UNIVERSIDAD DE CASTILLA-LA MANCHA
ESCUELA SUPERIOR DE INFORMÁTICA

GRADO EN INGENIERÍA INFORMÁTICA

TRABAJO FIN DE GRADO

Metodología para el desarrollo de procedimientos periciales en el ámbito de la informática forense

Juan Miguel Tocados Cano

Julio, 2015

METODOLOGÍA PARA EL DESARROLLO DE PROCEDIMIENTOS PERICIALES EN EL ÁMBITO DE LA INFORMÁTICA FORENSE

UNIVERSIDAD DE CASTILLA-LA MANCHA

ESCUELA SUPERIOR DE INFORMÁTICA

Tecnologías y Sistemas de Información

TECNOLOGÍA ESPECÍFICA DE
TECNOLOGÍAS DE LA INFORMACIÓN

TRABAJO FIN DE GRADO

Metodología para el desarrollo de procedimientos periciales en el ámbito de la informática forense

Autor: Juan Miguel Tocados Cano

Director: María José Santofimia Romero

Director: Juan Carlos López López

Julio, 2015

Juan Miguel Tocados Cano

Ciudad Real – Spain

E-mail: JuanMiguel.Tocados1@alu.uclm.es

TRIBUNAL:

Presidente:

Vocal:

Secretario:

FECHA DE DEFENSA:

CALIFICACIÓN:

PRESIDENTE	VOCAL	SECRETARIO
Fdo.:	Fdo.:	Fdo.:

Resumen

La informática forense es una rama de la informática relativamente reciente que tiene como objetivo la investigación de hechos con relevancia jurídica en sistemas informáticos y que surgió en Estados Unidos en la década de los 80 cuando empezaron a ser reconocidos ciertos delitos informáticos, como el sabotaje de los propios sistemas. Desde entonces y con motivo del avance de la tecnología, el número de posibilidades para romper la ley ha aumentado, incrementando cada vez más la popularidad de esta disciplina.

Este Trabajo Fin de Grado tiene como objetivo el desarrollo de una metodología que abarque el proceso completo llevado a cabo durante un análisis forense, desde la obtención de las evidencias que serán sometidas a análisis, hasta su fin, plasmándose los resultados obtenidos en el correspondiente informe pericial.

Para lograr dicho objetivo se abordará el tema tanto desde una perspectiva jurídica y normativa, con la finalidad de aportar el informe como medio de prueba en un proceso judicial (con especial énfasis en el proceso penal), como desde el propio punto de vista informático, mostrando el proceso de adquisición y análisis de evidencias y la posterior documentación y presentación del informe.

Abstract

Computer forensics is a recent branch of computer science that focuses in the investigation of facts with legal relevance within computer systems. It was born in the United States in the 80's, when some computer crimes became recognised, like sabotage of systems. Since then, as result of the technology evolution, the number of possibilities for breaking the law has risen, increasing more and more the popularity of this discipline.

This Bachelor's Thesis is intended to develop a methodology encompassing the whole proccess carried out during a forensic analysis, from the acquisition of the evidences which will be submitted to analysis, to its end, writing down the results in a final report.

To achieve that objective, the issue will be addressed on the one hand from a normative and legal perspective, in order to deliver the report as an evidence in judicial proceedings (with special attention to criminal procedures), and on the other hand from an IT point of view, showing the evidence acquisition and analysis processes, and the subsequent documentation and reporting.

Agradecimientos

Estas líneas de agradecimiento significan que ha llegado el final de mi etapa universitaria. En primer lugar me gustaría agradecer a mi familia, principalmente a mis padres por proporcionarme apoyo emocional y económico durante todos estos años.

En segundo lugar me gustaría agradecer a Elena, que me ha dado el ánimo que me faltaba durante estos últimos meses. También quiero hacer mención a los amigos y compañeros que he hecho durante estos años, con los que todo se ha hecho algo más ameno y llevadero en ciertos momentos.

Finalmente agradezco a María José Santofimia por ofrecerse a dirigir este proyecto, tan distinto a lo que se suele ver normalmente en este tipo de estudios universitarios. Por tener el valor de confiar en un proyecto en el que ningún otro profesor confió y por su ayuda en el desarrollo del mismo. También a Juan Carlos López por contribuir a la mejora de la calidad de este documento con sus recomendaciones.

Juanmi

A Luis Cano Rodríguez

Índice general

Índice de cuadros

Índice de figuras

Listado de acrónimos

2TDEA	2 Key Double DES
3TDEA	3 Key Double DES
ADN	Ácido DesoxirriboNucleico
AENOR	Asociación Española de Normalización y Certificación
AES	Advance Encryption Algorithm
ANTPJI	Asociación Nacional de Tasadores y Peritos Judiciales Informáticos
BIOS	Basic Input/Output System
CAdES	CMS Advanced Electronic Signatures
CAINE	Computer Aided INvestigative Environment
CC	Código Civil
CE	Constitución Española
CFReDS	Computer Forensic Reference Data Sets
CLI	Command Line Interface
CMS	Cryptographic Message Syntax
CP	Código Penal
CSV	Comma-Separated Values
DART	Digital Advanced Response Toolkit
DCO	Device Configuration Overlay
DDR	Double Data Rate
DEFT	Digital Evidence & Forensic Toolkit
DFF	Digital Forensics Framework
DFRWS	Digital Forensics Research Workshop
DLL	Dynamic-Link Library
ELA	Error Level Analysis
ESI	Escuela Superior de Informática
Exif	Exchangeable Image File Format

EXT	Extented File System
FAT	File Allocation Table
GPS	Global Positioning System
GUI	Graphical User Interface
HFS	Hierarchical File System
HPA	Host Protected Area
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
IDE	Integrated Device Electronics
IDIP	Integrated Digital Investigation Process
IJCSIT	International Journal of Computer Science and Information Technology
INCIBE	Instituto Nacional de Ciberseguridad
IP	Internet Protocol
JSON	JavaScript Object Notation
LEC	Ley de Enjuiciamiento Civil
LECRIM	Ley de Enjuiciamiento Criminal
LXDE	Lightweight X11 Desktop Environment
MAC	Media Access Control
MD5	Message-Digest Algorithm 5
MFT	Master File Table
MIME	Multipurpose Internet Mail Extensions
NFAT	Network Forensic Analysis Tool
NIST	National Institute of Standards and Technology
NSRL	National Software Reference Library
NTFS	New Technology File System
PADES	PDF Advanced Electronic Signatures
PATA	Parallel Advanced Technology Attachment
PDA	Personal Digital Assistant
PHVA	Planificar, Hacer, Verificar, Actuar
PIN	Personal Identification Number
PUK	Personal Unlocking Key
RAE	Real Academia Española

RAID	Redundant Array of Independent Disks
RAM	Random-Access Memory
RDS	Reference Data Set
SAS	Serial Attached SCSI
SATA	Serial Advanced Technology Attachment
SGEE	Sistema de Gestión de Evidencias Electrónicas
SGSI	Sistema de Gestión de la Seguridad de la Información
SHA-1	Secure Hash Algorithm 1
SIM	Subscriber Identity Module
S.M.A.R.T.	Self Monitoring Analysis and Reporting Technology
SMS	Short Message Service
SO	Sistema Operativo
SSD	Solid-State Drive
SSL	Secure Sockets Layer
TFG	Trabajo Fin de Grado
TSK	The Sleuth Kit
UCLM	Universidad de Castilla-La Mancha
UE	Unión Europea
UFS	Unix File System
UNE	Una Norma Española
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTM	Universal Transverse Mercator
VoIP	Voice over Internet Protocol
XAdES	XML Advanced Electronic Signatures
XML	eXtensible Markup Language
YAFFS2	Yet Another Flash File System

Capítulo 1

Introducción

Se podría decir que la informática forense tuvo su origen en Florida (EEUU), en el año 1978, cuando comenzaron a ser reconocidos ciertos delitos informáticos relacionados con copyright, el sabotaje de sistemas informáticos, etc. A raíz de esto, en la década de los 80 empezaron a surgir herramientas forenses como Copy II Central Point Software o UnErase: Norton Utilities, mediante las cuales se podían realizar copias de disquetes o recuperar archivos borrados, respectivamente. Durante estos años también se crearon diversas asociaciones con el fin de recoger conocimiento y formar a profesionales del ámbito forense.

Más tarde, en los 90, se acuñó el término *«computer forensics»* en el libro de *Collier* y *Spaul*: *«A Forensic Methodology for Countering Computer Crime»*[CS92].

Después de esto, se siguieron creando diversas organizaciones y grupos de debate relacionados con el mundo forense [Ram11], hasta que en pleno siglo XXI, la informática forense ha tomado un papel mucho más importante, debido a que el espectro de delitos que involucran alguna componente tecnológica es cada vez mayor. En este sentido, la tecnología ofrece actualmente a los criminales una gran variedad de nuevas opciones para romper la ley, a causa de sus avances [Sep13].

Dentro de los distintos aspectos que la informática forense aborda, este Trabajo Fin de Grado (TFG) presta atención al proceso de elaboración de informes forenses o periciales, además de conocer la normativa y legislación aplicable durante todo el proceso hasta que estos finalizan y el conocimiento y uso de las herramientas apropiadas que den soporte a la obtención de los datos necesarios cuyo posterior análisis dará lugar a los resultados que se plasmarán en dichos informes.

La elaboración de un informe forense o pericial es un proceso en el que la fase previa de recogida de información es esencial para el buen desarrollo del mismo. Ante el proceso de recogida de evidencias y del posterior análisis se suelen seguir una serie de procedimientos, que en el caso de España son algo imprecisos. Por ejemplo: si se siguiera estrictamente el **RFC 3227: *«Guía para la recogida y almacenamiento de evidencias»*** [BK02], podría darse el caso en el que un error cometido durante esta etapa podría ocasionar que las evidencias dejaran de ser válidas frente a un proceso judicial. El motivo sería la violación del principio «antes de tocar cualquier evidencia, prevalece la rigurosa recogida de la misma», ya que se

estaría modificando el escenario y prima el hecho de acreditar que las evidencias no hayan sido alteradas.

Entonces, si no se debe tocar el escenario y debido precisamente a la falta de regulaciones en cuanto a procedimientos forenses informáticos, lo más recomendable es seguir una serie de buenas prácticas extendidas en este campo, como documentar gráficamente mediante fotografías el escenario, por ejemplo. En cualquier caso, esto deja patente la falta de regulación y los problemas derivados de la misma.

Por lo tanto, el hecho de que no exista un único procedimiento que sistematice el proceso de elaboración de informes periciales pone en riesgo la validez de dicha tarea. Este TFG tratará de esclarecer ciertos aspectos que servirán para facilitar el proceso de elaboración y redacción de informes periciales que puedan ser utilizados en posteriores procesos judiciales, a saber: identificar el escenario que se presenta, determinar las evidencias a analizar y cómo preservarlas, al igual que identificar el tiempo disponible para la adquisición, también el proceso de análisis de las mismas.

El resultado de este proyecto será un manual de procedimientos que servirá de guía para la elaboración y redacción de informes periciales, conforme a la normativa y legislación vigente tanto a nivel nacional como en cuanto a directivas y recomendaciones de la Unión Europea. Aunque el uso de informes forenses o periciales no está limitado al ámbito de los procedimientos judiciales, es en esta esfera donde tienen un mayor impacto, especialmente cuando se trata de procedimientos penales. Generalmente este tipo de procedimientos suelen llevar aparejadas penas que interfieren en el ejercicio de los derechos fundamentales de las personas, como es el de libertad. Por lo tanto, las garantías aparejadas a este tipo de procedimientos, en cuanto a lo que se refiere a la fase probatoria, son mucho mayores que en otros procedimientos como pudieran ser los civiles o laborales. El perito tecnológico suele carecer de estos conocimientos jurídicos lo que podría llevarle a incurrir en graves errores que terminaran invalidando las pruebas e incluso el proceso. Este TFG revisa todas aquellas cuestiones, relevantes desde el punto de vista del proceso penal, que un perito judicial deberá tener en cuenta tanto durante la recogida de evidencias como durante la elaboración y defensa de su informe. En este sentido será necesario establecer una equiparación entre los procedimientos establecidos para la gestión de la evidencia física en contraste con las evidencias digitales que serán el principal elemento de trabajo de los peritos judiciales informáticos. Este proceso no es siempre sencillo pero de vital importancia por cuanto las mismas garantías que aplican a la evidencia física deben asegurarse para la evidencia digital.

Este trabajo también incluirá un análisis de las herramientas que pueden ser de utilidad durante todo el proceso que precede a la redacción del informe.

1.1 Estructura del documento

Capítulo 2: Objetivos

En este capítulo se describirá tanto el objetivo principal como los objetivos específicos planteados para este proyecto.

Capítulo 3: Objectives

Versión traducida al inglés del capítulo anterior.

Capítulo 4: Estado del arte de herramientas hardware y software para análisis forense

En este capítulo se hará por una parte un estudio genérico de ciertas herramientas disponibles actualmente para la realización de un análisis forense informático, tanto distribuciones orientadas a este fin como herramientas software y hardware. se mostrarán las fases de las que consta una investigación forense, describiendo una serie de modelos que pueden servir de guía.

Capítulo 5: Estado del arte de metodologías para la investigación forense

En este capítulo se mostrarán las fases de las que consta una investigación forense, describiendo una serie de modelos que pueden servir de guía.

Capítulo 6: El procedimiento probatorio en el proceso penal

En este capítulo se hablará sobre el procedimiento probatorio en el proceso penal español, exponiendo una serie de conceptos para mejor comprensión del capítulo.

También se hablará del tema, de la carga y de la valoración de la prueba, del propio procedimiento probatorio y de los medios de prueba existentes.

Capítulo 7: La evidencia digital

En este capítulo se hablará de aspectos relacionados con la evidencia digital, como el proceso de recogida de la misma y la documentación de dicho proceso y se establecerán ciertas analogías entre la evidencia física y la digital.

También se hablará de la cadena de custodia y de su importancia en el proceso penal español.

Capítulo 8: Extracción de evidencias digitales: casos de uso

En este capítulo se mostrará el proceso de extracción de ciertas evidencias electrónicas mediante la utilización de algunas de las herramientas descritas anteriormente.

Capítulo 9: Metodología propuesta

En este capítulo se mostrará la metodología propuesta durante este TFG, con el objetivo de abordar un análisis forense y la posterior elaboración del informe pericial.

Capítulo 10: Análisis forense de un caso ficticio

En este capítulo se realizará un análisis forense de un caso ficticio, pasando por todas las etapas y siguiendo la metodología propuesta en este trabajo.

Capítulo 11: Conclusiones

En este capítulo se enunciarán las conclusiones a las que se ha llegado, para concluir el proyecto.

Capítulo 12: Conclusions

Versión traducida al inglés del capítulo anterior.

Capítulo 2

Objetivos

ESTE capítulo planteará una serie de objetivos a cumplir durante la realización de este proyecto, tanto de manera general como de manera específica. Cuando el trabajo concluya, en el Capítulo 11 se analizará la manera en la que han sido abordados así como el grado de completitud de cada uno de ellos.

2.1 Objetivo general

Este TFG tendrá como objetivo principal la propuesta de un manual de procedimientos para la elaboración de informes periciales, que sea lo suficientemente genérico para abordar la gran variedad de dispositivos y tecnologías existentes que pueden ser sometidos a análisis. Se pretende así que este proyecto pueda llegar a ser una referencia, tanto para estudiantes o graduados en ingeniería informática como para personas que se decanten más por el mundo del derecho, aunando la parte técnica y la jurídica.

2.2 Objetivos específicos

Podríamos desglosar el objetivo general propuesto en la sección anterior en una serie de objetivos específicos con el fin de alcanzar dicho objetivo.

2.2.1 Estudio de la situación actual

En primer lugar será necesario identificar las características exigidas a cualquier herramienta software o hardware que pueda ser utilizada en un procedimiento de recogida y análisis de evidencias. Generalmente el uso de una única herramienta no bastará para llevar a cabo dicho proceso, sin embargo, dependiendo de las circunstancias de cada caso unas serán más apropiadas que otras. En este sentido, será necesario dar a conocer los medios de análisis disponibles actualmente, desplegados en varias categorías, principalmente software y hardware.

Se mostrará también la variedad disponible de modelos de investigación que servirán de guía para la propuesta metodológica que posteriormente se realizará en este TFG.

2.2.2 Elaboración de manuales de herramientas

El gran número de herramientas disponibles y su disparidad de uso puede ser considerada una barrera de entrada. Para facilitar este proceso, será necesario analizar cuáles, de entre el amplio abanico de herramientas disponibles son las más utilizadas en este tipo de procesos y redactar para ellas casos de uso que se muestren el proceso de extracción de evidencias y el uso básico de éstas.

2.2.3 Análisis comparativo de las distintas metodologías existentes para el análisis forense

La falta de un procedimiento concreto y unificado que describa las distintas fases por las que debe transcurrir un análisis forense contrasta con la existencia de distintas propuestas no sólo a nivel teórico sino también a nivel normativo. El objetivo será elaborar una metodología lo más completa posible que abarque todos los aspectos que de una u otra manera hayan sido identificados por las distintas propuestas existentes en el estado del arte. Esta metodología será la aportación principal de este TFG.

2.2.4 Aplicación de procedimientos adecuados y legislación vigente

Como la intención al redactar el informe pericial es que sea capaz de sostenerse como medio de prueba en un proceso legal, será necesario recoger en el presente documento toda la legislación vigente y aplicable para afrontar todo el proceso desde la recogida de las evidencias hasta la presentación del informe pericial con una serie de garantías.

2.2.5 Consideraciones jurídicas del informe pericial

A pesar de que el ámbito de los informes periciales no está estrictamente limitado al ámbito jurídico, sí es cierto que éste es el más relevante, especialmente si se trata de un procedimiento penal.

Durante la propuesta de una metodología unificada para el análisis forense y elaboración de informes periciales se habrán establecido las pautas que garanticen un proceso compatible con la legislación procesal vigente. Sin embargo, el rol técnico del perito no puede aislarse completamente del entorno jurídico en el que éste desarrollará su actividad. Por lo tanto, será necesario hacer una recopilación de todas aquellas cuestiones jurídicas que el perito deberá tener presente durante todo su trabajo, recordando que éste no finaliza con la elaboración del informe pericial, sino que puede ser llamado a su defensa.

La falta de conocimientos jurídicos del personal técnico hace necesario que este objetivo deba ser abordado de la manera más clara y concisa posible, limitándose a aquéllas cuestiones que afecten directamente al trabajo del perito judicial.

2.2.6 Construcción de un escenario de análisis

Una vez abordado el objetivo de propuesta de una metodología para el análisis forense será necesario llevar a cabo una validación de la misma. El proceso de validación consistirá en la construcción de un escenario de análisis que simule un caso forense ficticio, de forma que se aglutinen todos los conocimientos adquiridos. Se pretende que el escenario contenga distintos tipos de análisis, de manera que haya que aplicar distintas técnicas.

A la misma vez, se respetará la parte normativa, escogiendo un modelo a seguir y una serie de normas a aplicar que asegurarán la sostenibilidad del informe resultante como medio de prueba en juicio.

Capítulo 3

Objectives

THIS chapter will suggest a series of objectives to meet during the realization of this project, both generally and specifically. When the work ends, the way the objectives have been addressed will be analyzed in chapter 11, as well as the degree of completeness of each one.

3.1 General objective

This Bachelor's Thesis will have as main objective the proposal of a manual of procedures for developing expert reports, generic enough to address the existence of a great variety of devices and technologies that can be submitted to analysis. It's intended so that this project can become a reference, both for computer science students or graduates and people who prefer better the world of law, joining the technical and legal parts.

3.2 Specific objectives

We could itemize the general objective proposed in the previous section into a series of specific objectives in order to achieve that objective.

3.2.1 Study of the current situation

In first place, it will be necessary to identify the required features of every software or hardware tool that can be used in the evidence collection and analysis procedure. Generally, the use of a single tool won't be enough to carry out that process, however, depending on the circumstances of each case, some will be more appropriate than other. In this sense, it will be necessary to introduce the currently available analysis means, deployed in several categories, mainly software and hardware.

The available variety in terms of available investigation models will be also shown, so each person will be free to choose the one who prefers.

3.2.2 Tool manual development

The large number of available tools and their disparity of use can be considered a difficulty to deal with in the beginning. To make this process easier, it will be necessary to analyze

which ones, among the wide range of available tools will be more used in these type of processes and to write for them some uses cases that show the evidence extraction process and the basic use of these.

3.2.3 Comparative analysis of different existing methodologies for computer forensics

The lack of a specific and standardized procedure that describes the different phases a forensic analysis has to go through contrast with the existence of different proposals not only in a theoretical level but also a normative level. The objective will be to develop a methodology as complete as possible covering all the aspects that one way or another have been identified by the different existing proposals in the state of the art. This methodology will be the main contribution of this Bachelor's Thesis.

3.2.4 Application of proper procedures and applicable legislation

Since the intention writing the expert report is to be able to be presented as evidence in legal proceedings, it will be necessary to gather in this document all the applicable legislation to deal with the whole process from the evidence collection to the presentation of the expert report with certain guarantees.

3.2.5 Legal considerations of the expert report

Although the scope of the expert reports is not strictly limited to legal field, it's true that this is the most relevant, specially if it's a criminal procedure.

During the proposal of a unified methodology for the forensic analysis and the construction of expert reports, the guidelines that guarantee a process compatible with the applicable legislation will have been established. However, the expert's technical role can't be isolated completely from the legal environment in which he performs his activity. Thus, it will be necessary to make a compilation of all those legal issues the expert should have present throughout his work, having into consideration that the work doesn't end with the writing of the expert report, but he can be called to its defense.

The lack of legal knowledge of the technical staff makes necessary this objective to be addressed as clearly and concisely as possible, being restricted to those questions that affect directly to the work of the judicial expert.

3.2.6 Construction of an analysis scenario

Once the objective of proposing a methodology for the forensic analysis has been addressed, it will be necessary to carry out a validation of the same. The validation process will consist in the construction of an analysis scenario simulating a fictional forensic case, in order to bind together all the acquired knowledge. The scenario is pretended to contain several types of analysis, in this way, different techniques will have to be applied.

At the same time, the normative part will be respected, choosing a model to follow and a series of applying standards which will assure the sustainability of the resulting report as evidence in a trial.

Capítulo 4

Estado del arte de herramientas hardware y software para análisis forense

ESTE capítulo realizará un estudio genérico de las herramientas, tanto hardware como software, de las que se hacen uso durante la realización de un análisis forense informático. Se seguirá una estructura que a grandes rasgos va a consistir en tres grandes partes: distribuciones orientadas al análisis forense informático, herramientas software y finalmente herramientas hardware. Más concretamente, la parte de herramientas software va a estar dividida a su vez en: suites de utilidades forenses, propósito general, análisis de correo electrónico, captura de datos, análisis de archivos y datos, dispositivos móviles, análisis de Internet y análisis del registro. Por su parte, la sección de herramientas hardware quedará dividida en: análisis de dispositivos móviles, hardware forense y equipos forenses.

4.1 Distribuciones orientadas al análisis forense informático

Entre las múltiples distribuciones GNU/Linux existentes, una parte de ellas cuentan con un gran catálogo de programas preinstalados y/o características incorporadas que las hacen aptas para su uso dentro del análisis forense.

La necesidad de este tipo de distribuciones no es otra que facilitar al investigador toda la tarea que conlleva una investigación forense, empezando por recopilar múltiples herramientas útiles para dicho fin. Así, se elimina al usuario la tediosa tarea de realizar su propia selección de herramientas y el posterior creado de un entorno de trabajo mediante por ejemplo un *live cd*. Aparte de lo anterior, todas estas distribuciones tienen una característica en común: no se monta ningún dispositivo interno o externo hasta que no es realmente necesario, y solo entonces se monta con permisos de solo lectura, evitando así la modificación accidental de cualquier dato contenido en dicho dispositivo, dando lugar a la posible invalidación de las pruebas que pudieran extraerse durante su análisis.

Por el mismo motivo, tampoco se realiza el montaje automático de la partición swap, o espacio de intercambio, que consiste en un mecanismo de memoria virtual que permite simular que se dispone de más memoria de la que realmente se tiene, aliviando y liberando así a la memoria principal de la carga de procesos. De esta forma, no montando el área de intercambio de forma automática desde el inicio del sistema, se elimina de igual manera la posibilidad de modificar accidentalmente los datos. Además, podrá recuperarse información

para la extracción de posibles evidencias.

4.1.1 DEFT Linux

La distribución **DEFT (Digital Evidence & Forensic Toolkit)**[1] [FRD], basada en **Lubuntu** y cuya primera versión data de 2005, es actualmente mantenida y desarrollada por **Stefano Fratepietro**, con el apoyo de Alessandro Rossetti, Massimiliano Dal Cero, Paolo Dal Checco, Valerio Leomporra, Davide Gabrini, Marco Giorgi y Nicodemo Gawronski.

Además de contar con gran cantidad de aplicaciones y scripts, también incluye la suite de aplicaciones DART (Digital Advanced Response Toolkit), destinada a sistemas operativos Windows.

Cuenta con una serie de características destinadas a asegurar algo tan importante como la integridad de las posibles evidencias sometidas a análisis. Dichas características son:

1. En el arranque, el sistema no hace uso de las particiones swap
2. Durante el arranque del sistema, no hay scripts de montaje automáticos
3. No hay sistemas automatizados para ninguna actividad durante el análisis de la evidencia
4. Todas las herramientas de adquisición de almacenamiento masivo y de tráfico de red no alteran los datos que estuvieran siendo adquiridos

DEFT puede ser utilizado desde sistemas que dispongan de lector de CD/DVD-ROM o puerto USB, con arquitectura x86 y un mínimo de 64 MB de memoria RAM si se quiere arrancar en modo texto o 128 MB si se opta arrancar con la interfaz gráfica de usuario (GUI), en cuyo caso el entorno de escritorio Lightweight X11 Desktop Environment (LXDE)[2] será el utilizado.

Algunas de las herramientas más importantes incorporadas dentro de esta distribución son:

- Explorador de archivos con estado de montaje de disco
- Soporte a discos encriptados con Bitlocker
- The Sleuth Kit
- Digital Forensics Framework
- JD-GUI
- Skype Xtractor
- Maltego

[1] http://www.deftlinux.net/
[2] http://lxde.org/

El listado completo de herramientas y paquetes disponible se puede consultar en la sección *«Package list»*[3] de la propia página web.

Como ya se dijo previamente, el sistema no llevará a cabo ninguna acción a excepción de la detección de los dispositivos que se encuentran conectados al mismo. Si se quiere montar cualquier dispositivo de almacenamiento, con un simple click derecho sobre el dispositivo a montar serán presentadas tres opciones:

- **Mount Read Only:** el dispositivo será montado con permiso de solo lectura, sin alterar los datos almacenados
- **Mount Volume:** el dispositivo será montado con permisos de lectura y escritura
- **Eject Removable Media:** permite la extracción del dispositivo de forma segura

No obstante, el usuario podrá definir sus propias políticas de montaje con la herramienta *MountManager*, que puede encontrar en la sección *DEFT* del menú de aplicaciones.

También se habló anteriormente sobre la suite DART, que organiza y ejecuta una serie de aplicaciones para Windows, pudiendo el usuario elegir cuáles de estas estarán en la lista de programas a ejecutar simplemente modificando el archivo *dart.xml*. Dichas aplicaciones se ejecutarán en modo seguro y podrán ser utilizadas durante un *«live analysis»*, es decir, cuando el equipo a analizar se encuentra encendido.

Al ejecutar las aplicaciones en modo seguro, se llevará a cabo una comprobación de integridad antes de ejecutar cada programa, de este modo quedará asegurado que no han sido modificados.

Para finalizar, es necesario añadir que DART deberá ser ejecutado con privilegios de administrador y advertir de que algunos programas podrán ser detectados por el firewall o el antivirus del sistema como malware, por lo que éstos deberán ser desactivados.

4.1.2 CAINE

CAINE (Computer Aided INvestigative Environment)[4] es, al igual que DEFT, una distribución GNU/Linux proveniente de Italia y creada inicialmente como un proyecto de informática forense por Giancarlo Giustini, siendo mantenida desde 2009 hasta la actualidad por **Nanni Bassetti**. En este caso, CAINE está basada en Ubuntu y cuenta con el entorno de escritorio MATE[5].

Los principales objetivos que esta distribución consisten en crear un ambiente interoperable de forma que se apoye al investigador durante las fases de la investigación y ofrecer tanto una GUI como unas herramientas que sean intuitivas y fáciles de usar *(user-friendly)*.

[3] http://www.deftlinux.net/package-list/
[4] http://www.caine-live.net/
[5] http://mate-desktop.org/

Una lista de herramientas y paquetes incluidos en CAINE puede ser consultada en la correspondiente sección de su página web[6].

También se incluye esta vez una herramienta destinada al análisis en vivo de sistemas Windows llamada Win-UFO[7] (Windows-Ultimate Forensic Outflow), proporcionando un gran conjunto de herramientas útiles separadas en varias categorías.

Para asegurar el montaje seguro de dispositivos, se han incluido dos utilidades:

- **rbfstab:** se activa automáticamente durante el arranque del sistema o al conectar un dispositivo, de modo que escribe entradas en el archivo `/etc/fstab` para que los dispositivos sean montados de forma segura en modo de solo lectura
- **mounter:** es una herramienta de montaje con GUI situada en la barra de tareas, desde la cual se podrán seleccionar los dispositivos que se deseen. También permite cambiar la política de montaje con click derecho del ratón sobre el icono del programa

Desde el propio explorador de archivos se puede acceder a gran cantidad de scripts incluidos, mediante click derecho del ratón, permitiendo obtener información relacionada con historiales de Internet, archivos eliminados, metadatos EXIF, etc. Estos scripts también proporcionan acceso a funciones administrativas, como por ejemplo hacer que un dispositivo conectado sea escribible o abrir una ventana del explorador de archivos con privilegios de administrador. Con el script *«Save as Evidence»* se podrán guardar los archivos seleccionados en una carpeta del escritorio y crear un informe de texto sobre el archivo que contendrá los metadatos de los archivos y, si se desea, un comentario del investigador.

La política de montaje de CAINE se puede resumir como: no montar nunca ningún dispositivo, interno o externo, y cuando el usuario pinche con el ratón sobre el icono del dispositivo, el sistema lo montará con permiso de solo lectura.

4.1.3 Kali Linux

Esta distribución[8], aunque está orientada principalmente a seguridad informática y a auditorías de seguridad, cuenta también con una serie de herramientas forenses que la hace compatible con nuestros objetivos.

Kali está basada en Debian y es sucesora de BackTrack Linux[9]. Cuenta con más de 300 herramientas y da soporte a gran cantidad de dispositivos wireless. Su versión inicial fue lanzada en 2013.

Al contrario que en la mayoría de distribuciones, en Kali el usuario por defecto es **root** (superusuario), por tanto, no es recomendable para principiantes en GNU/Linux, pues se podrían cometer errores destructivos para el sistema.

[6] http://www.caine-live.net/page11/page11.html
[7] http://win-ufo.org/
[8] http://www.kali.org/
[9] http://www.backtrack-linux.org/

Algunas de las herramientas forenses incluidas son las siguientes:

- Bulk extractor
- dd, dc3dd, ddrescue
- Foremost
- Volatility
- Xplico
- RegRipper
- Guymager

El listado completo de herramientas se puede ver en la correspondiente sección de su página web[10].

Dentro de las posibilidades forenses, esta distribución cuenta con el **modo de arranque forense**, esto significa que hay un par de cambios importantes:

- El disco duro interno no se toca, es decir, que si hubiera una partición swap no sería usada y ningún disco interno será montado automáticamente
- Se ha deshabilitado el montaje automático de cualquier dispositivo extraíble

4.1.4 Otras distribuciones

Existen más distribuciones relacionadas u orientadas a la informática forense. A continuación se citarán algunas y se invitará al lector a dirigirse a sus respectivas páginas web si desea conocer más información sobre cada una de ellas:

- BackBox Linux (http://www.backbox.org/)
- Matriux (http://www.matriux.com/)
- BlackArch Linux (http://blackarch.org/)

Estos son simplemente unos pocos ejemplos de la multitud de distribuciones existentes. Si se desea realizar una búsqueda en profundidad, se recomienda visitar la web de DistroWatch[11].

4.1.5 Cuadro comparativo

Se muestra a continuación el cuadro comparativo de las distribuciones anteriormente descritas (ver cuadro 4.1).

[10] http://tools.kali.org/tools-listing
[11] http://distrowatch.com/

Distribución	Entorno de escritorio	Última versión	Distribución base	Formato de paquetes
DEFT Linux	LXDE	8.2	Lubuntu	deb
CAINE	MATE	6.0	Ubuntu	deb
Kali Linux	GNOME	1.0.9a	Debian	deb
BackBox Linux	Xfce	4.0	Ubuntu	deb
Matriux	GNOME	3 RC1	Debian	deb
BlackArch Linux	–	2014.10.07	Independiente	.pkg.tar.xz

Cuadro 4.1: Cuadro comparativo de distribuciones GNU/Linux

4.2 Herramientas software

Se darán a conocer en esta sección una serie de herramientas software, distribuidas en varias categorías, algunas de las cuales vienen incluidas en las distribuciones de las que se habló en la sección 4.1. La mayoría de las herramientas aquí descritas han sido escogidas de la página *Forensic Control*[12].

Como se dijo anteriormente, las distribuciones forenses contienen una serie de herramientas software con el objetivo de ayudar al investigador. En base a ello, diversos desarrolladores crearon herramientas que automatizaran ciertas tareas comunes en el proceso de análisis forense, como por ejemplo la captura y el análisis de datos, análisis de internet, etc.

4.2.1 Suites de utilidades forenses

Se dan aquí a conocer diversas suites forenses destinadas al análisis de datos.

The Sleuth Kit (TSK)

The Sleuth Kit (TSK)[13] es una colección de herramientas *open source* en línea de comandos disponible para entornos Windows y Unix, desarrollada por Brian Carrier [Car05a], liberada a principios del año 2001 y basada a su vez en *The Coroner's Toolkit (TCT)*. Actualmente la última versión disponible es la 4.1.3 (2014).

El objetivo de esta colección consiste en proporcionar al usuario una serie de herramientas destinadas al análisis forense de los sistemas de archivos y de volúmenes. De esta manera, TSK permite analizar distintos tipos de sistemas de archivo, como son NTFS, FAT, UFS1 y 2, EXT2, 3 y 4, HFS, ISO9660 y YAFFS2, independientemente de la plataforma en la que trabajemos [Gru08].

Según la utilidad que ofrezcan, las herramientas pertenecerán a diversas categorías, que Carrier denomina *«layers»*. La organización es la siguiente:

[12] https://forensiccontrol.com/resources/free-software/
[13] http://www.sleuthkit.org/

- **Media management layer:** mmls, mmcat, mmstat
- **File system layer:** fsstat
- **File name layer:** ffind, fls
- **Meta data layer:** icat, ifind, ils, istat
- **Data unit layer:** blkcalc, blkcat, blkls, blkstat
- **Herramientas de journal:** jcat, jls
- **Herramientas de disco:** disk_stat, disk_reset
- **Herramientas de archivos de imagen:** img_stat, img_cat
- **Otras herramientas:** hfind, sigfind, mactime, sorter

Para una información más detallada sobre TSK y cada una de sus herramientas, se puede consultar la propia página web y su correspondiente wiki[14].

Autopsy

Esta herramienta proporciona una GUI a TSK y fue, al igual que ésta, lanzada en 2001 y cuya versión más reciente es la 3.1.1 (2014). La versión 3 y posteriores pueden usarse desde entornos Windows, sin embargo, tendrá que usarse la versión 2 si se quiere utilizar desde entornos Unix.

Autopsy[15] pretende ser una herramienta de fácil uso e intuitiva, de forma que también pueda ser utilizada por usuarios con menos conocimientos técnicos que un investigador con cierta experiencia. Es por esto que cuenta con una serie de asistentes que guiarán a través de las diversas tareas.

Recién instalado cuenta con diversos módulos que proporcionan una serie de funcionalidades:

- **Análisis de *timelines*:** interfaz gráfica de visualización de eventos junto al instante de tiempo en que ocurrieron
- **Filtrado *hash*:** marca los archivos conocidos como maliciosos e ignora los conocidos como buenos
- **Análisis forense del sistema de archivos:** recupera archivos desde los formatos más comunes
- **Búsqueda de palabras clave:** realiza una búsqueda indexada de palabras clave, encontrando archivos que contengan dichas palabras
- **Artefactos web:** extrae el historial, los marcadores y las cookies de los navegadores más conocidos, para identificar la actividad del usuario

[14] http://wiki.sleuthkit.org/
[15] http://www.sleuthkit.org/autopsy/index.php

- **Multimedia:** extrae metadatos EXIF de imágenes y visualiza tanto vídeos como imágenes sin necesidad de visores externos

Existe también la posibilidad de añadir módulos de terceros[16], con objetivo de extender el número de funcionalidades.

Aparte de las mencionadas anteriormente, Autopsy cuenta con otras funcionalidades como pueden ser: análisis de registro, análisis de email, clasificación de archivos por tipo o extracción de cadenas unicode desde espacio no asignado o tipos de archivo desconocidos, al igual que dispone de posibilidades de creación de informes.

Volatility Framework

Consiste en una herramienta implementada en Python destinada a la extracción de artefactos digitales de imágenes de la memoria RAM, con multitud de plugins incluidos que brindan la funcionalidad a Volatility[17][18]. Fue lanzado en 2007 y su versión más reciente es la 2.4.

Soporta los volcados de memoria de la mayoría de versiones Windows de 32 y 64 bits y de Linux con kernels desde su versión 2.6.11, hasta la 3.16 y también volcados de memoria perteneciente a Mac OSX hasta su versión 10.9.4.

Se debe destacar que Volatility solo permite el análisis de la memoria, para realizar la adquisición de la memoria RAM se tendrá que recurrir a otras herramientas.

Digital Forensics Framework (DFF)

Digital Forensics Framework (DFF)[19] es una herramienta escrita en Python y C++ con un entorno modular, es decir, que ofrece una serie de módulos que ofrecen las distintas funcionalidades disponibles, por ejemplo: extraer y analizar datos provenientes de adquisiciones de discos duros o de RAM, recuperar archivos eliminados, etc. Funciona en entornos Windows y GNU/Linux y su versión más reciente es la 1.3.0.

Esta herramienta puede ser usada tanto por profesionales como por personas que no sean expertas dentro de la informática forense, de forma que podrán recrear los principales pasos de una investigación digital sin comprometer la integridad de los datos.

Algunas de sus características son:

- Preservar la cadena de custodia
- Acceso a dispositivos locales y remotos
- Reconstrucción de discos de máquinas virtuales (*virtual machine disks*)
- Análisis forense de sistemas Windows y Linux

[16] http://wiki.sleuthkit.org/index.php?title=Autopsy_3rd_Party_Modules
[17] http://www.volatilityfoundation.org/
[18] https://github.com/volatilityfoundation/volatility/
[19] http://www.digital-forensic.org/

- Recuperación de artefactos eliminados u ocultos
- Análisis forense de memoria RAM

4.2.2 Propósito general

En este espacio se mostrarán herramientas sin un propósito específico común.

NIST CFReDS

El proyecto Computer Forensic Reference Data Sets (CFREDS)[20] del NIST consiste en un conjunto de *data sets* o conjuntos de datos que forman un grupo de evidencias digitales simuladas, con objetivo de someterlas a investigación.

Los contenidos están documentados, por lo cual, el investigador podrá comparar sus resultados con los verdaderos resultados a obtener. De esta forma, CFREDS puede ser usado con varios propósitos, como el testeo de herramientas forenses, la comprobación de que un equipo funciona bien, pruebas de aptitud en habilidades específicas y el entrenamiento de personal.

Los diferentes *data sets* tienen diferentes enfoques, entre ellos podemos encontrar:

- Búsqueda de cadenas
- Búsqueda de imágenes y trazas de red
- Análisis de una captura de memoria
- File carving

NIST NSRL

El Reference Data Set (RDS) de la National Software Reference Library (NSRL)[21] contiene metadatos de archivos. Para cada archivo se incluyen los siguientes datos sobre él:

- Valores *hash* (MD5 y SHA-1) del contenido del archivo
- Datos sobre el origen del archivo, como el fabricante
- Otros datos sobre el archivo, como el nombre original y el tamaño

Para conocer más sobre el formato de los datos incluidos en el RDS, se podrá consultar el documento disponible en la página web del NSRL[22] [NIS].

Los datos contenidos en este herramienta se usan para identificar archivos en los sistemas a examinar. Típicamente se usa para eliminar archivos conocidos, como por ejemplo archivos del SO, reduciendo el número de archivos a examinar de forma manual.

[20] http://www.cfreds.nist.gov/
[21] http://www.nsrl.nist.gov/
[22] http://www.nsrl.nist.gov/Documents/Data-Formats-of-the-NSRL-Reference-Data-Set-16.pdf

Hay que destacar que esta herramienta solo contiene datos acerca de archivos «conocidos», por tanto, no podemos determinar si son dañinos o no. Para ello se deberá tener en cuenta el contexto de la investigación.

Firmas de archivo

Los archivos contienen en su cabecera una «firma», o número hexadecimal que caracteriza a los tipos de archivo. De esta forma, se pueden utilizar estas firmas para identificar o verificar el contenido de un archivo.

En la página de *File Signatures*[23] se pueden hacer búsquedas por firma o por extensión de archivo, disponiendo de gran cantidad de resultados que podrán ser útiles en una investigación.

Algunas firmas para distintos tipos de archivo son, por ejemplo:

- JPEG: `FF D8 FF E0 / FF D8 FF E1 / FF D8 FF FE`
- RAR: `52 61 72 21`
- TAR: `1F 8B 08 00`

HexBrowser

Relacionada con las firmas de archivo, esta herramienta, desarrollada por Peter Fiskerstrand[24], es capaz de identificar más de 1000 diferentes tipos de archivo mediante búsqueda de firmas, mostrando información detallada de cada archivo.

La primera versión fue lanzanda en 2010 y la última es la v0.72, lanzada en 2014. Está disponible para todas las versiones Windows que puedan ejecutar .NET 2.0.

Algunos de los formatos de archivo que HexBrowser reconoce son:

- **Audio:** wav, mp3, midi, adlib, adif, avr
- **Vídeo:** wmv, mpg, mov, 3gp, mp4, flac, swf
- **Gráficos:** jpg, bmp, gif, tiff, png, psd
- **Office:** Microsoft Office, OpenOffice, iWorks, txt, html, pdf, chm, xml
- **Archivos:** zip, rar, gzip, jar, 7-zip, deb, rpm

Agent Ransack

Es una herramienta cuyo objetivo es la búsqueda y localización de archivos, usando operadores booleanos y expresiones regulares (*regex*) Perl.

[23] http://www.filesignatures.net/
[24] http://www.hexbrowser.com/

La primera versión de Agent Ransack[25] fue lanzada en el año 2000 y actualmente sigue disponible, para plataformas Windows de 32 y 64 bits.

Algunas de las características disponibles son:

- Palabras resaltadas en los resultados para reducir el gasto de tiempo buscando
- Búsqueda de términos usando operadores booleanos
- Soporta formatos de Office
- Soporta expresiones regulares compatibles con Perl
- Búsqueda rápida y eficiente
- Los resultados pueden ser compartidos mediante informes, impresión o exportado

HashMyFiles

HashMyFiles[26] se trata de una pequeña herramienta para Windows, en versiones de 32 y 64 bits. Su primera versión fue lanzada en 2007 y actualmente, su versión más reciente es la 2.10.

Su utilidad consiste en calcular los *hashes* MD5 y SHA-1 de uno o más archivos. La lista de *hashes* obtenida se puede copiar en el portapapeles o guardarla en un archivo de texto o en archivos HTML o XML.

Tiene posibilidad de ser lanzado desde el menú contextual o desde la línea de comandos.

4.2.3 Análisis de correo electrónico

Las herramientas de esta subsección irán destinadas a mostrar a la figura del investigador datos e información relevante durante el análisis de correos electrónicos.

E-mail History Browser

Esta herramienta[27] recoge y muestra el historial de emails de distintos clientes de correo electrónicos de forma comprensiva para el investigador, mostrando detalles como el emisor, asunto del mensaje, fecha de recepción, receptor y tamaño.

El cuerpo del mensaje y los archivos adjuntos no se muestran, con motivo de mantener la intimidad del emisor o el receptor.

Está disponible para entornos Windows y los clientes de correo soportados son los siguientes:

- Microsoft Outlook Express

[25] http://www.mythicsoft.com/agentransack
[26] http://www.nirsoft.net/utils/hash_my_files.html
[27] http://www.mitec.cz/ehb.html

- Microsoft Windows Mail
- Microsoft Windows Live Mail
- Mozilla Thunderbird

MBOX Viewer

MBOX Viewer[28] es una herramienta con la que se podrán ver archivos MBOX junto a sus archivos adjuntos. Algunos de los clientes de correo que usan el formato MBOX son: Mozilla Thunderbird, Google Takeout, Apple Mail, SeaMonkey, etc. Se encuentra disponible para entornos Windows.

Como ya se ha dicho, se podrán visualizar los emails contenidos en el archivo MBOX, con sus correspondientes atributos y correctamente formateados, junto a los archivos adjuntos. Para ello, se realizará un escaneado rápido del archivo MBOX seleccionado y se listarán todos los emails en estructura de carpetas. A parte de eso, no es necesario que haya instalado ningún cliente de correo para poder utilizar esta herramienta.

4.2.4 Captura de datos

En esta sección se van a describir distintas herramientas destinadas a la captura de diversos tipos de datos, como los contenidos en medios de almacenamiento, en la memoria volátil (RAM) o el tráfico de red.

Guymager

Se trata de una herramienta para obtener archivos de imagen provenientes de la adquisición de un medio de almacenamiento. Está disponible para Linux y viene incluida en las distribuciones mostradas en la sección 4.1. Genera imágenes raw (dd), ewf (e01) y aff.

Guymager trabaja con dos archivos de configuración:

- `/etc/guymager/guymager.cfg`**:** se trata del archivo de configuración principal. **No se debe cambiar**, ya que los cambios se pierden al instalar una nueva versión.
- `/etc/guymager/local.cfg`**:** este es el archivo para realizar cambios locales. Los cambios realizados en este archivo tienen preferencia sobre el mencionado en el punto anterior.

También es posible probar un parámetro sin editar el archivo `local.cfg`, simplemente desde la línea de comandos. Se puede ver un ejemplo en la sección *Configuration and log* de la propia página web[29].

Si se desea más información sobre esta herramienta puede acudirse a su wiki[30].

[28] http://www.systoolsgroup.com/mbox-viewer.html
[29] http://guymager.sourceforge.net/
[30] http://sourceforge.net/p/guymager/wiki/Home/

Rekall Memory Forensic Framework

Rekall [31] es una colección de herramientas para la extracción de artefactos digitales de la memoria RAM, con ayuda de determinados plugins.

Esta herramienta funciona en cualquier plataforma que soporte Python. Soporta imágenes de memoria de 32 y 64 bits pertenecientes a Windows, Linux y Mac OSX.

Como podemos ver, Rekall presenta muchas similitudes con Volatility, descrita en la sección 4.2.1. Esto es así porque en un principio empezó siendo una nueva rama dentro del proyecto Volatility, sin embargo, debido a los cambios introducidos durante el desarrollo de la misma se decidió continuar como un proyecto aparte.

Adicionalmente, y siendo la siguiente característica una de las diferencias claves entre Volatility y Rekall, es posible realizar una adquisición completa de la memoria RAM.

Wireshark

Wireshark[32] es un analizador de paquetes de red, lo que comúnmente en el mundo de la informática se denomina *sniffer*. Tratará de capturar los paquetes de red y mostrará al usuario los datos de los paquetes capturados de forma detallada. De esta forma, algunos de los usos de Wireshark podrán ser aprender los entresijos del protocolo de red, examinar problemas de seguridad, etc.

El desarrollo de esta herramienta comenzó en 1997 con el nombre de *Ethereal*, pero con el paso de los años, el proyecto fue creciendo con las contribuciones de gran cantidad de colaboradores de diversos países y en 2006 se convirtió en Wireshark, cuya primera versión fue lanzada en 2008 y que actualmente se encuentra en la versión 1.12.3, disponible para Windows, Linux y Mac OSX.

Algunas de las características de Wireshark son:

- Inspección en profundidad de cientos de protocolos[33]
- Captura de paquetes en vivo y análisis offline
- Lectura/escritura de multitud de formatos de archivo de captura
- Filtrado y búsqueda de paquetes basado en múltiples criterios

4.2.5 Análisis de archivos y datos

Se realizará una breve descripción de diversas herramientas relacionadas con el análisis de distintos tipos de datos y archivos.

[31] http://www.rekall-forensic.com/
[32] https://www.wireshark.org/
[33] https://www.wireshark.org/docs/dfref/

Bulk Extractor

Bulk Extractor[34] es una herramienta que extrae datos como direcciónes de correo electrónico, números de tarjetas de crédito, URLs y otros tipos de información de archivos contenedores de evidencias digitales. La extracción se puede obtener de diversos medios de almacenamiento: discos duros, tarjetas de cámaras fotográficas e incluso de archivos de captura de paquetes de red, etc.

La búsqueda de estos datos se hace de forma que se ignora la estructura del sistema de archivos. Algunas ventajas de lo anterior son que debido al propio hecho de ignorar el sistema de archivos es posible procesar cualquier tipo de medio digital y además se consigue una mayor velocidad al procesar los datos [GB14].

Una vez los datos han sido extraídos, se construye un histograma de algunos de los datos obtenidos.

Algunas de las características de esta herramienta son:

- Encuentra datos que otras herramientas pasan por alto, pues procesa archivos comprimidos y datos incompletos o parcialmente corruptos
- Construye listas de palabras basándose en todas las palabras encontradas entre los datos, que más tarde pueden ser útiles para romper contraseñas
- Dispone de GUI
- Dispone de un pequeño número de programas en python para llevar a cabo análisis adicional

ExifTool

ExifTool[35] es una herramienta para leer, escribir o manipular los metadatos de distintos archivos (imagen, vídeo, sonido, etc.), soportando una gran cantidad de formatos[36]. Está escrita en Perl y disponible para Windows, Mac OSX y Linux. Actualmente, su versión más reciente es la 9.82 (2015), aunque cuenta con una gran historia de mejoras, pues su versión inicial fue lanzada en 2003.

Cuenta con una gran cantidad de características, pudiendo éstas ser consultadas en la sección correspondiente de la página web de la herramienta[37]. Algunas de estas características son:

- Soporta gran cantidad de archivos de metadatos
- Lee y escribe *maker notes* (información sobre configuraciones de la cámara) de muchos modelos de cámaras digitales

[34] https://github.com/simsong/bulk_extractor
[35] http://www.sno.phy.queensu.ca/ phil/exiftool/
[36] http://www.sno.phy.queensu.ca/ phil/exiftool/#supported
[37] http://www.sno.phy.queensu.ca/ phil/exiftool/#features

- Numerosas opciones para el formato de salida (HTML, XML, JSON, etc.)
- Elimina metadatos, ya sea de manera individual, en grupos o en general
- Posibilidad de modificar el lenguaje de la salida

Ghiro

Esta herramienta[38] tiene como objetivo el análisis forense de imágenes digitales de forma intuitiva. Todas las tareas (análisis completo de la imagen e informe de resultados) están totalmente automatizadas, relegando al usuario la simple tarea de subir las imágenes que desee analizar a la interfaz web desde la que se llevan a cabo todas las funciones de Ghiro.

La descarga de esta herramienta está disponible mediante el clonado del repositorio del proyecto[39] en el propio equipo de uso, la descarga del paquete en formato zip o tar.gz o como *virtual appliance* para ejecutar desde algún software de virtualización.

Algunas de sus características se muestran a continuación:

- Extracción de metadatos
- Se muestra información MIME
- Análisis ELA
- Extracción de miniaturas de imagen
- Búsqueda de imágenes por hash

Microsoft PsTools

PsTools[40] se trata de una suite de utilidades en línea de comandos dirigidas a entornos Windows, creada por Mark Russinovich. Esta suite permite tanto gestionar sistemas remotos como sistemas locales.

Las herramientas por las que está formado este conjunto de herramientas se puede observar en el cuadro 4.2:

Si se está interesado en conocer más al respecto, se recomienda leer el manual básico de PsTools, escrito por Wes Miller[41]

Nmap

Nmap[42] es una herramienta de exploración de redes y escaneo de puertos, utilizada generalmente en auditorías de seguridad. Fue creada en 1997 y actualmente su versión más reciente es la 6.40 (2013). Está disponible para Windows, Linux Y Mac OSX.

[38] http://www.getghiro.org/
[39] https://github.com/Ghirensics/ghiro
[40] https://technet.microsoft.com/en-us/sysinternals/bb896649.aspx
[41] https://technet.microsoft.com/es-es/magazine/2007.03.desktopfiles.aspx
[42] http://nmap.org/

Herramienta	Descripción
PsExec	Ejecuta procesos remotamente
PsFile	Muestra archivos abiertos de remotamente
PsGetSid	Muestra el SID (Identificador de seguridad) de un equipo o usuario
PsInfo	Muestra información sobre un sistema
PsPing	Muestra el rendimiento de una red
PsKill	Mata procesos por nombre o por ID de proceso
PsList	Muestra información detallada sobre los procesos en ejecución
PsLoggedOn	Muestra quién ha iniciado sesión localmente y los usuarios de recursos compartidos
PsLogList	Vuelca los registros de eventos
PsPasswd	Cambia contraseñas de cuenta de usuario
PsService	Visualiza y controla servicios
PsShutdown	Apaga, suspende o reinicia un equipo
PsSuspend	Suspende procesos en ejecución

Cuadro 4.2: Herramientas de la suite PsTools

Esta herramienta proporciona información como equipos que se encuentran disponibles en una red, los servicios que ofrecen, los sistemas operativos utilizados… entre muchas otras características. Esta información es proporcionada en forma de lista de los objetos que han sido analizados, junto a información extra que será variable en función de las opciones utilizadas.

Lo principal que se muestra es una tabla de puertos considerados interesantes, que se compone del número de puerto, su estado, el servicio que ofrece, la aplicación que se está ejecutando y si se usa la opción de detección de versiones, también se incluirán detalles sobre la versión de la aplicación.

En la sección *Docs* de la web[43] se puede encontrar la guía de referencia de Nmap traducida a varios idiomas.

Xplico

Xplico[44] es una NFAT que está instalada en la mayor parte de distribuciones orientadas al análisis forense, incluidas aquellas que se trataron en la sección 4.1. La interfaz de usuario consiste en una interfaz web y es multiusuario, permitiendo el acceso concurrente de varios usuarios.

El objetivo de esta herramienta consiste en extraer de una captura de tráfico de red los datos de aplicación contenidos en la misma, como pueden ser emails, contenidos HTTP, llamadas

[43] http://nmap.org/docs.html
[44] http://www.xplico.org/

VoIP, etc. Los protocolos soportados pueden ser consultados en la sección *Status* de la propia página web[45].

4.2.6 Dispositivos móviles

Esta sección se centrará principalmente en dispositivos con sistema operativo Android[46].

SAFT Mobile Forensics

SAFT[47] se trata de una herramienta destinada al análisis forense de dispositivos Android, con la cual (en su versión gratuita) se pueden obtener los mensajes SMS, registros de llamada y contactos contenidos en los mismos.

El modo de uso es bastante sencillo, simplemente se debe conectar el dispositivo al equipo mediante USB y seguir las instrucciones. Para poder utilizar esta herramienta, se deberán tener instalados los drivers del dispositivo que se quiere investigar y también activar el modo de depuración USB en los ajustes del teléfono.

NowSecure Forensics Suite: Community Edition

Esta herramienta, también orientada a dispositivos Android, nos permite a través de una máquina virtual preconfigurada realizar las siguientes operaciones:

- Adquirir y conectar a un dispositivo móvil
- Extraer datos usando el sistema de archivos, copias de seguridad (*backups*) o métodos lógicos
- Evitar la pantalla de bloqueo del dispositivo
- *Rootear* un dispositivo para extracciones de datos más profundas

Para consultar una lista detallada de características y más información sobre como utilizar esta herramienta se puede visitar la propia página de NowSecure[48].

4.2.7 Análisis de Internet

Se dedicará esta sección a describir herramientas destinadas a obtener algunos de los datos que pueden conseguirse mediante el análisis forense de navegadores.

Dumpzilla

Dumpzilla[49] está desarrollada en Python 3 y su objetivo es el de extraer datos útiles para una investigación forense de los navegadores Firefox, Iceweasel y SeaMonkey. Está dispo-

[45] http://www.xplico.org/status
[46] http://www.android.com/
[47] http://www.signalsec.com/saft/
[48] https://www.nowsecure.com/forensics/community/
[49] http://www.dumpzilla.org/

nible para Linux y Windows 32 y 64 bits y su uso se lleva a cabo a través de la línea de comandos.

Con Dumpzilla se pueden obtener los siguientes contenidos:

- Cookies + DOM Storage (HTML 5)
- Preferencias del usuario
- Descargas
- Uso de formularios web
- Historial
- Marcadores
- Visualización / Extracción de la caché HTML5 (Offline cache)
- Visualización / Extracción de los thumbnails de sitios visitados
- Add-ons (complementos) y rutas o URLs que han utilizado
- Contraseñas almacenadas
- Certificados SSL añadidos como excepciones
- Datos de sesiones
- Visualizar la navegación del usuario en tiempo real

Si se desea llevar acabo un análisis más completo del navegador, se pueden usar herramientas que sirvan para extraer datos de la caché, como por ejemplo MozCache[50] o MozillaCacheView[51].

Herramientas para extracción de datos de la caché

Análogamente a las recién mencionadas herramientas MozCache y MozillaCacheView, se dispone de herramientas similares pero destinadas a otros navegadores:

- ChromeCacheView[52], para el navegador Google Chrome
- OperaCacheView[53], sin embargo, ésta solo funciona con versiones antiguas del navegador

Con este tipo de herramientas es posible obtener datos asociados a los archivos contenidos en la caché: URL, tipo de contenido, tamaño de archivo, última fecha de acceso, etc.

[50] http://mozcache.sourceforge.net/
[51] http://www.nirsoft.net/utils/mozilla_cache_viewer.html
[52] http://www.nirsoft.net/utils/chrome_cache_view.html
[53] http://www.nirsoft.net/utils/opera_cache_view.html

MyLastSearch

MyLastSearch[54] es una herramienta que escanea la caché y el historial del navegador analizado, obteniendo las búsquedas que se realizaron con los principales motores de búsqueda y las redes sociales más populares.

Los datos mostrados en los resultados incluyen: texto de búsqueda, motor de búsqueda, fecha de la búsqueda, tipo de búsqueda (general, vídeo, imágenes), navegador utilizado y URL de la búsqueda. Estos resultados pueden copiarse al portapapeles o ser guardados en archivos de texto, HTML o XML.

Esta utilidad se encuentra disponible para Windows y no requiere de ningún proceso de instalación, simplemente debe ser ejecutada desde el archivo ejecutable o desde la línea de comandos. Para ver ejemplos de uso a partir de ésta última se puede consultar la propia página web de la herramienta.

4.2.8 Análisis del registro

En esta sección serán descritas herramientas cuya finalidad es obtener del registro de Windows datos útiles para una investigación forense.

RegRipper

Se trata de una herramienta escrita en Perl, cuyo objetivo es extraer información del registro para posteriormente someterla a análisis.

RegRipper[55] está formada por dos herramientas básicas:

- **RegRipper GUI**: permite seleccionar un *hive*[56] a analizar, un archivo de salida para guardar los resultados y una lista de plugins para ejecutar sobre el *hive*. Además, se creará un log de actividad en el mismo directorio del archivo de salida
- **RegRipper CLI**: llamada *rip*, que puede ser ejecutada sobre un *hive*, ejecutando a su vez sobre él una lista de plugins o un plugin individual, mostrando los resultados en la salida estándar (*stdout*). Rip puede ser incluido en archivos batch mediante operadores de redirección. No crea log de actividad

Se puede consultar más información sobre RegRipper en su propio blog [57].

UserAssistant

UserAssistant[58] es una herramienta que extrae ciertos valores contenidos en el *hive* NTUSER.DAT. Estos valores son: SID, nombres de usuario, índices, nombres de aplicación, con-

[54] http://www.nirsoft.net/utils/my_last_search.html
[55] https://code.google.com/p/regripper/
[56] Cada uno de los subárboles del registro, que comienzan siempre por «HKEY».
[57] https://regripper.wordpress.com/
[58] http://www.4discovery.com/our-tools/

tador de ejecución y atributos sobre la última ejecución, que pueden ser guardados en un archivo CSV para un análisis posterior.

Las claves UserAssist son usadas por Microsoft para poblar el menú de inicio de Windows con las aplicaciones usadas más frecuentemente por el usuario. Estas claves tienen valor forense, ya que a través de ella se pueden determinar aspectos como:

- Frecuencia de ejecución de un programa
- Última vez que un programa fue ejecutado
- El lugar desde el que los items fueron lanzados con más frecuencia
- Cambios de fecha u hora en el sistema
- Evidencia de programas después de que hayan sido desinstalados
- Cuánto tiempo ha estado interactuando con un programa un determinado usuario (Windows 7)
- Evidencia de ausencia[59] (por ejemplo, items que estaban en un determinado lugar en un determinado momento)

4.3 Herramientas hardware

En esta categoría serán descritos varios tipos de herramientas hardware, en distintas categorías, según la finalidad a la que las mismas se destinen. Todas las herramientas han sido seleccionadas de la página web *Forensic Store*[60]. Además de esta fuente, hay otras donde se analizan diferentes productos, como por ejemplo: *MediaClone*[61] o *Digital Intelligence*[62]

Una vez más el motivo de estas herramientas es el de facilitar ciertas tareas recurrentes en el mundo del análisis forense informático. Con las herramientas hardware es posible esquivar el contacto directo con las herramientas software para realizar de manera automática tareas como la adquisición de medios de almacenamiento (realización de clonados e imágenes de disco), todo ello de forma segura mediante sistema hardware de bloqueo de escritura, al igual que se da la posibilidad de realizar borrados seguros de los dispositivos.

4.3.1 Análisis de dispositivos móviles

En la actualidad, la mayoría de las personas que conocemos disponen de teléfono móvil, que cada vez disponen de mayor tecnología incorporada. Estos dispositivos también contienen datos que pueden ser sometidos a análisis. En esta sección se presentarán algunas herramientas que ayudarán a extraer dichos datos.

[59] http://www.4n6k.com/2013/05/userassist-forensics-timelines.html
[60] http://forensicstore.com/
[61] http://www.media-clone.net/
[62] http://www.digitalintelligence.com/forensichardware.php

Cellebrite UFED Touch Ultimate

Esta herramienta[63] ayuda a realizar la extracción, decodificado, análisis y reporte de los datos contenidos en el dispositivo.

Permite la extracción física y lógica de los datos contenidos en el dispositivo, y también la del sistema de archivos. Además, soporta una gran variedad de dispositivos, incluyendo dispositivos GPS y tablets, entre otros. Precio a consultar en la página web.

Paraben Mobile Field Kit

El Paraben Mobile Field Kit[64] es una herramienta portátil que contiene todo lo necesario para llevar a cabo un análisis forense exhaustivo de varios tipos de dispositivos, como teléfonos móviles, PDAs y dispositivos GPS en cualquier parte.

Su precio es de $ 3995 e incluye lo siguiente:

- Licencia para el producto *Device Seizure*[65], para adquirir, analizar y hacer reportes de dispositivos
- Licencia para el producto *DDS*, para un análisis rápido y básico
- Cables, cargadores y demás hardware necesario para extraer datos de los dispositivos
- Un portátil destinado a adquisiciones y análisis
- Varios lectores de tarjetas
- Maletín duro de transporte
- Un año de suscripciones software y nuevos cables
- Un dispositivo Project-A-Phone ICD-5200 para tomar imágenes de cada pantalla
- Una bolsa de secado Save-A-Phone para dispositivos electrónicos

Además, el Paraben Mobile Field Kit es ampliable, por lo cual se pueden añadir nuevas herramientas, tanto hardware como software para aumentar su utilidad.

4.3.2 Hardware forense

Aquí son presentadas y descritas varias herramientas destinadas a distintas aplicaciones, como el borrado de datos, conservación de la integridad de los mismos y creación de imágenes de medios de almacenamiento.

Wiebetech Media WriteBlocker

Este producto de Wiebetech se trata de un bloqueador hardware de escritura, que como su propio nombre indica, proporciona acceso con escritura bloqueada a distintos tipos de

[63] http://forensicstore.com/product/cellphone-analysis/cellebrite-products/
[64] http://forensicstore.com/product/cellphone-analysis/paraben-mobile-field-kit/
[65] http://forensicstore.com/product/cellphone-analysis/paraben-device-seizure-6-5/

medios de almacenamiento USB y tarjetas flash. Incluye también un modo lectura/escritura que permite acceso completo a los medios conectados.

Su uso es muy simple, solo hace falta conectar el dispositivo deseado al Wiebetech Media WriteBlocker, y éste al equipo. El LED indicará que la protección contra escritura está activa.

Su precio es de $ 249. Puede consultarse su página de producto[66] para mayor información sobre sus especificaciones técnicas.

Wiebetech Forensic UltraDock

El Forensic UltraDock[67] es una herramienta destinada a crear una imagen de un medio de almacenamiento conectado a él. Cuenta con 5 puertos en el lateral (1 Firewire 400, 2 Firewire 800, 1 USB 3.0 y 1 eSATA) y conexiones SATA y PATA (IDE).

Dispone también de tecnología bloqueadora de escritura, proporcionando acceso de solo lectura a los dispositivos conectados, de esta forma se facilita mantener la cadena de custodia. Es compatible con software de adquisición y análisis y detecta zonas HPA y DCO (ocultas para el SO). También soporta la tecnología S.M.A.R.T., relacionada con información sobre disco.

Su precio es de $ 279 y para usarlo tan solo se debe conectar el dispositivo deseado al Forensic UltraDock y éste a un equipo. Como siempre, las especificaciones técnicas pueden ser consultadas en la página web referenciada anteriormente.

Wiebetech Drive eRazer Ultra

Drive eRazer Ultra es un dispositivo que se encarga de borrar de forma segura todos los datos de un disco duro por si mismo (incluidas las zonas HPA y DCO), sin necesidad de conectarlo a un equipo. Además es más rápido que las soluciones software.

Dispone de varios modos de borrado, que pueden consultarse en su página de producto[68] junto a sus especificaciones técnicas, o crear uno personalizado. Es compatible con dispositivos SATA y PATA (IDE). Se puede adquirir por un precio de $ 249.

Wiebetech Ditto Forensic FieldStation

El Ditto Forensic FieldStation[69] se trata de un dispositivo que agrupa muchas de las características de las tres herramientas previamente descritas.

Por una parte, es capaz de realizar clonados e imágenes de disco, siendo posible configurar y llevar a cabo adquisiciones forenses sin necesidad de otro equipo. Para ello cuenta con una

[66] http://forensicstore.com/product/forensic-hardware/wiebetech-media-writeblocker/
[67] http://forensicstore.com/product/forensic-hardware/forensic-ultradock/
[68] http://forensicstore.com/product/forensic-hardware/drive-erazer-ultra/
[69] http://forensicstore.com/product/forensic-hardware/ditto-forensic-fieldstation/

serie de entradas: SATA, eSATA, PATA y USB 2.0, todas ellas con bloqueo de escritura.

Por otra parte, es capaz llevar a cabo un borrado completo y seguro de los dispositivos conectados, mediante modos de borrado preconfigurados o por algún patrón configurable por el usuario.

Soporta la tecnología S.M.A.R.T. y detecta zonas HPA y DCO, permitiendo eliminarlas temporal o permanentemente. Tiene un precio de $ 1489. Si se desea conocer el resto de especificaciones técnicas, se recomienda visitar su página de producto.

4.3.3 Equipos forenses

Esta sección va dedicada a presentar algunos equipos informáticos de alta gama destinados a la investigación forense.

HTCI Standard

El HTCI Standard[70] combina un procesador Intel Core i7 a 3.2 GHz (3.8 GHz Turbo) con 32 GB memoria RAM DDR3, un disco duro de 2 TB de capacidad y un disco SSD de 128 GB. Lleva instalado Windows 7 Ultimate por defecto.

Este equipo forense soporta dispositivos IDE, SATA, SAS y USB. Dispone también de bloqueador de escritura en el lector de tarjetas y en las conexiones para los dispositivos anteriormente citados. Además viene con una licencia de prueba de 30 días para el software *Internet Evidence Finder (IEF)* de Magnet Forensics[71].

Acudir a la página de producto de este equipo si se desea conocer el resto de especificaciones técnicas del mismo. Su precio es de $ 5995.

HTCI Extreme Series Laptop

En este caso, se trata de otro equipo destinado a la investigación forense, un ordenador portátil de 15.6" esta vez. Lleva incorporado un procesador Intel Core i7 a 2.8 GHz (3.8 GHz Turbo), 8 GB de memoria RAM DDR3 y un disco SSD de 256 GB de capacidad. El SO por defecto es Windows 7 Ultimate.

Dispone de varios tipos de puertos: 1 USB 2.0, 3 USB 3.0 y 1 eSATA, entre otros. Visitar la página web de producto[72] si se desea consultar las especificaciones técnicas completas. El precio es de $ 2495.

4.4 Conclusión

Se han mostrado gran cantidad de herramientas forenses, tanto distribuciones orientadas a este fin, como herramientas software y hardware. La necesidad de recurrir a herramientas

[70] http://forensicstore.com/product/forensic-computers/htci-standard/
[71] http://www.magnetforensics.com/
[72] http://forensicstore.com/product/forensic-computers/htci-extreme-series-laptop-15/

tanto hardware como software responde a la multitud de fases por las que debe pasar un análisis forense, que no suele limitarse a la investigación de un único tipo de dato. Es por ello necesario la combinación de varios tipos de las herramientas como las descritas en este capítulo, complementándose entre sí.

Por ejemplo, un determinado investigador o interesado en el tema que nos concierne puede decidir realizar un análisis forense a su propio equipo, por lo cual, si no dispone de una distribución GNU/Linux preparada para tal fin, cualquiera de las distribuciones anteriormente descritas puede ser tremendamente útil ya que proporciona tanto el entorno de trabajo como las herramientas software que serán de utilidad, agrupadas bajo distintas categorías para realizar los tipos de análisis que se estimen oportunos.

Capítulo 5

Estado del arte de metodologías para la investigación forense

DURANTE este capítulo se procederá a mostrar y a describir las fases de las que se compone una investigación forense. No obstante, ha de quedar claro que no hay una única manera de llevar a cabo una investigación, pues existen gran cantidad de modelos en los que basarse, cada uno con sus correspondientes fases bien diferenciadas. Por tanto, será aquí presentada una selección de algunos de ellos.

5.1 Según Forensic Control

La empresa *Forensic Control*[1] ofrece un modelo dirigido a una audiencia sin demasiados conocimientos técnicos, desde una perspectiva neutra, sin ceñirse a ninguna legislación específica.

De esta forma, han decidido dividir el proceso de la investigación forense en seis fases (ver figura 5.1) en orden cronológico, que serán expuestas a continuación.

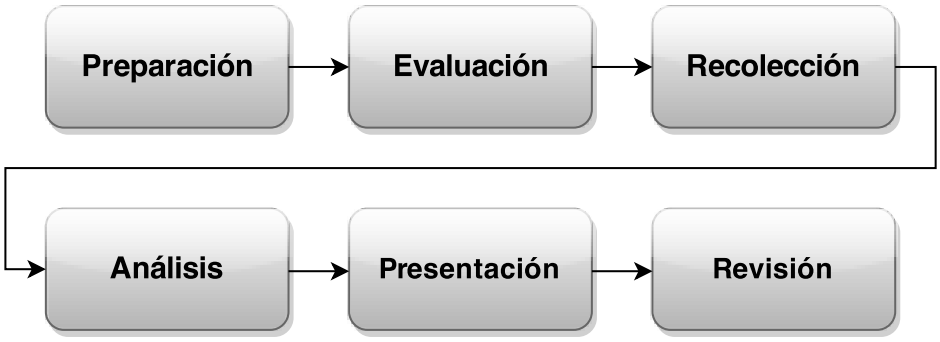

Figura 5.1: Fases según *Forensic Control*

5.1.1 Preparación

Esta es una fase importante, no obstante, en ocasiones es pasada por alto o ignorada durante el proceso de investigación.

La fase de preparación consiste, en el caso del propio examinador forense, en contar con un entrenamiento y una preparación adecuados, además de hacer chequeos habituales del

[1] https://forensiccontrol.com/resources/beginners-guide-computer-forensics/

correcto funcionamiento de su equipo, tanto hardware como software y además estar familiarizados con la legislación pertinente.

Por otra parte, también es importante hacer que el cliente adquiera concienciación sobre la preparación del sistema, por ejemplo: si las funciones de auditoría de éste fueron activadas previamente al momento en el que un incidente ocurrió, después será más fácil seguir la traza de lo que ocurrió, facilitando la investigación.

5.1.2 Evaluación

La fase de evaluación incluye la recepción de una serie de instrucciones, debiendo quedar éstas lo más claras posible, sin dejar hueco a la ambigüedad. También debe llevarse a cabo un análisis de riesgos y hacer una asignación de roles y de los recursos disponibles.

El análisis de riesgo tiene un significado diferente depende del ámbito en el que se lleve a cabo. Por ejemplo, para los cuerpos de seguridad puede incluir una evaluación sobre las probabilidades de recibir un daño físico al entrar en la propiedad de un sospechoso y qué hacer para contrarrestarlo.

En el caso de las organizaciones comerciales puede significar evaluar la probabilidad de sufrir pérdidas económicas o de perjudicar la reputación de la propia organización, tener en cuenta los problemas de conflicto de intereses, etc.

5.1.3 Recolección

En la fase de recolección se va a producir, por un lado, la adquisición de las evidencias, que en el caso de que tuviera que realizarse en el propio escenario, fuera del laboratorio forense, se asegurará la identificación y la protección de los dispositivos que pudieran contener las posibles evidencias y se documentará también el propio escenario.

En el caso anterior, sería bastante útil realizar alguna entrevista con las personas que pudieran proporcionar información relevante a la investigación.

Si se decidiera llevar a cabo la adquisición de los datos posteriormente en el laboratorio forense, entonces se deberían etiquetar adecuadamente los dispositivos y almacenarlos en un embalaje apropiado (normalmente en bolsas antiestáticas).

5.1.4 Análisis

La fase de análisis varía siempre en función de lo que se esté analizando. Normalmente el examinador proporciona un *feedback* al cliente durante el proceso, y en función de ésto el análisis tomará un camino u otro. El análisis debe ser un proceso preciso, meticuloso, imparcial, repetible y además finalizado dentro de unos límites de tiempo y con una determinada asignación de recursos.

Destinadas a esta fase hay gran variedad de herramientas, tanto software como hardware, como se pudo comprobar en el capítulo 4. Por tanto, queda a elección del examinador la

elección de las mismas.

Para confirmar la integridad de los resultados se podría emplear el método de verificación a través de dos herramientas, consistente en comparar el resultado arrojado por ambas herramientas y observando si ambos son iguales.

5.1.5 Presentación

En esta fase entra en juego el informe pericial, que contendrá los descubrimientos obtenidos por el examinador. En este caso dará respuesta a las cuestiones por las que se inició el proceso de investigación, junto a instrucciones subsecuentes. También podrá incluir cualquier información que considere oportuna, pertinente a la investigación.

El informe debe contener un lenguaje y una terminología entendibles para cualquier persona, puesto que a menudo el lector final del informe no cuenta con conocimientos técnicos avanzados. Debido a lo anterior, el examinador debe estar preparado para poder resolver cualquier duda que surja o para defender el propio informe en un proceso legal.

5.1.6 Revisión

Al igual que la fase de preparación, esta última fase es a menudo pasada por alto debido a que no es facturable o a la necesidad de empezar un nuevo trabajo.

No obstante, llevar a cabo una revisión de la investigación puede ayudar a ahorrar dinero y a elevar la calidad de futuras investigaciones, haciéndolas más eficientes. Cualquier cosa aprendida durante esta fase debería ser aplicada posteriormente.

La revisión puede ser sencilla y rápida y empezar durante cualquier fase anterior, incluyendo un análisis básico de lo que fue bien, de lo que fue mal y aprendiendo de estos aspectos de cara a futuras investigaciones.

5.2 Norma UNE 71506:2013, de AENOR

El contenido de esta norma está desarrollado en la sección B.2 del anexo B, por lo cual se va a proceder a continuación a hacer un simple resumen de las fases que la forman (ver figura 5.2).

Preservación

En esta fase se pretende mantener en todo momento la validez y confiabilidad de las evidencias originales.

Los técnicos que realicen el primer contacto con las evidencias deberán almacenar éstas en los soportes adecuados, llevar la indumentaria adecuada para evitar descargas electrostáticas, usar soportes aislados para evitar interferencias externas y almacenar dichas evidencias de forma segura hasta el final del proceso pericial.

Adquisición

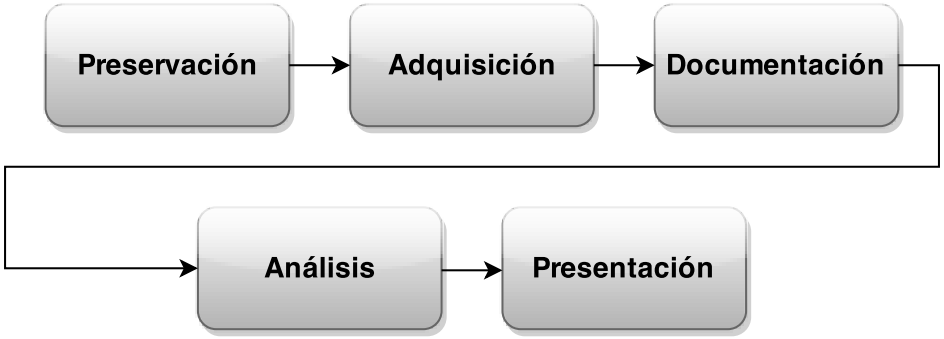

Figura 5.2: Fases de la norma UNE 71506:2013

Durante la fase de adquisición se va a realizar un clonado a bajo nivel de los datos originales, siguiendo una serie de precauciones antes de adquirir dichos datos si el lugar del incidente está delimitado físicamente.

Es importante el propio estado en el que se encuentran los sistemas, puesto que el proceso de adquisición no será el mismo si los sistemas están apagados que si están encendidos, en los que cualquier acción podría comprometer la integridad de las evidencias.

Documentación

En esta etapa se documentará el procedimiento al completo, desde que se inicia el análisis, hasta que se envía el informe pericial al solicitante.

Se documentarán todos los procesos llevados a cabo y las herramientas que se utilizaron, siguiendo una secuencia temporal definida.

En la cadena de custodia quedarán reflejados todos los pasos llevados a cabo durante el manejo de las evidencias.

Análisis

Durante esta fase de análisis se van a llevar a cabo una serie de procesos y tareas que intentarán dar respuesta a preguntas relacionadas al evento que motivó la investigación.

En términos generales, las acciones y procesos que van a llevarse a cabo durante esta fase van a ser:

- Recuperación de ficheros borrados
- Estudio de las particiones y sistemas de archivos
- Estudio del sistema operativo
- Estudio de la seguridad implementada en el sistema
- Análisis detallado de los datos obtenidos

Presentación

Durante la última fase se escribirá un informe pericial con toda la información obtenida

a lo largo del proceso de análisis. Dicho informe deberá escribirse con un lenguaje inteligible para un público no técnico.

Cuando el informe esté finalizado, éste será remitido al organismo solicitante, junto al documento de control de evidencias, para aportar una mayor trazabilidad al proceso.

5.3 Según Francisco Lázaro Domínguez

En su libro *«Introducción a la Informática Forense»*, Fco. Lázaro Domínguez divide la investigación forense en cuatro fases: adquisición, análisis, presentación y línea de tiempo [Lá13] (ver figura 5.3).

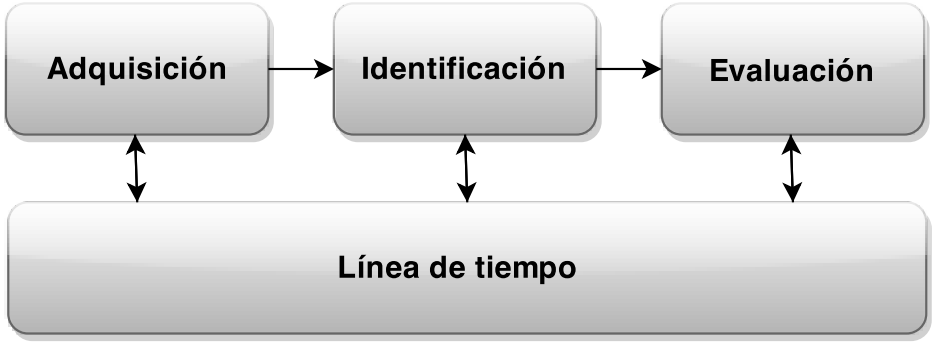

Figura 5.3: Fases según Fco. Lázaro Domínguez

5.3.1 Adquisición

Aquí se realizará el clonado de los datos contenidos en el soporte original. Puede realizarse de dos maneras: en un nuevo dispositivo físico que contendrá el duplicado u obteniendo una imagen completa de los datos originales del medio de almacenamiento. Este último método es denominado *imaging*.

El archivo de imagen resultante de dicho proceso contiene una copia exacta bit a bit de todos los datos que el dispositivo origen contenía, incluyendo espacio no asignado por el sistema de archivos, archivos eliminados, particiones, tabla de particiones, sector de arranque y zonas reservadas y ocultas al sistema operativo, como la HPA y la DCO que normalmente son usadas por el fabricante para introducir información especial o reducir la capacidad de almacenamiento.

La obtención de la imagen deberá realizarse en modo de solo lectura mediante un bloqueador de escritura y calcular el valor hash tanto del dispositivo original como del clon obtenido, empleando algoritmos ampliamente extendidos como por ejemplo: MD5 o SHA-1. Si ambos valores obtenidos son iguales, se puede garantizar que la información original y la obtenida durante la adquisición son idénticas.

5.3.2 Análisis

Durante la fase de análisis se va a llevar a cabo la identificación, el estudio y la interpretación de las posibles evidencias contenidas en el dispositivo de almacenamiento sospechoso. El investigador realizará en esta fase diversas tareas y procesos de investigación y como punto final realizará una interpretación de los resultados para elaborar el informe pericial.

5.3.3 Presentación

La fase de presentación sigue inmediatamente a la fase de análisis. Durante esta fase, el investigador deberá plasmar los resultados obtenidos en un informe pericial, que será destinado a la persona o personas correspondientes.

En dicho informe quedará constancia precisa de toda operación realizada, las evidencias encontradas y en definitiva todo aspecto relacionado que pueda ser considerado de interés.

5.3.4 Línea de tiempo

La línea de tiempo ayuda a comprender la evolución de los hechos y las relaciones causa-efecto que puedan darse entre los mismos, y además contendrá una sucesión de acontecimientos del caso. Ésta será construida a partir de todo tipo de evidencias que proporcionen una información temporal fiable, como por ejemplo aquella encontrada en metadatos de archivos o en logs de sistema, historiales, etc.

Realizar una línea de tiempo es un proceso principalmente manual, no obstante existen herramientas que extraen datos temporales del sistema, facilitando la tarea. Aunque pueda parecer trivial, realizar la línea de tiempo puede resultar importante. Por ejemplo, para dar una presentación ordenada de los hechos ante un tribunal y así reforzar las afirmaciones y el argumento expuesto por el investigador.

5.4 Fase de investigación de la escena digital del crimen, del modelo IDIP

Se ha escogido esta fase del modelo IDIP (Integrated Digital Investigation Process), propuesto por Carrier y Spafford [CS03], por ser la más interesante para nosotros en este caso. El modelo en cuestión consta de 5 fases:

1. Fase de preparación
2. Fase de despliegue
3. Fase de investigación de la escena física del crimen
4. Fase de investigación de la escena digital del crimen
5. Fase de revisión

No obstante, cada una de estas fases es a su vez un grupo de subfases, sumando en total 17. De ellas, 6 son las subfases de las que consta la propia fase de investigación de la escena digital del crimen, siendo éstas idénticas a las de la fase de investigación de la escena física del crimen (ver figura 5.4):

1. Subfase de preservación
2. Subfase de sondeo
3. Subfase de documentación
4. Subfase de búsqueda y recolección
5. Subfase de reconstrucción
6. Subfase de presentación

La subfase de búsqueda y recolección de la escena física del crimen es donde la investigación de la escena digital del crimen empieza. Cuando la fase de investigación de la escena digital del crimen finaliza, estos resultados proporcionan un *feedback* a la subfase de reconstrucción de la escena física del crimen.

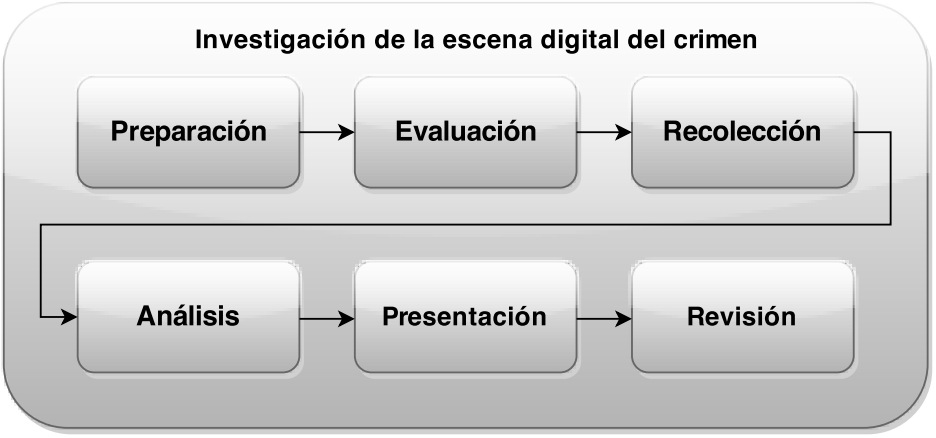

Figura 5.4: Subfases de la fase de investigación de la escena digital del crimen

5.4.1 Subfase de preservación

En esta subfase se intentará preservar el estado original de la escena digital del crimen, es decir, se asegurará su integridad mediante una serie de procesos, como pueden ser: aislar el sistema de la red, adquirir los datos volátiles que puedan perderse al apagar el sistema, identificar los procesos en ejecución sospechosos e incluso a los usuarios sospechosos que hayan iniciado sesión en dicho sistema.

Es común también realizar una imagen del sistema de forma que pueda ser analizado posteriormente en el laboratorio forense.

5.4.2 Subfase de sondeo

Esta etapa ocurre normalmente en un laboratorio forense, utilizando una de las imágenes del sistema obtenidas anteriormente. Se prefiere realizar esta subfase en laboratorio en lugar de hacerlo *en vivo* debido a que se dispone de un entorno controlado en el que los resultados pueden ser repetidos, si es necesario, con otra copia del sistema.

La subfase de sondeo empezará típicamente con una búsqueda en los sitios comunes donde pueden encontrarse evidencias, según el tipo de incidente. Mostrará al investigador el nivel de habilidad del sospechoso y qué técnicas de análisis se necesitarán.

5.4.3 Subfase de documentación

Aquí la finalidad consiste en documentar las evidencias digitales encontradas. Cada una de dichas evidencias, debe ser documentada claramente.

Para verificar la integridad de las evidencias, se calcula el *hash* de cada una de ellas, siendo MD5 y SHA-1 los algoritmos más comúnmente utilizados. Por la misma razón, se debe respetar y seguir rigurosamente el procedimiento de cadena de custodia.

5.4.4 Subfase de búsqueda y recolección

Esta subfase usa los resultados de la de sondeo con el objetivo de centrarse en el análisis adicional. Será aquí donde se emplee la mayor parte del tiempo dedicado a la investigación.

Algunos ejemplos de técnicas de búsqueda comunes son: búsqueda de archivos basándose en el nombre de archivo o patrones en sus nombres, buscando palabras clave en su contenido, fijándose en los datos temporales, etc.

Otro ejemplo sería, en el caso de estar analizado datos de red, buscar los paquetes que provengan de una determinada dirección de origen, o los que vayan dirigidos a un puerto específico [Car05b].

5.4.5 Subfase de reconstrucción

En la subfase de reconstrucción se identificará cómo han llegado las evidencias hasta el lugar en el que se encuentran y qué es lo que significa que se encuentren allí. Es decir, se usarán las evidencias encontradas y se tratará de determinar qué eventos sucedieron en el sistema analizado y cómo sucedieron.

5.4.6 Subfase de presentación

La subfase de presentación se encarga de presentar las evidencias digitales encontradas durante el proceso completo al equipo de investigación de la escena física del crimen, de modo que pueda ser usado en su correspondiente subfase de reconstrucción.

Por tanto, se documentarán y presentarán los hallazgos realizados sobre una escena digital

del crimen específica y se enviarán a otro equipo de investigadores, que en muchos casos suelen ser los mismos para ambas fases.

5.5 Otros modelos

Existen muchos más modelos a seguir, con características similares a los ya presentados, por eso se hará a continuación una breve descripción de algunos de ellos.

5.5.1 Según el NIST

El NIST, en su **Special Publication 800-86**[2], propone un modelo de 4 fases básicas para el proceso forense (ver figura 5.5) que puede ser adaptado al nivel de detalle que sea necesario, en función de las políticas a seguir, las pautas generales y demás aspectos del proceso forense. Estas fases son:

- Recolección
- Examinación
- Análisis
- Presentación de informes

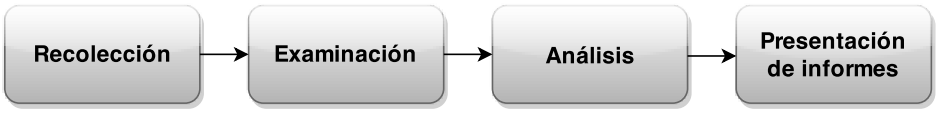

Figura 5.5: Fases según el NIST

5.5.2 Algunos modelos propuestos en el IJCSIT

En esta parte serán descritos algunos de los modelos recopilados en el artículo *Common Phases of Computer Forensics Investigation Models* [YIH11].

Proceso de investigación forense informático (1984)

En 1984, Mark M. Pollitt propuso un modelo formado por 4 fases[3] (ver figura 5.6) con el objetivo de que los resultados obtenidos de la investigación forense fueran confiables científicamente y legalmente aceptables.

Dichas fases son las siguientes:

- Adquisición
- Identificación

[2] http://www.nist.gov/customcf/get_pdf.cfm?pub_id=50875
[3] http://www.digitalevidencepro.com/Resources/Approach.pdf

- Evaluación
- Admisión

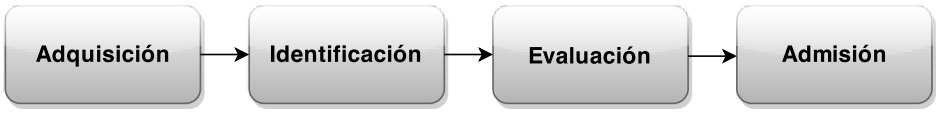

Figura 5.6: Fases según M.M. Pollitt

Modelo DFRWS (2001)

Se presenta en el informe técnico del primer Digital Forensics Research Workshop (DFRWS), que lleva por título *A Road Map for Digital Forensic Research* [DFR01], un modelo de investigación de propósito general que consta de 6 fases (ver figura 5.7), descrito en la página 17 de dicho informe.

Las fases son:

- Identificación
- Preservación
- Recolección
- Examinación
- Análisis
- Presentación

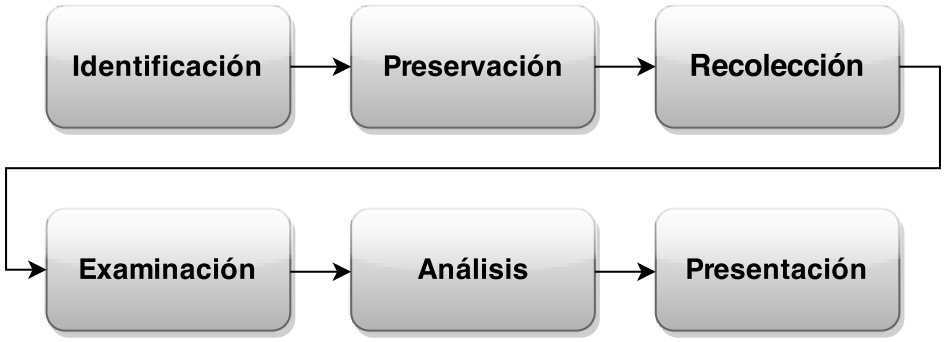

Figura 5.7: Fases del modelo DFRWS

Modelo IDIP (2003)

En la sección 5.4 ya hablamos de parte de este modelo[4], propuesto por Carrier y Spafford, donde se introduce el concepto de escena digital del crimen, formada por el entorno

[4]https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2003-29.pdf

virtual creado por el software y el hardware donde pueden estar contenidas las evidencias digitales.

Está formada por 5 fases, algunas de ellas con sus correspondientes subfases (ver figura 5.8):

- Fase de preparación
  - Preparación de la operación
  - Preparación de la infraestructura
- Fase de despliegue
  - Detección y notificación
  - Confirmación y autorización
- Fase de investigación de la escena física del crimen
  - Preservación
  - Sondeo
  - Documentación
  - Búsqueda y recolección
  - Reconstrucción
  - Presentación
- Fase de investigación de la escena digital del crimen
  - Mismas subfases que la fase anterior
- Fase de revisión

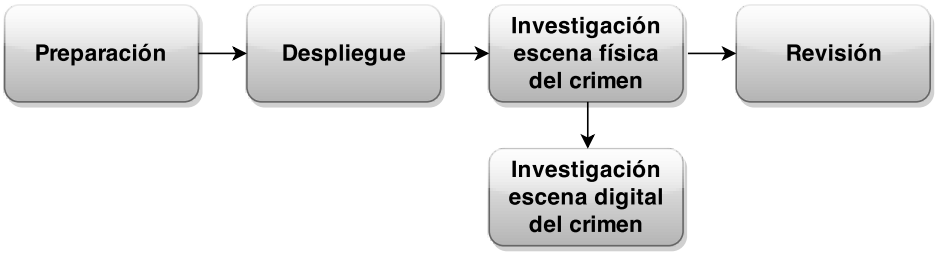

Figura 5.8: Fases del modelo IDIP

5.6 Conclusión

Como se puede observar, existen multitud de modelos que pueden aplicarse a la investigación forense. Todos reflejan en mayor o menor medida los mismos principios básicos, siendo la granularidad de las fases la principal diferencia entre ellos. Una vez dicho esto, cada uno

debería escoger el modelo que más se ajuste a sus necesidades, ya que mientras que algunos de los modelos tienden a ser demasiado detallados, otros son muy generales.

Para la elaboración de la metodología que se va a proponer en este trabajo se escogerá para su uso el modelo propuesto en la norma UNE 71506:2013, vista en este mismo capítulo en la sección 5.2, ya que es bastante completo y además es de aplicación a nivel nacional en España. No obstante, será complementado con la aplicación de las cuestiones jurídicas pertinentes, de modo que se respete la legislación vigente y el informe pericial resultante de haber seguido este modelo pueda ser aportado como medio probatorio en un proceso legal. Además de lo anterior, también se aportará una ampliación de la información relacionada con el tratamiento de la evidencia digital.

Capítulo 6

El procedimiento probatorio en el proceso penal

Se hablará en este capítulo sobre el procedimiento probatorio en el proceso penal, para ello se ha dividido el mismo en una estructura que comprende una serie de conceptos, que facilitarán la comprensión del resto del capítulo, seguido de una sección correspondiente a la determinación del tema, carga y valoración de la prueba.

A continuación se hablará del propio procedimiento probatorio, y finalmente de los distintos medios de prueba existentes, dando mayor importancia a la prueba pericial.

Para mayor información, se recomienda al lector acudir al *Manual de derecho procesal penal* [Gim14] y a *Enjuiciamiento criminal: octava lectura constitucional* [Ram06], los cuales han sido de gran ayuda para la redacción de este capítulo.

6.1 Conceptos

Antes de proceder a la descripción del proceso probatorio en un procedimiento judicial, se expondrán una serie de conceptos que serán importantes para comprender las sucesivas secciones de este capítulo, sobre todo si el lector no está familiarizado con términos relacionados con el campo del derecho.

6.1.1 Presunción de inocencia

La presunción de inocencia es un derecho contemplado en el **art. 24.2 CE** que asiste a todo imputado a lo largo de todas las fases del proceso penal (fase instructora, fase intermedia y juicio oral), consistente en que se debe presuponer la inocencia de éste mientras no se haya dictado una sentencia condenatoria contra él.

Por tanto, el imputado debe ser absuelto si no se han practicado pruebas válidas que confirmen los hechos de los cuales ha sido acusado. Dichas pruebas deben ser lícitas, es decir, deben respetar los derechos fundamentales.

6.1.2 Actos de prueba

Se entiende por actos de prueba a la actividad de las partes procesales, que como su nombre indica, son los litigantes que forman parte de un proceso, rigiéndose por los principios de igualdad y contradicción.

Dicha actividad tiene como objetivo producir una serie de evidencias que convenza al Juez o al Tribunal de los hechos que éstas intentan afirmar.

6.1.3 Actos de investigación

Los actos de investigación, también llamados actos instructorios o «diligencias sumariales», son aquellos que aportan hechos a la instrucción (o fase instructora). Se rigen por el principio de investigación y son practicados por el Juez de instrucción y por su personal colaborador.

Dichos actos tienen como objetivo determinar el delito y su autor, decidir si se abre o no el juicio oral contra un imputado o dictar resolución de sobreseimiento.

6.1.4 Prueba preconstituida

La prueba preconstituida es siempre una prueba documental sobre un hecho que no es posible reproducir posteriormente en la realización de un juicio oral, como por ejemplo una autopsia [Rob13].

Este tipo de prueba es practicada por el Juez de instrucción o, en caso de urgencia, por la policía judicial o el ministerio fiscal.

6.1.5 Prueba anticipada

La prueba anticipada, al igual que la preconstituida, parte de que el hecho que intenta probar es irrepetible. Se diferencia de ésta en que la preconstituida es siempre documental y la anticipada consiste en pruebas personales, como la prueba testifical y la pericial, además de que la prueba anticipada solo puede ser practicada por el Juez de instrucción.

6.1.6 Prueba prohibida

Se denomina prueba prohibida a aquella que sea obtenida a través de la vulneración de derechos fundamentales, de garantías constitucionales, o a través de medios prohibidos o no autorizados expresamente por la CE.

6.2 Tema, carga y valoración de la prueba

Como ya se anunció en la sección 6.1.2, es a las partes a las que corresponde determinar el **tema de la prueba** mediante la afirmación o la negación de los hechos que dan lugar a pretensión penal, a través de los escritos de calificación provisional o de acusación y de defensa. Tales hechos serán los hechos punibles resultantes del sumario (fase instructora), o circunstancias atenuantes, agravantes o eximentes del delito (**art. 650.1º** y **4º LECRIM**).

Determinar el tema es importante, puesto que el Tribunal examinará los medios de prueba y rechazará todo aquel que no guarde relación o no sea pertinente con el tema (**art. 659 LECRIM**).

En cuanto a la **carga de la prueba**, la presunción de inocencia pone la carga en las partes acusadoras, que deberán probar en el juicio oral los hechos constitutivos de delito. No se podrá dictar la sentencia condenatoria si no se prueban dichos hechos.

Si los hechos de la acusación se probaran, la parte de la defensa debería probar los hechos impeditivos, extintivos o excluyentes para conseguir la sentencia absolutoria, recayendo así en este caso la carga de la prueba sobre la defensa.

Después de las pruebas practicadas en el juicio, de las razones que expusieron las partes de acusación y defensa, y de lo manifestado por los procesados, el Tribunal apreciará según su conciencia todo lo anterior y dictará sentencia (**art. 741 LECRIM**). No obstante, aunque posee autoridad suprema e independiente en el proceso de valoración de la prueba, si el Tribunal basara su sentencia en una prueba prohibida (**art. 849 LECRIM**), habría lugar a recurso de casación.

6.3 Procedimiento probatorio

Se va a proceder en esta sección a describir las fases del procedimiento probatorio, que son tres: fase de **proposición**, fase de **admisión** y fase de **ejecución de la prueba**.

La **fase de proposición** comienza con los escritos de calificación provisional o de acusación y defensa, en los que las distintas partes plasmarán las pruebas de las que intentarán valerse durante el juicio oral. También presentarán las listas de peritos y testigos, que contendrán los nombres y apellidos, y el domicilio de éstos. Además, la parte que los presente indicará si los peritos y los testigos deben de ser citados judicialmente o si la propia parte se encargará de su comparecencia (**arts. 656, 657, 781.1, 784.1** y **784.2 LECRIM**).

La prueba pericial se puede proponer también en los escritos como medio de prueba, así como la exhibición del cuerpo del delito o de piezas de convicción, impugnando el informe pericial practicado en la fase instructora.

Con la prueba documental, se determinarán los documentos a examinar por el Tribunal y aquellos que deban leerse en el juicio oral por ser una prueba preconstituida o anticipada.

En el proceso penal abreviado, la proposición de la prueba documental o cualquier prueba que pueda ser llevada a cabo en el acto se podrá hacer al inicio del juicio oral.

La **fase de admisión** comienza con la recepción de los escritos de calificación por parte del magistrado ponente o por el Juez de lo penal, finalizando con la admisión o denegación de los medios de prueba propuestos (**arts. 658, 659, 785.1, 790.6** y **792.1 LECRIM**).

Los medios de prueba serán admitidos si son considerados pertinentes, es decir, aquellos que se adecuen al tema de la prueba propuesto en los escritos de acusación y defensa.

La denegación no procedente de alguno de los medios probatorios propuestos vulnera el derecho fundamental a un proceso con todas las garantías, por lo que puede interponerse un

recurso de casación por denegación de un medio probatorio propuesto a tiempo y considerado pertinente (**art 850.1º LECRIM**).

La **fase de ejecución de la prueba** será efectuada en el juicio oral. En este momento, cualquier persona interrogada o que se dirija al Tribunal deberá hacerlo en pie. Al interrogado se le preguntarán una serie de cuestiones generales, como nombre, apellidos, edad, etc. (**art. 388 LECRIM**) y si se declara culpable del delito del que se le acusa en el escrito de calificación y, en su caso, si está conforme con la petición de pena más amplia (**arts. 688-690 LECRIM**).

Si el interrogado no estuviera conforme, se llevará a cabo la *cross-examination*, mediante la cual el interrogatorio al acusado se practicará de forma que las partes acusadoras serán las que le hagan las preguntas en primer lugar, y posteriormente la defensa. Mediante este proceso serán llevados a cabo también tanto la prueba testifical, como los demás medios de prueba.

6.4 Medios de prueba

Existen varios medios de prueba, a saber:

- **Declaración del acusado**
- **Prueba testifical**, es decir, la declaración proporcionada por testigos directos o indirectos
- **Prueba pericial**, que consiste en el propio informe pericial y la defensa de éste por parte del perito o de los peritos, si se hace necesaria su comparecencia en juicio
- **Prueba documental**, todo documento o prueba de convicción que ayude a esclarecer los hechos (**art. 726 LECRIM**)
- **Reconocimiento judicial**, más concretamente la inspección ocular, contemplada en el **art. 727 LECRIM**

De los anteriores, se hará hincapié en la **prueba pericial**, pues es la que aplica en mayor medida al presente documento.

6.5 Prueba pericial

Como ya se dijo en la sección 6.3, la prueba pericial, como todas las demás, se propondrán en los escritos de calificación provisional, adjuntando la lista de peritos con diversa información de identificación y contacto referente a los mismos. También será indicado si éstos deben de ser citados judicialmente o si la propia parte se encargará de su comparecencia (**arts. 656, 657, 781.1** y **784.2 LECRIM**).

Si faltaran a su obligación de comparecer, los peritos incurrirían en una multa de 200 a 5000 €. Si continuaran en su negativa, podrían ser procesados por un delito de obstrucción

a la justicia (**arts. 175.5, 463** y **661 LECRIM**). Para más información sobre las funciones, derechos, deberes, etc. del perito, se recomienda al lector acudir al anexo D.

La prueba pericial, además, también puede llevarse a cabo como prueba preconstituida o como anticipada, que no entrarían al juicio oral como pruebas periciales, sino como documentales, según lo dispuesto en el **art. 788.2 LECRIM**. Por tanto, para que el Tribunal pueda finalmente basar su sentencia en dichos documentos, deben leerse en el juicio oral, siendo de aplicación en este caso el **art. 730 LECRIM**.

Los peritos podrán ser recusados en la fase intermedia, si se diera alguno de los motivos dispuestos en el **art. 723 LECRIM**. Posteriormente, aquellos que no hayan sido recusados responderán conjuntamente a las preguntas formuladas por las partes (**art. 724 LECRIM**). Dichas preguntas estarán relacionadas con el propio informe pericial, que contendrá, de manera general y según lo dispuesto en el **art. 478 LECRIM**:

1. Descripción del objeto del informe
2. Procedimiento y operaciones llevadas a cabo para la elaboración del informe
3. Conclusiones de los peritos, en base a los resultados del informe

Como se ha dicho, el contenido general de un informe pericial es el anteriormente referido, no obstante, si se desea, se podrá consultar el anexo C para ampliar información sobre la estructura y contenido del mismo.

Capítulo 7

La evidencia digital

ESTE capítulo irá dedicado, como su nombre indica, a la evidencia digital. Se establecerán una serie de analogías y similitudes entre ésta y la evidencia física. Se hablará también del proceso de recogida de la evidencia digital y de la documentación de dicho proceso, así como de la cadena de custodia, recalcando su importancia en el proceso penal español, describiéndola y enunciando una serie de características de la misma y hablando brevemente sobre la regulación legal que le aplica desde su inicio hasta su finalización y sobre el caso en que se produzca la rotura de la propia cadena.

7.1 Evidencia digital y evidencia física

Tradicionalmente, el concepto de evidencia ha sido asociado al de evidencia física o tradicional, sin embargo, con la aparición de las tecnologías de la información surgió también la evidencia digital, que puede ser también usada, al igual que la física, como medio de prueba en juicio [Ort08].

De esta manera, pueden establecerse ciertas analogías entre evidencias físicas y digitales, como por ejemplo: el correo ordinario y el electrónico, un documento en soporte material, como el papel y en soporte electrónico, como un documento en formato de *Microsoft Word*, etc.

Las evidencias digitales vienen contenidas en soportes físicos, por lo que se podría decir que una evidencia digital viene contenida en una evidencia física.

Como ventajas, la evidencia digital puede ser clonada, por lo que dicho clon podrá ser sometido a análisis y en caso de ser dañado o alterado, todavía se tendría la evidencia original.

Además, es más difícil que ésta sea destruida, ya que por ejemplo, un usuario sin demasiados conocimientos técnicos, creerá que simplemente con *«borrar»* un archivo, la evidencia de que éste ha existido se perderá. Sin embargo, puede llegar a ser posible recuperar los datos asociados a dicha evidencia mediante diversos métodos de recuperación, como los basados en **búsqueda de metadatos** asociados al archivo o mediante ***data carving***, consistente en buscar firmas de archivos, como se describió en la sección 4.2.2 del capítulo 4.

Como conclusión, podría decirse, tras una breve lectura a los párrafos anteriores, que tanto las evidencias digitales como las físicas comparten ciertas similitudes y que las acciones y operaciones que pueden realizarse sobre ambas son similares.

7.2 Recogida de la evidencia digital y documentación del proceso

La primera cosa a tener en cuenta en el momento de recogida de las evidencias digitales contenidas en los equipos informáticos relevantes para un caso determinado es que no se debe alterar el estado de ninguno de los elementos informáticos encontrados. Se trabajará en cambio, como ya se dijo en la sección anterior, con un clon de dichos elementos.

Se asegurará también la cadena de custodia, de manera que puedan asegurarse tanto la autenticidad como la integridad de las evidencias en el proceso penal. De la propia cadena de custodia se hablará más adelante, en la sección 7.3 de este mismo capítulo.

En la primera intervención, el perito deberá contemplar la escena en su totalidad, fijándose en el estado de cada elemento, como por ejemplo: equipos informáticos, discos duros, dispositivos USB, etc., incluyendo a las posibles personas que puedan encontrarse en dicha escena. También identificará al administrador de sistemas, en caso de necesitar apoyo técnico [ANT11].

Durante dicha intervención, se realizará un proceso de documentación de la misma, mediante fotografías de los elementos encontrados, la escritura del momento en el que se encontró cada uno de ellos en la escena y también se realizará un etiquetado de cada dispositivo con las correspondientes características:

- Equipo
- Marca
- Modelo
- Nº de serie

Tanto del proceso de recogida como del de documentación podrá el lector ampliar información, si lo desea, consultando la sección B.2 del anexo B. En dicha sección puede encontrarse también una serie de buenas prácticas a llevar a cabo durante todo el proceso forense.

7.3 Cadena de custodia

En esta sección se enunciará el concepto de cadena de custodia, al igual que una serie de características de ésta. Seguidamente se hablará sobre la regulación legal de la propia cadena de custodia durante los procedimientos de recogida, custodia y análisis de las evidencias y finalmente se hará una breve descripción del caso en el que se produzca una rotura de la misma.

7.3.1 Concepto y características

La cadena de custodia es un sistema formal, formado por el conjunto de actos que tienen cabida durante la recogida, traslado y custodia de las evidencias. Dichos actos se recogerán principalmente de manera documental, aunque también se podrán justificar de manera testimonial por aquellos que los llevaron a cabo [Ric13].

El objetivo de ésta consiste en dejar constancia de cada una de las actividades, relacionadas con el manejo de evidencias, que fueron realizadas por parte de cada una de las personas que tuvieron contacto con dichas evidencias, garantizando la trazabilidad de las mismas.

De esta forma se podrá garantizar que las evidencias son auténticas y permanecen inalteradas, minimizando así las posibilidades de que la prueba basada en estas evidencias sea declarada inválida en el proceso penal.

Se pueden citar una serie de características relacionadas con la cadena de custodia:

- Se establece una relación entre ésta y la prueba pericial (vista en la sección 6.5 del capítulo 6), ya que la propia cadena de custodia es la que garantiza que las evidencias analizadas son las mismas que las recogidas en la escena durante la investigación. Esto proporcionará validez a los resultados plasmados en el informe pericial
- Del punto anterior se obtiene que la cadena de custodia determina tanto la validez de la propia prueba, como la de su resultado, esto último indirectamente
- No afecta a la cadena de custodia el hecho de que hayan quedando evidencias en la escena tras una primera inspección. Este caso queda relacionado con la acreditación de autoría del delito

7.3.2 Regulación legal de la recogida, custodia y análisis de evidencias

La recogida, custodia y análisis de las evidencias se rigen por lo contenido en la LECRIM. No obstante, la regulación que se hace en dicho texto es imprecisa y deficiente. De este modo, se puede encontrar que se produce una mezcla de competencias del Juez y de la policía, de la misma forma que ocurría en el proceso probatorio dentro del proceso penal, como se pudo observar en las secciones 6.1.3, 6.1.4 y 6.1.5 del capítulo 6.

En la propia LECRIM se le otorga al Juez un importante rol, ya no solo como la persona encargada de resolver un conflicto legal entre las partes, sino también como individuo que puede participar en los propios actos de investigación, quedando incluida la recogida de evidencias, como puede leerse en gran cantidad de artículos a partir del 326. No obstante, aparte de que el Juez pueda presentarse en la escena, normalmente es la policía la que recoge las evidencias, según lo previsto en los **arts. 282** y **292 LECRIM**.

En las normas del procedimiento abreviado y del enjuiciamiento rápido se hace una regulación más apropiada: por un lado, el Juez de instrucción instruirá el procedimiento y dirigirá

la investigación, por otro, la policía recogerá todos los objetos útiles para la investigación de los hechos.

Dicho esto queda determinada la competencia para la recogida de evidencias, sin embargo, como se ha dicho anteriormente, la normativa contenida en la LECRIM no es suficiente para determinar como se ha de proceder de manera precisa en la recogida, custodia y envío de las evidencias al organismo adecuado, de forma que se garantice su integridad y por tanto, la validez de la prueba pericial. Algunos de los artículos referidos a esto último que se decía son el **326**, **330**, **334** y **338**.

Teniendo lo anterior en cuenta y mientras no se reforme el CP o la LECRIM para introducir una regulación adecuada de la cadena de custodia, en los tribunales se tendrán en cuenta unos requisitos a cumplir por la cadena de custodia acordes a normativa internacional.

7.3.3 Tratamiento de la rotura de la cadena de custodia

La falta de regulación referida en la sección anterior influye sobre el tratamiento que a las infracciones de la cadena de custodia se le da, ya que al no existir normas específicas a seguir, es difícil definir los requisitos a cumplirse durante el tratamiento de las evidencias.

De esta forma, se llega a una jurisprudencia en la que se distingue si la infracción es una irregularidad que es posible arreglar, o por el contrario puede producir la invalidez de la prueba. Es decir, realizar una irregularidad menor sobre la cadena de custodia no significa la automática nulidad de la prueba, sin embargo, si se cometiera una infracción que provocara una irregularidad mayor, la prueba no llegaría a ser valorada, ya que no puede asegurarse que dicha fuente de prueba sea auténtica.

La ausencia de algún documento relacionado con un acto referente al manejo de las evidencias sería un ejemplo de irregularidad leve y podría ser subsanado mediante la declaración de la persona que lo realizó. Por otra parte, la total falta de documentación sobre el manejo de evidencias sería considerado una irregularidad grave.

Las infracciones de la cadena de custodia deben impugnarse desde el mismo momento en que se sepa de ellas. La impugnación se puede hacer desde el inicio de la instrucción hasta el informe de conclusión definitiva.

En la impugnación se dejará constancia del momento en el que se cree que se produjo la infracción sobre la cadena de custodia, las normas que han sido infringidas y aquellas personas responsables de dicha infracción, argumentando por qué ésta convierte a la prueba en nula.

Capítulo 8

Extracción de evidencias digitales: casos de uso

Se realizará en este capítulo un pequeño despliegue del potencial de algunas de las herramientas descritas en el capítulo 4, construyendo unos pequeños casos de uso y mostrando el proceso de extracción de ciertas evidencias.

Se comenzará con la herramienta **Volatility Framework**, con la que se intentará obtener información de la memoria RAM en el momento de la adquisición, como por ejemplo procesos, servicios y conexiones activas, entre otros.

Se mostrará también la manera de realizar un clonado y un borrado seguro de un dispositivo de almacenamiento USB con **dd** y posteriormente el análisis de dicho dispositivo con **The Sleuth Kit**, mediante el cual se podrá conocer la estructura del sistema de particiones y también del sistema de archivos, así como los archivos y directorios, tanto activos como eliminados.

Finalmente, con **Dumpzilla** se obtendrá el historial de un usuario, la información que introdujo en formularios web y otros detalles de la actividad realizada por dicho usuario en una sesión web.

8.1 Volatility Framework

Los resultados para la demostración del uso de esta herramienta han sido obtenidos del análisis de dos imágenes de memoria RAM, llamadas *boomer-win2003-2006-03-17.img* y *jo-2009-11-19.mddramimage*, que han sido obtenidas de la web *Digital Forensics Tool Testing Images*[1] y de la wiki de Volatility, contenida en el grupo con nombre *NPS 2009-M57* y dentro de ese grupo, la imagen llamada *«jo»* del 19 de noviembre de 2009[2], respectivamente.

No obstante, podría también realizarse una adquisición manual de la memoria RAM. La forma más sencilla es mediante software, como por ejemplo Rekall Memory Forensic Framework (capítulo 4), Mandiant Memoryze[3], AccessData FTK Imager[4], etc. Existen también otros métodos, tanto software como hardware, e incluso una técnica denominada *«Cold boo-*

[1] http://dftt.sourceforge.net/test13/index.html
[2] http://digitalcorpora.org/corp/nps/scenarios/2009-m57-patents/ram/jo-2009-11-19.mddramimage.zip
[3] http://www.mandiant.com/resources/download/memoryze/
[4] http://accessdata.com/product-download/digital-forensics/ftk-imager-version-3.3.0

ting» o arranque en frío, que queda fuera del alcance de este trabajo y se recomienda al lector interesado consultar el artículo de *Grant Osborne* [Osb13] para mayor información sobre cada una de dichas técnicas.

Las evidencias extraídas mediante un análisis de la memoria pueden proporcionarnos información importante para detectar posible malware presente en el equipo analizado. Mediante la obtención de los procesos presentes en el momento de captura de la memoria pueden llegar a detectarse procesos ocultos, ejecutados por dicho malware. También mediante el estudio de las conexiones activas pueden conocerse indicios de la existencia de aplicaciones maliciosas. Con el mismo objetivo pueden examinarse las DLL, por si hubiera sido inyectada alguna DLL maliciosa. Estas son algunas de las posibles evidencias que podrían ser extraídas, útiles para realizar un informe final.

Los plugins usados han sido *imageinfo, pslist, pstree, connections, svcscan, consoles y notepad*, aunque existen multitud de ellos. Se han ejecutado los mismos plugins sobre cada una de las imágenes, a excepción de *notepad*, que fue ejecutado solo sobre la imagen *Boomer*, y de consoles, que fue ejecutado únicamente sobre la imagen *Jo*.

Para mostrar cuál sería el tipo de salida que proporcionarían los plugins que se han aplicado en común, será utilizada la imagen *Jo*, mientras que para los plugins *notepad* y *consoles* será utilizada la salida proporcionada por dichos plugins aplicados a la correspondiente imagen.

8.1.1 Plugin *imageinfo*

En la figura 8.1 se puede observar la salida proporcionada por dicho plugin, usado normalmente para conocer cierta información como el SO, el service pack del mismo, el tipo de arquitectura, etc.

En este caso, el plugin será utilizado para conocer el perfil que será cargado en los demás plugins citados anteriormente, mediante el parámetro `--profile=PROFILE`. Como se puede ver en la propia figura, se ha obtenido la recomendación de varios perfiles, pero si se echa un vistazo a `Image Type (Service Pack)`, nos podremos decantar finalmente por el perfil `WinXPSP3x86`.

8.1.2 Plugin *pslist*

Con *pslist* se puede observar una lista de procesos activos en el sistema, el resultado (figura 8.2) muestra atributos como el desplazamiento en la memoria, en este caso desplazamiento virtual (aunque puede mostrarse el físico con la opción `-P`), el nombre del proceso, los IDs del proceso y del proceso padre (columnas `PID` y `PPID` respectivamente), número de *threads* y *handles*, el ID de sesión, si el proceso es un proceso *Wow64* (usa un espacio de direcciones de 32 bits en un kernel de 64) y finalmente la fecha y la hora tanto de cuándo empezó, como de cuándo terminó el proceso.

```
$ volatility.exe -f jo-2009-11-19.mddramimage imageinfo

Determining profile based on KDBG search...

          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\Users\...\jo-2009-11-19.mddramimage)
                      PAE type : No PAE
                           DTB : 0x39000L
                          KDBG : 0x8054cde0L
        Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2009-11-20 00:01:50 UTC+0000
     Image local date and time : 2009-11-19 16:01:50 -0800
```

Figura 8.1: Salida del plugin *imageinfo*

```
$ volatility.exe -f jo-2009-11-19.mddramimage --profile=WinXPSP2x86 pslist

Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x82fc89c8 System                    4      0     59      531 ------      0
0x82eea0c8 smss.exe                824      4      3       19 ------      0 2009-11-19 01:17:57 UTC+0000
0x82d9ba40 csrss.exe               920    824     14      691      0      0 2009-11-19 01:17:59 UTC+0000
0x82ec1978 winlogon.exe            944    824     17      566      0      0 2009-11-19 01:18:00 UTC+0000
0x82c97c08 services.exe            988    944     18      270      0      0 2009-11-19 01:18:00 UTC+0000
0x82966da0 lsass.exe              1000    944     22      361      0      0 2009-11-19 01:18:00 UTC+0000
0x82ed7c20 svchost.exe            1172    988     19      196      0      0 2009-11-19 01:18:02 UTC+0000
0x82caada0 svchost.exe            1260    988      8      292      0      0 2009-11-19 01:18:02 UTC+0000
0x82d473e8 svchost.exe            1400    988     77     1566      0      0 2009-11-19 01:18:03 UTC+0000
0x82ee0390 avgchsvx.exe           1456    944     23      277      0      0 2009-11-19 01:18:03 UTC+0000
0x829125f8 avgrsx.exe             1464    944     28      244      0      0 2009-11-19 01:18:03 UTC+0000

[...]

0x826fd670 AVGIDSMonitor.e        3740   2876      3       35      0      0 2009-11-19 01:18:52 UTC+0000
0x827917b0 avgcsrvx.exe           3064   2140      7      171      0      0 2009-11-19 01:19:45 UTC+0000
0x82701c30 avgcmgr.exe            3712   1956      0 --------      0      0 2009-11-19 05:31:59 UTC+0000   2009-11-19 05:31:59 UTC+0000
0x827677d8 msimn.exe              3952    428     10      450      0      0 2009-11-19 17:07:20 UTC+0000
0x82daaa70 firefox.exe            2344    428     14      331      0      0 2009-11-19 17:08:47 UTC+0000
0x82d093d0 cmd.exe                1244    428      1       33      0      0 2009-11-19 17:10:30 UTC+0000
0x82cc4da0 avgsrmax.exe           3456   1956      0 --------      0      0 2009-11-19 20:03:34 UTC+0000   2009-11-19 20:03:34 UTC+0000
0x82f29020 python.exe              712   1244      1       79      0      0 2009-11-19 22:56:10 UTC+0000
0x827397e0 avgcmgr.exe            3036   1956      0 --------      0      0 2009-11-19 23:47:46 UTC+0000   2009-11-19 23:47:46 UTC+0000
0x82da4da0 cmd.exe                3660    428      1       33      0      0 2009-11-19 23:53:59 UTC+0000
0x8270c020 mdd_1.3.exe            3980   3660      1       24      0      0 2009-11-20 00:01:47 UTC+0000
```

Figura 8.2: Salida del plugin *pslist*

8.1.3 Plugin *pstree*

La salida de *pstree* (figura 8.3) proporciona la misma información que la del plugin *pslist*, pero en este caso se puede observar el listado en forma de árbol. Los procesos hijo se muestran indentados mediante puntos.

El desplazamiento mostrado aquí también es el virtual y se podría de igual forma conocer el físico mediante la opción `-P`, como en el caso de *pslist*.

8.1.4 Plugin *connections*

Este plugin muestra las conexiones activas en el momento de la adquisición de la memoria. Únicamente funciona con adquisiciones provenientes de Windows XP o Windows 2003 Server. La información obtenida puede observarse en la figura 8.4.

```
$ volatility.exe -f jo-2009-11-19.mddramimage --profile=WinXPSP2x86 pstree

Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x82fc89c8:System                                     4      0     59    531 1970-01-01 00:00:00 UTC+0000
. 0x82eea0c8:smss.exe                                824      4      3     19 2009-11-19 01:17:57 UTC+0000
.. 0x82d9ba40:csrss.exe                              920    824     14    691 2009-11-19 01:17:59 UTC+0000
.. 0x82ec1978:winlogon.exe                           944    824     17    566 2009-11-19 01:18:00 UTC+0000
... 0x82ee0390:avgchsvx.exe                         1456    944     23    277 2009-11-19 01:18:03 UTC+0000
... 0x82c97c08:services.exe                          988    944     18    270 2009-11-19 01:18:00 UTC+0000
.... 0x82dd2020:svchost.exe                         1536    988      5     81 2009-11-19 01:18:04 UTC+0000
.... 0x82964b28:spoolsv.exe                          264    988     10    105 2009-11-19 01:18:09 UTC+0000
.... 0x82ed7c20:svchost.exe                         1172    988     19    196 2009-11-19 01:18:02 UTC+0000
.... 0x82888da0:svchost.exe                         1432    988      4    105 2009-11-19 01:18:23 UTC+0000
.... 0x82f775b8:AVGIDSAgent.exe                      288    988     32    538 2009-11-19 01:18:09 UTC+0000
.... 0x829876a0:avgwdsvc.exe                        1956    988     43   1394 2009-11-19 01:18:23 UTC+0000
..... 0x82701c30:avgcmgr.exe                        3712   1956      0 ------ 2009-11-19 05:31:59 UTC+0000
..... 0x827e0980:avgnsx.exe                         2140   1956     25    333 2009-11-19 01:18:34 UTC+0000
...... 0x827917b0:avgcsrvx.exe                      3064   2140      7    171 2009-11-19 01:19:45 UTC+0000
..... 0x827f4020:avgam.exe                          2072   1956     15    292 2009-11-19 01:18:33 UTC+0000
..... 0x827397e0:avgcmgr.exe                        3036   1956      0 ------ 2009-11-19 23:47:46 UTC+0000

[...]
```

Figura 8.3: Salida del plugin *pstree*

```
$ volatility.exe -f jo-2009-11-19.mddramimage --profile=WinXPSP2x86 connections

Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------ ---
0x8283ae68 127.0.0.1:5152           127.0.0.1:1456           436
0x8275ee68 127.0.0.1:1459           127.0.0.1:1458           2344
0x828ea250 127.0.0.1:1455           127.0.0.1:1454           2344
0x82cf6728 127.0.0.1:1454           127.0.0.1:1455           2344
0x82d0a5a0 127.0.0.1:1458           127.0.0.1:1459           2344
0x8270ce68 127.0.0.1:4242           127.0.0.1:1723           2344
0x82e9ac48 127.0.0.1:1723           127.0.0.1:4242           712
0x8290ce68 192.168.1.102:1708       198.189.255.75:80        2912
0x82df7c00 192.168.1.102:1757       192.168.1.1:445          4
```

Figura 8.4: Salida del plugin *connections*

8.1.5 Plugin *svcscan*

Con *svcscan* se pueden conocer los servicios de Windows registrados en la imagen de memoria adquirida, mostrando información del tipo mostrado en la figura 8.5, en el que se puede ver el desplazamiento del proceso en la memoria, ID del proceso, nombre del servicio y nombre a mostrar, el tipo y el estado del servicio y la ruta para dicho servicio.

```
$ volatility.exe -f jo-2009-11-19.mddramimage --profile=WinXPSP2x86 svcscan

Offset: 0x382b58
Order: 24
Start: SERVICE_AUTO_START
Process ID: 1660
Service Name: avg9emc
Display Name: AVG E-mail Scanner
Service Type: SERVICE_WIN32_OWN_PROCESS
Service State: SERVICE_RUNNING
Binary Path: "C:\Program Files\AVG\AVG9\avgemc.exe"
```

Figura 8.5: Salida del plugin *svcscan*

8.1.6 Plugin *consoles*

Este interesante plugin proporciona el historial de comandos introducidos en *Símbolo del sistema* (cmd.exe). La información proporcionada se divide en 3 partes.

En primer lugar, el ejecutable lanzado desde *símbolo de sistema*, junto a la dirección de memoria en la que se encuentra esa ejecución y los procesos asociados (figura 8.6).

```
$ volatility.exe -f jo-2009-11-19.mddramimage --profile=WinXPSP2x86 consoles

**************************************************
ConsoleProcess: csrss.exe Pid: 920
Console: 0x1268ac8 CommandHistorySize: 50
HistoryBufferCount: 2 HistoryBufferMax: 4
OriginalTitle: Command Prompt
Title: Command Prompt - c:\Python26\python.exe patentauto.py
AttachedProcess: python.exe Pid: 712 Handle: 0x428
AttachedProcess: cmd.exe Pid: 1244 Handle: 0x918
----
CommandHistory: 0x1274e78 Application: python.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x428
----
CommandHistory: 0x4f4660 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 14 LastAdded: 13 LastDisplayed: 13
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x918
```

Figura 8.6: Salida del plugin *consoles*

En segundo lugar, la salida proporcionada muestra una lista de los comandos ejecutados (figura 8.7).

```
Cmd #0 at 0x1274c00: cd ..
Cmd #1 at 0x4f1f90: ls
Cmd #2 at 0x1268fd0: cd Desktop
Cmd #3 at 0x1274c90: dir
Cmd #4 at 0x1274ca0: cd Jo
Cmd #5 at 0x1274cb8: dir
Cmd #6 at 0x1274cc8: cd Desktop
Cmd #7 at 0x1274ce8: dir
Cmd #8 at 0x1274cf8: cd web
Cmd #9 at 0x1274d10: C:Python26\python.exe patentauto.py
Cmd #10 at 0x1274d60: c:Python26\python.exe patentauto.py
Cmd #11 at 0x1274db0: c: Python6\python.exe patentauto.py
Cmd #12 at 0x4f1fa0: c: Python26\python.exe patentauto.py
Cmd #13 at 0x1268d78: c:\Python26\python.exe patentauto.py
```

Figura 8.7: Salida del plugin *consoles*

Y finalmente, en la figura 8.8 se ve la salida por pantalla fruto de los comandos ejecuta-

dos.

```
Screen 0x1268dd0 X:80 Y:300
Dump:
http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetah
tml%2FPTO%2Fsearch-bool.html&r=18536.935597087522&f=G&l=50&co1=AND&d=PTXT&s1=qua
ntum&OS=quantum&RS=quantum
True
55.0711565345
content.location.href='http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect
2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=18536.935597087522&f=G&l=5
0&co1=AND&d=PTXT&s1=quantum&OS=quantum&RS=quantum'

[...]
```

Figura 8.8: Salida del plugin *consoles*

8.1.7 Plugin *notepad*

Como curiosidad, se detectó que en la máquina *Boomer* uno de los procesos activos era `notepad.exe` con PID 1568, correspondiente al bloc de notas de Windows, y precisamente este plugin que lleva el mismo nombre es capaz de mostrar el texto contenido en el bloc, como se puede ver en la figura 8.9.

```
$ volatility.exe -f boomer-win2003-2006-03-17.img --profile=Win2003SP0x86 notepad

Process: 1568
Text:
I am the very model of a modern major general.
```

Figura 8.9: Salida del plugin *notepad*

Y para finalizar la parte relativa a Volatility, se recomienda al lector ir a la propia web sobre referencia de comandos del proyecto[5] para mayor información.

8.2 Herramienta «dd»

En esta sección se mostrarán algunos de los posibles usos para dd, como por ejemplo el clonado bit a bit de un dispositivo de almacenamiento USB y como realizar un borrado seguro de cualquier tipo de medio de almacenamiento.

Como se trata una herramienta destinada a sistemas Linux en principio, se va a usar la distribución forense DEFT Linux, de la que se habló en la sección 4.1 del capítulo 4.

8.2.1 Clonado de dispositivo USB

En primer lugar, tras conectar el dispositivo USB que va a ser sometido al clonado, se ejecuta el comando `dmesg | grep sd` para conocer la letra que le ha sido asignada. Entre

[5] https://code.google.com/p/volatility/wiki/CommandReference23

la salida que nos proporciona el comando, podemos observar (figura 8.10) que el dispositivo tiene 1 GB de capacidad y que el sistema se va a referir a él como `sdb`.

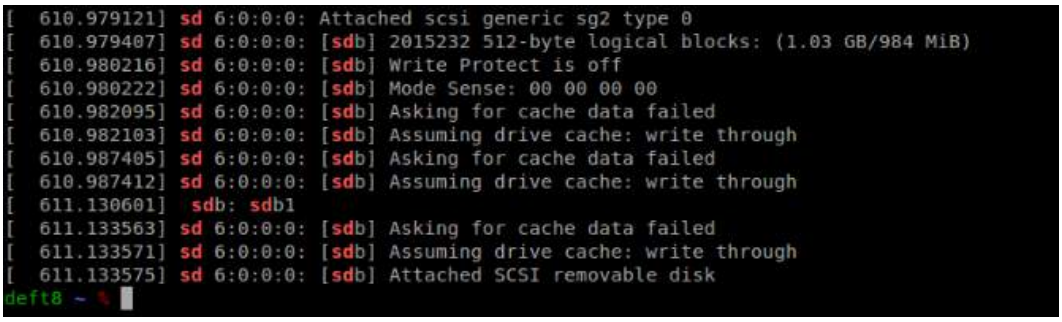

Figura 8.10: Salida del comando `dmesg`

Una vez hecho esto, se puede proceder al clonado. Para ello, se deberá calcular en primera instancia el valor *hash* del dispositivo, utilizando por ejemplo un algoritmo MD5. Esto se realiza en este caso con el comando `md5sum /dev/sdb`.

Después, el clonado propiamente dicho se realizará con un comando del tipo `dd if=/dev/sdb of=usb.dd bs=1M`. Como se puede ver se están usando tres opciones: `if`, que indica la ruta del archivo de entrada, que va a ser el `sdb`; `of`, similar a `if` pero del archivo de salida en este caso; finalmente `bs`, que indica el tamaño de bloque que `dd` leerá del archivo de entrada y que posteriormente escribirá en el archivo de salida. Se ha asignado un tamaño de bloque de 1 MB con el sufijo `M`, para consultar todos los sufijos disponibles y más información acerca del propio comando se recomienda leer su **man page**.

Una vez realizado el proceso de clonado, se comprobará el *hash* del archivo `usb.dd` resultante, de modo que podrá comprobarse si el clon obtenido mantiene la integridad. Si el *hash* que se obtuvo antes del clonado y éste coinciden, la integridad se ha mantenido. Todo esto puede verse en la figura 8.11.

Como detalle a resaltar, se puede observar que la salida nos proporciona un par de líneas que dicen:

```
984+0 registros leídos
984+0 registros escritos
```

Lo que estas líneas indican es que 984 bloques de 1 MB han sido leídos y posteriormente escritos, del dispositivo al archivo de salida, respectivamente.

8.2.2 Borrado seguro de un dispositivo de almacenamiento

Si deseamos borrar de forma segura un dispositivo de almacenamiento con dd, tenemos varias opciones. La primera sería llenando todo el dispositivo de ceros.

Figura 8.11: Clonado y comprobación de integridad

Por ejemplo, si se deseara hacer un borrado seguro del USB usado en la sección anterior, el comando a utilizar sería:

```
dd if=/dev/zero of=/dev/sdb bs=1M
```

De forma alternativa y para complicar un poco más el proceso de la posible recuperación de datos, se puede sobrescribir el dispositivo con patrones de datos aleatorios:

```
dd if=/dev/urandom of=/dev/sdb bs=1M
```

8.3 Análisis de un dispositivo USB con The Sleuth Kit

En esta sección se realizará un análisis del sistema de particiones y del sistema de archivos del dispositivo USB usado en las secciones anteriores. Antes de nada, se definirá el término *metadatos*, para mejor comprensión del texto posterior y se mencionará la importancia de los mismos.

Los metadatos son a su vez datos que describen datos. Contienen datos que describen un archivo, incluyendo información sobre la ubicación del mismo, su tamaño y datos temporales sobre su creación, modificación o último acceso al mismo. De este modo, se pueden conocer detalles de dicho archivo, o realizar búsquedas que se rijan por un criterio determinado, como por ejemplo los archivos creados en un cierto rango de tiempo.

8.3.1 Análisis del sistema de particiones

Para realizar el análisis del sistema de particiones se ha utilizado la herramienta `mmls` contenida en TSK. La salida proporcionada por esta herramienta se puede ver en la figura 8.12.

El análisis del sistema de particiones es importante para conocer la disposición de las mismas, ya que no siempre los sectores deben de estar necesariamente asignados a una partición, pudiendo contener información oculta, información de una instalación anterior, o incluso ceros, como se vio en la sección anterior de borrado seguro. Por ejemplo en el caso que nos concierne, los primeros 63 sectores antes de la partición se encuentran no asignados.

Los datos proporcionados se dividen en varias columnas, la columna `Slot` contiene una entrada `Meta` que indica donde se encuentran las estructuras de metadatos y una entrada `00:00`, este formato de cuatro dígitos separados en pares es el utilizado por aquellos sistemas de particiones que pueden tener varias tablas. En este caso, los dos dígitos de la izquierda indican el ID de la tabla de particiones #0, y los dos de la derecha la entrada en dicha tabla, es decir, según la imagen, la entrada 0 en la tabla de particiones 0.

También se muestran los sectores de inicio (`Start`) y de fin (`End`), la longitud de cada área (`Length`) en sectores de 512 bytes y una pequeña descripción (`Description`).

```
deft8 ~ % mmls -t dos usb.dd
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

     Slot    Start        End          Length       Description
00:  Meta    0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----   0000000000   0000000062   0000000063   Unallocated
02:  00:00   0000000063   0002015231   0002015169   Win95 FAT32 (0x0b)
deft8 ~ %
```

Figura 8.12: Salida de la herramienta `mmls`

Como se puede observar en la anterior figura, el dispositivo se encuentra formateado en FAT32. El primer sector contiene la tabla de particiones. La partición FAT32 tiene un tamaño de 2015169 sectores, que corresponden de manera aproximada a 1 GB, que es la capacidad del dispositivo. Esta partición viene precedida por un espacio sin asignar de 63 sectores (aprox. 32 KB).

8.3.2 Análisis del sistema de archivos

Para el análisis del sistema de archivos serán usadas varias de las herramientas contenidas en `TSK`, como `fsstat`, que muestra detalles generales del sistema de archivos y `fls`, que muestra los nombres de archivo y de directorio del mismo.

En el caso del análisis del sistema de archivos, la información que nos proporcionará será importante por ejemplo para recuperar datos a mano, ya que nos muestra información sobre la propia disposición del sistema de archivos. Se podría ocultar información a este nivel entre el final del sistema de archivos y el final del volumen en que éste se halle contenido. Este espacio es denominado *volume slack* [Car05c].

En el primer caso, la herramienta `fsstat`, a la que le indicaremos el desplazamiento en sectores hasta el comienzo del sistema de archivos en la imagen con la opción `-o`, nos muestra una serie de información, de la que explicaremos sus diferentes partes en las posteriores figuras.

En la figura 8.13 se puede observar la primera parte de la información arrojada por la herramienta, en la que se ve la disposición del sistema de archivos.

```
deft8 ~ % fsstat -o 63 usb.dd
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: FAT32

OEM Name: MSDOS5.0
Volume ID: 0x18354d3a
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory): JUANMI
File System Type Label: FAT32
Next Free Sector (FS Info): 220112
Free Sector Count (FS Info): 58920

Sectors before file system: 63

File System Layout (in sectors)
Total Range: 0 - 2015168
* Reserved: 0 - 4271
** Boot Sector: 0
** FS Info Sector: 1
** Backup Boot Sector: 6
* FAT 0: 4272 - 6231
* FAT 1: 6232 - 8191
* Data Area: 8192 - 2015168
** Cluster Area: 8192 - 2015167
*** Root Directory: 8192 - 1737079
** Non-clustered: 2015168 - 2015168
```

Figura 8.13: Información sobre el sistema de archivos

Se puede ver que existe un total de 2015169 (`Total Range: 0 - 2015168`) sectores en el sistema de archivos, de los cuales del 0 al 4271 están reservados, después se pueden ver el rango sectores que ocupan las FAT 0 y 1 (la primaria y la de backup) y el área de datos.

La segunda parte de la información proporcionada por esta herramienta se corresponde con información de metadatos e información de contenido (figura 8.14).

En este caso el rango válido de sectores asignados a estructuras de metadatos va del 2 al 32111638, con directorio raíz en el sector 2.

La información relacionada con el contenido indica el tamaño del sector y del cluster y el rango total de clusters. En este caso, un cluster estaría formado por 8 sectores (4096/512 = 8).

La última parte de la información proporcionada es una representación en forma de texto de los contenidos de la FAT, en forma de cadenas de clusters, o *cluster runs*. La FAT contiene punteros a los siguientes clusters de archivo, es decir, si a un archivo se le pueden asignar

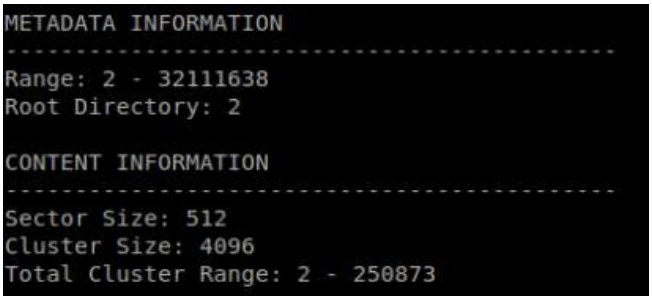

Figura 8.14: Información sobre metadatos y contenido

clusters consecutivos, el puntero será a `EOF`, de lo contrario, el puntero será a otro cluster, teniendo siempre en cuenta que los resultados se muestran en sectores (figura 8.15).

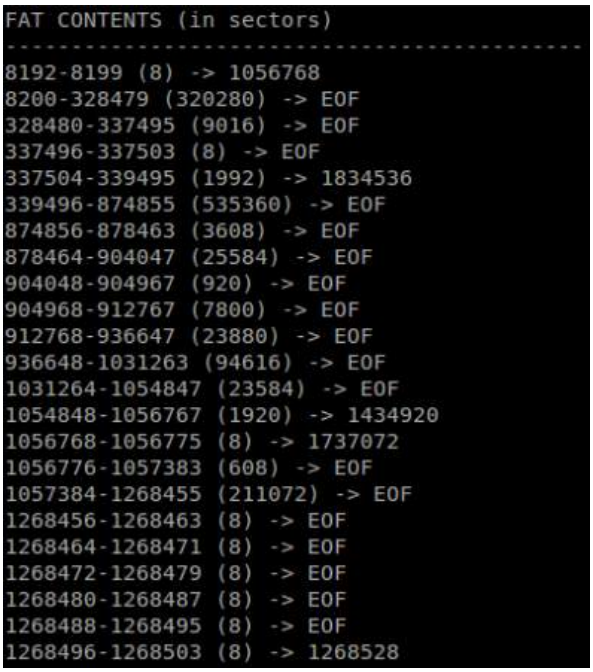

Figura 8.15: Representación de la FAT

Por ejemplo, en la primera línea se observa que a un archivo se le ha asignado un primer cluster, que comprende los sectores del 8192 al 8199, como no ha sido posible asignarle clusters consecutivos, se dirige el puntero hacia otro cluster que comienza en el sector 1056768, etc.

En la segunda línea se puede ver cómo a un archivo se le han asignado 320280 sectores (correspondientes a 40035 clusters) y el puntero apunta hacia `EOF`, esto quiere decir que no apunta hacia ningún otro cluster y el archivo termina ahí.

En la segunda parte de este análisis se va a utilizar `fls`, a la que le indicaremos de igual forma el desplazamiento en sectores hasta el comienzo del sistema de archivos en la imagen

con la opción `-o` y aparte también se usarán distintas opciones según el propósito.

En el primer caso se usarán las opciones `-u` y `-r`, con las que serán mostrados los archivos y directorios activos, éstos últimos de forma recursiva, como se puede observar en la figura 8.16, que muestra una pequeña porción de la salida mostrada por la herramienta con las opciones anteriormente citadas.

```
deft8 ~ % fls -o 63 -ur usb.dd
d/d 4:  IMMORTAL TABS
+ r/r 27474695: all_shall_fall.gp5
+ r/r 27474700: Immortal - A Sign For The Norse Hordes To Ride.gp4
+ r/r 27474704: Immortal - At The Heart Of Winter.gtp
+ r/r 27474708: Immortal - Battles In the North.gp3
+ r/r 27474713: Immortal - Blashyrkh (mighty Ravendark) (3).gp4
+ r/r 27474717: Immortal - Blizzard Beast.gp4
+ r/r 27474721: Immortal - Damned In Black.gtp
+ r/r 27474726: Immortal - Grim And Frosbitten Kingdom.gp4
+ r/r 27474730: Immortal - In My Kingdom Cold.gp4
+ r/r 27474734: Immortal - Mountains Of Might.gp4
+ r/r 27474738: Immortal - My Dimension.gp4
+ r/r 27474741: Immortal - One By One.gp4
+ r/r 27474745: Immortal - Pure Holocaust.gp4
+ r/r 27474748: Immortal - Solarfall.gtp
+ r/r 27474753: Immortal - Sons Of Northern Darkness.gp4
```

Figura 8.16: Archivos y directorios activos

Se puede ver en la primera línea que existe un directorio, indicado por `d/d`, con múltiples archivos normales (*regular files*) indicados por `r/r` e indentados con un símbolo `+`. Los números mostrados son los correspondientes a los inodos de los archivos.

En el segundo caso se usarán las opciones `-d`, `-p` y `-r` (figura 8.17), que mostrarán esta vez solo las entradas eliminadas, con su ruta completa y de forma recursiva.

```
deft8 ~ % fls -o 63 -dpr usb.dd
d/d * 25:       _005046_
r/r * 5268871:  Davidian/Davidian-Untitled (2).mp3
r/r * 5268874:  Davidian/Davidian-Untitled (2).mp3
r/r * 77:       _ERRYC~1.GP3
r/r * 116:      _ALORE~1.DOC
r/r * 120:      __rar_11.4750
r/r * 127:      _ractica.doc
r/r * 21562887: HOMEBREWS/GuitarHelperV05BCF.rar
r/r * 21562897: HOMEBREWS/UniversalGoMessengerCFplusv104.rar
r/r * 20167331: TORTURE KILLER TABS/torture_killer_sadistic.gp5
r/r * 16777251: Distortions.zip
```

Figura 8.17: Archivos y directorios eliminados

La salida es similar a la contemplada en el caso anterior, aunque puede verse el `*` en cada línea mostrada, que es el símbolo que indica que el archivo está eliminado.

8.4 Análisis de Mozilla Firefox con Dumpzilla

Para mostrar el funcionamiento de la herramienta Dumpzilla, se trabajará sobre la información proporcionada por la misma, en base a un pequeño caso de uso en el que el usuario ha accedido y creado una cuenta de correo en Gmail [6]. Así, se podrá ver un ejemplo mínimo de la información que puede llegar a obtenerse de un navegador web.

En el caso del análisis de navegadores web, es más fácil intuir la utilidad que nos van a proporcionar las evidencias obtenidas a partir de éste, que nos darán información sobre datos personales, conversaciones, correos, etc., que en ciertos casos nos será útil de cara a reconstruir ciertos delitos como por ejemplo un caso de robo de información.

8.4.1 Observación del historial con filtrado por url

Como se ha dicho, se sabe que el usuario ha accedido a Gmail y ha creado una cuenta. Esto se puede comprobar, tras indicar en el comando la localización de la directorio donde se encuentra el perfil de Firefox que va a ser analizado, mediante la opción `--History` y filtrando por url también con la opción `-url mail.google.com`.

El resultado de este comando nos proporciona, entre otras cosas, la fecha y hora de las últimas visitas realizadas a páginas web. En el caso que nos concierne, se puede ver, tal y como se muestra en la figura 8.18 una visita a la página de creación de cuenta del servicio de correo electrónico de Google. Posteriormente, parece que el servicio de red social de Google (Google+) ha solicitado al usuario configurar un perfil en el mismo. Por último, se puede ver como el usuario ha realizado el proceso de *login* correctamente y ha accedido a la bandeja de entrada del correo.

```
$ dumpzilla ~/.mozilla/firefox/XXXXX.default/ --History -url mail.google.com

================================================================================================
History              [SHA256 hash: edde893333b91c42225e64454dba7357a0888319c4442afbdb48d5b654d33c07]
================================================================================================
Last visit: 2015-05-18 01:58:47
Title: Crea tu cuenta de Google
URL: https://accounts.google.com/SignUp?service=mail&hl=es&continue=http%3A%2F%2Fmail.google.com%2Fm ...
Frequency: 1

Last visit: 2015-05-18 02:01:06
Title: Configurar tu perfil
URL: https://plus.google.com/up/accounts/?hl=es&service=mail&continue=http://mail.google.com/mail/?p ...
Frequency: 1

Last visit: 2015-05-18 02:01:14
Title: Cuentas de Google
URL: https://accounts.google.com/SignUpDone?hl=es&continue=http%3A%2F%2Fmail.google.com%2Fmail%2F%3F ...
Frequency: 1

Last visit: 2015-05-18 02:02:18
Title: Recibidos (3) - john.doe.tfg@gmail.com - Gmail
URL: https://mail.google.com/mail/#inbox
Frequency: 1
```

Figura 8.18: Dumpzilla con la opción `--History`

[6] www.gmail.com

Se puede apreciar también que el usuario se ha registrado con el nombre de usuario `john.doe.tfg@gmail.com`

8.4.2 Inspección de información introducida en formularios

Como el lector sabrá, al registrar una cuenta de correo electrónico, normalmente se suelen solicitar una serie de datos personales, que son introducidos por el usuario en formularios web, por tanto, se va a intentar obtener dicha información, esta vez utilizando la opción `--Forms` y además, teniendo en cuenta la información temporal visualizada en el historial.

De esta forma, se acortará el rango de tiempo desde las `00:30` del 18 de Mayo de 2015, hasta las `02:30` del mismo día con la opción `-range_forms "2015-05-18 00:30:00" "2015-05-18 02:30:00"`, pudiendo así observar únicamente los datos introducidos en formularios en ese período de tiempo (figura 8.19).

```
$ dumpzilla ~/.mozilla/firefox/XXXXX.default/ --Forms -range_forms "2015-05-18 00:30:00" "2015-05-18 02:30:00"

================================================================================================
Forms               [SHA256 hash: 0ad252233197df8efd322266fc1cdbdea4868ad9788ce71e723b8f104ab2a592]
================================================================================================
Name: FirstName
Value: John
Times Used: 1
First Used: 2015-05-18 02:00:58
LastUsed: 2015-05-18 02:00:58

Name: LastName
Value: Doe
Times Used: 1
First Used: 2015-05-18 02:00:58
LastUsed: 2015-05-18 02:00:58

Name: BirthDay
Value: 03
Times Used: 1
First Used: 2015-05-18 02:00:58
LastUsed: 2015-05-18 02:00:58

Name: BirthYear
Value: 1923
Times Used: 1
First Used: 2015-05-18 02:00:58
LastUsed: 2015-05-18 02:00:58
```

Figura 8.19: Dumpzilla con la opción `--Forms`

Según la observado en dicha figura, parece ser que los formularios corresponden al registro de la cuenta de correo, pudiendo deducirse que el nombre (real o no) del usuario es `John Doe`, según los formularios `FirstName` y `LastName`. También se muestran el día y año de nacimiento (formularios `BirthDay` y `BirthYear`).

8.4.3 Actividad realizada por el usuario durante la sesión

Antes de finalizar el análisis, se intentará sacar algo más de información sobre los movimientos del usuario antes de cerrar Firefox con la opción `--Session`, que muestra datos sobre la última y la penúltima sesión. Puede verse el resultado de este comando en la figura 8.20.

```
$ dumpzilla ~/.mozilla/firefox/XXXXX.default/ --Session

================================================================================================
Session             [SHA256 hash: 3378674f1464212e5207a692b6b3c8c96f9a8666336540a243f5385f70617bb1]
================================================================================================
Last update Mon May 18 02:03:25 2015:

Title: Recibidos (3) - john.doe.tfg@gmail.com - Gmail
URL: https://mail.google.com/mail/?pli=1#inbox
Form: {u'hist_state': u'inbox'}

================================================================================================
Backup session      [SHA256 hash: d699289dac4b26624242f809b31c041879394b29c5f84b494daa52001b1e1e50]
================================================================================================
Last update Mon May 18 02:01:57 2015:

Title: Cuentas de Google
URL: https://accounts.google.com/SignUpDone?hl=es&continue=http%3A%2F%2Fmail.google.com%2Fmail%2F%3Fp
c%3Dtopnav-about-es%26hl%3Des&service=mail&dsh=920400702268826176
Referrer: https://plus.google.com/up/accounts/?hl=es&service=mail&continue=http://mail.google.com/mail/
?pc%3Dtopnav-about-es&fvi=8o2EVI_akMoaFJZF3lO039t1koHJmgI&dsh=9204007022688261 76&srs=AFk7yJUHdDEOsufOVT
6dqAJLKLdnhWMaF86-mmZqQK4k_RS6W_tU5s3TE2kRX_Kyt65Y3x7xH-J7hreIYQmyawzHOE2IklzCPQ&ndt=1
```

Figura 8.20: Dumpzilla con la opción `--Session`

Y como puede verse en la propia figura, lo único que hizo el usuario en la última sesión fue visitar la bandeja de entrada de su cuenta de correo.

En la penúltima sesión, como se muestra en `Backup session`, parece que el usuario únicamente omitió el paso de crear un perfil en Google+. Damos aquí por finalizado este pequeño ejemplo de uso de la herramienta Dumpzilla.

Capítulo 9

Metodología propuesta

CON la redacción de este capítulo se pretende aportar una metodología completa que englobe todos los aspectos a considerar en cada fase para abordar un análisis forense y el posterior procedimiento de elaboración de un informe pericial. Dichos aspectos serán tanto técnicos: herramientas a utilizar durante el proceso de adquisición y análisis, como jurídicos: aquellos que irán destinados a satisfacer el cumplimiento de la legislación española vigente y también aquellos relacionados con la evidencia digital, de manera que se mantenga su integridad y no pierdan su validez y confiabilidad, evitando así la posible inhabilitación de la prueba en un proceso judicial. Todo lo anteriormente mencionado hará que finalmente el informe resultante pueda ser esgrimido como medio de prueba en juicio.

Cabe recordar que esta metodología tomará como base el modelo contenido en la norma UNE 71506:2013, descrita en la sección 5.2 del capítulo 5 y en la sección B.2 del anexo B, a su vez, dicha norma contiene la UNE 197001:2011, relacionada con la elaboración de informes periciales y abordada en el anexo C. No obstante, se recalca que la metodología propuesta en este capítulo es una unificación fruto de complementar a las previamente citadas con todos los aspectos mencionados anteriormente.

9.1 Preservación

En esta etapa lo que se proponía originalmente era mantener la validez y la confiabilidad de las evidencias originales, realizando los técnicos que tienen el primer contacto con las evidencias el almacenaje en soportes adecuados, como por ejemplo bolsas antiestáticas, soportes estancos que eviten interferencias y llevando la indumentaria adecuada para no ocasionar daños en las evidencias por descargas electrostáticas, como pulseras antiestáticas y en definitiva mantener seguras las evidencias hasta el final del proceso pericial.

Para mantener la integridad de las evidencias habrá que completar lo establecido en la norma con las siguientes garantías:

- No se alterará el estado en el que se encontraron las evidencias.
- Se comenzará etiquetando y fotografiando los dispositivos que serán sometidos a análisis, indicando: equipo, marca, modelo, número de serie y código de evidencia, relativo a la parte de etiquetado y que será el identificador único de dicha evidencia.

- Se garantizará la integridad mediante el mecanismo de cadena de custodia, abordado en la sección 7.3 del capítulo 7, donde se tratarán los aspectos legales aparejados a la misma.

- Se hará una distinción entre evidencia física y evidencia digital para seleccionar aquella de nuestro interés, así tendremos por ejemplo un disco duro, con todo su contenido; en este supuesto el contenido del disco es la evidencia digital de interés, contenida en la evidencia física, que es el disco duro. Del mismo modo, se podría tener un correo electrónico impreso en papel, y el correo electrónico original, que es la evidencia digital que nos interesa.

9.2 Adquisición

Se respetará lo propuesto originalmente en la norma, que como ya se dijo anteriormente, se ve en profundidad en la sección B.2 del anexo B. El propósito principal de esta etapa era adquirir un clonado a bajo nivel de las evidencias digitales.

Lo establecido en la norma debe completarse con las siguientes consideraciones:

- En primer lugar, el uso de una distribución forense de las descritas en el capítulo 4, en la sección 4.1, que como se sabe por la lectura de dicho capítulo contienen mecanismos que evitan la modificación accidental de los datos.

- Contenidas en dichas distribuciones se encuentra una de las herramientas más populares y útiles para el clonado de dispositivos de almacenamiento, la herramienta software `dd`, de la que se mostraron algunos de sus usos en la sección 8.2 del capítulo 8. Se pueden usar también cualquiera de las herramientas propuestas en la sección 4.2.4, también perteneciente al capítulo 4.

- En el caso particular de dispositivos móviles, pueden usarse las herramientas software propuestas en la sección 4.2.6 de dicho capítulo.

- Para los dos casos anteriores, también pueden usarse las herramientas hardware descritas en la sección 4.3.

- Con el fin de garantizar la integridad de los clonados resultantes de esta fase, deberá calcularse el *hash* del archivo resultante de cada clonado realizado, bien con la herramienta HashMyFiles para Windows descrita en la sección 4.2.2 o algunas de las contenidas en las distribuciones forenses GNU/Linux, como por ejemplo `md5sum`.

- Se continuará respetando la integridad de las evidencias plasmando cada uno de los procesos realizados en la cadena de custodia.

9.3 Documentación

En esta etapa, el objetivo es documentar el procedimiento al completo, desde el inicio del análisis hasta la emisión del informe pericial. Se documentará cada proceso llevado a cabo y qué herramientas fueron utilizadas.

Como aportación complementaria, se va a proponer lo siguiente:

- Como ya se viene repitiendo a lo largo de todo el proceso, se aportará trazabilidad al análisis forense mediante la cadena de custodia, cuya regulación legal está contenida en la sección 7.3, como se dijo anteriormente.
- Para facilitar la elaboración de ésta, se propondrá el siguiente contenido básico:
  - Identificador del caso: referencia identificativa del caso forense.
  - Tipo de incidente: pequeña descripción del caso.
  - Empresa afectada.
  - Dirección y teléfono de la empresa.
  - Fecha y hora de apertura de la cadena de custodia.
  - Nombre y apellidos del investigador.
  - Observaciones: las que sean necesarias, como por ejemplo quién recolectó la evidencia, el estado de dicha evidencia y qué procesos le fueron aplicados, el nombre del notario o fedatario público que estuvo presente durante la recogida de la evidencia si se tratara de un proceso penal.
  - Listado de evidencias: se debe dar el código de evidencia, la cantidad que se requisó de cada una de éstas y la descripción del artículo.
- Las herramientas utilizadas durante el análisis dependerán del tipo de dato a analizar, por tanto, se remite de nuevo al lector al listado de herramientas que fueron descritas en el capítulo 4.
- Tras el análisis, el documento resultante será el informe pericial, cuya regulación legal puede verse en el capítulo 6 y más concretamente en la sección 6.5.
- Para la elaboración del mismo se tendrá en cuenta la norma UNE 197001:2011 (anexo C), pero aplicada a aspectos informáticos, dentro del informe se hace referencia a los artículos 343 y 335.2 de la LEC para hacer la declaración de tachas y el juramento.
- Los apartados básicos serán: declaración de tachas y juramento, asunto del informe, evidencias recibidas, estudios efectuados sobre las evidencias, conclusiones y finalmente anexos, en los que se dejará constancia de toda aquella información que se crea necesaria.

9.4 Análisis

Esta fase, originalmente propone como objetivo la aplicación de una serie de procesos y tareas sobre las evidencias de las que se disponen para dar respuesta a las preguntas relacionadas con el incidente que causó el inicio de la investigación. Aquí, el tipo de análisis a realizar dependerá del tipo de incidente.

De nuevo, será necesario completar esta etapa con los siguientes de puntos:

- La elección de las herramientas a usar durante la fase actual, que dependerán del tipo de dato sujeto a análisis. Se remite nuevamente al lector al listado de herramientas del capítulo 4.
- Se volverán a tener en cuenta las consideraciones relacionadas con la evidencia digital citadas anteriormente.
- Los aspectos relacionados con la cadena de custodia, que será el elemento común durante todo el procedimiento.

9.5 Presentación

En esta fase final, se habrá obtenido el informe pericial resultante de todo el procedimiento llevado a cabo, con un lenguaje comprensible para un público no técnico y que se remitirá finalmente al solicitante de la pericial. Serán remitidos también al mismo los equipos y dispositivos que fueron sometidos a análisis, dando por finalizado el proceso.

Como proposiciones para complementar la norma original habrá de tenerse en cuenta lo siguiente:

- El informe final resultado del proceso de análisis será un documento cuya estructura deberá responder a la ya descrita anteriormente y concretada en el ejemplo del Anexo G, a saber:
  - Datos identificativos del informe (Identificador, nombre del perito, solicitante y fecha de emisión)
  - Declaración de tachas y juramento
  - Asunto
  - Evidencias recibidas
  - Estudios efectuados sobre las evidencias
  - Situación final de las evidencias
  - Conclusiones
  - Anexos (Notas internas sobre los análisis realizados)
- Las regulaciones legales y normativas asociadas al mismo. Teniendo en cuenta en esta etapa que el perito podrá ser llamado, durante la fase de juicio oral, a defender el informe emitido considerado éste como prueba anticipada. La obligación de comparecer

a la defensa del informe pericial está contemplada en la LECRIM, estableciendo multas económicas e incluso la posibilidad de ser procesado por delito de obstrucción a la justicia al perito que incumpliera dicha obligación.

Capítulo 10

Análisis forense de un caso ficticio

ESTE capítulo pretende ser el culmen del trabajo que comenzó al principio de este documento. En él se analizará un caso ficticio desde el principio hasta al final, siguiendo la metodología propuesta en las normas UNE 71506:2013 y UNE 197001:2011, abordadas en los anexos B y C, correspondientes a la metodología a seguir para el análisis forense de evidencias electrónicas y la elaboración del correspondiente informe pericial, respectivamente.

10.1 Escenario

El 29 de Mayo de 2015, Juan Carlos Pérez, de la ESI (Escuela Superior de Informática), situada en el campus de Ciudad Real de la UCLM, contacta con nuestro laboratorio forense para someter a análisis un ordenador portátil de empresa perteneciente a María José Santana, empleada recientemente despedida por la supuesta utilización de un período de baja laboral comprendido del 1 al 5 de Abril de 2015 para realizar un viaje de ocio. Ella alega que dicha afirmación es falsa y ha amenazado con demandar por motivo de despido improcedente, sin embargo, su compañera Aurora Vargas comunicó que ella misma vio una foto en el ordenador de María José en la que aparecía ésta última en su destino vacacional.

El uso de dicho portátil comprendía tanto las tareas propias del trabajo como un uso personal y se sabe que el sistema operativo utilizado habitualmente era una versión de Windows. El equipo se encuentra actualmente en las dependencias de la UCLM, apagado.

10.2 Preservación

Esta etapa representa el inicio del proceso. Se comenzará etiquetando y fotografiando todos los dispositivos que serán posteriormente sometidos a análisis. En este caso se han obtenido los siguientes elementos (figuras 10.1 y 10.2):

- **Equipo:** Ordenador portátil
- **Marca:** Dell
- **Modelo/nº:** Latitude E4300/PP13S
- **Nº de serie:** 5G1J64J

- **Código de evidencia (etiqueta):** PC20150530

Figura 10.1: Evidencia PC20150530

- **Equipo:** Disco duro interno SATA 2.5"250 GB
- **Marca:** Fujitsu
- **Modelo/nº:** MHZ2250BJ FFS G2
- **Nº de serie:** K83ET8C263NL
- **Código de evidencia (etiqueta):** HD20150530

Figura 10.2: Evidencia HD20150530

10.3 Adquisición

Una vez etiquetados y fotografiados los dispositivos, en este caso únicamente el portátil apagado con su disco duro interno, se procederá a realizar un clonado a bajo nivel de éste, siguiendo un procedimiento documentado.

Esta documentación podrá consultarse en los anexos F y G, correspondientes a la cadena de custodia de los dispositivos y al propio informe pericial resultante.

Para realizar el clonado se utilizará la herramienta dd, dentro de la distribución DEFT, siguiendo un procedimiento similar al observado en la sección 8.2 del capítulo 8. Pero primeramente se deberá extraer el disco duro del portátil y conectarlo a una *docking station*, para de este modo acceder a él desde DEFT como si se tratara de una unidad externa.

10.4 Documentación

Se documentará todo el procedimiento desde el inicio del análisis hasta que éste finaliza. En dicha documentación se indicarán los procedimientos y herramientas usadas, de modo que al final contaremos con una serie de documentos:

- Cadena de custodia (en el anexo F)
- Informe pericial (anexo G)

Para construir el documento de cadena de custodia se ha seguido la plantilla propuesta en *Guía de toma de evidencias en entornos Windows*, del INCIBE (Instituto Nacional de Ciberseguridad) [Mar14].

10.5 Análisis

Aquí se llevarán a cabo sobre el disco duro que obtuvimos una serie de procedimientos con los que se tratará de dar respuesta a cuestiones sobre el origen del incidente, qué métodos fueron usados, etc. En el caso que nos concierne, los objetos de interés son evidencias gráficas, como por ejemplo una fotografía. Los tipos de análisis que van a ser realizados serán los siguientes:

- Análisis de la papelera de reciclaje, en busca de alguna posible evidencia contenida en la misma
- Análisis del sistema de archivos, ante la posible existencia de evidencias no eliminadas
- Recuperación de archivos eliminados, igualmente en busca de posibles evidencias

Como nuestro objetivo es algún documento fotográfico que ayude a esclarecer el motivo del incidente, si llegara a encontrarse algún documento interesante:

- Análisis de los metadatos de la imagen
- Análisis de la imagen digital

10.6 Presentación

Para finalizar, en esta etapa se plasmarán los resultados obtenidos durante el análisis de las evidencias en el informe pericial que como ya se dijo, podrá leerse en el anexo G. Dicho informe será remitido al solicitante.

10.7 Estimación de costes

Para realizar una estimación de los costes que tendrá la elaboración del presente informe pericial tendremos en cuenta cada visita al juzgado (al menos 3), al escenario de los hechos, horas de redacción del informe, encuadernación, etc.

- **Desplazamiento del perito al juzgado de Ciudad Real:** 36 km. ida + 36 km. vuelta = 72 km. x 3 veces = 216 km. Teniendo en cuenta que el consumo del vehículo son 10 L por cada 100 km., en los 216 km. se consumen 21.6 L de gasolina 95 x 1,359 €/L = **30** €. aprox.
- **Desplazamiento del perito a juicio:** 36 km. ida + 36 km. vuelta = 72 km., correspondientes a un consumo de gasolina de 7.2 L x 1,359 €/L = **10** € aprox.
- **Desplazamiento del perito al escenario de los hechos:** 38 km. ida + 38 km. vuelta = 76 km., correspondientes a un consumo de gasolina de 7.6 L x 1,359 €/L = **10** € aprox.
- **Elaboración del informe:** del 30 de Mayo al 11 de Junio de 2015, a una media de 3 h. diarias = 13 días x 3 h./día = 39 h. x 25 €/h. = **975** €.
- **Impresión y encuadernación del informe (2 copias): 6** € aprox.

Coste total de la pericial: 30 + 10 + 10 + 975 + 6 € = **1031** €.

Capítulo 11

Conclusiones

En este capítulo se presentarán las conclusiones obtenidas como resultado de la realización de este trabajo abordando cada uno de los objetivos específicos y generales que se plantearon inicialmente y que han sido descritos en el capítulo 2.

11.1 Objetivos cumplidos

Este trabajo estaba inicialmente motivado por la falta de información específica acerca de la elaboración de informes periciales informáticos. La principal barrera que cualquier técnico interesado en realizar esta labor tenía que salvar era la de realizar un completo y exhaustivo análisis de las metodologías o normas existentes, para identificar después las fases y tareas comunes a todas ellas y fundamentales para dotar de solvencia jurídica y técnica al trabajo. El objetivo principal de este TFG es el de proporcionar a cualquier técnico interesado con una metodología concreta a seguir. Esta metodología debía tener presente las garantías procesales, especialmente las del proceso penal, que deben estar presentes en todo proceso de recogida y análisis de evidencias. La falta de legislación concreta al respecto de la evidencia digital hace necesario una tarea de adaptación. Así por ejemplo, la cadena de custodia es una cuestión esencial cuando ésta se aplica a evidencias físicas. Su aplicación a evidencias digitales no es tan directa como podría parecer[1] *a priori* y requiere de un análisis pormenorizado así como la proposición de tareas específicas dentro de la metodología propuesta de recogida y análisis de evidencias forenses.

En términos del objetivo general propuesto puede concluirse que éste ha sido satisfecho por cuanto el mismo se ha concretado en la documentación resultado de este TFG. Además, dicha metodología ha sido validada mediante la elaboración de un caso de uso específico al cual ha sido aplicada. El resultado de dicha validación ha sido un informe pericial que cumple con los requisitos para ser válidamente presentado como prueba en un proceso judicial.

La consecución de este objetivo general ha pasado por abordar todos y cada uno de los objetivos específicos que se listaron en la sección 2.2 y que se analizan a continuación en términos de su grado de completitud así como las conclusiones que de los mismos pueden

[1] Por ejemplo, no bastaría con asegurar la cadena de custodia del disco duro para que las evidencias del mismo queden sujetas a los requisitos que establecen las leyes procesales. La evidencia digital es algo más que el dispositivo físico que las contiene.

derivarse:

- El estado de la cuestión se ha analizado desde dos perspectivas fundamentalmente: la de las herramientas hardware y software existentes y la de las metodologías y normas que al respecto del análisis forense puede encontrarse en el estado del arte. Del análisis de herramientas puede extraerse no sólo las características y bondades de cada una de ellas, sino el análisis previo que se realiza para identificar aquellas características que convierten a una herramienta (hardware o software) en un elemento útil en el proceso de análisis forense. Se alcanzan conclusiones como la necesidad de que el sistema de montado de discos se haga de manera tal que no se permita la modificación del contenido del mismo o cuestiones como que la copia de datos no es lo mismo que el clonado y que hay que buscar herramientas que certifiquen el clonado, frente a la mera copia. Respecto de las metodologías, este capítulo presenta las más conocidas en este ámbito, concluyendo que aunque el nombre y contenido de las distintas etapas varía de unas a otras, generalmente suele ser una cuestión de granularidad, no habiendo diferencias importantes o invalidantes de unas a otras. Todo esto puede comprobarse en el capítulo 4.
- En el capítulo 8 se escogieron ciertas herramientas software con las que pueden llevarse a cabo una gran cantidad de operaciones relacionadas con la extracción de evidencias digitales. Además se proporciona información que permite al lector ayudar a interpretar los datos que estas evidencias muestran. En este sentido, la mayoría de las herramientas analizadas están disponibles bajo diferentes licencias de software libre, lo que permite su uso sin necesidad de adquirir licencias. Si se comparan estas herramientas con otras de licencias propietarias puede observarse que generalmente éstas simplemente facilitan las etapas de configuración y obtención de resultados, recurriendo a interfaces visualmente más agradables y fáciles de usar. De esta manera, este tipo de herramientas suele requerir menos conocimiento por parte del perito. Sin embargo, en términos de potencia o resultados obtenidos no hay diferencias importantes más allá de la amigabilidad de la herramienta.
- Se construyó también un escenario de análisis ficticio que abarca el capítulo 10 y los anexos F y G. Esta tarea iba encaminada a la validación de la metodología propuesta. Por lo tanto, como resultado del análisis de este caso ficticio se esperaba obtener un informe pericial que cumpliera con todos los requisitos establecidos para un análisis forense con solvencia jurídica.

  Como se dijo, se siguió una normativa y un modelo concretos (UNE 71506:2013 y 197001:2011) para realizar todo un procedimiento pericial y se construyó el escenario de tal forma que agrupara varios tipos de análisis: de papelera de reciclaje, sistema de archivos, etc., como pudo verse en la sección 10.5.
- Además se proporcionó gran cantidad de información sobre la legislación y normativa

vigentes que es necesario conocer para realizar la aplicación de todos los procedimientos de manera adecuada.

Se habló sobre la ciberdelincuencia en general, del procedimiento probatorio en un proceso penal, sobre la evidencia digital, su recogida y cómo mantener su integridad mediante la cadena de custodia y sobre los aspectos relacionados con el perito informático. Finalmente se realizó una recopilación de la legislación aplicable mencionada a lo largo de todo el documento.

Puede contemplarse todo lo anteriormente citado en los capítulos 6 y 7, y en los anexos A, B, C, D y E

Teniendo en cuenta la consecución de todos los objetivos específicos, se da por satisfecho finalmente el objetivo general de este trabajo.

Capítulo 12

Conclusions

In this chapter, the conclusions obtained from this Bachelor's Thesis will be presented, addressing both specific and general objectives presented at first and described in chapter 3.

12.1 Accomplished objectives

This work was initially motivated by the lack of specific information about the development of computer expert reports. The main obstacle every technician interested in this task had to overcome was carrying out a thorough analysis of the existing methodologies and standards, to identify after that the phases and tasks common to all of them and essential to provide this work legal and technical solvency. The main objective of this Bachelor's Thesis is to provide every interested technician a specific methodology to follow. This methodology should keep in mind the procedural guarantees, specially the ones from the criminal proceeding, that should be present in the whole process of evidence collection and analysis. The lack of specific legislation in respect of the digital evidence makes necessary and adaptation task. For example, the chain of custody is an evident matter when applied to physical evidences. Its application to digital evidences is not so direct as it might seem[1] beforehand and it needs a detailed analysis as well as the proposal of specific tasks inside the proposed methodology of forensic evidences collection and analysis.

In terms of the proporsed general objective, it can be said this has been fulfilled, since it has been specified in the resulting documentation of this Bachelor's Thesis. Besides, the stated methodology has been validated through the development of a specific use case which it has been applied to. The result of the mentioned validation has been an expert report that meets the requirements to be validly presented as a piece of evidence in judicial proceedings.

The achievement of this general objective has gone through the addressing of one and all the specific objectives listed in section 3.2 and analyzed below in terms of their degree of completeness as well as the conclusions thereof derived:

[1] For example, it wouldn't be enough to ensure the chain of custody of a hard disk for the evidences within to be subject to the requirements stablished by procedural laws. The digital evidence is something bigger than the physical device containing them.

- The current situation has been analyzed from two perspectives: on the one hand from the existing software and hardware tools and on the other hand from the methodologies and standards that in respect of the forensic analysis can be found in the state of the art. From the tool analysis can be extracted not only the features and virtues of each one of them, but the previous analysis conducted to identfiy those features that make a tool (hardware or software) into a useful item for the forensic analysis process. Certain conclusions can be reached, like the necessity of the disk mounting system is made in such a way that the modification of the content is not allowed or issues like the data copy is not the same thing as the clone, and it's necessary to search for tools that certify the clone, instead of the mere copy. In respect of the methodologies, this chapter shows the most known in this field, concluding that although the name and content of the different phases varies from each other, it's generally a matter of granularity, with no significant or invalidating differences between them. This can be seen in 4.
- In chapter 8 some software tools were chosen. With these tools, a large number of operations related to the extraction of digital evidences can be carried out. Furthermore, information useful for the reader is provided, in order to help him to interpret the data the evidences show. In this sense, most of the analyzed tools are available under different free software licenses, allowing their use with no need of buying licenses. If these tools are compared to others with proprietary licenses it can be seen that generally the last ones simply facilitate the stages of configuration and the obtainment of results, using visually pleasing interfaces, easier to use. In this way, this kind of tools need less knowledge for the expert. However, in terms of power or obtained results, there's no significant differences beyond the tool friendliness.
- A fictional analysis scenario was built. This scenario is included in chapter 10 and in annexes F and G. This task was intended to the validation of the proposed methodology. Thus, as a result of the analysis of this fictional case it was expected to get an expert report meeting all the established requirements for a forensic analysis with legal solvency.

  As stated earlier, a specific normative and model were followed (UNE 71506:2013 and 197001:2011) to make a whole expert procedure and the scenario was built to group together several types of analysis: recycle bin, file system, etc., as was seen in section 10.5.
- Furthermore, a great quantity of information about current legislation and normative was supplied. This was necessary for a better implementation of all the procedures in a proper way.

  It was talked about cybercrime in general and also about the evidentiary procedure in a criminal procedure, the digital evidence, its collection and how to keep its integrity through the chain of custody and about the related aspects of the computer expert. Fi-

nally, a compilation of the applicable legislation mentioned throughout this document was performed.

All aforementioned can be seen in chapters 6 and 7, also in annexes A, B, C, D and E

Taking into account the achievement of all the specific objectives, it's finally satisfied the general objective of this work.

ANEXOS

Anexo A

Sobre la ciberdelincuencia

A.1 Convenio sobre la ciberdelincuencia (Budapest, 2001)

El objetivo de este Convenio [dE01] es adoptar una legislación adecuada y mejorar la cooperación internacional para proteger a la sociedad de la ciberdelincuencia. Fue ratificado en España en el año 2010 y está abierto también a países de fuera de la Unión Europea (UE). Consta de 48 artículos, cuyo contenido será descrito lo más brevemente posible.

Entrando en el capítulo I se pueden encontrar una serie de definiciones que permitirán la mejor comprensión del documento. Estas definiciones serán «sistema informático», «datos informáticos», «proveedor de servicios» y «datos relativos al tráfico».

En el capítulo II se hace una descripción de diversos delitos, divididos en varias categorías. Dentro de la categoría de **delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos** se encuentran el **acceso ilícito** a todo o a parte de un sistema informático con la intención de conseguir datos informáticos o con cualquier otra intención delictiva, la **interceptación ilícita** de datos informáticos, también los **ataques tanto a la integridad de los datos como a la del sistema**, es decir, dañar, borrar, deteriorar, alterar o suprimir datos informáticos, u obstaculizar el funcionamiento de un sistema grave, deliberada o ilegítimamente. Como último delito dentro de esta categoría citaremos el **abuso de dispositivos**, lo que significa posesión, producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de cualquier dispositivo, incluyendo programas, contraseñas, códigos de acceso o datos informáticos para cometer cualquiera de los delitos anteriormente descritos. Como puntualización, no se impondrá responsabilidad penal si se trata de un caso de pruebas autorizadas o de la protección de un sistema informático.

Adentrándonos dentro de los **delitos informáticos** encontraremos la **falsificación informática**, o lo que es lo mismo, generar datos falsos para que sean tomados como auténticos, con intención delictiva. En cambio, el **fraude informático** consistirá en cometer actos delictivos que causen daños patrimoniales a otra persona.

Una tercera categoría sería la de **delitos relacionados con el contenido**, donde están incluidos los **delitos relacionados con la pornografía infantil**, que consiste en la producción, difusión, adquisición o posesión de material pornográfico que contenga una representación

visual de menores.

Y como última categoría referida a delitos, se encuentra la de **delitos relacionados con infracciones de la propiedad intelectual y de derechos afines**, que serán todos aquellos que infrinjan la propiedad intelectual que defina su legislación sobre los derechos de autor y derechos afines [Mar12a] [Mar12b].

Otras formas de responsabilidad y de sanción son también citadas. Además, se cuenta con una serie de disposiciones comunes sobre la aplicación de poderes y procedimientos a efectos de investigación o procesos penales. Otros temas tratados son la conservación de datos informáticos almacenados, la orden de presentación de éstos, su registro y confiscación, y su obtención en tiempo real.

Para concluir este capítulo, se hace mención de la **jurisdicción**. Aquí se tratará de aplicar las medidas legislativas o de otro tipo que sean necesarias para asegurar la jurisdicción de una Parte respecto de cualquier delito cometido.

La **cooperación internacional** tiene cabida dentro del capítulo III, abordando temas tan importantes como los principios generales de dicha cooperación, disposiciones específicas como la asistencia mutua en materia de medidas provisionales y en relación con los poderes de investigación. Se nombra también el concepto *Red 24/7*, que consiste en mantener puntos de contacto por ambas Parte de modo que se pueda garantizar una inmediata asistencia destinada a la investigación de delitos relacionados con los sistemas y los datos informáticos, o para obtener las pruebas de un delito.

Y para concluir, el capítulo IV trata las cláusulas finales, entre ellas la firma y entrada en vigor del presente Convenio, los efectos de éste y la adhesión de diversos Estados, tanto de dentro como de fuera de la UE.

A.1.1 Protocolo adicional relativo a los delitos de índole racista y xenófoba (Estrasburgo, 2003)

Este Protocolo [dE03], al igual que el Convenio sobre la ciberdelincuencia, está también compuesto de 4 capítulos distintos. En el capítulo I se hacen una serie de disposiciones comunes, como la finalidad y ciertas aclaraciones en cuanto a lo que debemos entender por material racista y xenófobo.

La finalidad no es otra que complementar al Convenio en lo que respecta a los actos de índole racista y xenófoba cometidos mediante sistemas informáticos, se entiende. Se ha citado el término «material racista y xenófobo» pero para no dar lugar a malas interpretaciones, se deberá entender como cualquier material o representación de ideas que incita al odio, discriminación o violencia por motivos de raza, color de piel, ascendencia o religión.

Dentro del capítulo II se explican los delitos relacionados a la cuestión que nos ocupa y las medidas a tomar a nivel nacional. Estos delitos son la **difusión de material racista y xe-**

nófobo a través de sistemas informáticos, **amenazas** por medio de un sistema informático por razón de la raza, color de piel, ascendencia o religión de una persona o grupo de éstas. Otro delito relacionado sería el de **insultos con motivación racista y xenófoba** por medio de un sistema informático.

Y finalmente, el de **negación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad**, mediante la difusión o puesta a disposición, por medio de un sistema informático, de este tipo de material. A raíz de lo anteriormente dicho, también podrán tomarse medidas contra la **cooperación y complicidad** en la comisión de cualquiera de los delitos tipificados en este Protocolo.

Las relaciones entre el Convenio y este Protocolo se muestran en el capítulo III. Y para concluir, al igual que en el Convenio, en el capítulo IV quedan explicadas una serie de disposiciones finales: la entrada en vigor, la adhesión de Estados y la aplicación territorial entre ellas.

Anexo B

Sobre la gestión de evidencias electrónicas

Se va a proceder a hablar en este anexo sobre varias normas que ayudan a aunar la gestión de las evidencias electrónicas, ya que establecen una serie de buenas prácticas que será recomendable seguir de cara a la presentación de dichas evidencias en un proceso judicial.

B.1 UNE 71505:2013 Sistema de Gestión de Evidencias Electrónicas (SGEE)

Esta norma se encarga de definir el Sistema de Gestión de Evidencias Electrónicas (SGEE) y consta de 3 partes:

- Parte 1: Vocabulario y principios generales [AEN13a]
- Parte 2: Buenas prácticas en la gestión de las evidencias electrónicas [AEN13b]
- Parte 3: Formatos y mecanismos técnicos [AEN13c]

Dichas partes son de aplicación en entornos propios de organizaciones o empresas.

B.1.1 UNE 71505-1: Vocabulario y principios generales

En esta primera parte se podrán consultar diversos términos y definiciones generales que serán comunes a toda la norma, es decir, tanto a ésta como a las dos partes restantes.

También se dará una visión general del proceso de gestión y de la relación entre las partes. Ésto se conseguirá dando como ya se ha dicho una descripción de términos y definiciones en primer lugar, seguido de una descripción a alto nivel del proceso y las tareas relacionadas con la gestión de evidencias electrónicas y finalmente, una pequeña descripción de las dos partes restantes que forman esta norma, que omitiremos debido a que serán descritas en las subsecciones sucesivas.

Entrando en las generalidades de la administración de evidencias electrónicas, se podrá observar que esta norma va a adoptar un enfoque por procesos para la creación, implementación, funcionamiento, supervisión, revisión, mantenimiento y mejora del SGEE de la organización. Y dentro de este enfoque se debe destacar la importancia de la comprensión de los requisitos de seguridad de la información de la organización y la necesidad de implantar una política de seguridad de las evidencias electrónicas, junto con sus objetivos.

También será importante implantar ciertos controles para administrar los riesgos de seguridad de la información, a la vez que se supervisará el rendimiento y la eficacia del SGEE. Por último, se decidirá si se va a integrar, o no, dicho SGEE en un SGSI.

B.1.2 UNE 71505-2: Buenas prácticas en la gestión de las evidencias electrónicas

En esta parte de la norma se establecerán los controles y procesos que van a ser aplicables a la gestión de seguridad de las evidencias electrónicas y su integración en el ciclo PHVA de gestión de la seguridad de la información de una organización.

Se habla en primera instancia de la **confiabilidad**, es decir, maximizar la veracidad y la exactitud de las evidencias electrónicas que se posean, basándose en sistemas, procesos y procedimientos confiables.

Para esto se deberán cumplir varias cosas:

En primer lugar la **autenticación** y la **integridad**, que garantizarán que la información no ha sido modificada. Se podría decir que una evidencia electrónica auténtica es aquella que es lo que afirma ser y que ha sido creada, almacenada y/o enviada en el momento en que se afirma, por la persona que afirma haberla creado, almacenado y/o enviado. Por otra parte, la integridad se referirá a la no alteración de la evidencia electrónica, que será necesario proteger contra modificaciones no autorizadas.

Seguidamente, se deben asegurar la **disponibilidad** y la **completitud**. La disponibilidad consiste en la cualidad que hace que una evidencia electrónica pueda ser localizada, recuperada, presentada e interpretada; mientras que la completitud hace referencia a la representación completa de la información que contiene la evidencia.

Asegurando estas dos cualidades, se garantizará el acceso y la utilización a la evidencia en los tiempos requeridos.

Por último, para asegurar la confiabilidad se deben cumplir un último par de atributos: **cumplimiento** y **gestión**, que garantizarán que la evidencia que se ha obtenido se ciñe a lo esperado después de haberse gestionado y utilizado los procedimientos que se planificaron previamente.

Para alcanzar dicha confiabilidad, se deberá tener un SGEE, cuyas generalidades ya se expusieron en la primera parte de esta norma. La gestión de las evidencias electrónicas de una organización incluye:

- Establecimiento de políticas, estrategias, controles y procedimientos
- Asignación de responsabilidades y competencias
- Integración de la gestión de las evidencias electrónicas en los sistemas y en los procesos que dan soporte a la organización.

La gestión de las evidencias nos proporciona una serie de beneficios, debido a que el SGEE nos podrá servir de ayuda en actividades posteriores o en una futura toma de decisiones.

En esta norma se va a seguir el ciclo de mejora continua Planificar, Hacer, Verificar y Actuar (PHVA), como puede observarse en el cuadro B.1.

Planificar (establecer el SGEE)	Establecer la política del SGEE, los objetivos, los procesos y procedimientos correspondientes a la gestión de riesgos y a la mejora de la confiabilidad de las evidencias electrónicas, para proporcionar unos resultados de acuerdo a los objetivos y políticas globales de la organización
Hacer (implantar y poner en marcha el SGEE)	Implantar y poner en marcha la política, controles, procesos y procedimientos del SGEE
Verificar (controlar y revisar el SGEE)	Evaluar y, cuando sea aplicable, medir el comportamiento de los procesos contra la política del SGEE, los objetivos y la experiencia práctica e informar de los resultados a la dirección para su revisión
Actuar (mantener y mejorar el SGEE)	Tomar medidas correctivas y preventivas, basadas en los resultados de la auditoría interna del SGEE y de la revisión por la dirección o de otra información importante, para conseguir la mejora continua del SGEE

Cuadro B.1: Modelo PHVA aplicado a los procesos del SGEE

Como ya se dijo, se adoptará un enfoque por procesos para el SGEE y esto requerirá que las organizaciones comprendan los requisitos y la necesidad de establecer una política y unos objetivos para gestionar correctamente las evidencias electrónicas, diseñando e implantando controles adecuados para la gestión de los riesgos globales del negocio en relación con las evidencias. Las organizaciones también deberán controlar y revisar la eficacia del SGEE adoptado y tratar mejorarlo continuamente.

El proceso de **planificación** constará de varias fases:

Definición del alcance y análisis de riesgos

El alcance del SGEE podrá ser global sobre la organización o bien sobre parte de ésta. Una vez determinado el alcance, éste deberá contener los elementos sobre los que se requiere evidencia y aquellas que forman parte del SGEE.

Para dicho alcance, se deberá efectuar un análisis de riesgo orientado a la seguridad de la información y considerando los aspectos legales y operacionales relativos a las evidencias.

Identificación de recursos y planificación de procesos

Una vez se hayan definido los objetivos, se deberá proceder con la identificación de recursos, tanto humanos, como de infraestructura y financieros para la gestión del sistema, junto a los roles y responsabilidades.

También se planificarán los procesos necesarios para implantar el SGEE, que se corresponderán con los objetivos obtenidos a partir del análisis de riesgo previo.

A la hora de la implantación, se deben asignar claramente las funciones y responsabilidades a cada integrante del SGEE. Estas responsabilidades deberían asignarse según el principio de «necesidad de conocer», asegurando una correcta separación de funciones.

Es importante también documentar todos los procesos de gestión de seguridad de las evidencias electrónicas. La documentación deberá detallar las actividades de la organización y las evidencias electrónicas que le corresponden, especificando los periodos de conservación y qué acciones se tomarán para su eliminación, así como las instrucciones necesarias para transferir las evidencias a otros medios de almacenamiento sin perder la integridad o la confidencialidad.

Se deberá tener en cuenta que el SGEE es tan solo una parte del sistema de gestión de la organización, existiendo otros sistemas como por ejemplo el SGSI. Ante la existencia de varios sistemas, será necesaria una correcta integración entre todos ellos, con fin de mejorar la eficiencia y la eficacia del sistema global de la organización.

Como punto final a esta parte de la norma, nos encontramos con dos anexos en los que se describen una serie de buenas prácticas específicas para el SGEE, haciendo mención a los controles a implantar y también a una matriz de funciones ejecutables por cada uno de los roles del SGEE.

B.1.3 UNE 71505-3: Formatos y mecanismos técnicos

En esta última parte de la norma serán definidos el formato de intercambio de evidencias electrónicas y los mecanismos que ayudarán a mantener la confiabilidad de éstas, dentro del entorno de una organización, y al intercambio de dichas evidencias entre organizaciones.

La elección de un formato de intercambio normalizado garantizará la interoperabilidad entre diferentes organizaciones y la confiabilidad del contenido de las evidencias.

En cuanto a los mecanismos, normas y estándares de seguridad aplicados a la evidencia electrónica, tendrán como objetivo garantizar su autenticidad e integridad para mantener su valor probatorio ante un proceso judicial.

Entre estos mecanismos podemos citar la **firma electrónica**, cuya finalidad es probar la integridad y la identidad de la evidencia a la que está asociada. Tiene diferentes variantes, como CMS, XAdES, CAdES, PAdES, etc. No obstante carece de dos propiedades básicas: la fiabilidad de la fecha de creación y la robustez de los algoritmos criptográficos, en los

que está basada, a largo plazo. El **sello de tiempo** (o *timestamp*) proporciona a la firma electrónica la propiedad de no repudio, garantizando que la clave de la firma seguía vigente en el momento en que los datos fueron firmados.

Por otra parte, al usar **criptografía asimétrica**, será más fácil garantizar la confidencialidad. Algunos algoritmos válidos son 2TDEA, 3TDEA, AES-128, 192 o 256. La elección del algoritmo a utilizar se hará en base al periodo de tiempo de validez que se prevee que tendrá la evidencia. Teniendo esto en cuenta, la organización establecerá una política de conservación a largo plazo.

Llegando al formato de intercambio de las evidencias electrónicas, se citará la estructura general, que se divide en 3 campos diferenciados:

- **Cabecera:** contendrá datos que aportarán contexto al contenido, a la estructura y a las credenciales de seguridad de la evidencia electrónica, por ejemplo: el tamaño de la propia cabecera, el creador, número de archivo, archivos totales, etc.
- **Contenido:** guardará información principal de la evidencia electrónica.
- **Credenciales de seguridad:** datos de identificación para la autenticación y validación de integridad de la evidencia electrónica, es decir, aquellos datos generados por los mecanismos de firma electrónica y sello de tiempo.

Finalmente, se tienen una serie de anexos con información adicional útil, como los algoritmos criptográficos válidos según la criticidad de la información y el periodo de tiempo previsible de validez, información sobre cuál es la fuente legal de tiempo en España, una relación de formatos de firma y sellos de tiempo admitidos, los requisitos para la reproducción e impresión de las evidencias electrónicas y un pequeño ejemplo del formato de un fichero contenedor de la evidencia en XML.

B.2 UNE 71506:2013 Metodología para el análisis forense de las evidencias electrónicas

Esta norma [AEN13d] tiene como objetivo definir el proceso de análisis forense dentro del ciclo de gestión de evidencias electrónicas, según se describe en la UNE 71505, complementándola. En ella se establecerá una metodología para la **preservación, adquisición, documentación, análisis** y **presentación** de las evidencias electrónicas.

Se ofrecen en primer lugar una serie de términos, definiciones y abreviaturas, que junto a los proporcionados en la norma UNE 71505-1 serán de utilidad dentro de este documento.

A continuación se habla en detalle de las diferentes fases del proceso de análisis forense, que serán comentadas en las posteriores subsecciones.

Y finalmente se encuentran una serie de anexos, el primero consiste en un **modelo de informe pericial**, en el que se toma como referencia el modelo de informe propuesto por la

norma UNE 197001, descrita en el anexo C del presente documento, en la subsección relativa al cuerpo del informe, y deben incluirse los siguientes apartados:

1. **Asunto**
2. **Evidencias/muestras recibidas**
3. **Resolución o estudios efectuados sobre las evidencias/muestras**
4. **Situación final de las evidencias/muestras**
5. **Conclusiones finales**
6. **Anexos del informe**

El segundo anexo trata genéricamente las **competencias** con las que ha de contar el personal involucrado en las diversas fases del análisis forense, separadas en diferentes categorías: competencias **técnicas, profesionales** y **personales**.

El último anexo descrito en la norma se refiere al **equipamiento para el análisis forense** de las evidencias electrónicas. Se debe contar con herramientas tanto hardware como software reconocidas por la comunidad forense internacional, aún no existiendo una normalización.

B.2.1 Preservación

En esta fase se pretende mantener en todo momento la validez y confiabilidad de las evidencias originales, siempre teniendo en cuenta una serie de principios, como tener protocolos que aseguren la integridad de las evidencias sometidas a estudio, de tal forma que se eviten modificaciones intencionadas, la exposición a campos magnéticos o la conexión accidental a redes inalámbricas.

Los técnicos que tengan el primer contacto con las evidencias deberán almacenar, precintar y sellar éstas en los soportes oportunos para preservar otro tipo de evidencias como pueden ser huellas o restos orgánicos que estén asociados con el ADN, etc. Así como llevar la indumentaria adecuada para evitar descargas electrostáticas y utilizar soportes aislados para evitar interferencias externas.

Del mismo modo, el personal técnico deberá almacenar dichas evidencias en un lugar seguro hasta que finalice el proceso pericial, o si no se dispone de dicho lugar, en una caja fuerte en el mismo entorno de trabajo.

B.2.2 Adquisición

Se realizará aquí un clonado a bajo nivel de los datos originales, siguiendo un procedimiento documentado para asegurar que el proceso de adquisición es reproducible y repetible.

Si el lugar del incidente está delimitado físicamente, se deben seguir una serie de precauciones antes de proceder a la adquisición:

1. Alejar a todas las personas no autorizadas de la escena
2. Identificar al administrador de los sistemas en caso de necesitar apoyo técnico
3. Mantener el estado de los dispositivos, si está encendido, no apagarlo y viceversa
4. Buscar posibles notas asociadas a las contraseñas o PINs de acceso a los equipos
5. Fotografiar la escena, para documentar el estado inicial y para una posible reconstrucción posterior
6. Etiquetar dispositivos y cableado
7. Localizar equipos inalámbricos instalados y determinar los modos de conexión que usan
8. No desconectar fuentes de alimentación cuando las evidencias estén almacenadas en soportes volátiles
9. En los distintos dispositivos digitales, revisar la existencia de dispositivos de almacenamiento adicionales introducidos en ellos

Es importante el estado en el que se encuentran los sistemas, de modo que el proceso de adquisición no será el mismo en sistemas apagados que en sistemas encendidos, en los que comprometer la integridad de las posibles evidencias es relativamente fácil.

Sistemas apagados

Si los sistemas están apagados, las recomendaciones básicas son: hacer un **borrado seguro** del soporte que va a contener el clonado forense; una vez comprobado esto, se usarán dispositivos **bloqueadores de escritura** (hardware o software) para garantizar la no alteración de los datos originales y se debe calcular el resumen *hash* tanto de la información contenida en el soporte original, como en el soporte copia obtenido, comprobando que ambos resúmenes son idénticos.

En el caso de **dispositivos móviles**, si llevan la tarjeta SIM se debería extraer la información contenida en ésta. En caso de que no se tuviera conocimiento del número PIN o PUK, se debería solicitar este último a la operadora de telefonía mediante una autorización judicial.

El dispositivo también contendrá información en la memoria interna, por lo que también deberemos realizar una copia a bajo nivel de los datos allí almacenados.

Es importante recordar que se deberá calcular el *hash* de toda la información extraída.

Sistemas encendidos

Cuando los sistemas están se encuentran en funcionamiento, se deberá proceder a su adquisición según el orden de volatilidad, de mayor a menor volatilidad. El grado de volatilidad posee, por lo general, dos niveles:

- Información de la memoria RAM, particiones y archivos de intercambio (*swap*), procesos de red y del sistema en ejecución
- Información de los sistemas de ficheros y datos contenidos en los sectores de los dispositivos de bloques

Cuando manipulamos **dispositivos móviles**, estos deberán ser aislados debidamente, de forma que no entren en contacto con redes inalámbricas que puedan manipular accidentalmente los datos contenidos dentro de ellos.

Una metodología de análisis a seguir sería realizar un clonado de las partes accesibles de la tarjeta SIM e introducir el clon de la tarjeta en el terminal. Una vez encendido el terminal, se hará una copia a bajo nivel de los datos contenidos en su memoria interna.

Si algún modelo específico de terminal no fuera soportado por las herramientas forenses disponibles, se podrá trasladar al informe la información que se lea en la pantalla o proceder como en el caso de los sistemas apagados.

Una vez se ha terminado con el proceso de análisis de los datos, no se deberá introducir de nuevo ni la batería ni la tarjeta SIM original y se deberá, como siempre, calcular el *hash* de toda la información extraída.

También podremos encontrarnos con **entornos virtualizados**, en los que cada una de las máquinas virtuales estará formada por varios ficheros, como el de configuración del hardware del equipo, el utilizado para la memoria y uno o varios discos físicos o virtuales. Aquí, la información a obtener serán los discos duros virtuales y un volcado de la parte de la memoria RAM utilizada por este entorno. De este modo, una vez obtenidos todos los ficheros de configuración de la máquina virtual y los discos virtuales, se deberá ser capaz de reproducir el entorno original para su análisis.

B.2.3 Documentación

Cualquier análisis forense requerirá un control sobre las evidencias que van a ser sometidas a estudio. Por tanto, se documentará todo el procedimiento desde que se inicia el análisis hasta que acaba a través de la redacción del informe pericial a enviar al solicitante, indicando todos los procesos y herramientas utilizadas y el momento en que fueron ejecutados dichos procesos, siguiendo una secuencia temporal definida con vistas a elaborar un registro auditable.

Consecuentemente, la cadena de custodia debe tener implementado un sistema de gestión documental donde van a quedar reflejados todos los pasos llevados a cabo. Esta gestión documental incluirá los siguientes documentos, entre otros:

- Documento de recepción de evidencias electrónicas, pudiendo llevar así un control de las peticiones de análisis y de las propias evidencias a estudiar

- Registro de la documentación recibida. Entre los documentos que acompañarán a la evidencia se pueden encontrar: una descripción de las evidencias y de la cadena de custodia hasta que dichas evidencias llegan al entorno de análisis, así como los estudios solicitados en dicho análisis y los permisos necesarios para realizar dichos estudios
- Registro de las evidencias en el que se describirá detalladamente cada evidencia y su estado en el momento de la recepción
- Registro del tratamiento inicial en el que se describirá el proceso de clonado (volcado de datos o realización de la imagen)
- Registro de situación de evidencias, en el que se reflejarán las operaciones practicadas a una evidencia, dónde se practicaron, por quién y en qué momento
- Registro de tareas del análisis inicial
- Registro de tareas del análisis de datos definitivo con la expresión temporal de los procesos llevados a cabo, y la ubicación temporal de la evidencia si se paralizara temporalmente su estudio

B.2.4 Análisis

Durante la fase de análisis se llevarán a cabo una serie de procesos y tareas que intentarán dar respuesta a preguntas relacionadas con una intrusión, como su origen, la lista de sistemas afectados, los métodos usados, etc. Y todos estos procesos y tareas deberán realizarse de forma metódica, auditable, repetible y defendible.

Al llegar las evidencias al laboratorio forense, se tendrán en cuenta una serie de acciones previas:

1. Comprobar que lo que se precisa estudiar está dentro de la competencia del laboratorio
2. Formar un mapa contextual de las evidencias, según la documentación adjunta, las relaciones entre las mismas y de éstas con los distintos actores implicados
3. Revisar la cadena de custodia previa a la llegada de las evidencias al laboratorio
4. Solicitar las autorizaciones que se precisen para el estudio solicitado, según la legislación vigente
5. Comprobar que las evidencias no están deterioradas y se pueden someter a estudio
6. Si aparecen nuevas evidencias no contempladas anteriormente, se generará un nuevo proceso de gestión, custodia y trazabilidad siguiendo la norma UNE 71505 previamente descrita y se notificará al solicitante
7. Revisar la hora de la BIOS del equipo sometido a estudio, de modo que pueda ser comparada con la fecha del momento en que se active el análisis forense
8. Establecer unos criterios de prioridades

Teniendo esto en cuenta, se describirán a continuación las acciones y procesos que van a llevarse a cabo, en líneas generales, durante la fase de análisis de las evidencias.

Recuperación de los ficheros borrados

Consiste en una recuperación total o parcial de los datos ubicados en áreas del disco no asignadas por el sistema en ese momento y en el espacio del disco sin utilizar, así como como de recuperar carpetas y archivos «huérfanos», de los que se ha perdido su vinculación.

Se buscarán también archivos completos o fragmentos de éstos a través de sus cabeceras.

En el informe pericial se especificará claramente de dónde se ha extraído la información y qué método se usó para dicha recuperación.

Estudio de las particiones y sistemas de archivos

Este proceso tendrá como finalidad estudiar las diversas estructuras de los contenedores de almacenamiento de los dispositivos a estudiar (particiones, sistemas RAID, etc.)

El proceso incluirá una serie de tareas básicas:

- Enumeración de las particiones actuales y de las que hubieran existido anteriormente
- Identificar zonas del disco ocultas no visibles para el SO, como las HPA o DCO
- Identificar los sistemas de archivos en los contenedores o en las particiones, con la identificación del contenedor que almacena el SO de inicio y el tipo de arranque o selector multiarranque
- Identificar también los sistemas de archivos de los discos compactos y los posibles archivos cifrados y/o protegidos por contraseña
- Proceder al montaje de los archivos contenedores de otros (comprimidos, empaquetados, etc.) verificando las cabeceras de los distintos formatos y sus resúmenes digitales

Al realizar un análisis de la memoria RAM se estudiarán, para un momento temporal concreto, los procesos activos, ficheros abiertos, puertos y tomas de corriente activas, así como claves de acceso a programas o volúmenes cifrados del soporte de almacenamiento.

Estudio del sistema operativo

Se estudiará durante este proceso el sistema operativo instalado, la actividad de los usuarios existentes en dicho sistema y su política de seguridad.

El proceso englobará ciertos pasos:

- Identificar el sistema operativo (SO) principal del equipo y su localización, así como otros SOs utilizados, su fecha de instalación y sus actualizaciones

- Identificar a los distintos usuarios junto a los privilegios y permisos de éstos dentro del SO, así como las fechas de último acceso al equipo de cada uno de los usuarios, y su política de seguridad
- Identificación de los dispositivos hardware y software reconocidos por el sistema o que pudieran haber estado instalados anteriormente

Estudio de la seguridad implementada

La finalidad de este proceso será estudiar si las evidencias electrónicas sometidas a estudio ha sido comprometidas.

Con el mismo fin se intentará identificar el posible software malicioso existente dentro de las distintas particiones identificadas, evaluando el grado de intrusión en el sistema informático y qué archivos fueron los comprometidos.

Análisis detallado de los datos obtenidos

Se incluirá el análisis detallado de las evidencias, teniendo en cuenta los análisis previos. Del mismo modo, se clasificarán los datos y opcionalmente se indexarán los mismos utilizando palabras clave, con el fin de agilizar posteriormente las búsquedas de indicios.

Un análisis forense detallado, contemplará los siguientes aspectos:

1. Hardware instalado, fecha, hora, datos de configuración regional, etc
2. Dispositivos físicos conectados en algún momento al equipo
3. Estudio del escritorio o pantalla principal y papelera de reciclaje
4. Conexiones de red y tarjetas instaladas y su dirección MAC, los protocolos usados y las direcciones IP
5. Estudio de las comunicaciones habidas desde el equipo
6. Estudio del registro del sistema y de los logs de auditoría del SO
7. Información contenida en los espacios no asignados en las particiones y en el espacio no ocupado por los archivos lógicos
8. Información contenida en los archivos de hibernación, paginación, particiones y archivos de intercambio (*swap*), etc.
9. Análisis de la cola de impresión
10. Enlaces a archivos y archivos accedidos recientemente
11. Estudio de las carpetas de usuario
12. Estudio de las aplicaciones instaladas
13. Estudio de los metadatos, en caso de ser de interés

14. Análisis de las aplicaciones de virtualización
15. Estudio de las bases de datos instaladas y de sus sistemas gestores
16. Estudio del software de cifrado y de los ficheros y particiones cifradas
17. Estudio de la navegación por Internet (cookies, historial, etc.)
18. Análisis de correos electrónicos
19. Análisis de registros de mensajería instantánea y conversaciones, junto a la lista de contactos

B.2.5 Presentación

Esta fase final consiste en plasmar toda la información obtenida durante el proceso de análisis de las evidencias en un informe pericial, dirigido al organismo o entidad que solicitó el estudio, teniendo en cuenta que este informe irá dirigido muchas veces a un público sin conocimientos técnicos profundos dentro del campo de la informática, por lo que deberá mantenerse un equilibrio entre la inteligibilidad y el rigor de lo escrito en dicho informe.

Una vez redactado, se debe remitir el informe al organismo solicitante, junto al documento de control de evidencias, finalizando así el proceso de custodia de las evidencias y aportando trazabilidad a dicho proceso.

Anexo C

Sobre la elaboración de informes periciales

Existen distintos tipos de peritos, según sus respectivas ramas profesionales, que elaboran informes periciales de distinto tipo. Por tanto, la intención de este anexo es la de dar unas directivas generales para tratar de estandarizar el proceso de redacción de estos documentos.

C.1 UNE 197001:2011 Criterios generales para la elaboración de informes y dictámenes periciales

Se establecerán en esta norma [AEN11] las consideraciones generales que permitirán precisar los requisitos formales que deben cumplir los informes periciales. No se entrará en métodos ni procesos específicos para la elaboración de los mismos.

Como en otras normas, en ésta se dan primeramente una serie de términos y definiciones que serán usados en este documento: **código o referencia de identificación**, **dato de partida** y **dictamen pericial**.

Los requisitos generales del informe general serán:

- **Título:** que identificará el informe de forma clara e inequívoca
- **Estructura:** será la estructura básica del informe
  - Identificación
  - Índice
  - Declaración de tachas y juramento (si procede)
  - Cuerpo del informe
  - Anexos
- **Paginación:** en todas las páginas del informe deberá aparecer el código de identificación, el número de página y el número total de páginas

La estructura anteriormente citada será descrita más en detalle en las posteriores subsecciones.

C.1.1 Identificación

Será el elemento que iniciará el informe pericial y contendrá la siguiente información:

- Título y código de identificación, que será único para cada informe
- Nombre del organismo al que se dirige el informe y si procede, el número de expediente o procedimiento
- Nombre y apellidos del perito, titulación, colegio profesional al que pertenece (si procede), documento de identificación, domicilio profesional, teléfono, email, y cualquier otro identificador profesional.
- Nombre y apellidos y documento de identificación del solicitante del informe, bien en nombre propio o en representación de otra persona física o jurídica, cuyos datos también figurarán y cualquier otro identificador.
- Si es el caso, se dará la dirección de un emplazamiento geográfico y las coordenadas UTM (*Universal Transverse Mercator*)
- Si es procedente, nombre y apellidos del letrado y del procurador del solicitante
- Fecha de emisión del informe

C.1.2 Índice general

Su finalidad será facilitar la localización de cada capítulo y apartado. Indicará el número de página en que se inicia cada uno de los capítulos y apartados del informe.

C.1.3 Declaración de tachas

Una tacha, según su definición [Sta14], consiste en:

> *Alegaciones que se hacen por algún litigante pretendiendo desvirtuar la fuerza probatoria de lo declarado por algún testigo o del dictamen emitido por algún perito, por considerar que puede ser parcial en sus declaraciones.*

El perito podrá aplicar, cuando proceda, el sistema de tachas o hacer constar su imparcialidad.

C.1.4 Juramento o promesa

El perito manifestará con este juramento que actuará con veracidad y objetividad, que ha tomado y tomará en consideración todo lo que pueda favorecer o perjudicar a cualquiera de las partes y que conoce las sanciones penales si incumple su deber como perito.

C.1.5 Cuerpo del informe pericial

Realmente esta es la parte principal del informe pericial y será donde se presenten y justifiquen las conclusiones, por lo cual deberá ser comprensible para todos los interesados. Los capítulos y apartados de los que estará compuestos serán los siguientes:

Objeto

En este capítulo se indicará la finalidad del informe.

Alcance

En este capítulo se indicarán las cuestiones planteadas por el solicitante.

Antecedentes

En este capítulo se indicarán hechos, cosas, sucesos o asuntos que hayan ocurrido antes del inicio del informe y que estén en conocimiento del perito.

Consideraciones preliminares

En este capítulo se indicarán todos los aspectos necesarios para la comprensión de la investigación llevada a cabo y de la metodología empleada.

Documentos de referencia

En este capítulo se recogerán las disposiciones normativas, otras normas de no obligado cumplimiento, la buena práctica profesional y la bibliografía que hayan sido usadas durante la realización del informe.

Terminología y abreviaturas

En este capítulo se indicarán todas las definiciones de palabras técnicas y de abreviaturas que se hayan utilizado.

Análisis

En este capítulo se indicarán las bases y datos de partida dados por el solicitante y también los que se deriven de:

- Legislación, reglamentación y normativa aplicables
- Investigación realizada encaminada a la definición de las conclusiones
- Referencias, documentos, muestras y procedimientos de toma y conservación de las mismas que fundamenten las conclusiones del informe

También se indicarán los razonamientos estudiados y cómo se ha llegado a ellos, ventajas e inconvenientes de cada uno y cuál es la justificación de las conclusiones.

Conclusiones

En este capítulo se indicará de forma resumida la interpretación técnica y experta emitida sobre los extremos que constan en el capítulo de Alcance, además de las posibles consideraciones adicionales que se crean necesarias para aportar matices a las conclusiones.

C.1.6 Anexos

Los anexos, que contendrán toda la información de interés adicional, deberán estar recogidos en el índice general y deberán estar identificados de manera correlativa y paginados de forma inequívoca.

Anexo D

Sobre el perito informático forense

En este anexo se realizará una descripción de algunos de los aspectos relacionados con el perito, como por ejemplo sus derechos y deberes y la justificación de la capacitación profesional de éste para el acceso a la profesión, entre otros. Todos estos detalles podrán afianzarse mediante cursos especializados de la ANTPJI [ANT].

D.1 La figura del perito

El **perito forense** o **perito judicial**, según la RAE[1], se define como: *«Persona que, poseyendo determinados conocimientos científicos, artísticos, técnicos o prácticos, informa, bajo juramento, al juzgador sobre puntos litigiosos en cuanto se relacionan con su especial saber o experiencia»*.

Puede dirigirse el lector para mayor información al **art. 335** de la **Ley 1/2000, de 7 de Enero, de Enjuiciamiento Civil (LEC)**, referente al objeto y finalidad del dictamen de peritos y a su juramento de actuar con objetividad. O al **art. 456** de la **Ley de Enjuiciamiento Criminal (LECRIM)**, según sea el ámbito del procedimiento civil o penal.

En concreto el **perito informático forense** será aquel profesional que posea unos conocimientos especializados en nuevas tecnologías y que proporcionará cierta información u opinión en forma de informe pericial a un solicitante (profesional, empresa o tribunal de justicia) sobre los puntos litigiosos materia de su dictamen, basándose en el análisis de elementos informáticos contenedores de datos que puedan constituir una posible evidencia digital a usar en un proceso legal, siempre de forma neutral, veraz e imparcial.

Si su presencia resultara necesaria, podría ser llamado a juicio, conforme al **art. 347 LEC**, referente a la posible actuación de los peritos en el juicio o en la vista.

D.2 Derechos y deberes del perito

El perito tendrá una serie de derechos y deberá cumplir una serie de deberes y obligaciones que serán descritos en esta sección.

[1] http://www.rae.es/

D.2.1 Derechos

El derecho básico con el que cuenta el perito, en el supuesto de un procedimiento civil, es el de cobrar honorarios por elaborar el dictamen que se le requiere, que será a costa de quien lo haya pedido, sin perjuicio de lo que pudiera llegar a acordarse posteriormente en materia de costas, según el **párrafo 1º** del **art. 339.2 LEC**.

Si el dictamen hubiera sido pedido por ambas partes desde el principio, si éstas están conformes, podrá ser designado un único perito para realizar el informe pericial solicitado, correspondiendo el pago de los honorarios a ambas partes de forma ecuánime, sin perjuicio de lo que pudiera acordarse en materia de costas (**párrafo 3º**, **art. 339.2 LEC**).

En un procedimiento penal, el perito podrá reclamar honorarios o indemnizaciones justas, si no tuviesen ya una retribución fija por el Estado, la Provincia o el Municipio (**art. 465 LECRIM**).

Por tanto, excepto en los casos de asistencia jurídica gratuita, según el **art. 241 LEC** referente al pago de las costas y gastos del proceso, en un procedimiento civil éstos se irán pagando a medida que se vayan produciendo. No obstante, el perito podrá solicitar una provisión de fondos que considere necesaria en el plazo de los tres días sucesivos a su nombramiento. Cuando el tribunal se pronuncie sobre la provisión, ordenará a la parte o partes solicitantes de la prueba pericial que abonen la cantidad fijada en el plazo de cinco días. Si transcurriera dicho plazo y no se hubiera depositado dicha cantidad, el perito quedará eximido de emitir el dictamen, sin posibilidad de procederse a una nueva designación, según el **art. 342.3 LEC**.

En el procedimiento penal y según el **art. 242 LECRIM**, el perito podrá exigir a la parte a la que representa el abono de los derechos, honorarios e indemnizaciones que le correspondan.

A su vez, el perito contará con otros derechos como pueden ser la propia aceptación del cargo y nombramiento como perito y a que no se perjudique su prestigio profesional [Car14]. Si esto ocurriera, podría llegar a imponerse una multa a la parte responsable.

D.2.2 Deberes

El deber fundamental del perito en un procedimiento civil es el de elaborar y emitir el dictamen correctamente, es decir, aplicando los conocimientos profesionales requeridos para el caso. Al emitir este dictamen, el perito tiene la obligación de prestar juramento o promesa de decir verdad y de actuar con la mayor objetividad posible, teniendo en cuenta tanto lo que favorezca como lo que pueda causar perjuicio a cualquiera de las partes, manifestando que conoce las sanciones penales a aplicar en el caso en que incumpla este deber (**art. 335 LEC**).

Una vez designado el perito, éste será comunicado por el Secretario judicial y se le requeri-

rá para aceptar el cargo en el plazo de dos días. Si lo aceptara, se efectuaría el nombramiento y realizaría el juramento o la promesa correspondiente. El perito únicamente podría quedar relevado de la obligación de aceptar su nombramiento en el caso en el que alegara una causa que le impidiera la aceptación y ésta fuera aceptada, siendo sustituido por el siguiente en la lista (**art. 342 LEC**).

Aportados los dictámenes, las partes podrán manifestar si desean la comparecencia de los peritos autores de los dictámenes en el juicio o vista del juicio verbal, con el objetivo de intervenir de cualquier forma útil para hacer entender el dictamen (**art. 337 LEC**). No obstante, el Tribunal podrá acordar en todo caso la presencia del perito (**art. 346 LEC**).

Para los casos en los que la intervención del perito sea necesaria, será obligatorio que éste comparezca en el día señalado para la celebración de la vista, a no ser que que concurra una causa de fuerza mayor u otro motivo de análoga entidad, que será comunicado al Tribunal y será solicitado un señalamiento de nueva vista, cuya fecha y hora serán comunicadas al Tribunal por parte del Secretario judicial (**arts. 183**, apartados **1** y **4**, y **430 LEC**).

Si la causa que provoca la situación de imposibilidad de comparecer fuera desestimada, el Tribunal mantendrá el señalamiento de la vista y el perito será notificado, requiriéndole comparecer (**art. 183.5 LEC**). Si el perito infringiera este deber, se le sancionaría con multa de 180 a 600 €, a la vez que se le requeriría que compareciese cuando se le citara de nuevo, bajo apercibimiento de proceder contra él por desobediencia a la autoridad (**art. 292 LEC**).

En el procedimiento penal, una vez nombrado, el perito deberá prestar juramento de proceder bien y fielmente con el único fin de descubrir y declarar la verdad (**art. 474 LECRIM**). Dicho nombramiento se le hará saber al perito por medio de oficio o, si la urgencia del caso lo exige, se podrá hacer el llamamiento verbalmente de orden del Juez (**arts. 460** y **461 LECRIM**).

En este caso, el perito tampoco podrá negarse a acudir al llamamiento para realizar un servicio pericial, a no ser que estuviese legítimamente impedido, en cuyo caso deberá ser comunicado al Juez en el acto de recibir el nombramiento, para que éste haga lo que crea conveniente (**art. 462 LECRIM**). Si se negara el perito a acudir a dicho llamamiento sin alegar excusa fundada, incurriría en la multa de 200 a 5000 € y si continuara negándose sería conducido a presencia del Juez instructor por los agentes de la autoridad, y perseguido por delito de obstrucción a la justicia, tipificado en el **art. 463.1 CP**, conforme a los **arts. 463**, **661** y **175.5 LECRIM**.

Si se considerara necesario, el Juez podría hacer las preguntas que estime oportunas o pedir las aclaraciones necesarias a los peritos con respecto a su informe. Las contestaciones de éstos formarán parte del informe también (**art. 483 LECRIM**).

Deberá también el perito guardar el secreto profesional, común a otras actividades pro-

fesionales, que en nuestro caso consistirá en que el perito mantenga en secreto cuestiones confidenciales que le hayan sido comunicadas por las partes, relacionadas con el estudio y resolución del caso, tanto previa como posteriormente a éste.

D.3 Capacitación profesional del perito

Para ejercer en los Juzgados y Tribunales españoles, un perito deberá poseer un título oficial relacionado con la materia objeto del dictamen y con la naturaleza de éste. Si se tratara de una materia no comprendida en un título oficial, se nombrarán personas entendidas en dichas materias (**art. 340 LEC**).

Tras esto, se seguirá el procedimiento para la designación judicial del perito, consistente en solicitar en el mes de enero de cada año a los distintos Colegios profesionales o a entidades análogas el envío de una lista de colegiados o asociados dispuestos a actuar como peritos, realizándose la primera designación de cada lista por sorteo y a partir de ahí en orden correlativo.

Si tuviera que designarse perito a una persona sin título oficial, se realizará mediante el mismo procedimiento comentado anteriormente, utilizándose una lista de personas que se solicitará anualmente a los sindicatos, asociaciones y entidades apropiadas, conforme al **art. 342 LEC**, la **instrucción 5/2001 de 19 de diciembre**, del Consejo General del Poder Judicial y el **Protocolo de 9 de febrero de 2005**, modificados estos dos documentos anteriores por el Acuerdo de 28 de octubre de 2010, del Pleno del Consejo General del Poder Judicial.

Todo lo anterior correspondería a un procedimiento civil, ahora bien, respecto a un procedimiento penal la LECRIM es más escueta: los peritos podrán ser nombrados de igual forma por el propio tribunal o a instancia de las partes. Podrán ser titulares o no, no obstante, el Juez se valdrá de los titulares con preferencia sobre los que no tuviesen título (**arts. 457** y **458 LECRIM**).

D.4 Responsabilidades del perito

Se tratarán en esta sección distintos tipo de responsabilidades del perito judicial, como pueden ser las responsabilidades civiles y la responsabilidades penales.

D.4.1 Responsabilidades civiles

Respecto a este tipo de responsabilidades, el perito será responsable de todo perjuicio y daño, tanto material como moral, causado a las partes o incluso a terceros como consecuencia de sus actos u omisión de éstos durante el reconocimiento o emisión del dictamen, como por ejemplo la destrucción de datos u objetos destinados a análisis [Car14].

Según el **art. 1902** del **Código Civil (CC)**, el que cause daño a otro por acción u omisión, interviniendo culpa o negligencia, tendrá que reparar el daño causado. Estas responsabilidades normalmente son extracontractuales cuando el perito sea designado judicialmente, ya

que aceptar éste el cargo no genera ninguna relación jurídica entre el perito y las partes, imposibilitando que éstas exijan la reparación de los daños provocados. Sin embargo, si se hubiera establecido un contrato entre el perito y su cliente, como ocurre cuando las partes son las que designan a los peritos, dicha relación jurídica existiría y conforme al **art. 1101 CC**, las partes podrían exigir la reparación de dichos daños.

D.4.2 Responsabilidades penales

Si el perito incumpliera su deber durante el desempeño de su profesión, podría incurrir en ciertas conductas constitutivas de infracción penal, que serán descritas a continuación.

Uno de los posibles delitos puede ser el de **cohecho**, consistente en sobornar o aceptar un soborno por parte de autoridades o funcionarios públicos, contemplado en los **arts. 419** a **422** del **Código Penal (CP)**. Este delito es también aplicable a peritos según lo establecido en el **art. 423 CP**.

Las sanciones impuestas serán variables:

- En el caso de recibir o solicitar cualquier tipo de soborno para realizar en el ejercicio de su cargo un acto contrario a sus deberes, no realizarlo o retrasarlo de forma injustificada, deberá hacer frente a una pena de prisión de tres a seis años, multa de doce a veinticuatro meses e inhabilitación al empleo por tiempo de siete a doce años **(art. 419 CP)**
- Si el soborno fuera recibido o solicitado para realizar un acto propio de su cargo, la pena de prisión sería de dos a cuatro años, la multa de doce a veinticuatro meses y la inhabilitación al empleo por tiempo de tres a siete años **(art. 420 CP)**
- En caso de ser recibido o solicitado como recompensa a las conductas citadas anteriormente, también serán aplicadas las penas señaladas **(art. 421 CP)**
- Si el soborno fuera admitido, la pena de prisión será de seis meses a un año y la suspensión de empleo y cargo se prolongará de uno a tres años **(art. 422 CP)**

También se le exigirá responsabilidad al perito si lleva a cabo alguna conducta de **falso testimonio**, imponiéndosele en su mitad superior las penas contempladas en el **art. 458 CP** a los peritos que falten a la verdad maliciosamente en su dictamen y además, una pena de inhabilitación especial para su profesión, empleo o cargo público por tiempo de seis a doce años **(art. 459 CP)**.

La dificultad en este supuesto consiste en demostrar que la falsedad testimonial del perito ha sido cometida maliciosamente, y no por simple negligencia, poca formación o falta de experiencia, etc.

Además, el perito puede también incurrir en falso testimonio si de forma maliciosa altera la verdad con inexactitudes, silenciando datos o hechos relevantes que estén en su conocimiento, etc., siendo castigado en este caso con la pena de multa de seis a doce meses y de

suspensión de empleo o cargo público, profesión u oficio por tiempo de seis meses a tres años **(art. 460 CP)**.

Solo quedará exento de pena aquel que se retracte, manifestando la verdad para que surta efecto antes de que se dicte sentencia. Si a consecuencia del falso testimonio se hubiese producido privación de libertad, se impondrán las penas correspondientes inferiores en grado **(art. 462 CP)**.

Por último, si el perito no compareciera por segunda vez después de ser citado a juicio, se procedería contra él por delito de **desobediencia a la autoridad**, del que se habla en el **art. 556 CP**, que castiga con la pena de prisión de seis meses a un año, siempre y cuando éste no acometa, intimide gravemente, emplee la fuerza ni haga resistencia activa grave contra la autoridad mientras ésta se halle ejecutando las funciones de sus cargos **(art. 550 CP)**.

Anexo E

Legislación aplicable

Este anexo irá dedicado a recoger todos los artículos referidos a lo largo de todo el documento, pertenecientes a textos legales, de forma que el lector se ahorrará tener que ir a una fuente externa para su consulta.

E.1 Constitución Española (CE)

Artículo 24.2

> Asimismo, todos tienen derecho al Juez ordinario predeterminado por la ley, a la defensa y a la asistencia de letrado, a ser informados de la acusación formulada contra ellos, a un proceso público sin dilaciones indebidas y con todas las garantías, a utilizar los medios de prueba pertinentes para su defensa, a no declarar contra sí mismos, a no confesarse culpables y a la presunción de inocencia.

E.2 Código Civil (CC)

Artículo 1101

> Quedan sujetos a la indemnización de los daños y perjuicios causados los que en el cumplimiento de sus obligaciones incurrieren en dolo, negligencia o morosidad, y los que de cualquier modo contravinieren al tenor de aquéllas.

Artículo 1902

> El que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado.

E.3 Código Penal (CP)

Artículo 419

> La autoridad o funcionario público que, en provecho propio o de un tercero, recibiere o solicitare, por sí o por persona interpuesta, dádiva, favor o retribución de cualquier clase o aceptare ofrecimiento o promesa para realizar en el ejercicio de su cargo un acto contrario a los deberes inherentes al mismo o para no realizar o retrasar injustificadamente el que debiera practicar, incurrirá en la pena de prisión de tres a seis años, multa de doce a veinticuatro meses e inhabilitación especial para empleo o cargo público por

tiempo de siete a doce años, sin perjuicio de la pena correspondiente al acto realizado, omitido o retrasado en razón de la retribución o promesa, si fuera constitutivo de delito.

Artículo 420

La autoridad o funcionario público que, en provecho propio o de un tercero, recibiere o solicitare, por sí o por persona interpuesta, dádiva, favor o retribución de cualquier clase o aceptare ofrecimiento o promesa para realizar un acto propio de su cargo, incurrirá en la pena de prisión de dos a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para empleo o cargo público por tiempo de tres a siete años.

Artículo 421

Las penas señaladas en los artículos precedentes se impondrán también cuando la dádiva, favor o retribución se recibiere o solicitare por la autoridad o funcionario público, en sus respectivos casos, como recompensa por la conducta descrita en dichos artículos.

Artículo 422

La autoridad o funcionario público que, en provecho propio o de un tercero, admitiera, por sí o por persona interpuesta, dádiva o regalo que le fueren ofrecidos en consideración a su cargo o función, incurrirá en la pena de prisión de seis meses a un año y suspensión de empleo y cargo público de uno a tres años.

Artículo 423

Lo dispuesto en los artículos precedentes será igualmente aplicable a los jurados, árbitros, peritos, administradores o interventores designados judicialmente, o a cualesquiera personas que participen en el ejercicio de la función pública.

Artículo 458

1. El testigo que faltare a la verdad en su testimonio en causa judicial, será castigado con las penas de prisión de seis meses a dos años y multa de tres a seis meses
2. Si el falso testimonio se diera en contra del reo en causa criminal por delito, las penas serán de prisión de uno a tres años y multa de seis a doce meses. Si a consecuencia del testimonio hubiera recaído sentencia condenatoria, se impondrán las penas superiores en grado
3. Las mismas penas se impondrán si el falso testimonio tuviera lugar ante Tribunales Internacionales que, en virtud de Tratados debidamente ratificados conforme a la Constitución Española, ejerzan competencias derivadas de ella, o se realizara en España al declarar en virtud de comisión rogatoria remitida por un Tribunal extranjero

Artículo 459

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

Artículo 460

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

Artículo 462

Quedará exento de pena el que, habiendo prestado un falso testimonio en causa criminal, se retracte en tiempo y forma, manifestando la verdad para que surta efecto antes de que se dicte sentencia en el proceso de que se trate. Si a consecuencia del falso testimonio, se hubiese producido la privación de libertad, se impondrán las penas correspondientes inferiores en grado.

Artículo 463.1

El que, citado en legal forma, dejare voluntariamente de comparecer, sin justa causa, ante un juzgado o tribunal en proceso criminal con reo en prisión provisional, provocando la suspensión del juicio oral, será castigado con la pena de prisión de tres a seis meses o multa de seis a 24 meses. En la pena de multa de seis a 10 meses incurrirá el que, habiendo sido advertido, lo hiciera por segunda vez en causa criminal sin reo en prisión, haya provocado o no la suspensión.

Artículo 550

Son reos de atentado los que acometan a la autoridad, a sus agentes o funcionarios públicos, o empleen fuerza contra ellos, los intimiden gravemente o les hagan resistencia activa también grave, cuando se hallen ejecutando las funciones de sus cargos o con ocasión de ellas.

Artículo 556

Los que, sin estar comprendidos en el artículo 550, resistieren a la autoridad o sus agentes, o los desobedecieren gravemente, en el ejercicio de sus funciones, serán castigados con la pena de prisión de seis meses a un año.

E.4 Ley de Enjuiciamiento Criminal (LECrim)

Artículo 175.5

La obligación, si la hubiere, de concurrir al primer llamamiento, bajo la multa de 200 a 5.000 euros o si fuese ya el segundo el que se hiciere, la de concurrir bajo apercibi-

miento de ser perseguido como reo del delito de obstrucción a la justicia tipificado en el artículo 463.1 del Código Penal.

Artículo 242

Cuando se declaren de oficio las costas no habrá lugar al pago de las cantidades a que se refiere los números 1 y 2 del artículo anterior.

Los Procuradores y Abogados que hubiesen representado y defendido a cualquiera de las partes, y los Peritos y testigos que hubiesen declarado a su instancia, podrán exigir de aquélla, si no se le hubiere reconocido el derecho a la asistencia jurídica gratuita, el abono de los derechos, honorarios e indemnizaciones que les correspondieren, reclamándolos del Juez o Tribunal que conociese de la causa.

Se procederá a su exacción por la vía de apremio si, presentadas las respectivas reclamaciones y hechas saber a las partes, no pagasen éstas en el término prudencial que el Secretario judicial señale, ni tacharen aquéllas de indebidas o excesivas. En este último caso se procederá con arreglo a lo dispuesto en la Ley de Enjuiciamiento Civil.

El Secretario judicial que interviniere en la ejecución de la sentencia hará la tasación de las costas de que habla el número 1 y 2 del artículo anterior. Los honorarios de los Abogados y Peritos se acreditarán por minutas firmadas por los que los hubiesen devengado. Las indemnizaciones de los testigos se computarán por la cantidad que oportunamente se hubiese fijado en la causa. Los demás gastos serán regulados por el Secretario judicial, con vista de los justificantes.

Artículo 282

La Policía judicial tiene por objeto, y será obligación de todos los que la componen, averiguar los delitos públicos que se cometieren en su territorio o demarcación; practicar, según sus atribuciones, las diligencias necesarias para comprobarlos y descubrir a los delincuentes, y recoger todos los efectos, instrumentos o pruebas del delito de cuya desaparición hubiere peligro, poniéndolos a disposición de la Autoridad judicial.

Si el delito fuera de los que sólo pueden perseguirse a instancia de parte legítima, tendrán la misma obligación expresada en el párrafo anterior, si se les requiere al efecto. La ausencia de denuncia no impedirá la práctica de las primeras diligencias de prevención y aseguramiento de los delitos relativos a la propiedad intelectual e industrial.

Artículo 292

Los funcionarios de Policía judicial extenderán, bien en papel sellado, bien en papel común, un atestado de las diligencias que practiquen, en el cual especificarán con la mayor exactitud los hechos por ellos averiguados, insertando las declaraciones e informes recibidos y anotando todas las circunstancias que hubiesen observado y pudiesen ser prueba o indicio del delito. La Policía Judicial remitirá con el atestado un informe dando cuenta de las detenciones anteriores y de la existencia de requisitorias para su

llamamiento y busca cuando así conste en sus bases de datos.

Artículo 326

Cuando el delito que se persiga haya dejado vestigios o pruebas materiales de su perpetración, el Juez instructor o el que haga sus veces ordenará que se recojan y conserven para el juicio oral si fuere posible, procediendo al efecto a la inspección ocular y a la descripción de todo aquello que pueda tener relación con la existencia y naturaleza del hecho.

A este fin, hará consignar en los autos la descripción del lugar del delito, el sitio y estado en que se hallen los objetos que en él se encuentren, los accidentes del terreno o situación de las habitaciones y todos los demás detalles que puedan utilizarse, tanto para la acusación como para la defensa.

Cuando se pusiera de manifiesto la existencia de huellas o vestigios cuyo análisis biológico pudiera contribuir al esclarecimiento del hecho investigado, el Juez de Instrucción adoptará u ordenará a la Policía Judicial o al médico forense que adopte las medidas necesarias para que la recogida, custodia y examen de aquellas muestras se verifique en condiciones que garanticen su autenticidad, sin perjuicio de lo establecido en el artículo 282.

Artículo 330

Cuando no hayan quedado huellas o vestigios del delito que hubiese dado ocasión al sumario, el Juez instructor averiguará y hará constar, siendo posible, si la desaparición de las pruebas materiales ha ocurrido natural, casual o intencionadamente, y las causas de la misma o los medios que para ello se hubieren empleado, procediendo seguidamente a recoger y consignar en el sumario las pruebas de cualquiera clase que se puedan adquirir acerca de la perpetración del delito.

Artículo 334

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

La diligencia será firmada por la persona en cuyo poder fueren hallados, notificándose a la misma el auto en que se mande recogerlos.

Artículo 338

Sin perjuicio de lo establecido en el Capítulo II bis del presente título, los instrumentos, armas y efectos a que se refiere el artículo 334 se recogerán de tal forma que se garantice su integridad y el Juez acordará su retención, conservación o envío al organismo

adecuado para su depósito.

Artículo 388

En la primera declaración será preguntado el procesado por su nombre, apellidos paterno y materno, apodo, si lo tuviere, edad, naturaleza, vecindad, estado, profesión, arte, oficio o modo de vivir, si tiene hijos, si fue procesado anteriormente, por qué delito, ante qué Juez o Tribunal, qué pena se le impuso, si la cumplió, si sabe leer y escribir y si conoce el motivo por que se le ha procesado.

Artículo 456

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

Artículo 457

Los peritos pueden ser o no titulares. Son peritos titulares los que tienen título oficial de una ciencia o arte cuyo ejercicio esté reglamentado por la Administración. Son peritos no titulares los que, careciendo de título oficial, tienen, sin embargo, conocimiento o prácticas especiales en alguna ciencia o arte.

Artículo 458

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

Artículo 460

El nombramiento se hará saber a los peritos por medio de oficio, que les será entregado por alguacil o portero del Juzgado, con las formalidades prevenidas para la citación de los testigos, reemplazándose la cédula original, para los efectos del artículo 175, por un atestado que extenderá el alguacil o portero encargado de la entrega.

Artículo 461

Si la urgencia del caso lo exige, podrá hacerse el llamamiento verbalmente de orden del Juez, haciéndolo constar así en los autos; pero extendiendo siempre el atestado prevenido en el artículo anterior el encargado del cumplimiento de la orden de llamamiento.

Artículo 462

Nadie podrá negarse a acudir al llamamiento del Juez para desempeñar un servicio pericial, si no estuviese legítimamente impedido. En este caso deberá ponerlo en conocimiento del Juez en el acto de recibir el nombramiento, para que se provea a lo que haya lugar.

Artículo 463

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

Artículo 465

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

Artículo 474

Antes de darse principio al acto pericial, todos los peritos, así los nombrados por el Juez como los que lo hubieren sido por las partes, prestarán juramento, conforme al artículo 434, de proceder bien y fielmente en sus operaciones y de no proponerse otro fin más que el de descubrir y declarar la verdad.

Artículo 478

El informe pericial comprenderá, si fuere posible:

- 1.º Descripción de la persona o cosa que sea objeto del mismo en el estado o del modo en que se halle. El Secretario extenderá esta descripción, dictándola los peritos y suscribiéndola todos los concurrentes.
- 2.º Relación detallada de todas las operaciones practicadas por los peritos y de su resultado, extendida y autorizada en la misma forma que la anterior.
- 3.º Las conclusiones que en vista de tales datos formulen los peritos conforme a los principios y reglas de su ciencia o arte.

Artículo 483

El Juez podrá, por su propia iniciativa o por reclamación de las partes presentes o de sus defensores, hacer a los peritos, cuando produzcan sus conclusiones, las preguntas que estime pertinentes y pedirles las aclaraciones necesarias. Las contestaciones de los peritos se considerarán como parte de su informe.

Artículos 650.1º y 4º

El escrito de calificación se limitará a determinar en conclusiones precisas y numeradas:

- 1.º Los hechos punibles que resulten del sumario.
- 4.º Los hechos que resulten del sumario y que constituyan circunstancias atenuantes o agravantes del delito o eximentes de responsabilidad criminal.

Artículo 656

El Ministerio Fiscal y las partes manifestarán en sus respectivos escritos de calificación las pruebas de que intenten valerse, presentando listas de peritos y testigos que hayan de declarar a su instancia.

En las listas de peritos y testigos se expresarán sus nombres y apellidos, el apodo, si por él fueren conocidos, y su domicilio o residencia; manifestando además la parte que

los presente si los peritos y testigos han de ser citados judicialmente o si se encarga de hacerles concurrir.

Artículo 657

Cada parte presentará tantas copias de las listas de peritos y testigos cuantas sean las demás personadas en la causa, a cada una de las cuales se entregará una de dichas copias en el mismo día en que fueren presentadas.

Las listas originales se unirán a la causa.

Podrán pedir además las partes que se practiquen desde luego aquellas diligencias de prueba que por cualquier causa fuera de temer que no se puedan practicar en el juicio oral, o que pudieran motivar su suspensión.

Artículo 658

Presentados los escritos de calificación, o recogida la causa de poder de quien la tuviere después de transcurrido el término señalado en el artículo 649, el Secretario judicial dictará diligencia teniendo por hecha la calificación, y acordará pasar la causa al ponente, por término de tercer día, para el examen de las pruebas propuestas.

Artículo 659

Devuelta que sea la causa por el Ponente, el Tribunal examinará las pruebas propuestas e inmediatamente dictará auto, admitiendo las que considere pertinentes y rechazando las demás.

Para rechazar las propuestas por el acusador privado, habrá de ser oído el Fiscal si interviniere en la causa.

Contra la parte del auto admitiendo las pruebas o mandando practicar la que se hallare en el caso del párrafo tercero del artículo 657 no procederá recurso alguno.

Contra la en que fuere rechazada o denegada la práctica de las diligencias de prueba podrá interponerse en su día el recurso de casación, si se prepara oportunamente con la correspondiente protesta.

A la vista de este Auto, el Secretario judicial establecerá el día y hora en que deban comenzar las sesiones del juicio oral, con sujeción a lo establecido en el artículo 182 de la Ley de Enjuiciamiento Civil.

Los criterios generales y las concretas y específicas instrucciones que fijen los Presidentes de Sala o Sección, con arreglo a los cuales se realizará el señalamiento, tendrán asimismo en cuenta:

- 1.º La prisión del acusado;
- 2.º El aseguramiento de su presencia a disposición judicial;
- 3.º Las demás medidas cautelares personales adoptadas;
- 4.º La prioridad de otras causas;

- 5.º La complejidad de la prueba propuesta o cualquier circunstancia modificativa, según hayan podido determinar una vez estudiado el asunto o pleito de que se trate.

En todo caso, aunque no sea parte en el proceso ni deba intervenir, el Secretario judicial deberá informar a la víctima por escrito de la fecha y lugar de celebración del juicio.

Artículo 661

Las citaciones de peritos y testigos se practicarán en la forma establecida en el título VII del libro I.

Los peritos y testigos citados que no comparezcan, sin causa legítima que se lo impida, incurrirán en la multa señalada en el número 5.º del artículo 175.

Si vueltos a citar dejaren también de comparecer, serán procesados por el delito de obstrucción a la justicia, tipificado en el artículo 463.1 del Código Penal.

Artículo 688

En el día señalado para dar principio a las sesiones, el Secretario judicial velará por que se encuentren en el local del Tribunal las piezas de convicción que se hubieren recogido, y el Presidente, en el momento oportuno, declarará abierta la sesión.

Si la causa que haya de verse fuese por delito para cuyo castigo se pida la imposición de pena correccional, preguntará el Presidente a cada uno de los acusados si se confiesa reo del delito que se le haya imputado en el escrito de calificación, y responsable civilmente a la restitución de la cosa o al pago de la cantidad fijada en dicho escrito por razón de daños y perjuicios.

Artículo 689

Si en la causa hubiere, además de la calificación fiscal, otra del querellante particular o diversas calificaciones de querellantes de esta clase, se preguntará al procesado si se confiesa reo del delito, según la calificación más grave, y civilmente responsable por la cantidad mayor que se hubiese fijado.

Artículo 690

Si fueren más de uno los delitos imputados al procesado en el escrito de calificación, se le harán las mismas preguntas respecto de cada cual.

Artículo 723

Los peritos podrán ser recusados por las causas y en la forma prescrita en los artículos 468, 469 y 470.

La sustanciación de los incidentes de recusación tendrá lugar precisamente en el tiempo que media desde la admisión de las pruebas propuestas por las partes hasta la apertura de las sesiones.

Artículo 724

Los peritos que no hayan sido recusados serán examinados juntos cuando deban declarar sobre unos mismos hechos, y contestarán a las preguntas y repreguntas que las partes les dirijan.

Artículo 726

El Tribunal examinará por sí mismo los libros, documentos, papeles y demás piezas de convicción que puedan contribuir al esclarecimiento de los hechos o a la más segura investigación de la verdad.

Artículo 727

Para la prueba de inspección ocular que no se haya practicado antes de la apertura de las sesiones, si el lugar que deba ser inspeccionado se hallase en la capital, se constituirá en él el Tribunal con las partes, y el Secretario extenderá diligencia expresiva del lugar o cosa inspeccionada, haciendo constar en ella las observaciones de las partes y demás incidentes que ocurran.

Si el lugar estuviere fuera de la capital, se constituirá en él con las partes el individuo del Tribunal que el Presidente designe, practicándose las diligencias en la forma establecida en el párrafo anterior.

En todo lo demás se estará, en cuanto fuere necesario, a lo dispuesto en el título V, capítulo I del libro II.

Artículo 730

Podrán también leerse a instancia de cualquiera de las partes las diligencias practicadas en el sumario, que, por causas independientes de la voluntad de aquéllas, no puedan ser reproducidas en el juicio oral.

Artículo 741

El Tribunal, apreciando según su conciencia las pruebas practicadas en el juicio, las razones expuestas por la acusación y la defensa y lo manifestado por los mismos procesados, dictará sentencia dentro del término fijado en esta Ley.

Siempre que el Tribunal haga uso del libre arbitrio que para la calificación del delito o para la imposición de la pena le otorga el Código Penal, deberá consignar si ha tomado en consideración los elementos de juicio que el precepto aplicable de aquél obligue a tener en cuenta.

Artículo 781.1

El escrito de acusación comprenderá, además de la solicitud de apertura del juicio oral ante el órgano que se estime competente y de la identificación de la persona o personas contra las que se dirige la acusación, los extremos a que se refiere el artículo 650. La acusación se extenderá a las faltas imputables al acusado del delito o a otras personas, cuando la comisión de la falta o su prueba estuviera relacionada con el delito. También

se expresarán la cuantía de las indemnizaciones o se fijarán las bases para su determinación y las personas civilmente responsables, así como los demás pronunciamientos sobre entrega y destino de cosas y efectos e imposición de costas procesales.

En el mismo escrito se propondrán las pruebas cuya práctica se interese en el juicio oral, expresando si la reclamación de documentos o las citaciones de peritos y testigos deben realizarse por medio de la oficina judicial.

En el escrito de acusación se podrá solicitar la práctica anticipada de aquellas pruebas que no puedan llevarse a cabo durante las sesiones del juicio oral, así como la adopción, modificación o suspensión de las medidas a que se refieren los artículos 763, 764 y 765, o cualesquiera otras que resulten procedentes o se hubieren adoptado, así como la cancelación de las tomadas frente a personas contra las que no se dirija acusación.

Artículo 784.1 y 2

1. Abierto el juicio oral, el Secretario judicial emplazará al imputado, con entrega de copia de los escritos de acusación, para que en el plazo de tres días comparezca en la causa con Abogado que le defienda y Procurador que le represente. Si no ejercitase su derecho a designar Procurador o a solicitar uno de oficio, el Secretario judicial interesará, en todo caso, su nombramiento. Cumplido ese trámite, el Secretario judicial dará traslado de las actuaciones originales, o mediante fotocopia, a los designados como acusados y terceros responsables en los escritos de acusación, para que en plazo común de diez días presenten escrito de defensa frente a las acusaciones formuladas.

   Si la defensa no presentare su escrito en el plazo señalado, se entenderá que se opone a las acusaciones y seguirá su curso el procedimiento, sin perjuicio de la responsabilidad en que pueda incurrirse de acuerdo con lo previsto en el Título V del Libro V de la Ley Orgánica del Poder Judicial.

   Una vez precluido el trámite para presentar su escrito, la defensa sólo podrá proponer la prueba que aporte en el acto del juicio oral para su práctica en el mismo, sin perjuicio de que, además, pueda interesar previamente que se libren las comunicaciones necesarias, siempre que lo haga con antelación suficiente respecto de la fecha señalada para el juicio, y de lo previsto en el párrafo segundo del apartado 1 del artículo 785. Todo ello se entiende sin perjuicio de que si los afectados consideran que se ha producido indefensión puedan aducirlo de acuerdo con lo previsto en el apartado 2 del artículo 786.
2. En el escrito de defensa se podrá solicitar del órgano judicial que recabe la remisión de documentos o cite a peritos o testigos, a los efectos de la práctica de la correspondiente prueba en las sesiones del juicio oral o, en su caso, de la práctica de prueba anticipada.

Artículo 785.1

En cuanto las actuaciones se encontraren a disposición del órgano competente para el enjuiciamiento, el Juez o Tribunal examinará las pruebas propuestas e inmediatamente dictará auto admitiendo las que considere pertinentes y rechazando las demás, y prevendrá lo necesario para la práctica de la prueba anticipada.

Contra los autos de admisión o inadmisión de pruebas no cabrá recurso alguno, sin perjuicio de que la parte a la que fue denegada pueda reproducir su petición al inicio de las sesiones del juicio oral, momento hasta el cual podrán incorporarse a la causa los informes, certificaciones y demás documentos que el Ministerio Fiscal y las partes estimen oportuno y el Juez o Tribunal admitan.

Artículo 788.2

El informe pericial podrá ser prestado sólo por un perito.

En el ámbito de este procedimiento, tendrán carácter de prueba documental los informes emitidos por laboratorios oficiales sobre la naturaleza, cantidad y pureza de sustancias estupefacientes cuando en ellos conste que se han realizado siguiendo los protocolos científicos aprobados por las correspondientes normas.

Artículo 790.6

Presentados los escritos de alegaciones o precluido el plazo para hacerlo, el Secretario, en los dos días siguientes, dará traslado de cada uno de ellos a las demás partes y elevará a la Audiencia los autos originales con todos los escritos presentados.

Artículo 792.1

La sentencia de apelación se dictará dentro de los cinco días siguientes a la vista oral, o dentro de los diez días siguientes a la recepción de las actuaciones por la Audiencia, cuando no hubiere resultado procedente su celebración.

Artículo 849

Se entenderá que ha sido infringida la Ley para el efecto de que pueda interponerse el recurso de casación:

- 1.º Cuando, dados los hechos que se declaren probados en las resoluciones comprendidas en los dos artículos anteriores, se hubiere infringido un precepto penal de carácter sustantivo u otra norma jurídica del mismo carácter que deba ser observada en la aplicación de la Ley penal.
- 2.º Cuando haya existido error en la apreciación de la prueba, basado en documentos que obren en autos, que demuestren la equivocación del juzgador sin resultar contradichos por otros elementos probatorios.

Artículo 850.1º

El recurso de casación podrá interponerse por quebrantamiento de forma:

- 1.º Cuando se haya denegado alguna diligencia de prueba que, propuesta en tiempo y forma por las partes, se considere pertinente.

E.5 Ley de Enjuiciamiento Civil (LEC)

Artículo 183.1, 4 y 5

1. Si a cualquiera de los que hubieren de acudir a una vista le resultare imposible asistir a ella en el día señalado, por causa de fuerza mayor u otro motivo de análoga entidad, lo manifestará de inmediato al Tribunal, acreditando cumplidamente la causa o motivo y solicitando señalamiento de nueva vista o resolución que atienda a la situación.
2. El Secretario judicial pondrá en conocimiento del Tribunal la fecha y hora fijadas para el nuevo señalamiento, en el mismo día o en el día hábil siguiente a aquél en que hubiera sido acordado.
3. Cuando un testigo o perito que haya sido citado a vista por el Tribunal manifieste y acredite encontrarse en la misma situación de imposibilidad expresada en el primer apartado de este precepto, el Secretario judicial dispondrá que se oiga a las partes por plazo común de tres días sobre si se deja sin efecto el señalamiento de la vista y se efectúa uno nuevo o si se cita al testigo o perito para la práctica de la actuación probatoria fuera de la vista señalada. Transcurrido el plazo, el Tribunal decidirá lo que estime conveniente, y si no considerase atendible o acreditada la excusa del testigo o del perito, mantendrá el señalamiento de la vista y el Secretario judicial lo notificará así a aquéllos, requiriéndoles a comparecer, con el apercibimiento que prevé el apartado segundo del artículo 292.

Artículo 241

1. Salvo lo dispuesto en la Ley de Asistencia Jurídica Gratuita, cada parte pagará los gastos y costas del proceso causados a su instancia a medida que se vayan produciendo. Se considerarán gastos del proceso aquellos desembolsos que tengan su origen directo e inmediato en la existencia de dicho proceso, y costas la parte de aquéllos que se refieran al pago de los siguientes conceptos:
   - 1.º Honorarios de la defensa y de la representación técnica cuando sean preceptivas.
   - 2.º Inserción de anuncios o edictos que de forma obligada deban publicarse en el curso del proceso.
   - 3.º Depósitos necesarios para la presentación de recursos.
   - 4.º Derechos de peritos y demás abonos que tengan que realizarse a personas que hayan intervenido en el proceso.

- 5.º Copias, certificaciones, notas, testimonios y documentos análogos que hayan de solicitarse conforme a la Ley, salvo los que se reclamen por el tribunal a registros y protocolos públicos, que serán gratuitos.
- 6.º Derechos arancelarios que deban abonarse como consecuencia de actuaciones necesarias para el desarrollo del proceso.
- 7.º La tasa por el ejercicio de la potestad jurisdiccional, cuando sea preceptiva. No se incluirá en las costas del proceso el importe de la tasa abonada en los procesos de ejecución de las hipotecas constituidas para la adquisición de vivienda habitual. Tampoco se incluirá en los demás procesos de ejecución derivados de dichos préstamos o créditos hipotecarios cuando se dirijan contra el propio ejecutado o contra los avalistas.

2. Los titulares de créditos derivados de actuaciones procesales podrán reclamarlos de la parte o partes que deban satisfacerlos sin esperar a que el proceso finalice y con independencia del eventual pronunciamiento sobre costas que en éste recaiga.

Artículo 292

1. Los testigos y los peritos citados tendrán el deber de comparecer en el juicio o vista que finalmente se hubiese señalado. La infracción de este deber se sancionará por el Tribunal, previa audiencia por cinco días, con multa de ciento ochenta a seiscientos euros.
2. Al tiempo de imponer la multa a que se refiere el apartado anterior, el Tribunal requerirá, mediante providencia, al multado para que comparezca cuando se le cite de nuevo por el Secretario judicial, bajo apercibimiento de proceder contra él por desobediencia a la autoridad.
3. Cuando, sin mediar previa excusa, un testigo o perito no compareciere al juicio o vista, el tribunal, oyendo a las partes que hubiesen comparecido, decidirá, mediante providencia, si la audiencia ha de suspenderse o debe continuar.
4. Cuando, también sin mediar previa excusa, no compareciere un litigante que hubiese sido citado para responder a interrogatorio, se estará a lo dispuesto en el artículo 304 y se impondrá a aquél la multa prevista en el apartado 1 de este artículo.

Artículo 335

1. Cuando sean necesarios conocimientos científicos, artísticos, técnicos o prácticos para valorar hechos o circunstancias relevantes en el asunto o adquirir certeza sobre ellos, las partes podrán aportar al proceso el dictamen de peritos que posean

los conocimientos correspondientes o solicitar, en los casos previstos en esta ley, que se emita dictamen por perito designado por el tribunal.

2. Al emitir el dictamen, todo perito deberá manifestar, bajo juramento o promesa de decir verdad, que ha actuado y, en su caso, actuará con la mayor objetividad posible, tomando en consideración tanto lo que pueda favorecer como lo que sea susceptible de causar perjuicio a cualquiera de las partes, y que conoce las sanciones penales en las que podría incurrir si incumpliere su deber como perito.
3. Salvo acuerdo en contrario de las partes, no se podrá solicitar dictamen a un perito que hubiera intervenido en una mediación o arbitraje relacionados con el mismo asunto.

Artículo 337

1. Si no les fuese posible a las partes aportar dictámenes elaborados por peritos por ellas designados, junto con la demanda o contestación, expresarán en una u otra los dictámenes de que, en su caso, pretendan valerse, que habrán de aportar, para su traslado a la parte contraria, en cuanto dispongan de ellos, y en todo caso cinco días antes de iniciarse la audiencia previa al juicio ordinario o de la vista en el verbal.
2. Aportados los dictámenes conforme a lo dispuesto en el apartado anterior, las partes habrán de manifestar si desean que los peritos autores de los dictámenes comparezcan en el juicio regulado en los artículos 431 y siguientes de esta Ley o, en su caso, en la vista del juicio verbal, expresando si deberán exponer o explicar el dictamen o responder a preguntas, objeciones o propuestas de rectificación o intervenir de cualquier otra forma útil para entender y valorar el dictamen en relación con lo que sea objeto del pleito.

Artículo 339.2

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

Salvo que se refiera a alegaciones o pretensiones no contenidas en la demanda, no se podrá solicitar, con posterioridad a la demanda o a la contestación o una vez transcurrido el plazo señalado en los apartados 1 y 2 de este artículo para la prueba pericial de los juicios verbales sin contestación escrita, informe pericial elaborado por perito

designado judicialmente.

La designación judicial de perito deberá realizarse en el plazo de cinco días desde la presentación de la contestación a la demanda, con independencia de quien haya solicitado dicha designación, o en el plazo de dos días a contar desde la presentación de la solicitud en los supuestos contemplados en el párrafo segundo del apartado 1 y en el apartado 2 de este precepto. Cuando ambas partes la hubiesen pedido inicialmente, el Tribunal podrá designar, si aquéllas se muestran conformes, un único perito que emita el informe solicitado. En tal caso, el abono de los honorarios del perito corresponderá realizarlo a ambos litigantes por partes iguales, sin perjuicio de lo que pudiere acordarse en materia de costas.

Artículo 340

1. Los peritos deberán poseer el título oficial que corresponda a la materia objeto del dictamen y a la naturaleza de éste. Si se tratare de materias que no estén comprendidas en títulos profesionales oficiales, habrán de ser nombrados entre personas entendidas en aquellas materias.
2. Podrá asimismo solicitarse dictamen de Academias e instituciones culturales y científicas que se ocupen del estudio de las materias correspondientes al objeto de la pericia. También podrán emitir dictamen sobre cuestiones específicas las personas jurídicas legalmente habilitadas para ello.
3. En los casos del apartado anterior, la institución a la que se encargue el dictamen expresará a la mayor brevedad qué persona o personas se encargarán directamente de prepararlo, a las que se exigirá el juramento o promesa previsto en el apartado segundo del artículo 335.

Artículo 342

1. En el mismo día o siguiente día hábil a la designación, el Secretario judicial comunicará ésta al perito titular, requiriéndole para que en el plazo de dos días manifieste si acepta el cargo. En caso afirmativo, se efectuará el nombramiento y el perito hará, en la forma en que se disponga, la manifestación bajo juramento o promesa que ordena el apartado 2 del artículo 335.
2. Si el perito designado adujere justa causa que le impidiere la aceptación, y el Secretario judicial la considerare suficiente, será sustituido por el siguiente de la lista, y así sucesivamente, hasta que se pudiere efectuar el nombramiento.
3. El perito designado podrá solicitar, en los tres días siguientes a su nombramiento, la provisión de fondos que considere necesaria, que será a cuenta de la liquidación final. El Secretario judicial, mediante decreto, decidirá sobre la provisión

solicitada y ordenará a la parte o partes que hubiesen propuesto la prueba pericial y no tuviesen derecho a la asistencia jurídica gratuita, que procedan a abonar la cantidad fijada en la Cuenta de Depósitos y Consignaciones del Tribunal, en el plazo de cinco días.

Transcurrido dicho plazo, si no se hubiere depositado la cantidad establecida, el perito quedará eximido de emitir el dictamen, sin que pueda procederse a una nueva designación.

Cuando el perito designado lo hubiese sido de común acuerdo, y uno de los litigantes no realizare la parte de la consignación que le correspondiere, el Secretario judicial ofrecerá al otro litigante la posibilidad de completar la cantidad que faltare, indicando en tal caso los puntos sobre los que deba pronunciarse el dictamen, o de recuperar la cantidad depositada, en cuyo caso se aplicará lo dispuesto en el párrafo anterior.

Artículo 343

1. Sólo podrán ser objeto de recusación los peritos designados judicialmente. En cambio, los peritos no recusables podrán ser objeto de tacha cuando concurra en ellos alguna de las siguientes circunstancias:
   - 1.º Ser cónyuge o pariente por consanguinidad o afinidad, dentro del cuarto grado civil de una de las partes o de sus abogados o procuradores.
   - 2.º Tener interés directo o indirecto en el asunto o en otro semejante.
   - 3.º Estar o haber estado en situación de dependencia o de comunidad o contraposición de intereses con alguna de las partes o con sus abogados o procuradores.
   - 4.º Amistad íntima o enemistad con cualquiera de las partes o sus procuradores o abogados.
   - 5.º Cualquier otra circunstancia, debidamente acreditada, que les haga desmerecer en el concepto profesional.
2. Las tachas no podrán formularse después del juicio o de la vista, en los juicios verbales. Si se tratare de juicio ordinario, las tachas de los peritos autores de dictámenes aportados con demanda o contestación se propondrán en la audiencia previa al juicio.

   Al formular tachas de peritos, se podrá proponer la prueba conducente a justificarlas, excepto la testifical.

Artículo 346

El perito que el Tribunal designe emitirá por escrito su dictamen, que hará llegar al Tribunal en el plazo que se le haya señalado. De dicho dictamen se dará traslado por el Secretario judicial a las partes por si consideran necesario que el perito concurra

al juicio o a la vista a los efectos de que aporte las aclaraciones o explicaciones que sean oportunas. El Tribunal podrá acordar, en todo caso, mediante providencia, que considera necesaria la presencia del perito en el juicio o la vista para comprender y valorar mejor el dictamen realizado.

Artículo 347

1. Los peritos tendrán en el juicio o en la vista la intervención solicitada por las partes, que el tribunal admita.

   El tribunal sólo denegará las solicitudes de intervención que, por su finalidad y contenido, hayan de estimarse impertinentes o inútiles, o cuando existiera un deber de confidencialidad derivado de la intervención del perito en un procedimiento de mediación anterior entre las partes.

   En especial, las partes y sus defensores podrán pedir:

   - 1.º Exposición completa del dictamen, cuando esa exposición requiera la realización de otras operaciones, complementarias del escrito aportado, mediante el empleo de los documentos, materiales y otros elementos a que se refiere el apartado 2 del artículo 336.
   - 2.º Explicación del dictamen o de alguno o algunos de sus puntos, cuyo significado no se considerase suficientemente expresivo a los efectos de la prueba.
   - 3.º Respuestas a preguntas y objeciones, sobre método, premisas, conclusiones y otros aspectos del dictamen.
   - 4.º Respuestas a solicitudes de ampliación del dictamen a otros puntos conexos, por si pudiera llevarse a cabo en el mismo acto y a efectos, en cualquier caso, de conocer la opinión del perito sobre la posibilidad y utilidad de la ampliación, así como del plazo necesario para llevarla a cabo.
   - 5.º Crítica del dictamen de que se trate por el perito de la parte contraria.
   - 6.º Formulación de las tachas que pudieren afectar al perito.

2. El tribunal podrá también formular preguntas a los peritos y requerir de ellos explicaciones sobre lo que sea objeto del dictamen aportado, pero sin poder acordar, de oficio, que se amplíe, salvo que se trate de peritos designados de oficio conforme a lo dispuesto en el apartado 5 del artículo 339.

Artículo 430

Si cualquiera de los que hubieren de acudir al acto del juicio no pudiere asistir a éste por causa de fuerza mayor u otro motivo de análoga entidad podrá solicitar nuevo señalamiento de juicio. Esta solicitud se sustanciará y resolverá conforme a lo previsto en el artículo 183.

Anexo F

Cadena de custodia relativa al capítulo 10

F.1 Cadena de custodia

Número de caso: NID2015

Tipo de incidente: Debe realizarse un análisis forense a un ordenador portátil perteneciente a una empleada de la ESI de Ciudad Real, en busca de evidencias que demuestren la utilización de un período de baja comprendido del 1 al 5 de Abril de 2015 para realizar un viaje de ocio.

La empresa afectada (ESI Ciudad Real) se enfrenta a una demanda por despido improcedente.

Empresa afectada: ESI del campus de Ciudad Real de la UCLM.

Dirección: Paseo de la Universidad, 4, 13071, Ciudad Real (Ciudad Real).

Teléfono: 926 29 53 00

Fecha y hora: 30/05/2015 19:00

Investigador: Juan Miguel Tocados

F.1.1 Observaciones

Ordenador portátil con referencia **PC20150530** recolectado por el investigador **Juan Miguel Tocados**. Se encontraba apagado y se trasladó al laboratorio forense en una bolsa antiestática.

Una vez en el laboratorio se extrajo el **disco duro** con referencia **HD20150530** al que se le realizó un clonado mediante **dd** de su partición en sistema NTFS, conectando en primer lugar el disco duro extraído del portátil a una *docking station* **Sharkoon SATA QuickPort PRO** (figura F.1), comenzando el proceso de clonado a las 3:37 del 31 de Mayo de 2015 y finalizando a las 4:15 del mismo día. El hash correspondiente a la imagen con el algoritmo MD5, calculado también dicho día a las 4:30 es: **3f4725dcbb728e7ff995f93999d163d7**

F.1.2 Listado de evidencias

Figura F.1: Docking Station Sharkoon

Evidencia (Código)	Cantidad	Descripción del artículo
PC20150530	1	Dell Latitude E4300/PP13S Nº. serie: 5G1J64J
HD20150530	1	Fujitsu MHZ2250BJ FFS G2 250 GB Nº. serie: K83ET8C263NL

Cuadro F.1: Listado de evidencias

Anexo G

Informe pericial relativo al capítulo 10

CASO NIDAROS

Identificador:

NID2015

Perito:

Tocados Cano, Juan Miguel
Graduado en Ingeniería Informática
JuanMiguel.Tocados1@alu.uclm.es

Solicitante:

Pérez Pérez, Juan Carlos

Fecha emisión del informe: 11 de Junio de 2015

Índice

G.1 Declaración de tachas y juramento

De acuerdo con lo establecido en el Artículo 343 de la Ley 1/2000 de 7 de Enero de Enjuiciamiento Civil, este perito manifiesta:

- No ser cónyuge o pariente por consanguinidad o afinidad, dentro del cuarto grado civil de una de las partes o de sus abogados o procuradores
- No tener interés directo o indirecto en el asunto o en otro semejante
- No estar o haber estado en situación de dependencia o de comunidad o contraposición de intereses con alguna de las partes o con sus abogados o procuradores
- No tener amistad íntima o enemistad con cualquiera de las partes o sus procuradores o abogados
- No creer que exista cualquier otra circunstancia, debidamente acreditada, que le haga desmerecer en el concepto profesional

De acuerdo con lo establecido en el Artículo 335.2 de la Ley 1/2000 de 7 de Enero de Enjuiciamiento Civil, este perito promete que cuanto afirma es verdad y que ha actuado, y en su caso actuará, con la máxima objetividad posible, tomando en consideración tanto lo que pueda favorecer como perjudicar a cualquiera de las partes, conociendo las sanciones en las que podría incurrir en caso contrario.

G.2 Asunto

Se ha solicitado el análisis de la partición perteneciente a Windows de un ordenador portátil en busca de evidencias gráficas que demuestren una supuesta utilización de días correspondientes a baja laboral para la realización de un viaje de ocio por parte de una empleada de la ESI UCLM del campus de Ciudad Real.

Este informe ha sido realizado entre los días 30 de Mayo y 11 de Junio de 2015 por el perito Juan Miguel Tocados.

G.3 Evidencias recibidas

Contamos con las evidencias obtenidas en la escena, contenidas en el documento adjunto de cadena de custodia (Anexo F):

- **Evidencia PC20150530:** ver figura 10.1
  - Ordenador portátil Dell Latitude E4300/PP13S
  - Nº. Serie: 5G1J64J
- **Evidencia HD20150530:** ver figura 10.2
  - Disco duro Fujitsu MHZ2250BJ FFS G2 250 GB
  - Nº. Serie: K83ET8C263NL

Al disco duro con referencia HD20150530, instalado en el propio ordenador portátil con referencia PC20150530 y extraído en el propio laboratorio forense, se le realizó un clonado, que no es otra cosa que duplicar su contenido de manera exacta. Este clonado fue realizado de la forma detallada en el anteriormente citado documento de cadena de custodia.

G.4 Estudios efectuados sobre las evidencias

Tras el clonado de la partición que es de nuestra incumbencia, se realizó un **análisis del sistema de archivos**. Éste se encuentra formateado en NTFS, con un tamaño de 35.4 GB. Como dato característico, el número de serie del volumen es: 264C3FF64C3FBEFD.

Analizando más a fondo el sistema de archivos, se realizó una búsqueda por tipos de archivo en formato JPG, correspondiente a imágenes, tanto para archivos y directorios eliminados como para aquellos que aún permanecían en activo en el ordenador.

En la búsqueda para archivos y directorios eliminados no se encontró ningún elemento de interés, sin embargo en la misma búsqueda para archivos y directorios activos se encontró una imagen de título ***vacaciones.jpg*** que muestra a una mujer, supuestamente Mª José Santana junto a una estatua en un puerto, situada en la ruta *Documents and Settings/Mª José/Mis documentos/Mis imágenes/vacaciones.jpg*.

Se realizó también un **análisis de la papelera de reciclaje** y no se encontró ningún contenido en ella, por lo cual se recurrió a la herramienta *Foremost* para la recuperación de

archivos eliminados de tipo JPG, mediante la cual obtuvimos 3158 archivos y entre ellos un indicio interesante, una imagen de título ***01108856.jpg*** que muestra de nuevo a Mª José Santana junto a Juan Carlos Pérez y un grupo de gente, con una vestimenta y postura similar a aquella que muestra en la imagen *vacaciones.jpg*. Se consultó con el propio Juan Carlos Pérez para saber si conocía de la existencia de dicha foto, confirmando que dicha foto era real y fue tomada entre el 26 y el 27 de Febrero de 2013.

El sistema operativo se trata de **Windows XP**, con un único usuario llamado "Mª José".

Una vez obtenidos dichos posibles indicios (ambas imágenes referidas anteriormente), se realizó un **análisis de los metadatos** de las imágenes. Los metadatos son a su vez datos que describen a la imagen, incluyendo información como las dimensiones de la imagen, el tamaño de archivo, tiempo de creación, etc.

El resultado de este análisis proporcionó un dato de utilidad: la imagen *vacaciones.jpg* había sido editada con el software de edición de imágenes Adobe Photoshop CS5. No obstante, los metadatos pueden manipularse fácilmente, por lo que se realizó un análisis más profundo de dicha imagen, conocido como **análisis ELA**, que mediante diferencias de coloreado, basándose en el nivel de compresión JPEG, puede dar pistas sobre la manipulación de la imagen.

Según los resultados arrojados por este último análisis, podría inferirse que efectivamente, el software de Adobe ha sido aplicado sobre *vacaciones.jpg*, y que la figura de Mª José ha sido añadida posteriormente a la toma de la foto y que, según las coincidencias de vestuario y postura de la mujer, dicha figura fue tomada originalmente de la otra foto que se obtuvo, *01108856.jpg*.

Para concluir, se puede observar que la estatua tiene una leyenda que dice «DEN SISTE VIKING». Realizando una búsqueda rápida en Google Imágenes con los términos «Den Siste Viking estatua», podemos ver que esta estatua está emplazada en la ciudad noruega de Trondheim.

G.5 Situación final de las evidencias

La evidencia HD20150530 (disco duro), se volvió a ensamblar en la evidencia PC20150530 (ordenador portátil) y se devolvió el conjunto al responsable: Juan Carlos Pérez Pérez.

G.6 Conclusiones

El análisis permitió obtener dos posibles indicios, las imágenes *vacaciones.jpg* y *01108856.jpg*. Tras someterlas a un análisis de los datos descriptivos de la imagen (metadatos), se observó la posibilidad de que *vacaciones.jpg* estuviera modificada mediante Photoshop (un software de edición de imágenes digitales).

Un análisis más profundo, llamado análisis ELA, de *vacaciones.jpg* muestra que efectiva-

mente la foto ha sido modificada y la figura de Mª José Santana, presumiblemente obtenida de la imagen *01108856.jpg*, fue añadida posteriormente a la toma de la foto.

G.7 Anexos

G.7.1 Notas internas sobre los análisis realizados

Para el **análisis del sistema de archivos** se utilizó la herramienta `fsstat` y como la imagen que será sometida a análisis, con hash MD5 `3f4725dcbb728e7ff995f93999d163d7` contiene una única partición, con un sistema de archivos que comienza desde el principio, no será necesario el uso de la opción `-o` para indicar el desplazamiento en sectores hasta éste. La salida de `fsstat` es la siguiente:

```
# fsstat ntfs.dd

FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: NTFS
Volume Serial Number: 264C3FF64C3FBEFD
OEM Name: NTFS
Version: Windows XP

METADATA INFORMATION
--------------------------------------------
First Cluster of MFT: 786432
First Cluster of MFT Mirror: 4634752
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 100112
Root Directory: 5

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 9269503
Total Sector Range: 0 - 74156038

$AttrDef Attribute Values:
$STANDARD_INFORMATION (16)   Size: 48-72   Flags: Resident
$ATTRIBUTE_LIST (32)   Size: No Limit   Flags: Non-resident
$FILE_NAME (48)   Size: 68-578   Flags: Resident,Index
$OBJECT_ID (64)   Size: 0-256   Flags: Resident
$SECURITY_DESCRIPTOR (80)   Size: No Limit   Flags: Non-resident
$VOLUME_NAME (96)   Size: 2-256   Flags: Resident
$VOLUME_INFORMATION (112)   Size: 12-12   Flags: Resident
$DATA (128)   Size: No Limit   Flags:
$INDEX_ROOT (144)   Size: No Limit   Flags: Resident
$INDEX_ALLOCATION (160)   Size: No Limit   Flags: Non-resident
$BITMAP (176)   Size: No Limit   Flags: Non-resident
$REPARSE_POINT (192)   Size: 0-16384   Flags: Non-resident
$EA_INFORMATION (208)   Size: 8-8   Flags: Resident
$EA (224)   Size: 0-65536   Flags:
$LOGGED_UTILITY_STREAM (256)   Size: 0-65536   Flags: Non-resident
```

Se puede observar que es una partición en formato NTFS, el número de serie del volumen es 264C3FF64C3FBEFD y el sistema operativo instalado es Windows XP. Se pueden obser-

var otro tipo de información, como el tamaño de cluster y de sector y el rango total de éstos, aparte del tamaño de las entradas del MFT y dónde comienza el primer cluster de éste.

Como se puede ver, un cluster tiene un tamaño de 4096 bytes, y teniendo en cuenta que el tamaño de un sector son 512 bytes, tenemos que cada cluster está formado por 8 sectores (4096/512). Teniendo esto en cuenta, mirando al rango total de clusters o de sectores y realizando los cálculos oportunos, obtenemos un tamaño de volumen de 35.4 GB.

Siguiendo con el **análisis de los archivos**, se realizó una búsqueda por tipos de archivo con formato JPG, en primer lugar para archivos y directorios activos, con la herramienta `fls` y las opciones `-u`, `-p` y `-r`, que muestran los archivos y directorios activos, la ruta completa de cada uno y todo de forma recursiva, respectivamente. La salida es la siguiente:

```
# fls -upr ntfs.dd | grep jpg

r/r 52562-128-3:        Archivos de programa/SMPlayer/themes/
    blackPanther-VistaLike/preview.jpg
r/r 6015-128-3: Archivos de programa/Archivos comunes/Microsoft Shared
    /Stationery/Fondo de Dia luminoso.jpg
r/r 6018-128-3: Archivos de programa/Archivos comunes/Microsoft Shared
    /Stationery/Fondo de Fiesta.jpg
r/r 6034-128-3: Archivos de programa/Archivos comunes/Microsoft Shared
    /Stationery/Fondo de Girasol.jpg
r/r 6020-128-3: Archivos de programa/Archivos comunes/Microsoft Shared
    /Stationery/Fondo de Glaciar.jpg
r/r 6031-128-3: Archivos de programa/Archivos comunes/Microsoft Shared
    /Stationery/Fondo de Graficos circulares.jpg
r/r 6024-128-3: Archivos de programa/Archivos comunes/Microsoft Shared
    /Stationery/Fondo de Hojas.jpg
r/r 6026-128-3: Archivos de programa/Archivos comunes/Microsoft Shared
    /Stationery/Fondo de Maiz.jpg
r/r 6028-128-3: Archivos de programa/Archivos comunes/Microsoft Shared
    /Stationery/Fondo de Naturaleza.jpg
r/r 5903-128-3: Archivos de programa/Movie Maker/Shared/Sample1.jpg
r/r 5904-128-3: Archivos de programa/Movie Maker/Shared/Sample2.jpg
[...]
r/r 43101-128-3:        Documents and Settings/Ma Jose/Escritorio/
    portadaBanda/Imagen1.jpg
r/r 45967-128-3:        Documents and Settings/Ma Jose/Escritorio/
    portadaBanda/Imagen3.jpg
r/r 14610-128-3:        Documents and Settings/Ma Jose/Escritorio/
    portadaBanda/portada.jpg
r/r 13593-128-4:        Documents and Settings/Ma Jose/Mis documentos/
    Mis imagenes/vacaciones.jpg
```

De aquí se obtuvo el primer indicio, *vacaciones.jpg* (figura G.1), como puede observarse en la última línea del listado anterior, que fue restaurado en nuestra estación de trabajo mediante la herramienta `icat`, que vuelca los contenidos de un archivo basándose en su número de inodo, de la siguiente manera:

```
# icat -f ntfs ntfs.dd 13593-128-4 > vacaciones.jpg
```

Figura G.1: Imagen vacaciones.jpg

El hash MD5 de esta imagen es: `23a10c396394edf816d5bbd523db7952`

El **análisis de la papelera de reciclaje** no reportó ningún contenido en ella, como se ve en el siguiente listado:

```
d/d 23689-144-1:        RECYCLER
d/d 23690-144-7:        RECYCLER/S
    -1-5-21-299502267-527237240-1801674531-1003
r/r 23692-128-3:        RECYCLER/S
    -1-5-21-299502267-527237240-1801674531-1003/INFO2
r/r 13590-128-1:        RECYCLER/S
    -1-5-21-299502267-527237240-1801674531-1003/desktop.ini
```

Por lo cual se procedió a realizar una recuperación de los archivos eliminados con formato JPG con la herramienta **Foremost**, proceso que empezó a la 1:43 del 2 de Junio de 2015 y finalizó a la 1:53 del mismo día, de la siguiente forma:

```
foremost -t jpg -i ntfs.dd
```

Se recuperaron un total de 3158 archivos, del cual el único indicio de interés fue la imagen *01108856.jpg* (figura G.2)

Figura G.2: Imagen 01108856.jpg

Su hash MD5: `b9a619c58bc16775d63ebdbfbcaa0ed7`

Posteriormente se realizó el **análisis de los metadatos** con la herramienta **ExifTool**, primero de *vacaciones.jpg*:

```
ExifTool Version Number         : 8.60
File Name                       : vacaciones.jpg
Directory                       : Desktop
File Size                       : 442 kB
File Modification Date/Time     : 2015:06:02 04:13:03+00:00
File Permissions                : rw-r--r--
File Type                       : JPEG
MIME Type                       : image/jpeg
Exif Byte Order                 : Big-endian (Motorola, MM)
Orientation                     : Horizontal (normal)
X Resolution                    : 96
Y Resolution                    : 96
Resolution Unit                 : inches
Software                        : Adobe Photoshop CS5 Windows
Modify Date                     : 2015:04:02 12:01:23
Create Date                     : 2015:04:02 12:01:23
Color Space                     : Uncalibrated
Exif Image Width                : 2005
Exif Image Height               : 2500
Compression                     : JPEG (old-style)
Thumbnail Offset                : 342
Thumbnail Length                : 5756
IPTC Digest                     : 00000000000000000000000000000000
Displayed Units X               : inches
Displayed Units Y               : inches
Global Angle                    : 120
Global Altitude                 : 30
Photoshop Thumbnail             : (Binary data 5756 bytes, use -b
   option to extract)
Photoshop Quality               : 8
```

```
Photoshop Format                : Progressive
Progressive Scans               : 3 Scans
XMP Toolkit                     : Image::ExifTool 7.89
Format                          : image/jpeg
Color Mode                      : RGB
ICC Profile Name                : Adobe RGB (1998)
Creator Tool                    : Adobe Photoshop CS5 Windows
Metadata Date                   : 2015:04:02 12:01:23+02:00
Document ID                     : xmp.did:612
   AC9349904E5119C5DD14D9A2F92D5
History Action                  : created, saved
History Instance ID             : xmp.iid:612
   AC9349904E5119C5DD14D9A2F92D5, xmp.iid:622
   AC9349904E5119C5DD14D9A2F92D5
History Software Agent          : Adobe Photoshop CS5 Windows, Adobe
   Photoshop CS5 Windows
History When                    : 2015:04:02 12:01:23+02:00
History Changed                 : /
Instance ID                     : xmp.iid:622
   AC9349904E5119C5DD14D9A2F92D5
Original Document ID            : xmp.did:612
   AC9349904E5119C5DD14D9A2F92D5
Profile CMM Type                : ADBE
Profile Version                 : 2.1.0
Profile Class                   : Display Device Profile
Color Space Data                : RGB
Profile Connection Space        : XYZ
Profile Date Time               : 1999:06:03 00:00:00
Profile File Signature          : acsp
Primary Platform                : Apple Computer Inc.
CMM Flags                       : Not Embedded, Independent
Device Manufacturer             : none
Device Model                    :
Device Attributes               : Reflective, Glossy, Positive, Color
Rendering Intent                : Perceptual
Connection Space Illuminant     : 0.9642 1 0.82491
Profile Creator                 : ADBE
Profile ID                      : 0
Profile Copyright               : Copyright 1999 Adobe Systems
   Incorporated
Profile Description             : Adobe RGB (1998)
Media White Point               : 0.95045 1 1.08905
Media Black Point               : 0 0 0
Red Tone Reproduction Curve     : (Binary data 14 bytes, use -b option
    to extract)
Green Tone Reproduction Curve   : (Binary data 14 bytes, use -b option
    to extract)
Blue Tone Reproduction Curve    : (Binary data 14 bytes, use -b option
    to extract)
Red Matrix Column               : 0.60974 0.31111 0.01947
Green Matrix Column             : 0.20528 0.62567 0.06087
Blue Matrix Column              : 0.14919 0.06322 0.74457
DCT Encode Version              : 100
APP14 Flags 0                   : (none)
APP14 Flags 1                   : (none)
Color Transform                 : YCbCr
Image Width                     : 2005
Image Height                    : 2500
```

```
Encoding Process                : Progressive DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:4:4 (1 1)
Image Size                      : 2005x2500
Thumbnail Image                 : (Binary data 5756 bytes, use -b
   option to extract)
```

Se aprecian algunas etiquetas interesantes, como las siguientes:

```
Software                        : Adobe Photoshop CS5 Windows
Modify Date                     : 2015:04:02 12:01:23
Create Date                     : 2015:04:02 12:01:23
Creator Tool                    : Adobe Photoshop CS5 Windows
History Action                  : created, saved
Photoshop Quality               : 8
```

Mediante ellas puede deducirse que la imagen fue creada y guardada con Adobe Photoshop CS5 el día 2 de Abril de 2015 a las 12:01, con un nivel de calidad 8, que para el standard JPG equivaldría aproximadamente a un 86 %, considerada una calidad media-alta. Esta fecha y hora se corresponden con el período de baja laboral, sin embargo, ya se dijo que estos metadatos son fácilmente manipulables. No obstante, es aconsejable confirmar o desmentir dicha información mediante un análisis ELA posterior.

El análisis de los metadatos de la imagen *01108856.jpg* corresponden a los generados durante la recuperación de la foto y no muestran información aprovechable:

```
ExifTool Version Number         : 8.60
File Name                       : 01108856.jpg
Directory                       : Desktop/mount/foremost/jpg
File Size                       : 82 kB
File Modification Date/Time     : 2015:06:02 01:43:48+00:00
File Permissions                : rwxrwxrwx
File Type                       : JPEG
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Exif Byte Order                 : Little-endian (Intel, II)
Software                        : Picasa
Exif Version                    : 0220
User Comment                    :
Image Width                     : 1068
Image Height                    : 801
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 1068x801
```

Se procederá entonces al **análisis ELA** de *vacaciones.jpg* (ver figura G.3), realizado mediante la página web **FotoForensics**[1].

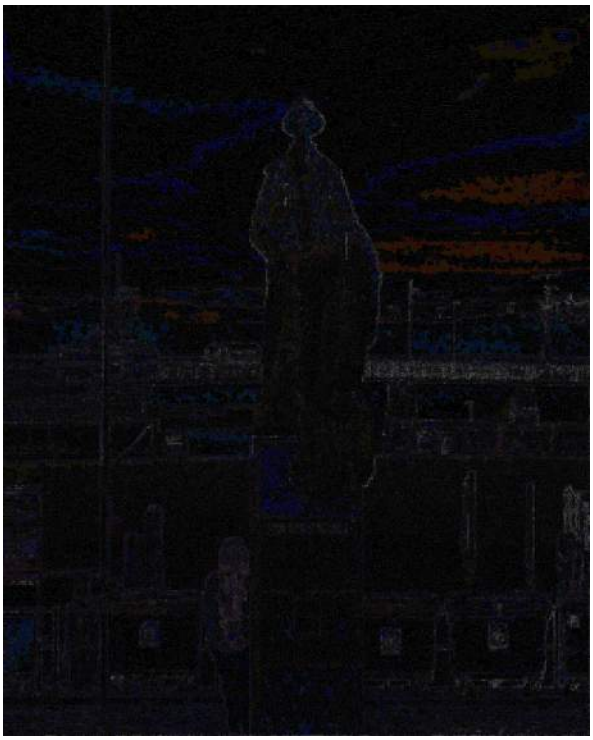

Figura G.3: Análisis ELA.jpg

Según esto, se aprecia en principio un claro ejemplo de *«rainbowing»* (sobre todo en las nubes), un fenómeno que puede producirse con Photoshop, aunque no de forma exclusiva. Dicho fenómeno consiste en zonas que presentan un coloreado rojo, azul o morado.

En general, el nivel ELA es bastante bajo, lo que indica que ha sido sometida a guardados sucesivos, provocando un resultado más oscuro. De igual manera, los bordes brillantes de las figuras que aparecen indican un reescalado de la imagen.

Los bordes son casi todos similares entre sí, como los de los contenedores, los postes, etc. Sin embargo, la figura de Mª José, que aparece junto a la estatua, presenta unos bordes menos nítidos, más borrosos y con un nivel ELA distinto al resto de la foto, tanto los bordes como la propia figura de la mujer (ver figura G.4), lo que da lugar a pensar que efectivamente Photoshop ha sido aplicado sobre la imagen y que la figura de Mª José fue añadida posteriormente a la toma de la foto.

[1] http://fotoforensics.com/

Figura G.4: Detalle ampliado de la figura de Mª José

El presente dictamen consta de 12 páginas. Y para que así conste a los efectos oportunos, extiendo el presente dictamen certificado, según mi leal saber y entender y a la práctica de la profesión, sometiéndolo a otro mejor fundado pericialmente, en Ciudad Real a 11 de Junio de 2015.

D. Juan Miguel Tocados

Anexo H

GNU Free Documentation License

Version 1.3, 3 November 2008

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format,

SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

The "publisher" means any person or entity that distributes copies of the Document to the public.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H. Include an unaltered copy of this License.
- I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
- N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
- O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version. 5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

5. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

6. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

7. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

8. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

9. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

10. RELICENSING

"Massive Multiauthor Collaboration Site" (or "MMC Site") means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A "Massive Multiauthor Collaboration" (or "MMC") contained in the site means any set of copyrightable works thus published on the MMC site.

"CC-BY-SA" means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

"Incorporate" means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is "eligible for relicensing" if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.

Referencias

[AEN11] AENOR. UNE 197001:2011. Criterios generales para la elaboración de informes y dictámenes periciales, 2011.

[AEN13a] AENOR. UNE 71505-1:2013. Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 1: Vocabulario y principios generales. AEN/CTN 71/SC 27 - Técnicas de Seguridad, 2013.

[AEN13b] AENOR. UNE 71505-2:2013. Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 2: Buenas prácticas en la gestión de las evidencias electrónicas., 2013.

[AEN13c] AENOR. UNE 71505-3:2013. Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 3: Formatos y mecanismos técnicos., 2013.

[AEN13d] AENOR. UNE 71506:2013. Tecnologías de la Información (TI). Metodologia para el análisis forense de las evidencias electrónicas., 2013.

[ANT] ANTPJI. Curso de perito telemático forense.

[ANT11] ANTPJI. *Curso de Perito Telemático Forense*, chapter Guía del peritaje informático, pages 43–45. 2011.

[BK02] D. Brezinski and T. Killalea. Rfc 3227: Guidelines for evidence collection and archiving. `https://www.ietf.org/rfc/rfc3227.txt`, February 2002. Internet Engineering Task Force (IETF).

[Car05a] B. Carrier. *File System Forensic Analysis*, chapter Appendix A. The Sleuth Kit and Autopsy, pages 377–382. Addison-Wesley, Upper Saddle River, NJ, USA, 2005.

[Car05b] B. Carrier. *File System Forensic Analysis*, chapter Digital Investigation Foundations, pages 14–15. Addison-Wesley, Upper Saddle River, NJ, USA, 2005.

[Car05c] B. Carrier. *File System Forensic Analysis*, chapter File System Analysis, page 132. Addison-Wesley, Upper Saddle River, NJ, USA, 2005.

[Car14] J. A. Carreras Espallardo. Actividad pericial y responsabilidad de los peritos. http://noticias.juridicas.com/articulos/60-Derecho-Procesal-Civil/201403-actividad-pericial-y-responsabilidad-de-los-peritos.html, Marzo 2014. Noticias Jurídicas. Artículos doctrinales: Derecho Procesal Civil.

[CS92] Philip A Collier and BJ Spaul. A forensic methodology for countering computer crime. *Artificial intelligence review*, 6(2):203–215, 1992.

[CS03] B. Carrier and E. H. Spafford. Getting Physical with the Digital Investigation Process. *International Journal of Digital Evidence*, 2(2), Noviembre 2003.

[dE01] Consejo de Europa. Convenio sobre la ciberdelincuencia. Serie de tratados europeos nº 185, 2001.

[dE03] Consejo de Europa. Protocolo adicional al convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos. Serie de tratados europeos nº 189, 2003.

[DFR01] DFRWS. A Road Map for Digital Forensic Research, 2001.

[FRD] S. Fratepietro, A. Rossetti, and P. Dal Checco. DEFT 7 manual.

[GB14] S. Garfinkel and J. R. Bradley. Bulk Extractor User Manual. http://digitalcorpora.org/downloads/bulk_extractor/BEUsersManual.pdf, 2014.

[Gim14] V. Gimeno Sendra. *Manual de derecho procesal penal*. Colex, 2014.

[Gru08] B. J. Grundy. *The Law Enforcement and Forensic Examiner's Introduction to Linux*. LinuxLEO, 2008.

[Lá13] F. Lázaro Domínguez. *Introducción a la Informática Forense*, chapter 2. La investigación forense, pages 38–40. Ra-Ma, Paracuellos de Jarama, Madrid, España, 2013.

[Mar12a] J. Martínez de Aguirre. Breve introducción a los derechos de propiedad intelectual (I). http://propiedadintelectualhoy.com/2012/01/25/breve-introduccion-a-los-derechos-de-propiedad-intelectual-i/, Enero 2012. Propiedad Intelectual Hoy.

[Mar12b] J. Martínez de Aguirre. Breve introducción a los derechos de propiedad intelectual (y II). http://propiedadintelectualhoy.com/2012/01/27/

breve-introduccion-a-los-derechos-de-propiedad-intelectual-y-ii/ , Enero 2012. Propiedad Intelectual Hoy.

[Mar14] A. Martínez Retenaga. Guía de toma de evidencias en entornos Windows. https://www.incibe.es/extfrontinteco/img/File/intecocert/ManualesGuias/incibe_toma_evidencias_analisis_forense.pdf, 2014.

[NIS] NIST. Data Formats of the NSRL Reference Data Set (RDS) Distribution. http://www.nsrl.nist.gov/Documents/Data-Formats-of-the-NSRL-Reference-Data-Set-16.pdf.

[Ort08] R. Orta Martínez. Informática forense como medio de pruebas. http://www.dragonjar.org/informatica-forense-como-medio-de-pruebas.xhtml, Enero 2008. Visto en DragonJAR.

[Osb13] G. Osborne. Memory Forensics: Review of Acquisition and Analysis Techniques. Noviembre 2013.

[Ram06] F. Ramos Méndez. *Enjuiciamiento criminal: octava lectura constitucional*. Atelier Libros Jurídicos, 2006.

[Ram11] A. Ramos. Historia de la informática forense. http://www.securitybydefault.com/2011/03/historia-de-la-informatica-forense.html, Marzo 2011. Security By Default.

[Ric13] M. Richard Gonzalez. La cadena de custodia en el proceso penal español. *Diario La Ley*, (8187):1–12, Noviembre 2013. Año XXXIV.

[Rob13] E. Robaina Espinosa. Historias de la Justicia: Qué es la prueba anticipada y qué es la prueba preconstituida. http://tinyurl.com/lawcenter-pruebas, Agosto 2013. Law Center Social.

[Sep13] J.A. Sepúlveda. Historia informática forense. http://informaticaforense1.blogspot.com.es/2013/11/historia-informatica-forense.html, Noviembre 2013. Institución Universitaria Antonio José Camacho.

[Sta14] C. Stamatoulos. Enciclopedia jurídica. http://www.enciclopedia-juridica.biz14.com/d/tacha/tacha.htm, 2014.

[YIH11] Y. Yusoff, R. Ismail, and Z. Hassan. Common Phases of Computer Forensics Investigation Models. *International Journal of Computer Science and Information Technology*, 3(3), Junio 2011.

Este documento fue editado y tipografiado con LaTeX
empleando la clase **esi-tfg** que se puede encontrar en:
`https://bitbucket.org/arco_group/esi-tfg`