UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf

Escola Tècnica Superior d'Enginyeria Informàtica

Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Pruebas y evidencias telemáticas

Trabajo Fin de Grado

Grado en Ingeniería Informática

Autor: Jordi Magraner Gimeno

Tutor: Juan Vicente Oltra Gutiérrez

2014-2015

Resumen

En este trabajo se documenta la problemática que ha surgido a la hora de identificar, esclarecer y posteriormente imputar los delitos informáticos. Por una parte se analizan las características que ofrecen los medios telemáticos para la comisión de dichos delitos y el ámbito legal que intenta combatirlos. Por otra parte se detalla el papel de la informática forense, concretamente en lo que refiere a la evidencia digital y el concepto de prueba. Finalmente se describe el perfil del perito informático y se proponen una serie de herramientas de apoyo al análisis forense digital.

Palabras clave: delitos informáticos, medios telemáticos, ámbito legal, informática forense, evidencia, prueba, perito.

Abstract

This work is a review about the problem that has emerged in order to identify, clarify and impute the cybercrimes. On one hand it is analyzed the characteristics that telematics offer to perform mentioned crimes and the legal scope that try to fight them. On the other hand, it is also detailed the role of forensic informatics, specifically the concepts of digital evidence and proof of the crime. Finally, it is described the proficient informatics profile and it is proposed a list of support tools for the digital forensic analysis.

Keywords : cybercrimes, telematics, legal scope, forensic informatics, evidence, proof.

Tabla de contenidos

Índice de tablas y figuras

1. OBJETO Y OBJETIVOS

El objeto del presente Trabajo Fin de Grado, es la obtención del título de graduado en Ingeniería Informática, expedido por la Universitat Politècnica de València.

En lo que a objetivos se refiere, el presente trabajo alberga dos con la misma importancia:

- El primer objetivo es dar a conocer al lector, teniendo en cuenta que éste puede ser ajeno al mundo de la informática, conceptos básicos y avanzados sobre las pruebas y evidencias telemáticas.

- El segundo es exponer la problemática que presentan las nuevas tecnologías de la información en lo que a seguridad se refiere. Se pretende que al leer el presente trabajo se adquiera conocimiento sobre los delitos informáticos, sus consecuencias, la manera de combatirlos y la legislación que los controla.

Finalmente, con el objetivo de seguir ampliando conocimientos en el futuro, al margen de este trabajo, se ha realizado un blog donde publicar artículos e información de interés relacionada con la temática tratada, para que sea fácilmente accesible a cualquier usuario que esté interesado.

2 INTRODUCCIÓN

A lo largo de la historia el ser humano ha tenido la necesidad de intercambiar información, por ello, no han dejado de desarrollarse métodos y tecnologías para poder llevar a cabo esta comunicación. Con ése fin nace la informática y posteriormente internet, una tecnología capaz de comunicar a millones de personas en todo el mundo de forma instantánea y que se ha convertido en una herramienta indispensable para realizar las acciones del día a día.

Este constante progreso tecnológico que ha experimentado nuestra sociedad en los últimos tiempos, ha supuesto ventajas y facilidades en el manejo de la información que son obvias en pleno siglo XXI. Por el contrario las desventajas y riesgos no son tan obvios, ya que el desarrollo de las tecnologías informáticas ha supuesto la aparición y evolución de nuevas formas de delinquir, dando lugar a los denominados delitos informáticos.

El Trabajo Fin de Grado que aquí se presenta, titulado “pruebas y evidencias telemáticas” pretende describir la problemática que ha supuesto la aparición de los delitos informáticos, haciendo especial hincapié en sus características y en el ámbito legal que intenta combatirlos. Además se detallará el papel de la informática forense como medio de resolución de los conflictos telemáticos que tienen lugar en la actualidad, haciendo referencia a la evidencia digital y a los medios de prueba existentes. Por último, y no por ello menos importante, se describirá el perfil del perito informático y de algunas herramientas que le pueden ser de utilidad para realizar un correcto análisis forense digital.

3 METODOLOGÍA Y HERRAMIENTAS

Para el desarrollo de este trabajo, se ha recabado, filtrado y revisado gran cantidad de información a través de internet, algunos libros, apuntes de asignaturas, y con el apoyo de otros trabajos fin de grado o proyectos final de carrera que guardan relación o tienen características similares a las del presente trabajo.

Entre las herramientas principales empleadas para la realización de este trabajo tenemos las siguientes: Microsoft Word para la redacción, la herramienta riunet para la búsqueda de trabajos de otros años y la herramienta politube para la consulta de videos docentes, ambas herramientas pertenecientes a la Universitat politècnica de València.

En lo que respecta a la creación de la bitácora web, cabe destacar la herramienta Godaddy para la gestión del dominio, y la herramienta Webempresa para la gestión del *hosting*. Además de otras herramientas de creación de imágenes como pixlr.

4 DELITOS INFORMÁTICOS

4.1 Definición:

El constante progreso tecnológico que ha experimentado nuestra sociedad en los últimos tiempos, sobre todo en lo relacionado a aspectos informáticos y al uso de esta tecnología para realizar acciones del día a día, ha supuesto la aparición y evolución de nuevas posibilidades de delinquir, apoyándose en técnicas o mecanismos informáticos.

El aumento de los delitos relacionados con las redes, sistemas y datos informáticos ha creado la necesidad de utilizar una definición que agrupe todos estos comportamientos delictivos bajo el nombre de **delitos informáticos**, aunque también se suelen usar otras denominaciones como **ciberdelito** o **delitos telemáticos.**

Existe una compleja situación a la hora de definir los delitos informáticos, ya que este término, no tiene ninguna definición formal. Un delito según la RAE, es la acción u omisión voluntaria penada por la ley, con lo cual, se considerará delito todo el hecho regulado en el código penal. El código penal español no contempla los delitos informáticos como tal, pero si están tipificados una serie de delitos como por ejemplo: delitos de estafa, delitos contra la propiedad intelectual o casos de mayor gravedad como la pornografía infantil o apoyo al terrorismo, que teniendo a los sistemas informáticos como objeto del ataque, o como fin de este, quedarían englobados dentro del término delitos informáticos.

Pese a no tener una tipificación en el código penal, se hace necesario aceptar la expresión y por tanto tener una definición de esta. Existen numerosas definiciones del llamado delito informático, por su claridad recurrimos a la construcción doctrinal de Miguel Angel Davara quien en el manual de derecho informático (2008) define el delito informático como " *la realización de una acción que, reuniendo las características que delimitan el concepto delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software"*

La expresión "elemento informático" empleada por Davara, se usa en un sentido muy amplio, ya que el delito puede haber sido cometido utilizando un ordenador (incluidos programas), contra un ordenador o sobre la información y los procesos a los que se pueda tener acceso aprovechando las facilidades de la informática y telemática.

4.2 Características de los delitos informáticos

Aquellos delitos considerados informáticos, reúnen unas determinadas características que dificultan la detección de los hechos, el esclarecimiento y la posterior detención e imputación de los autores.

Debido a la naturaleza de las tecnologías de la información actuales, resulta muy complicada la detección a simple vista de cualquier acción fraudulenta, esto es debido a que la información se encuentra codificada en recursos magnéticos. Además aunque se intente analizar en profundidad un sistema, por tener indicios de que se haya llevado a cabo un acto delictivo, este análisis es posible que no sea capaz de esclarecer los hechos, ya que programas y datos se pueden alterar y posteriormente borrar las pruebas fácilmente sin dejar rastro con una instrucción de borrado, camuflando el cambio como un error de sistema o con la modificación de un programa que al realizar la actividad ilícita que beneficia al autor, vuelva a su estado inicial.

Si la detección del acto delictivo y la obtención de las pruebas y evidencias resulta una tarea compleja, más difícil aún es comprobar quién fue el autor de los hechos, debido a que incluso los sistemas más simples precisan de altos conocimientos técnicos para ser penetrados. Esta capacidad técnica que debe tener el delincuente generalmente le permite utilizar métodos para debilitar los análisis de computación forense y no ser detectado.

Además, la gran expansión de internet unida con la descentralización de los actuales sistemas informáticos, que permiten ser accedidos remotamente aunque el usuario no se encuentre sentado frente al ordenador, son un arma potente para los delincuentes informáticos, que pueden realizar sus actos delictivos, sin necesidad de presencia física en el lugar de los hechos y en cuestión de segundos.

El anuario estadístico del ministerio del interior del 2013, introduce un apartado dedicado a la cibercriminalidad. En este informe podemos encontrar datos sobre el número de delitos informáticos detectados, el número de hechos esclarecidos y el número de imputados por dichos actos. Los datos corresponden a la actividad registrada por los cuerpos y fuerzas de seguridad del estado y cuerpos de la policía local, que fueron facilitados al sistema estadístico de criminalidad durante el año 2013.

Figura 1: Número de hechos conocidos, esclarecidos y detenidos e imputados por delitos informáticos en los años 2011, 2012, 2013. Fuente: Ministerio del interior, 2013

En la **Figura 1**, se puede apreciar el numero de delitos detectados y el escaso número de detenidos e imputados en relación a los hechos conocidos, quedando de manifiesto la dificultad de detectar al autor de los actos fraudulentos, debido a las características que se han comentado sobre los delitos informáticos.

4.3 Clasificación de los tipos de delito

Con la intención de conseguir frenar los delitos informáticos, favorecidos por el uso cada vez mayor de tecnologías de la información y por la necesidad de crear un marco legal común, los países miembros de la unión europea junto con Estados Unidos, Canadá y Japón, el 23 de noviembre de 2001 firman en Budapest el Convenio de Ciberdelincuencia del Consejo de Europa. Este convenio supone el primer tratado internacional que tiene como objetivo hacer frente a los delitos informáticos.

Las conductas ilícitas que aparecen en este tratado, transpuestas a nuestra legislación, quedan clasificadas en los siguientes cuatro grupos de delitos informáticos:

1. **Delitos de intrusión contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos**. Dentro de estos delitos se incluirían, los accesos ilícitos tanto a la totalidad como a una parte de los sistemas informáticos, interceptación ilícita, interferencia en los datos, atentado contra la integridad del sistema y abuso de los dispositivos técnicos. Algunos ejemplos de este grupo de delitos son el robo de identidades, intercepción de claves, difusión de información o acceso a redes sin autorización.

2. **Delitos informáticos como la falsificación de datos informáticos**, introduciendo, alterando o borrando datos con el objetivo de que sean tomados en cuenta a efectos legales. También se incluiría en este punto el fraude informático, siendo estos, actos fraudulentos o delictivos, que intentan obtener para uno mismo o para otra persona, un beneficio económico ilegitimo.

3. **Delitos relacionados con el contenido**, donde se incluye la producción, la oferta, la puesta a disposición, difusión, adquisición y posesión de pornografía infantil con vistas a su difusión por medio de sistemas informáticos.

4. **Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines** como la piratería informática o la copia y distribución de programas informáticos.

Posteriormente, en el año 2003 se promulgó el Protocolo Adicional al convenio de Ciberdelincuencia relativo a la penalización de actos de índole xenófoba o racista cometidos por medio de sistemas informáticos. Firmado por España en noviembre de 2013, en él se incluyen los siguientes delitos:

- Difusión de material xenófobo o racista.
- Insultos o amenazas con motivación xenófoba o racista.
- Negociación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad.

Existen otras clasificaciones de los delitos informáticos siguiendo distintos criterios, puede resultar interesante la clasificación de estos tipos de delitos propuesta por las Naciones Unidas:

- Fraudes cometidos mediante manipulación informática como manipulación de datos de entrada/salida o manipulación de programas informáticos.
- Falsificación informática, teniendo a esta tanto como objeto del delito como instrumento.
- Daños o modificaciones de programas o datos como el sabotaje informático, el acceso no autorizado a servicios y sistemas informáticos, la reproducción no autorizada de programas informáticos de protección legal.

4.4 Ámbito legal

En este apartado se va ha hablar de aquellos aspectos legales que guardan relación con los delitos informáticos y que forman la base de un proceso judicial. El proceso judicial, es el conjunto de actos realizados por un tribunal, desde la demanda hasta la sentencia o decisión judicial.

Podemos hablar de proceso en distintos contextos y con diferentes normativas, así, tenemos:

- Procesos Civiles: Ley de Enjuiciamiento Civil 1/2000. (normativa de aplicación supletoria al resto de los procedimientos).
- Procesos Penales: Ley de Enjuiciamiento Criminal.
- Procesos Sociales: Ley reguladora de la Jurisdicción social.
- Procesos Contencioso Administrativos: Ley reguladora de la Jurisdicción Contencioso administrativa.

Todos estos procesos, constan de tres fases que se muestran en la siguiente tabla:

Fase de alegaciones
•Las partes exponen los hechos y las razones jurídicas en virtud de las cuales quieren obtener un pronunciamiento judicial favorable a sus intereses.
Fase de prueba
•Las partes intentan convencer al juez o tribunal de la existencia o no, verdad o falsedad de un dato procesal determinado. Hay que probar lo que se alega, por ejemplo, aportando un dictamen pericial.
Fase de conclusiones
•Las partes argumentarían al tribunal las razones por las cuales consideran que han sido probados los hechos alegados por ellos.

Tabla 1: Fases de los procesos judiciales.

En relación a lo que venimos denominando delitos informáticos, el nuevo Código Penal Español, aprobado por Ley Orgánica 10/1995, de 23 de noviembre, supone un gran acercamiento a este tipo de delitos, aunque como se ha dicho no se contemplen estos como tal, ya que la informática no ha generado delitos nuevos sino nuevas formas de poder cometerlos. Aunque todavía es insuficiente y se manifiesta un cierto grado de desconocimiento en lo que a fenómenos informáticos y telemáticos se refiere, supone

un gran avance en la lucha contra la delincuencia informática, ya que por primera vez figuran en la legislación penal términos como informática, internet, soportes informáticos o correo electrónico.

Son varios los artículos del código penal (con las sucesivas reformas que ha sufrido hasta la actualidad) que directa o indirectamente se refieren a las acciones dolosas o imprudentes cometidas a través de medios informáticos. Frente a este hecho, aparecen opiniones enfrentadas, debido a que no todos apoyan los artículos del nuevo código penal, alegando que atentan contra algunos derechos y libertades, como el derecho a la intimidad o el derecho a la libertad de acceso a la información.

En el articulo 18 de la Constitución Española se garantiza " el derecho al honor, a la intimidad personal y familiar y a la propia imagen". Algunos detractores de la reforma, argumentan que en el intento de prevenir o investigar algunos delitos, se invade la privacidad de las comunicaciones y se vulnera la intimidad. Por otro lado se hace necesaria esta regulación para evitar que exista impunidad ante actos que atenten contra este derecho.

Algunos usuarios también creen que la libertad de acceso a la información, está un escalón por encima de la ley de propiedad intelectual o la propiedad de los datos, es decir, que la información que se puede encontrar en la red, no esta sujeta a las leyes de propiedad del autor, sino que son de dominio público.

Hay que ser conscientes de que aunque en la legislación española no se contemplen los delitos informáticos, algunos países como Alemania o Francia, si que han implantado leyes especificas para combatir los crímenes informáticos. Por este hecho, lo que en España puede considerarse una infracción generalmente castigada con sanción económica, en otro país puede suponer un delito que en algunos casos se pagaría con privación de la libertad.

En el nuevo Código Penal español, tan susceptible de múltiples interpretaciones y de diversas opiniones, se incluyen multitud de conductas ilícitas que guardan una estrecha relación con los llamados delitos informáticos. A continuación se citan aquellos delitos de nuestro Código Penal que guardan más relación con la clasificación de los delitos informáticos propuesta en el convenio de ciberdelincuencia del consejo de Europa, y los distintos artículos donde podemos encontrarlos, teniendo en cuenta las últimas reformas publicadas en el BOE el 31/03/2015 y recopiladas en: Red derecho TICS, Lorenzo Cotino, 2015, Código Penal versión 2015.

- Delitos contra la propiedad intelectual o la propiedad industrial

- En relación a la propiedad intelectual, se castigará a quienes reproduzcan, distribuyan o comuniquen públicamente, parte o totalidad de una obra literaria, artística o científica, con ánimo de lucro y en perjuicio de terceros (CP arts. 270 a 272).
- Respecto a la propiedad industrial, no sólo es delito la copia directa (CP arts. 273 a 277) sino también comerciar con copias ilegales de productos protegidos (CP arts. 294 a 308).

- Delitos contra el derecho a la intimidad

- Interceptación de comunicaciones utilizando la informática como medio, para el descubrimiento, revelación de secretos y otras agresiones a la intimidad. (CP arts. 197 a 201). Si además del delito contra la intimidad, los datos personales están protegido, se sumaría una sanción por la infracción de la LPD.

- Delitos contra el patrimonio

- En los delitos contra el patrimonio, se consideran los actos de estafas, apropiación indebida (CP arts. 252 a 254) y fraudes (CP arts. 255 y 256)

- Delitos de sabotaje informático

- En este caso, la informática no sería el medio del delito, si no el objeto de este, estando ante un delito de daños y estragos. El código penal regula estos daños y/o estragos en los artículos 263 a 269, 346,376, 351 y siguientes.

- Delitos convencionales

- Puede darse el caso que al margen de los delitos, se lleven a cabo infracciones administrativas en nuestro país, pero que en otros pueden constituir un delito propiamente dicho. Este sería el caso del espionaje, espionaje industrial o terrorismo industrial

- Delitos de mal uso de la red

- Usos comerciales no éticos (*spam*).
- Actos parasitarios: Enviar excesivo texto insultar o interrumpir conversaciones por ejemplo en chats.
- Obscenidades: Es el caso en el que se pública información ofensiva.

- Delitos contra la libertad y amenazas

- Efectuar amenazas sirviéndose de la informática o la telemática, por ejemplo a través de redes sociales o mail (CP arts. 169 y siguientes).

- Delitos contra el honor: Injurias y calumnias

- La injuria es toda acción o expresión que lesiona la dignidad de una persona, mientras que la calumnia es toda imputación de un delito con conocimiento de su falsedad o desprecio hacia la verdad.

- Delitos contra el mercado y los consumidores

- Revelación de secretos (CP art. 278).
- Publicidad engañosa (CP art. 282).
- Falsedades documentales (CP arts. 390 y siguientes).

- Delitos contra la libertad sexual

- Distribución o exhibición con fines pornográficos de menores e incapacitados (CP arts. 187 a 189).

5 INFORMÁTICA FORENSE

Con la llegada de la sociedad de la información, las nuevas tecnologías irrumpen prácticamente en todos los aspectos de nuestra vida cotidiana y es en este contexto de información electrónica, donde la informática forense está adquiriendo una gran importancia, debido al aumento del valor de los datos, su crecimiento exponencial y el aumento de actos delictivos y fraudulentos.

La informática forense, también denominada análisis forense, computación forense o examinación forense digital, es una disciplina criminalística auxiliar a la justicia moderna, una rama de las ciencias forenses, cuyo objetivo es la resolución de conflictos tecnológicos que tienen relación con la protección de datos y la seguridad informática.

Cabe señalarse, que a diferencia de la medicina forense donde existe la figura del médico forense, en el sector de la informática, tal como indica nuestro ordenamiento legal no existen "informáticos forenses" siendo el perito informático la figura más similar. Teniendo en cuenta este hecho, podría considerarse que la informática forense no existe como disciplina, debido a que no existen practicantes de la misma.

El ámbito de actuación de esta disciplina engloba todo hecho en el que un sistema informático esté involucrado, tanto si es el fin del delito como si es el medio para cometerlo haciendo que dicho sistema pueda ser objeto de análisis y estudio, y consecuentemente ser presentado como forma de prueba ante un tribunal. Para ello, se realiza un estudio exhaustivo con la intención de conocer la historia del sistema procesado y que el informe pueda ayudar a determinar:

- La compensación de los daños causados por los criminales o intrusos.
- La persecución y procesamiento judicial de los criminales.
- La creación y aplicación de medidas para prevenir casos similares.

Existen diferentes metodologías para ayudar a realizar con éxito una investigación. La que se ha propuesto consiste en una mezcla entre los protocolos propuestos por EDRM y CTOSE. El primero es un grupo de trabajo formado por miembros de todas las áreas de descubrimiento y análisis forense, del cual puede conocerse más en www.EDRM.net. La segunda propuesta proviene de CTOSE, un proyecto cofinanciado por la Unión Europea, donde diferentes universidades y empresas colaboran en busca de las buenas prácticas de la seguridad de la información.

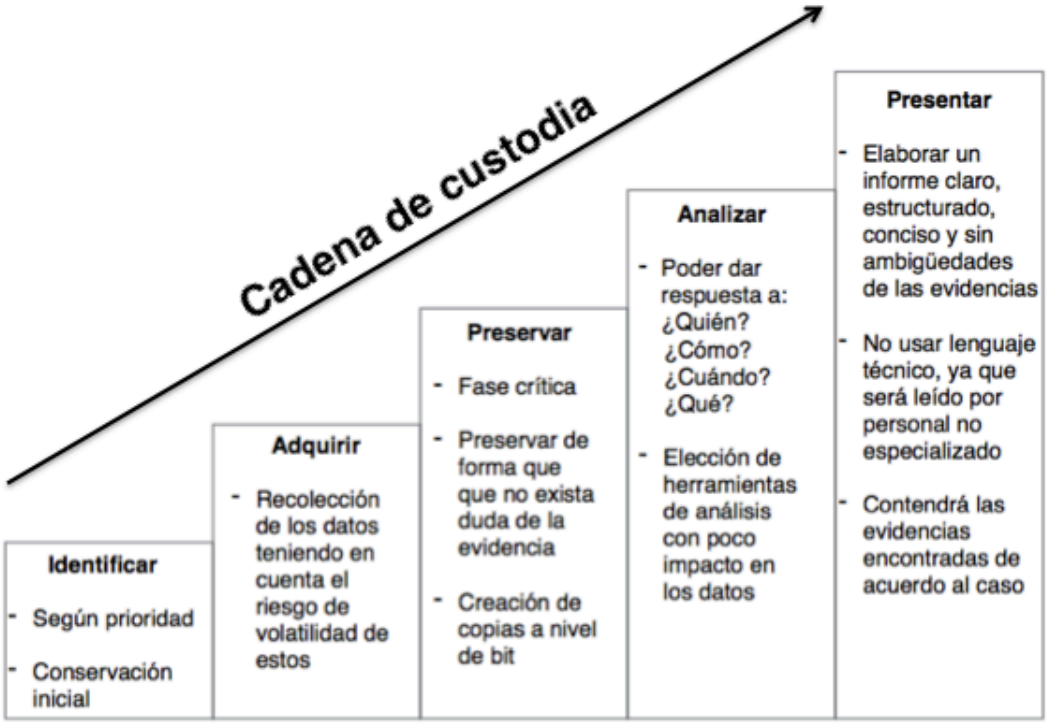


Figura 2: Metodología de un análisis forense

Como se muestra en la **Figura 2**, existen diferentes fases claramente diferenciadas para llevar a cabo un análisis forense. La metodología que se ha propuesto debido a su claridad, consiste en las fases de identificar, adquirir, preservar, analizar y presentar. Se tendrá en cuenta esta guía para obtener los datos que han sido procesados electrónicamente y guardados en un medio computacional, para su uso en un asunto legal.

Como se ha dicho, existen diferentes metodologías o fases para ayudar a realizar una investigación con éxito, las diferencias dependen del autor o incluso del caso concreto a tratar, por ejemplo, si el dispositivo sobre el que se va a realizar el análisis forense se encuentra apagado, con lo que no tenemos información volátil ni procesos en activo que pudieran ser de interés, puede resultar conveniente variar el orden de la segunda y tercera fase, pasando a preservar 'los datos realizando una copia del disco, para posteriormente pasar a la fase de adquisición. Es por este hecho que algunos autores o entidades como el EDRM, conciben estas dos fases como solo una denominándola recolección y conservación.

Todas las fases de la metodología del análisis forense por las que se van pasando, deben cumplir la denominada **cadena de custodia.**

La cadena de custodia en el caso de las evidencias informáticas tiene el objetivo de guardar un registro de las acciones y accesos, de manera que se protejan de una manipulación y se puedan controlar las acciones que se han realizado sobre las mismas.

El primer objetivo de una custodia es mantener la integridad de las pruebas, en el caso de las evidencias informáticas, esta integridad se asegura con los denominados hashes criptográficos.

El inicio de la cadena de custodia tiene lugar en la primera fase de la metodología de análisis forense, y se mantiene hasta el final, con esto se asegura que en un proceso judicial, el tribunal no llegue a excluir dichas pruebas por posibles dudas sobre el control, acceso y modificación de las pruebas,

La persona encargada de realizar el análisis, antes de empezar su investigación y tener contacto con los datos y evidencias, debe conocer bajo que condiciones sus evidencias serán consideradas como:

- Admisibles
- Completas
- Auténticas
- Confiables

El análisis forense realizado apoyándose en gran parte en la recolección de evidencias, debe responder a una serie de preguntas fundamentales como las siguientes:

- ¿Quién ha sido el sujeto que ha realizado la acción?
- ¿En qué momento se ha producido la actuación maliciosa?
- ¿Qué técnica o metodología se ha empleado para poder llevarla a cabo?
- ¿Qué daños o modificaciones se han realizado en el sistema?

Si al finalizar un análisis de evidencias, no se puede dar respuesta a las preguntas anteriores, o a otras similares que se puedan plantear, no se habrán cumplido correctamente los objetivos, es decir, no tendremos información útil y nuestras pruebas no se sostendrían ante un juez si fuese el caso, sin dejar de lado que existe la posibilidad de que se repitiesen los mismos ataques utilizando la misma vulnerabilidad.

5.1 Principio de Locard

El principio de intercambio de Locard, fue un concepto desarrollado y enunciado por el Dr.Edmon Locard (1877-1966). Considerado un pionero en su época en lo que al ámbito de la criminalística se refiere, Locard desarrolló metodologías que, aplicadas a determinadas pruebas, convertían a éstas en evidencias irrefutables ante un juez.

Locard fue famoso por sus frases y principios como por ejemplo: "*Los restos microscópicos que cubren nuestra ropa y nuestros cuerpos son testigos mudos, seguros y fieles, de nuestros movimientos y de nuestros encuentros."* o " *Es imposible que un criminal actúe, especialmente en la tensión de la acción criminal, sin dejar rastros de su presencia."* Aunque el principio más conocido es el que lleva su propio nombre: **el principio de Locard.** Se expresa de la siguiente manera:

"Siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto"

Figura 3: Imagen ilustrativa del Principio de Locard

En definitiva, se puede afirmar que al entrar en contacto con objetos o sustancias, se lleva a cabo un intercambio de material. El propio Locard estudió probabilidades de balas que emparejan, pelos y patrones de salpicaduras de sangre; y demostró que un delincuente puede ser conectado a una escena del crimen por partículas de polvo.

Muchos serían los ejemplos que podemos encontrar en la vida real que apoyan y permiten ilustrar el principio de Locard, como caminar por terrenos fangosos, las

huellas dejan un rastro durante cierto tiempo en dicho terreno, y además parte del fango también permanece en las suelas de los zapatos.

En el mundo de la informática forense, concretamente en lo que a la localización de evidencias se refiere, se puede establecer una conexión directa con el principio de Locard. Cada vez que se interactúa con un equipo se dejan ciertas huellas, por ejemplo durante una investigación se puede detectar una dirección IP sospechosa, gracias a que durante un tiempo prudencial estas permanecen en los ficheros de registro de acceso de los proveedores de servicios de Internet, podemos transformar una dirección digital en una localización física o dirección postal.

Los rastros digitales si se investigan con suficiente rigor, pueden servir para identificar a la persona que operó con el equipo, o con los procesos que en él se desarrollan. Como diría el propio Locard "*cada contacto deja un rastro"*

5.2 Evidencia Digital

En un análisis forense digital una de las tareas más importantes de la investigación es la captura de evidencias digitales o también llamadas evidencias electrónicas. Antes de empezar a detallar la compleja red que envuelve la evidencia en el área de la informática forense, se hace necesario definir éste término. Según la RAE, se define evidencia como: "*certeza clara y manifiesta de la que no se puede dudar*." En el área de la informática, una evidencia digital es cualquier información electrónica encontrada en un sistema informático, que pueda ser contrastable como por ejemplo una transacción, documento o cualquier tipo de información registrable digitalmente.

Las evidencias digitales son el elemento principal para los investigadores, y tienen una serie de características únicas que las diferencian de las evidencias de otras ramas forenses, como la medicina forense. Entre estas características podemos destacar las siguientes:

- Volátil
- Anónima
- Modificable

Estas características hacen que las evidencias digitales sean muy complejas a la hora de ser adquiridas, ya que estamos ante pruebas que no son físicas que además pueden desaparecer fácilmente, pueden dejar de existir, y son fácilmente modificables.

Estas características en comparación con otras áreas forenses son un inconveniente, y para ello vamos a demostrarlo con un ejemplo: Supongamos que un hombre ha decidido atracar un banco a punta de pistola y para ello el ladrón ha tenido que disparar al guardia de seguridad, y ha huido con un coche que tenía en la puerta. En este caso el médico forense encargado de investigar el cuerpo del guardia tiene ante si una prueba física que en mejor o en peor estado siempre va ha existir, lo mismo ocurre con el investigador experto en balística encargado de comprobar que esa bala a sido disparada con una determinada pistola, el arma puede estar en la escena del crimen o puede habérsela llevado el atracador, pero tanto la bala como la pistola, son pruebas físicas no volátiles, que van a existir, no se pueden eliminar con un formateo y tampoco se van a volatilizar. Obviamente se puede constatar que el atracador a estado en el lugar de los hechos a una hora y un lugar determinado, como se podrá comprobar por cámaras de seguridad y que además ha huido con un coche que se puede modificar, pintar o quemar pero no borrar como ocurre con las evidencias digitales.

Todo lo contrario ocurre si éste mismo atraco se lleva a cabo mediante recursos informáticos y telemáticos, es decir, un pirata informático logra acceder a los servidores de un determinado banco y efectuar una serie de transacciones para robar dinero. En primer lugar y como se ha visto en el apartado 4.2 sobre las características de los delitos informáticos, el autor del hurto muy probablemente no ha estado físicamente en el lugar de los hechos, sino que ha realizado su delito a distancia, con lo que nos encontramos con un primer problema. En segundo lugar no tenemos pruebas físicas como la bala, pistola o coche, no podremos ver y palpar las evidencias, sino que tendremos que realizar un análisis forense digital para poder averiguar que ha pasado. Por la naturaleza del entorno y como característica de los delitos informáticos, sabemos que estas pruebas pueden ser borradas fácilmente sin dejar ningún tipo de rastro, o ser hábilmente camufladas. Además estas evidencias al no ser físicas en algunos casos se pueden volatilizar.

No todo van a ser dificultades a lo que a evidencias digitales se refiere en comparación con las otras ramas de las ciencias forenses, ya que en algunos casos aporta grandes ventajas, el informático forense puede duplicar las evidencias tantas veces como quiera de manera muy fácil y trabajar con ellas realizando varias pruebas y análisis sin perjudicar la evidencia original. Siguiendo con el ejemplo, en el caso de atraco mediante elementos informáticos, el investigador puede clonar los discos de los ordenadores del banco y trabajar sobre estos, hecho que no se puede hacer con el

ejemplo del atracador a mano armada, ya que no se puede clonar una pistola o un coche para poder realizar pruebas.

La dificultad en los análisis forenses, no es la falta de evidencias digitales, ya que en el mundo conectado de hoy es casi imposible estar fuera de la red, de tal manera que nuestros registros no creen ningún tipo de registro electrónico. La expansión de las redes sociales como Twitter o Facebook, ha creado una nueva área de pruebas electrónicas persistentes. Casi cada acción o transacción realizada en algún momento deja rastro digitalizado: Visitas al médico, retirada de efectivo, compras, fotos, e incluso las cámaras de tráfico, que son capaces de captar la matricula de su vehículo, y situarle en un lugar concreto a una hora determinada.

Uno de los desafíos de la informática forense, no es si puede existir o no una evidencia digital, si no ¿Dónde está almacenada la evidencia? Cada vez hay más dispositivos de almacenamiento, discos duros, memorias USB, móviles, tablets, almacenamiento en la nube, entre otros. La mitad de la batalla es saber donde están las evidencias y como acceder a ellas, la otra mitad es recogerlas y manejarlas.

5.2.1 Recolección y manejo de evidencias

La recolección de información digital, es el punto más crítico de todo el proceso de análisis forense de un determinado sistema, ya que, es el primer punto de contacto con la evidencia y donde más probabilidades hay de modificar o dañar una prueba. La evidencia digital, dada su naturaleza, es bastante compleja y frágil. Por esta razón es de vital importancia procesar correctamente los datos, debido a que una mala manipulación de estos, puede dar lugar a la modificación de miles de pruebas, induciendo a conclusiones erróneas en el análisis, disminuyendo las posibilidades de seguir la ruta que nos permita identificar a los atacantes y teniendo un menor número de pruebas incriminatorias para el juzgamiento de los intrusos. Además de una correcta manipulación de los datos, no se deben dejar a parte, los requerimientos legales para no vulnerar en ningún momento derechos de terceros que puedan estar afectados y por si se diera un caso de litigio, las evidencias sean aceptadas como pruebas ante un tribunal.

5.2.1.1 RFC 3227

A la hora de recoger evidencias de un sistema, se deben seguir una serie de pautas, garantizando que el proceso sea útil para poder realizar un análisis forense. Existen diferentes metodologías o guías que recogen pautas y procesos de actuación a la hora de realizar este tipo de análisis. De entre ellos, nos centraremos en el documento RFC 3227 por tratarse de uno de los referentes en lo que a procesos tecnológicos se refiere.

Los artículos RFC o "Requests For Comments" son documentos públicos, que recogen propuestas de expertos y están sometidos al debate de la comunidad. En ellos encontramos la base teórica de los principales protocolos, procesos y tecnologías una guía de alto nivel que recoge los procedimientos y recomendaciones a la hora de tratar pruebas digitales.

El RFC 3227 escrito en febrero de 2002 por Dominique Brezinski y Tom Killalea, ingenieros del Network Working Group, es un documento que recoge las directrices y recomendaciones para la recolección de evidencias, su almacenamiento y algunos aspectos del ámbito legal. Su estructura es:

1. **Principios para la recolección de evidencias.**
   Realizar un análisis forense, es una tarea delicada que debe cumplir unos requisitos básicos para que el proceso resulte un éxito.

   - **Orden de volatilidad de los datos.** A la hora de recoger evidencias, hay que tener en cuenta el marco temporal, ya que no todas las evidencias tienen el mismo orden de volatilidad. Teniendo en cuenta esto, se procederá a la recolección de datos dando preferencia a los contenidos más volátiles, es decir, si tenemos que recoger información de una memoria RAM y de un CD, se dará preferencia al primer caso debido al alto riesgo de volatilidad de este dispositivo de almacenamiento.

   - **Acciones que deben ser evitadas.** Es muy fácil destruir una evidencia por error, invalidar un proceso de análisis forense o corromper una prueba destinada a una causa legal. Para evitar estas acciones, hay que tomar ciertas precauciones como pueden ser: no parar hasta que se concluya la recolección de pruebas, no fiarse de los programas del sistema, o no ejecutar programas que modifiquen el tiempo de acceso de todos los archivos del sistema.

- **Consideraciones relativas a la privacidad de los datos.** En un análisis forense se tiene acceso a datos que pueden estar sujetos a una ley de privacidad, con lo que hay que respetar el marco legal y velar por la seguridad y privacidad de dichos datos. Por ejemplo, datos personales en un disco duro, o credenciales de acceso a redes sociales. La mejor consideración es no inmiscuirse en la información personal, si no existe una justificación de que estos datos puedan aportar evidencias para el análisis.

- **Consideraciones legales.** Para que las evidencias recabadas en un proceso de análisis forense, formen parte de un proceso legal, se deben de tomar una serie de precauciones. Por ejemplo, que no exista evidencia alguna de una mala manipulación de los datos o que sea fácilmente comprensible por un tribunal sin conocimientos informáticos. Además, se debe tener en cuenta que la legislación cambia dependiendo del país, y puede que una determinada prueba sea aceptada en un juicio y en otro no.

2. Procedimientos de recolección

Los procedimientos de recolección deben ser lo más detallados posibles, intentando que exista la menor perdida de información, y que esta sea lo más pura que se pueda.

- **Transparencia.** Los métodos utilizados para reunir pruebas deben ser transparentes y reproducibles. Hay que evitar herramientas y procedimientos de los que no se conozca el uso que esta haciendo de la información, para evitar extraer conclusiones erróneas. Es recomendable utilizar técnicas y herramientas que permitan conocer como se están tratando las evidencias.

- **Pasos de recolección.**
  - ¿Dónde está la evidencia? Listar los sistemas involucrados en el incidente.
  - Determinar qué información es relevante, en caso de duda, es mejor recopilar más de la cuenta.
  - Fijar el orden de volatilidad para cada sistema.
  - Obtener la información acorde al orden establecido en el paso anterior.
  - Comprobar el grado de sincronización con el reloj del sistema.

- Según se realicen los pasos de recolección, preguntarse que más podría considerarse una evidencia.
- Documentar cada paso incluyendo fechas y horas.
- No olvidar la gente involucrada, tomar nota de que personas estaban presentes, que estaban haciendo, que observaron y como reaccionaron.

3. Procedimiento de almacenamiento

Para que las evidencias tengan validez en un proceso judicial deben estar debidamente protegidas y la custodia debe estar claramente documentada.

- **Cadena de custodia de la información.** Se trata de la protección general de las pruebas. En todo momento se debe poder describir la forma de conseguir la evidencia, como se manejó y todo lo que pasó con ella. Además, tiene que ser posible constatar quién entrega la información y quién es el responsable de custodiarla, para que se pueda conocer el flujo de la misma desde la recolección hasta su utilización como prueba.

- **Metodologías de almacenamiento de evidencias.** Almacenar las evidencias es una parte muy importante para garantizar la seguridad y la validez de estas. Para ello es necesario que estos medios de almacenamiento aseguren tener un periodo de vida mayor al tiempo que pueda durar el proceso judicial, pero también se tiene que probar la seguridad de estos dispositivos y a través de medios de solo lectura.

4. Recomendaciones

El documento recoge la problemática de la realización de un análisis forense riguroso y propone una serie de recomendaciones.

- Comprometer al personal para la aplicación de la ley y la adecuada operativa frente a la aparición de incidentes.
- Capturar una imagen tan exacta del sistema como sea posible, para trabajar sobre ella y dejar la original intacta.
- Almacenar toda la información posible sobre la investigación en curso para ayudar a entender el incidente producido.

5.3 Concepto de prueba

En el anterior apartado se ha detallado el concepto de evidencia, concretamente el de evidencia electrónica o digital así como las recomendaciones para que estas evidencias sean válidas o aceptadas como prueba. Ante este hecho, nos puede surgir la duda sobre ¿Cuál es la diferencia entre evidencia y prueba?, para ello nos acogemos al diccionario de la Real Academia de la Lengua Española (RAE) quien define la prueba como: "*acción y efecto de probar. Razón, argumento, instrumento u otro medio con que se pretende mostrar y hacer patente la verdad o falsedad de algo".* En el Ordenamiento Jurídico español, concretamente en los artículos 299 a 386 de la Ley de Enjuiciamiento Civil (LEC) se puede definir la prueba como, aquella actividad que generalmente se desarrolla por iniciativa o a instancia de las partes, en virtud de la cual una o varias personas expertas en la materia a peritar, elaboran o transmiten al Tribunal información especializada dirigida a permitir a éste el conocimiento y apreciación de hechos y circunstancias perteneciente o relativo a hechos del proceso. Teniendo en cuenta lo dispuesto en la LEC, desde el punto de vista del perito informático, la diferencia es básicamente semántica, ya que la recolección de evidencias realizada en su investigación supondrán pruebas en un proceso judicial.

5.3.1 Medios de prueba

Los medios de prueba son un instrumento corporal o material que permiten a cada una de las partes, establecer los motivos y fundamentos en los que se basan sus pretensiones, y cuya apreciación constituye para el juez la fuente de donde ha de obtener la convicción sobre el hecho que se trate de probar.

El artículo 299 de la LEC, establece los medios de prueba de los que se podrá hacer uso en un juicio. Estos son los siguientes:

- Interrogatorio de las partes.
- Documentos públicos.
- Documentos privados.
- Dictamen de peritos.
- Reconocimiento judicial.
- Interrogatorio de testigos.

5.3.2 Derechos concernientes a la prueba

En el artículo 24.2 de la Constitución Española, queda recogido que "…todos tienen derecho… a utilizar los medios de prueba pertinentes para su defensa...". De este derecho constitucional se derivan los siguientes derechos:

- **El derecho a proponer la prueba.** Según el art. 282 de la LEC, en los procesos civiles son las partes las que proponen los medios de prueba que sirven para demostrar y probar los hechos por ellas presentados. Con independencia de lo anterior el órgano jurisdiccional puede acordar el uso de medios adicionales de prueba.
- **El derecho a la admisión de la prueba.** El legislador debe garantizar este derecho y no existen limitaciones que obliguen a descartar o seleccionar determinadas pruebas siempre que estas, como se especifica en el art. 283 de la LEC, tengan finalidad demostrativa o esclarecedora para el asunto que se juzgue.
- **El derecho a practicar la prueba admitida.** Una vez la prueba sea admitida lo lógico es que ésta sea practicada, aunque no es obligatorio que esto ocurra, pudiendo darse el caso que no todas las pruebas admitidas sean practicadas, dependiendo de las circunstancias propias de cada proceso.
- **El derecho a la correcta valoración de la prueba practicada.** El objetivo de la prueba es convencer al juez en relación al asunto tratado, por lo tanto la valoración de la prueba corresponde al juez. Tal como indica el artículo 384.3 de la LEC, el Tribunal valorará los instrumentos y elementos que se le presenten como prueba conforme a las reglas de la sana crítica, es decir, sin que tengan que sujetarse a los dictámenes aportados por los peritos.

Teniendo en cuenta los derechos concernientes a la prueba conviene hablar del artículo 283 de la LEC:

1. No deberá admitirse ninguna prueba que, por no guardar relación con lo que sea objeto del proceso, haya de considerarse impertinente.

2. Tampoco deben admitirse por inútiles, aquellas pruebas que, según reglas y criterios razonables y seguros, en ningún caso puedan contribuir a esclarecer los hechos controvertidos.

3. Nunca se admitirá como prueba cualquier actividad prohibida por la Ley.

5.4 Buenas prácticas para la recogida y análisis de los datos

Ya se ha explicado la importancia de la recolección manejo y custodia de evidencias, pero no solo es importante el tratamiento de datos, estamos ante una investigación en la que todos los detalles son indispensables, por tanto la persona encargada de analizar los equipos debe conocer y seguir las mejores prácticas para el ejercicio de su función. Para que el análisis forense sea correcto, el analista debe ser una persona muy metódica, que realice todas las fases del proceso siguiendo las recomendaciones y que con meticulosidad pase por las distintas etapas de un análisis forense digital.

Las mejores prácticas suelen centrarse en las partes más críticas que son la recolección y preservación de evidencias, pero se hace necesario prestar especial atención al equipo que se va a analizar, se debe conocer su arquitectura, que tipo de software y hardware emplea y como trabaja. Sin el conocimiento del sistema, capturar las evidencias puede resultar bastante complicado y puede dar lugar a errores al finalizar el análisis. Evidentemente también obtendremos resultados no válidos si tenemos un alto conocimiento del sistema pero no realizamos la captura de huellas digitales siguiendo unas pautas o metodologías como por ejemplo las que se indican en el documento RFC 3327. Otro aspecto crucial en la investigación, es la utilización de la herramienta adecuada que permita la recogida de evidencias de un determinado tipo en un equipo concreto. Si la herramienta necesaria no existe, o no se adapta al caso investigado, se deberá crear y por tanto nuevamente es necesario un conocimiento de la arquitectura de los sistemas analizados.

5.4.1 Estudio preliminar del entorno

El paso inicial de cualquier análisis forense, es realizar un estudio preliminar en el que se detalle qué ha ocurrido para que se decida iniciar un análisis forense, cuál fue la acción maliciosa, cómo se realizó y cuándo se detectó. También es necesaria información de la persona o entidad apoderada de los equipos que van a ser objeto de análisis, y todo lo que nos pueda ayudar a saber que a ocurrido, como tipología de red empleada, por si existen otros equipos conectados a la misma red que puedan estar implicados. El medio donde se encuentran él o los sistemas implicados, también debe ser tomado en cuenta así como la gente que ha podido estar implicada directamente con el suceso o indirectamente como testigo de los hechos.

En el estudio preliminar del escenario donde se encuentran los equipos a analizar, es conveniente llevar una cámara fotográfica o de video, para poder tener una imagen del

entorno, de los posibles equipos implicados y de las pantallas de los ordenadores que se encuentran en funcionamiento. También es necesario un rotulador para CD, todos los soportes de datos deberán ser incluidos en un inventario y estar fotografiados, para poder demostrar en el futuro que dichos dispositivos fueron encontrados en el lugar intervenido.

5.4.2 Equipos involucrados en la incidencia

Ante un equipo afectado por un determinado ataque o incidencia, nos puede surgir el dilema de apagarlo o no, para intentar minimizar las consecuencias de la intrusión. Es necesario recordar que al apagar el sistema toda la información volátil se perderá, pudiendo ser ésta de vital importancia para el transcurso de la investigación, como puede ser, tener una copia de la información almacenada en la memoria RAM. Por otro lado, mantener el equipo encendido, puede suponer un riesgo para otros sistemas conectados a la misma red, que podrían ser atacados fácilmente. Además mantener encendido el sistema, puede ser beneficioso para el atacante que tendrá tiempo de borrar todos sus rastros, siendo perjudicial para la posterior investigación.

Ante esta disyuntiva, de mantener encendido o apagar el equipo, se deben tener en cuenta las circunstancias de cada caso y tomar la decisión que más favorezca a la investigación.

Si se opta por apagar el sistema, la forma de hacerlo será desconectando el equipo directamente de la red eléctrica, o quitando la batería si se diera el caso de un ordenador portátil u otro dispositivo móvil. La razón, es que en un apagado ordenado, gran parte de los ficheros temporales que podrían ser de gran ayuda para la investigación, serían borrados automáticamente por el sistema. Por este riesgo de borrado o modificación de ficheros durante el apagado ordenado, es más conveniente desconectar la fuente de energía.

Si por el contrario la decisión es mantener el equipo o equipos encendidos, en la medida que sea posible se tendrán que aislar de las conexiones con otros sistemas, para evitar que el ataque se propague, por ejemplo desconectando el equipo atacado de la red local i de cualquier conexión con otros dispositivos.

5.4.3 Utilización de herramientas

Realizado adecuadamente el estudio preliminar del entorno de los equipos y tomada la decisión de apagar o no los sistemas en el caso de que estén encendidos, se debe pasar a uno de los puntos más críticos de un análisis forense, la elección de las herramientas sobre las que trabajar. En la investigación necesitamos la máxima cantidad de información posible, y hay que tener en cuenta que cada bit que nuestra herramienta ocupe en memoria, será un bit de memoria que no podremos analizar. Es por este hecho, que debemos utilizar herramientas lo menos intrusivas posibles, que sean simples, con pocos elementos gráficos y que no requieran instalación con el objetivo de evitar que se produzca un alto consumo de memoria RAM. Bajo ningún caso utilizaremos herramientas del sistema, ya que pueden estar manipuladas y es recomendable que las aplicaciones utilizadas, estén almacenadas en algún soporte externo como CD o memorias flash.

5.4.4 Copia del sistema

Para poder preservar la información y poder realizar el posterior análisis, es necesario obtener una copia de seguridad del sistema. Al realizar una copia se buscará que sea lo más idéntica y fiel al sistema original, utilizaremos herramientas punteras que nos permitan realizar una copia “bit a bit” pudiendo asegurar la integridad. Lo recomendable es realizar varias copias y que queden almacenadas físicamente de forma segura en algún dispositivo. Las copias deben estar firmadas digitalmente con algún algoritmo de autenticación (hash) como SHA-1, SHA2 o MD5 aunque este último se utiliza cada vez menos.

Por sus características las funciones hash son ideales para asegurar la integridad:

- Dada la salida no se puede generar la entrada que la genera.
- Cualquier cambio de entrada provoca cambio en el resultado.

Una de las copias deberá ser guardada asegurando su custodia, otra copia la destinaremos al trabajo de análisis y es recomendable que exista una tercera copia para entregar a la persona o entidad afectada por si desea iniciar una investigación paralela para tener una segunda opinión. Bajo ningún concepto se debe analizar o modificar los ficheros del sistema almacenados en el dispositivo de almacenamiento original, ya que este hecho podría suponer la invalidación del mismo como prueba.

6. PERFIL DEL PERITO INFORMÁTICO

Ante la situación cada vez más habitual en estos tiempos de encontrarnos con delitos informáticos, se hacen necesarios expertos profesionales informáticos, que ante estos hechos sean capaces de generar un dictamen pericial que sirva de prueba para esclarecer las cuestiones surgidas del acto delictivo.

En el Diccionario de la Lengua española se define **pericia** como: *"Sabiduría, práctica, experiencia y habilidad en una ciencia o arte."* Y **Perito** como: " *Persona que, poseyendo especiales conocimientos teóricos o prácticos, informa bajo juramento, al juzgador sobre puntos litigiosos en cuanto se relaciona con su especial saber o experiencia"*

Así pues, un perito informático, será aquella persona especialista en informática que mediante la realización de un análisis forense informático , interpretará los puntos dudosos por medio de un informe o dictamen que constituirá una prueba o indicio útil, para el proceso jurídico.

Los dictámenes periciales son un elemento de prueba para un juicio tal como indica el artículo 299 de la Ley de Enjuiciamiento Civil, además la tarea del perito no solamente consistirá en escribir el informe, sino que casi con toda seguridad le llamaran el día del juicio para hacer las aclaraciones que solicite un fiscal, abogado o juez. Estas actuaciones englobadas en los procesos judiciales, son hechos muy serios que requieren de un alto empeño y seriedad para no incurrir en ninguno de los tres tipos de responsabilidades: civil, penal y profesional.

6.1 Ámbitos de actuación

Los ámbitos de actuación de un perito informático son muy diversos, estos pueden tener carácter judicial o extrajudicial.

- **Perito Extrajudicial**: Es aquel que actúa fuera de un procedimiento penal o judicial, donde se precise su dictamen para un mejor conocimiento de los hechos y en los casos solicitados por particulares. Podrá ejercer de perito en los casos de arbitraje y mediación. Se entiende por arbitraje la institución en que las personas físicas o jurídicas puedan someter, previo convenio, a la decisión de uno o varios árbitros las cuestiones litigiosas surgidas o que puedan surgir en una materia.

Mediante el arbitraje se evita llegar a los tribunales, siempre que no se haya infringido alguna ley, en este caso no se podría llevar a cabo la ley de arbitraje y pasaríamos a un proceso judicial.

Aceptar el arbitraje obliga a cumplir el encargo, siendo el árbitro responsable de los daños y prejuicios que cause por mala fe, temeridad o dolo. El árbitro debe tratar a las partes con igualdad y dar a cada una de ellas la posibilidad de hacer valer sus derechos. Los árbitros, las partes y las instituciones arbitrales, deben mantener la confidencialidad de las informaciones tratadas, por esto el árbitro debe ser independiente, preservar la igualdad entre las partes y ser discreto.

El proceso arbitral es mucho más flexible que el proceso judicial, pues queda en manos de las partes determinar el lugar donde tratar el conflicto, el idioma, e incluso acordar que no tenga parte oral y se lleve a cabo por escrito. Por último cabe destacar los dos tipos de arbitraje existentes, el arbitraje formal, que se realiza de acuerdo en lo dispuesto en la ley de arbitraje, y el informal que se realiza al margen de dicha ley.

- **Perito judicial**: En el caso de que nos encontremos ante un caso de peritaje judicial, el perito podrá ser nombrado por el juzgado, o por una de las partes litigantes. La Ley de Enjuiciamiento Civil dedica sus artículos 610 a 632 a los peritos, y en estos consta el deber de tener títulos en la ciencia o arte sobre la que se va a realizar el dictamen, quedando su profesión reglamentada por las leyes o por el gobierno.

  No habiendo peritos de la clase requerida, si las partes no llegan a un acuerdo para designarlos de otro modo, podrán ser nombrados peritos a personas entendidas, con conocimientos o prácticas especiales en alguna ciencia aunque no posean titulo.

  Por la vía penal, la Ley de Enjuiciamiento Criminal divide a los peritos en titulares y no titulares, siendo de preferencia para un juez asignar a los peritos titulares frente a los que no poseen titulo (art. 458 LECR). Además los reconocimientos periciales se harán por dos peritos, exceptuando el caso de que no hubiera más de uno y esperar la llegada de otro tuviese graves consecuencias para el curso del sumario (art. 459 LECR).

6.1.1 Factores influyentes en los diferentes ámbitos de actuación

Papel desempeñado	Tipo de caso	Condiciones de trabajo	Cuando está involucrado
Apoyo al demandante	Civil	Amistoso	Antes de toda actuación legal
Apoyo al demandado	Criminal	Neutral	Durante la investigación
Actuación como parte neutral	Empleo	Carencia de apoyo	Durante la captura de datos
Investigar para un particular/empresa	Divorcio	Hostil	Durante la revisión y análisis de los datos
Investigar para un particular/empresa	Fraude	Modo invisible	Justo antes del inicio del juicio

Tabla 2: Situaciones a las que se puede enfrentar un perito informático, adaptación del libro de Linda Volonino (Computer forensics pág 121 y ss)

En la **Tabla 2**, podemos apreciar los diferentes papeles que puede desempeñar un perito informático, dependiendo del tipo del caso y las condiciones de trabajo. Linda Volonio describe las distintas condiciones que envuelven el trabajo de peritaje, de la siguiente forma:

- Ambiente hostil: Un ejemplo sería un perito contratado por la parte del demandante para investigar un caso en el que se sospecha que un ex empleado robó unos planos de ingeniería y se los suministró a su nuevo jefe. El investigador copia ficheros, correo electrónico y registros de red, del antiguo ordenador del empleado, mientras el personal de sistemas TIC pone mala cara, ya que ellos son los responsables de controlar el acceso a archivos confidenciales y que obviamente no hicieron su trabajo como debían.

- Modo invisible: El director de recursos humanos de una empresa, contrata a un perito para que lleve a cabo una investigación con el objetivo de saber si un empleado esta violando la política de empresa viendo pornografía. Esta investigación debe ser realizada sin alertar al empleado ni a cualquier otra persona de la empresa, y por tanto se trabaja a partir de las 10 pm, cuando la oficina está vacía, para poder crear la copia de ficheros.

- Ambiente neutral: El abogado de una persona acusada de haber comprado o descargado pornografía infantil, contacta con un perito y le envía un cd que contiene la imagen del ordenador de su cliente. El investigador también recibe los detalles de las cookies y los archivos utilizados recientemente. La revisión y análisis demuestran la presencia de unos pocos ficheros de imágenes, todas con tamaño de archivo más pequeño a 10 kilobytes (KB), la mayoría menor a 5k. Los tamaños de archivo obtenido demuestran que son miniaturas de imagen, además no existe evidencia de comportamiento pederasta (por ejemplo, archivos no organizados, sin directorios ni nombres de usuario ni cuentas de correo electrónico que demostraran su interés en este tipo de contenido). La revisión muestra muchas visitas a páginas con contenido pornográfico para adultos, donde las miniaturas podrían haber sido descargadas inconscientemente.

- Entorno amistoso o carente de apoyo: Justo una semana antes de que comience un juicio, el fiscal pide a un perito informático que confirme que el sospechoso ha enviado amenazas por correo electrónico, tal como corroboran otro tipo de pruebas como cartas, faxes y amenazas en persona. El análisis muestra que el correo había sido enviado desde la cuenta del sospechoso, pero ¿Cómo ligar esos correos con el sospechoso? ¿Cómo saber que era él y no otra persona, la que envió el correo? Nadie puede responder a eso por lo que no se pueden vincular los mensajes con el sospechoso.

6.2 Nombramiento de los peritos judiciales

Los peritos que entrarán a formar parte de un proceso judicial, se pueden nombrar de las siguientes formas:

- Por acuerdo de las partes, este se manifiesta de manera oral y en comparecencia ante el juez.

- Por insaculación o sorteo (ante una causa civil, al menos se insacularán cinco).

- Por designación judicial (como se ha dicho en el apartado de ámbitos de actuación de un perito judicial, ante causa criminal se exigirán dos informes periciales).

En el mes de enero de cada año, según el artículo 341 de la LEC, se remite a los juzgados una lista de peritos informáticos, estas listas son facilitadas por los colegios y asociaciones profesionales que dan una relación de los colegiados o asociados que pueden intervenir como peritos en asuntos judiciales, tanto civiles como penales. En la elección del perito es de vital importancia tener en cuenta la materia y objeto de trabajo a realizar y mas teniendo en cuenta la amplitud de las diferentes áreas de la tecnología.

Una vez que un perito a sido nombrado por un tribunal o juez, por propuesta de las partes implicadas o por el mismo tribunal, el perito puede ser recusado. La recusación significa no ser admitido, en este caso como perito, para intervenir en un proceso judicial por una serie de razones que especifica la ley. Entre las causas de recusación se encuentran:

- Ser perito con parentesco a una de las partes, bien sea por consanguinidad o afinidad dentro del cuarto grado civil de la parte contraria.

- Tener interés directo o indirecto en el asunto a tratar u otro semejante.

- Haber prestado servicios como tal perito al litigante contrario o ser dependiente o socio del mismo.

- Tener amistad íntima o enemistad manifiesta con alguna de las partes, incluidos los procuradores o abogados.

- Haber dado anteriormente sobre el mismo asunto dictamen contrario a la parte recusante.

Al margen de poder ser recusado, el perito debe aceptar o rechazar el cargo explícitamente si desea o no desea realizarlo. Además un perito debe rechazar el trabajo, si cree que no corresponde con el perfil de informático, si cree que sus conocimientos y experiencia no son suficientes para poder realizar un dictamen o si cree que no dispone de la información necesaria para realizar el trabajo y consecuentemente llevarle a tener una mala actuación pericial, lo que puede conllevar fuertes sanciones.

6.3 Dictamen o informe pericial

Una vez obtenido el resultado de la investigación teniendo en cuenta todo lo expuesto en el apartado 5, sobre la evidencia digital, su manejo y las buenas prácticas para la recogida y análisis, llega el momento de elaborar el dictamen. Un dictamen es un informe escrito que es elaborado y debidamente razonado por un profesional en la materia que será entregado para su estudio, con el objetivo de que pase a convertirse en prueba.

Siempre que sea posible el informe realizado debe contrastarse con otros expertos, asegurándonos de que se mantiene la confidencialidad. Estos expertos a partir de la documentación elaborada pueden determinar si a su juicio las conclusiones obtenidas son las adecuadas y para aportar diferentes ideas o subsanar algunas lagunas que puedan surgir.

No hay que olvidar que el informe o dictamen pericial pretende aclarar preguntas o asuntos a quienes no tienen los conocimientos técnicos necesarios, por lo que deben ser redactados pensando en el lector con la mayor claridad y concisión, es decir sin utilizar tecnicismos y sin excederse en más páginas de las necesarias. La mayoría de las veces se complementa el informe con un anexo que contiene la documentación más técnica con el objetivo de que sirva en caso de posibles revisiones periciales y como no para cubrirse las espaldas. Además de este anexo, se suelen adjuntar otros documentos como la relación de los elementos utilizados en la investigación y una relación de ficheros como pueden ser cuentas de correo, con una descripción del contenido de cada uno de ellos.

No existe un modelo perfecto para la elaboración de un informe ya que en la práctica los peritos se ajustan a los diferentes casos, pero a modo orientativo, las partes que debe contener son las que se muestran a continuación:

Consulta: Se expone brevemente la consulta que nos hacen. En caso de que la consulta sea por vía judicial, deberán aparecer los datos del juzgado, los autos, clases de juicio junto con nombre y apellidos del demandado.

Antecedentes: Se detallarán de forma clara y concisa los antecedentes del caso.

Limitaciones: Se reflejará todo lo que haya podido suponer un impedimento en la obtención de las pruebas (por ejemplo si no se a podido obtener una determinada información).

Alegaciones y consideraciones: En función de todo lo anterior, se harán las alegaciones de carácter técnico, científico y jurídico. Estas tendrán una base práctica (basada en la experiencia) y otra teórica (basada en libros, manuales, etc.).

Conclusiones: Se terminará el dictamen con la opinión del perito según lo expuesto anteriormente, como siempre con claridad, concisión y evitando términos técnicos para que el juez no interprete de forma equivocada la opinión.

Observaciones: Destinadas a posibles desconocedores de la materia.

Firma: Preferiblemente en todas las hojas.

7. HERRAMIENTAS PARA EL ANÁLISIS FORENSE

Hasta ahora se han desarrollado las características de los delitos informáticos, las diferentes fases de un análisis forense digital y el perfil del perito informático. Nos queda una parte muy importante, que no es otra que las herramientas a utilizar durante la investigación.

Las herramientas utilizadas para dar soporte a las tareas periciales con base en la informática forense son muy variadas. La elección de estas herramientas no es tarea sencilla, en primer lugar puede generarnos un gran dilema debido a los reiterados problemas de confiabilidad, seguridad y soporte, entre las dos corrientes existentes: Aquellas con un propósito y fin comercial que normalmente mantienen los procedimientos cerrados, es decir, aquellas por las que se debe pagar para su uso y aquellas que nacen de la iniciativa de una organización o comunidad, que tiene el propósito de servir como herramienta abierta. En segundo lugar se plantea el problema de los requisitos mínimos que deben cumplir para que su uso sobre las evidencias no haga más daño que bien.

Para garantizar el correcto funcionamiento y fiabilidad de las herramientas de informática forense, existen organizaciones que las prueban y validan, como el Instituto Nacional de Estándares y Tecnología (NIST) dentro de su proyecto de test de herramientas de informática forense (CFTT). El objetivo de esta organización es establecer una metodología para los equipos, criterios y procedimientos de prueba, que permitan el desarrollo de las especificaciones de la herramienta. Los resultados proporcionan la información necesaria para que los fabricantes puedan mejorar sus herramientas, y para que los usuarios tengan información suficiente para decidir que software adquirir para obtener resultados precisos y objetivos.

Una herramienta de análisis forense digital debe cumplir unos criterios mínimos para que sea conveniente utilizarla sin que pueda suponer un peligro para la investigación, estos son:

- **Definible:** Uno de los aspectos fundamentales de cualquier proceso forense, es que el propósito y resultado deseado se pueda definir, en otras palabras, a grandes rasgos y dependiendo de cada situación, debemos ser capaces de plantear el problema, saber el resultado deseado y poder describir el algoritmo utilizado en el proceso. A modo de ejemplo, imaginemos que queremos obtener la copia de una imagen digital:

Podemos definir el problema, que es la necesidad de contar con una herramienta forense que nos permita realizar una copia de la evidencia digital. El resultado esperado y deseado es obtener dicha copia idéntica y que sea verificable y repetible. Por último se debe poder describir el algoritmo que ha utilizado la herramienta durante el proceso, desglosado en pasos lógicos. Una descripción informal y lejos de la realidad que serviría para este ejemplo sería la utilización de pseudocódigo, es decir una descripción en código sencillo de lo que realmente está realizando el algoritmo con su código real, en este caso se vería algo similar a lo siguiente:

Si el sistema está encendido, escritura bloqueo está activado: (Proteger el original de la modificación)

Está bien para iniciar el proceso de copia
Mientras se está ejecutando proceso de copia
Compruebe cada bloque de datos de errores
Si no hay errores, aceptar y almacenar
Calcula MD 5-valor y el hash para ese bloque de datos para fines de verificación

De lo contrario, rechazar bloque de datos y volver a copiar
Volver a copiar bloque de datos anterior
Volver a comprobar los errores
Si todavía contiene errores después de tantos intentos, marcar como bloques dañados en almacén de información de bloques malos
Continúe con el siguiente bloque de datos
Repita hasta que todos los datos se copien y sean verificados.

- **Predecible:** Cualquier función que realice la herramienta debe ser predecible. Si la herramienta no puede dar resultados predecibles, entonces no es conveniente apostar por dicha herramienta forense. La previsibilidad en este caso significa que la herramienta se va a comportar de una manera predecible a través de cualquier uso o de cualquier función específica. En un lenguaje sencillo y siguiendo con el ejemplo de encontrar imágenes, si se supone que la herramienta encuentra ciertos tipos de imagen en un formato concreto, la predicción es que siempre va a encontrar ese tipo de imágenes y de ese formato.

- **Repetible:** La función realizada por la herramienta debe ser repetible al cien por cien, con cierta tolerancia de error. Tomemos un ejemplo de las cadenas de montaje: Una de las características de los robots que actúan en una cadena de montaje es su repetitividad, es decir tomando el caso de la Ford, el robot encargado de apretar los tornillos de las ruedas puede repetir ese mismo movimiento miles de veces de manera exacta, dentro de una tolerancia definida. En el caso de las herramientas de análisis forense digital, debe ocurrir exactamente lo mismo. Volviendo al software encargado de buscar y hacer copia de las imágenes, si en su primera ejecución obtiene 20 imágenes, si realizásemos esta misma ejecución cientos de veces, deberíamos obtener el mismo resultado.

- **Verificable:** Uno de los aspectos más importantes en el área de la informática forense, es la capacidad de verificar los resultados que hemos obtenido. En el caso de las herramientas forenses, no solo dentro de un caso de prueba en particular, sino que debe ser verificable incluso con el uso de herramientas del mismo tipo. Por ejemplo si dos examinadores distintos utilizan distinto software para poder obtener las imágenes guardadas en un mismo dispositivo, y los resultados obtenidos por cada uno de ellos difieren, sabiendo que no estamos ante un problema de interpretación del examinador, podemos concluir que una de las dos herramientas utilizadas no es verificable. La idea es que no importa qué herramienta forense esté siendo utilizada por el examinador, los resultados de su examen deben ser verificables por otro examinador, independiente de la herramienta que se utiliza siempre que las herramientas sean comparables en la especificación y función.

7.1 Clasificación de herramientas de análisis forense

Hasta el momento no existe una clasificación formal de las herramientas de software forense, pero no nos encontramos ante una tarea difícil ya que podemos agrupar las diferentes herramientas en categorías generales, tanto por tipo de disponibilidad (*open source* o comercial) como por función que realizan.

En la clasificación que se ha propuesto, se han agrupado las herramientas según su funcionalidad principal, intentando respetar el orden en el que serían utilizadas dichas herramientas en una investigación forense. Se ha analizado una herramienta de cada tipo en profundidad, y se han aportado algunas herramientas con funciones similares.

7.1.1 Adquisición de datos volátiles

7.1.1.1 Memorize: es una herramienta forense gratuita desarrollada por la compañía Mandiant, que podemos obtener en www.mandiant.com. La función que tiene esta herramienta es la de realizar un análisis de la memoria principal. Memorize no solo adquiere la memoria física de un determinado sistema, sino que es capaz de realizar un análisis avanzado de la memoria mientras el ordenador esta funcionando, es decir, puede realizar un análisis sobre una imagen del sistema o sobre el sistema en vivo.

Memorize es capaz de realizar una imagen de la memoria para posteriormente poder analizarla, aunque es capaz de trabajar sobre imagen realizada por otra herramienta de adquisición de datos volátiles.

Entre las características más relevantes que encontramos en la descripción de esta herramienta tenemos:

- Permite realizar una imagen completa de la memoria del sistema.
- Permite realizar una imagen de todos los controladores cargados en el disco.
- Es capaz de enumerar todos los procesos en ejecución (incluidos los que están escondidos por *rootkits*) y lista el espacio de direcciones virtuales del proceso .
- Memorize puede informar de todos los identificadores abiertos en un proceso (por ejemplo, todos los archivos, claves de registro etc.). También informa de los sockets abiertos; funciones importadas y exportadas por el ejecutable, calcula su firma hash (MD5, SHA-1, SHA256); verifica la firma digital de los ejecutables y sus librerías dinámicas y muestra todos los *strings* en memoria separados por procesos.

Memorize crea documentos XML que contienen el resultado del análisis, se puede utilizar la herramienta redline de Mandiant o cualquier visor de archivos XML.

La manera de trabajar con Memorize es mediante línea de comandos, para ello cada script XML ha sido envuelto por un archivo por lotes. Todo los parámetros en el script de ejecución XML se pueden modificar desde la línea de comandos con argumentos al archivo por lotes. Algunos de estos archivos son:

- MemoryDD.bat para adquirir una imagen de la memoria física.
- ProcessDD.bat para adquirir una imagen del espacio de direcciones del proceso.
- DriverDD.bat para adquirir una imagen de los drivers.

- Process.bat enumera todo lo relacionado con un proceso, como pueden ser puertos de red o memoria virtual.
- HookDetection.bat para buscar ganchos o *hooks* dentro del sistema operativo.
- DriverWalkList.bat para enumerar todos los módulos y los controladores en una lista enlazada.

Memorize se encuentra disponible para Windows 2000/XP/Vista/7/2008/Server 2012 y Mac OS X Snow Leopard/Mountain Lion. Se puede descargar en la siguiente URL: https://www.mandiant.com/resources/download/mac-memoryze.

7.1.1.2 Otras herramientas de adquisición de datos volátiles

- **Encrypted disk detector (EDD):** Una herramienta gratuita en línea de comandos que puede comprobar de forma rápida y no intrusiva volúmenes cifrados en un sistema informático durante la respuesta a incidentes. Se puede obtener en http://info.magnetforensics.com/encrypted-disk-detector.

- **The volatilty Framework:** Se trata de una herramienta open source con licencia GNU GPL, implementada en python, que permite la extracción de la memoria volátil del sistema. Esta herramienta se encuentra disponible en la siguiente URL:http://www.volatilityfoundation.org/#!releases/component_71401.

- **NotMyFault**: Con esta herramienta desarrollada por el equipo SysInternals, sólo disponible para entornos Windows, es posible provocar un BSOD (Blue Screen of death), desencadenando en un volcado controlado de la memoria principal junto al conocido pantallazo azul y pudiendo configurar la herramienta para que realice el volcado en función de unos errores específicos. Esta herramienta está disponible en: https://live.sysinternals.com/Files/.

7.1.2 Análisis de procesos

7.1.2.1 Process Monitor de Microsoft: Se trata de una herramienta avanzada de monitoreo para entornos Windows totalmente gratuita, que muestra la actividad de los registros, procesos y hilos del sistema de archivos en tiempo real. Combina las características de dos utilidades de Sysinternals heredados de Filemon y Regmon, y añade una extensa lista de mejoras que incluyen el filtrado no destructivo, propiedades de eventos como identificadores de sesión y nombres de usuario, información sobre procesos y pilas de subprocesos entre otras. Sus características son muy poderosas y hacen que Process Monitor sea una utilidad esencial en el sistema de solución de problemas y como herramienta de análisis de procesos. Podemos descargarla en la siguiente URL: https://technet.microsoft.com/en-us/library/bb896645.aspx.

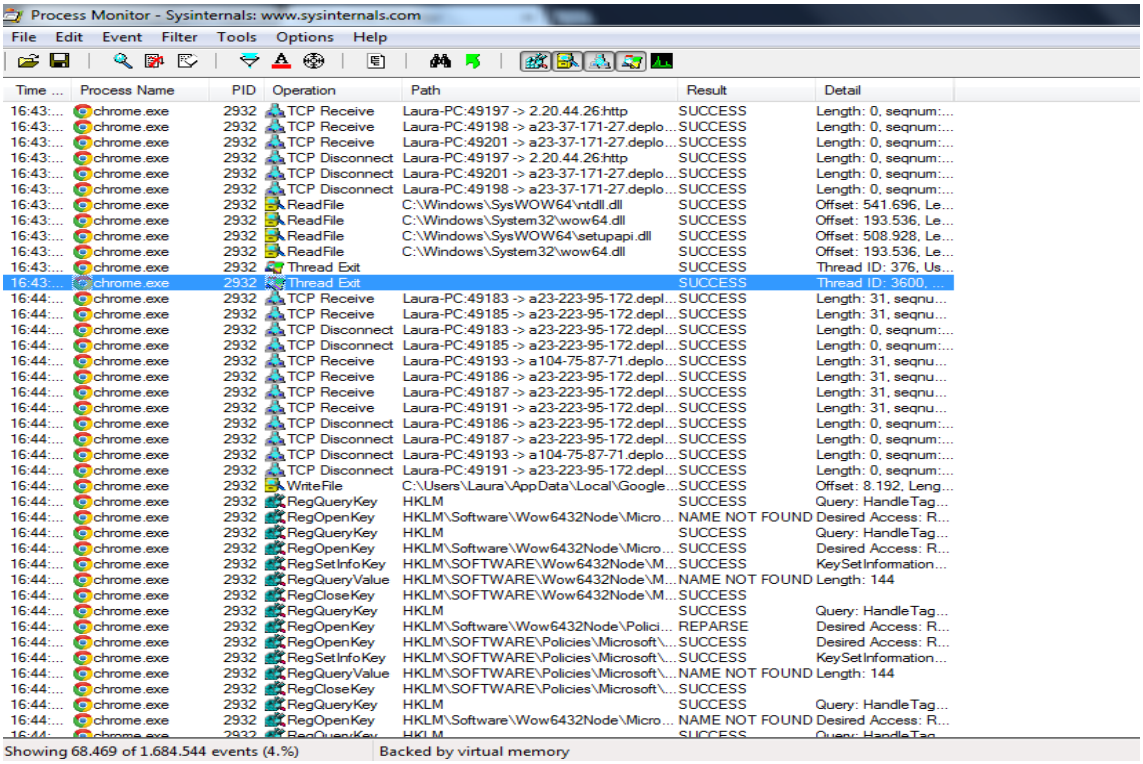


Figura 4: Ejemplo de ejecución del programa Process Monitor.

7.1.2.2 Otras herramientas de análisis de procesos

- **Process Explorer (Sysinternals):** ProcessExplorer.exe de Sysinternals es una herramienta gratuita creada por Mark Russinovich, permite analizar los procesos que se encuentran en ejecución en nuestro equipo de manera gráfica. Las posibilidades que nos ofrece esta herramienta son infinitas, y para el análisis forense de una máquina activada, es de gran utilidad. Esta herramienta se puede descargar gratuitamente en la siguiente URL: https://technet.microsoft.com/en-us/sysinternals/bb896653.aspx.

- **ProcL (Scanit.net):** Esta herramienta es realmente útil para poder descubrir procesos ocultos de un sistema, ésta es capaz de examinar todos los objetos cargados por el kernel de Microsoft Windows, inicialmente extrae la lista de procesos que es suministrada por la API del propio sistema, para posteriormente acceder con sus propias funciones a la misma información, de esta manera los procesos que se encuentren en la segunda lista que no estén en la primera será información oculta.

- **UsserAssist:** Se trata de una herramienta de código abierto creada por Didier Stevens que nos muestra una tabla con los programas que se encuentran en ejecución en una máquina con sistema operativo Windows. Esta tabla nos muestra cuando se ha realizado la última ejecución, que duración tuvo esta ejecución y cuantas veces se ha ejecutado. El explorador de Windows guarda esta información en sus entradas UsserAssist del registro.
  Esta herramienta se puede descargar desde la siguiente URL: http://blog.didierstevens.com/programs/userassist/.

7.1.3 Análisis de discos físicos.

7.1.3.1 Autopsy es una herramienta gratuita desarrollada por Brian Carrier, inicialmente desarrollada para plataformas UNIX, pero en la actualidad también se encuentra disponible para OS X y Windows. Esta herramienta ofrece una amplia variedad de funciones para los análisis de medios de almacenamiento. Entre las principales características que nos ofrece autopsy tenemos las siguientes:

- Puede analizar discos en formatos NTFS, FAT, UFS1/2, EXT2/3/4, HFS, ISO 9660 y YAFFS2.
- Permite el análisis del disco de una máquina mientras se encuentra encendida.
- Ordena los archivos por tipos, analizando sus firmas internas para saber si se han intentado ocultar cambiando la extensión.
- Permite la búsqueda de palabras clave o expresiones regulares.
- Es muy útil para la recuperación de archivos borrados ya que analiza los meta-datos en el sistema de archivos.
- Es muy útil para crear líneas temporales, ya que muestra entradas de modificación, acceso y cambio en una interfaz gráfica para ayudar a identificar la actividad.
- Visualiza archivos en gran variedad de formatos, entre ellos ASCII o Hexadecimal.
- Permite al investigador guardar notas rápidas sobre archivos para posteriormente revisarlas.
- Mantiene un control exhaustivo de la imagen mediante el valor MD5 de archivos importados y exportados.
- Permite extraer la ubicación geográfica y la información de la cámara de los archivos JPEG.
- Extrae datos de SMS, registros de llamadas, contactos… de dispositivos android.

Se ha decido probar esta herramienta debido a su gran éxito en casos de informática forense, llevados a cabo por fuerzas del orden y examinadores.

La descarga e instalación es bastante sencilla, además en la misma web de descarga podemos encontrar una guía de usuario, donde se detalla el proceso de instalación y posterior uso de la herramienta.

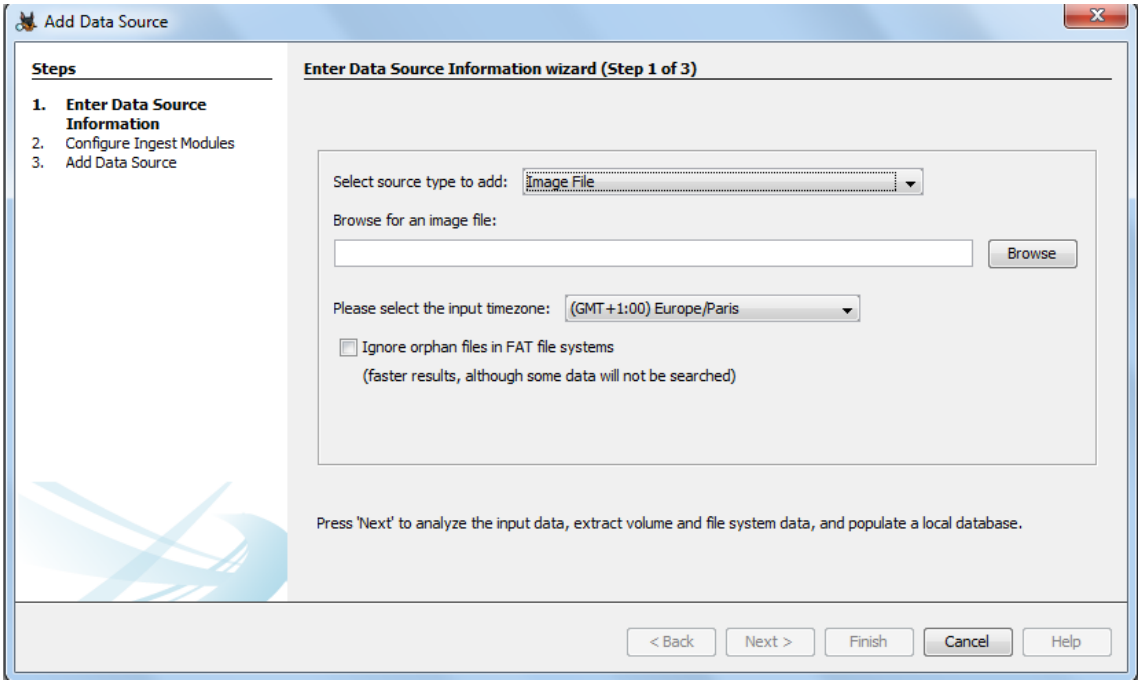


Figura 5: Ejemplo de definición del directorio destino donde almacenar los datos resultantes del análisis con el software Autopsy.

Después de descargar el software Autopsy y realizar la instalación, al entrar en la herramienta nos solicita dar un nombre al caso, y posteriormente elegir donde guardar los datos del caso. Una vez realizado estos pasos, pasamos a configurar los módulos de análisis.

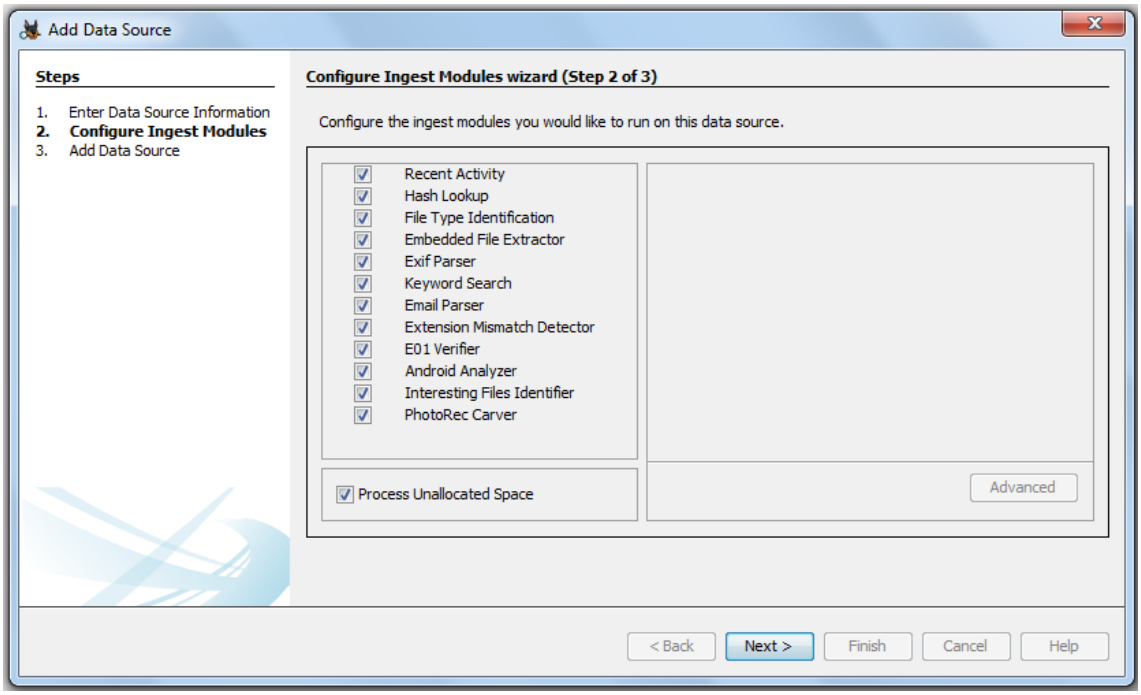


Figura 6: Captura de los módulos de análisis de Autopsy.

Podemos apreciar en la imagen, que Autopsy nos ofrece una gran cantidad de módulos para el descubrimiento de información relevante como, extraer Actividad reciente que se ha realizado en la computadora, definir una lista de palabras clave, archivos android, información EXIF de imágenes JPEG, entre otros.

A partir de este momento comienza de forma automática el análisis de módulos que hemos seleccionado. Para realizar esta operación, se ha decido utilizar un USB antiguo que contenía fotos entre otro tipo de ficheros, se ha borrado toda la información para poner a prueba la herramienta. Completado el progreso obtenemos la información que se muestra en la siguiente imagen.

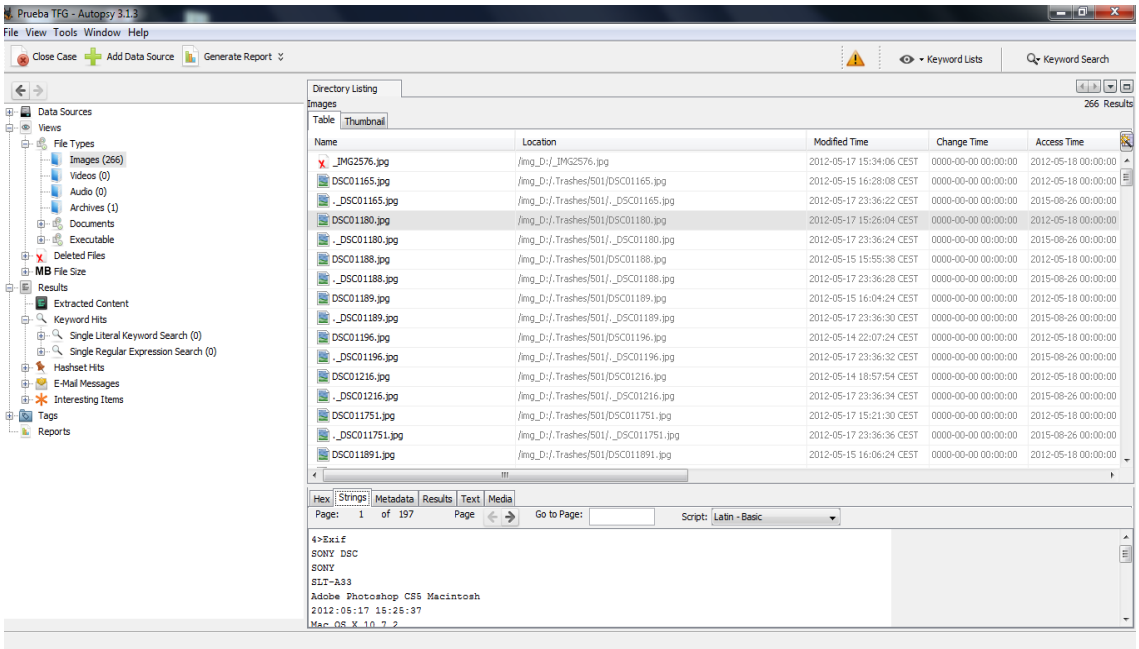


Figura 7: Captura de los datos analizados por Autopsy

La herramienta Autopsy en la parte derecha nos muestra los diferentes módulos que hemos escogido, en la parte izquierda en nuestro caso tenemos las imágenes que contenía la memoria USB, ha sido capaz de recuperar imágenes desde el año 2012, además nos muestra la línea temporal de estos archivos, como la creación y la fecha de modificación, incluso podemos obtener información más detallada si nos situamos en la pestaña Strings, donde nos muestra que la imagen seleccionada ha sido realizada con una cámara Sony, y editada por el programa adobe Photoshop CS5 en un sistema Macintosh con el sistema operativo Mac OS X 10.7.2, una información realmente sorprendente y de gran utilidad si el objetivo es encontrar evidencias digitales para un determinado caso. Esta herramienta se puede descargar en la URL: http://www.sleuthkit.org/.

7.1.3.2 Otras herramientas para el análisis de discos físicos

- **The Sleuth kit**: Se trata de un kit de herramientas desarrolladas por Brian Carrier al igual que la herramienta Autopsy. Trabaja en línea de comandos y una biblioteca de C, ésta permite analizar imágenes de un disco y recuperar archivos de estas. Es capaz de analizar diferentes sistemas de archivos independientemente de la plataforma sobre la que se use. Esta herramienta puede descargarse dese la siguiente URL: http://www.sleuthkit.org/

- **Foremost:** Una herramienta por línea de comandos desarrollada por las fuerzas áreas y el centro de estudios de seguridad de sistemas de información de los Estados Unidos. Esta herramienta esta destinada a la recuperación de archivos basándose en las estructuras internas y cabeceras de estas. Es capaz de trabajar en modo sólo lectura, preservando la validez y la integridad. Puede analizar imágenes de disco generadas por herramientas de análisis como dd, Safeback, EnCase, etc, o directamente en un disco en vivo. Podemos descargar este software en: http://foremost.sourceforge.net/.

- **Ftimes:** La herramienta software para análisis forense digital Ftimes, tiene la función de recolectar información topográfica y atributos sobre directorios y archivos. Ftimes está implementada en C, que trabaja bajo línea de comandos. Se trata de una herramienta poco intrusiva y rápida, ya que no requiere ser instalada para trabajar sobre un sistema. Entre las características básicas tenemos:
  - Monitor de integridad de todos los archivos.
  - Recolección de evidencias en sistemas en vivo y sistemas remotos.
  - Análisis de intrusiones en directorios, archivos o flujos de datos.
  - Validación de copias de seguridad.

  La herramienta se puede descargar en el siguiente enlace URL: http://ftimes.sourceforge.net/FTimes/index.shtml.

7.1.4 Análisis de redes

7.1.4.1 Wireshark: Se trata de una herramienta distribuida bajo licencia GNU GPL, desarrollada por Gerald Pintes, cuya función es capturar paquetes de red y mostrarlos de manera detallada. Wireshark es uno de los más importantes analizadores de protocolos de red del mundo, anteriormente conocido como Etheral, permite saber que ocurre en la red casi a nivel microscópico. Se ejecuta sobre la mayoría de sistemas basados en UNIX así como con Microsoft Windows. Esta herramienta es utilizada para análisis, solución de problemas de comunicación, desarrollo de software, desarrollo de protocolos y como herramienta didáctica. Puede ser descargada en: http://www.wireshark.org/.

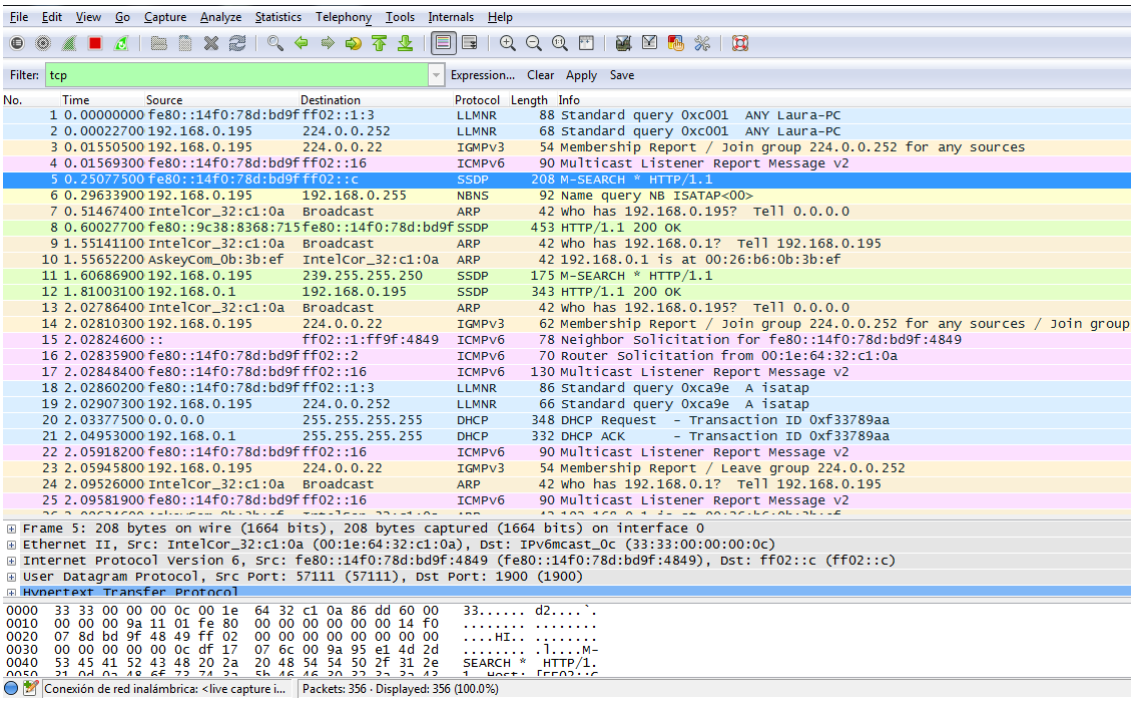


Figura 8: Ejemplo de ejecución del programa Wireshark.

Entre las funciones que nos ofrece Wireshark, cabe destacar las siguientes:

- Inspección en profundidad de centenares de protocolos.
- Captura en vivo de paquetes que circulan por la red.
- Compatibilidad con ficheros de captura elaborados con otros programas.
- Muestra los detalles de los protocolos de los paquetes capturados.
- Tiene la capacidad de exportar los paquetes en diferentes formatos.
- Puede filtrar y colorear tanto las capturas como las búsquedas, basándose en los criterios que selecciona el usuario.
- Permite calcular estadísticas sobre los datos analizados.

7.1.4.2 Otras herramientas para realizar análisis de redes

- **Netstat:** Se trata de una herramienta nativa de Microsoft Windows, disponible mediante línea de comandos que determina las conexiones activas que se encuentran abiertas en un momento dado en un determinado equipo. Aunque parezca una herramienta simple, el comando nos permite un gran número de posibilidades mediante el uso de modificadores como: La opción –a para conocer todas las conexiones o puertos en escucha abiertos, la opción –b que permite determinar cuál es el ejecutable para crear una conexión TCP/IP, o el parámetro –n que nos muestra información sobre el *socket* de conexión con sus direcciones IP y puertos tanto local como remoto.

- **Netcat:** Es una herramienta de red en línea de comandos, capaz de leer y escribir datos a través de la conexiones de red utilizando el protocolo TCP/IP. Está diseñada para que sea muy fiable y pueda ser utilizada por otras herramientas o *scripts.* Entre las características principales de este software tenemos:
  - Conexiones entrantes o salientes, TCP o UDP, desde o hasta cualquier puerto.
  - Modo *Tunneling,* con la posibilidad de especificar los parámetros de red, tales como puerto en escucha o interfaz.
  - Integra un escáner de puertos, que se puede activar para una búsqueda aleatoria.

  La herramienta Netcat se distribuye libremente bajo licencia GNU GPL, y esta disponible para su descarga en la siguiente URL: http://netcat.sourceforge.net/.

- **Tcpdump:** Esta herramienta al igual que las comentadas con anterioridad, tiene la utilidad principal de analizar el tráfico que circula por la red. Permite mostrar los paquetes transmitidos y recibidos en tiempo real. Funciona en la mayoría de sistemas basados en UNIX como Linux, Solaris, BSD o Mac os X, aunque existe una adaptación de la misma herramienta llamada WinDump, para trabajar sobre entornos Windows. Usos comunes para esta herramienta son: depurar aplicaciones que se comunican mediante la red o capturar y leer datos enviados por otros usuarios, aprovechando que algunos protocolos como el http, no cifran los datos que envían por la red. Esta herramienta se puede obtener en el siguiente enlace: http://www.tcpdump.org/.

8 Bitácora web

Gran parte de la información que contiene este documento se encuentra publicada en un sitio web que a servido como repositorio digital, a modo de blog personal.

El dominio que se deseaba para esta web, era uno que tuviese el mismo nombre que el de este trabajo, es decir, pruebas y evidencias telemáticas. Para ello con la herramienta de búsqueda de dominios Godaddy, se ha constatado que el dominio deseado estaba disponible, y posteriormente se ha pasado a contratar el dominio, que es www.pruebasyevidenciastelematicas.com.

El segundo paso ha sido contratar el hosting donde hospedar el dominio adquirido y subir nuestro blog Wordpress. Para ello se ha elegido la herramienta WebEmpresa que nos ofrece el hosting Wordpress necesario para nuestra web y los servidores de nombres necesarios para configurar los DNS. Una vez adquirido el dominio y el hosting, se configuraron los DNS y se descargó la última versión de Wordpress desde la página oficial para posteriormente pasar a configurar la base de datos.

Con la web ya en funcionamiento se empezó a dar forma de blog, para poder ir subiendo los contenidos que en este trabajo se encuentran, con la finalidad de utilizar esta herramienta a modo de bitácora y como posible ayuda, apoyo o recurso para personas interesadas en el mundo de la informática forense y sus variantes.

9 Conclusiones

Tras la realización de este trabajo, se puede concluir, que el avance de las tecnologías de la información que tantos beneficios y facilidades nos aporta en la actualidad, ha favorecido la aparición de nuevas formas para cometer actos delictivos apoyándose en los sistemas informáticos, ya sea como medio de ataque o como fin de este.

Las características que presentan los sistemas informáticos como pueden ser la volatilidad de la información, la facilidad para modificar evidencias digitales, o la capacidad de cometer los delitos remotamente, supone una gran dificultad para los peritos informáticos que intentan demostrar qué a ocurrido, cómo, cuándo y por quién.

Todo lo anterior, unido a la lentitud con la que cambian, se crean o se reestructuran nuevas leyes relacionadas con el sector tecnológico y las notables diferencias que presentan éstas dependiendo del país en el que nos encontremos, tiene como consecuencia una legislación obsoleta e insuficiente, con cierto grado de desconocimiento en tecnologías de la información y susceptible de múltiples interpretaciones, lo que hace que la lucha contra los delitos informáticos sea cada vez más complicada.

10 Glosario

• **Bit**: Un bit es un dígito del sistema de numeración binario. En el sistema de numeración decimal se usan diez dígitos, en el binario sólo dos dígitos, el 0 y el 1.

• **Cibercrimen**: Se trata de un nuevo concepto que sirve para definir las actividades delictivas que se apoyan en herramientas informáticas o telemáticas.

• **Dominio**: En este trabajo el término dominio hace referencia a los dominios de internet, que se refiere al nombre que identifica a una determinada página web.

• **Driver**: Es un programa informático que permite al sistema operativo interacción con un determinado dispositivo, en otras palabras, es una pieza esencial del software, sin la cual el hardware sería inutilizable.

• **GNU GPL**: Del Inglés GNU General Public License, se trata de un tipo de licencia software que permite la copia, distribución y modificación del código, con la condición de que cualquier modificación se distribuya bajo la misma licencia GPL.

• **Hardware**: Se refiere a todas las partes físicas de un sistema informático, tales como cables, cajas, componentes mecánicos y todo tipo de periféricos.

• **Hash o hash criptográfico**: Una función hash es un método basado en operaciones matemáticas, que sirve para generar claves que representen de manera unívoca un determinado conjunto de datos. Existen diferentes tipos de funciones hash dependiendo básicamente del número de bits utilizados. Entre las funciones hash más utilizadas tenemos SH-1, SH2 y MD5

• **Hook**: Se denomina hook al código que trata las llamadas a función, eventos o mensajes interceptados. El hooking consistes en utilizar técnicas para alterar el comportamiento de un sistema operativo, aplicaciones u otros componentes software mediante la intercepción de llamadas a función, mensajes o eventos.

• **Hosting**: Es el término en inglés utilizado para denominar los alojamientos web. La principal función de los hosting, es proveer a los usuarios de un sistema capaz de almacenar la información, imágenes, videos o cualquier contenido accesible vía web.

• **Imagen**(referida a discos): Es un archivo o unos dispositivos que contiene la estructura y contenidos completos de un dispositivo o medio de almacenamiento de datos, como un disco duro. Una imagen de disco usualmente se produce una copia

completa, sector por sector y por lo tanto replicando perfectamente la estructura y contenidos de un dispositivo de almacenamiento.

• **Kernel**: Es la parte fundamental de un sistema operativo. Es el software encargado de gestionar los recursos a través de servicios de llamada al sistema. Al haber muchos programas y el acceso al hardware ser limitado, el kernel o núcleo del sistema, es el encargado de decidir que programa podrá hacer uso de un determinado dispositivo y durante cuánto tiempo.

• **Open-Source**: Se trata del término utilizado para referirse al código fuente abierto, con el que se conoce al software o hardware distribuido y desarrollado libremente.

• **Proceso**: El término proceso utilizado en este trabajo, se refiere a un programa en ejecución. Formalmente, un proceso es: “Una unidad de actividad que se caracteriza por la ejecución de una secuencia de instrucciones, un estado actual, y un conjunto de recursos del sistema asociados”.

• **Pseudocódigo**: Es una descripción de alto nivel compacta e informal que utiliza las convenciones estructurales de un lenguaje de programación real, pero está diseñado para la lectura humana en lugar de la lectura mediante máquina, y con independencia de cualquier otro lenguaje de programación.

• **RAM**: La memoria RAM (Memoria de acceso aleatorio) se utiliza como memoria de trabajo de computadoras para el sistema operativo, los programas y la mayor parte del software.

• **Rootkits**: Es un conjunto de herramientas que permite un acceso de privilegio continuo a una computadora pero que mantiene su presencia activamente oculta al control de los administradores al corromper el funcionamiento normal del sistema operativo o de otras aplicaciones.

• **Script**: En informática un script es un programa simple que usualmente se almacena en texto plano y tiene la función de realizar tareas como: combinar componentes, interactuar con el sistema operativo o con el usuario.

• **Sistema informático**: (SI) es un sistema que permite almacenar y procesar información; es el conjunto de partes interrelacionadas: hardware, software y personal informático.

• **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.

• **Software**: Se refiere a todas las partes lógicas de un sistema informático, tales como aplicaciones o sistema operativo.

• **String**: Este término en inglés se refiera a una cadena de caracteres, se trata de la manera utilizada para almacenar de forma sencilla, datos en memoria.

• **Telemática**: El término surge de la convergencia entre las tecnologías de las telecomunicaciones y la informática. Con esta unión de disciplinas, la telemática cubre un amplio campo científico y tecnológico.

• **Tunneling**: Se conoce como tunneling a la técnica que consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel de información dentro de una red de computadoras.

• **XML**: Siglas en ingles de eXtensible Markup Language ('lenguaje de marcas extensible'), es un lenguaje de marcas desarrollado por el World Wide Web Consortium (W3C) utilizado para almacenar datos en forma legible.

11 Abreviaturas

RAE: Diccionario de la Real Academia de la Lengua Española

BOE: Boletín Oficial del Estado

CP: Código Penal

Art. : Artículo

TIC: Tecnologías de la información y la comunicación

LEC: Ley de Enjuiciamiento Civil

LECR: Ley de Enjuiciamiento Criminal

API: Interfaz de programación de aplicaciones.

12 Bibliografía

Libros y artículos

Garrido Caballero, Juan. (2010). “Análisis Forense Digital en Entornos Windows”. Informática64, Madrid.

Davara Rodriguez, Miguel Ángel. (2008). “Manual de derecho informático”. Editorial Aranzadi, SA, Navarra.

De Miguel Molina, María del Rosario y Juan Vicente Oltra. (2007). “Deontología y aspectos legales de la informática: cuestiones éticas, jurídicas y técnicas básicas”. Servicio de publicaciones de la Universitat Politècnica de València, Valencia.

Del Peso Navarro, Emilio. (1995). “Manual de dictámenes y peritajes informáticos: Análisis de casos prácticos”. Ediciones Diaz de Santos, Madrid.

Daniel Larry. (2012). “Digital Forensics for Legal Professionals”. EISEVIER, United States of America.

López Rivera, Rafael ……”Peritaje Informático y Tecnológico”…..

Vacca, J. R. (2005). Computer Forensics: Computer Crime Scene Investigation. Boston, EEUU: Thomson.

Volonino, L., & Anzaldua, R. (2008). “Computer Forensics For Dummies”. New York, EEUU: Wiley.

Tesis o PFC previos

Giménez Solano, Vicente Miguel. (2011). “Hacking y ciberdelito”. Universitat Politècnica de València.

Nebot Hernández Manuel. (2013). “Herramientas para la Informática Forense: Catalogación”. Universitat Politècnica de València.

Álvarez Galarza, María Daniela y Verónica Alexandra Guamán Reibán. (2008). “Metodologías, estrategias y herramientas de la informática forense aplicables para la dirección nacional de comunicación y criminalística de la Policía Nacional”. Universidad Politécnica Salesiana.

Recursos de Internet

Abogados Portaley Madrid Penal, Civil e Internet, http://www.portaley.com/delitos-informaticos/ (Junio 2015)

Acuario del Pino, Santiago. " Delitos informáticos: Generalidades", http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf (Junio 2015)

Agencia Española de Protección de datos (2001) ."Convenio sobre ciberdelincuencia", http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia.pdf (Julio 2015)

Boixo, Ignacio. (2003). "Guía de buenas prácticas para el peritaje informático en recuperación de imágenes y documentos", http://www.infoperitos.com/guiaimagenes.pdf(Julio 2015)

Delitos informáticos, http://www.delitosinformaticos.info (Julio 2015)

Instituto Nacional de Ciberseguridad (INCIBE), (2014). "Guía de toma de evidencias en entornos Windows", https://www.incibe.es/extfrontinteco/img/File/intecocert/ManualesGuias/incibe_toma_evidencias_analisis_forense.pdf (Julio 2015)

Instituto Nacional de Ciberseguridad (INCIBE), (2014). "RFC 3227 – Directrices para la recopilación de evidencias y su almacenamiento", https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/rfc3227 (Julio 2015)

Ley de Enjuiciamiento Civil (vigente hasta el 01 de Octubre de 2015), http://noticias.juridicas.com/base_datos/Privado/l1-2000.html (Julio 2015)

Ministerio del Interior (2013). "Cibercriminalidad", http://www.interior.gob.es/documents/10180/1207668/Avance+datos+ciberciminalidad+2013.pdf/5de24ec6-b1cc-4451-bd06-50d93c006815 (Julio 2015)

Wikipedia, https://es.wikipedia.org/ (Julio 2015)

Vídeos

Oltra Gutiérrez, Juan Vicente. (2015). “Introducción al peritaje informático”, http://hdl.handle.net/10251/52382 Universitat Politècnica de València. Escuela Técnica Superior de Ingeniería Informática- ETSINF, UPV, Valencia (Julio 2015)

Oltra Gutiérrez, Juan Vicente. (2015). “La e-evidencia”, http://hdl.handle.net/10251/51019 Universitat Politècnica de València. Escuela Técnica Superior de Ingeniería Informática- ETSINF, UPV, Valencia (Julio 2015)

13 Anexos

Anexo I: Ampliación de Autopsy mediante módulos de Basis technology

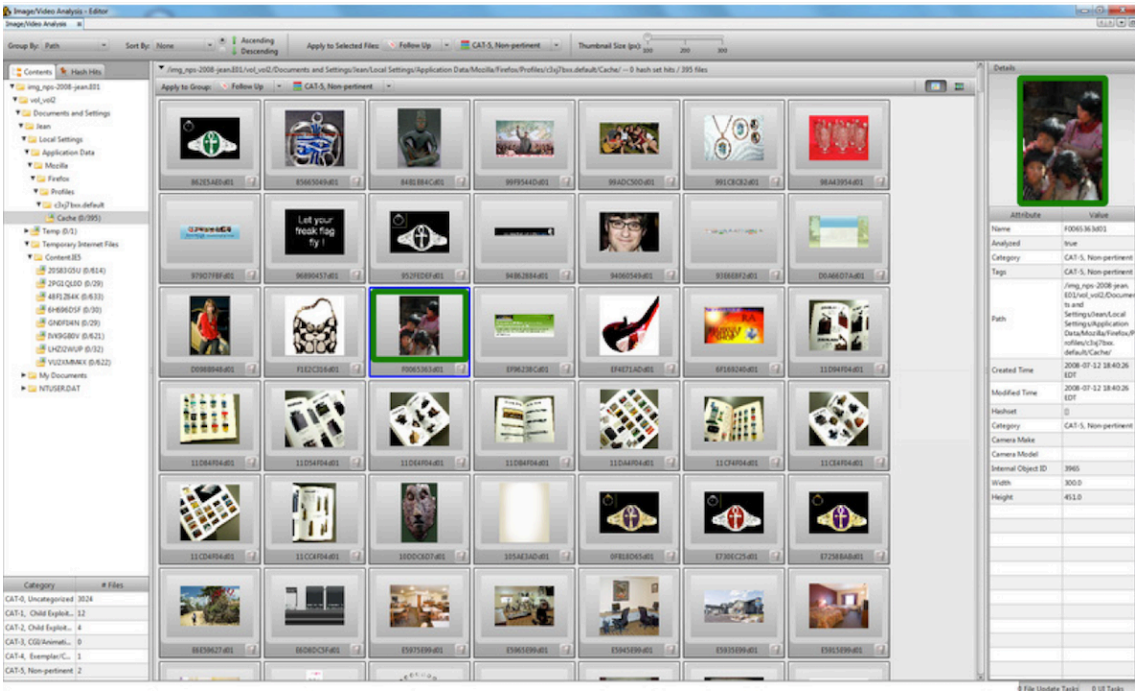
Autopsy es una plataforma de código abierto para el análisis forense digital, que tiene todas las características que normalmente podemos encontrar en herramientas forenses comerciales. Esta herramienta es extensible, es por ello que empresas como Basis technology proporciona módulos y ampliaciones, dando la posibilidad de crear funciones personalizadas a las necesidades del usuario sin tener que pagar por un sistema completo desarrollado desde cero.

A continuación se muestran los módulos que podemos añadir a Autopsy creados por Basis technology, junto a las características de cada uno de ellos. Todo ello extraído y disponible en su página web, accesible mediante la siguiente dirección URL: http://www.basistech.com/digital-forensics/autopsy/

Además, podemos encontrar un video en youtube de la ejecución de la herramienta Autopsy, proporcionado por la misma organización. Este video está disponible en el siguiente enlace https://www.youtube.com/watch?v=IUAMWvYVZD4

Modulo de análisis avanzado de imágenes y categorización

El modulo permite revisar fácilmente y de manera rápida todas las imágenes almacenadas en un determinado dispositivo, mostrándolas por categorías, identificando las coincidencias hash, para finalmente elabora un informe.



Entre los casos de uso de este módulo encontramos:

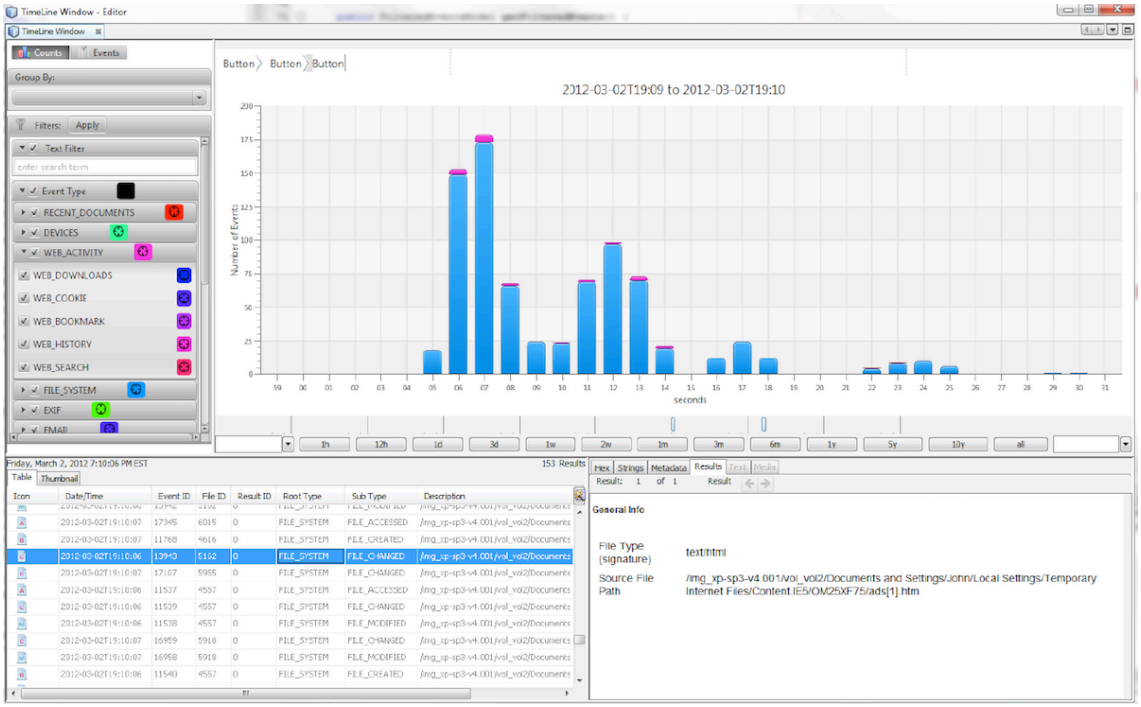
- Casos de explotación infantil donde estén involucrados cientos de miles de imágenes y vídeos para su revisión.
- Categorización y revisión de material explícito y no explícito.
- La búsqueda y filtrado de imágenes basándose en la información EXIF de la cámara como la marca y modelo, así como la información de geo localización.

Las características de este módulo son:

- Teclas de acceso para poder categorizar rápidamente.
- La agrupación y el filtrado basado en EXIF meta información, así como la ubicación en el disco.
- Fácil de usar y entender, interfaz optimizada para la revisión de grandes conjuntos de imágenes.
- Clara visualización para categorización de imágenes tanto en miniatura.
- Capacidad de clasificación que permite la revisión de las imágenes que se encuentran en los directorios de usuario de una manera fácil.

Módulo de Cronología Avanzada

Este módulo recoge información acerca de los eventos que ocurrieron en el sistema y permite visualizar la actividad. Los enfoques tradicionales de esto a menudo dan lugar a la sobrecarga de datos y hacen que sea difícil determinar qué es exactamente lo que pasó. Como parte de nuestro trabajo, hemos incorporado varias técnicas de visualización y zoom para evitar la sobrecarga y permiten al usuario centrarse en lo que es relevante.



Casos de uso

- Revisar rápidamente toda la actividad en una imagen de disco para identificar las fechas específicas de interés para la investigación.
- Identificar cuando la actividad web para sitios web específicos y servicios de comunicación en línea que pasó y la secuencia de la actividad.
- Encuentra puntos en el tiempo, donde grandes volúmenes de imágenes o documentos fueron copiados a un dispositivo.
- Identifica el plazo más probable de una intrusión basado en una anomalía registro, web, y la actividad del sistema de archivos.

Módulo de síntesis de texto multilingüe

Este módulo se utiliza cuando un investigador se encuentra con un documento en un idioma que no habla. El módulo de Autopsy identificará los nombres de personas, lugares y organizaciones y los traducirá al Inglés. También puede usar un diccionario suministrado por el usuario de palabras clave que puedan ser comparadas y destacadas.

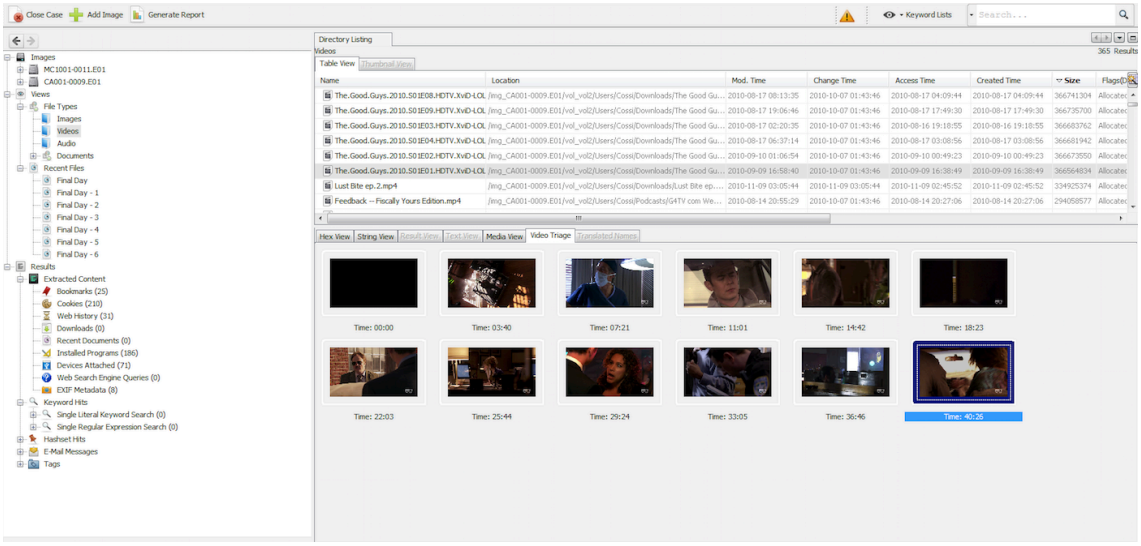
Esta es una prueba, se puede personalizar para sus necesidades de la misión.

Casos de uso:

- Permite búsquedas especificas en profundidad.
- Proporciona oportunidades para una amplia búsqueda de palabras clave, archivos o hash.
- Permite búsquedas de palabras clave ad-hoc basándose en nombres y conceptos que se mencionan por los sospechosos y testigos.

Módulo de clasificación de videos

El módulo de clasificación de videos v1.1, se integra directamente en la interfaz de usuario de Autopsy y divide un vídeo en fotogramas clave, mostrando las imágenes en miniatura. Proporciona grandes facilidades para analistas e investigadores ya que tiene una capacidad de clasificación muy eficiente.



Casos de uso:

- Identifica rápidamente archivos de video que esconde contenido que no se puede observar en los primeros minutos.
- Obtener la esencia de cualquier contenido de los archivos de video que se han encontrado en la investigación, sin necesidad de ver el contenido real de este.
- Determina la probabilidad de que algo interesante aparezca en un archivo de video en cuestión de segundos.

Características

- Produce un número estático de miniaturas a intervalos iguales de tiempos basándose en la longitud del vídeo, para un rápido resumen del contenido total de video.
- Uso de formatos de vídeo MOV, M4V, FLV, MP4, 3GP, AVI, MPG.
- Se integra directamente en la interfaz de usuario de Autopsy.

Módulo de aplicación de la Ley Bundle

La versión estándar de Autopsy tiene las características necesarias para llevar a cabo investigaciones de la explotación infantil. Este módulo hace que sean aún más fácil de realizar esas investigaciones, permitiendo al usuario aprovechar la información de las bases de datos C4All y Proyecto Vic.

Tanto este módulo como las bases de datos mencionadas, solo están disponibles para agentes y fuerzas de seguridad del estado.

Desarrollo personalizado de Autopsy.

El kit Sleuthkit y Autopsy son herramientas forenses digitales de código abierto, plataformas que en gran medida tienen marcos que fueron diseñados para permitir la creación de sistemas flexibles y extensibles. Las plataformas vienen con un conjunto estándar de módulos para cubrir la gama más amplia de casos de uso, como la investigación de un disco duro, pero fueron diseñados sabiendo que diferentes organizaciones tienen diferentes necesidades y flujos de trabajo. Estas plataformas nos permiten construir de manera eficiente, módulos que resulten una solución personalizada para la investigación de su equipo. Hay disponibles tres tipos generales:

Análisis de archivos: Estos módulos se centran en el contenido del archivo y los atributos. Módulos personalizados pueden extraer datos de los formatos de archivo menos comunes, aplicar técnicas de detección patentados, e interactuar con bases de datos de correlación.

Módulo de informes: Estos módulos organizan los resultados del análisis en un informe. Los módulos de informes personalizados pueden producir una salida en formatos que son requeridos por su organización.

Módulos de análisis de visualización gráfica: Estos módulos de análisis favorecen la visualización, para así mejorar la eficiencia de los exámenes. Módulos personalizados en esta categoría incluyen la visualización de la línea de tiempo de grandes cantidades de eventos y la clasificación de imágenes gráficas.