# Anexo I. English summary

## Introduction

This document contains the final year project developed by Lucas González de Alba, student at Universidad Carlos III de Madrid. This research project analyzes from a digital forensics standpoint, the structure, behavior and artifacts created by Microsoft’s Your Phone application.

### 1.2 Abstract

Microsoft’s Your Phone is a service which facilitates the user access to phone devices by integrating its notifications, messages, photos and calls directly into Windows. All this data can have huge value on forensic investigation, so the work we are presenting today will analyze Your Phone app on the look for digital artifacts. The project began with a large research of existing knowledge; that is articles, publications, blogs, forums...etc. After a brief overview of the app's behavior, several digital samples were collected. With this in mind, a formal study of the app's behavior was conducted using process monitoring. Then both format and structure from any relevant system artifact was analyzed. With the obtained knowledge, a Python script to facilitate extraction and search analysis was developed. This program parses call logs, sms and mms messages, settings and a list of installed applications and supports facial recognition. The identity verification module uses OpenCV and DeepFace and its objective is to detect one or multiple faces within an image, allow for attributes comparison and support search for similarities based on a descriptive profile. A hybrid between OpenCV and DeepFace was chosen for its favorable results and versatility. Finally, the quality of the developed software was evaluated using a large test set.

### 1.3 Motivation

This project was first conceived as the author’s personal research on analysis techniques used in cybersecurity and computer forensics. But, since it quickly grew in length and complexity, a larger goal was set. Why computer forensics? Because, unfortunately, it is a subject that is not taught in the computer science degree, but offers transversal knowledge to many areas such as cybersecurity, software engineering and data science.

The analysis of Microsft’s Your Phone application can offer very positive benefits to the forensic community. A few are:

* Exposing the formal study of the structure and artifacts by determining what information can be extracted from the artifacts of the application.
* Creating a link mobile and computer environment through Your Phone.
* Automating extraction of the images stored by the system. Avoid the tedious and repetitive task of searching, selecting and saving each image in the application.
* Enabling "live" evidence analysis

In summary, studying Microsoft’s Your Phone application from a forensic perspective not only provides the advantages outlined above, but it’s also offers a unique opportunity to develop an innovative research with substantial work.

### 1.4 Work methodology

The chapter is divided in two section, analysis and development.

The first stage, analysis, was dedicated to the study of the program behavior. In order to acquire as much information as possible about the program behavior, an incremental examination based on the following phases was established:

* Preliminary phase: the working environment and the analysis tools are set up.
* Functionalities exploration: getting acquainted with the app’s capabilities.
* Dynamic analysis: real time monitoring to identify and collect system artefacts.
* Static analysis: study the main digital traces and artifacts previously discovered.

The second stage, development, focused on the implementation of a software solution dedicated to facilitating access to the previously analyzed information.

* Requirements identification: capturing the needs and constraints of the problem.
* Design: study and establish the best possible software architecture
* Implementation: develop the program for the selected architecture
* Testing: evaluate results and verify compliance with the requirements.

### 1.5 Goals

This chapter sets out the main goal of the work and establishes the various specific objectives that comprise it.

Primary goals:

1. Analyze and report Your Phone’s artifacts identifying any forensically valuable information they might contain.
2. Implement a software solution to collect, parse and export the information presented by the Microsoft Your Phone application

Secondary goals

1. Extract the multimedia content of the application and apply face detection and categorization
2. Implement a facial profile search system. Develop a software tool to locate people given the main characteristics of their face.
3. Evaluate the correctness and accuracy of the software solution that was developed
4. Evaluate if there exists content safeguarded by the application
5. Extract deleted content from the application

# State of the art

### External resources

In the field of computer forensics and cybersecurity, it is common to find publications related to the study and monitoring of free, corporate and malicious software programs. Such studies usually apply both static and dynamic analysis and usually involve hash analysis, carving, network monitoring, process and thread recognition, Windows registry tracing and artifact examination. As far as Microsoft Your Phone is concerned, only three publications have been found. These are Digital Forensics Tips&Tricks: "Your Phone" app Forensics [3], Digital forensic artifacts of the Your Phone application in Windows 10 [4] and its subsequent review Microsoft's Your Phone environment from a digital forensic perspective [5]. The first came just after Windows 10’s Insider Preview Build 18999 (20H1) was released and it briefly reviewed the functionalities of the newly introduced application. By contrast, in the second article the authors Patricio Domingues, Miguel Frade, Luis Miguel Andrade and Joao Victor Silva analyze versions 1.0.20453 and 3.4.4.4 of Windows 10's Your Phone and Android’s app Your Phone Companion respectively. In addition, they proposed a Python script designed to run on Autopsy. Finally, the third article examines updates 1.21011.127.0 (Windows) and 1.21021.81.0 (android) and follows the previous line of development, extending some aspects that were left out of the previous study and expanding the functionalities of the proposed program. Compared to the first analysis proposed by Panov the last two publications really expand the knowledge and explain with greater detail how the application was organized and how it stored the user's data.

Overall, these three studies manage to meet some of the objectives of this paper, but nevertheless they leave others out. Some of the technical issues they do not solve are process monitoring, Windows registry analysis and description of artifact configurations, and that is without adding the challenge of new updates. The application has continued to renew itself, including new features such as the expansion of its gallery, instant messaging, and screen sharing which renders some of the previous work obsolete. This phenomenon of obsolescence happens all the time in computer science, but its effect is especially felt in the forensic field.

As far as photos and videos are concerned, digital image-processing services embedded in forensic applications is becoming norm. Companies such as Belkasoft, Magnet, and Cellebrite with their consolidated products such as Platform X, Axiom Cyber or Physical Analyzer are betting on programs with a variety of utilities, especially image recognition. These services include optical character recognition (OCR), image categorization or auto-detection of objects and people. This trend acknowledges the power of IA by incorporating it to the forensic tool kit to facilitate the work of analysts. Interestingly, none of the previous publications face this challenge, which opens the possibility for innovation.

### Legislation

Computer forensics is a highly regulated industry because it deals with sensitive information often in a judicial context.

#### 2.3.1 Legislation and legal regulations.

In 2010 Spain ratified The Cybercrime Convention [6], drawn up in Budapest on 23 November 2001. Along this convention and the spanish code of law XXX crimes against privacy, espionage, theft, impersonation, fraud, forgery, embezzlement, manipulation of devices, damage or alteration of data programs or files are contemplated.

It is worth mentioning that the forensic profession relies heavily on ethical integrity. There are various codes of ethics and recommendations such as the ISCF code of conduct from the International School of Computer Forensics or the SANS institute work-ethic guidelines. These documents signify the importance of honesty, defense of intellectual property, confidentiality and individual rights and freedoms In summary professionalism and commitment to safeguarding of the truth. Likewise, it condemns any form of corruption (blackmail, bribery or commission), prevaricating attitude, premeditated attempt against privacy or discrimination based on sex, race, religion, age, ethnicity, politics or any other condition.

#### 2.3.2 The figure of the computer expert in the courts.

The law defines this role as a professional specialized in computer science whose work consists on providing technical advice in judicial proceedings, as well as contributing to mediation and conflict resolution. He/she can exercise several roles, mediator, arbitrator and auditor, all of which are overseen by judges.

#### 2.3.3 Chain of custody

When presenting a digital evidence to the judge there are a number of prerequisites that must be met for admission. For any evidence collected, the original evidence must be preserved together with its chain of custody. The chain of custody is a control procedure that covers the process of obtaining, handling, transferring, assigning and preserving evidence in order to rigorously ensure that the evidence has been delivered and remains unaltered (as demonstration by hash complience).

#### 2.4 Socio-economic environment

The economic impact is difficult to estimate given that in principle the product is oriented to a narrow niche, forensic investigations involving evidences containing Your Phone artifacts. According to vestigeltd [8] the average costs of a forensic investigation are usually around $5,000 to $15,000 on average. According to the agency, a cost of $250 per hour of effective work can be considered standard. In this sense, the developed project could have a positive impact since it would reduce the analysis time. The software solution developed could also be exported to different contexts such us image extraction functionality. Any application that seeks to interact (input or extract) multimedia content from Your Phone. The same would be true for the face comparator and face grouper, which if generalized and refined could be marketed as an add-on module for some of the forensic programs described above (Belkasoft, Magnet and Cellbrite).

As for the social and ethical implications, it is worth mentioning that since this is a program designed to discover and work with personal data (conversations, calls, images), strict confidentiality should be maintained

# Implementation

### 3.1 Planificación

# conclusions

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 |