Lab 1

Virtual Machines

ITSC 306: Computer Forensics

ITSC306: Computer Forensics

Lab 1: Virtual Machines

Lab Outcome

- Create a VMWare image that can be used for the forensic analysis of digital evidence.

Readings

- SIFT Documentation (https://www.sans.org/tools/sift-workstation/)
- Remnux Docs: (https://docs.remnux.org/)
- Remnux Installation: (https://docs.remnux.org/install-distro/install-from-scratch)

Introduction

An important part of the forensic process is having the proper environment to analyze the evidence once it has been collected. It is important to have the required tools to conduct the analysis and to be able to view the evidence in a read-only format. One of the most important rules of digital analysis is not changing the evidence during the analysis.

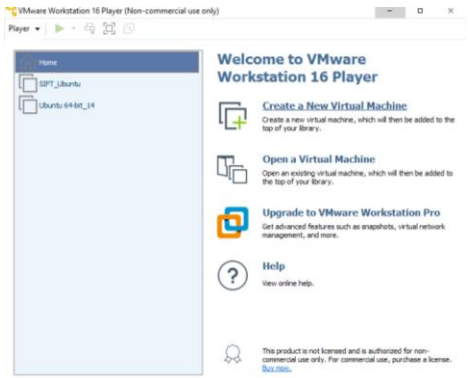
In this lab, you will create a VMware image using Ubuntu Desktop 20.04 as the operating system, and then add the SIFT (forensic tools) and REMnux (malware analysis tools) packages. In this Lab, we will install SIFT on Ubuntu. We will use VMWare and VirtualBox. You can choose one only.

VMWare

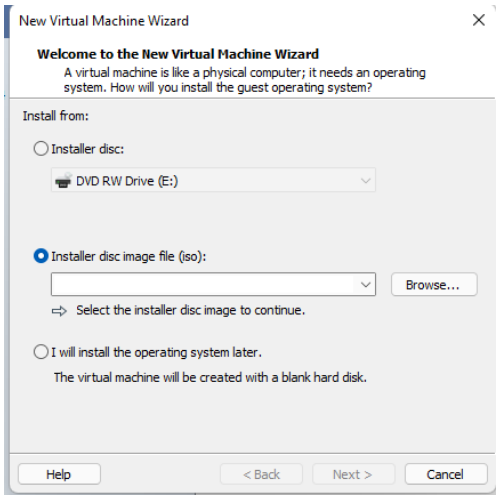
For Reading: https://www.sans.org/tools/sift-workstation/

For this part, we will use Ubuntu 20.04. Then we will install SIFT package.

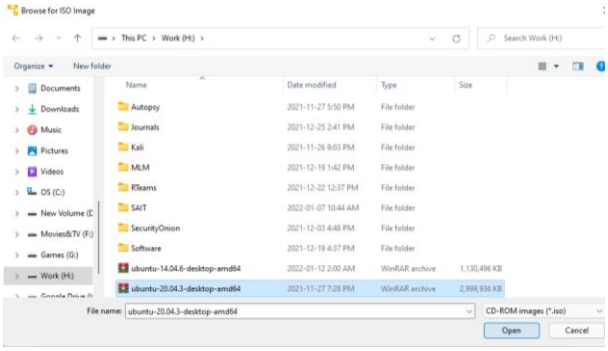
Step 1: Using VMWare, create the machine. Follow the screenshots below



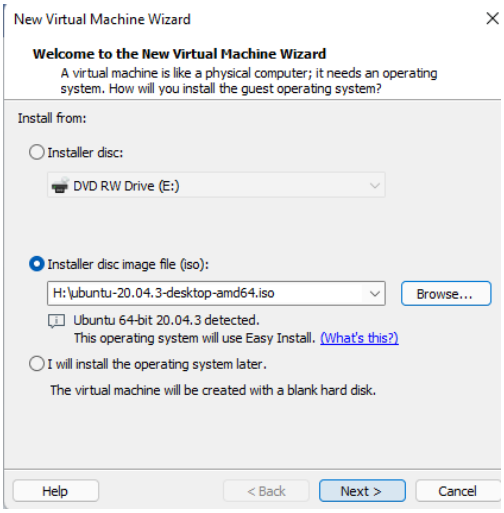
-Open VMWare and click “Create New Virtual Machine”



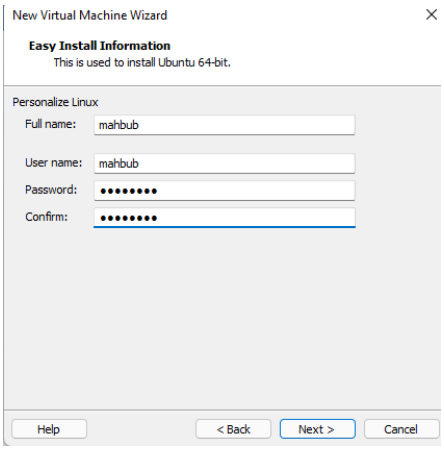
-Select the option shown above and click “Browse”



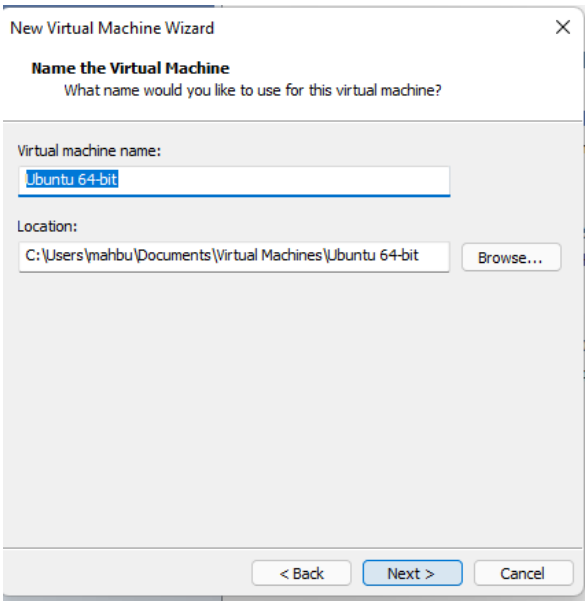
-Locate the installer file and click “Open”



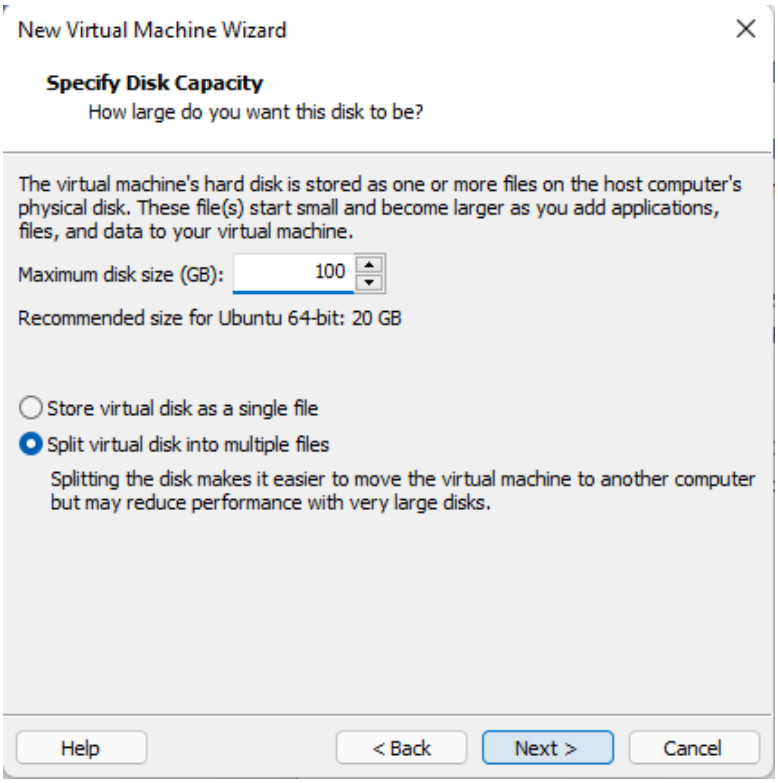
-Click Next



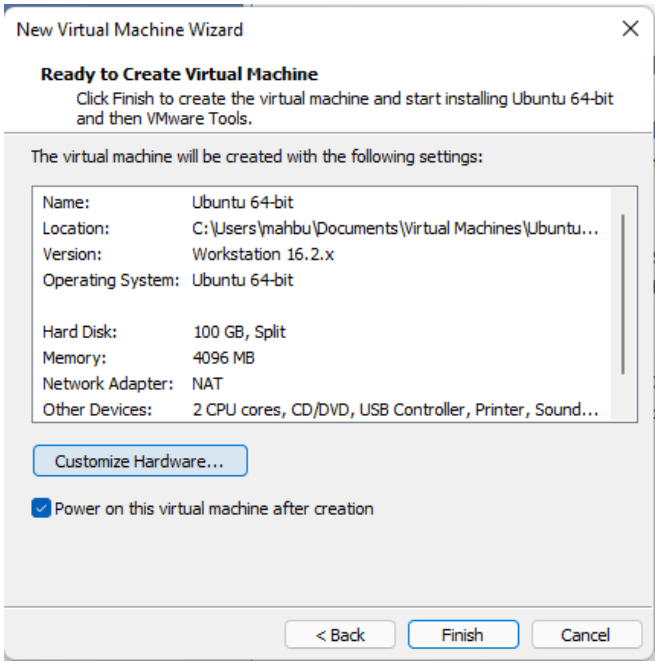
-Create user account with password



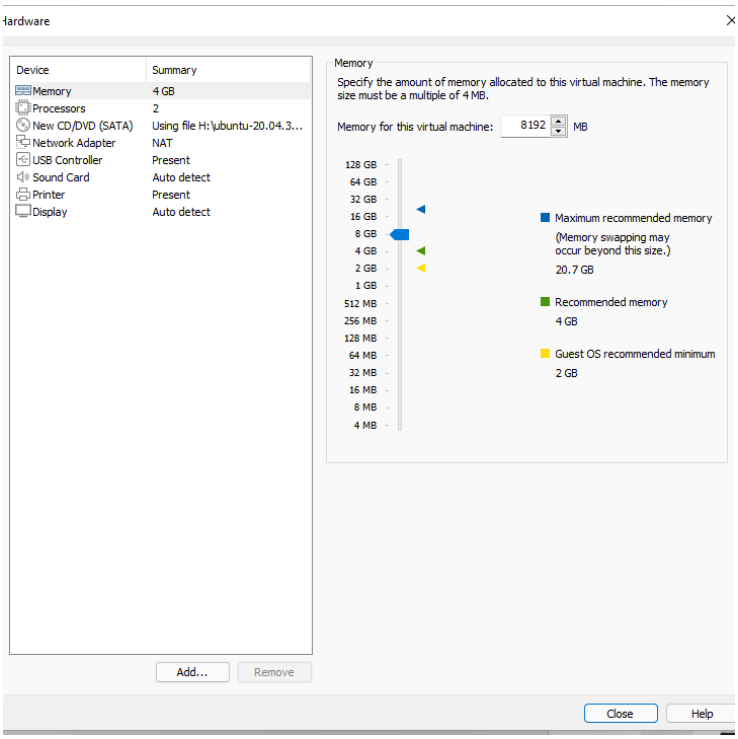
Click Next



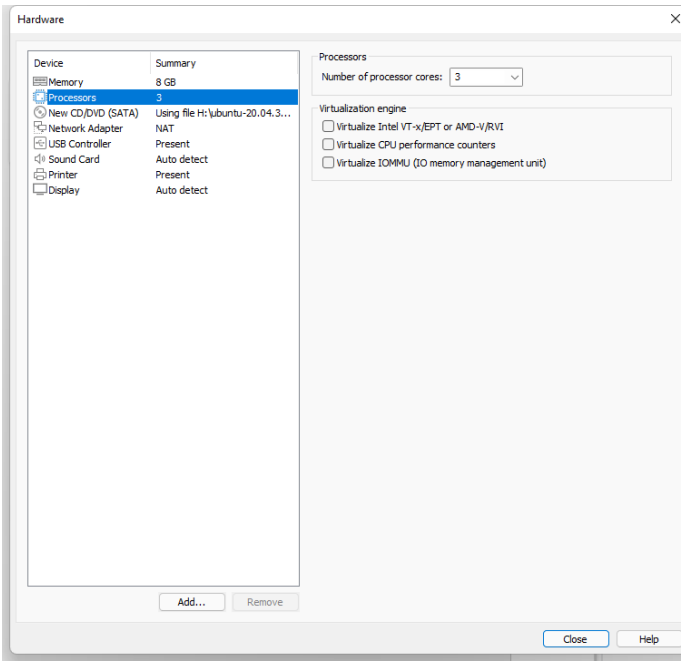
Now, Select the size of the disk and click Next

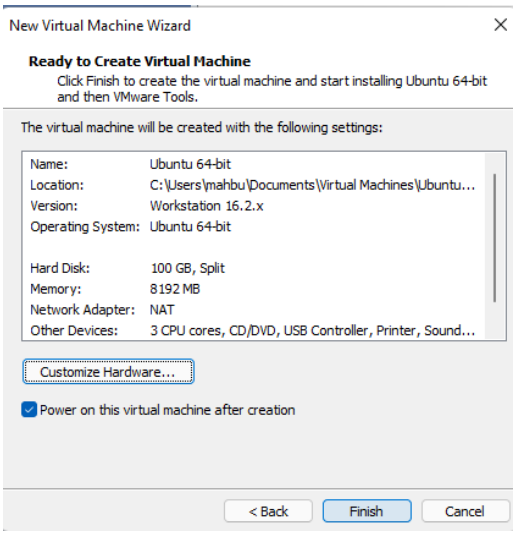


Before you click “Finish”, it is recommended that you customize the Hardware for VM.

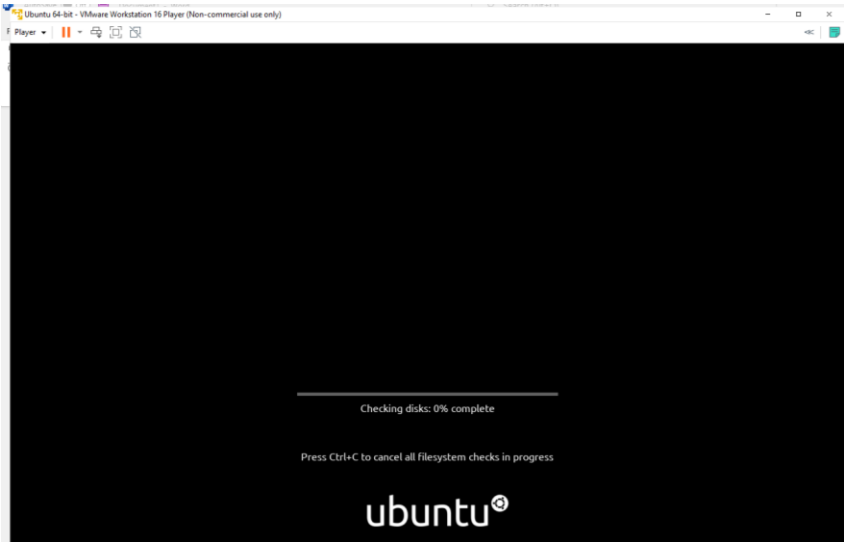


Select the memory and CPU cores for your VM

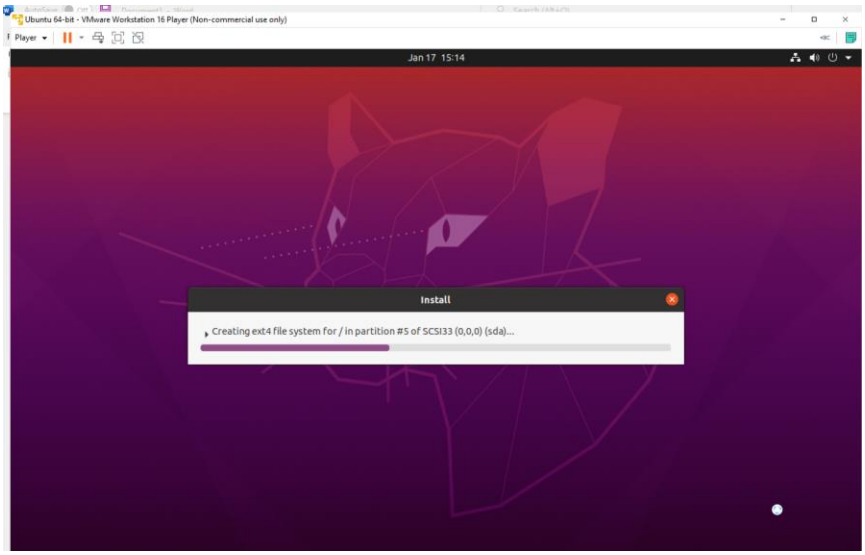




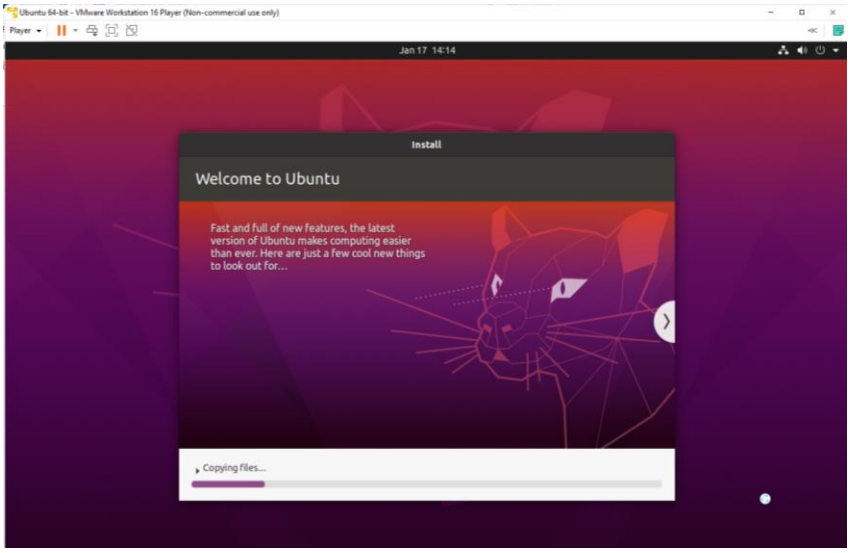
Click Finish

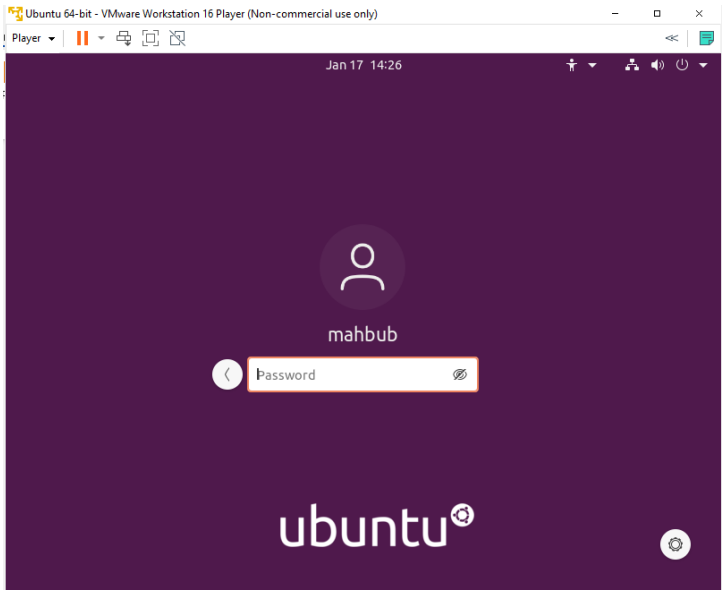


The Installation will start



Installation will take some time.





Enter the Username and Password to start

Before you start installing SIFT and REMnux, it is better if you update and upgrade the VM using the following commands:

sudo apt update

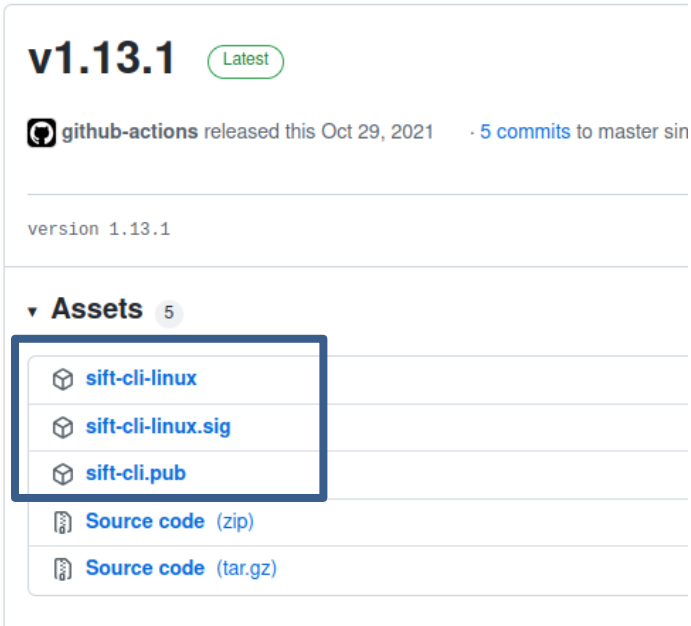
sudo apt upgrade

This will take a while…

Now lets start installing SIFT.

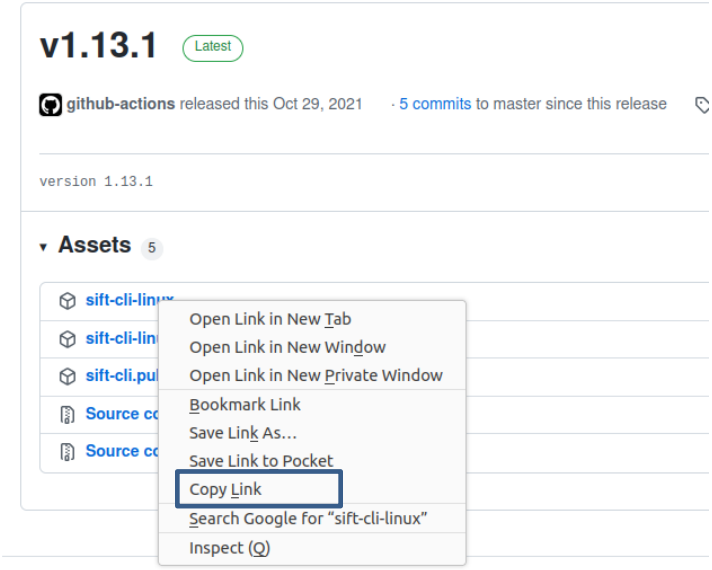
To install SIFT, visit the link below and download the latest distributions.

https://github.com/teamdfir/sift-cli/releases/tag/v1.13.1

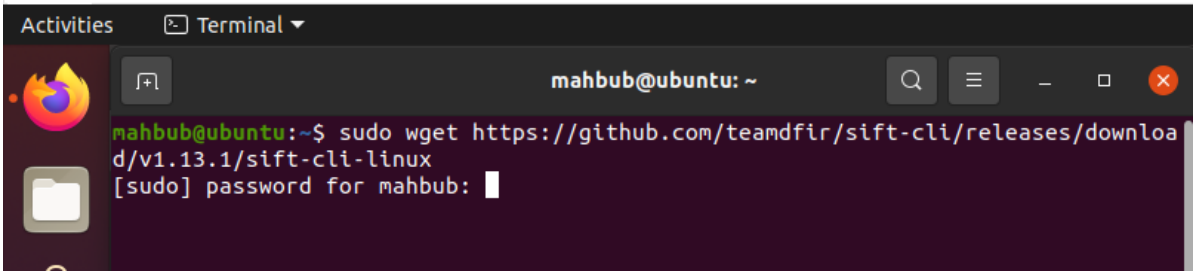


You will require to download the above highlighted files in your VM.

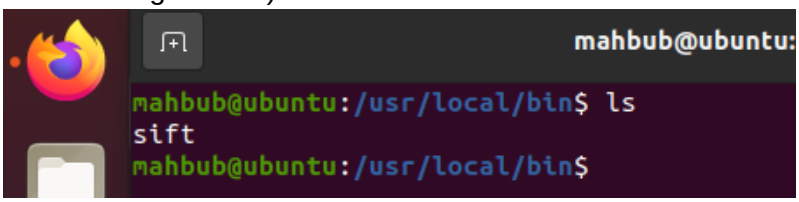
At first right click on sift-cli-linux and copy the link (see image below)



Now open the command prompt in your VM and type the following command
sudo wget ***past the link you copied***

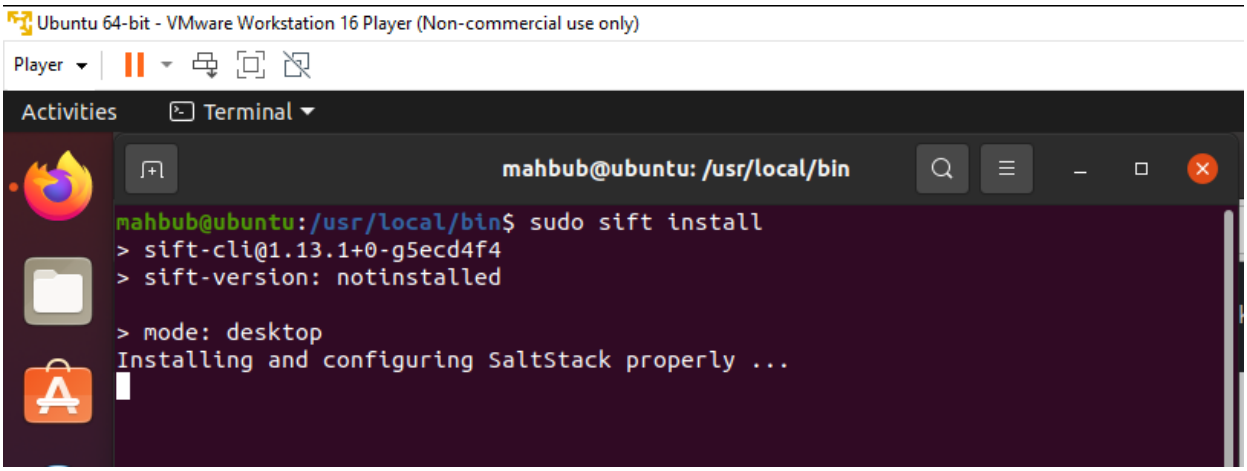


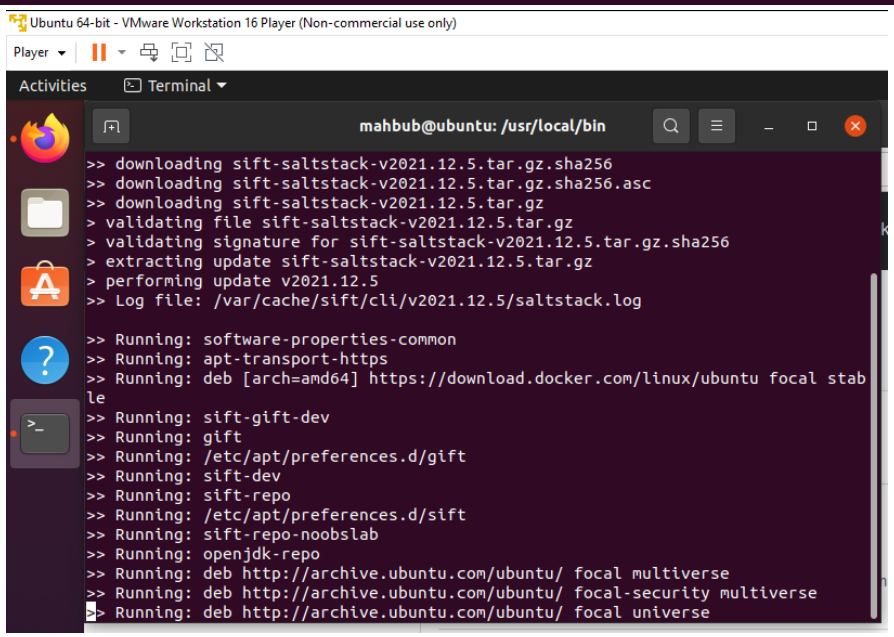
Enter your password and it will start installing.
Repeat these steps for sift-cli-linux.sig and sift-cli.pub
Next, install golang-go using the following command
sudo apt install golang-go
Then use the following command to move sift to bin folder.
sudo mv sift-cli-linux /usr/local/bin/sift
Verify the move (see the image below)



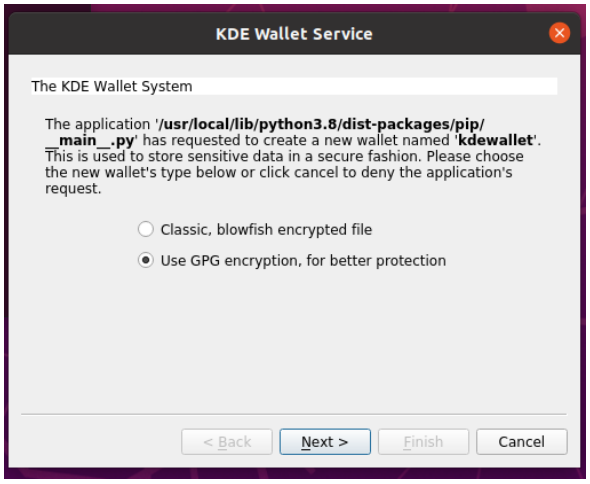
Use the following command to import the key
gpg --keyserver pgp.mit.edu --recv-keys 22598A94
Use the following command before you Run Sift
sudo chmod 755 /usr/local/bin/sift
Use the following command to Run:

sudo sift install

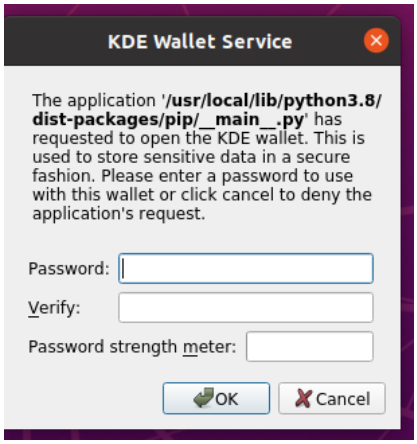




During the installation, you will be asked to select the following.

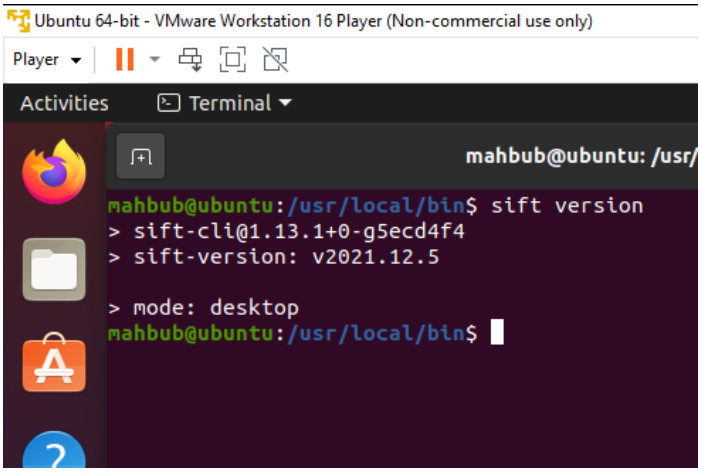


Select ***Classic, blowfish encrypted file*** option and click Finish. It will ask you to confirm the password. Select password and click ok.



Now are you done with SIFT installation. To verify your installation, type the following command and verify it.

sift version



Installing REMnux Package

Download the latest REMnux package using the following command

sudo get https://REMnux.org/remnux-cli

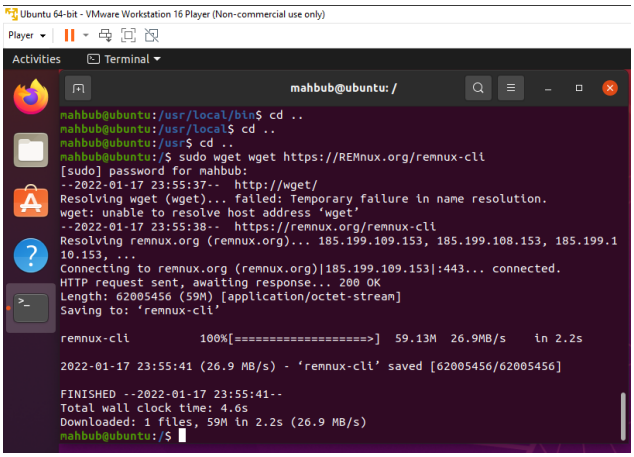
Then move to a folder called remnux using the following command

sudo mv remnux-cli remnux

sudo chmod +x remnux

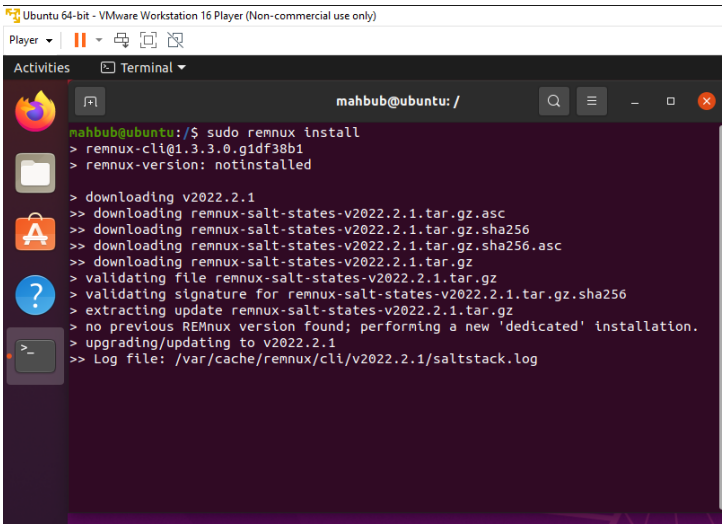
Then move to bin folder using the following command

sudo mv remnux /usr/local/bin



To install use the following command:

sudo remnux install



Once the installation is completed, Reboot your VM.

Virtual Box

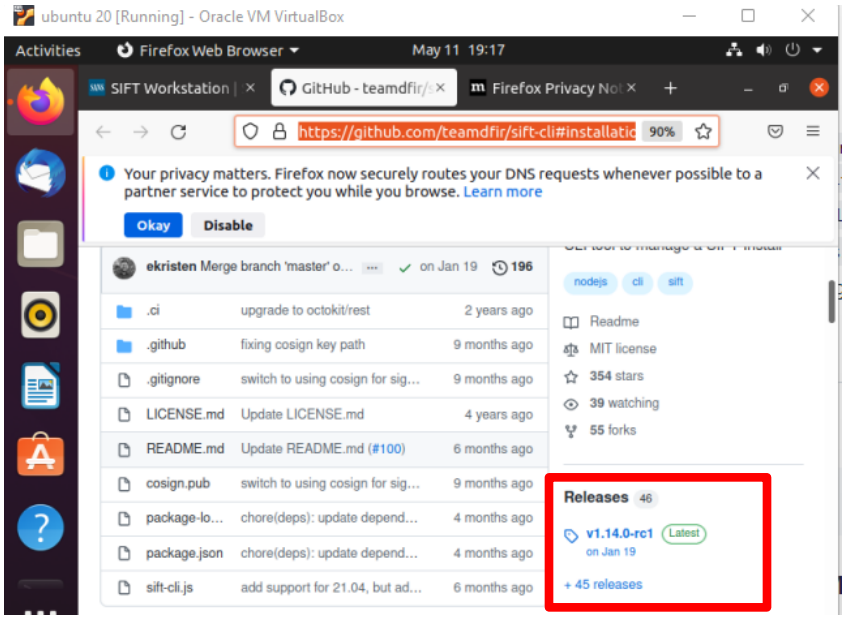
Step 1: Update and Upgrade Ubuntu.

sudo apt-get update

sudo apt-get upgrade

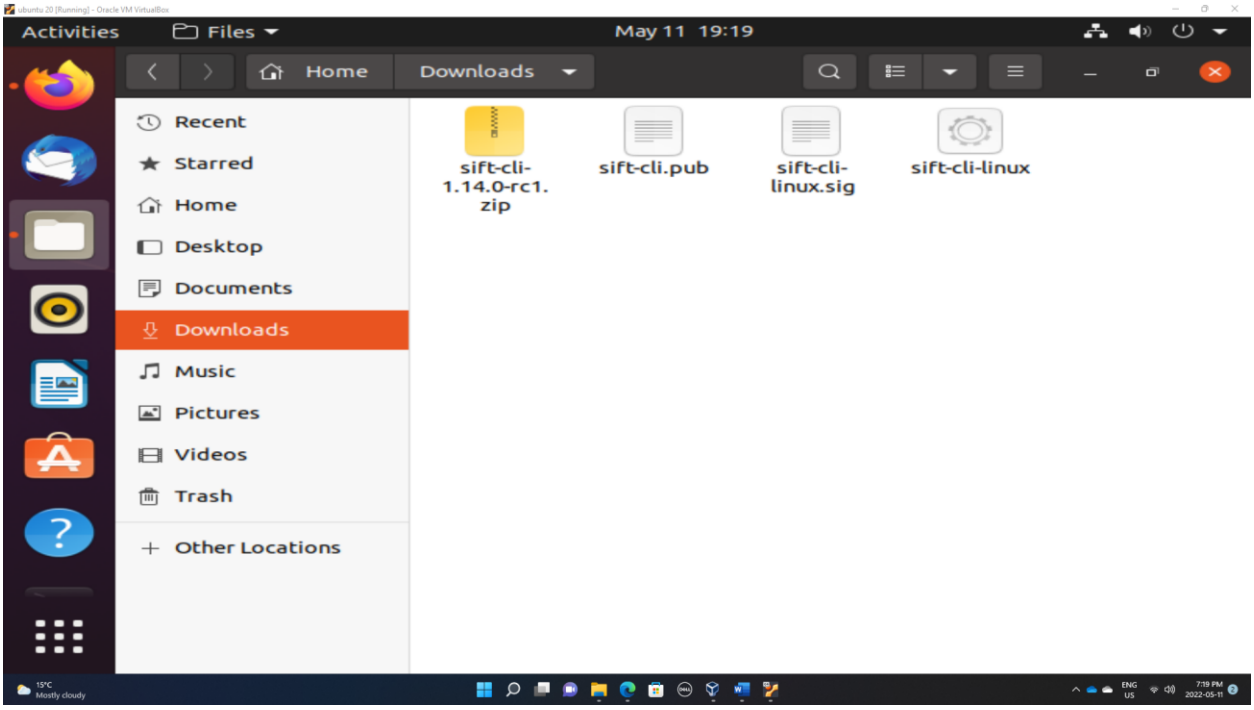
Step 2: Download SIFT from the link below.

Link: https://github.com/teamdfir/sift-cli#installation

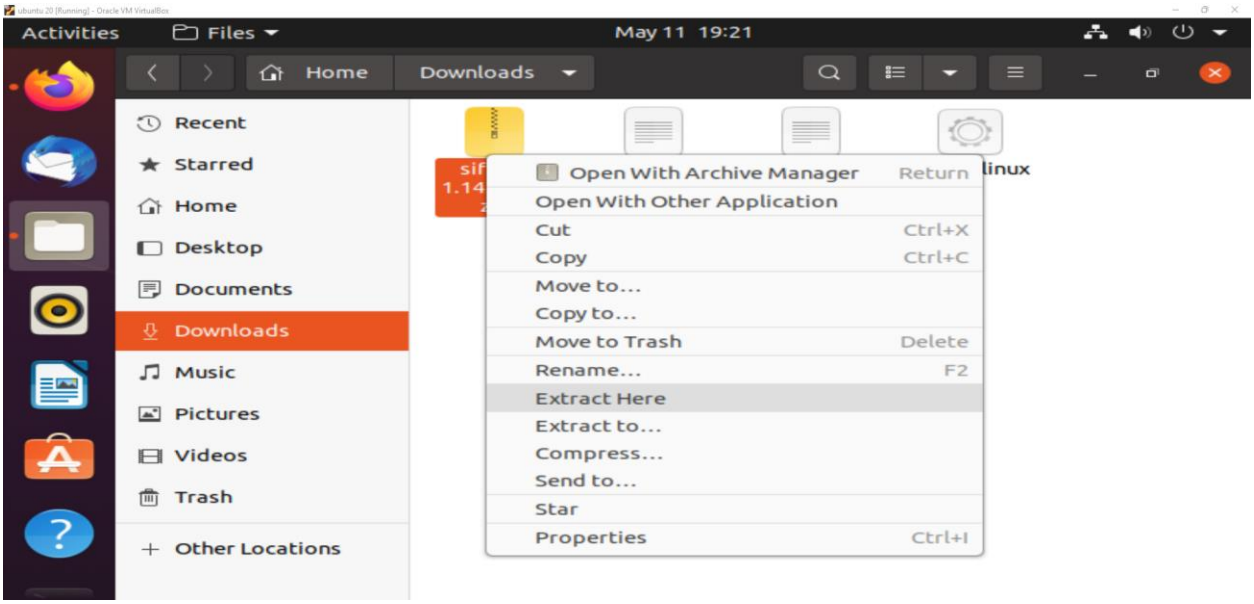


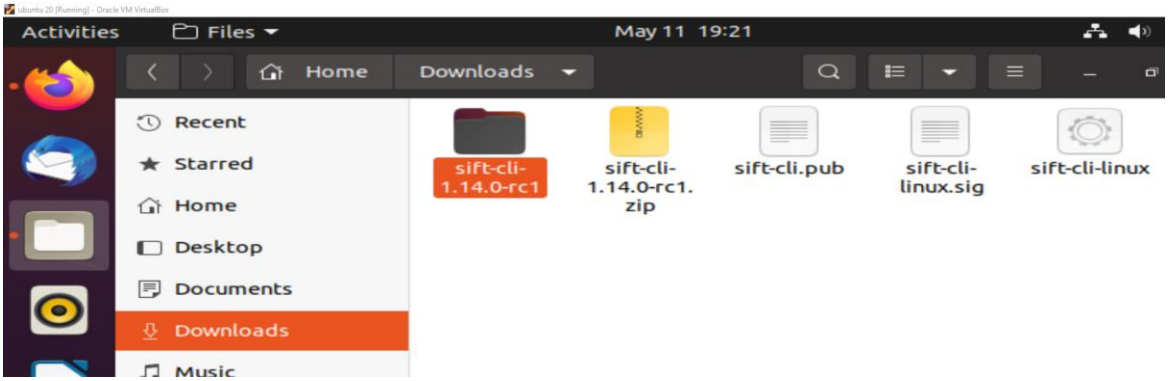
Click on Latest.

Now, download the highlighted files in your Downloads folder.



Step 3: Unzip the sift-cli-1.14.0-rc1.zip in Downloads folder.



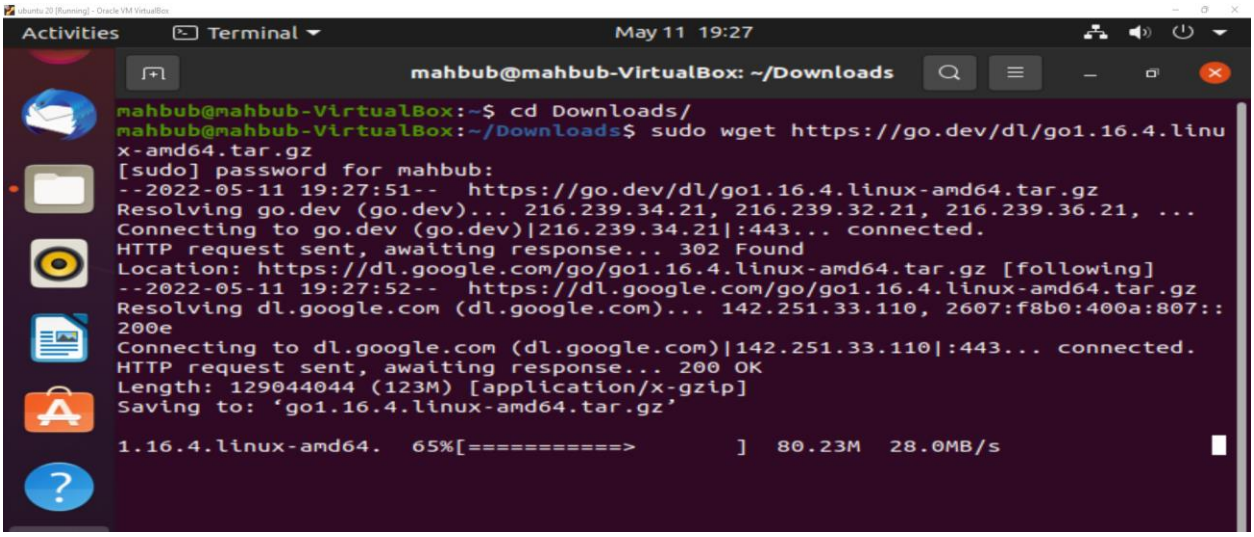


Step 4: Installation of GO language.

To Install GO language, First, you need to download it. Use the following command. This will download the GO language.

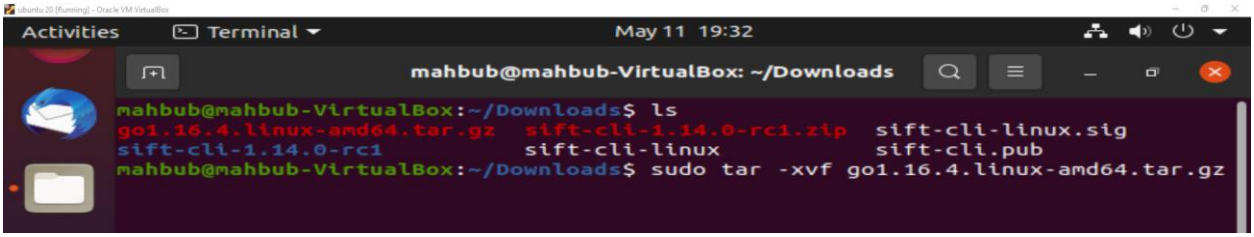
sudo wget https://go.dev/dl/go1.16.4.linux-amd64.tar.gz

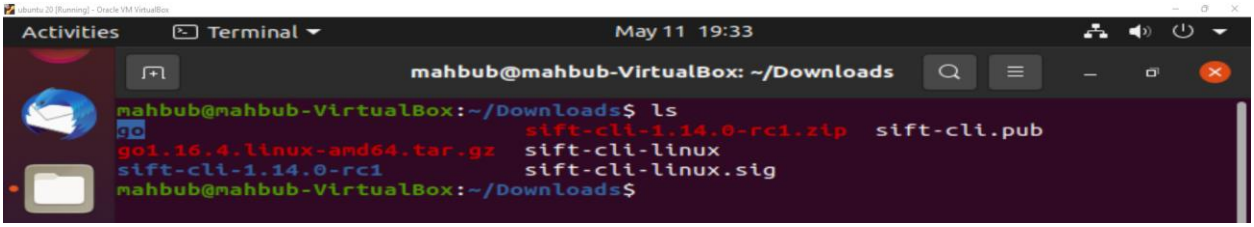
You will need version 1.16.4. **DO NOT** download and install any other version. It will not work!



Next, unzip the GO by using the following command:

sudo tar -xvf go1.16.4.linux-amd64.tar.gz



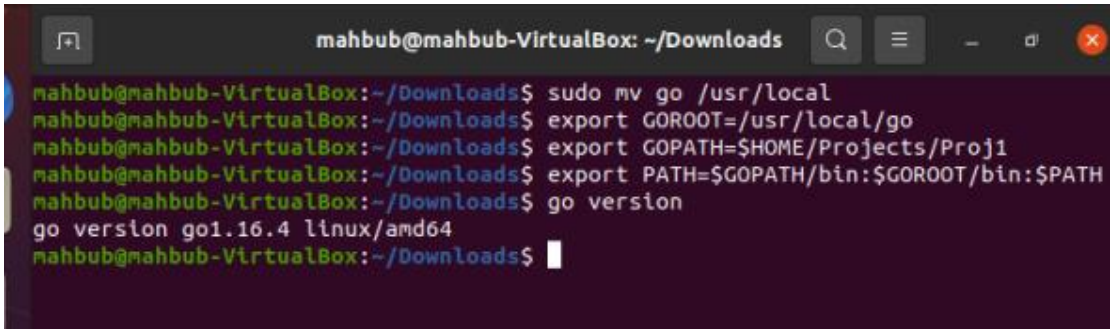


Now, move the go to /usr/local folder. Then set the following environment for GO.

export GOROOT=/usr/local/go

export GOPATH=$HOME/Projects/Proj1

export PATH=$GOPATH/bin:$GOROOT/bin:$PATH

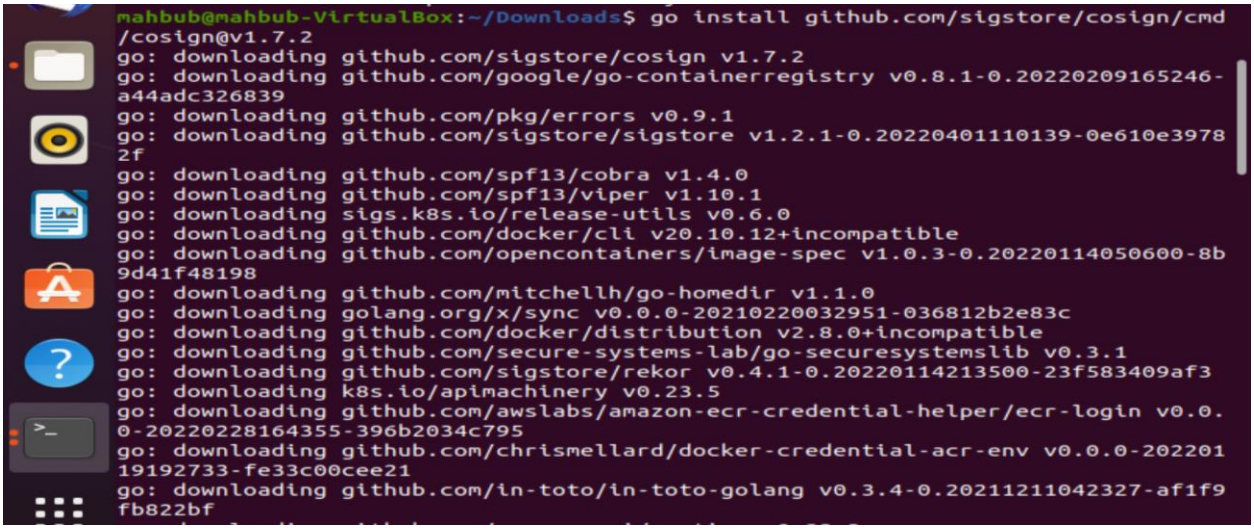


Step 5: Installing cosign

To Install cosign, use the following command.

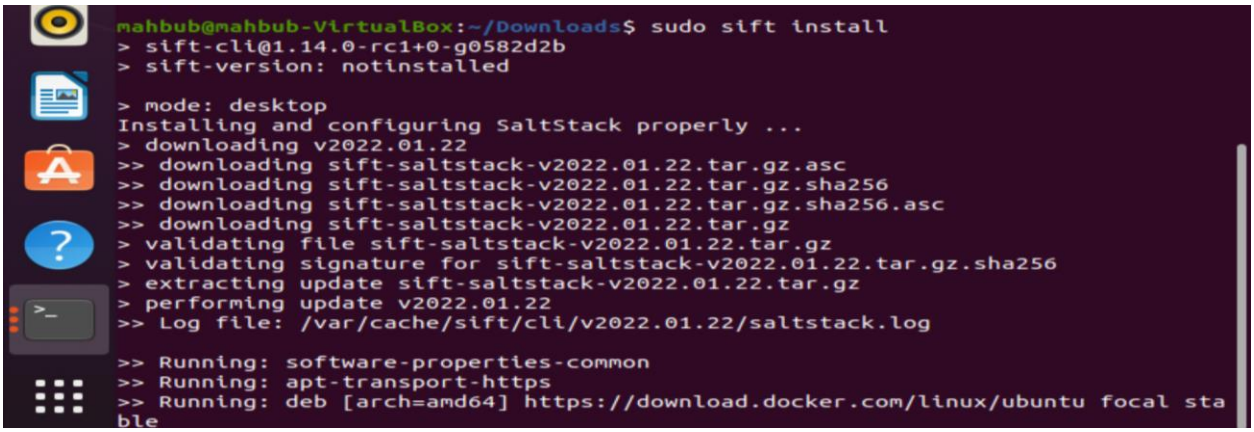
go install github.com/sigstore/cosign/cmd/cosign@v1.7.2

Here version 1.7.2 is used. If you want to install the latest version then type “@latest”.

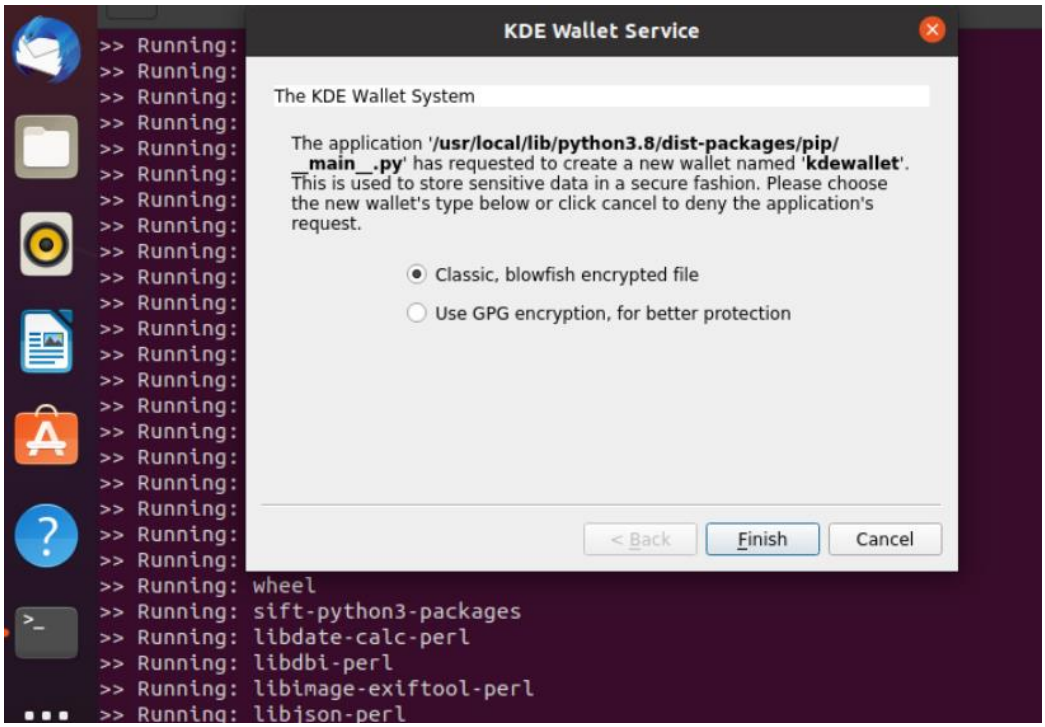


When the installation is done, move sift-cli-linux from Downloads to /usr/local/bin/sift then use ***sudo chmod 775 /usr/local/bin/sift***.

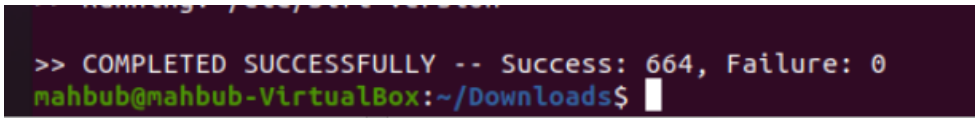
Then type: ***sudo sift install***



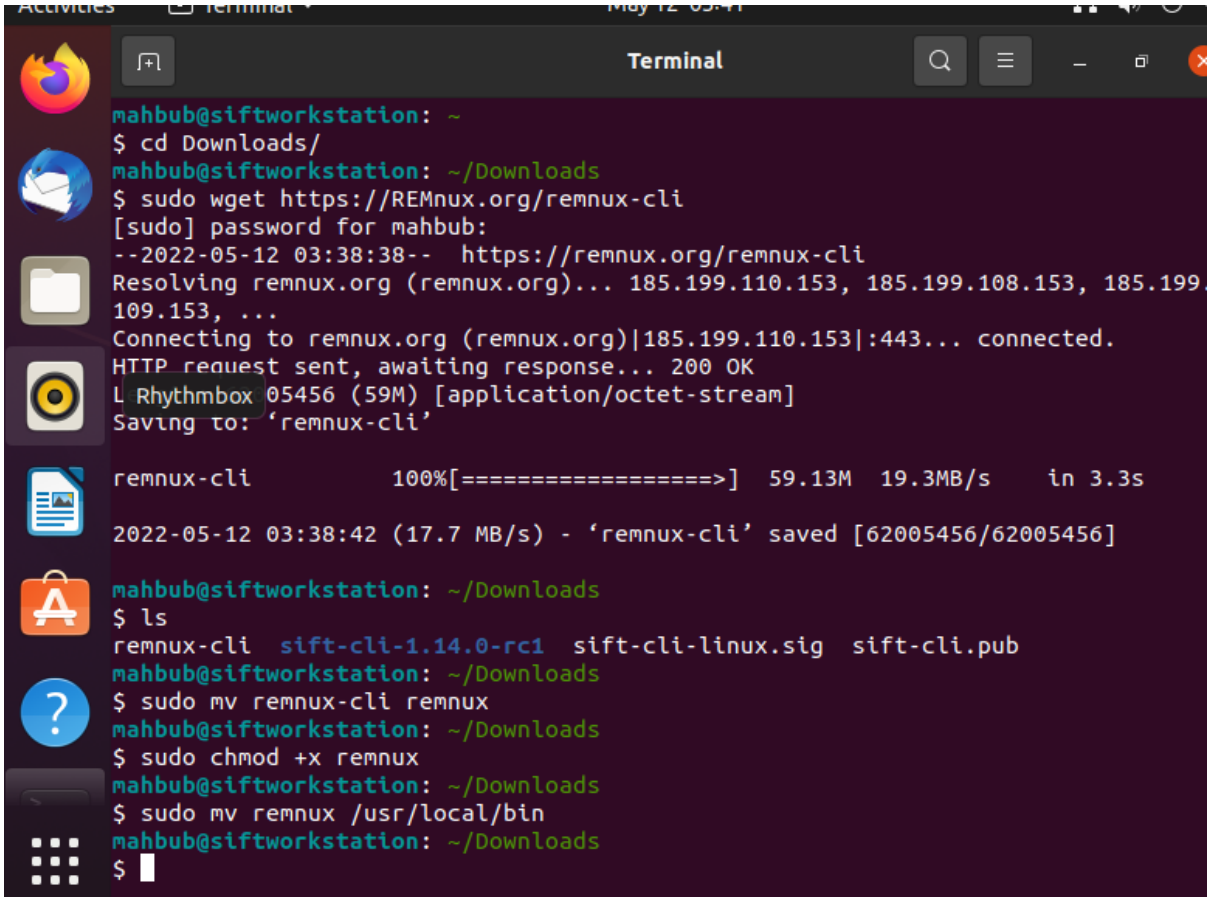
This installation will require 40-60 minutes.



Select Classic, blowfish mode then click finish. You will also need to set the password.



Installing REMnux on VirtualBox



Finally type: sudo install remnux.

References

Ubuntu. (2020). Ubuntu 20.04.4 LTS [Operating system]. Retrieved from http://releases.ubuntu.com/20.04/

VMware, Inc. (2017). VMware Workstation Player [Desktop virtualization tool]. Retrieved from https://my.vmware.com/en/web/vmware/free#desktop_end_user_computing/vmware_workstation_player/14_0

For more information, contact:
Director, Centre for Instructional Technology and Development
Southern Alberta Institute of Technology
1301 16 Ave. N.W., Calgary, AB T2M 0L4