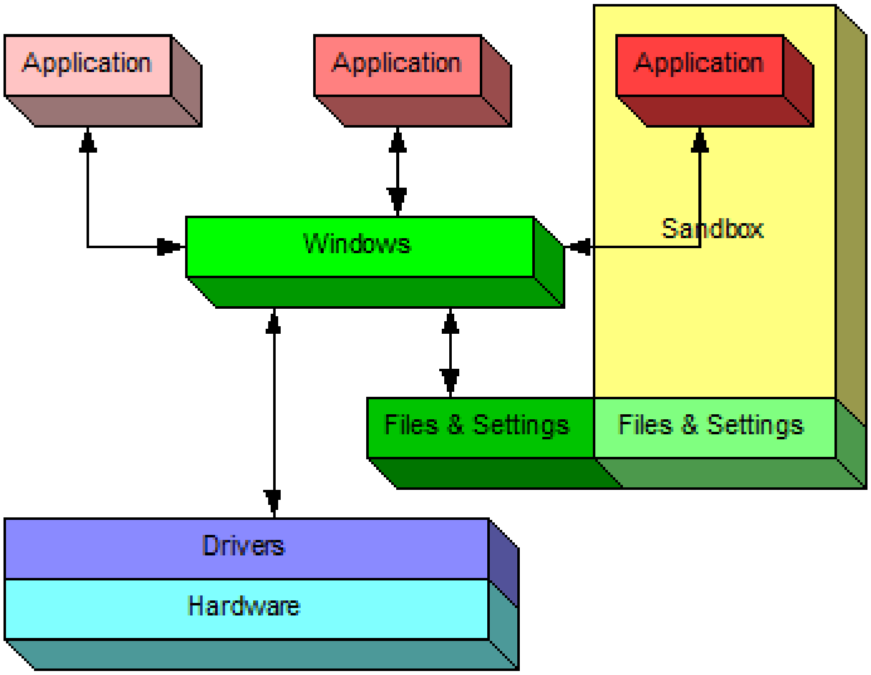
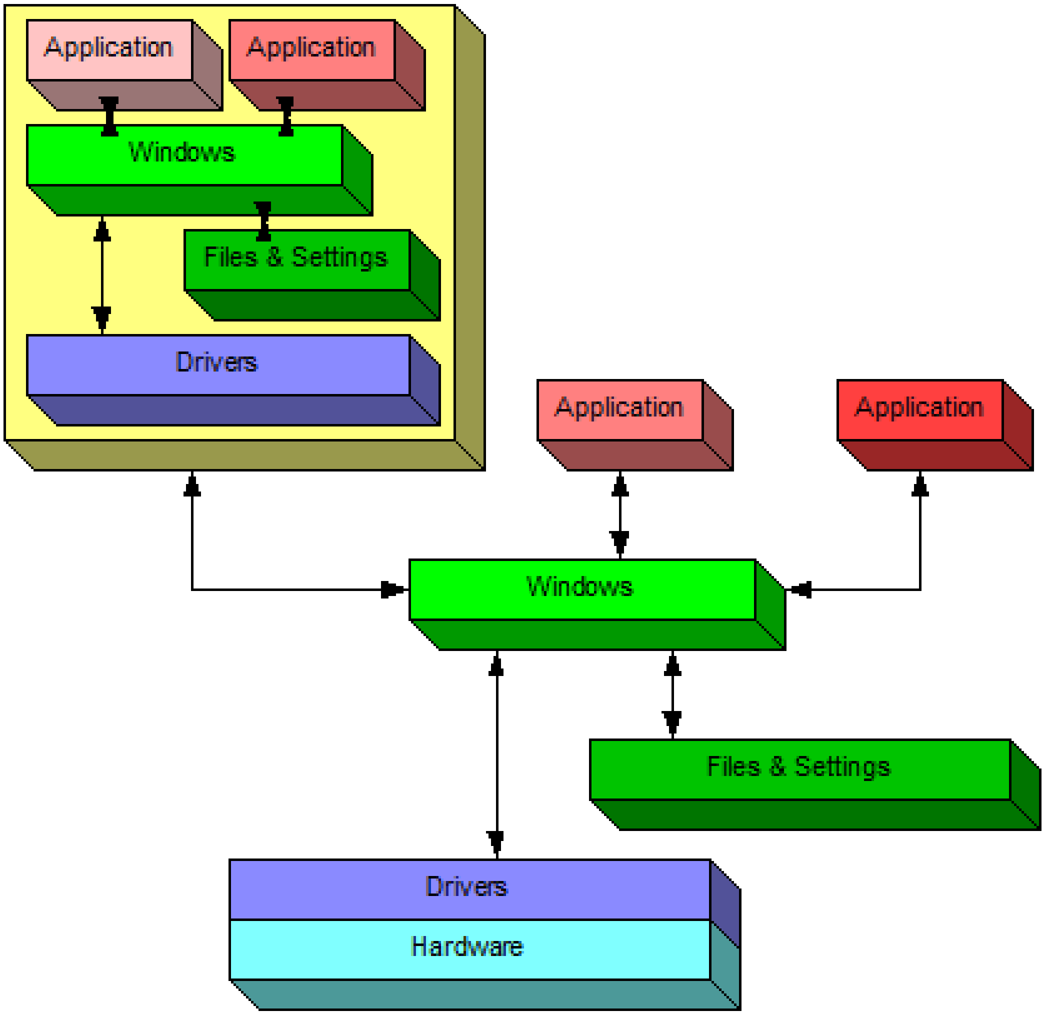
Lab 5: Sandbox Setup and Configuration

Sandbox vsvirtual machine



Sandbox vsvirtual machine



Some SandBox:

- VirusTotal
- Anubis
- VxStream
- Malwr
- SandSift

SANS Investigative Forensic Toolkit (SIFT) Workstation

- An international team of forensics experts CREATED SIFT Workstation for incident response and digital forensics use. The free SIFT that can match any modern incident response and forensic tool suite.
- It demonstrates that advanced investigations and responding to intrusions can be accomplished using cutting-edge open-source tools that are freely available and frequently updated.

Key new features of SIFT

- ➢ Ubuntu LTS 16.04 Base
- ➢ 64 bit base system
- ➢ Better memory utilization
- ➢ Auto-DFIR package update and customizations
- ➢ Latest forensic tools and techniques
- ➢ VMware Appliance ready to tackle forensics
- ➢ Cross compatibility between Linux and Windows
- ➢ Option to install stand-alone via (.iso) or use via VMware Player/Workstation
- ➢ Online Documentation Project athttp://sift.readthedocs.org/
- ➢ Expanded FilesystemSupport

Two ways to install SIFT

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

Option 1: SIFT Workstation VM Appliance

Login to download

Click the 'Login to Download' button and input (or create) your SANS Portal account credentials to download the virtual machine. Once you have booted the virtual machine, use the credentials below to gain access.

- Login = **sansforensics**
- Password = **forensics**
- $ **sudo su -**
  - Use to elevate privileges to root while mounting disk images.

- Hash Values
  - MD5: 6d82c7287e15ecc0c4f90f74d629e282
  - SHA256: fb7c343e65c21d0ff5591957f7a1890b1eaf76acd20f31de619ea6c5c7e4dcf2

Having trouble downloading SIFT?

If you are having trouble downloading the SIFT Workstation VM, please contact sift-support@sans.org and include the URL you were given, your public IP address, browser type, and if you are using a proxy of any kind.

Option 2A: SIFT Easy Installation on Native Ubuntu System

1. Download Ubuntu 22.04 ISO file and install Ubuntu 22.04 on any system - http://www.ubuntu.com/download/desktop

2. Install the Latest Cast Binary from its release page

3. Run '**sudo cast install teamdfir/sift**' to install the latest version of SIFT

4. Congrats -- you now have a SIFT workstation!

1. Login = **sansforensics**

2. Password = **forensics**

3. $ **sudo su -**

1. Use to elevate privileges to root while mounting disk images.

Option 2B: SIFT Easy Installation on Microsoft Windows using Windows Subsystem for Linux

1. Install Windows Subsystem for Linux (WSL) according to Microsoft's latest guidance, currently located at https://docs.microsoft.com/en-us/windows/wsl/install-win10. The SIFT distribution can be installed on either WSL version 1 or version 2.

1. Choose Ubuntu 22.04 during the WSL installation process.

2. Launch the Ubuntu Bash Shell and elevate to root (**sudo su**) to avoid permissions issues during the installation process.

3. Install the Latest Cast Binary from its release page

4. Run '**sudo cast install --mode=server teamdfir/sift-saltstack**' to install the latest version of SIFT in WSL

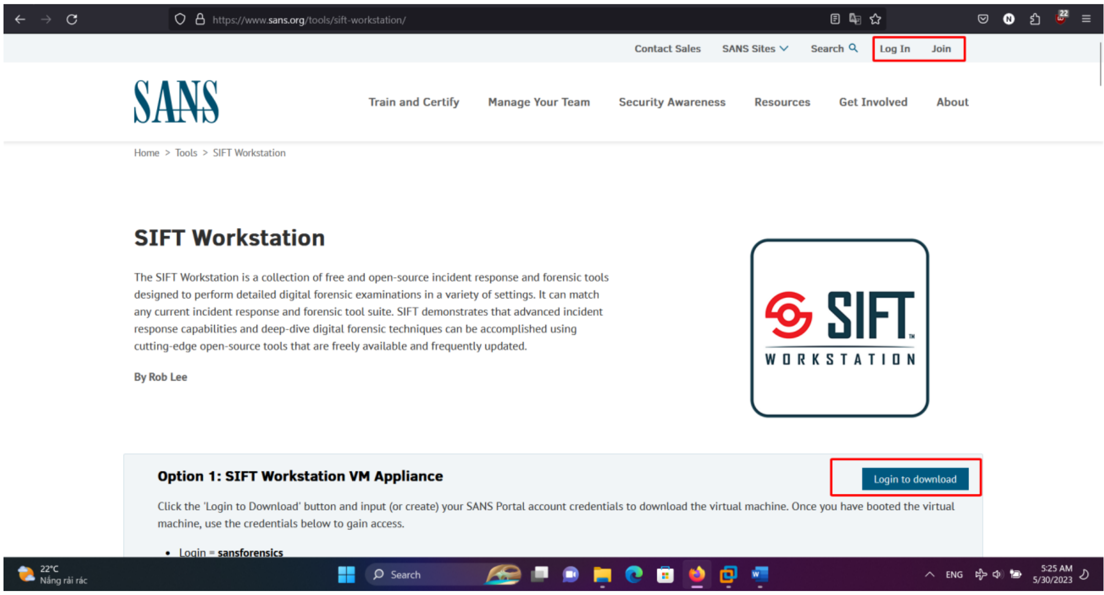
5. Congrats -- you now have a SIFT Workstation in Windows!

- Download SIFT Workstation VMware Appliance (https://www.sans.org/tools/sift-workstation/)

Here, we will install Sans Sift and perform Virus analysis on Sans Sift's Ubuntu environment. Sans Sift is an environment specialized for performing forensics.

Just go to https://www.sans.org/tools/sift-workstation/ and log in or create an account before installing, Sans will ask that we need an account before installing.

After creating an account/login, we can start downloading



SIFT Workstation

The SIFT Workstation is a collection of free and open-source incident response and forensic tools designed to perform detailed digital forensic examinations in a variety of settings. It can match any current incident response and forensic tool suite. SIFT demonstrates that advanced incident response capabilities and deep-dive digital forensic techniques can be accomplished using cutting-edge open-source tools that are freely available and frequently updated.

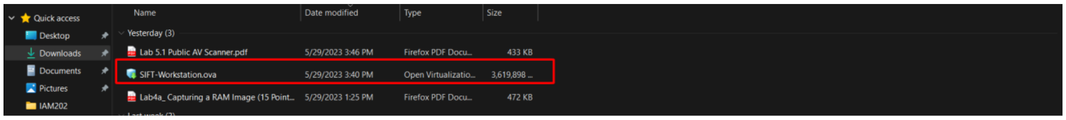
By Rob Lee

Option 1: SIFT Workstation VM Appliance

Click the 'Login to Download' button and input (or create) your SANS Portal account credentials to download the virtual machine. Once you have booted the virtual machine, use the credentials below to gain access.

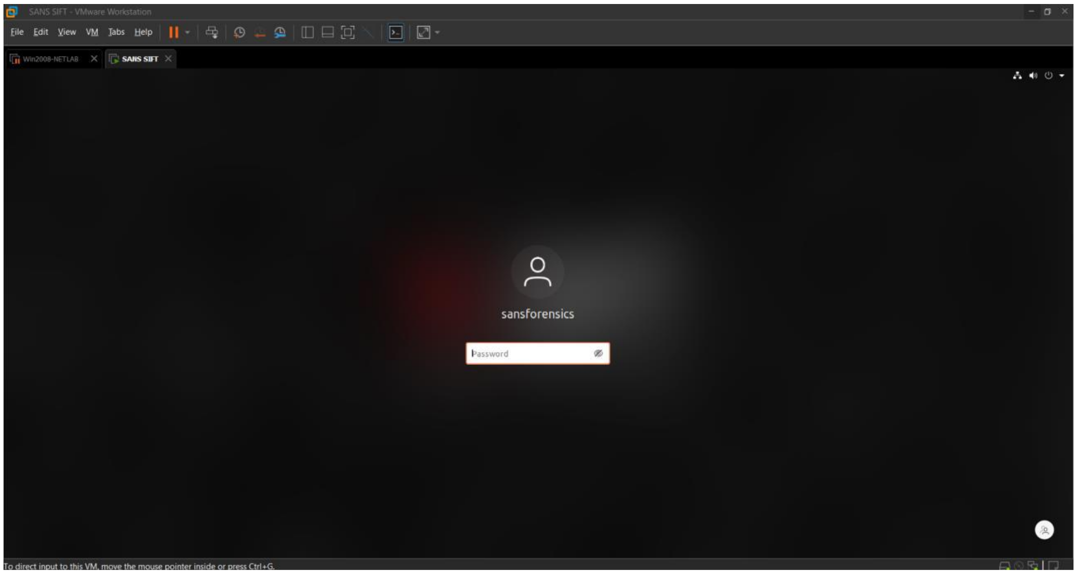
- Login = sansforensics

When downloaded, we will have a file with the ova extension. This is a pre-configured virtual machine file, we just need to double click to run it in VMware.



Name	Date modified	Type	Size
Yesterday (3)			
Lab 5.1 Public AV Scanner.pdf	5/29/2023 3:46 PM	Firefox PDF Docu...	433 KB
SIFT-Workstation.ova	5/29/2023 3:40 PM	Open Virtualizatio...	3,619,898 ...
Lab4a_ Capturing a RAM Image (15 Point...	5/29/2023 1:25 PM	Firefox PDF Docu...	472 KB

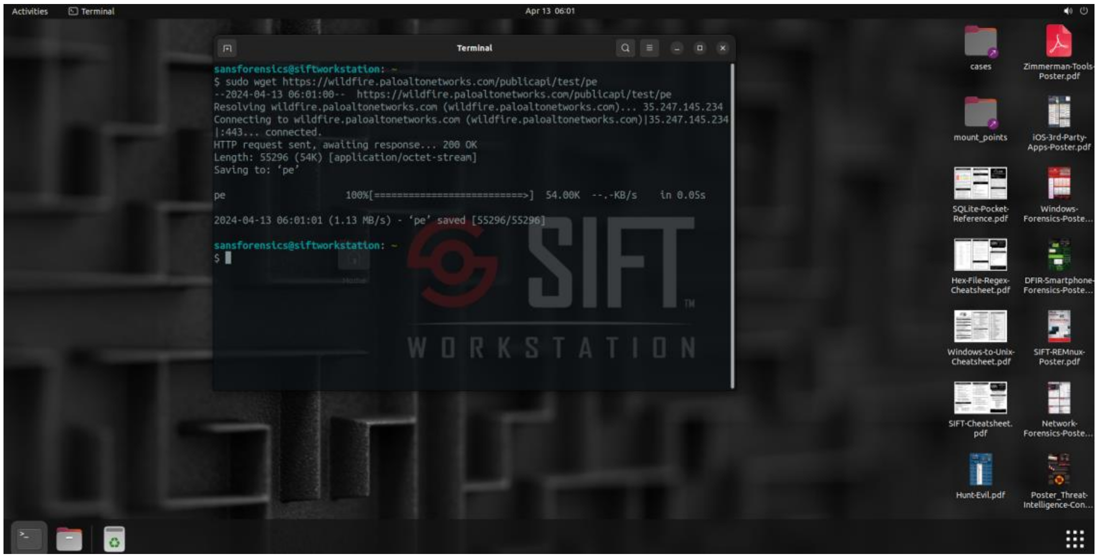
After importing, we will log in with the user name: **sansforensics** and password: **forensics**



To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

We download the following sample to test:

sudo wget https://wildfire.paloaltonetworks.com/publicapi/test/pe


Activities
Terminal
Apr 13 06:01
Terminal
cases
Zimmerman-Tools-Poster.pdf
mount_points
iOS-3rd-Party-Apps-Poster.pdf
SQLite-Pocket-Reference.pdf
Windows-Forensics-Poste...
Hex-File-Regex-Cheatsheet.pdf
DFIR-Smartphone-Forensics-Poste...
Windows-to-Unix-Cheatsheet.pdf
SIFT-REMnux-Poster.pdf
SIFT-Cheatsheet.pdf
Network-Forensics-Poste...
Hunt-Evil.pdf
Poster_Threat-Intelligence-Con...

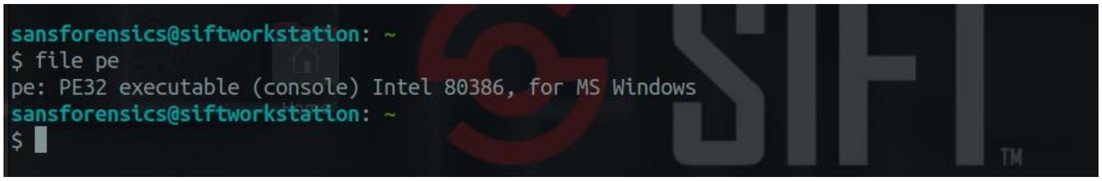
```
sansforensics@siftworkstation: ~
$ sudo wget https://wildfire.paloaltonetworks.com/publicapi/test/pe
--2024-04-13 06:01:00--  https://wildfire.paloaltonetworks.com/publicapi/test/pe
Resolving wildfire.paloaltonetworks.com (wildfire.paloaltonetworks.com)... 35.247.145.234
Connecting to wildfire.paloaltonetworks.com (wildfire.paloaltonetworks.com)|35.247.145.234
|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 55296 (54K) [application/octet-stream]
Saving to: ‘pe’

pe                      100%[==========================>]  54.00K  --.-KB/s    in 0.05s

2024-04-13 06:01:01 (1.13 MB/s) - ‘pe’ saved [55296/55296]

sansforensics@siftworkstation: ~
$ 
```

Using the file to check, we can see that this is a 32bit executable file, using Intel 80386, used to execute on the Windows operating system.



```
sansforensics@siftworkstation: ~
$ file pe
pe: PE32 executable (console) Intel 80386, for MS Windows
sansforensics@siftworkstation: ~
$ 
```

- Install for yourself(https://github.com/sans-dfir/sift-cli#instructions)

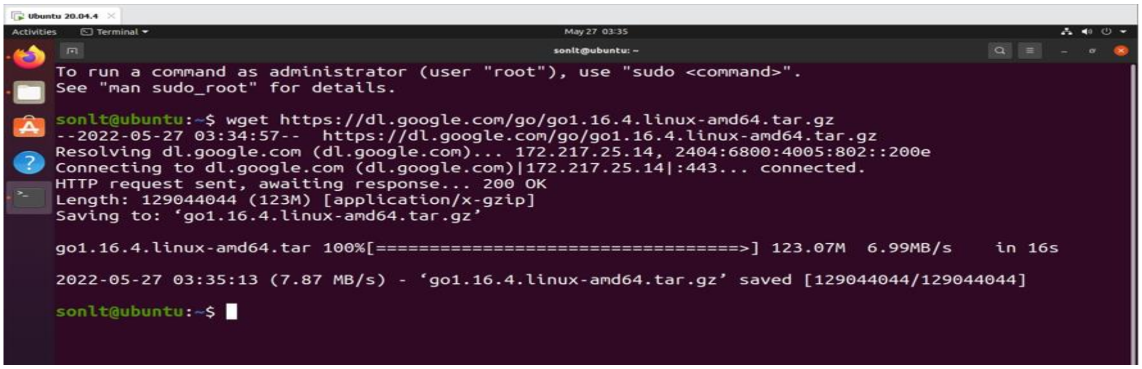
Need Ubuntu version 20.04.4 or higher because 16.04 does not support SIFT and 18.04 has installation errors

Download related files at **https://github.com/teamdfir/sift-cli/releases/tag/v1.14.0- rc1**, including

- sift-cli-linux
- sift-cli-linux.sig
- sift-cli.pub

Download GO's zip file, used to compile and use Cosign software to check the integrity of the above 3 SIFT files

wget https://dl.google.com/go/go1.16.4.linux-amd64.tar.gz



```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

sonlt@ubuntu:~$ wget https://dl.google.com/go/go1.16.4.linux-amd64.tar.gz
--2022-05-27 03:34:57--  https://dl.google.com/go/go1.16.4.linux-amd64.tar.gz
Resolving dl.google.com (dl.google.com)... 172.217.25.14, 2404:6800:4005:802::200e
Connecting to dl.google.com (dl.google.com)|172.217.25.14|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 129044044 (123M) [application/x-gzip]
Saving to: ‘go1.16.4.linux-amd64.tar.gz’

go1.16.4.linux-amd64.tar 100%[===================================>] 123.07M  6.99MB/s    in 16s

2022-05-27 03:35:13 (7.87 MB/s) - ‘go1.16.4.linux-amd64.tar.gz’ saved [129044044/129044044]

sonlt@ubuntu:~$ 
```

Unzip GO: **sudo tar -xvf go1.16.4.linux-amd64.tar.gz**

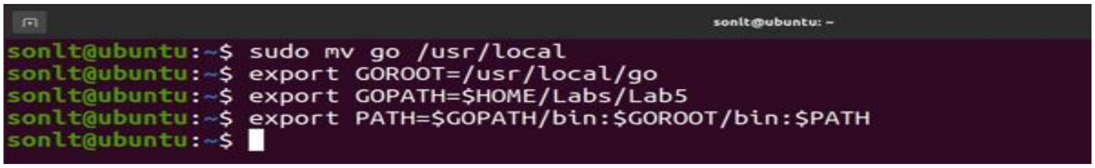
Create environment for GO**: sudo mv go /usr/local**

Create environment variables for GO:

export GOROOT=/usr/local/go

export GOPATH=$HOME/Labs/Lab5

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

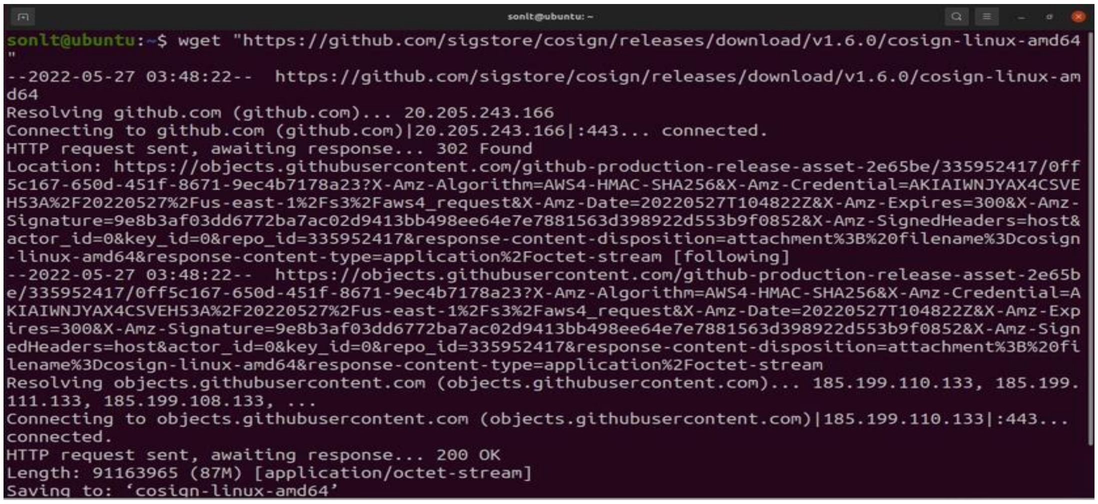


```
sonlt@ubuntu:~$ sudo mv go /usr/local
sonlt@ubuntu:~$ export GOROOT=/usr/local/go
sonlt@ubuntu:~$ export GOPATH=$HOME/Labs/Lab5
sonlt@ubuntu:~$ export PATH=$GOPATH/bin:$GOROOT/bin:$PATH
sonlt@ubuntu:~$ 
```

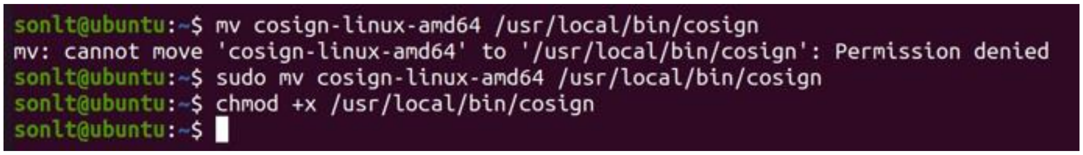
Install Cosign:

get "https://github.com/sigstore/cosign/releases/download/v1.6.0/cosign- linux-amd64"

sudo mv cosign-linux-amd64 /usr/local/bin/cosign chmod +x /usr/local/bin/cosign



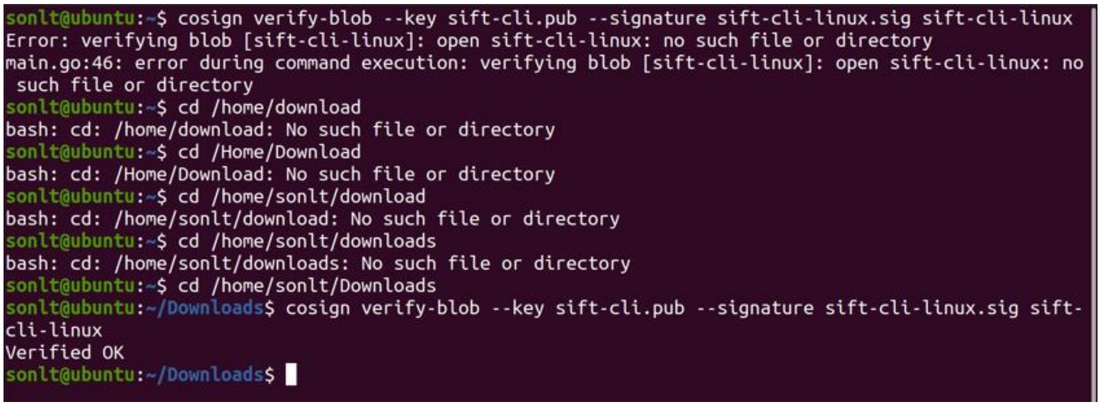
```
sonlt@ubuntu:~$ wget "https://github.com/sigstore/cosign/releases/download/v1.6.0/cosign-linux-amd64
"
--2022-05-27 03:48:22--  https://github.com/sigstore/cosign/releases/download/v1.6.0/cosign-linux-am
d64
Resolving github.com (github.com)... 20.205.243.166
Connecting to github.com (github.com)|20.205.243.166|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/335952417/0ff
5c167-650d-451f-8671-9ec4b7178a23?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVE
H53A%2F20220527%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20220527T104822Z&X-Amz-Expires=300&X-Amz-
Signature=9e8b3af03dd6772ba7ac02d9413bb498ee64e7e7881563d398922d553b9f0852&X-Amz-SignedHeaders=host&
actor_id=0&key_id=0&repo_id=335952417&response-content-disposition=attachment%3B%20filename%3Dcosign
-linux-amd64&response-content-type=application%2Foctet-stream [following]
--2022-05-27 03:48:22--  https://objects.githubusercontent.com/github-production-release-asset-2e65b
e/335952417/0ff5c167-650d-451f-8671-9ec4b7178a23?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=A
KIAIWNJYAX4CSVEH53A%2F20220527%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20220527T104822Z&X-Amz-Exp
ires=300&X-Amz-Signature=9e8b3af03dd6772ba7ac02d9413bb498ee64e7e7881563d398922d553b9f0852&X-Amz-Sign
edHeaders=host&actor_id=0&key_id=0&repo_id=335952417&response-content-disposition=attachment%3B%20fi
lename%3Dcosign-linux-amd64&response-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.110.133, 185.199.
111.133, 185.199.108.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.110.133|:443...
connected.
HTTP request sent, awaiting response... 200 OK
Length: 91163965 (87M) [application/octet-stream]
Saving to: ‘cosign-linux-amd64’
```



```
sonlt@ubuntu:~$ mv cosign-linux-amd64 /usr/local/bin/cosign
mv: cannot move 'cosign-linux-amd64' to '/usr/local/bin/cosign': Permission denied
sonlt@ubuntu:~$ sudo mv cosign-linux-amd64 /usr/local/bin/cosign
sonlt@ubuntu:~$ chmod +x /usr/local/bin/cosign
sonlt@ubuntu:~$ 
```

Verify SIFT Signature:

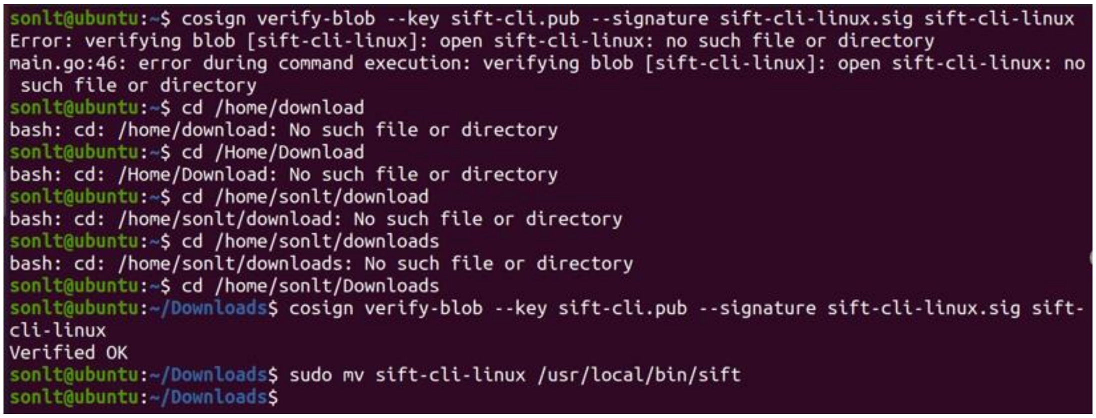
cosign verify-blob --key sift-cli.pub --signature sift-cli-linux.sig sift-cli-linux



```
sonlt@ubuntu:~$ cosign verify-blob --key sift-cli.pub --signature sift-cli-linux.sig sift-cli-linux
Error: verifying blob [sift-cli-linux]: open sift-cli-linux: no such file or directory
main.go:46: error during command execution: verifying blob [sift-cli-linux]: open sift-cli-linux: no
 such file or directory
sonlt@ubuntu:~$ cd /home/download
bash: cd: /home/download: No such file or directory
sonlt@ubuntu:~$ cd /Home/Download
bash: cd: /Home/Download: No such file or directory
sonlt@ubuntu:~$ cd /home/sonlt/download
bash: cd: /home/sonlt/download: No such file or directory
sonlt@ubuntu:~$ cd /home/sonlt/downloads
bash: cd: /home/sonlt/downloads: No such file or directory
sonlt@ubuntu:~$ cd /home/sonlt/Downloads
sonlt@ubuntu:~/Downloads$ cosign verify-blob --key sift-cli.pub --signature sift-cli-linux.sig sift-
cli-linux
Verified OK
sonlt@ubuntu:~/Downloads$ 
```

Transfer files to the created GO environment:

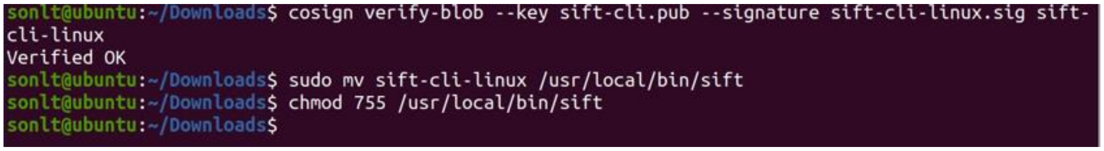
sudo mv sift-cli-linux /usr/local/bin/sift



```
sonlt@ubuntu:~$ cosign verify-blob --key sift-cli.pub --signature sift-cli-linux.sig sift-cli-linux
Error: verifying blob [sift-cli-linux]: open sift-cli-linux: no such file or directory
main.go:46: error during command execution: verifying blob [sift-cli-linux]: open sift-cli-linux: no
 such file or directory
sonlt@ubuntu:~$ cd /home/download
bash: cd: /home/download: No such file or directory
sonlt@ubuntu:~$ cd /Home/Download
bash: cd: /Home/Download: No such file or directory
sonlt@ubuntu:~$ cd /home/sonlt/download
bash: cd: /home/sonlt/download: No such file or directory
sonlt@ubuntu:~$ cd /home/sonlt/downloads
bash: cd: /home/sonlt/downloads: No such file or directory
sonlt@ubuntu:~$ cd /home/sonlt/Downloads
sonlt@ubuntu:~/Downloads$ cosign verify-blob --key sift-cli.pub --signature sift-cli-linux.sig sift-
cli-linux
Verified OK
sonlt@ubuntu:~/Downloads$ sudo mv sift-cli-linux /usr/local/bin/sift
sonlt@ubuntu:~/Downloads$
```

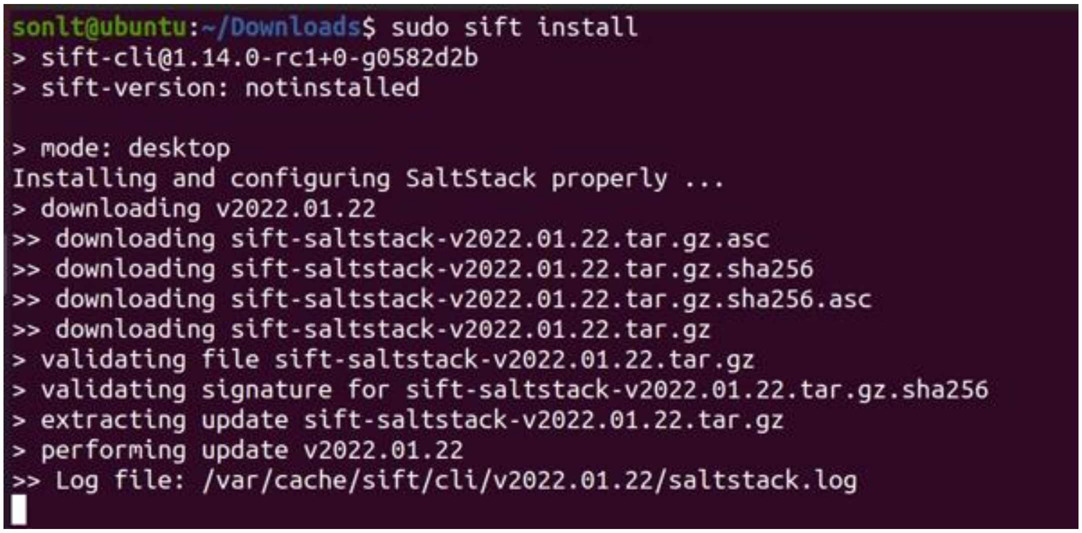
Use chmod to grant permissions to read and execute the file:

chmod 755 /usr/local/bin/sift



```
sonlt@ubuntu:~/Downloads$ cosign verify-blob --key sift-cli.pub --signature sift-cli-linux.sig sift-
cli-linux
Verified OK
sonlt@ubuntu:~/Downloads$ sudo mv sift-cli-linux /usr/local/bin/sift
sonlt@ubuntu:~/Downloads$ chmod 755 /usr/local/bin/sift
sonlt@ubuntu:~/Downloads$
```

Install SIFT**: sudo sift install**



```
sonlt@ubuntu:~/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
```