www.eysglobal.com

MÓDULO 3
PRACTICA 3:

Realización práctica del proceso de recopilación de evidencias y análisis de las mismas. Los asistentes se familiarizan con el proceso y con las herramientas más comúnmente utilizadas en el Análisis Informático Forense.

- 3.2.1 Análisis informático con distintas herramientas software de investigación

Utilización de herramientas:

- ● Encase
- ● WinHex

METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

El celular se ha convertido en el medio masivo de comunicación por excelencia gracias a su portabilidad, servicios y bajos costos en las tarifas. Esta explosión tecnológica que no da tregua, nos sorprende con la gran variedad de sofisticados equipos y la frecuencia vertiginosa con la que unos modelos dejan en la obsolescencia a los modelos anteriores.

Nuevos servicios como la transmisión de vídeo digital, fotografía, posicionamiento global, wi-fi, capacidad para ejecutar una gran variedad de aplicaciones, han hecho de este medio de comunicación, un dispositivo que se utiliza hoy en día por millones de personas en el mundo para algo mas que hacer una llamada.

METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

Las compañías y organismos de seguridad estatales, reúnen sus esfuerzos para crear nuevas técnicas de análisis forense, esta vez orientadas a los dispositivos móviles, entre ellos los celulares. Aunque si bien es cierto, la dificultad para que estas técnicas sean exitosas en la investigación criminal, no se puede considerar como un medio para frenar el avance que como herramienta, viene siendo utilizado el celular. A continuación, veremos una herramienta de gran popularidad entre los organismos de seguridad de muchos gobiernos, utilizada para la investigación forense en celulares, oxigen forensic suite 2010, que pueden descargar una versión trial de http://www.oxygen-forensic.com/en/.

METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

Voy a omitir los detalles de instalación y de activación del software, cabe anotar, que cuando te registras para realizar la descarga del trial, te envían un serial al correo electrónico de registro, y te da la posibilidad de ejecutar la aplicación 30 veces, tiempo suficiente para conocer las bondades de esta aplicación.

En nuestro ejemplo, utilizaremos un celular marca Nokia modelo 5530 XpressMusic y lo enlazaremos con oxigen forensic suite 2010, usando una conexión bluetooth, IMPORTANTE!!! No deben tener en ejecución ningún software como pc suite, u otro de celulares, esto impide la conexión, de igual forma, como observaran, no activaremos el celular en modo conexión de transferencia de datos, usaremos según el modelo, la opción de conexión con pc suite, pero recuerden no tenerlo ejecutando en el sistema.

METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

Primeros pasos para realizar el análisis forense de un celular

Conectamos el celular al PC, oxigen forensic suite 2010 nos da la posibilidad de usar tres modos de conexión, vía cable, bluetooth o infrarrojos; en nuestro ejemplo, utilizaremos una conexión bluetooth, ya que los celulares de gama media/alta, cuentan generalmente con este medio de comunicación, y es una ventaja frente a la gran variedad de cables de conexión existente de acuerdo al modelo o marca del equipo de comunicaciones.

Cuando iniciamos la suite, nos sale un marco de trabajo bastante intuitivo y amigable, no se requiere ser un bilingüe para identificar los menús y su aplicación.

Una vez se inicia la aplicación, debemos proceder a detectar el dispositivo, en el siguiente cuadro, oxigen forensic suite 2010 nos permite seleccionar el medio que estamos utilizando para la conexión del dispositivo.

METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

Seleccionamos la marca y el modelo del celular, recuerden que oxigen forensic suite 2010 puede detectar más de 15.000 dispositivos.

METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

En el siguiente paso seleccionamos el drivers de conexión usb, en nuestro caso, he seleccionado el driver genérico de Microsoft.

METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

En el siguiente paso, iniciamos la detección del dispositivo.

METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

En la siguiente imagen podemos ver como la suite ha detectado el dispositivo

METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

En esta parte del proceso, nos aparece otra ventana donde nos da tres opciones para continuar, la primera opción, que es la que debemos seleccionar si es la primera conexión del teléfono, es el instalar el programa cliente de oxigen forensics 2010 en el celular. Pueden surgir muchos comentarios e interrogantes en esta parte del proceso, y es, “se invalida la evidencia obtenida?”; si analizamos un poco, los datos a examinar o evaluar en un dispositivo móvil, en este caso un celular, es la información referente a contactos, llamadas realizadas o recibidas, tiempos y fecha de duración, números telefónicos entrantes y salientes, mensajes, fotografías, etc. Por lo tanto, no debería invalidarse ya que se conserva la integridad de los datos de interés para la investigación.

METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

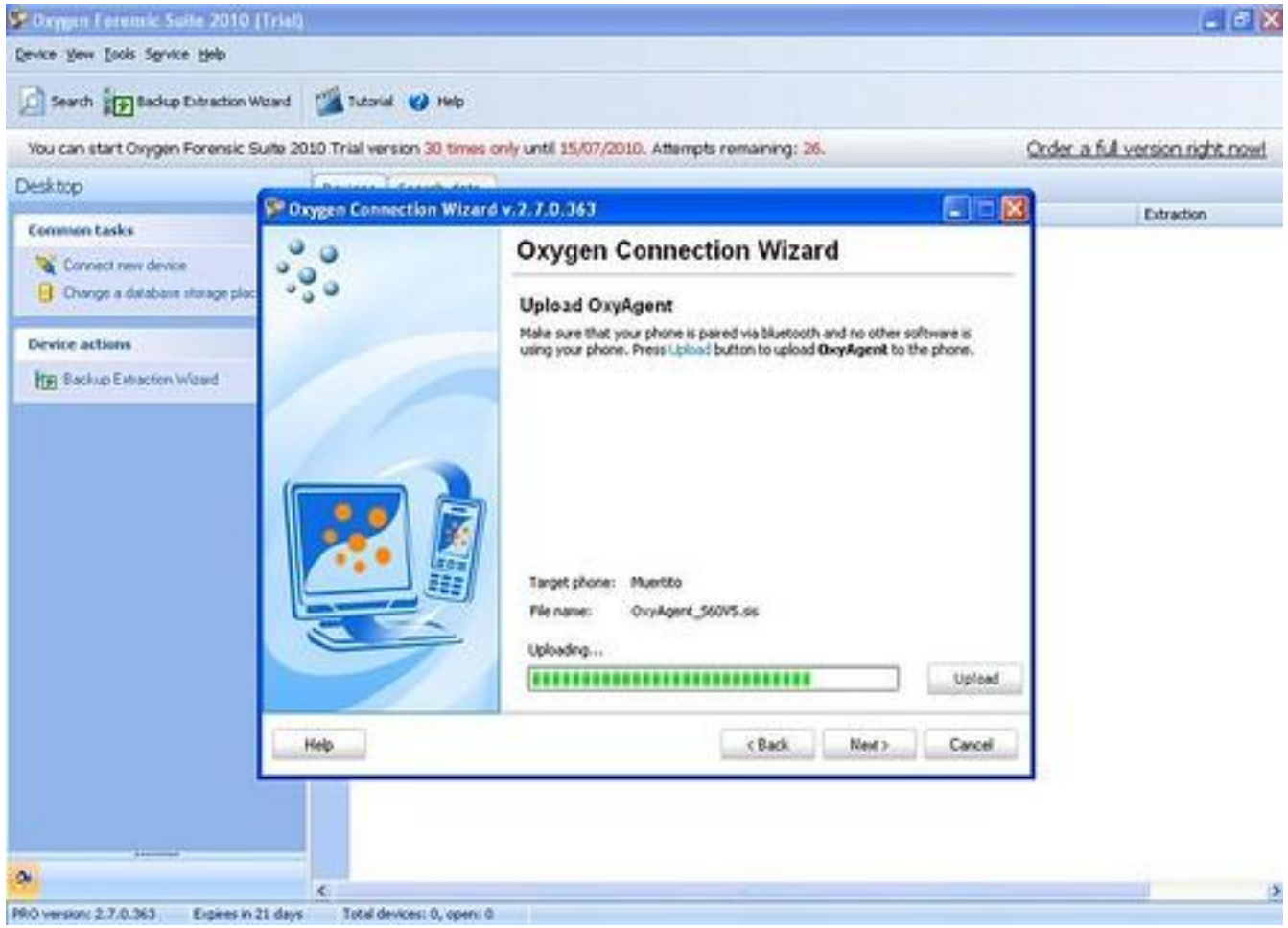
Existen otras alternativas para la extracción de datos sin instalación de programa cliente, que se tratara en futuros artículos y de acuerdo al interés particular sobre el mismo.

Para nuestro ejemplo, hemos seleccionado la primera opción

De clic en next (siguiente), en la ventana a continuación se iniciará el proceso de transferencia en el momento que le de click en el botón Upload, como toda aplicación, primero se transfiere el setup al celular, una vez finaliza la transferencia, aparecerá en pantalla del móvil un mensaje indicándole si desea instalar la aplicación, permítale instalarla y siga los pasos a continuación.

METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

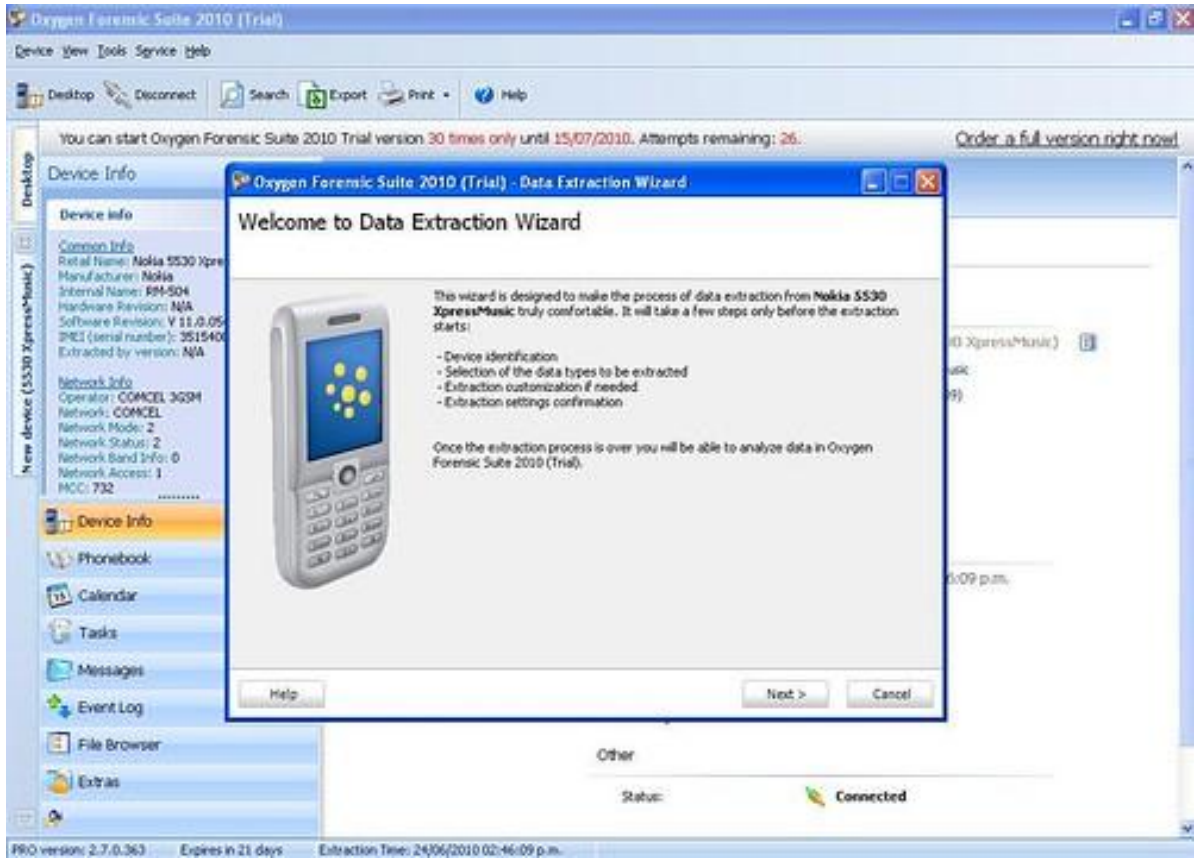
METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES



METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

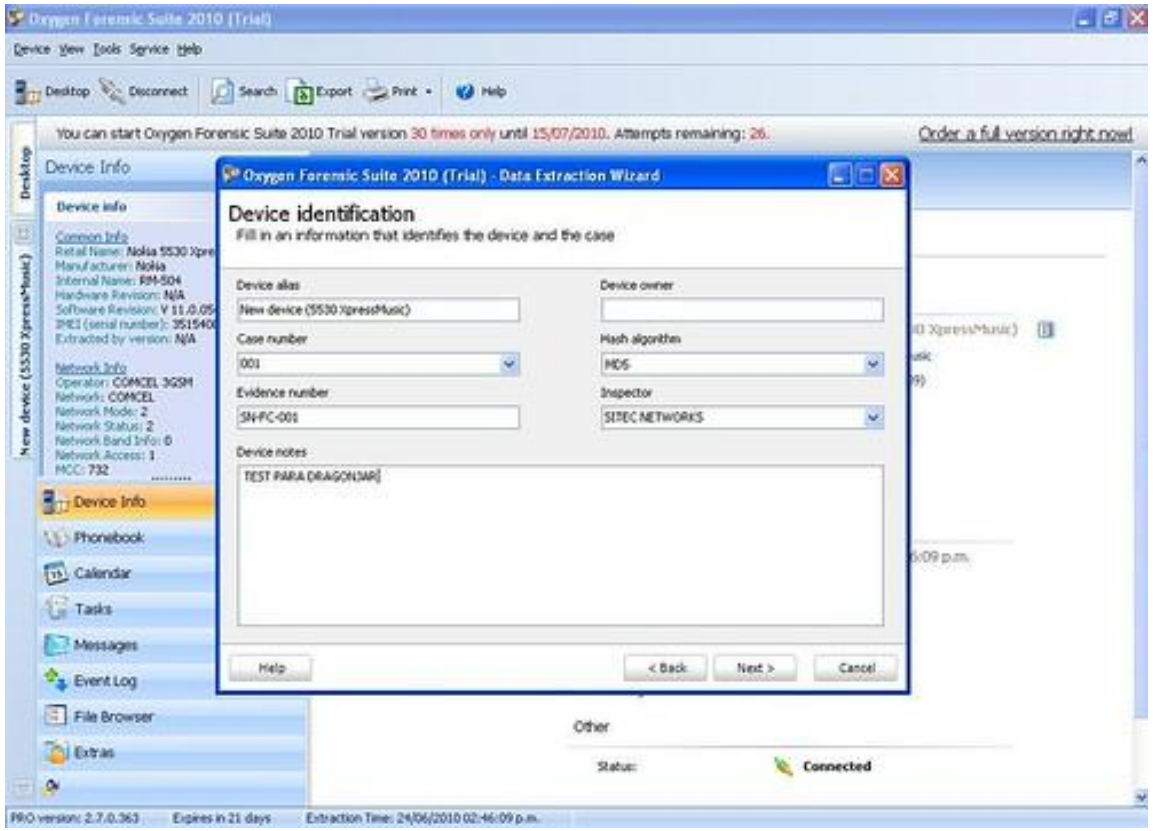
METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

A partir de este momento se inicia el asistente para la extracción de datos.

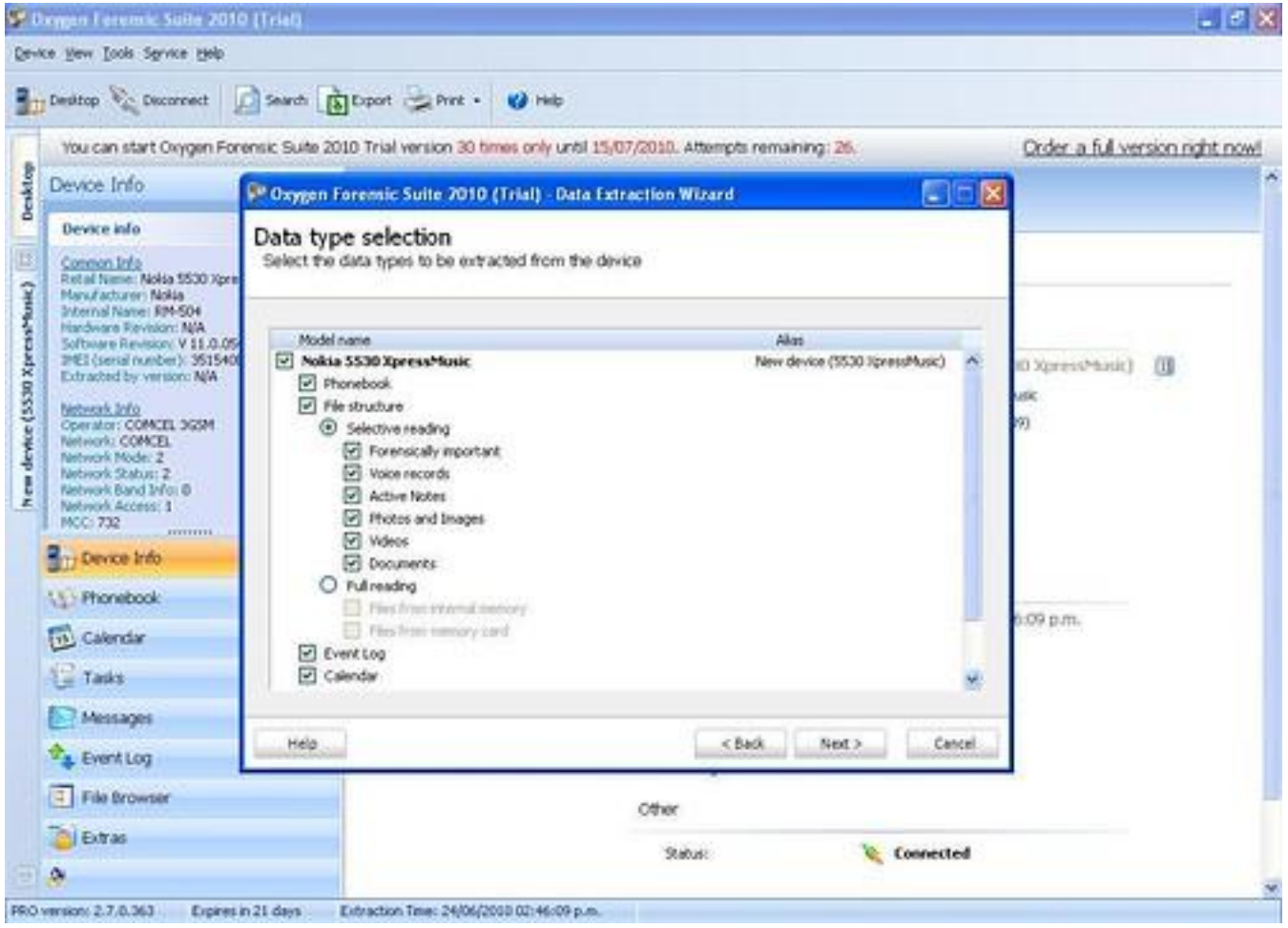


METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

Damos clic en siguiente (next), en la siguiente ventana se colocan los datos de información para identificar el caso

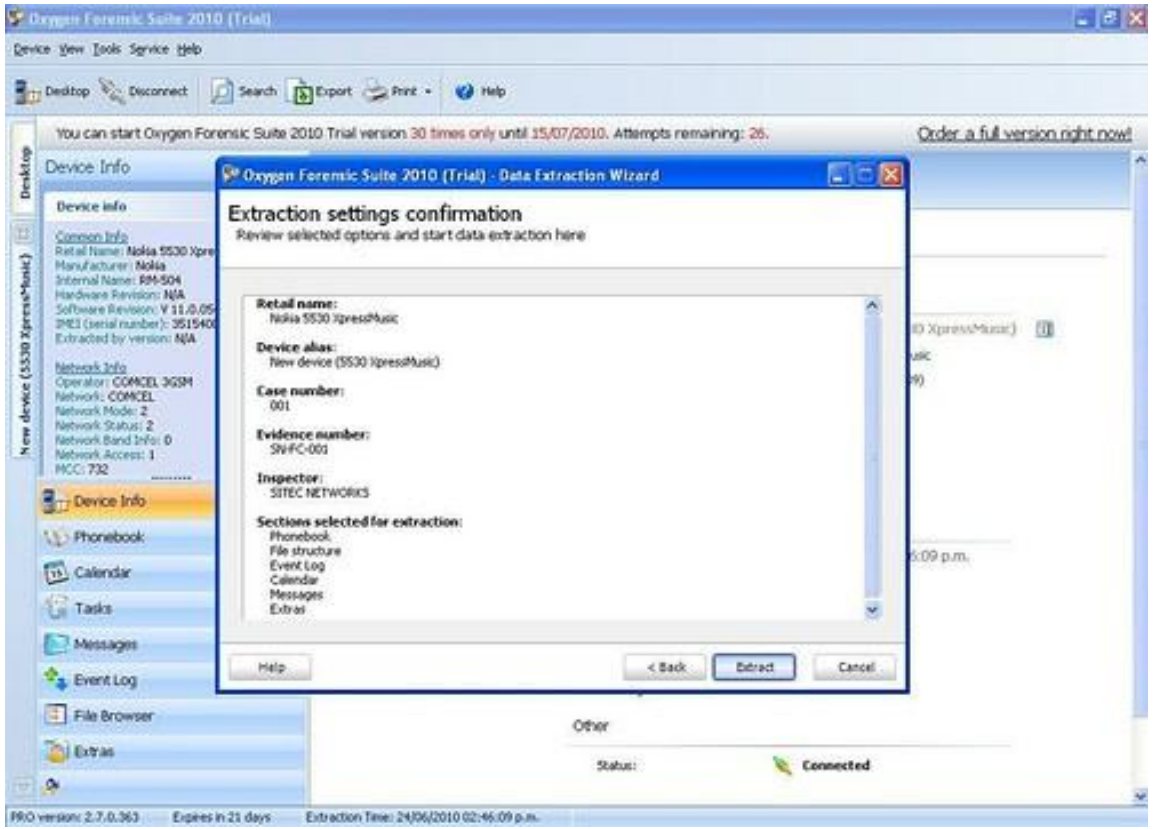


METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES



METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

Se nos da en el siguiente cuadro un informe de confirmación, damos en siguiente (next).

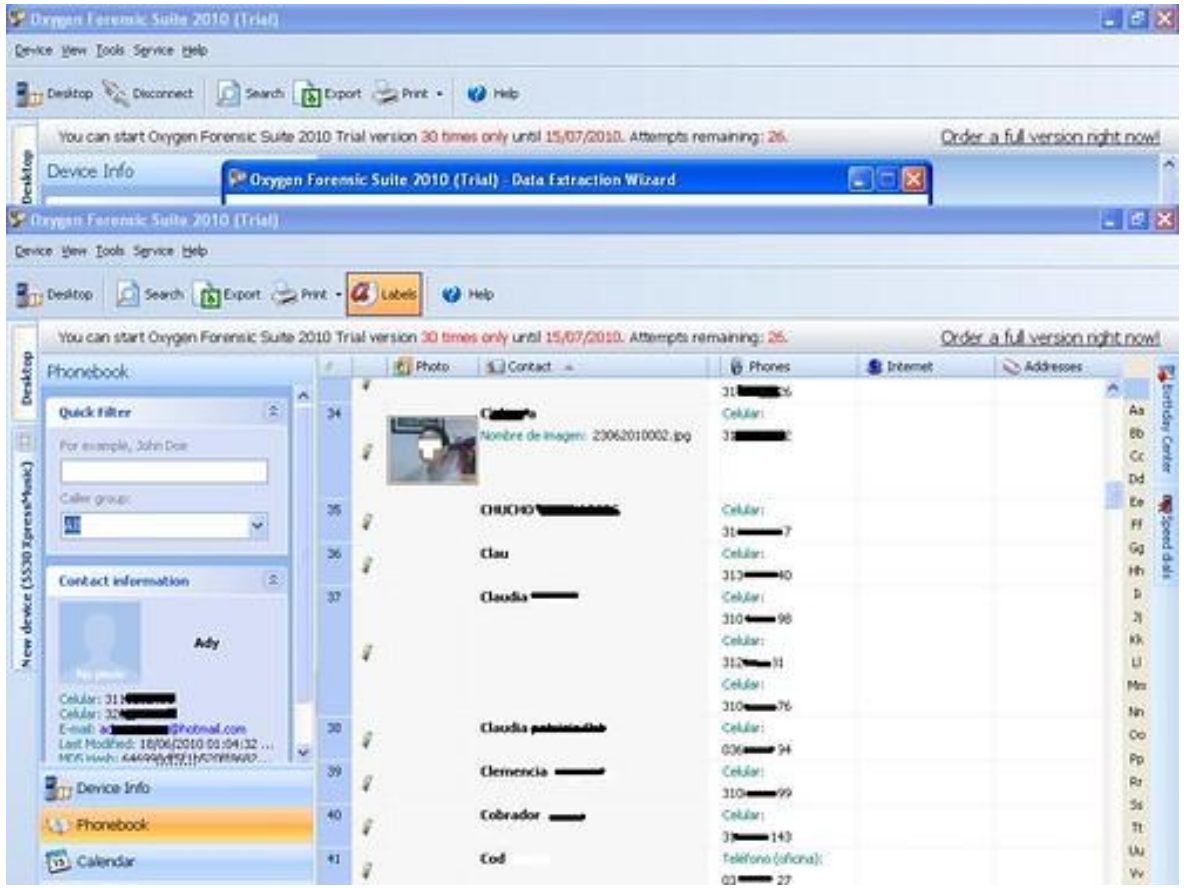


METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

se mostraràn algunas pantallas de la información que se puede extraer con esta aplicación se menciono en un principio, es una aplicación usada por los cuerpos de seguridad de más de 50 países en el mundo.
veamos los pantallazos.

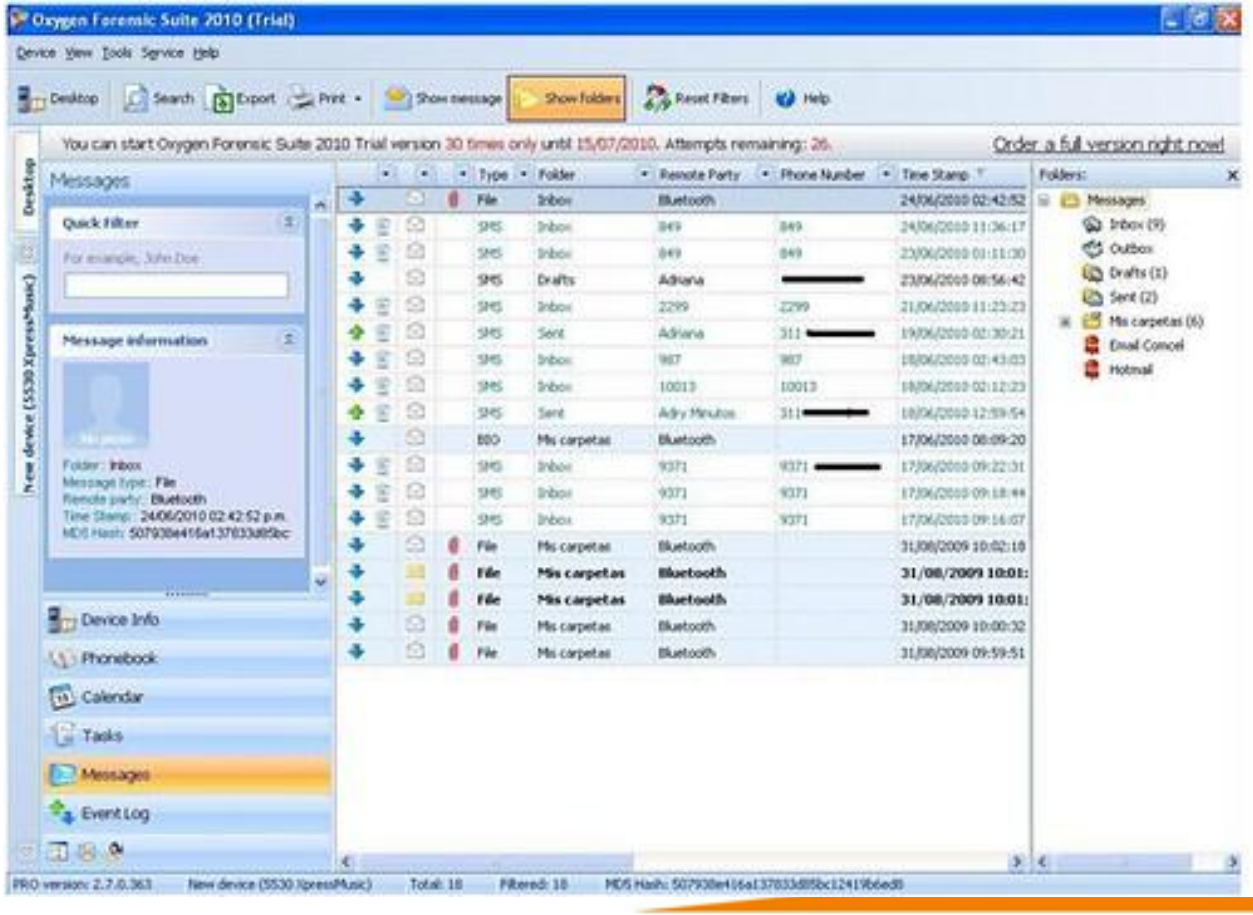
METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

Directorio de Contactos con su respectiva foto.



METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

Listado de Mensajes SMS



METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

Opciones por categorías.