mayo 760 (C1084AAP) - Ciudad Autónoma de Buenos Aires - Argentina
(54-11) 4338-4300
www.mpf.gob.ar | www.fiscales.gob.ar