



VE&S

Engineering & Services



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

¿YA REGISTRASTE EL IMEI DE TU CELULAR?

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, oxygen 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



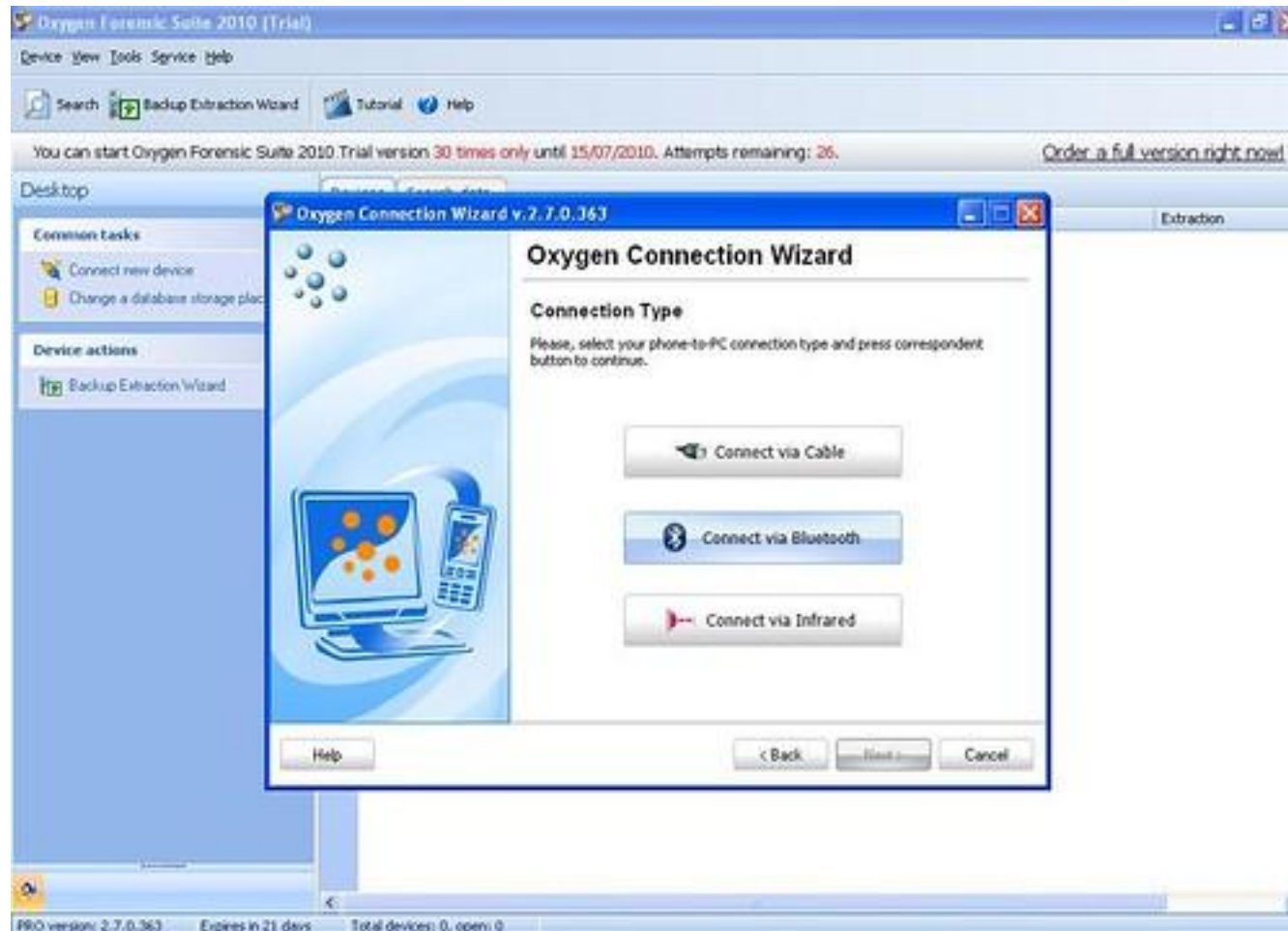
Primeros pasos para realizar el análisis forense de un celular

Conectamos el celular al PC, oxygen 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.

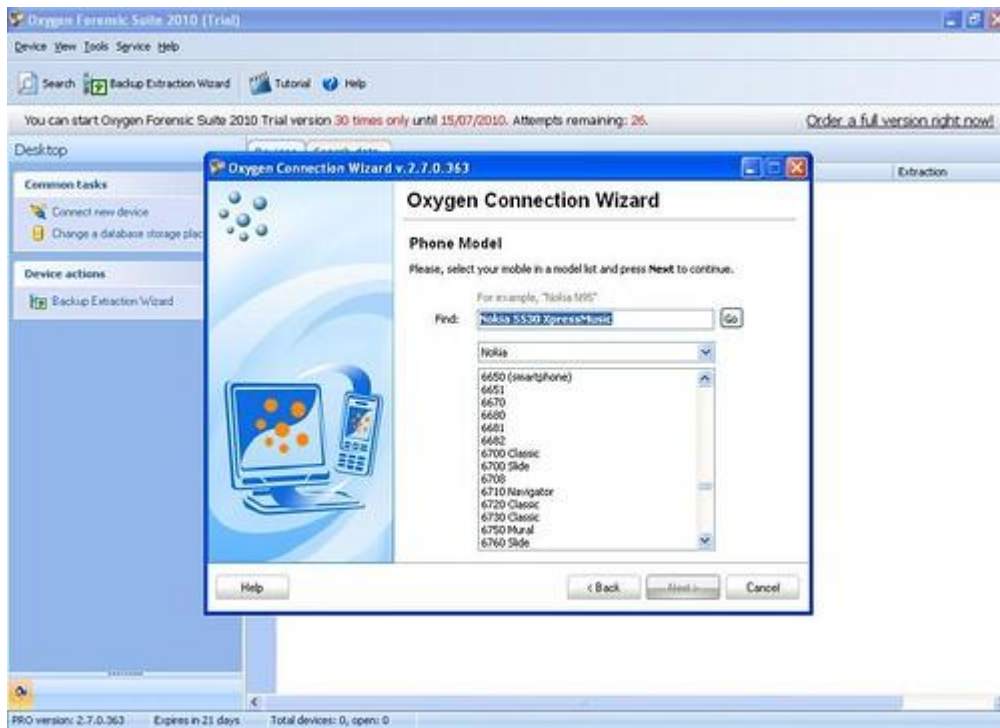
Una vez se inicia la aplicación, debemos proceder a detectar el dispositivo, en el siguiente cuadro, oxygen forensic suite 2010 nos permite seleccionar el medio que estamos utilizando para la conexión del dispositivo.

METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES



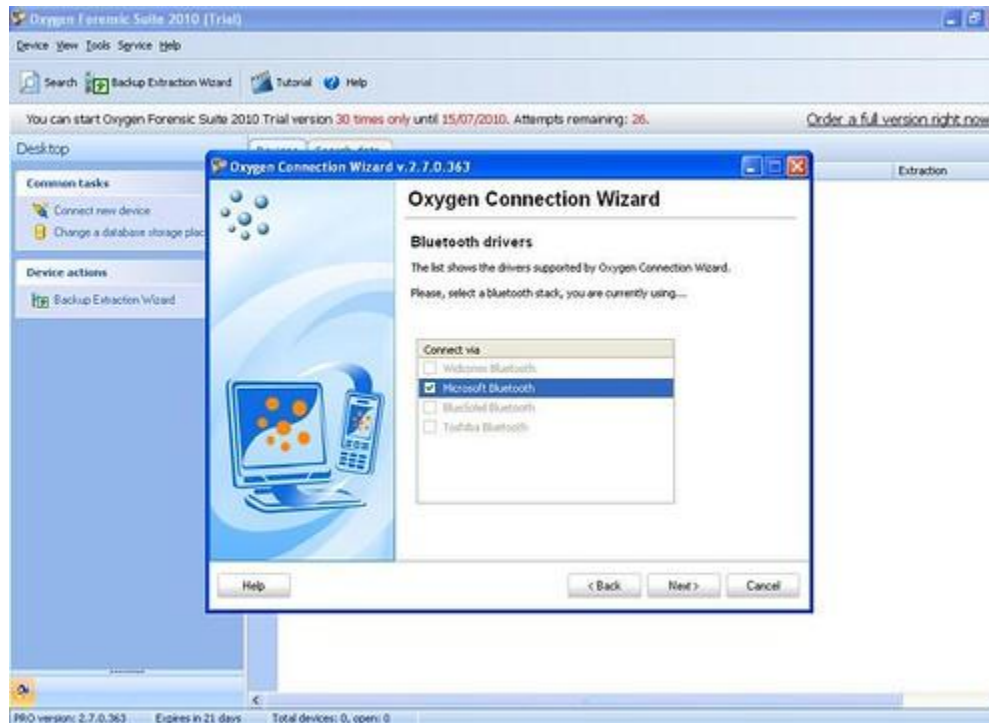
METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

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



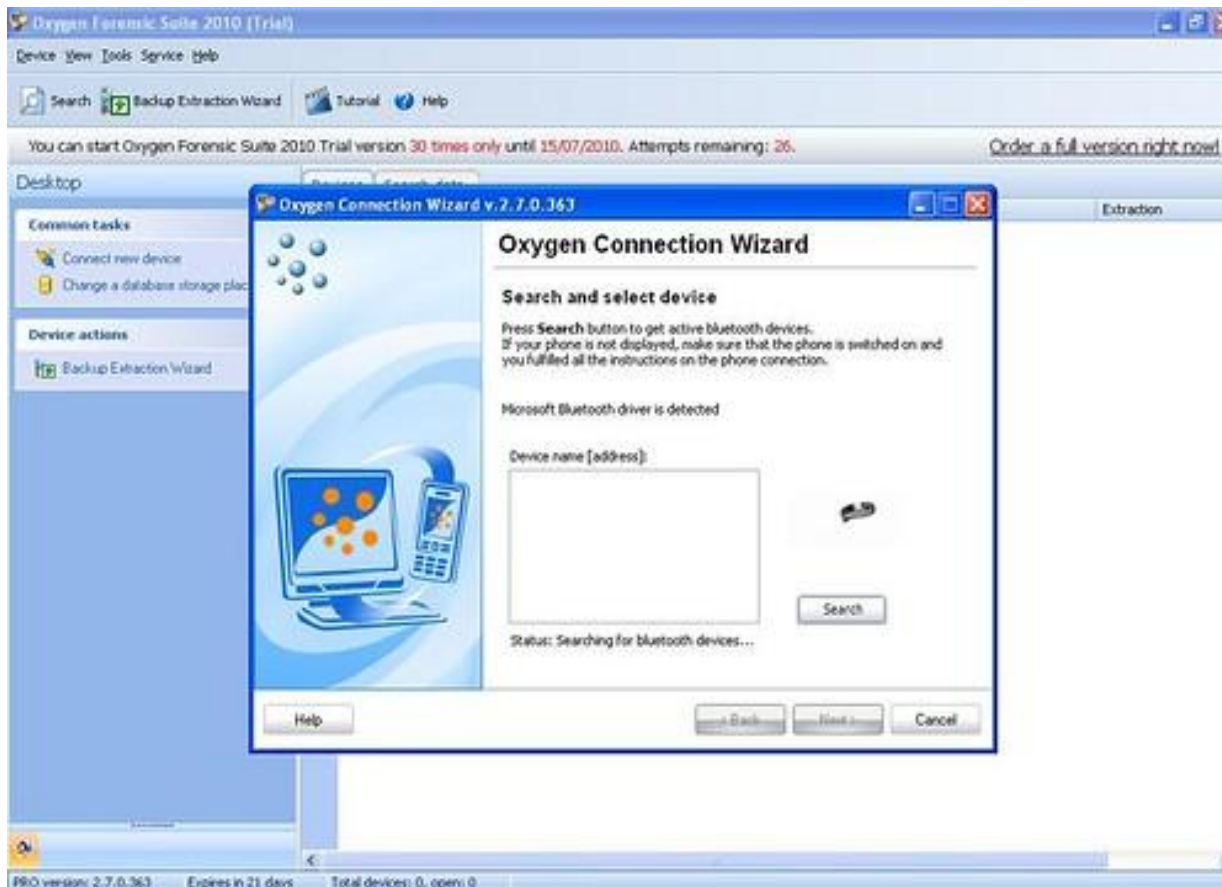
METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

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



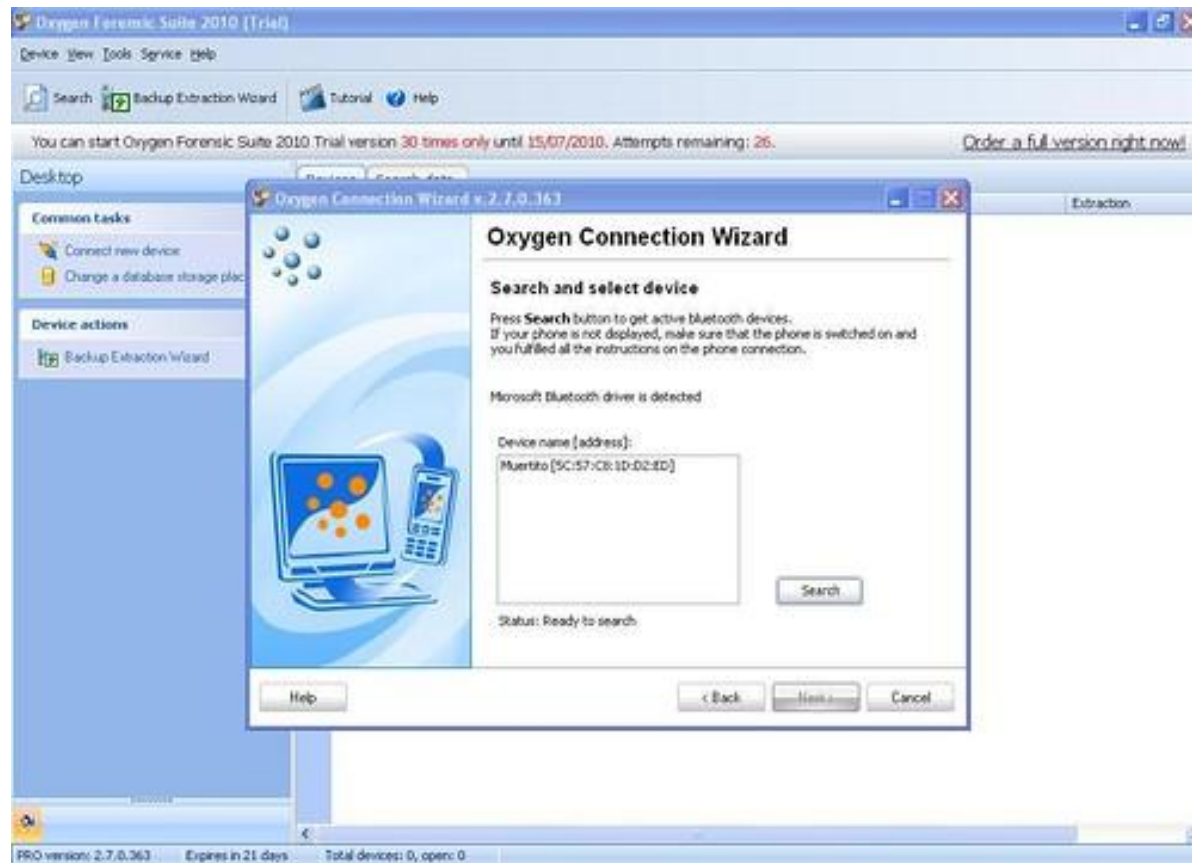
METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

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

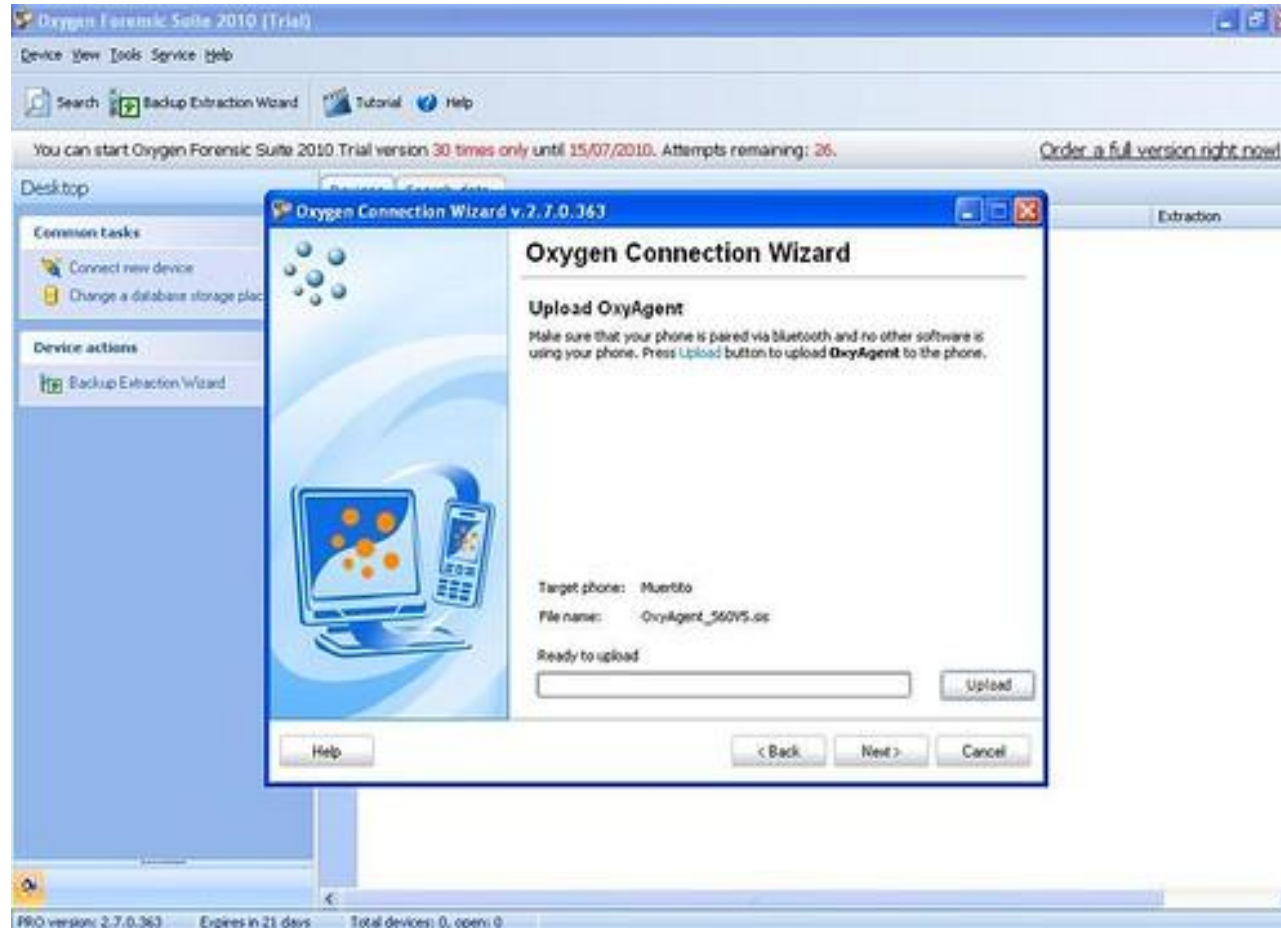


Existen otras alternativas para la extracción de datos sin instalación de programa cliente, que se tratara en futuros artículos y de acuerdo al interés particular sobre el mismo.

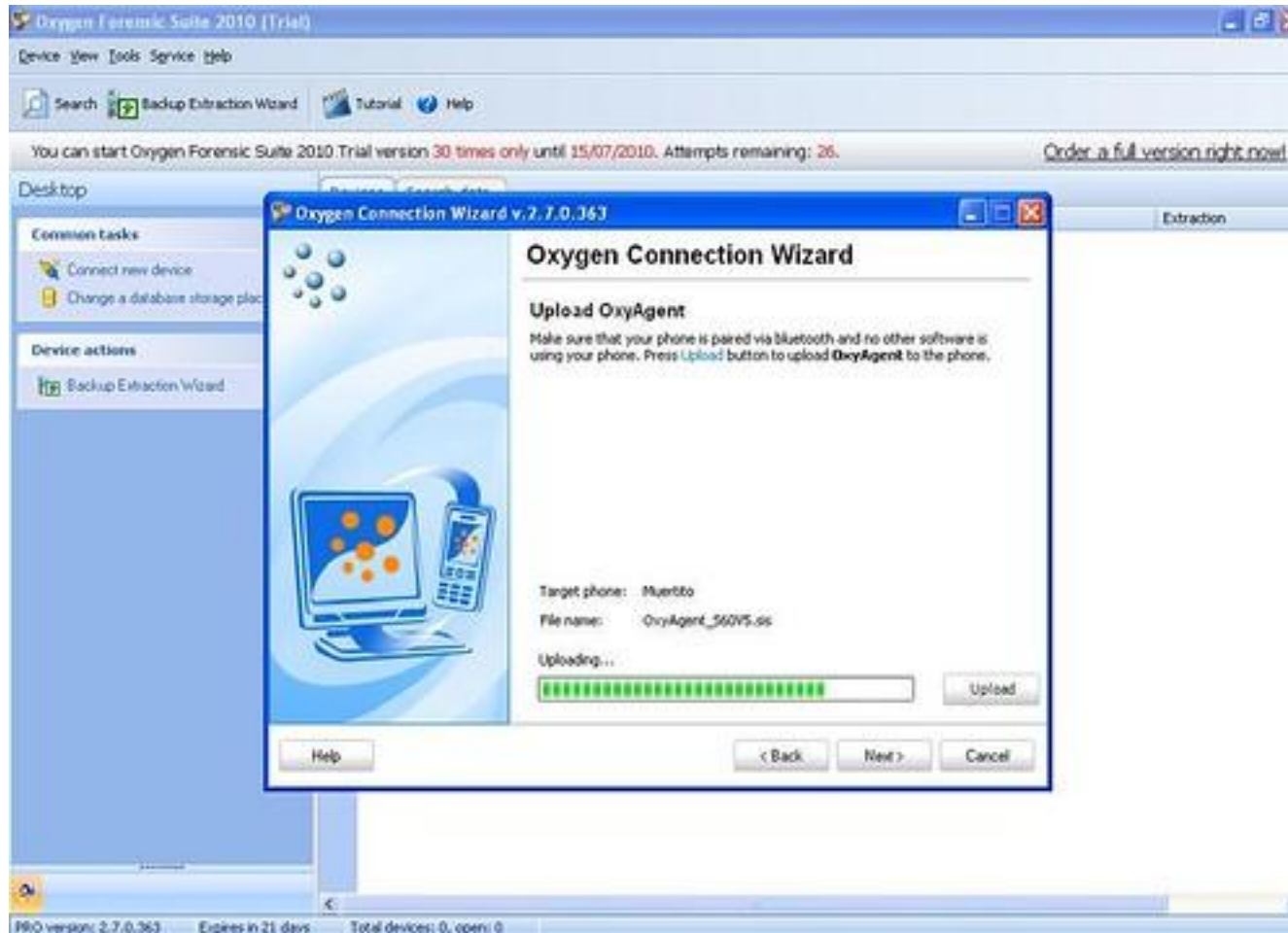
Para nuestro ejemplo, hemos seleccionado la primera opción

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.

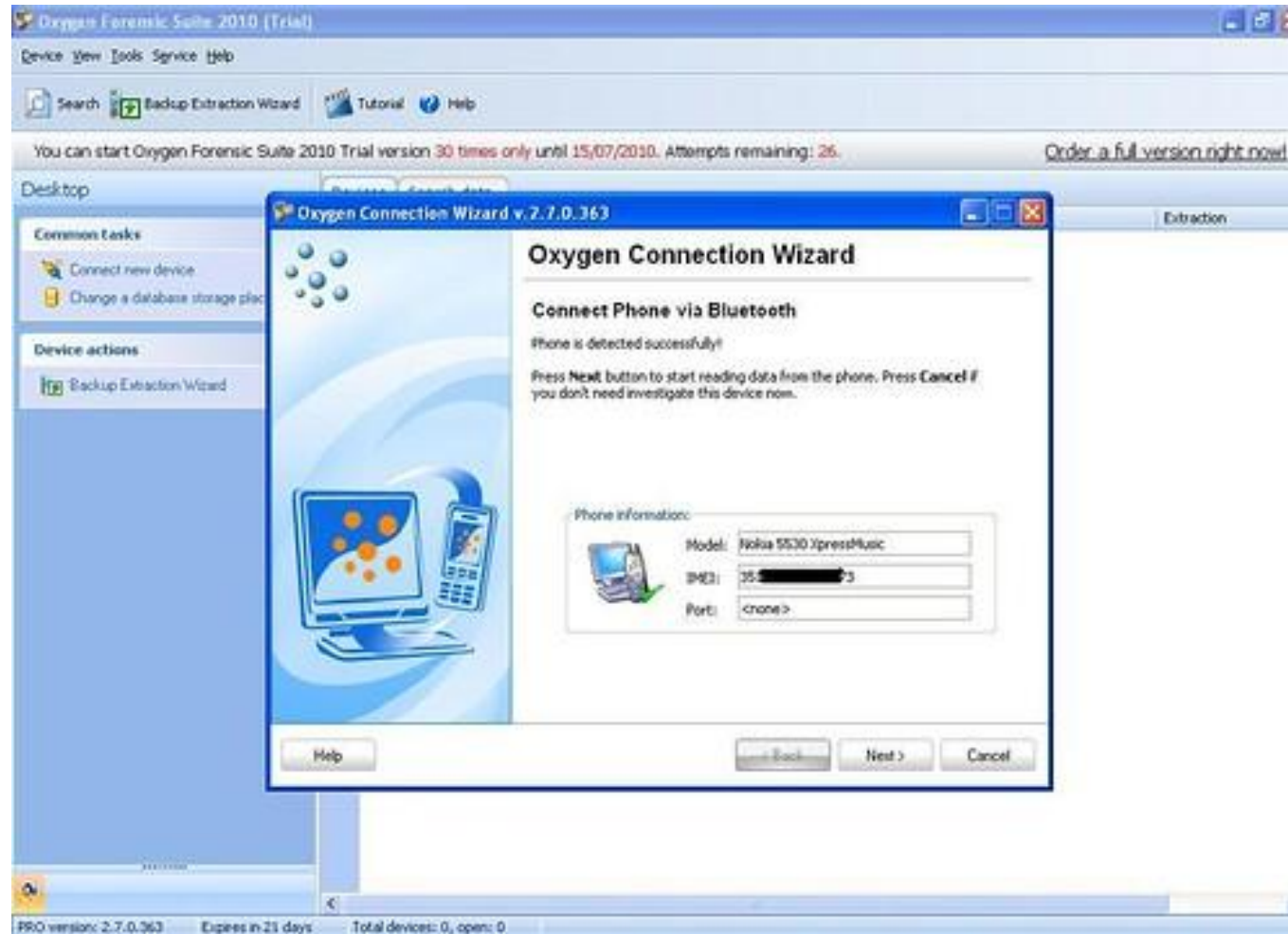
METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES



METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES



METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES



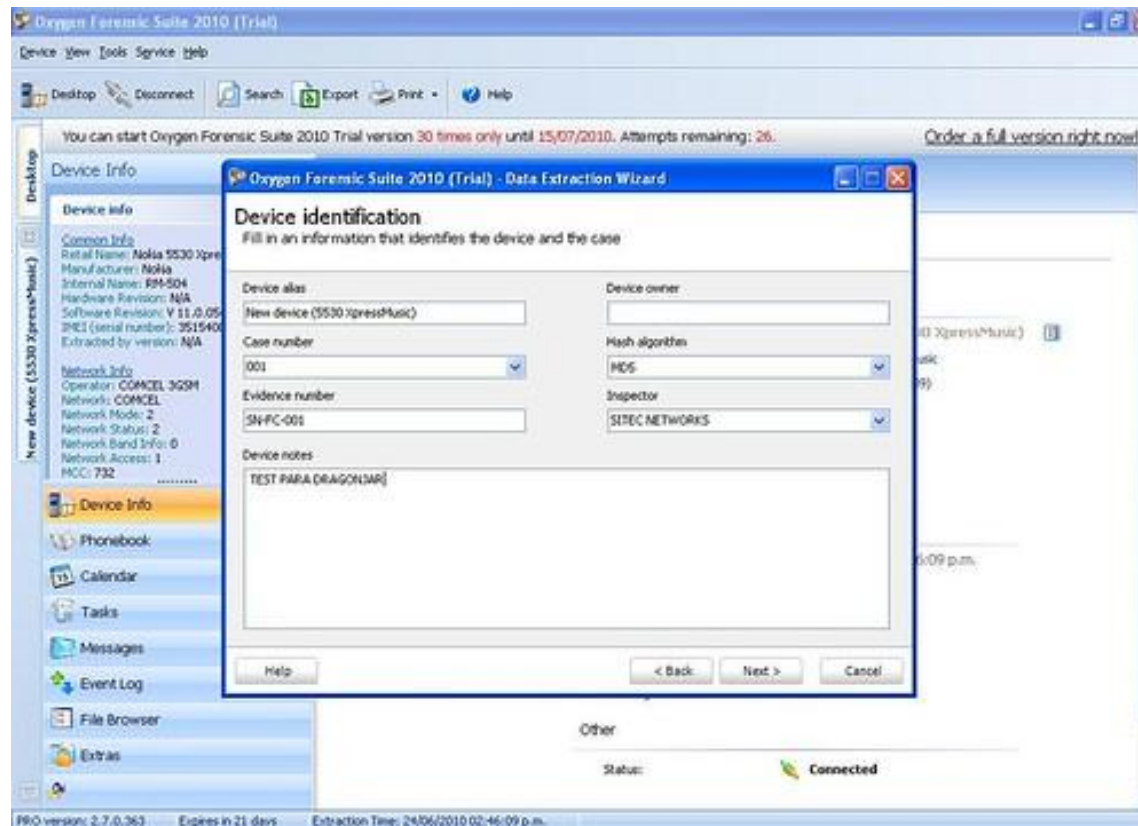
METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

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

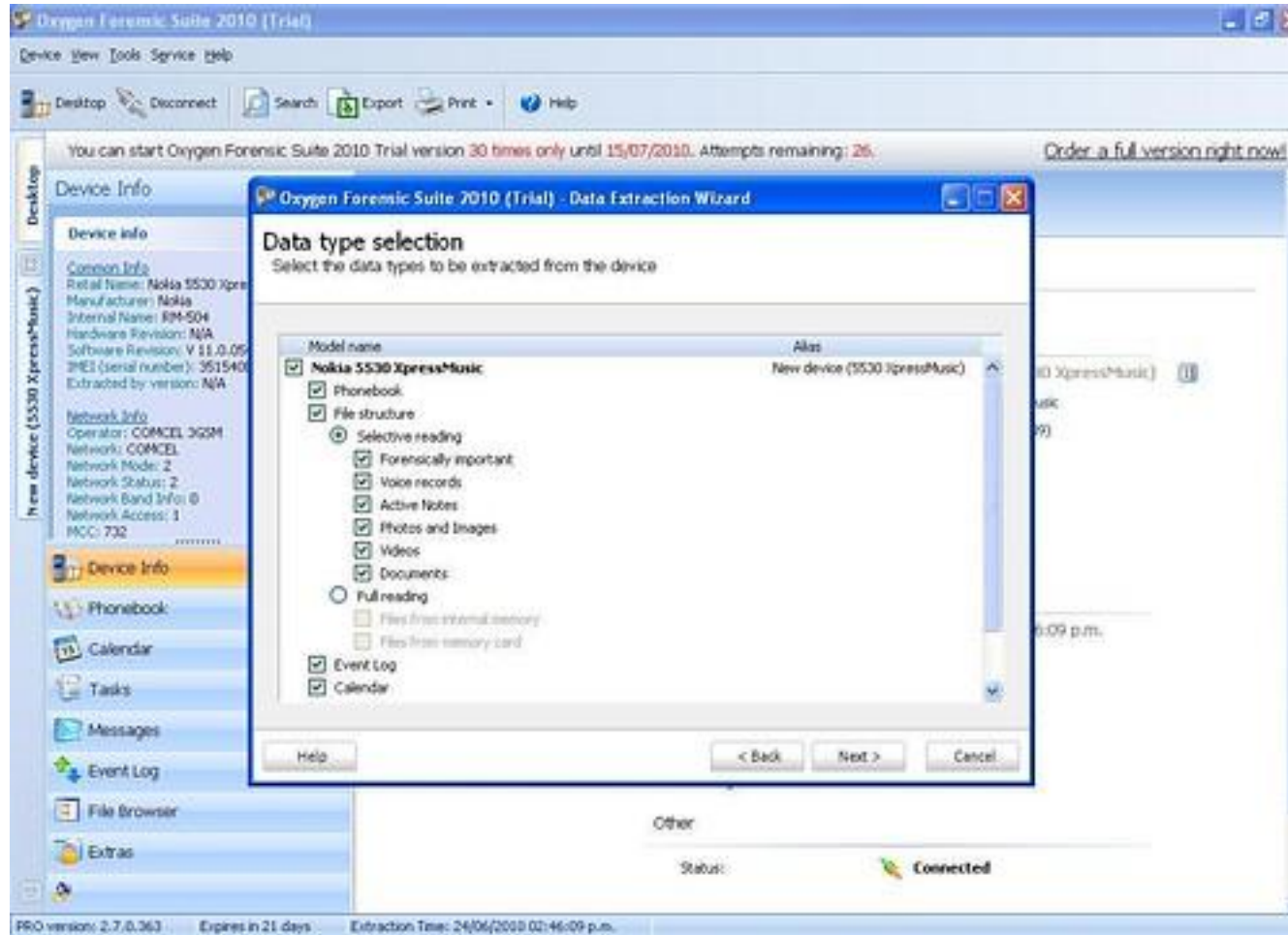


METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

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

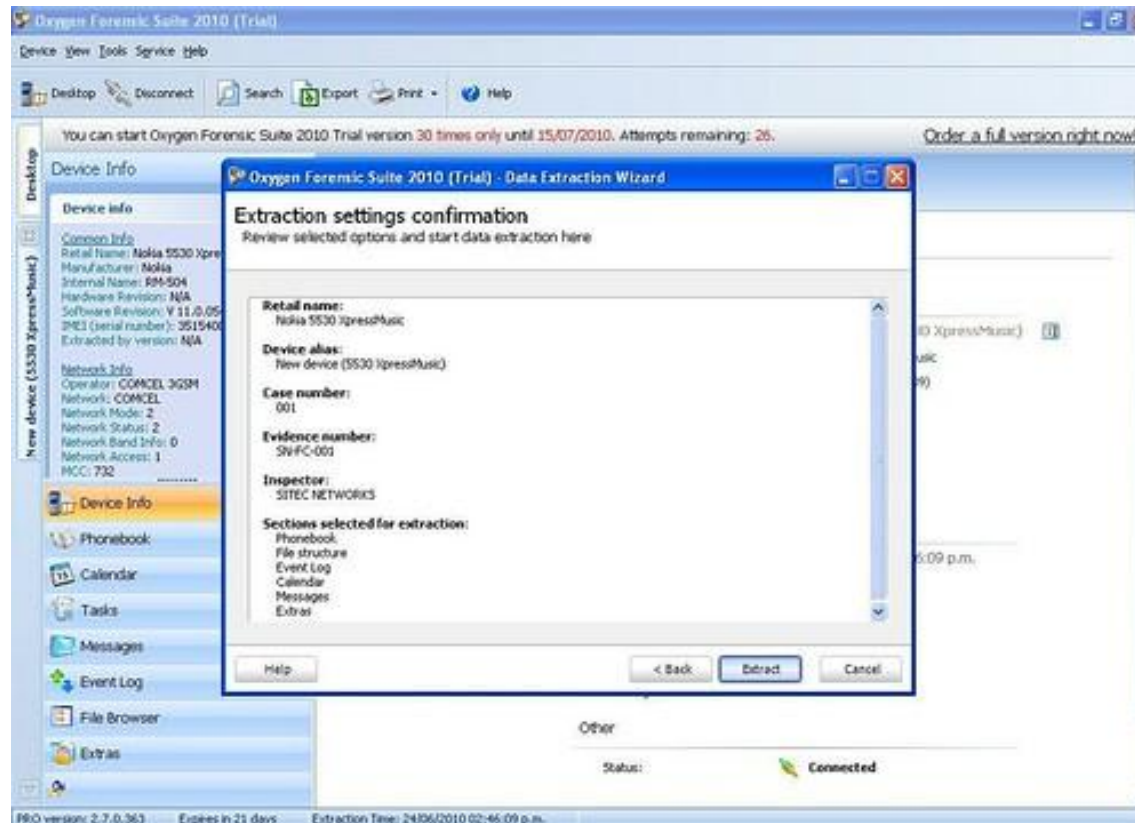


METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES



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 mostrarán 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.

The screenshot displays the Oxygen Forensic Suite 2010 (Trial) interface. The top window is the 'Data Extraction Wizard', which shows a progress bar and a message: 'You can start Oxygen Forensic Suite 2010 Trial version 30 times only until 15/07/2010. Attempts remaining: 26.' Below this, the 'Phonebook' view is shown, displaying a list of contacts with their names, phone numbers, and email addresses. The contacts are sorted by name, and the list includes entries like 'Claudio', 'Claudia', 'Clementia', 'Cobrador', and 'Cod'. The interface also features a 'Quick filter' section on the left and a 'Device Info' section at the bottom.

METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

Listado de Mensajes SMS

The screenshot displays the Oxygen Forensic Suite 2010 (Trial) interface. The main window shows a list of SMS messages extracted from a device. The interface includes a menu bar (Device, View, Tools, Service, Help), a toolbar with icons for Desktop, Search, Export, Print, Show message, Show folders, Reset filters, and Help. A notification banner at the top states: "You can start Oxygen Forensic Suite 2010 Trial version 30 times only until 15/07/2010. Attempts remaining: 26. Order a full version right now!".

The left sidebar contains a "Messages" section with a "Quick filter" and a "Message information" panel. The "Message information" panel shows details for a selected message: Folder: Inbox, Message type: File, Remote party: Bluetooth, Time Stamp: 24/06/2010 02:42:52 p.m., MD5 Hash: 507930b416a137633d8f5bc1241966ed3.

The main area displays a table of messages with columns: Type, Folder, Remote Party, Phone Number, and Time Stamp. The table lists various messages, including SMS and MMS, with details on their folders, remote parties, phone numbers, and timestamps.

The right sidebar shows a "Folders" list with icons and names: Messages, Inbox (9), Outbox, Drafts (1), Sent (2), Mis carpetas (6), Email Correo, and Hotmail.

The bottom status bar indicates: PRO version: 2.7.0.363, New device (SS30 XpressMusic), Total: 18, Filtered: 18, MD5 Hash: 507930b416a137633d8f5bc1241966ed3.

Type	Folder	Remote Party	Phone Number	Time Stamp
File	Inbox	Bluetooth		24/06/2010 02:42:52
SMS	Inbox	849	849	24/06/2010 11:36:17
SMS	Inbox	849	849	23/06/2010 01:11:00
SMS	Drafts	Adriana		23/06/2010 08:56:42
SMS	Inbox	2299	2299	21/06/2010 11:23:23
SMS	Sent	Adriana	311	19/06/2010 02:30:21
SMS	Inbox	987	987	18/06/2010 02:43:03
SMS	Inbox	10013	10013	18/06/2010 02:12:23
SMS	Sent	Adriana	311	18/06/2010 12:59:54
MMS	Mis carpetas	Bluetooth		17/06/2010 08:09:20
SMS	Inbox	9371	9371	17/06/2010 09:22:31
SMS	Inbox	9371	9371	17/06/2010 09:18:44
SMS	Inbox	9371	9371	17/06/2010 09:16:07
MMS	Mis carpetas	Bluetooth		31/08/2009 10:02:10
File	Mis carpetas	Bluetooth		31/08/2009 10:01:11
File	Mis carpetas	Bluetooth		31/08/2009 10:01:11
File	Mis carpetas	Bluetooth		31/08/2009 10:00:32
File	Mis carpetas	Bluetooth		31/08/2009 09:59:51

METODOLOGÍA PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE EN DISPOSITIVOS MÓVILES

Opciones por categorías.

