UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf
Escola Tècnica Superior d'Enginyeria Informàtica

Escola Tècnica Superior d'Enginyeria Informàtica

Universitat Politècnica de València

Guía actualizada para futuros peritos informáticos. Últimas herramientas de análisis forense digital. Caso práctico

Trabajo Fin de Grado

Grado en Ingeniería Informática

Autor: Jorge Navarro Clérigues

Tutor: Eva Cutanda García

2015 / 2016

Resumen

La finalidad de este trabajo es ofrecer un documento de referencia actualizado, de carácter general y práctico, con los aspectos técnico-legales que el futuro perito informático forense debe conocer. Y brindar una mirada introductoria a la informática forense mediante un caso práctico completo, donde la evidencia digital es la protagonista del proceso que finaliza con el dictamen del informe pericial. Uno de los objetivos es enfocar esta ciencia desde el prisma del derecho informático, la deontología, la ética y el profesionalismo del perito informático. La gran demanda de expertos en peritaje y análisis forense digital abre las puertas al mercado laboral a estudiantes y profesionales informáticos. En este contexto, el presente trabajo sirve para consolidar conceptos y encauzar al lector en esta novedosa ciencia: Informática Forense.

Palabras clave: forense, seguridad, ciberseguridad, análisis, perito, evidencia, digital

Abstract

The purpose of this paper is to provide an updated and practical reference document which will be of use to future computer forensic experts. It provides an introductory look at forensics using an example case where digital evidence was a determining factor in the judicial process which relied on an expert opinion.
One of its aims is to highlight the relationship between the law and the professional ethics of the computer expert.
The high demand for experts with digital forensics expertise opens doors to the labour market for students and professionals. In this context, this paper serves to consolidate concepts and direct the reader to this new science: Computer Forensics.

Keywords: forensics , security, cybersecurity , analysis, expert, evidence , digital

Tabla de contenidos

1 Introducción 9
2 El mercado de la seguridad informática 11
Ciberseguridad e Informática Forense. Sectores en crecimiento 12
Datos estadísticos en Ciberseguridad y delitos informáticos 15
Principales riesgos en el ciberespacio 16
Principales amenazas en el ciberespacio 17
Tendencias en técnicas de prevención y respuesta 19
Estrategia de Ciberseguridad Nacional 21
3 El perito informático 25
Ámbitos de actuación 26
Deberes del perito informático 28
Deontología y ética profesional 29
Tipos de peritajes informáticos y áreas de actuación 31
Requisitos para ejercer como perito informático 33
Asociaciones nacionales y colegios oficiales 35
El informe o dictamen pericial 36
4 Informática forense digital 45
Fases del análisis forense digital 46
La evidencia digital. La reina del proceso 48
Metodologías en análisis forense digital. Normas y guías actuales 50
5 Marco legal en el peritaje informático 57
Derecho informático 59
Legislación nacional aplicada al perito informático 61
El delito informático en la reforma del Código Penal 62
La nueva ley en la investigación tecnológica 64

6 Herramientas de análisis forense digital 69
Utilidades y *software* portable en informática forense 70
Distribuciones *software* para el análisis forense digital 76
Laboratorio forense. Dispositivos *hardware* y *software* 83
7 Como crear nuestro laboratorio forense 95
Herramientas y utilidades forenses para trabajo de campo 95
Equipo forense para investigación en laboratorio 98
8 Caso práctico de análisis forense digital 105
Descripción del caso práctico. Antecedentes judiciales 106
Identificación y preservación de las pruebas originales 109
Allanamiento y registro domiciliario 112
Adquisición en vivo de datos forenses 112
Análisis en laboratorio de las evidencias recopiladas 119
Informe de resultados en la investigación del caso 142
Conclusiones finales 143
Bibliografía 145

Indice de figuras

Figura 1. Estafas y fraudes cibernéticos. Phishing. *18*
Figura 2. Declaración de independencia del Ciberespacio *24*
Figura 3. Ámbito multidisciplinar del peritaje informático *32*
Figura 4. Fases del Análisis Forense Digital. *47*
Figura 5. Delitos informáticos *58*
Figura 6. Aplicación de herramientas y equipos forense en la investigación *69*
Figura 7. Unidad USB Live Response de E-fense *80*
Figura 8. Escritorio de Kali Linux *81*
Figura 9. Laboratorio informático forense de una empresa privada *84*
Figura 10. Estación forense Zeus *85*
Figura 11. Estación forense Hades *85*
Figura 12. Logicube Forensic Falcón *86*
Figura 13. Logicube Forensic Talon *86*
Figura 14. Logicube Forensic Dossier *86*
Figura 15. Duplicadora Tableau TD2 ..... *87*
Figura 16. Duplicadora Tableau TD3 ..... *87*
Figura 17. Duplicadora CRU Ditto *87*
Figura 18. Duplicadora Voom Hardcopy 3 ..... *88*
Figura 19. Análisis forense Voom Shadow 3 ..... *88*
Figura 20. Puerto JTAG para móvil *88*
Figura 21. Flasheo de móviles *89*
Figura 22. Herramientas forenses para trabajo de campo *89*
Figura 23. Sistema integral análisis de móviles XRY Complete *90*
Figura 24. UFED Physical Analyzer. Análisis forense para móviles *92*
Figura 25. E-Detective. Sistema forense para red *93*
Figura 26. E-Detective. Diagrama de Implementación de interceptación de Internet. *94*
Figura 27. Diagrama de E-Detective Telco ISP de interceptación legal en masa *94*
Figura 28. Software portable "live forensics" para trabajo de campo *95*
Figura 29. Herramientas y utilidades del pendrive / DVD de trabajo de campo *96*
Figura 30. Rufus para crear Live USB NBCaine 4.0 ..... *97*
Figura 31. Configuración VMware Virtual Box para Caine 7 ..... *99*
Figura 32. GParted para crear las particiones de disco *99*
Figura 33. Systemback para realizar la instalación de Caine 7 ..... *100*
Figura 34. System Install. Datos de usuario y hostname *100*
Figura 35. System Install. Punto de montaje en root. *101*
Figura 36. Systemback Install. Iniciar la instalación del sistema live *101*
Figura 37. Reiniciar Linux tras la instalación *102*
Figura 38. Caine 7.0 instalado y listo para trabajar. Nuevo escritorio Deepspace *102*
Figura 39. Modo writer de la partición sda con el programa UnBlock *103*
Figura 40. Crear y montar la partición swap de Linux *103*
Figura 41. Escritorio definitivo de Caine 7.0 herramientas forenses *104*
Figura 42. Captura de pantalla del mensaje de correo electrónico *109*
Figura 43. Crear copia forense de las pruebas originales con FTK Imager *110*
Figura 44. Hash de la imagen creada y pruebas originales. *110*
Figura 45. Metadatos de las fotografías originales *111*
Figura 46. Imágenes fotográficas de la investigación de campo *112*
Figura 47. Imagen fotográfica del contenido de la pantalla del portátil *113*
Figura 48. Hashes generados con la utilidad HashMyFiles *114*
Figura 49. Volcado de memoria RAM con AccessData FTK Imager *115*
Figura 50. Herramientas y utilidades incluidas en Investigador 2.0 ..... *116*
Figura 51. Investigador 2.0 para recolección automática evidencias en Windows *117*
Figura 52. Investigador 2.0 estructura carpetas de resultados del análisis *117*
Figura 53. Archivos forenses generados por cada utilidad seleccionada en Investigador 2.0 ..... *118*
Figura 54. Pendrive EVI02 listo para crear su copia / imagen forense *120*

Figura 55. GuyMager para crear doble copia de imagen forense del pendrive *120*
Figura 56. GuyMager ejecutando la copia/imagen del pendrive *121*
Figura 57. QuickHash para comparar hashes de ambas imágenes creadas *121*
Figura 58. Brasero para crear DVD EVI02 (Joliet) con la imagen evidencia02 ..... *122*
Figura 59. Crear un nuevo caso con Autopsy de Caine 7.0 ..... *123*
Figura 60. Autopsy. Añadir nueva imagen al caso. *123*
Figura 61. Autopsy. Seleccionar volumen a analizar *124*
Figura 62. Autopsy. Resultado del análisis de ficheros *124*
Figura 63. Autopsy. Archivos borrados del pendrive *125*
Figura 64. Bulk Extractor Viewer (BE Viewer) para análisis en bruto *126*
Figura 65. BE Viewer. Resultado de Exif - metadatos *126*
Figura 66. BE Viewer. Resultados de archivos ZIP encontrados *126*
Figura 67. BE Viewer. Resultado de comparativa de hashes de imágenes forenses *127*
Figura 68. BE Viewer contenido archivo ZIP recuperado *127*
Figura 69. BE Viewer. Ficheros recuperados -wordlist *127*
Figura 70. BE Viewer. Fotografías recuperadas mediante carving *128*
Figura 71. Datos forenses de EVI03 en DVD *129*
Figura 72. FTK Imager para añadir datos forenses de EVI03 y crear imagen *130*
Figura 73. FTK Imager. Contraseña del correo en la RAM *131*
Figura 74. Unidad E:\ y nombre de las fotografías, vídeo y ZIP *131*
Figura 75. Número de serie del pendrive EVI02 introducido en el portátil. *132*
Figura 76. Búsqueda y descarga de programas de esteganografía - Camouflage *132*
Figura 77. Resultado de la utilidad UsbDview *134*
Figura 78 Resultado de la utilidad ChromePass. Contraseña del correo. *135*
Figura 79. Resultado de la utilidad ChromeHistory. Acceso al correo / enviados *135*
Figura 80. Usuarios de Windows con UserProfileView *136*
Figura 81. Ficheros abiertos recientemente con RecentFilesView *136*
Figura 82 Programas ejecutados por usuario activo con UserAssistView *136*
Figura 83. Resultado de la utilidad WirelessKeyView *137*
Figura 84. Resultado de búsquedas realizadas. MyLastSearch *137*
Figura 85. Serial Number del pendrive investigado proporcionada por UsbDView *137*
Figura 86. Análisis forense del pendrive con Autopsy 4.0 ..... *139*
Figura 87. Archivos encontrados con Autopsy 4.0 ..... *140*
Figura 88. Archivos contenidos en el pendrive exportados con Autopsy 4.0. ..... *140*
Figura 89. Hash de los archivos exportados con Autopsy 4.0 ..... *141*
Figura 90. Mismatch File con OSForensics *141*
Figura 91. Fotografía camuflada en fichero README.LOG *141*
Figura 92. Resultado negativo en la búsqueda de esteganografía con Xteg. *142*

Indice de tablas

Tabla 1. Organismos e instituciones nacionales en Ciberseguridad *22*
Tabla 2. Acuerdos internacionales en ciberseguridad *23*
Tabla 3. Clases de Peritajes informáticos *31*
Tabla 4. Asociaciones nacionales de peritos informáticos *35*
Tabla 5. Colegios Oficiales de ingenieros en informática *35*
Tabla 6. Artículos de la LECriminal y LECivil en materia informática *61*
Tabla 7. Herramientas y utilidades software de investigación forense digital *75*

1 Introducción

El uso fraudulento de Internet y de las Nuevas Tecnologías de la Información y la Comunicación (TIC) ha elevado la cantidad de delitos informáticos como el *hacking*, el *phishing*, el *pharming*, el acoso a través de las redes sociales, el fraude-online o la pornografía infantil. Hoy en día prácticamente todas las formas de delincuencia tienen un componente tecnológico digital que puede ser usado como prueba –evidencia digital- ante un proceso judicial. Esto obliga a gobiernos, empresas, abogados, jueces y cuerpos de seguridad del estado solicitar los servicios de peritos informáticos forenses. Esta demanda proporciona una interesante salida laboral para universitarios y profesionales en Informática.

De la mano del avance tecnológico, es necesario y primordial que los gobiernos adapten su marco legal y jurídico a las nuevas actividades delictivas, elaboren normas, y firmen acuerdos internacionales para combatir el Cibercrimen organizado.

Por otro lado, los peritos tienen que conocer las últimas herramientas y metodologías en análisis forense informático, y estar al día en seguridad informática, delitos cibernéticos y ciberseguridad. Además de ser expertos informáticos, por la importancia de sus dictámenes periciales, y su vinculación con el 'mundo' jurídico, han de conocer la legislación vigente y su responsabilidad civil, penal y profesional en la investigación y dictamen pericial. El profesionalismo, la ética y la deontología son pilar fundamental para un buen perito informático.

Resulta difícil, ante estos avances y continuos cambios, encontrar bibliografía actualizada que recopile: las últimas versiones de software forense, el nuevo ordenamiento legislativo, recientes estándares y normas publicadas, y demás contenidos divulgados por asociaciones, colegios y organismos. En pocos años las ediciones bibliográficas son prácticamente obsoletas, y la búsqueda y recopilación de tanta información dispersa en internet es una labor tediosa y complicada.

En este contexto, la finalidad de este trabajo es ofrecer un documento de referencia actualizado, de carácter general y práctico, con los aspectos técnico-legales que el futuro perito informático forense debe conocer, y brindar una mirada introductoria a la tecnología *hardware* y *software* utilizada en la investigación forense digital, mediante un caso práctico completo, donde la evidencia digital es la protagonista del proceso que finaliza con el dictamen o informe pericial.

La primera parte de la guía se compone de los capítulos dos, tres y cuatro. El capítulo dos, *El mercado de la seguridad informática*, describe el panorama actual de la informática forense digital y la ciberseguridad en esta "sociedad de la información digital" de este siglo XXI, bien como apoyo a la justicia para esclarecimiento de delitos donde existe un componente tecnológico que aporte evidencias digitales en un juicio penal/criminal, o bien para combatir la ciberdelincuencia en este nuevo entorno, el ciberespacio, donde la gran demanda a

nivel mundial de expertos profesionales, ofrece una excelente salida laboral en un mercado en pleno auge. El capítulo tres, *El perito informático,* sobre todo presenta al lector las consideraciones en el ejercicio del peritaje informático en el ámbito judicial. Destacar los principios éticos y deontológicos asumidos por estos profesionales, así como los deberes y responsabilidades penales en el desarrollo de su pericia. Se describen los requisitos legales para ejercer como perito informático, y las asociaciones de profesionales y colegios oficiales reconocidos en España. Por último, se tratan los aspectos a tener en cuenta, así como, su estructura y normas publicadas para la elaboración de dictámenes e informes periciales. El capítulo cuatro, *Informática forense digital,* desarrolla los conceptos, metodologías, últimas normas UNE e ISO y fases para el desarrollo de un análisis forense digital, donde destaca la importancia de mantener la evidencia digital integra e inalterada manteniendo su cadena de custodia para que las pruebas aportadas sean válidas ante un juicio.

La segunda parte de esta guía formada por el capítulo cinco, *Marco legal en el peritaje informático*, presenta una relación actualizada de la legislación española y directivas europeas e internacionales de aplicación al peritaje informático forense. Destacar el delito informático en la nueva reforma del Código Penal y la nueva Ley en la Investigación Tecnológica.

La tercera parte, está compuesta por los capítulos seis y siete. En el capítulo seis, *Herramientas de análisis forense digital*, se detallan las últimas versiones y enlaces de descarga de herramientas, utilidades y distribuciones *software* más destacadas del mercado, en especial, las distribuciones basadas en *Live GNU Linux*. Además, se describen los nuevos dispositivos y equipos *hardware* del mercado –duplicadoras, clonadoras, bloqueadoras, etc.- utilizados por los Cuerpos de Seguridad del Estado y laboratorios dedicados a la investigación forense digital. El capítulo siete, ofrece una guía paso a paso para que el lector cree su propio laboratorio forense. Por un lado, se explican las herramientas, utilidades y equipos necesarios para trabajo de campo, y por otro, la estación forense, *hardware* y distribuciones necesarias para trabajar en laboratorio. Resaltar en este apartado, la ilustración gráfica de capturas de pantalla en todo el proceso de instalación, configuración y puesta en marcha de la distribución *Linux Ubuntu* de Caine 7.0 en VirtualBox.

En la última parte de esta guía, se ponen en práctica los conceptos y conocimientos teóricos vistos en capítulos anteriores mediante la realización de un caso práctico completo de investigación y análisis forense digital. Se ilustra con imágenes y capturas de pantalla cada fase de la investigación, se describen los programas y herramientas utilizadas, se discuten los resultados obtenidos en base a los requerimientos del expediente judicial y finalmente se elaboran las conclusiones.

2 El mercado de la seguridad informática

En este capítulo se describe el panorama actual de la seguridad informática y su impacto directo en el mercado laboral. No pretende ser un estudio en profundidad de conceptos en seguridad informática, sino más bien, hacer llegar al lector la importancia que en este siglo XXI tiene la información digital y todo lo que le rodea.

En este sentido, gobiernos, empresas, organizaciones y profesionales, a nivel mundial, se esfuerzan en garantizar la seguridad de la información digital, de los sistemas informáticos, de los servicios digitales y de las infraestructuras de red. Este esfuerzo se materializa en destinar más recursos profesionales y económicos en investigación tecnológica y seguridad de las TIC.

> ***"El Ministerio de Industria destina 215 millones de euros al plan de ayudas del sector TIC y de los Contenidos Digitales."***
> ***(Red.es, 2015) 1***

Por otro lado, el incremento de la Cibercriminalidad y delitos relacionados con la tecnología digital bien de forma directa o donde la información digital es parte de las pruebas de una investigación judicial, abren las puertas laborales a expertos en ciberseguridad y análisis forense digital.

> ***"420.000 millones de euros es el coste anual estimado de la ciberdelincuencia para la economía global, según Allianz"***
> ***(Ipconnecting, 2015) 2***

Sin duda el mercado laboral de las TIC, la Ciberseguridad[3] e Informática Forense digital está en auge y es uno de los menos afectados por la crisis económica mundial.

[1] **Red.es (2015)** del Ministerio de Industria, Energía y Turismo [Citado el: 03 de junio de 2015] http://www.red.es/redes/sala-de-prensa/noticia/el-ministerio-de-industria-destina-215-millones-de- euros-al-plan-de-ayudas-de

[2] **Ipconnecting (2015).** La ciberseguridad se dispara ante las nuevas amenazas [Citado el: 6 de diciembre 2015] http://ipconnecting.com/es_ES/news/la-ciberseguridad-se-dispara-ante-las-nuevas-amenazas/

[3] **ISACA (s.f.)** (Information Systems Audit and Control Association) define Ciberseguridad como: "Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados". https://www.isaca.org/Pages/default.aspx

Ciberseguridad e Informática Forense. Sectores en crecimiento

El vertiginoso avance de los servicios digitales y de las Tecnologías de la Información y la Comunicación (TIC), su accesibilidad y su rápida adaptación en la sociedad, están aportando grandes beneficios a nivel social, cultural y económico. Si añadimos, la hiperconectividad, como fruto de la globalización, que ofrece formas más rápidas y efectivas de comunicación, con acceso a gran cantidad de información digital en una nueva dimensión donde se desdibujan las fronteras geográficas, nos encontramos ante un nuevo entorno, el ciberespacio, el cual ha cambiado la forma en que las organizaciones, empresas, administraciones públicas e individuos se relacionan.

Este traslado de la actividad diaria y la dependencia de la sociedad en los servicios que ofrece el ciberespacio –internet, redes sociales, correo electrónico, cibereconomía, teletrabajo, administración electrónica, etc. – aumenta drásticamente el número de riesgos y amenazas con un alto grado de repercusión económica y social. Incluso los gobiernos, dentro del marco de la Seguridad Nacional, consideran de vital importancia la seguridad del ciberespacio, sobre todo ante los posibles ciberataques dirigidos a las infraestructuras críticas y sistemas de defensa.

Según el SCSI [4] las ciberamenazas se pueden englobar en dos grandes grupos:

- ✓ las dirigidas contra la información, y
- ✓ las que su objetivo son las infraestructuras TIC.

A nivel general las ciberamenazas se caracterizan por:

- ✓ Ser difíciles de prever, identificar, controlar y erradicar.
- ✓ Su dimensión global.
- ✓ Su gran impacto social.
- ✓ Su sofisticación y bajo coste de ejecución.

Por todo ello, gobiernos, empresas, organizaciones e instituciones necesitan aplicar medidas de seguridad no solo reactivas sino también proactivas, y adoptar la Ciber-Resiliencia[5] como elemento primordial de respuesta ante los "inevitables" ataques.

---

[4] **SCSI** (2012) -Spanish Cyber Security Institute- e **ISMS** Forum Spain -Asociación Española para el Fomento de la Seguridad de la Información- en su informe publicado en 2012: La Ciberseguridad Nacional, un compromiso de todos (pag. 6)

[5] **Ieee.es (2015)** -Instituto Español de Estudio Estratégicos-, en Documento de Opinión 35/2015 publicado 3 de abril de 2015 define Ciber-Resiliencia como: "la *cualidad inherente a un organismo, entidad, empresa o estado que le permite hacer frente a una crisis cibernética sin que su actividad se vea afectada.*"

Así pues, en el supuesto de sufrir un ciberataque, es vital identificar: a su autor/es, el objetivo, los sistemas informáticos afectados, como se ha realizado –brechas de seguridad- y el impacto global en la organización. Aquí es donde la figura del perito informático forense es un eslabón esencial en la cadena de la seguridad informática. Su labor de investigación y análisis, sus habilidades y su experiencia en *hacking* ético, y su conocimiento en sistemas y redes informáticas, entre otras muchas cualidades, proporciona valiosos conocimientos en la investigación del incidente. Además, en calidad de perito, su informe o pericia resultado de su investigación, puede ser presentada ante un tribunal en el supuesto que el incidente termine en los tribunales, o puede utilizarse como prueba del ataque o incidente en la denuncia presentada ante las autoridades nacionales y europeas. Según la Directiva Europea de Ciberseguridad las empresas, organizaciones y demás instituciones del país están obligadas a comunicar a las autoridades judiciales cualquier ataque o amenaza tecnológica recibida.

Otro aspecto relevante, desde el punto de vista penal y criminal, es la indudable existencia en cualquier investigación policial de un componente tecnológico y el "rastro" que éste deja –huella digital-. La gran cantidad de delitos colapsa el sistema policial y jurídico del país. Para agilizar y mejorar los procedimientos jurídicos, se contratan los servicios de expertos tecnológicos privados, provocando un aumento de la demanda de profesionales -peritos informáticos forenses- con capacidades técnico-legales en el desarrollo de informes periciales que aporten evidencias digitales válidas.

Debido al imparable avance tecnológico y las cada vez más sofisticadas técnicas anti-forense utilizadas por los cibercriminales, se hace imprescindible la continua formación de los miembros de las Fuerzas y Cuerpos de Seguridad del Estado, a través de conferencias y cursos especializados impartidos por empresas privadas, asociaciones y colegios. Esta colaboración público-privada en ciberseguridad se engloba dentro de las medidas establecidas en las Directivas Europeas.

Por otro lado, los gobiernos, en su apuesta de implantar la administración electrónica, y ante el riesgo de ciberamenazas que esto acarrea, están implantando medidas de seguridad que permitan proteger la confidencialidad de los datos personales de los ciudadanos –cumplimiento de la Ley Orgánica de Protección de Datos de carácter personal (LOPD). En este sentido, los centros nacionales y autonómicos de respuesta ante incidentes cibernéticos son vitales para el aseguramiento de las infraestructuras críticas, la privacidad y la disponibilidad de los servicios telemáticos públicos.

Otras ciberamenazas emergentes como las relativas al uso de soluciones basadas en la "nube" –de bajo coste y utilizadas por la mayoría de PYMES-, el uso de dispositivos móviles, la inclusión del Internet de las cosas, la difusión de empresas en prácticas *BYOD*[6] (*Bring Your Own Device),* y la aparición de amenazas persistentes (APT), están abriendo grandes oportunidades laborales en el mercado de la seguridad.

---

[6] **BYOD s.f.** -Bring your Own Device- en castellano *"trae tu propio dispositivo",* según Wikipedia es: *"Una política empresarial donde los empleados llevan sus propios dispositivos a su lugar de trabajo para tener acceso a recursos de la empresa tales como correos electrónicos, bases de datos y archivos en servidores así como datos y aplicaciones personales."* http://es.wikipedia.org/wiki/BYOD

Sectores críticos como el aeroespacial, la defensa, la banca, la administración pública, la inteligencia y las industrias, coinciden que la ciberseguridad es una de sus principales preocupaciones de este siglo XXI.

Si a lo comentado en párrafos anteriores, le sumamos el aprovechamiento tecnológico y sofisticación de las técnicas y tácticas utilizadas por los cibercriminales, el interés económico o terrorista que les motiva y la difícil atribución del delito informático, es patente la incapacidad de gobiernos, departamentos de las TI (Tecnologías de la Información) y profesionales para garantizar la seguridad global del ciberespacio.

Es evidente el auge del sector de la ciberseguridad y del análisis forense digital.

Un estudio publicado en 2014 por la empresa **CISCO**, indica que:
"*En 2015 el déficit de profesionales en ciberseguridad, a nivel global, se estima es más de un millón de expertos"*
(Cisco, 2014)

http://globalnewsroom.cisco.com/es/es/release/Los-ataques-avanzados-y-el-tr%C3%A1fico-malicioso-experimentan-un-crecimiento-sin-precedentes-1881684

********&*********

INCIBE (Instituto Nacional de Ciberseguridad) asegura que (2015):

"*En España hay más de 42.500 profesionales trabajando en el ámbito de la seguridad y en los próximos años crecerá exponencialmente.*"

"*Ha destinado en 2015 unos 400.000 € en becas para la formación de expertos en ciberseguridad."*

"*A través de su Equipo de Respuesta ante Emergencias Informáticas de Seguridad e Industria (CERT), ha resuelto de enero a septiembre de 2015 un total de 52 ataques a infraestructuras críticas y servicios básicos del país."*

*********&*********

La redacción de **Computing.es** cita: "*España necesita 10.000 expertos en Informática Forense, una nueva profesión que se abre camino para muchos universitarios*"
(Agosto de 2014)

*********&*********

Según datos de MarketsandMarkets (2015):

"*Desde el punto de vista de los negocios, los datos son la huella de una oportunidad dentro de un mercado, el de la ciberseguridad, que crecerá desde los 106.000 millones de dólares generados en 2015 hasta los 170.000 en 2020".*
(Panda Security News publicado el 3 de diciembre de 2015)

http://www.pandasecurity.com/spain/mediacenter/seguridad/especialistas-ciberseguridad/

Datos estadísticos en Ciberseguridad y delitos informáticos

A nivel autonómico

Según información publicada en 2015 por CSIRT-CV (Centro de Seguridad TIC de la Comunidad Valenciana):

> *El Centro, consolidado ya como pieza indispensable para la seguridad corporativa de la Generalitat Valenciana, procesa actualmente una media diaria de 200.000 alertas provenientes de sus sistemas de prevención y detección de intrusiones, ha gestionado cerca de 5.500 incidentes de seguridad desde su creación, y recibe mensualmente alrededor de 130 peticiones de servicio, destinadas principalmente a mejorar la seguridad en las Administraciones Públicas Valencianas de forma proactiva. Los ciudadanos de la Comunidad también se han beneficiado de sus servicios, destacando la formación gratuita en materia de seguridad con más de 26.000 cursos impartidos entre ellos.*

A nivel nacional

Según información publicada en la memoria anual de 2014 del Ministerio Fiscal:

> *"Análisis de diligencias de investigación y procedimientos judiciales incoados y acusaciones del Ministerio Fiscal. Sala de Criminalidad Informática y las secciones de criminalidad informática de las Fiscalías en el año 2014. "*

	TOTAL	%
Daños, sabotaje informático.	143	0,70
Acceso sin autorización.	297	1,45
Descubrimiento y revelación de secretos.	561	2,73
Contra los servicios de radiodifusión.	15	0,07
Estafa.	17.328	84,39
Acoso a menores de 13 años.	60	0,29
Pornografía y corrupción de menores o discapacitados.	581	2,83
Contra la propiedad intelectual.	58	0,28
Falsificación documental.	156	0,76
Injurias y calumnias contra funcionario público.	381	1,86
Amenazas y coacciones.	527	2,57
Contra la integridad moral.	130	0,63
Apología o incitación a la discriminación.	30	0,15
Otra tipología delictiva.	150	0,73
Denuncias por suplantación de identidad.	117	0,57
TOTAL	**20.534**	**100,00**

Para garantizar una interpretación correcta de estos resultados ha de recordarse, como en anteriores Memorias, que uno de los problemas que complican el análisis de este fenómeno criminal es, precisamente, la especial dificultad en la detección e identificación de los procedimientos judiciales/diligencias de investigación que tienen por objeto hechos ilícitos vinculados al uso de las TIC. Ello es consecuencia de la transversalidad de esta forma de delincuencia que puede manifestarse en comportamientos ilícitos de muy diversa naturaleza, y encuadrables en diferentes tipos penales, por lo que su reflejo a efectos estadísticos en muchas ocasiones puede quedar oculto en los datos globales correspondientes al registro genérico de los distintos delitos, circunstancia que ocurre siempre que no se deja constancia en las aplicaciones, con la debida precisión, del carácter informático de la infracción.

Principales riesgos en el ciberespacio

Seguridad en Internet de las cosas

Internet de las cosas es la interconexión de dispositivos y elementos inteligentes –sensores, dispositivos de vehículos, electrodomésticos, domótica, etc.- a través de la red Internet. La facilidad de ejecutar ataques malintencionados expone tanto la confidencialidad de la información del usuario como la integridad de estos productos o servicios. Como ejemplo, la posibilidad de manipular un vehículo de forma remota aumenta las preocupaciones en el sector.

Seguridad en Smart Grid

Redes eléctricas inteligentes donde el flujo de información bidireccional que se genera puede ser interceptado, poniendo en riesgo los datos confidenciales de los usuarios. Se requieren medidas de seguridad tanto de sus sistemas de control como de las redes de intercambio de información.

Seguridad en infraestructuras críticas

Las infraestructuras críticas como centrales nucleares y redes energéticas, sistema financiero, salud, transportes, entre otras, son recursos importantes para un país. Proporcionan servicios esenciales y no disponen de una alternativa en el supuesto de sufrir un ataque. Los sistemas SCADA (Supervisión, Control y Adquisición de Datos) son objeto de ciberataques por sus problemas de seguridad y protección. El CNPIC (Centro Nacional para la Protección de Infraestructuras Críticas) es el encargado de supervisar, coordinar e impulsar su seguridad en España.

Seguridad en dispositivos móviles, BYOD

BOYD (*bring your own device*) se refiere al uso de dispositivos móviles propiedad del empleado en tareas corporativas de la empresa. Aporta beneficios económicos para la empresa y satisfacción en los empleados, sin embargo, introduce unos riesgos y amenazas importantes en las organizaciones. La falta de medidas de seguridad y el uso particular de *smartphones, tablets*, *netbooks*, ... los hacen vulnerables frente a posibles ciberataques.

Principales amenazas en el ciberespacio

Crime-as-a-service

El crimen como servicio, donde grupos criminales altamente cualificados y bien organizados ofrecen sus servicios – ciberataques, datos de tarjetas de crédito robadas, etc.- como negocio. Estos servicios se pueden contratar a través de la "*deep web*"[6] *o también llamada "internet profunda", "internet invisible" o "internet oculta".*

Ciberespionaje y Ciberguerra

La ciberguerra y el ciberterrorismo suponen la mayor amenaza para la ciberseguridad de los intereses nacionales. Utilizan técnicas APT (*Advanced Persistent Threat*) dirigidas a departamentos de las administraciones públicas, industrias de la defensa nacional, infraestructuras críticas, TIC, sectores energéticos, etc.

Según información publicada en 2015 por CCN-CERT (Centro Criptográfico Nacional – Equipo de Respuesta ante Emergencias Informáticas), "*la tendencia a reducir el ciberespionaje y la ciberguerra se incrementará en los próximos años por su dificultad de atribución y la eficacia de sus técnicas. No solo incumbe a gobiernos también se han detectado casos de ciberespionaje entre empresas privadas internacionales.*" *[En línea]* *https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/795-ccn-cert-resumen-ia-09-15-ciberamenazas-2014-tendencias-2015/file.html*

Malware

El *Ransonware* y *Cryptoware* son los *malware* más difundidos en el ciberespacio. Consiste en el secuestro del equipo atacado –*Ransonware*- o el cifrado de sus archivos -*Cryptoware*-, con el fin de pedir una cantidad de dinero a la víctima a cambio de su desinfección.

Según información publicada en 2015 por CCN-CERT, "*En los próximos años, aumentarán las incidencias de Ransonware agresivo.*"

El *Scareware* es otro tipo de *malware* que infecta el equipo y se manifiesta como un *software* de seguridad. Este muestra alertas de riesgos engañosas, con el fin de que la víctima compre el *software*.

---

[6] **Deep Web** según Wikipedia se refiere "Al contenido de internet que no es indexado por los motores de búsqueda convencionales, debido a diversos factores. El término se atribuye al informático Mike Bergman. Es el opuesto al Internet Superficial." [En línea] https://es.wikipedia.org/wiki/Internet_profunda

Hacktivismo

Sus actuaciones suelen estar ligadas a grandes conflictos sociales y políticos de actualidad. Son grupos organizados que realizan ciberataques de bajo impacto económico. Tienen como principal objetivo divulgar su causa en el ciberespacio.

Estafas

Phishing es una estafa por correo electrónico cuyo fin es obtener datos personales de los ciudadanos –contraseñas cuentas bancarias, etc.- para su posterior uso fraudulento. *Spear-Phishing* es similar pero aplicando técnicas de ingeniería social para recopilar datos de navegación, de redes sociales, etc., de la víctima, y utilizarlos posteriormente en la estafa, dando así una mayor credibilidad. En la figura 1, se observa la extensa área de acción de este tipo de delitos de estafa.

Figura 1. Estafas y fraudes cibernéticos. Phishing.

[Fuente] Antifraudnews por Ted Mapother (18 de marzo de 2013)

Ataques contra el punto de venta

Los métodos de pagos digitales a través de dispositivos móviles abren nuevas puertas a los ciberdelincuentes. También, los ataques contra cajeros automáticos pondrán en jaque la seguridad de la banca. Es preciso adoptar medidas de seguridad y concienciar a los usuarios de la importancia en su uso correcto. Estos ataques tendrán un impacto directo sobre los ciudadanos.

Tendencias en técnicas de prevención y respuesta

Security as a Service

Se refieren a servicios de seguridad basados en la nube. Permiten a las PYMES reducir costes en personal y satisfacer las normas de seguridad. Los servicios que ofrecen, entre otros, son correo electrónico seguro, monitorización de vulnerabilidades, prevención pérdida de datos, gestión de accesos, *gateway* y servicios *web*. El uso de estos tipos de servicio en las empresas ha aumentado considerablemente.

Big Data Analytics

La gran cantidad de datos almacenados en el *Big Data*[7] representa uno de los principales riesgo en ciberseguridad. Por el contrario, esta cantidad de datos es aprovechada por *Big Data Analytics* para analizar y gestionar las vulnerabilidades, riesgos y ataques, y responder eficientemente al incidente. La ciberseguridad basada en el análisis en tiempo real de los datos permite identificar y corregir las amenazas internas y externas de la empresa. Esta técnica por su elevado coste y recursos humanos cualificados suele ser utilizada en grandes empresas.

Seguridad en movilidad: MDM y MAM

Para minimizar los riesgos del BYOD, las empresas están implantando soluciones tecnológicas para la gestión de los dispositivos móviles a nivel corporativo, Mobile Device Management (MDM), y de las aplicaciones instaladas (borrado remoto, *tracking*, licencias *software*, etc.), Mobile Application Management (MAM).

Servicios de Seguridad Gestionada (MSS)

La sofisticación y complejidad de la ciberamenazas obliga a las empresas solicitar la ayuda de proveedores de servicios de seguridad gestionada (MSSP). Los servicios que ofrecen los MSSP incluyen, entre otros, bloqueo de *spam* y virus, detección de intrusos, *firewalls*, protección DoS (Denegación de Servicio), gestión VPN (Virtual Private Network) y actualizaciones de *firmware*, *software* y sistemas operativos.

---

[7] **Big Data**, Daniel J. Ollero en publicación (31/12/2014) en **Elmundo.es** lo define como: *"Una nueva tecnología que permite analizar grandes cantidades de datos de una forma rápida y eficaz de fuentes muy diversas. Una parte se recogen sobre nuestras llamadas telefónicas, transacciones bancarias, pagos con tarjeta o búsquedas en Google o movimientos a través de las señales GPS procedentes de nuestros teléfonos móviles. Otros los generamos de forma voluntaria cuando publicamos entradas y enviamos mensajes en blogs y redes sociales."*

Autenticación mejorada

Son técnicas utilizadas para evitar la suplantación de la identidad. Mejora la política de contraseñas sobre todo en el sector bancario, salud y administración. Los métodos más utilizados son: las contraseñas de un solo uso y enviadas a dispositivos móviles, biometría, autentificación de dos factores y *token* físico en la nube.

Simulación de incidentes de ciberseguridad

La experiencia práctica ante ciberataques aumenta la seguridad de la empresa u organización y permite el desarrollo de respuestas adecuadas, así como una eficiente gestión de los riesgos. Se realizan simulacros para el adiestramiento en técnicas y tácticas de prevención y recuperación ante ciberataques en un entorno lo más real posible "Ciber-Resiliencia".

> *"El Instituto Nacional de Ciberseguridad (Incibe), con sede en León, ha celebrado el primer encuentro 'International CyberEx 2015', el mayor ciberejercicio liderado por España en el que se realiza un simulacro de ataque cibernético con más de 300 profesionales de 21 países."* *León, 24 sep. (EFE)*
>
> LaVanguardia.com (24 de septiembre de 2015)
> http://www.lavanguardia.com/tecnologia/20150924

Hacking ético

Los denominados Hackers de "sombrero blanco" por cuenta ajena o contratados por las empresas realizan ataques "*pen test*" –test de penetración- a los sistemas informáticos e infraestructuras. La finalidad de sus actuaciones no busca un beneficio económico, político o social sino detectar vulnerabilidades con el objeto de aplicar acciones preventivas. Esta especialidad la están practicando analistas forenses informáticos, entre otros profesionales, por su cualificación y experiencia en esta materia.

Estrategia de Ciberseguridad Nacional

Desde 2013 España cuenta con su propio plan Estratégico en Ciberseguridad Nacional (ECN) al amparo del Plan Estratégico de Seguridad Nacional.

La Estrategia de Ciberseguridad Nacional es el documento que desarrolla los aspectos en materia de protección del ciberespacio con el fin de implantar las acciones de prevención, defensa, detección, respuesta y recuperación frente a las ciberamenazas. (U-Tad, 2015)

Según se refleja en el documento de Estrategia de Ciberseguridad Nacional (ECN) publicado en 2013 por la Presidencia de Gobierno con acceso desde enlace [En línea]:

http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf

Sus principales propósitos son:

- ✓ Identificar los riesgos y amenazas relacionadas con el ciberespacio.
- ✓ Definir los diferentes organismos responsables de la ciberseguridad nacional.
- ✓ Elaborar y difundir documentos donde se recogen las medidas que se deben abordar en materia de seguridad en el ciberespacio.
- ✓ Establecer la cooperación internacional con otros países.
- ✓ Liderar las relaciones público-privadas y fomentar la cooperación entre todos los actores del ciberespacio.

Sus principales líneas de acción son:

- ✓ Mejorar los sistemas de prevención y recuperación ante ciberamenazas, “Ciber-Resiliencia”.
- ✓ Garantizar la seguridad de los sistemas de las administraciones públicas e infraestructuras críticas de país.
- ✓ Fomentar la investigación y persecución de la ciberdelincuencia y el ciberterrorismo, en base a un marco legal nacional e internacional.
- ✓ Promover la cooperación internacional.
- ✓ Impulsar el uso responsable del ciberespacio y de las TICs.
- ✓ Promover la formación a profesionales y la I+D+i en materia de ciberseguridad.

Organismos nacionales en materia de Ciberseguridad

Las competencias nacionales relacionadas con la gestión de la ciberseguridad se reparten entre organismos e instituciones dependientes de diferentes ministerios del gobierno central o autonómico, como se muestra en la tabla 1.

Organismo	Acrónimo	Ámbito	Competencias en ciberseguridad
Instituto Nacional de Ciberseguridad	INCIBE	Nacional	Entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital en el ciberespacio.
Centro de Respuesta de Seguridad e Industria	CERT	Nacional	Centro de Respuesta a incidentes de Ciberseguridad operado por INCIBE. Prevención de amenazas e investigación en ciberdelitos y ciberterrorismo.
Capacidad de respuesta a incidentes de seguridad de la información del Centro Criptológico Nacional.	CCN-CERT	Nacional	Centro nacional de alerta y respuesta rápida ante ciberataques a los sistemas de la administración pública y empresas de sectores estratégicos.
Centro Nacional para la Protección de Infraestructuras Críticas	CNPIC	Nacional	Garantizar seguridad de las infraestructuras que proporcionan servicios esenciales a la sociedad.
Centro de Seguridad de la Información y nuevas Tecnologías de la Comunidad Valenciana	CSIRT-CV	Autonómico	Contribuir a la mejora de la seguridad de los sistemas de información públicos e infraestructuras críticas de la CV. Representante de la Generalitat Valenciana en seguridad.
Grupo de Delitos Telemáticos de la Guardia Civil	GDT	Nacional	Dentro de la UCO (Unidad Central Operativa de la Guardia Civil) el GDT fue creado para investigar todos aquellos delitos relacionados con Internet.
Brigada de Investigación Tecnológica del Cuerpo Nacional de Policía	BIT	Nacional	Creada para responder a estos nuevos delitos y dedicada a obtener pruebas, perseguir a los delincuentes y poner a unas y a otros a disposición judicial.
Agencia Española de Protección de Datos	AEPD	Nacional	Velar por el cumplimiento de la normativa en materia de protección de datos personales. LOPD.
Mando Conjunto de Ciberdefensa	MCCD	Nacional	Centro de Respuesta a incidentes de seguridad de la información de los ejércitos.

Tabla 1. Organismos e instituciones nacionales en Ciberseguridad

Directiva Europea y acuerdos internacionales en materia de Ciberseguridad

Para garantizar la seguridad global en la Unión Europea, el Consejo Europeo propuso en 2013 la creación de la Directiva Europea sobre Ciberseguridad[8] (NIS –*Network Information Security*). Esta Directiva tiene como objetivos:

- ✓ Mejorar la cooperación entre sus estados miembros, sectores públicos y privados.

- ✓ Exigir a las empresas de sectores críticos implanten políticas de seguridad y gestión de riesgos. Certificación de cumplimiento de la nueva ISO 27001:2013. Así como, elevar a las autoridades nacionales los incidentes acaecidos.

- ✓ Mejorar las capacidades de ciberseguridad nacional a sus estados miembros.

En la siguiente tabla se describen los **acuerdos internacionales** adoptados como medida de colaboración y coordinación de la ciberseguridad global.

Acuerdo	**Descripción**
Proceso Meridian	Conferencias anuales para Intercambio de ideas y acciones sobre la protección de las infraestructuras críticas de la información.
Convenio sobre Ciberdelincuencia	Este documento firmado en Budapest en 2001, se centra en establecer una legislación uniforme donde detalle las actividades consideradas delictivas en el ciberespacio. Su finalidad es facilitar la imputación a nivel internacional del Ciberdelito.
SOG-IS	Establecer criterios comunes en evaluación de seguridad de tecnología de la información. Estandarización de los perfiles de protección y políticas de certificación entre Organismos Europeos de Certificación. Coordinar la implantación nacional de leyes y acuerdos dictadas por la Comisión Europea en materia Seguridad de la Información.
FIRST	Forum of Incident Response and Security Teams. Red de equipos individuales de respuesta a incidentes de seguridad informática, que se agrupan para hacer frente a ciberataques y cómo prevenirlos. Está formado por gobiernos, policías, empresas, universidades …
iWWn	International Watch and Warning network. Red de colaboración internacional ante ciberataques y vulnerabilidades detectadas. Se comparte información y se fomenta la concienciación de la situación del ciberespacio.
PCR	Partnering for Cyber-Resilence. Creado a iniciativa del Foro Económico Mundial en 2012 para dar respuesta a la importancia de la ciberseguridad. Se encarga de cuantificar y evaluar las ciberamenazas y fomentar la Ciber-Resiliencia.

Tabla 2. Acuerdos internacionales en ciberseguridad

[8] **Directiva Europea sobre Ciberseguridad** [En línea] http://ec.europa.eu/digital-agenda/en/news/network-and-information-security-nis-directive

Declaración de independencia del ciberespacio

La ciberseguridad, como aplicación de medidas de proteccón, seguridad, control y fiscalización que los gobiernos europeos e internacionales imponen en el ciberespacio provocan el rechazo de los sectores más liberales y pro-anarquistas de la cibersociedad. Estos proclaman un espacio social global independiente por naturaleza de las tiranías que los gobiernos imponen.

Según texto presentado en, Suiza, el 8 de febrero de 1996 por John Perry Barlow [9], fundador de la Electronic Frontier Foundation (EFF). *"Barlow se convirtió en el Thomas Jefferson de la generación 'wired' por su autoría del documento que se transmitió por 'todo el mundo': 'Una declaración de independencia del ciberespacio.' Es una reivindicación contra la interferencia del gobierno al mundo de Internet y a favor de un ciberespacio soberano."*

Figura 2. Declaración de independencia del Ciberespacio

[Fuente] Barlow, 1996

[9] **Barlow (1996).** Una declaración de Independencia del Ciberespacio [En línea] http://austroanarquistas.com/?p=3521

3 El perito informático

Lo primero que el lector se pregunta es: ¿Qué es un perito informático?

Se define **perito informático** como "*Un profesional experto y titulado, dotado de conocimientos legales, teóricos y prácticos especializados en informática y tecnologías de la información, capaz de asesorar o elevar un dictamen comprensible y a la vez técnico sobre un litigio o cualquier otra situación que se le requiera*" (del Peso Navarro, 2001).

Respecto a sus ámbitos de actuación estos se agrupan básicamente en dos, aquellos que tienen carácter judicial y los que no son requeridos por un tribunal, los extrajudiciales. Aunque el resultado de sus dictámenes, así como el propio procedimiento de investigación y análisis, no deben estar condicionados a esta situación. Por esto, el perito debe realizar su labor profesional al margen de si ha sido requerido por acto judicial como si no. Este aspecto es una cualidad que diferencia al "buen" perito informático.

De forma generalizada el perito informático en el desempeño de su labor tiene como objetivos: el desarrollo de un informe pericial -tasación, estudio, auditoria, dictamen forense- tanto en el ámbito judicial como extrajudicial, y el desarrollo de una actividad particular de consultoría, asesoramiento, mediación y arbitraje solicitada por empresas u organismos privados.

Las áreas de conocimiento de un perito informático son extensas y requieren de una constante actualización tanto en aspectos tecnológicos y metodológicos como legales. Por ello, el perito informático forense, debe ser consciente de sus limitaciones profesionales, -es imposible ser experto en todas las ramas y especialidades- y recurrir a equipos de peritos, en caso de necesidad, para abarcar todas las áreas de especialización. No basta con poseer los conocimientos técnicos, legales y prácticos sino que debe garantizar que el resultado de su trabajo sea objetivo, metódico, demostrable, reproducible, veraz, auditable, creíble, honesto y profesional.

En el ámbito penal y criminal, el fin en toda investigación policial, es poner a los delincuentes y criminales en manos de la justicia. Para ello, es importante que el perito informático forense proceda de acuerdo a derecho, aplicando técnicas y métodos que garanticen la autenticidad e integridad de la información procesada para que esta sea válida ante un tribunal.

Por lo expuesto anteriormente, es relevante conocer en que ámbito se desarrolla la labor de un perito informático forense y ser conscientes del grado de responsabilidad legal que tiene en el procedimiento de la causa.

Ámbitos de actuación

Si echamos la mirada atrás, la mayoría de demandas de peritaciones informáticas se desarrollaban dentro del ámbito particular o empresarial, pero cada vez más, la figura del perito informático forense es requerida como auxiliar de la justicia para el dictamen de evidencias tecnológicas que faciliten al juez el esclarecimiento de un litigio.

Por otro lado, sus conocimientos de análisis forense digital son demandados por empresas, organizaciones y gobiernos para fortalecer la seguridad informática, y del resultado de su investigación ante un ciberataque, determinar las medidas de respuesta y nuevas políticas de seguridad a implantar.

Apuntar, que los especialistas en ciberseguridad requieren de conocimientos, entre otros, de análisis forense, análisis de malware, análisis y evaluación de vulnerabilidades, gestión de incidentes, manejo de herramientas *hacking* ético, auditoria de redes; áreas todas ellas con competencias del perito informático forense.

Ámbito judicial

El perito informático judicial, es aquel perito informático que desarrolla su labor dentro de un procedimiento judicial sea penal o criminal. Puede ser designado por cualquiera de las partes o a petición del tribunal. Cuando un perito informático forense es nombrado por un magistrado o un juez, se transforma en auxiliar de la justicia y debe realizar la función pública según el cargo conferido y de acuerdo a derecho, como se establece la Ley Orgánica del Poder Judicial en sus artículos del 470 al 480.

En el ámbito judicial, el perito informático forense, es un experto designado por la autoridad del proceso judicial, para que mediante investigación especializada en materia informática en base a los requerimientos exigidos, dictamine con objetividad, honestidad, imparcialidad y veracidad, las conclusiones de su pericia mediante un informe o dictamen pericial.

El resultado de su investigación es aportado en función de la localización de las evidencias digitales, las herramientas utilizadas para el análisis forense, los métodos y normas aplicadas y su desempeño como experto en la materia encomendada.

La administración de justicia y abogados, están comprobando lo expeditivo e infalible que resulta la localización de las evidencias digitales, que sirven de apoyo para el esclarecimiento de los casos, por lo que contar con un perito informático forense puede ser vital para evitar o imputar una condena.

Para ejercer como perito informático judicial –perito de oficio- en España, es indispensable una titulación oficial y/o ser reconocido por una entidad profesional de peritos informáticos, o colegio oficial reconocido por el Ministerio del Interior, en la que haya acreditado sus conocimientos y su pericia, de conformidad con lo establecido en los artículos 340 y 341 de la Ley de Enjuiciamiento Criminal y la instrucción 5/2001 de 19 de diciembre del Consejo General del Poder Judicial y el Protocolo de 9 de febrero de 2005, modificada por el Acuerdo del Pleno del Consejo General del Poder Judicial de 28 de octubre de 2010 sobre la remisión y validez de las listas de Peritos Judiciales remitidas a los Juzgados y Tribunales por las Asociaciones y Colegios Profesionales, publicado en el BOE nº 279 de 18 de noviembre de 2010.

Además, al perito informático judicial se le exigen ciertas cualidades adecuadas para su correcta función, entre ellas su neutralidad hacia las partes. Y poseer un perfil técnico en análisis forense digital, con grandes conocimientos legales y en ciencia criminalística, que le permitan ejercer ante los tribunales de modo que su labor no sea impugnada o descalificada por la parte contraria.

Respecto al informe o dictamen del perito informático judicial, según el Consejo General de Peritos Judiciales en su web (http://www.consejoperitos.com/-dictamen-pericial-.html) lo define: "C*omo el documento en el que se refleja las anotaciones y conclusiones minuciosas llevadas a cabo por el perito y debe destacar por su redacción sencilla, comprensible y detallada, en la que se incluya descripción de "la cosa", con algún dato de interés y obviando lo insignificante. Se debe reflejar la situación de forma clara y concisa para que sea entendido y procesado correctamente por parte del Juez, sin necesidad de tecnicismos que lleven a la incomprensión."*

Hay que tener en cuenta que este documento servirá como asesoramiento a los abogados en el momento de aportar la prueba ante un tribunal, de manera que el principal objetivo del informe o dictamen pericial será la reproducción exacta de lo requerido. Por tanto, el perito informático judicial deberá recopilar la información que es puesta a su disposición –pruebas originales-, analizar la misma en busca de los datos –evidencias- que el juez le ha requerido y formular un informe o dictamen pericial donde se reflejen las conclusiones de la investigación realizada.

Ámbito extrajudicial

La peritación extrajudicial surge de las relaciones entre empresas, profesionales y particulares en situaciones en las que se requiere a un experto en la materia en cuestión, garantizando una visión objetiva, imparcial y experta en la investigación. Es posible que el informe pericial aportado por el perito sea utilizado como prueba en un futuro procedimiento judicial. Por norma general, el perito es solicitado para casos de arbitraje y de mediación.

Los casos de **arbitraje** se ejercen con el fin de evitar juicios en los tribunales, siempre que no se haya infringido la ley. Serán los árbitros quienes tomen las decisiones e informen ante cuestiones litigiosas surgidas o que puedan surgir en una materia. Este arbitro independiente –perito- debe tratar a las partes con igualdad y garantizar los

derechos de las partes en litigio. El proceso arbitral es más flexible que el judicial llegando incluso a llevarse a cabo por escrito sin necesidad de parte oral.

La **mediación** es un proceso voluntario en el que dos o más partes involucradas en un conflicto trabajan con un profesional imparcial, el mediador, para generar sus propias soluciones para resolver sus diferencias.

A diferencia de un juez, o un árbitro cuyas decisiones obligan a las partes, e implican que una parte gana y la otra pierde, la mediación busca obtener una solución válida para ambas partes.

La mediación es una forma flexible de resolución de conflictos, que permite a las partes en disputa una solución previa a lo que hubiera constituido un litigio. La mediación ofrece a las partes una oportunidad de ganar una mayor comprensión de su conflicto, y disminuir el coste (tanto en tiempo como en dinero) que implica un procedimiento legal completo.

Deberes del perito informático

- Ser objetivo y ajeno completamente al proceso en el cual se le requiere o se presenta su participación.
- Ser una persona imparcial y sin intereses particulares.
- Poseer los conocimientos, la experiencia y la formación teórico-práctica como experto en la materia.
- Rechazar cualquier proceso que le sea imputado por coacción y no pueda ejercer de manera voluntaria.
- Aceptar el cargo que le es asignado, colaborar con los asesores jurídicos y el resto de los peritos o consultores técnicos y declarar ante el juez en el caso de que este lo requiera.
- Fundamentar sus conclusiones técnicas, expresando claramente los elementos analizados y las técnicas utilizadas para llegar a las mismas.
- Respetar el código de ética que le impone su profesión.

Deontología y ética profesional

La **deontología** informática recoge los principios éticos que deben ser asumidos por todos los profesionales de la informática pertenecientes a una asociación, colegio oficial u organismo. En ellos residen los criterios fundamentales de la profesión de perito informático forense aplicados con un sentimiento imperativo del deber autoimpuesto, es decir, unos deberes que lejos de ser impuestos, aspira a que sean libremente asumidos por los propios profesionales. Sin embargo, para garantizar el cumplimiento de esta normativa deontológica por parte de las instituciones, generalmente su infracción está sujeta al régimen sancionador definido en sus Estatutos internos.

La ética presenta algunos principios -no exigibles pero sí deseables- que sirvan de guía en el comportamiento profesional, en el sentido de animar y potenciar aquellas actitudes que proporcionan, a través del ejercicio de la profesión, un mayor bien a las personas directamente relacionadas con el ingeniero en informática y la sociedad en general.

Como estándares de referencia para elaboración de códigos éticos y deontológicos cabe destacar:

- El Código de Ética y Práctica Profesional de Ingeniería del Software de la ACM (Assocation for Computing Machinery) / IEEE Computer Society / (Institute of Electrical and Electronic Engineers, Inc.) (1992)

- 'Propuesta de Código Deontológico' de ALI Nacional (Asociación de Titulados en Ingeniería Informática).

Los códigos de conducta ética y deontológica van más allá de la pura normativa legal, puesto que ayudan a guiar el comportamiento en infinidad de situaciones para las que no existe ninguna referencia legal.

En base a los principios profesionales del código deontológico de la Asociación de Ingenieros Informática –ALI- en su documento de 2009 "Código Deontológico" en pág. 6 apdo. 5 [línea] http://www.ali.es/wp-content/uploads/sites/4/2015/10/COD_DEONT_20081010-CON-modificacionesMD-y-AGE-v03.pdf, el profesional deberá:

- *Promover el conocimiento general de la profesión y su aportación al bien público.*

- *Difundir el conocimiento de ingeniería en informática, en especial el peritaje informático mediante la participación en organizaciones profesionales, congresos y publicaciones.*

- *Apoyar, como miembros de la profesión, a otros Ingenieros en Informática que se esfuercen a actuar según este código.*

- *No anteponer el interés propio al de la profesión, el cliente o el empresario.*

- *Observar todas las leyes que rigen su profesión, a menos que, en circunstancias excepcionales, tal cumplimiento sea antepuesto al del interés general.*

- *Definir con veracidad las características y funcionalidades de los sistemas informáticos y/o proyectos en los que trabajan, evitando exageraciones, falsas expectativas y especulaciones.*

- *Asumir la responsabilidad de detectar, corregir y documentar errores en los sistemas, proyectos y documentaciones en las que se trabaje.*
- *Asegurarse que los clientes y empresarios conocen la obligación de el/la Ingeniero de Informática con respecto a este código, y las consecuencias derivadas de tal obligación.*

- *Evitar asociaciones con organizaciones y empresas que estén en conflicto con este código.*

- *Expresar las objeciones pertinentes a las personas implicadas cuando se detecten incumplimientos significativos de este código.*

- *Informar sobre las vulneraciones de este código, a las autoridades pertinentes en caso de que se trate de un delito, cuando esté claro que consultar a las personas implicadas en estas inobservancias es contraproducente o peligroso.*

Destacar la importancia del cumplimiento del código deontológico y ético profesional asumido por el profesional, pues los colegios oficiales están obligados por ley a inhabilitar a todo aquel colegiado que lo incumpla. Para las asociaciones no existe ley que obligue a la inhabilitación de sus asociados aunque suelen disponer de estatutos y normas sancionadoras al respecto, bien es cierto que salvo caso fragante, no se suelen dar de baja puesto que dejarían de percibir la cuota de este miembro.

Por todo esto, a la hora de elegir al perito informático se aconseja ir a los colegios oficiales, de esta forma se garantiza tanto la acreditación de su titulación universitaria en informática, como su ética y deontología profesional.

Tipos de peritajes informáticos y áreas de actuación

En la tabla 3, se detallan los distintos tipos de peritaje informático y sus desempeños. Se observa como el aspecto multidisciplinar del peritaje informático desemboca en una especialización profesional de la figura del perito informático. El desarrollo de este trabajo se centra principalmente en el estudio del peritaje forense digital o tecnológico.

	Descripción	**Actuaciones**
FORENSE DIGITAL O TECNOLOGICO	El peritaje más relacionado con la tecnología. Se podría incluir el análisis forense en materia de ciberseguridad y peritaje judicial. Su objetivo es obtener evidencias digitales que se encuentran en dispositivos físicos o virtuales. Realizar el análisis forense en busca de indicios y aportar como resultado de su investigación un informe o dictamen pericial.	- Identificación y recopilación de evidencias. - Análisis forense de dispositivos IT. - Análisis de redes y su tráfico. - Análisis de la información y contenido. - Trazas y rastros de los ficheros. - Falsedad y manipulación de ficheros. - Recuperación y reconstrucción inf. - Tratamiento de imágenes y multimedia. - Ciberseguridad y hacking ético.
DE GESTIÓN O DE MANAGEMENT	Su objetivo es la obtención de la información, evaluación y constatación de la misma para poder establecer las relaciones y compromisos contractuales que se originan entre proveedor y cliente bien sean en los conceptos de proyectos, implantaciones de soluciones, productos o servicios, diseño y desarrollo de aplicaciones informáticas, la explotación de los sistemas, implementaciones de seguridad y estándares normativos.	- Gestión de la protección de datos. - Gestión de proyectos. - Explotación de los servicios. - Gestión IT *Governance.* - Gestión de categorías y roles. - Gestión contractual y de acuerdos. - Gestión de consultoría y soporte. - Propiedad intelectual e industrial. - Gestión de la seguridad informática.
TASADOR TECNOLOGICO	El objetivo de la tasación informática es valorar económicamente determinados activos informáticos, mediante distintas técnicas que incluyen el cálculo del retorno de la inversión para un proyecto informático, del esfuerzo en personas-meses invertido en la construcción de un proyecto software, del costo de determinadas licencias de software ilegalmente utilizadas, del valor económico de equipos informáticos teniendo en cuenta la antigüedad de los mismos y la inflación, etc.	- Estimaciones de daños y perjuicios. - Creación y fusión de empresas. - Compra de empresas y procesos. - Escisiones o disoluciones de empresas. - Liquidación de empresas a concurso de acreedores. - Estimación de inversiones. - Valoraciones internas de activos. - Auditorias contables. - Recapitalización de la empresa.
AUDITOR	Los principales objetivos de la auditoria informática son: - el análisis de la eficiencia de los sistemas informáticos, evaluando si hay carencias o si, por el contrario, están sobredimensionados. - la verificación de la existencia de unas mínimas pautas de protección de la información, tanto desde el interior, como desde el exterior. - la revisión de la eficaz gestión de los recursos informáticos, estableciendo mecanismos de control pasivos (prevención de ataques), y activos (capacidad resiliencia). - generar un balance de los riesgos en TI (Tecnologías de la Información). - realizar un control de la inversión en un entorno de TI.	- Auditoría de la gestión de la contratación de bienes y servicios. - Auditoría legal, cumplimiento LOPD. - Auditoría de los datos. - Auditoría de las bases de datos. - Auditoría de la seguridad de datos como disponibilidad, integridad, confidencialidad, autenticación y no repudio. - Auditoría de la seguridad lógica, referida a autentificación. - Auditoría de las comunicaciones. - Auditoría de la seguridad en producción, frente a errores, accidentes y fraudes.
MEDIADOR	La mediación puede permitir el realizar un acercamiento entre dos partes bajo un conflicto. Proporciona un ahorra de tiempo y costes a las empresas.	- Mediación en conflictos de programación de páginas webs. - Incumplimiento de servicios TI. - Incumplimiento de soporte técnico.

Tabla 3. Clases de peritajes informáticos

En la figura 3 se muestran las distintas áreas multidisciplinares del peritaje informático y análisis forense digital, todas ellas desempañadas por el perito informático. Notar, que el mercado laboral del peritaje y análisis forense informático ofrece a los estudiantes en ingeniería informática y profesionales del sector una excelente 'salida' en estos tiempos de crisis global.

Figura 3. Ámbito multidisciplinar del peritaje informático

[Fuente propia]

Requisitos para ejercer como perito informático

Como se constata en apartados anteriores, la profesión de perito informático es una ciencia multidisciplinar, que abarca desde derecho legal, la ciencia criminalística, seguridad informática, ingeniería informática y análisis forense digital, entre otras, hasta conceptos, más allá de los puros técnico – científicos, que permitan observar el entorno a investigar –ciberespacio- como una estructura de relaciones virtuales en la actual cibersociedad.

Para ser perito informático, hay que cumplir una serie de requisitos que establece el actual reglamento legislativo, y nada sencillas de cumplir. Esto es así porque por las decisiones de un perito informático son muy importantes y pueden afectar directamente a la vida de los ciudadanos.

En el apartado referido al "Ámbito de actuación judicial" se detallan los requisitos que debe tener un perito informático para ejercer en el ámbito judicial, a continuación se completa y amplia esta información desde un visto de vista de ámbito general.

Requisitos generales

La regulación de la actividad del perito se establece en la Ley de Enjuiciamiento Civil (L.E.C. 1/2000), que regula los procedimientos judiciales civiles y los medios de prueba, que es al fin y al cabo lo que aporta el perito.

En el artículo 299 se detallan los medios de prueba de que se podrán hacer uso durante el juicio, entre las que se encuentra en el punto 4 el dictamen de peritos.

En el artículo 339 se regula la solicitud de designación de peritos y sus honorarios y en el artículo 340 se fijan las condiciones que habrán de reunir los peritos donde establece que *"el perito deberá estar en posesión de la titulación oficial relacionada con la materia del dictamen."*

Por ello, el **primero** de los requisitos para ejercer como perito informático es disponer de alguna de las titulaciones siguientes:

- Ingeniero en Informática.
- Licenciado en Informática.
- Master en Ingeniería Informática.
- Ingeniero Técnico en Informática.
- Diplomado en Informática.
- Grado en Ingeniería Informática.
- Título extranjero equivalente, convalidado según ley española.

Como **segundo** requisito para ejercer como perito informático judicial es carecer de antecedentes penales. No puede ser perito de oficio y tomar decisiones que afecten a un juicio si antes has sido condenado.

El **tercer** requisito es demostrar que se sabe peritar. La formación específica en análisis forense digital, en derecho informático y criminalística, en nuevas tecnologías, y demás áreas relacionadas con el peritaje informático, es considerada a la hora de elegir el perfil del perito que investigue un caso. En este aspecto es recomendable realizar cursos y másteres impartidos por los colegios oficiales, por las universidades y/o por las asociaciones reconocidas. También, es necesario acreditar la experiencia práctica en casos similares, información proporcionada por colegios y asociaciones a los tribunales y abogados en el supuesto de procesos judiciales.

El **cuarto** requisito es pertenecer a una asociación de peritos informáticos reconocida por el ministerio y/o ser miembro del colegio oficial de ingenieros de informática de su comunidad autónoma. En este sentido existen controversias, pues cada uno 'barre para casa', a la hora de establecer los criterios que siguen los tribunales para solicitar los servicios de un perito informático. Realmente para ejercer como perito informático judicial es muy importante estar incluido en las listas de peritos de oficio que anualmente remite el colegio oficial a los juzgados de su comunidad, y de estas el juez escoge el profesional más cualificado o aquel propuesto por el colegio oficial.

Por otro lado, si nuestro interés se centra en trabajar en las áreas científicas y tecnológicas, relacionadas con el análisis forense digital, de las Fuerzas y Cuerpos de seguridad del estado, será necesario, un **quinto** requisito, aprobar las pruebas básicas de acceso a los determinados cuerpos –oposiciones-, realizar los cursos y superar los exámenes en las distintas academias oficiales del cuerpo, que dan acceso a cubrir las plazas vacantes ofertadas.

Asociaciones nacionales y colegios oficiales

En la tabla 4 se muestran las asociaciones nacionales, más conocidas, de peritos y tasadores informáticos, y en la tabla 5 algunos colegios oficiales de ingenieros en informática, donde comprobar las condiciones y requisitos para darse de alta como socio o colegiado, y recabar información sobre cursos, másteres y certificaciones ofertados.

En sus contenidos web se pueden encontrar artículos y publicaciones muy interesantes y recomendables para todo futuro perito informático.

Asociaciones		
ACPJT	Asociación Catalana de Peritos Judiciales Tecnológicos.	www.acpjt.cat
APTAN	Asociación de Peritos Judiciales Tecnológicos	www.aptan.es
ANCITE	Asociación Nacional de Ciberseguridad y Pericia Tecnológica.	www.ancite.es
AEMPJ	Asociación Española de Mediación y Peritación Judicial.	www.aempj.org
AEDEL	Asociación Española de Evidencias Electrónicas.	aedel.es
ANTPJI	Asociación Nacional de Tasadores y Peritos Judiciales Informáticos	www.antpji.com/antpji2013/

Tabla 4. Asociaciones nacionales de peritos informáticos

Colegios oficiales de Ingenieros en Informática		
CCII	Consejo General de Colegios Profesionales de Ingeniería en Informática	www.ccii.es
CPIIA	Colegio Profesional de Ingenieros en Informática de Andalucía	cpiiand.es
COIIPA	Colegio Oficial de Ingenieros en Informática del Principado de Asturias	coiipa.org
CPIICM	Colegio Profesional de Ingenieros en Informática Comunidad de Madrid	cpiicm.es
COIICV	Colegio Oficial de Ingenieros en Informática de la Comunidad Valenciana	www.coiicv.org
COEINF	Colegio Oficial de Ingeniería en Informática de Catalunya	enginyeriainformatica.cat

Tabla 5. Colegios Oficiales de ingenieros en informática

El informe o dictamen pericial

El valor del trabajo realizado en una investigación de análisis forense digital reside en la documentación que se entrega como resultado de todo el proceso, el informe pericial, siendo este el principal elemento de juicio respecto de la labor del perito informático forense.

A la hora de afrontar el desarrollo de un informe pericial hay que tener en cuenta que:

- El objetivo es transmitir información objetiva y clara, con la mínima carga de términos técnicos pero sin desestimar aquellos datos técnicos que puedan producir una pérdida de rigor en la información presentada.
- Es necesario dejar constancia de la condición de imparcialidad del perito.
- Posiblemente, el receptor del informe no sea un experto en la materia, y por tanto, el informe debe ser redactado utilizando métodos pedagógicos que faciliten su comprensión.
- No debe parecer que sea una demostración de las habilidades y capacidades técnicas del perito.
- El informe debe dar respuesta a las cuestiones planteadas en el inicio de la investigación.
- No debe contener otra información que no sean los resultados objetivos obtenidos durante la investigación.
- Debe presentar una línea maestra bien definida.
- Los objetivos iniciales deben estar alineados con el desarrollo del informe.
- No puede presentar cuestiones no resueltas adecuadamente.
- La información recabada debe de justificar cuestiones relativas a la resolución del caso.
- El informe debe seguir una estructura documental claramente definida.

Según lo establecido por Babitsky, S. y Mangraviti, J.r, J.(2002) un informe pericial persuasivo, comprensivo y formal debe considerar las siguientes pautas (Cano 2009, pág 172):

- No especule o trate de adivinar cosas.
- Evite el uso de universales o absolutos como “siempre”, “nunca”, “para todos los casos”.
- Evite expresiones que sugieran vaguedad, aspectos equívocos o incertidumbre.
- Evite el uso de lenguaje empático, signos de exclamación, uso de formatos, como negrita, itálicas y mayúsculas para enfatizar los hallazgos o conclusiones.
- Use lenguaje preciso sin jerga.
- Use un lenguaje seguro, sin adornos literarios y evite las palabras como “se ve cómo”, “podría”, “aparentemente”, “yo creo”, “es probable que”, entre otras.

- Defina todo término técnico propio del informe.
- Use un lenguaje concreto sobre los hechos, y evite caracterizaciones subjetivas para describir la investigación, los hallazgos y las conclusiones.
- Explique cualquier abreviatura utilizada.
- Evite lenguaje argumentativo que pueda sugerir un interés particular.
- Evite comentarios sobre la credibilidad de los testigos y las pruebas.
- Validar la consistencia del informe.
- Evite cualquier sesgo en su informe.
- Numere las líneas de su informe, para que en caso de requerirse alguna revisión de sus resultados, se remitan de manera rápida al sitio en el mismo.

Estructura general

Si bien cada informe pericial tiene su propia característica y dinámica, se presenta a manera de ejemplo la estructura general de un informe o dictamen pericial orientado particularmente a la investigación y análisis forense digital (Cano, 2009, pág 174).

La estructura y contenidos de cada uno de sus apartados son:

1. *Encabezado del informe* que identifica, la fecha de entrega del informe, que se quiere hacer, número de identificación del caso, quienes participan, la clasificación del nivel de seguridad y los peritos participantes en la investigación.

2. *Introducción,* donde se detalla las características básicas del caso extraídas de los datos ofrecidos por las partes solicitantes. Se determina el alcance de la pericia que se adelanta, con el fin de limitar los análisis y exploraciones a lo que requiere para el caso particular.

3. *Validación y verificación de la cadena de custodia,* aquí se detalla y registra la evidencia con su formato de cadena de custodia, donde se describe, que se recibe, de quién, en qué fecha, las características de los elementos, sus marcas y modelos, números de serie, los nombres de los peritos que lo reciben, la identificación del caso…

4. *Procedimientos de preparación y adecuación de la evidencia recibida*, se describen los procedimientos relacionados con los dispositivos informáticos que se disponen para la copia del material recibido, las herramientas y programas utilizados para esta labor y posterior análisis, las verificaciones de las copias y el detalle del análisis que se va a realizar según lo descrito en la introducción.

5. *Análisis de evidencias*, aquí se realiza el análisis detallado de las copias de las evidencias, usando herramientas *software* y *hardware* validados y verificados en

la fase anterior. Se detallan las técnicas utilizadas para identificar y extraer los datos de los dispositivos entregados para su análisis.

6. *Hallazgos identificados,* en esta sección se presenta lo relevante encontrado de la exploración de las evidencias y que sea relacionado con la investigación del caso. Se presentan tal y como se indica en las herramientas, sin análisis ni opiniones al respecto.

7. *Conclusiones,* aquí se describen los análisis de los hallazgos en el contexto de la investigación, basados en las formas científicas y técnicas que sean válidas por un tercero si así se requiere. Las afirmaciones que se hagan deben corresponder a lo que la formalidad técnica establece, a las características de los dispositivos analizados y los hechos investigados en el caso.

8. *Firma de los peritos,* con la firma el perito refrenda y se hace responsable del contenido del informe o dictamen y todo lo que allí se encuentre. Conviene firmar con pluma especial y de color distinto al negro y en todas las hojas como medida de confiabilidad sobre el informe, por si un tercero quisiera alterar el contenido del mismo sin autorización.

Para complementar esta estructura general y orientativa, se deberían aplicar las normas UNE relacionadas con la elaboración de informes y dictámenes periciales, donde se describen los requisitos que deben tener dichos informes en general y en concreto en el ámbito de las TIC.

Estas normas son:

- ✓ UNE 197001:2011 “Criterios generales para la elaboración de informes y dictámenes periciales”

- ✓ UNE 197010:2015 “Criterios generales para la elaboración de informes y dictámenes periciales sobre Tecnologías de la Información y las Comunicaciones”

En esta guía se describen las normas UNE 197001 y UNE 197010 de manera conjunta al ser estas complementarias y necesarias para la elaboración correcta de informes o dictámenes periciales TIC.

Las Normas UNE 197001:2011 y UNE 197010:2015

En estas normas se establecen los requisitos formales que deben tener los informes y dictámenes periciales, y en concreto, en el ámbito de las TIC, sin determinar los métodos y procesos específicos para la elaboración de los mismos.

Como referencia se estudia el contenido de la norma UNE 19010:2015, que como ya se ha comentado, engloba los aspectos y contenidos de la norma UNE 197001:2011.

Para definir el cuerpo del informe o dictamen pericial se hace referencia a la norma UNE 50132 donde se enumeran los puntos que componen el cuerpo del informe como: título, capítulos y apartados.

UNE 197010:2015[10]

En su introducción se tratan los principios que deben acompañar al proceso de selección, obtención, presentación y almacenado de las evidencias digitales. También, se hace referencia explícita del uso de la norma UNE 197001:2011 en aquellos apartados que se requiera.

Estos principios son:

- La Relevancia, es la propiedad que resalta unas evidencias sobre otras en función de su transcendencia y valor que aportan en el informe pericial.

- La Fiabilidad, que se puedan reproducir los resultados del proceso de forma consistente con investigadores independientes, obteniendo las mismas evidencias.

- La Suficiencia, es la demostración que la evidencia presentada es representativa, acorde y proporcionada con el objeto del informe.

- La Oportunidad, se refiere a las circunstancias y momento temporal en la que se presenta la evidencia como prueba y pueda ser transcendente en el juicio.

[10] **Norma UNE 197010:2015** Obtenida a texto completo a través del servicio de la Biblioteca de la UPV. Base de datos en Aenormás.

En su apartado 4 se describen los requisitos generales del informe pericial:

1. Título, es imprescindible y debe identificar de forma clara e inequívoca el proceso de investigación.
2. Estructura básica, donde se especifica los contenidos mínimos que debe tener todo informe pericial:
    - Identificación.
    - Índice.
    - Cuerpo del informe.
    - Anexos (si corresponde).
3. Además de la estructura básica, todo informe pericial TIC debe contener:
    - Declaración de imparcialidad.
    - Juramento o promesa (si procediera).
    - Conclusiones.
    - Firma.
    - Visado (cuando proceda).
4. Paginación, en todas las páginas debe figurar la identificación del informe, el número de página y el total de páginas.
5. Contenido, la información con la que debe iniciarse el informe es:

    - título y su código o referencia de identificación,
    - nombre del organismo/s a los que se dirige y número de expediente,
    - nombre y apellidos del perito, su titulación, colegio o entidad a la que pertenece, DNI, domicilio profesional, teléfono y correo electrónico,
    - nombre, apellidos y documento de identificación del solicitante o representante,
    - en caso de que se contemple un emplazamiento geográfico concreto, debe indicarse dirección y población y si fuera necesario coordenadas UTM (Universal Transverse Mercator),
    - nombre y apellidos del letrado y del procurador del solicitante (si procede),
    - la fecha de emisión del informe o dictamen pericial,
    - competencia y capacidades del perito o peritos, deben figurar la titulación, formación y experiencia correspondiente a la materia objeto del informe o dictamen,

    - firma del perito o peritos, si se proporciona el informe en soporte digital, este debe ir firmado digitalmente.

6. Declaración de tachas, cuando proceda el perito puede aplicar el sistema de tachas o hacer constar su imparcialidad.
7. Juramento o promesa, cuando proceda, el perito manifiesta bajo juramento o promesa decir la verdad, que actúa con veracidad y con objetividad y que conoce las sanciones penales en que puede incurrir.
8. Índice general, este tiene como misión facilitar la localización de todos y cada uno de los capítulos y apartados del informe o dictamen.
9. Cuerpo del informe o dictamen pericial, debe ser claramente comprensible por los interesados, especialmente en lo referente a sus objetivos, las investigaciones y las razones que conducen a las conclusiones.
    - Objeto, indicar la finalidad, esta debe de ser especificada por el solicitante.
    - Alcance, se debe indicar las cuestiones planteadas por el solicitante y el ámbito del mismo.
    - Antecedentes, hay describir los hechos, sucesos o asuntos que se hayan producido anteriormente.
    - Consideraciones preliminares, se deben enumerar todos los aspectos necesarios para comprender la investigación, así como, la metodología empleada.
    - Documentos de referencia, este capítulo debe recoger las normas, la buena práctica profesional y la bibliografía citada en el informe.
    - Terminología y abreviaturas, relación de definiciones técnicas, así como, el significado de las siglas utilizadas en el informe.
    - Análisis, en este capítulo se deben describir los datos de partida y bases establecidas por el solicitante, y los que se deriven de la legislación aplicable, de la investigación realizada, de las referencias, documentos, procedimientos y conservación de las mismas que puedan dar fundamento a las conclusiones del informe. En el próximo apartado se describen los contenidos mínimos de los informes periciales TIC según cada caso.
    - Conclusiones, describir de manera inequívoca la interpretación técnica y experta resumida. Si el solicitante plantea preguntas concretas, se deberán incluir tanto las preguntas como las respuestas.
    - Anexos, estos deben ser identificados de manera correlativa y paginados de forma inequívoca.

Contenido mínimo de los informes periciales TIC

A continuación se describen, las evidencias digitales mínimas que deben contener los informes o dictámenes periciales TIC según cada caso:

1. Sistemas de Información:

- Descripción del sistema de información analizado.
- Gestión de la cadena de custodia.
- Fecha y hora de intervención.
- Condiciones de funcionamiento del sistema.
- Medidas que se han tomado para salvaguardar el sistema de información.
- Procedimiento y documentación.
- Política de seguridad de la instalación donde está operando el equipo, incluyendo copias de seguridad.
- Identificación del personal con acceso al equipo, como mínimo el administrador el sistema.
- Topología de red, cortafuegos, NAT (*Network Address Translation*), VPN (*Virtual Private Network*), enlaces a internet, entre otros.
- Normativa aplicada en la instalación afectada.

2. Autenticación del correo electrónico:

- Valorar la seguridad del mecanismo de firma electrónica del correo.
- Si no va firmado, hacer análisis de la cabecera o ver si existe un tercero con copia del mensaje.
- Cotejo de las cabeceras del correo electrónico con los históricos de los servidores utilizados.
- Informe del proveedor de internet, si procediera.

3. Delitos contra la propiedad intelectual e industrial en formato digital. Identificación, manipulación o utilización de:

- componentes *hardware,*
- elementos *software,*
- documentos digitales, películas, vídeos, música y juegos,
- patentes y propiedad intelectual relacionadas con las TIC.

4. Utilización e identificación de metadatos encontrados en:

- correos electrónicos,
- fotografías y documentos gráficos,
- documentos electrónicos de texto.

5. Contenido *web*:

- captura de la pantalla en modo gráfico,
- acta testimonial del contenido,
- acceso a la página *web* en cuestión.

6. Soporte de almacenamiento digital (discos duros, *pendrives, memorias SD, etc.):*

- inventario del contenido,
- si se ha iniciado o continuado la cadena de custodia,
- si se ha realizado copia forense del componente original,
- si se ha aplicado las claves *HASH*[11] al elemento original y a la copia.

---

[11] ***HASH***. En publicación s.f. del Instituto Nacional de Tecnologías de la Información (INTECO) en su cuaderno de notas del observatorio, en su documento "Como comprobar la integridad de los ficheros" con acceso a documento en formato pdf desde el enlace: https://www.incibe.es/file/5ZOhqplBAZMCN-GUWrwDAQ detalla que:

Las funciones hash son estructuras de datos muy conocidas en matemáticas y ciencias de la computación y se encuentran ligadas muy estrechamente con la criptografía en general y la integridad de los datos en particular. Las funciones hash criptográficas convierten un mensaje de cualquier tamaño en un mensaje de una longitud constante. Lo que se obtiene al aplicar una función hash criptográfica a un mensaje (flujo de datos, o más usualmente, un archivo) se llama resumen criptográfico, huella digital o message digest. Es decir, a partir de un número indeterminado de bits, siempre se obtiene un número constante y diferente que identifica de forma unívoca a ese flujo de datos.

Los algoritmos más utilizados para calcular el hash son:

· MD5. Ante la entrada de cualquier flujo de datos, devuelve un bloque de 128 bits. En 2006 se publicó un método capaz de encontrar colisiones en unos minutos y por tanto, aunque muy usado, no se considera totalmente seguro hoy día.

· SHA256 (y sus sucesores: SHA512, por ejemplo). Ante la entrada de cualquier flujo de datos, devuelve un bloque de 256 bits. Al aumentar los bits de salida (hasta 2256 frente a 2128 del MD5), la posibilidad de colisión es menor y por tanto es más seguro. Se utiliza en los principales protocolos de cifrado: SSL, SSH, PGP o IPSec. Los métodos para encontrar colisiones, aunque existen, en SHA no tienen suficiente potencia como para poder proporcionar un ataque práctico, por tanto se considera relativamente seguro hoy día.

4 Informática forense digital

La Informática forense digital, es la disciplina, dentro de la seguridad informática, encargada de la identificación, preservación, análisis, interpretación y presentación de evidencias digitales. Nos permite detallar, validar y sustentar las hipótesis que sobre un evento se formulen.

El análisis forense informático, se podría decir que es "*la forma de aplicar los conceptos, estrategias y procedimientos de la criminalística a la tecnología digital, con el fin de apoyar a la justicia en su lucha contra la delincuencia y el crimen, o como recurso especializado en esclarecimiento de incidentes de seguridad informática*" (Lopez Delgado, 2007).

En concreto, análisis forense digital es la aplicación de la tecnología informática a una cuestión de derecho en la que las pruebas –evidencias digitales - incluyen, información digital, creada por los individuos y la generada por los propios dispositivos –*logs*, *caché*, temporales, etc.- como resultado de la interacción con el individuo u otros elementos.

Al hilo del párrafo anterior, es fundamental tener presente el principio de intercambio de Locard –base de la ciencia forense- que dice: "siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto". Por cierto, Locard también se cumple cuando se manipulan las evidencias. Por ello, es importante ser meticuloso y cuidadoso en todo el proceso de análisis para que las evidencias no se alteren o contaminen.

El proceso de análisis forense ante incidentes de seguridad, básicamente y de forma general, intenta dar respuesta a cuestiones como:

- ✓ ¿qué investigar? … tipo de delito. pruebas a buscar …
- ✓ ¿dónde? … sistemas, redes, ordenador, móvil, etc
- ✓ ¿cuándo se cometió el delito? … fecha y hora local / UTC
- ✓ ¿por qué? … el fin buscado
- ✓ ¿Quién o quiénes son los autores? tarea difícil en el mundo virtual
- ✓ ¿Cómo se llevó a cabo? … importante aspectos de resiliencia.

Fases del análisis forense digital

Dentro de procedimiento del análisis forense digital, se pueden destacar las siguientes fases[12]:

- ✓ Identificación del incidente.
- ✓ Recopilación de evidencias.
- ✓ Preservación de la evidencia.
- ✓ Análisis de la evidencia.
- ✓ Documentación y presentación de los resultados.

Estas fases no son estrictamente secuenciales. Es imprescindible documentar desde el principio todo lo que se va haciendo.

En la figura 4 se muestra la línea de tiempo del proceso de análisis y las acciones más relevantes a desarrollar cada fase:

1. Identificación del incidente.

   Se debe informar al perito forense informático, lo más detalladamente posible, de los hechos, efectos producidos, escena del delito o entorno, quién ha informado del incidente a las autoridades o responsables, como se ha detectado, etc.

2. Recopilación de evidencias.

   Se debe garantizar la recopilación de todas las evidencias, no perder ninguna es lo ideal. Acciones como: no apagar los equipos, identificar los dispositivos a recopilar, documentar el proceso, precintar todos los elementos objeto de análisis para su transporte, etc.

3. Preservación de la evidencia.

   Es la etapa en la que se adquieren las evidencias. Esta fase es muy importante. Cualquier error en la toma de evidencias podría echar por tierra la investigación o que las pruebas no sean admisibles ante un tribunal. Importante iniciar proceso de cadena de custodia.

4. Análisis

   A la hora de realizar el análisis de la información recopilada hay que tener presente el tipo de incidente al que se dará respuesta. De esta forma se agiliza el proceso al fijar las evidencias objeto de un análisis en profundidad. Aunque nunca se debe caer en el error de descartar lo que nos pueda parecer obvio, hay que ser totalmente objetivos en todo el proceso.

5. Documentación y presentación.

   La documentación debe ser metódica, detallada y patente desde el principio del análisis. El archivo documental de la investigación debe contener, al menos: videos o fotografías del escenario y de las pruebas tecnológicas, control en la cadena de custodia de las pruebas y una bitácora con fechas y horas de las acciones realizadas sobre las evidencias.

   La presentación del informe o dictamen tiene que ser de fácil comprensión, donde se detalle objetivamente las conclusiones obtenidas y se explique claramente el proceso de obtención de las evidencias. No realizar juicios de valor ni afirmaciones que no se puedan demostrar.

Diagrama de fases del análisis forense digital

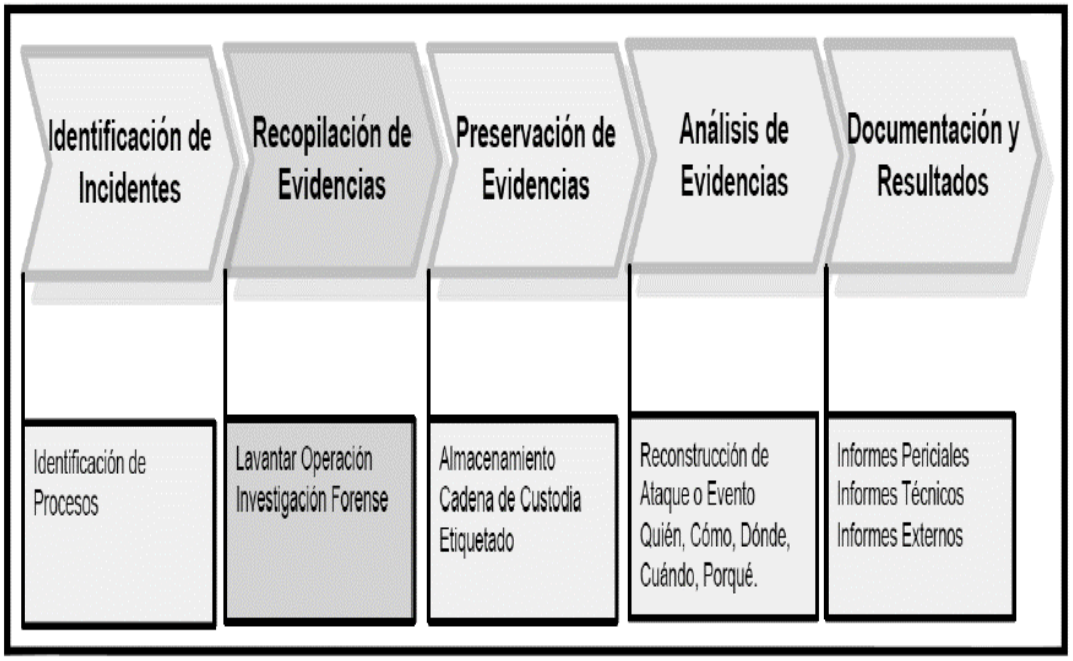


Figura 4. Fases del Análisis Forense Digital.

[Fuente] López Delgado, Análisis Forense digital, 2007

---

[12] **Análisis forense digital.** López Delgado, 2ª Edición (junio 2007). El presente documento se distribuye bajo la licencia conocida como "GNU Free Documentation License" en: http://www.gnu.org/copyleft/fdl.html

La evidencia digital. La reina del proceso

Según *Guidelines for the Management of IT Evidence* [13], la evidencia digital es: "*cualquier información digital, que sujeta a la intervención humana u otra semejante, ha sido extraída de un medio informático*".

En términos generales, evidencia digital, se puede utilizar para describir "*cualquier registro generado por o almacenado en un sistema informático o dispositivo digital que pueda ser utilizado como prueba en un proceso legal*".

Las evidencias deben ser:

- ✓ **Auténticas**

  Para ello se debe poder demostrar que no han sufrido ningún cambio. Mediante obtención de *hashes* se puede asegurar su integridad. Se verá más adelante en que consiste esta técnica.

- ✓ **Creíbles**

  Se puedan entender y comprender fácilmente.

- ✓ **Completas**

  Desde el punto de vista objetivo y técnico de la prueba a la que representa. Dejando de lado perjuicios o valoraciones personales.

- ✓ **Confiables**

  Las técnicas para su obtención no pueden generar dudas sobre su autenticidad y veracidad.

- ✓ **Admisibles**

  Desde el punto de vista legal.

[13] ***HB:171 (2003).*** *Guidelines for the Management of IT Evidence.* Standards Australia International. Enlace http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN016411.pdf

Clasificación

- ✓ Evidencia física

  Se refiere al componente tecnológico como los discos duros, *pendrives*, *tablets*, *smartphones*, *routers*, etc.

- ✓ Evidencia digital

  Cuando se hace referencia a la información almacenada en los dispositivos electrónicos recopilados o a la información obtenida por otros medios formales y válidos –*sniffer*, etc.-. Como por ejemplo: ficheros de discos duros, proceso en ejecución, temporales, *caché*, registros del sistema, *logs* …

El reconocimiento de la Evidencia Digital

En el seno de una investigación criminal o comisión de un ciberdelito, es importante tener claros los conceptos y utilizar los términos más adecuados que determinen el rol que tiene el componente o sistema informático en el procedimiento. Esto nos determinará el tipo de análisis o investigación, la obtención de indicios y más adelante las pruebas necesarias donde se sustente nuestro caso.

Por ejemplo, el procedimiento por un delito de estafa –*pshising*- es totalmente distinto al de una investigación de un componente tecnológico –móvil- en un delito de tráfico de drogas, por tanto el rol que cumple el componente tecnológico –huella digital- determinará como debe ser usada la evidencia y donde se ubique.

Con este propósito se categorizan las pruebas para distinguir entre el elemento *hardware,* evidencia electrónica, y la información digital contenida en éste, evidencia digital. Esta distinción facilita el diseño de las metodologías y procedimientos adecuados en el manejo y estudio de cada tipo de evidencia consiguiendo un paralelismo entre el escenario físico y el entorno digital.

Se debe prestar especial atención a los procedimientos de recopilación y almacenamiento de las evidencias en la escena del delito, y asegurar la cadena de custodia de las mismas. Aplicar métodos y pautas para que estas no se alteren a lo largo del proceso y que sean reproducibles por terceras partes en cualquier momento. Y seguir en todo el proceso las fases de análisis forense digital basadas un método normalizado.

Para lograrlo, los peritos informáticos forenses basan sus investigaciones periciales y análisis forenses digitales, en normas y guías nacionales e internacionales publicadas al respecto, como RFC (*Request for Comments*), UNE (Una Norma Española) e ISO *(International Organization for Standardization*), entre otras.

Metodologías en análisis forense digital. Normas y guías actuales

Las evidencias digitales están adquiriendo formas cada vez más inesperadas en nuevos dispositivos o componentes tecnológicos que desafían los procedimientos y metodologías actuales. En este sentido, los peritos informáticos forenses tratan de entender y asimilar el conocimiento de la tecnología y su forma de operar, para dar cuenta de la evidencia en ella, la complejidad que exhibe el mundo digital donde se encuentra, supera a las investigaciones efectuadas sobre realidades estáticas y conocidas. Para ello, los comités e instituciones normalizadores están haciendo grandes esfuerzos en actualizar o publicar nuevas normas y guías que contemplen estos avances.

En la actualidad, existen diferentes guías, metodologías y normas a la hora de realizar un análisis forense informático, la mayoría de ellas con aspectos comunes.

En este apartado, se van a estudiar las recientes normas internacionales ISO, españolas UNE y las referencias documentales RFC, en tratamiento de evidencias, metodologías para el análisis forense digital y elaboración de informes o dictámenes periciales:

- ✓ RFC 3227 "Directrices para la recopilación de evidencias y su almacenamiento"
- ✓ ISO/IEC 27037:2012 "Guía para la identificación, recolección, adquisición y preservación de evidencias digitales"
- ✓ UNE 71505-2:2013 "Buenas prácticas en la gestión de evidencias electrónicas"
- ✓ UNE 71506:2013 "Metodología para el análisis forense de evidencias electrónicas"
- ✓ ISO/IEC 27041:2015 "*Guidance on assuring suitability and adequacy of incident investigative method*"
- ✓ ISO/IEC 27042:2015 "*Guidelines for the analysis and interpretation of digital evidence*"
- ✓ ISO/IEC 27043:2015 "*Incident investigation principles and processes*"
- ✓ UNE 197010:2015 "Criterios generales para la elaboración de informes y dictámenes periciales sobre Tecnologías de la Información y las Comunicaciones"
- ✓ ISO/IEC WD 27044 "Security Information and Event Management (SIEM)"

RFC 3227[14] - Directrices para la recopilación de evidencias y su almacenamiento

Fue elaborada y escrita en febrero de 2002 por Dominique Brezinski y Tom Killalea, ingenieros del Network Working Group.

Todavía sirve de estándar a instituciones nacionales para la recopilación de información en incidentes de seguridad.

El documento recoge los principios durante la recolección de evidencias, el procedimiento de recolección, el procedimiento de almacenamiento y herramientas necesarias.

ISO/IEC 27037[15] - Guía para la identificación, recolección, adquisición y preservación de evidencias digitales

Publicada el 15 de Octubre de 2012.

Es una guía que proporciona directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales potenciales localizadas en teléfonos móviles, tarjetas de memoria, dispositivos electrónicos personales, sistemas de navegación móvil, cámaras digitales y de video, redes TCP/IP, entre otros dispositivos, para que puedan ser utilizadas con valor probatorio y en el intercambio entre las diferentes jurisdicciones.

Esta norma proporciona orientación para los siguientes dispositivos y circunstancias:

1. medios de almacenamiento digital, como discos duros, discos ópticos, cintas, etc, que se suelen emplear en ordenadores y sistemas informáticos.
2. teléfonos móviles, *PDAs*, dispositivos personales electrónicos, tarjetas de memoria
3. sistemas de navegación móviles (*GPS*)
4. cámaras digitales y de vídeo
5. equipos con conexión de red
6. redes TCP/IP y otros protocolos digitales
7. y todos aquellos dispositivos con funciones similares a los anteriores

A diferencia de la RFC 3227, la norma ISO/IEC 27037 hace referencia a componentes tecnológicos más avanzados y tiene esta característica en cuenta en el desarrollo de la misma. Por ejemplo, para el análisis de teléfonos móviles es más adecuada esta norma.

UNE 71505-2[16] - Buenas prácticas en la gestión de evidencias electrónicas

Norma española publicada en julio de 2013.

Esta norma establece los controles y procesos para la gestión de seguridad de las evidencias electrónicas. Se aplica a entornos propios de las organizaciones con independencia de su actividad o tamaño. Puede ser aplicada por empresas que desempeñen servicios de los que se describen en relación con el ciclo de vida y/o controles descritos en la norma.

Determina los datos que debe incluirla evidencia electrónica, además de su propio contenido, con el fin de documentar una determinada operación.

- su estructura –formato y relaciones entre elementos que la integran- debería permaneces intacta.
- la fecha que fue creada, recibida y manipulada, así como, los participantes a lo largo del proceso.
- en caso de existir, identificar el vínculo entre evidencias.

En su apartado 4.2 trata sobre la confiabilidad de los sistemas, procesos y procedimientos, para minimizar la posibilidad de que se cuestione con éxito la veracidad y la exactitud de lo custodiado, gestionado y/o almacenado.

- disponibilidad y completitud
- autenticación e integridad
- cumplimiento y gestión

En su apartado 4.3 se describen los beneficios de la gestión de las evidencias y la importancia, como recurso valioso en una organización, de las evidencias electrónicas.

El Sistema de Gestión de Evidencias (SGEE) se trata en el apartado 5. Donde se describe la gestión del ciclo de vida de la evidencia electrónica, incluso antes de su adquisición: generación, almacenamiento, transmisión, recuperación, comunicación y preservación.

Esta norma adopta un enfoque por procesos para establecer, implantar, poner en funcionamiento, controlar, revisar, mantener y mejorar un SGEE.

Describe como la política de la organización debe reflejar la implicación del marco normativo y regulatorio en sus procesos de negocio.

En su anexo A, se explica en código de buenas prácticas específicas para el SGEE.

En su anexo B, se detalla la matriz utilizada para asignar nuevas funciones a los responsables de la implantación de la norma (funciones x responsable).

UNE 71506[17] -Metodología para el análisis forense de las evidencias electrónicas

Norma española publicada en julio de 2013.

La presente norma establece una metodología para la preservación, adquisición, documentación y presentación de las evidencias electrónicas. Esta norma es de aplicación a cualquier organización, así como profesional competente en este ámbito, como por ejemplo el perito informático forense. Va dirigida especialmente a los equipos de respuesta a incidentes y seguridad, así como al personal técnico de laboratorios o entornos de análisis forense de evidencias digitales.

Define el proceso de análisis forense para complementar el SGEE de la norma UNE 71505 descrita en el punto anterior.

El capítulo 5 está dedicado a la preservación de las evidencias originales garantizando su inalterabilidad y validez legal, lo que permite la reproducibilidad de estudios sobre ellas. Almacenamiento en lugares y soportes estancos y aislados de interferencias o posibles agentes externos.

El siguiente capítulo trata la adquisición de las evidencias, distinguiendo el trato a seguir si el sistema está apagado o encendido. También se valora que el análisis forense puede ser sobre datos de origen estático, datos en tránsito de sistemas en funcionamiento, datos volátiles, sistemas embebidos, datos de móviles y redes, así como grandes sistemas almacenamiento con información repartida en varios repositorios.

El capítulo 7 se refiere a la documentación, garantizar la cadena de custodia y la trazabilidad de las evidencias, a través de la implantación de un sistema de gestión documental que registre las actuaciones sobre dichas evidencias, bien sean originales o clonadas.

En su capítulo 8 se dedica al análisis de las evidencias digitales objeto de investigación. Y por último, su capítulo 9 trata la presentación de los resultados obtenidos a la autoridad judicial o entidad que solicita el informe pericial.

En sus anexos tenemos el modelo de informe pericial, las competencias para el análisis forense de las evidencias electrónicas y equipamiento para el análisis forense de evidencias electrónicas.

Esta norma junto con la UNE 71505 son una metodología muy utilizada por profesionales y organismos nacionales en la actualidad, así como las fuerzas y cuerpos de seguridad del estado.

ISO/IEC 27041[18] - Guidance on assuring suitability and adequacy of incident investigative method

Norma internacional (en inglés) publicada en junio de 2015.

Ofrece orientación sobre los mecanismos para garantizar que los métodos y procesos utilizados en la investigación de incidentes de seguridad informática son los adecuados.

Incluye la consideración de cómo los proveedores y pruebas de terceros se pueden utilizar para ayudar a este proceso de garantía.

Sus objetivos son:

- proporcionar pautas sobre la captura y el posterior análisis de los requisitos tanto funcionales como no funcionales relacionados con la seguridad en la investigación de incidentes,
- utilizar la validación como medio de garantías de la idoneidad de los procesos involucrados en la investigación,
- a partir de un ejercicio de validación determinar nuevos niveles de validación que se requieran y las pruebas requeridas
- determinar pruebas externas y la documentación a incorporar en el proceso de validación

Esta norma puede resultar útil para garantizar la validez de las evidencias digitales ante un proceso judicial.

ISO/IEC 27042[19] - Guidelines for the analysis and interpretation of digital evidence

Norma internacional (en inglés) publicada en junio de 2015.

Proporciona una guía para el análisis e interpretación de la evidencia digital. Provee información sobre como adelantar un análisis e interpretación de la evidencia digital potencial en un incidente con el objeto de identificar y evaluar aquella que se puede utilizar para ayudar a su comprensión.

Ofrece un marco común para el análisis e interpretación de la gestión de incidentes de seguridad, que pueda utilizarse para implementar nuevos métodos.

También introduce una serie de definiciones relevantes para la práctica del análisis forense digital.

Trata los modelos analíticos que pueden ser usados por los peritos informáticos forenses en sistemas estáticos o activos y las consideraciones, a tener en cuenta en cada caso, en especial atención a incidentes en sistemas vivos o activos como: dispositivos móviles, sistemas cifrados, redes, etc.

Se definen dos formas de adelantar el análisis en vivo:

- En sistemas que no pueden ser copiados o no se puede crear una imagen

  Existe el riesgo de perder la evidencia digital cuando se está copiando. Importante tener cuidado para minimizar el riego de daño de la evidencia y asegurar que se tiene un registro completo de los procesos.

- En sistemas que si se puede copiar o realizar la imagen

  Examinar el sistema interactuando u observándolo en su operación. Ser cuidadoso para emular el hardware o software del entorno original, usando máquinas virtuales verificadas, copias del hardware original con el fin de permitir un análisis lo más cercano posible al real.

Por otro lado, se detalla el contenido de los resultados del análisis en el informe pericial y sus consideraciones legales.

Finalmente, recoge las competencias de los peritos forenses: formación, aprendizaje, habilidades, objetividad y ética profesional.

ISO/IEC 27043[20] – Incident investigation principles and processes

Norma internacional (en inglés) publicada en marzo de 2015.

Proporciona una guía de principios para los procesos de investigación de incidentes que involucran evidencias digitales. Incluye los procesos de preparación previa al incidente a través del cierre de la investigación, así como advertencias al respecto.

Las directrices describen los procesos y principios aplicables a los distintos tipos de investigaciones delictivas, como por ejemplo, violaciones de seguridad, fallos del sistema, accesos no autorizados, entre muchos otros.

No ofrece detalles particulares para cada tipo de investigación pero si una visión general de los principios y procesos de investigación aplicables.

ISO/IEC WD 27044[21] - Security Information and Event Management (SIEM)

Norma internacional todavía en desarrollo.

Describe un sistema para la gestión de eventos y de la seguridad de la información (SIEM).

Con esta norma se pretende dar solución a los actuales problemas que existe a la hora de recoger evidencias en sistemas activos, complejos o con falta de recursos.

Estas herramientas permiten monitorizar en tiempo real los eventos, proporciona la visibilidad de toda la estructura de información, captura y análisis de redes y dispositivos móviles, control de aplicaciones y eventos que generan. Análisis de sistemas objeto de ataque, antes, durante y después del mismo. Administrador de riegos de la organización o entorno. Gestión de *logs* de los elementos y dispositivos del sistema global. Capacidad de resiliencia en las organizaciones objeto de ataque.

En resumen, proporciona a las organizaciones una plataforma de inteligencia de la seguridad.

UNE 197010[22] - Criterios generales para la elaboración de informes y dictámenes periciales sobre Tecnologías de la Información y las Comunicaciones (TIC)

Norma española publicada en marzo de 2011.

La norma enumera los apartados mínimos necesarios a incluir en la elaboración de un informe, sin ser esta una enumeración excluyente, limitativa ni exhaustiva. También se describen los requisitos formales que deben tener los informes, sin especificar los métodos y procesos de elaboración.

Es la norma más empleada en España en el ámbito del peritaje y la recomendada por la mayoría de colegios, expertos y organizaciones profesionales. El empleo de esta norma se considera admisible ante un procedimiento judicial.

---

[14] **RFC 3227.** http://www.ietf.org/rfc/rfc3227.txt

[15] **ISO/IEC 27037.** www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44381

[16] **UNE 71505-2** http://www.aenor.es/aenor/normas/buscadornormas/resultadobuscnormas.asp#.Vt3DfvnhBMw

[17] **UNE 71506** http://www.aenor.es/aenor/normas/buscadornormas/resultadobuscnormas.asp#.Vt3DvPnhBMw

[18] **ISO/IEC 27041**. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44405

[19] **ISO/IEC 27042** http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44406

[20] **ISO/IEC 27043** http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44407

[21] **ISO/IEC WD 27044** http://www.iso.org/iso/catalogue_detail.htm?csnumber=62287

[22] **UNE 19710** http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0055393&PDF=Si#.VtSiwPnhBMw

5 Marco legal en el peritaje informático

En este capítulo, principalmente, se trata la legislación española de aplicación a peritos informáticos, informes y dictámenes periciales, y al análisis forense digital.

El objetivo es proporcionar al lector una recopilación sistemática y actualizada del actual marco legal en vigor, indicando a que texto, disposición o artículo acudir si fuera necesario.

Es importante señalar que la comprensión y entendimiento de los textos legales para inexpertos juristas son ciertamente complicados, una imprecisa o ambigua interpretación de los mismos puede acarrear graves problemas legales. Por esto, es recomendable remitirse al texto completo de la ley publicado en los distintos boletines oficiales[23].

Antes de entrar en materia es importante analizar que dice la constitución Española sobre la informática y su uso. En este contexto, la Constitución Española en su artículo dieciocho, punto cuatro, textualmente dispone que "*la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*". Hace cuarenta años, cuando la informática apenas se conocía e internet no existía, nuestros legisladores ya eran conscientes del peligro que la informática podía suponer para la sociedad. Lo grave es que a día de hoy, cuarenta años después, la sociedad española sigue en algunos aspectos indefensa. Conscientes de esta situación los gobiernos nacionales, europeos e internacionales están aplicando medidas urgentes para adaptar la legislación vigente a las nuevas exigencias de la actual Cibersociedad, en la que la ciberdelincuencia y la ciberseguridad van por delante de una "obsoleta" y "lenta" jurisprudencia.

Si profundizamos un poco, la legislación española todavía se muestra ambigua, por ejemplo, al referirse a un ordenador como un aparato puramente electrónico, ya que los programas que un ordenador se ejecutan, a diferencia de un componente puramente electrónico, realizan tareas muy complejas que precisan de la interacción de un individuo. Por lo que el ordenador si puede ser utilizado para cometer un delito, por tanto, el ordenador debería considerarse como una prueba informática y no electrónica.

[23] **BOE** Boletín Oficial del estado. Enlace buscador publicaciones oficiales: http://www.boe.es/buscar
EUR-Lex Acceso al Derecho de la Unión Europea: http://eur-lex.europa.eu/homepage.html?locale=es
Unión Europea – legislación http://europa.eu/eu-law/index_es.htm

Igualmente, cuando se refiere al medio telemático, se produce confusión ya que telemático no es más que la fusión de la palabra "telecomunicaciones" e "informática", pero la infraestructura de red, en sí misma, no puede utilizarse para cometer delitos, si bien los ordenadores o dispositivos conectados a estas redes con el uso del *software* si son capaces, por lo que estaríamos hablando de medios informáticos y no medios telemáticos. De hecho cuando nos referimos a perito, no lo llamamos perito electrónico ni telemático, sino perito informático.

Bien es cierto, que con las nuevas reformas del marco legal y las adaptaciones a las Directivas Europeas y Convenios Internacionales, donde, ya se habla de tecnología digital, ciberdelitos, dispositivos móviles, redes sociales, internet de las cosas, la 'nube', servicios digitales, y demás términos de esta nueva sociedad digital, se han corregido algunas de estas lagunas y ambigüedades, se han mejorado y acelerado los procedimientos judiciales, en definitiva, se ha fortalecido la justicia española.

Se prestan especial atención a las modificaciones de relevancia en Delitos Informáticos tras la reforma del Código Penal por la Ley Orgánica 1/2015, y la modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica por la Ley Orgánica 13/2015, de 5 de octubre.

Figura 5. Delitos informáticos

[Fuente] Incibe. Guía de toma de evidencias en entornos Windows (pág. 13)

Derecho informático

A continuación se detallan las leyes, decretos y órdenes relacionadas con la materia objeto del trabajo, destacar la incorporación de las últimas reformas legislativas del pasado año 2015.

Es necesario conocer el marco legal de esta profesión, y en especial aquellas que regulan las sanciones que le pueden ser imputadas a un perito informático judicial.

Los textos de las leyes subrayadas se consideran, en el contexto informático, más importantes y relevantes, por lo que se les debe prestar especial atención.

- Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.
- Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 28 de noviembre, del Código Penal, desde el punto de vista del derecho informático y Delitos Informáticos.
- Ley 8/2011, de 28 de abril, por la se establecen Medidas de Protección de las Infraestructuras Críticas.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Ley 23/2006, de 7 de julio, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Ley 32/2003, de 3 de noviembre, ley General de Telecomunicaciones.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Ley Orgánica 19/1994, de 23 de diciembre, de protección a testigos y peritos en causas criminales.
- Ley Orgánica 1/1992, de 21 de febrero, de Protección de la Seguridad Ciudadana.
- Ley Orgánica 6/1985 de 1 de julio, del Poder Judicial.
- Constitución Española 1978.
- Código Civil español RD de 24 de Julio 1889
- Real Decreto ley 12/2012, de 30 de marzo, por el que se transponen directivas en materia de mercados interiores de electricidad y gas y en materia de comunicaciones electrónicas.

- Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de Protección de las Infraestructuras Críticas.
- Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el Texto Refundido de la Ley de Contratos del Sector Público.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Pública.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Orden PRE/2740/2007, de 19 de Septiembre, por la que se regula el Reglamento de Evaluación y Certificación de Seguridad de las Tecnologías de la Información
- Protocolo Adicional, 28 Enero de 2003, al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos.
- BOE 14221/ 2010, de 17 Septiembre, Instrumento de Ratificación del Convenio de la Ciberdelincuencia, redactado en Budapest el 23 de noviembre de 2001.
- Real Decreto Legislativo 1/1996, de 2 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.
- Real Decreto 980/2013, de 13 de diciembre, por el que se desarrollan determinados aspectos de la Ley 6 de julio de Mediación en asuntos civiles y mercantiles.
- Ley Orgánica 5/2011, de 20 de mayo, complementaria a la Ley 11/2011, de 20 de mayo, de reforma de la Ley 60/2003, de 23 de diciembre, de Arbitraje y de regulación del arbitraje institucional en la Administración General del Estado para la modificación de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.
- Ley 60/2003, de 23 de diciembre, de Arbitraje.
- Ley 17/2009, de 23 de noviembre, sobre el libre acceso a las actividades de servicio y su ejercicio.
- Ley 25/2008, de 22 de diciembre, de modificación de diversas leyes para su adaptación a la ley sobre libre acceso a las actividades de servicios y su ejercicio.
- Ley 2/2007, de 18 de marzo, de Sociedades Profesionales.
- Ley 2/1994, de 13 de febrero, sobre Colegios Profesionales.
- Ley Orgánica 1/2002, de 22 de marzo, reguladora del Derecho de Asociación.
- Orden JUS/419/2009, de 17 de diciembre, relativa al pago de los peritajes judiciales a cargo del Departamento de Justicia de la Generalitat.

- Directiva 2006/24/UE "*Obligación de los proveedores de servicios de comunicaciones de acceso público en relación con la conservación de determinados datos generados o tratados por los mismos, para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves.*"

- Directiva 2013/40/UE "*Normas mínimas a la definición de las infracciones y a las sanciones aplicables en el ámbito de los ataques contra los sistemas de información."*

Legislación nacional aplicada al perito informático

La legislación española de aplicación al perito informático es:

- La ley concursal.
- La ley de enjuiciamiento civil.
- La ley de enjuiciamiento criminal.
- El código de comercio y código civil.

En la tabla 6 se recogen los artículos de la Ley de Enjuiciamiento Civil y Criminal relacionados con el análisis forense digital y peritajes informáticos, y por supuesto, con la figura del perito informático judicial.

Ley de enjuiciamiento civil		Ley de enjuiciamiento criminal	
Texto	**Artículos**	**Texto**	**Artículos**
La abstención	99, 100, 105, 639	Apercibimiento de procesarle por denegación de auxilio por no comparecencia	175.II
La aceptación	342	La celebración del acto de reconocimiento	476, 477, 479, 480, 182.II y III
Comunicaciones	159	Citación al juicio oral	660, 661.1
Las condiciones	340	Discordia y nombramiento de perito tercero	484
Actuación en el juicio	338.2, 346, 347	En diligencia de inspección ocular	328
Auxilio judicial	169	Honorarios, derecho percibirlos y costas	121, 242, 241.3
Designación judicial	338.2, 339, 347.2 349.3	Informe, contenido y aclaraciones	478, 482
" en audiencia previa	427	Causa de recusación del personal	54.4
" por acuerdo de partes	339.4	Juramento	474
" por los litigantes	336 a 338	Listas, copias y lectura juicio oral	675, 701.III
" Procedimiento	341, 342	Nombramiento	460, 461
Falso testimonio/revisión	510	" por las partes	471
Interrupción de la vista	193	Notificación de nombramiento de peritos inf	466
Juramento o promesa	335.2, 340, 342	Numero de peritos	459
Minuta tasación de costas	241 a 246	Único en procedimiento abreviado	778.1, 788.2
Multa	292	Obligatoriedad del cargo	462
Nombramiento	342	Responsabilidad	463
Obligación comparecencia	292	Prohibición de emitir informe. Supuestos	464
Provisión de fondos	342	Reconocimiento del cuerpo del delito	336
Oposición por pluspetición	558	Reconocimiento de estimar el valor de cosa	365
Recusación	343, 638	Recusación en el juicio oral	662, 663, 723
Suspensión de vista	182, 292	" en el sumario	467 a 470
Tacha	124.2, 343, 344	Sanciones por incomparecencia	661.II y III y 996.II
Testigo-perito	370, 380.2	Señalamiento del objeto del informe	475

Tabla 6. Artículos de la LECriminal y LECivil en materia informática

El delito informático en la reforma del Código Penal

El día 1 de julio de 2015 entró en vigor la Ley Orgánica 1/2015 por la que se modifica la Ley Orgánica 10/1995 del Código Penal. Lo más destacado de esta ley es sin duda la eliminación de la mayoría de faltas y la modificación de aspectos relativos al ámbito de las nuevas tecnologías, delitos informáticos, internet y redes sociales.

Si bien se echa en falta la inclusión de la suplantación de identidad, que tanto afecta a las redes sociales, se ha recogido algunas otras acciones que era necesario adecuarlas en el Código Penal.

Algunas de estas reformas incluidas en la **Ley Orgánica 1/2015** son:

Grooming [24]

En su artículo 183 ter se cita textualmente:

El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño. El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor, será castigado con una pena de prisión de seis meses a dos años.

Delitos contra la propiedad intelectual y las webs de enlaces

En su artículo 270.2 se cita textualmente:

La misma pena se impondrá a quien, en la prestación de servicios de la sociedad de la información, con ánimo de obtener un beneficio económico directo o indirecto, y en perjuicio de tercero, facilite de modo activo y no neutral y sin limitarse a un tratamiento meramente técnico, el acceso o la localización en internet de obras o prestaciones objeto de propiedad intelectual sin la autorización de los titulares de los correspondientes derechos o de sus cesionarios, en particular ofreciendo listados ordenados y clasificados de enlaces a las obras y contenidos referidos anteriormente, aunque dichos enlaces hubieran sido facilitados inicialmente por los destinatarios de sus servicios.

Delitos de odio en las redes sociales

En su artículo 510.3 se cita textualmente:

Las penas previstas en los apartados anteriores se impondrán en su mitad superior cuando los hechos se hubieran llevado a cabo a través de un medio de comunicación social, por medio de internet o mediante el uso de tecnologías de la información, de modo que, aquel se hiciera accesible a un elevado número de personas.

Redes sociales y difusión de imágenes intimas

En su artículo 197.7 se cita textualmente:

Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona. La pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa.

---

[24] **Grooming (s.f.).** Según Wikipedia es: "*Una serie de conductas y acciones deliberadamente emprendidas por un adulto con el objetivo de ganarse la amistad de un menor de edad, creando una conexión emocional con el mismo, con el fin de disminuir las inhibiciones del niño y poder abusar sexualmente de él. En algunos casos, se puede buscar la introducción del menor al mundo de la prostitución infantil o la producción de material pornográfico*." [En línea] https://es.wikipedia.org/wiki/Grooming

Black Hacking, cracking y demás técnicas de acceso no consentido

En su artículo 197 bis se cita textualmente:

El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años. El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses. Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis: un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

La nueva ley en la investigación tecnológica

Con el fin de adecuar el marco legal a las nuevas formas de delincuencia y mejorar la jurisprudencia normativa relativa a la investigación tecnológica, el pasado 5 de octubre de 2015 se aprobó la modificación de la Ley de Enjuiciamiento Criminal.

La Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

De su preámbulo V se extrae parte del texto referente a las medidas en investigación tecnológica:

La Ley de Enjuiciamiento Criminal no ha podido sustraerse al paso del tiempo. ***Renovadas formas de delincuencia ligadas al uso de las nuevas tecnologías han puesto de manifiesto la insuficiencia de un cuadro normativo*** *concebido para tiempos bien distintos. Los flujos de información generados por los sistemas de comunicación telemática advierten de las posibilidades que se hallan al alcance del delincuente, pero también proporcionan poderosas herramientas de investigación a los poderes públicos. (....)*

Toda medida deberá responder al principio de ***especialidad****. Ello exige que la* ***actuación de que se trate tenga por objeto el esclarecimiento de un hecho punible concreto,*** *prohibiéndose pues las medidas de investigación tecnológica de naturaleza prospectiva, (....)*

*Las **medidas de investigación tecnológica** deben además satisfacer los principios de idoneidad, excepcionalidad, necesidad y proporcionalidad, cuya concurrencia debe encontrarse suficientemente justificada en la resolución judicial habilitadora, donde el juez determinará la naturaleza y extensión de la medida en relación con la investigación concreta y con los resultados esperados.*

*La reforma ha considerado adecuado no abandonar los aspectos formales de la solicitud y del contenido de la resolución judicial habilitante. La **práctica forense** no es ajena a casos de solicitudes policiales y de ulteriores resoluciones judiciales que adolecen de un laconismo argumental susceptible de vulnerar el deber constitucional de motivación. A evitar ese efecto se orienta la **minuciosa regulación del contenido de esa solicitud, así como de la resolución judicial** que, en su caso, habilite la medida de injerencia. (...)*

*En relación con la **interceptación de las comunicaciones telefónicas** y telemáticas, en la determinación del ámbito material de aplicación, se sigue el mismo criterio ya evidenciado más arriba por remisión, aunque **se suman a la lista de delitos los cometidos por medio de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación.***

*En la nueva regulación se confiere sustantividad propia a otras formas de comunicación telemática que han carecido de tratamiento normativo en la ley procesal. Las dificultades asociadas a ese vacío se han visto multiplicadas en la práctica por una interpretación jurisprudencial de la legislación llamada a reglar la **obligación de las operadoras de conservar los datos** generados por las comunicaciones electrónicas, que ha degradado los muy extendidos instrumentos de comunicación telemática –por ejemplo, los mensajes de SMS o el correo electrónico– a la condición de aspectos accesorios, de obligado sacrificio siempre que se adopte una decisión jurisdiccional de intervención telefónica. Frente a esta concepción, el nuevo texto **autoriza la intervención y registro de las comunicaciones de cualquier clase que se realicen a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual**. (...)*

*Con el fin de **asegurar la autenticidad e integridad de los soportes** puestos a disposición del juez, se impone la utilización de un sistema de sellado o firma electrónica que garantice la información volcada desde el sistema central. (...)*

*En la investigación de algunos hechos delictivos, la incorporación al proceso de los datos electrónicos de tráfico o asociados puede resultar de una importancia decisiva. La reforma acoge el criterio fijado por la Ley 25/2007, de 18 de octubre, de **conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones**, e impone la exigencia de autorización judicial para su cesión a los agentes facultados, siempre que se trate de datos vinculados a procesos de comunicación. (...)*

*Se da un tratamiento jurídico individualizado al **acceso por agentes de policía al IMSI, IMEI, dirección IP** y otros elementos de identificación de una determinada tarjeta o terminal, en consonancia con una jurisprudencia del Tribunal Supremo ya consolidada sobre esta materia. (...)*

La experiencia demuestra que, en la investigación de determinados delitos, la ***captación y grabación de comunicaciones orales abiertas mediante el empleo de dispositivos electrónicos*** *puede resultar indispensable. (…) La primera, la exigencia de que sea el juez de instrucción el que legitime el acto de injerencia; la segunda, la* ***necesidad de que los principios rectores de especialidad, excepcionalidad, idoneidad, necesidad y proporcionalidad actúen como elementos de justificación de la medida****. Esta medida solo podrá acordarse para encuentros concretos que vaya a mantener el investigado, debiéndose identificar con precisión el lugar o dependencias sometidos a vigilancia. Por tanto,* ***no caben autorizaciones de captación y grabación de conversaciones orales de carácter general o indiscriminadas****, y, en consecuencia, el* ***dispositivo de escucha y, en su caso, las cámaras a él asociadas, deberán desactivarse tan pronto finalice la conversación cuya captación fue permitida****, como se desprende del artículo 588 quater c.*

La reforma aborda también la ***regulación de la utilización de dispositivos técnicos de seguimiento y localización****. (…)*

se ***habilita la grabación de la imagen en espacio público*** *sin necesidad de autorización judicial,* ***en la medida en que no se produce afectación a ninguno de los derechos fundamentales del artículo 18 de nuestro texto constitucional****. (…)*

Se trata del ***registro de dispositivos informáticos de almacenamiento masivo y el registro remoto de equipos informáticos****. Respecto del primero de ellos, la reforma descarta cualquier duda acerca de que esos* ***instrumentos de comunicación y, en su caso, almacenamiento de información son algo más que simples piezas de convicción****. De ahí la exigente regulación respecto del acceso a su contenido. Por lo que afecta al* ***registro remoto –diligencia ya presente en buena parte de las legislaciones europeas****–, el intenso grado de injerencia que implica su adopción justifica que incluso se refuerce el ámbito objetivo de la medida, para lo que se han* ***acotado con un listado numerus clausus los delitos que la pueden habilitar,*** *y a que se limite la duración temporal, habiéndose optado por una duración de un mes prorrogable como máximo por iguales periodos de tiempo hasta los tres meses.*

Finalmente y por lo que se refiere a las ***diligencias de investigación tecnológica,*** *la reforma contempla como medida de aseguramiento la* ***orden de conservación de datos, cuyo fin es garantizar la preservación de los datos e informaciones*** *concretas de toda clase que se encuentren almacenados en un sistema informático hasta que se obtenga la autorización judicial correspondiente para su cesión. De este modo* ***su posterior aportación como medio de prueba o, en su caso, su análisis forense no se verá frustrado por la desaparición, alteración o deterioro de unos elementos inherentemente volátiles****. Esta norma* ***toma como referencia el artículo 16 del Convenio sobre la Ciberdelincuencia, de 23 de noviembre de 2001****, ratificado por España el 20 de mayo de 2010, y se establece un plazo máximo de vigencia de la orden de noventa días prorrogable hasta que se autorice la cesión o se cumplan ciento ochenta días. (…)*

se prevé la posibilidad de que ***los agentes encubiertos puedan obtener imágenes y grabar conversaciones,*** *siempre que recaben específicamente una autorización judicial para ello; y de otra, se regula la figura del agente encubierto informático, que requiere autorización judicial para actuar en canales cerrados de comunicación (puesto que en los canales abiertos, por su propia naturaleza, no es necesaria) y que a su vez, requerirá una* ***autorización especial*** *(sea en la misma resolución judicial, con motivación separada y suficiente, sea en otra distinta)* ***para intercambiar o enviar archivos ilícitos por razón de su contenido en el curso de una investigación.***

Las medidas aplicadas en la citada reforma legal se pueden resumir en:

- Aplicación del **principio de especialidad**, donde se prohíben las medidas de investigación tecnológica -incluida la interceptación de las comunicaciones telefónicas y telemáticas- de naturaleza prospectiva. Deben tener por objeto el esclarecimiento de un hecho punible concreto.

- Se **autoriza la intervención y registro de las comunicaciones** de cualquier clase que se realicen a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual.

- Respecto del registro de **dispositivos informáticos de almacenamiento masivo**, se descarta cualquier duda acerca de que esos instrumentos de comunicación y, en su caso, almacenamiento de información **son algo más que simples piezas de convicción**, estableciendo una exigente regulación respecto del acceso a su contenido.

- En cuanto al registro remoto de dispositivos informáticos se ha acotado con un **listado "numerus clausus" de los delitos** que la pueden habilitar, y también se ha limitado la duración temporal de un mes prorrogable como máximo por iguales periodos de tiempo hasta los tres meses.

- Se contempla como medida de aseguramiento la **orden de conservación de datos**, cuyo fin es garantizar la preservación de los datos e informaciones concretas de toda clase que se encuentren almacenados en un sistema informático hasta que se obtenga la autorización judicial correspondiente para su cesión.

6 Herramientas de análisis forense digital

En la actualidad existen diversas herramientas destinadas al análisis forense digital que se aplican sobre los distintos aspectos del dispositivo o componente a analizar, como por ejemplo, sobre discos duros, memorias de almacenamiento, infraestructuras de red, *software*, móviles, portátiles, etc.

Dependiendo del objetivo de la investigación y/o ámbito de actuación se aplican unas herramientas u otras (figura 6). En general, en la fase de adquisición de evidencias, la más crítica, se deben utilizar herramientas *software* portables, ejecutables desde unidades *externas –dvd* y/o *usb-* con el fin de no alterar la escena del delito por la instalación de aplicaciones forenses en los sistemas a analizar.

Por otro lado, una vez recopiladas y custodiadas las pruebas, estas se analizan en el laboratorio forense donde se puede aplicar la tecnología *hardware* y *software* forense más sofisticado para la obtención y análisis de las evidencias extraídas (figura 6).

Así pues, tenemos *software* portable forense, y *hardware* tecnológico y *suites* de *software* o distribuciones utilizado en los laboratorios forenses por equipos de expertos.

A continuación en la tabla 7 se detalla las herramientas más utilizadas y válidas para investigación forense digital, indicando su área de trabajo, su descripción, la última versión y enlace actualizado de descarga.

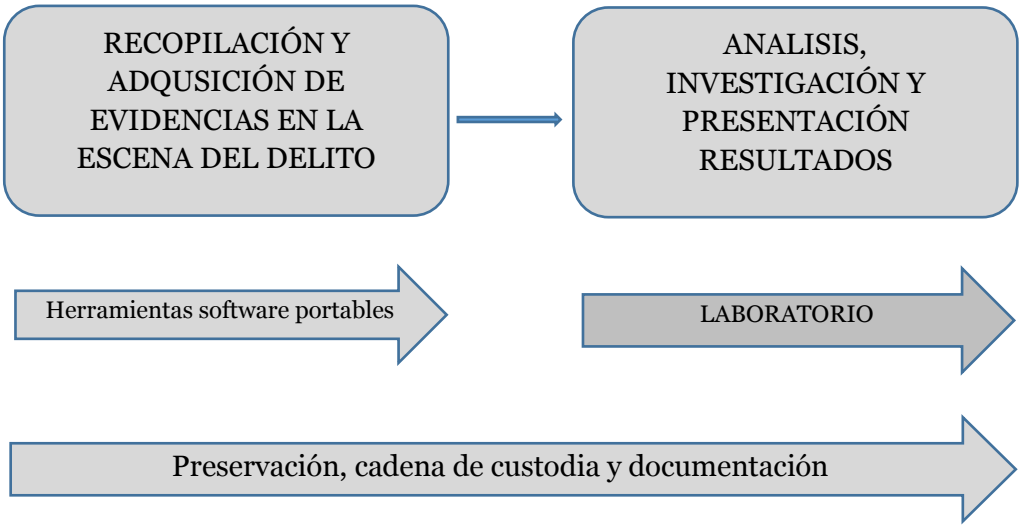


Figura 6. Aplicación de herramientas y equipos forense en la investigación

[Fuente propia]

Utilidades y software portable en informática forense

Utilidades y herramientas portables [25]	
Montaje y virtualización de unidades	
ImDisk	Controlador de disco virtual. Versión actual 2.0.9 16 diciembre 2015 http://www.ltr-data.se/opencode.html/
OsfMount	Montar imágenes de discos locales en Windows Versión 1.5.1015 7 febrero de 2014 http://www.osforensics.com/tools/mount-disk-images.html#downloadosfm-32
FTK Imager	Montar imágenes de discos, volcado de memoria, entre otras funciones. Versión 3.4.2 23 febrero de 2016 http://accessdata.com/product-download/digital-forensics/ftk-imager-version-3.4.2
LiveView	Crear una máquina virtual VMware[26] de la imagen del disco Versión 07b http://liveview.sourceforge.net/
MountImagePro	Montar imágenes de discos locales en Windows Versión v6.1.3.1626 http://www.mountimage.com/
Raw2mdk	Permite montar raw disk image creados por "dd" usa VMware Versión 0.1.3.1 https://sourceforge.net/projects/raw2vmdk/
Análisis y adquisición de la memoria	
DumpIt	Vuelca el contenido de la memoria a un fichero Versión 2.0 http://www.moonsols.com/windows-memory-toolkit/
Proccess Dumper	Convierte un proceso de la memoria a fichero Versión 1.1 14 de julio de 2006 http://www.trapkit.de/research/forensic/pd/
Responder CE	Captura y analiza el contenido de la memoria Versión Pro trial 30 días http://www.countertack.com/
RedLine	Entorno gráfico para capturar y analizar la memoria Versión 1.14 de 12 de junio de 2015 https://www.fireeye.com/services/freeware/redline.html
Memorize	Captura la memoria en entorno Windows y OSX Versión 3.0 de 23 de julio 2013 https://www.fireeye.com/services/freeware/memoryze.html
Volatility	Extrae y analiza los procesos para su análisis Versión Volatile Systems - Volatility Framework v1.3 http://www.securitybydefault.com/2013/07/analisis-forense-en-linux-analizando-la.html

[25] **Conexión Inversa [En línea]:** http://conexioninversa.blogspot.com.es/
Listado de herramientas forenses digitales. Forensics PowerTools. Enlaces de descarga y versiones actualizadas en este trabajo a fecha 08 marzo 2016. Se han suprimido o añadido herramientas.

Utilidades y herramientas *software I*	
Recuperación y tratamiento de discos	
PhotoRec	Recuperación de imágenes y vídeos borrados Versión 7.0 http://www.cgsecurity.org/wiki/PhotoRec
Scalpel	Recuperar ficheros y directorios independientemente del sistema de archivos. http://www.enlinux.org/recuperar-archivos-con-scalpel-en-gnulinux-centos-6/
NTFS Recovery	Permite recuperar datos incluso de discos formateados Versión 7.5 del 13 de mayo de 2015 http://www.ntfs.com/recovery-toolkit.htm
Recovery RS	Recuperar documentos de unidades formateadas y refragmentadas. Versión 3.8 del 3 de diciembre de 2014 http://rs-file-recovery.softonic.com/
Recuva	Recuperación de archivos borrados Versión 1.52.1086 http://www.piriform.com/recuva/download
RaidReconstructor	Recupera datos de un RAID dañado, incluso si se desconocen los parámetros. Versión 4.32 http://www.runtime.org/raid.htm
Restoration	Utilidad para recuperar ficheros borrados. Versión 2.5.14 del 21 de agosto del 2003 http://www.snapfiles.com/get/restoration.html
FreeRecover	Utilidad para recuperar ficheros borrados. Versión 15 de abril de 2013 https://sourceforge.net/projects/freerecover/
R-Studio	Recuperación de datos de cualquier sistema de disco Versión 7.x http://www.r-studio.com/
IEF	Internet Evidence Finder. Realiza Carving sobre una imagen de disco. Versión 5.0 https://www.magnetforensics.com/
Bulk Extractor Viewer	Permite extraer datos desde una imagen, carpeta o ficheros. Versión 1.5.5 http://digitalcorpora.org/downloads/bulk_extractor
CNWrecovery	Recupera sectores dañados y corruptos. Incorpora técnicas de Carving[27]. Versión 1.8.0.1 de abril 2015 http://www.cnwrecovery.com/html/data_carving.html
GuyMager	Herramienta Linux para adquisición de imágenes forenses de evidencias. Versión 0.5.9 http://packages.ubuntu.com/precise/x11/guymager
GParted	Editor gráfico manipulación de particiones de discos en Linux. Versión 0.25 http://gparted.org/download.php
UnBlock	Permite cambiar permisos a dispositivos en Linux RO/RW. Viene con la distribución Linux GNU Caine 7.0

Utilidades y herramientas *software II*	
Análisis del sistema de ficheros	
AnalyzeMFT	Utilidad programada en lenguaje *python* que permite extraer la MFT (Tabla de Asignación de Archivos) del disco. Versión 2.0.4 https://github.com/dkovar/analyzeMFT
INDXParse	Herramienta para los índices y fichero $I30. Es una licencia sobre Apache 2.0 http://www.williballenthin.com/forensics/indx/index.html
MFT Tools	Conjunto de utilidades para el acceso a la MFT Versión 1.0.x ... https://code.google.com/archive/p/mft2csv/downloads
MFT Parser	Utilidad que extrae y analiza la MFT Versión 08b http://redwolfcomputerforensics.com/downloads/MFT_Parser_08b_Setup.exe
Prefetch Parser	Utilidad que extrae y analiza el directorio *prefetch* Versión 1.5 http://redwolfcomputerforensics.com/downloads/parse_prefetch_info_v1.5.zip
FileAssassin	Utilidad que desbloquea ficheros bloqueados por los programas Versión 1.06 https://www.malwarebytes.org/fileassassin/
WinHex	Completo editor hexadecimal, datos de memoria RAM, borrado seguro, etc. Versión 18.7 http://www.winhex.com/winhex/index-m.html
Análisis del registro de Windows	
RegRipper	Permite la extracción, la correlación, y visualización de la información del registro Versión 2.8 del 22 de mayo de 2013 https://code.google.com/archive/p/regripper/
Windows Registry Recovery	Herramienta gráfica obtiene datos del sistema, usuarios y aplicaciones del registro Versión 1.5.30 del 3 de enero de 2015 http://www.mitec.cz/wrr.html
Shellbag Forensics	Análisis de los *shellbag* de Windows Versión 0.24 http://www.williballenthin.com/forensics/shellbags/index.html
Registry Decoder	Extrae y realiza correlación de datos del registro aún encendida la máquina. Versión 1.3 http://www.digitalforensicssolutions.com/registrydecoder/

[26] **VMware (s.f.)** Según Wikipedia se refiere "un sistema virtual por software es un programa que simula un sistema físico (un computador, un hardware) con unas características de hardware determinadas" [En línea] https://es.wikipedia.org/wiki/VMware

[27] ***Carving (2015).*** Según Asier Martínez (INCIBE) 30/06/2015 es: "*una técnica forense para extraer información a partir de una cantidad de datos en bruto sin necesidad de conocer el sistema de ficheros con el que se han creado los ficheros.* "
https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/file_carving

Recuperación de contraseñas en Windows	
Ntpasswd	Editor de contraseñas de Windows Versión 14.02.01 http://www.pogostick.net/~pnh/ntpasswd/
Pwdump7	Vuelca los *hash*. Se ejecuta mediante la extracción de los binarios SAM http://www.tarasco.org/security/pwdump_7/
SAMInside	Volcado de los hash. Incluye diccionarios para ataques por fuerza bruta http://www.insidepro.com/
Ophcrack	Volcado de los hash. Incluye diccionarios para ataques por fuerza bruta. Versión 3.6.0 http://ophcrack.sourceforge.net/download.php
L0phtcrack	Volcado de los hash. Incluye diccionarios para ataques por fuerza bruta. Versión 6.0.20 http://www.l0phtcrack.com/
ChromePass	Extrae las contraseñas almacenadas en Google Chrome. versión 1.36 http://www.nirsoft.net/utils/chromepass.html
Utilidades de análisis de Red	
WireShark	Herramienta para la captura y análisis de paquetes de red Versión 2.0.2 https://www.wireshark.org/
NetworkMiner	Herramienta forense para el descubrimiento de información de red Versión 2.0 http://www.netresec.com/?page=NetworkMiner
Netwitness Investigator	Herramienta de captura y análisis de tráfico de red. -- https://www.rsa.com/en-us/products-services/security-operations
Network Appliance Forensic	Conjunto de utilidades para la adquisición y análisis de trafico de red Versión 0.0.9 http://didierstevens.com/files/software/NAFT_V0_0_9.zip
Xplico	Es capaz de extraer todos los correos electrónicos que llevan los protocolos POP y SMTP, y todo el contenido realizado por el protocolo HTTP. http://www.xplico.org/
Snort	Herramienta de detección de intrusos Versión 2.8.9.0 https://www.snort.org/
Splunk	Indexa y aprovecha los datos generados por todos los sistemas e infraestructura de IT: física, virtual o en la nube. Motor Base de datos *logs* .... http://www.splunk.com/
AlientVault	Recolecta los datos y *logs* aplicándoles una capa de inteligencia para la detección de anomalías, intrusiones o fallos en la política de seguridad. https://www.alienvault.com/
Firebug	Análisis de aplicaciones web. Versión 2.0.14 http://getfirebug.com/

Herramientas de análisis de amenazas y vulnerabilidades	
PDF Tools	Herramienta para el análisis y gestión de archivos en formato *pdf.* Versión 0.64 http://blog.didierstevens.com/programs/pdf-tools/
PDFStreamDumper	Herramienta gratuita para el análisis de archivos PDF maliciosos. Versión 0.9.590 http://sandsprite.com/blogs/index.php?uid=7&pid=57
SWF Mastah	Programa lenguaje *python* que extrae el *stream SWF* de ficheros PDF. -- http://blog.9bplus.com/snatching-swf-from-pdfs-made-easier/
Captura BAT	Permite la monitorización de la actividad del sistema o de un ejecutable. Versión 2.0.0.5574 https://www.honeynet.org/node/315
Regshot	Crea *Snapshots* del registro pudiendo comparar los cambios entre ellos. Versión 1.9.0 https://sourceforge.net/projects/regshot/files/latest/download
LordPE	Herramienta para editar ciertas partes de los ejecutables y volcado de memoria de los procesos ejecutados.
OllyDbg	Desensamblador y depurador de aplicaciones o procesos. Versión 2.0.1 http://www.ollydbg.de/
Jsunpack-n	Emula la funcionalidad del navegador al visitar una URL. Su propósito es la detección de *exploits.* Versión 0.3.2a https://github.com/urule99/jsunpack-n
OfficeMalScanner	Su objetivo es buscar programas o ficheros maliciosos en Office. Versión 25.11.2013 http://www.reconstructer.org/code.html
SAS	SuperAntiSpyware. Analiza y elimina el spyware del ordenador. Versión 6.0.1216 http://www.superantispyware.com/
ClamWin	Antivirus portable para Windows. Elimina troyanos y demás amenazas. Versión 0.99 http://es.clamwin.com/
Xteg	Herramienta de detección automática de esteganografía en archivos JPEG. Versión 0.4 https://www.dropbox.com/sh/1bgdym7c2m9agix/AAA-iywYauv2HV_vWN2hzZkLa/stegdetect-0.4.zip?dl=0
ProcessHacker	Potente herramienta para monitorizar los procesos del sistema. Versión 2.38 http://processhacker.sourceforge.net/

Utilidades de análisis de dispositivos móviles y *tablets*	
IPhone	
iPhoneBrowser	Accede al sistema de ficheros del *iphone* desde entorno gráfico. Versión 1.9.0.0 https://code.google.com/archive/p/iphonebrowser/
iPhone Analyzer	Explora la estructura de archivos interna del *iphone*. Versión 2.1.0 https://sourceforge.net/projects/iphoneanalyzer/
iPhone-Dataprotection	Contiene herramientas para crear un disco RAM forense, realizar fuerza bruta con contraseñas simples (4 dígitos) y descifrar copias de seguridad. https://code.google.com/archive/p/iphone-dataprotection/
SpyPhone	Explora la estructura de archivos interna. -- https://github.com/nst/spyphone
Android	
android-locdump	Permite obtener la geo-localización de la cache del dispositivo. -- https://github.com/packetlss/android-locdump
androguard	Permite obtener, modificar y desensamblar formatos DEX / ODEX / APK / AXML / ARSC. Versión 2.0 https://github.com/androguard/androguard/
Viaforensics	Framework de utilidades para el análisis forense de dispositivos *Android*. -- https://github.com/viaforensics/android-forensics
Osaf	Completo software de utilidades para el análisis forense *Andorid*. Versión 2.7 http://www.osaf-community.org/
Santoku	Distribución Linux para pruebas de seguridad, análisis de malware y análisis forenses para teléfonos móviles, válida para dispositivos con Android, BlackBerry, iOS y Windows Phone. Versión 0.5 https://santoku-linux.com/?fid=santoku-0.1-alpha.iso

Tabla 7. Herramientas y utilidades software *de investigación forense digital*

Distribuciones software para el análisis forense digital

Para iniciarse en el estudio del análisis forense digital, una buena opción es utilizar los paquetes *software* –distribuciones y *suites*- comerciales y *freeware* del mercado. Hay que considerar que las soluciones que se ofrecen son muy similares en cuanto a posibilidades, de modo que utilizar una u otra opción dependerá casi del gusto de cada uno y de la facilidad con la que nos familiaricemos con cada herramienta. En este trabajo se tiene especial atención a las distribuciones *Live DVD/USB/CD* desarrolladas *GNU/Linux*.

Estas distribuciones generalmente funcionan como *Live DVD* y no altera ningún dato del disco duro o dispositivo de almacenamiento del equipo a analizar. Recordar que para realizar un análisis forense es fundamental no alterar las pruebas, en este caso los datos del almacenamiento interno.

Por tanto, se montan todas las particiones de los discos en modo de sólo lectura, una medida fundamental para preservar los datos intactos. Una vez hayamos realizado la copia sector a sector del dispositivo de almacenamiento a analizar, ya podemos pasar a modo escritura con las opciones ofrecidas en cada distribución.

Algunas distribuciones *GNU/Linux* más utilizadas son: Kali y Backtrack para *pentesting*, Santoku para análisis forense en móvil y Deft, Caine y Helix para análisis forense en ordenadores, entre otras, aunque son *frameworks*, tienen herramientas para realizar otras tareas relacionadas con *pentesting* y el análisis forense informático. Hay otras herramientas que tienen versión Linux como Autopsy, Volatility, Accees FTK Imager y herramientas incluidas como QPhotorec Testdisk y Foremost. En redes una buena opción son, por ejemplo, Nessus y Wireshark, o Nmap para recopilar información de vulnerabilidades.

Una alternativa para desarrollar el trabajo de perito informático forense es utilizar herramientas de código abierto, son útiles y permiten realizar las mismas tareas que las comerciales de pago. *Linux* es la mejor plataforma para herramientas de análisis forense, existen más herramientas para este sistema operativo que para cualquier otro y la mayoría son gratuitas y de código abierto, lo que permite adaptarlas a las necesidades.

Por otro lado se pueden analizar otros sistemas operativos sin problema alguno desde *Linux*. El único inconveniente, quizás sea que es un poco más complejo en su uso y mantenimiento, y además, al no ser comerciales, no tienen un soporte continuo. Respecto a la validez y consistencia del *software* utilizado ante la jurisprudencia, las aplicaciones comerciales, por ejemplo EnCase, ofrecen más garantías que las *freeware* o de código abierto, estas últimas pueden haber sufrido modificaciones o sus versiones beta no estar totalmente certificadas, por lo que un abogado puede utilizar esto como motivo de invalidez de la prueba en un juicio. Siempre hay que utilizar herramientas tanto *software* como *hardware* totalmente admisibles ante un tribunal.

A continuación se analizan las últimas distribuciones *software* utilizadas en análisis forense digital:

Caine - Computer Aided INvestigative Environment

Versión 7.0 (05/11/2015)

Descarga: http://www.caine-live.net/page5/page5.html

Es una distribución Live CD GNU/Linux, creada por Giancarlo Giustini y actualmente su director de proyecto es Nanni Bassetti.

Es una de las mejores opciones para realizar una investigación forense de equipos informáticos. Destaca del resto de distribuciones por su facilidad de manejo gracias a su interfaz gráfica homogénea, la cual guía a los profesionales durante las fases de adquisición y análisis de las evidencias digitales. Además, ofrece un procedimiento semiautomático de documentación y generación de los informes periciales.

Esta nueva versión está basada en *Ubuntu* 14.04.01 LTS, y se puede ejecutar en modo *live dvd/usb*. Viene con el *Kernel Linux* 3.13 y con el escritorio MATE 1.8.2, dispone de una gran cantidad de *software* para llevar a cabo las tareas, además está organizado por diferentes categorías para facilitar la investigación forense y la búsqueda de las herramientas necesarias.

CAINE 7.0 únicamente tiene versión de 64 bits. Además también soporta *UEFI*/*Secure Boot*, para compatibilidad con las nuevas placas base del mercado. Otra característica de CAINE es que se puede instalar en local, con un mayor rendimiento para fines de aprendizaje e investigación.

Algunas de las herramientas más interesantes es Autopsy para análisis de imágenes forenses, OPHCrack para averiguar contraseñas, aplicaciones para clonar dispositivos y discos como GuyMager e incluso analizar la memoria *RAM* con Inception o Volatily, entre otras muchas.

En la página web oficial de CAINE 7.0 hay un listado de las herramientas (http://www.caine-live.net/page11/page11.html) que se han actualizado o agregado a esta nueva versión.

Asimismo, también están disponible en su web varios enlaces con diferentes métodos de descarga con un tamaño de 3GB la ISO.

Esta distribución se puede instalar en un *pendrive* con un tamaño mínimo de 4GB, y por ejemplo, con la utilidad Unetbootin hacerlo *booteable*.

También existe una versión ligera llamada NBCaine 4.0 disponible para Live DVD / USB, más ligera e ideal para análisis de trabajo de campo en equipos apagados.

Descarga: http://www.caine-live.net/page5/page5.html

Santoku

Versión 0.5

Descarga: https://santoku-linux.com/?fid=santoku-0.1-alpha.iso

Es una distribución Linux basada en *OWASP's MobiSec* [28] especializada en pruebas de seguridad, análisis de malware y análisis forenses para teléfonos móviles, válida para dispositivos con *Android*, *BlackBerry*, iOS y Windows *Phone*.

Incluye las siguientes utilidades y herramientas:

De desarrollo

> Android SDK Manager, Apple Xcode IDE, BlackBerry JDE, BlackBerry Tablet OS SDK, BlackBerry WebWorks, DroidBox, Eclipse IDE, Windows Phone SDK, Android 2.3.3, 3.2, and 4.0.3 Emulators, Security Compass Lab Server (HTTP and HTTPS), BlackBerry Ripple, BlackBerry Simulators.

Para test de penetración

> CeWL, DirBuster, Fierce, Nikto, nmap, Burp Suite, Mallory, w3af Console, w3af GUI, ZAP, BeEF, Ettercap, iSniff, Metasploit Console, Metasploit GUI, NetSed, SET, SQLMap, SSLStrip.

De ingeniería inversa

> PK Tool, Dex2Jar, Flawfinder, Java Decompiler, Strace.

Analizadores *wireless*

> Aircrack-ng, Kismet, Ubertooth Kismet, Ubertooth Spectrum Analyzer, Wireshark.

Para análisis forense de dispositivos

> AFLogical Open Source Edition, Android Encryption Brute Force, BitPim, BlackBerry Desktop Manager, Foremost, iPhone Backup Analyzer, MIAT, Paraben Device Seizure, Sift Workstation, Sleuth Kit, SQLiteSpy.

De infraestructura móvil

> BES Express, Google Mobile Management, iPhone Configuration Tool.

[28] ***OWASP's MobiSec.*** Se define "El Proyecto de Seguridad OWASP móvil" como: "Un soporte centralizado destinado a dar a los desarrolladores y equipos de seguridad los recursos que necesitan para construir y mantener aplicaciones móviles seguras. A través del proyecto, nuestro objetivo es clasificar los riesgos de seguridad móvil y proporcionar controles de desarrollo para reducir su impacto o la probabilidad de explotación." https://www.owasp.org/index.php/OWASP_Mobile_Security_Project

DEFT - Digital Evidence & Forensic Toolkit

Versión 8.2

Descarga: http://na.mirror.garr.it/mirrors/deft/deft-8.2.iso

DEFT es una distribución GNU/Linux de origen italiano, creada y mantenida por Stefano Fratepietro y su equipo. Dirigida a auditorías de seguridad y especializada en la informática forense, especialmente en tareas como: recuperación de datos de discos duros, *pendrives* o dispositivos móviles; análisis de metadatos; recopilación de pruebas o cualquier tipo de evidencia digital, etc…

Estas tareas las realiza sin contaminar, alterar, borrar o sobrescribir ningún dato de la evidencia, lo que hace que sea muy apreciada por parte de los Cuerpos y Fuerzas de Seguridad del Estado, peritos judiciales, auditores tecnológicos, y todo tipo de investigadores.

La última versión presenta el escritorio LXDE y los programas que habitualmente nos encontramos en este entorno, incluyendo además una gran cantidad de herramientas para auditoría informática como: análisis de datos, antivirus y *antimalware*, recuperación de datos borrados o dañados, *hashing*, *imaging* –crear imágenes y clonados de discos-, análisis forense de dispositivos móviles, análisis forense en redes, recuperación de contraseñas, generación de informes y dictámenes, documentación y por último, *OSINT*, con un conjunto de aplicaciones para obtener inteligencia de fuentes de información abiertas o accesibles.

Algunas de las novedades de esta versión son:

- El gestor de archivos, donde muestra el *status* de los discos del sistema.
- Soporte para *Bitlocker* para cifrado de discos.
- The Sleuthkit 4.1.3
- Digital Forensics Framework 1.3
- Soporte para adquisiciones lógicas -copia bit a bit de los directorios y archivos de una partición- en Android y iOS 7.1.
- JD GUI
- Skype Extractor 0.1.8.8
- Una nueva versión de OSINT browser

Se han actualizado a sus últimas versiones la mayoría de herramientas y programas, como *DART -Digital Advanced Response Toolkit-* una *suite* forense bajo Windows con herramientas *freeware* y que en las últimas versiones de DEFT viene integrada para ejecutarse mediante *Wine*.

Existe una versión más liviana, Deft Zero, orientada a la adquisición de evidencias y clonado de discos y soportes de almacenamiento.

Descarga: http://www.deftlinux.net/2015/01/25/deft_zero_beta_ready_for_download/

HELIX e-fense

Descarga: http://www.e-fense.com/products.php

La empresa e-fense dispone de varias opciones para satisfacer las necesidades en informática forense y ciberseguridad. Dispone de una versión gratuita de evaluación durante 30 días.

Helix3 Enterprise, permite auditar la red en busca de violación de las políticas de seguridad, piratería o código malicioso, entre otras tareas.

Helix3 PRO, es la opción para análisis forense digital, permite realizar imágenes de la memoria RAM y dispositivos de almacenamiento. Además determina si un dispositivo está cifrado y permite realizar un análisis de datos tanto a ordenadores como a dispositivos móviles.

Live Response, es la herramienta para análisis en vivo –*live forensics*-, para adquirir datos volátiles de un equipo encendido, como: el historial de navegación de internet, capturas de pantalla, memoria, etc., de un sistema en una unidad *flash* USB con respuesta en vivo (figura 7).

Figura 7. Unidad USB Live Response de E-fense
Fuente [En línea]: http://www.e-fense.com

En general, Helix es una distribución Linux Live basada en *Knoppix linux*, que permite ser ejecutada en el equipo a investigar con su sistema operativo nativo. Está destinada al análisis forense para entornos Microsoft Windows, GNU Linux y MacOSX.

Una de las características que hace a Helix especial es la mejora en la detección de multitud de fabricantes *hardware*.

Helix dispone de una *suite* de herramientas muy potentes, entre las que destacan: Wireshark, varios antivirus, recuperadores de contraseña, copias de seguridad y restauración de particiones, navegador de particiones MAC, examinador de archivos binarios, Autopsy, entre otros.

Tiene la posibilidad de elegir entre XFPROT y ClamTk, para realizar el análisis de archivos y carpetas en las máquinas sospechosas.

KALI Linux

Versión 2016.1

Descarga: https://www.kali.org/downloads/

Es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática. Fue fundada y es mantenida por Offensive Security Ltd. Mati Aharoni and Devon Kearns, ambos pertenecientes al equipo de Offensive Security, desarrollaron la distribución a partir de la reescritura de BackTrack, que se podría denominar como la antecesora de Kali Linux.

Kali puede ser usado desde un Live CD / USB y también puede ser instalada como sistema operativo principal.

En esta versión (figura 8) se introdujo la opción Forensics Boot al sistema operativo y se vio continuada en BackTrack 5, existe al día de hoy en Kali Linux. Sirve para poner a trabajar las herramientas de *software* libre (http://tools.kali.org/tools-listing) más populares en materia forense de forma rápida y sencilla. A su vez, Kali cuenta con el *software* libre forense más conocido instalado y es sencillo de crear un Live USB / DVD *booteable*.

Se realizaron algunos cambios importantes como que el disco duro no se utiliza en absoluto. Lo que trae como consecuencia que si existe una partición *swap* no va a ser usada, ni se monta automáticamente ningún disco interno y se deshabilitó el auto-montado de medios removibles. Entonces, ni los *pendrives* ni los lectores de CD van a ser montados automáticamente.

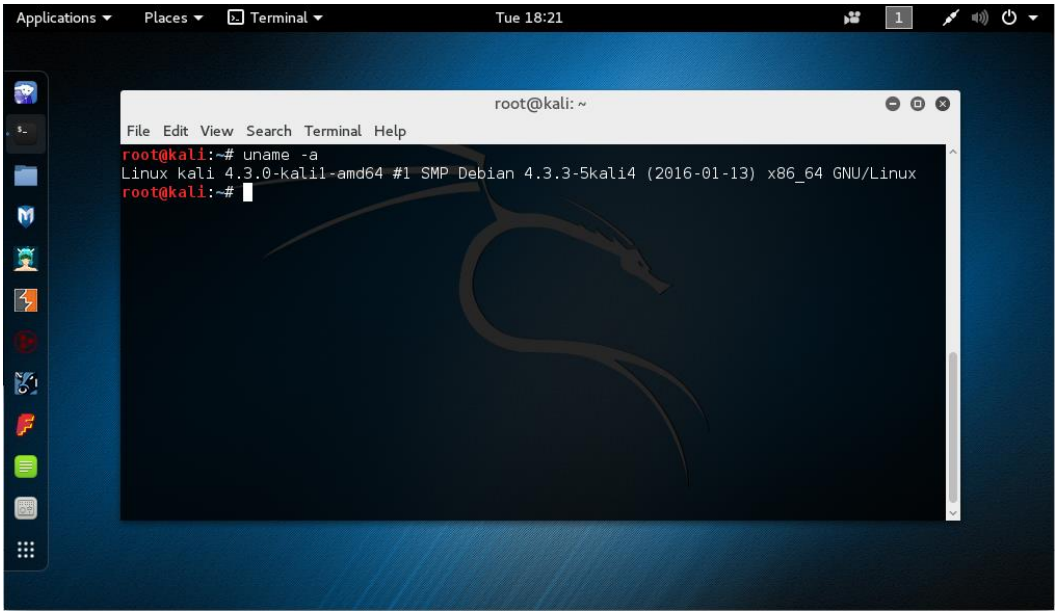


Figura 8. Escritorio de Kali Linux

Fuente [En línea]: http://www.kali.org

EnCase Forensic

Versión 7

Guía de productos: http://www.ondata.es/recuperar/forensics-guidance.htm#

EnCase Forensic es una poderosa plataforma de investigación para recolección y adquisición de datos digitales. Sirve para realizar análisis, informar sobre descubrimientos y preservar en un formato válido a efectos legales y valido por los tribunales. EnCase es la *suite* forense más utilizada por los Cuerpos de Seguridad en sus laboratorios forenses, junto con Ilook (de uso exclusivo por la policía).

Características principales:

- Obtiene adquisiciones válidas a efectos legales

  Produce una duplicación bit a bit exacta del dispositivo o medio original y posteriormente genera los valores *hash* de las imágenes y asigna valores de CRC a los datos. Estas verificaciones revelan si la evidencia ha sido contaminada, alterada o manipulada indebidamente, ayudando a mantener toda la evidencia digital con validez a efectos legales para su uso en procedimientos judiciales.

- Funciones de productividad avanzadas

  Se puede obtener una vista previa de los datos mientras se obtiene acceso a las unidades u otros medios. Una vez creados los archivos de imagen, se pueden buscar y analizar varias unidades u otros medios simultáneamente. Su indexador de casos crea un índice completo en varios idiomas, lo que permite realizar consultas de forma rápida y sencilla. Los índices se pueden asociar entre sí para buscar palabras clave comunes a otras investigaciones. Este índice compatible con *Unicode* contiene documentos personales, archivos eliminados, artefactos de sistemas de archivos, demora de archivos, archivos intercambiados, espacio no asignado, correos electrónicos y páginas web. Además, EnCase ofrece una amplia compatibilidad con distintos sistemas de archivos, brindándoles a las organizaciones la posibilidad de analizar todo tipo de datos.

Dispone de versión portable, una versión automática de EnCase para búsqueda y adquisición de datos instalada y ejecutada desde un dispositivo *USB bootable*.

Con este dispositivo cualquiera puede adquirir datos forenses, incluso sin tener grandes conocimientos de análisis forense o informática. Es un gran complemento si ya se dispone de una licencia EnCase.

Laboratorio forense. Dispositivos *hardware y software*

La elevada demanda de servicios en informática forense, peritaje informático y auditorias seguridad, entre otros, ha provocado –lo que hasta ahora solamente era 'terreno' de gobiernos y cuerpos de seguridad de estado- la aparición de empresas de laboratorio de análisis forense digital. Estas empresas disponen de profesionales cualificados, equipos forense de campo -con tecnología hardware y software para adquisición de evidencias en la escena del delito-, y laboratorios con la infraestructura tecnológica, medidas de seguridad, herramientas *hardware* y *software* de análisis, y metodologías de investigación admisibles para la elaboración de informes y dictámenes periciales.

Para su acreditación por la agencia ENAC (Entidad Nacional de Acreditación), estos laboratorios tecnológicos deben cumplir la legislación española vigente, entre otras, la aplicación de la Norma UNE EN ISO / IEC 17025:2005 de "*Evaluación de la conformidad. Requisitos generales para la competencia de los laboratorios de ensayo y de calibración*".

Como se ha comentado a lo largo del trabajo, las evidencias electrónicas o digitales requieren de un análisis forense detallado para aportar las pruebas del incidente o delito cometido, previa labor de localización y recopilación de las mismas.

En la fase de adquisición o captura forense de las evidencias se debe realizar el clonado forense o imagen de los datos de interés almacenados en los distintos soportes digitales. Aquí ocurren dos situaciones a tener en cuenta la adquisición de datos en: sistemas apagados o en sistemas encendidos "en vivo".

En este último caso, sistemas encendidos, se tiene que actuar con cautela, realizar fotografías de la pantalla, y utilizar equipos de adquisición hardware y software específicos que garanticen la integridad de la información recopilada para su análisis posterior en los laboratorios. En este caso, la adquisición de la información volátil del sistema es necesaria realizarla desde el propio equipo o dispositivo a investigar utilizando para ello medios externos -*dvd/usb*- o remotos desde donde ejecutar las utilidades, o bien utilizar dispositivos *hardware* homologados que faciliten y garanticen el proceso de adquisición y preservación de evidencias. Nunca se deben instalar programas en los equipos objeto de investigación.

En el caso de teléfonos móviles encendidos lo primero será pasar a modo 'avión' (si dispone de esta opción) para aislarlo de las redes. Posteriormente, utilizando los mencionados dispositivos y equipos *hardware* forense, realizar un clonado de la información accesible de la tarjeta SIM, y arrancar de nuevo el móvil con la SIM clonada. Entones se procede a realizar la copia a bajo nivel de todos los datos almacenados.

Para sistemas apagados, se debe realizar el clonado de los discos o soportes de almacenamiento utilizando dispositivos bloqueadores *hardware* que eviten la escritura de ningún dato adicional a los ya almacenados.

De igual forma se debe efectuar un resumen digital '*hash*' de la información contenida en el disco o soporte de almacenamiento original de forma simultánea al procedimiento de clonado usando herramientas *hardware* o *software* específicas.

Una vez se adquieren las evidencias, los discos o soportes originales de almacenamiento se deben volver a precintar y sellar junto con los equipos donde iban instalados, documentando la información relativa a la cadena de custodia de las evidencias recopiladas. En caso necesario se utilizarán cajas de Faraday u otros contenedores de transporte especiales que aseguren la información original de las evidencias a analizar en el laboratorio.

Por lo dicho, para realizar un análisis informático forense es imprescindible contar con el equipamiento necesario, no solo para investigar sino también para proteger la integridad de los dispositivos a analizar, de forma que sigan siendo válidos como prueba judicial. Para ello se utilizan dispositivos *hardware* como: bloqueadores de escritura, copiadoras, duplicadoras, creadoras de imágenes ultrarrápidas, equipos para investigación en "vivo" no intrusivos y que no dejan huella, así como equipos para borrado seguro de los soportes de almacenamiento donde se realiza el clonado o copia imagen del original.

En el siguiente apartado se estudian los dispositivos y equipos portátiles *hardware* para '*live forensic*', y los dispositivos, sistemas y equipos *hardware* utilizados en los laboratorios de análisis forense digital (figura 9).

Figura 9. Laboratorio informático forense de una empresa privada

Fuente [En línea]: http://hard2bit.com

Estaciones forenses avanzadas

Las estaciones forenses deben ser potentes servidores que permitan desarrollar las tareas de investigación, donde se precisa gran capacidad de almacenamiento para los clonados y copias de seguridad y altas prestaciones de procesamientos con recursos tecnológicos de última generación.

Algunos ejemplos de estaciones forenses son las descritas a continuación fabricadas por la empresa Adalid, que dispone de modelos de alto rendimiento (figura 10) y modelos de gama media (figura 11).

Fuente [En línea]: http://www.adalid.com/productos/

Figura 10. Estación forense Zeus

Estación forense de alto desempeño en el procesamiento de evidencia digital, acorde a necesidades de altos volúmenes de análisis de datos, especial para Laboratorios que requieran una muy alta disponibilidad de espacio de almacenamiento mediante arreglos RAID 0, 1, o 5; con excelente disipación de altas temperaturas, convirtiéndose en la mejor opción para ejecución de Software Forense de nueva generación que demanda varios recursos del equipo.

Board Dual Socket GA-7PESH3 LGA2011
Intel® Xeon® Procesador E5-2600 V2 LGA 2011 (x2)
Monitor 27-Inch Full-HD 2ms LED con Webcam y Sonido
Memoria RAM 64GB DDR3 2400Mhz HyperX Beast (Max 256GB)
Conexiones eSATA, SATA3, FireWire, USB 3.0.
Disco Duro estado sólido SSD 512GB CSSD-F512GBLX, Array x2 HDD 2TB
Quemador BluRay DL, DVD RW, CD RW.
Fuente de alto desempeño modular 1200W
Chasis Última Generación
Disipación por Radiador All-In-One Liquid Cooling System CLW0224
GB GDDR5 DIGI+ VRM technology Graphic Card HD7770-2GD5 x3DVI x1 HDMI
Kit de Bloqueadores de escritura Tableau modelo Ultra Kit II

Figura 11. Estación forense Hades

Estación forense avanzada en procesamiento de evidencia digital, especial para Laboratorios donde se necesite velocidad en adquisición y estudio de datos sin que estos pierdan fuerza probatoria, excelente disipación de altas temperaturas, capacidad de interconexión con diversas tecnologías de avanzada transferencia de datos (Thunderbolt, WiFi 2ways, eSATA, SATA3, Bluetooth 4.0, NFC).

Board 97-DELUXE (NFC & WLC) ATX DDR3 2600 LGA 1150
Intel Core i7-4790K (8M Cache, up to 4.40 GHz) New 4ta Generation
Monitor 27-Inch Full-HD 2ms LED con Webcam y Sonido
Memoria RAM 32GB DDR3 2400Mhz HyperX Beast
Conexiones eSATA, SATA3, FireWire, USB 3.0, USB 2.0, Thunderbolt, WiFi 2ways, Bluetooth 4.0, NFC,
Wireless Charger
Disco Duro estado sólido SSD 512GB CSSD-F512GBLX, x1 HDD 2TB
Quemador BluRay DL, DVD RW, CD RW.
Fuente de alto desempeño modular 1200W
Chasis Última Generación
Disipación por Radiador All-In-One Liquid Cooling System One Socket
GB GDDR5 DIGI+ VRM technology Graphic Card HD7770-2GD5 x3DVI x1 HDMI
Kit de Bloqueadores de escritura Tableau modelo Ultra Kit II

Equipos hardware portátiles de análisis forense

Fuente [En línea]: http://www.ondata.es/recuperar/equipos-forensics.htm

Equipo de análisis forense Logicube modelo Forensic Falcón	
• *Creación rápida de imagen forense a 20GB/min* • *Creación de imagen y verificación desde 4 discos origen a 5 destinos* • *Crea imagen hacia o desde una ubicación en red* • *Multitarea. Realiza tareas de creación de imagen, borrado y hash simultáneamente* • *Interfaz de usuario web. Permite el acceso remoto mediante un navegador de internet.*	 *Figura 12. Logicube Forensic Falcón*

Duplicadora Logicube modelo Forensic Talon	
Diseñada especialmente para las investigaciones forenses, Forensic Talon es un sistema que asegura la adquisición y captura mediante los procedimientos correctos aumentando la velocidad significativamente. Forensic Talon es el sucesor del altamente aclamado MD5 y forma parte de la quinta generación de herramientas de Logicube orientadas a la informática forense. *Velocidades cercanas a los 4GB/min con UDMA5.* *Cálculo de MD5 o SHA-256 a tiempo real.* *Búsqueda de palabras clave durante el proceso de captura o separado.* *Captura de datos en formato DD con posibilidad de fraccionar la imagen en trazas de 650MB, 2GB y 4GB.* *Tarjeta Compact Flash para almacenamiento de listas de palabras, reportes, actualizaciones de Firmware etc.* *Teclado QWERTY integrado.*	 *Figura 13. Logicube Forensic Talon*

Duplicadora Logicube modelo Forensic Dossier	
Diseñada exclusivamente para la captura forense de datos, Forensic Dossier es la sexta generación de soluciones forenses de Logicube. Forensic Dossier está provista de tecnología de última generación junto con una interfaz de fácil uso. Perfecta para trabajo de campo y de laboratorio. *Capaz de ofrecer la captura simultánea de 1 o 2 discos objetivo a 1 o 2 discos de evidencia.* *Soporte nativo para SATA e IDE y conectividad USB y Firewire.* *Velocidades de hasta 7GB/min.* *Soporta adquisición formato E01 compatible con EnCase y FTK v3.x* *Soporte opcional para dispositivos SCSI y SAS.* *Autenticación MD5 y SHA.* *Soporte para dispositivos de 2TB y más en formato NTFS* *Búsqueda avanzada de palabras clave.* *Compatible con MPFS.* *Captura de HPA y DCO.* *Teclado QWERTY integrado.* *Módulo opcional para el acceso a través de red.*	 *Figura 14. Logicube Forensic Dossier*

Duplicadora Tableau modelo TD2	
Construida sobre la fuerza y reputación de la venerada TD1, la duplicadora forense TD2 cuenta con funciones avanzadas y un rendimiento excepcional en un formato compacto, duradero y de fácil manejo. *Este producto de segunda generación ha sido diseñado para adquisiciones forenses tanto en campo como en laboratorio, con una interfaz nativa que permite adquirir dispositivos SATA e IDE/PATA con una velocidad de hasta 9 GB/min. Utilizando el mismo protocolo que TD1, las investigaciones pueden incluir (opcionalmente) objetivos USB y SAS.* *Entre las nuevas capacidades de TD2 se encuentran la duplicación 1:2, duplicación disco a disco o disco a imagen, formateo de unidades, Wipe, Hash (MD5 o SHA-1), detección y eliminación de HPA/DCO, capacidad para realizar imágenes en RAW DD, E01 (EnCase comprimido) y EX01.*	 *Figura 15. Duplicadora Tableau TD2*

Duplicadora Tableau modelo TD3	
Están las herramientas de imagen forense y después está la Tableau TD3 Forensic Imager. *Una herramienta con un núcleo TD3 de alto rendimiento, fiable y fácil de usar. Su interfaz de usuario con pantalla táctil de alta resolución hace sencilla la captura forense de datos desde dispositivos SATA, IDE, USB 3.0/2.0/1.1, SAS y FireWire (1394A/B). Ninguna de las duplicadoras forenses del mercado actuales es capaz de igualar a la TD3 en su combinación única de rendimiento, encapsulado, capacidades forenses y modos de uso.* *Pensando en la necesidad de acceder a dispositivos de almacenamiento de forma remota, TD3 Forensic Imager soporta el bloqueo de escritura a través de la red, permitiendo la previsualización o la adquisición de datos desde máquinas remotas utilizando la IP adecuada.*	 *Figura 16. Duplicadora Tableau TD3*

Duplicadora CRU modelo Ditto	
CRU presenta el nuevo estándar de explotación de datos digitales y adquisición forense. Ditto es mucho más que una máquina de clonado forense al uso. con velocidades de operación de hasta 6.5GB/min, *Ditto ofrece un gran abanico de posibilidades:* *Capacidad de navegación y adquisición de datos a través de la red mediante conexión SSL por sus puertos, origen y destino Gigabit Ethernet.* *Perfecta para el trabajo de campo al estar equipada con una batería de larga duración.* *Sin ruido de ventilación debido a su arquitectura.* *Copia simultánea a dos dispositivos en modo RAW DD, clon o mixto* *Interfaz sencilla y amigable.* *Capacidad de adquisición desde dispositivos con interfaz SATA/eSATA, PATA, USB 2.0 GbE y PCIe Expansion Module.* *Modo silencioso que permite operaciones con baja visibilidad* *Soporte para destino de EXT2/3/4, XFS, HFS+ y FAT32* *Bypass temporal o permanente de HPA/DCO* *Módulos de expansión para permitir la interacción con USB3.0, SAS, FireWire, SCSI, ThunderBolt y PCI/PCI x4*	 *Figura 17. Duplicadora CRU Ditto*

Duplicadora Voom modelo Hardcopy 3	
Dispositivo Hardware diseñado para ayudar a los investigadores forenses. *Principales características:* *Velocidad de hasta 7.5 Gb por minuto en la transferencia de datos.* *Realiza 2 copias a la vez de un mismo disco duro.* *Verificación SHA256.* *Modos de duplicación (clonación y creación de imágenes).* *Copia DCO y HPA (copia todos los datos incluidos los protegidos).* *Diferentes métodos de borrado.* *Duplicación de otros discos duros (ATA, portátiles...).* *Ingeniería de duplicación de discos.*	 *Figura 18. Duplicadora Voom Hardcopy 3*

Equipo análisis forense Voom modelo Shadow 3	
Dispositivo hardware diseñado para ayudar a los investigadores forenses a acceder al soporte magnético sin alterar su contenido. *Principales características:* *Permite investigar discos duros origen en la escena del crimen en cuestión de minutos, antes de crear la imagen. Con el constante aumento de capacidad de los discos duros, el ahorro de tiempo a la hora de priorizar el orden de los discos de los que se creará la imagen, o incluso eliminar la necesidad de crear la imagen de ciertos discos cuando se trata de una captura múltiple, se ha convertido en algo de vital importancia.* *Permite investigar y analizar discos origen una y otra vez en el laboratorio forense en cuestión de segundos sin necesidad de volver a crear la imagen.* *Permite ver las evidencias en su ambiente nativo.* *Permite presentar las evidencias de una forma comprensible para los no expertos en el propio ordenador investigado.* *Cuando se sospecha una actividad ilícita, como la descarga nocturna de archivos confidenciales, utilice Shadow para verificar la actividad y preservar los metadatos.*	 *Figura 19. Análisis forense Voom Shadow 3*

JTAG para móviles	
Un puerto JTAG, y dependiendo del dispositivo móvil, suele utilizarse para la realización de testeos por el fabricante, y de forma muy particular para realizar tareas de debugging. Dicho puerto JTAG podría llegar a ser utilizado para acceder a la memoria flash del dispositivo móvil, lo cual sería algo muy positivo para un examinador forense.	 *Figura 20. Puerto JTAG para móvil*

Equipo de *flasheo* de móviles.	Figura 21. *Flasheo* de móviles		
1. Extracción directa desde el chip de memoria con desoldador por aire caliente. *2. Reprogramadora Universal de memorias.* *3. Zócalo de adaptación de encapsulado TSOP (el más comúnmente utilizado en memorias FLASH) para una reprogramadora universal.*	1	2	3

Herramientas de campo

El perito informático deberá portar las siguientes herramientas:

Figura 22. Herramientas forenses para trabajo de campo

[Fuente en línea]
Informática pericial. http://periciasinformaticas.sytes.net

- *Lector / grabadora externa de CD/DVD USB*
- *Switch (Networking)*
- *Computadora portátil (Laptop)*
- *Impresora portátil y cámara video/fotos*
- *Dispositivos de almacenamiento externo con conector USB y un Pen drive*
- *Disco rígido inicializado para copias*
- *Cables UTP CAT6 para conexión Ethernet: Directo y cruzado*
- *Destornilladores*
- *Kit de pinzas*
- *Marcadores indelebles*
- *Cinta de embalaje*
- *Etiquetas de seguridad*
- *Guantes de látex y cúter*
- *Cables de datos PATA para conexión de discos rígidos*
- *Cables de alimentación para PC*
- *CD-R y DVD-R vírgenes*
- *Software forense.*

Equipos de análisis forense de móviles y tablets

XRY Complete

Fuente [En línea]: http://ondatashop.com/xry-complete/

Figura 23. Sistema integral análisis de móviles XRY Complete

El sistema integral de análisis forenses de móviles de Micro Systemation

XRY Complete es el sistema integral de análisis forenses de móviles de Micro Systemation; una combinación de nuestras soluciones lógicas y físicas en un solo paquete. XRY Complete permite a los investigadores el acceso completo a todos los métodos posibles para recuperar datos desde un dispositivo móvil.

XRY es una solución basada en un software fabricada expresamente para tal fin que incluye todo el hardware necesario para la recuperación de datos de dispositivos móviles de una manera segura desde el punto de vista forense. Con XRY Complete puede conseguir más y profundizar en más detalle en un dispositivo móvil para recuperar datos vitales. Con una combinación de herramientas de análisis lógicas y físicas disponibles para dispositivos compatibles, XRY Complete puede crear informes combinados con datos actuales y eliminados procedentes del mismo terminal.

El sistema XRY es la primera opción de organismos internacionales que desarrollan su labor en el ámbito del orden público y representa un sistema completo para análisis forenses de móviles, con todo el equipo necesario para realizar un examen forense de un dispositivo móvil – de instalación simple. La aplicación de software que se suministra de XRY se ejecuta con Windows y dispone de la potencia suficiente para responder a todas las demandas modernas de los examinadores forenses. La interfaz de usuario es de fácil navegación con un asistente sencillo diseñado para ayudarle en todo el proceso desde principio a fin. De esta forma, usted puede comenzar inmediatamente a recuperar datos con total confianza.

Con XRY, se crea un informe en minutos a prueba de manipulación, que se puede personalizar de forma sencilla de acuerdo a las necesidades del usuario, incluyendo referencias y una marca propia de usuario, según se necesite. El informe que se genera se puede imprimir en su totalidad o prepararse con los datos seleccionados por los investigadores. Con la función de exportación de XRY, a los usuarios se les ofrece una amplia gama de funcionalidad que facilita la mayor distribución y el análisis de los datos.

El paquete XRY Complete incluye:

- *Software de la aplicación XRY y clave de licencia*
- *Maletín con organizador de cable*
- *Unidad de comunicación XRY*
- *Kit de cable de teléfono móvil XRY Logical*
- *Kit de cable de teléfono móvil XRY Physical*
- *Dispositivo SIM id-Cloner con licencia de 12 meses*
- *5 tarjetas de examen SIM id-cloner regrabables*
- *Lector de tarjeta de memoria protegida contra escritura*
- *Licencia de software Logical de 12 meses*
- *Licencia de software Physical de 12 meses*
- *Aplicación de software de visor hexadecimal XACT*
- *Cepillo de limpieza de contacto*
- *Soporte telefónico gratuito, foro en Internet o por correo electrónico*
- *Mantenimiento y actualizaciones de software gratuitos*

UFED Physical Analyzer

Fuente [En línea]: http://ondatashop.com/ufed-physical-analyzer/

Figura 24.UFED Physical Analyzer. Análisis forense para móviles

UFED Physical Analyzer está disponible con la licencia Ultimate, UFED Physical Analyzer es la aplicación más avanzada de análisis, decodificación y generación de informes en la industria del análisis forense para dispositivos móviles. Esta aplicación incluye detección de programas maliciosos, funciones de decodificación y generación de informes mejoradas, gráfico de línea de tiempo, capacidades de exportación de datos y mucho más.

Capacidades avanzadas para:

iOS

- *Eludiendo contraseñas simples y complejas al realizar extracciones físicas y del sistema de archivos en determinados dispositivos con iOS 3.0 o superior, incluyendo iOS 6*
- *Desencriptado y decodificación en tiempo real de datos, aplicaciones y desencriptado de llavero en tiempo real, revelando contraseñas de usuario.*
- *Decodificación avanzada de aplicaciones*

BlackBerry

- *Decodificación avanzada de mensajes de BlackBerry Messenger (BBM), correos electrónicos, ubicaciones, aplicaciones y más*
- *Desencriptado en tiempo real de contenido protegido por contraseña de determinados dispositivos BlackBerry con OS 4 o posterior*

Android

- *Decodificación avanzada de todas las extracciones físicas realizadas en dispositivos Android en cualquiera de sus versiones*
- *Decodificación avanzada de aplicaciones y archivos de aplicaciones*

GPS

- *Extracción y decodificación de dispositivos GPS portátiles*
- *Exclusivo – Extracción física de archivos de registro de viaje Tom Tom.*

Fuente: http://www.cellebrite.com/es/mobile-forensics/products/applications/ufed-physical-analyzer

Equipos forenses de análisis de red

E-Detective

Fuente [En línea]: http://ondatashop.com/e-detective/

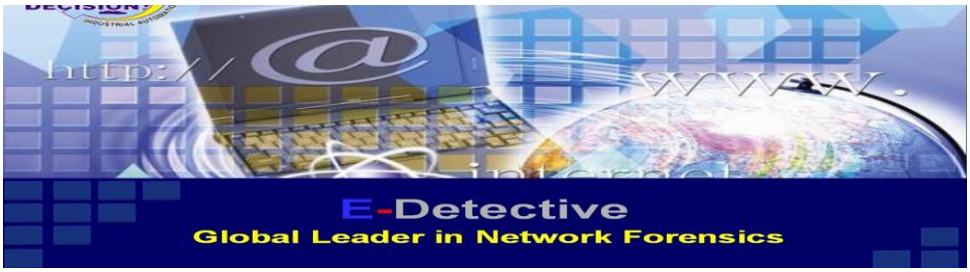


Figura 25. E-Detective. Sistema forense para red

Análisis forense de red en tiempo real y sistema de interceptación legal

E-Detective *es un sistema forense que intercepta y monitoriza el tráfico de Internet en tiempo real., capaz de capturar y reconstruir varios tipos de tráfico de red. Es un sistema de interceptación legal utilizado por la mayoría de Agencias de seguridad, Departamentos de policía y Defensa, Gobiernos, etc.*

E-Detective es capaz de descifrar, reensamblar y reconstruir varias aplicaciones de Internet y servicios como el correo electrónico (POP3, IMAP y SMTP), Webmail (Gmail, Yahoo Mail, Windows Live Hotmail, etc.), mensajería instantánea (Yahoo, MSN, ICQ, QQ, Google Talk, salas de Chat IRC, UT, Skype), transferencia de archivos (FTP, P2P), juegos en línea, Telnet, HTTP (enlace, contenido, reconstruir, cargar y Descargar, Streaming de Video), VOIP (módulo opcional) etc..

E-Detective incluye gran variedad de características y funciones administrativas y de gestión. Le proporciona varios tipos de informe con vista de arriba hacia abajo. Informes que se pueden crear, incluyen informe estadístico, informe de servicio de red (diaria, semanal), Top webs etc.. Todas las estadísticas pueden mostrarse por dirección IP o por cuenta de usuario.

E-Detective también ofrece variedades de funciones de búsqueda. Ofrece búsqueda de texto libre (búsqueda por palabras clave con apoyo booleano), búsqueda condicional, búsqueda Similar y asociación con la búsqueda de la relación. También viene con alerta y notificación (rendimiento, condicional y alerta de palabras clave) funciones que permiten al administrador de red configurar parámetros y reglas diferentes de alerta. Esto permite alertas por correo electrónico (correo electrónico que se enviarán al administrador) una vez que el contenido especificado se encuentra en el contenido capturado y reconstruido.

Función de copia de seguridad permite al usuario hacer backup de los archivos de datos raw capturados o reconstruido. El Usuario puede configurar un auto backup a un backup al disco externo (SAN o NAS) a través de FTP upload método automático. Además, el usuario puede optar por un backup manual y asi grabar estos archivos en CD/DVD e incluso guardarlos en un disco duro local unidad/PC.

Otras funciones disponibles son: marcadores (Bookmarks), capturar archivo de lista (comparando el contenido de dos archivos), lista en línea de IP, asignación de autoridad, Syslog Server etc.. Otras funciones incluyen la exportación hash (backup) y comparación del contenido del archivo.

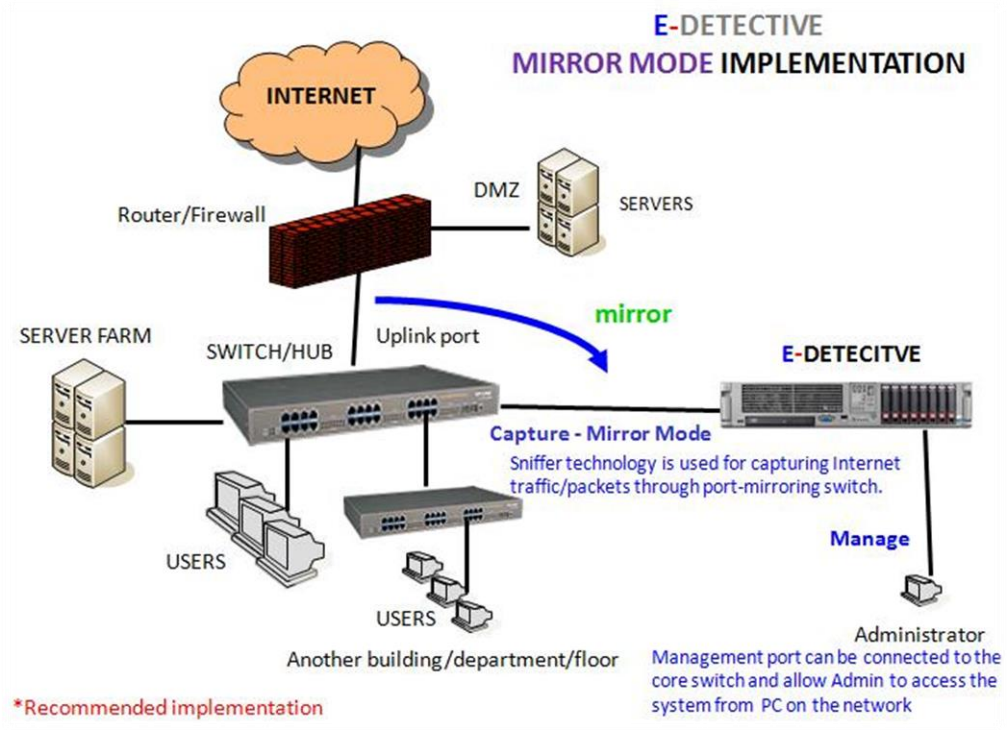


Figura 26. E-Detective. Diagrama de Implementación modo Mirror para interceptación de Internet.

Fuente [En línea]: http://ondatashop.com/e-detective/

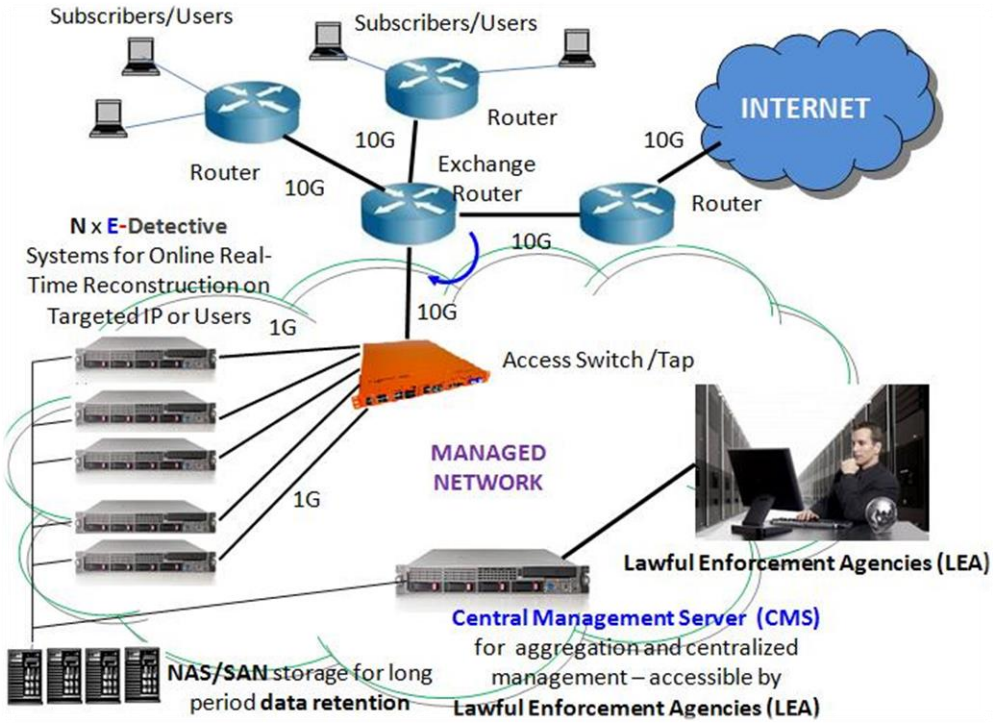


Figura 27. Diagrama de E-Detective Telco ISP de interceptación legal en masa

Fuente [En línea]: http://ondatashop.com/e-detective/

7 Como crear nuestro laboratorio forense

El entorno de trabajo de un informático forense se reduce básicamente a la investigación en la escena del delito –análisis forense de campo- , y el análisis forense en laboratorio. En este sentido, todo perito informático en su labor de informática forense debe de estar preparado y equipado con las herramientas *hardware* y *software* para el desempeño de la pericia encomendada. A continuación se ofrece una guía para crear el entorno de trabajo del perito informático forense.

Herramientas y utilidades forenses para trabajo de campo

- DVD / USB con las herramientas y utilidades de *software* ligero portables para análisis de sistemas encendidos.
- Live USB NBCaine 4.0 para adquisición y análisis en sistemas apagados.
- Disco duro *usb* 'limpio' para copia de datos forenses adquiridos.
- Ordenador portátil HP con Windows 7 Ultimate.
- Y en general, el equipamiento descrito en el capítulo anterior apartado "*Herramientas necesarias para el trabajo de campo".*

Contenido del usb /dvd de trabajo. Software portable para "live forensics"

Figura 28. Software portable "live forensics" para trabajo de campo

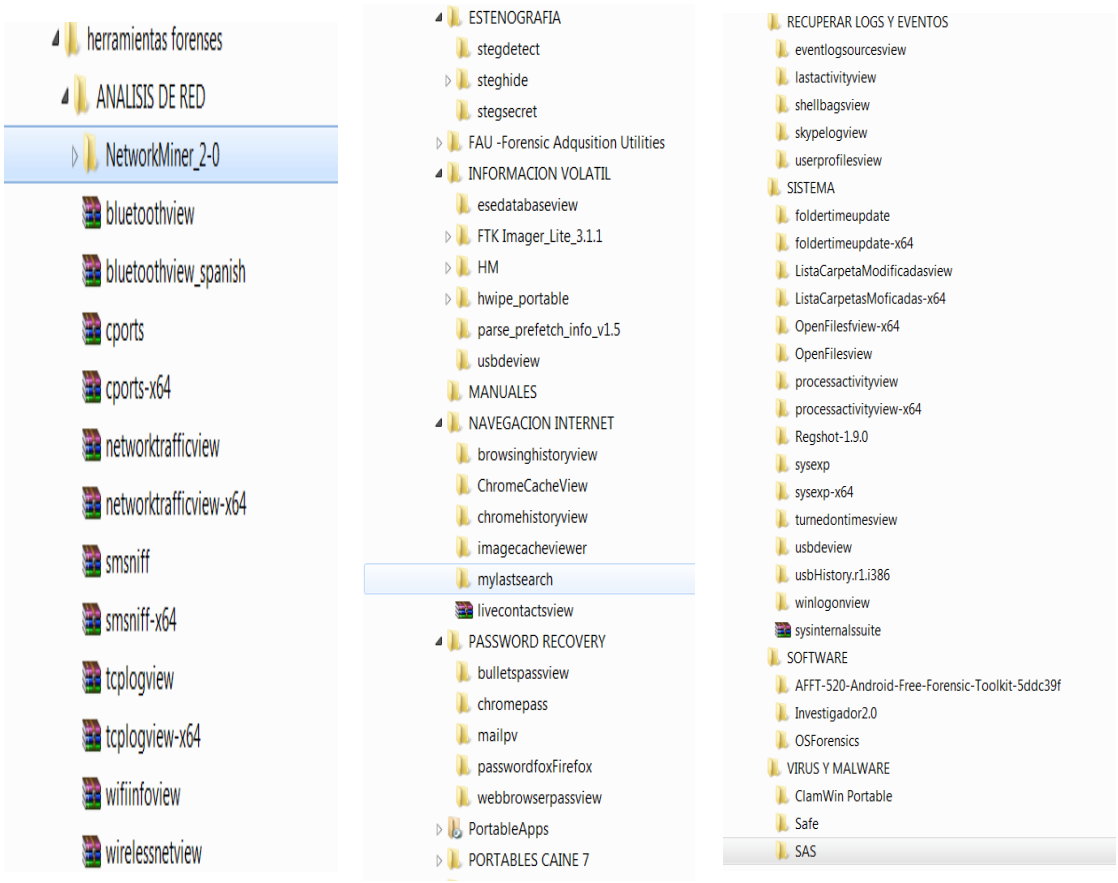


Figura 29. Herramientas y utilidades del pendrive / DVD de trabajo de campo

Todas las utilidades y programas de la lista (figura 29) son de libre distribución (*freeware*) y válidos legalmente para el uso forense digital. La carpeta SOFTWARE contiene algunas utilidades instalables, como OsForensics.

Se adjunta a la memoria de Trabajo de Fin de Grado un DVD con todas estas utilidades.

Por otro lado, si se solicita al perito la investigación *in-situ* –escena del delito- de cualquier dispositivo digital apagado –ordenadores, portátiles, servidores,...- es necesario arrancar el mismo desde una unidad externa *usb*, *dvd*, red, etc, con un sistema que garantice que nunca se montará automáticamente ningún dispositivo. Cuando se hace clic en el icono del dispositivo, el sistema lo montará en modo de sólo lectura. De esta forma se asegura la integridad de la prueba original –información contenida en discos duros-. Esto se consigue con distribuciones ligeras GNU *Linux Live* dvd / usb *Forensic*, como por ejemplo, NBCaine que ofrece las herramientas necesarias para la adquisición de imágenes forenses y clonado de discos, análisis de datos y generación de *hashes* e informes.

Preparar Live USB NBCaine 4.0

1. Descargar ISO NBCaine 4.0 desde el enlace web de la página oficial: http://www.caine-live.net/page5/page5.html

2. Utilizar el programa Rufus para crear el dispositivo Usb *booteable* a partir de la imagen ISO de NBCaine (figura 30).

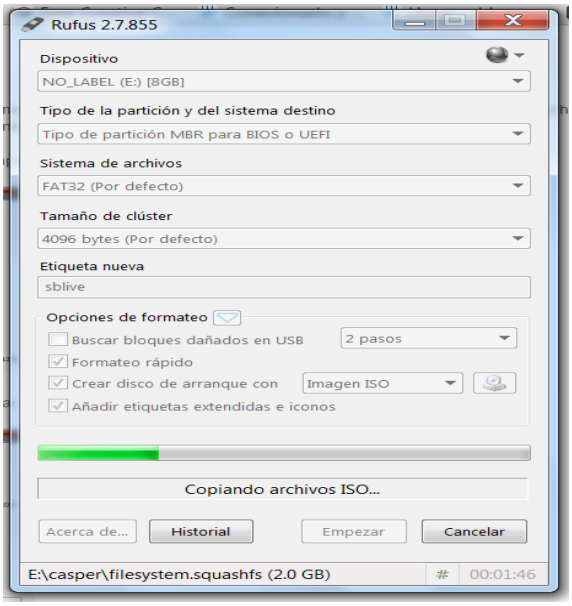


Figura 30. Rufus para crear Live USB NBCaine 4.0

Descarga: http://rufus.akeo.ie/?locale

3. Ahora ya podemos utilizar el *pendrive* como herramienta de trabajo de campo en equipos apagados. Tendremos que elegir al inicio del equipo a analizar el *boot* correspondiente al dispositivo *usb*.

4. Una vez en NBCaine hay que crear y montar las particiones / directorios, modo *write,* donde copiaremos las copias de las imágenes forenses adquiridas.

5. Finalizada la copia bit a bit de las evidencias debemos poner en modo de solo lectura los directorios / particiones donde se almacenan las imágenes forenses a analizar. De esta forma se evita su contaminación.

Equipo forense para investigación en laboratorio

En primer lugar, es necesario disponer de un ordenador / servidor con las aplicaciones y distribuciones de análisis forense instaladas, con los suficientes recursos tecnológicos y capacidad de procesamiento.

Para este caso disponemos de una estación forense con las siguientes características:

- Cuatro procesadores principales 2,67Ghz
- 6 Gb de memoria RAM
- 150 Gb de Disco duro SATA interno
- Disco externo SATA de 400 Gb.
- Grabadora de DVDs
- Tarjeta Gráfica NVidia Quatro con 3Gb de RAM dedicada.
- Windows 7 Ultimate de 64 bits
- VMWare VirtualBox versión 5.0.16

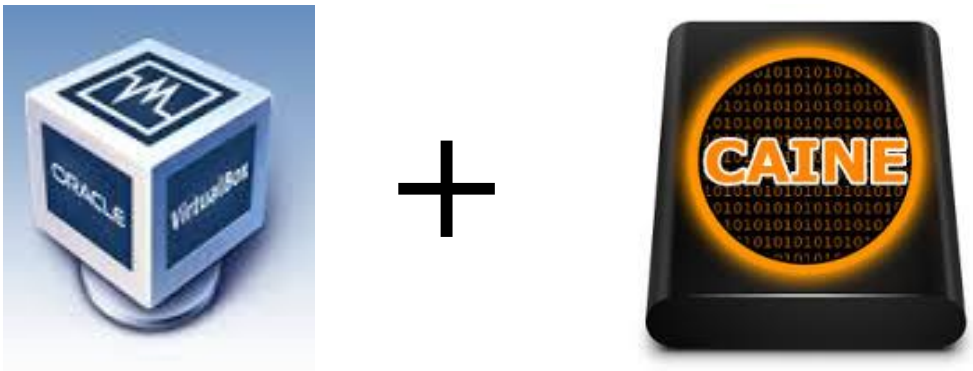
Aplicaciones Windows de informática forense instaladas:

- WinHex 18.1
- OsForensics 3.3 64 bits – Versión gratuita
- Directory Snoop 5.11 Trial
- Autopsy 4.0
- Access Data FTK Imager 3.1.2.0
- ProcessHacker 2.22
- Win-UFO versión 6.0

Además, se dispone de todas las herramientas y utilidades portables del *usb / dvd* para trabajo de campo.

También se ha instalado la distribución Live GNU Linux Ubuntu de Caine 7.0 en Virtual Box 5.0.16. Descarga de Virtual Box 5.0.16 para Windows 7 x64:

http://download.virtualbox.org/virtualbox/5.0.16/VirtualBox-5.0.16-105871-Win.exe



1. Descargar la ISO de Caine 7.0 desde: http://caine.mirror.garr.it/mirrors/caine/caine7.0.iso
2. Crear la máquina virtual con un disco dinámico para el *kernel* de Linux y otro disco para el *swap* de Linux (figura 31).

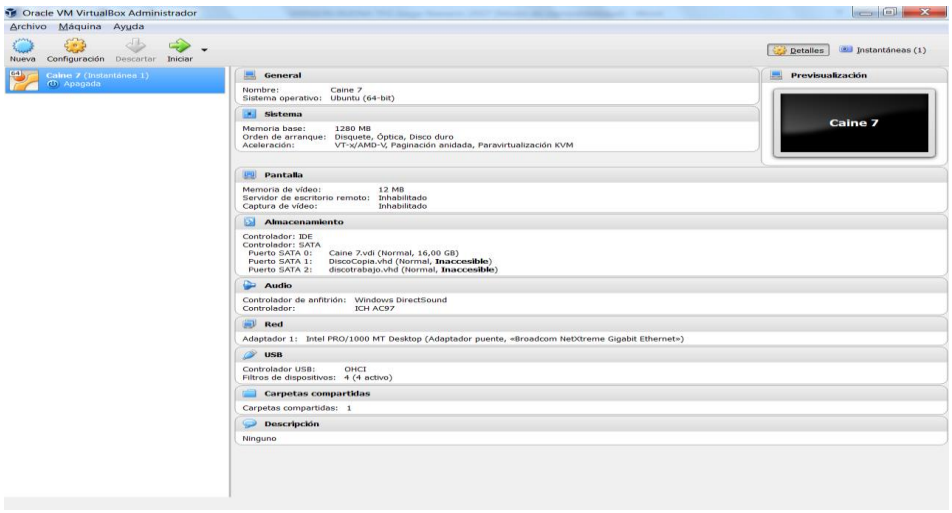


Figura 31. Configuración VMware Virtual Box para Caine 7

3. Al arrancar la máquina virtual por primera vez aparece la ventana "*select start up disk*" donde elige la opción imagen ISO de Caine 7 descargada.
4. Una vez arrancado Caine 7 hay que crear la partición del disco *kernel*. Para ello se utiliza el programa GPARTED (figura 32).
   Ir al menú *Device-> Create Partition Table* y después *Partition-> New*

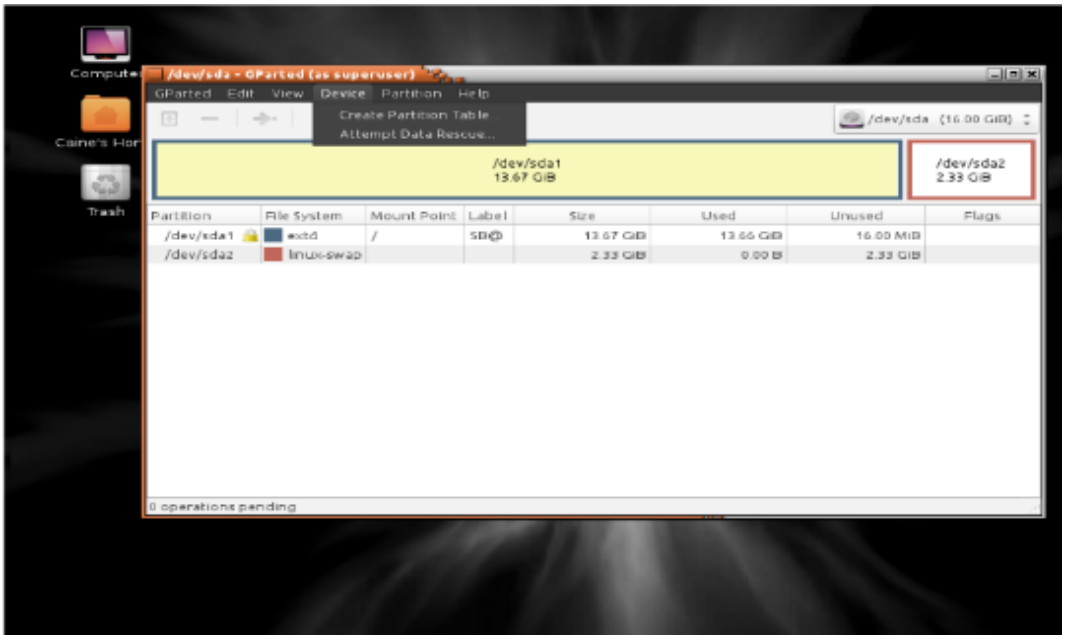


Figura 32. GParted para crear las particiones de disco

5. Ejecutar Systemback para finalizar la instalación de Caine 7 (figura 33). Pulsar en el botón >>*System Install*

Figura 33. Systemback para realizar la instalación de Caine 7

5.1. Completar datos de usuario. Dejar *password* de *root* en blanco, VCaine como *nombre de host y finalmente* pulsar botón *Next* (figura 34).

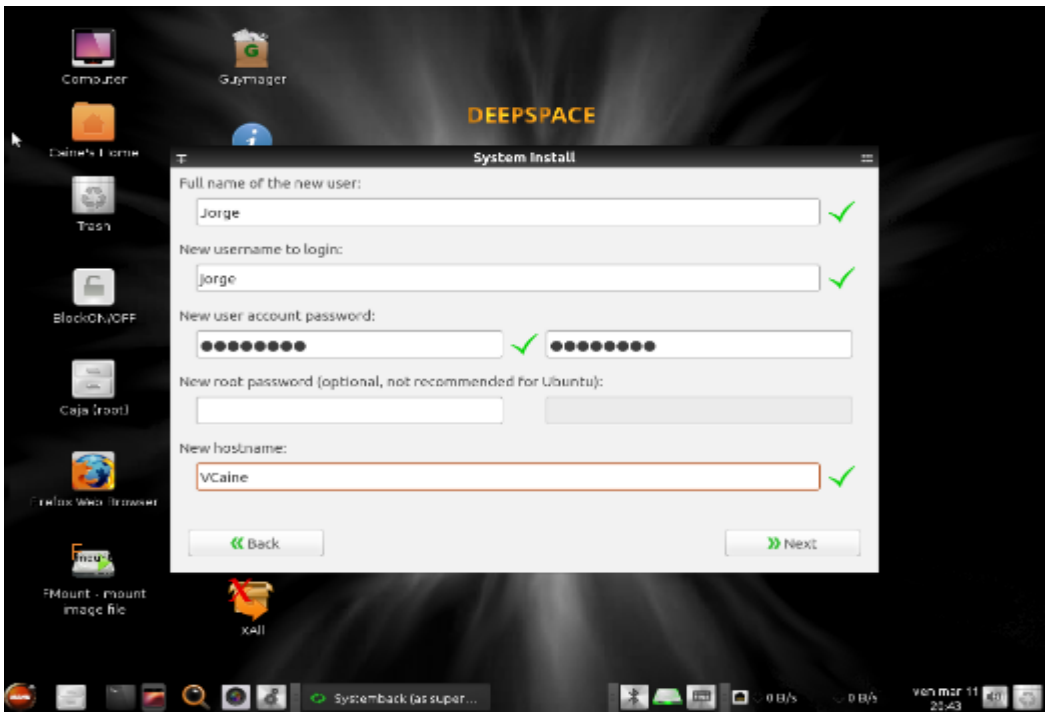


Figura 34. System Install. *Datos de usuario y hostname*

5.2. Seleccionar partición "*sda1*" y el directorio para punto de montaje -> / (*root*). Pulsar la flecha verde para aplicar cambios (figura 35).

Figura 35. System Install. *Punto de montaje en* root.

5.3. Pulsar el botón *start* para instalar el sistema (figura 36).

Figura 36. Systemback Install. Iniciar la instalación del sistema live

5.4. AL finalizar la instalación debemos reiniciamos Linux (figura 37).

Figura 37. Reiniciar Linux tras la instalación

6. Una vez reiniciamos se cargará el nuevo escritorio de *login*. Pulsar en *Login in*. No pide contraseña de usuario (figura 38).

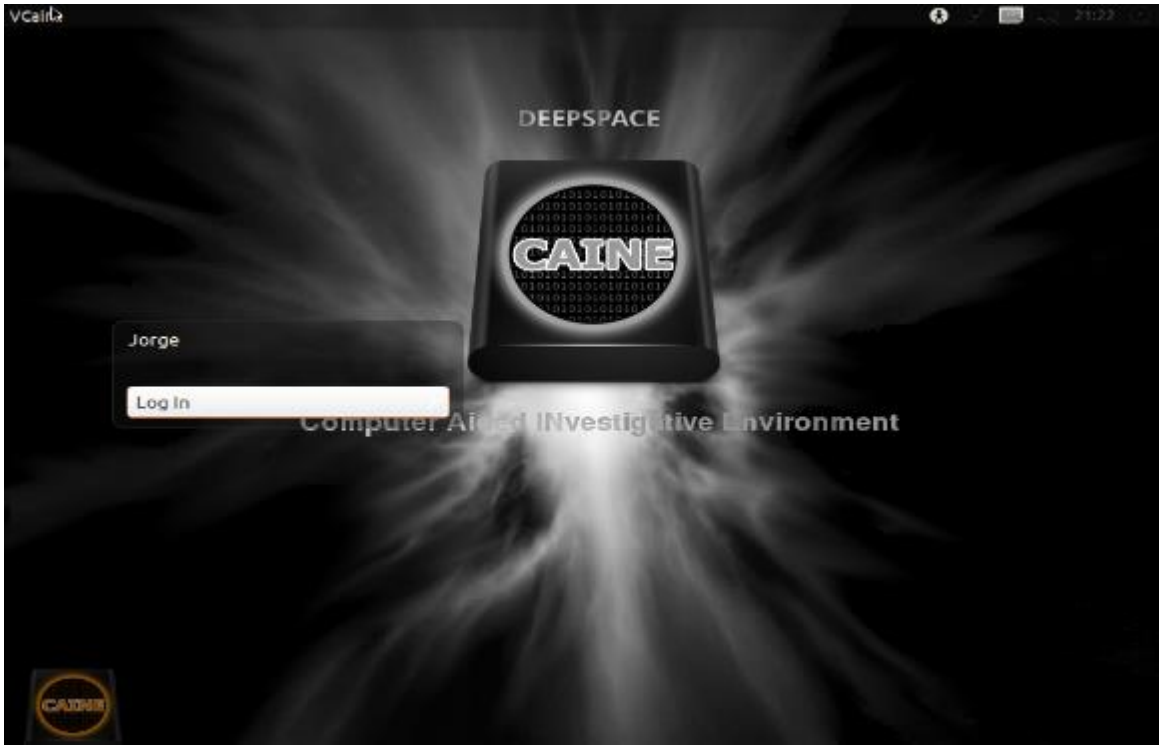


Figura 38. Caine 7.0 instalado y listo para trabajar. Nuevo escritorio Deepspace

7. Hay que tener en cuenta que Caine carga por defecto todas sus particiones en modo solo lectura, por lo que debemos cambiar la partición del *kernel* a modo escritura. Utilizamos la aplicación UnBlock como muestra la figura 39.

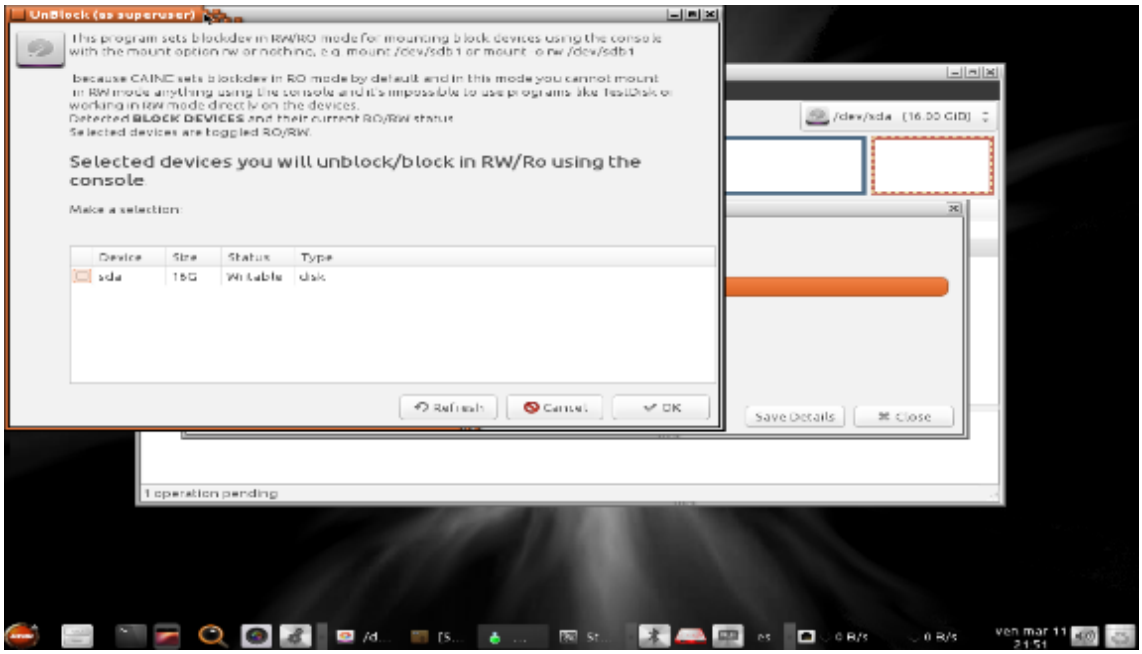


Figura 39. Modo writer *de la partición sda con el programa UnBlock*

8. Crear y montar la partición *swap* de Linux. Observaremos que al volver a arrancar Caine el sistema funcionará mucho más rápido (figura 40).

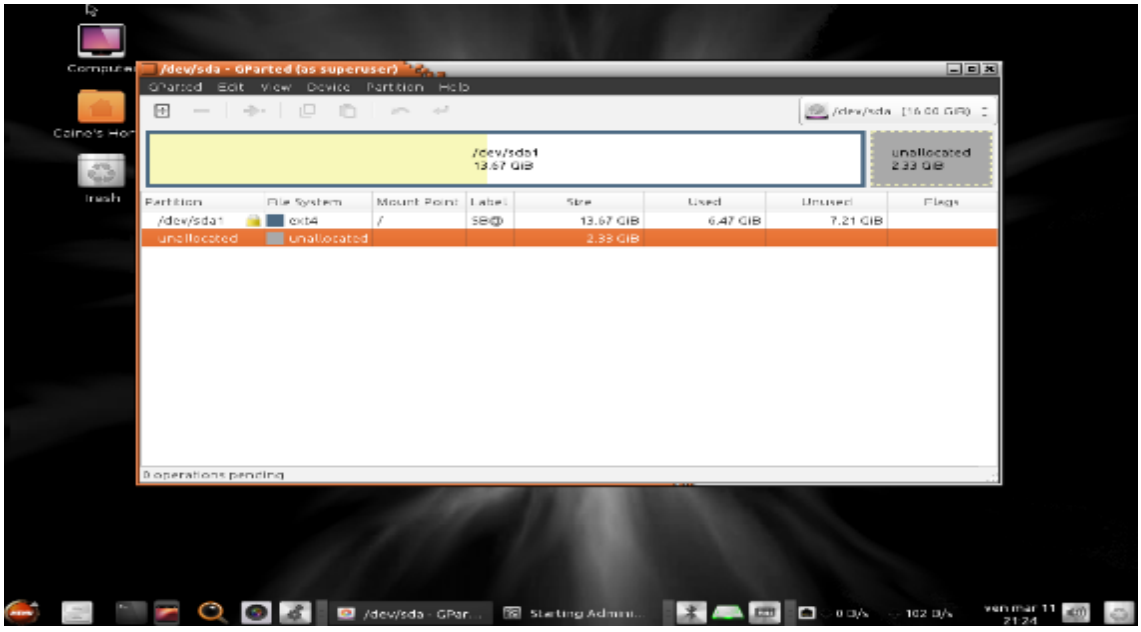


Figura 40. Crear y montar la partición swap de Linux

9. Ya tenemos instalado y configurado Caine 7.0 y disponibles las herramientas para comenzar a trabajar (figura 41).

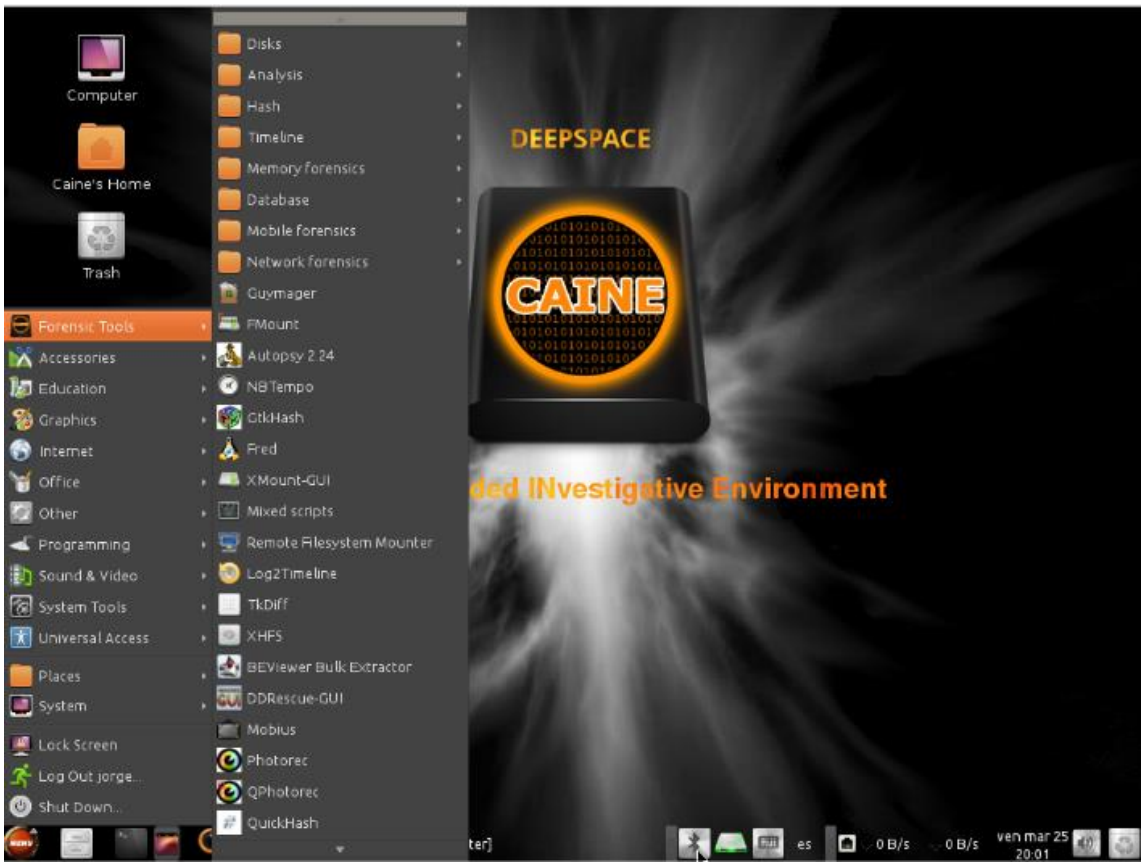


Figura 41. Escritorio definitivo de Caine 7.0 herramientas forenses

8 Caso práctico de análisis forense digital

En este último capítulo se ponen en práctica los conceptos y conocimientos teóricos desarrollados en esta guía, y se ofrece una visión real de la labor del perito informático en la investigación y análisis forense digital.

En esta ciencia, con la continua formación y la experiencia práctica de casos reales, se van adquiriendo los conocimientos para el desempeño de los distintos peritajes informáticos forenses.

A medida que avanza el tiempo –aparición de nuevas tecnologías y entornos cómo el ciberespacio, entre otros- ser perito experto en todos los ámbitos de esta ciencia está al alcance de muy pocos privilegiados. Por ello, el ámbito multidisciplinar de la informática forense digital la convierte en una ciencia tendente a la especialización como ocurre por ejemplo en medicina.

Elegir el tipo de peritaje forense para el desarrollo de este caso práctico ha sido tarea complicada. Es imposible exponer en un solo capítulo la práctica de todos los escenarios posibles del peritaje forense. Así pues, se ha escogido un caso de investigación pericial representativo para el cometido del perito informático judicial.

El caso práctico presentado se descompone en varios sub-casos con la finalidad de poder abarcar la mayor casuística de investigación posible.

Para la realización del caso se consideran las siguientes normas y metodologías:

- ✓ RFC 3227 "Directrices para la recopilación de evidencias y su almacenamiento".
- ✓ UNE 71505-2:2013 "Buenas prácticas en la gestión de evidencias electrónicas"
- ✓ UNE 71506:2013 "Metodología para el análisis forense de evidencias electrónicas".
- ✓ UNE 197010:2015 "Criterios generales para la elaboración de informes y dictámenes periciales sobre Tecnologías de la Información y las Comunicaciones".

Recordar que es importante seguir un adecuado protocolo de actuación –bien documentado y de acuerdo a derecho-, determinar claramente los objetivos de la investigación en base al requerimiento inicial y describir las herramientas y utilidades forenses utilizadas. El perito se centrará en investigar aquello que se le encomiende y para ello, recabará toda la información que considere relevante para el caso. Es responsabilidad de este conocer que evidencias son las que se deben adquirir. La regla de oro es recopilar y preservar todo dispositivo digital de la escena del delito para su posterior análisis en laboratorio.

Descripción del caso práctico. Antecedentes judiciales.

La autoridad judicial solicita los servicios del perito informático judicial JNC para dar apoyo a la investigación tecnológica en un caso de delito informático.

Se facilita el expediente del procedimiento judicial con el fin de aportar al perito toda la información del caso.

Caso "AMPARO CONTRA JAVIER"

En primer lugar, se detalla la denuncia interpuesta por la victima Amparo ante la policía nacional contra Javier dueño de una empresa de servicio técnico informático.

Trascripción de la declaración de Amparo:

1. Amparo deposita su ordenador portátil para su reparación en la empresa YoReparoTuPC -servicio técnico informático - de Xiva (Valencia). Le atiende Javier dueño de la empresa y único técnico y empleado de la misma.

2. Ese mismo día Amparo recoge el portátil ya reparado. Desde su móvil marca LG realiza un video y varias fotos personales e íntimas. Las descarga a su ordenador y las envía por correo electrónico (amparo.xiva@gmail.com) a su novio Jorge (jorge.chiva@gmail.com).

3. Al día siguiente, Juan un amigo de Javier informa a Amparo que Javier le ha enseñado unas fotografías y un video de ella en los que aparece semidesnuda. Esto ocurrió en la oficina de la empresa de Javier desde su portátil y cree que estaban almacenadas en un pendrive negro de piel que ponía El Corte Inglés y con lados plateados. También afirma Juan que Javier le dijo que podía acceder al correo de Amparo pero que iba a borrar todo rastro por seguridad.

A la vista de la denuncia el Juez declara a Javier como presunto acusado de los delitos que se citan a continuación y ordena el registro de la empresa de Javier para recabar las pruebas.

Presuntos delitos cometidos por Javier:

1. Intromisión informática.

El artículo 197.3 del Código penal establece:

> *El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.*
>
> *Del presente precepto debe distinguirse dos modalidades distintas que tienen objeto proteger la intimidad. En primer lugar, la conducta típica consiste en acceder a datos o programas informáticos contenidos en un sistema informático o en parte*

del mismo, buscando castigar a la figura del hacker informático que accede a datos personales o programas informáticos sin el consentimiento de su titular. Por otro lado, la segunda conducta persigue castigar a aquellas personas que se mantengan en el sistema informático en contra de la voluntad de quien tenga el derecho legítimo de excluirlo, presuponiendo previamente un acceso autorizado por el afectado.

2. Revelación de secretos laborales o profesionales.

El Código penal establece en su artículo 199:

1. El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a once meses.

2. El profesional que, con cumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años."

Se pretende castigar a aquéllos que en virtud del cargo que ocupan tienen acceso a secretos ajenos de manera lícita y revelan éstos sin el consentimiento de la víctima.

En primer lugar, la conducta ilícita exige que se conozcan los secretos por razón del oficio o relaciones laborales, quedando en manos del titular del secreto el poder decidir la revelación del mismo cuando se haya terminado la relación laboral que unía contractualmente a ambas partes. Y por último, en segundo lugar, el secreto profesional consiste en la obligación que tiene un profesional de sigilo o reserva de información que sus clientes le confían y desean mantener en secreto, castigándose la conducta de revelación por el profesional.

3. Manipulación de datos reservados registrados en ficheros o soportes informáticos.

Establece el artículo 197.2 del código penal:

Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

El carácter material de este delito son los datos reservados de carácter personal o familiar. Los datos reservados se protegen cuando están almacenados en un sistema informático, electrónico o telemático o en cualquier otro tipo de archivo o registro público o privado. Para que se consideren de ámbito reservado deberán formar parte de la esfera privada del sujeto afectado, cuya disponibilidad a dicha información estará limitada a personas autorizadas por el sujeto en concreto.

> *El artículo 197.2 del Código penal regula dos supuestos que en virtud del caso en concreto pueden incluso sobreponerse. En primer lugar, se castiga a quien se apodere, utilice o modifique datos reservados de carácter personal o familiar; y el segundo supuesto castiga el llamado espionaje informático; esto es, acceder, modificar o utilizar datos de carácter reservado.*

Por todo lo anterior, la instrucción del caso solicita tácitamente al perito JNC que elabore un informe pericial en base a los siguientes requerimientos:

Requerimiento 01

Recopilar las fotografías y video originales realizados por Amparo y enviados por correo desde su portátil. Aportar las pruebas del envió del correo de Amparo a Jorge y su contenido según declarado por Amparo.

Requerimiento 02

Identificar, requisar y preservar el dispositivo almacenamiento extraíble *usb* negro de piel –p*endrive*- para su posterior análisis en laboratorio.

- **Buscar y extraer los archivos que contienen las fotografías y video de Amparo (pruebas originales).**

Requerimiento 03

Determinar si el portátil Toshiba propiedad de Javier sito en la oficina de su empresa contiene indicios que incriminen o no a éste de los delitos que se le acusa.

- **Acceso a la cuenta de amparo.xiva@gmail.com - contraseña robada.**
- **Rastro digital de las fotografías y video de Amparo (prueba original).**
- **Determinar si el *pendrive* citado ha sido conectado a dicho portátil.**

Una vez se tiene claro el tipo de pericia que se va a realizar se debe planificar las actuaciones y documentar la línea de investigación con los métodos y herramientas a emplear.

En caso de cualquier duda, antes de comenzar la investigación, es necesario realizar todas preguntas pertinentes a fin de solventarlas.

Identificación y preservación de las pruebas originales

En primer lugar se van a identificar y custodiar las fotografías y vídeo almacenados en el portátil propiedad de Amparo –pruebas originales-, y enviadas como adjunto en el mensaje de correo electrónico. Se incluirán como prueba original en la investigación.

Obtener información del mensaje de correo electrónico enviado

Se realiza un respaldo digital de contenido original de la cabecera, cuerpo y adjuntos del mensaje enviado con el nombre "Gmail - Fotos y video enviadas por Amparo.pdf" se protege contra escritura para evitar su manipulación y se realiza una captura de pantalla (figura 42), todo esto se realiza ante el secretario judicial que da fe del proceso. El contenido del mensaje es:

MIME-Version: 1.0
Received: by 10.31.234.197 with HTTP; Mon, 14 Mar 2016 08:52:55 -0700 (PDT)
Date: Mon, 14 Mar 2016 16:52:55 +0100
Delivered-To: amparo.xiva@gmail.com
Message-ID: CAKCdkKMsKF+8n302M2zCqAu3sOf_Lb1Y4k7QbGn2=nEax6ebUg@mail.gmail.com
Subject: Fotos y video
From: =?UTF-8?Q?Amparo_S=C3=A1nchez?= amparo.xiva@gmail.com
To: Jorge Navarro jorge.chiva@gmail.com
Content-Type: multipart/mixed; boundary=001a1140ffd6254820052e0446c7
--001a1140ffd6254820052e0446c7
Content-Type: multipart/alternative; boundary=001a1140ffd6254819052e0446c5
--001a1140ffd6254819052e0446c5
Content-Type: text/plain; charset=UTF-8--001a1140ffd6254819052e0446c5Content-Type: text/html; charset=UTF-8

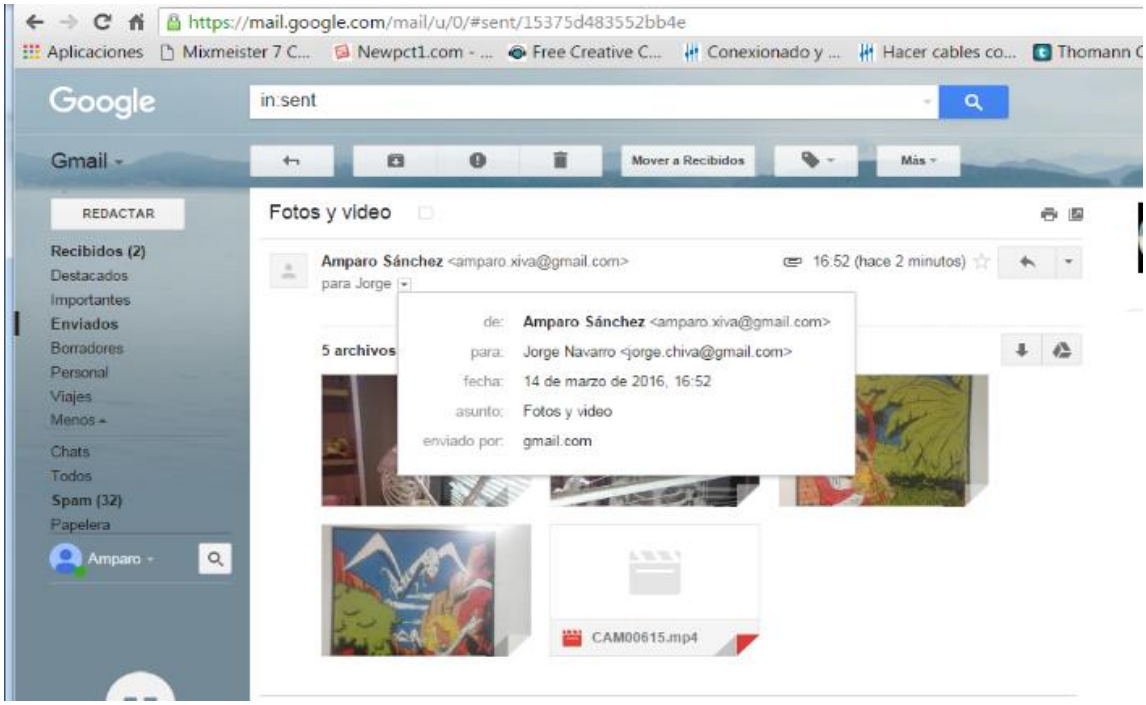


Figura 42. Captura de pantalla del mensaje de correo electrónico.

Es importante especificar el servidor de correo electrónico por si esta prueba fuera recurrida en caso de procedimiento judicial. Servidor: GMAIL.COM /empresa Google/

Crear imagen forense de las pruebas

En el laboratorio con la aplicación portable **AccessData FTK Imager** v3.1.18 creamos la imagen de los ficheros originales en "pruebaoriginal.ad1" y sus correspondientes *hashes*. Se copian por duplicado finalmente en CD para su custodia y preservación (figura 43).

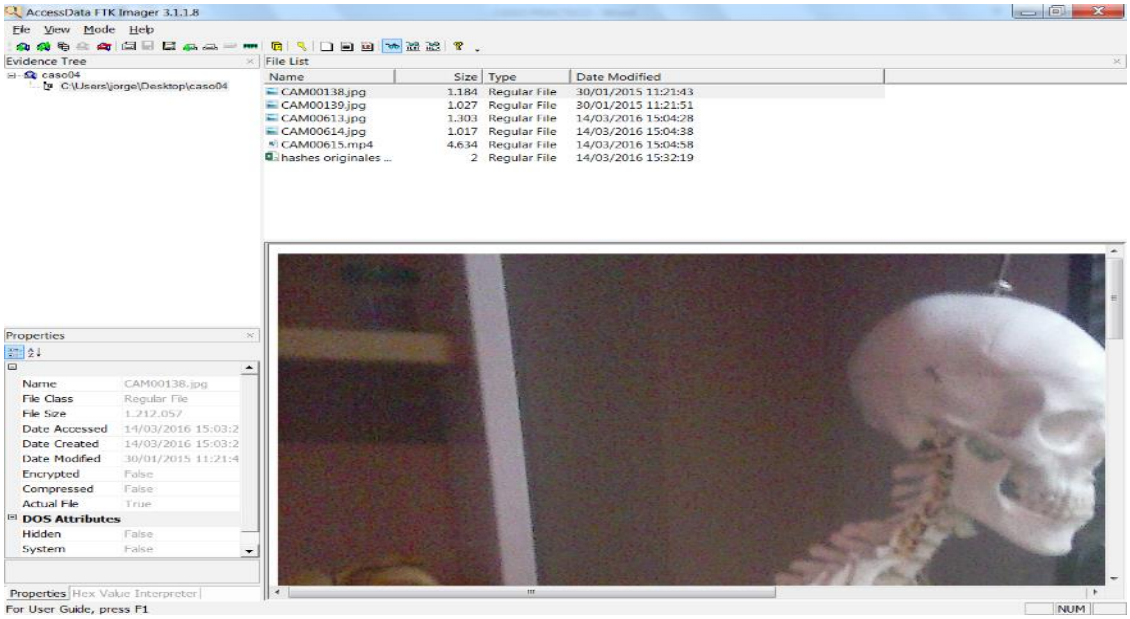


Figura 43. Crear copia forense de las pruebas originales con FTK Imager

Hash de la imagen creada pruebaoriginal.ad1 y ficheros originales con sus *hashes* (figura 44).

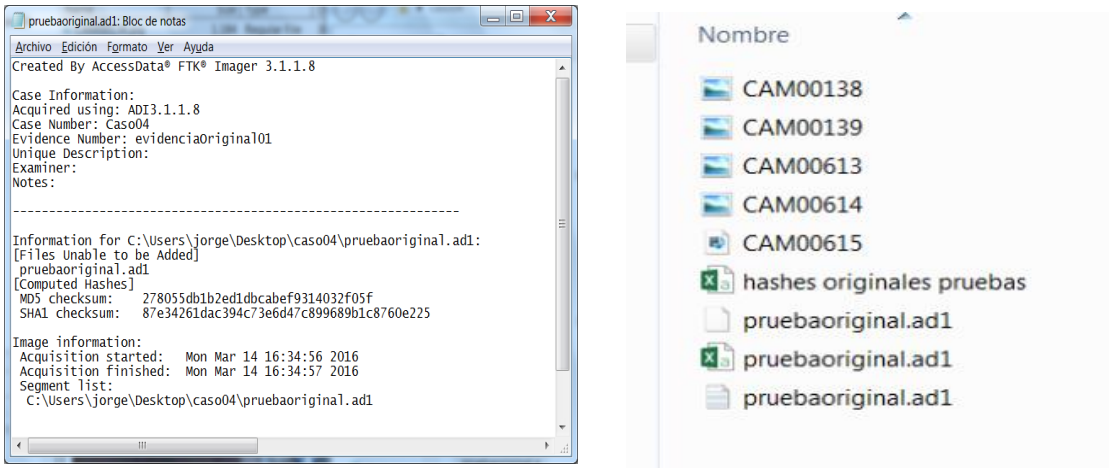


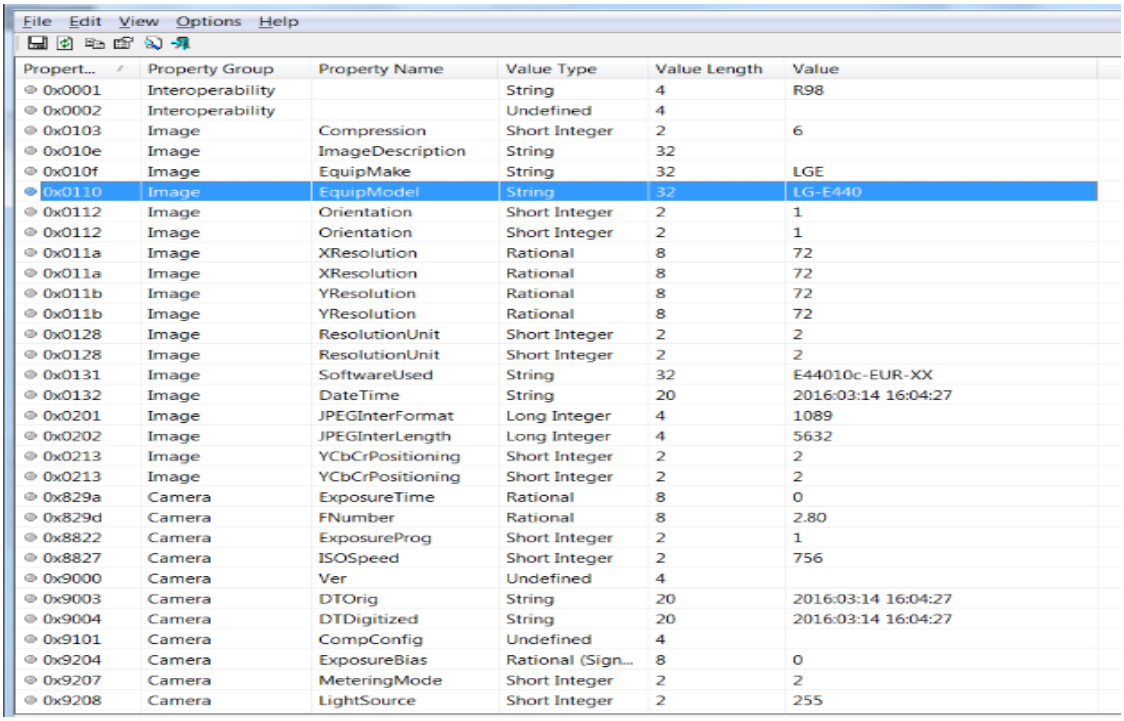
Figura 44. Hash de la imagen creada y pruebas originales.

Se comprueban los *hashes* de las dos copias para asegurar su integridad y se comprueba que coinciden. Se etiquetan con el nombre EVI01 y número de identificación de cada soporte. Se entrega una copia - CD EVI01-01- al funcionario encargado de la custodia de evidencias y se documenta. Se anota en el documento de custodia que la copia -CD EVI01-02 - se traslada al laboratorio para la investigación.

Metadatos de los archivos de prueba originales

Los metadatos nos proporcionan una valiosa información de las fotografías, como el día y hora que se realizaron, la marca y modelo del dispositivo / móvil cámara con que se hicieron y el software utilizado.

Para realizar la tarea se utiliza la herramienta portable **ExifDataView 1.2** (figura 45).


File Edit View Options Help

Propert...	Property Group	Property Name	Value Type	Value Length	Value
0x0001	Interoperability		String	4	R98
0x0002	Interoperability		Undefined	4	
0x0103	Image	Compression	Short Integer	2	6
0x010e	Image	ImageDescription	String	32	
0x010f	Image	EquipMake	String	32	LGE
0x0110	Image	EquipModel	String	32	LG-E440
0x0112	Image	Orientation	Short Integer	2	1
0x0112	Image	Orientation	Short Integer	2	1
0x011a	Image	XResolution	Rational	8	72
0x011a	Image	XResolution	Rational	8	72
0x011b	Image	YResolution	Rational	8	72
0x011b	Image	YResolution	Rational	8	72
0x0128	Image	ResolutionUnit	Short Integer	2	2
0x0128	Image	ResolutionUnit	Short Integer	2	2
0x0131	Image	SoftwareUsed	String	32	E44010c-EUR-XX
0x0132	Image	DateTime	String	20	2016:03:14 16:04:27
0x0201	Image	JPEGInterFormat	Long Integer	4	1089
0x0202	Image	JPEGInterLength	Long Integer	4	5632
0x0213	Image	YCbCrPositioning	Short Integer	2	2
0x0213	Image	YCbCrPositioning	Short Integer	2	2
0x829a	Camera	ExposureTime	Rational	8	0
0x829d	Camera	FNumber	Rational	8	2.80
0x8822	Camera	ExposureProg	Short Integer	2	1
0x8827	Camera	ISOSpeed	Short Integer	2	756
0x9000	Camera	Ver	Undefined	4	
0x9003	Camera	DTOrig	String	20	2016:03:14 16:04:27
0x9004	Camera	DTDigitized	String	20	2016:03:14 16:04:27
0x9101	Camera	CompConfig	Undefined	4	
0x9204	Camera	ExposureBias	Rational (Sign...	8	0
0x9207	Camera	MeteringMode	Short Integer	2	2
0x9208	Camera	LightSource	Short Integer	2	255

Figura 45. Metadatos de las fotografías originales

Destacar que dichas fotografías se realizaron con la cámara de un móvil marca LG modelo E400 y con el software descrito en el campo *SoftwareUsed*, en la fecha y hora mostrada en la fila *DateTime*.

Resumen de las tareas realizadas en este procedimiento

En esta tarea se han recopilado, preservado y custodiado las pruebas originales. Donde se obtienen: cuatro archivos JPG de fotografías, un archivo de video MP4 (ver más arriba) y la prueba del envío del mensaje por correo electrónico con los citados archivos adjuntos. Se obtiene además información de cuándo y con que marca y modelo de dispositivo se realizaron dichas fotografías y video. Se hace copia duplicada de todo en CD. Y se generan y anotan en el documento de cadena de custodia los hashes correspondientes a los archivos.

Herramientas forenses utilizadas en la investigación

AccessData FTK Imager v 3.1.2: para crear la copia forense de las evidencias originales y generación de *hashes*.

ExifDataView v 1.2: para obtener los metadatos de las fotografías.

Allanamiento y registro domiciliario

Se acompaña a los funcionarios, policía y secretario judicial al domicilio de la empresa de Javier para el registro e incautación de los dispositivos digitales y demás pruebas relevantes para el caso, sobre todo el dispositivo *usb pendrive* y el portátil Toshiba.

Una vez en la escena se realizarán fotografías y vídeos (figura 46) de los equipos e instalaciones asociados al procedimiento. Un funcionario requisará el *pendrive,* considerado como elemento de prueba, hallado sobre la mesa del escritorio. Se almacena en una bolsa especial aislado de campos electromagnéticos que lo puedan dañar y se identifica como **EVI02**. Se inicia la cadena de custodia y su traslado posterior al laboratorio forense para su análisis.

Figura 46. Imágenes fotográficas de la investigación de campo

Una vez identificadas las pruebas que se van a investigar y documentada la escena completa, se debe, dependiendo del escenario, actuar de una manera u otra. En este caso, en primer lugar se investigará el portátil encendido por considerarlo una prueba volátil con riesgo de pérdida de información relevante, en caso de bloqueo o corte de suministro eléctrico. Se identificará como **EVI03** en el documento de campo y en la cadena de custodia.

Adquisición en vivo de datos forenses

Este tipo de investigación forense denominada –*live forensics*- requiere herramientas software portables poco intrusivas (recordar que no se dispone de equipos hardware forense, que sería lo ideal) para la recolección de evidencias en la información volátil del sistema Windows del portátil Toshiba.

Se realizará en primer lugar una **fotografía del contenido de la pantalla** (figura 47), a ser posible que se vea la fecha y hora del sistema. Es recomendable realizar un vídeo o al menos fotografías y capturas de pantalla de todo el procedimiento de investigación y documentar cada acción realizada. Indicar que la investigación de un sistema encendido "vivo" es irrepetible por esto cuanto más documentada más fácil será su exposición y defensa.

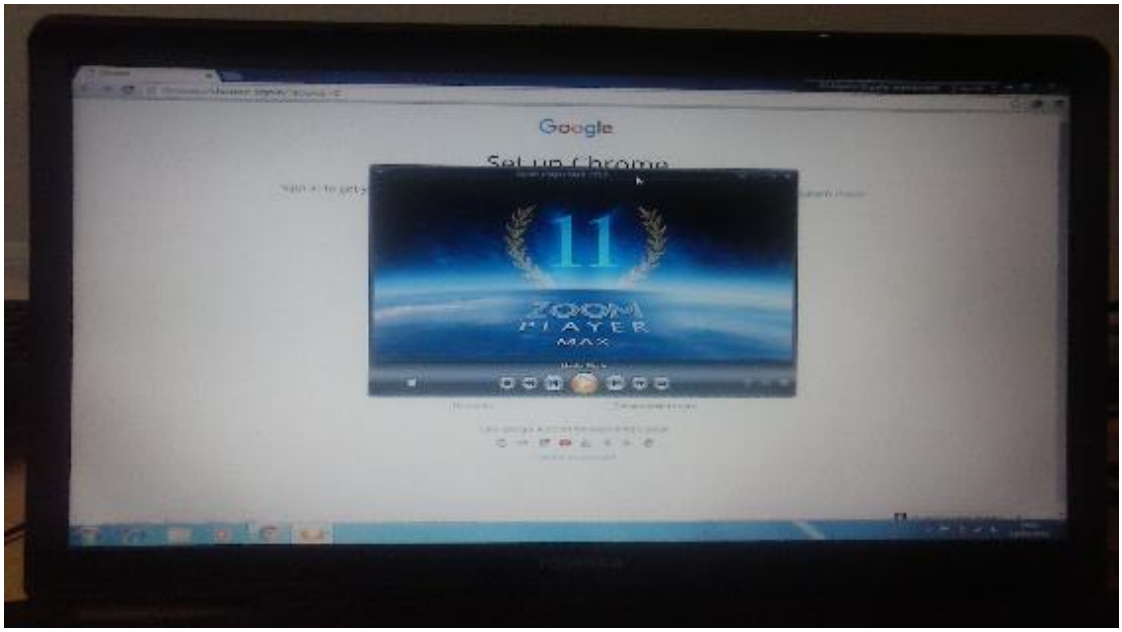


Figura 47. Imagen fotográfica del contenido de la pantalla del portátil

Para realizar la adquisición y análisis de los datos forenses volátiles se utilizan las herramientas portables forenses contenidas en el ***pendrive* de trabajo de campo** descrito en el capítulo anterior. Se protege contra escritura y se conecta al portátil Toshiba donde el sistema Windows le asigna la unidad de disco E:\.

Se **chequea todo el sistema Windows en busca virus, *malwares* y *rootkits*** que puedan perjudicar la investigación o dañar el contenido del pendrive de trabajo. Desde la Shell de Windows como administrador se ejecutan los programas **SuperAntiSpyware** (SAS) y **ClamWin** desde la carpeta E:\VIRUS Y MALWARE. En ambos casos el resultado ha sido: "**NO SE HAN ENCONTRADO AMENAZAS**".

Determinar la fecha y hora del sistema Windows

Para comprobar la diferencia horaria con respecto a la proporcionada por UTC[29] se ejecuta desde la Shell de Windows el siguiente comando:

```
# date /t  > fechayhoradeportatilEv03.txt & time /t >> fechayhoradeportatilEv03.txt
```

El archivo de salida "**fechayhoradeportatilEv03.txt"** se almacena en la carpeta de recopilación de datos forenses (E:\DATOS CASO).

La hora del portátil tiene un **adelanto de 5 minutos** respecto a UTC. Es posible que durante la investigación está información sea relevante por ejemplo si es necesario un "*time line*" o para determinar la fecha y hora exacta de sucesos.

---

[29] **UTC** (Tiempo Universal Coordinado) principal estándar de tiempo por el cual el mundo regula sus relojes y tiempo. Enlace ver UTC http://www.worldtimeserver.com/hora-exacta-UTC.aspx.
Indicar que nuestra zona horaria corresponde al Horario Europeo Central UTC+1 y en verano UTC+2.

Seguidamente, se obtiene el *hash* del fichero de salida y se anota en el documento de cadena de custodia.

Para obtener los *hashes*, si no se indica lo contrario, se utilizará durante todo el desarrollo del caso la utilidad **HashMyFiles.** Este programa genera los hashes MD-5, SHA1, SHA-256, SHA-384 y SHA-512 proporcionando mayor validez a las pruebas recopiladas (figura 48).

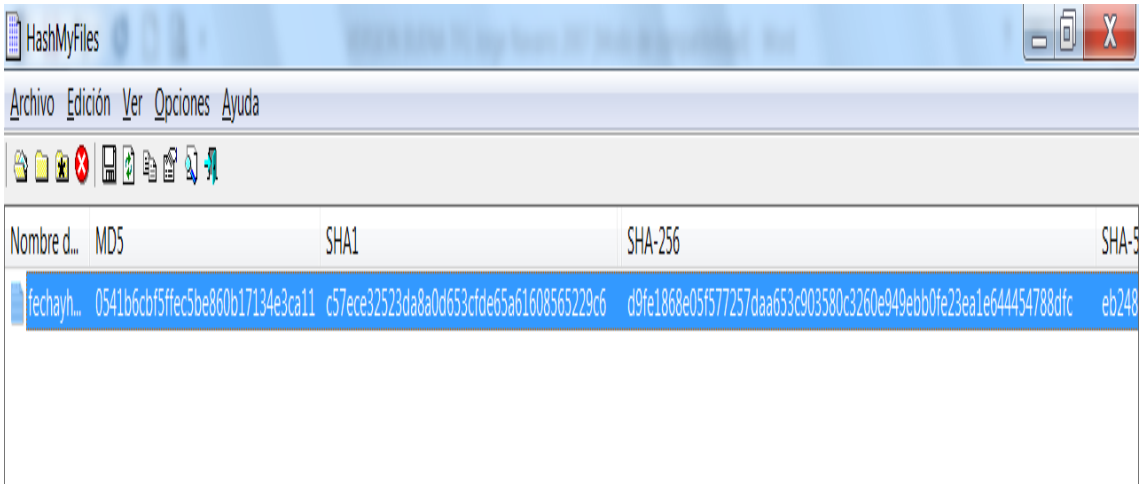


Figura 48. Hashes *generados con la utilidad HashMyFiles*

Seguidamente, se procede a adquirir la información forense volátil en orden de más a menos volatilidad, de acuerdo a la recomendación de las normas aplicadas en la investigación.

Apuntar que, la información de la memoria de un sistema Windows se encuentra en la propia RAM -memoria física- y en el fichero de intercambio "*pagefile.sys*" -memoria virtual-. En nuestro caso se adquiere solamente la memoria física –RAM- puesto que el fichero "*pagefile*" está almacenado en el disco duro y puede ser analizado posteriormente en el laboratorio.

Adquisición de la información almacenada en la memoria RAM

La información forense contenida en la memoria RAM es importante sobre todo, para obtener contraseñas de discos o archivos cifrados, procesos en ejecución, conexiones establecidas, contraseñas de correo electrónico u otros accesos web autenticados.

Mediante la versión portable del programa **AccessData FTK Imager** se realiza la captura de la memoria RAM a fichero, se crea la imagen forense y se calculan los *hashes*, todo ello en el mismo proceso. En la ventana siguiente se elige la carpeta de destino, el nombre del fichero de volcado ".mem", la opción incluir *pagefile* (desmarcar) y crear la imagen (marcar) según se muestra en la figura 49.

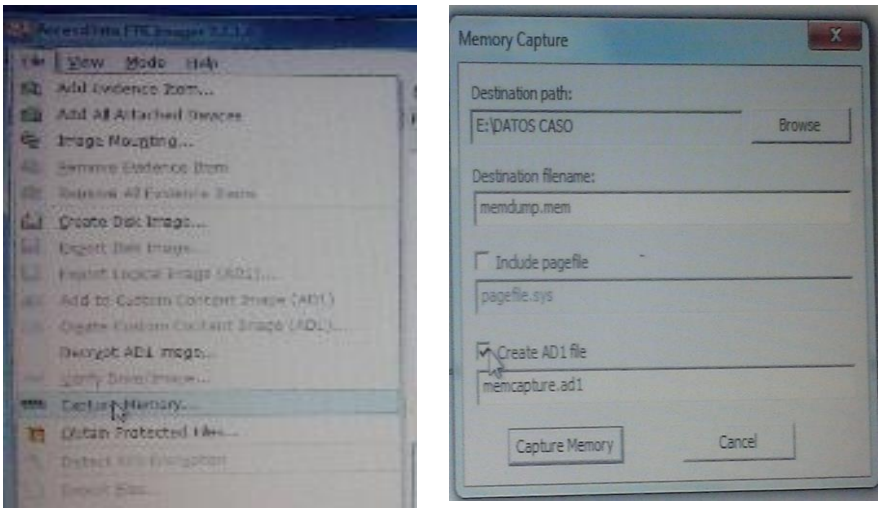


Figura 49. Volcado de memoria RAM con AccessData FTK Imager

Una vez obtenida la imagen correspondiente al volcado de memoria física se genera su *hash* correspondiente y se anota en el documento de cadena de custodia.

Hash

Nombre de archivo: **memcapture.ad1**

Ruta completa : E:\DATOS CASO\memcapture.ad1
MD5 : 8a42eeb99be91ec88bbf02a55fee991c
SHA1 : 8c016a8eb6ec600e79058330155f62c0a3e8c43c
CRC32 : 1cbf12e5
SHA-256 : 65e5ee3b78e5b703729cbc040902bd1998c2a2ae0a7258987ee7b7e9e76075f3
SHA-512 :
5dc1784a2b23571923c059c8f029634ded8999f7f1c6e5b19e991d4d7ec3f3a975a1402ee1b3a5d340f5a690534ecbd79f
57baecc7eac7f7a1766695d7ef0a6d
SHA-384 :
b0c456f339d59854ca025a017a628f450538fab749ae070190fd044db619a946a2af2343f0144efeffe1e461f665cab5
Extensión : ad1
Atributos del archivo: R

Adquisición del resto de información volátil del portátil

Una manera de realizar esta tarea de forma rápida, eficaz, segura y poco intrusiva es mediante una utilidad que ejecute un proceso *batch* con todas las herramientas forenses de adquisición que consideremos apropiadas para el tipo de investigación.

Se ha decidido escoger la herramienta **Investigador 2.0**, idónea para la recolección automática de evidencias digitales en sistemas Windows encendidos. Desarrollada por ingeniero del Laboratorio Pericial Informático - Neuquen - Argentina.

Fuente [En línea] http://www.informaticapericial.com.ar

Este software utiliza aplicaciones gratuitas para realizar la recolección de información digital forense asociada a un equipo informático (figura 50).

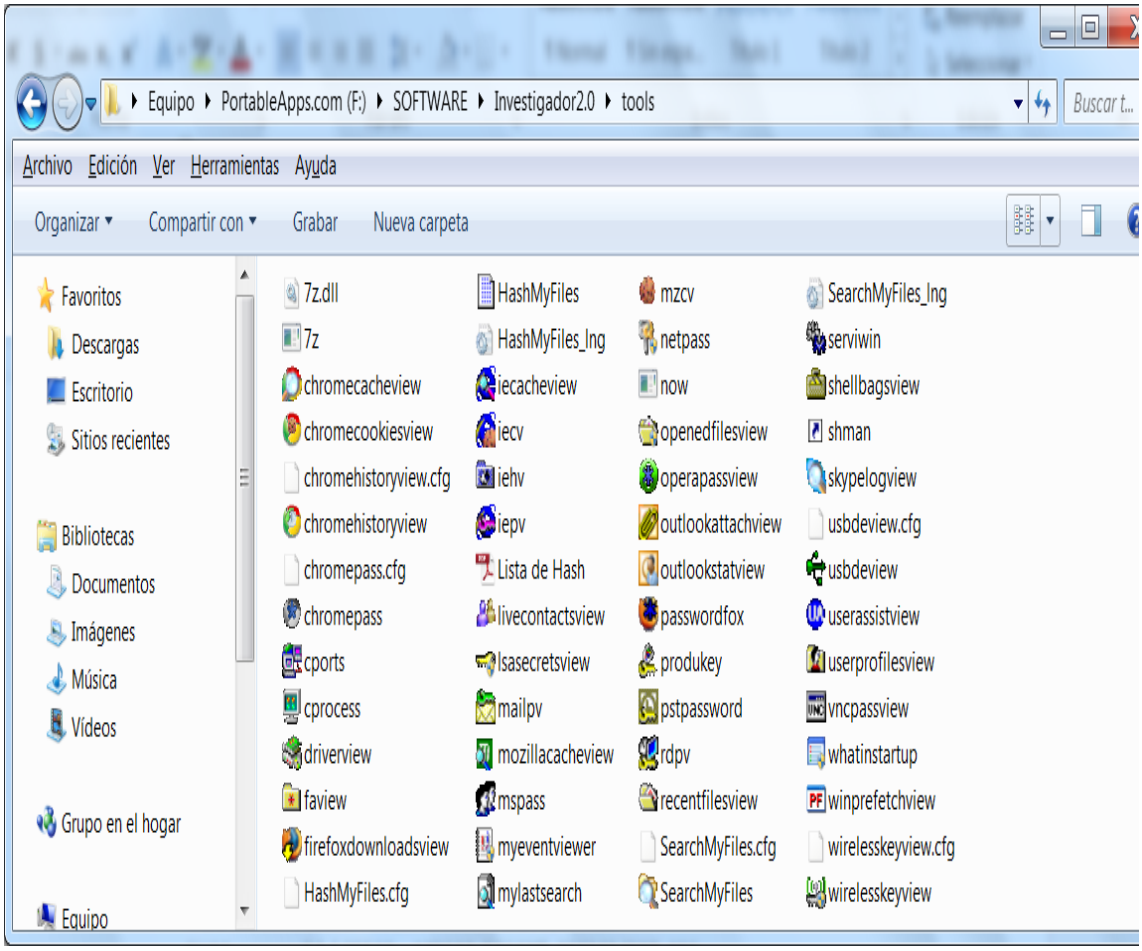


Figura 50. Herramientas y utilidades incluidas en Investigador 2.0

Para lanzar el proceso como administrador, desde la Shell de Windows, ir al directorio E:\SOFTWARE\Investigador2.0 y ejecutar la aplicación INVESTIGADOR. Puede demorar varios minutos. No se debe cancelar ni cerrar las ventanas emergentes que la aplicación vaya desplegando.

Los resultados son guardados dentro del mismo dispositivo y carpeta desde el que se ejecuta el software. Asimismo, el software Investigador crea una carpeta comprimida con todos los archivos resultantes de la inspección digital automatizada y un fichero de texto con los *hashes*.

Al lanzar la aplicación aparece una ventana con varios menús de pestañas con casillas de verificación para seleccionar la información a recopilar según el tipo de caso a investigar (figura 51). Es aconsejable marcar la casilla “Abrir Report” para que nos muestre los resultados una vez terminado el proceso. Finalmente pulsamos el botón EJECUTAR.

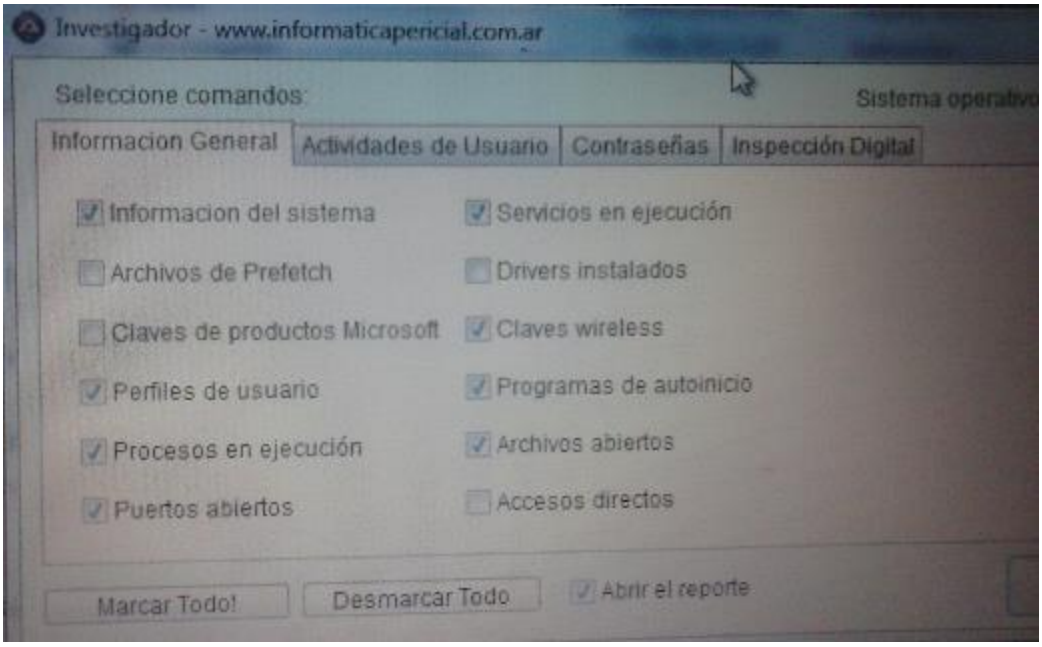


Figura 51. Investigador 2.0 para recolección automática evidencias en Windows

La aplicación genera una estructura (figura 52) de carpetas y archivos con la intención de crear posteriormente un DVD *Autorun* para navegar por los resultados obtenidos. Destacar el archivo de resultados comprimido y el fichero *hashes* generado. En la figura 53 se muestran los archivos que contienen la información forense a analizar en busca de las evidencias requeridas.

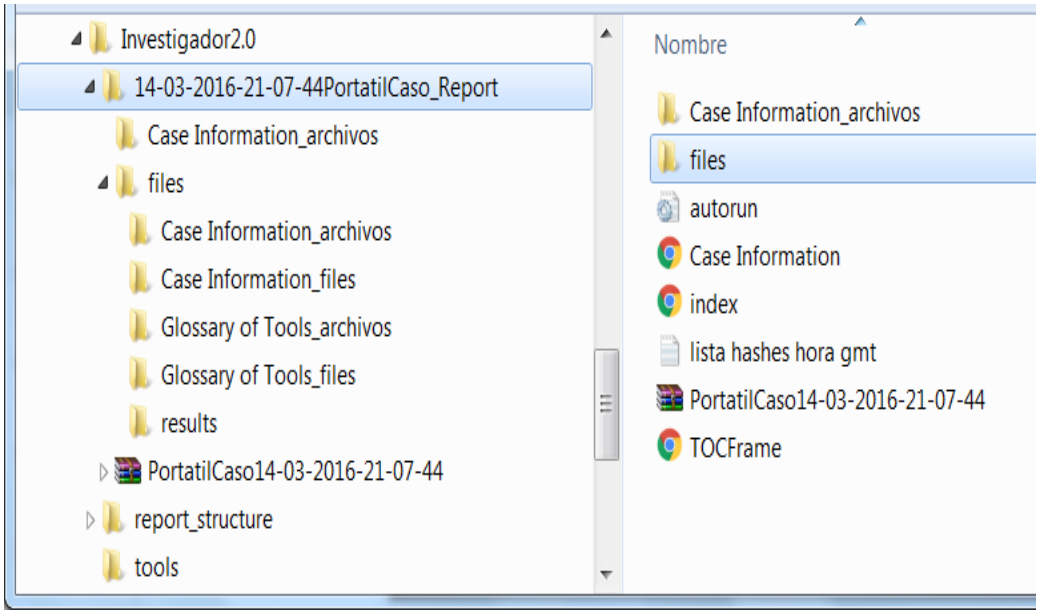


Figura 52. Investigador 2.0 estructura carpetas de resultados del análisis

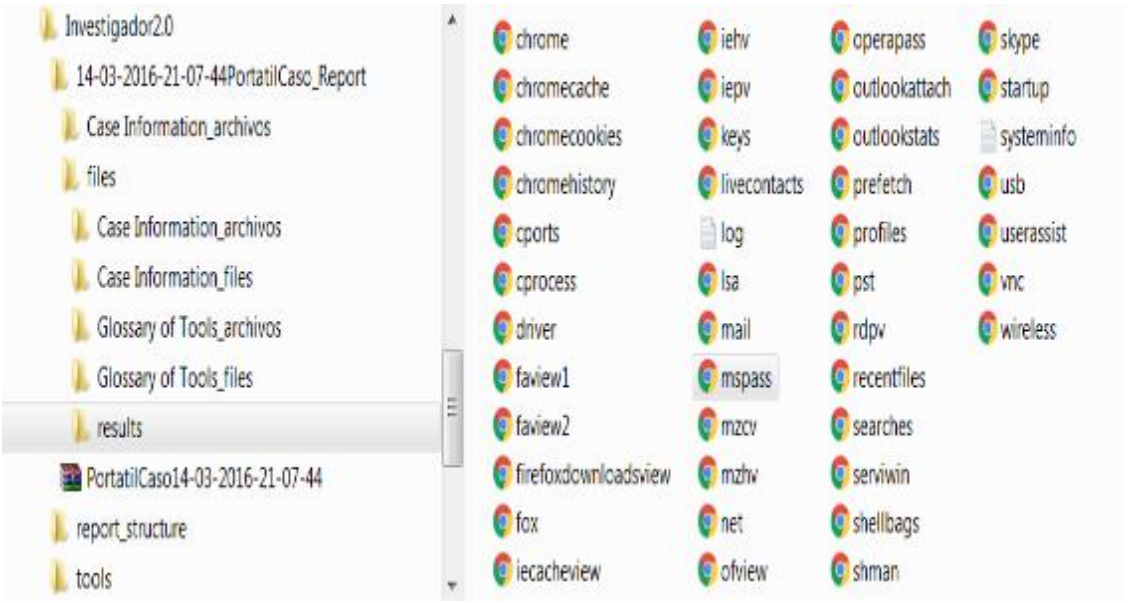


Figura 53. Archivos forenses generados por cada utilidad seleccionada en Investigador 2.0

Una vez finalizado el proceso de adquisición de datos forenses, y antes de navegar por los resultados obtenidos, se realizarán dos copias en *DVD* con el contenido de la carpeta de salida generada en este apartado (ver figura 52) y la imagen de captura de memoria RAM "**memcapture.ad1** ..." del aparado anterior. Se identifican los *DVDs* como **EVI03-1 / EVI03-2** y se preparan para su traslado. Junto con los hashes generados se anotan las evidencias en el documento de cadena de custodia donde se especifica que una copia debe ir al laboratorio forense para ser analizada. Y finalmente, se documenta la investigación con los pasos realizados y la secuencia fotográfica / video realizada.

Resumen de las tareas realizadas en este procedimiento

En primer lugar se analiza el sistema en busca de amenazas (virus, *malware*, *rootkits*, etc). Seguidamente, se comprueba el desfase horario de Windows respecto a UTC y se realiza la imagen forense del volcado de la memoria RAM. Para finalizar con la recopilación y adquisición del resto de información volátil de Windows (logs, procesos, información del sistema, caches de navegación, contraseñas, datos de red, etc).

Copia en DVD por duplicado de los datos adquiridos. Documentación del proceso añadiendo fotografías y videos así como cumplimentar la información en las hojas de cadena de custodia.

Herramientas forenses utilizadas

Análisis en busca de posibles amenazas: **SAS** y **WinClam**

Imagen de volcado de la memoria RAM: **AccessData FTK Imager**

Adquisición de información volátil de Windows: **Investigador 2.0** (conjunto de utilidades forenses). En la fase de análisis se detalla cada herramienta ejecutada y su cometido en la investigación.

Generación de hashes: **HashMyFile**

Una vez adquirida toda la información volátil del portátil se debe desconectar del suministro eléctrico de forma "brusca", tirando del cable, o sea, no apagar de manera ordenada. Así nos aseguramos que durante el proceso de apagado no se ejecute ningún programa oculto que pueda alterar la información de los dispositivos de almacenamiento. Una vez apagado el portátil se precintará, identificará y se preservará para su traslado al laboratorio por si fuera necesario y a requerimiento judicial realizar el análisis forense de sus discos duros.

Análisis en laboratorio de las evidencias recopiladas

Una vez en el laboratorio forense se procede con la fase de análisis en busca de las evidencias requeridas en el expediente judicial.

Pruebas recopiladas en la fase de adquisición:

1. EVI01 pruebas originales (fotografías, vídeo y mensaje de correo).
2. EVI02 pendrive *usb* requisado en el registro domiciliario.
3. EVI03 información volátil del portátil Toshiba (volcado de la memoria RAM y resto de datos del sistema Windows).

A continuación se solicitan las pruebas –evidencias a analizar- al funcionario encargado, se actualiza la información en el documento de cadena de custodia, se planifica el proceso de investigación y se prepara el entorno de trabajo.

Se comenzará realizando la adquisición y preservación de la información forense del *pendrive* EVI02 para su posterior análisis en búsqueda de evidencias.

Posteriormente, se analizará la información volátil del sistema operativo Windows del portátil Toshiba adquirida durante el registro domiciliario y preservada en el DVD EVI03.

Adquisición de datos y análisis forense del pendrive - EVI02

Para realizar la investigación de un dispositivo *usb* de almacenamiento es necesario utilizar un sistema que no altere ni contamine la información del mismo cuando se conecta a la estación forense. Para ello, se utiliza la distribución *Live GNU/Linux Ubuntu* de Caine 7.0, que monta sus dispositivos automáticamente en modo lectura.

En primer lugar se ejecuta VirtualBox y se arranca la máquina virtual Caine 7. Una vez aparece el escritorio de Caine se introduce al pendrive EVI02 y se monta el dispositivo (doble clic). El sistema le asigna el nombre **USB 2.0 Flash Drive 2,1 Gb Volume** en **/dev/sdb** (figura 54). Se comprueba que realmente solo tiene permisos de lectura.

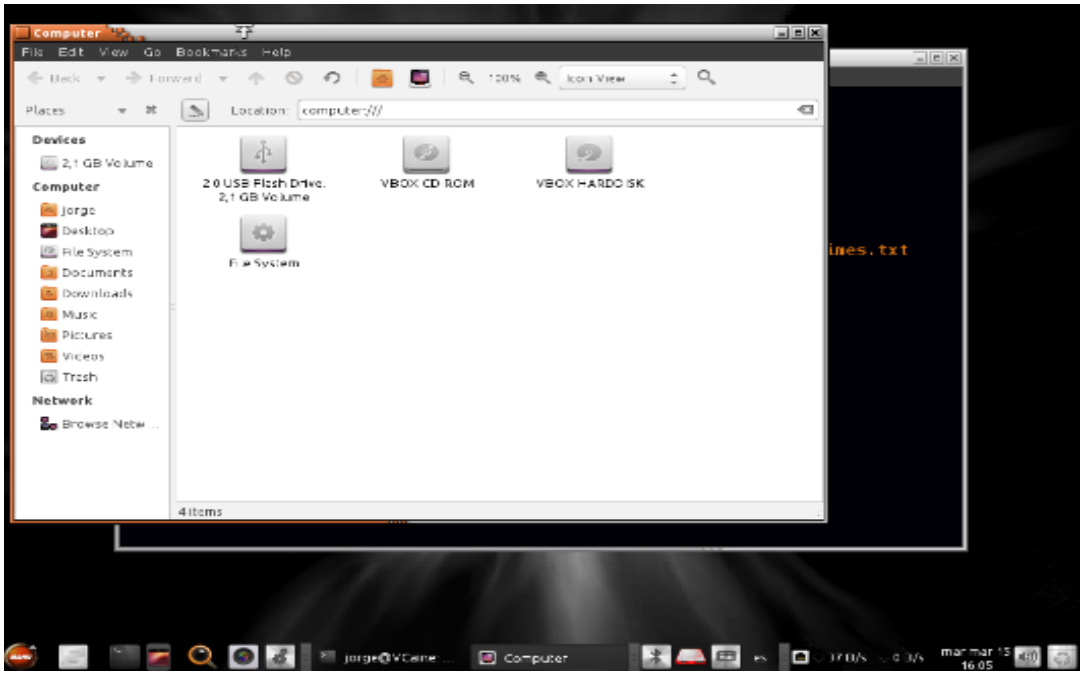


Figura 54. Pendrive EVI02 listo para crear su copia / imagen forense

Lo primero que se debe hacer es crear la imagen forense del dispositivo requisado como EVI02, utilizando la herramienta **GUYMAGER** (figura 55) para adquisición de imágenes forenses. Esta herramienta gráfica permite crear en un solo proceso dos copias de imágenes forenses en distintos formatos –dd, raw, ev, ad..- del mismo dispositivo, una para trabajar y la otra como *backup*.

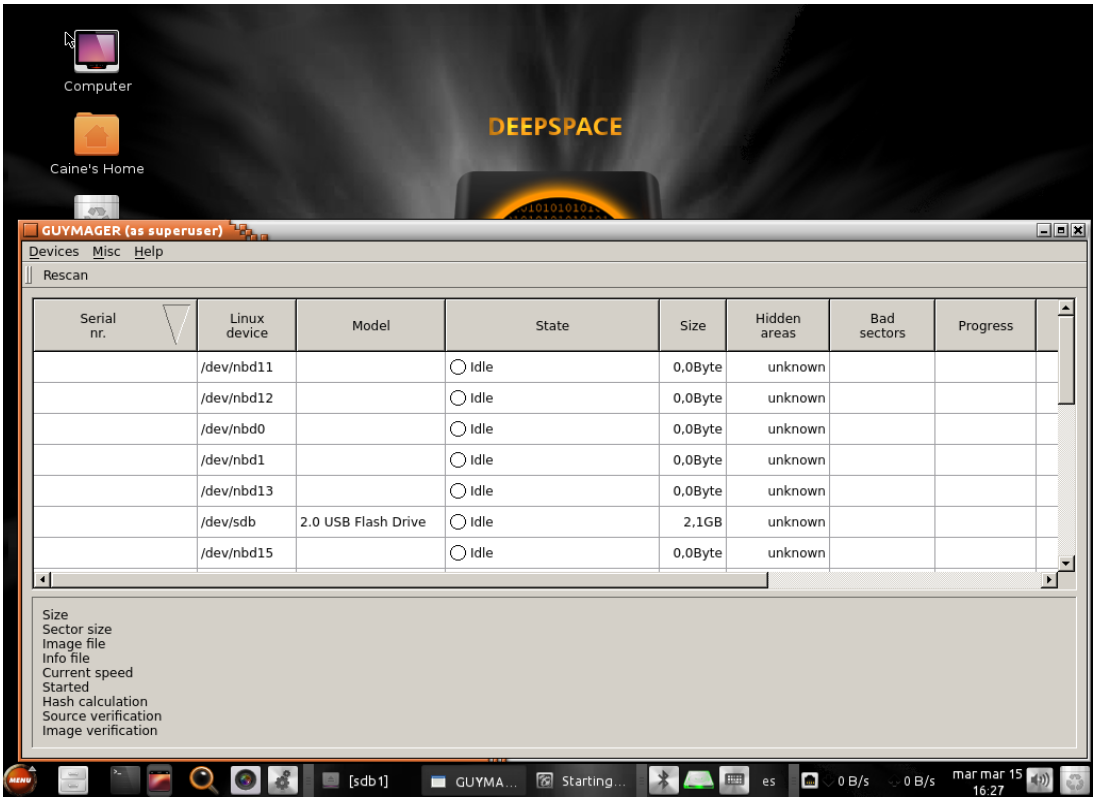


Figura 55. GuyMager para crear doble copia de imagen forense del pendrive

Las imágenes se crearán con el nombre **evidencia02** en los directorios (figura 56):

/home/jorge/Documents/Caso
/Copia
/CopiaTrabajar

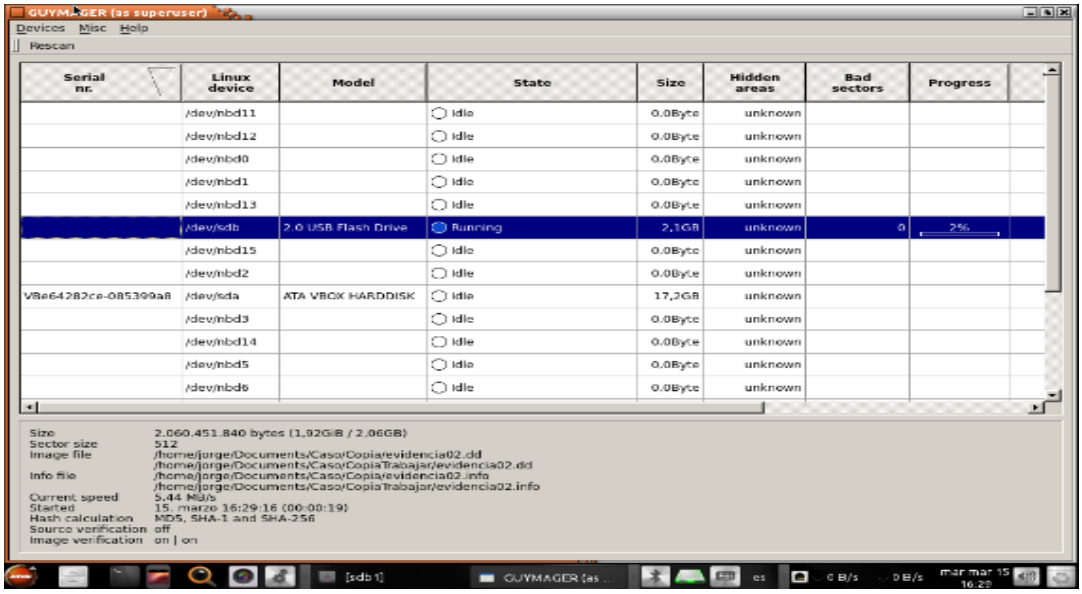


Figura 56. GuyMager ejecutando la copia/imagen del pendrive

Una vez creada la imagen forense del pendrive se debe comprobar los *hashes* correspondientes antes de continuar con la investigación. Si no coincidieran se debería repetir el proceso.

Se utiliza la herramienta **QuickHash** que tienen la facilidad de comparar los *hashes* de dos archivos y mostrar el resultado obtenido (figura 57). Se oberva que el resultado obtenido el CORRECTO.

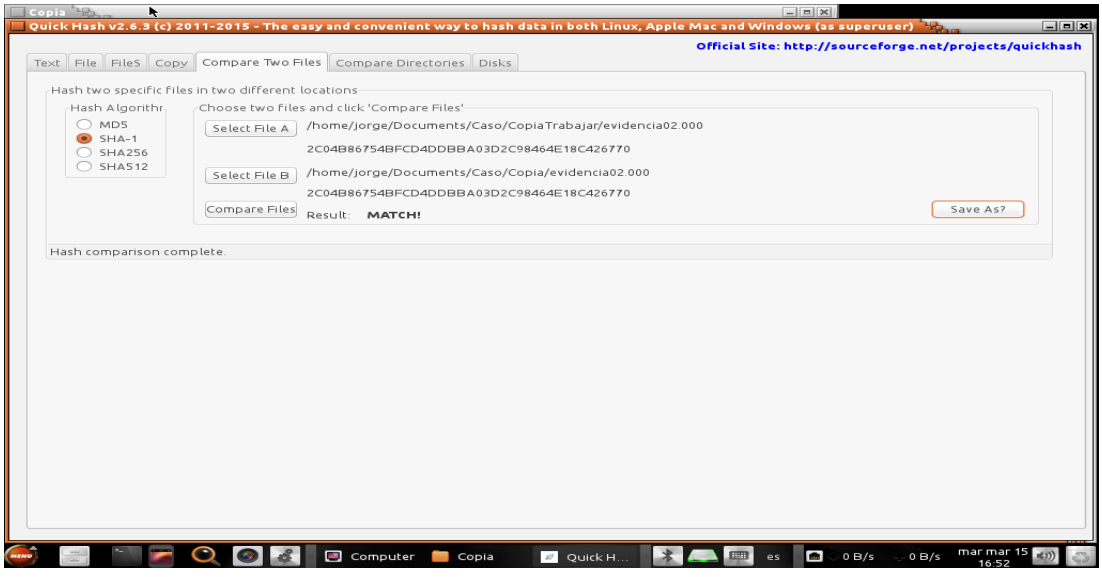


Figura 57. QuickHash para comparar hashes de ambas imágenes creadas

Ahora se procede a desmontar el pendrive para preservar su información y devolver al almacén actualizando el documento de la cadena de custodia. Seguidamente, se copia el resultado de los *hashes* al documento de investigación junto con el nombre de las imágenes creadas.

Seguidamente, se cambia los permisos a modo solo lectura –*AccessData*- los directorios .../Copia y ... /CopiaTrabajar para asegurar que durante la investigación no se alteren las imágenes forenses.

Para asegurar todavía más la imagen forense –evidencia02.000- se realiza una copia a DVD utilizando la herramienta de Linux Ubuntu **Brasero** (figura 58). Para poder utilizar el DVD en el sistema operativo Windows debe estar activada la opción *Joliet*. Se etiqueta con identificador **DVD EVI02** y se realiza el *hash* para anotarlo en el documento de la cadena de custodia.

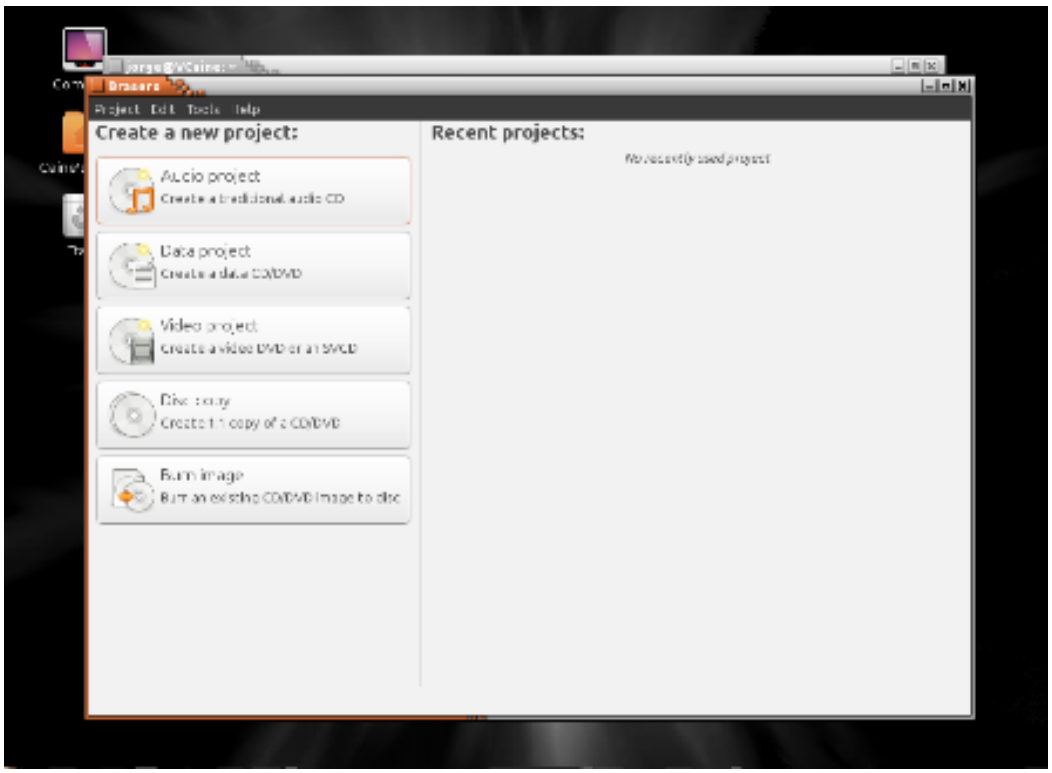


Figura 58. Brasero para crear DVD EVI02 (Joliet) con la imagen evidencia02

A partir de este momento ya estamos listos para comenzar el análisis forense de la imagen "evidencia02.000" del directorio .../CopiaTrabajar.

En primer lugar con la herramienta **Autopsy** creamos un nuevo caso (figura 59) para realizar el análisis en busca de evidencias, archivos de fotografías y vídeo aportados como prueba original a la investigación. Se añade un *host* y se crea la imagen forense a partir de la imagen "evidencia02.000", se observa como Autopsy ha reconocido que se trata de un disco con formato de sistema de ficheros FAT32 (figura 60).

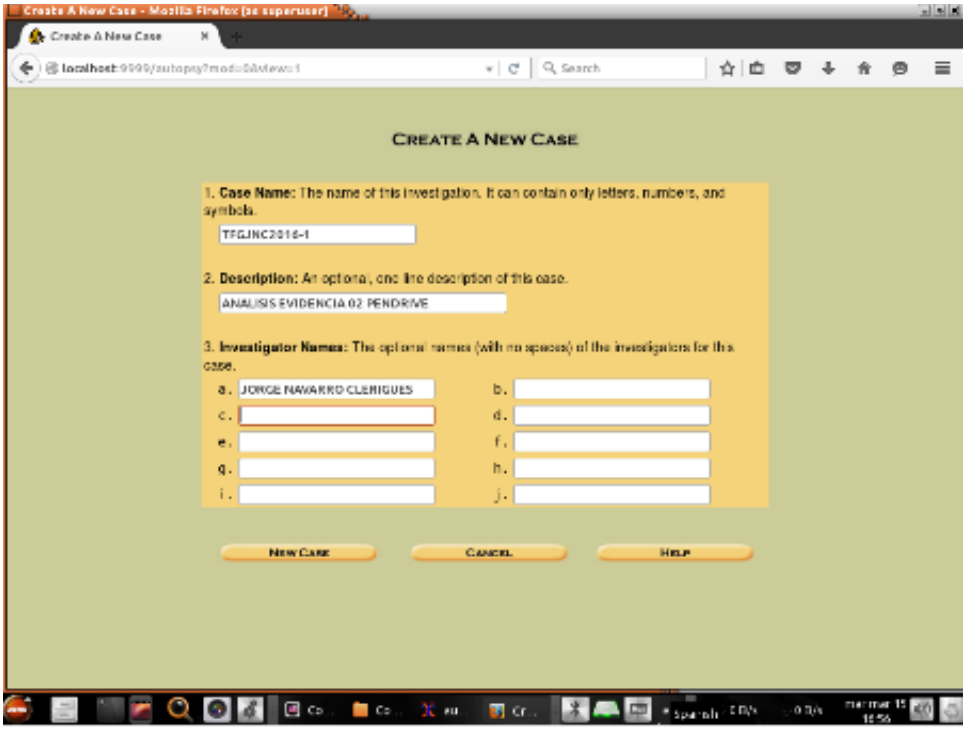


Figura 59. Crear un nuevo caso con Autopsy de Caine 7.0

En la figura 60 se muestran los detalles de la imagen forense realizada del pendrive. Seguidamente pulsar ADD para elegir el volumen y comenzar el análisis pulsando botón ANALYZE (figura 61).

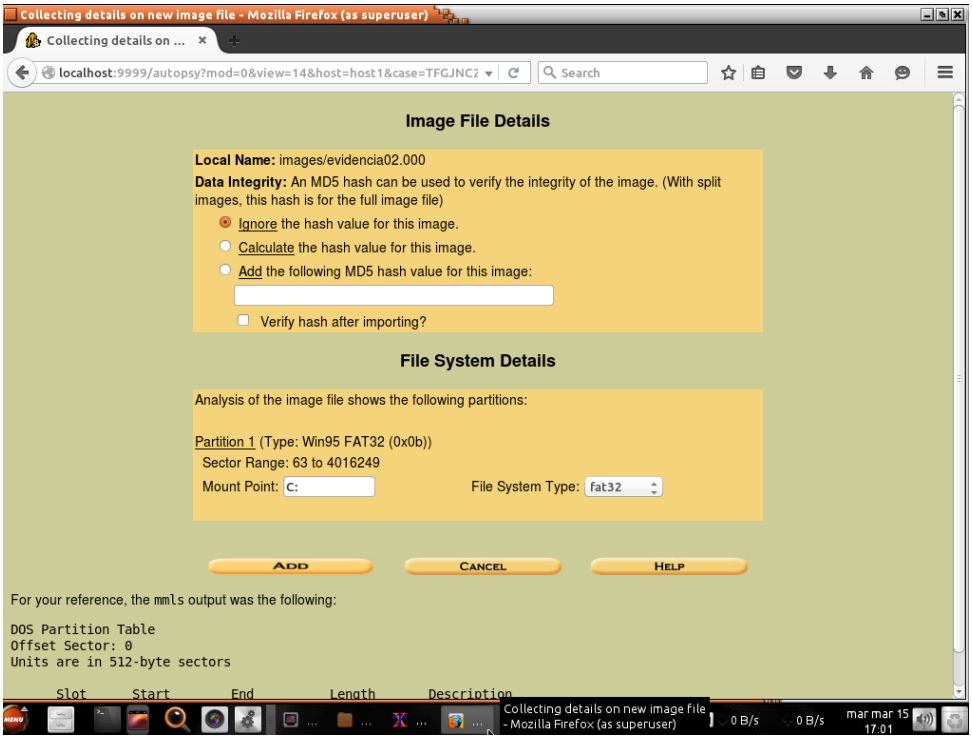


Figura 60. Autopsy. Añadir nueva imagen al caso.

Figura 61. Autopsy. Seleccionar volumen a analizar

El análisis con Autposy nos revela que el pendrive no contiene ningún archivo. Se muestran las carpetas ocultas del sistema de archivos y la carpeta de archivos borrados $OrphanFiles/. La columna META nos proporciona información de los metadatos de cada directorio así como sus hashes correspondientes (figura 62)

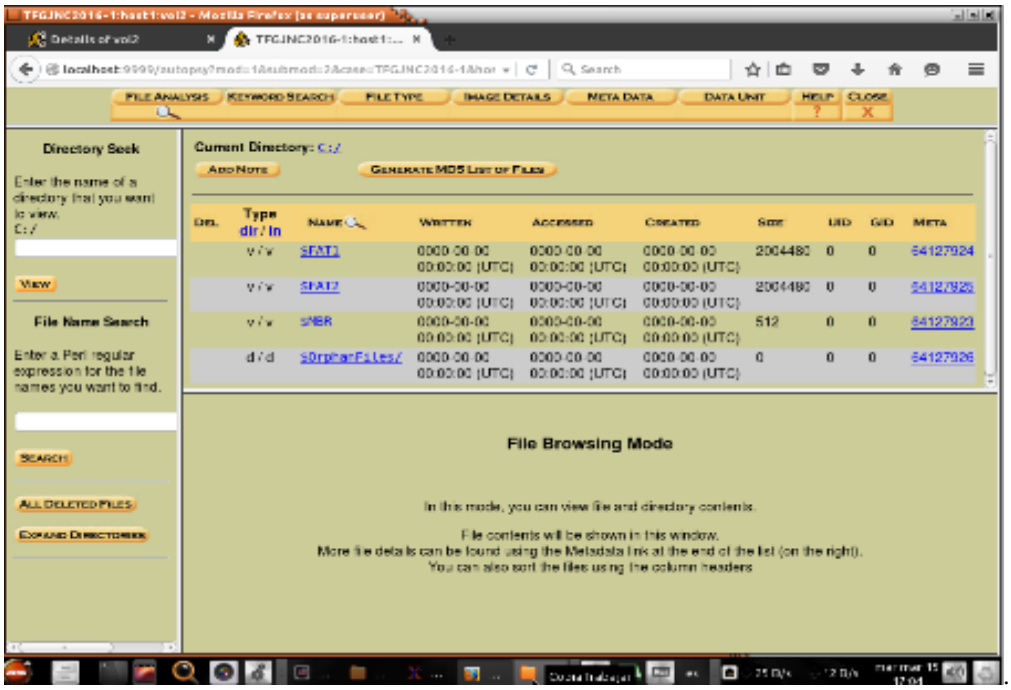


Figura 62. Autopsy. Resultado del análisis de ficheros

Para la búsqueda evidencias, en **File Name Search** escribimos el nombre de algún archivo de fotografía por ejemplo: “CAM” y pulsamos el botón SEARCH. No encuentra ningún archivo. Intentamos con otra expresión por ejemplo: “JPG” y nos devuelve una lista de archivos borrados extensión JPG (figura 63). Lo mismo ocurre al pulsar el botón “ALL DELETED FILES”, nos devuelve la lista completa de archivos eliminados.

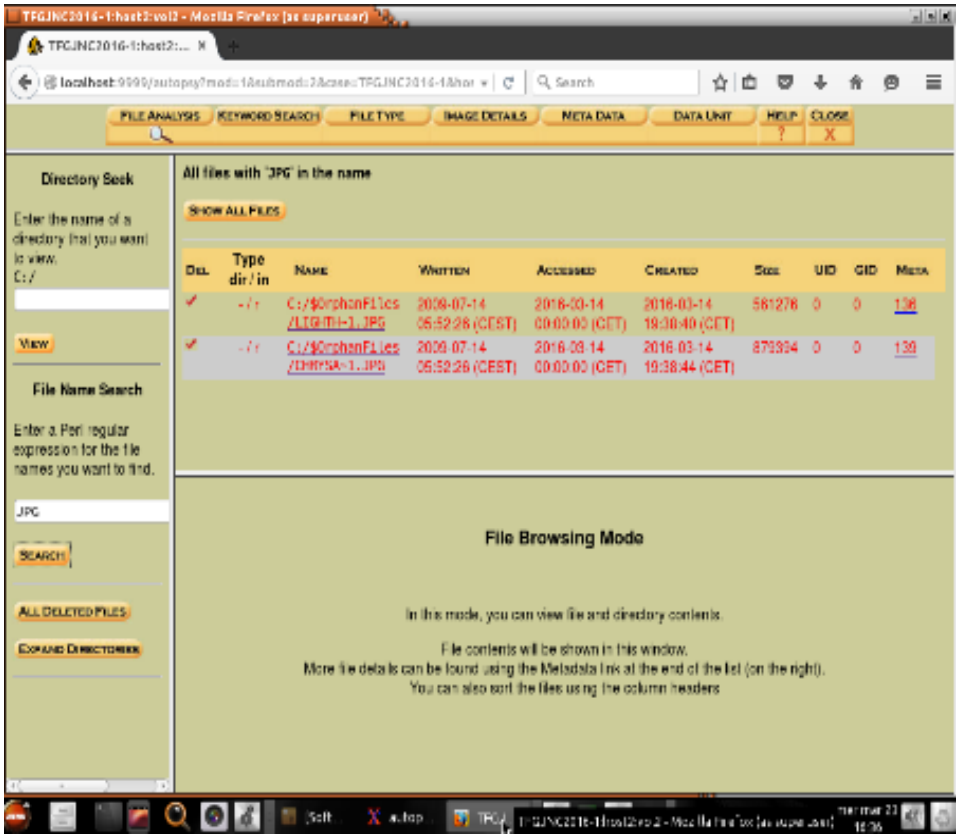


Figura 63. Autopsy. Archivos borrados del pendrive.

Ni el nombre, ni contenido, ni *hash* de los archivos hallados corresponden con las fotografías y video que se buscan.

Autopsy no aporta evidencias probatorias que demuestren que las pruebas originales –fotografías y vídeo- han sido almacenadas o eliminadas del pendrive alguna vez. Se determina que el pendrive no contiene archivos visibles porque ha sido formateado o borrado mediante otra técnica. Los archivos hallados (figura 63) fueron borrados antes de formatear el dispositivo *usb* pero no corresponden con los buscados en la investigación.

En estos casos, se debe documentar todo el proceso realizado y utilizar otras herramientas de análisis de datos en "bruto" –que no tengan en cuenta el tipo de sistema de ficheros del volumen a analizar- como por ejemplo, **Bulk Extractor Viewer** que posee, entre otros, un módulo para técnicas *caring*[26] *en archivos JPG.*

Seguidamente, se realiza el análisis forense de la imagen "evidencia02.000" con la herramienta **Bulk Extractor Viewer** 1.5.5 como muestra la figura 64.

Ir a menú Tools -> Run Bulk Extractor … aparece una ventana donde seleccionamos la imagen a analizar, dejar por defecto los módulos que van ejecutarse durante el análisis (mails, jpg, urls, zip, hiberfile, etc) e introducir los nombres de las imágenes Copia y CopiaTrabajar para comprobar los *hashes* automáticamente después del análisis de datos.

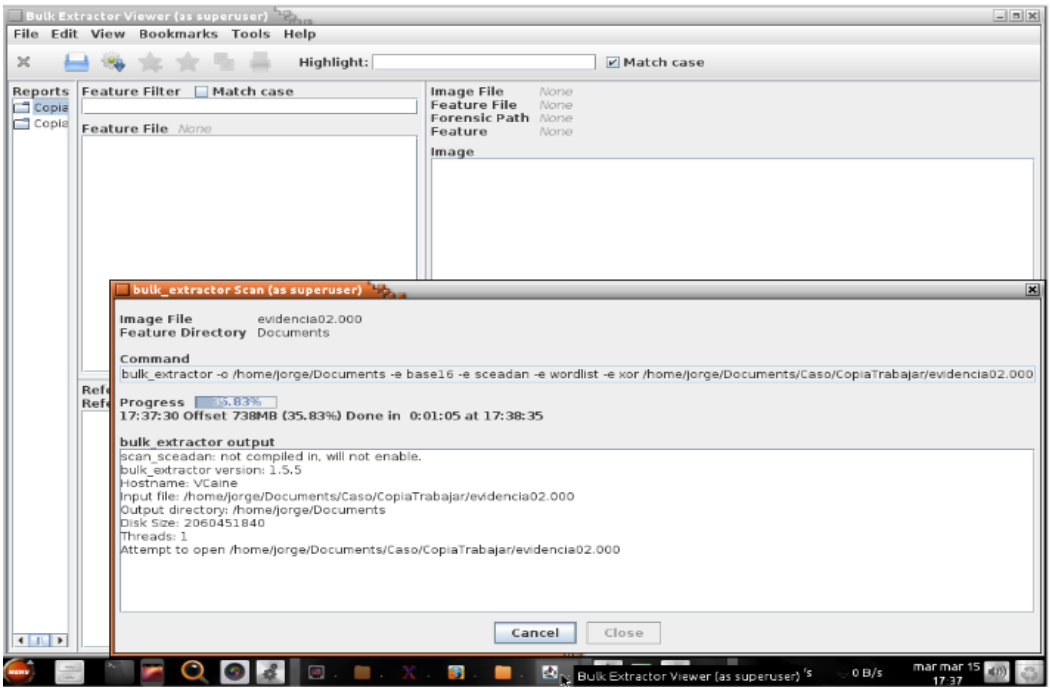


Figura 64. Bulk Extractor Viewer (BE Viewer) para análisis en bruto

Bulk Extractor Viewer genera varios *reports* de texto con los resultados obtenidos en el directorio */home/jorge/Documents* y un directorio con los archivos *jpg* hallados.

exif.txt

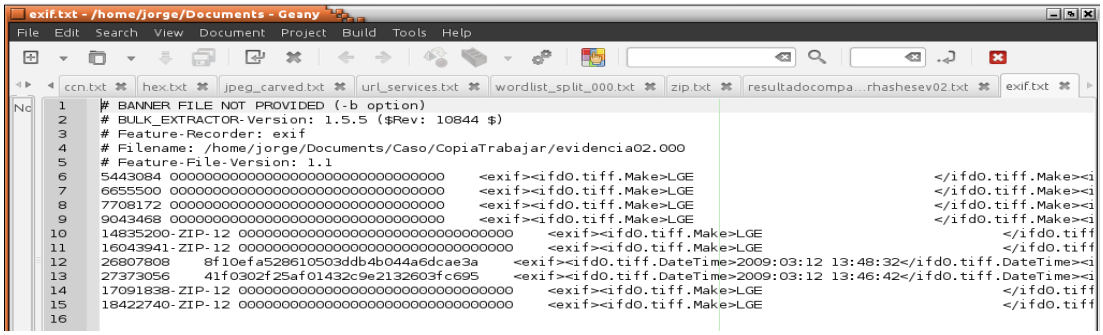


Figura 65. BE Viewer. Resultado de Exif - metadatos

zip.txt

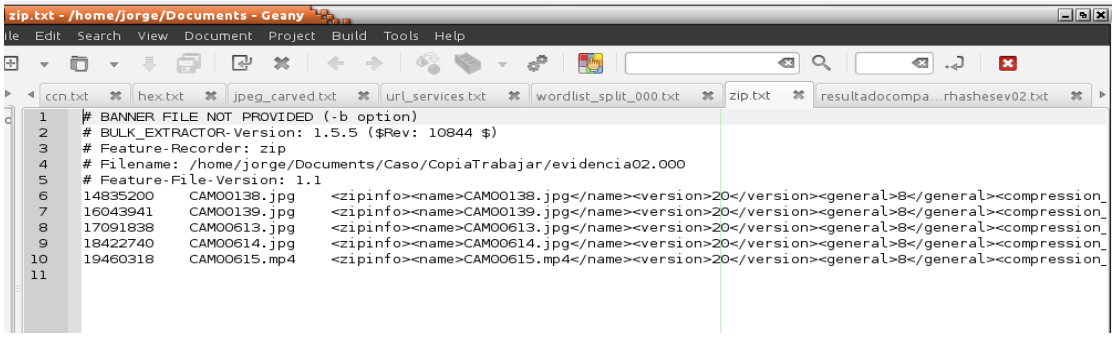


Figura 66. BE Viewer. Resultados de archivos ZIP encontrados

resultadocompararhashesev02.txt

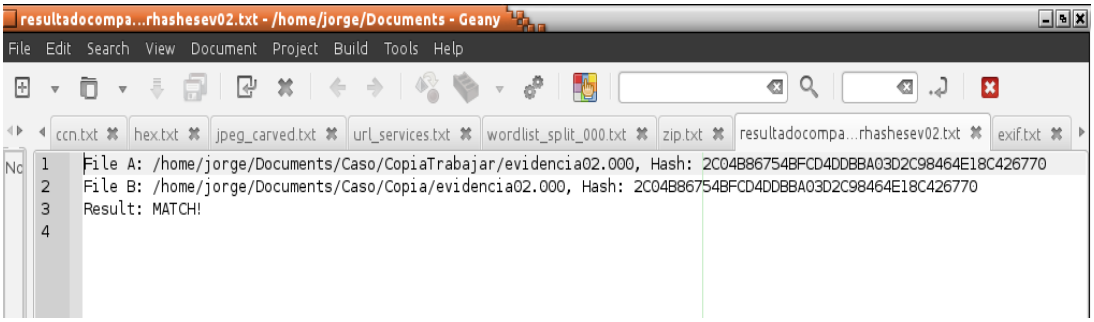


Figura 67. BE Viewer. Resultado de comparativa de hashes de imágenes forenses

En la figura 68 se muestra el contenido del archivo ZIP recuperado, con las cuatro fotografías y el vídeo.

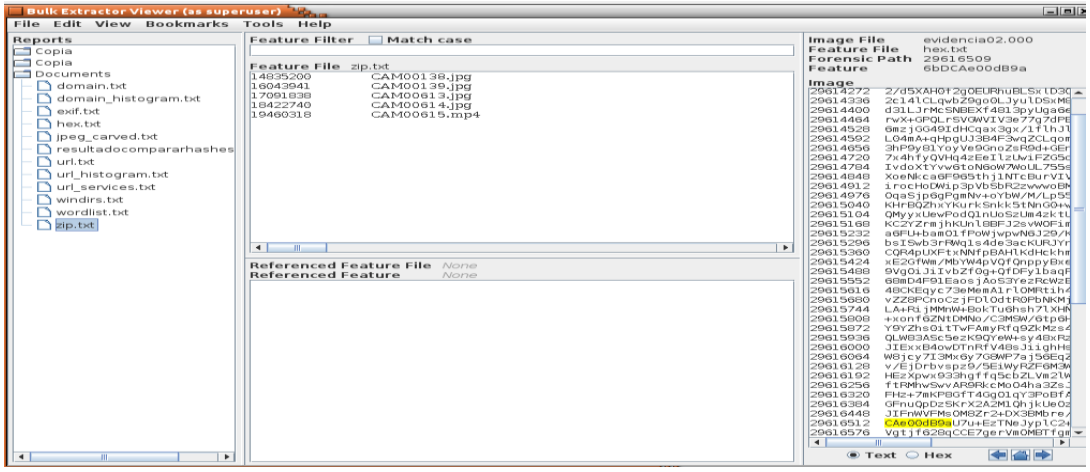


Figura 68. BE Viewer contenido archivo ZIP recuperado.

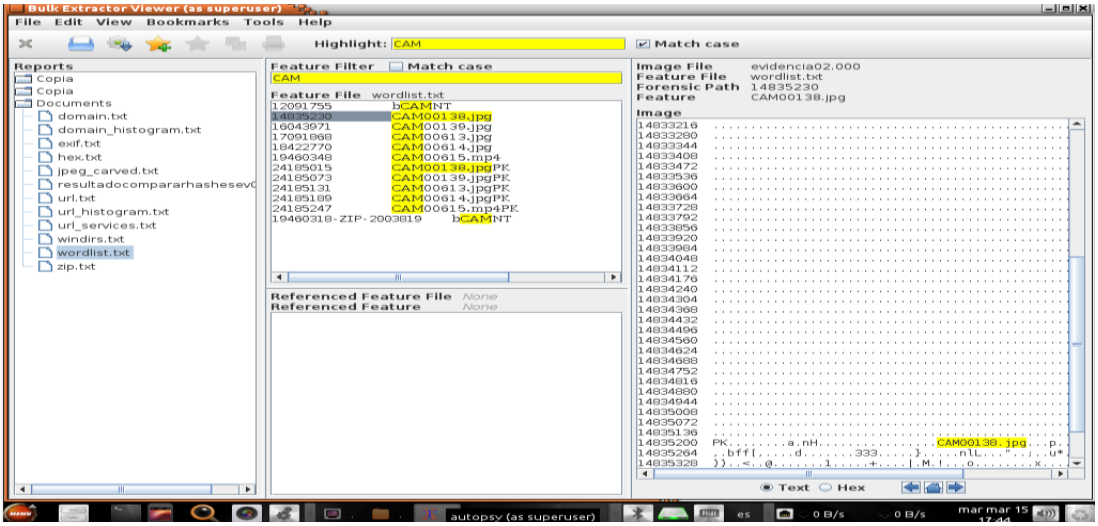


Figura 69. BE Viewer. Ficheros recuperados -wordlist

En la figura 70 se muestra el contenido del directorio "…/jpeg_carved/000" con las fotografías recuperadas.

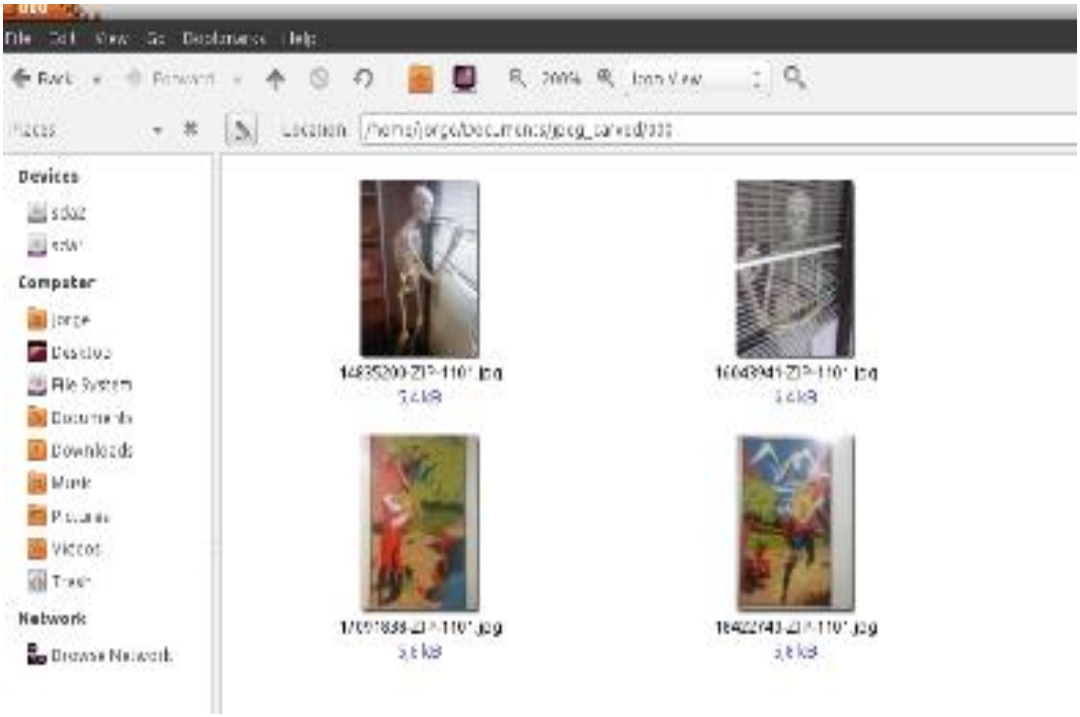


Figura 70. BE Viewer. Fotografías recuperadas mediante carving.

Los resultados obtenidos se copian a DVD para reportarlos al caso, entre otra información, los archivos con las imágenes fotográficas recuperadas del pendrive.

Dichas fotografías corresponden con las pruebas originales al poder ser visionadas y comprobar que son idénticas, el vídeo ha sido imposible recuperarlo pero si se tiene la información de sus metadatos con su nombre, tamaño, fecha creación, etc. El módulo *Exif* (figura 65) ha proporcionado los metadatos de los archivos CAMxxx.JPG en los que se observa la marca y modelo del móvil/cámara fotográfica utilizada, móvil LG modelo E400.

Además, se han obtenido al final del análisis los hashes de las imágenes forenses de trabajo y copia preservada comprobando que son idénticos, de esta forma se asegura la validez de la investigación.

El análisis forense digital de la evidencia02 (contenido del pendrive) con la herramienta Bulk Extractor Viewer si nos proporciona información suficiente para afirmar que las fotografías y vídeo aportados como prueba original al caso han sido almacenados y, posteriormente mediante formateo u otra técnica anti-forense, eliminados del pendrive. Además, se creó un archivo comprimido zip con dichos archivos.

Análisis forense digital de la información volátil del portátil - EVI03

Se solicita al funcionario responsable de la custodia de evidencias uno de los dos DVD EVI03 para proceder a su análisis en laboratorio. Se actualiza el documento de cadena de custodia y se planifica la investigación.

Como la información proporcionada está almacenada en DVD -protegido contra escritura- no es obligado trabajar en Linux con Caine 7.0. Con fines didácticos, se van a utilizar en este apartado herramientas y utilidades forenses digitales desarrolladas para Windows. Apuntar que la información adquirida con Investigador 2.0 resultado de la investigación está en ficheros *html* y de texto, solamente se debe realizar la búsqueda de texto / palabras / *strings* relevantes en la investigación. Se deben buscar indicios probatorios que demuestren el intento de acceso a la cuenta de correo electrónico de Amparo –amparo.xiva@gmail.com- desde el portátil Toshiba, así como cualquier otra información relacionada con la investigación, como por ejemplo, si el pendrive ha sido utilizado en el portátil, si se han descargado las fotografías y video, si se ha ocultado información intencionadamente, si conoce la contraseña de la cuenta de correo, si se han utilizado herramientas anti-forense, etc.

Análisis del volcado de la memoria RAM

La figura 71 muestra los archivos adquiridos en la captura de la información en memoria RAM del portátil y copiados por duplicado en DVD para su preservación.

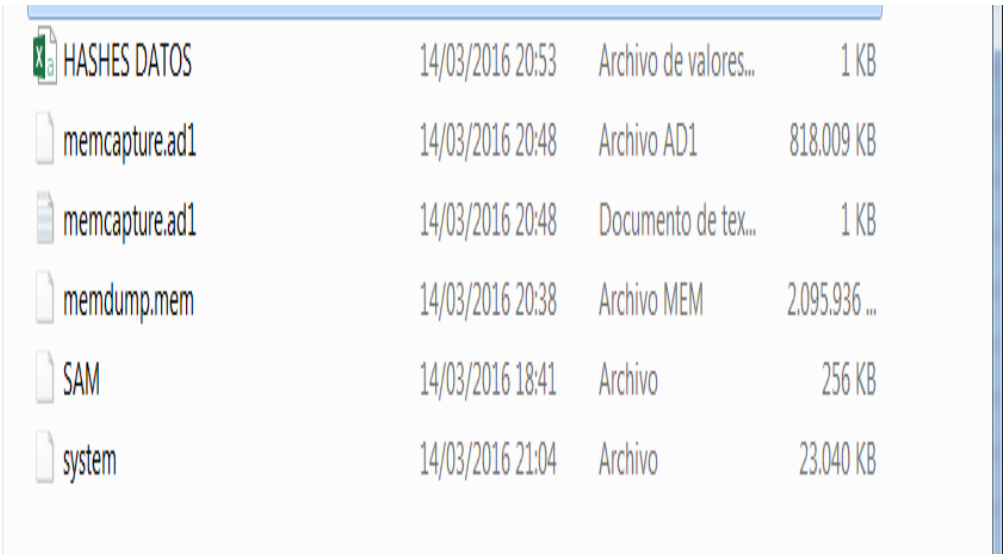


Figura 71. Datos forenses de EVI03 en DVD

Con la herramienta **AccessData FTK Imager,** en primer lugar se añaden los archivos con datos forenses y se crea la imagen (figura 72).

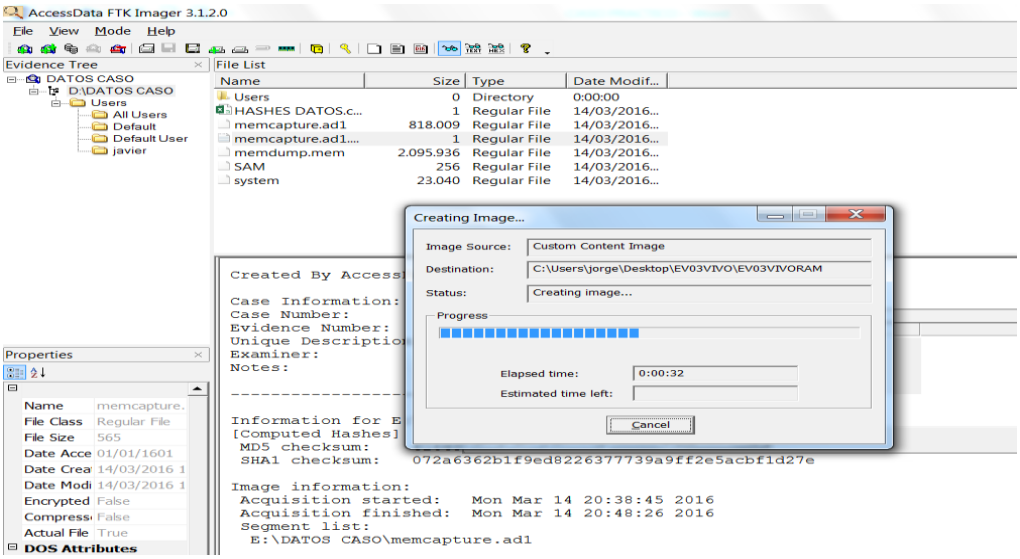


Figura 72. FTK Imager para añadir datos forenses de EVI03 y crear imagen

Sumario del proceso

Case Number: EV03FTKVOLATILAMPARO
Evidence Number: 03
Examiner: JORGE NAVARRO
Notes: DATOS VIVO PORTATIL EVIDENCIA 03 RAM
Information for C:\Users\jorge\Desktop\EV03VIVO\EV03VIVORAM.ad1:
[Custom Content Sources]
DATOS CASO:D:\DATOS CASO|memcapture.ad1(Exact)
DATOS CASO:D:\DATOS CASO|memdump.mem(Exact)
DATOS CASO:D:\DATOS CASO|SAM(Exact)
DATOS CASO:D:\DATOS CASO|system(Exact)
DATOS CASO:D:\DATOS CASO|memcapture.ad1.txt(Exact)
[Computed Hashes]
MD5 checksum: bc39fb76b06e04b0a78b88b63a719a07
SHA1 checksum: 0bb02c73299136ced8c182ed831c66aa7dca4766
Image information:
Acquisition started: Tue Mar 15 14:26:29 2016
Acquisition finished: Tue Mar 15 14:30:58 2016
Segment list:
C:\Users\jorge\Desktop\EV03VIVO\EV03VIVORAM.ad1
C:\Users\jorge\Desktop\EV03VIVO\EV03VIVORAM.ad2

A continuación se marca la opción "Show text only" y se ejecuta"Find …" para buscar la cadena "amparo.xiva" en el volcado de memoria RAM. El resultado ha sido positivo, la cadena se ha encontrado varias veces. Extracto del resultado:

.J.7.E
*https://accounts.google.com/**ServiceLoginEmailamparo.xiva@gmail.comPasswd**https://accounts.google.com/*

También se encuentran evidencias de que se ha introducido la contraseña de la cuenta de Amparo –amparo.xiva@gmail.com- como demuestra la figura 73.

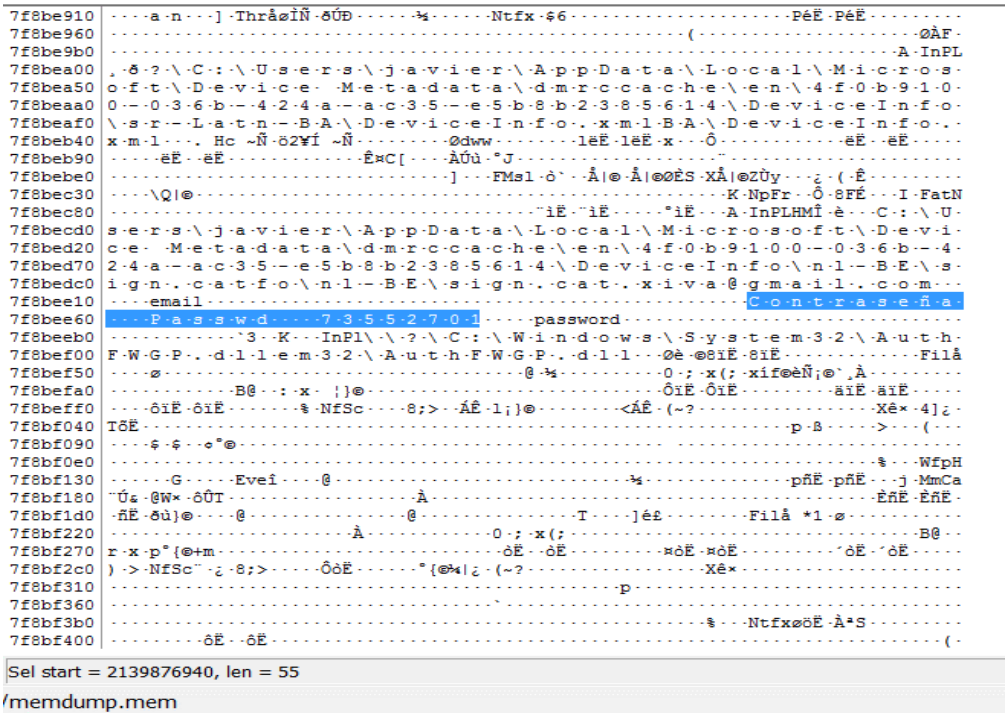


Figura 73. FTK Imager. Contraseña del correo en la RAM

También se busca por nombre o extensión de archivo, por ejemplo, “CAM” o “JPG” y se observa que bajo *library folder* - unidad E:\ existen los nombres de los archivos que son similares a las fotografías y vídeo de la prueba original. Y además, el fichero ZIP con los archivos comprimidos “FOTOSYVIDEO.ZIP” (figura 74).

Figura 74. Unidad E:\ y nombre de las fotografías, vídeo y ZIP

Se encuentran evidencias que demuestran que el pendrive requisado se ha introducido en el portátil Toshiba como se observa en la figura 75, USb 2.0 … y número de serie.

Figura 75. Número de serie del pendrive EVI02 introducido en el portátil.

Se buscan evidencias del uso de técnicas anti-forense, y se observa que se han realizado búsquedas en internet sobre "esteganografía" y se ha accedido a la web de descarga de *softonic* con la intención de descargar el programa "Camouflage" utilizado para ocultar información mediante técnicas de esteganografía[30] (figura 76).

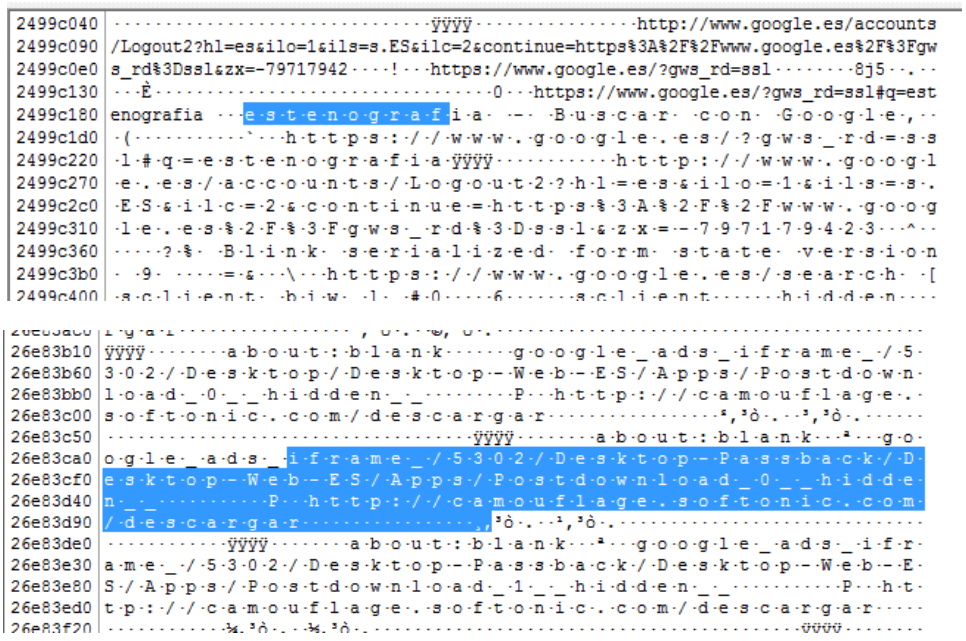


*Figura 76. Búsqueda y descarga de programas de esteganografía - C*amouflage

Esta información resulta muy útil para el equipo forense encargado del análisis de los discos duros del portátil Toshiba, además, evidencian el interés por estas técnicas de ocultación de información, utilizada, entre otros, por pederastas para camuflar contenido de pornografía infantil, por redes criminales, en ciberespionaje, etc.

Análisis de la información de Windows del portátil

Para finalizar con el análisis de la información volátil del portátil vamos localizar evidencias referentes al caso en los ficheros reportados con la herramienta **Investigador 2.0**. Recordar que éstos se encuentran almacenados en la carpeta RESULTS del DVD EVI03.

De toda la información investigada se extrae la que es relevante para el caso. A continuación se detalla el resultado del análisis.

En primer lugar se realiza el *hash* de todos los documentos reportados con el fin de garantizar la validez de las pruebas en el juicio. Para ello con la herramienta **HashMyFiles** elegiremos la carpeta *Results* y automáticamente se realiza el *hash* de todos los archivos de prueba.

Ejemplo de un fichero de salida proporcionado por HashMyFiles:

Nombre de archivo: mspass.html
Ruta completa : D:\results\mspass.html
MD5 : ec6bdbe0fafcdaca1f0927cb8bad7418
SHA1 : 6947a6c4cfbc48c2566d0e4bacf0fa34d76c13e2
CRC32 : b5f01e1b
SHA-256 : 2e9a49fb497aa8c3951fed9a93728ebe1a751f8d117ac49dc69a79e41053b728
SHA-512 :
c9654bb68edae2f044ca723180c6a594f0ff703bd331aff30dcf4879fa4835c16322a3bb2ddc1b08271
6557f0b121656599ad82c063b44bda1b9385bb241ee6b
SHA-384 :
4d339d8683b6c11c0020e6930d0160fc4cb9faa674ac9aea2b2a1cd81cf08bf5405bf026e44d353b7f
b242480c2a8a1a
Fecha de modificación: 14/03/2016 21:11:02
Fecha de creación: 14/03/2016 21:11:02
Tamaño : 432
Versión del archivo:
Versión del producto:
Idéntico :
Extensión : html
Atributos del archivo: R

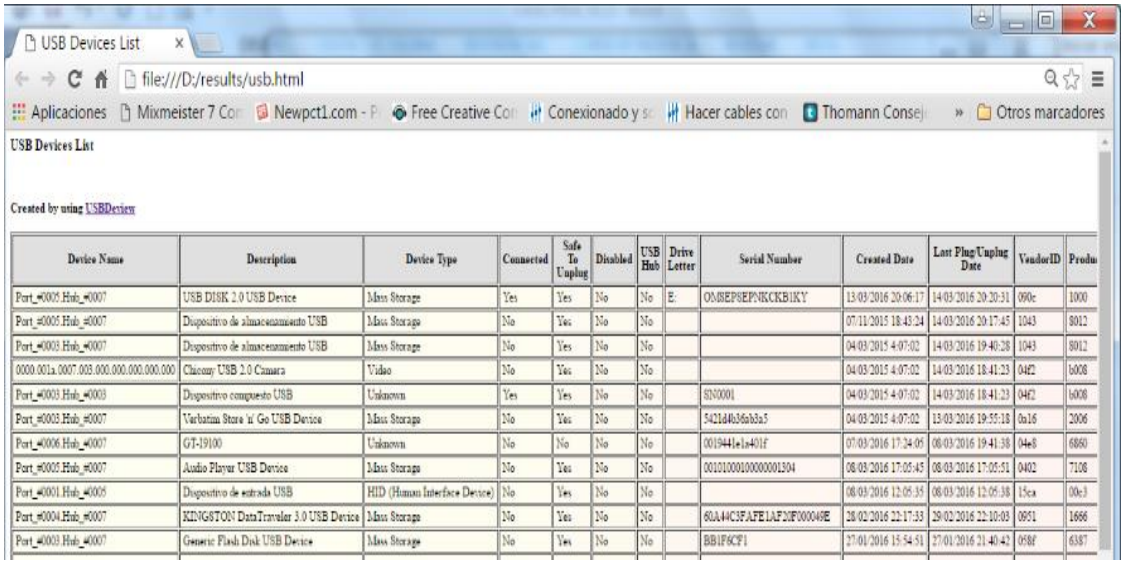
A continuación se estudia el contenido de los ficheros de datos forenses adquiridos:

systeminfo.txt

Información del portátil
Nombre de host: LAPTOP-TOSHIBA
Nombre del sistema operativo: Microsoft Windows 7 Ultimate
Versión del sistema operativo: 6.1.7600 N/D Compilación 7600
Fabricante del sistema operativo: Microsoft Corporation
Configuración del sistema operativo: Estación de trabajo independiente
Tipo de compilación del sistema operativo: Multiprocessor Free
Propiedad de: Javier
Organización registrada: YoReparoTuPC
Id. del producto: 00426-OEM-8992662-00400
Fecha de instalación original: 30/07/2013, 21:36:54
Tiempo de arranque del sistema: 14/03/2016, 18:41:06
Fabricante del sistema: TOSHIBA
Modelo el sistema: Satellite Pro P200
Tipo de sistema: X86-based PC

Procesador(es): 1 Procesadores instalados.
[01]: x64 Family 6 Model 15 Stepping 11 GenuineIntel ~2201 Mhz
Versión del BIOS: TOSHIBA V2.70, 13/12/2010
Directorio de Windows: C:\Windows
Directorio de sistema: C:\Windows\system32
Dispositivo de arranque: \Device\HarddiskVolume3
Configuración regional del sistema: es; Español (internacional)
Idioma de entrada: es; Español (tradicional)
Zona horaria: (UTC+01:00) Bruselas, Copenhague, Madrid, París
Cantidad total de memoria física: 2.046 MB
Memoria física disponible: 1.369 MB
Memoria virtual: tamaño máximo: 4.093 MB
Memoria virtual: disponible: 3.078 MB
Memoria virtual: en uso: 1.015 MB
Ubicación(es) de archivo de paginación: C:\pagefile.sys
Dominio: YOREPAROTUPC
Servidor de inicio de sesión: \\LAPTOP-TOSHIBA
Revisión(es): 1 revisión(es) instaladas. [01]: KB958488
Tarjeta(s) de red: 3 Tarjetas de interfaz de red instaladas.
[01]: Intel(R) Wireless WiFi Link 4965AGN
Nombre de conexión: Conexión de red inalámbrica
DHCP habilitado: S¡
Servidor DHCP: 192.168.1.1
Direcciones IP [01]: 192.168.1.133
[02]: Realtek PCIe FE Family Controller
Nombre de conexión: Conexión de rea local
Estado: Hardware ausente
[03]: VirtualBox Host-Only Ethernet Adapter
Nombre de conexión: VirtualBox Host-Only Network
Estado: Hardware ausente

UsbDview: Obtiene evidencias de que el pendrive USB 2.0.. con número de serie mostrado en la figura 77 corresponde con el investigado -ver figura 85- y ha sido utilizado en el portátil Toshiba.



Device Name	Description	Device Type	Connected	Safe To Unplug	Disabled	USB Hub	Drive Letter	Serial Number	Created Date	Last Plug/Unplug Date	VendorID	Produ
Port_#0005.Hub_#0007	USB DISK 2.0 USB Device	Mass Storage	Yes	Yes	No	No	E:	OMBEP8EPNKCKB1KY	13/03/2016 20:06:17	14/03/2016 20:20:31	090c	1000
Port_#0005.Hub_#0007	Dispositivo de almacenamiento USB	Mass Storage	No	Yes	No	No			07/11/2015 18:43:24	14/03/2016 20:17:45	1043	8012
Port_#0003.Hub_#0007	Dispositivo de almacenamiento USB	Mass Storage	No	Yes	No	No			04/03/2015 4:07:02	14/03/2016 19:40:28	1043	8012
0000.001a.0007.003.000.000.000.000.000	Chicony USB 2.0 Camera	Video	No	Yes	No	No			04/03/2015 4:07:02	14/03/2016 18:41:23	04f2	b008
Port_#0003.Hub_#0003	Dispositivo compuesto USB	Unknown	Yes	Yes	No	No		SN0001	04/03/2015 4:07:02	14/03/2016 18:41:23	04f2	b008
Port_#0003.Hub_#0007	Verbatim Store 'n' Go USB Device	Mass Storage	No	Yes	No	No		5421d4b36a0a5	04/03/2015 4:07:02	13/03/2016 19:55:18	0a16	2006
Port_#0006.Hub_#0007	GT-I9100	Unknown	No	No	No	No		0019441e1e401f	07/03/2016 17:24:05	08/03/2016 19:41:38	04e8	6860
Port_#0005.Hub_#0007	Audio Player USB Device	Mass Storage	No	Yes	No	No		0010100010000001304	08/03/2016 17:05:45	08/03/2016 17:05:51	0402	7108
Port_#0001.Hub_#0005	Dispositivo de entrada USB	HID (Human Interface Device)	No	Yes	No	No			08/03/2016 12:05:35	08/03/2016 12:05:38	15ca	00e3
Port_#0004.Hub_#0007	KINGSTON DataTraveler 3.0 USB Device	Mass Storage	No	Yes	No	No		60A44C5FAFE1AF20F000049E	28/02/2016 22:17:33	29/02/2016 22:10:03	0951	1666
Port_#0003.Hub_#0007	Generic Flash Disk USB Device	Mass Storage	No	Yes	No	No		BB1F9CF1	27/01/2016 15:54:51	27/01/2016 21:40:42	058f	6387

Figura 77. Resultado de la utilidad UsbDview

ChromePass: Obtiene las contraseñas almacenadas en Chrome. Se evidencia que desde este portátil se ha accedido a la cuenta de amparo y que se conocía evidentemente la contraseña (figura 78).

Origin URL	Action URL	User Name Field	Password Field	User Name	Password
https://accounts.google.com/ServiceLogin	https://accounts.google.com/ServiceLoginAuth	Email	Passwd	amparo.xiva@gmail.com	73552701

Figura 78 Resultado de la utilidad ChromePass. Contraseña del correo.

ChromeHistory: Se observa en la figura 79 como desde este portátil se ha accedido a la carpeta de correos Enviados y abierto el mensaje de asunto Fotos y vídeo.

Google	14/03/2016 20:02:28	1	1	
Recibidos (2) - amparo.xiva@gmail.com - Gmail	14/03/2016 19:36:27	3	0	https://mail.google.com/mail/u/0/
Gmail	14/03/2016 19:36:22	4	0	https://mail.google.com/mail/?auth=DQAAANgAAABpKTQgtt0Un
Gmail	14/03/2016 19:36:22	1	0	https://mail.google.com/accounts/SetOSID?continue=https%3A%2F
Gmail	14/03/2016 19:36:22	1	0	https://accounts.google.com/ServiceLoginAuth
Gmail	14/03/2016 19:36:22	2	0	https://mail.google.com/mail/
Cuentas de Google	14/03/2016 19:36:21	2	0	https://accounts.google.com/ServiceLogin?service=mail&passive=tr
Gmail	14/03/2016 19:36:14	2	0	https://mail.google.com/mail/
Gmail	14/03/2016 19:36:14	2	0	
Gmail	14/03/2016 19:36:14	4	0	https://mail.google.com/
gmail - Buscar con Google	14/03/2016 19:36:09	2	0	http://www.google.es/accounts/Logout2?hl=es&ilo=1&ils=s.ES&ilc
	14/03/2016 19:36:08	1	0	http://www.google.com/accounts/Logout2?hl=es&ilo=1&ils=doritos
	14/03/2016 19:36:07	1	0	https://accounts.youtube.com/accounts/Logout2?hl=es&ilo=1&ils=s
Cuentas de Google	14/03/2016 19:36:06	1	0	
Cuentas de Google	14/03/2016 19:36:06	1	0	https://accounts.google.com/Logout?hl=es&continue=https://www.g
gmail - Buscar con Google	14/03/2016 19:35:42	2	0	
Hackea Contraseñas de Correo Electrónico | Hackear Una Cuenta	14/03/2016 19:03:53	1	0	
hackear la contrase correo - Buscar con Google	14/03/2016 19:03:48	1	0	
Google	14/03/2016 19:02:41	1	1	
Google	14/03/2016 19:02:41	1	0	https://www.google.com/
Recibidos (2) - amparo.xiva@gmail.com - Gmail	14/03/2016 18:49:10	3	0	https://accounts.google.com/CheckCookie?checkedDomains=youtub
Fotos y video - amparo.xiva@gmail.com - Gmail	14/03/2016 18:48:18	1	0	https://accounts.google.com/CheckCookie?checkedDomains=youtub
Enviados - amparo.xiva@gmail.com - Gmail	14/03/2016 18:48:14	1	0	https://accounts.google.com/CheckCookie?checkedDomains=youtub
Recibidos (2) - amparo.xiva@gmail.com - Gmail	14/03/2016 18:48:08	3	0	https://mail.google.com/mail/u/0/

Figura 79. Resultado de la utilidad ChromeHistory. Acceso al correo / enviados

[30] **Esteganografía** según Alfonso Muñoz en el documento "Manual de StegSecert v.01" lo define como: 'La ciencia y/o arte de ocultar una información dentro de otra, que haría la función de "tapadera" (estegomedio o cubierta).'
StegSecret. Copyright (C) 2007. Alfonso Muñoz http://stegsecret.sourceforge.net

Otra información forense de interés obtenida durante la adquisición de evidencias:

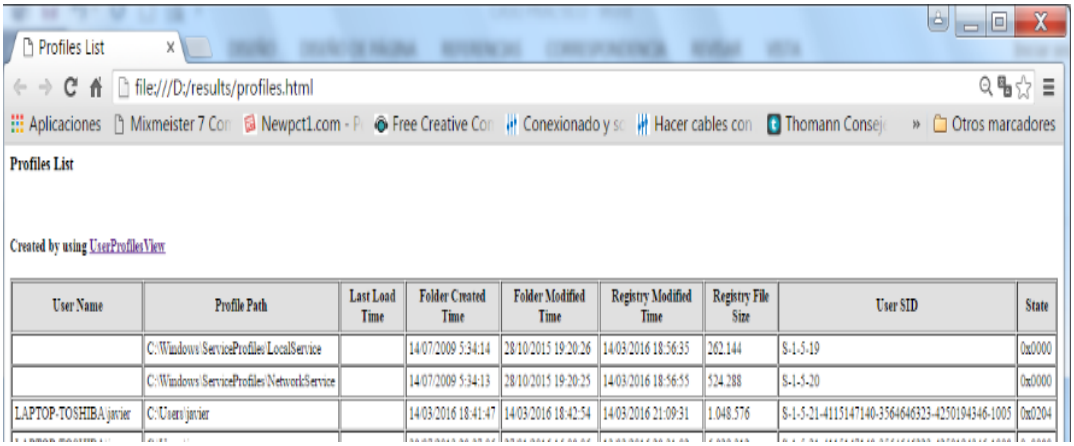


Figura 80. Usuarios de Windows con UserProfileView

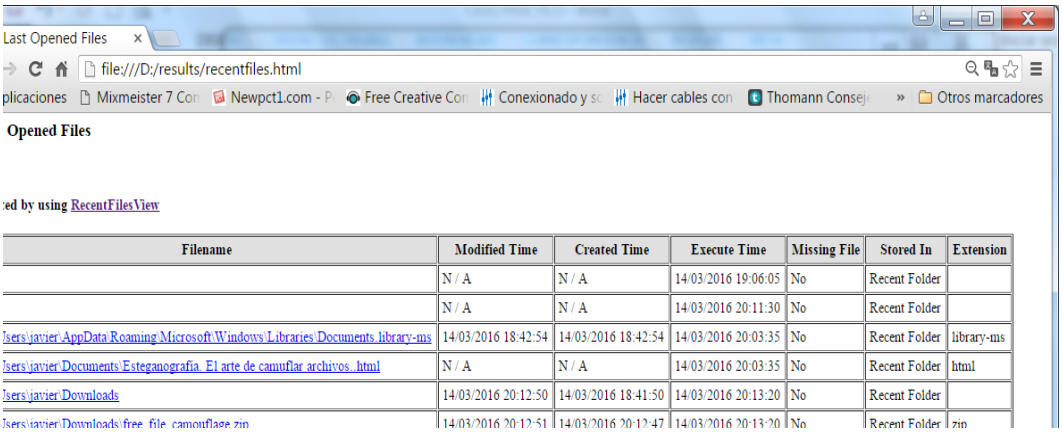


Figura 81. Ficheros abiertos recientemente con RecentFilesView

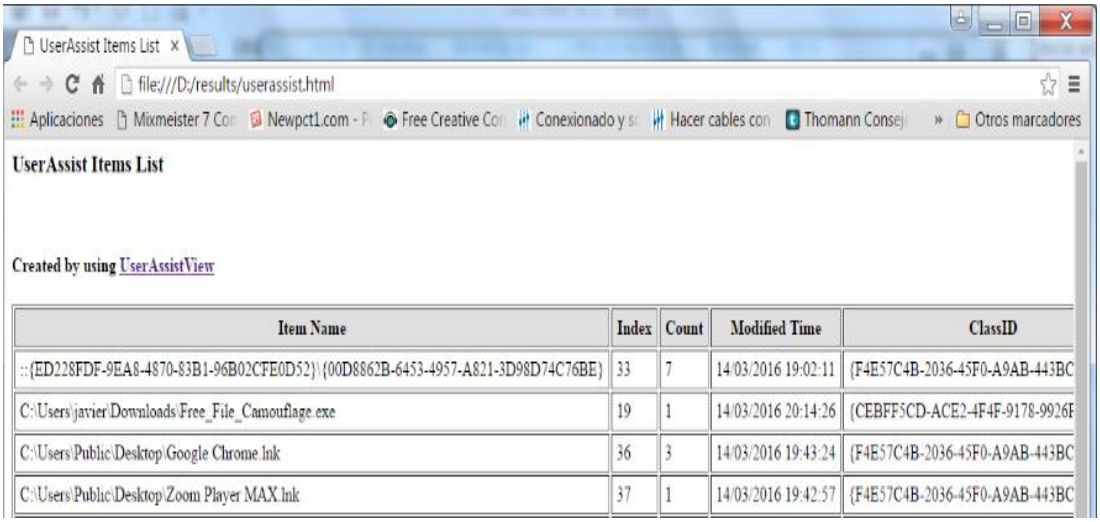


Figura 82 Programas ejecutados por usuario activo con UserAssistView

Se observa que el usuario de Windows "javier" ha ejecutado el programa "Camouflage", entre otros, recientemente en el portátil, ver figuras 81, 82 y 83.

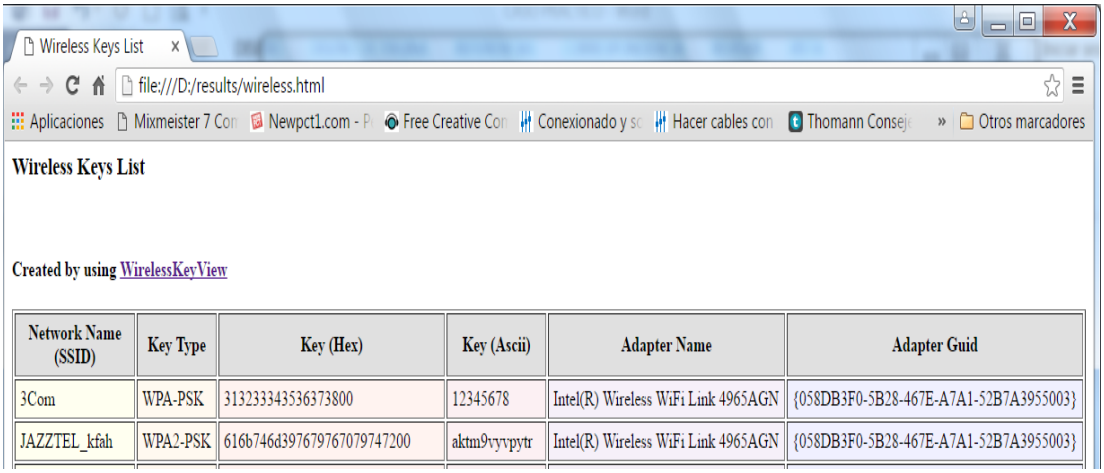


Figura 83. Resultado de la utilidad WirelessKeyView

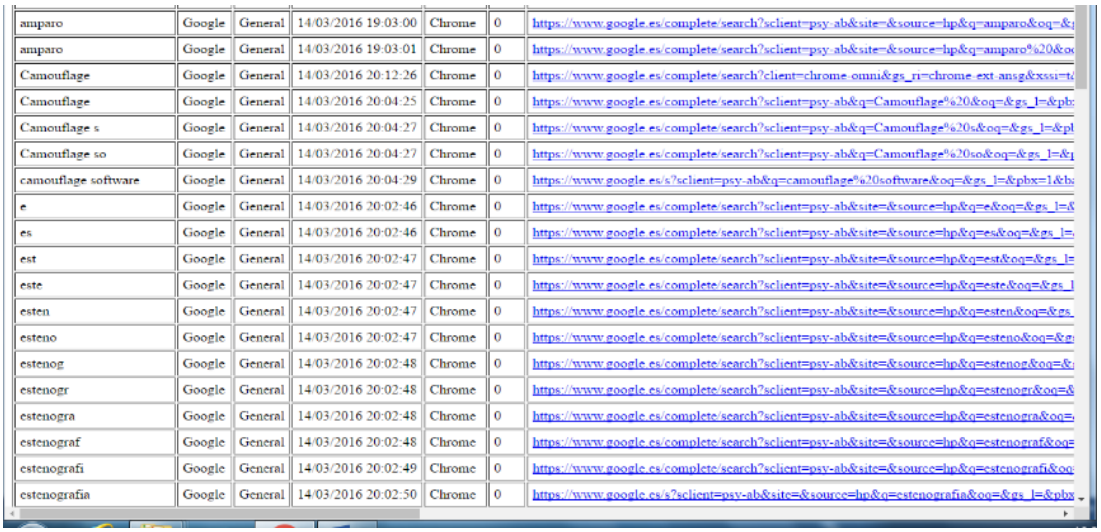


Figura 84. Resultado de búsquedas realizadas. MyLastSearch

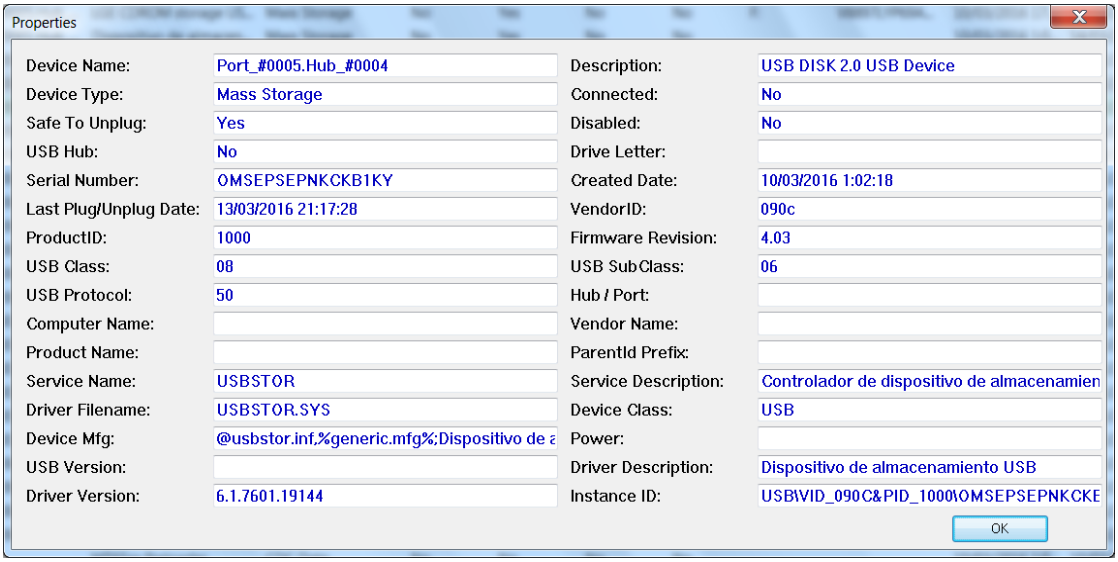


Figura 85. Serial Number del *pendrive investigado proporcionada por UsbDView*

Conclusiones de la investigación forense de la información volátil evi03

El resultado de la investigación forense realizada en laboratorio de la información volátil recopilada –EVI03- en el portátil Toshiba con nombre LAPTOP-TOSHIBA\\ determina que:

1. El usuario de Windows con nombre "javier" e identificador "S-1-5-21-4115147140-3564646323-4250194346-1005" ha accedido con el navegador Chrome a la cuenta de correo "amparo.xiva@gmail.com" y que evidentemente conoce la contraseña de acceso a dicha cuenta y ésta ha sido además tecleada, registrada y mostrada en los resultados "735527…".

2. Se ha accedido a la carpeta Enviados de dicha cuenta, se ha abierto el mensaje con Asunto "Fotos y vídeo" y se han descargado los adjuntos en formato ZIP con el nombre "Fotos y video.zip" y además cada uno por separado:

    a. Archivos en formato JPG con nombre CAM00138, CAM00139, CAM00613, CAM00614.
    b. Archivo formato vídeo MP4 con nombre CAM00615.

3. El pendrive requisado como prueba Ev02 con número de serie OMSEPSEP… ha sido utilizado en el portátil Toshiba.

4. Se han realizado búsquedas en internet referentes a técnicas de esteganografía –ocultar información- y se ha descargado, instalado y utilizado el programa Camouflage (utilizado para camuflar ficheros en otros, por ejemplo, fotografías en imágenes de fondo de Windows, un texto en una imagen o para cifrar archivos, etc).

Consideraciones de la investigación forense del pendrive - evi02

En este punto se podría dar por satisfactoria la investigación forense puesto que se ha evidenciado lo requerido en el expediente del procedimiento judicial. No obstante, a la vista de los resultados obtenidos del análisis del pendrive -evi02-, en los que se ha localizado un vídeo que no ha podido ser recuperado y además se ha descargado e instalado el programa Camouflage utilizado para ocultar información, según ofrecen los resultados de la investigación de la evi03, es necesario ampliar la investigación forense con otras herramientas desarrolladas principalmente para este tipo de casos.

A continuación se realiza el análisis forense de la imagen adquirida del pendrive y almacenada en DVD – evi02-. El objetivo es localizar evidencias de ocultación de información e intentar recuperar el vídeo u otros archivos relevantes utilizando herramientas forenses desarrolladas para entornos Windows como Autopsy 4.0, OsForensics 3.3 x64 y Xteg.

Ampliación del análisis forense del pendrive - EVI02 con Autopsy 4.0

Autopsy 4.0 funciona en entornos Windows y es muy útil para el tipo de investigación que se va a realizar: localizar y extraer archivos eliminados o dañados de un dispositivo *usb* y localizar archivos ocultos con técnicas estenográficas, entre otras.

El modo de trabajar en Autopsy 4.0 es:

1. Crear el caso a investigar.
2. Añadir la imagen forense con la información a analizar:
    a. Imagen almacenada en DVD "evidencia02".
3. Ejecutar los módulos de investigación *–Ingest Módules-. Nada más cargar la imagen –fuente de datos- automáticamente se lanzan los módulos de investigación.*
4. *Localizar en el árbol de resultados aquellas evidencias relevantes para el caso.*
5. *Crear informe de resultados.*

Una vez cargada la imagen forense "evidencia02" y finalizada la ejecución de los módulos analíticos, procedemos a estudiar los resultados obtenidos (figura 86).

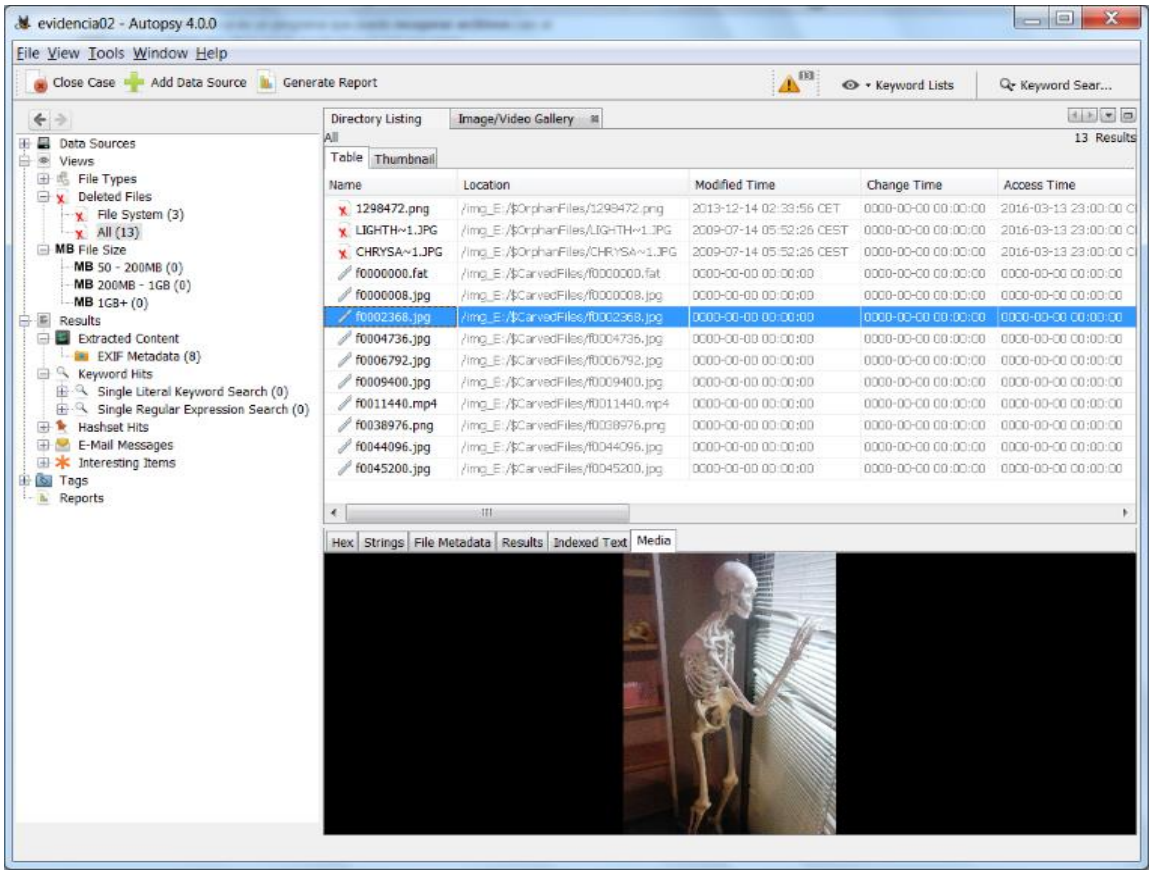


Figura 86. Análisis forense del pendrive con Autopsy 4.0

En principio, la información encontrada por Autopsy 4.0 es similar a la obtenida anteriormente, las tres imágenes borradas, las cuatro fotografías, el vídeo … (figura 87).

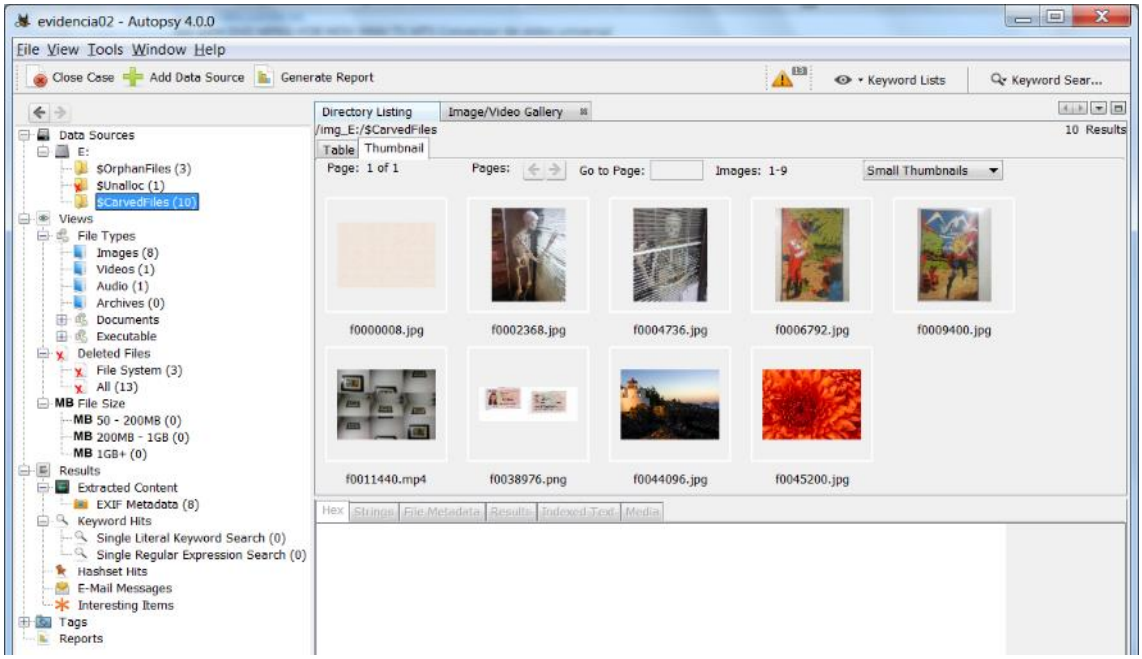


Figura 87. Archivos encontrados con Autopsy 4.0

Utilizamos la función exportar para intentar recuperar los archivos encontrados. Se han exportado todos los archivos (figura 88) y éstos se abren correctamente. Se comprueba que hasta el vídeo se visiona correctamente y su contenido es similar al vídeo de la prueba original.

Vemos que además se han exportado otros archivos como “README”.

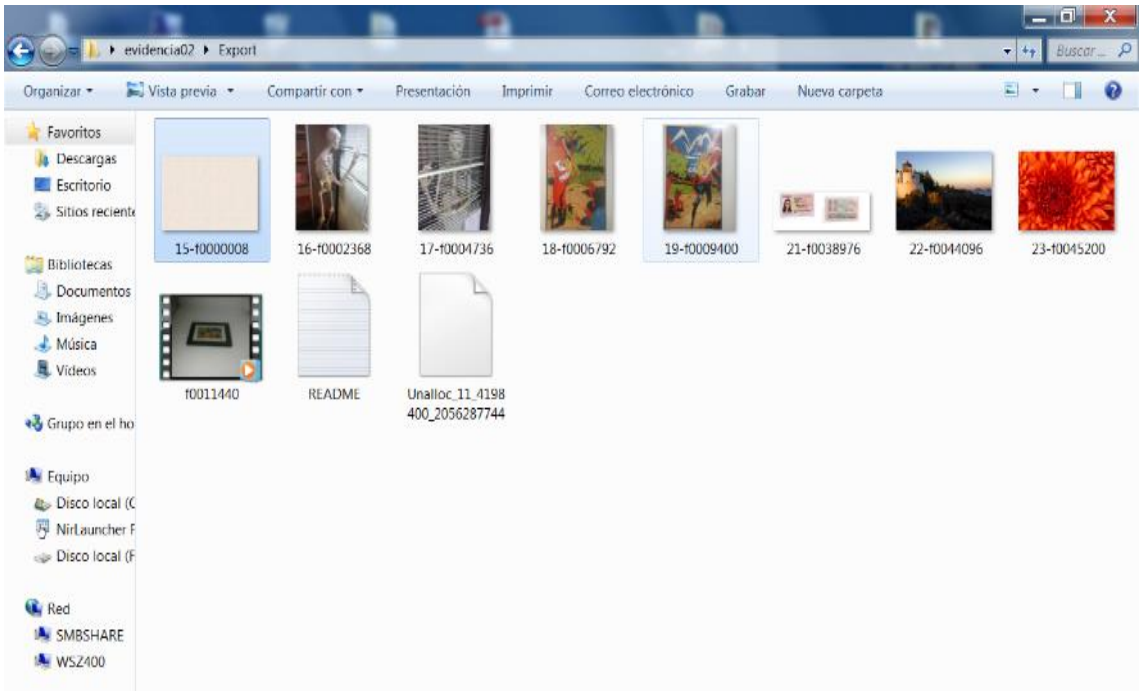


Figura 88. Archivos contenidos en el pendrive exportados con Autopsy 4.0.

Una vez recuperados los archivos con Autopsy 4.0 se realizan los *hash* (figura 89) de todos ellos con la utilidad HashMyFiles, se documenta y se realiza imagen para su custodia.

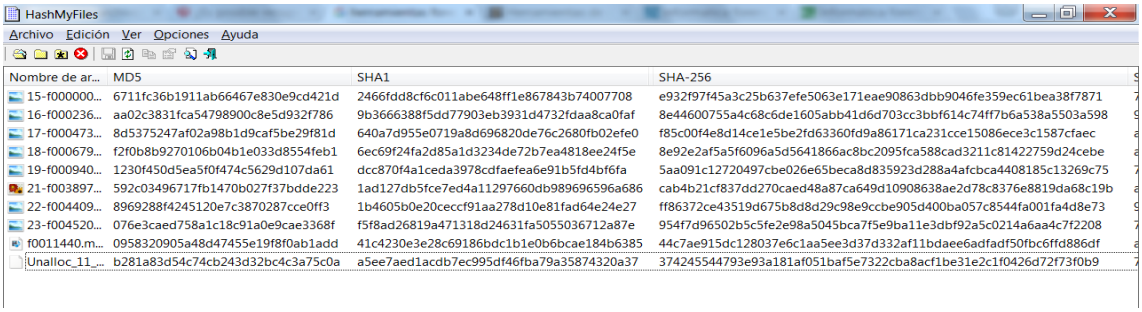


Figura 89. Hash de los archivos exportados con Autopsy 4.0

OsForensics. Análisis de ocultación de información de los archivos exportados

Con OSForensics se van a analizar todos los archivos exportados en búsqueda de técnicas de ocultación. Como se puede observar en la figura 90, el módulo "*Mismatch Files"* alerta de la existencia de un fichero que oculta su identidad real, sustituyendo su nombre y extensión por otro.

En concreto el archivo "README.LOG" no es lo que parece. En realidad es una fotografía –archivo JPG- de Amparo oculta bajo una extensión log (figura 91).

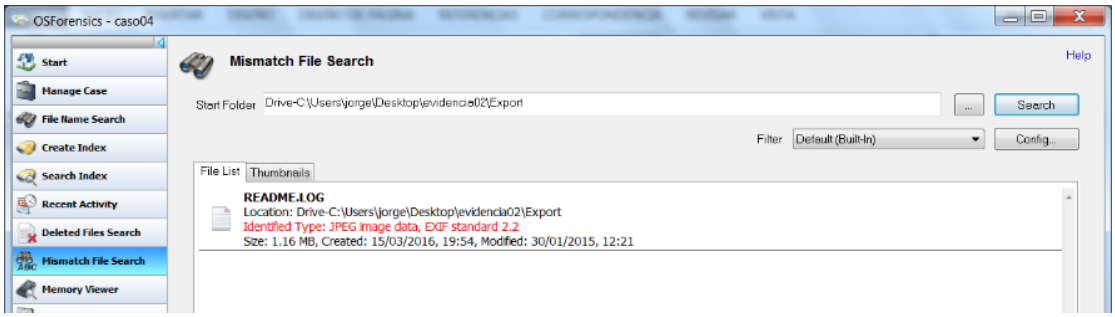


Figura 90. Mismatch File con OSForensics

Figura 91. Fotografía camuflada en fichero README.LOG

Xteg. Localizar archivos con esteganografía.

A la vista de los resultados en los que se observaba la instalación del programa Camouflage, es necesario realizar la investigación en los archivos exportados con Autopsy 4.0 para ver si contienen muestras de técnicas estenográficas. El programa Xteg nos indica que en estos archivos no se encuentran evidencias de ocultación de información mediante esteganografía (figura 92).

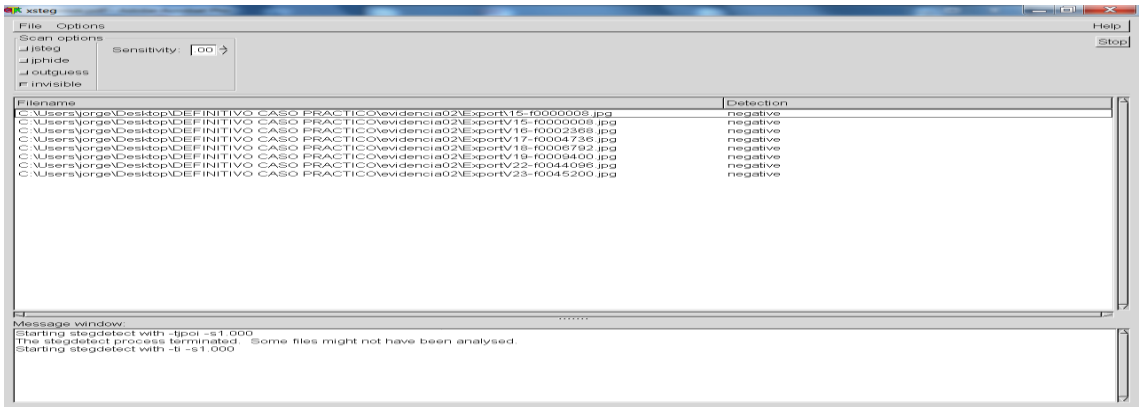


Figura 92. Resultado negativo en la búsqueda de esteganografía con Xteg.

Conclusión del análisis realizado al pendrive "evi02" con Autopsy 4.0, OSForensics y Xteg.

Con Autopsy 4.0 se ha conseguido exportar el vídeo y otros archivos que antes no había sido posible recuperar. Además, con OSForensics se ha descubierto que el archivo README.LOG oculta su información real, una fotografía de Amparo. También, se ha utilizado la herramienta Xteg para localizar evidencias de esteganografía en los archivos exportados, siendo el resultado negativo.

Informe de resultados en la investigación del caso

Existen evidencias de que, en el *pendrive usb* -evi02- investigado se han copiado y posteriormente eliminado -mediante formateo u otra técnica- las fotografías y vídeo presentados como pruebas al caso. Además, se demuestra que el usuario de Windows con nombre "javier" del portátil Toshiba investigado, ha accedido a la cuenta de correo electrónico "amparo.xiva@gmail.com, abierto la carpeta enviados, leído el mensaje con asunto "FOTOS y VIDEO" y descargado el archivo ZIP con sus adjuntos -pruebas originales- lo que evidencia que se conoce la contraseña. Además, se consigue averiguar con la utilidad ChromePass y de la información de la RAM con FTK Imager, siendo ésta "73552…". Por otro lado, se obtienen pruebas que afirman que el pendrive con número de serie "OMSEPSEP…" es el pendrive a investigar –evi02- y éste se ha conectado al portátil Toshiba, tal y como se declara en la denuncia. Y por último, se ha averiguado que el pendrive contiene un archivo eliminado README.LOG que en realidad es una fotografía de Amparo.

Conclusiones finales

Como ya se ha comentado a lo largo del trabajo, vivimos en un mundo digitalmente conectado donde el flujo de información en los medios tecnológicos define un escenario complejo. Por ello, los peritos informáticos forenses deben aplicar otros "sentidos" que no solo se basen en la dimensión estática del hecho "causa-efecto". Deben desarrollar la capacidad de analizar y comprender la complejidad de este nuevo mundo virtual, donde se hace necesario identificar la estructura global que origina el contexto de la investigación y tener en cuenta las relaciones entre individuos, infraestructuras de interconexión y la tecnología.

En este nuevo escenario, el ciberespacio, donde se integran y convergen, entre otras, las transacciones en la "nube", la computación móvil, el *Big Data,* los servicios digitales y "el internet de las cosas", la investigación de conductas delictivas se traduce en un reto interdisciplinario que puede llegar a superar la capacidad del perito informático forense.

A medida que las nuevas tecnologías se vayan introduciendo en nuestras vidas, más difícil será garantizar la veracidad de las evidencias digitales en la comisión de un delito. En parte esto se debe, a la in-percepción y desconocimiento que los usuarios tienen de las TIC y de los sistemas interconectados que hacen posible interrelacionarse.

Para un perito informático forense uno de los retos en su investigación es poder dar respuesta a la pregunta ¿quién ha cometido…?. A la vista del panorama actual, donde lo virtual y lo real se funden, con infraestructuras gestionadas por terceros, donde los individuos tienen varias identidades virtuales y las fronteras geográficas se diluyen; dar respuesta a esta pregunta puede ser el mayor de los retos para el analista forense. Por otro lado, esta situación le puede acarrear más de un problema legal en un proceso judicial.

Así pues, es imprescindible analizar las pericias actuales y revisar las metodologías que entran en conflicto o parecen insuficientes en este nuevo y futuro entorno. Por ejemplo, combinar los actuales estilos metodológicos basados principalmente en causa-efecto con fundamentos basados en teorías del conocimiento teniendo en cuenta aspectos sociales, las relaciones de individuos o entornos, y siempre desde un punto de vista objetivo, veraz y confiable.

Parece púes necesario, estudiar lo ocurrido no solamente desde la parte estática, sino además evidenciar la parte dinámica de la escena o entorno del delito, y así poder conocer la estructura global que sostienen los hechos.

Aunque las tecnologías evolucionen, los principios en el proceso de toma de evidencias deben prevalecer, así como, el resto de las fases metodológicas. Únicamente sería necesario agregar aquellos aspectos de la nueva tecnología objeto de análisis que deban modificarse para asegurar los criterios de preservación y confiabilidad de las evidencias recolectadas.

Por otro lado, es necesario crear un espacio de investigación “abierto” con el fin de mejorar los diálogos entre los profesionales, los procedimientos aplicados, la tecnología y la jurisprudencia, que permita llevar a la informática forense a una nueva dimensión que responda a las exigencias del ciberespacio.

Bibliografía

Alfonso Beltán, J.I. (2015). Ataques entre estados mediante Internet. Valencia: PFC ESTINF UPV.

Arellano, L., & Darahuge, E. (2011). *Manual de Informática Forense.* Buenos Aires: Errepar.

Cano Martinez, J. (2009). *Computación Forense. Descubriendo los rastros informáticos.* Mexico: Alfaomega.

Capell, J. (2010). *Actuación policial: Causas de nulidad.* Barcelona: Mossos d'Esquadra. Revista Catalana de Seguretat Pública.

Cellebrite. (2015). *Unlock Digital Intelligence. Accelerate Investigations Anywhere.* Cellebrite Mobile Forensics.

COIICV. (2014). *Seguridad para tod@s en la Sociedad de la Información.* Valencia: Colegio Oficial de Ing. Informática de Valencia.

De Salvador, L. (2015). *Documento de Opinión 35/2015. Ciber-Resiliencia.* Ieee.

Del Peso Navarro, E. (2001). *Peritajes Informáticos.* Madrid: Diaz de Santos.

Del Peso Navarro, E., & Piattini, M. (2000). *Auditoría Informática. Un enfoque práctico.* RA-MA.

EC-Council. (2010). *Computer Forensics. Investigating Wireless Networks and Devices.* EEUU: Cengage Learning.

elcano, C. (2015). *Informe mensual de ciberseguridad.* Madrid: Real Insituto Ciber elcano y Thiber.

Ferrer, J., & Fernandez, J. (s.f.). *Seguridad Informática y software Libre.* Hispalinux.

Fojón, E., Coz, J., Miralles, R., & Linares, S. (2012). *La Ciberseguridad Nacional,Un compromiso de todos.* SCSI.

Gallagher, P. (2012). *Anual Report. Computer Division Special Publication 800-165.* EEUU: National Institute of Standards and Technology.

García Rambla, J. (s.f.). *Un forense llevado a juicio.* Sidertia.

Garrido Caballero, J. (2010). *Análisis forense digital en entornos Windows.* Madrid: Informática64.

GC. (2015). *Pericias desarrolladas en el servicio de criminalística de la Guardia Civil.* Peritajes y Arbitrajes.

Gobierno, P. d. (2013). *Estrategia de Ciberseguridad Nacional.* Madrid.

Gómez Vieites, A. (2011). *Enciclopedia de la seguridad informática.* España: RA-MA.

Hennessy, J. L. (2007). *Computer architecture : a quantitative approach.*

Info-Lab. (2015). *Guía integral de empleo de la informática forense en el proceso penal.* Mar del Plata: Unversidad FASTA.

Inteco. (s.f.). *Hash. Cómo comprobar la integridad de los ficheros.* Observatorio cuaderno de notas.

Jerez Guerrero, J. (julio de 2015). Investigación informática forense basada en Emacs. Madrid: Universidad Politécnica de Madrid.

Jonhson, T. A. (2005). *Forensic Computer Crime Investigation*. NW: Taylor & Francis Group.

Lazaro, F. (4/2010). Informática forense y software libre. *LINUX+*, 12-20.

López Delgado, M. (2007). *Análisis Forense Digital.* GNU Free Documentation.

Martinez Retenaga, A. (2014). *Toma de evidencias en entornos Windows*. Incibe.

Martos, J. (2006). *Peritaciones y arbitrajes.* Madrid: Recobery Labs.

Nebot Hernández, M. (2013). *Herramientas para la informática forense: Catalogación*. Valencia: PFC Dpto. de Organización de Empresas - ETSINF - Universidad Politécnica de Valencia.

Oltra, J. (2015). *Dictámenes y peritajes informáticos*. Valencia: Dpto. de Organización de Empresas - ETSINF - Universidad Politécnica de Valencia.

Oltra, J. (2015). Apuntes. *La e-Evidencia*. Valencia: Dpto. de Organización de Empresas - ETSINF Universidad Politécnica de Valencia.

Oltra, J. (2015). *Introducción a la deontología.Panorama actual*. Valencia: Dpto. de Organización de Empresas - ETSINF Universidad Politécnica de Valencia.

Oltra, J. (2015). *Etica* informática. Valencia: Dpto. de Organización de Empresas - ETSINF - Universidad Politécnica de Valencia.

Ortiz Pradillo, J. (2013). *La investigación del delito en la era digital.* Fundación alternativas.

Otero, J. (2011). *Policía Científica. 100 Años de Ciencia al Servicio de la Justicia.* Madrid: Ministerio del Interior.

Presman, G. (2014). *Normalizando la práctica forense informática.* Argentina: Congreso Argentino de Informática Forense.

Rivas, J. (2009). *Análisis Forense de Sistemas Informáticos*. Barcelona: Universitat Oberta Catalunya.

Rodriguez, A. (2013). *Nuevos retos y desafios de la informática forense.* Madrid: Dirección General de la Guardia Civil.

Sebastián, L. (2009). *Guía de implementación de un laboratorio forense.* Argentina.

Segura Serrano, A., & Gordo, G. F. (2014). *Ciberseguridad Global.* Universidad de Granada.

Sepin. (2015). *Modificación de la Ley Orgánica 10/1995 del CP.* Madrid: Editorial Jurídica SEPIN.

Sierra, J. (2003). *Retos de la informática forense.* Madrid: AgoraSic UPM.

Steve, B. (2008). *EnCase Computer Forensics - Study Guide Certified Examiner*. Canada: Wiley Publishing.

Steven Babitsky, E., & Mangraviti, J. (2002). *Writing and Defending your Expert Report*. EEUU: Seak.

Tocados, J. (2015). *Metodología para el desarrollo de procedimientos periciales en la informática forense*. Universidad de Castilla-La Mancha.

U-Tad. (2015). *Estado de la ciberseguridad.* Centro Universitario de Tecnologia y Arte digital.

Valenzuela, I. (2015). *Últimos avances en Análisis Forense de Sistemas Android.* Madrid: McAfee.

Verdezoto, R., & Espinoza, J. (2015). *El rol de la auditoría forense en los nuevos delitos*. Guayaquil: Universidad Politécnica Salesiana.

Recursos web

Aldama. *Informática Legal. Peritajes informáticos*. Obtenido de http://aldama.es/

ANCITE. *Asociación Nacional de Ciberseguridad y Pericia Tecnológi*ca. Obtenido de http://www.ancite.es/w3/

ANTPJI. *Asociación Nacional de tasadores y peritos judiciales informáticos*. Obtenido de http://www.antpji.com/antpji2013/

ASPEI. *Asociación Nacional de Peritos Informáticos*. Obtenido de http://www.aspei.es/

Asuejo, R. *La Seguridad de la Información*. Obtenido de http://Ausejo.net

Blueliv. *Proveedor líder en Análisis de amenazas cibernéticas para grandes empresas y proveedores de servicios*. Obtenido de http://www.blueliv.com

Caballero, A. *Hacking Ético, Informática Forense, GNU/Linux y Software Libre*. Obtenido de http://www.reydes.com/d/

CCN-CERT. *Centro Criptológico Nacional. Capacidad de Respuesta a incidentes de Seguridad de la Información*. Obtenido de https://www.ccn-cert.cni.es/

CiberSec Cert. *Prevenir y responder de manera efectiva y oportuna a incidentes de ciberseguridad*. Obtenido de http://www.globalcybersec.com

Conexión Inversa. *Incident Response, Security and Forensics*. Obtenido de http://conexioninversa.blogspot.com.es

CSIRT-CV. *Centre de Seguretat TIC de la Comunitat Valenciana*. Obtenido de http://www.csirtcv.gva.es/

Delitos Informáticos. *Revista legal*. Obtenido de http://www.delitosinformaticos.com

Derecho.com. *Toda la información de Derecho Informático*. Obtenido de http://legislacion.derecho.com/

Diaz, G., & Usme, J. *El software libre en la informática forense*. Obtenido de http://software-libre-if.blogspot.com.es/

DragonJar. *Comunidad de investigadores, estudiantes, profesionales y entusiastas de la Seguridad Informática*. Obtenido de http://www.dragonjar.org/

Forensic & Security. *Peritos Informáticos Forenses & Auditores de Seguridad*. Obtenido de http://forensic-security.com/

Forensic Control. *Computación Forense*. Obtenido de https://forensiccontrol.com/

GITS. *Sobre Ciberseguridad GITS Informática*. Obtenido de http://www.gitsinformatica.com/

Grupo S21sec Gestión. *Comprometidos con la Ciberseguridad*. Obtenido de http://www.s21sec.com/es/

HighSec. *Aprender ciberseguridad de forma práctica*. Obtenido de http://highsec.es/

ICFS. *Instituto de Ciencias Forenses y Seguridad de la UAM*. Obtenido de https://www.icfs.es/

INCIBE. *Instituto Nacional de Ciberseguridad*. Obtenido de https://www.incibe.es/home/instituto_nacional_ciberseguridad/

INFOFOR. *Informática Forense. Estaciones forenses. Dispositivos.* Obtenido de http://www.infoforense.com/index.html

INTERPOL *La mayor organización policial internacional del mundo.* Obtenido de http://www.interpol.int/es

Investigaciones Informaticas Norte. *Empresa líder en España de peritaje informático y seguridad informática.* Obtenido de http://www.peritosinformaticos.biz/

Inza, J. *Valor probatorio de los documentos electrónicos.* Obtenido de Evidencias electrónicas: http://www.foroevidenciaselectronicas.org/

ITInsecurity. *La inseguridad informática.* Obtenido de http://insecurityit.blogspot.com.es/

La Huella Oculta. *Seguridad y Análisis Forense Informáticos.* Obtenido de https://lahuellaoculta.wordpress.com/

LabSec. *Laboratorio de seguridad informática.* Obtenido de http://siberiano.aragon.unam.mx/labsec/

Netmind. *Cursos y certificaciones seguridad informática y forense.* Obtenido de http://www.netmind.es/

NIST. *National Institute of Standars and Technology.* Obtenido de http://www.nist.gov/

OnData. *Productos profesionales de Seguridad Informática y Computer Forensics.* Obtenido de http://ondatashop.com/

Perez, A. *Ciberseguridad y peritaje judicial informático.* Obtenido de http://ciberseguridad.eu/

PeritoIT. *Peritaje informático y tecnológico.* Obtenido de http://peritoit.com/

PoderJudicial. *Información del Consejo del Poder Judcicial de España.* Obtenido de http://www.poderjudicial.es/cgpj/es/Poder_Judicial

Portico Legal. *Toda la información legal.* Obtenido de https://porticolegal.expansion.com/

Real Insituto Elcano. *Think-tank de estudios internacionales y estratégicos.* Obtenido de http://www.realinstitutoelcano.org/

Recobery Labs. *Servicios de peritaje informático.* Obtenido de http://www.delitosinformaticos.info/index.html/

SBD. *Security By Default.* Obtenido de http://www.securitybydefault.com/

Sebastián, L. *Informática pericial.* Obtenido de http://periciasinformaticas.sytes.net/index.php

WeliveSecurity. *Noticias, opiniones y análisis de la comunidad de seguridad de ESET.* Obtenido de http://www.welivesecurity.com/la-es/