UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Universidad Internacional de La Rioja
Máster Universitario en Seguridad Informática

Metodología de intrusión en equipos para la investigación de delitos

Trabajo Fin de Máster

Presentado por: Salguero Cruz, Antonio

Director/a: Cobos Guzmán, Salvador

Ciudad: Burgos
Fecha: 05-07-2017

Resumen

El presente Trabajo de Fin de Máster persigue el **objetivo** de **crear una metodología para realizar intrusiones en equipos informáticos** (incluyendo ordenadores personales y teléfonos móviles con Sistema Operativo Android), amparándose en la reciente modificación de la Ley de Enjuiciamiento Criminal, concretamente en el artículo 588 septies y relacionados (Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, 2015).

Se analizarán, por tanto, **los requisitos legales que resultan obligatorios** para la realización de dicha intrusión, incluyendo las solicitudes a la Autoridad Judicial, así como todo el proceso de recopilación de información acerca del objetivo para poder llevar a cabo la intrusión.

Una vez propuesta la metodología, que será genérica para cualquier dispositivo informático, se podrán llevar a cabo exitosamente las diferentes intrusiones, puesto que se cumplirá con todos los requisitos (legales y operativos) necesarios.

De este modo, todas aquellas investigaciones que se realicen, contarán con todas las garantías necesarias en el proceso Penal, evitando su nulidad.

Palabras Clave: Reforma Ley de Enjuiciamiento Criminal, Registro remoto, Intrusión, Android, Ingeniería Social.

Abstract

The purpose of this Master's Degree Job is to create a new methodology for intrusions in computer devices (including personal computers and Android O.S. based smartphones), based on the recent modification of the Criminal Procedure Law, specifically article 588 septies and related (Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, 2015)

Therefore, the legal requirements that are mandatory for the execution of any intrusion, including the requests to the Judicial Authority, as well as the whole process of collecting information about the objective to be able to carry out the intrusion, will be analyzed.

Once the methodology, which will be generic for any computer device, has been proposed, different intrusions can be successfully carried out, since all necessary (legal and operational) requirements will be met.

In this way, all the investigations that are carried out, will have all the necessary guarantees in the criminal process, avoiding their nullity.

Keywords: Criminal Procedure Law Reform, Remote Record, Intrusion, Android, Social Engineering.

Índice de contenidos

Índice de imágenes

1. Introducción

El presente Trabajo nace con la finalidad de poder ofrecer **cierta seguridad a los investigadores a la hora de realizar investigaciones en las que sea necesario el uso de la medida del registro remoto** y, por lo tanto, es **necesario cumplir todos y cada uno de los requisitos que la legislación vigente marca**. Si no se cumple con alguno de los requisitos, no sería posible realizar la intrusión en un equipo informático y proceder, posteriormente, con el registro remoto, ya que la información o datos obtenidos no serían válidos en el proceso penal.

De este modo, se puede ofrecer cierto grado de seguridad a los investigadores sobre la conformidad con los requisitos legales necesarios y sobre la realización de las actividades técnicas/operativas relevantes para la investigación.

Es por ello que, **ante la falta de una metodología a seguir en las investigaciones, cuando es necesaria la realización del registro remoto de equipos informáticos**, se ofrece la **metodología planteada en el presente Trabajo de Fin de Máster**, la cual cubre desde el inicio de la investigación, hasta la finalización de la misma.

1.1 Justificación

Debido a la reciente modificación de la Ley de Enjuiciamiento Criminal (Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, 2015), a día de hoy no se tienen definidos claramente los supuestos o de qué forma práctica y con qué limitaciones, puede llevarse a cabo la medida establecida en los artículos 588 septies a, b y c, recogidos en el Capítulo IX del Título VII del Libro II, Registros remotos sobre equipos informáticos, de la citada Ley.

Se trata de un tema que no es baladí, puesto que, hoy en día, en los dispositivos electrónicos se almacena gran cantidad de información, sobre todo personal, que puede ayudar a la resolución de diversos delitos.

Como ejemplo de la importancia de estos registros remotos, en investigaciones sobre personas relacionadas con la comisión de delitos contra la salud pública, o incluso delitos de terrorismo, el acceso y registro de los equipos informáticos de los investigados facilitaría gran cantidad de información que permitiría la resolución de los mismos, ya que diversa información como contactos, imágenes o chats, se almacenan en dichos dispositivos y, tanto la

información que puede proporcionar el contenido de dichos archivos, así como la información asociada a ellos, los metadatos, pueden resultar cruciales para una investigación.

1.2 Planteamiento del trabajo

El **objetivo general**, es proporcionar un **marco o metodología a seguir**, para poder **realizar intrusiones** en equipos informáticos**, con todas las garantías legales** y de modo que el **aprovechamiento de la información recabada sea máximo,** con la finalidad de realizar un registro remoto de los citados dispositivos. De nada sirve recopilar una gran cantidad de información si luego no puede ser utilizada durante el proceso penal.

Además, al ser una **medida que limita alguno de los derechos recogidos en el artículo 18 de la Constitución Española** (Constitución Española, 1978)**, que son derechos fundamentales**, el llevarla a cabo conforme a la legislación vigente es de suma importancia, ya que la información que se puede llegar a recabar incluye aquella que se genera en la esfera personal e íntima del investigado, y por ello es una información especialmente sensible y protegida, por lo que recabar esta información sin cumplir con total rigurosidad todos los requisitos exigidos, conllevaría su anulación en el proceso penal, además de las posibles responsabilidades penales derivadas para los actuantes.

Para que se lleve a cabo esta medida limitativa, se deben **cumplir una serie de requisitos** acerca del delito que se pretende investigar. Además, se debe **cumplir con un procedimiento** para llevar a cabo dichas medidas limitativas, que pasa, obligatoriamente, por la solicitud de dichas medidas al Juez Instructor competente.

Para que dicho Juez Instructor acuerde la ejecución de dicha medida, en la solicitud que se realice se deben incluir, y justificar, todos aquellos requisitos que la legislación vigente marca.

El presente trabajo se marca como meta ofrecer un **método, desde el inicio de la investigación**, para poder saber si la adopción de la medida de los registros remotos estaría acorde con los supuestos que establece la legislación vigente y, consecuentemente, estaría permitido realizar la intrusión, previa al registro remoto.

Una vez que se tiene la certeza de que la Ley lo permite, en el caso concreto del delito a investigar, la presente metodología permitiría llevar a cabo, de una forma lógica y cronológica, todas las gestiones necesarias para proceder con la solicitud de la ejecución de la medida al Juez Instructor competente. Una vez conseguida la autorización (caso de que así fuera), también permitiría tener en cuenta los diferentes escenarios posibles en los que se pudiera llevar a cabo efectivamente.

Pero aquí no acaba el proceso, puesto que, una vez realizada la intrusión, también hay que seguir cumpliendo lo que nos indica la legislación vigente, en concreto a lo establecido respecto a la explotación de esa información adquirida durante el registro remoto. También se pretende dar un marco que proporcione seguridad a los investigadores, de modo que la información que se pudiera recabar durante la realización de los registros remotos, no sea desechada durante el proceso penal, permitiendo comprobar la integridad de todos aquellos datos que se logren recoger y de este modo, poder asociar de una forma inequívoca información-dispositivo-usuario.

1.3 Estructura de la memoria

En **primer lugar**, se describirá el **contexto actual** existente sobre los registros remotos en equipos informáticos y la relevancia social que ha adquirido su introducción en la legislación vigente.

A continuación, se describirán los **requisitos legales** necesarios para llevarla a cabo conforme a la legislación vigente y, de este modo, poder utilizar toda la información adquirida mediante dichos registros en el proceso penal, de forma que no sean anulados posteriormente.

Una vez se tiene definida la situación actual, se propone el **objetivo general** del presente Trabajo de Fin de Máster, así como los diferentes **objetivos específicos**, los cuales llevarán a la consecución del objetivo general.

Para poder llevar a buen término los anteriores objetivos, **se describirá la metodología utilizada** para la realización del presente Trabajo de Fin de Máster, de forma que se puedan alcanzar los objetivos específicos y, por ende, se pueda llegar a completar la consecución del objetivo general.

En el siguiente punto se abordará el **desarrollo específico de la contribución del autor**, describiendo una **metodología para realizar intrusiones en equipos informáticos, como instrumento de investigación de delitos, previa a la realización efectiva de los registros remotos**.

Es en este apartado donde: se definirán los **requisitos necesarios** para llevar a cabo correctamente la metodología propuesta; se desarrollará dicha **metodología**, paso a paso y a modo de checkpoints; y se realizará una **simulación práctica** utilizando dicha metodología. Esta simulación práctica, será llevada a cabo realizando una intrusión en un teléfono móvil

con Sistema Operativo Android, simulando todo el proceso desde el inicio de la investigación, Tanto **los dispositivos electrónicos** (teléfono móvil)**, como la red utilizada, son propiedad del autor del presente Trabajo de Fin de Máster**.

Finalmente, se mostrarán las **conclusiones** a las que se ha podido llegar a través, tanto del desarrollo de la metodología, como de su puesta en práctica, **proponiéndose líneas de trabajo** que podrían ser llevadas a cabo con posterioridad, indicando los usos que podría tener la aplicación del contenido del presente Trabajo y las formas en la que podría mejorarse la metodología propuesta.

2. Contexto y estado del arte

Desde la última reforma de la Ley de Enjuiciamiento Criminal (Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, 2015), en la que se introdujeron varias novedades, varias de ellas dirigidas a actualizar las herramientas a utilizar de las investigaciones, adaptándose a la realidad tecnológica actual, se ha hablado mucho acerca de dichas reformas.

En concreto, sobre la materia que versa este Trabajo de Fin de Máster, los registros remotos, hay numerosas referencias (fundamentalmente en Internet) que tratan los problemas, las características y la reacción de los ciudadanos sobre dichos registros remotos.

Por ejemplo, Dña. Ofelia Tejerina Rodríguez (Tejerina Rodríguez, 2015), expresaba sus dudas acerca de los delitos a los que sería aplicable dicha medida, en concreto al establecido en el artículo 588 septies a).1.e (Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, 2015), por la amplitud de su redacción y su falta de precisión. Alega Ofelia Tejerina Rodríguez que, en cualquier delito cometido utilizando cualquier medio informático o servicio de comunicación, independientemente de su gravedad, podría ser utilizada la medida del registro remoto.

Si bien es cierto que, en base a la redacción del propio artículo, se podría dar esta situación, según lo expresado por D. Cándido Conde-Pumpido Tourón (Conde-Pumpido Tourón, 2016), Magistrado de la Sala de lo Penal del Tribunal Supremo y Ex Fiscal General del Estado, para aplicar dicha medida a los referidos delitos del artículo 588 septies a 1.e (Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, 2015), expone que se debe interpretar de una forma muy restrictiva, limitándose únicamente a delitos de especial gravedad.

Sin embargo, para Dª Lorena Bachmaier Winter (Winter, 2016), este extremo no queda tan claro, puesto que la Ley Orgánica 13/2015 (Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, 2015) no indica con claridad esa limitación. Como ejemplo muestra que, mientras para una intervención telefónica es necesario que hecho delictivo investigado tenga una pena de prisión de, al menos, tres años, para los registros remotos eso no es así, puesto que la mencionada Ley Orgánica

establece directamente los tipos delictivos (como son los delitos de terrorismo, o los delitos cometidos sobre menores) sobre los que es aplicable, no definiendo la pena de prisión mínima que han de tener esos delitos.

Así pues, queda patente que, **incluso entre reputados expertos en la legislación vigente como los anteriormente referidos, la Ley deja lagunas (deliberadamente abiertas o no) sobre la aplicación de esta medida**.

Sin ahondar más en el asunto anterior, la última reforma de la LECrim, en la que se incluyó la posibilidad de registros remotos, ha causado malestar en la comunidad online, puesto que la injerencia en los derechos fundamentales que se realiza es de muy alta intensidad y, la citada comunidad, teme por el hecho de que esta medida pueda ser aplicada indiscriminadamente por las unidades de investigación policiales.

Además, la falta de una redacción clara sobre los límites de estos registros, no es algo que pueda gustar a los ciudadanos. Muchas son las páginas web en las que se ha reflejado ese malestar, aumentado por la novedad de la medida y la falta de ejemplos prácticos de ejecución y jurisprudencia aplicable.

No se ha conseguido encontrar ningún tipo de protocolo establecido para la realización de los registros remotos, seguramente por la novedad de esta posibilidad legal, por lo que, **la metodología propuesta en el presente Trabajo de Fin de Máster es un novedoso primer paso para realizar la ejecución efectiva de la medida por las Unidades de Investigación**.

La bibliografía consultada versa sobre intrusiones en diferentes equipos informáticos, todos con interés académico, pero en ningún momento se hace referencia a la posibilidad de su uso, como herramienta en la investigación de hechos delictivos, en dichos registros remotos.

Tampoco en dicha bibliografía, se relacionan las diferentes técnicas existentes con las permitidas por la legislación vigente, o su aplicación práctica para esos fines, por lo que **el presente Trabajo de Fin de Máster es pionero en ese aspecto: indicar una metodología, la cual aplica técnicas existentes, que permita la realización de registros remotos conforme a la legislación, ofreciendo a los investigadores los requisitos necesarios para la ejecución de dicha medida, así como una serie de herramientas que pueden ser utilizadas para llevarla a efecto**.

2.1 Base teórica y legal

En **primer lugar**, se deben contemplar aquellos **requisitos y condiciones que impone la legislación vigente** para poder llevar a cabo una medida restrictiva de derechos fundamentales, como es el registro remoto sobre equipos informáticos.

Las "*disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos*", recogidas en el Capítulo IV, del Título VIII, del Libro II (Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, 2015), indican que, como requisitos "genéricos" comunes a todas las medidas mencionadas anteriormente, tenemos los siguientes:

- Es necesaria la **autorización judicial**, cumpliendo con los principios de "**especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad"** de la medida, recogidos en el artículo 588 bis a (Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, 2015):
    - **Especialidad**: la medida se aplicará a la investigación relacionada con la comisión de un delito concreto. Es decir, sólo se autorizará la medida si se está llevando a cabo la investigación de un delito. No podrá ser autorizada para prevenir, descubrir delitos o despejar sospechas acerca de la comisión de posibles delitos. Los indicios que se tengan de la comisión, deben ser suficientes para poder hacer efectiva la ejecución de la medida y, además, ese hecho debe estar siendo investigado ya por la Policía Judicial.
    - **Idoneidad**: definirá el ámbito objetivo y subjetivo de la medida que se va a ejecutar, así como la duración temporal de la misma.
    - **Excepcionalidad y necesidad**: sólo se podrá acordar la medida si:
        - No se puede disponer, durante la investigación, de otras medidas que sean menos intrusivas o lesivas de los derechos fundamentales de la persona que se está investigando, y que pudieran resultar de igual utilidad en la investigación (como por ejemplo las vigilancias y seguimientos).
        - Si para poder comprobar efectivamente la comisión del hecho delictivo, averiguar la identidad del autor, el lugar en el que reside o la localización de los efectos del delito, se necesitara de dicha medida, puesto que, en el

caso de no llevarla a cabo, los anteriores extremos resultarían prácticamente imposibles.

- La adopción de la medida (que como ya se ha dicho, es tremendamente intrusiva) debe ser **proporcionada** a los hechos delictivos que se está investigando.

En el supuesto concreto de este Trabajo, la medida se tomaría a instancia de la Policía Judicial, es decir, son éstos quienes solicitan al juez competente cualquiera de las medidas enumeradas anteriormente, así que la petición que realicen debe contener los siguientes extremos:

- Es necesario describir los hechos delictivos que se están investigando. Igualmente, hay que facilitar la identidad de la persona, o personas, que va a ser investigada (o una tercera persona que se pueda ver afectada por la medida). Estos datos, claro está, siempre y cuando sean conocidos.
- Hay que exponer, de una forma completa y detallada, todas las razones objetivas por las que la adopción de la medida resulte necesaria. También se deben detallar todos los hechos relevantes y relacionados con los hechos delictivos investigados, que se hayan descubierto durante la investigación previa que se ha realizado.
- Para poder llevar a cabo la medida, son necesarios datos que identifiquen a la persona investigada, así como de los medios de comunicación que emplee, si fuera el caso.
- Hay que especificar la medida que se va a solicitar y los requisitos específicos de la misma. Es decir, qué, de todas las opciones que ofrece la legislación, es lo que se solicita (pueden ser todas las opciones recogidas en la legislación, o sólo alguna de ellas).
- Grupo o Unidad de la Policía Judicial que se va a encargar de llevar a cabo la ejecución de la medida. Es decir, qué Grupo, va a llevar a cabo tanto la intrusión como el posterior registro.
- De qué manera va a ser llevada a cabo la ejecución de la medida (acceso físico al equipo o mediante Ingeniería Social).
- Cuánto a va durar la ejecución de la medida (teniendo en cuenta los límites establecidos legalmente).
- Si fuera necesaria la colaboración de algún sujeto obligado, de cara a obtener datos que faciliten, o posibiliten, la ejecución de la medida, deben facilitarse sus datos. Si no es necesaria la intervención de ningún sujeto obligado, entonces este extremo no debe constar en la solicitud.

Todos estos extremos, deben figurar claramente en el Oficio de solicitud de la medida. Igualmente, el Juez podría solicitar cualquier tipo de ampliación o aclaración de la información facilitada en el citado Oficio, si lo estimase pertinente o necesario.

Si fuera necesaria la **prórroga de la medida**, la solicitud debe justificar la **necesidad de continuar con la intervención**. Además, se debe incluir en dicha solicitud un informe que detalle de todos los resultados que se han obtenido como resultado de la aplicación de la medida hasta ese momento.

Como medida de control de la ejecución de la medida por parte del Juez Instructor, durante el desarrollo de la misma, **la Policía Judicial deberá informar al Juez de cómo se está desarrollando y de los resultados obtenidos de la aplicación de la medida**, tan pronto como sean requeridos por el Juez y de la forma en que éste indique.

Además de los requisitos anteriores, o complementando y especificando a éstos, **los registros remotos sobre equipos informáticos tienen los siguientes requisitos,** recogidos en el Capítulo IX, del Título VIII, del Libro II (Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, 2015):

Se autoriza al uso de cualquier tipo de dato de identificación, códigos de acceso, así como la instalación de un programa de software, bien mediante el acceso físico a los equipos informáticos, bien de forma remota, que pueda permitir a los investigadores el registro de los citados equipos a distancia, de forma remota, y sin que el titular de los mismos tenga conocimiento de estos hechos. La variedad de equipos sobre los que se puede ejecutar la medida es amplia, incluyendo ordenadores personales, teléfonos móviles, tabletas o bases de datos.

Se podrán **utilizar datos de identificación y códigos**, así como **instalar un software**, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos, **siempre y cuando se persiga la investigación de uno de los siguientes delitos relacionados en el artículo 588 septies a** (Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, 2015), **cuyo contenido se transcribe literalmente entrecomillado**:

- *"Delitos cometidos en el seno de organizaciones criminales",* los cuales se encuentran recogidos en el artículo 570 (Ley Orgánica 1/2015, de 30 de marzo, del Código Penal, 2015)
- *"Delitos de terrorismo",* los cuales se encuentran recogidos en artículos del 573 al 580 (Ley Orgánica 1/2015, de 30 de marzo, del Código Penal, 2015)

- *"Delitos cometidos contra menores o personas con capacidad modificada judicialmente"*
- *"Delitos contra la Constitución, de traición y relativos a la defensa nacional",* los cuales se encuentran recogidos, respectivamente, en los Títulos XXI y XXIII (Ley Orgánica 1/2015, de 30 de marzo, del Código Penal, 2015)
- *"Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación"*

En relación a lo especificado anteriormente, D. Cándido Conde-Pumpido Tourón (Conde-Pumpido Tourón, 2016) confirma que se permite la instalación de programas de carácter malicioso, si bien con un fin y uso legítimos. Esa instalación, abunda D. Cándido Conde-Pumpido Tourón, puede realizarse, bien penetrando físicamente en el equipo informático, o bien enviando dicho software mediante un mensaje o correo electrónico, que la persona investigada abra (o ejecute) y permita la instalación de dicho software en el dispositivo. Este último extremo se refiere a la Ingeniería Social, que forma parte de la metodología propuesta en el presente Trabajo Fin de Máster.

En idénticos términos se expresa Dª Lorena Bachmaier Winter (Winter, 2016), quien ejemplifica que, en otros países, como Suecia, Holanda o Bélgica, la Ley permite el acceso remoto a los equipos informáticos, es decir, se permite la realización de los registros remotos como tal, pero sólo se permite que la instalación del software necesario se realice con acceso físico al dispositivo a registrar. Este no sería el caso en España, salvo que futura jurisprudencia del Tribunal Supremo lo determine así, puesto que en la legislación relacionada no se establece dicho límite para la ejecución de la medida, es decir, se da libertad al Juez de Instrucción para autorizar tanto la instalación con acceso físico, como a distancia.

Es más, implícitamente el Sr. Conde-Pumpido Tourón (Conde-Pumpido Tourón, 2016) da por sentado que ésta sería la forma "normal" o "habitual" de realizar la instalación, puesto que indica que habría que recurrir al primero de los supuestos (acceso físico al dispositivo) cuando el investigado sea especialmente precavido, resultando imposible la instalación por envío remoto.

En el mismo documento, también se hace referencia al software utilizado para el registro remoto. Se indica que debiera establecerse una serie de protocolos o normas reglamentarias que permitan disponer de sistemas de validación de los diferentes sistemas de registro, para de este modo evitar que se cuestione su funcionamiento o fiabilidad a posteriori (lo que podría invalidar lo obtenido mediante este método durante la investigación).

Además, se refiere que uno de los mayores problemas acerca de la ejecución de los registros remotos, es determinar qué tipo de software se va a utilizar, y dónde se van a poner los límites de lo que van a ser capaces de hacer esos programas.

En ciertas investigaciones, se ha hecho uso de “keyloggers” para registrar el texto que se escribe mediante el teclado en los ordenadores personales de los investigados, si bien este tipo de software queda muy lejos de los objetivos de los registros remotos.

Actualmente, a falta de conocer los proveedores específicos que puedan tener los distintos cuerpos policiales, el software que más se aproxima a la finalidad de los registros remotos podría ser el utilizado para la realización de test de penetración, como pueden ser (Metasploit, 2017) o (Core Impact, 2017).

Por lo tanto, **actualmente no se cuenta con un listado de software permitido o recomendado para la realización de los registros remotos**. **En la metodología propuesta**, se **facilitan herramientas para la creación de ese tipo de software, que permiten llevar a cabo registros remotos, cuyo uso resultaría totalmente válido** pues, como ya se ha explicado, no existe ni software prohibido, ni software obligatorio, para realizar los registros remotos. Si bien, **la decisión final queda a criterio del Juez Instructor competente**.

La **resolución judicial**, mediante la que el Juez Instructor autorizará el registro remoto (caso de que sea así claro, puesto que puede denegar la solicitud efectuada por la Policía Judicial), **debe especificar claramente sobre qué equipo** (o equipos) **o sistema informático** (ordenador personal, tableta, Smartphone o base de datos) **se va a ejecutar la medida** (y, consecuentemente, la intrusión previa). También debe especificar el alcance que va a tener la medida a ejecutar. Como se ha expuesto anteriormente, puede ser necesario el uso de todas las posibilidades que ofrece la legislación vigente, o que sólo se necesite el uso de una parte de las mismas.

Debe especificar **cómo se va a proceder a acceder a los equipos afectados por la medida y cómo se va a proceder a recabar la información** o datos durante el registro remoto (información o datos que deben ser los que resulten relevantes o de interés para la investigación que se está llevando a cabo).

Además, se debe **especificar el software que se va a utilizar** para realizar el registro remoto.

Los **agentes de la Policía Judicial que se harán cargo de la ejecución efectiva** de la medida también deben estar identificados (mediante su correspondiente carné profesional).

Deberá constar **si se concede autorización para realizar copias de los datos** que se hayan recogido durante el registro remoto (así como si se concede dicha autorización para su conservación).

Finalmente, deberá **especificar las medidas que resultan necesarias para preservar la integridad** de los datos que se encuentren almacenados en los dispositivos registrados, así como para **hacerlos inaccesibles al titular** de los mismos **o proceder directamente al borrado de éstos del dispositivo** (o sistema) que está siendo objeto de la medida del registro remoto.

Como la autorización judicial debe contener todos estos extremos, **en el Oficio de solicitud todos los datos anteriores deberán ser incluidos**, puesto que, de lo contrario, o bien no se autorizará la medida o, si se autoriza, puede que hayan quedado fuera de la misma algunos extremos que debieran figurar (por ejemplo, si no se incluye la solicitud de autorización para la realización y conservación de copias, éstas no se podrán realizar por no estar autorizadas, lo que puede perjudicar la investigación). **El Oficio de solicitud ha de ser lo más amplio y detallado posible**, para que abarque todas aquellas acciones que resulten necesarias para la resolución del hecho delictivo investigado.

Si hay razones, tras la autorización del registro remoto, para creer que hay datos, necesarios para la investigación, almacenados en otro lugar que el inicialmente autorizado (recordemos que puede ser un equipo o un sistema informático), se pondrá este hecho en conocimiento del Juez Instructor competente, de forma inmediata, para que éste pueda autorizar, o no, una ampliación del registro remoto inicial (por ejemplo, puede que se solicite autorización para el registro de un PC, pero resulta que hay razones fundadas para los investigadores que indican que parte de la información buscada se almacena en el teléfono móvil del investigado. Entonces, habría que poner en conocimiento del juez estos extremos para que pueda autorizar una ampliación de la medida, que incluya el registro de ese teléfono móvil).

Para llevar a cabo la medida solicitada, siempre que el juez competente la autorice, puede ser necesaria la colaboración de terceros. Esta obligación de colaboración viene recogida en el artículo **588 septies b, deber de colaboración** (Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, 2015) e incluye los siguientes, **los cuales se citan textualmente entrecomillados**:

> "*1. Los prestadores de servicios y personas señaladas en el artículo 588 ter e y los titulares o responsables del sistema informático o base de datos objeto del registro están obligados a facilitar a los agentes investigadores la colaboración precisa para*

la práctica de la medida y el acceso al sistema. Asimismo, están obligados a facilitar la asistencia necesaria para que los datos e información recogidos puedan ser objeto de examen y visualización.

2. Las autoridades y los agentes encargados de la investigación podrán ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria para el buen fin de la diligencia. Esta disposición no será aplicable al investigado, a las personas dispensadas de la obligación de declarar por razón de parentesco, y a aquellas que, de conformidad con el artículo 416.2, no pueden declarar en virtud del secreto profesional.

3. Los sujetos requeridos para prestar colaboración tendrán la obligación de guardar secreto de las actividades requeridas por las autoridades.

4. Los sujetos mencionados en los apartados 1 y 2 de este artículo quedarán sujetos a la responsabilidad regulada en el apartado 3 del artículo 588 ter e".

De este modo, tanto los prestadores de servicios, como podría ser una operadora de telefonía como Movistar o Vodafone, por ejemplo, estarían obligados a dar la información que estuviera en su poder que coadyuvara a la consecución de la ejecución del registro remoto. Esta ayuda se puede concretar, por ejemplo, en la comunicación del modelo de teléfono móvil que está utilizando la persona investigada o en el envío de determinados mensajes haciendo uso de su infraestructura.

También afecta a los titulares o responsables de los sistemas. Aquí se podría incluir al administrador de una base de datos que se quiera registrar, estando éste obligado a facilitar las claves de acceso de determinado usuario. Clarificando el ejemplo, el administrador de un foro, estaría obligado a facilitar la información de acceso al sistema que posea, en relación con la persona que está siendo investigada.

Pero no sólo el artículo se queda ahí, sino que también se incluye en la obligación de colaborar con la ejecución de la medida a las personas que conozcan el funcionamiento de los diferentes sistemas o dispositivos a registrar remotamente. Esto puede incluir a cualquier experto en la materia concreta que sea necesaria, con la finalidad de ejecutar la medida correctamente. Sobre esta obligación existen ciertas limitaciones, las cuales vienen recogidas en los artículos 416.1 y 416.2 (Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, 2015), y que hacen referencia, de forma resumida, a las relaciones de parentesco con el investigado y a los abogados que tuviesen una relación laboral con el mismo.

En el caso de no acceder a las solicitudes realizadas por los agentes que llevan a cabo la investigación, o por la propia autoridad en sí, responderían por un delito de desobediencia del artículo 556.1 (Ley Orgánica 1/2015, de 30 de marzo, del Código Penal, 2015)

La duración temporal máxima que puede ser autorizada por el Juez de Instrucción, respecto de esta medida de registro remoto, es como máximo de 1 mes (podría decretarse una autorización por un tiempo menor, claro está), si bien, se puede prorrogar la duración hasta un máximo de 3 meses. Es decir, como mucho, la medida del registro remoto puede durar 3 meses, un corto período de tiempo si lo comparamos con el límite establecido para una intervención telefónica, por ejemplo.

Aunque 1 mes parezca mucho tiempo, hay que tener en cuenta que no se puede comenzar la ejecución de la medida hasta que ésta es autorizada por el Juez. Esto es, se puede recabar cierto tipo de información previamente, pero hasta que no se va a ejecutar de forma efectiva la medida realmente no se conocen los diferentes problemas y situaciones que pueden surgir, por lo que ese mes inicial puede quedarse muy corto si, por ejemplo, el investigado no lee los mensajes que se le envían o no realiza la instalación del software.

Seguramente esta estricta limitación temporal se debe a lo invasiva que resulta la ejecución de esta medida para las personas investigadas.

2.2 Análisis del estado actual legislativo

De toda la legislación existente hasta la fecha, se puede deducir, por ejemplo, que **no se contempla en ningún texto legal que el software instalado deba ser eliminado una vez finalizada la medida** (este extremo dificultaría aún más su implementación).

En iguales términos se expresa D. Cándido Conde-Pumpido Tourón (Conde-Pumpido Tourón, 2016). El citado manifiesta que en la doctrina se cuestiona si la instalación permanente de determinado software sería legítima, ya que teóricamente se trata de una medida limitada a la copia de los archivos en un momento concreto. Este argumento queda desmontado ya que la propia duración de la medida, que puede llegar a alcanzar los 3 meses incluyendo potenciales prórrogas, no avala la anterior afirmación.

Igualmente, se puede concluir que **las intrusiones pueden ser llevadas a cabo tanto con acceso físico a los equipos, como mediante el envío del software que pretende ser instalado en el equipo del investigado**. Esto abre la puerta al uso de la Ingeniería Social, lo que en muchas ocasiones puede facilitar que el software utilizado para los registros remotos sea instalado en el equipo objeto de la medida.

En caso de ser necesario, los diferentes **sujetos obligados a colaborar deberán facilitar la información de que dispongan**. Por ejemplo, esto permitiría conocer con exactitud el teléfono móvil que está utilizando el investigado, puesto que las operadoras de telefonía disponen de dicha información. Así, la elección del software a utilizar y el método de instalación podrían quedar mejor definidos desde un principio.

También se puede extraer que, en base a la legislación vigente y a la bibliografía consultada, **para el caso de hacer uso de Ingeniería Social**, con el objetivo de que la persona investigada instale un software, el cual permita a los investigadores realizar de forma exitosa el registro remoto, **no sería necesaria la figura del agente encubierto**, prevista también en la legislación.

Finalmente, también se puede concluir que, en estos momentos, si bien existen criterios estrictamente legales para la ejecución de los registros remotos, **no existe aún suficiente jurisprudencia por parte del Tribunal Supremo que delimite o pula esos límites**.

Sólo el tiempo, y las sentencias del Tribunal Supremo que creen jurisprudencia, podrán establecer de una forma más clara y precisa todos aquellos límites necesarios en la aplicación de la medida, para conseguir que la información obtenida en base a la ejecución de la misma, sea totalmente válida en el proceso penal.

3. Objetivos concretos y metodología de trabajo

A continuación, se pasa a describir el objetivo general del presente Trabajo de Fin de Máster, así como los objetivos específicos que llevan a la consecución del objetivo general. Igualmente, se expondrá la metodología seguida para la elaboración del presente TFM.

3.1. Objetivo general

Crear una **metodología para realizar intrusiones en equipos informáticos, que permita la ejecución de registros remotos** en dichos equipos, sin el conocimiento de la persona investigada.

3.2. Objetivos específicos

- **Identificar los requisitos legales** específicos para realizar una intrusión en equipos informáticos, con el objetivo de llevar a cabo en los mismos un registro remoto.
- **Determinar, de la forma más completa posible, el dispositivo que va a ser objeto de la intrusión** y posterior registro remoto.
- **Determinar los medios técnicos necesarios** para poder ejecutar de forma exitosa una intrusión, con el objetivo de realizar registros remotos.
- **Realizar un "oficio tipo" para la solicitud** de la medida del registro remoto al Juez de Instrucción competente.
- **Desarrollar una simulación de intrusión en un dispositivo concreto**. Lo ideal sería poder llevar a cabo una prueba en un entorno real, pero por motivos obvios se va a realizar una **prueba en una red propia y con equipos propios**.

3.3. Metodología del trabajo

Para la correcta elaboración del presente Trabajo de Fin de Máster, se ha recogido (y desechado) gran cantidad de información acerca de los registros remotos. Gran parte de esa información trata sobre la novedad de la medida y de los posibles efectos en los ciudadanos de la adopción de dicha medida, por parte de un Juez de Instrucción, en una investigación por la comisión de un hecho delictivo, llevando el debate a los terrenos sobre la privacidad y los límites que debieran tener las técnicas aplicadas en las investigaciones.

Se ha tratado de recoger todos los requisitos legales necesarios, así como la interpretación de esos requisitos, en base a la información de consulta bibliográfica y a la interpretación que se hace de las mismas por parte de expertos en la materia.

Es la propia Ley la que dicta qué es necesario, pero en ocasiones deja casos sin cubrir, o extremos sin definir. Estos últimos casos son los que la jurisprudencia va delimitando, a medida que se dictan sentencias por parte, fundamentalmente, del Tribunal Supremo, para realizar los registros remotos, si bien a día de hoy no se ha hallado evidencia de las mismas. Sólo con el tiempo se irá perfilando de verdad qué es lo que se puede hacer y cómo, en base a las citadas sentencias, que definirán y perfilarán los límites de esta medida.

Al no existir prácticamente bibliografía acerca de la realización de estos registros remotos, tanto en el apartado legal como técnico (obviando las Leyes existentes, claro está), se ha solicitado la colaboración de miembros de la fiscalía, así como de miembros de grupos de investigación especializados.

Dicha colaboración se ha basado en la respuesta a preguntas planteadas por el autor, en aras de clarificar la Ley y de conocer la operativa habitual de los investigadores.

Con respecto a la operativa de investigación, no se ha podido conseguir información acerca del software específico utilizado, por tratarse de materia reservada. Este último extremo no afectaría a la metodología propuesta, puesto que ésta es independiente de las herramientas disponibles. Es evidente que, con mejores herramientas, la ejecución práctica se simplifica enormemente.

Una vez recopilada esa información, se ha llevado a cabo un trabajo de análisis, para poder establecer una metodología que recogiera todos aquellos puntos necesarios para realizar los registros remotos contemplados en la Ley.

Este extremo resulta de notable importancia, puesto que, aunque dispongamos de toda la información necesaria, así como de las herramientas oportunas, si la intrusión no se realiza

conforme a la Ley, toda la información recabada quedaría inmediatamente invalidada para el proceso penal, por no hablar de las posibles repercusiones legales para los actuantes. Es por ello que es de suma importancia conocer qué pasos hay que dar legalmente, previos a realizar de forma operativa una intrusión en un equipo informático.

Una vez analizada la información recabada, se procede al desarrollo de la metodología propuesta, que contempla tanto la parte legal como la operativa, para llevar a cabo de forma efectiva la medida del registro remoto.

Para comprobar la validez de dicha metodología, ésta se ha puesto a prueba con una simulación en un entorno controlado, si bien se podría aplicar por los grupos investigadores en un entorno real, adaptando los contenidos a la situación concreta de cada investigación.

En la "Ilustración 1" se muestra el flujo de la metodología seguida para la elaboración del presente Trabajo de Fin de Máster.

Ilustración 1. Proceso de la metodología utilizada para la realización del TFM

4. Desarrollo específico de la contribución

En el presente capítulo se pasa a describir la metodología propuesta para realizar una intrusión en un dispositivo informático, haciendo uso de técnicas de Ingeniería Social, con el objetivo de poder ejecutar la medida prevista en la legislación vigente del registro remoto.
Al no existir, por el momento, ningún tipo de protocolo de actuación en estos casos, la contribución que se realiza viene a paliar, en cierta forma, esa falta de desarrollo.
De este modo, se procede a identificar todos aquellos requisitos que se estiman necesarios para que la intrusión, y posterior registro remoto, puedan ejecutarse con éxito.
Aparte de lo establecido por la legislación vigente, se proponen métodos o formas de realizar las acciones que hasta este momento no se utilizaban de forma generalizada por los investigadores. Esto ha sido así debido a la novedad de la posibilidad de realizar registros remotos con la autorización de un Juez y a la falta de especificaciones concretas para la ejecución de la misma.
Por ello, se proponen herramientas y escenarios específicos para que, en función de la investigación concreta que se esté llevando a cabo, se pueda llevar a efecto, de forma exitosa, el registro remoto de un equipo informático.
Todo el proceso de la metodología requiere que se vayan cumpliendo los diferentes pasos de forma completa, es decir, si no se ha logrado completar una etapa de la metodología, no se podrá continuar con la siguiente, pues esto querrá decir que alguno de los requisitos para llevarla a efecto no se ha completado.
Por lo tanto, las **principales novedades y aportaciones** de la presente metodología son: **clarificar y especificar los requisitos necesarios** para poder llevar a cabo, de manera exitosa, un registro remoto sobre un equipo informático; **facilitar herramientas y métodos** de actuación concretos, acordes con los requisitos necesarios; **ofrecer un camino**, paso a paso, desde el inicio de una investigación, que permita conocer si se puede llevar a cabo un registro remoto y, de ser así, la forma de llevarlo a cabo.

4.1. Desarrollo de metodología

Como se ha expuesto anteriormente, la metodología propuesta es del tipo lineal, siendo necesario completar un apartado para poder continuar con los siguientes, y completar el desarrollo de la metodología.
Y es necesario completar cada uno de los pasos propuestos porque, de lo contrario, alguno de los requisitos planteados no se habría podido cumplir, con la consecuente pérdida de validez en el proceso penal (caso de conseguirse la intrusión en el dispositivo de forma

efectiva) o con la imposibilidad de llevar a cabo dicha intrusión para la realización del posterior registro remoto.
Previamente al desarrollo de la metodología, se describen todos aquellos requisitos que se han estimado necesarios, siempre contando con las limitaciones tecnológicas actuales y con las posibles tecnologías accesibles únicamente a entidades gubernamentales (de las cuales, obviamente, no se ha podido obtener información por motivos de confidencialidad).

4.1.1. Identificación de requisitos

Para la correcta puesta en marcha de la metodología propuesta, se han reconocido 3 tipos de requisitos necesarios. Estos requisitos incluyen las condiciones previas necesarias para llevar a cabo, de una forma completa, la metodología propuesta.

Con respecto a los requisitos legales, hay que indicar que todos y cada uno de ellos son necesarios y obligatorios, puesto que de lo contrario los registros remotos no se realizarían conforme a la legislación vigente lo que, como ya se ha dicho en anteriores puntos de este Trabajo de Fin de Máster, provocaría que todo lo recabado no sería de utilidad durante el proceso penal, además de poder conllevar responsabilidad, de tipo penal y disciplinaria, a los actuantes que hayan ejecutado el registro remoto.

Con respecto a los requisitos técnicos, si bien alguno de ellos no resulta obligatorio (puesto que siempre se va a depender de las capacidades económicas o presupuestarias del Cuerpo policial que lleve a cabo la investigación), sí que todos ellos resultan recomendables, para poder llevar a buen término la ejecución de la medida.

Finalmente, en relación a los requisitos de formación, del personal que va a llevar a cabo la medida, son requisitos recomendables, puesto que no siempre se va a poder contar con personal que disponga de los conocimientos que se sugieren.

Lo que sí se puede hacer, con respecto a los requisitos de formación, es tratar de gestionar cursos de formación, para que el personal dedicado a este tipo de investigaciones, se pueda especializar en la materia y, de este modo, la ejecución de la medida se pueda mejor y más rápidamente.

En relación al párrafo anterior, los cursos de formación se tornan imprescindibles, puesto que, al ser una medida eminentemente tecnológica, los cambios se producen (nuevos equipos, nuevos sistemas operativos o nuevas vulnerabilidades) a ritmos vertiginosos.

A continuación, se exponen los requisitos genéricos para realizar los registros remotos, si bien, para esta metodología en concreto, se puntualizarán los que son necesarios.

Requisitos legales

Los requisitos legales han sido ampliamente tratados en el apartado "2.1 Base teórica y legal" del presente Trabajo de Fin de Máster.

De todos modos, se vuelven a listar, de forma resumida y sin la aclaración y justificación, ya descrita en el apartado indicado anteriormente.

En este punto se van a relacionar todos los requisitos exigibles, desde el punto de vista legal, par que, de este modo, se pueda tener un listado de comprobación, en aras de poder comprobar si la ejecución de la medida del registro remoto es posible en la investigación que se está llevando a cabo:

La medida del registro remoto sólo se podrá llevar a cabo cuando los **hechos delictivos investigados correspondan a uno de los delitos recogidos en el artículo 588 septies a 1** (Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, 2015). Si los hechos investigados no se corresponden con uno de esos delitos, entonces no se podrá ejecutar la medida, puesto que el Juez competente no lo autorizará.

Se hace necesaria la autorización del Juez competente, para poder llevar a cabo la ejecución de la medida por parte de los investigadores.

Para obtener la autorización por parte del Juez de Instrucción competente, cuando la solicitud se realice de parte de la Policía Judicial, será necesaria la redacción de un **Oficio de solicitud**, en el que se debe incluir, de forma clara, detallada y ampliamente justificada, los siguientes extremos:

- Qué hecho delictivo se está investigando. Debe ser un hecho delictivo concreto y se debe indicar en el oficio de solicitud (por ejemplo, si se trata de un delito contra la salud pública o de un delito de terrorismo).
- No sólo hay que indicar qué delito se está investigando. Se deben incluir todos los indicios que se conozcan acerca de la comisión de ese hecho, explicados profusamente y con todo detalle posible. Es decir, debemos facilitar al Juez Instructor todas aquellas gestiones, previas a la solicitud, que se han realizado hasta el momento, que estén directamente relacionadas con los hechos y explicar por qué llevan a los investigadores a pensar que se está cometiendo por la persona (o personas) investigada. El Juez Instructor no puede imaginar o suponer, sino que

se va a basar en los datos que figuren en la solitud para conceder la autorización o no, por lo que, mientras más detallada y concisa sea ésta, más información tendrá aquél para poder decidir la adopción de la medida.

- Se debe facilitar la identidad completa de la persona investigada o, en su caso, de la persona (o personas) que vaya a ser afectada por la ejecución de la medida.
- Concretar al Juez Instructor qué medida es la que solicitamos y, dentro de ésta, qué es lo que se quiere solicitar en concreto. En este punto y, dado que en caso de conceder la autorización el Juez de Instrucción, sólo la concederá en aquellos términos que figuren en la solicitud, se debe incluir todo aquello que se estime necesario para llevar a buen término la investigación (por ejemplo, si en la solicitud no figura el uso de códigos, no se podrá realizar una intrusión en la red inalámbrica del investigado, y eso puede llevar a que la investigación no avance como debería). En este punto se debe justificar la especialidad (el hecho investigado concreto), la idoneidad de la medida (que no exista otra medida, menos lesiva, con la que se puedan conseguir los mismos resultados), la excepcionalidad y la necesidad de la medida (debido a que, de otro modo, sería imposible conseguir los resultados necesarios para realizar la investigación) y la proporcionalidad de la misma con respecto al hecho investigado (se debe tratar de un hecho grave, que la aplicación de esta medida altamente restrictiva sea proporcionada al hecho investigado).
- Debe figurar qué unidad concreta de la Policía Judicial es la que se va a hacer cargo de la investigación, así como los agentes concretos que la van a llevar a cabo.
- De qué forma se va a proceder a la ejecución del registro remoto (acceso físico, Ingeniería Social).
- Por cuánto tiempo se solicita la aplicación de la medida.
- Caso de que fuera necesaria la colaboración de algún sujeto obligado, en la solicitud debe figurar la identidad completa del mismo.
- Sobre qué dispositivo (o sistema informático, en su caso) se va a ejecutar la medida. Debemos especificarlo con el mayor detalle posible: tipo de dispositivo, marca, modelo, sistema operativo y software que utiliza.
- Qué software se va a utilizar para llevar a cabo de manera efectiva el registro remoto.

- Si va a haber necesidad de hacer copias y conservar los datos que se obtengan durante el registro informático.

- Qué tipo de medidas se precisan para garantizar la integridad de los datos que estén almacenados, así como para hacerlos inaccesibles o eliminarlos del dispositivo sobre el que se realiza el registro remoto.

Durante el desarrollo de la ejecución de la medida, el Juez Instructor competente tiene que ser informado de los progresos realizados, es decir, de la nueva información o datos conseguidos gracias a la aplicación de la medida en la investigación. Si no se obtienen datos relacionados con la medida, evidentemente, el Juez decretará el cese de aplicación de la misma. Esta información se le facilitará al Juez, cuándo y cómo éste determine, mediante la redacción de un escrito (Oficio) en el que se describan, de forma amplia y detallada, toda información relevante para la investigación, que haya sido averiguada gracias a la aplicación de la medida.

En el caso de que sea necesaria la prórroga de la medida (porque no haya dado tiempo a recabar toda la información necesaria o porque existan indicios de que todavía puede introducirse en el dispositivo registrado más información relevante para la causa).

Todos los requisitos legales expuestos anteriormente, son necesarios para llevar a cabo de forma correcta la metodología.

Requisitos técnicos

En función del tipo de intrusión (y de explotación de la misma) que vayamos a realizar, habrá que contar con diferentes medios:

- Si el registro remoto se realiza desde la propia red (inalámbrica) de la persona investigada: debemos disponer de una tarjeta de red inalámbrica que permita “modo monitor” o “promiscuo”), para poder introducirnos en la misma. Se entiende que es un adaptador o tarjeta de red independiente del que ya lleve instalado el equipo informático a utilizar. Por ejemplo, un adaptador USB de red podría valer perfectamente. El modo “promiscuo” permite escuchar todo el tráfico producido por esa red, aun sin estar autenticado en la misma, lo que resulta necesario para tratar de vulnerar la seguridad en introducirnos en la misma sin conocer las credenciales. Si ya se conocieran las claves de acceso, con una tarjeta de red inalámbrica normal sería suficiente. Este método no resulta recomendable para los registros remotos, puesto que obliga a estar cercano físicamente al investigado y, además, estaríamos dentro de su propia red, con lo que sería de suma facilidad para éste averiguar que alguien se

ha introducido en su red inalámbrica. Además, dependeríamos de que estuviera conectado a esa red para poder realizar los registros remotos.

Una circunstancia especial de este caso, es que la persona investigada se conecte regularmente a una red inalámbrica pública (como puede ser un restaurante o un centro cívico). En ese caso sí que podría ser recomendable el realizar el registro remoto utilizando la misma red del investigado, puesto que a dichas redes se conectan infinidad de personas y el investigado no detectaría una presencia anómala en la misma. Aquí habría que tener en cuenta que también otras personas podrían monitorizar la información que circula por la misma, por lo que se haría necesario el uso de mecanismos de seguridad que garantizasen la integridad y la confidencialidad de la información recabada durante el registro remoto. Para este caso no sería necesario el adaptador USB de red inalámbrica.

En este último caso también se podría realizar un (Rogue AP, 2017) (un punto de acceso falso o fake AP) para que el investigado se conectara a una red con el mismo nombre que la red a la que se suele conectar, pero controlada por los investigadores en su totalidad. El (Rogue AP, 2017) se crearía utilizando el adaptador de red USB que se ha mencionado anteriormente.

- El registro remoto se realiza a través de Internet: obviamente, sería necesario contar con una conexión a Internet. Lo ideal es que dicha conexión esté anonimizada (que no se pueda vincular la dirección IP utilizada con los investigadores) y que tengamos una dirección IP pública fija (si el registro se va a realizar directamente desde un ordenador "normal" conectado a la red). Esta IP pública fija debería cambiar con cada registro remoto diferente que se realizara, es decir, sólo sería utilizada para un registro remoto en particular (durante la duración de la medida) de una investigación particular.

Independientemente de que la intrusión para el registro remoto se realice desde la propia red del investigado o desde fuera de la misma, será necesario contar con un (o varios) **ordenador para controlar la ejecución efectiva del registro remoto**.

En el supuesto de este Trabajo de Fin de Máster, que se va a hacer uso de la Ingeniería Social para la instalación del software que permita el registro remoto, como Sistema Operativo una opción válida es (Kali Linux, 2017), puesto que ya trae de serie, preinstaladas, un gran número de herramientas que permiten, tanto la generación del software que se va a utilizar en los registros remotos (mediante el uso de Framework de (Metasploit, 2017)), como herramientas para el uso de Ingeniería Social.

Este Sistema Operativo es recomendable que se encuentre instalado en una máquina virtual, puesto que se simplifica mucho el hecho de volver a puntos anteriores en el tiempo, gracias a los *"snapshots"* o capturas de estado de la máquina virtual.

Por lo tanto, también se necesitaría un software de virtualización, como pudiera ser (Oracle VM VirtualBox, 2017) o (VMWare Inc., 2017).

Para el desarrollo concreto de la presente metodología, los requisitos técnicos son:

- Ordenador Personal.
- Software de virtualización (Oracle VM VirtualBox, 2017).
- Máquina virtual (Kali Linux, 2017) 2016.2 de 64 bits, actualizada al completo.
- Adaptador USB de red inalámbrica (TP-LINK TL-WN722N, 2017) (no permite conexiones a redes Wi-Fi AC o en la banda de los 5 GHz) u otro tipo de hardware específico para auditoría de redes inalámbricas, como puede ser (WiFi Pineapple, 2017).
- En el caso de realizar el registro remoto a través de Internet (no en red local), sería necesaria una conexión con IP pública fija.
- Si el envío del correo al investigado se realiza con un dominio creado al efecto, sería necesario adquirir dicho dominio y configurar el servidor de correo electrónico para realizar los envíos desde el mismo.

Requisitos de formación

Se debe tener conocimiento de qué es lo que permite la Ley, las posibilidades que ofrece y qué no se puede realizar. Por lo tanto, aparte de la formación generalista que se posee, no estaría de más una formación legal específica en la materia.
También es necesario que los actuantes posean los conocimientos necesarios en el uso de las diferentes aplicaciones o software que se vaya a utilizar, como, por ejemplo: conocimientos de Linux (para el uso de (Kali Linux, 2017)), conocimiento del uso y posibilidades de (Metasploit, 2017) o del software que se vaya a utilizar para generar o utilizar con el objetivo de realizar los registros remotos, conocimientos de seguridad informática.
Esto conlleva el que los actuantes puedan estar actualizados con respecto a las nuevas vulnerabilidades que vayan apareciendo, las cuales podrían facilitar la instalación del software de registro remoto en los dispositivos a registrar. También, estarían actualizados en lo que respecta a las diferentes técnicas de intrusión que se pueden llevar a cabo (por ejemplo, las

nuevas técnicas para acceder a una red inalámbrica ajena), así como a las posibilidades que puede ofrecer el trabajar dentro de la misma red que el dispositivo que sobre el que se pretende ejecutar la medida.

Para la presente metodología, son necesarios los siguientes requisitos de formación:

- Conocimientos legales (ya reflejados en el primer apartado).
- Conocimiento en el uso de (Kali Linux, 2017) (fundamentalmente en el uso de herramientas de auditoría de seguridad y de ingeniería social).
- Conocimiento en el uso del Framework de (Metasploit, 2017) (instalado ya por defecto en (Kali Linux, 2017)), así como de las herramientas de inyección de (payload, 2017) en una aplicación o programa original.
- En el caso de realizar una intrusión en la red inalámbrica del investigado, o en el caso de crear un (Rogue AP, 2017), conocimiento en el uso de las herramientas de auditoría de redes inalámbricas.
- Caso de usar un dominio propio: conocimientos para registro de dominios en Internet, así como configuración del servidor de correo electrónico.
- Conocimiento de las técnicas de Ingeniería Social, así como de las herramientas utilizadas.

4.1.2. Descripción de la metodología

A continuación, en este apartado se procede a describir la metodología de intrusión en equipos para la investigación de delitos, mediante el envío del software necesario para el registro remoto al investigado. Por lo tanto, **se hará uso de la Ingeniería Social** para que éste proceda a abrir el mensaje recibido y/o proceda a la instalación del software indicado.

a) Descubrimiento del delito

El primer paso de todos es el de la **investigación de un hecho delictivo**.

Cuando se tiene conocimiento, por el medio que sea, de un hecho delictivo, éste es investigado por los correspondientes Grupos de Policía Judicial.

Una vez que se tiene conocimiento, **el hecho delictivo es calificado, de forma provisional,** pues al final será el Juez competente el que estime qué delito es, por los citados Grupos de investigación.

El hecho de calificar correctamente el hecho delictivo investigado resulta fundamental para la posibilidad de la solicitud de la medida del registro remoto, puesto que, como se ha mencionado anteriormente, tan sólo se permite la ejecución de dicha medida en una serie de hechos delictivos concretos.

Por lo tanto, una vez que se ha calificado el hecho delictivo, se debe **comprobar si éste es uno de los que se recogen en la legislación vigente, concretamente en el artículo 588 setpies a** (Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, 2015).

Si el hecho delictivo investigado no es uno de los recogidos en el citado artículo, entonces no se podrá solicitar autorización para la concesión del registro remoto.

Si se trata de uno de esos hechos delictivos, entonces, una vez agotadas todas las posibilidades de investigación (mediante el uso de las diferentes técnicas y fuentes de investigación), y siempre que resultara pertinente para la investigación, se podría solicitar la autorización de concesión de la medida del registro remoto.

Si se estima que resulta de interés el registrar remotamente algún dispositivo informático propiedad (o utilizado) por el investigado, se debe continuar con la adquisición de información, previa a la solicitud de la autorización de la medida.

b) Footprinting del objetivo

El footprinting consiste en **recabar toda aquella información que figure en fuentes abiertas del objetivo a investigar**. Es decir, a través de la consulta de información pública, accesible a todas las personas, se recabarán todos aquellos datos acerca del investigado que resulten de interés para la investigación.

No hay que olvidar que, en el escrito de solicitud de autorización del registro remoto, se deben incluir una serie de datos y éstos deben ser obtenidos por los investigadores, previamente a la realización de la solicitud.

Además, si queremos que la instalación del software para registro remoto se haga a distancia, se debe conocer el correo electrónico del investigado, o el teléfono móvil (caso de que el dispositivo a registrar sea éste y se envíe el enlace mediante un servicio de mensajería instantánea), o cualquier dato que permita la comunicación electrónica con el mismo.

Para recabar toda esta información, se muestran los pasos a seguir:

- La primera opción, y la más sencilla, es **hacer uso de un buscador estándar**, como puede ser Google. Con los datos conocidos de la persona investigada se realizan búsquedas simples en Google para observar qué información aparece en el buscador. Estas búsquedas se realizan mediante la introducción en buscadores como Google de los datos conocidos del investigado como: nombre y apellidos, DNI, matrículas de vehículos y demás datos que se conozcan. Lo que nos dará una primera aproximación de los datos que existen en Internet acerca del investigado.

- En relación con la anterior, y haciendo uso también de los buscadores genéricos, se realizarían búsquedas más refinadas, utilizando para ello los denominados (Dorks, 2017) **de Google o Bing**. Estos (Dorks, 2017) son operadores de consulta que se pueden utilizar en los buscadores, lo que permite realizar búsquedas más refinadas. Por ejemplo, se puede buscar por tipo de fichero (filetype:) o en un dominio concreto (site:) (Universidad de Costa Rica, 2017).

- Se puede hacer uso de las fuentes **OSINT** (*Open Source Intelligence*), como por ejemplo https://inteltechniques.com y http://osintframework.com, con los datos que se van obteniendo del objetivo.

A medida que se vayan consultando las anteriores fuentes, se irán obteniendo más datos del investigado que, a su vez, deberán volver a ser consultados en las mismas fuentes.

Mediante el uso de estos recursos, se recabará la mayor cantidad de información posible, relacionada con la investigación que, posteriormente, se incluirá en la solicitud de autorización el Juez de Instrucción.

Con los datos obtenidos a través de la realización del footprinting del objetivo, así como los datos de interés recabados durante la investigación policial, pasaríamos al siguiente punto, siempre y cuando esa información sea suficiente para poder realizar la solicitud con ciertas garantías. Por ello, se debe cotejar la información de la que se dispone, con la información que ha de constar en el escrito de solicitud y, por ende, en la ulterior autorización.

De no disponer de los datos suficientes, no se deberá realizar la solicitud de autorización, sino que se continuará con la utilización de técnicas de investigación policiales y con la adquisición de más datos a través del footprinting.

c) Elección del software para registro remoto a instalar (en función de los datos obtenidos durante el footprinting y la investigación anterior)

Este es uno de los puntos críticos en la metodología. Si bien, **queda a criterio del Juez la elección del software a utilizar**, como bien comenta Dª Lorena Bachmaier Winter (Winter, 2016), **los jueces no son expertos técnicos, por lo que tomarán muy en cuenta las indicaciones de los investigadores**, y de expertos externos a los que pueden consultar, a la hora de seleccionar el software a utilizar durante el registro remoto.

Por una parte, en función de los datos recabados anteriormente, puede ser que se tenga información completa acerca del dispositivo que se quiere registrar remotamente. Si se dispone de una información veraz y completa, entonces la elección del software a instalar se simplifica enormemente.

Con la información anterior se simplifica enormemente el proceso de elección porque, si se conoce la marca y modelo del dispositivo, el sistema operativo que utiliza y la versión instalada de éste, se puede elegir un software específico que ofrezca más garantías de cara a la instalación. Con esta información también se puede **comprobar si existen** (exploit, 2017) **operativos** (utilizando para ello el Framework de (Metasploit, 2017)), que pueden hacer más sencilla la diligencia del registro remoto del dispositivo.

Tristemente, este no suele ser el caso, puesto que, si bien podría ser relativamente sencillo averiguar la marca del dispositivo, e incluso el modelo, en el aspecto del sistema operativo ya habría mayores dificultades. Y no sólo respecto al sistema operativo en sí, sino sobre todo respecto a la versión que tiene instalada. No es lo mismo que esté instalado un Windows XP que un Windows 10 64 bits con todas las actualizaciones al día.

Se deben conocer, previamente a la redacción de la solicitud, al menos datos genéricos que permitan exponer en el oficio de solitud un software genérico que se pueda llegar a instalar.

Una opción que nos permite conocer más datos acerca del software que está instalado en los dispositivos es la herramienta (nmap, 2017), utilizada en redes públicas, puesto que aún no existe autorización para realizar la intrusión en la red del investigado. Esta herramienta puede proporcionarnos información muy útil como, por ejemplo, el sistema operativo instalado y los puertos que tiene abiertos dicho dispositivo.

Con la información adquirida, en la que, al menos, se debe conocer el sistema operativo (o qué software es, en caso de bases de datos), existen dos opciones para determinar el software a utilizar para el registro remoto, haciendo uso del Framework de (Metasploit, 2017):

- **Si se tiene un conocimiento completo y específico del sistema operativo utilizado por el dispositivo a registrar, así como la versión del mismo**, se realizaría la **búsqueda de un** (exploit, 2017) para el mismo, que será el utilizado para el registro remoto mediante el uso de (payload, 2017) asociado al mismo. De este modo, normalmente, evitaremos que el investigado tenga que realizar una instalación al uso, ya que nos aprovecharemos de una vulnerabilidad del sistema, que facilitará el acceso al mismo, con el objetivo de realizar el registro remoto.

- **Si se conoce el sistema operativo utilizado, pero se desconoce la versión utilizada, o no se ha podido encontrar un** (exploit, 2017) **disponible**, se utilizaría una **aplicación o programa comercial original, que sería modificado mediante la inyección de un** (payload, 2017) de (Metasploit, 2017). Para ello se puede hacer uso de herramientas como (msfvenom, 2016), (apkinjector, 2017) o (spade, 2016), con las que se puede generar el software que se utilizará para el registro remoto. Se deberá especificar la dirección IP por la que los investigadores van a recibir la información (ya que se utilizará una conexión tipo *"reverse"*, es decir, es el dispositivo del investigado el que realiza la conexión con los investigadores y no al revés). Por lo tanto, si el registro se va a realizar a través de Internet, se deberá poner la IP pública que utilicen éstos. Si se va a realizar en una red local, habrá que introducir la IP privada que se vaya a utilizar.

El asunto de la IP utilizada por los investigadores es crucial, ya que, si la IP introducida no coincide con la que efectivamente tengan en el momento de realizar el registro, éste no se podrá llevar a efecto. Por lo tanto, hay que asegurarse de que la IP que se introduce se va a mantener en el tiempo. Una buena medida temporal serían 3 meses, puesto que es el tiempo máximo total (prórrogas incluidas) por el que puede autorizarse la medida del registro remoto en un equipo informático.

De todos modos, aunque en este punto se realice la elección del software a utilizar, es una vez que se ha concedido la autorización cuando se debe realizar de forma efectiva la generación del software. Por lo tanto, es en la preparación de la instalación cuando se deben tener en cuenta los extremos que se refieren a la IP que se va a utilizar.

Siempre existe la opción de, si la autorización se concede, explicar los extremos que se vayan averiguando en relación al dispositivo a registrar, mediante posteriores oficios al Juez competente, de modo que se pueda especificar mucho más el software que se podría utilizar.

d) Solicitud al Juez de Instrucción

Una vez completada la fase anterior, teniendo la seguridad de que se poseen todos los datos necesarios para realizar la solicitud, es cuando se realizaría ésta.

Nunca está de más **hablar directamente con el Juez Instructor competente** y también con el Fiscal, puesto que siempre podrán facilitar información acerca de si los datos recabados hasta el momento, o la gravedad de los hechos delictivos investigados, son suficientes para poder llegar a conceder la autorización de la medida del registro remoto.

Está claro que toda la información ha de ser facilitada mediante el correspondiente escrito (Oficio), pero siempre quedará mucho más clara la explicación, y la envergadura de la investigación, mediante una exposición de los mismos de viva voz.

Además, de este modo implicaremos aún más a los anteriormente mencionados en la investigación, lo que permitirá que ésta avance y se resuelva de una mejor forma y con todas las garantías.

Si existe necesidad de que uno de los sujetos obligados por la legislación vigente, artículo 588 septies b (Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, 2015), **colabore en la investigación, deberá reflejarse también en la solicitud de autorización**.

Puede ser de interés solicitar la colaboración de los sujetos obligados en casos como los siguientes:

- Para realizar el envío de los mensajes al investigado. Este mensaje contendrá el enlace al software a utilizar en el registro remoto.
- Para conocer los datos específicos del software que utiliza el dispositivo a registrar.
- Para facilitar la instalación del software en el dispositivo a investigar.

Ya se ha abundado anteriormente en la **información y datos que han de figurar en el escrito de solicitud**, por lo que se remite al **apartado "4.1.1 Identificación de requisitos", apartado de "Requisitos legales", del presente Trabajo de Fin de Máster**.

En el **Anexo I** figura un **Oficio tipo para la solicitud de la medida** de registro remoto en equipos informáticos.

e) Instalación del malware (mediante ingeniería social)

Este paso es el paso crucial de la metodología, puesto que, **si no se consigue que el investigado instale el software en el dispositivo a registrar (o haga click en el enlace que se le ha enviado), no se podrá llevar a efecto la ejecución de la medida**.

La Ingeniería Social se basa en actuar en el eslabón más débil en la cadena de la seguridad en los equipos informáticos: las personas.

Por muy bien protegido que esté un sistema o dispositivo informático, si se consigue "convencer" a una persona para que realice una acción insegura, de nada servirán todos los mecanismos de seguridad que posea aquél.

Tal y como indica Pablo F. Iglesias (F. Iglesias, 2015), para que esta técnica tenga más opciones de éxito, debemos ofrecer algo al objetivo, **algo que sea de su interés** y que pueda tener cierto valor para esa persona. Por ejemplo, se le puede ofrecer una nueva aplicación que es sólo para clientes Premium. O bien ofrecerle un enlace que garantiza una actualización de una aplicación, para evitar que ésta sea atacada. Es decir, algo que tenga valor para esa persona.

Debe inculcarse una sensación de **cierta premura**, es decir, que esa persona no tenga demasiado tiempo para pensar en las acciones que va a realizar, puesto que, de lo contrario, es probable que no realice la acción que se desea (instalar el software o hacer clic en el enlace). Siguiendo con el ejemplo anterior, se le comunicaría que esa aplicación para clientes *Premium* estará disponible por un tiempo muy limitado, porque es muy valiosa. O en el caso de la actualización de seguridad, habrá que comunicar que es una actualización muy urgente, porque se están produciendo ataques masivos que están permitiendo a los atacantes obtener información personal de ese dispositivo.

Hay que dar **confianza al objetivo**, de tal modo que no sospeche que la acción que se le invita a realizar, realmente no es beneficiosa para éste. El aspecto que pueda tener el correo o mensaje que se le envía es de suma importancia. Nuevamente, siguiendo con los ejemplos anteriores, si se le ofrece una actualización de la aplicación en la que el correo enviado contiene los logos de esa aplicación, con las direcciones y demás datos de la empresa propietaria, es mucho más probable que lleva a cabo a acción que si, simplemente, se le envía una página en blanco con un enlace. Lo mismo ocurriría en el caso de la actualización. Es muy importante dar sensación de que el remitente es la empresa auténtica (o al menos es una entidad de carácter oficial o serio).

Si en ese mismo correo o mensaje, **indicamos al objetivo que ya se han realizado multitud de actualizaciones anteriormente**, añadiendo, por ejemplo, nuevas funcionalidades, dudará menos de una nueva actualización, que además es de seguridad. Quizá piense que las actualizaciones anteriores le llegaban automáticamente, pero si se le justifica que, justo esta actualización no se realiza de esa manera porque, al tratarse del arreglo de un problema de seguridad, se necesitan permisos especiales para realizarla, facilitará el camino a que finalmente se instale el software.

También en relación con lo anterior, si el mensaje va firmado por el "Jefe del Departamento de Seguridad" o similar, que denote **cierta autoridad** al remitente, facilitará también la instalación del software.

Finalmente, si en el mensaje que se envíe podemos ofrecer cierta **sensación de pertenencia a un grupo concreto**, hará que el objetivo no perciba que está realizando una acción que sólo él la va a llevar a cabo, sino que existen más personas que ya la han realizado y que están contentas con el resultado obtenido. Un ejemplo podría ser el añadir en el mensaje cierto número de opiniones de otros usuarios, manifestando lo satisfechos que están por haber actualizado determinada aplicación, o por haber instalado ese software *Premium* y al que sólo unos pocos han podido tener acceso.

Ilustración 2. Ejemplo de correo Ingeniería Social (El Confidencial, 2015)

En la "Ilustración 2" se puede observar el correo electrónico que suele llegar todos los años a una gran cantidad de personas, cuando llega el momento de realizar la Declaración de la Renta.

Como se puede observar, se utiliza el nombre de la “Agencia Tributaria” para dar aspecto de seriedad, autoridad y confianza. Además, la Declaración de la Renta es algo que todo el mundo realiza, con lo que da sensación de pertenencia al grupo y no se tiene la percepción de que es una acción aislada, pues el propio objetivo también realiza la Declaración de la Renta anualmente. En este caso, además, se ofrece algo que es muy valioso para el objetivo, nada menos que una devolución de dinero, y de este modo se incluye también la urgencia a la hora de rellenar los datos, puesto que, cuanto antes se envíen, antes, supuestamente, se recibirá el dinero en la tarjeta introducida.

Para poder hacer uso de este modo de envío, es **necesario conocer todos los datos obligatorios, como puede ser el email** que usa la persona investigada.

Caso de no conocerse alguno de esos datos, se podrían llevar a cabo las **siguientes acciones, siempre antes de realizar el envío con el enlace al software a instalar**:

- La principal medida sería **introducirse en la red inalámbrica del investigado y capturar el tráfico**, con el objetivo de conocer aquellos datos que fueran necesarios. Para conocer esos datos que pudieran faltar, se puede hacer uso de las siguientes herramientas:
    - Escaneo de puertos con (nmap, 2017).
    - Un framework para (MITM, 2017) como (bettercap, 2017), el cual puede ofrecer información acerca de los dispositivos de la red.
    - Capturar el tráfico con herramientas como (wireshark, 2017) o similares.
- Para acceder a dichas red inalámbrica, se haría uso de un adaptador inalámbrico independiente del que posee el ordenador utilizado (hay que recordar que se trabaja utilizando una máquina virtual, por lo que el adaptador inalámbrico del ordenador no es accesible), así como la herramienta (wifite, 2014) de (Kali Linux, 2017). También se puede hacer uso de hardware específico para auditoría de redes inalámbricas, como puede ser (WiFi Pineapple, 2017).
- **Caso de que el investigado no tuviera red inalámbrica en su domicilio** (o en un domicilio de un tercero), se averiguaría si se conecta regularmente a través de alguna **red inalámbrica pública**. Si es así, caben 2 opciones: **aplicar las herramientas anteriores** directamente en esa red, o; **crear un** (Rogue AP, 2017) haciendo uso de (Kali Linux, 2017) o (WiFi Pineapple, 2017), para que el dispositivo del investigado se conecte a éste en vez de conectarse a la red inalámbrica legítima. Este último caso

sería mejor, puesto que el tráfico y los dispositivos conectados serían menores, lo que facilitaría la investigación, aunque también es cierto que técnicamente es más complicado crear este (Rogue AP, 2017) que directamente capturar el tráfico de la red inalámbrica pública.

Una vez que se poseen todos los datos necesarios, en el caso del presente Trabajo de Fin de Máster, en el que se usa la Ingeniería Social, se propone la **siguiente secuencia**:

- Con los datos que se han conseguido del objetivo, y del dispositivo que se quiere registrar remotamente, tendremos información suficiente para conocer los gustos de aquél. Por lo tanto, mediante el uso de una herramienta como (httrack, 2017) **clonaremos una página web de una temática que resulte de su interés**. Es decir, la página mostrará una descarga o programa a instalar que resulte atractivo para el objetivo. Hay que recordar que parte de la Ingeniería Social es ofrecer algo y darle confianza y autoridad a la página que se le envía.

  Puede ocurrir que, si la página clonada es demasiado pesada, dé problemas al enviar el correo y no supere el filtro de *spam* del correo del investigado. Para solucionar este problema, lo que se puede hacer es utilizar como referencia la página clonada y construir una propia, con el aspecto e imágenes de la anterior.

  Para tratar de evitar el filtro de *spam*, la dirección URL en la que se aloja el software que se pretende instalar, no deberá figurar en el cuerpo del correo, pudiéndola incluir en una etiqueta “”Texto””. En el texto tampoco deberán figurar palabras como “pincha aquí” o similares, puesto que los filtros de *spam* las detectarían.

- Una vez clonada la página, **modificamos la zona de descarga (si la hay, y si no, se puede crear)** para **que apunte directamente al software que se pretende instalar en el dispositivo a registrar remotamente**, y que ya se ha generado en función del dispositivo concreto a registrar (teniendo en cuenta las recomendaciones referentes a la URL del primer punto, así como lo referente a la dirección IP que se va a utilizar para la conexión).

  - Como medida extra, sería factible realizar un **acortamiento de la URL** a la que se apunta (con servicios como (tinyurl, 2002)), de modo que no se vea la dirección del servidor desde que será descargada la aplicación que se quiere instalar.

  - Además, en los casos en los que la intrusión se realice en una red local en la que estemos identificados, y el envío que se realice sea de un enlace, junto

con el dispositivo a registrar, podremos realizar (DNS spoofing, 2017) para que afecte al citado dispositivo. De este modo, el enlace que se puede enviar al investigado puede contener una dirección "real", pero, sin embargo, al hacer click sobre la misma, le llevará a la dirección que nosotros hemos preparado con el software a descargar e instalar. Así, el propio enlace no generará tanta desconfianza como si la URL mostrara la IP real o fuese una URL acortada.

- Una vez se tiene la página clonada modificada a conveniencia, apuntando al software que se pretende instalar, debemos **enviar un correo electrónico al objetivo**. En este correo electrónico figurará citada página. El "asunto" del *email* y el "remitente" son campos muy sensibles pues, como ya se ha dicho anteriormente, se debe generar confianza y dar sensación de autoridad sobre el investigado, además de tener en cuenta a los filtros de *spam*. Con respecto al envío de los emails, habría que seguir una de las siguientes opciones:

    - **Contar con un servidor de correo propio**, para evitar que los correos enviados al investigado sean trasladados a la carpeta de *spam* del investigado.

    - Como la legislación vigente prevé, en el artículo 588 septies b (Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, 2015), los investigadores pueden **solicitar la colaboración de los sujetos obligados**. Esto podría incluir el remitir el correo utilizando el servidor de correo del ISP (como pueden ser Movistar o Vodafone) utilizado por el investigado, lo que ayudaría con respecto a la sensación de veracidad del mismo.

    - **Crear una cuenta de correo en uno de los servicios gratuitos** (como Gmail, Outlook o Yahoo!), que será la utilizada para realizar el envío, haciendo uso de herramientas para anonimizar la conexión (como, por ejemplo, realizar el alta y las conexiones a través de (TOR, 2017)). Esta opción no nos permitirá el modificar el dominio utilizado por el remitente (los correos llegarán como @gmail.com, @outlook.es, o el nombre del proveedor que se haya elegido), pero permitirá que el correo enviado no acabe en la carpeta de *spam* y dará más opciones a que el investigado abra el correo que se le envió previamente.

    - Si no se puede hacer uso de ninguna de las anteriores opciones, se podría hacer uso de una herramienta como (sees, 2014), que permite el **envío de emails suplantando la identidad del remitente**. Para hacer uso de esta

herramienta también es necesaria la instalación de (postfix, 2017) y de (mailutils, 2010), todo ello en (Kali Linux, 2017). Probablemente, el correo enviado mediante el uso de las herramientas mencionadas acabe filtrado como *spam*.

Además, desde el 1 de junio de 2017, Google ha mejorado la seguridad y el filtro anti spam (Wen, 2017), por lo que los correos electrónicos enviados de esta forma no llegarán al destinatario.

El día 5 de junio de 2017 se han realizado pruebas, tratando de enviar un email suplantando la identidad del remitente a una cuenta de Gmail y, efectivamente, el correo ni siquiera aparece en la carpeta de *spam*. Gmail directamente lo descarta y no lo entrega al usuario, al detectarlo como posible spam. Cabe decir que el citado correo enviado, ni siquiera incluía enlace alguno o imágenes. Es por ello, que **este método no se recomienda para la práctica de la metodología propuesta**.

- **Caso de que el equipo a registrar sea un teléfono móvil**: en este caso también existe la opción de **enviar al investigado un mensaje SMS o similar**, es decir, en vez de utilizar su correo electrónico como dirección de envío, utilizar su número de teléfono. Aquí también se puede hacer uso del deber de colaboración que prevé la legislación en el artículo 588 septies b (Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, 2015) y que sea el propio ISP el que facilite la tarea del envío de dichos mensajes (que contendrán un enlace apuntando al software de registro remoto que se desea instalar).

- Ahora llega el paso más difícil: que el investigado pulse sobre el enlace al archivo, lo descargue y lo instale. No se puede hacer nada, excepto seguir todas las recomendaciones anteriores respecto a la Ingeniería Social, para poder llegar a este punto con éxito. Aun haciendo todo correctamente, depende de la voluntad del investigado el instalar la aplicación o no hacerlo.

  En el **correo (o mensaje) que se ha enviado**, no estaría de más **introducir una breve explicación del proceso de instalación**, para que la persona investigada reduzca sus sospechas cuando el sistema le solicite permisos durante la instalación. Esto es de especial utilidad con los teléfonos móviles, pues se va a intentar instalar una aplicación que no proviene de un "*market*" oficial, por lo que, en teléfonos con sistema

operativo “Android” será necesario el permitir la instalación de otras fuentes (por defecto, Android únicamente permite la instalación de aplicaciones provenientes de (Google Play, 2017)). Explicar las acciones a realizar puede dar sensación de confianza al investigado para que, efectivamente, instale el software enviado.

Además, se pueden explicar las “razones” de enviarle el enlace de descarga por ese medio, así como opiniones positivas de “clientes” y otra información que pueda facilitar la instalación.

Si se ha hecho todo correctamente, el investigado ha creído en los datos que figuran en el correo electrónico que se le ha enviado y, por lo tanto, ha instalado el software de registro remoto, se puede pasar al siguiente paso de la metodología.

Si, agotado el tiempo inicial de la autorización, no se ha conseguido, por motivos técnicos, lograr la ejecución efectiva del registro remoto (no existen (exploit, 2017) operativos, el objetivo no ha accedido al correo electrónico enviado o el investigado no ha instalado el software), habría que informar de estos extremos al Juez competente, solicitando una prórroga alegando los motivos anteriormente expuestos (ver apartado “Solicitud de prórroga”). Incluso, si se observa que la intrusión a distancia, mediante el uso de Ingeniería Social, no es factible, debido a las medidas de seguridad técnicas que adopta el investigado (no apertura de correos de remitentes desconocidos o no instala software no proveniente de markets oficiales), se podría llegar a solicitar que la instalación del software se realice mediante el acceso físico al dispositivo (si fuera posible).

f) Explotación del dispositivo (ejecución efectiva de la medida de registro remoto)

Una vez que se ha conseguido la instalación del software necesario para la ejecución del registro remoto, hay que proceder a realizar dicho registro.

Para ello haremos uso de (msfconsole, 2017), el manejador que tiene el Framework de (Metasploit, 2017). De este modo, mediante el uso de (msfconsole, 2017) y ejecutando un (payload, 2017) tipo (meterpreter, 2017), podremos llevar a cabo el registro remoto una vez que el software ha sido instalado en el dispositivo.

La herramienta de escucha debe ser configurada con la IP utilizada por los investigadores. En este caso, sólo hay que introducir la IP privada de los mismos, puesto que, aun en el caso de utilizarse Internet para realizar el registro remoto, la IP pública ya figura en el (payload, 2017) instalado en el dispositivo a registrar, por lo que tan solo es necesaria al IP desde la que los investigadores se encuentran a la escucha (por ejemplo, si la conexión de los investigadores por Internet se realiza a través de un router, éste facilitará una IP privada a los mismos, que

es la que se debe introducir, puesto que la petición de conexión llegará al router mediante la correspondiente IP pública que se ha introducido en el (payload, 2017) instalado en el dispositivo).

Recordemos que ese software, lleva embebido un (payload, 2017) creado con (Metasploit, 2017), que va a permitir registrar el equipo de forma remota (y otras muchas más opciones, como la geolocalización, que no serán de aplicación al registro remoto, por las limitaciones legales del mismo).

Así, se podrá navegar por todos los datos del dispositivo, llevando a efecto el registro remoto del mismo. Es decir, se deben localizar todos aquellos datos que sean de relevancia para la investigación.

Una vez localizados dichos datos, si en el escrito de solicitud al Juez, se ha solicitado la realización de copias de los datos que figuren en el dispositivo (que será lo habitual y lo recomendado en la presente metodología), que puedan resultar de interés para la investigación, se deben realizar esas copias manteniendo la integridad de los datos.

Lo ideal sería realizar un (hash, 2017) de los archivos que se van a copiar cuando están todavía en el propio dispositivo registrado.

En el caso de uso de (Metasploit, 2017) esto sí que es posible, haciendo uso del comando “checksum” de (meterpreter, 2017), aunque sólo permite la opción de utilizar (MD5, 2017) o (SHA-1, 2017), ambas funciones hash ampliamente superadas por nuevas funciones (hash, 2017) más robustas, como (SHA-2, 2017).

Después de realizar ese (hash, 2017) previo, se procede al copiado de los datos del dispositivo registrado a un dispositivo en poder de los investigadores.

Una vez finalizada la copia de los datos que sean relevantes para la investigación, volvemos a realizar un hash de los archivos originales en el dispositivo y realizamos un (hash, 2017) a los archivos copiados en el dispositivo externo.

Esos hashes calculados se comparan y, si los tres valores son idénticos, indica que esos archivos no han variado desde que han sido observados en el dispositivo hasta que han sido copiados por los investigadores. Como se observa en la figura de debajo (Ilustración 2), si “Valor 1=Valor 2=Valor 3”, significa que el archivo no ha sido modificado. Estos valores, reflejados en la correspondiente Acta, permitirán comprobar que, desde que se ha realizado la copia, el archivo no ha sido modificado (comparándolo con el valor del (hash, 2017) que se calcule en cualquier momento del proceso penal) durante todo el proceso.

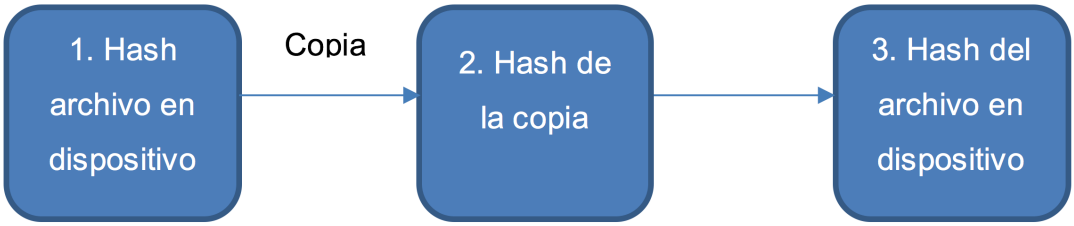

Ilustración 3. Flujo de cálculo de hash de los datos copiados

Todo este proceso debe estar documentado, realizando las pertinentes Actas de registro del dispositivo, firmadas por los agentes que han sido autorizados por el Juez para la realización de la medida.

Aquí merece la pena hacer un inciso con respecto a este apartado del registro remoto.

En un registro domiciliario, es el Secretario judicial quien se encarga de levantar la correspondiente Acta de registro y, de este modo, dar fe pública de lo que se está realizando. Además, en los registros domiciliarios, se cuenta, normalmente, con la presencia de la persona investigada (o detenida), así como con la presencia de su abogado, lo que da a la citada diligencia de registro domiciliario muchas garantías legales.

Sin embargo, en los registros remotos no se cuenta con la presencia del Secretario judicial durante la práctica del registro. Tampoco se cuenta con la presencia del investigado (algo obvio por otra parte, ya que el objetivo de la medida del registro remoto es ser llevada a cabo sin el conocimiento de éste). Estas y otras reflexiones las ofrece Dª Lorena Bachmaier Winter (Winter, 2016), y son extremos que la jurisprudencia se encargará de delimitar, aunque está claro que no está previsto en la legislación vigente (como sí que lo está en el caso de los registros domiciliarios). Por estas razones, es por lo que se propone la realización de un Acta, por parte de los agentes habilitados para el registro remoto, en el que consten todas las acciones que se han llevado a cabo durante el mismo. De este modo, quedará constancia por escrito de todas ellas.

g) Informe periódico al Juez de Instrucción con las novedades de la investigación

A medida que el registro remoto se está ejecutando, se debe informar al Juez competente de los avances que se han realizado en la investigación en curso.

Es muy importante el describir la relevancia de lo encontrado durante la ejecución de la medida. De lo contrario, si el Juez observa que no se han realizado avances en la investigación o, mejor dicho, que la aplicación de la medida no está sirviendo a los efectos

para los que se autorizó, decretará el cese de la misma, puesto que una medida de este tipo, con una alta injerencia en los derechos del investigado, no puede ser mantenida en el tiempo injustificadamente.

Aparte de informar sobre la cantidad de datos que se han encontrado, habrá que realizar un análisis de los mismos (tanto del propio contenido del fichero, como de los metadatos asociados), para que puedan facilitar una información lo más completa posible en relación con la investigación.

Ello se debe a los requisitos legales que exige la medida, los cuales ya han sido expuestos anteriormente en el presente Trabajo de Fin de Máster.

Este informe, debe ser remitido con la frecuencia que haya indicado el Juez competente a la hora de conceder la medida. Por lo tanto, habrá que atenerse a lo que figure en el Auto de autorización correspondiente.

h) Solicitud de prórroga (en su caso)

En el caso de que la duración de la autorización inicial concedida no sea suficiente, a criterio de los investigadores, se puede solicitar al Juez competente que autorice una prórroga de dicha autorización. Como ya se ha reflejado anteriormente, la duración máxima de la medida, incluyendo las posibles prórrogas que se concedan, jamás podrá ser superior a tres meses.

El tiempo de la autorización inicial puede no ser suficiente si se dan las siguientes circunstancias:

- **No se ha conseguido instalar el software necesario** para realizar el registro remoto en el período inicial autorizado. Esto puede deberse a varios factores, como, por ejemplo: que el investigado no haya abierto (o recibido) el correo electrónico que se le ha enviado; que el mensaje sí que haya sido recibido, e incluso abierto, pero el investigado no haya procedido a instalar el software en el dispositivo a registrar.

- **El software esté efectivamente instalado, pero no se haya podido llevar a efecto el registro en sí por parte de los investigadores** (debido, fundamentalmente, a que la instalación se haya producido en el tramo final de la autorización o a que el investigado no se hubiera conectado a la red desde la instalación del software).

- Además del caso anterior (que el período inicial de la autorización no sea suficiente), también puede ocurrir que, **a criterio de los investigadores y justificado por los datos objetivos reunidos por éstos durante la investigación en curso, se estime necesario prorrogar la medida,** aunque ya se haya procedido a la ejecución del

registro, debido a que se espera que se almacene más información en dicho dispositivo, que pueda resultar de interés para la investigación.

La solicitud de la prórroga deberá cumplir con los mismos requisitos indicados para la solicitud de autorización inicial, además de incluir todos aquellos hechos de interés que se hayan descubierto gracias a la aplicación de la medida hasta el momento, y justificando la necesidad, para llevar a buen fin la investigación, de una prórroga de la medida inicialmente autorizada.

i) Solicitud de cese de la medida

Esta es una solicitud que, en numerosas ocasiones, no se realiza. Normalmente se suele esperar a que expire el período concedido una vez que se ha obtenido toda la información posible mediante la aplicación de la medida.

Pero el método ideal sería **solicitar al Juez competente el cese de la medida una vez que se han completado los objetivos planteados en la investigación**.

De este modo, los derechos fundamentales del investigado no se verían intervenidos sin necesidad.

En el escrito de solicitud habría que justificar esta solicitud de cese, mediante la explicación detallada al Juez de toda aquella información que se ha conseguido obtener, relevante para la investigación, y los indicios que se tienen por parte de los investigadores de que la continuación de la medida no va a ofrecer nuevos datos relevantes para la misma.

Los investigadores han de estar muy seguros de que, efectivamente, no van a obtenerse más datos de interés con la aplicación de la medida del registro remoto. De lo contrario, lo más prudente es continuar con la aplicación del registro remoto hasta la finalización de la autorización. De este modo, puede que, aunque en un principio no se estimara muy probable la aparición de nuevos datos relevantes, efectivamente éstos aparezcan en la ejecución de la medida durante el tiempo autorizado. A continuación, la “Ilustración 4” muestra el diagrama de flujo de la metodología propuesta.

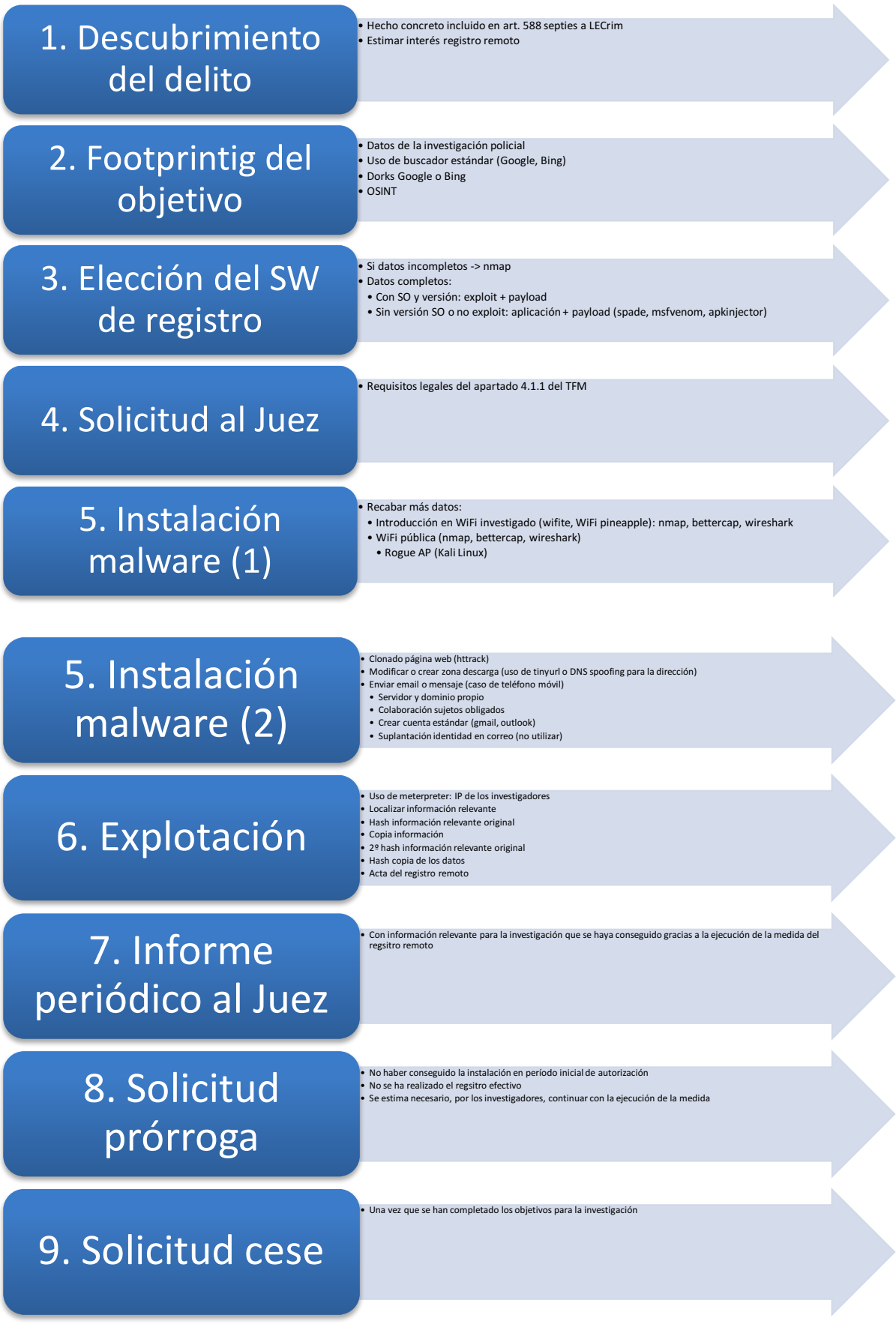

Ilustración 4. Flujo de la metodología propuesta

4.1.3. Evaluación

En el supuesto que se va a llevar a cabo (una simulación práctica, pero sin ninguna relación con ninguna investigación real, se deben tener ciertas condiciones o requisitos, las cuales se exponen a continuación:

- El Grupo de Investigación que va a llevar a cabo la investigación es el Grupo de Delitos Tecnológicos de una Comisaría Provincial de Policía, aunque podría ser cualquier grupo de investigación de cualquier Cuerpo de Policía competente para la investigación al caso, como podría ser Guardia Civil, Ertzaintza o Mossos d'Esquadra.

- El software utilizado para la evaluación es en su totalidad gratuito, debido a que no se tiene acceso, por motivos de confidencialidad, al software específico que pudieran usar las diferentes unidades de investigación.

- El hardware utilizado es en su totalidad propiedad del autor del presente Trabajo de Fin de Máster, no pudiendo tener acceso a otro tipo de hardware que pudiera resultar más especializado, como puede ser (WiFi Pineapple, 2017).

- Evidentemente, no se puede contar en la simulación con la colaboración de los sujetos obligados. Esta colaboración haría mucho más sencillo el envío del enlace (o directamente del software a utilizar) a la persona investigada.

a) Descubrimiento del delito

Por el Grupo de Investigación se ha tenido conocimiento de que una persona, cuyo nombre es Arturo ESPAÑOL ESPAÑOL (en adelante "Arturo"), podría estar realizando fotografías de carácter sexual a menores, haciendo uso de su teléfono móvil particular.

Igualmente, se tiene conocimiento de que, una vez realizadas las fotografías, éstas son copiadas a un dispositivo de almacenamiento USB (un *pendrive*), el cual remite a diferentes personas mediante el uso de una empresa de paquetería urgente.

Una vez se conocen estos datos, lo primero que se debe realizar es una calificación provisional de los hechos de los cuales se tiene conocimiento, con el fin de comprobar si resulta ser un hecho delictivo y encuadrarlo dentro de un delito del Código Penal (Ley Orgánica 1/2015, de 30 de marzo, del Código Penal, 2015).

En este caso concreto, los hechos de los que se tiene conocimiento podrían encuadrarse en el artículo 189.1.a) (Ley Orgánica 1/2015, de 30 de marzo, del Código Penal, 2015) por elaborar material pornográfico utilizando a menores de edad, ya que, supuestamente, realiza

él mismo las fotografías con su teléfono móvil; artículo 189.1.b) (Ley Orgánica 1/2015, de 30 de marzo, del Código Penal, 2015) por realizar la distribución de pornografía de menores, puesto que envía las imágenes a terceros; artículo 189.2.a) (Ley Orgánica 1/2015, de 30 de marzo, del Código Penal, 2015), ya que pudiera ser que la edad de los menores fuera inferior a los 16 años; artículo 189.5 (Ley Orgánica 1/2015, de 30 de marzo, del Código Penal, 2015) con respecto a los receptores de las imágenes pornográficas de menores.

Como se puede observar, los hechos relatados resultan delictivos en función del actual Código Penal, por lo que procede su investigación por el Grupo correspondiente.

Una vez se tiene la calificación provisional de los hechos, se debe comprobar si éstos se incluyen en el listado de delitos del artículo 588 septies a (Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, 2015) sobre los que se permite la ejecución de la medida del registro remoto.

Se comprueba el citado artículo y, efectivamente, cabe la aplicación de dicha medida en la investigación del presente delito, puesto que se trata de un delito cometido contra menores de edad.

Como se cumplen las condiciones de que el hecho investigado constituya un delito, y que dicho delito se encuentra en los supuestos contemplados en la legislación para la adopción de la medida del registro remoto, ahora se debe estimar la necesidad de la aplicación de dicha medida.

En el presente supuesto, está claro que la gravedad de los hechos (hasta 9 años de prisión) aconseja el llevar a cabo todas aquellas opciones que sean posibles en la investigación, entre las que se encuentra el registro remoto.

Además, al utilizar el investigado de su teléfono móvil para realizar las fotografías, hace que la adopción de la medida del registro remoto se torne ideal para la investigación. Una vez que se hayan agotado todas las anteriores opciones de investigación, por supuesto.

Si se autoriza esta medida, además de poder comprobar que las fotografías se realizan con su teléfono móvil, se podría averiguar la dirección de las personas que requieren de esas imágenes, puesto que pueden estar almacenadas en dicho dispositivo.

De no poder demostrar que es “Arturo “quien realiza directamente las fotografías, no se le podría condenar por el delito previsto en el artículo 189.1.a) (Ley Orgánica 1/2015, de 30 de marzo, del Código Penal, 2015), ya que no se podría llegar a demostrar la elaboración.

Es un hecho que resulta de interés, puesto que la pena no será la misma si se demuestra que él elabora el material pornográfico y, además, lo distribuye o vende, que, si sólo se consiguiera demostrar que lo distribuye, sin poder acreditar la elaboración.

Por estas razones, una vez agotadas todas las anteriores técnicas de investigación, se estima necesario para el buen término de la investigación, la solicitud de autorización de registro remoto del teléfono móvil de “Arturo”.

b) Footprinting del objetivo

En este paso de la metodología, se trata de recabar la mayor cantidad de información posible del objetivo, utilizando fuentes abiertas.

Como complemento, también se tiene en cuenta la información recabada durante la investigación policial habitual, que puede facilitar datos que harán más completa la búsqueda de información.

En el presente caso, los datos que se conocen sobre el investigado (resultado de las investigaciones policiales previas y consulta a diversas fuentes de información) son los siguientes:

- Número de teléfono 66-666-666
- Correo electrónico: jreacherprueba@gmail.com
- Teléfono móvil: Samsung Galaxy S4, con sistema operativo Android (se desconoce la versión).
- Nombre, apellidos, DNI y domicilio del investigado.

Con estos datos, se deben realizar búsquedas en los motores de búsqueda tradicionales como Google o Bing. Hay que tener en cuenta que, para la realización de la presente simulación, el nombre del investigado no es real y, por lo tanto, su actividad en numerosas páginas no es la habitual (no tiene facturas, ni coches, ni figura en una universidad).

Sin embargo, al realizar una búsqueda mediante OSINT, sí que aparece que tiene una cuenta en Facebook, en la que figura el nombre de “Arturo Brichburguer Español”, como se puede observar en la “Ilustración 5” e “Ilustración 6”. También se tiene acceso, aun sin estar registrado en Facebook, a la información que figura en la “Ilustración 7”.

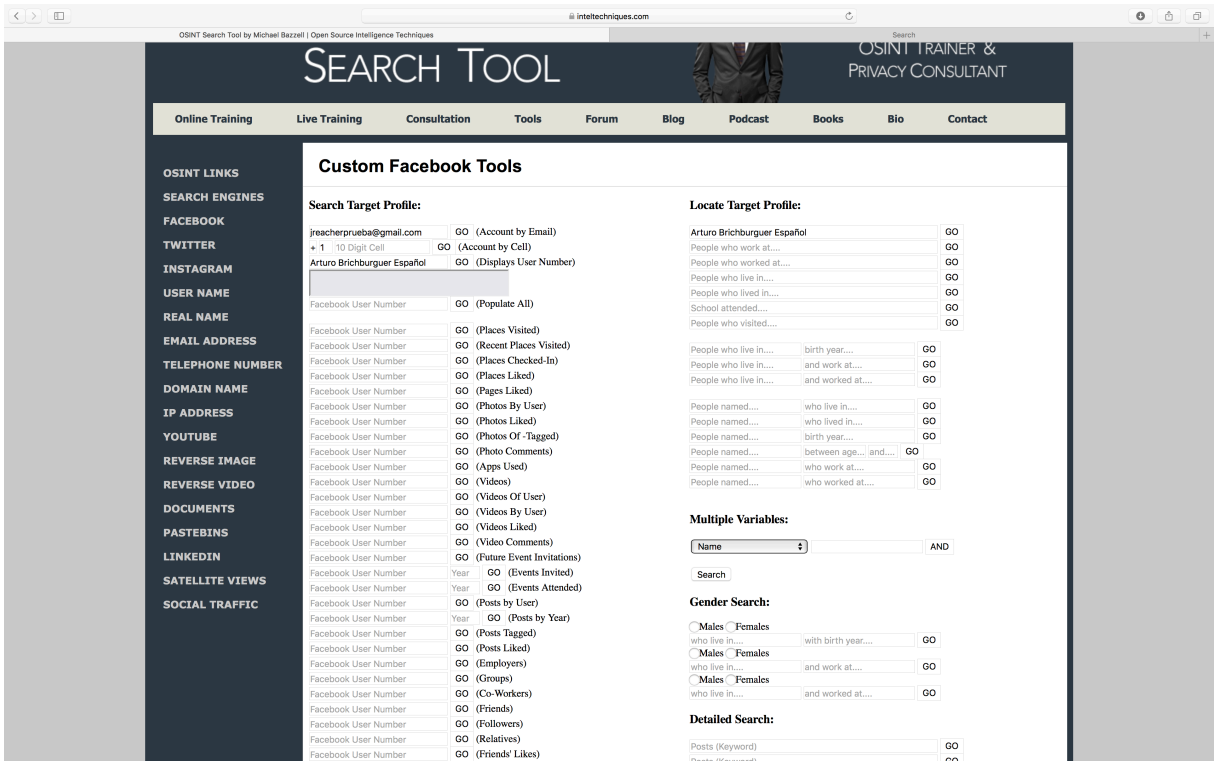

Ilustración 5. Consulta OSINT del correo del investigado

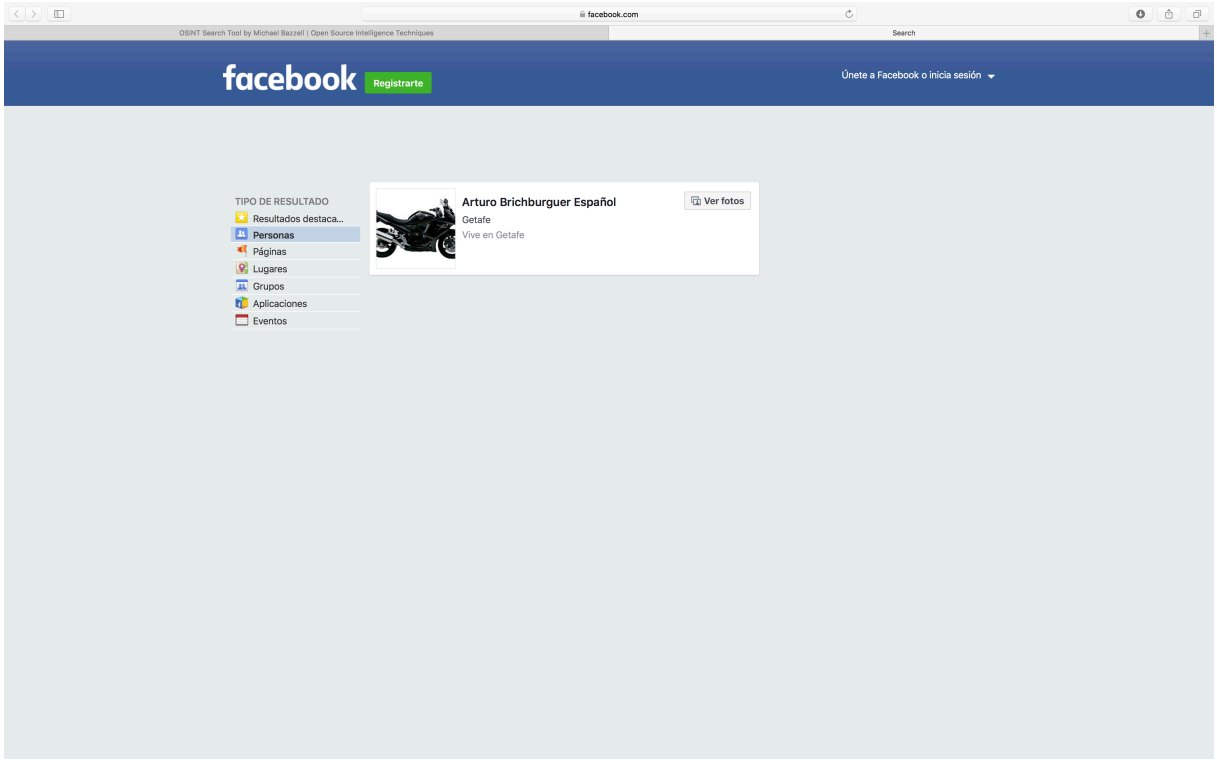

Ilustración 6. Resultado que ofrece Facebook de la consulta del correo del investigado

Ilustración 7. Información pública del investigado

Una vez consultado el citado perfil, que tiene actividad reciente, se observa que no aparece en las publicaciones la típica etiqueta de “publicado desde mi Android” o similar, por lo que se puede interpretar que, o bien no utiliza la aplicación que existe para el teléfono que posee y publica mediante el acceso web de la página de Facebook, o bien las publicaciones las realiza desde otro dispositivo.

c) Elección del software para registro remoto a instalar

Con la información que se ha obtenido en los pasos anteriores, se puede inferir un posible vector de ataque para la instalación del software de registro remoto del teléfono: ofrecerle una aplicación de Facebook modificada, haciéndole ver las ventajas de instalarla en su dispositivo.

Claro está, que dicha aplicación contendrá un (payload, 2017) que permitirá a los investigadores realizar de forma efectiva el registro remoto de su teléfono móvil.

Otra posible elección, sería buscar un (exploit, 2017) que afectara al software y al dispositivo que posee. Los datos que se conocen es que es un teléfono móvil Samsung Galaxy S4 con sistema operativo Android.

Se realiza una búsqueda de información en Internet acerca de dicho dispositivo. Al conocer la marca y modelo del teléfono, se realiza una consulta en la página web de (sammobile, 2017),

la cual ofrece información sobre las últimas actualizaciones de software oficiales del dispositivo.

Como resultado, ofrece la información de que la última versión de Android oficial que se ha distribuido al Samsung Galaxy S4 fue la 5.0.1, tal y como se puede observar en la "Ilustración 8".

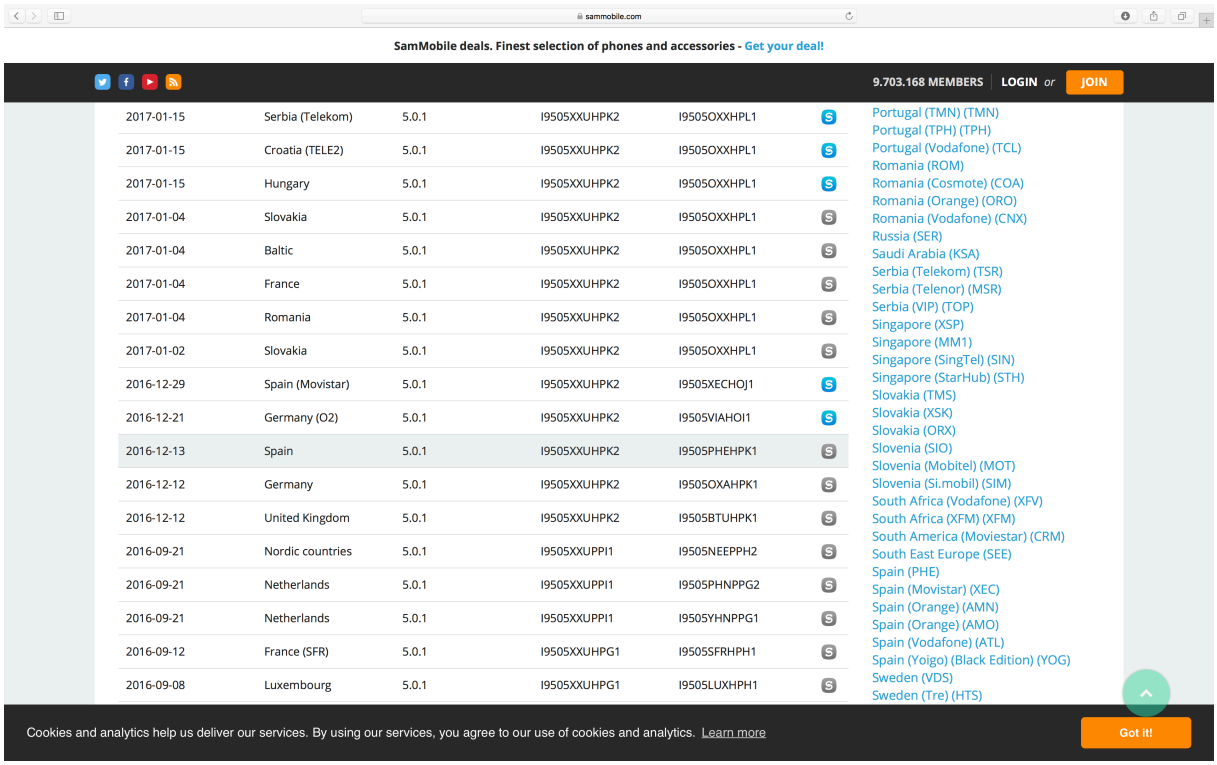

Ilustración 8. Última versión de Android oficial del dispositivo

Con esa información disponible, y teniendo como herramienta (Metasploit, 2017), se puede concluir que, con la versión 5.0.1 de Android instalada en el dispositivo, es probable que ninguno de los (exploit, 2017) disponibles en dicho Framework llegue a funcionar correctamente.

Es cierto que la versión del sistema operativo instalada en el dispositivo del investigado puede ser una anterior, en la que llegue a funcionar alguno de los (exploit, 2017) disponibles. Pero, ante la imposibilidad de realizar más comprobaciones previas, y teniendo en cuenta que el (payload, 2017) inyectado en un a aplicación de Android va a funcionar casi con total seguridad (siempre y cuando el objetivo la instale en el dispositivo, claro), se opta por elegir esta última opción.

d) Solicitud al Juez de Instrucción

Acerca de la solicitud de autorización al Juez de Instrucción competente, en el Anexo I figura el escrito de petición que se realizaría.

En el mismo, como ya se ha reiterado en el presente Trabajo de Fin de Máster, se hace referencia al hecho delictivo que se está investigando. Igualmente, se describen todas las gestiones realizadas, previas a la solicitud de la autorización del registro remoto, de modo que el Juez pueda entender que, sin la aplicación de la medida solicitada, no se pueda continuar con las averiguaciones en la investigación.

Además, se facilita la identidad completa de la persona que está siendo investigada. Dichos datos, en este caso concreto, han sido conocidos por medio de la investigación policial tradicional, lo que, por otra parte, será lo más común en el resto de investigaciones.

En el escrito figura la medida para la que se solicita autorización (registro remoto), indicando además que se quiere realizar una copia de los datos contenidos en el dispositivo, una vez se lleve a efecto el registro remoto. También se explica cómo se va a llevar a cabo el control de la integridad de los datos copiados en un dispositivo extraíble, en poder de los investigadores. Dicho soporte, o copia del mismo, será remitido al Juez Instructor posteriormente.

Con la explicación de los hechos delictivos, y las gestiones llevadas a cabo, así como la información adquirida en el conjunto de la investigación, se hace hincapié en que la medida resultaría proporcionada al delito investigado, debido a la alta pena de prisión que puede acarrear. Del mismo modo, se informa de que, sin la aplicación de la medida, sería prácticamente imposible continuar de un modo satisfactorio con la investigación, siendo la medida solicitada necesaria. Además, la medida es idónea en relación con los hechos investigados y la forma en que se están cometiendo por el investigado.

Ya al comienzo del documento, se informa del Grupo de Policía Judicial que se hace cargo de la investigación, así como de los números de carné profesional de los investigadores que llevarían a cabo la medida, caso de concederse.

Englobado en los datos que se facilitan al Juez, se explica el tipo de software que va a utilizarse para el registro remoto, aunque no se indique explícitamente qué aplicación concreta se va a utilizar. De todos modos, es el Juez de Instrucción el que decide el software que se va a utilizar para realizar la medida, pero se le informa de las opciones que tienen disponibles los investigadores.

Ese tipo de software seleccionado, va en relación con el dispositivo a registrar, siendo los datos que se facilitan al Juez que se trata de un teléfono móvil Samsung Galaxy S4, con sistema operativo Android, con número de teléfono 66-666-666 y que hace uso del correo electrónico jreacherprueba@gmail.com.

También se le indica al Juez de Instrucción la forma en la que se va a proceder a la instalación del software anterior. Se le informa de que dicha instalación se va a realizar a distancia, mediante el uso de Ingeniería Social.

En relación con el párrafo anterior, también se solicita la colaboración de una empresa, sujeto obligado a colaborar, para realizar el envío del correo (o mensaje) que incluirá el enlace con el software utilizado para el registro remoto, que el investigado deberá instalar (en el ejemplo práctico no se va a poder hacer uso de esa colaboración, por tratarse de una simulación y no de un caso real).

Finalmente, se le informa al Juez del período temporal para el que se solicita la medida, siendo en este caso de 1 mes. Este tiempo se usará para instalar el software en el dispositivo a registrar y realizar de forma efectiva el registro.

Puede parecer una cantidad exagerada de tiempo, pero en muchas ocasiones los investigadores encontrarán grandes dificultades en instalar el software necesario, y el tiempo de la autorización comienza desde que se concede, no desde que el software ya está instalado. Y, además, no se pueden realizar pruebas de instalación reales hasta que la autorización haya sido concedida. Por lo que el mes solicitado será un tiempo ajustado a la realidad.

Una vez solicitada, y concedida por el Juez, la autorización, se procedería a la instalación del software elegido en el dispositivo a registrar.

e) Instalación del malware (mediante Ingeniería Social)

Como ya se ha expuesto durante el desarrollo de la metodología, este es el punto clave de la misma, puesto que, si no se consigue que el investigado instale el software, no se podrá llevar a cabo el registro remoto del dispositivo.

Para llevarlo a efecto, se va a remitir un correo electrónico al investigado, que contiene un enlace de descarga al software que se desea instalar. La opción ideal, que se muestra en la metodología, sería contar con la colaboración de algún sujeto obligado (en el escrito de solicitud de autorización se solicita la colaboración de Movistar, por ejemplo). De este modo,

tanto el correo recibido por el investigado, como el servidor en el que se aloje el archivo, serán de una entidad conocida por el investigado (ya que, se supone, es su operador de telefonía).

Otra opción, también “ideal”, es contar con un dominio propio, y tener cuentas de correo electrónico asociadas a dicho dominio, para poder realizar los envíos al investigado, pero conlleva un coste económico.

En la presente simulación, no es posible optar por ninguna de las 2 opciones anteriores (que aparecen en la metodología propuesta), así que se opta por crear una cuenta de correo electrónico, en un proveedor gratuito, a través de la red (TOR, 2017), lo que nos dará cierto anonimato.

Se ha elegido una cuenta de Gmail, puesto que, al ser el mismo proveedor que el del correo del investigado, es mucho menos probable que el correo enviado acabe en la carpeta de spam y que, de esta manera, el investigado abra el correo e instale el software.

También hay que tener en cuenta las costumbres de conexión a Internet de la persona investigada. En este caso concreto, se tiene conocimiento de que el investigado utiliza una red inalámbrica pública a diario (de lunes a viernes), a la cual se conecta su dispositivo automáticamente.

Los investigadores se conectan a dicha red inalámbrica, con el objetivo de conocer el rango de IP que asigna que, en este caso, es 192.168.1.xxx.

De este modo, todo el proceso se realizaría haciendo uso de dicha red, lo que permite montar un servidor web propio, en local, que albergue el software de registro remoto.

No es necesaria la creación de un (Rogue AP, 2017), puesto que el espacio temporal es suficiente para que el investigado realice la instalación del software mientras permanece conectado a esa red.

Si se observara que el investigado abandona el lugar, y no ha realizado la instalación, sí que podría tomarse como opción el crear un (Rogue AP, 2017) que suplante el del Centro Cívico y seguir al objetivo para que el teléfono móvil permanezca conectado a dicho (Rogue AP, 2017).

Por lo tanto, el primer paso será crear una cuenta de Gmail, desde la que enviaremos el correo electrónico al investigado.

Con el fin de anonimizar los datos de conexión, la cuenta se creará haciendo uso de (TOR Browser, 2017) desde la máquina virtual de (Kali Linux, 2017) 64 bits instalada en el ordenador utilizado.

En la “Ilustración 9” se observan los datos introducidos para la creación de la cuenta de correo.

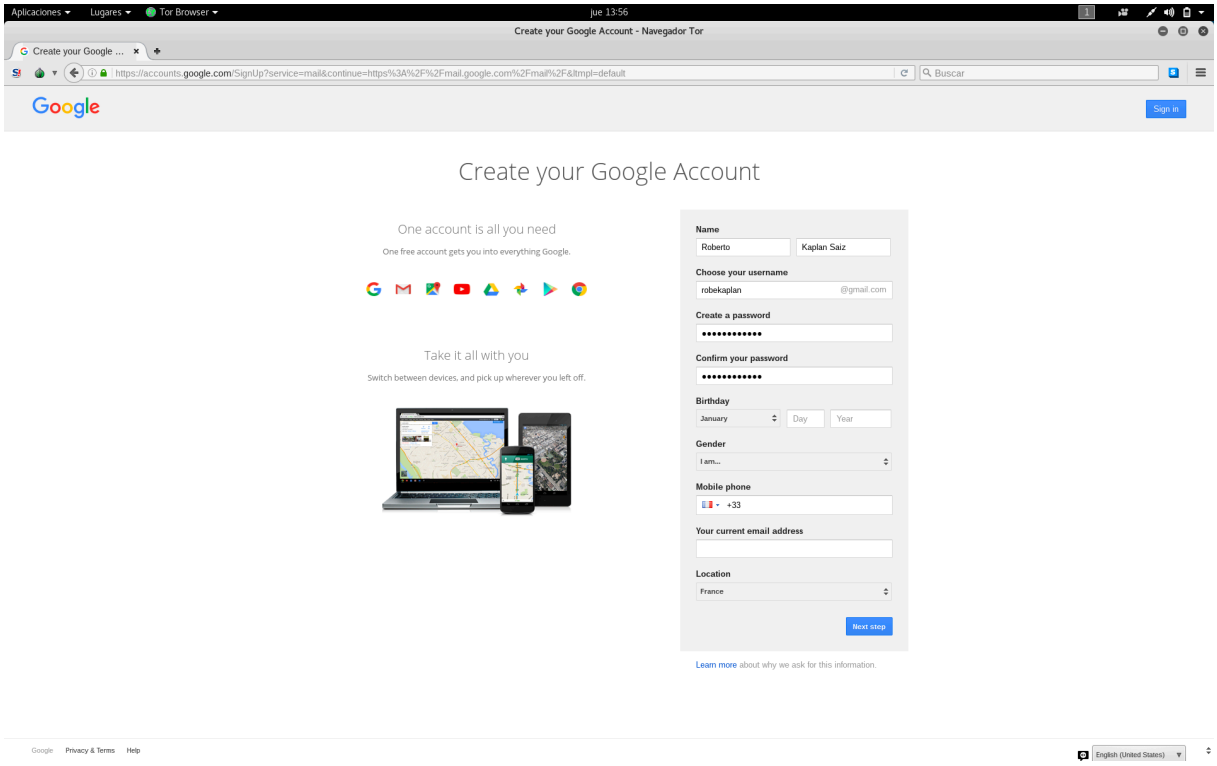

Ilustración 9. Datos de creación de la cuenta de Gmail

El correo electrónico que se ha creado es robekaplan@gmail.com, y como nombre del usuario propietario de la cuenta se ha introducido “Roberto Kaplan Saiz”. Debe ser un nombre que no incite demasiada desconfianza en la persona investigada, y que pueda interpretarse como acorde con el contenido del correo enviado y el motivo del envío.

La idea es enviar un correo en el que se le ofrezca al investigado una aplicación móvil para acceder a Facebook, puesto que, por las investigaciones practicadas, se estima que el investigado no la utiliza.

Pero no se le va a ofrecer la aplicación estándar, sino que se le va a ofrecer la aplicación de Facebook-Lite, la cual utiliza menos recursos del teléfono móvil (cabe recordar que el teléfono que utiliza tiene ya cierta antigüedad).

Se le va a ofrecer como una novedad para ciertos usuarios seleccionados, de los cuales se ha detectado que no utilizan la aplicación del teléfono móvil, sino que acceder a Facebook desde el navegador.

De este modo, y personalizando el mensaje para el usuario de Facebook que posee, se tratará de que el investigado confíe e instale la aplicación deseada.

Además, se le va a explicar por qué se le ofrece la aplicación de esta forma (que no es, en absoluto, la habitual) y qué pasos son necesarios para poder instalarla en su dispositivo.

Una vez configurada la cuenta desde la que se va a enviar el correo, queda por crear el propio correo.

Primero se debe elegir qué aplicación es la que se va a utilizar para inyectar el (payload, 2017) necesario para la realización del registro remoto. Como se ha expuesto anteriormente, la elegida en este caso sería “Facebook-Lite” para Android. Realizando una búsqueda en Internet, se observa que existe la opción de descargar directamente el fichero “.apk” de la página oficial (si esto no fuera posible, mediante el uso de diversas páginas web, como (apk-downloader, 2017), se puede realizar la descarga del fichero “.apk” indicando la identificación de la misma en (Google Play, 2017)), tal y como se observa en la “Ilustración 10” y en la “Ilustración 11”.

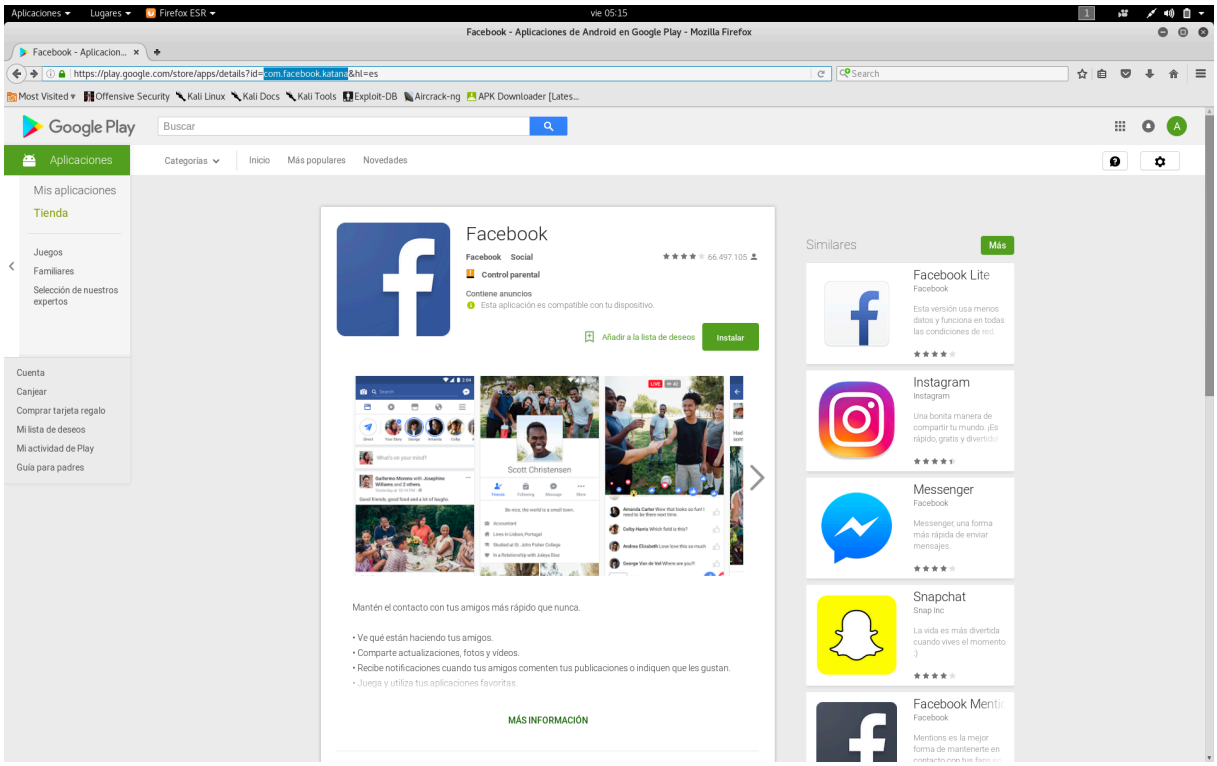

Ilustración 10. Localización de la identificación de la aplicación en Google Play

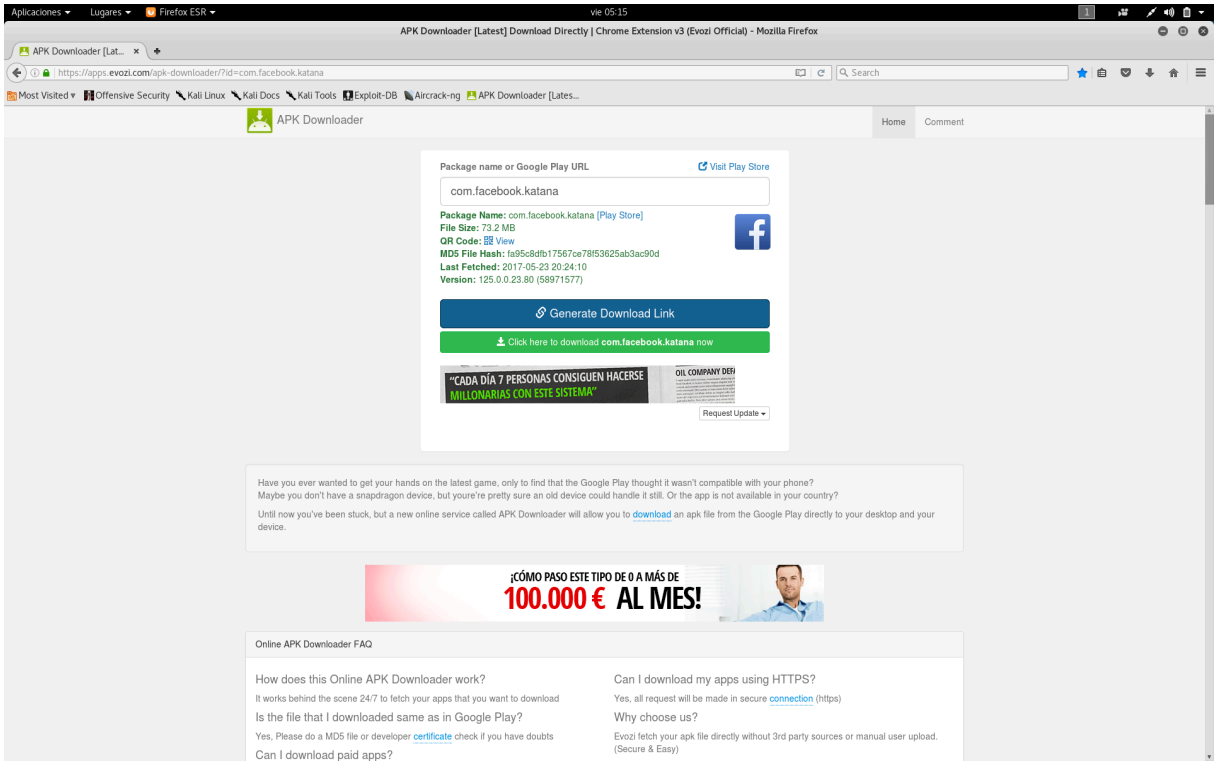

Ilustración 11. Generación del link de descarga del ".apk" de la aplicación

Como se ha dicho, en el caso de Facebook-Lite la propia página web permite la descarga del ".apk" de la aplicación, sin necesidad de recurrir al método anterior, como se observa en la "Ilustración 12". Por lo tanto, pulsando en el botón de "Descargar", se descargará el fichero ".apk" de la aplicación de Facebook Lite.

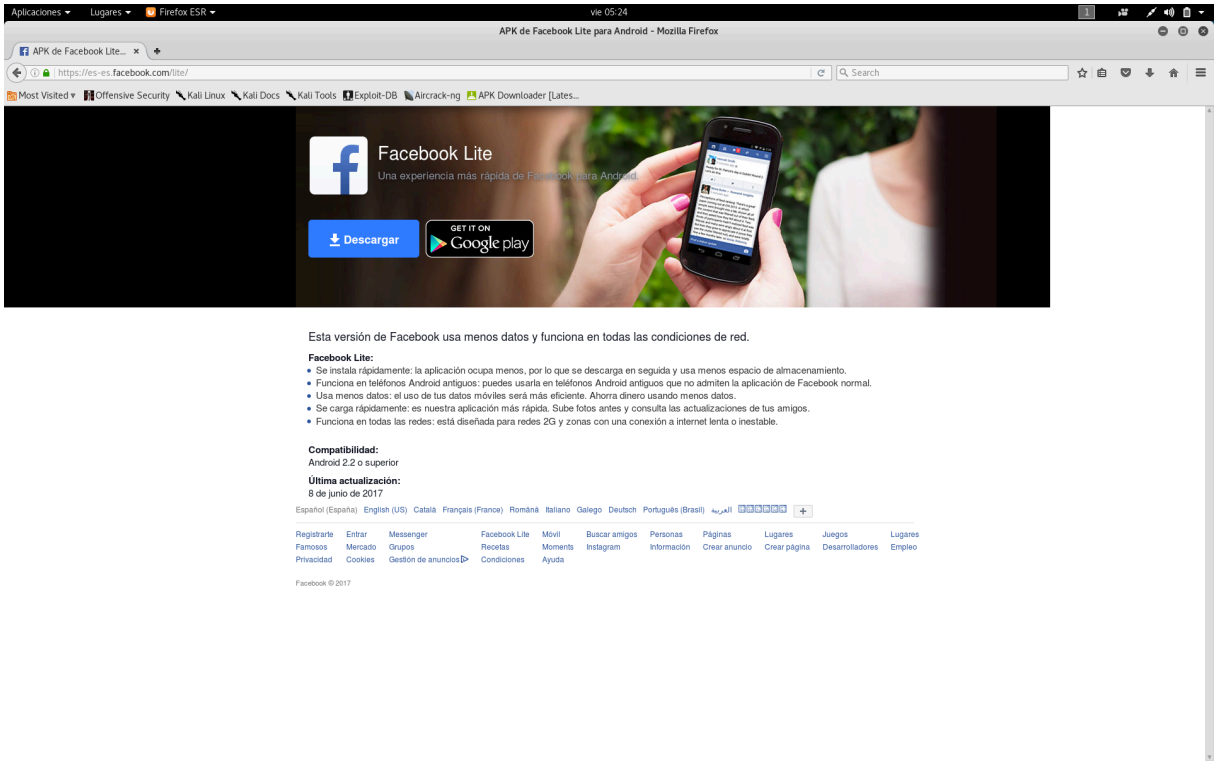

Ilustración 12. Página de descarga del ".apk" de Facebook Lite

Como se observa, aparece un botón para descargar el “.apk” directamente y otro que permite la descarga desde (Google Play, 2017). Como el aspecto de la página resulta convincente, mediante la herramienta “hhtrack” se procederá al clonado de esta página web, para ser remitida a la persona investigada.

Una vez clonada, se harán las modificaciones pertinentes en la misma, como: variar la dirección donde se encuentra alojado el “.apk” para que apunte al servidor propio en el que se colocará la aplicación modificada, eliminar el botón de descarga de (Google Play, 2017), e introducir algún texto más que explique el proceso de instalación y los permisos que se le van a requerir durante la instalación. Todo ello en aras de dar un aire de oficialidad al correo e infundir confianza.

Se comienza con el primer paso, que es la clonación de la página web mediante el uso de (httrack, 2017). En la “Ilustración 13” se observa el comando introducido para realizar la clonación, y en la “Ilustración 14” se muestra el resultado de dicha clonación.

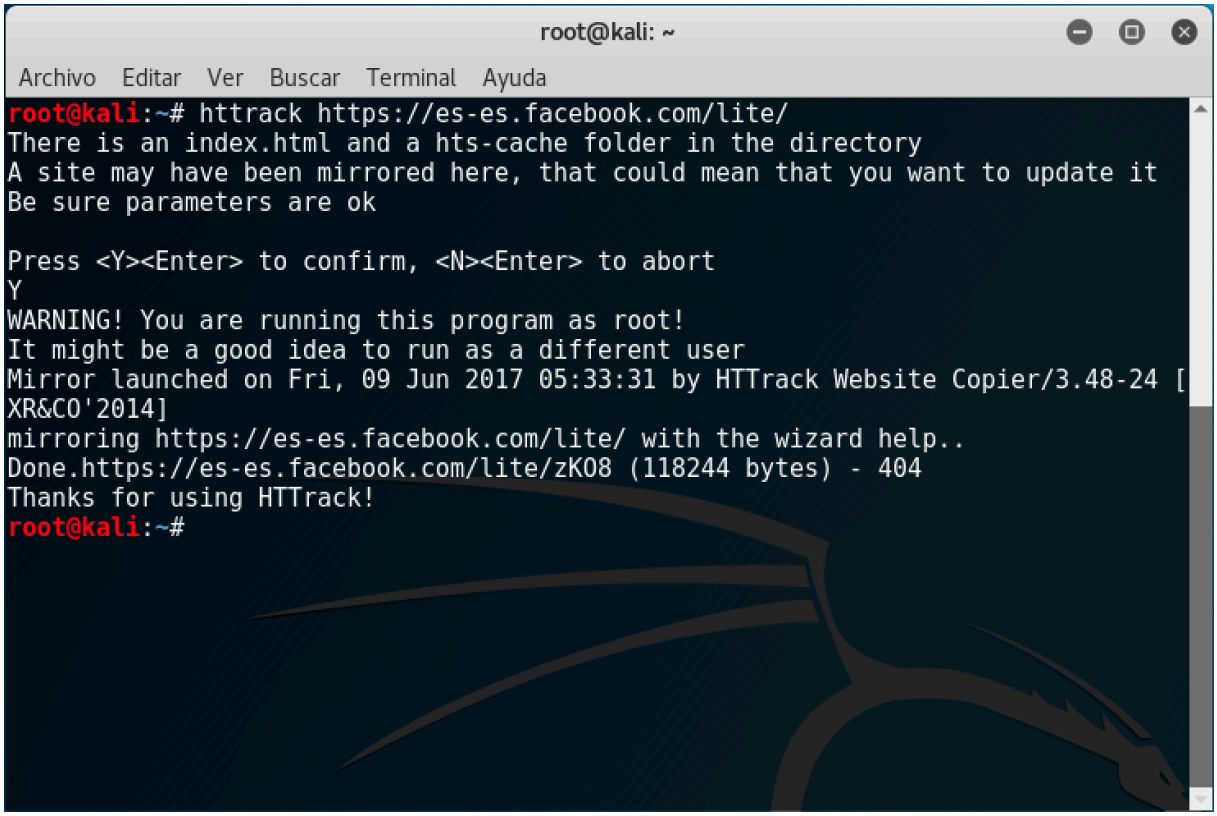

Ilustración 13. Comando para realizar la clonación de la página web

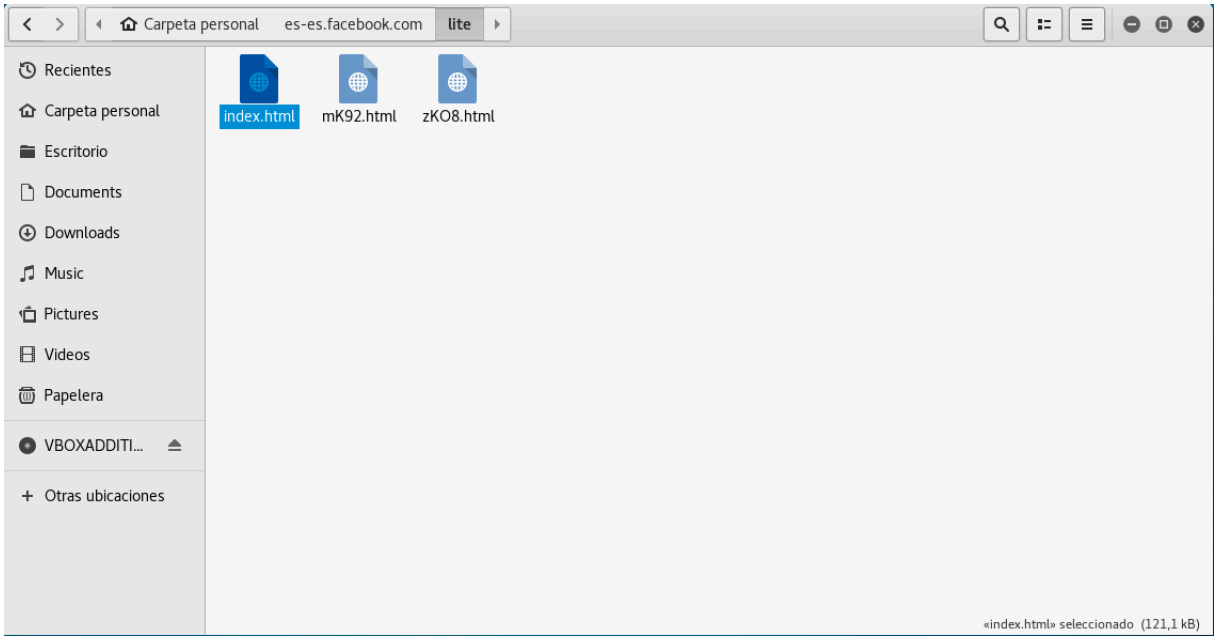

Ilustración 14. Resultado del proceso de clonación.

El fichero que se observa en la “Ilustración 14”, con el nombre de “index.html”, es el que contiene el código de la página web clonada. Por lo tanto, ése será el fichero a modificar a conveniencia de los investigadores.

Para poder modificar dicho fichero convenientemente, primero se deben realizar otras acciones, en aras de preparar, tanto el software a instalar en el dispositivo del investigado (modificar la aplicación de Facebook Lite descargada), como el lugar dónde estará alojado dicho software.

Primero, se va a llevar a cabo la modificación de la aplicación original descargada. Para ello, se hará uso de la herramienta (spade, 2016). Para generar el (payload, 2017) a inyectar, hace uso de (msfvenom, 2016), por lo que pide la selección del (payload, 2017) a utilizar, así como la IP y puerto de escucha. Estos datos se pueden observar en la “Ilustración 15”.

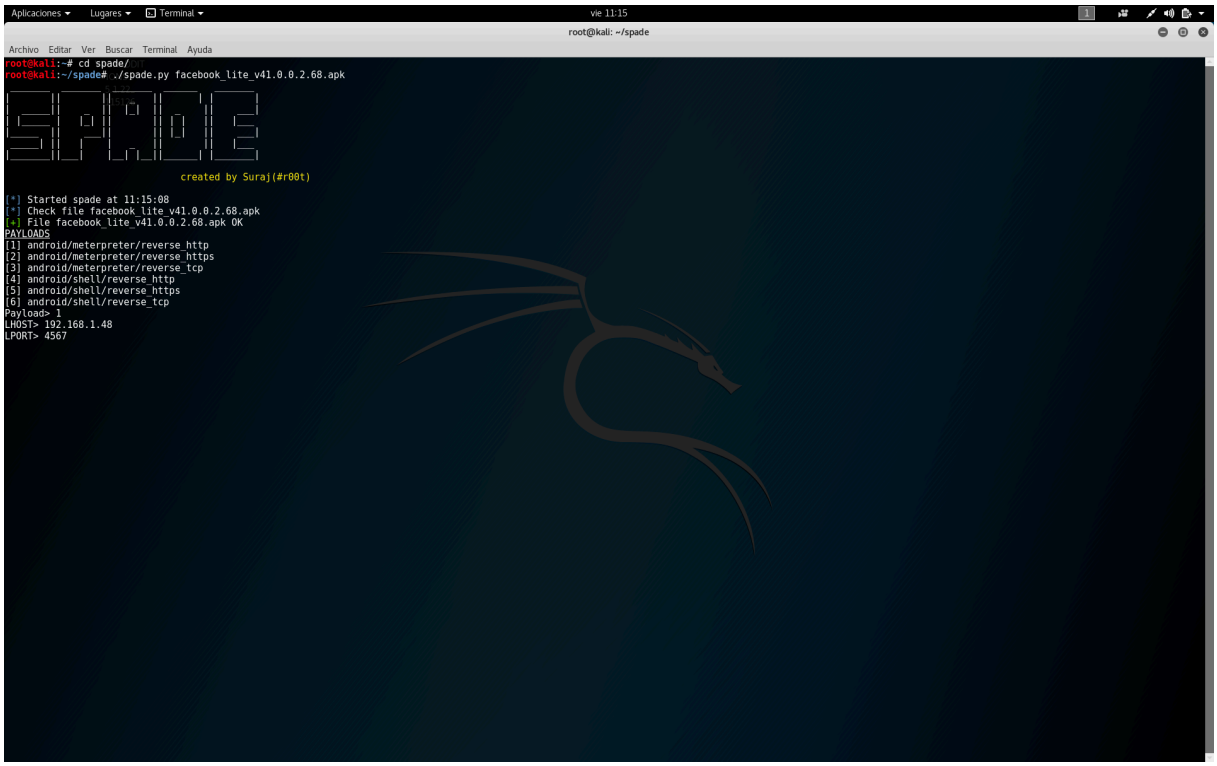

Ilustración 15. Proceso de generación de la inyección del "payload" en la aplicación de Facebook Lite mediante "Spade"

Como se observa en la “Ilustración 15”, el (payload, 2017) generado se va a conectar a la IP privada de los investigadores mediante “http”, a través del puerto “4567”. La IP es una IP privada, ya que todo el proceso se va a realizar desde la red inalámbrica pública a la que se conecta el investigado. Si el proceso se realizara a través de Internet, el argumento “LHOST” debería ser la IP publica de los investigadores (hay que recordar que es imprescindible que dicha IP no varíe a lo largo del tiempo, por lo que debe ser una IP fija).

Una vez finalizada la ejecución de la herramienta, informa de que se ha conseguido inyectar el (payload, 2017) satisfactoriamente, el nombre de la aplicación modificada que se ha creado (facebook_lite_v41.0.0.2.68-final.apk) y pregunta si se quiere configurar la herramienta de escucha. Se introduce que no, puesto que dicha herramienta será la que se utilice para realizar

el registro remoto, una vez que la aplicación esté instalada en el dispositivo a registrar, por lo que, por el momento, no es necesaria su ejecución. Esta información se puede observar en la “Ilustración 16”.

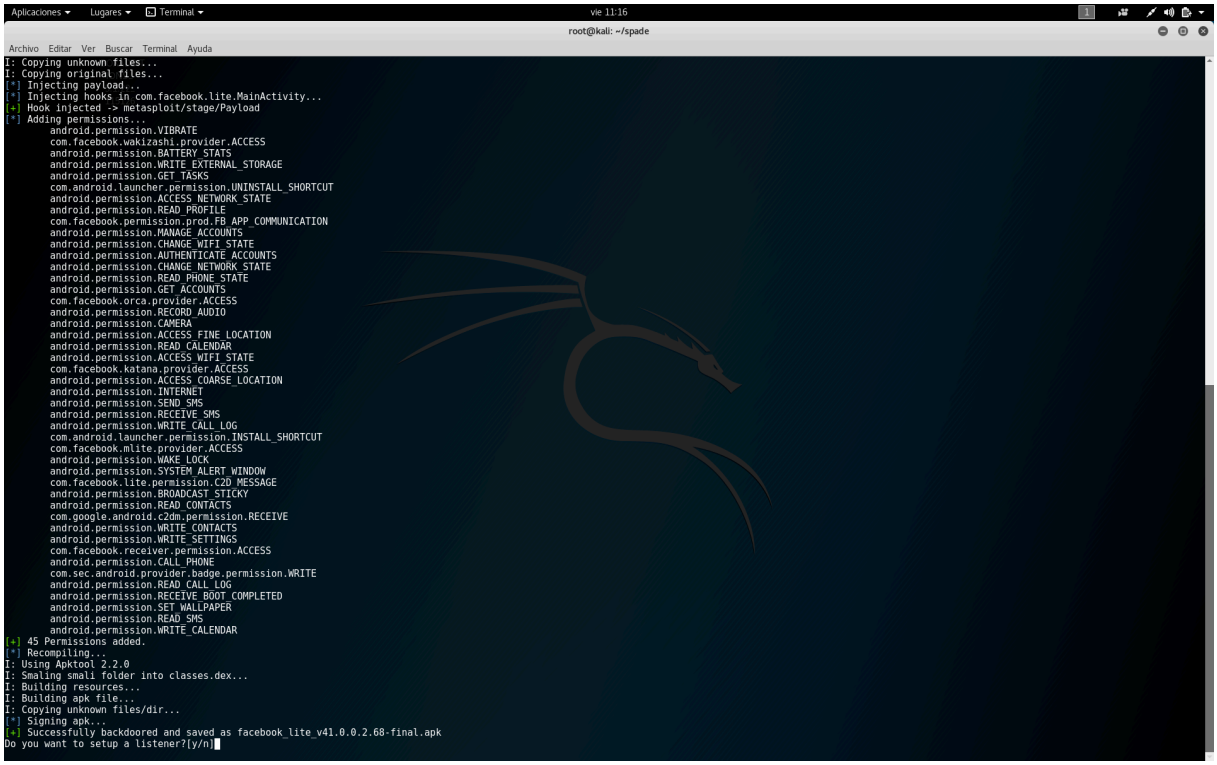

Ilustración 16. Finalización del proceso de inyección del "payload" en la aplicación Facebook Lite mediante "Spade"

Una vez finalizada la ejecución, se renombra la aplicación generada como “facebook_lite.apk”.

El siguiente paso es colocar dicha aplicación en el propio servidor web de los investigadores. Lugar desde el que será descargada por el investigado.

Para ello, se hace uso del propio servidor web “Apache” que viene instalado en (Kali Linux, 2017). La dirección en la que se va a colocar el fichero es “192.168.1.48/Aplicaciones/Facebook_lite.apk”. Esta será la dirección a la que apunte el botón de “Descargar” del html modificado.

Una vez está la aplicación en el servidor, se prepara el correo electrónico a enviar. Para ello, se modifica el “html” de la página clonada convenientemente: se modifica la dirección del lugar en el que se encuentra la aplicación a descargar y se añaden varias líneas de texto para explicar la instalación de la misma. Con respecto a la dirección donde se encuentra la aplicación, se ha optado por acortar la URL mediante el uso de (tinyurl, 2002), para que no aparezca la dirección IP del servidor de los investigadores, y eso dirección es la que figura en la página modificada, que es http://tinyurl.com/y7enj2yt. El resto de modificaciones realizadas,

junto con la de la URL, se pueden observar en el texto resaltado del fichero html modificado de la “Ilustración 17”.

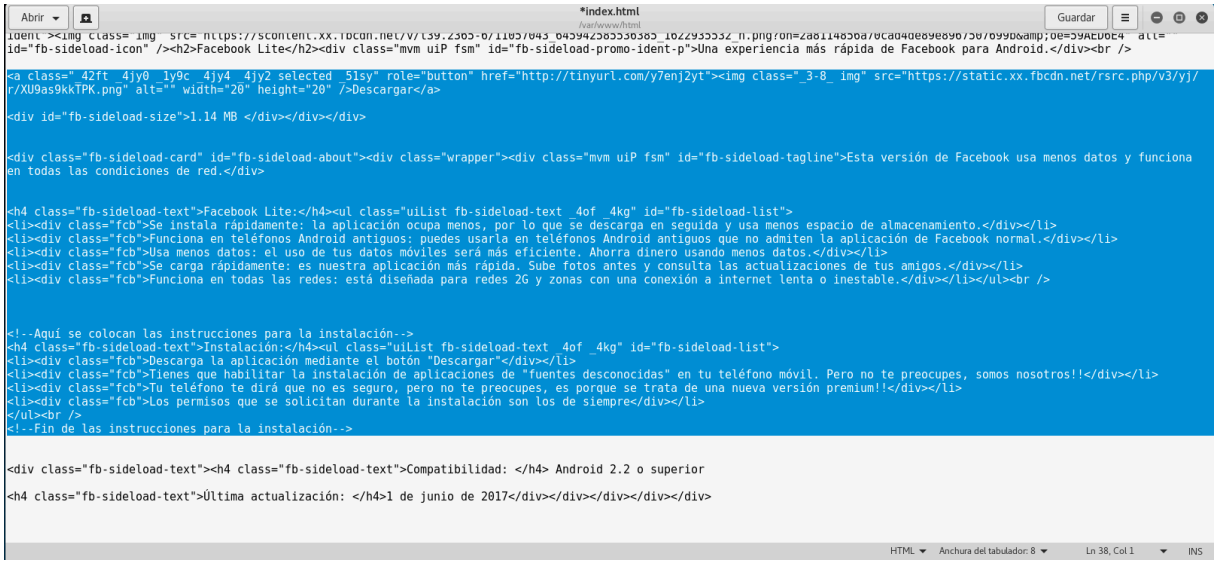

Ilustración 17. Modificación del fichero html clonado

A continuación, en la “Ilustración 18”, se muestra el resultado de las modificaciones (abajo a la izquierda en la “Ilustración 18”, se observa la URL que aparece para el botón de Descargar).

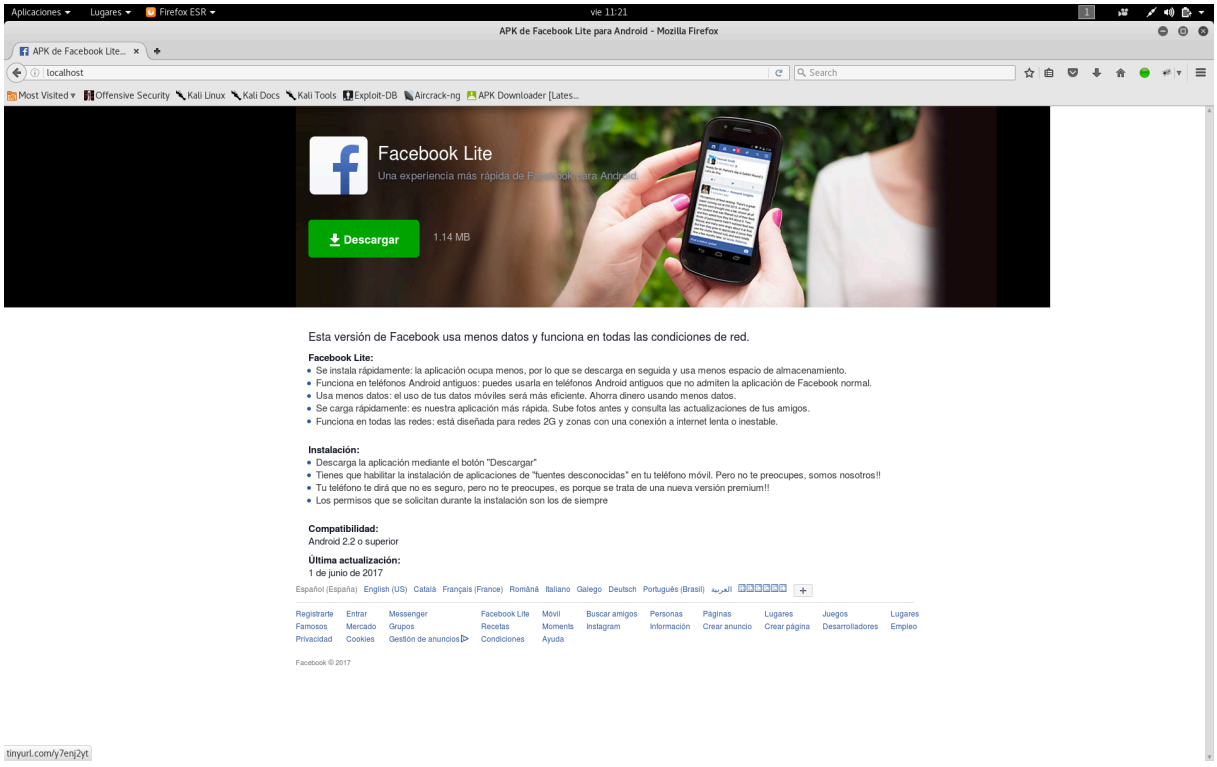

Ilustración 18. Resultado de la modificación de la página web clonada

Una vez se ha modificado la página convenientemente, y se ha colocado la aplicación modificada lista para ser descargada, el siguiente paso es realizar el envío del correo electrónico al investigado.

Para ello, utilizaremos la cuenta creada en Gmail con anterioridad. En la “Ilustración 19” se muestra el mensaje que va a ser enviado. Como se puede observar, el mismo da apariencia de veracidad y se le explica al investigado la forma de realizar la instalación de la aplicación y por qué se hace por este medio (que no es el habitual).

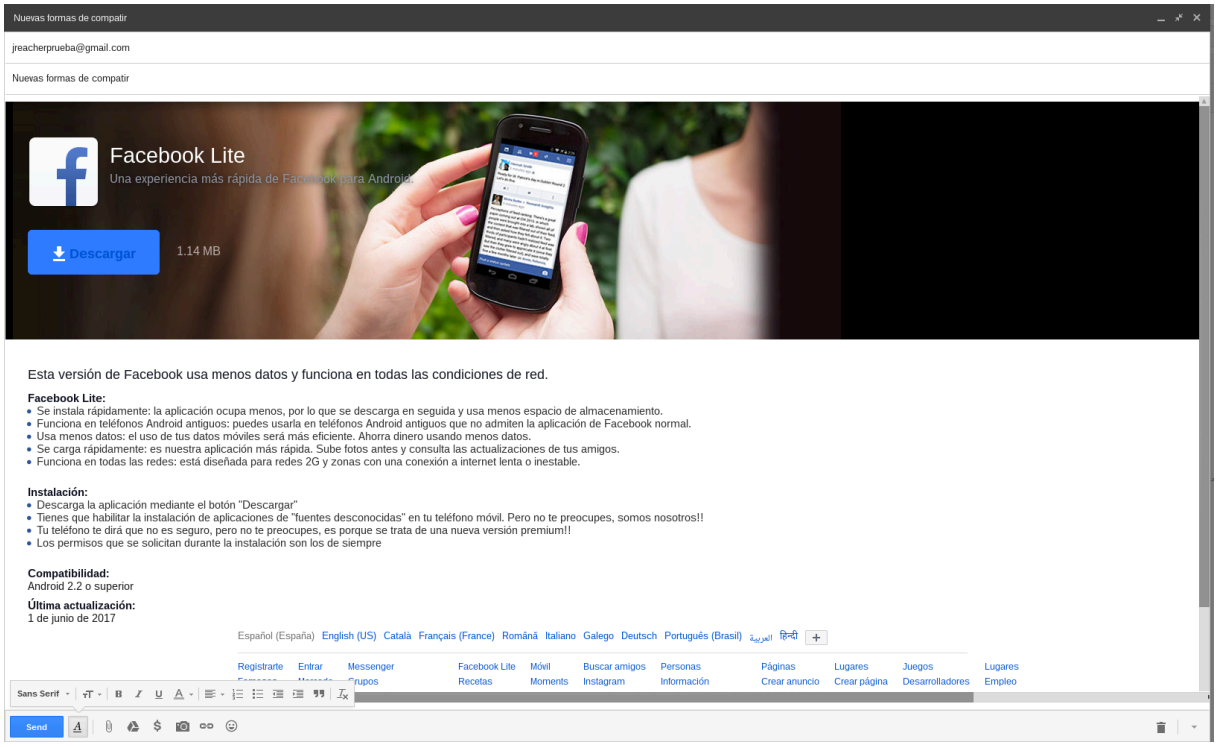

Ilustración 19. Aspecto del correo electrónico que se le va a enviar al investigado

Una vez enviado el correo electrónico, sólo resta esperar a que el investigado realice la instalación de la aplicación, mientras los investigadores quedarán a la espera con la herramienta de escucha en estado operativo.

En el Anexo II se pueden observar las capturas de pantalla del teléfono móvil durante la recepción del mensaje, descarga e instalación (Ilustraciones de la 30 a la 37).

f) Explotación del dispositivo (ejecución efectiva del registro remoto)

Una vez que se ha realizado el envío, hay que permanecer con la herramienta de escucha en espera.

Para ello, se inicia el Framework de (Metasploit, 2017), utilizando el comando (msfconsole, 2017), y se configura la herramienta de escucha, tal y como se muestra en la “Ilustración 20”.

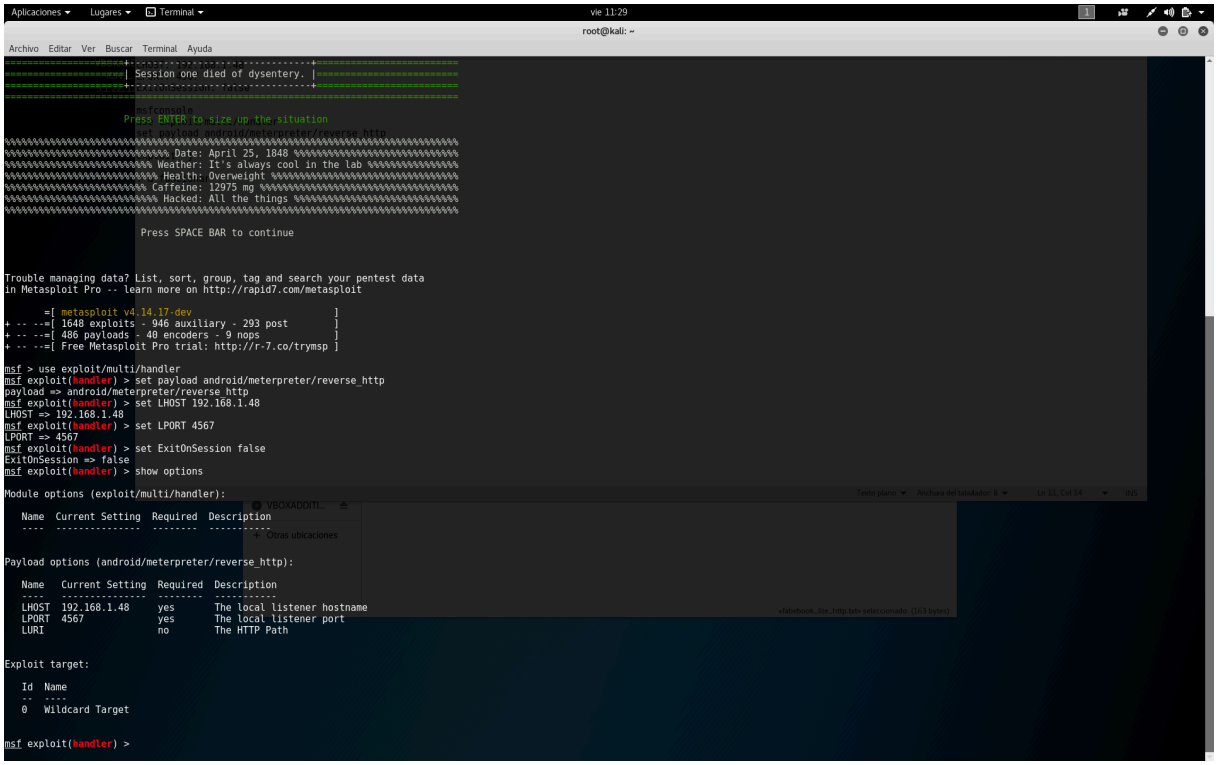

Ilustración 20. Configuración de la herramienta de escucha de Metasploit

Una vez configurada la herramienta, la iniciamos mediante el comando “exploit -j”, quedando ésta a la espera de recibir la conexión del dispositivo con el software instalado.

Una vez que la herramienta comunica que el investigado está en línea, se procede a capturar la sesión iniciada en (meterpreter, 2017) y a realizar el registro remoto del dispositivo, como se puede observar en la “Ilustración 21”.

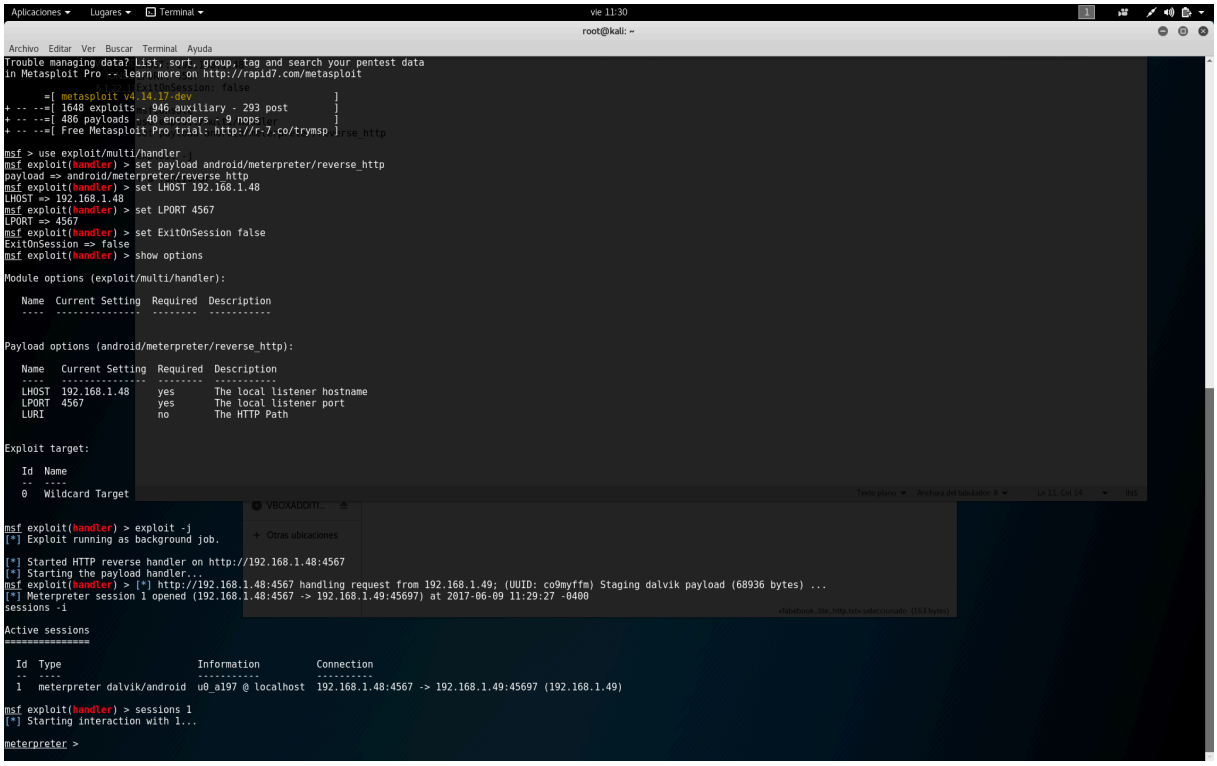

Ilustración 21. Captura de la sesión iniciada por el dispositivo del investigado con "meterpreter"

Mediante el comando “help”, la herramienta lista todas las acciones que se pueden llevar a cabo, como se observa en la “Ilustración 22” e “Ilustración 23”.

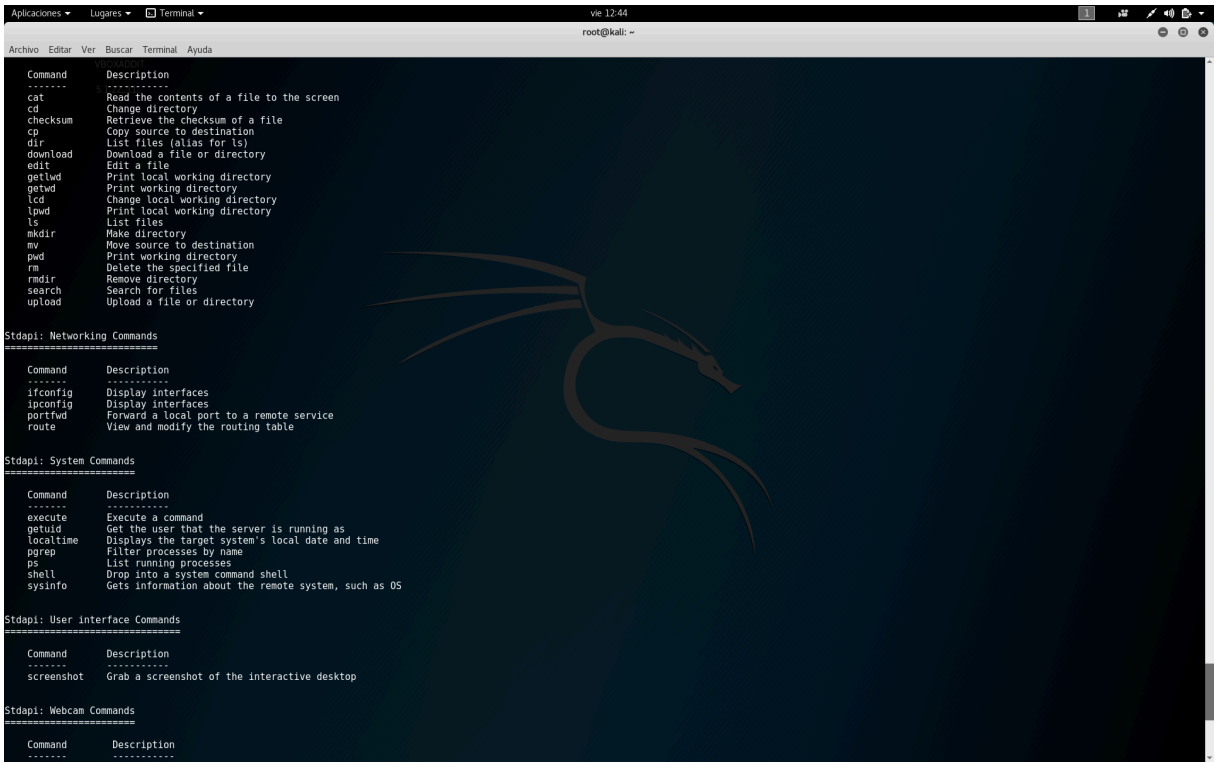

Ilustración 22. Listado de acciones disponibles con "meterpreter" 1 de 2

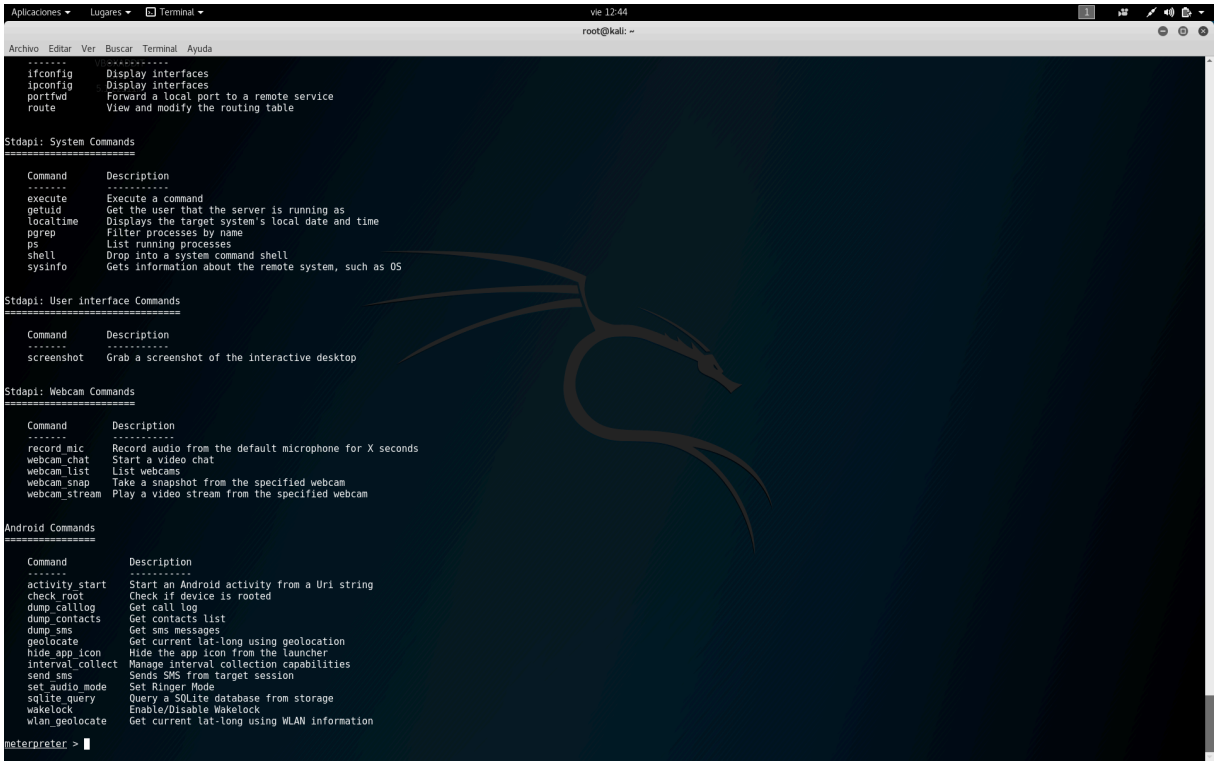

Ilustración 23. Ilustración 20. Listado de acciones disponibles con "meterpreter" 2 de 2

Como en el caso concreto que se está realizando, lo que interesa es conocer si hay imágenes de menores en el móvil del investigado, se realiza una búsqueda por las carpetas del dispositivo, con la finalidad de encontrarlas (nota: en el dispositivo móvil se han introducido imágenes, pero en absoluto de menores. Simplemente son 3 fotografías realizadas a objetos).

Normalmente, las imágenes en Android se almacenan en la carpeta “DCIM”, por lo que se procede a acceder a la misma, y se muestra su contenido, como se observa en la “Ilustración 24”.

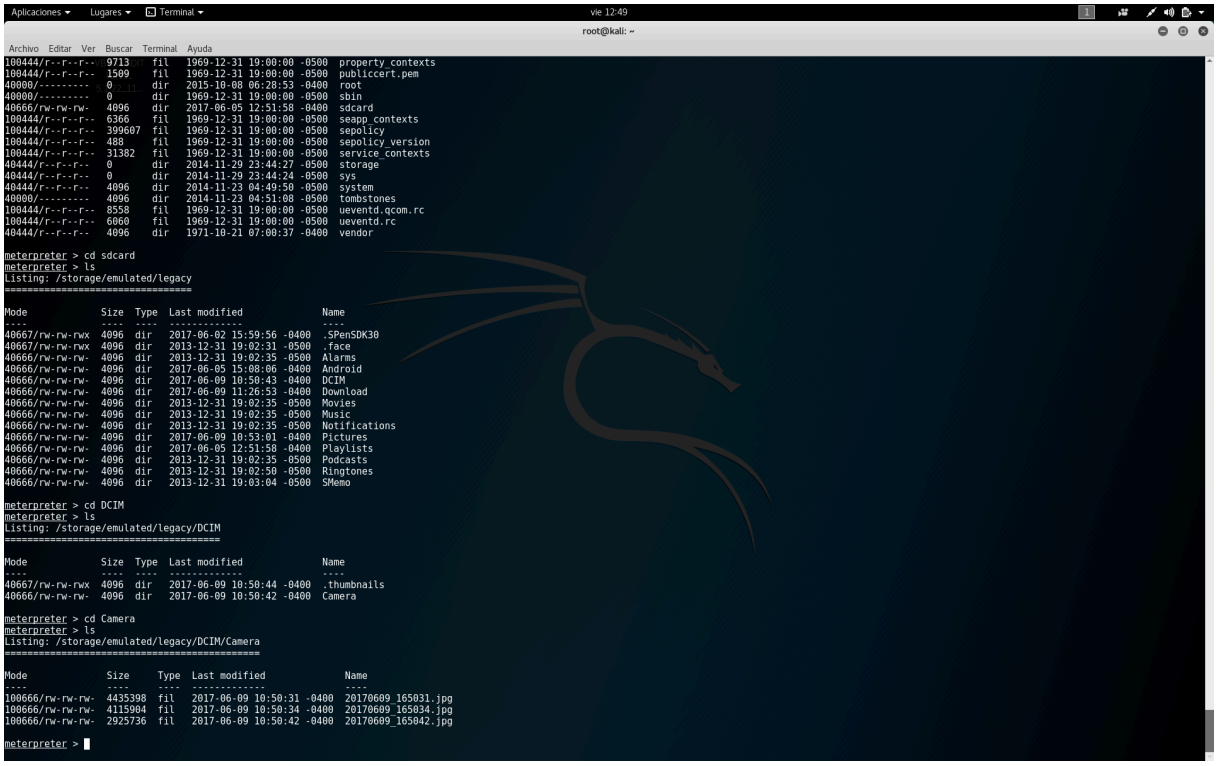

Ilustración 24. Acceso y contenido a la carpeta de almacenamiento de las fotografías

Una vez localizadas las fotografías, se procede a realizar el “hash” de los archivos, mediante el comando “checksum”. Para el ejemplo se va a utilizar la función hash (SHA-1, 2017), como se observa en la “Ilustración 25”.

```
Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100666/rw-rw-rw-  4435398  fil   2017-06-09 10:50:31 -0400  20170609_165031.jpg
100666/rw-rw-rw-  4115904  fil   2017-06-09 10:50:34 -0400  20170609_165034.jpg
100666/rw-rw-rw-  2925736  fil   2017-06-09 10:50:42 -0400  20170609_165042.jpg

meterpreter > checksum sha1 20170609_165031.jpg
44492c289acbfefbd209908dab55761c9846f741  20170609_165031.jpg
meterpreter > checksum sha1 20170609_165034.jpg
c9a400551414d94285ced0472b7ff0b79c3d3b48  20170609_165034.jpg
meterpreter > checksum sha1 20170609_165042.jpg
22b29f6edecf2771cbad609d5cacd7edbb86c34b  20170609_165042.jpg
meterpreter >
```

Ilustración 25. Hash SHA-1 de las fotografías que se van a descargar

A continuación, se procede a la descarga de las imágenes mediante el comando “download”, como se observa en la “Ilustración 26”.

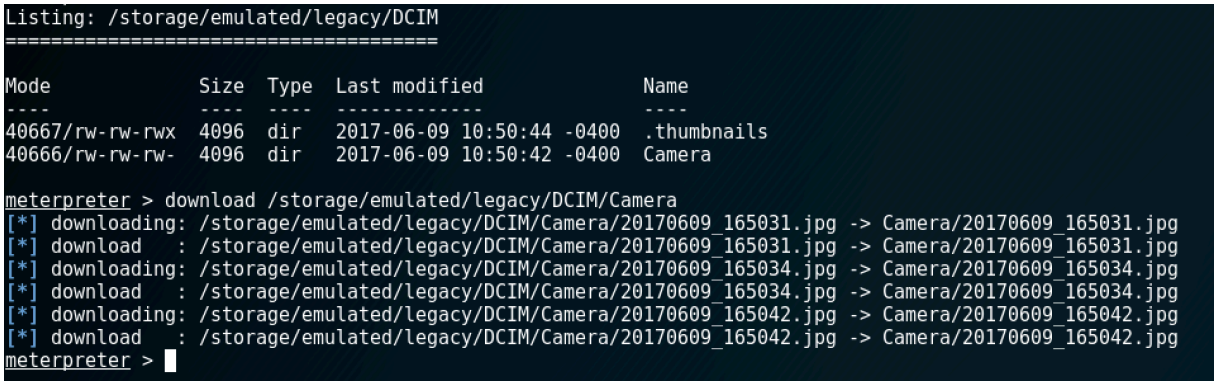

Ilustración 26. Descarga de las fotografías

El siguiente paso es volver a realizar la función hash sobre los archivos originales (Ilustración 27) y, después, sobre los que se han descargado (Ilustración 28). Si los 3 valores calculados para cada fichero coinciden, es que no se han producido modificaciones en los mismos.

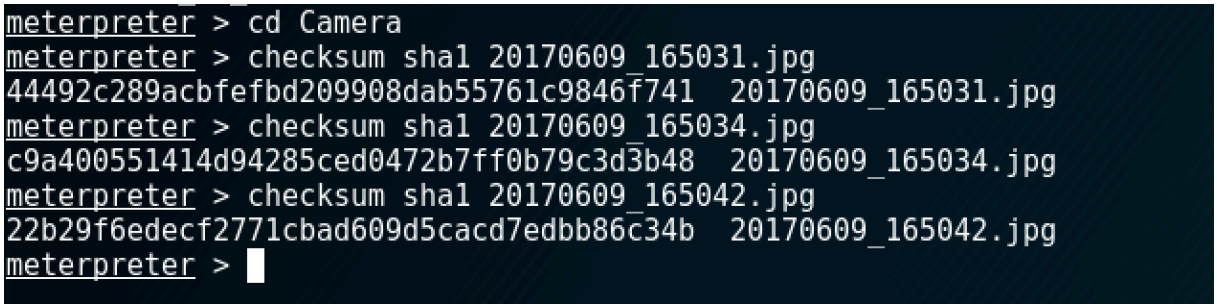

Ilustración 27. Comprobación de los valores hash de los archivos originales en el dispositivo

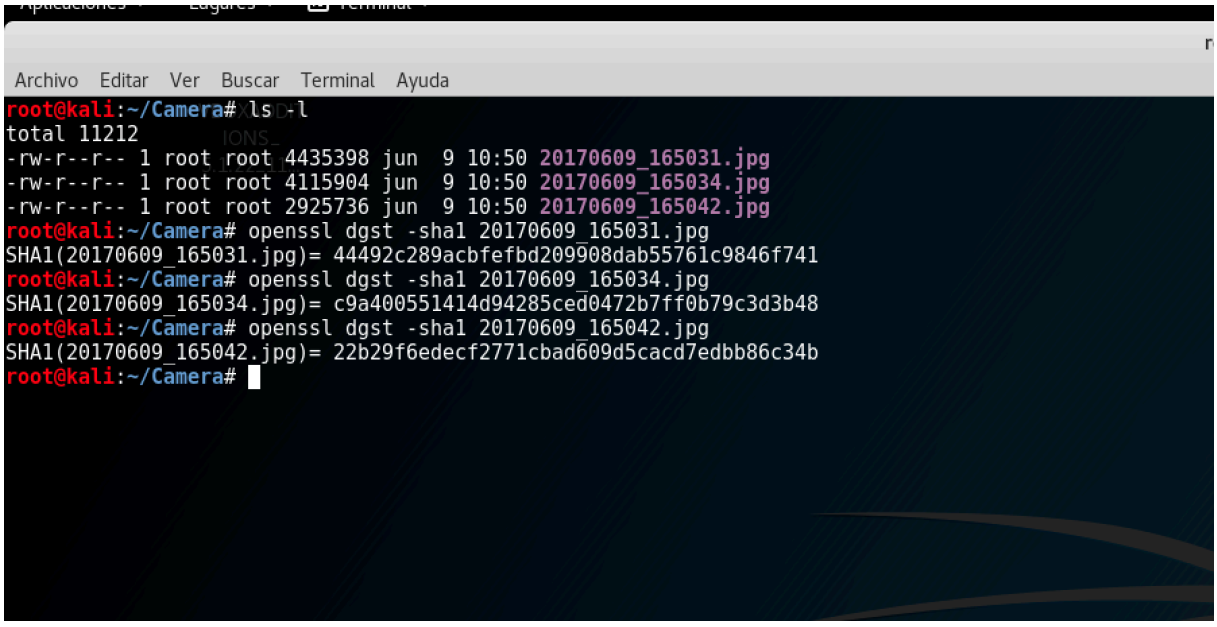

Ilustración 28. Comprobación de los valores hash de los archivos copiados

Estos valores hash calculados, serán la referencia durante todo el proceso penal, para poder comprobar que los archivos no han sido modificados.

A partir de las acciones anteriores, se realizaría un Acta de registro remoto, por parte de los agentes habilitados por el Juez de Instrucción, en la que constaría el proceso realizado durante el registro remoto (añadiendo imágenes), así como el cálculo de los valores hash de los archivos copiados. De este modo, se dejará constancia escrita de todas las acciones llevadas a cabo.

g) Informe periódico al Juez de Instrucción con las novedades de la investigación

Durante el desarrollo de la ejecución de la medida y, según lo indicado por el Juez de Instrucción en el Auto de autorización, éste deberá ser informado de todas las novedades y avances en la investigación, si los hubiera, explicitando toda aquella información nueva y relevante, conseguida gracias a la aplicación de la medida.

En el presente supuesto, se informaría al Juez de Instrucción de las fotografías que se han hallado en el dispositivo, remitiéndole el Acta de registro remoto llevada a cabo, así como un informe del análisis del contenido de dichas fotografías (incluyendo los metadatos de esos archivos, que pueden dar información acerca de la autoría de las fotografías).

h) Solicitud de prórroga (en su caso)

Si el tiempo inicial de la solicitud se agotara sin resultados o, si en base a los datos que se han obtenido durante el registro remoto del dispositivo.

En el presente caso se han hallado diversas fotografías, almacenadas en la carpeta que utiliza la cámara de fotografías del dispositivo, pero eso no indica que hayan sido realizadas con ese dispositivo. Sin embargo, el análisis de los metadatos de esas fotografías sí que puede dar información a los investigadores sobre el lugar en el que se realizaron, así como el dispositivo utilizado, lo que sí que resultaría muy relevante para la investigación.

Para examinar esos metadatos se hará uso de (exiftool, 2003). Como se observa en la “Ilustración 27”, aparece el dispositivo desde el que se realizó la fotografía, un Samsung GT-I9505, que es un Samsung Galaxy S4, es decir, el mismo modelo del teléfono del investigado.

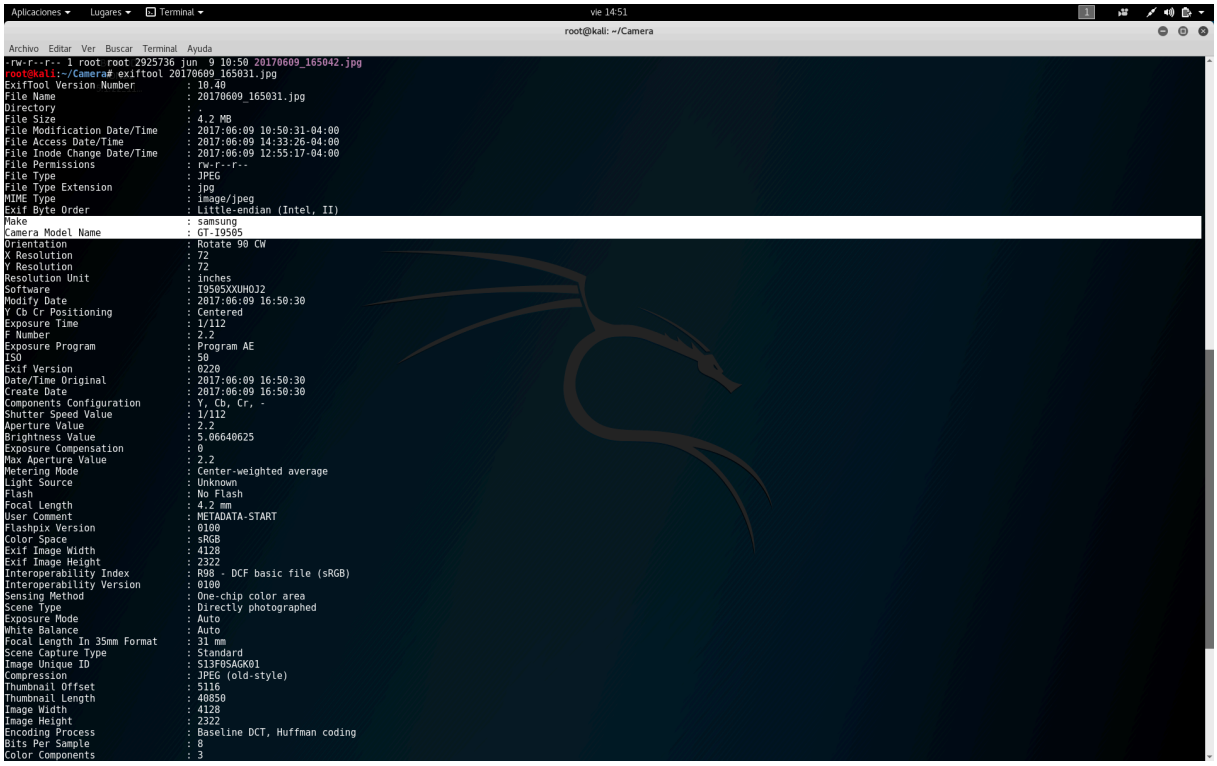

Ilustración 29. Metadatos de una imagen utilizando "exiftool"

En este caso no se tienen datos del lugar donde se realizó la fotografía, supuestamente por no tener conectado dicho servicio el investigado en su teléfono móvil.

Con los datos recogidos durante todo el proceso, en el presente caso no se estima procedente la solicitud de la prórroga de autorización del registro remoto puesto que, con la información que se posee, es suficiente para realizar la detención por los delitos mencionados anteriormente (incluyendo el de elaborar el material pornográfico).

i) Solicitud de cese de la medida

Como ya se han conseguido toda la información necesaria antes de la finalización del plazo inicial de la autorización concedida, el paso final con respecto a ésta es solicitar su cese al Juez de Instrucción.

La solicitud de cese se realizará mediante un escrito (Oficio) en el que se explicará al Juez por qué se solicita el cese de la medida. Es decir, hay que explicar al Juez que ya se ha conseguido toda la información que se estima necesaria para la investigación, y que no es necesario continuar con la práctica del registro remoto.

5. Conclusiones y trabajo futuro

5.1. Conclusiones

El presente Trabajo de Fin de Máster ha tratado de **poner un inicio de solución a un problema para el que se han planteado muy pocas preguntas**.

Se ha tratado de dar una guía, paso a paso, desde el inicio de la investigación, para **dar solución a cada uno de los objetivos específicos propuestos y, por lo tanto, conseguir dar solución al objetivo general**.

Con respecto a los objetivos específicos, la identificación de los requisitos legales se ha llevado a cabo teniendo en cuenta la legislación vigente en España. Además, para la interpretación de algunos de los preceptos, **se ha contado con la opinión de expertos en la materia**, referenciados en la Bibliografía, si bien, ante la falta de jurisprudencia, necesaria para afinar mucho más varios conceptos de la legislación, así como su alcance, se ha hecho una interpretación estricta de los textos legales (por ejemplo, en la colaboración de los sujetos obligados, no se hace referencia a ningún tipo de limitación en el texto legal, por lo que se interpreta la norma tal cual, es decir, se puede pedir y el Juez puede conceder autorización, para cualquier tipo de colaboración de la que dicho sujeto obligado sea capaz, sin más limitación que su capacidad real). De este modo, se ofrece una **explicación clara y simple de la legislación vigente**, lo que permite que los investigadores pueden tener mucho más claro qué es lo que se necesita, y qué es lo que se puede conseguir, legalmente.

En lo que respecta a la identificación, de la forma más completa posible, del dispositivo a registrar, se ha ofrecido el **uso de diversas herramientas de escaneo y captura de tráfico**, que pueden aportar una gran cantidad de datos sobre el mismo. Igualmente, todas las técnicas de investigación policiales que se utilicen, pueden servir para la identificación, aunque sólo sea de modo parcial, del dispositivo a registrar. Quizá, **en alguna ocasión, incluso pudiera no ser necesario hacer uso de aquellas herramientas por haber identificado por completo el dispositivo mediante el uso de técnicas de investigación policial** (aunque no es lo más habitual). Además, también se ha relacionado a los sujetos obligados a colaborar, los cuales pueden ser solicitados (como podrían ser Movistar, Vodafone u Orange) para facilitar todos los datos del dispositivo de los que dispongan.

En lo referente a los medios técnicos necesarios para llevar a cabo la metodología propuesta con éxito, se ha ofrecido una serie de **hardware y software recomendado para realizarlo**. Este hardware y software es el que se encuentra, por decirlo así, al alcance de cualquier persona y organización. Claro está que existirán tanto nuevo software como hardware, específico para los fines del presente Trabajo de Fin de Máster, pero que sólo están al alcance

de entidades gubernativas, por lo que se trataría de materia reservada. Los medios propuestos facilitan un punto de partida, el cual permite realizar en su totalidad la metodología propuesta, y que puede ser actualizado y mejorado continuamente, en función de la disponibilidad que se vaya generando en el futuro.

También se ha ofrecido un **"oficio tipo" de solicitud de autorización de la medida**, el cual incluye todos aquellos puntos que se consideran importantes para su concesión. Dicho "oficio tipo" se puede adaptar a cualquier tipo de investigación que requiera de la realización de un registro remoto en un dispositivo informático. De este modo, a la hora de solicitar autorización para la ejecución de la medida, no se olvidará solicitar ninguna que pueda resultar de interés para la investigación.

Finalmente, **se ha realizado una intrusión y posterior registro remoto sobre un dispositivo Android, aplicando la metodología propuesta**. Dicho registro remoto se ha realizado a modo de simulación con dispositivos y redes propios, puesto que por motivos legales obvios no se puede realizar sobre terceros sin su consentimiento o con autorización del Juez (que, evidentemente, no la va a conceder para realizar una prueba). Así, se ha seguido la metodología, paso a paso, sobre un caso "de fantasía", hasta llegar a la finalización de la misma, consiguiendo así realizar la realización del registro remoto sin el conocimiento de su titular.

Por lo tanto, los objetivos específicos propuestos para este Trabajo de Fin de Máster se han visto completados. De este modo, mediante el cumplimiento de diversas etapas intermedias, se consigue la consecución del objetivo general, que no es otro que ofrecer una metodología para poder llegar a realizar registros remotos, mediante la instalación de un programa destinado a tal fin, haciendo uso para ello de la Ingeniería Social y, por lo tanto, sin el conocimiento de su titular.

Para finalizar con las conclusiones, se ha llegado a un convencimiento: si bien el eslabón más débil de la seguridad son las personas, también es cierto que para que un programa se instale y ejecute, habiendo utilizado Ingeniería Social, es necesaria la voluntad de las personas para realizarlo. Es decir, se depende totalmente de la persona investigada para que el registro remoto tenga éxito. Y para conseguir se la voluntad de la persona investigada sea la de instalar el software que le ha sido enviado, se han ofrecido una serie de herramientas para ganarse la confianza del objetivo y conseguir que instale la aplicación que se desea.

5.2. Líneas de trabajo futuro

Como líneas principales de trabajo futuro, se proponen las siguientes:

- Contar con un **mayor número de herramientas**, que permitan que la instalación del software destinado a realizar el registro remoto sea llevada a cabo sin apenas participación por parte de la persona investigada.

- Contar con software más específico para la realización de los registros remotos. Un buen punto de partida sería la elaboración de un listado de software permitido o recomendado por parte de la Autoridad Judicial.

- **Aplicación de la metodología propuesta** en el presente Trabajo Fin de Máster por parte de las Fuerzas y Cuerpos de Seguridad competentes para la investigación de este tipo de delitos, y conocimiento y aplicación de la misma por parte del Poder Judicial y Fiscalía. De este modo, se podrían realizar mejoras en la metodología, así como tasar y perfilar, de una forma más precisa, los límites que presentaría la legislación vigente en su aplicación real.

6. Bibliografía

apk-downloader. (2017). Recuperado el 09 de 06 de 2017, de https://apps.evozi.com/apk-downloader/

apkinjector. (03 de 04 de 2017). Recuperado el 25 de 05 de 2017, de https://github.com/jbreed/apkinjector

bettercap. (15 de 05 de 2017). Recuperado el 10 de 06 de 2017, de https://www.bettercap.org

Conde-Pumpido Tourón, C. (10 de octubre de 2016). *La reforma procesal. Registro de sistemas informáticos, ampliación del registro a otros sistemas. El regsitro remoto de dispositivos informáticos (Arts 588 sexies y 588 septies LECrim).* Recuperado el 27 de mayo de 2017, de www.fiscal.es: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Conde-Pumpido%20Tourón.pdf?idFile=4d9fe168-e9ee-4cd9-a783-68eab6158e47

Constitución Española. (29 de diciembre de 1978). España: Agencia Estatal Boletín Oficial del Estado.

Core Impact. (06 de 06 de 2017). Recuperado el 06 de 06 de 2017, de https://www.coresecurity.com/core-impact

DNS spoofing. (11 de 02 de 2017). Recuperado el 20 de 05 de 2017, de https://es.wikipedia.org/wiki/Envenenamiento_de_DNS

Dorks. (10 de 06 de 2017). Recuperado el 10 de 06 de 2017, de https://es.wikipedia.org/wiki/Google_Hacking

El Confidencial. (10 de octubre de 2015). *El Confidencial*. Recuperado el 24 de mayo de 2017, de http://www.elconfidencial.com/tecnologia/2015-04-10/phishing-hacienda-agencia-tributaria-correo-electronico_757163/

exiftool. (19 de 11 de 2003). Recuperado el 08 de 06 de 2017, de http://www.sno.phy.queensu.ca/~phil/exiftool/

exploit. (07 de 02 de 2017). Recuperado el 03 de 06 de 2017, de https://es.wikipedia.org/wiki/Exploit

F. Iglesias, P. (26 de febrero de 2015). *PabloYglesias*. Recuperado el 23 de abril de 2017, de https://www.pabloyglesias.com/mundohacker-ingenieria-social/

Google Play. (2017). Recuperado el 10 de 06 de 2017, de https://play.google.com/store?hl=es

Google, O. y. (27 de mayo de 2017). Recuperado el 02 de junio de 2017, de http://www.ts.ucr.ac.cr: http://www.ts.ucr.ac.cr/bv/operadores-google.pdf

hash. (23 de 04 de 2017). Recuperado el 09 de 06 de 2017, de https://es.wikipedia.org/wiki/Función_hash

httrack. (20 de 05 de 2017). Recuperado el 03 de 06 de 2017, de https://www.httrack.com

Kali Linux. (06 de 06 de 2017). Recuperado el 06 de 06 de 2017, de https://www.kali.org

Ley Orgánica 1/2015, de 30 de marzo, del Código Penal. (31 de marzo de 2015). *Ley Orgánica*. Agencia Estatal Boletín Oficial del Estado.

Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. (6 de octubre de 2015). España: Agencia Estatal Boletín Oficial del Estado.

mailutils. (2010). Recuperado el 02 de 06 de 2017, de https://mailutils.org

MD5. (09 de 06 de 2017). Recuperado el 10 de 06 de 2017, de https://es.wikipedia.org/wiki/MD5

Metasploit. (06 de 06 de 2017). Recuperado el 06 de 06 de 2017, de https://metasploit.com

meterpreter. (2017). Recuperado el 02 de 06 de 2017, de Offensive Security: https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/

MITM. (17 de 03 de 2017). Recuperado el 07 de 06 de 2017, de https://es.wikipedia.org/wiki/Ataque_de_intermediario

msfconsole. (2017). Recuperado el 01 de 06 de 2017, de Offensive Security: https://www.offensive-security.com/metasploit-unleashed/msfconsole/

msfvenom. (14 de 09 de 2016). Recuperado el 17 de 05 de 2017, de https://github.com/rapid7/metasploit-framework/wiki/How-to-use-msfvenom

nmap. (10 de 06 de 2017). Recuperado el 10 de 06 de 2017, de https://nmap.org

Oracle VM VirtualBox. (28 de 04 de 2017). Recuperado el 09 de 06 de 2017, de tps://www.virtualbox.org

payload. (28 de 04 de 2017). Recuperado el 07 de 06 de 2017, de https://es.wikipedia.org/wiki/Carga_útil_(informática)

postfix. (17 de 06 de 2017). Recuperado el 17 de 06 de 2017, de https://es.wikipedia.org/wiki/Postfix

Rogue AP. (17 de 01 de 2017). Recuperado el 08 de 06 de 2017, de https://en.wikipedia.org/wiki/Rogue_access_point

sammobile. (08 de 06 de 2017). Recuperado el 08 de 06 de 2017, de https://www.sammobile.com

sees. (16 de 10 de 2014). Recuperado el 02 de 06 de 2017, de https://github.com/galkan/sees

SHA-1. (17 de 06 de 2017). Recuperado el 17 de 06 de 2017, de https://es.wikipedia.org/wiki/Secure_Hash_Algorithm

SHA-2. (25 de 04 de 2017). Recuperado el 09 de 06 de 2017, de ttps://es.wikipedia.org/wiki/SHA-2

spade. (12 de 09 de 2016). Recuperado el 20 de 05 de 2017, de https://github.com/suraj-root/spade

Tejerina Rodríguez, O. (08 de julio de 2015). *www.internautas.org*. Recuperado el 25 de mayo de 2017, de https://www.internautas.org/html/8833.html

tinyurl. (2002). Recuperado el 02 de 06 de 2017, de http://tinyurl.com

TOR. (03 de 07 de 2017). Recuperado el 03 de 07 de 2017, de https://torproject.org

TOR Browser. (2017). Recuperado el 09 de 06 de 2017, de https://www.torproject.org/projects/torbrowser.html.en

TP-LINK TL-WN722N. (23 de 05 de 2017). Recuperado el 09 de 06 de 2017, de http://www.tp-link.es/products/details/cat-11_TL-WN722N.html

Universidad de Costa Rica. (27 de mayo de 2017). Recuperado el 02 de junio de 2017, de http://www.ts.ucr.ac.cr: http://www.ts.ucr.ac.cr/bv/operadores-google.pdf

VMWare Inc. (06 de 06 de 2017). Recuperado el 06 de 06 de 2017, de http://www.vmware.com

Wen, A. (01 de junio de 2017). *Blog Oficial de Google España*. Recuperado el 05 de junio de 2017, de https://espana.googleblog.com

WiFi Pineapple. (26 de 05 de 2017). Recuperado el 26 de 05 de 2017, de https://www.wifipineapple.com

wifite. (18 de 02 de 2014). Recuperado el 20 de 05 de 2017, de http://tools.kali.org/wireless-attacks/wifite

Winter, L. B. (12 de diciembre de 2016). *Ministerio de Justicia.* (B. d. Justicia, Ed.) Recuperado el 1 de junio de 2017, de http://www.mjusticia.gob.es/cs/Satellite/Portal/1292428206148?blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadername2=EstudioDoctrinal&blobheadervalue1=attachment%3B+filename%3D1701_Estudio.pdf&blobheadervalue2=1288794492107

wireshark. (19 de 05 de 2017). Recuperado el 02 de 06 de 2017, de https://www.wireshark.org.

Anexos

Anexo I – Oficio de solicitud

O F I C I O

S/REF:

N/REF: xxxxxx/2015

FECHA: xx-xx-2017

ASUNTO: Solicitud autorización registro remoto de equipo informático

DESTINATARIO: JUZGADO DE INSTRUCCIÓN NÚMERO XXXX, XXXXXXX

El Grupo de Investigación Tecnológica, perteneciente la Brigada Provincial de Policía Judicial, de la Comisaría Provincial de XXXXXXXX del Cuerpo Nacional de Policía, se encarga de la investigación de todos los delitos cometidos a través del uso de equipos informáticos y de las llamadas “nuevas tecnologías”.

En fecha XXXXX, por parte del citado Grupo de Investigación, se tuvo conocimiento de que Arturo ESPAÑOL ESPAÑOL, presuntamente, se dedicaba a realizar fotografías con su teléfono móvil a menores de entre 5 y 15 años, los cuales debían posar en actitud de carácter erótico o sexual.

Según la información recibida, tras la realización de dichas fotografías, éstas eran compartidas por el filiado a través de pendrives USB, haciendo uso de envíos de paquetería urgente para hacer llegar dichos dispositivos, los cuales contenían las fotografías de los menores, ya referenciadas, a los diferentes destinatarios.

Tras la realización de diferentes investigaciones, se llegó a determinar que el anteriormente filiado, acudía con una periodicidad de, al menos, 2 veces por semana, a una empresa de paquetería, en la que realizaba envíos.

En fecha xxxxx, se procedió a solicitar al Juzgado de Instrucción XXXXXXX autorización para la interceptación de dichos envíos postales, con el objetivo de verificar que, efectivamente, contenían fotografías de menores en actitud sexual o erótica.

Por funcionarios adscritos a este Grupo de Investigación, en fecha XXXX se procedió a la interceptación de un paquete postal, cuyo remitente era Arturo ESPAÑOL ESPAÑOL y cuyo destinatario era XXXXXXXXXXX, realizado por la empresa XXXXX, sita en la calle XXXXXXX. Dicho paquete intervenido, el cual ya fue remitido al citado Juzgado de Instrucción para su posterior apertura en sede Judicial, la cual fue llevada a cabo en fecha xxxxxxx.

Tras la apertura de dicho paquete, por parte de este Grupo de investigación, se solicitó el análisis del contenido del dispositivo USB que se encontraba dentro del paquete. Resultado del citado análisis, se hallaron xxxx imágenes de menores, de entre 4 y 14 años de edad, todas ellas fotografías de carácter sexual explícito. Se remitió informe al Juzgado de Instrucción XXXXXX en fecha xxxxxx con las conclusiones del análisis del dispositivo USB.

Mediante vigilancias y seguimientos realizados, se ha constatado que el anteriormente filiado utiliza un cable USB OTG (USB on the go, que permite la descarga de datos directamente desde un teléfono móvil a un pendrive USB) varias veces a la semana. Dicha acción la realiza tras la permanecer varias horas en un piso sito en la calle XXXXXXX, si bien no se ha observado la salida de ningún menor del citado lugar posteriormente a la salida del filiado.

También se ha constatado que Arturo ESPAÑOL ESPAÑOL utiliza las redes inalámbricas abiertas de diferentes comercios con su teléfono móvil, el cual se conecta a las mismas de forma automática, lo que da a entender que tiene activado el servicio “WiFi” de su teléfono móvil continuamente. Sobre todo, se ha observado que todos los días de lunes a viernes, de 14 a 22 horas permanece en el Centro Cívico El Carmen, sito en xxxxxxxx, en el cual trabaja y que en el mismo hace uso de su teléfono móvil, estando conectado a la red inalámbrica pública de dicho lugar. Por ello, el envío del correo electrónico con el software y posterior instalación, se realizaría utilizando dicha red, puesto que se ha comprobado que el número de usuarios conectados a esas horas es muy bajo (una media de 3 usuarios).

Igualmente, realizadas las comprobaciones pertinentes, en dicho lugar no consta como ocupante ningún menor.

Por todo lo anterior, se tienen importantes indicios de que Arturo ESPAÑOL ESPAÑOL es quien realiza directamente las fotografías a los menores, para después remitirlas a diferentes destinatarios, lo que podría ser constitutivo de un delito previsto en el artículo 189 del Código Penal, para el cual tiene competencia investigadora este Grupo de Delitos Tecnológicos.

Con el fin de poder comprobar, pues no es posible determinarlo mediante las técnicas de investigación habituales, aplicadas hasta el momento, que es Arturo ESPAÑOL ESPAÑOL quien efectivamente realiza directamente las fotografías a los menores, realiza la copia de dichas fotografías a un pendrive USB y posteriormente envía el dispositivo que contiene las

imágenes mediante paquetería urgente, se solicita de V.I. que libre mandamiento de autorización, con una duración inicial de 1 mes, para la utilización de datos de identificación y códigos, así como la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos, concretamente para el teléfono móvil personal de Arturo ESPAÑOL ESPAÑOL, del cual se conocen los siguientes datos: número de teléfono móvil 66-666-666, Samsung Galaxy S4, Sistema Operativo Android, email utilizado "jreacherprueba@gmail.com".

Se procederá al acceso al dispositivo de forma remota (mediante el uso de Ingeniería Social), utilizando software específico para el Sistema Operativo Android para el registro remoto.

Igualmente, se solicita que libre mandamiento a "MOVISTAR XXXXXXXX", con CIF xxxxx y domicilio social en xxxxxxxxxxxxxxxx, para que preste colaboración en lo referente a las cuestiones técnicas necesarias para la instalación del software indicado de forma remota, pues se tiene conocimiento de que el número de teléfono anteriormente indicado, pertenece a dicha operadora de telefonía.

También se solicita a V.I. que conceda autorización para la realización de copia de los datos relevantes para la presente investigación, los cuales quedarán almacenados en un dispositivo extraíble, en poder de este Grupo, garantizando la integridad de los mismos mediante la aplicación de funciones hash a los mismos, lo que permite comprobar, durante todo el proceso, que no han sido modificados.

Se significa que los funcionarios adscritos a este Grupo de Investigación que llevarán a cabo la medida, caso de ser autorizada, se identifican mediante los números de carné profesional xxxxx y xxxxxx.

Vista la cantidad de indicios existentes para presumir racionalmente que Arturo ESPAÑOL ESPAÑOL podría estar realizando fotografías de carácter sexual a menores de edad, y dada la gravedad del delito que corresponde a la realización de dichas acciones, correspondientes a un delito previsto en el artículo 189 del Código Penal, es por lo que se estima proporcionada la adopción de la medida solicitada a V.I., con una duración inicial de 1 mes. Que dicha medida se torna imprescindible para la investigación, pues se han agotado todas las técnicas policiales de investigación hasta el momento y es la medida idónea para realizar la comprobación efectiva de los hechos descritos anteriormente.

Anexo II – Capturas de pantalla del teléfono móvil

Ilustración 30. Imagen del correo electrónico recibido en el dispositivo a registrar remotamente.

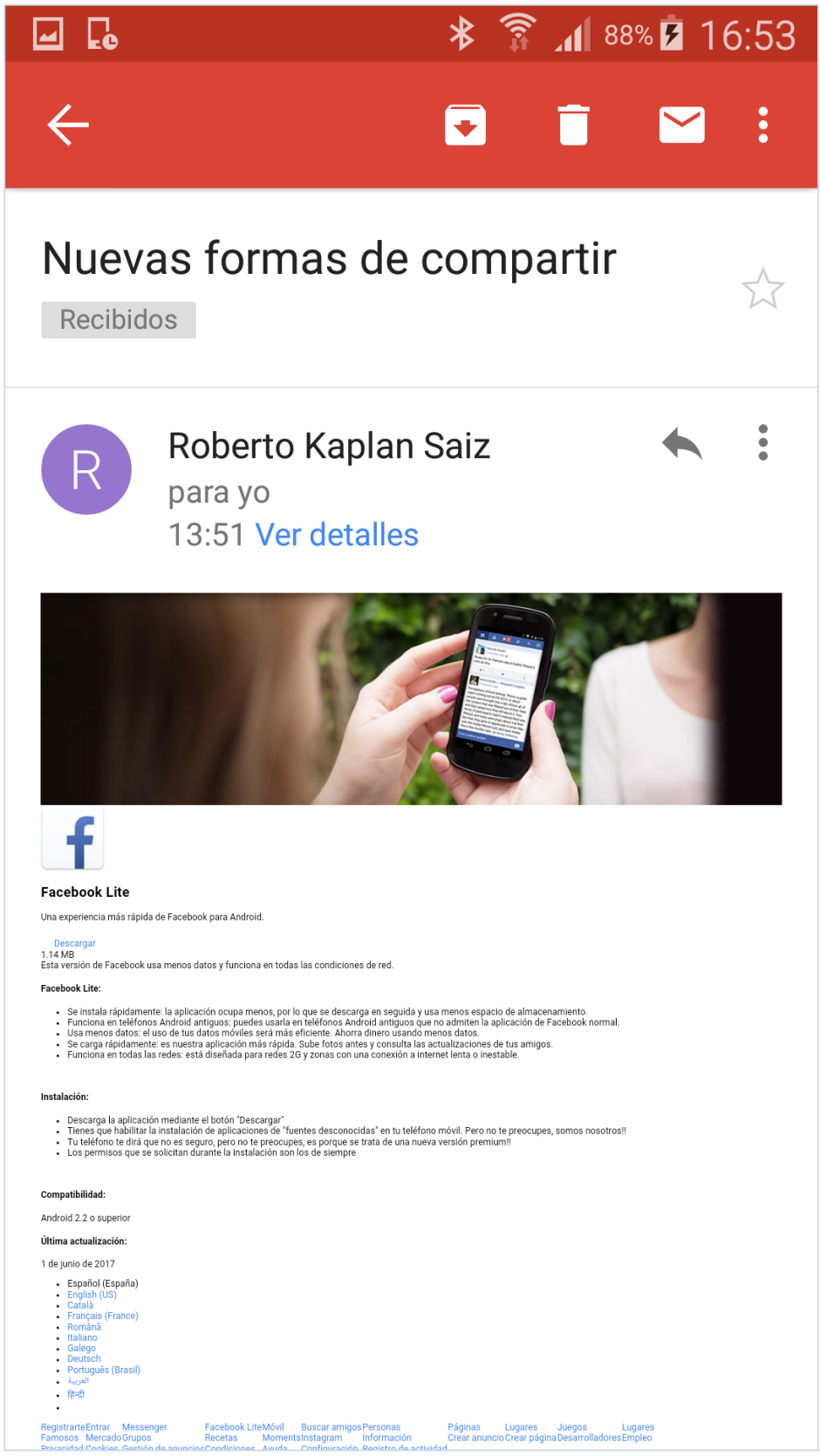

Ilustración 31. Aspecto del contenido del correo electrónico recibido en el dispositivo a registrar

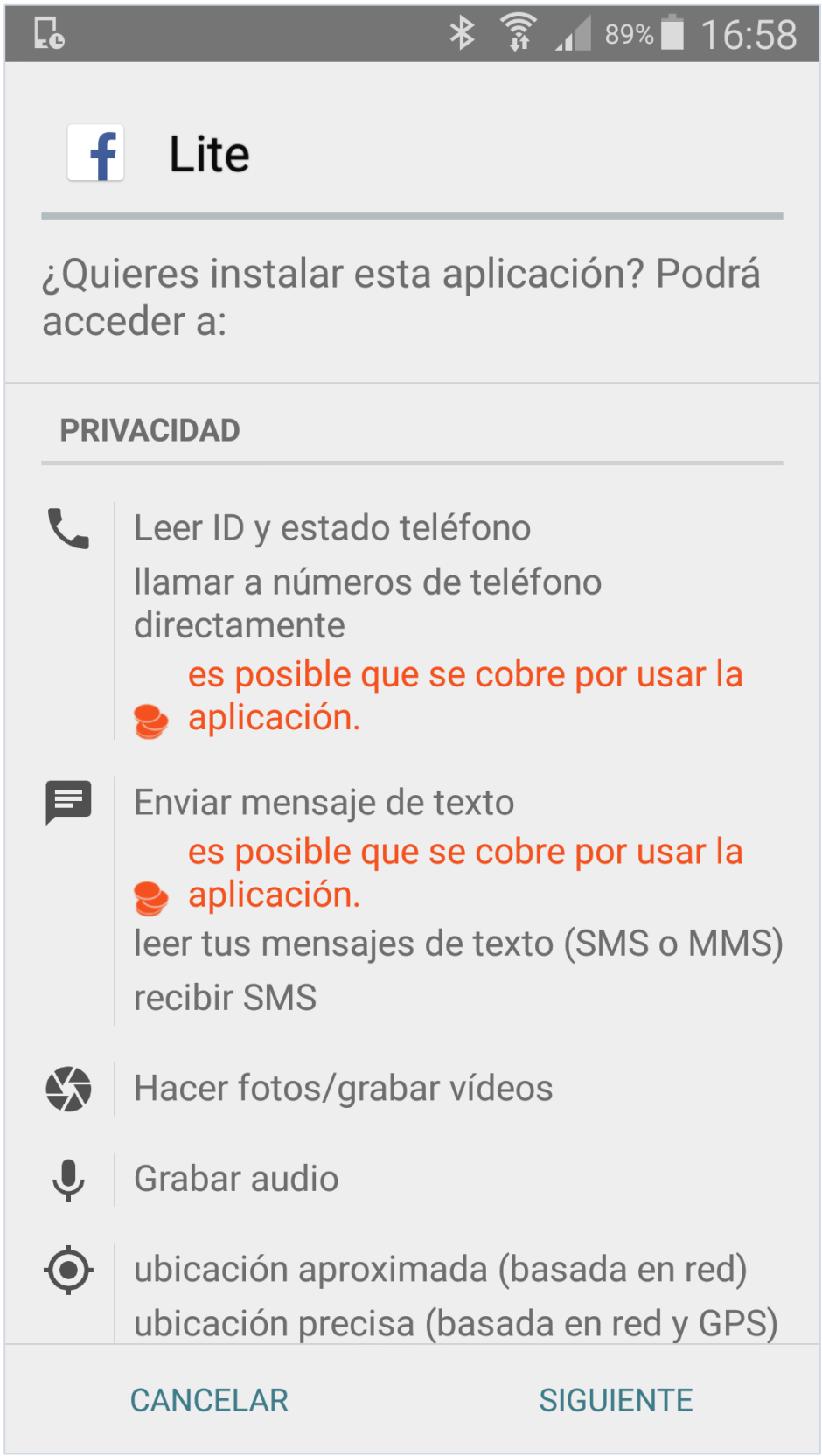

Ilustración 32. Permisos solicitados durante la instalación (1 de 3)

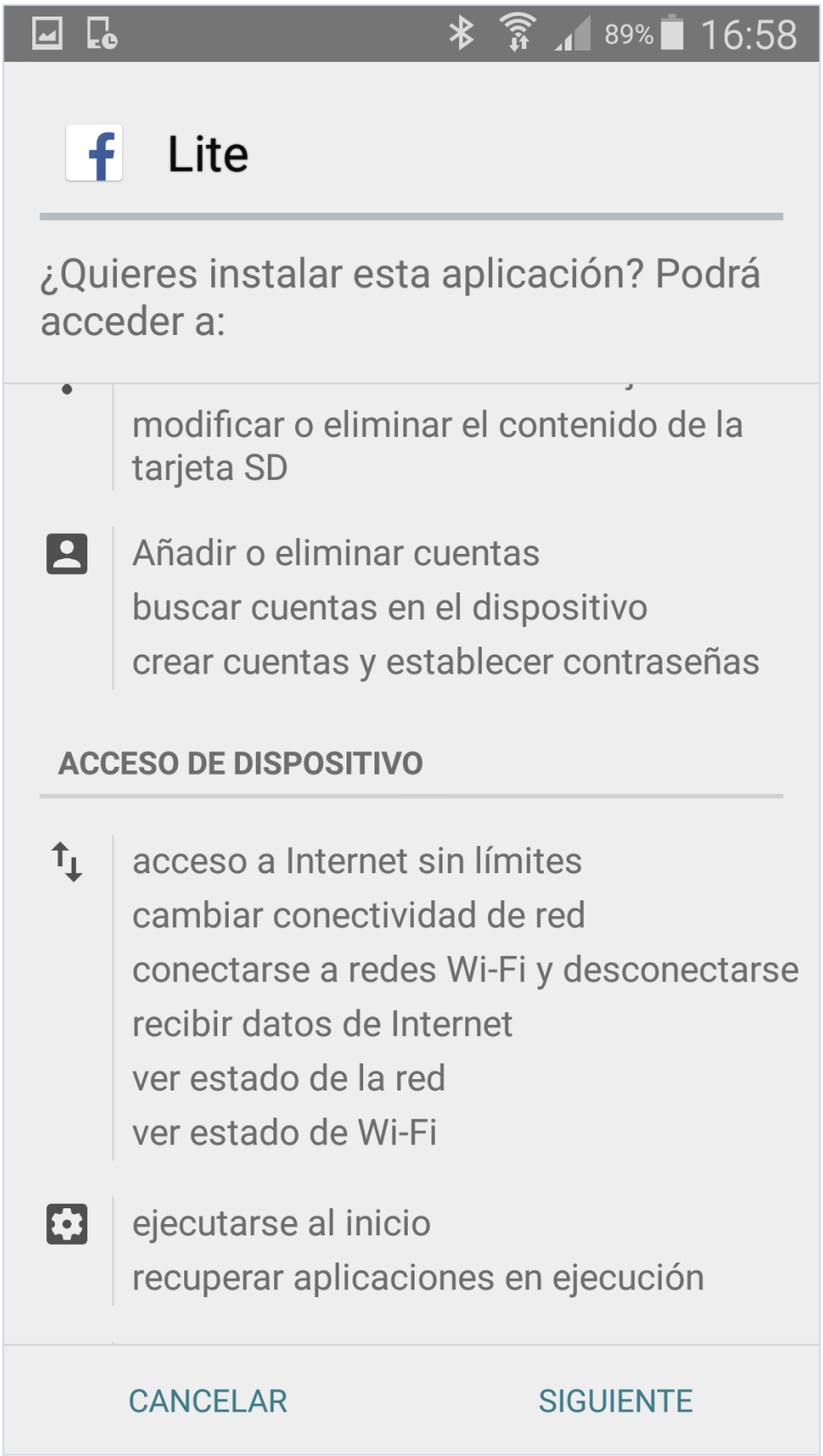

Ilustración 33. Permisos solicitados durante la instalación (2 de 3)

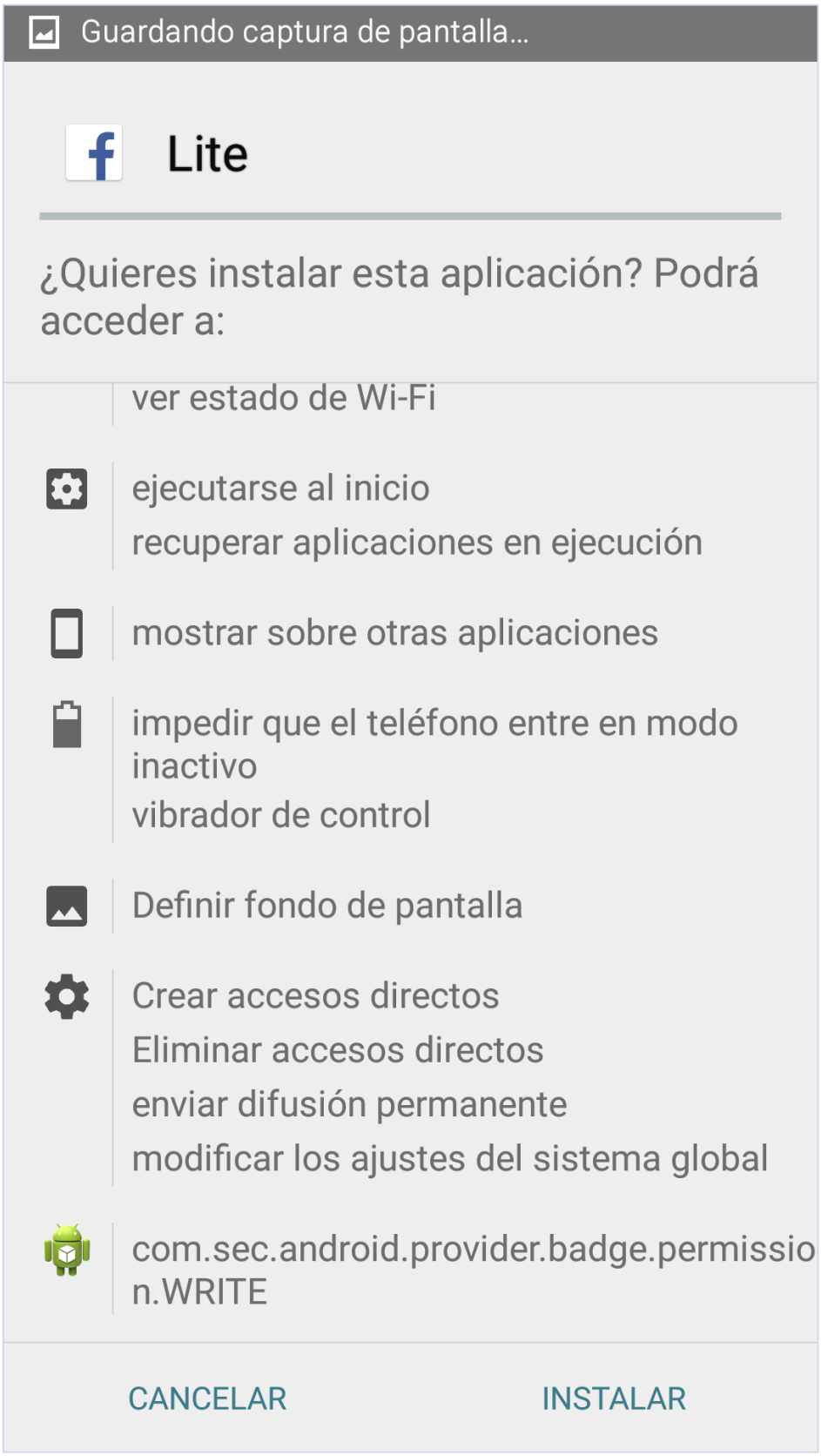

Ilustración 34. Permisos solicitados durante la instalación (3 de 3)

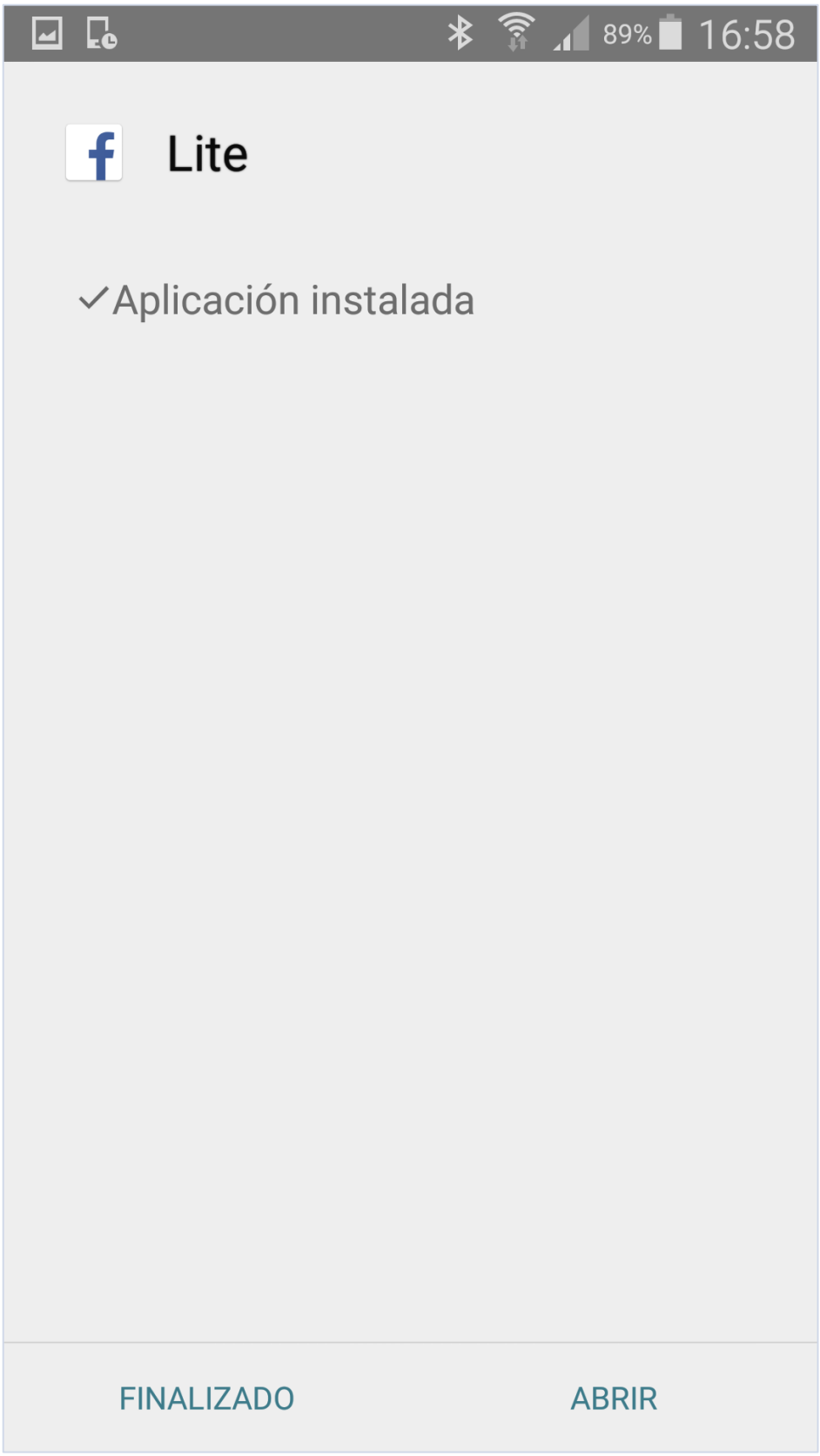

Ilustración 35. Mensaje de aplicación instalada en el dispositivo.

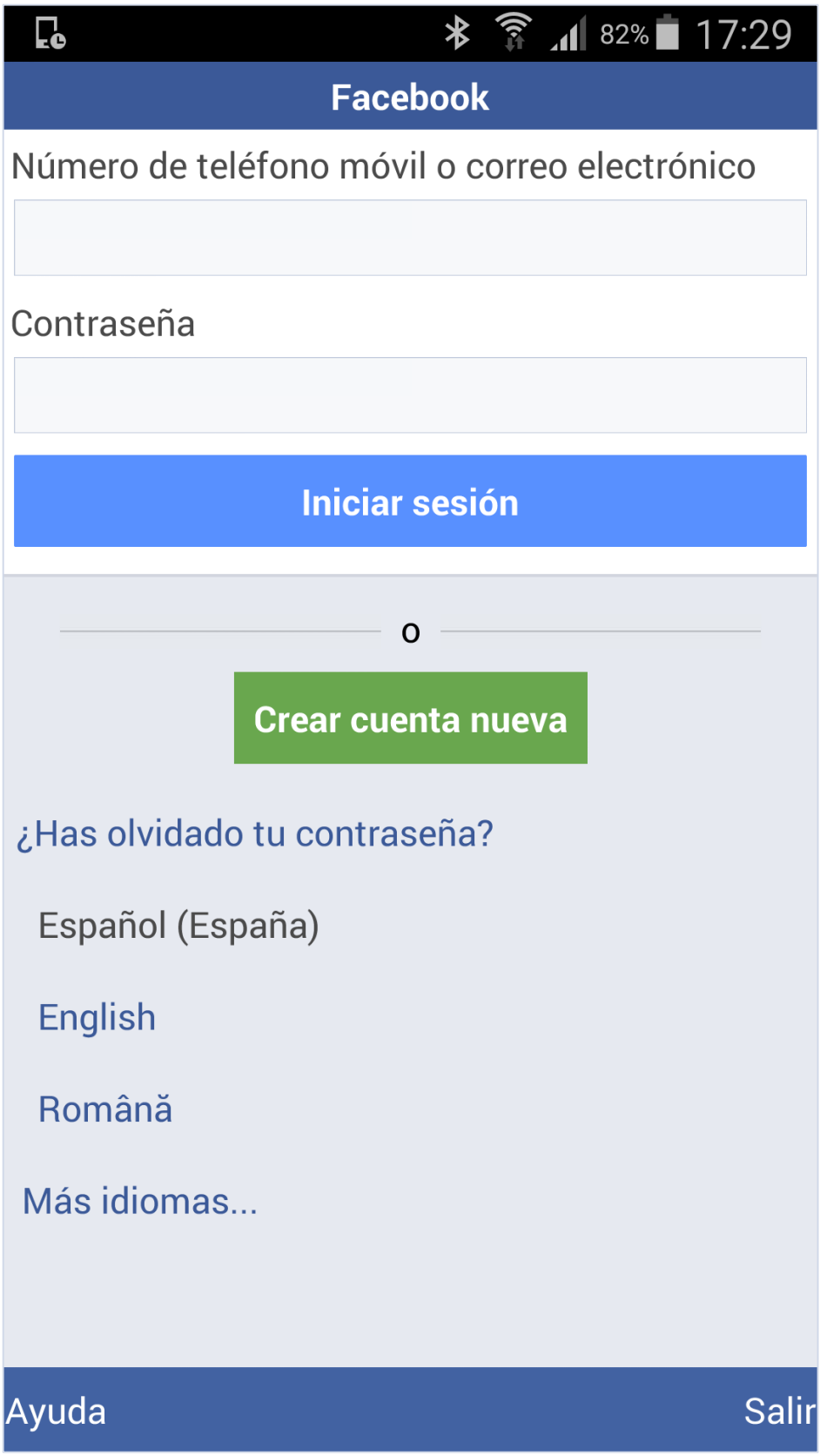

Ilustración 36. Aplicación modificada en funcionamiento en el dispositivo, totalmente funcional

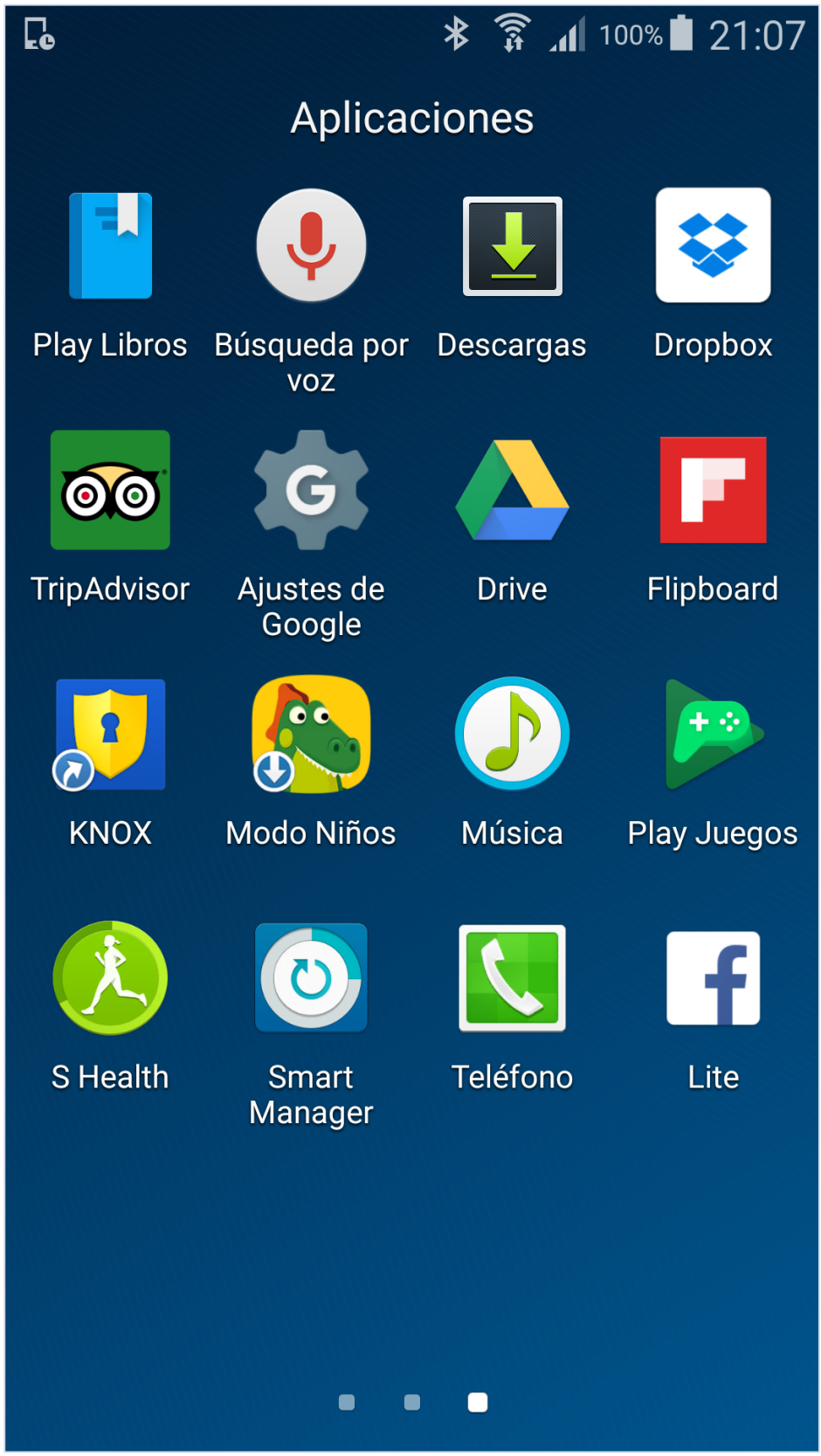

Ilustración 37. Conjunto de aplicaciones instaladas en el dispositivo, incluyendo "Facebook Lite" modificada.