Capítulo 8

Dispositivo Móvil- Forense

Introducción

*Andrés Hrenak*

[*https://www.canva.com/design/DAGDYB7nqYw/pcsbLcNrJupLFmNoGLL2fQ/edit*](https://www.canva.com/design/DAGDYB7nqYw/pcsbLcNrJupLFmNoGLL2fQ/edit)

*Modelp Canvas*

## CONTENIDO

[Introducción](#_bookmark30)  [292](#_bookmark30)

[Computadora forense versus móvil dispositivo forense 292](#_bookmark31)

[Móviles dispositivos 292](#_bookmark32)

[Móvil dispositivo endurecimiento 292](#_bookmark33)

[Móviles dispositivos: a ojeada dentro 293](#_bookmark34)

[Personal computadora forense vs móvil dispositivo forense 293](#_bookmark35)

[Ahora para el último diferencia. Él ¡Depende! 294](#_bookmark36)

[El móvil dispositivo: operando especificaciones 295](#_bookmark38)

[Móvil dispositivo datos recuperación y análisis 297](#_bookmark40)

[Móvil dispositivo forense suites 299](#_bookmark41)

[El móvil dispositivo forense proceso 300](#_bookmark42)

[Aprovechar el móvil dispositivo 301](#_bookmark44)

[Seguro el móvil dispositivo 302](#_bookmark45)

[Identificar el dispositivo 303](#_bookmark46)

[Datos recuperación 304](#_bookmark47)

[JTAG 305](#_bookmark50)

[Accediendo móvil dispositivo memoria 306](#_bookmark52)

[En Sistema Programación (ISP) 308](#_bookmark57)

[donde esta mi ¿datos? 311](#_bookmark66)

[Chip apagado 311](#_bookmark67)

[NI destello memoria 312](#_bookmark68)

[NAND destello memoria 312](#_bookmark69)

[Chip apagado – Calor fluir técnica 314](#_bookmark72)

[Chip apagado – Mecánico técnica 315](#_bookmark73)

[Análisis 315](#_bookmark74)

[Caso ejemplo 317](#_bookmark76)

[Usuario atribución 317](#_bookmark77)

[SQLite bases de datos 318](#_bookmark78)

[Informes](#_bookmark81)  [320](#_bookmark81)

[Resumen](#_bookmark82)  [320](#_bookmark82)

[Acrónimos](#_bookmark83)  [320](#_bookmark83)

[Notas](#_bookmark84)  [322](#_bookmark84)

291

## [INTRODUCCIÓN](#_bookmark0)

**Forense de Computadora versus forense de dispositivo móvil.**

En el curso de mis investigaciones, a menudo se plantea la comparación entre el procesamiento forense informático y el de dispositivos móviles. Obviamente, la arquitectura de hardware del procesamiento forense informático es la principal diferencia entre ambos. Por lo general, los ordenadores se han diseñado para un servicio prolongado, y la memoria interna es sustituible. La disposición de una unidad de disco duro intercambiable o de una unidad de estado sólido dentro del chasis del ordenador ofrece la posibilidad de seguir un proceso forense fiable y coherente.

1. Documente el hardware mediante fotografías,
2. Extraiga la memoria secundaria,
3. Evite la alteración de la memoria mediante el uso de un dispositivo de bloqueo de escritura.
4. Cree la imagen forense.
5. Una vez completados los esfuerzos de verificación y validación, introduzca la imagen forense en la herramienta forense de su elección y ¡encuentre pruebas! Bastante sencillo, ¿verdad?

La estandarización de las conexiones de datos y alimentación ofrece al examinador la posibilidad de establecer una conexión física con el soporte a través de cualquier cable o conector que se utilice.

Posteriormente, el proceso de obtención de imágenes es relativamente benigno y se consigue el acceso a los datos almacenados.

Sin embargo, el modelo descrito depende de la ausencia o presencia de cifrado.

Una vez encontrado, el cifrado crea una serie de pasos alternativos al proceso.

Teniendo en cuenta que éste no es el capítulo dedicado a la informática forense, concluiremos con la descripción del procesamiento informático en este punto.

## [DISPOSITIVOS](#_bookmark2) MOVILES

En comparación, los dispositivos móviles son casi tan diferentes como sus propietarios. Los factores de forma pueden ser el de una barra, un bloque o un estilo flip open. El teclado y los botones de control básicos son botones físicos o representaciones virtuales dentro de la pantalla digitalizadora.

El puerto de datos estará basado en serie, pero es de muchas configuraciones. USB A, B o C, o alguna combinación patentada de los mismos; como lo demuestra el primer conector de datos de treinta pines de Apple y el actual cable Lightning.

Históricamente, el puerto de datos se ha dejado "abierto" para la alimentación y la conectividad de datos, lo que resulta en un punto de acceso bastante fácil en el sistema operativo (OS).

Dependiendo del sistema operativo, se podía acceder a los datos almacenados en el dispositivo a través del puerto de datos.

La tendencia a poner énfasis en la seguridad de la información personal ha cambiado el "fácil acceso a los datos que, como examinadores forenses, disfrutábamos anteriormente.

# Endurecimiento del Dispositivo Movil.

Pero, ¿por qué no eliminar la memoria del dispositivo móvil como en los ordenadores personales? Pues bien,

1. la arquitectura de hardware de los dispositivos móviles es muy distinta a la de los ordenadores tradicionales. Los dispositivos móviles se fabrican para resistir el maltrato del usuario y, por tanto, son resistentes.
2. La presencia de precintos, cinta adhesiva, clips y tornillos crea una especie de carrera de obstáculos para acceder al interior del dispositivo.
3. Una vez dentro, la placa controladora impresa (PCB) lleva soldados diversos componentes montados en superficie, cada uno de ellos con una finalidad distinta y siguiendo la regla de la economía de espacio.
4. A medida que mejoran los procesos de fabricación, el tamaño del hardware es cada vez menor. A medida que disminuye el tamaño, aumenta la dificultad para identificar los dispositivos montados en superficie (SMD) y la accesibilidad a los mismos.
5. A diferencia de la mayoría de los ordenadores, el módulo de memoria de un dispositivo móvil está soldado a la placa de circuito impreso. Esto requiere técnicas especializadas para retirarlo sin causar daños y posibles pérdidas de datos.
6. Por no hablar del variado número de adaptadores que hay que utilizar para facilitar la conexión con el módulo de memoria tras su extracción de la PCB.
7. Existen factores adicionales relativos a extracción del módulo de memoria que se abordarán más adelante en esta sección. Pero por ahora, entienda que no es deseable separar el módulo de memoria de la PCB.

Eso nos deja con el acceso al puerto de datos. Como se ha indicado, el sistema operativo y la arquitectura de seguridad que residen en el dispositivo móvil pueden obstruir la transferencia de datos en el puerto de datos.

Esto requiere que el examinador conozca las características de seguridad por defecto de los distintos sistemas operativos, así como los matices de cada versión del sistema operativo.

Una vez identificadas las características de seguridad, se requieren rutas para eludir las características habilitadas para establecer la conexión y el acceso a los datos almacenados.

# [Dispositivos Móviles: Una ojeada adentro](#_bookmark4)

Además de las funciones de seguridad basadas en el sistema operativo, los fabricantes utilizan ahora hardware que incorpora varios niveles de seguridad.

Cada modelo de dispositivo suele tener una unidad central de procesamiento (CPU) y un módulo de memoria diferentes. A menos que el examinador se encuentre con un dispositivo móvil de modelo básico, los datos pueden almacenarse en un formato cifrado mientras están en reposo.

Los datos pueden cifrarse utilizando el cifrado de disco completo (FDE), el cifrado de volumen completo (FVE) o el cifrado basado en archivos (FBE).

Así, sin conocer la clave de cifrado, que suele basarse en el código de acceso, los datos se recuperan en un formato cifrado. Si esto ocurriera, el intento de recuperar los datos descifrados podría llevar mucho tiempo y esfuerzo.

Baste decir que conocer el código de acceso es un elemento esencial en la investigación forense moderna de dispositivos móviles.

Históricamente, el examen de los ordenadores personales también requería que el examinador conociera la comunicación basada en la red. Más estratégicamente, para garantizar que los datos contenidos en la memoria del ordenador personal permanecían en su estado actual.

En la mayoría de las instalaciones de red, podemos aislar el ordenador personal desconectando el cable de red. Si se conecta a una red inalámbrica, puede haber un interruptor físico en el chasis del ordenador para desconectarlo. O se debe interactuar con el ordenador personal y desactivar el WiFi a través de los ajustes de configuración.

## 

## El aislamiento también es un elemento a tener en cuenta en la investigación forense de dispositivos móviles.

## La propia naturaleza del funcionamiento de los dispositivos móviles consiste en mantener una conexión continua con la red de servicios, un punto de conexión inalámbrica y dispositivos Bluetooth según las preferencias del usuario.

## Este funcionamiento da como resultado una memoria que está en un estado de cambio, casi continuamente. Desde una perspectiva forense, esto no es deseable.

## Los datos entrantes pueden sobrescribir información previamente asignada, pero ya no deseada. En algunos casos, esta información puede estar marcada para ser "borrada" por el usuario y ser crítica para la investigación. Aunque estén marcados para ser borrados, los datos pueden seguir siendo recuperables a menos que se sobrescriban.

## Por lo tanto, el cumplimiento estricto del aislamiento de radio es fundamental para preservar los datos almacenados. Esto puede lograrse a través de diversos mecanismos, como una caja de atenuación, la retirada del Módulo de Identificación del Suscriptor (SIM) o la activación del "Modo Avión". Los mecanismos enumerados se han presentado en orden de mayor a menor aislamiento fiable.

**DIFERENCIA ENTRE EL ANÁLISIS FORENSE DE ORDENADORES PERSONALES Y EL DE DISPOSITIVOS MÓVILES**

Una diferencia inmediata que se observa entre el análisis forense de ordenadores personales y el de dispositivos móviles es la forma en que se almacenan los datos generados por el usuario.

Por definición, los sistemas de archivos almacenan los datos de forma jerárquica para facilitar el almacenamiento y la recuperación de datos para la interacción del usuario. Teniendo en cuenta los distintos fabricantes de dispositivos móviles, los formatos de los sistemas de archivos asociados a los ordenadores personales son muy distintos a los de los dispositivos moviles.

Sí, los datos se almacenan de forma fiable y son totalmente accesibles para el usuario. Simplemente se almacenan en una combinación de archivos y aplicaciones o Apps. Las aplicaciones se componen de bases de datos, diversos archivos de apoyo y listas de preferencias (.plist), o archivos de lenguaje de marcado extensible (.xml)

La presencia de bases de datos en las aplicaciones requiere que el examinador forense tenga capacidad para interrogar bases de datos. Este conjunto de habilidades permite al examinador localizar y extraer la información pertinente de la base de datos cuando la herramienta elegida simplemente no es compatible con esa aplicación concreta. Esta habilidad es aún más importante dado el creciente número de aplicaciones que se ponen a disposición de los usuarios finales cada día.

Tanto los ordenadores personales como los dispositivos móviles dependen de las redes para la comunicación y la transferencia de datos. Ambos pueden utilizar servicios basados en la nube para el almacenamiento de datos, el correo electrónico y la funcionalidad de aplicaciones de terceros.

Sin embargo, es con el uso de dispositivos móviles cuando la globalización de datos se convierte en un área de recursos de investigación para el examinador forense. Las personas, los usuarios finales, quieren que sus datos sean accesibles en todos sus dispositivos autenticados. Por ejemplo, una presentación informativa elaborada con su ordenador personal en el trabajo se "comparte" a través de servicios en la nube.

Esto permite al usuario final viajar "ligero de equipaje" y seguir teniendo acceso a su información en el lugar físico de la presentación, siempre que el lugar sea accesible por WiFi o servicio celular.

A continuación, se accede a través de su dispositivo móvil y se baja para completar la presentación.

Otro ejemplo es la fotografía tomada durante las vacaciones que se publica en el servicio en la nube del usuario y se comparte entre los dispositivos móviles asociados a la cuenta principal, o a otras personas con acceso a la cuenta.

El predominio de este tipo de intercambio y almacenamiento de datos requiere que el examinador considere no sólo lo que está presente, sino también lo que no está presente en el dispositivo móvil.

A continuación, debe considerar por qué los datos no están presentes y cómo documentarlos desde la ubicación en la que están almacenados, que está más allá del propio dispositivo móvil.

**[Ahora para el último diferencia.](#_bookmark6) *[Él ¡Depende!](#_bookmark6)***

Según un estudio de investigación de Pew sobre el uso de dispositivos móviles, realizado en junio de 2019. Aproximadamente el 96% de los adultos en Estados Unidos posee un dispositivo móvil.1

Esto permite un número significativo de dispositivos móviles de diversos fabricantes, varios sistemas operativos y subversiones.

De gran importancia es la presencia de aplicaciones de terceros en el dispositivo móvil que atienden a las preferencias del propietario del dispositivo.

Esto es en comparación con las aplicaciones de línea base dentro de un ordenador personal basado en Windows, Mac o Linux.

Si se añade un paquete de ofimática u otra utilidad para facilitar la tabulación de datos, la edición de texto y la edición de imágenes, los archivos se almacenan como archivos.

En cambio, un dispositivo móvil almacena la información generada por el usuario como archivos, en tablas de bases de datos y como BLOB (Binary Large Objects) dentro de la base de datos. La información relevante puede encontrarse en archivos generados por el sistema, previamente identificados como archivos de preferencias PLIST o XML

En mi experiencia, no he encontrado dos dispositivos móviles definidos como "teléfonos inteligentes" que contengan el mismo número y tipo de aplicaciones para satisfacer las necesidades del usuario. Esto es especialmente cierto cuando un usuario posee y utiliza varios dispositivos móviles; uno para uso personal y otro para uso laboral. Comparativamente, he encontrado ordenadores personales con perfiles similares que comparten exactamente el mismo software.

Recapitulando, las principales diferencias entre los exámenes forenses de ordenadores personales y los de dispositivos móviles son:

* Factor de forma
* Memoria
* Cifrado
* Aislamiento
* Almacenamiento de datos
* Globalización de datos

## [DISPOSITIVO MOVIL: ESPECIFICACIONES](#_bookmark7) DE OPERACION

Hay muchas compañías que producen dispositivos móviles , la siguiente lista present a unos pocos.

* Alcatel
* Apple
* Blackberry
* CoolPad (Jeyung)
* Google
* Huawei
* Kyocera
* Motorola
* nokia
* One
* Samsung

Cada uno de los fabricantes suministra hardware de dispositivos móviles a los distintos proveedores de servicios del mundo.

Para que se entienda mejor, en adelante hablaremos de las principales formas de modulación de frecuencia que se utilizan en Estados Unidos.

Se trata del **Acceso Múltiple por División de Código (CDMA**) **y el Sistema Global de Comunicaciones Móviles (GSM)**

**El Acceso Múltiple por División de Código,** **o CDMA,**

Facilita la comunicación a través de un único canal, por múltiples dispositivos móviles simultáneamente. Mediante el uso de códigos de identificación asignados, los mensajes se transmiten simultáneamente. La presencia del código único garantiza que el mensaje sea recibido por el destinatario previsto. Este método de comunicación se basa en la tecnología de espectro ensanchado para transmitir y recibir mensajes a través de un único canal.

En el momento de redactar esta información, los principales proveedores de servicios de Estados Unidos que utilizan CDMA son:

* Sprint
* Verizon
* US Celular

**Sistema Global de Comunicaciones Móviles (GSM)**

**GSM** utiliza la modulación de frecuencia basada en el tiempo para transmitir y recibir mensajes. Conocido como acceso múltiple por división de tiempo, o **TDMA**, ofrece a varios usuarios la posibilidad de transmitir mensajes a través de un único canal. A cada usuario se le asigna una franja horaria específica dentro del canal para enviar y recibir mensajes.

Además de TDMA, la infraestructura de una red GSM permite transferir mensajes de forma precisa y confidencial. Esto se facilita mediante una clave de autenticación. La clave de autenticación actúa como una clave precompartida reconocida por la infraestructura de la red. Tras la autenticación, se facilita la mensajería. La clave reside en el módulo de identificación del abonado (SIM) situado en el chasis del dispositivo móvil.

Los principales proveedores de servicios de Estados Unidos que utilizan GSM son:

* AT&T
* T-Mobile

Los dispositivos móviles que admiten la transferencia de datos a través del servicio de red celular emplearán una SIM a efectos de autenticación. La presencia de la SIM no define necesariamente el tipo de frecuencia, CDMA o GSM, en uso. Esto se debe a que las tarjetas SIM están presentes en cualquier dispositivo que utilice el estándar Long-Term Evolution (LTE) para la comunicación inalámbrica de banda ancha.

**En cambio, el proveedor de servicios específico** se define a través del Identificador de Tarjeta de Circuito Integrado o **ICCID.** Este código se compone de una serie de números de entre 19 y 20 caracteres de longitud. El ICCID tiene un formato definido que identifica las siguientes características:

* Major industry identifier
* Country code or ‘CC’
* Issuer Identifier or ‘II’
* Account Identifier or ‘SIM Number’

Todo de esta información es presentado en un formato lineal representado como ##### #### #### ##### # #

o como MMCC III# #### #### ##C X

(El '#' simboliza el del usuario único cuenta identificación)

Más definido como:

**Industria Identificador (\*2), País Código (\*2), Editor Identificador (x3), Cuenta IDENTIFICACIÓN (\*11), Suma de comprobación (\*1), X**

O comúnmente visto en un AT&T ICCID como ser:

**8901 410# #### #### ##4 X**

En este ejemplo, "89" representa el identificador del sector asociado a las comunicaciones móviles.

El "01" representa el código de país de Estados Unidos.

A continuación, aparece el identificador de emisor de AT&T "410".

Los dígitos restantes representan el código de identificación de cuenta único para el usuario y la suma de comprobación calculada.

En los Estados Unidos se proporciona como referencia la siguiente lista de operadores y sus respectivos códigos de identificación de emisor.

* AT&T: 030, 150, 170, 410, 560, 680
* Verizon: 004, 005, 012, 480
* T-Mobile: 026, 160, 260, 490
* Sprint: 120

Las tarjetas SIM vienen en varios tamaños. Estas especificaciones se recogen en la Tabla 8.1.

Además de las tarjetas SIM extraíbles, cada vez son más los fabricantes que incluyen la **SIM integrada o eSIM** en el proceso de fabricación.

Esta tecnología permite al usuario final disponer de múltiples servicios de operador en el mismo dispositivo móvil, sin necesidad de cambiar la SIM física. Esencialmente, la eSIM se asignaría a la cuenta principal y una SIM física secundaria soportaría una cuenta secundaria.

*Mesa 8.1* SIM tarjeta tamaños y especificaciones

|  |  |  |  |
| --- | --- | --- | --- |
| *Forma factor* | *Altura* | *Ancho* | *Profundidad* |
| **Estándar** | 3,37 ″ | 2,12 ″ | .029 ″ |
| **Mini** | 0.984 ″ | 0.590 ″ | .029 ″ |
| **Micro** | 0.590 ″ | 0.472 ″ | .029 ″ |
| **nano** | 0.484 ″ | 0.346 ″ | .029 ″ |

* Esto permite al usuario final cambiar entre los dos servicios dentro de la interfaz gráfica de usuario (GUI).
* La eSIM también admite el aprovisionamiento en línea. Esta función facilita un proceso de fabricación más coherente y permite al usuario final utilizar el dispositivo en más de una red.
* Elimina la necesidad de "desbloquear" un dispositivo provisto para una red de operador antes de migrar a otra red de operador.

Otra ventaja de la eSIM es su relación con el Internet de las Cosas (IoT). Dado que la tecnología eSIM está integrada en la placa de circuito impreso, puede implantarse en dispositivos IoT portátiles, lo que permite globalizar el intercambio de datos para mayor beneficio del usuario final. Para más información sobre este tema, véase el capítulo 2, IoT y el papel de la ciber ciencia forense, de Patrick Wilds.

El conocimiento de los principios básicos de las redes celulares, así como de los fundamentos de la modulación de frecuencia utilizada, aumenta la eficacia de la investigación de un dispositivo móvil. Sin embargo, la información relativa a la funcionalidad específica y las características de seguridad de las operaciones de red CDMA o GSM es bastante profunda. Es importante conocer esta amplitud de conocimientos si uno se dedicara a la práctica "legal" de interceptar comunicaciones en directo. Esta práctica va mucho más allá de este debate, por lo que continuaremos con el propio dispositivo móvil.

Un dispositivo móvil puede compararse con un automóvil. Ambos son utilizados a diario por los consumidores y necesitan energía y una red para cumplir su función. Más concretamente, ambos necesitan energía eléctrica y las redes WiFi y de telefonía móvil utilizadas para la comunicación son similares a las carreteras o autopistas que facilitan la circulación de los vehículos.

## [RECUPERACIÓN Y ANÁLISIS](#_bookmark8) DE DATOS DE DISPOSITIVO MÓVIL

El análisis forense de dispositivos móviles es más parecido a tener un buen taller de reparación de vehículos en el barrio que un centro de servicio de un concesionario.

El taller del barrio está atendido por un mecánico relativamente amable, algo gruñón, aunque ocupado, que escucha la descripción del problema, identifica la causa, repara el problema y ofrece información preventiva. El taller está limpio, pero es un lugar de trabajo con piezas aquí y allá y un poco de polvo en un rincón. También tiene herramientas, y me refiero a muchas herramientas, herramientas viejas, herramientas nuevas, así como herramientas construidas para una tarea de reparación específica. El mecánico sabe lo que hace falta para mantener su automóvil.

En comparación, el centro de servicio está impoluto, con suelos limpios y pintados y una sala de espera con un camarero. Usted entra en el centro de servicio, se acerca al asesor de servicio y le explica su problema. A continuación, le separan de su vehículo y éste se dirige a algún lugar dentro del centro de servicio, supuestamente a un técnico de servicio. Un tiempo después, su coche reaparece y el asesor de servicio le informa de que el problema se ha solucionado, le entrega una factura en la que se indica la sustitución de una pieza y le indica que pague en la caja. Después de salir del concesionario y recorrer unos cincuenta kilómetros, el testigo de revisión del motor vuelve a encenderse. Tras volver al concesionario, se entera de que el técnico ha utilizado una pieza de recambio con un firmware incorrecto.

La analogía de los dos centros de reparación se hizo, en parte en broma, para ilustrar la diferencia entre ser un examinador centrado en las herramientas, o "técnico de servicio", y un examinador forense agnóstico en cuanto a las herramientas, también conocido como "mecánico".

El análisis forense de dispositivos móviles requiere que el examinador domine la recuperación de datos, el análisis de datos y la elaboración de informes. Cada área tiene su propia profundidad de conocimiento que debe buscarse individualmente para ser plenamente realizada e implementada.

Desde mi primer examen de dispositivos móviles en 2006, ha habido una explosión en las capacidades de las "suites forenses móviles". Estas suites ofrecen funciones similares a las de sus homólogas para ordenadores personales, como XWays, AccessData's Forensic Tool Kit, Autopsy y Forensic Explorer, por citar algunas. Su capacidad para analizar los distintos tipos de datos y su posterior clasificación en categorías de uso ha supuesto un ahorro de tiempo inestimable.

En cuanto a la gestión del tiempo, aprovechan al máximo el tiempo del examinador, liberándole del análisis sintáctico rutinario. Lo ideal es que la fase de procesamiento se lleve a cabo mientras el empleado no está en el trabajo, lo que facilita la revisión de los datos a su regreso. Mediante el desarrollo de un flujo de trabajo, se pueden procesar múltiples dispositivos móviles de forma eficiente, proporcionando información procesable a quienes la buscan. En los casos que lo merecen, la suite forense móvil permite disponer de más tiempo para profundizar en los artefactos directamente relevantes para el caso.

Por desgracia, los puntos fuertes de la suite forense móvil tienen algunas consecuencias. La confianza no verificada en una suite forense puede resultar en una vergüenza profesional, como se describe a continuación.

Si recuerdan, anteriormente señalé información relativa a la interrogación de bases de datos y su importancia en el almacenamiento de información generada por el usuario. También mencioné el creciente número de aplicaciones de terceros utilizadas para mejorar la experiencia del usuario. Pues bien, hace unos años las suites forenses comerciales se vieron envueltas en una carrera. En ese momento, las aplicaciones de terceros estaban irrumpiendo en el campo de las aplicaciones, cada una con porciones individualizadas de codificación. Por lo tanto, las secuencias de comandos de las suites forenses utilizadas para analizar los datos de las aplicaciones necesitaban asignar la aplicación individual debido a las variables existentes en el desarrollo de las aplicaciones. Con las actualizaciones de las aplicaciones se producían alteraciones en la base de datos.

Si el script de análisis no se actualizaba del mismo modo, los resultados de dicho script dejaban de ser fiables en cierta medida. Por lo tanto, el examinador tuvo que identificar un método fiable para revelar los datos de la aplicación no mapeada anteriormente. O bien, indicar que los datos no estaban presentes, ya que la suite forense móvil no los revelaba.

Para contrarrestar esta queja de los examinadores, las distintas empresas lanzaron actualizaciones de versiones a un ritmo cada vez mayor. No para corregir errores o añadir dispositivos compatibles. Sino para mejorar la compatibilidad de las aplicaciones. El mercado de las suites forenses para móviles se convirtió en una carrera a pie para determinar qué suite forense para móviles tenía la mayor compatibilidad con aplicaciones. Una vez liberado, la carrera a pie comenzaba de nuevo hasta la siguiente versión importante del software.

A los examinadores forenses se les enseña a validar y verificar. Los examinadores que no establecieron una práctica de validación de versiones se vieron expuestos a situaciones embarazosas. En un ejemplo, una suite forense para móviles envió una actualización que no descodificaba correctamente las marcas de tiempo de las aplicaciones nativas dentro de una versión específica del sistema operativo. Esto dio lugar a un error de descodificación en los metadatos del archivo. En los casos en los que la referencia cronológica era relevante, este defecto creaba un informe erróneo no intencionado de los hechos. Algo que un fiscal no suele aceptar de buen grado. Sin embargo, gracias a los procesos de validación, los problemas de codificación se detectaron y solucionaron rápidamente.

No malinterpreten mi mensaje. Las suites forenses para dispositivos móviles son imprescindibles. Si tu tienda/laboratorio puede permitirse tener suites forenses para dispositivos móviles de varios proveedores, estoy totalmente a favor. Estos activos se pueden aprovechar entre sí para agilizar el proceso de validación de versiones, así como para soportar el procesamiento múltiple de dispositivos móviles de forma simultánea. Obviamente, esta sugerencia tiene sus costes.

Estos incluyen la cuota de adquisición inicial, la cuota anual de soporte, así como la formación centrada en la herramienta necesaria para operar el conjunto de herramientas forenses a un nivel óptimo de competencia. Costoso sí, pero el rendimiento de la inversión (ROI), dependiendo de su modelo de negocio, puede justificarlo.

Como alternativa, su taller o laboratorio puede emplear a "mecánicos" altamente cualificados que puedan analizar los datos mediante secuencias de comandos y validar las herramientas tallándolas a la antigua usanza. Esta recomendación puede ser tan costosa como mantener varias suites forenses de dispositivos móviles y formación debido a la escala salarial asociada al L33T, o digamos, a alguien que sea muy bueno en lo que hace. Otra preocupación puede ser el ciclo de retención de los examinadores. Las personas en este campo suelen buscar la superación personal, ya sea a través de la educación o de la trayectoria profesional. El desgaste de los empleados es bastante común una vez conseguidas las certificaciones. Sencillamente, un salario más alto es una motivación importante para cambiar de trabajo.

La adquisición y retención de examinadores puede dar más peso al despliegue de la(s) suite(s) forense(s) móvil(es) en su taller/laboratorio. La curva de aprendizaje del proceso disminuye, mientras que la producción puede mantenerse en el L33T o ligeramente por debajo. Y lo que es más importante, la suite forense móvil no le dejará adivinando: "¿Y ahora cómo ha funcionado el script que ha escrito Juan?". En ausencia de un empleado, la producción no se vería interrumpida por una cuestión de conocimientos patentados.

.

# Suites forenses para dispositivos móviles

Ahora que hemos discutido algunas de las cuestiones que rodean el método de recuperación y análisis de datos, vamos a aventurarnos a discutir algunas de las suites forenses móviles que he tenido la oportunidad de utilizar.

La siguiente lista de herramientas forenses para dispositivos móviles no es exhaustiva, ni se presenta en ningún orden de preferencia.

- Belcasoft Evidence Center

- BlackLight de Cellebrite

- Dispositivo universal de extracción forense (UFED) de Cellebrite

- Analizador físico de Cellebrite

- MD-NEXT/MD-LIVE de Hancom

- Axiom de Magnet Forensic

- XRY/XAMN de Micro Systemation

- Final Mobile de MobileEdit

- Detective de Oxygen Forensic

- E3:DS de Paraben Forensic

- DataPilot de Susteen

Cada una de estas utilidades incluye una capacidad de extracción compatible con los principales sistemas operativos de dispositivos móviles que se utilizan en la actualidad. Las utilidades admiten varios niveles de recuperación de datos, como categórica, del sistema de archivos o física.

La informática forense básica define que es preferible una copia a nivel físico, o a nivel de bits, de los datos almacenados. Por desgracia, no todas las combinaciones de procesadores y módulos de memoria son compatibles con este nivel de recuperación. Además, el caso puede dictar que el tiempo que llevaría obtener una recuperación de datos a nivel físico excedería lo razonable y, por lo tanto, no sería una solución probable. Este suele ser un problema cuando el registro se basa en el consentimiento, o en casos que implican operaciones encubiertas.

Para repasar, se espera que el nivel físico de la documentación de datos comience al principio del módulo de memoria, o conjunto de datos, y continúe hasta que alcance el bit final de datos almacenados dentro del módulo de memoria.

Se considera que es una representación completa y exacta de los datos almacenados en el módulo de memoria en el momento de la captura. Puede o no incluir sumas de comprobación de redundancia cíclica (CRC).

El nivel de documentación de datos del sistema de archivos no comienza al principio del módulo de memoria, sino al principio del volumen. En función del tipo específico de sistema operativo, los datos capturados deben incluir tanto el sistema operativo como los archivos generados por el usuario. Cabe señalar que el número de archivos de sistema que se capturarán depende del tipo de sistema operativo y de la versión específica de dicho sistema. En comparación con el análisis forense de ordenadores personales, este nivel de documentación de datos es similar al que se obtiene durante la adquisición lógica de un sistema informático cifrado, como en los casos relacionados con BitLocker.

Por último, está la captura categórica o de "cubos". Me refiero a ella como la captura de "cubos" simplemente porque la utilidad forense móvil barre a través del dispositivo conectado y captura los cubos de datos que comprenden las áreas clave de la información generada por el usuario que se almacena en un dispositivo móvil.

Los cubos de datos suelen incluir los siguientes tipos de información generada por el usuario.

- Lista de contactos

- Historial de llamadas

- Buzón de voz/Archivos de audio

- Sistema de mensajes cortos (SMS) comunicación basada en texto

- Sistema de mensajes múltiples (MMS)

- Archivos de imágenes gráficas

- Archivos de vídeo

- Archivos de datos: Estos archivos incluyen archivos App comunes de terceros que pueden, o no, descodificarse automáticamente

El nivel categórico de extracción de datos es el único que permite al examinador elegir qué tipo de datos específicos se extraen. Esto puede ser relevante si el alcance de la búsqueda es limitado en casos que implican una búsqueda justificada, o si se trata de información comercial privada.

Teniendo en cuenta lo anterior, según mi experiencia, un flujo de trabajo de extracción debe seguir un orden sistemático para garantizar el mejor resultado en el examen. El orden preferido es:

1. Físico

2. Sistema de archivos

3. Nivel categórico o de bucket

Una vez más, cada caso tiene sus propias circunstancias y cada dispositivo móvil tiene sus propios factores que influyen en el nivel de extracción de datos que debe realizarse. Corresponde al examinador forense asegurarse de que se utiliza la extracción más adecuada para cumplir los requisitos del caso.

## 

## EL PROCESO FORENSE DE DISPOSITIVOS MÓVILES

## Según mi experiencia, el elemento más influyente en el análisis forense de dispositivos móviles es el proceso de recuperación de datos. Sencillamente, si los datos han sido alterados o son inaccesibles, el examen y el análisis se ven muy afectados. Para reducir la probabilidad de recuperar datos alterados, hay una serie de cosas que se pueden hacer durante el proceso de incautación para limitar las alteraciones y proporcionar una mayor probabilidad de éxito. Los siguientes pasos, o fases, se presentan para proporcionar orientación en el proceso forense de dispositivos móviles. Estos pasos son: Incautar, Asegurar, Identificar, Recuperar, Analizar e Informar..

## Incautación del dispositivo móvil

## El proceso utilizado durante la incautación del dispositivo móvil puede determinar los resultados del examen. Dado el énfasis actual en la seguridad, el cifrado de los datos en reposo se ha convertido en la nueva normalidad. Atrás quedaron los días en que los datos esperaban a ser extraídos de la memoria sin que estuviera presente alguna forma de cifrado. Tanto si se trata de un volumen completo como de un archivo, el cifrado le impedirá acceder a los datos que necesita para responder a las preguntas planteadas. Por lo tanto, se reconoce que la mejor práctica para incautar un dispositivo móvil que está encendido es dejar el dispositivo encendido y mantener la energía en él. Un dispositivo móvil apagado debe dejarse apagado. En los casos de dispositivos móviles propiedad de la empresa, la presencia de un código de acceso no debería impedir el acceso a los datos almacenados. El administrador de la red debe mantener una palabra clave (código de acceso) en custodia de cada dispositivo emitido. De este modo, se facilitará la recuperación en caso de que el empleado deje de trabajar o sea necesario realizar una investigación sobre el uso del dispositivo.

## Además, debe mantenerse un programa de copias de seguridad.

## Lamentablemente, en la mayoría de las investigaciones penales el código de acceso no está a disposición del forense. La falta de un código de acceso puede impedir el acceso a los datos generados por el usuario en un formato legible. Aunque existen salvedades a esta afirmación que se basan en la versión del sistema operativo y la arquitectura del hardware, el mejor escenario para el éxito incluye conocer, o identificar, el código de acceso que está impidiendo el acceso al dispositivo móvil.

## Puesto que la experiencia del usuario es un punto importante a tener en cuenta por el fabricante. Esta consideración ha creado grietas en la armadura del cifrado, por así decirlo. Pequeños portales pueden permanecer accesibles facilitando la extracción de datos aparentemente inocuos que pueden ayudar en la identificación del código de acceso. O bien, permitir vías alternativas a los propios datos evitando por completo el sistema operativo. Discutiremos estos elementos en mayor profundidad, pero por ahora es importante recordar que si el dispositivo móvil está encendido, déjelo encendido y manténgalo encendido.

## Identifique el dispositivo móvil lo mejor que pueda. Observe las etiquetas de fabricación, u otros caracteres identificativos, o secuencias numéricas. Documente lo que vea e incluso fotografíe el dispositivo para utilizarlo como referencia en el futuro.

## Aquí es donde la información en relieve del dispositivo, o debajo de la batería, cobra importancia. Por lo general, un dispositivo móvil llevará una identificación que ayudará a identificar cierta información del abonado que puede utilizarse en el proceso de investigación.

## En la incautación de dispositivos que utilizan una red CDMA, se encontrarán varios códigos de identificación.

## Estos pueden consistir en un identificador de equipo móvil (MEID) o un número de serie electrónico (ESN), un número de serie, un número de modelo y posiblemente un número de identificación de la Comisión Federal de Comunicaciones (FCC ID).

## En comparación, un dispositivo que utilice GSM encontrará un MEID, un número de serie y un ICCID grabados en la SIM. Dentro de los datos almacenados en la SIM se almacena otro código de identificación de red de servicio, que es la Identidad Internacional de Abonado Móvil (IMSI).

## El MEID es una secuencia de 14 dígitos, que ocupa 56 bits, que identifica un dispositivo de hardware a la red de servicio. Su predecesor es el ESN, de 11 dígitos y 32 bits. A medida que la producción de ESN se acercaba al máximo de 4.000 millones de secuencias posibles de 11 dígitos que admite, se vio que el formato ESN era insuficiente para etiquetar el creciente número de dispositivos móviles del mercado. Por ello, en 2005 se estableció el MEID como estándar para los dispositivos de nueva fabricación. Se discute el año exacto de la implantación, pero tanto si fue en 2005 como en 2006, la cuestión es que las secuencias de numeración eran insuficientes para satisfacer las necesidades de la fabricación.

## 

## Otra característica del MEID era la posibilidad de etiquetar un dispositivo móvil específico como perdido o robado.

## Tanto el MEID como el ESN son indicadores de que el dispositivo que lo lleva ha estado asociado a una red CDMA. Al igual que el SIM ICCID, el MEID sigue un formato utilizado para definir el dispositivo.

## Ese formato consta de los tres campos siguientes: un código regional, un código de fabricación y un número de serie.

## Cuando se divide en los tres campos, la secuencia de 14 dígitos se parecerá a la siguiente.

## Código regional (x 2)|Código de fabricación (x 6)| Número de serie (x 6), representado como:

## RC,RC,MC,MC,MC,MC,MC,MC,SN,SN,SN,SN,SN,SN

**La Identidad Internacional de Equipo Móvil (IMEI)** es un código de identificación único de 15 dígitos asignado a un dispositivo móvil específico. Dependiendo del año de fabricación, el dispositivo puede mostrar un código de 17 dígitos. El IMEI sigue un formato estandarizado que identifica al fabricante, el modelo y el número de serie del dispositivo. Al igual que el MEID, el IMEI tiene un formato específico para representar la información antes mencionada.

1. El código de asignación de tipo (TAC) ocupa los ocho (8) primeros caracteres. Esta serie identifica el fabricante de origen y el modelo del dispositivo.
2. Los seis (6) caracteres siguientes identifican el número de serie del aparato.
3. Los dígitos restantes son descriptivos del dígito de control en el caso de un formato de 15 caracteres, o de la versión del software del sistema operativo que se había instalado en el dispositivo móvil en el código más largo de 17 dígitos.
4. Los dígitos restantes son descriptivos bien del dígito de control en el caso de un formato de 15 caracteres. O bien, la versión del software del sistema operativo que se había instalado en el dispositivo móvil en el código más largo de 17 dígitos.

El IMEI suele estar grabado en la tapa trasera del chasis, en el soporte de la tarjeta SIM o debajo de la batería en la etiqueta del fabricante. Como se ha indicado, el IMEI está codificado en el dispositivo. Si no es visible en el exterior del terminal, introduzca los caracteres \*#06# en el teclado y pulse intro. Esto revelará el IMEI dentro de la pantalla digitalizadora.

Dado que las redes de servicio **GSM** utilizan la **SIM** para autenticarse en el contrato de servicio, ¿qué proporciona el IMEI? En pocas palabras, el **IMEI es la huella digital de su dispositivo móvil.** Es un identificador único para un dispositivo específico. Si su dispositivo requiere reparación, el centro registrará el IMEI para asociarlo a su ticket de servicio.

También puede compararse con el número de identificación del vehículo, o VIN, de su automóvil. Al igual que en caso de robo de un vehículo de motor, el número de bastidor se introduce en una base de datos de las fuerzas de seguridad para su seguimiento.

El IMEI puede introducirse en la base de datos de la red de servicios como dispositivo perdido o robado, poniéndolo en una lista negra que impide su uso. En comparación con el IMEI, el MEID se utiliza para autenticarse con la red de servicios CDMA, se utiliza para identificar el propio dispositivo y puede utilizarse para incluirlo en una lista negra.

El IMSI es un código de 15 dígitos que identifica una SIM específica ante la red de servicio. Proporciona un código único que se utiliza para identificar el nivel o niveles de servicio soportados por el contrato de servicio. La clave de autenticación (Ki) dentro de la SIM proporciona autenticación al servicio, una vez establecida la IMSI se utiliza para enrutar el tráfico hacia y desde el Número Internacional de Directorio de Suscriptor de Estación Móvil (MSISDN) específico.

Funciona para enrutar el servicio a nivel de red, y puede, o no, ser conocido por el usuario final, ya que se almacena dentro de la SIM. Normalmente, sólo se puede descubrir mediante un análisis de la SIM o a partir de registros obtenidos de la red de servicio. La capacidad de relacionar un código de identificación específico con un dispositivo concreto respaldará un argumento a favor de la atribución al usuario. También ofrecen al investigador un vínculo para recuperar información basada en la red que puede ser útil en el proceso de investigación.

***Asegurar el dispositivo móvil***

Para funcionar como está diseñado, un dispositivo móvil debe estar en constante estado de conexión, ya sea móvil o de red (WiFi). Este estado crea una vía de fallo para el examinador, ya que el dispositivo está continuamente recibiendo comunicaciones, lo que altera la memoria. El aislamiento del dispositivo móvil de las señales de radio impide que se alteren los datos almacenados.

Un estado constante de conectividad es similar a un arroyo de montaña. Los datos fluyen hacia el dispositivo móvil, del mismo modo que el agua se desliza por el lecho del arroyo y a lo largo de las orillas. Este flujo aporta los datos deseados al usuario, igual que el agua agitada aporta sedimentos fértiles a los campos que alimenta el arroyo. Los usuarios se alegran de que su dispositivo esté repleto de información, igual que las cosechas que crecen en los campos están repletas de la corriente.

Esta actividad es aceptable hasta que se determina que el dispositivo móvil está implicado en una denuncia u otro problema. Entonces el flujo de datos empieza a alterar los datos almacenados, igual que la erosión del arroyo cambia su recorrido con el tiempo. Lo que una vez fue la ruta conocida de la corriente se modifica para siempre, para nunca volver a ese estado previamente conocido.

Una vez que los datos se escriben en el módulo de memoria integrada, están sujetos a múltiples capas de protocolos de hardware y software. Los términos "nivelación de desgaste", "recogida de basura" y "vaciado" cobran importancia en el proceso de documentación de datos. Se trata de un resultado directo del módulo de memoria integrado y de los parámetros bajo los que funciona la memoria.

Baste decir que evitar la entrada de datos en un dispositivo móvil incautado es primordial.

Cualquier dato, independientemente de su cantidad, puede causar un daño irreparable al proceso de examen.

Puede ser algo tan simple como un cambio de fecha y hora de un sitio web visitado anteriormente.

O tan perjudicial como la recepción de una orden de "borrado" que restaure el dispositivo móvil a un estado de fábrica.

En relación con las normas sobre pruebas, el dispositivo móvil, si no se aísla, deja de estar en las mismas condiciones en las que estaba cuando se incautó.

Los abogados defensores pueden utilizar este error para atacar la voracidad de las pruebas, así como para atacar la credibilidad del examinador.

Para quienes no lo han experimentado, el estrado de los testigos es un lugar solitario. Una vez que se pasa de acusar al acusado a defenderse a uno mismo, el testimonio se hace largo y desagradable.

Para evitar estos cambios no deseados, es fundamental desconectarse de la conectividad de la red, lo que puede lograrse de varias maneras.

Aquí es donde la comprensión de la transmisión y recepción de radio juega un papel importante. La referencia a nuestro debate sobre la importancia de identificar la modulación de frecuencia con la que opera el dispositivo móvil objetivo ayuda a determinar qué forma(s) de aislamiento puede(n) utilizarse.

1. En el caso de un dispositivo que se comunique mediante GSM, la extracción de la tarjeta SIM puede ser suficiente para aislar el dispositivo.
2. En los casos de CDMA, se debe reducir la atenuación de la señal de radio para interrumpir las señales de radio. Esto puede hacerse mediante una envoltura de tela metalizada o colocando el dispositivo en una bolsa o cámara de aislamiento comercial.
3. Dependiendo de la marca, el modelo y la versión del sistema operativo, colocar el dispositivo móvil en "modo avión" puede aislar suficientemente el dispositivo. Sin embargo, puede que no sea así, por lo que se recomienda realizar esfuerzos de reducción de la atenuación de las ondas de radio.

Cuando incaute el dispositivo, documente el día, la fecha y la hora de la incautación. Documente su observación del estado en que se encuentra el dispositivo. Es decir, si está encendido, con el código de acceso activado, conectado a WiFi, etc.

A continuación, ponga el dispositivo en "modo avión", envuélvalo o colóquelo en material aislante y llévelo a su tienda o laboratorio.

**Identificar el aparato**

Durante el paso de incautación ya debería haber documentado la marca, el modelo y los códigos numéricos de identificación.

1. Ahora, es importante identificar qué tipo de sistema operativo tiene el dispositivo, o al menos con qué versión se lanzó al mercado por primera vez.
2. Además, conocer el tipo de unidad central de procesamiento, así como el tipo y la capacidad de la memoria, también es importante para acceder al dispositivo y verificar la cantidad de datos que se extraen.
3. Utilizando la información sobre la marca y el modelo junto con recursos de Internet como "phonescoop.com" o "gsmarena.com" se puede obtener información sobre las especificaciones del fabricante en relación con el dispositivo objetivo. Este recurso proporciona información necesaria que resulta útil en el proceso de extracción de datos.

En concreto, un método de adquisición concreto para dispositivos CDMA basado en la unidad central de procesamiento. O que los datos se almacenan, o no, en un estado cifrado en reposo basado en el análisis de las especificaciones del hardware y del sistema operativo.

Una revisión exhaustiva de la información disponible antes de intentar recuperar los datos almacenados en un dispositivo móvil ahorrará tiempo y frustración al examinador.

También puede resultar esencial para identificar una vía para la recuperación de datos de "dispositivos problemáticos".

1. Los dispositivos problemáticos son aquellos que muestran una separación de sus compañeros desde el punto de vista operativo. Arrancan con normalidad, pero cuando se conectan para la documentación de datos no se comportan de la misma manera que un dispositivo de la misma marca y modelo.
2. El dispositivo problemático puede haberse presentado en un caso en el que intervengan varios dispositivos, muchos de ellos de la misma marca y modelo. Siguiendo mi flujo de trabajo preferido, obtengo datos de uno o más dispositivos y luego me encuentro con el dispositivo problemático.
3. Por razones que se me escapan, el dispositivo no responde como los demás. Sin embargo, al conocer las especificaciones del hardware y del sistema operativo, normalmente se puede encontrar una solución.
4. Otros dispositivos problemáticos tienen algún defecto físico concreto, como una pantalla digitalizadora dañada o un puerto de datos dañado. Esos defectos son relativamente fáciles de mitigar si se dispone de piezas de repuesto, tiempo y cierta habilidad para soldar.

**Recuperación de datos**

Una vez analizado el dispositivo desde el punto de vista del software, el hardware y la red, podemos pasar a la fase de documentación de los datos.

Este paso depende de si su taller/laboratorio utiliza conjuntos de herramientas forenses para dispositivos móviles, o si lo hace con herramientas propias o de código abierto.

Mis experiencias comenzaron utilizando herramientas básicas de código abierto para la recuperación de datos. Al principio, fotografiábamos la información relevante en la pantalla del dispositivo móvil y preparábamos un informe que reflejaba nuestros hallazgos.

El creciente número de servicios registrados por dispositivos móviles puso rápidamente de manifiesto que el uso de la fotografía era ineficaz.

El siguiente paso consistió en establecer la conectividad mediante comandos AT para "OBTENER" datos del dispositivo. Sin embargo, el creciente número de versiones propietarias del entorno de ejecución binario para redes inalámbricas (BREW)3 creaba problemas en la documentación de los datos. BREW es un componente de los dispositivos móviles de tipo "básico" y "funcional".

Estaba asociado a dispositivos móviles con procesadores Qualcomm. Estos procesadores tenían su propio software operativo que gestionaba la interfaz del sistema. Esto permitía ejecutar aplicaciones sin tener que codificarlas para gestionar las operaciones del sistema, ya que eso lo gestionaba el chipset.

A medida que avanzaba la evolución de los dispositivos móviles, el creciente número de fabricantes de dispositivos dio lugar a un variado número de sistemas operativos y entornos. Además, algunos fabricantes optaron por crear sus propias versiones propietarias de un conector de datos. En algunos ejemplos, la transferencia de datos con el dispositivo sólo era posible a través del servicio celular o de puntos de acción de destino en la placa de circuito impreso.

El habitual conector USB "Tipo A" era demasiado grande para los chasis cada vez más pequeños de los dispositivos móviles. Esto dio lugar a la implementación de conexiones en serie mediante conectores USB mini, micro y, ahora, "C".

Debido a la gran variedad de configuraciones de hardware, sistemas operativos y accesos a puertos de datos, los primeros examinadores de dispositivos móviles tenían mucho trabajo en sus tareas de recuperación de datos.

Por muy variados que fueran los dispositivos móviles, una empresa canadiense conocida como Research In Motion, o RIM, estaba creando una forma de continuidad debido al éxito de la comercialización de sus dispositivos móviles Blackberry. Estos dispositivos tenían teclados QWERTY y cada vez proliferaban más en el mercado de los dispositivos móviles.

De este modo, se estableció una especie de estándar para la configuración del hardware. Aunque las versiones del sistema operativo Blackberry eran relativamente sencillas de adquirir, el proceso podía ser poco completo si el examinador no mantenía una versión actualizada del software de gestión de Blackberry.

La introducción por parte de Apple de su iPhone en 2007 inició un cambio drástico en el análisis forense de dispositivos móviles.

Seguíamos encontrándonos con un cable de datos propietario, ahora en forma de cable de datos de 30 patillas. Sin embargo, contenía un sistema operativo empaquetado que utilizaba aplicaciones para proporcionar servicios al usuario final. El IPSW, o archivo de software del iPhone, permitía al usuario sustituir un sistema dañado por una instalación nueva. El IPSW era un paquete que era, y sigue siendo, capaz de recibir actualizaciones sin afectar a las aplicaciones instaladas ni a los datos generados por el usuario.

Después, la aparición del sistema operativo Android en 2008 supuso otra preocupación para los examinadores. Gestionado por Google, las primeras preocupaciones se referían a que era de código abierto y funcionaba de forma algo diferente a la arquitectura del iPhone de Apple. Comparte con iOS el uso de aplicaciones para dar servicio a los intereses del usuario final. Sin embargo, Android no compartía los estrictos protocolos de desarrollo impuestos por Apple en aquella época. Con el paso del tiempo, las distintas plataformas de dispositivos móviles en las que se ha instalado han demostrado ser un sistema operativo desafiante.

La evolución de los principales sistemas operativos actuales, iOS y Android, está documentada y disponible en Internet. Si practicas tu 'Google-Fu' recibirás alrededor de 1.430.000.000 de resultados de búsqueda para 'La historia de iOS', mientras que 'La historia del sistema operativo Android' te devolverá 444.000.000 de resultados de búsqueda. Huelga decir que hay más información disponible para satisfacer el área específica de interés que pueda tener para cualquiera de los sistemas operativos. Mucha más de la que podría ofrecer en esta sección.

Desde mi experiencia como examinador forense digital, el área de interés más importante tiene que ver con la seguridad. Específicamente, las características de seguridad que están habilitadas por defecto en el sistema operativo en comparación con las soportadas por el hardware.

He descubierto que en algunas versiones de los sistemas operativos, el software puede anunciar ciertas funciones de seguridad. Sin embargo, el hardware, ya sea el procesador o la memoria flash, no soporta esa funcionalidad anunciada. Teniendo en cuenta estas observaciones, he adoptado un mantra de "menos intrusivo a más intrusivo" en la realización de mi documentación de datos.

Un ejemplo de método "menos intrusivo" de documentación de datos, o extracción de datos como se ha acuñado, consistiría en establecer una conexión con el dispositivo móvil a través del puerto de datos del dispositivo. Este proceso puede implicar la carga de un cliente en el dispositivo de pruebas que extrae los datos almacenados según lo determinado por el alcance de la búsqueda. Puede basarse en la activación de una forma de "modo de descarga" en el dispositivo para eludir los dispositivos de seguridad. En algunos casos, puede ser necesario acceder a la PCB para crear un cortocircuito en el sistema, creando una vía abierta a los datos almacenados. En cada uno de los procesos mencionados se produce una intrusión limitada en el chasis del dispositivo.

En comparación, los procesos "más intrusivos" implican el desmontaje del dispositivo móvil para acceder a la placa de circuito impreso. Tras el desmontaje, los datos contenidos en la memoria flash pueden documentarse mediante procesos que implican el establecimiento de una conexión con diversos puntos de acceso de destino (TAP) montados en superficie, componentes montados en superficie (SMC) o incluso la extracción de la memoria flash incrustada. Estos procesos suelen denominarse con la siguiente nomenclatura: JTAG, ISP y chip off.

**JTAG**

El Grupo de Acción de Pruebas Conjuntas (JTAG) se creó para establecer una norma que debe seguirse en el proceso de fabricación de placas de circuitos integrados. En concreto, para abordar la incapacidad de probar circuitos integrados (IC) individuales que se instalan muy cerca unos de otros en la placa de circuito impreso, lo que impide los procesos de prueba de conexión directa.

La necesidad de estandarizar las pruebas de CI se hizo patente y dio lugar a la creación de la norma IEEE 1149 en 1985. La norma IEEE 1149 consta de varias revisiones y, a efectos forenses, nos interesa sobre todo la versión 1149.1, de 1990.5

La norma facilita la comprobación de los canales de comunicación entre los distintos circuitos integrados de la placa de circuito impreso. El proceso también se conoce como "Boundary Scan" y utiliza paquetes de instrucciones que se envuelven con instrucciones específicas del circuito integrado.

A medida que los paquetes fluyen a través de los distintos circuitos integrados montados en la placa de circuito impreso. Un conjunto específico de instrucciones para un CI específico se desenvuelve y provoca una respuesta en el CI. Si las instrucciones no están relacionadas con ese CI específico, se pasa al siguiente CI. Este proceso continúa a través de la placa de circuito impreso. A medida que las instrucciones son recibidas por el CI apropiado, se recibe una respuesta en el otro extremo. La respuesta posterior indica que el CI funciona correctamente.

En la PCB hay Puntos de Acción de Prueba (TAPS) que contienen registros que responden a la cadena envuelta de paquetes. A medida que la instrucción fluye a través del TAP, si la instrucción está relacionada con el CI específico al que se dirige, la instrucción entra en el CI a través de la Entrada de Datos de Prueba (TDI).

Si la instrucción no es específica del CI que se está tratando, se envía a través de la salida de datos de prueba (TDO). Para gestionar adecuadamente el proceso, el TAP utiliza tres señales adicionales. Las tres señales son Test Clock (TCK), Test Reset (TRST) y Test Mode Select (TMS).

TMS controla las instrucciones mientras que TCK controla la cadencia de la carga global y el procesamiento de las instrucciones. Por último, TRST simplemente reinicia las instrucciones.

La capacidad de interactuar con los distintos circuitos integrados que afectan al flujo de datos hacia y desde el módulo de memoria integrado ofrece al forense la posibilidad de ordenar a la memoria que libere los datos. Mediante el uso de varios emuladores como Medusa Pro, RIFF Box2, Easy JTAG y Octoplus Pro se copian los datos de la memoria.

El uso de JTAG en la recuperación de datos se basa en una serie de consideraciones:

1. Si el dispositivo móvil en cuestión no es compatible con una herramienta disponible comercialmente
2. Si el dispositivo está protegido por un código de acceso
3. Si está dañado física o lógicamente y no arranca

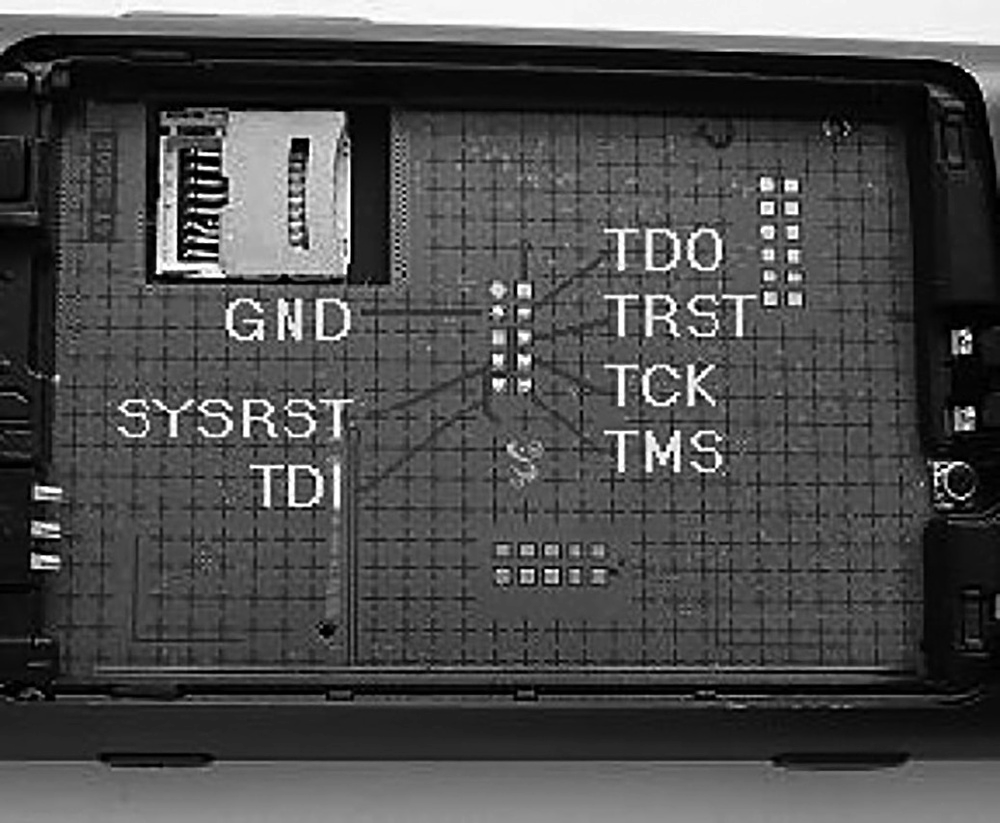
Cuando se da una situación como la descrita, el proceso de recuperación de datos es bastante sencillo. Acceda a la memoria

**Acceso a la memoria del dispositivo móvil**

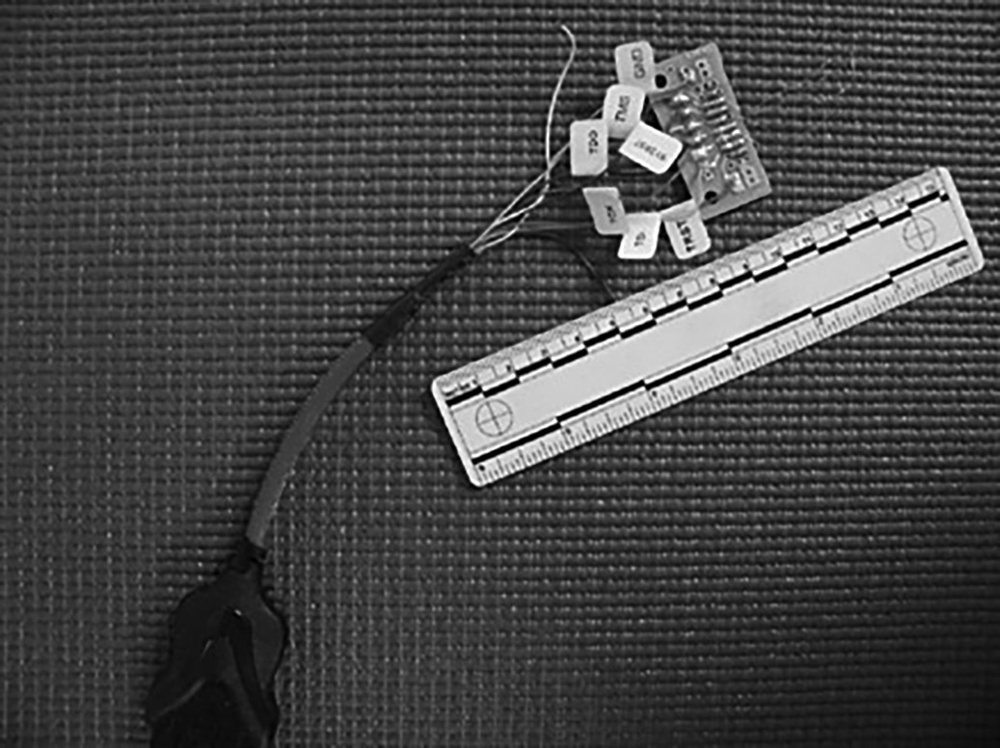
El primer elemento a tener en cuenta es si el dispositivo encontrado es compatible con JTAG y si el emulador de su tienda/laboratorio es compatible con el modelo específico en cuestión. Si no es así, busque en varios listservs para encontrar la dirección correcta. Una vez que haya identificado que el dispositivo es compatible. La siguiente cuestión es localizar los TAPS correctos necesarios para facilitar la comunicación con la memoria.

La ubicación de los TAPS se proporciona generalmente en forma de archivo de ayuda dentro del software del emulador. A continuación, limpie los TAPS y prepárese para soldar el cable a los TAPS designados. El extremo suelto del cable soldado a un TAP se suelda entonces a una placa hija que se utiliza como puente entre el TAPS y el conector del emulador. Compruebe la conducción de cada TAP e inicie el proceso de recuperación de datos a través del software del emulador.

La figura 8.1 muestra los TAPS situados en un dispositivo móvil Samsung Wave. En este caso, los TAPS se encuentran debajo de la etiqueta del fabricante, pero pueden estar situados en otro lugar de la placa de circuito impreso.



*Cifra 8.1* JTAG asignación de pines Samsung Ola [6](#_bookmark90)



*Figure 8.2* JTAG emulator connector to daughter board[7](#_bookmark91)

La figura 8.2 muestra el cable de conexión al dispositivo emulador. Se ha soldado a una placa hija. Utilizando un cable esmaltado de 0,09 milímetros de diámetro, la conexión se realiza a los TAPS JTAG de la PCB.

Esto facilita el movimiento del conector del emulador a la vez que mantiene la conexión con la PCB, y prolonga la vida útil del conector del emulador.

Algunas versiones del software del emulador permiten verificar los datos extraídos mediante la medición de la capacidad. Desde una perspectiva forense digital, esta medición debe complementarse con el hash del conjunto de datos recuperado utilizando MD5, SHA1 o SHA256.

A continuación, debe crearse un duplicado, o copia de trabajo, del conjunto de datos con hash y someterse a un hash posterior para verificar que es una representación exacta del conjunto de datos original recuperado. Una vez finalizado el proceso de duplicación y verificación, la copia de trabajo puede introducirse en la herramienta de su elección y buscarse artefactos relevantes para la reclamación.

**Programación dentro del sistema (ISP)**

La programación DENTRO del sistema (o procesamiento) (ISP) implica principios similares a los descritos en el proceso JTAG.

ISP implica establecer conexión con la memoria flash integrada a través de componentes montados en superficie (SMC) que facilitan la comunicación entre la unidad central de procesamiento (CPU) y el módulo de memoria.

Al igual que en el proceso JTAG, es necesario soldar cables a los distintos puntos que controlan la comunicación. Estos puntos son

- Datos 0 o D0

- VCC que equivale a 2,8-3,3 voltios

- VCCQ que equivale a 1.8 voltios

- Reloj o CLK

- Comando o CMD

- Tierra o GRND

Los SMD de VCC, VCCQ y CMD pueden ser una resistencia o un condensador.

El CLK puede ser una resistencia, un condensador o un punto de contacto en la PCB.

El GRND es cualquier superficie conectada a tierra, como un escudo térmico o la placa principal de conexión a tierra de la PCB. Mediante el uso de un emulador como el Z3X, o el RIFF2, se recuperan los datos almacenados en el módulo de memoria.

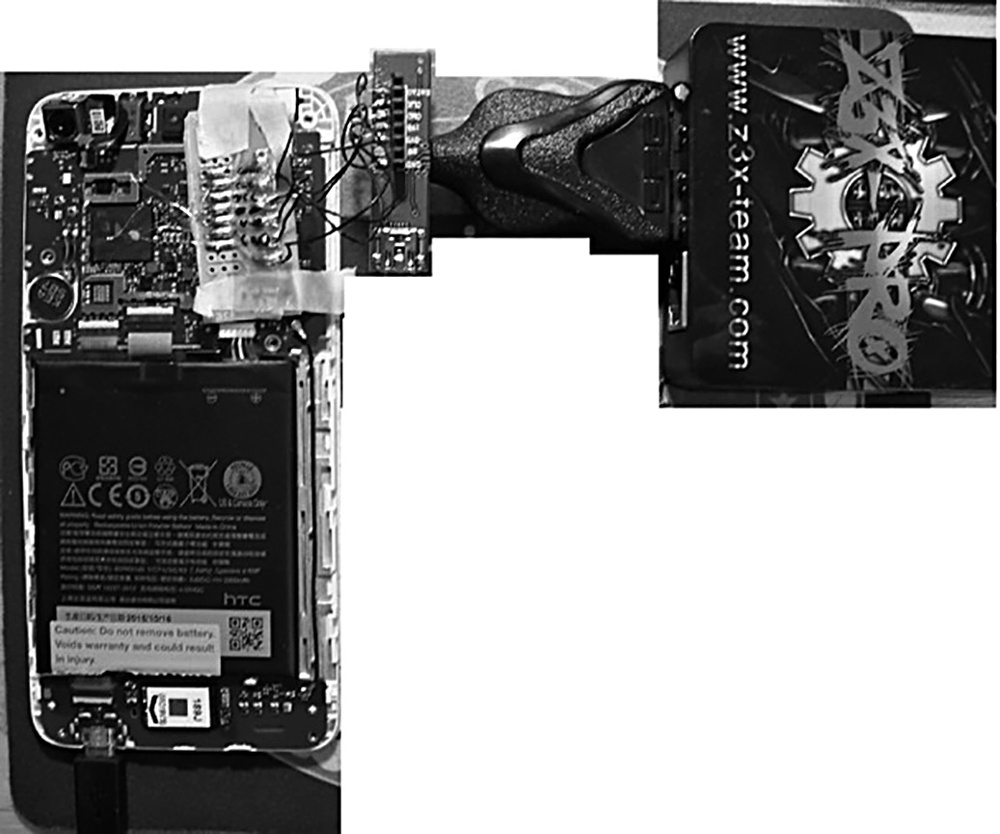
Para identificar la ubicación específica de los cinco puntos de conexión primarios, es necesario conocer la ubicación de los canales de comunicación dentro de la PCB.

El fabricante no los etiqueta para nosotros como D0, CLK, CMD, VCC, y VCCQ. Esta información está disponible en el emulador, a menudo denominada "pinout".

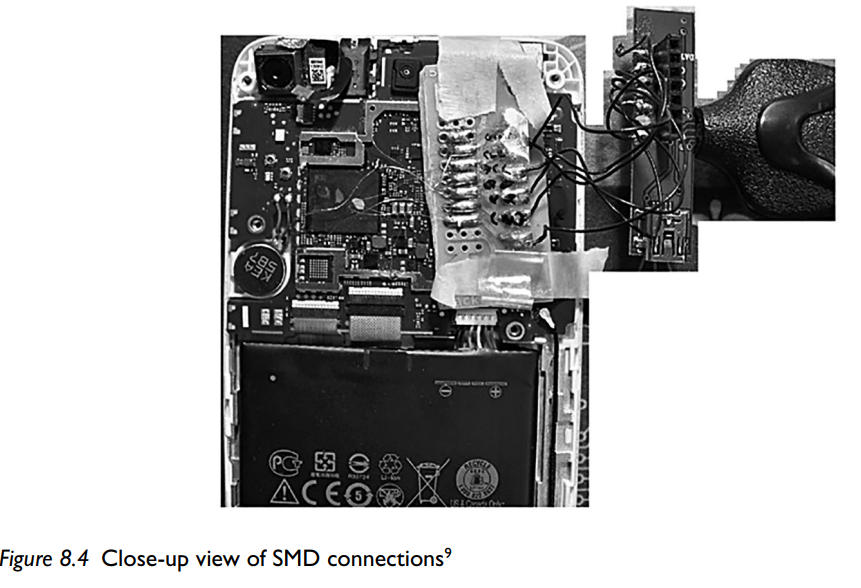
La figura 8.3 muestra un dispositivo móvil HTC sometido al proceso de extracción utilizando la caja Z3X.

El cable de conexión que se suelda entre la placa hija y el SMD específico que suministra un canal de comunicación tiene un diámetro de 0,09 milímetros. La figura 8.4 muestra una vista en primer plano de estas conexiones.

Si el dispositivo del que intenta recuperar datos no está soportado directamente por su emulador comercial, el "pinout" no estará disponible a través del emulador.



*Figure 8.3* Z3X extraction[8](#_bookmark92)



Aquí es donde tus conocimientos sobre procesadores y módulos de memoria cobran importancia. A través de la interfaz del emulador, se suele encontrar un modo "genérico". El modo genérico le permitirá introducir algunos parámetros específicos relativos al tipo de procesador o memoria a la que se dirige. Si se establece conexión con D0, CLK, CMD, VCC, VCCQ y GRND, el emulador realizará su función.

Esto plantea la cuestión de qué hacer si no se dispone de un esquema de pines para el dispositivo que se está procesando. ¿Cómo localizamos D0, CLK, CMD, VCC, VCCQ?

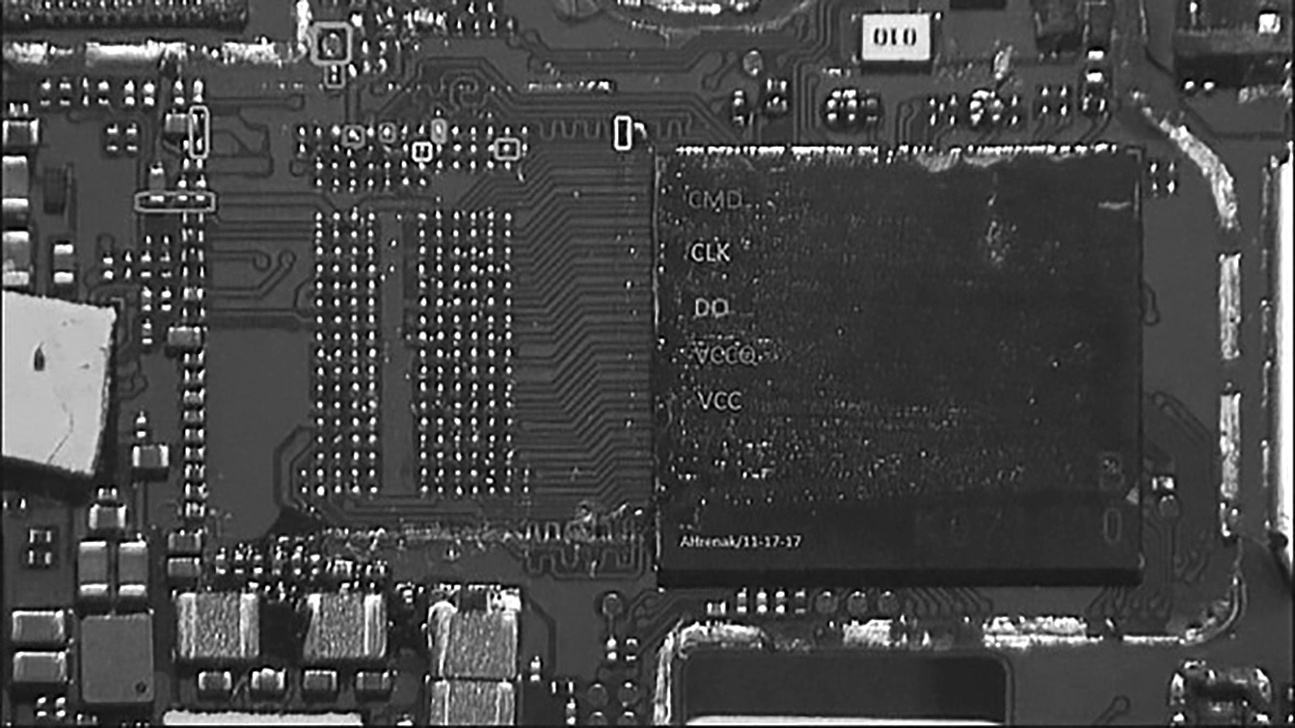
Mediante el uso de un dispositivo donante de la misma marca y modelo, puede identificar los puntos de contacto correctos. Para ello, retire el módulo de memoria de la placa de circuito impreso del dispositivo donante. A continuación, utilizando los conocimientos adquiridos de la hoja de datos del módulo de memoria. Trace un mapa de los puntos de conexión aplicables utilizando su voltímetro para comprobar la continuidad entre los zócalos de la placa de circuito impreso situados debajo del módulo de memoria extraído y los SMD de la placa de circuito impreso.

El proceso de ingeniería inversa antes mencionado no es difícil, pero puede resultar laborioso debido al número de SMD integrados en la placa de circuito impreso. El siguiente gráfico muestra la PCB de un Coolpad, modelo 3632A que se recibió para la recuperación de datos. En ese momento, esta marca y modelo específicos de dispositivo no eran compatibles con las herramientas forenses comerciales, ni habían sido previamente "mapeados" para ISP. Por lo tanto, se retiró el módulo de memoria y se completó el proceso de ingeniería inversa para identificar los puntos de acceso de destino asociados que permitieran la recuperación de datos mediante ISP (figura 8.5).

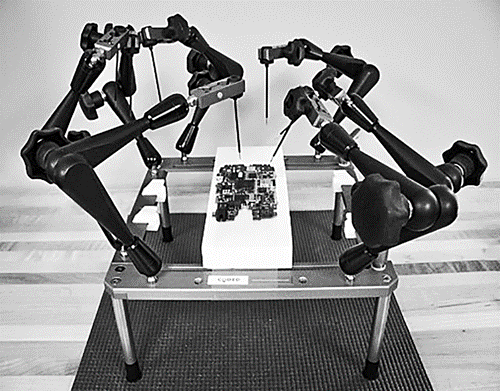
Si usted es miembro de una "Comunidad Forense Móvil", muchos miembros están dispuestos a compartir sus pinouts. Por lo tanto, también es una opción preguntar si alguien del grupo tiene un pinout para ese dispositivo. Esto está relacionado con la práctica de compartir el producto del trabajo con la comunidad. El análisis forense de dispositivos móviles es tan eficaz como lo es hoy en día gracias al intercambio de conocimientos y experiencias.

Para quienes sufren de "ojo de anciano" o tienen temblores que interfieren con la destreza manual, una opción es utilizar una mesa VR (que permite a los forenses adquirir datos de dispositivos móviles, dispositivos GPS y otras unidades electrónicas) o el kit CODED (que permite a los forenses adquirir datos de dispositivos móviles sin necesidad de soldar).

Ambos facilitan la conexión a los puntos TAPS o ISP mediante el uso de clavijas pogo. Los pogo pins son clavijas de cobre accionadas por resorte que se sujetan a brazos segmentados que se bloquean en su sitio. El pogo pin puede colocarse en contacto con el CI objetivo y mantenerse en su sitio gracias al brazo de bloqueo.



*Figure 8.5* Reverse engineering of Coolpad 3632A[10](#_bookmark94)



*Figure 8.6* The CODED[11](#_bookmark95)

*Cifra 8.2* JTAG emulador conector a hija tablero [7](#_bookmark91)

El CODED se representa en la figura 8.6. La placa de circuito impreso descansa sobre un trozo de plástico no conductivo que le sirve de soporte. Esto es necesario ya que se aplica presión a la placa cuando los pivotes se colocan en los respectivos SMD. La presión aplicada hace que la PCB se flexione, lo que da lugar a una superficie inestable, provocando una comunicación inconsistente a través de los pogo pins.

Los cables de conexión del emulador elegido se conectan al extremo del pin pogo y ya está. Bueno, no siempre, ya que hay veces en las que el pogo pin puede resbalar de un SMD mientras estás localizando otro punto de contacto. O que accidentalmente golpees la mesa. Al igual que con la soldadura, el tiempo y la práctica con tus herramientas te llevarán a completar la tarea con éxito. La Mesa VR y el Kit CODED son buenas herramientas para tener en tu caja de herramientas, pero los procesos ISP y JTAG pueden ser completados a través de buenas técnicas de soldadura.

¿**Dónde están mis datos?**

Entonces, los pinouts ISP han sido localizados y las conexiones a D0, CMD, CLK, VCC, VCCQ, y GRND han sido establecidas. Se ha comprobado la continuidad de las conexiones entre los distintos puntos de conexión de la PCB y el emulador y se ha verificado que son "buenas". Al activar la función de lectura del emulador, se extraen los datos almacenados. A continuación, los datos se codifican, verifican y duplican con fines de copia de trabajo. Con la cálida sensación del éxito, la copia de trabajo se procesa con la herramienta de análisis de su elección. Un tiempo después, los datos analizados se revelan, o no.

Acaba de recibir el mensaje de error "No hay datos".

Una rápida revisión de los datos utilizando su herramienta de edición hexadecimal revela que los datos están presentes en su copia de trabajo. Sin embargo, los datos están codificados de una manera no reconocida. En este punto, revisa los pasos que has seguido para obtener los datos de la memoria incrustada de tus notas. Al finalizar, confirma que no se ha observado ninguna anomalía o desviación durante el proceso. Entonces, ¿qué ha fallado?

Es probable que sea el resultado de no haber actuado con la diligencia debida durante la fase de identificación del proceso forense del dispositivo móvil. El proceso ISP fue un éxito; se extrajeron los datos almacenados en el módulo de memoria. El problema es que se extrajeron datos cifrados. ISP es un proceso muy potente, pero tiene un talón de Aquiles. Esa debilidad es la encriptación.

Los datos que se almacenan cifrados en reposo deben descifrarse durante el proceso de recuperación para poder ser analizados. ISP no proporciona esa funcionalidad. La lección es que hay que ser consciente de las capacidades del dispositivo móvil que se está procesando antes de seleccionar un método de recuperación específico. Esta práctica permite obtener el mejor resultado posible de su esfuerzo.

**Chip off**

El proceso de recuperación de datos más intrusivo y destructivo en la investigación forense de dispositivos móviles es el chip off.

El proceso consiste en extraer el módulo de memoria integrado de la placa de circuito impreso. Los principales métodos utilizados para separar el módulo de memoria de la PCB son:

- Flujo de calor

- Mecánico

1. El método de flujo de calor implica el uso de calor para aumentar gradualmente la temperatura de los componentes hasta alcanzar la velocidad de flujo de la soldadura que une los dos componentes. Una vez alcanzada la velocidad de flujo, se separan los componentes.
2. El método mecánico consiste en la eliminación de material que aísla el componente deseado del no deseado. En este caso, se separa el módulo de memoria de la placa de circuito impreso rectificando la placa de circuito impreso del módulo de memoria.

Ambos métodos requieren que se investigue tanto el hardware del dispositivo móvil como el propio módulo de memoria. El principal elemento a tener en cuenta durante la investigación es la compatibilidad con el cifrado. Si la información indica que el cifrado está activado, no proceda con el proceso de chip off.

En consonancia con el proceso ISP, la presencia de datos encriptados se aplica también al chip off. Si se completara un chip off en el que el módulo de memoria contiene datos encriptados, los datos se recuperarían de forma inutilizable. Para descifrar los datos, podríamos utilizar algunas herramientas de descifrado para intentar recuperarlos. Sin embargo, teniendo en cuenta el nivel de cifrado que se utiliza hoy en día, se trata de un esfuerzo poco razonable debido a la cantidad de tiempo que llevaría, si es que fuera posible. En los casos en los que se utiliza 256 AES (Advanced Encryption Standard), personalmente no tengo 27 años para esperar. Además, dados los esquemas de cifrado propietarios que algunos fabricantes utilizan para la generación de claves para su Cifrado Basado en Ficheros, los esfuerzos de descifrado se vuelven aún más irrazonables.

A modo de ejemplo, considere la siguiente pregunta y respuesta.

Pregunta: ¿No deberíamos poder volver a colocar el módulo de memoria en la placa de circuito impreso e intentar un método alternativo de recuperación de datos? Al fin y al cabo, el dispositivo vuelve a su estado original.

Respuesta: Aunque es posible volver a fundir un módulo de memoria en la placa de circuito impreso después de retirarlo, la probabilidad de que se logre la funcionalidad operativa del dispositivo móvil es cuestionable. Dependiendo del método de separación utilizado, flujo de calor o mecánico, puede que ni siquiera sea físicamente posible.

La conclusión es sencilla: Que un proceso sea posible no aumenta la probabilidad de éxito. Investiga el sistema operativo y la arquitectura de hardware del dispositivo y formula un plan que tenga en cuenta las variables presentes.

**Memoria flash NOR**

Lo primero es lo primero. ¿Qué es el módulo de memoria flash integrado? Esencialmente es un componente integrado dentro de un sistema que almacena la información necesaria para que el sistema cumpla su función.

La memoria flash es una forma de memoria de sólo lectura programable y borrable eléctricamente (EEPROM). Al ser no volátil, puede mantener los datos almacenados en su interior sin alimentación.

Hay dos formas básicas de memoria flash en los dispositivos móviles: NOR y NAND.

1. La memoria flash NOR se diseñó para almacenar código y tener un acceso aleatorio rápido dentro de la memoria. Como tal, es muy adecuada para la ejecución del código.
2. La memoria flash NAND está diseñada para proporcionar un acceso aleatorio relativamente lento a través de la memoria, en comparación con la NOR.

Sin embargo, NAND es mucho más fácil de programar (escribir) y borrar que NOR. Esto se debe a la arquitectura presente en la memoria flash.

Las celdas de la memoria flash NOR están conectadas a la línea de bits en paralelo, mientras que las celdas de la memoria flash NAND están conectadas en serie.

Esto hace que las memorias NOR tengan un acceso más rápido (lectura), ya que se puede escribir en cada celda individualmente.

Debido a la capacidad de la NAND de acceder a las celdas en ráfagas de 512 bytes, realiza la programación (escritura) y el borrado a un ritmo mucho más rápido que la NOR. Además, la NAND es más barata de fabricar y tiene más capacidad que la NOR, si se compara el tamaño de la matriz.

En la implementación de dispositivos móviles, NAND es la mejor opción para la memoria flash.

Para el propósito de esta discusión, me referiré a la memoria **flash NAND** que se encuentra comúnmente en los dispositivos móviles de hoy en día.

La memoria flash utiliza puertas controladas electrónicamente, también denominadas celdas de memoria, para almacenar los datos.

Las celdas de memoria al unísono forman el módulo de memoria y son gestionadas por un controlador.

El controlador puede estar situado dentro de la propia matriz del módulo de memoria o muy cerca de ella. En el proceso de chip off de la mayoría de los dispositivos móviles, el controlador es un componente del módulo de memoria.

**Memoria flash NAND**

Cada celda de memoria tiene un estado positivo o negativo, que representa un '0' o un '1' binario.

Por defecto, estas celdas reflejan el estado negativo de '1'. Una celda de memoria NAND con carga positiva representa un "0", mientras que la puerta con carga negativa representa un "1". Una celda individual consta de tres componentes. Estos son:

1. una puerta de control,
2. una puerta flotante y
3. un drenaje.

La puerta de control facilita el flujo de electrones en la célula.

La Puerta Flotante simplemente bloquea el flujo de electrones de la Puerta de Control que viajan hacia el Drenaje.

Un estado negativo dentro de la Puerta Flotante cierra la puerta, bloqueando el flujo de electrones entre la Puerta de Control y el Drenaje. Mientras que un estado positivo abre la Puerta Flotante permitiendo que los electrones lleguen al Drenador.

Para describir completamente este concepto, el material consumiría el espacio de este libro.

Una descripción más simplificada es una analogía utilizando el tráfico de barcazas remontando el río Mississippi. Una barcaza que transporta productos río arriba entrará en una "esclusa" para evitar las diversas presas que se encuentran a lo largo de su ruta.

Una esclusa es un canal de inundación situado junto a la orilla del río perpendicular a una presa. La esclusa tiene una compuerta aguas arriba y otra aguas abajo controladas por un operador. El operador de la esclusa controla los ciclos de inundación y vaciado de la esclusa y el tráfico de barcazas está programado para utilizar el sistema de esclusas en un sentido de la marcha cada vez.

Cuando la barcaza viaja río arriba, la compuerta de la esclusa ya está cerrada y el nivel del agua dentro de la esclusa está en el nivel río abajo. La barcaza entra en la esclusa por la compuerta de aguas abajo, que se cierra detrás de la barcaza. Una vez cerrada la compuerta, el nivel del agua dentro de la esclusa se eleva hasta el nivel de aguas arriba. Una vez igualado, la compuerta de aguas arriba se abre y la barcaza continúa aguas arriba.

A nuestros efectos, el río representa la compuerta de control, mientras que el conjunto de compuertas dentro de la esclusa representa la compuerta flotante. La propia esclusa representa el Drenaje. El operador de la esclusa representa el transistor que controla la tensión umbral dentro de la Puerta de Control. Con estos emparejamientos, los electrones fluyen continuamente a través de cada celda de la memoria flash. Esto se debe a que las Compuertas Flotantes están todas abiertas por defecto, y cada una representa un "1". Cuando es necesario almacenar datos, una carga positiva cierra la puerta flotante, impidiendo que los electrones continúen hacia el drenaje. Dentro de la Puerta de Control se monitoriza el voltaje umbral de la célula. Si se registra una tensión ligeramente negativa, la célula representa un "1", mientras que una tensión positiva representa un "0". Cuando se borra la célula de memoria, se elimina la carga positiva y la puerta flotante vuelve a la posición abierta, permitiendo que los electrones fluyan hacia el drenaje.

Ésta es una descripción muy simple de un proceso complejo que evoluciona continuamente para satisfacer las demandas de rendimiento. El ejemplo es descriptivo de la memoria SLC (Single-Level Cell), que representa un estado para cada celda de memoria. Otros tipos de memoria son la de celda de nivel múltiple (MLC) y la de celda de nivel triple (TLC). Los factores de forma MLC y TLC proporcionan un almacenamiento de direccionamiento de dos y tres bits por celda, respectivamente. Obviamente, esto aumenta la capacidad de almacenamiento sin aumentar el tamaño del módulo de memoria.

La lógica de la memoria NAND es similar a la de las unidades de disco duro, ya que utiliza bloques para almacenar páginas que contienen archivos de datos.

Existe un controlador para gestionar los bloques de datos. Normalmente, el tamaño de un bloque es de 512 bytes, pero puede ser mayor. Los datos se escriben en la memoria a nivel de página. Ciento veintiocho (128) páginas componen el bloque si éste es de 512 bytes. A medida que el bloque se llena con páginas de datos, los datos continúan escribiéndose en una página subsiguiente ubicada dentro de otro bloque.

A medida que los datos se escriben en la memoria, el controlador gestiona la resistencia de toda la memoria NAND mediante un proceso denominado nivelación de desgaste. Este proceso gestiona los bloques de datos en toda la memoria para limitar el número de ciclos de borrado. Como todo lo creado por el hombre, la memoria NAND tiene un ciclo de vida. Escribir datos en toda la memoria flash antes de que se produzca un ciclo de borrado sería el método ideal para garantizar que las celdas de memoria alcancen la vida útil prevista.

Por desgracia, esto no es tan práctico como parece debido a los requisitos de almacenamiento de cada aplicación y a la codificación del sistema operativo. Por lo tanto, el firmware o el sistema de archivos realizan una nivelación del desgaste para reasignar automáticamente los bloques de datos con el fin de hacer un uso eficaz de la mayor cantidad de memoria con el menor número de ciclos de borrado.

Cuando se selecciona un archivo para ser borrado, el proceso de borrado ocurre a nivel de bloque. Si un fichero ocupa un bloque completo, las páginas que contienen los datos vuelven al estado '1', o borrado. Esto significa que si un fichero marcado para borrado en el sistema de ficheros no ocupa un bloque completo. Ese archivo, aunque no sea visible para el usuario a nivel lógico, puede recuperarse a nivel físico.

La memoria flash NAND se fabrica en varias formas denominadas 'die' para adaptarse a las necesidades del sistema, cada una de ellas con un número variado de pines. Esto se conoce comúnmente como "paquete" de memoria, que define el número y el patrón utilizados por un módulo de memoria específico. El término "ball grid array", o BGA, se refiere a un único tipo de encapsulado. Otros tipos son: encapsulado simple en línea (SIP), encapsulado doble en línea (DIP) y encapsulado delgado de contorno pequeño (TSOP).

Una vez finalizada la investigación del dispositivo móvil presentado para su examen, ha identificado que la marca y el modelo específicos del dispositivo móvil investigado son susceptibles de recuperación de datos mediante el proceso de chip off. Teniendo en cuenta que existen dos posibles vías para realizar el chip off, ¿qué camino debe seguir?

Para ayudarle en el proceso de toma de decisiones, analizaremos cada técnica con más detalle.

**Chip off - Técnica de flujo de calor**

La técnica de flujo de calor, tal y como se ha definido, requiere el uso de una mayor temperatura de los componentes para alcanzar la velocidad de flujo de la soldadura. El módulo de memoria se fija a la placa de circuito impreso mediante una matriz de bolas de soldadura (BGA). Es a través de la BGA que las señales se dirigen al módulo de memoria. Cuando se alcanza la velocidad de flujo de la soldadura, el módulo de memoria se retira de la placa de circuito impreso. Si se hace correctamente, el BGA se levantará en el módulo de memoria y se verán los "zócalos" vacíos en la PCB.

Este proceso es sencillo en teoría, pero requiere conocer el módulo de memoria y el umbral térmico que el fabricante ha identificado para él. En pocas palabras, si sobrecalienta el módulo de memoria, el controlador integrado y las celdas de memoria que contiene se dañan y no se pueden leer. Por lo tanto, es necesario investigar cada módulo de memoria para averiguar el umbral térmico antes de iniciar el proceso de flujo de calor. El umbral térmico de una determinada matriz se encuentra en la hoja de datos del módulo de memoria específico.

Una vez identificado el umbral térmico del módulo de memoria, se puede iniciar el proceso de chip off. Mediante el uso de aire caliente forzado, o una lámpara de calor infrarrojo que se ajusta a la temperatura mínima del umbral térmico. El módulo de memoria se calienta y posteriormente se separa de la placa de circuito impreso. Aunque no es necesario, se recomienda el uso de un precalentador, ya que calentar la placa de circuito impreso antes de aplicar calor al módulo de memoria proporcionará el mayor porcentaje de éxito.

En los procesos de separación mecánica, la placa de circuito impreso se separa del módulo de memoria extrayéndola poco a poco. Para ello se suele utilizar una fresa de mesa o un disco de pulir de joyero. La placa de circuito impreso se separa del módulo de memoria, lo que permite conectarla a la rejilla de bolas que conecta el módulo de memoria a los zócalos correspondientes de la placa de circuito impreso. Debe extremarse el cuidado para asegurarse de que la placa de circuito impreso se retira uniformemente para evitar dañar el módulo de memoria penetrando en el encapsulado de la matriz.

Una vez separado el módulo de memoria de la placa de circuito impreso, debe establecerse una conexión con los puertos de comunicación del módulo de memoria que se encuentran dentro de la matriz de rejilla. Esto se establece más fácilmente mediante el uso de adaptadores de zócalo de prueba. Sin embargo, también se puede realizar mediante el uso de conexión directa utilizando soldadura, o la Tabla VR, o el Kit CODED.

**Chip off - Técnica mecánica**

El adaptador Sireda resulta muy práctico para leer memorias flash de tipo MultiMedia Controller (eMMC), MultiChip Package (eMCP) y Universal Flash Storage (UFS). El adaptador Sireda utiliza el controlador integrado del módulo de memoria para comunicarse a través de puertos de bus serie universales (USB). Esto facilita el uso de dispositivos de bloqueo de escritura entre el sistema forense y el módulo de memoria.

Cada tipo de paquete requiere su propio adaptador de zócalo de pruebas para comunicarse eficazmente. Como alternativa, existen varios programadores de chips que permiten leer los datos almacenados en los distintos módulos de memoria. Algunos ejemplos son el UP-828P y el XelTec SuperPro.

Al igual que con los adaptadores de zócalo de prueba Sireda, el programador requerirá un adaptador específico para el paquete que se está procesando. Cuantos más tipos de encapsulados se quieran procesar por chip off, más adaptadores se necesitarán. Este punto se plantea porque algunos de los adaptadores no son baratos

y la decisión repercutirá en el retorno de la inversión.

Los programadores proporcionan versatilidad a su taller/laboratorio en cuanto a las formas de memoria que puede leer. En cambio, el adaptador de zócalo de prueba está dedicado a las formas eMMC, eMCP y UFS. Un programador puede leer estos y muchos otros. Como se mencionó anteriormente, no todas las memorias flash tienen un controlador integrado. En estos casos, se necesita un programador para establecer comunicación con la memoria, leer los datos y reconstruirlos en un formato fácil de usar para el análisis.

Existe un proceso que puede permitir la recuperación de datos de la memoria flash y que implica el uso de un microscopio electrónico. El proceso consiste en raspar finas capas de la matriz para revelar las células de memoria. Se registra el estado de cada célula, se retira otra capa y se anotan las condiciones de la célula. Este proceso continúa hasta que se han registrado todas las células de memoria. Los datos registrados se reconstruyen y se ponen a disposición para su análisis.

Este proceso no es rentable para la mayoría de las empresas debido a los gastos generales que conlleva. Se presenta para demostrar que sólo porque algo sea posible, puede no ser probable.

Independientemente del método de recuperación de datos que se utilice para documentar los datos almacenados en la memoria flash, la verificación es una necesidad.

Si los datos se extrajeron con una herramienta comercial, asegúrese de que el registro y el hash están activados.

Al avanzar por los procesos "de menos a más intrusivos", utilice procesos probados para realizar el hash de los datos y verificar las copias de trabajo posteriores antes de pasar al análisis de los datos.

**Análisis**

El procesamiento de los datos recuperados de la memoria flash se ha facilitado considerablemente con la aparición de conjuntos de herramientas comerciales. Como ya se ha indicado, cada conjunto de herramientas tiene sus puntos fuertes y sus puntos débiles, pero todas son capaces de analizar los datos identificando el formato individual del artefacto (archivo) y clasificándolos por su uso. El proceso de categorización es beneficioso para el examinador por varias razones.

La posibilidad de revisar contenedores de datos directamente relacionados con la investigación reduce la probabilidad de que el examinador o analista se extralimite en la búsqueda. En derecho penal, excederse en el ámbito de la búsqueda es una violación de la Cuarta Enmienda de la Constitución de los Estados Unidos.

En pocas palabras, se trata de una violación de los derechos civiles que, de ser perseguida, podría acarrear el encarcelamiento. Exceder el alcance de la busqueda puede manchar la evidencia que se presenta.

Por ejemplo, la investigación es relevante para la distribución ilegal de narcóticos. El alcance de la búsqueda incluye la búsqueda de datos de comunicación relacionados con estupefacientes y su distribución.

Lógicamente, el ámbito de la búsqueda incluiría cualquier forma de comunicación basada en texto, así como la comunicación de voz grabada en el dispositivo, como mensajes de voz o grabaciones de audio.

Dado que la comunicación basada en texto puede producirse a través del sistema de mensajes simples (SMS), mensajería multimedia (MMS), o una serie de Apps de terceros. Es razonable realizar una búsqueda en todas estas categorías. Una revisión de los SMS reveló artefactos de comunicación relevantes para la investigación, así como fotografías que mostraban el producto. Las fotografías se enviaron como archivos adjuntos con la comunicación basada en texto.

Si el examinador informara sobre estos artefactos y obtuviera autoridad adicional para buscar en la categoría "Archivos de imagen", todo estaría bien. Sin embargo, si el examinador sigue el rastro del archivo de imagen gráfica enviado por SMS hasta la categoría "Imágenes gráficas" y realiza una búsqueda sin obtener autorización, es probable que se excluya cualquier artefacto localizado más allá del que estaba asociado al archivo adjunto del SMS.

La pérdida de unas pocas imágenes gráficas de contrabando puede no comprometer el caso por completo. Sin embargo, sí expone al examinador a un examen crítico de su personalidad por parte del abogado defensor. Esto puede ser desagradable en el mejor de los casos, y acabar con su carrera en el peor.

En el derecho de daños, que se aplica a las empresas, el registro intrusivo podría dar lugar a un litigio civil. Un resultado común de los litigios para la parte declarada responsable es proporcionar algún tipo de compensación a la parte ofendida. Históricamente, se ha hecho de forma económica.

En ambas situaciones, el proceso de exceder la autoridad de búsqueda puede ser perjudicial para la propia investigación, los ingresos personales o empresariales y la libertad personal.

El uso de herramientas comerciales o scripts propietarios puede servir para segregar los datos categóricamente. Como se ha mencionado anteriormente, esto acelerará el proceso de revisión, proporcionará argumentos sustanciales para negar una reclamación de extralimitación y ofrecerá al examinador protección personal frente a posibles perjuicios.

El Instituto Nacional de Normalización y Tecnología (NIST) ha sometido a prueba un número considerable de herramientas comerciales a través de su Programa de pruebas de herramientas informáticas forenses para dispositivos móviles (CFTT).

Este proceso se inició como resultado del creciente número de plataformas de dispositivos móviles, la evolución de sus capacidades y la importancia que tienen en el proceso de investigación. Para más información sobre el CFTT y sus conclusiones, véase el capítulo 10, de Douglas Menéndez, "Cyber Forensic Tools and Utilities".

El uso de conjuntos de herramientas comerciales para llevar a cabo el análisis de los datos extraídos se ha convertido en la práctica habitual entre los examinadores forenses de dispositivos móviles. Debido a la creciente capacidad de memoria de los dispositivos móviles, las continuas actualizaciones de los distintos sistemas operativos móviles y el número de aplicaciones de terceros disponibles. Se ha vuelto poco razonable mantener una biblioteca personal de scripts propietarios para hacer frente a la continua evolución de los dispositivos móviles.

Esto no significa que el forense deba confiar ciegamente en los resultados de las suites de herramientas forenses.

El conocimiento de la conversión de la hora coordinada uniforme (UTC) a la hora local es esencial. Esto se debe simplemente a la observancia de la UTC por parte de las redes de servicios para documentar la transferencia de datos.

Dado que las suites forenses comerciales hacen referencia a la hora local del sistema forense en el que están instaladas. La anotación de la zona horaria desde la que se utilizaron las pruebas puede repercutir en la exactitud de las marcas de tiempo notificadas en los datos analizados. Algunas suites de herramientas comerciales ofrecen la posibilidad de convertir a la hora local o de mantener el sesgo horario registrado que observaba el dispositivo en el momento de la incautación. Se trata de un elemento importante a tener en cuenta, especialmente si la hora del sistema forense no se gestiona correctamente.

La ordenación cronológica de los datos es uno de los métodos más eficaces dentro del proceso de análisis. Localizar la categoría de datos que está dentro de la autoridad de búsqueda y ordenar cronológicamente puede revelar información sustantiva procesable en el menor tiempo posible. Posteriormente, pueden localizarse artefactos relacionados con el incidente en cuestión, pero que anteriormente no habían sido cubiertos.

**Ejemplo de caso**

Haciendo referencia al ejemplo de infracción en materia de estupefacientes presentado anteriormente. Un SMS reveló una comunicación basada en texto, así como fotografías del producto. Mediante orden cronológico, se documentó el mensaje original enviado al destinatario "A". Una revisión cronológica posterior revela un mensaje entrante de la parte remitente "B" con fotografías adjuntas. La fecha del mensaje es posterior a la del mensaje inicial enviado al destinatario "A". En este mensaje se solicita más información sobre la disponibilidad del producto que aparece en las fotografías.

El examen de las fotografías revela una similitud de "contenido" con las fotografías originales enviadas anteriormente a "A". Un análisis más detallado de las fotografías recibidas permitió identificar metadatos en ellas. De los metadatos se desprende una similitud adicional en forma de sello(s) de fecha y modelo de cámara que asocia los dos conjuntos de fotografías.

Finalmente, un análisis hash de los dos conjuntos de fotografías valida que los dos conjuntos de fotografías son, de hecho, el mismo.

Mediante la realización de la clasificación cronológica, se identificó a un sujeto adicional asociado a la denuncia original.

Mediante prácticas de análisis forense digital aplicables tanto en informática forense como en dispositivos móviles, se establecieron declaraciones de hechos.

**Atribución de usuarios**

Otro aspecto de gran importancia en el proceso de análisis es el de la "atribución al usuario".

¿Qué datos del dispositivo pueden ser relevantes para asociar al usuario del dispositivo con los datos almacenados en el mismo? Obviamente, la información de identificación personal (PII), que puede consistir en nombres completos, direcciones, números de tarjetas de crédito y la información de sus cuentas, con cualquier archivo de imagen gráfica que represente "selfies", permiso de conducir o información de la Seguridad Social, puede utilizarse para identificar al propietario del dispositivo. Sin embargo, esto no proporciona información suficiente para asociar datos específicos al propietario.

La atribución al usuario se establece mediante un proceso metódico. Seguir el adagio de investigación "quién, qué, cuándo, dónde, por qué y cómo" sirve de guía para establecer la atribución del usuario.

La siguiente lista se ofrece para una mejor comprensión y aplicación:

- ¿Quién lo hizo?

- ¿Qué se hizo?

- ¿Cuándo ocurrió?

- ¿Dónde ocurrió?

- ¿Por qué ocurrió?

- ¿Cómo ocurrió?

Esta lista se presenta en orden cronológico de ocurrencia, pero no necesariamente de descubrimiento.

Cuando se recibe una denuncia, las fases "Qué" y "Cuándo" se descubren al menos parcialmente. Por lo tanto, el proceso de investigación se parece mucho a un rompecabezas.

Algunas respuestas son obvias y se obtienen con relativa rapidez, mientras que otras requieren un esfuerzo considerable para encontrarlas, si es que se encuentran. Se necesita un análisis de los artefactos utilizados para responder a las preguntas antes mencionadas para llegar a un argumento concluyente de hecho.

Volviendo al ejemplo de la investigación sobre estupefacientes, en primer lugar validamos la denuncia o "qué ha ocurrido". Usando el artefacto o artefactos localizados dentro del dispositivo que están asociados a la denuncia.

Ampliar gradualmente el análisis a partir del artefacto o artefactos específicos en un esfuerzo por identificar el "Cuándo" y el "Cómo" se almacenó el artefacto.

A partir de ahí, determine qué estaba procesando el sistema operativo en el momento en que se almacenó el artefacto para obtener pistas adicionales.

Si el dispositivo estaba conectado a WiFi, ¿se ha registrado el identificador del conjunto de servicios (SSID) o el identificador básico del conjunto de servicios (BSSID)?

Esto podría aclarar el "dónde". ¿Se utilizaron comunicaciones basadas en texto o la cámara? Esto puede ser tanto un "cómo" como un "qué".

¿Alguna de estas aplicaciones almacena información que pueda hacer referencia a una ubicación geográfica? Si es así, esta información es otra forma de "dónde" y posiblemente de "cuándo".

Tras la identificación del sujeto "A" y del sujeto "B" a través de la actividad SMS. ¿Existe información relacional que ayude a su identificación positiva? Este sería otro "quién". Además, el análisis de la duración de conservación de los mensajes, el programa de copias de seguridad del dispositivo y el método de copia de seguridad pueden resultar relevantes.

Bases de datos SQLite

Una nota final sobre el proceso de análisis. Anteriormente, he indicado que los dispositivos móviles han integrado el uso de bases de datos como soporte de las aplicaciones. Esta práctica ha proporcionado al examinador una estructura más estandarizada para analizar, lo que supone una gran mejora con respecto a la variedad de formatos de archivo utilizados anteriormente para almacenar datos. Por ello, una herramienta importante que debe poseer el examinador moderno es la capacidad de interrogar bases de datos SQLite.

Las bases de datos SQLite son autónomas y pueden almacenarse como un archivo dentro del sistema de archivos. Se han convertido en un estándar tanto en el sistema operativo nativo como en el desarrollo de aplicaciones de terceros. Como tales, se utilizan para almacenar la agenda telefónica (lista de contactos), el historial de llamadas, SMS, MMS, mensajería instantánea, así como una variedad de redes sociales y procesos específicos de aplicaciones de terceros.

Una clave para localizar las bases de datos SQLite es realizar una búsqueda en los datos extraídos del término "SQLite format 3".15. Este es el indicador de cabecera de este tipo de base de datos. Si se completa la búsqueda con este término, aparecerán todos los archivos que contengan ese encabezado. Esto incluiría bases de datos asociadas a aplicaciones previamente desinstaladas.

Algunas suites de herramientas forenses realizan esta búsqueda como parte de su código de procesamiento; sin embargo, yo soy un examinador del tipo "verificar pero confiar" y he convertido esta búsqueda en un hábito.

La base de datos SQLite se compone de tablas que contienen columnas que describen las filas de datos introducidos bajo los encabezados de columna. Cuando se crea, la base de datos puede depender de archivos adicionales que proporcionan cierta redundancia para la base de datos. Dichos ficheros son el Write Ahead Log (WAL) y el fichero Journal.

El WAL se crea (opcionalmente) y se utiliza como ubicación para almacenar los nuevos datos destinados a la base de datos. Tras un número determinado de cambios de página, los datos contenidos en el archivo WAL se escriben en la base de datos. El Journal se crea por defecto y almacena los datos originales. Mantiene los datos originales para proporcionar redundancia en caso de que la base de datos sufra un error y requiera restauración.

Si se crea, el WAL se utiliza para almacenar datos mientras el sistema operativo gestiona servicios para mejorar la experiencia del usuario. Por ejemplo, se está creando un mensaje de texto mediante SMS. El remitente escribe "Esto es un mensaje", pero le interrumpe una llamada de voz. La WAL ha grabado "Esto es un mensaje" y lo conserva sin escribirlo en la base de datos. Al terminar la llamada de voz, el remitente vuelve a la aplicación SMS y se le presenta la entrada "Esto es un mensaje". A continuación, el remitente sigue escribiendo "Esto es un mensaje que describe lo que es un WAL" y vuelve a ser interrumpido. Esta vez por una aplicación de terceros. Tras la comunicación a través de la aplicación de terceros, el remitente vuelve a la aplicación SMS y se le presenta la entrada "Este es un mensaje que muestra lo que es una WAL". El remitente vuelve a escribir y completa el mensaje como "Este es un mensaje que muestra lo que hace un archivo WAL".

La base de datos SMS se procesa y sólo tiene una entrada de mensaje que contiene la frase "Este es un mensaje que describe lo que hace un archivo WAL". Sin embargo, en un análisis del archivo WAL se localizan tres artefactos. Se trata de los tres mensajes parciales que preceden al mensaje almacenado en la base de datos. Específicamente, 'Este es un mensaje' y 'Este es un mensaje que representa lo que hace un archivo WAL.'

A través de la comparación de los mensajes activos dentro de la base de datos SMS con los registrados dentro del archivo WAL. Puede descubrirse el marco temporal durante el cual se produjo el borrado de un SMS.

Entonces, ¿cómo puedes determinar qué archivo de soporte está utilizando la base de datos SQLite que estás revisando? ¿Recuerdas el encabezado "SQLITE formato 3"? Utilizándolo como punto de partida en un editor hexadecimal, navegando a la siguiente lista de Offset identificará qué archivo de soporte está en uso.

- Archivo Journal

- Archivo Offset 18 (1 byte) = "x01" = Journaling

- Archivo Offset 19 (1 byte) = "x01" = Journaling

- Registro de escritura anticipada (WAL)

- Archivo Offset 18 (1 byte) = "x02" = WAL

- Archivo Offset 19 (1 byte) = "x02" = WAL

En referencia a la importancia que le di a la ordenación cronológica durante mi análisis. El método de registro del tiempo en las distintas bases de datos SQLite depende del tipo de sistema operativo utilizado.

Entiéndase, el valor representado se supone que es un equivalente matemático del Tiempo Uniforme Coordinado. Pero se representa según la representación numérica soportada por el sistema operativo.

Ejemplos de representaciones numéricas comúnmente encontradas son:

- UNIX Epoch que consiste en un número de 10 dígitos que representa el número de segundos desde el 1 de enero de 1970 a las 00:00:00 horas (01/01/1970 00:00:00)

- UNIX Epoch Milliseconds es un número de 13 dígitos que representa el número de milisegundos desde el 1 de enero de 1970 a las 00:00:00 horas (01/01/1970 00:00:00)

- La hora absoluta Mac es el número de segundos transcurridos desde el 1 de enero de 1971 a las 00:00:00 horas (01/01/2001 00:00:00). Se representa mediante un número de 9 dígitos. El tiempo absoluto Mac también se almacena en un número de 18 dígitos. Cuando se encuentra, representa los nanosegundos transcurridos desde el 1 de enero de 1971.

Cada una de las suites de herramientas forenses enumeradas anteriormente ofrece análisis de bases de datos SQLite. Algunas incluyen visores para revisar las tablas de la base de datos en un formato de base de datos nativo que también incluye la opción de exportar tablas o contenidos específicos para la elaboración de informes. Algunas también incluyen herramientas forenses SQLite que permiten al examinador crear y ejecutar consultas para agilizar los procesos de búsqueda, así como crear informes que reflejen "nombres fáciles de usar" que describan el contenido de las columnas individuales dentro de una tabla documentada.

Como en el caso de la memoria flash, la forma y la función de la base de datos SQLite exceden la extensión de nuestro análisis. Para más información, visite el sitio web de SQLite: <https://sqlite.org>.

Al igual que con cualquier proceso, la formación y la práctica son necesarias para llegar a ser competente. Puede obtener más información en las siguientes fuentes:

- www.tutorialspoint.com/sqlite/

- www.sqlitetutorial.net/

- sandersonforensics.com

**Elaboración de informes**

Debe prepararse un informe que refleje la sinopsis del caso y el estado en que se recibió el dispositivo móvil.

En la narración se deben registrar los pasos dados para identificar el dispositivo móvil, así como el método o métodos utilizados para documentar los datos almacenados recuperados del dispositivo.

Si se trata de procesar contrabando que contiene imágenes ilícitas, la descripción debe hacer referencia a un informe de artefactos que contenga los archivos reales identificados como pruebas para la investigación.

El informe de artefactos resultante del análisis de un dispositivo móvil debe incluir todos los artefactos que representen los hechos representados por los datos.

Utilizando un formato cronológico, prepare el informe para describir el suceso desde su inicio hasta su finalización.

Esto puede incluir información posterior al incidente que pueda respaldar el "conocimiento y la previsión", como artículos de noticias consultados en Internet.

Si se puede identificar la atribución al usuario, hay que asegurarse de que se represente con claridad. Los artefactos pueden documentarse en formato HTML o PDF, dependiendo del destinatario. Ambos formatos son compatibles con las herramientas comerciales.

RESUMEN

En este capítulo se ha presentado información sobre las similitudes y diferencias entre la investigación forense de ordenadores y la de dispositivos móviles. Se han analizado los factores de forma de los teléfonos móviles, sus sistemas operativos y su memoria.

Se definió la identificación de dispositivos móviles que se utiliza para asociar un dispositivo específico a una red de servicio y se proporcionó una descripción de la topografía de la red celular.

A continuación, se pasó al proceso forense que sigue los pasos de incautar, asegurar, identificar, recuperar, analizar e informar. En cada una de estas secciones se proporcionó orientación sobre el mejor método que debía utilizarse para completar cada sección del proceso. Se proporcionó información complementaria para ayudar a determinar el mejor proceso a seguir en función de las condiciones existentes en el dispositivo móvil en relación con la investigación.

Este cuerpo de trabajo se ofrece a usted después de 15 años de experiencia forense digital para la aplicación de la ley. El trabajo contiene sugerencias relativas al proceso de recuperación de datos de dispositivos móviles. El aspecto de recuperación de datos del proceso forense se ha vuelto cada vez más difícil debido a las mejoras en las políticas de seguridad del propio dispositivo móvil, así como a las disposiciones de actos legislativos como la Ley de privacidad de las comunicaciones electrónicas (ECPA) y el Reglamento general de protección de datos (GDPR). Los cambios legislativos crean una relación casi adversa entre las comunidades de fabricantes y forenses cuando se intenta identificar la "verdad" que puede existir en un dispositivo móvil. El proceso continuará gracias al conocimiento de las diversas técnicas de recuperación y a la puesta en práctica de nuevas técnicas.

## [ACRONYMS](#_bookmark25)

AES Advanced Encryption Standard BGA Ball Grid Array

BLOBs Binary Large Objects

BREW Binary Runtime Environment for Wireless BSSID Basic Service Set Identifier

CDMA Code Division Multiple Access

CFTT Computer Forensics Tool Testing Program, Mobile Devices CPU Central Processing Unit

CRCs Cyclical Redundancy Checksums DIP Dual Inline Package

eMCP embedded MultiChip Package eMMC embedded MultiMedia Controller ESE Extensible Storage Engine

ESN Electronic Serial Number FBE File-Based Encryption

FCC ID Federal Communications Commission Identification FDE Full Disk Encryption

FVE Full Volume Encryption

GSM Global System for Mobile communication GUI Graphical User Interface

IC Integrated Circuit

ICCID Integrated Circuit Card Identifier IoT Internet of Things

IMEI International Mobile Equipment Identity IMSI International Mobile Subscriber Identity ISP In System Programming (Processing) IPSW iPhone Software

JTAG Joint Test Action Group Ki Authentication Key

L33T Also ‘L337.’ Is really ‘leet,’ a corruption of ‘elite’ and meaning someone who is very good at what they do

LTE Long-Term Evolution MEID Mobile Equipment Identifier MLC Multi-Level Cell

MMS Multimedia Messaging

MSISDN Mobile Station International Subscriber Directory Number NIST National Institute for Standards and Technology

OS Operating System

PCB Plastic Controller Board

PII Personally Identifiable Information PLIST Preference Lists

SIM Subscriber Identification Module SIP Single Inline Package

SLC Single-Level Cell

SMC Surface-Mounted Component SMS Simple Message System

TAC Type Allocation Code TAP Target Access Point TAPS Test Action Points TCK Test Clock

TDI Test Data In

TDO Test Data Out

TDMA Time Division Multiple Access TLC Triple-Level Cell

TMS Test Mode Select

TRST Test Reset

TSOP Thin Small Outline Package UFS Universal Flash Storage USB Universal Serial Bus

UTC Uniform Coordinated Time VIN Vehicle Identification Number WAL Write Ahead Log

WiFi A trademarked phrase that refers to IEEE 802.11x standards XML Exchange Markup Language

## [NOTES](#_bookmark25)

1. (n.a.), (June 12, 2019), “Mobile Fact Sheet,” Pew Research Center, Internet & Technology, [www.](http://www.pewresearch.org/) [pewresearch.org/internet/fact-sheet/mobile/](http://www.pewresearch.org/), retrieved June 10, 2020.
2. Cynthia, D., Murphy, A., (2013), “Developing Process for Mobile Device Forensics.” digital- forensics.sans.org/media/mobile-device-forensic-process-v3.pdf, retrieved July 7, 2020.
3. Rouse, M., (November 16, 2010), “What Is BREW (Binary Runtime Environment for Wireless)? - Definition from WhatIs.com.” SearchMobileComputing, searchmobilecomputing.techtarget.com/ definition/BREW, retrieved November 20, 2020.
4. Hoog, A., (June 15, 2011), Android Forensics: Investigation, Analysis, and Mobile Security for Google Android, 1st edition, ISBN-13: 978-1597496513, Waltham, Ma: Syngress.
5. Mishra, P., (2020), “Joint Test Action Group (JTAG): Definition, Uses & Process | Study.com” Study.com,” study.com/academy/lesson/joint-test-action-group-jtag-definition-uses-process.html., retrieved July 12, 2020.
6. Image, JTAG Pinout ZTE Z222, provided courtesy of the Author.
7. Image, JTAG Emulator Connector To Daughter Board, courtesy of the Author.
8. Image, Z3X Extraction, courtesy of the Author.
9. Image, Close-Up View of SMD Connections, courtesy of the Author.
10. Image, Reverse Engineering of Coolpad 3632A, courtesy of the Author.
11. Image, The CODED, courtesy of the Author.
12. Schwarz, T., (2003), “COEN 180.” Www.Cse.Scu.Edu, [www.cse.scu.edu/~tschwarz/coen180/LN/](http://www.cse.scu.edu/) [flash.html](http://www.cse.scu.edu/)., retrieved June 29, 2020.
13. Painter, Z., (April 12, 2018), “The Basics of NAND Flash Memory Technology | Silicon Power.” Silicon Power Blog. April 12, 2018. [www.silicon-power.com/blog/index.php/guides/nand-flash-](http://www.silicon-power.com/) [memory-technology-basics/](http://www.silicon-power.com/)., retrieved June 29, 2020.
14. Ayers, R. (n.d.), “Mobile Device Forensics – Tool Testing.” [www.nist.gov/system/files/docu-](http://www.nist.gov/) [ments/2017/05/08/mobiledeviceforensics-mfw08.pdf](http://www.nist.gov/), retrieved June 16, 2020.
15. Sanderson, P., (May 12, 2018), SQLite Forensics, Edited by Richard Hipp, Heather Mahalik, Brett Shavers, and Eric Zimmerman. 1st ed., ISBN-13 : 978-1980293071.
16. Ibid.