Programa de Doctorado en Ciencias Forenses

CONTRIBUCIONES AL ANÁLISIS FORENSE DE EVIDENCIAS DIGITALES PROCEDENTES DE APLICACIONES DE MENSAJERÍA INSTANTÁNEA

Tesis Doctoral presentada por

Jesús María De Gregorio Melgar

2020

Programa de Doctorado en Ciencias Forenses

CONTRIBUCIONES AL ANÁLISIS FORENSE DE EVIDENCIAS DIGITALES PROCEDENTES DE APLICACIONES DE MENSAJERÍA INSTANTÁNEA

Tesis Doctoral presentada por

Jesús María De Gregorio Melgar

Directores: Dr. Bernardo Alarcos Alcázar

Dr. Alfredo Gardel Vicente

Alcalá de Henares, 2020

AGRADECIMIENTOS

En primer lugar, agradecer de todo corazón a mi director y tutor, los doctores Bernardo Alarcos Alcázar y Alfredo Gardel Vicente, mentores y amigos, que han formado parte de este gran proyecto personal y profesional. Porque sin ellos nada de esto habría sido posible, gracias por su actitud, conocimientos, energía y apoyo incondicional, pero sobre todo por su tiempo. Conocerles ha sido un verdadero privilegio y espero que perdure la amistad forjada durante este tiempo.

Gracias a la Universidad de Alcalá de Henares y al Instituto Universitario de la Investigación en Ciencias Policiales por ofrecerme la posibilidad de desarrollar este trabajo y desarrollarme en el ámbito de las Ciencias Forenses.

Agradecer a Dña. María Jesús Llorente Vega por brindarme la oportunidad hace ya muchos años de entrar en el apasionante campo de la Informática Forense. Siempre la estaré agradecido por todo lo ha hecho y continúa haciendo por mi tanto personal como profesionalmente.

Gracias a mis compañeros y amigos Emilio, Matu, Alex, Javi, Miguel y Ruth por los muchos conocimientos compartidos y por el apoyo brindado. Gracias a todas aquellas personas que han estado a mi lado durante todos estos años, por su aguante y apoyo.

Por último, dar las gracias a toda mi familia, porque de cada una de las personas que lo forman aprendo algo nuevo cada día. Espero que todos ellos, sin excepción, estén orgullosos de mí, porque ellos me dan la fuerza necesaria para desarrollarme personalmente y querer ser mejor persona.

Hay una fuerza motriz más poderosa que el vapor, la electricidad y la energía atómica: la voluntad.

Albert Einstein

INDICE

RESUMEN

La continua evolución de las Tecnologías de la Información y Comunicaciones (TICs) está propiciando que, cada vez más, nos encontremos ante una sociedad más interconectada, permitiendo el intercambio inmediato de información digital desde casi cualquier lugar del planeta.

Desde el punto de vista social, esta evolución implica el desarrollo de dispositivos electrónicos cada vez más pequeños e inteligentes, como es el caso de los teléfonos, televisores, relojes, tabletas, dispositivos IoT (*Internet of Things*), etc. Estos dispositivos electrónicos inteligentes ofrecen a sus propietarios la capacidad de transmitir ingentes cantidades de datos (con y sin su consentimiento), a través de una gran diversidad de aplicaciones de intercambio de información (mensajería instantánea, correos electrónicos, redes sociales, etc.), con independencia del momento y ubicación. Especial importancia está adquiriendo, dentro de estas aplicaciones de intercambio de información, las aplicaciones de mensajería instantánea (IM). Este tipo de aplicaciones han modificado notablemente tanto la forma como en el modo de interactuar con el resto de la sociedad desde su creación. El uso impulsivo de las aplicaciones de IM, como WhatsApp, Telegram Messenger o Facebook Messenger, está sustituyendo en muchas ocasiones, las interacciones físicas que se realizan con otras personas, tanto a nivel personal como profesional. Este tipo de aplicaciones, permiten una comunicación más rápida y fluida, modificando la manera en la cual se notifican eventos (reuniones, cumpleaños, etc.), se comparten documentos (currículums, nominas, contratos, etc.) o se envían archivos multimedia (imágenes, videos, audios, notas de voz, etc.).

Desde el punto de vista legal, la evolución de las TICs, así como Internet, y el uso inapropiado de estos, implica que surjan nuevos tipos delictivos, y que sean modificados muchos otros. En la actualidad, delitos relacionados con las amenazas, estafas, contra la libertad e identidad sexual, defraudaciones de fluido en las telecomunicaciones, inducción al suicidio, homicidios, asesinatos, daños informáticos, propiedad intelectual e industrial, falsedad documental, revelación de secretos, coacciones, calumnias, etc., son cometidos a través de las TICs, llegándose incluso a acuñarse nuevos términos como *sexting*, *ciberbullying*, *grooming*, *stalking* o *phishing*, para definir esta nueva tipicidad delictiva. De igual manera, las capacidades de los dispositivos electrónicos inteligentes,

sumado a la globalización de las comunicaciones, ha conllevado a una transnacionalización en la comisión de los hechos delictivos, no siendo necesario una cercanía física entre víctima y agresor. En la actualidad, el uso de las aplicaciones de IM para la comisión de hechos delictivos es creciente ya que proporcionan al agresor una comunicación directa, gratuita e inmediata con su o sus víctimas. Este tipo de aplicaciones están adquiriendo una gran relevancia en multitud de procesos judiciales, siendo en ocasiones, elemento inicial y pieza principal de investigaciones criminales.

Desde el punto de vista de las ciencias forenses, como ciencia que estudia los elementos recolectados en la escena de un crimen para el esclarecimiento de un hecho delictivo, el nacimiento y la rápida evolución de las Tecnologías de la Información y Comunicaciones implica que deban adaptarse, estudiando y validando continuamente el uso de diferentes métodos y técnicas científicas de análisis que contribuyan en la resolución de los hechos delictivos cometidos a través el uso de las TICs. Durante muchos años la ciencia forense se centró únicamente en el análisis de los vestigios biológicos (pelo, sangre, huellas dactilares, etc.) encontrados en la escena de un crimen, los cuales eran utilizados principalmente para identificar al autor. En la actualidad individuos ataviados con traje blanco, guantes, calzas, grandes maletines (bolsas de plástico y papel, pinzas, polvos reveladores, etc.), portando dispositivos electrónicos de última generación con *software* y *hardware* especializado, procesan la escena de un crimen, identificando posibles elementos probatorios a través de testigos métricos y recogiendo infinidad de vestigios tanto biológicos como digitales, para después ser analizados en el laboratorio. La identificación, recogida y análisis de dispositivos o vestigios digitales tienen un gran peso en las investigaciones de hechos delictivos, permitiendo en muchos casos la resolución de delitos que de otra forma no habrían podido ser resuelto. De esta manera, las ciencias forenses digitales o *digital forensics* en inglés, son las encargadas de la adquisición, preservación, análisis, exposición y emisión de resultados realizados sobre la información contenida en los dispositivos digitales incluidos en procesos judiciales. Todos estos procedimientos deben apoyarse en métodos científicos que proporcione un soporte conceptual y procedimental a la investigación, garantizando en todo momento la integridad de la información extraída de los dispositivos electrónicos incluidos en la comisión de un hecho delictivo.

La ciencia forense digital es tan amplia como la cantidad de dispositivos electrónicos, diversidad de sistemas operativos o número de las aplicaciones (clientes y

versiones) que se incluyen en estos. El uso que se realiza en concreto de las aplicaciones de intercambio de información en la comisión de hechos delictivos implica que éstas deban ser objeto de un análisis forense minucioso, a partir del cual identificar, recuperar y extraer toda aquella información relativa con el hecho investigado, manteniendo en todo momento el valor probatorio de la misma. El documento que aquí se presenta lleva a cabo la primera investigación en el mundo en la cual se evalúa la evolución de las aplicaciones de IM y su impacto en el ámbito de las ciencias forenses. La investigación realizada pretende reseñar la transformación de este tipo de aplicaciones en cuanto a los diferentes métodos de acceso e infinidad de funcionalidades ofrecidas a sus usuarios. Así mismo se persigue contribuir de forma directa en los métodos científicos utilizados en el análisis forense que se vienen realizando sobre las aplicaciones de IM, medio de prueba principal en multitud de procesos judiciales.

En este documento expone el estado actual de los procesos utilizados tanto en el proceso de adquisición como en el proceso de análisis de las aplicaciones de IM, así como las diferentes problemáticas a las que se enfrenta el especialista forense digital en el análisis forense de este tipo de aplicaciones. Se desarrolla una metodología específica para el análisis forense de las aplicaciones de IM, suma de diversos métodos de estudios, la cual permitirá identificar, decodificar e interpretar la información generada por este tipo de aplicaciones con independencia del dispositivo electrónico, sistema operativo o aplicación analizada. A partir de los tres métodos de estudio incluidos en la metodología propuesta, se pretende verificar y validar la integridad de la información extraída más allá del uso generalizado de soluciones forenses comerciales. Por último, se expondrán los resultados y conclusiones obtenidas de aplicar la metodología de análisis forense propuesta en esta investigación sobre alguno de los clientes de las principales aplicaciones de IM que existen en la actualidad.

Palabras clave: Ciencias forenses, Informática forense, Dispositivos electrónicos, Metodología de análisis forense, Aplicaciones de mensajería instantánea.

ABSTRACT

The continuous evolution of Information and Communication Technologies (ICTs) is stimulating that we are facing a more and more interconnected society, allowing the immediate exchange of digital information from almost anywhere in the world.

From the society point of view, this evolution implies the development of increasingly small and smart devices such as phones, televisions, watches, tablets, IoT (Internet of Things) devices, etc. These smart electronic devices offer their owners the ability to transmit huge amounts of data (sometimes without their explicit consent), through a wide variety of information exchange applications (instant messaging, emails, social networks, etc.), regardless of time and location. The instant messaging (IM) applications are one of the most relevant tools for information exchange. Since its beginnings, this kind of applications have meaningfully modified both, the way and how to interact with the rest of society. The impulsive use of IM applications, such as WhatsApp, Telegram Messenger or Facebook Messenger, is replacing on many occasions, the physical interactions with other people, both at the personal and professional level. These types of applications allow faster and more fluid communication, transforming how events are notified (meetings, birthdays, etc.), attaching documents (resumes, payrolls, contracts, etc.) or sharing multimedia files (images, videos, audios, voice, memos, etc.).

From the legal point of view, the ICTs evolution, as well as the Internet, and the inappropriate use of these, implies that new criminal types arise and that many others are modified. At present, crimes related to threats, scams, against freedom and sexual identity, fraud of telecommunications flows, suicide induction, homicides, murders, computer damage, intellectual and industrial property, documentary forgery, disclosure of secrets, coercion, slander, etc., are committed through ICTs, even new terms such as sexting, cyberbullying, grooming, stalking or phishing has been coined to define new types of crimes. Similarly, the capabilities of intelligent electronic devices, coupled with the globalization of communications, have led to a trans-nationalization in the commission of criminal acts, not being necessary a physical closeness between victim and offender. Currently, the use of IM applications to commit crimes is increasing as provide the aggressor with immediate direct and free communication with his/her victims.

Such applications are becoming extremely relevant in many lawsuits, being sometimes a starting element or central piece of criminal investigations

From the point of view of forensic science, as a science that studies the elements collected at the crime scene for the clarification of a criminal act, the birth and fast evolution of ICTs implies that digital forensic science should adapt, study and increasingly validate the use of different methods and scientific analysis techniques that contribute to the resolution of criminal acts committed through the use of ICTs. For many years, forensic science focused solely on the analysis of biological vestiges (hair, blood, fingerprints, etc.) found at the crime scene, mainly to identify the author. Nowadays, forensic technicians are dressed in white suits, gloves, shoes, carrying large briefcases (plastic and paper bags, tweezers, revealing powders, etc.), using the latest generation of electronic devices with specialized forensic software and hardware, in order to process the crime scene, identifying possible evidence through metric identifications and collecting countless traces both biological and digital to later be analysed in the laboratory. The identification, collection, and analysis of digital devices or vestiges have a great weight/impact in the investigations of criminal acts, allowing in many cases the resolution of crimes that otherwise could not have been resolved. In this way, the digital forensic sciences or solely digital forensics, embrace the acquisition, preservation, analysis, exposure, and results reporting made on the information contained in the digital devices included in legal proceedings. All these procedures must be supported by scientific methods that provide conceptual and procedural support to the investigation, guaranteeing at all times the integrity of the information extracted from the electronic devices related to the commission of a criminal act.

Digital forensic science is as wide as the number of electronic devices, diversity of operating systems or number of applications (different clients even different versions). The use of information exchange applications in the commission of criminal acts implies that they must be subject to a thorough forensic analysis, from which to identify, retrieve and extract all information related to the investigated fact, maintaining at all times the probative value of it. The document presented here carries out the first research in the world in which the evolution of IM applications and their impact in the field of digital forensic science is evaluated. The research conducted aims to review the transformation of such applications taking into consideration the different access methods and host functions available to users. It also seeks to contribute directly to the scientific methods

used in the forensic analysis that is being carried out on IM applications, the main evidence in many judicial proceedings.

This document presents the current status of the processes used both in the acquisition process and in the process of IM application analysis, as well as the different problems faced by the digital forensic specialist in the forensic analysis of this type of application. A specific methodology has been developed for the forensic analysis of IM applications, a sum of various study methods, which allow the investigator to identify, decode and interpret the information generated by this type of application regardless of the electronic device, operating system or application analysed. Based on the three study methods included in the proposed methodology, it is intended to verify and validate the integrity of the information extracted beyond the widespread use of commercial forensic solutions. Finally, the results and conclusions obtained from applying the forensic analysis methodology proposed in this investigation on some of the clients of the main IM applications that currently exist are presented.

Keywords: Forensic sciences, Computer forensics, Electronic devices, Forensic analysis methodology, Instant messaging applications.

LISTA DE TABLAS

LISTA DE FIGURAS

ABREVIATURAS

APFS: Apple File System.

Art: Artículo**.**

BEF: Belkasoft Evidence Finder.

BLOB: Binary Large Object.

CCN: Centro Criptológico Nacional.

CENDOJ: Centro de Documentación Judicial.

CGPJ: Consejo General del Poder Judicial.

CP: Código Penal.

DEFT: Digital Evidence & Forensic Toolkit.

eMMC: embedded MultiMedia Card.

eMCP: embedded Multi-Chip Package.

FFCCSE: Fuerzas y Cuerpos de Seguridad del Estado.

HDD: Hard Disk Drive.

IE: Internet Explorer.

IEC: International Electrotechnical Commision.

IEF: Internet Evidence Finder.

ISO: International Organization for Standardization.

ISP: In-System Programming.

INCIBE: Instituto Nacional de Cibeseguridad.

INTECO: Instituto Nacional de Tecnologías de la Comunicación.

IM: Instant Messenger.

IoT: Internet of Things.

IP: Internet Protocol.

ISP: In-System Programing.

JTAG: Joint Test Action Group.

LO: Ley Orgánica.

LOPD: Ley Orgánica de Protección de Datos de carácter personal.

LECrim: Ley de Enjuiciamiento Criminal.

macOS: mac Operating System.

MD5: Message-Digest Algorithm 5.

MTK: MediaTek.

NIJ: National Institute of Justice.

NIST: National Institute Standar and Tecnology.

RAM: Random Access Memory.

RAID: Redundant Array of Independent Disks.

RTOS: Real Time Operating System.

SHA: Secure Hash Algorithm.

SMS: Short Message Service.

SO: Sistema Operativo**.**

SSD: Solid State Disk.

STS: Sentencia del Tribunal Supremo**.**

SWGDE: Scientific Working Group on Digital Evidence.

TAC: Test Access Port.

TC: Tribunal Constitucional.

TIC: Tecnologías de la Información y Comunicaciones**.**

UFED: Universal Forensic Extraction Device.

UNE: Una Norma Española.

USB: Universal Serial Bus.

VoIP: Voz over Internet Protocol.

WiFi: Wireless Fidelity.

WP: Windows Phone**.**

XML: Extensible Markup Language.

GLOSARIO DE TERMINOS TECNICOS

Android: Sistema operativo utilizado mayoritariamente en dispositivos móviles, como teléfonos, relojes o televisores inteligentes.

Bots: Aplicaciones informáticas utilizadas para la automatización de tareas o procesos.

Bloqueadores de escritura: Dispositivos hardware usados en la adquisición de evidencias electrónicas. Estos dispositivos bloquean contra escritura el acceso a la información de la evidencia electrónica, permitiendo únicamente el acceso de lectura a la información para realizar la adquisición.

Ciberbullying: Es definido como "*el uso y difusión de información lesiva o difamatoria en formato electrónico a través de medios de comunicación como el correo electrónico, la mensajería instantánea, las redes sociales, la mensajería de texto a través de teléfonos o dispositivos móviles o la publicación de vídeos y fotografías en plataformas electrónicas de difusión de contenidos*", en la Guía Legal sobre Ciberbullying y Grooming de por INCIBE (antiguo INTECO). Observatorio de la seguridad de la información. Área Jurídica de la Seguridad y las TIC.

Ciberstalking: Dícese del acoso ilegitimo de manera reiterada e insistente a una persona a través de Internet.

Cliente móvil: Aplicación desarrollada para sistemas operativos móviles**.**

Cliente de escritorio: Aplicación desarrollada para sistema operativos de escritorio.

Cliente web: Aplicación desarrollada para ser ejecutada a través de navegadores de Internet**.**

Clonadoras: Son dispositivos hardware usados en la adquisición de evidencias electrónicas. Estos dispositivos realizan una copia exacta de la información contenida en una evidencia electrónica origen sobre otro destino.

Chat: Corresponden a las comunicaciones digitales que se realiza a través de Internet entre varios usuarios. A través de un chat se pueden compartir diferente contenido digital, como mensajes de texto o archivos multimedia.

Día cero: Es definido como "*Son aquellas vulnerabilidades en sistemas o programas*

informáticos que son conocidas por determinados atacantes, pero no lo son por los fabricantes o por los usuarios. Son las más peligrosas ya que un atacante puede explotarlas sin que el usuario sea consciente de que es vulnerable.", en la guía CCN-STIC-401 Glosario y Abreviaturas del Centro Criptológico Nacional. (*Zero Day* en inglés).

Emojis: Imágenes o pictogramas en formato Unicode utilizados en los medios de comunicación digital**.**

Gestor de arranque: Procesos que se ejecutan antes del normal inicio de arranque del sistema operativo (*bootloaders* en inglés).

Grooming*:* Se define como aquel conjunto de estrategias de acercamiento a través de la red de Internet desarrolladas por una persona adulto al objeto de ganarse la confianza de un menor obteniendo con ello contenido multimedia comprometido o incluso contacto físico.

HASH: Corresponde a la función resumen generada por un algoritmo matemático el cual es utilizado para identificar de manera univoca una información digital. Existen diferentes tipos, siendo los más utilizados en el ámbito forense digital MD5, SHA1, o SHA256.

IM: siglas de mensajería instantánea (*instant messaging* en inglés). Identifica al servicio de mensajería que permite la comunicación en tiempo real.

Imagen forense: Fichero o ficheros que contienen la información contenida (*bit* a *bit*) de un dispositivo digital.

Internet: en forma muy resumida, red de ordenadores o equipos informáticos que se comunican entre sí empleando un lenguaje común conocido como conjunto de protocolos.

IoT: siglas de Internet de las cosas (*Internet of Things* en inglés). Identifica a aquellos dispositivos digitales de pequeño tamaño con conectividad a Internet.

Nube: es el concepto aplicado a determinados servicios alojados en Internet, que facilita la utilización de recursos digitales desde una ubicación remota (*Cloud* en inglés).

LiveCD: Distribución forense en soporte disco compacto (*Compat Disk* en inglés), creada normalmente bajo sistema operativo Linux y utilizada para procedimientos forenses como la adquisición y análisis de dispositivos informáticos.

LiveUSB: Distribución forense en soporte memoria USB utilizada para procedimientos forenses como la adquisición y análisis de dispositivos informáticos.

Log: Archivo de eventos que registra movimientos y actividades de un determinado programa o sistema operativo para el control de su ejecución.

macOS: Sistema operativo de escritorio creado por la compañía Apple para sus dispositivos informáticos.

Navegador de Internet: Programa informático que proporciona acceso a diferentes servicios alojados en Internet. Este programa es utilizado normalmente para visualizar el contenido de una página de Internet (*Web Browser* en inglés**)**.

Phishing*:* Dícese de las técnicas utilizadas para obtener información de carácter personal a través del envío de correos electrónicos. El emisor del correo, haciéndose pasar por una entidad de confianza, solicita al receptor información relativa a las claves de acceso a sus servicios bancarios, plataformas de pago, o correo electrónico.

Recuperación de datos: es el proceso por el cual se recupera la información contenida en un dispositivo digital. Este proceso se realiza a partir de la búsqueda del inicio y final de un fichero a partir de su cabecera y pie en formato hexadecimal (*datacarving* en inglés**)**.

Redes sociales: son sitios formados en Internet cuya finalidad es comunicar y compartir contenidos digitales entre grupos de personas y relacionarse con otros grupos.

Sexting: Dícese de la difusión sin consentimiento de contenido digital privado, normalmente imágenes o videos, de carácter sexual en la red de Internet valiendo de dispositivos electrónicos.

Stickers*:* Imágenes o pegatinas utilizados en los medios de comunicación digital para compartir de manera sencilla ideas, sentimientos, etc. Aplicaciones como WhatsApp ofrece la posibilidad a sus usuarios de crear sus propias pegatinas.

Streaming*:* Tecnología utilizada para compartir contenido en tiempo real entre ordenadores o móviles a través de Internet.

VoIP: Voz sobre protocolo IP. Identifica aquellas llamadas de voz realizada a través de una red de datos como Internet (*Voz over Internet Protocol* en inglés).

Windows Phone. Sistema operativo móvil creado por la compañía Microsoft para

dispositivos electrónicos móviles.

1 LAS CIENCIAS FORENSES EN EL MUNDO DIGITAL

En este primer capítulo de la memoria de la tesis doctoral se expondrá de manera generalizada la inclusión de las Tecnologías de la Información y Comunicaciones (TIC) en las Ciencias Forenses. Se realizará una breve introducción al concepto de las TIC y de las aplicaciones de intercambio de información, centrándose el análisis en las aplicaciones de mensajería instantánea (IM) como medio de comunicación y el uso de estas para la comisión de delitos. Por último, se definirá el concepto de Informática Forense como parte de las Ciencias Forenses y los diferentes procedimientos seguidos para el tratamiento de evidencias electrónicas.

1.1 Las TIC y las aplicaciones de intercambio de información personal

A continuación, se expondrá la evolución sufrida por las Tecnologías de la Información y Comunicaciones y la aparición de las aplicaciones de intercambio de información personal en la sociedad.

1.1.1 La evolución de las TIC

El termino de Tecnologías de la Información y Comunicaciones tiene diversas definiciones si bien el mismo puede resumirse perfectamente en:

> TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (TIC) = Cuando unimos estas tres palabras hacemos referencia al conjunto de avances tecnológicos que nos proporcionan la informática, las telecomunicaciones y las tecnologías audiovisuales, que comprenden los desarrollos relacionados con los ordenadores, Internet, la telefonía, los "mas media", las aplicaciones multimedia y la realidad virtual. Estas tecnologías básicamente nos proporcionan **información**, herramientas para su **proceso** y canales de **comunicación**. (Graells, 2000, p.3)

La evolución de las TIC, así como la aparición de Internet, ha provocado una transformación tecnológica, ofreciendo a la sociedad actual un amplio abanico de nuevos bienes y servicios, funcionalidades y oportunidades hasta ahora inéditas pero posibles con la llegada de nuevas aplicaciones y equipos electrónicos. En la actualidad, las TIC se encuentran presentes en casi todos los aspectos de la sociedad, transformando multitud de tareas cotidianas de la vida moderna, gestionando infinidad de recursos, automatizando tareas, ahorrando costes, mejorando el rendimiento y la productividad, incrementando la sostenibilidad o proporcionando una comunicación rápida y fluida entre las personas.

Podemos encontrar el uso de las TIC e Internet en múltiples ámbitos de nuestro día a día tales como la educación, la agricultura, la política, el sistema judicial, banca o medicina. En estos ámbitos, el comercio electrónico, el acceso a recursos y la atención permanente (24 horas - 7 días a la semana), el acceso en tiempo real a la información, la automatización de servicios, el teletrabajo, la digitalización de documentos, reuniones virtuales online desde diferentes puntos geográficos, estudios de mercados online, el marketing digital o el uso de las redes sociales (RRSS), implican todos ellos una mejora sustancial en el rendimiento y la productividad de los equipos de trabajo. Por otra parte, se puede analizar cuál ha sido la implementación del uso de las TIC en el ámbito personal. Las personas se comunican e intercambian todo tipo de información a través de pequeños dispositivos electrónicos móviles inteligentes. Estos dispositivos, con capacidades similares a las de un ordenador, disponen de multitud de aplicaciones las cuales permiten a su usuario transmitir y compartir infinidad de información bien sea tanto de carácter personal como profesional. Así mismo, estos dispositivos móviles inteligentes disponen de una conexión de datos inalámbrica que permite una comunicación en tiempo real con otras personas en ubicaciones remotas pudiendo transferir una ingente cantidad de información en pocos segundos.

Las TIC e Internet han transformado de manera drástica la sociedad hacia un entorno cada vez más digitalizado, sustituyendo métodos tradicionales como es el envío de cartas a través el servicio de correos por el uso de aplicaciones de correo electrónico (Outlook, Thunderbird, etc.), la consulta de libros en una biblioteca se está sustituyendo por la consulta de información digitalizada en Internet a partir de navegadores (Chrome, Internet Explorer, Edge, Firefox, Opera, etc.) o libros digitales (*ebooks*), las relaciones

personales físicas se sustituyen o complementan por las relaciones personales digitales a través de Redes Sociales (Facebook, Twitter), la llamada de teléfono o mensaje de texto se sustituye por el envío instantáneo de información (WhatsApp, Telegram Messenger, Signal Private Messenger, Threema, etc.) los gestores de contenido online (WordPress, Joomla, etc.), el almacenamiento de documentación en papel se sustituye por servicios de información en Internet (Google Drive, Dropbox, etc.), o los métodos tradicionales de pago se sustituyen por métodos de pago online (PayPal, Payline, Amazon Pay, etc.). Poco a poco se está eliminando el documento en papel como soporte físico, dando paso a una sociedad en la digitalizada, en la cual la información es transmitida de manera instantánea a través de redes de datos y guardados de manera redundante en dispositivos de almacenamiento masivo (HDD o SSD), sistemas de almacenamiento de red, sistemas de redundancia de datos (RAID) o sistema de copia de seguridad.

Tanto en los estudios estadísticos relativos al uso del dispositivo electrónico en la población adulta Española en el año 2018[1] realizados por *We Are Social* como en la encuesta relativa al uso de las TIC en hogares españoles en el año 2019[2] realizada por el Instituto Nacional de Estadística (INE), muestran que los usuarios españoles dedican cada vez más tiempo al uso de Internet, realizando búsquedas de texto, consultando información en redes sociales, visualizando videos, escuchando música en línea (*streaming)* o enviando datos de manera continua a través de aplicaciones de intercambio de información. Existen múltiples definiciones al respecto de los conceptos TIC e Internet, si bien, la evolución de ambos se puede enmarcar dentro de un concepto más amplio y general como es el de era digital. La era digital en la cual se encuentra sumida la sociedad hoy en día, con la dependencia en el uso de los bienes y servicios que engloban las tecnologías de la información y comunicaciones, implica que, según indica el informe *We Are Social*, más de un 5.1 billones de la población disponga de un dispositivo móvil, más de un 4.3 billones sean usuarios de Internet y que existan alrededor de 3 billones de usuarios con cuentas activas en redes sociales. La figura 1.1, muestra las estadísticas

[1] We are social. (2019). *Digital in 2019 España*. Recuperado el 5 de julio de 2019, de: https://wearesocial.com/es/digital-2019-espana.

[2] Instituto Nacional de Estadistica. (2019). *Equipamiento y uso de TIC en los hogares - Año 2019*. Recuperado el 13 de noviembre de 2019, de: https://www.ine.es/prensa/tich_2019.pdf.

acerca del uso de dispositivos móviles, Internet y redes sociales en el mundo a fecha de 2019, correspondiente con la recopilación de información realizada por *We Are Social*.

Figura 1.1. Ejemplo del avance de la era digital en el año 2019. Fuente: https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates.

La era digital está cambiando en gran medida como interactuamos con los demás o incluso nuestro estilo de vida. Existe una continua interconexión a través de relojes, teléfonos, televisiones, frigoríficos, vehículos, casas, oficinas o incluso redes de todos ellos en lo que se denomina ciudades inteligentes. En la actualidad nos encontramos con dispositivos electrónicos inteligentes capaces de tomar decisiones por nosotros frente a ciertas situaciones. Un ejemplo práctico de esto, lo encontramos en los frigoríficos inteligentes, dispositivos electrónicos que, sin necesidad de ninguna interacción por parte del ser humano, están programados para solicitar alimentos cuando se prevea una falta de existencias o avisar al usuario de la caducidad de los alimentos almacenados.

Si bien, la evolución de las TIC e Internet conlleva infinidad de beneficios para nuestra sociedad, también implica ciertos riesgos para sus usuarios. La cantidad de información digital que se genera diariamente es inmensa, se publica, comparte o transfiere tanta cantidad que incluso en ocasiones sus propietarios pierden el control sobre la misma. Este

tipo de información, en ocasiones sensible, fluye a través de la red y se almacena en servidores remotos de los cuales no se conoce ni tan siquiera su ubicación. Aunque parezca extraño la información digital actualmente es más accesible y lucrativa que los documentos o el dinero de papel. Los cibercriminales o hackers lo saben y utilizan multitud de técnicas para hacerse con este tipo de información obteniendo grandes beneficios de forma remota. El uso incorrecto de las TIC proporciona a estos cibercriminales las herramientas necesarias para cometer infinidad de hechos delictivos sin límite fronterizo u horario, utilizando técnicas avanzadas para el robo de información sensible, el secuestro de sistemas informáticos corporativos o incluso el robo de carteras de dinero virtual. Así mismo, los fallos de seguridad de las TIC pueden ser utilizados para recopilar información digital de carácter tanto personal como profesional. Empresas como ZERODIUM[3] ofrecen grandes recompensas a quien proporcione fallos de seguridad de día cero o *zero day* en inglés no conocidos por sus creadores, encontrándose catalogados por sistema operativo, servidores web, servidores de correo electrónico, navegadores web, clientes o ficheros, teléfonos inteligentes, etc. En este sentido, entidades españolas como el Centro Criptológico Nacional (CCN) elaboran guías anuales en las que se informan sobre la evolución de diferentes dispositivos electrónicos (Centro Criptológico Nacional, 2019a) así como informes sobre el estado de la seguridad de las TIC tanto para Administraciones Públicas (Centro Criptológico Nacional, 2018a) y guías y procedimientos del uso de las TIC para usuarios particulares en las cuales se marcan las directrices para el correcto manejo de los diferentes dispositivos electrónicos móviles que existen en el mercado (Centro Criptológico Nacional, 2018b, 2019b).

1.1.2 Las aplicaciones de intercambio de información

Hoy en día, casi todo el intercambio de información se desarrolla a través de la red, sin presencia física. Se comparte información de manera continua a través de múltiples aplicaciones contenidas en dispositivos electrónicos (ordenadores, teléfonos inteligentes, tabletas, televisores inteligentes, etc.), en ocasiones sin tan siquiera saberlo, siendo las propias aplicaciones preinstaladas las que transmiten automáticamente y de

[3] ZERODIUM. (2019). *Our Exploit Acquisition Program*. Recuperado el 11 de julio de 2019, de: https://zerodium.com/program.html.

forma transparente al usuario ingente cantidad de información a terceros (Gamba, J., Rashed, M., Razaghpanah, A., Tapiador, J., & Vallina-Rodriguez, N., 2019). De manera constante se desarrollan aplicaciones con nuevas funcionalidades que son utilizadas para transmitir, comunicar, gestionar, compartir o visualizar contenido digital de múltiples maneras. Tal es así que, la cantidad de aplicaciones desarrolladas dieron paso a la creación de los mercados de aplicaciones digitales. Estas plataformas digitales catalogan las aplicaciones que ofrecen a los usuarios en relación con su funcionalidad (comunicación, citas, finanzas, noticias, social, mapas, etc.). En este sentido en los diferentes mercados digitales se pueden encontrar aplicaciones para la gestión del correo electrónico (Gmail, Hotmail, ProtonMail, etc.), mensajería instantánea (Signal Private Messenger, Telegram Messenger, WhatsApp, Line, etc.), redes sociales (Facebook, Twitter, Instagram, etc.), mapas (Google Maps, Waze, etc.) o salud y bienestar (Endomondo, Runtastic, etc.).

1.1.2.1 Las aplicaciones de mensajería instantánea

Las aplicaciones de IM son aquellas aplicaciones que permiten el intercambio de casi cualquier tipo información digital en tiempo real. Este tipo de aplicaciones han cambiado de manera significativa el modo de comunicarse.

Las comunicaciones realizadas a través de correos electrónicos, llamadas telefónicas o mensajes de texto han sido reemplazadas en un gran porcentaje por el uso de las aplicaciones de IM que permiten el intercambio de información de manera instantánea con funcionalidades más avanzadas e incorporando en la comunicación a grupos de usuarios seleccionados. El impacto de este tipo de aplicaciones en las comunicaciones puede verse reflejado en el número de usuarios activos, existiendo en el año 2018 más de 2 billones de usuarios activos de aplicaciones de mensajería instantánea.

La figura 1.2 muestra de manera gráfica, la evolución que viene sufriendo el número de usuarios de aplicaciones de mensajería instantánea y su previsión en los próximos 2 años.

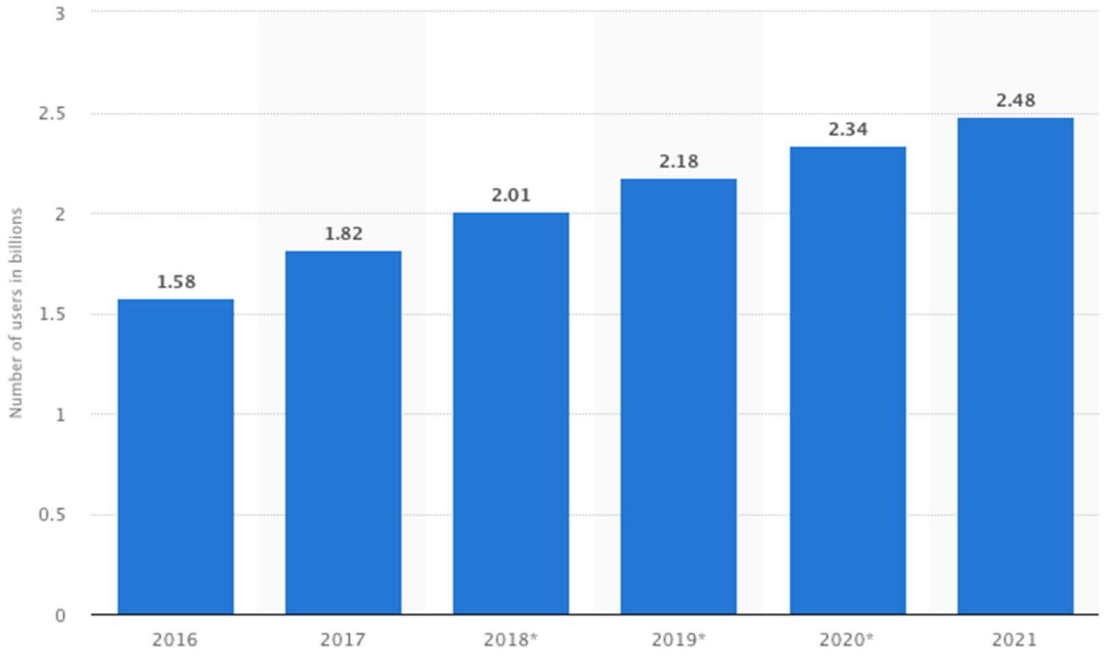


Figura 1.2. Evolución del número usuarios activos en aplicaciones móviles de mensajería desde 2016 a 2021. Fuente: https://www.statista.com/statistics/483255/number-of-mobile-messaging-users-worldwide/.

Las aplicaciones de IM surgieron inicialmente con el objeto de intercambiar simples mensajes de texto de manera instantánea entre sus usuarios, sustituyendo al conocido mensaje de texto (*SMS*)[4] [5]. Basta decir, que este tipo de aplicaciones no tardaron mucho en incluir otras muchas funcionalidades, como el intercambio de imágenes, videos, geolocalizaciones, contactos, documentos, *emojis*, *stickers*, etc., las cuales no se encontraban disponibles a través del SMS. Así mismo este tipo de aplicaciones posibilitan, no solo el intercambio de información de manera personal o individual, si no que ofrecen una comunicación mucho más global de intercambio de información en forma de grupo (cientos de personas) o de canales (miles de personas). De igual manera este tipo de aplicaciones a lo largo de los años han incluido características tan diversas como la programación de robots (*bots*) para la automatización de tareas, la posibilidad de realizar videollamadas y llamadas sobre *VoIP* (con la consiguiente repercusión sobre las

[4] Lundgren, J. (2015). *Will Messaging Apps Kill Sms.* Recuperado el 29 de septiembre de 2016, de: http://www.sinch.com/opinion/will-messaging-apps-kill-sms/.

[5] Woollaston, V. (2013). *The end of the text message? Mobile chat apps overtake SMS for the first time*. Recuperado el 29 de septiembre de 2016, de: https://www.dailymail.co.uk/sciencetech/article-2316629/The-end-text-message-Mobile-chat-apps-overtake-SMS-time.html.

llamadas telefónicas convencionales), el borrado programado de mensajes, el borrado de metadatos en archivos compartidos o la gestión de servicios de pago. La evolución de este tipo de aplicaciones es tal que, si bien fueron ideadas para las comunicaciones personales cada vez más son utilizadas en entornos laborales y profesionales. Este es el ejemplo de la aplicación de mensajería instantánea WhatsApp, la cual ha desarrollado una versión específica para pequeñas y medianas empresas que incorpora funcionalidades específicas para interactuar con clientes[6].

La tabla 1.1 muestra la evolución temporal de la aplicación de mensajería instantánea WhatsApp desde la constitución de la compañía en el año 2009.

Tabla 1.1. Evolución de la aplicación de mensajería instantánea WhatsApp.

#	Año	Características
1	Febrero de 2009	Se constituye WhatsApp.
2	Agosto de 2009	Se presenta el cliente móvil para IPhone.
3	Diciembre de 2009	Se añade la compartición de fotos y videos.
4	Junio de 2010.	Se añade la compartición de localización.
5	Octubre de 2010	Se presenta el cliente móvil para Android.
6	Febrero 2011	Se añaden las conversaciones de grupo.
7	Agosto 2013	Se añaden los mensajes de voz.
8	Noviembre 2014	Se añade la verificación de lectura (doble verificación o doble *check*).
9	Enero 2015	Se presenta el cliente web.
10	Abril 2016	Se añade el cifrado punto a punto.
11	Mayo 2016	Se presenta el cliente de escritorio.
12	Noviembre 2016	Se añade las video llamadas.
13	Febrero 2017	Se añade el estado de usuario.
14	Enero 2018	Se presenta el cliente específico para empresas WhatsApp Business.
15	Julio 2018	Se añade las llamadas de grupo.
16	Octubre 2018	Se añaden los *Stickers*.

En la actualidad, existe una inmensa cantidad de aplicaciones móviles de IM, si bien, genéricamente el concepto aplicación de mensajería instantánea se asocia al cliente móvil de WhatsApp. Este cliente fue uno de los primeros en aparecer en los principales mercados de aplicaciones digitales, soportando los principales sistemas operativos

[6] WhatsApp. (2019). *WhatsApp Business*. Recuperado el 5 de junio de 2019, de: https://www.whatsapp.com/business.

móviles y llegando a ser la aplicación de mensajería instantánea con mayor número de descargas y usuarios activos en el mundo.

La figura 1.3 muestra el listado de las aplicaciones móviles de mensajería instantánea más populares por número de usuarios activos mensuales a fecha de enero de 2019.

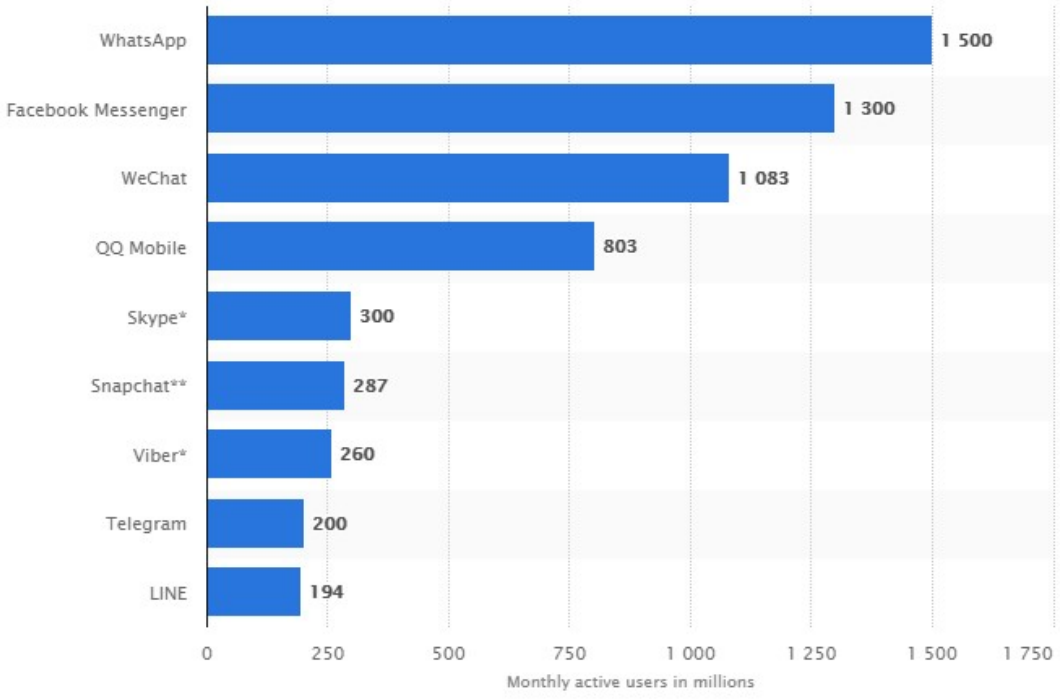


Figura 1.3. Popularidad de las aplicaciones móviles de mensajería en enero de 2019. Fuente: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/.

El impacto de este tipo de aplicaciones en nuestra sociedad queda plasmado en los diferentes informes emitidos por el Centro Criptológico Nacional, en los cuales se exponen los problemas de seguridad de aplicaciones de mensajería instantánea como Telegram Messenger (Centro Criptológico Nacional, 2017a), WhatsApp (Centro Criptológico Nacional, 2017b) o Line (Centro Criptológico Nacional, 2018c), siendo posible el robo o secuestro de cuentas de estas aplicaciones, la monitorización de usuarios o la difusión de información sensible.

Si bien, como se mostrará a continuación, las aplicaciones de IM ofrecen a sus usuarios diferentes formas de acceder a sus comunicaciones, más allá de la aplicación móvil.

1.1.2.1.1 Los clientes de las aplicaciones de IM

Inicialmente las aplicaciones de IM fueron desarrolladas para ser utilizadas desde un dispositivo móvil con sistema operativo y conexión a una red de datos, almacenando la información en el propio dispositivo. Si bien, con el paso del tiempo, muchas de estas aplicaciones de IM han ofrecido a sus usuarios múltiples formas de acceder a sus comunicaciones, independientemente del dispositivo electrónico utilizado, lo que conlleva que, de una u otra forma, una copia de los datos de usuario se encuentre alojados en la nube. De hecho, en ocasiones, la información no se almacena en el dispositivo móvil, sólo se visualiza de forma temporal.

Actualmente muchas de las aplicaciones de IM, como es el caso de WhatsApp[7] o Telegram Messenger[8], disponen de diferentes clientes para facilitar el acceso del usuario a sus comunicaciones.

- Cliente móvil para dispositivos móviles.
- Cliente de escritorio para dispositivos informáticos.
- Cliente web acceso a través de navegador de Internet con independencia del dispositivo electrónico utilizado.

En el caso de los dos primeros clientes, los mismos están disponibles para ser descargados e instalados desde los principales mercados de aplicaciones digitales (Google Play, App Store, Windows Store, etc.). En el caso del cliente web, únicamente es necesario disponer de uno los principales navegadores de Internet (Chrome, IE, Edge, Firefox, etc.).

La figura 1.4 muestra a modo de ejemplo, varios de los clientes móviles de las aplicaciones de IM que pueden ser encontradas en el mercado de aplicaciones digitales Google Play.

[7] WhatsApp. Recuperado de: https://www.whatsapp.com.

[8] Telegram Messenger. Recuperado de: https://www.telegram.org.

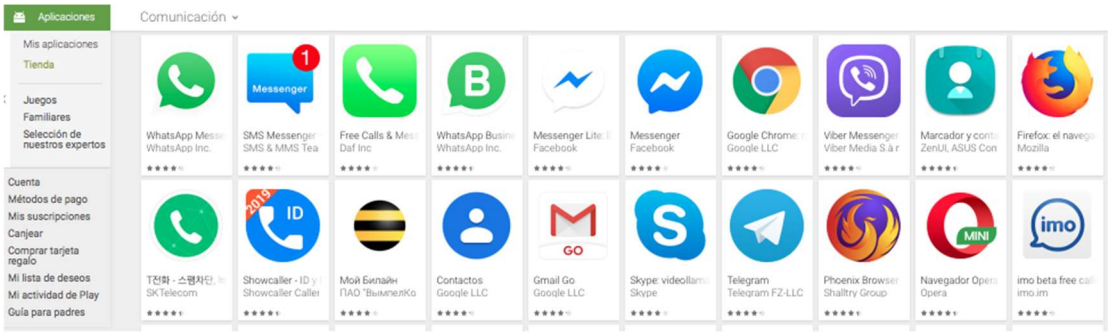


Figura 1.4. Ejemplo de listado de clientes móviles de aplicaciones de IM en Google Play. Fuente: https://play.google.com/store/apps/category/COMMUNICATION.

De igual manera en la figura 1.5 se muestra a modo de ejemplo, varios de los clientes de escritorio de las aplicaciones de IM que pueden ser encontradas en el mercado de aplicaciones digitales App Store.

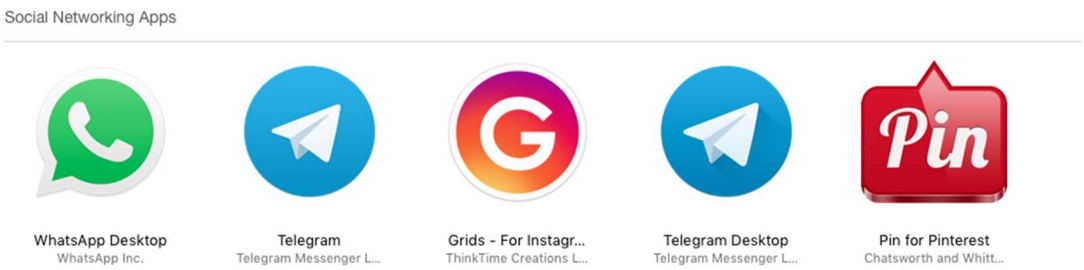
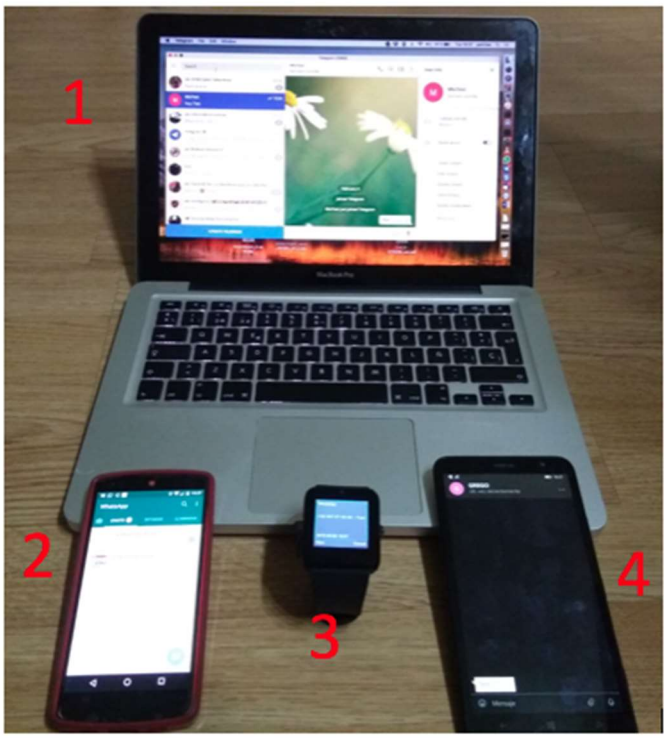


Figura 1.5. Ejemplo de listado de clientes de escritorio de aplicaciones de IM en App Store.

El hecho de que este tipo de aplicaciones de IM ofrezcan diferentes formas de acceso a las comunicaciones de usuario con independencia del dispositivo electrónico, permite hacerse una idea del impacto que tienen este tipo de aplicaciones en nuestra sociedad y de la total dependencia que los usuarios tienen de las mismas.

En la figura 1.6 se muestra a modo de ejemplo la ejecución del cliente móvil y del cliente de escritorio de dos de las principales aplicaciones de mensajería instantánea que existen en la actualidad. En esta figura se identifica el cliente móvil de la aplicación de IM WhatsApp en un teléfono inteligente con Android, el cual se encuentra a su vez vinculado con un reloj inteligente con sistema operativo Nucleus RTOS, replicando esas notificaciones. Además, se observa el cliente móvil de la aplicación de IM Telegram

Messenger en el teléfono inteligente con Windows Phone y el cliente de escritorio de la aplicación de IM Telegram Messenger en el ordenador portátil con macOS.



1. Cliente de escritorio de la aplicación de IM Telegram Messenger en ordenador con S.O. macOS.
2. Cliente móvil de la aplicación de IM WhatsApp en teléfono inteligente con S.O Android.
3. Notificaciones del cliente móvil WhatsApp (Android) recibidas en reloj inteligente con S.O. Nucleus RTOS.
4. Cliente móvil de la aplicación de IM Telegram Messenger en teléfono inteligente con S.O. Windows Phone.

Figura 1.6. Ejemplo de la ejecución del cliente móvil y de escritorio de varias aplicaciones de mensajería instantánea.

Los proveedores de estos servicios de mensajería instantánea informan que, tanto los datos transmitidos como los alojados en sus servidores se encuentran cifrados, no pudiendo tener acceso al contenido de estos y por consiguiente no pudiendo proporcionar las comunicaciones transmitidas por este tipo de aplicaciones a la autoridad policial o judicial que las solicite. En este sentido, como se reflejará en adelante, se hace imprescindible el análisis forense de los dispositivos electrónicos intervenidos en la comisión de hechos delictivos para poder extraer la información de estas aplicaciones de IM, siendo este uno de los motivos por el cual surge la presente Tesis.

1.2 La comisión de hechos delictivos a través de las aplicaciones de IM

Una vez visto un resumen sobre las aplicaciones de IM y su impacto en la sociedad actual, nuestro análisis se centrará en la implicación que tienen este tipo de aplicaciones en la comisión de hechos delictivos.

Actualmente, resulta extraño el hecho delictivo en el cual no esté incluido un dispositivo electrónico, ya sea de forma directa o indirecta. En los últimos años, la perpetración de tales hechos viene sufriendo un cambio en cuanto al modo y medios utilizados para su comisión, encontrándose las TIC entre las herramientas empleadas para la comisión de estos.

La figura 1.7 muestra a modo de ejemplo, la imagen del material intervenido en un presunto delito de distribución de billetes falsos. En esta imagen, se observa además de otros elementos, diferentes dispositivos electrónicos como equipos informáticos, dispositivos móviles e impresoras utilizados para la comisión del delito.

Figura 1.7. Desarticulada una organización criminal dedicada a la distribución de billetes falsos de 200 euros por España. Fuente: https://www.policia.es/prensa/20130110_1.html.

La relevancia de la comisión de delitos a través de las TIC, se muestran en las modificaciones sufridas por la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. En tal sentido, en el Libro II de la última modificación de esta LO de fecha 21 de febrero de 2019, hace referencia explícita a los delitos cometidos a través de los medios telemáticos.

- ✓ Título VI. Capítulo II. De las amenazas. Art. 169 del CP. En este artículo se tipifican delitos como el acoso a través de medios telemáticos (*Ciberbullying*), hecho por el cual se puede provocar un maltrato físico, verbal o psicológico de forma reiterada a través de medios telemáticos. Este artículo expone que:

  > El que amenazare a otro con causarle a él, a su familia o a otras personas con las que esté íntimamente vinculado un mal que constituya delitos de homicidio, lesiones, aborto, contra la libertad, torturas y contra la integridad moral, la libertad sexual, la intimidad, el honor, el patrimonio y el orden socioeconómico, será castigado: (…)
  > Las penas señaladas en el párrafo anterior se impondrán en su mitad superior si las amenazas se hicieren por escrito, por teléfono o por cualquier medio de comunicación o de reproducción, o en nombre de entidades o grupos reales o supuestos. (Boletín Oficial del Estado, 2019a, p.61).

- ✓ Título VI. Capítulo III. De las coacciones. Art. 172 ter del CP. En este artículo se tipifican delitos como el acoso ilegitimo (*Ciberstalking*), hecho por el cual, a través de medios telemáticos, se puede producir un hostigamiento, vigilancia o persecución hacia una persona determinada de forma reiterada. Este artículo expone que:

  > Será castigado con la pena de prisión de tres meses a dos años o multa de seis a veinticuatro meses el que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo

de su vida cotidiana:

1.ª La vigile, la persiga o busque su cercanía física.

2.ª Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas. (Boletín Oficial del Estado, 2019a, p.64).

- ✓ Título VII. Capítulo II bis. De los abusos y agresiones sexuales a menores de dieciséis años. Art. 183 ter del CP. En este articulo se tipifican delitos como el engaño de menores a través del uso de medios telemáticos (*Grooming*). Este artículo expone que:

(…)

1. El que, a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento (…).

2. El que, a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor. (Boletín Oficial del Estado, 2019a, p.69).

- ✓ Título XIII. Capítulo VI. De las defraudaciones. Sección 1.ª. De las estafas. Art. 248 del CP. En este articulo se tipifican delitos como la estafa a través del uso de medios telemáticos. Este artículo expone que:

(…)

1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

2. También se consideran reos de estafa:

a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo. (Boletín Oficial del Estado, 2019a, p.87).

- ✓ Título XIII. Capitulo IX. De los daños. Art. 264 ter del CP. En este articulo se tipifican delitos como los daños de sistemas informáticos a través del uso de medios telemáticos. Este artículo expone que:

Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los dos artículos anteriores:

a) un programa informático, concebido o adaptado principalmente para cometer alguno de los delitos a que se refieren los dos artículos anteriores; o

b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información. (Boletín Oficial del Estado, 2019a, p.94).

La importancia de las Tecnologías de la Información y las Comunicaciones en la comisión de hechos delictivos queda reflejada en las últimas modificaciones sufridas en el Código Penal, si bien, no solo esta Ley evidencia el cada vez más proliferante peso de las TIC en dicho tipo de actividades. Los estudios elaborados en base a la Memoria Anual de la Fiscalía General del Estado revelan un crecimiento del uso incorrecto de las TIC.

En el año 2018, la estadística judicial obtenida de la Actividad del Ministerio Fiscal[9] contabiliza un total de 8748, los procedimientos judiciales relacionados con delitos informáticos (penales, civiles y laborales), entendiendo los delitos informáticos como aquellas acciones ilegales o delictivas que se realizan a través de dispositivos electrónicos e Internet.

En la tabla 1.2 se muestra el número de procedimientos judiciales incoados por delitos informáticos a nivel nacional en 2018 clasificado por tipo delictivo y delito asociado. Esta tabla refleja como los delitos de pornografía infantil o personas con discapacidad cometidos a través de las TICs (art. 189) tienen casi un 9% de los procedimientos abiertos en el año 2018.

Tabla 1.2. Procedimientos judiciales incoados en 2018 relacionados con las TICs.

Tipo delictivo	**Delito asociado a su artículo del CP.**	**Año 2018**
Delitos contra la libertad	Amenazas/coacciones cometidos a través de las TICs (arts. 169 y ss. y 172 y ss.)	841
	Acoso cometido a través de las TICs (art. 172 ter)	336
Delitos contra la integridad moral	Trato degradante cometido a través de las TICs (art. 173)	65
Delitos contra la libertad sexual	Delitos de pornografía infantil o personas con discapacidad cometidos a través de las TICs (art. 189)	727
	Acoso a menores de 16 años a través de las TICs (art. 183 ter)	122
	Cualquier otro delito contra la libertad sexual cometido a través de las TICs	323
Delitos contra la intimidad	Ataques a sistemas informáticos/interceptación transmisión datos (arts. 197 bis y ter)	76
	Descubrimiento y revelación de secretos a través de las TICs (art. 197)	419
Delitos contra el honor	Calumnias/injurias contra funcionario o autoridad cometidas a través de TICs (art. 215)	159
Delitos contra el patrimonio	Estafa cometida a través de las TICs (art 248 y 249)	5405
	Descubrimiento de secretos empresariales (art 278 y ss.)	25
	Delitos contra los servicios de radiodifusión e interactivos (art 286)	9
	Delitos de daños informáticos (arts. 264, 264 bis y 264 ter)	64
	Delitos contra la propiedad intelectual en la sociedad de la información (art. 270 y ss.)	36
Delitos de falsedad	Falsificación a través de las TICs	49
Delitos contra la constitución	Delitos de discriminación cometidos a través de las TICs (art. 510)	92
Total		**8748**

[9] Poder Judicial España. (2019). *Compendios Delitos – Año 2018*. Recuperado el 10 de septiembre de 2019, de: http://www.poderjudicial.es/cgpj/es/Temas/Estadistica-Judicial/Estadistica-por-temas/Datos-penales--civiles-y-laborales/Delitos-y-condenas/Actividad-del-Ministerio-Fiscal/.

De igual manera, los estudios estadísticos elaborados por el Ministerio del Interior[10] reflejan que, se dieron un total de 81.307 hechos conocidos por infracciones penales relacionadas con la cibercriminalidad en el año 2017. En estos estudios, tal y como se refleja en la tabla 1.3, se observa que existe un incremento en el número de hechos por delitos informáticos entre los años 2012 a 2017. En esta tabla se observa como existe un repunte de casos entre los años 2016 y 2017 de casi 15.000 casos.

Tabla 1.3. Estadísticas del Ministerio del Interior relacionadas con la cibercriminalidad entre 2017 y 2012.

Tipo delictivo	**2017**	**2016**	**2015**	**2014**	**2013**	**2012**
Acceso e interceptación ilícita	2.505	2.579	2.386	1.851	1.805	1.701
Amenazas y coacciones	11.270	11.473	10.112	9.559	9.064	9.207
Contra la propiedad industrial/intelectual	1.537	1.524	2.131	2.212	1.963	1.891
Contral el honor	109	121	167	183	172	144
Delitos sexuales	1.312	1.188	1.233	974	768	715
Falsificacion informatica	2.961	2.697	2.361	1.874	1.608	1.625
Fraude informático	60.511	45.894	40.864	32.842	26.664	27.231
Interferencia en los datos y en el sistema	1.102	1.110	900	440	359	298
Total	**81.307**	**66.586**	**60.154**	**49.935**	**42.403**	**42.812**

Las modificaciones sufridas en el CP sumado a los diversos estudios estadísticos del Ministerio Fiscal y del Ministerio del Interior relativos a los delitos informáticos, refleja de manera clara un incremento en la comisión de hechos delictivos a través de las TIC en nuestra sociedad. Dicha actividad delictiva implica que, cada vez sea más frecuente la aportación de pruebas de origen digital o pruebas electrónicas en los procesos judiciales, la cual es considerada a toda aquella información con valor probatorio contenida en un dispositivo electrónico o transmitida a través de este.

[10]Ministerio del Interior. (2019). *Hechos conocidos de infracciones penales relacionadas con la cibercriminalidad por provincias, grupo penal y periodo (2017-2012)*. Recuperado el 10 de septiembre de 2019, de: https://estadisticasdecriminalidad.ses.mir.es/jaxiPx/Tabla.htm?path=/Datos5//l0/&file=05002.px&type=pcaxis&L=0.

Debido a las especiales características de la prueba electrónica, ésta debe ser recabada con las suficientes garantías legales, garantizando en todo momento la integridad de la información. Por estos motivos se hace necesario que, para mantener el valor probatorio de la prueba electrónica, ésta sea:

- ***Lícita***. La obtención de la evidencia electrónica no pueda vulnerar bajo ningún concepto los derechos fundamentales.
- ***Integra***. Bajo ningún concepto se altere el contenido de la evidencia electrónica original (indubitada). Para ello se deberá realizar una copia forense del contenido de la evidencia original en otro soporte digital.
- ***Autentica***. Garantizado en todo momento que la copia forense realizada es idéntica de la evidencia electrónica (indubitada). La cadena de custodia permite la trazabilidad de la evidencia preservando en todo momento la autenticidad de la misma. En la cadena de custodia debe quedar reflejado y documentado en todo momento el recorrido y tratamiento que realiza de la evidencia electrónica desde su intervención hasta su entrega a la Autoridad Judicial.
- ***Clara***. La evidencia electrónica deba ser comprendida por todos los intervinientes en el proceso judicial, ya se tenga o no conocimientos técnicos.

Se puede determinar la prueba electrónica como la recopilación o recolección de los diferentes tipos de datos de origen digital (archivos de datos, archivos multimedia, documentos ofimáticos, comunicaciones electrónicas, metadatos, páginas web, localización, etc.) contenidos localmente o transmitidos remotamente a partir del uso de dispositivos electrónicos (ordenadores, teléfonos y relojes inteligentes, tabletas o memorias USB, etc.). En este sentido, dentro de las comunicaciones electrónicas podemos encontrar aquellas mantenidas a través de las aplicaciones mensajería instantánea, las cuales pueden ser contenidas y transmitidas independientemente del dispositivo electrónico utilizado. El impacto del uso de las aplicaciones de IM como medio utilizado en la comisión de hechos delictivos queda patente en los organismos públicos encargados de su investigación. Si bien en la actualidad no se han elaborado estudios estadísticos específicos al respecto, este hecho queda reflejado en la diferente documentación publicada por estos organismos. El uso indebido de este tipo de

aplicaciones queda reflejado en multitud de investigaciones realizadas por las diferentes Fuerzas y Cuerpos de Seguridad del Estado del Ministerio del Interior y publicadas en los diferentes gabinetes de prensa.

En la página web de la Policía Nacional[11] se pueden identificar múltiples notas de prensa en las cuales se hace referencia al uso de aplicaciones de IM como herramienta principal en la comisión de hechos delictivos. En esta página web se pueden encontrar delitos relativos a la inducción de menores, al abandono de domicilio, exhibicionismo y provocación sexual tal y como queda reflejado a continuación:

> Su víctima era un chico de trece años, residente en la provincia de Toledo, con el que había contactado por primera vez en noviembre de 2012 a través de WhatsApp. Le enviaba mensajes en los que manifestaba su intención de viajar hasta su lugar de residencia para recogerlo y trasladarse ambos hasta Málaga en donde "tendrían una vida inmejorable". (Policía Nacional, 2013, p.1).
>
> En Madrid se detuvo a un joven de 25 años que, de una forma muy activa, compartía vídeos de niñas de edades comprendidas entre los diez y los doce años. Para ello contaba con diversos canales de mensajería instantánea y chats de Internet. (Policía Nacional, 2019, p.1).

Así mismo, en la página web de la Guardia Civil[12] se pueden identificar múltiples notas de prensa en las cuales se hace referencia al uso de aplicaciones de IM como herramienta en la comisión de hechos delictivos como los relacionados con la explotación sexual y corrupción de menores tal y como queda reflejado:

> La Guardia Civil, con la colaboración de Interpol y Europol, ha desmantelado una importante red internacional de producción, ten distribución de pornografía infantil a través de internet y del servicio de mensajería de Whatsapp. Han sido

[11] Policia Nacional. Recuperado de: https://www.policia.es.

[12] Guardia Civil. Recuperado de: http://www.guardiacivil.es.

> detenidas e investiga personas en España e identificados más de 400 usuarios en distintos países. (Guardia Civil, 2018, p.1).

En este sentido, y de igual manera que en el caso de las FFCCSE, el uso incorrecto de las aplicaciones de IM queda también reflejado en las múltiples sentencias publicadas a través del Centro de Documentación Judicial (CENDOJ)[13] del Consejo General del Poder Judicial (CGPJ). En el listado de delitos cometidos en el año 2019 y en los cuales está incluida una aplicación de mensajería instantánea como medio de prueba se encuentran sentencias a delitos relativos con las coacciones o con la explotación sexual:

> El acusado en el periodo comprendido entre el 18/3716 y 26/9/16 mientras estaba en proceso de separación judicial envió una serie de comunicaciones a la Sra. Marcelina desde el email DIRECCION000 o vía whatsapp con intención de humillarla. (Romera, M.C. 2019, p.1)
>
> En el marco de la investigación llevada a cabo a nivel nacional por la Brigada Central de Investigación Tecnológica sobre la proliferación de grupos dedicadas a la producción y distribución de pornografía infantil a través de mensajería instantánea WhatsApp formado por usuarios de cualquier lugar del mundo en los que cualquiera de los participantes podía ver, descargar y modificar el contenido, se accedió al enlace a uno de estosgrupos. (Perez, V., 2019, p.1)

En la actualidad las comunicaciones mantenidas a través de las aplicaciones de mensajería instantánea están adquiriendo una gran transcendencia en la investigación de hechos delictivos lo que implica que la obtención de estas deba realizarse respetando en todo momento el valor probatorio de esta prueba electrónica. La forma de obtener las comunicaciones de este tipo de aplicaciones difiere bastante de la realizada sobre las comunicaciones tradicionales. En el caso de estas últimas, las comunicaciones (llamadas telefónicas, mensajes de texto, etc.) son almacenadas por el operador telefónico, pudiendo obtener una copia de las mismas previa mandamiento judicial tal y como queda reflejado

[13] Poder Judicial. Recuperado de: http://www.poderjudicial.es/search/indexAN.jsp.

en el Informe Transparencia Comunicaciones de Telefónica del año 2019[14], en el cual fija en 34252 el número total de peticiones de interceptación legal de las comunicaciones solicitadas por los Juzgados de Instrucción españoles. Sin embargo, en el caso las comunicaciones mantenidas a través de las aplicaciones de mensajería instantánea, estas son almacenadas de manera cifrada y temporal en los servidores remotos del proveedor de este tipo de aplicaciones, imposibilitando la obtención de una copia de estas aun con mandamiento judicial. De estas limitaciones se hace eco la Unidad de Criminalidad Informática de la Fiscalía General del Estado, tal y como se refleja a continuación:

> En relación con ello, y comenzando por la primera modalidad, ha de tenerse en cuenta que tanto Whatsapp (disponible para terminales móviles con sistema operativo IOS, Blackberry, Android, Symbian y Windows Phone) como los similares sistemas de mensajería instantánea (Line, Telegram…) son aplicaciones que operan por la red móvil o wiffi. Sin perjuicio de ello, Whatsapp actualmente puede también ser usado, visualizado y sincronizado en cualquier PC tras la implementación de la WhatsApp Web. Este tipo de aplicaciones de mensajería multiplataforma presentan determinadas notas características que habrán de tenerse en cuenta a estos efectos.
>
> a) (...). ☒
>
> b) No existe un servidor externo que conserve la información sobre los contenidos de los mensajes, sino que la misma se encuentra alojada -generalmente una vez ha sido encriptada- únicamente en las bases de datos alojadas en los propios dispositivos utilizados para llevar a efecto la transmisión o, en su caso, accesibles desde los mismos cuando se haya configurado la aplicación para hacer copias en la nube. (FISCALÍA GENERAL DEL ESTADO, 2016, p.3-4).

[14] Telefonica España. (2019). *Informe Transparencia Comunicaciones de Telefonica 2019*. Recuperado el 21 de noviembre de 2019, de: https://www.telefonica.com/documents/153952/183394/Informe-Transparencia-Comunicaciones-2019.pdf/00cb6cba-dbe7-df8d-64d1-df8510830960.

En este sentido, cuando se trata de delitos cometidos a través de las aplicaciones de mensajería instantánea, la adquisición de las comunicaciones mantenidas a través de este tipo aplicaciones quedara acotada, bien al acceso proporcionado voluntariamente por el propio usuario a sus comunicaciones, o bien al análisis forense de los dispositivos electrónicos personales intervenidos (aprehensión de dispositivos y acceso a la información). En cuanto al registro de dispositivos de almacenamiento masivo de información incluidos en la investigación de hechos delictivos se estará a lo dispuesto en lo descrito en el Capítulo VII. Título VIII del Libro II articulo 588 sexies introducido por la L.O 13/2015 de 5 octubre, que modifica la LECrim (Boletín Oficial del Estado, 2015); así como a la Circular 5/2019, de 6 de marzo, de la Fiscal General del Estado (Boletín Oficial del Estado, 2019b).

En base a esta normativa, y para su aplicación, podríamos subdividir la práctica del registro en dos fases:

- ✓ Primera fase: Intervención o aprehensión del dispositivo electrónico
- ✓ Segunda fase: Acceso a la información contenida en estos dispositivos.

En relación a la primera fase, los investigadores tecnológicos de estas nuevas formas delictivas deben transformarse, adaptándose a investigación de los delitos cometidos a través de las TIC, realizando las pertinentes pesquisas tanto en el mundo real como en el mundo digital o virtual, verificando identidades digitales, correos electrónicos, contenido multimedia, conversaciones, direcciones IP, posicionamientos, etc., reconstruyendo los hechos e interviniendo los dispositivos electrónicos involucrados en la comisión de hechos delictivos. En relación con la segunda fase, el acceso al dispositivo electrónico se asocia con la Informática Forense, disciplina de las Ciencias Forenses, la cual utiliza procedimientos científicos para adquirir y analizar la información contenida en el interior de los dispositivos electrónicos intervenidos, manteniendo en todo momento a través de la cadena de custodia el valor probatorio de la prueba electrónica.

1.3 Las Ciencias Forenses en el ámbito digital: Informática Forense

El término de Ciencias forenses engloba al conjunto de disciplinas científicas que aplica conocimientos y métodos científicos al objeto de determinar las circunstancias exactas de la comisión de un hecho delictivo e identificar a sus autores en base a los vestigios producidos en el delito. Dentro de las disciplinas que se incluyen en las Ciencias Forenses se encuentran áreas tan diversas como la biología, la química, la acústica, la fotografía, la antropología, la entomología, la informática o la balística, siendo la diversidad de casos sustentados a través de estas disciplinas tan amplia como las casuísticas en la comisión del delito.

La Informática Forense conocida en inglés como *Digital forensics*, se identifica como la ciencia forense que aplica los conocimientos y métodos científicos sobre evidencias electrónicas contenidas y/o transmitidas en la comisión de delitos informáticos. La Informática Forense se sirve de procedimientos y técnicas forenses para adquirir, preservar, analizar, documentar y presentar la información digital obtenida de dispositivos electrónicos incluidos en la investigación de hechos delictivos, garantizando en todo momento la trazabilidad de la prueba electrónica a partir de la cadena de custodia de las evidencias electrónicas estudiadas. Los procedimientos y técnicas forenses utilizadas en el tratamiento de evidencias electrónicas deben responder a métodos científicos, los cuales deben ser auditables, reproducibles y defendibles.

A continuación, se describen, de manera general, estos procedimientos:

- ***Adquisición***. La adquisición es el procedimiento forense por el que se realiza una copia del contenido de las evidencias, el cual debe ser reproducible y repetible. Existen diversos tipos de adquisición (manual, lógica, sistema de archivos o física), si bien, el objetivo principal de la misma es, obtener una copia de la información almacenada en la evidencia electrónica, evitando cualquier tipo de alteración de los datos. En el proceso de adquisición se debe verificar que la información contenida en la evidencia origen es igual a los datos adquiridos, utilizándose para esta comprobación el cálculo de una función matemática (función matemática *hash*). Dependiendo del tipo de adquisición realizada, el

proceso de análisis y recuperación de información será más o menos completo. En la adquisición de evidencias electrónicas se utilizan diversas soluciones forenses, como bloqueadores contra escritura o clonadoras, que automatizan este proceso y las cuales permiten mantener el valor probatorio de la prueba electrónica. Existen diversas guías en las cuales se exponen los procedimientos y estándares que deben ser seguidos para la adquisición en comunicaciones y tecnología (Internet Engineering Task Force, 2002).

- ***Preservación***. Se entiende como preservación, al procedimiento forense por el cual se debe garantizar la inmutabilidad de la evidencia electrónica. De este modo, aparece el concepto de cadena de custodia, como aquel proceso que debe ser seguido por todos los intervinientes desde el momento de la adquisición de una evidencia electrónica hasta el momento de entrega a la Autoridad Judicial. El objeto principal de la cadena de custodia es el control en todo momento de la evidencia electrónica, reflejando cualquier cambio en cuanto a su custodia en un acta que deberá ser adjuntada a las diligencias, indicando lugar de depósito, fecha y hora de entrada y salida, persona que entrega y que se hace cargo, estado de la evidencia, etc. (International Organization for Standardization, 2013).

- ***Análisis***. El análisis corresponde al procedimiento por el cual se realiza un examen, a través de técnicas de investigación científica, de los registros o artefactos generados en una evidencia electrónica. Este análisis debe responder a cuestiones tan diversas como el qué, quién, cuándo o el cómo se causó/tuvo lugar un hecho delictivo. El análisis de evidencias electrónicas es bastante complejo, en gran medida debido a la diversidad de dispositivos, sistemas operativos, aplicaciones, capacidad de almacenamiento, volumen y volatilidad de los datos que deben ser examinados. Esto implica que, en la actualidad no haya un estándar o metodología que pueda ser utilizado de manera global en el análisis de evidencias electrónicas. Numerosas organizaciones desarrollan diversas guías de buenas prácticas, en las cuales se expone de manera general los procedimientos de análisis seguidos en la obtención y recuperación de rastros digitales (Asociación Española de Normalización, UNE, 2013d). En la actualidad, el

análisis queda supeditado en muchas ocasiones al uso de soluciones forenses (hardware y software), soluciones específicamente diseñadas para automatizar los procesos de identificación, decodificación e interpretación de artefactos generados en una evidencia electrónica. Estas herramientas son capaces de procesar la información, indexando datos, realizando búsquedas predefinidas, extrayendo datos y metadatos de múltiples tipos de archivos, identificando múltiples sistemas de archivos, identificando programas instalados, ejecutados, o eliminados, recuperando registros de llamadas, mensajes de texto, extrayendo conversaciones mantenidas a través aplicaciones de IM, correos electrónicos o histórico de navegación web, identificando datos de sesión de usuario (fechas de conexión o desconexión, número de inicio de sesión fallidas, cambio de contraseñas, etc.), elementos eliminados específicamente por un usuario e incluso recuperar información eliminada, si bien, el resultado de este análisis depende en gran medida de las soluciones forenses utilizadas, siendo una buena práctica forense el uso de varias soluciones para el análisis de una evidencia electrónica, así como el examen de sus resultados.

En el caso específico de las aplicaciones de mensajería instantánea, la necesidad de identificar, decodificar e interpretar las comunicaciones mantenidas a través de este tipo de aplicaciones de manera correcta, precisa, clara y concisa, dota de especial importancia el análisis forense de sus registros o artefactos. La identificación de usuarios, decodificación de mensajes o estados, así como la interpretación de fechas es de suma importancia cuando se trata del análisis forense de este tipo de aplicaciones.

- ***Documentación***. En muchas ocasiones la documentación se asocia a la presentación o generación del informe pericial, si bien este, corresponde al proceso por el cual se debe registrar de manera metódica y detallada la secuencia de procesos seguidos durante el análisis forense. La documentación conlleva de forma implícita la trazabilidad de las evidencias electrónicas analizadas, por tal motivo, desde la recepción de la muestra hasta la finalización del análisis forense, se deben referenciar los procesos y herramientas utilizadas. De este modo se establece una relación entre la información obtenida y los procesos y herramientas utilizadas, asegurando de esta forma que cualquier especialista forense digital

pueda repetir la investigación y obtener los mismos resultados. En este sentido, la documentación puede ser utilizada tanto para el control de la evidencia (recepción, registro, estado o situación), como el registro de su tratamiento (volcado, imagen forense, análisis realizado, herramientas utilizadas, resultado, etc.). En el caso del tratamiento de la evidencia, es fundamental documentar tanto las soluciones forenses y versión utilizadas como el resultado obtenido, ya que, con cada nueva versión, las soluciones forenses añaden nuevas capacidades que pueden dejar obsoleto el análisis realizado.

- ***Presentación***. La presentación corresponde a proceso en el cual se expone y refleja todo el conocimiento que tiene el especialista forense digital de la evidencia electrónica objeto de análisis. En este sentido el artículo 478 de la LECrim dice que:

> El informe pericial comprenderá, si fuere posible:
>
> 1º. Descripción de la persona o cosa que sea objeto del mismo, en el estado o del modo en que se halle. El Secretario extenderá esta descripción, dictándola los peritos y suscribiéndola todos los concurrentes.
>
> 2º. Relación detallada de todas las operaciones practicadas por los peritos y de su resultado, extendida y autorizada en la misma forma que la anterior.
>
> 3º. Las conclusiones que en vista de tales datos formulen los peritos, conforme a los principios y reglas de su ciencia o arte. (Boletín Oficial del Estado, 2015, p. 90)

El informe pericial es aquel documento que muestra los aspectos más importantes del análisis forense realizado sin entrar en una exposición demasiado técnica. Este informe debe ser muy claro y conciso, y no debe exponer bajo ningún concepto ideas o suposiciones por parte del especialista. El formato de este informe puede variar, si bien, como norma general siempre debe contener los antecedentes del hecho, objeto del estudio, estudios realizados, resultados obtenidos y las

conclusiones. De igual manera, es recomendable realizar un segundo informe interno o informe técnico, en el cual, se expondrá de forma detallada y minuciosa el análisis forense realizado, resaltando los procedimientos técnicos realizados (simulación de entorno, búsquedas específicas de patrones, recuperación en crudo de información, transformación de datos, etc.) para posibles reproducciones y exponiendo los resultados, tanto positivos como negativos, obtenidos del examen realizado.

Si bien los procesos expuestos son ampliamente conocidos en Informática Forense, la evolución de las TIC, con la continua aparición de nuevos dispositivos electrónicos y de servicios alojados en la nube, y su uso en la comisión de hechos, implica que, las metodologías forenses utilizadas en estos procesos deban adaptarse de manera constante, ajustándose a la realidad de la situación. En este sentido, existen diversos organismos independientes, los cuales publican estándares o guías de buenas prácticas en los cuales se muestran los procedimientos forenses seguidos para el tratamiento de evidencias digitales, y que pueden ser utilizadas por los especialistas forenses digitales, en caso de no disponer de protocolos propios, al objeto de, a partir de métodos científicos, adquirir, preservar, analizar, documentar y presentar de manera correcta la información ubicada en las evidencias objeto de análisis.

1.4 Resumen. Contenidos de la memoria.

En este primer capítulo se ha expuesto de forma teórica la evolución de las TIC e Internet, así como su impacto en la sociedad actual. Se ha introducido el concepto de aplicación de mensajería instantánea, haciendo hincapié en la relevancia que tiene en la actualidad el uso de este tipo de aplicaciones en la comisión de hechos delictivos.

Por último, se ha realizado una somera introducción a los procedimientos forenses seguidos en el tratamiento de evidencias electrónicas, como parte de la Informática Forense, los cuales sostienen el valor probatorio de la prueba electrónico en los procesos judiciales.

A continuación, en la memoria de la tesis doctoral se presentan los contenidos siguientes:

- El capítulo 2 revisa el estado de la cuestión en relación con el análisis forense de las aplicaciones de IM. Se revisan las metodologías de análisis actuales y se fundamenta la motivación del trabajo de investigación que se persigue con la realización de la presente tesis doctoral.
- El capítulo 3 propone una metodología de análisis particular para las nuevas aplicaciones de IM incorporando al análisis el estudio de fuentes abiertas, artefactos y código fuente. En los siguientes capítulos se particulariza esta metodología de análisis forense para diferentes dispositivos electrónicos.
- En el capítulo 4 se presenta el análisis forense de aplicaciones IM en teléfonos inteligentes. Este tipo de dispositivos es el más frecuente a la hora de recabar información de estas aplicaciones por parte del perito forense. Se estudiarán los casos de sistemas operativos de dispositivos móviles como son Android y Windows Phone para la aplicación IM Telegram Messenger.
- En el capítulo 5 se particulariza el análisis en los rastros y evidencias digitales de aplicaciones IM instaladas en ordenadores. Se plantean diferentes escenarios de análisis de aplicaciones IM como WhatsApp y Telegram sobre MacOS, buscando en lo posible contribuir y proporcionar novedades en el campo de las pericias informáticas forenses.
- En el capítulo 6 se enfoca el análisis a otro tipo de dispositivos como son los relojes inteligentes. En particular a aquellos relojes que son de bajas capacidades y que no disponen de un sistema operativo tipo Android si no un sistema operativo propietario con unas funcionalidades básicas pero que pueden proporcionar igualmente una información importante en un análisis forense de los datos de aplicaciones IM.
- El último capítulo de la tesis resume las principales contribuciones que se derivan del desarrollo de la tesis doctoral, presenta las conclusiones del análisis realizado y propone algunas líneas de trabajos futuros.
- Adicionalmente, la memoria se completa con un anexo donde se revisan las publicaciones que se han realizado a lo largo del desarrollo de la tesis doctoral, indicando brevemente los contenidos de cada una de ellas.

2 ESTADO DE LA CUESTION

En este segundo capítulo de la memoria de la tesis doctoral, se expone el estado de la cuestión relativo a la situación del análisis forense de aplicaciones de IM, desde la identificación y decodificación de sus artefactos, hasta la interpretación de la información. Se describirá la situación actual del análisis forense de evidencias digitales, a través de las diferentes estándares y guías de buenas prácticas, tanto internacionales como nacionales, así como las metodologías utilizadas en los estudios técnico-forenses de diversos investigadores para identificar, decodificar e interpretar los artefactos generados por las aplicaciones de IM. Finalmente se desarrollarán las razones fundamentales por las que se lleva a cabo la presente investigación.

2.1 El análisis forense de las aplicaciones de IM

Las aplicaciones de IM han transformado la manera que tiene la sociedad de comunicarse en la actualidad, llegando a sustituir medios de comunicación utilizados como las llamadas telefónicas, los mensajes de texto o el correo electrónico. El mal uso que se realiza en ocasiones de este tipo de aplicaciones implica que, desde el punto de vista de la informática forense se deban desarrollador procedimientos científicos, los cuales respeten en todo momento el valor probatorio de esta prueba electrónica. La identificación, decodificación e interpretación de los registros generados por este tipo de aplicaciones son de vital importancia. Así queda reflejado en los numerosos procedimientos judiciales en los cuales se solicita como objeto del informe pericial, la adquisición, análisis y recuperación de la información relativa a las comunicaciones mantenidas a través de los dispositivos electrónicos.

La cantidad de aplicaciones de mensajería instantánea que existen en la actualidad sumada a la velocidad con la cual se actualizan de versión, hace que sea sumamente complicado el análisis forense de cada una de las versiones de este tipo de las aplicaciones de mensajería instantánea tal y como se indica:

> The frequent updates of IM clients will require you to be able to properly test each client to ensure that the results returned from any tool or method used are accurate. We recommend that you use a docmented methodology for testing. This can help ensure you are not embarrassed or wrong ni any conclusions you draw base on an analysis of an IM client (Luttgens, J. T., Pepe, M., & Mandia, K., 2014, p. 529).

Así mismo, en la actualidad este tipo de aplicaciones brindan a sus usuarios de diversos clientes (móvil, escritorio, web), los cuales permiten el acceso a sus comunicaciones con independencia del dispositivo electrónico o sistema operativo.

El análisis forense de las aplicaciones de IM debe afrontarse desde una perspectiva mucho más global que el realizado sobre otro tipo de aplicaciones. El acceso a través de diferentes clientes implica que, pueda existir más de una fuente de datos para el análisis forense de este tipo de aplicaciones, no limitándose a un único dispositivo electrónico como sucede con otras aplicaciones. El análisis forense de las aplicaciones de IM debe ser integral a todos aquellos dispositivos electrónicos en los cuales puedan ejecutarse sus clientes, así como cualquier otro dispositivo en el que se puedan replicar las comunicaciones del usuario. Si bien el dispositivo electrónico por antonomasia de este tipo de aplicaciones es el teléfono inteligente, en múltiples ocasiones a partir de la intervención de otros dispositivos electrónicos (ordenadores, tabletas, relojes inteligentes, etc.), se pueden obtener toda aquella información que no puede ser extraída del análisis forense del primero.

¿Pero qué sucede cuando se debe analizar de manera forense una nueva aplicación de IM o una nueva versión no soportada por las soluciones forenses? ¿Cuál es la metodología que se debe utilizar para identificar, decodificar e interpretar de manera forense los artefactos generados por este tipo de aplicaciones con independencia del dispositivo electrónico?

En las siguientes secciones, se describirá el estado de la cuestión relativo a la metodología utilizada para el análisis forense de las aplicaciones de IM. Se expondrán los diferentes estándares y guías de buenas prácticas utilizadas para el análisis forense de evidencias

digitales, tanto a nivel internacional como nacional, así como las metodologías utilizadas por diferentes investigadores en el análisis forense de las aplicaciones de IM.

2.1.1 Estándares y guías de buenas prácticas internacionales

A continuación, se enumeran y describen varios de los estándares y guías de buenas prácticas existentes a nivel internacional.

2.1.1.1 International Organization for Standardization (ISO)

Una de las principales organizaciones internacionales de estándares es ISO - International Organization for Standardization[15]. Esta organización dispone de diversa documentación en la cual se exponen los estándares o guías de buenas prácticas a seguir en los procedimientos relativos a la gestión y análisis forense de evidencias digitales.

La norma *ISO/IEC 27037:2012 Guidelines for identification, collection, acquisition and preservation of digital evidence* (International Organization for Standardization, 2012) publicada por ISO, proporciona las directrices necesarias para la identificación, recogida, adquisición y preservación de evidencias digitales. Este estándar se centra en el manejo de las evidencias digitales y en los procedimientos de intercambio de las mismas, los cuales deben respetar en todo momento la cadena de custodia de la evidencia, preservándolas de cualquier tipo de manipulación.

La norma ISO/IEC 27042:2015 *Guidelines for the analysis and interpretation of digital evidence* (International Organization for Standardization, 2015a) publicada por ISO y ratificada también por AENOR en diciembre de 2016 (UNE-EN ISO/IEC

[15] International Organization for Standardization. Recuperado de, https://www.iso.org/home.html.

27042:2016[16]), proporciona las directrices necesarias para el análisis e interpretación de evidencias digitales. En esta norma se desarrollan los procesos seguidos para la selección, diseño, implementación de procesos analíticos y recopilación de información necesarios para el desarrollo del análisis e interpretación de evidencias digitales. La norma deja patente la complejidad que existe en los procesos, e indica que, ante la necesidad de aplicar o incorporar nuevos métodos de análisis e interpretación, estos deben estar justificados, demostrando que los mismos son adecuados para el propósito que se persigue.

La norma ISO/IEC 27042:2015 describe los procesos de:

- ***Análisis***, como el procedimiento en el cual se identifican los artefactos o registros ubicados en una evidencia digital. En el proceso de análisis, la norma diferencia dos modelos analíticos.
    - ***Análisis estático***, como la inspección de datos (contenido de ficheros de log, de paquetes de red o de volcados de memoria, etc.) y metadatos (permisos y fechas de ficheros, etc.) que se ejecuta sobre sistema apagados. Este análisis se realiza sobre la copia o imagen forense de la evidencia original.
    - ***Análisis en vivo***, como la inspección de datos y metadatos que se ejecuta sobre sistemas encendidos, el cual se subdivide en:
        - Análisis en vivo de sistemas que no pueden ser copiados. Este análisis se realiza cuando, por razones técnicas u operacionales, es necesario inspeccionar un sistema encendido. Dicho análisis implica el riesgo de modificación de la evidencia original, motivo por el cual, debe ser documentado cualquier tipo de operación llevada a cabo sobre el sistema encendido.
        - Análisis en vivo de sistemas que pueden ser copiados. Este análisis se realiza emulando el sistema original a partir de una copia o imagen forense de la evidencia original. Este tipo de análisis no

[16] Una Norma Española. (2016). *UNE-EN ISO/IEC 27042:2016 (Ratificada). Directrices para el análisis y la interpretación de las evidencias electrónicas. (ISO/IEC 27042:2015) (Ratificada por AENOR en diciembre de 2016.)*. Recuperado el 6 de octubre de 2019, de: https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0057471.

implica el riesgo de modificar la evidencia original, si bien, debe realizarse con las garantías necesarias.

- ***Interpretación***, como el procedimiento en el cual se evalúa la información obtenida en el proceso de análisis, al objeto de obtener el significado de los hechos ocurridos en la evidencia digital en su conjunto.

La norma ISO/IEC 27042:2015 no hace mención específica a las herramientas que deben ser utilizadas en los procesos de análisis e interpretación, si bien, indica que la combinación de *software* y *hardware*, deben ser acordes a los requisitos establecidos en dichos procesos, siendo validadas previamente a su uso. La norma establece un marco general de actuación y unas mínimas bases para elaborar procedimientos científicos, pero no ofrece soluciones técnicas a los problemas que las aplicaciones IM actuales.

2.1.1.2 Scientific Working Group on Digital Evidence (SWGDE)

El Scientific Working Group on Digital Evidence[17] (SWGDE), es uno de los principales grupos de trabajo dedicados al análisis forense de evidencias digitales a nivel internacional. Este grupo dispone de diferentes guías de buenas prácticas, en las cuales se exponen los procedimientos que deben seguirse en la identificación, recogida, adquisición, análisis y preservación de diferentes evidencias digitales.

El documento *SWGDE Best Practices for Computer Forensic Examination* (Scientific Working Group on Digital Evidence, 2018) tiene como objeto exponer las buenas prácticas seguidas en el examen y análisis de ordenadores, así como de dispositivos de almacenamiento asociados.

Dicha guía describe dos procesos:

- ***Examen***, como el procedimiento en el cual se revisan aquellos datos que pudieran ser relevantes ubicados en una evidencia digital (artefactos de registro y de sistema operativo, metadatos, ficheros de log, navegación de Internet, correos electrónicos, ficheros eliminados, etc.).

[17] Scientific Working Group on Digital Evidence. Recuperado de, https://www.swgde.org.

- ***Análisis***, como el procedimiento en el cual se evalúa la información obtenida en el proceso de examen, interpretando los datos y obteniendo conclusiones.

Debido a la cantidad de circunstancias que pueden darse en el análisis forense de evidencias digitales, esta norma no especifica los procedimientos o soluciones forenses comerciales utilizados para el desarrollo de los procesos de examen y análisis, si bien, indica que estos deben regirse por unas buenas prácticas, documentando las situaciones encontradas durante los procesos de examen y análisis, acciones realizadas y los resultados obtenidos.

La guía *SWGDE Best Practices for Mobile Phone Examinations* (Scientific Working Group on Digital Evidence, 2013) tiene como objeto exponer las buenas prácticas seguidas en la adquisición de evidencias almacenadas en teléfonos móviles.

Esta guía describe entre otros, los procesos de:

- ***Intervención***, como el procedimiento en el cual se deben tomar las medidas oportunas para la recogida de un teléfono móvil y mantenimiento de la cadena de custodia (aislamiento de red, recogida de muestras biológicas, etc.).
- ***Adquisición***, como el procedimiento en el cual se obtiene la información obtenida en un teléfono móvil (manual, lógica, sistema de archivos, física no invasiva, física invasiva). En este proceso se hace distinción entre la obtención de datos con el teléfono encendido y apagado.
- ***Documentación***, como el procedimiento de registrar todo el proceso seguido por la evidencia digital (intervención, adquisición, etc.).

El documento *SWGDE Best Practices for the Acquisition of Data from Novel Digital Devices* (Scientific Working Group on Digital Evidence, 2017) muestra las directrices seguidas en el examen de dispositivos IoT, sistemas embebidos y otros dispositivos novedosos. Para este tipo de dispositivos, dicha guía lleva a cabo un examen previo, al objeto de obtener la mayor información posible del dispositivo intervenido (modelo, marca, producto, fabricante, puertos de comunicación, ubicación del sistema de almacenamiento, etc.).

Así mismo, esta guía describe los procesos de:

- ***Adquisición***, como el método en el cual se obtiene la información obtenida, si bien, esta guía indica que, con estos dispositivos novedosos, el proceso de adquisición debe retirarse de los procedimientos tradicionales, debiéndose evaluar y chequear las técnicas utilizadas, identificando y documentando los cambios y el impacto del uso de estas. En este sentido, hace la diferenciación entre las técnicas de adquisición utilizadas sobre el almacenamiento local del dispositivo y el almacenamiento en la nube.
- ***Análisis***, el cual no difiere de la técnica utilizada para evaluar la información obtenida expuestas en otras de las guías del SWGDE.

2.1.1.3 National Institute of Standards and Technology (NIST)

Una de las principales organizaciones de estándares tecnológicos de Estados Unidos es NIST - National Institute of Standards and Technology[18]. Este instituto dispone de diferentes guías, definidas como *NIST Special Publication (NIST SP)*, en las cuales se exponen los procedimientos que deben seguirse en el análisis forense de evidencias digitales o los procedimientos realizados para la revisión de *software* y *hardware* forense.

La guía NIST SP 800-86 *Guide to Integrating Forensic Techniques into Incident Response* (Kent, A.K., Chevalier, S., Grance, T., Dang, H., & Kent, K., 2006) publicada por National Institute Standards and Technology, proporciona las directrices necesarias para la recogida, examen, análisis y emisión de informe de evidencias digitales.

El documento NIST SP 800-86 describe estos procesos como:

- ***Recogida***, procedimiento en el cual se identifica los dispositivos electrónicos y se realiza una adquisición. El proceso de adquisición se subdivide en el desarrollo de un plan de adquisición, el proceso de adquisición y la verificación de la integridad de los datos adquiridos.
- ***Examen***, proceso en el cual se realiza una catalogación de los datos adquiridos, accediendo y extrayendo la información más importante. Según indica este documento, el proceso de examen incluye la identificación de los ficheros a través

[18] National Institute of Standars and Technology. https://www.nist.gov/.

de técnicas como la búsqueda de texto y patrones o catalogación por tipos o familias de archivos.

- ***Análisis***, procedimiento en el cual se realiza el estudio de los datos examinados para obtener unas conclusiones, identificando a todos los actores involucrados (personas, lugares, eventos, etc.).
- ***Informe***, proceso en el cual se prepara y presenta la información resultante del análisis. Según indica esta guía, el informe puede incluir explicaciones alternativas, consideraciones de audiencia e información adicional.

Así mismo, la guía NIST SP 800-86 identifica y describe, sin entrar en procedimientos o técnicas forenses para su examen o análisis, los diferentes tipos de datos que pueden ser encontrados en las evidencias digitales (datos provenientes de ficheros de datos, del Sistema Operativo, de tráfico de red, de aplicaciones o de otras fuentes de datos).

La guía NIST SP 800-101 *Guidelines on Mobile Device Forensic* (Ayers, R., Brothers, S., & Jansen, W., 2014) publicada por National Institute Standards and Technology, describe las características de los dispositivos móviles y proporciona las directrices necesarias para el análisis forense de estos. En esta guía se desarrollan los procesos de preservación, adquisición, examen y análisis, e informe de dispositivos móviles.

La guía NIST SP 800-101 expone los diferentes procedimientos utilizados para:

- ***Preservar la evidencia***; asegurando y documentando la escena o aislando el dispositivo de todo tipo de comunicación.
- ***Adquirir la evidencia***; identificando y desarrollando los diferentes métodos de adquisición (manual, lógico, JTAG, *Chip-Off*, etc.).
- ***Examinar y analizar la evidencia***; identificando, catalogando y estudiando los diferentes tipos de datos (agenda de contactos, mensajes de texto, registro de llamadas, aplicaciones, documentos, navegación web, etc.).

Así mismo, en esta guía se muestra el listado y las capacidades de las principales herramientas (UFED, EnCase Forensics, XRY, Oxygen Forensics, etc.) utilizadas para el análisis forense de dispositivos móviles.

2.1.1.4 European Network of Forensic Science Institutes (ENSFI)

ENFSI - European Network of Forensic Science Institutes[19], es una de las principales organizaciones europeas relacionadas con las Ciencias Forenses. Esta organización dispone de diversas guías de buenas prácticas, en las que se incluyen y desarrollan los procedimientos seguidos en diferentes ámbitos de las Ciencias Forenses.

La guía *Best Practice Manual for the Forensic Examination of Digital Technology* (European Network of Forensic Science Institute, 2015) tiene como objeto exponer las buenas prácticas seguidas en el análisis forense de ordenadores y teléfonos. En este documento se desarrollan los procesos seguidos para la identificación, adquisición, análisis de evidencias digitales y generación de informe.

Esta guía subdivide los procedimientos seguidos en los procesos de ***identificación y adquisición*** de evidencias digitales, entre los ejecutados fuera y dentro del laboratorio forense. Así mismo, el proceso de ***análisis*** responde a los procedimientos, en los cuales se realiza una revisión inicial e identificación de la información contenida en las evidencias digitales (aplicaciones, actividad de usuario, archivos comprimidos, archivos cifrados, etc.), para posteriormente ***evaluar e interpretar*** los datos obteniendo conclusiones. Por último, según se indica en esta guía, el informe puede constar de dos documentos, uno técnico, que refleje de manera clara todos los resultados obtenidos en el análisis de la evidencia digital y otro de opinión.

2.1.1.5 Interpol Global Complex for Innovation

La guía *Global Guidelines for Digital Forensics Laboratories* (Interpol, 2019) publicada por Interpol Global Complex for Innovation, identifica los procedimientos forenses que deben seguirse en un laboratorio para el tratamiento de las evidencias digitales. Además de aspectos relativos a la gestión del laboratorio (localización, seguridad, descripción de trabajos, equipamiento, gestión de casos, etc.), esta guía expone las herramientas necesarias y los procedimientos utilizados en los procesos de

[19] European Network of Forensic Science Institutes. http://enfsi.eu

adquisición, examen, análisis y presentación de resultados de dispositivos informáticos y dispositivos móviles.

El documento *Global Guidelines for Digital Forensics Laboratories* describe los procesos de*:*

- ***Adquisición***: Procedimiento de creación de copia forense de evidencias electrónicas en forma de imágenes forenses, preservando con ello la integridad del contenido de la evidencia original. Desarrolla el proceso de adquisición, definiendo los diferentes tipos de adquisición, así como las diferentes casuísticas que pueden darse en la adquisición de ordenadores y en dispositivos móviles.
- ***Examen*****:** Método en el cual se examina la información contenida en una evidencia electrónica encendida o apagada. En el primer caso, el sistema está ejecutándose y se pueden obtener diversa información volátil (volcado de memoria RAM, procesos en ejecución, conexiones de red, etc.). En el segundo caso, el examen se realiza sobre la imagen forense generada y se pueden obtener información no volátil (archivos borrados, ficheros encriptados, ficheros de Log, navegación de Internet, correos electrónicos, etc.)
- ***Análisis***: Consiste en categorizar los rastros digitales del examen realizado e indicar los procedimientos seguidos para identificar y extraer los datos de dispositivos informáticos (a correos electrónicos, documentos ofimáticos, imágenes y videos, navegación de Internet, aplicaciones, actividad de usuario, ficheros de log, datos encriptados, espacio sin asignar y datos remotos o ubicados en la nube), así como de dispositivos móviles (histórico de llamadas, lista de contactos, mensajes de texto y correo electrónico, ficheros multimedia (imágenes, videos, audio), navegación de Internet, archivos de conversaciones y aplicaciones de mensajería, cuentas de redes sociales, calendario y notas, conexiones, mapas y aplicaciones).
- ***Presentación***: Método en el cual se genera un documento forense con todos aquellos datos que han sido encontrados en el proceso de análisis y el resultado de este.

Con respecto a proceso de análisis que debe ser realizado sobre de las aplicaciones de IM, este documento cataloga su existencia e indica que se debe realizar una copia de seguridad

de los registros de las conversaciones o chats para su entrega como evidencia ante la Autoridad Judicial:

> There are several available chat applications and messaging apps. Example include Whatsapp, Telegram, Skype, Line, Weebo, WeChat, QQ, Windows Live Messenger, Google Talk, and BlackBerry Messenger. Users of these applications usually choose to save the chat logs. The chat logs can be used as digital evidence in court as to what the owner communicated to others. Some chat logs are backed up in the cloud or local storage such as a computer, so analysing the computer may be useful to gain more data.
>
> Messaging apps can also offer VoIP (Voice over IP) service. This enables the owner of the smartphone to communicate with many people using the IP protocol, without leaving a record in the call history of the device. The suspect may use this software to communicate with a criminal or a victim. For example, in child abuse cases, the criminal may communicate with the child using these messaging apps. (Interpol, 2019, p. 50)

2.1.2 Estándares y guías de buenas prácticas nacionales

A continuación, se enumeran y describen varios los estándares existentes a nivel nacional.

2.1.2.1 Asociación Española de Normalización y Certificación (AENOR)

La Asociación Española de Normalización y Certificación engloba el sistema de gestión de evidencias electrónicas bajo la norma UNE 71505:2013 la cual se compone de:

- *UNE 71505-1:2013: Parte 1: Vocabulario y principios generales* (Asociación Española de Normalización, UNE., 2013a).
- *UNE 71505-2:2013: Parte 2: Buenas prácticas en la gestión de las evidencias electrónicas* (Asociación Española de Normalización, UNE., 2013b).

- *UNE 71505-3:2013: Parte 3: Formados y mecanismos técnicos* (Asociación Española de Normalización, UNE., 2013c).

Estas normas marcan la directrices y buenas prácticas para la gestión de evidencias electrónicas, controles de seguridad, formatos de intercambio y mecanismos técnicos para el mantenimiento de la confiabilidad garantizando con ello la eficacia probatoria de las evidencias digitales. Así mismo, se identifica el ciclo de vida de la evidencia digital (generación, almacenamiento, transmisión, recuperación, tratamiento y comunicación) y los atributos que debe tener esta para ser confiable (autenticidad e integridad, disponibilidad y completitud, cumplimento y gestión).

La norma UNE 71506:2013. *Metodología para el análisis forense de las evidencias electrónica* (Asociación Española de Normalización, UNE., 2013d) publicada por la Asociación Española de Normalización y Certificación (AENOR), complementa a la norma UNE 71505:2013 y tiene como objetivo establecer una metodología de análisis forense de evidencias electrónicas desarrollando los procesos de preservación, adquisición, documentación, análisis y presentación de evidencias electrónicas.

En la norma UNE 71506:2013 se describen los procesos de:

- ***Preservación***, como aquel procedimiento en el cual se debe mantener en todo momento la validez y confiabilidad de las evidencias digitales.
- ***Adquisición***, como el método en el cual se realiza la copia forense de los datos contenidos en la evidencia digital original. El proceso de adquisición debe ser reproducible y repetible, siendo verificado la inalterabilidad del contenido a partir del cálculo de un algoritmo matemática o función *hash*. En el proceso de adquisición se diferencia entre la realizada en sistemas apagados y la realizada sobre sistema encendidos.
- ***Documentación***, como aquel procedimiento en el cual se realiza un control sobre todas las evidencias digitales objeto de estudio. Este proceso se realizará desde que se inicia el análisis de la evidencia hasta la entrega de la misma, indicando los procesos ejecutados, así como las herramientas utilizadas y el resultado obtenido.
- ***Análisis*** en el cual se pretende dar respuesta a diferentes preguntas relacionadas

con una intrusión en un sistema (origen y método de intrusión, fechas y horas, sistemas afectados, etc.). El análisis debe proceder, de manera metódica, auditable, repetible y defendible, a la recuperación de los ficheros borrados, estudio de las particiones y sistemas de archivos, estudio del sistema operativo, estudio de la seguridad implementada y el análisis detallado de los datos obtenidos. En relación con el análisis detallado de los datos obtenidos, este, según la norma, debe ser realizado a través de *software* contrastado en el ámbito forense. Así mismo, el análisis detallado de los datos obtenidos clasificará los datos obtenidos, pudiéndose indexar los mismos, para poder realizar búsquedas a partir del uso de palabras clave o patrones. En el análisis forense detallado de los datos obtenidos se enumeran, no entrando en detalle, los diferentes estudios que se deben realizar sobre la evidencia electrónica (información del sistema, dispositivos físicos conectados, escritorio y papelera de reciclaje, conexiones de red y tarjetas instaladas, comunicaciones llevadas a cabo desde el equipo, aplicaciones instaladas, metadatos, software de cifrado y de los ficheros y particiones cifradas, navegación por Internet, análisis de correos electrónicos o análisis de los registros de mensajería instantánea y conversaciones, junto con las listas de contactos).

- ***Presentación*** como el procedimiento de reflejar el proceso de análisis en un documento o informe pericial, el cual será enviado al organismo solicitante.

La norma UNE 197010:2015 *Criterios generales para la elaboración de informes y dictámenes periciales sobre Tecnologías de la Información y las Comunicaciones (TIC)* (Asociación Española de Normalización, UNE., 2015) tiene como objetivo definir principalmente las características particulares que engloban el informe pericial, así como la tipología del mismo, sin entrar en el desarrollo de los procesos de preservación, adquisición, análisis y documentación de las evidencias digitales expuestos en la norma UNE 71506:2013.

2.2 Metodologías utilizadas en el análisis forense de aplicaciones de IM

En cuanto al examen de los estándares y guías de buenas prácticas descritos en el punto anterior se puede concluir que estas identifican el proceso de preservación, adquisición, documentación, análisis y presentación para el correcto desarrollo del análisis forense sobre evidencias digitales. En estos estándares y guías de buenas prácticas se hace una breve mención a los procedimientos seguidos en estos procesos, si bien, en cuanto al desarrollo del proceso de análisis, se centran en gran medida en tres puntos principales, la identificación y catalogación de los artefactos, el uso de soluciones forenses validadas (*software* y *hardware*) y los conocimientos de los investigadores o especialistas forenses. Estos estándares y guías de buenas prácticas dejan patente la complejidad del análisis forense de evidencias digitales, por cuanto al número de casuísticas que pueden darse en el estudio de este tipo de evidencias. Estos estándares y guías de buenas prácticas dejan supeditado el análisis forense de las aplicaciones de IM al uso de procedimientos estándar, lejos de exponer una metodología especifica que englobe la globalidad de este tipo de aplicaciones, así como complejidad de su análisis.

Este punto expondrá la revisión del estado actual de las metodologías de análisis utilizadas por diversos investigadores para identificar, decodificar e interpretar los registros generados por las aplicaciones de mensajería instantánea en evidencias digitales a partir del uso de procedimientos forenses.

Actualmente, la metodología utilizada para el análisis forense específico de aplicaciones de mensajería instantánea se centra en el análisis comparativo de los artefactos generados por este tipo de aplicaciones. El desarrollo de esta metodología de análisis forense y la estandarización de la misma queda reflejada en los muchos estudios realizados sobre aplicaciones de mensajería instantánea llevados a cabo por diversos investigadores (Husain, M.I. & Sridhar, R., 2010; Mahajan, A., Dahiya, M., & Sanghvi, H., 2013; Anglano, C., 2014; Wu, S., Zhang, Y., Wang, X., Xiong, X., & Du, L., 2017; Yang, T. Y., Dehghantanha, A., Choo, K. R., Muda, Z., & Khan, M. K., 2016; Sgaras C., Kechadi M., & Le-Khac N., 2015; Al Mutawa, N., Baggili, I., & Marrington, A., 2012; Alghafli, K. A., Jones, A., & Martin, T. A., 2011; Onovakpuri, P., 2018; Iqbal, A., Marrington, A., & Baggili, I., 2013; Ovens, K. M., & Morison, G., 2016 y Sudozai, M. A. K., Saleem,

S., Buchanan, W. J., Habib, N., & Zia, H., 2018). Esta metodología de análisis consiste en, generar diferentes casos de uso para la aplicación de IM en un entorno de pruebas (dispositivo físico o virtual) y realizar los procedimientos de adquisición de la evidencia electrónica y de análisis forense estático de artefactos por cada uno de estos casos. De esta manera, a partir del análisis comparativo de registros, se identifican, decodifican e interpretan los datos generados, modificados o eliminados por la aplicación de IM sin verificar el resultado obtenido. Esta metodología de análisis es utilizada para obtener los registros relativos a la agenda de contactos (números de teléfono, fotografía, estado del contacto, etc.), tipos de conversaciones, mensajes intercambiados (marcas de tiempo, estado, origen, destino, contenido, etc.), recuperación de mensajes, archivos multimedia compartidos, etc., si bien, esta metodología de análisis resulta bastante compleja debido a la gran casuística.

De igual manera, la metodología de análisis utilizada se basan únicamente el uso de soluciones forenses las cuales automatizan el proceso de análisis forense de los clientes de las aplicaciones de mensajería instantánea lejos del control de los investigadores, tal y como a continuación queda reflejado:

> We use the Cellebrite UFED4PC platform (Cellebrite LTD, 2015b) to perform device memory extraction, and the UFED Physical Analyzer (Cellebrite LTD, 2015a) to decode its contents. (Anglano, C., Canonico, M., & Guazzone, M., 2016, p. 46)

> The final step of this research was to analyse the datasets using a range of forensically recognised tools (as highlighted in Table 3) and present the findings. Both indexed and non-indexed as well as Unicode and non-Unicode string searches were included as part of the evidence searches. The experiments were repeated at least thrice (at different dates) to ensure consistency of findings. (Yang, T. Y., Dehghantanha, A., Choo, K. R., Muda, Z., & Khan, M. K., 2016, p.5).

For the data extraction and analysis from the devices, we use specialised mobile forensic tools:

Cellebrite UFED Touch Ultimate -data extraction / acquisition –with the following extraction modes:

-Logical extraction: Quick extraction of target data (e.g. sms, emails, IM chats) performed at the OS level.

-File system extraction: In depth extraction of the entire file system of the device.

Cellebrite UFED Physical Analyzer -data analysis. (Sgaras, C., & Le-Khac, N., 2016, p. 5).

Several tests on Nokia mobile phones were conducted using forensically sound tools like MOBILedit, Oxygen Phone Manager, TULP 2G, MOBILedit, Seizure and Paraban Cell. **(**Onovakpuri, P., 2018, p. 120**)**

2.3 Razones fundamentales del estudio

Las aplicaciones de mensajería instantánea han ido sustituyendo progresivamente a los medios tradicionales de comunicación digital (llamadas telefónicas, mensajes de texto, mensajes multimedia, correo electrónico, etc.). Este tipo de aplicaciones se ha convertido casi en un estándar de comunicación y es ampliamente utilizado en todos los ámbitos de nuestra sociedad. Del estado de la cuestión se concluye que, las metodologías utilizadas para el análisis forense de las aplicaciones de mensajería instantánea se basan en la catalogación de artefactos más que en el desarrollo de los procedimientos científicos, que deben ser utilizados para el análisis de este tipo de aplicaciones.

A continuación, se indican las razones fundamentales que han motivado la realización de la investigación en esta tesis doctoral.

2.3.1 Incremento del uso indebido de las aplicaciones IM

El uso de las aplicaciones de IM como medio de comunicación estándar y su utilización, en ocasiones, como medio principal en la comisión de hechos delictivos implica que, este tipo de aplicaciones sean consideradas cada vez más, fuente principal de información en la investigación de delitos. Este tipo de aplicaciones son objeto de análisis forense en procesos judiciales por delitos de amenazas, coacciones, injurias, calumnias, abusos sexuales, libertad e identidad sexual, revelación de secretos e incluso homicidios y asesinatos.

2.3.2 Continua evolución de las aplicaciones de IM – necesidad de una metodología estable

En la actualidad, las aplicaciones IM implementan nuevas formas de acceso a las comunicaciones de usuario. Aplicaciones de IM como WhatsApp, Telegram Messenger o Threema, permiten el acceso a las comunicaciones de usuario, a través de su cliente móvil (teléfono inteligente), cliente de escritorio (equipo informático o cliente web (navegador web). Cada cliente de este tipo de aplicaciones genera una serie de rastros o registros distintos, relativos a las comunicaciones del usuario y a la propia aplicación de IM, dependiendo del dispositivo digital utilizado.

El análisis forense de las aplicaciones de IM no acaba al interpretar los datos relativos a las comunicaciones de un usuario, siendo necesario además el estudio de todos aquellos registros que genera la propia aplicación, exportando toda esa información en un formato humano legible y mostrando unas conclusiones con al respecto del análisis realizado.

2.3.3 Déficit de soluciones forenses. Análisis forense de IMs

La diversidad de dispositivos digitales, sistemas operativos y aplicaciones de IM hace que resulte improbable la existencia de soluciones forenses capaces de identificar, decodificar e interpretar la información generada por la multitud de aplicaciones de IM. Esto se agrava, además, cuando se trata de aplicaciones multiplataforma (Android, iOS,

WP, Windows, macOS, Linux, etc.), las cuales disponen de diferentes clientes (móvil, escritorio, web) y son actualizadas de manera continua.

Actualmente, existen multitud de soluciones forenses comerciales (UFED de Cellebrite[20], IEF de Magnet Forensics[21], BEF de Belkasoft[22] u Oxygen Forensics Analysis de Oxygen Forensics[23]), que proporcionan soluciones integrales, tanto *hardware* como *software*, capaces de automatizar todo el proceso de análisis forense realizado sobre el cliente móvil de muchas aplicaciones de IM. El problema del uso de estas herramientas de caja negra surge en el listado de aplicaciones de IM de son capaces de analizar, el cual se basa principalmente, en la cuota o cantidad de descargas de la aplicación o en la solicitud de estudio específico de una aplicación de IM por parte de algún cliente, omitiendo de sus soluciones el análisis forense de aquellas aplicaciones de mensajería instantánea que no tienen una gran cantidad de descargas. De igual manera, estas soluciones no incorporan en muchos casos el análisis forense de los clientes de escritorio o web de las aplicaciones de IM.

En muchas ocasiones, estas mismas soluciones forenses comerciales se desprestigian entre ellas mismas, notificando a sus consumidores la disponibilidad de soluciones forenses más completas que las de sus rivales directos, pudiendo identificar, decodificar e interpretar una mayor cantidad de información de un importante número de dispositivos electrónicos[24]. Este hecho conlleva que muchas ocasiones el especialista forense digital deba cuestionarse la fiabilidad o creencia ciega en el análisis forense realizado a través de este tipo de soluciones forenses de caja negra.

[20] Cellebrite LTD. Recuperado de: http://www.cellebrite.com.

[21] Magnet Forensics, Inc. Recuperado de: https://www.magnetforensics.com.

[22] Belkasoft LLC. Recuperado de: https://www.belkasoft.com.

[23] Oxygen Forensics, Inc. Recuperado de: http://www.oxgygen-forensics.com.

[24] Andrade. R. (2019). *Top 5 Reasons Why You Should Use Axiom with Your UFED Extractions*. Recuperado el 25 de septiembre de 2019, de: https://www-magnetforensics-com.cdn.ampproject.org/c/s/www.magnetforensics.com/blog/top-5-reasons-why-you-should-use-axiom-to-verify-your-ufed-results/amp/.

2.3.4 Mejoras en las herramientas de ayuda a la labor de los especialistas forense digitales

El especialista forense digital es el encargado de adquirir, a través de procedimientos forenses, el contenido de una evidencia digital sin alterar el contenido los datos extraídos, así como de analizar (identificar, decodificar e interpretar) los artefactos generados en las evidencias digitales objeto de estudio.

Desde hace ya varios años, el especialista forense digital se ve sometido a una carga de trabajo enorme (diversidad y numero de dispositivos digitales, volumen de información, complejidad de análisis, etc.), lo que le lleva cada vez más a utilizar herramientas de caja negra, las cuales automatizan todos los procesos del análisis forense de dispositivos digitales, incluso generando de manera instantánea el informe con los resultados. Estas soluciones forenses de caja negra son utilizadas de forma generalizada para analizar los artefactos de generados por las aplicaciones de IM y para realizar informes forenses de manera mecánica, reduciendo el trabajo realizado por el especialista. Si bien estas soluciones pueden ayudar al especialista, nunca debe ser sustitutivas del análisis forense realizado por el especialista, ya que éstas pueden omitir o interpretar erróneamente información.

Por otra parte, el especialista forense digital, en ocasiones desconocedor de la evolución de las aplicaciones de IM, puede centrar el análisis forense sobre el cliente móvil de este tipo de aplicaciones, obviando cualquier otra información contenida en otro tipo de dispositivo digital. En este sentido, el análisis forense realizado sobre diferentes clientes de una aplicación de IM puede dotar al especialista de una mayor cantidad de datos, así como aportar una mayor validez a la integridad de la información obtenida.

2.3.5 Falta de una metodología de análisis forense para el estudio de las aplicaciones de IM

En muchos de los procedimientos judiciales, en los cuales se incluyen el análisis forense de dispositivos electrónicos, se solicitan principalmente los datos relativos a las comunicaciones de usuario. En relación a las mismas (mensajes de texto, imágenes, videos, archivos, audio, localización, etc.), cada vez más, se especifica que se realice el

análisis de las diferentes aplicaciones de IM utilizadas por el usuario de un dispositivo digital, si bien, debido a la controversia sobre las implicaciones legales de este tipo de aplicaciones y a los continuos fallos de seguridad, también se vienen solicitando el análisis forense de la propia aplicación (configuración de seguridad, fechas de instalación o desinstalación, configuración de borrado de mensajes, configuración de descarga de ficheros, fechas y horas de uso de la aplicación, etc.).

En la actualidad, organizaciones tanto internacionales (ISO, NIST, SWGDE, ENFSI, Interpol, etc.) como nacionales (AENOR, UNE, FFCCSE, etc.) publican diferentes guías en las cuales exponen las buenas prácticas y procedimientos a seguir en el tratamiento y análisis forense de evidencias digitales (archivos de Log, de sistema operativo, metadatos de archivos, correo electrónico, historio de Internet, análisis de firmas, últimos programas utilizados, etc.), sí bien, no existe una metodología de análisis forense que cubra las casuísticas que engloban a las aplicaciones de IM.

El uso generalizado de las aplicaciones de IM como medio principal de comunicación, junto a su continua evolución, implica que este tipo de aplicaciones deban ser consideradas de una manera más global que cualquier otra aplicación, siendo tratadas como una entidad aparte en el análisis forense. El examen de este tipo de aplicaciones depende en gran medida del dispositivo digital, del sistema operativo e incluso del cliente o versión de la aplicación de IM. Así mismo, la utilización por parte de estas aplicaciones de servicios ubicados en la nube provoca un nuevo paradigma en cuanto a los métodos de adquisición y análisis forense.

2.3.6 Escasez de estudios técnico-forenses de aplicaciones de IM

En la actualidad, existe una falta de estudios técnico-forenses en relación con los artefactos generados en un dispositivo electrónico por las aplicaciones de IM, así como una carencia en la actualización de estos.

Debido al aumento de la cantidad de aplicaciones de IM, los especialistas forenses digitales a menudo deben realizar sus propios estudios, identificando e interpretando la relación de artefactos generados por este tipo de aplicaciones, si bien, muchos de estos estudios, como norma general, se centran en el análisis forense de los registros generados para un caso de uso específico (borrado de contacto, cambio de estado, entrega y lectura

de un mensaje, etc.). Los estudios técnico-forenses realizados sobre aplicaciones de IM, deben ser minuciosos, exponiendo de manera detallada cada dato encontrado en cada caso de uso analizado, si bien, estos estudios no son populares en la comunidad forense, ya que los mismos deben ser validados en cada nueva actualización, verificando si la información de la versión estudiada ha sido o no modificada en la nueva versión proporcionada por el desarrollador de la aplicación. El estudio detallado de artefactos, el coste de recursos (material, tiempo, etc.) y la complejidad de publicación, limitan que muchos de estos estudios se publiquen, perdiendo así la información y el conocimiento forense más allá del obtenido por el propio especialista. Es en este punto en el cual se hace necesario establecer una metodología de análisis forense, que permita al especialista forense digital el desarrollo de estudios técnico-forenses, en los cuales se expongan los resultados correspondientes con el análisis de aplicaciones de IM, validando y verificando en todo momento, que la información obtenida respeta las garantías legales.

2.4 Resumen.

En este segundo capítulo, revisadas las citas bibliográficas más relevantes, se ha puesto de manifiesto la falta de una metodología de análisis forense que permita identificar, decodificar e interpretar los artefactos generados por los diferentes clientes de las aplicaciones de IM con independencia del dispositivo electrónico o sistema operativo, más allá del uso de soluciones forenses o de caja negra.

Se ha expuesto el estado de la cuestión en cuanto a la situación actual del análisis forense en evidencias digitales, revisando los diferentes estándares y guías de buenas prácticas, tanto de ámbito internacional como nacional. De igual manera, se han revisado las metodologías de análisis forenses especificas utilizadas por diversos investigadores para el estudio de los diferentes clientes de las aplicaciones de IM.

Por último, se han enumerado y expuesto las razones fundamentales que han llevado al desarrollo de la presente investigación.

3 METODOLOGÍA DE ANALISIS

Los capítulos anteriores han mostrado la fundamentación teórica del presente trabajo de investigación. En este tercer capítulo de la memoria de la tesis doctoral se exponen los aspectos fundamentales del estudio, describiendo los objetivos, problemas y diseño que servirán de base para esta investigación. Por último, se propondrá una metodología de análisis, la cual ha sido seguida para el desarrollo del examen forense de diversas aplicaciones de IM, permitiendo el cumplimiento de objetivos y resolviendo así los problemas propuestos.

Debido a la evolución de las TIC y más concretamente a la continua transformación de las aplicaciones de IM, el diseño de esta investigación ha sido reenfocada en diversas ocasiones. Inicialmente esta investigación fue diseñada al objeto de contribuir al examen forense de diversas aplicaciones de IM no examinadas hasta la fecha, identificando y exponiendo a partir de procedimientos estándar forenses, los artefactos generados por los clientes móviles de este tipo de aplicaciones, si bien, durante el desarrollo de esta investigación, la variedad de clientes de aplicaciones de IM, sistemas operativos y dispositivos electrónicos utilizados para transmitir información a través de este tipo de aplicaciones generaron un cambio en el diseño de esta investigación, concluyendo con la propuesta de una nueva una metodología de análisis que, aplicando procedimientos científicos, pueda ser utilizada para el examen forense de las múltiples aplicaciones de IM que han existido, existen y existirán con independencia del dispositivo electrónico, sistema operativo o aplicación.

3.1 Objetivos de investigación

La evolución de las TIC, así como los avances de Internet han provocado en la sociedad actual una transformación tecnológica proporcionando de una mejora continua tanto en las capacidades de los dispositivos electrónicos como en la velocidad de las comunicaciones. Estas implican para el usuario de a pie una serie de ventajas y beneficios, si bien, en ocasiones son utilizadas de manera incorrecta. La diversidad de dispositivos electrónicos, sistemas operativos y aplicaciones de IM incluidos en y para la comisión de

hechos delictivos implica, desde el punto de vista del análisis forense digital, la elaboración de múltiples estudios técnico-forenses, los cuales son necesarios para la confección del examen forense de este tipo de aplicaciones para su presentación ante la Autoridad Judicial como prueba electrónica.

El objetivo principal de la presente investigación es, desarrollar una metodología de análisis a partir de la cual, se puedan desarrollar estudios técnico-forenses sobre los artefactos generados por una aplicación de IM en una evidencia electrónica, con independencia del dispositivo digital, sistema operativo, cliente o versión analizado, validando la integridad de los datos obtenidos y realizando las transformaciones necesarias para su correcta interpretación.

A continuación, se desgranan distintos objetivos más particulares que se persiguen con la investigación de la tesis doctoral.

1. Estudiar el impacto del uso de las aplicaciones de mensajería instantánea en la sociedad y su utilización en la comisión de hechos delictivos.
2. Analizar las especiales características que engloban al análisis forense de los diferentes clientes de las aplicaciones de mensajería instantánea.
3. Evaluar el impacto de los diferentes clientes de las aplicaciones de mensajería instantánea en la Informática Forense. Poner de relieve que las aplicaciones IM pueden ser utilizadas desde diferentes clientes, sistemas operativas o formas de acceso a las comunicaciones de usuario, al contrario que sucede con otro tipo de aplicaciones sólo disponibles para un dispositivo o sistema en particular.
4. Analizar los procedimientos forenses específicos en cuanto al análisis forense de los diferentes clientes de las aplicaciones de mensajería instantánea.
5. Analizar del uso estandarizado de las soluciones forenses comerciales existentes y su impacto en el análisis forense de las aplicaciones de mensajería instantánea.
6. Analizar la información generada por las clientes de las aplicaciones de mensajería instantánea. Estudio de estandarización del análisis forense con respecto a la identificación, decodificación e interpretación de la información

generada por este tipo de aplicaciones con independencia de la evidencia electrónica.

7. Evaluar el impacto en la Informática Forense de los sistemas de cifrado implementados por los clientes de las aplicaciones de mensajería instantánea.
8. Propuesta de una metodología común para el análisis forense los diferentes clientes de las aplicaciones de mensajería instantánea, la cual permita verificar la integridad de la información obtenida.
9. Desarrollar la metodología propuesta en el análisis forense de aplicaciones de mensajería instantánea que no hayan sido analizados, exponiendo los resultados obtenidos, así como los problemas encontrados.

3.2 Problemas de la investigación

Esta tesis tiene su origen en una inquietud personal y profesional que posteriormente se ha visto reflejada en una necesidad académica. La experiencia y la revisión de material sobre el estado del análisis forense de las aplicaciones de mensajería instantánea ha permitido comprobar la idoneidad de esta investigación.

A continuación, se exponen los diferentes problemas encontrados durante el diseño de la investigación llevada a cabo como parte de esta Tesis, las cuales quedan expuestos en los diferentes estudios científicos-técnicos-forenses realizados como parte de esta investigación.

Diversidad de dispositivos electrónicos.

Desde la perspectiva del análisis forense digital, la rápida evolución de las TIC implica una serie de inconvenientes en cuanto al examen forense de los dispositivos electrónicos. La diversidad de equipos informáticos (ordenadores portátiles, de sobremesa, servidores, etc.), dispositivos móviles (teléfonos inteligentes, tabletas, etc.) o dispositivos IoT (*wearables*, relojes inteligentes, etc.), sumado a la cantidad de marcas y modelos que existen en el mercado, provocan que, en ocasiones, el examen forense

realizado sobre un dispositivo electrónico determinado sirva únicamente y exclusivamente para ese dispositivo.

Diversidad de sistemas operativos.

De igual manera, en relación con el análisis forense digital de los sistemas operativos, este implica un verdadero reto al especialista, en cuanto a la cantidad y versiones de estos. La diversidad de sistemas operativos de escritorio (Windows, macOS, Linux, etc.), sistemas operativos móviles (Android, iOS, WP, etc.) o sistemas operativos de IoT (WearOS, WatchOS, Nucleus RTOS, etc.), provoca que, se haga necesario desarrollar multitud de estudios en los cuales se expongan la cantidad de registros o artefactos generados por estos. Si bien, existe diversa documentación forense en relación con los sistemas operativos conocidos, en muchas ocasiones, el problema consiste en el análisis que debe ser realizado sobre aquellos sistemas operativos no conocidos.

Actualizaciones de las aplicaciones de IM.

Desde la perspectiva del análisis forense digital, la rápida evolución de las aplicaciones de mensajería lleva consigo una serie de inconvenientes. La continua actualización de los diferentes clientes de las aplicaciones de mensajería instantánea provoca que el estudio técnico-forense realizado sobre una determinada aplicación de IM deba ser revisado, verificando la diferentes entre los rastros generados por cada nueva versión.

Volumen e interpretación de los datos.

La cantidad de datos generados por las aplicaciones de IM es cada vez mayor, lo que conlleva que el especialista se enfrente a grandes volúmenes de información por cada una de las aplicaciones de IM analizada. La interpretación de los datos generados por cada una de las aplicaciones de IM supone de igual manera que el especialista deba lidiar con organizaciones de datos diferentes, debiendo realizar diferentes análisis forenses, para poder examinar la información generada por la misma aplicación en sistemas operativos distintos.

Cifrado de información.

El cifrado aplicado a los datos almacenados en los dispositivos electrónicos, implica que, en muchas ocasiones, el análisis forense tradicional de las aplicaciones de IM resulte infructuoso. Los dispositivos electrónicos, los SO e incluso las propias aplicaciones de IM desarrollan sistemas de cifrado que limitan el acceso a los datos personales del usuario, tanto para el propio usuario del dispositivo como para el especialista forense digital.

3.3 Metodología propuesta para el análisis de IM.

En este punto se exponen los diferentes métodos de estudios que formaran parte de la metodología de análisis de las aplicaciones de IM, describiendo los procedimientos, técnicas y herramientas utilizadas para identificar, decodificar e interpretar los datos generados por este tipo de aplicaciones, más allá del simple análisis forense estático de artefactos. Cada uno de los métodos de estudios pertenecientes a la metodología de análisis que se propone en esta investigación ha sido desarrollado siguiendo las indicaciones de la norma ISO/IEC 27041:2015 *Guidance on assuring suitability and adequacy of incident investigative method.* (International Organization for Standardization, 2015b).

El estándar ISO/IEC 27041:2015 describe una serie de procesos que servirán de guía en la búsqueda y selección de nuevos métodos utilizados en el análisis de evidencias digitales. Estos procesos se corresponden con:

1. ***Captura de requisitos y análisis***. En este proceso consiste en descubrir, identificar, revisar, documentar y analizar las necesidades de un nuevo método de análisis que asegurarán su correcta elección.

Por cada uno de los tres métodos incluidos en la metodología de análisis

propuesta en esta investigación, se han identificado los requisitos necesarios para su desarrollo, revisando los diferentes procedimientos existentes y analizando las necesidades de las técnicas utilizadas de acuerdo con las buenas prácticas forenses.

2. ***Proceso de diseño***. El diseño de un nuevo método de análisis debe evaluar todos los requisitos y el estado de los mismos, dando una idea de cómo debe ser el nuevo método de análisis. En este punto no es necesario especificar cada procedimiento o técnica utilizada, si bien, ello debería estar claramente identificado. Así mismo, en este punto se deben identificar, seleccionar y clasificar las posibles herramientas.

   El proceso de diseño debe ser tomado en cuenta desde una perspectiva de conjunto cuando se trata del diseño de la metodología de análisis propuesta en esta investigación. De igual manera, el proceso de diseño debe ser visto desde la perspectiva individual cuando se trata de cada uno de los tres métodos de estudio que se incluyen en metodología. En el primer caso, el diseño responde a la inclusión de la suma de métodos en la metodología propuesta, respondiendo el diseño en el segundo caso, a la descripción de los procedimientos, técnicas y herramientas que serán utilizadas en cada uno de esos métodos.

3. ***Proceso de Implementación***. Este atañe al proceso en el cual se procede a generar la documentación, de forma detallada, relativo a los procedimientos, técnicas y herramientas utilizadas en el nuevo método de análisis.

   El proceso de implementación de los diferentes métodos incluidos en la metodología de análisis propuesta en esta investigación será desarrollado con posterioridad.

4. ***Proceso de verificación y validación.*** El proceso de verificación, el cual será opcional, permite asegurar que los procedimientos, técnicas y herramientas utilizadas en el nuevo método de análisis propuesto, dispongan de las suficientes garantías. De igual modo, el proceso de validación permite comprobar como a

partir que los procedimientos, técnicas y herramientas utilizadas se obtengan resultados correctos.

El proceso de verificación y validación, en el caso de esta investigación, puede ser visto desde la perspectiva global de la metodología de análisis propuesta, así como desde la perspectiva individual de cada uno de los tres métodos de estudio que se incluyen en esta. El proceso de validación de la metodología viene dado por la suma de métodos incluidos en la misma, los cuales permiten corroborar el resultado obtenido de hasta tres fuentes de datos distintas. Así mismo el proceso validación de cada uno de estos métodos se evalúa de forma independiente y viene dado por los resultados obtenidos en cada uno de los procedimientos, técnicas y herramientas utilizadas. El proceso de verificación se realizará sobre cada una de las múltiples soluciones forenses comerciales y gratuitas utilizadas indicando las conclusiones obtenidas.

5. ***Confirmación***. La confirmación es el proceso que precede al despliegue y en el cual se evalúan de manera formal que los procedimientos, técnicas y herramientas son válidas para su inclusión en el nuevo método de análisis de evidencias digitales.

   En el caso de esta investigación, el proceso de confirmación se realiza de forma continua, evaluando y validando los diferentes procedimientos, técnicas y herramientas elegidas en cada uno de los métodos incluidos en la metodología de análisis expuesta, las cuales deben, en todo momento, formar parte del método científico.

6. ***Despliegue***. En este proceso se confirma el nuevo método para ser utilizado en el análisis de evidencias digitales. El resultado del despliegue del método de análisis debe ser documentado, dejando constancia de los resultados obtenidos, así como de los problemas acaecidos durante su desarrollo.

   El despliegue de los diferentes métodos, incluidos en la metodología de análisis propuesta en esta investigación, será expuesto en los capítulos 4, 5 y 6.

7. ***Revisión y mantenimiento***. Una vez desplegado el nuevo método de análisis de evidencias digitales, es momento de revisas los procesos identificando y evaluando las posibles necesidades y problemas encontrados.

   En el caso de esta investigación, el mantenimiento y revisión de los diferentes métodos incluidos en la metodología de análisis propuesta, serán expuestos a modo de conclusión en los capítulos 4, 5 y 6.

La figura 3.1 muestra el flujo de procesos utilizados en la norma ISO/IEC 27041 para asegurar la idoneidad y adecuación de la incorporación de nuevos métodos científicos al análisis de evidencias digitales.

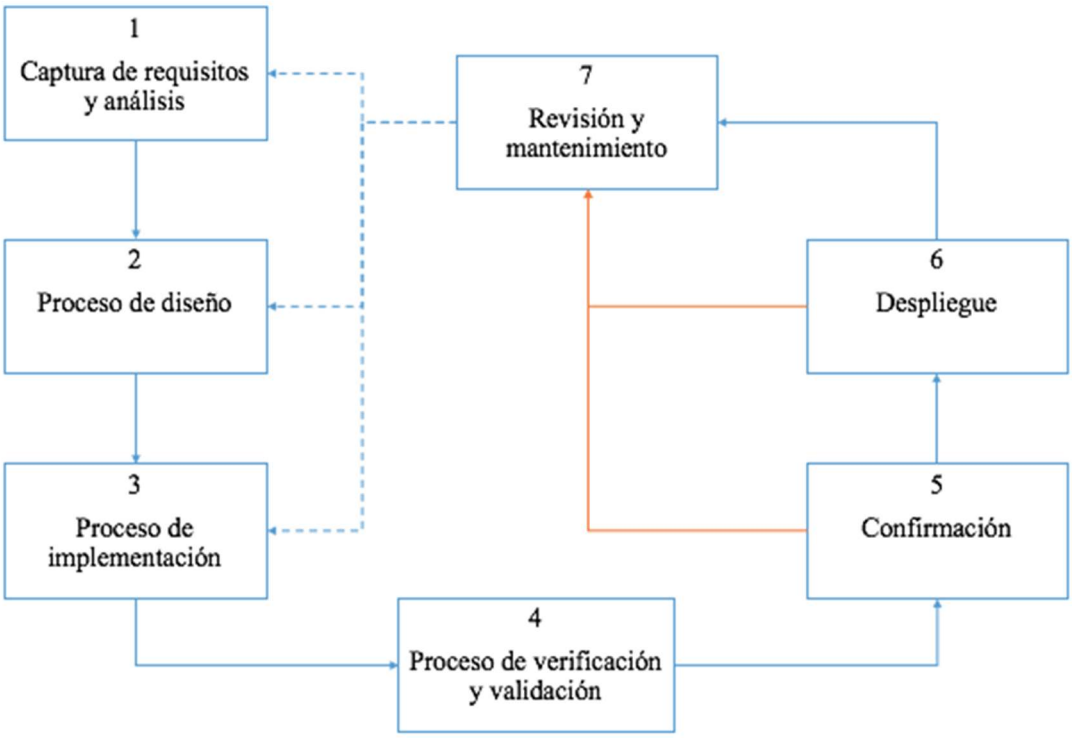


Figura 3.1. Flujo de procesos utilizados para la selección de métodos de análisis de evidencias digitales.

A continuación, se exponen los tres métodos de estudio incluidos en la metodología de análisis propuesta, en los cuales se exponen los procedimientos, técnicas

y herramientas utilizadas. Esta metodología de análisis pretende proporcionar del conocimiento funcional, técnico y forense necesario para el desarrollo de cualquier examen forense con independencia del dispositivo electrónico, sistema operativo o aplicación de IM. Así mismo, la suma de estos tres métodos permite identificar, decodificar e interpretar la información generada por este tipo de aplicaciones, complementando y validando la información obtenida más allá del análisis forense estático de artefactos.

3.3.1 Estudio de fuentes abiertas

El estudio de fuentes abiertas es el proceso de búsqueda y análisis de toda fuente de datos fiable que proporcione conocimiento funcional, técnico y forense respecto a la aplicación de IM examinada. Este estudio debe ser realizado de manera recurrente, ya que, la evolución de las nuevas tecnologías de la información e Internet implica la publicación de forma constante de infinidad de documentación forense.

El estudio de fuentes abiertas se subdivide en las siguientes fases:

- Planificación

  La planificación debe ser el punto inicial de partida, en el cual el especialista, ante la necesidad de realizar el examen forense de una determinada aplicación de IM, recopile el conocimiento, datos y herramientas de las que dispone y pueda plantear de forma eficaz, eficiente y efectiva lo que necesita. Si la planificación no es correcta, puede perderse gran cantidad de tiempo las siguientes fases.

- Obtención de datos

  La obtención de datos es el proceso en el cual se realiza una búsqueda de información, en función de palabras clave o conceptos sobre todas aquellas fuentes de datos disponibles (abiertas, semiabierta, cerradas, etc.). En la

actualidad, el uso de las TIC e Internet facilitan la búsqueda de información en multitud de fuentes de datos a la vez (revistas tecnológicas, documentación Universitaria, conferencias tecnológicas, etc.), ya que estas consultas pueden ser realizadas de manera casi inmediata sobre toda la información que tienen indexada los motores de búsqueda de Internet (Bing, Google, Google Scholar, etc.).

- Procesamiento y análisis de la información

  Los resultados obtenidos de las diferentes búsquedas realizadas deben ser procesados, siendo necesariamente catalogados en relación a su origen, autor, fecha de publicación, nivel de detalle de estudio, idioma, dispositivo electrónico, sistema operativo, aplicación de IM (cliente, versión, etc.), proporcionando de esta manera un mayor o menor valor o utilidad a la información obtenida de la fuente de datos. Posteriormente, una vez procesada toda la información, se debe realizar el correspondiente análisis sobre todos aquellos datos que puedan proporcionar al especialista de manera directa o indirecta, el conocimiento funcional, técnico o forense sobre la aplicación de IM.

- Explotación de la información

  Finalmente, después del análisis de la información, el resultado debe ser la transformación de esa información en conocimiento útil y valioso, la cual será utilizada por el especialista para ayudar y facilitar el examen forense de las aplicaciones de IM.

3.3.2 Estudio de artefactos

El estudio de artefactos es el análisis realizado sobre todos los registros que son generados por una determinada aplicación en un dispositivo electrónico. Dicho estudio se divide en el procedimiento forense de adquisición y en el análisis de los registros. La evolución de las aplicaciones de IM implica que, en ocasiones, el estudio de artefactos de este tipo de aplicaciones se deba alejar de los métodos tradicionales, si bien, los

procedimientos seguidos siempre deben mantener el valor probatorio de la prueba electrónica.

3.3.2.1 Adquisición forense

La adquisición forense, es el procedimiento por el cual se obtiene la información de un dispositivo electrónico, sin alterar el contenido de la evidencia electrónica original.

La adquisición forense estática o tradicional, es aquel proceso forense por el cual se obtiene la información almacenada en un dispositivo electrónico apagado. Para ello, como norma general, se genera una o varias imágenes forenses con la información contenida en el sistema de almacenamiento masivo. Si bien existen diferentes métodos de adquisición, en todo momento, se debe evitar la alteración de los datos contenidos en la evidencia electrónica original.

La adquisición forense estática se puede subdividir en función al tipo de sistema de almacenamiento en:

- Sistema de almacenamiento datos extraíbles: Este es el caso de dispositivos electrónicos, como ordenadores personales, portátiles o servidores, en los cuales el sistema de almacenamiento de datos (HDD, SSD, etc.) son fáciles de extraer, pudiendo adquirir la información de manera sencilla, bien desmontado el sistema de almacenamiento o bien a través de distribuciones forenses (*liveUSB, liveCD,* etc.).

- Sistema de almacenamiento de datos no extraíbles: Este es el caso de dispositivo electrónicos como teléfonos o relojes inteligentes o tabletas, en los cuales el sistema de almacenamiento de datos (chip de memoria) es de difícil extracción, pudiendo adquirir la información a través de los diferentes procedimientos[25]:
    - Lectura a través de puerto de datos: El acceso al contenido del dispositivo

[25] Teel Technologies. (2015). *What is JTAG, Chip-off and ISP?* Recuperado el 13 de octubre de 2019, de: https://www.teeltech.com/ufaqs/what-is-jtag-chip-off-and-isp/.

electrónico se realiza a través de *software* específico evitando el inicio del SO del dispositivo electrónico.

- Uso de procesos de carga inicial (*bootloaders):* El acceso al contenido del dispositivo se realiza a partir de la carga inicial de programas que evitan el inicio del SO del dispositivo electrónico.
- Lectura directa en placa (JTAG). Es el proceso en el cual se obtiene la información del dispositivo electrónico a través del puerto de testeo (TAP). Esto es posible debido estándar *JTAG* utilizado para el chequeo de los chips en ubicados en la placa (PCB).
- Lectura directa en chip (ISP). Es el proceso por el cual se obtiene el contenido a través del puerto de testeo (TAP) del propio chip de memoria. Esta técnica se realiza sobre chip de tipo eMMC y eMCP.
- Desoldado de chip *(Chip-Off).* Es el proceso por el cual se desuelda el chip de memoria de la placa base del dispositivo electrónico, para a continuación conectar el chip a un lector de memorias *flash* con el fin de copiar su contenido.

3.3.2.2 Análisis forense

El análisis forense es el procedimiento por el cual se examinan los registros que han sido o están siendo generados, modificados o eliminados por una determinada aplicación en un dispositivo electrónico.

3.3.2.2.1 Análisis forense estático

El análisis forense estático, tiene por objetivo el examen detallado sobre los rastros que han sido almacenados por una aplicación de IM en un dispositivo electrónico, identificando cada registro generado, modificado y eliminado por el sistema operativo y por la aplicación, generando la línea temporal de uso. Posteriormente se decodificará la información relativa a los artefactos almacenados por este tipo de aplicaciones en un dispositivo electrónico.

A continuación, se mencionan aquellos rastros que el especialista forense digital debe examinar como parte del análisis forense estático realizado sobre las aplicaciones de IM.

- ***Sistema Operativo***. Los registros generados en el Sistema Operativo son tan variables que dependen en gran medida tanto del mismo SO (Windows, macOS, Linux, Android, iOS, WP, etc.), como de la versión (Windows 7, Windows 8, Windows 10, Oreo, Pie Android 10, iOS 11, iOS 12, etc.). En relación con el análisis forense estático de aplicaciones de IM, se identificarán entre otras cosas, fechas de Instalación o eliminación de la aplicación, listado de aplicaciones de IM instaladas, versión de la aplicación, etc.

- ***Sistemas de archivos***. De igual manera, los registros generados en el sistema de archivos son de carácter variable por lo que dependerán de sus propias características (FAT, exFAT, NTFS, Ext3, Ext4, HFS, APFS, etc.). En este caso, en el análisis forense estático de aplicaciones de IM, se identificarán datos relativos a fechas de creación, modificación, acceso y borrado de los archivos generados por este tipo de aplicación.

- ***Aplicaciones de IM***. El examen de los clientes móviles, de escritorio y web de las aplicaciones de IM, se realizará sobre los datos contenidos en los propios archivos. En este caso, el análisis forense estático identificará los datos relativos a la de configuración (idioma, país, servidores y puertos utilizados, número máximo de participantes en un grupo, etc.), preferencias (uso de código bloqueo, uso de doble verificación, almacenar archivos multimedia en dispositivo, permiso localización, sonido específico para un contacto) o archivos de Log (identificaran fechas y horas de ejecución, de actualización, gestión de copias de seguridad, numero registrado, cambio de número de teléfono asociado a la aplicación, etc.).

- ***Archivos compartidos***. El examen de los archivos de multimedia (Imagen, audio y video, documentos, etc.) se realizará sobre el contenido de estos, así como la información (tipo de archivo, origen, destino, fechas, etc.) que genera en la propia aplicación de IM. En el caso de los metadatos de los archivos compartidos, cabe

mencionar que los mismos carecen de ellos, ya que, este tipo de aplicaciones los eliminan al minimizar el tamaño para su envío.

- ***Archivos de datos o bases de datos.*** El examen de los archivos de datos o bases de datos, son en muchas ocasiones el objeto principal del análisis forense estático. En este caso, se identificarán los ficheros que contienen los datos personales del usuario de la aplicación de IM, para posteriormente interpretar toda la información relativa a las comunicaciones de usuario. Interpretar esta información no solo consiste en reseñar aquellos datos que son almacenados en un formato legible y que pueden ser visualizados por cualquier ser humano, sino que, se deben describir y decodificar aquella información no legible realizando las transformaciones necesarias para que pueda ser reconocida por el ser humano.

- ***Recuperación de datos***. La recuperación de datos es una parte esencial en el análisis forense estático de las aplicaciones de IM, ya que, en numerosas ocasiones, la información relativa a las comunicaciones de un usuario ha sido eliminada de manera accidental o intencionadamente. En este caso, la recuperación de datos depende del método de adquisición forense estático realizado.

El análisis forense estático de las aplicaciones de IM dependerá en gran medida de las capacidades técnicas, de formación y de la experiencia del especialista forense digital, las cuales permitirán identificar de manera fehaciente los artefactos además de interpretar la información generada por este tipo de aplicaciones.

3.3.2.2.2 Análisis forense dinámico

El análisis forense dinámico es el procedimiento forense por el cual se obtiene la información de un dispositivo electrónico encendido, sin perjuicio claro está de que todo dispositivo encendido modifica su contenido. El análisis forense dinámico persigue

simular el uso normal del mismo evitando la alteración de los datos contenidos en la evidencia electrónica original. La idea principal es obtener toda aquella información que no haya podido ser recopilada a partir del análisis forense estático (listado de procesos en ejecución, configuración de sistema o aplicaciones, datos cifrados, volúmenes cifrados, etc.). La nube o *cloud* está cambiando en muchos casos los formas que tiene el usuario para acceder a su información. Si se pretende obtener las comunicaciones de usuario de las aplicaciones de IM preservando el valor probatorio de la prueba electrónica, el análisis forense estático o tradicional debe evolucionar hacia un nuevo paradigma, ya que, en muchos casos los datos del usuario no estarán contenidos en el propio dispositivo electrónico.

Los métodos forenses utilizados para simular la ejecución de una evidencia electrónica pueden subdividir en:

- ***Copia forense***: Es la opción más sencilla de implementar, ya que, consiste en copiar de manera forense la información relativa a una aplicación específica (datos de la aplicación, configuración y preferencias, datos de usuario, etc.), ubicada en la evidencia electrónica origen, para posteriormente incluirla en un entorno forense controlado, simulando de esta forma la normal ejecución de la aplicación original.

- ***Emulación***: En este caso, se emula la evidencia electrónica original a partir de la imagen o clon forense realizada del sistema de almacenamiento masivo original. La virtualización es la opción más rápida de implementar, ya que, existen diversas soluciones forenses (Forensics Explorer, OpenVL, Perlustro, etc.) que forense con ayuda de software de virtualización (VMware, VirtualBox, Parallels, etc.) emulan un sistema a partir de una imagen o clon forense. Cabe mencionar que, pueden encontrarse ciertas incompatibilidades de hardware o problemas de acceso al sistema (contraseña, cifrado, etc.), que limiten el proceso de virtualización (Shavers B., 2008).

- ***Clonado***: Este caso consiste en introducir el clon forense o copia exacta realizada sobre sistema de almacenamiento masivo original, en el mismo dispositivo electrónico origen. En este caso se utiliza el dispositivo electrónico original como herramienta de trabajo junto a un duplicado del sistema de almacenamiento masivo, evitando de esta manera incompatibilidades de hardware, así como la alteración del sistema de almacenamiento masivo original.

El análisis forense dinámico ofrece la posibilidad de emular de manera forense el normal uso de la evidencia electrónica, permitiendo obtener tanto la información relativa a la configuración de la aplicación de IM, como a las comunicaciones mantenidas por el usuario de este tipo de aplicación. Este tipo de análisis puede ser utilizado en aquellas ocasiones en las cuales las aplicaciones de IM implementan sistemas de cifrado sobre los datos de configuración de la propia aplicación como sobre los datos relativos a las comunicaciones de usuario, dificultando el análisis forense estático y por ende la obtención de esta información.

3.3.2.3 Desarrollo aplicado en el estudio de artefactos

A continuación, se expone el procedimiento seguido para el estudio de los artefactos generados por aplicaciones de IM en dispositivos electrónicos.

El desarrollo de este tipo de estudio se subdivide en:

1. Realizar un listado de casos de uso. Instalar o eliminar de aplicación de IM, crear o eliminar grupo o canal, incluir o excluir usuario en grupo, generar o eliminar mensaje, estado del mensaje (enviado, recibido, pendiente, etc.), envió de archivos (localización, imágenes, video, etc.), etc.
2. Generar cada caso de uso en un dispositivo electrónico (físico o virtual)
3. Realizar la adquisición forense estática de tipo física, es decir, una copia bit a bit de toda la información contenida en el dispositivo digital en forma de imagen

forense.

4. Realiza el análisis forense estático de artefactos de la imagen forense, identificando toda aquella información que haya sido generada, modificada o eliminada.
5. Decodificar todos aquellos registros correspondientes a cada uno de los casos de uso.
6. Para cada uno de los casos de uso, repetir los puntos 2, 3, 4 y 5.
7. Análisis comparativo e interpretación de la información.
8. Conclusiones del análisis forense estático.
9. Realizar análisis forense dinámico. Emulación del entorno original a partir de procedimientos forenses.
10. Obtener la información del entorno emulado.
11. Conclusiones del análisis forense dinámico.

3.3.3 Estudio de código fuente

El estudio de código fuente es aquel proceso en el cual se examina e interpreta las líneas de código escritas para el desarrollador de una aplicación proporcionando conocimiento funcional y técnico respecto a la aplicación de IM examinada.

Las técnicas utilizadas en el estudio del código fuente de una aplicación de IM se pueden comparar con la revisión que se realiza en el análisis estático de ingeniería del software. En el análisis estático de software se utilizan una serie de mecanismos los cuales permiten realizar el examen sistemático del código fuente al objeto de chequear y mejorar la calidad de este antes de su puesta en producción (corrección de errores de codificación, verificación de eficiencia de programación, etc.). En el estudio de código fuente se utilizan estos mismos mecanismos, analizando las líneas de código que permitan apoyar o aportar conocimiento forense de una determinada aplicación de IM.

El estudio de las líneas de código fuente de una la aplicación de IM debe centrarse en el análisis de aquellas partes del código que proporcionen información para:

- Determinar la ubicación de la información (directorios, archivos de datos, ficheros de eventos, archivos multimedia, etc.).
- Identificar los tipos de archivos (ficheros de datos, bases de datos, archivos de enlace, archivos especiales, etc.).
- Identificar estructuras de datos almacenadas (fijas o dinámicas).
- Reconocer datos legibles (identificadores, nombres, teléfonos, etc.) e ilegibles (datos cifrados, formatos especiales, etc.).
- Determinar las transformaciones realizadas sobre los datos (*Unix Epoch*, *Little Endian*, *Big Endian*, Hexadecimal, Binario, etc.).
- Decodificar los datos legibles e ilegibles a formato humano.
- Determinar las razones por las que el especialista no se pueden decodificar los datos.
- Identificar cualquier otro dato no obtenido de estudios anteriores.

Este estudio de código fuente puede resultar complejo, largo y tedioso, ya que, por una parte, obliga a que el especialista conozca el lenguaje de programación, y por otra parte implica el análisis y comprensión de grandes cantidades de líneas de código. En el estudio de código fuente pueden darse dos situaciones:

1. Disponer del código fuente. El desarrollador o un tercero proporcionan el código fuente de la aplicación de IM, pudiéndose de manera relativamente sencilla, analizar en claro las diferentes líneas de código fuente (clases, funciones, variables, estructuras, etc.). En este caso, se puede realizar una búsqueda por palabras clave si se conoce algún dato o patrón, así como realizar una revisión integra de las líneas de código. Se pueden utilizar diferentes herramientas informáticas para el análisis del código fuente (entornos integrados de desarrollo, editores de texto, etc.).

2. No disponer del código fuente. El desarrollador no proporciona el código fuente de la aplicación, limitando el acceso a parte de este o incluso ofuscándolo, debiéndose recurrir a técnicas de ingeniería inversa para poder analizar las líneas de programación de la aplicación. En este caso, el análisis que se debe realizar es

mucho más complejo debiendo conocer lenguajes de bajo nivel. Se pueden utilizar diferentes herramientas informáticas para realizar ingeniería inversa de una aplicación como son los depuradores de código, desensambladores o decompiladores inversos.

3.4 Resumen.

En este tercer capítulo se han expuesto los objetivos de la investigación, así como los diferentes problemas encontrados en el análisis forense de los diferentes clientes de las aplicaciones de mensajería instantánea. Se ha propuesto una metodología para el análisis forense de este tipo de aplicaciones que permita identificar, decodificar e interpretar los artefactos generados por los diferentes clientes de las aplicaciones de IM con independencia del dispositivo electrónico, describiendo esta como la suma de tres métodos (estudio de fuentes abiertas, estudio de artefactos y estudio de código fuente) y desarrollando los procedimientos utilizados en cada uno de los mismos.

4 ANALISIS FORENSE IM EN TELÉFONOS INTELIGENTES

En este cuarto capítulo se exponen las contribuciones realizadas al análisis forense del cliente móvil de las aplicaciones de mensajería instantánea en teléfonos inteligentes como parte de la investigación realizada en la presente Tesis.

4.1 Introducción

En la actualidad, los dispositivos móviles y más concretamente los teléfonos inteligentes son parte inherente de la sociedad. El *hardware* y *software* de este tipo dispositivos los hacen igualar o incluso superar las capacidades de un ordenador personal, si bien, el reducido tamaño de los teléfonos inteligentes sumado a las redes de datos móviles proporciona una disponibilidad de conexión con otras personas de manera constante.

El análisis forense de la telefonía móvil ha evolucionado desde el examen que se realizaba sobre los teléfonos móviles al que se realiza sobre los teléfonos inteligentes. Lejos queda los datos que albergaban las tarjetas SIM o los teléfonos móviles antiguamente en comparación a la cantidad de información que son capaces de almacenar los teléfonos inteligentes en la actualidad. Los teléfonos inteligentes son aquellos dispositivos electrónicos que disponen de un sistema operativo móvil y que, además de albergar los datos relativos a un teléfono móvil (contactos, registro de llamadas, mensajes de texto o mensajes multimedia) pueden almacenar un número cada vez mayor de información digital (correos electrónicos, conversaciones, navegación web, geolocalización, archivos multimedia, contraseñas, archivos de configuración, archivos de datos, bases de datos, etc.). El análisis forense debe adaptarse a la realidad actual de los datos contenidos en los dispositivos móviles y aplicar los procedimientos científicos necesarios para adquirir, analizar e interpretar todos los artefactos contenidos en un teléfono inteligente manteniendo en todo momento la inalterabilidad de los datos.

4.1.1 Adquisición forense en teléfonos inteligentes

La adquisición forense estática o adquisición tradicional es aquella en la que se obtiene la información del teléfono inteligente previniendo su normal encendido y evitando con ello la alteración de los datos contenidos en la evidencia por parte del sistema operativo, aplicaciones o usuario. A partir de este tipo de adquisición se consigue generar una imagen forense (copia *bit* a *bit*) de la información contenida en el teléfono inteligente. En la actualidad los procedimientos utilizados en este tipo de adquisición van desde los menos destructivos como la carga inicial de procesos (*bootloaders*), la lectura directa en placa (JTAG) o la lectura directa a chip (ISP) a los más destructivos como la extracción y lectura directa de chip (*Chip-Off*).

Al igual que sucede en la adquisición forense estática, la adquisición forense dinámica se realiza, como norma general, con soluciones forenses especializadas. Estas soluciones forenses permiten realizar una copia lógica de los datos volátiles y no volátiles de un teléfono inteligente encendido. Se debe tener presente que, al realizar una adquisición forense dinámica con el teléfono inteligente encendido, tanto el sistema operativo como las aplicaciones alteran la información almacenada en este dispositivo.

4.1.2 Análisis forense en teléfonos inteligentes

El análisis forense de un teléfono inteligente, como sucede con la adquisición, se puede subdividir en análisis forense estático y análisis forense dinámico de artefactos. En el primer caso se realiza un análisis forense de la información obtenida del proceso de adquisición. En el segundo caso, se realiza el análisis de los rastros que están siendo generados en el teléfono inteligente durante su ejecución.

Cuando se trata específicamente del análisis forense del cliente móvil de las aplicaciones de mensajería instantánea en teléfonos inteligentes, este debe abordarse desde una perspectiva más amplia de la adquisición e interpretación de las comunicaciones de usuario. Este tipo de aplicaciones no solo son utilizadas para las comunicaciones tradicionales, sino que, debido a sus funcionalidades (mejoradas en cada nueva versión) permiten a su usuario capacidades tan diversas como la búsqueda de contactos por geo-posición, el borrado de los mensajes en el dispositivo destino con una periodicidad

determinada, envío de diferentes tipos de archivos, transferencia de archivos de tamaño elevado, llamadas *VoIP*, etc.

Existen diversas soluciones forenses comerciales especializadas en automatizar tanto el proceso de adquisición, como en proceso de análisis forense de las aplicaciones de mensajería instantánea en teléfonos inteligentes, si bien, tal y como quedará demostrado en los siguientes puntos, estas soluciones no pueden cubrir la enorme cantidad de aplicaciones de mensajería instantánea que han existido, existen o existirán y mucho menos el análisis forense de cada característica.

Debido al número de aplicaciones de IM disponibles para teléfonos inteligentes, a la velocidad a la que se actualizan este tipo de aplicaciones y la limitación de las soluciones forenses comerciales, es por lo que se hace necesario realizar de manera más continua estudios técnico-forenses que desarrollen el análisis forense de este tipo de aplicaciones identificando, decodificando e interpretando todos aquellos registros que son generados por los clientes móviles en los teléfonos inteligentes.

4.2 Escenarios: Telegram Messenger sobre Android y Windows Phone

En este punto se expondrán los estudios técnico-forenses realizados sobre el cliente móvil de una de las aplicaciones de mensajería instantánea más descargada de los principales mercados digitales oficiales de aplicaciones móviles y más utilizada en el mundo. Esta aplicación de mensajería instantánea fue una de las primeras aplicaciones de este tipo en proteger el contenido de sus mensajes con un cifrado punto a punto además de ofrecer la posibilidad de transferir diferentes tipos de archivos o posibilitar autodestrucción de mensajes enviados en un tiempo determinado.

Estos estudios aplican el análisis realizado sobre el cliente móvil de la aplicación de mensajería instantánea Telegram Messenger para los sistemas operativos móviles Android y Windows Phone, exponiendo los resultados obtenidos relativos a los registros que genera en cada uso de los diferentes sistemas estudiados.

4.2.1 Cuestiones y herramientas comunes en el análisis forense IM

Los estudios técnico-forenses que a continuación se exponen, se llevan a cabo a partir de la metodología de análisis forense propuesta en la presente tesis, compuesta por la suma de tres métodos de estudio, con los cuales se pretende proporcionar un conocimiento tanto funcional, técnico y forense del cliente estudiado, así como validar la integridad de la información obtenida. Los estudios técnicos-forenses del cliente móvil de la aplicación de mensajería instantánea Telegram Messenger son desarrollados sobre diferentes sistemas operativos móviles al objeto de corroborar la validez de la metodología de análisis forense propuesta con independencia del sistema operativo examinado, así como de la versión del cliente móvil. Cabe mencionar que, en el momento del desarrollo de estos estudios no existía documentación forense al respecto de los artefactos que genera el cliente de móvil de la aplicación de IM Telegram Messenger en el sistema operativo WP.

Debido al volumen de la información generado por las aplicaciones de mensajería instantánea, es normal que el análisis forense se apoye ciegamente en soluciones comerciales o gratuitas, aunque éstas, no siempre identifican y decodifican toda la información o pueden incluso dar falsos positivos. No se puede encontrar una única solución forense que abarque, ni la totalidad de aplicaciones de IM, ni la totalidad de sus funcionalidades, por ello se hace necesario disponer de varias de estas soluciones para cubrir el amplio espectro de las aplicaciones móviles del mercado. Muchas soluciones comerciales basan su listado de aplicaciones de IM en función del número de descargas, la popularidad de la aplicación o incluso en la petición de análisis de una determinada aplicación por parte de potenciales clientes. El especialista forense digital debe ejercer como tal y no centrar el análisis forense de los clientes móviles de las aplicaciones de IM en el resultado que obtiene de este tipo de soluciones. En el caso específico del cliente móvil de la aplicación de IM Telegram Messenger para los sistemas operativos Windows Phone y Android se comprueba que, en el momento del desarrollo de los estudios técnico-forenses que a continuación se exponen, las principales soluciones forenses comerciales (UFED de Cellebrite, Oxygen Forensics Analysis de Oxygen Forensics o IEF de Magnet Forensics) no realizaban el análisis forense en el caso de WP o efectuaban un análisis forense limitado en el caso de Android.

A continuación, se desarrollarán los tres métodos de estudios incluidos en la metodología de análisis propuesta, exponiendo los resultados obtenidos de aplicar esta metodología al análisis forense sobre el cliente de móvil de la aplicación de mensajería instantánea Telegram Messenger para Android y Windows Phone.

4.3 Análisis de Telegram Messenger en Android

Este punto expondrá el resultado obtenido del estudio de fuentes abiertas, de artefactos y de código fuente, incluidos en la metodología de análisis forense propuesta, sobre los registros que genera el cliente móvil de aplicación de IM Telegram Messenger sobre el sistema operativo Android.

4.3.1 Estudio de fuentes abiertas

El estudio de fuentes abiertas ha sido desarrollado a partir de los procedimientos descritos en el punto 3.3.1 de esta Tesis. Estos procedimientos permitirán recopilar de manera fiable toda aquella documentación que pueda de una u otro forma contribuir en el análisis forense del cliente móvil de la aplicación de IM Telegram Messenger para sistema operativo Android.

El estudio de fuentes abiertas es realizado sobre los resultados obtenidos de las consultas realizadas en diferentes motores de búsqueda indexados de Internet (Bing, Google, Google Scholar, etc.), a partir de la búsqueda de diferentes palabras clave en diferentes idiomas (Telegram Messenger, Android, Instant Messenger, IM, Forensics, Forense, Analysis, Análisis, etc.). En el momento del estudio de fuentes abiertas como resultado de la búsqueda realizada se encuentran, varios artículos, varios estudios técnicos, así como información técnica del desarrollador de la aplicación.

En los artículos *Digital Forensic Analysis of Telegram Messenger on Android Devices* (G. B. Satrya, P. T. Daely, & M. A. Nugroho., 2016) y *Forensic analysis of Telegram Messenger on Android smartphones* (Anglano, C., Canonico, M., & Guazzone, M., 2017), sus autores desarrollan el estudio de los artefactos generados por el cliente móvil de la aplicación de IM Telegram Messenger en el sistema operativo Android a través del análisis comparativo de artefactos, si bien estos artículos identifican los artefactos, aunque no decodifican la totalidad de rastros. Estos estudios al ser examinados son utilizados como documentación de apoyo para el análisis forense del cliente móvil de la aplicación de IM Telegram Messenger en Android.

En los estudios técnicos *Telegram investigation*[26] y *Telegram App Store Secret-Chat Messages in Plain Text Database*[27], sus autores analizan la base de datos del cliente móvil de la aplicación Telegram Messenger sobre iOS con la solución forense comercial EnCase Forensics y las conversaciones secretas generadas por el cliente móvil la aplicación de IM Telegram Messenger sobre Android respectivamente. Estos estudios al ser examinados son utilizados como documentación de apoyo para el análisis forense del cliente móvil de la aplicación de IM Telegram Messenger en Android.

Por último, en la página web del desarrollador de la aplicación Telegram Messenger[28] se encuentra el listado detallado de las estructuras de datos utilizadas por este para gestionar la información de la aplicación. En este caso, la información proporcionada por el propio desarrollador de la aplicación será utilizada como apoyo en el análisis forense de cliente móvil de la aplicación de IM Telegram Messenger para Android. La figura 4.1, muestra impresión de pantalla de parte de la página web del desarrollador en la cual se exponen los diferentes tipos de datos ("userSelf", "userForeign", "chatEmpty", "chatFull", etc.) incluidos en los diferentes objetos ("User", "UserProfilePhoto"[29], "UserStatus", "Chat", etc.) que almacenan la información de la aplicación Telegram Messenger.

[26] Digirec Mobile Forensics. (2015). *Telegram investigation*. Recuperado el 4 de octubre de 2016, de: http://www.mobileforensics.eu/en/telegram-investigation/.

[27] Patterson, J. (2015). *Telegram App Store Secret- Chat Messages in Plain Text Database*. Recuperado el 4 de octubre de 2016, de: https://blog.zimperium.com/telegram-hack/.

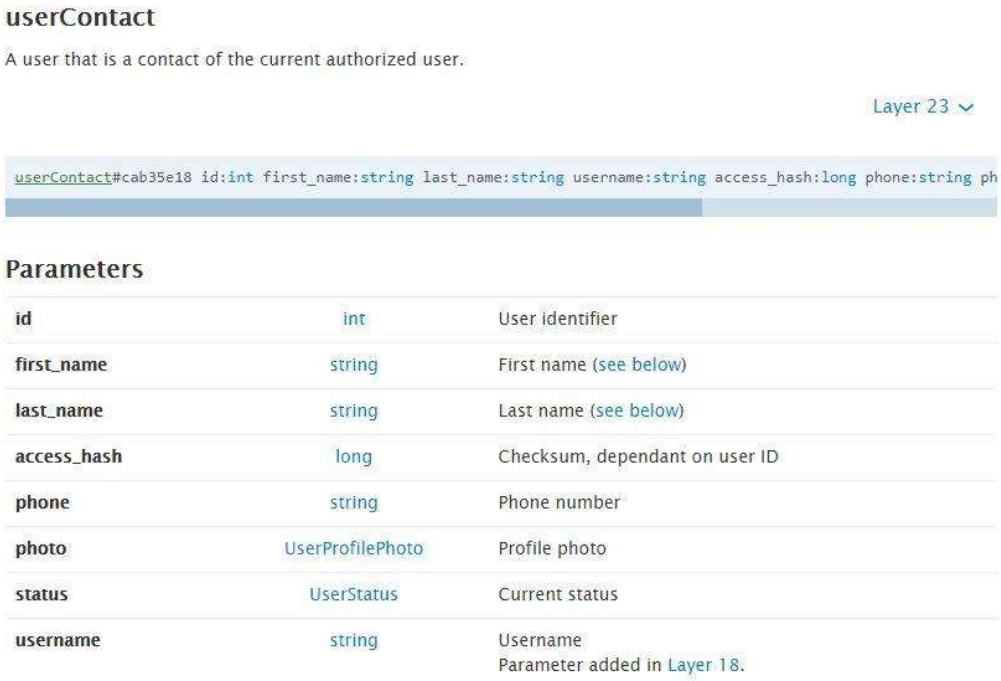
[28] Telegram Messenger. (2016). *Schema*. Recuperado el 7 de octubre de 2016, de: https://core.telegram.org/schema.

[29]Telegram Messenger. (2016). *userProfilePhoto*. Recuperado el 7 de octubre de 2016, de: https://core.telegram.org/constructor/userProfilePhoto.

```
userEmpty#200250ba id:int = User;
userSelf#7007b451 id:int first_name:string last_name:string username:string phone:string photo:UserProfilePhoto
userContact#cab35e18 id:int first_name:string last_name:string username:string access_hash:long phone:string ph
userRequest#d9ccc4ef id:int first_name:string last_name:string username:string access_hash:long phone:string ph
userForeign#75cf7a8 id:int first_name:string last_name:string username:string access_hash:long photo:UserProfil
userDeleted#d6016d7a id:int first_name:string last_name:string username:string = User;

userProfilePhotoEmpty#4f11bae1 = UserProfilePhoto;
userProfilePhoto#d559d8c8 photo_id:long photo_small:FileLocation photo_big:FileLocation = UserProfilePhoto;

userStatusEmpty#9d05049 = UserStatus;
userStatusOnline#edb93949 expires:int = UserStatus;
userStatusOffline#8c703f was_online:int = UserStatus;
userStatusRecently#e26f42f1 = UserStatus;
userStatusLastWeek#7bf09fc = UserStatus;
userStatusLastMonth#77ebc742 = UserStatus;

chatEmpty#9ba2d800 id:int = Chat;
chat#6e9c9bc7 id:int title:string photo:ChatPhoto participants_count:int date:int left:Bool version:int = Chat;
chatForbidden#fb0ccc41 id:int title:string date:int = Chat;

chatFull#630e61be id:int participants:ChatParticipants chat_photo:Photo notify_settings:PeerNotifySettings = Ch
```

Figura 4.1. Ejemplo de objetos y sus estructuras de datos dinámicas. Fuente: https://core.telegram.org/schema.

La figura 4.2 muestra a modo de ejemplo la estructura de datos del tipo “userContact”, correspondiente al objeto “User” en la cual se almacena la información de un usuario de tipo contacto. En esta figura se observa como la estructura del tipo “userContact” contiene entre otros, los campos relativos al nombre (“first_name”), apellidos (“last_name”), número de teléfono (“phone”) o foto de contacto (“photo”).



userContact

A user that is a contact of the current authorized user.

Layer 23

```
userContact#cab35e18 id:int first_name:string last_name:string username:string access_hash:long phone:string ph
```

Parameters

id	int	User identifier
first_name	string	First name (see below)
last_name	string	Last name (see below)
access_hash	long	Checksum, dependant on user ID
phone	string	Phone number
photo	UserProfilePhoto	Profile photo
status	UserStatus	Current status
username	string	Username Parameter added in Layer 18.

Figura 4.2. Estructura de datos del tipo de objeto "userContact". Fuente: https://core.telegram.org/schema.

Del análisis de la información obtenida en el estudio de fuentes abiertas se puede inferir que el cliente móvil de la aplicación de mensajería instantánea Telegram Messenger en el sistema operativo Android puede utilizar una serie de objetos, tipos y estructuras de datos dinámicas para gestionar la información de usuario, así como que la información relativa a las comunicaciones de usuario se almacena en una base de datos.

Tal y como se reflejará en el siguiente punto, el estudio de fuentes abiertas realizado será utilizado para identificar, decodificar, interpretar y validar la información analizada en el estudio estático de artefactos.

4.3.2 Estudio de artefactos

El estudio de artefactos ha sido desarrollado a partir de los procedimientos descritos en el punto 3.3.2 de esta Tesis. Estos procedimientos permitirán identificar, decodificar e interpretar los rastros generados por el cliente de móvil de la aplicación de mensajería instantánea Telegram Messenger en el sistema operativo Android a partir del análisis comparativo de registros.

4.3.2.1 Análisis forense estático

A continuación, se muestran los resultados obtenidos del análisis comparativo realizado sobre los rastros generados por el cliente de móvil de la aplicación de IM Telegram Messenger en el sistema operativo Android. Este ha sido elaborado a partir del análisis forense estático incluido en el estudio de artefactos de la metodología propuesta, el cual permite identificar, decodificar e interpretar los rastros generados por este cliente en este sistema operativo. La tabla 4.1 muestra, el listado artefactos generados por el cliente móvil de la aplicación de mensajería instantánea Telegram Messenger en Android.

Tabla 4.1. Artefactos generados por el cliente móvil de la aplicación de IM Telegram Messenger en Android.

#	Contenido	Directorio	Fichero/s
1	Ficheros de aplicación.	/data/app/org.telegram.messenger-1/	Diferentes ficheros (base.apk, base.odex, etc.).
2	Ficheros de aplicación.	/data/app/org.telegram.messenger/lib/	libtmessages.19.so
3	Ficheros de configuración y preferencias.	/data/data/org.telegram.messenger/shared_prefs/	Diferentes ficheros (userconfig.xml, logininfo.xml, mainconfig.xml, etc.).
4	Ficheros de usuario.	/data/data/org.telegram.messenger/files/	Diferentes ficheros (cache4.db, tgnet.dat, etc.).
5	Otros ficheros.	/data/data/org.telegram.messenger/code_cache/	com.android.opengl.shaders_cache
6	Otros ficheros.	/data/data/org.telegram.messenger/no_backup/	com.google.android.gms.appid-no-backup
7	Ficheros de cache.	/data/data/org.telegram.messenger/cache/	Diferentes ficheros (“.jpg”, “.mp4”, etc.).
8	Ficheros multimedia	/mnt/sdcard/Telegram/	Diferentes carpetas (Video, Audio, Documentos, Imágenes).

4.3.2.1.1 Análisis de ficheros de configuración y preferencias

Los ficheros “mainconfig.xml” y “userconfig.xml” corresponden con los archivos de datos que almacenan la información de configuración de la aplicación y las preferencias usuario respectivamente.

Del estudio realizado del archivo “mainconfig.xml” a partir de la metodología de análisis propuesta en la presente Tesis, se desprende que el mismo contiene la definición de variables y valores, correspondientes con los parámetros de configuración de la aplicación Telegram Messenger. La figura 4.3 muestra el listado de estos campos, así como sus valores. Se pueden observar entre otros los campos “maxGroupCount”, “language”, “invitetext” y “maxMegagroupCount” que almacenan respectivamente, el

número máximo de integrantes en un grupo, el idioma en el que está configurada la aplicación, el texto que será enviado si envías un mensaje de invitación y el número máximo de integrantes en un grupo grande ("groupBigSize"), que es un tipo específico de grupo en la aplicación Telegram Messenger con características determinadas.

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
<int name="maxGroupCount" value="200" />
<int name="maxBroadcastCount" value="100" />
<string name="disabledFeatures">AAAAAA==
</string>
<long name="lastReloadStatusTime" value="1441796225447" />
<int name="selectedBackground" value="103" />
<int name="selectedColor" value="0" />
<boolean name="privacyAlertShowed" value="true" />
<int name="invitetexttime" value="1441562683" />
<boolean name="needGetStatuses" value="true" />
<string name="invitetext">Oye, cambiémonos a Telegram:
https://telegram.org/dl</string>
<int name="groupBigSize" value="10" />
</map>
```

Figura 4.3. Ejemplo del contenido del fichero de configuración "mainconfig.xml".

Así mismo, del estudio realizado sobre el archivo "userconfig.xml", a partir de la metodología de análisis propuesta en la presente Tesis, se desprende que el mismo contiene la definición de variables y valores correspondientes con los parámetros de la configuración propia del usuario de la aplicación. La figura 4.4 muestra el listado de estos campos, así como sus valores del fichero "userconfig.xml". En esta imagen se pueden observar, entre otros, los campos con nombre "appLocked", "lastUpdateVersion2", "lastSendMessageId" y "saveIncomingPhotos", los cuales indican respectivamente, si la aplicación tiene código de bloqueo para su acceso, la versión de la aplicación instalada, el identificador del último mensaje enviado y si el cliente móvil de la aplicación de IM Telegram Messenger guarda las fotos en la galería del dispositivo. Cierta información mostrada en la figura 4.4 ha sido ocultada para garantizar la privacidad del usuario.

Figura 4.4. Ejemplo del contenido del fichero de configuración “userconfig.xml”.

4.3.2.1.2 Análisis de los ficheros de datos de usuario

En este caso el análisis se centra en el estudio de las diferentes tablas (registros y campos) contenidas en el fichero “cache4.db”. Este fichero corresponde con la base de datos en la cual se almacenan entre otros datos, el listado de contactos de la aplicación o mensajes intercambiados.

Durante el análisis de la información, se han realizado diversas transformaciones en los datos para que los mismos sean mostrados en un formato legible, debido su complejidad no es objeto principal de este estudio el desarrollo de esas transformaciones realizadas.

4.3.2.1.2.1 Análisis de la información de contactos

La lista de contactos de la aplicación Telegram Messenger se gestiona a través de diversas tablas contenidas en el fichero “cache4.db”. La gestión de la lista de contactos de la aplicación se realiza con la importación de la lista de contactos de la agenda telefónica del dispositivo móvil, es decir, cada nuevo contacto añadido a la agenda telefónica se añade a la lista de contactos de la aplicación.

Entre las diferentes tablas que gestionan la lista de contactos de la aplicación, se encuentra la tabla “users”, la cual contiene información adicional (identificador único o foto de perfil de un contacto) a la almacenada por la agenda telefónica del dispositivo móvil. La tabla 4.2, muestra el listado de campos que tiene la tabla “users” así como su significado.

Tabla 4.2. Estructura de la tabla “users”. Base de datos “cache4.db”.

#	Tabla	Nombre del campo	Significado
1	users	RowID	Número de registro de la tabla.
2	users	uid	Identificador único de contacto.
3	users	name	Nombre del contacto.
4	users	status	Estado del contacto. (en línea, fuera de línea, etc.)
5	users	data	Información adicional del contacto. (formato binario)

La figura 4.5 muestra a modo de ejemplo como se organizan los datos de contacto de la aplicación de IM Telegram Messenger en la tabla “users”. En esta figura se pueden identificar los campos “uid”, “name”, “status” y “data” del registro número 10 cuyo contenido es “12819934”, “Rulo;;;”, “1445705078” y “BLOB” respectivamente. Cierta información mostrada en la figura 4.5 ha sido ocultada para garantizar la privacidad del usuario.

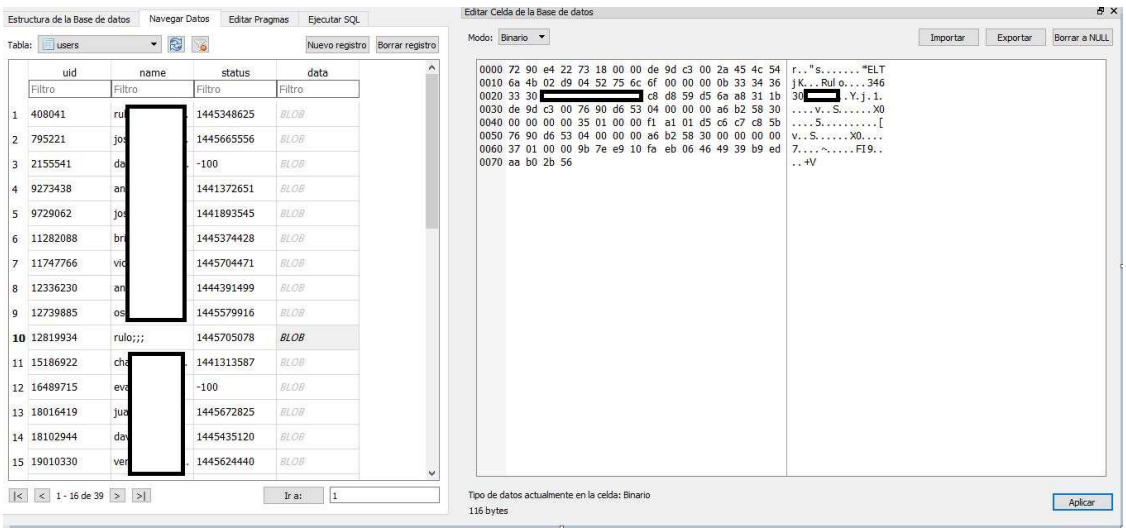


Figura 4.5. Ejemplo del contenido del campo “data”. Tabla “users” del fichero “cache4.db”.

Además del identificador único de usuario, nombre de usuario y estado, del análisis del campo “data” se puede obtener información adicional del contacto (número de teléfono del contacto, foto de perfil o la fecha de ultima conexión). La información del campo “data” se encuentra almacenada en formato binario siendo necesaria su decodificación para poder ser interpretada. La tabla 4.3 muestra la interpretación de los valores

hexadecimal del campo “data” mostrados en la figura 4.5. Cierta información mostrada en la tabla 4.3 ha sido ocultada para garantizar la privacidad del usuario.

Tabla 4.3. Interpretación de los datos del campo “data”.

#	Nombre de campo	Tamaño (bytes)	Valor del campo (Formato Hexadecimal)	Significado del campo
1	user type	4	0x7290E422	Tipo de usuario. Usuario contacto.
2	flags	4	0x73180000	Campos de la estructura de datos.
3	Id	4	0xDE9DC300	Identificador único de contacto. Valor: “12819934” .
4	access_hash	8	0x2A454C546A4B02D9	Hash de acceso.
5	first_name	variable	0x04 (longitud) 0x52756C6F (valor)	Nombre del contacto. Longitud de campo: 4; valor: “Rulo”.
6	last_name	variable	0x000	Segundo nombre del contacto. Valor: Vacío.
7	username	variable	0x000	Alias del contacto. Valor: Vacío.
8	phone	variable	0x0b (long) 0x3334363330???????????? (valor)	Número de teléfono del contacto. Longitud campo:11; valor: “34630??????”.
9	photo	variable	0xC8D859D5 - 0x7B077D38.	Foto de perfil de contacto.
10	status	4	0x4939B9ED	Estado del contacto.
11	expiration date	4	0xAAB02B56	Fecha de última conexión. Valor: “24/10/2015-16:24:10 GMT”.

Como se observa en la tabla 4.3, la información almacenada en este campo “data” se compone a su vez de campos fijos y variables, así como de estructuras de datos variables. El campo “photo” (fila 9, tabla 4.3) almacena en la estructura de datos de tipo “TL_UserProfilePhoto” del objeto “Photo” la información correspondiente a la foto del contacto (identificador, nombre de la foto, ubicación, etc.) en tal y como se refleja en la tabla 4.4.

Tabla 4.4. Interpretación de los datos de campo “photo”.

#	Nombre de campo	Tamaño (bytes)	Valor del campo (Hexadecimal)	Significado del campo
1	TL_UserProfilePhoto	4	0xC8D859D5	Tipo foto. Estructura foto de perfil.
2	TL_UserProfilePhoto.Id	4	0x6AA8311BDE9DC300	Identificador de foto.
3	TL_fileLocation	4	0x7690D653	Tipo localización. Estructura ubicación imagen pequeña.
4	TL_fileLocation.Dc_id	4	0x04000000	Identificador del centro de datos que contiene el archivo.
5	TL_fileLocation.Volume_id	8	0xA6B2583000000000	Identificador de volumen. Valor: “56144550”.
6	TL_fileLocation.local_id	4	0x35010000	Identificador de local. Valor: “309”.
7	TL_fileLocation.secret	8	0xF1A101D5C6C7C85B	Suma de comprobación para acceder al archivo.
8	TL_fileLocation	4	0x7690d653	Tipo localización. Estructura ubicación imagen grande.

9	TL_fileLocation.Dc_id	4	0x04000000	Identificador del centro de datos que contiene el archivo.
10	TL_fileLocation.volume_id	8	0xA6B2583000000000	Identificador de volumen: Valor: “56144550”.
11	TL_fileLocation.local_id	4	0x37010000	Identificador de local. Valor: “311”.
12	TL_fileLocation.secret	8	0x9B7EE910FAEB0646	Suma de comprobación para acceder al archivo.

Tras el análisis de las diferentes estructuras de datos que componen el campo “photo” se comprueba que este campo guarda la foto de perfil de contacto en miniatura y normal. A partir de los campos “volume_id” (filas 5 y 10, tabla 4.4) y “local_id” (filas 6 y 11, tabla 4.4) se pueden obtener los nombres de los ficheros que almacenan la foto en miniatura y normal. En el caso del usuario con identificador “12819934” (fila 3, tabla 4.3) el nombre de los ficheros que almacenan la foto de contactos en miniatura y normal son “56144550_309.jpg” (formato: registro5_registro6.jpg) y “56144550_311.jpg” (formato: registro10_registro11.jpg) respectivamente.

4.3.2.1.2.2 Análisis de la información de mensajes

Al igual que en el caso de los contactos, la información de mensajes intercambiados a través del cliente móvil de la aplicación de IM Telegram Messenger en Android se gestiona también a través de las tablas contenidas en el fichero “cache4.db”. Los mensajes de la aplicación Telegram Messenger pueden ser intercambiados a través de diferentes tipos de chats (personal, grupo o canal).

Entre las diferentes tablas que gestionan los mensajes de la aplicación se encuentra la tabla “messages” la cual centra el contenido de los mensajes que se realizan a través de los diferentes tipos de chat. La tabla 4.5 muestra a modo de ejemplo la estructura de campos de la tabla “messages”, así como el significado de su contenido.

Tabla 4.5. Estructura de la tabla “messages”. Base de datos “cache4.db”.

#	Tabla	Campo	Significado
1	messages	rowID	Número de registro de la tabla.
2	messages	mid	Identificador único de mensaje.
3	messages	uid	Identificador único de contacto.
4	messages	read_state	Estado de lectura del mensaje. (2: sin leer; 3: leído, etc.).
5	messages	send_state	Estado de envío de mensaje. (0: enviado; 1: sin enviar, etc.).
6	messages	date	Fecha y hora del mensaje enviado / recibido del mensaje.
7	messages	data	Información adicional del mensaje.

8	messages	out	Origen del mensaje (enviado / recibido).
9	messages	ttl	Valor dependiente del tipo de conversación. Campo utilizado en conversaciones entre usuarios.
10	messages	media	Tipo de archivos multimedia.
11	messages	replydata	Indica si el mensaje ha sido reenviado desde otra conversación.

4.3.2.1.2.2.1 Análisis de mensajes normales

Los mensajes normales son aquellos mensajes que son intercambiados desde el cliente móvil de la aplicación de IM Telegram Messenger entre los diferentes tipos de chat (personal, grupo o canal).

La figura 4.6 muestra a modo de ejemplo los registros que se pueden encontrar en la tabla "messages". En esta figura se pueden identificar entre otros, los datos relativos al registro cuyo campo "RowID" tiene el valor "8". Este registro almacena los valores "8", "12819934", "3", "0", "1445704329", "BLOB", "0", "0", "-1" y "NULL" para los campos "mid", "uid", "read_state", "send_sate", "date", "data", "out", "ttl" "media" y "replydata". El registro cuyo campo "RowID" tiene el valor "8" contiene la información relativa a un mensaje normal enviado por el contacto con identificador único de usuario "12819934" (contacto con nombre "Rulo") el sábado 24 de octubre de 2015 a las 16 horas 32 minutos y 09 segundos.

Tabla: messages

	mid	uid	read_state	send_state	date	data	out	ttl	media	replydata	imp
	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro
1	1	12819934	3	0	1445703564	BLOB	0	0	-1	NULL	0
2	2	12819934	3	0	1445703567	BLOB	0	0	-1	NULL	0
3	3	12819934	3	0	1445703577	BLOB	1	0	-1	NULL	0
4	4	12819934	3	0	1445703671	BLOB	0	0	-1	NULL	0
5	5	12819934	3	0	1445704294	BLOB	1	0	-1	NULL	0
6	6	12819934	3	0	1445704303	BLOB	1	0	-1	NULL	0
7	7	12819934	3	0	1445704327	BLOB	0	0	-1	NULL	0
8	8	12819934	3	0	1445704329	BLOB	0	0	-1	NULL	0
9	9	12819934	3	0	1445704337	BLOB	0	0	-1	NULL	0
10	10	12819934	3	0	1445704344	BLOB	1	0	-1	NULL	0

Figura 4.6. Ejemplo del contenido de la tabla "messages" del fichero "cache4.db".

El campo "data", al igual que sucede en el caso de contactos, almacena la información adicional del mensaje en formato binario (tipo de dato "BLOB"). En la figura 4.7 se muestra el contenido del campo "data" del registro cuyo campo "RowID" tiene el valor "8". Este campo es esencial, ya que en el mismo se define entre otras cosas, el tipo de mensaje (normal, secreto, de servicio, etc.), el texto del mensaje, identificador de contacto

de envío y recepción, etc. El tipo del mensaje viene identificado a través de los primeros 4 bytes de este campo "data", correspondiendo el valor hexadecimal "136CA65B" a un mensaje de tipo normal.

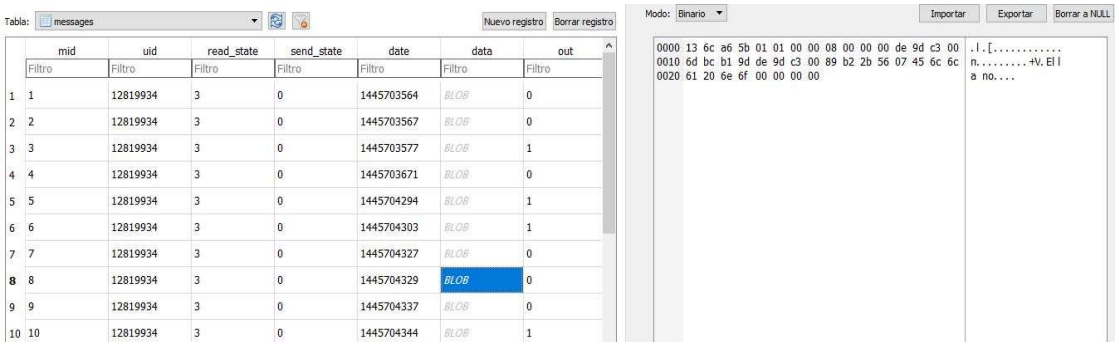


Figura 4.7. Ejemplo del campo "data" de la tabla "messages" del fichero "cache4.db". Mensaje normal.

La tabla 4.6 identifica los campos almacenados en el campo "data" de la figura 4.7, e interpreta de los valores, así como indica el significado de su contenido.

Tabla 4.6. Interpretación de los datos del campo binario "data".

#	Nombre del campo	Tamaño (bytes)	Valor	Significado
1	message type	4	0x136CA65B	Estructura tipo de mensaje. Mensaje normal.
2	flags	4	0x01010000	Campos de la estructura de datos.
3	Id	4	0x08000000	Identificador de mensaje. Valor: "8".
4	from_id	4	0xDE9DC300	Identificador único de contacto. Origen del mensaje. Valor: "12819934".
5	to_id	8	0x6DBCB19DDE9DC300	Identificador único de contacto. Destino del mensaje. Estructura tipo Peer.
6	date	4	0x89B22B56	Fecha del mensaje. Valor: "24/10/2015 16:32:09 PM- GMT".
7	message	variable	0x07 (longitud) 0x456C6C61206E6F(valor)	Mensaje. Longitud campo: 7; valor: "Ella no".
8	media	4	0x00000000	Tipo de adjunto. Sin adjunto.

Como se observa en la tabla 4.6, la información almacenada en este campo "data" se compone a su vez de campos fijos y variables, así como de estructuras de datos variables. El campo "message" (fila 7, tabla 4.6) almacena en un campo variable (longitud del campo y valor del campo) el mensaje transmitido. El campo "to_id" (fila 5, tabla 4.6) almacena en la estructura de datos de tipo "TL_peerUser" del objeto "Peer" la

información correspondiente al contacto que envía el mensaje en tal y como se refleja en la tabla 4.7.

Tabla 4.7. Interpretación de los datos del campo “to_id”.

#	Nombre de campo	Tamaño (bytes)	Valor del campo (Hexadecimal)	Significado del campo
1	TL_peerUser	4	0x6DBCB19D	Tipo Peer. Estructura de usuario.
2	TL_peerUser.User_id	4	0xDE9DC300	Identificador de usuario. Valor: “12819934”.

4.3.2.1.2.2.2 Análisis de mensajes secretos

Los mensajes secretos son aquellos mensajes que son transmitidos desde el cliente móvil de la aplicación de IM Telegram Messenger con una capa de seguridad extra. Este tipo de mensajes solo se transmite de persona a persona (*user-to-user*) a través del cliente móvil, nunca entre otros tipos de chat (grupos o canales) o clientes (web o de escritorio).

La figura 4.8 muestra a modo de ejemplo los registros que se pueden encontrar en la tabla “messages”. En esta figura se pueden identificar entre otros, los datos relativos al registro cuyo campo “RowID” tiene el valor “219”. Este registro almacena los valores “-222721”, “2067140791465148416”, “1”, “0”, “1441194402”, “BLOB”, “1”, “0”, “-1” y “NULL” para los campos “mid”, “uid”, “read_state”, “send_sate”, “date”, “data”, “out”, “ttl” “media” y “replydata”. El registro cuyo campo “RowID” tiene el valor “219” contiene la información relativa a un mensaje secreto enviado por el contacto con identificador único de usuario “2067140791465148416” el miércoles 2 de septiembre de 2015 a las 11 horas 46 minutos y 42 segundos.

Tabla: messages

	mid	uid	read_state	send_state	date	data	out	ttl	media	replydata
	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro
212	-222828	2067140791465148416	1	0	1441213563	BLOB	1	0	-1	NULL
213	-222827	2067140791465148416	1	0	1441213558	BLOB	1	0	-1	NULL
214	-222826	2067140791465148416	1	0	1441213533	BLOB	0	0	-1	NULL
215	-222725	2067140791465148416	1	0	1441194402	BLOB	1	0	-1	NULL
216	-222724	2067140791465148416	1	0	1441194402	BLOB	1	0	-1	NULL
217	-222723	2067140791465148416	1	0	1441194402	BLOB	1	0	-1	NULL
218	-222722	2067140791465148416	1	0	1441194402	BLOB	1	0	-1	NULL
219	-222721	2067140791465148416	1	0	1441194402	*BLOB*	1	0	-1	NULL
220	-222720	2067140791465148416	1	0	1441194402	BLOB	1	0	-1	NULL
221	-222628	2067140791465148416	1	0	1441134190	BLOB	1	0	-1	NULL

Figura 4.8. Contenido de los mensajes intercambiados. Tabla “messages” del fichero “cache4.db”.

Al igual que sucede en el caso de los mensajes normales, el campo "data" se pueden encontrar almacenada información adicional. En la figura 4.9 se muestra el contenido del campo "data" del registro cuyo campo "RowID" tiene el valor "219". Este campo "data" es esencial, ya que en el mismo se define entre otras cosas, el tipo de mensaje (normal, secreto, de servicio, etc.), el texto del mensaje, identificador de contacto de envío y recepción, etc. El tipo del mensaje viene identificado a través de los primeros 4 bytes de este campo "data", correspondiendo el valor hexadecimal "F8555555" a un mensaje de tipo secreto. Cierta información mostrada en la figura 4.9 ha sido ocultada para garantizar la privacidad del usuario.

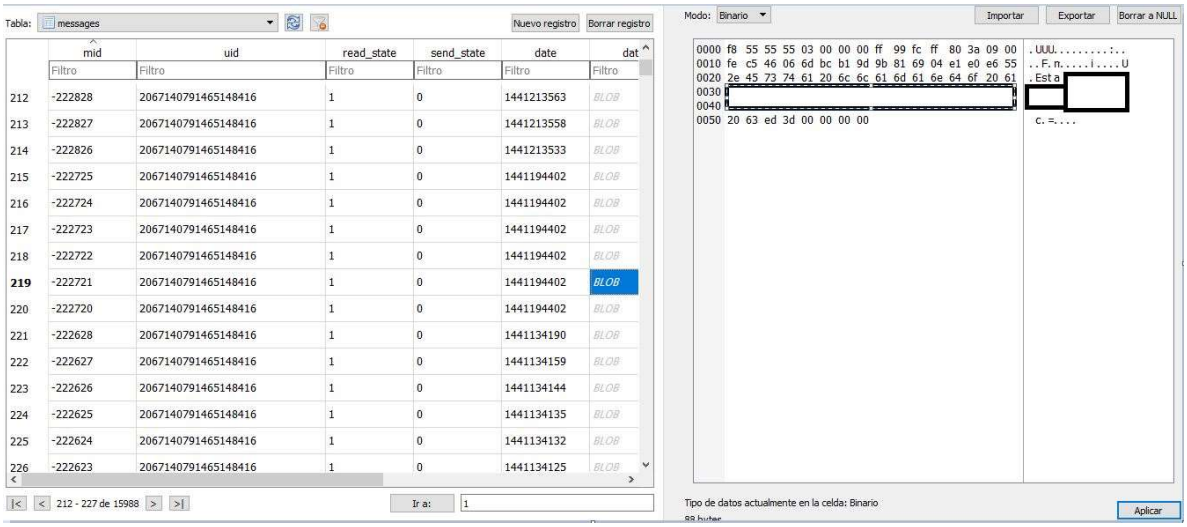


Figura 4.9. Contenido del registro de mensaje secreto y su campo "data". Tabla "messages" del fichero "cache4.db".

La tabla 4.8 identifica los campos almacenados en el campo "data" de la figura 4.9, e interpreta de los valores, así como indica el significado de su contenido. Cierta información mostrada en la tabla 4.18 ha sido ocultada para garantizar la privacidad del usuario.

Tabla 4.8. Interpretación de los datos del campo binario "data".

#	Nombre del campo	Tamaño (bytes)	Valor del campo (Hexadecimal)	Significado
1	message type	4	0xF8555555	Tipo de mensaje. Mensaje secreto.
2	flags	4	0x03000000	Campos de la estructura de datos.
3	Id	4	0xFF99FCFF	Identificador de mensaje. Valor: "-222721".

4	Ttl	4	0x803A0900	Tiempo de vida del mensaje. Valor: “604800”.
5	from_id	4	0xFEC54606	Identificador unico de contacto (desde donde se envia el mensaje). Valor: “105301502”.
6	to_id	8	0x6DBCD19D9B816904	dentificador unico de contacto (hacia donde se envia el mensaje). Valor: “74023323”.
7	date	4	0x89B22B56	Fecha del mensaje. Valor: “2/09/2015 11:43:29 AM – GMT”.
	message	variable	0x2E (longitud) 0x4573746120 - 002063ED3D (valor)	Mensaje. Longitud de campo:46; Valor: “Esta ?????????????????????????????? c”.
9	media	4	0x00000000	Tipo de adjunto. Sin adjunto.

Como se observa en la tabla 4.8, la información almacenada en este campo “data” se compone a su vez de campos fijos y variables, así como de estructuras de datos variables. El campo “to_id” (fila 6, tabla 4.8) almacena en la estructura de datos de tipo “TL_peerUser” del objeto “Peer” la información correspondiente al contacto que envía el mensaje en tal y como se refleja en la tabla 4.9.

Tabla 4.9. Interpretación de los datos del campo “to_id”.

#	Nombre de campo	Tamaño (bytes)	Valor del campo (Hexadecimal)	Significado del campo
1	TL_peerUser	4	0x6DBCB19D	Tipo Peer. Estructura de usuario.
2	TL_peerUser.User_id	4	0x9B816904	Identificador de usuario. Valor: “74023323”.

4.3.3 Estudio de código fuente

El estudio de código fuente ha sido desarrollado a partir de los procedimientos descritos en el punto 3.3.3 de esta Tesis. Estos procedimientos permitirán identificar, decodificar, interpretar y validar los registros generados por el cliente móvil de la aplicación de mensajería instantánea Telegram Messenger en el sistema operativo Android a partir del análisis de código fuente.

En el caso del cliente móvil de la aplicación Telegram Messenger para el sistema operativo móvil Android el propio desarrollador de la aplicación proporciona el código fuente [30]. Al realizar el estudio de código fuente de la aplicación, se observa que el mismo se encuentra escrito en lenguaje “java”, siendo este un lenguaje orientado a objetos. El

[30] Telegram Messenger. (2016). *Telegram Applications*. Recuperado el 4 de octubre 2016, de: https://telegram.org/apps.

código fuente del cliente móvil de la aplicación de IM Telegram Messenger para Android contiene alrededor de 821 ficheros con extensión ".java", encontrándose solamente el fichero con el nombre "TLRPC.java" un total de 28.539 líneas de código.

Entre los diferentes ficheros que contiene el código fuente del cliente móvil de la aplicación de IM Telegram Messenger para Android se encuentra el archivo con nombre "UserConfig.java" el cual se aloja en la carpeta "Telegram-master/TMessagesProj/src/main/java/org/telegram/messenger/". Este archivo contiene entre otras, las funciones de lectura y escritura de datos en el fichero de configuración "userconfig.xml". La figura 4.10 muestra parte de la función "saveConfig" ubicada en el fichero de código fuente con nombre "USerConfig.java". En esta figura se observan los diferentes campos ("saveIncomingPhotos", "appLocked", "passcodeType", "allowScreenCapture", etc.) que son almacenados en el fichero de configuración "userconfig.xml".

```
public static void saveConfig(boolean withFile, File oldFile) {
    synchronized (sync) {
        try {
            SharedPreferences preferences = ApplicationLoader.applicationContext.getSharedPreferences("userconfing", Context.
            MODE_PRIVATE);
            SharedPreferences.Editor editor = preferences.edit();
            editor.putBoolean("registeredForPush", registeredForPush);
            editor.putString("pushString2", pushString);
            editor.putInt("lastSendMessageId", lastSendMessageId);
            editor.putInt("lastLocalId", lastLocalId);
            editor.putString("contactsHash", contactsHash);
            editor.putBoolean("saveIncomingPhotos", saveIncomingPhotos);
            editor.putInt("lastBroadcastId", lastBroadcastId);
            editor.putBoolean("blockedUsersLoaded", blockedUsersLoaded);
            editor.putString("passcodeHash1", passcodeHash);
            editor.putString("passcodeSalt", passcodeSalt.length > 0 ? Base64.encodeToString(passcodeSalt, Base64.DEFAULT) : "");
            editor.putBoolean("appLocked", appLocked);
            editor.putInt("passcodeType", passcodeType);
            editor.putInt("autoLockIn", autoLockIn);
            editor.putInt("lastPauseTime", lastPauseTime);
            editor.putLong("lastAppPauseTime", lastAppPauseTime);
            editor.putString("lastUpdateVersion2", lastUpdateVersion);
            editor.putInt("lastContactsSyncTime", lastContactsSyncTime);
            editor.putBoolean("useFingerprint", useFingerprint);
            editor.putInt("lastHintsSyncTime", lastHintsSyncTime);
            editor.putBoolean("draftsLoaded", draftsLoaded);
            editor.putBoolean("notificationsConverted", notificationsConverted);
            editor.putBoolean("allowScreenCapture", allowScreenCapture);
            editor.putBoolean("pinnedDialogsLoaded", pinnedDialogsLoaded);
```

Figura 4.10. Líneas de código de la función "saveConfig". Fichero "UserConfig.java".

Otro de los ficheros incluidos en el código fuente del cliente móvil de aplicación de IM Telegram Messenger es el archivo con nombre "TLRPC.java", el cual se aloja en la carpeta "Telegram-master/TMessagesProj/src/main/java/org/telegram/messenger/tgnet". Este archivo contiene diferentes funciones, entre las cuales se encuentran la lectura y escritura de los datos contenidos en el campo "data" de la tabla "messages". La figura 4.11 muestra parte de la función "readParams" contenida en el archivo "TLRPC.java",

en el cual se realiza la lectura de los parámetros del campo “data” (“flags”, “date”, “from_id”, “to_id”, “message”, “media”, etc.) de un mensaje secreto.

```
public static class TL_message_secret extends TL_message {
    public static int constructor = 0x555555f9;

    public void readParams(AbstractSerializedData stream, boolean exception) {
        flags = stream.readInt32(exception);
        unread = (flags & 1) != 0;
        out = (flags & 2) != 0;
        mentioned = (flags & 16) != 0;
        media_unread = (flags & 32) != 0;
        id = stream.readInt32(exception);
        ttl = stream.readInt32(exception);
        from_id = stream.readInt32(exception);
        to_id = Peer.TLdeserialize(stream, stream.readInt32(exception), exception);
        date = stream.readInt32(exception);
        message = stream.readString(exception);
        media = MessageMedia.TLdeserialize(stream, stream.readInt32(exception), exception);
        int magic = stream.readInt32(exception);
        if (magic != 0x1cb5c415) {
            if (exception) {
                throw new RuntimeException(String.format("wrong Vector magic, got %x", magic));
            }
            return;
        }
        int count = stream.readInt32(exception);
        for (int a = 0; a < count; a++) {
            MessageEntity object = MessageEntity.TLdeserialize(stream, stream.readInt32(exception), exception);
            if (object == null) {
                return;
            }
            entities.add(object);
        }
        if ((flags & 2048) != 0) {
            via_bot_name = stream.readString(exception);
```

Figura 4.11. Líneas de código de la función “readParams” de la clase “TL_message_secret”. Fichero “TLRPC.java”.

El estudio de las diferentes líneas de código fuente del cliente móvil de la aplicación de IM Telegram Messenger para Android ha sido utilizado para identificar las estructuras de datos estáticas y dinámicas almacenadas en la base de datos que almacenan la información del usuario. Así mismo, a través de este estudio se han podido identificar las diferentes transformaciones realizadas por este cliente, sobre los datos de usuario necesarias para poder interpretar y presentar en un formato legible para el ser humano las comunicaciones mantenidas a través de esta aplicación.

4.3.4 Resultados del análisis realizado

La metodología de análisis forense propuesta en la presente investigación y desarrollada en el estudio técnico-forense del cliente móvil de la aplicación de mensajería instantánea Telegram Messenger para el sistema operativo móvil Android desprende que:

a) Del estudio de las fuentes abiertas, correspondiente con la búsqueda de toda aquella información funcional, técnica y forense que pudiera encontrarse en cualquier fuente de datos abiertas o semiabiertas en el momento del estudio, se obtienen diversas fuentes de datos que pueden ser utilizadas, una vez analizadas, para apoyar el análisis forense del cliente móvil de la aplicación de IM Telegram Messenger para Android.

   Cada una de estas fuentes de datos es analizada individualmente, descartando aquellas que no ofrecen información de utilidad para el desarrollo del análisis forense de la aplicación. En el caso del cliente móvil de la aplicación de IM Telegram Messenger para Android se selecciona como fuente principal la proporcionada por el propio desarrollador, el cual expone cómo se organiza la información de la aplicación a partir de estructuras fijas y dinámicas de datos.

b) Del estudio de los artefactos, correspondiente al análisis forense estático de los rastros generados por el cliente móvil de la aplicación de IM Telegram Messenger, se obtienen tanto los registros generados por la aplicación como los datos relativos a las comunicaciones mantenidas por el usuario en un teléfono inteligente con sistema operativo Android.

   Estudiados los diferentes rastros generados a partir del análisis comparativo se identifica que, la información de configuración del cliente móvil de la aplicación Telegram Messenger en Android se almacena en ficheros con formato etiqueta (“XML”), siendo el contenido fácilmente decodificable e interpretable. Igualmente, a partir del análisis comparativo se identifica que, la información relativa a las comunicaciones de usuario la cual se encuentra almacenada en el fichero de nombre “cache4.db”. Tal y como ha quedado demostrado esta base de datos almacena información legible (metadatos de las comunicaciones) e

información ilegible (contenido de las comunicaciones). Para interpretar esta última, se debe utilizar la información obtenida tanto del estudio de fuentes abiertas como del estudio del código fuente, la cual ayudará a decodificar la información almacenada en las estructuras de datos para su correcta visualización.

c) Del estudio del código fuente, correspondiente al análisis de las líneas de código del lenguaje de programación "java" en el cual se encuentra desarrollado el cliente móvil de la aplicación Telegram Messenger para Android, se obtienen todos aquellos datos necesarios para identificar, decodificar, interpretar y validar la información obtenida del estudio de fuentes abiertas y del estudio estático de artefactos.

   De esta manera, a través de este estudio se analizan las diferentes funciones del código fuente de la aplicación identificando y validando las estructuras de datos almacenados en los ficheros de configuración de la propia aplicación y en la base de datos "cache4.db". Así mismo se analiza y coteja que tanto los objetos como las estructuras de datos dinámicas proporcionadas en la página web del desarrollador corresponden con los que se almacenan en los campos de la base de datos.

Tal y como ha quedado demostrado, la metodología de análisis forense propuesta permite identificar, decodificar, interpretar y validar la información generada por el cliente móvil de la aplicación de mensajería instantánea Telegram Messenger en el sistema operativo Android.

4.4 Análisis de Telegram Messenger en Windows Phone

Este punto expondrá el resultado obtenido del estudio de fuentes abiertas, de artefactos y de código fuente, incluidos en la metodología de análisis forense propuesta, sobre los registros que genera el cliente móvil de aplicación de IM Telegram Messenger sobre el sistema operativo Windows Phone.

4.4.1 Estudio de fuentes abiertas

El estudio de fuentes abiertas ha sido desarrollado a partir de los procedimientos descritos en el punto 3.3.1 de esta Tesis. Estos procedimientos permitirán recopilar de manera fiable toda aquella documentación que pueda de una u otro forma contribuir en el análisis forense del cliente de móvil de la aplicación de IM Telegram Messenger para sistema operativo Windows Phone.

El estudio de fuentes abiertas es realizado sobre los resultados obtenidos de las consultas realizadas en diferentes motores de búsqueda indexados de Internet (Bing, Google, Google Scholar, etc.), a partir de la búsqueda de diferentes palabras clave en diferentes idiomas (Telegram Messenger, Windows Phone, WP, Instant Messenger, Forensics, Analysis, Análisis, etc.). Debido a la cuota de mercado de dispositivos móviles con sistema operativo Windows Phone, en el momento del estudio de fuentes abiertas no se encuentran resultados en relación con el cliente móvil de la aplicación de IM Telegram Messenger más allá de la proporcionada por el propio desarrollador de la aplicación. Este facilita a través de su página web[31] información relativa a las estructuras de datos que gestionan la información de la aplicación de IM, la cual será utilizada de apoyo para el análisis forense del cliente móvil de la aplicación de IM Telegram Messenger en WP. En la figura 4.12, muestra impresión de pantalla de parte de la página web del desarrollador en la cual se exponen los diferentes tipos de datos (“messageEmpty”, “message”,

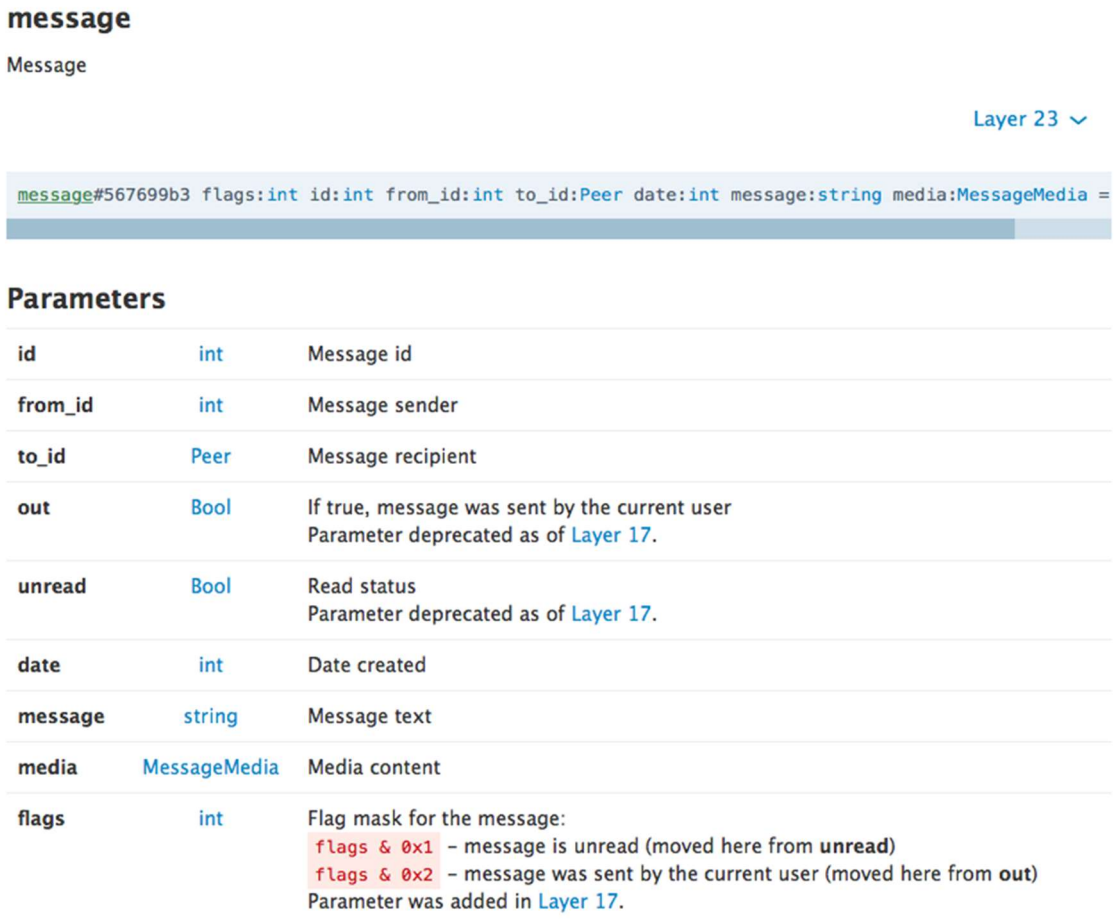
[31] Telegram Messenger. *Schema*. Recuperado el 20 de noviembre de 2016, de: https://core.telegram.org/schema.

"photoEmpty", "photo", etc.) incluidos en los diferentes objetos ("Message", "Photo", etc.) que almacenan la información de la aplicación Telegram Messenger.

```
messageEmpty#83e5de54 id:int = Message;
message#567699b3 flags:int id:int from_id:int to_id:Peer date:int message:string media:MessageMedia
= Message;
messageForwarded#a367e716 flags:int id:int fwd_from_id:int fwd_date:int from_id:int to_id:Peer date:
int message:string media:MessageMedia = Message;
messageService#1d86f70e flags:int id:int from_id:int to_id:Peer date:int action:MessageAction = Mess
age;

messageMediaEmpty#3ded6320 = MessageMedia;
messageMediaPhoto#c8c45a2a photo:Photo = MessageMedia;
messageMediaVideo#a2d24290 video:Video = MessageMedia;
messageMediaGeo#56e0d474 geo:GeoPoint = MessageMedia;
messageMediaContact#5e7d2f39 phone_number:string first_name:string last_name:string user_id:int = Me
ssageMedia;
messageMediaDocument#2fda2204 document:Document = MessageMedia;
messageMediaAudio#c6b68300 audio:Audio = MessageMedia;

messageActionEmpty#b6aef7b0 = MessageAction;
messageActionChatCreate#a6638b9a title:string users:Vector<int> = MessageAction;
messageActionChatEditTitle#b5a1ce5a title:string = MessageAction;
messageActionChatEditPhoto#7fcb13a8 photo:Photo = MessageAction;
messageActionChatDeletePhoto#95e3fbef = MessageAction;
messageActionChatAddUser#5e3cfc4b user_id:int = MessageAction;
messageActionChatDeleteUser#b2ae9b0c user_id:int = MessageAction;

dialog#ab3a99ac peer:Peer top_message:int unread_count:int notify_settings:PeerNotifySettings = Dial
og;

photoEmpty#2331b22d id:long = Photo;
photo#22b56751 id:long access_hash:long user_id:int date:int caption:string geo:GeoPoint sizes:Vecto
r<PhotoSize> = Photo;
```

Figura 4.12. Ejemplo de objetos y sus estructuras de datos dinámicas. Fuente: https://core.telegram.org/schema.

En la figura 4.13, se muestra impresión de pantalla de la estructura de datos de tipo "message" correspondiente al objeto "Message" en la cual almacena la información correspondiente con los mensajes intercambiados por el usuario de la aplicación. En esta figura se observa como la estructura de tipo "message" almacena los campos identificador contacto origen ("from_id"), identificador contacto destino ("to_id"), estado del mensaje ("unread"), fecha del mensaje ("date"), texto del mensaje ("message") o archivo adjunto ("media").



message

Message

Layer 23

```
message#567699b3 flags:int id:int from_id:int to_id:Peer date:int message:string media:MessageMedia =
```

Parameters

id	int	Message id
from_id	int	Message sender
to_id	Peer	Message recipient
out	Bool	If true, message was sent by the current user Parameter deprecated as of Layer 17.
unread	Bool	Read status Parameter deprecated as of Layer 17.
date	int	Date created
message	string	Message text
media	MessageMedia	Media content
flags	int	Flag mask for the message: `flags & 0x1` – message is unread (moved here from **unread**) `flags & 0x2` – message was sent by the current user (moved here from **out**) Parameter was added in Layer 17.

Figura 4.13. Estructura de datos de tipo "message" del objeto "Message". Fuente: https://core.telegram.org/schema.

Del análisis de la información obtenida en el estudio de fuentes abiertas, se puede inferir que el cliente móvil de la aplicación de mensajería instantánea Telegram Messenger en el sistema operativo Windows Phone puede utilizar una serie de objetos, tipos y estructuras de datos estáticas y dinámicas para organizar la información del usuario.

Tal y como se reflejará en el siguiente punto, el estudio de fuentes abiertas realizado será utilizado para identificar, decodificar, interpretar y validar la información obtenida en el estudio estático de artefactos.

4.4.2 Estudio de artefactos

El estudio de artefactos ha sido desarrollado a partir de los procedimientos descritos en el punto 3.3.2 de esta Tesis. Estos procedimientos permitirán identificar, decodificar e interpretar los rastros generados por el cliente de móvil de la aplicación de mensajería instantánea Telegram Messenger en el sistema operativo Windows Phone a partir del análisis comparativo registros.

4.4.2.1 Análisis forense estático

A continuación, se muestran los resultados obtenidos del análisis comparativo realizado sobre los rastros generados por el cliente de móvil de la aplicación de IM Telegram Messenger en el sistema operativo Windows Phone. Este ha sido elaborado a partir del análisis forense estático incluido en el estudio de artefactos de la metodología propuesta, el cual permite identificar, decodificar e interpretar los rastros generados por este cliente en este sistema operativo.

La tabla 4.10 muestra, el listado artefactos generados por el cliente móvil de la aplicación de IM Telegram Messenger para WP.

Tabla 4.10. Artefactos generados por el cliente móvil de la aplicación de IM Telegram Messenger en WP.

#	Contenido	Fichero/s	Descripción
1	Ficheros de configuración	_ApplicationSettings. CommonNotifySettings.xml	Preferencias y configuración de notificaciones de la aplicación.
2	Ficheros de Log	{YYYY}-{MM}-{DD}.txt	Registro de eventos de la aplicación.
3	Datos de contactos	users.dat	Fichero de datos de contactos.
4	Datos de conversación y conversaciones cifrados	chats.dat, encryptedChats.dat	Ficheros de datos de conversaciones y conversaciones secretas.
5	Datos de dialogos y mensajes	dialogs.dat	Ficheros de datos de mensajes.
6	Ficheros temporales	temp_dialogs.dat, temp_users.dat, temp_chats.dat, temp_encryptedChats.dat etc.	Ficheros de datos temporales.
7	Ficheros multimedia	Video, audio, documentos, imágenes, etc.	Ficheros transferidos.
8	Datos varios.	allStickers.dat, broadcasts.dat, cachedServerFiles.dat, importedPhones.dat, passcode_params.dat, PeopleHub.dat, state.dat	Ficheros de datos con diferente información.

4.4.2.1.1 Análisis de ficheros de configuración y preferencias

Los ficheros "_ApplicationSettings" y "CommonNofifySettings.xml" se corresponden con los archivos de datos que almacenan información de ajustes de la aplicación y de usuario.

Del estudio realizado sobre el archivo "_ApplicationSettings" (fila 1, tabla 4.10) a través de la metodología de análisis propuesta en la presente Tesis se desprende que, este fichero contiene los registros donde se define diferentes parámetros de configuración del cliente móvil de la aplicación de IM Telegram Messenger para WP, como el país del número de teléfono ("country") o las direcciones IP y puertos de conexión a los servidores de la aplicación ("IpAddress v4", "IpAddress v6", "Port")

Así mismo, del estudio realizado sobre el fichero "CommonNofifySettings.xml" (fila 1, tabla 4.10) se desprende que, este fichero contiene los registros donde se almacenan las preferencias de notificaciones de usuario, como servicios de localización ("AskAllowingLocationServices"), sonidos para contactos ("ContactSound"), si el cliente móvil de la aplicación de IM Telegram Messenger este teléfono inteligente guarda las fotos en la galería del dispositivo ("SaveIncomingPhotos") o si al pulsar la tecla introducción en el teclado del teléfono inteligente se envía el mensaje ("SendByEnter").

El fichero con formato {YYYY}-{MM}-{DD}".txt" corresponden al archivo de eventos que almacena los registros relativos al funcionamiento del cliente móvil de la aplicación de IM Telegram Messenger (fila 2, tabla 4.10). El nombre de estos ficheros de texto corresponde con su fecha de creación.

La figura 4.14 muestra, a modo de ejemplo, parte de los registros generados por la aplicación el día 4 de octubre de 2016 en el fichero "2016-10-04.txt". En este fichero se almacenan eventos relativos al inicio la aplicación, a la actualización de datos o a la creación de un chat de tipo canal.

```
2016-10-04 09:56:39.622 Startup
2016-10-04 09:56:39.645 Launch
2016-10-04 09:56:42.956 UpdatesService.LoadStateAndUpdate 141 client_state=[p=132 d=1474999048 q=244093701]
2016-10-04 09:56:42.980 UpdatesService.LoadStateAndUpdate ptsList=[133, 135, 136]
2016-10-04 09:56:42.987 UpdatesService.LoadFileState processDiff state=[p=133 q=244093701 s=509 u_c=8 d=1475059547 [28/09/2016 12:45:47]]
messages=1 other=1 elapsed=00:00:00.0206945
Telegram.Api.TL.TLUpdateEncryption

2016-10-04 09:56:42.994 UpdatesService.LoadFileState processDiff state=[p=135 q=244093701 s=509 u_c=9 d=1475059734 [28/09/2016 12:48:54]]
messages=1 other=1 elapsed=00:00:00.0007361
TLUpdateReadHistoryOutbox peer=ChatId=125444893 max_id=84 pts=135 pts_count=0

2016-10-04 09:56:42.964 UpdatesService.LoadStateAndUpdate start LoadFileState
2016-10-04 09:56:43.007 UpdatesService.LoadStateAndUpdate LoadFileState publish UpdateCompletedEventArgs
2016-10-04 09:56:43.013 UpdatesService.LoadStateAndUpdate stop LoadFileState elapsed=00:00:00.0301694
2016-10-04 09:56:43.016 UpdatesService.LoadStateAndUpdate 141 start GetDifference
2016-10-04 09:56:43.029 UpdatesService.GetDifference 141 state=[p=136 d=1475059817 q=244093701]
2016-10-04 09:56:43.001 UpdatesService.LoadFileState processDiff state=[p=136 q=244093701 s=509 u_c=10 d=1475059817 [28/09/2016 12:50:17]]
messages=1 other=0 elapsed=00:00:00.0002994
2016-10-04 09:56:43.082 WNSPushService start creating channel
2016-10-04 09:56:43.092 ShellViewModel.UpdateChannels start count=null
2016-10-04 09:56:43.106 PushServiceBase.RegisterDeviceAsync channelUri=null
```

Figura 4.14. Lista de eventos correspondientes al fichero de Log “2016-10-04.txt”.

4.4.2.1.2 Análisis de los ficheros de datos de usuario

En este caso el análisis se centra en el estudio de los datos contenidos en los ficheros “users.dat”, “chats.dat”, “encryptedChats.dat” y “dialogs.dat”, los cuales almacenan, entre otros, la información relativa a los contactos de la aplicación, conversaciones, así como mensajes normales y secretos.

La figura 4.15 muestra a modo de ejemplo, que tipo de datos contienen cada uno de estos archivos, así como la relación entre los diferentes archivos de datos.

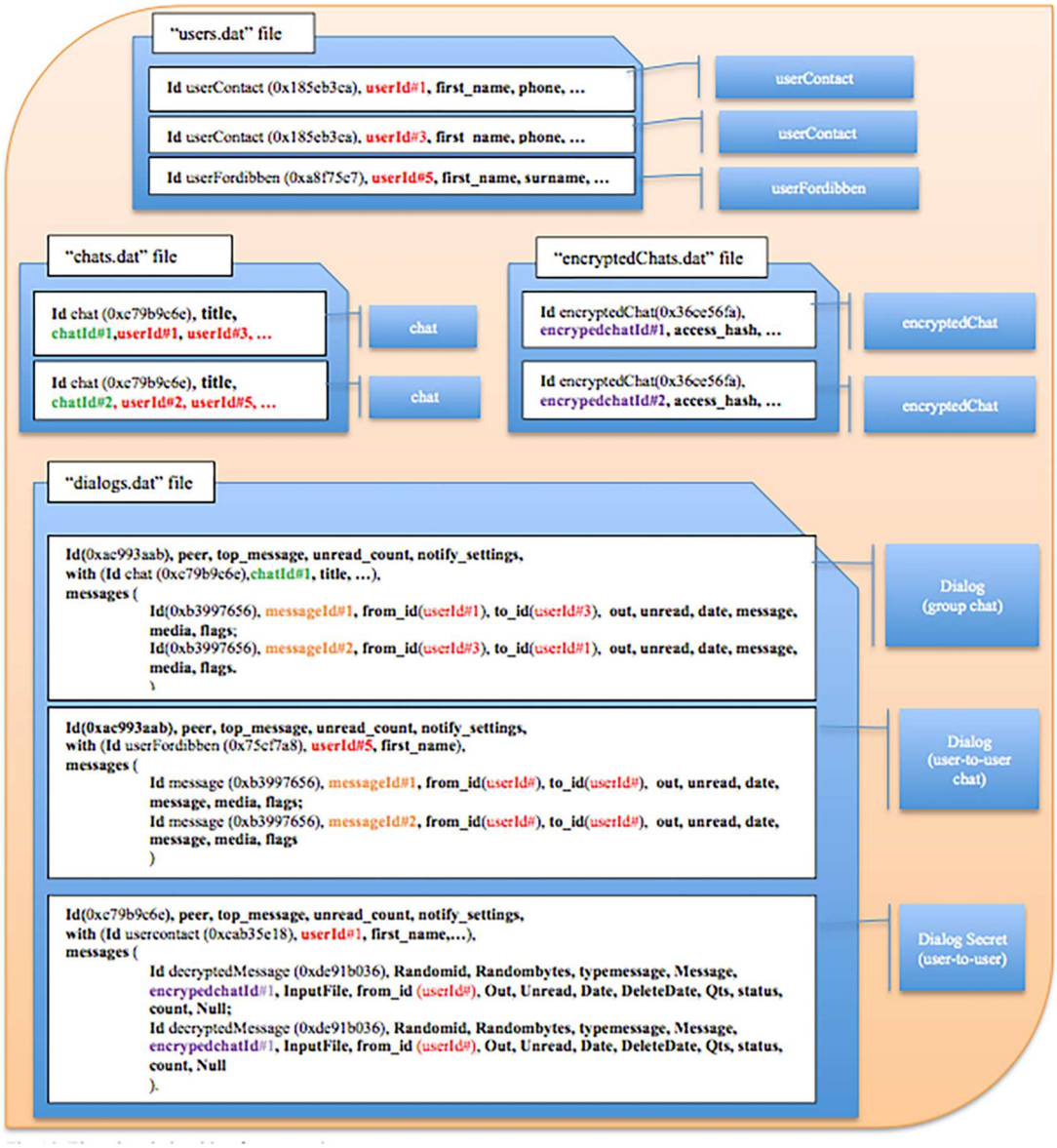


Figura 4.15. Visión global de ficheros y estructuras de datos de la aplicación de IM Telegram Messenger en WP.

Es necesario interpretar la información contenida en cada uno de estos ficheros de datos para extraer las conversaciones mantenidas por el usuario, ya que, de otra forma no se obtendría la totalidad de los datos relativos a los mensajes intercambiados.

4.4.2.1.2.1 Análisis de la información de contactos

Al igual que ocurre con cualquier otro tipo de aplicación (no solo de IM), la información que se obtiene de la agenda de contactos es de suma importancia en la investigación de un hecho delictivo. La información relativa a los contactos gestionados por el cliente móvil de la aplicación IM Telegram Messenger en WP se almacenan en el fichero de datos "users.dat". En este fichero se pueden encontrar los diferentes tipos de contactos disponibles para este cliente móvil (contacto, propietario, vacío, eliminado, etc.). Este tipo de contactos se organizan en las estructuras de datos dinámicas bajo el objeto "User". La tabla 4.11 muestra los diferentes tipos de contactos del objeto "User", así como su significado.

Tabla 4.11. Listado de tipos de usuario del objeto "User".

#	Objeto	Tipo	Nombre	Descripción
1	User	Contact	userContact	Usuario de la lista de contactos.
2	User	Request	userRequest	Usuario no incluido en la lista de contactos, pero se conoce el número de teléfono (ej. número de soporte de la aplicación, número telefónico 42777).
3	User	Foreing	userForeing	Usuario no incluido en la lista de contactos (ejemplo formato @{username}).
4	User	Deleted	userDeleted	Usuario eliminado de la aplicación.
5	User	Empty	userEmpty	Usuario vacío.
6	User	Owner	userSelf	Usuario propietario de la aplicación.

A continuación, la figura 4.16 muestra a modo de ejemplo, una simulación de las diferentes estructuras de datos expuestas en la tabla 4.11, que pueden ser encontradas en el fichero de datos "users.dat". Tal y como se observa en esta figura, las diferentes estructuras de datos disponen de un número diferente de campos en función del tipo de objeto que se trate.

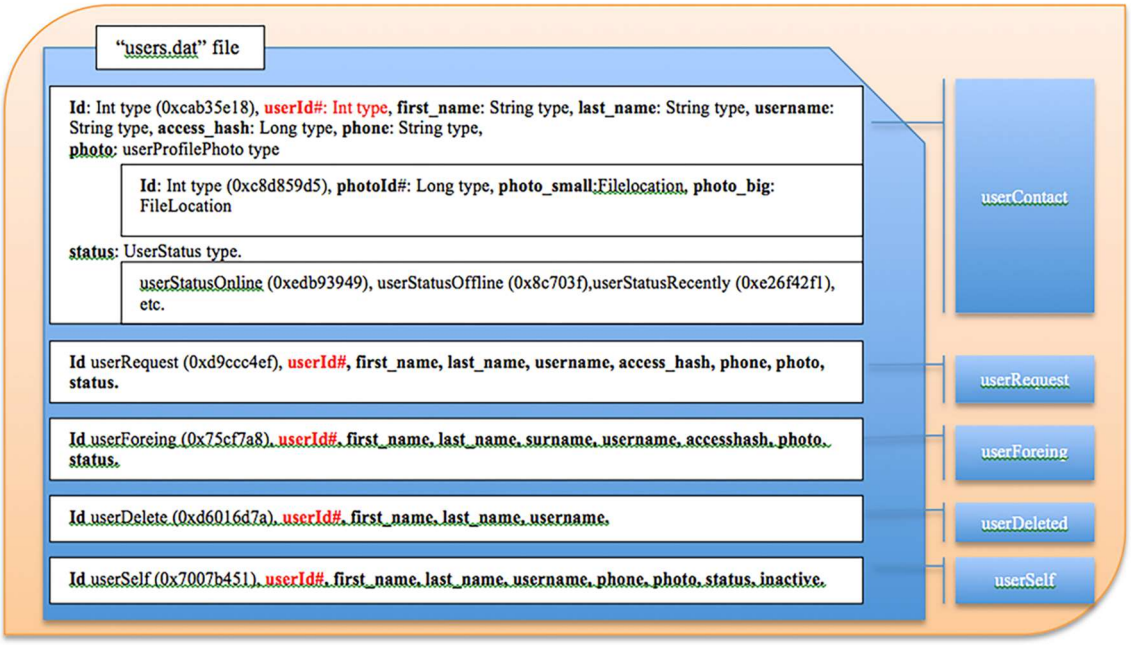


Figura 4.16. Estructuras de datos de los diferentes tipos de objetos del objeto "User" contenidos en el fichero "users.dat".

La figura 4.17 muestra a modo de ejemplo parte del fichero de datos "users.dat" en el cual se identifican los diferentes campos de la estructura de datos el tipo de objeto "userContact" del objeto "User". Cierta información mostrada en la figura 4.17 ha sido ocultada para garantizar la privacidad del usuario.

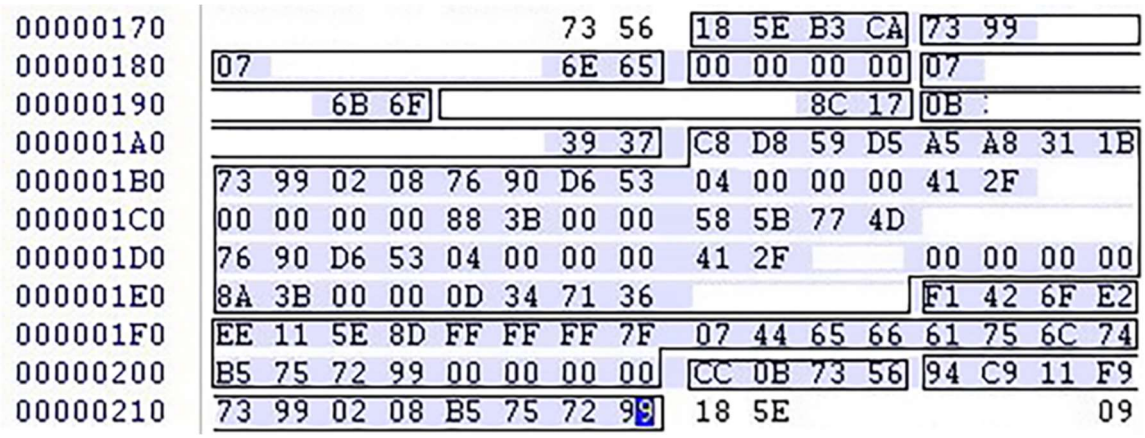


Figura 4.17. Ejemplo de la estructura del tipo "userContact" ubicada en el interior del fichero "users.dat".

La tabla 4.12 identifica los campos almacenados en el fichero "users.dat" de la figura 4.17, e interpreta de los valores relativos al tipo de contacto "userContact" del objeto "User", así como indica el significado de su contenido. Cierta información mostrada en la tabla 4.12 ha sido ocultada para garantizar la privacidad del usuario.

Tabla 4.12. Interpretación de la estructura de datos "userContact".

#	Campo	Tamaño (bytes)	Tipo dato	Valor del campo (Hexadecimal)	Significado del campo
1	User type	4	int	0x185EB3CA	Tipo de usuario. Usuario contacto.(Tipo userContact).
2	User_id	4	int	0x7399????	Valor: "13??????3".
3	FirstName	Variable	string	0x07; 0x??????????6E65	Long: 7; Valor: "?????ne".
4	LastName	Variable	String	0x00000000	Valor: Vacio.
5	UserName	Variable	String	0x07; 0x??????????6B6F	Long:7; Valor: "?????ko".
6	AccessHash	8	long	0x????????????8C17	Valor: "169??????????????33".
7	Phone	Variable	string	0x0B; 0x????????????????????3937	Long:11; Valor:"'??????????97".
8	Photo.userProfilePhoto	4	int	0xC8D859D5	Tipo userProfilePhoto .
9	Photo.photo_id	8	long	0xA5A8311B73990208	Valor: "577192421913372837".
10	Photo.fileLocation	4	int	0x7690D653	Ubicacion del fichero minuatura. Tipo fileLocation. Objeto FileLocation.
11	Photo.Location.dc_id	4	int	0x04000000	Valor: "4".
12	Photo.fileLocation.volume_id	8	long	0x412F????00000000	Valor: "42??????5".
13	Photo.fileLocation.local_id	4	int	0x883B0000	Valor: "15240".
14	Photo.fileLocation.secret	8	long	0x585B774D????????	Valor "-62??????????????088".
15	Photo.fileLocation	4	int	0x7690D653	Ubicacion del fichero normal. Tipo fileLocation. Objeto FileLocation.
16	Photo.fileLocation.dc_id	4	int	0x04000000	Valor: "4".
17	Photo.fileLocation.volume_id	8	long	0x412F????00000000	Valor "42??????5".
18	Photo.fileLocation.local_id	4	int	0x8A3B0000	Valor: "15242".
19	Photo.fileLocation.secret	8	long	0x0D347136????????	Valor: "-92??????????????635".
20	Status	4	int	0xF1426FE2	Valor: *UserStatusRecently*.
21	NotifySettings	4	int	0xEE115E8D	Ajuste de notificacion. Tipo PeerNotifySettings.
22	NotifySettings.MuteUntil	4	int	0xFFFFFF7F	Valor: "Tue, 19 Jan 2038 03:14:07 GMT".
23	NotifySettings.Sound	variable	string	0x07; 0x44656661756C74	Long:7; Valor: "default".
24	NotifySettings.ShowPreviews	4	int	0xB5757299	Valor: *boolTrue*.
25	NotifySettings.EventsMask	4	int	0x00000000	Valor: "0".
26	ExtendedInfo	4	int	0xCC0B7356	Valor: *Null*.
27	Contact.Contact	4	int	0x94C911F9	Tipo Contacto.
28	Contact.id_user	4	int	0x7399????	Valor: "13??????3".
29	Contact.mutual	4	int	0xB5757299	Valor: *boolTrue*.

4.4.2.1.2.2 Análisis de la información de mensajes

Al igual que sucede con la información relativa a los diferentes tipos de contactos, los datos relacionados con de mensajes intercambiados a través del cliente móvil de la aplicación de mensajería instantánea Telegram Messenger en WP se almacenan en ficheros de datos, si bien, en este caso, para conocer la información de los mensajes intercambiados se deben analizar los ficheros de datos "chats.dat", "encryptedChats.dat" y "dialogs.dat".

4.4.2.1.2.2.1 Análisis de mensajes normales

El fichero "chats.dat" contiene los registros de los diferentes tipos de chats ("usuario a usuario", "grupo", "supergrupo" y "canal"). La información que almacena el fichero "chats.dat" corresponde a la información relativa a los chats (identificador de conversación, número e identificador único de participante en una conversación, fecha de creación, título de la conversación, foto de grupo de la conversación, etc.). Esta información no se debe confundir con los mensajes intercambiados, si bien, la información ubicada en el interior del fichero "chats.dat" es necesaria para estructurar y ordenar los mensajes. La información de los diferentes tipos de conversaciones o chats se organiza en las estructuras de datos.

La tabla 4.13 muestra los diferentes tipos de conversaciones o chats que se incluyen en el objeto "Chat".

Tabla 4.13. Tipos de conversaciones del objeto "Chat".

#	Objeto	Tipo	Nombre	Descripción
1	Chat	Empty	chatEmpty	Conversación vacía.
2	Chat	Chat	chat	Conversación de grupo.
3	Chat	Forbidden	chatForbidden	Conversación de grupo que no puede ser accedido por el usuario.

A continuación, la figura 4.18 muestra a modo de ejemplo una simulación de las diferentes estructuras de datos que pueden ser almacenadas en el fichero de datos "chats.dat". Tal y como se observa en esta figura, las estructuras de datos "chatEmpty",

"chat" y "chatForbidden" disponen de un número diferentes de campos en función del tipo de chat que se trate.

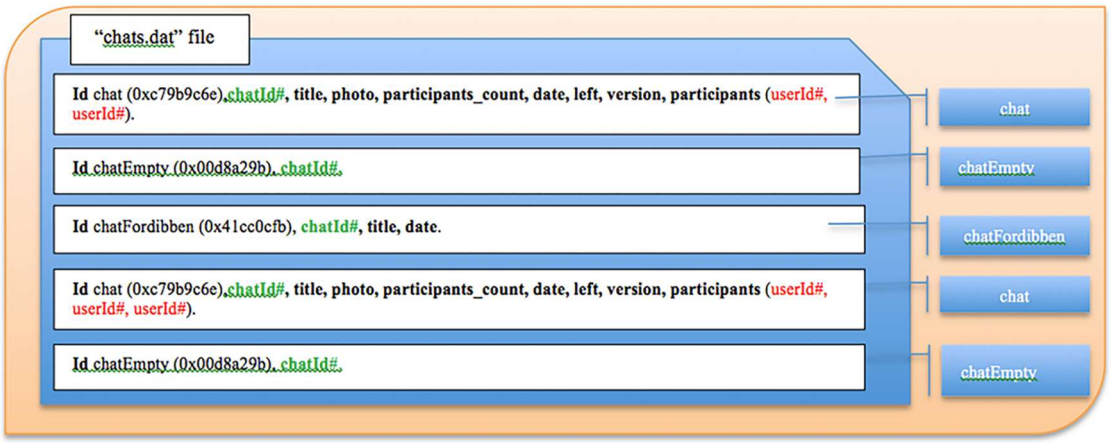


Figura 4.18. Ejemplo de las estructuras de conversaciones. Fichero "Chats.dat".

La figura 4.19 muestra a modo de ejemplo, parte del contenido del fichero de datos "chats.dat", en el cual se identifican los diferentes campos de la estructura de datos del tipo "chat" del objeto "Chat". Cierta información mostrada en la figura 4.19 ha sido ocultada para garantizar la privacidad del usuario.

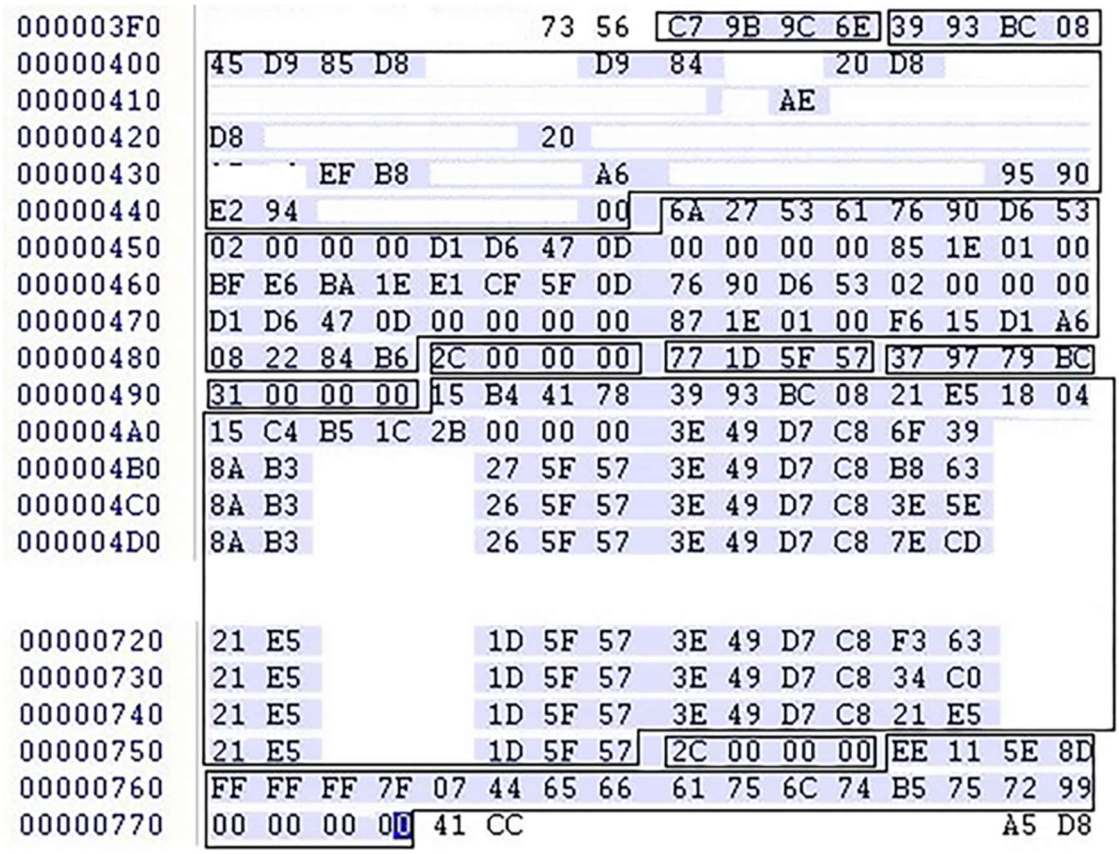


Figura 4.19. Ejemplo de la estructura de campos de tipo “chat” ubicada en el interior del fichero “chats.dat”.

La tabla 4.14 identifica los campos almacenados en fichero “chats.dat” de la figura 4.19, e interpreta de los valores del tipo de conversación “chat” del objeto “Chat”, así como indica el significado de su contenido. Cierta información mostrada en la tabla 4.14 ha sido ocultada para garantizar la privacidad del usuario.

Tabla 4.14. Interpretación de la estructura de datos “chat”.

#	Campo	Tamaño (bytes)	Tipo dato	Formato Hexadecimal	Formato legible
1	chat type	4	int	0xC79B9C6E	Tipo chat. Objeto Chat .
2	Id	4	int	0x3993BC08	Valor: “146576185”.
3	Title	variable	string	0x45; from 0xD985D8 to 0x??????00	Long: 69; Valor: “??????????”.
4	Photo.Id	4	int	0x6A275361	Datos de la foto del grupo. Tipo Photo.
5	Photo.fileLocation	4	int	0x7690D653	Ubicacion de la foto miniatura del grupo. Tipo fileLocation. Objeto FileLocation.
6	Photo.fileLocation.dc_id	4	int	0x02000000	Valor: “2”.
7	Photo.fileLocation.volume_id	8	long	0xD1D6470D00000000	Valor: “222811857”.

8	Photo.fileLocation.local_id	4	int	0x851E0100	Valor: “73349”.
9	Photo.fileLocation.secret	8	long	0xBFE6BA1EE1CF5F0D	Valor: “963717411070731967”.
10	Photo.fileLocation	4	int	0x7690D653	Tipo fileLocation. Ubicacion del foto normal del grupo.
11	Photo.fileLocation.dc_id	4	int	0x02000000	Valor: “2”.
12	Photo.fileLocation.volume_id	8	long	0xD1D6470D00000000	Valor: “222811857”.
13	Photo.fileLocation.local_id	4	int	0x871E0100	Valor: “73351”.
14	Photo.fileLocation.secret	8	long	0xF615D1A6082284B6	Valor: “-5295069841327057418”.
15	ParticipantsCount	4	int	0x2C000000	Valor: “44”.
16	Date	4	int	0x771D5F57	Valor: “Mon, 13 Jun 2016 20:54:15 GMT”.
17	Left	4	int	0x379779BC	Valor: “*Booltrue”*. Verdadero.
18	Version	4	int	0x31000000	Valor: “49”.
19	chatParticipants.	4	int	0x15B44178	Tipo chatParticipants. Datos del participante número 1 de la conversación.
20	chatParticipants.chat_id	4	int	0x3993BC08	Valor: “146576185”.
21	chatParticipants.admin_id	4	int	0x21E51804	Valor: “68740385”.
22	Participants	4	int	0x15C4B51C	Tipo Vector. Lista de objetos.
23	Participants.count	4	int	0x2B000000	Valor: “43”.
24	Participants[1]	4	int	0x3E49D7C8	Tipo chatParticipant. Datos del participante numero 2 de la conversación.
25	Participants[1].user_id	4	int	0x6F39????	Valor: “14?????67”.
26	Participants[1].inviter_id	4	int	0x8AB3????	Valor: “18?????42”.
27	Participants[1].date	4	int	0x16275F57	Valor: “Mon, 13 Jun 2016 21:35:18 GMT”.
28	Participants[2]	4	int	0x3E49D7C8	Datos del participante numero 3 de la conversación. Tipo chatParticipant.
29	Participants[2].user_id	4	int	0xB863????	Valor: “11?????52”.
30	Participants[2].inviter_id	4	int	0x8AB3????	Valor: “18?????42”.
31	Participants[2].date	4	int	0xF8265F57	Valor: “Mon, 13 Jun 2016 21:34:48 GMT”.
32	ParticipantsCount	4	int	0x2C000000	Valor: “44”.
33	NotifySettings.NotifySettings	4	int	0xEE115E8D	Tipo PeerNotifySettings. Notificaciones de la conversación.
34	NotifySettings.MuteUntil	4	int	0xFFFFFF7F	Valor: “Tue, 19 Jan 2038 03:14:07 GMT”.
35	NotifySettings.Sound	variable	string	0x07; 0x44656661756C74	Long:7; Valor:”default”.
36	NotifySettings.ShowPreviews	4	int	0xB5757299	Valor: “*boolTrue”*. Verdadero.
37	NotifySettings.EventsMask	4	int	0x00000000	Valor: “0”.

Una vez conocida la información relativa a las conversaciones o chats, como el título el chat, la fecha de creación, la foto de perfil del chat, el número de participantes, el identificador de cada participante, etc., se pueden obtener los diferentes mensajes intercambiados en el mismo.

A través del análisis del fichero “dialogs.dat” se obtienen los diferentes mensajes intercambiados en cada chat. Dependiendo del contenido, los mensajes se organizan bajo

el objeto "Message" cuando son mensajes de texto y bajo el objeto "MessageMedia" cuando son mensajes con adjunto.

La tabla 4.15 muestra los diferentes tipos de mensajes de texto del objeto "Message" y los diferentes tipos mensajes con contenido multimedia del objeto "MessageMedia", así como su significado.

Tabla 4.15. Tipos de mensaje de los objetos "Message" y "MessageMedia".

#	Objeto	Tipo	Nombre	Descripción
1	Message	Empty	messageEmpty	Mensaje vacio.
2	Message	Message	message	Mensaje de texto.
3	Message	Service	messageService	Mensaje de servicio.
4	Message	Forbidden	messageForbidden	Mensaje reenviado.
5	MessageMedia	Empty	messageMediaEmpty	Mensaje adjunto vacio.
6	MessageMedia	Photo	messageMediaPhoto	Mensaje adjunto tipo foto.
7	MessageMedia	Video	messageMediaVideo	Mensaje adjunto tipo video.
8	MessageMedia	Geo	messageMediaGeo	Mensaje adjunto posicionamiento.
9	MessageMedia	Contact	messageMediaContact	Mensaje adjunto tipo contacto.
10	MessageMedia	Message Document	messageMediaDocument	Mensaje adjunto tipo documento.
11	MessageMedia	Message Audio	messageMediaAudio	Mensaje adjunto tipo audio.

A continuación, la figura 4.20 muestra a modo de ejemplo una simulación de las diferentes estructuras de datos que pueden ser almacenadas en el fichero de datos "dialogs.dat". Tal y como se observa en esta figura, las estructuras de datos "message", "messageService", "messageMediaPhoto y "messageMediaDocument" disponen de un número diferentes de campos en función del tipo de mensaje que se trate.

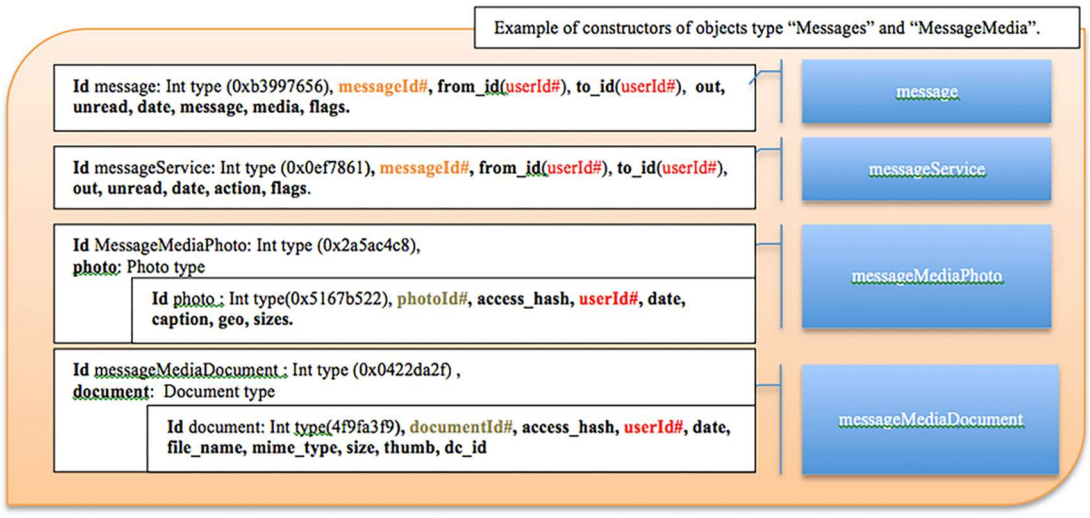


Figura 4.20. Ejemplo de tipos de mensaje contenidos en el fichero "dialogs.dat".

La figura 4.21 muestra a modo de ejemplo, parte del contenido del fichero de datos "dialogs.dat", en el cual se identifican los diferentes campos de la estructura de datos del tipo "message" del objeto "Message". Cierta información mostrada en la figura 4.21 ha sido ocultada para garantizar la privacidad del usuario.

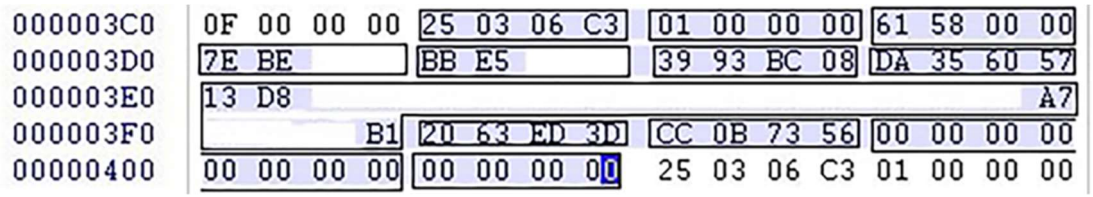


Figura 4.21. Ejemplo de la estructura de campos del tipo de objeto "message" ubicada en el interior del fichero "dialogs.dat".

La tabla 4.16 identifica los campos almacenados en fichero "dialogs.dat" de la figura 4.21, e interpreta de los valores del tipo "message" del objeto "Message", así como indica el significado de su contenido. Cierta información mostrada en la tabla 4.16 ha sido ocultada para garantizar la privacidad del usuario.

Tabla 4.16. Valores del tipo "message" (objeto "Message") en formato legible para el ser humano.

#	Campo	Tamaño (bytes)	Tipo dato	Valor del campo (Hexadecimal)	Significado del campo
1	message type	4	int	0x250306C3	Tipo de mensaje. "message".
2	flags	4	int	0x01000000	Valor: "1".
3	id	4	int	0x61580000	Identificar del mensaje. Valor: "22625".
4	from_id	4	int	0x7EBE????	Identificador unico de usuario. Envia mensaje. Valor: "19?????98".
5	to_id	4	int	0xBBE5????	Identificador unico de usuario. Recibe mensaje. Valor: "31???????75".
6	reply	4	int	0x3993BC08	Valor "146576185". Identificador de chat.
7	date	4	int	0xDA356057	Fecha se recepcion del mensaje. Valor: "Tue, 14 Jun 2016 16:50:34 GMT".
8	message	variable	string	0x13; 0xD8??????????????????? ???????A??????B1	Long:19; Valor: "?????????????".
9	media	8	long	0x2063ED3D	Valor: "*MessageMediaEmpty*".
10	customFlags	4	int	0xCC0B7356	Valor: "*Null*".
11	randomId	8	long	0x0000000000000000	Valor: "0".
12	status	4	int	0x00000000	Valor: "0".

4.4.2.1.2.2.2 Análisis de mensajes secretos

El fichero "encryptedChats.dat" contiene los registros relativos a las conversaciones secretas (*user-to-user*). Al igual que sucede con la información que almacena el fichero "chats.dat", los datos ubicados en el interior del fichero "encryptedChats.dat" corresponden a la información relativa a las conversaciones secretas (identificador único, número de participantes, fecha de creación, título del chat, foto del chat, etc.). La información contenida en este archivo no se debe confundir con los registros relativos a los mensajes secretos intercambiados, si bien, la información ubicada en el fichero "encryptedChats.dat" es necesaria para estructurar y ordenar los mensajes secretos. La información de los diferentes tipos de conversaciones secretas se organiza en las estructuras de datos. La tabla 4.17 muestra los diferentes tipos de conversaciones o chats secretos que se incluyen en el objeto "EncryptedChat".

Tabla 4.17. Tipos de conversaciones cifradas del objeto "EncryptedChat".

#	Objeto	Tipo	Nombre	Descripcion
1	EncryptedChat	Empty	encryptedChatEmpty	Chat secreto vacío.
2	EncryptedChat	Waiting	encryptedChatWaiting	Chat secreto a la espera de ser aprobado por el Segundo participante.
3	EncryptedChat	Requested	encryptedChatRequested	Chat secreto aceptado para su creación.
3	EncryptedChat	Chat secret	encryptedChat	Chat secreto.
4	EncryptedChat	Discarded	encryptedChatDiscarded	Chat secreto descartado. Chat eliminado.

A continuación, la figura 4.22 muestra a modo de ejemplo una simulación de las diferentes estructuras de datos que pueden ser almacenadas en el fichero de datos "encryptedChats.dat". Tal y como se observa en esta figura, las estructuras de datos "encryptedChat", "encryptedChatRequested" "encryptedChatEmpty", "encryptedChatDiscarded" y "encryptedChatWaiting" disponen de un número diferentes de campos en función del tipo de chat que se trate.

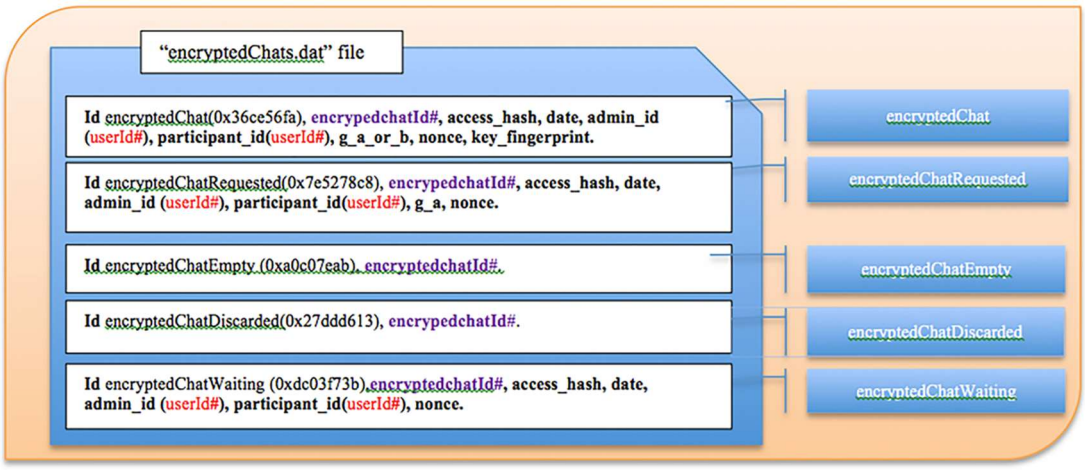


Figura 4.22. Ejemplo de las estructuras de conversaciones secretas. Fichero "encryptedChats.dat".

Una vez obtenida la información relativa a las conversaciones secretas, (fecha de creación, identificador participante, identificador del administrador de la conversación, etc.) del fichero "encryptedChats.dat" se pueden buscar en el fichero "dialogs.dat" los diferentes mensajes secretos intercambiados.

A través del análisis del fichero "dialogs.dat" se obtienen los diferentes mensajes intercambiados en cada chat secreto. Dependiendo del contenido, los mensajes secretos se organizan bajo el objeto "DecryptedMessage" cuando son mensajes de texto y bajo el objeto "DecryptedMessageMedia" cuando son mensajes con adjunto. La tabla 4.18 muestra los diferentes tipos de mensajes secretos de texto del objeto "DecryptedMessage" y los diferentes tipos mensajes secretos con contenido multimedia del objeto "DecryptedMessageMedia", así como su significado.

Tabla 4.18. Tipos de mensajes secretos de los objetos "DecryptedMessage" y "DecryptedMessageMedia".

#	Tipo	Objeto	Nombre	Descripción
1	DM	DM	decryptedMessage	Mensaje secreto.
2	DM Service	DM	decryptedMessageService	Mensaje secreto de servicio.
3	DMM Empty	DMM	decryptedMessageMediaEmpty	Mensaje secreto vacío.
4	DMM Photo	DMM	decryptedMessageMediaPhoto	Mensaje secreto con adjunto tipo foto.
5	DMM Video	DMM	decryptedMessageMediaVideo	Mensaje secreto con adjunto tipo video.
6	DMM GeoPoint	DMM	decryptedMessageMediaGeoPoint	Mensaje secreto con adjunto tipo geo-posición.
7	DMM Contact	DMM	decryptedMessageMediaContact	Mensaje secreto con adjunto tipo contacto.
8	DMM Document	DMM	decryptedMessageMediaDocument	Mensaje secreto con adjunto tipo documento.
9	DMM Audio	DMM	decryptedMessageMediaAudio	Mensaje secreto con adjunto tipo audio.

*DM = DecryptedMessage, DMM= DecryptedMessageMedia

A continuación, la figura 4.23 muestra a modo de ejemplo una simulación de las diferentes estructuras de datos que pueden ser almacenadas en el fichero de datos "dialogs.dat". Tal y como se observa en esta figura, las estructuras de datos "decryptedMessage", "decryptedMessageService", "decryptedmessageMediaPhoto" "decryptedmessageMediaDocument" y "decryptedmessageMediaAudio" disponen de un número diferentes de campos en función del tipo de mensaje secreto que se trate.

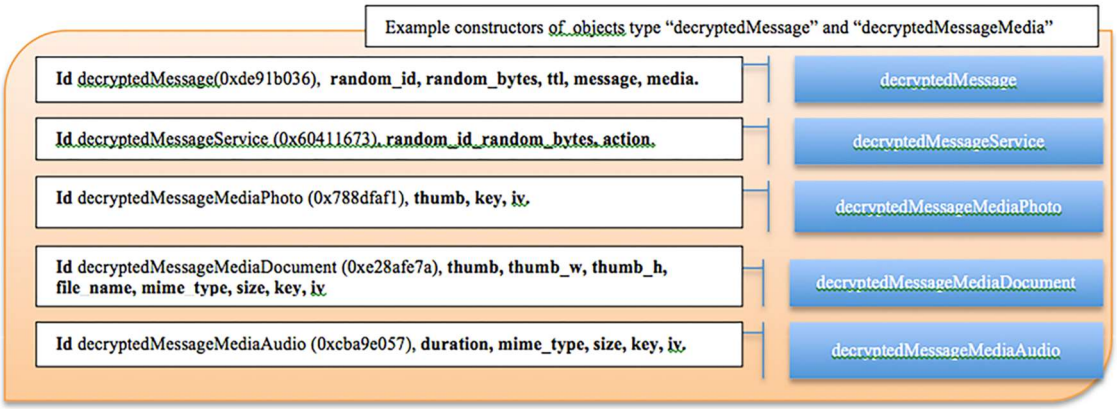


Figura 4.23. Ejemplo estructura de datos de los objetos "decryptedMessages" y "decryptedMessageMedia".

Debido a que la identificación y decodificación de la información contenida en estas estructuras y relativa a los mensajes secretos ubicados en el fichero "dialogs.dat" se realiza de igual manera que la expuesta en el punto de mensajes normales, es por lo que la misma se da por descrita.

4.4.3 Estudio de código fuente

El estudio de código fuente ha sido desarrollado a partir de los procedimientos descritos en el punto 3.3.3 de esta Tesis. Estos procedimientos permitirán identificar, decodificar, interpretar y validar los registros generados por el cliente móvil de la aplicación de mensajería instantánea Telegram Messenger en el sistema operativo Windows Phone a partir del análisis de código fuente.

En el caso del cliente móvil de la aplicación Telegram Messenger para el sistema operativo móvil Windows Phone, el propio desarrollador de la aplicación proporciona el código fuente [32]. Al realizar el estudio de código fuente de la aplicación, se observa que el mismo se encuentra escrito en lenguaje "C#", siendo este un lenguaje orientado a objetos. El código fuente de este cliente móvil, contiene alrededor de 321 ficheros con extensión ".cs", encontrándose que solamente el fichero con el nombre "TLMessage.cs" contiene un total de 2250 líneas de código. Este estudio se realizará de aquellas partes del código que en primera instancia aporten información sobre los datos de interés para el análisis forense.

Entre los diferentes ficheros del código fuente se encuentra el archivo con nombre "TLUserBase.cs" ubicado en la carpeta "telegram_wp.src\Telegram WP\Telegram WP\HexRequest\HexRequest\TL\". Este archivo contiene entre otras cosas, las funciones de lectura y escritura de datos de contactos. Analizando estas líneas de código se pueden identificar las estructuras de datos que son extraídas o guardadas en el fichero "users.dat". La figura 4.24 muestra parte la función "ToStream" ubicada en el fichero de código fuente "TLUserBase.cs". En esta figura se observar los diferentes campos ("FirstName", "LastName", "UserName", "Phone", "Photo", etc.) que son guardados en el fichero de datos "users.dat".

[32] Telegram Messenger. (2016). *Telegram Applications*. Recuperado el 4 de octubre 2016, de: https://telegram.org/apps.

```
public override void ToStream(Stream output)
{
    output.Write(TLUtils.SignatureToBytes(Signature));
    output.Write(Id.ToBytes());
    output.Write(FirstName.ToBytes());
    output.Write(LastName.ToBytes());
    output.Write(UserName.ToBytes());
    output.Write(Phone.ToBytes());
    Photo.ToStream(output);
    Status.ToStream(output);
    output.Write(Inactive.ToBytes());

    NotifySettings.NullableToStream(output);
    ExtendedInfo.NullableToStream(output);
    Contact.NullableToStream(output);
}
```

Figura 4.24. Líneas de código de la función “ToStream”. Fichero “TLUserBase.cs”.

Otro de los ficheros incluidos en el código fuente del cliente móvil e la aplicación de IM Telegram Messenger para WP, es el archivo con nombre “TLMessage.cs” el cual se ubicada en la carpeta “telegram_wp.src\Telegram WP\Telegram WP\HexRequest\HexRequest\TL\”. Este archivo contiene entre otras, las funciones de lectura y escritura de la información relativa a los mensajes intercambiados. Analizando estas líneas de código se pueden identificar las estructuras de datos que son extraídas o guardadas en el fichero “dialogs.dat”. La figura 4.25 muestra parte de la función “ToStream” contenida en el archivo “TLMessage.cs”, en el cual se realiza la escritura de los datos relativos a un mensaje (“flags”, “date”, “from_id”, “to_id”, “message”, etc.) el fichero de datos “dialogs.dat”.

```
public override void ToStream(Stream output)
{
    output.Write(TLUtils.SignatureToBytes(Signature));

    Flags.ToStream(output);
    Id = Id ?? new TLInt(0);
    output.Write(Id.ToBytes());
    output.Write(FromId.ToBytes());
    ToId.ToStream(output);

    if (IsSet(Flags, (int)MessageFlags.Fwd))
    {
        FwdFromId.ToStream(output);
        FwdDate.ToStream(output);
    }

    if (IsSet(Flags, (int)MessageFlags.Reply))
    {
        ReplyToMsgId.ToStream(output);
    }

    output.Write(Date.ToBytes());
    Message.ToStream(output);
    _media.ToStream(output);

    if (IsSet(Flags, (int)MessageFlags.ReplyMarkup))
    {
        ReplyMarkup.ToStream(output);
    }
    if (IsSet(Flags, (int)MessageFlags.Entities))
    {
        Entities.ToStream(output);
    }

    CustomFlags.NullableToStream(output);

    RandomId = RandomId ?? new TLLong(0);
    RandomId.ToStream(output);
    var status = new TLInt((int)Status);
    output.Write(status.ToBytes());
}
```

Figura 4.25. Líneas de código de la función “ToStream”. Fichero “TLMessage.cs”.

El estudio de las diferentes líneas de código fuente del cliente móvil de la aplicación de IM Telegram Messenger para WP ha sido utilizado para identificar las estructuras de datos contenidas en los archivos que almacenan la información del usuario. Así mismo, a través de este estudio se han podido identificar las diferentes transformaciones realizadas por este cliente sobre los datos de usuario necesarias para poder interpretar y presentar en un formato legible por el ser humano las comunicaciones mantenidas a través de esta aplicación.

4.4.4 Resultados del análisis realizado

La metodología de análisis forense propuesta en la presente tesis y utilizada en el desarrollo del estudio técnico-forenses del cliente móvil de la aplicación de mensajería instantánea Telegram Messenger para el sistema operativo móvil Windows Phone desprende que:

a) Del estudio de las fuentes abiertas, correspondiente con la búsqueda de toda aquella información funcional, técnica y forense que pudiera encontrarse en cualquier fuente de datos abiertas o semiabiertas en el momento del estudio, se obtiene como única fuente de datos la proporcionada por el desarrollador de la aplicación. Este expone en su página web la lista de objetos ("Message", "Chat", etc.) y de tipos[33] ("Message.messageEmpty", "Message.message", "Message.messageService", "Chat.chat", "Chat.chatFordibben" etc.) que almacenan la información del cliente móvil de la aplicación de mensajería instantánea Telegram Messenger para WP.

b) Del estudio de los artefactos, correspondiente al análisis forense estático de los rastros generados por el cliente móvil de la aplicación de mensajería instantánea Telegram Messenger, se obtienen los registros que generan tanto la aplicación como las comunicaciones de usuario en el teléfono inteligente con sistema operativo Windows Phone.

   Estudiados los diferentes rastros generados a partir del análisis comparativo se identifica que la información de configuración del cliente móvil de la aplicación Telegram Messenger en Windows Phone se almacena en ficheros con formato etiqueta ("XML"), siendo el contenido fácilmente decodificable e interpretable. Igualmente, a partir del análisis comparativo se identifica que, la información relativa a las comunicaciones de usuario la cual se encuentra almacenada en cuatro archivos de datos ("users.dat", "chats.dat", "chatEncrypted.dat" y "dialogs.dat").

[33] Por ejemplo, un objeto Message tiene diferentes tipos dependiendo de la informacion que almacena. El tipo message del objeto Message guarda mensaje de texto. El tipo messageService del objeto Message guarda mensajes enviados por la aplicacion Telegram (notific aciones, actualizaciones, etc.).

Estos cuatro ficheros de datos contienen, entre otras cosas, la información relativa a los contactos, conversaciones normales y secretas, así como mensajes normales y secretos. Tal y como ha quedado demostrado esta base de datos almacena información legible (metadatos de las comunicaciones) e información ilegible (contenido de las comunicaciones). Para interpretar esta última, se debe utilizar la información obtenida tanto del estudio de fuentes abiertas como del estudio del código fuente, la cual ayudará a decodificar la información almacenada en las estructuras de datos para su correcta visualización.

c) Por último, realizado el estudio del código fuente, correspondiente al análisis de las líneas de código del lenguaje de programación C# en el cual se encuentra desarrollado el cliente móvil de la aplicación Telegram Messenger para WP, se obtiene todos aquellos datos necesarios para identificar, decodificar, interpretar y validar la información obtenida del estudio de fuentes abiertas y del estudio estático de artefactos.

   De esta manera, a través de este estudio se analizan las diferentes funciones del código fuente de la aplicación identificando y validando las estructuras de datos almacenados en los ficheros de configuración de la propia aplicación, así como en los ficheros de datos (“users.dat”, “chats.dat”, “chatEncrypted.dat” y “dialogs.dat”). Así mismo se analiza y coteja que tanto los objetos como las estructuras de datos dinámicas proporcionadas en la página web del desarrollador corresponden con los que se almacenan en los campos de la base de datos.

Tal y como ha quedado demostrado, la metodología de análisis forense propuesta permite identificar, decodificar, interpretar y validar la información generada por el cliente móvil de la aplicación de mensajería instantánea Telegram Messenger en el sistema operativo Windows Phone.

4.5 Comparativa de los resultados obtenidos. Telegram Messenger en Android y Windows Phone

A continuación, se muestra los resultados obtenidos de los estudios técnico-forenses del cliente móvil de la aplicación de mensajería instantánea Telegram Messenger para los sistemas operativos móvil Android y Windows Phone. Estos serán expuestos comparando el resultado obtenido de los diferentes métodos definidos en la metodología de análisis propuesta.

Estudio de fuentes abiertas.

Del estudio de fuentes abiertas correspondiente al análisis de toda fuente de datos que pudiera contener cualquier tipo información funcional, técnica o forense, y que pudiera ser utilizada para apoyar el análisis forense de los clientes móviles de la aplicación de IM Telegram Messenger para los sistemas operativos Android y WP, se concluye que, la principal fuente de datos para este estudio es la proporcionada por el propio desarrollador de la aplicación. Este expone, a través de su página web, como la información de la aplicación de IM Telegram Messenger se organiza a partir de una serie objetos que se subdividen a su vez en tipos incluyendo cada tipo una estructura de datos con diferentes campos definidos (TL Language[34]). En este sentido, el objeto "User" u objeto que guarda la información sobre los usuarios, tiene entre otros, el tipo "userContact" con la información de usuario de tipo contacto y el tipo "userDelete" con la información de un usuario eliminado. El objeto "Chat" u objeto que almacena la información sobre las conversaciones, tiene entre otros, el tipo "chat" con las propiedades de un chat y el tipo "chatEmpty" con las propiedades de un chat vacío.

Así mismo existen tipos, en cuyas estructuras de datos se incluyen otras estructuras a su vez, formando estructuras de datos anidadas. Es el caso del tipo "userProfilePhoto" (incluido en el objeto "UserProfilePhoto") el cual almacena la estructura con los datos correspondientes con la foto de perfil de un usuario. En la estructura de datos del tipo "userProfilePhoto" se incluye, además de otros campos, el campo que contiene el nombre

[34] Telegram Messenger. *TL Language*. Recuperado el 6 de agosto de 2016, de: https://core.telegram.org/mtproto/TL.

del fichero de imagen. Ese campo almacena esa información bajo la estructura de datos del tipo “fileLocation” (objeto “FileLocation”).

La figura 4.26 muestra a modo de ejemplo los cuatro campos que componen la estructura de datos del tipo “userProfilePhoto” (Objeto “UserProfilePhoto”). El primer campo “Id” (tipo “Int”) es el identificador único del tipo “userProfilePhoto” y corresponde con el valor 0xC8D859D5, el segundo campo “photo_id” (tipo “Long”) es el identificador único de la foto, los dos últimos campos “photo_small” y “photo_big” (tipo “fileLocation” del objeto “FileLocation”) identifican la ubicación del fichero de imagen de perfil en formato miniatura y normal. Los dos campos “photo_small” y “photo_big” contienen los campos “Id” (0x7690D653), “dc_id”, “volumen_id”, “local_id” y “secret” correspondientes con la estructura de datos del tipo “fileLocation” (objeto “FileLocation”).

Figura 4.26. Ejemplo estructura de “userPofilePhoto”

La figura 4.27 muestra a modo de ejemplo como se almacenaría la estructura de datos “userProfilePhoto” en el interior del fichero de datos “users.dat” (Windows Phone), de igual manera que se almacenaría en el campo “data” de la tabla “users” de la base de datos “cache4.db” (Android). En esta figura se puede identificar el inicio de la estructura de datos de tipo “userProfilePhoto” (0xC8D859D5). Seguidamente se localiza “photo_id” (0xAAA7311B6BB2????) para posteriormente identificarse la estructura de datos de tipo “fileLocation” (0x7690D653) repetida en dos ocasiones correspondiente con los campos “photo_small” y “photo_big” de la estructura de datos de tipo “userProfilePhoto”. Cierta información mostrada en la figura 4.27 ha sido ocultada para garantizar la privacidad del usuario.

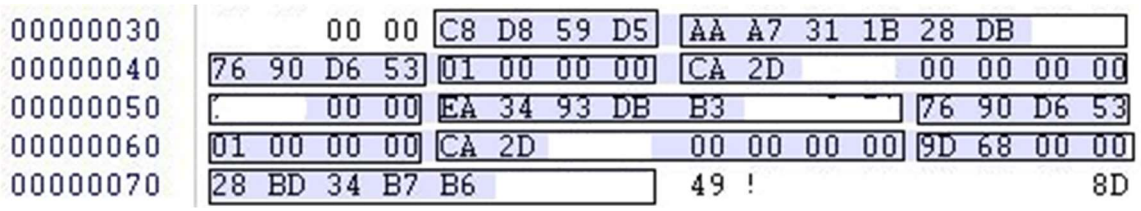


Figura 4.27. Ejemplo de la estructura de campos del tipo de objeto "userProfilePhoto" (objeto "UserProfilePhoto").

Estudio de artefactos.

Del estudio estático de los artefactos se obtiene como resultado los diferentes registros que generan los clientes móviles la aplicación de IM Telegram Messenger tanto en el sistema operativo móvil Android como Windows Phone.

Del análisis comparativo de los artefactos de los clientes móviles estudiados se obtienen los registros que se generan, modifican y eliminan en el teléfono inteligente, identificando aquellos ficheros y directorios utilizados por los clientes móviles para almacenar los datos tanto de la aplicación como del usuario. La tabla 4.19 expone de manera comparativa el listado de artefactos los clientes móviles de la aplicación de mensajería instantánea Telegram Messenger para los sistemas operativos móviles Android y Windows Phone.

Tabla 4.19. Lista de artefactos aplicación Telegram Messenger en Android y WP.

#	Contenido	Artefactos Android	Artefactos WP	Descripción
1	Configuración de aplicación	userconfig.xml, logininfo.xml, mainconfig.xml.	ApplicactionSettings, CommonNotifySettings.xml.	Archivos temporales de configuración de la aplicación.
2	Ficheros de Log	-	{YYYY}-{MM}-{DD}".txt".	Archivos de eventos de la aplicación.
3	Datos de usuario	cache4.db, tgnet.dat.	users.dat, chats.dat, encryptedChats.dat, dialogs.dat.	Diferentes carpetas y archivos de datos de usuario.
4	Datos de temporales	com.android.opengl.shders_cache	temp_dialogs.dat, temp_users.dat, temp_chats.dat, temp_encryptedChats.dat.	Diferentes archivos temporales.
5	Ficheros multimedia	/mnt/sdcard/Telegram/*	/Data/Root/Users/DefApps/*	Diferentes carpetas (videos, audios, documentos, imágenes, etc.).
6	Ficheros de cache	/data/data/org.telegram.messenger/cache/*	-	Diferentes ficheros (".jpg", ".mp4", etc.).
7	Otros ficheros	com.google.android.gsm.appid-no-backup	allStickers.dat, broadcasts.dat, cachedServerFiles.dat, importedPhones.dat.	Otros ficheros.

Una vez identificados los ficheros y directorios utilizados por los clientes móviles de la aplicación de IM Telegrama Messenger para los sistemas operativos Android y WP, se debe realizar el análisis del contenido de la información almacenada en estos ficheros.

Con respecto a los datos de la aplicación, el estudio estático de artefactos es utilizado identificar e interpretar los datos contenidos en el interior de los ficheros propios de la aplicación, así como el significado de esos datos. Estos ficheros almacenan su contenido en un formato legible, siendo la información relativa tanto a las preferencias como a la configuración de la aplicación interpretada de forma sencilla. Los dos clientes móviles de la aplicación de IM Telegram Messenger almacenan la información de la aplicación en archivos de tipo XML (fila 1, tabla 4.19).

Con respecto a los datos de usuario, el estudio estático de artefactos es utilizado para identificar, decodificar e interpretar la información relativa a las comunicaciones de usuario. Del estudio estático de artefactos se desprende que esta información se almacena de manera distinta en función del sistema operativo.

Para el sistema operativo móvil Android, el cliente móvil de aplicación de IM Telegram Messenger almacena los datos relativos a las comunicaciones de usuario en una base de datos con nombre “cache4.db” (fila 3, tabla 4.19). Al contrario de lo que sucede en Android, el sistema operativo WP almacena los datos de las comunicaciones de usuario en cuatro ficheros de datos con nombre “users.dat”, “chats.dat”, “chatEncrypted.dat” y “dialogs.dat” (fila 3, tabla 4.19).

Analizados los diferentes archivos relativos al sistema operativo Android, se identifica que en la base de datos “cache4.db” se almacena información legible correspondiente a los metadatos de las comunicaciones (identificador del mensaje, fecha/hora, estado, etc.) así como información ilegible correspondiente a la información de las comunicaciones de usuario. De igual manera, analizados los diferentes ficheros de datos relativos al sistema operativo WP se identifica que los ficheros “users.dat”, “chats.dat”, “chatEncrypted.dat” y “dialogs.dat” contienen información ilegible correspondiente tanto a los metadatos de las comunicaciones como a las propias comunicaciones mantenidas por el usuario.

Tanto para el sistema operativo Android como WP los datos ilegibles (formato binario) son analizados identificando en su interior diversas estructuras de datos. La decodificación de esta información es posible gracias a los datos obtenidos tanto del

estudio de fuentes abiertas como del estudio del código fuente, los cuales proporcionan los conocimientos necesarios para interpretar las diferentes estructuras de datos, realizando las transformaciones necesarias para visualización en formato humano.

A continuación, se muestran a modo comparativo como se almacenada la estructura de datos que alberga la información de un usuario de tipo contacto en función al sistema operativo del cliente móvil de la aplicación de IM Telegram Messenger. La figura 4.28 corresponde a un usuario de tipo contacto almacenado en el campo "data" de la tabla "users" del archivo "cache4.db" para Android. Cierta información mostrada en la figura 4.28 ha sido ocultada para garantizar la privacidad del usuario.

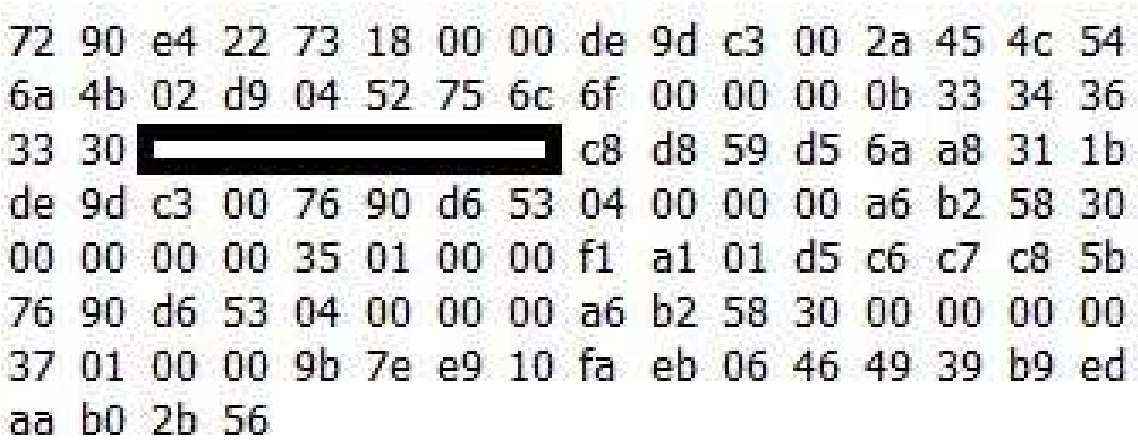


Figura 4.28. Ejemplo de la estructura de campos del tipo de objeto "userContact" del objeto "User" en el archivo "cache4.db".

Así mismo la figura 4.29 muestra la información de un usuario de tipo contacto extraída del archivo "users.dat". Cierta información mostrada en la figura 4.29 ha sido ocultada para garantizar la privacidad del usuario.

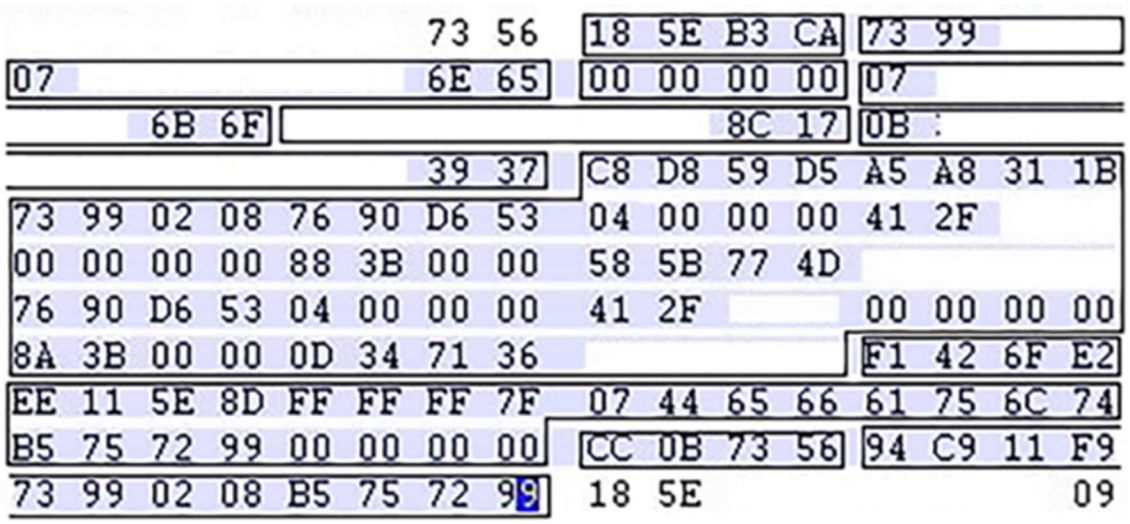


Figura 4.29. Ejemplo de la estructura de campos del tipo de objeto “userContact” del objeto “User” en el archivo "Users.dat".

La tabla 4.20 muestra la correspondencia de cada uno de los campos incluidos en las figuras 4.28 y 4.29 relativas a un usuario de tipo contacto (tipo “userContact” del objeto “User”). Cierta información mostrada en la tabla 4.20 ha sido ocultada para garantizar la privacidad del usuario.

Tabla 4.20. Interpretación de los datos del campo binario.

#	Nombre de campo	Tamaño (bytes)	Android (Hexadecimal)	WP (Hexadecimal)	Significado del campo
1	user	4	0x7290E422	0x185EB3CA	Tipo “userContact”. Contacto.
2	flags	4	0x73180000	NO EXISTE	Flags de campos.
3	Id	4	0xDE9DC300	0x7399????	Identificador único de contacto.
4	hash_access	8	0x2A454C546A4B02D9	En Android, fila 8.	Hash de acceso.
5	first_name	variable	0x04; 0x52756C6F	0x07; 0x??????????6E65	Nombre del contacto.
6	last_name	variable	0x00	0x00000000	Segundo nombre del contacto.
7	username	variable	0x0000	0x07; 0x??????????6B6F	Alias del contacto.
8	AccessHash	8	En WP, fila 4.	0x???????????8C17	Hash de acceso.
9	phone	variable	0x0B; 0x3334363330?????????	0x0B; 0x????????????????????3937	Número de teléfono del contacto.
10	Photo	4	0xC8D859D5 - 7B077D38.	0xC8D859D5 - 0x0D347136????????	Tipo “userProfilePhoto”. Foto de perfil de contacto.
11	Status	4	0x4939B9ED	0xF1426FE2	Estado del contacto.
12	NotifySettings	variable	NO EXISTE	0xEE115E8D - 0x00000000	Tipo “PeerNotifySettings”. Información sobre notificaciones.
13	ExtendedInfo	variable	NO EXISTE	0xCC0B7356	Informacion extendida.
14	Contact.mutual	variable	NO EXISTE	0x94C911F9 - 0xB5757299	Mas información sobre contacto.
15	Expiration date	4	0xAAB02B56	NO EXISTE	Fecha de última conexión.

Estudio de código fuente.

Del estudio del código fuente correspondiente al análisis de las líneas de código del lenguaje de programación "Java" y "C#", en el cual se encuentra desarrollado los clientes móviles de la aplicación de IM Telegrama Messenger para Android y WP respectivamente, se obtiene el conocimiento técnico y funcional de la aplicación.

El análisis del código fuente de los clientes móviles de la aplicación de IM Telegram Messenger para Android y WP, han sido realizado sobre todas aquellas clases, funciones, variables, etc., de las líneas de programación necesarias, tanto para apoyar y validar tanto la información obtenida en el estudio de fuentes abiertas y del estudio de artefactos, así como identificar, decodificar e interpretar cualquier otro tipo de información no obtenida de los estudios anteriores.

Del análisis del código fuente se identifica como la información relativa a un contacto en el cliente móvil en Android se almacena en una estructura dinámica de datos. Esta estructura dinámica depende de un campo "flags" ubicado en la propia estructura, el cual indica qué campo está activo o no para guardar información. Caso que no ocurre con el cliente móvil en WP, cuya información relativa a un contacto se almacena en una estructura de datos estática.

La figura 4.30 muestra la función "readParams" de la clase "TL_user_old" contenida en el fichero "TLRPC.java" del código fuente para Android. En esta función se puede observar el campo "flags" anteriormente descrito y como dependiendo de su valor incluye o no un campo a la estructura de datos de contacto.

```
public static class TL_user_old extends TL_user {
        public static int constructor = 0x22e49072;

        public void readParams(AbstractSerializedData stream, boolean exception) {
                flags = stream.readInt32(exception);
                self = (flags & 1024) != 0;
                contact = (flags & 2048) != 0;
                mutual_contact = (flags & 4096) != 0;
                deleted = (flags & 8192) != 0;
                bot = (flags & 16384) != 0;
                bot_chat_history = (flags & 32768) != 0;
                bot_nochats = (flags & 65536) != 0;
                verified = (flags & 131072) != 0;
                explicit_content = (flags & 262144) != 0;
                id = stream.readInt32(exception);
                if ((flags & 1) != 0) {
                        access_hash = stream.readInt64(exception);
                }
                if ((flags & 2) != 0) {
                        first_name = stream.readString(exception);
                }
                if ((flags & 4) != 0) {
                        last_name = stream.readString(exception);
                }
                if ((flags & 8) != 0) {
                        username = stream.readString(exception);
                }
                if ((flags & 16) != 0) {
                        phone = stream.readString(exception);
                }
                if ((flags & 32) != 0) {
                        photo = UserProfilePhoto.TLdeserialize(stream, stream.readI
                }
                if ((flags & 64) != 0) {
                        status = UserStatus.TLdeserialize(stream, stream.readInt32(
                }
                if ((flags & 16384) != 0) {
                        bot_info_version = stream.readInt32(exception);
                }
        }
```

Figura 4.30. Función “readParams” del código fuente del cliente móvil de la aplicación de IM Telegram Messenger para Android.

La figura 4.31 corresponde a la información obtenida de la función “ToStream” contenida en el fichero “TLUserBase.cs” del código fuente para WP, función equivalente a la indicada anteriormente en el código fuente para Android. En esta figura se muestra como la información de un usuario de tipo contacto se almacena en una estructura de datos fija no dependiente de ningún campo.

```
public override void ToStream(Stream output)
{
    output.Write(TLUtils.SignatureToBytes(Signature));
    output.Write(Id.ToBytes());
    output.Write(FirstName.ToBytes());
    output.Write(LastName.ToBytes());
    output.Write(UserName.ToBytes());
    output.Write(Phone.ToBytes());
    Photo.ToStream(output);
    Status.ToStream(output);
    output.Write(Inactive.ToBytes());

    NotifySettings.NullableToStream(output);
    ExtendedInfo.NullableToStream(output);
    Contact.NullableToStream(output);
}
```

Figura 4.31. Función “ToStream” del código fuente del cliente móvil de la aplicación de IM Telegram Messenger WP.

5 ANALISIS FORENSE IM EN ORDENADORES

En este quinto capítulo se exponen las contribuciones realizadas al análisis forense del cliente de escritorio de las aplicaciones de mensajería instantánea en ordenadores como parte de la investigación realizada en la presente Tesis.

5.1 Introducción

Los dispositivos informáticos, ya sean ordenadores, portátiles o servidores, debido a su elevada capacidad de procesamiento y almacenamiento han sido y son actualmente uno de los principales dispositivos electrónicos incluidos en la comisión de hechos delictivos. La evolución de las nuevas tecnologías de la información ha ocasionado que el volumen de información almacenada en estos dispositivos informáticos sea un problema cuando se trata desde el punto de vista del análisis forense. El volumen y disparidad de los datos que pueden alojarse en los sistemas de almacenamiento masivo incluidos en este tipo de dispositivos (HDD, SSD, etc.), conlleva que deban realizarse estudios técnico-forenses sobre los rastros que se generan tanto el sistema operativo como las aplicaciones informáticas utilizadas por el usuario o usuarios del dispositivo electrónico. Si bien, cada vez es menos extendido el uso de los dispositivos informáticos en aras de los dispositivos móviles, del análisis forense de los sistemas de almacenamiento masivo incluidos en un ordenador se puede obtener infinidad de artefactos, entendiendo como tal, documentos ofimáticos, correos electrónicos, navegación web (histórico, descargas, etc.), archivos multimedia, contraseñas, contenedores de archivos, archivos de configuración, archivos de datos, bases de datos, registros de eventos, archivos de Log, metadatos de archivos, etc. El análisis forense debe adaptarse a la realidad actual de los datos contenidos en los dispositivos informáticos objeto de estudio y aplicar los procedimientos científicos necesarios para adquirir, analizar e interpretar todos los artefactos contenidos en un ordenador manteniendo en todo momento la inalterabilidad de los datos.

5.1.1 Adquisición forense en ordenadores

La adquisición forense estática o adquisición tradicional, es aquella que se realiza sobre un dispositivo informático apagado utilizando soluciones forenses especificas a partir de las cuales puede ser verificada tanto la integridad de los datos originales como de la copia realizada. Estas soluciones generan una imagen o varias imágenes forenses del contenido total del sistema de almacenamiento masivo incluido en el ordenador. Existen diferentes procedimientos forenses que permiten realizar este tipo de adquisición con las suficientes garantías, si bien por lo general, la adquisición forense estática se realiza conectando el sistema de almacenamiento masivo extraído del ordenador origen, generalmente disco duro o disco de estado sólido, en un dispositivo *hardware* forense (clonadoras o bloqueadores) para posteriormente a través de *software* forense generar la imagen o imágenes forenses del contenido.

La adquisición forense dinámica es aquella que se realiza sobre un dispositivo informático encendido utilizando soluciones forenses especificas a partir de las cuales puede ser verificada tanto la integridad de la copia realizada. Estas soluciones permiten realizar una copia lógica de los datos que están siendo generados por un sistema en ejecución. Este tipo de adquisición se realiza en aquellas situaciones en las que el equipo este encendido y se necesita extraer la información volátil no accesible con el sistema apagado (memoria RAM, archivo de paginación, archivo de hibernación, archivos temporales, procesos de red, procesos de sistemas, contenedores cifrados, etc.). Se debe tener presente que, mientras el ordenador este encendido tanto el sistema operativo como las aplicaciones en ejecución alteran la información almacenada en el dispositivo de almacenamiento masivo.

5.1.2 Análisis forense en ordenadores

El análisis forense de un ordenador al igual que sucede con el proceso de adquisición, puede también subdividirse en análisis forense estático y análisis forense dinámico de artefactos. En el primer caso se realiza el análisis forense de los registros contenidos en la imagen o imágenes forenses generadas durante el proceso de adquisición. En el segundo caso se realiza el análisis forense a partir de los artefactos que están siendo generados en el ordenador durante su ejecución.

Al igual que ocurre con el cliente móvil de las aplicaciones de mensajería instantánea, el análisis forense del cliente de escritorio de este tipo de aplicaciones debe abordarse desde una perspectiva más amplia de la adquisición e interpretación de las comunicaciones de usuario. Existen diversas soluciones forenses comerciales especializadas en automatizar tanto el proceso de adquisición como en proceso de análisis forense del cliente de escritorio de las aplicaciones de mensajería instantánea, si bien, tal y como quedará demostrado en los siguientes puntos, estas soluciones no pueden cubrir la enorme cantidad de aplicaciones de mensajería instantánea que han existido, existen o existirán y mucho menos el análisis forense de cada característica.

En la actualidad, uno de los mayores problemas en el análisis forense de los clientes de escritorio de las aplicaciones de mensajería instantánea es el cifrado de la información. Este tipo de clientes, como norma general, cifran el contenido tanto de los datos generados por la propia aplicación de IM como de los datos relativos a las comunicaciones mantenidas por el usuario. En este caso, el análisis forense estático proporciona información limitada con respecto a los artefactos generados por este tipo de clientes, siendo hace necesario evolucionar hacia el análisis forense dinámico, el cual debe incluir procedimientos y técnicas forenses que permitan obtener las comunicaciones de usuario asegurando en todo momento la inalterabilidad de la evidencia digital original.

5.2 Escenarios: Telegram Messenger y WhastApp sobre macOS

En los siguientes puntos, se desarrollan los estudios técnico-forenses realizados sobre los clientes de escritorio de las aplicaciones de mensajería instantánea Telegram Messenger y WhatsApp en el sistema operativo macOS, exponiendo los resultados obtenidos relativos a los registros que generan cada una de estas aplicaciones.

Estos estudios son realizados sobre estos clientes de escritorio, ya que, corresponden con dos de las aplicaciones de mensajería instantánea más utilizadas en el mundo, siendo estas las primeras aplicaciones de IM en encriptar sus mensajes punto a punto, transferir diferentes tipos de archivos, crear diferentes tipos de chats (canales, grupos públicos y privados, etc.) además de proporcionar diversos métodos de conexión a través de sus clientes móvil, de escritorio y web.

De igual manera, la escasa documentación forense relativa a los clientes de escritorio de estas dos aplicaciones de IM sumada al auge del sistema operativo macOS, hace necesario el desarrollo de estudios técnico-forenses en los cuales se exponga el análisis forense realizado sobre los rastros generados por los clientes de escritorio de las aplicaciones de IM Telegram Messenger y WhatsApp en este sistema.

5.2.1 Cuestiones y herramientas comunes en el análisis forense IM

Los estudios técnico-forenses que a continuación se exponen se llevan a cabo a partir de la metodología de análisis forense propuesta en la presente tesis, compuesta por la suma de tres métodos de estudio. Estos métodos de estudio pretenden proporcionar un conocimiento funcional, técnico y forense del cliente de escritorio estudiado, así como validar la integridad de la información obtenida. Los estudios técnico-forenses son desarrollados sobre el cliente de escritorio de las aplicaciones de mensajería instantánea Telegram Messenger y WhatsApp en el sistema operativo macOS al objeto de certificar la metodología de análisis forense propuesta con independencia de la aplicación de mensajería instantánea examinada. Cabe mencionar que en el momento del desarrollo de estos estudios no existía documentación forense al respecto de los artefactos generados por los clientes de escritorio de estas aplicaciones de IM en el sistema operativo macOS.

La complejidad del análisis forense, así como el volumen de la información generado por este tipo de aplicaciones implica que en muchas ocasiones se haga uso de soluciones forenses comerciales o gratuitas que automatizan el análisis forense de este tipo de aplicaciones si bien, aunque no siempre estas soluciones identifican, decodifican o interpretan toda la información generada por los clientes de escritorio de las aplicaciones de mensajería instantánea. Al igual que sucede con el cliente móvil de este tipo de aplicaciones, no es posible encontrar una única herramienta forense que abarque la totalidad de clientes de escritorio de las aplicaciones de IM, ni la totalidad de sus funcionalidades. En el caso específico del cliente de escritorio de la aplicación de mensajería instantánea Telegram Messenger y WhatsApp para el sistema operativo macOS se comprueba que, en el momento del desarrollo de los estudios técnico-forenses que a continuación se exponen, varias de las principales soluciones forenses comerciales (BEC de Belkasoft o IEF de Magnet Forensics) no realizaban el análisis forense de estos clientes de escritorio.

A continuación, se desarrollarán los tres métodos de estudios incluidos en la metodología propuesta, exponiendo los resultados obtenidos de aplicar ésta al análisis forense de los clientes de escritorio de las aplicaciones de mensajería instantánea Telegram Messenger y WhatsApp para macOS.

5.3 Análisis de Telegram Messenger en macOS

Este punto expondrá el resultado obtenido del estudio de fuentes abiertas, de artefactos y de código fuente, incluidos en la metodología de análisis forense propuesta, sobre los registros que genera el cliente de escritorio de aplicación de IM Telegram Messenger sobre el sistema operativo macOS.

5.3.1 Estudio de fuentes abiertas

El estudio de fuentes abiertas ha sido desarrollado a partir de los procedimientos descritos en el punto 3.3.1 de esta Tesis. Estos procedimientos permitirán recopilar de manera fiable, toda aquella documentación que pueda de una u otro forma contribuir en el análisis forense del cliente de escritorio de la aplicación de IM Telegram Messenger para sistema operativo macOS.

El estudio de fuentes abiertas es realizado sobre los resultados obtenidos de las consultas realizadas en diferentes motores de búsqueda indexados de Internet (Bing, Google, Google Scholar, etc.), a partir de la búsqueda de diferentes palabras clave en diferentes idiomas (Telegram Messenger, Desktop, Instant Messenger, IM, mensajería instantánea, Forensics, Forense, Analysis, Análisis, macOS, etc.). En este caso, la búsqueda correspondiente con al cliente de escritorio de la aplicación de mensajería instantánea Telegram Messenger en macOS se realiza sobre aquellas fuentes de datos abiertas o semiabiertas disponibles, como puede ser la web del desarrollador (whatsapp.com), revistas de investigación digital (journals.elservier.com/digital-investigation; commons.erau.edu/jdfsl, etc.), foros técnicos (focusforensics.com; forensicswiki.com; incibe.com, etc.), investigadores independientes (dinosec.com/es/lab.html, etc.), ponencias técnicas (RootedCon, Blackhat, etc.), bibliotecas virtuales (http://biblioteca.uah.es, etc.) o en gestores de contenido (scholar.google.com, etc.). En el momento del estudio de fuentes abiertas como resultado de la búsqueda realizada se encuentran, un artículo, un foro técnico, así como información técnica del desarrollador de la aplicación.

En el articulo *Anwendungsanalyse des Messengers Telegram Desktop (Version 0.9.15) unter Windows 10* (Oertle, C., 2016), su autor realiza un estudio sobre los artefactos generados por el cliente de escritorio de la aplicación de IM Telegram Messenger en el sistema operativo Windows 10. El documento muestra los registros generados en el sistema operativo Windows 10 al ejecutar diferentes casos de uso sobre el cliente de escritorio de la aplicación de IM Telegram Messenger, si bien, este estudio no valida los resultados obtenidos ni obtiene conclusiones que ayude al análisis forense del cliente de escritorio. Este estudio al ser examinado es utilizado como documentación de apoyo para el análisis forense del cliente de escritorio de la aplicación de IM Telegram Messenger en macOS.

En el foro técnico *Unofficial Telegram Wiki*[35], se muestra cierta información relativa a las carpetas que genera el cliente de escritorio de la aplicación de IM Telegram Messenger en un sistema operativo macOS. Este foro una vez examinado es utilizado como documentación de apoyo para el análisis forense del cliente de escritorio de la aplicación de IM Telegram Messenger en macOS.

Por último, en la página web del desarrollador de la aplicación Telegram Messenger[36] se encuentra diversa información relativa a estructuras de datos (objetos, tipos, etc.), API (*Applicacion Programming Interface*), código fuente e incluso el protocolo utilizado por la aplicación para sus comunicaciones (MTProto), si bien, no se indica de manera específica información relativa al cliente de escritorio de la aplicación de IM Telegram Messenger para macOS más allá del código fuente. En este caso, la información proporcionada por el propio desarrollador de la aplicación será utilizada como apoyo en el análisis forense de cliente de escritorio de la aplicación de mensajería instantánea Telegram Messenger para macOS.

Tal y como se reflejará en el siguiente punto, el estudio de fuentes abiertas realizado podrá ser utilizado para identificar la información obtenida en el estudio de artefactos.

[35] Unofficial Telegram Wiki. Recuperado de, https://telegram.wiki/#telegram_desktop. Accedido el 13-03-2018.

[36] Telegram Messenger. Recuperado de, https://telegram.org

5.3.2 Estudio de artefactos

El estudio de artefactos ha sido desarrollado a partir de los procedimientos descritos en el punto 3.3.2 de esta Tesis. Estos procedimientos permitirán identificar, decodificar e interpretar los rastros generados por el cliente de escritorio de la aplicación de mensajería instantánea Telegram Messenger en el sistema operativo macOS a partir del análisis comparativo registros.

Como ya fue mencionado anteriormente, el análisis forense tradicional puede verse limitado debido a las especiales características tanto de los sistemas operativos como de las aplicaciones instaladas en los dispositivos informáticos. Este es el caso del cliente de escritorio de la aplicación de IM Telegram Messenger para macOS, el cual hace necesario que el estudio de artefactos sea una combinación el análisis forense estático y dinámico de artefactos. A partir del análisis forense estático de artefactos se identificarán todos aquellos registros generados, modificados o eliminados por el cliente de escritorio de la aplicación de IM Telegram Messenger, siendo necesario el análisis forense dinámico para obtener la información en claro de las comunicaciones del usuario.

En los puntos sucesivos se desarrolla el estudio de artefactos realizado sobre del cliente de escritorio de la aplicación de IM Telegram Messenger en un sistema operativo macOS, suma del análisis de forense estático y dinámico de artefactos.

5.3.2.1 Análisis forense estático de artefactos

A continuación, se muestran los resultados obtenidos del análisis comparativo realizado sobre los rastros generados por el cliente de escritorio de la aplicación de IM Telegram Messenger en el sistema operativo macOS. Este ha sido elaborado a partir del análisis forense estático incluido en el estudio de artefactos de la metodología propuesta, el cual permite identificar, decodificar e interpretar los rastros generados por este cliente de escritorio en el sistema operativo macOS. La tabla 5.1 muestra, el listado de artefactos generados por el cliente de escritorio de la aplicación de IM Telegram Messenger para macOS.

Tabla 5.1. Listado de artefactos generados por el cliente de escritorio de la aplicación de IM Telegram Messenger en macOS.

#	Contenido	Nombre	Directorio	Descripción
1	Aplicación	Telegram.app	/Applications/	Datos de la aplicación.
2	Datos de Log	Log.txt	/Users/{USER}/Library/Application Support/Telegram Desktop/	Registro de eventos.
3	Datos de usuario	Diferentes ficheros (usertag, settings1, etc.).	/Users/{USER}/Library/Application Support/Telegram Desktop/tdata	Diferentes archivos de usuario. Datos encriptados.
4	Datos temporales y de configuración	data.data, windows.plist, window_1.data	/Users/{USER}/Library/Saved Application State/com.tdesktop.Telegram.savedState	Ficheros temporales de configuración.
5	Archivos	Diferentes tipos de ficheros. (*.mp4, *.jpg, *.pdf, etc.)	/Users/{USER}/Downloads (Default)	Archivos descargados.
6	Conexión (Socket).	7852aa807d0e61276974ee878396a1c4-{87A94AB0-E370-4cde-98D3-ACC110C5967D}	/tmp/	Información sobre conexión.

5.3.2.1.1 Análisis de los ficheros de datos de usuario

El análisis de los ficheros de datos de usuario se centra en el estudio del contenido de la carpeta "/Users/{USER}/Library/Application Support/Telegram Desktop/tdata" (fila 3, tabla 5.1). En el interior de este directorio "tdata" se ubican, entre otros, los ficheros con nombre "usertag", "settings1" y "D877F783D5D3EF8C1", así como una carpeta con el nombre "D877F783D5D3EF8C". A su vez, en el interior de esta carpeta "D877F783D5D3EF8C" se almacena un fichero con nombre "map1", así como diversos archivos cuyo nombre está formado por 16 caracteres alfanumérica aleatorios.

La figura 5.1 muestra a modo de ejemplo el listado de archivos y directorios que almacena la carpeta "/Users/{USER}/Library/Application Support/Telegram Desktop/tdata".

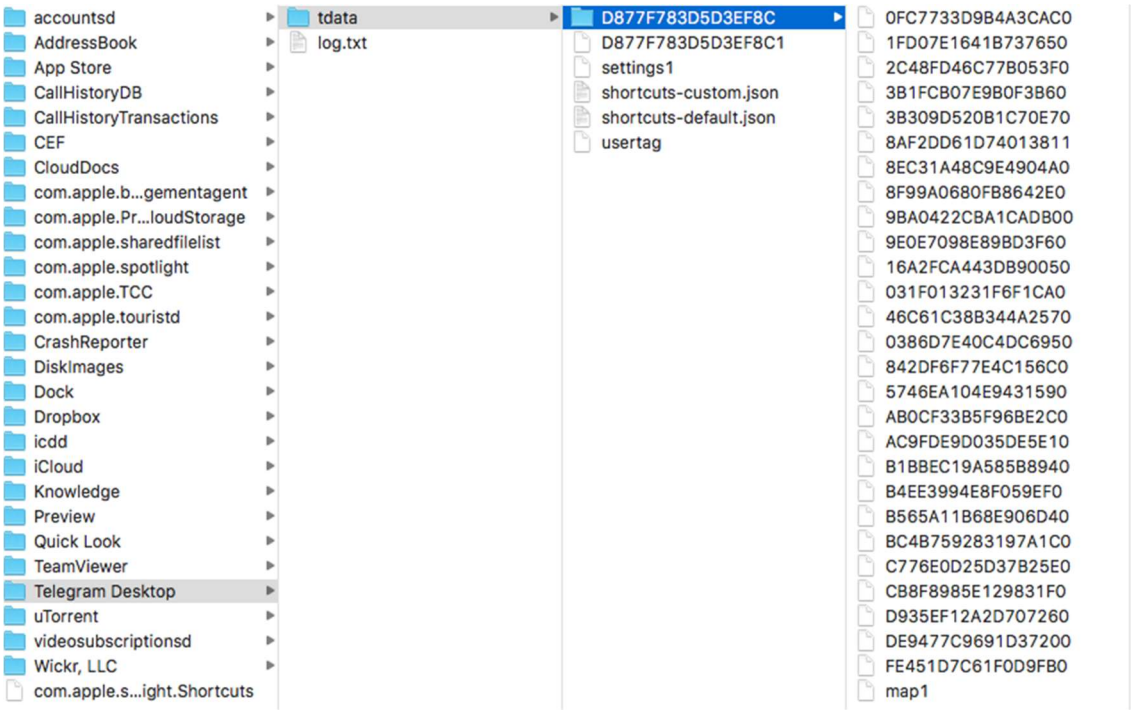


Figura 5.1. Ejemplo de contenido carpeta “Telegram Desktop” generada por el cliente de escritorio de la aplicación Telegram Messenger.

Analizado el contenido de los diferentes ficheros de datos expuestos con anterioridad, se observa que todos estos ficheros contienen información ilegible, si bien, lo único que tienen en común todos estos ficheros es el inicio del fichero, el cual corresponde con el valor hexadecimal “54444624” (“TDF$”).

La figura 5.2 muestra a modo de ejemplo el inicio y parte del contenido del fichero “settings1” ubicado en la carpeta “/Users/{USER}/Library/Application Support/Telegram Desktop/tdata” en el cual se identifica la cabecera “TDF$”, siendo el resto del contenido ilegible.

```
00000000  54 44 46 24 3f 46 0f 00  00 00 00 20 e4 f1 0f e4  |TDF$?F..... ....|
00000010  e3 12 b3 44 5e 27 f5 4e  e6 79 45 6b 16 e6 b6 95  |...D^'.N.yEk....|
00000020  88 97 fe 63 2f a9 37 31  0c 8a b3 e5 00 00 02 c0  |...c/.71........|
00000030  b2 c6 b6 4c 3e e1 27 9a  d5 8f 5c 66 75 fa 1f 0e  |...L>.'...\fu...|
00000040  38 e2 be 8a 3e e9 36 27  6e 13 fa 0c c6 70 15 7c  |8...>.6'n....p.||
00000050  7f a3 82 a0 83 67 b1 94  55 29 40 d7 e5 fc 9c 8e  |.....g..U)@.....|
00000060  3f 7a 8d 0a 1f ff cb b5  22 d8 be 07 96 4f bf df  |?z......"....O..|
00000070  27 43 7e f6 db 16 ff fc  4d ba 0d 5b 8b b6 f8 f4  |'C~.....M..[....|
00000080  88 d8 13 9f 4e 62 49 76  e4 38 d8 0c b1 32 ab 7e  |....NbIv.8...2.~|
00000090  d7 33 3b 41 a1 f2 fb ac  71 bd 60 55 21 9a 75 fd  |.3;A....q.`U!.u.|
```

Figura 5.2. Inicio del fichero “settings1”.

De igual manera la figura 5.3 muestra a modo de ejemplo el inicio y parte del contenido del fichero "5746EA104E9431590" ubicado en la carpeta "/Users/{USER}/Library/Application Support/Telegram Desktop/tdata D877F783D5D3EF8C" en el cual se identifica la cabecera "TDF$", siendo el resto del contenido ilegible.

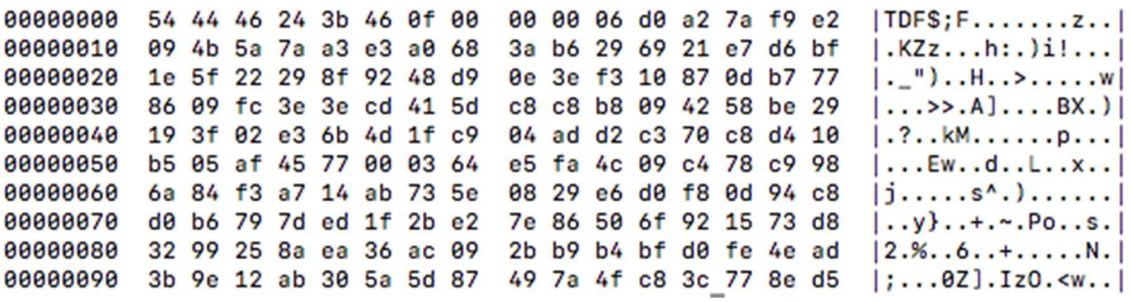


Figura 5.3. Inicio del fichero "5746EA104E9431590" ubicado en la carpeta "D877F783D5D3EF8C".

Del análisis forense estático realizado se desprende que, si bien el contenido de los archivos de datos contenidos en la carpeta "/Users/{USER}/Library/Application Support/Telegram Desktop/tdata" se encuentran cifrado, los archivos con nomenclatura alfanumérica contenidos en la carpeta "D877F783D5D3EF8C" corresponden con los mensajes de las diferentes conversaciones que el usuario de la aplicación. Estos ficheros cuyo nombre está formado por 16 caracteres alfanuméricos aleatorios se crean en la carpeta "D877F783D5D3EF8C" cuando el usuario de la aplicación visualiza por primera vez un mensaje, si bien, del análisis forense estático no es posible obtener la relación de mensajes intercambiados a partir del cliente de escritorio de mensajería instantánea de Telegram Messenger en macOS.

Tras el análisis forense estático de los diferentes rastros generados por el cliente de escritorio de la aplicación de IM Telegram Messenger se puede concluir que, no se pueden obtener datos relativos a la aplicación ni a las comunicaciones o datos del usuario, si bien, se pueden conocer datos como la fecha de instalación y registros de eventos de la aplicación o ficheros descargados por el usuario.

Del estudio del código fuente del cliente de escritorio de la aplicación de IM Telegram Messenger, tal y como se expondrá posteriormente, se obtiene el conocimiento necesario para comprender la información obtenida durante este análisis forense estático. A partir

del análisis del código fuente se llega a la conclusión de como el contenido de los ficheros de datos se almacena de forma cifrada (localstorage.cpp; archivo del código fuente) o de como el nombre de la carpeta "D877F783D5D3EF8C" alojada bajo la carpeta "/Users/{USER}/Library/Application Support/Telegram Desktop/tdata" corresponde a los primeros 16 caracteres del valor de una función matemática (utils.cpp; archivo del código fuente).

5.3.2.2 Análisis forense dinámico de artefactos

El análisis forense dinámico de artefactos parte de las conclusiones obtenidas del estudio realizado en el análisis forense estático sobre el cliente de escritorio de la aplicación de IM Telegram Messenger en el sistema operativo macOS. Identificados los artefactos generados a partir del análisis forense estático se procede al análisis forense dinámico utilizando el método de copia forense expuesto en el punto 3.3.2 de esta Tesis. El método de copia forense permitirá simular el entorno original de manera controlada permitiendo el análisis y obtención de las comunicaciones de usuario mantenidas a partir del cliente de escritorio de la aplicación de IM Telegram Messenger en macOS.

A continuación, se expone de manera práctica como se obtienen las comunicaciones mantenidas por este cliente a partir de la combinación del análisis forense estático y dinámico de artefactos.

5.3.2.2.1 Identificación de artefactos

A partir del análisis forense estático de artefactos se identifica toda aquella información relacionada tanto con el cliente de escritorio de la aplicación de mensajería instantánea como con los datos del usuario. En este caso práctico, el análisis forense estático de artefactos se realiza sobre todos aquellos registros que el cliente de escritorio de la aplicación de IM Telegram Messenger (v1.1.23) genera en un ordenador de la marca "Apple" modelo "MacBook Pro" con sistema operativo "macOS High Sierra" (v12.13).

- La adquisición forense y generación de imagen forense se realiza a través de un

"*liveCD*" con la distribución forense "DEFT Zero"[37]. Para poder realizar este tipo de adquisición se debe tener en cuenta que sistema de cifrado "*FileVault*" [38] no se encuentre activo.

- El tratamiento de la imagen forense se realiza en un entorno forense controlado con sistema operativo macOS. Esto debe ser así, ya que, en el momento de la realización de este estudio técnico-forense, las principales soluciones forenses comerciales no soportaban el sistema de archivos de Apple (APFS[39]). La imagen forense resultante de la adquisición será analizada a través las aplicaciones nativas "DiskImageMounter.app" y "Finder.app" del entorno forense controlado con macOS.

En la figura 5.4 se identifica como se muestra la imagen forense con nombre "image_27_09_2017.dmg" realizada sobre el ordenador original en el entorno forense controlado con macOS.

[37] DEFT. Deft Zero. Recuperado el 23 de septiembre de 2019, de: https://na.mirror.garr.it/mirrors/deft/zero/. Accedido el 23-09-2019.

[38] Apple. (2018). *Utilizar FileVault para encriptar el disco de arranque del Mac*. Recuperado el 6 de julio de 2018, de: httsp://support.apple.com/es-es/HT204837.

forensicexplorer.com/.

[39]Apple. (2018). *About Apple File System*. Recuperado el 18 de junio 2018, de: https://developer.apple.com/documentation/foundation/file_system/about_apple_file_system

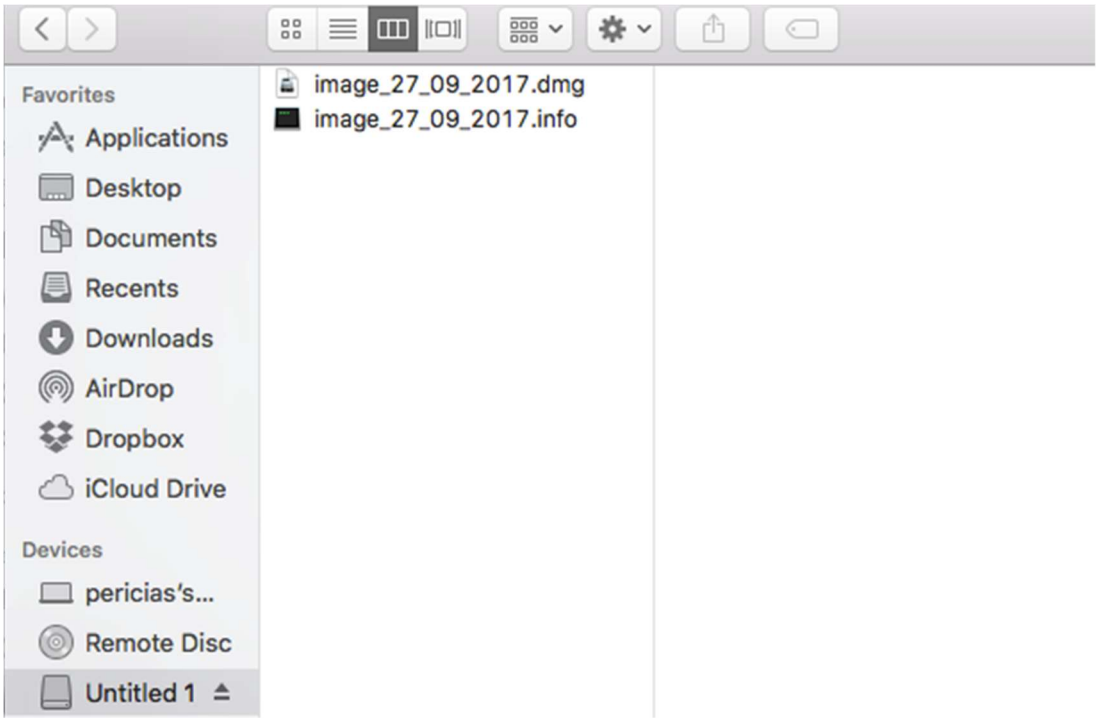


Figura 5.4. Imagen forense "Image_27_09_2017.dmg" en el entorno forense controlado.

Esta imagen forense ("image_27_09_2017.dmg") puede ser analizada a partir de las diferentes aplicaciones nativas ("Finder.app", "Terminal.app", etc.) del entorno forense controlado con sistema operativo macOS.

La figura 5.5 muestra como a partir de la aplicación nativa "Finder.app" del entorno forense controlado se pueden visualizar el contenido de la imagen forense "image_27_09_2017.dmg". En esta figura se identifica el listado de aplicaciones instaladas en el ordenador original, encontrándose entre ellas el cliente de escritorio de la aplicación de IM Telegram Messenger ("/Applications/Telegram.app").

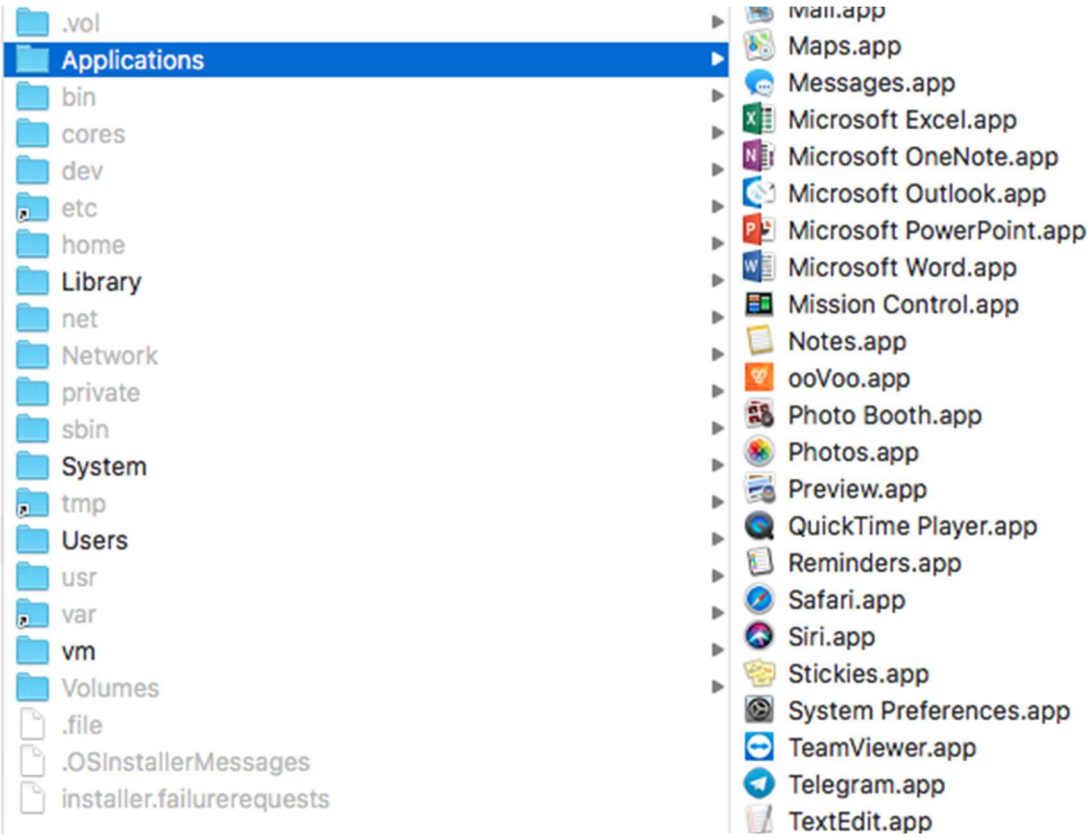


Figura 5.5. Listado de aplicaciones. Imagen forense "Image_27_09_2017.dmg".

Así de igual manera, la figura 5.6 muestra como a partir de la aplicación nativa "Finder.app" del entorno forense controlado se pueden visualizar el contenido de la imagen forense "image_27_09_2017.dmg". En esta figura se identifica el contenido de la carpeta "/Users/{USER}/Library/Application Support/Telegram Desktop/" del ordenador original.

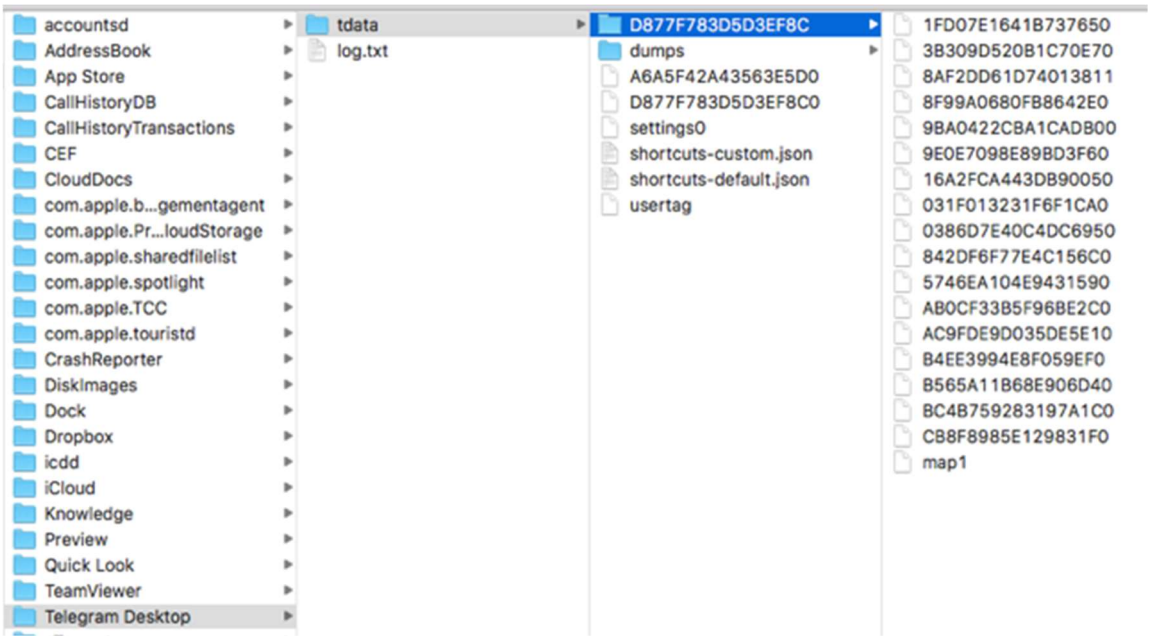


Figura 5.6. Contenido del directorio "Telegram Desktop". Imagen forense "Image_27_09_2017.dmg".

Localizados estos directorios y archivos relativos al cliente de escritorio de la aplicación de IM Telegram Messenger en la imagen forense con nombre "image_27_09_2017.dmg" realizada sobre el ordenador original, basta con realizar una copia forense tanto de los datos de la aplicación ("/Applications/Telegram.app") como los datos de usuario ("/Users/{USER}/Library/Application Support/Telegram Desktop/") en el entorno forense controlado con macOS.

5.3.2.2.2 Obtención de información

A continuación, se detalla el procedimiento a partir del cual se obtienen las conversaciones mantenidas a través del cliente de escritorio de la aplicación de IM Telegram Messenger, centrando este en los conceptos técnicos sin entrar en los aspectos legales necesarios. El proceso expone como se realiza el análisis forense dinámico de los artefactos a partir de la copia forense realizada en el punto anterior.

- La copia forense de los datos incluidos en la imagen forense resultante de la adquisición realizada del ordenador original ("image_27_09_2017.dmg") será realizada a través de las aplicaciones nativas del entorno forense controlado. En

el caso del cliente de escritorio de la aplicación de IM Telegram Messenger se realizará la copia forense de los datos relativos a la aplicación ("/Applications/Telegram.app"), así como la copia forense de los datos relativos al usuario ("/Users/{USER}/Library/Application Support/Telegram Desktop/").

Se realiza la copia forense de los datos de la aplicación ("Applications/Telegram.app") incluidos en la imagen forense con nombre "image_27_09_2017.dmg" en el entorno forense controlado, creándose la aplicación "/Applications/Telegram 2.app" en el entorno forense controlado. De igual forma se realiza la copia forense de los datos de usuario ("/Users/{USER}/Library/Application Support/Telegram Desktop/") incluidos en la imagen forense con nombre "image_27_09_2017.dmg" en el entorno forense controlado, creándose el directorio "/Users/{FORENSIC_USER}/Library/Application Support/Telegram Desktop/" en el entorno forense controlado. En el caso del cliente de escritorio de la aplicación, se crea la aplicación "/Applications/Telegram 2.app" (copia forense) ya que la aplicación "Applications/Telegram.app" (nueva instalación) corresponde con una instalación limpia del cliente de escritorio de la aplicación de IM Telegram Messenger el cual servirá para demostrar posteriormente diversas características de este cliente de escritorio.

La figura 5.7 muestra parte del listado de aplicaciones ubicadas en la carpeta "/Applications/" del entorno forense controlado. En esta figura se pueden identificar la aplicación "Telegram.app" (nueva instalación) así como la aplicación "Telegram 2.app" (copia forense).

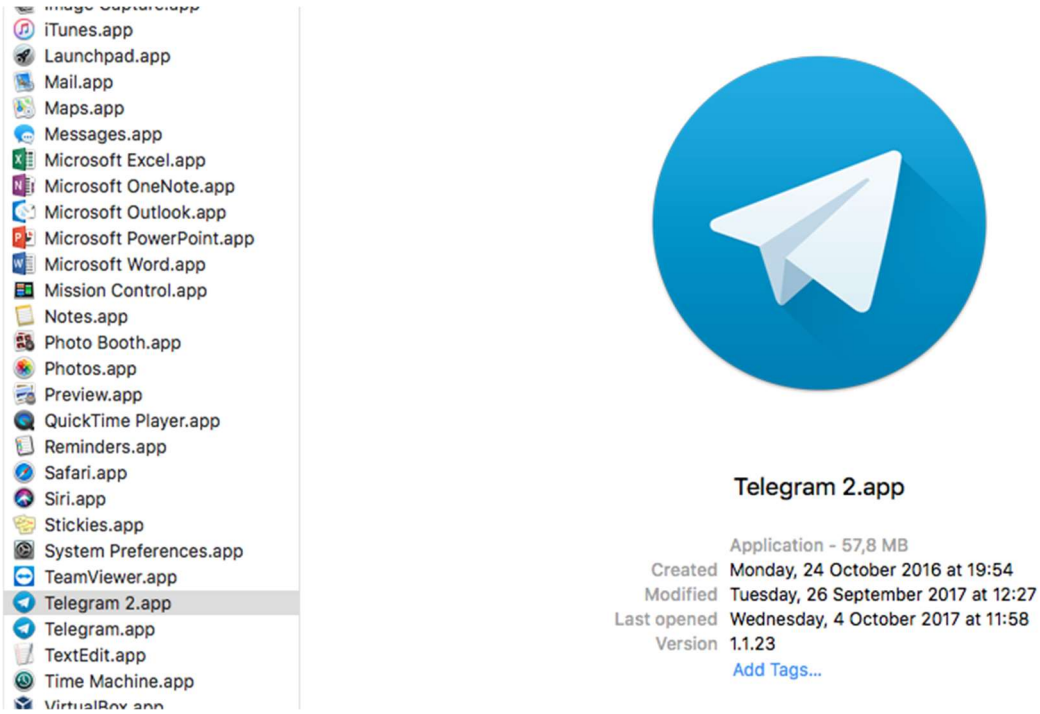


Figura 5.7. Listado de aplicaciones. “Telegram.app” (nueva instalación). “Telegram 2.app” (copia forense).

Si se ejecuta la aplicación “/Applications/Telegram.app” (nueva instalación) con la copia forense de los datos del usuario (“/Users/{USER}/Library/Application Support/Telegram Desktop/”) en el entorno forense controlado (“/Users/{FORENSIC_USER}/Library/Application Support/Telegram Desktop/”), esta solicita el número de teléfono para proceder a su verificación.

La figura 5.8 muestra el resultado de la ejecución de la aplicación “/Applications/Telegram.app” (nueva instalación). Tal como se puede observar en esta figura en este caso se muestra la pantalla de inicio de aplicación en la cual se solicita el número de teléfono asociado.

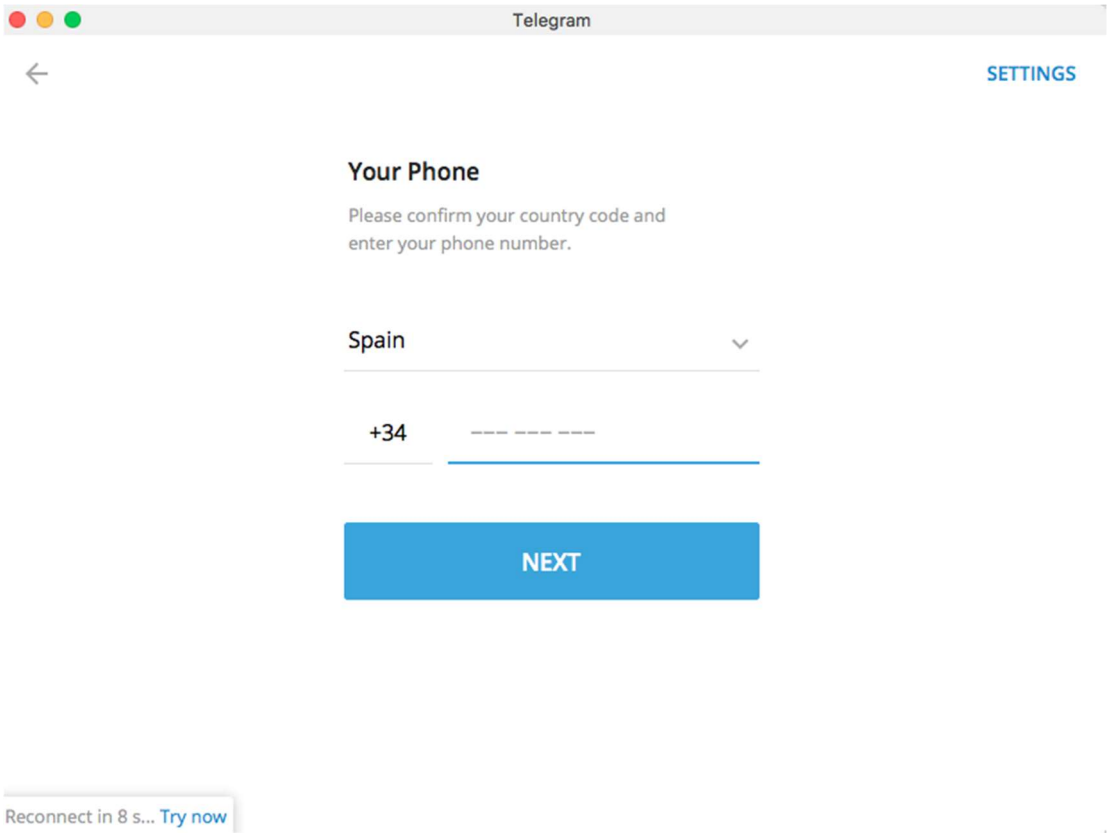


Figura 5.8. Ejecución aplicación "/Applications/Telegram.app" (nueva instalación) sin acceso a Internet.

Si por el contrario se ejecuta la aplicación "/Applications/Telegram 2.app" (copia forense) con la copia forense de los datos del usuario ("/Users/{USER}/Library/Application Support/Telegram Desktop/") en el entorno forense controlado ("/Users/{FORENSIC_USER}/Library/Application Support/Telegram Desktop/"), esta mostrará el entorno gráfico correspondiente con el cliente de escritorio de la aplicación desde el cual se podrá tener acceso a la información de las conversaciones del usuario.

La figura 5.9 muestra el resultado de la ejecución de la aplicación "/Applications/Telegram 2.app" (copia forense). Esta figura muestra la pantalla de conversaciones, si bien, no se recuperan los mensajes del cliente de escritorio de la aplicación de IM Telegram Messenger debido a que el entorno forense controlado no dispone de acceso a Internet.

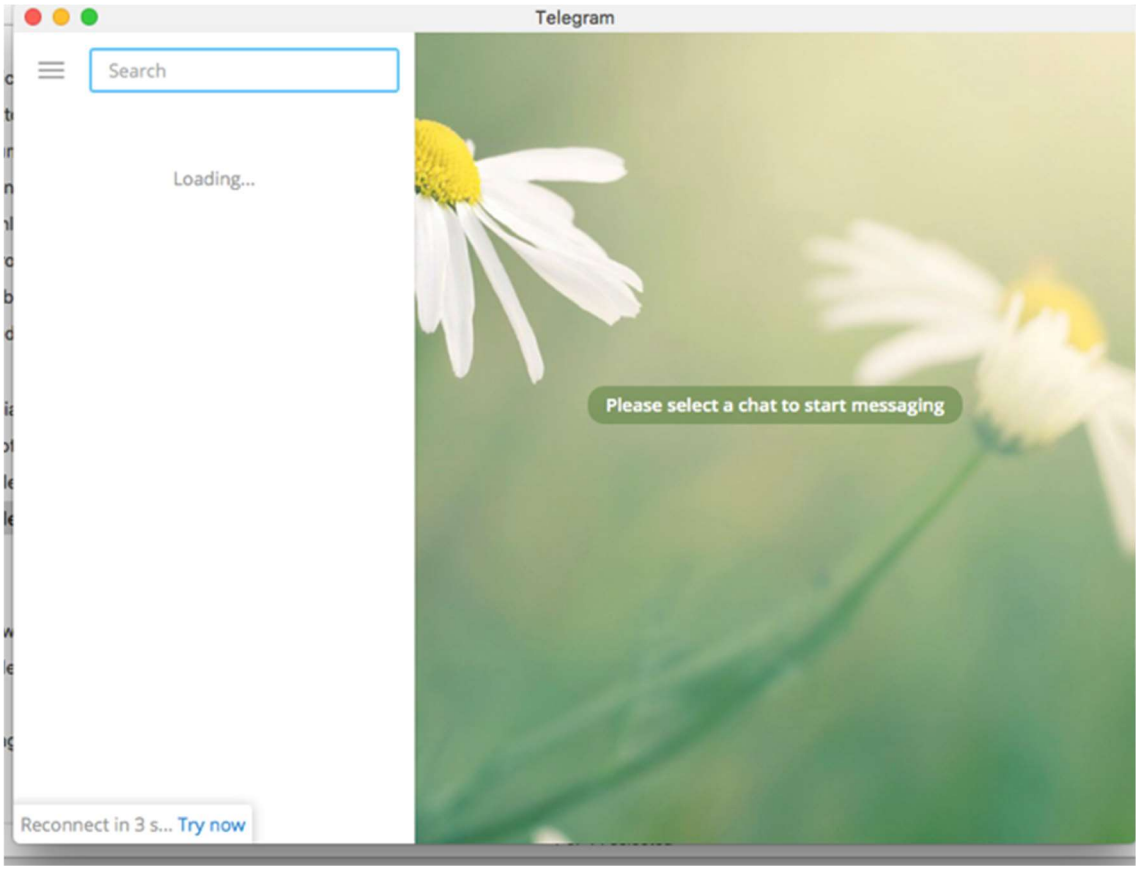


Figura 5.9. Ejecución aplicación "/Applications/Telegram 2.app" (copia forense) sin acceso a Internet.

La figura 5.10 muestra la ejecución de la aplicación "/Applications/Telegram 2.app" (copia forense) con acceso a Internet. En esta figura se puede observar cómo se recuperan del servidor los mensajes del cliente de escritorio de la aplicación Telegram Messenger correspondientes al usuario. Es de mencionar que al tratarse de una aplicación que almacena los datos de usuario en la nube, en el momento de la ejecución de la aplicación "/Applications/Telegram 2.app" (copia forense) se obtendrán todos los mensajes que se han intercambiado con el usuario hasta ese mismo momento, no solo hasta el momento que se genera la imagen forense.

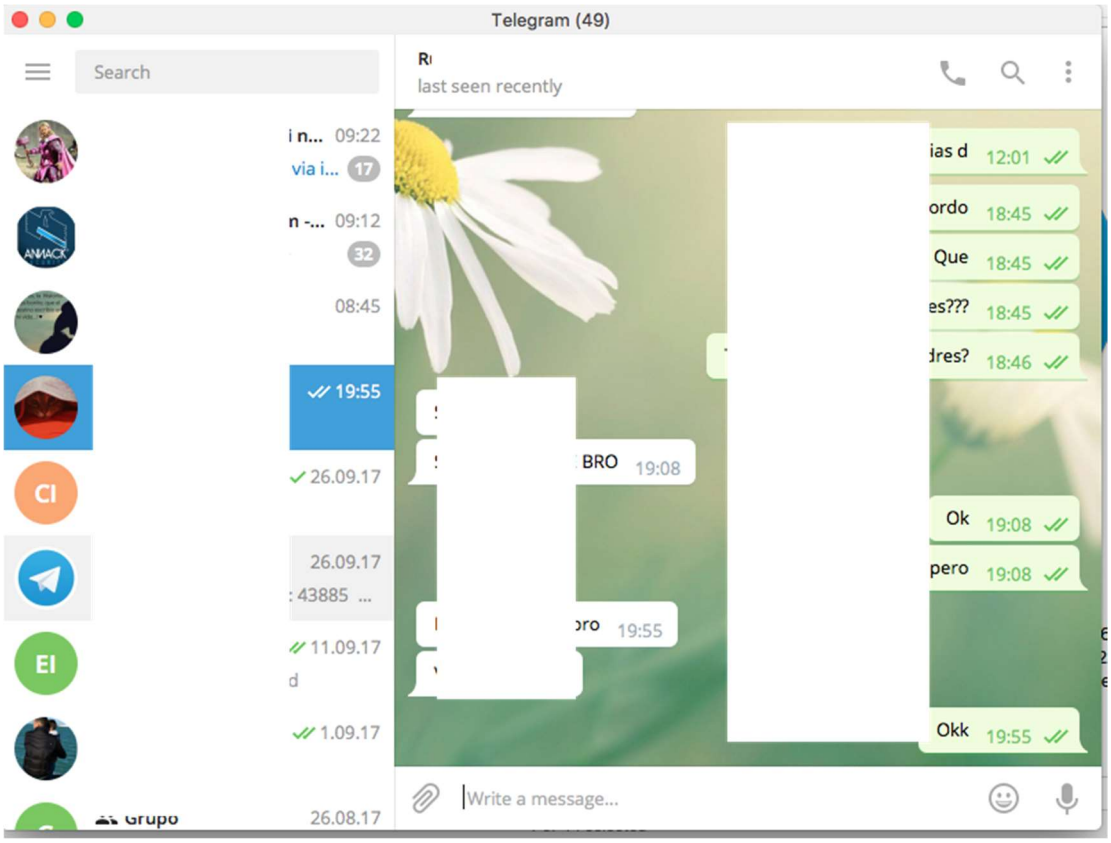


Figura 5.10. Ejecución aplicación "/Applicacions/Telegram 2.app" (copia forense) con acceso a Internet.

Se puede concluir que, para poder visualizar los mensajes del cliente de escritorio de aplicación de IM Telegram Messenger en macOS, además de disponer de la copia forense de los archivos de datos de usuario ("/Users/{USER}/Library/Application Support/Telegram Desktop/"), se debe ejecutar la aplicación obtenida de la imagen forense ("/Applications/Telegram 2.app"), ya que esta, contiene la configuración original de usuario.

5.3.3 Estudio de código fuente

El estudio de código fuente ha sido desarrollado a partir de los procedimientos descritos en el punto 3.3.3 de esta Tesis. Estos procedimientos permitirán identificar e interpretar los registros generados por el cliente de escritorio de la aplicación de IM Telegram Messenger en el sistema operativo macOS a partir del análisis de código fuente.

En este caso del cliente de escritorio de la aplicación Telegram Messenger para el sistema operativo macOS, el propio desarrollador de la aplicación proporciona el código fuente[40]. Al realizar el estudio de código fuente de la aplicación se observa que el mismo se encuentra escrito en lenguaje "C/C++" y que contiene alrededor de 1209 ficheros con extensión ".cpp" los cuales incluyen miles de líneas de código. El estudio de código fuente se centra en el análisis de las líneas de código de aquellos archivos que puedan contener definiciones o funciones en las cuales se identifiquen dónde y cómo se almacena la información generada por este cliente de escritorio. No es objeto principal de este estudio el análisis de todo el código fuente del cliente de escritorio de aplicación de IM Telegram Messenger, por tal motivo a continuación, y a modo de ejemplo, se mostrará el contenido de varios de estos archivos con extensión ".cpp" y su relación con los registros que genera en un ordenador con sistema operativo macOS.

El fichero "localstorage.cpp" ubicado en la carpeta "tdesktop-dev\tdesktop-dev\Telegram\SourceFiles\storage\" del código fuente contiene, entre otras, las funciones que gestionan la lectura y escritura de los ficheros de datos de usuario. La figura 5.11 muestra parte de las líneas de código del fichero "localstorage.cpp" en el cual se identifica la variable con nombre "tdfMagic" y se define su valor "TDF$" (hexadecimal "54444624"). Tal y como quedo reflejado en el análisis forense estático de artefactos, este valor se incluye como cabecera en cada uno de los diferentes ficheros de datos utilizados por la aplicación.

[40] Telegram Messenger. (2018). *Telegram Desktop - Official Messenger*. Recuperado el 16 de Julio de 2018, de: https://github.com/telegramdesktop/tdesktop.

```
#include <openssl/evp.h>

namespace Local {
namespace {

constexpr int kThemeFileSizeLimit = 5 * 1024 * 1024;

using FileKey = quint64;

constexpr char tdfMagic[] = { 'T', 'D', 'F', '$' };
constexpr int tdfMagicLen = sizeof(tdfMagic);

QString toFilePart(FileKey val) {
    QString result;
    result.reserve(0x10);
    for (int32 i = 0; i < 0x10; ++i) {
        uchar v = (val & 0x0F);
        result.push_back((v < 0x0A) ? ('0' + v) : ('A' + (v - 0x0A)));
        val >>= 4;
    }
    return result;
}
```

Figura 5.11. Definición de la variable “tdfMagic”. Fichero “localstorage.cpp”

Así mismo en la figura 5.12 se muestra parte de las líneas de código del fichero “localstorage.cpp” en el cual se identifican las funciones “writeData”, “writeEncrypted” y “prepareEncrypted”. Estas funciones son las encargadas de guardar la información del usuario de forma cifrada en los diferentes ficheros de datos del cliente de escritorio de la aplicación de mensajería instantánea Telegram Messenger en macOS.

```
bool writeData(const QByteArray &data) {
    if (!file.isOpen()) return false;

    stream << data;
    quint32 len = data.isNull() ? 0xffffffff : data.size();
    if (QSysInfo::ByteOrder != QSysInfo::BigEndian) {
        len = qbswap(len);
    }
    md5.feed(&len, sizeof(len));
    md5.feed(data.constData(), data.size());
    dataSize += sizeof(len) + data.size();

    return true;
}
static QByteArray prepareEncrypted(EncryptedDescriptor &data, const MTP::AuthKeyPtr &key = LocalKey) {
    data.finish();
    QByteArray &toEncrypt(data.data);

    // prepare for encryption
    uint32 size = toEncrypt.size(), fullSize = size;
    if (fullSize & 0x0F) {
        fullSize += 0x10 - (fullSize & 0x0F);
        toEncrypt.resize(fullSize);
        memset_rand(toEncrypt.data() + size, fullSize - size);
    }
    *(uint32*)toEncrypt.data() = size;
    QByteArray encrypted(0x10 + fullSize, Qt::Uninitialized); // 128bit of sha1 - key128, sizeof(data), data
    hashSha1(toEncrypt.constData(), toEncrypt.size(), encrypted.data());
    MTP::aesEncryptLocal(toEncrypt.constData(), encrypted.data() + 0x10, fullSize, key, encrypted.constData());

    return encrypted;
}
bool writeEncrypted(EncryptedDescriptor &data, const MTP::AuthKeyPtr &key = LocalKey) {
    return writeData(prepareEncrypted(data, key));
}
void finish() {
    if (!file.isOpen()) return;
```

Figura 5.12. Funciones cifrado de información. Archivo “localstorage.cpp”.

El análisis realizado sobre el código fuente del cliente de escritorio de la aplicación de IM Telegram Messenger para macOS proporciona un conocimiento más detallado de la aplicación. Al igual que sucede en el análisis de fuentes abiertas y análisis forense estático de artefactos, tras el análisis realizado del código fuente de la aplicación se comprueba que, si bien este estudio proporciona diversa información con relación a cómo se gestionan los datos de la aplicación y del usuario, no se puede obtener el contenido de los mensajes de usuario al encontrarse cifrados.

5.3.4 Resultados del análisis realizado

La metodología de análisis forense propuesta en la presente tesis y utilizada en el desarrollo del estudio técnico-forenses del cliente de escritorio de la aplicación de mensajería instantánea Telegram Messenger para el sistema operativo macOS desprende que:

a) Del estudio de las fuentes abiertas, correspondiente con la búsqueda de toda aquella información funcional, técnica y forense que pudiera encontrarse en cualquier fuente de datos abiertas o semiabiertas en el momento del estudio, se comprueba que, si bien existen diversas fuentes con información relativa este cliente de escritorio, las mismas proporcionan información limitada o no concluyente. Cada una de estas fuentes de datos es analizada individualmente, descartando aquellas que no ofrecen información de utilidad para el desarrollo del análisis forense de la aplicación. En el caso del cliente de escritorio de la aplicación de IM Telegram Messenger para macOS se selecciona como fuente principal la proporcionada por el propio desarrollador, si bien, como se observará en los sucesivos estudios esta información deberá ser desechada no siendo de utilidad.

b) Del estudio de los artefactos, infiere que este debe ser desarrollado como la suma del análisis forense estático y dinámico de artefactos:

   - Del análisis forense estático de los rastros generados por el cliente de escritorio de la aplicación de IM Telegram Messenger se identifican las diferentes carpetas y ficheros que se generan, modifican y eliminan, tanto a nivel de la aplicación como a nivel de las comunicaciones de usuario en el ordenador con sistema operativo macOS. Una vez analizados estos ficheros de datos al objeto de obtener la información relativa a las comunicaciones de usuario se concluye que, los ficheros almacenan su contenido de forma cifrada no pudiéndose interpretar los datos contenidos en ellos.

   - Del análisis forense dinámico, producto de aplicar el método de copia forense

sobre los datos originales de la aplicación y usuario, e incluirlos en un entorno forense controlado imitando de esta forma el dispositivo original, se obtiene como resultado las conversaciones relativas a las comunicaciones mantenidas por el usuario del cliente de escritorio de la aplicación de IM Telegram Messenger en macOS.

c) El estudio del código fuente correspondiente al análisis de las líneas de código del lenguaje de programación "C/C++" en el cual se encuentra desarrollado el cliente de escritorio de la aplicación Telegram Messenger para macOS, se obtiene todos aquellos datos necesarios para apoyar y clarificar toda aquella información obtenida y no obtenida del estudio de fuentes abiertas y del estudio estático de artefactos. De esta manera con este estudio se analiza las líneas de código fuente de la aplicación identificando las funciones utilizadas para gestionar la información de la propia aplicación y de los datos de usuario. A partir de este análisis se identifican las funciones utilizadas para la escritura y lectura de ficheros, y se observa como estas funciones aplican un cifrado a los datos al escribir y leer, el cual imposibilita, como se ha indicado en el análisis forense estático de artefactos, la obtención de la información contenida en los diferentes archivos de datos generados por el cliente de escritorio de la aplicación de mensajería instantánea Telegram Messenger en macOS.

Tal y como ha quedado demostrado, la metodología de análisis forense propuesta permite identificar, interpretar y obtener la información generada por el cliente de escritorio de la aplicación de mensajería instantánea Telegram Messenger en el sistema operativo macOS.

5.4 Análisis de WhatsApp en macOS

Este punto expondrá el resultado obtenido del estudio de fuentes abiertas, de artefactos y de código fuente, incluidos en la metodología de análisis forense propuesta, sobre los registros que genera el cliente de escritorio de aplicación de mensajería instantánea WhatsApp sobre el sistema operativo macOS.

5.4.1 Estudio de fuentes abiertas

El estudio de fuentes abiertas ha sido desarrollado a partir de los procedimientos descritos en el punto 3.3.1 de esta Tesis. Estos procedimientos permitirán recopilar de manera fiable toda aquella documentación que pueda de una u otra forma contribuir en el análisis forense del cliente de escritorio, de la aplicación de IM WhatsApp para sistema operativo macOS.

El estudio de fuentes abiertas es realizado sobre los resultados obtenidos de las consultas realizadas en diferentes motores de búsqueda de Internet (Bing, Google, Google Scholar, etc.), a partir de la búsqueda de diferentes palabras clave en diferentes idiomas (WhatsApp, WhatsApp Escritorio, WhatsApp Desktop, macOS, Instant Messenger, IM, mensajería instantánea, Forensics, Analysis, análisis, etc.). En este caso, la búsqueda correspondiente al cliente de escritorio de la aplicación de mensajería instantánea WhatsApp en macOS se realiza sobre aquellas fuentes de datos abiertas o semiabiertas disponibles, como puede ser la web del desarrollador (whatsapp.com), revistas de investigación digital (journals.elservier.com/digital-investigation; commons.erau.edu/jdfsl, etc.), foros técnicos (focusforensics.com; forensicswiki.com; incibe.com, etc.), investigadores independientes (dinosec.com/es/lab.html, etc.), ponencias técnicas (RootedCon, Blackhat, etc.), bibliotecas virtuales (http://biblioteca.uah.es, etc.) o en gestores de contenido (scholar.google.com, etc.).

Analizadas las diferentes fuentes de datos consultadas, se han encontrado diversos artículos en los cuales sus autores realizan el análisis forense estático de los artefactos generados por el cliente móvil de la aplicación de mensajería instantánea WhatsApp, si

bien, en el momento del estudio no se encuentra ningún tipo de información que pueda ser utilizada como apoyo al análisis forense del cliente de escritorio de esta aplicación para macOS.

En este caso, el estudio de fuentes abiertas realizado no podrá ser utilizado para identificar, decodificar, interpretar y validar la información obtenida en el estudio de artefactos.

5.4.2 Estudio de artefactos

El estudio de artefactos ha sido desarrollado a partir de los procedimientos descritos en el punto 3.3.2 de esta Tesis. Estos procedimientos permitirán identificar, decodificar e interpretar los rastros generados por el cliente de escritorio de la aplicación de IM WhatsApp para el sistema operativo macOS a partir del análisis comparativo registros.

Las especiales características que engloban al cliente de escritorio de la aplicación de IM WhatsApp para macOS, hace necesario combinar el análisis forense estático y dinámico de artefactos. A partir del análisis forense estático de artefactos se identificarán todos aquellos registros generados, modificados o eliminados por el cliente de escritorio de la aplicación de IM WhatsApp, siendo necesario el análisis forense dinámico para obtener la información en claro de las comunicaciones del usuario.

En los puntos sucesivos se desarrolla el estudio de artefactos realizado sobre del cliente de escritorio de la aplicación de IM WhatsApp en un sistema operativo macOS, suma del análisis de forense estático y dinámico de artefactos.

5.4.2.1 Análisis forense estático de artefactos

A continuación, se muestran los resultados obtenidos del análisis comparativo realizado sobre los rastros generados por el cliente de escritorio de la aplicación de IM WhatsApp en el sistema operativo macOS. Este ha sido elaborado a partir del análisis forense estático incluido en el estudio de artefactos de la metodología propuesta, el cual permite identificar, decodificar e interpretar los rastros generados por este cliente en este sistema operativo. La tabla 5.2 muestra, el listado artefactos generados por el cliente de escritorio de la aplicación de mensajería instantánea WhatsApp para macOS.

Tabla 5.2. Artefactos generados por el cliente de escritorio WhatsApp en macOS.

#	Contenido	Nombre de fichero	Carpeta	Descripción
1	Aplicación	WhatsApp.app	/Applications/	Ubicación de la instalación de la aplicación.
2	Configuración de aplicación	data.data, windows.plist, window_{N}.data	/Users/{USER}/Library/Saved Application State/WhatsApp.savedState	Archivos temporales de configuración de la aplicación.
3	Datos de conexión	SingletonCookie, SingletonLock y SS	/Users/{USER}/Library/Application Support/WhatsApp	Archivos temporales de enlace (link) de conexión.
4	Datos de usuario	Diferentes carpetas y ficheros.	/Users/{USER}/Library/Application Support/WhatsApp	Diferentes carpetas y archivos de usuario.
5	Multimedia	Diferentes archivos.	/Users/{USER}/Downloads (Por Defecto)	Diferentes ficheros multimedia descargados.

5.4.2.1.1 Análisis de los ficheros de datos de usuario

El análisis de los ficheros de datos de usuario se centra en el estudio del contenido de la carpeta "/Users/{USER}/Library/Application Support/WhatsApp" (fila 3 y 4, tabla 5.2). En el interior de esta carpeta se ubican, entre otros, los ficheros "SingletonCookie", "SingletonLock", "SS", "settings.json" y "Preferences", así como las carpetas con nombre "Cache", "database" o "Local Storage".

La figura 5.13 muestra a modo de ejemplo el listado de archivos y directorios que almacena la carpeta "/Users/{USER}/Library/Application Support/WhatsApp".

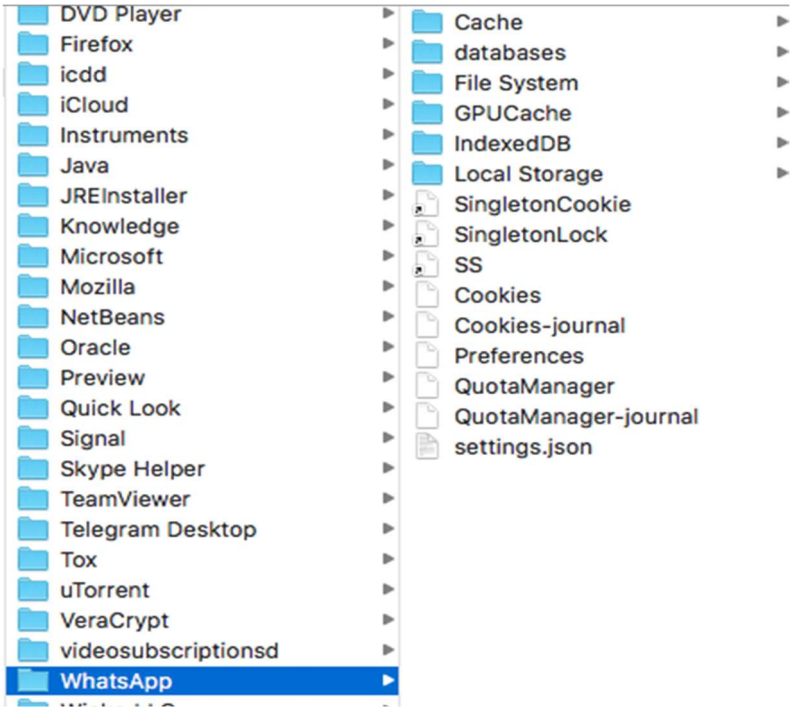


Figura 5.13. Ejemplo del contenido de la carpeta "/Users/{USER}/Library/Application Support/WhatsApp/".

Ubicados en la raíz del directorio "/Users/{USER}/Library/Application Support/WhatsApp/", como muestra la figura 5.13, se identifican los ficheros con nombre "SingletonCookie", "SingletonLock" y "SS" (fila 3, tabla 5.2). Estos ficheros de enlace son creados en el sistema macOS cuando el usuario se identifica por primera vez con el cliente de escritorio de la aplicación de IM WhatsApp. Los archivos "SingletonCookie" y "SingletonLock" contienen información relativa al dispositivo informático en el cual se ejecuta el cliente de escritorio de la aplicación de IM WhatsApp, y el archivo "SS" contiene información relativa a la conexión realizada por este cliente de escritorio. Estos tres archivos de enlace identifican de manera única la conexión del cliente de escritorio de la aplicación de IM WhatsApp a través de un dispositivo informático. Estos ficheros almacenan una estructura fija de cuatro registros. El primer registro siempre contiene el literal "XSym", el segundo registro es un valor numérico, el tercero registro es un valor alfanumérico que corresponde con valor de aplicar la función matemática MD5 al cuarto registro y el cuarto contiene un literal que depende del fichero.

Las figuras 5.14, 5.15 y 5.16 muestran a modo de ejemplo el contenido de los ficheros "SingletonCookie", "SingletonLock" y "SS" ubicados en el directorio "/Users/{USER}/Library/Application Support/WhatsApp/".

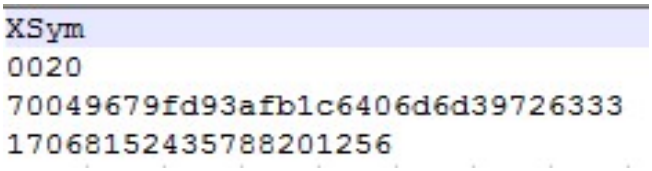


Figura 5.14. Ejemplo contenido fichero "SingletonCookie".

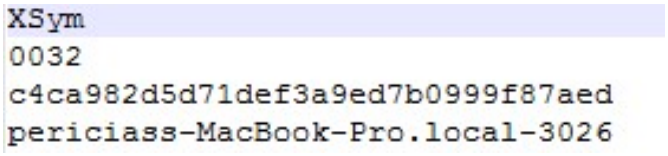


Figura 5.15. Ejemplo contenido fichero "SingletonLock".

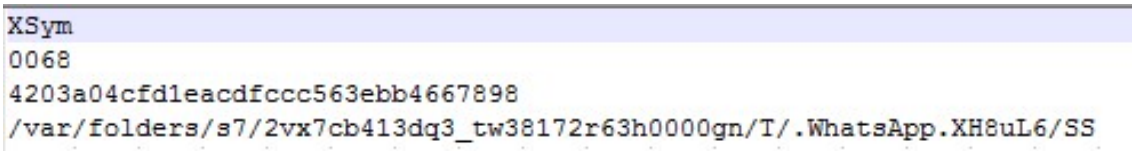


Figura 5.16. Ejemplo contenido fichero "SS".

De igual manera, cabe comentar que en la raíz del directorio "/Users/{USER} /Library/Application Support/WhatsApp" se encuentran los ficheros con nombre "settings.json" y "Preferences", los cuales contienen información relativa con la configuración de la aplicación y del dispositivo informático (ubicación y tamaño de la ventana de aplicación, carpeta de descarga, etc.).

Ubicados en la raíz del directorio "/Users/{USER}/Library/Application Support/WhatsApp/Cache", como muestra la figura 5.17, se almacenan diversos archivos, diferenciando entre los ficheros cuyo nombre está formado por "data_"{NUMERO} y aquellos ficheros cuyo nombre está formado por "f_"{VALOR}.

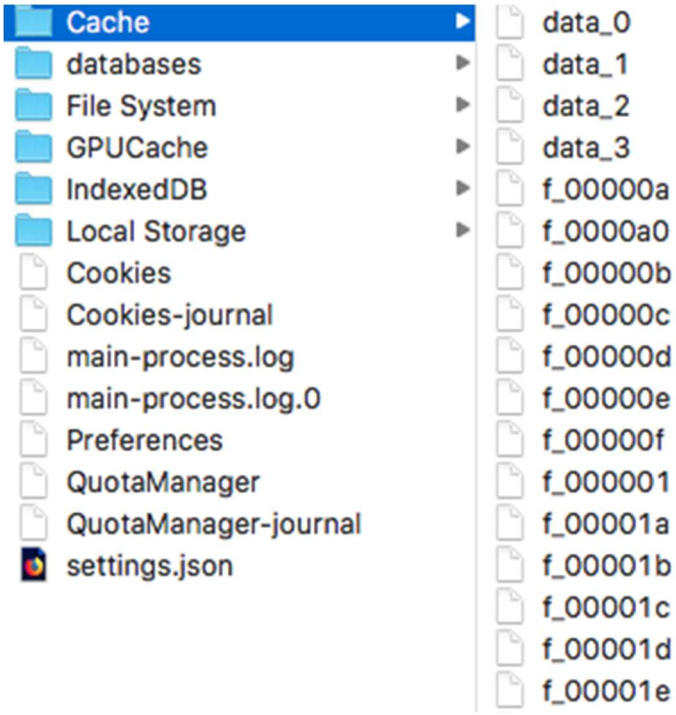


Figura 5.17. Contenido carpeta "/Users/{USER}/Library/Application Support/WhatsApp/Cache".

Analizado el contenido de los diferentes ficheros de datos expuestos anteriormente al objeto de conocer el contenido de los mismos, se observa que todos los archivos cuyo nombre sigue el esquema "data_"{NUMERO}, ubicados en la carpeta "/Users/{USER}/Library/Application Support/WhatsApp/Cache", tienen en común que el inicio del fichero corresponde con el valor hexadecimal "C3CA04C100000200". La figura 5.18 muestra a modo de ejemplo el inicio y parte del contenido del fichero cuyo nombre está formado por "data_"{NUMERO}, en el cual se identifica el valor hexadecimal indicado.

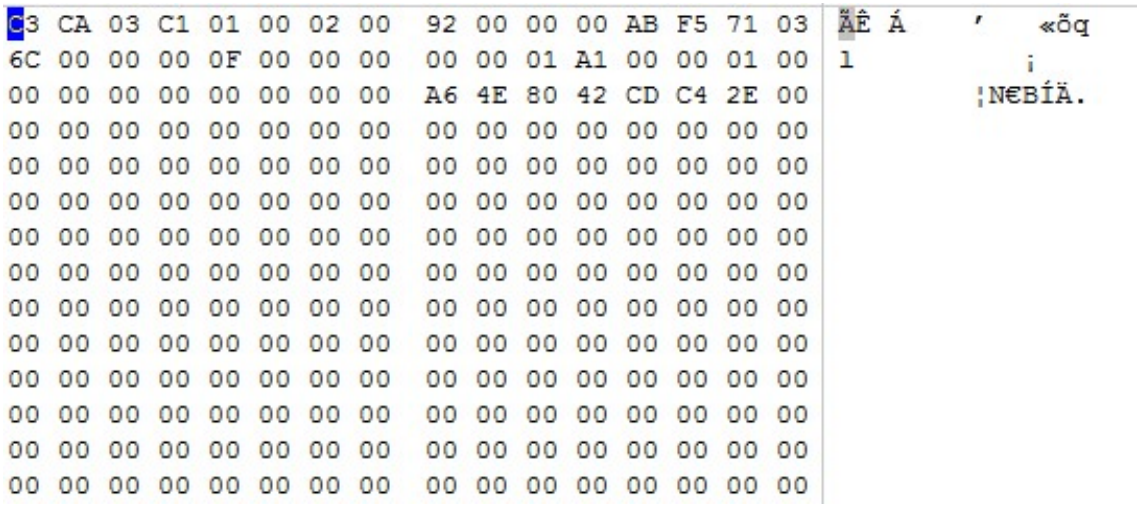


Figura 5.18. Inicio hexadecimal de los ficheros con nombre "data_"{NUMERO}.

Estos ficheros "data_"{NUMERO} contienen diversa información relacionada con las conversaciones o *chats* de la aplicación. Del análisis realizado sobre estos ficheros "data_"{NUMERO}, se observa como los ficheros con nombre "data_1" y "data_2" contienen información que puede resultar de gran utilidad en el análisis del cliente de escritorio de la aplicación de IM WhatsApp en macOS. El archivo "data_1" contiene información sobre los números de teléfono incluidos en los diferentes conversaciones o *chats* mantenidos a través del cliente de escritorio de la aplicación de IM WhatsApp en macOS.

La figura 5.19 muestra a modo de ejemplo, tres registros contenidos en el fichero "data_1". En esta figura se puede identificar a simple vista el número de contacto del creador de un grupo y la fecha de creación "349???????7-1494959928@g.us" (formato: numerotelefonico-fechadecreaciondelgrupo@g.us) incluidos en una conversación de grupo, así como el número de contacto "3463??????0@c.us" (formato: numerotelefonico@c.us) incluido en una conversación personal.

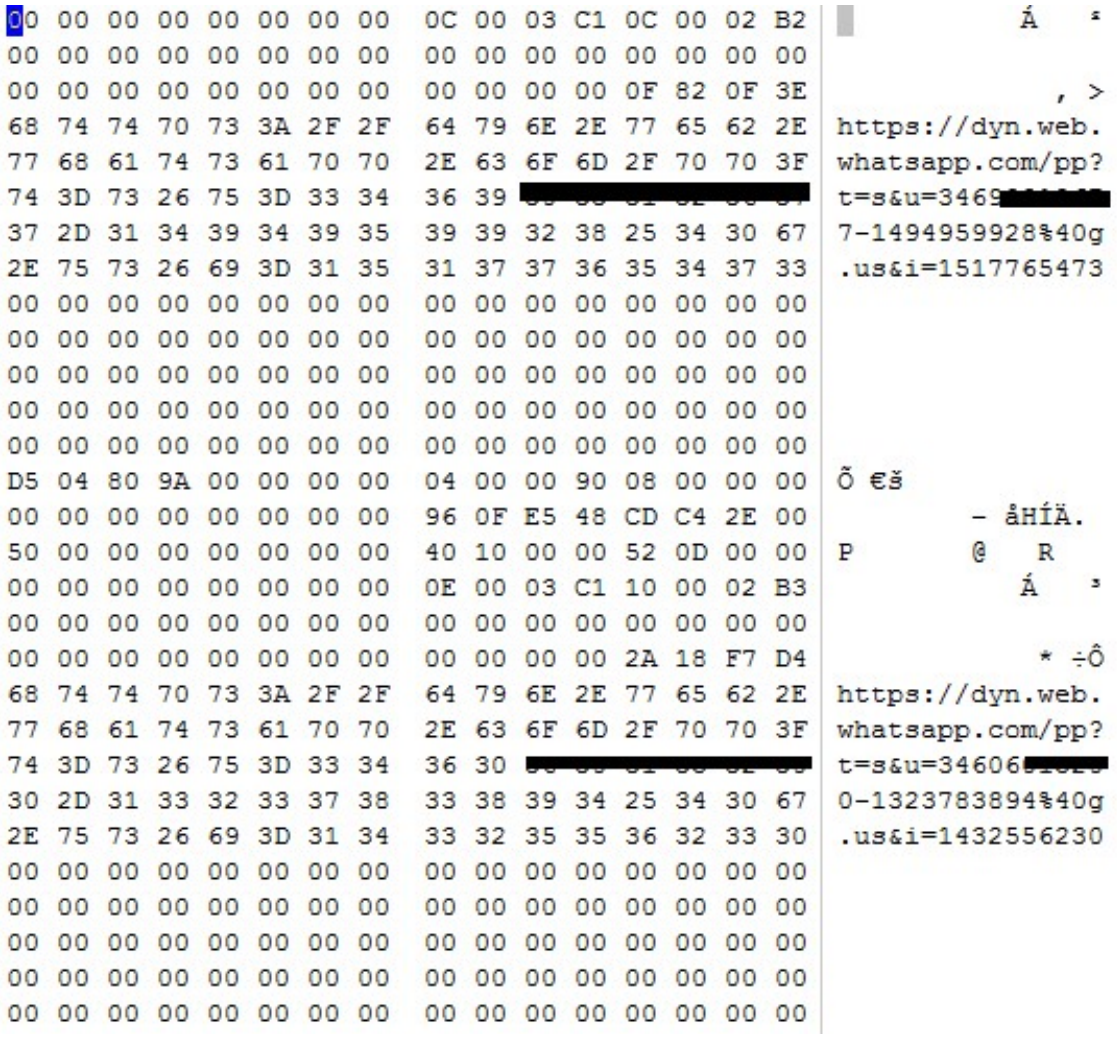


Figura 5.19. Ejemplo contenido parcial del fichero “data_1”.

El archivo “data_2” contiene las imágenes de perfil relativas a los diferentes conversaciones o *chats* mantenidos a través del cliente de escritorio de la aplicación de IM WhatsApp en macOS. Las mismas pueden ser extraídas del interior del fichero “data_2” realizando técnicas de recuperación de datos (*datacarving)*.

La figura 5.20 muestra a modo de ejemplo, parte del contenido en el fichero “data_2” en la cual se puede identificar la cabecera hexadecimal de un fichero de imagen.

```
FF D8 FF E0 00 10 4A 46  49 46 00 01 02 00 00 01  ÿØÿà  JFIF
00 01 00 00 FF ED 00 84  50 68 6F 74 6F 73 68 6F      ÿí „Photosho
70 20 33 2E 30 00 38 42  49 4D 04 04 00 00 00 00  p 3.0 8BIM
00 67 1C 02 28 00 62 46  42 4D 44 30 31 30 30 30   g   ( bFBMD01000
61 38 38 30 31 30 30 30  30 36 37 30 32 30 30 30  a880100006702000
30 65 37 30 33 30 30 30  30 34 62 30 34 30 30 30  0e70300004b04000
30 63 65 30 34 30 30 30  30 61 31 30 36 30 30 30  0ce040000a106000
30 38 30 30 38 30 30 30  30 63 35 30 38 30 30 30  080080000c508000
30 32 31 30 39 30 30 30  30 39 30 30 39 30 30 30  0210900009009000
30 37 65 30 63 30 30 30  30 00 FF DB 00 43 00 06  07e0c0000 ÿÛ C
04 05 06 05 04 06 06 05  06 07 07 06 08 0A 10 0A
0A 09 09 0A 14 0E 0F 0C  10 17 14 18 18 17 14 16
16 1A 1D 25 1F 1A 1B 23  1C 16 16 20 2C 20 23 26     %   #    , #&
27 29 2A 29 19 1F 2D 30  2D 28 30 25 28 29 28 FF  ')*)  -0-(0%()(ÿ
DB 00 43 01 07 07 07 0A  08 0A 13 0A 0A 13 28 1A  Û C           (
```

Figura 5.20. Ejemplo contenido parcial fichero “data_2”.

La figura 5.21 muestra el resultado de aplicar las técnicas de recuperación de datos (*datacarving)* sobre del fichero “data_2” (inicio de imagen o cabecera hexadecimal: “FFD8FFE0” / final de imagen o pie hexadecimal: “EE7FFFD9”). En esta imagen se muestra la imagen de perfil extraída del fichero “data_2” correspondiente a un chat de grupo.

Figura 5.21. Imagen perfil de grupo. Fichero de imagen extraído del fichero “data_2”.

Cabe mencionar que si bien se pueden extraer del fichero “data_2” las imágenes de perfil de las conversaciones o *chats*, no se ha encontrado información que relacione esta imagen de perfil con su correspondiente nombre, creador o cualquier otro tipo de datos del *chat*.

De igual modo, analizado el contenido de los diferentes ficheros de datos expuestos anteriormente al objeto de conocer el contenido de los mismos, se observa que todos los archivos con nombre “f_”{VALOR} ubicados en la carpeta “/Users/{USER}/Library/Application Support/WhatsApp/Cache”, no disponen de una cabecera o inicio de fichero común. Así mismo del análisis realizado sobre la información contenida en su interior de este tipo de ficheros se desprende que el mismo es ilegible.

La figura 5.22 muestra a modo de ejemplo el inicio y parte del contenido del fichero “f_000068”, en cual se puede observar como los datos almacenados en el mismo son ilegibles.

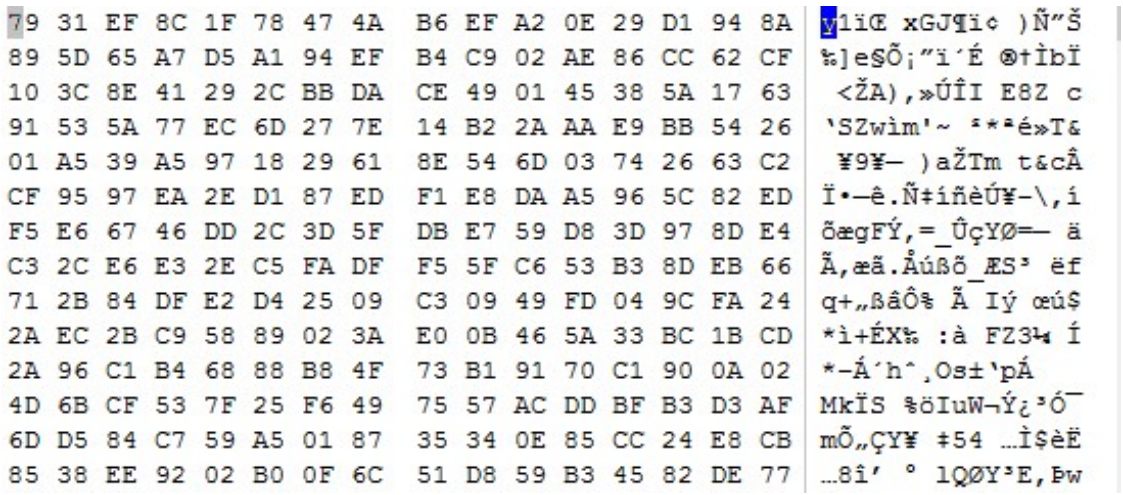
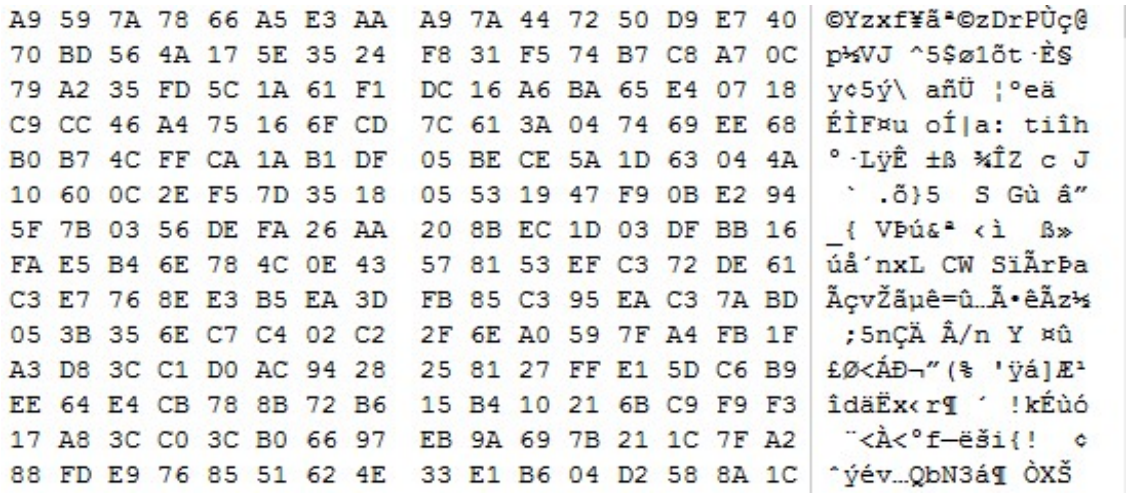


Figura 5.22. Inicio del fichero “f_000068”.

Así mismo, la figura 5.23 muestra parte del contenido del fichero “f_000036”, el cual se observa que los datos almacenados en el mismo son ilegibles.



```
A9 59 7A 78 66 A5 E3 AA  A9 7A 44 72 50 D9 E7 40  ©Yzxf¥ãª©zDrPÙç@
70 BD 56 4A 17 5E 35 24  F8 31 F5 74 B7 C8 A7 0C  p½VJ ^5$ø1õt·È§
79 A2 35 FD 5C 1A 61 F1  DC 16 A6 BA 65 E4 07 18  y¢5ý\ añÜ ¦ºeä
C9 CC 46 A4 75 16 6F CD  7C 61 3A 04 74 69 EE 68  ÉÌF¤u oÍ|a: tiîh
B0 B7 4C FF CA 1A B1 DF  05 BE CE 5A 1D 63 04 4A  °·LÿÊ ±ß ¾ÎZ c J
10 60 0C 2E F5 7D 35 18  05 53 19 47 F9 0B E2 94  ` .õ}5  S Gù â”
5F 7B 03 56 DE FA 26 AA  20 8B EC 1D 03 DF BB 16  _{ VÞú&ª ‹ì  ß»
FA E5 B4 6E 78 4C 0E 43  57 81 53 EF C3 72 DE 61  úå´nxL CW SïÃrÞa
C3 E7 76 8E E3 B5 EA 3D  FB 85 C3 95 EA C3 7A BD  ÃçvŽãµê=û…Ã•êÃz½
05 3B 35 6E C7 C4 02 C2  2F 6E A0 59 7F A4 FB 1F  ;5nÇÄ Â/n Y ¤û
A3 D8 3C C1 D0 AC 94 28  25 81 27 FF E1 5D C6 B9  £Ø<ÁÐ¬”(% 'ÿá]Æ¹
EE 64 E4 CB 78 8B 72 B6  15 B4 10 21 6B C9 F9 F3  îdäËx‹r¶ ´ !kÉùó
17 A8 3C C0 3C B0 66 97  EB 9A 69 7B 21 1C 7F A2  ¨<À<°f—ëši{!  ¢
88 FD E9 76 85 51 62 4E  33 E1 B6 04 D2 58 8A 1C  ˆýév…QbN3á¶ ÒXŠ
```

Figura 5.23. Inicio del fichero “f_000036”.

Del análisis forense estático realizado se desprende que, si bien el contenido de los archivos de datos con nombre “f_”{VALOR} ubicados en la carpeta “/Users/{USER}/Library/Application Support/WhatsApp/Cache” se encuentran cifrados, se puede inferir que estos ficheros corresponden con los mensajes de las diferentes conversaciones que el usuario de la aplicación. Igualmente, del análisis forense estático realizado se desprende que de los ficheros con nombre “data_”{NUMERO} ubicados en la carpeta “/Users/{USER}/Library/Application Support/WhatsApp/Cache”, se puede extraer información que puede ser de utilidad para el análisis forense, si bien, no se pueden obtener las conversaciones mantenidas por el usuario a través del cliente de escritorio de la aplicación de mensajería instantánea WhatsApp en macOS.

5.4.2.2 Análisis forense dinámico de artefactos

El análisis forense dinámico de artefactos, parte de las conclusiones obtenidas del estudio realizado en el análisis forense estático sobre el cliente de escritorio de la aplicación de mensajería instantánea WhatsApp en el sistema operativo macOS. Identificados los artefactos generados a partir del análisis forense estático se procede al análisis forense dinámico utilizando el método de copia forense expuesto en el punto 3.3.2 de esta Tesis. El método de copia forense permitirá simular el entorno original de manera controlada, permitiendo el análisis y obtención de las comunicaciones de usuario mantenidas a partir del cliente de escritorio de la aplicación de IM WhatsApp en macOS.

A continuación, se expone de manera práctica como se obtienen las comunicaciones mantenidas por el cliente de escritorio de la aplicación de IM WhatsApp en macOS a partir de la combinación del análisis forense estático y dinámico de artefactos.

5.4.2.2.1 Identificación de artefactos

A partir del análisis forense estático de artefactos se identifica toda aquella información relacionada tanto con el cliente de escritorio de la aplicación de mensajería instantánea como con los datos del usuario. En este caso práctico, el análisis forense estático de artefactos se realiza sobre todos aquellos registros que el cliente de escritorio de la aplicación de mensajería instantánea WhatsApp genera en un ordenador de la marca "Apple" modelo "MacBook Pro" con sistema operativo "macOS High Sierra" (v12.13).

- La adquisición forense y generación de imagen forense se realiza a través de un "*liveCD*" con la distribución forense "DEFT Zero". Para poder realizar este tipo de adquisición se debe tener en cuenta que sistema de cifrado "*FileVault*" no se encuentre activo.
- El tratamiento de la imagen forense se realiza en un entorno forense controlado con sistema operativo macOS. Esto debe ser así, ya que, en el momento de la realización de este estudio técnico-forense, las principales soluciones forenses comerciales no soportaban el sistema de archivos de Apple (APFS). La imagen forense resultante de la adquisición será analizada a través las aplicaciones nativas "DiskImageMounter.app" y "Finder.app" del entorno forense controlado con macOS.

La figura 5.24 muestra como a partir de la aplicación nativa "Finder.app" del entorno forense controlado se pueden visualizar el contenido de la imagen forense "image_27_09_2017.dmg". En esta figura se identifica el contenido de la carpeta "/Users/{USER}/Library/Application Support/WhatsApp/" del ordenador original.

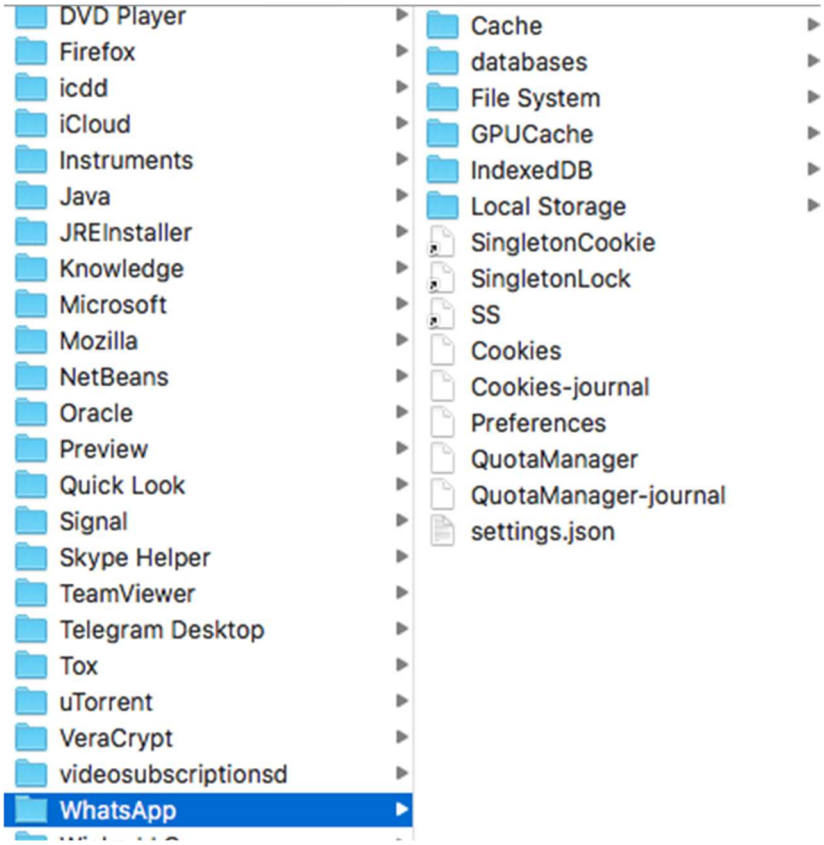


Figura 5.24. Contenido de la carpeta "/Users/{USER}/Library/Application Support/WhatsApp/".

Localizados estos directorios y archivos relativos al cliente de escritorio de la aplicación de IM WhatsApp en la imagen forense con nombre "image_27_09_2017.dmg" realizada sobre el ordenador original, basta con realizar una copia forense de los datos de usuario ("/Users/{USER}/Library/Application Support/WhatsApp/") en el entorno forense controlado con macOS. En este caso, como se expondrá posteriormente no es necesario realizar la copia forense de los datos de la aplicación ("/Applications/WhatsApp.app").

5.4.2.2.2 Obtención de información

A continuación, se detalla el procedimiento a partir del cual se obtienen las conversaciones mantenidas a través del cliente de escritorio de la aplicación de IM WhatsApp, centrando este en los conceptos técnicos sin entrar en los aspectos legales necesarios. El proceso expone como se realiza el análisis forense dinámico de los artefactos a partir de la copia forense realizada en el punto anterior.

- La copia forense de los datos incluidos en la imagen forense resultante de la adquisición realizada del ordenador original ("image_27_09_2017.dmg") será realizada a través de las aplicaciones nativas del entorno forense controlado. En el caso del cliente de escritorio de la aplicación de IM WhatsApp, se realizará la copia forense de los datos relativos al usuario ("/Users/{USER}/Library/Application Support/WhatsApp/").

Se realiza la copia forense de los datos de usuario ("Users/{USER}/Library/Application Support/WhatsApp/") incluidos en la imagen forense con nombre "image_27_09_2017.dmg" en el entorno forense controlado, creándose el directorio "/Users/{FORENSIC_USER}/Library/Application Support/WhatsApp/" en el entorno forense controlado. En el caso del cliente de escritorio de la aplicación de mensajería instantánea WhatsApp para macOS, no es necesario realizar la copia forense de los datos relativos a la aplicación ("/Applications/WhatsApp.app"), basta con instalar la aplicación WhatsApp o ejecutarla desde el instalador.

La figura 5.25 muestra el contenido del fichero instalador "WhatsApp.dmg" desde el cual se puede ejecutar el cliente de escritorio WhatsApp o instalarlo bajo la carpeta "/Applications" del entorno forense controlado.

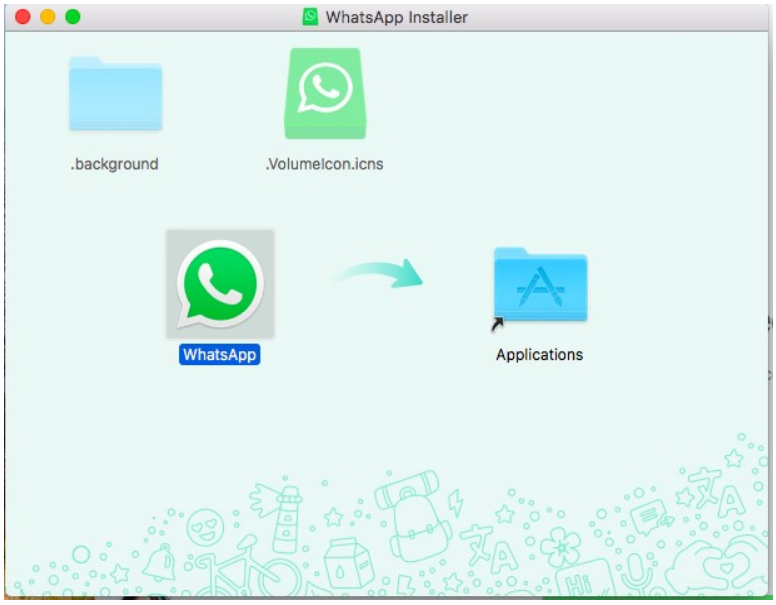


Figura 5.25. Instalador del cliente de escritorio WhatsApp. Archivo WhatsApp.dmg.

Si se ejecuta la aplicación "WhatsApp.app" desde el instalador de la aplicación "WhatsApp.dmg" con la copia forense de los datos del usuario ("Users/{USER}/Library/Application Support/WhatsApp/") en el entorno forense controlado ("/Users/{FORENSIC_USER}/Library/Application Support/WhatsApp/"), basta con habilitar el acceso a una conexión de datos en el entorno forense controlado para obtener las conversaciones del usuario.

La figura 5.26 muestra, la ejecución del cliente de escritorio de la aplicación de IM WhatsApp en el entorno forense controlado con conexión a Internet. En esta figura se identifican de manera se obtienen de manera clara las conversaciones del usuario.

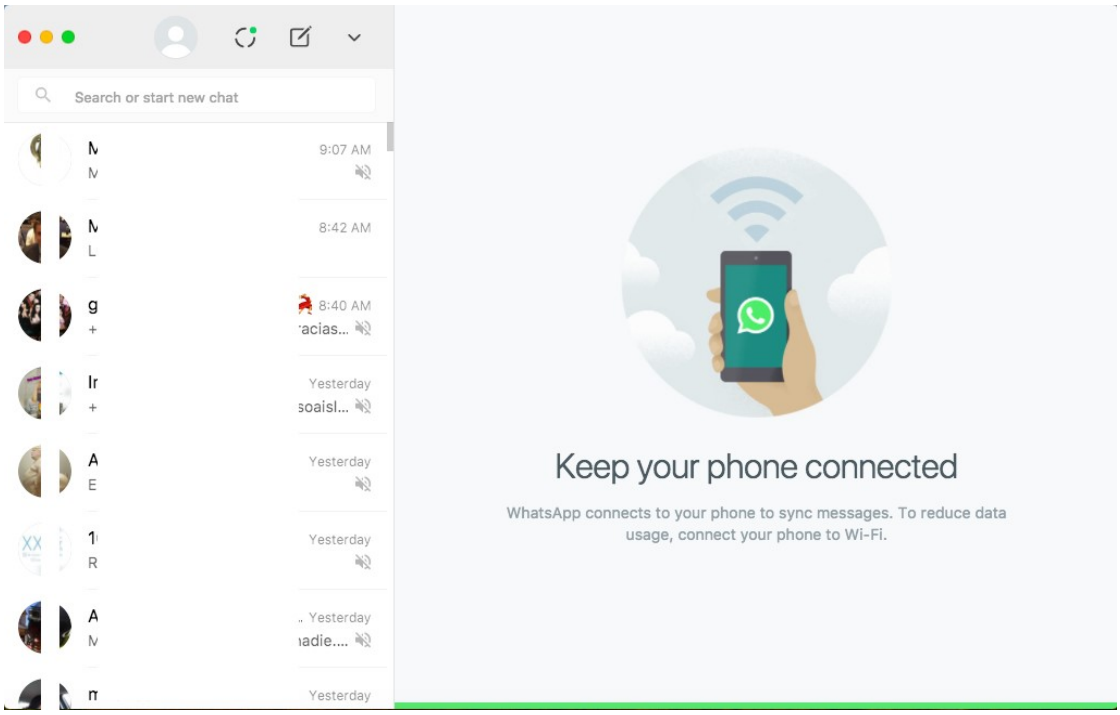


Figura 5.26. Conversaciones del cliente de escritorio WhatsApp. Entorno forense controlado.

Al ejecutar el cliente de escritorio a través del instalador de la aplicación de IM WhatsApp, se generan en el interior de la carpeta "/Users/{FORENSIC_USER}/Library/Application Support/WhatsApp/" del entorno forense controlado los archivos de conexión "SingletonCookie", "SingletonLock" y "SS". Estos ficheros contienen la información relativa al entorno forense controlado,

siendo el contenido de estos ficheros, diferentes al de los ficheros ubicados en la carpeta "/Users/{USER}/Library/Application Support/WhatsApp/" del dispositivo informático origen.

Es de mencionar que el proceso para la obtención de las conversaciones de usuario del cliente de escritorio de la aplicación de mensajería instantánea WhatsApp para macOS tiene diversas singularidades.

- Primera; para que el proceso se realice con éxito es necesario que el teléfono inteligente vinculado con la cuenta de la aplicación de IM WhatsApp disponga de conexión a Internet, si no, no es posible recuperar las conversaciones.
- Segunda; al realizar este proceso, en el teléfono inteligente vinculado con la cuenta de la aplicación de mensajería instantánea WhatsApp se mostrará una notificación, tal y como se muestra en la figura 5.27. Esta notificación informa a su usuario de la existencia de una conexión desde un cliente no móvil (escritorio o web).

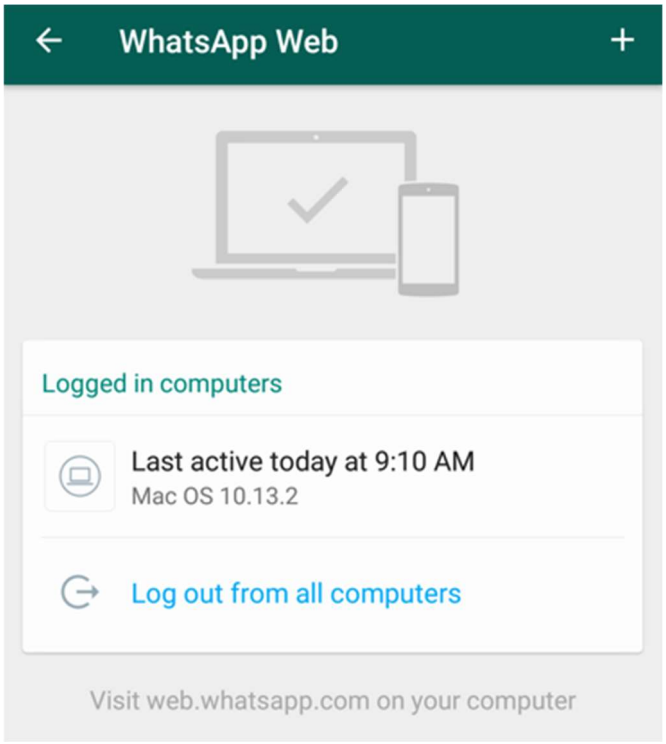


Figura 5.27. Notificación de acceso a través del cliente de escritorio WhatsApp.

5.4.3 Estudio de código fuente

El estudio de código fuente ha sido desarrollado a partir de los procedimientos descritos en el punto 3.3.3 de esta Tesis. Estos procedimientos permitirán identificar e interpretar los registros generados por el cliente de escritorio en cuestión a partir del análisis de código fuente.

En el caso del cliente de escritorio de la aplicación de mensajería instantánea WhatsApp para el sistema operativo macOS, el desarrollador de la aplicación no proporciona el código fuente, limitando el análisis de las líneas de código fuente a los datos obtenidos de aplicar el proceso de ingeniería inversa sobre la propia aplicación. Este se realiza sobre el cliente de escritorio al objeto de identificar entre las múltiples líneas de código fuente (definiciones, funciones, variables etc.), aquella información no obtenida en el estudio de fuentes abiertas y estudio de artefactos.

La figura 5.28 muestra a modo de ejemplo, el listado de funciones que pueden encontrase en el código fuente del cliente de escritorio de la aplicación de IM WhatsApp en macOS. Este listado de funciones es proporcionado por la aplicación IDA Free del análisis realizado sobre el fichero "/Applications/WhatsApp.app/Contents/Frameworks/Electron Framework/Version/A/Electron Framework" incluido en el cliente de escritorio de la aplicación de IM WhatsApp en macOS.

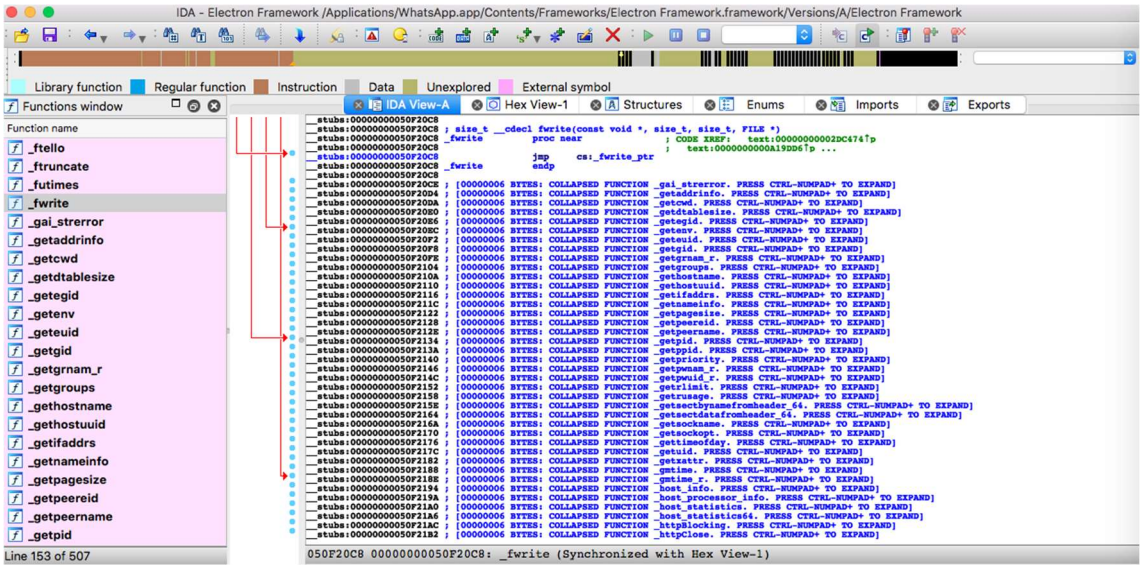


Figura 5.28. Definición de función "_fwrite". Fichero "Electron Framework".

De igual manera, la figura 5.29 muestra a modo de ejemplo, el resultado de realizar una búsqueda de la cadena de texto “Singleton” a través de la aplicación “IDA Free”, sobre el contenido del cliente de escritorio de la aplicación de IM WhatsApp en macOS.

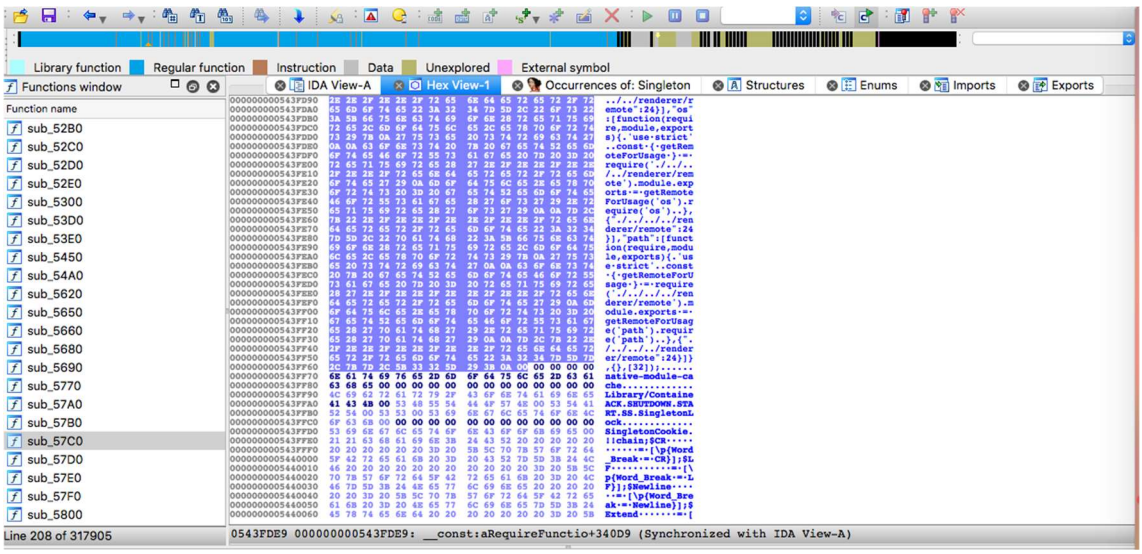


Figura 5.29. Resultado de la búsqueda de la cadena “Singleton”. Fichero “Electron Framework”.

La ingeniería inversa realizada sobre el código fuente del cliente de escritorio de la aplicación de IM WhatsApp para macOS proporciona una visión más detallada con relación al funcionamiento de la aplicación, si bien, al igual que sucede en el análisis de fuentes abiertas y análisis forense estático de artefactos, tras el análisis realizado del código fuente de la aplicación, se comprueba que no se puede obtener el contenido de los mensajes de usuario al encontrarse cifrados.

5.4.4 Resultados del análisis realizado

La metodología de análisis forense propuesta en la presente tesis (suma de los estudios de fuentes abiertas, estudio de artefactos y estudio de código fuente) utilizada en el desarrollo del estudio técnico-forense del cliente de escritorio de la aplicación de IM WhatsApp para el sistema operativo macOS desprende que:

a) Del estudio de las fuentes abiertas correspondiente con la búsqueda de toda aquella información funcional, técnica y forense que pudiera encontrarse en cualquier fuente de datos abiertas o semiabiertas en el momento del estudio se comprueba que, no existe ninguna fuente de datos que aporte información relativa al cliente de escritorio de la aplicación de IM WhatsApp para macOS que pueda ser utilizada en el análisis forense de la aplicación.

b) El estudio de los artefactos infiere que este estudio debe ser desarrollado a partir de la suma del análisis forense estático y dinámico de artefactos.

   - Del análisis forense estático de los rastros generados por el cliente de escritorio de la aplicación de IM WhatsApp se identifican las diferentes carpetas y ficheros que se generan, modifican y eliminan en el ordenador con macOS, tanto a nivel de la aplicación como a nivel de las comunicaciones de usuario. Analizados estos ficheros de datos al objeto de obtener la información relativa a las comunicaciones, se concluye que los mismos se almacenan de forma cifrada, no pudiéndose obtener la información contenida en los mismos.

   - Del análisis forense dinámico, producto de aplicar el método de copia forense sobre los datos originales de la aplicación y usuario, e incluirlos en un entorno forense controlado imitando de esta forma el dispositivo original, se obtiene como resultado las conversaciones relativas a las comunicaciones mantenidas por el usuario del cliente de escritorio de la aplicación de IM WhatsApp en macOS.

c) Del estudio del código fuente correspondiente al análisis de las líneas de código

obtenidas de realizar el proceso de ingeniería inversa sobre cliente de escritorio de la aplicación WhatsApp para macOS se concluye que, del mismo se pueden obtener datos que apoyen y clarifiquen la información obtenida del estudio de fuentes abiertas y del estudio estático de artefactos, si bien, ya que el propio desarrollador de la aplicación no proporciona el código fuente para ninguno de sus clientes, el estudio que pueda ser realizado de las líneas del código fuente se limita a la información que se pueda obtener del proceso de ingeniería inversa.

Tal y como ha quedado demostrado, la metodología de análisis forense propuesta permite identificar, interpretar y obtener la información generada por el cliente de escritorio de la aplicación de mensajería instantánea WhatsApp en el sistema operativo macOS.

5.5 Comparativa de los resultados obtenidos. Telegram Messenger y WhatsApp en macOS

A continuación, se muestra los resultados obtenidos de los estudios técnico-forenses realizados sobre los clientes de escritorio de las aplicaciones de mensajería instantánea Telegram Messenger y WhatsApp para el sistema operativo macOS. Estos serán expuestos comparando el resultado obtenido de aplicar la metodología de análisis forense propuesta en la presente tesis.

Estudio de fuentes abiertas.

Del estudio de fuentes abiertas correspondiente al análisis de toda fuente de datos que pudiera contener información funcional, técnica o forense, y que pudiera ser utilizada para apoyar el análisis forense de los clientes de escritorio de las aplicaciones de IM Telegram Messenger y WhatsApp para el sistema operativo macOS, se concluye que con relación al cliente de escritorio de la aplicación de IM Telegram Messenger se encuentran diversas fuentes de datos. Estas fuentes son analizadas siendo las mismas utilizadas como apoyo en el análisis forense del citado cliente. Caso contrario ocurre el estudio de fuentes abiertas realizado sobre el cliente de escritorio de la aplicación de IM WhatsApp para macOS, del cual no se obtiene ningún tipo de información que pudiera ser utilizada en el análisis forense de este cliente.

Estudio de artefactos.

Del estudio de los artefactos suma del análisis forense estático y dinámico de artefactos se concluye que:

Análisis forense estático de los artefactos.

De este análisis se obtienen como resultado los diferentes rastros o registros que generan los clientes de escritorio de las aplicaciones de IM Telegram Messenger y WhatsApp sobre el sistema operativo macOS. A través del análisis de los rastros, se

identifican las carpetas y ficheros utilizados por estos clientes de escritorio con el fin de guardar los datos tanto de la aplicación como del usuario.

La tabla 5.3 expone de manera comparativa el listado de artefactos el cliente de escritorio de las aplicaciones de IM Telegram Messenger y WhatsApp para el sistema operativo macOS.

Tabla 5.3. Lista de artefactos aplicación Telegram Messenger y WhatsApp en macOS.

#	Contenido	Artefactos Telegram Messenger	Artefactos WhatsApp	Descripción
1	Aplicación	/ Applications/Telegram.app	/ Applications/WhatsApp.app	Datos de la aplicación.
2	Datos de Log	Log.txt	-	Registro de eventos.
3	Datos de usuario	/Users/{USER}/Library/Application Support/Telegram Desktop/tdata/	/Users/{USER}/Library/Application Support/WhatsApp/	Diferentes archivos de usuario. Datos encriptados.
4	Datos temporales y de configuración	data.data, windows.plist, window_1.data	data.data, windows.plist, window_{N}.data	Ficheros temporales de configuración.
5	Archivos	/Users/{USER}/Downloads/ (*.mp4, *.jpg, *.pdf, etc.).	/Users/{USER}/Downloads/ (*.mp4, *.jpg, *.pdf, etc.).	Archivos descargados.
6	Conexión (Socket)	7852aa807d0e61276974ee878396a1c4-{87A94AB0-E370-4cde-98D3-ACC110C5967D}	SingletonCookie, SingletonLock y SS	Información sobre conexión.

Con respecto a los datos de usuario, el estudio estático de artefactos es utilizado al objeto de identificar, decodificar e interpretar la información relativa a las comunicaciones de usuario. Del estudio estático de artefactos se desprende que esta información se almacena de manera distinta en función del sistema operativo.

El cliente de escritorio de aplicación de IM Telegram Messenger almacena los datos relativos a las comunicaciones de usuario en el interior de la carpeta "D877F783D5D3EF8C", ubicada bajo el directorio "/Users/{USER}/Library/Application Support/Telegram Desktop/tdata/" (fila 3, tabla 5.3). Dentro de esta carpeta "D877F783D5D3EF8C" se encuentran un numero diverso de ficheros cuyo formato de nombre responde con un valor alfanumérico de 16 caracteres alfanuméricos. Estos ficheros disponen de un inicio de fichero común (0x54444624), si bien el resto de la información almacenada en estos es ilegible. De igual modo, el cliente de escritorio de la aplicación de IM WhatsApp almacena los datos de las comunicaciones de usuario en cuatro ficheros "/Users/{USER}/Library/Application Support/WhatsApp/Cache" (fila 3, tabla 5.3). Dentro de esta carpeta se encuentran un numero diverso de ficheros cuyo nombre sigue el esquema "f"{VALOR}. Estos ficheros,

al contrario que sucede con el cliente de escritorio de Telegram Messenger, no disponen de un inicio de fichero común, siendo ilegible toda la información almacenada en los mismos.

La figura 5.30 muestra a modo de ejemplo el inicio y parte del contenido del fichero "5746EA104E9431590" ubicado en la carpeta "/Users/{USER}/Library/Application Support/Telegram Desktop/tdata/D877F783D5D3EF8C" el cual almacenan parte de las comunicaciones mantenidas por el usuario en el cliente de escritorio de la aplicación de IM Telegram Messenger en macOS.

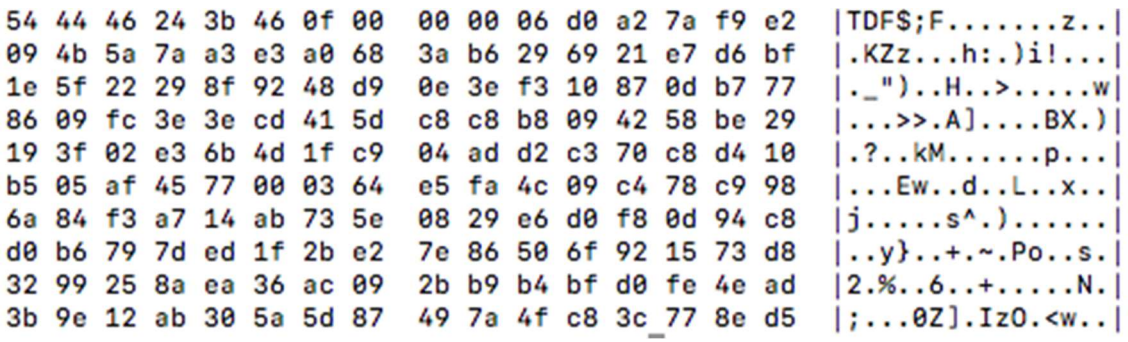


Figura 5.30. Ejemplo fichero "5746EA104E9431590". Cliente de escritorio Telegram Messenger.

Así mismo, la figura 5.31 muestra a modo de ejemplo el inicio y parte del contenido del fichero de datos "f_000068" ubicado en la carpeta "/Users/{USER}/Library/Application Support/WhatsApp/Cache" el cual almacena parte de las comunicaciones mantenidas por el usuario a través del cliente de escritorio de la aplicación de IM WhatsApp en macOS.

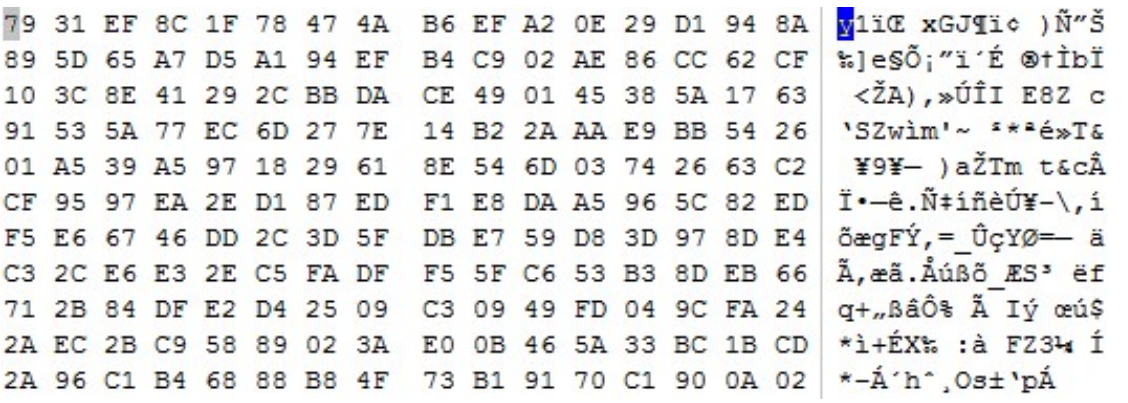


Figura 5.31.Ejemplo fichero "f_000068". Cliente de escritorio WhatsApp.

Del análisis forense estático de artefactos realizado sobre los clientes de escritorio, de las aplicaciones de mensajería instantánea Telegram Messenger y WhatsApp para macOS se concluye que la información relativa a las comunicaciones de usuario no puede ser obtenidas al ser almacenada ésta en un formato ilegible, si bien, en el caso del cliente de escritorio de la aplicación de IM WhatsApp es posible obtener de los ficheros con formato de nombre "data_"{NUMERO} ubicados en la carpeta "/Users/{USER}/Library/Application Support/WhatsApp/Cache" información relativa a las conversaciones o chats (números de teléfono, fechas de creación de grupos o imágenes de perfil de los chats).

Análisis forense estático. Resultado soluciones forenses comerciales.

Al objeto de comprobar el resultado obtenido del análisis forense estático realizado sobre los clientes de escritorio de las aplicaciones de IM Telegram Messenger y WhatsApp en el sistema operativo macOS, éste es comparado con el arrojado por varias de las principales soluciones forenses comerciales. En este caso, se utilizan las soluciones forenses comerciales Belkasoft Evidence Center (v8.5.2273 - trial versión) e Internet Evidence Finder (v6.12.0.7538), las cuales serán ejecutadas bajo un entorno forense con sistema operativo Windows. Ambas soluciones forenses son ampliamente conocidas y utilizadas en la comunidad forense para el análisis forense estático de artefactos tanto de dispositivos informáticos como móviles.

La solución comercial forense Belkasoft Evidence Center (BEC) identifica las diferentes particiones incluidas en el sistema operativo macOS, si bien, tal y como se observa en la figura 5.32, esta solución no reconoce el sistema de archivos de Apple (APFS) correspondiente con la segunda posición "Partition: Allocated, vol_409640_234031968".

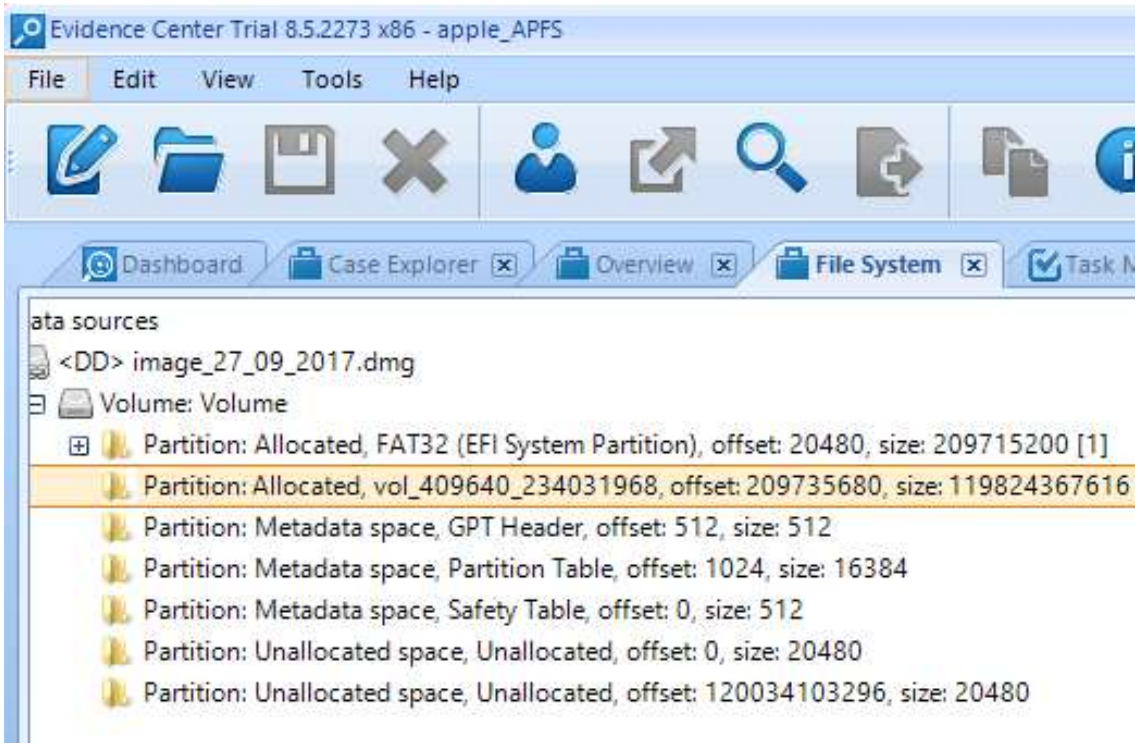


Figura 5.32. Identificación de sistemas de archivos de la solución forense BEC.

Entre el listado de las aplicaciones de mensajería soportadas por la solución forense comercial Belkasoft Evidence Center para el sistema operativo macOS, no se encuentran los clientes de escritorio de las aplicaciones de IM Telegram Messenger ni WhatsApp. La figura 5.33 muestra a modo de ejemplo el listado de clientes de escritorio soportado por esta solución forense comercial correspondientes con el sistema operativo macOS.

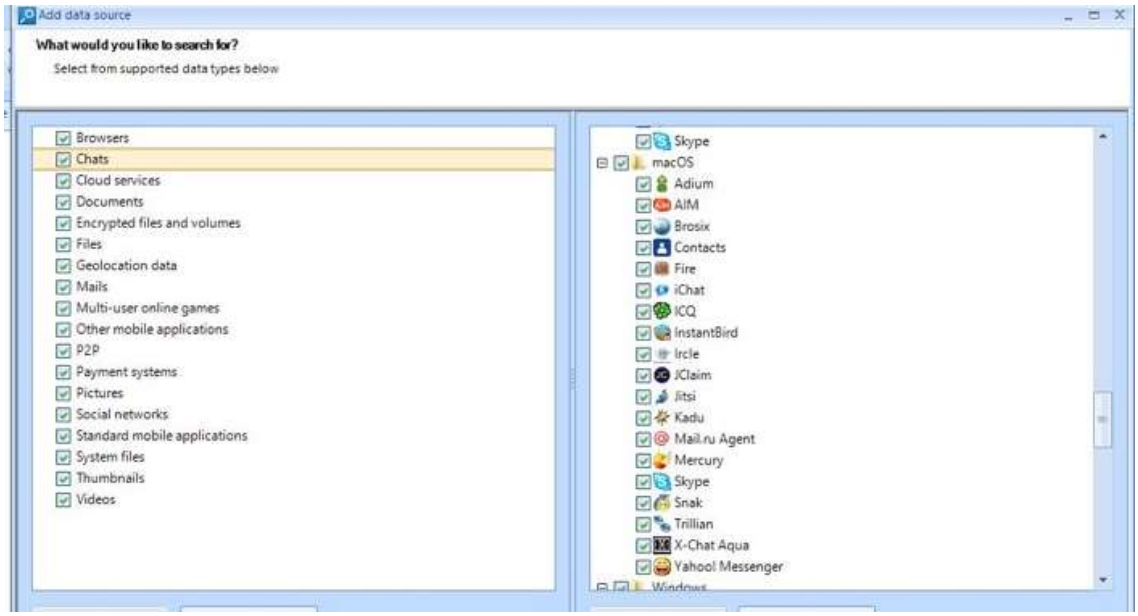


Figura 5.33. Listado de clientes de escritorio para macOS de la solución forense BEC.

De igual manera, la solución comercial forense Internet Evidence Finder (IEF) identifica las diferentes particiones incluidas en el sistema operativo macOS, si bien, tal y como se observa en la figura 5.34, esta solución no reconoce el sistema de archivos de Apple (APFS) correspondiente con la segunda posición "Particion 2 (111.6 GB)".

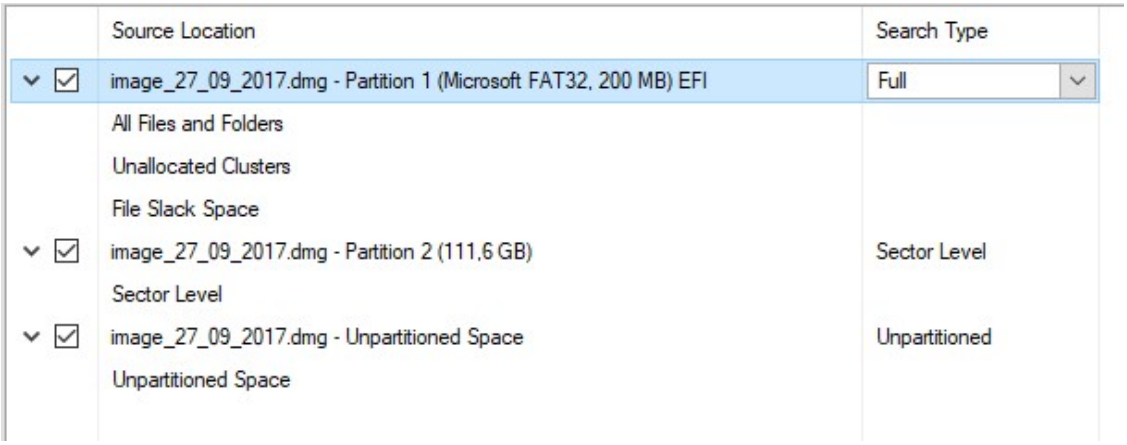


Figura 5.34. Identificación de sistema de archivos de la solución forense IEF.

Entre el listado de las aplicaciones de mensajería soportadas por la solución forense comercial Internet Evidence Finder para el sistema operativo macOS ("Windows and Mac Artifacts") no se encuentran los clientes de escritorio de las aplicaciones de IM

Telegram Messenger ni WhatsApp. La figura 5.35 muestra a modo de ejemplo el listado de clientes de escritorio soportado por esta solución correspondientes con el sistema operativo macOS.

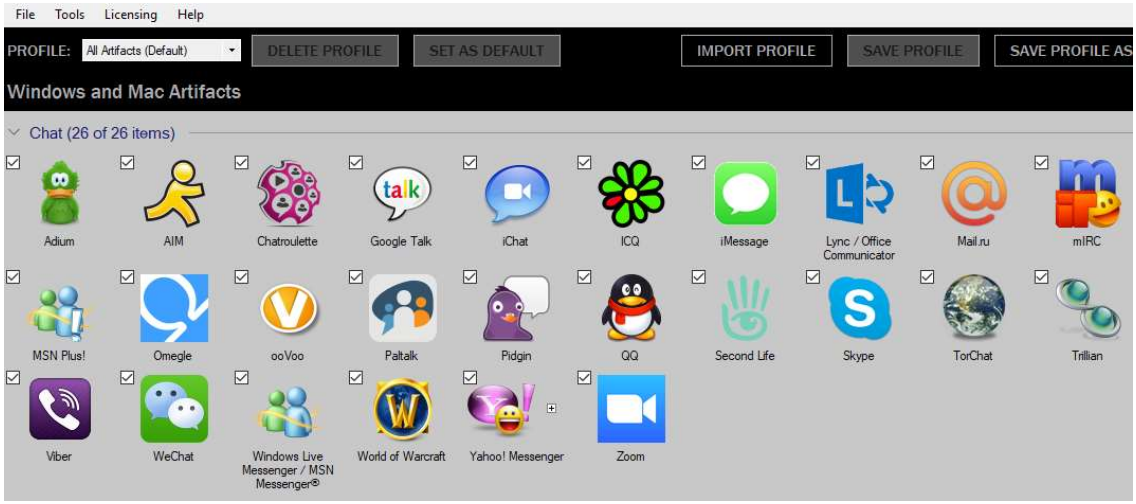


Figura 5.35 Listado de clientes de escritorio para macOS de la solución forense IEF.

Indicar que además de estas soluciones forenses comerciales especializadas en el análisis forense estático de artefactos, se han utilizado otras soluciones forenses comerciales (X-Ways Forensics[41], EnCase Forensics[42], Forensic Explorer[43], etc.) las cuales tampoco proporcionan en el momento del desarrollo de los estudios realizados soporte para el nuevo sistema de archivos APFS. De igual manera estas soluciones forenses comerciales tampoco son capaces de arrojar ningún tipo de información con respecto a los registros generados por los clientes de escritorio de las aplicaciones de IM Telegram Messenger ni WhatsApp.

[41] X-Ways Software Technology AG. X-Ways Forensics: Integrated Computer Forensics Software. Recuperado de: http://x-ways.net/forensics/index-m.html.

[42] OpenText. Encase Forensics. Recuperado de: https://www.guidancesoftware.com/encase-forensic.

[43] GetData Software Company. Forensic Explorer. Recuperado de: http://www.forensicexplorer.com/.

Análisis forense dinámico de artefactos.

Del análisis forense dinámico realizado sobre los clientes de escritorio de las aplicaciones de IM Telegram Messenger y WhatsApp en macOS, se obtiene como resultado las comunicaciones mantenidas por el usuario de estos clientes.

El análisis forense dinámico consiste en la copia forense de los datos identificados en el análisis forense estático de artefactos, e incluirlos en un entorno forense controlado. En el caso del cliente de escritorio de la aplicación de IM Telegram Messenger se realiza la copia forense de los datos de la aplicación (fila 1, tabla 5.3) y de los datos usuario (fila 3, tabla 5.3), siendo únicamente necesario realizar una copia de los datos de usuario (fila 3, tabla 5.3) en el caso del cliente de escritorio de la aplicación de IM WhatsApp. Los datos obtenidos de la copia forense son incluidos en un entorno forense controlado lo que imita el normal uso de los clientes de escritorio en el entorno forense controlado. Hay que mencionar que para poder recuperar las comunicaciones es necesario disponer de conexión a una red de datos en el entorno forense controlado.

En las figuras 5.36 se muestra la ejecución del cliente de escritorio de la aplicación de IM WhatsApp sobre el sistema operativo macOS en un entorno forense controlado con conexión de datos. Cierta información mostrada en la figura 5.36 ha sido ocultada para garantizar la privacidad del usuario.

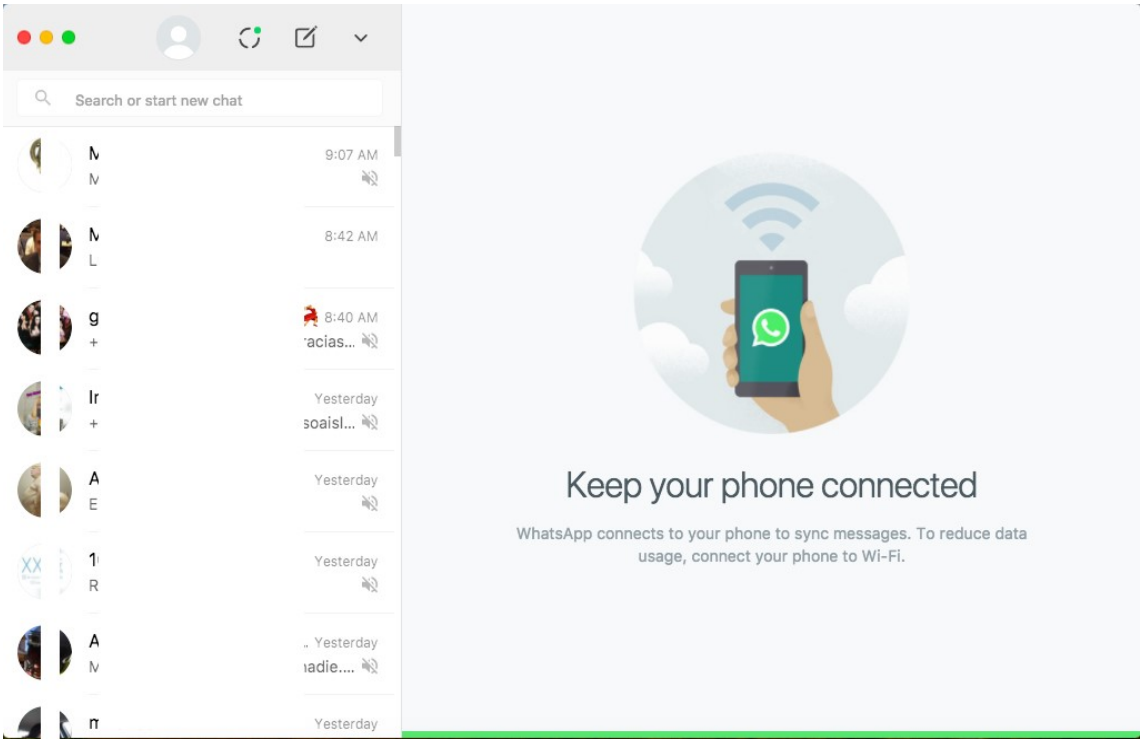


Figura 5.36. Conversaciones de usuario a través de la aplicación WhatsApp. (Entorno forense controlado).

Así mismo, en la figura 5.37 se muestra la ejecución del cliente de escritorio de la aplicación de IM Telegram Messenger en un entorno forense controlado con conexión de datos. Cierta información mostrada en la figura 5.37 ha sido ocultada para garantizar la privacidad del usuario.

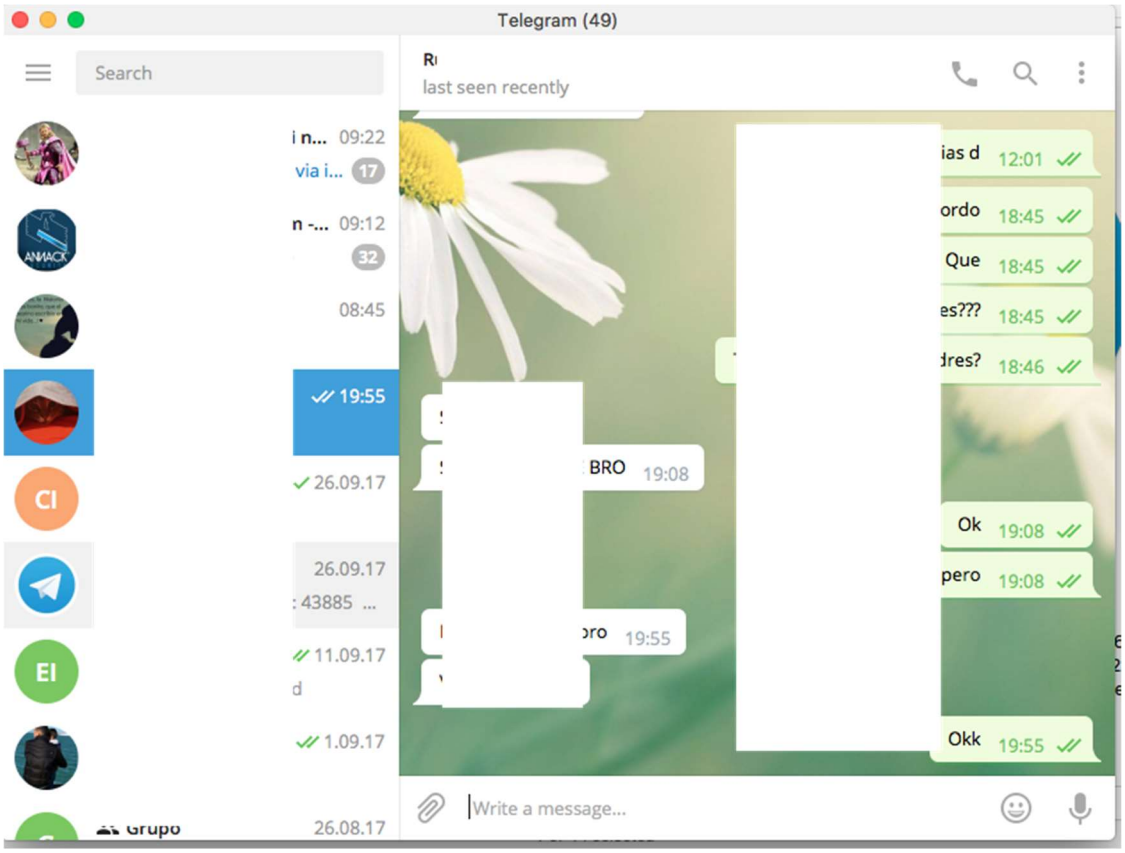


Figura 5.37. Conversaciones de usuarios a través de la aplicación Telegram Messenger (Entorno forense controlado).

Estudio de código fuente.

Del estudio del código fuente correspondiente al análisis de las líneas de código del lenguaje de programación en el cual se encuentra desarrollado en los clientes de escritorio de las aplicaciones Telegram Messenger y WhatsApp para macOS se obtiene el conocimiento técnico y funcional de la aplicación. Con respecto al estudio del código fuente del cliente de escritorio de la aplicación de IM Telegram Messenger y WhatsApp para macOS han sido analizadas todas aquellas clases, funciones, variables, etc., de las líneas de programación necesarias, tanto para apoyar, interpretar y validar tanto la información obtenida en el estudio de fuentes abiertas y del estudio estático de artefactos, así como conseguir cualquier otro tipo de información no obtenida de los estudios anteriores.

En el caso del cliente de escritorio de la aplicación Telegram Messenger el propio desarrollador de la aplicación proporciona el código fuente, siendo necesario realizar el

proceso de ingeniería inversa para acceder a las líneas de código en el caso del cliente de escritorio de la aplicación WhatsApp para el sistema operativo macOS ya que su desarrollador no proporciona el código fuente.

En el análisis realizado sobre las líneas de código de estos clientes de escritorio se identifican aquellas funciones utilizadas por los clientes para realizar la escritura y lectura los ficheros de datos. Del examen de estas funciones se concluye que, la información almacenada en estos ficheros se realiza de forma cifrada, limitando el acceso al contenido de estos que le señalo en el análisis forense estático de artefactos.

6 ANALISIS FORENSE EN RELOJES INTELIGENTES

En este sexto capítulo se exponen las contribuciones realizadas al análisis forense de las aplicaciones de mensajería instantánea en relojes inteligentes como parte de la investigación realizada en la presente Tesis.

6.1 Introducción

El origen del llamado Internet de las cosas o *Internet of Things* (IoT) y la aparición de los dispositivos digitales *wearables* ha generado que existan multitud de dispositivos electrónicos conectados continuamente a Internet y transmitiendo constantemente información. Entre la multitud de dispositivos *wearables* podemos encontrar a los relojes inteligentes, dispositivos que, además de otras muchas, tienen la capacidad de vincularse con un teléfono inteligente replicando la información recibida en este. Así mismo, muchos de estos relojes inteligentes tienen la capacidad de funcionar como un dispositivo independiente, sin estar vinculado a otro, ofreciendo a su usuario funcionalidades similares a las de un teléfono inteligente.

Tal y como queda patente en el estudio estadístico "Global Wearables Market Grows 7.7% in 4Q17 and 10.3% in 2017 as Apple Seizes the Leader Position, Says IDC"[44] realizado por el International Data Corporation (IDC), la cuota de mercado de los dispositivos wearables este crecimiento, siendo el reloj inteligente gran culpable de este crecimiento. Los relojes inteligentes además de disponer de las características típicas de un reloj convencional (fecha, hora, alarma, etc.), incorporan aplicaciones para la gestión de comunicaciones móviles (llamadas telefónicas, mensajes de texto, mensajería instantánea, etc.), aplicaciones para el manejo de sensores (posicionamiento, medición de frecuencia cardiaca, etc.), así como muchas otras aplicaciones y usos (cámara, reproductor de música, grabación de audio, etc.). Esta diversidad de aplicaciones es lo que hace que, estos dispositivos sean cada vez más utilizados tanto para uso personal

[44] International Data Corporation. (2018). *Global Wearables Market Grows 7.7% in 4Q17 and 10.3% in 2017 as Apple Seizes the Leader Position, Says IDC*. Recuperado el 10 de junio de 2018, de: https://www.idc.com/getdoc.jsp?containerId=prUS43598218.

como profesional. En su origen las funcionalidades de los relojes inteligentes eran muy limitadas, si bien, en la actualidad estas han evolucionado ofreciendo a sus usuarios una serie de funcionalidades parecidas a las de un teléfono inteligente (conectividad a redes de datos independiente, comunicaciones, posicionamiento, aplicaciones de mensajería instantánea, etc.).

En la actualidad los relojes inteligentes, como norma general, no son utilizados como medio principal en la comisión de un hecho delictivo, si bien, en el interior de estos se pueden almacenar información de especial relevancia relativa al dispositivo al cual se encuentren vinculado. El análisis forense de relojes inteligentes no esta tan desarrollado en cuanto a las soluciones forenses como sucede en el caso del análisis forense de teléfonos inteligentes u ordenadores. Este se centra en la adquisición y análisis de los datos contenidos en el teléfono inteligente vinculado, si bien, los relojes inteligentes pueden contener información no accesible o eliminada del dispositivo vinculado. El análisis forense debe adaptarse a la realidad actual de los datos contenidos en los dispositivos *wearables* y aplicar los procedimientos científicos necesarios para adquirir, analizar e interpretar todos los rastros contenidos en un reloj inteligente manteniendo en todo momento la inalterabilidad de los datos.

6.1.1 Adquisición forense en relojes inteligentes

La adquisición forense estática o adquisición tradicional es aquella en la que se obtiene la información del reloj inteligente previniendo su normal encendido y evitando con ello la alteración de los datos contenidos en la evidencia por parte del sistema operativo, aplicaciones o usuario. A partir de este tipo de adquisición se consigue generar una imagen forense de la información contenida en el reloj inteligente. En la actualidad, a diferencia del proceso de adquisición estática de los teléfonos inteligentes o dispositivos informáticos, las soluciones forenses soportan un numero de relojes inteligentes bastante limitado debiéndose recurrir en muchas ocasiones a las aplicaciones de actualización propias del dispositivo, para poder realizar una adquisición forense estática.

La adquisición forense dinámica es aquella en la que se obtiene una copia lógica de la información contenida de un reloj inteligente encendido. En el caso de los relojes inteligentes, a diferencia de lo que sucede con los teléfonos inteligentes, no disponen de

aplicaciones propias para la copia de información. La adquisición forense dinámica se centra actualmente en la adquisición manual de la información, proceso por el cual se realizan fotografías o videos de lo que muestra la pantalla del dispositivo.

6.1.2 Análisis forense de relojes inteligentes

El análisis forense de un reloj inteligente, como sucede con la adquisición, puede también subdividirse en análisis forense estático y análisis forense dinámico de artefactos. Como se ha venido explicando en capítulos anteriores, el análisis forense estático se realiza sobre los datos contenidos en la imagen forense generada en la adquisición y el análisis forense dinámico, se realiza sobre los registros que están siendo generados en el reloj inteligente durante su ejecución.

La evolución de los relojes inteligentes implica que, cuando se trata específicamente del análisis forense de los registros generados este tipo de dispositivos, este deba abordarse desde una perspectiva más amplia a la identificación, decodificación e interpretación de las comunicaciones de usuario. Los fabricantes de los relojes inteligentes, así como los desarrolladores de sistemas operativos *wearables*, no proporcionan información respecto a los datos almacenados en estos dispositivos más allá de los que puedan encontrarse en el teléfono inteligente vinculado. Las soluciones forenses comerciales actuales pueden automatizar el análisis de la información obtenida de los relojes inteligentes, si bien tal y como se mostrará en los siguientes puntos, no pueden cubrir la totalidad de los rastros generados ni la cantidad de relojes inteligentes.

La evolución continua de los relojes inteligentes y la limitación por parte de las soluciones forenses comerciales hace necesario el desarrollo de manera continua de estudios técnico-forenses. Estos estudios deben exponer los procesos utilizados durante la adquisición y análisis de la información contenida en los relojes inteligentes manteniendo en todo momento el valor probatorio de la prueba electrónica.

6.2 Escenarios: Relojes inteligentes con Nucleus RTOS

En los siguientes puntos se expondrá el resultado de los estudios técnico-forenses realizados sobre diversos relojes inteligentes con sistema operativo Nucleus RTOS. Se

describirá el análisis forense realizado sobre los artefactos que se generan en este tipo de dispositivos y se expondrán las conclusiones obtenidas.

En la actualidad, la mayoría de los análisis forenses realizados se centran en el análisis de los rastros generados en relojes inteligentes con sistemas operativos *wearables* populares como sucede con wearOS, watchOS, Android o Android Wear, si bien, es de mencionar que existe una gran variedad de relojes inteligentes que no incluyen estos sistemas operativos tan conocidos como en el caso de los relojes inteligentes con sistema operativos Nucleus RTOS. La falta de documentación forense, sumado al auge de este sistema operativo en relojes inteligentes de bajo coste, el cual puede ser encontrado en más de 3 billones de dispositivos según su desarrollador[45], hace necesario el desarrollo de estudios técnico-forenses específicos que identifiquen, decodifiquen y analicen los registros generados por este sistema operativo. Así mismo es de mencionar que, en el momento de la realización de los estudios técnicos-forenses que se exponen, las principales soluciones forenses comerciales como UFED de Cellebrite, Oxygen Forensics Analysis de Oxygen, XRY de MSAB o IEF de Magnet Forensics no proporcionan soporte específico sobre relojes inteligentes con sistema operativo Nucleus RTOS. El análisis forense de los registros generados en un reloj inteligente por el sistema operativo Nucleus RTOS, se llevará a cabo a partir de la metodología de propuesta, suma de tres métodos de estudios complementarios, siendo desarrollada sobre tres modelos de relojes inteligentes diferentes. Es de mencionar que en el momento de la realización de estos estudios técnico-forenses no existía documentación en relación con los registros que se generaban en relojes inteligentes con sistema operativo Nucleus RTOS.

A continuación, se desarrollarán los tres métodos de estudios incluidos en la metodología de análisis propuesta, exponiendo los resultados obtenidos de aplicar esta metodología al análisis forense sobre el sistema operativo Nucleus RTOS.

[45] Mentor. (2019). *Nucleus RTOS*. Recuperado el 10 de enero de 2019, de: https://www.mentor.com/embedded-software/nucleus/.

6.3 Análisis de Nucleus RTOS

Este punto expondrá el resultado obtenido del estudio de fuentes abiertas, de artefactos y de código fuente, incluidos en la metodología de análisis forense propuesta, sobre los registros que genera el sistema operativo Nucleus RTOS en un reloj inteligente.

6.3.1 Estudio de fuentes abiertas

El estudio de fuentes abiertas ha sido desarrollado a partir de los procedimientos descritos en el punto 3.3.1 de esta Tesis. Estos procedimientos permitirán recopilar de manera fiable toda aquella documentación, que pueda de una u otra forma contribuir en el análisis forense del sistema operativo Nucleus RTOS.

El estudio de fuentes abiertas se corresponde con el análisis realizado sobre los resultados obtenidos de la búsqueda de palabras clave (Nucleus RTOS, RTOS, Real Time Operating System, Sistema Operativo Tiempo Real, Artefactos, Artifacts, Notifications, Instant Messenger, IM, mensajería instantánea, Forensics, Forense, Analysis, Análisis, etc.) sobre diversas fuentes de datos abiertas o semiabiertas. Estas fuentes de datos incluyen toda aquella documentación recopilada de revistas de investigación digital (journals.elservier.com/digital-investigation; commons.erau.edu/jdfsl, etc.), foros técnicos (focusforensics.com; forensicswiki.com; incibe.com, etc.), investigaciones independientes (dinosec.com/es/lab.html, etc.), ponencias técnicas (RootedCon, Blackhat, etc.), bibliotecas virtuales (http://biblioteca.uah.es, etc.) o de gestores de contenido (scholar.google.com, etc.).

En el momento del estudio no se encuentran resultados con relación al sistema operativo Nucleus RTOS más allá de información técnica proporcionada por el propio desarrollador del sistema operativo. Este facilita a través de su página web[46] información relativa a las características del sistema operativo Nucleus RTOS (seguridad, conectividad, interfaz de

[46] Mentor. (2019). *Nucleus RTOS*. Recuperado el 10 de enero de 2019, de: https://www.mentor.com/embedded-software/nucleus/.

usuario, etc.), así como a los diferentes tipos de sistemas de archivos soportados por este (VFAT y Nucleus SAFE)[47].

Una vez analizadas las diferentes fuentes de datos expuestas se concluye que las mismas no proporcionan información de especial relevancia para el análisis forense del sistema operativo Nucleus RTOS, si bien, estas podrán ser utilizadas para apoyar, validar o interpretar los datos obtenidos de los demás estudios incluidos en la metodología de análisis propuesta.

6.3.2 Estudio de artefactos

El estudio de artefactos ha sido desarrollado a partir de los procedimientos descritos en el punto 3.3.2 de esta Tesis. Estos procedimientos permitirán identificar, decodificar e interpretar los rastros generados por el sistema operativo Nucleus RTOS a partir del análisis comparativo registros.

6.3.2.1 Análisis forense estático

A continuación, se muestran los resultados obtenidos del análisis comparativo realizado sobre los registros generados por varios relojes inteligentes con sistema operativo Nucleus RTOS. Este ha sido elaborado a partir del análisis forense estático recurrente incluido en el estudio de artefactos de la metodología propuesta, el cual permite identificar, decodificar e interpretar los rastros generados en este sistema operativo.

6.3.2.1.1 Ejecución análisis comparativo de artefactos

El análisis forense de los artefactos generados en un reloj inteligente con sistema operativo Nucleus RTOS puede ser elaborado de forma manual analizando en crudo a través de editores hexadecimales las adquisiciones realizadas sobre los diferentes

[47] Mentor (2019). *File Systems and Storage with Nucleus RTOS*. Recuperado el 10 de enero de 2019, de: https://www.mentor.com/embedded-software/nucleus/storage.

modelos relojes inteligentes objeto de este estudio (“NO.1 G6”, “DAWONO DZ09” y “KINGSTART GT08”).

En este caso, para el análisis comparativo de las adquisiciones realizadas sobre los relojes inteligentes objeto de estudio se ha utilizado la solución forense comercial UFED Physical Analyzer, la cual permite identificar el sistema de archivos (estructura de carpetas y ficheros) del sistema operativo Nucleus RTOS a partir de a partir de la ejecución de una serie de cadenas o procesos automáticos. De igual manera para decodificar e interpretar la información se utilizará el editor hexadecimal incluido en esta solución.

La figura 6.1 muestra la pantalla de la opción avanzada del menú abrir (“*Open (Advanced)*”) de la solución forense comercial UFED Physical Analyzer a partir de la cual se puede seleccionar la cadena o proceso automático (“*Selected Chain*”) y añadir la imagen forense de la adquisición realizada (“*Add Binary Dump*”).

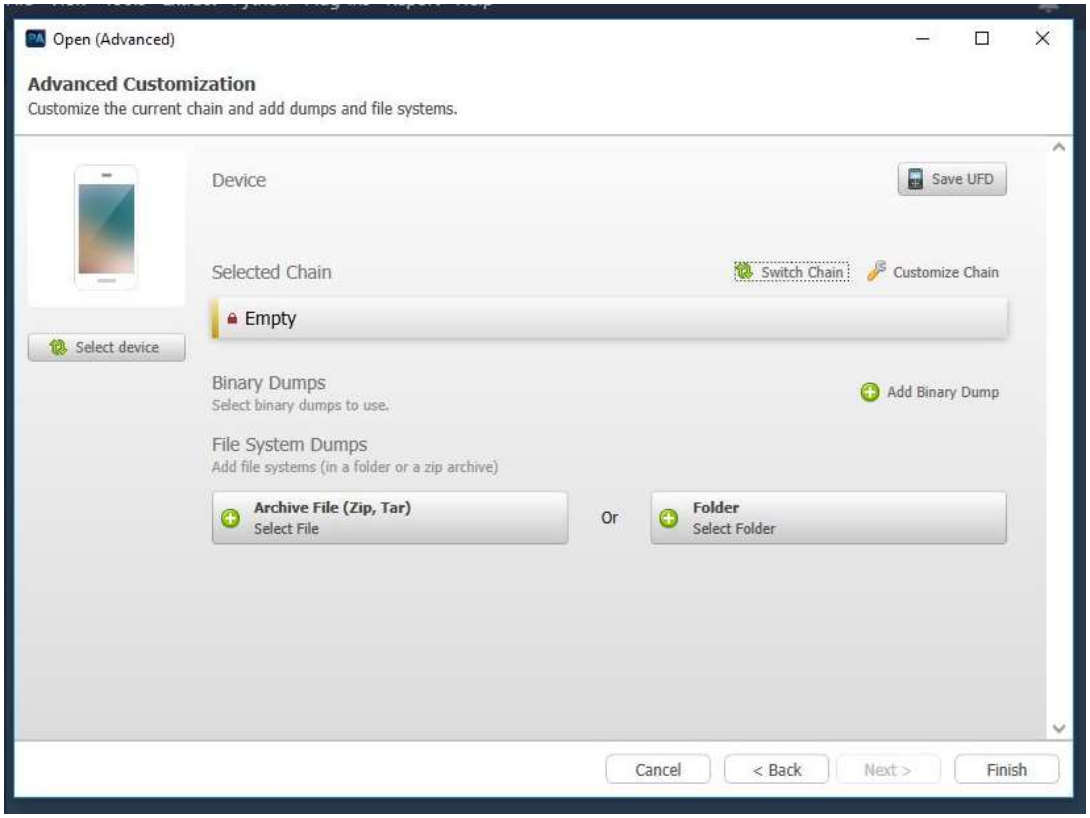


Figura 6.1. Abrir (Avanzado). Solución forense comercial UFED Physical Analyzer.

La solución forense comercial UFED Physical Analyzer, dispone de multitud de cadenas en relación con las características de un dispositivo electrónico (marca y modelo del dispositivo, marca y modelo del procesador, sistema operativo, sistema de archivos, etc.). Cada cadena incluye una serie de procesos utilizados para identificar y decodificar los registros contenidos en los dispositivos electrónicos.

En el caso de los relojes inteligentes objeto del estudio, ya que los mismos disponen de procesador MediaTek (MTK) así como de un sistema operativo distinto a Android, la solución forense UFED Physical Analyzer dispone de la cadena "*Non Android MTK*", la cual se comprende estas características.

La figura 6.2 muestra la pantalla de la opción cambiar de cadena ("*Switch Chain*") en la cual se identifican las cadenas disponibles en la solución forense comercial UFED Physical Analyzer con el literal "MTK". Esta figura muestra los procesos incluidos en la cadena "*Non Android MTK*" utilizados para identificar y decodificar la información contenida en dispositivos electrónicos con procesador MediaTek o MTK y sistema operativo distinto a Android.

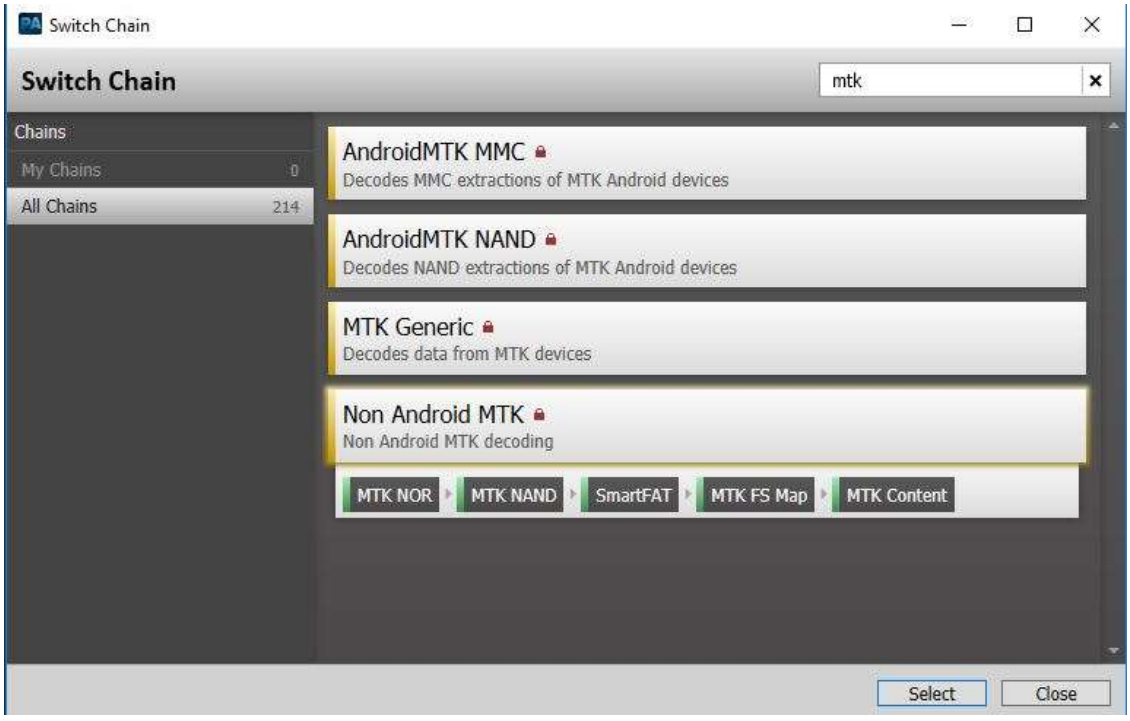
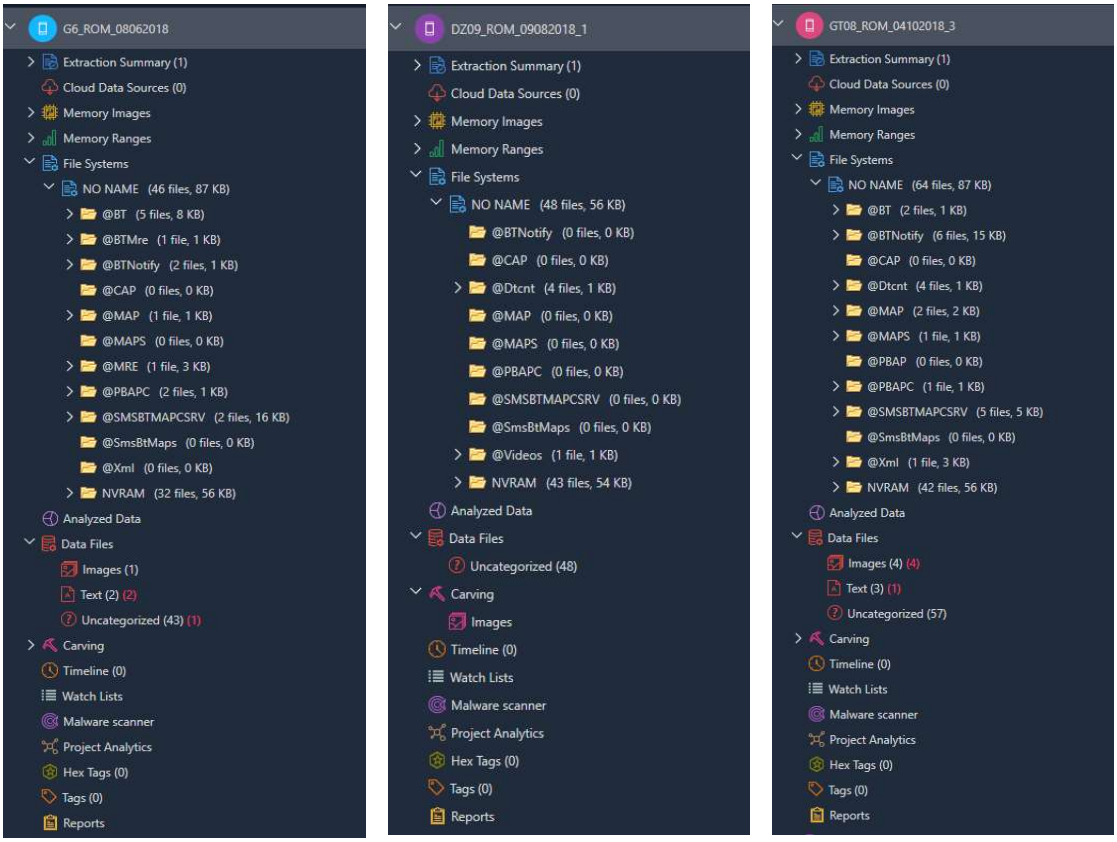


Figura 6.2. Selección de cadena. Solucion forense comercial UFED Physical Analyzer.

La ejecución de la cadena "*Non Android MTK*" sobre las múltiples adquisiciones realizadas, permite identificar la estructura de carpetas y ficheros contenidas en el sistema de archivos, catalogando los ficheros de datos encontrados por familias, si bien como ya se ha mencionado, esta solución forense comercial no decodifica la información contenida en estos ficheros de datos. La figura 6.3 (a, b y c) muestra la estructura de carpetas contenida en el sistema de archivos ("*File Systems*") así como los ficheros catalogados por tipo ("*Data Files*"). La decodificación de artefactos generados en el sistema operativo Nucleus RTOS se encuentra vacía. ("*Analyzed Data*").



a. Ejemplo del sistema de archivos de "NO.1 G6"

b. Ejemplo del sistema de archivos de "CAWONO DZ09"

c. Ejemplo del sistema de archivos de "KINGSTART GT08"

Figura 6.3. Ejemplo del sistema de archivos de Nucleus RTOS. Solucion forense comercial UFED Physical Analyzer.

A partir del análisis comparativo del contenido de los diferentes archivos identificados en este punto, se puede decodificar e interpretar la información almacenada en los mismos.

La tabla 6.1 muestra el listado de artefactos identificados en el análisis comparativo realizado sobre el sistema operativo Nucleus RTOS, así como la información contenida.

Tabla 6.1. Artefactos generados en Nucleus RTOS.

#	Contenido	Directorio	Fichero/s
1	Agenda de contactos.	NO NAME/@PBAPC	LIST.TMP y ENTRY.TMP
2	Registro llamadas.	NO NAME/@BTDIALER	FOLDER.TMP
3	Mensajes de texto.	NO NAME/@SMSBTMAPCSRV	Diferentes ficheros con formato {numero}.O y msg_btmapc_node.o
4	Notificaciones.	NO NAME/@BTNofity	bt_notify_0000.xml
5	Índice de notificaciones.	NO NAME/@MAP	bt_notify_map.xml
6	Registro conexiones Bluetooth	NO NAME/@BT	COD y DEVDB
7	Información del dispositivo vinculado	NO NAME/NVRAM/NVD_DATA/PACKALID/	MP25_001

A continuación, se describe el resultado del análisis comparativo realizado sobre la información contenida en los archivos contenidos en la tabla 6.1.

6.3.2.1.2 Información relativa a agenda de contactos

Los ficheros de datos “LIST.TMP” y “ENTRY.TMP” ubicados en el directorio “NO NAME/@PBAPC”, contienen la información relativos a la agenda de contactos del teléfono inteligente vinculado.

El fichero “LIST.TMP” de tipo XML almacena únicamente el listado de nombres de la agenda de contactos. La figura 6.4 muestra a modo de ejemplo, parte del contenido del fichero “LIST.TMP”. En esta figura se puede identificar el atributo con nombre “name” y el valor “Jonas” siendo este, el nombre de uno de los contactos ubicado en la agenda de telefónica del teléfono inteligente vinculado.

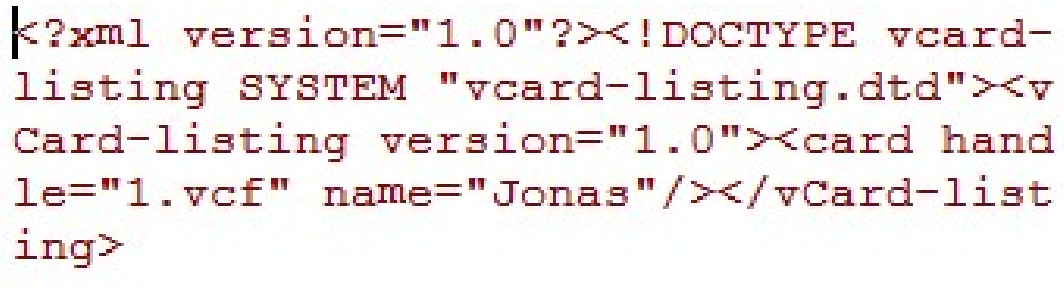


Figura 6.4. Ejemplo del fichero “LIST.TMP” ubicado en la carpeta “NO NAME/@PBAPC”.

El fichero “ENTRY.TMP” contiene una estructura de etiquetas y atributos donde se almacena el listado de nombres y sus números de teléfono de la agenda de contactos. La figura 6.5 muestra parte del contenido del fichero “ENTRY.TMP”. En esta figura se puede identificar los atributos con nombre “N” y “FN” y el valor “Jonas” así como el atributo “TEL;CELL” y el valor “60XXXXXXX”, siendo estos, el nombre y número de teléfono de uno de contactos ubicado en la agenda de telefónica del teléfono inteligente vinculado. Cierta información mostrada en la figura 6.5 ha sido ocultada para garantizar la privacidad del usuario.

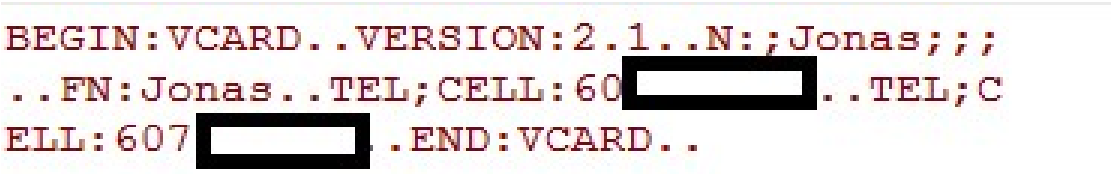


Figura 6.5. Ejemplo del fichero “ENTRY.TMP” ubicado en la carpeta “NO NAME/@PBAPC”.

Se significa que los ficheros “LIST.TMP” y “ENTRY.TMP” también pueden ser encontrados en el interior del directorio “NO NAME/@BTDIALER”.

6.3.2.1.3 Registro de llamadas

El fichero de datos “FOLDER.TMP” ubicado en el interior de la carpeta “NO NAME/@BTDIALER” contiene una estructura de etiquetas y atributos donde se

almacena la información relativa al registro de llamadas del teléfono inteligente vinculado (nombre, número de teléfono, fecha y tipo de llamada).

La figura 6.6 muestra a modo de ejemplo parte del contenido del fichero "FOLDER.TMP". En esta figura se puede identificar los registros de llamadas del teléfono inteligente vinculado.

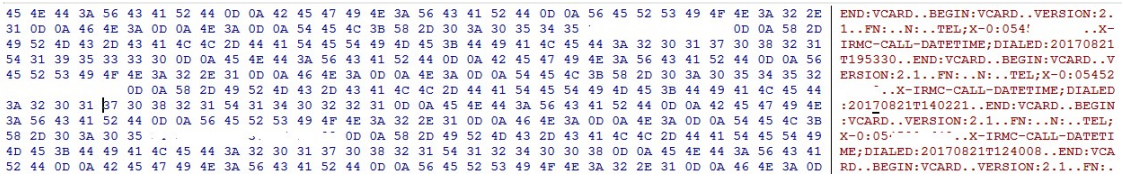


Figura 6.6. Ejemplo del fichero "FOLDER.TMP" ubicado en la carpeta "NO NAME/@BTDIALER".

La figura 6.7 muestra con más detalle uno de los registros de llamadas contenidos del fichero "FOLDER.TMP". En esta figura se puede observar como entre las etiquetas "BEGIN:VCARD" y "END:VCARD" se encuentran los atributos de nombre de contacto ("N" y "FN"), número de teléfono ("TEL;X-") y tipo y fecha de la llamada ("X-IRMC-CALL-DATETIME"). Cierta información mostrada en la figura 6.7 ha sido ocultada para garantizar la privacidad del usuario.

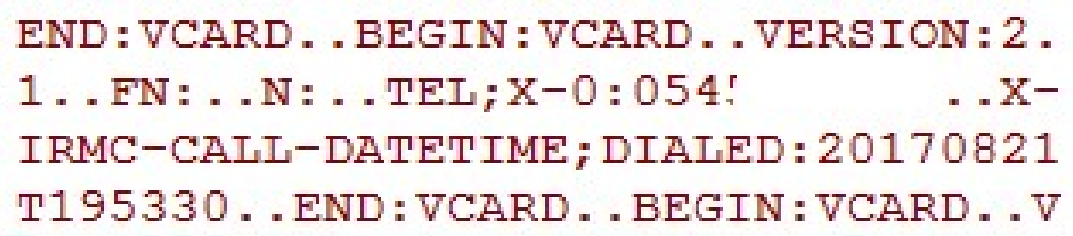


Figura 6.7. Ejemplo de registro llamada realizada. Fichero "FOLDER.TMP" ubicado en la carpeta "NO NAME/@BTDIALER".

Se significa que el fichero "FOLDER.TMP" también puede ser encontrado en el interior del directorio "NO NAME/@PBAPC/".

6.3.2.1.4 Mensajes de texto

Los mensajes de texto del teléfono inteligente vinculado pueden ser encontrados en el interior de la carpeta "NO NAME/@SMSBTMAPCSRV". En esta carpeta los mensajes de texto pueden ser localizados de manera independiente en ficheros con nombre {numero}".O" o de manera total en el archivo de datos con nombre "msg_btmapc_node.o".

La figura 6.8 muestra a modo de ejemplo el mensaje de texto contenido en el fichero con nombre "1.O" ubicado en el interior de la carpeta "NO NAME/@SMSBTMAPCSRV".

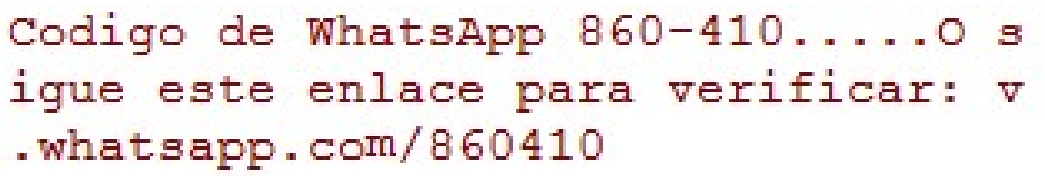


Figura 6.8. Ejemplo del fichero "1.O" ubicado en la carpeta "NO NAME/@SMSBTMAPCSRV".

La figura 6.9 muestra a modo de ejemplo parte del contenido del fichero con nombre "msg_btmapc_node.o" ubicado en el interior de la carpeta "NO NAME/@SMSBTMAPCSRV" en el cual se pueden identificar el listado de mensajes de texto.

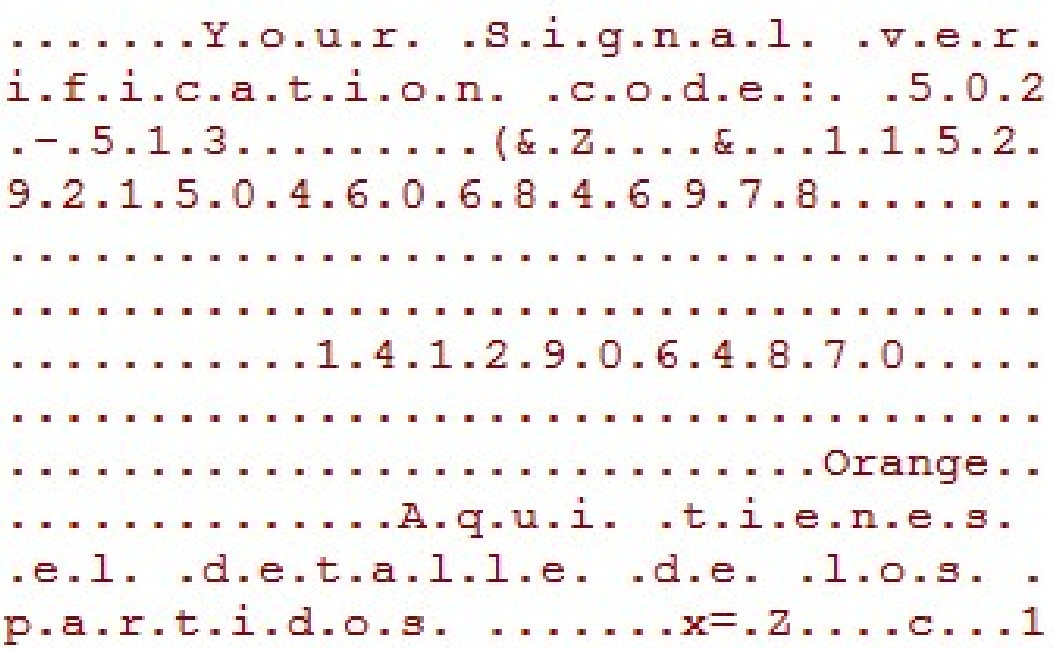


Figura 6.9. Ejemplo del fichero "msg_btmapc_node.o" ubicado en la carpeta "NO NAME/@SMSBTMAPCSRV".

Se significa que el fichero de datos "bt_notify_map.vcf" ubicado en el interior del directorio "NO NAME/@MAP/", también contiene la información relativa a los mensajes de texto del teléfono inteligente vinculado. Los datos en este archivo se estructuran en etiquetas y atributos en los que se almacena la información de nombre, número de teléfono, fecha, estado, longitud y texto del mensaje.

La figura 6.10 muestra a modo de ejemplo parte del contenido del fichero "bt_notify_map.vcf". En esta figura se puede observar como entre las etiquetas "BEGIN:BMSG" y "END:BMSG" se identifican los atributos de estado del mensaje ("STATUS"), tipo de mensaje ("TYPE"), longitud del mensaje ("LENGTH") así como el texto del mensaje entre las etiquetas "BEGIN:MSG" y "END:MSG".

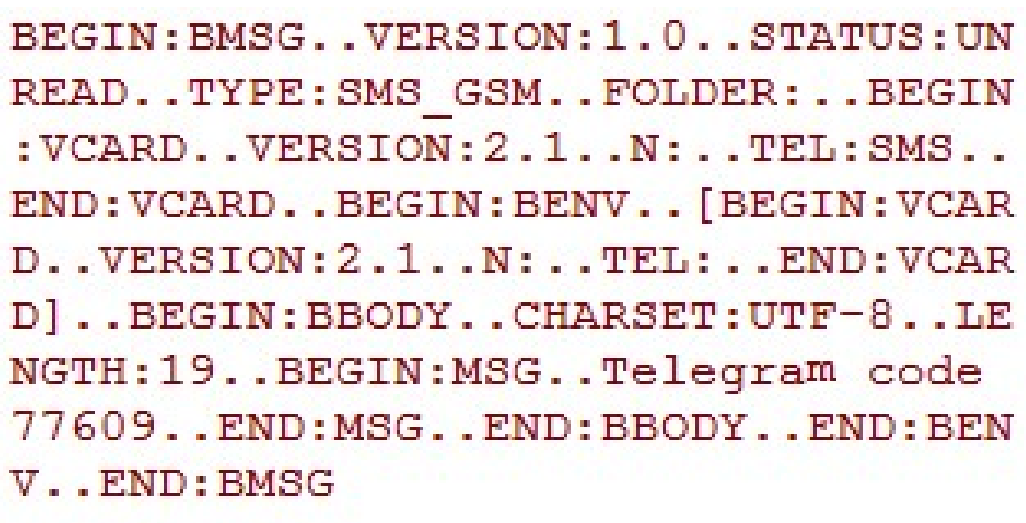


Figura 6.10. Ejemplo del fichero "bt_notify_map.vcf" ubicado en la carpeta "NO NAME/@MAP".

6.3.2.1.5 Notificaciones

Los ficheros de datos "bt_notify_0000.xml" y "bt_notify_map.xml" ubicados en el directorio "NO NAME/@BTNofity" y "NO NAME/@MAP" respectivamente, contienen la información relativos a las notificaciones recibidas en el teléfono inteligente vinculado.

El fichero de datos "bt_notify_0000.xml" de tipo XML almacena la información de la última notificación recibida en el reloj inteligente. Entre los diferentes campos que contiene este archivo se encuentran el identificador del mensaje ("msgId"), la aplicación que realiza la notificación ("sender"), el identificador de la aplicación ("appId"), el contenido de la notificación ("ticker_text") y la fecha de la notificación ("timestamp") almacenada en formato *epochunix*.

La figura 6.11 muestra a modo de ejemplo el contenido del fichero "bt_notify_0000.xml" en el cual se muestran los atributos "category", "sender", "ticker_text" y "timestamp" así como sus valores. Estos campos indican que la última notificación en el teléfono inteligente fue emitida por la aplicación "BTNotificacion" con el texto "WOO Partner conectado al dispositivo remoto" el día jueves 4 de octubre de 2018 a las 12:25:33 PM (GMT +2).

Figura 6.11. Ejemplo del fichero “bt_notify_0000.xml” ubicado en la carpeta “NO NAME/@BTNotify”.

Así mismo el fichero con nombre “bt_notify_map.xml” de tipo XML contiene un índice de las notificaciones vinculadas en el reloj inteligente. Este fichero incluye entre otros campos un identificador numérico (“handle”), la fecha de envío de la notificación (“datetime”), aplicación o número que envía (“sender_name”), el tipo de notificación (“type”), el tamaño (“size”), si es texto o no (“text”) o el estado (“read”). La figura 6.12 muestra a modo de ejemplo parte del contenido del fichero “bt_notify_map.xml” en el cual se observa que cada notificación se almacena en una estructura de datos independiente bajo la etiqueta “msg”.

Figura 6.12. Ejemplo del fichero "bt_notify_map.xml" ubicado en la carpeta "NO NAME/@MAP".

6.3.2.1.6 Registros conexiones Bluetooth

Los ficheros de datos con nombre "COD" y "DEVDB" ubicados en el directorio "NO NAME/@BT" contienen la dirección Bluetooth del dispositivo electrónico vinculados. Esta información se almacena en formato hexadecimal y en sentido inverso.

La figura 6.13 muestra parte del contenido del fichero de datos "COD" en el cual se identifica el valor hexadecimal "70B9AAD0A9F8".

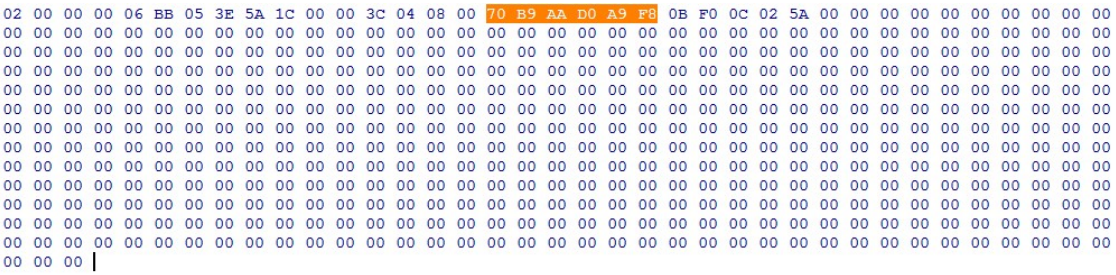


Figura 6.13. Ejemplo del fichero "COD" ubicado en la carpeta "NO NAME/@BT/".

Así mismo, la figura 6.14 muestra el parte del contenido del fichero de datos “DEVDB” identificándose en su interior el valor hexadecimal “70B9AAD0A9F8”.

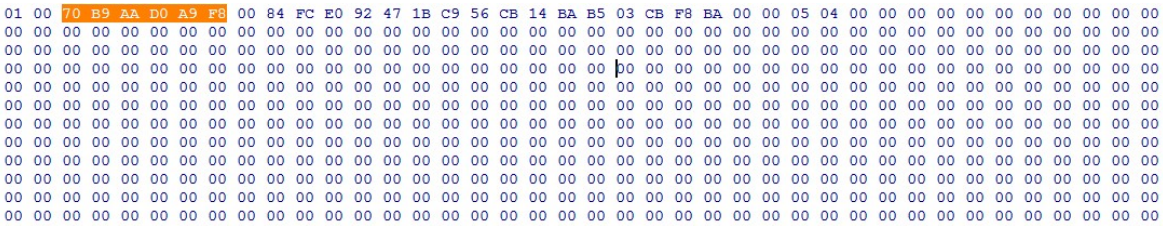


Figura 6.14. Ejemplo del fichero “DEVDB” contenido en el directorio “NO NAME/@BT/”.

El valor hexadecimal “70B9AAD0A9F8” encontrado en los archivos de datos “COD” y “DEVDB” corresponde a la dirección Bluetooth “f8:a9:d0:aa:b9:70” del teléfono inteligente marca “LG” modelo “Nexus5” vinculado a los relojes inteligentes objeto de estudio. La figura 6.15 muestra a modo de ejemplo la pantalla de búsqueda de dispositivos Bluetooth de uno de los relojes inteligentes utilizados en esta investigación.

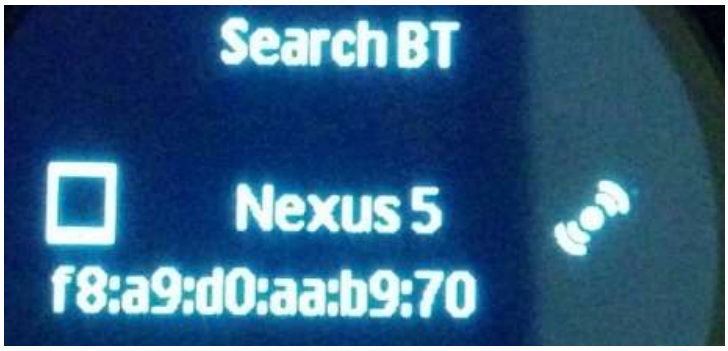


Figura 6.15. Notificación de vinculación del teléfono inteligente en el reloj inteligente.

De igual manera, los ficheros de datos “MP26_001” y “MP80_000” ubicados en los directorios “NO NAME/NVRAM/NVD_DATA” y “NO NAME/NVRAM/NVD_DATA/PACKALID/” respectivamente, almacenan diversa información relativa al nombre del teléfono inteligente vinculado al reloj inteligente, así como su dirección Bluetooth.

La figura 6.16 muestra a modo de ejemplo el contenido del fichero “MP26_0001”, en el cual se identifican el nombre de dos teléfonos inteligentes vinculados (Samsung Galaxy

J3 y Smartphone6.1) y sus respectivas direcciones Bluetooth (24:92:0E:A3:FF y 60:FE:1E:A6:90) en formato hexadecimal (FFA3000E009224 y 90A6001E00FE60).

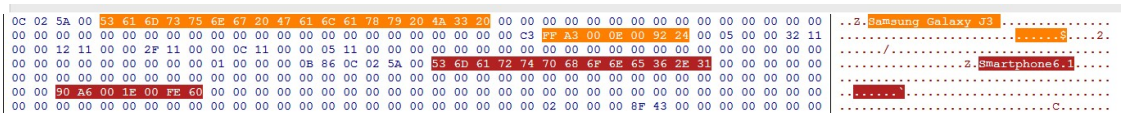


Figura 6.16. Ejemplo de fichero “MP26_001” ubicado en “NO NAME/NVRAM/NVD_DATA/”.

Así mismo la figura 6.17 muestra a modo de ejemplo el contenido del fichero “MP80_000”, en el cual se identifica el nombre del teléfono inteligente vinculado (Smartphone6.1) así como su estado (“Connected”).

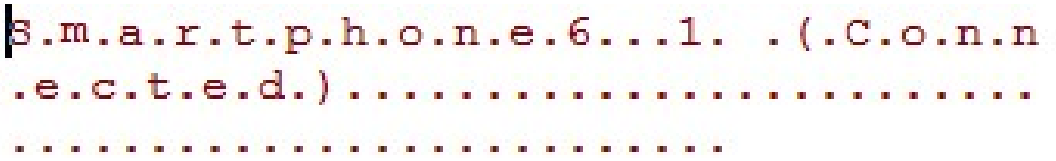


Figura 6.17. Ejemplo del fichero “MP80_000” contenido en la carpeta “NO NAME/NVRAM/NVD_DATA/PACKALID/”.

6.3.2.1.7 Información del reloj inteligente

En fichero “MP25_001” ubicado en el directorio “NO NAME/NVRAM/NVD_DATA/PACKALID/” almacena la información correspondiente al nombre y la dirección Bluetooth del reloj inteligente.

La figura 6.18 muestra a modo de ejemplo el contenido del fichero “MP25_001” en el cual se identifica el valor “GT08” correspondiente al nombre del reloj inteligente y el valor hexadecimal “6162F7005A007F3A” correspondiente a su dirección Bluetooth “3a:7f:5a:f7:62:61”.

Figura 6.18. Ejemplo del fichero “MP25_001” ubicado en el directorio “NO NAME/NVRAM/NVD_DATA/PACKALID/".

6.3.3 Estudio de código fuente

El estudio de código fuente ha sido desarrollado a partir de los procedimientos descritos en el punto 3.3.3 de esta Tesis. Estos procedimientos permitirán identificar, decodificar, interpretar y verificar los registros generados en el sistema operativo Nucleus RTOS a partir del análisis de código fuente.

Dicho estudio se corresponde con el análisis realizado sobre las líneas de código, siendo la forma de obtener el código fuente del sistema operativo Nucleus RTOS a través del envío de una solicitud y evaluación de la misma por parte de su desarrollador.

Esta solicitud puede ser gestionada a través de la propia página web del desarrollador[48], si bien, en el caso de no recibir respuesta ante la solicitud como fue en el caso del desarrollo de este estudio y debido a que el código fuente del sistema operativo Nucleus RTOS es cerrado, el acceso a las líneas de código quedaría supeditado al proceso de ingeniería inversa.

[48] Mentor. (2019). *Embedded Software Downloads*. Recuperado el 10 de enero de 2019, de: https://www.mentor.com/embedded-software/request?&fmpath=/embedded-software/downloads/nucleus-source-interest_reg&id=6d73df.

6.3.4 Resultados del análisis realizado

De la suma de estudios incluidos en la metodología propuesta para el desarrollo del análisis forense de los registros que se generan en un reloj inteligente con sistema operativo Nucleus RTOS se desprende que:

a) Del estudio de las fuentes abiertas correspondiente al análisis de toda aquella fuente de datos que pudiera contener información funcional, técnica y forense relativa al sistema operativo Nucleus RTOS no se obtiene ningún tipo información que pueda ser utilizada para contribuir al análisis forense de este sistema operativo.

b) Del estudio de artefactos correspondiente al análisis forense estático del sistema operativo Nucleus RTOS se obtienen los diferentes registros generados por el teléfono inteligente vinculado. A partir del análisis comparativo se logra identificar el listado de carpetas y archivos de datos contenidos en el sistema de archivos de este sistema operativo, así como decodificar e interpretar la información contenida en estos archivos de datos concerniente a la agenda de contactos, registro de llamadas, mensajes de texto, notificaciones, conexiones y datos relativos al teléfono inteligente vinculado.

c) Del estudio del código fuente correspondiente al análisis de las líneas de código del lenguaje de programación no se obtiene ningún tipo de información que pueda ser utilizada para identificar, decodificar, interpretar y verificar la información obtenida en el estudio de artefactos.

Tal y como ha quedado demostrado, la metodología de análisis forense propuesta permite identificar, decodificar e interpretar la información contenida en los relojes inteligentes con sistema operativo Nucleus RTOS.

7 CONCLUSIONES Y CONTRIBUCIONES DERIVADAS DE LA TESIS

7.1 Resumen de las principales conclusiones de la tesis doctoral

La evolución de las Tecnologías de la Información y de las Comunicaciones junto al nacimiento de Internet han transformado de manera drástica el funcionamiento de nuestra sociedad dando paso a una era en la cual el uso diario de dispositivos electrónicos personales, así como la transferencia de información digital esta homogeneizada. En la actualidad, la sociedad vive continuamente interconectada a través de un amplio abanico de dispositivos electrónicos personales (ordenadores, portátiles, teléfonos y relojes inteligentes, tabletas, dispositivos IoT, etc.) cuyas capacidades y funcionalidades eran inimaginable hace años. Nos encontramos frente a dispositivos electrónicos cada vez más pequeños e inteligentes que han transformado tanto los medios como los métodos utilizados para interactuar o comunicarse con la sociedad. Estos dispositivos, disponen de múltiples aplicaciones las cuales permiten a su usuario realizar gestiones bancarias, realizar compras en línea, consultar documentación a través de Internet, visualizar contenido multimedia en directo, hacer fotografías o videos, controlar su frecuencia cardiaca, compartir contenido o comunicarse de manera inmediata a través de aplicaciones de mensajería instantánea, con total independencia de horario o ubicación.

La Informática Forense como parte de las Ciencias Forenses, es la encargada de realizar el análisis forense de las aplicaciones de mensajería instantánea ubicadas en las evidencias electrónicas incluidas en la investigación de hechos delictivos. El análisis forense de las evidencias electrónicas debe ser realizado a partir de procedimientos científicos los cuales garanticen la inalterabilidad de la información obtenida manteniendo en todo momento la trazabilidad de la prueba electrónica a través de la cadena de custodia. En el caso específico de las aplicaciones de mensajería instantánea, el análisis forense resulta sumamente complejo en cuanto al número de versiones disponibles por cada uno de los clientes de este tipo de aplicaciones. La periodicidad con la que se actualizan cada uno de los clientes de este tipo de aplicaciones implica que, se deba realizar un análisis forense independiente por cada nueva versión comprobando la

diferencia de rastros generados, modificados o eliminados con respecto a versiones anteriores. Esto conlleva que exista una tendencia generalizada en el uso de soluciones forenses comerciales o de caja negra que automatizan la identificación, decodificación e interpretación del enorme volumen de información generado por este tipo de aplicaciones. Este tipo de soluciones automatizan en tal medida el análisis forense de las aplicaciones de mensajería instantánea que son capaces de generar informes estándar con los resultados obtenidos, si bien, se debe tener presente que las mismas tienen limitaciones. Estas soluciones forenses no pueden incorporar cada versión de cada cliente de cada una de las aplicaciones de mensajería instantánea que ha existido, existen o existirán. Así mismo, las empresas desarrolladoras de este tipo soluciones, ante la necesidad de superar a otras compañías en cuanto al número de versiones, clientes, aplicaciones de mensajería instantánea, sistemas operativos o dispositivos electrónicos soportados pueden precipitarse en el lanzamiento o actualización de sus soluciones forenses, pudiéndose dar el caso de encontrarnos ante un análisis forense pobre o erróneo de una determinada aplicación de mensajería instantánea.

El especialista debe ser consciente de las limitaciones de este tipo de soluciones forenses y de las especiales características que engloban el análisis forense de las aplicaciones de mensajería instantánea. Es esencial tener presente que la celeridad con la que evolucionan este tipo de aplicaciones supera con creces a la respuesta que pueden proporcionar las soluciones forenses. El especialista en muchas ocasiones debe efectuar por sí mismo el análisis forense de este tipo de aplicaciones sin ayuda de este tipo de soluciones. Para ello se debe aplicar una metodología de análisis forense especifica cuyos procedimientos y técnicas científicas permitan identificar, decodificar e interpretar de forma específica los datos generados por las diferentes aplicaciones de mensajería instantánea con independencia de la versión, cliente, sistema operativo o dispositivo electrónico utilizado.

En la actualidad, las metodologías utilizadas en el análisis forense de evidencias digitales se basan en las directrices marcadas por los estándares, guías de buenas prácticas o manuales desarrollados por diferentes organismos de ámbito internacional y nacional. Estos estándares, guías de buenas practica y manuales subdividen la metodología de análisis forense de evidencias electrónicas en los procesos de adquisición, preservación, análisis, documentación y presentación de la información obtenida en una evidencia digital, desarrollando el proceso de análisis como aquel procedimiento en el cual se identifican y catalogan por familias los rastros que han sido o son generados en una

evidencia digital para finalmente con ayuda de soluciones forenses validadas recuperar e interpretar la información obtenida. Las metodologías de análisis forenses expuestas en estos estándares, guías de buenas prácticas y manuales en ningún caso abordan de manera específica la idiosincrasia de las aplicaciones de mensajería instantánea, más allá de la catalogación de las mismas con dependencia del tipo de evidencia electrónica. En el caso de los estudios técnico-forenses realizados específicamente sobre los diferentes clientes de este tipo de aplicaciones se observa que la metodología utilizada se centra en gran medida en el resultado obtenido del análisis comparativo realizado a través de soluciones comerciales forenses o de caja negra. El único método de estudio incluido en la metodología desarrollada en estos estudios consiste en la adquisición y análisis forense estático de los rastros generados por este tipo de aplicaciones en una evidencia electrónico a partir de una batería de casos de uso. Este único método de estudio permite identificar los artefactos generados en una evidencia electrónica si bien puede limitar los resultados obtenidos en cuanto a la decodificación e interpretación de la información por cuanto a la batería de casos seleccionados además de por las soluciones forenses utilizadas.

Ninguno de estos estándares, guías de buenas prácticas, manuales o estudios técnico-forenses desarrollan una metodología específica para el análisis forense de las aplicaciones de mensajería instantánea que permita afrontar desde una perspectiva global el examen de este tipo aplicaciones, más allá del análisis comparativo de artefactos de un determinado cliente. El análisis forense realizado sobre este tipo de aplicaciones se centra en los artefactos generados por el cliente móvil en un teléfono inteligente, obviando el resto de los registros generados por los clientes de escritorio o web en cualquier otro dispositivo electrónico.

La investigación realizada como parte de esta Tesis infiere la necesidad de disponer de una metodología específica permita englobar las diferentes casuísticas del análisis forense de las aplicaciones de mensajería instantánea y que pueda ser desarrollada con independencia de la versión o cliente de la aplicación de mensajería instantánea, así como del sistema operativo o dispositivo electrónico analizado. La metodología de análisis forense de aplicaciones de mensajería instantánea propuesta se compone de tres métodos complementarios entre si los cuales incorporan procedimientos y técnicas auditables, reproducibles y defendibles. Estos tres métodos responden al estudio de fuentes abiertas, al estudio de artefactos como suma del análisis forense estático y dinámico, y al estudio de código fuentes.

El estudio de fuentes abiertas pretende ser el método inicial de análisis y dependerá en gran medida de la popularidad de la aplicación de mensajería instantánea analizada y del tipo de información proporcionada por el desarrollador. En este estudio se realiza una búsqueda de toda aquella fuente de datos fiable que pueda proporcionar cualquier información respecto a la aplicación. De toda esta información recopilada se realizará un análisis detallado, desechando toda aquella información que no aporte conocimiento sobre la aplicación de mensajería instantánea. Basta decir que este estudio debe ser realizado de manera recurrente, ya que, la cantidad de documentación que se genera actualmente es constante.

El estudio de artefactos pretende aportar más información al análisis y apoyar la obtenida del estudio de fuentes abiertas. Este estudio se subdivide en análisis forense estático forense y análisis forense dinámico, siendo necesario realizar primero el análisis forense estático de una aplicación de mensajería instantánea para poder llevar a cabo de manera correcta el análisis forense dinámico. El análisis forense estático forense difiere bastante poco del realizado en los estudios técnico-forenses expuestos y consiste en el examen comparativo de los artefactos generados por la aplicación de mensajería instantánea en una evidencia electrónica. El análisis forense dinámico, por su parte añade un nivel más al análisis y permite hacer frente a las limitaciones que pueden encontrarse durante el análisis forense estático. El análisis forense dinámico permite a través de técnicas forenses imitar el normal uso de una aplicación de mensajería instantánea en la evidencia electrónica posibilitando de este modo el acceso a la información que está generando la aplicación de mensajería instantánea en un sistema encendido y por ende la obtención a las comunicaciones de usuario.

El estudio de código fuente pretende ser el método final de análisis, ya que el mismo implica un mayor nivel de especialización. Este estudio pretende aportar más información al análisis y apoyar la obtenida en los dos estudios previos. En este estudio se analizan e interpretan las líneas de código en las que se encuentra desarrollada la aplicación de mensajería instantánea.

La suma del estudio de fuentes abiertas, de artefactos y de código fuentes incluidas en la metodología de análisis forense propuesta proporciona del conocimiento funcional, técnico y forense necesario para identificar, decodificar e interpretar los datos generados por este tipo de aplicaciones con independencia de la versión, clientes, sistema operativo

o dispositivo electrónico. Así mismo, la suma de estudios permite identificar y corroborar la información obtenida por cada uno de los estudios validando con ello la integridad de los datos obtenidos.

La metodología de análisis propuesta en la presente investigación ha sido utilizada en el desarrollo de diversos estudios técnico-forenses, permitiendo llevar a cabo el análisis forense del cliente móvil de la aplicación de mensajería instantánea Telegram Messenger para los sistemas operativos Windows Phone y Android, el análisis forense del cliente de escritorio de las aplicaciones de mensajería instantánea Telegram Messenger y WhatsApp para el sistema operativo macOS, así como el análisis forense de los registros generados por el sistema notificaciones en el sistema operativo Nucleus RTOS.

Como ha quedado demostrado en los diferentes estudios técnico-forenses realizados, la metodología de analisis propuesta conlleva una serie de ventajas en cuanto a las metodologías actuales utilizadas para análisis forense de aplicaciones de mensajería instantánea. La suma de estudios incluidos en la metodología de análisis propuesta pretende complementar y apoyar la información obtenida en cada uno de los diferentes estudios retroalimentándose, tal y como queda reflejado en los estudios técnico-forenses realizados.

En el caso del cliente móvil de las aplicaciones de mensajería instantánea Telegram Messenger para el sistema operativo Windows Phone y Android, el estudio de fuentes abiertas identifica las diferentes estructuras de datos que utiliza la aplicación de mensajería instantánea para albergar la información de las comunicaciones de usuario. El estudio de artefactos (análisis forense estático), junto con la información obtenida del estudio de fuentes abiertas, permite identificar, decodificar e interpretar los rastros generados por este cliente. Por último, el estudio de código fuente, junto a la información obtenida de los otros dos estudios, permite identificar y decodificar la información ilegible realizando las transformaciones necesarias para su correcta visualización

En el caso del cliente de escritorio de las aplicaciones de mensajería instantánea Telegram Messenger y WhatsApp para el sistema operativo macOS, el estudio de fuentes abiertas permite identificar las diferentes estructuras de datos que utiliza la aplicación de mensajería instantánea para albergar la información de las comunicaciones de usuario en el caso de la aplicación Telegram Messenger, no encontrándose datos con respecto a la aplicación WhatsApp. El estudio de artefactos (análisis forense estático), junto con la

información obtenida del estudio de fuentes abiertas, permite identificar, decodificar e interpretar alguno de los rastros generados por el cliente de escritorio. Por último, el estudio de código fuente, junto a la información obtenida de los otros dos estudios, permite identificar la información ilegible. La suma de estudios expuestos permite concluir que la información relativa a las comunicaciones de usuario generadas por el cliente de escritorio de las aplicaciones de mensajería instantánea estudiadas, se almacena de forma cifrada en el equipo informático no siendo posible la obtención de las mismas a partir el estudio de fuentes abiertas, estudio de artefactos (análisis forense estático de artefactos) y estudio de código fuentes. En este sentido es necesario realizar el estudio de artefactos, como suma del análisis forense estático y dinámico de artefactos, para obtener las comunicaciones mantenidas a través del escritorio estudiados.

En el caso de los registros generados por el sistema notificaciones en el sistema operativo Nucleus RTOS, el estudio de fuentes abiertas proporciona diversos datos técnicos referentes al sistema de archivos del sistema operativo. El estudio de artefactos (análisis forense estático), junto con la información obtenida del estudio de fuentes abiertas, permite identificar, decodificar e interpretar los rastros generados por la aplicación en el dispositivo electrónico. Por último, el estudio de código fuente no aporta información para su uso en el análisis forense.

Si bien, como también ha quedado demostrado en los diferentes estudios técnico-forenses realizados, la metodología de analisis propuesta conlleva una serie de dificultades a diferencia de las metodologías utilizadas actualmente en el análisis forense de aplicaciones de mensajería instantánea. La suma de tres métodos de estudios implica un mayor nivel de formación y especialización, así como una mayor cantidad de recursos.

En el caso del estudio de fuentes abiertas, el desarrollador de una aplicación de mensajería instantánea no siempre proporciona información respecto a la misma, o si la facilita, esta se centra más en las capacidades funcionales de la aplicación que en la parte técnica. Así mismo, la popularidad de la aplicación de mensajería instantánea puede ser uno de los mayores escollos en el estudio de fuentes abiertas, ya que, a menor popularidad menos documentación existirá. En este sentido, el estudio de fuentes abiertas queda en gran medida supeditado al análisis de aquellos estudios publicados en la comunidad forense.

De igual manera, en el caso del estudio de código fuente, al igual que sucede con el estudio de fuentes abiertas, no siempre el desarrollador de una aplicación de mensajería

instantánea proporciona el código fuente de la aplicación, o si lo facilita, puede ocultar u ofuscar parte de su contenido. En este sentido, el estudio de código fuente de la aplicación queda supeditado en gran medida al análisis de las líneas de código fuente proporcionado por un tercero o al análisis de las líneas de código obtenido a partir de procesos de ingeniería inversa.

Esta metodología de análisis pretende alejarse de aquellas soluciones comerciales forenses automatizadas o de caja negra, las cuales, pueden omitir o incluso interpretar de manera incorrecta los registros generados por los diferentes clientes de las aplicaciones de mensajería instantánea. En este sentido, tal y como ha quedado reflejado en los diferentes estudios técnico-forenses realizados como parte de la presente investigación, el análisis forense realizado por estas soluciones forenses comerciales sobre los diferentes clientes de las aplicaciones de mensajería instantánea estudiadas en el momento de su realización era escueto o nulo.

A continuación, se exponen las contribuciones resultantes de la investigación y que han sido desarrolladas en la presente tesis.

7.2 Contribuciones e implicaciones de la investigación.

7.2.1 Propuesta de una metodología de análisis forense de aplicaciones IM

En este punto se expone la contribución resultante de la propuesta de una nueva metodología de análisis forense de aplicaciones de mensajería instantánea.

La diversidad de dispositivos digitales, de sistemas operativos, y de aplicaciones de mensajería instantánea sumado a su uso en la comisión de hechos delictivos, acarrea que, deban elaborase estudios técnicos-forense en los cuales se describan los rastros generados por las diferentes aplicaciones de mensajería instantánea con independencia del sistema operativo o dispositivo digital analizado. De igual manera, la continua evolución de las aplicaciones de mensajería instantánea (cantidad de funcionalidades, numero de versiones, diversidad de clientes, etc.) conlleva una transformación de los procedimientos tanto de adquisición como de análisis forense.

Como respuesta, se propone una nueva metodología de análisis, la cual permite el examen forense de aplicaciones de mensajería instantánea, con independencia del dispositivo digital, sistema operativo, aplicación o cliente utilizado. Esta metodología, ha sido desarrollada en diversos estudios científicos-técnicos-forenses exponiéndose los resultados obtenidos del examen de diferentes clientes de diversas aplicaciones de mensajería instantánea. A partir de la suma de métodos de estudio incluida en la metodología de análisis propuesta se identifica, decodifica, interpreta y valida la información generada por las aplicaciones de mensajería instantánea más allá del análisis comparativo de registros.

La metodología de análisis propuesta en la presente tesis está compuesta por la suma de tres métodos de estudio.

- Estudio de fuentes abiertas, en el cual se realiza una búsqueda recurrente y un análisis de cualquier tipo de información ubicadas en fuentes de datos abiertas, semiabiertas o cerradas.

- Estudio de artefactos, en el cual se utilizan los métodos de adquisición y análisis forense para el examen de los rastros generados en un determinado dispositivo digital. El estudio de artefactos es la suma del análisis forense estático y análisis forense dinámico. El primer análisis se realizada sobre los registros de un dispositivo apagado, siendo el segundo análisis el que se realiza sobre los registros que están siendo generados en un dispositivo encendido.
  El análisis forense dinámico se lleva a cabo posteriormente al análisis forense estático y siempre a partir de procedimientos forenses. Este estudio de artefactos dependerá en gran medida del dispositivo digital, sistema operativo, aplicación de mensajería instantánea, cliente o versión analizada. Los resultados obtenidos en el estudio de fuentes abiertas son utilizados para identificar, decodificar, interpretar, apoyar y validar los datos obtenidos del estudio de artefactos.

- Estudio de código fuente, en el cual se realiza un análisis de las líneas de programación en el cual se encuentre desarrollado el elemento digital

investigado.

Este es utilizado para identificar e interpretar la información que no haya sido posible obtener a partir del estudio de fuentes abiertas y del estudio de artefactos, de igual manera que este estudio es utilizado para validar los resultados obtenidos en los demás estudios.

Se concluye que, al aplicar la metodología de análisis propuesta en la presente Tesis, se proporciona el conocimiento funcional, técnico y forense necesario, para el correcto desarrollo de un examen forense, permitiendo identificar los rastros generados por las aplicaciones de mensajería instantánea con independencia de dispositivo digital, sistema operativo, aplicación, cliente o versión. De igual manera, la suma del estudio de fuentes abiertas, del estudio de artefactos y del estudio de código fuente permite identificar e interpretar tanto los datos legibles como los datos no legibles, pudiéndose efectuar llegado el caso, las transformaciones necesarias para su correcta interpretación. De igual modo, se puede utilizar la suma de estos tres métodos tanto para validar la información extraída de los dispositivos digitales analizados, así como para verificar la integridad de los registros obtenidos.

7.2.2 Análisis forense sobre clientes móviles de aplicaciones de IM

En este punto se expone la contribución relativa a los estudios técnico-forenses realizados sobre clientes móviles de aplicaciones de mensajería instantánea.

Los estudios realizados como parte de esta tesis contribuyen de forma específica al análisis forense del cliente móvil de la aplicación de mensajería instantánea Telegram Messenger. Estos estudios, no solo exponen de forma teórica la metodología de análisis propuesta, sino que además desarrollan de manera practica la suma de estudios (fuentes abiertas, artefactos y código fuente) incluidos en esta. A partir de la suma de estos estudios se ha logrado identificar, interpretar y validar tanto los datos relativos a las comunicaciones de usuario como los registros relativos al cliente móvil para los sistemas operativos móviles Android y Windows Phone.

En el examen forense realizado sobre los registros que genera al cliente móvil de la aplicación Telegram Messenger sobre los sistemas operativos Android y Windows Phone

se expone el análisis realizado sobre los registros generados en varios dispositivos, identificando la organización de los datos que almacenan la información de las comunicaciones de usuario y obteniendo como resultado las preferencias y configuración de la aplicación así como la información relativa a las comunicaciones de usuario (contactos, conversaciones, mensajes normales y secretos, archivos multimedia, etc.).

Cabe mencionar que en relación con el examen forense del cliente móvil para Windows Phone, no existía ningún documento previo, siendo el primer estudio técnico-forenses el desarrollado como parte de esta Tesis. De igual modo, con relación al examen forense del cliente móvil para Android, si bien existía documentación forense previa, esta se desarrolla única y específicamente en base al análisis forense estático de artefactos. Una vez examinada esta documentación y vista la necesidad, se desarrolla como parte de esta Tesis, el estudio técnico-forenses a partir de la metodología de análisis propuesta en el cual se identifica, interpreta y valida la información generada por este cliente, así como la omitida en la documentación.

Los estudios técnico-forenses realizados sobre el cliente móvil de la aplicación de mensajería instantánea Telegram Messenger en Android y Windows Phone son novedosos, ya que los mismos aportan además de una nueva metodología de análisis forense, la información relativa a los registros generados por estos clientes móviles no existente hasta la fecha.

7.2.3 Análisis forense sobre clientes de escritorio de aplicaciones de IM

En este punto se expone la contribución relativa a los diferentes estudios técnico-forenses realizados sobre diversos clientes de escritorio de las principales aplicaciones de mensajería instantánea que existen actualmente.

Los estudios realizados como parte de esta tesis contribuyen de forma específica al análisis forense del cliente de escritorio de las aplicaciones de mensajería instantánea WhatsApp y Telegram Messenger. Estos estudios, no solo exponen de forma teórica la metodología de análisis propuesta, sino que además desarrollan de manera practica la suma de estudios incluidos en esta. A partir de los estudios de fuentes abiertas, artefactos y código fuente se identifican, decodifican, interpretan tanto los datos relativos a las comunicaciones de usuario como los registros relativos a la configuración del cliente

móvil de las aplicaciones de mensajería instantánea WhatsApp y Telegram Messenger en el sistema operativo de escritorio macOS.

En el estudio técnico-forense realizado sobre los registros que genera al cliente de escritorio de la aplicación WhatsApp y Telegram Messenger sobre el sistema operativo macOS, se expone el análisis realizado sobre los registros generados por varios clientes de escritorio, identificando la organización de la información relativa a la aplicación y al usuario y obteniendo como resultado los registros relativos a las comunicaciones de usuario (contactos, conversaciones, mensajes, archivos multimedia, etc.) a partir de la metodología de análisis forense propuesta en la presente Tesis.

Cabe mencionar que en relación con el examen forense del cliente de escritorio de las aplicaciones de mensajería instantánea WhatsApp y Telegram Messenger, no existía ningún documento previo, siendo el primer estudio técnico-forenses forense el desarrollado como parte de esta Tesis.

Los estudios técnico-forenses realizados sobre el cliente de escritorio de las aplicaciones de mensajería instantánea WhatsApp y Telegram Messenger sobre el sistema operativo macOS son novedosos, ya que, los mismos aportan además de una nueva metodología de análisis, información no existente hasta la fecha sobre estos clientes de escritorio, la cual permiten obtener las comunicaciones del usuario a partir de procedimientos forenses.

7.2.4 Análisis forense sobre relojes inteligentes

En este punto se expone la contribución relativa a los diferentes estudios técnico-forenses realizados sobre clientes de escritorio de aplicaciones de mensajería instantánea.

Los estudios realizados como parte de esta tesis contribuyen de forma específica al análisis forense de los registros digitales generados en relojes inteligentes con sistema operativo Nucleus RTOS. Estos estudios, no solo exponen de forma teórica la metodología de análisis propuesta, sino que además desarrollan de manera practica la suma de estudios (fuentes abiertas, artefactos y código fuente) incluidos en esta. A partir de la suma de estos estudios se identifican, interpretan y validan los datos relativos a las comunicaciones de usuario en el sistema operativo Nucleus RTOS.

En el examen forense realizado sobre relojes inteligentes con sistema operativo Nucleus RTOS, se ha realizado un análisis comparativo sobre los registros generados en varios dispositivos, identificando la organización de los datos que almacenan la información de las comunicaciones de usuario y obteniendo como resultado los registros relativos a la agenda de contactos, registro de llamadas, mensajes de texto, notificaciones e información relativa al dispositivo vinculado.

Cabe mencionar que en relación con el examen forense de los registros generados en relojes inteligentes con sistema operativo Nucleus RTOS, no se ha encontrado documentación de ámbito forense previa, siendo el primer estudio técnico-forenses desarrollado como parte de esta Tesis.

Los estudios técnico-forenses realizados sobre los relojes inteligentes con sistema operativo Nucleus RTOS son novedosos, ya que, los mismos aportan información sobre los registros generados en este tipo de relojes no existente hasta la fecha.

7.3 Trabajos futuros

El análisis forense de evidencias digitales resulta tan amplio como la diversidad de dispositivos electrónicos, sistemas operativos y aplicaciones incluidos en la comisión de hechos delictivos. La investigación desarrollada en la presente Tesis pretende establecer una metodología de análisis forense especifica para las aplicaciones de mensajería instantánea en evidencias electrónicas.

Como líneas de trabajo de futuro de la investigación desarrollada como parte de esta Tesis se proponen los siguientes:

- Trabajar para lograr la inclusión en un estándar la metodología de análisis forense propuesta para el desarrollo de la documentación técnica-forense. Esta documentación permitirá conocer de forma detallada los procesos científicos utilizados en la identificación, decodificación y tratamiento de la información generada por de las aplicaciones de mensajería instantánea, proporcionando al especialista del conocimiento funcional, técnico y forense necesario para defender ante la Autoridad Judicial el análisis forense realizado sobre este tipo de aplicaciones.

- Incluir los estudios técnico-forenses desarrollados a partir de la metodología de análisis forense propuesta como base documental en herramientas gratuitas como "IM Analyzer". Así mismo, a partir de los estudios técnico-forenses realizados, desarrollar procesos automatizados para el análisis forense de las diferentes versiones de cada uno de los clientes de las aplicaciones de mensajería instantánea.
- Ampliar el uso de la metodología propuesta para el análisis forense de cualquier cliente con independencia de la aplicación de mensajería instantánea, sistema operativo, dispositivo electrónico. Utilizar la suma de estudios incluidos en la metodología propuesta para realizar el análisis forense de nuevas versiones y clientes no incluidos en las soluciones forenses automatizadas. Así mismo, utilizar la metodología de análisis forense propuesta para verificar el resultado obtenido por estas soluciones.
- Comprobar la validez de la metodología propuesta en la presente investigación para el análisis forense de cualquier tipo de aplicación. La diversidad de delitos informáticos y de aplicaciones utilizadas para la comisión de hechos delictivos conlleva que estas deban ser analizadas a partir de procedimientos científicos obteniendo toda aquella información generada por estas aplicaciones. Utilizar la suma de estudios incluidos en la metodología propuesta en el análisis forense de las aplicaciones contenidas en las evidencias electrónicas, identificando, decodificando, interpretando y validando toda la información digital que pueda servir como medio de prueba electrónica en los procesos judiciales.

8 ANEXO – RESUMEN DE PUBLICACIONES

Finalmente, en este octavo punto se enumeran y describen brevemente las distintas publicaciones resultantes como parte de la investigación realizada, dando cuenta del interés que suscita está en el ámbito de las Ciencias Forenses.

8.1 Forensic analysis of Telegram Messenger for Windows Phone.

El artículo *Forensic analysis of Telegram Messenger for Windows Phone* (Gregorio, J., Gardel, A., & Alarcos, B., 2017) publicado en la revista Digital Investigation (JCR Q3), expone el estudio técnico-forenses realizado sobre los registros que genera el cliente móvil de la aplicación de mensajería instantánea Telegram Messenger sobre un teléfono inteligente con sistema operativo Windows Phone.

En el mismo se desarrolla el examen forense realizado, detallando como se organizan y estructuran los datos generados por el cliente móvil de la aplicación de mensajería instantánea Telegram Messenger, en pos de exponer esta información de forma clara y relacionada. Debido a las múltiples funcionalidades disponibles de este tipo de aplicaciones, este examen se centra en la decodificación de la información que viene siendo utilizada en la comisión de hechos delictivos, como es, la identificación de los diferentes tipos de contactos, grupos, mensajes normales y secretos, transferencia de archivos y la interpretación de su contenido.

Este artículo ha sido desarrollado a partir de la metodología de análisis propuesta en esta tesis, cuya suma de métodos de estudio permite obtener los registros generados por el cliente móvil y verificar la integridad de la información obtenida.

8.2 Forensic analysis of Nucleus RTOS on MTK smartwatches.

El artículo *Forensic analysis of Nucleus RTOS on MTK smartwatches* (Gregorio, J., Alarcos, B., & Gardel, A., 2019) publicado en la revista Digital Investigation (JCR Q3), expone el estudio técnico-forenses realizado sobre los rastros digitales que pudieran

quedar almacenados en un reloj inteligente de bajo coste con sistema operativo Nucleus RTOS.

En el mismo se desarrolla el examen forense realizado sobre diferentes relojes inteligentes con sistema operativo Nucleus RTOS, detallando como se organizan y estructuran los datos de este sistema operativo, en pos de obtener de los datos extraídos la información de forma relacionada. Se identifica y decodifica la información que viene siendo utilizada en la comisión de hechos delictivos, como es, la identificación de los diferentes datos de contacto, registros de llamadas, mensajes de texto, notificaciones y conexiones de tipo *Bluetooth*.

Este artículo ha sido desarrollado a partir de la metodología de análisis propuesta en esta tesis, cuya suma de métodos de estudio permite obtener los registros generados en el dispositivo wearable y verificar la integridad de la información obtenida.

8.3 The Evolution of Instant Messaging Applications from a Forensic Perspective.

El artículo *The Evolution of Instant Messaging Applications from a Forensic Perspective* (Gregorio, J., Gardel, A. & Alarcos, B., 2018a) publicado en la revista Forensic Science & Addiction Research analiza los métodos forenses utilizados para la adquisición de evidencias digitales incluidos en la comisión de hechos delictivos.

Cada vez más, las aplicaciones de mensajería instantánea utilizan servicios basados en la nube, ofreciendo a sus usuarios total disponibilidad a sus comunicaciones indistintamente del dispositivo utilizado. El usuario de este tipo de aplicaciones puede acceder desde cualquier lugar a sus datos, ya que, la información o una copia de la misma, se encuentra almacenada en servidores de la propia aplicación. De igual manera, este tipo de aplicaciones proporcionan al usuario diferentes formas de acceso a sus comunicaciones, ya sea a partir de un cliente móvil instalado en un teléfono inteligente, de un cliente de escritorio instalada en un equipo informático o incluso de un cliente web a través de un navegador web.

En este estudio se describe la transformación que están sufriendo las aplicaciones de mensajería instantánea y cómo deben evolucionar los actuales métodos tanto de adquisición como análisis forense de este tipo de aplicaciones si se pretende obtener la información relativa a las comunicaciones de usuario con las suficientes garantías legales.

8.4 Contribuciones al análisis forense de evidencias digitales procedentes de aplicaciones de mensajería instantánea y su uso en el análisis forense de la aplicación WhatsApp Desktop en macOS.

El artículo *Contribuciones al análisis forense de evidencias digitales procedentes de aplicaciones de mensajería instantánea y su uso en el análisis forense de la aplicación WhatsApp Desktop en macOS* (Gregorio, J., 2018a) publicado en la revista técnica Ciencia Policial del Cuerpo Nacional de Policía, expone el estudio técnico-forense realizado sobre los rastros digitales que genera el cliente de escritorio de la aplicación de mensajería instantánea WhatsApp sobre el sistema operativo macOS y las casuísticas de este tipo de aplicaciones. En este artículo se desarrolla el análisis forense llevado a cabo sobre el cliente de escritorio de la aplicación WhatsApp, identificando y decodificando los datos generados por este.

En este artículo se desarrolla la metodología de análisis propuesta en esta tesis, suma de tres métodos de estudio, los cuales permiten identificar, decodificar e interpretar la información relativa a los rastros generados por el cliente de escritorio de la aplicación de mensajería instantánea WhatsApp en macOS verificando la integridad de la información obtenida. De igual manera, a partir de esta metodología de análisis propuesta se obtiene la información relativa a las comunicaciones de usuario, las cuales a través del análisis forense estático de artefactos no pueden ser recuperadas al encontrarse cifradas.

8.5 Contribuciones al análisis forense de evidencias digitales procedentes de aplicaciones de mensajería instantánea y su uso en el análisis forense de la aplicación Telegram Messenger en Android.

El artículo *Contribuciones al análisis forense de evidencias digitales procedentes de aplicaciones de mensajería instantánea y su uso en el análisis forense de la aplicación Telegram Messenger en Android* (Gregorio, J., 2018b) publicado en la revista técnica Ciencia Policial del Cuerpo Nacional de Policía expone, el estudio técnico-forenses

realizado sobre los rastros digitales que genera el cliente móvil de la aplicación de IM Telegram Messenger sobre el sistema operativo Android.

En el mismo se desarrolla el examen forense realizado, detallando como se organizan y estructuran los datos generados por el cliente móvil de la aplicación Telegram Messenger, en pos de exponer esta información de forma clara y relacionada. Debido a las múltiples funcionalidades disponibles en las aplicaciones de IM, este examen se centra en la decodificación de la información que viene siendo utilizada en la comisión de hechos delictivos, como es, la identificación de los diferentes tipos de contactos, grupos, mensajes normales y secretos, transferencia de archivos y la interpretación de su contenido.

Este articulo ha sido desarrollado a partir de la metodología de análisis propuesta en esta tesis, cuya suma de métodos de estudio permite obtener los registros generados por el cliente móvil examinado, así como verificar la integridad de la información obtenida.

8.6 Forensic analysis of Telegram Messenger Desktop on macOS.

El artículo *Forensic analysis of Telegram Messenger Desktop on MacOS* (Gregorio, J., Gardel, A. & Alarcos, B., 2018b) publicado en la revista International Journal of Research in Engineering and Science expone, el estudio técnico-forenses realizado sobre los rastros digitales que genera el cliente de escritorio de la aplicación de mensajería instantánea Telegram Messenger sobre el sistema operativo macOS y las casuísticas de este tipo de aplicaciones. En este artículo se desarrolla el análisis forense llevado a cabo sobre el cliente de escritorio de la aplicación Telegram Messenger, identificando y decodificando los datos generados por este.

En este articulo se desarrolla la metodología de análisis propuesta en esta tesis, suma de tres métodos de estudio, los cuales permiten identificar, decodificar e interpretar la información relativa a los rastros generados por el cliente de escritorio de la aplicación Telegram Messenger en macOS verificando la integridad de la información obtenida. De igual manera, a partir de esta metodología de análisis propuesta se obtiene la información relativa a las comunicaciones de usuario, las cuales a través del análisis forense estático de artefactos no pueden ser recuperadas al encontrarse cifradas.

8.7 Relojes Inteligentes. Desde su identificación a su análisis forense.

El artículo *Relojes Inteligentes. Desde su identificación a su análisis forense* (Gregorio, J., 2018c) publicado en el III Anuario Internacional de Criminología y Ciencias Forenses de la Sociedad Española de Criminología y Ciencias Forenses analiza, el impacto de los relojes inteligentes desde la perspectiva de su uso en la comisión de hechos delictivos. Este articulo razona la importancia de este tipo de dispositivos digitales en la investigación de delitos, exponiendo los procedimientos de identificación, recogida y preservación previos a su examen forense. Así mismo, en este artículo se desarrollan los actuales métodos de adquisición y análisis forense de los relojes inteligentes, exponiendo la falta de soluciones forenses especializadas para el examen de los relojes inteligentes.

8.8 Avances en los métodos forenses de adquisición y análisis forense de las aplicaciones de mensajería instantánea: Primeros resultados.

El artículo *Avances en los métodos forenses de adquisición y análisis forense de las aplicaciones de mensajería instantánea: Primeros resultados* (Gregorio, J., 2019) publicado en el libro Séptimas Jornadas de Jóvenes Investigadores de la Universidad de Alcalá, expone los resultados obtenidos durante los tres primeros años de investigación. En estos primeros años se hace una revisión del estado en el cual se encuentra el análisis forense de los diferentes dispositivos digitales incluidos en la comisión de hechos delictivos y más concretamente del estado del análisis forense de las aplicaciones de mensajería instantánea. Este articulo hace hincapié en la evolución que están sufriendo las aplicaciones de mensajería instantánea y en la necesidad de una metodología de análisis forense especifica que permita identificar, decodificar e interpretar la información generada por este tipo de aplicaciones al objeto de obtener las comunicaciones de usuario contenidas en los dispositivos electrónicos incluidos en la comisión de hechos delictivos.

9 Referencias bibliográficas

About Apple File System. (2018). Recuperado el 18 de junio 2018, de: https://developer.apple.com/documentation/foundation/file_system/about_apple_file_system.

Al Barghuthi, N.B. & Said, H.E. (2013). Social Networks IM Forensics: Encryption Analysis. *Journal of Communications, 8* (11), pp. 708-715. doi: 10.12720/jcm.8.11.708-715.

Al Mutawa, N., Baggili, I., & Marrington, A. (2012). Forensic analysis of social networking applications on mobile devices. *Digital Investigation, 9*, pp. 24-33. doi:10.1016/j.diin.2012.05.007

Alabdulsalam, S., Schaefer, K., Kechadi, T., & Le-Khac, N. (2018). Internet of things forensics: Challenges and case study. Peterson G., Shenoi S. (eds) *Advances in Digital Forensics XIV. DigitalForensics 2018. IFIP Advances in Information and Communication Technology, 532, 3-5 de enero 2018.* New Delhi, India, pp. 35-48. doi:10.1007/978-3-319-99277-8_3.

Alenezi, A., Atlam, H., & Wills, G. (2019). Experts reviews of a cloud forensic readiness framework for organizations. *Journal of Cloud Computing, 8*(1), pp. 1-14. doi:10.1186/s13677-019-0133-z.

Alex, M., & Kishore, R. (2016). Forensic model for cloud computing: An overview. *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, *23-25 de marzo 2016*. Chennai, India, pp. 1291-1295. doi: 10.1109/WiSPNET.2016.7566345

Alghafli, K. A., Jones, A., & Martin, T. A. (2011). Guidelines for the digital forensic processing of smartphones. *9th Australian Digital Forensics Conference*, *5-7 de diciembre 2011*. Edith Cowan University, Perth Western Australia, pp. 1-8. doi:10.4225/75/57b2b82a40ce7.

Aminnezhad, A., Dehghantanha, A., Abdullah, M.T. & Damshenas, M. (2013). Cloud Forensics Issues and Opportunities. *International Journal of Information Processing and Management, 4* (4), pp. 76-85. doi: 10.4156/ijipm.vol4.issue4.9.

Andrade, R. (25 de septiembre de 2019). *Top 5 Reasons Why You Should Use Axiom with Your UFED Extractions*. [Mensaje en un blog]. Recuperado de: https://www-magnetforensics-com.cdn.ampproject.org/c/s/www.magnetforensics.com/blog/top-5-reasons-why-you-should-use-axiom-to-verify-your-ufed-results/amp/.

Anglano, C. (2014). Forensic analysis of WhatsApp messenger on android smartphones. *Digital Investigation, 11*(3), pp. 201-213. doi: 10.1016/j.diin.2014.04.003

Anglano, C., Canonico, M., & Guazzone, M. (2016). Forensic analysis of the ChatSecure instant messaging application on android smartphones. *Digital Investigation, 19*, pp. 44-59. doi: 10.1016/j.diin.2016.10.001

Anglano, C., Canonico, M., & Guazzone, M. (2017). Forensic analysis of telegram messenger on android smartphones. *Digital Investigation, 23*, pp. 31-49. doi: 10.1016/j.diin.2017.09.002.

Asociación Española de Normalización, UNE. (2013a). *UNE 71505-1:2013: Parte 1: Vocabulario y principios generales*. Recuperado de: https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0051411.

Asociación Española de Normalización, UNE. (2013b). *UNE 71505-2:2013: Parte 2: Buenas practicas en la gestión de las evidencias electrónicas*. Recuperado de: https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0051412.

Asociación Española de Normalización, UNE. (2013c). *UNE 71505-3:2013: Parte 3: Formados y mecanismos técnicos*. Recuperado de: https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0051413.

Asociación Española de Normalización, UNE. (2013d). *UNE 71506:2013: Metodología para el análisis forense de las evidencias electrónicas*. Recuperado de: https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0051414.

Asociación Española de Normalización, UNE. (2015). *UNE 197010:2015; Criterios generales para la elaboración de informes y dictámenes periciales sobre Tecnologías de la Información y las Comunicaciones (TIC)*. Recuperado de: https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0055393.

Asociación Española de Normalización, UNE. (2016). *UNE-EN ISO/IEC 27037:2016 (Ratificada): Directrices para la identificación, recogida, adquisición y preservación de evidencias electronicas*. Recuperado de: https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0057481.

Asociación Española de Normalización, UNE. (2016). *UNE-EN ISO/IEC 27042:2016 (Ratificada): Directrices para el análisis y la interpretación de las evidencias electrónicas*. Recuperado de: https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0057471.

Armenta Deu, M. T. (2018). Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, WhatsApp, redes sociales): Entre la

insuficiencia y la incertidumbre. *IDP Revista De Internet Derecho Y Política,* (27), pp. 67-78. doi:10.7238/idp.v0i27.3149

Arnatovich, Y. L., Wang, L., Ngo, N. M., & Soh, C. (2018). A comparison of android reverse engineering tools via program behaviors validation based on intermediate languages transformation. *IEEE Access, 6*, pp. 12382-12394. doi:10.1109/ACCESS.2018.2808340.

Ayers, R., Brothers, S., & Jansen, W. (2014). Guidelines on Mobile Device Forensics. *NIST Special Publications.* Recuperado de: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-101r1.pdf.

Ballesteros, M. (2019). Medidas de investigación tecnológica en el proceso penal: La nueva redacción de la ley de enjuiciamiento criminal operada por la ley orgánica 13/2015. *Anuario Jurídico Y Económico Escurialense,* (52), pp. 179-204. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=6883978.

Ballesteros, M., & Hernández, J. (2014). Cibercrimen: Particularidades en su investigación y enjuiciamiento/cybercrime: Particularities in investigation and prosecution. *Anuario Jurídico Y Económico Escurialense,* (47), pp. 209-233. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=4639646.

Boletin Oficial del Estado. (2015). *Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal*. Recuperado de: https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036.

Boletin Oficial del Estado. (2019). *Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal*. Recuperado de: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444.

Boletin Oficial del Estado. (2019b). *Circular 5/2019, de 6 de marzo, de la Fiscal General del Estado, sobre sobre registro de dispositivos y equipos informáticos*. Recuperado de: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-4244.

Cahyani, N., Rahman, N., Glisson, W., & Choo, K. (2017). The role of mobile forensics in terrorism investigations involving the use of cloud storage service and communication apps. *Mobile Networks and Applications, 22*(2), pp. 240-254. doi:10.1007/s11036-016-0791-8

Cano, J. J. (2015). *Computación forense: Descubriendo los rastros.* México D.F., México D.F.: Alfaomega.

Casey, E. (2010). *Handbook of digital forensics and investigation*. [Versión electrónica de Elsevier]. doi:10.1016/C2009-0-01683-3.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers and the internet*. Burlington, MA: Academic Press.

Centro Criptológico Nacional. (2015). *CCN-STIC-401. Glosario y Abreviaturas*. Recuperado de: https://www.ccn-cert.cni.es/guias/glosario-de-terminos-ccn-stic-401.html**.**

Centro Criptológico Nacional. (2017a). *CCN-CERT IA-23/17. Informe de Amenazas. Riesgos de uso de Telegram*. Recuperado de: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2443-ccn-cert-ia-23-17-riesgos-de-uso-de-telegram-1/file.html.

Centro Criptológico Nacional. (2017b). *CCN-CERT IA-21/16. Informe de Amenazas. Riesgos de uso de WhatsApp*. Recuperado de: https://www.ccn-

cert.cni.es/informes/informes-ccn-cert-publicos/1746-ccn-cert-ia-21-16-riesgos-de-uso-de-whatsapp/file.html.

Centro Criptológico Nacional. (2018a). *CCN-STIC 824 Informe Nacional del estado de seguridad de los sistemas TIC*. Recuperado de: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/542-ccn-stic-824-información-del-estado-de-seguridad/file.html.

Centro Criptológico Nacional. (2018b). *CCN-STIC-455D Guía práctica de seguridad en dispositivos móviles: iPhone (iOS 12.x)*. Recuperado de: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3158-ccn-stic-455d-guia-practica-de-seguridad-en-dispostivos-moviles-iphone-ios-12/file.html.

Centro Criptológico Nacional. (2018c). *CCN-CER IA-13/18.Informe de Amenazas. Riesgos de uso de Line*. Recuperado de: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2922-ccn-cert-ia-13-18-riesgos-de-uso-de-line/file.html.

Centro Criptológico Nacional. (2019a). *CCN-CERT IA-04/19 Informe Anual 2018 Dispositivos y comunicaciones móviles*. Recuperado de: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3464-ccn-cert-ia-04-19-informe-anual-2018-dispositivos-moviles/file.html.

Centro Criptológico Nacional. (2019b). *CCN-STIC-1606 Configuración segura de dispositivos Samsung Galaxy S10 con Android 9*. Recuperado de: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/1000-procedimientos-de-empleo-seguro/3860-ccn-stic-1606-configuracion-segura-de-dispositivos-samsung-galaxy-s10/file.html.

Centro Criptológico Nacional. (2019c). *CCN-STIC-458 Guía práctica de seguridad de macOS 10.14 Mojave.* Recuperado de: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/400-guias-generales/3845-ccn-stic-458-seguridad-macos-mojave/file.html.

Collier, P., y Spaul, B. (1992). A forensic methodology for countering computer crime. *Artificial Intelligence Review, 6*(2), pp. 203-215. doi:10.1007/BF00150234.

Cowen, D. (2013). *Computer forensics electronic resource.* New York: New York: McGraw-Hill Education.

Craiger P., Burke P., Marberry C., & Pollitt M. (2008) A Virtual Digital Forensics Laboratory. En Ray I., Shenoi S. (eds) *Advances in Digital Forensics IV. DigitalForensics 2008. IFIP — The International Federation for Information Processing, vol 285*, *28-30 de enero 2008*. Kyoto, Japon, pp. 357-365. doi: 10.1007/978-0-387-84927-0_28

Curry, S. (2009). Chapter 27 - instant-messaging security. En Vacca J. R. (Ed.), *Computer and Information Security Handbook.* (pp. 453-466). Boston: Morgan Kaufmann. doi:10.1016/B978-0-12-374354-1.00027-3.

Daniel, L. (2012). *Digital forensics for legal professionals. Understanding Digital Evidence From The Warrant To The Courtroom*. [Versión electrónica de Elsevier]. doi:10.1016/C2010-0-67122-7.

Dargahi, T., Dehghantanha, A., & Conti, M. (2017). Chapter 2 - forensics analysis of android mobile VoIP apps. En Choo K. R., Dehghantanha A.(Eds.), *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications* (pp. 7-20). Syngress. doi:10.1016/B978-0-12-805303-4.00002-2.

Delgado, J. (2013). La prueba electrónica en el proceso penal. *Diario La Ley*, (8167), pp. 1. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=4407363.

Delgado, J. (2015). La prueba del whatsapp. *Diario La Ley*, (8605), pp. 1. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=5181062.

Delgado, J. (2016). Investigación del entorno virtual: El registro de dispositivos digitales tras la reforma por LO 13/2015. *Diario La Ley*, (8693), pp. 1. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=5320721.

Digirec Mobile Forensics. (2014). *Telegram investigation*. [Mensaje en un blog]. Recuperado de: http://www.mobileforensics.eu/en/telegram-investigation/.

European Network of Forensic Science Institute. (2015). *ENFSI-BPM-FIT-01. Best Practice Manual for the Forensic Examination of Digital Technology* (Version 1). Recuperado de: http://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf.

Embedded Software Downloads. (2019) Recuperado el 12 de enero de 2019, de: https://www.mentor.com/embedded-software/request?&fmpath=/embedded-software/downloads/nucleus-source-interest_reg&id=6d73df.

Ferguson, J. (2008). *Reverse engineering code with IDA pro electronic resource*. Burlington, Mass.: Burlington, Mass.: Syngress Pub.

Figueroa, M. C., & Álvarez de Neyra. S. (2015). *La cadena de custodia en el proceso penal / carmen figueroa navarro, directora; autores, susana álvarez de neyra kappler ... et al.]*. Madrid: Madrid: Edisofer.

File Systems and Storage with Nucleus RTOS. (2019). Recuperado el 12 de enero de 2019, de: https://www.mentor.com/embedded-software/nucleus/storage.

FISCALÍA GENERAL DEL ESTADO. (2016). *Dictamen nº 1/2016 Sobre la valoración de las evidencias en soporte papel o en soporte electrónico aportadas al proceso penal como medio de prueba de comunicaciones electrónicas*. Recuperado de: https://www.fiscal.es/documents/20142/146597/Dictamen+n+1_2016+Sobre+la+valoración+de+las+evidencias+en+soporte+papel+o+en+soporte+electrónico+aportadas+al+proceso+penal+como+medio+de+prueba+de+comunicaciones+electrónicas.pdf/f1f4b75c-5a89-511d-cca5-ce94c544adf5?version=1.1.

Gamba, J., Rashed, M., Razaghpanah, A., Tapiador, J., & Vallina-Rodriguez, N. (2019). An Analysis of Pre-installed Android Software. *arXiv preprint.* arXiv:1905.02713.

G. B. Satrya, P. T. Daely, & M. A. Nugroho. (2016). Digital forensic analysis of Telegram Messenger on Android devices. *2016 International Conference on Information & Communication Technology and Systems (ICTS), 12 de octubre 2016.* Surabaya, Indonesia, pp.1-7. doi:10.1109/ICTS.2016.7910263.

García, D. (2018). *Aportación de mensajes de WhatsApp a los procesos judiciales: Tratamiento procesal*. Granada, España: Comares.

Garfinkel, S. (2013). Digital forensics. *American Scientist, 101*(5), pp. 370-377. doi:10.1511/2013.104.370

Golden, T. W. (2011). *A guide to forensic accounting investigation.* Hoboken, New Jersey: John Wiley & Sons, Inc.

GONZÁLEZ, J., A. (2013). *Delincuencia informática: daños informáticos del artículo 264 del código penal y propuesta de reforma*. (Tesis doctoral), Universidad Complutense de Madrid, Departamento de Derecho Penal, Madrid.

Graells, P. M. (2000). Las TIC y sus aportaciones a la sociedad. *Departamento De Pedagogía Aplicada, Facultad.* Recuperado de: http://www.sld.cu/galerias/pdf/sitios/santiagodecuba/las_tic_y_sus_aportaciones_a_la_sociedad.pdf.

Gregorio, J. (2018a). Contribuciones al análisis forense de evidencias digitales procedentes de aplicaciones de mensajería instantánea y su uso en el análisis forense de la aplicación WhatsApp Desktop en MacOS. *Ciencia Policial, Revista Técnica del Cuerpo Nacional de Policía, 149,* pp. 135-156. Recuperado de: https://www.policia.es/iep_web/publicaciones/ciencia_policial/pdf/cp149.pdf

Gregorio, J. (2018b). Contribuciones al análisis forense de evidencias digitales procedentes de aplicaciones de mensajería instantánea y su uso en el análisis forense de la aplicación Telegram Messenger en Android. *Ciencia Policial, Revista Técnica del Cuerpo Nacional de Policía, 145,* pp. 123-147. Recuperado de: https://www.policia.es/iep_web/publicaciones/ciencia_policial/pdf/cp145.pdf.

Gregorio, J. (2018c). Relojes Inteligentes. Desde su identificación a su análisis forense. *III Anuario Internacional de Criminología y Ciencias Forenses, Sociedad Española de Criminología y Ciencias Forenses, 3*, pp. 207-221. Recuperado de: https://revistaqdc.es/iii-anuario-internacional-de-criminologia-y-ciencias-forenses/.

Gregorio, J. (2019). Avances en los métodos forenses de adquisición y análisis forense de las aplicaciones de mensajería instantánea: Primeros resultados. *Séptimas*

Jornadas de Jóvenes Investigadores de la Universidad de Alcalá (Ciencias e Ingenierías), UAH obras colectivas. Ciencias 18, pp. 217-225. Alcalá de Henares: Universidad de Alcalá, Servicio de Publicaciones.

Gregorio, J., Gardel, A., & Alarcos, B. (2017). Forensic analysis of telegram messenger for windows phone. *Digital Investigation, 22*, pp. 88-106. doi:10.1016/j.diin.2017.07.004.

Gregorio, J., Gardel, A. & Alarcos, B. (2018a). The Evolution of Instant Messaging Applications from a Forensic Perspective. *Forensic Science & Addiction Research*. *3* (1), pp. 194-195. Recuperado de: https://crimsonpublishers.com/fsar/pdf/FSAR.000557.pdf.

Gregorio, J., Gardel, A. & Alarcos, B. (2018b). Forensic analysis of Telegram Messenger Desktop on MacOS. *International Journal of Research in Engineering and Science, 6* (8), Ver. I, pp. 39-48. Recuperado de: http://www.ijres.org/papers/Volume%206/Vol-Issue8/Version-1/F0608013948.pdf

Gregorio, J., Alarcos, B., & Gardel, A. (2019). Forensic analysis of nucleus RTOS on MTK smartwatches. *Digital Investigation, 29*, pp. 55-66. doi:10.1016/j.diin.2019.03.007.

Guardia Civil. (2018). *La Guardia Civil desarticula una red internacional de pornografía infantil*. Recuperado el 12 noviembre de 2019, de: http://www.guardiacivil.es/es/prensa/noticias/6822.html.

GUDÍN, A., E. (2014). Incorporación al proceso del material informático intervenido durante la investigación penal. *Boletín del Ministerio de Justicia,* (2163), pp. 1-21. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=4682569.

Gunasekera, S. (2012). *Android apps security electronic resource*. Berkeley, CA: Apress.

Guo, H., Jin, B., & Shang, T. (2012). Forensic investigations in Cloud environments. *2012 International Conference on Computer Science and Information Processing (CSIP)*, *24-26 de agosto 2012.* Xi'an, Shaanxi, China, pp.248-251. doi:10.1109/CSIP.2012.6308841.

Heiser, J. G., & Kruse, W. G. (2001). *Computer forensics: Incident response essentials*. Boston, Mass.; London: Addison-Wesley.

Hegarty, R. C., Lamb, D. J., & Attwood, A. (2014). Digital Evidence Challenges in the Internet of Things. En Dowland, P.S., Furnell, S.M., Guita, B.V., (eds) *Proceedings of the Tenth International Network Conference, INC 2014, 8-9 de julio 2014.* Reino Unido: Universidad de Plymounth, pp. 163-172. Recuperado de: https://www.researchgate.net/publication/288660566_Digital_evidence_challenges_in_the_internet_of_things.

Hoopes, J. (2009). *Virtualization for security: Including sandboxing, disaster recovery, high availability, forensic analysis, and honeypotting*. Burlington, MA: Syngress Pub. doi: 10.1016/B978-1-59749-305-5.X0001-1.

Husain, M.I. & Sridhar, R. (2010). iForensics: Forensic Analysis of Instant Messaging on Smart Phones. En Goel S. (eds) *Digital Forensics and Cyber Crime. ICDF2C 2009. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 31*, *30 de septiembre – 02 de octubre 2009*. Albany, NY, USA, pp. 9-18. doi:10.1007/978-3-642-11534-9_2.

Hoog, A. (2011). *Android Forensics: Investigation, Analysis and Mobile Security for Google Android (first edition)*. [Versión Electronica de Elsevier]. doi:10.1016/B978-1-59749-651-3.10007-X.

Instituto Nacional de Estadistica. (2019). *Equipamiento y uso de TIC en los hogares - Año 2019*. Recuperado el 13 de noviembre de 2019, de: https://www.ine.es/prensa/tich_2019.pdf.

International Data Corporation. (2018). *Global Wearables Market Grows 7.7% in 4Q17 and 10.3% in 2017 as Apple Seizes the Leader Position, Says IDC*. Recuperado de: https://www.idc.com/getdoc.jsp?containerId=prUS43598218.

International Organization for Standardization. (2012). *ISO/IEC 27037:2012. Guidelines for identification, collection, acquisition, and preservation of digital evidence*. Recuperado de: https://www.iso.org/standard/44381.html.

International Organization for Standardization. (2013). *ISO/IEC 27002:2013. Code of practice for information security controls*. Recuperado de: https://www.iso.org/standard/54533.html.

International Organization for Standardization. (2015a). *ISO/IEC 27042:2015 Guidelines for the analysis and interpretation of digital evidence*. Recuperado de: https://www.iso.org/obp/ui/#iso:std:iso-iec:27042:ed-1:v1:en.

International Organization for Standardization. (2015b). *ISO/IEC 27041:2015. Guidance on assuring suitability and adequacy of incident investigative method*. Recuperado de: https://www.iso.org/standard/44405.html.

Internet Engineering Task Force. (2002). *RFC 3227. Guidelines for Evidence Collection and Archiving*. Recuperado de: https://tools.ietf.org/html/rfc3227.

Internet Engineering Task Force. (2007). *RFC 4810. Long-Term Archive Service Requirements*. Recuperado de: https://tools.ietf.org/html/rfc4810.

Internet Engineering Task Force. (2007b). *RFC 4998. Evidence Record Syntax*. Recuperado de: https://tools.ietf.org/html/rfc4998.

Interpol. (2019). *Global Guidelines for Digital Forensics Laboratories*. Recuperado de: https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf

Iqbal, A., Al Obaidli, H., Marrington, A., & Jones, A. (2014). Windows surface RT tablet forensics. *Digital Investigation, 11*(1), pp. 87-93. doi:10.1016/j.diin.2014.03.011.

Iqbal, A., Marrington, A., & Baggili, I. (2013). Forensic artifacts of the ChatON instant messaging application. *2013 8th International Workshop on Systematic Approaches to Digital Forensics Engineering (SADFE), 21-22 de noviembre 2013*. Hong Kong, China, pp. 1-6. doi:10.1109/SADFE.2013.6911538.

Kanellis, P. (2006). *Digital crime and forensic science in cyberspace*. Hershey PA, Hershey PA: Idea Group Pub.

Karabiyik, U., Canbaz, M., Aksoy, A., Tuna, T., Akbas, E., Gonen, B., & Aygun, R. (2016). A survey of social network forensics. *The Journal of Digital Forensics, Security and Law: JDFSL, 11*(4), pp. 55-128. doi: 10.15394/jdfsl.2016.1430

Karpisek, F., Baggili, I., & Breitinger, F. (2015). WhatsApp network forensics: Decrypting and understanding the WhatsApp call signaling messages. *Digital Investigation, 15*, pp. 110-118. doi:10.1016/j.diin.2015.09.002.

Kent, A.K., Chevalier, S., Grance, T., Dang, H., & Kent, K. (2006). 800-86. Guide to Integrating Forensic Techniques into Incident Response. *NIST Special Publications.* Recuperado de: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf.

Keyvanpour, M., Moradi, M., & Hasanzadeh, F. (2014). Digital forensics 2.0: A review on social networks forensics. *Studies in Computational Intelligence, 555*, pp. 17-46. doi:10.1007/978-3-319-05885-6_2.

Kharpal, A. (19 de noviembre de 2015). Secretive messaging app used by IS takes down posts. *Consumer News and Businness Channel (BNBC online)*. Recuperado de: https://www.cnbc.com/2015/11/19/telegram-the-messaging-app-used-by-isis-takes-down-78-posts.html.

Kiley, M., Dankner, S., & Rogers, M. (2008). Forensic Analysis of Volatile Instant Messaging. En *Ray I., Shenoi S. (eds) Advances in Digital Forensics IV. DigitalForensics 2008. IFIP — The International Federation for Information Processing, 285, 28-30 de enero 2008*. Kyoto, Japon, pp. 129-138. doi: 10.1007/978-0-387-84927-0_11.

Ko, R. K., & Choo, R. (2015). *The Cloud Security Ecosystem: Technical, Legal, Business and Management Issues*. [Versión electrónica de Elsevier]. doi:10.1016/C2014-0-00456-X.

Levendoski, M., Datar, T., & Rogers, M. (2012). Yahoo! Messenger Forensics on Windows Vista and Windows 7. En Gladyshev P., Rogers M.K. (Eds), *Digital Forensics and Cyber Crime,* (pp 172-179). Heidelberg, Berlin: Springer.

Lillis, D., Becker, B., O'Sullivan, T., & Scanlon, M. (2016). Current challenges and future research areas for digital forensic investigation. *The 11th ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016), 24-26 de mayo 2016.* Daytona Beach, FL, USA, pp. 9-20. doi: 10.13140/RG.2.2.34898.76489.

Locard, E. (2010). *Manual de técnica policíaca*. Valladolid: Maxtor.

Luttgens, J. T., Pepe, M., & Mandia, K. (2014). *Incident response & computer forensics (third edition)*. McGraw-Hill Education.

Lundgren, J. (2015). *Will Messaging Apps Kill Sms*. [Mensaje en un blog]. Recuperado de http://www.sinch.com/opinion/will-messaging-apps-kill-sms/.

Mahajan, A., Dahiya, M., & Sanghvi, H. (2013). Forensic analysis of instant messenger applications on android devices. *International Journal of Comuter Applicaiones (0975-8887), 68*(8), pp. 38-44. doi:10.5120/11602-6965.

Marchena, M. (Magistrado). (19 de mayo de 2015). *Sentencia 300/2015, Sala Segunda, de lo Penal, Tribunal Supremo*. [Fondo documental]. Recuperado de: https://supremo.vlex.es/vid/571257698

Mestre, E. (2016). Nuevas formas de investigación de los delitos. *La Ley Penal: Revista De Derecho Penal, Procesal Y Penitenciario*, (118), pp. 1. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=5978480.

Ministerio del Interior. (2019). *Hechos conocidos de infracciones penales relacionadas con la cibercriminalidad por provincias, grupo penal y periodo (2017-2012)*. Recuperado de: https://estadisticasdecriminalidad.ses.mir.es/jaxiPx/Tabla.htm?path=/Datos5//l0/&file=05002.px&type=pcaxis&L=0.

Mrdovic, S., Huseinovic, A., & Zajko, E. (2009). Combining static and live digital forensic analysis in virtual environment. *2009 XXII International Symposium on Information, Communication and Automation Technologies, 29-31 de octubre 2009. Bosnia, Serbia,* pp. 1-6. *doi:10.1109/ICAT.2009.5348415.*

Ochoa, P. (2018). El tratamiento de la evidencia digital, una guía para su adquisición y/o recopilación. *Revista Economía Y Política*, (28), pp. 35-46. doi: 10.25097/rep.n28.2018.03.

Oertle, C. (2016). *Anwendungsanalyse des Messengers Telegram Desktop (Version 0.9.15) unter Windows 10*. [Informe Tecnico]. Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU). Departamento de Informática 1 de Friedrich. Alemania. Recuperado de: https://www1.cs.fau.de/df-whitepapers

Oliva, R., Valero, S., & Dolado, A. (2016). *LA PRUEBA ELECTRÓNICA Validez y eficacia procesal.* España: Juristas con Futuro.

Onovakpuri, P. (2018). Forensics Analysis of Skype, Viber and WhatsApp Messenger on Android Platform. *International Journal of Cyber-Security and Digital Forensics*, 7, pp. 119-131. doi:10.17781/P002369.

Oriwoh, E., Jazani, D., Epiphaniou, G., & Sant, P. (2013). Internet of things forensics: Challenges and approaches. *9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing, 20-23 de octubre 2013.* Austin, TX, USA, pp. 608-615. doi:10.4108/icst.collaboratecom.2013.254159.

O'shaughnessy, S., & Keane, A. (2013). Impact of Cloud Computing on Digital Forensic Investigations. E*n: Peterson G., Shenoi S. (eds) Advances in Digital Forensics IX. DigitalForensics 2013. IFIP Advances in Information and Communication*

Technology, vol 410, 28-30 de enero 2013. Orlando, FL, USA, pp. 291-303. doi:10.1007/978-3-642-41148-9_20

Our Exploit Acquisition Program. (2019). Recuperado el 11 de julio de 2019, de: https://zerodium.com/program.html.

Ovens, K. M., & Morison, G. (2016). Forensic analysis of kik messenger on iOS devices. *Digital Investigation, 17*, pp. 40-52. doi:10.1016/j.diin.2016.04.001.

Patterson, J. (23 de febrero de 2015). *Telegram App Store Secret-Chat Messages in Plain Text Database.* [Mensaje de un blog] Recuperado de: https://blog.zimperium.com/telegram-hack/.

Perez, V. (Magistrado). (28 de junio de 2019). *Sentencia 184/2019, Sección nº 2 de la Audiencia Provincial de Caceres.* [Fondo documental]. Recuperado de: http://www.poderjudicial.es/search/AN/openDocument/15a01d79b92616fb/20190812.

Perumal, S., Norwawi, N. M., & Raman, V. (2015). Internet of things(IoT) digital forensic investigation model: Top-down forensic approach methodology. 2015 *Fifth International Conference on Digital Information Processing and Communications (ICDIPC*), *7-9 de octubre 2015*. Sierre, Switzerland, pp.19-23. doi:10.1109/ICDIPC.2015.7323000.

Poder Judicial España. (2019). *Compendios Delitos - Año 2018*. Recuperado de: http://www.poderjudicial.es/cgpj/es/Temas/Estadistica-Judicial/Estadistica-por-temas/Datos-penales--civiles-y-laborales/Delitos-y-condenas/Actividad-del-Ministerio-Fiscal/.

Policia Nacional. (2013). *La Policía Nacional detiene a un hombre que indujo a abandonar su domicilio a un menor con el que contactó a través de Whatsapp*. Recuperado el 19 de noviembre de 2019, de: https://www.policia.es/prensa/20190205_1.html.

Policia Nacional. (2019). *La Policía Nacional detiene a ocho individuos por intercambiar pornografía infantil a través de Internet*. Recuperado el 19 de noviembre de 2019, de: https://www.policia.es/prensa/20131220_2.html

Quevedo, J. (2017). *Investigación y prueba del ciberdelito*. Madrid, Madrid: Sepín.

Ragan, S. (2015). After Paris, ISIS moves propaganda machine to Darknet. *CSO online*. Recuperado de: https://www.csoonline.com/article/3004648/after-paris-isis-moves-propaganda-machine-to-darknet.html.

Rathi, K., Karabiyik, U., Aderibigbe, T., & Chi, H. (2018). Forensic analysis of encrypted instant messaging applications on Android. *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, *22-25 de marzo 2018*. Antalya, Turkia, pp 1-6. doi: 10.1109/ISDFS.2018.8355344.

Riadi, I., & Firdonsyah, A. (2018). Forensic Analysis of Android-based Instant Messaging Application. *2018 12th International Conference on Telecommunication Systems, Services, and Applications (TSSA)*, *4-5 de octubre 2018*. Yogyakarta, Indonesia, Indonesia, pp. 1-6. doi: 10.1109/TSSA.2018.8708798

Romera, M.C. (Presidenta-Magistrada,). (19 de julio de 2019). *Sentencia 498/2019, Sección nº 27 de la Audiencia Provincial de Madrid.* [Fondo documental]. Recuperado de:

http://www.poderjudicial.es/search/AN/openDocument/196f2397cd4c6862/20190906.

Rongen, J., & Geradts, Z. (2017). Extraction and Forensic analysis of artifacts on wearables. *International Journal of Forensic Science & Pathology (IJFP) 5*(1), pp. 312-318. doi: 10.19070/2332-287X-1700070.

Ruan, K., Carthy, J., Kechadi, T., & Baggili, I. (2013). Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results. *Digital Investigation,10*(1), pp. 34-43. doi: 10.1016/j.diin.2013.02.004.

Sammons, J. (2012). *The basics of digital forensics. The Primer for Gettings Started in digital forensics*. [Versión electrónica de Elsevier]. doi:10.1016/C2010-0-68337-4.

Satrya, G.B., Daely, P.T. & Shin, S.Y. (2016). Android Forensics Analysis: Private Chat on Social Messenger. 2016 *Eighth International Conference on Ubiquitous and Future Networks (ICUFN), 5-8 de julio de 2016*. Vienna, Austria, pp. 430-435. doi:10.1109/ICUFN.2016.7537064.

Schema. (2017). Recuperado de: https://core.telegram.org/schema.

Scientific Working Group on Digital Evidence. (2013). *SWGDE Best Practices for Mobile Phone Forensic*. Recuperado de: https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Mobile%20Phone%20Forensics.

Scientific Working Group on Digital Evidence. (2017). *SWGDE Best Practices for the Acquisition of Data from Novel Digital Devices*. Recuperado de: https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20P

ractices%20for%20the%20Acquisition%20of%20Data%20from%20Novel%20Digital%20Devices.

Scientific Working Group on Digital Evidence. (2018). *SWGDE Best Practices for Computer Forensic Examination*. Recuperado de: https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Computer%20Forensic%20Examination.

Sgaras C., Kechadi M., & Le-Khac N. (2015). Forensics Acquisition and Analysis of Instant Messaging and VoIP Applications. En Garain U., Shafait, F. (eds) *IWCF 2014, Lecture Notes in Computer Science, 8915, 24 de Agosto 2014.* Stockholm, Suiza, pp. 188-199. doi:10.1007/978-3-319-20125-2_16.

Shah, M., Saleem, S., & Zulqarnain, R. (2017). Protecting digital evidence integrity and preserving chain of custody. *The Journal of Digital Forensics, Security and Law: JDFSL, 12*(2), pp. 121-129. Doi:10.15394/jdfsl/vol12/iss2/12

Shavers, B. (2008). *A Discussion of Virtual Machines Related to Forensics Analysis*. Recuperado de: http://www.forensicfocus.com/downloads/virtual-machines-forensics-analysis.pdf.

Shirkhedkar, D., & Patil, S. (2014). Analysis of various digital forensic techniques for cloud computing. *International Journal of Advanced Research in Computer Science, 5*(4), pp. 104-107. Recuperado de: https://www.ijarcs.info/index.php/Ijarcs/article/viewFile/2113/2101

Simou, S., Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2014). Cloud forensics: Identifying the major issues and challenges. *Lecture Notes in Computer Science, 8484*, pp. 271-284. doi:10.1007/978-3-319-07881-6_19

Sindhu, K., & Meshram, B. (2012). Digital forensic investigation tools and procedures. *International Journal of Computer Network and Information Security, 4*(4), pp. 39-48. doi:10.5815/ijcnis.2012.04.05.

Sommer, P. (1997). *Computer evidence: A forensic investigation handbook*. [Version electronica de Elsevier] doi:10.1016/S1361-3723(97)81033-0.

Sudozai, M. A. K., Saleem, S., Buchanan, W. J., Habib, N., & Zia, H. (2018). Forensics study of IMO call and chat app. *Digital Investigation, 25*, pp. 5-23. doi:10.1016/j.diin.2018.04.006.

Taylor, M., Haggerty, J., Gresty, D., & Hegarty, R. (2010). Digital evidence in cloud computing systems. *Elsevier Computer Law & Security Review, 26*(3), pp. 304–308. doi:10.1016/j.clsr.2010.03.002.

Teel Technologies. (9 de diciembre de 2015). *What is JTAG, Chip-off and ISP?*. [Mensaje de un blog]. Recuperado de: https://www.teeltech.com/ufaqs/what-is-jtag-chip-off-and-isp/.

Telefonica España. (2019). *Informe Transparencia Comunicaciones de Telefonica 2019*. Recuperado de: https://www.telefonica.com/documents/153952/183394/Informe-Transparencia-Comunicaciones-2019.pdf/00cb6cba-dbe7-df8d-64d1-df8510830960.

Telegram Applications. (2019). Recuperado de: https://telegram.org/apps.

Telegram Wiki. (2016). Recuperado de: https://telegram.wiki/#telegram_desktop.

TL Language. (2017). Recuperado de: https://core.telegram.org/mtproto/TL.

Trček, D., Abie, H., Skomedal, A., & Starc, I. (2010). Advanced framework for digital forensic technologies and procedures. *Journal of Forensic Sciences, 55(*6), pp. 1471–1480. doi:10.1111/j.1556-4029.2010.01528.x

Utilizar FileVault para encriptar el disco de arranque del Mac. (2018) Recuperado de: httsp://support.apple.com/es-es/HT204837.

Velasco, E. (2007). Fraudes informáticos en red. *La Ley Penal: Revista De Derecho Penal, Procesal Y Penitenciario*, (37), pp. 57-66. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=2259209.

Velasco, E. (2010). La investigación de delitos informáticos con garantías judiciales. *Telos*, (85), pp. 113-115. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=3414655.

Velasco, E. (2013). Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc. *Diario La Ley*, (8183), pp. 1. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=4453606.

Velasco, E. (2014). La prueba pericial. *Diario La Ley*, (8258), pp. 1. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=4598924.

Velasco, E. (2015). Los delitos informáticos. *Práctica Penal*, (81), pp. 14-28. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=5287595.

Velasco, R. (2017). DEFT Zero, la nueva distribución Linux lingera para análisis forense [Mensaje en un blog]. Recuperado de: https://www.redeszone.net/2017/02/14/deft-zero-la-nueva-distribución-linux-ligera-para-análisis-forense/.

Wahyudi, E., Riadi, I & Prayudi, Y. (2018). Virtual Machine Forensic Analysis And Recovery Method For Recovery And Analysis Digital Evidence. *International Journal of Computer Science and Information Security, 16*(2), pp.1-7. Recuperado de: https://www.researchgate.net/publication/323676948_Virtual_Machine_Forensic_Analysis_And_Recovery_Method_For_Recovery_And_Analysis_Digital_Evidence.

We are social. (2019). *Digital in 2019 España*. Recuperado el 5 de julio de 2019, de: https://wearesocial.com/es/digital-2019-espana.

Woollaston, V. (2013). The end of the text message? Mobile chat apps overtake SMS for the first time. D*aily Mail Online*. Recuperado de: https://www.dailymail.co.uk/sciencetech/article-2316629/The-end-text-message-Mobile-chat-apps-overtake-SMS-time.html.

Wu, S., Zhang, Y., Wang, X., Xiong, X., & Du, L. (2017). Forensic analysis of WeChat on android smartphones. *Digital Investigation, 21*, pp. 3-10. doi:10.1016/j.diin.2016.11.002

Yang, T. Y., Dehghantanha, A., Choo, K. R., Muda, Z., & Khan, M. K. (2016). Windows instant messaging app forensics: Facebook and skype as case studies. *PLoS ONE, 11*(3). doi:10.1371/journal.pone.0150300.

Yasin, M., Kausar, F., Aleisa, E., & Kim, J. (2014). Correlating messages from multiple IM networks to identify digital forensic artifacts. *Electronic Commerce Research, 14*(3), pp. 369-387. doi:10.1007/s10660-014-9145-4.

Yasinsac, A., Erbacher, R. F., Marks, D. G., Pollitt, M. M., & Sommer, P. M. (2003). Computer forensics education. *IEEE Security & Privacy, 1*(4), pp. 15-23. doi:10.1109/MSECP.2003.1219052.

Yusoff, M. N., Dehghantanha, A. & Mahmod, R. (2017). Forensic Investigation of Social Media and Instant Messaging Services in Firefox OS: Facebook, Twitter, Google++, Telegram, OpenWapp and Line as Case Studies. *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*, Chapter 4, pp. 41-62. doi:10.1016/B978-0-12-805303-4.00004-6.

Zhang, H., Chen, L., & Liu, Q. (2018). Digital Forensic Analysis of Instant Messaging Applications on Android Smartphones. *2018 International Conference on Computing, Networking and Communications (ICNC), 5-8 de marzo 2018.* Maui, HI, USA, pp. 647-651. doi: 10.1109/ICCNC.2018.8390330.