
**UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA**

**FACULTAD DE SISTEMAS Y TELECOMUNICACIONES**

**TECNOLOGÍAS DE LA INFORMACIÓN**

**PROYECTO DE UNIDAD DE INTEGRACIÓN CURRICULAR**

Previo a la obtención del Título de:

**INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN**

# Técnicas de recuperación de datos en dispositivos móviles mediante el método ISP (In System Programming) y extracción de la memoria eMMC (Controlador Multimedia Embebido) para el análisis de datos.

**AUTOR**

MARLON KEVIN ORTIZ DE LA CRUZ

LA LIBERTAD – ECUADOR

2023

# UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
# FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

## TRIBUNAL DE SUSTENTACIÓN

Ing. José Sánchez Aquino Mgtr.
DIRECTOR DE LA CARRERA

LIDICE VICTORIA HAZ LOPEZ

**Ing. Lídice Haz López**
**Tutor**

Ing. Iván Coronel Suárez Mgtr.
DOCENTE ESPECIALISTA

Ing. Mónica Jaramillo Infante Mgtr.
DOCENTE GUÍA UIC

# UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
# FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

## CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por Marlon Kevin Ortiz De La Cruz, como requerimiento para la obtención del título de Ingeniero en Tecnologías de la Información.

La Libertad, a los 22 días del mes de agosto del año 2023

**TUTOR**

Firmado electrónicamente por:
LIDICE VICTORIA HAZ LOPEZ

**Ing. Lídice Haz López**

# UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
# FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

## DECLARACIÓN DE RESPONSABILIDAD

Yo, **Ortiz De La Cruz Marlon Kevin**

## DECLARO QUE:

El trabajo de Titulación, **"Técnicas de recuperación de datos en dispositivos móviles mediante el método ISP (In System Programming) y extracción de la memoria eMMC (Controlador Multimedia Embebido) para el análisis de datos."** previo a la obtención del título en Ingeniero en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.
En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

La Libertad, a los 22 días del mes de agosto del año 2023

**Marlon Kevin Ortiz De La Cruz**

# UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENAFACULTAD DE SISTEMAS Y TELECOMUNICACIONES

## CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado **Técnicas de recuperación de datos en dispositivos móviles mediante el método ISP (In System Programming) y extracción de la memoria eMMC (Controlador Multimedia Embebido) para el análisis de datos**, presentado por el estudiante, **MARLON KEVIN ORTIZ DE LA CRUZ** fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud


correspondienteal 10%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación

**TUTOR**

Firmado electrónicamente por:
LIDICE VICTORIA HAZ LOPEZ

**Ing. Lídice Haz López**

# UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
# FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

## AUTORIZACIÓN

Yo, **Ortiz De La Cruz Marlon Kevin**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de artículo profesional de alto nivel con fines de difusión pública, además apruebo la reproducción de este artículo académico dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

Santa Elena, a los 22 días del mes de agosto del año 2023

**EL AUTOR**

**Marlon Kevin Ortiz De La Cruz**

## AGRADECIMIENTO

*A Dios, por haberme acompañado a lo largo de mi carrera universitaria, por permitir tener una buena experiencia dentro de mi universidad, por ser guía y fortaleza en tiempos difíciles, por haberme brindado una familia maravillosa sobre todo por darme fuerzas para seguir esforzándome y seguir adelante llenándome de fe y sabiduría.*

*A mis padres, les agradezco por haberme inoculado valores y principios, especialmente a mi madre enseñándome que con esfuerzo, voluntad y perseverancia podemos alcanzar objetivos, por haber dado la oportunidad y el privilegio de una buena educación.*

*A mi pequeña hija quien ha sido el principal motor de inspiración para dándome fuerzas para seguir adelante y no ceder, siendo para ella un motivo de ejemplo de superación.*

*A los docentes que me impartieron sus conocimientos para que hoy pueda alcanzar el tan anhelado objetivo. A mis compañeros también por su amistad apoyo y esfuerzo. Gracias a todos he podido concluir con éxito un proyecto que en un principio podría parecer tarea titánica e interminable. Muchas gracias a todos.*

*Marlon Kevin Ortiz De La Cruz*

# DEDICATORIA

*Dedico este trabajo a Dios, por bendecirme en todo momento y seguir dándome fuerzas para continuar alcanzando mis objetivos propuestos.*

*A mis padres quienes me dieron la vida, educación, apoyo y consejos.*

*A mis compañeros de estudio, a mis maestros y amigos, quienes sin ayudas no hubiera podido hacer este trabajo. A todos ellos siempre les tendré presente y les dedico este trabajo con el amor del mundo.*

*Marlon Kevin Ortiz De La Cruz*

**TABLA DE CONTENIDO**

## ÍNDICE DE TABLAS



## ÍNDICE DE ANEXOS

## ÍNDICE DE FIGURA



## ÍNDICE DE IMÁGENES

## RESUMEN

En el marco de este trabajo de investigación, se llevó a cabo una exhaustiva evaluación de las técnicas de análisis forenses para la extracción de datos de dispositivo móviles mediante métodos invasivos, en ambientes controlados, garantizando la aplicación efectiva de cada proceso. Se tomo como base la metodología DoJ2, adaptándola para cada etapa del análisis, incluyendo el método ISP y extracción de memoria (Chip Off) a partir de la memoria eMMC.

Para lograr la efectividad de los dos procesos, se establecieron 5 escenarios controlados que replicaban situaciones reales de perdida de datos o situaciones en las que el acceso a la información era limitado por bloqueos de seguridad o daños en el sistema operativo. La metodología DoJ2 fue una herramienta clave en este trabajo, ya que brinda un enfoque estructurado y meticuloso para llevar a cabo los análisis forenses de evidencias digitales. Cada etapa del proceso se ajustó y aplico cuidadosamente a los procedimientos de ISP y extracción de memoria, siguiendo las pautas establecidas por la metodología antes mencionada.



**Palabras Claves:** DoJ2, Método ISP, Método extracción de memoria (Chip Off), Memoria eMMC.

## ABSTRACT

In the context of this research, we conducted a comprehensive evaluation of forensic analysis techniques for data extraction from mobile devices using invasive methods in controlled environments, ensuring the effective implementation of each process. The DoJ2 methodology was used as a foundation, adapting it to each stage of the analysis, including the ISP method and memory extraction (Chip Off) from the eMMC memory.

To achieve the effectiveness of these two processes, we established 5 controlled scenarios that replicated real data loss situations or instances where access to information was limited due to security locks or system damage. The DoJ2 methodology was a key tool in this study, offering a structured and meticulous approach to conducting forensic analysis of digital evidence. Each stage of the process was carefully adjusted and applied to the ISP and memory extraction procedures, following the guidelines established by the aforementioned methodology.



Keywords: DoJ2, ISP method, Memory extraction (Chip Off), eMMC Memory.

## INTRODUCCIÓN:

En la era digital actual, los dispositivos móviles se han convertido en una parte esencial de nuestra vida cotidiana, sirviendo como herramientas fundamentales para la comunicación, el trabajo, el entretenimiento y el almacenamiento de información personal y profesional. Sin embargo, esta dependencia creciente de nuestros dispositivos móviles también ha traído consigo nuevos desafíos, especialmente en lo que respecta a la pérdida de datos y la seguridad de la información. Desde fallos del sistema hasta daños físicos o incluso actos malintencionados, son diversos los factores que pueden resultar en la pérdida de datos valiosos. Ante esta problemática, se han desarrollado técnicas avanzadas y sofisticadas para recuperar datos de dispositivos móviles de manera efectiva y segura.

En este contexto, el presente trabajo de investigación se enfoca en abordar un tema de gran relevancia y actualidad en el campo de la recuperación de datos: "Técnicas de recuperación de datos en dispositivos móviles mediante el método ISP (In System Programming) y extracción de la memoria eMMC (Controlador Multimedia Embebido) para el análisis de datos." Estas técnicas, que han ganado popularidad en el ámbito de la ciberseguridad y la investigación forense, ofrecen soluciones efectivas para acceder a datos previamente inaccesibles debido a bloqueos de seguridad o problemas de software.

El método ISP (In System Programming) se ha convertido en una de las herramientas más potentes para recuperar datos en dispositivos móviles. Esta técnica implica la conexión directa al hardware interno del dispositivo, lo que permite sortear las limitaciones impuestas por el sistema operativo y el software de seguridad. Con el acceso a nivel de hardware, los expertos en recuperación de datos pueden recuperar información incluso en situaciones en las que el sistema operativo está dañado o no responde.

Por otro lado, la extracción de la memoria eMMC (Controlador Multimedia Embebido) es otra técnica crucial en la recuperación de datos. La eMMC es una solución de almacenamiento utilizada en dispositivos móviles y ofrece ventajas como el menor consumo de energía y una mayor fiabilidad. Sin embargo, debido a su naturaleza integrada, puede resultar más difícil acceder a los datos almacenados en ella. En este trabajo, exploraremos en detalle cómo la extracción de la memoria eMMC, combinada con el método ISP, se convierte en una poderosa herramienta para el análisis de datos en dispositivos móviles.

El objetivo de esta investigación es proporcionar una visión exhaustiva y completa de estas técnicas de recuperación de datos. Se abordarán aspectos teóricos y prácticos, desde los

fundamentos y principios detrás del método ISP y la extracción de la memoria eMMC, hasta las herramientas y procedimientos específicos utilizados en estos procesos. También se analizarán casos de estudio y ejemplos reales de su aplicación exitosa en situaciones donde la recuperación de datos tradicional no ha sido suficiente.

Además, este trabajo también explorará los desafíos y consideraciones éticas asociadas con estas técnicas. Si bien son herramientas valiosas en el campo de la recuperación de datos, su aplicación debe llevarse a cabo con la máxima precaución y respeto a la privacidad de los usuarios y las leyes aplicables.

El presente trabajo de investigación representa una contribución significativa al campo de la recuperación de datos en dispositivos móviles. Al entender a fondo las técnicas de ISP y la extracción de la memoria eMMC, los profesionales en ciberseguridad, la investigación forense y la protección de datos estarán mejor preparados para enfrentar los desafíos actuales y futuros en la recuperación de datos en el mundo móvil. A través del conocimiento y aplicación adecuada de estas técnicas, se podrán preservar datos valiosos y garantizar la integridad y seguridad de la información en un entorno cada vez más digitalizado y conectado.

# 1. FUNDAMENTACIÓN

## 1.1. ANTECEDENTES

A nivel mundial, el uso extensivo de dispositivos móviles ha llevado a un aumento en el almacenamiento y transmisión de enormes volúmenes de datos Con los avances en tecnología, los fabricantes de dispositivos continúan agregando más funciones lo que lleva al lanzamiento de nuevos modelos cada semana [1]. La protección con contraseña y el cifrado predeterminado del dispositivo ahora son la norma para muchos de estos dispositivos, lo que dificulta que las fuerzas del orden encuentren formas precisas de extracción y análisis de datos que podrían utilizarse potencialmente como evidencia digital en una investigación forense, la dificultad también se da cuando el dispositivo ha sufrido daños externos y no encienda [1].

El análisis forense en dispositivos móvil es a menudo una tarea difícil en algunos casos como, por ejemplo: las condiciones organizativas internas, falta de conocimiento o falta de estándares o buenas prácticas; y condiciones tales como: el desconocimiento o la falta de leyes hacen incluso imposible la investigación [2]. Pero no siempre la imposibilidad viene determinada por la capacidad técnica sino más bien por los requisitos legales que exigen en el momento de presentar una evidencia que proceden de este tipo de dispositivos, una de las condiciones clave para la recopilación de pruebas es la asepsia, una práctica que garantiza que las pruebas recopiladas no estén contaminadas y, por lo tanto, puedan utilizarse de manera efectiva en procesos, judiciales cuando todas las operaciones se llevan a cabo bajo una estricta cadena de custodia. completamente documentada [2].

En otros casos, la dificultad es técnica, porque para preservar suficientemente la evidencia, debe haber sido recolectada con éxito con anterioridad, es decir. dentro de la ley y durante el cobro de manera que se garantice su integridad; la principal desventaja es que no existe un estándar global para tales tareas. Otro aspecto que considerar es la variedad de marcas de dispositivos móviles y sistemas operativos. Como resultado, deja insubsistente la evidencia recopilada, ya sea por deficiencias en las normas o por amenazas a la integridad de la información debido a un procesamiento incorrecto de la información [2].

La extracción de la memoria eMMC para la obtención de datos es uno de los métodos utilizado dentro de una investigación forense, cuando el dispositivo móvil ha sufrido daños: caídas, restablecimiento de fábricas, ataques al chip de memoria, etc. [3]. El eMMC, que consiste en memoria flash y el controlador de memoria se utilizan en los dispositivos digitales modernos como medio de almacenamiento. Sin embargo, sus funciones seguras, como Secure Erase y

Sanitize, hacen que la recuperación de datos sea una tarea desafiante en su proceso [3]. Por la poca información de las técnicas adecuadas que se deben aplicar cuando se extraen dicha memoria surge la necesidad de desarrollar una investigación.

En la revista tecnológica "**Guía práctica abierta para el análisis forense digital en dispositivos Android (Revista Ibérica de sistemas y tecnologías de la Información - Colombia)"**, nos indica que como resultado dentro de las herramientas que manejan la filosofía del software libre se encuentran una gama de posibilidades que posibilitan realizar un análisis forense en un entorno académico. Las herramientas de fácil adquisición por su disponibilidad para su descarga y uso, su bajo costo es fundamentales en un entorno académico donde los recursos son limitados, donde el proceso se centra en la investigación y aprendizaje [4]. Pero también nos hace referencia que las guías que se tiene al nivel internacional para el análisis forense de los dispositivos móviles se están quedando cortas debido al rápido avance que tienen estos aparatos y por la falta de actualización de estas por parte de las instituciones que las soportan, además nos indica que los modelos forenses estudiados están más orientados al proceso forense en general, a los equipos de cómputos tradicionales y a las redes de comunicación [4]. No se encuentran muchos modelos que estén orientados a dispositivos móviles y los pocos que hay hacen énfasis al proceso de la cadena de custodia. Es por ello, que surge la necesidad de identificar las técnicas que permitan el manejo correcto de los dispositivos para la extracción de la información y su posterior análisis.

En la tesis **"Marco de trabajo y herramientas para el análisis forense en la atención de los delitos informáticos de cibergrooming bajo los dispositivos móviles Android (Universidad Católica de Cuenta - Ecuador)",** indica que como resultado la aplicación de metodología Digital Forensics Research Workshop (DFRW) propuesta para el desarrollo del dicho estudio, permitió identificar el proceso a seguir, al momento de realizar una investigación forense en dispositivos móviles ya que permite analizar, obtener y manejar adecuadamente la evidencia [5].

## 1.2. DESCRIPCIÒN DEL PROYECTO

El proyecto consiste en un estudio sobre técnicas de recuperación de datos en dispositivos móviles mediante el método ISP y extracción de la memoria eMMC para su respectivo análisis de datos. Con el objetivo de explorar las diversas técnicas y herramientas disponibles como Easy Jtag Plus, UFI box, para extraer datos de dispositivos móviles y analizar la información almacenada en la memoria.

Los dispositivos móviles que serán examinados corresponden a teléfonos inteligentes que utilizan la plataforma Android. El proyecto tiene como enfoque principal la preservación de la integridad y privacidad de los datos recuperados. Esto implica garantizar que la información extraída sea confiable y no se vea comprometida de ninguna manera durante el proceso de recuperación y análisis, para lo cual se utilizara la guía forense internacional DoJ2.

El proyecto incluirá la realización de pruebas y experimentos en dispositivos móviles, para evaluar la eficacia de las técnicas de recuperación de datos. Utilizando herramientas forenses digitales para realizar análisis en profundidad. Estas técnicas pueden ser utilizadas por investigadores y profesionales de la seguridad digital.

La guía forense DoJ2 es una guía del departamento de justicia de los EE. UU., es el "Examen Forense de Evidencia Digital" (Forensic Examination of Digital Evidence: A Guide for Law Enforcement ).esta guía establece estándares y mejores prácticas para garantizar que las pruebas digitales sean recopiladas, preservadas, analizadas y presentadas de manera adecuada y legalmente válida y está estructurada de la siguiente manera:

- **Desarrollar políticas y procedimientos con el fin de darle un buen trato a la evidencia**
- **Determinar el curso de la evidencia a partir del alcance del caso.**
- **Adquirir la evidencia.**
- **Examinar la evidencia.**
- **Documentación y reportes.**
- **Anexos.**

## 1.3. OBJETIVOS DEL PROYECTO

### 1.3.1. OBJETIVO GENERAL

Aplicar técnicas forenses para recuperación de datos en dispositivos móviles, por medio de herramientas especializadas para extracción y análisis según el modelo de los dispositivos.

### 1.3.2. OBJETIVOS ESPECÍFICOS

- Utilizar técnicas forenses para garantizar la integridad de los datos almacenados en la memoria eMMC del dispositivo móvil.
- Diseñar 5 escenarios experimentales para obtener los datos de la memoria eMMC mediante un archivo de imagen forense.

- Definir procedimientos forenses de acuerdo con los escenarios experimentales que permitan garantizar la efectividad de la recuperación de datos.
- Elaborar informes técnicos con los resultados de los casos de manera estructurada de acuerdo con la guía forense DoJ2.

## 1.4. JUSTIFICACIÓN DEL PROYECTO

La informática forense es una disciplina que permite la identificación, adquisición, preservación y análisis de evidencia a través de la investigación, utilizando modelos y técnicas forenses en áreas específicas de casos penales y civiles, permite la resolución de disputas legales en los tribunales [6]. No obstante, el conocimiento técnico es imprescindible para la recuperación de datos e información, con el desarrollo de la tecnología en los últimos años, la demanda de conocimientos informáticos se ha incrementado, ya que la evidencia digital se ha convertido en información muy importante para la reconstrucción de los hechos en las investigaciones [6]. El personal técnico requiere de profundo conocimiento, correcto trabajo, sistema y métodos de aplicación para identificar, obtener, recuperar y analizar información visible u oculta.

La integridad de la información asegura que la evidencia digital se mantenga durante todo el proceso de investigación. Cualquier modificación o alteración de los daos podría invalidar y afectar la credibilidad de los hallazgos, también es importante para el reconocimiento legal de las evidencias en los tribunales ya que los sistemas de justicias requieren pruebas solidad y confiables para estableces la culpabilidad o inocencia de una persona, si la integridad de la información se ve comprometida, se cuestionará la validez de la evidencia presentada.

Frente a los desafíos de utilizar la evidencia digital en el sistema de justicia penal como prueba para resolver delitos, las autoridades judiciales necesitan una regulación adecuada que brinde acceso a la evidencia digital legalmente admisible que ayude a resolver conflictos con base en la recopilación, los métodos científicos. Análisis y validación.

El proyecto está dirigido a cualquier persona o entidad que tenga interés en el estudio de técnicas de recuperación de datos en dispositivos móviles y en la preservación de la integridad y privacidad de los datos recuperados a continuación se presentan los beneficiarios del proyecto:

- Expertos en informática forense: Utilizando el proyecto como guía para mejorar su capacidad para recuperar datos de dispositivos móviles y llevar a cabo investigaciones forenses.

- Agencias de aplicación de la ley: Al tener acceso a la información presentada mediante este proyecto de las herramientas y métodos aplicadas en la extracción y recuperación de datos en dispositivos móviles en el contexto de investigaciones criminales.
- Empresas de recuperación de datos: las empresas especializadas en recuperación de datos pueden utilizar las técnicas y herramientas desarrolladas para mejorar su capacidad para recuperar datos de dispositivos móviles y ofrecer servicios más efectivos y eficientes a sus clientes.
- Usuarios finales: los usuarios finales que hayan perdido sus datos en dispositivos móviles y no tengan acceso a ellos podrían beneficiarse al tener mayores posibilidades de recuperar su información perdida.
- Académicos e investigadores: los resultados de la tesis pueden ser útiles para académicos e investigadores interesados en el campo de la informática forense y la recuperación de datos en dispositivos móviles.

El proyecto se encuentra orientado a los objetivos que detalla el Plan Creación de Oportunidades, haciendo énfasis en el eje de seguridad integral y en el eje institucional, detallando los siguiente:

**Para el eje Seguridad Integral**

**Objetivo 9** se basa en Garantizar la seguridad ciudadana, orden público y gestión de riesgos [7].

**Política 10.1. -** Fortalecer al estado para mantener la confidencialidad, integridad y disponibilidad de información frente a amenazas provenientes de ciberespacio y proteger su infraestructura critica [7].

## 1.5. ALCANCE DEL PROYECTO

Teniendo en cuenta los beneficios del trabajo el alcance de proyecto se centra en la recuperación de dispositivos móviles que utilizan el sistema operativo Android, específicamente desde la versión 4.0 hasta la 10.0 y de los fabricantes de dispositivos móviles como Samsung, Huawei, Xiaomi, Oppo, Vivo, Realme, Tecno y LG ya que todos ellos utilizan la plataforma Android en sus dispositivos. Las memorias pueden variar según sus particiones y unidades lógicas.

El desarrollo de las técnicas empleadas estará desglosado con actividades que permitan a la investigación tener conocimientos claros y concisos en cada escenario que representen las pruebas de análisis.

- **Fase 1:** Identificación del incidente y alcance de la investigación.
    - Establecer políticas y procedimientos para garantizar la integridad y la protección de la evidencia.
    - Determinar alcance del caso y fuentes potenciales de evidencia.
- **Fase 3:** Adquirir la evidencia.
    - Verificación del estado del dispositivo.
    - Datos claves como marca, versión, etc., del equipo a utilizar
- **Fase 4:** Examinar la evidencia.
    - Recuperación de archivos eliminados.
    - Identificación de patrones en registros de actividad
    - Búsqueda de archivos cifrados.
- **Fase 5:** Documentación y reportes.
    - Proceso de manejo de evidencia.
    - Detalles de hallazgos.
    - Conclusiones del caso.
    - Anexos.

Estas fases están diseñadas para garantizar el manejo de la evidencia en informática forense de una manera cuidadosa y rigurosa, lo que a su vez ayuda a garantizar que se obtengan los resultados más precisos y confiables posibles.

## 1.6. METODOLOGÍA DE LA INVESTIGACÓN

Los estudios de alcance exploratorio son comunes en la investigación para familiarizarnos con fenómenos relativamente desconocidos, realizando una indagación completa de un tema específico [8]. Este estudio técnico contendrá aspectos importantes que ayuden a servir de base para la investigación de la tecnología jurídica en el desarrollo de un ambiente controlado como caso de estudio.

Existiendo trabajos relacionados al tema, utilizando técnicas de forma independiente con confianza en sus casos para que no se interfieran con diferentes pruebas. Así, combinado con un estudio detallado y dirigido al tema, se obtiene un amplio conocimiento del proceso requerido. La investigación se realizará utilizando una bibliografía de trabajos relacionados lo

propuesto, implementar, una comparación con las estructuras y diferencias involucradas en el desarrollo.

El estudio experimental distingue dos escenarios generales en los que se puede utilizar el diseño experimental: laboratorio y campo, en este caso se basa en experimentos de campo realizados en una manipulación realista de una o más variables independientes en un ambiente controlado [8].

En términos de enfoque, se podría comenzar la investigación con la exploración de información existente sobre técnicas de recuperación de datos en dispositivos móviles y la extracción, análisis de la memoria eMMC, realizando pruebas experimentales para comparar diferentes técnicas y determinar cuáles son más efectivas. También sería importante considerar la validez y fiabilidad de los resultados obtenidos.

### 1.6.1. DISEÑO DE LA INVESTIGACIÓN

El diseño de la investigación se realizó con una adaptación de la guía forense del departamento de justicia de los EE. UU. (DOJ2) proporcionando una estructura sólida para llevar a cabo la investigación.

### 1.6.2. VARIABLES

- Eficacia de la recuperación de los datos
- Uso de los métodos ISP y extracción de memoria.

### 1.6.3. RECOLECCIÓN Y PROCESAMIENTO DE LA INFORMACIÓN

#### 1.6.3.1. TÉCNICAS DE RECOLECCIÓN DE LA INFORMACIÓN

En esta sección, se proporcionará las técnicas que serán empleadas en la recolección de la información para llevar a cabo este proyecto.

**Estudios bibliográficos:** Se recopiló información de múltiples fuentes, incluyendo guías relacionadas con el análisis forense y la legislación vigente en Ecuador. Para esto, se revisaron diversos artículos científicos, libros electrónicos, tesis, guías para el manejo de evidencia, así como en el Código Orgánico Integral Penal actualmente vigente en el país.

**Observación:** A través de varios casos o situaciones, se evaluó la efectividad de los métodos de extracción de datos, permitiendo identificar cuál de ellos es más adecuado según el estado en que se encuentra el dispositivo.

### 1.6.3.2. PROCESAMIENTO DE LA INFORMACIÓN

Bases de datos indexadas

Ficha de resultados de experimentos

## 1.7. METODOLOGIA DE DESARROLLO DEL PROYECTO

El presente estudio se llevó a cabo en el ámbito de la investigación forense digital de dispositivos móviles adaptando la metodología DoJ2 como referencia, con el objetivo de analizar las técnicas de recuperación de datos mediante el método ISP y la extracción de la memoria eMMC. Orientado en la aplicación de las técnicas para obtener evidencia digital en investigaciones criminales, análisis de incidentes de seguridad y recuperación de datos en casos donde las técnicas tradicionales no son suficientes.

**Fase 1: Identificación del incidente y alcance de la investigación**

Cuando se trata de un dispositivo móvil, esta fase implica identificar el incidente o el motivo de la investigación relacionado con el dispositivo en particular. Esto puede ser un incidente de seguridad, actividad sospechosa, delito cibernético, etc. Además, se define el alcance de la investigación, es decir, los aspectos específicos del equipo y los datos que serán examinados.

**Fase 2: Adquisición de la evidencia**

En esta fase implica la recolección de la evidencia digital del dispositivo. Algunas acciones que pueden llevarse a cabo incluyendo:

- Asegurar el dispositivo (cadena de custodia): Medidas para evitar la alteración o eliminación de la evidencia presente en el dispositivo.
- Hacer una copia forense: Copia bit a bit del contenido del dispositivo, asegurando la integridad de los datos permitiendo el análisis sin modificar los datos originales.
- Recopilar metadatos: Obtener metadatos relevantes del dispositivo como información de fecha y hora, ubicación, registros de llamadas, etc.
- Capturar imágenes: Tomar fotografías o capturas de pantallas de la interfaz del dispositivo, incluidas las aplicaciones relevantes, configuración y cualquier otro detalle importante.

Teniendo aquellos requisitos es aquí donde entran en juego las técnicas de ISP o Chip Off.

**Fase 3: Examinar la evidencia**

Después de la adquisición de la evidencia, se procede a examinar los datos obtenidos durante el análisis forense de un dispositivo móvil. Implica analizar datos extraídos del proceso ya sea por el método ISP o Chip Off, así como de otras fuentes de evidencias recopiladas, como registros de llamadas, mensajes, archivos multimedia, etc.

**Fase 4: Documentación y reportes**

Una vez que se ha realizado el examen de la evidencia y se han obtenido los hallazgos, se procede a documentar y generar informes detallados. Esto incluye describir el proceso de adquisición, técnicas utilizadas, resultados obtenidos del análisis forense y cualquier otra información relevante para la investigación.

### 1.7.1. METODOLOGÍA

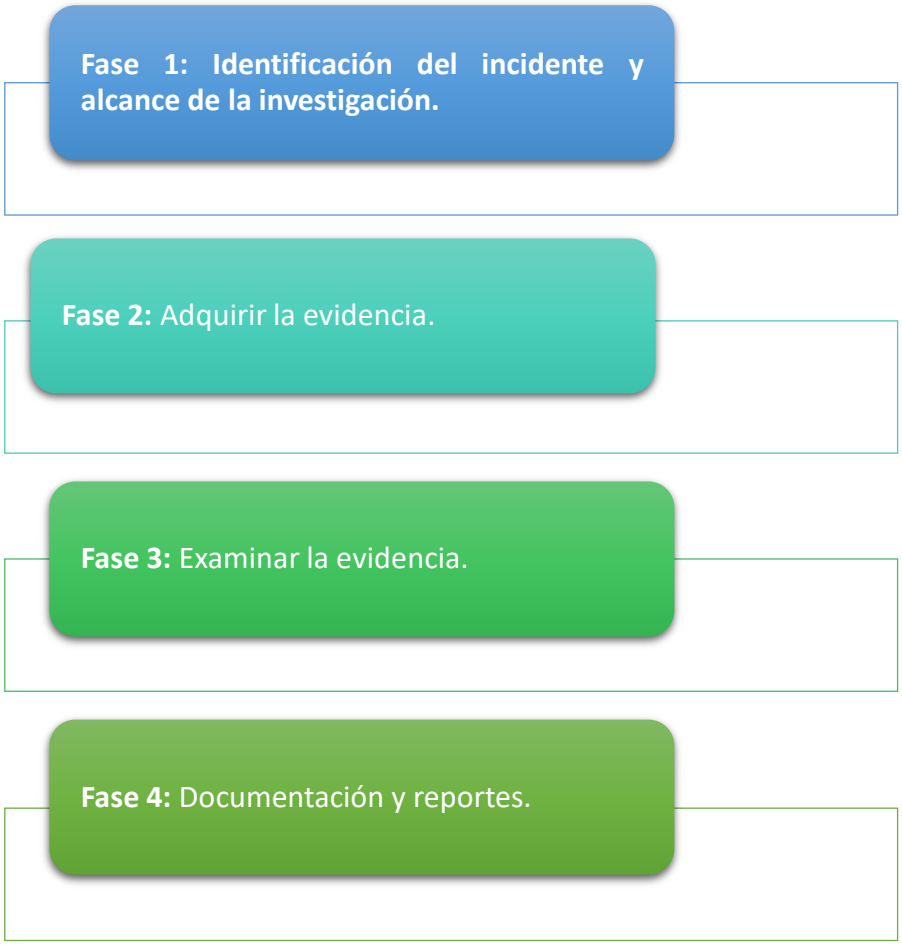



*Figura 1: Metodología Guía del DoJ2 EE. UU.*

# 2. MARCO REFERENCIAL

## 2.1. MARCO TEÓRICO

### 2.1.2. ANTECEDENTES DEL ESTUDIO

En los últimos años, existe un creciente interés en el campo de la recuperación de datos y el análisis forense de dispositivos móviles debido a la cantidad de información digital almacenada en estos dispositivos y su relevancia en investigaciones criminales y análisis de incidentes de seguridad. En el libro "**Seeking the truth from mobile evidence (editorial Acadenic press)**" centrado en el análisis forense, se incluye varias técnicas que permiten la extracción, recuperación y análisis de la información tomando en cuenta las mejores prácticas para manejar evidencia digital, mantener la cadena de custodia, garantizando la integridad de los datos para que sean admisibles en los tribunales [9].

En la tesis "**Herramientas de análisis forense para Android"** de Luisa Araujo Costa Silva se exploran diversas herramientas disponibles para llevar a cabo el análisis forense de dispositivos móviles, específicamente enfocado en dispositivos Android. Concluyendo que no existe una única herramienta que pueda satisfacer todas las necesidades posibles de forma integral. En cambio, resalta la importancia de que el analista esté familiarizado con una amplia variedad de herramientas para poder seleccionar la más adecuada según las particularidades de cada caso. Además, la tesis incluye una guía detallada para acceder a los datos y funcionalidades, presentando una serie de pasos a seguir para completar la documentación necesaria en un proyecto forense [10].

En el trabajo de investigación "**Definición de una metodología de adquisición de evidencia digitales basadas en estándares internacionales**", publicada por la revista ibérica de sistemas y tecnologías de investigación, lleva a cabo un análisis de las normas y estándares internacionales existentes y relacionados con la adquisición de datos en medios digitales, generando una comparación que permitió el desarrollo de una nueva metodología [11].

El presente trabajo que tiene como objeto de estudio la recuperación de datos por medio de técnicas como la ISP y la extracción de memoria en los diferentes escenarios propuestos. En el campo de la informática forense, los expertos se enfrentan a diversos desafíos al examinar dispositivos móviles, especialmente aquellos que ejecutan el sistema operativo Android, que es el más comúnmente utilizado en el mundo. Estas dificultades incluyen: Falta de soporte para todos los dispositivos, gran cantidad de programas y datos, diversidad de datos valiosos, eliminación de archivos por parte de los delincuentes, costo de herramientas especializadas, son algunos obstáculos que deben superar en su labor [12].

Los expertos en informática forense que realizan pruebas de penetración a menudo combinan diferentes métodos para maximizar las posibilidades de obtener los datos necesarios. Cada método tiene sus propias ventajas y desafíos, y la elección del método dependerá de las circunstancias específicas del caso o escenarios y las limitaciones del dispositivo [12].

El método ISP permite la comunicación directa con el procesador del dispositivo móvil para acceder a la memora eMMC sin tener que desoldarla físicamente. Mediante una interfaz especializada y un conjunto de cables que conectan a los puntos de conexión (VCC, VCCQ, CMD, DAT0/DAT3, CLK, VSS.), dependiendo del tipo de memoria estas son eMMC/eMCP. Mediante este método se puede leer los datos directamente en la memoria lo que permite extraer información importante del dispositivo.

Mediante el método de extracción de la memoria eMMC que implica desmontar la memoria de la placa principal del dispositivo utilizando un lector de memoria para lectura o escritura de los datos almacenados. Siguiendo el proceso para la obtención de la información se crea una copia o imagen completa de la memoria para luego ser analizado por herramientas forenses o de recuperación de datos.

### 2.1.3. EFICACIA DE LA RECUPERACIÓN DE LOS DATOS

La eficacia de la recuperación de datos refleja la capacidad de las técnicas aplicadas, se evalúa considerando la tasa de éxito de la información recuperada, la proporción de los casos en los que las técnicas aplicadas logran extraer los datos deseados de manera correcta, una alta tasa de éxito indicaría que las técnicas utilizadas son efectivas para la recuperación de datos de manera consistente.

También depende de la calidad de los datos recuperados, refiriéndose a la integridad y la exactitud de los datos que se desea recuperar la calidad de los datos se evalúa considerando si la información recuperada es completa, precisa y coherente con los datos originales. Una buena calidad de los datos recuperados indica que las técnicas utilizadas preservan la integridad de la información.

Y por último se evalúa la cantidad de datos que se logra recuperar en comparación con la cantidad total de datos perdidos o inaccesibles. Una alta cantidad de información recuperada indica que las técnicas de recuperación son efectivas para extraer la mayor cantidad posible de datos perdidos.

### 2.1.4. USO DE LOS MÉTODOS ISP Y EXTRACCIÓN DE MEMORIA.

El uso de los métodos ISP y extracción de memoria implica la aplicación de técnicas especializadas para acceder y extraer los datos almacenados en la memoria eMMC de los dispositivos móviles. Estos métodos se diferencian en la forma en que se accede a la memoria, ya sea a través de la comunicación directa con el procesador o mediante la extracción física de la memoria. Al utilizar estos métodos, se pueden obtener beneficios potenciales, como un mayor grado de acceso a los datos y una mayor capacidad de recuperación.

#### 2.1.4.1. MÉTODO ISP Y SU APLICACIÓN EN LA RECUPERACIÓN DE DATOS.

Utilizado en la extracción de datos es el método ISP (In-system programming) o ICSP (in circuit serial programming). A diferencia del método JTAG, el método ISP es invasivo, pero no destructivo. Permite realizar un volcado completo de la memoria incluso en dispositivos dañados, como placas principales, pantallas rotas, conectores USB dañados, microprocesadores o circuitos de alimentación, siempre y cuando la memoria de datos esté funcionando [13].

Este método es capaz de extraer datos de dispositivos protegidos con claves de usuario, como patrones o contraseñas. Sin embargo, es importante destacar que el volcado de memoria solo será legible si la memoria de datos no está encriptada. Para aplicar el proceso, es necesario localizar los siguientes pines en la placa base:

- VPP o VDDF: Tensión de Programación
- VDD: Alimentación Positiva
- VSS: Alimentación Negativa
- CLK: Reloj
- DAT0: Bus de Datos Serie
- CMD: Bus de Comandos

Estos pines permiten establecer una conexión para acceder a la memoria de datos y realizar el volcado de la misma [13].

#### 2.1.4.2. MÉTODO CHIP-OFF Y SU APLICACIÓN EN LA RECUPERACIÓN DE DATOS.

La extracción de datos a través del método de chip-off es una técnica invasiva y destructiva que se utiliza cuando otros métodos, como ISP, no son viables debido a la falta de conexiones necesarias en la placa de circuito impreso (PBC). Este método permite realizar un volcado completo de la memoria inclusivo en dispositivos dañados, como placas principales, pantallas

rotas, conectores USB dañados, microprocesadores o circuitos de alimentación, siempre y cuando la memoria de datos esté funcionando [13].

El método Chip-off también posibilita la extracción de datos incluso en dispositivos que tienen tipo de seguridad con clave de usuario, como patrones o contraseñas. Sin embargo, es importante destacar que el volcado de memoria solo será legible si la memoria de datos no está encriptada. Implica extraer el chip que contiene los datos mediante la de soldadura de la placa de circuito, una vez extraído, el chip se puede leer para obtener una imagen de los datos almacenados en él. Con este enfoque, es posible recuperar archivos, incluso aquellos que han sido eliminados, de dispositivos que están físicamente dañados [13].

## 2.2. MARCO CONCEPTUAL

### 2.2.1. PROCESO DE ARRANQUE DE UN DISPOSITIVO ANDROID

Entender el proceso de arranque de un dispositivo Android es fundamental para comprender otras técnicas forenses que implican interactuar con el dispositivo en diferentes niveles. Cuando encendemos un dispositivo Android por primera vez, se sigue una secuencia de pasos que permite cargar en la memoria el firmware, el sistema operativo, los datos de las aplicaciones, entre otros elementos necesarios. A continuación, se presenta la secuencia de pasos involucrados en el proceso de arranque de Android [14]:

1. Boot ROM. Inicio de la ejecución del código ROM de arranque.
2. Bootloader. El administrador de arranque.
3. Kernel de Android.
4. Init. El proceso de inicio del sistema.
5. Zygote y Dalvik.
6. System Server. El servidor del sistema.

BootROM es el encargado de ejecutar el código de arranque ROM cuando se presiona el botón de encendido. Esta ROM, protegida contra escritura y ubicada en el chip de la CPU, realiza la inicialización del resto del hardware del dispositivo. Una vez completada esta tarea, busca la partición de arranque, generalmente ubicada en la memoria NAND, y copia el Bootloader en la memoria RAM [14].

El Bootloader, también conocido como gestor de arranque, es un código que se ejecuta antes del sistema operativo. Su función principal es configurar un entorno mínimo que permita la ejecución del sistema operativo y dar inicio al proceso de arranque. Aunque el Bootloader no es específico de Android, contiene las instrucciones que indican al dispositivo cómo iniciar y

localizar el núcleo del sistema (KERNEL) [14]. Además, el Bootloader es donde el fabricante puede establecer bloqueos y restricciones en el dispositivo. Es fundamental porque verifica la integridad de las particiones de arranque y recuperación antes de transferir el control al núcleo del sistema (KERNEL). También proporciona acceso a otros modos de arranque, como el modo de flasheo/fastboot y el modo de recuperación [14].

El kernel de Android es el núcleo central del sistema operativo, encargado de manejar procesos, gestionar la memoria y aplicar medidas de seguridad en el dispositivo. Una vez que se carga el kernel, se inicia la caché de configuración, la memoria protegida y la programación [14]. También se cargan los controladores iniciando los demonios del kernel. Posteriormente, se inicia el sistema de archivos raíz (rootfs). Una vez que el kernel ha completado la configuración del sistema, busca el archivo "init" en los archivos del sistema y comienza a ejecutar el proceso [14].

INIT: El inicio del sistema operativo Android comienza con el proceso "Init", que desempeña un papel fundamental al ser el proceso primario y el punto de partida. El proceso Init inicia su búsqueda de un archivo denominado "init.rc" en el Sistema de Archivos (File System), el cual contiene la configuración esencial para el arranque inicial del sistema [14]. A través de este archivo, se pondrán en marcha los procesos de servicio del sistema necesarios. Finalmente, como resultado de este proceso, el logotipo distintivo de Android se mostrará en la pantalla, indicando que el sistema ha sido cargado correctamente.

Zygote y Dalvik: El proceso Zygote recibe solicitudes para iniciar aplicaciones a través de /dev/socket/zygote. Una vez que recibe una solicitud, desencadena una llamada fork(). La bifurcación (fork) crea un clon del proceso actual en un espacio de memoria separado, de manera eficiente. Cuando esto ocurre en Zygote, se crea un nuevo Dalvik VM limpio y exacto como un hilo, pre-cargado con todas las clases y recursos necesarios que cualquier aplicación pueda requerir [14]. Esto permite que el proceso de creación de una VM y carga de recursos sea altamente eficiente y propicia el intercambio de código en la máquina virtual Dalvik, lo que contribuye a lograr un tiempo de inicio mínimo para las aplicaciones en Android [14].

System Server: El servidor del sistema, conocido como "System Server", entra en funcionamiento después de que Zygote precarga todas las clases y recursos necesarios. El primer paso es cargar una biblioteca nativa llamada "android_servers", que proporciona interfaces para funcionalidades nativas [14]. Luego, se llama al método nativo "init", que configura los servicios nativos. A continuación, se crea el hilo del servidor, el cual iniciará los

servicios restantes en el sistema según el orden de inicio necesario. Cada servicio se ejecuta en un hilo Dalvik separado dentro del System Server [14].

Una vez que los servicios del sistema están en funcionamiento en la memoria, Android ha completado el proceso de arranque. En este momento, se activa la acción de transmisión estándar "ACTION_BOOT_COMPLETED". Tras esto, el dispositivo muestra la pantalla de inicio y está listo para interactuar con el usuario. Este proceso asegura que todos los servicios y componentes del sistema estén disponibles y funcionando correctamente, lo que permite una experiencia de usuario fluida y completa [14].

### 2.2.2. RECUPERACIÓN DE DATOS EN DISPOSITIVOS MÓVILES.

La recuperación de datos en dispositivos móviles se refiere al proceso de acceder y recuperar información almacenada en teléfonos inteligentes, tabletas u otros dispositivos móviles. Se aplica generalmente cuando los datos se pierden debido a un fallo del sistema, eliminación accidental, daño físico, bloqueo del dispositivo, entre otros escenarios [15].

El proceso de recuperación de datos en dispositivos móviles puede implicar diferentes técnicas y enfoques, que incluyen:

- **Copias de seguridad y sincronización:** Si el usuario ha realizado copias de seguridad regulares de sus datos móviles, se pueden restaurar fácilmente desde la copia de seguridad. Esto puede implicar utilizar servicios de almacenamiento en la nube, como iCloud o Google Drive, o herramientas de respaldo específicas proporcionadas por el fabricante del dispositivo [15].
- **Software de recuperación de datos:** Existen herramientas de software especializadas que pueden escanear el dispositivo móvil en busca de datos eliminados o perdidos. Estos programas pueden recuperar mensajes de texto, contactos, fotos, videos y otros tipos de archivos. Sin embargo, su efectividad puede variar según el estado del dispositivo y el tipo de datos que se intenta recuperar [15].
- **Extracción física de datos:** En casos más complejos, donde el dispositivo está dañado o no puede iniciarse correctamente, se pueden utilizar técnicas de extracción física. Esto puede implicar la extracción de memoria, así como el uso de técnicas de soldadura para acceder directamente a los chips de memoria del dispositivo [15].

### 2.2.3. TÉCNICAS DE RECUPERACIÓN DE DATOS: MÉTODOS Y PROCEDIMIENTOS.

La información que se obtiene mediante el análisis forense actualmente tiene mucha relevancia en los procesos judiciales, forma parte de la evidencia que se presenta en los casos para su resolución. Existen diferentes métodos y procedimientos utilizados para extraer y analizar datos de dispositivos móviles en el campo de la investigación forense digital los más comunes son [16]:

- **Extracción física:** Consiste en obtener una copia bit a bit de la memoria del dispositivo móvil, incluyendo el sistema operativo y los datos almacenados. Esto se puede lograr mediante la extracción del chip eMMC o mediante la clonación del dispositivo utilizando herramientas especializadas [16].
- **Extracción lógica:** En este método, se extraen los datos del sistema operativo y las aplicaciones sin acceder directamente a la memoria física del dispositivo. Esto se realiza mediante el uso de herramientas de software que se conectan al dispositivo a través de interfaces como USB o Wi-Fi y extraen los datos a nivel de archivo [16].
- **Adquisición del sistema de archivos:** Permite obtener los archivos visibles mediante el sistema de archivos, no incluye archivos eliminados ni particiones ocultas. Dependiendo del tipo de investigación, puede utilizarse este método que es menos complicado que la extracción física [16]. Para ello se utiliza el mecanismo integrado en el sistema operativo para realizar una copia de los archivos, Android Device Bridge (ADB) en caso de Android. Con este método, se puede recuperar parte de la información eliminada, ya que algunos SO como Android e iOs utilizan una infraestructura que almacena la mayor parte de la información mediante una base de datos SQlite [16].

### 2.2.4. TÉCNICAS INVASIVAS DE ADQUISICIÓN.

Las técnicas invasivas de adquisición son métodos utilizados en la investigación forense digital que implican la manipulación física del dispositivo o medios de almacenamiento para obtener acceso a los datos. Estas técnicas se utilizan en situaciones en las que los métodos convencionales de extracción de datos no son viables o no brindan los resultados deseados.

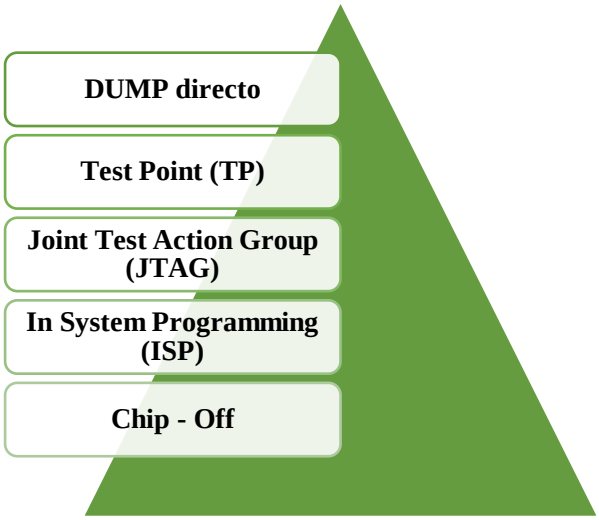



*Figura 2: Técnicas Invasivas.*

### 2.2.4.1. DUMP

El "DUMP directo" es una técnica de adquisición invasiva que implica extraer directamente la memoria o el almacenamiento del dispositivo y realizar una copia bit a bit de todos los datos presentes en ella. Es una forma de obtener una imagen forense del dispositivo que es una réplica exacta de los datos almacenados en su memoria [17].

Para realizar un DUMP directo, se requiere el acceso físico al dispositivo y generalmente implica desmontar el dispositivo y acceder directamente a la memoria o al chip de almacenamiento. Esta técnica se utiliza en situaciones en las que otros métodos no son viables, como cuando el dispositivo está dañado, bloqueado o no se puede acceder a él mediante métodos convencionales [17]. Al realizar un DUMP directo, se copia toda la memoria o el almacenamiento del dispositivo, incluyendo el sistema operativo, los archivos, los metadatos y cualquier otro dato almacenado.

### 2.2.4.2. TEST POINT (TP)

Un "Test Point" (TP) es un punto de prueba utilizado en dispositivos electrónicos, especialmente en dispositivos móviles, para realizar pruebas o realizar acciones específicas durante el proceso de fabricación, reparación o modificación. Estos puntos están diseñados para permitir el acceso a ciertos circuitos o componentes del dispositivo [17].

En el contexto de la recuperación de datos o la extracción de evidencia digital, los Test Point pueden ser utilizados como una técnica invasiva para obtener acceso a áreas críticas del dispositivo que de otra manera serían inaccesibles. Esto se puede realizar utilizando equipos y herramientas especializadas, como cables o sondas, que se conectan a test point y permiten la

comunicación y la extracción de datos. La ubicación y la función varían según el dispositivo y el fabricante [17]. Los Test Point pueden permitir el acceso a la memoria interna, la interfaz del procesador, el controlador de la pantalla u otros componentes importantes del dispositivo. Al utilizarlos, es posible sortear bloqueos de software, recuperar datos o incluso realizar modificaciones en el dispositivo [17].

#### 2.2.4.3. JOINT TEST ACTION GROUP (JTAG)

El Joint Test Action Group (JTAG) es un estándar de comunicación utilizado en la industria electrónica para realizar pruebas, depuración y programación de circuitos integrados (ICs). Fue desarrollado por el grupo de trabajo JTAG y se basa en el estándar IEEE 1149.1 [18].

El propósito principal de JTAG es proporcionar una interfaz estandarizada para acceder a los pines de prueba de los ICs y permitir la comunicación con ellos durante el proceso de producción, diagnóstico, reparación o investigación de dispositivos electrónicos. Estos pines de prueba, también conocidos como pines JTAG o TAP (Test Access Port), se encuentran en la mayoría de los ICs modernos [18].

La interfaz JTAG permite realizar diversas acciones, entre ellas:

- **Pruebas funcionales:** Se pueden realizar pruebas de continuidad y funcionamiento de los circuitos internos del IC.
- **Depuración:** Permite depurar los circuitos internos del IC y realizar pruebas de diagnóstico.
- **Programación y configuración:** Se utiliza para programar y configurar los ICs, como microcontroladores o FPGA, durante su proceso de fabricación o actualización de firmware.

Dentro de la investigación forense digital, el método de JTAG o llamado también forense de JTAG se utiliza para acceder a los ICs de dispositivos móviles y otros dispositivos electrónicos a nivel de hardware. Esto permite la lectura y escritura de datos en los chips internos del dispositivo, como la memoria flash o los controladores, para obtener acceso a los datos almacenados [18]. La utilización de JTAG requiere equipos y herramientas especializadas, como programadores y software específico. Sin embargo, es importante destacar que no todos los dispositivos electrónicos admiten la interfaz JTAG, y su disponibilidad puede variar según el dispositivo y el fabricante [18].

### 2.2.4.4. IN SYSTEM PROGRAMMING (ISP)

In System Programming (ISP) es un método utilizado para acceder y programar directamente el circuito integrado de un dispositivo electrónico sin la necesidad de retirarlo de su placa base. Permite la actualización o reprogramación del firmware y la configuración de un dispositivo sin desmontarlo [18].

ISP se utiliza en una amplia variedad de dispositivos electrónicos, incluyendo microcontroladores, circuitos integrados, placas de desarrollo, dispositivos de almacenamiento, entre otros. La principal ventaja de ISP es la posibilidad de actualizar o reprogramar un dispositivo sin necesidad de desoldar el circuito integrado o retirarlo de la placa base, lo que ahorra tiempo y evita posibles daños al dispositivo [18].

El proceso de ISP generalmente implica el uso de un programador ISP, que se conecta al dispositivo a través de puertos o pines de prueba específicos en la placa base. El programador ISP establece comunicación directa con el circuito integrado y permite la transferencia de datos para la programación o actualización del firmware [18].

Aplicaciones que incluyen en el ISP:

- **Actualización de firmware:** ISP se utiliza para actualizar el firmware de dispositivos electrónicos, como routers, impresoras, cámaras de seguridad, entre otros. Esto permite corregir errores, agregar nuevas funciones o mejorar el rendimiento del dispositivo.
- **Recuperación de datos:** En situaciones en las que un dispositivo no se inicia correctamente o tiene problemas de software, ISP puede ser utilizado para acceder a la memoria del dispositivo y recuperar datos importantes.
- **Reparación de dispositivos:** ISP permite la reprogramación de circuitos integrados en dispositivos electrónicos, lo que puede ayudar a reparar problemas de funcionamiento o solucionar errores en el firmware.

### 2.2.4.5. CHIP – OFF (Extracción de memoria eMMC)

El término "Chip-Off" se refiere a una técnica invasiva utilizada en la investigación forense digital para extraer el chip de memoria eMMC o almacenamiento de un dispositivo electrónico con el fin de acceder a los datos almacenados en él. Esta técnica implica el retiro físico del chip de la placa base del dispositivo y su posterior lectura utilizando herramientas especializadas [18].

Procesos del Chip - off:

1. **Desmontaje del dispositivo**

Se desmonta el dispositivo electrónico para acceder a la placa base y al chip de memoria o almacenamiento que se desea extraer. Esto puede requerir habilidades y herramientas específicas para desoldar o retirar el chip de forma segura.

2. **Extracción del chip**

Una vez expuesto el chip, se procede a retirarlo de la placa base. Esto se puede realizar mediante técnicas de desoldado, corte controlado u otros métodos especializados dependiendo del tipo de dispositivo y la tecnología del chip.

3. **Preparación del chip**

Una vez extraído, el chip debe ser preparado para su lectura. Esto puede incluir la limpieza de cualquier residuo de soldadura, la preparación de los pines o contactos del chip y la protección de la integridad física del chip.

4. **Lectura del chip**

El chip extraído se coloca en un lector o programador especializado que permite la lectura de los datos almacenados en él. Esto implica la conexión de los pines o contactos del chip al lector para la transferencia de dato. Se realiza una copia de los datos para su análisis y evitar modificar la original o en caso de que exista algún daño.

5. **Análisis de los datos**

Una vez que se ha realizado la lectura del chip, los datos obtenidos se analizan para su interpretación y extracción de la evidencia digital relevante. Esto puede incluir la recuperación de archivos, registros de actividad, metadatos u otros datos de interés forense.

### 2.2.5. TIPOS DE MEMORIAS

Los dispositivos móviles utilizan diferentes tipos de memorias para cumplir diversas funcionalidades esenciales, como el almacenamiento temporal de datos, el funcionamiento del sistema operativo y aplicaciones, los principales tipos de memoria son:

La memoria RAM (Random Access Memory) es una memoria volátil que se utiliza para almacenar temporalmente los datos en ejecución, es de acceso rápido esto permite que cargue y ejecute de manera eficiente las aplicaciones. Cuando el dispositivo se apaga, los datos

almacenados en la memoria se borran, por tanto, tiene una capacidad limitada y su función es proporcionar un espacio de trabajo para el procesador.

La memoria interna ROM (Read-Only Memory) es la memoria de almacenamiento principal del dispositivo móvil. Aquí se almacena el sistema operativo Android, las aplicaciones preinstaladas y los datos del usuario a diferencia de la memoria RAM, la memoria interna no es volátil, lo que significa que los datos almacenados permanecen incluso cuando se apaga el dispositivo. Determina la capacidad de almacenamiento del dispositivo y puede variar el tamaño según el modelo del dispositivo.

En los dispositivos móviles modernos, la memoria interna es reescribible, lo que permite que los datos se guarden, actualicen y eliminen según ser necesario.

1. La memoria eMMC (Controlador Multimedia Embebido) es una forma común de memoria ROM que combina el almacenamiento flash NAND y el controlador de memoria en un solo chip. Es ampliamente utilizada en smartphones y tabletas debido a su tamaño compacto, bajo consumo de energía y eficiencia de costos. La eMMC se utiliza para almacenar el sistema operativo, aplicaciones preinstaladas y datos del usuario.
2. La memoria UFS (Universal Flash Storage) es una tecnología más avanzada que ofrece una mayor velocidad de transferencia de datos en comparación con la eMMC. Esto la convierte en una opción popular para dispositivos de gama alta que requieren un rendimiento más rápido y eficiente. La UFS se utiliza en algunos smartphones y otros dispositivos móviles de alta gama.
3. La memoria NAND es una tecnología de memoria flash utilizada tanto en dispositivos móviles de gama baja como en algunos modelos más antiguos. Ofrece una capacidad de almacenamiento más económica, pero puede tener velocidades de escritura y lectura más bajas en comparación con las tecnologías más nuevas como la eMMC y la UFS.

Cabe recalcar que existen diferentes tipos de memorias que desempeñan roles importantes en el almacenamiento y funcionamiento de los dispositivos móviles, en (Anexo_1) se presenta una tabla con la descripción y características de los distintos tipos de memoria.

### 2.2.6. ESTRUCTURA DE UNA MEMORIA.

Cada partición tiene un propósito específico, almacena datos, archivos relacionados con las funciones clave del dispositivo.

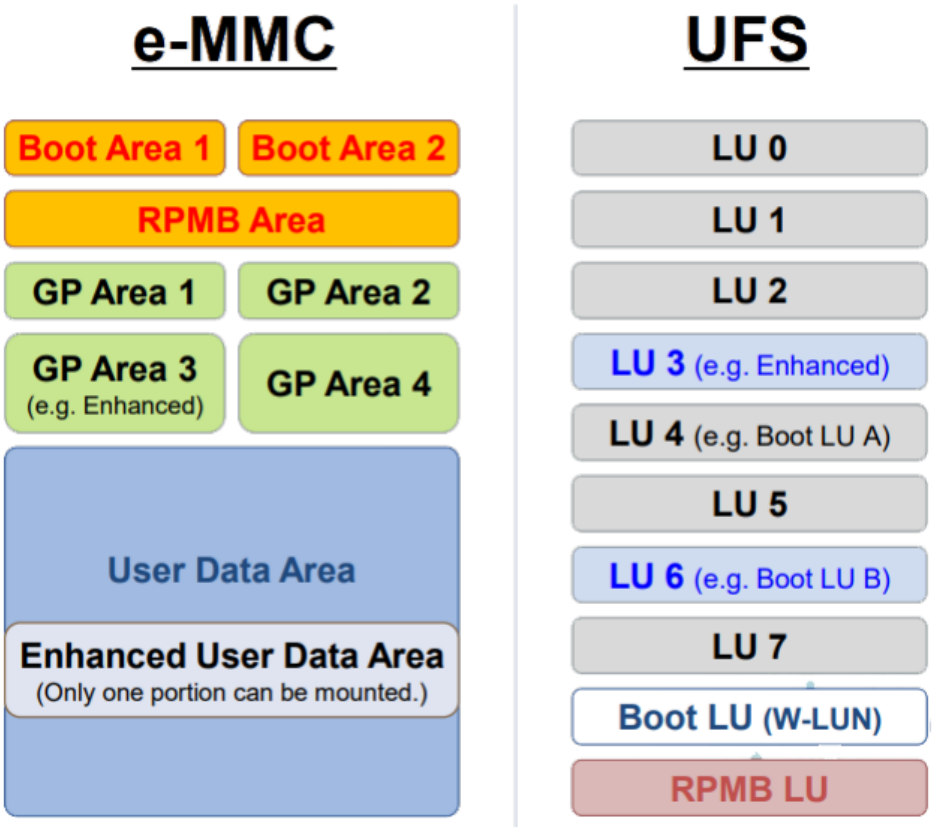



*Imagen 1: Particiones eMMC, Unidades Lógicas UFS.*

| **USERAREA/0X 00/0X38** | **BOOT1/0X08** | | **BOOTI/0X08** | **BOOTI/0X08** |
|---|---|---|---|---|
| **Qualcomm** | **EXYNOS** | **MEDIATEK** | **Spreadtrum** | **HISILICON** |
| GPT | GPT | GPT | GPT | GPT |
| FSG | EFS | NVDATA | L_FIXNV1 | OEMINFO |
| MODEMST1 | SEC_EFS | NVRAM | L_FIXNV2 | CERTIFICATIO N |
| MODEMST2 | | PROTECT1 | L_RUNTIMEN V1 | MODEMNVM_F ACTORY |
| | | PROTEC2 | L_RENTIMEN V2 | MODEMNVM_B ACKUP |
| | | NVCFG | PRODNV | VRL |
| | | | | VRL_BACKUP |
| | | | | NVME |
| | | | | MODEM_SECU RE |

| | | | | |
|---|---|---|---|---|
| | | | | SECURE_STOR AGE |

*Tabla 1: Tipos de memoria y sus particiones.*

### 2.2.7. HERRAMIENTAS

- **EASY JTAG PLUS BOX**

Herramienta de servicio universal que ofrece una solución integral para arranque del teléfono, reparación del firmware del chip, recuperación de datos y el análisis forense digital, admite una variedad de protocolos incluyendo eMMC, Jtag, ISP, SPI y NAND. Permitiendo realizar operaciones de escritura y lectura de memorias proporcionado soluciones de problemas de software y restaurar el funcionamiento del dispositivo [19].

- **UFI BOX**

Es una herramienta de servicio EMMC de gran potencia que brinda diversas funciones relacionadas con el manejo de datos en dispositivos EMMC, es capaz de leer datos de usuarios almacenados en la memoria, ofrece opciones para reparar, cambiar tamaño, formatear, borrar, leer, escribir y actualizar el firmware en EMMC de dispositivos de varias marcas incluyendo Samsung, teléfonos chinos, SK Hynix, Kingston entre otros [20].

- **MEDUSA PRO V2**

Es una herramienta completa y altamente confiable para el servicio y reparación de circuitos de memoria en teléfonos dañados. Ofrece trabajar con memorias UFS y EMMC a velocidades elevadas y programar circuitos sin necesidad de desoldarlos, gracias al uso de enchufes BGA de alta precisión [21].

- **DZKJ**

Herramienta profesional de consulta de información de reparación de teléfonos móviles, cuenta con diagramas completos para la interpretación de circuitos y sus conexiones [22].

- **ADAPTADORES LECTORES DE MEMORIAS EMMC**

Conjunto de adaptadores que está diseñado para ser utilizado con una caja de liberación Box y ofrece la capacidad de trabajar con memorias EMMC en microchips de diversas marcas, como Samsung, china pone SK Hynix, Toshiba, Kingston, Micron y otras [21].

- **ESTACIÓN DE CALOR**

Estación de soldadura de aire caliente es un tipo de herramienta de soldadura que utiliza aire caliente para fundir la soldadura de los componentes electrónicos. Esta estación es especialmente útil para desmontar o soldar componentes de tipo SMD (Surface Mount Device), debido a su capacidad para alcanzar temperaturas precisas y controladas [23].

- **MICROSCOPIO**

Es una herramienta de investigación muy valiosa debido a su capacidad para ampliar imágenes, es posible aumentar el tamaño de las muestras a niveles muchos más altos, permitiendo observar detalles minuciosos y obtener imágenes de alta resolución [24].

- **MULTÍMETRO**

Es una herramienta esencial para los técnicos en las industrias eléctricas y electrónicas, permite medir y evaluar los valores clave de tensión, corriente y resistencia. Esto les ayuda en el diagnóstico y solución de problemas en sistemas eléctricos y electrónicos [25].

- **ALAMBRE BARNIZADO**

Es un tipo de alambre que está recubierto con múltiples capas de esmalte, lo que le proporciona aislamiento eléctrico y resistencia mecánica, este tipo de alambre se fabrica tanto de cobre como en aluminio y se utiliza en una variedad de industrias [26].

- **FLUX**

También denominado fundente para soldar es un producto químico que se presenta en forma de una fluida. Su función principal es eliminar el óxido presente en los componentes que van a ser soldados, al aplicar el flux sobre los componentes, se logra una limpieza efectiva que facilita el proceso de soldadura [27].

- **ESTAÑO**

Se emplea durante el proceso de soldadura para mejorar la calidad y eficiencia de unión de componentes, actúa como un agente limpiador y desoxidante, facilitando la correcta adhesión del estaño a las superficies metálicas [27].

- **LIMPIA CONTACTO**

Este producto es útil para eliminar la suciedad de una amplia variedad de dispositivos eléctricos y electrónicos, como circuitos impresos, conectores eléctricos, mecanismos de relojería e instrumentos de precisión [28].

- **PLANCHA SEPARADORA DE PANTALLA**

Esta herramienta garantiza una separación segura y sin complicaciones ayudando a optimizar el tiempo de trabajo [29].

- **CABLE USB**

El mercado ofrece una amplia variedad de cables USB con diferentes tipos de conexiones, niveles de calidad y precios, son utilizados para conectar y transferir datos entre dispositivos electrónicos, como teléfonos móviles, tables, computadoras entre otros periféricos [30].

- **FUENTE DE ALIMENTACIÓN**

También conocida como fuente de laboratorio, se utiliza para suministrar energía eléctrica controlada y ajustable a diferentes dispositivos y componentes en entornos de laboratorio [31].

- **LIMPIADOR ULTRASÓNICO**

Un limpiador ultrasónico es un equipo especializado que utiliza ondas de alta frecuencia y cavitación acústica para proporcionar una limpieza optima en objetos delicados o de difícil acceso. Este dispositivo es especialmente útil para eliminar suciedad y bacterias que otros métodos de limpieza no pueden alcanzar [32].

**Herramientas forenses**

| Herramienta | Descripción |
|---|---|
| **Autopsy** | En un programa forense digital de código abierto que sirve para analizar discos duros y teléfonos inteligentes de una manera eficiente |
| **Open-Source Android Forensics** | Un framework que se emplea para la distribución a través de imágenes de una máquina virtual que recoge diversas herramientas que nos dan la posibilidad de analizar aplicaciones de dispositivos móviles. Los análisis disponibles sin tanto estáticos, dinámicos o forenses. |
| **Lime Linux Memory Extractor** | Es un software que nos da la opción de obtener un volcado de información, de forma volátil, en dispositivos con base Linux. Como por ejemplo los teléfonos con sistema operativo de Android. |
| **Android Data Extractor Lite (ADEL)** | Herramienta desarrollada por Python que nos da la posibilidad de sacar un flujograma forense derivado de la base de datos del dispositivo móvil analizado. Para poder llevar a cabo este proceso necesitamos que el móvil este rooteado o instalar previamente un *recovery* personalizado. |
| **Forensic Toolkit** | Forensic Toolkit (FTK) es una herramienta forense informática desarrollada por AccessData, una empresa especializada en soluciones de seguridad digital y análisis forense. FTK es ampliamente utilizado en investigaciones forenses digitales para analizar y recuperar datos de dispositivos electrónicos y medios de almacenamiento, como discos duros, memorias USB, smartphones y otros dispositivos. |
| **Caine** | CAINE (Computer Aided INvestigative Environment), que es una distribución de Linux especializada en análisis forense digital. CAINE es una herramienta de código abierto diseñada para ayudar a los investigadores y analistas forenses en la recuperación y análisis de datos en medios digitales, como discos duros, memorias USB, smartphones, etc. |

| | |
|---|---|
| **Foca** | FOCA (Fingerprinting Organizations with Collected Archives), que es una herramienta desarrollada por ElevenPaths, una compañía de ciberseguridad perteneciente a Telefónica. FOCA es una herramienta de código abierto utilizada para realizar análisis de seguridad y obtención de información sobre la infraestructura y sistemas de una organización. |
| **Forensic Toolkit** | La herramienta Forensic Toolkit (FTK) es un software de análisis forense digital desarrollado por AccessData. Es ampliamente utilizada en investigaciones legales y forenses para adquirir, analizar y presentar evidencia digital recopilada de dispositivos y medios de almacenamiento. |

*Tabla 2: Herramientas forenses.*

## 2.3. MARCO LEGAL

Cuando se trata de extraer información de dispositivos móviles, es fundamental tener en cuenta la legislación vigente en Ecuador y cómo se aplica durante las distintas etapas del análisis forense. A continuación, se presentan algunos artículos y reglamentos relevantes extraídos del Código Integral Penal, que son de especial importancia para el presente trabajo de investigación.

Código Orgánico Integral Penal **(COIP)**, el código integral penal del Ecuador contempla una serie de consecuencias legales para los delitos informáticos y de telecomunicaciones cometidos en el país. Entre estos delitos se encuentran acciones como:

**Art. 190.-** Apropiación fraudulenta por medios electrónicos. - La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona mediante la alteración, manipulación o modificación del funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, es sancionada con pena privativa de libertad de una tres años [33].

La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes [33].

**Art. 191.-** Reprogramación o modificación de información de equipos terminales móviles. - La persona que reprograme o modifique la información de identificación de los equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años [33].

**Art. 232.-** Ataque a la integridad de sistemas informáticos. - La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años [33].

Con igual pena será sancionada la persona que:

a) Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo [33].
b) Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general [33].

Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad [33].

**Art. 233.-** Delitos contra la información pública reservada legalmente. - La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años [33].

La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años [33].

Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad [33].

**Art. 234.-** Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años [33].

**Art. 456.-** Cadena de custodia. - Se aplicará cadena de custodia a los elementos físicos o contenido digital materia de prueba, para garantizar su autenticidad, acreditando su identidad y estado original; las condiciones, las personas que intervienen en la recolección, envío, manejo, análisis y conservación de estos elementos y se incluirán los cambios hechos en ellos por cada custodio [33].

La cadena inicia en el lugar donde se obtiene, encuentra o recauda el elemento de prueba y finaliza por orden de la autoridad competente. Son responsables de su aplicación, el personal del Sistema especializado integral de investigación, de medicina legal y ciencias forenses, el personal competente en materia de tránsito y todos los servidores públicos y particulares que tengan relación con estos elementos, incluyendo el personal de servicios de salud que tengan contacto con elementos físicos que puedan ser de utilidad en la investigación [33].

**Ley de comercio electrónico, firmas y mensajes de datos.**

El propósito de la Ley de Comercio Electrónico, firmas y mensajes de datos es establecer normas y sanciones para regular las actividades relacionadas con sistemas de información, redes relacionadas con sistemas de información, redes electrónicas e internet. Algunos de los aspectos que abarca esta ley incluyen:

**Art. 2.-** Reconocimiento jurídico de los mensajes de datos. - Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta ley y su reglamento [34].

**Art. 7.-** Información original. - Cuando la ley requiera u obligue que la información sea presentada o conservada en su forma original, este requisito quedará cumplido con un mensaje de datos, si siendo requerido conforme a la ley, puede comprobarse que ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos [34].

Se considera que un mensaje de datos permanece integro, si se mantiene completo e inalterable su contenido, salvo algún cambio de forma, propio del proceso de comunicación, archivo o presentación [34].

Por acuerdo de las partes y cumpliendo con todas las obligaciones previstas en esta ley, se podrán desmaterializar los documentos que por ley deban ser instrumentados físicamente [34].

Los documentos desmaterializados deberán contener las firmas electrónicas correspondientes debidamente certificadas ante una de las entidades autorizadas según lo dispuesto en el artículo 29 de la presente ley, y deberán ser conservados conforme a lo establecido en el artículo siguiente [34].

**Art. 8.-** Conservación de los mensajes de datos. - Toda información sometida a esta ley, podrá ser conservada; este requisito quedará cumplido mediante el archivo del mensaje de datos, siempre que se reúnan las siguientes condiciones [34]:

a) Que la información que contenga sea accesible para su posterior consulta;
b) Que sea conservado con el formato en el que se haya generado, enviado o recibido, o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida;
c) Que se conserve todo dato que permita determinar el origen, el destino del mensaje, la fecha y hora en que fue creado, generado, procesado, enviado, recibido y archivado; y,
d) Que se garantice su integridad por el tiempo que se establezca en el reglamento a esta ley.

Toda persona podrá cumplir con la conservación de mensajes de datos, usando los servicios de terceros, siempre que se cumplan las condiciones mencionadas en este artículo. La información que tenga por única finalidad facilitar el envío o recepción del mensaje de datos, no será obligatorio el cumplimiento de lo establecido en los literales anteriores [34].

**Art. 9.-** Protección de datos. - Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros [34].

La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los

cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente [34].

No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato [34].

El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo [34].

**Art. 10.-** Procedencia e identidad de un mensaje de datos. - Salvo prueba en contrario se entenderá que un mensaje de datos proviene de quien lo envía y, autoriza a quien lo recibe, para actuar conforme al contenido de este, cuando de su verificación exista concordancia entre la identificación del emisor y su firma electrónica, excepto en los siguientes casos [34]:

a) Si se hubiere dado aviso que el mensaje de datos no proviene de quien consta como emisor; en este caso, el aviso se lo hará antes de que la persona que lo recibe actúe conforme a dicho mensaje. En caso contrario, quien conste como emisor deberá justificar plenamente que el mensaje de datos no se inició por orden suya o que el mismo fue alterado; y [34],
b) Si el destinatario no hubiere efectuado diligentemente las verificaciones correspondientes o hizo caso omiso de su resultado [34].

**Art. 54.-** Práctica de la prueba. - La prueba se practicará de conformidad con lo previsto en el Código de Procedimiento Civil y observando las normas siguientes [34]:

a) Al presentar un mensaje de datos dentro de un proceso judicial en los juzgados o tribunales del país, se deberá adjuntar el soporte informático y la transcripción en papel del documento electrónico, así como los elementos necesarios para su lectura y verificación, cuando sean requeridos [34];
b) En el caso de impugnación del certificado o de la firma electrónica por cualesquiera de las partes, el juez o tribunal, a petición de parte, ordenará a la entidad de certificación de información correspondiente, remitir a ese despacho los certificados de firma electrónica y documentos en los que se basó la solicitud del firmante, debidamente certificados; y [34],

c) El facsímile, será admitido como medio de prueba, siempre y cuando haya sido enviado y recibido como mensaje de datos, mantenga su integridad, se conserve y cumpla con las exigencias contempladas en esta ley [34].

En caso de que alguna de las partes niegue la validez de un mensaje de datos, deberá probar, conforme a la ley, que éste adolece de uno o varios vicios que lo invalidan, o que el procedimiento de seguridad, incluyendo los datos de creación y los medios utilizados para verificar la firma, no puedan ser reconocidos técnicamente como seguros [34].

Cualquier duda sobre la validez podrá ser objeto de comprobación técnica.

**Art. 55.-** Valoración de la prueba. - La prueba será valorada bajo los principios determinados en la ley y tomando en cuenta la seguridad y fiabilidad de los medios con los cuales se la envió, recibió, verificó, almacenó o comprobó si fuese el caso, sin perjuicio de que dicha valoración se efectúe con el empleo de otros métodos que aconsejen la técnica y la tecnología. En todo caso la valoración de la prueba se someterá al libre criterio judicial, según las circunstancias en que hayan sido producidos [34].

Para la valoración de las pruebas, el juez o árbitro competente que conozca el caso deberá designar los peritos que considere necesarios para el análisis y estudio técnico y tecnológico de las pruebas presentadas [34].

**Reglamento del Sistema Pericial Integral de la Función Judicial.**

El reglamento del sistema pericial integral de la función judicial establece directrices particulares que los peritos deben seguir en el desempeño de sus funciones, así como los procedimientos para presentar los informes periciales. Algunos de los aspectos abordados en dicho reglamento incluyen [34]:

**Art. 19.-** Obligaciones Específicas.- Son obligaciones específicas de los peritos:

1. (Sustituido por el Art. 15 de la Res. 067-2016, R.O. 756-2S, 17-V-2016). - Cumplir la orden de la autoridad judicial una vez que han sido designados. En caso de que la calificación pericial venza luego de la designación del perito, éste tendrá igualmente la obligación de presentar su informe y cumplir con todos los deberes inherentes a la orden judicial. El informe y las actuaciones periciales cumplidas en este supuesto tendrán toda la validez legal y procesal que el caso lo amerite [34].

Los peritos podrán presentar su excusa debidamente documentada dentro del proceso, en los siguientes casos [34]:

a) Causas de fuerza mayor o caso fortuito;
b) Ausencia del país previa a la designación;
c) Tener a su cargo más de tres informes periciales pendientes de presentación, ¡tener otra diligencia en otra judicatura o fiscalía; y,
d) Las demás que determine la ley.

2. Presentar el informe correspondiente oportunamente, en la forma, plazos y términos previstos por la normativa o por la autoridad judicial correspondiente. En caso de dificultad o complejidad en su trabajo, tendrá la posibilidad de solicitar motivadamente a la autoridad competente, un solo plazo adicional para presentar su informe, la ampliación o aclaración al mismo, salvo que la normativa legal disponga lo contrario. Se podrán solicitar plazos adicionales al antes establecido de forma excepcional y tomando en consideración las dificultades para la presentación del informe. La jueza, el juez, o la o el fiscal, ¡motivarán la aceptación o no de esta nueva solicitud de ampliación de plazo que presente la o el perito [34];

3. (Sustituido por el Art. 15 de la Res. 067-2016, R.O. 756-2S, 17-V-2016). - Presentar el informe correspondiente, de forma verbal y/o escrita, según lo que la normativa procesal establezca, con los requisitos mínimos establecidos en este reglamento y la ley; y, subirlo al Sistema Informático Pericial, en archivo tipo PDF. En el caso de informes de avalúos de bienes, obligatoriamente se subirán también las fotografías de estos [34];

4. Presentar obligatoriamente y dentro del plazo otorgado, las aclaraciones, ampliaciones o complementos al informe presentado que ordene la autoridad judicial competente. Estas aclaraciones se presentarán de forma verbal y escrita según la normativa que lo establezca [34];

5. Explicar y defender el informe presentado y sus conclusiones, en las audiencias orales, de prueba, o de juicio para las cuales fuere notificado legalmente, si la ley así lo prevé [34];

6. Presentar juntamente con su informe en todos los procesos judiciales o pre procesales, la copia certificada de la factura de honorarios emitida por su persona, por el trabajo pericial realizado [34];

7. Abstenerse de cobrar valores adicionales a los incluidos en la factura presentada en el proceso judicial o pre procesal, por el informe presentado, por las aclaraciones o ampliaciones hechas, por la defensa del informe en audiencia oral, de prueba o de juicio, o por cualquier otra

actividad inherente a su actividad pericial. Los valores de honorarios facturados son únicos, y abarcan todas las obligaciones de los peritos constantes en el presente artículo [34];

8. Aprobar los cursos de capacitación determinados en el presente reglamento; y,

9. Cualquier otra obligación establecida en la normativa legal, en este reglamento y/o por la o el administrador del sistema pericial [34].

**Art. 20.-** Forma. - El informe pericial, sus explicaciones o aclaraciones, se presentarán de forma verbal y por escrito, de conformidad con la normativa procesal correspondiente. En caso de que el informe sea escrito, la jueza o juez o la o el fiscal obligatoriamente lo sube sin los anexos al sistema informático que administra el proceso correspondiente, mediante la constancia e inclusión al momento de hacerlo, el número del código de calificación de perito [34].

Los informes periciales realizados en procesos calificados por la ley como reservados, o que tienen que ver con información restringida por la ley, no, se subirán al sistema informático que administra el proceso correspondiente [34].

| **Artículo COIP** | **Delito** |
|---|---|
| **190** | Aprobación fraudulenta por medios electrónicos. |
| **190** | Aprobación fraudulenta por medios electrónicos con inutilización de alarma, descifrado de claves o encriptados. |
| **234** | Acceso no consentido a un sistema informático, telemático o de telecomunicaciones. |
| **232** | Ataque a la integridad de sistemas informáticos. |
| **231** | Transferencia electrónica del archivo patrimonial. |
| **230** | Interceptación ilegal de datos. |
| **229** | Revelación ilegal de bases de datos. |
| **231** | Transferencia electrónica del archivo patrimonial. La persona que facilite o proporcione su cuenta bancaria para recibir de forma ilegitima un archivo. |

| | |
|---|---|
| **232** | Ataque a la integridad de sistemas informáticos. Persona que diseñe, desarrolle, programe, adquiera, envié, introduzca, ejecute, venda o distribuya dispositivos o programas informáticos maliciosos. |
| **233** | Delitos contra la información pública reservada legalmente. |

**Tabla 3: Delitos de la dirección de política criminal de fiscalía del Ecuador.**

**Nota:** Adaptada de **estadísticas delitoscopio de la dirección de política criminal de fiscalía del Ecuador** [35].

# 3. PROPUESTA

## 3.1. DESARROLLO

### 3.1.1 Fase 1: Identificación del incidente y alcance de la investigación

En el desarrollo de esta fase se hace el proceso de identificación de incidente y la definición del alcance de la investigación. Esta esta etapa es importante para establecer las bases del proceso de investigación y garantizar que se aborden adecuadamente los problemas identificados. Es decir, la evidencia electrónica obtenida en la escena del suceso es recibida para su análisis. Una vez en el laboratorio, el investigador debe identificar la naturaleza del delito bajo investigación para determinar qué evidencias son pertinentes y necesarias para resolver el caso.

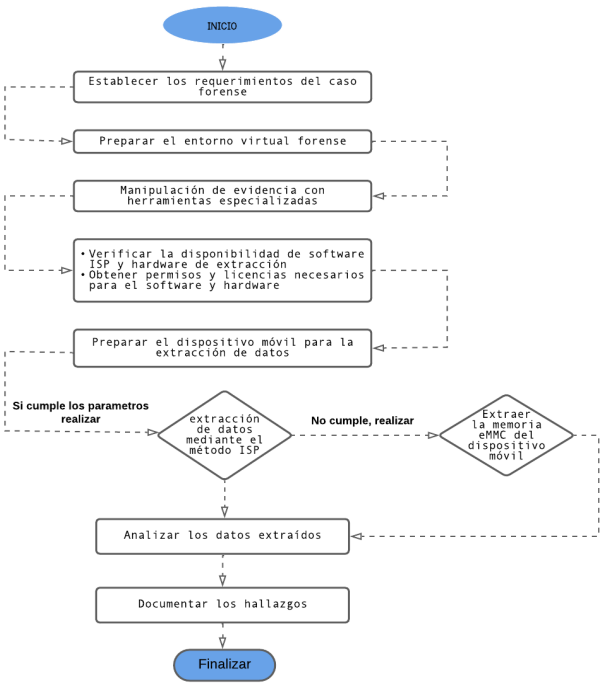



*Figura 1: Proceso de manejo de evidencias.*

Mediante la recepción del dispositivo que se va a analizar, es importante asegurarse de que se mantenga la cadena de custodia (Anexo:7), para garantizar la integridad de la evidencia y pue se pueda utilizar los resultados en el proceso legal. Se registra toda la información relevante del dispositivo, como el modelo, número de serie, IMEI, número de teléfono, versión de sistema operativo, y cualquier otro dato identificativo importante. Además, se debe documentar el estado del dispositivo incluyendo si está bloqueado (Anexo:5 y 6).

Se establece el alcance del análisis del dispositivo, esto incluye que tipo de datos se buscaran, cual es el objetivo del análisis, y que sistemas o aplicaciones específicas se investigarán, se puede incluir la revisión de aplicaciones, registros (logs), mensajes, llamadas, conexiones de red, entre otros.

Dentro de la planificación y preparación para el análisis forense se incluyen las herramientas y técnicas a utilizar dependiendo del escenario y las condiciones en que se encuentra el dispositivo, así como los procedimientos para evitar contaminar o modificar la evidencia.

| PROCEDIMIENTOS | DESCRIPCIÓN |
|---|---|
| **Identificación de dispositivos móviles** | Identificar correctamente el modelo y la marca del dispositivo móvil conectado para determinar la compatibilidad y los métodos de extracción aplicables. |
| **Conexión ISP y CHIP OFF** | Proporcionar una conexión segura y confiable mediante el método ISP para establecer comunicación con el dispositivo móvil y permitir la extracción de datos. |
| **Extracción de datos** | Extraer datos de forma precisa y completa de la memoria eMMC del dispositivo móvil utilizando el método ISP y CHIP OFF, asegurando que no se modifiquen ni dañen los datos originales durante el proceso. |
| **Recuperación de archivos y metadatos** | Recuperar archivos y metadatos relevantes de la memoria eMMC, incluyendo imágenes, videos, mensajes, registros de llamadas, contactos y otra información importante almacenada en el dispositivo móvil. |
| **Análisis forense de datos** | Proporcionar herramientas y funcionalidades para el análisis forense de los datos extraídos, permitiendo la identificación y extracción de evidencia digital, como mensajes eliminados, registros de actividad, geolocalización, etc. |

| | |
|---|---|
| **Generación de informes** | Permitir la generación de informes forenses detallados que documenten de manera clara y organizada los hallazgos, los métodos utilizados, los datos extraídos y cualquier evidencia digital relevante encontrada durante el análisis. |
| **Seguridad y confidencialidad** | Cumplir con altos estándares de seguridad para garantizar la integridad y confidencialidad de los datos extraídos y analizados. |
| **Compatibilidad con diferentes sistemas operativos** | El sistema debe ser compatible con una variedad de sistemas operativos utilizados en dispositivos móviles. |
| **Actualizaciones y mantenimiento** | El sistema debe ofrecer actualizaciones regulares y un soporte adecuado para mantenerse al día con los avances tecnológicos y las nuevas técnicas de recuperación de datos en dispositivos móviles. |

*Tabla 4: Procedimiento para el alcance de la investigación.*

### 3.1.1. Fase 2: Adquirir la evidencia.

El propósito de esta fase consiste en diseñar cuidadosamente el procedimiento de extracción de la evidencia digital, documentarlo adecuadamente para evitar la pérdida de datos relevantes para el caso, y emplear las funciones Hash para asegurar la integridad de dicha evidencia digital, es esencial tener en cuenta:

- Selección de las herramientas forense para la extracción.
- Procedimiento de extracción
- Garantizar la preservación de la evidencia digital.

Se lleva a cabo los procedimientos para obtener una copia forense de los datos almacenados en el dispositivo móvil de manera que la evidencia sea preservada y no se modifique durante el proceso del análisis, es esencial mantener una cadena de custodia adecuada para garantizar la integridad y valides de la información obtenida.

Cuando se habla de cadena de custodia se refiere al registro detallado de todos los movimientos y manipulaciones que se realizan sobre la evidencia desde el momento de su recolección hasta su presentación en un procedimiento legal. El objetivo principal es garantizar que la evidencia sea confiable y que no haya sido alterada o contaminada en ningún momento del proceso, algunos aspectos importantes incluyen:

- Etiquetado: La evidencia debe ser etiquetada con la información específica que la identifique claramente, como el nombre, numero de caso, descripción del dispositivo, fecha y hora de recolección de la información.
- Registro: Todas las personas que manejan la evidencia deben registrar sus nombres, funciones, y el momento en que tuvieron contacto con la misma.
- Seguridad: La evidencia debe almacenarse en un lugar seguro y protegido contra acceso no autorizados o manipulaciones, se debe mantener la integridad de la evidencia, asegurándose de que no se realicen modificaciones, eliminaciones o agregados a los datos durante el proceso de análisis.

Realizar una copia forense de un dispositivo móvil es un paso importante en el análisis, ya que permite obtener una réplica exacta de los datos almacenados en equipos sin modificar datos originales, asegurando que la evidencia preserve su estado original y se evite cualquier alteración involuntaria durante el proceso de análisis. Para realizar la copia se utilizan herramientas especializadas diseñadas para adquirir los datos, estas pueden variar dependiendo del sistema operativo y tipo de dispositivo.

Existen dos enfoques principales para realizar la copia forense, el acceso físico (método ISP y el Chip-Off) y lógico, siendo el acceso físico el que se implementó en el desarrollo del proyecto, esto implica obtener una copia de bit a bit directamente desde el almacenamiento del dispositivo (chip de almacenamiento interno).

Escenarios de pruebas Funcionales para ISP (In System Programming) y Chip-Off considerando diferentes situaciones de dispositivos móviles y tipos de evidencia a recuperar.

| | CARACTERÍSTICAS | DESCRIPCIÓN |
|---|---|---|
| PROCESO ISP (In System Programming) | Conexión confiable | Asegurar una conexión estable y confiable entre el equipo de extracción y el dispositivo móvil a través del ISP, minimizando las interrupciones o pérdidas de comunicación durante el proceso de extracción. |
| | Compatibilidad amplia | Compatible con una amplia gama de dispositivos móviles, incluyendo diferentes marcas, modelos y sistemas operativos, para garantizar la aplicabilidad en diversos escenarios forenses. |

| | | |
|---|---|---|
| | Seguridad de datos | Implementar medidas de seguridad adecuadas para proteger la integridad y confidencialidad de los datos durante el proceso de extracción mediante ISP, evitando la alteración o pérdida de información sensible. |
| | Tiempo de extracción eficiente | Optimizar el tiempo requerido para la extracción de datos mediante ISP, minimizando el impacto en el tiempo total de investigación forense y permitiendo una recuperación rápida de la información necesaria. |
| | Verificación de la integridad | Contar con mecanismos de verificación de integridad de los datos extraídos mediante ISP, garantizando que la información recuperada sea precisa y no se haya modificado durante el proceso de extracción. |

*Tabla 5: Características del proceso ISP.*

| | CARACTERÍSTICAS | DESCRIPCIÓN |
|---|---|---|
| PROCESO CHIP-OFF | Manipulación cuidadosa del dispositivo | El proceso de Chip-Off requiere una manipulación física del dispositivo móvil. Por lo tanto, se debe tener especial cuidado para evitar daños adicionales al dispositivo durante el proceso de extracción del chip. |
| | Equipamiento adecuado | Es necesario contar con el equipamiento y las herramientas adecuadas para realizar el proceso de Chip-Off de manera precisa y segura, incluyendo herramientas de soldadura, desmontaje y lectura de chips. |
| | Protección contra descargas estáticas | Implementar medidas de protección contra descargas estáticas durante el proceso de Chip-Off para evitar daños irreversibles en el chip y garantizar la integridad de los datos almacenados. |
| | Extracción segura del chip | Asegurar una extracción cuidadosa y precisa del chip de la placa del dispositivo, minimizando los |

| | | |
|---|---|---|
| | | riesgos de dañar o romper el chip durante el proceso. |
| | Almacenamiento adecuado del chip | Una vez extraído, el chip debe ser almacenado adecuadamente para garantizar su seguridad y protección contra daños físicos o estáticos, evitando la pérdida de datos y asegurando su integridad. |

*Tabla 6: Características del proceso CHIP-OFF.*

Pruebas Funcionales para Chip-Off

- Dispositivo irreparable o no operativo
- Chip en dispositivos bloqueados o con contraseñas
- Chip en dispositivos dañados físicamente
- Chip en dispositivos con memoria no extraíble

Pruebas Funcionales para ISP

- Dispositivo mojado
- Dispositivo apagado
- Dispositivo dañado o trizado
- Dispositivo bloqueado o con contraseña

| ESCENARIO | ENTORNO | NIVEL DE CRITICIDAD | DERSCRIPCIÓN | RESULTADO |
|---|---|---|---|---|
| **#1 Por Método ISP** | Dispositivo mojado | ALTO | Este escenario simula la exposición del dispositivo móvil a líquidos como agua, lluvia o inmersión durante un período de tiempo. El dispositivo puede abrirse o cerrarse y mostrar signos de humedad. | Capacidad del sistema ISP para recuperar datos del dispositivo cuando se expone a líquidos. Se espera que el sistema pueda recuperar los datos requeridos sin problemas por los daños presentados. |

| DETALLE: **Escenario 1** |
|---|

*Tabla 7: Prueba funcional para ISP escenario 1.*

| ESCENARIO | ENTORNO | NIVEL DE CRITICIDAD | DERSCRIPCIÓN | RESULTADO |
|---|---|---|---|---|
| **#2 Por Método ISP** | Dispositivo apagado | ALTO | Simula un dispositivo móvil apagado que no responde. El dispositivo puede estar apagado o se ha producido un corte de energía. El equipo no puede hacer acciones interactivas por su estado. | Verificar capacidad del proceso ISP para establecer una conexión y recuperar datos del dispositivo, incluso cuando el equipo esta apagado y no funciona. Se espera recuperar datos requeridos sin tener que encender el dispositivo. |
| DETALLE: **Escenario 2** | | | | |

*Tabla 8: Prueba funcional para ISP escenario 2.*

| ESCENARIO | ENTORNO | NIVEL DE CRITICIDAD | DERSCRIPCIÓN | RESULTADO |
|---|---|---|---|---|
| **#3 Por Método ISP** | Dispositivo dañado o trizado | MEDIO | Simula un equipo móvil con daños físicos visibles, como pantalla rota, carcasa rota u otros daños externos. El dispositivo puede estar encendido o pagado, pero presenta daños físicos evidentes. | Probar la capacidad del proceso ISP o Chip-Off para extraer datos del dispositivo a pesar del daño físico. Se espera que el sistema pueda recuperar los datos requeridos a pesar de las condiciones corruptas. |
| DETALLE: **Escenario 3** | | | | |

*Tabla 9: Prueba funcional para ISP escenario 3.*

| ESCENARIO | ENTORNO | NIVEL DE CRITICIDAD | DERSCRIPCIÓN | RESULTADO |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| **#4 Por Método ISP** | Dispositivo bloqueado o con contraseña | MEDIO | Simula un equipo móvil bloqueado o protegido con contraseña. El dispositivo se puede encender, pero no se puede acceder a los datos si no se ingresa la contraseña o el patrón correcto. | Probar capacidad del proceso ISP o Chip-Off para recuperar datos del dispositivo sin necesidad de contraseña o patrón de desbloqueo. Se espera que el sistema pueda descargar los datos necesarios sin ingresar una contraseña. |
| **DETALLE: Escenario 4** | | | | |

*Tabla 10: Prueba funcional para ISP escenario 4.*

| ESCENARIO | ENTORNO | NIVEL DE CRITICIDAD | DERSCRIPCIÓN | RESULTADO |
|---|---|---|---|---|
| **#5 Método Chip-Off** | Dispositivo irreparable o no operativo | ALTO | Este escenario simula un dispositivo móvil que no se puede reparar o encender debido a daños físicos o fallas críticas. El dispositivo no responde a los intentos de encenderlo y no se puede interactuar con él. | Probar la capacidad del proceso de Chip-Off para ver si el dispositivo es reparable o no, quitando el chip del dispositivo y recuperar datos necesarios. Dado que el equipo no enciende y no se puede reparar, se espera que el proceso permita el acceso a la información accediendo directamente al chip. |
| **DETALLE: Escenario 5** | | | | |

*Tabla 11: Prueba funcional para Chip-Off escenario 5.*

| ESCENARIO | ENTORNO | NIVEL DE CRITICIDAD | DERSCRIPCIÓN | RESULTADO |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| **#6 Método Chip-Off** | Chip en dispositivo bloqueados o con contraseña | ALTO | El equipo requiere acceso al chip para recuperar los datos almacenados en el dispositivo. El dispositivo se puede encender, pero no se puede acceder a los datos si no se ingresa la contraseña o patrón correcto. | Probar capacidad del proceso Chip-Off para quitar el chip del equipo y extraer los datos almacenados en el sin necesidad de una contraseña o patrón. El proceso está destinado a proporcionar acceso directo al chip y recuperar los datos necesarios. |
| **DETALLE: Escenario 6** | | | | |

*Tabla 12: Prueba funcional para Chip-Off escenario 6.*

| ESCENARIO | ENTORNO | NIVEL DE CRITICIDAD | DERSCRIPCIÓN | RESULTADO |
|---|---|---|---|---|
| **#7 Método Chip-Off** | Chip en dispositivo dañados físicamente | ALTO | Simula un dispositivo móvil con daños físicos graves, como pantalla rota entre otros, tipo de daño visible. A pesar del daño, el acceso al chip es necesario para extraer los datos almacenados. | Probar capacidad del proceso para extraer de forma segura el chip de un dispositivo sin dañarlo. Se espera que el proceso Chip-Off permita el acceso al chip y la recuperación de los datos a pesar de los daños físicos del equipo. |
| **DETALLE: Escenario 7** | | | | |

*Tabla 13: Prueba funcional para Chip-Off escenario 7.*

Es importante adaptar los escenarios de pruebas funcionales a necesidades específicas con las herramientas forenses utilizadas. Teniendo en cuenta que, en algunos casos, un dispositivo completamente dañado, es posible que requiera técnicas adicionales o que la recuperación de datos no sea posible.

### 3.1.2. Fase 3: Examinar la evidencia.

Durante esta etapa se analizan minuciosamente los datos obtenidos para buscar información relevante y descubrir posibles pruebas que ayuden entender el incidente o delito que se está siendo investigado.

Una vez extraídos los datos del dispositivo de almacenamiento son preparados para su análisis, esto implica descomprimir archivos, organizar la estructura de las carpetas y preparar la configuración adecuada de las herramientas de análisis. Se revisan y analizan los datos estructurados, como mensajes de textos, registros de llamadas, contactos, calendarios, y otros datos que se encuentran en formatos fácilmente accesibles y entendibles. Además de los datos estructurados se examinan los no estructurados, como fotos, videos, archivos de audio y otros archivos multimedia, se revisan también los datos de aplicaciones específicas que pueden contener información relevante.

Se realiza una búsqueda activa de evidencia relacionada con el incidente o delito en cuestión, esto puede incluir palabra claves, números de teléfonos, nombres de personas involucradas, y ubicaciones, detalles relevantes que puedan ayudar a la investigación. Las aplicaciones instaladas en el dispositivo se investigan para encontrar posibles comportamientos anómalos, datos almacenados en el cache, contraseñas guardadas, cookies y se recuperan datos eliminados del dispositivo.

Se analizan los metadatos asociados con los archivos multimedia y otros datos, como la fecha y hora de creación, ubicación geográfica (geolocalización) información que puede proporcionar pistas adicionales sobre el incidente o delito. Durante esta fase del proceso de análisis se realiza también una documentación de los resultados, hallazgos y conclusiones de la investigación, un análisis meticuloso y detallado garantiza la obtención de resultados precisos y confiables.

### 3.1.3. Fase 4: Documentación y reportes.

Se realiza la documentación y elaboración de los reportes finales, en esta etapa se organizan y presentan de manera clara y concisa los resultados obtenidos durante el proceso del análisis forense.

Antes de generar los reportes, es importante organizar y clasificar todos los datos obtenidos, se elabora un resumen que brinda un enfoque general de los hallazgos más importantes y las conclusiones, permitiendo una visión rápida. El reporte debe contener detalles técnicos sobre el proceso, las herramientas utilizadas, los métodos aplicados y los resultados específicos

encontrados en cada una de las fases de la investigación. Una vez que los reportes estén completos, se presentan y entregan a los interesados.

# 4. ANÁLISIS DEL RESULTADO.

## 4.2. INTERPRETACION DE RESULTADOS EXPERIMENTALES

### 4.2.1. ANÁLISIS Y EVALUACIÓN DE MÉTRICAS

En el proceso forense de extracción y recuperación de información se deben diseñar métricas para medir de manera objetiva la eficacia, eficiencia y calidad del proceso.

| Nombre de la métrica | Método ISP |
|---|---|
| **Objetivo de uso** | Evaluar el rendimiento del proceso forense de extracción y recuperación de información en dispositivos móviles. |
| **Método de medición** | A través del tiempo total de extracción, el número de datos recuperados y la precisión de la extracción.<br>- Tiempo tota: medido en horas, minutos y segundos.<br>- Cantidad de datos recuperados: número total de archivos, mensajes, contactos recuperados durante el proceso.<br>- Precisión de la extracción: porcentaje de datos recuperados con éxitos en relación con los datos totales disponibles en el dispositivo. |
| **Formula y elemento de cálculo** | Tiempo de Extracción = (Hora de finalización de extracción) – (hora de inicio de extracción) |
| **Interpretación de la métrica** | El criterio de éxito para la precisión de la extracción puede ser un mínimo del 90% de datos recuperados. |

| | |
|---|---|
| **Escala** | Escala numérica.<br>Del 1 al 5 donde 1 representa un rendimiento deficiente y 5 representa un rendimiento excelente. |
| **Tipo de métrica** | Numérica |
| **Fuentes de datos** | - Informe de resultados. |

*Tabla 14: Evaluación de métricas por el método ISP.*

| **Nombre de la métrica** | **Método CHIP-OFF** |
|---|---|
| **Objetivo de uso** | Evaluar el rendimiento del proceso forense de extracción y recuperación de información en dispositivos móviles. |
| **Método de medición** | A través del tiempo total de extracción, el número de datos recuperados y la precisión de la extracción.<br>- Tiempo tota: medido en horas, minutos y segundos.<br>- Cantidad de datos recuperados: número total de archivos, mensajes, contactos recuperados durante el proceso.<br>- Precisión de la extracción: porcentaje de datos recuperados con éxitos en relación con los datos totales disponibles en el dispositivo. |
| **Formula y elemento de cálculo** | Tiempo de Extracción = (Hora de finalización de extracción) – (hora de inicio de extracción) |
| **Interpretación de la métrica** | El criterio de éxito para la precisión de la extracción puede ser un mínimo del 90% de datos recuperados. |

| | |
|---|---|
| **Escala** | Escala numérica.<br>Del 1 al 5 donde 1 representa un rendimiento deficiente y 5 representa un rendimiento excelente. |
| **Tipo de métrica** | Numérica |
| **Fuentes de datos** | - Informe de resultados. |

*Tabla 15: Evaluación de métricas por el método CHIP-OFF*

## CONCLUSIONES

- El método ISP (In System Programming) y la extracción de la memoria eMMC son técnicas efectivas para la recuperación de datos n dispositivos móviles. estas técnicas permiten obtener una copia forense de los datos almacenados en el equipo sin modificar los datos originales, lo que garantiza la integridad de la evidencia y su validez en un contexto legal.

- La extracción de la memoria eMMC es útil en casos donde el dispositivo este bloqueado, dañado o no es posible acceder a los datos de manera convencional. Esta técnica permite acceder directamente a la memoria interna del equipo y recuperar datos en situaciones difíciles.

- El análisis forense de la memoria eMMC en ambos procesos requiere de herramientas y conocimientos especializados. Es fundamental que los profesionales forenses estén capacitados y actualizados en estas técnicas para garantizar un análisis preciso y confiable.

- La cadena de custodia es esencial durante todo el proceso de recuperación de datos y análisis forense. Es importante mantener un registro detallado de todas las acciones realizadas sobre la evidencia para garantizar su integridad y admisibilidad en un proceso legal.

## RECOMENDACIONES

- Los profesionales que se dediquen al análisis forense en dispositivos móviles deben mantenerse actualizados en las últimas técnicas y herramientas disponibles en el campo. La capacitación continua asegura un análisis más eficiente y preciso.

- Es fundamental utilizar herramientas forenses certificadas y confiables para llevar a cabo la recuperación de datos y el análisis forense. El uso de herramientas de calidad garantiza resultados más precisos y evita daños a la evidencia.

- El análisis forense debe realizarse de acuerdo con estándares y practicas reconocidas en el campo de la informática forense. Esto incluye el cumplimiento de normas de procedimiento, protección de la cadena de custodia y presentación de informes claros y detallados.

- Durante el análisis forense, se manejarán datos personales y confidenciales. Es esencial garantizar la privacidad y seguridad de los datos durante todo el proceso y cumplir con las leyes y regulaciones de protección de datos aplicables.

# BIBLIOGRAFÍA


[1] S. Krishnan, B. Zhou y M. Kyung An, «Smartphone Forensic Challenges,» 2019. [En línea]. Available: Smartphone Forensic Challenges.

[2] Universidad de las Fuerzas Armadas, «Metodología de análisis forense orientada a incidentes en dispositivos moviles.,» 2018. [En línea]. Available: file:///C:/Users/Emi/Downloads/edison-timbe-721-2231-1-ce.pdf.

[3] S. S. F. R. Z. G. y. C. D. L. A. Fukami, «"Experimental Evaluation of e.MMC Data Recovery",» 2022. [En línea]. Available: https://ieeexplore.ieee.org/abstract/document/9777707.

[4] J. S. Rueda Rueda, D. Rico Bautista y C. D. Guerrero, «Guía práctica abierta para el análisis forense digital en dispositivos Android.,» 2019. [En línea]. Available: https://www.researchgate.net/profile/Dewar-Rico-Bautista/publication/333198221_Open_Practice_Guide_for_Digital_Forensics_on_Android_Devices/links/5e9fdc474585150839f40e5c/Open-Practice-Guide-for-Digital-Forensics-on-Android-Devices.pdf.

[5] M. J. MURUDUMBAY HUERTA, «MARCO DE TRABAJO Y HERRAMIENTAS PARA EL ANÁLISIS,» 05 2022. [En línea]. Available: https://dspace.ucacue.edu.ec/bitstream/ucacue/12840/1/articulo_Informe%20final%20%283%29.pdf.

[6] K. W. BELTRÁN TAPIA, «MODELO PARA ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES CON,» 09 2021. [En línea]. Available: https://repositorio.pucesa.edu.ec/bitstream/123456789/3293/1/77448.pdf.

[7] S.N.d., «Planificación, «Plan de creación de oportunidades 2021 -2025,» 2021. [En línea]. Available: https://www.protrade.ec/wp-content/uploads/2022/06/PND-Plande-Creaci%C3%B3n-de-Oportunidades-2021-2025-.pdf.

[8] C. F. C. -. P. B. Lucio, Metodología de la Investigacion, sexta edición .

[9] J. Bair, Seeking the Truth from Mobile, Academic press, 2018.

[10] L. A. C. Silva, «Herramientas de análisis forense para android,» 11 2019. [En línea]. Available: https://crea.ujaen.es/bitstream/10953.1/11909/1/TFM_LuizaAraujoCostaSilva_vf.pdf. [Último acceso: 07 2023].

[11] L. Coronel Rojas, Y. Arévalo Areniz, F. Cuesta Quintero y E. Rico Bautista, «Definición de una metodología de adquisición de evidencias digitales basadas en estándares internacionales,» 02 2020. [En línea]. Available: https://www.researchgate.net/profile/Dewar-Rico-Bautista/publication/340617686_Definition_of_a_digital_evidence_acquisition_methodology_based_on_international_standards/links/5e9526fb299bf1307997945c/Definition-of-a-digital-evidence-acquisition-methodolog. [Último acceso: 07 2023].

[12] W. Jarvis, «Seguridad de la Información,» Universidad Veracruzana, 31 01 2019. [En línea]. Available: https://www.uv.mx/infosegura/general/noti_forense/. [Último acceso: 26 05 2023].

[13] F. Fernando, «Guía de procedimientos para la extracción de datos en dispositivos móviles dañados,» 2022.

[14] Viuda Negra, «Emmc Repair Software,» 2022. [En línea]. [Último acceso: 07 2023].

[15] S. Fouad, «Forence Digital,» de *Forense Digital: Cómo el análisis forense digital está ayudando a llevar el trabajo de investigación de la escena del crimen al mundo real*, Mil millones de conocimeintos, 2022, p. 308.

[16] J. E. Isidor Galeana, L. J. Cortez Organista, V. lvarez Hilario y E. Rodríguez Peralta, «ANÁLISIS DE HERRAMIENTAS PARA LA ADQUISICIÓN, PRESERVACIÓN Y ANÁLISIS DE RECUPERACIÓN DE DATOS,» 2020. [En línea]. Available:

https://www.innovaingenieria.uagro.mx/innova/index.php/innova/article/view/94/45. [Último acceso: 05 2023].

[17] Martínez Ródenas, Cristina, «Análisis Forense en Dispositivos Móviles: Un caso practico,» 31 07 2020. [En línea]. [Último acceso: 05 2023].

[18] M. Guerra Soto, de *Análisis forense informático*, RA-MA S.A. Editorial y Publicaciones, 2021, p. 464.

[19] JTAG FÁCIL, «JTAG fácil MÁS,» Etnosoft, [En línea]. Available: http://plus.easy-jtag.com/. [Último acceso: 26 05 2023].

[20] UFI Universal Flashing Interface, UFI-Box, 2023. [En línea]. Available: https://www.ufi-box.com/pages/ufi-box-features. [Último acceso: 26 05 2023].

[21] GSM SERVER, «Medusa Pro II,» Gradus Studio, 2023. [En línea]. Available: https://medusabox.com/spa. [Último acceso: 26 05 2023].

[22] Nanzhao.org, «Esquemas DZKJ,» DZKJ PhoneRepair Tools, 2023. [En línea]. Available: https://www.dzkj16888.com/. [Último acceso: 26 05 2023].

[23] Final Test, «Instrumentos de Prueba y Medición,» 2023. [En línea]. Available: https://www.finaltest.com.mx/product-p/art-5.htm#:~:text=ESTACION%20DE%20SOLDADURA%20DE%20AIRE,se%20puede%20valer%20de%20algunos. [Último acceso: 26 05 2023].

[24] Mundo Microscopio , [En línea]. Available: https://www.mundomicroscopio.com/microscopio-electronico/. [Último acceso: 26 05 2023].

[25] FLUKE, 2023. [En línea]. Available: https://www.fluke.com/es-ec/informacion/blog/electrica/que-es-un-multimetro-digital#:~:text=Un%20mult%C3%ADmetro%20digital%20(DMM)%20es,las%20industrias%20el%C3%A9ctricas%20y%20electr%C3%B3nicas.. [Último acceso: 26 05 2023].

[26] CENTELSA , «Una marca viable,» [En línea]. Available: https://www.centelsa.com/archivos/alambresesmaltadosflyer.pdf. [Último acceso: 26 05 2023].

[27] Movilone, «Movilone Reparación de Móviles,» 03 06 2018. [En línea]. Available: https://www.movilone.es/blog/flux-para-soldar-que-es-y-como-utilizarlo/#:~:text=El%20flux%20para%20soldar%2C%20tambi%C3%A9n,la%20calidad%20de%20la%20soldadura.. [Último acceso: 26 05 2023].

[28] M. Leroy, «Bricopedia,» 27 10 2022. [En línea]. Available: https://www.leroymerlin.es/ideas-y-consejos/bricopedia/limpiador-de-contactos.html#:~:text=Sirve%20para%20eliminar%20la%20suciedad,elemento%20que%20se%20desea%20limpiar.. [Último acceso: 26 05 2023].

[29] a. spares. [En línea]. Available: https://all-spares.com/es/articles-and-video/how-to-use-touchscreen-glass-separator-sm-252/#:~:text=El%20separador%20permite%20de%20manera,herramienta%20permite%20ahorrar%20su%20tiempo.. [Último acceso: 26 05 2023].

[30] SELECT, [En línea]. Available: https://selectonline.co/blog//cables-y-conexionestodo-lo-que-debes-saber-para-una-mejor-conectividad.html#:~:text=El%20USB%20Tipo%20C%20es,tel%C3%A9fonos%20celulares%20en%20el%20mercado.. [Último acceso: 26 05 2023].

[31] G. Breixo, «Profesional review,» 30 06 2022. [En línea]. Available: https://www.profesionalreview.com/2022/06/30/fuente-de-alimentacion-regulable/. [Último acceso: 26 05 2023].

[32] Kalstein, «Limpiador Ultrasónico,» 2021. [En línea]. Available: https://kalstein.ec/limpiador-ultrasonico/. [Último acceso: 26 05 2023].

[33] VLEX, «Información Jurídica Inteligente,» [En línea]. Available: https://vlex.ec/vid/codigo-organico-integral-penal-631464447. [Último acceso: 07 2023].

[34] eSilec Profesional, «Ley de comercio electrónico, firmas y mensajes de datos,» [En línea]. Available: https://www.telecomunicaciones.gob.ec/wp-

content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf. [Último acceso: 07 2023].

[35] A. Carlos, B. Glenda y C. Juan, «Revista Espacios,» 04 06 2018. [En línea]. Available: https://www.revistaespacios.com/a18v39n42/a18v39n42p15.pdf. [Último acceso: 26 05 2023].

[36] J. J. P. Rivadeneira, «Guia Peritaje,» [En línea]. Available: https://issuu.com/juanjosepaezrivadeneira/docs/guia_peritaje. [Último acceso: 4 Mayo 2023].

[37] H. C. Cory Altheide, «Technical Editor,» [En línea]. Available: https://es.scribd.com/read/282543021/Digital-Forensics-with-Open-Source-Tools#__search-menu_738838. [Último acceso: 4 Mayo 2023].

[38] M. Luis, «Emmc Repair Software,» Quito, 2022.

[39] F. H. Llamozas Escalante y C. Márquez Sánchez, «Guía de trabajo para el análisis forense de los delitos informáticos en Perú.,» 08 2021. [En línea]. Available: https://renati.sunedu.gob.pe/bitstream/sunedu/3396554/1/LlamozasEscalanteFH.pdf.

# ANEXOS

| | Memoria | Particiones | Unidades Lógicas | Puertos |
|---|---|---|---|---|
| **Qualcomm** | eMMC | BOOT1,BOOT2, RPMB, USER, GP1, GP2, GP3, GP4. | Boot Partition 1, Boot Partition 2, RPMB, User Partition, General Purpose Partition 1, General Purpose Partition 2, General Purpose Partition 3, General Purpose Partition 4. | SD/eMMC Ports |
| **Qualcomm** | UFS | BOOT1,BOOT2, RPMB, USER, GP1, GP2, GP3, GP4. | Boot Partition 1, Boot Partition 2, RPMB, User Partition, General Purpose Partition 1, General Purpose Partition 2, General Purpose Partition 3, General Purpose Partition 4. | |
| **Enos** | | BOOT1,BOOT2, RPMB, USER, GP1, GP2, GP3, GP4. | Boot Partition 1, Boot Partition 2, RPMB, User Partition, General Purpose Partition 1, General Purpose Partition 2, General Purpose Partition 3, General Purpose Partition 4. | |
| **Exynos** | | BOOT1,BOOT2, RPMB, USER, GP1, GP2, GP3, GP4. | Boot Partition 1, Boot Partition 2, RPMB, User Partition, General Purpose Partition 1, General Purpose Partition 2, General Purpose Partition 3, General Purpose Partition 4. | |
| **MediaTek** | | BOOT1,BOOT2, RPMB, USER, GP1, GP2, GP3, GP4. | Boot Partition 1, Boot Partition 2, RPMB, User Partition, General Purpose Partition 1, General Purpose Partition 2, General Purpose | |

| | | | | |
|---|---|---|---|---|
| | | | Partition 3, General Purpose Partition 4. | |
| **MediaTek** | | BOOT1,BOOT2, RPMB, USER, GP1, GP2, GP3, GP4. | Boot Partition 1, Boot Partition 2, RPMB, User Partition, General Purpose Partition 1, General Purpose Partition 2, General Purpose Partition 3, General Purpose Partition 4. | |
| **Spreadtrum** | | BOOT1,BOOT2, RPMB, USER, GP1, GP2, GP3, GP4. | Boot Partition 1, Boot Partition 2, RPMB, User Partition, General Purpose Partition 1, General Purpose Partition 2, General Purpose Partition 3, General Purpose Partition 4. | |
| **Spreadtrum** | | BOOT1,BOOT2, RPMB, USER, GP1, GP2, GP3, GP4. | Boot Partition 1, Boot Partition 2, RPMB, User Partition, General Purpose Partition 1, General Purpose Partition 2, General Purpose Partition 3, General Purpose Partition 4. | |
| **Hisilicon** | | BOOT1,BOOT2, RPMB, USER, GP1, GP2, GP3, GP4. | Boot Partition 1, Boot Partition 2, RPMB, User Partition, General Purpose Partition 1, General Purpose Partition 2, General Purpose Partition 3, General Purpose Partition 4. | |

**Anexo 1: Tipos de memorias y sus características.**

# ANEXO 2: GUÍA FORENSE

La siguiente guía esta basada en cuadro fases, tomando como referencia la guía forense DOJ2, para realizar de manera adecuada el proceso de extracción de evidencia digitales a través de dos métodos dependiendo del estado en que se encuentre el dispositivo móvil. Tomando en cuneta los reglamentos del Código Orgánico de Integración Penal (COIP), normativa legal vigente en el país.

Es crucial asegurarse de seguir todas las fases de la metodología establecida para crear la guía de manera adecuada. Esto implica considerar los procesos involucrados en cada etapa del análisis de la evidencia digital. En todo momento es fundamental preservar la integridad de la evidencia.

- Identificacion del investigador forense encargado de la recoleccion de la información digital.
- La evidencia debe estar acompañada de una cadena de custodia cerfiticada y garantizada.
- Completar un formulario con los datos personales del perito o investigador.

**Fase 1**

En esta etapa, se realiza la verificacion del equipo a analizar para asegurar que se encunetre en las condiciones que fueron entregadas siguiendo la cadena de custodia. Además, de identificar a la persona responsable de llevar acabo la extración de la evidencia. Según el articulo 12 de la resolucion 040-2014, la selección de peritos, tanto en caso civiles como penales, será realizada por un juez, asegurando los principios de profesionalidad, especialidad, transparencia, alternabilidad e igualdad. Es esencial que la persona seleccionada este debidsmente calificada y tenga la capacidad de cumplir con la responsabilidad que se le ha asignado.

**Dispositivos por analizar dentro de la fase**

*Imagen 2: Verificación del estado de los dispositivos.*

| Especificacion | Datos de dispositivo 1 | Datos de dispositivo 2 |
|---|---|---|
| **Marca** | Xiaomi | Xiaomi |
| **Modelo** | Redmi 5 plus Vince | Redmi note 8 |
| **IMEI** | 859645221078452 | 867122053352846 |
| **Version de android** | 8.1.0 Oreo ZQL1711-vince-build-20191108142512 | 9 PKQ1.190616,001 |
| **Version de banda base** | XRMI.CT.3.584-008868-PBFI_GEN_RFLI-1.2.72545 | MPSS.AT.4.3.1-00270-NICOBAR_GEN_PACK-1.317803 |
| **Version de kernel** | 0011-8500-8154 | 11.0.12.0 PCOMIXM |
| **Numero de compilacion** | 78950045 | 95358875 |

*Tabla 16: Especificaciones técnicas de los dispositivos.*

Previo al inicio de desmontaje del dispositivo, se deben completar un formulario con la información relevante del caso. Se proporcionará infomración personal del perito responsable del proceso de investigación.

**Formulario Nº 1**

| | |
|---|---|
| **Lugar y fecha** | |
| **Nombre y apellido** | |
| **Numero de cedula** | |
| **e-mail** | |
| **Especialización** | |
| **Codigo del perito** | |
| **Institución** | |

**Firma del perito acargo del caso**

_____

**Firma**

*Anexo 3: Formulario de información personal del perito a cargo de la investigación.*

**Fase 2**

Durante esta etapa, se realizará la selección de las herramientas que serán utilizadas en el porceso de extracción de evidencia. Es importante comprender el propósito del hardware y software, estos se mencionarán en la tabla que se presentará a continuación. Estas herramientas se emplearán una vez que el equipo haya sido previamente identificado, siguiendo los porcesos establecidos en la fase anterior.

| Herramienta Hardware |
|---|
| Microscopio |
| Easy jtag y ufi box |
| Adaptadores de memorias |
| Multimetro |
| Probador USB |
| Estacion de soldadura |
| Plantillas para reballing |
| Insumos de soldadura |

*Tabla 17: Herramientas de hardware utilizadas dentro del proceso.*

| Nombre de la herramienta | Versión | Función principal | Disposnible en |
|---|---|---|---|
| **DZKJ** | 1.0.0.49 | Soluciones de hardware | https://www.dzkj16888.com/ |
| **Easy Jtag** | 3.8.0.4 | Reoprogramadora de memorias y extraccion de datos | https://easy-jtag.com/ |
| **Ufi Box** | 1.6.0.2333 | Reprogramadora de memorias y extraccion de datos | https://www.ufi-box.com/pages/downloads |
| **Forensic Toolkit** | | Herramineta para analisis forense | Descarga Forensic Toolkit GRATIS-5.1.1.4 gratuitamente (freedownloadmanager.org) |

| | | | |
|---|---|---|---|
| **Caine** | 13.0.0 | Herramineta para analisis forense | DESCARGAS (caine-live.net) |
| **Foca** | 3.4.7.1 | Herramineta para analisis forense | Descargar FOCA 3.4.7.1 para Windows - Filehippo.com |

*Tabla 18: Herramientas de software utilizadas dentro del proceso.*

## Anexo 4: Instalación de Software Easy Jtag.

1. Se ingresa a la pagina oficial para descargar el software easy jtag (Downloads | EasyJtag – Fastest Memory Programmer in the word! (easy-jtag.com)) se requiere de tres progrmas para maniupular la caja box.

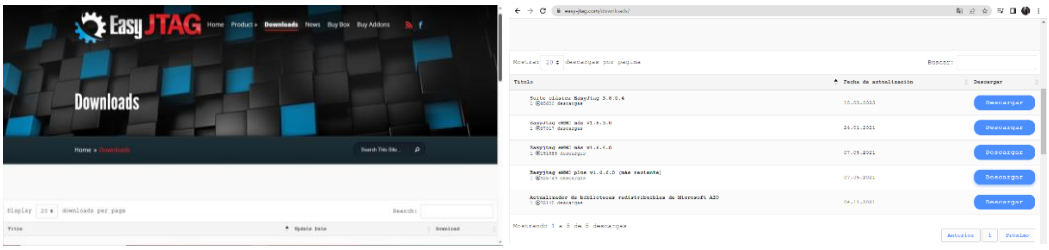



*Imagen 3: Descarga del programa.*

2. Después de descargar el primer programa, Easy Jtag Tool, que posibilita la realización de operaciones como el volcado de memoria, escritura y lectura, procedemos con la instalación siguiendo los pasos proporcionados a continuación.

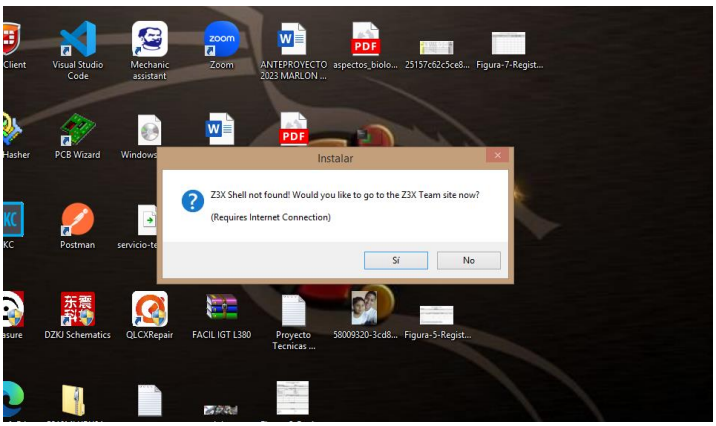



*Imagen 4: Ejecución del instalador.*

Se acepta los terminos de la instalación

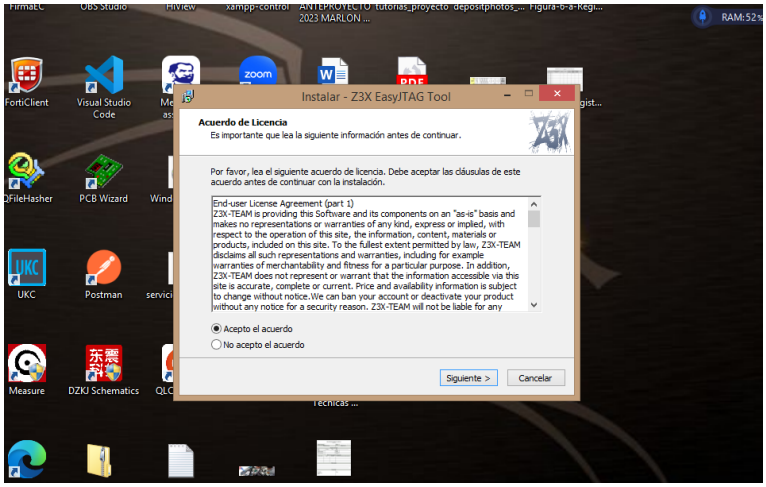



*Imagen 5: Términos y condiciones.*

En las ventanas posteriores, se solicita que elijamos la ubicación del programa y realicemos la selección de tareas adicionales.

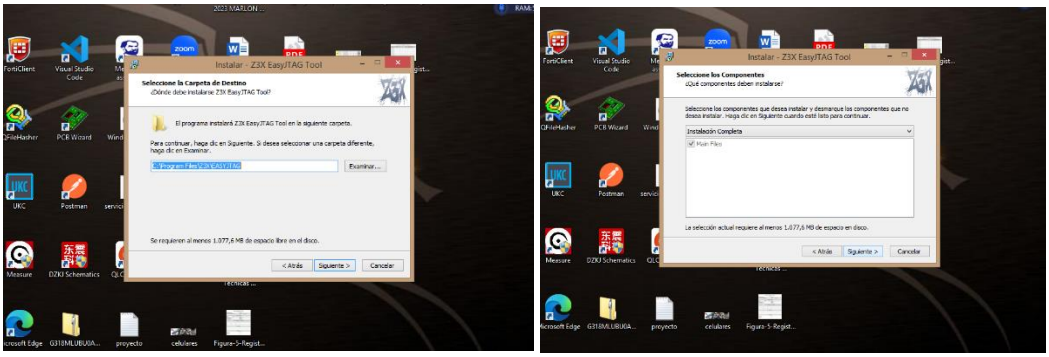


*Imagen 6: Selección de ubicación donde se instalará el programa.*

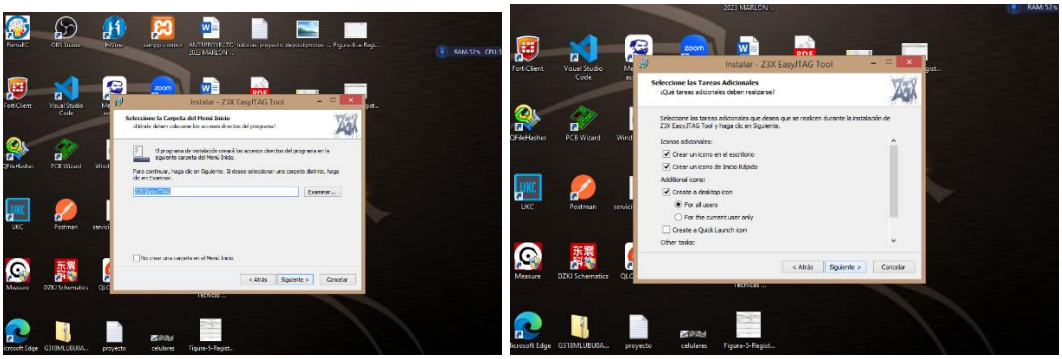


*Imagen 7: Selección de tareas adicionales.*

*Imagen 8: Instalación del programa.*

3. Después de completar la instalación del primer programa, procedemos con el siguiente, que es el Z3X Easy Jtag Tool. Este programa nos brinda la capacidad de revivir el equipo en situaciones como una instalación defectuosa del firmware, eliminar cuentas FRP, RPMB, KG LOCK, PAYJOY, Cuenta MI, entre otras opciones.

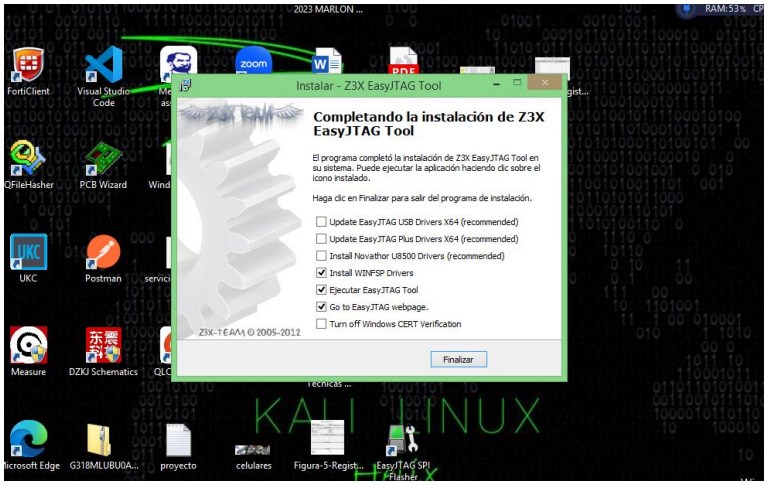



*Imagen 9: Ventana principal del instalador.*

En las ventanas siguientes, se nos solicita que elijamos el idioma en el cual deseamos instalar el programa y también la ubicación donde se realizará la instalación.

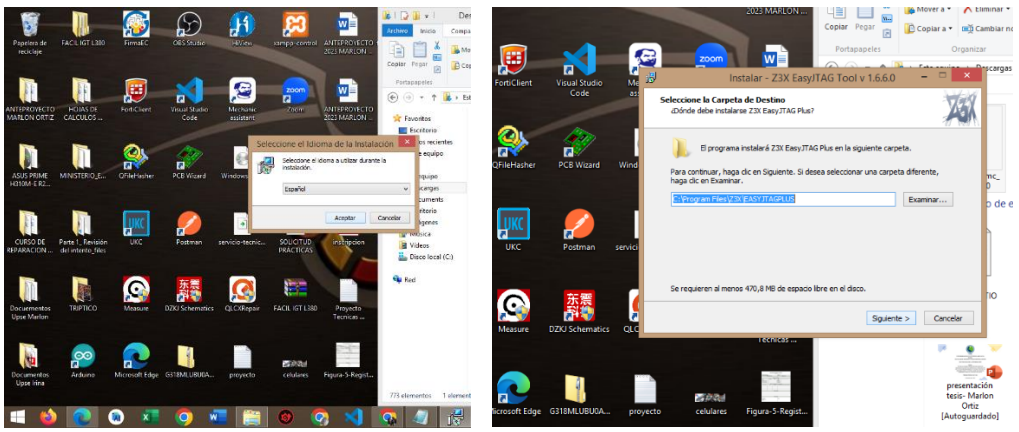


*Imagen 10: Selección de idioma y ubicación del programa.*

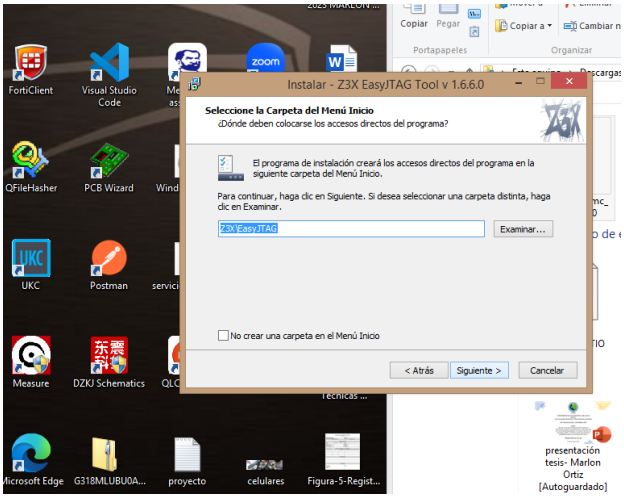



*Imagen 11: Creación del acceso directo del programa.*

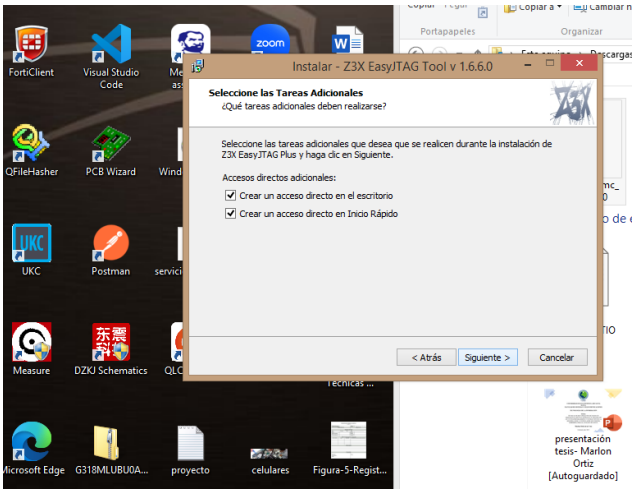



*Imagen 12: Selección de tareas adicionales.*

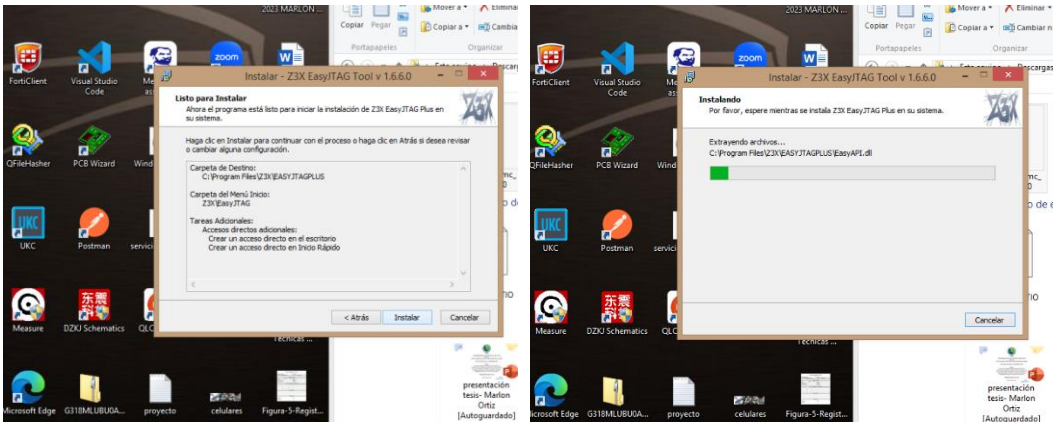



*Imagen 13: Proceso listo para instalación.*

4. Después de completar la instalación, aparecerá una ventana emergente que nos solicitará permiso para enviar informes de errores futuros que puedan ocurrir durante el uso del programa, con el propósito de corregirlos adecuadamente.

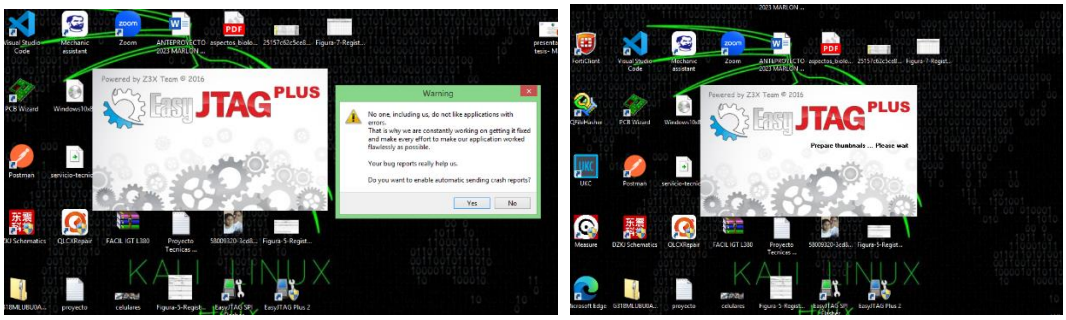



*Imagen 14:Ventana emergente antes de ingresar al programa.*

5. Continuamos con la instalación del programa Easy Jtag Plus 2, que nos brinda la posibilidad de llevar a cabo las mismas funciones que el programa anterior, pero esta vez, específicamente para memorias UFS.

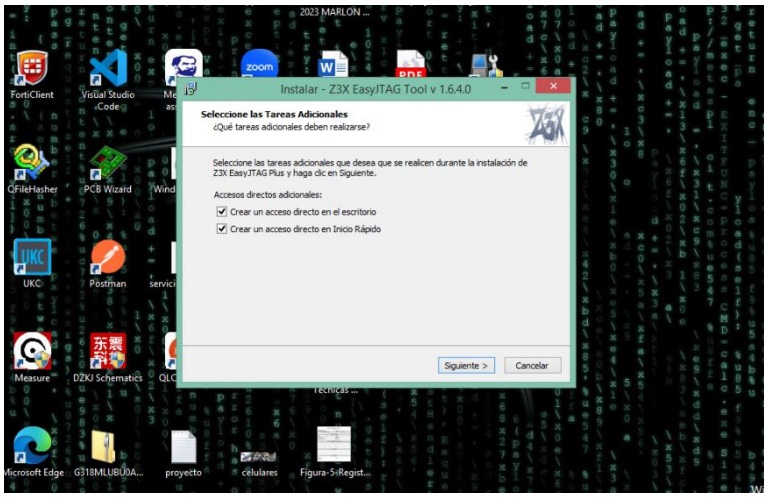



*Imagen 15: Ventana principal del instalador.*

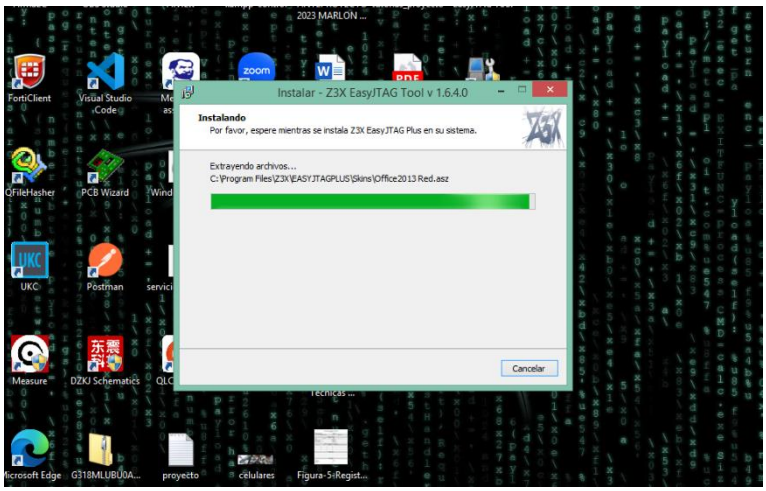


*Imagen 16: Instalando el programa.*


*Imagen 17: Proceso de instalación finalizado.*

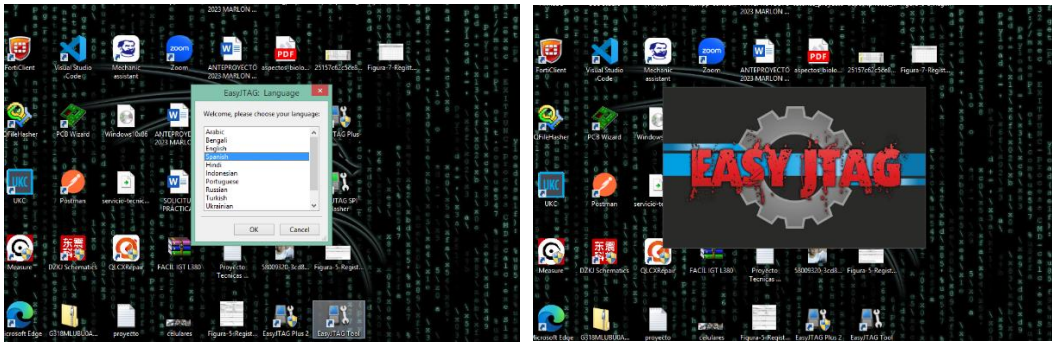



*Imagen 18: Ejecución del programa.*

6. La ejecución del programa no es posible debido a la ausencia del programa Microsoft Visual C++ en el equipo.

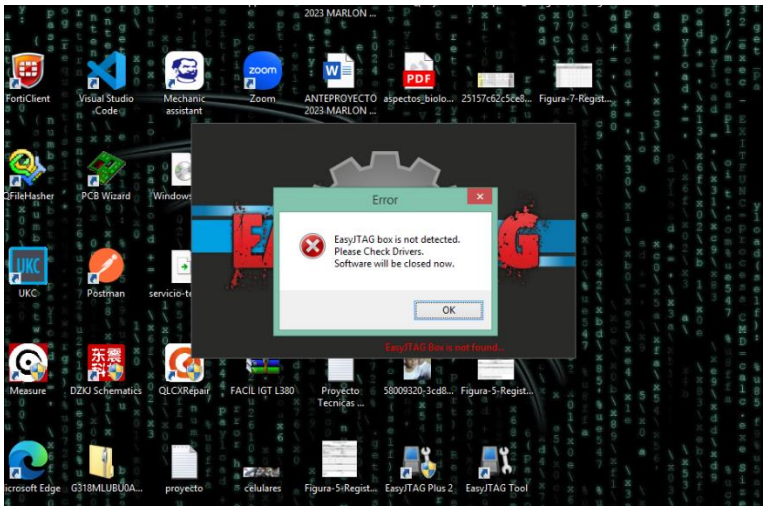



*Imagen 19: Ventana emergente de error.*

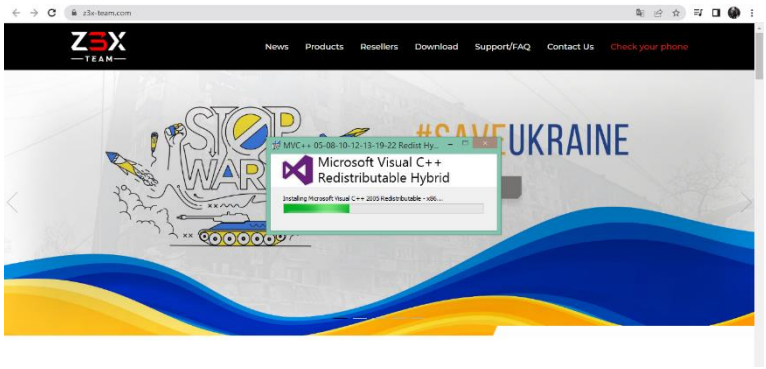



*Imagen 20: Instalación del programa Microsoft Visual C++.*

7. Dentro del directorio donde se encuentra el programa, se inicia la ejecución de los controladores de Easy Jtag.

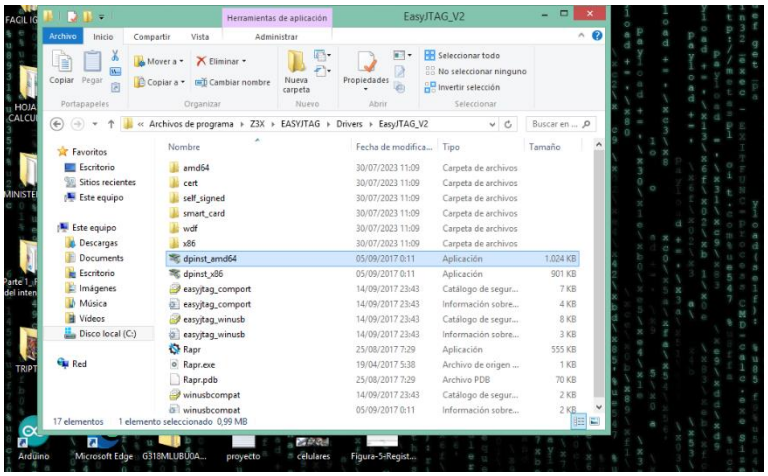



*Imagen 21:Ubicación del driver de la caja box.*

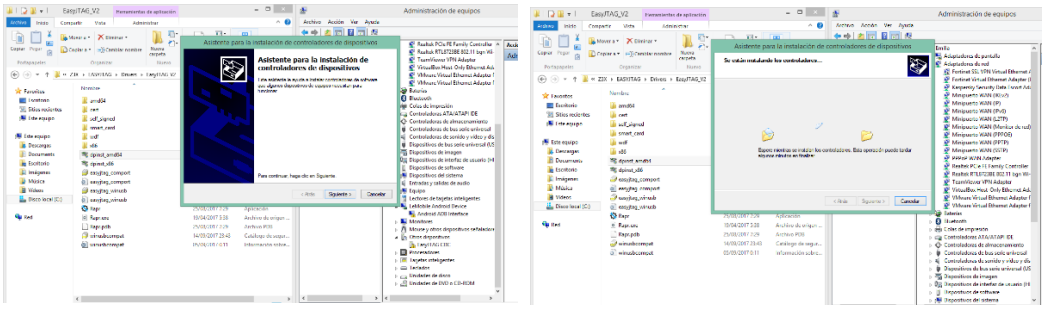



*Imagen 22: Instalación del driver.*

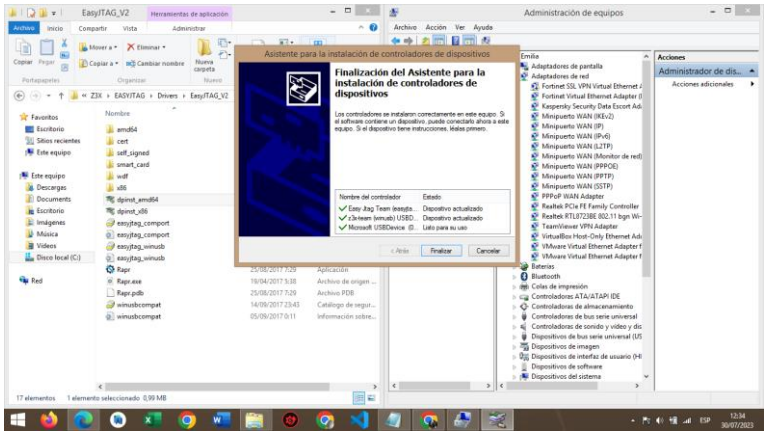



*Imagen 23:Finalización de la instalación del driver.*


*Imagen 24: Ventana del programa ejecutándose sin errores.*

Una vez que el equipo se identifica se procede con el desmontaje del dispositivo, se retira la placa base donde se realizará el método respectivo.

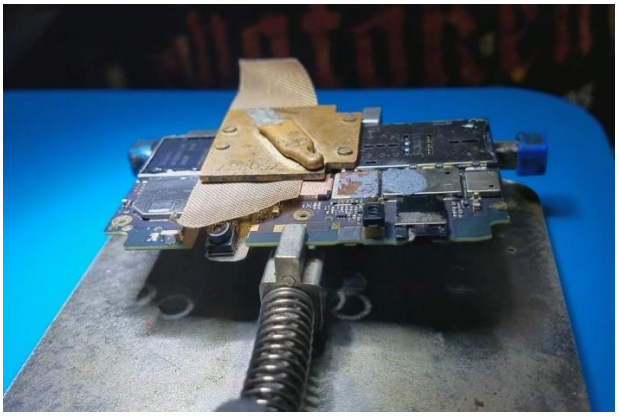


*Imagen 25: Mainboard de los dispositivos móvil.*

Se determina el enfoque a seguir en función a las condiciones del dispositivo y las características de la memoria. Por ejemplo, si se trata de un celular dañado y que no enciende, se procede a extraer directamente la memoria para su posterior lectura. En cambio, si el celular este encendido y en buenas condiciones, se lleva a cabo el proceso de ISP. En otro caso se revisa la característica de la memoria ya que hay memorias que no resisten altas temperaturas y pueden sufrir daños en el proceso, se debe tomar las medidas necesarias.

Se inicia el proceso de limpieza de la placa base en preparación para la soldadura, se buscará en programas de soluciones de hardware, como DZKJ o el programa que viene predeterminado en la caja box para localizar la conexión adecuada de pin-out para ISP.

**Punto de conexión eMMC**

- Vcc = 2.8V (voltaje de alimentación principal de la Nand flash)
- VccQ = 1,8V (voltaje de alimentación de interfaz MMC)
- CMD = Línea de comando.
- DAT0 / DAT3 = Transferencia de datos.
- CLK = Frecuencia de reloj.
- Vss o GND = Tierra o referencia de tensión

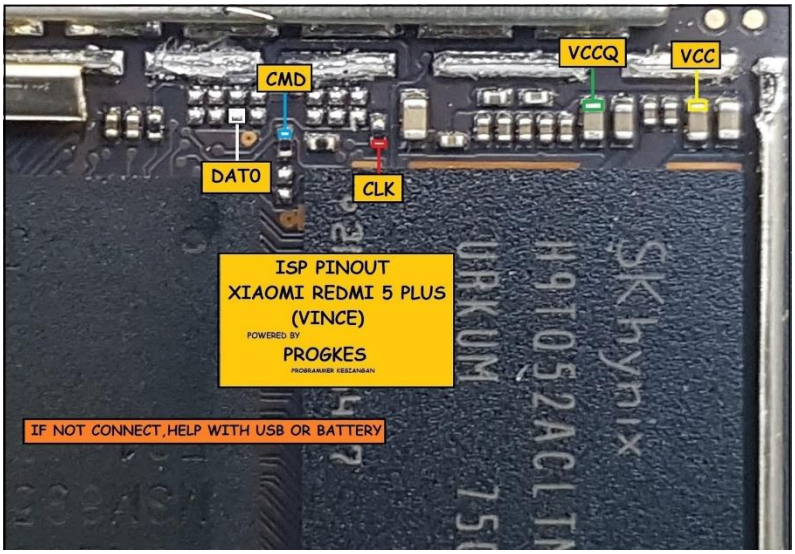



Imagen 26: Conexión PINOUT_ISP.

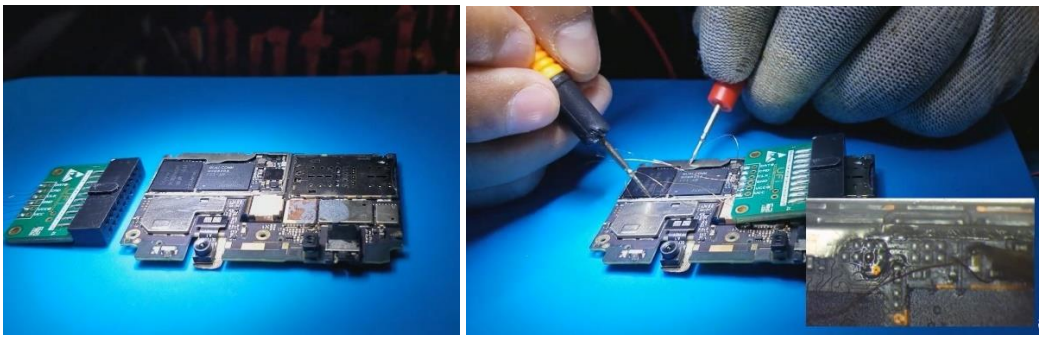


*Imagen 27: Conexión de los pines en adaptador ISP.*

Una vez que los pines se hayan conectado al adaptador se verifica si la conexión esta correcta por medio del multimetro, tambien se hace la verificacion de los voltajes antes mencionados, esto una vez conectado a la caja, luego se ejecutara el proceso para que el dispositivo sea reconocido por la computadora y el programa UFI – Emmc toolbox que es el programa determinado de la box.


*Imagen 28: Conexión de placa base al adaptador y caja box.*

Si la placa principal no es detectada por la caja box es porque el voltaje no es suficiente, se puede aplicar el voltaje necesario mediante el puerto USB que se encuentra en la sub placa, específicamente esto sucede solo en ciertos modelos de dispositivos.

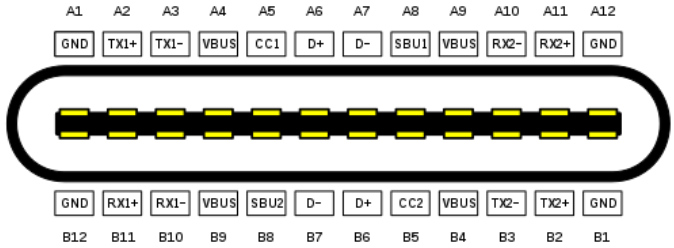



*Imagen 29: Puerto de carga USB tipo C.*


*Imagen 30: Puerto de carga USB tipo V8.*

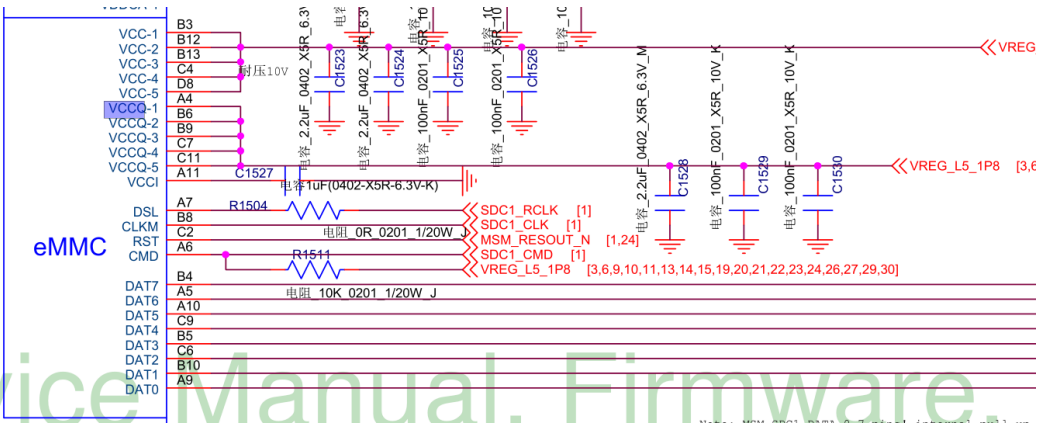



*Imagen 31: Diagrama para identificar líneas de testpoint (Xiaomi 5 Plus)*

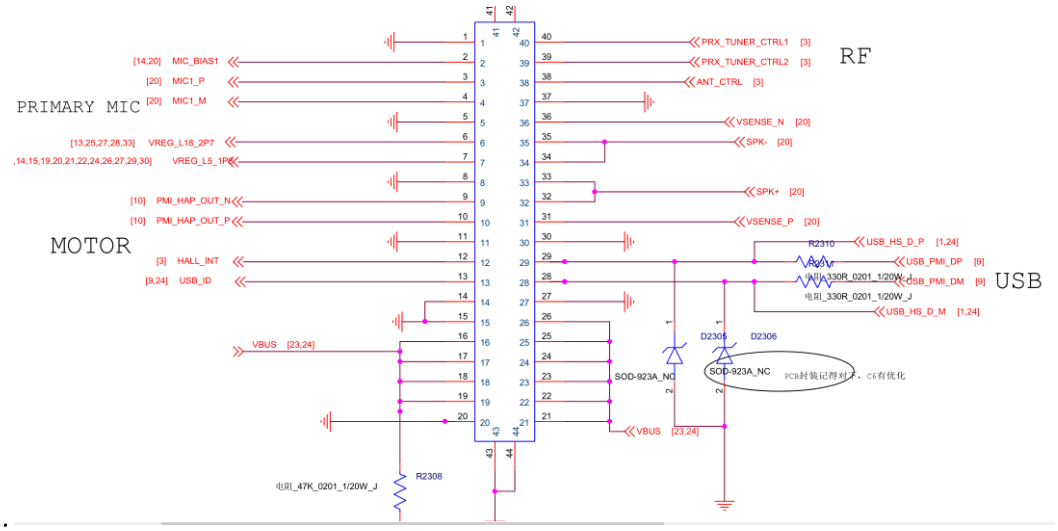



*Imagen 32: Diagrama de puerto de carga USB (Xiaomi 5 Plus)*

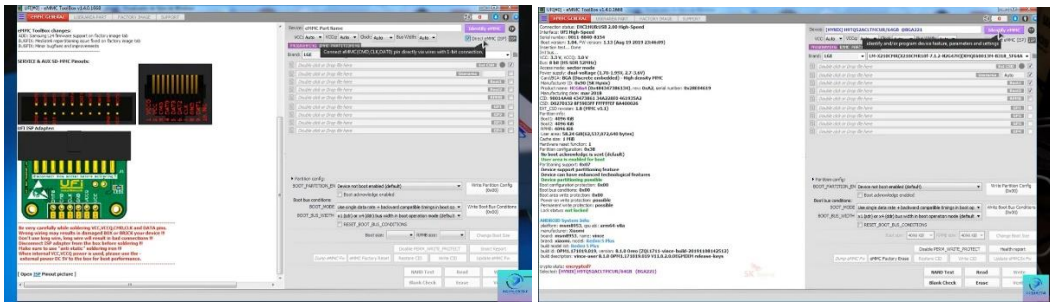


*Imagen 33: reconocimiento de la información de la memoria en software del box.*

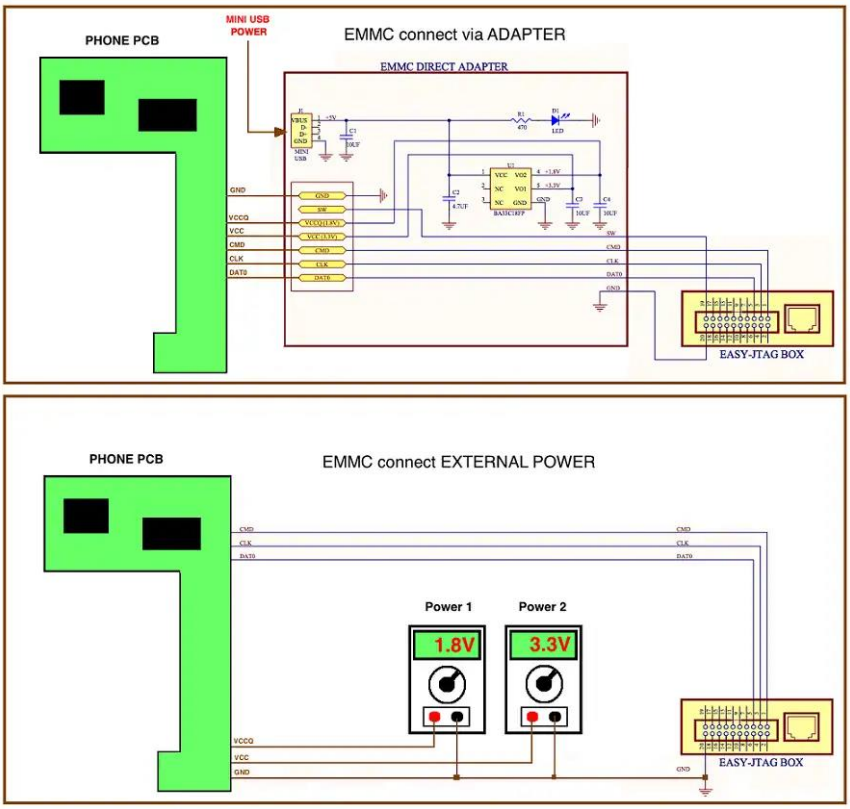



*Imagen 34: Arquitectura de conexión método ISP.*

Si se encuentran problemas en la conexión o los puertos seriales de la caja box, esto puede impedir la realización de una copia bit a bit y generar errores de comunicación. Si estos problemas persisten durante más de tres intentos, se optará por llevar a cabo el método del CHIP-OFF.

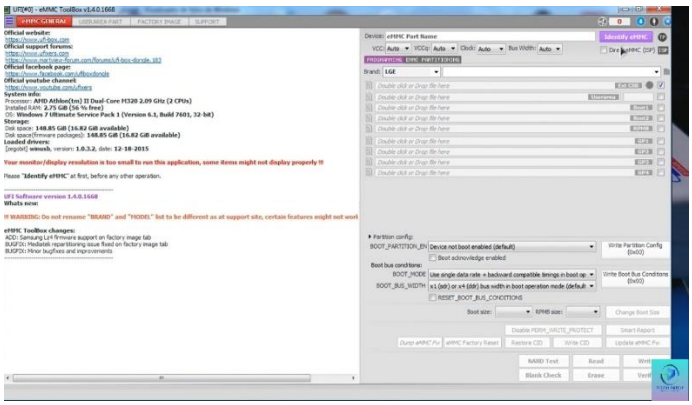


*Imagen 35: Error de comunicación.*

**Proceso CHIP-OFF**

Se procede a preparar la placa de manera que se pueda identificar la memoria y extraerla utilizando herramientas e insumos certificados para el proceso forense. Durante este proceso, se deben tomar precauciones adecuadas para evitar daños a la memoria, tanto por una manipulación incorrecta como por el estrés térmico.

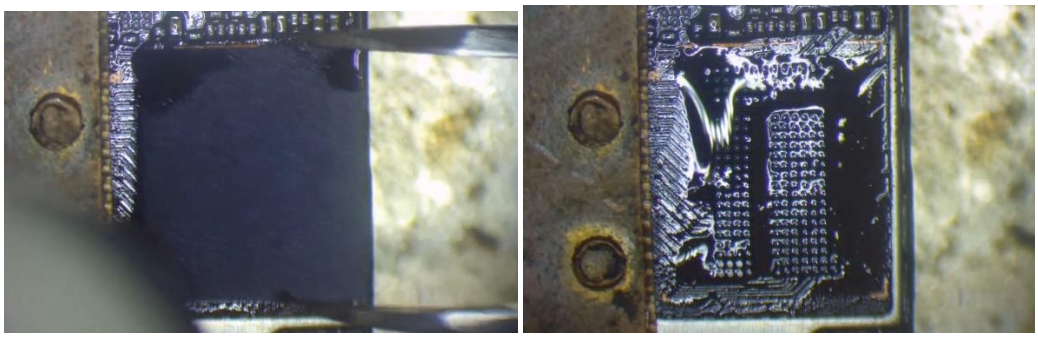


*Imagen 36: Proceso de extracción.*

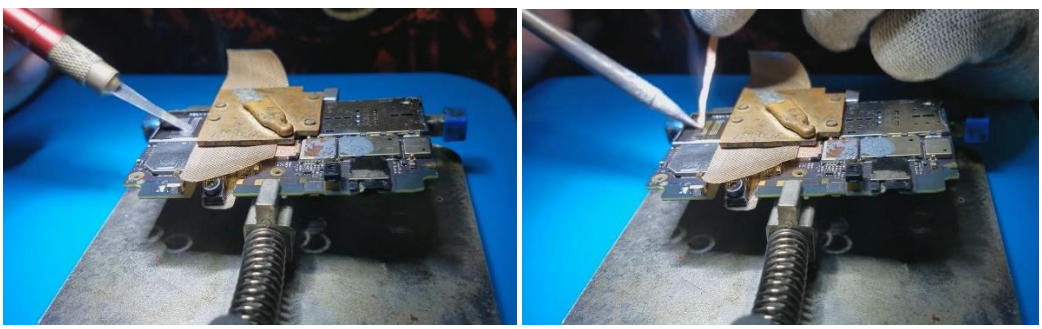


*Imagen 37: Limpieza de la placa base.*

*Imagen 38: Limpieza de la memoria.*

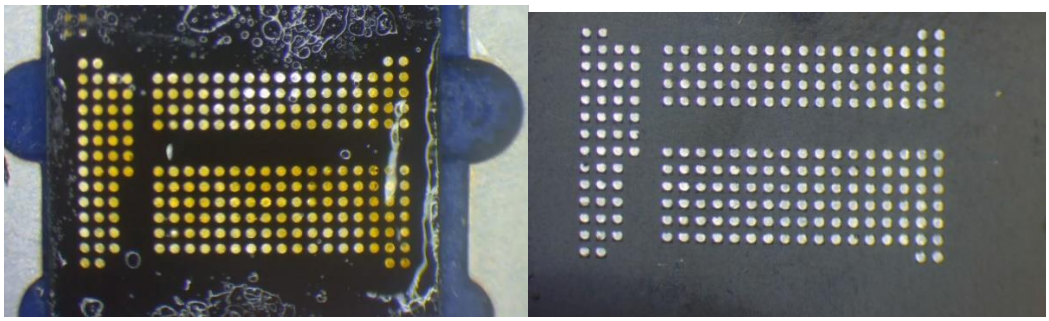


*Imagen 39: Preparación de la memoria para reballing.*

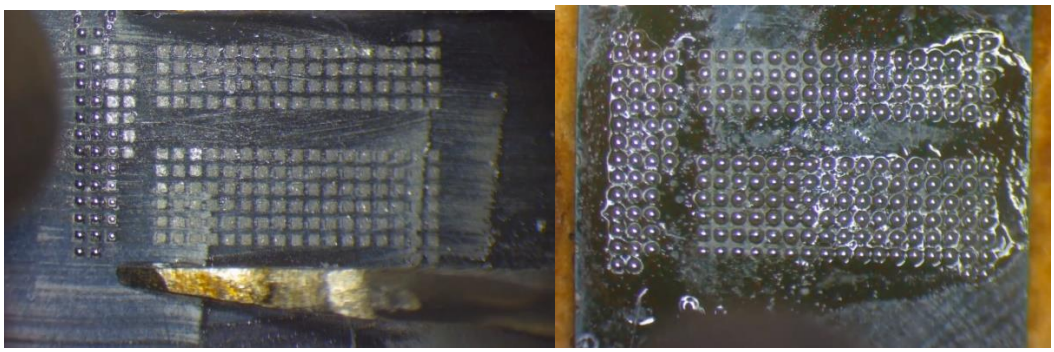


*Imagen 40: Proceso de reballing.*

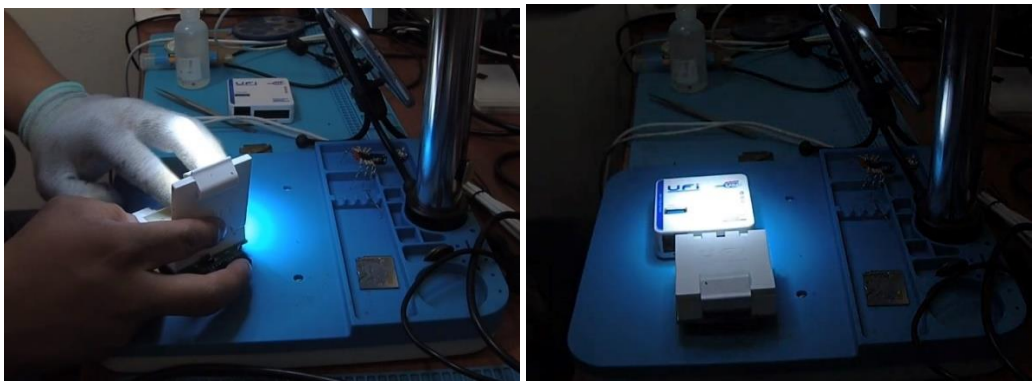


*Imagen 41: Inserción de la memoria a la caja Box.*

Después de completar la extracción de la memoria y colocarla en la caja box usando el programa predeterminado, se procede a realizar una copia bit a bit de los datos.

El programa Z3X Easy Jtag Classic se utiliza para establecer la configuración en el método CHIP-OFF, donde se verifica el voltaje, la frecuencia, la interfaz, el ancho de banda y se realiza una verificación de la memoria.

- Voltaje: 1,8V
- Frecuencia: 36 MHz
- Interfaz: Easy Jtag2/E-Socket
- Bus Width: 8 bit

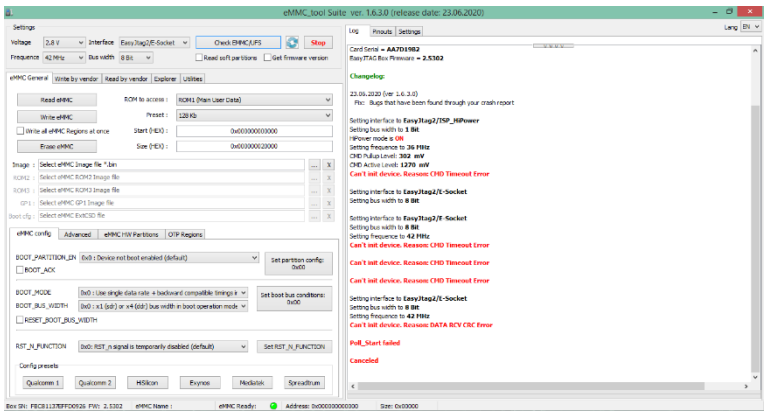


*Imagen 42: Chequeo de memoria eMMC.*

En el programa se identifica las particiones de la memoria dependiendo del procesador que tiene el dispositivo.

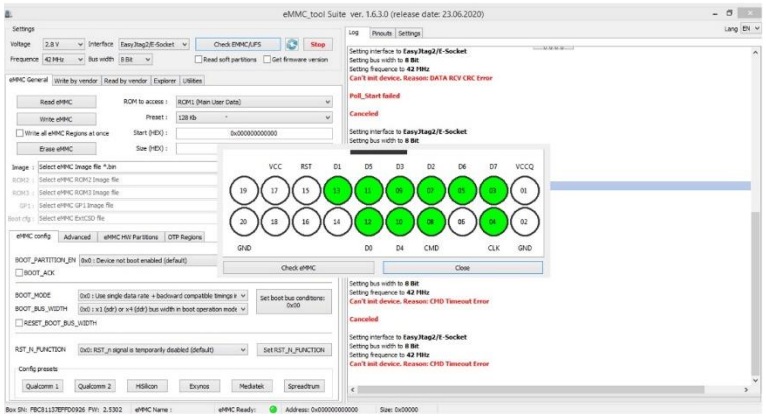


*Imagen 43: Reconocimiento del Socket.*

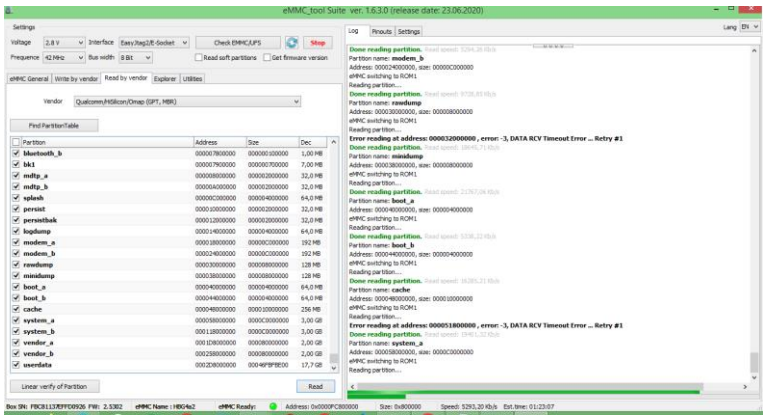


*Imagen 44: Particiones de la memoria.*

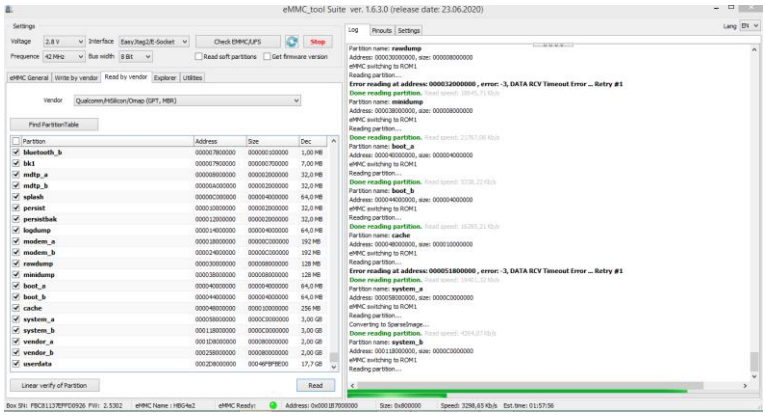
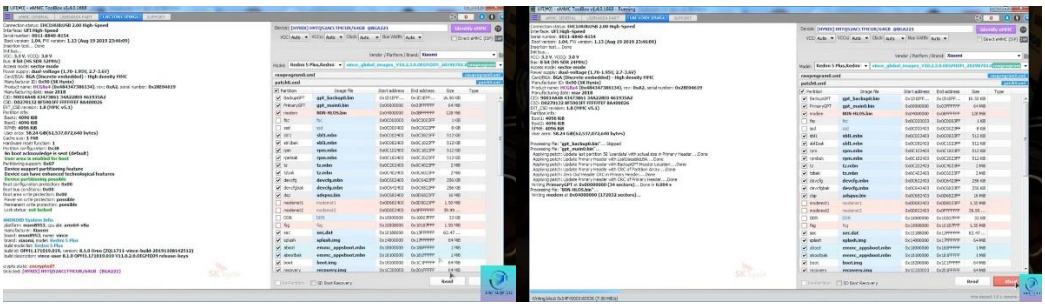


*Imagen 45: Lectura de las particiones de la memoria.*



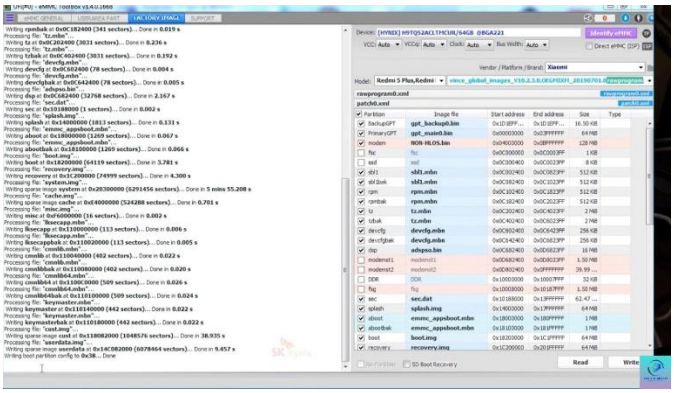


*Imagen 46: Copia de bit a bit.*

**Fase 3**

Durante esta etapa, se inicia el análisis de la memoria, teniendo en cuenta que el formato en que se almacenó la copia puede no ser compatible con todas las herramientas de análisis, por lo que se debe contar con varias opciones para asegurar su adecuada interpretación.


*Imagen 47: Herramientas de análisis.*

**Fase 4**

En esta etapa, se lleva a cabo la elaboración de un informe pericial, el cual será realizado por el perito informático o por la persona responsable de realizar todo el proceso de extracción de la evidencia digital. Una vez que se haya elaborado el informe, se considera presentarlo ya sea en formato físico o en PDF, según corresponda.

El formato base para el informe pericial puede ser descargado desde la página oficial del Consejo de la Judicatura, en la sección de peritos. Es esencial que el perito informático incluya toda la información necesaria y redacte el informe de manera adecuada.

El propósito de un informe pericial es brindar la información necesaria para permitir al tribunal, al juez o al abogado realizar sus funciones de manera adecuada. Para la elaboración del informe, se sugiere tener en cuenta los siguientes puntos:

- Identificación del perito
- Objetivo del informe
- Descripción detallada del dispositivo analizado
- Métodos y herramientas utilizadas en el análisis
- Presentación de los hallazgos y resultados obtenidos
- Conclusiones basadas en el análisis realizado
- Firma del responsable del informe

Es importante considerar todos estos elementos al redactar el informe pericial para garantizar que sea completo, claro y útil para el proceso legal o la investigación en cuestión.

**REGISTRO DE EVIDENCIA DIGITAL**
**Versión 1.0**

| **Código documento** | | **Fecha** | D D M M A A |
|---|---|---|---|
| **Nombre del caso** | | **Código de caso** | |
| | | | |
| **Dispositivo de origen** | | | |
| Tipo | Teléfono ( ) Tablet ( ) Otro: _____ | | |
| Marca | | Modelo | |
| Sistema operativo | | Versión | |
| Tipo de memoria | | Capacidad | |
| | | | |

| **Medio de almacenamiento de la prueba** | | | |
|---|---|---|---|
| Nro. de serie | Tipo | Capacidad | Ubicación del medio de almacenamiento |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| **Observaciones** |
|---|
| _____ |
| _____ |
| _____ |
| _____ |

| **Responsable** | |
|---|---|
| Encargado:<br>Identificación:<br>Cargo: | Firma: |

*Anexo 5: Registro de evidencia digital.*

**REGISTRO DE DISPOTIVO MÓVIL**
**Versión 1.0**

| **Código documento** | | **Fecha** | D D M M A A |
|---|---|---|---|
| **Nombre del caso** | | **Código de caso** | |
| | | | |
| **Especificaciones del dispositivo móvil** | | | |
| Tipo | Teléfono ( ) Tablet ( ) Otro: _____ | | |
| Marca | | Modelo | |
| Fabricante | | | |
| Número de serie | | | |
| IMEI | | | |
| Sistema operativo | | Versión | |
| Número de teléfono | | Proveedor | |
| Procesador | | | |

| **Almacenamiento** | | | |
|---|---|---|---|
| Tipo | Marca/Modelo | Velocidad/Capacidad | Nro. de serie |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| **Observaciones** |
|---|
| _____ |
| _____ |
| _____ |
| _____ |

| **Responsable** | |
|---|---|
| Encargado:<br>Identificación:<br>Cargo: | Firma: |

*Anexo 6: Registro de dispositivo móvil.*

**REGISTRO CADENA DE CUSTODIA DE PRUEBAS DIGITALES**
**Versión 1.0**

| Fecha | | | | | | Hora militar | Nombre y apellidos de quien recibe el elemento material de prueba o evidencia física | Cédula de ciudadanía | Entidad | Calidad en la que actúa (examinador, custodio, perito, transportador) | Traspaso o traslado (Entrega almacén, Almacenamiento, Análisis, Presentación, Audiencia, Consulta, Disposición final) | Observación al estado en que se recibe el embalaje o contenedor del elemento materia de prueba o evidencia física | Firma |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| D | D | M | M | A | A | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |

*Anexo 7: Registro de cadena de custodia de evidencia sigital.*

| 3. Registro de continuidad de los elementos materia de prueba o evidencia | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Fecha | | | | | | Hora militar | Nombre y apellidos de quien recibe el elemento material de prueba o evidencia física | Cédula de ciudadanía | Entidad | Calidad en la que actúa (custodio, perito, transportador) | Traspaso o traslado (Entrega almacén, Almacenamiento, Análisis, Presentación, Audiencia, Consulta, Disposición final) | Observación al estado en que se recibe el embalaje o contenedor del elemento materia de prueba o evidencia física | Firma |
| D | D | M | M | A | A | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |

**NOTA:**

1) Nunca interrumpa el registro de cadena de custodia.
2) el registro de cadena de custodia siempre debe acompañar al elemento materia de prueba o evidencia física.
3) si esta hoja no alcanza para diligenciar los registros de continuidad de cadena de custodia, se puede utilizar tantas hojas adicionales sean necesario. De ser así, en la parte superior derecha de cada hoja se indicara el número único del caso y el de la hoja a que corresponde del total de hojas que conforman el registro de continuidad.

*Anexo 8: Registro de continuidad de la evidencia.*

| FORULARIO DE ANÁLISIS DEL DISPOSITIVO | | | |
|---|---|---|---|
| **Código de Evidencia:** | 1001-1 | Caso: | 1001-1 |
| **Investigador:** | | Examinador: | |
| **Descripción del Caso:** | | | |
| **Recepción para el análisis (dd/mm/yy):** | | | Hora: |
| **Análisis (dd/mm/yy):** | | | Hora: |
| **Detalles del Teléfono Celular** | | | |
| **Propietario (si es conocido)** | | | |
| **Condición** | | | |
| **Fabricante** | | | |
| **Modelo** | | | |
| **Serial** | | | |
| **IMEI** | | | |
| **Número de Teléfono** | | | |
| **Operadora** | | | |
| **PIN** | | | |
| **Número de Tarjeta SIM** | | | |
| **IMSI** | | | |
| **Interfaz de Conexión** | | | |
| **Fecha/Hora Dispositivo** | | | |
| **Fecha/Hora Examinador** | | | |
| **Características del Teléfono Celular** | | | |
| | | | |
| **Particularidades** | | | |
| **Clave del Dispositivo:** | | Cargador: | |
| **Cable:** | | Programa: | |
| | | | |
| **Detalle de la Batería** | | | |
| | | Fabricante de la Batería: | |
| | | Cap. de Voltaje de la Batería: | |
| | | Número de Serie Batería: | |
| | | Resultado Voltímetro/Batería: | |
| **Notas:** | | | |
| **Características de la Tarjeta SIM** | | | |

| | | | |
|---|---|---|---|
| **Información de la Tarjeta SIM:** | | | |
| **Número ICCID en la Tarjeta SIM:** | | | |
| **Proveedor:** | SIM Card dañada: | SI: | NO: |
| | | | |
| | | | |
| | | | |
| | | | |
| **Información de Localización** | | | |
| | | | |
| **Observaciones y Conclusiones:** | | | |

*Anexo 9: Formulario de análisis del dispositivo.*

| | |
|---|---|
| **GUÍA DE LABORATOTIO** | **FECHA: --/--/----** |

| |
|---|
| **PRACTICA No --.** |
| **TITULO:** |

**INTRODUCCIÓN.**

Las particularidades inestables, anónimas, replicables, ajustables, adaptables y eliminables de la evidencia digital (elementos en su mayoría abstractos) hacen necesarios que los funcionarios que interactúan con la evidencia electrónica tengan conocimientos fundamentales para llevar a cabo una correcta obtención de la prueba digital.

En este análisis se abordan los conceptos esenciales para llevar a cabo la identificación, recopilación, preservación, solicitud de análisis y comprensión

de los resultados obtenidos en el manejo de la evidencia digital, adquirida en diligencias o actividades como primeros respondedores de la prueba digital.

**OBJETIVOS.**

E objetivo es adquirir conocimientos sobre el procedimiento de identificación, recolección, preservación, solicitud de análisis y compresión de los resultados obtenidos en el tratamiento de la evidencia digital.

Los objetivos específicos incluyen la extracción y análisis de información de una memoria de un dispositivo móvil a través de una imagen forense.

Se emplearán herramientas como UFI box o Easy Jtag Plus para extraer datos de la memoria, así como programas forenses (nombre de herramientas) para montar y previsualizar la imagen forense.

Se revisará y explicará el reporte generado por el programa forense, detallando el proceso de creación de la imagen.

Identificación de sumas de verificación HASH del dispositivo de origen y de la imagen. Finalmente, se llevarán a cabo los procesos de extracción de datos y se visualizara la información contenida en la imagen forense en un entorno seguro.

**EQUIPOS Y MATERIALES NECESARIOS.**

Equipos para revisión de hardware de dispositivos móviles, manteniendo su respectiva seguridad y preservación de datos. Software para análisis de datos obtenidos

**PROCEDIMIENTO.**

**EJERCICIO PRINCIPAL**

## Evidencia Original

1. Asegurar el dispositivo electrónico: Describa el procedimiento para garantizar la seguridad de la Evidencia Digital.
   Nota: Tenga en cuenta que en este caso se proporcionará una imagen forense previamente creada.
2. Una vez visualizada la imagen forense, verifique su integridad mediante la comparación de Hashes y documente los resultados obtenidos en un informe.

**Sobre la Imagen Forense**

3. Utilice el programa mencionado para llevar a cabo el análisis de la imagen forense.
   Siga los siguientes pasos:

a) Genere un listado de archivos junto con sus respectivos valores Hash y almacene esta información en un documento llamado "Hash archivos USB.csv". Guarde dicho documento.

b) Realice una búsqueda de información relevante para apoyar la investigación, prestando especial atención a posibles archivos eliminados. Asegúrese de que la extensión de los archivos coincida con el tipo de archivo buscado, y exporte los hallazgos al escritorio.

c) Para recuperar archivos eliminados, emplee programas de análisis forense recomendados.

**Cuestionario:**

1. ¿Cuál es el nombre que corresponde al dispositivo y, por ende, a la imagen obtenida? ¿Qué relevancia tiene esta información en relación con el caso?
2. Explique la importancia de asegurar la evidencia original y cómo la imagen forense puede presentar inconvenientes en este proceso.
3. En el informe, incluya una ilustración de las extensiones de los archivos encontrados y cómo la alteración de los nombres, propiedades o extensiones puede generar problemas.
4. Proporcione argumentos técnicos que respalden sus respuestas anteriores y describa cómo garantizar la integridad de la evidencia obtenida.

**AL FINALIZAR, ENTREGUE UN ARCHIVO EN FORMATO .DOC QUE CONTENGA EL INFORME CON LOS RESULTADOS DEL ANÁLISIS Y LAS RESPUESTAS A LAS PREGUNTAS PLANTEADAS.**

**BIBLIOGRAFÍA.**

Anexo 10: Informe pericial de la evidencia.