UNIVERSIDAD AUTÓNOMA DE MADRID

ESCUELA POLITÉCNICA SUPERIOR

PROYECTO FIN DE CARRERA

PROTOCOLO DE ACTUACIÓN EN PERITACIONES INFORMÁTICAS

Ingeniería de Telecomunicación

Autor: Luis Miguel Gómez Aparicio

ABRIL 2016

PROTOCOLO DE ACTUACIÓN EN PERITACIONES INFORMÁTICAS

Versión adaptada para su cesión a la plataforma digital de la Universidad Autónoma de Madrid

AUTOR: Luis Miguel Gómez Aparicio
TUTOR: Álvaro Ortigosa Juárez

Escuela Politécnica Superior
Universidad Autónoma de Madrid
Abril de 2016

PROYECTO FIN DE CARRERA

Título: Protocolo de actuación en Peritaciones Informáticas

Autor: Luis Miguel Gómez Aparicio
Tutor: Álvaro Ortigosa Juárez

“This demonstrates the value of not being seen.”
Monty Python

Agradecimientos

A mi familia, que me lo ha dado todo.
Y a Julián, el autodidacta genial que me hizo recuperar la ilusión por estos "cachivaches".

RESUMEN

Los peritos judiciales informáticos son profesionales con amplia formación universitaria y una cuidada especialización que tienen como objeto y finalidad el asesoramiento de jueces, fiscales, abogados o particulares para la recogida, tratamiento y estudio de evidencias digitales. Estos se encargan de recabar toda la información que se encuentre disponible en cualquier elemento dispositivo electrónico que tenga interés judicial o empresarial. Deben de ser capaces de resolver los problemas que requieran jueces o empresas para la utilización de esa información.

La información será utilizada para la realización de informes periciales. El objetivo principal del Proyecto Fin de Carrera será la redacción de un Protocolo de actuación para la peritación forense informática. Para ello se realizará un estudio detallado de la situación actual de los sistemas de peritación actuales, exponiendo como se realizan los informes periciales llevados a cabo por expertos peritos que realizan en la actualidad peritaciones civiles y peritaciones en la administración.

Identificaremos y definiremos los aspectos más significativos de la figura de la peritación informática para dar respuesta a todos los campos de estudio a los que los Peritos Tecnológicos Informáticos Forenses se tienen que enfrentar en el desarrollo de sus funciones. Todos estos apartados se generan a través del estudio cuidadoso de la legislación para el desarrollo de la peritación, de su normativa aplicable, con especial interés en la jurisprudencia existente que surge como respuesta a las múltiples actuaciones judiciales en el ámbito del estudio de la evidencia digital. Para posteriormente centrarnos en la realización de la peritación en sí; enumerando y describiendo sus partes, las peculiaridades de las peritaciones informáticas, así como sus novedades legislativas, debido a su nueva incorporación a la terminología jurídica.

Ilustraremos la adaptación de la legislación a las nuevas tecnologías mediante la jurisprudencia generada y posterior legislación que producirá la aplicación de estas actuaciones judiciales. Desarrollando un estudio pormenorizado de la preparación de la pericia informática, su presentación, análisis y la defensa de nuestro trabajo ante sus requirentes. Para eso nos serviremos de numerosos ejemplos, definiciones de la terminología comúnmente utilizada y de las herramientas actuales, de este mundo tecnológico que se mueve a una velocidad vertiginosa, en la que tenemos que estar continuamente actualizados.

En definitiva, estamos ante la guía de actuación para la peritación y el análisis de cualquier dispositivo electrónico que sea capaz de almacenar o hacer fluir información. Ya que la información es poder, y estamos en la era de la gestión de la información.

“True genius resides in the capacity for evaluation of uncertain, hazardous, and conflicting information.”

Winston Churchill

Palabras clave: Perito, forense, evidencia digital, imagen y protocolo.

SUMMARY

The qualified judicial I.T. technicians are experts with a wide universitary formation and a careful specialization, which main purpose is to assess judges, public prosecutors, lawyers and individuals for the evidence collection, their treatment and their case study.

They are in charge of collecting all the available information in any digital device, element or physical device which could be judicially or corporatively pertinent. They must be able to solve all the matters required by judges or companies for the treatment of the mentioned information. This information will be used to elaborate expert reports. Their main objective will be to write up an intervention protocol for the forensic I.T. punditry. For this, a detailed study should be done about the current punditry systems, moreover a procedure about how this process was done by the beforehand mentioned experts who are in charge of that civil and public punditries at the moment.

We will identify and define the most significant aspects about the I.T. punditry figure to give an answer to all the fields which forensic technical I.T. experts have to face up during the technical performance. We should study carefully all the legislation in the technical performance process, the applicable legislation with extra care about the jurisprudence which is the answer to the digital multiple judicial acts in the evidence field. Afterwards, we should focus on the punditry per se; enumerating and describing its parts, the I.T. punditry peculiarities, as well as the judicial novelties in order to their addition to the judicial terminology. This will show the legislation adaptation to these judicial acts.

We will develop a detailed study about the preparation for the I.T. punditry performance, its presentation, analysis, and defense about our work to our inquirer. For that, we will use multiple examples, definitions from the common terminology and current tools, coexisting in this technological word, which is spinning at a vertiginous speed to update them continuously.

In conclusion, we are facing the definitive punditry performance guide, owing to the power of the information nowadays and also because we are in the information management era.

"True genius resides in the capacity for evaluation of uncertain, hazardous, and conflicting information."

Winston Churchill

Keywords: Expert qualification witness, forensic, digital evidence, backup and protocol.

ÍNDICE DE CONTENIDOS

(El índice puede presentar pequeñas variaciones debido a la adaptación)

ÍNDICE DE FIGURAS

ÍNDICE DE FIGURAS DE HERRAMIENTAS FORENSES

ÍNDICE DE TABLAS

1. Introducción

La evolución de la sociedad de la comunicación e información produce una transformación continua de las tecnologías que la rodean, haciéndose más complejas de estudiar. Estos cambios, afectan de forma notable a la interacción de los individuos con la propia sociedad en sí. Esta evolución de la comunicación y el uso de la información hace que la gestión de estos datos sea en estos días una de las piezas fundamentales del funcionamiento de la sociedad actual. El conocimiento de la utilización de esta información, el tratamiento que se realice a los datos y su almacenamiento en los numerosos componentes electrónicos, hace que su estudio técnico sea una herramienta imprescindible en los procesos judiciales y empresariales.

Entendemos internet como uno de los pilares principales para la comunicación y la transmisión de la información. Esta queda posteriormente registrada y grabada en los dispositivos. La Red informática mundial se ha convertido en una interfaz para la distribución de información; desde los mensajes, las fotografías, los correos electrónicos, la gestión de identidades, las transacciones bancarias, las redes sociales... se intercambian paquetes con datos personales y confidenciales. En estos días existen una gran cantidad de equipos que contienen información personal; ordenadores, teléfonos inteligentes, tabletas, gadgets tecnológicos... se han convertido en una parte indispensable de nuestras vidas tanto a nivel personal como profesional. Las nuevas tecnologías son uno de los pilares básicos del funcionamiento de nuestra sociedad, formando parte en cada una de las actividades cotidianas de la misma, esto trae consigo también la parte menos visible, pero si presente y perseguible; los delitos que utilizan medios informáticos y que quedan registrados en los dispositivos electrónicos que son utilizados para realizarlos.

Los peritos judiciales informáticos son profesionales con amplia formación universitaria y una alta especialización. Estos se encargan de recabar toda la información que se encuentre disponible en cualquier elemento electrónico que tenga interés judicial o empresarial. Deben de ser capaces de resolver los problemas que requieran jueces o empresas para la utilización de esa información.

La recogida, tratamiento, estudio y posterior realización de los informes periciales requieren un protocolo esquematizado que se perfila como uno de los elementos fundamentales en el ámbito judicial y empresarial. La información de estos dispositivos se debe conseguir de manera muy estructurada y donde quede de manifiesto que ha sido recogida y tratada de manera aséptica, es decir sin interferencias exteriores de ningún tipo. Haciendo que el estudio de la información sea en todo momento objetiva y eficaz, evitando la manipulación de estos datos.

Los informes periciales deben de tener un perfil técnico y tecnológico, fundamentados en procesos forenses, de investigación legal y criminalística, apoyados con amplios conocimientos legales en derecho penal, civil y administrativo. Dada la complejidad de estos informes, se debe proceder de una manera esquemática y dirigida por medio de un Protocolo de actuación, que estandarice el estudio de esta la información.

En nuestros días a través de equipos electrónicos se gestiona el mundo. La electricidad, el tráfico, el tráfico aéreo, las comunicaciones como no podía ser de otra manera

y un largo etcétera. Ante esto el derecho penal ha querido reaccionar y contemplar la sanción y la protección de varios bienes jurídicos, que son necesarios de proteger porque afectan directamente a unos de los intereses más relevantes: La privacidad y la seguridad. Para esto, se puede referir a los sistemas informáticos, otros se pueden referir a la realización de estafas utilizando estas tecnologías, por esto, en la reforma de finales del año 2015, una de las figuras que contempla es el espionaje y sabotaje, el art 197 bis el tercer, el cuarter, el quintuer, permiten atajar estas medidas con controles sobre esta nueva figura que aparece en nuestros días, como es el sabotaje informático, por supuesto que la tecnología incorpora varias conductas delictivas y por tanto también deben tener relevancia las penas contra esta de manera notoria. Los artículos, hacen mención no sólo a las interceptaciones de comunicaciones personales que ya estaban sancionados, sino también a aquellas conductas que se produzcan en sistemas.

Hasta ahora lo que se protegía para las personas, era la intercomunicación para las relaciones interpersonales, el derecho a la intimidad de las personas, hacía que toda intercomunicación tuviera una protección especial del derecho penal. Lo que se conocía como un delito de revelación de secretos. Sin embargo, aquí se va más allá, se contempla la comunicación entre dos equipos informáticos entre los que no se tiene que dar necesariamente comunicación interpersonal. Entre los que no tienen que estar comunicándose dos personas necesariamente. Y por otra parte, otra de las novedades de la reforma legislativa es la conducta delictiva, tanto la producción, como el almacenamiento para su uso o facilitación a terceros, de programas informáticos para la vulneración de la seguridad de terceros, así como desvelar contraseñas o códigos de ordenador o acceso personales que permitan acceder a todo o parte de un sistema de información, son conductas que se realizaban de manera displicente por parte de usuarios conociendo de antemano su falta de legislación propia. No solamente el que facilite las contraseñas o los programas informáticos, si no el proporcionar las propias contraseñas, agravando cuando estos actos se produzcan en el seno de una organización criminal que potencian todo ese tipo de actividades. También en el delito de daños se contempla una figura que se refiere a ella como sabotaje informático, en la que se producen importantes modificaciones. Este sabotaje informático está dirigido a producir daños importantes a empresas o entidades que requieren los sistemas atacados para su normal funcionamiento. Se tipifica la conducta consistente en dañar, destruir, modificar... con la finalidad de acceder inaccesibles los programas informáticos o documentos electrónicos.

Actuaciones policiales diversas en este ámbito como las producidas por informáticos de una empresa, que han sido despedidos o que han sido contratados por otra empresa del sector que realizan este hecho punible para presionar a la empresa para recibir mayores indemnizaciones, haciendo inaccesibles datos informáticos y demás actuaciones delictivas.

El legislador actual es consciente de que las conductas que eran vistas como algo inusual y con frecuencia poco menos que anecdótica se han ido convirtiendo, con el paso de los días, en algo habitual, como está ocurriendo en estos momentos.

Ante esta situación de la relevancia del mundo informático en nuestras vidas y que es capaz de acumular datos de una gran potencia y al mismo tiempo que es imprescindible la informática para nuestro trabajo diario, realmente la protección penal es la única que puede poner coto a cualquier abuso o cualquier situación que interfiera notablemente en estos instrumentos que son imprescindibles para nuestra vida.

Intentaré mostrar cómo se puede estudiar las partes de una comunicación con un ejemplo que utilizaba en clase el Excmo. Magistrado Juez Decano de los Juzgados de Madrid Sr. D. Francisco J. Vieira Morante, que utilizaba una naranja como analogía. En la naranja tiene relevancia el gajo, la cáscara no se suele utilizar, pero la cáscara y el gajo tienen relevancia. Actualmente, el núcleo principal de la comunicación es el gajo, pero en la cáscara de la comunicación se han ido quedando adheridos a la misma un gran número de datos muy relevantes sobre todo lo que informa sobre otros aspectos de la comunicación, que ya no hacen referencia al secreto, pero si a la intimidad, esa es la evolución del derecho, ya que ahora se pide muchas veces la cáscara y no el gajo, intentas referirte a los datos accesorios. Pues la jurisprudencia del tribunal europeo sobre esa materia ha sido contundente y se ha ido expandiendo, y eso es como consecuencia que para la protección y mantenimiento de esos gajos es necesario que la cáscara no sufra ningún tipo de desperfecto. Se trata de un concepto de la proporcionalidad que se ha ido utilizado en tanto la norma no determina de forma específica los criterios para la escisión del derecho.

Las medidas restrictivas de derechos fundamentales que no sólo en las comunicaciones telefónicas aparecen reguladas, ni en la inviolabilidad domiciliaria, es el derecho a la intimidad. El convenio europeo de derechos humanos, del que España es dignataria, exige que tiene que haber previsión normativa expresa para que se pueden restringir esos derechos fundamentales. Es cierto que invades la esfera de intimidad cuando a través de un micrófono ambiente o un equipo de escucha en un domicilio o un software introducido en un equipo electrónico, son medidas que planteaba como necesidad de la investigación debía desarrollarse algún de debilitación o supresión de un derecho fundamental, se pudiera plasmar. Claro el problema que se plantea, es que el legislador se plantea un periodo de investigación, que en sucesos anteriores a la legislación actual se realizaban este tipo de actuaciones, la observación es que ahora tenemos una norma habilitante para este tipo de proceder en el seno de investigaciones. Con lo cual poniéndonos en la posición expost del legislador de las actuaciones llevadas a cabo por la Policía Judicial, estas medidas deben tener una eficacia determinante para las acciones criminales efectuadas. De manera análoga no solo las escuchas sino los programas informáticos para la escucha o seguimiento de las personas.

Así lo indicó en 1995 Bill Gates: “Llegará un día, no muy distante, en que seremos capaces de dirigir negocios, de estudiar, de explorar el mundo y sus culturas, de hacer surgir algún gran entretenimiento, hacer amigos, asistir a mercados locales y enseñar fotos a parientes lejanos sin abandonar nuestra mesa de trabajo o nuestro sillón. Esta red será nuestro pasaporte para un modo de vida nuevo”

“*Si los años ochenta fueron el decenio de la calidad y los noventas el de la reingeniería de procesos, el primero de los 2000 será el de la velocidad. Estos cambios se producirán debido a un factor de engañosa simplicidad: el flujo de la información digital*” – Bill Gate

Pues bien, este día es hoy.

1.1 Motivación

El objetivo principal del trabajo será la redacción de un **Protocolo de actuación para la peritación forense informática.**

El principal resultado del Proyecto será la elaboración de un protocolo en forma de memoria que constará de los siguientes bloques fundamentales en los que se podrá dividir cualquier tipo de peritación. Así quedando de manifiesto que, según la entidad de la pericia, varios de los siguientes puntos pueden ser solapados o incluso realizados al mismo tiempo:

- Diseño del sistema experto de recogida técnica de indicios y evidencias.
- Diseño de los informes técnicos para establecer los parámetros de estudio.
- Estudio de informes técnicos, lectura y esclarecimiento de los elementos necesarios para la realización de los informes periciales.
- Desarrollo de los informes periciales
- Análisis, lectura y resultados de los informes periciales.
- Redactar un informe final, que sería el encargado de marcar las pautas de la realización de cada uno de los procesos, realizando un protocolo esquemático que sirva de guía práctica.

1.2 Objetivos

El objetivo del trabajo consistirá en realizar un estudio detallado de la situación actual de los sistemas de peritación actuales llevados a cabo por expertos peritos que realizan en la actualidad peritaciones civiles y peritaciones de la administración. Se procederá a realizar entrevistas con los distintos grupos de trabajo que sean los usuarios del mismo, organizando como realizar los pasos a seguir para la comunicación entre los mismos. Para eso se realizarán contactos con los dos grandes bloques a los que va dirigido este proyecto por una parte los representantes de empresas del sector y por otra parte los organismos de Seguridad del Estado, del diferentes Peritos Informáticos y de la Administración de Justicia. Todo ello para tratar de protocolizar que cada una de sus actuaciones sea la suma del proceso, haciendo este más eficaz y productivo.

Se pretende conseguir un protocolo que sirva de base para la actuación de cada una de las partes del proceso, consiguiendo que tanto los diferentes tipos de software, sus actualizaciones, dispositivos que puedan aparecer en el mercado, o las futuras leyes que sean aplicables al sector, sean fácilmente adaptables. Que se trate de un protocolo vivo, que sirva de base para la estandarización del proceso.

2.Estado del arte

Ambrosio Paré (1560-1592)
"*Losjueces deciden según se les informa*"

El Estado de Arte identificará y definirá los aspectos más significativos de la figura de la peritación informática. Las peritaciones informáticas deben estar realizadas por un perito informático, esto que a priori parece ser una obviedad manifiesta, predispone una de las bases fundamentales del objetivo de este protocolo. Marcar las características que debe tener un perito informático.

Un Perito Informático o Perito Auditor Forense es un profesional dotado de conocimientos especializados y reconocidos, es un experto tecnológico especializado en el ámbito de las 'TICs', que realiza pericia sobre puntos en litigio. Existiendo tres grupos diferenciados; los nombrados por medio de un juez (Perito Judicial Informático), los propuestos por una de las partes interesadas, que deberán ser aceptados por el juez y el nombrado por cualquier particular para formalizar una opinión fundada. Los Peritos Forenses informáticos estarán capacitados para la ejecución, aplicación y utilización de técnicas que de manera esquematizada y científica aseguren, preserven y recolecten las evidencias digitales y físicas que sirvan para el esclarecimiento de lo ocurrido, manteniendo la cadena de custodia de las pruebas.

En el momento en el que un Perito Tecnológico e Informático es nombrado por un Juez, Magistrado o la propia Administración, pasa a ser lo que se conoce como auxiliar de justicia, esto le confiere la potestad de realizar labores en la función pública en el ejercicio de sus funciones; esto le hace regirse por la legislación y reglamento propio.

Se trata de un especialista experto. Debe de contar con conocimientos en metodología forense, amplios conocimientos legales e aptitudes en investigaciones criminalistas y forenses. Es obvio afirmar que debe ser experto en la extracción de evidencias electrónicas (se trata de los datos que tienen carácter probatorio que se encuentran almacenados en los dispositivos electrónicos y que pueden ser transmitidos en forma digital por componentes electrónicos). Su principal tarea es la de búsqueda de la información mediante procedimientos técnicos, análisis, estrategias y demás modos científicos para la observación y estudio de estos datos. Deben de ser capaces de la extracción, obtención, estudio, análisis preservando la integridad de los mismos con exactitud.

2.1 CAMPOS DE ESTUDIO

Los campos de estudio de los Peritos Tecnológicos Informáticos Forenses son cuantiosos y van aumentando según crece nuestro uso de los dispositivos electrónicos en nuestra sociedad. Entre las más utilizadas destacaremos:

Figura 2.1: Campos estudio peritaciones informáticas

Robo de identidad, uso indebido de internet, sabotajes, espionajes, uso indebido de datos y abuso de material informático. De la extensa lista que pudiéramos enumerar, significaremos de entre otros los más comunes:

- Espionaje y/o revelación de secretos.
- Acceso o copia de ficheros de la empresa, planos, fórmulas, costes,
- Uso de información: Competencia desleal de un empleado.
- Vulneración de la intimidad.
- Lectura de correo electrónico.
- Despido por causas tecnológicas.
- Valoraciones de bienes informáticos.
- Interceptación de telecomunicaciones.
- Protección de datos personales y datos reservados de personas jurídicas.
- Apoderamiento y difusión de datos reservados.
- Manipulación de datos o programas.
- Valoraciones de bienes informáticos.
- Hardware, redes y componentes (todos los sistemas).
- Instalaciones y desarrollos llave en mano.
- Vulneración de la buena fe contractual.
- Publicidad engañosa,
- Competencia desleal.
- Delitos económicos, monetarios y societarios.
- Delitos contra el mercado o contra los consumidores.
- Delitos contra la propiedad intelectual.
- Uso de software sin licencia.
- Piratería.
- Copia y distribución no autorizada de programas de ordenador.
- Daños mediante la destrucción o alteración de datos.
- Sabotaje.
- Estafa, fraudes, conspiración para alterar el precio de las cosas.

- Pornografía infantil: acceso o posesión, divulgación, edición.
- Uso indebido de equipos informáticos: daños o uso abusivo.
- Revelación de secretos, espionaje industrial y confidencialidad
- Delitos económicos, societarios o contra el mercado o los consumidores
- Delitos contra la propiedad intelectual e industrial
- Vulneración de la intimidad
- Sabotaje
- Uso indebido de equipos
- Amenazas, calumnias e injurias
- Cumplimiento de obligaciones y contratos
- Delitos contra la Propiedad Intelectual, en caso de Software Pirata o documentos con el debido registro de derechos de Autor.
- Robo de Propiedad Intelectual y Espionaje industrial (que aunque no se crea, sí existe en nuestro país).
- Blanqueo de Dinero, vía transferencia de fondos por Internet.
- Acoso Sexual (vía e-mail); Chantaje o amenazas (vía e-mail).
- Acceso no autorizado a propiedad intelectual.
- Corrupción.
- Destrucción de Información Confidencial.
- Fraude (en apuestas, compras, etc. Vía e-mail).

2.2 LEGISLACIÓN PERITO INFORMÁTICO FORENSE

Tenemos que ser conscientes de que la figura de Perito se conoce y se regula desde hace siglos, pero el concepto de delito informático, como tal, no se recogía ni se definía en el Código Penal hasta 1995 por lo que destacamos que se trata de una tipología de delitos recientes en los que el legislador está tratando de identificar y clasificar su naturaleza. Esto queda de manifiesto en las recientes actualizaciones de las diferentes normas con las que intentan adaptar la legislación a las necesidades de la sociedad. Y las futuras que aún tienen que venir sobre el tema.

El objeto y finalidad del dictamen de los Peritos sería la del asesoramiento de jueces, fiscales, abogados o particulares relativo a los temas de su interés. Destacando en nuestro caso, evidencias digitales o físicas que hayan sido producidas con motivo de la utilización de los mismos. Evidencias como archivos, datos, metadatos, registros, logs, los propios dispositivos… capaces de constituir evidencias o indicios digitales. Estas pruebas evidenciales serán destinadas para la investigación y formulación de las peritaciones judiciales. La Legislación española que desarrolla este apartado queda definida en la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil en su Sección 5: Del dictamen de Peritos, entre los artículos 335 a 352, donde se destacará los siguientes:

Artículo 335

> Objeto y finalidad del dictamen de peritos. Juramento o promesa de actuar con objetividad

> **1.** Cuando sean necesarios conocimientos científicos, artísticos, técnicos o prácticos para valorar hechos o circunstancias relevantes en el asunto o adquirir certeza sobre ellos, las partes podrán aportar al proceso el dictamen de peritos que posean los conocimientos correspondientes o solicitar, en los casos previstos en esta ley, que se emita dictamen por perito designado por el tribunal.

Artículo 340

Condiciones de los peritos

> **1.** Los peritos deberán poseer el título oficial que corresponda a la materia objeto del dictamen y a la naturaleza de éste. Si se tratare de materias que no estén comprendidas en títulos profesionales oficiales, habrán de ser nombrados entre personas entendidas en aquellas materias.

El Perito Informático es un experto que ha desarrollado sus competencias y habilidades en el campo de la ingeniería informática y electrónica. Como escribe el legislador se debe tratar de un profesional que debe disponer de certificaciones oficiales para el desarrollo y la realización de peritajes.

Un perito informático debe estar en posesión del título de ingeniería, como lo son de ingeniería de Telecomunicación o Informática y realizar los cursos y homologaciones necesarias para obtener la titulación. La legislación española se refiere a los Peritos en extensa normativa legal, apareciendo en la Ley de Enjuiciamiento Criminal de 1882 en el Capítulo II: Del cuerpo del Delito de los artículos 334 a 367 destacando

Artículo 334

> El Juez instructor ordenará recoger en los primeros momentos las armas, instrumentos o efectos de cualquiera clase que puedan tener relación con el delito y se hallen en el lugar en que éste se cometió, o en sus inmediaciones, o en poder del reo, o en otra parte conocida. El Secretario judicial extenderá diligencia expresiva del lugar, tiempo y ocasión en que se encontraren, describiéndolos minuciosamente para que se pueda formar idea cabal de los mismos y de las circunstancias de su hallazgo.

Artículo 335

> Siendo habida la persona o cosa objeto del delito, el Juez instructor describirá detalladamente su estado y circunstancias, y especialmente todas las que tuviesen relación con el hecho punible.

Artículo 336

> En los casos de los dos artículos anteriores ordenará también el Juez el reconocimiento por peritos, siempre que esté indicado para apreciar mejor

la relación con el delito, de los lugares, armas, instrumentos y efectos a que dichos artículos se refieren, haciéndose constar por diligencia el reconocimiento y el informe pericial.

Artículo 456

El Juez acordará el informe pericial cuando, para conocer o apreciar algún hecho o circunstancia importante en el sumario, fuesen necesarios o convenientes conocimientos científicos o artísticos.

Artículo 457

Los peritos pueden ser o no titulares.

Son peritos titulares los que tienen título oficial de una ciencia o arte cuyo ejercicio esté reglamentado por la Administración.

Son peritos no titulares los que, careciendo de título oficial, tienen, sin embargo, conocimientos o práctica especiales en alguna ciencia o arte.

Cabe destacar que, en la legislación vigente, en ninguno de sus artículos, se hace mención alguna sobre estar colegiado o no, ya que como queda bien definido en el articulado de la Ley lo único necesario es el título oficial o conocimientos o práctica especiales.

Artículo 458

El Juez se valdrá de peritos titulares con preferencia a los que no tuviesen título.

Articulo 335 (LEC).

Objeto y finalidad del dictamen de peritos. Juramento o promesa de actuar con objetividad.

1. Cuando sean necesarios conocimientos científicos, artísticos, técnicos o prácticos para valorar hechos o circunstancias relevantes en el asunto o adquirir certeza sobre ellos, las partes podrán aportar al proceso el dictamen de peritos que posean los conocimientos correspondientes o solicitar, en los casos previstos en esta ley, que se emita dictamen por perito designado por el tribunal.

Artículo 340 LEC. Condiciones de los peritos.

> 1. Los peritos deberán poseer el título oficial que corresponda a la materia objeto del dictamen y a la naturaleza de éste. Si se tratare de materias que no estén comprendidas en títulos profesionales oficiales, habrán de ser nombrados entre personas entendidas en aquellas materias.
>
> 2. Podrá asimismo solicitarse dictamen de Academias e instituciones culturales y científicas que se ocupen del estudio de las materias correspondientes al objeto de la pericia. También podrán emitir dictamen sobre cuestiones específicas las personas jurídicas legalmente habilitadas para ello.

Artículo 339 (LEC).

> Solicitud de designación de peritos por el tribunal y resolución judicial sobre dicha solicitud. Designación de peritos por el tribunal, sin instancia de parte.

Artículo 339.2 (LEC).

> El demandante o el demandado, aunque no se hallen en el caso del apartado anterior, también podrán solicitar en sus respectivos escritos iníciales que se proceda a la designación judicial de perito, si entienden conveniente o necesario para sus intereses la emisión de informe pericial. En tal caso, el tribunal procederá a la designación, siempre que considere pertinente y útil el dictamen pericial solicitado. Dicho dictamen será a costa de quien lo haya pedido, sin perjuicio de lo que pudiere acordarse en materia de costas.

2.2.1 La responsabilidad del Perito Judicial Informático en el proceso judicial

Una vez conocidos la definición de Perito Informático Judicial, sus competencias, aptitudes y demás datos relevantes, es también importante conocer los Delitos Graves y Leves que puede cometer en el ejercicio de sus funciones. Y para ello enunciaremos los artículos en los que se hace mención en el Código penal.

CAPÍTULO VI

Del falso testimonio

Artículo 458

1. El testigo que faltare a la verdad en su testimonio en causa judicial, será castigado con las penas de prisión de seis meses a dos años y multa de tres a seis meses.

2. Si el falso testimonio se diera en contra del reo en causa criminal por delito, las penas serán de prisión de uno a tres años y multa de seis a doce meses. Si a consecuencia del testimonio hubiera recaído sentencia condenatoria, se impondrán las penas superiores en grado.

3. Las mismas penas se impondrán si el falso testimonio tuviera lugar ante Tribunales Internacionales que, en virtud de Tratados debidamente ratificados conforme a la Constitución Española, ejerzan competencias derivadas de ella, o se realizara en España al declarar en virtud de comisión rogatoria remitida por un Tribunal extranjero.

Artículo 459

Las penas de los artículos precedentes se impondrán en su mitad superior a los peritos o intérpretes que faltaren a la verdad maliciosamente en su dictamen o traducción, los cuales serán, además, castigados con la pena de inhabilitación especial para profesión u oficio, empleo o cargo público, por tiempo de seis a doce años.

Artículo 460

Cuando el testigo, perito o intérprete, sin faltar sustancialmente a la verdad, la alterare con reticencias, inexactitudes o silenciando hechos o datos relevantes que le fueran conocidos, será castigado con la pena de multa de seis a doce meses y, en su caso, de suspensión de empleo o cargo público, profesión u oficio, de seis meses a tres años.

Artículo 461

1. El que presentare a sabiendas testigos falsos o peritos o intérpretes mendaces, será castigado con las mismas penas que para ellos se establecen en los artículos anteriores.

La LECr y la LEC establecen las funciones y condiciones que se debe cumplir para ejercer la función del Perito Judicial, esto hace que, en el ejercicio de sus funciones, el Juez ante la solución de parte, pueda sancionarlo, conforme a la legislación que compete al proceso judicial como son por ejemplo los artículos:

Artículo 292 (LEC) Obligatoriedad de comparecer a la audiencia. Multas

1. Los testigos y los peritos citados tendrán el deber de comparecer en el juicio o vista que finalmente se hubiese señalado. La infracción de este deber se sancionará por el Tribunal, previa audiencia por cinco días, con multa de ciento ochenta a seiscientos euros.

   Número 1 del artículo 292 redactado por el apartado ciento cincuenta y seis del artículo decimoquinto de la Ley 13/2009, de 3 de noviembre, de reforma de la legislación procesal para la implantación de la nueva Oficina judicial («B.O.E.» 4 noviembre). Vigencia: 4 mayo 2010

Artículo 463(LECr)

El perito, que sin alegar excusa fundada, deje de acudir al llamamiento del Juez o se niegue a prestar el informe, incurrirá en las responsabilidades señaladas para los testigos en el artículo 420.

2.2.2 La Responsabilidad administrativa

La responsabilidad administrativa se puede definir como la obligación económica que resulta por el incumplimiento a las normas del sistema. Estos hechos o sucesos que por acción u omisión se realizan ya sea a título de dolo o culpa, siempre que esta conducta, se encuentre tipificada como antijurídica dentro de la legislación.

Los ya reseñados artículos 457 de la LECr y el artículo 335 de la LEC entienden más a la forma del informe pericial y al contenido del mismo, por el cuál fue concebido. Siempre que el informe pericial haya sido anulado.

La nueva modificación del artículo 346 de la LEC hace referencia a la obligatoriedad del Perito Informático a la contestación en forma de dictamen;

Artículo 346

Emisión y ratificación del dictamen por el perito que el tribunal designe

El perito que el tribunal designe emitirá por escrito su dictamen, que hará llegar por medios electrónicos al tribunal en el plazo que se le haya señalado. De dicho dictamen se dará traslado por el secretario judicial a las partes por si consideran necesario que el perito concurra al juicio o a la vista a los efectos de que aporte las aclaraciones o explicaciones que sean oportunas. El tribunal podrá acordar, en todo caso, mediante providencia, que considera necesaria la presencia del perito en el juicio o la vista para comprender y valorar mejor el dictamen realizado.

> Artículo 346 redactado por el apartado cuarenta y cuatro del artículo único de la Ley 42/2015, de 5 de octubre, de reforma de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil («B.O.E.» 6 octubre).Vigencia: 7 octubre 2015

Esto hace que en los casos de incumplimiento de este deber por parte del perito se pueden establecer sanciones por el Juez, como pueden ser la suspensión o la exclusión definitiva (en los artículos 456 de CP o el art. 292 de LEC)

En el ejercicio propio de su cargo en su función Pública-Judicial, el Perito Judicial, a parte de los derechos que le asisten, tiene una serie de límites en su actuación, y que las ejecuciones de tales acciones puedan constituir abuso de autoridad, regulado por el legislador en el Código Penal en varios artículos, destacando estos:

CAPÍTULO VI

Del falso testimonio

Artículo 460

> Cuando el testigo, perito o intérprete, sin faltar sustancialmente a la verdad, la alterare con reticencias, inexactitudes o silenciando hechos o datos relevantes que le fueran conocidos, será castigado con la pena de multa de seis a doce meses y, en su caso, de suspensión de empleo o cargo público, profesión u oficio, de seis meses a tres años.

CAPÍTULO III

De la desobediencia y denegación de auxilio

Artículo 410

> 1. Las autoridades o funcionarios públicos que se negaren abiertamente a dar el debido cumplimiento a resoluciones judiciales, decisiones u órdenes de la autoridad superior dictadas dentro del ámbito de su respectiva competencia y revestidas de las formalidades legales, incurrirán en la pena de multa de tres a doce meses e inhabilitación especial para empleo o cargo público por tiempo de seis meses a dos años.

CAPÍTULO III

Del encubrimiento

Artículo 451

> Será castigado con la pena de prisión de seis meses a tres años el que, con conocimiento de la comisión de un delito y sin haber intervenido en el mismo como autor o cómplice, interviniere con posterioridad a su ejecución, de alguno de los modos siguientes:

> 3.º Ayudando a los presuntos responsables de un delito a eludir la investigación de la autoridad o de sus agentes, o a sustraerse a su busca o captura, siempre que concurra alguna de las circunstancias siguientes:
>
> b) Que el favorecedor haya obrado con abuso de funciones públicas. En este caso se impondrá, además de la pena de privación de libertad, la de inhabilitación especial para empleo o cargo público por tiempo de dos a cuatro años si el delito encubierto fuere menos grave, y la de inhabilitación absoluta por tiempo de seis a doce años si aquél fuera grave.

En los artículos reseñados es el Perito Informático Judicial el Sujeto activo, (que es aquel que puede realizar el tipo delictivo), y se trata de sujeto pasivo del delito (que es el titular del bien jurídico protegido) o bien el Estado, ya que compromete la responsabilidad del Estado, o bien el particular, sobre el que se produce el delito.

Otro tipo de actuaciones de los Peritos Judiciales que deben realizar o infligirán en una conducta tipificada por el legislador, serían las siguientes:

Artículo 463

> El perito, que sin alegar excusa fundada, deje de acudir al llamamiento del Juez o se niegue a prestar el informe, incurrirá en las responsabilidades señaladas para los testigos en el artículo 420.

Artículo 420

> El que sin estar impedido no concurriere al primer llamamiento judicial, excepto las personas mencionadas en el artículo 412, o se resistiere a declarar lo que supiese acerca de los hechos sobre que fuere preguntado, a no estar comprendido en las exenciones de los artículos anteriores, incurrirá en la multa de 200 a 5.000 euros, y si persistiere en su resistencia será conducido en el primer caso a la presencia del Juez instructor por los agentes de la autoridad, y perseguido por el delito de obstrucción a la justicia tipificado en el artículo 463.1 del Código Penal, y en el segundo caso será también perseguido por el de desobediencia grave a la autoridad.*Párrafo 1.º del artículo 420 redactado por el apartado 2 del artículo cuarto de la Ley 38/2002, de 24 de octubre, de reforma parcial de la Ley de Enjuiciamiento Criminal, sobre procedimiento para el enjuiciamiento rápido e inmediato de determinados delitos y faltas, y de modificación del procedimiento abreviado («B.O.E.» 28 octubre).Vigencia: 28 abril 2003*

Artículo 464

> No podrán prestar informe pericial acerca del delito, cualquiera que sea la persona ofendida, los que según el artículo 416 no están obligados a declarar como testigos.
>
> El perito que, hallándose comprendido en alguno de los casos de dicho artículo, preste el informe sin poner antes esa circunstancia en conocimiento del Juez que le hubiese nombrado incurrirá en la multa de 200 a 5.000 euros, a no ser que el hecho diere lugar a responsabilidad criminal.*Párrafo 2.º del artículo 464 redactado por el apartado 4 del artículo cuarto de la Ley 38/2002, de 24 de octubre, de reforma parcial de la Ley de Enjuiciamiento Criminal, sobre procedimiento para el enjuiciamiento rápido e inmediato de determinados delitos y faltas, y de modificación del procedimiento abreviado («B.O.E.» 28 octubre).Vigencia: 28 abril 2003*

Artículo 465

> Los que presten informe como peritos en virtud de orden judicial tendrán derecho a reclamar los honorarios e indemnizaciones que sean justos, si no tuvieren en concepto de tales peritos, retribución fija satisfecha por el Estado, por la Provincia o por el Municipio.

Todo este compendio de responsabilidades nos lleva a la necesidad certera de que, en el ejercicio de sus funciones, un perito informático debe contratar un seguro de responsabilidad civil en el que consten las principales posibles indemnizaciones civiles a las que un perito en el ejercicio de su actividad pueda ser condenado en un tribunal, estos conjuntos de cuantías se encuentran desarrolladas y actualizadas en los diferentes portales del consejo de Peritos Judiciales.

Significar tras esta exposición la importancia manifiesta del artículo 458 en este proyecto que nos abarca, ya que marca el camino a seguir en las actuaciones periciales. La jurisprudencia y la legislación amparan que siempre que haya un perito titular al que se le pueda encargar dicha peritación, siempre tendrá preferencia ante los que no lo son. Esta afirmación es apoyada por la Sentencia 2047/2015 dictaminada el 19 mayo de 2015 por el Tribunal Supremo de España.

Esta sentencia es resultado de la impugnación de la autenticidad de conversaciones mediante la aplicación WhatsApp, la cual se encuentra muy extendida y con una penetración del 70% según últimos estudios realizados, siendo un 98% de los teléfonos inteligentes; mal denominados por parte de la sociedad, si se me permite la licencia. En dicho juicio se ponía en duda la autenticidad de las conversaciones que fueron aportadas a la causa, mediante archivos de impresión por una de las partes intentando probar unos hechos. En este caso se indica que tendrá que ser indispensable la realización de una peritación que pueda aclarar e identificar origen, fecha, hora, identidad de los interlocutores y demás datos necesarios para verificar la integridad de su contenido y su inequívoca naturaleza. A continuación, los artículos enumerados para la redacción de este párrafo:

- http://www.abc.es/tecnologia/moviles-aplicaciones/20150225/whatsapp-espana-cuarto-pais-mundo-cuota-mercado-201502241120.html
- http://www.elmundo.es/economia/2015/07/20/55ad0053ca474131318b4587.html
- http://politica.elpais.com/politica/2015/02/13/actualidad/1423848194_845485.html

En el escrito del Tribunal se reseña que una conversación mantenida por dos personas en cualquiera de las múltiples aplicaciones de las redes sociales, así como en cualquier chat de cualquier naturaleza para que pueda ser considerada como prueba válida debe ser peritada por un perito informático en un dictamen pericial informático. La sentencia es clara en ese punto, destacando que no puede ser presentados las meras impresiones de pantalla de la conversación mantenida, ya que estos pueden ser manipulados, simulados o imprecisos, debe ser un perito informático el que verifique esa conversación, realizando informes periciales con el objetivo de verificar la integridad de su contenido e identificarlo inequívocamente.

Esta Sentencia del Tribunal Supremo ratifica la obligatoriedad de la realización de un informe pericial que tiene que ser realizado y firmado por un perito informático que autentifique los datos transmitidos en cualquier tipo de comunicación en las plataformas de mensajes y transmisión de archivos.

2.3 NORMATIVA APLICABLE

Como observamos, un Perito Tecnológico debe tratar y estudiar minuciosamente una gran cantidad de legislación para la realización de sus informes periciales para encuadrarlos en un contexto de seguridad judicial, entre la numerosa Legislación Actual se enumerará la de utilización más normalizada para el desarrollo de sus funciones:

- La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (LOPD).

  Esta Ley Traspone al Ordenamiento Jurídico Español la Directiva Europea 95/46 CE de 24 de octubre de 1995, relativa a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos.

- El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, Desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal.

- La Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE).

- Ley 32/2003, General de Telecomunicaciones. (Arts. 33-35).

- Ley 59/2003, de 19 de diciembre, de Firma Electrónica

- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual (LPI), regularizando, aclarando y armonizando las disposiciones vigentes en la materia.

- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. (BOE 25 de 29-01-2010 páginas 8089 a 8138)

- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica. (BOE 25 de 29-01-2010 páginas 8139 a 8156).

- Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

- Directiva 2009/136/CE/ del Parlamento Europeo y del Consejo, de 25 de noviembre.[Documento disponible en PDF (Directiva 2009/136/CE/)].

  La Directiva 2009/136/CE modifica la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) nº 2006/2004 sobre la cooperación en materia de protección de los consumidores.

- Directiva 2009/140/CE del Parlamento Europeo y del Consejo, de 25 de noviembre. [Documento disponible en PDF (Directiva 2009/140/CE)].

  La Directiva 2009/140/CE modifica la Directiva 2002/21/CE relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/19/CE relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión, y la Directiva 2002/20/CE relativa a la autorización de redes y servicios de comunicaciones electrónicas.

- Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de cámaras o videocámaras.

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

- Ley 23/1992, de 30 de julio, de Seguridad Privada.

- Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el reglamento de seguridad privada.

- Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las fuerzas y cuerpos de seguridad en lugares públicos.

- Ley Orgánica 1/1992 de 21 de febrero sobre protección civil de la seguridad ciudadana.

- Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y a la propia imagen.

- Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre privacidad y las comunicaciones electrónicas).

2.4 LEGISLACIÓN EN EL DESARROLLO DE LA PERITACION

Destacar que debido a la complejidad de las sentencias dada la creciente y reciente incorporación de este tipo de delitos, se está produciendo numerosa Jurisprudencia que debe ser estudiada y revisada. Como ejemplo reseño una sentencia en el que se destaca que el derecho a la intimidad en la red prevalece sobre la supuesta comisión, de delitos leves, dando relevancia a que la IP es individualizadora y por lo tanto se trata de un derecho a la intimidad por el cual, si se quisiera conocer el usuario de esa IP se consideraría vulnerado el derecho a la intimidad y es un bien a proteger que requiere ser defendido. Nota: Sentencia basada sobre direcciones IP e intercambios de archivos P2P

ROJ: **SAN 3907/2011**– ECLI:**ES:AN:2011:3907**

Parte de la sentencia:

"Todo ello, sin embargo, no puede servir para justificar, como pretende la parte recurrente que se lleve a cabo una aplicación de la LOPD que sea claramente lesiva de los derechos en materia de protección de datos. La protección de los derechos de propiedad intelectual, que está en la base de lo pretendido por la entidad recurrente, merece todo el respeto de esta Sala, pero no puede hacerse sobre la base de violar derechos, que también merecen protección, como son los derivados de la protección de datos (entendida en un conceptomucho más amplio que el simple derecho a la intimidad). No puede dejar de señalarse que si bien lo que solicitó la parte recurrente fue una aplicación puntual del artículo 5.5 de la LOPD , en su escrito de demanda se han vertido otras muchas consideraciones que no tienen que ver propiamente con la materia de protección de datos sino que se han desbordado sus pretensiones olvidando el objeto inicial de su reclamación entendiendo esta Sala que la respuesta ofrecida por la Agencia de Protección de Datos es plenamente acomodada al ordenamiento jurídico."

En el estudio de la legislación que es imprescindible para la realización en el ejercicio de la función de Perito Informático debemos tener en cuenta, cuándo y de qué manera se puede acceder a la información y cuando se debe realizar peticiones al requirente de la peritación, ya sea un Juez, Magistrado o particular. Como ha quedado claro en numerosa jurisprudencia, el objeto a investigar o el objeto a descubrir o el delito a investigar para las peticiones realizadas, siempre debe ser mayor que el derecho que en la petición se pide interrumpir.

Uno de los llamados derechos fundamentales que debemos tener muy presente en cada peritación es la Defensa de la Intimidad, que podría producir una impugnación de la misma.

Artículo 18 de la Constitución Española, 1978

> 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
>
> 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
>
> 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
>
> 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

Artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea (2000/C364/01)

Artículo 8 Resolución de 5 de abril de 1999, de la Secretaría General Técnica, por la que se hacen públicos los textos refundidos del Convenio para la protección de los derechos y de las libertades fundamentales, hecho en Roma el 4 de noviembre de 1950; el protocolo adicional al Convenio, hecho en París el 20 de marzo de 1952, y el protocolo número 6, relativo a la abolición de la pena de muerte, hecho en Estrasburgo el 28 de abril de 1983.

Y una Ley que desarrolla este derecho, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Tenemos que recordar que según nos comenta en un descanso del curso de peritaciones judiciales el Excmo. Presidente del Tribunal Superior de Justicia de Madrid, D. Francisco J. Vieira Morante, las directivas son pautas para que el ordenamiento jurídico de

cada país realice la transposición de las directivas europeas a sus leyes, para la aplicación de la directiva, normalmente tiene un plazo para esa transposición. Pero a diferencia de estas mismas, los Convenios Internacionales de Comités de Ministros de Consejo Europa o Consejo Internacional, como así los Tratados Internacionales son de cumplimiento una vez realizada la firma y la adscripción a la misma por el país, es de obligado cumplimiento por el País firmante, pudiendo ser denunciado ante el consejo de Europa de Estrasburgo o ante los consejos pertinentes, el incumplimiento de los mismos.

La necesidad de acometer el elevado número de delitos que se están produciendo en la actualidad mediante el uso de la tecnología hizo que el 5 de octubre de 2015 el legislador realizara la modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación mediante la Ley Orgánica 13/2015. En esta Ley se tratan numerosos aspectos de reciente aparición y enunciaré los artículos que están más dirigidos para la realización de la función de Perito Informático:

En primer término, estudiaremos un tema de difícil tratamiento, que en el ejercicio de nuestro trabajo ocurre con más frecuencia de lo esperado, es el conocido como Descubrimiento Casual.

El Descubrimiento Casual lo definimos como la aparición de hechos delictivos nuevos o distintos a los investigados en el curso de una peritación, que en su origen no estaban definidos en la resolución judicial, que mediante oficio o petición me habilita para la búsqueda de estos hechos. Esta diligencia o petición me habilita para la obtención de información, y ante la investigación de estos hechos se descubre por casualidad otros distintos, así como la posible aparición de nuevos sujetos implicados, y observando que el hallazgo no corresponde con la finalidad originaria del mandamiento. Los descubrimientos casuales como a priori parece obvio no podrán ser utilizados como fuente de prueba en un proceso diferente del que se obtienen. Como bien hablan en la LeCrim en su

Artículo 17

> ***1.*** *Cada delito dará lugar a la formación de una única causa. No obstante, los delitos conexos serán investigados y enjuiciados en la misma causa cuando la investigación y la prueba en conjunto de los hechos resulten convenientes para su esclarecimiento y para la determinación de las responsabilidades procedentes salvo que suponga excesiva complejidad o dilación para el proceso.*

Los descubrimientos casuales serán, si así lo estima oportuno el órgano jurídico, una notitia criminis, que es el nombre genérico con el que se han reunido los distintos medios por los cuales puede iniciarse la actividad de la justicia penal, mediante la promoción del proceso, dando así inicio la instrucción independiente para la investigación del nuevo hecho delictivo. La Sentencia del Tribunal Supremo de 11 octubre de 1994 manifiesta que se debe iniciar la investigación de la notitia criminis descubierta de manera casual en una intervención iniciada con otro fin. Aunque para ello se precisará la autorización judicial específica. Así la fiscalía siguiendo la jurisprudencia y legislación relativa a delitos conexos, actuará por la necesidad de otorgar una orden judicial ampliatoria.

Realizada la definición y sus implicaciones judiciales, debemos tener claro cómo actuar ante esos casos, la denuncia de los hechos en el ejercicio de nuestras funciones es una obligación como queda definido en la Lecrim en su

LIBRO II

TÍTULO PRIMERO

De la denuncia

Artículo 259

El que presenciare la perpetración de cualquier delito público está obligado a ponerlo inmediatamente en conocimiento del Juez de instrucción, de paz, comarcal o municipal, o funcionario fiscal más próximo al sitio en que se hallare, bajo la multa de 25 a 250 pesetas. *Artículo 259 redactado por Ley 14 abril 1955 («B.O.E.» 15 abril), por la que se modifica la base económica de algunos artículos de la Ley de Enjuiciamiento Criminal.*

Artículo 260

La obligación establecida en el artículo anterior no comprende a los impúberes ni a los que no gozaren del pleno uso de su razón.

Artículo 261

Tampoco estarán obligados a denunciar:

1.º El cónyuge del delincuente no separado legalmente o de hecho o la persona que conviva con él en análoga relación de afectividad.

2.º Los ascendientes y descendientes del delincuente y sus parientes colaterales hasta el segundo grado inclusive.

Artículo 261 redactado por el apartado cuatro de la disposición final primera de la Ley 4/2015, de 27 de abril, del Estatuto de la víctima del delito («B.O.E.» 28 abril). Vigencia: 28 octubre 2015

Artículo 262

Los que por razón de sus cargos, profesiones u oficios tuvieren noticia de algún delito público, estarán obligados a denunciarlo inmediatamente al Ministerio Fiscal, al Tribunal competente, al Juez de instrucción y, en su defecto, al municipal o al funcionario de policía más próximo al sitio, si se tratare de un delito flagrante.Los que no cumpliesen esta obligación incurrirán en la multa señalada en el artículo 259, que se impondrá disciplinariamente.Si el que hubiese incurrido en la omisión fuere empleado público, se pondrán además en conocimiento de su superior inmediato para los efectos a que hubiere lugar en el orden administrativo.Lo dispuesto en este artículo se

entiende cuando la omisión no produjere responsabilidad con arreglo a las Leyes.

En el caso del que realice el Descubrimiento Casual sea un Policía en su actuación como Perito Judicial nos tendremos que ir al;

Artículo 292

Los funcionarios de Policía judicial extenderán, bien en papel sellado, bien en papel común, un atestado de las diligencias que practiquen, en el cual especificarán con la mayor exactitud los hechos por ellos averiguados, insertando las declaraciones e informes recibidos y anotando todas las circunstancias que hubiesen observado y pudiesen ser prueba o indicio del delito. La Policía Judicial remitirá con el atestado un informe dando cuenta de las detenciones anteriores y de la existencia de requisitorias para su llamamiento y busca cuando así conste en sus bases de datos.*Párrafo 2.º del artículo 292 introducido por la letra c) del número 2 de la disposición final primera de la L.O. 15/2003, de 25 de noviembre, por la que se modifica la L.O. 10/1995, de 23 de noviembre, del Código Penal («B.O.E.» 26 noviembre). Vigencia: 27 noviembre 2003*

Artículo 297

Los atestados que redactaren y las manifestaciones que hicieren los funcionarios de Policía judicial, a consecuencia de las averiguaciones que hubiesen practicado, se considerarán denuncias para los efectos legales.

Artículo 588 bis i

Utilización de la información obtenida en un procedimiento distinto y descubrimientos casuales

El uso de las informaciones obtenidas en un procedimiento distinto y los descubrimientos casuales se regularán con arreglo a lo dispuesto en el artículo 579 bis.

CAPÍTULO III

De la detención y apertura de la correspondencia escrita y telegráfica»

Artículo 579 bis

Utilización de la información obtenida en un procedimiento distinto y descubrimientos casuales

3. La continuación de esta medida para la investigación del delito casualmente descubierto requiere autorización del juez competente, para la cual, éste

> comprobará la diligencia de la actuación, evaluando el marco en el que se produjo el hallazgo casual y la imposibilidad de haber solicitado la medida que lo incluyera en su momento. Asimismo, se informará si las diligencias continúan declaradas secretas, a los efectos de que tal declaración sea respetada en el otro proceso penal, comunicando el momento en el que dicho secreto se alce.»

Siguiendo con el articulado de la modificación de la Lecrim destacando los puntos que nos afectan a la hora de realizar las peritaciones:

CAPÍTULO IV

> 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

En su primer artículo, en el

Artículo 588 bis a

> *Principios rectores*
>
> *Destacamos el apartado 5*
>
> **5.** Las medidas de investigación reguladas en este capítulo solo se reputarán proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho.

Recordando que en el ejercicio de nuestras funciones debemos siempre ponderar que el interés público y de terceros deberá acreditar la gravedad de los hechos investigados si al realizarlo se pusiera en peligro o supusiera la eliminación de un derecho mayor. Es importante reseñar la relevancia del resultado perseguido con la restricción del derecho que pedimos realizar.

Una vez realizada la toma de información debemos tener en cuenta cómo proceder con la información y registros generados, como marca el siguiente artículo:

Artículo 588 bis k

Destrucción de registros

1. Una vez que se ponga término al procedimiento mediante resolución firme, se ordenará el borrado y eliminación de los registros originales que puedan constar en los sistemas electrónicos e informáticos utilizados en la ejecución de la medida. Se conservará una copia bajo custodia del secretario judicial.

2. Se acordará la destrucción de las copias conservadas cuando hayan transcurrido cinco años desde que la pena se haya ejecutado o cuando el delito o la pena hayan prescrito o se haya decretado el sobreseimiento libre o haya recaído sentencia absolutoria firme respecto del investigado, siempre que no fuera precisa su conservación a juicio del Tribunal.

3. Los tribunales dictarán las órdenes oportunas a la Policía Judicial para que lleve a efecto la destrucción contemplada en los anteriores apartados.»»

CAPÍTULO V

La interceptación de las comunicaciones telefónicas y telemáticas

Sección 3

Acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad

Artículo 588 ter k

Identificación mediante número IP

Cuando en el ejercicio de las funciones de prevención y descubrimiento de los delitos cometidos en internet, los agentes de la Policía Judicial tuvieran acceso a una dirección IP que estuviera siendo utilizada para la comisión algún delito y no constara la identificación y localización del equipo o del dispositivo de conectividad correspondiente ni los datos de identificación personal del usuario, solicitarán del juez de instrucción que requiera de los agentes sujetos al deber de colaboración según el artículo 588 ter e, la cesión de los datos que permitan la identificación y localización del terminal o del dispositivo de conectividad y la identificación del sospechoso.

Artículo 588 ter l

Identificación de los terminales mediante captación de códigos de identificación del aparato o de sus componentes

1. Siempre que en el marco de una investigación no hubiera sido posible obtener un determinado número de abonado y este resulte indispensable a los

fines de la investigación, los agentes de Policía Judicial podrán valerse de artificios técnicos que permitan acceder al conocimiento de los códigos de identificación o etiquetas técnicas del aparato de telecomunicación o de alguno de sus componentes, tales como la numeración IMSI o IMEI y, en general, de cualquier medio técnico que, de acuerdo con el estado de la tecnología, sea apto para identificar el equipo de comunicación utilizado o la tarjeta utilizada para acceder a la red de telecomunicaciones.

2. Una vez obtenidos los códigos que permiten la identificación del aparato o de alguno de sus componentes, los agentes de la Policía Judicial podrán solicitar del juez competente la intervención de las comunicaciones en los términos establecidos en el artículo 588 ter d. La solicitud habrá de poner en conocimiento del órgano jurisdiccional la utilización de los artificios a que se refiere el apartado anterior. El tribunal dictará resolución motivada concediendo o denegando la solicitud de intervención en el plazo establecido en el artículo 588 bis c.

Artículo 588 ter m

Identificación de titulares o terminales o dispositivos de conectividad

Cuando, en el ejercicio de sus funciones, el Ministerio Fiscal o la Policía Judicial necesiten conocer la titularidad de un número de teléfono o de cualquier otro medio de comunicación, o, en sentido inverso, precisen el número de teléfono o los datos identificativos de cualquier medio de comunicación, podrán dirigirse directamente a los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, quienes estarán obligados a cumplir el requerimiento, bajo apercibimiento de incurrir en el delito de desobediencia.

En lo siguiente encontraremos los siguientes artículos que son en el desarrollo de nuestra actividad, una vez iniciada la peritación para la toma de información de la misma:

CAPÍTULO VIII

Registro de dispositivos de almacenamiento masivo de información

Artículo 588 sexies a

Necesidad de motivación individualizada

1. Cuando con ocasión de la práctica de un registro domiciliario sea previsible la aprehensión de ordenadores, instrumentos de comunicación telefónica o telemática o dispositivos de almacenamiento masivo de información digital o el acceso a repositorios telemáticos de datos, la resolución del juez de instrucción habrá de extender su razonamiento a la justificación, en su caso, de las razones que legitiman el acceso de los agentes facultados a la información contenida en tales dispositivos.

2. La simple incautación de cualquiera de los dispositivos a los que se refiere el apartado anterior, practicada durante el transcurso de la diligencia de registro domiciliario, no legitima el acceso a su contenido, sin perjuicio de que dicho acceso pueda ser autorizado ulteriormente por el juez competente.

Artículo 588 sexies b

Acceso a la información de dispositivos electrónicos incautados fuera del domicilio del investigado

La exigencia prevista en el apartado 1 del artículo anterior será también aplicable a aquellos casos en los que los ordenadores, instrumentos de comunicación o dispositivos de almacenamiento masivo de datos, o el acceso a repositorios telemáticos de datos, sean aprehendidos con independencia de un registro domiciliario. En tales casos, los agentes pondrán en conocimiento del juez la incautación de tales efectos. Si éste considera indispensable el acceso a la información albergada en su contenido, otorgará la correspondiente autorización.

Artículo 588 sexies c

Autorización judicial

1. La resolución del juez de instrucción mediante la que se autorice el acceso a la información contenida en los dispositivos a que se refiere la presente sección, fijará los términos y el alcance del registro y podrá autorizar la realización de copias de los datos informáticos. Fijará también las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación para hacer posible, en su caso, la práctica de un dictamen pericial.

2. Salvo que constituyan el objeto o instrumento del delito o existan otras razones que lo justifiquen, se evitará la incautación de los soportes físicos que contengan los datos o archivos informáticos, cuando ello pueda causar un grave perjuicio a su titular o propietario y sea posible la obtención de una copia de ellos en condiciones que garanticen la autenticidad e integridad de los datos.

3. Cuando quienes lleven a cabo el registro o tengan acceso al sistema de información o a una parte del mismo conforme a lo dispuesto en este capítulo, tengan razones fundadas para considerar que los datos buscados están almacenados en otro sistema informático o en una parte de él, podrán ampliar el registro, siempre que los datos sean lícitamente accesibles por medio del sistema inicial o estén disponibles para este. Esta ampliación del registro deberá ser autorizada por el juez, salvo que ya lo hubiera sido en la autorización inicial. En caso de urgencia, la Policía Judicial o el fiscal podrán

llevarlo a cabo, informando al juez inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, de la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la interceptación.

4. En los casos de urgencia en que se aprecie un interés constitucional legítimo que haga imprescindible la medida prevista en los apartados anteriores de este artículo, la Policía Judicial podrá llevar a cabo el examen directo de los datos contenidos en el dispositivo incautado, comunicándolo inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, por escrito motivado al juez competente, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de 72 horas desde que fue ordenada la medida.

5. Las autoridades y 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, siempre que de ello no derive una carga desproporcionada para el afectado, bajo apercibimiento de incurrir en delito de desobediencia.

Esta disposición no será aplicable al investigado o encausado, a las personas que están 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.

2.5 COMPENDIO

Una vez expuesta la legislación vigente, queda de manifiesto, que para el ejercicio como Perito Informático es necesario la titulación universitaria, principalmente ingeniero superior licenciado o ingeniero técnico. En su defecto y ante la ausencia de estos, es indispensable la obtención de una certificación homologada por una Universidad habilitada y homologada o un Instituto de Certificaciones reglado, aceptado y reconocido. Estos serán los encargados de acreditar las capacidades profesionales del interesado, avalando los conocimientos adquiridos.

El desarrollo de la función de Perito Informático Judicial como "ad hoc" de la Administración de Justicia o de Particulares y empresas, está tomando una relevancia importante en nuestros días, siendo una parte indispensable en casi cualquier decisión judicial en la que se requieren presentar pruebas de las conocidas como tecnológicas. Esto se debe a la nueva reforma de la Ley de Enjuiciamiento Criminal que ha sido introducida en el Boletín Oficial del Estado número 239, de 6 de octubre, donde se publicó la 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. Cuya entrada en vigor se producirá el próximo día 6 de diciembre de 2015. Estas medidas ponen de manifiesto la necesidad de contar con expertos o especialistas en nuevas tecnologías y con amplios conocimientos científicos como medio para la realización de peritaciones que sirvan de pruebas para el esclarecimiento de las actuaciones procesales o hechos particulares de interés.

3. PROTOCOLO ACTUACIÓN EN PERITACIONES INFORMÁTICAS

3.1 LA PERITACIÓN

3.1.1 ESTIMACIÓN DE PERICIA

El Perito Informático antes de iniciar cualquier peritación debe realizar una estimación de si procede el desarrollo de la pericia o por el contrario debe proceder a la desestimación de la misma en el momento del requerimiento. Es importante elaborar un estudio inicial de la petición que se ha recibido como base principal para la confección de la peritación. Como inicio, se evaluará la fuente de la que se recibe el encargo, el requirente. A priori distinguiremos dos categorías; la fuente particular y la remitida por la administración. Normalmente las peticiones de peritaciones de la administración son mucho más abiertas a la investigación, suelen ser las que se realizan por intervenciones policiales o denuncias en la propia administración de justicia. Por lo que suelen tener un carácter más enfocado al esclarecimiento de hechos, en estos casos la peritación tenga un carácter más dirigido al desarrollo de una conclusión, y se preocupa menos al procedimiento realizado, siempre dentro de los parámetros que permite el legislador. Es en el ámbito particular donde el abanico de opciones, es mucho más amplio, esto es debido a que puede ser solicitado desde auténticos expertos en este campo de actuación como podrían ser empresas muy especializadas, así como verdaderos desconocedores de la materia.

Es esta primera valoración de la petición formalizada, la que debe ser estudiada con mucho detenimiento. Lo primero que se debe valorar es si el actual marco legislativo posibilita la peritación, si realmente disponemos de los medios que nos posibiliten la realización del peritaje, lo que suele ser más difícil de encuadrar, si nuestras habilidades pueden desarrollar este tipo de trabajo, ya que un contra-peritaje realizado por un experto puede realizar una impugnación de nuestro trabajo con las responsabilidades que eso puede conllevar. Una vez elaborado el estudio se procederá a dar contestación por escrito al requirente.

3.1.2 PREPARACIÓN

La preparación de la peritación debe tener como objetivo principal la determinación de las medidas a adoptar tanto legales como técnicas para el desarrollo de la pericia. El resultado de la misma vendrá marcado por las primeras valoraciones de lo requerido. Por lo que es imprescindible la realización y diferenciación de las partes iniciales con el desarrollo y el diseño de los informes técnicos para establecer los parámetros de estudio.

La segunda actuación que se tiene que realizar es; la de la formalización de la recepción del encargo. Recogiendo el autor de la petición, su cargo o puesto como encargado o función o su simple identificación, la actuación que se solicita del perito de manera

detallada, qué dispositivos tendrá acceso, como la definición más amplia posible de los mismos, las infraestructuras, las circunstancias… Como punto más importante es conocer la información a la que se va a poner acceder para realizar la petición.

En el caso de la administración de justicia, además de lo arriba expuesto, es imprescindible conocer el número de juzgado, diligencia, atestado, exhorto o Juicio… en definitiva el número de referencia, para la individualización del caso, debido a la gran cantidad de procesos abiertos por cada juzgado. Significar que antes de la aceptación debemos leer y conocer bien el caso, por si se incurriera en un conflicto de intereses o saliera de nuestras competencias, o si ni siquiera requiera una peritación debido a que se necesitan una serie de trámites anteriores. Realizando una especial mención a la provisión de fondos que hay que realizar en los casos del ámbito civil, en los que se dispone de tres días laborables para la presentación de los registros. Una vez estudiado cada una de las posibilidades y procedimientos se podría empezar a trabajar en la peritación.

3.1.3 CONSIDERACIONES GENERALES

En esta parte del trabajo debemos tener en cuenta qué es lo que realmente buscamos para la elaboración de un peritaje, se trata del concepto de nueva aparición de “Evidencia Digital”, o la también conocida como “Prueba Electrónica”, más acertada ya que es palabra y concepto propio de derecho; que es la actividad necesaria que implica demostrar la verdad de un hecho, su existencia o contenido según los medios establecidos por la ley. La numerosa jurisprudencia producida, por las cuantiosas sentencias dictadas, ha generado un gran número de terminología y status quo normativo y de facto.

3.1.4 PRUEBA ELECTRÓNICA

3.1.4.1 DEFINICIÓN

La prueba electrónica debe ser definida para entender qué es y cómo forma parte de los juicios, para eso debemos entender el concepto de prueba. La Ley de Enjuiciamiento Civil 1/2000, en el artículo 299 Medios de Prueba, nos define los medios de prueba como los medios de que se podrá hacer uso en juicio, enumerando las llamadas clásicas como documentos, interrogatorio, dictamen de peritos… en el apartado 1, en el apartado 2 del mismo artículo enumeran los medios digitales y el apartado 3 dejan la puerta abierta para “**3.** Cuando por cualquier otro medio no expresamente previsto en los apartados anteriores de este artículo pudiera obtenerse certeza sobre hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias”, entendiendo que debe ser claramente justificada.

Resaltar en esta sentencia de la Audiencia y en este artículo como concepto de la prueba y todos los hechos que pueden ser definidos como tal:

Sentencia de la Audiencia Provincial de Barcelona, sección 13, de 2 de mayo de 2007: "*Con la L.E.C., se regulan un conjunto de "medios de prueba" (aunque en realidad son "fuentes" de prueba) cuya característica común es la capacidad para retener palabras y/o imágenes que se desarrollaron en un momento determinado, con posibilidad de reproducirlas después, facilitándose la oralidad, la inmediación y la concentración; pero el problema que planteaban era el de su utilización, cuando no estaban previstos expresamente, en el proceso: es decir, el cauce a través del cual introducirlos en el proceso, máxime cuando el art. 24.2 C.E . constitucionalizaba el derecho –sin limitación "objetiva", salvo la licitud, pertinencia- a utilizar los medios de prueba pertinentes para la defensa y el art. 3.1 C.C. imponía la interpretación conforme a la realidad social. En un principio se acogió la tesis de la analogía con la prueba documental, el reconocimiento judicial o la pericial, que de alguna forma se "mantiene" pues la analogía con la documental se alude en la Exposición de Motivos, singularmente los "instrumentos" del art. 384 (incluso algún precepto, expresamente los regula como documentos, como el art. 812 L.E.C ., entre los que pueden acceder al monitorio; o respecto de la aportación, art. 265 y ss. o las posibilidades de exhibición, arts. 329 a 334), con la pericial, como complementaria respecto de la autenticidad (art. 382 L.E.C .) o con el reconocimiento judicial (art. 382 , como el "video").*"

Destacar que las fuentes de prueba como se define en numerosos documentos jurídicos, como es en el artículo Fuentes de prueba de Claudio Menesses; “son el principio, fundamento o punto de origen de la información sobre hechos. Ellas, además, se sitúan fuera del juicio y con anterioridad a él; emergen y se forman extraprocesalmente; están compuestas por personas y cosas”. Las fuentes de la prueba, por tanto, son los hechos que han ocurrido en la realidad, son los hechos que se producen exista o no el proceso que se investiga.

Las fuentes de prueba a las que nos referimos con las pruebas electrónicas se encuentran definidas por tanto en el artículo 299.2 de la Ley 1/2000 la LEC, ya que se trata de una adaptación de los documentos públicos o privados con soportes electrónicos. Significando que es la prueba electrónica la que intenta probar que ese hecho que es real y verídico es el ocurrido.

En nuestro trabajo debemos trabajar con la conocida como Prueba electrónica, esta tiene un uso extendido en la actualidad en nuestro campo, y también se encuentra mencionada en numerosa Jurisprudencia, entre ella resaltamos, la Audiencia Provincial de Madrid en el Nº de Recurso: 1505/2015 con el Nº de Resolución:696/2015 en el cual se ponen en duda los “criterios para la admisibilidad de la prueba electrónica que se mencionan en el recurso” haciendo una muy aclarativa valoración de la prueba electrónica en este caso, que como es obvio comentar, sirven de jurisprudencia para hechos siguientes de igual índole, también lo vemos mencionada en sentencias como; Audiencia Provincial de Madrid, Sección:7, Nº de Recurso:518/2014 y Nº de Resolución:268/2015, Audiencia Provincial de Madrid,Sección:2,Nº de Recurso:986/2014 y Nº de Resolución:613/2014, Audiencia Provincial de Málaga,Sección:8, Nº de Recurso:62/2013 y Nº de Resolución:341/2013, Tribunal Supremo. Sala de lo Penal, Nº de Recurso:10445/2012 y Nº de Resolución:722/2012.

La prueba electrónica en el derecho de las TIC queda reflejada en la legislación en los siguientes artículos:

El Artículo 26 del Código Penal:

> "*todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica*."

Artículo 743.1 de la LECRIM:

> Medios de registro de la sesión. Documento electrónico.
>
> "*El desarrollo de las sesiones del juicio oral se registrará en soporte apto para la grabación y reproducción del sonido y de la imagen*."

En el Artículo 299 de la LEC;

Mediante documento privado, como puede ser correo electrónico, con peritación de autenticidad. Documento público, mediante acta notarial de la prueba electrónica o la propia peritación.

Una de las primeras definiciones minuciosas sobre el concepto de la Prueba Electrónica se encuentra ampliamente definida en el Convenio de Budapest; se trata por tanto de pruebas que por su naturaleza y características propias poseen información y datos que se podrán estudiar como el clásico documento probatorio, pero con un formato electrónico. Este carácter electrónico le confiere una facilidad de manipulación, reproducción, copia, almacenado, certificación, autentificación, que debemos estudiar y aprovechar. No obstante, esto conlleva también un número alto de dificultades perceptivas a la valoración de las pruebas por la administración de justicia en las partes públicas o privadas, que aseguren la autenticidad del hecho investigado.

3.1.4.2 CARACTERISTICAS DE LA PRUEBA ELECTRÓNICA

La prueba electrónica posee muchas características comunes con la prueba clásica pero también se pueden enumerar un grupo de características distintivas, con las que destacaremos;

A. Requiere personal especializado para su recogida y custodia.

Los datos o elementos que se encuentran en los dispositivos electrónicos, requieren ser recogidos por expertos que sean capaces de discernir sobre cuáles son los datos relevantes y cuáles son los accesorios. En el momento de la recogida es necesario seguir un protocolo estricto que estructure la información a estudiar. El modo de recogida de los datos puede habilitar o imposibilitar la realización de las peritaciones encomendadas. Los dispositivos electrónicos.

B. Personal experto para su interpretación:

Los datos o elementos que se encuentran en los dispositivos electrónicos, requieren ser tratados por personal especialista para su posterior estudio, esto evitará que se produzcan

posibles alteraciones que repercutirán en la peritación. Mucha de la información que se encuentra en los equipos electrónicos se encuentra de manera invisible a personal no experto por lo que es imprescindible una buena formación y experiencia para el tratamiento de estos datos. La interpretación de los datos de manera minuciosa conseguirá unas conclusiones en la peritación mucho más fieles a la realidad.

C. Son pruebas volátiles:

Las pruebas electrónicas son inestables, variables, e incluso con un estudio inadecuado pueden ser manipulables; consciente o inconscientemente, modificando el estado de los dispositivos, o la realidad de los hechos a estudiar. El mero encendido o apagado del equipo, la introducción de dispositivos de memoria, o elementos de control puede variar los logs de los equipos, modificando la escena a estudiar.

D. Duplicado de la información:

Una de las ventajas sin duda es el duplicado de la información de los dispositivos electrónicos, que eso sí facilita el tratamiento de los datos para la peritación o para la posible contra-peritación, así como para futuras investigaciones con diferentes herramientas. Una vez extraída toda la información, se puede hacer copia de la misma, y ser una copia exacta.

E. Almacenamiento:

El almacenamiento de esta información es una ventaja importante. Los datos correctamente extraídos de los equipos, o perfectamente duplicados a posteriori, son fácilmente almacenados, ocupando un espacio mínimo, con un acceso muy sencillo para futuros estudios. Destacar que el almacenamiento de los propios dispositivos o elementos electrónicos tienen también unas particularidades para su almacenamiento; las bolsas de Faraday, almacenes libres de campos electromagnéticos potentes o los muy comunes de humedad y temperatura, estos últimos tienen un rango más amplio que otro tipo de pruebas.

F. Evolución y cambio de fuentes y pruebas electrónicas:

Una de las características más destacadas de la prueba electrónica es el continuo cambio y evolución que encontramos en la multitud de tipología de elementos y pruebas electrónicas. Los instrumentos electrónicos están en continua fase de desarrollo, lo que supone una constante actualización de conocimientos por parte del perito experto. Esto conlleva una necesidad de actualización constante por parte del perito para el desarrollo de sus funciones, no sólo por la tipología de la información sino por como diagnosticarla, tratarla, captarla y en definitiva convertirla en una peritación veraz. Esto lleva de manera anexa el conocimiento de las técnicas y herramientas recientes para la obtención de la información o pruebas que deberemos utilizar.

TABLA 3.1: Fases de la evidencia digital

3.1.4.3 JURISPRUDENCIA PRUEBA ELECTRÓNICA

El Tribunal Supremo se pronunció el día 19 de mayo de 2015 sobre el valor probatorio de las llamadas evidencias digitales. Dictaminando así y en este contexto, la Sala Segunda del Alto Tribunal, en su STS 300/2015 el 19 de mayo y, al enjuiciar la aceptación incondicional de los pantallazos aportados al proceso, viene a confirmar que toda prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería instantánea "*debe ser abordada con todas las cautelas",* recogiendo los planteamientos de Audiencias Provinciales, especialmente fecundas en este campo, como la Audiencia Provincial de Cádiz, SAP 31/2014 de 28 enero o la Audiencia Provincial de Madrid, SAP 1260/2012 de 1 octubre.

Sentencia esta que se produjo después de que en 2013 ya admitieran como prueba electrónica válida los mensajes WhatsApp, eso sí, aclarando que conocen la posibilidad de su manipulación, por lo que tiene que ser recogida la prueba con cautela. Así que recogemos la sentencia del tribunal supremo y sentencias de otros tribunales que surgieron al realizar las consultas sobre las mismas.

El Auto del Tribunal Supremo de 14 de febrero de 2013 que considera el sistema de mensajería WhatsApp como un medio válido para acreditar determinados hechos. En dicho asunto, el condenado por un delito contra la salud pública por tráfico de sustancias estupefacientes, decidió recurrir ante el Tribunal Supremo la sentencia de la Audiencia Provincial de Madrid que lo había condenado, siendo la base de su recurso la vulneración del artículo 18.3 de la CE , en relación con el artículo 24.2 de la misma (derecho a la presunción de inocencia) dado que éste interpretaba que las conversaciones intervenidas en el teléfono del recurrente por medio de la aplicación WhatsApp de su teléfono, eran nulas por vulnerar la doctrina jurisprudencial sobre las escuchas telefónicas, el hallazgo casual y el descubrimiento inevitable.

El Tribunal Supremo, partiendo de la doctrina del Tribunal Constitucional que posibilita el que por resolución judicial se pueda acordar la medida de intervención telefónica siempre que se expresen o exterioricen las razones fácticas y jurídicas que apoyan la necesidad de tal intervención, entendió que el acceso por parte de los agentes de la Guardia Civil al contenido de las aplicaciones del teléfono móvil del condenado, si bien afectaba al derecho constitucional al secreto de las comunicaciones protegido en el artículo 18.3 de la CE, se llevó a cabo previa autorización judicial mediante auto adoptado como consecuencia del requerimiento de la Policía Judicial para el encendido del teléfono y la comprobación de los datos obrantes en el mismo.

En dicho auto judicial se autorizaba al equipo de Policía Judicial para que pudiera encender el terminal telefónico intervenido al recurrente, al objeto de comprobar y reseñar datos sobre las comunicaciones existentes vía SMS, vía MMS, vía Whatsapp, y datos de contacto de la agenda... Partiendo de esa base, no puede alegarse que se haya vulnerado el derecho al secreto de las comunicaciones.

- Sentencia de la Audiencia Provincial de Cádiz, 31/2014 de 28 enero. JUR 2014\95996 "[…] *pues no habiendo declarado los dos implicados, de la existencia de lesiones no puede desprenderse el origen de su autoría y unos mensajes de wasap sobre los que ningún técnico ha declarado y que no consta que sean veraces o emitidos por el apelante o que no hayan podido ser manipulados, no es suficiente prueba para sustentar en ella el pronunciamiento condenatorio que se combate, razón que hace procedente la estimación del recurso* […]".

- Sentencia de la Audiencia Provincial de Pontevedra, 10/2014 de 10 enero. JUR 2014\25448 "[…] *la prueba que sustenta la condena del recurrente, aparte del dato objetivo de la existencia de los carteles y whatsapp, de indiscutible carácter vejatorio y ofensivo, se deriva de las manifestaciones de la denunciante, pues no consta siquiera la titularidad del teléfono desde el que se envían los mensajes y las declaraciones de los testigos no son concluyentes. Tales datos, se estima son manifiestamente insuficientes para deducir de ellos, con el nivel de certeza necesario para sustentar una Sentencia condenatoria* […]".

- Sentencia de la Audiencia Provincial de Madrid, 12/2013 de 5 abril. JUR 2013\175198 "*Mensajes, enviados a través del whatsapp, que han resultado transcritos en el Juzgado de Violencia Sobre la Mujer nº 3 de Madrid, al inicio de las actuaciones judiciales que, como ya anticipábamos adquieren un singular valor probatorio, porque, tanto por la secuencia horaria en que las comunicaciones entre Celia y Concepción se realizan, como por el contenido de las mismas, suponen un elemento de corroboración objetiva puntual y exacta de lo declarado, coincidentemente, por las dos testigos*."

- Sentencia de la Audiencia Provincial de Madrid, 1260/2012 de 1 octubre. JUR 2012\341849 "*También considera que el contenido las WHAT'S APP son fácilmente manipulables, y se pueden borrar parte las conversaciones, por lo que entiende que el libre acceso que han tenido los agentes a estas WHAT'S APP, contactos y todo tipo de aplicaciones del teléfono móvil del terminal de don Elias vulneran el artículo 18,3 de la Constitución y por lo tanto considera que debe existir una nulidad de todas las transcripciones y los pantallazos incorporados a las actuaciones* […].

3.1.5 OBJETIVO PRINCIPAL

El objetivo principal de la toma de información y realización, es la elaboración de una peritación concluyente, que dé respuesta a la necesidad por la que surgió o que pueda asegurar su admisión como prueba. Para eso debe cumplir una serie de características legales que se diferencian de la prueba tradicional. Estas son enumeradas a continuación:

A. Certeza en la carga de la prueba:

LECiv*Artículo 217Carga de la prueba (en su apartado 2)*

Corresponde al actor y al demandado reconviniente la carga de probar la certeza de los hechos de los que ordinariamente se desprenda, según las normas jurídicas a ellos aplicables, el efecto jurídico correspondiente a las pretensiones de la demanda y de la reconvención.

La toma de datos y el posterior análisis pormenorizado de la prueba original, la cadena de custodia en el ejercicio de las funciones, entrega y recepción, no cometer alteraciones en la prueba, debe tener como finalidad la no modificación de la prueba electrónica. Para que no sea rechazada en la elaboración de la peritación.

B. Objetividad:

La prueba electrónica debe ser objetiva, nunca una visión particular. No confundir con la valoración de la peritación.

C. Verificación:

Los elementos utilizados en el desarrollo de las funciones de la peritación deben estar registrados, numerados y homologados para el aseguramiento de la veracidad de los datos obtenidos.

D. Claridad:

La peritación debe ser realizada por expertos, debe ser técnica, verídica, pero sin olvidar que debe ser realizada para su comprensión y estudio para personas no versadas en la materia. Debe tener unas conclusiones, claras, entendibles, evidentes y perceptibles.

E. Proporcionalidad:

El principio de proporcionalidad en la legislación nos lleva a la

recogida de pruebas de manera que cumpla estas características; Adecuación al fin, necesidad, o consideración de la medida a realizar dependiendo de los hechos cometidos.

La descripción legal del principio de proporcionalidad se encuentra contemplada en los artículos 15, 17 o 55 de la Constitución. También en el artículo 25.1 de la Constitución. El Tribunal Constitucional, redacta una Sentencia del Tribunal Constitucional de 22 de mayo de 1986, sobre el artículo 25.1 de la Constitución y el principio de proporcionalidad, en definitiva, en el desarrollo de las funciones de un perito informático debe seguir este principio en las peritaciones.

3.1.6 CONSIDERACIONES ADICIONALES

3.2 ELABORACIÓN DEL INFORME PERICIAL

En esta parte del proyecto iniciaremos cómo enfocar las peritaciones de los diferentes dispositivos electrónicos que podemos encontrar en el desarrollo de nuestras funciones como perito informático, e iniciaremos desde lo más estructurado y mecanizado, como es la elaboración de la pericia en tarjetas de memoria hasta lo más abierto y dependiente de sistemas operativos o demás software que se encuentre en su interior como serían los dispositivos móviles.

Cuando nos referimos en el proyecto a dispositivos de memoria nos referimos a cualquiera de estos: discos duros, tarjetas de memoria y demás dispositivos electrónicos de almacenamiento. Así como los elementos de memoria interna o externa para:

Grabación de video y fotografía

- *Cámaras digitales*
- *Cámaras de video digital*
- *Grabadoras de vídeo*
- *Grabadoras de audio digitales*
- *Camaras de Circuito Cerrado (CCTV)*
- *Reproductores portátiles*

EL INFORME PERICIAL

Como todo trabajo debe seguir un escrupuloso orden y meticulosa presentación, es obvio que cuanto mayor es el rigor de un trabajo, mejor estructurado debe ser este, la peritación debe contar de los siguientes apartados:

3.2.1 LA PORTADA

La peritación debe contar con una portada en el que se establezca, los siguientes puntos:

- El encargado de realizar la peritación: Si es un perito, el número de colegiado si lo tuviera y el nombre, si es una empresa o en la administración, el encargado de realizarlo con su cargo y su identificación.
- El título, que debe ser una frase informativa de lo que trata la peritación.
- La persona que encarga esa peritación o en su caso a la persona o institución a la que va destinada esa peritación.
- Número de referencia de la peritación:
  - En la administración, si se trata de un expediente debe ser reflejado el número de expediente al que va adherida la peritación
  - Administración justicia; número de juicio, diligencia previa…
  - En el ámbito privado, número de pedido, número de caso, o informe solicitado

De la misma manera que cuenta con la portada, debe presentar una contraportada, esto no se trata de un mero capricho formal del escritor de este proyecto, una peritación está diseñada para pasar por diferentes manos, ser revisada, estudiada, leída y adjuntada a diferentes procesos administrativos, o penales, ya sean juicios, diligencias o demás, pasando

por diferentes despachos y personas, esto hace que la portada debe ser muy clara y ordenada, definiendo lo interior, la numeración y el título identifica el trabajo que se expone.

3.2.2 EL ÍNDICE

En el caso de que la peritación sea extensa, es conveniente realizar un índice donde enumere las diferentes partes de la peritación, ya que estas pueden ir de un simple folio a cientos de ellos, dependiendo del caso, por lo que en algunos casos la realización de índice es imprescindible para el estudio del mismo. Se debe enumerar por apartados y paginar las hojas de la peritación, así como referenciar y numerar los ANEXOS que son muy comunes en este tipo de trabajos.

3.2.3 EXPLICACIÓN DE MOTIVOS

En la explicación de motivos de una peritación, se debe presentar de manera más detallada, quién realiza el requerimiento por el cual se realiza la peritación. En este apartado, debemos consignar la fecha de la petición, y de dónde proviene la petición;

- Número de referencia de la peritación:
  - En la administración, si se trata de un expediente debe ser reflejado el número de expediente al que va adherida la peritación
  - Administración justicia; número de juicio, diligencia previa…
  - En el ámbito privado, número de pedido, número de caso, o informe solicitado

- Una explicación de por qué se nos requiere, en definitiva, el motivo por el cual se nos requiere y se nos hace partícipes para el desarrollo de nuestras funciones.

En este punto se nos abre la puerta a los dos tipos de inicio de nuestra gestión:

- Entrega de dispositivos electrónicos para su estudio.

- Entrega de petición para la realización de un estudio de diferentes elementos, con el objetivo de formalizar posteriormente una petición. Este caso engloba casos como el estudio de elementos para incautar o qué elementos se deben pedir para posteriormente realizar la entrega de la petición para la peritación. Muchas veces los clientes, jueces o empresas, saben lo que quieren, pero al no tener conocimientos técnicos del asunto en cuestión, no conocen la forma de realizar la petición en sí.

3.2.4 MATERIAL RECIBIDO

3.2.5 DATOS DEL PERITO

En este punto se pasa a describir los datos del perito informático que va a realizar la peritación, significando el número de perito, su nombre, su titulación más especializada dirigida al caso en cuestión, la pertenencia a una empresa o administración, y lugar donde se va a realizar la peritación si procede, como es en los casos de laboratorios, o despachos especialistas para el desarrollo de sus competencias.

3.2.6 OBJETO DEL INFORME

Para describir el objeto del informe que se va a realizar, se deben enumerar las actuaciones que el perito va a desarrollar en la peritación, que deberán ir encaminadas a la resolución del requerimiento realizado. Debe ser una enumeración de cada una de las partes del proceso que se va a trabajar, dejando evidencia del orden de trabajo. Dependiendo de la tipología de la peritación y del destinatario de la peritación, debe ser o muy dirigida, enfocada y especializada, o más amplia, donde se indique de manera superficial, lo realizado; un ejemplo de una simple extracción de archivos de voz de una tarjeta de memoria podría ser enumerada de la siguiente forma:

- Análisis forense delatarjeta de memoria.
- Extracción de grabaciones requeridas.
- Extracción de archivos de voz.
- Transformarlas a un formato audible.
- Grabación de las mismas a soporte físico.
- Transcripción del archivo de voz.

3.2.7 MATERIAL TÉCNICO UTILIZADO

3.2.9 INFORME TÉCNICO

3.2.10 ACTAS; TRANSCRIPCIÓN, ARCHIVOS, VISUALIZACIÓN, ANEXOS…

Las Actas son elementos que se adjuntan a la realización del informe, que son partes explicativas, descriptivas o informativas, a los que se hace mención en la peritación que deben de ser adheridos. Esta información se adjunta porque explica elementos de la pericia, como son las transcripciones de datos que se encuentran en los dispositivos electrónicos entregados y sólo se pueden oír, ver o reproducir con herramientas especializadas. Sin estos elementos técnicos no podrían ser reproducidos, por lo que se transfiere la información a otro tipo de formatos, o incluso soportes físicos. En diferentes ocasiones también puede ocurrir que esta información deba de ser estudiada de forma paralela por otros expertos y deben ser tratados de forma externa al informe pericial.

En todos los casos se debe reseñar siempre la localización de los mismos, la fecha y hora de escucha, visualización o lectura, los diferentes elementos que han sido utilizados para su captación, así como una pequeña explicación de por qué han sido encuadrados en un acta adherida a la pericia y no forman parte del informe principal. En ciertos casos más específicos también debe ser explicada su aportación a la peritación y una valoración si procede, como son datos que se encuentran en la peritación y que no formando parte de la misma, puede explicar algún hilo argumental de las conclusiones finales.

Cada uno de los elementos que se presenten en las actas deben de ser referenciados, y anotados, dejando constancia de la procedencia y su estado a la hora de la captación. Así como la aportación de los datos técnicos necesarios para la prueba de su naturaleza cierta.

3.2.11 RESULTADO

El resultado es un punto que se debe desarrollar dependiendo del tipo de pericia requerida, debido a que en algunos casos se requiere la opinión del perito y sólo la transmisión de la información encontrada por lo que se realizará el resultado obtenido. En otros casos la pericia requerirá de una conclusión donde el perito realice un juicio de sus actuaciones, y en el desarrollo de la peritación tenga que hacer una valoración a modo de resumen de lo realizado, estudiado y encontrado. En este punto se expondrá el total de las apreciaciones y deliberaciones que se obtengan una vez terminada la peritación. Las conclusiones se deben realizar sobre lo que el requirente haya solicitado, es decir, no realizar valoraciones de lo que no se realiza petición, ya que puede anular la objetividad y el motivo de nuestra pericia. Siempre deben de ser conclusiones realizadas como consecuencia del análisis y comprobaciones de los resultados. Es muy importante destacar que no deben presentar valoraciones jurídicas, ni de responsables de los hechos, ni elementos jurídicos. No se deben presentar datos que no puedan ser entendidos o analizados sin conocimientos especializados, es decir, los datos no deben ser entendibles y analizables sólo por expertos.

Cuando las afirmaciones con las que se concluye la peritación requieran ser matizadas debe de ser precedida por una sección denominada reservas. Es fácil de entender en el desarrollo de nuestras funciones, ya que, al presentar información, muchas veces viene sesgada, tanto por delante como por detrás, por lo que es muy conveniente explicar el motivo

de tal sesgo, fundamentando con datos lo realizado, siempre dejando constancia de que todo queda registrado en el caso de futuras observaciones.

3.2.12 REMISIÓN

La remisión es el apartado donde se informa de todo lo que se remite al requirente de la pericia. Es una prueba escrita del mantenimiento de la cadena de custodia de los elementos entregados, y de los que se adhieren al proceso, o simplemente el trámite donde queda reflejado cada una de los elementos de la peritación. Es decir, los elementos con los que se finaliza y se entrega, por ejemplo: Se remite a su empresa PFC & Asociados el presente informe técnico el cual consta de 23 folios escritos por una cara, portada, contraportada, la transcripción realizada de los archivos reseñados, el disco duro externo y el CD con los archivos reseñados en soporte y formato reproducible.

4 Análisis de dispositivos

Es la parte principal del proyecto, y es donde abordaremos la manera de proceder con el tipo de dispositivos electrónico que es el presente y futuro de la tecnología personal, los terminales móviles. En la primera parte, estudiamos los elementos electrónicos de almacenamiento de información o los que son elementos propios de información. Sólo realizar un pequeño inciso, debemos distinguir los discos duros conectados a servidores, de almacenamiento conectado en red NAS (Network Attached Storage) o directamente a una red para operar como discos duros de varios equipos a la vez, ya sea en forma de "nube" o bien vía wifi. En estos casos debemos proceder a realizar antes del estudio, el mismo protocolo que en los dispositivos electrónicos conectados a una red, que son los que vamos a estudiar a continuación.

Debo repetir esto porque es de vital importancia: Los puntos definidos en esta parte del proyecto sirven de estructura para cada una de las peritaciones que se puedan realizar en el desarrollo de las funciones del perito forense tecnológico. En este apartado se encuentran las diferencias más notables, no sólo en estructura, si no de manera de enfocar cada pericia, por lo que para seguir cada uno de los tipos de análisis de los diferentes tipos de dispositivos, es muy importante entender que debemos tener claro el concepto del dispositivo a estudiar y de las herramientas que debemos utilizar. Esto es debido a que tanto los dispositivos, como las herramientas, se encuentran en constante evolución, por lo tanto, lo único que tendríamos que estudiar cuidadosamente es la herramienta actual que realice las funciones que nosotros perseguimos en el desarrollo de la pericia. Por lo que es de importancia asentar el concepto que hay que tener como referente, y es que no se trata de la herramienta a utilizar, si no del resultado y la finalidad que perseguimos, lo que queremos obtener y cómo queremos realizar ese resultado. Las siguientes herramientas desarrolladas y elegidas en los ejemplos, no están elegidas al azar, son las herramientas que realizan la metodología correcta para la peritación. Esto se debe a que, para su desarrollo o utilización, lo único que varía es el software de los dispositivos y no la información que el usuario ha ido almacenado en los mismos. De esta manera, cuando cambien los dispositivos o los softwares forenses, debemos buscar los que cumplan con los requisitos técnicos generales, aunque procedan de distintos desarrolladores o dispongan de diferentes formatos, entornos gráficos o sistemas operativos. Este conjunto de reglas es lo que convierte a este protocolo en un documento vivo, que no depende de las herramientas desarrolladas, sino que busca el asentar el concepto de cómo se debe realizar y enfocar el estudio del dispositivo, sin importar las futuras evoluciones de los mismos.

Dispositivos electrónicos conectados

Los dispositivos electrónicos conectados son todos aquellos que se encuentran con conexión a una red. En nuestros días, disponemos de una gran cantidad de elementos que disponen de conexión a red:

- Ordenadores:

  - Portátiles
  - De Sobremesa
  - De torre
  - Sistemas Rack
  - Microcomputadores
  - Mainframes (súper computadores)

- Un monitor u otro dispositivo de visualización.
- Memoria interna
- Memoria externa
- Un teclado.
- Un ratón.
- Unidades de almacenamiento externo conectadas
- Periféricos:
  - Impresoras
  - Escáneres
  - Routers
  - Replicadores de puertos (dockingstations)
  - Unidades de cinta
  - Webcams
  - Altavoces
  - Micrófonos
  - Calculadoras
  - Fax
  - Contestadores automáticos
  - Lector de tarjetas

- Tabletas
- Dispositivos de almacenamiento
- Discos Duros y solid state disks
- *Teléfonos móviles*

- Consolas de videojuegos

Se escapa a los objetivos de este proyecto el estandarizar para cada uno de los elementos electrónicos un protocolo, lo que si debemos trazar es una directriz común en todos ellos, para una manera de actuación. Siendo así el perito, el que con su experiencia, aplique cada una de las guías o cada una de las herramientas que enumeraremos en esta parte para el desarrollo de la pericia.

Nos centraremos en dos grandes grupos, los ordenadores y los dispositivos móviles (móvil, Tablet…) para cada uno de los cuales desarrollaremos un procedimiento que tendremos que ir adaptando al objetivo que se persigue y adecuándolo a los sistemas que dispongan los elementos.

4.1 PERITACIÓN DE EQUIPOS INFORMÁTICOS

La peritación de ordenadores o dispositivos móviles requiere un estudio de regeneración constante para ser un especialista en la materia, ya que se trata sin lugar a dudas de una rama en constante evolución. Esto no interfiere en el objeto de este proyecto que es marcar unas pautas que sirvan de directrices para la actuación misma, pero si dista en una parte importante de la esquematizada anteriormente para elementos de memoria. Los ordenadores o los móviles actuales (que no difieren mucho de ser ordenadores personales al presentar unas características muy similares), son elementos capaces de modificar su información de manera rápida, y se encuentran en continuo desarrollo y evolución debido al elevado número de dinero que mueve su industria. Esto le confiere unas características muy singulares que debemos de atender para realizar la pericia, el cómo tratar desde que se recibe el dispositivo hasta que se devuelve, puede marcar el resultado de la misma y puede resultar clave para acciones posteriores ya que puede inutilizar o destruir no sólo la información contenida, si no el dispositivo electrónico en sí.

La primera parte de la peritación es análoga con la descrita en el apartado anterior, compartiendo los conceptos de:

- Portada
- Índice
- Explicación de motivos de la petición
- Datos de perito
- Material que se nos entrega
- Objeto del informa
- Material técnico utilizado

4.2 INSPECCIÓN OCULAR

El análisis del dispositivo entregado que se nos remite, se inicia con lo que se conoce como inspección ocular.

4.3 INFORMÁTICA FORENSE “EN VIVO”

La información, los datos, las imágenes y las backups de la RAM obtenidas de los dispositivos han tomado relevancia en los últimos años con el importante aumento de las memorias RAM y el tamaño de los datos volátiles. Tenemos que tener en cuenta que las memorias RAM en la actualidad son capaces de gestionar gigabytes de datos, y esto, es una gran cantidad de datos e información a estudiar. Cuando se encuentran encendidos los terminales, manejan una gran cantidad de información que hace años era pasada desapercibida. Los estudios realizados de estos datos en la actualidad por parte de muchos investigadores y cómo esta información hace un verdadero retrato del usuario, puso de manifiesto la importante relevancia de los mismos en la peritación, ya que puede ayudar a

determinar pruebas decisivas en el informe forense. Es por supuesto, la información que se obtiene de un dispositivo que se encuentra encendido y por lo tanto, muchas veces facilita mucho la entrada al contenido del mismo debido a que se encuentra accesible. Otro de los factores importantes, es conocer cómo y con qué se encuentra conectado, o que se estaba realizando en el momento de la intervención in situ, en definitiva, una multitud de posibilidades que sólo incrementan la necesidad de realizarlo cuando la situación se encuentre disponible.

Este tipo de procedimiento es el que requiere mayor grado de conocimiento, mayor nivel de especialización, que el llamado en frío (o deadboxforensics), por lo que debe ser dirigido y realizado con cautela, ya que un mal desarrollo del mismo, puede llevar incluso la pérdida de los datos del dispositivo.

4.3.1 LA MEMORIA VOLÁTIL

La memoria volátil se caracteriza por estar compuesta por datos que se consiguen cuando el dispositivo se encuentra encendido y se perderían en el momento del apagado. Se trata, por tanto, de datos de carácter temporal, que tendrá una duración temporal dependiendo del tipo de registro o dato, o su localización, etcétera. El tipo de Memorias actuales de varios Gigas de datos hace que sea una cantidad de datos que no se puede despreciar.

Diferenciar entre los tipos de datos volátiles, entre los procesos internos del equipo, con los que se producen con los sistemas de acceso remoto, conexiones a redes, diferentes tipologías de conexiones exteriores, caché, etcétera. También la memoria puede contener datos relevantes de encriptación, contraseñas, datos de navegación, certificados que han funcionado, programas en funcionamiento, un elevado número de información útil. Entre los fragmentos más destacados, enumeraremos los siguientes: *(lista extraída del documento GEE)

- Procesos en funcionamiento
- Servicios en funcionamiento
- Información del Sistema
- Usuarios logueados
- Puertos abiertos y de escucha
- Caché del protocolo ARP (protocolo de resolución de direcciones)
- Cachés DNS
- Información de reinicio
- Información de registro no copiada en la memoria
- Documentos no guardados
- Binarios de procesos y servicios, que incluyen aquellos de malware que residen en la memoria.

En este punto de la peritación debemos resaltar como guía para realizar consulta una extensa guía de software para realizar comprobaciones y extracción de información, que ha sido realizada por Kuhlee and Voelzow. Está diseñada para la obtención de fragmentos concretos de datos de memoria volátil.

Fragmento Volátil	Herramientas para Windows	Herramientas para LINUX
Contenido de la memora RAM	Dumpit, Winen, Mdd	dd, fmem
Tablas de enrutamiento, cachés ARP, estadísticas Kernel	Rúter PRINT, arp –a, netstat	netstat –r –n route arp –a
DNS cachés	Ipconfig /displaydns	rndcdumpdb (ifinstalled)
Listas de procesos	PsList, ListDLLs, CurrProcess, tasklist	ps –ef, lsof
Conexiones abiertas de red (enchufes)	netstat –a	netstat –a, ifconfig
Programas y servicios que utilicen conexión de red	scqueryex, netstat -ab	netstat –tunp
Archivos abiertos	Handle, PsFile, Openfiles, net file	lsof, fuser
Recursos compartidos de red	Net share, Dumpsec	showmount –e, showmount –a smbclient –L
Puertos abiertos	OpenPorts, ports, netstat –an	netstat –an, lsof
Registro de usuarios conectados	Psloggedon, whoami, ntlast, netusers /l	w, who -T, last
Sistema de archivos cifrado	Manage-bde (Bitlocker), efsinfo (EFS)	mount -v, ls /media
Sistemas de archivo conectados temporalmente	Fsinfo, reg (MountedDevices)	mount -v, ls /media
Accesos remotos y monitorización de datos	Psloglist	/etc/syslog.conf Port UDP 514
Configuración física, topología de red	Systeminfo, msinfo32, ipconfig /all	ifconfig –a netstat –in
Dispositivos de almacenamiento	reg (Mounted Devices), Net share, netstat –a	mount -v, ls /media
Sistema horario (para establecer el reloj de la radio)	time /T, date /T, uptime	time, date, uptime
Ámbitos variables	cmd /c set	env, set
Portapapeles	Pclip	
Contenido del disco	FTK Imager, EnCase, TableauImager	Dc3dd, ewfacquire, Guymager

Tabla 4-1: Guía de herramientas Kuhlee and Voelzow

La gran mayoría de este software se encuentra en Sysinternals suite de Microsoft o en el repositorio CERT de Linux:

- Windows Sysinternals Live
  - http://technet.microsoft.com/en-gb/sysinternals

- Digital Intelligence and Investigation Tools
  - http://www.cert.org/digital-intelligence/tools/index.cfm

Debemos ser conscientes que uno de los puntos a analizar una vez estudiado los datos volátiles del dispositivo, es el tráfico del dispositivo en parado. Es decir, tenemos que observar si el elemento electrónico se encuentra transmitiendo datos, incluso cuando no hay aplicaciones o software del sistema en funcionamiento. Este tráfico de datos nos podría en la pista de una serie de malware o programas espía que nos indicaría que el dispositivo ha sido manipulado con la intención de mandar información a un tercero, o sin que este tuviera conocimiento o con conocimiento del mismo. Para este tipo de comprobaciones existe numeroso software en la actualidad, e incluso aplicaciones para realizarlas. Algunas de ellas expuestas en el apartado de herramientas forenses en este PFC. El malware o los programas espías son bastante más comunes de lo que la gente se piensa, son numerosos los casos de programas instalados en ordenadores de empresa que una vez al día o de manera semanal, lanzan informes de todo lo acontecido en el ordenador a un tercero, otras veces ocurre con los terminales de teléfono o Tablet. En estos casos son los propios terminales lo que envían, ya sea mensajes, intercambio de información de lo realizado, registros de llamadas, incluso una copia literal del sistema a una nube la cual controla un tercero. Ejemplos variados en jurisprudencia donde juzgan y penalizan estos comportamientos, o como en otros casos, ratifican la utilización por parte de la empresa de este tipo de software para el seguimiento de los terminales informáticos de los empleados. Sirva como ejemplo la STS 8876/2011 del Tribunal Supremo. Sala de lo Social, donde dicta sentencia en este asunto, permitiendo el uso de este tipo de software, en situaciones especiales.

No pensemos que sólo estos programas maliciosos se encuentran en ordenadores, en la actualidad, lo que está evolucionando con mayor intensidad son los malware en móviles, u otros dispositivos electrónicos conectados a internet, aquí ofrezco un listado de las numerosas Sandboxes, son herramientas para aislamiento de procesos, para el análisis de los mismos, para el tratamiento de archivos .apk

- http://www.apk-analyzer.net
- http://mobilesandbox.org
- https://anubis.iseclab.org
- https://code.google.com/p/droidbox

También introduciré una lista de herramientas de análisis de Malware en los móviles:

- Android SDK
- Dex2Jar
- Dexter

- JD-GUI

Y la que requiere un apartado especial por su tipología, tratándose de una máquina virtual para en análisis de malware en móvil, la conocida Santoku, explicada en este proyecto en la parte de herramientas forenses.

Una vez plasmada la importancia del estudio en vivo de los dispositivos y como debemos para ello realizar el análisis de la memoria RAM, como siempre respaldaré mis comentarios con notas jurídicas sobre el tema, en este caso es de Estados Unidos en la que en marzo de 2007, la Corte del Distrito Central de California, Estados Unidos, determinó en el juicio de Columbia Pictures Industries contra Justin Bunneli, donde se exponía que la memoria RAM constituía un conjunto de información electrónica que debía ser tratada como cualquier otro soporte físico, ya que no tenía ninguna limitación temporal, ni mínima, ni máxima de perdurabilidad de los datos, ya que estos, dependen de la utilización del sistema. Dando una relevancia en la jurisprudencia a este tipo de prácticas.

4.3.2 EJEMPLO DE REALIZACIÓN DE ESTUDIO DE MEMORIA RAM

Realizaremos un volcado de la memoria RAM para su estudio. Para eso seguiremos un método que vamos a considerar estándar en nuestras peritaciones, que será generar siempre una imagen, o archivo de los datos a estudiar, posteriormente realizaremos dos hashes de ese archivo a estudiar, uno lo dejaremos de salvaguarda para posteriores comprobaciones si fuera necesario, y sobre el otro realizaremos el estudio que dará como resultado la pericia.

La imagen de esa memoria RAM se puede realizar con múltiples programas de los que se disponen en la actualidad, entre los que destacaremos:

La situación más idílica que nos podemos encontrar para el estudio de una memoria RAM: que en el equipo nos encontraremos con un puerto FireWire como el de la imagen a continuación:

Figura 4-1: Puerto FireWire

El puerto FireWire o más técnicamente como IEEE1394 se trata de un puerto que nos da acceso directo a la memoria RAM de un ordenador, tenga o no bloqueo de entrada de usuario, o clave de acceso, se encuentre bloqueado, en definitiva, encuentre como se encuentre el equipo, (es obvio decir que debe estar en funcionamiento☺). Mediante la utilización del software Passware, a través del puerto firewire, conectando dos ordenadores directamente se puede copiar la RAM del dispositivo, se encuentre con clave oculta, encriptada para su entrada o demás impedimentos que al lector se le puedan ocurrir, ya que por el sistema de capas de la OSI, este software no va de arriba a abajo a leer la información, sino que accede directamente a su contenido, obviando el sistema operativo del Ordenador o dispositivo que queramos peritar. En el caso de no encontrar este tipo de puerto, debemos realizar el estudio de otra manera, mediante el acceso al ordenador y mediante uno de las siguientes herramientas.

El MagnetRam Capture de MagnetForensic; de software libre, que en la actualidad se encuentra muy orientado al envío de información a una nube, es decir del estudio de datos mientras están siendo procesados por la RAM para su traslado a una nube, es fácil de utilizar y se puede solicitar una licencia trial, con cuenta de universidad.

La herramienta a mi juicio más potente y más utilizada desde principio de 2010 a nuestros días es Dumpit de Moonsools, lleva un tiempo sin actualizaciones, pero su versitilidad y potencia está por ahora fuera de toda duda. Se trata de una herramienta portable, de poco peso (de tamaño en bits pequeño) que a grandes rasgos, una vez instalada o dejándola correr desde una memoria usb, realiza un fichero .raw, con una copia de toda la memoria para su posterior utilización. Hay que destacar que puede ser usada desde cualquier tipo de arquitectura. Otra de sus ventajas es que, al ser fácilmente adaptable al equipo, no ocupa mucha memoria en su utilización evitando así solapar parte de la memoria RAM que queremos realizar el estudio, es muy intuitiva, interfaz poco trabajada pero muy simple y trasladable en un USB, para no tener que instalar ningún programa en el ordenador a realizar la peritación. Podemos elegir donde realizar el volcado de la información por lo que, con Memoria externa suficiente, se puede realizar una copia en vivo, modificando de manera muy superficial la información a estudiar.

Con el archivo obtenido es sencillo realizar los dos HASH de ese archivo para su estudio y posteriores comprobaciones. Otra de sus funcionalidades más interesantes es que esta herramienta posee unos indicadores de compromiso, que son una serie de reglas de lo que se encuentra realizando un registro en el sistema. Y usa estos indicadores de compromiso para realizar comparaciones y establecer que software está utilizando el sistema de manera fiable y que parte del sistema no opera con él de manera conjunta por lo que se trata de un malware.

Otra herramienta es el BelkasoftRamCapturer, también software libre, pero que sólo son utilizables hasta Windows 8 y anteriores, por lo que no vamos a describir mucho esta herramienta, con sus posteriores actualizaciones podrá ser (o no), bastante interesante, y por último la herramienta software de RekallWinpmem, que como particularidad, puede hacer adquisiciones de memoria RAM desde remoto, y poder lanzarlo, al equipo desde el que estamos trabajando, es una característica bastante útil cuando estudiamos equipos conectados con aplicaciones como el TeamViewer, que se encuentran enlazadas a otros equipos, otros grupos de ordenadores u otras redes. Tiene un potencial alto de crecimiento

si se produce, como así parece, el despegue del uso de este tipo de tecnología.

Todo este grupo de herramientas anteriormente expuestas son de reciente implantación y crecimiento, es sencillo entender que si proliferan en la actualidad, su instalación y aprovechamiento gratuitos se irá restringiendo según vayan siendo más utilizadas y depuradas, es por otra parte, su evolución natural como software, por lo que esto sirve de guía de uso que se irá modificando según se vayan incorporando otras nuevas, esto debe servir como herramienta de comparación, para la búsqueda de nuevas aplicaciones que vayan surgiendo con el uso de nuevos equipos y necesidades.

MoonSolsDumpIt es una fusión de win32dd y win64dd en un único ejecutable para el usuario final. Con un doble clickeado en el ejecutable se generará una copia física de la memoria en la carpeta elegida. DumpIt es una herramienta versátil, rápida, cómoda y útil, debido a que es exportable y ejecutable a través de una memoria USB.

Para la realización del ejemplo del estudio de la memoria RAM utilizaremos el software Dumpit; como su nombre indica se trata de un volcado de la memoria en un archivo con extensión .raw, para eso se ejecuta el programa y realizamos la copia de manera muy intuitiva:

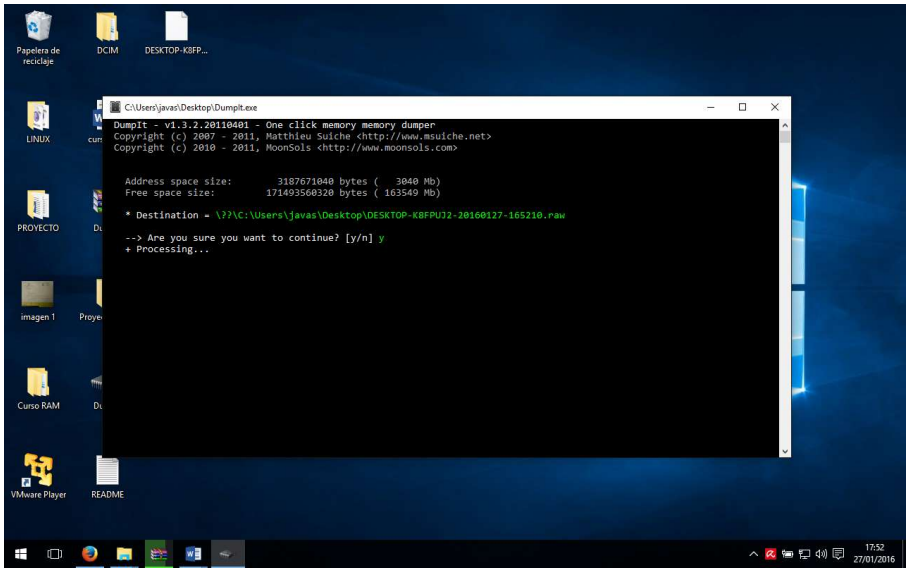

Figura 4-2: DumpIt

Una vez terminado el proceso se genera, como explicaba en líneas anteriores, un fichero .raw donde nosotros indiquemos en el equipo. Realizaremos una copia de ese mismo fichero y sobre esos ficheros .raw debemos realizar los dos HASH, que serán md5 y SHA1 (de la misma forma que hemos visto en apartados anteriores). Uno de los ficheros lo utilizaremos como siempre para el estudio y otro para posteriores comprobaciones, es importante mantener una dinámica estructurada de realización de estas herramientas, ya que, en posibles entrevistas, o en posibles preguntas en un juicio, si se realizan las acciones de manera estructurada, nunca habrá duda de la metodología a seguir, y de posibles errores en el desarrollo de nuestras funciones.

Realizado el fichero .raw se realiza el estudio de la imagen mediante la herramienta

Volatility, debido a que se trata de una herramienta que funciona en entorno Linux. O bien se trabaja con este sistema operativo, o bien proyectamos una máquina virtual desde la que lanzarla. En nuestro caso mediante el programa VMwarePlayer montamos una máquina virtual (por supuesto encontramos un extensísimo repertorio de montadores de máquinas virtuales por lo que podemos elegir el software con el que nos encontremos más seguros)

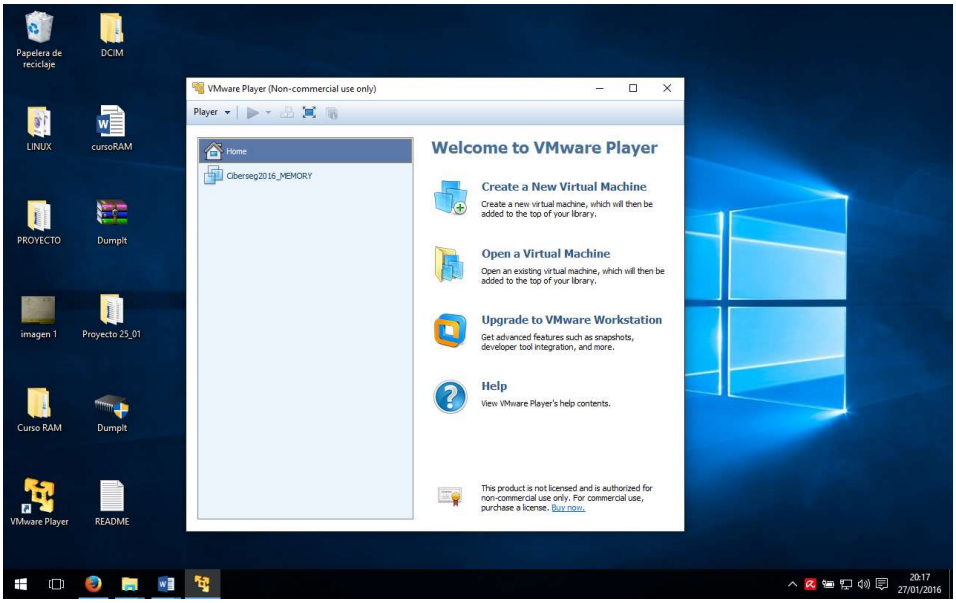

Figura 4-3: VMware Player

Allí abrimos nuestra máquina virtual, en este caso la he llamado Ciberseg2016_MEMORY y la ejecutamos,

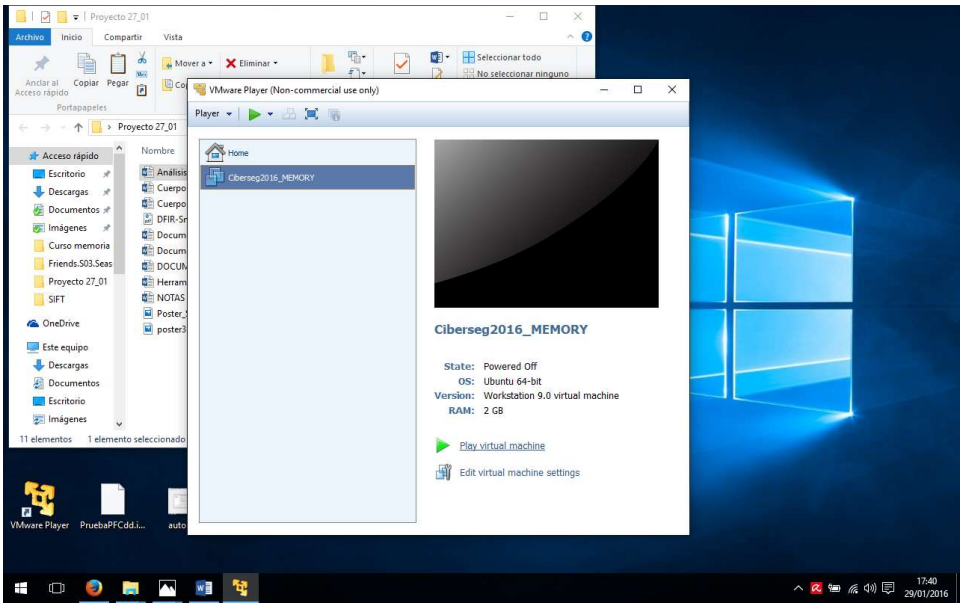

Figura 4-4: Máquina virtual

dentro del entorno Linux abrimos una terminal. Abierto el terminal, hacemos correr la herramienta Volatility, que se puede encontrar dentro del repertorio de apadrinamiento de software de google, https://code.google.com/archive/p/volatility/ , pero que como en ocasiones anteriores es de rápida evolución, como todo este tipo de herramientas, por lo que puede sufrir cambios y alteraciones, con lo que debemos quedarnos con el concepto y realizar las gestiones con los programas a nuestro alcance.

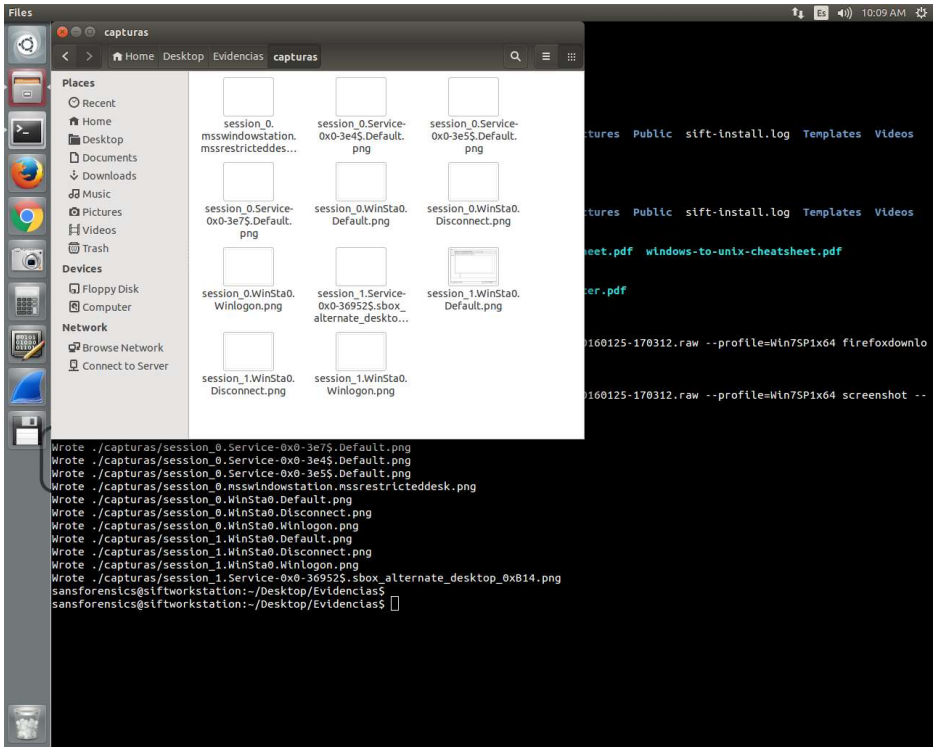

Figura 4-5: Volatility

Dentro de este software, podemos encontrar un gran abanico de herramientas para la obtención de todo tipo de evidencias y pruebas electrónicas, desde email, logs, páginas visitadas, lo recibido y mandado en los sockets de esas páginas, los strings (que son las cadenas de asteriscos que tapan las contraseñas), podemos incluso separar los datos mediante palabras clave tipo Facebook, y demás pestañas en un sinfín de características definidas, de hecho el concepto importante, es saber que este software, no solo coge grandes cantidades de memoria y las estudia, sino que separa proceso a proceso en particular, y realiza el estudio de todos los registros de cada uno de los procesos. Como comandos que podemos utilizar, de ejemplo nombraremos;

- :~$ vol.py -f ./PC-20160125-170312.raw --profile=Win7SP1x64 screenshot --dump-dir ./capturas/

Este comando mostrará las capturas de pantalla que se encontraban en la RAM a la hora de hacer la imagen, lo que puede ser muy útil en el caso de encontrar en la pantalla pruebas importantes para el desarrollo de nuestra peritación. Otra de las más llamativas

para la memoria;

- :~$ vol.py -f ./PC-20160125-170312.raw --profile=Win7SP1x64 memdump -p 3988 --dump-dir ./

Como se puede observar se estudian procesos por separado y se puede sacar la información de cada uno de ellos. Para esto hagamos un pequeño juego de imaginación e imaginemos la memoria como una tabla de datos en forma de pila en capas, donde la vamos separando cada capa y el programa coge las capas de cada proceso por separado para realizar el posible estudio. Una vez abierta esta herramienta podemos mediante la línea de órdenes del terminal, extraer una gran cantidad de información, incluso las propias imágenes que había en la pantalla en el momento de la realización de la imagen.

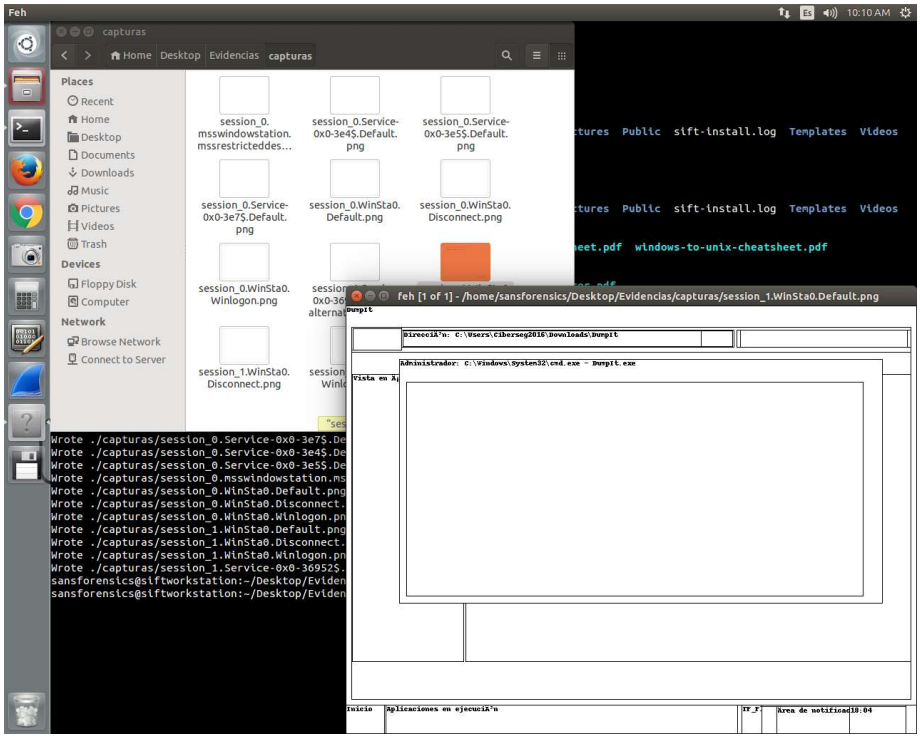

Figura 4-6: Contenido de la pantalla al realizar la imagen

Es aquí donde se pone de manifiesto la habilidad y la experiencia del perito para la minería de estos datos y poder sacar toda la información necesaria para el desarrollo de nuestra pericia. (http://www.volatilityfoundation.org)

Elegimos una herramienta muy potente para el análisis de la información de la memoria RAM en este caso ejecutaremos desde terminal el software, mejor en este caso es ponernos de administrador del sistema Linux con un su sudo, contraseña y llamamos al software como BEviewer; (puede sufrir variaciones el nombre del programa, dependiendo de las versiones, actualizar los nombre en su propia página web) Y realizamos el análisis con Bulk Extractor ViewerVersion 1.5.5 también presente en el grupo de estudio de Google:

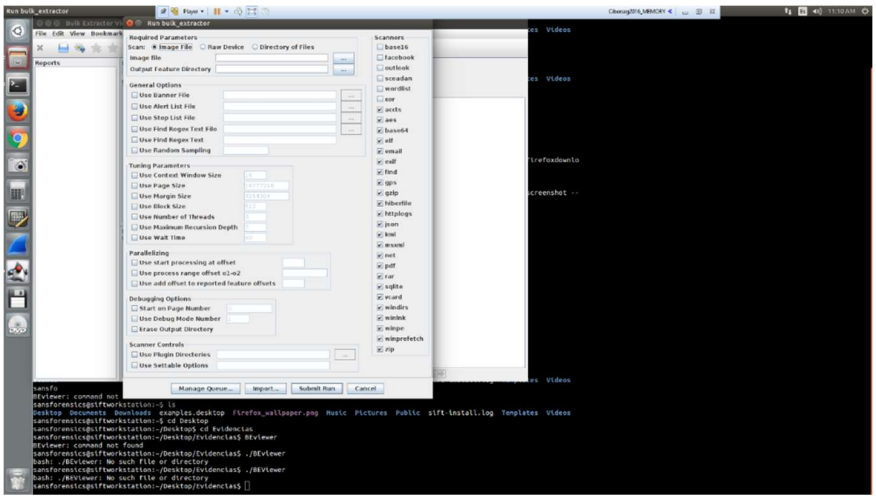

Figura 4-7: Campos de estudio de Bulk Extractor

Si nos fijamos detenidamente en la parte de la derecha de la ventana, vemos todos los datos que podemos disponer de un informe, dentro del repositorio de especificaciones del software podremos precisar más de cada uno de ellos, por defecto vienen marcados los más comunes pero podemos elegir que necesitamos o que vamos a estudiar, entre ellos los "AES" donde se encuentran los pares de datos de las contraseñas donde luego tendremos que realizar el conocido como "grep" en el mundo de los desencriptadores, de datos exif, páginas, url… en definitiva lo que busquemos. Se realiza el escaneo al archivo de la imagen:

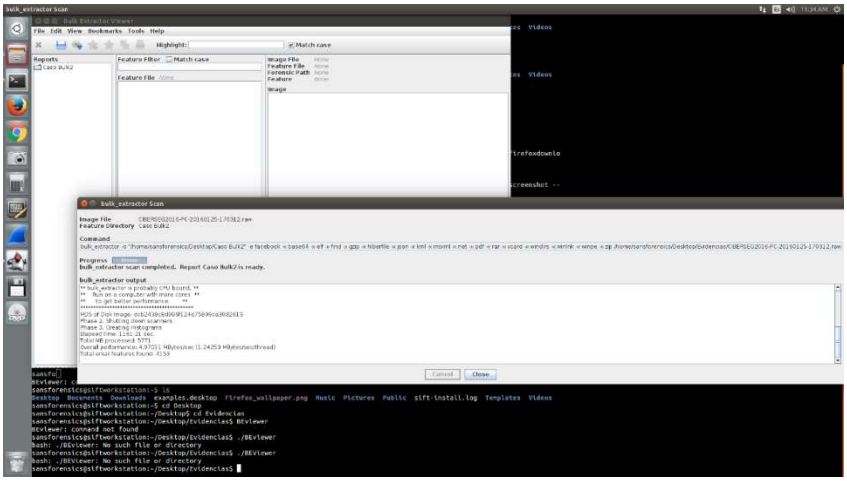

Figura 4-8: Bulk Extractor

Y se prosigue con el estudio de los resultados, se trata de unas ventanas desplegables, de muy fácil acceso y muy intuitivas, donde están separados por procesos o por motivos de búsqueda, pondremos varios ejemplos como los más vistosos dependiendo de los objetivos perseguidos, el primero es el de las claves de contraseñas con códigos AES (AdvancedEncryption Standard),

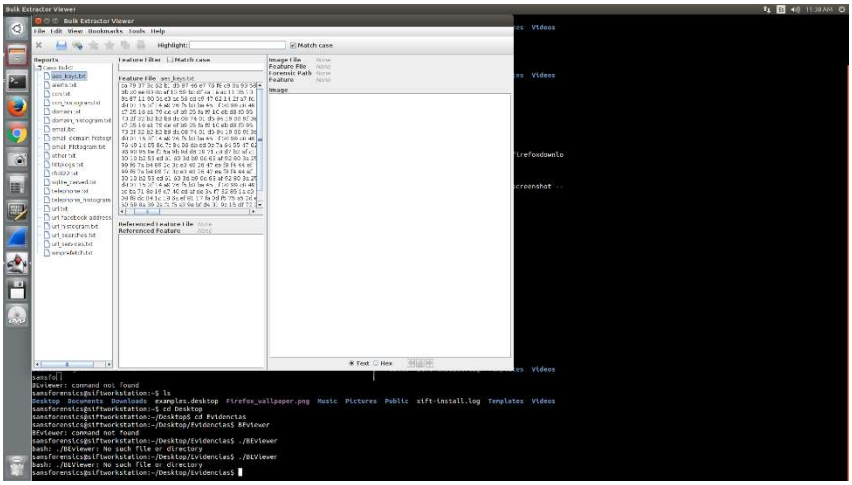

Figura 4-9: Códigos AES

O como ejemplo más vistoso incluso números de teléfonos consultados:

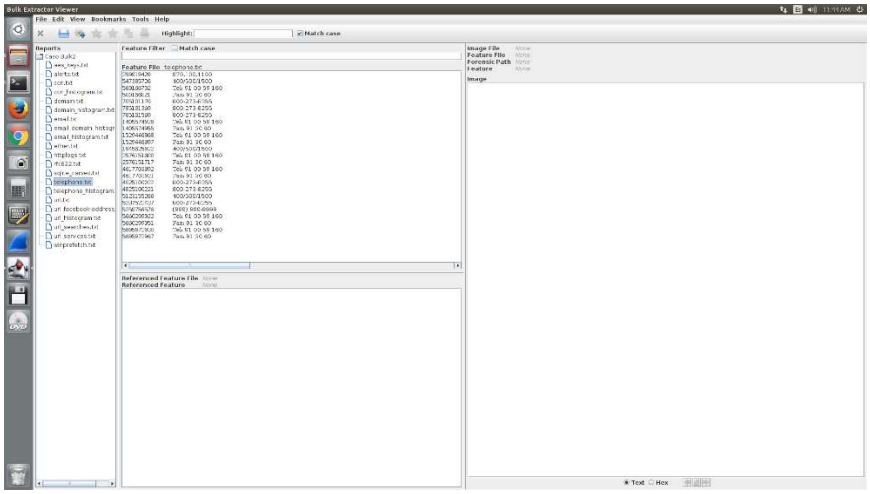

Figura 4-10: Teléfonos consultados

4.4 Proceso Forense peritación dispositivos móviles

La peritación de dispositivos móviles requiere una preparación cuidadosa debido a la gran complejidad y constante evolución que tienen estos dispositivos. Requiere del perito informático, un desarrollo constante de sus habilidades forenses mediante la preparación especializada y el seguimiento de las últimas actualizaciones del sector móvil. Realizaremos a modo de esquema una serie de pasos que deben ser tomados en cuenta para la realización de la peritación, sin olvidar que, a la hora de la realización del mismo, se debe seguir la propuesta antes expuesta para la elaboración de la peritación. Debido a la singularidad de este dispositivo electrónico realizaré una línea de seguimiento del trabajo que se debe realizar en la pericia, la mayoría de los conceptos han sido desarrollados y comentados en apartados anteriores, pero es importante definir una estructura de trabajo, que será:

1. Admisión
    - α Estudio del recibo de la evidencia digital y el requerimiento.

2. Catalogación
    - α Examen de las características legales del requerimiento.
    - α Identificación de las metas de nuestro objetivo.
    - α Estudio de los datos a encontrar y de relevancia.
    - α Realización de estudio de la capacitación de información para su desarrollo.

3. Preparación
    - α Preparación de herramientas y protocolos a desarrollar en la peritación.
    - α Preparación del equiponecesario para desarrollar la petición.
    - α Revisión de las herramientas que debemos utilizar, valorando su eficacia y su actualización.
    - α Preparación de la legislación que va afectará al requerimiento.

4. Protección de datos
    - α Proteger las evidencias digitales de posible deterioro o pérdida.
    - α Prevenir la destrucción remota de datos.
    - α Aislar los dispositivos electrónicos de conexiones como redes, Wi-Fi

5. Proceso
    - α Adquisición forense de datos.
    - α Análisis forense de la adquisición.
    - α Realizar escaneado por si se descubre conexión exterior o malware.

6. Comprobaciones
    - α Comprobaciones de la adquisición de datos forenses.
    - α Comprobación y validación de los datos encontrados y analizados.

7. Documentación
    - α Realizar la peritación
    - α Argumentar la peritación y el motivo de selección de esa información.

8. Presentación de peritación
    - α Exhibición de pruebas forenses encontradas
    - α Conclusiones y presentaciones en formatos universales

Una vez realizada la primera parte de estudio, y recordando la manera de proceder con el dispositivo en vivo, estudiado en apartados anteriores, nos encontramos ante el dispositivo móvil y procederemos a su análisis. Para eso debemos extraer los datos del terminal, será una tarea que depende en gran medida de las distintas posibilidades en las que nos lo encontremos. A modo de esquema analizaremos las distintas posibilidades y posteriormente realizaremos el desarrollo de las mismas.

4.5 Desbloquear un código de patrón o contraseña en un teléfono móvil sin pérdida de datos

La nueva implantación de códigos para proteger la información del equipo hace que el uso de herramientas para poder acceder a ella, eludiendo o recuperando esos códigos sea uno de los objetivos en el desarrollo de nuestra función. En este apartado estudiaremos los métodos que tenemos a nuestra disposición para el desbloqueo de los equipos, diferenciando por las dos grandes ramas, los dispositivos iOS y los Android. Definiremos los métodos más fiables y de uso especializado para realizar el desbloqueo de un terminal, mediante la consecución o inhabilitación de su código de patrón o contraseña. Como siempre tenemos que tener presente a la hora de elegir una de las opciones, comenzaremos por la menos intrusiva al terminal, acabando con la más lesiva al software inicial de nuestro dispositivo.

Dispositivos Android

4.5.1 Método Android SDK

Desbloqueo del terminal Android sin pérdida de datos

Realizar el desbloqueo de un terminal Android a medida que va evolucionando el software de los terminales, va haciendo que las posibilidades sean cada vez menos numerosas, más restrictivas y con una clara evolución a la eliminación de esas llamadas puertas traseras de datos, que fueron diseñadas en su origen para la protección en caso de pérdida o mal funcionamiento, que ahora son utilizadas como una auténtica grieta de seguridad. Para la realización de este método deberemos seguir los siguientes pasos:

1. Instalación de Android SDK y SDK Tools

    - Descargar e instalar Android SDK Tools.
    - Descargar e instalar los paquetes del programa Android SDK Platform-tools

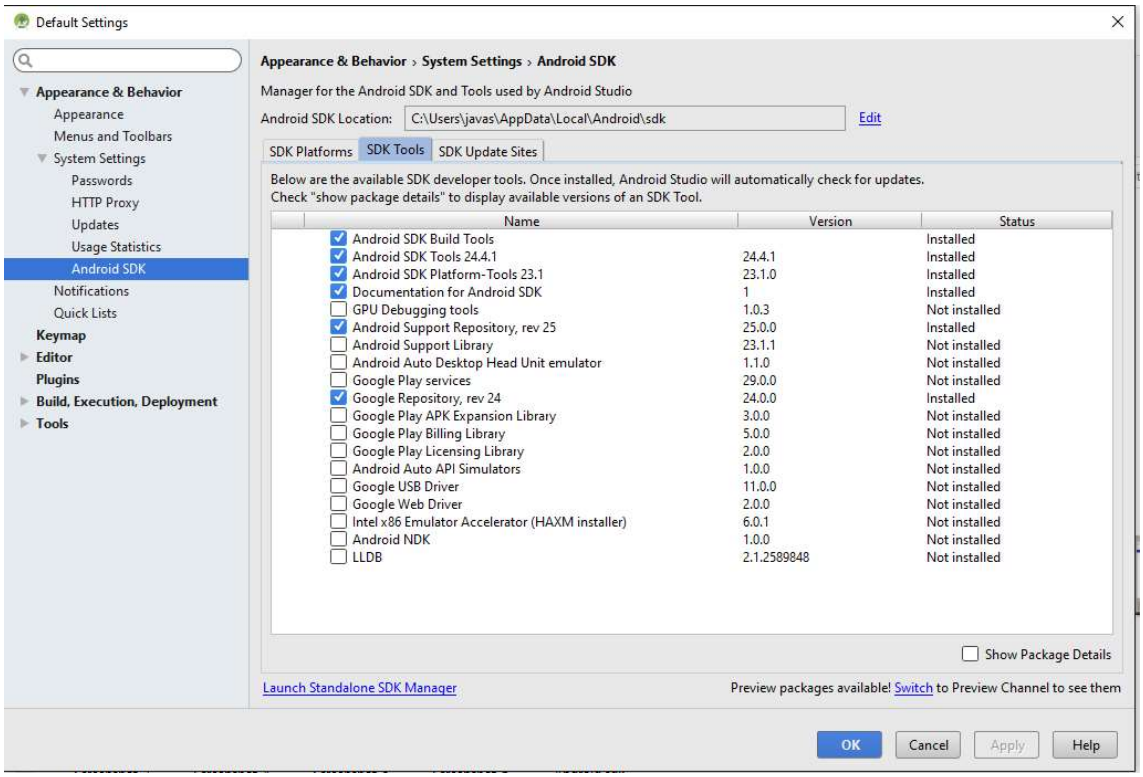

Figura 4-12: Android SDK Manager

*Destacar que para que este método pueda ser ejecutado, el terminal en su origen debe de tener activada el USB Debugging en el software del dispositivo. Y deben estar instalados todos los drivers correctos del dispositivo en el ordenador. Las páginas oficiales de los terminales disponen de este software para su uso, por lo que una vez iniciada la peritación el ordenador debe disponer de los drivers propios del terminal a estudiar

En el Android SDK realizamos los siguientes pasos:

2. Conectar el terminal con el equipo forense mediante USB.
3. Abrir una terminal y en la carpeta donde se encuentra instalado Android SDK Tools Users>> App Data >> Local >> Android >> Android-SDK >>Platform-Tools y realiza click con el botón de la derecha del ratón sobre la opción de la ventana que se despliega siguiente “open command window here”.

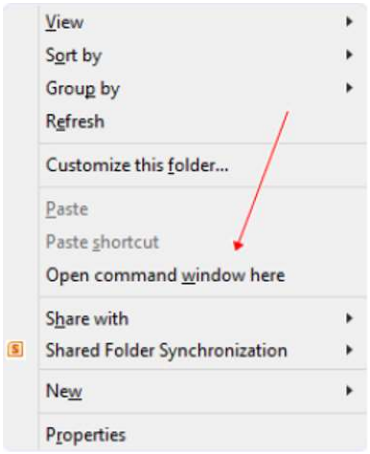

Figura 4-13: Pantallazo opciones de Linux al pulsar botón derecho

*En el caso de Windows abrir un terminal y pegar el camino donde tenemos la carpeta Platform-tools en la cabecera del buscador de archivos, o en cualquier carpeta, en el caso del equipo donde estoy trabajando en estos momentos seria la frase a copiar: C:\Users\javas\AppData\Local\Android\sdk\platform-tools

4. Se abrirá una ventana con un terminal para escribir sobre línea de comandos:

   a. Para comprobar si el terminal se encuentra conectado al equipo:

      i. adbdevices

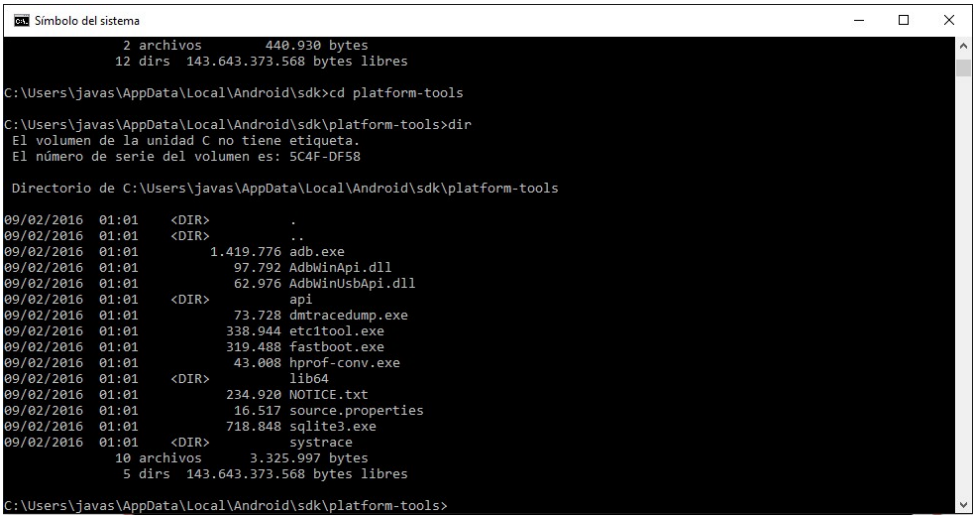

Figura 4-14: Terminal con Android SDK Platform-tools

ii. Se debe introducir esta línea de código:

adb shell cd /data/data/com.android.providers.settings/databases sqlite3 settings.db update system set value=0 where name='lock_pattern_autolock';update system set value=0 where name='lockscreen.locketpermanendoutly';.quit

iii. Podremos realizar esta comprobación, especialmente si el anterior comando no ha funcionado:

adb shell rm /data/system/gesture.key

5. Una vez realizados estos pasos, se reinicia o se recarga la aplicación del terminal Android y el patrón de desbloqueo aparecerá desactivado. *Exponer como siempre que estas líneas de datos pueden sufrir ligeras modificaciones dependiendo del tipo de software o del tipo de dispositivo. Para solucionar este punto se debe realizar una búsqueda técnica de los comandos a utilizar y realizar el mismo proceso seleccionado en este ejemplo.

4.5.2 Método Aroma File Manager

Desbloqueo del terminal Android sin pérdida de datos

Para la realización de este método deberemos seguir los siguientes pasos:

1. Instalación de Aroma File Manager

   - Descargar e instalar Aroma File Manager
   - Tarjeta de memoria para dispositivo Android
   - Desbloqueo de patrón de desbloqueo o código de desbloqueo

Figura 4-15: AROMA Filemanager

2. Cargar en la tarjeta de memoria SD del dispositivo el Aroma File Manager e insértala en el dispositivo.

3. Abre Stock Recovery Mode con el reinicio de tu dispositivo Android y presiona el botón de apagado y el botón de subir volumen de forma simultánea. *Esta es la forma más común de realizarlo, pero depende del dispositivo y de los botones del mismo, se recomienda que en caso de duda se verifique que botones mantener pulsados para la realización de este paso.

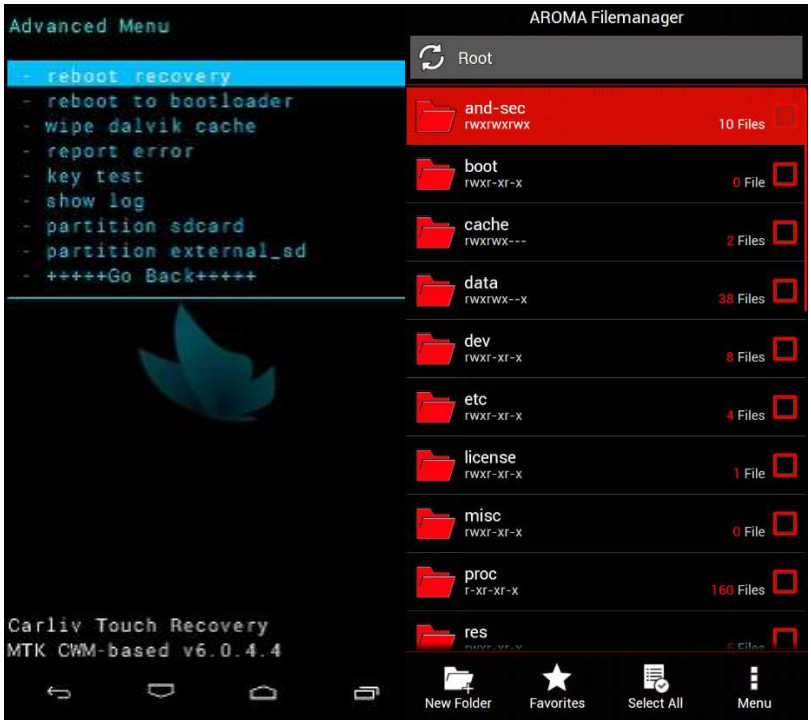

Figure 4-16: Distintos modos de Aroma File Manager

4. Una vez dentro del modo de recuperación del dispositivo, con los botones más y menos, muévete por la pantalla.

5. Se debe pulsar en “Install Zip from SD Card” y dentro de ella, instalar el “Aroma File Manager” desde la SD card.

6. Se instala el archive y este abrirá en modo de recuperación el dispositivo.

7. Navega por las funciones de Aroma File Manager ensettings ve hacia “Automountalldevicesonstart” selecciónalo y posteriormente o bien se cerrará el equipo o apágalo.

8. Se repiten los pasos del 4 al 5 de Nuevo.

9. Después de esto abre de nuevo“Aroma File Manager”.

10. Ahora selecciona la carpetaData Folder>>SystemFolder y encuentra “gesture.key” o “password.key” que son los códigos de bloqueo o el patrón de desbloqueo.

11. Copia en un archivo en el equipo los datos existentes en “gesture.key” o “password.key” para adjuntarlos como prueba en la pericia.

12. Borra los archivos “gesture.key” o “password.key” y cierra el “aroma file manager”.

13. Reinicia el dispositivo Android. Y se comprobará que el dispositivo carece de código de bloqueo o patrón de desbloqueo. En el caso en el que aparezca la pantalla de desbloqueo, pulsa cualquier código o patrón, y se podrá entrar en el dispositivo. En caso contrario, repite los pasos. Y ya se tendrá acceso a la información del terminal para iniciar la pericia.

4.5.3 MétodoAjustes de fábrica

Desbloqueo del terminal Android con pérdida de datos

En el caso de no funcionar ninguno de los métodos propuestos en este Proyecto, se podría realizar el siguiente paso, pero en este caso, no sólo varía el software del dispositivo, sino que también nos exponemos a la pérdida de datos en el terminal, ya que cuando se reinstala el dispositivo a los ajustes de fábrica para su realización puede pisar una cantidad indeterminada de datos. El resto posteriormente podrán ser recuperados con las herramientas forenses de análisis de datos borrados o las de rescate de datos. En este caso la metodología es muy sencilla y se realiza de la siguiente forma:

1. Apaga el dispositivo Android bloqueado.

2. Reinicia el dispositivo en modo de recuperación o “RecoveryMode” usando las diferentes formas para realizarlo dependiendo del modelo, proponemos como antes hemos expuesto la forma más común que será pulsar de manera simultánea los botones de encendido y subir volumen.

3. Una vez abierto el Modo de recuperación o “RecoveryMode”

    - Seleccionamos restablecer ajustes de fábrica o “wipe data/factory reset”
    - Seleccionar “wipecache partition” para limpiar los datos de la caché

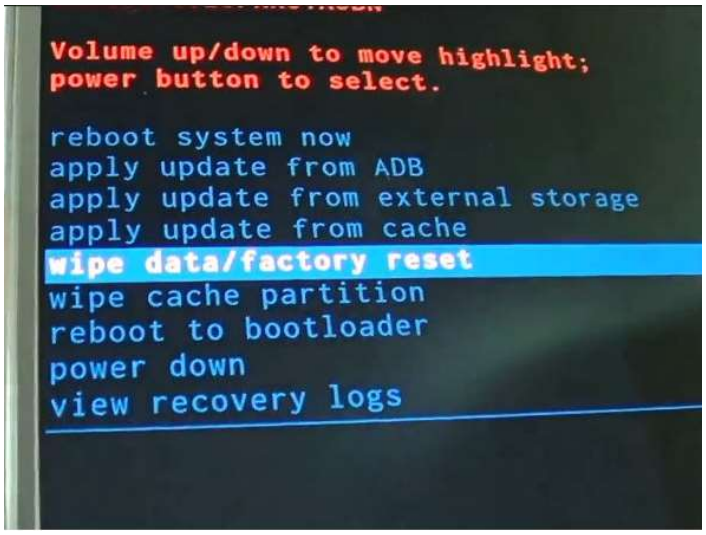

Figure 4-17: Modos recuperación de Android

4. Inicia el dispositivo y realiza un estudio de la imagen de la memoria interna para rescatar y recuperar todos los datos del equipo.

4.6 Análisis del dispositivo

Una vez accedido al terminal iniciamos la comprobación de tarjetas de memoria externa, que serán estudiadas como elementos paralelos, mediante el procedimiento anteriormente explicado. Con la información contenida en el dispositivo accedido se opera de la misma forma que si fuera con una memoria externa, mediante la realización de una imagen y estudiando cada parte de la misma. Esto supone numerosas variaciones con respecto a un dispositivo de almacenamiento tradicional, ya que los móviles son verdaderos ordenadores de bolsillo que contienen en el caso de la mayoría de las personas un verdadero resumen de sus vidas y la información que contiene es rica y variada.

Para la realización de un estudio pormenorizado de la información encontrada en un terminal debemos reseñar una serie de puntos que tienen especial relevancia,

4.7 Estudio Redes Sociales

Para el estudio de las redes sociales debemos mencionar una de las herramientas forenses de mayor crecimiento en la actualidad y que viene ya incorporada en KaliLinux 2.0. que es Maltego, un software creado por Paterva. Está diseñado como herramienta de inteligencia forense y de software libre. Maltego está enfocado para el descubrimiento y análisis de información mediante minería de datos, en redes abiertas para crear en forma de gráficos el listado de conexiones de cualquier dato a buscar. Maltego permite la creación de una búsqueda de entidades representando cada nexo de unión entre ellas en el gráfico, así podremos analizar en las relaciones entre distintas personas, grupos, empresas, sitios webs, dominios, diferente infraestructura web e incluso las diferentes cuentas en redes sociales, como pueden ser, Instagram, Twitter, Facebook…Es a día de hoy la herramienta más eficiente y utilizada para la búsqueda de identidades y relaciones entre los diferentes tipos de entidades en internet. Relacionando cada punto del diagrama con cualquiera de la información que disponga la red de ese punto, que como podemos entender, ese "punto" puede ser cualquiera de nosotros.

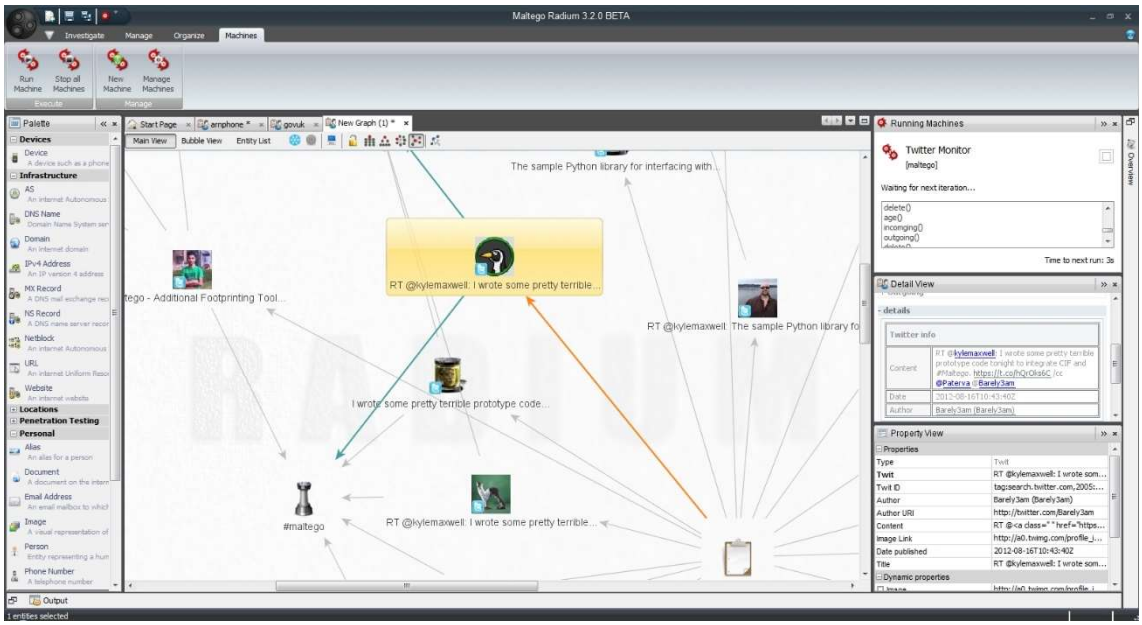

Figure 4-18: Maltego

Las conversaciones o intercambio de archivos en las redes sociales deben ser autentificados e identificados en el desarrollo de nuestra función si fuera necesario. Para este tipo de efectos debemos estar familiarizados con el concepto de IDs internos, el id de Facebook es un número que identifica de manera inequívoca a usuarios, imágenes, chats, sesiones, grupos, en definitiva identifica cada acción que se produce en la red social, y lo que hacen es registrar cada movimiento de un usuario. Destacar que el target_id corresponde con la identificación de facebook interna sobre los chats mantenidos por un usuario. Por

ejemplo, la URL de un usuario de Facebook sería el siguiente https://www.facebook.com/659255024. El número que aparece a la derecha es el id que identifica al usuario, con ese número puede ser identificado, para buscar ese número hay numerosas páginas (por ejemplo: http://findmyfbid.com/) con las que buscar el id, para realizar posteriormente búsquedas técnicas en otras plataformas o en otras aplicaciones como el comentado Maltego para la obtención de los datos requeridos. Con este dato id, se puede poner en contacto con la propia página de Facebook para autentificar que ese id pertenece a la persona de la que requerimos información.

4.8 Peritación Correo electrónico

4.9 Nube – Cloudcomputing

4.10 PROCESO DE ROOTEADO DE EQUIPOS

Pasaremos ahora a comentar como realizar el acceso al terminal, cuando no se disponen de las contraseñas de acceso mediante los root moderado y root fuerte. En el caso del root moderado del terminal para el acceso a los datos del mismo se tiene que realizar mediante el rooteo del equipo o el jailbreak del mismo. Explicar que las aplicaciones y métodos existentes para Rootear Android son muy diversas, destacaremos Kingroot**.** Se trata de la aplicación con mayor crecimiento en la actualidad para los dispositivos que cuenten con sistema Android.

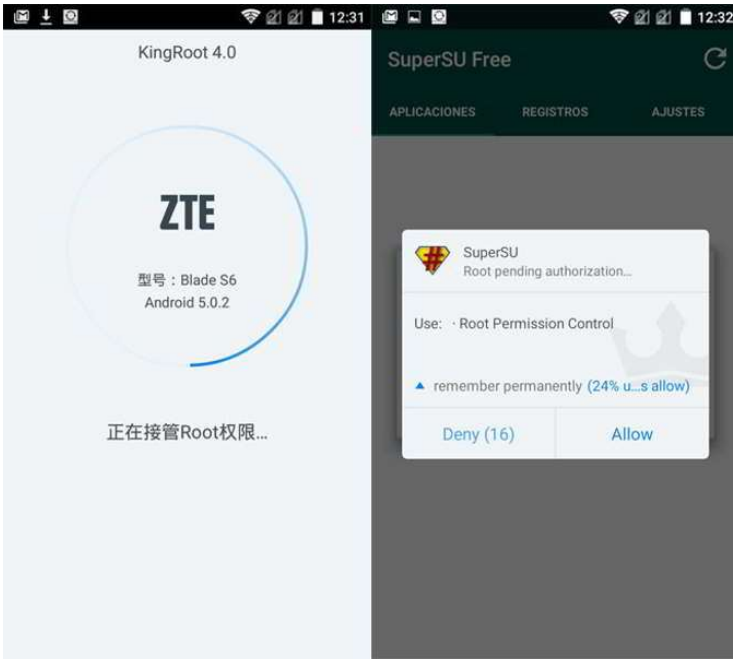

Figure 4-20: KingRoot 4.0

Para los sistemas de Apple debemos utilizar el rooteador conocido como jailbreak para sistemas iOS. Es importante distinguir entre las dos acciones ya que el jailbreak no es un root puro, ya que su estructura está diseñada para liberar el dispositivo del control de Apple, en cambio el root puro consigue que el dispositivo obtenga los permisos de súper-usuario, palabra utilizada ya que la línea de código es su para identificarse como tal, también llamado administrador. Este permiso o nivel en el sistema operativo es útil para realizar un gran número de acciones sobre el software del dispositivo para su posterior estudio. Una vez realizado sobre el equipo cualquiera de estas dos acciones, dependiendo del modelo, se podría acceder a la información contenida en el mismo, realizando así la peritación siguiendo el esquema planteado y realizando las comprobaciones estudiadas en esta parte del proyecto.

Figure 4-21: JailBreak para iOS 9.2

Por último comentar destacar que cuando nos encontremos ante un terminal con una codificación muy fuerte, que no sea posible de utilizar ninguno de los métodos arriba dispuestos, nos encontramos ante la única solución de realizar lo que se conoce como rooteo fuerte, esto es, extraer la información existente en el dispositivo realizando un volcado bit a bit de los datos mediante software especializado que posteriormente realizará un plasmado de la información resultante mediante la obtención de informes. El UFED de Cellebrite es una herramienta forense diseñada para la extracción de datos en los dispositivos electrónicos móviles. Es una herramienta expresamente creada para smartphones y dispositivos PDA. Es capaz de generar informes claros y concisos en formato HTML y XML para consultas en procesos judiciales y clonar el ID de la tarjeta SIM para trabajar con un terminal sin conectarlo a la red. Se trata de la herramienta de más fuerte introducción en el mercado, con unos resultados destacados, y es la herramienta más utilizada en los laboratorios profesionales.

Figure 4-22: UFED deCellebrite

4.11 ARCHIVOS A EXTRAER EN PERITACIÓN FORENSE DE DISPOSITIVOS MÓVILES

Una vez accedido al terminal por cualquiera de los medios reseñados, se debe seguir una línea de trabajo estructurada y ordenada, para ello diferenciaremos entre los dos grandes grupos de elementos recibidos como son:

4.11.1 MOVILES iOS

Donde el orden de adquisición de la información en los equipos debe ser la siguiente:

- Adquisición Backup terminal
- Adquisición desde Backup de iTunes
- Adquisición desde icloud
- Adquisición desde copia bit a bit por falta de contraseña
- Adquisición desde la imagen

Una vez realizada la imagen del dispositivo con sistema iOS, estos son los distintos archivos que debemos estudiar para el desarrollo de la pericia, y las carpetas del directorio raíz donde se encuentran:

DISPOSITIVOS IOS	
ARCHIVOS DE INTERÉS	DESCRIPCIÓN
mobile/Library/DataAccess	Cuentas de información usadas por las aplicaciones del usuario (Email, #...)
Var/mobile/Library/Keyboard	dynamic-text.dat
DCIM/100APPLE Folder	Fotos Creadas por el usuario
/private/mobile/var/applications	Carpetas de las aplicaciones
Media/PhotoData/*	Fotos
Library/Cookies/Cookies.binarycookies	Actividad del navegador Safari
Library/Preferences/com.apple.assistant*	Siri
Library/Preferences/com.apple.imservice*	SMS, iMessage&FaceTime
Media/Recordings/*	Memoria de notas de voz
Library/Voicemail/*	Voicemail
Library/SpringBoard/LockBackgroundThumbnail.jpg	Fotos de interés
Library/SpringBoard/HomeBackground.cpbitmap	Fotos de interés
Library/SpringBoard/HomeBackgroundThumbnail.jpg	Fotos de interés
Library/SpringBoard/LockBackground.cpbitmap	Fotos de interés

Tabla 4-2: Guía de archivos a consultar en una imagen a sistema iOS

4.11.2Análisis forense de Android

La información que se debe extraer para el análisis de dispositivos Android sigue a grandes rasgos el siguiente sistema de archivos:

- SDK
- Android Internals
- Sistema de ficheros YAFFS2
- Dalvik VM frentea ART

De la imagen de la información de los móviles en los que se está realizando la peritación debemos obtener los datos que se encuentran en estas carpetas o archivos:

ANDROID	
ARCHIVO	**DESCRIPCIÓN**
Root/Property/persist.sys.timezone	Zona horaria
Root/Property/netpolicy.xml	Política de zona horaria
com.android.providers.contacts/contacts2.db	Historico de llamadas
com.android.providers.contacts/contacts2.db	Información de los logs
com.android.providers.contacts/contacts2.db	Contactos
com.android.providers.telephony/mmssms.db	SMS/MMS
com.google.android.apps.maps/da_destination_history	Histórico de mapas
com.google.android.apps.maps/search_history.db	Mapas utilizados
com.android.email/webviewCache.db	Historial de internet
com.android.browser/databases/Browser.db	Historial de internet
com.android.browser/databases/webview.db	Historial de internet
com.android.browser/databases/webviewCache.db	Historial de internet

Tabla 4-3: Guía de archivos a consultar en una imagen a sistema Android

ANDROID	
ARCHIVOS	**DESCRIPCIÓN**
com.android.browser/app_databases/http_www. google.com_0.localstorage	Historial de internet
com.android.browser/app_geolocation/GeolocationPermissions.db	Historial de internet
/data/com.google.android.gm/databases/<mail-name>.db	Gmail

Tabla 4-4: Guía de otros archivos a consultar en una imagen a sistema Android

4.11.3 BLACKBERRY

Se realizan tablas de archivos de imágenes de dispositivosBlackberry, debido a que en la actualidad, un movimiento cultural está volviendo a utilizar este modelo de dispositivo, por lo que se adjunta también las tablas de los directorios. Siendo estos los distintos archivos que debemos estudiar para el desarrollo de la pericia, y las carpetas del directorio raíz donde se encuentran:

BLACKBERRY	
BASE DE DATOS	**INFORMACIÓN**
Address Book	Contactos del usuario con fotos si están indexadas
Attachment Data	Archivos adjuntos descargados en el dispositivo
Auto Text	Diccionario del usuario del dispositivo
BBGroups	BlackBerry Messenger Groups
Browser Bookmarks	Páginas web marcadas como favorito
Browser URLs	URLs utilizadas por el usuario
Folders	Carpetas de mensajes creados por el usuario
Location-BasedServices	Caminos "Tracks" usados por el usuario con su BES
Messages	Mensajes del dispositivo
MMS Messages	Mensajes MMS
PhoneCall Logs	Histórico de llamadas actual
PhoneHistory	Histórico de llamadas desde inicio de memoria
PIN Messages	Mensajes PIN

Tabla 4-5: Guía de archivos a consultar en una imagen a Blackberry

BLACKBERRY	
BASE DE DATOS	**INFORMACIÓN**
PurgedMessages	Información relative a los mensajes borrados
RMS Databases	Base de datos de las aplicaciones instaladas
Saved Email Messages	Correos electrónicos del dispositivo
SMS Messages	Histórico de SMS

Tabla 4-6: Guía de otros archivos a consultar en una imagen a Blackberry

De cada uno de estos archivos o carpetas se debe seleccionar la información necesaria para desarrollar las funciones encomendadas.

5 Conclusiones

Referencias

1. AccesData. FTK Forensics Toolkit. [Software] http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk

2. Agencia Española de Protección de Datos [En línea] https://www.agpd.es/

3. Ahmad Amarullah. Aroma file manager. [Software] https://github.com/amarullz

4. Andrey Bogdanov, Dmitry Khovratovich, y Christian Rechberger. (2013) Cryptanalysis of the Full AES; Microsoft Research Redmond, USA; ENS Paris, Francia.

5. Apple. iCloud: Borrar tu dispositivo. [En línea] https://support.apple.com/kb/PH2701?locale=es_ES&viewlocale=es_ES

6. Associazione DEFT. DEFT. [Software] http://www.deftlinux.net

7. BrowserSpy (Microsoft Corporation, 2011) [Online] http://browserspy.dk/

8. Brian Carrier. Sleuthkit. [Software] http://www.sleuthkit.org/sleuthkit/index.php

9. Brian Carrier. Autopsy. [Software] http://www.sleuthkit.org/autopsy/index.php

10. Buscador de jurisprudencia [En línea] http://www.poderjudicial.es/cgpj/es/Servicios/Jurisprudencia/

11. Cegarra Sánchez, José (2011) “Metodología de la investigación científica y tecnológica” Madrid, Dias Santos

12. Cellebrite GmbH. Central Europa. [En línea] http://www.cellebrite.com/Mobile-Forensics

13. Cuerda Arnau, M.L. (2014) “Menores y redes sociales: protección penal de los menores en el entorno digital”, Cuadernos de Política Criminal

14. Cyrus Farivar. (2011) "The Internet of Elsewhere: The Emergent Effects of a Wired World". Rutgers University Press

15. Dan Hersam. Snap MD5. [Software] http://dan.hersam.com/software/snap-md5/

16. De Luz, Sergio (2010) “Criptografía: Algoritmos de autenticación (hash)”. Redeszone.

17. Dolev, D.; Yao, A. C. (1983), "On the security of public key protocols", IEEE trans. on Information Theory, IT-29: 198–208

18. e-fense. Helix. [Software] http://www.e-fense.com

19. Enrique Arellano, Luis (2012)"La cadena de Custodia Informático Forense" ACTIVA

20. Ernesto Martínez de Carvajal Hedrich (2012), "Informática Forense - 44 casos reales".

21. Fowler, Geoffrey A. (2012). "Tor: An Anonymous, And Controversial, Way to Web-Surf - WSJ.com". Online.wsj.com.

22. Gándara Trueba, Esteban. (2010) “Inhibidores de frecuencia”. Informe UCSP nº: 2010/009. Dirección general de la policía y de la guardia civil.

23. Google. Ayuda de cuentas google. [En línea] https://support.google.com/accounts/answer/3265955?hl=es

24. González Rus, JJ (2006) “Los Ilícitos en la red: hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes”

25. Guidance Software, Inc. Encase. [Software] http://www.guidancesoftware.com

26. Instituto SANS. SIFT [Software] http://digital-forensics.sans.org

27. IntelliJ, JetBrains. Apache. Android Studio SDK [Software] http://developer.android.com/intl/es/sdk/index.html

28. Kuhlee and Voelzow (2012), Computer Forensik Hacks, O’Reilly, ISBN 978-3-86899-121-5, http://www.forensikhacks.de

29. LiveHttpHeaders. Es un sitio web donde podemos ver los encabezados que nuestro navegador envía en una solicitud HTTP. http://livehttpheaders.mozdev.org

30. M. Bellare, P. Rogaway, D. Wagner,A (2003) “Conventional Authenticated-Encryption Mode“

31. Matellanes Rodríguez, Nuria (Julio 2008) Vías para la tipificación del acceso ilegal a los sistemas informáticos. Profesora de Derecho Penal de la Universidad de Salamanca. Revista Penal, n.º 22.

32. Mendo Estrella, A. (2014) “Delitos y Redes Sociales: mecanismos formalizados de lucha y delitos más habituales. El caso de la suplantación de identidad”, Revista General de Derecho Penal, 2014

33. MH Themes. (2016) unlockicloud.info “How to find passcode and icloud password with Elcomsoft”

34. MihirBellare, Phillip Rogaway, y D. Wagner. EAX (2003) “A conventional authenticated-encryption mode”. IACR Cryptology

35. Miró Llinares, F. (2014) “Cibercrimen y vida diaria en el mundo 2.0. Las teorías del crimen y la oportunidad en ámbitos específicos” Centro Crímina para el Estudio y Prevención de la Delincuencia, Universidad Miguel Hernández de Elche

36. Nanni Bassetti. CAINE Computer Aided Investigative Environment [Software] http://www.caine-live.net

37. NetRivet. Identifica a usuarios Facebook. [En línea] http://findmyfbid.com/

38. Noticias jurídicas [En línea] http://noticias.juridicas.com/

39. Paladin Live-CD, Sumuri Forensics, [Software] https://www.sumuri.com/

40. Peter Wayne, (2009) "Disappearing Cryptography: Information Hiding: Steganography & Watermarking". Morgan Kaufmann

41. Rafael López Rivera (2012), "Peritaje Informático y Tecnológico".

42. Santoku Linux CE [Software] https://santoku-linux.com/

43. Stevens, Marc (2012) “Cryptanalysis of MD5 & SHA-1”, CWI, Amsterdam

44. X-Ways Software Technology AG. X-Ways. [Software] http://www.x-ways.net/forensics/index-m.html

HERRAMIENTAS FORENSES

La realización de peritaciones informáticas se basa en herramientas forenses de análisis y estudio de datos. Como hemos ido observando a lo largo del proyecto podemos observar que son numerosas y que se encuentran en una continua evolución, ya que muchas dependen en gran forma de la legislación y sobre todo del software al que se encuentran realizando el desarrollo. Al tratarse en su mayoría de herramientas generadas por empresas independientes a los desarrolladores de los dispositivos electrónicos, hace que estas herramientas sean a veces de uso efímero, como lo fueron en su día, los softwares de estudio de la aplicación WhastApp en sus primeras versiones, donde ni los datos, ni las conexiones, ni el almacenamiento, ni las conversaciones eran encriptadas. Aun así, debido al enorme incremento de utilización de este tipo de herramientas, y al gran número de usuarios interesados en software mucho más especializado, hace que muchas de estas herramientas se encuentren en el mercado de manera libre o comercial desde hace años. En esta parte del trabajo de describirá y enumerará las herramientas usadas para los ejemplos de peritaciones y las análogas que podrían haber sido utilizadas:

A

AUTOPSY Y SLEUTH KIT

Sleuth Kit es de Conjunto herramientas de análisis forense de libre distribución. Autopsy es el interfaz gráfico para TheSleuth Kit. También de libre distribución.

Figura H-1: Autopsy de Sleuth Kit

AutopsyForensic Browser es una interfaz gráfica para las herramientas de investigación digital Sleuth Kit. Se ejecuta principalmente sobre plataformas Linux. Su filosofía de funcionamiento se basa en dos tipos de análisis: análisis de sistema muerto (se utiliza la herramienta desde otro sistema operativo y con el sistema a investigar en su soporte sin cargar) o análisis de sistema vivo (cuando se está analizando el sistema sospechoso mientras está funcionando).

C

CAINE

Caine (ComputerAidedInvestigativeEnvironment) Es una distribución Live CD basada en Ubuntu. Ofrece un completo entorno forense, de modo que integra herramientas de software existentes, proporcionando una interfaz gráfica amigable. Entre otras posibilidades, permite clonar y montar unidades, manipular volúmenes de diferentes sistemas operativos (Windows, Unix, Macintosh), recuperar archivos o borrarlos de forma segura, recuperar unidades de disco, auditar los dispositivos conectados a la red (incluso determinando qué puertos tienen abiertos), editores hexadecimales, recuperar archivos de imágenes y de vídeo, recuperar contraseñas, examinar el contenido de los archivos de respaldo que los móviles Iphone dejan en el disco, recuperar datos deDVDs… Además, incluye a otras herramientas como Autopsy.

Figura H-2: CAINE

Cellebrite mirar UFED (Universal ForensicExtractionDevice)

Cifrado “Herramientas”

Las herramientas de cifrado de datos más destacadas según su sistema operativo son:

- Bitlockeren Windows 7
- FileVaultenMacOS X
- eCryptFS en distribuciones Linux.
- Para los sistemas operativos más antiguos es posible instalar:
    - Un software de cifrado como TrueCrypt o PGP.

COFFE

COFEE es una herramienta gratuita distribuida por Interpol para Fuerzas y Cuerpos de Seguridad y es de las más conocidas. Esta herramienta sirve para analizar dispositivos con sistema operativo Microsoft Windows. Esta herramienta incluye más de 100 tests que se ejecutan de manera automática desde un USB y realiza un informe de los resultados obtenidos en formato estandarizado XML.

D

DEFT

DEFT (Digital Evidence&ForensicToolkit) es una distribución Live CD basada en Linux Kernel 3 y DART (Digital Advanced Response Toolkit). DEFT cuenta con la suite de DART que contiene aplicaciones de Windows.

Figura H-3: DEFT

DNS Herramientas

Para solicitar los registros DNS y convertir DNS a IP, hay muchas herramientas y webs diseñadas para automatizar y ayudar al investigador en esta tarea. Algunas de las más conocidas son DnsStuff (www.dnsstuff.com), DomainTools (www.domaintools.com) y CentralOps. Son webs a tener en cuenta a lo largo proceso.

E

ENCASE

Encase es la herramienta comercial profesional posiblemente más utilizada, se trata de un software específico para el análisis forense de sistemas informáticos. Entre sus muchas características, EnCase permite escanear discos, crear imágenes de discos para su posterior análisis, recuperar archivos de unidades que hayan sido formateadas, realizar borrado seguro de unidades a bajo nivel, consultas de archivos por tiempos de creación, último acceso y última escritura, identificación de extensiones de archivos, en múltiples soportes de archivos. Lo más destacado es que permite el análisis sobre discos duros, dispositivos USB, tablets, smartphones y exportar evidencias generando informes precisos.

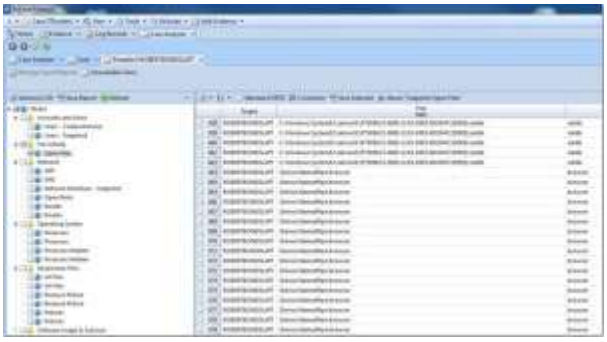

Figura H-4: ENCASE

F

FORENSIC TOOLKIT

ForensicTool Kit (FTK) es un paquete de herramientas forenses con distribución comercial. Permite análisis de correo electrónico y de archivos comprimidos, opciones de búsqueda de archivos y restauración de datos, así como múltiples archivos y formados de adquisición.

Figura H-5: Forensicstoolkit

G

GUYMAGER

Guymager es un generador de imágenes para investigaciones forenses. Como características principales destacan que se trata de una herramienta basada en entorno GNU/Linux, puede ser utilizada en entornos de multiprocesador y que genera archivos (dd), EWF (E01) and AFF images, realizando las clonaciones de disco. Es un software de código abierto.

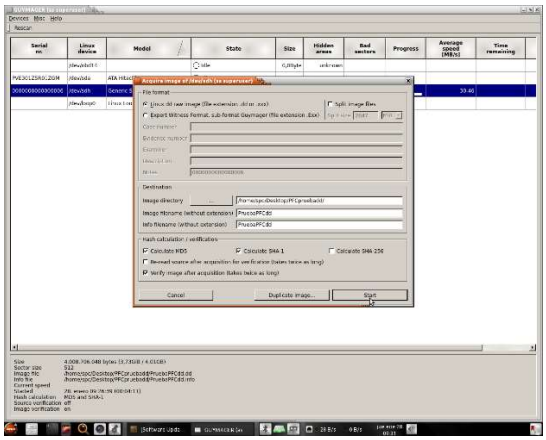

Figura H-6: GUYMAGER

H

HELIX

HELIX es una herramienta forense con distribución Linux basada en Ubuntu para respuesta a incidentes y análisis forense. Está desarrollada por e-fense y, las primeras versiones eran gratuitas, pero ahora tienen carácter comercial.

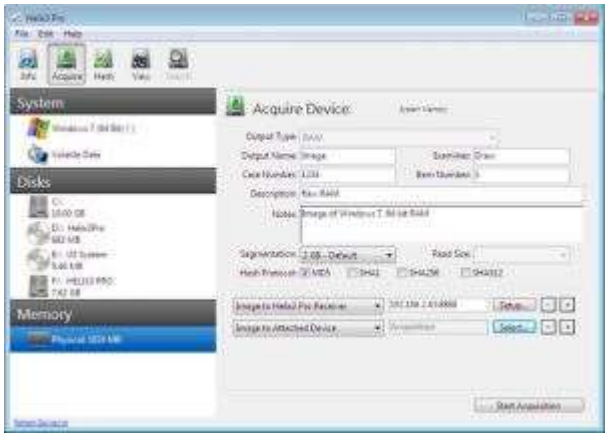

Figura H-7: HELIX

M

MALTEGO

La herramienta forense de mayor crecimiento en la actualidad y que viene ya incorporada en Kali Linux 2.0. Maltego es un software creado por Paterva. Está diseñado como herramienta de inteligencia forense y de software libre. Maltego está enfocado para el descubrimiento y análisis de información mediante minería de datos, en redes abiertas para crear en forma de gráficos el listado de conexiones de cualquier dato a buscar. Maltegopermite la creación búsqueda de entidades representando cada nexo de unión entre ellas en el gráfico, así podremos analizar en las relaciones entre distintas personas, grupos, empresas, sitios webs, dominios, diferente infraestructura web e incluso las diferentes cuentas en redes sociales, como pueden ser, Instagram, Twitter, Facebook…Es a día de hoy la herramienta más eficiente y utilizada para la búsqueda de identidades y relaciones entre los diferentes tipos de entidades en internet. Relacionando cada punto del diagrama con cualquiera de la información que disponga la red de ese punto, que como podemos entender puede ser cualquiera de nosotros.

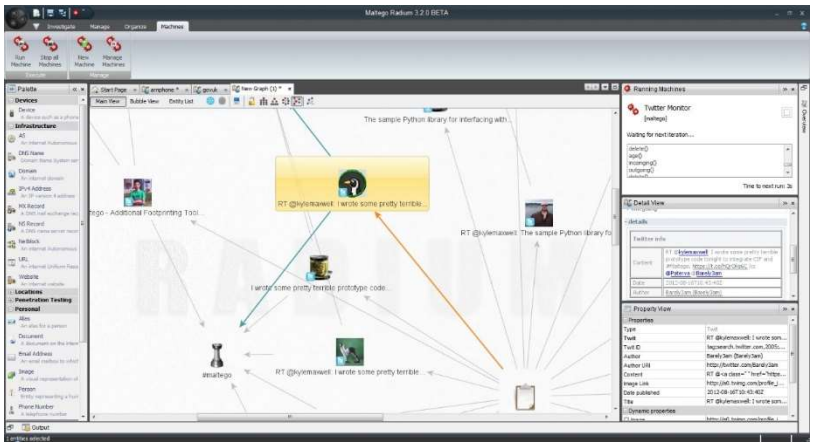

Figura H-8: MALTEGO

N

NetCleanAnalyze

NetCleanAnalyze es una herramienta gratuita de reconocimiento de imágenes disponible para los agentes de seguridad. Esta herramienta reconoce imágenes comunes de pornografía infantil que previamente han sido remitidas por las autoridades competentes a las bases de datos de las organizaciones y unidades en contra del maltrato a menores.

P

PALADIN

Paladines una herramienta forense con distribución Linux basada en Ubuntu para respuesta a incidentes y análisis forense, creada porsumuriforensics. Incluye una gran cantidad de herramientas para el desarrollo de las peritaciones.

Figura H-9: PALADIN

PhotoRec – QphotoRec

Herramienta para la recuperación de archivos borrados diseñadas por de CGsecurity, de software libre que funcionan en distintos sistemas operativos. Diseñadas para la recuperación de archivos que han sido borrados incluso cuando el Sistema de archivo ya no haga referencia a los mismos analizando todos los sectores del dispositivo electrónico investigado que el sistema de archivo considera disponible y comprobando si existe algún dato en ese sector.

S

SLEUTH KIT ir a AUTOPSY

SIFT

SIFT (SANS InvestigateForensicToolkit, SIFT) es una herramienta forense con distribución Linux basada en Ubuntu para respuesta a incidentes y análisis forense. Incluye la mayoría de las herramientas comentadas con anterioridad como SleuthKit/Autopsy, Wireshark, Pasco…

Figura H-10: SIFT

StegHide

StegHide Software esteganográfico que soporta cifrado y compresión. Trabaja con archivos JPEG, BMP, WAV y AU y tiene licencia GNU.

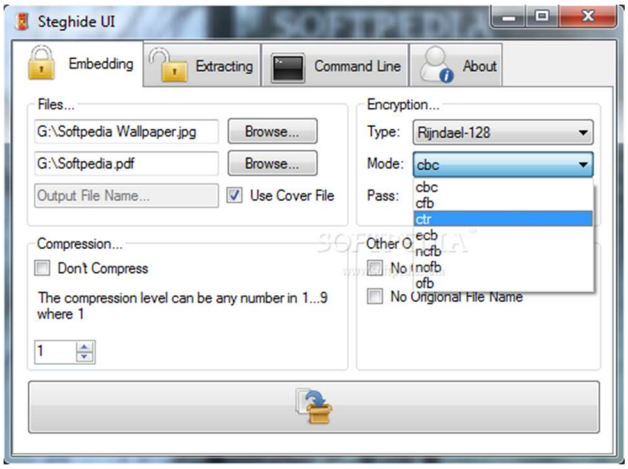

Figura H-11: StegHide

U

UFED (Universal ForensicExtractionDevice) de Cellebrite

UFED (Universal ForensicExtractionDevice) de Cellebrite herramienta forense para la extracción de datos en los dispositivos electrónicos móviles. Es una herramienta expresamente diseñada para smartphones y dispositivos PDA. Es capaz de generar informes claros y concisos en formato HTML y XML para consultas en procesos judiciales y clonar el ID de la tarjeta SIM para trabajar con un terminal sin conectarlo a la red.

Figura H-12: UFED (Universal ForensicExtractionDevice) de Cellebrite

Se trata de la herramienta de más fuerte introducción en el mercado, con unos resultados destacados, y es la herramienta más utilizada en los laboratorios profesionales, entre los datos que puede llegar a extraer, con o sin acceso a códigos de desbloqueo su página destaca:

- Registros de llamadas, incluso historiales de llamadas borrados de la SIM
- Contactos
- Datos del teléfono (IMEI/ESN, nº de teléfono)
- ICCID e IMSI
- Fotografías
- Vídeos
- Archivos de sonido
- Información de localización de la SIM: TMSI, MCC, MNC, LAC
- Geoetiquetas gráficas en Google Maps

W

Whois

Servicio web diseñado para el localizar al propietario de un nombre de dominio específico. En este sentido el perito forense podrá averiguar quién es el propietario, su nombre, apellidos, dirección de correo electrónico y dirección física, su número de teléfono y demás información relevante. Destacar que esta información puede, sin embargo, no ser real (por haber sido falsificada por el propietario). El perito, por lo tanto, puede encontrar datos directamente inútiles o datos que, intencionadamente, que dirijan la investigación por un camino erróneo. (www.who.is)

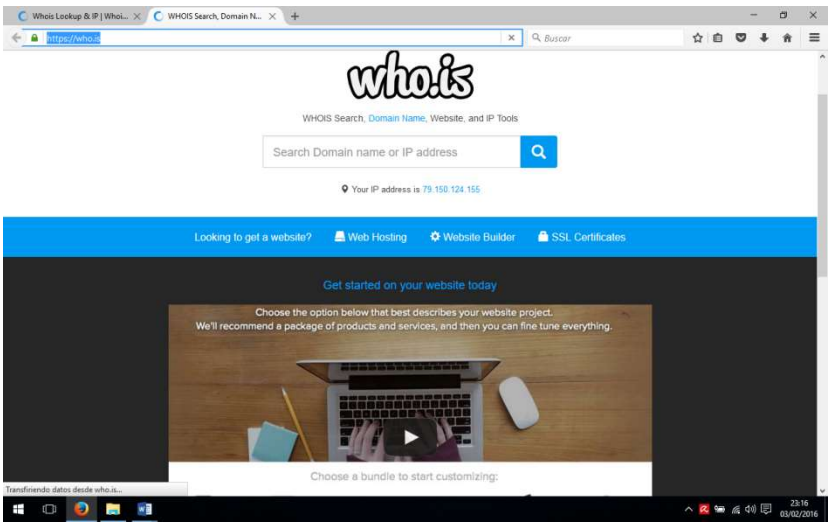

Figura H-13: Who.is

Whoisinverso

Este tipo de servicio incluye todos los registros DNS/IP (que la herramienta o web conoce) registrados bajo la identidad que se facilita. El perito forense podrá buscar por nombre, correo electrónico, teléfono o dirección física.

X

X-WAYS FORENSIC: Integrated Computer Forensics Software

Es una herramienta forense diseñada para realizar análisis forenses. Se trata de un software comercial integrado que ofrece la firma alemana X-Ways. Ofrece herramientas forenses, recuperación de datos, seguridad IT. Destacando WinHex, software para informática forense, recuperación de archivos y editor hexadecimal de archivos, discos y RAM.

Figura H-14: X-Ways Forensics

Glosario

A continuación, se podrán las definiciones de los términos más utilizados en las peritaciones informáticas, como también los distintos conceptos que debemos conocer para el desarrollo de nuestras funciones periciales.

A

Ataque informático

Es un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático (ordenador, red privada, etcétera).

B

Banners

Es un formato publicitario en Internet. Esta forma de publicidad online consiste en incluir una pieza publicitaria dentro de una página web. Prácticamente en la totalidad de los casos, su objetivo es atraer tráfico hacia el sitio web del anunciante que paga por su inclusión.

C

Cabecera

Header en inglés, se refiere a la información suplementaria situada al principio de un bloque de información que va a ser almacenada o transmitida y que contiene información necesaria para el correcto tratamiento del bloque de información.

Caminos, paths o ruta

Es la forma de referenciar un archivo informático o directorio en un sistema de archivos de un sistema operativo determinado. Una ruta señala la localización exacta de un archivo o directorio mediante una cadena de caracteres concreta.

Capa de aplicación

Es el séptimo nivel del modelo OSI.Ofrece a las aplicaciones (de usuario o no) la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (POP y SMTP), gestores de bases de datos y protocolos de transferencia de archivos (FTP).Esta capa contiene las aplicaciones visibles para el usuario. Algunas consideraciones son: seguridad y cifrado, DNS (DomainNameService) Una de las aplicaciones más usadas hoy en día en Internet es el WWW (World Wide Web).

Certificado digital o certificado electrónico

Es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad. Es un documento que permite al firmante identificarse en Internet. Es necesario para realizar trámites, tanto con las administraciones públicas como con numerosas entidades privadas.

Cifrado

En criptografía un cifrado, es un procedimiento que utilizando un algoritmo (algoritmo de cifrado) con cierta clave (clave de cifrado) transforma un mensaje, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender, a toda persona que no tenga la clave secreta (clave de descifrado) del algoritmo que se usa para poder descifrarlo (algoritmo de descifrado). Por tanto, tenemos dos algoritmos (el de cifrado y el de descifrado) y dos claves (clave de cifrado y clave de descifrado). Estas dos claves pueden ser iguales (criptografía simétrica) o no (criptografía asimétrica).

Clave pública

La criptografía asimétrica (en inglés asymmetrickencryptography), también llamada criptografía de clave pública (en inglés publickencryptography) o criptografía de dos claves1 (en inglés two-keycryptography), es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

Clave privada

La criptografía simétrica (en inglés symmetrickeycryptography), también llamada criptografía de clave secreta (en inglés secretkeycryptography) o criptografía de una clave1 (en inglés single-keycryptography), es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez que ambas partes tienen acceso a esta clave, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y éste lo descifra con la misma clave.

Codificación

La codificación de caracteres es el método que permite convertir un carácter de un lenguaje natural en un símbolo de otro sistema de representación, como un número o una secuencia de caracteres, aplicando normas o reglas de codificación.

Conexiones SSH

SecureSHell, en español: intérprete de órdenes segura es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X (en sistemas Unix y Windows) corriendo.Además de la conexión a otros dispositivos, SSH nos permite copiar datos de forma segura (tanto archivos sueltos como simular sesiones FTP cifradas), gestionar claves RSA para no escribir claves al conectar a los dispositivos y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH.

Control de la congestión

Control para la congestión de redes que es el fenómeno producido cuando a la red (o parte de ella) se le ofrece más tráfico del que puede cursar.

Cookies

Una cookie es una pequeña información enviada por un sitio web y almacenada en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del usuario.Sus principales funciones son:

- Llevar el control de usuarios: cuando un usuario introduce su nombre de usuario y contraseña, se almacena una cookie para que no tenga que estar introduciéndolas para cada página del servidor. Sin embargo, una cookie no identifica solo a una persona, sino a una combinación de computador-navegador-usuario.

- Conseguir información sobre los hábitos de navegación del usuario, e intentos de spyware (programas espía), por parte de agencias de

publicidad y otros. Esto puede causar problemas de privacidad y es una de las razones por la que las cookies tienen sus detractores.

Cracker

Cracker, 'romper', se utiliza para referirse a las personas que rompen algún sistema de seguridad. Los crackers pueden estar motivados por una multitud de razones, incluyendo fines de lucro, protesta, o por el desafío.

Cracking

Es la modificación del software con la intención de eliminar los métodos de protección de los cuales este disponga: protección de copias, versiones de prueba, números de serie, claves de hardware, verificación de fechas, verificación de CD o publicidad y adware.

Criptografía

Definida como la parte de la criptología que se ocupa de las técnicas, bien sea aplicadas al arte o la ciencia, que alteran las representaciones lingüísticas de mensajes, mediante técnicas de cifrado o codificado, para hacerlos ininteligibles a intrusos (lectores no autorizados) que intercepten esos mensajes. Por tanto el único objetivo de la criptografía era conseguir la confidencialidad de los mensajes. Para ello se diseñaban sistemas de cifrado y códigos. En esos tiempos la única criptografía que había era la llamada criptografía clásica.

Criptología

Esla disciplina científica que se dedica al estudio de la escritura secreta, es decir, estudia los mensajes que, procesados de cierta manera, se convierten en difíciles o imposibles de leer por entidades no autorizadas.Los campos en los que se divide la Criptología son:

- Criptografía. Se ocupa del estudio de los algoritmos, protocolos y sistemas que se utilizan para proteger la información y dotar de seguridad a las comunicaciones y a las entidades que se comunican.

- Criptoanálisis. Se ocupa de conseguir capturar el significado de mensajes construidos mediante Criptografía sin tener autorización para ello. Podríamos decir que el criptoanálisis tiene un objetivo opuesto al de la criptografía. Su objetivo es buscar el punto débil de las técnicas criptográficas para explotarla y así reducir o eliminar la seguridad que teóricamente aportaba esa técnica criptográfica. A cualquier intento de criptoanálisis se le llama ataque. Un ataque tiene éxito, y se dice que el sistema se ha roto,

cuando el atacante consigue romper la seguridad que la técnica criptográfica aporta al sistema.

D

DNS

El DNS es un sistema distribuido que actúa como una gran agenda telefónica, manteniendo un registro sobre qué dirección IP (o direcciones) se asigna a cada nombre y viceversa. Como se puede intuir, ésta relación no es siempre de uno a uno, sino que un nombre puede estar asignado a múltiples direcciones IP y a la inversa.Los nombres de los dominios son gestionados por registradores de dominios que necesitan ser acreditados por ICANN (Internet CorporationforAssignedNames and Numbershttp://www.icann.org/) o por el listado de registros de IANA (Internet AssignedNumbersAuthorityhttps://www.iana.org). Para los Dominios de Nivel Superior (Top LevelDomains) genéricos (gTIDs) como .com, .net, .org, .biz, etc, ICANN acredita a registradores de dominios ella misma, mientras que para los Code Top LevelDomains (ccRLEDs) como .es, .us, .uk, .ieetc, IANA delega el registro a agencias locales como Nominet UK, DeniceG, etc.

Dominio de Internet

Es una red de identificación asociada a un grupo de dispositivos o equipos conectados a la red Internet.El propósito principal de los nombres de dominio en Internet y del sistema de nombres de dominio (DNS), es traducir las direcciones IP de cada nodo activo en la red, a términos memorizables y fáciles de encontrar. Esta abstracción hace posible que cualquier servicio (de red) pueda moverse de un lugar geográfico a otro en la red Internet, aun cuando el cambio implique que tendrá una dirección IP diferente.

E

Enrutador

Es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un encaminador (mediante bridges), y que por tanto tienen prefijos de red distintos.

Encaminamiento

Enrutamiento, ruteo es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad.Cuando la red de conmutación de paquetes funciona en modo circuito virtual, generalmente la función de encaminamiento establece una ruta que no cambia durante el tiempo de vida de ese circuito virtual. En este caso el encaminamiento se decide por sesión.Una red que funciona en modo datagrama no tiene el compromiso de garantizar la entrega ordenada de los paquetes, por lo que los nodos pueden cambiar el criterio de encaminamiento para cada paquete que ha de mandar.

Encaminamiento de cebolla

Enrutamiento de cebolla, en inglés onionrouting, fue introducido por David M. Goldshlag, Michael Reed y Paul Syverson1 aplicando las ideas de las redes de mezclado de David Chaum a los sistemas de encaminamiento, para conseguir redes que preserven la privacidad (tanto del mensaje en si como de los interlocutores) de forma transparente a las entidades que se comunican. De esta forma podemos tener infraestructuras para comunicaciones privadas sobre una red pública.

Estenografía

La esteganografía trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia. Es decir, procura ocultar mensajes dentro de otros objetos y de esta forma establecer un canal encubierto de comunicación, de modo que el propio acto de la comunicación pase inadvertido para observadores que tienen acceso a ese canal.Se ocupa de ocultar mensajes con información privada por un canal inseguro, de forma que el mensaje no sea ni siquiera percibido.

Estegoanálisis

Se ocupa de detectar mensajes ocultos con técnicas esteganográficas. A cualquier intento de estegoanálisis se le llama ataque. Un ataque tiene éxito, y se dice que el sistema se ha roto, cuando el atacante detecta que se ha usado esteganografía y por tanto puede obtener el mensaje.

Exif - Imágenes

Exchangeableimage file format (abreviatura oficial Exif, no EXIF) es una especificación para formatos de archivos de imagen usado por las cámaras digitales. Las etiquetas (tags) de metadatos definidas en el estándar Exif cubren un amplio espectro incluido:

- Información de fecha y hora. Las cámaras digitales registran la fecha y la hora actual y la almacenan en los metadatos.

- Configuración de la cámara. Esta incluye información estática como el modelo de cámara y el fabricante, e información que varía con cada imagen como la orientación, apertura, velocidad del obturador, distancia focal, medidor de exposición y la velocidad de la película.

- Información sobre localización, la cual podría provenir de un GPS conectado a la cámara.

F

Filtro

Un filtro es un programa informático para procesar una corriente de datos.

Firma Digital

Una firma digital es un mecanismo criptográfico que permite al receptor de un mensaje firmado digitalmente determinar la entidad originadora de dicho mensaje (autenticación de origen y no repudio), y confirmar que el mensaje no ha sido alterado desde que fue firmado por el originador (integridad)

Firmas de apertura

Enlace de dos firmas y la decisión de decidir si estas firmas han sido emitidas por el miembro del mismo grupo o no

FQDN

Un FQDN (sigla en inglés de fullyqualifieddomainname) es un nombre que incluye el nombre de la computadora y el nombre de dominio asociado a ese equipo.

G

Gestor de clave

Un gestor de contraseñas es un programa que se utiliza para almacenar una gran cantidad de parejas usuario/contraseña. La base de datos donde se guarda esta información está cifrada mediante una única clave (contraseña maestra o en inglés master password), de forma que el usuario sólo tenga que memorizar una clave para acceder a todas las demás. Esto facilita la administración de contraseñas y fomenta que los usuarios escojan claves complejas sin miedo a no ser capaces de recordarlas posteriormente.

Gestor de firma

es el encargado de proporcionar al usuario la posibilidad de firmar documentos electrónicos utilizando certificados digitales X509, del tipo de los emitidos por la FNMT, en un entorno centralizado, independientemente del origen del documento. Para ello es necesario que las distintas aplicaciones de gestión que generan los documentos envíen sus documentos a ésta para su firma.

Grep

El comando grep nos permite buscar, dentro de los archivos, las líneas que concuerdan con un patrón. Grep es una utilidad de la línea de comandos escrita originalmente para ser usada con el sistema operativo Unix. Usualmente, grep toma una expresión regular de la línea de comandos, lee la entrada estándar o una lista de archivos, e imprime las líneas que contengan coincidencias para la expresión regular. Grep generalmente ejecuta alguna variante del algoritmo Boyer-Moore (para búsqueda de strings), utilizando expresiones regulares para definir la consulta. Puede manejar archivos, directorios (y subdirectorios), o la entrada estándar (stdin).

H

Hacker

Es alguien que descubre las debilidades de una computadora o de una red informática, aunque el término puede aplicarse también a alguien con un conocimiento avanzado de computadoras y de redes informáticas.

Hash

Se llaman funciones hash criptográficas a aquellas funciones hash que se utilizan en el área de la criptografía. Este tipo de funciones se caracterizan por cumplir propiedades que las hacen idóneas para su uso en sistemas que confían en la criptografía para dotarse de seguridad. Estas propiedades las hacen resistentes frente ataques maliciosos que intentan romper esa seguridad.Una función hash es método para generar claves o llaves que representen de manera unívoca a un documento o conjunto de datos. Es una operación matemática que se realiza sobre este conjunto de datos de cualquier longitud, y su salida es una huella digital, de tamaño fijo e independiente de la dimensión del documento original. El contenido es ilegible. A partir de un hash o huella digital, no podemos recuperar el conjunto de datos originales. Los más conocidos son el MD5 y el SHA-1. Cifrar una huella digital se conoce como firma digital.Requisitos que deben cumplir las funciones hash:

- Imposibilidad de obtener el texto original a partir de la huella digital.
- Imposibilidad de encontrar un conjunto de datos diferentes que tengan la misma huella digital.
- Poder transformar un texto de longitud variable en una huella de tamaño fijo (como el SHA-1 que es de 160bits).

Herramientas de Aplicación

es un tipo de programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de trabajos. Esto lo diferencia principalmente de otros tipos de programas como los sistemas operativos (que hacen funcionar al ordenador), las utilidades (que realizan tareas de mantenimiento o de uso general), y los lenguajes de programación (con el cual se crean los programas informáticos).

HTTP

El protocolo de transferencia de hipertexto es el protocolo usado en cada transacción de la World Wide Web. HTTP es un protocolo sin estado, es decir, que no guarda ninguna información sobre conexiones anteriores. El desarrollo de aplicaciones web necesita frecuentemente mantener estado. Para esto se usan las cookies, que es información que un servidor puede almacenar en el sistema cliente. Esto le permite a las aplicaciones web instituir la noción de "sesión", y también permite rastrear usuarios ya que las cookies pueden guardarse en el cliente por tiempo indeterminado.

Huellas Digitales

La intención de la tecnología de huella digital es identificar de manera precisa y única a una persona por medio de su huella digital. Certificando la autenticidad de las personas de manera única e inconfundible por medio de un dispositivo electrónico

que captura la huella digital y de un programa que realiza la verificación.

I

Imagen de disco

Una imagen de disco es un archivo que contiene la estructura y contenidos completos de un dispositivo o medio de almacenamiento de datos, como un disco duro, un disquete o un disco óptico (CD, DVD). Una imagen de disco usualmente se produce creando una copia completa, sector por sector, del medio de origen y por lo tanto replicando perfectamente la estructura y contenidos de un dispositivo de almacenamiento.La creación de imágenes forense es el proceso en el cual los contenidos enteros del disco duro son copiados a un archivo y los valores checksum son calculados para verificar la integridad del archivo de imagen. Las imágenes forenses son obtenidas mediante el uso de herramientas de software (algunas herramientas de clonación de hardware han añadido funcionalidades forenses).

IP

Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del Modelo OSI. Dicho número no se ha de confundir con la dirección MAC, que es un identificador de 48 bits para identificar de forma única la tarjeta de red y no depende del protocolo de conexión utilizado ni de la red. La dirección IP puede cambiar muy a menudo por cambios en la red o porque el dispositivo encargado dentro de la red de asignar las direcciones IP decida asignar otra IP (por ejemplo, con el protocolo DHCP). A esta forma de asignación de dirección IP se denomina también dirección IP dinámica.

ISDN

La UIT-T (CCITT) define la Red Digital de Servicios Integrados (RDSI o ISDN en inglés) como: red que procede por evolución de la Red Digital Integrada (RDI) y que facilita conexiones digitales extremo a extremo para proporcionar una amplia gama de servicios, tanto de voz como de otros tipos, y a la que los usuarios acceden a través de un conjunto de interfaces normalizados.

K

Kernel

es un software que constituye una parte fundamental del sistema operativo. Es el principal responsable de facilitar a los distintos programas acceso seguro al hardware de la computadora o en forma básica, es el encargado de gestionar recursos, a través de servicios de llamada al sistema.

L

Latencia

En redes informáticas de datos se denomina latencia a la suma de retardos temporales dentro de una red. Un retardo es producido por la demora en la propagación y transmisión de paquetes dentro de la red.

Log (registro)

El registro o log es una base de datos jerárquica que almacena los ajustes de configuración y opciones en los sistemas operativos. Contiene la configuración de los componentes de bajo nivel del sistema operativo, así como de las aplicaciones que hay funcionando en la plataforma: hacen uso del registro el núcleo (kernel, en inglés), los controladores de dispositivos, los servicios, el SAM, la interfaz de usuario y las aplicaciones de terceros. El registro también proporciona un medio de acceso a los contadores para generar un perfil del rendimiento del sistema.La mayoría de los logs son almacenados o desplegados en el formato estándar, el cual es un conjunto de caracteres para dispositivos comunes y aplicaciones. De esta forma cada log generado por un dispositivo en particular puede ser leído y desplegado en otro diferente. A su vez la palabra log se relaciona con el término evidencia digital.

M

MD5

MD5 abreviatura de *Message-DigestAlgorithm 5*, Algoritmo de Resumen del Mensaje 5, es un algoritmo de reducción criptográfico de 128 bits ampliamente usado. La codificación del MD5 de 128 bits es representada típicamente como un número de 32 dígitos hexadecimal.

Metadatos

Los metadatos, o los datos sobre los datos, representan aquella información que hace referencia al archivo en sí, en vez de a su contenido. Los archivos electrónicos almacenados en el sistema de archivos pueden ofrecer información adicional tal como la fecha y hora en la que se creó un documento, cuándo fue modificado o cuándo fue el último acceso. Un archivo de imagen normalmente incluye bastantes metadatos en relación a cómo se tomó la imagen en una sección del archivo denominada EXIF.

Multiplataforma

Es un atributo conferido a los programas informáticos o los métodos de cálculo y los conceptos que se ejecutan e interoperar en múltiples plataformas informáticas, una aplicación multiplataforma puede ejecutarse en Microsoft Windows en la arquitectura x86, Linux en la arquitectura x86 y Mac OS X ya sea en el PowerPC o sistemas Apple Macintosh basados en x86.

N

NAT

Network AddressTranslation - Traducción de Dirección de Red es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.

Nombre de equipo HOSTS

Es un nombre único y relativamente informal que se le da a un dispositivo conectado a una red informática. Puede ser un ordenador, un servidor de ficheros, un dispositivo de almacenamiento por red, una máquina de fax, impresora, etc.En Internet, generalmente se trabaja con equipos funcionando como servidores (hosts), en estos casos el equivalente para "nombre de equipo" en inglés seria "hostname". Estos servidores siempre tienen una dirección IP asignada.

P

Password cracking

es un proceso informático que consiste en descifrar la contraseña de determinadas aplicaciones elegidas por el usuario. Se busca codificar los códigos de cifrado en todos los ámbitos de la informática. Se trata del rompimiento o desciframiento de clavespasswords.

Pérdida de la información PII

La Información Personalmente Identificable (PII): Identifica a una persona como individuo.

Plug-ins

Un complemento es una aplicación que se relaciona con otra para aportarle una función nueva y generalmente muy específica. Esta aplicación adicional es ejecutada por la aplicación principal e interactúan por medio de la API. También se conoce como plug-in, enchufable o inserción, add-on, añadido, conector o extensión.

Portabilidad

La portabilidad es uno de los conceptos clave en la programación de alto nivel.Se define como la característica que posee un software para ejecutarse en diferentes plataformas, el código fuente del software es capaz de reutilizarse en vez de crearse un nuevo código cuando el software pasa de una plataforma a otra. A mayor portabilidad menor es la dependencia del software con respecto a la plataforma.

Privoxy

Es un programa que funciona como proxy web, usado frecuentemente en combinación con Squid. Tiene capacidades avanzadas de filtrado para proteger la privacidad, modificar el contenido de las páginas web, administrar cookies, controlar accesos y eliminar anuncios, banners, ventanas emergentes y otros elementos indeseados de Internet. Privoxy tiene una configuración muy flexible y puede ser personalizado para adaptarse a las necesidades y gustos individuales. Privoxy es útil tanto para sistemas aislados como para redes multiusuario.

Protocolo de estado de certificados en línea (OCSP)

Online Certificate Status Protocoles un método para determinar el estado de revocación de un certificado digitalX.509 usando otros medios que no sean el uso de CRL (Listas de Revocación de Certificados). Este protocolo se describe en el RFC 2560 y está en el registro de estándares de Internet.

Proxy

Es un programa o dispositivo que realiza una acción en representación de otro, esto es, si una hipotética máquina A solicita un recurso a una C, lo hará mediante una petición a B; C entonces no sabrá que la petición procedió originalmente de A. Esta situación estratégica de punto intermedio suele ser aprovechada para soportar una serie de funcionalidades: proporcionar caché, control de acceso, registro del tráfico, prohibir cierto tipo de tráfico, etc.Su finalidad más habitual es la de servidor proxy, que consiste en interceptar las conexiones de red que un cliente hace a un servidor de destino, por varios motivos posibles como seguridad, rendimiento, anonimato, etc.

Pseudónimo

Conocido como alias, sirve para identificar a la persona que está accediendo a Internet mediante una computadora, identificando así a dicha persona más prácticamente que a través del número de dirección IP, aunque en estos casos normalmente se utiliza el anglicismo Nick.

Public Key Infrastructure PKIX.509

Es un estándar UIT-T para infraestructuras de claves públicas. X.509 específica, entre otras cosas, formatos estándar para certificados de claves públicas y un algoritmo de validación de la ruta de certificación. Su sintaxis, se define empleando el lenguaje ASN. (AbstractSyntaxNotationOne), y los formatos de codificación más comunes son DER (DistinguishEncoding Rules) o PEM (PrivacyEnhanced Mail).

R

Redes privadas virtuales (VPNs)

Una red privada virtual, RPV, o VPN de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.1 Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

Revocación de certificados (CRL)

La Lista de Revocación de Certificados es conocida por sus siglas en inglés CRL

("CertificateRevocationList"). En la operación de algunos sistemas criptográficos, usualmente los de infraestructura de clave pública (PKI), una CRL es una lista de certificados (más concretamente sus números de serie) que han sido revocados, ya no son válidos y en los que no debe confiar ningún usuario del sistema.

S

Scripts

Un lenguaje interpretado es un lenguaje de programación que está diseñado para ser ejecutado por medio de un intérprete, en contraste con los lenguajes compilados. Teóricamente, cualquier lenguaje puede ser compilado o ser interpretado, así que esta designación es aplicada puramente debido a la práctica de implementación común y no a alguna característica subyacente de un lenguaje en particular. Sin embargo, hay lenguajes que son diseñados para ser intrínsecamente interpretativos, por lo tanto, un compilador causará una carencia de la eficacia. Muchos autores rechazan la clasificación de lenguajes de programación entre interpretados y compilados, considerando que el modo de ejecución (por medio de intérprete o de compilador) del programa escrito en el lenguaje es independiente del propio lenguaje. A ciertos lenguajes interpretados también se les conoce como lenguajes de script.

Sellado de tiempo (Time stamping)

Sellado de tiempo o time stamping es el proceso mediante el cual se guarda registro del momento de creación o modificación de un documento de modo seguro. En este contexto, la seguridad significa que nadie – ni siquiera el propietario del documento - debe ser capaz de modificarlo una vez ha sido grabado (suponiendo que la integridad del time stamper no haya sido comprometida).

Servidores de directorio

Un servicio de directorio (SD) es una aplicación o un conjunto de aplicaciones que almacena y organiza la información sobre los usuarios de una red de ordenadores, sobre recursos de red, y permite a los administradores gestionar el acceso de usuarios a los recursos sobre dicha red. Además, los servicios de directorio actúan como una capa de abstracción entre los usuarios y los recursos compartidos.

Servicio de Internet (ISP)

Un proveedor de servicios de Internet (o ISP, por la sigla en inglés de Internet ServiceProvider) es una empresa que brinda conexión a Internet a sus clientes. Un ISP conecta a sus usuarios a Internet a través de diferentes tecnologías como DSL, Cablemódem, GSM, Dial-up.

Servicios ocultos

Los servicios que ocultan la localización (por ejemplo, la dirección IP) son los servicios ocultos (HiddenService) que permiten crear una página web, o cualquier servicio TCP, sin la necesidad de tener un IP público y con la ubicación anónima

SHA

El SHA*Secure Hash Algorithm*, Algoritmo de *Hash* Seguro, es una familia de funciones hash de cifrado publicadas por el Instituto Nacional de Estándares y Tecnología (NIST). La primera versión del algoritmo fue creada en 1993 con el nombre de SHA, aunque en la actualidad se la conoce como SHA-0 para evitar confusiones con las versiones posteriores. La segunda versión del sistema, publicada con el nombre de SHA-1, fue publicada dos años más tarde. Posteriormente se han publicado SHA-2 en 2001 (formada por diversas funciones: SHA-224, SHA-256, SHA-384, y SHA-512) y la más reciente, SHA-3, que fue seleccionada en una competición de funciones hash celebrada por el NIST en 2012. Esta última versión se caracteriza por ser la que más difiere de sus predecesoras.SHA-1 ha sido examinado muy de cerca por la comunidad criptográfica pública, y no se ha encontrado ningún ataque efectivo. SHA-0 y SHA-1 producen una salida resumen de 160 bits (20 bytes) de un mensaje que puede tener un tamaño máximo de 2^{64} bits, y se basa en principios similares a los usados por el profesor Ronald L. Rivest del MIT en el diseño de los algoritmos de resumen de mensaje MD4 y MD5.

Sistema virtual

Un sistema de archivos virtual (VFS) o conmutador de sistema de archivos virtual es una capa de abstracción encima de un sistema de archivos más concreto. El propósito de un VFS es permitir que las aplicaciones cliente tengan acceso a diversos tipos de sistemas de archivos concretos de una manera uniforme. Puede ser utilizada para tender un puente sobre las diferencias en los sistemas de archivos de Windows, de Mac OS y Unix, de modo que las aplicaciones pudieran tener acceso a archivos en los sistemas de archivos locales de esos tipos sin tener que saber a qué tipo de sistema de archivos están teniendo acceso.

Sniffing

Un analizador de paquetes es un programa de captura de las tramas de una red de computadoras.Es algo común que, por topología de red y necesidad material, el medio de transmisión (cable coaxial, cable de par trenzado, fibra óptica, etc.) sea compartido por varias computadoras y dispositivos de red, lo que hace posible que un ordenador capture las tramas de información no destinadas a él. Para conseguir esto el analizador pone la tarjeta de red en un estado conocido como "modo promiscuo" en el cual en la capa de enlace de datos no son descartadas las tramas no destinadas a la dirección MAC de la tarjeta; de esta manera se puede capturar (sniff,

"olfatear") todo el tráfico que viaja por la red.

Socks

Socket designa un concepto abstracto por el cual dos programas (posiblemente situados en computadoras distintas) pueden intercambiar cualquier flujo de datos, generalmente de manera fiable y ordenada.El término socket es también usado como el nombre de una interfaz de programación de aplicaciones (API) para la familia de protocolos de Internet TCP/IP, provista usualmente por el sistema operativo.Los sockets de Internet constituyen el mecanismo para la entrega de paquetes de datos provenientes de la tarjeta de red a los procesos o hilos apropiados. Un socket queda definido por un par de direcciones IP local y remota, un protocolo de transporte y un par de números de puerto local y remoto.

SSL / TLS

Secure Sockets Layer (SSL; en español «capa de conexión segura») y su sucesor TransportLayer Security (TLS; en español «seguridad de la capa de transporte») son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet.

W

Web bugs

Un web bug, también llamado baliza web o faro web, o por el término inglés web beacon, es una diminuta imagen, normalmente invisible, en una página web o en un mensaje de correo electrónico que se diseña para controlar quién lo lee. Normalmente se utilizan para realizar análisis web.Su tamaño es inapreciable, pudiendo ser un único píxel en formato GIF y de color transparente. Se representan como etiquetas HTML y pueden incluir código JavaScript.

Presupuesto

Ejecución Material	Coste €
Clonadora Marca Logicube modelo Falcon…….. Forensic Falcon SAS/SATA/USB/FW multi-source/multi-destination forensic imaging solution. Includes soft case, SAS/SATA cables (qty. 4), USB 3.0 cables (qty. 2) , USB 3.0 device cable (qty. 1), Firewire cable (qty. 1), 3.5/2.5" IDE adpater (qty. 1), 1.8" IDE adapter (qty. 1), ZIF-2 adapter (qty. 1), mictoSATA converter (qty. 1), mSATA to SATA adapter and power supply	3.300
Duplicadora de discos marca Tableau modelo TD2uKit…… TD2u Forensic Duplicator Kit. Includes TD2u, TP5, TC2-8-R2, TC3-8, TC4-8-R2 (x3), TC5-8-R2, TC6-8, TC8, TPKG-VCT-5, TPKG-CLOTH, and QuickStart Guide. Packaged in 18.25" x 12" x 6" white cardboard box with foam inserts	1.599
Ordenador forense……. Procesador Intel Core i7, SSD 120GB, Disco SATA 2TB16GB RAM, Conexiones: USB 2.0, USB 3.0, HDMI, RJ-45S.O. Windows 8.1, Software OnData para monitorización y control del estado de los discos.Monitor 27”, Teclado y Ratón inalámbricos. Software forense	1.830
Velociraptor Workstation……. 32GB RAM, SSD 128GB, RAID 2TB, S.O. Windows 8.1 VMWare, UltraIso, Bloqueador de escritura USB, SATA/SAS, IDE, FireWire,Bahías de conexión en caliente. Conexiones: USB 2.0, USB 3.0, HDMI, RJ-45, Software OnData para monitorización y control delestado de los discos.Monitor 27”. Teclado y Ratón inalámbricos.	4.450
Destructora Rexel P180CD……	248
Mobiliario de oficina……...	200
Póliza seguros de RC ……	135
Licencias de explotación software forense productos anuales …….	2.100
ComunicacionesTelefónicas Informáticas……. Telefonía fija y móvil, así como los de alta o conexión al servicio Gastos correspondientes a sellos, franqueos, apartados de correos,paquetería, mensajería, etc.	800
Material **fotográfico**…….	850
Material diverso de consumo y reposición de carácter periódico……	350
PRESUPUESTO DE EJECUCIÓN MATERIAL……...	**15.862**

Gastos generales	
13 % sobre Ejecución Material……..	2.062,06
Beneficio Industrial	
6 % sobre Ejecución Material……..	951,72
TOTAL…… …….	3.013,78
16% de IVA……..…… ……..	482,21
Presupuesto de Ejecución por Contrata……	**3.495,99**
Honorarios Proyecto	
Soportes físicos de memoria	
Realizar imagen de memoria: 5horas	
Estudio de información: 40 horas	
Realización de informe: 12 horas	
Total estimado: 57 horas a 20 €/hora……..	**1.140**
Correo electrónico	
Recopilar información sobre correo electrónico: 3 horas	
Estudio de información: 20 horas	
Realización de informe: 12 horas	
Total estimado: 35 horas a 20 €/hora……..	**700**
Nube	
Recopilar información sobre correo electrónico: 3 horas	
Estudio de información: 20 horas	
Realización de informe: 12 horas	
Total estimado: 35 horas a 20 €/hora……..	**700**
Ordenador	
Clonado de discos duros o tarjetas: 5horas	
Estudio de información: 80 horas	
Realización de informe: 12 horas	
Total estimado: 97 horas a 20 €/hora……..	**1.940**
Móvil	
Realizar imagen de móvil: 25 horas	
Estudio de información: 60 horas	
Realización de informe: 12 horas	
Total estimado: 97 horas a 20 €/hora……..	**1.940**

Subtotal del presupuesto		
Subtotal Presupuesto…….		**22.282**
I.V.A. aplicable		
21%	Subtotal	**4.679,22**
Presupuesto……..		
TOTAL PRESUPUESTO……...		**26.961,22**

Madrid, Abril de 2016

El Ingeniero Jefe de Proyecto

Fdo.: Luis Miguel Gómez Aparicio

Ingeniero de Telecomunicación

Pliego de Condiciones

Condiciones que rigen el contrato para la realización de trabajos de peritación

CAPÍTULO I

DISPOSICIONES GENERALES

Cláusula 1. *Régimen jurídico.*

El presente contrato tiene carácter administrativo. Las partes quedan sometidas expresamente a lo establecido en este pliego y en su correspondiente de prescripciones técnicas particulares.

Para lo no previsto en este pliego, el contrato se regirá por la legislación básica del Estado en materia de contratos: Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación o si se trata de un contrato público por la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público (LCSP). Supletoriamente, se aplicarán las normas estatales sobre derecho administrativo de derecho privado y, en su defecto, las de contratos públicos que no tengan carácter básico.

Cláusula 2. *Objeto del contrato.*

El objeto del contrato al que se refiere el presente pliego es la ejecución de los trabajos de peritación que serán definidos en la descripción de pliego del proyecto, donde se desarrollarán las técnicas particulares y en el que se especifican las necesidades a satisfacer mediante el contrato y los factores de todo orden a tener en cuenta.

Tanto el pliego de prescripciones técnicas particulares como el pliego de cláusulas administrativas particulares revisten carácter contractual, por lo que deberán ser firmados, en prueba de conformidad por el adjudicador como por el adjudicatario, en el mismo acto de formalización del contrato.

Cláusula 3. *Presupuesto base de contratación y precio del contrato.*

El presupuesto base de contratación asciende a la cantidad expresada en el Presupuesto, del que forma parte el presente pliego.

Su cálculo incluye todos los factores de valoración y gastos que, según los

documentos contractuales y la legislación vigente son de cuenta del adjudicatario, así como los tributos de cualquier índole. Incluido el Impuesto sobre el Valor Añadido, que figura como partida independiente.

El precio del contrato será aquél al que ascienda la adjudicación definitiva, que en ningún caso superará la cantidad expresada en el presupuesto base.

Cláusula 4. *Forma y contenido de las proposiciones.*

Las proposiciones constarán preceptivamente, de los siguientes documentos:

1.- Si la empresa fuera persona jurídica, la escritura de constitución o modificación, en su caso, inscrita en el Registro Mercantil, cuando este requisito fuera exigible conforme a la legislación mercantil que le sea aplicable. Si no lo fuere, la escritura o documento de constitución, estatutos o acto fundacional en los que consten las normas por las que se regula su actividad, inscritos, en su caso, en el correspondiente Registro oficial, así como el Código de Identificación Fiscal (CIF), todo ello en original o copia que tenga el carácter de auténtica conforme a la legislación vigente, o fotocopia compulsada por funcionario habilitado para ello. Estos documentos deberán recoger el exacto régimen jurídico del solicitante en el momento de la presentación de la proposición.

2.- Si se trata de empresario individual, el DNI o documento que, en su caso, le sustituya reglamentariamente, en copia que tenga el carácter de auténtica conforme a la legislación vigente, o fotocopia compulsada por funcionario habilitado para ello.

3.- Cuando se trate de empresarios no españoles de Estados miembros de la Unión Europea o signatarios del Acuerdo sobre el Espacio Económico Europeo, se acreditará mediante su inscripción en un registro profesional o comercial, para los contratos de servicios.

4.- Cuando se trate de empresas extranjeras no comprendidas en el párrafo anterior, informe de la Misión Diplomática Permanente u Oficina Consular de España del lugar del domicilio de la empresa en el que se haga constar, previa acreditación por la empresa, que figuran inscritas en el Registro local profesional, comercial o análogo, o en su defecto, que actúan con habitualidad en el tráfico local en el ámbito de las actividades a las que se extiende el objeto del contrato.

5.- Los que comparezcan o firmen solicitudes en nombre de otro o representen a una persona jurídica, deberán acompañar también poder acreditativo de su representación, todo ello en original o copia compulsada. Igualmente deberá presentar fotocopia compulsada del D.N.I. de la persona a cuyo favor se otorgó el apoderamiento o representación. Si el documento acreditativo de la representación contuviese delegación permanente de facultades, deberá figurar inscrito en el Registro Mercantil.

CAPÍTULO II

ADJUDICACIÓN Y FORMALIZACIÓN

Cláusula 5. *Adjudicación y formalización del contrato.*

El contrato se perfeccionará mediante la formalización definitiva realizada por el director de contratación, formalizándose en documento administrativo dentro del plazo de diez días hábiles a contar desde el siguiente a la notificación de la notificación definitiva del mismo.

El contrato podrá formalizarse en escritura pública si así lo solicita el contratista, corriendo a su cargo los gastos derivados de su otorgamiento. En este caso el contratista deberá entregar a la Administración una copia legitimada y una simple del citado documento en el plazo máximo de un mes desde su formalización.

CAPÍTULO III

EJECUCIÓN DEL CONTRATO

Cláusula 6. *Programa de trabajo.*

El director del proyecto, si procede, en el plazo de diez días, contado desde la formalización del contrato, habrá de presentar el programa para su realización, en el que consten las tareas que considere necesario realizar para atender el contenido del trabajo proponiendo, en su caso, los plazos parciales correspondientes a cada tarea. A estos efectos, se utilizarán como unidades de tiempo el día, la semana y el mes, salvo indicación en contrario del pliego de prescripciones técnicas. El programa de trabajo respetará todas las fechas o plazos de entrega fijados en el contrato, y contendrá todos los datos exigidos en aquel pliego, o, de no especificarse en el mismo, los previstos en la cláusula 24 del Pliego de Cláusulas Administrativas Generales para la Contratación de Estudios y Servicios Técnicos aprobados por Orden de 8 de marzo de 1972.

El director del proyecto resolverá sobre el mismo, pudiendo imponer al programa de trabajo presentado la introducción de modificaciones, ampliaciones y el grado de definición que estime necesario para el cumplimiento del contrato.

Si para el desarrollo de los trabajos se precisare establecer por el adjudicatario contactos con entidades u organismos públicos, necesitará la previa autorización del órgano de contratación.

Cada vez que se modifiquen las condiciones contractuales, el contratista queda obligado a la actualización y puesta al día de este programa.

Cláusula 7. *Dirección de los trabajos.*

La dirección de los trabajos corresponde al responsable del contrato o, en su defecto, al representante que designe el director del proyecto.

Son funciones del responsable del contrato o del representante del director del proyecto:

a) Interpretar el Pliego de Prescripciones Técnicas y demás condiciones técnicas establecidas en el contrato o en disposiciones oficiales.

b) Exigir la existencia de los medios y organización necesarios para la ejecución del contrato en cada una de sus fases.

c) Dar las órdenes oportunas para lograr los objetivos del contrato.

d) Proponer las modificaciones que convenga introducir.

e) Expedir, en su caso, las certificaciones parciales y conformar las facturas correspondientes a los trabajos realizados según los plazos de ejecución y abono que se hayan acordado.

f) Tramitar cuantas incidencias surjan durante el desarrollo del contrato.

g) Convocar cuantas reuniones estime pertinentes para el buen desarrollo de los trabajos y su supervisión, a la que estará obligada a asistir la representación de la empresa adjudicataria, asistida de aquellos facultativos, técnicos, letrados o especialistas de la misma que tengan alguna intervención en la ejecución del contrato.

Cláusula 8. *Plazo de ejecución.*

El plazo total y los parciales de ejecución de los trabajos a que se refiere este pliego serán los que figuran en el programa de trabajoo el que se determine en la adjudicación definitiva del contrato, siendo los plazos parciales los que se fijen como tales en la aprobación del programa de trabajo, en su caso.

Los plazos parciales que se fijen en la aprobación del programa de trabajo, con los efectos que en la aprobación se determinen, se entenderán integrantes del contrato a los efectos legales pertinentes.

Cláusula 9. *Prórroga del contrato.*

Sin perjuicio de lo dispuesto en la cláusula anterior, el contrato podrá prorrogarse de forma expresa y por mutuo acuerdo de las partes antes de su finalización, sin que las prórrogas, consideradas aislada o conjuntamente, puedan exceder del plazo fijado originariamente.

La garantía definitiva constituida inicialmente se podrá aplicar al período de prórroga sin que sea necesario reajustar su cuantía, salvo que junto con la prórroga se acuerde la modificación del contrato.

Cláusula 10. *Cumplimiento del plazo, y penalidades por demora y ejecución defectuosa.*

El contratista está obligado a cumplir el contrato dentro del plazo total fijado para la realización del mismo, así como de los plazos parciales señalados para su ejecución sucesiva.

Si los trabajos sufriesen un retraso en su ejecución y siempre que el mismo no fuere imputable al contratista, si éste ofreciera cumplir sus compromisos se concederá por el órgano de contratación un plazo que será por lo menos igual al tiempo perdido, a no ser que el contratista pidiese otro menor.

Cuando el contratista, por causas imputables al mismo, hubiese incurrido en demora respecto al cumplimiento del plazo total o de los plazos parciales, si éstos se hubiesen previsto, para lo que se estará al presente pliego.

Cada vez que las penalidades por demora alcancen un múltiplo del 5 por 100 del precio del contrato, el órgano de contratación estará facultado para proceder a la resolución del mismo o acordar la continuidad de su ejecución con imposición de nuevas penalidades. En este último supuesto, el órgano de contratación concederá la ampliación del plazo que estime necesaria para la terminación del contrato.

En caso de cumplimiento defectuoso de la ejecución del contrato, o, en su caso, incumplimiento del compromiso de dedicar o adscribir a la ejecución del contrato los medios personales y materiales suficientes, o de las condiciones especiales de ejecución del contrato, el órgano de contratación podrá estimar la terminación del contrato.

La aplicación y el pago de las penalidades no excluyen la indemnización a que el contratista pueda tener derecho por daños y perjuicios ocasionados con motivo del retraso imputable al contratista.

Cláusula 11. *Responsabilidad del contratista por daños y perjuicios.*

El contratista será responsable de todos los daños y perjuicios directos e indirectos que se causen a terceros como consecuencia de las operaciones que requiera la ejecución del contrato. Si los daños y perjuicios ocasionados fueran consecuencia inmediata y directa de una orden dada por el órgano de contratación, éste será responsable dentro de los límites señalados en las leyes.

Igualmente, el contratista será responsable de la calidad técnica de los trabajos y de las prestaciones y servicios realizados, así como de las consecuencias que se deduzcan para terceros por errores u omisiones o métodos inadecuados o conclusiones incorrectas en la ejecución del contrato.

Cláusula 12. *Modificación del contrato.*

El órgano de contratación podrá acordar, una vez perfeccionado el contrato y por razones de interés particular, modificaciones en el mismo cuando sean consecuencia de causas imprevistas, justificándolo debidamente en el expediente. Estas modificaciones no podrán afectar a lascondiciones esenciales del contrato.

Cláusula 13. *Cesión del contrato.*

Los derechos y obligaciones dimanantes del presente contrato podrán ser cedidos por el adjudicatario a un tercero siempre que se cumplan todos los artículos del presente pliego de contratación.

Cláusula 14. *Subcontratación.*

El adjudicatario del contrato podrá concertar con terceros la realización parcial del mismo siempre que se cumplan los requisitos establecidos en el presente pliego de contratación quedando obligado al cumplimiento de los requisitos y obligaciones establecidos en este. En todo caso, el contratista asumirá la total responsabilidad de la ejecución del contrato frente al órgano de contratación.

El contratista deberá comunicar al órgano de contratación su intención de subcontratar, las partes del contrato a que afectará y la identidad del subcontratista, así como justificar la aptitud de éste por referencia a los elementos técnicos y humanos de que dispone y a su experiencia, salvo si el subcontratista tuviera la clasificación adecuada para realizar la parte del contrato objeto de la subcontratación.

CAPÍTULO V

DERECHOS Y OBLIGACIONES DEL CONTRATISTA

Cláusula 15. *Abonos y relaciones valoradas.*

El contratista tiene derecho al abono, con arreglo a los precios convenidos, de los trabajos que realmente ejecute con sujeción al contrato, a sus modificaciones aprobadas y a las instrucciones dadas por el órgano de contratación, a través del responsable del contrato, en su caso, siendo la forma de pago: 20% de la cantidad establecida en el presupuesto a la formalización del contrato y el 80% restante a la entrega del proyecto, a la que se unirá la factura emitida por el contratista.

El contratista deberá aportar, junto con la factura, justificante de entrega y recepción por el órgano de contratación del informe sobre la peritación correspondiente.

La demora en el pago por plazo superior a sesenta días devengará a favor del contratista los intereses de demora y la indemnización por los costes de cobro en los términos previstos en la Ley 3/2004, de 29 de diciembre, por la que se establecen medidas de lucha contra la morosidad en las operaciones comerciales.

El responsable del contrato o el representante del órgano de contratación, a la vista de los trabajos realmente ejecutados y de los precios contratados, redactará las correspondientesvaloraciones. Las valoraciones se efectuarán siempre al origen, concretándose los trabajos realizados en el período de tiempo de que se trate, observándose, en cuanto a la audiencia del contratista.

El coste máximo para el acreedor será de Euribor a tres meses más un diferencial máximo de 0,50%, estando exenta la operación de todo tipo de comisión.

Cláusula 16. *Obligaciones, gastos e impuestos exigibles al contratista.*

Son de cuenta del contratista los gastos e impuestos. Asimismo vendrá obligado a satisfacer todos los gastos que la empresa deba realizar para el cumplimiento del contrato, como son los generales, financieros, de seguros, transportes y desplazamientos, materiales, instalaciones, honorarios del personal a su cargo, de comprobación y ensayo, tasas y toda clase de tributos, el IVA, el impuesto que por la realización de la actividad pudiera corresponder y cualesquiera otros que pudieran derivarse de la ejecución del contrato durante la vigencia del mismo, sin que por tanto puedan ser éstos repercutidos como partida independiente.

El contratista deberá respetar, el carácter confidencial de la información a que tenga acceso con ocasión de la ejecución del contrato, o que por su propia naturaleza deba ser tratada como tal.

Cláusula 17. *Obligaciones laborales y sociales.*

El contratista está obligado al cumplimiento de la normativa vigente en materia laboral, de seguridad social, de integración social de minusválidos y de prevención de riesgos laborales, conforme a lo dispuesto en la Ley 31/1995, de 8 de noviembre, sobre Prevención de Riesgos Laborales, Real Decreto 171/2004, de 30 enero, por el que se desarrolla el artículo 24 de dicha Ley en materia de coordinación de actividades empresariales, en el Reglamento de los Servicios de Prevención, aprobado por Real Decreto 39/1997, de 17 de enero, así como las que se promulguen durante la ejecución del contrato.

CAPÍTULO VI

EXTINCIÓN DEL CONTRATO

Cláusula 18. *Entrega de los trabajos y realización de los servicios.*

El contratista deberá entregar los trabajos dentro del plazo estipulado, efectuándose por el representante del órgano de contratación, en su caso, un examen de la documentación presentada y si estimase cumplidas las prescripciones técnicas propondrá que se lleve a cabo la recepción.

En el caso de que estimase incumplidas las prescripciones técnicas del contrato, dará por escrito al contratista las instrucciones precisas y detalladas con el fin de remediar las faltas o defectos observados, haciendo constar en dicho escrito el plazo que para ello fije y las observaciones que estime oportunas.

Si existiese reclamación por parte del contratista respecto de las observaciones formuladas por el representante del órgano de contratación, éste la elevará, con su informe, al órgano de contratación, que resolverá sobre el particular.

Si el contratista no reclamase por escrito respecto a las observaciones del representante del órgano de contratación se entenderá que se encuentra conforme con las mismas y obligado a corregir o remediar los defectos observados.

A la extinción del contrato, no podrá producirse en ningún caso la consolidación de las personas que hayan realizado los trabajos objeto del contrato como personal del organismo contratante.

Cláusula 19. *Cumplimiento del contrato y recepción del servicio.*

El contrato se entenderá cumplido por el contratista cuando, transcurrido el plazo de vigencia total del contrato, aquél haya realizado de acuerdo con los términos del mismo y a satisfacción del órgano de contratación de su objeto.

Una vez cumplidos los trámites señalados en la cláusula anterior, si se considera que la prestación objeto del contrato reúne las condiciones debidas, se procederá mediante acto formal a su recepción, que tendrá lugar dentro de los siete días siguientes de haberse producido la entrega o realización del objeto del contrato, levantándose al efecto el acta correspondiente.

Si los trabajos efectuados no se adecuan a la prestación contratada, como consecuencia de vicios o defectos imputables al contratista, el órgano de contratación podrá rechazar la misma, quedando exento de la obligación de pago o teniendo derecho, en su caso, a la recuperación del precio satisfecho.

Cláusula 20. *Liquidación del contrato.*

Dentro del plazo de siete días a contar desde la fecha de recepción del contrato el órgano de contratación deberá acordar y notificar al contratista la liquidación del contrato y abonarle, en su caso, el saldo resultante. Si se produjese demora en el pago del saldo de liquidación, el contratista tendrá derecho a percibir los intereses de demora y la indemnización por los costes de cobro en los términos previstos en la Ley por la que se establecen medidas de lucha contra la morosidad en las operaciones comerciales.

Cláusula 21. *Propiedad de los trabajos y protección de datos de carácter personal.*

Todos los estudios y documentos elaborados en ejecución del contrato serán propiedad del órgano de contratación quien podrá reproducirlos, publicarlos y divulgarlos total o parcialmente sin que pueda oponerse a ello el adjudicatario autor de los trabajos.

El adjudicatario no podrá hacer ningún uso o divulgación de los estudios y documentos elaborados con motivo de la ejecución de este contrato, bien sea en forma total o parcial, directa o extractada, sin autorización expresa del órgano de contratación.

El contratista, como encargado del tratamiento, tal y como se define en la letra g) del artículo 3 de ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, queda obligado al cumplimiento de lo dispuesto en la citada Ley y especialmente en lo indicado en sus artículos 9, 10, 12 y adoptará las medidas de seguridad que le correspondan según el Reglamento de Medidas de Seguridad, aprobado por Real Decreto 994/1999, de 11 de junio.

Anexos

Anonimia, Unlinkability, invisibilidad y pseudónimia

El conjunto de la terminología que utilizamos en este trabajo es precisa.Define claramente los límites de la privacidad, pero sobre todo el modo de la observación de la misma por parte de las diferentes interfaces. Más concretamente, se define la anonimia (anonymity), unlinkability, invisibilidad(unobservability), y los pseudonimia (pseudonymity). Este capítulo se hace con la finalidad de la adopción por el lector de la terminología utilizada, aunque no dejan de ser unas palabras que los investigadores utilizan de manera inventada desde cero para marcar el concepto.

Se desarrolla esta terminología en el campo de la transmisión de información entre remitentes que envían mensajes a destinatarios mediante una red de comunicación. Todas estas definiciones y conceptos nuevos se realizan desde la perspectiva de un atacante que se encuentra interesado en la captación de la información que se está produciendo en la red. Lo que refiere a los patrones de comunicación, o incluso en la manipulación de la comunicación.

Anonimia (anonymity)

La anonimia es el estado de ser no identificable dentro de un conjunto de temas. El conjunto de los temas de la anonimia es el conjunto de todos los temas posibles que pueden causar una acción. Por lo tanto, un remitente puede ser anónimo sólo dentro de un conjunto potencial de remitentes, su conjunto de remitentes anónimos, puede ser a su vez un subconjunto de todos los sujetos del mundo que pueden enviar mensajes en la red global. Lo mismo es cierto para el receptor, que puede ser anónimo dentro de un conjunto de posibles receptores, que forman el conjunto de destinatarios anónimos. Ambos conjuntos de anonimia pueden ser el mismo o pueden ser parte uno del otro, etc.

El anonimato es el estado más fuerte o rocoso, cuanto mayor sea el conjunto de anonimia respectivo y es el que se distribuye más uniformemente el envío o la recepción, respectivamente, de los sujetos dentro de ese conjunto.

Unlinkability

La Unlinkability de dos o más elementos significa que dentro de un sistema, estos elementos no puedan ser relacionados entre sí más de lo que eran a priori de su conexión. Esto nos indica que la probabilidad de que esos elementos de la conexión sean relacionados entre sí permanece igual a la que tenían antes de la conexión y después de la conexión en el sistema, que es donde recibe el posible conocimiento el

atacante. Normalmente, el conocimiento del atacante sólo puede aumentar a medida que se van realizando conexiones.

Por ejemplo, dos mensajes son unlinkability si la probabilidad de que sean enviados por el mismo remitente y/o recibidos por el mismo receptor es la misma que las impuestas por el conocimiento que tenemos de esa conexión a priori.

El anonimato en Términos de Unlinkability

Si tenemos en cuenta el envío y recepción de mensajes como los elementos de interés (IOIs), el anonimato puede ser definido como unlinkability de un IOI y un identificador de un sujeto (ID). Más concretamente, podemos describir el anonimato de un IOI de tal manera que no es enlazable en cualquier ID, y el anonimato de un ID como no siendo vinculable a cualquier IOI.

Así que entendemos el anonimato remitente como las propiedades que posee un mensaje en particular de no ser vinculable a cualquier remitente y que, para un determinado remitente, ningún mensaje es enlazable. Lo mismo es cierto para el anonimato relativo al destinatario, lo que significa que un mensaje particular no se pueda vincular a cualquier destinatario y que a un destinatario particular, no se puede enlazar ningún mensaje.

Una propiedad más débil para el caso del anonimato entre el remitente y destinatario es el anonimato de relación, es decir, que pueda ser trazable el envío de los mensajes y también que pueda ser posible determinar los mensajes que recibe, pero que sea imposible encontrar qué se comunica con quién. En otras palabras, que el remitente y el destinatario (o destinatarios en caso de multicast) son unlinkable.

Inobservabilidad o invisibilidad (unobservability)

Imposibilidad de observación es el estado de IOIs ser indistinguible desde cualquier IOI de la red. Esto significa que los mensajes no son detectables a partir de "ruido aleatorio". Como en la anonimia también podemos hablar de conjuntos o grupos, en la inobservabilidad contamos con los conjuntos con respecto a la imposibilidad de determinados IOIs de observación.

La inobservabilidad del conjunto remitente consiste en que no es perceptible si algún remitente de dentro del conjunto envía información. Por simetría tenemos que la inobservabilidad del conjunto receptor entonces significa que no es distinguible si algún destinatario dentro del conjunto inobservable recibe paquetes. Por último, la relación de inobservabilidad, entonces significa, que no es perceptible cualquier conexión, dato, etc. que se pudiera enviar desde un conjunto de remitentes a un conjunto de receptores.

Pseudonimia

Los pseudónimos son identificadores de los sujetos, en nuestro contexto del remitente y del destinatario. Pseudonimia es el uso de seudónimos como identificadores (IDs). Así el remitente pseudónimo se define por el uso del remitente de un pseudónimo, receptor pseudónimo se define por el uso del destinatario de un pseudónimo.

Un pseudónimo digital es una cadena de bits que da:

- Identificación única
- Autentificación al titular y a su IOI o IOIs, comopor ejemplo, sus mensajes.

Seudonimia con respeto a linkability

La pseudonimia comprende todos los grados de linkability a un sujeto. Algunos tipos de pseudónimos permiten hacer frente a las reclamaciones a titulares en caso de abuso de unlinkability: En primer lugar, un tercero puede tener la posibilidad de revelar la identidad del titular con el fin de proporcionar los medios necesarios para la investigación o el enjuiciamiento. En segundo lugar, terceras personas puedan actuar como intermediarios de responsabilidad del titular para borrar una deuda o resolver una reclamación.Hay muchas propiedades de los pseudónimos que pueden ser de importancia en contextos específicos de aplicación. Por ejemplo, destacaremos las más importantes que entran de lleno en el tema que nos abarca con la relación de la linkability debido a su utilización:

Los mecanismos conocidos y otras propiedades de Seudónimos

Un seudónimo digital podría ser utilizado como una clave pública para comprobar las firmas digitales cuando el titular del pseudónimo puede probar titularidad mediante la formación de una firma digital que se ha creado usando la clave privada correspondiente. El ejemplo más destacado de seudónimos digitales son las claves públicas generadas por el usuario como, por ejemplo, utilizando PGP8.

Para el uso de PGP, cada usuario puede crear un número ilimitado de pares de claves por él mismo, como podría ser; uniendo cada uno de ellos a una dirección de e-mail, auto-certificando cada clave pública usando su firma digital, etc.

Un certificado de clave pública tiene una firma digital de un certificado denominado autoridad y se refiere a la unión de una clave pública a un sujeto. Un certificado de atributo es un certificado digital que contiene información adicional (los atributos) y claramente se refiere a un determinado certificado de clave pública. Independientemente de la certificación TES, los atributos pueden ser utilizados como identificadores de conjuntos de temas. Normalmente, los atributos se refieren a grupos de sujetos, y no a un sujeto específico.