**Encryption using encfs (Encrypt FileSystem)**

On your Mac:

1. Install encfs
   1. Download [*encfs.rb*](https://amazon.awsapps.com/workdocs/index.html#/folder/c7d3a9cb4db80cb0959395e7e9530b10cce68c6557fe5a2ecefe2a7a5f0788ca)
   2. Install encfs with *brew install -s encfs.rb*
2. Format a USB key with *Disk Utility*:
   1. Name: USB **<= choose what you want**
   2. format: MS-DOS (FAT)

On the Coral board:

1. Install encfs with *sudo apt-get install encfs*
2. Become root user by *sudo su –* (Note: when in root user mode, you DO NOT need to use *sudo* for mounting)
3. Make usb directory in the media folder to mount the usb (*mkdir /media/usb-drive)*
4. Check where the usb stick is connected using *fdisk -l*
5. Mount the usb stick to the created folder (*mount /dev/sda(x) /media/usb-drive*)
6. Initialize the encryption layer with: *encfs /media/.images /media/images*

This will create two folders. The first one, .***images***, will contain the encrypted information. The second one, ***images***, is where the decrypted version will be mounted when you want to access your information. If neither of these folders exist already, you will be prompted asking if you want to create them. Enter '**y**' at the prompts to allow the folders to be created. When asked for encryption level, just hit **[Enter]** and your new encrypted folder will be created with the standard options.

1. Run the capture.py script- *python3 capture.py –image –output /media/usb-drive/images*
2. After running the script go back to being root user and unmount the encryption layer- *fusermount -u /media/usb-drive/images*
3. Unmount the usb- *umount /media/usb-drive*

On your Mac:

1. You won’t be able to view the data on the USB stick just by plugging it in.
2. Mount the encryption layer to the USB stick- *encfs /Volume/USB/.images /Volume/USB/images*
3. Enter the password
4. You should be able to see the images taken on the coral board