aedel
asociación española
de evidencias electrónicas

[TUTORIAL DE LA HERRAMIENTA ad|quiere]

La Asociación Española para el Desarrollo de las Evidencias Electrónicas - AEDEL es una organización sin ánimo de lucro que tiene como finalidad la promoción, fomento e impulso de todas aquellas medidas que contribuyan al desarrollo del estudio, regulación, confiabilidad y apoyo a la normalización de las Evidencias Electrónicas y la certificación de profesionales.

ad|quiere

Contenido

Introducción 3

Características actuales 3

"*TO DO list*" colaborativa 3

Descarga 4

Arranque inicial de AD | QUIERE 4

Paso 1 4

Paso 2 4

Paso 3 5

Paso 4 5

Paso 5 8

Paso 6 9

Paso 7 10

Paso 8 10

Paso 9 11

Aviso Legal 12

Definiciones 12

Concesión de la licencia 12

Derechos de propiedad 12

Exención de garantías y limitación de responsabilidades 13

Introducción

AD|QUIERE una distribución forense en CD. Existen muchas distribuciones gratuitas para realizar análisis forenses, pero todas acaban haciéndose de pago o no tienen herramientas suficientes para poder hacer, por ejemplo, adquisiciones en diferentes formatos. Por ello, nace **AD|QUIERE**, la primera distribución forense para la comunidad de habla Hispana, realizada por **AEDEL** con la colaboración de **blueliv**.

Características actuales

AD|QUIERE v. 0.8 es una distribución basada en Ubuntu Linux, la cual incorpora en su versión 0.8 el siguiente software:

- Herramientas nativas de Linux para la creación de imágenes de discos duros.
- Herramientas nativas de Linux para la firma digital.
- Linen, un software de adquisición facilitado por *Guidance Software* para realizar adquisiciones seguras en formato ENCASE.
- AIR, una herramienta GNU para realizar adquisiciones de discos duro o restaurar éstas.

Por otro lado, AD|QUIERE está preparado para reconocer discos externos USB para poder realizar las adquisiciones. Para ello, se facilitan diversos menús paso a paso, en el caso de Linen, para realizar las adquisiciones por cualquier persona, sin tener que tener altos conocimientos de administración sistemas, facilitando así una segregación de funciones a la hora de realizar proyectos forenses.

"*TO DO list*" colaborativa

Cómo modelo de partida y previamente a la versión 1.0, **AEDEL** conjuntamente con **blueliv** han querido publicar una versión 0.8 y someterla a la prueba de los expertos y usuarios al modo de un ***TO DO colaborativo***.

De esta forma, se ve cumplido el espíritu de **AEDEL** de promover en todos los ámbitos el buen uso de las evidencias electrónicas en diferentes colectivos: nuestros asociados, usuarios, profesionales, etc. Así, se permite que todos ellos puedan valorar la utilidad, seguridad y usabilidad de la herramienta, haciéndonos llegar sus ideas, opiniones y/o evaluaciones con el fin de que aquellas necesidades y características más innovadoras puedan ser incorporadas en la versión 1.0.

A tal fin, hemos habilitado una cuenta de correo-e: adquiere@aedel.es.

Previamente a la publicación de la versión 1.0, publicaremos una entrada en la página de AEDEL (http://aedel.es), en donde se especificarán las nuevas características de la versión 1.0.

Descarga

Para descargar una Imagen en formato ISO de AD|QUIERE, se puede descargar del siguiente enlace también facilitado en la web: http://www.blueliv.com/ad-Quiere/ad-Quiere_i386_v0.8.zip

Una vez descargada y descomprimida, se debe utilizar cualquier lector de imágenes ISO que permita grabar estas en formato CD-Rom. La capacidad mínima requerida para grabarlo son 700 Mb lo que supone un CD-Rom convencional.

Arranque inicial de AD|QUIERE

Para realizar la adquisición de un disco duro de cualquier PC, deben seguirse los siguientes pasos.

Paso 1

Extraer todos los dispositivos externos tales como pen drives, discos usb externos, etc. Cabe destacar que el dispositivo usb en donde se volcarán los datos de la adquisición, no debe conectarse al PC hasta **el paso 7.**

Paso 2

Insertar el CD con AD|QUIERE y arrancar el sistema destino de la investigación. Al principio y durante el arranque se podrá observar la siguiente pantalla:

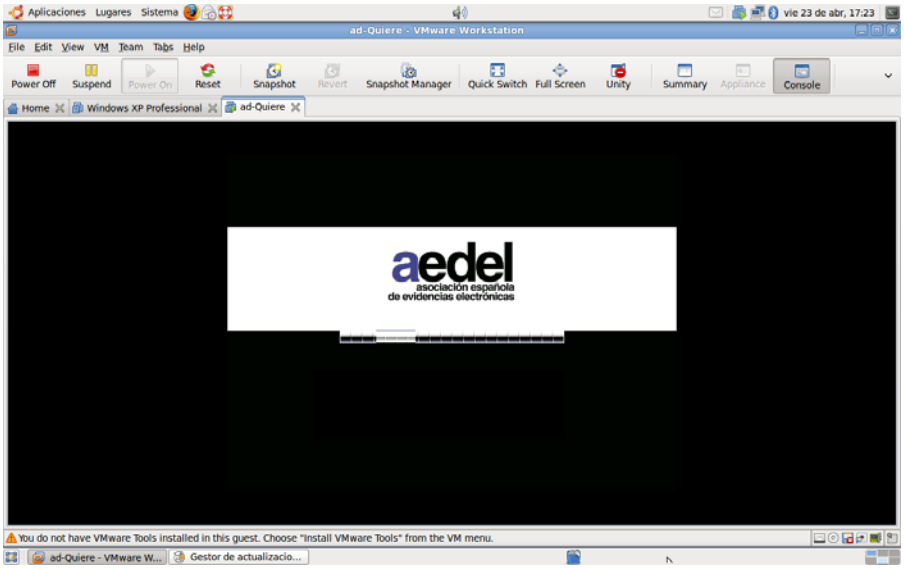


Figura 1: Arranque de AD-QUIERE

Paso 3

Si el proceso de arranque no se inicia pasados 30 segundos, pulse la tecla enter dos veces.

Paso 4

Cabe destacar que sólo si el disco destino está formateado en formato FAT32, y existe espacio en el disco duro, puede ir al **paso 5**. Por el contrario, realice las siguientes tareas:

- Conecte el dispositivo externo destinatario.
- Clickee en el icono “Format External Hard Disk” en el escritorio.
- Clickee “Select Volume (External Hard Disk)”

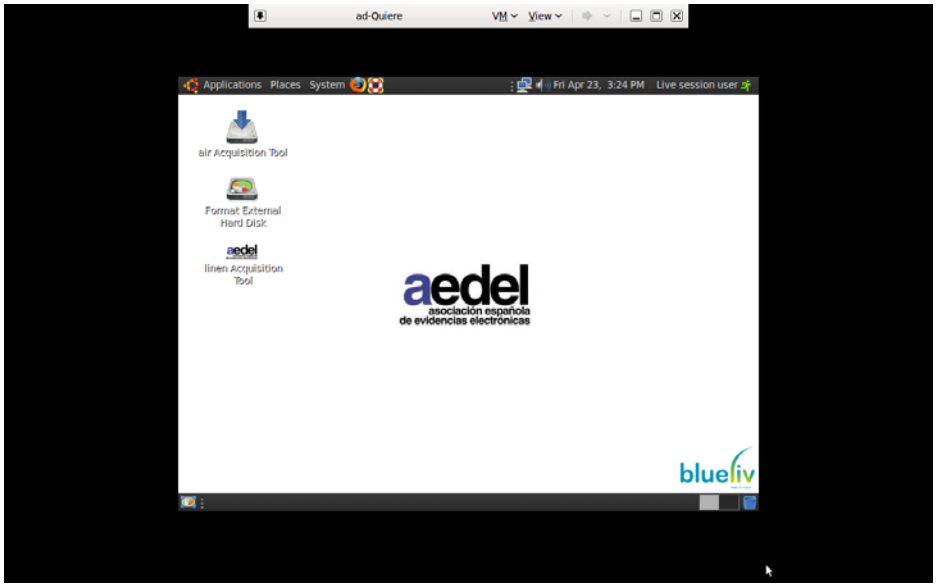


Figura 2: Ejecutar utilidad de formateo de disco duro

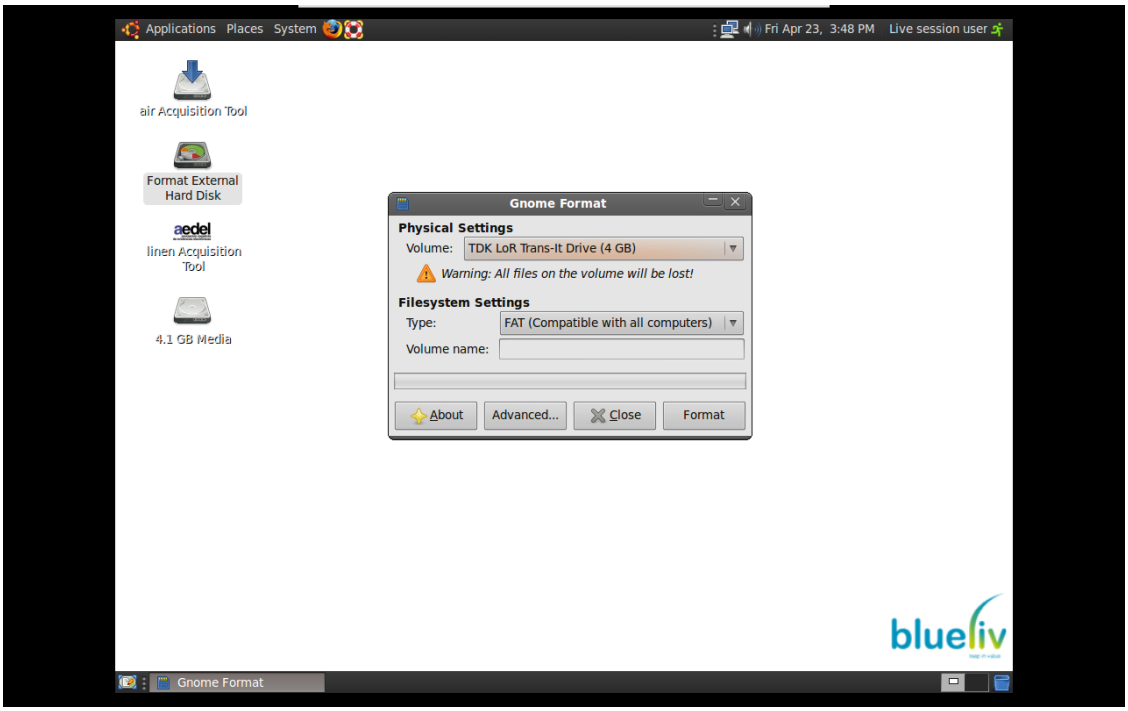


Figura 3: Opción de formateo en fat 32

- Clickee “Advanced” button y seleccione “/dev/sdb”

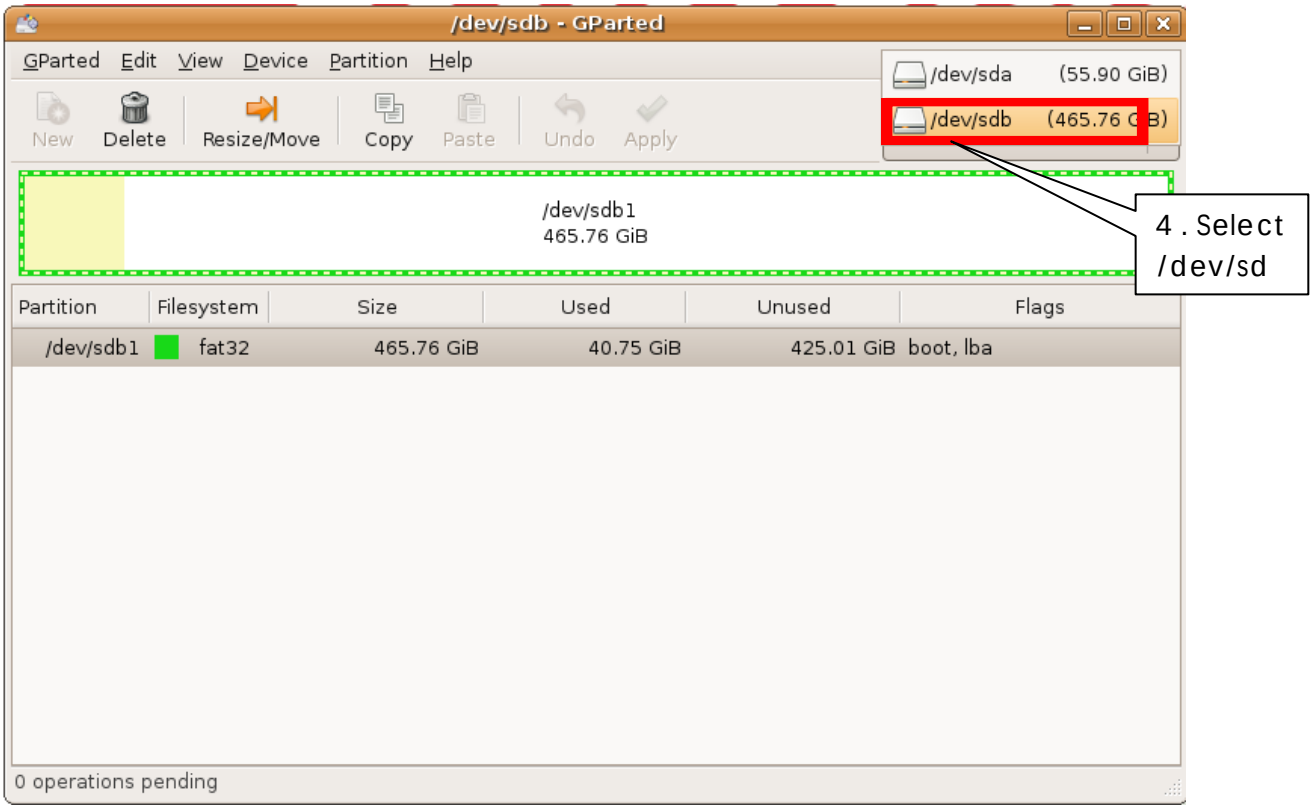


Figura 4: seleccione el disco externo destinatario

- Pulse el botón derecho del raton y en “external partition (/dev/sdb1)”, luego seleccione “Format to” y seleccione “Fat32”:

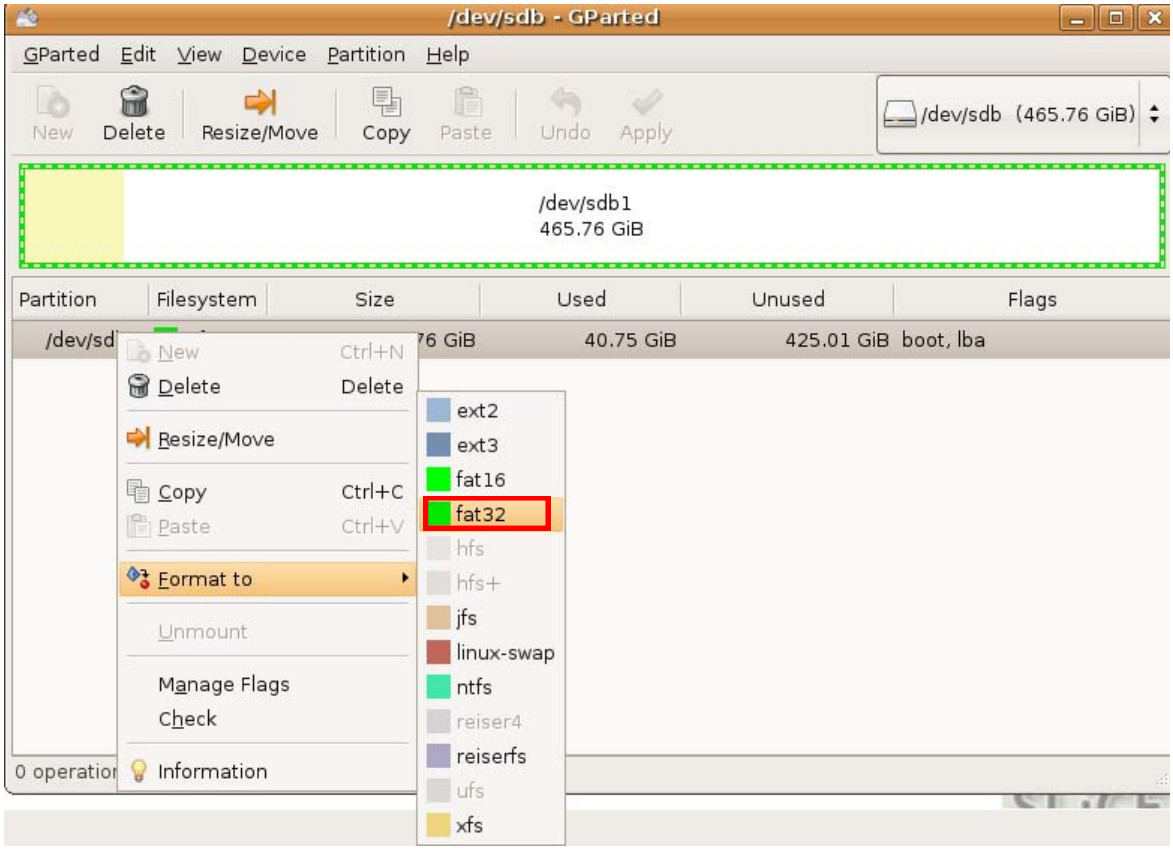


Figura 5: Select filesystem

- Clickee “Apply” para proceder al formateo

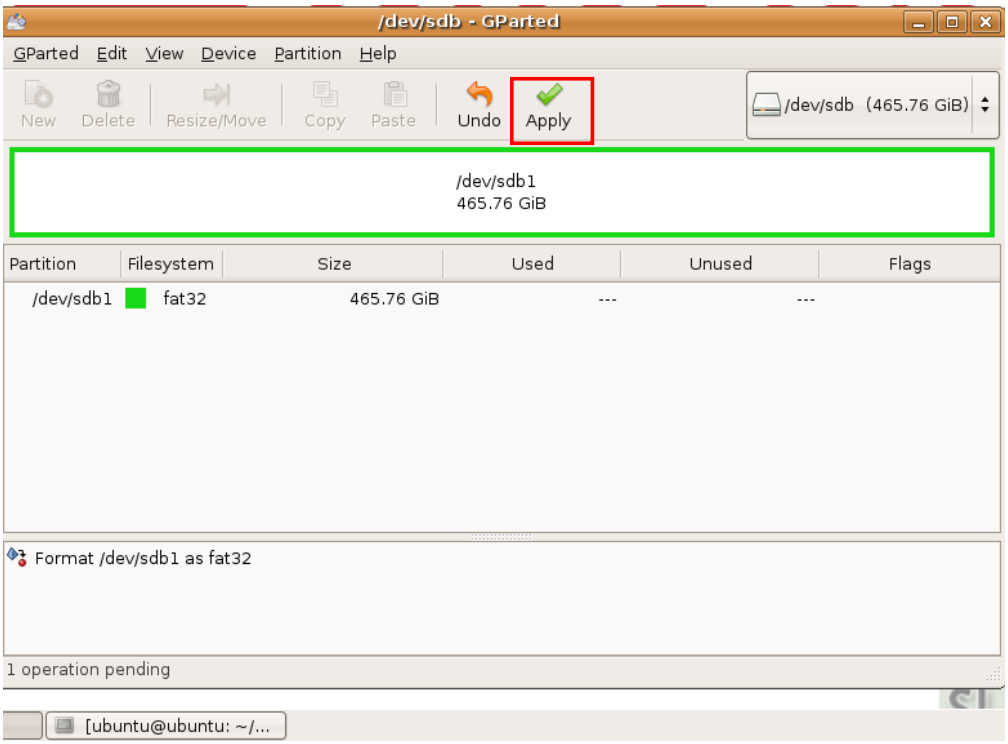
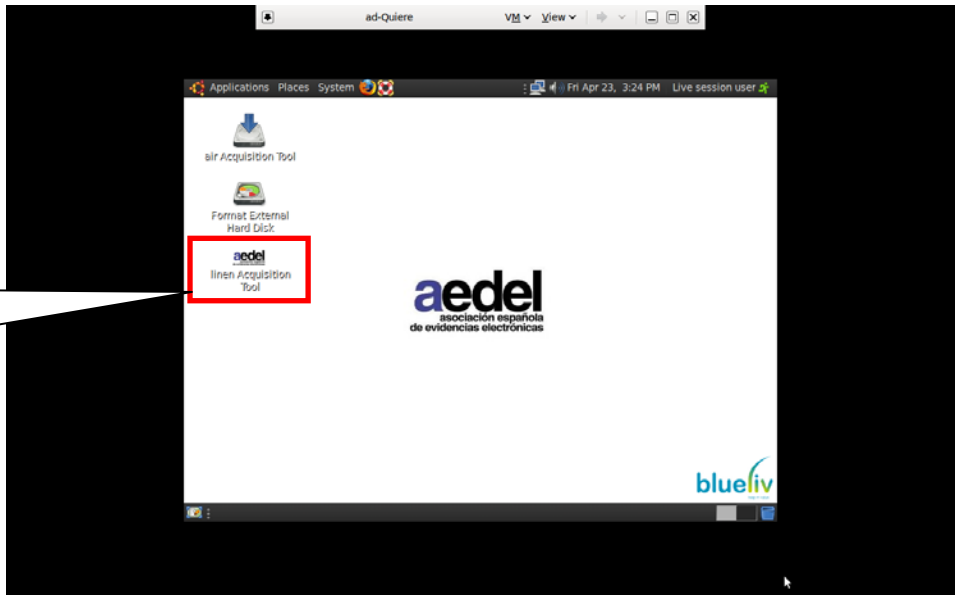


Figura 6: Proceso de formateo

- Una vez finalizado el procedimiento, desconecte de nuevo, el disco externo destinatario.

Paso 5

Clickee doblemente en el icono Linen Acquisition tool



Herramient a de adquisició

Figura 7: Ejecución de Linen Acquisiton tool

Paso 6

Una vez se haya arrancado la herramienta, esperará a que se conecte el disco externo destinatario.

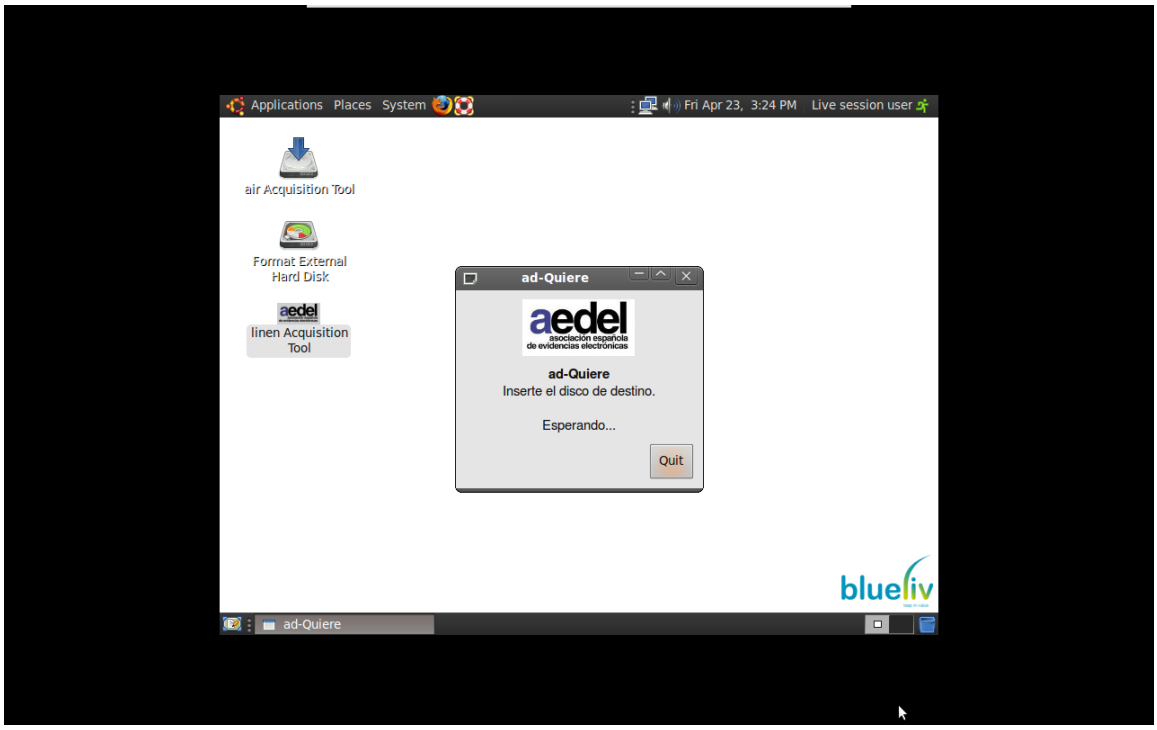


Figura 8: AD|QUIERE espera a la conexión del disco externo

Paso 7

Conecte el disco destinatario interno. Nótese que es muy importante que el disco duro externo en el cual se va a depositar la adquisición, debe conectarse ahora y no en los pasos previos (salvo para la necesidad de ser formateado).

Una vez conectado el Disco duro destinatario, será detectado automáticamente por AD|QUIERE en unos poco segundos y aparecerá una pantalla como la siguiente:

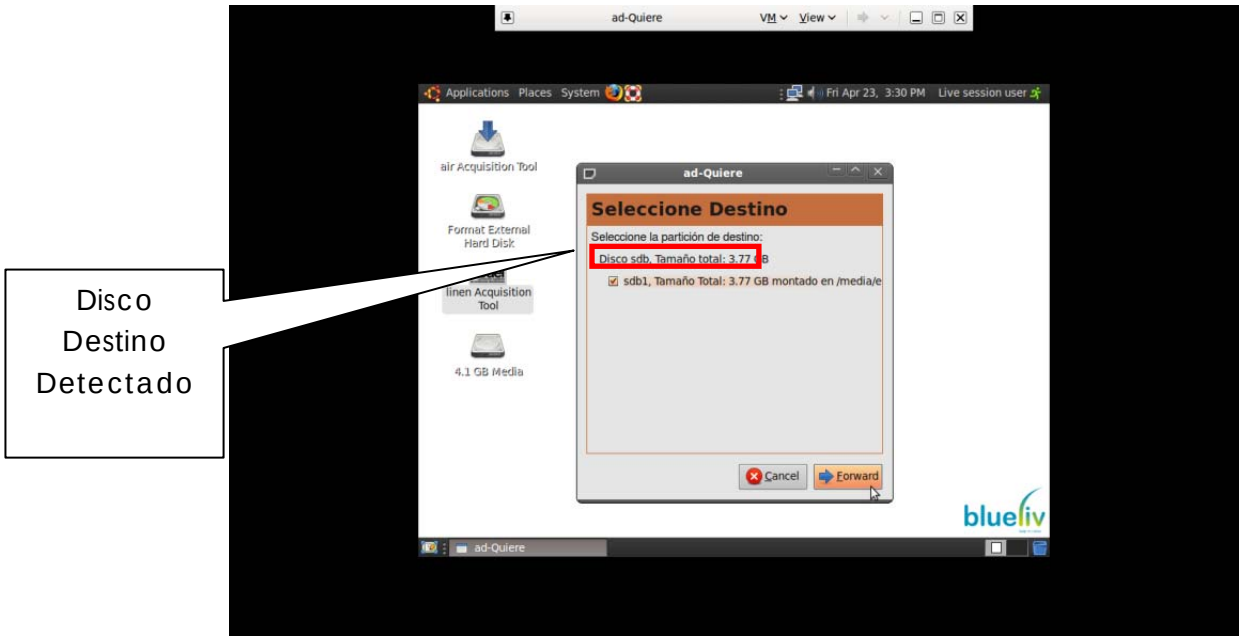


Figura 9: Detección del Disco Duro Destinatario

Paso 8

Seleccione el Disco Destino detectado clicando en el nombre del dispositivo, seguidamente pulse forward, para empezar el proceso de adquisición.

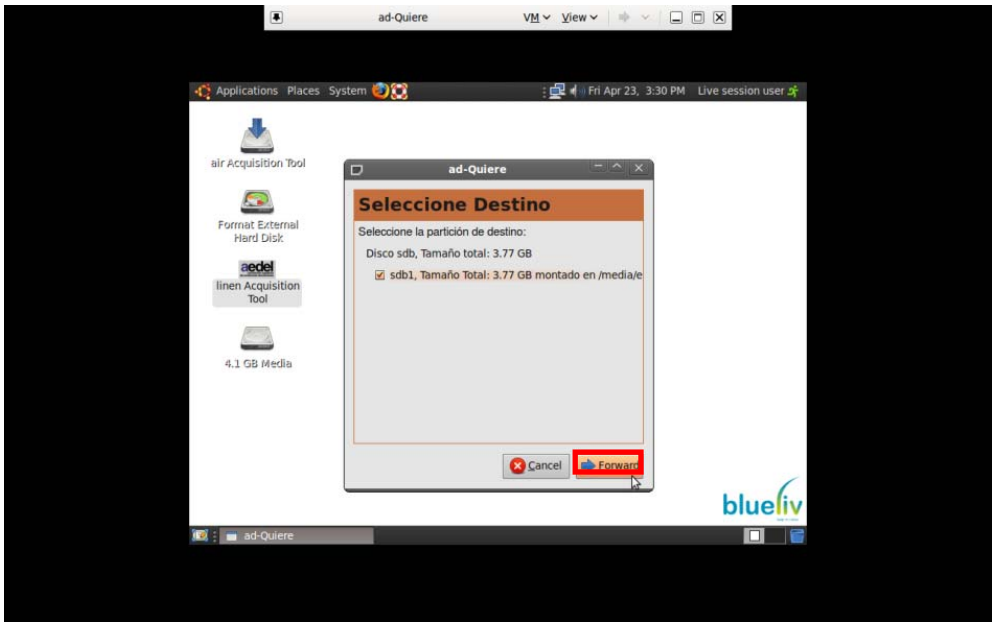


Figura 10: Selección de disco duro externo detectado e inicio adquisición

Paso 9

Seguidamente se arrancará la herramienta Linen, el proceso de adquisición será totalmente guiado con una ayuda en la parte izquierda de la pantalla.

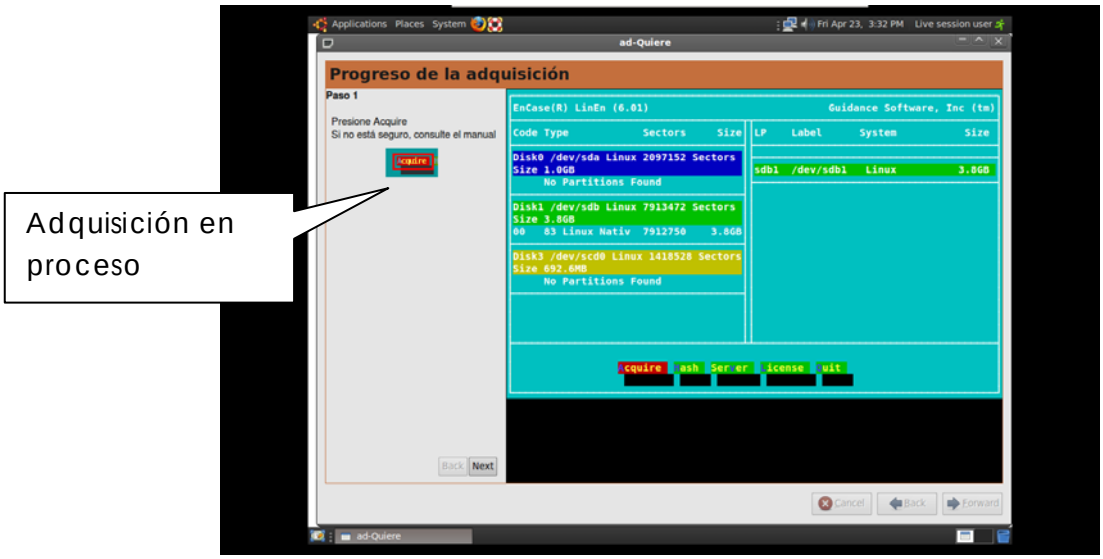


Figura 11: Proceso de adquisición autoguiado

Cada vez que se complete un paso, debe clicar “next” en la ayuda para ver la siguiente pantalla de ayuda.

Aviso Legal

Definiciones

Usuario: particular o la entidad comercial que descarga el AD|QUIERE.

Concesión de la licencia

Derechos y limitaciones de la concesión.
AEDEL concede al Usuario el derecho no exclusivo e intransferible de utilizar el AD|QUIERE, teniendo en cuenta las limitaciones siguientes:

Derechos.
AD|QUIERE diseñado exclusivamente para ser utilizado en el sistema operativo Linux/FreeBSD/OpenSolaris podrá ser copiado y redistribuido, siempre y cuando no se modifiquen en modo alguno los archivos binarios (salvo para descomprimirlos).

Limitaciones.
Queda prohibida la separación de los componentes. Se autoriza el uso del AD|QUIERE como un producto único.

Anulación
La licencia quedará automáticamente anulada si el Usuario no cumple las condiciones establecidas. En tal caso, el Usuario destruirá todas las copias del AD|QUIERE y sus componentes.

Derechos de propiedad

Todos los derechos de propiedad intelectual del AD|QUIERE (incluidas imágenes, fotografías, animación, vídeo, audio, música, texto y otros elementos que forman parte del AD|QUIERE), la documentación adjunta y todas las copias del AD|QUIERE corresponden a AEDEL. AD|QUIERE está protegido por las leyes y tratados internacionales relativos al derecho de propiedad. Por consiguiente, el Usuario deberá utilizar el AD|QUIERE como cualquier otro material protegido por las leyes de propiedad intelectual, salvo que se disponga lo contrario en virtud de la presente LICENCIA

Exención de garantías y limitación de responsabilidades

No existe garantía alguna.
En la medida en que lo permita la legislación aplicable, AD|QUIERE se facilita "tal cual" y AEDEL no ofrece ninguna garantía, explícita ni implícita, incluyendo las garantías implícitas de comerciabilidad y adecuación a un fin particular.

No existe responsabilidad alguna sobre daños y perjuicios.
En la medida en que lo permita la legislación aplicable, en ningún caso se podrá considerar AEDE responsables de cualesquiera daños ya sean especiales, directos o indirectos (incluidos, a título informativo pero no limitativo, los de lucro cesante, interrupción de las actividades comerciales o pérdida de información) derivados del uso o la imposibilidad de uso de los materiales, incluso aunque AEDEL haya recibido aviso de la posibilidad de este tipo de daños.