Forensic FOCA 1.0

Manual de usuario

Informática 64 S.L.

support@informatica64.com

13/02/2012

Índice

1. Introducción

Forensic FOCA es una herramienta para analistas forenses enfocada en la utilización de los metadatos de los ficheros para, en última instancia, generar un caso forense.

La herramienta está pensada para hacer un análisis offline, el analista debe tener en su poder los ficheros del caso, o un disco copiado y montado en el sistema. Estos ficheros son los que utilizará Forensic FOCA para realizar el análisis.

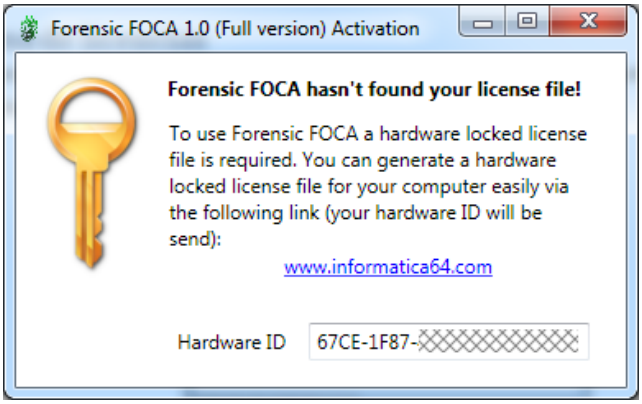
La herramienta es capaz de analizar los metadatos de una larga lista de formatos que se listan a continuación:

- Microsoft Office 2007 y posterior (.docx, .xlsx, .pptx, .ppsx)
- Microsoft Office 97 al 2003 (.doc, .xls, .ppt, .pps)
- OpenOffice (.odt, .ods, .odg, .odp, .sxw, .sxc, .sxi)
- Documentos PDF
- Información EXIF de imágenes JPG
- WordPerfect (.wpd)
- Imágenes SVG
- Documentos de InDesign (.indd)

Tras el análisis de la información la herramienta permite visualizar la información en diferentes vistas, siendo especialmente útil el Timeline donde se crea una línea temporal con todos los eventos relacionados con los ficheros analizados.

2. Sistema de licencias

La primera vez que arranque Forensic FOCA se le mostrará una ventana informando que no se ha hallado ninguna licencia de Forensic FOCA.



Deberá pulsar el enlace mostrado que le llevará a la página de generación de licencias.

Esta página es la encargada de generar un fichero de licencia válido para el equipo con el Hardware ID que especifique.

Este fichero de licencia le permitirá ejecutar Forensic FOCA en su equipo durante un año. Si cambia de place base o CPU la licencia no funcionará, así que asegurase de generar la licencia para el equipo que vaya a usar el próximo año.

En la página deberá introducir la dirección de email que utilizó en la compra de Forensic FOCA al comprar el producto mediante la web de Paypal. También deberá introducir el identificador de compra, este identificador se le envía a su correo electrónico cuando completa correctamente el pago en Paypal. Si no encuentra el identificador de compra en su correo electrónico puede utilizar la opción de recuperar identificador de compra que le renviará el mismo a su email.

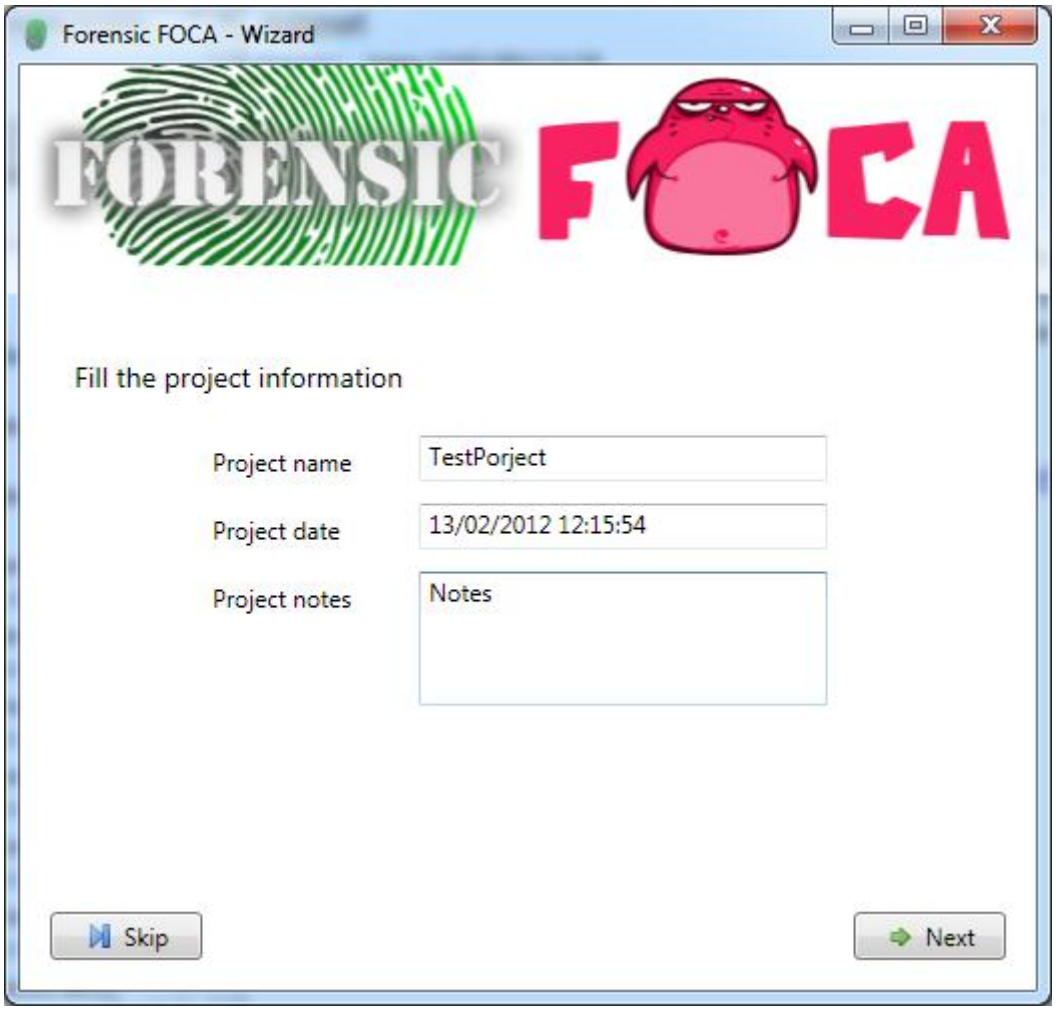
Una vez completados todos los campos del formulario pulse el botón Generar Licencia. Le llegará un correo con la licencia, el fichero "*license.license*" adjunta. Guarde ese archivo en la ruta donde se ha instalado Forensic FOCA, por defecto:

C:\Program Files (x86)\Informatica64\Forensic FOCA 1.0 (Full version)

Una vez copiado el archivo vuelva a arrancar la aplicación. Si todo ha ido bien Forensic FOCA arrancará correctamente mostrándole la pantalla inicial de Wizard.

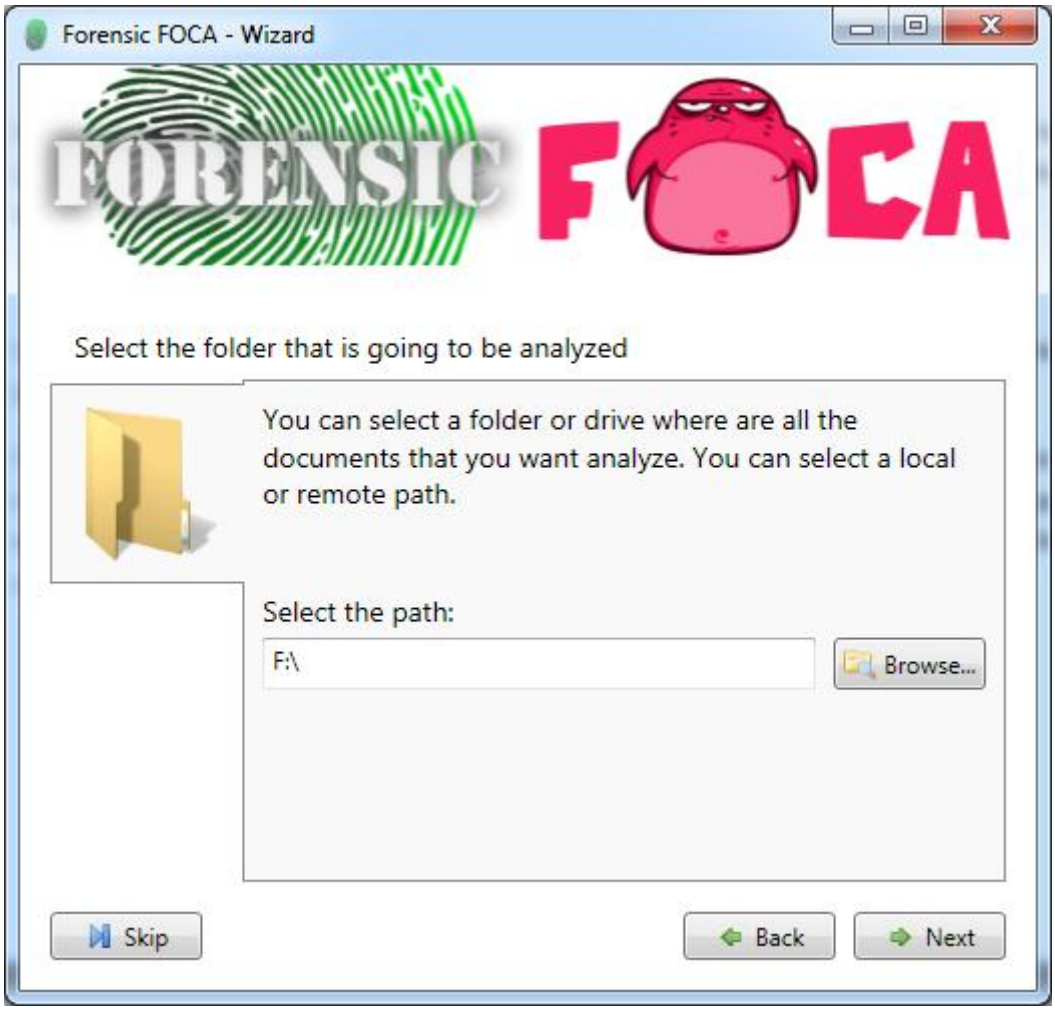
3. Wizard

Lo primero que se muestra al arrancar Forensic FOCA es un asistente que te guía para la correcta utilización de la herramienta.



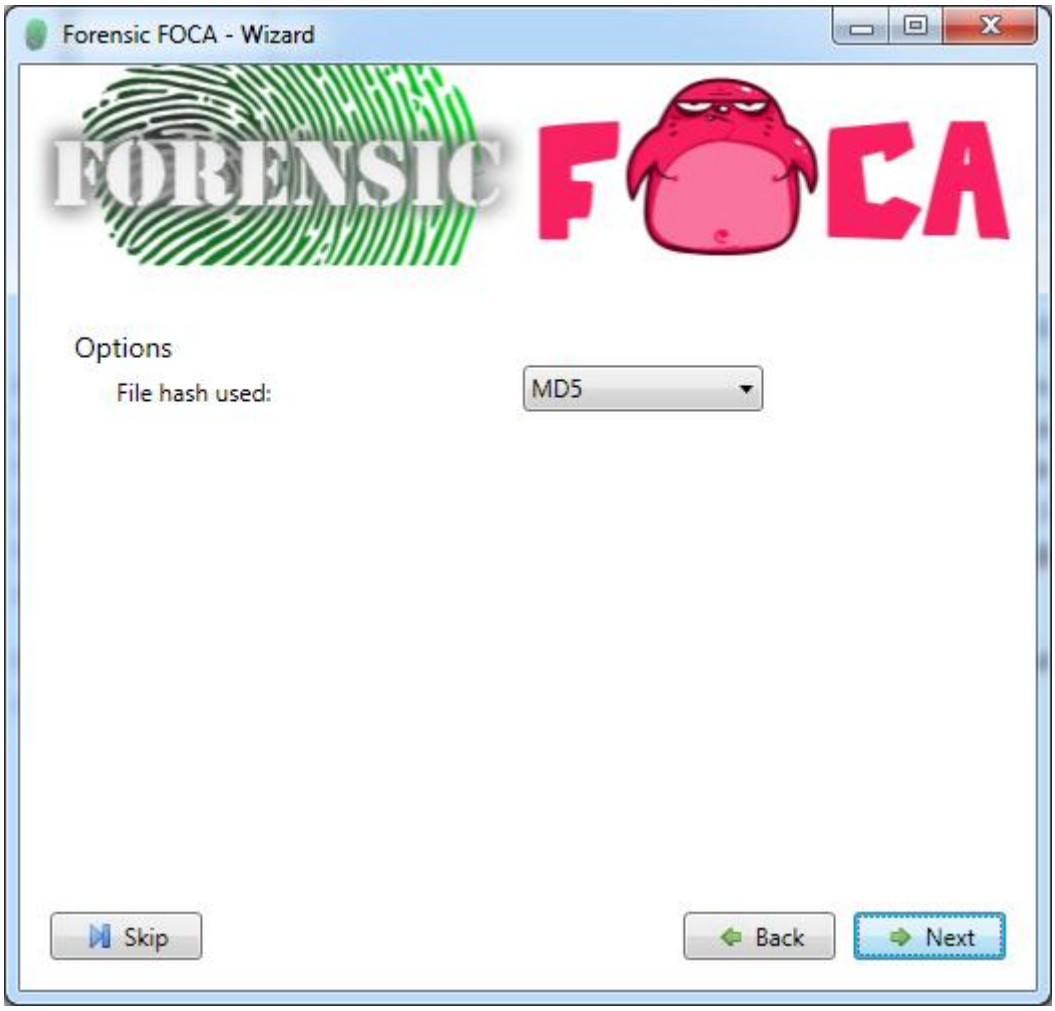
En el primer paso se configura el nombre del proyecto, la fecha y unas notas descriptivas del mismo.

En el segundo punto se debe seleccionar una carpeta desde donde se cargaran los ficheros para ser analizados. Típicamente esta carpeta será una unidad de un equipo distinto que ha sido montada en el equipo local para ser analizada.



En el siguiente apartado se deben seleccionar los tipos de documentos que se quieren analizar. Están por un lado los documentos ofimáticos, en este grupo se encuentran los ficheros PDF, los ficheros de Microsoft Office tanto las versiones antiguas (MS Office 97, 2003) como las nuevas (MS Office 2007, 2010), así como los documentos de OpenOffice, los de WordPerfect. Por otro lado están los ficheros de imágenes, imágenes JPG y su información EXIF, fichero *.svg y aquellos generados con In Design.

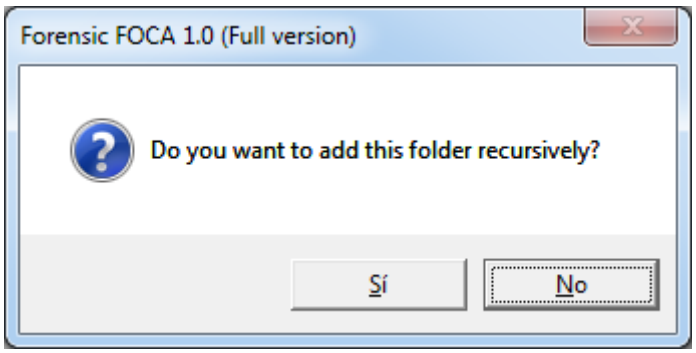
El último apartado del wizard es el de opciones donde se puede elegir el tipo de hash que se utilizará durante todo el proceso.



4. Vista por documentos

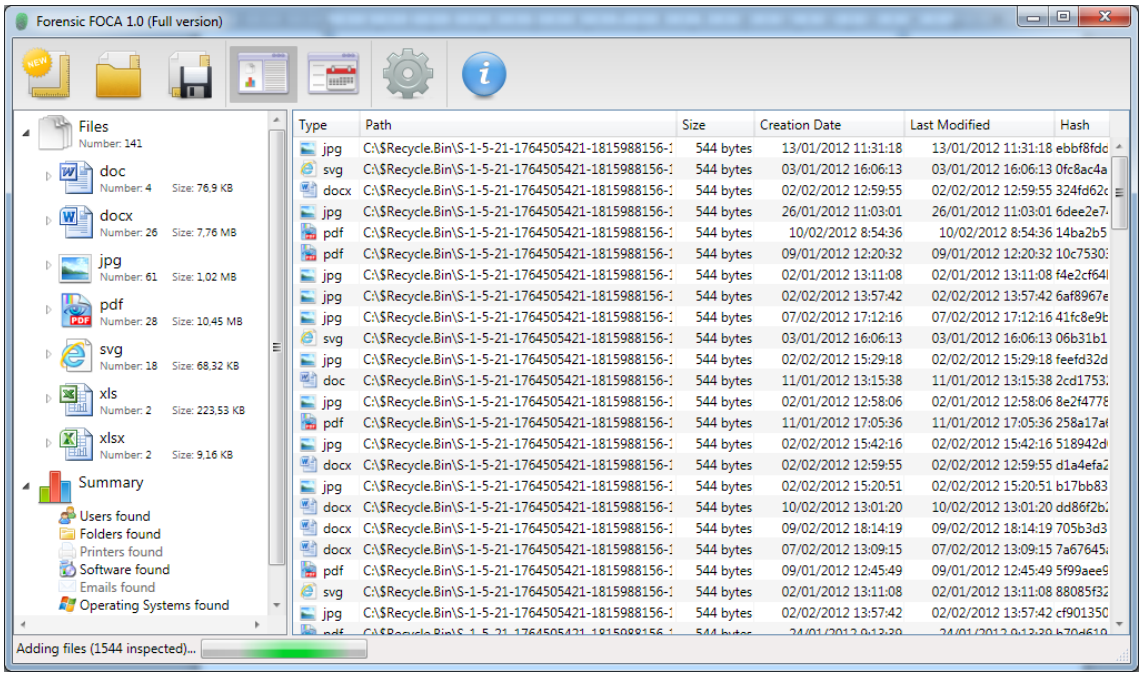
Una vez finalizado todo el proceso se cargará la vista principal de Forensic FOCA, la vista por documentos.

Si se ha seleccionado una carpeta mediante el wizard Forensic FOCA empezará automáticamente a analizar ficheros. En este caso uno de los primeros mensajes que se mostrarán será el siguiente:



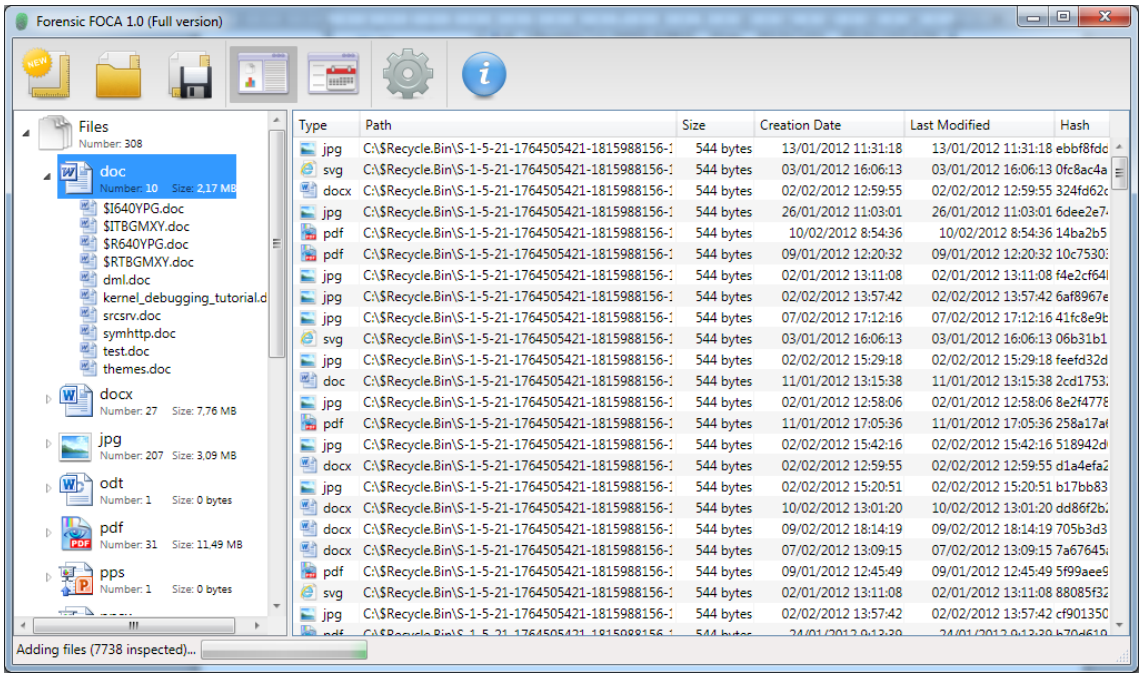
En él se pregunta si se desea analizar recursivamente la carpeta que está siendo añadida, si se selecciona “Si”, se analizaran las subcarpetas recursivamente de la carpeta analizada.

En caso de que no se haya seleccionado una carpeta en el wizard siempre será posible arrastrar carpetas ó ficheros sobre la aplicación y esta los analizara.

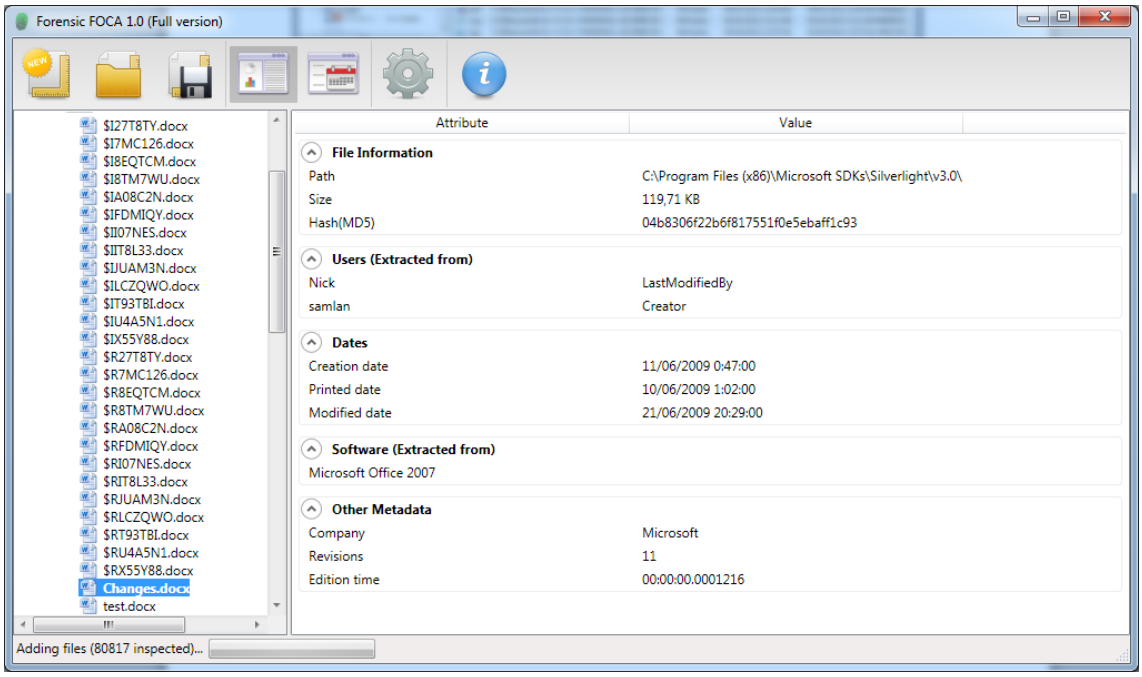


En esta vista a la derecha se muestran los ficheros analizados con su extensión, ruta, tamaño, fecha de creación, de última modificación y el hash. Es posible ordenar la lista haciendo clic sobre las diferentes columnas.

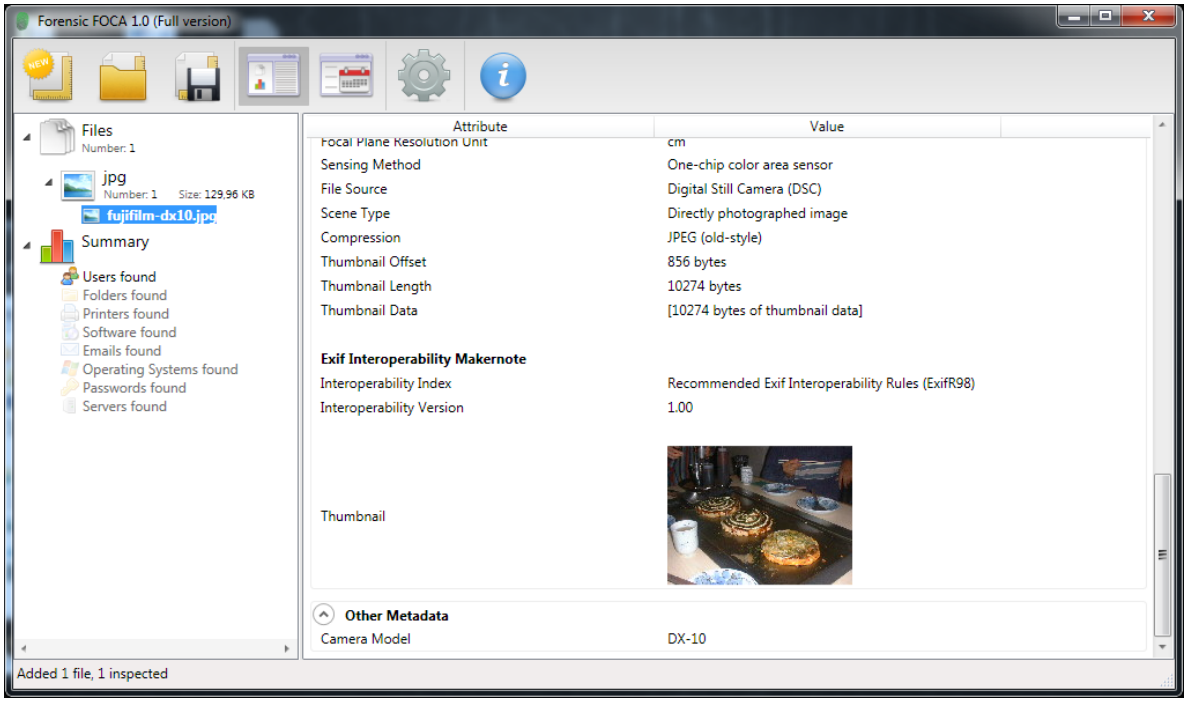
A la izquierda de la vista aparecen arriba los ficheros agrupados por extensión. Es posible desplegar una a una cada extensión.



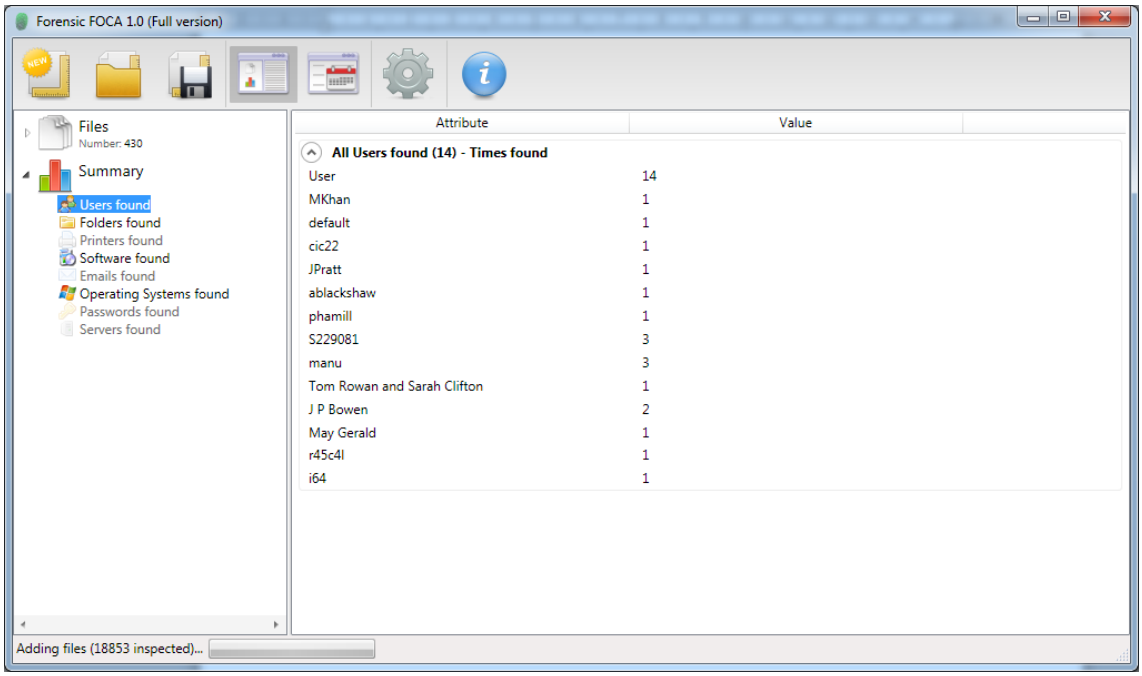
Cuando se selecciona alguno de los documentos se muestra la información del mismo detalladamente, así como los metadatos que se hayan localizado. Estos metadatos dependen altamente del tipo de documento que se analice.



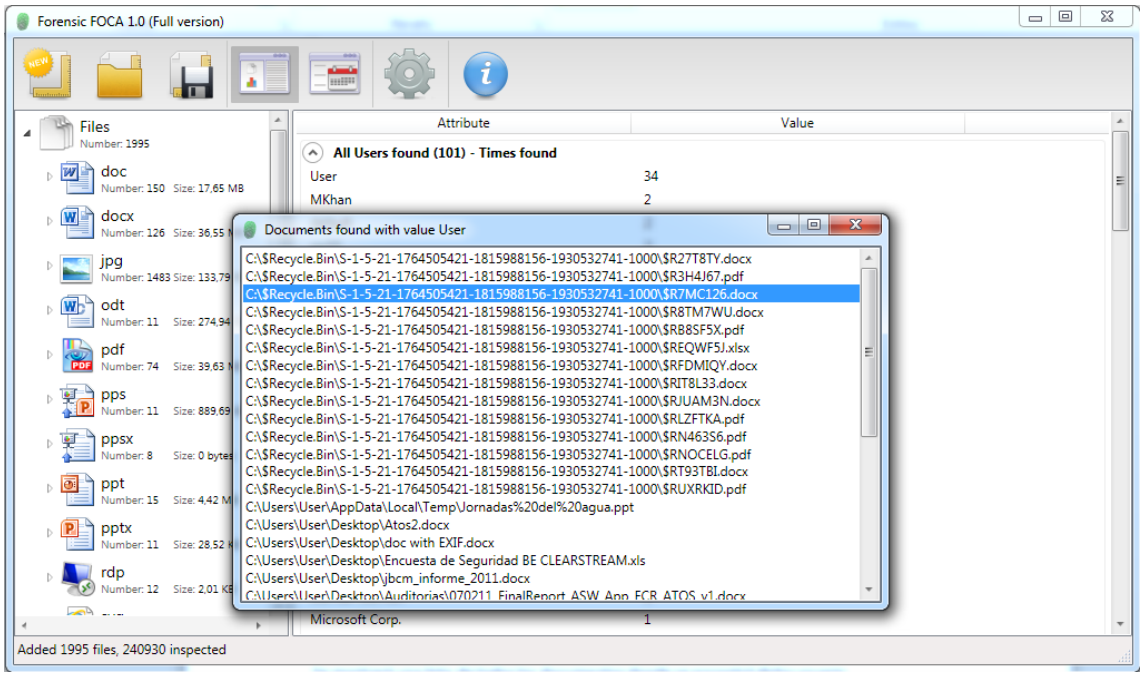
Por ejemplo cuando se analiza un JPG es muy posible que se encuentre información EXIF, incluso una imagen en miniatura de la imagen original.



Otra información interesante que se muestra en el panel izquierdo es el resumen de metadatos. En él pueden verse los usuarios, carpetas, impresoras, aplicaciones, emails, sistemas operativos, contraseñas y servidores encontrados en los metadatos.

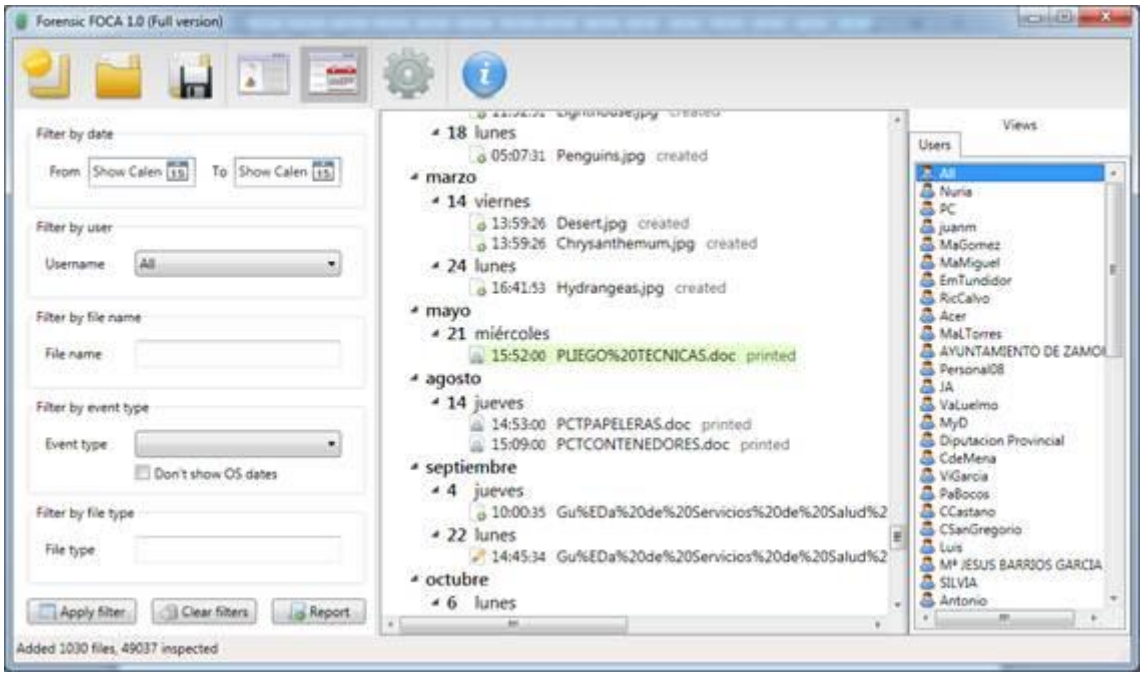


Existe la posibilidad de localizar el documento desde el que se encontró un determinado dato, para ello basta con pulsar el botón derecho del ratón sobre uno de los usuarios encontrados. Se mostrará una lista de todos los documentos donde se encontró dicho usuario y pulsando sobre ellos se mostrarán los detalles del documento.



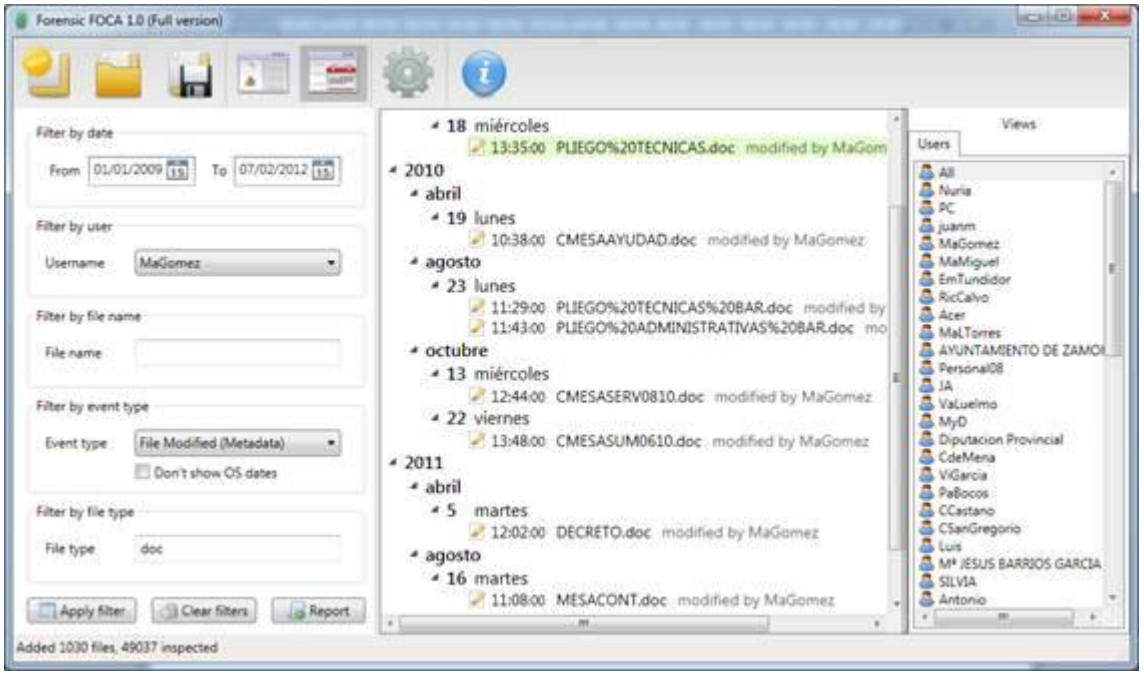
5. Vista Timeline

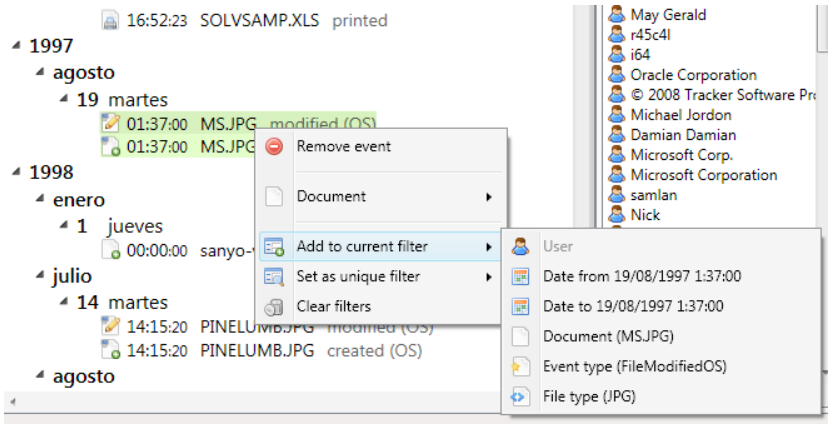
La otra modalidad de visualizar los datos es mediante un Timeline donde se muestran los eventos relacionados con los ficheros organizados por fechas. De este modo es posible visualizar rápidamente los eventos ocurridos en una determinada fecha.



Los diferentes eventos que existen son la creación, modificación e impresión de documentos, esta información es obtenida de los metadatos. También se obtienen fechas desde el propio sistema operativo, pero estas pueden ser erróneas si los ficheros han sido copiados o movidos.

Para que sea cómodo moverse entre toda la lista de información se ha añadido un sistema de filtrado por fechas, por tipo de documentos, por usuarios, por tipo de evento y por extensión que puede accederse desde el panel izquierdo o a través del menú contextual.

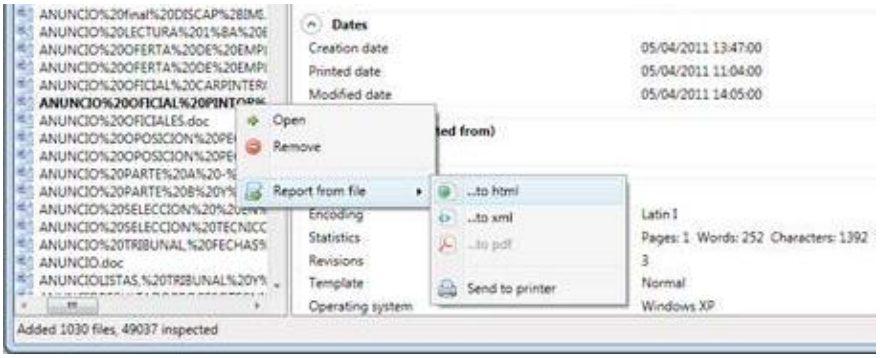


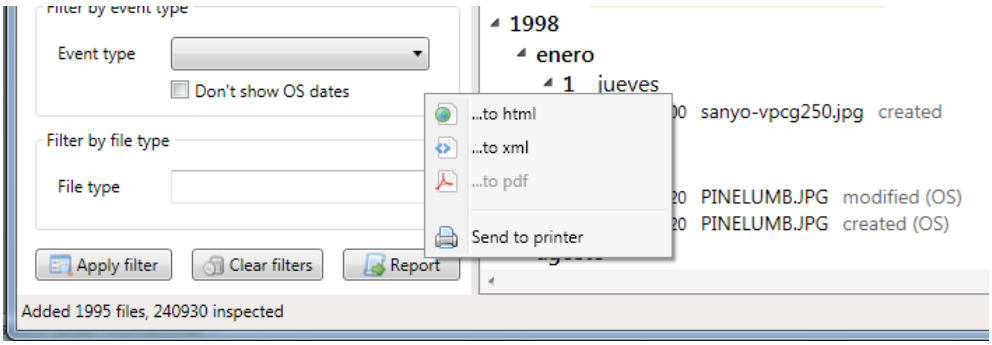


A la derecha se encuentra una vista de usuarios este sistema hace que baste con hacer clic en un usuario para que se acceda a la línea temporal de esa única persona.

6. Exportación de resultados

Forensic FOCA permite exportar toda la información obtenida en los formatos XML o HTML para utilizar dicha información como más convenga, así como imprimir estos datos. Es posible exportar datos por documento, por tipo de documento, mediante los resúmenes o desde el Timeline.

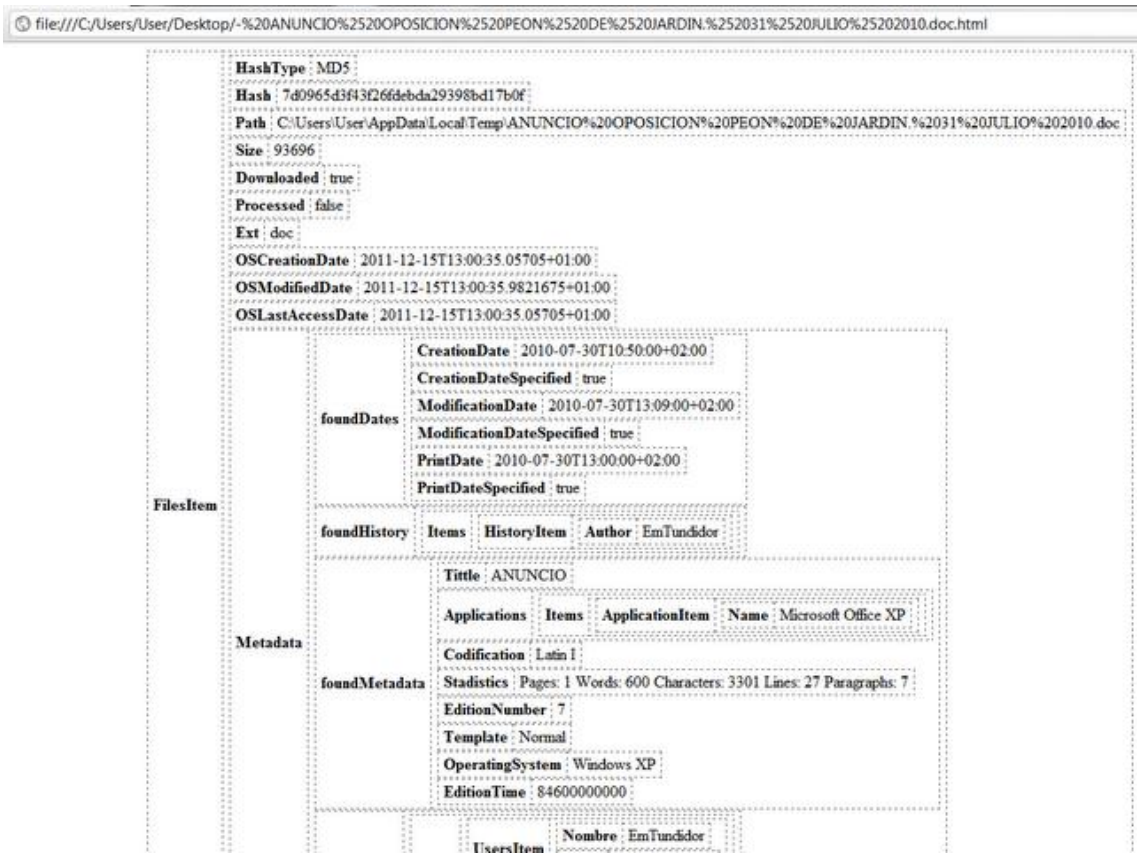




Los datos exportados en XML se visualizan de la siguiente manera:

```xml
<?xml version="1.0"?>
<FilesItem xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <Info />
  <HashType>MD5</HashType>
  <Hash>7d0965d3f43f26fdebda29398bd17b0f</Hash>
  <Path>C:\Users\User\AppData\Local\Temp\ANUNCIO%20OPOSICION%20PEON%20DE%20JARDIN.%2031%20JULIO%202010.doc</Path>
  <Size>93696</Size>
  <Downloaded>true</Downloaded>
  <Processed>false</Processed>
  <Ext>doc</Ext>
  <OSCreationDate>2011-12-15T13:00:35.05705+01:00</OSCreationDate>
  <OSModifiedDate>2011-12-15T13:00:35.9821675+01:00</OSModifiedDate>
  <OSLastAccessDate>2011-12-15T13:00:35.05705+01:00</OSLastAccessDate>
  <Metadata xsi:type="Office972003">
    <foundEmails>
      <Items />
    </foundEmails>
    <foundDates>
      <CreationDate>2010-07-30T10:50:00+02:00</CreationDate>
      <CreationDateSpecified>true</CreationDateSpecified>
      <ModificationDate>2010-07-30T13:09:00+02:00</ModificationDate>
      <ModificationDateSpecified>true</ModificationDateSpecified>
      <PrintDate>2010-07-30T13:00:00+02:00</PrintDate>
      <PrintDateSpecified>true</PrintDateSpecified>
    </foundDates>
    <foundPrinters>
      <Items />
    </foundPrinters>
```


Y en HTML se visualiza de esta otra manera



7. Salvar cargar proyectos

Forensic FOCA permite guardar un proyecto y cargarlo mas adelante. Para guardar basta con pulsar sobre el botón “Save Project”.

El fichero se guardara con la extensión FF.

El proceso de carga es sencillo basta con pulsar el botón “Open Project” y seleccionar el fichero anteriormente guardado.