

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

Lugar y fecha de presentación prevista

   
*[Incluir en el caso del interés de su publicación en el archivo abierto]*

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

# Resumen

**Palabras clave:**

Trabajo intelectual; Investigación científica

# Dedictoria

A MR potato

# Índice de contenidos

[Resumen III](#_Toc94601597)

[Dedictoria V](#_Toc94601598)

[Índice de contenidos VII](#_Toc94601599)

[Índice de figuras X](#_Toc94601600)

[Índice de tablas XII](#_Toc94601601)

[Lista de abreviaturas 1](#_Toc94601602)

[Introducción 3](#_Toc94601603)

[1.1 Estructura 3](#_Toc94601604)

[1.2 Resumen 4](#_Toc94601605)

[1.3 Motivación 4](#_Toc94601606)

[1.4 Metodología de trabajo 5](#_Toc94601607)

[1.5 Objetivos 7](#_Toc94601608)

[Estado del arte 8](#_Toc94601609)

[2.1 Definiciones 8](#_Toc94601610)

[2.2 Recursos externos 8](#_Toc94601611)

[2.3 Marco regulador 9](#_Toc94601612)

[2.4 Entorno socio-económico 14](#_Toc94601613)

[Desarrollo del proyecto 16](#_Toc94601614)

[3.1 Planificación 16](#_Toc94601615)

[Presupuesto 16](#_Toc94601616)

[3.3 Tecnologías empleadas 19](#_Toc94601617)

[3.4 Análisis 24](#_Toc94601618)

[3.5 Diseño de la solución 30](#_Toc94601619)

[3.6 Evaluación de la solución 31](#_Toc94601620)

[Conclusiones y trabajos futuros 31](#_Toc94601621)

[4.1 Objetivos cumplidos 31](#_Toc94601622)

[4.2 Líneas futuras de trabajo 31](#_Toc94601623)

[Bibliografía 32](#_Toc94601624)

# Índice de figuras

# Índice de tablas

# Lista de abreviaturas

|  |  |
| --- | --- |
| BBDD | Bases de datos |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## 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: “Análisis forense de la aplicación Microsoft Your Phone”, un estudio exhaustivo de la estructura, comportamiento y artefactos de este programa.

### 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

### 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.
* 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 para este propósito.

En resumen, me he propuesto estudiar desde la perspectiva forense la aplicación Microsft Your Phone ya que aparte de aportar las ventajas previamente expuestas 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.

**Autopsy**. Es una interfaz gráfica para el análisis forense informático, mediante herramientas de líneas de comandos. El cual permite a los investigadores lanzar auditorías forenses no intrusivas en los sistemas a investigar. Estos análisis se centran en análisis genérico de sistemas de archivos y líneas temporales de ficheros. Se puede analizar los discos de Windows y UNIX y sistemas de archivos (NTFS, FAT, UFS1 / 2, Ext2 / 3).

<https://www.ecured.cu/Autopsy>

### 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. 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 ha encontrado una publicación que realice este análisis. En Digital forensic artifacts of the Your Phone application in Windows 10 los autores Patricio Domingues, Miguel Frade, Luis Miguel Andrade y Joao Victor Silva analizan las versiones 1.0.20453 y 3.4.4 de Your Phone para Windows 10's y la app para Android Your Phone Companion respectivamente. El trabajo es realmente revelador ya que en gran medida presenta como se organiza la aplicación en su totalidad y como esta almacena los datos del usuario. Este trabajo xxx Además, su investigación propone un script de Python diseñado para ejecutar en Autopsy.

El estudio resulta muy completo y sus autores consiguen cumplir con algunos de los objetivos que este trabajo persigue, pero no obstante deja otros fuera. Algunos de los aspectos que la publicación no resuelve definitivamente son la Monitorización de procesos, análisis del registro de Windows, XXX.Sobre el primero comentar que….

Otro problema adicional son las nuevas actualizaciones**.** La aplicación ha continuado actualizándose, 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.

### 2.3 Marco regulador

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

#### 2.3.1 La legislación y normativa legal.

https://peritoit.com/delitos-informaticos/

El Convenio de la Ciberdelincuencia, 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.

https://informaticajudicial.es/normativa/

<https://informatico-forense-madrid.es/que-es-perito-informatico>

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)

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

*Entorno socio-económico El TFG deberá deberá incorporar el desarrollo de los siguientes apartados:*

*• Presupuesto de la elaboración del TFG.*

*• Impacto socio-económico (impacto económico, social, medioambiental, ético, etc.)*

*¿Por aquí bien?*

El impacto económico resulta difícil de estimar dado el contexto. No obstante, se podría esperar que la aplicación del trabajo desarrollado trajese algunas mejoras en el desempeño de los analistas. Según vestigeltd 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.

Las posibles aplicaciones del programa software desarrollado no se limitan exclusivamente al contexto de investigaciones forenses. 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 categorizador de rostros.

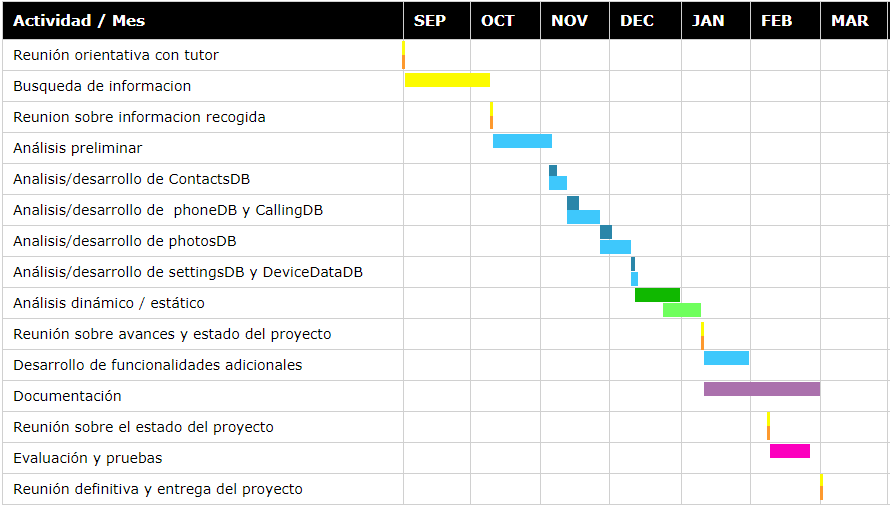
En cuanto a las implicaciones éticas cabe mencionar que al tratarse de un programa destinado a descubrir y trabajar con datos personales (conversaciones, llamadas, imágenes) se debe mantener estricta confidencialidad.

## Desarrollo del proyecto

### 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:



Puesto que el proyecto se compagina con la beca de estudios descrita previamente 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 y 33.862 € 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:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 € |

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

* **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.

|  |  |  |  |
| --- | --- | --- | --- |
| Presupuesto para 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 |
| File:APK format icon (2014-2019).png - Wikimedia Commons | Android | 5.1.1 / 11 | Gratuito |
| Microsoft Your Phone for Android: What is it and how does it work? |  Android Central | Your phone companion | 1.21113.85.0 | Gratuito |
| Sysinternals Suite Alternativas y software similar - ProgSoft.net | Sysinternals |  | Gratuito |
| ProcDOT&#39;s Home - Online Documentation | procDot | 1.22 | 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€ |

* **Herramientas hardware:** el equipo y dispositivos sobre los que se ha trabajado o realizado pruebas han sido un portátil DELL Latitude E7270 de 1.179,27 €, XXX móviles Samsung A20e, XXX valorados en 145,20 € y 124 € respectivamente. 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 del teléfono Samsung J3 no se ha imputado gasto ya que el uso ha sido infimo.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Presupuesto para herramientas hardware | | | | | |
| Recurso | Precio  € | Horas de uso | Horas de vida útil | % uso | Subtotal |
| DELL E7270 | 1.179,27 € | 310 h | ~ 1.825 h | ~16% | ~190 € |
| Samsung A20e | 145.2 € | 125 h | ~ 1.825 h | ~7% | ~10 € |
| Samsung J3 | 124 € | ~ 0 h | ~ 1.825 h | ~ 0.0% | 0 € |
| Coste total | | | | | 200€ |

El presupuesto total del proyecto es:

|  |  |
| --- | --- |
| 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:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Características técnicas de los dispositivos empleados | | | | | | |
| Tipo | Modelo | Conexión | Pantalla | CPU | Memoria | Discos |
| Archivo:Dell Logo.svg - Wikipedia, la enciclopedia libre  PC | DELL Latitude E7270 | Ethernet, Bluetooth, Wi-Fi | 12.5’’  1366 x 768 pixeles | i5-6300 2 Cores  2.4 GHz | DDR4-SDRAM  16 GB  2133 MHz | SSD  128 GB |
| Rubrin Shopping – Indian Most trusted shopping store  Móvil | Samsung A20e  SM-A202 | Bluetooth, Wi-Fi, GSM 4G / 3G / 2G, NFC | 5.8’’  720 x 1560 píxeles | Exynos  7884 2 Cores  1.6 GHz | LPDDR4  3 GB | eMMC 5.1  32 GB  microSD  1 TB |
| Rubrin Shopping – Indian Most trusted shopping store  Móvil | Samsung J3  SM-J320FN | Bluetooth, Wi-Fi, GSM 4G / 3G / 2G, NFC | 5”  720 x 1280 píxeles | ARM Cortex A7, 4 Cores  1.5 GHz | LPDDR3  1.5 GB | eMMC 4.5  8 GB  microSD  4 GB |
| Rubrin Shopping – Indian Most trusted shopping store  Móvil | Samsung | Bluetooth, Wi-Fi, GSM 4G / 3G / 2G, NFC |  |  |  |  |

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*: 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).

https://github.com/python/cpython/blob/main/Lib/io.py

* + *time*: librería diseñada para manipular formatos fechas, horas, minutos y segundos. Necesaria para recoger el tiempo de ejecución del programa

https://docs.python.org/3/library/time.html

* + *datetime* librería diseñada para manipular fechas, Necesaria para parsear los timestamps en formato LDAP a dd,mm,yyyy – h,m,s

https://github.com/python/cpython/blob/main/Lib/datetime.py

* + *os*: 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…)

https://github.com/python/cpython/blob/main/Lib/os.py

* + *sys:* 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())

https://github.com/python/cpython/blob/main/Python/sysmodule.c

* + *uuid:* 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.

https://github.com/python/cpython/blob/main/Lib/uuid.py

Imágenes

* + *PIL*: Python Imaging Library, también abreviada como Pillow, es una biblioteca diseñada en colaboración por Alex Clark https://github.com/python-pillow/Pillow/ orientada a abrir, manipular y guardar imágenes en distintos formatos. Necesaria para operar con las imágenes.
  + *Deepface*: es un framework ligero de reconocimiento facial y análisis de atributos faciales diseñado por Serengil, Sefik Ilkin and Ozpinar, Alper. https://github.com/serengil/deepface Necesario para detectar y comparar rostros.
  + *Cv2*: consiste en una librería de OpenCV de Bradski, G para Python. Permite manipular imágenes y transformar sus formatos.

https://github.com/opencv/opencv/wiki/CiteOpenCV

* Consola
  + *argparse*: 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)

https://github.com/python/cpython/blob/3.10/Lib/argparse.py

* + *Termcolor*: 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 azul y recibidos verde, errores rojo, etc…)

https://github.com/hfeeki/termcolor

* + *Halo*: 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.

https://github.com/manrajgrover/halo

* Ficheros
  + *csv*: consiste en una librería para leer, escribir o maniplular ficheros csv. Permite exportar el contenido en formato separado por comas

https://github.com/python/cpython/blob/main/Lib/csv.py

* + *Sqlite3* 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.

https://github.com/python/cpython/blob/main/Doc/library/sqlite3.rst

* Matemática
  + *Numpy:* librería diseñada para cálculo numérico y análisis de datos. Necesario para el cálculo matricial en el que se basa el procesamiento de imágenes

https://github.com/numpy/numpy

* Expresiones regulares
  + *RE*: 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)

https://github.com/python/cpython/blob/main/Lib/re.py

### 3.4 Análisis

#### 3.4.1 Aspectos generales sobre Microsoft 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.



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

|  |  |  |  |
| --- | --- | --- | --- |
| **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 a |
| 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 telefono y aplicaciones reqieren un dispositivo compatible

|  |  |  |  |
| --- | --- | --- | --- |
| **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 | | |

#### 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, entradas y salidas de red, 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. Posteriormente se utilizó procdot, un servicio de diagramado para ilustrar gráficamente y así facilitar el estudio de las operaciones capturadas por procmon. Para cargar en procdot la monitorización de procmon es necesario configurar los siguientes parámetros:

PROCMON PROCDOT

Una vez hecho se realzó el siguiente estudio:

|  |  |  |  |
| --- | --- | --- | --- |
| **Procmon - Procdot** | | | |
| n | Descripción | Conclusión | Hallazgos |
| 1 | Instalación del programa |  |  |
| 2 | Llamada telefónica |  |  |
| 3 |  |  |  |
| 4 |  |  |  |

#### 3.4.3 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 las bases de datos de Your Phone. Ambas revelaron que: (REVISAR EXPRESION)

En primer lugar, la agenda se almacena en *contactsDB,* 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 adicional 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. Esto parece indicar que su función es la de salvaguardar y actualizar el contenido a medida que la aplicación agrega o elimina contactos. Algo mas?

En segundo lugar, el registro de llamadas, que se encuentra en *call\_history* en *callingDB*. 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 PAPER permanecían al día en la nueva versión de la aplicación. El resto de campos o bien se repiten por defecto o son directamente nulos.

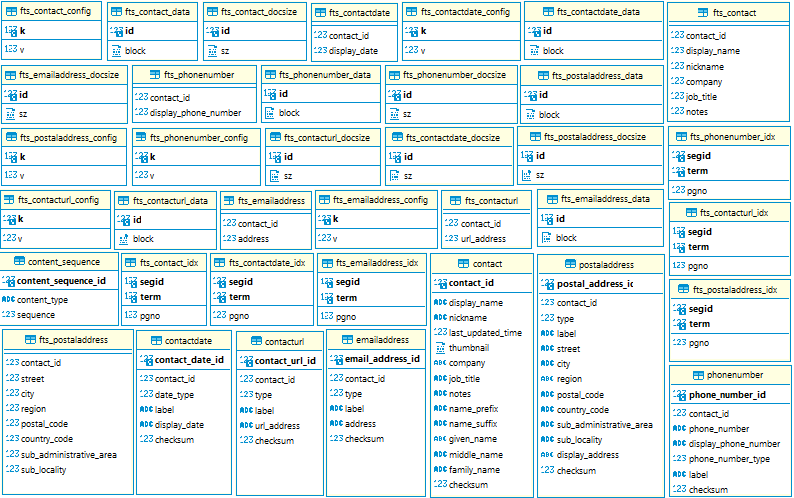
En tercer lugar, tenemos phoneDB, donde se almacena la información del dispositivo. Por un lado, en *subscription,* se tiene el contrato de telecomunicaciones (teleoperadora, país, sim, características de la tarifa, condiciones de roaming, mensajes multimedia, rcs y limitaciones en el envío). Sobre la 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, settingsDB, 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, pero sí de aplicaciones instaladas y de estas la información relevante es nombre y versión. El resto 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.

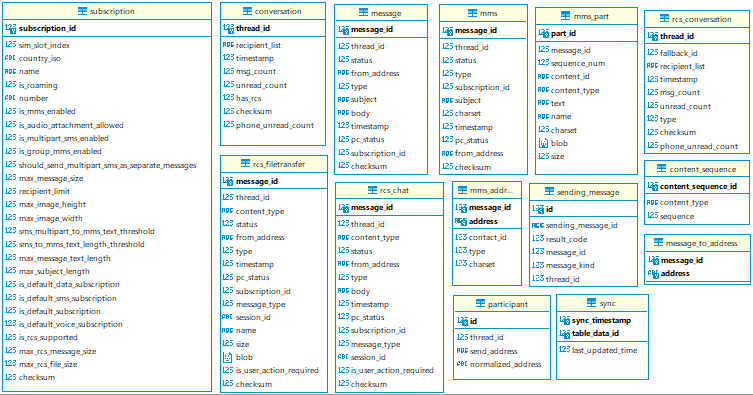
En quinto lugar, photosDB y deviceDataDB, dos bases de datos que contienen la galería de imágenes de Your Phone (*media, photos*) y el fondo de pantalla del teléfono móvil (*wallpaper*). Ambas BBDDs guardan como blob (cadena de bytes) las imágenes en sus registros. PhotosDB también agrega información 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.

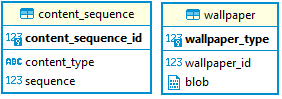
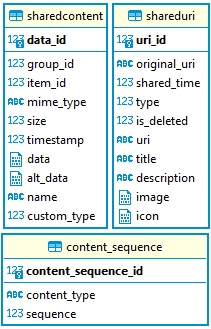
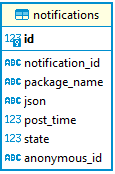
En sexto puesto, notificationsDB, que almacena los avisos que las aplicaciones envían al usuario del teléfono. En un primer momento se creyó que se trataría de una fuente muy valiosa de datos, pero pronto se desestimó ya que el análisis mostró que tan solo se almacena la cola de notificaciones del teléfono. 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. No se descarta que exista algún registro en unallocated space ….

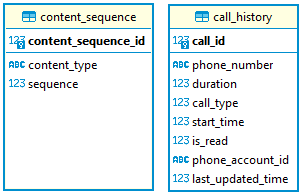
**Bases de datos de Your Phone**

ContactsDB

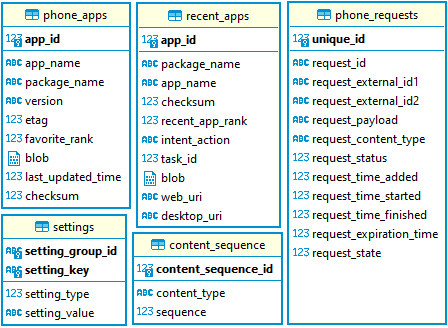
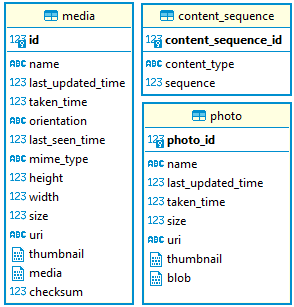
PhoneDB



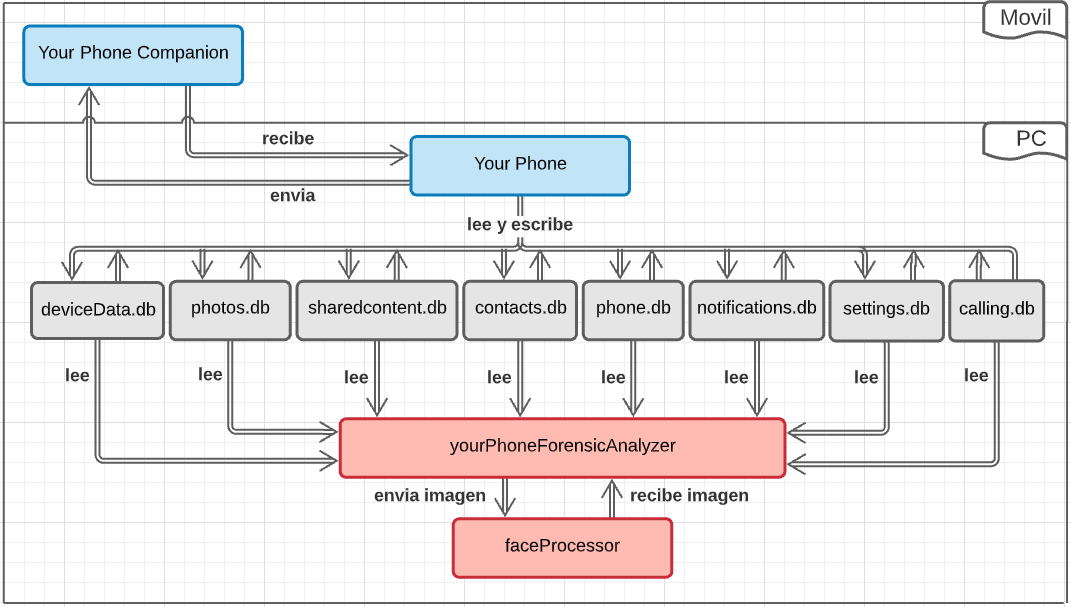
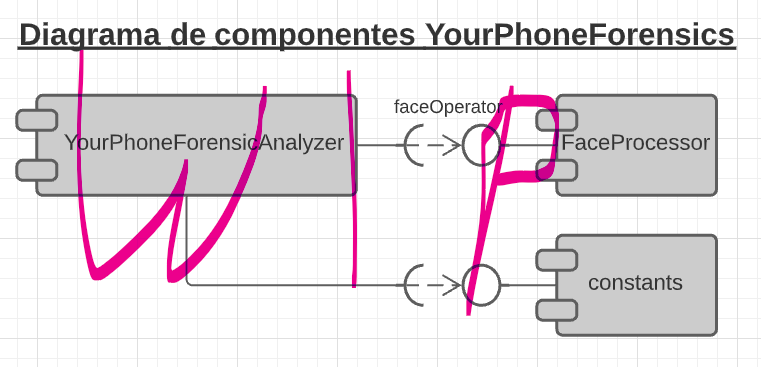
deviceDataDB sharedContentDB notificationsDB

callingDB

settingsDB photosDB

### 3.5 Diseño de la solución

Una vez conocida la forma en que el programa almacena la información se procedió a desarrollar la aplicación para extraerla y estudiarla. AAAA: Diagrama de flujo de la información

Este diagrama muestra cómo la información viaja entre app y programa de Your Phone así como el script recoge los artefactos para analizar su contenido. Se trata de una vista adicional del sistema que en ningún caso representa la estructura de clases. Sirve como guía para comprender cómo fluyen los datos una vez el usuario comienza a interactuar con el teléfono y el programa.

Una vez obtenidos el problema se organizó el en dos partes; 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 lo

#### 3.5.2 Reconocimiento facial

El tratamiento de las imágenes se basa en dos modelos, OpenCV y DeepFace. 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 DeepFace. Esto provocaba que, a la hora de extraer las características identificativas de los rostros (encodings de 128bits) 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 ninguno. En estos casos se descarta ya que una imagen no se puede realizar comparaciones con imágenes cuyo rostro no es reconocible.

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 mas similares. Para hacerlo se utiliza la AMPLIAR

* Comparador de rostros.

Consiste en, a partir de una cara, encontrar rostros similares en el set de imágenes extraídas. La diferencia con el agrupador de rostros es que la tarea no trata de juntar individuos parecidos entre si, sino que busca aquellos individuos cuya similitud sea superior a un determinado umbral AMPLIAR

* Buscador de perfiles faciales.

Consiste en buscar y extraer aquellos rostros que encajen con una determinada descripción de un sujeto.

|  |  |  |
| --- | --- | --- |
| **Perfiles faciales** | | |
| Edad | Entero | Signo de comparación {<,<=,==,!=,>=,>} |
| Genero | Hombre (Man) y mujer(Woman) | |
| Expresión facial | Enfado (angry), miedo (fear), neutral (neutral), (tristeza) sad, (asco) disgust, (felicidad) happy y sorpresa (surprise) | |
| Raza | Asiático (asian), Blanco (white), árabe (middle eastern), indio (indian), latino (latino) y negro(black) | |

### 3.6 Implementación

El primer paso hacia la implementación consistió en preparar la queries o consultas sql que obtienen los registros de las bases de datos. Todas las consultas a una misma tabla comparten un cuerpo común (Select … FROM) por lo que la parte constante se guarda en el fichero constants y la parte variable (WHERE…) se va modificando a lo largo del programa

### 3.7 Evaluación de la solución

La batería de pruebas

## Conclusiones y trabajos futuros

### 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] P. Domingues, L. M. Andrade, and M. Frade, “Microsoft’s Your Phone environment from a digital forensic perspective,” vol. 38, p. 301177, 2021, doi: https://doi.org/10.1016/j.fsidi.2021.301177.

[2] P. Domingues, M. Frade, L. M. Andrade, and J. V. Silva, “Digital forensic artifacts of the Your Phone application in Windows 10,” vol. 30, pp. 32–42, 2019, doi: https://doi.org/10.1016/j.diin.2019.06.003.

[] «Glassdor» [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 2022].

[] «Glassdor» [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 2022].

[] «International Society of Forensics Computer Examiners» [En línea]. Available: https://www.isfce.com/ethics2.htm [Último acceso: 01 2022].

[] «elvidence» [En línea]. Available: <https://www.elvidence.com.au/home/rates/#:~:text=FLAT%2DFEE%20PRICING&text=From%20our%20experience%2C%20the%20typical,increase%20this%20cost%20by%2030%25>. [Último acceso: 01 2022].

<https://intercompras.com/p/laptop-dell-latitude-e7270-intel-core-i5-6300u-ghz-8gb-256gb-ssd-graficos-110266>

<https://www.movilcelular.es/especificaciones/samsung/galaxy-a20e/sm-a202fds/>

<https://www.dell.com/community/Pc-de-Escritorio-General/Vida-util/td-p/5295179>

<https://www.muycomputer.com/2021/09/10/vida-util-de-un-smartphone/#:~:text=Gama%20baja%20y%20media%20baja,de%20OS%20y%20de%20Seguridad>.

<https://blog.masmovil.es/cuantos-anos-dura-un-movil/>

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>

[] 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)