



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.

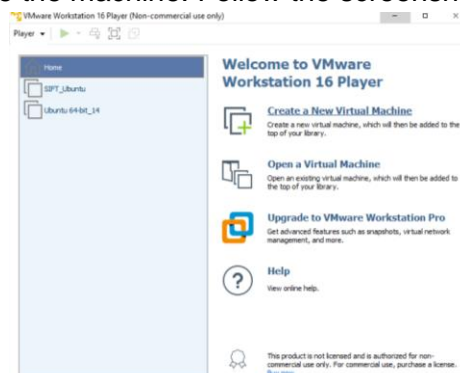
In this lab, you will create a VMware image using Ubuntu Desktop 20.04 as the operating system, and then add the SIFT (forensic tools) and REMnux (malware analysis tools) packages. In this Lab, we will install SIFT on Ubuntu. We will use VMWare and VirtualBox. You can choose one only.

VMWare

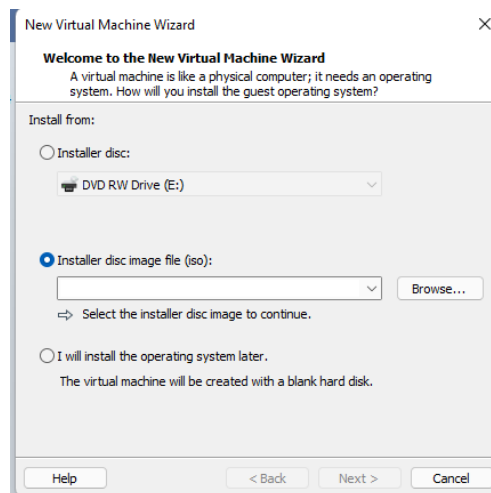
For Reading: <https://www.sans.org/tools/sift-workstation/>

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

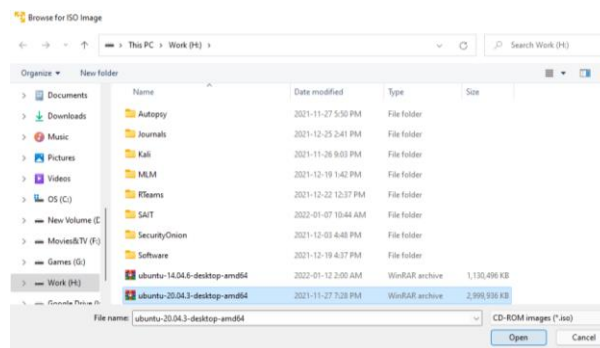
Step 1: Using VMWare, create the machine. Follow the screenshots below



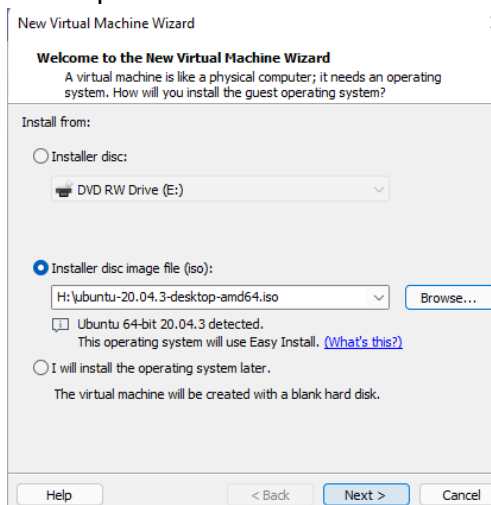
-Open VMWare and click “Create New Virtual Machine”



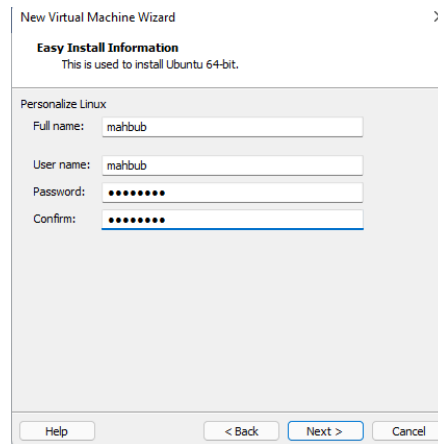
-Select the option shown above and click “Browse”



-Locate the installer file and click “Open”



-Click Next



New Virtual Machine Wizard

Easy Install Information
This is used to install Ubuntu 64-bit.

Personalize Linux

Full name: mahbub

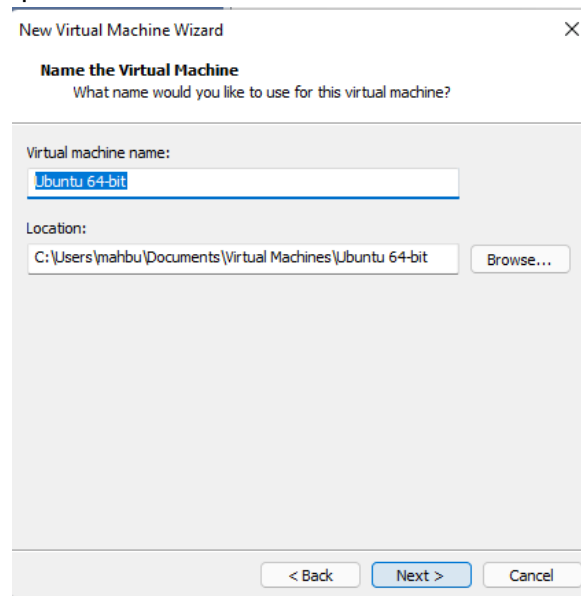
User name: mahbub

Password:

Confirm:

Help < Back Next > Cancel

-Create user account with password



New Virtual Machine Wizard

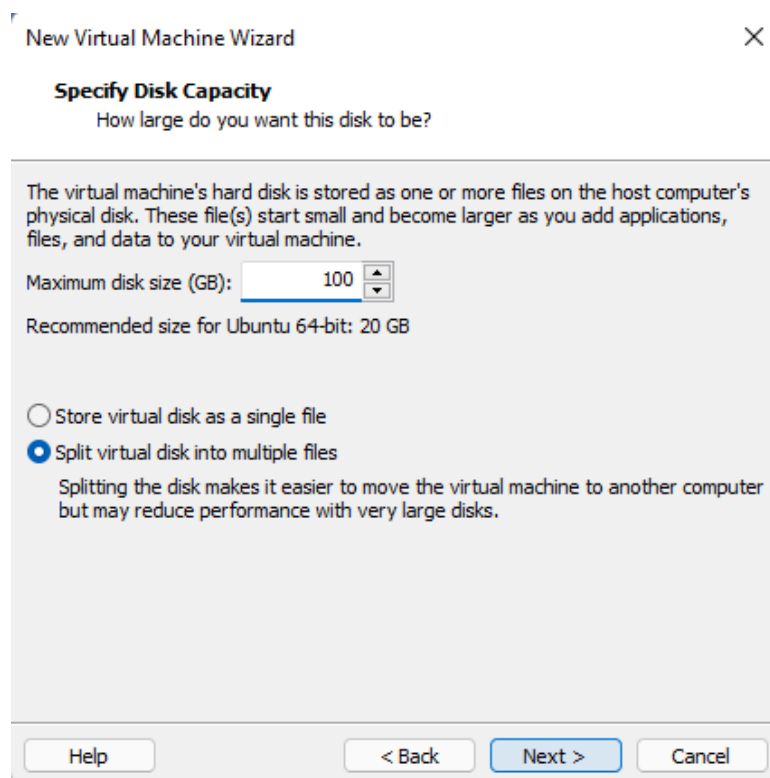
Name the Virtual Machine
What name would you like to use for this virtual machine?

Virtual machine name:
Ubuntu 64-bit

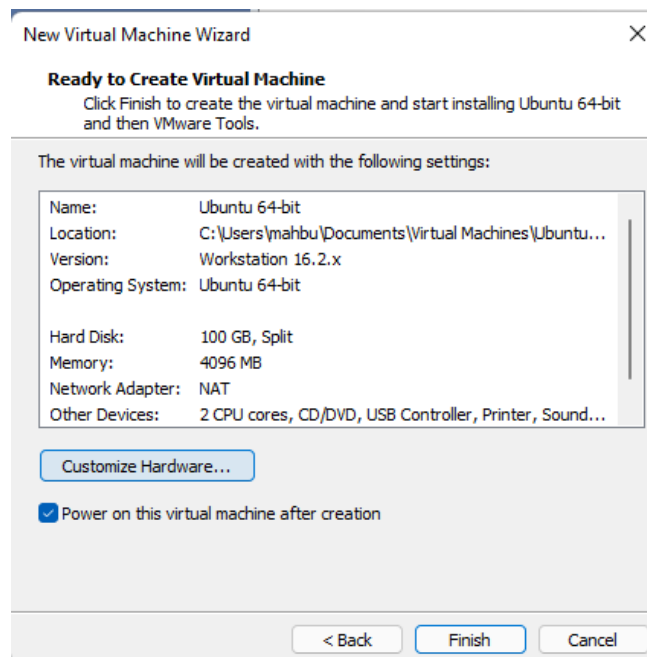
Location:
C:\Users\mahbu\Documents\Virtual Machines\Ubuntu 64-bit Browse...

< Back Next > Cancel

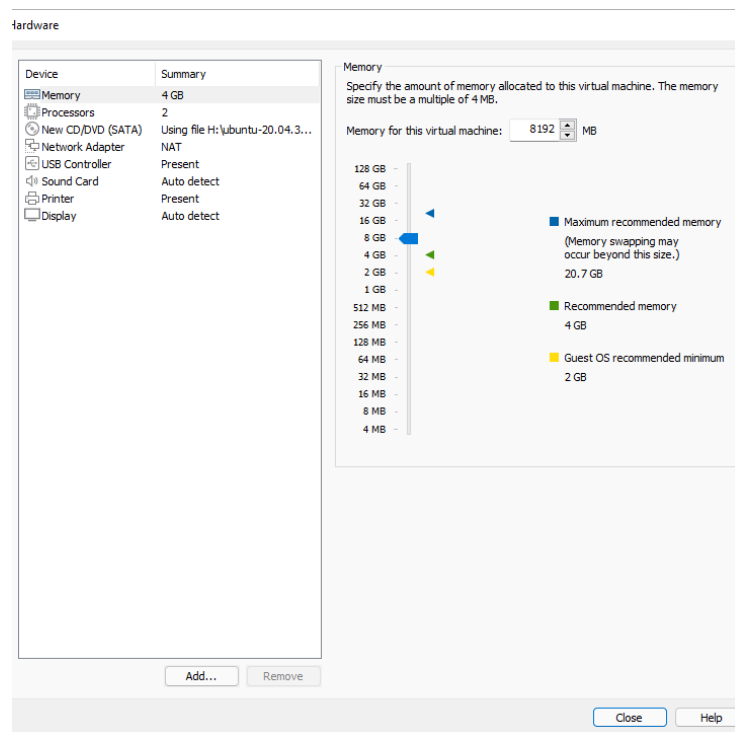
Click Next



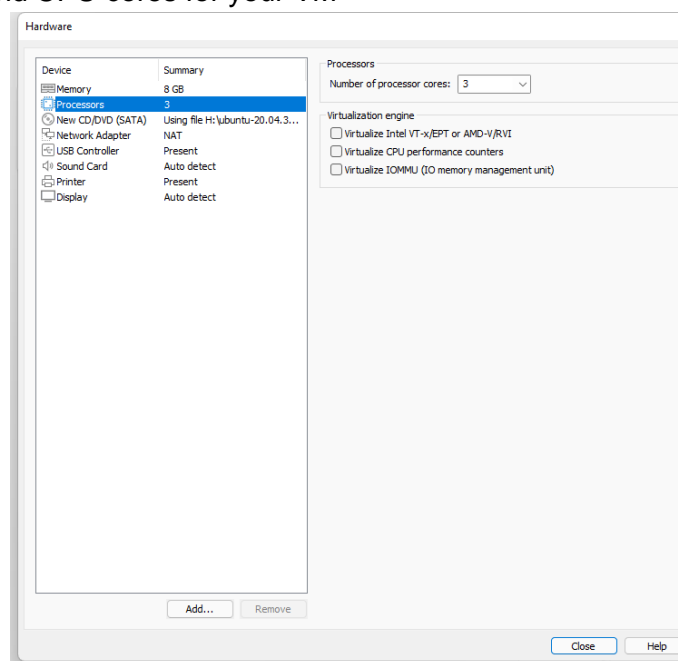
Now, Select the size of the disk and click Next

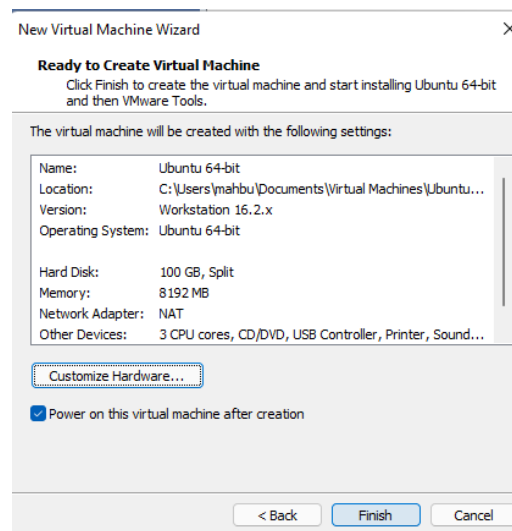


Before you click “Finish”, it is recommended that you customize the Hardware for VM.

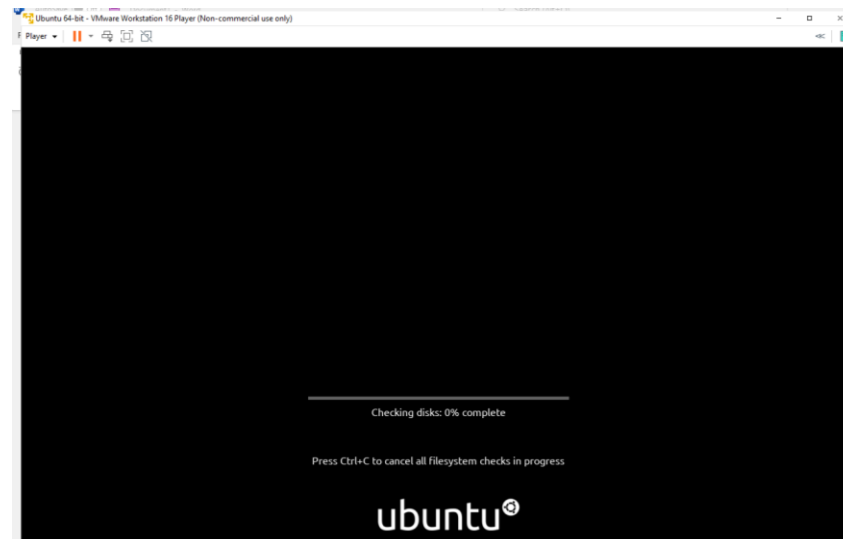


Select the memory and CPU cores for your VM

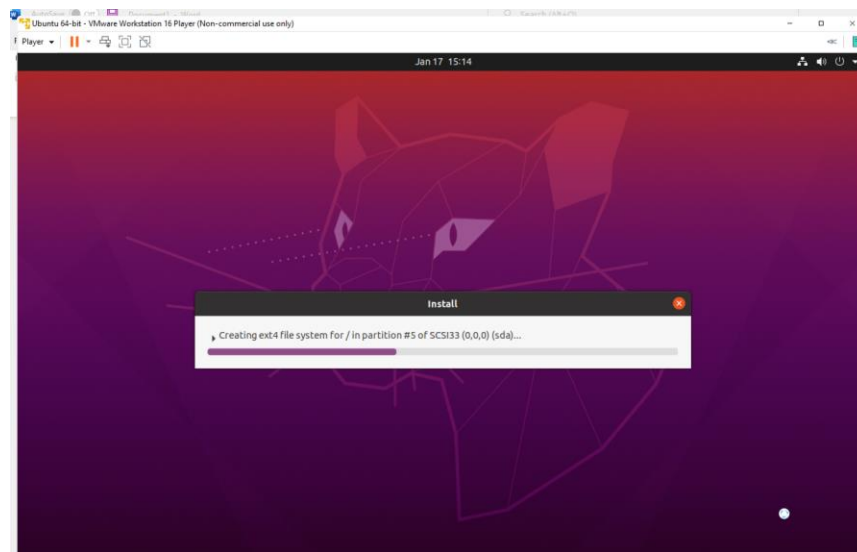




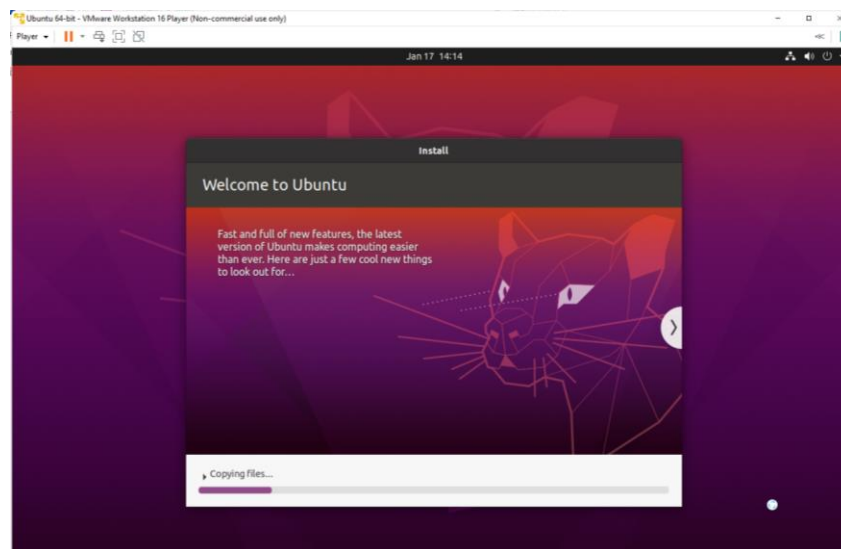
Click Finish

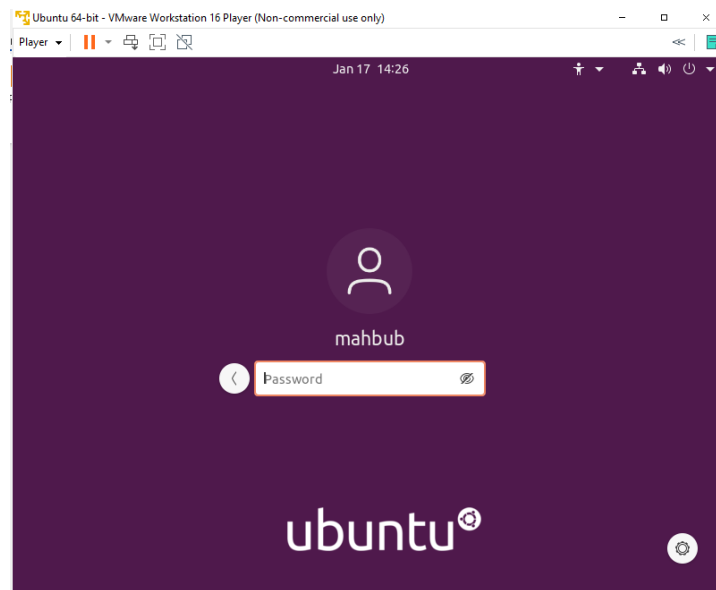


The Installation will start



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

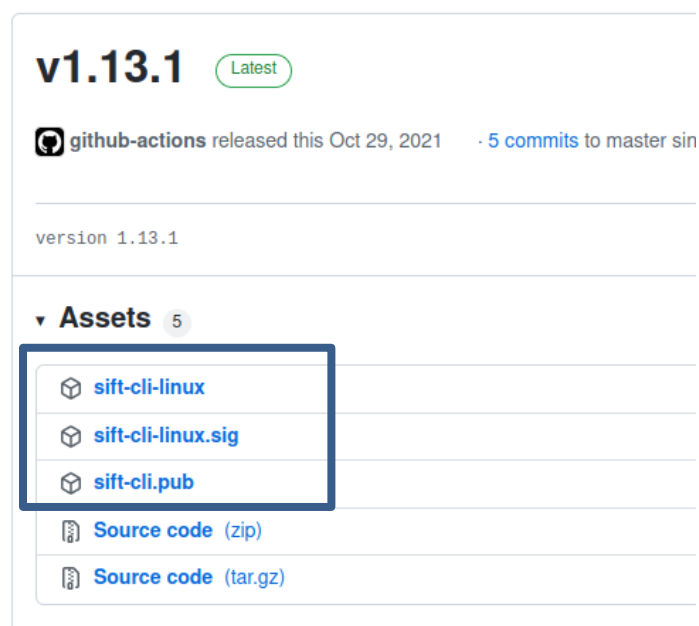
sudo apt upgrade

This will take a while...

Now lets start installing SIFT.

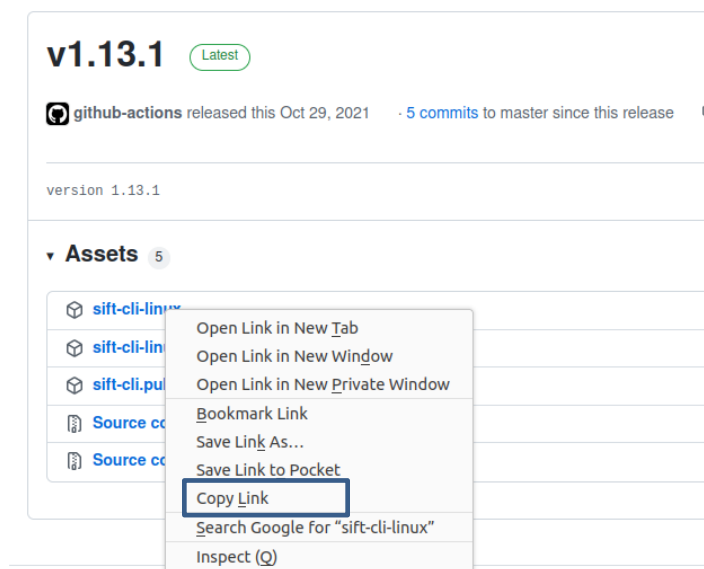
To install SIFT, visit the link below and download the latest distributions.

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

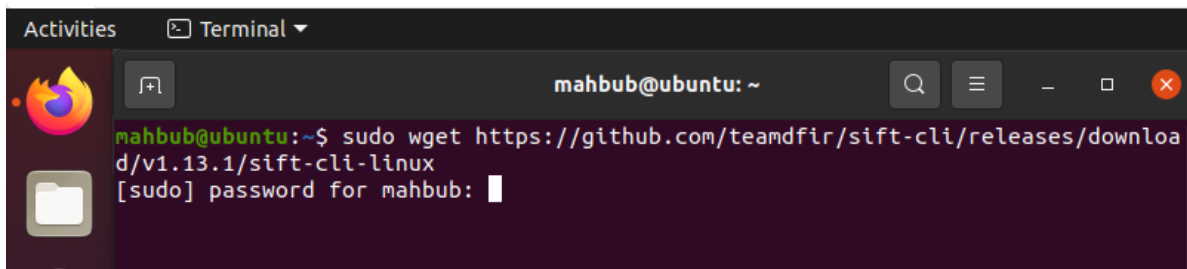


You will require to download the above highlighted files in your VM.

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

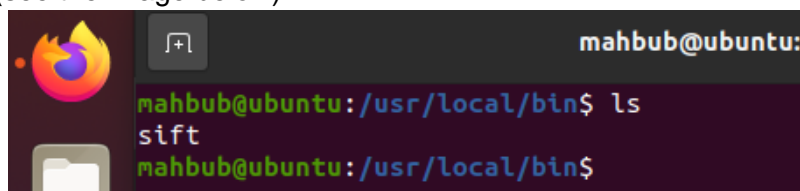
Next, install golang-go using the following command

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

```

Ubuntu 64-bit - VMware Workstation 16 Player (Non-commercial use only)
Player ▾ | || ▾ | ⏏ | ⏏ | ⏏
Activities ▾ | Terminal ▾
mahbub@ubuntu: /usr/local/bin
mahbub@ubuntu:/usr/local/bin$ sudo sift install
> sift-cli@1.13.1+0-g5ecd4f4
> sift-version: notinstalled

> mode: desktop
Installing and configuring SaltStack properly ...

```

```

Ubuntu 64-bit - VMware Workstation 16 Player (Non-commercial use only)
Player ▾ | || ▾ | ⏏ | ⏏ | ⏏
Activities ▾ | Terminal ▾
mahbub@ubuntu: /usr/local/bin
>> downloading sift-saltstack-v2021.12.5.tar.gz.sha256
>> downloading sift-saltstack-v2021.12.5.tar.gz.sha256.asc
>> downloading sift-saltstack-v2021.12.5.tar.gz
>> validating file sift-saltstack-v2021.12.5.tar.gz
>> validating signature for sift-saltstack-v2021.12.5.tar.gz.sha256
>> extracting update sift-saltstack-v2021.12.5.tar.gz
>> performing update v2021.12.5
>> Log file: /var/cache/sift/cli/v2021.12.5/saltstack.log

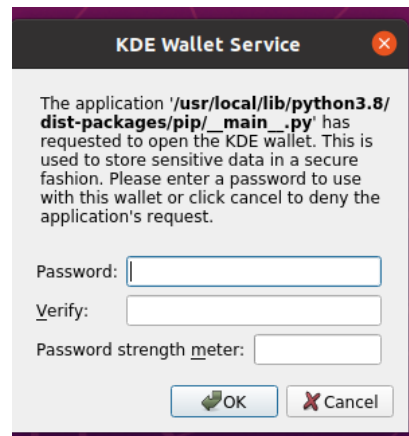
>> Running: software-properties-common
>> Running: apt-transport-https
>> Running: deb [arch=amd64] https://download.docker.com/linux/ubuntu focal stable
>> Running: sift-gift-dev
>> Running: gift
>> Running: /etc/apt/preferences.d/gift
>> Running: sift-dev
>> Running: sift-repo
>> Running: /etc/apt/preferences.d/sift
>> Running: sift-repo-noobs
>> Running: openjdk-repo
>> Running: deb http://archive.ubuntu.com/ubuntu/ focal multiverse
>> Running: deb http://archive.ubuntu.com/ubuntu/ focal-security multiverse
>> Running: deb http://archive.ubuntu.com/ubuntu/ focal universe

```

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

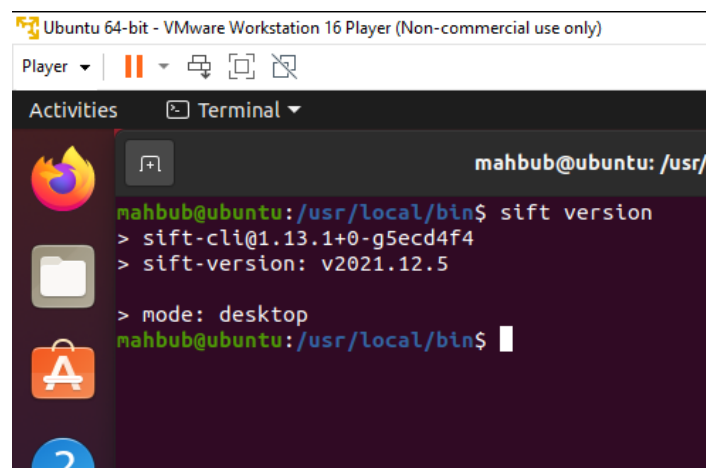


Select **Classic, blowfish encrypted file** option and click Finish. It will ask you to confirm the password. Select password and click ok.



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

```

mahbub@ubuntu: /usr/local/bin$ cd ..
mahbub@ubuntu: /usr/local$ cd ..
mahbub@ubuntu: /usr$ cd ..
mahbub@ubuntu: /$ sudo wget https://remnux.org/remnux-cli
[sudo] password for mahbub:
--2022-01-17 23:55:37-- http://wget/
Resolving wget (wget)... failed: Temporary failure in name resolution.
wget: unable to resolve host address 'wget'
--2022-01-17 23:55:38-- https://remnux.org/remnux-cli
Resolving remnux.org (remnux.org)... 185.199.109.153, 185.199.108.153, 185.199.107.153, ...
Connecting to remnux.org (remnux.org)|185.199.109.153|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 62005456 (59M) [application/octet-stream]
Saving to: 'remnux-cli'

remnux-cli      100%[=====] 59.13M  26.9MB/s  in 2.2s

2022-01-17 23:55:41 (26.9 MB/s) - 'remnux-cli' saved [62005456/62005456]

FINISHED --2022-01-17 23:55:41--
Total wall clock time: 4.6s
Downloaded: 1 files, 59M in 2.2s (26.9 MB/s)
mahbub@ubuntu: /$

```

To install use the following command:
sudo remnux install

```

mahbub@ubuntu: /$ sudo remnux install
> remnux-cli@1.3.3.0.g1df38b1
> remnux-version: notinstalled

> downloading v2022.2.1
>> downloading remnux-salt-states-v2022.2.1.tar.gz.asc
>> downloading remnux-salt-states-v2022.2.1.tar.gz.sha256
>> downloading remnux-salt-states-v2022.2.1.tar.gz.sha256.asc
>> downloading remnux-salt-states-v2022.2.1.tar.gz
> validating file remnux-salt-states-v2022.2.1.tar.gz
> validating signature for remnux-salt-states-v2022.2.1.tar.gz.sha256
> extracting update remnux-salt-states-v2022.2.1.tar.gz
> no previous REMnux version found; performing a new 'dedicated' installation.
> upgrading/updating to v2022.2.1
>> Log file: /var/cache/remnux/cli/v2022.2.1/saltstack.log

```

Once the installation is completed, Reboot your VM.

Virtual Box

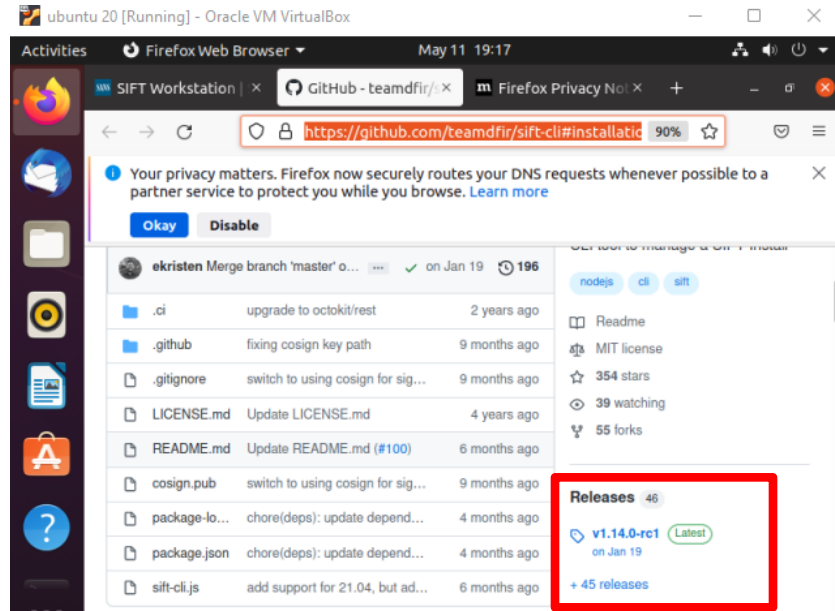
Step 1: Update and Upgrade Ubuntu.

sudo apt-get update

sudo apt-get upgrade

Step 2: Download SIFT from the link below.

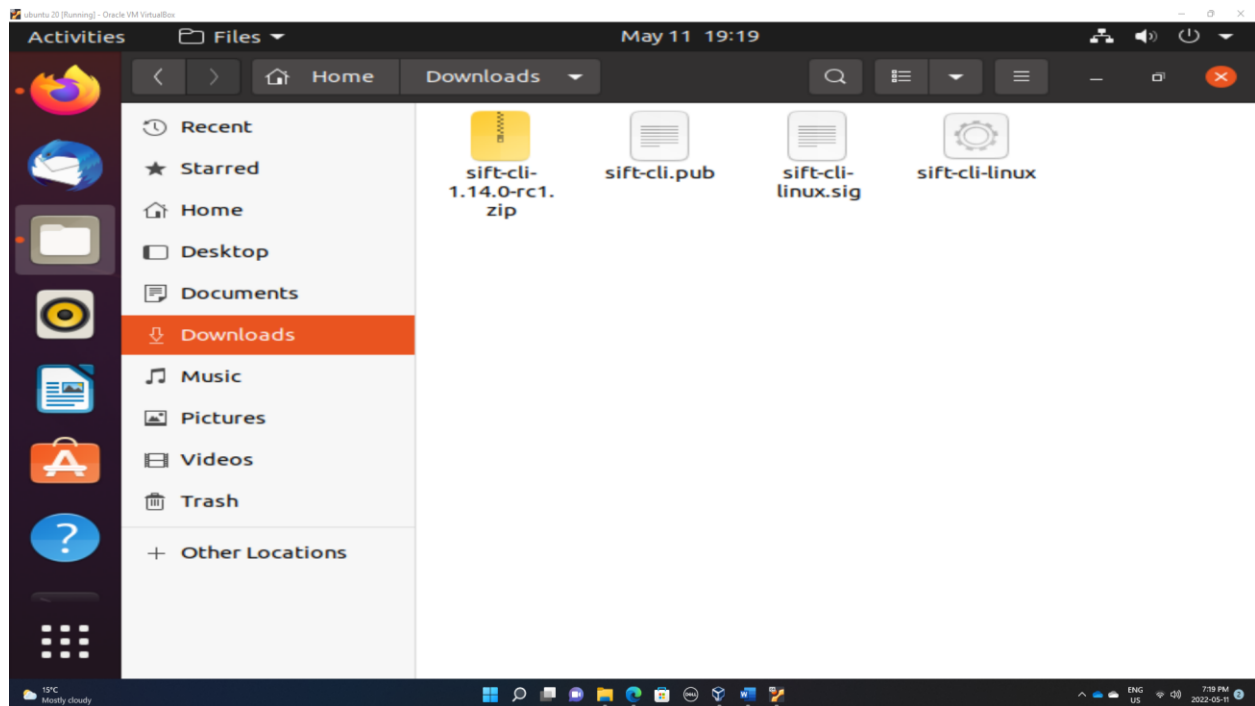
Link: <https://github.com/teamdfir/sift-cli#installation>



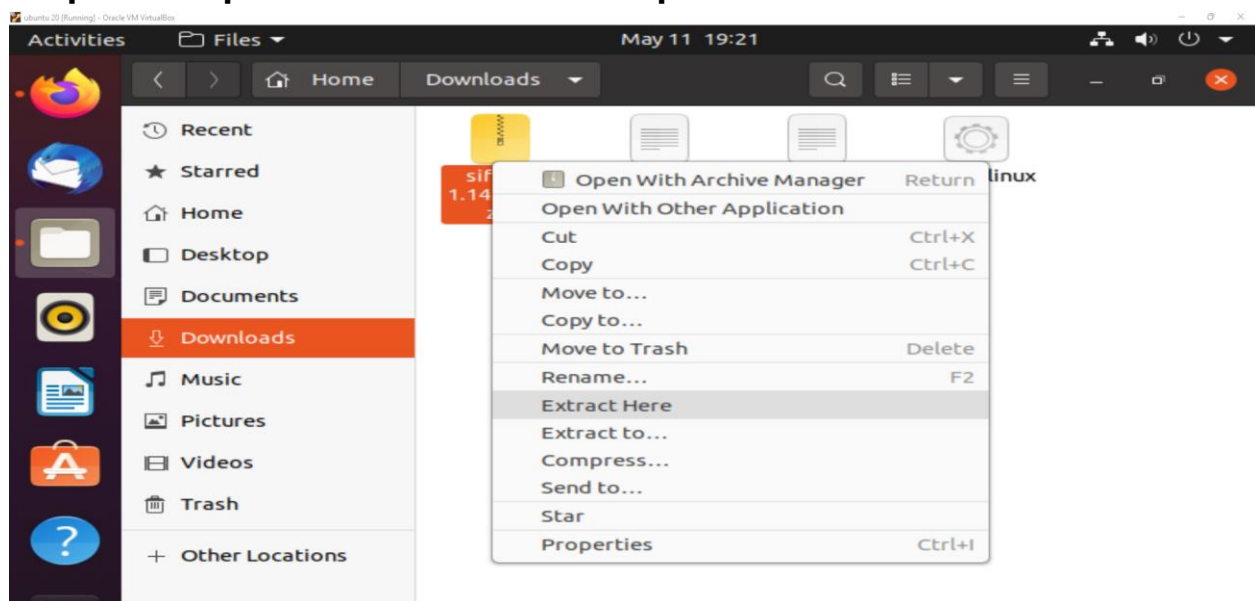
Click on Latest.

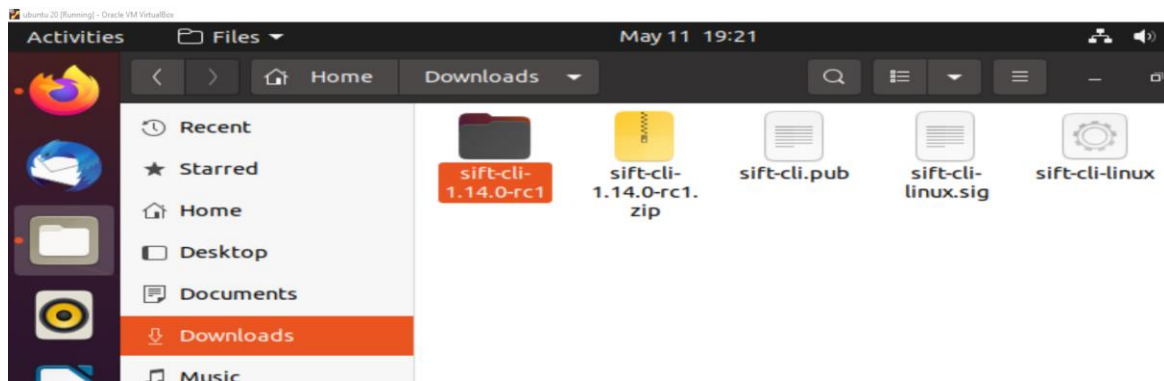


Now, download the highlighted files in your Downloads folder.



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



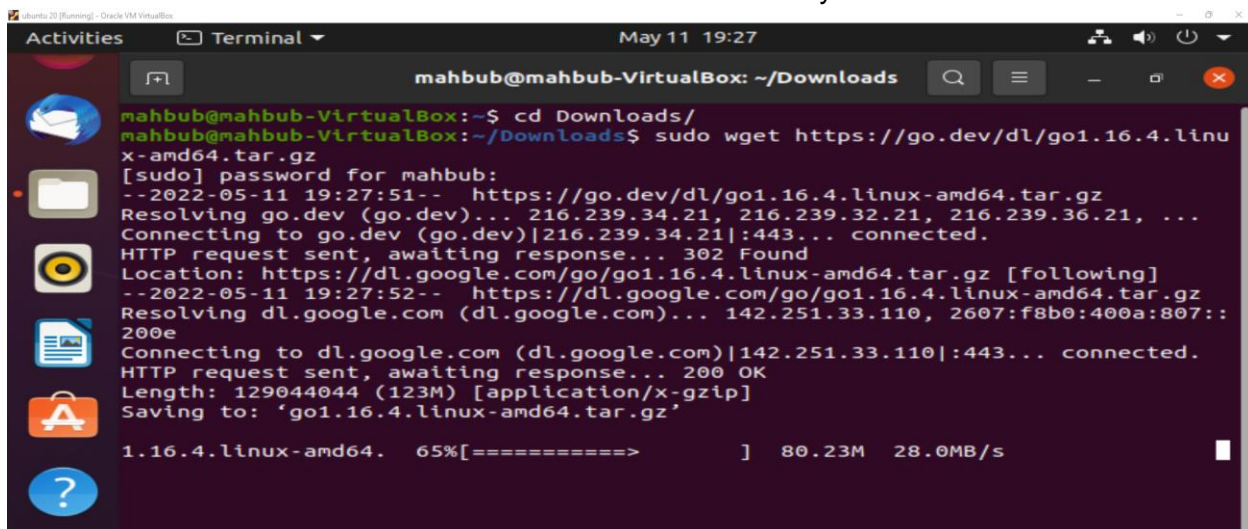


Step 4: Installation of GO language.

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

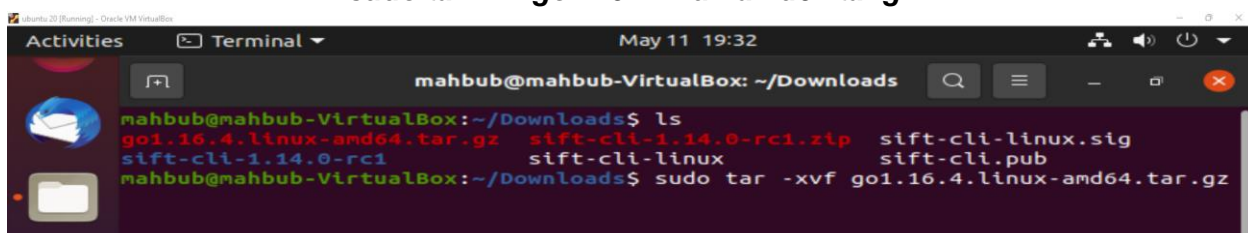
`sudo wget https://go.dev/dl/go1.16.4.linux-amd64.tar.gz`

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`




```

mahbub@mahbub-VirtualBox: ~/Downloads
mahbub@mahbub-VirtualBox:~/Downloads$ ls
go                                sift-cli-1.14.0-rc1.zip  sift-cli.pub
go1.16.4.linux-amd64.tar.gz      sift-cli-linux          sift-cli-linux.sig
sift-cli-1.14.0-rc1             sift-cli-linux.sig
mahbub@mahbub-VirtualBox:~/Downloads$

```

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

```

```

mahbub@mahbub-VirtualBox: ~/Downloads
mahbub@mahbub-VirtualBox:~/Downloads$ sudo mv go /usr/local
mahbub@mahbub-VirtualBox:~/Downloads$ export GOROOT=/usr/local/go
mahbub@mahbub-VirtualBox:~/Downloads$ export GOPATH=$HOME/Projects/Proj1
mahbub@mahbub-VirtualBox:~/Downloads$ export PATH=$GOPATH/bin:$GOROOT/bin:$PATH
mahbub@mahbub-VirtualBox:~/Downloads$ go version
go version go1.16.4 linux/amd64
mahbub@mahbub-VirtualBox:~/Downloads$

```

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”.

```

mahbub@mahbub-VirtualBox:~/Downloads$ go install github.com/sigstore/cosign/cmd/cosign@v1.7.2
go: downloading github.com/sigstore/cosign v1.7.2
go: downloading github.com/google/go-containerregistry v0.8.1-0.20220209165246-a44adc326839
go: downloading github.com/pkg/errors v0.9.1
go: downloading github.com/sigstore/sigstore v1.2.1-0.20220401110139-0e610e39782f
go: downloading github.com/spf13/cobra v1.4.0
go: downloading github.com/spf13/viper v1.10.1
go: downloading sigs.k8s.io/release-utils v0.6.0
go: downloading github.com/docker/cli v20.10.12+incompatible
go: downloading github.com/opencontainers/image-spec v1.0.3-0.20220114050600-8b9d41f48198
go: downloading github.com/mitchellh/go-homedir v1.1.0
go: downloading golang.org/x/sync v0.0.0-20210220032951-036812b2e83c
go: downloading github.com/docker/distribution v2.8.0+incompatible
go: downloading github.com/secure-systems-lab/go-securesystemslib v0.3.1
go: downloading github.com/sigstore/rekor v0.4.1-0.20220114213500-23f583409af3
go: downloading k8s.io/apimachinery v0.23.5
go: downloading github.com/awslabs/amazon-ecr-credential-helper/ecr-login v0.0.0-20220228164355-396b2034c795
go: downloading github.com/chrmellard/docker-credential-acr-env v0.0.0-20220119192733-fe33c00cee21
go: downloading github.com/in-toto/in-toto-golang v0.3.4-0.20211211042327-af1f9fb822bf

```

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***

```

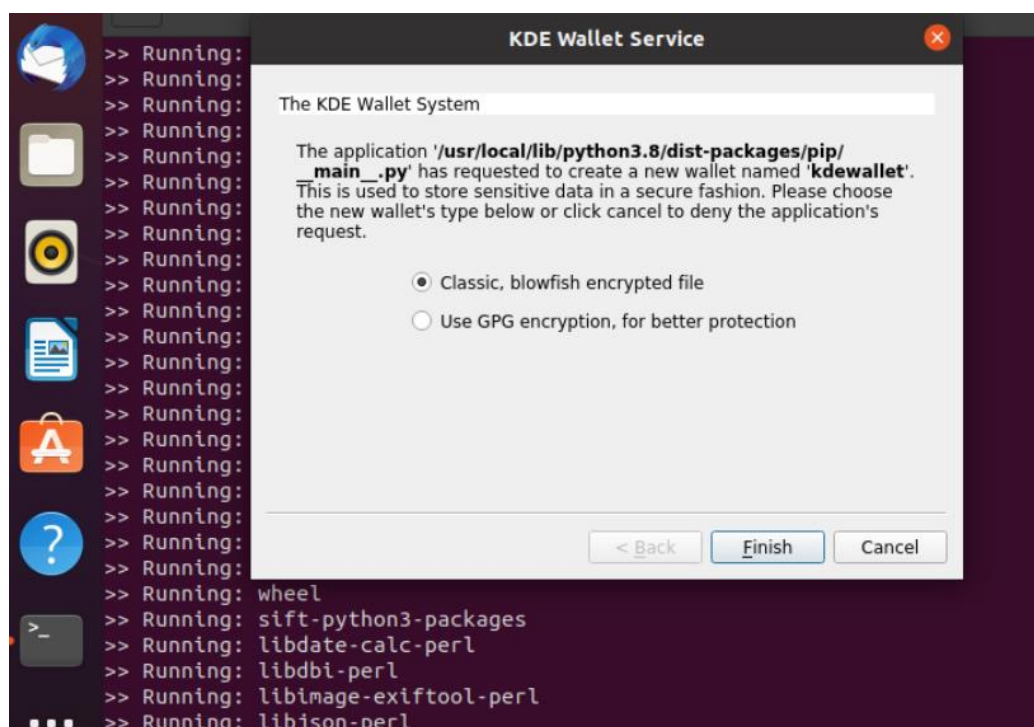
mahbub@mahbub-VirtualBox:~/Downloads$ sudo sift install
> sift-cli@1.14.0-rc1+0-g0582d2b
> sift-version: notinstalled

> mode: desktop
Installing and configuring SaltStack properly ...
> downloading v2022.01.22
>> downloading sift-saltstack-v2022.01.22.tar.gz.asc
>> downloading sift-saltstack-v2022.01.22.tar.gz.sha256
>> downloading sift-saltstack-v2022.01.22.tar.gz.sha256.asc
>> downloading sift-saltstack-v2022.01.22.tar.gz
> validating file sift-saltstack-v2022.01.22.tar.gz
> validating signature for sift-saltstack-v2022.01.22.tar.gz.sha256
> extracting update sift-saltstack-v2022.01.22.tar.gz
> performing update v2022.01.22
>> Log file: /var/cache/sift/cli/v2022.01.22/saltstack.log

>> Running: software-properties-common
>> Running: apt-transport-https
>> Running: deb [arch=amd64] https://download.docker.com/linux/ubuntu focal sta
ble

```

This installation will require 40-60 minutes.



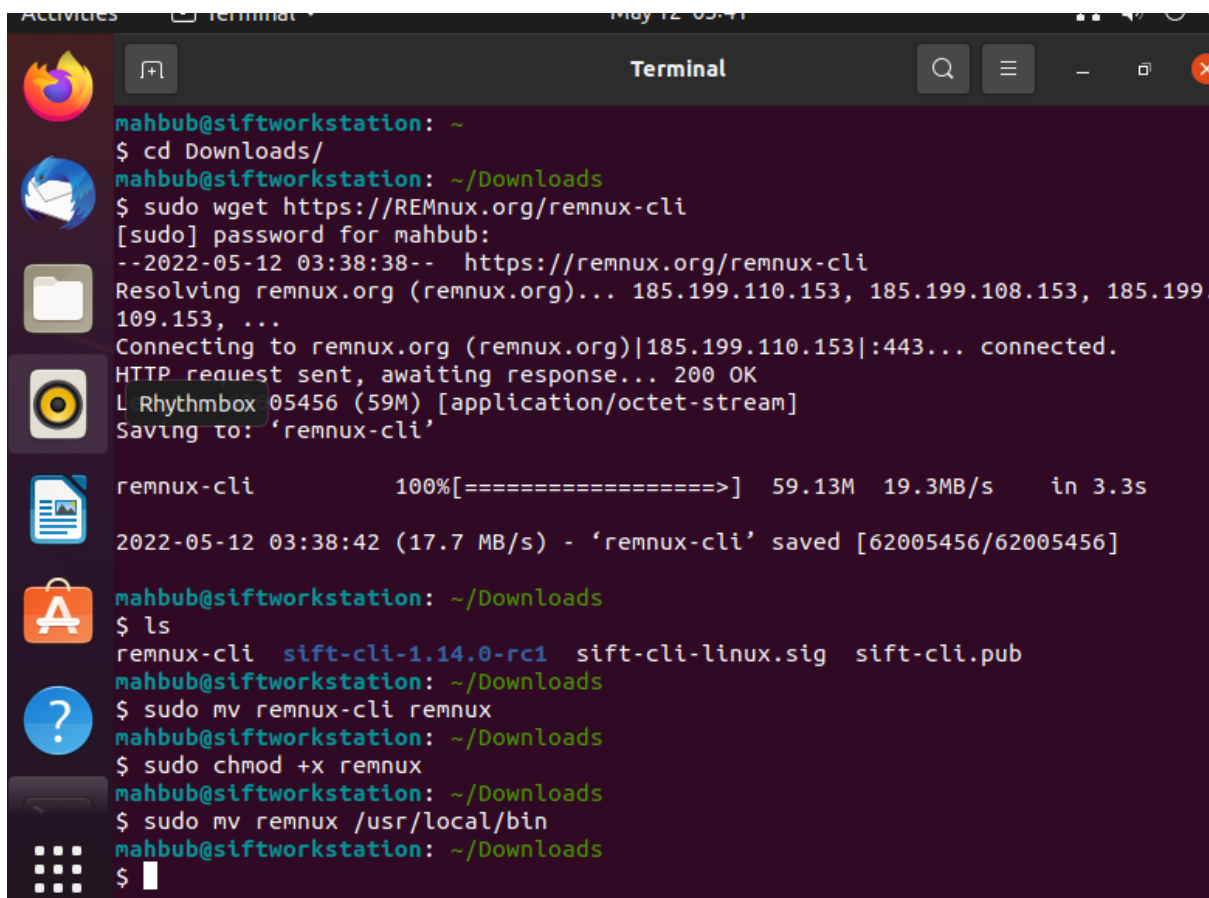
Select Classic, blowfish mode then click finish. You will also need to set the password.

```

>> COMPLETED SUCCESSFULLY -- Success: 664, Failure: 0
mahbub@mahbub-VirtualBox:~/Downloads$

```

Installing REMnux on VirtualBox



```
mahbub@siftworkstation: ~
$ cd Downloads/
mahbub@siftworkstation: ~/Downloads
$ sudo wget https://REMnux.org/remnux-cli
[sudo] password for mahbub:
--2022-05-12 03:38:38-- https://remnux.org/remnux-cli
Resolving remnux.org (remnux.org)... 185.199.110.153, 185.199.108.153, 185.199.109.153, ...
Connecting to remnux.org (remnux.org)|185.199.110.153|:443... connected.
HTTP request sent, awaiting response... 200 OK
L Rhythmbox 05456 (59M) [application/octet-stream]
Saving to: 'remnux-cli'

remnux-cli          100%[=====>]  59.13M  19.3MB/s   in 3.3s

2022-05-12 03:38:42 (17.7 MB/s) - 'remnux-cli' saved [62005456/62005456]

mahbub@siftworkstation: ~/Downloads
$ ls
remnux-cli  sift-cli-1.14.0-rc1  sift-cli-linux.sig  sift-cli.pub
mahbub@siftworkstation: ~/Downloads
$ sudo mv remnux-cli remnux
mahbub@siftworkstation: ~/Downloads
$ sudo chmod +x remnux
mahbub@siftworkstation: ~/Downloads
$ sudo mv remnux /usr/local/bin
mahbub@siftworkstation: ~/Downloads
$
```

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

© 2022, Southern Alberta Institute of Technology. All rights reserved.

This publication and materials herein are protected by applicable intellectual property laws.
Unauthorized reproduction and distribution of this publication in whole or part is prohibited.

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