- 2025 -

Recomendaciones sobre manejo de prueba digital 2

—

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

Laboratorio Técnico de Informática y Telecomunicaciones

MINISTERIO PÚBLICO
FISCAL
PROCURACIÓN GENERAL DE LA NACIÓN
REPÚBLICA ARGENTINA

Recomendaciones sobre manejo de prueba digital 2

Metodología forense para el análisis de registros en sistema operativo Android con el objeto de determinar posibles eventos de restablecimiento a fábrica ocurridos sobre dispositivos celulares en el marco de procesos de recolección de prueba digital en el ámbito de la Justicia Penal Nacional y/o Federal Argentina

---

Elaborado por la Dra. M. R. Del Buono (Directora General de DATIP) – Ing. N.E. Sanguineti (Jefe de los Laboratorios Técnicos de Informática y Telecomunicaciones) – Lic. L. Cossio (Integrante del Laboratorio Técnico de Informática y Telecomunicaciones)

Diseño: Dirección de Comunicación Institucional

Publicación: febrero 2025

- 2025 -

Recomendaciones sobre manejo de prueba digital 2

Metodología forense para el análisis de registros en sistema operativo Android con el objeto de determinar posibles eventos de restablecimiento a fábrica ocurridos sobre dispositivos celulares en el marco de 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

Laboratorio Técnico de Informática y Telecomunicaciones

Índice

I. RESUMEN | ABSTRACT

En las causas donde se investiga criminalidad compleja es frecuente el secuestro y posterior adquisición, preservación y análisis de distintos tipos de dispositivos móviles, en los cuales subyace información con elevada densidad probatoria que podría resultar crucial para el esclarecimiento de los sucesos delictivos. Es frecuente que la recolección de prueba digital se lleve a cabo en los distintos laboratorios de las fuerzas federales o en la DATIP, utilizando herramientas forenses comerciales y open source con el objeto de posibilitar la concreción de las tareas periciales, adquiriendo y luego procesando la mayor cantidad de información que sea posible extraer de los celulares bajo estudio. Desafortunadamente, en algunas ocasiones, en el transcurso del peritaje pueden ocurrir situaciones que produzcan el deterioro de la prueba digital o incluso su completa supresión. Una de las características destacadas de este tipo de prueba es la facilidad para permear la barrera de la no adulteración, encontrando en los casos de restablecimiento a fábrica de los dispositivos celulares uno de los mayores exponentes de esta particular cualidad, los cuales pueden generar verdaderos inconvenientes en el proceso investigativo.

Haciendo foco en la labor pericial del perito y los profesionales técnicos intervinientes, este trabajo de investigación ensayará algunas técnicas forenses que permitirán analizar algunos logs en un dispositivo con sistema operativo Android para determinar con precisión los motivos del restablecimiento a fábrica, pudiendo encontrar datos adicionales que podrían ser de utilidad para el esclarecimiento de los hechos, ya sea por causales de mala praxis pericial como por intencionalidad manifiesta de los legítimos usuarios en aras de conseguir la eliminación parcial o total de potenciales elementos de prueba.

Palabras clave: Extracción forense de dispositivos móviles. *History Log. Bootloader unlock. Wipe. Factory Reset.*

Introducción y motivación: Antes de comenzar con el desarrollo de esta investigación es importante conocer la estructura de particiones del sistema operativo Android, para pasar luego a centrarnos en las particiones donde se encontrarán los insumos de esta investigación, tanto en */Cache* como en */Data.*

PARTICIONES SISTEMA OPERATIVO ANDROID

Fig.1

Estas particiones son espacios de memoria donde el fabricante gestiona los recursos necesarios para el correcto funcionamiento del dispositivo móvil.

La partición de /boot es la encargada de gestionar el arranque del dispositivo. En ella se encuentra el *kernel y la ramdisk*[1].

La partición */system* contiene los archivos del sistema operativo (archivos instalados por defecto, interfaz gráfica, etc).

La partición de */recovery* es donde se gestiona el menú de recuperación desde donde se puede recuperar el sistema operativo en caso de falla, vaciar la cache[2], realizar un *wipe* data o supresión de los datos existentes en la partición /data donde se almacenan los datos de usuario, reiniciar el cargador de arranque, entre otras cosas.

La partición */data* contiene todos los datos de usuario (información personal, aplicaciones instaladas, etc). Si el dispositivo se restaura de fábrica toda la información de usuario aquí contenida será sanitizada.[3]

La partición de */cache* es un espacio de memoria donde se almacenan los datos que son accedidos con frecuencia, tanto por parte de los usuarios como por parte del sistema operativo. En esta partición se encuentran algunos registros de operaciones realizadas en modo *recovery.*

Finalmente, la partición */misc* es donde se almacenan ajustes de hardware del dispositivo.

El presente trabajo de investigación estará centrado en el análisis de distintos registros obtenidos mediante una adquisición forense del sistema de archivos para intentar determinar las causales de los restablecimientos a fábrica en dispositivos celulares.

II. RECOMENDACIONES SOBRE EL MANEJO DE PRUEBA DIGITAL

Finalizada la introducción teórica y la motivación de la presente recomendación, pasaremos a analizar la metodología de extracción forense que esta DATIP puede recomendar a los operadores judiciales,

1. El *kernel* es el corazón del sistema operativo. Se encarga de gestionar y conceder el acceso al hardware a medida que el software lo solicita. Por otro lado la ramdisk es una memoria virtual donde se ejecutan algunos procesos de arranque cuando el dispositivo está booteando.

2. Hemos demostrado que las acciones *wipe cache* no eliminan registros del tipo *history* donde se almacena información correspondiente a eventos del modo *recovery*.

3. En un próximo trabajo de investigación se analizará la eficacia de los métodos de borrado sobre la información de usuario implementados en las distintas versiones de Android.

utilizando herramientas comerciales[4] y open source[5], para aplicarse al tratamiento de la prueba digital sobre dispositivos móviles en los cuales se tiene certeza que han ocurrido eventos disruptivos como restablecimientos a fábrica, desconociendo a *prima facie* los motivos que desencadenaron el *factory reset* con la consiguiente pérdida de información de usuario que podría contener alto valor probatorio. Esta metodología podrá ser utilizada en investigaciones penales donde los operadores judiciales requieran conocer con exactitud los factores que podrían haber generado este desenlace y el momento exacto de manifestación del suceso, siendo vinculante no sólo para el caso de supresión voluntaria de información en dispositivos móviles previo al secuestro (acto intencional) sino también para la comprensión cabal de posibles errores o dificultades que podrían manifestarse en un peritaje a razón de múltiples factores, entre los que se destacan una incorrecta manipulación dentro del modo de recuperación y/o el modo descarga con el *bootloader* desbloqueado.

A continuación, se muestra una imagen ilustrativa del alcance del presente trabajo de investigación:

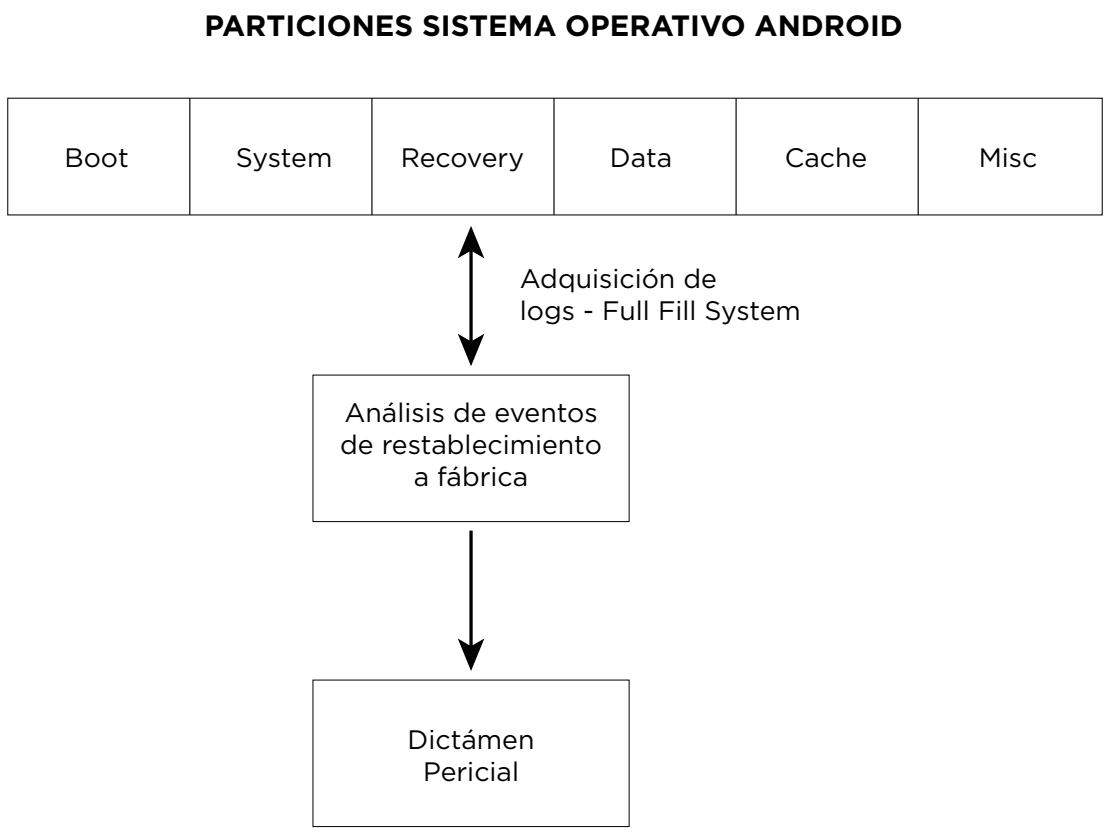

Fig.2

4. UFED/INSEYETS/GRAY KEY de las empresas Cellebrite y Magnet Forensic.
5. Tsurugui Linux. Comandos ADB desde shell

III. ANALÍSIS DE LA METODOLOGÍA RECOMENDADA MEDIANTE ENSAYO DE LABORATORIO

Serán utilizados los siguientes dispositivos, provistos por el Laboratorio Técnico de Telecomunicaciones de la DATIP – MPF para llevar adelante las pruebas de concepto.

1) Celular SAMSUNG SM - A50 con Android 11 inicialmente
2) Celular SAMSUNG S8 con Android 10 inicialmente
3) Celular SAMSUNG SM-G532M con Android 9

Las pruebas de concepto tendrán 3 (etapas) que serán aplicadas sobre cada dispositivo repitiendo los mismos pasos. En primer término, se procederá, luego de energizar los celulares, a ingresar al modo de recuperación aplicando la combinación de teclas adecuada[6] al inicio del proceso de *booteo.* Seguidamente se aplicará un *wipe data/factory reset* desde la consola del modo de recuperación, como se ilustra en la siguiente imagen.

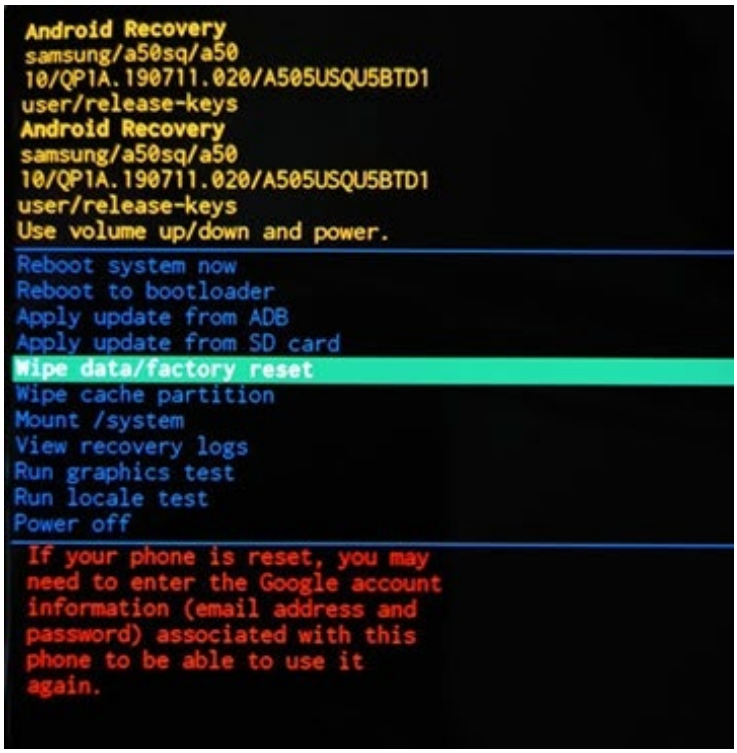

Fig.3

6. Describir combinación de teclas

Para el presente desarrollo no se configurarán previamente los dispositivos con credenciales de Google (cuenta de Gmail asociada), evitando la activación del *factory reset protection (FRP)* cuando se procede al restablecimiento de fábrica. Esta medida de protección que impide la reutilización del dispositivo (a menos que se aplique un procedimiento técnico para conseguir el *unlock* del FRP) será analizada en una próxima recomendación.

En segundo término, se procederá a colocar los dispositivos en *modo desarrollador*[7] para operativizar la función de *desbloqueo OEM.* Esta operación, una vez que está activada permite desbloquear la protección de fábrica generada por el fabricante para evitar la instalación de firmware no oficial, como podrían ser ROMs personalizadas. Estas prácticas usuales permiten personalizar el dispositivo, modificando las particiones y los parámetros de configuración entre otras acciones.

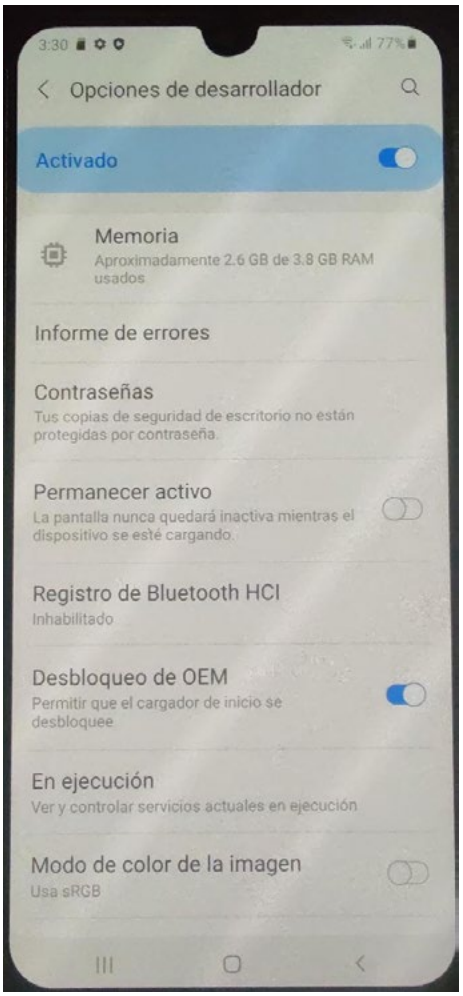

Fig.4

7. El modo desarrollador es un modo especial dentro del sistema operativo que permite realizar configuraciones avanzadas.

Con el desbloqueo OEM activado es posible, ahora sí, proseguir con la prueba de concepto. Seguidamente se reiniciarán los dispositivos ingresando luego al *modo descarga*[8]. Se observará la siguiente pantalla, en donde tenemos visiblemente dos opciones principales. Presionando *"volume up"* podremos intentar instalar un sistema operativo customizado, por fuera del soporte del fabricante. Para llevar a cabo esta operación deberemos previamente desbloquear el bootloader para poder tener acceso a la partición del sistema. Por otro lado, presionando y manteniendo *"volume up"* el sistema procederá a desbloquear el bootloader, quedando de esta forma en un estado de vulnerabilidad respecto a las condiciones endógenas con las cuales el dispositivo salió de fábrica. El desbloqueo del bootloader es el paso inicial para luego poder acceder a las distintas particiones, la del sistema en caso de querer instalar un sistema operativo nuevo o la partición de *recovery* en caso de requerir la instalación de un gestor de recuperación alternativo como puede ser TWRP.

Una vez iniciada la secuencia correspondiente al desbloqueo del bootloader, el dispositivo inmediatamente después inicia un proceso de *factory reset* como medida de protección de los datos de usuario, desencadenando de esta forma un evento de supresión de la información de usuario que pudiera estar almacenada en el teléfono, juntos a las aplicaciones instaladas y sus bases de datos asociadas.

8. El modo descarga permite actualizar el firmware del sistema

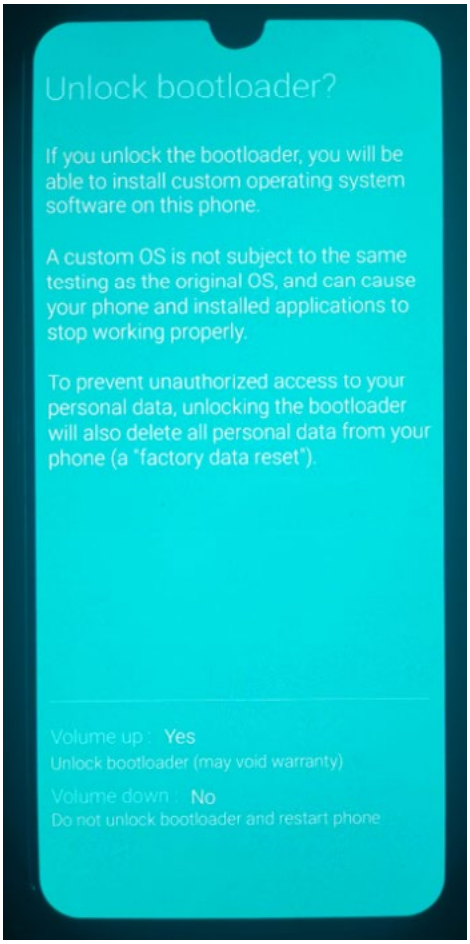

Fig.5

Hasta aquí hemos aplicado **dos procesos distintos** que implicaron el reseteo a fábrica del dispositivo. Continuando con la prueba de concepto y el ensayo de Laboratorio para comprender los alcances de esta recomendación, en tercer término, restará iniciar los dispositivos (ya en modo fábrica) y comenzar con el proceso de adquisición forense con alguna herramienta comercial como INSEYETS de *Cellebrite.* Se realizarán extracciones del tipo full file system y/o física en caso de ser posible, necesarias para poder recolectar las particiones donde se alojan los logs que motivaron el presente trabajo. Una vez finalizadas las extracciones se procederá a decodificar la información obtenida con el software *Physical Analyzer* de la misma empresa, el cual **nos permitirá acceder a los *logs* de los eventos de recovery,** registrados tanto en la partición /Cache como en la partición */Efs*[9]. Comencemos aquí un análisis detallado, con el objeto de intentar correlacionar los eventos de restablecimiento a fábrica producidos intencionalmente en este ensayo de Laboratorio y las sentencias que a continuación se detallarán en las imágenes subsiguientes. **Una vinculación positiva entre eventos *"factory reset – impacto en log del recovery"* nos permitirá delimitar la metodología de la presente recomendación,** materializando un

9. Esta partición contiene información relevante del S.O como número IMEI, configuraciones de red, registros de hardware, etc.

aspecto principal de las motivaciones que dieron origen a la investigación y sintetizando un *framework* adecuado para que los operadores Judiciales puedan aplicar en casos concretos, con el objetivo de obtener al menos los motivos y marco temporal de este evento disruptivo de la prueba digital.

Análisis del *recovery.log*

Como ya fue explicado en la introducción, en este log se registran las operaciones principales del modo de recuperación, entre las que se destacan las operaciones de la partición propiamente, el *flasheo* de la ROM, y como se puede observar aquí, los eventos de restablecimiento a fábrica denominados *"wiping data"* ejecutados manualmente desde la consola de recuperación.

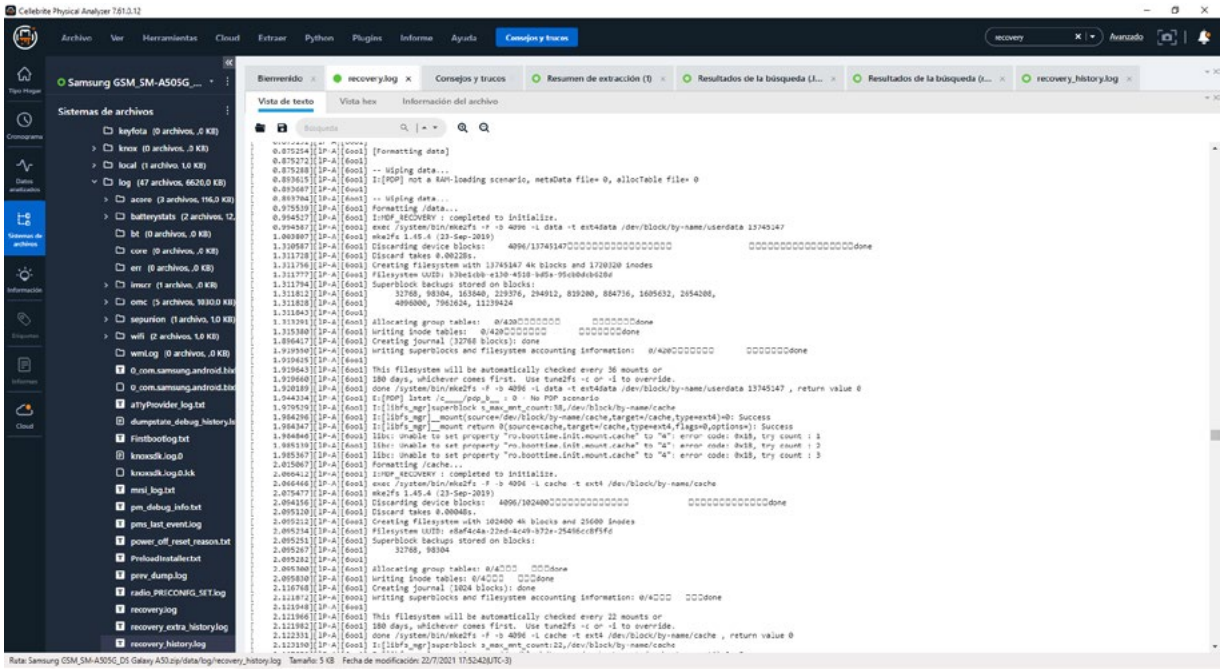

Fig.6

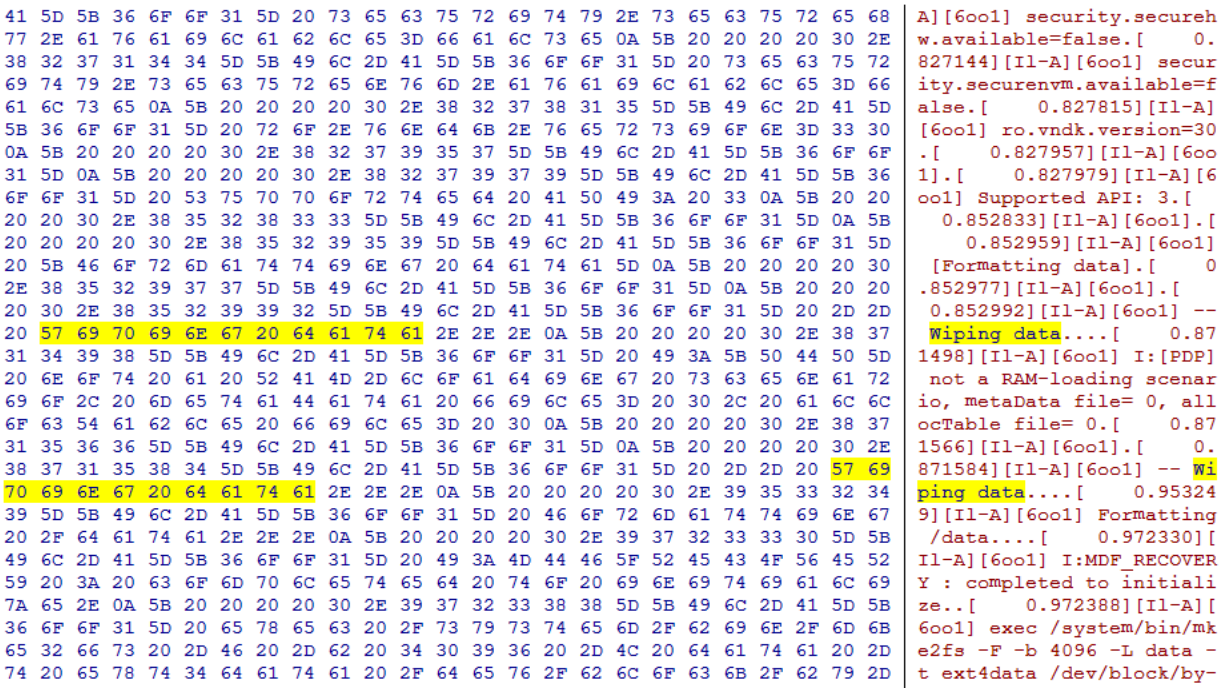

Fig.7

La ruta en donde se encuentra el log es la siguiente:

/data/log/

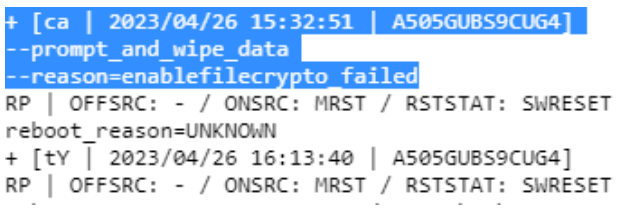

Fig.8

Análisis del *last_history.log*

Este otro registro almacena un histórico de las operaciones realizadas en el modo de recuperación. Un análisis detallado desde la consola del Physical Analyzer, ya sea desde vista en modo texto como hexadecimal **permite encontrar la sentencia que estábamos buscando,** siendo esta la conexión entre los eventos de *factory reset* causados por un desbloqueo del bootloader y su manifestación a través del log histórico.

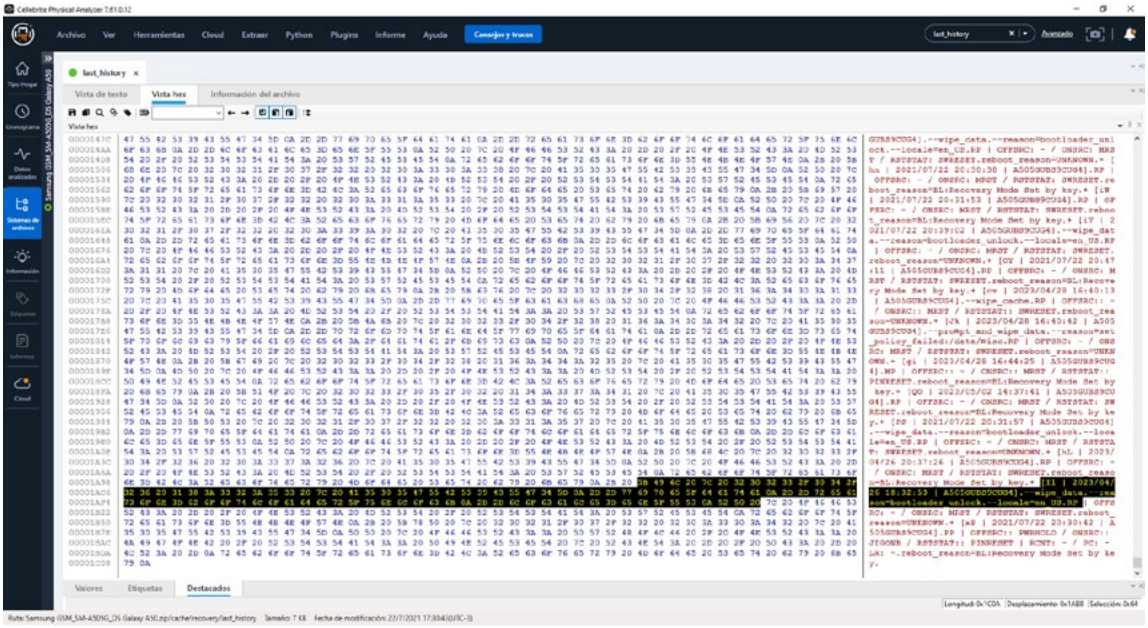

Fig.9

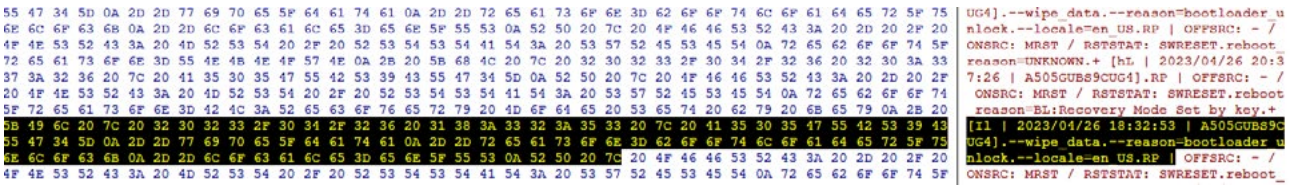

Fig.10

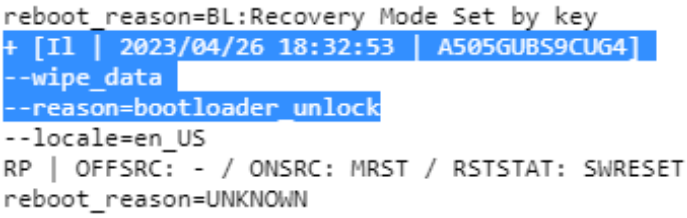

Fig.11

En las capturas anteriores (Fig.9, 10 y 11) se puede observar que para el día 26/04/2023, en el cual se llevaron a cabo las pruebas de concepto y ensayos de Laboratorio, existe un evento ***"wipe_data"*** con una leyenda que indica ***"reason = bootloader_unlock"*** quedando determinado expresamente el suceso de supresión de información de usuario motivado por un intento de desbloqueo del gestor de arranque. Este evento puede manifestarse en la vida del dispositivo por manejo del propio usuario intentando customizar su dispositivo (explorando el log se podría reconstruir la historia de las restauraciones a fábrica debido a desbloqueo o bloqueo del bootloader) o en las actuaciones procedimentales y

periciales en el marco de la investigación de un suceso delictivo. Ningún procedimiento pericial está exento de este tipo de situaciones en donde la meta final suele ser es la adquisición completa de todo el espacio de memoria del dispositivo electrónico; los obstáculos se encuentran diseminados en cada paso de la pericia, estando en conflicto permanente el modelo de seguridad implementado por el fabricante del móvil para asegurar la privacidad del usuario y las tácticas empleadas por los cuerpos periciales en combinación con la tecnología para lograr acceder al contenido digital con valor probatorio, vulnerando y esquivando cuanta medida de seguridad sea capaz de franquear. Esta dialéctica de la informática forense a veces genera una síntesis donde los resultados no son los esperados. Por eso creemos en la importancia de comprender los motivos técnicos que podrían desencadenar estos eventos de restauración a fábrica y sobre todo, que nuestros operadores judiciales tengan los conceptos básicos que les permitan derivar este tipo de situaciones a nuestro Laboratorio especializado.

IV. CONCLUSIÓN

A través del desarrollo de esta **Recomendación de manejo de Prueba Digital** fue posible explicar una metodología técnica que permite adquirir y luego analizar algunos de los logs más importantes del modo de recuperación. Generando las pruebas de concepto óptimas fue posible reconstruir mediante el análisis del *last_history.log* y el *recovery.log,* cada evento de *factory reset,* entendiendo además los motivos subyacentes para el desencadenamiento de estos sucesos, describiendo con claridad los dos tipos más frecuentes en Android; el desbloqueo del bootloader desde el modo descarga y el *wiping* data disparado manualmente desde la consola del modo de recuperación. **La comprensión cabal de estos fenómenos dotará de una herramienta adicional a todas las Fiscalías Nacionales y Federales para poder abordar junto a la DATIP aquellas situaciones de restauración a fábrica de dispositivos celulares, ya sea por eventos anteriores a la recolección de los potenciales elementos de prueba como ulteriores, incluso aunque esta problemática se manifieste durante el transcurso de un peritaje, pudiendo con esta metodología aquí desarrollada desentrañar y luego dictaminar acerca de lo ocurrido; ayudando de esta forma al conocimiento y comprensión precisa de estos eventos brindando mayores certidumbres a nuestros representantes fiscales y sus hipótesis acusatorias.**

Quedará para una próxima recomendación un análisis exhaustivo del resto de los registros del modo de recuperación, como *last_log* y *last_kmsg*, que podrían entregar información adicional sobre las interacciones de reinicio y algunos impactos en el kernel del sistema operativo, siendo también vinculante con lo aquí desarrollado un desarrollo similar para el caso de dispositivos iOS.

V. BIBLIOGRAFÍA CONSULTADA

[1] Rajaram, M. N, & Subhash, K. R., & Mayashankar, P. H. (2022).
Exploration of Android Data Recovery. IJCRT, Volume 10, Issue 4, ISSN: 2320-2882. Department of Information Technology, Pillai College of Engineering, Navi Mumbai.

[2] Simon, L. & Anderson, R. (2018).
Security Analysis of Android Factory Resets. University of Cambridge.

[3] Khramova, M., & Martinez, S. (2021).
Analysis of data remanence after factory reset, and sophisticated attacks on memory chips. Blancco Technology Group.

[4] Schwamm, R. (2014).
Effects of the factory reset on mobile devices. Journal of digital forensics, security and law, vol. 9, no. 2, pp. 20-220.

[5] Hoog, A. (2011).
Android Forensics. Investigation, Analysis and Mobile Security for Google Android. EEUU: Syngress.

[6] Byrd, B., & Zhou, B., & Liu, Q.(2017).
Android System Partition to Traffic Data. International Journal of Knowledge Engineering, Vol. 3, No. 2.

[7] Makalik, H., Tamma, R., & Skulkin, O. (2019).
Practical Mobile Forensics. Forensically Investigate and analyze iOS, Android and Windows devices. EEUU: Packt.

[8] Sanderson,P., Zimmerman, E., & Makalik, H. (2018).
Sqlite Forensics. EEUU.

[9] Chukwuemeka, B., & Onyemaechi, O. (2017).
Performance of Android Forensics Data Recovery Tools. En Contemporary Digital Forensic Investigations Of Cloud And Mobile Applications (pp.91-110). United Kingdom: Elsevier.

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

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

[12] Hikmatyar, G., & Sugiantoro, B. (2018).
Digital Forensic Analysis on Android Smartphones for Handling Cybercrime Cases. International Journal on Informatics for Development, Vol. 7, pp. 19-22.

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