

Grado en ingeniería informática

Grado 2021-2022

*Trabajo Fin de Grado*

“Análisis forense de la aplicación

Microsoft Your Phone”

Lucas González de Alba

Tutor/es

Pedro Peris López

Colmenarejo, 15/03/2022



Esta obra se encuentra sujeta a la licencia Creative Commons **Reconocimiento – No Comercial – Sin Obra Derivada**

# Resumen

**Palabras clave:**

Microsoft

Your Phone

Informática forense

Análisis de artefactos

# Dedictoria

Este trabajo ha sido posible gracias a mi tutor Pedro Peris López que me ayudó en la selección de temáticas y desarrollo de la investigación y Josué Tapia, con quien he podido discutir algunas de las metodologías de análisis que mejor se ajustaban al trabajo. Finalmente agradecer a la Universidad Carlos III y a la empresa Álvarez y Marsal el apoyo y los recursos de los que me han dotado.

# Índice de contenidos

[Resumen III](#_Toc95815398)

[Dedictoria V](#_Toc95815399)

[Índice de contenidos VII](#_Toc95815400)

[Índice de figuras X](#_Toc95815401)

[Índice de tablas XI](#_Toc95815402)

[Lista de abreviaturas 1](#_Toc95815403)

[Introducción 2](#_Toc95815404)

[1.1 Estructura 2](#_Toc95815405)

[1.2 Resumen 3](#_Toc95815406)

[1.3 Motivación 4](#_Toc95815407)

[1.4 Metodología de trabajo 5](#_Toc95815408)

[1.5 Objetivos 7](#_Toc95815409)

[Estado del arte 8](#_Toc95815410)

[2.1 Definiciones 8](#_Toc95815411)

[2.2 Recursos externos 9](#_Toc95815412)

[2.3 Marco regulador 11](#_Toc95815413)

[2.4 Entorno socio-económico 16](#_Toc95815414)

[Desarrollo del proyecto 18](#_Toc95815415)

[3.1 Planificación 18](#_Toc95815416)

[3.2 Presupuesto 18](#_Toc95815417)

[3.3 Tecnologías empleadas 21](#_Toc95815418)

[3.4 Análisis del problema 25](#_Toc95815419)

[3.5 Diseño de la solución 36](#_Toc95815420)

[3.6 Implementación de la solución 41](#_Toc95815421)

[3.7 Evaluación de la solución 46](#_Toc95815422)

[Conclusiones y trabajos futuros 46](#_Toc95815423)

[4.1 Objetivos cumplidos 46](#_Toc95815424)

[4.2 Líneas futuras de trabajo 47](#_Toc95815425)

[Bibliografía 48](#_Toc95815426)

[Anexo 53](#_Toc95815427)

# Índice de figuras

[Fig. 1 Diagrama de Gant 18](#_Toc95815428)

[Fig. 2 Your Phone para Windows y Android [21] 25](file:///C:\Users\lucas\Documents\TrabajoFinalDeGrado\Final\YourPhoneApp\Microsoft-Your-Phone-parser\memoria_Microsoft_Your_Phone.docx#_Toc95815429)

[Fig. 3 Vinculando PC y móvil 27](#_Toc95815430)

[Fig. 5 HKU\sid\SOFTWARE\Microsoft\IdentityCRL\UserExtendedProperties\cuenta 28](#_Toc95815431)

[Fig. 4 Eliminar equipos vinculados. Izquierda Your Phone (Windows), derecha Your Phone Companion (Android) 30](#_Toc95815432)

[Fig. 6 Configuración de BBDD SQL 31](file:///C:\Users\lucas\Documents\TrabajoFinalDeGrado\Final\YourPhoneApp\Microsoft-Your-Phone-parser\memoria_Microsoft_Your_Phone.docx#_Toc95815433)

[Fig. 7 Metadatos de la imagen original 34](file:///C:\Users\lucas\Documents\TrabajoFinalDeGrado\Final\YourPhoneApp\Microsoft-Your-Phone-parser\memoria_Microsoft_Your_Phone.docx#_Toc95815434)

[Fig. 8 Metadatos de la imagen almacenada en media 34](file:///C:\Users\lucas\Documents\TrabajoFinalDeGrado\Final\YourPhoneApp\Microsoft-Your-Phone-parser\memoria_Microsoft_Your_Phone.docx#_Toc95815435)

[Fig. 9 Metadatos de la imagen almacenada en thumbnails 34](#_Toc95815436)

[Fig. 10 Tablas SQL de ContactsDB 35](#_Toc95815437)

[Fig. 11 Tablas SQL de PhoneDB 35](#_Toc95815438)

[Fig. 12 Tablas SQL de devideDataDB, sharedContentDB, notificationsDB y callingDB 36](#_Toc95815439)

[Fig. 13 Tablas SQL de SettingsDB y PhotosDB 36](#_Toc95815440)

[Fig. 14 Diagrama de componentes de YourPhoneForensicAnalyzer 37](#_Toc95815441)

[Fig. 15 Diagrama de flujo de información entre aplicación, programa y analizador 37](#_Toc95815442)

[Fig. 16 Ficheros CSV para buscar en YourPhoneForensicAnalyzer 41](#_Toc95815443)

[Fig. 17 Flujo de ejecución de YourPhoneForensicAnalyzer 42](#_Toc95815444)

# Índice de tablas

[Tabla 1 Matriz de costes de recursos humanos 19](#_Toc95815445)

[Tabla 2 Matriz de costes de herramientas software 20](#_Toc95815446)

[Tabla 3 Matriz de costes para herramientas hardware 21](#_Toc95815447)

[Tabla 4 Presupuesto total del proyecto 21](#_Toc95815448)

[Tabla 5 Características técnicas de los dispositivos empleados 22](#_Toc95815449)

[Tabla 6 Permisos de Your Phone Companion 25](#_Toc95815450)

[Tabla 7 Permisos de Your Phone 26](#_Toc95815451)

[Tabla 8 Firma de archivo según la extension 45](#_Toc95815452)

# Lista de abreviaturas

TFG: Trabajo final de grado

BBDD o db: Base de datos

DFIR: Digital Forensics and Incident Response

IA: Inteligencia Artificial

UUID: Universally Unique IDentifier o Identificador único universal

TCP: Transport-Control-Protocol

ICP: Internet Control Protocol

TLS: Transport-Layer-Security

NBNS: NetBIOS Name Service

## Introducción

El presente documento recoge el trabajo de fin de grado desarrollado por Lucas González de Alba, alumno de la Universidad Carlos III de Madrid. En él se presenta el siguiente proyecto de investigación sobre la estructura, comportamiento y artefactos de de la aplicación Microsoft Your Phone.

### 1.1 Estructura

La organización del documento viene dada por la siguiente estructura.

* Introducción. En primer lugar, este apartado se compone de una breve sinopsis del proyecto, un resumen del cuerpo de trabajo donde se resaltan los aspectos clave del mismo. En segundo lugar, las motivaciones que originaron el mismo, así como la coyuntura y propósitos que justifican su desarrollo. En tercer lugar, se explicará la metodología de trabajo y por último los objetivos del estudio.
* Estado del arte. Esta sección se centra en el proceso de investigación. En ella se muestran los distintos estudios encontrados relacionados con la temática del proyecto, exponiendo sus resultados y limitaciones. Asimismo, se presenta el marco legal en el que se engloba. Dado que en el campo de la informática está íntimamente ligado a la labor judicial, resulta muy relevante exponer el statu quo legal, así como indicar los distintos principios que se han seguido para garantizar la correcta protección, extracción y manipulación de la información sujeta a estudio. El criterio aquí recogido permite que la investigación conserve garantías legales.
* Desarrollo del proyecto. En este apartado se describe el cuerpo de trabajo, desde la planificación, preparación del presupuesto, aspectos técnicos de las tecnologías empleadas, su implementación y evaluación de resultados.
* Conclusiones y trabajos futuros. Esta sección está dedicada a la resolución de la investigación y el análisis de las soluciones propuestas. Finalmente, se plantean futuras vías de estudio para las cuales el trabajo desarrollado sirva de fundamento.

### 1.2 Resumen

Microsoft Your Phone es un servicio de Microsft para sincronizar ordenador y móviles con el objetivo facilitar al usuario el acceso a sus dispositivos integrando notificaciones, mensajes, fotos, llamadas y otras opciones del teléfono directamente en Windows. En las propias palabras de Microsoft:

“Obtén acceso instantáneo a todo lo que te gusta de tu teléfono, directamente desde tu PC. Vincula tu teléfono Android y tu PC para ver y responder a los mensajes de texto, hacer y recibir llamadas y mucho más, todo directamente en tu PC.” [1]

Dado que toda esta información puede resultar valiosa en el contexto de una investigación, el trabajo que aquí se presenta analizará la aplicación Your Phone desde la perspectiva forense en busca de sus artefactos y trazas digitales. Para ello se comenzó por indagar en el conocimiento ya existente sobre Microsoft Your Phone (artículos, publicaciones, blogs, foros…etc.) y al descubrir que el número de trabajos relacionadas con el proyecto era escaso se decidió expandirlo.

El primer paso consistió en adquirir una visión general del funcionamiento de la app. Se recogieron varias muestras digitales mediante pruebas con distintos dispositivos que fueron variando su contenido e interacciones. Luego se observó el efecto que dichas evidencias producían en la muestra. Con esta idea en mente se procedió a realizar un estudio formal del comportamiento de la aplicación utilizando técnicas de monitorización de procesos para encontrar aquellos artefactos del sistema relevantes. Sobre estos, se evaluó el formato y estructura y se estimó el valor forense de los datos que almacenan y se desarrolló un servicio que facilitase la extracción búsqueda y análisis. El script en Python programado se compuso de, por un lado, un marco dedicado a parsear e indagar en el contenido escrito o textual del teléfono (registros de llamadas, conversaciones y aplicaciones instaladas) y, por otro lado, otro para al tratamiento de imágenes, en concreto el reconocimiento facial. Sobre este último se probaron librerías con distintos modelos que permitiesen identificar múltiples caras dentro de una imagen, compararlas entre sí y buscar similitud en base a un perfil descriptivo. Se terminó escogiendo un híbrido entre OpenCV y DeepFace por sus resultados favorables y versatilidad. Finalmente se evaluó la calidad del software desarrollado a través de una batería de pruebas similar a la del paso preliminar.

En conclusión, se QUE PONGO?

### 1.3 Motivación

La investigación inicialmente surgió como un proyecto personal dedicado a conocer más a fondo algunas de las técnicas de análisis utilizadas en ciberseguridad e informática forense. Rápidamente creció en extensión, complejidad y alcance por lo que decidí orientarlo en una dirección mayor, mi trabajo final de grado. Pero ¿Por qué informática forense? Porque desgraciadamente es una asignatura que no se llega a impartir en el grado de informática y creo que su estudio puede resultar muy beneficioso para el currículo del alumno, ya que ofrece conocimientos trasversales a muchas otras áreas de las tecnologías de la información (seguridad, sistemas y computación).

Otro aspecto motivador fue la colaboración interdisciplinaria entre la escuela politécnica y la empresa privada. Gracias a la labor del equipo de orientación y empleo de la UC3M pude acceder al sector laboral a través una beca en prácticas dentro del departamento de informáticos forenses en la empresa Alvarez & Marsal. Esta entrada como becario me ha formado en los conocimientos y metodologías especificas a este aérea y me ha dotado de herramientas y espacio de trabajo (copiadoras, discos, licencias software…) lo que en último término ha favorecido escoger la temática.

Respecto a la elección de la materia, considero muy positivos los beneficios que aportaría el trabajo de análisis de Microsft Your Phone. Esta es una aplicación no demasiado estudiada, por lo que ahondar y expandir el conocimiento que se tiene de ella permitiría que futuros casos de estudio se valiesen del desarrollo realizado. Entre algunas de las ventajas se encuentra:

* Exponer el estudio formal de la estructura y artefactos determinando qué información se puede extraer de los artefactos de la aplicación. Con ello los analistas forenses podrían estimar que información está a su alcance en las investigaciones.
* Vincular el entorno móvil (teléfonos, llamadas, chats…) al de los computadores (usuario y programas) a través de la app. Conectar ambos permitiría obtener información del comportamiento de aquellos teléfonos vinculados con la aplicación, lo cual es de gran valor cuando se investiga una evidencia ya que exclusivamente a través de un PC no se tiene ninguna información de móviles. Cabe agregar que cada vez más son las personas que utilizan el móvil como método no solo de comunicación, sino también para la gestión del entorno laboral, para el ocio y entretenimiento etc.. por lo que ampliar el alcance de una investigación puede suponer todo un punto de inflexión.
* Extracción automatizada de imágenes almacenadas por el sistema. Esto evitaría la tarea tediosa y repetitiva de buscar, seleccionar y guardar cada imagen de la app.
* Permitir análisis ‘live’ o ‘en vivo’ de evidencias. Ejecuciones en tiempo real sobre la evidencia agilizaría las investigaciones en las que no se dispone de evidencias para análisis pasivo. Gracias al software que específicamente se ha desarrollado se podrían procesar casos en vivo

En resumen, estudiar desde la perspectiva forense la aplicación Microsft Your Phone no solo aporta las ventajas previamente expuestas, sino que también resulta novedoso y ofrece una oportunidad personal única para desarrollar un trabajo sustancial.

### 1.4 Metodología de trabajo

La metodología de trabajo se compone de dos grandes apartados, análisis y desarrollo.

Por un lado, el apartado dedicado al estudio del programa. Para adquirir la mayor cantidad de información posible del comportamiento del programa se establece un análisis incremental basado en las siguientes fases:

* Fase preliminar: se dispone el entorno de trabajo y las herramientas del análisis. Al instalar la aplicación tanto en móvil como en PC se recogen los permisos y propiedades de las instalaciones.
* Familiarización: esta fase determina una primera fuente de estudio y busca conocer intuitivamente que requisitos y capacidades tiene la aplicación.
* Análisis dinámico consiste en monitorizar en tiempo real la aplicación para conocer las interacciones de sus procesos y así poder recopilar aquellos artefactos del sistema que resulten relevantes
* Análisis estático: consiste en estudiar las principales trazas y artefactos descubiertos previamente.

Por otro lado, el apartado centrado en el desarrollo de una solución software dedicada a facilitar el acceso a la información previamente analizada. De nuevo la metodología a seguir es progresiva e incremental, comenzando por:

* Identificación de requisitos: captación de las necesidades y restricciones del problema.
* Diseño: establecer cuál de entre todas las distintas arquitecturas y soluciones software mejor se adapta al problema.
* Implementación: desarrollar el programa identificando
* Pruebas: evaluar el correcto funcionamiento del programa y verificar el cumplimiento de los requisitos.

La principal desventaja de dividir el proyecto en dos grandes bloques sucesivos, análisis y desarrollo, es que el primero condiciona al segundo. Esto implica que se debe retrasar la implementación del programa hasta conocer exhaustivamente la forma en la que se almacena la información en la aplicación, y hacerlo no es demasiado recomendable ya que exige demorar el desarrollo. Para evitarlo, se ha optado por romper el problema en sub-problemas de forma que estos sí se puedan paralelizar. Para ello se realizará un estudio preliminar, no muy extenso, de Microsoft Your Phone para determina cuales son las trazas que ésta deja en el sistema, así como sus principales características. Una vez se tenga se analizará y desarrollará para cada una de esas características un módulo y así, de esta forma, se logrará adquirir la precisión del estudio a la par que los avances en la implementación.

Otra desventaja del esquema análisis-desarrollo es que exige “duplicar” las pruebas. En la primera fase de análisis es necesario interactuar con la aplicación para conocer su funcionamiento en los distintos casos de uso, y en la última fase de desarrollo, hay que repetir las pruebas para comprobar que el código cumple con el comportamiento esperado. Este aspecto por desgracia resulta irreconciliable ya que no es recomendable construir un sistema basándose en una conjetura que debe probarse cierta en la última fase del proyecto. No obstante, el progreso escalonado presentado previamente permite construir software que rápidamente pase a ser funcional, acercando así la primera y última fase de test.

En resumen, la metodología escogida adopta tanto el análisis como el desarrollo de forma que ambos se complementen. Al combinarse con un avance incremental e iterativo se consigue una mayor cobertura del problema, además de permitir agregar nuevas funcionalidades de forma modular. Este esquema se ajusta muy bien al programa que se busca desarrollar ya que se trata de construir un software multitarea (parseado, extracción y manipulación multimedia). Finalmente agregar que, puesto que el trabajo de paralelización nunca es sencillo puesto que exige una extensa planificación y una laboriosa tarea de sincronización se ha optado por organizar el proyecto siguiendo un diagrama de Gant (figura Y página X)

### 1.5 Objetivos

Este capítulo recoge la principal meta del trabajo y establece los distintos objetivos específicos que la componen.

Principales metas:

1. **Detallar los procesos que componen a la aplicación Microsoft Your Phone y los artefactos que estos dejan en el sistema.** Recoger en un informe las trazas digitales del programa e identificar qué información de valor se almacena en el sistema.
2. **Implementar una solución software que permita recoger, parsear y exportar la información que presente la aplicación Microsft Your Phone.** A partir de los descubrimientos previos construir un sistema que facilite el acceso a la información almacenada y permita su extracción. Así mismo deberá generar un informe de todo el proceso.

Objetivos específicos:

1. **Extraer contenido salvaguardado por la aplicación:** Siempre que sea posible, se valorará positivamente la capacidad de recuperar contenido almacenado automáticamente por el programa. Para cumplirlo se utilizarán técnicas de carving
2. **Extraer contenido eliminado de la aplicación:** Siempre que sea posible, se valorará positivamente la capacidad de extraer contenido borrado. Para cumplirlo se utilizarán técnicas de carving sobre Unallocated Space
3. **Extraer el contenido multimedia de la aplicación y aplicar sobre este detección y categorización de rostros.** Entornos de trabajo especializados para analistas menudo incluyen servicios de procesado de imágenes, entre los más comunes se encuentra la detección de rostros. Esto permite al analista ahorrar un ingente número de horas de revisión en busca de un individuo.
4. **Evaluar el correcto funcionamiento de desarrollo mediante un amplio espectro de evidencias.** Comprobar si el programa funciona adecuadamente al enfrentarse a los distintos casos de uso de Microsoft Your Phone.

## Estado del arte

### 2.1 Definiciones

A continuación, se detallan los conceptos más importantes del proyecto con el objetivo de esclarecer ambigüedades y facilitar la comprensión y lectura del documento.

* Artefacto: “Todo aquello que puede obtener una evidencia, y cabe recalcar que son los diferentes ficheros, cadenas de registro, rutas de acceso y configuraciones que pueden determinar la actividad de un malware o de un usuario malicioso, así como las evidencias necesarias para una prueba.” [2]
* Carving
* TLS: se trata de un protocolo de comunicaciones que utiliza criptografía asimétrica para proporcionar comunicaciones seguras y confidenciales a través de una red.
* unallocated space.

### 2.2 Recursos externos

En el ámbito de la informática forense y ciberseguridad es común encontrar publicaciones relacionadas con el estudio y monitorización de programas de software libre, corporativo a malicioso. En dichos estudios se suele aplicar tanto análisis estático como dinámico y suelen involucrar hash análisis, carving, monitorización de red, reconocimiento de procesos y threads y rastreo del registro de Windows e investigación de artefactos . Comúnmente el trabajo de monitorización suele ser similar a todos los programas, y por tanto generalizable, pero cuando se trata de extraer de este, conocimiento e información propios de un programa, la labor se vuelve específica al caso. En otras palabras; puesto que cada aplicación es distinta, el análisis debe ser único para cada programa.

En lo que respecta a Microsoft Your Phone solo se han encontrado tres publicaciones que realicen este análisis y son Digital Forensics Tips&Tricks: «Your Phone» app Forensics [3], *Digital forensic artifacts of the Your Phone application in Windows 10* [4] y su posterior revisión *Microsoft’s Your Phone environment from a digital forensic perspective* [5]. El primero surgió como respuesta a la publicación del Insider Preview Build 18999 (20H1) de Windows 10 y se trata de un breve y superficial examen de los artefactos que la aplicación, recién introducida, producía. Por contraste, en el segundo los autores Patricio Domingues, Miguel Frade, Luis Miguel Andrade y Joao Victor Silva analizan las posteriores versiones 1.0.20453 y 3.4.4 de Your Phone para Windows 10's y la app para Android Your Phone Companion respectivamente. Además, su investigación propuso un script de Python diseñado para ejecutar en Autopsy. Por último, el tercero evalúa las actualizaciones 1.21011.127.0 (windows) y 1.21021.81.0 (android) y sigue la línea de desarrollo anterior, ampliando algunos aspectos que quedaron fuera del estudio previo y expandiendo las funcionalidades del programa propuesto. En comparación con el análisis que plantea Panov ambos trabajos son realmente reveladores ya que en gran medida presentan en mayor detalle cómo se organizaba la aplicación y como esta almacenaba los datos del usuario. En conjunto, los dos estudios hacen un análisis bastante completo y los autores consiguen cumplir con algunos de los objetivos que este trabajo persigue, pero no obstante dejan otros fuera. Algunos de los aspectos técnicos que la publicación no resuelve definitivamente son la monitorización de procesos, análisis del registro de Windows, descripción de la configuración de los artefactos. Otro problema adicional son las nuevas actualizaciones**.** La aplicación ha continuado renovándose, incluyendo nuevas funcionalidades y variando su estructura interna. Esto hace que algunas partes de su investigación queden relegadas a versiones anteriores y por tanto no se pueda utilizar como punto de partida. De la misma forma, el script de Python aparte de resultar inservible para las nuevas versiones está obsoleto ya que Autopsy tampoco lo reconoce.

En cuanto a fotos y videos se refiere son cada vez más comunes los servicios de procesamiento digital de imágenes embebidos en aplicaciones de carácter forense. Compañías como Belkasoft,, Magnet y Cellbrite están apostando por programas con utilidades variadas, especialmente con servicios orientados al reconocimiento de imágenes. Las últimas versiones de productos consolidados como Belkasoft X, Axiom Cyber o Cellebrite Physical Analyzer incluyen reconocimiento óptico de caracteres OCR, categorización de imágenes o auto detección de objetos y personas. En este sentido, se observa una tendencia que fomenta agregar los últimos avances del machine learning e IA, ya que al hacerlo se expanden las capacidades del software y se facilita el trabajo de los analistas.

P

A

J

A

### 2.3 Marco regulador

La informática forense es un sector ampliamente regulado puesto que en él se trata información sensible normalmente en un contexto judicial. Existen tres aspectos clave en lo que investigaciones forenses se refiere:

#### 2.3.1 La legislación y normativa legal.

El Convenio de la Ciberdelincuencia [6], elaborado en Budapest el 23 de Noviembre de 2001 y ratificado por España en 2010 cataloga los ciberdelitos en cuatro ramas:

1. Delitos que atentan contra el derecho a la confidencialidad, integridad y la disponibilidad de sistemas informáticos (sea ataque, intercepción o interferencia)
2. Delitos de falsificación y fraude informático mediante introducción, alteración o destrucción de datos o sistemas informáticos
3. Delitos por tenencia, adquisición, producción o difusión de contenido pornográfico infantil.
4. Delitos contra la autoría y propiedad intelectual

Así en España, la ley prevé delitos contra la privacidad, el espionaje, robo, suplantación de la personalidad, fraudes, falsificaciones, malversación, manipulación de dispositivos, daños o alteraciones de programas de datos o archivos…etc, todo ello ejemplos en los que la informática forense interviene.

Cabe mencionar dentro de este apartado las connotaciones éticas de la profesión, para la cual existen distintos códigos éticos o recomendaciones. Según la escuela internacional de informáticos forenses o la International Society of Forensics Computer Examiners (ISFCE) algunos de los requisitos éticos necesarios para certificarse como profesional son:

1. Demostrar compromiso y diligencia en el desempeño de las funciones asignadas.
2. Demostrar integridad en la realización de tareas profesionales.
3. Mantener la máxima objetividad en todos los exámenes forenses y los hallazgos actuales con precisión.
4. Realizar exámenes basados en lo establecido, procedimientos validados.
5. El cumplimiento con los más altos estándares morales y éticos y cumplir con el Código de la ISFCE
6. Testificar en sinceridad en todos los asuntos ante cualquier junta, tribunal o procedimiento.
7. Evitar cualquier acción que pudiera presentar a sabiendas un conflicto de intereses.
8. Cumplir con todos los ordenamientos jurídicos de los tribunales
9. Examinar objetivamente y a fondo todas las pruebas dentro del alcance del trabajo.
10. Las personas certificadas son responsables de mantener la certificación en los más altos estándares éticos y demostrar integridad, imparcialidad, diligencia y profesionalidad.
11. No ser cómplice ni participar en conductas no éticas o ilegales

Otras instituciones como el instituto SANS, además de todas estas guías incluyen el respeto por la integridad y honestidad, la defensa de la propiedad intelectual, confidencialidad y los derechos y libertades individuales y en definitiva la profesionalidad y la salvaguarda de la verdad. Del mismo modo condena cualquier forma de corrupción (chantaje, soborno o comisión), actitud prevaricadora, atentado premeditado contra la privacidad o la discriminación por sexo, raza, religión, edad, etnia, política o cualquier otra condición.

En conclusión, la normativa y la ética profesional dentro de este campo buscan, ante todo, proteger y mantener la honradez y entereza, para que así sea posible esclarecer la verdad y legislar en base a ella.

#### 2.3.2 La figura del perito informático en los juzgados.

La ley define a esta persona como aquel profesional especializado en la informática y en las nuevas tecnologías cuya labor consiste en proveer asesoramiento técnico en procedimientos judiciales, así como contribuir a la mediación y resolución de conflictos. Puede ejercer varios roles, el de mediador u arbitro y el de auditor. Los primeros se toman cuando dos partes están en desacuerdo y el perito debe intervenir para resolver las diferencias. Más concretamente es mediador si dirige o interviene activamente en las negociaciones y arbitro si su papel es pasivo, objetivo e imparcial. El arbitraje se resuelve mediante el “laude arbitral”, el dictamen alcanzado tras peticiones, reivindicaciones y alegatos. Para poder ejercer y ser reconocido como perito, se debe disponer de titulación y pertenecer a un colegio de profesionales de Informática. De lo contrario si se ejerce sin titulación o sin estar colegiado se está cometiendo un delito de intrusismo profesional (Art. 340 y Art 341 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil y Art 403 del Código Penal) [7]

El peritaje informático puede llevarse a cabo judicial o extrajudicialmente, siendo la motivación del análisis la principal diferencia. En uno, el procedimiento se centra en la obtención de pruebas para presentar ante el juez, mientras que, en el otro, las pruebas se recogen para esclarecer hechos o recabar mayor información. A menudo, si los abogados lo recomiendan, se puede presentar o ampliar una denuncia con el peritaje ratificado por el forense. Naturalmente también existe el contraperitaje, que consiste en rebatir el informe pericial de otra persona para poder impugnarlo mediante argumentos técnicos válidos. Esto último es importante ya que el forense debe testificar ante el juez que el informe es veraz y la evidencia del caso no ha sido alterada de ningún modo. Para asegurarse de que el procedimiento tiene garantías se sigue una extensa documentación y validación de cada interacción con la prueba (física o digital) y el cliente.

#### 2.3.3 La cadena de custodia

A la hora de presentar una prueba digital ante el juez existen una serie de requisitos previos que se deben cumplir para que esta sea admitida. La normativa legal determina que para cualquier prueba recogida se debe preservar la evidencia original junto con su cadena de custodia. La cadena de custodia es un procedimiento de control que recoge el proceso de obtención, manipulación, transferencia, cesión y preservación de evidencias para asegurar de forma rigurosa que la prueba ha sido entregada y permanece inalterada (demostración mediante hash). Existen distintos tipos de cadenas de custodia según la evidencia (móvil, portátil, servidor, memoria etc…), pero todas ellas comparten los siguientes campos:

1. Información general
   1. Nombre del cliente
   2. Nombre del proyecto
   3. Nombre del custodio
   4. Número de la evidencia
2. Información del dispositivo original
   1. Nombre del fabricante ☐ n/a
   2. Número de serie y modelo ☐ n/a
   3. Tipo de dispositivo ☐ n/a
      1. Portátil
      2. Sobremesa
      3. Tablet
      4. Móvil
      5. Servidor
      6. Otro
   4. Estado del dispositivo ☐ n/a
      1. Apagado
      2. Encendido con sesión iniciada
      3. Encendido sin sesión iniciada
   5. Tipo de información ☐ n/a
      1. Imagen forense
      2. Correo electrónico
3. Información sobre el medio
   1. Nombre del fabricante ☐ n/a
      1. Seagate
      2. Western Digital
      3. Intel
      4. Samsung
      5. Toshiba
      6. Hitachi
      7. IBM
      8. Maxtor
      9. Otros
   2. Factor y forma ☐ n/a
      1. 1.8”
      2. 2.5”
      3. 3.5”
      4. mSATA
      5. uSATA
      6. USB
   3. Tipo de conexión ☐ n/a
      1. SATA
      2. eSATA
      3. SCSI
      4. USB
      5. IDE
      6. ZIFF
   4. Tipo de almacenamiento ☐ n/a
      1. HDD
      2. SSD
      3. RAID
      4. Memoria FLASH
      5. Memoria RAM
      6. Cinta
      7. Floppy
      8. CD/DVD
      9. Nube/Web
      10. FTP
      11. Otro
   5. Número de serie y modelo ☐ n/a
   6. Capacidad ☐ n/a
   7. Encriptado ☐ n/a
4. Información sobre la adquisición
   1. Tipo
      1. Imagen física
      2. Imagen lógica
      3. Copia lógica
   2. Versión ☐ n/a
   3. Fecha y hora según dispositivo ☐ n/a
   4. Tiempo de adquisión ☐ n/a
   5. Localización ☐ n/a
   6. Herramienta utilizada ☐ n/a
      1. Software (EnCase, Magnet Cyber, FTK Imager,…)
      2. Hardware (Tableau, Cellebrite, Dossier, Disco de booteo Live…)
5. Información sobre la copia original y su salvaguardado
   1. Nombre de los fabricantes
   2. Números de serie y modelos
6. Cadena de custodia
   1. Fecha de recepción la evidencia ☐ n/a
   2. Nombre y apellidos de emisor ☐ n/a
   3. Fecha de devolución de la evidencia ☐ n/a
   4. Nombre y apellidos de receptor ☐ n/a
   5. Notas del proceso ☐ n/a
   6. Imágenes tomadas ☐ n/a

### 2.4 Entorno socio-económico

El impacto económico resulta difícil de estimar dado que en principio el producto se orienta a un nicho reducido, investigaciones forenses que involucren evidencias que contengan artefactos de Your Phone. No obstante, se podría esperar que la aplicación y el trabajo de investigación desarrollado trajesen algunas mejoras en el desempeño de los analistas para los casos en los que se presenten dichas evidencias. Según vestigeltd [8] los costes promedios de una investigación forense suelen rondar en promedio entre 5.000$ a 15.000$. No obstante, ninguna estimación es buena ya que depende en gran medida del tamaño del caso, su complejidad, estado de las evidencias, la premura con la que esta debe concluir y otro compendio de casuísticas como el tipo de actividad investigada, el volumen de datos y restricciones según cada país. A pesar de ello según la agencia se puede considerar estándar un coste de 250$ por hora de trabajo efectiva. En este sentido, el proyecto desarrollado podría tener un impacto positivo ya que lograría reducir el tiempo de análisis lo que podría repercutir en mayores beneficios y menos perdida por sobrecostes debido a extensiones de plazos. Luego también sucede que las posibles aplicaciones del programa software desarrollado no se limitan exclusivamente al contexto de investigaciones forenses ya que el script podría servir como base para otros ejercicios. Por ejemplo, su funcionalidad de extracción de imágenes serviría para cualquier aplicación que busque interactuar (introducir o extraer) el contenido multimedia de Your Phone. Lo mismo ocurriría con el comparador y agrupador de rostros, que en caso de generalizarse y perfeccionarse podría comercializarse como módulo adicional para algunas de los programas forenses descritos previamente (Belkasoft,, Magnet y Cellbrite).

*¿Por aquí bien?*

En cuanto a las implicaciones sociales y éticas cabe mencionar que al tratarse de un programa destinado a descubrir y trabajar con datos personales (conversaciones, llamadas, imágenes) se debería mantener estricta confidencialidad. Esto es parte de la guía de buenas prácticas de todos investigador y esta herramienta no es más que otro medio eficaz de conocer y analizar la información. Los beneficios de su correcta utilización son directos, un análisis veraz y eficiente de las evidencias digitales de un caso

## Desarrollo del proyecto

### 3.1 Planificación

Siguiendo la metodología escogida la planificación resultante es aproximadamente la siguiente; búsqueda de información, mes y medio, análisis y desarrollo, tres meses, documentación, mes y medio y evaluación y pruebas quince días.

A partir de este esquema se deriva el siguiente diagrama de Gant:

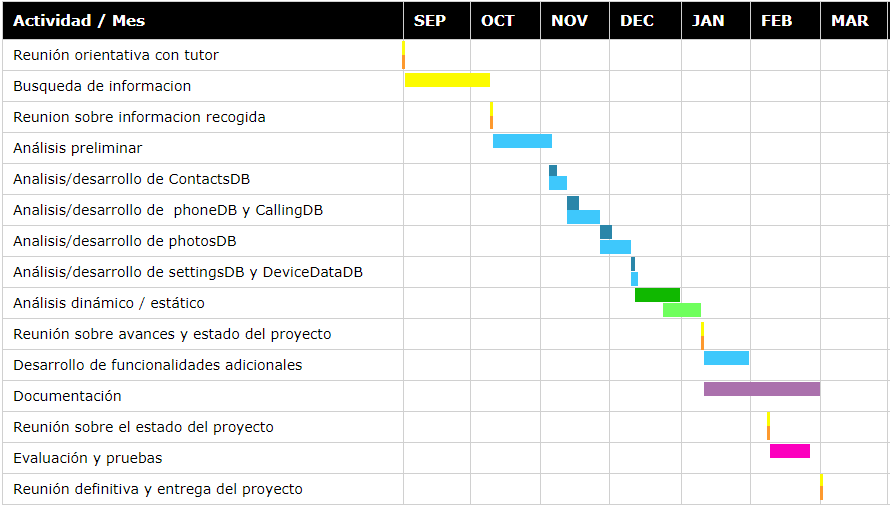


Fig. 1 Diagrama de Gant

Puesto que el proyecto se compagina con la beca de estudios descrita previamente en el apartado de motivación, el número de horas asignadas al TFG se asemeja a una jornada parcial, por lo que el tiempo total estimado dedicado a la ejecución será de 290 horas.

### 3.2 Presupuesto

El presupuesto se divide en costes derivados del personal y herramientas de trabajo:

**Recursos humanos:** el número de horas incurridas en investigación y desarrollo. Dado que el Trabajo final de Grado se compone de tutor y alumno, para estimar el coste de su participación se han tomado como referencias los salarios medio de un programador junior (novato) y un profesor universitario en España. Según glassdoor el promedio anual es de 19.745 [9] y 33.862 € [10] respectivamente, es decir aproximadamente 1.646 € y 2.822 € al mes, Partiendo de una jornada laboral completa (8 horas) a 21 días laborables por mes, el coste por hora es de alrededor de 10 y 18€. Si multiplicamos este valor por el número de horas de los participantes queda:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TABLA 3.1 Matriz de costes de recursos humanos | | | | |
| Puesto | Horas empleadas | Coste por hora | Subtotal | Total |
| Autor | 310 h | 10 € | 3.100 € | 3.244 € |
| Tutor | 8 h | 18 € | 144 € |

Tabla 1 Matriz de costes de recursos humanos

**Herramientas de trabajo:** el gasto derivado de licencias y maquinaria.

* **Herramientas hardware:** el equipo y dispositivo sobre los que mayormente se ha trabajado yo realizado pruebas ha sido un portátil DELL Latitude E7270 de 1.179,27 € y un móvil Samsung A20e, 145,20 €. Para calcular el coste total se ha calculado el porcentaje de uso (tiempo utilizado / tiempo de vida estimado) y se ha multiplicado por el precio de adquisición del recurso para así sacar su coste descontando su amortización. En el caso de teléfonos como el Samsung J3, HomTom HT20 Pro, XXX o el portátil HP EliteBook 840 G60 no se ha imputado gasto ya que el uso ha sido ínfimo.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| TABLA 3.3 Matriz de costes para herramientas hardware | | | | | |
| Recurso | Precio | Horas de uso | Horas de vida útil | % uso | Subtotal |
| DELL Latitude E7270 | 1.179,27 € | 310 h | ~ 1.825 h | ~16% | ~190 € |
| Samsung A20e | 145.2 € | 125 h | ~ 1.825 h | ~7% | ~10 € |
| HP EliteBook 840 G60 | 1.270 € | ~ 0 h | ~ 1.825 h | ~ 0.0% | 0 € |
| Samsung J3 | 124 € | ~ 0 h | ~ 1.825 h | ~ 0.0% | 0 € |
| Samsung A8 | 256 € | ~ 0 h | ~ 1.825 h | ~ 0.0% | 0 € |
| HomTom HT20 Pro | 110 € | ~ 0 h | ~ 1.825 h | ~ 0.0% | 0 € |
| Coste total |  |  |  |  | 200€ |

Tabla 3 Matriz de costes para herramientas hardware

* **Herramientas software:** la totalidad del trabajo se ha planteado desde la perspectiva del software de libre distribución por lo que no se incurre en gastos de licencias, no obstante, puesto que Your Phone es un programa desarrollado para Windows, sería necesario agregar el coste de uso del sistema operativo. Se comercializan cuatro versiones, una gratuita para estudiantes, por 145 euros Windows 10 Home, por 259 euros Windows 10 Pro, y a 439 euros Windows 10 Pro for Workstations pero puesto que la Universidad Carlos III tiene acuerdo con Microsoft se utiliza una licencia educativa gratuita.

|  |  |  |  |
| --- | --- | --- | --- |
| TABLA 3.2 - Matriz de costes de herramientas software | | | |
|  | Software | Versión | Precio |
| Windows 10 Icon - EVO | Windows 10 Pro | 21H1 / 19043.1415 (Licencia estudiante) | Gratuito |
| Microsoft Word 2013 – Material de apoyo centro imb-pc Computación | Microsoft Word 2016 | MSO 16.0.4498.1000 (Licencia estudiante) | Gratuito |
| Archivo:Visual Studio Code 1.35 icon.svg - Wikipedia, la enciclopedia libre | Visual Studio | 1.63.2 | Gratuito |
| Microsoft Your Phone | Logopedia | Fandom | Your Phone | 1.21113.36.0 | Gratuito |
| Microsoft Your Phone for Android: What is it and how does it work? |  Android Central | Your phone companion | 1.21113.85.0 | Gratuito |
| File:APK format icon (2014-2019).png - Wikimedia Commons | Android | 5.1.1 / 6 / 11 | Gratuito |
| Sysinternals Suite Alternativas y software similar - ProgSoft.net | Sysinternals | - | Gratuito |
| ProcDOT&#39;s Home - Online Documentation | procDot | 1.22 | Gratuito |
| Wireshark · Go Deep. | WireShark | 3.6.2 | Gratuito |
| Archivo:Python.svg - Wikipedia, la enciclopedia libre | Python | 3.8.2 | Gratuito |
| GitHub - sleuthkit/autopsy: Autopsy® is a digital forensics platform and  graphical interface to The Sleuth Kit® and other digital forensics tools.  It can be used by law enforcement, military, and corporate examiners | Autopsy | 4.19.2 | Gratuito |
| AccessData FTK Imager latest version - Get best Windows software | FTK Imager | 4.5.03 | Gratuito |
|  | DB Browser | 3.12.2 | Gratuito |
| DBeaver Documentation – DBeaver | DBeaver Lite | 21.3.0.202112052011 | Gratuito |
| Coste total |  |  | 0€ |

Tabla 2 Matriz de costes de herramientas software

El presupuesto total del proyecto es:

Tabla 4 Presupuesto total del proyecto

|  |  |
| --- | --- |
| tabla 3.4 Presupuesto total del proyecto | |
| Recursos humanos | 3.244 € |
| Herramientas hardware | 200 € |
| Herramientas software | 0 € |
| Total | 3500 € |

### 3.3 Tecnologías empleadas

El proyecto se sirvió de los siguientes dispositivos:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| TABLA 3.5 - Características técnicas de los dispositivos empleados | | | | | | | |
| Tipo | Modelo | Red | Pantalla | CPU | Memoria | Discos | Soportado |
| Archivo:Dell Logo.svg - Wikipedia, la enciclopedia librePC | DELL Latitude  E7270 | Ethernet, Bluetooth Wi-Fi | 12.5 pulgadas  1366x768 píxeles | i5-6300 2-Cores 2.4 GHz | DDR4 SDRAM 16GB 2133 MHz | SATA SSD  SKhynix SC311  256GB | Your Phone |
| Archivo:HP New Logo 2D.svg - Wikipedia, la enciclopedia libre PC | HP EliteBook  840 G60 | Ethernet, Bluetooth Wi-Fi | 14 pulgadas  1920x1080 píxeles | i7-8565U 4-Cores 1.8 GHz | DDR4 SDRAM 16GB 2400 MHz | SSD NVMe  KBG30ZMV512G KIO  512GB | Your Phone |
| Rubrin Shopping – Indian Most trusted shopping storeMóvil | Samsung A20e  SM-A202 | Bluetooth, Wi-Fi,GSM 4G/3G/2G, NFC | 5.8 pulgadas  720x1560 píxeles | Exynos 7884 2-Cores 1.6 GHz | LPDDR4  3GB  2133 MHz | eMMC 5.1  32GB  MicroSD 1TB | Your Phone Companion |
| Rubrin Shopping – Indian Most trusted shopping storeMóvil | Samsung A8  SM-A530FZKDPHN | Bluetooth, Wi-Fi,GSM 4G/3G/2G, NFC | 5.6 pulgadas  1080x2220 píxeles | Exynos 7885 7-Cores 2.2 GHz | LPDDR4  4GB  2133 MHz | eMMC 5.1  ‎256 GB  MicroSD 32GB | Your Phone Companion |
| Rubrin Shopping – Indian Most trusted shopping storeMóvil | Samsung J3  SM-J320FN | Bluetooth, Wi-Fi, GSM 4G/3G/2G, | 5 pulgadas  720x1280 píxeles | ARM CortexA7 4-Cores 1.5 GHz | LPDDR3  1.5GB  800 MHz | eMMC 4.5  8GB  MicroSD 4GB | No |
| Homtom Employee&#39;s Club - Creative Logo &quot;HOMTOM&quot; BeSmarter | Facebook Móvil | HomTom  HT20 Pro | Bluetooth, Wi-Fi,GSM 4G/3G/2G | 4.7 pulgadas  1280x720 píxeles | ARM CortexA5 8-Core 1.3 GHz | LPDDR3  3GB  800 MHz | 32GB  microSD - | No |

Tabla 5 Características técnicas de los dispositivos empleados

Microsoft lista los dispositivos soportados en la página oficial de Your Phone [11]

Para el software desarrollado se utilizó como lenguaje Python, versión 3.8.2. A continuación se recogen las librerías empleadas de acuerdo al siguiente formato.

* Tipo de librería
  + *Librería:*

Justificación

* Sistema
  + *Io* [12]: consiste en una librería para entradas y salidas de texto, binario, y contenido sin formato. Necesaria para manipular bytes de las imágenes y texto (e.j io.BytesIO).
  + *time* [13]: librería diseñada para manipular formatos fechas, horas, minutos y segundos. Necesaria para recoger el tiempo de ejecución del programa
  + *datetime* [14]*:* librería diseñada para manipular fechas, Necesaria para parsear los timestamps en formato LDAP a dd,mm,yyyy – h,m,s
  + *os* [15]: Librería diseñada para interactuar con el sistema operativo y facilitar la portabilidad de programas entre plataformas. Necesaria para manipular ficheros y directorios (e.j open, close, makedirs, getcwd etc…)
  + *sys* [16]*:* consiste en una librería por defecto de Python y sirve para ofrecer acceso a algunas variables y funciones del intérprete, por ejemplo la funcionalidad de escape del programa (sys.exit())
  + *uuid* [17]*:* consiste en una librería para generar UUID (identificadores universalmente únicos) según la norma RFC 4122, lo cual permite nombrar aquellos ficheros cuyo nombre es desconocido de forma que no exista colisión con el resto.

Imágenes

* + *PIL* [18]: Python Imaging Library, también abreviada como Pillow, es una biblioteca diseñada en colaboración por Alex Clark orientada a abrir, manipular y guardar imágenes en distintos formatos. Necesaria para operar con las imágenes.
  + *Deepface* [19]: es un framework ligero de reconocimiento facial y análisis de atributos faciales diseñado por Serengil, Sefik Ilkin and Ozpinar, Alper. Necesario para detectar y comparar rostros.
  + *Cv2* [20]: consiste en una librería de OpenCV de Bradski, G para Python. Permite manipular imágenes y transformar sus formatos.
* Consola
  + *argparse* [21]: librería diseñada por Steven J. Bethard [steven.bethard@gmail.com](mailto:steven.bethard@gmail.com) para recoger y validar los argumentos de un programa. Facilita la recogida de argumentos opcionales y posicionales además de generar automáticamente el mensaje de ayuda (-h, --help)
  + *Termcolor* [22]: librería diseñada por Konstantin Lepa [konstantin.lepa@gmail.com](mailto:konstantin.lepa@gmail.com) para imprimir en la terminal código ANSII coloreado. Facilita la comprensión de la salida por consola del programa (SMS enviados y recibidos verde, errores rojo, etc…)
  + *Halo* [23]: librería diseñada por Manraj Singh [manrajsinghgrover@gmail.com](mailto:manrajsinghgrover@gmail.com) para generar símbolos de carga (espirales rotativas) en la terminal. Favorece la comprensión de la salida por pantalla al indicar al usuario que la ejecución continua e imprimiendo su resultado al concluir.
* Ficheros
  + *csv* [24]: consiste en una librería para leer, escribir o maniplular ficheros csv. Permite exportar el contenido en formato separado por coma
  + *Sqlite3* [25]*:* consiste en una interfaz DB-API 2.0 diseñada por Gerhard Häring gh@ghaering.de para facilitar las interacciones con bases de datos SQLite (versiones superiores a la 3.7.15). Necesaria para extraer los datos de las bases de datos.
* Matemática
  + *Numpy* [26]*:* librería diseñada para cálculo numérico y análisis de datos. Necesario para el cálculo matricial en el que se basa el procesamiento de imágenes
* Expresiones regulares
  + *RE* [27]: librería de Secret Labs AB para manipular expresiones regulares basadas en strings de 8bits o UNICODE. Necesaria para evitar discrepancias al enlazar los teléfonos de la agenda con los teléfonos de las llamadas, sms… (Ejemplo +34 123 45 67 89, +34123456789, 123456789…etc)

### 3.4 Análisis del problema

#### 3.4.1 Aspectos generales de Your Phone

El servicio de Microsoft your phone se compone de dos partes, el programa para Windows Your Phone y la aplicación para Android Your Phone Companion (Figura a la izquierda). Desde la versión 1809.7 de Windos 10 Your Phone pasó a ser un programa por defecto, por lo que viene preinstalado en *C:\ProgramFiles\WindowsApps,* donde se encuentran una serie de directorios que identifican las aplicaciones estándar de Windows. Estas se catalogan según version, arquitectura y proveedor, por lo que en este caso se tiene M*icrosoft.YourPhone\_1.21121.256.0\_x64\_\_8wekyb3d8bbwe* donde 8wekyb3d8bbwe es el PublisherId de Microsoft, que identifica todos los nombres de paquetes de sus aplicaciones. El programa se instala independientemente en cada usuario y guarda sus datos en *%Appdata%* concretamente en local, ya que está asociada a un único ordenador.

Los requisitos de instalación de la aplicación móvil y su versión para computador son:

|  |  |  |  |
| --- | --- | --- | --- |
| TABLA 3.6 - Permisos de Your Phone | | | |
| C:\Users\lucas\Downloads\llamada-telefonica.png | Tiene acceso a todas las líneas telefónicas del dispositivo | C:\Users\lucas\Downloads\bluetooth.png | Se comunica con dispositivos Bluetooth ya emparejados |
| C:\Users\lucas\Downloads\almacenamiento-de-datos.png | Usa todos los recursos del sistema Administra otras aplicaciones directamente | C:\Users\lucas\Downloads\wifi.png | Acceso a la conexión de Internet y a la red doméstica o de trabajo |
| C:\Users\lucas\Downloads\icons8-program-100.png | Detectar e iniciar aplicaciones en otros dispositivos en los que se ha iniciado sesión.  Se cierra y cierra sus ventanas y retrasa el cierre | | |
| \* Requiere como mínimo un sistema operativo Windows 10 versión 18362.0 o superior Xbox y una arquitectura ARM, ARM64, x64 o x86 | | |

Tabla 7 Permisos de Your Phone

|  |  |  |  |
| --- | --- | --- | --- |
| tabla 3.5 - Permisos de Your Phone Companion | | | |
| C:\Users\lucas\Downloads\camara-de-fotos.png | Cámara: Realizar fotos y videos | C:\Users\lucas\Downloads\contactos.png | Consultar agenda de contactos |
| C:\Users\lucas\Downloads\sms.png | Leer SMS o MMS y enviar SMS | C:\Users\lucas\Downloads\llamada-telefonica.png | Consultar registro de llamadas, la identidad y estado del teléfono |
| C:\Users\lucas\Downloads\mapa.png | Ubicación: Acceso solo en primer plano | C:\Users\lucas\Downloads\bluetooth.png | Acceder a ajustes Bluetooth y vincular dispositivos. |
| C:\Users\lucas\Downloads\almacenamiento-de-datos.png | Leer o modificar contenido de la tarjeta SD y almacenamiento compartido | C:\Users\lucas\Downloads\wifi.png | Ver acceso a las conexiones de red y recibir datos de internet |
| C:\Users\lucas\Downloads\mas.png | Ejecución en segundo plano, al inicio, aparecer sobre otras apps y recuperar aplicaciones en ejecución.  Denegar optimización de batería y modo suspensión e inhabilitar bloqueo de pantalla.  Permite establecer alarmas, leer notificaciones  Api install Referrer de Play | | |
| \* Las llamadas requieren conexión Bluetooth y un PC con Windows 10 y una versión posterior a mayo de 2019  \*\* La funcionalidad de arrastra y suelta, pantalla de teléfono y aplicaciones requieren un dispositivo compatible | | |

Tabla 6 Permisos de Your Phone Companion

Según se ha podido observar Your Phone requiere tanto permisos de conexión wifi/datos móviles como bluetooth. La conexión a internet se utiliza para sincronizar el contenido del teléfono con el ordenador (transferir imágenes, logs, notificaciones…). Por defecto la app Your Phone Companion desactiva el envío de datos ya que puede suponer gastos elevados al usuario. Esto se puede editar en los ajustes de la aplicación. Según Microsoft, pc y móvil han de estar conectados a la misma red aunque posteriores pruebas demostraron que no es necesario. No obstante, para poder gestionar llamadas salientes y entrantes desde el ordenador se necesita vincular los dispositivos mediante una conexión bluetooth.

#### 3.4.2 Análisis dinámico

Para estudiar el comportamiento del programa se ha utilizado los servicios del paquete de aplicaciones sysinternals, concretamente uno llamado Procmon. Procmon es un programa de seguimiento de procesos muy utilizado en ciberseguridad que sirve para capturar lecturas y escrituras a ficheros o registros, eventos de Windows, creación y finalización de threads etc.… todo ello filtrando según el tipo de operación o valor y ajustando el periodo de monitorización. Paralelamente se ejecuta WireShark para atender las entradas y salidas de red. Posteriormente se utilizó Procdot, un servicio de diagramado para ilustrar gráficamente y así facilitar el estudio de las operaciones capturadas. El programa se articula a través de YourPhone.exe y YourPhoneServer.exe

**Emparejar ordenador y móvil**

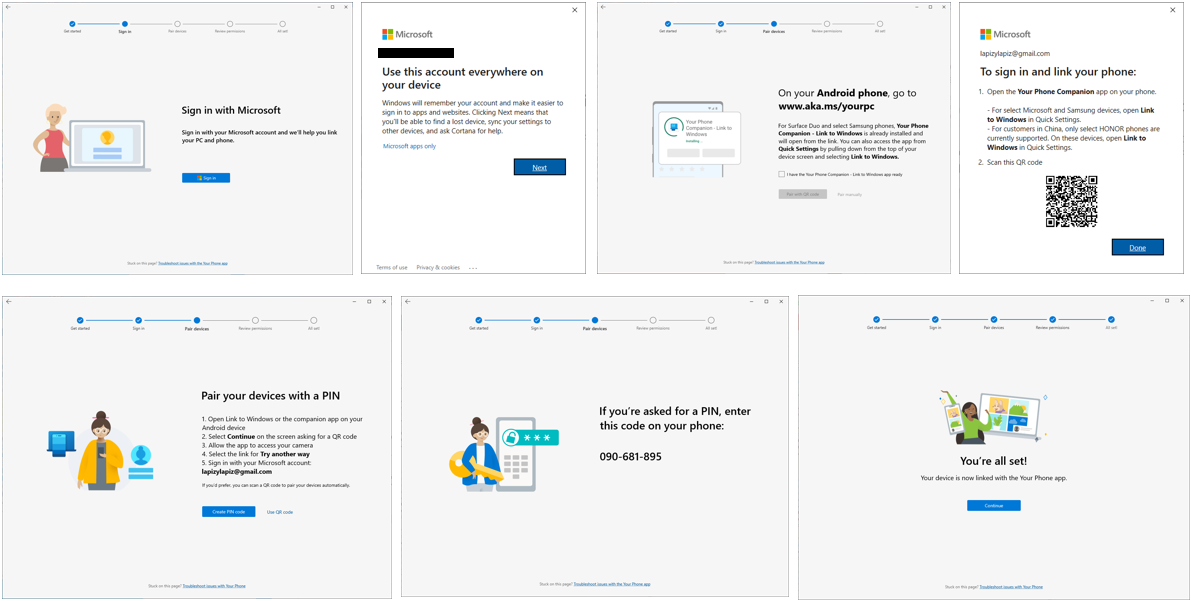
En un primer momento el contenido se encuentra exclusivamente en el teléfono, y para extraerlo es necesario iniciar sesión con una cuenta Outlook o MS tanto en móvil como en PC. A continuación, para emparejar los dispositivos el usuario debe vincularlos, o bien a través un código enviado a su cuenta de correo, o mediante un código QR que se autogenera periódicamente. En el primero el usuario deberá introducir sus datos de inicio de sesión en el teléfono y validarse mediante el código de siete dígitos enviado a su dirección de correo electrónico. A continuación, como método de segunda verificación aparece en la pantalla del PC donde se inició sesión un código de nueve dígitos que el usuario deberá insertarlo en el teléfono. En el segundo, el PC crea un QR y Your Phone Companion lo escanea. Ya sea a través de uno u otros se transfiere por la red los datos del teléfono, y luego en el PC se crea un nuevo directorio en la subcarpeta *Indexed* para almacenar los datos del dispositivo. Cada dispositivo tiene una carpeta con un uuid propio, con lo que se evitan colisiones de datos. A continuación, se muestra un ejemplo de los pasos descritos previamente, así como la estructura de carpetas una vez se ha vinculado un dispositivo, por ejemplo, el Samsung A20e genero el *0857d319-bd80-495f-a54a-34c472f351aa* y el Samsung A8 c2a273c1-0af6-487e-b4c3-6963db1d2caf.

Fig. 2 Vinculando PC y móvil

El siguiente árbol ha sido generado con *tree /a /f* y ejecutado sobre el directorio *C:\Users\username\AppData\Local\Packages\Microsoft.YourPhone\_8wekyb3d8bbwe* ilustra cómo queda la estructura de carpetas una vez se agregan los dos dispositivos Samsung de ejemplo. Se han agrupado los ficheros \*.db \*.db-wal y \*.db-shm para facilitar su lectura.

+---AC

| +---Temp

| \---TokenBroker

| \---Cache

+---AppData

+---LocalCache

| | YppCryptoTrustRelationships

| |

| +---Indexed

| | +---0857d319-bd80-495f-a54a-34c472f351aa

| | | \---System

| | | \---Database

| | | \*.db

| | | \*.db-shm

| | | \*.db-wal

| | |

| | |---c2a273c1-0af6-487e-b4c3-6963db1d2caf

| | \---System

| | \---Database

| | \*.db

| | \*.db-shm

| | \*.db-wal

| +---Local

| | \---Microsoft

| \---Roaming

| \---Microsoft

| \---Windows

| \---Start Menu

| \---Programs

+---LocalState

+---RoamingState

+---Settings

| roaming.lock

| settings.dat

|

+---SystemAppData

| \---Helium

| User.dat

| UserClasses.dat

|

\---TempState

\---amplicons

Mediante ProcDot observamos como YourPhone.exe, comienza a leyendo y escribiendo en algunos registros y que al seleccionar el inicio de sesión, se lanza svchost.exe, que inicia un enlace TCP (icp 4) dirigido a login.live.com, dirección 20.190.160.7. Más adelante TLSv1.2 inicia el intercambio de claves criptográficas para establecer una comunicación segura con el servidor con el que se validan usuario y contraseña e intercambian certificados. Algunos de datos del correo electrónico de Microsoft con la que está iniciando sesión en Windows se van almacenando en registro (Figura X).

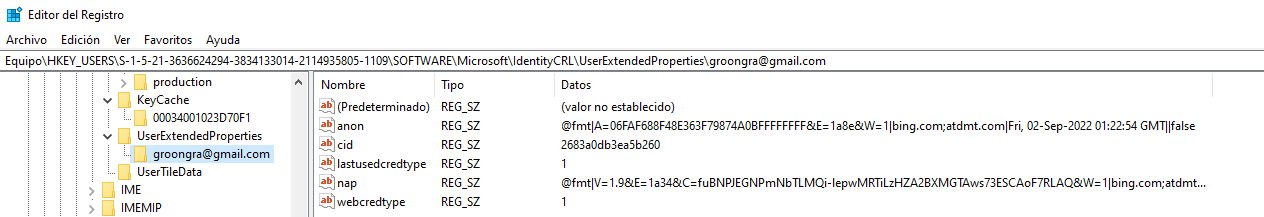


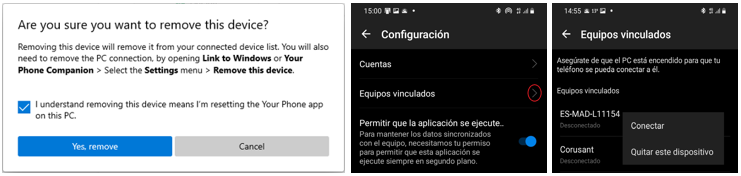
Fig. 3 HKU\sid\SOFTWARE\Microsoft\IdentityCRL\UserExtendedProperties\cuenta

Más adelante se genera en *AC\TokenBroker\Cache\* un fichero denominado f22b36b69223efe531c87b229e75ddc69c1f0246.tbres. Este tipo de extensión .tbres es un fichero de caché utilizado para administrar permisos de programas descargados desde Microsoft Store. Microsoft Windows TokenBroker se encarga de controlar que todas las aplicaciones cumplen con sus permisos y no realizan otro tipo de acciones maliciosas. Según avanza la ejecución YourPhone guarda en el registro *\REGISTRY\A\{5472abfe-5b7e-89ff-d098-98132f6eed9d}\ LocalState\ Devices\ 0857d319-bd80-495f-a54a-34c472f351aa\* algunos de los datos del teléfono como DevicePlatform, FriendlyName, Capabilities, Locale, CountryIso, PhotosDeviceermission, ContentDevicePermission, ContactsPcPermission, MessagesPcPermission, NotificationsPcPermission, MessagesDevicePermission, MessageMMSSendPermission…etc. Luego se generan los principales artefactos del programa; ocho bases de datos sobre las que se escribe de manera recursiva. Para cada uno de ellos se crean también dos ficheros con extensión .db-wal y .db-shm. En el análisis se observa como los ficheros generados son inspeccionados por MsMpEng.exe, el principal proceso de la aplicación antimalware Windows Defender. Entre sus funciones está generar y almacenar en *C:\ProgramData\Microsoft\Windows Defender\Scans\mpenginedb.db-wal* hashes de la información del disco para así monitorizar actividad maliciosa.

REGISTRYKEY:\registry\a\{5472abfe-5b7e-89ff-d098-98132f6eed9d}\localstate\apptelemetryuseraccountid

**Desemparejar ordenador y móvil**

También es posible desvincular los dispositivos vinculados en Your Phone, para ello simplemente hay que entrar en Mis dispositivos y seleccionar la opción ‘Eliminar’ sobre el teléfono en cuestión. Al hacerlo la aplicación lo borra del listado, pero no elimina sus artefactos. Es por esto que incluso tras haber quitado un teléfono es posible encontrar su contenido en el PC, lo cual supone una oportunidad para que los analistas obtengan conocimiento valioso. El programa también advierte que se debe eliminar manualmente el enlace al PC del móvil Figura X. No se ha estudiado artefactos en Android por lo que no se puede estimar si se genera o perdura algún tipo de rastro.

Fig. 4 Eliminar equipos vinculados. Izquierda Your Phone (Windows), derecha Your Phone Companion (Android)

Una vez hecho se realzó el siguiente estudio:

|  |  |  |  |
| --- | --- | --- | --- |
| TABLA 3. - Procmon - Procdot | | | |
| n | Descripción | Conclusión | Hallazgos |
| 1 | Vincular dispositivo | Emparejar movil y pc | REGISTRYKEY:\registry\a\{5472abfe-5b7e-89ff-d098-98132f6eed9d}\localstate\yppappprovidercontainer\0857d319-bd80-495f-a54a-34c472f351aa  \REGISTRY\A\{5472abfe-5b7e-89ff-d098-98132f6eed9d}\LocalState\ExpOverrides\ExpFileOverrideEnabled |
| 2 | Desvincular dispositivo | Desmparejar movil y pc | Hay registros LastSelectedView |
| 3 | Llamada telefónica desde el PC |  |  |
| 4 | Guardar imagen de la galería |  |  |
|  |  | Permite mostrar la última fecha en que se actualizó | \REGISTRY\A\{5472abfe-5b7e-89ff-d098-98132f6eed9d}\LocalState\Devices\0857d319-bd80-495f-a54a-34c472f351aa\PhoneAppsLastUpdatedTime |
|  |  | Muestra al usuario el nivel de bateria | \REGISTRY\A\{5472abfe-5b7e-89ff-d098-98132f6eed9d}\LocalState\YppTelemetry\LinkedDeviceBatteryInformation |

#### 3.4.4 Análisis estático

Una vez se identificaron las trazas de Your Phone en el sistema, se procedió a estudiarlas individualmente. Para conocer la estructura interna de las bases de datos, sus tablas y registros almacenados, se ha utilizado DB Browser y DBeaver Lite. Estas herramientas permiten operar y visualizar cualquier formato, y particularmente SQLite, que es el de Your Phone.

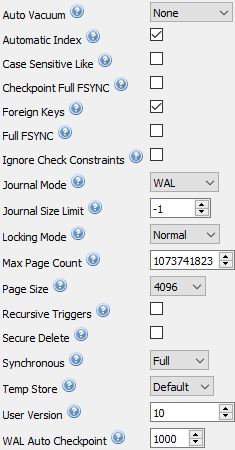
Su estudio reveló que las BBDD están dispuestas siguiendo la configuración de sentencias Pragma que muestra la figura de la izquierda. Pragma es una extensión SQL específica para el formato SQLite que permite para alterar el funcionamiento de la librería, así como consultar sus metadatos. En este caso resulta relevante que la opción “Auto Vacum” o auto-vaciado se encuentre inhabilitada dado que implica que la base de datos no reduce su tamaño tras aplicar operaciones de borrado, sino que las páginas del archivo db no utilizadas se añaden a una "lista libre" y se reutilizan para las siguientes inserciones. Asimismo, que “Secure Delete” esté también desactivada implica que las operaciones de borrado no sobrescriban el contenido con ceros. Finalmente está “Journal Mode” que toma la configuración Wal de entre Delete, Truncate Persist Memory y Off. La sentencia pragma especifica que el tratamiento de conflictos en la BBDD ha de ser Write-Ahead Log, lo que explica por qué se generan dos ficheros .db-wal y .db-shm por cada archivo db. Estos ficheros son archivos temporales que se generan o actulizan cada vez que se abre una conexión y sirven para dar respaldo a las operaciones internas en caso de que se produzcan fallos. Concretamente los Write-Ahead Logs son registros/diarios pensados para conflictos de escritura en commits y rollbacks, mientras que los archivos de memoria compartida, shared memory file o shm se utilizan cuando dos o más conexiones comparten el mismo archivo db y deben actualizar la misma ubicación de memoria. Esta última solo está presente cuando SQLite se ejecuta en modo WAL, como es el caso. El hecho es que al tener las BBDD configuradas en este modo se puede intentar recuperar algunos registros mediante carving. Undark es una herramienta que examina base de datos SQLite y vuelca en csv las filas de datos que encuentra intactas (tanto las actuales como las eliminadas) sin diferenciar entre los datos actuales y los borrados. Utilizando UnDark se pudo comprobar que es posible recuperar filas borradas, lo cual es muy positivo para la tarea de forense digital. No obstante, siendo pragmáticos, hay que reconocer que el alcance de estas metodologías es a reducido ya que a menudo solo aparece información parcial o corrupta. De la misma forma tampoco se descarta que exista algún registro en unallocated space.

Fig. 5 Configuración de BBDD SQL

Respecto a las tablas y su contenido se comprobó que:

En primer lugar, la agenda se almacena en contacts.db*,* donde reside la tabla principal *contact* que se relaciona a través de un identificador único *contact\_id* con otras tablas *phonenumber, postaladress, emailaddresss, contactDate, contactUrl* La experimentación llevada a cabo indica que mayoritariamente estas se encuentran vacías, pero podría deberse a las condiciones de prueba (modelo de teléfono y versión de Android). De lo que si se dispone es de teléfonos, localizados en *phonenumber*. Además, se ha observado que para cada tabla expuesta anteriormente existe una virtual con prefijo ‘fts’ así como que la base de datos cuenta con tres disparadores (trigger AFTER {DELETE, UPDATE, INSERT} ON) por cada una de estas tablas. En un primer momento se pensó que su función era la de salvaguardar y actualizar el contenido a medida que la aplicación agrega o elimina contactos, pero resultó ser una hipótesis incorrecta. Se trata de Full-Text-Search, un método de búsqueda optimizado por el cual a través de tablas virtuales se puede examinar eficazmente una o más instancias de un término de búsqueda en la BDDD.

En segundo lugar, el registro de llamadas, que se encuentra en *call\_history* en calling.db. De aquí se averiguó que los únicos valores que ofrecen información útil son el teléfono establece la llamada, si esta fue entrante o saliente, si fue aceptada o declinada, su duración y fecha. Your Phone registra números enteros en estos campos por lo que la información requiere análisis y parseo. Para ello se realizaron pruebas con las distintas casuísticas (véase tabla X), lo que permitió descifrar el significado de cada valor en los campos. Así mismo, se pudo comprobar que las observaciones de las publicaciones con respecto a anteriores versiones permanecían al día en la actual. El resto de campos o bien se repiten por defecto o son directamente nulos.

En tercer lugar, tenemos phone.db donde se almacena la información del dispositivo. Por un lado, en *subscription,* se tiene el contrato de telecomunicaciones (teleoperadora, país, sim, características de la tarifa, condiciones de roaming, mensajes multimedia, rcs y limitaciones en el envío). Sobre la actividad relativa al registro de sms y mms todos ellos se asocian a un chat (*conversation)* mediante un identificador denominado *Thread\_id* donde los primeros se guardan en *messages* mientras que los segundos en *mms*. Al igual que sucedía con las llamadas, los campos relativos a mensajes (tiempo del envío, tipo, status) contienen valores aparentemente cifrados, que requirieron pruebas y análisis para parseo.

En cuarto lugar, settings.db, que contiene la información de las aplicaciones, instaladas y recientes, del dispositivo, así como phone\_request. Por desgracia las evidencias recogidas no muestran ninguna traza de apps recientes o phone\_requests por lo que no se puede determinar si en algún caso traerían alguna información relevante. Sin embargo, sí se puede de aplicaciones donde lo relevante es nombre y versión. El resto de campos no ofrece ningún valor adicional ya que conociendo la app siempre se puede obtener su id o el de su paquete, por ejemplo 2926454279753648442 com.whatsapp o 2534083964653685902 com.google.

En quinto lugar, notifications.db, que almacena los avisos que las aplicaciones envían al usuario del teléfono. En un primer momento se creyó que se trataría de una fuente muy valiosa de datos, pero pronto se desestimó ya que el análisis mostró que tan solo se almacena la cola de notificaciones del teléfono. Your Phone actualiza notificationsDB y su pantalla cada vez que una aplicación envía un aviso, pero si el usuario las elimina o bien desde el teléfono o bien desde el PC esto se ve reflejado en la base de datos. Por ello tan solo queda registrado el último estado de la cola.

En sexto puesto, potos.db y deviceData.db, dos bases de datos que contienen la galería de imágenes (*media, photos*) y el fondo de pantalla del teléfono móvil (*wallpaper*). Complementando al estudio de P. Domingues, L. M. Andrade y M.Frade [5] se ha confirmado que la tabla *photos,* ahora obsoleta, era parte del funcionamiento de versiones anteriores donde se almacenaban las últimas 25 imágenes del dispositivo. Ahora *media* almacena en sus registros hasta 2000 imágenes del teléfono. en forma de blob (cadena de bytes). Photos.db también agrega información útil como el timestamp de la última vez que se actualizó o abrió, su extensión, tamaño, altura y anchura, y su uri. Al estudiar Your Phone se observó la galería del teléfono no se previsualiza completa, sino que el programa carga en sus registros las imágenes a medida que el usuario se desplaza por la galería. Por tanto, a la hora de estudiar una evidencia las imágenes almacenadas dependerán del uso que haya hecho el usuario de Your Phone. Respecto a estas imágenes de la BBDD, se ha examinado la persistencia de metadatos (la configuración de la cámara utilizada al tomar las fotografías, la información sobre la fecha, la ubicación, y las miniaturas) mediante un visor en línea denominado Jeffrey Friedl's Image Metadata Viewer [28]. Este ha permitido comprobar que YourPhone no almacena la imagen original en sus registros, sino que guarda, por un lado, una previsualización (thumbnail) sin metadatos EXIF, y una copia de menor tamaño con una sección reducida de estos.

**Metadatos de 20210719\_131234.jpg**

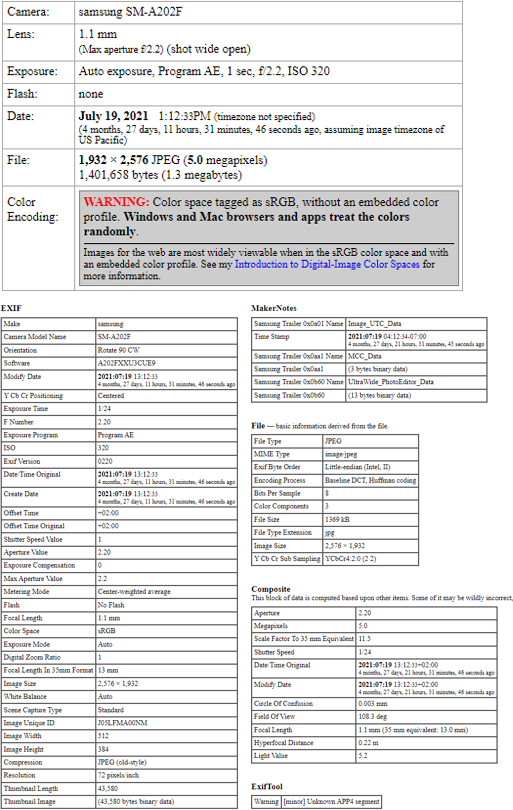
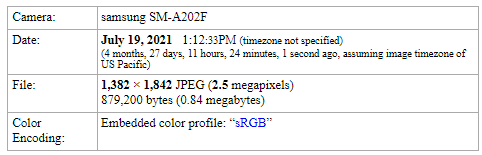
Fichero original Media

Fig. 6 Metadatos de la imagen original

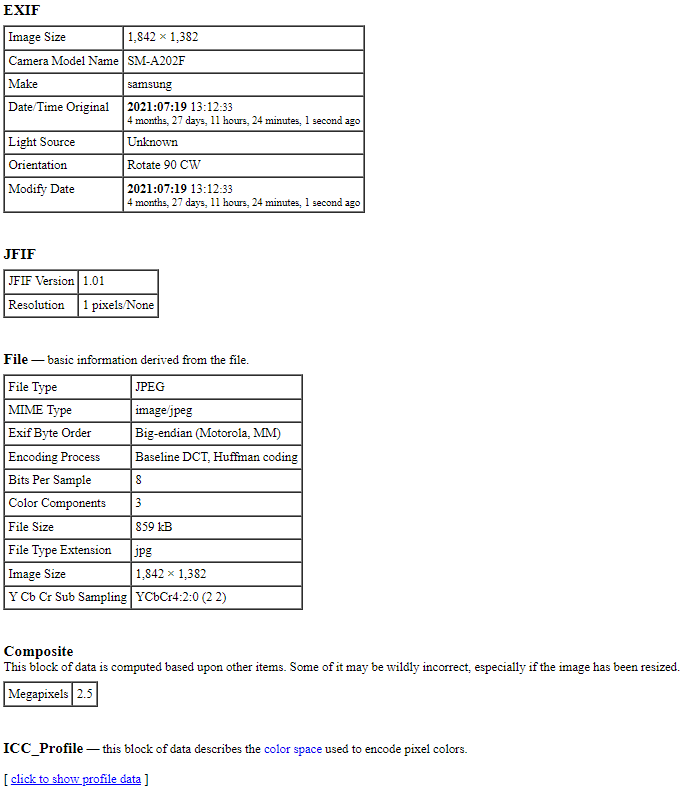


Fig. 7 Metadatos de la imagen almacenada en media

Thumbnail

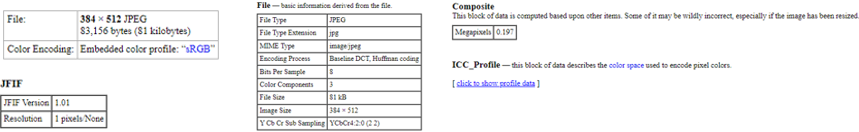
****

Fig. 8 Metadatos de la imagen almacenada en thumbnails

**Bases de datos de Your Phone**

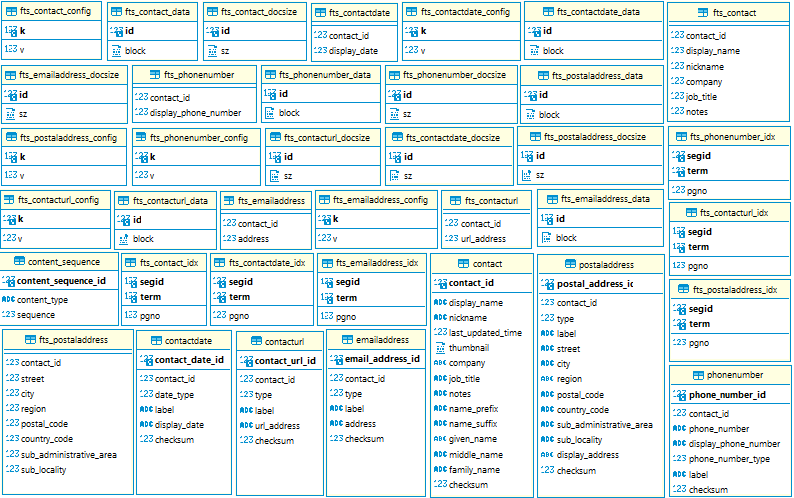
ContactsDB

Fig. 9 Tablas SQL de Contacts.db

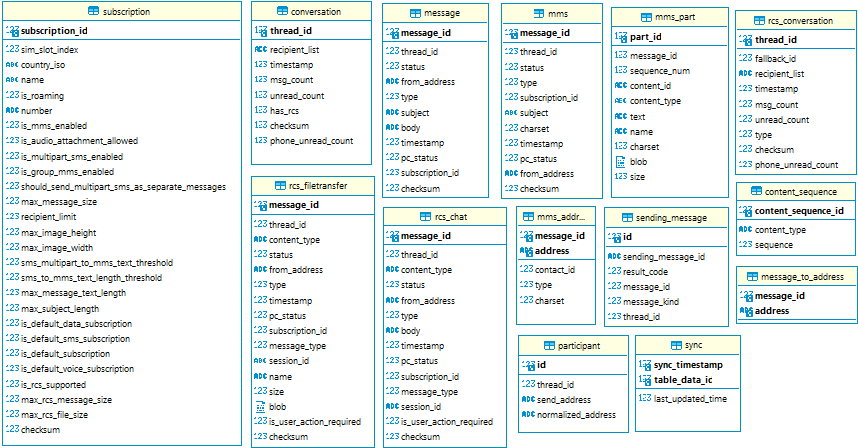
PhoneDB

Fig. 10 Tablas SQL de Phone.db

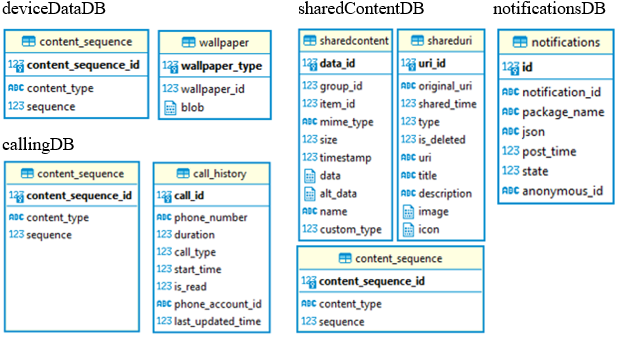


Fig. 11 Tablas SQL de devideDataDB, sharedContentDB, notificationsDB y callingDB

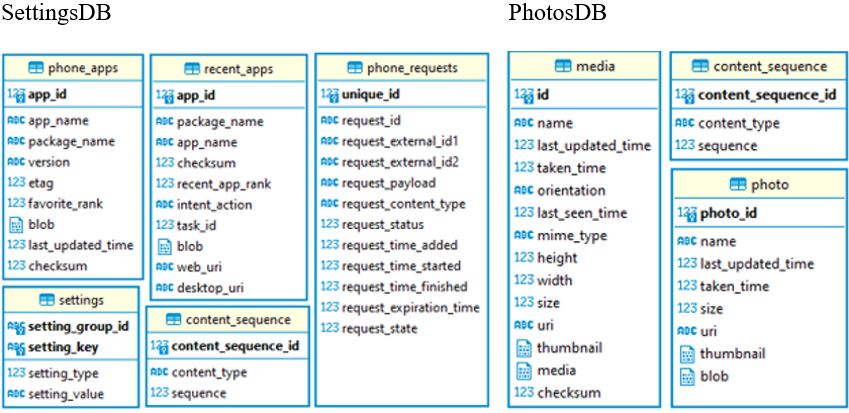


Fig. 12 Tablas SQL de settings.db y photos.db

### 3.5 Diseño de la solución

Una vez conocida la forma en que el programa almacena la información se procedió a desarrollar un script que permitiese extraerla y estudiarla. Para ello, primero se organizó la funcionalidad y luego la estructura del programa. La figura X ilustra los componentes que lo conforman mientras que la figura U revela cómo se organizan las clases. Por último la figura Z muestra como fluye la información desde el origen (aplicación de Android), al ordenador (programa de Windows), hasta el script de análisis forense. Es decir, el diagrama de componente y clases exponen la arquitectura software y sus dependencias y el diagrama de flujo indica cómo la información del usuario viaja entre la app y el programa de Your Phone, además de como está se recoge en el script para analizar su contenido.

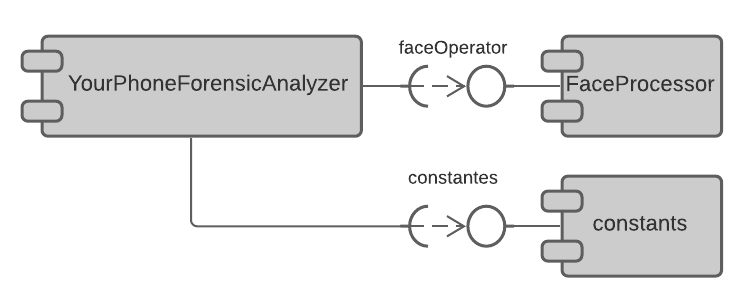


Fig. 13 Diagrama de componentes de YourPhoneForensicAnalyzer

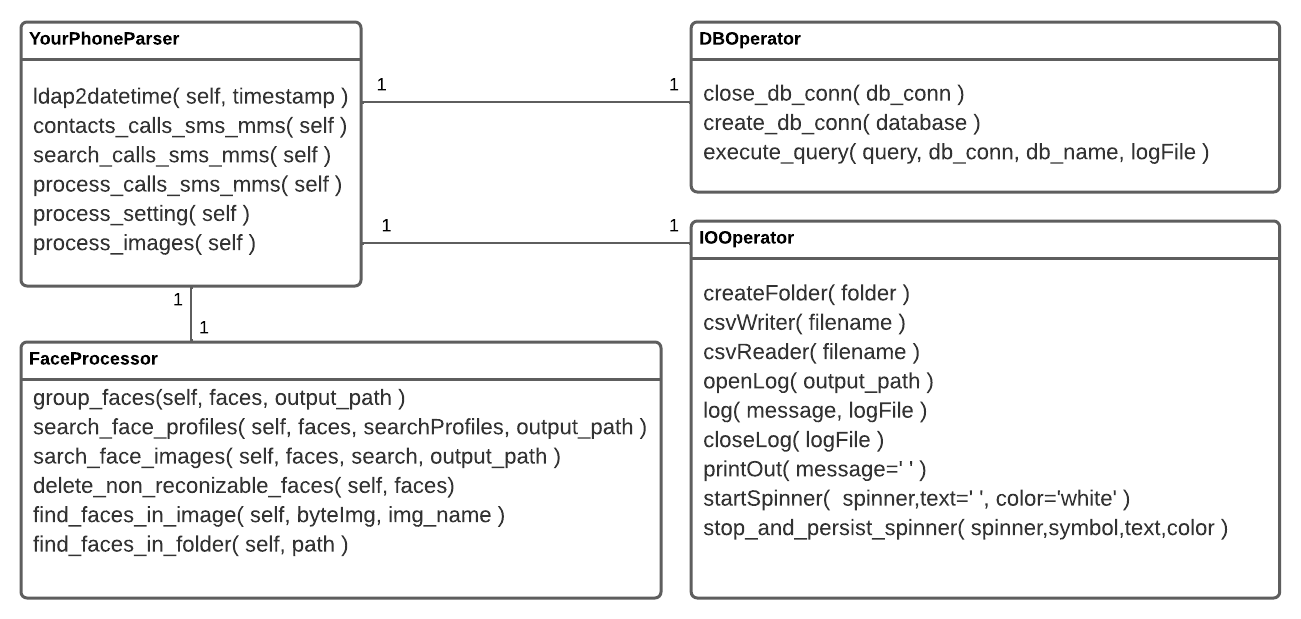


Fig. 14 Diagrama de clases

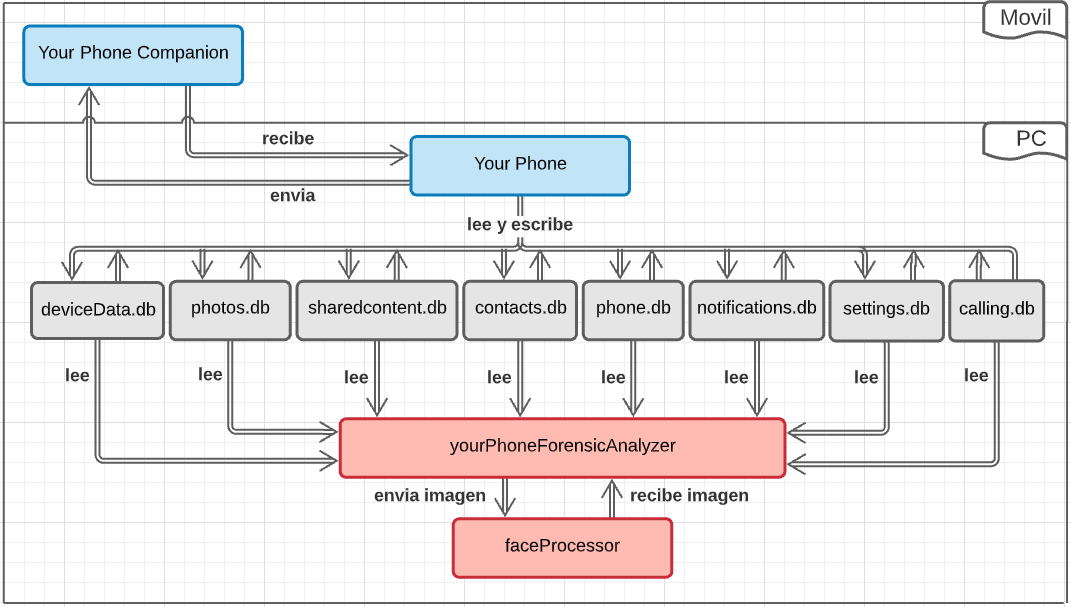


Fig. 15 Diagrama de flujo de información entre aplicación, programa y analizador

Una vez comprendido el flujo de datos y organizado la estructura de componentes el siguiente paso consistió en desarrollar el código. Esta etapa se dividió en dos fases; por un lado, la extracción y parseo de datos de índole numérica o textual y por otro el de obtención y reconocimiento facial de las imágenes.

#### 3.5.1 Parseo del formato

Para transformar los campos se estudió el formato y la casuística con la que se presentaban llamadas, mensajes y notificaciones.

Llamadas de teléfono

* Teléfono: Casa 1, Móvil 2, Trabajo 3, trabajo 4, Principal 5, Otros 6 y Escuela 7
* Tipo: Entrante 1, Saliente 2, Perdida 3, Desconocido 4, Declinada 5 y Bloqueada 6
* Estado: Leído 1, No leído 2

Sms – mms

* Estado: Leído 1, No leído 2
* Estado móvil: Recibido 1, No recibido 2

Timestamps

* Windows NT Time format: Utiliza el formato de tiempo Win32 filetime también llamado systemtime. Son marcas de tiempo de 18 dígitos que corresponden al número de intervalos de 100 nanosegundos desde el 1 de enero de 1601 UTC.

Notificaciones (JSON format)

* {"id": number,
* "key": string,
* "groupKey": string,
* "tag": string,
* "packageName": string,
* "appName": string,
* "isClearable": true/false,
* "isGroup": true/false,
* "isOngoing": true/false,
* "featureFlags": number,
* "platform": number,
* "version": number,
* "category": string
* "tickerText": string,
* "flags": number,
* "eventCount": number,
* "priority": number,
* "postTime": Windows NT time format,
* "timestamp": Windows NT time format,
* "notificationClass": number,
* "notificationActions":[

{

* + - "actionName":String,
    - "isActionInlineReply":true/false,
    - "actionIndex": number},
    - "template": string,
    - "text": string,
    - "title" string:
    - "showWhen":true/false,
    - "messages": string,
    - "senderNames" string:
    - "importance" string:

}

]

#### 3.5.2 Reconocimiento facial

El tratamiento de las imágenes se basa en dos modelos, OpenCV [29] y DeepFace [19]. El primero se utiliza para detectar rostros humanos, aislarlos y recortar un rectángulo alrededor suyo. El segundo se utiliza para aplicar reconocimiento facial sobre los rostros obtenidos. ¿Por qué se combinan ambos? Si bien es cierto que ambas librerías proporcionan por separado los medios para lograr las tareas de clasificación y comparación, existían ciertas limitaciones a la hora de implementarlas. Para OpenCV se observó que el modelo importado resultaba menos preciso a la par que menos versátil que de DeepFace. Esto provocaba que, a la hora de extraer las características identificativas de los rostros (encodings de 128 bits) y comparar mediante distancia euclidea, se obtuviese una mayor métrica del error. En contraposición DeepFace permitía corregir este error ajustando el modelo (VGG-Face, Facenet, Facenet512, OpenFace, DeepFace, DeepID, ArcFace, Dli") y la distancia a usar (coseno, euclidea, euclidean\_l2) por lo que resultaba más beneficioso utilizarlo como comparador. No obstante, a diferencia de DeepFace, OpenCV es capaz de aislar múltiples rostros dentro de una imagen, lo que permite separar las caras. Combinando ambas alternativas se logra identificar, aislar, recortar y evaluar los rostros de las imágenes presentes en Your Phone. Al tratarse de dos modelos trabajando conjuntamente puede ocurrir que primero, OpenCV, detecte y recorte un rostro, y después DeepFace no reconozca ninguna cara. En estos casos se descarta el recorte ya que, una imagen sin rostro reconocible es una imagen sobre la que no se pueden realizar comparaciones.

Sobre el reconocimiento facial se tomó la decisión de ofrecer tres servicios al analista:

* Agrupador de rostros.

Consiste en buscar y juntar rostros similares a partir del set de imágenes extraídas, con el objetivo de facilitar el estudio de los individuos identificados. Con ello se busca agrupar los rostros según individuo, es decir, juntar los rostros más similares. Para hacerlo se compara cada rostro con las caras detectadas, se compara con un umbral y se escogen, exportan y eliminan del listado aquellos que lo superen. El algoritmo se repite hasta haber eliminado la lista de caras a agrupar.

* Comparador de rostros.

Consiste en encontrar a partir de una cara rostros similares dentro del set de imágenes extraídas. La diferencia con el agrupador de rostros es que la tarea no trata de juntar individuos parecidos entre sí a base de excluir rostros ya evaluados, sino que busca aquellos individuos cuya similitud sea superior a un determinado umbral sin realizar descartes.

* Buscador de perfiles faciales.

Consiste en buscar y extraer aquellos rostros que encajen con una determinada descripción basada en edad, género, gesto y raza de un sujeto. Permite concatenar características para afinar las búsquedas. El programa localizará todos los rostros reconocibles y obtendrá un perfil aproximado para cada uno. La búsqueda devuelve todos los rostros coincidentes con los perfiles generados para cada perfil proporcionado.

La siguiente tabla recoge las variables que componen los CSVs de las búsquedas:

|  |  |  |
| --- | --- | --- |
| TABLA 3. - Ficheros CSV | | |
| Búsqueda | Campo | Valor |
| Teléfonos | Número | Formato E.164 de la UIT [30] |
| Perfiles faciales | Signo | Comparador <, <=, ==, !=, >=, o null (Null) para ignorar |
| Edad | Entero o null (Null) para ignorar |
| Genero | Hombre (Man), mujer (Woman) o null (Null) para ignorar |
| Gesto | Enfado (angry), miedo (fear), neutral (neutral), tristeza (sad), asco (disgust), felicidad (happy) y sorpresa (surprise) o null (Null) para ignorar |
| Raza | Asiático (asian), Blanco (white), árabe (middle eastern), indio (indian), latino (latino), negro (black) o null (Null) para ignorar |

Fig. 16 Ficheros CSV para buscar en YourPhoneForensicAnalyzer

### 3.6 Implementación de la solución

El primer paso hacia la implementación de yourPhoneForensicAnalizer consistió en desarrollar el control de ejecución. Como mínimo el script exige facilitar la ruta al directorio que contiene las bases de datos (-i o --inputPath entrada). De no hacerlo o en caso de suministrar una dirección incorrecta se aborta la ejecución. Si se desea también se puede añadir una ruta para dirigir su salida al directorio que se desee (-o o --outputPath salida).

El programa continúa evaluando los modos de ejecución proporcionados por el analista.

* Modos sin parámetros de entrada.
  + Modo ayuda: -h o –help
  + Modo verbose: -v o –verbose
  + Modo exportar imágenes: -e o –export
  + Modo agrupar caras similares: -gfi o –groupFaceImages
* Modos con parámetros de entrada.
  + Modo buscar mediante cara//s: -sfi –searchFaceImages *rutaImagenes*
    - *rutaImagenes :* directorio con la o las imágenes a buscar (cada imagen se considera como una búsqueda). Si el directorio no existe se notifica y aborta la ejecución
  + Modo buscar mediante perfiles faciales: -sfp –searchFaceProfiles *rutaCSV*
    - *rutaCSV :* fichero csv con el o los perfiles a buscar. Cada fila del csv se considera como una búsqueda. Si se proporciona una ruta incorrecta o un fichero con un formato incorrecto se finaliza la ejecución lanzando un mensaje de error.
  + Modo buscar mediante teléfonos: -spn –searchPhoneNumbers *rutaCSV*
    - *rutaCSV :* ficheros csv con el o los teléfonos a buscar. Cada fila del csv se considera como una búsqueda. Si se proporciona una ruta incorrecta o un fichero con formato incorrecto se finaliza la ejecución lazando un mensaje de error

El siguiente esquema ilustra las etapas que sigue el algoritmo del programa:

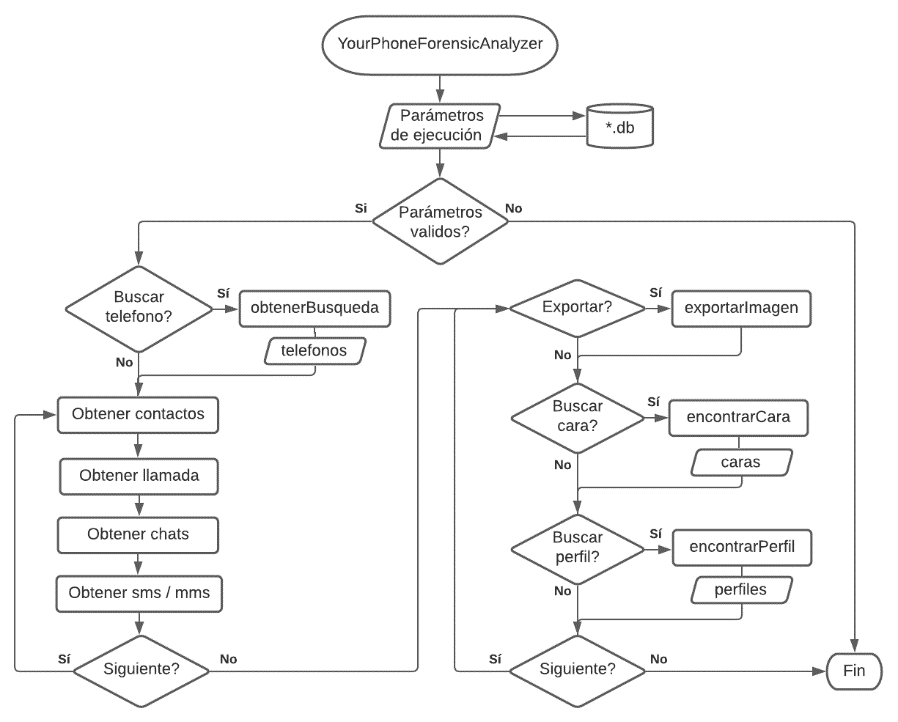


Fig. 17 Flujo de ejecución de YourPhoneForensicAnalyzer

Tal y como se muestra en la figura X, una vez se validan los parámetros de ejecución se procede a explorar las BBDD en busca de la información del usuario. Lo primero que hace el algoritmo es preparar la base de queries o consultas sql que obtienen los registros de las bases de datos. Todas las consultas a una misma tabla comparten un cuerpo común y constante (Select … FROM), por lo que esta se parte de la conslta se guarda en la clase constants mientras que la parte variable (WHERE…) se va modificando a lo largo del programa. Si se ha establecido el modo búsqueda el sondeo se limitará a los criterios de búsqueda proporcionados, es decir, no se realizará un rastreo en amplitud, sino que se impondrá el criterio de búsqueda sobre las instancias de la base de datos que cumplan con los parámetros proporcionados.

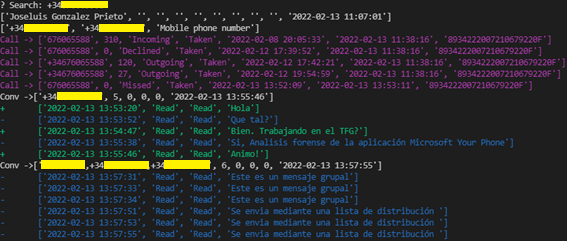
#### 3.6.1 Contactos, teléfonos, llamadas, sms y mms

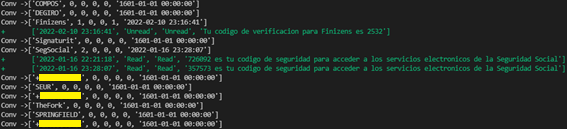
El algoritmo comienza por la agenda de contactos, de donde extrae el identificador de contacto. Para cada una de las entradas de la BBDD se buscan los teléfonos asociados al identificador y con estos se explora el registro de llamadas y a su vez se rastrean las conversaciones. Cuando un teléfono aparece en el registro de llamadas se muestra por pantalla sus características, duración, tipo, leído o no leído, fecha de comienzo y actualización e id del teléfono. Similarmente, si en un chat interviene uno de los teléfonos se muestra el número total de mensajes que colecciona, cuantos no han sido leídos desde el PC y cuantos no han sido leídos desde el móvil, si rcs está soportado, y el timestamp del último mensaje. Para facilitar la visualización de la salida sobre las llamadas se utiliza el color morado y sobre el chat se implementa un código de colores para cada mensaje, siendo verdes salientes y azules entrantes. Cada mensaje contiene quien lo envía, cuando lo envía y de nuevo cuantos no han sido leídos desde el PC y cuantos no han sido leídos desde el móvil. Cabe agregar que no todos los mensajes de la BBDD tienen relación con los teléfonos agregados a la agenda, algunos pueden ser conversaciones con teléfonos desconocidos, mensajes automáticos, spam, etc… Todos ellos se agrupan en una salida denominada “Unnasociated phones, calls, sms and mms” es decir, teléfonos, llamadas, sms y mms sin asociar. Por último, se muestran las aplicaciones instaladas en el dispositivo, nombre, versión, Favorite rank, y última fecha de actualización. Al finalizar se muestra un reporte de todas las operaciones:

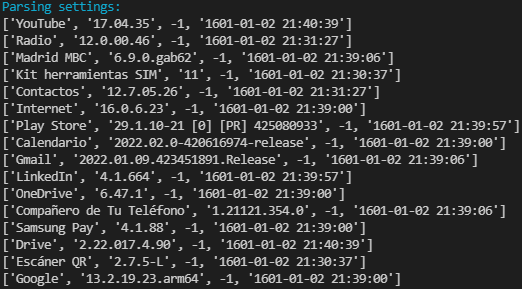
|-> Total contacts: |-> Total phone: |-> Total sms exchanged:

|-> Total calls: |-> Total sms chats:

Las figuras X Y Z muestran un ejemplo de la salida del algoritmo.







#### 3.6.2 Tratamiento de imágenes

Una vez concluido el parseo se obtienen la galería de imágenes de photos.db. Para ello, el algoritmo recorre todas las filas de la tabla *Media* y evalúa si los campos thumbnail y media se encuentran vacíos. El primero almacena una miniatura y el segundo una versión reducida del original, por lo que siempre que exista se preferirá la extracción del segundo ya que mantiene una resolución superior. Asimismo, se extrae el fondo de pantalla que guarda deviceData.db. Aquí cabe mencionar que la tabla de la que procede, wallpaper, no guarda ninguna información de la imagen original, por lo que el script le genera y adjudica un uuid como nombre y analiza la firma de archivo (file signature) de la cadena de bytes para adivinar su extensión.

|  |  |
| --- | --- |
| TABLA XXX – EXTENSIONES DE IMAGENES | |
| Extensión | Firma de archivo |
| .png | 0x89, 0x50, 0x4E, 0x47, 0x0D, 0x0A, 0x1A, 0x0A |
| .jpg | 0xFF, 0xD8, 0xFF, 0xE0 |
| .gif | 0x47, 0x49, 0x46, 0x38 |

Tabla 8 Firma de archivo según la extensión

A cada imagen disponible se le aplica detección de rostros con OpenCV. Este utiliza modelo zzzz y si la predicción es mayor de 0.5 el módulo recorta un rectángulo alrededor de los píxeles analizados. Dado que una imagen puede contener varias caras se le asocia internamente el nombre de la imagen al prefijo face\_N, siendo ‘N’ un numero entero que se va incrementando conforme se detectan caras en la imagen. A continuación, se estudia el recorte mediante DeepFace. Los modelos que utiliza DeepFace son redes neuronales convolucionales con entradas de tamaño estándar, por lo que la librería las normaliza antes de enviarlas al modelo. Después de la detección y la alineación añade píxeles negros de relleno para evitar deformar la entrada. Luego se propagan por el modelo y, o bien la librería produce una excepción al no detectar ningún rostro, o devuelve un diccionario de Python con las distintas categorías que identifican la cara. Finalmente, nombre, recorte del rostro y perfil son almacenados en memoria para posteriormente aplicar clustering y búsquedas. El clustering agrupa rostros del listado con un índice de similitud mayor o igual a 0.6, y va descartando en función de esto las instancias de la lista seleccionadas. Las búsquedas siguen el mismo razonamiento que el apartado anterior; se elabora un sondeo para cada criterio proporcionado, recogiendo los perfiles o las fotos y realizando el mismo proceso de análisis. Como resultado se obtiene otro listado de rostros reconocidos sobre el que comparar similitudes.

#### 3.6.3 Salida del programa

Por

### 3.7 Evaluación de la solución

#### 3.7.1 Pruebas realizadas para el análisis

#### 3.7.2 Batería de pruebas de YourPhoneForensicAnalyzer

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| tabla x.x - evaluacion de la aplicación | | | | |
| Tema | Descripción | Resultado esperado | Salida | OK |
| Input | Sin parametros | Aborta ejecución y produce un mensaje de error | Invalid input path. | ✔ |
| Parametros válidos: –input | Completa el algoritmo | - | ✔ |
| Parametros inválidos: –input  Directorio vacio | Lanza una excepción | ❌ Contacts, calls, sms and mms  ❌ Installed apps | ✔ |
| Parametros inválidos: –input  Falta alguna BBDD | Lanza una excepción y continua con las existentes | ❌ Contacts, calls, sms and mms | ✔ |
|  |  |  |  |
| verbose | Parametros válidos : –v | Muestra cada operación por pantalla | - | ✔ |
| output | Parametros válidos : –output  Directorio ya existente | Envia la salida al directorio ya existente | - | ✔ |
| Parametros válidos : –output  Directorio inexistente para –output | Envia la salida al directorio recién creado | - | ✔ |
| export | Parametros válidos : –export | Genera una carpeta denominada exported en el directorio de ejecución | - | ✔ |
| Parametros válidos : –output –export | Genera una carpeta denominada exported en el directorio de indicado por output | - | ✔ |
| CSVs | Parametros válidos :  –searchPhoneNumbers o –searchFaceProfiles | Se muestran exclusivamente las búsquedas | - | ✔ |
| Parametros inválidos : csv vacio  –searchPhoneNumbers o –searchFaceProfiles | No se muestra ningin resultado por pantalla | - | ✔ |
| Parametros inválidos : csv con header y sin body  –searchPhoneNumbers o –searchFaceProfiles | No se muestra ningin resultado por pantalla | - | ✔ |
| Parametros inválidos : csv incorrecto  –searchPhoneNumbers o –searchFaceProfiles | No se muestra ningin resultado por pantalla | ❌ Search phones | ✔ |
| Parametros inválidos : csv inexistente  –searchPhoneNumbers o –searchFaceProfiles | Aborta ejecución y produce un mensaje de error | Phone search csv provided doesn't exist. | ✔ |
| Imagenes | Parametros válidos : directorio con imágenes válidas  –searchFaceImages | Se muestra el numero de imagens y el numero de rostros reconocibles | - | ✔ |
| Parametros válidos : directorio sin imágenes  –searchFaceImages | Se muestra el numero de imagens y el numero de rostros reconocibles | - | ✔ |
| Parametros válidos : directorio inexistente  –searchFaceImages | Aborta ejecución y produce un mensaje de error | Face search folder doesn't exist. | ✔ |
|  |  |  |  | ✔ |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

La batería de pruebas

TABLA

## Conclusiones y trabajos futuros

Tal y como se puede comprobar, se han abarcado temáticas dentro de la ciberseguridad, el diseño de sistemas y la inteligencia artificial, lo que hace de del proyecto uno creativo y multidisciplinar. La finalidad, en cualquier caso, no ha sido la de centrarse únicamente en una de los ámbitos expuestos, sino que desde un primer momento se ha buscado ofrecer un estudio en amplitud de las características definitorias de Your Phone, así como un servicio distinguido por sus múltiples funcionalidades

Como conclusión señalar que el campo de la informática forense es un ámbito extenso, interdisciplinar y siempre en constante avance donde cada día surgen nuevas tecnologías y las que ya existen, cambian a lo largo del tiempo. Los retos a los que se enfrentan los analistas también cambian por lo que en este sector es de gran importancia mantener la discusión e investigación abierta, ya que retribuye en una comunidad actualizada y formada. Siguiendo estas líneas, el objetivo final de este trabajo consiste en expandir el conocimiento del que dispone la comunidad divulgando libremente tanto el estudio, como el programa desarrollado.

### 4.1 Objetivos cumplidos

### 4.2 Líneas futuras de trabajo

Adicionalmente es posible que en investigaciones de índole criminalista se traten imágenes sensibles como pornografía infantil, homicidios, violencia, etc… Por ello sería conveniente introducir medios para censurarlas total o parcialmente.

<https://docs.microsoft.com/es-es/windows-insider/apps/your-phone>

# Bibliografía

|  |  |
| --- | --- |
| [1] | Microsoft Corporation, «Microsoft,» [En línea]. Available: https://www.microsoft.com/en-us/p/your-phone/9nmpj99vjbwv#activetab=pivot:overviewtab. [Último acceso: 09 02 2020]. |
| [2] | S. Cordero, Análisis forense informático, Barcelona, 2015. |
| [3] | N. Panov, «Digital Forensics Tips&Tricks,» 2019. [En línea]. Available: https://habr.com/en/post/470952/.. [Último acceso: 01 12 2020]. |
| [4] | L. M. A. y. M. F. y. J. V. S. Patricio Domingues, «Digital forensic artifacts of the Your Phone application in Windows 10,» *elsevier,* vol. 30, nº 1742-2876, pp. 32-42, 2019. |
| [5] | L. M. A. y. M. F. Patricio Domingues, «Microsoft’s Your Phone environment from a digital forensic perspective,» *elsevier,* vol. 38, nº 2666-2817, 2021. |
| [6] | R. L. Rivera, «peritoit,» [En línea]. Available: https://peritoit.com/delitos-informaticos/. [Último acceso: 01 01 2022]. |
| [7] | E. Peris, «informaticajudicial,» [En línea]. Available: https://informaticajudicial.es/normativa/. [Último acceso: 09 02 22]. |
| [8] | B. Betsy Mikalacki, «How much does digital forensic services cost,» Vestige, [En línea]. Available: https://www.vestigeltd.com/thought-leadership/digital-forensic-services-cost-guide-vestige-digital-investigations/. [Último acceso: 2022 02 09]. |
| [9] | glassdoor, «glassdoor,» [En línea]. Available: https://www.glassdoor.es/Sueldos/madrid-programador-junior-sueldo-SRCH\_IL.0,6\_IM1030\_KO7,25.htm?clickSource=searchBtn/. . [Último acceso: 01 01 2022]. |
| [10] | glassdoor, «glassdoor,» [En línea]. Available: https://www.glassdoor.es/Sueldos/madrid-profesor-universitario-sueldo-SRCH\_IL.0,6\_IM1030\_KO7,29.htm?clickSource=searchBtn. [Último acceso: 01 01 2022]. |
| [11] | Microsoft, «Supported devices for Your Phone app experiences,» [En línea]. Available: https://support.microsoft.com/en-us/topic/supported-devices-for-your-phone-app-experiences-cb044172-87aa-9e41-d446-c4ac83ce8807. [Último acceso: 09 02 2022]. |
| [12] | Python, «GitHub,» [En línea]. Available: https://github.com/python/cpython/blob/main/Lib/io.py. [Último acceso: 09 02 2022]. |
| [13] | Python, «Python Documentation,» [En línea]. Available: https://docs.python.org/3/library/time.html. [Último acceso: 09 02 2022]. |
| [14] | Python, «GitHub,» [En línea]. Available: https://github.com/python/cpython/blob/main/Lib/datetime.py. [Último acceso: 09 02 2022]. |
| [15] | Python, «GitHub,» [En línea]. Available: https://github.com/python/cpython/blob/main/Lib/os.py. [Último acceso: 09 02 2022]. |
| [16] | Python, «GitHub,» [En línea]. Available: https://github.com/python/cpython/blob/main/Python/sysmodule.c. [Último acceso: 09 02 2022]. |
| [17] | Python, «GitHub,» [En línea]. Available: https://github.com/python/cpython/blob/main/Lib/uuid.py. [Último acceso: 09 02 2022]. |
| [18] | A. C. a. Contributors., «Python Imaging Library,» [En línea]. Available: https://github.com/python-pillow/Pillow/ . [Último acceso: 09 02 2022]. |
| [19] | S. I. y. O. A. Serengil, «GitHub,» [En línea]. Available: https://github.com/serengil/deepface. [Último acceso: 09 02 2022]. |
| [20] | G. Bradski, «GitHub,» [En línea]. Available: https://github.com/opencv/opencv/wiki/CiteOpenCV. [Último acceso: 09 02 2022]. |
| [21] | S. J. Bethard, «GitHub,» [En línea]. Available: https://github.com/python/cpython/blob/3.10/Lib/argparse.py. [Último acceso: 09 02 2022]. |
| [22] | K. Lepa, «GitHub,» [En línea]. Available: https://github.com/hfeeki/termcolor. [Último acceso: 09 02 2022]. |
| [23] | M. Singh, «GitHub,» [En línea]. Available: https://github.com/manrajgrover/halo. [Último acceso: 09 02 2022]. |
| [24] | Python, «GitHub,» [En línea]. Available: https://github.com/python/cpython/blob/main/Lib/csv.py. [Último acceso: 09 02 2022]. |
| [25] | G. Häring, «GitHub,» [En línea]. Available: https://github.com/python/cpython/blob/main/Doc/library/sqlite3.rst. [Último acceso: 09 02 2022]. |
| [26] | Numpy, «GitHub,» [En línea]. Available: https://github.com/numpy/numpy. [Último acceso: 09 02 2022]. |
| [27] | Secret Labs, «GitHub,» [En línea]. Available: https://github.com/python/cpython/blob/main/Lib/re.py. [Último acceso: 09 02 2022]. |
| [28] | J. Friedl, «Jeffrey's Image Metadata Viewer,» [En línea]. Available: http://exif.regex.info/exif.cgi. [Último acceso: 21 12 2022]. |
| [29] | K. Bhanot, «GitHub,» [En línea]. Available: https://github.com/kb22/Create-Face-Data-from-Images. [Último acceso: 11 02 2022]. |
| [30] | Union Internacional de telecomunicaciones, «itu,» [En línea]. Available: itu.int/rec/T-REC-E.164/es. [Último acceso: 04 01 2022]. |
| [31] | International Society of Forensics Computer Examiners, «isfc,» [En línea]. Available: https://www.isfce.com/ethics2.htm. [Último acceso: 05 01 2022]. |

https://www.flaticon.es/iconos-gratis/fotografia

https://www.flaticon.es/iconos-gratis/telefono

https://www.flaticon.es/iconos-gratis/contacto

https://www.flaticon.es/iconos-gratis/sms

https://www.flaticon.es/iconos-gratis/wifi

https://www.flaticon.es/iconos-gratis/almacenamiento

https://www.flaticon.es/iconos-gratis/mapa

https://www.flaticon.es/iconos-gratis/mas

https://www.flaticon.es/iconos-gratis/bluetooth

<https://icons8.com/icons/set/program>

# Anexo

[] Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

[www.boe.es/aeboe/consultas/bases\_datos/doc.php?id=BOE-A-2007-18243](http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-2007-18243)

[] Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil (LEC).

[www.boe.es/aeboe/consultas/bases\_datos/doc.php?id=BOE-A-2000-323](http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-2000-323)

[] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).

[www.boe.es/aeboe/consultas/bases\_datos/doc.php?id=BOE-A-1999-23750](http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-1999-23750)

[] Ley Orgánica 19/1994, de 23 de diciembre, de protección a testigos y peritos en causas criminales.

[www.boe.es/aeboe/consultas/bases\_datos/doc.php?id=BOE-A-1994-28510](http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-1994-28510)

[] Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de Protección de las Infraestructuras Críticas (PIC).

[www.boe.es/diario\_boe/txt.php?id=BOE-A-2011-8849](http://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-8849)

[] Orden PRE/2740/2007, de 19 de Septiembre, por la que se regula el Reglamento de Evaluación y Certificación de Seguridad de las Tecnologías de la Información

[www.boe.es/boe/dias/2007/09/25/pdfs/A38781-38805.pdf](http://www.boe.es/boe/dias/2007/09/25/pdfs/A38781-38805.pdf)

[] Protocolo Adiccional, 28 Enero de 2003, al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos.

[www.gdt.guardiacivil.es/webgdt/media/Legislacion/Protocolo\_adicional\_convencion\_cibercrimen.pdf](http://www.gdt.guardiacivil.es/webgdt/media/Legislacion/Protocolo_adicional_convencion_cibercrimen.pdf)

[] BOE 14221/ 2010, de 17 Septiembre, Instrumento de Ratificación del Convenio de la Ciberdelincuencia, redactado en Budapest el 23 de noviembre de 2001.

[www.boe.es/boe/dias/2010/09/17/pdfs/BOE-A-2010-14221.pdf](http://www.boe.es/boe/dias/2010/09/17/pdfs/BOE-A-2010-14221.pdf)

[] Real Decreto Legislativo 1/1996, de 2 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

[www.boe.es/aeboe/consultas/bases\_datos/doc.php?id=BOE-A-1996-8930](http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-1996-8930)

[] Ley 11/2011, de 20 de mayo, de reforma de la Ley 60/2003, de 23 de diciembre, de Arbitraje y de regulación del arbitraje institucional en la Administración General del Estado.

[www.boe.es/aeboe/consultas/bases\_datos/doc.php?id=BOE-A-2011-8847](http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-2011-8847)

[] Ley Orgánica 5/2011, de 20 de mayo, complementaria a la Ley 11/2011, de 20 de mayo, de reforma de la Ley 60/2003, de 23 de diciembre, de Arbitraje y de regulación del arbitraje institucional en la Administración General del Estado para la modificación de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

[www.boe.es/aeboe/consultas/bases\_datos/doc.php?id=BOE-A-2011-8846](http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-2011-8846)