

00. Introducción a Kali Linux.

Debería usar Kali Linux?

Diferencias Entre Kali Linux y Debian

Kali Linux está orientado a pruebas de penetración profesional y auditorías de seguridad. Como tal, varios cambios han sido implementados en Kali Linux para que reflejen estas necesidades:

1. **Un solo usuario, acceso root por diseño:** Debido a la naturaleza de las auditorías de seguridad, Kali Linux está diseñado para ser usado en un escenario "[de un solo usuario](#)"
2. **Servicio de redes deshabilitado en forma predeterminada:** Kali Linux contiene ganchos sysvinit los cuales [deshabilitan los servicios de redes](#) por defecto. Estos ganchos nos permiten instalar varios servicios en Kali Linux, mientras aseguran que nuestra distribución permanezca segura en forma predeterminada, no importando que paquetes estén instalados. Adicionalmente los servicios tales como Bluetooth son también puestos en lista negra por defecto.
3. **kernel de linux modificado:** Kali Linux usa un kernel, parchado para la inyección wireless.

Es Kali Linux correcto para Tí?

Como desarrolladores de la distribución, uno esperaría que recomendamos a todos el uso de Kali Linux. De hecho sin embargo, por ser Kali una distribución específicamente generada para profesionales en penetration testing y auditorías de seguridad, nosotros **NO** recomendamos esta distro para personas que no estén familiarizadas con Linux.

Adicionalmente, el mal uso de las herramientas de seguridad dentro de la red, sobre todo sin permiso, pueden causar daños irreparables y tener consecuencias significativas.

Si estas buscando una distribución de Linux para aprender las bases y tener un buen punto de partida, Kali Linux no es la distribución ideal para tí. Deberías comenzar con [Ubuntu](#) or [Debian](#) en su lugar.

¿Qué es Kali Linux?

Características de Kali Linux

[Kali Linux](#) es una distribución de Linux avanzada para pruebas de penetración y auditorías de seguridad.

Kali es una completa re-construcción de [BackTrack Linux](#) desde la base hacia arriba, y se adhiere completamente a los estándares de desarrollo de [Debian](#). Toda la nueva infraestructura ha sido puesta en el lugar, todas las herramientas fueron revisadas y fueron embaladas, y hemos cambiado a [Git](#) para nuestro VCS.

- **Más de 300 herramientas de pruebas de penetración:** Después de revisar todas las herramientas que se incluyen en BackTrack, hemos eliminado una gran cantidad de herramientas que, o bien no funcionaban o tenían otras herramientas disponibles que proporcionan una funcionalidad similar.
- **Gratis y siempre lo será:** Kali Linux, al igual que su predecesor, es completamente gratis y siempre lo será. Nunca, jamás, tendrás que pagar por Kali Linux.
- **Git - árbol de código abierto:** Somos partidarios enormes de software de código abierto y nuestro árbol de desarrollo está disponible para todos y todas las fuentes están disponibles para aquellos que desean modificar y reconstruir paquetes.
- **Obediente a FHS:** Kali ha sido desarrollado para cumplir con el [Estándar de jerarquía del sistema de ficheros](#), permitiendo que todos los usuarios de Linux puedan localizar fácilmente archivos binarios, archivos de soporte, bibliotecas, etc.
- **Amplio apoyo a dispositivos inalámbricos:** Hemos construido Kali Linux para que soporte tantos dispositivos inalámbricos como sea posible, permitiendo que funcione correctamente en una amplia variedad de hardware y hacerlo compatible con varios USB y otros dispositivos inalámbricos.
- **Kernel personalizado con parches de inyección:** Como probadores de penetración, el equipo de desarrollo a menudo tiene que hacer evaluaciones inalámbricas para que nuestro kernel tenga los últimos parches de inyección incluidos.
- **Entorno de desarrollo seguro:** El equipo de Kali Linux está compuesto por un pequeño grupo de personas de confianza que sólo puede comprometer e interactuar con los paquetes de los repositorios, haciendo uso de múltiples protocolos seguros.
- **Paquetes firmado con PGP y repos:** Todos los paquetes de Kali son firmados por cada desarrollador individualmente cuando se construyen y son comprometidos. Los repositorios posteriormente firman los paquetes también.
- **Multi-lenguaje:** Aunque las herramientas de penetración tienden a ser escritas en Inglés, nos hemos asegurado de que Kali tenga soporte multilingüe, lo que permite a más usuarios poder operar en su idioma nativo y encontrar las herramientas necesarias para el trabajo.
- **Totalmente personalizable:** Estamos completamente conciente de que no todo el mundo estará de acuerdo con nuestras decisiones de diseño por lo que hemos hecho lo más fácil posible para nuestros usuarios más aventureros puedan [personalizar Kali Linux](#) a su gusto, todo el camino hasta el núcleo.
- **Soporte ARMEL y ARMHF:** Dado a que los sistemas basados en ARM son cada vez más frecuentes y de bajo costo, sabíamos que [el soporte de ARM de Kali](#) tendrían que ser tan robusta como podríamos administrar, resultando en instalaciones que trabajan en sistemas de [ARMEL y ARMHF](#). Kali Linux tiene repositorios ARM integrado con la línea principal de distribución de modo que las herramientas para ARM serán actualizada en relación con el resto de la distribución. Kali está disponible para los dispositivos ARM siguientes:
 - [rk3306 mk/ss808](#)
 - [Raspberry Pi](#)
 - [ODROID U2/X2](#)
 - [MK802/MK802 II](#)
 - [Samsung Chromebook](#)

Kali está diseñado específicamente para las pruebas de penetración y, por tanto, toda la documentación de este sitio asume el conocimiento previo del sistema operativo Linux.

01. Descargando Kali Linux

Descarga Imágenes Oficiales de Kali

Alert! Asegúrese siempre de que está descargando Kali Linux desde fuentes oficiales y asegúrese de verificar las sumas de comprobación MD5 en contra de nuestros valores oficiales. Sería fácil para una entidad maligna poder modificar una instalación de Kali para que contenga código maligno y sea acogida extraoficial.

Imágenes de Kali Linux

Ficheros tipo ISO

Kali Linux está disponible como una ISO de arranque en formatos de 32 y 64 bits.

- [Descarga ISOs de Kali](#)

Imágenes de VMware

Kali está disponible como una máquina pre-hecha virtual de VMware con VMware Tools instalado. Las imágenes de VMware están disponibles en formatos de 32-bit y 64-bit.

- [Descarga Imágenes VMware de Kali](#)

Imágenes de ARM

Debido a la naturaleza de la arquitectura ARM, no es posible tener una sola imagen que funcione en todos los dispositivos ARM. Tenemos [Imágenes Oficiales de ARM](#) disponible para los siguientes dispositivos:

- rk3306 mk/ss808
- Raspberry Pi
- ODROID-U2/X2
- MK802/MK802 II
- Samsung Chromebook

Verificando las sumas de verificación MD5 de las imágenes descargadas

Es muy importante verificar la suma de control MD5 de la descarga en contra de las sumas de comprobación oficiales proporcionados por Kali Linux.

Verificando las sumas de verificación MD5 en Linux

```
md5sum kali-i386.iso
2455da608852a7308e1d3a4dad34d3ce kali-i386.iso
```

Verificando las sumas de verificación MD5 en OSX

```
md5 kali-i386.iso
```

```
MD5 (kali-i386.iso) = 2455da608852a7308e1d3a4dad34d3ce
```

Verificando las sumas de verificación MD5 en Windows

Windows no tiene la capacidad nativa para calcular las sumas de comprobación MD5 por lo que tendrá que utilizar una utilidad como [MD5summer](#) para verificar su descarga.

03. Instalando Kali Linux

Instalar Kali Linux en disco encriptado

A veces, tenemos datos personales sensible que preferiríamos cifrar mediante el cifrado de disco completo. Con el instalador de Kali Linux puede iniciar una instalación LVM cifrado en cualquiera de los discos duros o unidades USB. El procedimiento de instalación es muy similar a un "instalación normal de Kali Linux", con la excepción de la elección de una partición LVM cifrada durante el proceso de instalación.

Requisitos de instalación cifrados de Kali Linux

La instalación de Kali Linux en su ordenador es un proceso fácil. En primer lugar necesitará hardware compatible. Los requisitos de hardware son mínimos y se enumeran a continuación, aunque mejor hardware, naturalmente, ofrece un mejor rendimiento. Las imágenes i386 tienen un núcleo predeterminado PAE, por lo que puede ejecutarse en sistemas con más de 4 GB de RAM. [Descarga Kali Linux](#) y, o bien grabe el ISO en un DVD, o [prepare una memoria USB con Kali Linux Live](#) como medio de instalación.

Requisitos previos de instalació

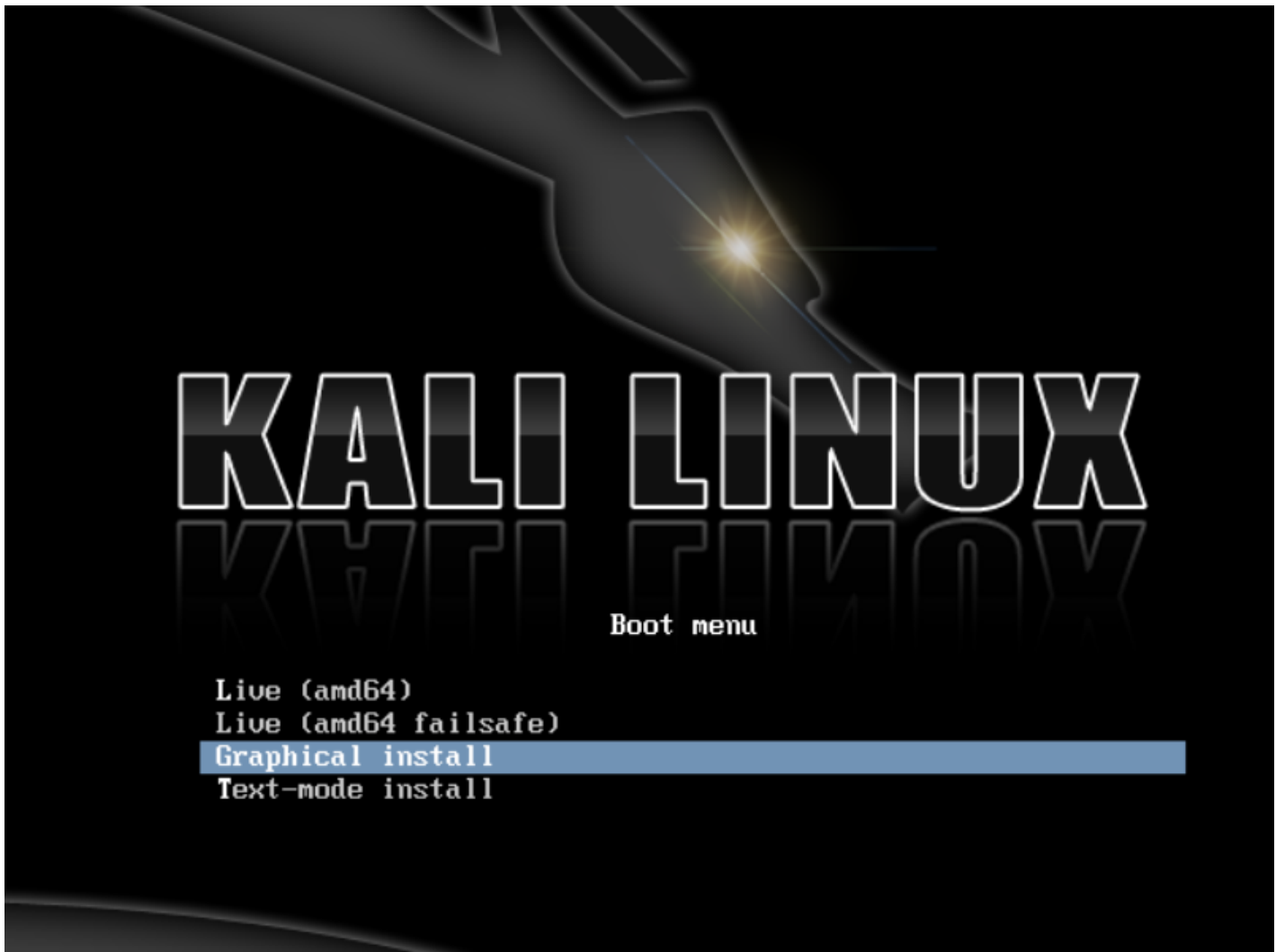
- Un mínimo de 8 GB de espacio en disco para la instalación de Kali Linux.
- Para las arquitecturas i386 y amd64, un mínimo de 512 MB de RAM.
- CD-DVD Drive / Soporte de arranque mediante USB

Preparación para la instalación

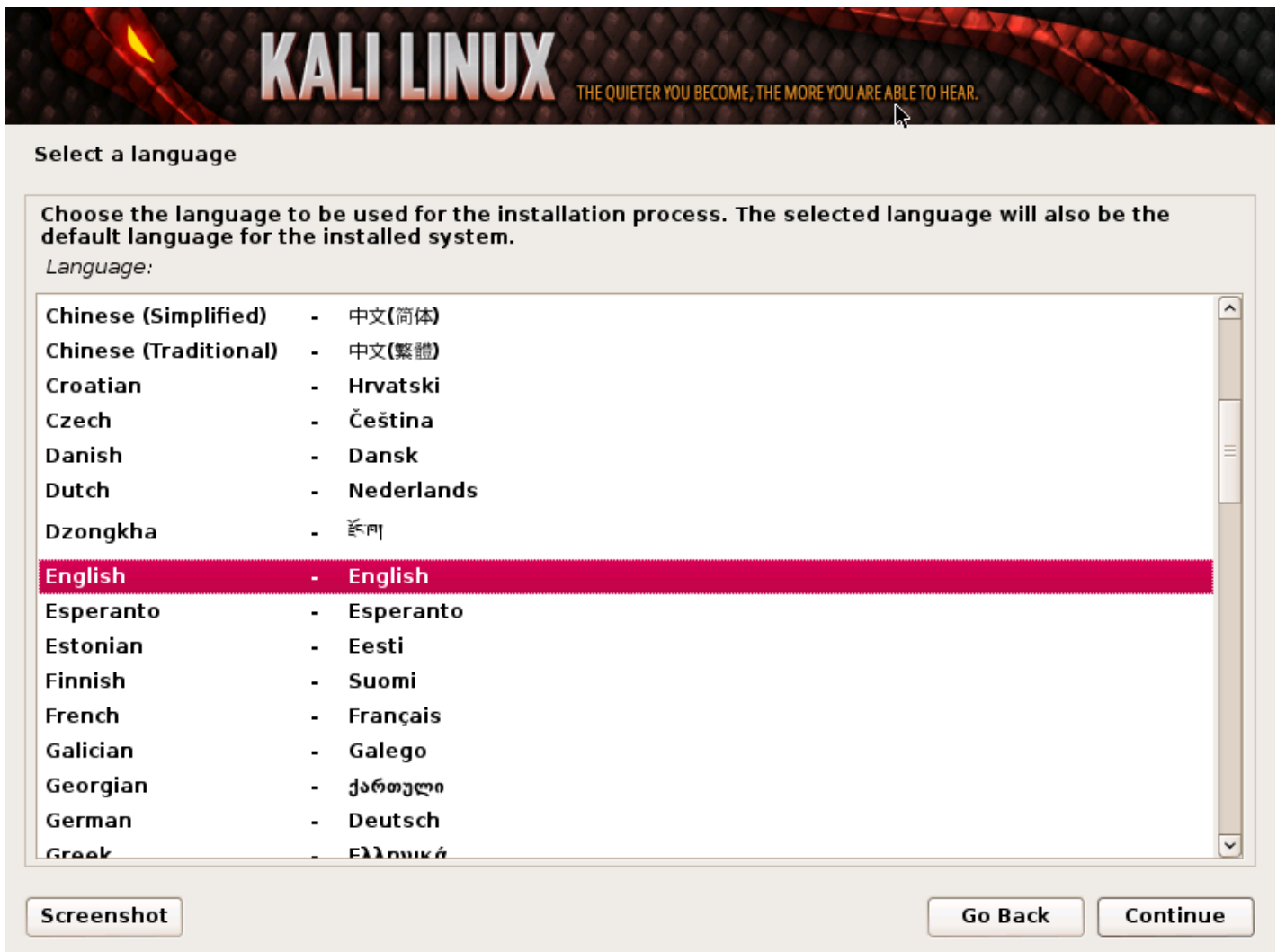
1. [Descargue Kali linux](#).
2. Queme el ISO de Kali Linux en un DVD o [cree una imagen de Kali Linux Live en una memoria USB](#).
3. Asegúrese de que su ordenador está configurado para arrancar desde CD / USB en la BIOS.

Procedimiento de instalación de Kali Linux


1. Para iniciar la instalación, arranque con el medio de instalación elegido. Usted debe ser recibido con la pantalla de arranque de Kali. Elegir una instalación gráfica o en modo texto. En este ejemplo, hemos elegido una instalación gráfica.



2. Seleccione el idioma que desee y luego su país de localización. También se le pedirá que configure su teclado con el mapa de teclado adecuado.



3. El programa de instalación copiará la imagen en su disco duro, probará las interfaces de red, y luego le pedirá que introduzca un nombre de host para el sistema. En el siguiente ejemplo, hemos entrado "Kali", como el nombre de host.



Configure the network

Please enter the hostname for this system.

The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.

Hostname:

[Screenshot](#) [Go Back](#) [Continue](#)

4. Introduzca una contraseña robusta para la cuenta de root y cree las cuentas adicionales que desee.



Set up users and passwords

You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.

Note that you will not be able to see the password as you type it.

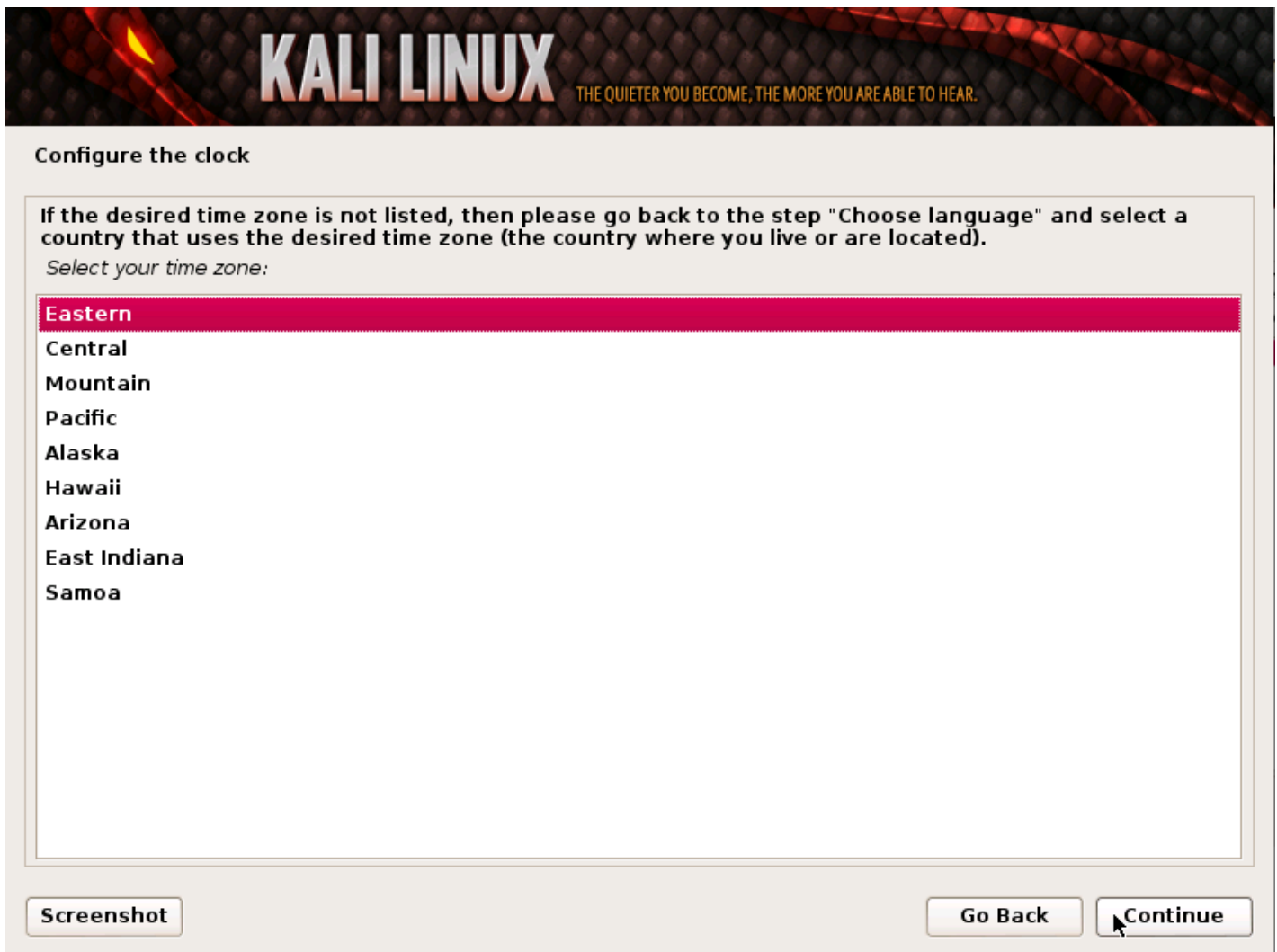
Root password:

Please enter the same root password again to verify that you have typed it correctly.

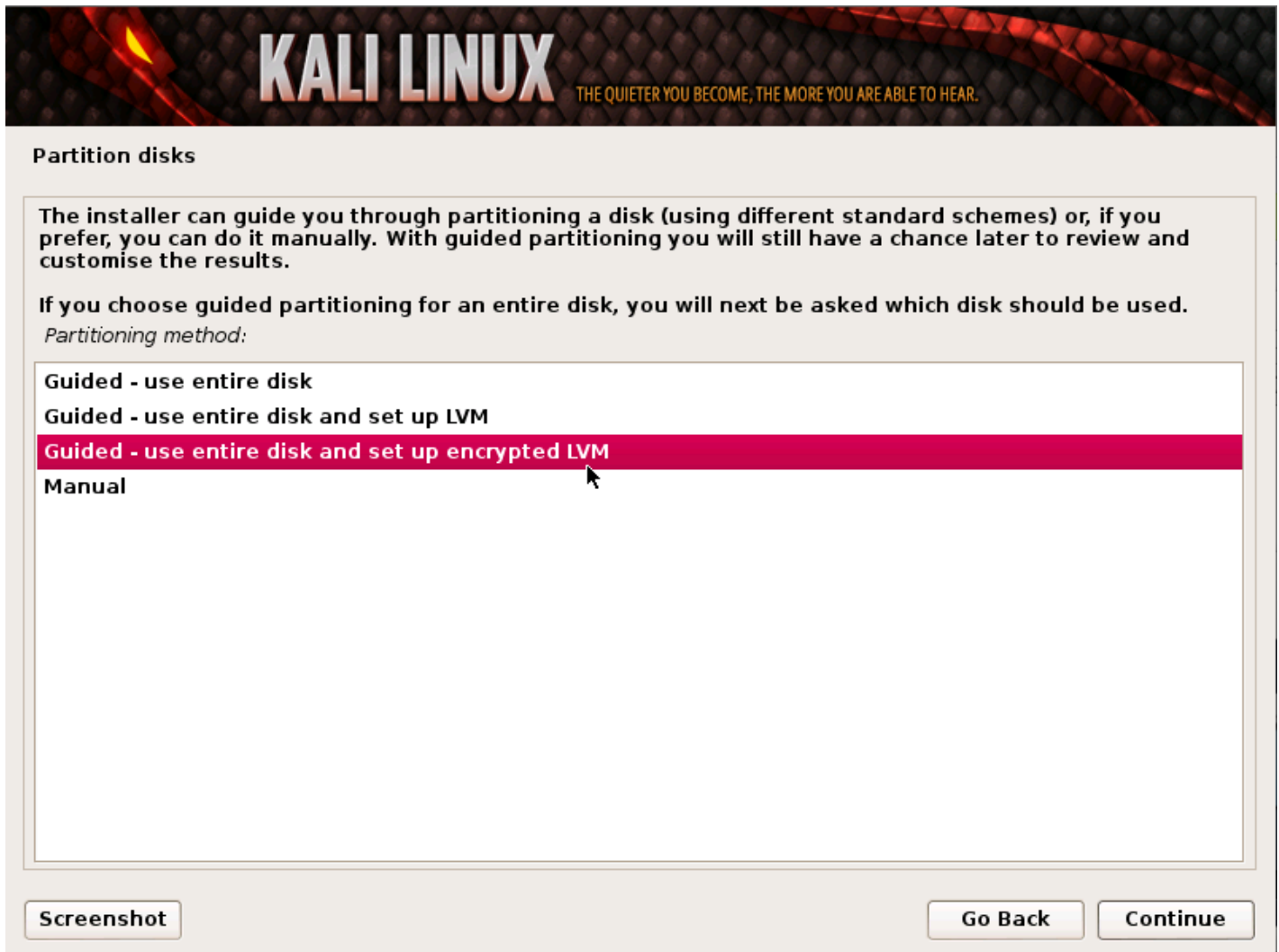
Re-enter password to verify:

[Screenshot](#) [Go Back](#) [Continue](#)

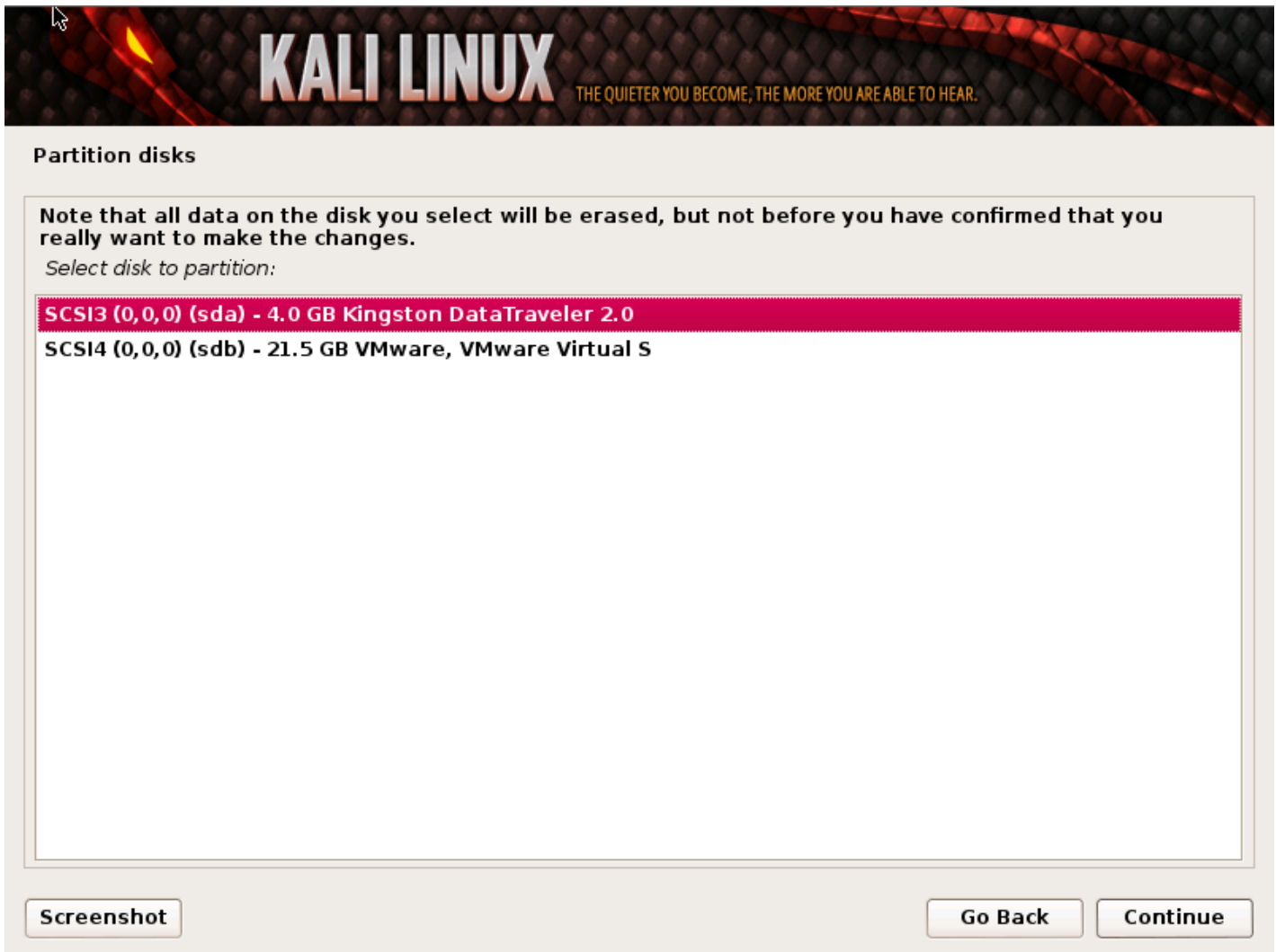
5. Configure su zona horaria.



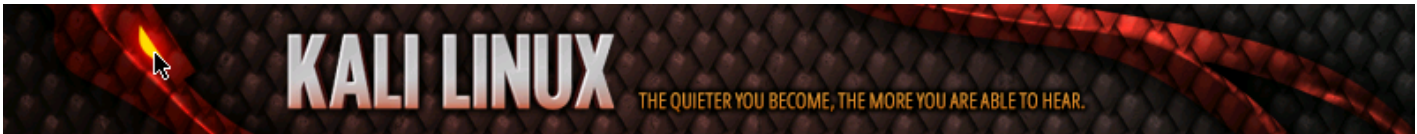
6. El instalador probará sus discos, y le ofrecerá cuatro opciones. Para una instalación LVM cifrado, elija la opción "**utilize todo el disco y configure LVM cifrado**" como se muestra a continuación.



7. Seleccione la unidad de destino para instalar Kali. En este caso, hemos elegido un destino de unidad USB. Vamos a utilizar esta unidad USB para arrancar una instancia cifrado de Kali.



8. Confirme su esquema de particionamiento y continúe con la instalación.



KALI LINUX THE QUIETER YOU BECOME, THE MORE YOU ARE ABLE TO HEAR.

Partition disks

This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.

Configure encrypted volumes

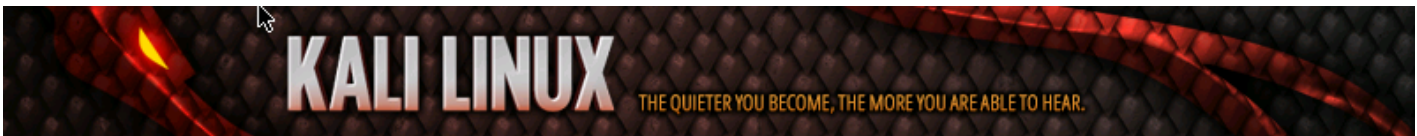
- ▼ LVM VG kali, LV root - 3.5 GB Linux device-mapper (linear)
 - > #1 3.5 GB f ext4 /
- ▼ LVM VG kali, LV swap_1 - 209.7 MB Linux device-mapper (linear)
 - > #1 209.7 MB f swap swap
- ▼ Encrypted volume (sda5_crypt) - 3.8 GB Linux device-mapper (crypt)
 - > #1 3.8 GB K lvm
- ▼ SCSI3 (0,0,0) (sda) - 4.0 GB Kingston DataTraveler 2.0
 - > #1 primary 254.8 MB F ext2 /boot
 - > #5 logical 3.8 GB K crypto (sda5_crypt)
- ▼ SCSI4 (0,0,0) (sdb) - 21.5 GB VMware, VMware Virtual S
 - > #1 primary 20.5 GB B ext4
 - > #5 logical 922.7 MB swap

Undo changes to partitions

Finish partitioning and write changes to disk

Screenshot Help Go Back Continue

9. A continuación, se le pedirá una contraseña de cifrado. Usted tendrá que recordar la contraseña y usarla cada vez que inicie la instancia cifrado de Kali Linux.



Partition disks

You need to choose a passphrase to encrypt SCSI3 (0,0,0), partition #5 (sda).

The overall strength of the encryption depends strongly on this passphrase, so you should take care to choose a passphrase that is not easy to guess. It should not be a word or sentence found in dictionaries, or a phrase that could be easily associated with you.

A good passphrase will contain a mixture of letters, numbers and punctuation. Passphrases are recommended to have a length of 20 or more characters.

Encryption passphrase:

Please enter the same passphrase again to verify that you have typed it correctly.

Re-enter passphrase to verify:

10. Configurar espejos de red. Kali utiliza un repositorio central para distribuir aplicaciones. Tendrá que introducir la información de proxy adecuado según sea necesario.

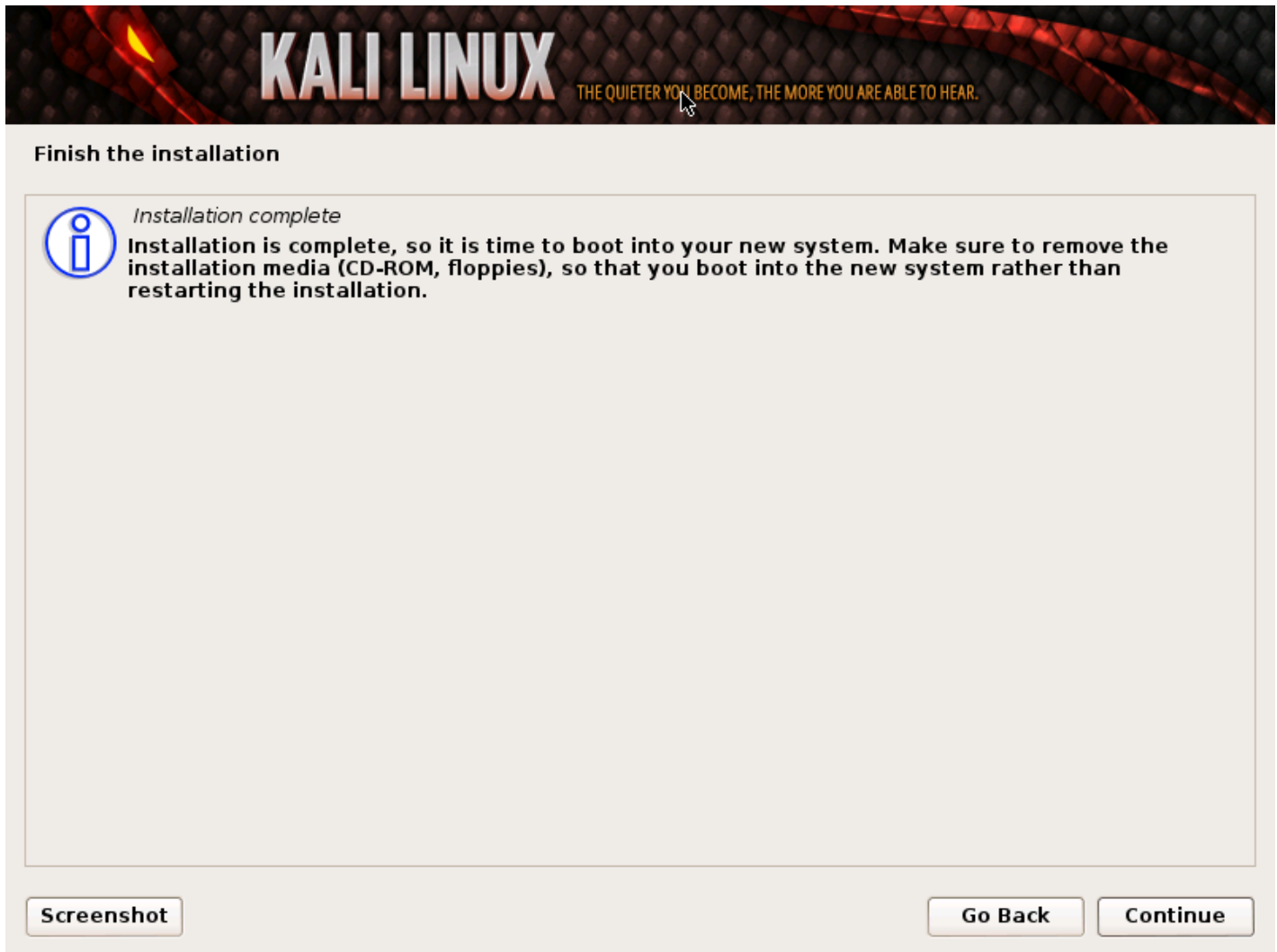
NOTA! Si selecciona "NO" en esta pantalla, **NO** podrá instalar paquetes desde los repositorios de Kali.



11. Next install GRUB.



12. Por último, haga clic en continuar para reiniciar a su nueva instalación de Kali. Si uso una memoria USB como unidad de destino, asegúrese de que ha habilitado el arranque desde dispositivos USB en la BIOS. Se le pedirá la contraseña la cual estableció anteriormente en cada arranque.



Después de la instalación

Ahora que ha completado la instalación de Kali Linux, es el momento de personalizar el sistema. La sección del [Uso General de Kali](#) en nuestro sitio tiene más información y también pueden encontrar consejos sobre cómo sacar el máximo provecho de Kali en nuestro [foros de usuarios](#).

Instalación de Kali Linux desde una memoria USB

El arranque y la instalación de Kali desde una memoria USB es nuestro método preferido y es la manera más rápida de correrlo. Para hacer esto, primero tenemos que crear la imagen ISO de Kali en una unidad de USB. Si a usted le gustaría añadir persistencia a la memoria USB de Kali Linux, por favor lea el documento completo antes de proceder a crear su imagen.

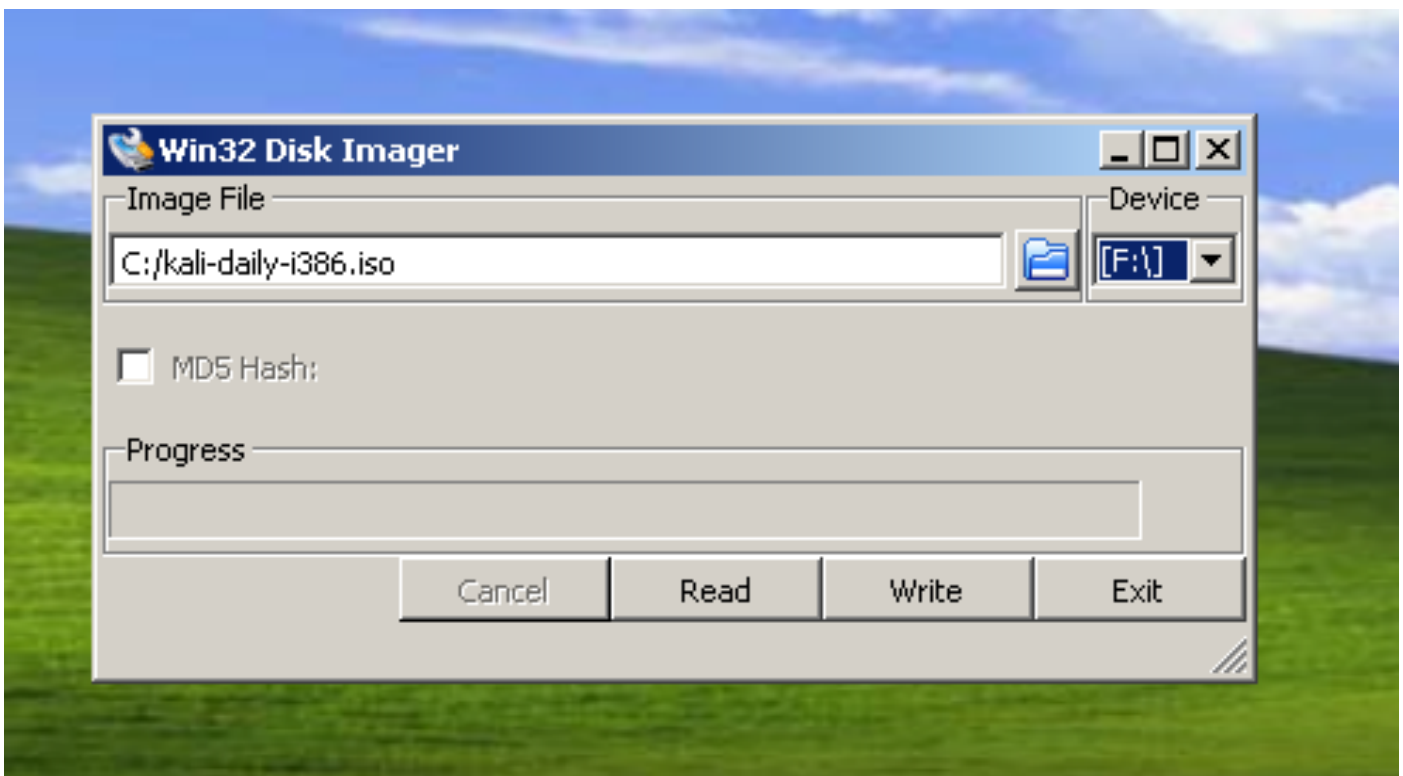
Preparativos para la copia USB

1. [Descarga Kali linux](#).
2. En Windows, descargar [Win32 Disk Imager](#).
3. No se necesita software especial si usa Linux como su sistema operativo.
4. Una memoria USB (con por lo menos 2GB de capacidad).

Procedimiento para la instalación de Kali Linux desde una memoria USB

Creando una imagen de Kali en Windows

1. Conecte su memoria USB en el puerto USB de Windows. Inicie el software Disk Imager Win32.
2. Elija el archivo ISO de Kali Linux con el que creará la imagen y verifique que la unidad USB que será sobrescriba es la correcta.



3. Una vez que la imagen haya sido creada, expulsar de forma segura la unidad USB desde la máquina Windows. Ahora puede utilizar la memoria USB para arrancar Kali Linux.

Creando una imagen de Kali en Linux

La creación de una memoria USB desde la cual pueda arrancar Kali Linux en un entorno de Linux es fácil. Una vez que haya descargado el archivo ISO de Kali, puede utilizar dd para copiarlo a la memoria USB:

ADVERTENCIA. Aunque el proceso de creación de imágenes de Kali en una memoria USB es muy fácil, usted puede fácilmente destruir particiones arbitrarias con **dd** si usted no entiende lo que está haciendo. Queda advertido.

1. Conecte el dispositivo USB al puerto USB de su ordenador Linux.
2. Compruebe que la ruta de su dispositivo de almacenamiento USB con `dmesg`.
3. Proceda (con cuidado) a crear la imagen de Kali Linux en el dispositivo USB:

```
dd if=kali.iso of=/dev/sdb
```

Eso es todo, de verdad! Ahora puede arrancar en un entorno Kali Live / Instalador usando el dispositivo USB.

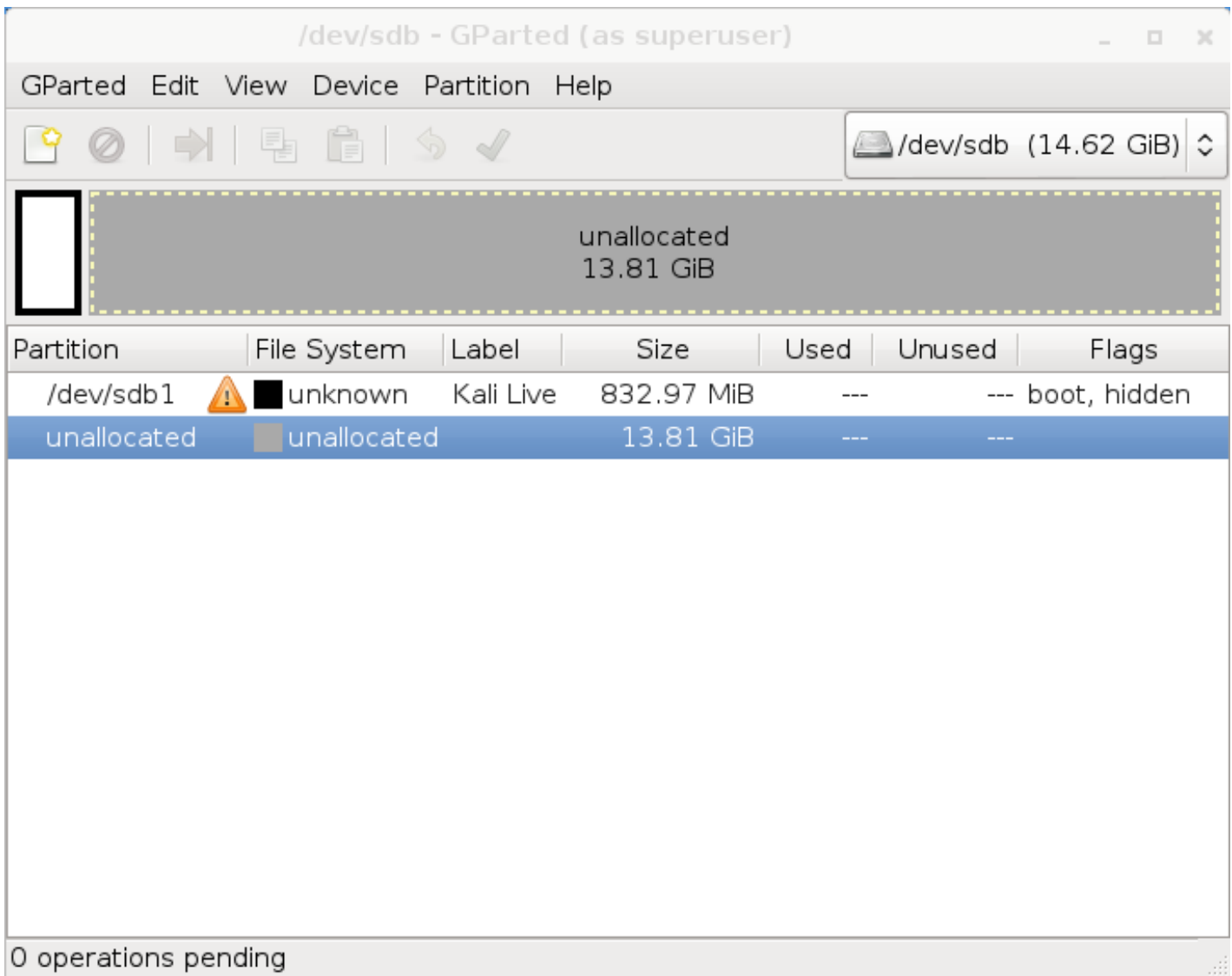
Agregando persistencia a su memoria USB de Kali Linux

La adición de persistencia (la capacidad de guardar archivos y los cambios a través de arranques en directo) a su imagen de Kali Linux puede ser muy útil en ciertas situaciones. Para agregar persistencia a su memoria USB de Kali Linux, siga estos pasos. **En este ejemplo, asumimos nuestra unidad USB es `/dev/sdb`**. Si desea agregar la persistencia, usted necesitará un dispositivo USB más grande que el que encontrará en nuestros requisitos anteriores.

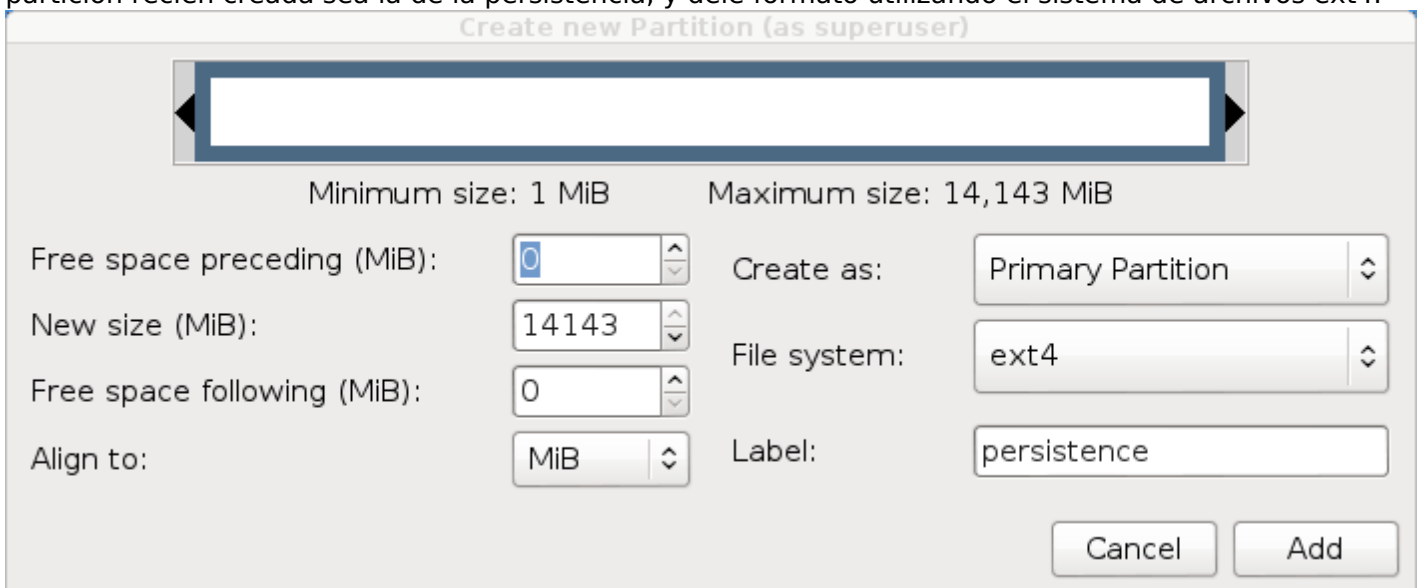
1. Cree la imagen de Kali Linux en su memoria USB como se ha explicado anteriormente, utilizando el "Método de Linux" y **dd**.
2. Cree y formatee una partición adicional en la memoria USB. En nuestro ejemplo, podemos utilizar `gparted` invocando:

```
gparted /dev/sdb
```

3. Su esquema de particionamiento actual debe ser similar a este:



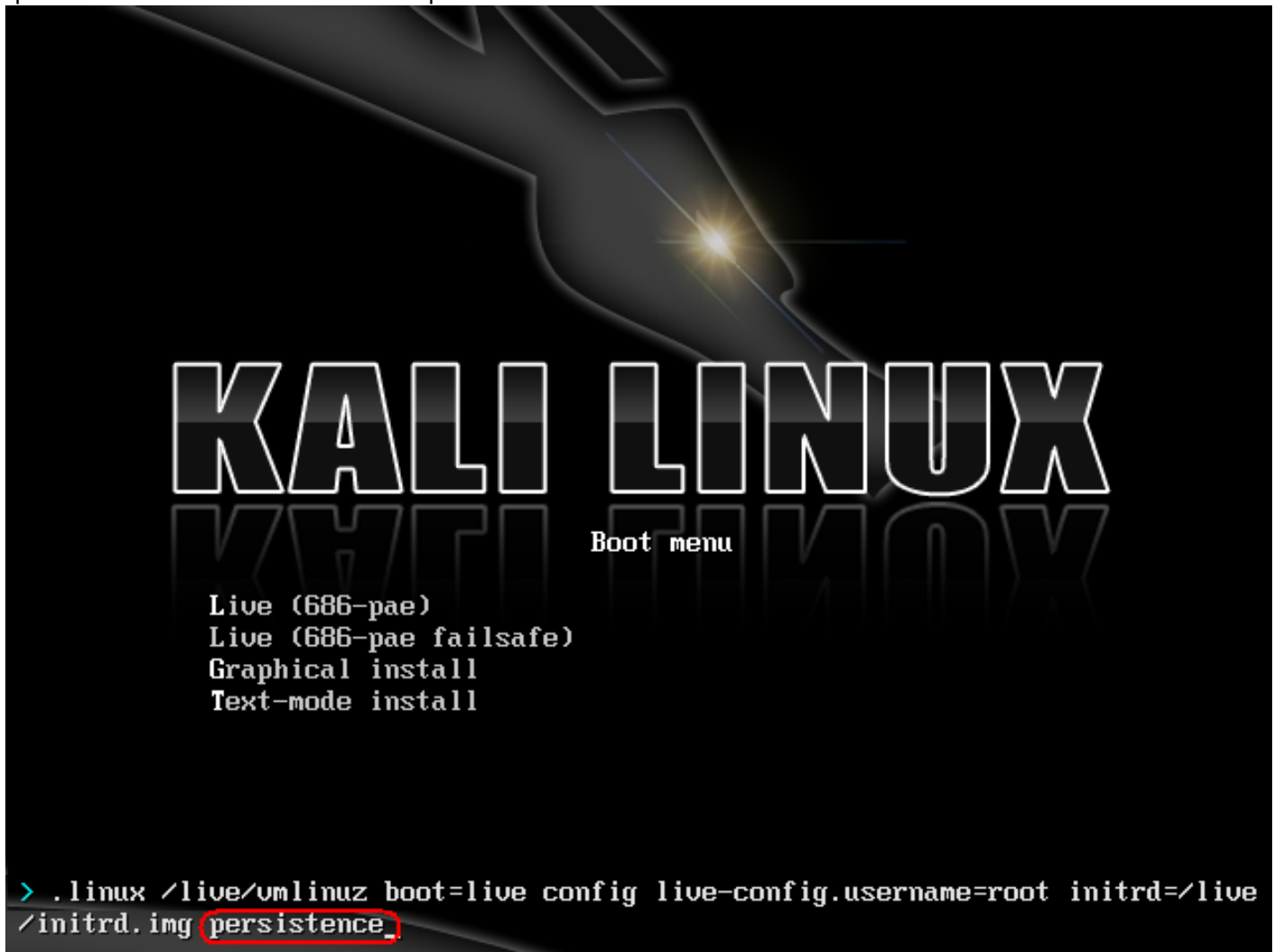
4. Proceda a formatear la nueva partición para ser utilizada para la persistencia. En nuestro ejemplo, hemos utilizado todo el espacio disponible restante. Asegúrese de que la etiqueta de volumen de la partición recién creada sea la de la persistencia, y dele formato utilizando el sistema de archivos ext4.



5. Una vez que el proceso se haya completado, monte su partición persistente USB utilizando los siguientes comandos:

```
mkdir /mnt/usb  
mount /dev/sdb2 /mnt/usb  
echo "/ union" && /mnt/usb/persistence.conf  
umount /mnt/usb
```

6. Conecte la memoria USB en el equipo que desea arrancar. Asegúrese de que su BIOS arrancará desde el dispositivo USB. Cuando la pantalla de arranque de Linux Kali aparezca, seleccione "boot en vivo" en el menú (no presione enter), y presione el botón de tabulación. Esto le permitirá editar los parámetros de arranque. Agregue la palabra "persistence" al final de la línea de parámetro de arranque cada vez que quiera montar su almacenamiento permanente.



Instalación de Kali Linux en un disco duro

Requisitos de instalación de Kali Linux

Instalar Kali Linux en su ordenador es un proceso fácil. Primero necesitará hardware que sea compatible en su ordenador. Kali es soportado en las siguientes plataformas: i386, en amd64, y en ARM (tanto armel como armhf). Los requisitos de hardware son mínimos y se enumeran a continuación, aunque mejor hardware naturalmente ofrece un mejor rendimiento. Las imágenes i386 tienen un núcleo predeterminado PAE, por lo que pueden ejecutarse en sistemas con más de 4 GB de RAM. [Descargue Kali Linux](#) y, o bien grabe el ISO en un DVD, o [prepare una memoria USB con Kali Linux Live](#) como medio de instalación. Si usted no tiene una unidad de DVD o un puerto USB de su ordenador, visite [Instalación de Kali Linux a través de la red](#).

Requisitos previos de instalación

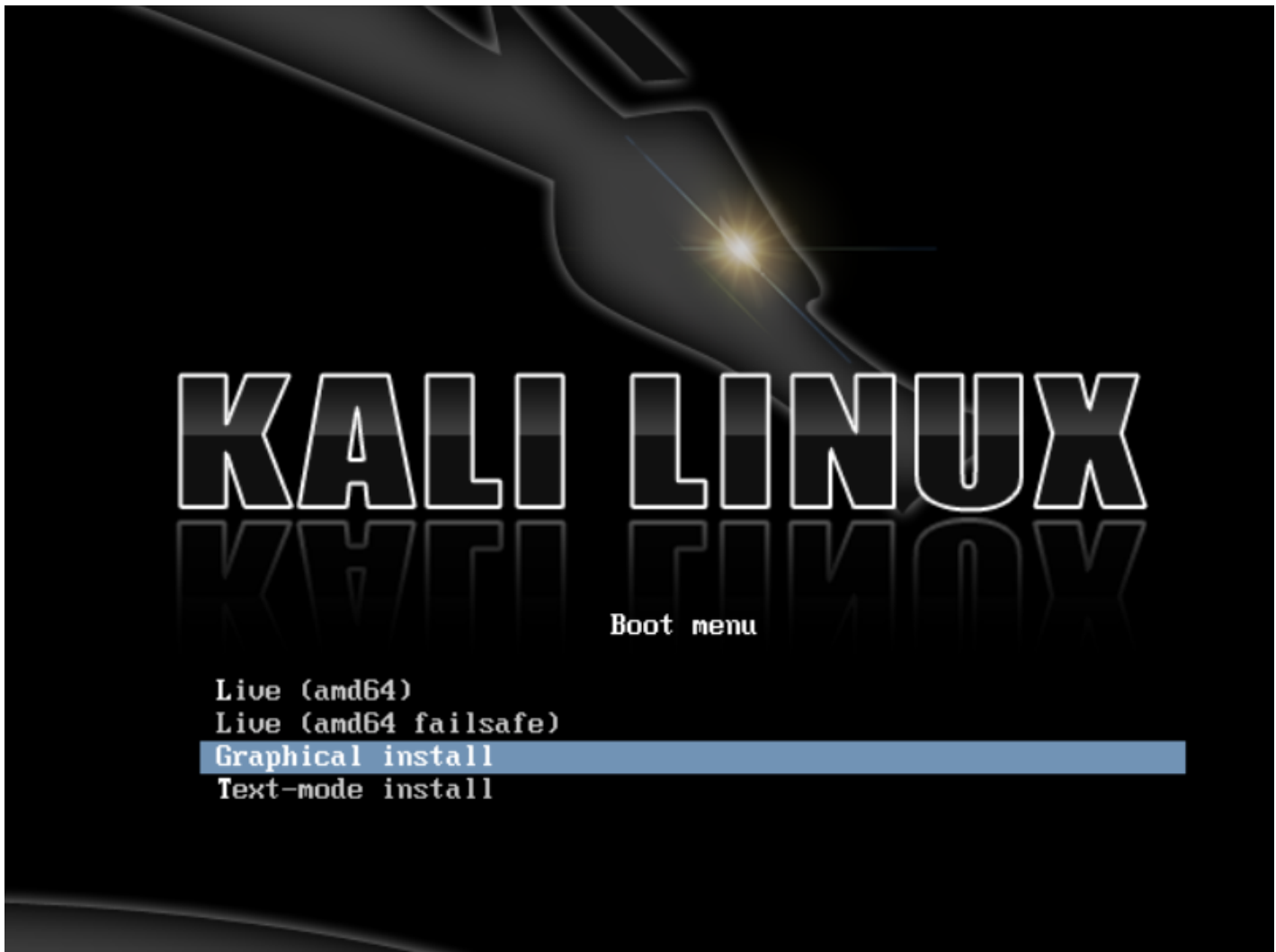
- Un mínimo de 8 GB de espacio en disco para la instalación de Kali Linux.
- Para las arquitecturas i386 y amd64, un mínimo de 512 MB de RAM.
- Lectora de CD/DVD / Soporte para iniciar desde una memoria USB

Preparandose la instalación

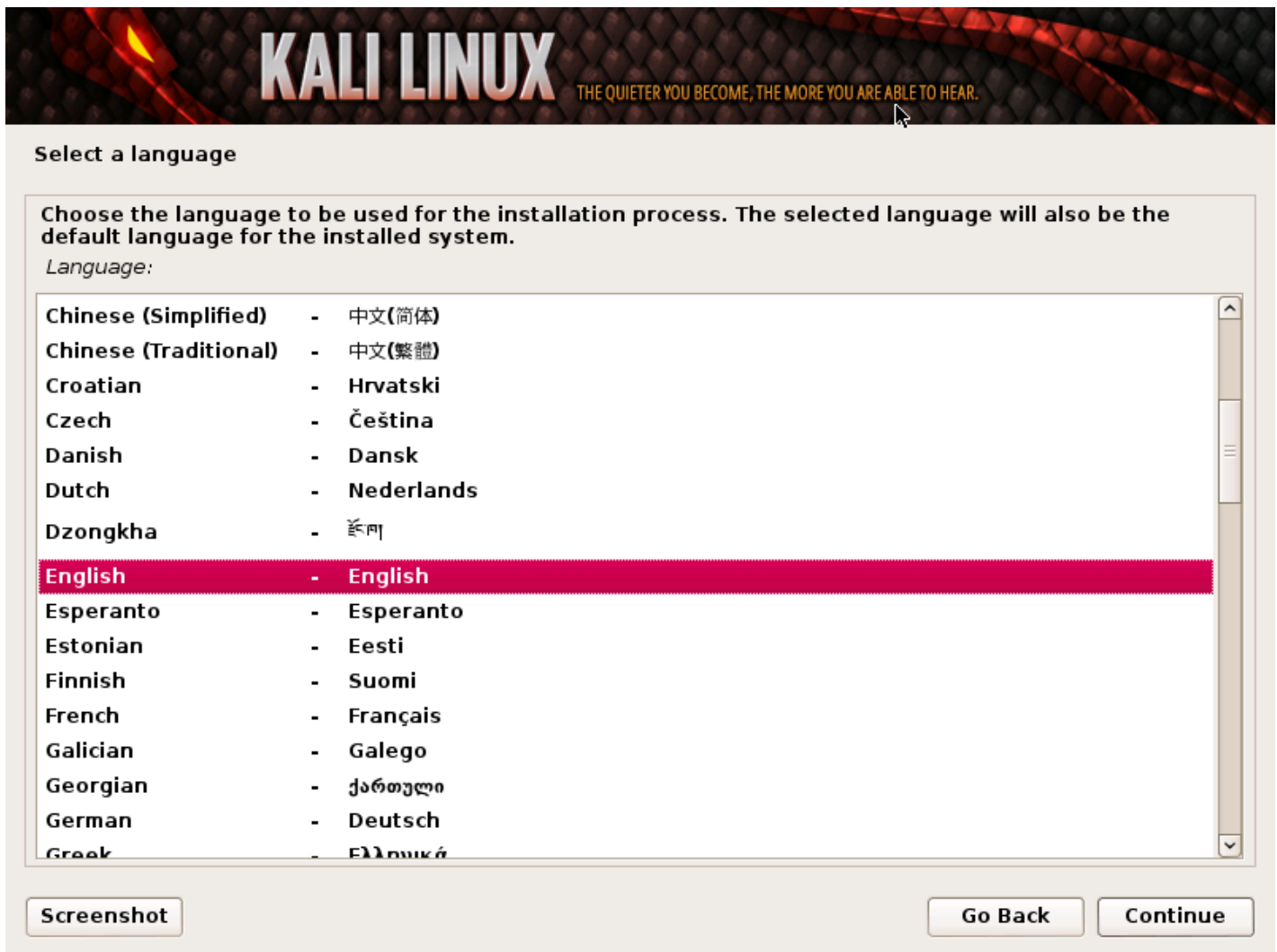
1. [Descargue Kali Linux](#).
2. Queme el Kali Linux ISO a DVD o [prepare una memoria USB con Kali Linux Live como medio de instalación](#).
3. Asegúrese de que su ordenador está configurado para arrancar desde un CD / USB en el BIOS.

Procedimiento de instalación de Kali Linux

1. Para iniciar la instalación, arranque con el medio de instalación elegido. Usted debe ser recibido con la pantalla de arranque de Kali. Elegir si desea proceder con una instalación gráfica o en modo texto. En este ejemplo, hemos elegido una instalación gráfica.



2. Seleccione el idioma que desee y luego su país de localización. También se le pedirá que configure su teclado con el mapa de teclado adecuado.



3. El programa de instalación copiará la imagen en su disco duro, probará las interfaces de red, y luego le pedirá que introduzca un nombre de host para el sistema. En el siguiente ejemplo, hemos entrado "Kali", como el nombre de host.



Configure the network

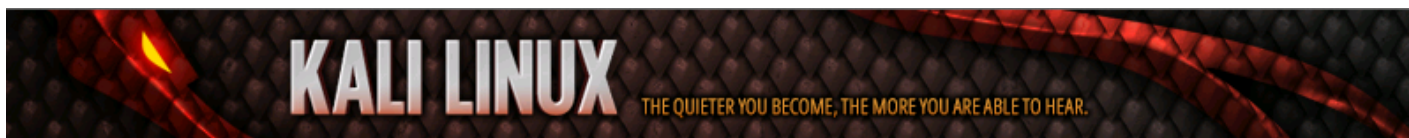
Please enter the hostname for this system.

The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.

Hostname:

[Screenshot](#) [Go Back](#) [Continue](#)

4. Introduzca una contraseña robusta para la cuenta de root y cree las cuentas adicionales que desee.



Set up users and passwords

You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.

Note that you will not be able to see the password as you type it.

Root password:

Please enter the same root password again to verify that you have typed it correctly.

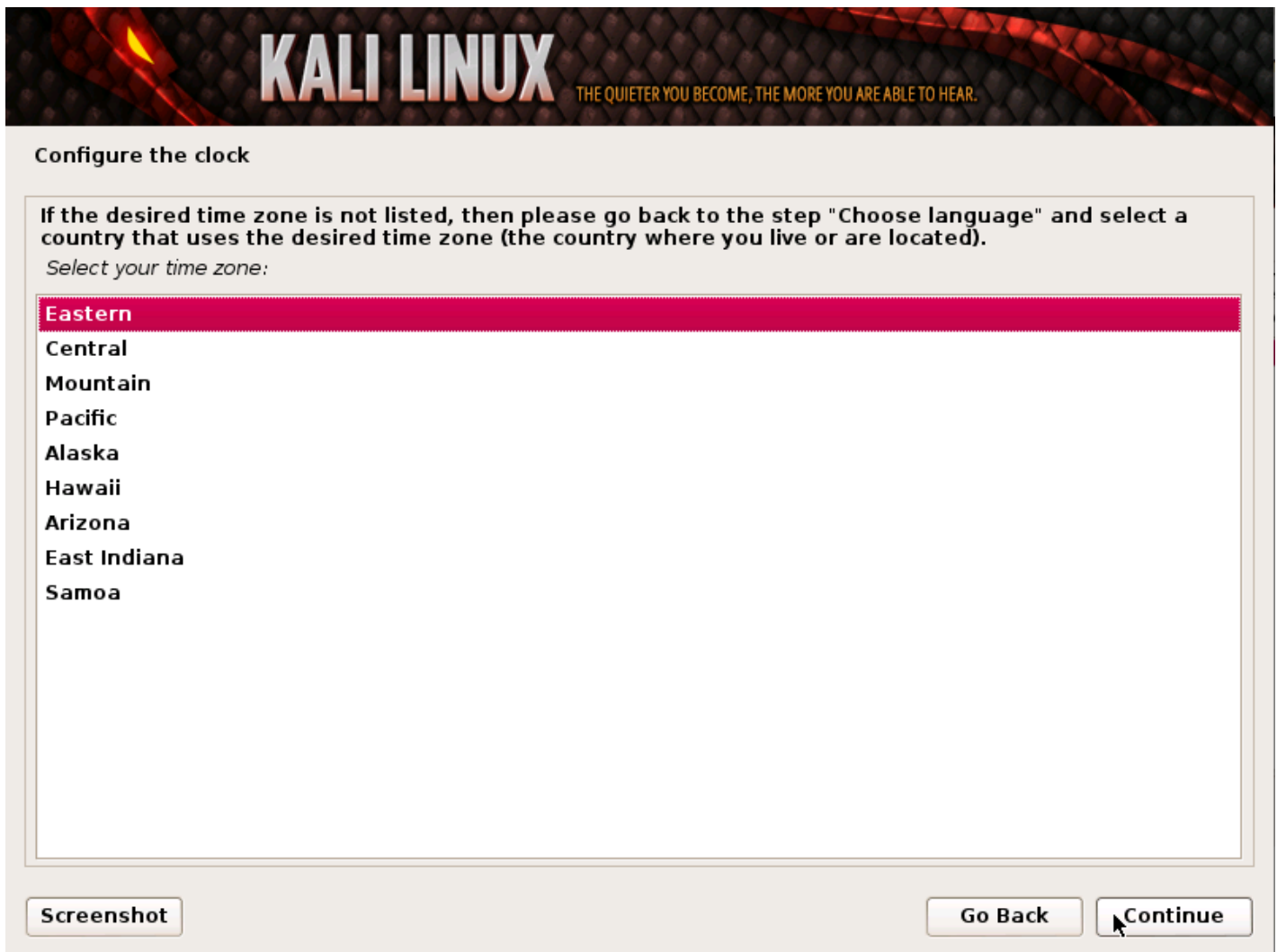
Re-enter password to verify:

Screenshot

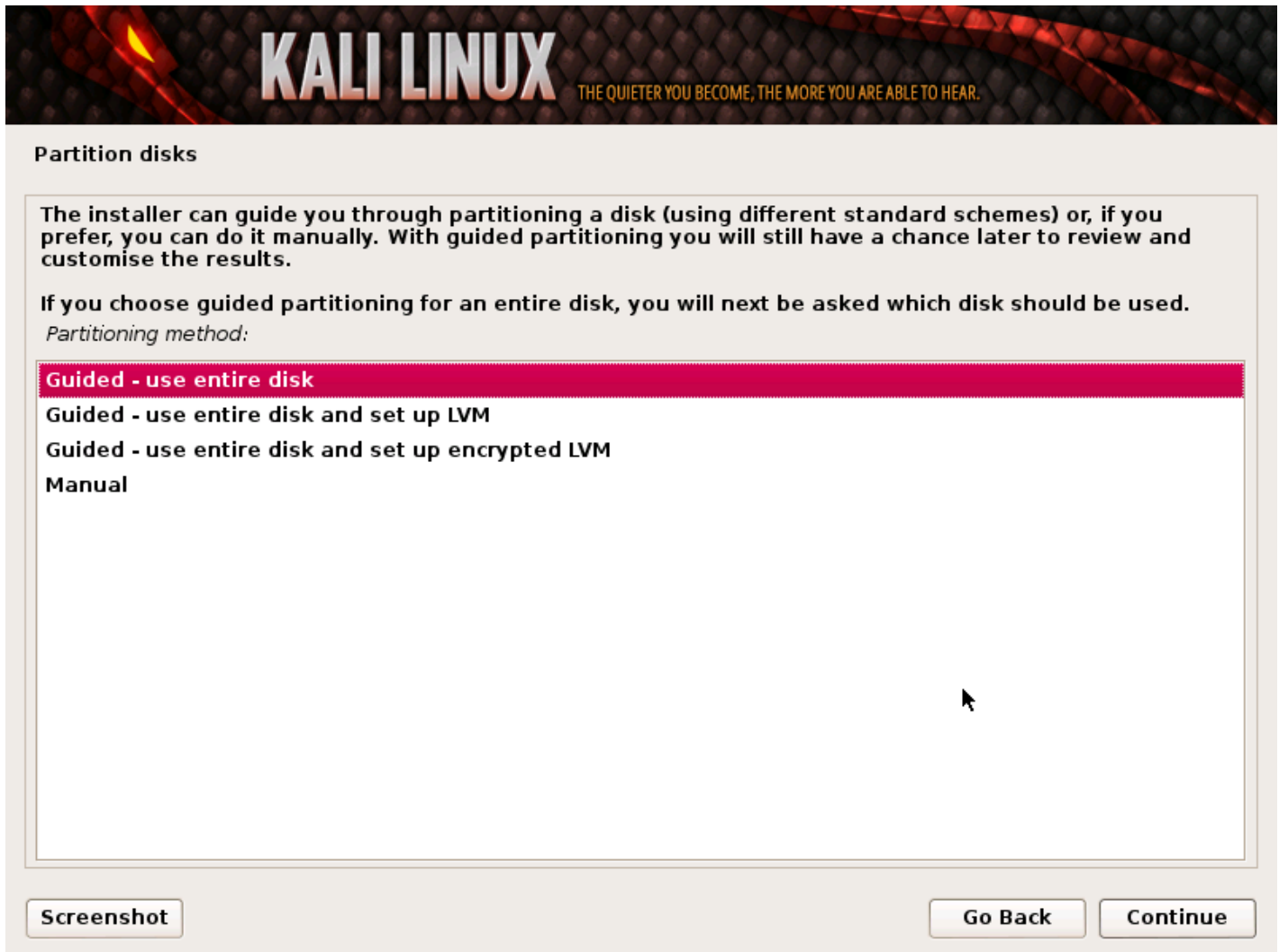
Go Back

Continue

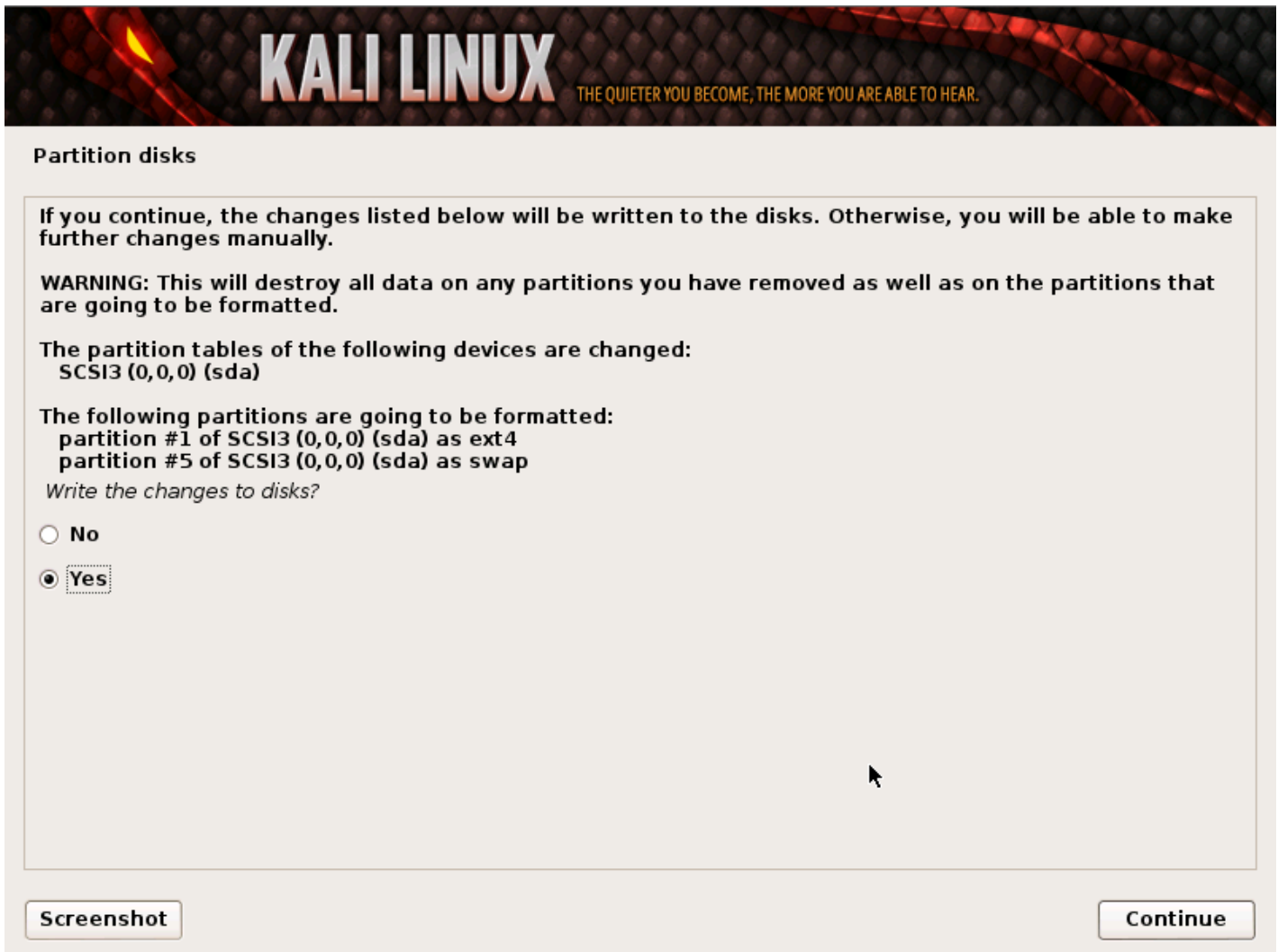
5. Configure su zona horaria.



6. El instalador probará sus discos, y le ofrecerá cuatro opciones. En nuestro ejemplo, vamos a usar el disco entero en nuestro ordenador y no la configuración de LVM (Logical Volume Manager). Los usuarios experimentados pueden utilizar el método manual de partición para una configuración más granular.

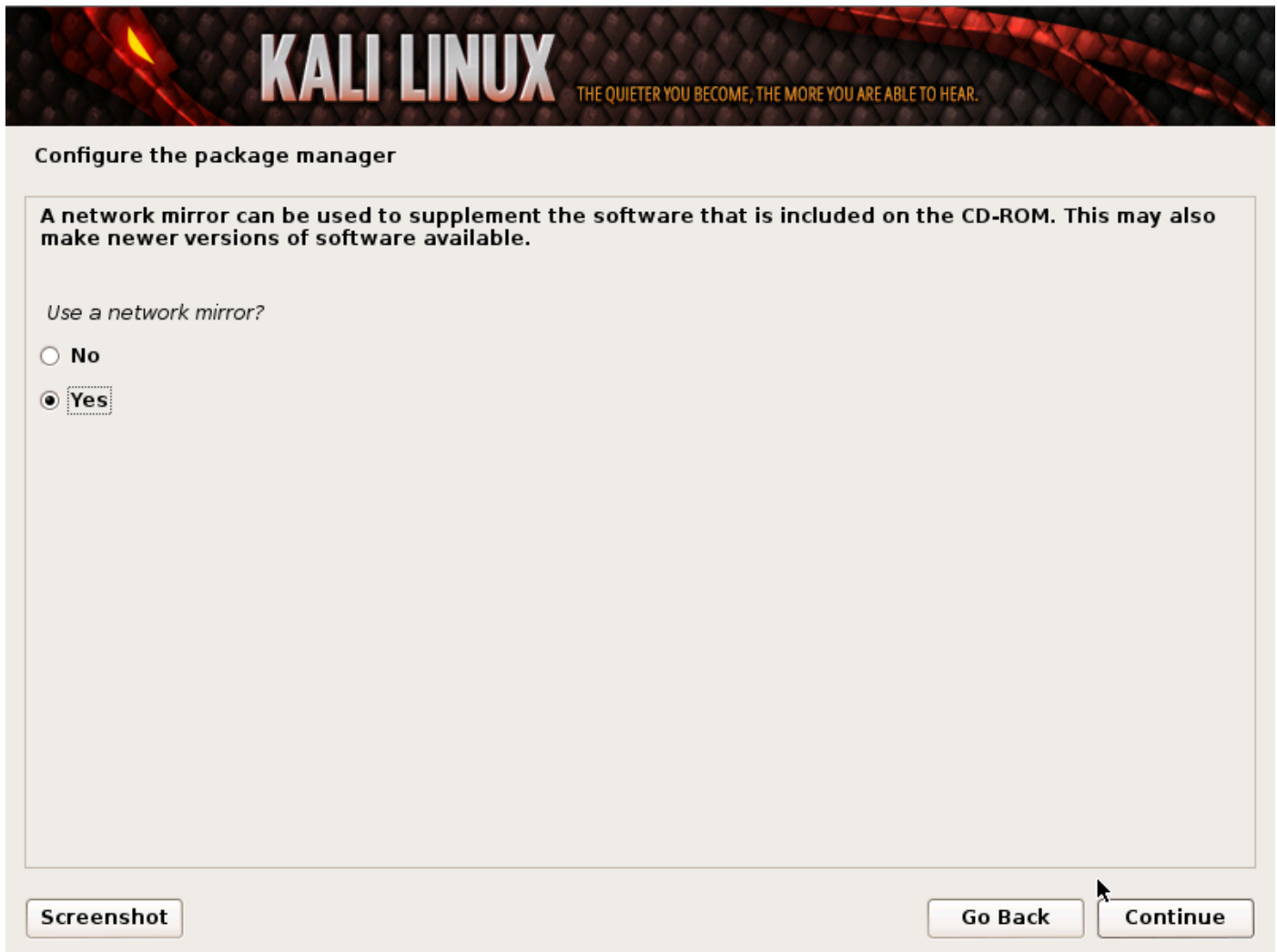


7. Entonces tendrá una última oportunidad para revisar la configuración de su disco antes de que el instalador haga que los cambios sean irreversibles. Después de hacer clic en Continuar, el instalador irá a trabajar y usted tendrá una instalación casi terminada.



8. Configurar espejos de red. Kali utiliza un repositorio central para distribuir aplicaciones. Tendrá que introducir la información de proxy adecuado según sea necesario.

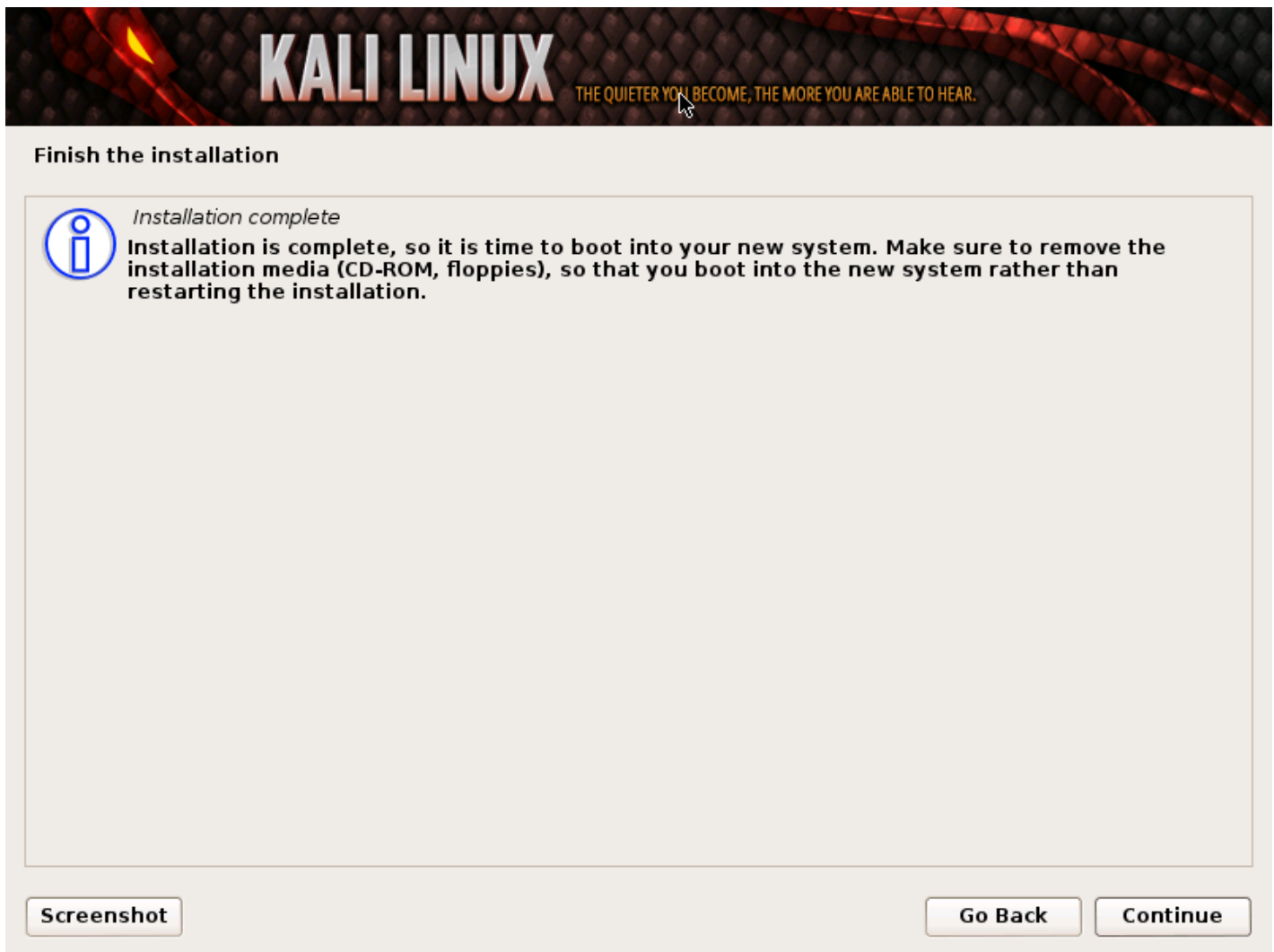
NOTE! Si selecciona “NO” en esta pantalla, **NO** usted no será capaz de instalar paquetes desde repositorios de Kali.



9. El próximo paso es instalar GRUB.



10. Por último, haga clic en Continuar para reiniciar en su nueva instalación de Kali.



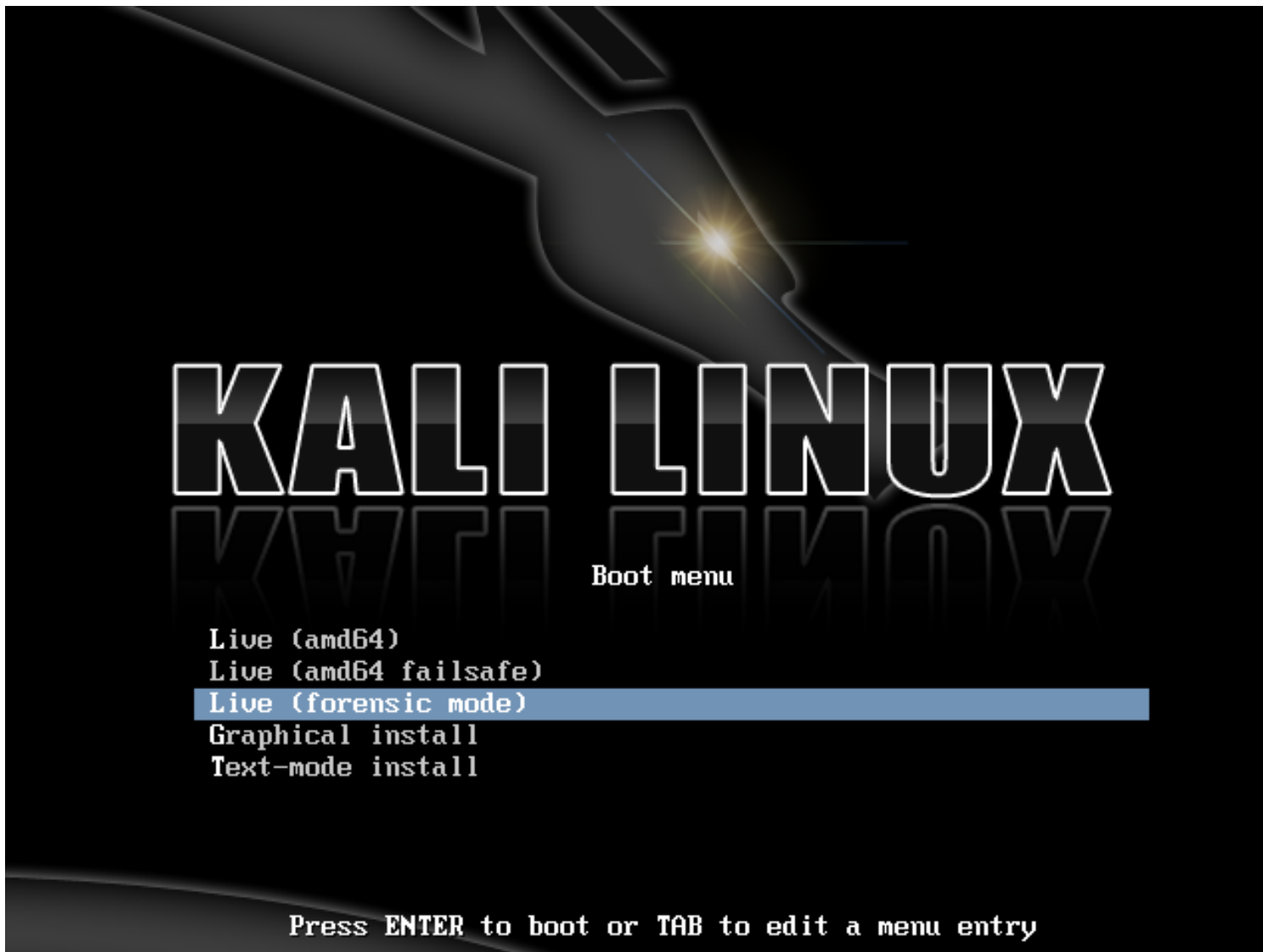
Después de la instalación

Ahora que ha completado la instalación de Kali Linux, es el momento de personalizar el sistema. La sección [Uso General de Kali Linux](#) en nuestro sitio tiene más información y también se pueden encontrar consejos sobre cómo sacar el máximo provecho de Kali en nuestros [Foros De Usuarios](#).

05. Uso general de Kali Linux

Modo Forense de Kali Linux

BackTrack Linux introdujo un “Arranque Forense” para el sistema operativo que se prolongó a través de BackTrack 5 y ahora existe en Kali Linux. La opción del “Arranque Forense” ha demostrado ser muy popular debido a la amplia disponibilidad de nuestro sistema operativo. Muchas personas tienen ISOs de Kali por ahí y cuando surge la necesidad forense pueden usar Kali Linux para hacer cualquier trabajo ya que es rápido y fácil de usar. Pre-cargado con el software de código abierto más popular forense, Kali es una herramienta muy útil cuando se necesita hacer un trabajo utilizando código abierto forense.



Cuando se inicia en el modo de arranque forense, hay algunos cambios muy importantes que se realizan.

1. En primer lugar, el disco duro interno no se toca. Esto significa que si hay una partición de “swap” no será utilizada y los discos internos no serán montados automáticamente. Para comprobar esto, tomamos un sistema estándar y retiramos el disco duro. Lo conectamos a un paquete comercial forense y tomamos un hash de la unidad. Luego volvimos a conectar el disco duro al ordenador y arrancamos desde el disco de Kali en el modo de arranque forense. Después de haber usado Kali por un período de tiempo apagamos el sistema, quitamos el disco duro, y le tomamos el hash de nuevo. Estos hashes

coincidieron, lo que indica que en ningún momento fue cambiado algo en la unidad del todo.

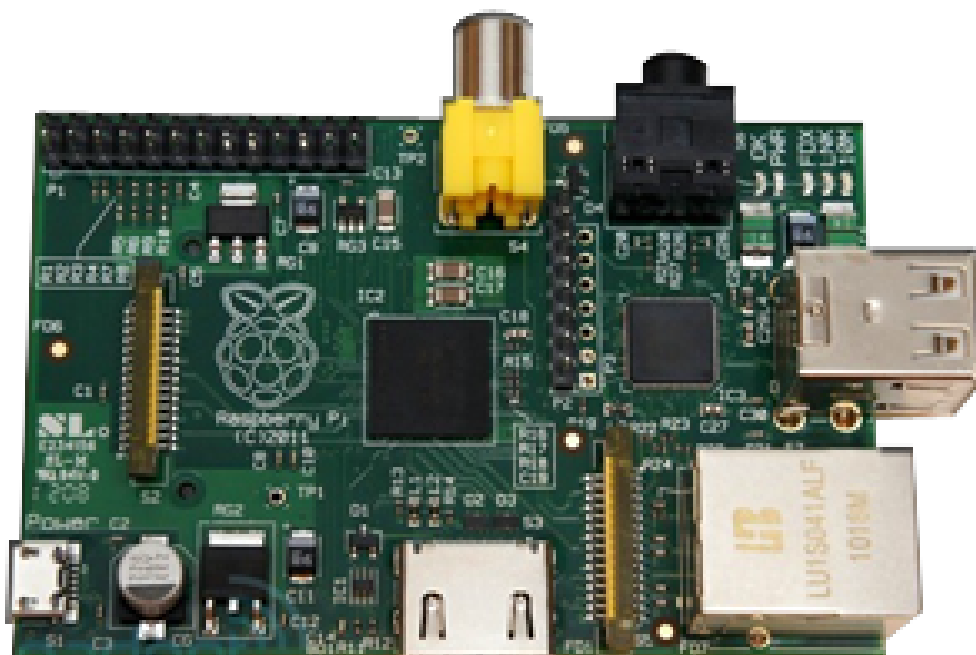
2. El otro cambio igual de importante que se hizo fue que desactivamos el soporte automático de cualquier medio externo. Así que memorias USB, discos compactos, etc no serán montado automáticamente cuando sean insertados. La idea detrás de esto es simple: nada debe suceder en cualquier medio sin la acción directa del usuario. Cualquier cosa que usted hace como un usuario es su culpa.

Si usted está interesado en el uso de Kali para el análisis forense real de cualquier tipo, le recomendamos que usted no tome nuestra palabra, sino pruébelo usted mismo. Todas las herramientas forenses debe ser siempre validadas para asegurarse de que sabe cómo se comportarán en cualquier circunstancia en que pueda usarlas.

Y finalmente, como Kali se enfoca en tener la mejor colección de herramientas de código abierto de pruebas de penetración disponible, es posible que hayamos perdido su herramienta favorita forense de código abierto. De ser así, [háganoslo saber](#)! Estamos siempre en la búsqueda de herramientas de alta calidad de código abierto que podamos añadir a Kali para que sea aún mejor.

06. Arquitectura ARM de Kali

Instalando Kali ARM en un Raspberry Pi



Raspberry Pi

El Raspberry Pi es una computadora ARM de gama baja y barata. A pesar de sus menos-que-estelares pliego de especificaciones, la capacidad de financiación hace que sea un excelente opción para un sistema Linux pequeño y puede hacer mucho más que actuar como un PC multimedia.

Stock Kali en Raspberry Pi - Manera Fácil

Si todo lo que quiere hacer es instalar Kali en su Raspberry Pi, siga estas instrucciones:

1. Obtenga una tarjeta SD de 8 GB (o más). Tarjetas Clase 10 son altamente recomendadas.
2. Baje la imagen Kali Linux para Raspberry Pi de nuestra area [downloads](#).
3. Use el utilitario **dd** para crear la imagen que ira en su tarjeta SD. En nuestro ejemplo, nosotros asumimos que el dispositivo de almacenamiento esta localizado en /dev/sdb. **Cambie este si es necesario.**

Alerta! Este proceso borrara su tarjeta SD. Si usted escoge un dispositivo de almacenamiento distinto, podria estar borrando su disco duro.

```
root@kali:~ dd if=kali-pi.img of=/dev/sdb bs=512k
```

Este proceso puede tomarse su tiempo dependiendo de la velocidad de su dispositivo USB y tamaño de la imagen. Una vez que la operación dd este completa, reinicie su Raspberry Pi con su tarjeta SD conectada. Estaras habilitado para loguearte en Kali (root / toor) y digitar **startx**. Y eso es, esta listo!

Kali en Raspberry Pi - Versión Larga

Si usted es un desarrollador y quiere jugar con la imagen de Kali Raspberry Pi, incluyendo cambiar la configuración del kernel, aventurese y chequee nuestro articulo de personalización de Raspberry Pi.

TBD.

Preparación de un Kali Linux chroot en ARM.

Aunque puede [descargar imagenes ARM de Kali](#) desde nuestra zona de descargas, algunos prefieren construir sus propios rootfs en Kali. El siguiente procedimiento muestra un ejemplo de la construcción de un Kali rootfs tipo armhf.

Instalar las herramientas necesarias y las dependencias

```
apt-get install debootstrap qemu-user-static
```

Definir la arquitectura y paquetes personalizados

Aquí es donde se definen algunas variables de entorno para la arquitectura de ARM requerida (armel vs armhf), y listan los paquetes que serán instalados en la imagen. Serán usado en todo el artículo, así que asegúrese de modificarlos dependiendo de sus necesidades.

```
export packages="xfce4 kali-menu kali-defaults nmap openssh-server"  
export architecture="armhf"  
#export disk="/dev/sdc"
```

Construir el rootfs de Kali

Creamos una estructura de directorios estándar y arrancamos usando el rootfs de ARM desde los repositorios de Linux Kali. A continuación, copiar **qemu-arm-static** desde nuestro equipo anfitrión a el rootfs para iniciar la 2da etapa chroot.

```
cd ~  
mkdir -p arm-stuff  
cd arm-stuff/  
mkdir -p kernel  
mkdir -p rootfs  
cd rootfs  
  
debootstrap --foreign --arch $architecture kali kali-$architecture http://repo.kali.org/kali  
cp /usr/bin/qemu-arm-static kali-$architecture/usr/bin/  
LANG=C chroot kali-$architecture /debootstrap/debootstrap --second-stage
```

2nda etapa chroot

Aquí es donde debemos configurar los ajustes básicos de imagen como mapas de teclado, repositorios, el comportamiento predeterminado de interfaz de red (cambiar si es necesario), etc.

```
cat &lt; kali-$architecture/debconf.set  
console-common console-data/keymap/policy    select Select keymap from full list
```

```
console-common console-data/keymap/full      select en-latin1-nodeadkeys
EOF

cat kali-$architecture/etc/hostname

cat &lt; kali-$architecture/etc/network/interfaces
auto lo
iface lo inet loopback
auto usbmon0
iface usbmon0 inet dhcp
EOF
```

3ra etapa chroot

Aquí es donde entra en juego la personalización. Sus \$paquetes serán instalados y contraseña de root será establecida como "toor", así como otros cambios de configuración y correcciones..

```
mount -t proc proc kali-$architecture/proc
mount -o bind /dev/ kali-$architecture/dev/
mount -o bind /dev/pts kali-$architecture/dev/pts

cat &lt; kali-$architecture/third-stage
#!/bin/bash
debconf-set-selections /debconf.set
rm -f /debconf.set
apt-get update
apt-get -y install git-core binutils ca-certificates
apt-get -y install locales console-common less nano git
echo "root:toor" | chpasswd
sed -i -e 's/KERNEL!="&quot;eth*"/KERNEL!="&quot;/' /lib/udev/rules.d/75-persistent-net-generator.rules
rm -f /etc/udev/rules.d/70-persistent-net.rules
apt-get --yes --force-yes install $packages
rm -f /third-stage
EOF

chmod +x kali-$architecture/third-stage
LANG=C chroot kali-$architecture /third-stage
```

Configuración manual dentro del chroot

Usted puede realizar las modificaciones finales en el entorno rootfs manualmente mediante chrooting y haciendo los últimos cambios necesarios.

```
LANG=C chroot kali-$architecture
{realizar cambios adicionales en el chroot}
exit
```

Limpiando los archivos bloqueados en el chroot

Considere el hecho de que algunos paquetes que haya instalado pueden haber bloqueado los archivos en el rootfs (como el funcionamiento de los servicios dentro de la jaula), que deben ser “liberado” antes de que podamos cerrar nuestro chroot. Usted probablemente tendrá que dejar algunos servicios en su jaula antes de que pueda desmontar. Los comandos para desmontar proc y dev son:

```
umount kali-$architecture/proc
umount kali-$architecture/dev/pts
umount kali-$architecture/dev/
```

Sin embargo, si usted todavía tiene algunos servicios que se ejecutan dentro del chroot, recibirá un error similar a este:

```
root@rootfs-box:~ umount kali-$architecture/proc
root@rootfs-box:~ umount kali-$architecture/dev/pts
root@rootfs-box:~ umount kali-$architecture/dev/

umount: kali-armhf/dev: dispositivo está ocupado.
(En algunos casos, los comandos lsof(8) o fuser(1) nos dan información
útil acerca de los procesos que utilizan el dispositivo)
root@rootfs-box:~
```

Si este es el caso, se puede comprobar que el archivo / servicio está bloqueando el chroot con el siguiente comando:

```
root@rootfs-box:~/arm-stuff/rootfs:~ lsof |grep kali-armhf
...
dbus-daem 4419 messagebus mem REG 8,1 236108 15734602 dbus-daemon
dbus-daem 4419 messagebus mem REG 8,1 93472 17705250 ld-2.13.so
...
dbus-daem 4419 messagebus mem REG 8,1 100447 17705251 libpthread-2.13.so
dbus-daem 4419 messagebus mem REG 8,1 22540 17705240 librt-2.13.so
dbus-daem 4419 messagebus mem REG 8,1 893044 17705232 libc-2.13.so
...
```

A partir de este resultado, podemos ver que el proceso dbus todavía se está ejecutando dentro del chroot. Tenemos que parar el proceso dentro de la jaula antes de continuar. Si ya ha desmontado PROC o dev con éxito, vuelvalos a montar usando los mismos comandos que hemos usado anteriormente, chroot dentro del rootfs y detenga el servicio dbus (y cualquier otro que pueda ser necesario):

```
# mount -t proc proc kali-$architecture/proc
# mount -o bind /dev/ kali-$architecture/dev/pts

LANG=C chroot kali-$architecture
/etc/init.d/dbus stop
exit
```

Una vez que todos los archivos bloqueados y los servicios sean liberados, usted podrá desmontar proc y dev limpiamente:

```
root@rootfs-box:~/arm-stuff/rootfs~ umount kali-$architecture/proc
root@rootfs-box:~/arm-stuff/rootfs~ umount kali-$architecture/dev/pts
root@rootfs-box:~/arm-stuff/rootfs~ umount kali-$architecture/dev/
root@rootfs-box:~/arm-stuff/rootfs~
```

Cleanup

Por último, se ejecuta un script de limpieza en nuestro entorno chroot para liberar el espacio utilizado por los archivos almacenados en caché, y otros trabajos de limpieza que se requieran:

```
cat &lt; kali-$architecture/cleanup
#!/bin/bash
rm -rf /root/.bash_history
apt-get update
apt-get clean
rm -f cleanup
EOF

chmod +x kali-$architecture/cleanup
LANG=C chroot kali-$architecture /cleanup

/etc/init.d/dbus stop

umount kali-$architecture/proc
umount kali-$architecture/dev/pts
umount kali-$architecture/dev/

cd ..
```

¡Felicitaciones! Su Kali rootfs ARM personalizado se encuentra en el directorio de \$kali-arquitectura. Ahora puede comprimir este directorio, o copiarlo en un archivo de imagen para seguir trabajando.