# Creating A Kali Linux Bootable USB with Encrypted Persistence with MacOS

Creating a Kali Linux bootable USB with encrypted persistence was more complicated than I thought. I couldn't seem to find an up-to-date guide that uses only tools available to MacOS users, so I decided to create one in hopes it might help others looking to do the same thing. Almost all of the commands will require sudo, so I recommend just switching to root using sudo -s.

### Creating The Bootable USB

1. Download the Kali Live .iso image from the official website (https://www.kali.org/downloads/). Verify the checksums with the command:

```
shasum -a 256 /path/to/file
```

The output should match the sha256sums listed next to the download.

2. Backup your computer. It's incredibly easy to reformat your device's hard drive instead of the USB, so this is a good precautionary measure.

3. Find the name of the USB drive. Enter

```
diskutil list
```

while the USB drive is not plugged in. Plug in the USB and re-enter the command. The new item is the name of the USB.

4. Transfer the .iso image onto the USB drive.

```
diskutil eraseDisk FAT32 KALI /dev/<disk>
disutil unmountDisk /dev/<disk>
dd if=/path/to/file of=/dev/<disk> bs=1m
```

4. Boot into the disk by pressing alt key while the computer restarts. Choose Live Kali.

### Setting Up Persistence (with Encryption)

5. Create new partition to store files on. The name of your USB will be different in Kali than in MacOS.

```
fdisk -l
fdisk /dev/<disk>
type n, for new partition
type p, for primary and select defaults
type w, to save your changes
```

6. Reboot from the UBS again.

```
reboot
```

7. (optional) Setup encryption on said partition if desired. This will create a mapping inside. If you do this, refer to the partition as /dev/mapper>/ after this step. If not, just refer to it as /dev/

```
cryptsetup create my_usb /dev/<disk>/
cryptsetup -vy luksFormat /dev/<disk>/<name>
cryptsetup luksOpen /dev/<disk>/<name>
```

8. Create file system on new partition.

```
mkfs.ext3 -L persistence /dev/mapper/<name>
e2label /dev/mapper/<name> persistence
```

9. Create mount point on new partition.

```
mkdir -p /mnt/<name>
mount /dev/mapper/<name> /mnt/<name>
echo “/ union” > /mnt/<name>/persistence.conf
```

10. Unmount and reboot.

```
umount /dev/mapper/<name>
cryptsetup luksClose /dev/mapper/<name>
reboot now
```