UNIVERSIDAD MICHOACANA DE SAN NICOLÁS DE HIDALGO

FACULTAD DE INGENIERÍA ELÉCTRICA

LA EVIDENCIA DIGITAL FORENSE USANDO UFED DE CELLEBRITE

REPORTE DE EXPERIENCIA LABORAL

PARA OBTENER EL TÍTULO DE INGENIERO EN COMPUTACIÓN

PRESENTA
SERGIO RAMÍREZ MÉNDEZ

ASESOR
MTRO. GALILEO CRISTIAN TINOCO SANTILLÁN

MORELIA, MICHOACÁN ENERO DE 2021

AGRADECIMIENTOS

Empezare expresando mi agradecimiento a mi familia. Sin ellos no habría podido llegar a este punto. He necesitado su cariño, comprensión y su apoyo incondicional en unas dosis extraordinariamente elevadas. Mi padre **Sergio** y mi madre **María Teresa** (que ya no se encuentra con nosotros, pero sé que has estado al pendiente de mí, te amo mamá), y de mis hermanos **Daniel** y **David** han sido, por así decirlo, los cimientos sobre los que se apoya este reporte de experiencia laboral. Tampoco puedo olvidarme del resto de mi familia, que me ha apoyado y comprendido en todo momento. En este periodo tan largo y, en ocasiones, tan difícil, han logrado que siguiera avanzando hacia mi objetivo.

Este trabajo no se habría podido realizar sin la colaboración de muchas personas que me han brindado su ayuda, sus conocimientos y su apoyo. Quiero agradecerles a todos ellos cuanto han hecho por mí, para que este trabajo saliera adelante de la mejor manera posible. Quedo especialmente agradecido y hago una mención especial al **M.C. Galileo Cristian Tinoco Santillán** por ser mi asesor de experiencia laboral, el cual me ha ayudado y apoyado en todo momento, ha corregido minuciosamente este trabajo y me dado la posibilidad de mejorarlo, tengo que agradecerle sus comentarios, direcciones, sugerencias y las correcciones con las que he podido elaborar una adecuada memoria de todo el trabajo realizado durante estos últimos dos años. Y en general a mis docentes académicos, que fueron parte esencial para desarrollarme como profesionista, a cada uno de ellos gracias por su tiempo y por los consejos que me brindaron.

Quedo infinitamente agradecido por todo el apoyo incondicional y sus consejos dentro y fuera de lo laboral. Químico Julio, le agradezco por ser parte fundamental en mi vida profesional, y todos y cada uno de mis colegas,

Y he dejado de nombrar a muchas personas que me han ayudado de una forma u otra en este trabajo, en gran parte para no extenderme en exceso. Ellos ya saben quiénes son y tienen mi más sincera gratitud por todo.

DEDICATORIA

A mis padres Sergio y María Teresa quienes con su amor, paciencia y esfuerzo me han permitido llegar a cumplir hoy un sueño más, gracias por inculcar en mí el ejemplo de esfuerzo y valentía, de no temer las adversidades y nunca rendirme e ir por todo.

A mis hermanos Daniel y David por su cariño y apoyo incondicional, durante todo este proceso, por estar conmigo en todo momento gracias. A toda mi familia porque con sus oraciones, consejos y palabras de aliento hicieron de mí una mejor persona y de una u otra forma me acompañan en todos mis sueños y metas.

A mi esposa Alejandra, que siempre ha estado en las buenas y en las malas, su apoyo y su amor es incondicional. Te amo.

Finalmente quiero dedicar este reporte laboral a:
Al Combo Cuates: Gerardo Ulises, Jonathan, Guillermo, Emmanuel, Enrique.
Al club de Wolfs: Carlos, Saúl Santiago y Valeria.

A mis profesores M.A. Enrique Manuel Báez, M.C. Luis Ernesto Ceja Martínez, C.P. Jorge Soto, M.I. Cuauhtémoc Gómez Suarez, Dr. Juan José Flores Romero.
Al maestro Rodrigo y mi jefe QFB. Julio Cesar, a mis colegas Nancy y Claudia. Por permitirme ser parte del equipo de trabajo de UECS.

A todos por apoyarme cuando más las necesito, por extender su mano en momentos difíciles y por el amor brindado cada día, de verdad mil gracias, siempre los llevo en mi corazón.

RESUMEN

Mi experiencia profesional la inicie en junio de 2018 justo al terminar mis materias en la Facultad de Ingeniería Eléctrica, y la he adquirido en el área gubernamental dentro de la Fiscalía General del Estado, antes llamada Procuraduría General de Justicia en el área de Servicios Periciales de la Unidad Especializada en Combate al Secuestro, realizando dictamines e informes de análisis de videos, capturando y almacenando muestras de voz y extracción de información forense de dispositivos de comunicación (celulares).

Mis primeros pasos fueron conocer el sistema pericial, como y de que se conformaban las funciones de un perito, principalmente le brindamos servicios al Gobierno del estado por medio de la Fiscalía General del Estado; mis funciones principales fueron en el área de Evidencia digital, ahí realizaba La extracción y análisis forense de evidencia digital en teléfonos celulares inteligentes permite obtener pruebas auténticas e íntegras, que aporten como pruebas en un estrado frente a un proceso judicial, de igual manera como se realiza con los elementos de computación desde hace algunos años.

Posteriormente me dedique a realizar análisis de video y fotografía, el cual la función básica es investigar e identificar los tipos de parámetros como son el tipo de archivo, el peso, el día de creación, etc. Finalmente, he recibido capacitaciones constantes dentro del ámbito del cual laboro obteniendo certificados con valor curriculares.

Seguridad, Extracción, Información, Telefonía, Tecnología

ABSTRACT

My professional experience began in June 2018 right after finishing my classes at the Electrical Engerineering Faculty. Such experience has been in the governmental field at the Fiscalia General del Estado, formerly known as Procuraduria General de Justicia, specifically in the department of Servicios Periciales de la Unidad de Secuestro. My tasks within that department include doing video expert opinions, known as Dictamenes, video analysis reports, capturing and storing voice samples and doing forensic information extraction from communication devices (cell phones).

My first steps were learning the Pericial system, what the role of a proficient included and how to achieve the tasks included within that role. We primarily provide services to the State Government through the State Attorney Fiscalia General del Estado. My primary role was in the area of digital evidence where I would do extraction and forensic analysis of digital evidence on smart cell phones, which allowed for authentic and reliable information that could be presented as part of judicial process similar to the way it has been done with computer elements for many years now.

Prior to my experience in the governmental field, I used to do video and photography analysis where my primary role was to investigate and identify different parameters such as file type, size, date created, etc. Finally, I have received constant training in the field I work in, allowing me to receive various certifications.

CONTENIDO

AGRADECIMIENTOS ____ ***2***

DEDICATORIA ____ ***3***

RESUMEN ____ ***4***

ABSTRACT ____ ***5***

CAPÍTULO 1. INTRODUCCIÓN ____ ***7***

Antecedentes. ____ 7

Teléfonos Inteligentes (Smartphones) ____ 8

CAPÍTULO 2. EVIDENCIA DIGITAL ____ ***9***

2.1. Metodología ____ 9

2.2. Infraestructura Telefonía Celular ____ 9

2.3. Evidencia digital en teléfonos con tecnología GSM ____ 10

2.4 Evidencia Digital en los Teléfonos Inteligentes (Smartphone) ____ 11

2.5. Evidencia Digital en la Tarjeta SIM (Módulo de Identidad del Suscriptor, por sus siglas en Ingles) ____ 11

2.6. Técnicas de Extracción de Evidencia Digital en Teléfonos Celulares. ____ 13

2.7. Protección de la Información. ____ 15

CAPÍTULO 3. HERRAMIENTAS PARA EXTRACCIÓN DE INFORMACIÓN ____ ***16***

3.1 Oxygen Forensic ____ 16

3.2 CellDEK Logicube ____ 19

3.3 Cellebrite UFED Physical Analizer ____ 20

3.4 Xry Complete ____ 21

3.5 Mobile PhoneExaminer ____ 22

CAPÍTULO 4. EXTRACCIÓN DIGITAL CON UFED 4PC ____ ***24***

4.1 Introducción ____ 24

4.2 Extracción lógica ____ 29

4.3. Extracción del sistema de archivos ____ 37

4.4 Extracción física ____ 46

4.5. Physical Analizer ____ 52

5. CONCLUSIONES ____ ***58***

OPORTUNIDADES DE MEJORA ____ 59

Lista de Figuras ____ ***60***

Lista de Tablas ____ ***61***

Lista de Símbolos y Abreviaturas ____ ***61***

Bibliografía ____ ***62***

CAPÍTULO 1. INTRODUCCIÓN

Antecedentes.

Desde el inicio de la civilización moderna hasta nuestros días, la necesidad de comunicación del ser humano lo ha motivado a desarrollar sistemas cada vez más sofisticados, que le permitan satisfacer dicha necesidad, incorporando recientemente conceptos de movilidad y por ende inalámbricos. Es por esta razón que las comunicaciones inalámbricas móviles representadas principalmente por la telefonía celular, se han convertido en uno de los ejes más destacados de las telecomunicaciones a nivel global. Es tal su crecimiento que la Unión Internacional de Telecomunicaciones (UIT) afirmó en un reciente informe que para 2014 existirán más suscripciones de telefonía móvil que habitantes en el mundo alcanzando una cifra cercana a los 7 mil millones de abonados. De otro lado, los teléfonos celulares ya no son utilizados tan solo para tareas tradicionales como hacer y recibir llamadas, enviar y recibir mensajes, sino que la mayoría de ellos proveen las mismas funcionalidades que brinda una computadora de escritorio e inclusive las capacidades unidas de un computador de escritorio, la resolución de audio y video de un reproductor de Blue-Ray e inclusive funciones de reconocimiento de voz, reconocimiento biométrico y demás funcionalidades antes no imaginable en dispositivos tan pequeños y portables. Todo lo anterior explica porque los celulares inteligentes (smartphones) son hoy en día una valiosa fuente de evidencia en el evento de un análisis forense. Es por ello que se requiere un procedimiento adecuado tanto desde el punto de vista técnico como legal, actuando como guía para realizar un adecuado manejo de la evidencia electrónica y digital en la investigación judicial bajo la cual esté involucrado el teléfono celular.

Teléfonos Inteligentes (Smartphones)

Un teléfono inteligente, también denominado teléfono táctil (smartphone en inglés) es un teléfono móvil construido sobre una plataforma informática móvil, con una mayor capacidad de almacenar datos y realizar actividades semejantes a una mini computadora y conectividad que un teléfono móvil convencional. El término “inteligente” hace referencia a la capacidad de usarse como un ordenador de bolsillo, llegando incluso a remplazar a un ordenador personal en algunos casos. Generalmente los teléfonos con pantallas táctiles son los llamados "teléfonos inteligentes", pero el completo soporte al correo electrónico parece ser una característica indispensable encontrada en todos los modelos existentes y anunciados desde 2007. Casi todos los teléfonos inteligentes también permiten al usuario instalar programas adicionales, normalmente inclusive desde terceros (hecho que dota a estos teléfonos de muchísimas aplicaciones en diferentes terrenos). Entre otras características comunes está la función multitarea, el acceso a Internet vía WiFi o red 3G, funciones multimedia (cámara y reproductor de videos y archivos mp3), los programas de agenda, administración de contactos, acelerómetros, GPS y algunos programas de navegación así la habilidad de leer documentos de negocios en variedad de formatos como PDF y Microsoft Office. Mientras más bandas de radio soporten un smartphone, más frecuencias podrá usar. Los teléfonos de cuatro bandas, operan a lo largo de cuatro frecuencias, por lo tanto, en teoría proporcionan una mejor cobertura comparándose con cualquier otro teléfono móvil que sea tri banda, banda dual o banda simple. Estos smartphones de cuatro bandas, también han sido llamados smartphones globales, ya que son compatibles con las cuatro frecuencias GSM prevalentes en todo el mundo, por lo cual pueden funcionar en cualquier parte del mismo. Los sistemas operativos móviles más frecuentes utilizados por los teléfonos inteligentes son Android (de Google), iOS (de Apple), Symbian (de Nokia), RIM (de BlackBerry), y Windows Phone (de Microsoft). Otros sistemas operativos de menor uso son FirefoxOS (de Mozilla), Bada (de Samsung), MeeGo (de Moblin y Maemo), webOS, Windows CE, etc.

CAPÍTULO 2. EVIDENCIA DIGITAL

2.1. Metodología

Es importante que el acceso a los datos y la extracción de la evidencia sean llevados a cabo con un procedimiento correcto, sobre todo si la evidencia va a ser utilizada en juicios civiles y penales o para litigios internos en una organización.

Los elementos de prueba o evidencias dentro de un proceso judicial son de vital importancia, ya que mediante su investigación se puede llegar a determinar la confirmación o desvirtuación de una hipótesis o afirmación precedente de lo que corresponde a la verdad. La evidencia digital, es una herramienta de especial cuidado, para el proceso de investigación de delitos tecnológicos; debe ser tratada por parte de especialistas que conserven todas las medidas de precaución necesarias para no contaminarla (alterarla), con el fin que ésta no sea objeto de desestimación ante un proceso legal. Es por ello que la evidencia digital no solo está limitada a la información que se encuentra en los computadores, sino que también se extiende a todos aquellos dispositivos electrónicos, como teléfonos celulares, Tablet PC´s, reproductores MP3, memorias flash y USB (pendrives), Ipod´s, entre otros elementos de multimedia y telecomunicaciones.

2.2. Infraestructura Telefonía Celular

Con el fin de entender más fácilmente todos los elementos de hardware y los componentes de infraestructura que intervienen en la conexión de los dispositivos móviles a las redes de telefonía y a internet, se definen las siglas de sus principales componentes:

- PTSN: Red de Telefonía Pública Conmutada (PublicTelephoneSwitched Network).
- MSC: Centro de Conmutación Móvil. (Mobile Switching Center).
- BSC: Controladores de Estaciones Base. (Base StationController).
- BTS: Estación Transmisora Base. (Base TransceiverStation).
- Cells: Celdas Celulares

El siguiente grafico muestra la estructura jerárquica de los componentes y su interacción con lo cual se logra el establecimiento de la comunicación, tanto a la Red Conmutada, como a Internet

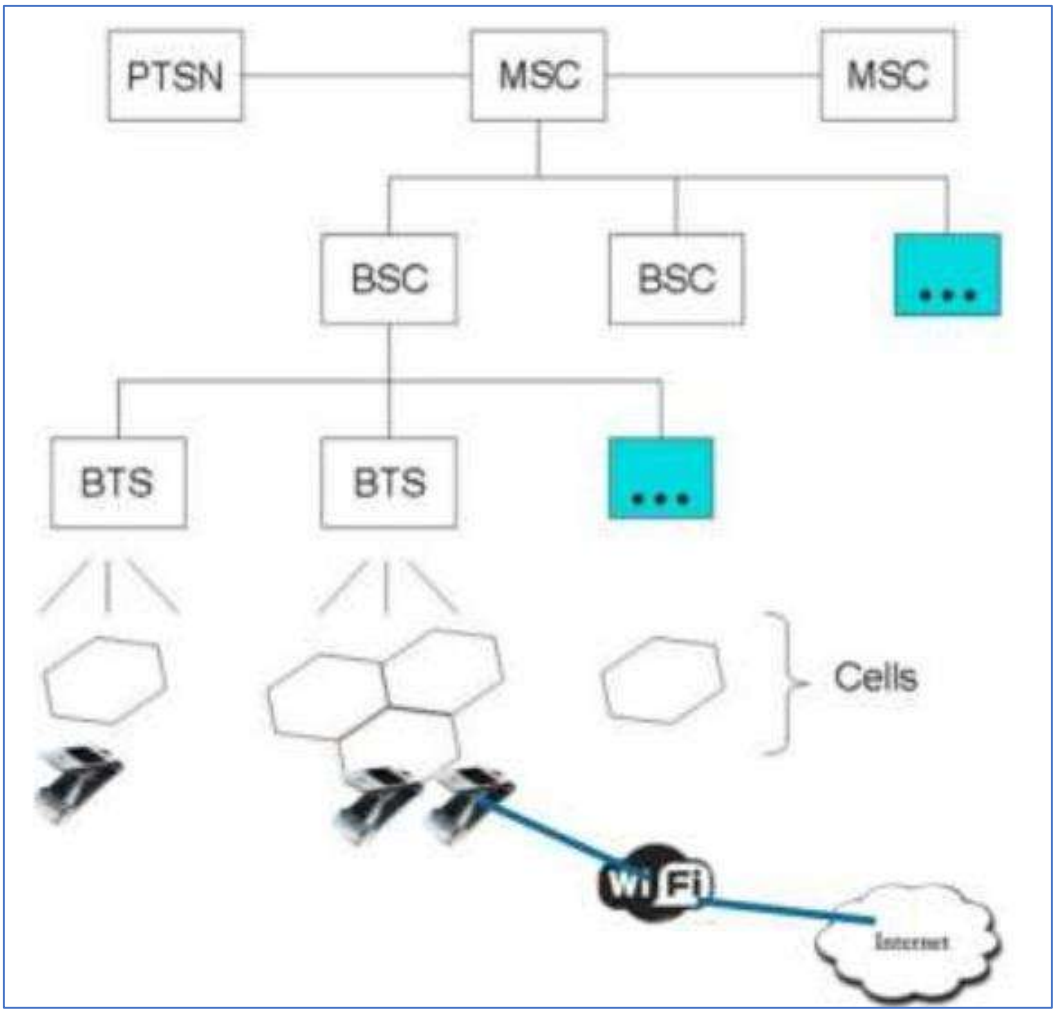


Figura 2.2.1 Estructura estándar de la telefonía móvil.

2.3. Evidencia digital en teléfonos con tecnología GSM

Dentro de la Arquitectura Instalada Fija de GSM, son de interés como evidencia digital los registros de detalles de llamadas ó CDRs (Call Detail Records), que se crean y almacenan en la central de conmutación móvil ó MSC (Mobile Switching Center) con el propósito de facturación e identificación de los controladores de estaciones base ó BSC(Base Station Controller) sobre las cuales fueron efectuadas llamadas y mensajes

de texto, además de información de tiempo y localización. Este análisis requiere de la participación en su totalidad de la Operadora de Telefonía Móvil. De otro lado la combinación del análisis de los CDRs con la estación móvil puede ayudar a establecer hechos relacionados con un acto delictivo o puede ayudar a corroborar una coartada.

2.4 Evidencia Digital en los Teléfonos Inteligentes (Smartphone)

La evidencia digital potencial, es la encontrada en las memorias del Equipo Móvil, ya que muchos fabricantes de teléfonos celulares usan la memoria interna del equipo móvil, para implementar nuevas funciones y almacenar cierta información que no puede ser almacenada en la tarjeta SIM, debido a que tienen especificaciones que permiten el almacenamiento de cierto tipo de información. En general la evidencia digital está constituida por:

- IMEI (International Mobile Equipment Identity)
- Directorio Telefónico
- Historial de Llamadas Mensajes cortos (SMS), Mensajes multimedia (MMS), buscadores Web/WAP y correos electrónicos
- Calendario
- Otros dispositivos, por ejemplo, memorias externas.

2.5. Evidencia Digital en la Tarjeta SIM (Módulo de Identidad del Suscriptor, por sus siglas en Ingles)

La tarjeta SIM contiene detalles del suscriptor móvil como el número telefónico, identificación de red codificada, el PIN y otros datos como la agenda de teléfonos. La tarjeta SIM se puede cambiar de un teléfono a otro porque contiene toda la información requerida para activar el teléfono. La Tarjeta SIM reside en la memoria permanente, el sistema de archivos está estructurado jerárquicamente. Cuenta con tres componentes

principales: el Archivo Principal o la raíz del sistema de archivos (MF), los Archivos Dedicados (DF) que son utilizados como directorios, y los Archivos Elementales (EF) que permiten el almacenamiento de los datos.

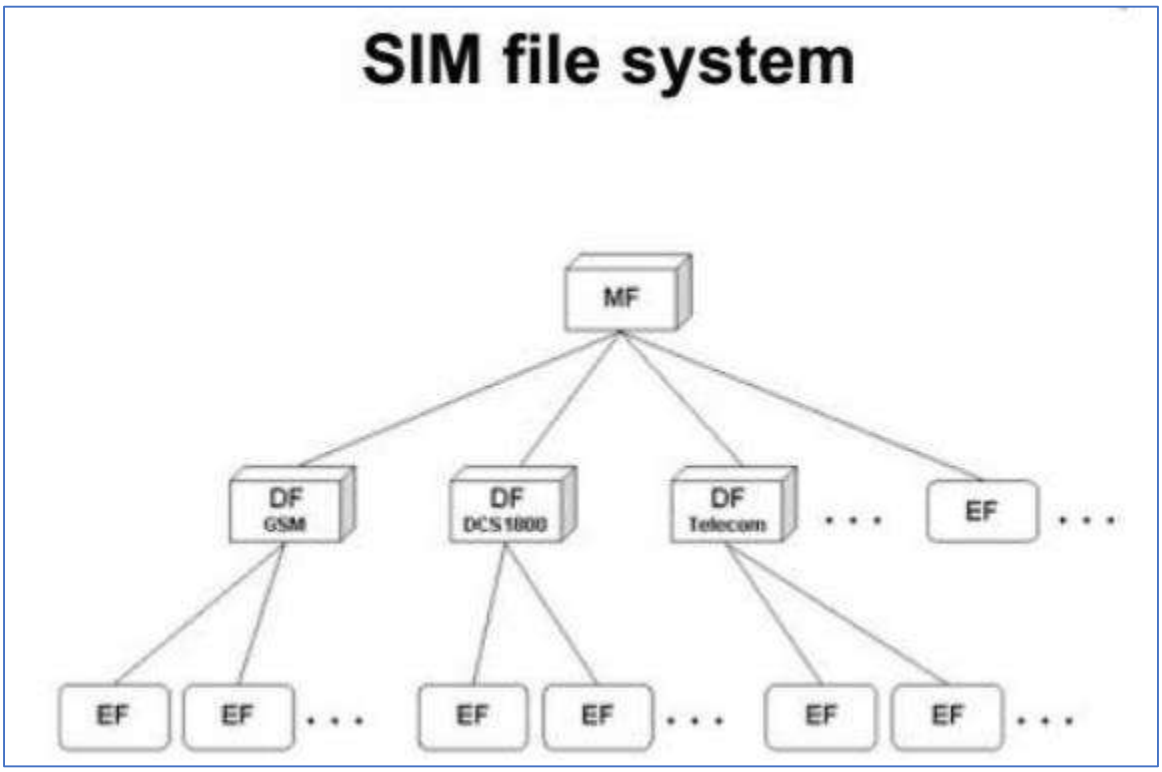


Figura 2.5.1 Sistema de archivos en la tarjeta SIM

Se muestra un esquema del sistema de archivos que suele encontrarse en las tarjetas SIM.

Los archivos no son identificados por el nombre debido a que la memoria es limitada, estos son identificados por dígitos hexadecimales que tienen 2 bytes de extensión.

Físicamente la tarjeta SIM forma parte de la evidencia electrónica, el analista forense debe tener en cuenta la información almacenada allí con el propósito de encontrar evidencia digital.

2.6. Técnicas de Extracción de Evidencia Digital en Teléfonos Celulares.

Existen dos técnicas para la extracción de evidencia digital.

a) Análisis físico: Es una copia bit a bit de una entrada física de almacenamiento (chip de memoria).
b) Análisis lógico: Es una copia bit a bit de los objetos lógicos (archivos) que residen sobre un almacenamiento lógico.

2.6.1. Técnicas de Análisis Lógico.

Las técnicas de análisis lógico para la extracción de la evidencia digital habitualmente involucran la utilización de software cuando la información se encuentra protegida por sistemas de autenticación, este software permite vulnerar estos mecanismos de autenticación, y obtener acceso a la información almacenada.

1. Extracción Manual:
   Es realizada cuando no se encontran elementos que sean compatibles ya sea en cuanto al hardware o al software de los dispositivos que a los que se les va a realizar una extracción de evidencia. Es una técnica que requiere al analista forense hacer una grabación de cada una de las pantallas que se van mostrado en el análisis.

2. Extracción Lógica:
   Se realiza utilizando los protocolos de los fabricantes y herramientas que permitan la no alteración de los datos es de solo lectura, los dispositivos móviles necesitan cables con entradas especiales dependiendo de la marca y referencia al igual que sus respectivos controladores que permiten tener conexión esto en muchos casos hace que la extracción sea más complicada.

2.6.2. Técnicas de Análisis Físico.

Este tipo de técnicas utiliza software y hardware que permite acceder a la información que se encuentra protegida por métodos de autenticación.

1. Micro Read:

Es un proceso que involucra el uso de un microscopio de alta potencia que da una vista física de los circuitos electrónicos de memoria del dispositivo móvil. Este método se utiliza mientras se obtienen los datos de los chips de memoria físicamente dañados. Este es un método costoso que permite la extracción y verificación de todos los datos de la memoria del teléfono móvil.

2. HexDump:

Esta técnica consiste en una combinación de hardware y software empleando ciertas interfaces disponibles en el teléfono celular. Se pueden utilizar cajas desarrolladas por los fabricantes para desbloquear y reprogramar el teléfono, añadiendo métodos forenses.

3. Chip-Off:

Consiste básicamente, en obtener evidencia directamente de la memoria del dispositivo celular; se lo puede hacer desoldando los componentes de memoria y leerlos en un lector o utilizando las conexiones o puntos de prueba dentro de la placa de circuitos conocidos como JTAG (Joint Test Action Group).

Figura 3. Técnicas de extracción de evidencia digital en dispositivos móviles

2.7. Protección de la Información.

La generación de huella digital o algoritmo matemático Hash es un proceso que toma un bloque arbitrario de datos y devuelve una cadena de bits de tamaño fijo (valor hash) de tal manera que cualquier cambio en los datos modificaría este valor hash. El Instituto Nacional de Estándares y Tecnología NIST (National Institute of Standards and Technology) define una adquisición consistente como dos adquisiciones consecutivas que producen diferentes hash generales de la memoria, mientras que los valores hash de los archivos individuales siguen siendo consistentes.

CAPÍTULO 3. HERRAMIENTAS PARA EXTRACCIÓN DE INFORMACIÓN

Debido a la multiplicidad de tipos de dispositivos móviles, así como sus sistemas operativos y las aplicaciones que pueden correr sobre ellos, las herramientas a utilizar dependen primordialmente del dispositivo a analizar, por lo cual es común que se presenten las siguientes situaciones:

La adquisición de datos a través de la interfaz de software del fabricante, puede ser limitada, debido a restricciones de acceso a ciertas ubicaciones de almacenamiento.

Datos importantes pueden ser omitidos en teléfonos que responden a determinado comando o protocolo. Los comandos utilizados exitosamente con un dispositivo móvil, inclusive del mismo fabricante y/o sistema operativo no necesariamente serán satisfactorios en otro dispositivo móvil, debido a los aplicativos y configuraciones personalizadas que pueden encontrarse en la escena.

3.1 Oxygen Forensic

Una gran cantidad de modelos de dispositivos móviles son compatibles con esta herramienta, Oxygen Forensic extrae datos de Nokia, iPhone, Sony Ericsson, Samsung, Motorola, Blackberry, Panasonic, Siemens y muchos otros teléfonos móviles. Utilizada en más de 50 países con éxito y en diferentes entidades nacionales como la Fiscalía General del Estado.

Oxygen Forensic Suite puede extraer una gran cantidad de información, utilizando protocolos de bajo nivel que le permiten al perito extraer:

- Información básica del teléfono y datos de la tarjeta SIM
- Lista de contactos
- Grupos de llamadas
- Marcaciones rápidas perdidas / salientes / llamadas entrantes SMS/MMS/carpetas de correo estándar, SMS / MMS / carpetas de correo personalizadas
- SMS eliminados (con algunas restricciones) y marcas de tiempo del centro de SMS
- Calendario de eventos del calendario
- Tareas
- Notas de texto

- Fotos
- Vídeos
- Sonidos
- Datos Lifeblog (todos los eventos principales del teléfono y sus coordenadas geográficas)
- Aplicaciones Java
- Sistema de archivos de la memoria del teléfono
- Tarjeta de memoria flash
- GPRS
- Actividad Wi-Fi
- Registros de voz.

Sin embargo esta lista de características soportadas depende del modelo determinado de teléfono.

Figura 4. Inicio software forensic

Realiza análisis y exportación de datos, permite la generación de informes, su Interfaz está diseñada para el análisis forense y la búsqueda de datos al igual que la presentación de informes

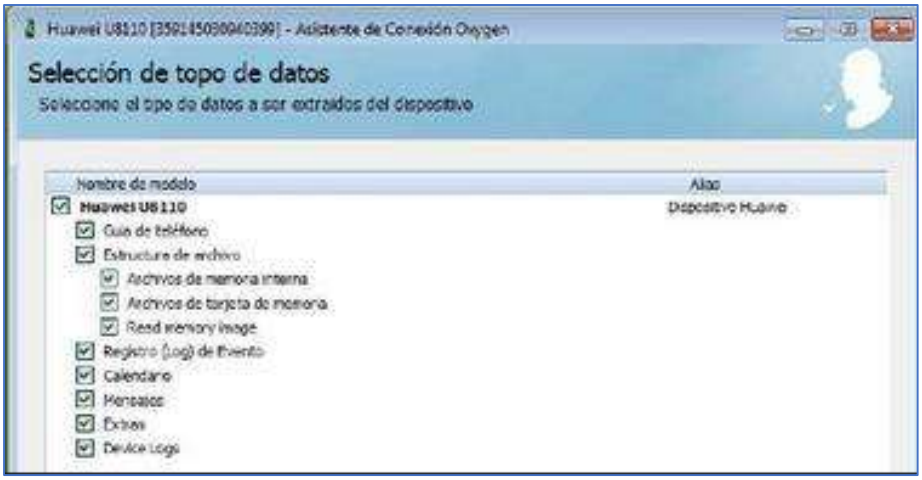


Figura 5. Tipos de datos de extracción.

Oxygen Forensic Suite exporta a los formatos de archivo más populares

Figura 6. Importar archivos copia de seguridad

No realiza modificaciones a los datos cuando se accede desde el programa y esta soportado en diferentes idiomas.

3.2 CellDEK Logicube

CellDEK ha sido el líder mundial en hardware de imagen y duplicación forense de discos duros. Cuenta con una solución forense de confianza para la extracción de evidencias digitales, recopilación de datos forenses en un entorno seguro. CellDEK de Logicube fue desarrollado para adquirir datos de los teléfonos móviles que operan a través de redes GSM y no GSM, PDA, tarjetas SIM y los medios de comunicación basados en memoria flash.

Figura 7. Hardware cellDEK

CellDEK contiene una pantalla táctil, cables de datos de diferentes dispositivos, PC/SC, un lector de tarjetas SIM y un lector de memoria protegida contra escritura. Se conecta a los teléfonos móviles y PDA mediante una conexión de cable, Bluetooth o IrDA. La información que es almacenada en el disco duro del CellDEK puede realizar copias de seguridad en memorias USB. **Utiliza el algoritmo MD5 para la obtención de Hash que garantizan la integridad de los datos para su posterior verificación.** Los informes son

generados en formato HTML donde se encuentran todos los datos recuperados, permite la edición de logotipos con el fin de personalizar los informes.

3.3 Cellebrite UFED Physical Analizer

Cellebrite ofrece extracción física y decodificación para equipos Blackberry, Nokia, iOS, Android, tablets, GPS y teléfonos chinos

Puentea cualquier tipo de bloqueo utilizando motores de arranque propios, la extracción física de estos dispositivos puede realizarse con cualquier versión de sistema operativo, sin necesidad de establecer directorios raíz; cuenta con descifrado en tiempo real

Figura 8. Equipo UFED

Aplica técnicas de descifrado y decodificación avanzadas que permiten recuperar datos eliminados desde bases de datos SQLite, mensajes, imágenes, videos, historial de llamadas, contactos. Extrae y presenta posiciones GPS, redes Wi-Fi e ID de celdas de

todos los dispositivos con iOS y muestra la información en un informe claro, puede ver las ubicaciones y las rutas en Google Earth y Google Maps.

Figura 9. UFED Touch

3.4 Xry Complete

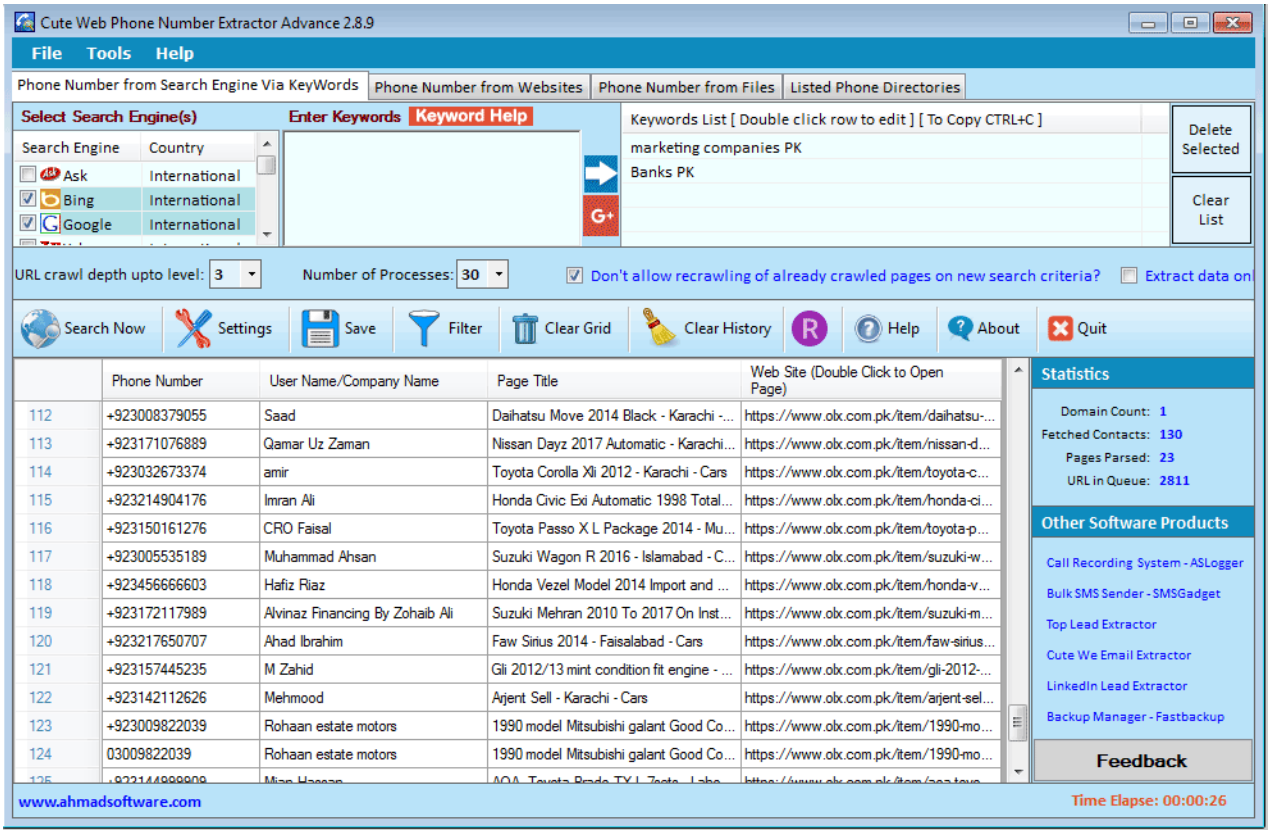
Se trata de un sistema de informática forense para dispositivos móviles “todo en uno”, que combina herramientas lógicas y físicas en un solo empaque, con lo cual brinda a los investigadores completo acceso a los métodos de recuperación de datos desde un dispositivo móvil

Gracias a esto ofrece los medios para extraer datos de dispositivos GSM y CDMA, así como las tarjetas SIM. Requiere de un dongle USB para la operación del software, el cual provee una interfaz para los cables de dongle y el dispositivo, e interfaces para Bluetooth e IrDA, Xry viene con los cables para los teléfonos compatibles, así como el

software de aplicación, la información obtenida del teléfono celular se almacena en la aplicación, su formato no se puede modificar, pero se pueden exportar a otros formatos. Xry encripta los datos de casos y compara la firma digital para mantener la integridad. Los expedientes de los casos pueden ser protegidos mediante contraseña, proporcionando seguridad adicional para evitar alteraciones, crea informes personalizados, realiza búsquedas en los datos adquiridos.

3.5 Mobile PhoneExaminer

Es una solución de software forense para móviles que se encuentra también en una versión preconfigurada en un tablet-PC que permite la portabilidad para análisis en la escena del incidente.



Mobile Phone Inspector Plus crea imágenes que se pueden integrar con la herramienta forense FTK, lo que permite integrar la evidencia forense de múltiples dispositivos móviles con la evidencia de múltiples equipos dentro de una misma interfaz.

Figura 10. Visualizacion de lineas del tiempo

MPE Soporta más de 6800 teléfonos celulares y dispositivos móviles, incluyendo iOS, Android, Blackberry, dispositivos chinos, teléfonos y dispositivos con Windows Mobile. De igual manera, permite a los analistas forenses realizar investigaciones en diferentes dispositivos móviles sin tener que adquirir una Suite adicional o módulos de software o hardware costosos y complejos. Cuenta con avanzadas opciones de filtrado y escarbado de datos, así como un amplio soporte incluso para los dispositivos móviles más exigentes, lo cual facilita el análisis detallado de la información.

CAPÍTULO 4. EXTRACCIÓN DIGITAL CON UFED 4PC

4.1 Introducción

UFED 4PC es una solución de nueva generación que ha capacitado al personal de fuerzas de seguridad, ejército, inteligencia, seguridad empresarial y descubrimiento electrónico para capturar pruebas forenses críticas procedentes de cualquier dispositivo móvil. Esto incluye teléfonos móviles, tabletas, dispositivos GPS portátiles y dispositivos fabricados con conjuntos de chips chinos, discos de almacenamiento digital (HDD, SSD), cámaras de video vigilancia, entre otras. A continuación se describirá el funcionamiento y uso del UFED de CELLEBRITE en extracciones forenses.

4.1.1 Descripción general

UFED 4PC nos permite:

- Realizar extracciones físicas, de sistemas de archivos y lógicas de datos y contraseñas del dispositivo.
- Extraer datos vitales, como registros de llamadas, entradas de la agenda telefónica, mensajes de texto (SMS), imágenes, vídeos, archivos de audio, información de ESN IMEI, ICCID e IMSI y mucho más, desde una amplia gama de dispositivos móviles.
- Extraer datos desde la más amplia selección de sistemas operativos, como Apple iOS, BlackBerry, Android, Symbian, Microsoft Mobile y Palm OS.
- Clonar el ID de la SIM, lo que le permitirá extraer datos del teléfono impidiendo que el dispositivo móvil se conecte a la red. También puede resultar útil si no se dispone de la tarjeta SIM.
- Extraer los datos de un dispositivo móvil mediante una conexión basada en cable (de serie o USB) o una conexión inalámbrica Bluetooth. El kit de cables y puntas está formado por cuatro cables maestros y varias puntas.

Los datos extraídos se guardan y generan posteriormente en formato de informes claros y concisos.

4.1.2 Requisitos del sistema

Tabla 1. Requisitos UFED

PC	PC compatible con Windows con procesador Intel i5 o compatible a 1,9 GHz o más		
Sistema operativo	Microsoft Windows 7 o superior Microsoft Windows 7 Boot Camp en MAC		
Memoria (RAM)	SO 64 bits	Recomendada 8 GB	Mínima 4 GB
Requisitos de espacio	500 MB de espacio de disco libre para la instalación		
Requisitos adicionales	Microsoft .Net versión 4.0		
Permisos	Si tiene previsto activar la aplicación mediante una clave de licencia de hardware (mochila) proporcionada por Cellebrite, debe tener derechos de administración para el ordenador		

4.1.3 Tipos de extracción y herramientas de dispositivo de UFED 4PC

UFED 4PC incluye distintos tipos de extracción de datos a los que se puede acceder a través de la pantalla Seleccionar tipo de extracción.

Tabla 2. Tipos de extracción

Funcionalidad	UFED 4PC Logical	UFED 4PC Ultimate
Extracción lógica	Sí	Sí
Extracción de datos desde SIM	Sí	Sí
Extracción de contraseñas	Sí	Sí
Clonar SIM	Sí	Sí
Extracción del sistema de archivos	No disponible	Sí
Extracción física	No disponible	Sí
Capturar imágenes e instantáneas	Opcional	Sí

En esta sección se describe los tipos de extracción:

- ***Extracción lógica:*** Permite extraer varios tipos de datos. Esto incluye registros de llamadas, entradas de la agenda telefónica, mensajes de texto SMS, MMS, correos electrónicos, eventos de calendario y archivos multimedia (imágenes, vídeos, etc.), entre otros.
- ***Extracción de datos desde SIM:*** Permite extraer información desde una tarjeta SIM o USIM.
- ***Extracción del sistema de archivos:*** Permite una extracción total del sistema desde la memoria de un dispositivo móvil de origen.
- ***Extracción de contraseñas:*** Permite extraer y visualizar contraseñas desde un dispositivo móvil de origen directamente en la pantalla Contraseña obtenida.
- ***Clonar SIM:*** Copia el ID de una SIM desde una tarjeta SIM a otra tarjeta SIM o a una tarjeta de acceso a ID de SIM de UFED.
- ***Extracción física:*** Emplea métodos avanzados para extraer una imagen física bit a bit de la memoria flash de un dispositivo móvil, incluyendo el espacio sin asignar. A diferencia de los procesos de extracción lógica convencionales, la extracción física sortea al sistema operativo del dispositivo y extrae datos directamente desde la memoria flash interna del dispositivo. El espacio no asignado puede contener elementos eliminados, como SMS, registros de llamadas, entradas de la agenda telefónica, imágenes y archivos de vídeo y audio.
- ***Capturar imágenes e instantáneas:*** Emplea la cámara UFED para tomar fotografías o grabar vídeos de un dispositivo. También puede capturar instantáneas internas directamente desde el dispositivo conectado.

Todos los tipos de extracción se pueden guardar en un PC o en un dispositivo de almacenamiento extraíble.

4.1.4 Accesorios de UFED 4PC

Aquí se plasman los tipos de cables empleados en la extracción, los cables se encuentran numerados para el modelo a trabajar.

Figura 11. Puntas y cables de UFED 4PC

Figura 12. Adaptador de dispositivos

El adaptador de dispositivos cuenta con los siguientes conectores para dispositivos de origen:

- Lector de tarjetas SIM
- Puertos USB
- Puerto RJ45

Cada conector tiene un LED que nos indica la disponibilidad durante la extracción y parpadea para indicar dónde conectar el dispositivo de origen. Además, hay varios LED de alimentación y Bluetooth.

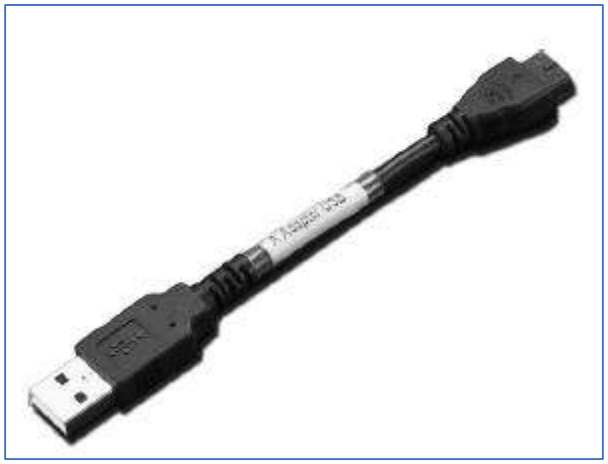


Figura 13. Cable sencillo

Para facilitar su identificación, las puntas están numeradas y codificadas con colores, donde el color representa al proveedor.

Figura 14. Punta UFED

Antes de cada extracción, el número de cable y punta necesarios se especifica en la zona **Origen** de la pantalla

Por consiguiente Seleccionamos “tipos de contenido”

Figura15. Notificación de tipo de cable a usar.

4.2 Extracción lógica

La función Extracción lógica nos permite extraer varios tipos de datos, como registros de llamadas, registros de la agenda telefónica, mensajes de texto SMS, eventos del calendario y archivos multimedia (imágenes, vídeos, etc.), desde un dispositivo de origen y guardarlos en su PC o en un dispositivo de almacenamiento extraíble, según se desee.

4.2.1 Realizar una extracción lógica

En esta sección se muestra el procedimiento para realizar una extracción lógica **de un dispositivo móvil utilizando el UFED 4PC:**

- hacemos clic en **Extraer desde dispositivo móvil**, identificando el dispositivo y, a continuación, hacemos clic en **Extracción lógica**.

Conectamos el dispositivo móvil

Figura 16. Seleccionamos el tipo de conexión

Selección de memoria de teléfono

En este paso extraemos datos desde la memoria del dispositivo, desde las tarjetas de memoria y desde la memoria SIM del dispositivo. Podemos seleccionar todas las memorias o solo una. Los tipos de memoria pueden variar de un dispositivo a otro. Si solo hay una memoria disponible, esta pantalla no se mostrará.

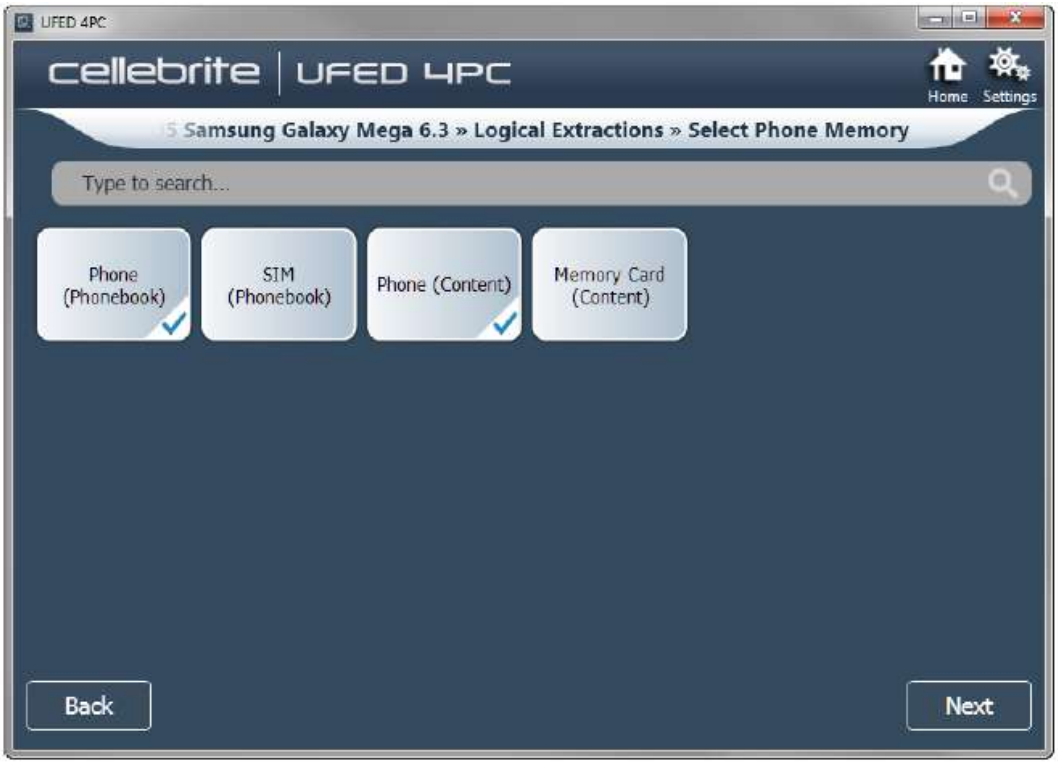
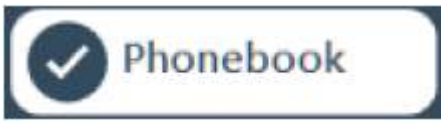
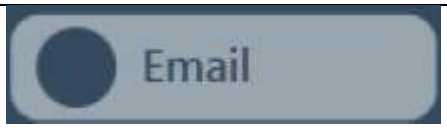


Figura 17. Selección de extracción.

Para seleccionar la memoria del teléfono:

1. El cuadro de selección de la memoria del teléfono está seleccionado de forma predeterminada. Es posible deseleccionarlo si lo requerimos.
2. Seleccionamos otras memorias, si lo deseamos.
3. hacemos clic en **Siguiente** para continuar.

Tabla 3. Los tipos de contenido se muestran en una lista de tres formas distintas.

	Tipos seleccionados de forma predeterminada: se muestran con una marca de verificación.
	Tipos disponibles para ser seleccionados: se muestran sin marca de verificación
	Tipos no disponibles: se muestran oscurecidos

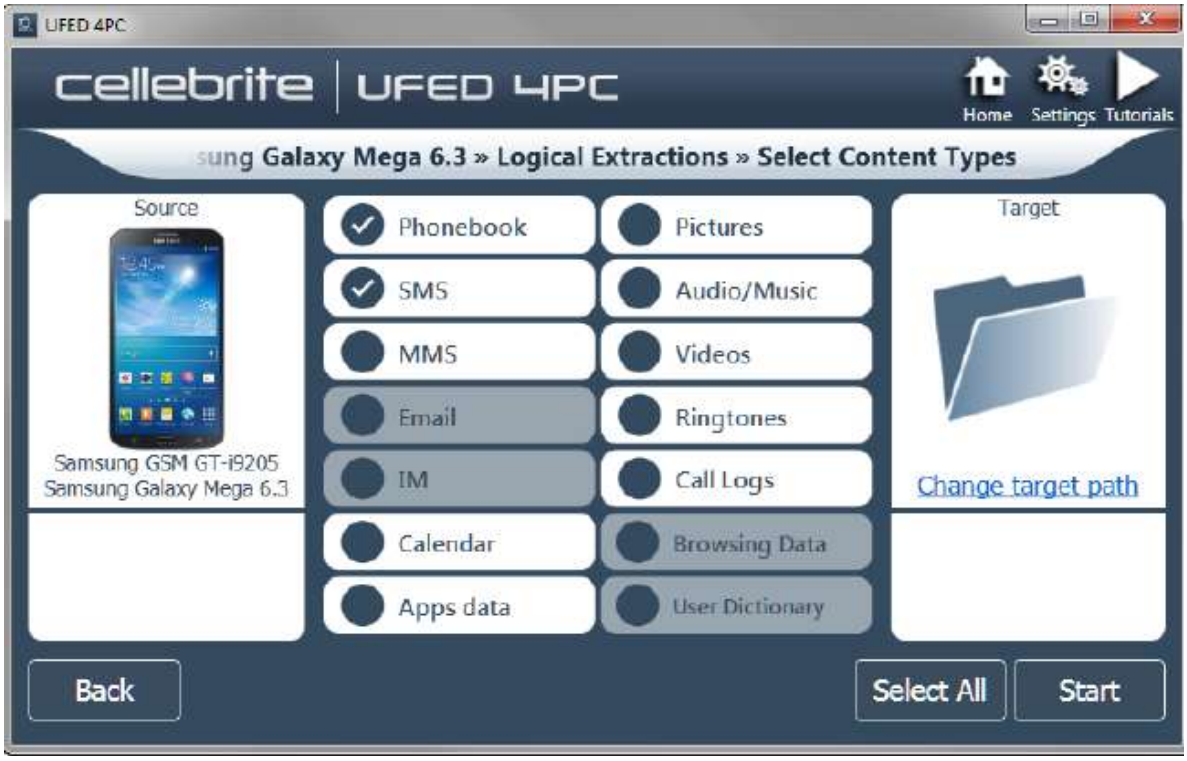


Figura 18. Tipos de contenidos.

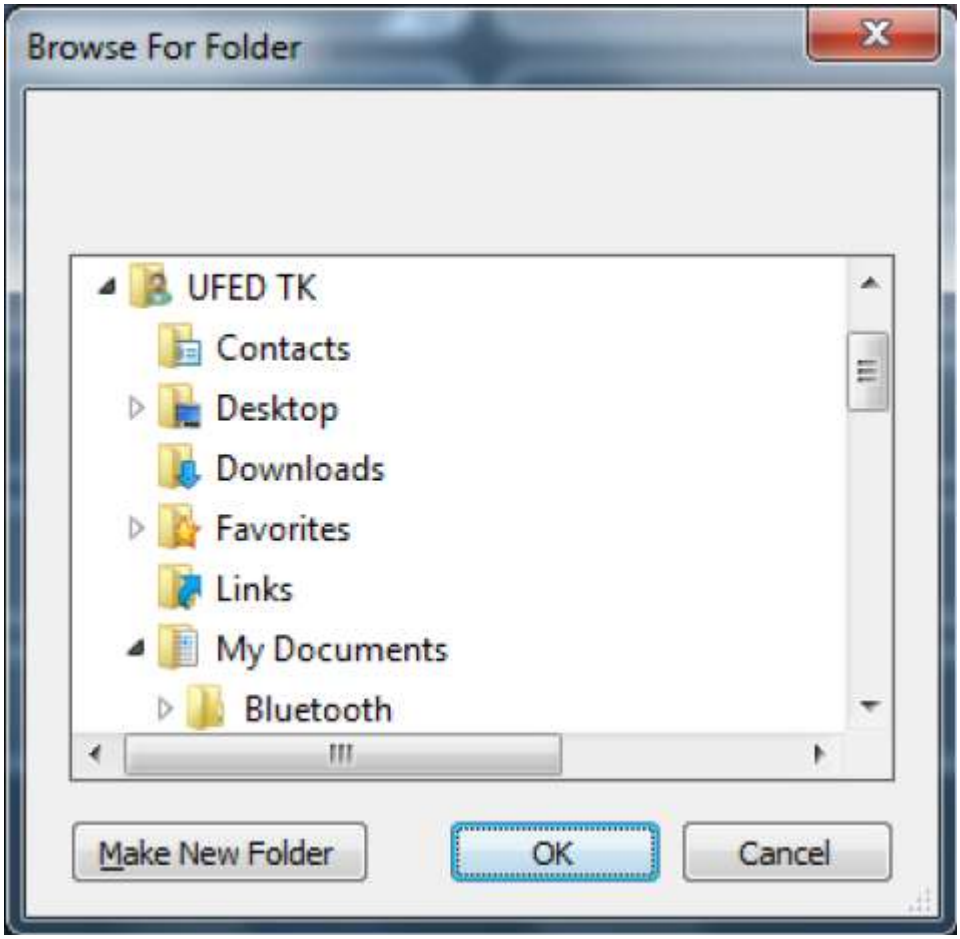
Para seleccionar los tipos de contenido:

1. Seleccionamos los demás tipos de contenido que desee incluir en la información extraída de este dispositivo.

2. Seleccionamos **Seleccionar todo** para seleccionar todos los tipos disponibles.

3. Hacemos clic en **Iniciar** para continuar.

4. Para cambiar la ruta de destino:
   a. Hacemos clic en **Cambiar ruta de destino**.



b. En el diálogo Buscar carpeta, nos dirigimos hasta la ubicación en la que deseamos guardar la extracción.

c. Seleccionamos la ubicación deseada o hacemos clic en **Crear nueva carpeta** para crear un directorio de destino.

d. Hacemos clic en **Aceptar**.

La ruta de destino ha sido definida.
Aparecerá la pantalla **En espera del dispositivo**.

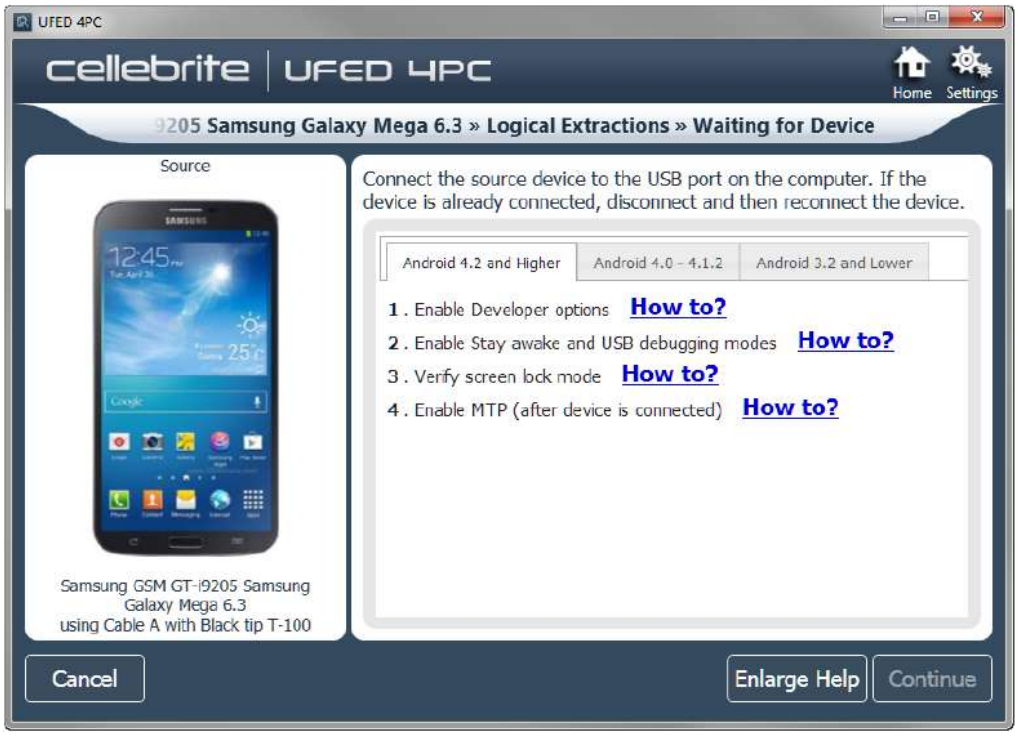


Figura 18. Esperando el dispositivo

5. Conectamos el dispositivo de origen al puerto USB del ordenador. Si el dispositivo ya está conectado, lo desconectamos y volvemos a conectarlo.

6. Hacemos clic en **Continuar**.

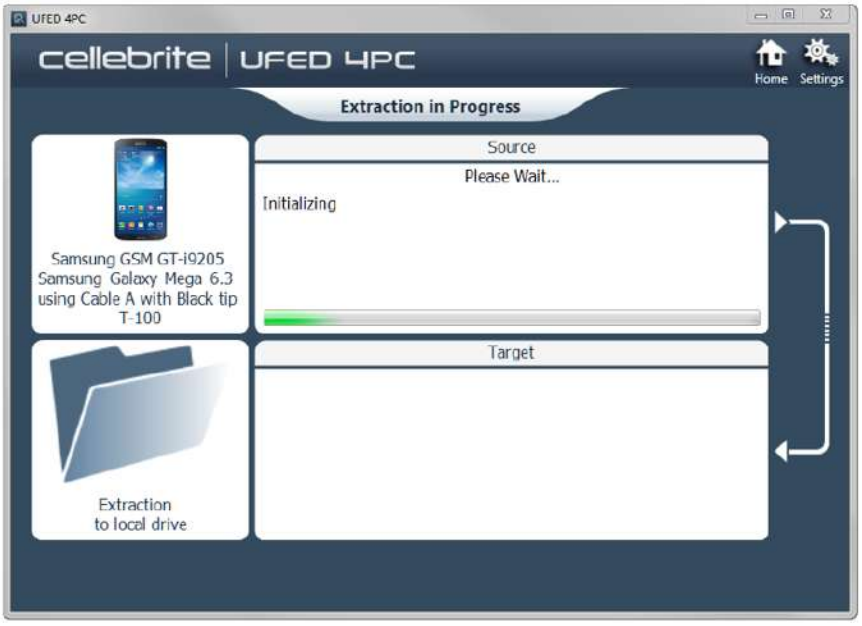
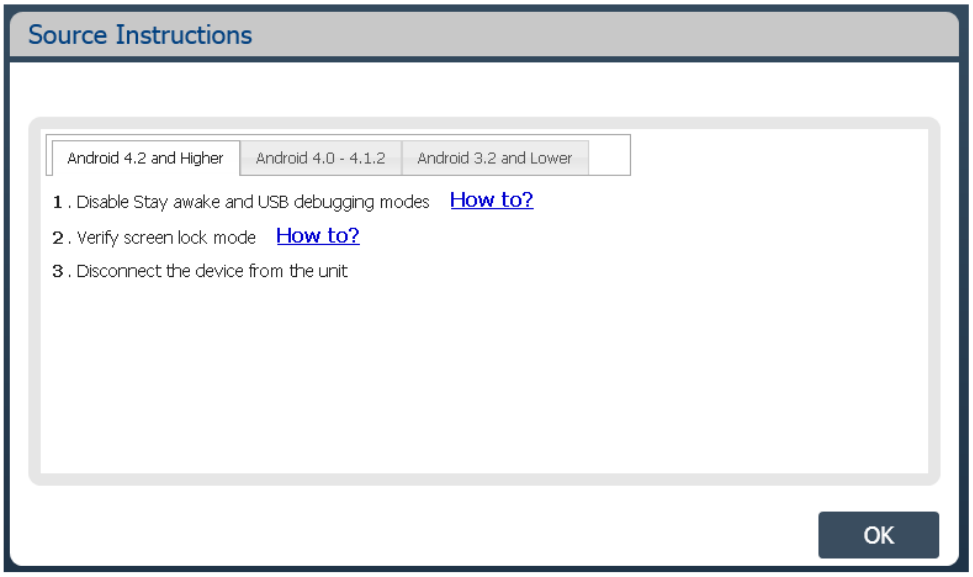


Figura 19. Extracción en curso

Durante el proceso de extracción, la barra de progreso del origen y, posteriormente, del destino estarán activas.



1. Devolvemos los parámetros del dispositivo móvil a su configuración inicial.
2. Hacemos clic en **Aceptar**.

Aparecerá la pantalla Resumen de extracción de teléfono.

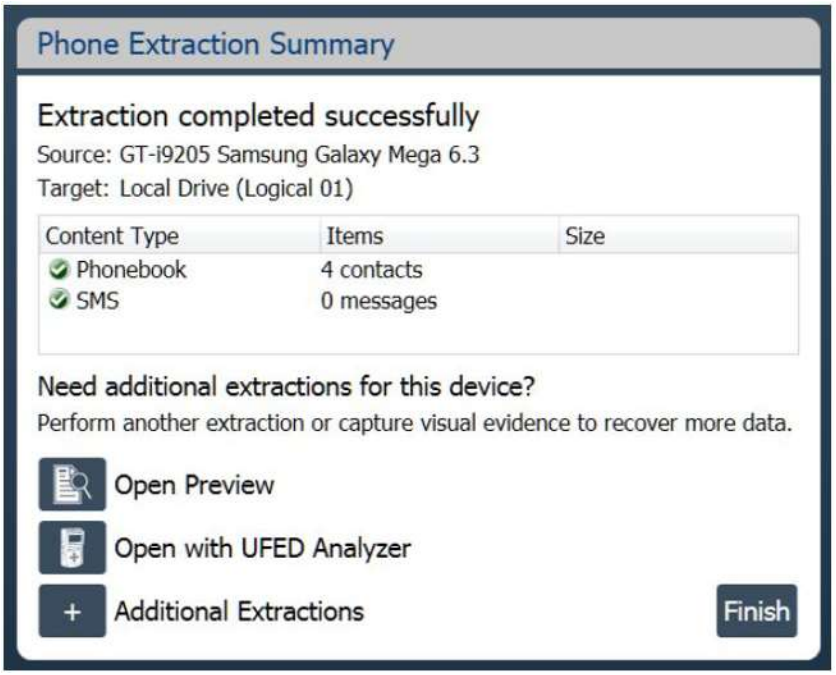
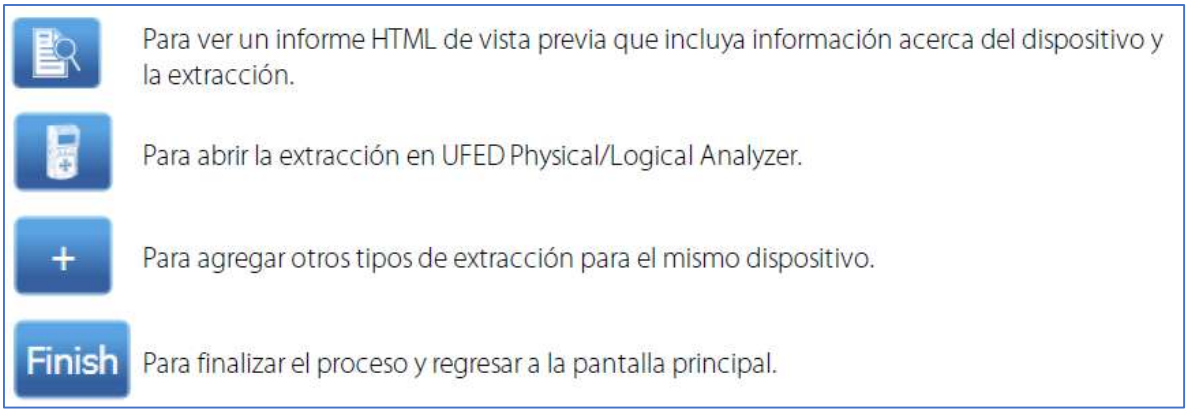


Figura 20. Extracción exitosa

Los siguientes botones describen el funcionamiento.



A continuación, se muestra un ejemplo del informe de vista previa y de la pantalla para agregar otros tipos de extracción.

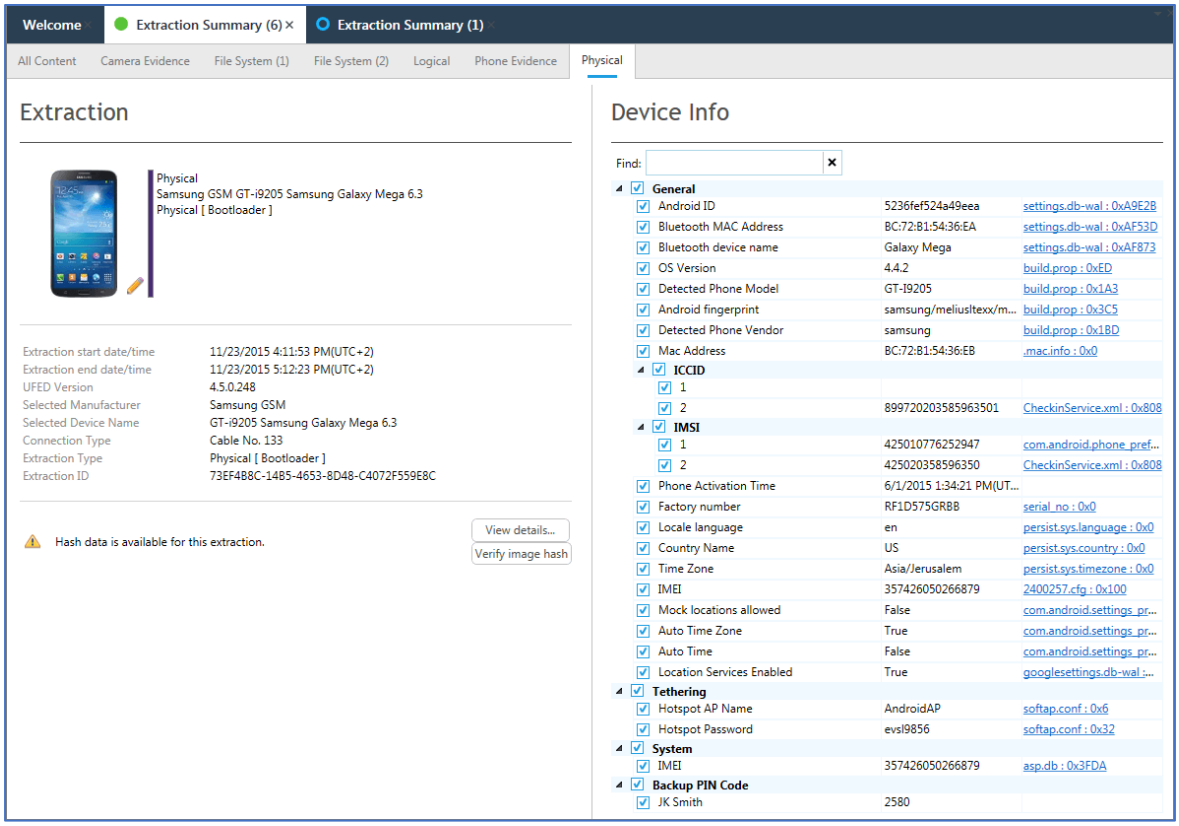


Figura 21. Vista previa del informe.

Carpeta de datos extraídos

Al final del proceso de extracción de datos, los datos extraídos se guardarán en la ubicación seleccionada.

La carpeta de datos extraídos contiene:

- Carpetas de archivos multimedia llamadas Audio, Imágenes, Tonos y Vídeo, cada una de las cuales contiene el tipo correspondiente de archivos multimedia.
- Archivos de informes de extracción del teléfono en formatos HTML y XML. (Un informe HTML por tipo de contenido).
- Archivos de UFED Manager del registro de llamadas (*.clog), agenda telefónica (*.pbb), mensajes SMS (*.sms) y calendario (*.cal) y de los datos de correo electrónico (*.Email), MMS (*.MMS) e IM (*.IM) extraídos.
- Archivo UFD.

4.3. Extracción del sistema de archivos

La función Extracción del sistema de archivos nos permite realizar una extracción completa del sistema de archivos de un dispositivo.

4.3.1. Cómo extraer el sistema de archivos

En este secciona veremos cómo realizar una extracción de sistema de archivos.

Figura 21. Selección del tipo de extracción.

1. Hacemos clic en **Extraer desde dispositivo móvil**, identificamos el dispositivo y, a continuación, hacemos clic en **Extracción del sistema de archivos**.

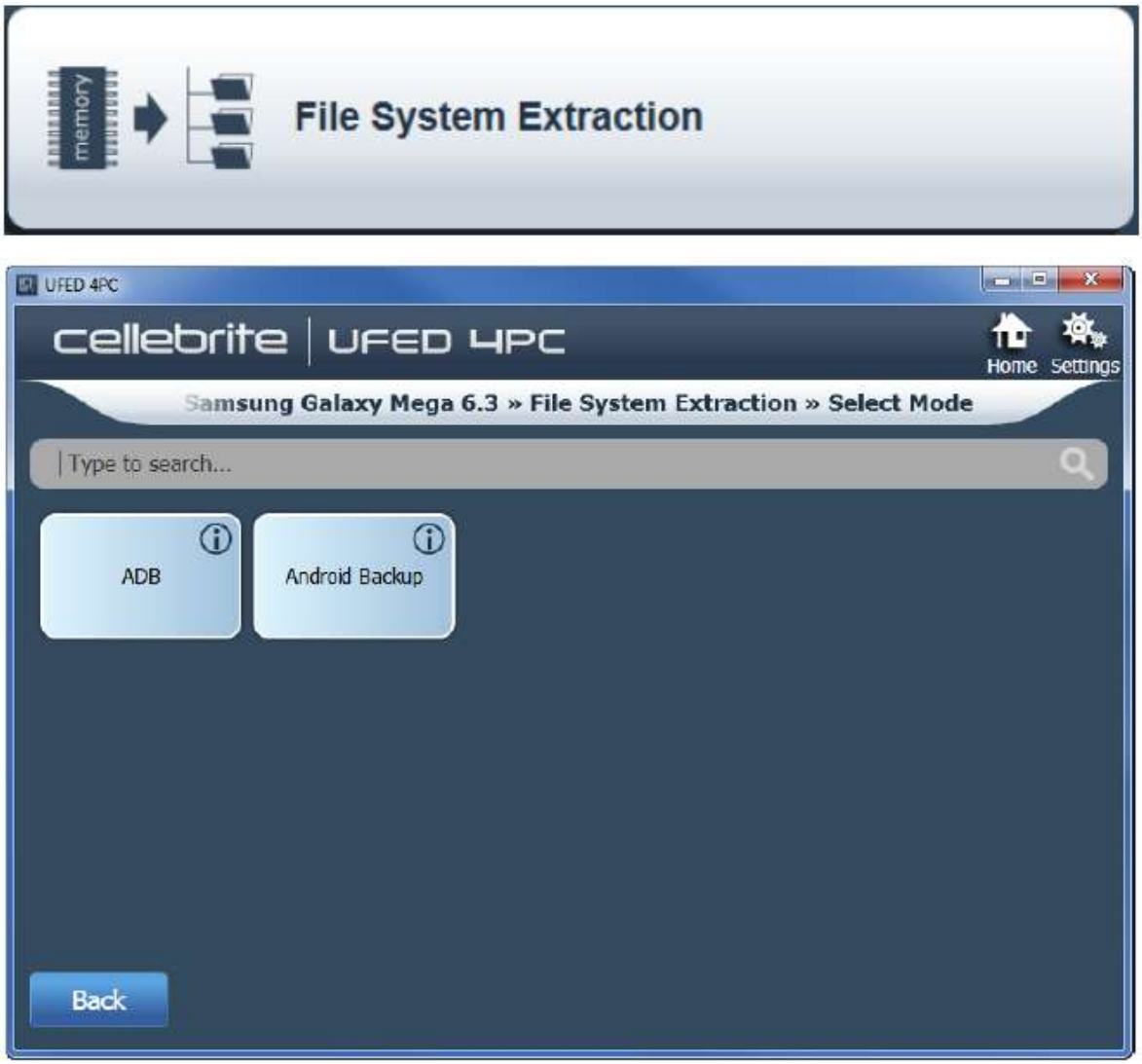


Figura 22. Seleccionamos el modo de extracción.

2. Seleccionamos **ADB**

Aparecerá la pantalla Seleccionar ubicación para la extracción.

Hacemos clic en **Siguiente**.

Aparecerá la pantalla En espera del dispositivo.

Figura 23. Esperando el dispositivo.

3. Seleccionamos el cable y la punta adecuados para el dispositivo móvil en función de la información que aparece en la pantalla.

4. Cambiamos la configuración del dispositivo siguiendo las instrucciones.

5. Conectamos el dispositivo.

6. Hacemos clic en **Continuar**.

Aparecerá la pantalla Extracción en curso.

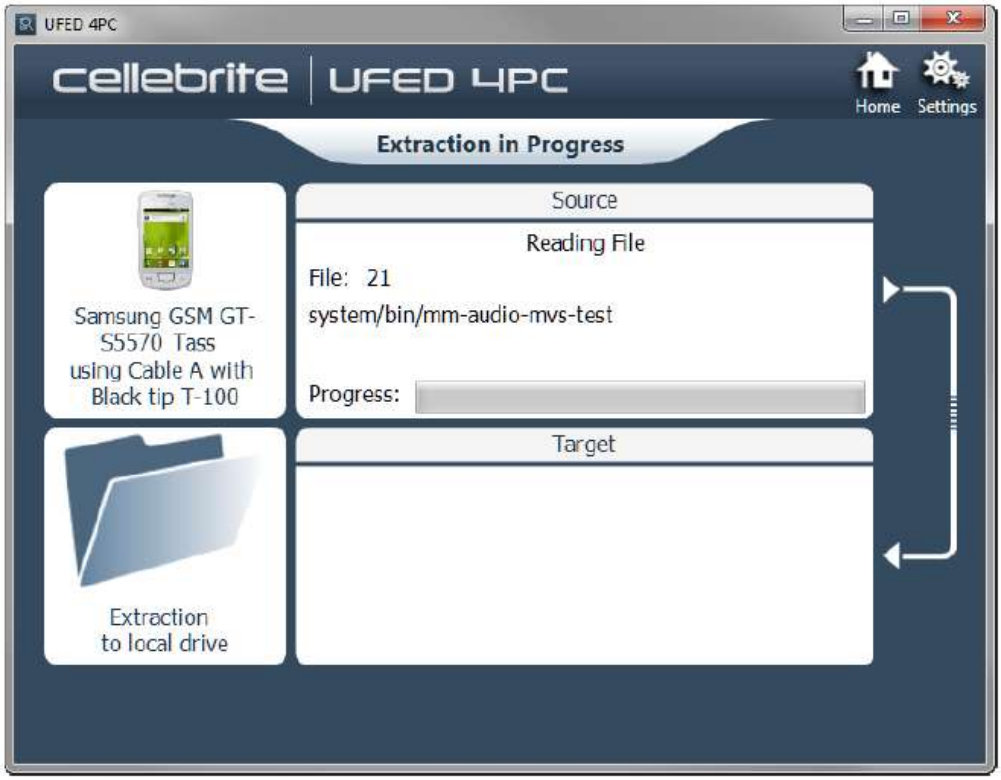


Figura 24. Extracción en progreso.

Durante el proceso de extracción, la barra de progreso del origen y, posteriormente, del destino estarán activas. Cuando la extracción haya finalizado, aparecerá la pantalla Resumen de extracción del sistema de archivos.

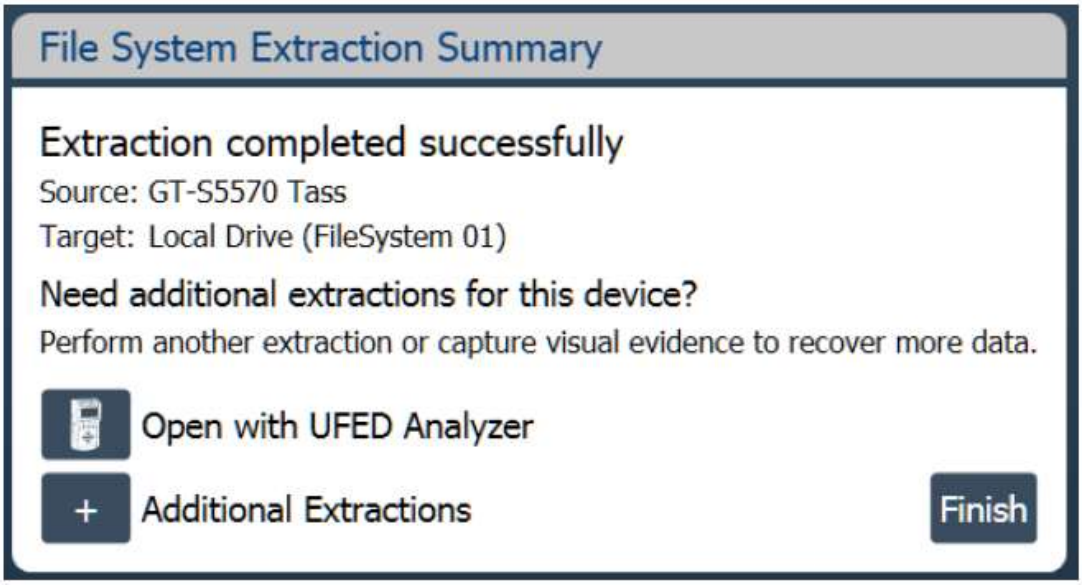
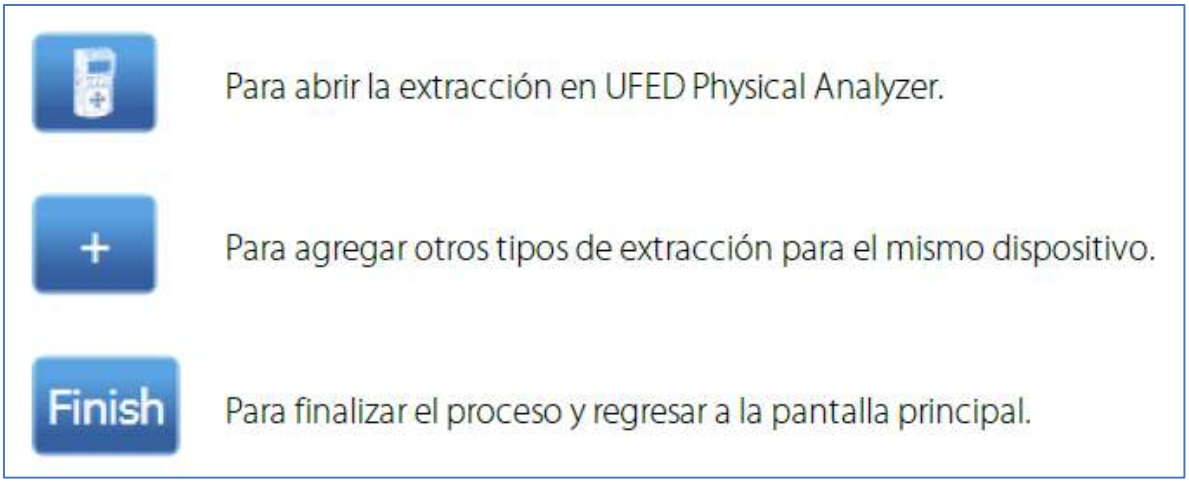


Figura 25. Mensaje de extracción completada.



4.3.2 Carpeta de extracción del sistema de archivos

Al final del proceso de extracción del sistema de archivos, los datos extraídos se guardarán en la ubicación que haya seleccionado previamente.

La carpeta de datos extraídos contiene:

- Un archivo comprimido del sistema de archivos del dispositivo con los archivos y carpetas en la misma estructura en que fueron extraídos.
- Un archivo UFD que contiene la información de extracción del sistema, utilizado por la aplicación UFED Physical Analyzer.
- Un archivo PM.

La extracción del sistema de archivos se puede visualizar utilizando UFED Physical Analyzer

4.3.3 Copia de seguridad de Android (Android backup)

En este apartado la copia de seguridad de Android establece comunicación con un dispositivo Android conectado y le permite extraer datos del mismo. Los datos extraídos dependerán de las características específicas del dispositivo. La función de copia de seguridad de Android admite dispositivos Android con versión 4.1 y posterior.

Es posible que la función de copia de seguridad de Android proporcione menos datos que otros métodos, por lo que solo utilizamos esta función cuando los demás métodos de extracción del sistema de archivos, como ADB, fallen o no estén disponibles para ese dispositivo (por ejemplo, si la versión de Android no es compatible).

A continuación se describe el método para extraer datos utilizando la copia de seguridad de Android:

1. Hacemos clic en **Extraer desde dispositivo móvil**, identifique el dispositivo y, a continuación, haga clic en
Extracción del sistema de archivos.

Figura 26. Seleccionamos el modo de extracción.

2. Hacemos clic en **Copia de seguridad Android**.
Aparecerá un mensaje indicando que el modo de copia de seguridad de Android extraerá los datos en función de las características específicas del dispositivo.

3. Hacemos clic en **Continuar**.

4. Seleccionamos la ruta de destino y hacemos clic en **Siguiente**.
Aparecerá la pantalla En espera del dispositivo.

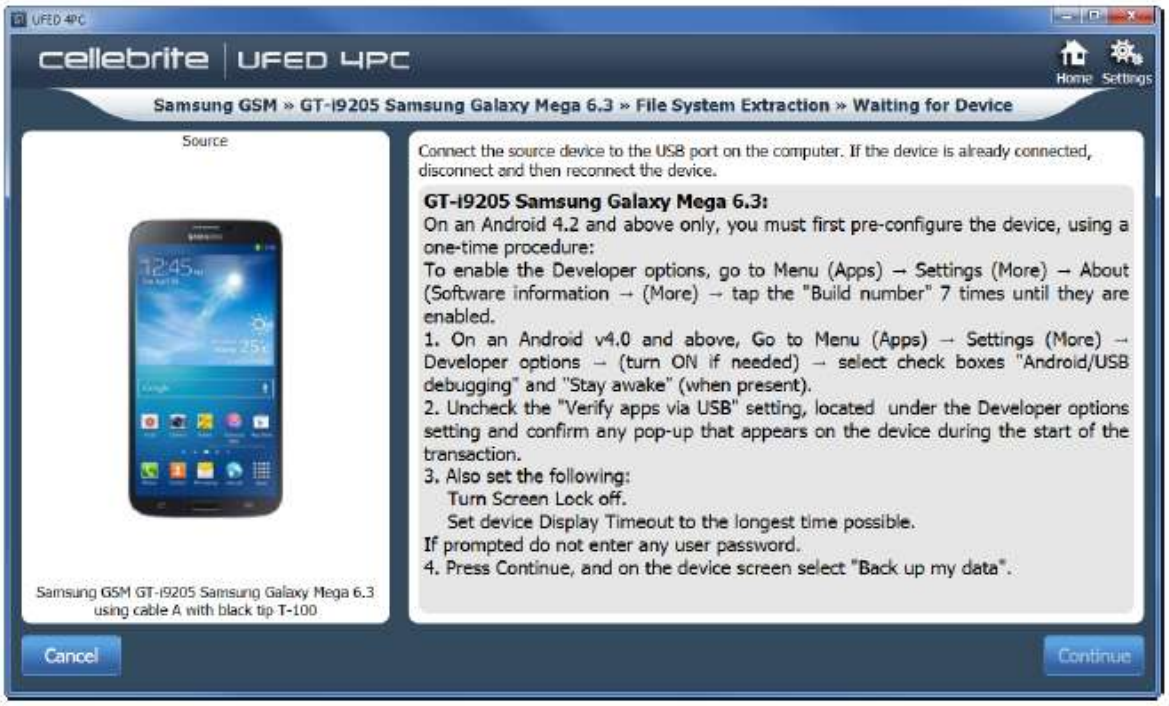


Figura 27. Esperando al dispositivo.

5. Conectamos el dispositivo de origen al puerto USB. Si el dispositivo ya está conectado, lo desconectamos y volvemos a conectarlo.

6. Hacemos clic en **Continuar** y, a continuación, seleccionamos **Copia de seguridad de datos** en el dispositivo.
Aparecerá la siguiente pantalla.

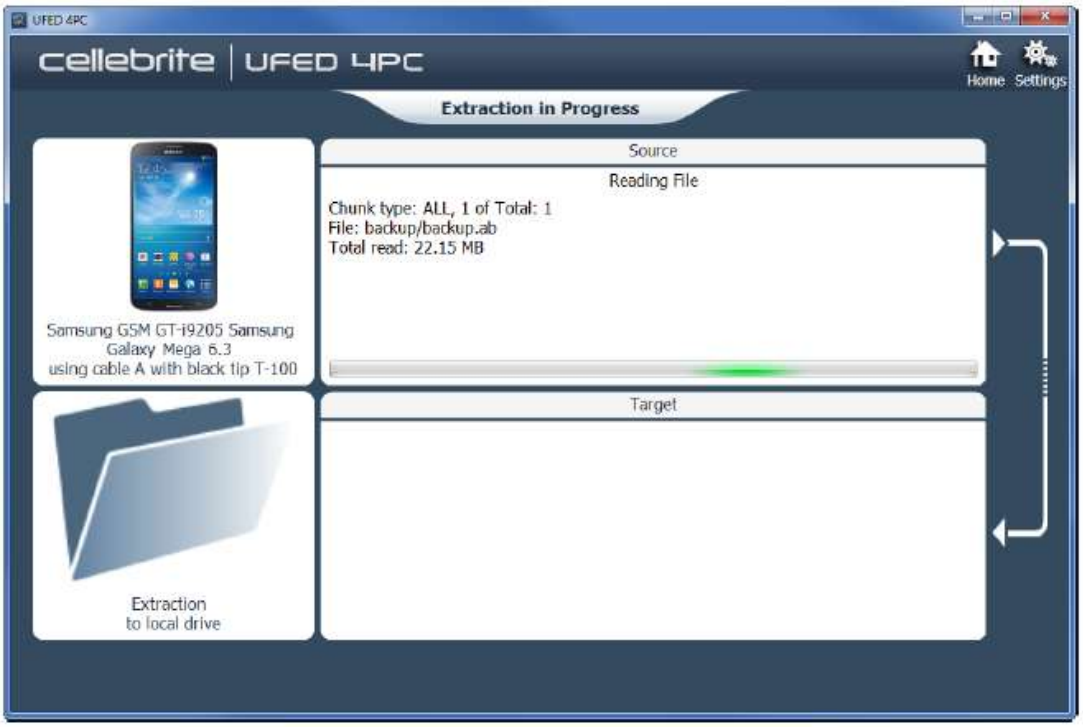
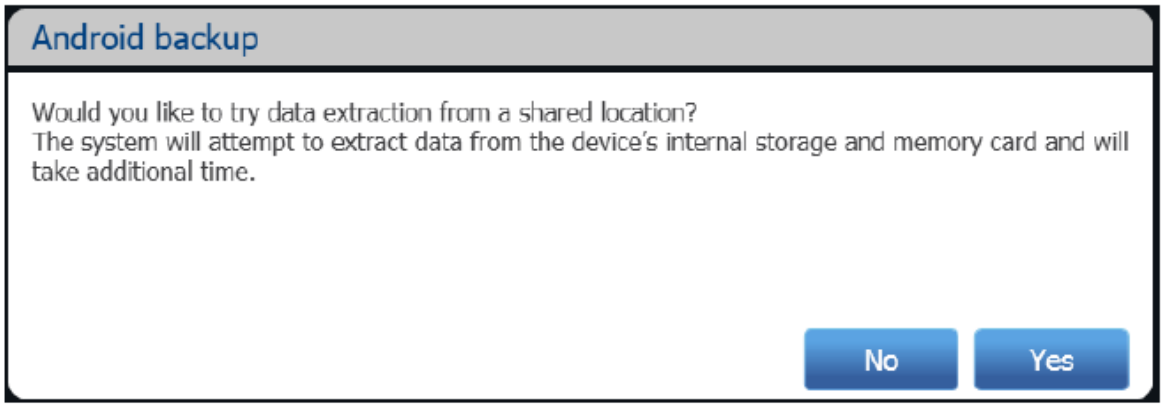
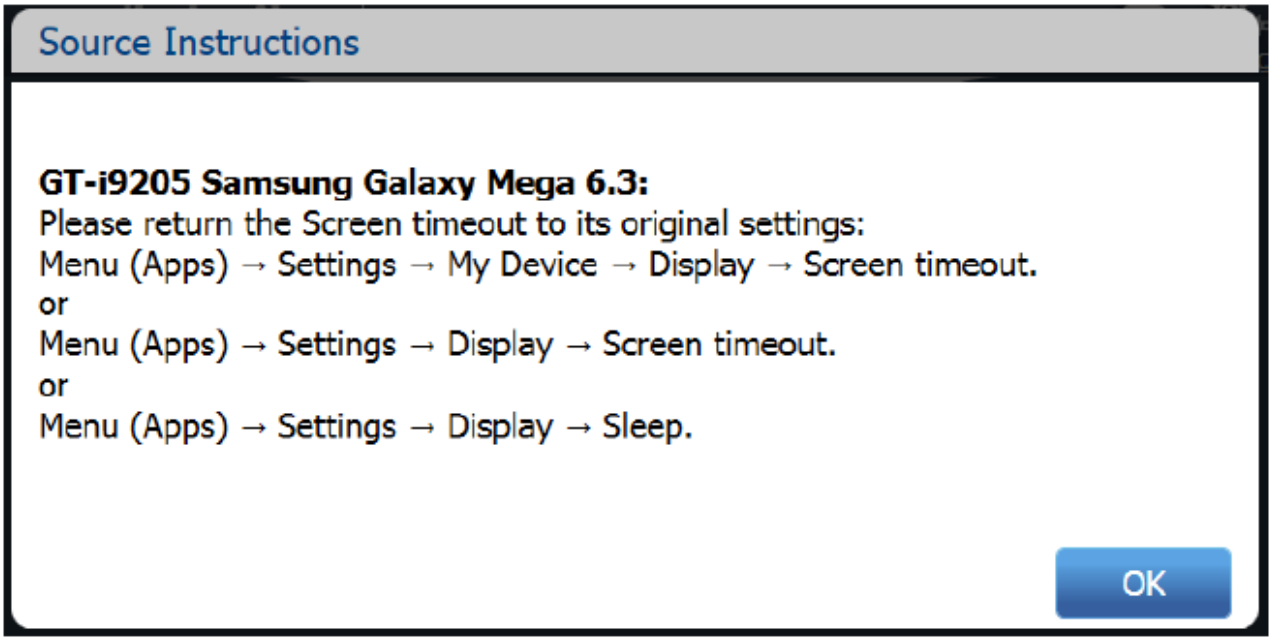


Figura 28. Extracción en progreso.



7. Hacemos clic en **No** si no deseamos extraer datos desde una ubicación compartida, oh hacemos clic en **Sí** si deseamos intentar extraer información desde una ubicación compartida. Con una ubicación compartida UFED 4PC extrae todas las aplicaciones (nativas y no nativas) que residen en el dispositivo, además de los datos del almacenamiento interno y la tarjeta de memoria del dispositivo (como imágenes, vídeos, etc.), lo que lleva más tiempo.

Aparecerá la siguiente pantalla.



Seguimos las instrucciones y haga clic en **Aceptar**.

Cuando la extracción haya finalizado, aparecerá la pantalla Resumen de extracción del sistema de archivos.

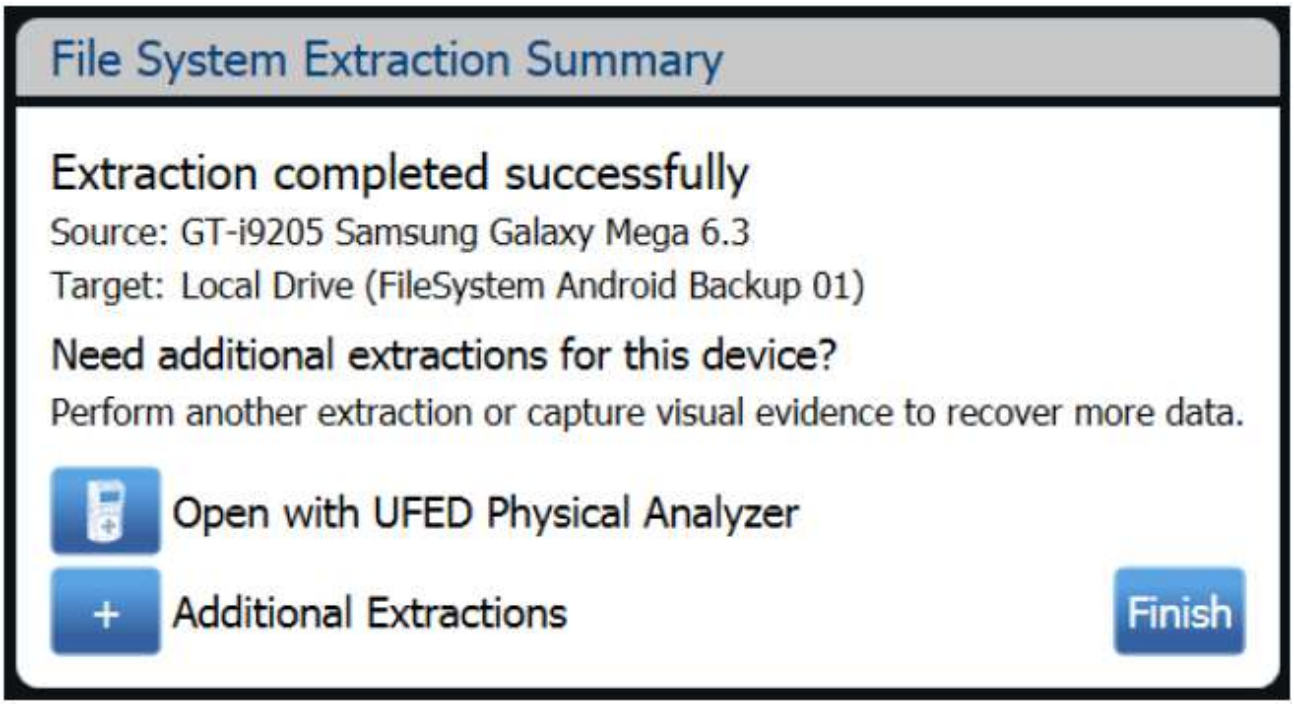
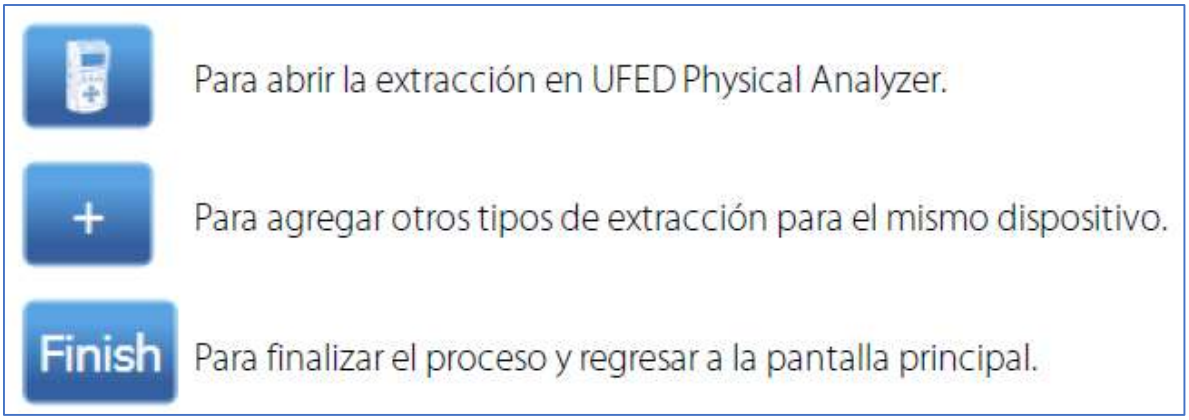


Figura 29. Extracción de sistema de archivos finalizada con éxito.



4.4 Extracción física

En este apartado se explica la función **Extracción física** la cual nos permite generar una imagen física bit a bit de la memoria del dispositivo de origen en un dispositivo de almacenamiento extraíble o PC.

4.4.1 Realizar una extracción física.

Se muestra como realizar la extracción física de un dispositivo móvil. Lo primero que haremos es:

1. Clic en **Extraer desde dispositivo móvil**, identificamos el dispositivo y, a continuación, clic en **Extracción física**.

Aparecerá la pantalla Seleccionar modo.

Figura 30. Seleccionamos el tipo de extracción física.

Hacemos clic en **ADB** o **Cargador de arranque** (recomendado).

Aparecerá la pantalla Seleccionar ubicación para la extracción

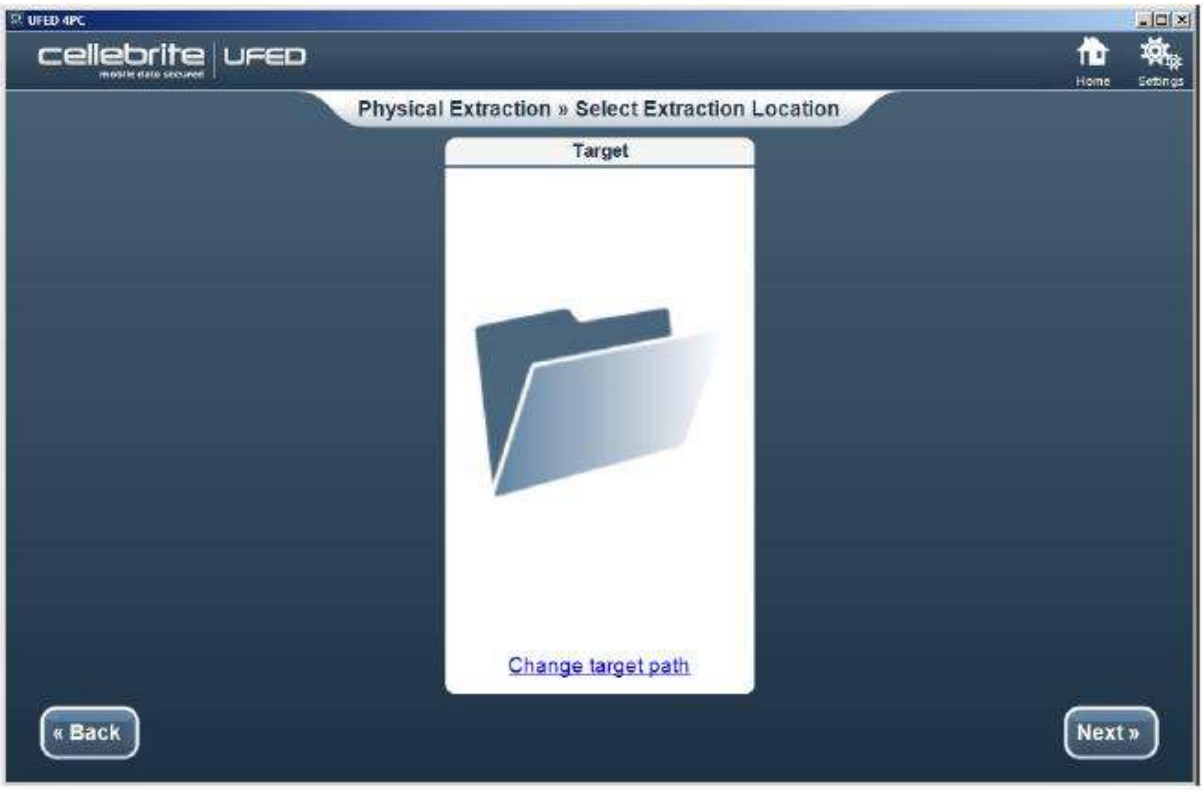


Figura 31. Seleccionamos la carpeta destino donde se almacenara la extracción.

Hacemos clic en **Siguiente**.

En función de si el dispositivo requiere o no UFED Device Adapter, aparecerá la pantalla “**En espera del dispositivo”** o **“En espera del adaptador de dispositivos”.**

Figura 32. Esperando el dispositivo.

Realizamos una de las siguientes acciones:

- Seleccionamos el cable y la punta adecuados para el dispositivo móvil en función de las instrucciones que aparecen en la pantalla.
- Cambiamos la configuración del dispositivo siguiendo las instrucciones.
- Conectamos el dispositivo al PC.

Si el dispositivo requiere UFED Device Adapter para realizar la extracción:

- Conectamos UFED Device Adapter a un puerto USB del ordenador.

El puerto de origen de UFED Device Adapter parpadeará.

- Conectamos el dispositivo a UFED Device Adapter.

5. Hacemos clic en **Continuar**.

Aparecerá la pantalla Extracción en curso.

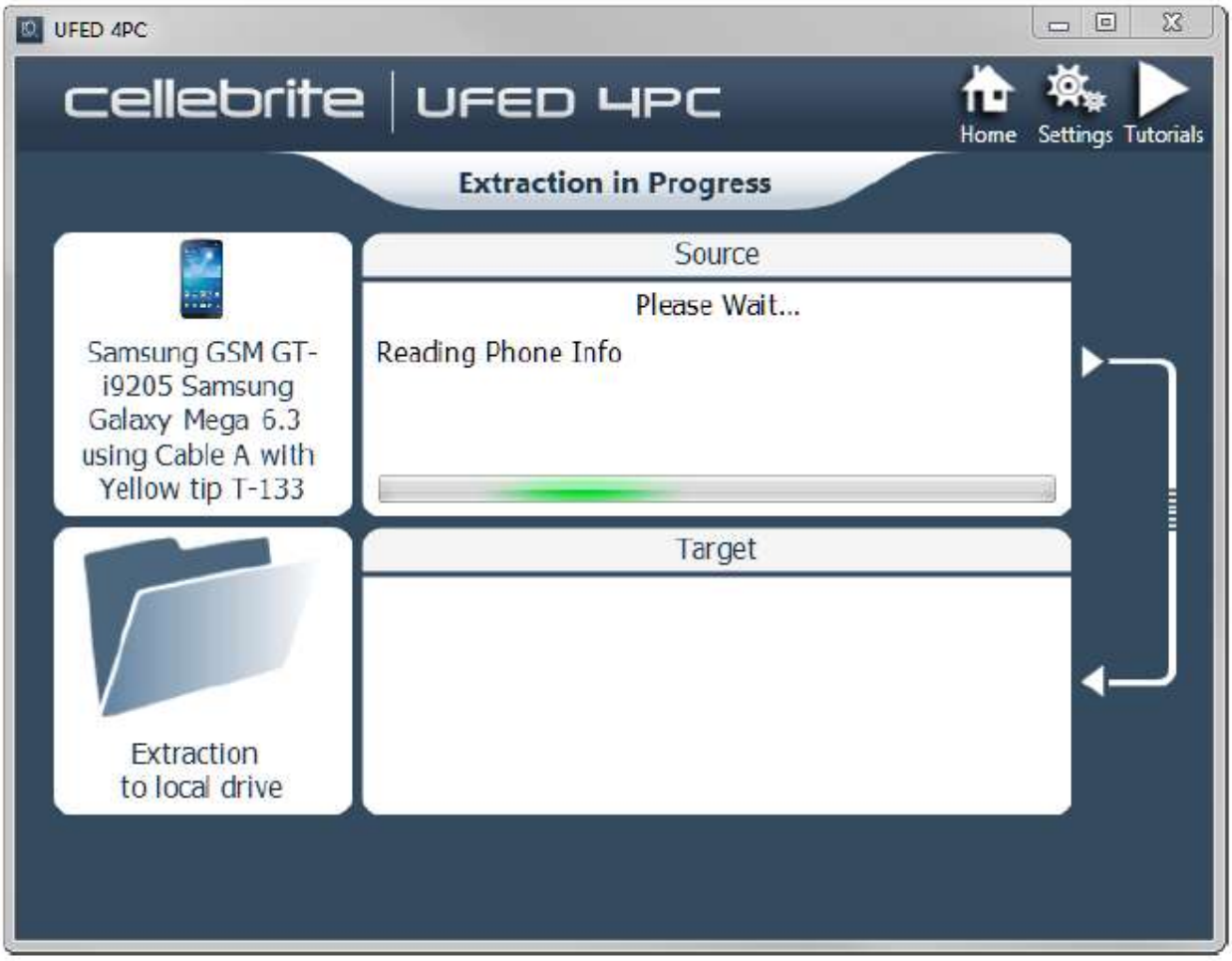


Figura 33. Extracción en progreso.

Durante el proceso de extracción, la barra de progreso del origen y, posteriormente, del destino estarán activas.

6. Seguimos las instrucciones de la pantalla. Aparecerá la siguiente pantalla.

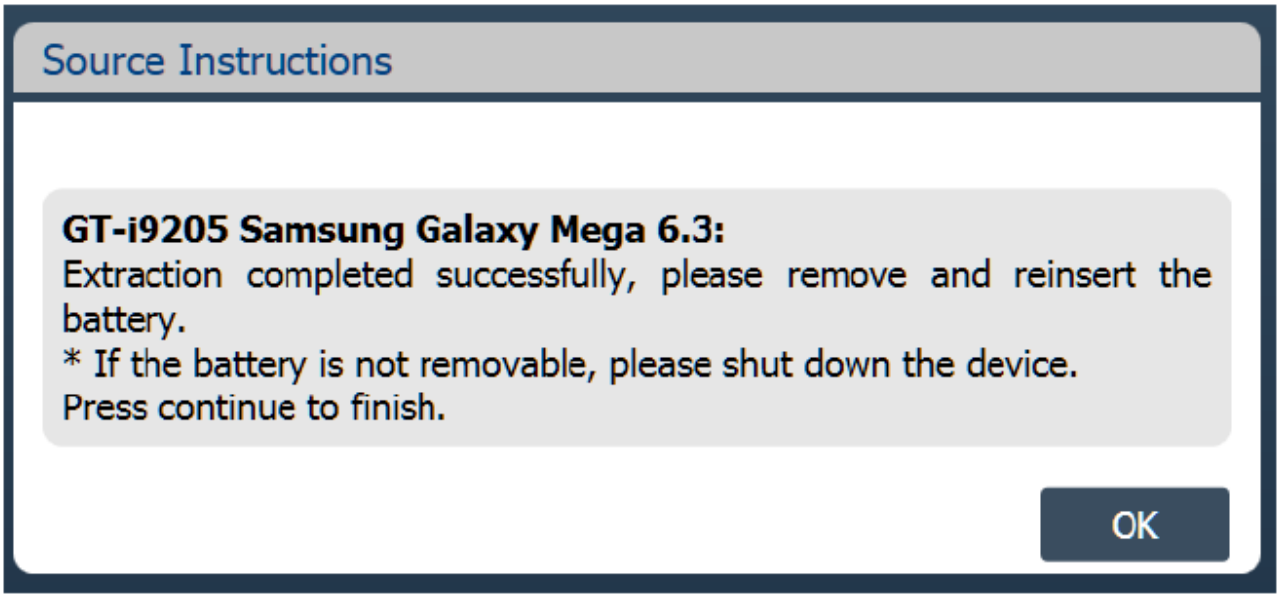


Figura 34. Extracción completa con éxito.

Hacemos clic en **Aceptar**. Cuando la extracción haya finalizado, aparecerá la pantalla Resumen de extracción física.

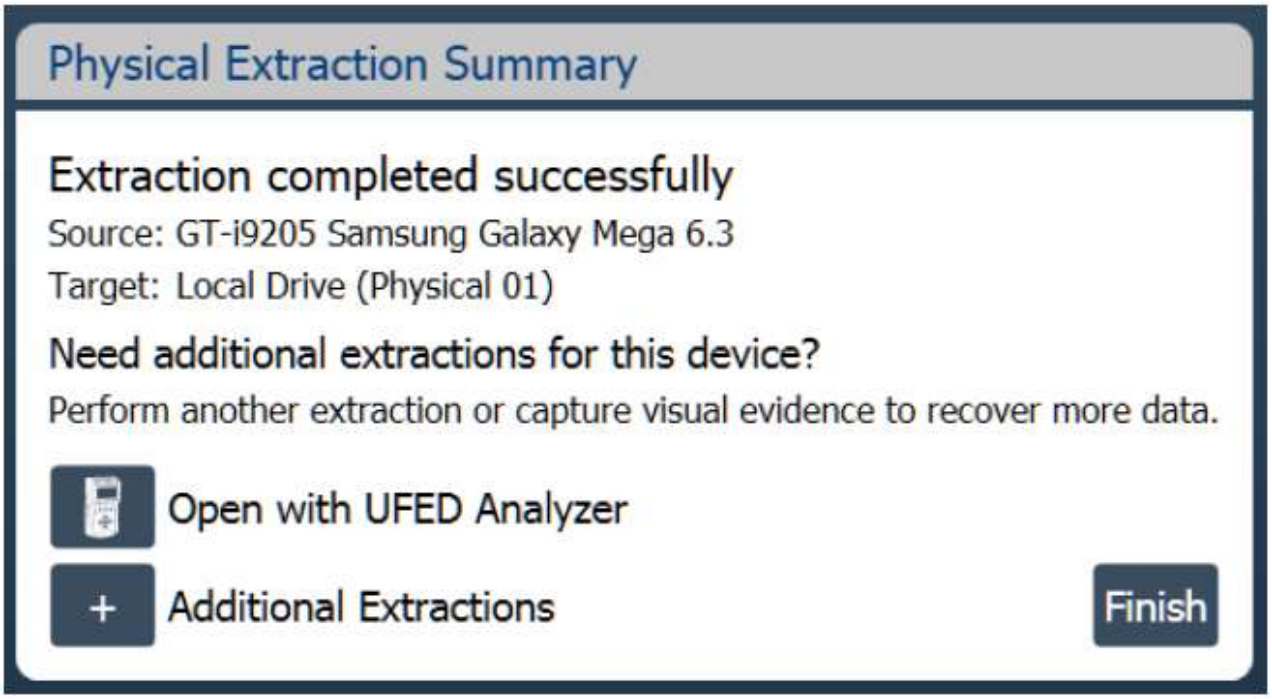
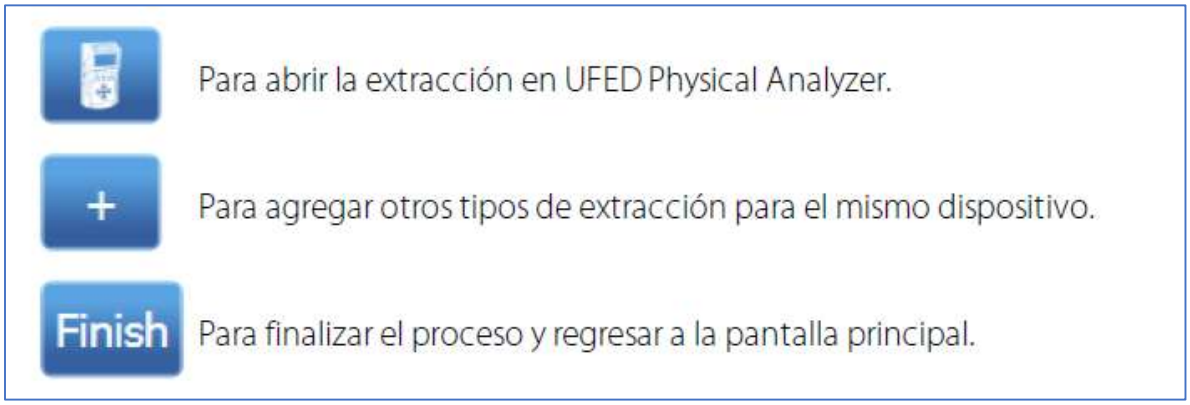


Figura 35. Finalizar extracción física.

8. Hacemos clic en el botón pertinente.



En caso de que el sistema no pueda establecer conexión con el dispositivo, aparecerá la pantalla “Resumen de extracción” con un mensaje de error.

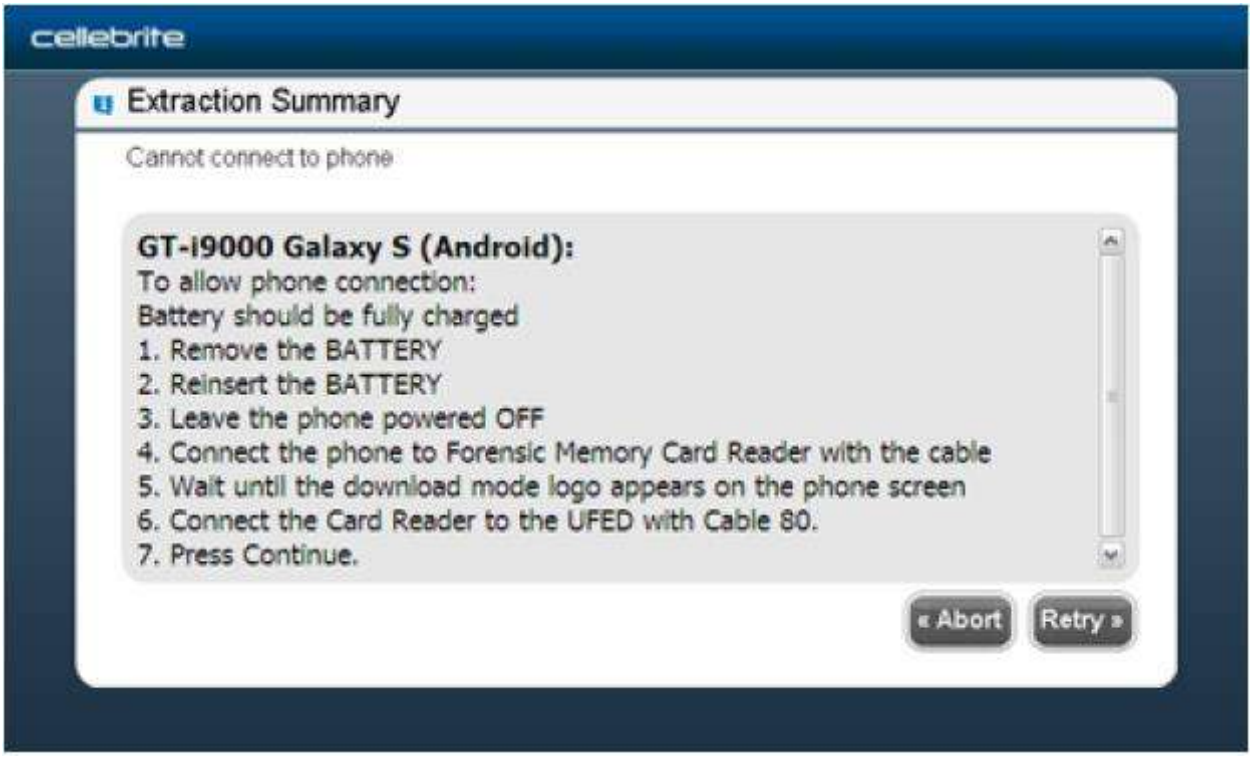


Figura 36. Mensaje de error.

9. Seguimos las instrucciones que aparecen en la pantalla y hacemos clic en **Reintentar**.

10. si continuamos recibiendo el mensaje de error es que quizás este fallando el cableado, o el dispositivo no sea compatible, o los parches de seguridad de Android estén actualizados.

Para poder descifrar y decodificar todo el contenido de la extracción, utilizaremos el software Physical Analizer de Cellebrite.

4.5. Physical Analizer

En este apartado se describe como decodificar la información. Al final del proceso de extracción, los datos extraídos se guardarán en la ubicación que hayamos seleccionado durante el proceso de extracción.

La información de extracción la visualizamos con UFED Physical Analyzer. Para optimizar, el espacio de trabajo contiene dos áreas principales: el árbol de proyectos y el área de visualización de datos.

El espacio de trabajo contiene los siguientes componentes:

1. Barra de menús de la aplicación
2. Árbol proyectos
3. Área de visualización de datos
4. Búsqueda de todos los proyectos

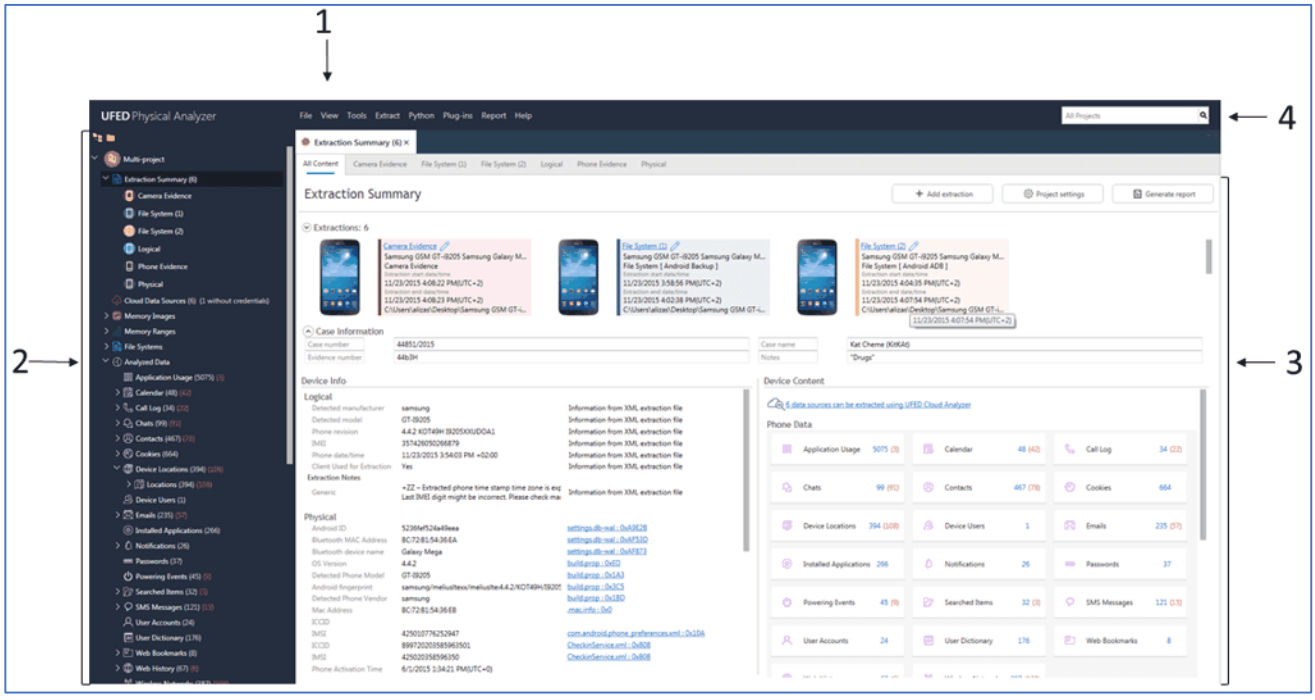


Figura 37. Decodificación de la información extraída mediante el software Physical Analizer.

Esta sección incluye información relacionada con las extracciones del dispositivo.

Figura 38. Extracción individual

Figura 39. Extracciones múltiples.

El área Extracciones incluye la siguiente información:

Tabla 4. Información de la extracción.

Enlace de extracción	Enlace a la pestaña de extracción.
Modelo del dispositivo	Modelo detectado, por ejemplo, MB7171, Samsung GT-I9205.
Tipo de extracción	Tipo de extracción realizada por ejemplo, Física (Bootloader).
Fecha/hora inicio de extracción ***Fecha/hora fin de extracción***	Cuándo comenzó y finalizó la extracción.
Ruta al archivo de extracción	La ubicación del archivo de extracción.

Esta sección muestra un resumen de la información específica del dispositivo obtenida desde el archivo de extracción.

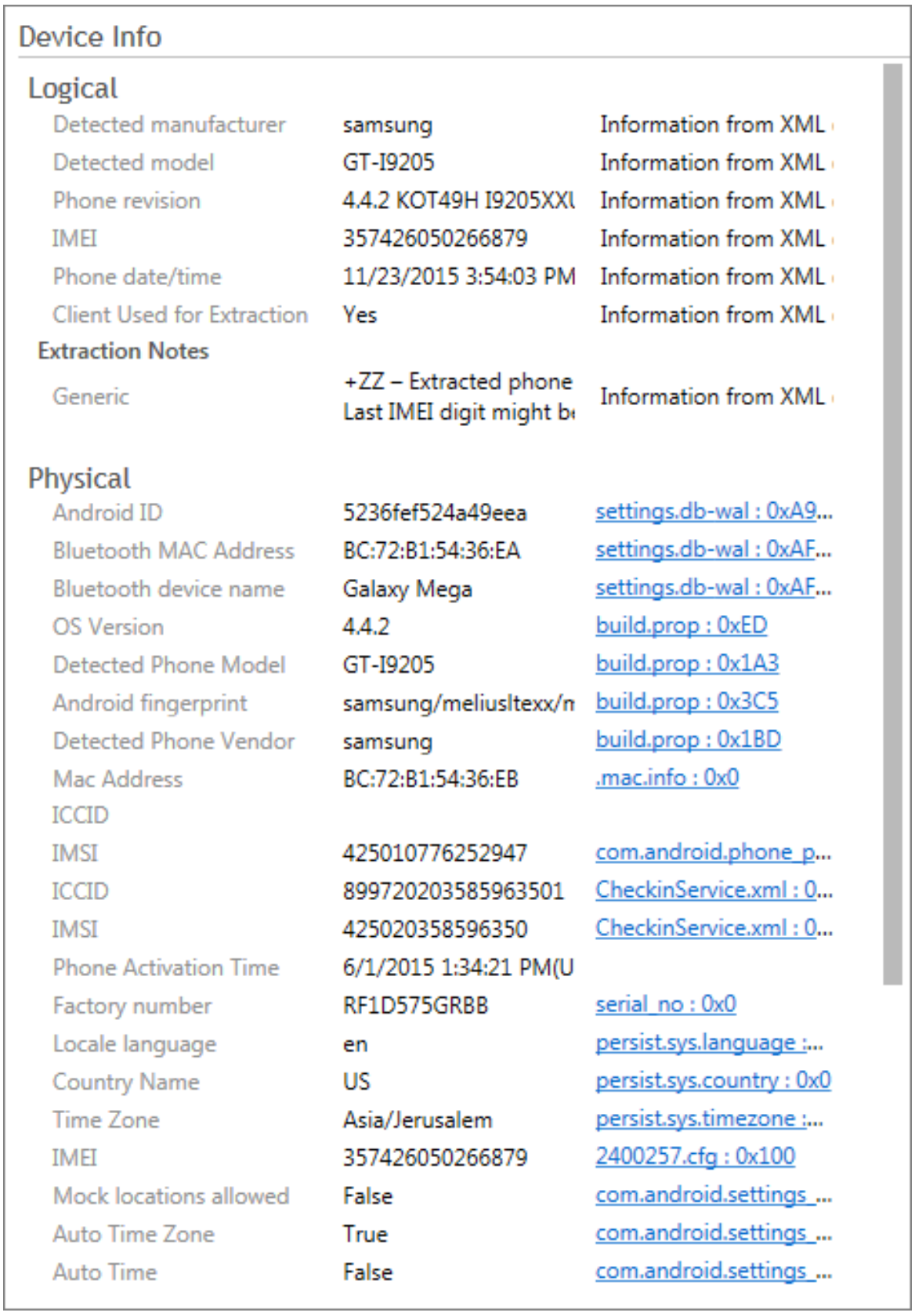


Figura 40. Información de dispositivo

Esta sección incluye el contenido analizado, que se divide en las siguientes categorías:

- Datos del teléfono: tipos de datos de los dispositivos analizados encontrados en la extracción, como registro de llamadas, contactos, mensajes SMS, etc.

- Archivos de datos: los tipos de archivos de datos estándares encontrados en la extracción, como aplicaciones, audio, configuraciones, imágenes, vídeos, archivos de texto y no categorizados.

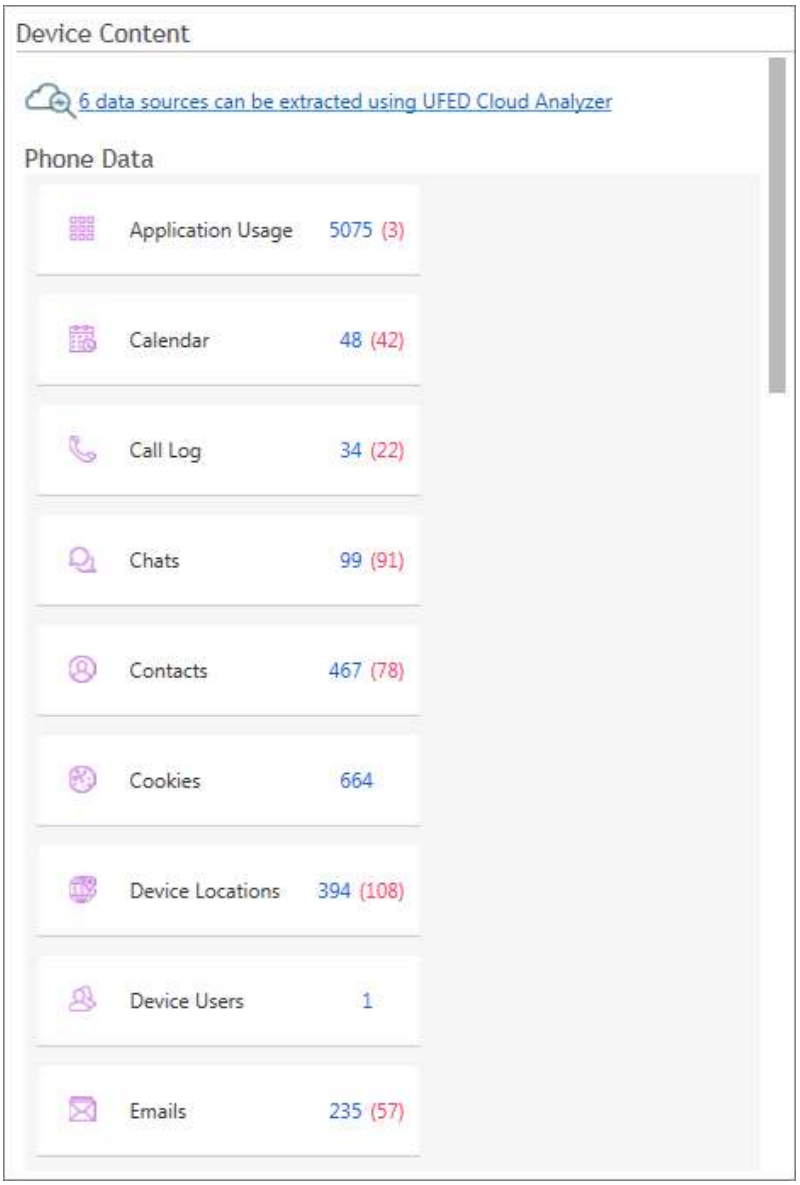


Figura 41. Contenido de dispositivo (el número en azul indica el número total de elementos, y el número en rojo (entre paréntesis) indica que el elemento se ha encontrado en los datos eliminados)

4.5.1 Generar informes

La aplicación Physical Analyzer permite crear informes de los hallazgos en diversos formatos de archivo, como HTML, PDF, Excel (*.xlsx) y XML

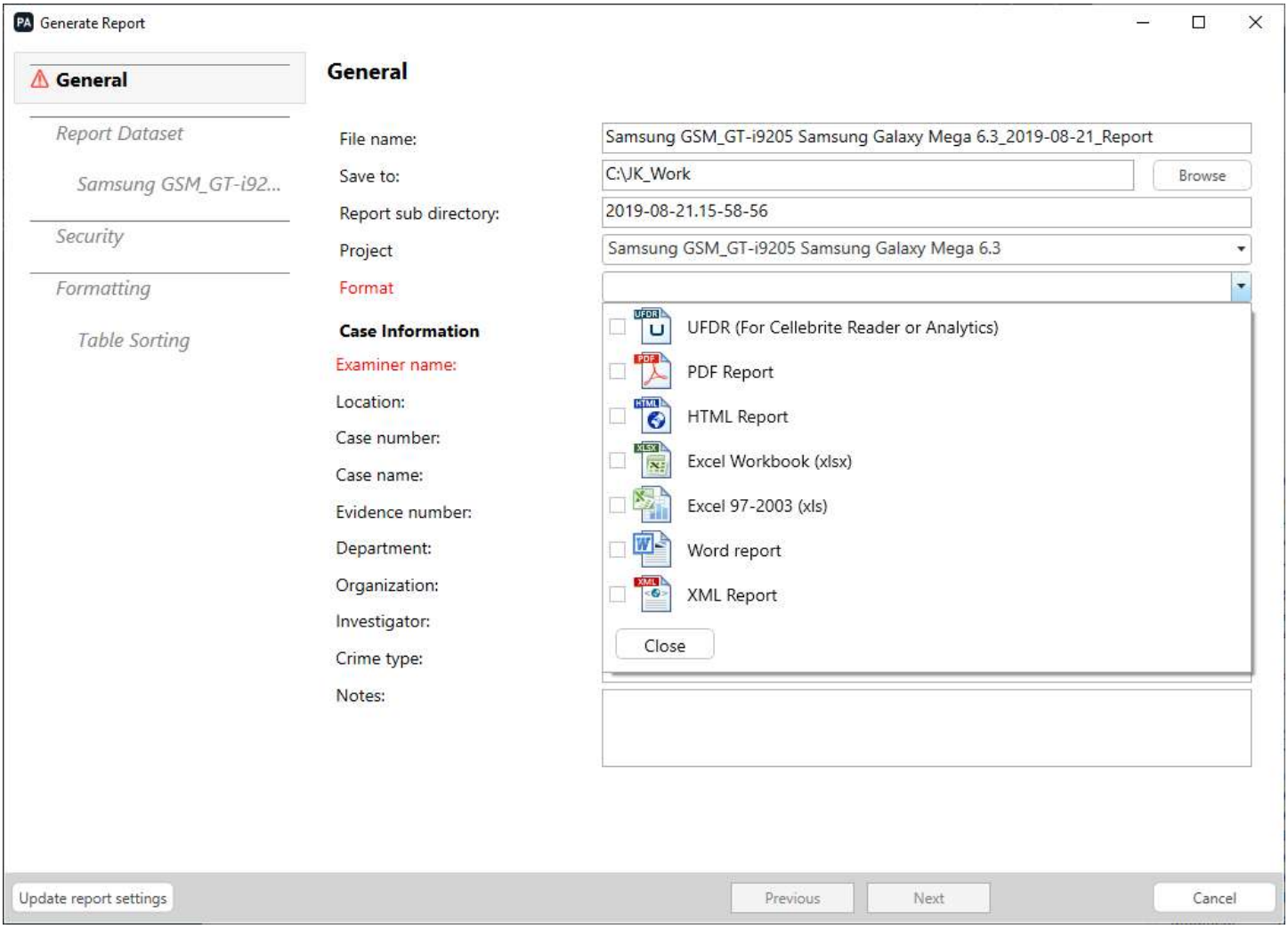
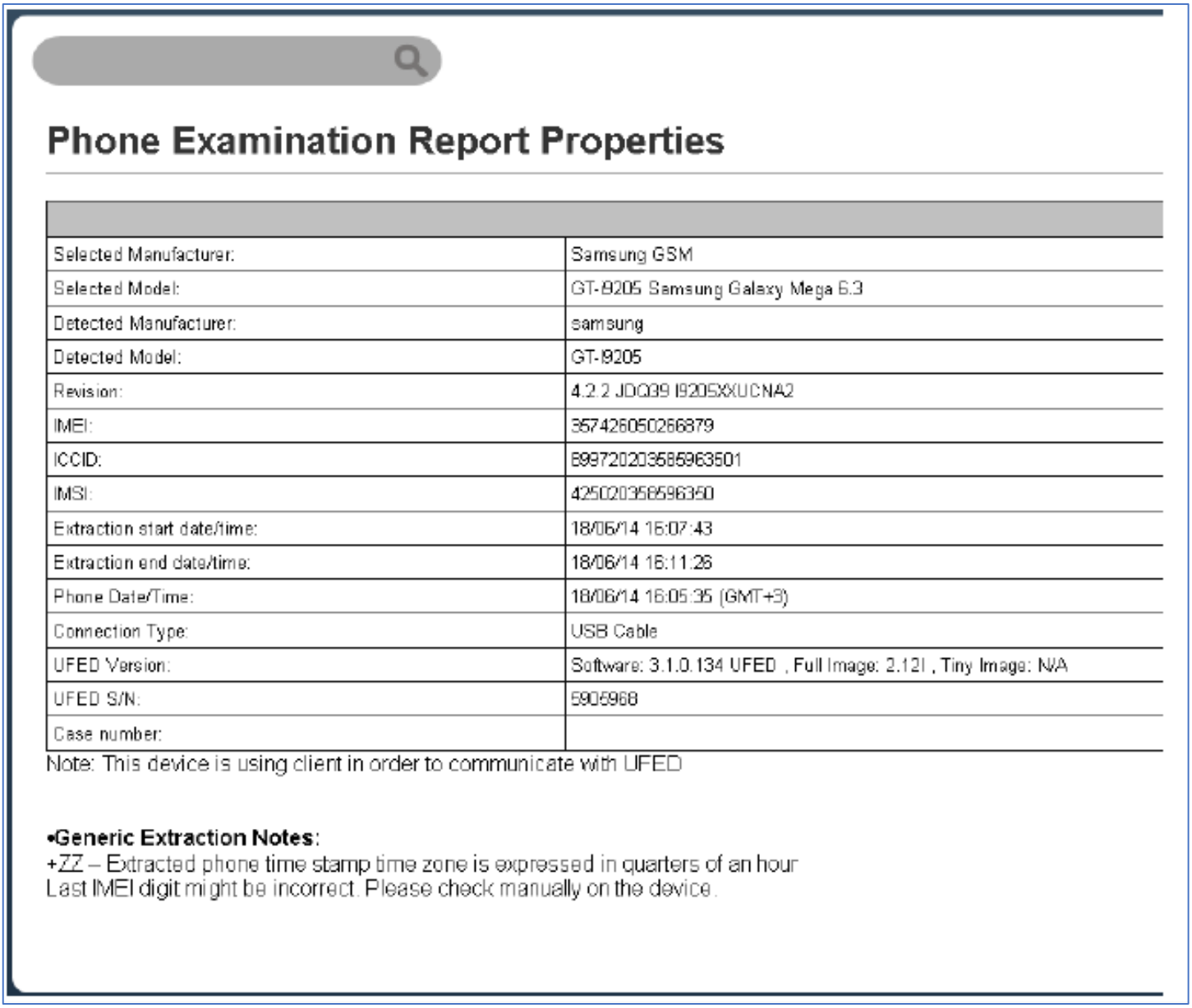


Figura 42. Generando reportes de extracción.

Aquí es donde podemos visualizar la extracción de los datos y registros del dispositivo móvil, generando un reporte en PDF o Word para anexar al dictamen o informe. Puede ser completo o parcial dependiendo de lo que se necesite.



Phone Examination Report Properties

Selected Manufacturer:	Samsung GSM
Selected Model:	GT-I9205 Samsung Galaxy Mega 6.3
Detected Manufacturer:	samsung
Detected Model:	GT-I9205
Revision:	4.2.2 JDQ39 I9205XXUCNA2
IMEI:	357426050266879
ICCID:	8997202035859635O1
IMSI:	425020358596350
Extraction start date/time:	18/06/14 16:07:43
Extraction end date/time:	18/06/14 16:11:26
Phone Date/Time:	18/06/14 16:05:35 (GMT+3)
Connection Type:	USB Cable
UFED Version:	Software: 3.1.0.134 UFED , Full Image: 2.12l , Tiny Image: N/A
UFED S/N:	5905968
Case number:	

Note: This device is using client in order to communicate with UFED

•Generic Extraction Notes:
+ZZ – Extracted phone time stamp time zone is expressed in quarters of an hour
Last IMEI digit might be incorrect. Please check manually on the device.

Figura 43. Propiedades del reporte.

5. CONCLUSIONES

Desde junio de 2018 que entre a laborar a la UECS, desde un inicio me empecé a forjar como investigador en el ámbito de la evidencia digital, realizando desde primer instancia la fijación del indicio hasta el análisis y estudio del mismo, es importante conocer las leyes y el sistema de derecho penal acusatorio, los protocolos y los procedimientos para ser Perito en cualquier ámbito.

Concretamente en el ámbito de la evidencia digital debemos obtener acceso a datos de aplicaciones de terceros, conversaciones de chat, correos electrónicos descargados y archivos adjuntos de correo electrónico, contenido eliminado y más, de dispositivos digitales para la investigación del caso. Utilizamos herramientas y software como UFED de Cellebrite que nos permita llegar a lo que nos solicitan los ministerios públicos, a fin de que aumente las posibilidades de encontrar pruebas incriminatorias y de resolver el caso.

El usar UFED de Cellebrite, como lo mencione anteriormente, nos facilita la obtención de a información que se requiere., aun en el hipotético caso de que el o los dispositivos digital estén dañados, bloqueados, o borrados se puede realizar extracción de información , teniendo un 80% de efectividad, también tengamos en cuenta que día con día los dispositivos digitales se van actualizando, marcas como Android e IOS invierten muchos recursos para proteger sus sistemas operativos (que el cliente tenga la seguridad que su información este segura) de que aplicaciones como UFED puedan extraer información de los mismos.

El UFED de Celebrite también tiene la particularidad de que podemos realizar informes totales o parciales (según lo que se requiera) para la elaboración de reportes y plasmarlos en dictámenes, que es un documento formal de un perito investigador para presentarlo ante un juicio.

Como nota final, se debe tener en cuenta que el procedimiento del equipo UFED y en sí de la extracción de información solo pueden realizarse por medio de profesionistas certificados ya que la información solo puede ser extraída mediante la autorización de un Juez bajo las leyes del Sistema de Justicia Penal Acusatorio, cualquier persona que no tenga el nombramiento para realizar búsquedas forenses caerá en un delito federal el cual se castiga con cárcel.

OPORTUNIDADES DE MEJORA

En la actualidad los datos digitales desempeñan un rol cada vez más importante en las investigaciones y operaciones de todo tipo. Convertir estos datos en accesibles, colaborativos y accionables es lo que realizamos día con día en la unidad. Es por eso que es importante actualizarnos en materia de extracción de evidencia forense, y podremos lograrlo con capacitaciones, cursos, diplomados, aunado a ello las experiencias que obtenemos al momento de realizar la fijación y estudio de un indicio podemos obtener resultados satisfactorios en casi todo los casos que se puedan presentar. También es importante mencionar que podemos obtener software libre e inclusive programar sistemas que nos permitan poder optimizar y mejorar el trabajo de oficina y/o campo. Con respecto al mundo de la telefonía donde hay infinidad de equipos telefónicos, tendremos que estudiarlos y analizarlos en todo momento, ya que siempre se van actualizando y por tanto se es más complicado realizar un estudio y análisis. Por igual se requieren capacitaciones para obtener los mejores resultados y por tanto lograr cumplir las misiones de forma más precisa y efectiva.

Lista de Figuras

Figura 1 Estructura estándar de la telefonía móvil.
Figura 2 Sistema de archivos en la tarjeta SIM
Figura 3. Técnicas de extracción de evidencia digital en dispositivos móviles
Figura 4. Inicio software FORENSIC
Figura 5. Tipos de datos de extracción.
Figura 6. Importar archivos copia de seguridad
Figura 7. Hardware CELLDEK
Figura 8. Equipo UFED
Figura 9. UFED Touch
Figura 10. Visualizacion de lineas del tiempo
Figura 11. Puntas y cables de UFED 4PC
Figura 12. Adaptador de dispositivos
Figura 13. Cable sencillo
Figura 14. Punta UFED
Figura 15. Notificación de tipo de cable a usar.
Figura 16. Seleccionamos el tipo de conexión
Figura 17. Selección de extracción.
Figura 18. Esperando el dispositivo
Figura 19. Extracción en curso
Figura 20. Extracción exitosa
Figura 21. Selección del tipo de extracción.
Figura 22. Seleccionamos el modo de extracción.
Figura 23. Esperando el dispositivo.
Figura 24. Extracción en progreso.
Figura 25. Mensaje de extracción completada.
Figura 26. Seleccionamos el modo de extracción.
Figura 27. Esperando al dispositivo.
Figura 28. Extracción en progreso.
Figura 29. Extracción de sistema de archivos finalizada con éxito.
Figura 30. Seleccionamos el tipo de extracción física.
Figura 31. Seleccionamos la carpeta destino donde se almacenara la extracción.
Figura 32. Esperando el dispositivo.
Figura 33. Extracción en progreso.
Figura 34. Extracción completa con éxito.
Figura 35. Finalizar extracción física.
Figura 36. Mensaje de error.
Figura 37. Decodificación de la información extraída mediante el software Physical Analizer.
Figura 38. Extracción individual
Figura 39. Extracciones múltiples.
Figura 40. Información de dispositivo
Figura 41. Contenido de dispositivo
Figura 42. Generando reportes de extracción.
Figura 43. Propiedades del reporte.

Lista de Tablas

Tabla 1. Requisitos UFED
Tabla 2. Tipos de extracción
Tabla 3. Los tipos de contenido se muestran en una lista de tres formas distintas.
Tabla 4. Información de la extracción.

Lista de Símbolos y Abreviaturas

- FGE Fiscalía General Del Estado
- UECS Unidad Especializada en Combate al Secuestro
- SP Servicios Periciales
- AF Análisis Forense.
- DM Dispositivos Móviles
- ED Evidencia digital
- TI Tecnologías de Información
- PA Phisical Analizer
- DVR Digital Video Recorder
- FB FastBoot
- PTSN Red de Telefonía Pública Conmutada (PublicTelephoneSwitched Network).
- MSC Centro de Conmutación Móvil. (Mobile Switching Center).
- BSC Controladores de Estaciones Base. (Base StationController).
- BTS Estación Transmisora Base. (Base TransceiverStation).
- Cells Celdas Celulares
- IMEI (International Mobile Equipment Identity)
- SIM (Módulo de Identidad del Suscriptor
- NIST (Instituto Nacional de Estándares y Tecnología National Institute of Standards and Technology)
- UIT UNIÓN INTERNACIONAL DE TELECOMUNICACIONES
- JTAG (Joint Test Action Group).
- GPRS servicio general de paquetes vía radio

Bibliografía

1. Internet
   https://www.fiscaliamichoacan.gob.mx/
2. Internet
   https://www.gob.mx/segob/acciones-y-programas/unidades-especializadas-en-combate-al-secuestro-uecs
3. Internet
   http://cdn5.cellebrite.org/Forensic/Forensic%20Documents/User%20Manuals/UFED_Physical_Analyzer/7.33.0/es-es/Content/UFED%20Physical%20Analyzer/UFEDPhysical%20Analyzer/Introduction.htm
4. Internet
   https://www.medigraphic.com/pdfs/forense/mmf-2018/mmf182f.pdf
5. Internet
   http://cdn5.cellebrite.org/Forensic/Forensic%20Documents/User%20Manuals/UFED_Physical_Analyzer/7.33.0/es-es/Content/UFED%20Physical%20Analyzer/Shared%20Topics/Installation%20and%20activation.htm
6. Internet
   http://cdn5.cellebrite.org/Forensic/Forensic%20Documents/User%20Manuals/UFED_Physical_Analyzer/7.33.0/es-es/Content/UFED%20Physical%20Analyzer/UFEDPhysical%20Analyzer/Getting%20started1.htm
7. Internet
   http://cdn5.cellebrite.org/Forensic/Forensic%20Documents/User%20Manuals/UFED_Physical_Analyzer/7.33.0/es-es/Content/UFED%20Physical%20Analyzer/Shared%20Topics/Orientation%20to%20the%20workspace.htm
8. Internet
   http://cdn5.cellebrite.org/Forensic/Forensic%20Documents/User%20Manuals/UFED_Physical_Analyzer/7.33.0/es-es/Content/UFED%20Physical%20Analyzer/Shared%20Topics/Locating%20and%20analyzing%20information.htm
9. Internet
   http://cdn5.cellebrite.org/Forensic/Forensic%20Documents/User%20Manuals/UFED_Physical_Analyzer/7.33.0/es-es/Content/UFED%20Physical%20Analyzer/Shared%20Topics/Translating%20decoded%20data1.htm
10. Internet
    http://cdn5.cellebrite.org/Forensic/Forensic%20Documents/User%20Manuals/UFED_Physical_Analyzer/7.33.0/es-es/Content/UFED%20Physical%20Analyzer/Shared%20Topics/GeneratingReport.htm
11. Internet
    http://cdn5.cellebrite.org/Forensic/Forensic%20Documents/User%20Manuals/UFED_Physical_Analyzer/7.33.0/es-es/Content/UFED%20Physical%20Analyzer/UFEDPhysical%20Analyzer/Performing%20extractions.htm