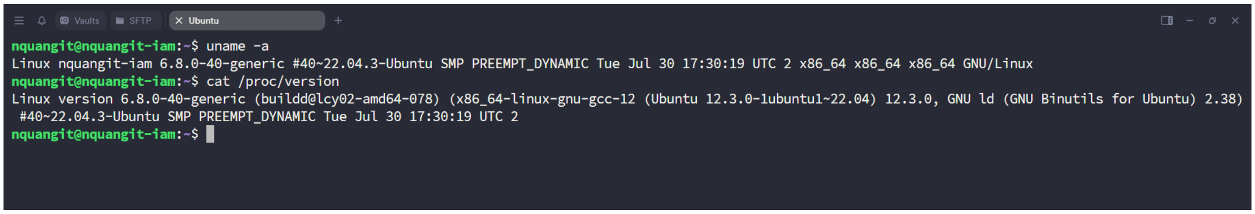
Lab 2 (2-3-4)

Huỳnh Ngọc Quang SE181838

Install and Use ClamAV

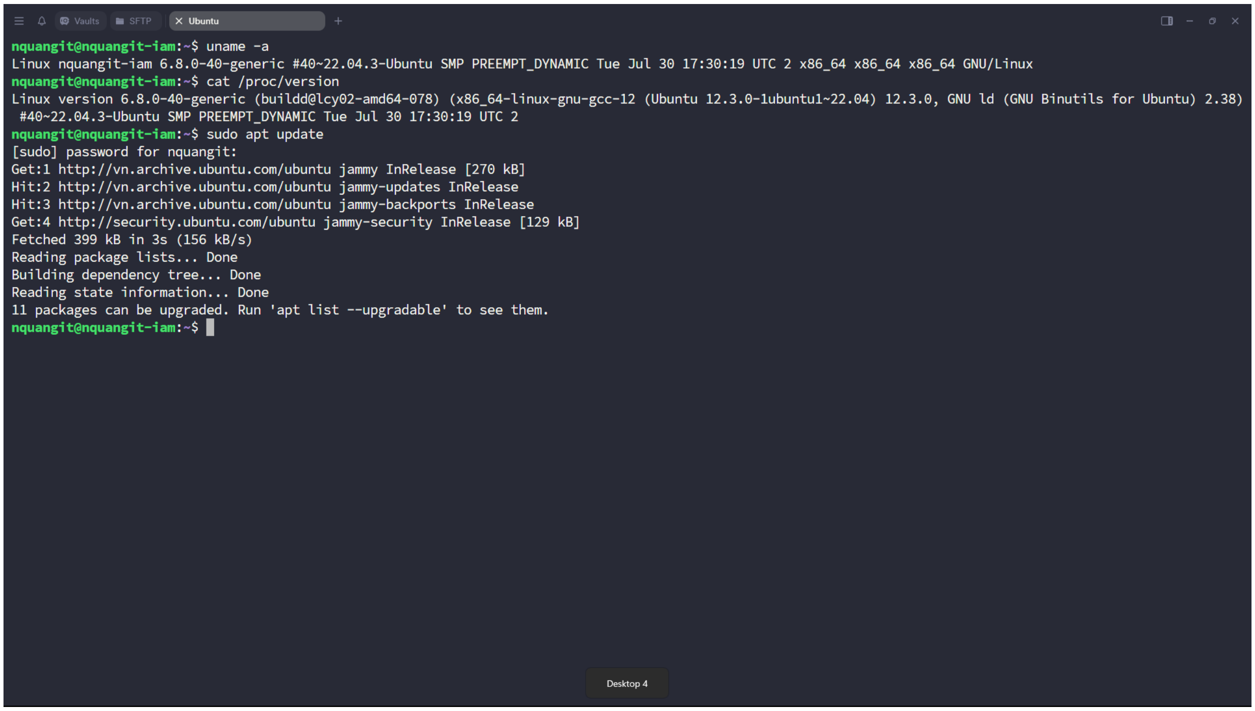
OS Install:



```
nquangit@nquangit-iam:~$ uname -a
Linux nquangit-iam 6.8.0-40-generic #40~22.04.3-Ubuntu SMP PREEMPT_DYNAMIC Tue Jul 30 17:30:19 UTC 2 x86_64 x86_64 x86_64 GNU/Linux
nquangit@nquangit-iam:~$ cat /proc/version
Linux version 6.8.0-40-generic (buildd@lcy02-amd64-078) (x86_64-linux-gnu-gcc-12 (Ubuntu 12.3.0-1ubuntu1~22.04) 12.3.0, GNU ld (GNU Binutils for Ubuntu) 2.38)
 #40~22.04.3-Ubuntu SMP PREEMPT_DYNAMIC Tue Jul 30 17:30:19 UTC 2
nquangit@nquangit-iam:~$
```

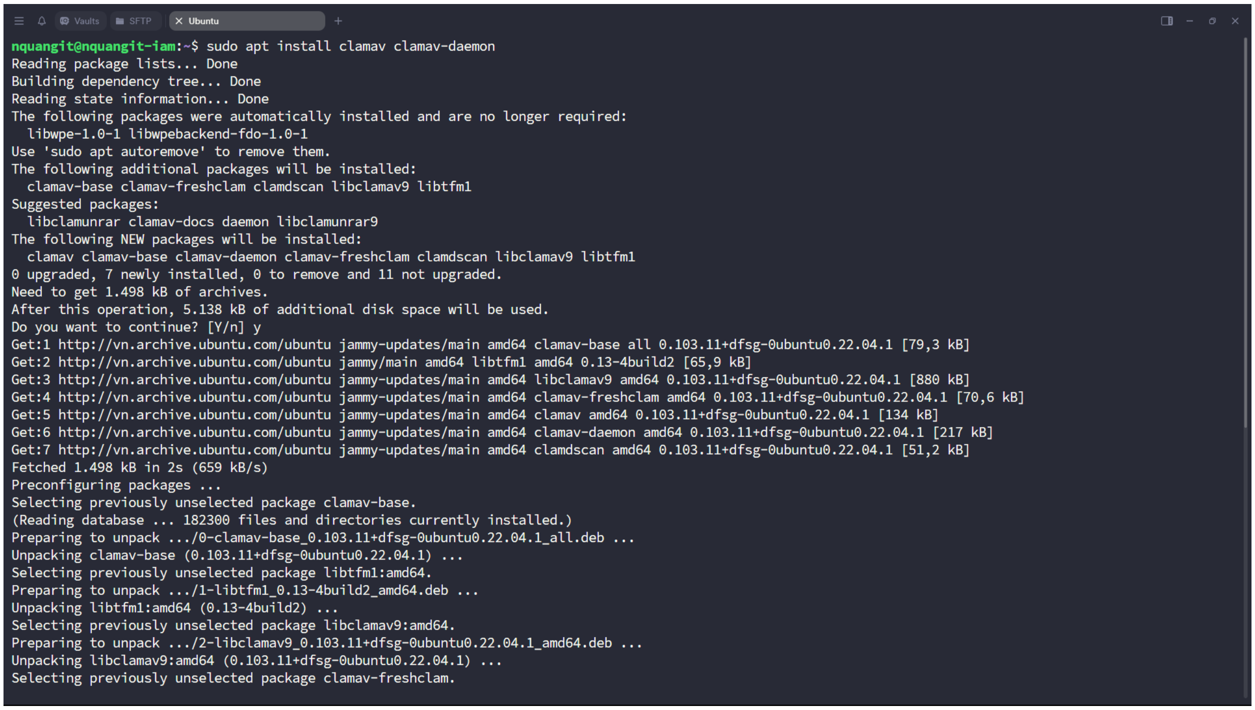
Install ClamAV on Ubuntu

Step 1: Update the Repository

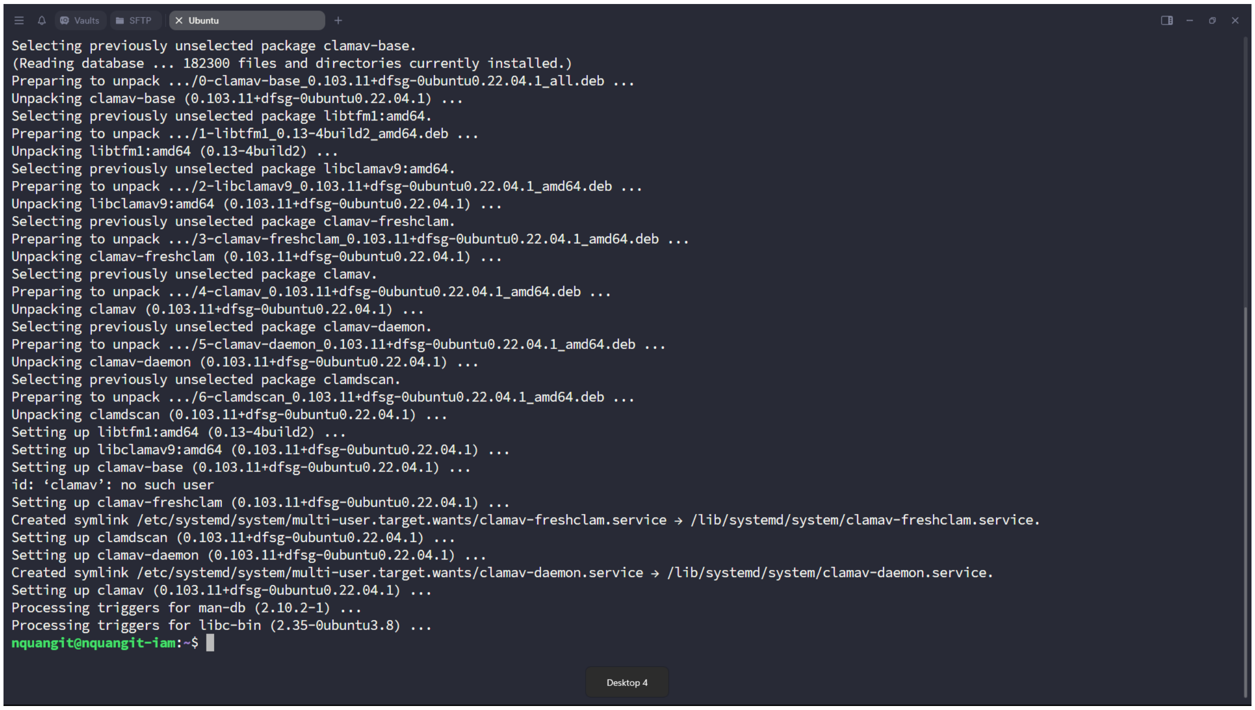


```
nquangit@nquangit-iam:~$ uname -a
Linux nquangit-iam 6.8.0-40-generic #40~22.04.3-Ubuntu SMP PREEMPT_DYNAMIC Tue Jul 30 17:30:19 UTC 2 x86_64 x86_64 x86_64 GNU/Linux
nquangit@nquangit-iam:~$ cat /proc/version
Linux version 6.8.0-40-generic (buildd@lcy02-amd64-078) (x86_64-linux-gnu-gcc-12 (Ubuntu 12.3.0-1ubuntu1~22.04) 12.3.0, GNU ld (GNU Binutils for Ubuntu) 2.38)
 #40~22.04.3-Ubuntu SMP PREEMPT_DYNAMIC Tue Jul 30 17:30:19 UTC 2
nquangit@nquangit-iam:~$ sudo apt update
[sudo] password for nquangit:
Get:1 http://vn.archive.ubuntu.com/ubuntu jammy InRelease [270 kB]
Hit:2 http://vn.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://vn.archive.ubuntu.com/ubuntu jammy-backports InRelease
Get:4 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Fetched 399 kB in 3s (156 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
11 packages can be upgraded. Run 'apt list --upgradable' to see them.
nquangit@nquangit-iam:~$
```

Step 2: Install ClamAV

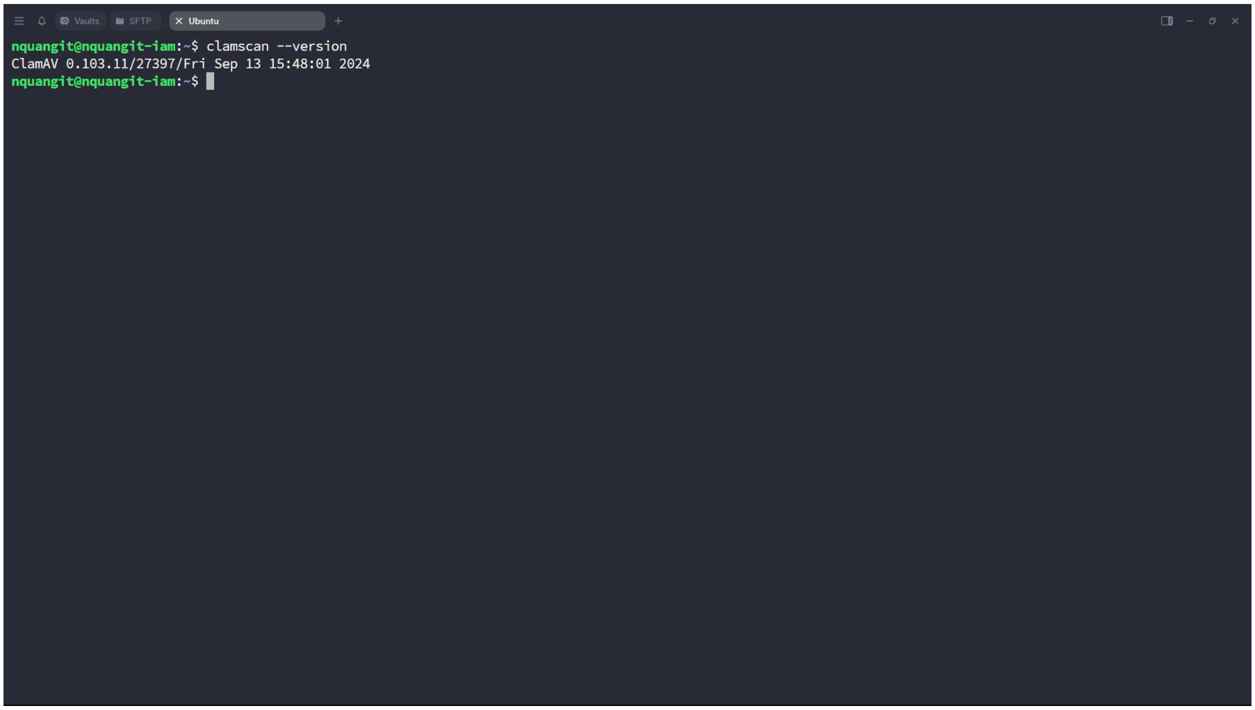


```
nquangit@nquangit-iam:~$ sudo apt install clamav clamav-daemon
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libwpe-1.0-1 libwpebackend-fdo-1.0-1
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  clamav-base clamav-freshclam clamdscan libclamav9 libtfm1
Suggested packages:
  libclamunrar clamav-docs daemon libclamunrar9
The following NEW packages will be installed:
  clamav clamav-base clamav-daemon clamav-freshclam clamdscan libclamav9 libtfm1
0 upgraded, 7 newly installed, 0 to remove and 11 not upgraded.
Need to get 1.498 kB of archives.
After this operation, 5.138 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://vn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 clamav-base all 0.103.11+dfsg-0ubuntu0.22.04.1 [79,3 kB]
Get:2 http://vn.archive.ubuntu.com/ubuntu jammy/main amd64 libtfm1 amd64 0.13-4build2 [65,9 kB]
Get:3 http://vn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libclamav9 amd64 0.103.11+dfsg-0ubuntu0.22.04.1 [880 kB]
Get:4 http://vn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 clamav-freshclam amd64 0.103.11+dfsg-0ubuntu0.22.04.1 [70,6 kB]
Get:5 http://vn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 clamav amd64 0.103.11+dfsg-0ubuntu0.22.04.1 [134 kB]
Get:6 http://vn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 clamav-daemon amd64 0.103.11+dfsg-0ubuntu0.22.04.1 [217 kB]
Get:7 http://vn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 clamdscan amd64 0.103.11+dfsg-0ubuntu0.22.04.1 [51,2 kB]
Fetched 1.498 kB in 2s (659 kB/s)
Preconfiguring packages ...
Selecting previously unselected package clamav-base.
(Reading database ... 182300 files and directories currently installed.)
Preparing to unpack .../0-clamav-base_0.103.11+dfsg-0ubuntu0.22.04.1_all.deb ...
Unpacking clamav-base (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Selecting previously unselected package libtfm1:amd64.
Preparing to unpack .../1-libtfm1_0.13-4build2_amd64.deb ...
Unpacking libtfm1:amd64 (0.13-4build2) ...
Selecting previously unselected package libclamav9:amd64.
Preparing to unpack .../2-libclamav9_0.103.11+dfsg-0ubuntu0.22.04.1_amd64.deb ...
Unpacking libclamav9:amd64 (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Selecting previously unselected package clamav-freshclam.
```



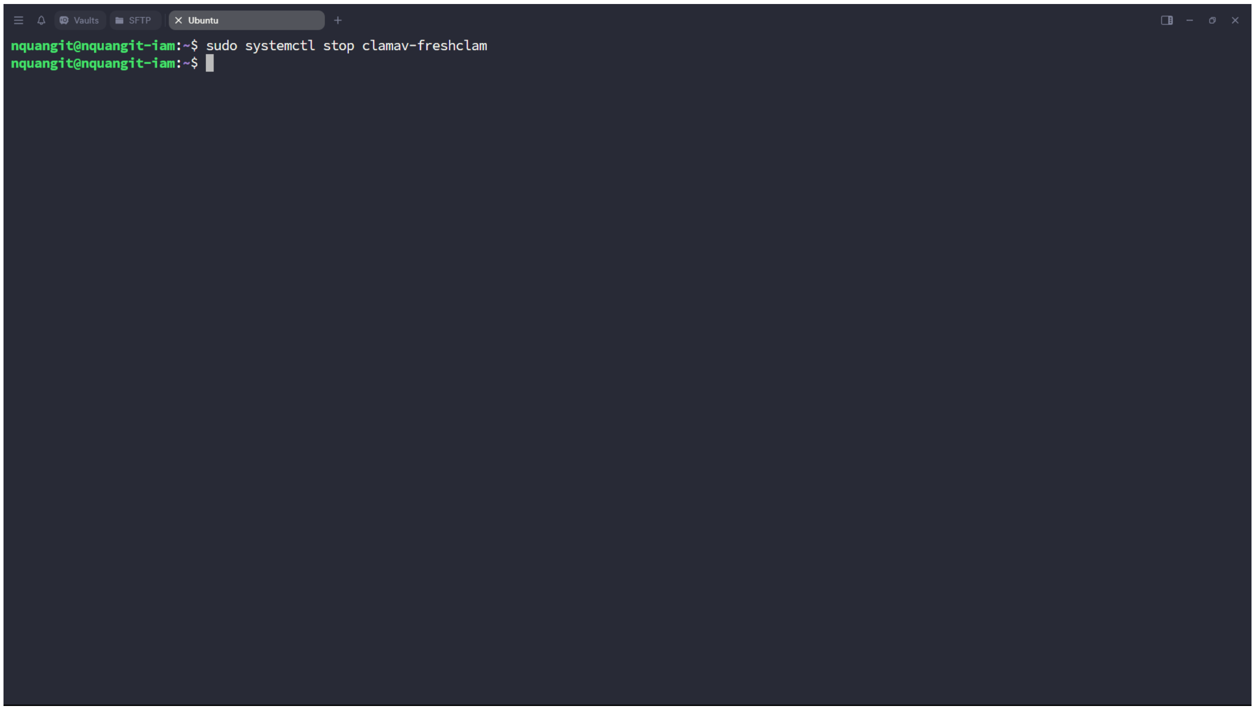
```
Selecting previously unselected package clamav-base.
(Reading database ... 182300 files and directories currently installed.)
Preparing to unpack .../0-clamav-base_0.103.11+dfsg-0ubuntu0.22.04.1_all.deb ...
Unpacking clamav-base (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Selecting previously unselected package libtfm1:amd64.
Preparing to unpack .../1-libtfm1_0.13-4build2_amd64.deb ...
Unpacking libtfm1:amd64 (0.13-4build2) ...
Selecting previously unselected package libclamav9:amd64.
Preparing to unpack .../2-libclamav9_0.103.11+dfsg-0ubuntu0.22.04.1_amd64.deb ...
Unpacking libclamav9:amd64 (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Selecting previously unselected package clamav-freshclam.
Preparing to unpack .../3-clamav-freshclam_0.103.11+dfsg-0ubuntu0.22.04.1_amd64.deb ...
Unpacking clamav-freshclam (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Selecting previously unselected package clamav.
Preparing to unpack .../4-clamav_0.103.11+dfsg-0ubuntu0.22.04.1_amd64.deb ...
Unpacking clamav (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Selecting previously unselected package clamav-daemon.
Preparing to unpack .../5-clamav-daemon_0.103.11+dfsg-0ubuntu0.22.04.1_amd64.deb ...
Unpacking clamav-daemon (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Selecting previously unselected package clamdscan.
Preparing to unpack .../6-clamdscan_0.103.11+dfsg-0ubuntu0.22.04.1_amd64.deb ...
Unpacking clamdscan (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Setting up libtfm1:amd64 (0.13-4build2) ...
Setting up libclamav9:amd64 (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Setting up clamav-base (0.103.11+dfsg-0ubuntu0.22.04.1) ...
id: ‘clamav’: no such user
Setting up clamav-freshclam (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/clamav-freshclam.service → /lib/systemd/system/clamav-freshclam.service.
Setting up clamdscan (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Setting up clamav-daemon (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/clamav-daemon.service → /lib/systemd/system/clamav-daemon.service.
Setting up clamav (0.103.11+dfsg-0ubuntu0.22.04.1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.8) ...
nquangit@nquangit-iam:~$
```

Step 3: Verify ClamAV



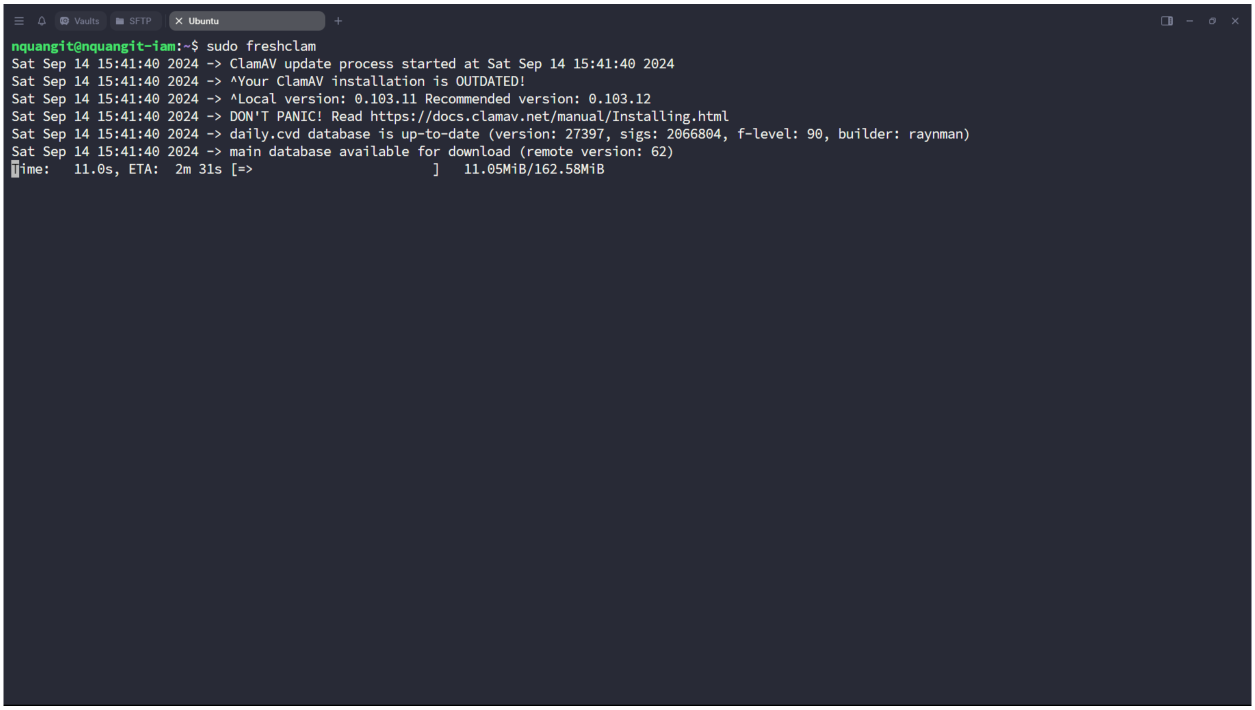
```
nquangit@nquangit-iam:~$ clamscan --version
ClamAV 0.103.11/27397/Fri Sep 13 15:48:01 2024
nquangit@nquangit-iam:~$
```

Disable the “freshclam” Service

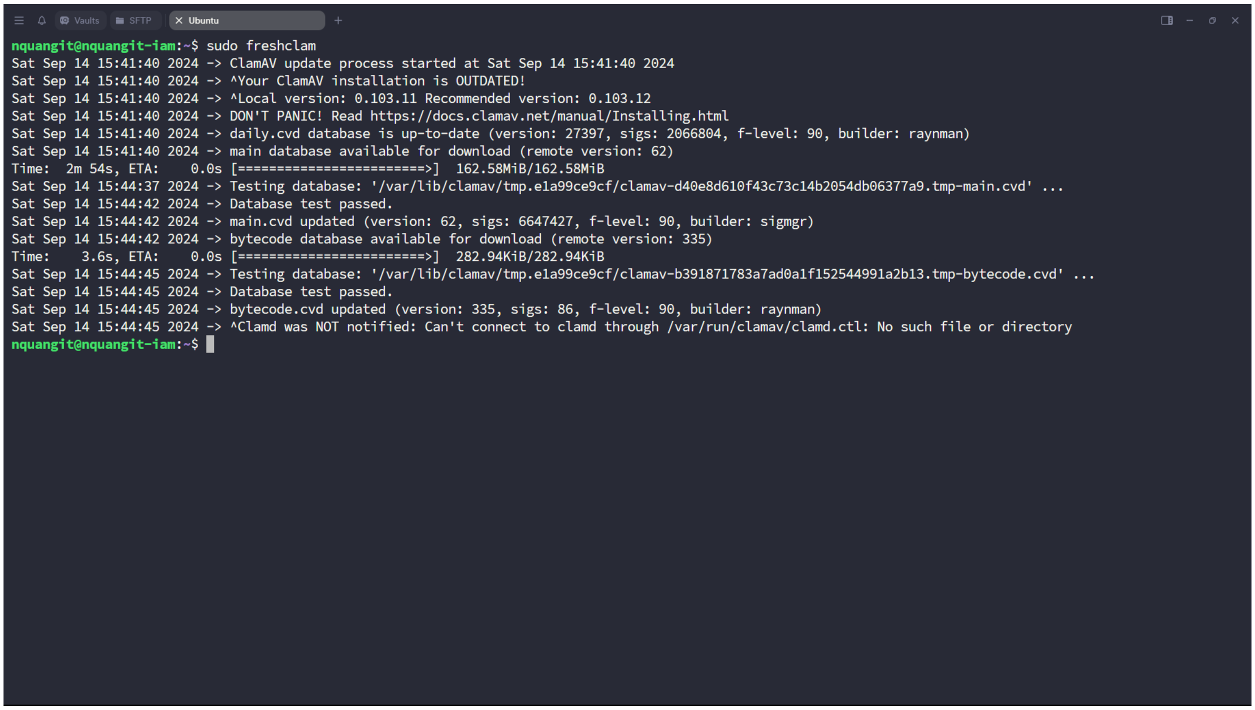


```
nquangit@nquangit-iam:~$ sudo systemctl stop clamav-freshclam
nquangit@nquangit-iam:~$
```

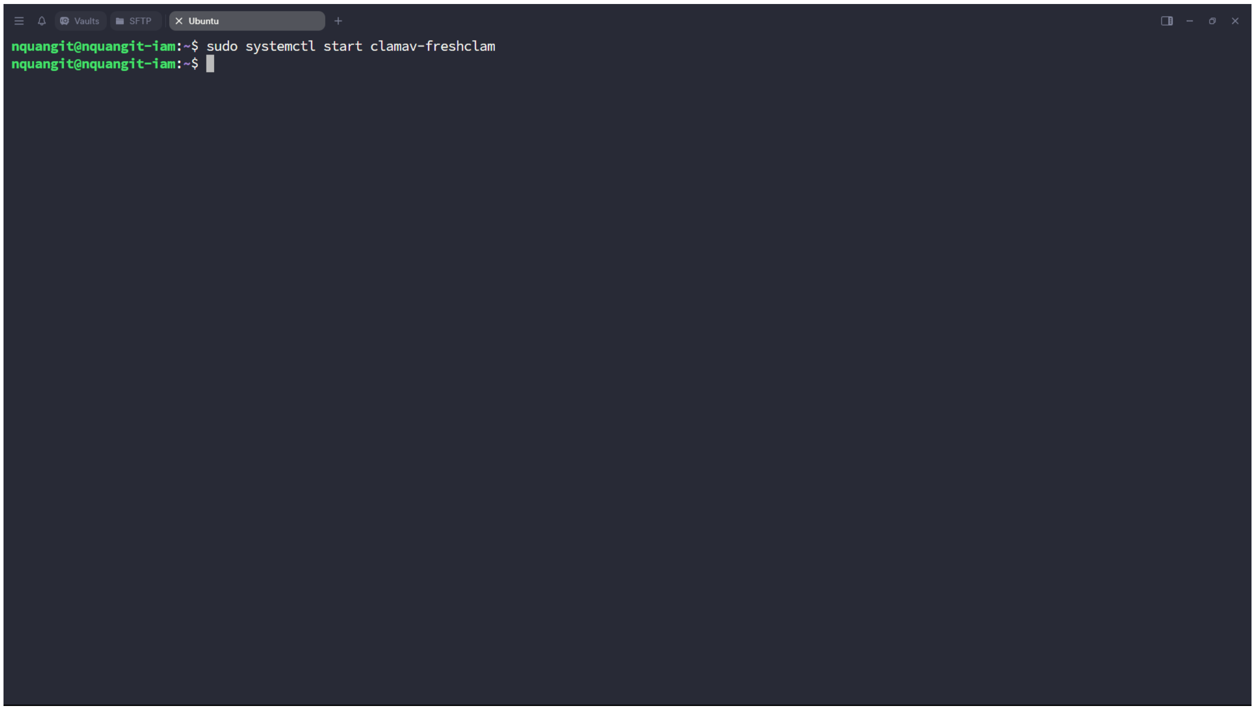
Download Updates Using freshclam (First Method)



```
nquangit@nquangit-iam:~$ sudo freshclam
Sat Sep 14 15:41:40 2024 -> ClamAV update process started at Sat Sep 14 15:41:40 2024
Sat Sep 14 15:41:40 2024 -> ^Your ClamAV installation is OUTDATED!
Sat Sep 14 15:41:40 2024 -> ^Local version: 0.103.11 Recommended version: 0.103.12
Sat Sep 14 15:41:40 2024 -> DON'T PANIC! Read https://docs.clamav.net/manual/Installing.html
Sat Sep 14 15:41:40 2024 -> daily.cvd database is up-to-date (version: 27397, sigs: 2066804, f-level: 90, builder: raynman)
Sat Sep 14 15:41:40 2024 -> main database available for download (remote version: 62)
Time:   11.0s, ETA:  2m 31s [=>                       ]   11.05MiB/162.58MiB
```



```
nquangit@nquangit-iam:~$ sudo freshclam
Sat Sep 14 15:41:40 2024 -> ClamAV update process started at Sat Sep 14 15:41:40 2024
Sat Sep 14 15:41:40 2024 -> ^Your ClamAV installation is OUTDATED!
Sat Sep 14 15:41:40 2024 -> ^Local version: 0.103.11 Recommended version: 0.103.12
Sat Sep 14 15:41:40 2024 -> DON'T PANIC! Read https://docs.clamav.net/manual/Installing.html
Sat Sep 14 15:41:40 2024 -> daily.cvd database is up-to-date (version: 27397, sigs: 2066804, f-level: 90, builder: raynman)
Sat Sep 14 15:41:40 2024 -> main database available for download (remote version: 62)
Time:  2m 54s, ETA:    0.0s [========================>]  162.58MiB/162.58MiB
Sat Sep 14 15:44:37 2024 -> Testing database: '/var/lib/clamav/tmp.e1a99ce9cf/clamav-d40e8d610f43c73c14b2054db06377a9.tmp-main.cvd' ...
Sat Sep 14 15:44:42 2024 -> Database test passed.
Sat Sep 14 15:44:42 2024 -> main.cvd updated (version: 62, sigs: 6647427, f-level: 90, builder: sigmgr)
Sat Sep 14 15:44:42 2024 -> bytecode database available for download (remote version: 335)
Time:    3.6s, ETA:    0.0s [========================>]  282.94KiB/282.94KiB
Sat Sep 14 15:44:45 2024 -> Testing database: '/var/lib/clamav/tmp.e1a99ce9cf/clamav-b391871783a7ad0a1f152544991a2b13.tmp-bytecode.cvd' ...
Sat Sep 14 15:44:45 2024 -> Database test passed.
Sat Sep 14 15:44:45 2024 -> bytecode.cvd updated (version: 335, sigs: 86, f-level: 90, builder: raynman)
Sat Sep 14 15:44:45 2024 -> ^Clamd was NOT notified: Can't connect to clamd through /var/run/clamav/clamd.ctl: No such file or directory
nquangit@nquangit-iam:~$
```

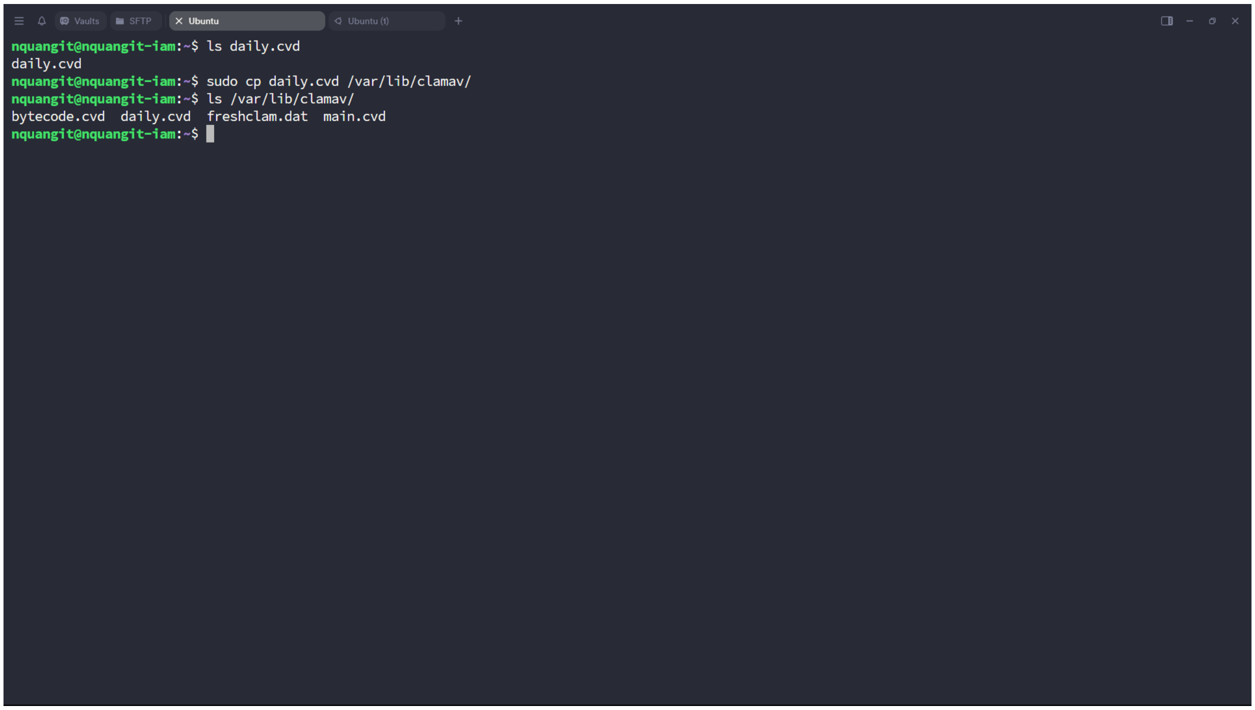


```
nquangit@nquangit-iam:~$ sudo systemctl start clamav-freshclam
nquangit@nquangit-iam:~$ 
```

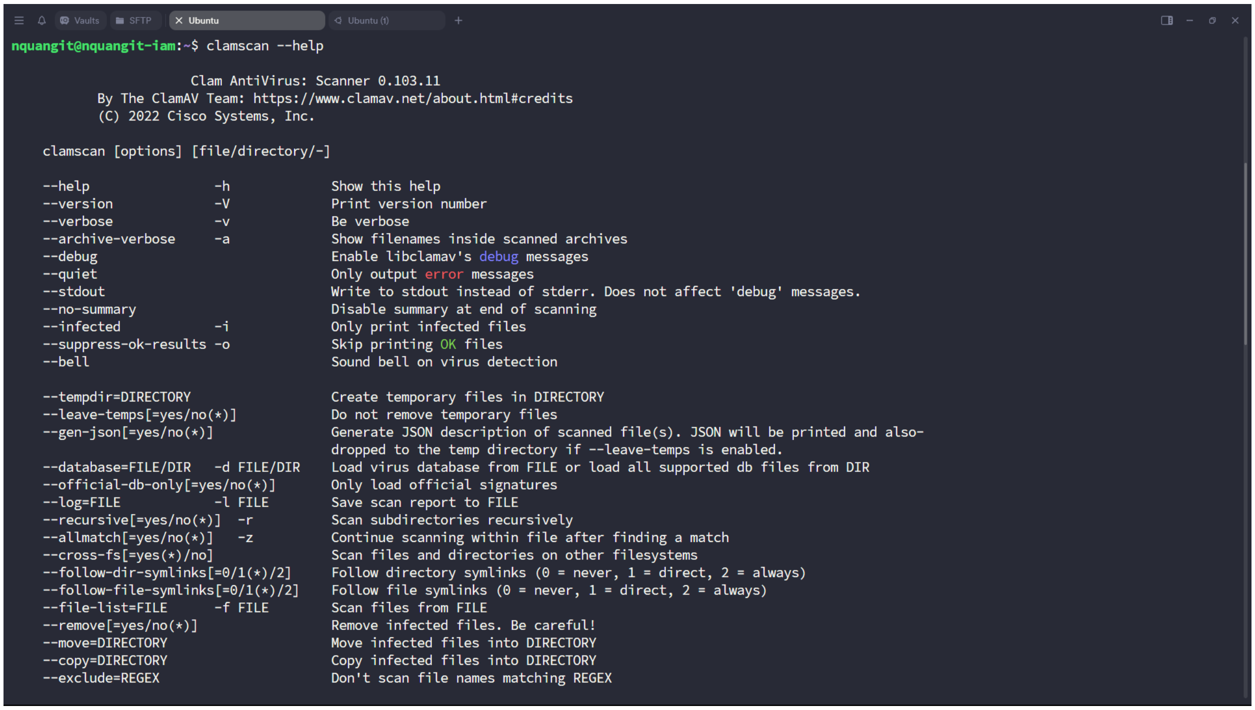
Download Updates Using Official Website (Second Method)

Another way is to download the “ClamAV” database from its official website https://database.clamav.net/daily.cvd

Then copy the “daily.cvd” file into the “var/lib/clamav” file through the copy command “cp”:

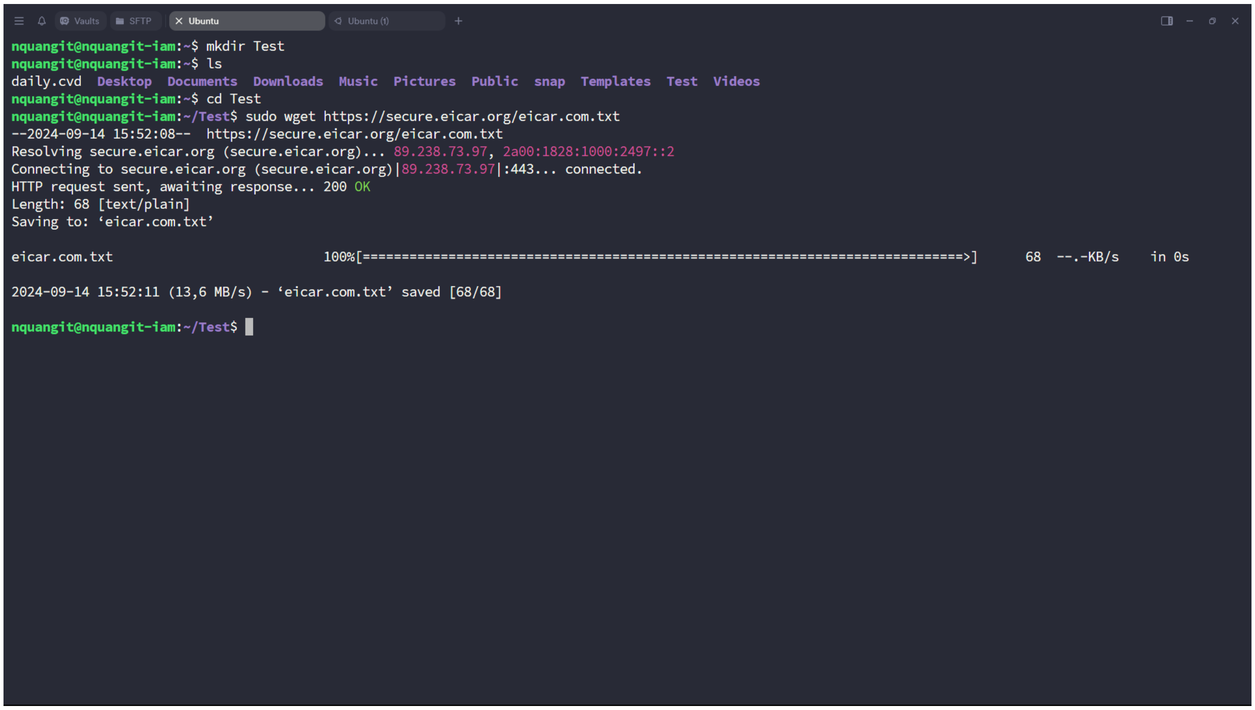


```
nquangit@nquangit-iam:~$ ls daily.cvd
daily.cvd
nquangit@nquangit-iam:~$ sudo cp daily.cvd /var/lib/clamav/
nquangit@nquangit-iam:~$ ls /var/lib/clamav/
bytecode.cvd  daily.cvd  freshclam.dat  main.cvd
nquangit@nquangit-iam:~$ 
```



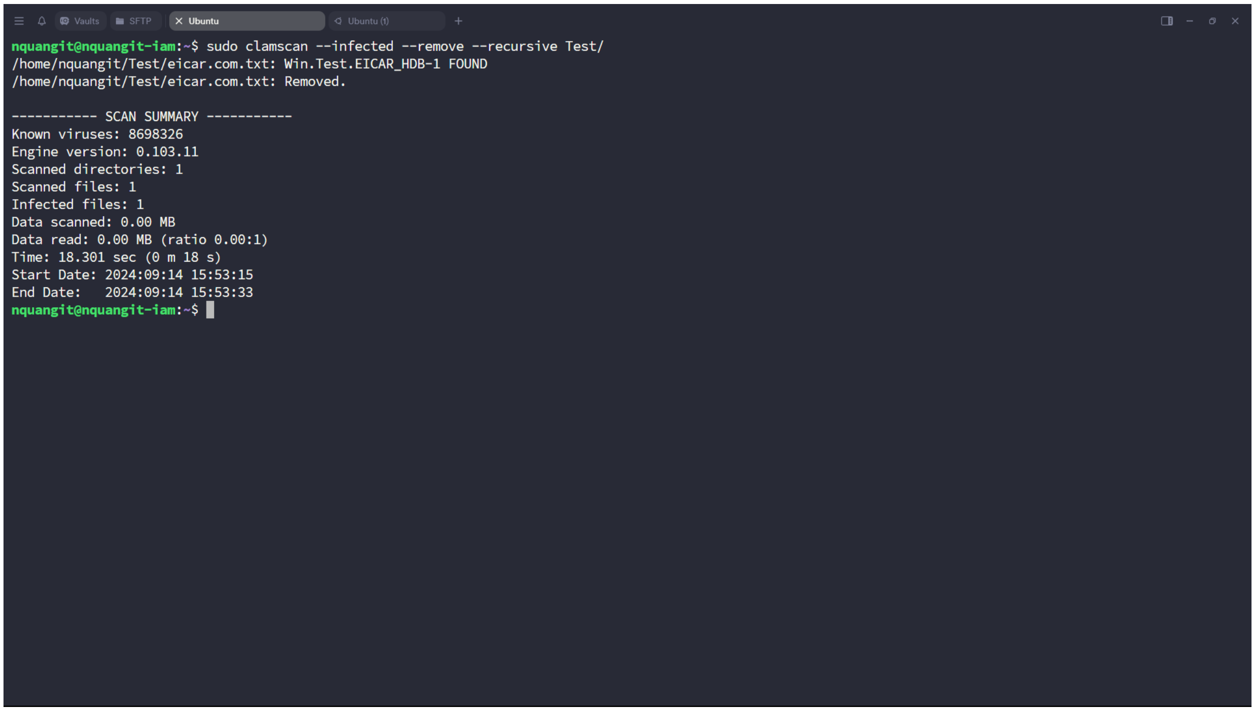
```
nquangit@nquangit-iam:~$ clamscan --help

                       Clam AntiVirus: Scanner 0.103.11
           By The ClamAV Team: https://www.clamav.net/about.html#credits
           (C) 2022 Cisco Systems, Inc.

    clamscan [options] [file/directory/-]

    --help                -h             Show this help
    --version             -V             Print version number
    --verbose             -v             Be verbose
    --archive-verbose     -a             Show filenames inside scanned archives
    --debug                              Enable libclamav's debug messages
    --quiet                              Only output error messages
    --stdout                             Write to stdout instead of stderr. Does not affect 'debug' messages.
    --no-summary                         Disable summary at end of scanning
    --infected            -i             Only print infected files
    --suppress-ok-results -o             Skip printing OK files
    --bell                               Sound bell on virus detection

    --tempdir=DIRECTORY                  Create temporary files in DIRECTORY
    --leave-temps[=yes/no(*)]            Do not remove temporary files
    --gen-json[=yes/no(*)]               Generate JSON description of scanned file(s). JSON will be printed and also-
                                         dropped to the temp directory if --leave-temps is enabled.
    --database=FILE/DIR   -d FILE/DIR    Load virus database from FILE or load all supported db files from DIR
    --official-db-only[=yes/no(*)]       Only load official signatures
    --log=FILE            -l FILE        Save scan report to FILE
    --recursive[=yes/no(*)]  -r          Scan subdirectories recursively
    --allmatch[=yes/no(*)]   -z          Continue scanning within file after finding a match
    --cross-fs[=yes(*)/no]               Scan files and directories on other filesystems
    --follow-dir-symlinks[=0/1(*)/2]     Follow directory symlinks (0 = never, 1 = direct, 2 = always)
    --follow-file-symlinks[=0/1(*)/2]    Follow file symlinks (0 = never, 1 = direct, 2 = always)
    --file-list=FILE      -f FILE        Scan files from FILE
    --remove[=yes/no(*)]                 Remove infected files. Be careful!
    --move=DIRECTORY                     Move infected files into DIRECTORY
    --copy=DIRECTORY                     Copy infected files into DIRECTORY
    --exclude=REGEX                      Don't scan file names matching REGEX
```

Scan a Directory

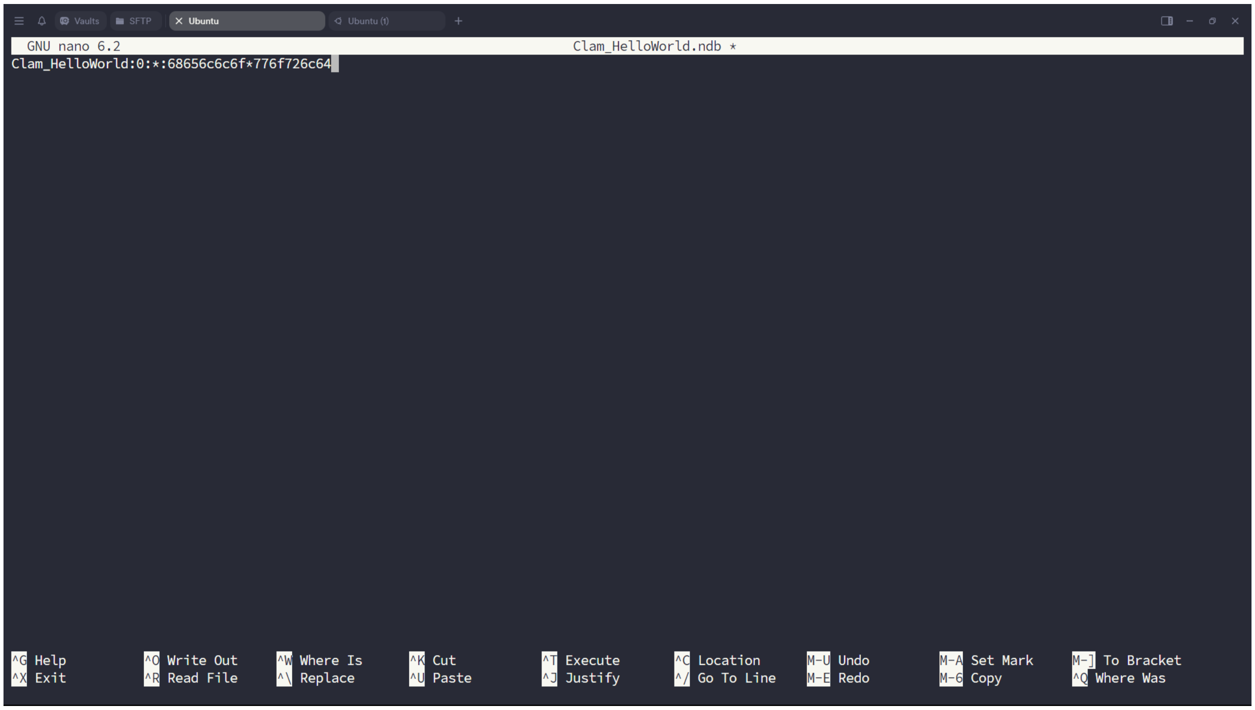


```
nquangit@nquangit-iam:~$ mkdir Test
nquangit@nquangit-iam:~$ ls
daily.cvd  Desktop  Documents  Downloads  Music  Pictures  Public  snap  Templates  Test  Videos
nquangit@nquangit-iam:~$ cd Test
nquangit@nquangit-iam:~/Test$ sudo wget https://secure.eicar.org/eicar.com.txt
--2024-09-14 15:52:08--  https://secure.eicar.org/eicar.com.txt
Resolving secure.eicar.org (secure.eicar.org)... 89.238.73.97, 2a00:1828:1000:2497::2
Connecting to secure.eicar.org (secure.eicar.org)|89.238.73.97|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 68 [text/plain]
Saving to: ‘eicar.com.txt’

eicar.com.txt                           100%[=============================================================================>]      68  --.-KB/s    in 0s

2024-09-14 15:52:11 (13,6 MB/s) - ‘eicar.com.txt’ saved [68/68]

nquangit@nquangit-iam:~/Test$ 
```

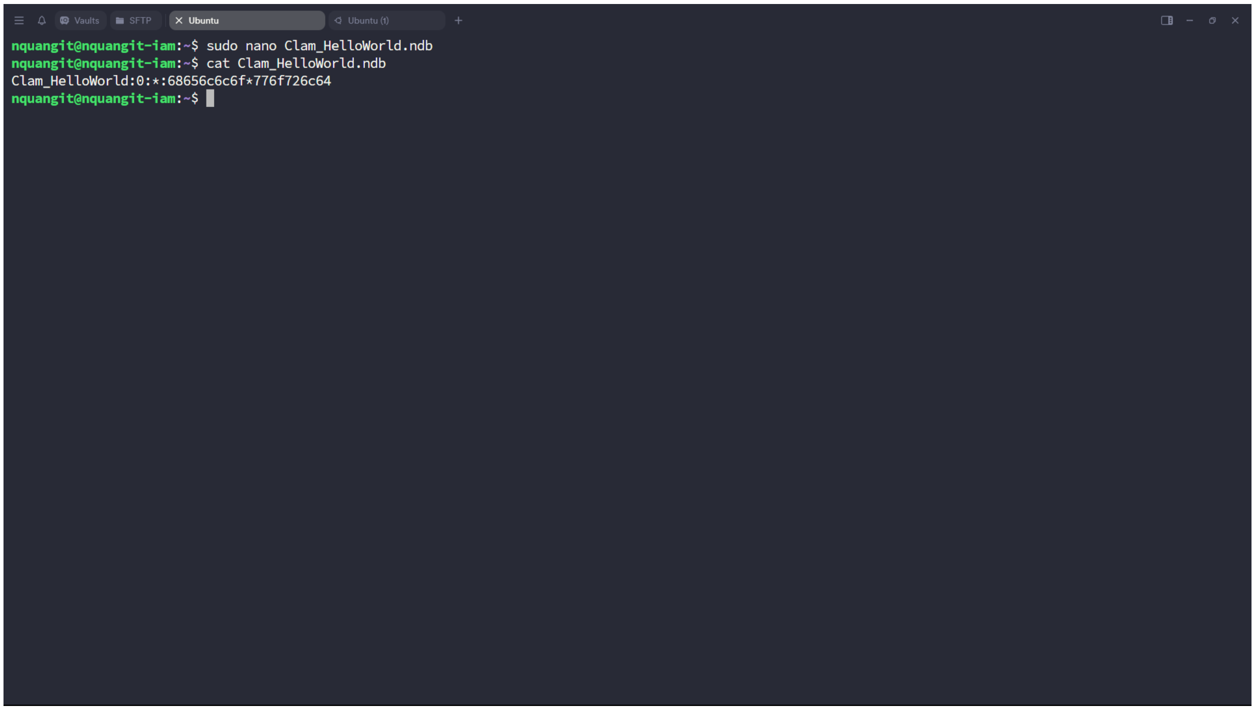
Scan a Directory



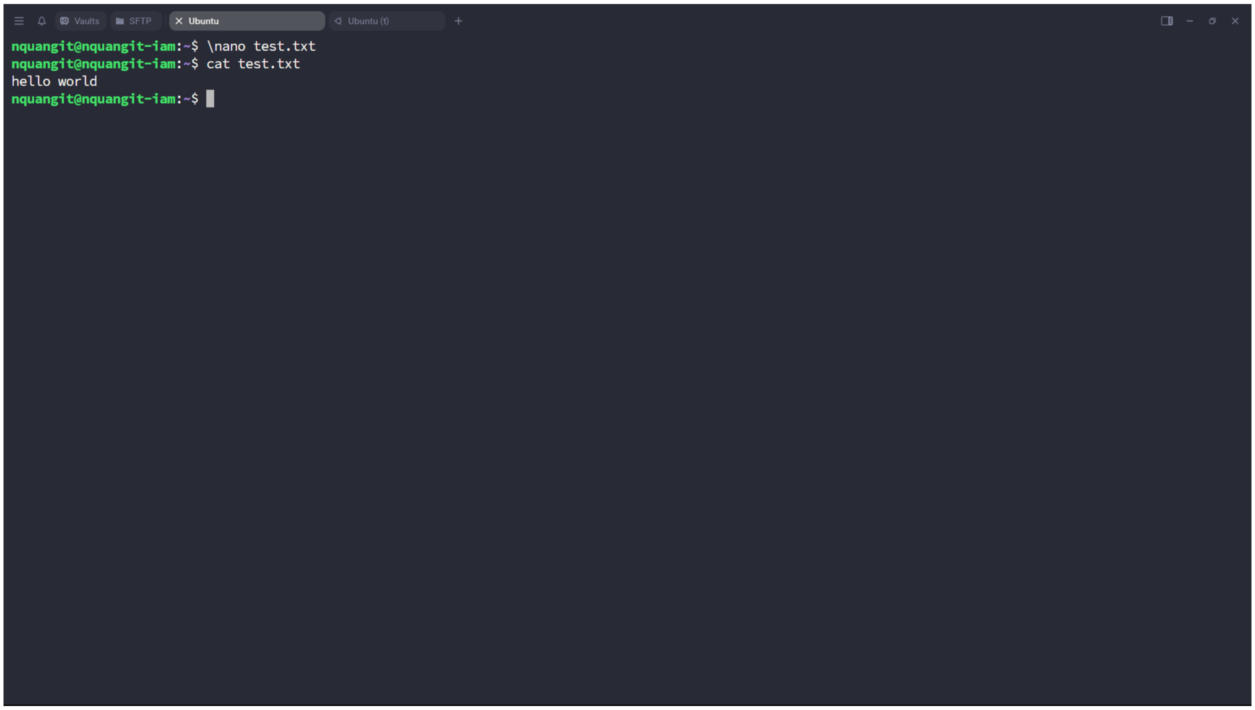
```
nquangit@nquangit-iam:~$ sudo clamscan --infected --remove --recursive Test/
/home/nquangit/Test/eicar.com.txt: Win.Test.EICAR_HDB-1 FOUND
/home/nquangit/Test/eicar.com.txt: Removed.

----------- SCAN SUMMARY -----------
Known viruses: 8698326
Engine version: 0.103.11
Scanned directories: 1
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 18.301 sec (0 m 18 s)
Start Date: 2024:09:14 15:53:15
End Date:   2024:09:14 15:53:33
nquangit@nquangit-iam:~$ 
```



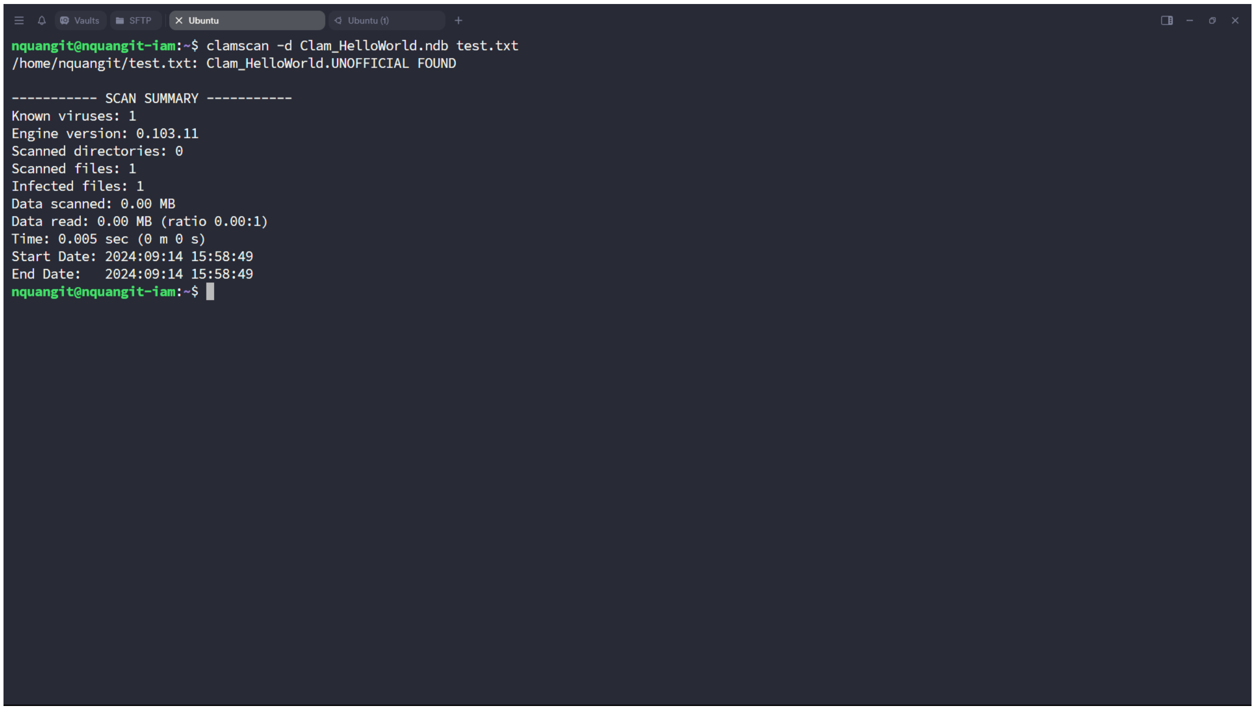
```
  GNU nano 6.2                                    Clam_HelloWorld.ndb *
Clam_HelloWorld:0:*:68656c6c6f*776f726c64
```



```
nquangit@nquangit-iam:~$ sudo nano Clam_HelloWorld.ndb
nquangit@nquangit-iam:~$ cat Clam_HelloWorld.ndb
Clam_HelloWorld:0:*:68656c6c6f*776f726c64
nquangit@nquangit-iam:~$ 
```



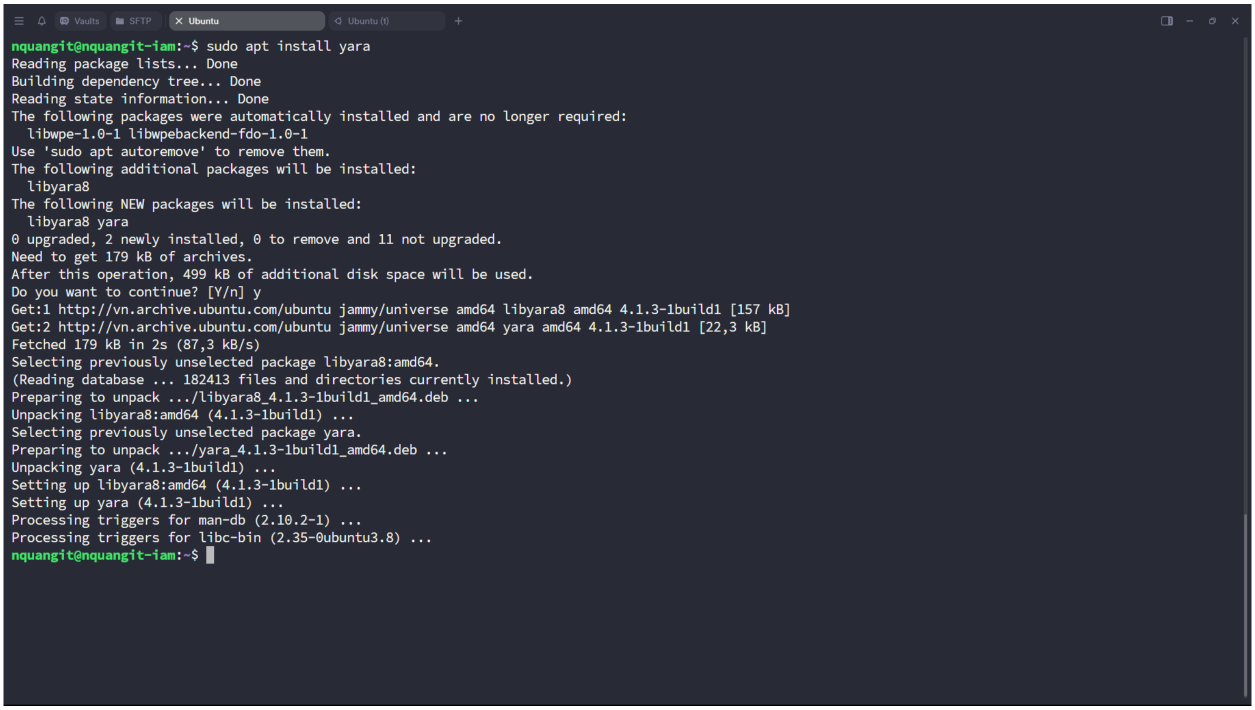
```
nquangit@nquangit-iam:~$ \nano test.txt
nquangit@nquangit-iam:~$ cat test.txt
hello world
nquangit@nquangit-iam:~$ 
```



```
nquangit@nquangit-iam:~$ clamscan -d Clam_HelloWorld.ndb test.txt
/home/nquangit/test.txt: Clam_HelloWorld.UNOFFICIAL FOUND

----------- SCAN SUMMARY -----------
Known viruses: 1
Engine version: 0.103.11
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 0.005 sec (0 m 0 s)
Start Date: 2024:09:14 15:58:49
End Date:   2024:09:14 15:58:49
nquangit@nquangit-iam:~$ 
```

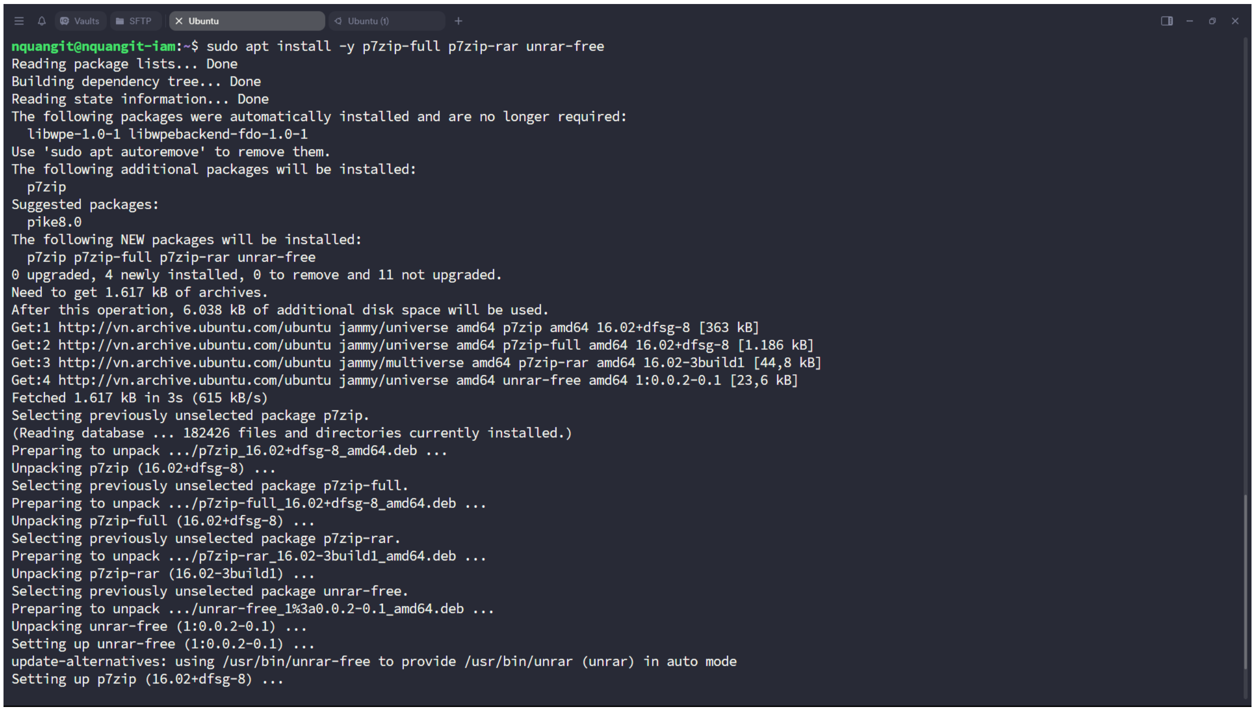
LAB 4:Detect Malware Capabilities with YARA

Install YARA

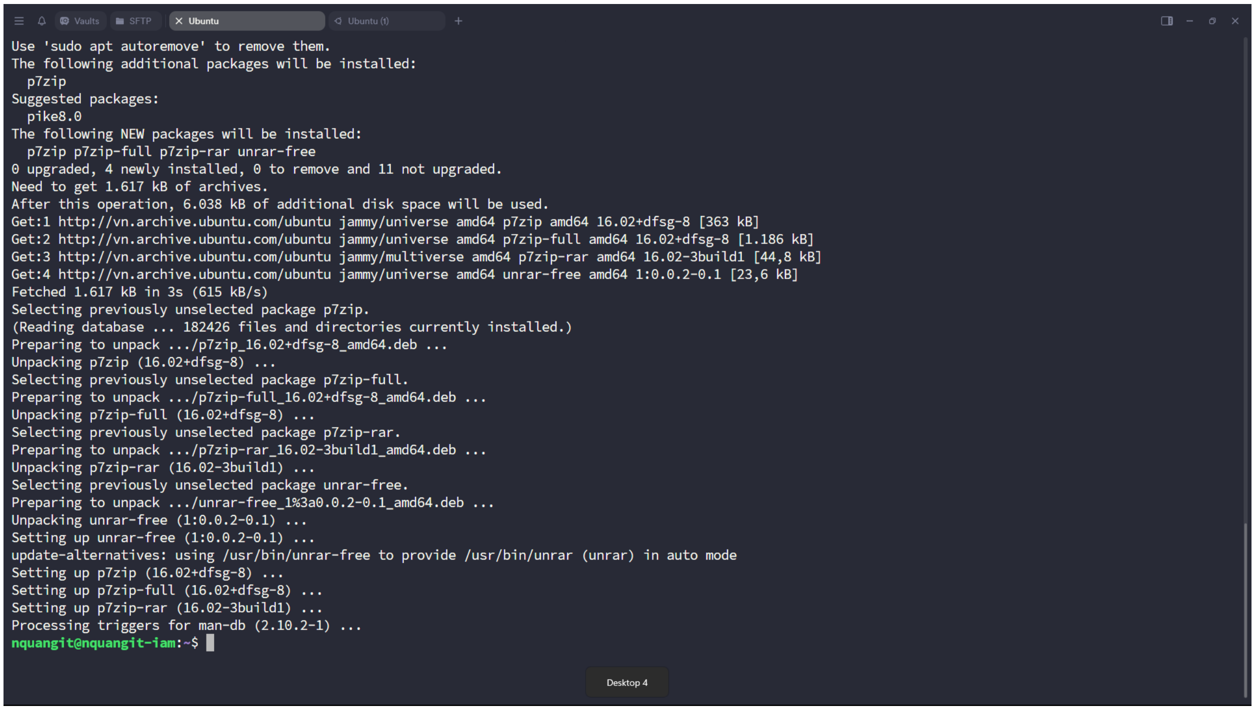


```
nquangit@nquangit-iam:~$ sudo apt install yara
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libwpe-1.0-1 libwpebackend-fdo-1.0-1
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libyara8
The following NEW packages will be installed:
  libyara8 yara
0 upgraded, 2 newly installed, 0 to remove and 11 not upgraded.
Need to get 179 kB of archives.
After this operation, 499 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://vn.archive.ubuntu.com/ubuntu jammy/universe amd64 libyara8 amd64 4.1.3-1build1 [157 kB]
Get:2 http://vn.archive.ubuntu.com/ubuntu jammy/universe amd64 yara amd64 4.1.3-1build1 [22,3 kB]
Fetched 179 kB in 2s (87,3 kB/s)
Selecting previously unselected package libyara8:amd64.
(Reading database ... 182413 files and directories currently installed.)
Preparing to unpack .../libyara8_4.1.3-1build1_amd64.deb ...
Unpacking libyara8:amd64 (4.1.3-1build1) ...
Selecting previously unselected package yara.
Preparing to unpack .../yara_4.1.3-1build1_amd64.deb ...
Unpacking yara (4.1.3-1build1) ...
Setting up libyara8:amd64 (4.1.3-1build1) ...
Setting up yara (4.1.3-1build1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.8) ...
nquangit@nquangit-iam:~$
```

Install p7zip-full:

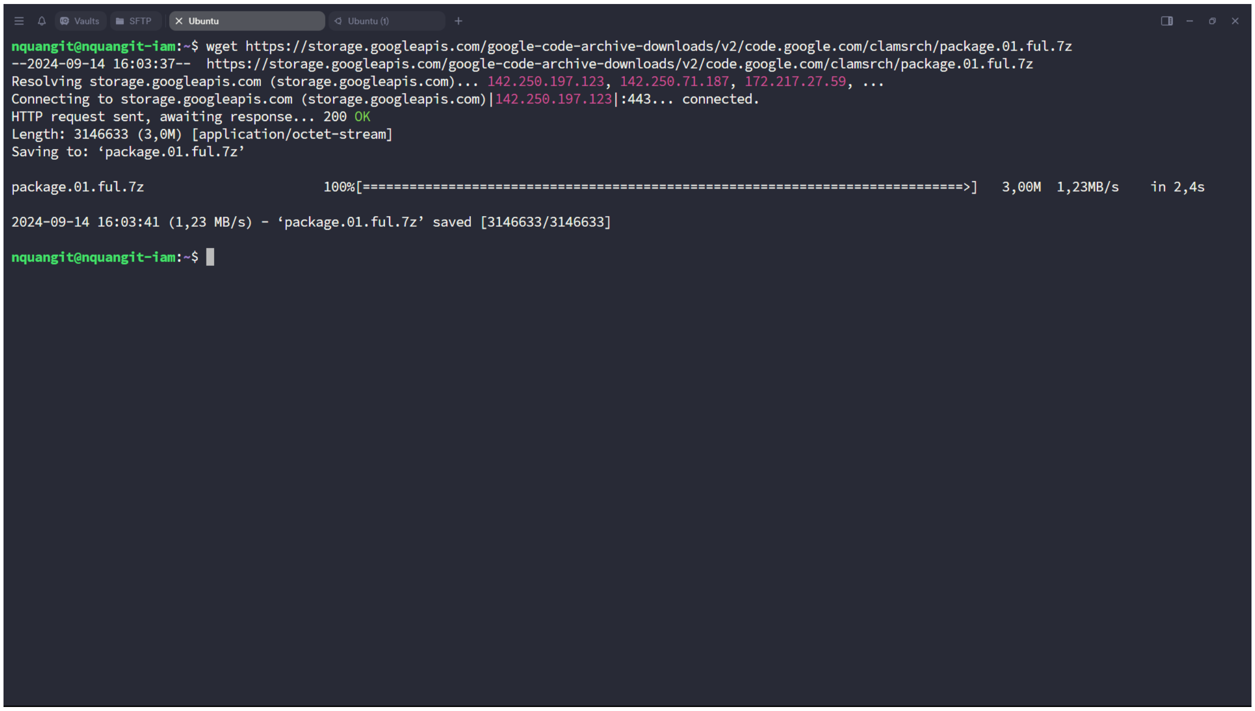


```
nquangit@nquangit-iam:~$ sudo apt install -y p7zip-full p7zip-rar unrar-free
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libwpe-1.0-1 libwpebackend-fdo-1.0-1
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  p7zip
Suggested packages:
  pike8.0
The following NEW packages will be installed:
  p7zip p7zip-full p7zip-rar unrar-free
0 upgraded, 4 newly installed, 0 to remove and 11 not upgraded.
Need to get 1.617 kB of archives.
After this operation, 6.038 kB of additional disk space will be used.
Get:1 http://vn.archive.ubuntu.com/ubuntu jammy/universe amd64 p7zip amd64 16.02+dfsg-8 [363 kB]
Get:2 http://vn.archive.ubuntu.com/ubuntu jammy/universe amd64 p7zip-full amd64 16.02+dfsg-8 [1.186 kB]
Get:3 http://vn.archive.ubuntu.com/ubuntu jammy/multiverse amd64 p7zip-rar amd64 16.02-3build1 [44,8 kB]
Get:4 http://vn.archive.ubuntu.com/ubuntu jammy/universe amd64 unrar-free amd64 1:0.0.2-0.1 [23,6 kB]
Fetched 1.617 kB in 3s (615 kB/s)
Selecting previously unselected package p7zip.
(Reading database ... 182426 files and directories currently installed.)
Preparing to unpack .../p7zip_16.02+dfsg-8_amd64.deb ...
Unpacking p7zip (16.02+dfsg-8) ...
Selecting previously unselected package p7zip-full.
Preparing to unpack .../p7zip-full_16.02+dfsg-8_amd64.deb ...
Unpacking p7zip-full (16.02+dfsg-8) ...
Selecting previously unselected package p7zip-rar.
Preparing to unpack .../p7zip-rar_16.02-3build1_amd64.deb ...
Unpacking p7zip-rar (16.02-3build1) ...
Selecting previously unselected package unrar-free.
Preparing to unpack .../unrar-free_1%3a0.0.2-0.1_amd64.deb ...
Unpacking unrar-free (1:0.0.2-0.1) ...
Setting up unrar-free (1:0.0.2-0.1) ...
update-alternatives: using /usr/bin/unrar-free to provide /usr/bin/unrar (unrar) in auto mode
Setting up p7zip (16.02+dfsg-8) ...
```



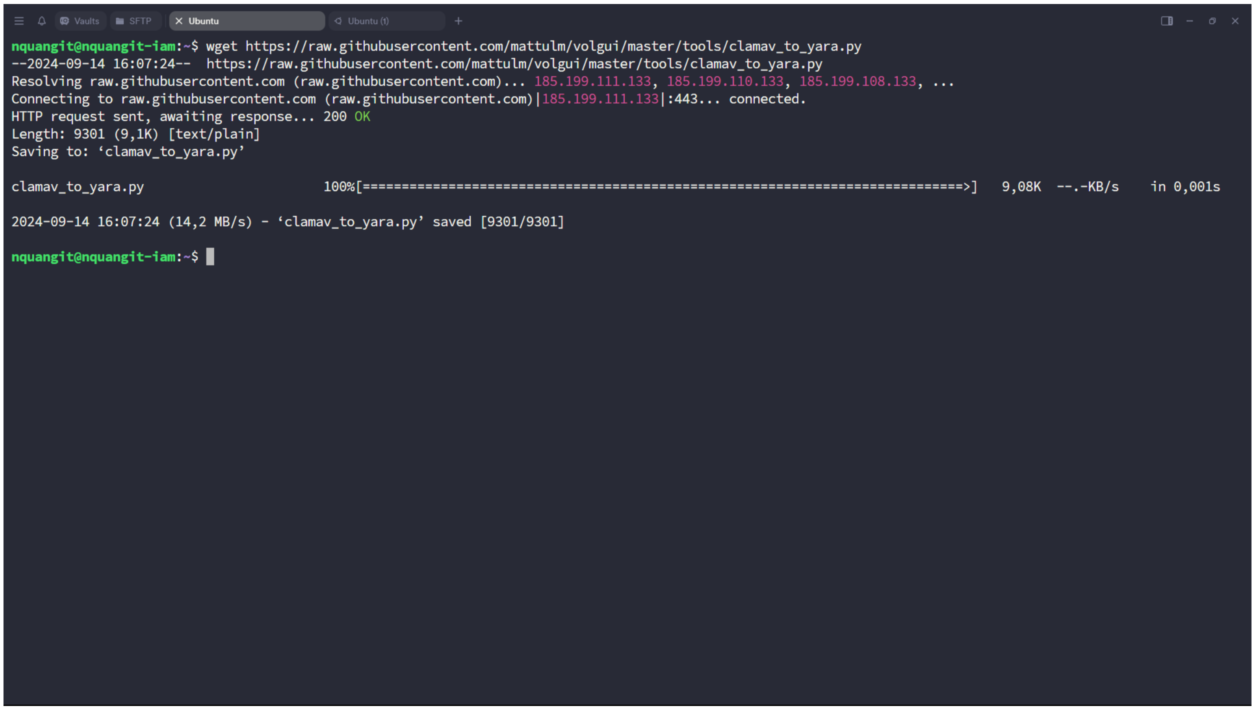
```
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  p7zip
Suggested packages:
  pike8.0
The following NEW packages will be installed:
  p7zip p7zip-full p7zip-rar unrar-free
0 upgraded, 4 newly installed, 0 to remove and 11 not upgraded.
Need to get 1.617 kB of archives.
After this operation, 6.038 kB of additional disk space will be used.
Get:1 http://vn.archive.ubuntu.com/ubuntu jammy/universe amd64 p7zip amd64 16.02+dfsg-8 [363 kB]
Get:2 http://vn.archive.ubuntu.com/ubuntu jammy/universe amd64 p7zip-full amd64 16.02+dfsg-8 [1.186 kB]
Get:3 http://vn.archive.ubuntu.com/ubuntu jammy/multiverse amd64 p7zip-rar amd64 16.02-3build1 [44,8 kB]
Get:4 http://vn.archive.ubuntu.com/ubuntu jammy/universe amd64 unrar-free amd64 1:0.0.2-0.1 [23,6 kB]
Fetched 1.617 kB in 3s (615 kB/s)
Selecting previously unselected package p7zip.
(Reading database ... 182426 files and directories currently installed.)
Preparing to unpack .../p7zip_16.02+dfsg-8_amd64.deb ...
Unpacking p7zip (16.02+dfsg-8) ...
Selecting previously unselected package p7zip-full.
Preparing to unpack .../p7zip-full_16.02+dfsg-8_amd64.deb ...
Unpacking p7zip-full (16.02+dfsg-8) ...
Selecting previously unselected package p7zip-rar.
Preparing to unpack .../p7zip-rar_16.02-3build1_amd64.deb ...
Unpacking p7zip-rar (16.02-3build1) ...
Selecting previously unselected package unrar-free.
Preparing to unpack .../unrar-free_1%3a0.0.2-0.1_amd64.deb ...
Unpacking unrar-free (1:0.0.2-0.1) ...
Setting up unrar-free (1:0.0.2-0.1) ...
update-alternatives: using /usr/bin/unrar-free to provide /usr/bin/unrar (unrar) in auto mode
Setting up p7zip (16.02+dfsg-8) ...
Setting up p7zip-full (16.02+dfsg-8) ...
Setting up p7zip-rar (16.02-3build1) ...
Processing triggers for man-db (2.10.2-1) ...
nquangit@nquangit-iam:~$ 
```

Download package.01.ful.7z:



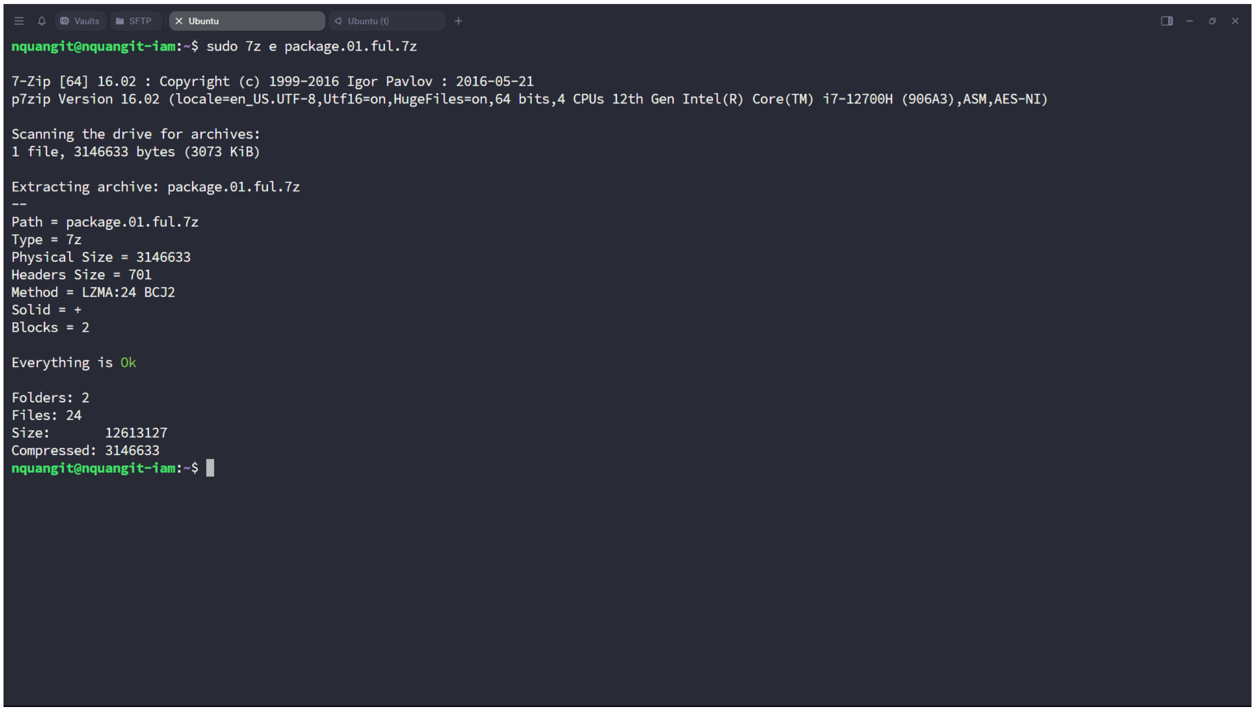
```
nquangit@nquangit-iam:~$ wget https://storage.googleapis.com/google-code-archive-downloads/v2/code.google.com/clamsrch/package.01.ful.7z
--2024-09-14 16:03:37--  https://storage.googleapis.com/google-code-archive-downloads/v2/code.google.com/clamsrch/package.01.ful.7z
Resolving storage.googleapis.com (storage.googleapis.com)... 142.250.197.123, 142.250.71.187, 172.217.27.59, ...
Connecting to storage.googleapis.com (storage.googleapis.com)|142.250.197.123|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3146633 (3,0M) [application/octet-stream]
Saving to: ‘package.01.ful.7z’

package.01.ful.7z                  100%[=============================================================================>]   3,00M  1,23MB/s    in 2,4s

2024-09-14 16:03:41 (1,23 MB/s) - ‘package.01.ful.7z’ saved [3146633/3146633]

nquangit@nquangit-iam:~$ 
```

Download file clam_to_yara.py:



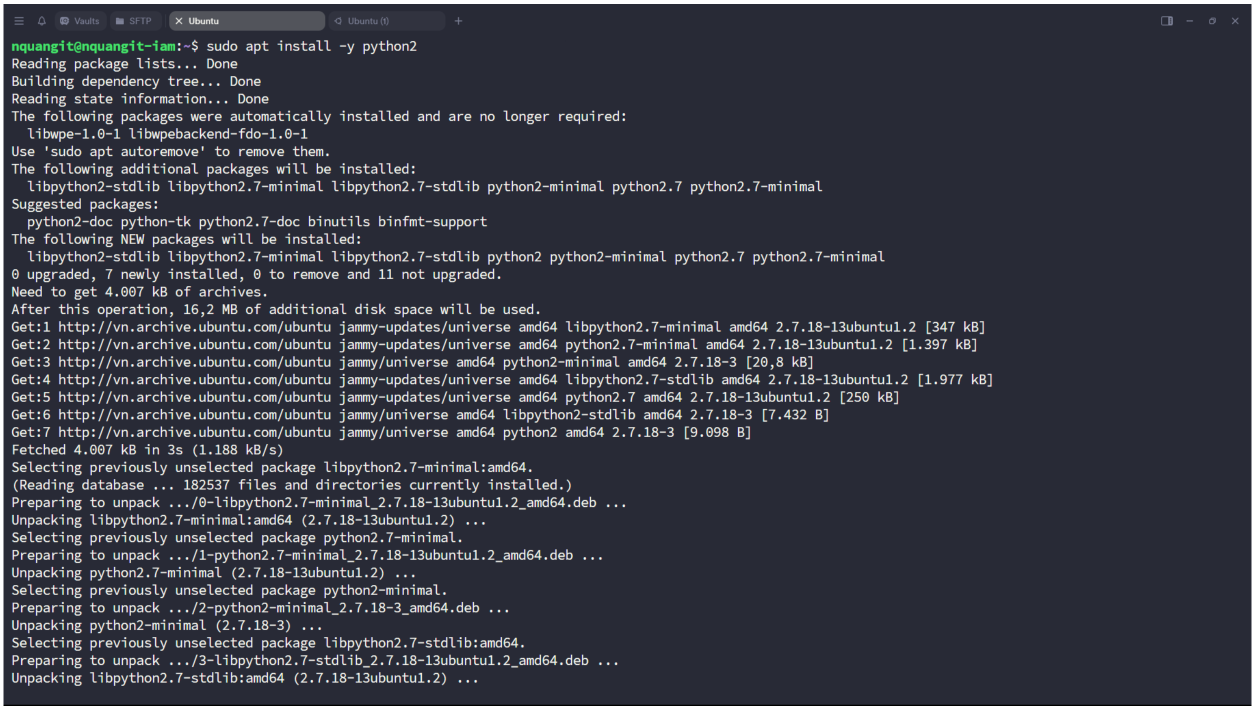
```
nquangit@nquangit-iam:~$ wget https://raw.githubusercontent.com/mattulm/volgui/master/tools/clamav_to_yara.py
--2024-09-14 16:07:24--  https://raw.githubusercontent.com/mattulm/volgui/master/tools/clamav_to_yara.py
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.111.133, 185.199.110.133, 185.199.108.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9301 (9,1K) [text/plain]
Saving to: ‘clamav_to_yara.py’

clamav_to_yara.py                       100%[=============================================================================>]   9,08K  --.-KB/s    in 0,001s

2024-09-14 16:07:24 (14,2 MB/s) - ‘clamav_to_yara.py’ saved [9301/9301]

nquangit@nquangit-iam:~$ 
```

Convert file clamav sang yara:

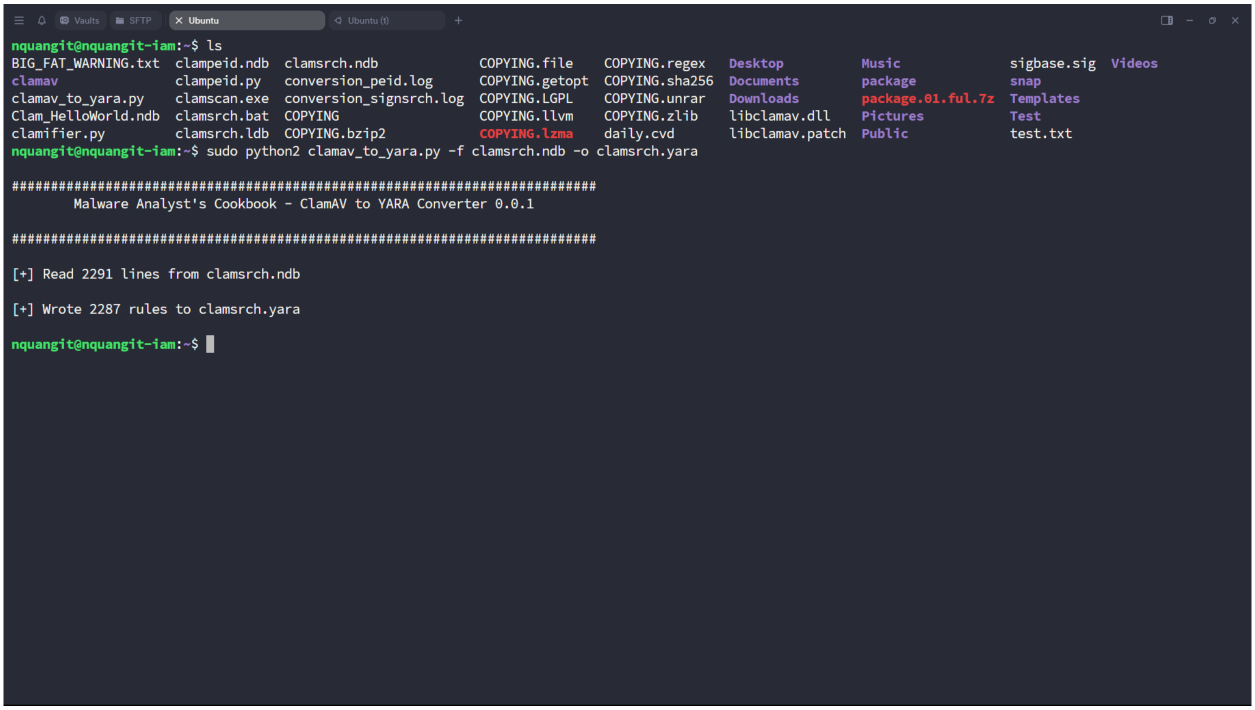


```
nquangit@nquangit-iam:~$ sudo 7z e package.01.ful.7z

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,4 CPUs 12th Gen Intel(R) Core(TM) i7-12700H (906A3),ASM,AES-NI)

Scanning the drive for archives:
1 file, 3146633 bytes (3073 KiB)

Extracting archive: package.01.ful.7z
--
Path = package.01.ful.7z
Type = 7z
Physical Size = 3146633
Headers Size = 701
Method = LZMA:24 BCJ2
Solid = +
Blocks = 2

Everything is Ok

Folders: 2
Files: 24
Size:       12613127
Compressed: 3146633
nquangit@nquangit-iam:~$ 
```

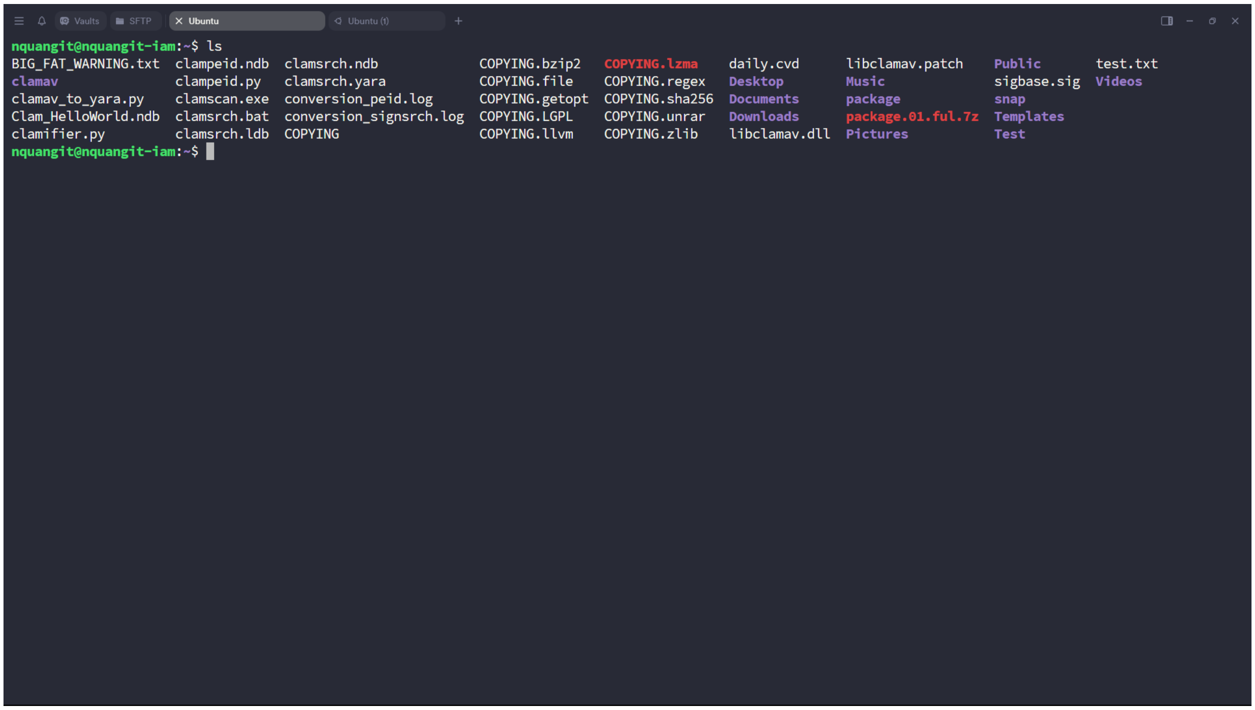
Install python2



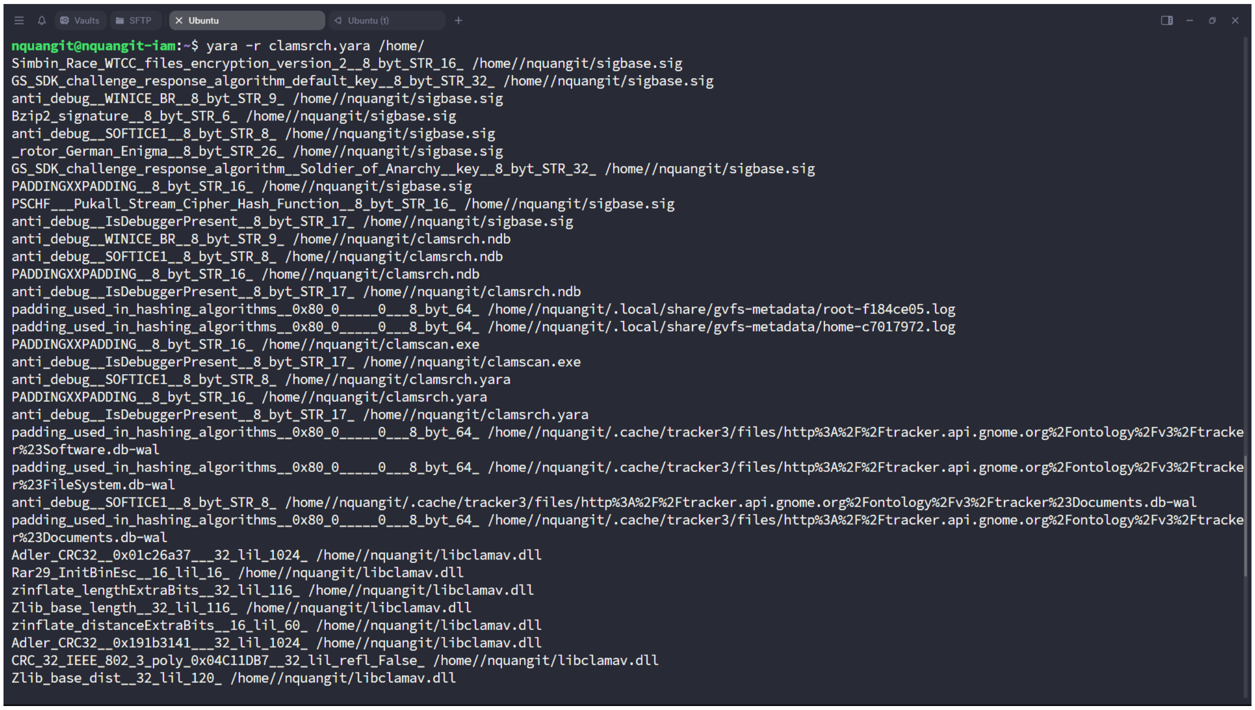
```
nquangit@nquangit-iam:~$ sudo apt install -y python2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libwpe-1.0-1 libwpebackend-fdo-1.0-1
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libpython2-stdlib libpython2.7-minimal libpython2.7-stdlib python2-minimal python2.7 python2.7-minimal
Suggested packages:
  python2-doc python-tk python2.7-doc binutils binfmt-support
The following NEW packages will be installed:
  libpython2-stdlib libpython2.7-minimal libpython2.7-stdlib python2 python2-minimal python2.7 python2.7-minimal
0 upgraded, 7 newly installed, 0 to remove and 11 not upgraded.
Need to get 4.007 kB of archives.
After this operation, 16,2 MB of additional disk space will be used.
Get:1 http://vn.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 libpython2.7-minimal amd64 2.7.18-13ubuntu1.2 [347 kB]
Get:2 http://vn.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 python2.7-minimal amd64 2.7.18-13ubuntu1.2 [1.397 kB]
Get:3 http://vn.archive.ubuntu.com/ubuntu jammy/universe amd64 python2-minimal amd64 2.7.18-3 [20,8 kB]
Get:4 http://vn.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 libpython2.7-stdlib amd64 2.7.18-13ubuntu1.2 [1.977 kB]
Get:5 http://vn.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 python2.7 amd64 2.7.18-13ubuntu1.2 [250 kB]
Get:6 http://vn.archive.ubuntu.com/ubuntu jammy/universe amd64 libpython2-stdlib amd64 2.7.18-3 [7.432 B]
Get:7 http://vn.archive.ubuntu.com/ubuntu jammy/universe amd64 python2 amd64 2.7.18-3 [9.098 B]
Fetched 4.007 kB in 3s (1.188 kB/s)
Selecting previously unselected package libpython2.7-minimal:amd64.
(Reading database ... 182537 files and directories currently installed.)
Preparing to unpack .../0-libpython2.7-minimal_2.7.18-13ubuntu1.2_amd64.deb ...
Unpacking libpython2.7-minimal:amd64 (2.7.18-13ubuntu1.2) ...
Selecting previously unselected package python2.7-minimal.
Preparing to unpack .../1-python2.7-minimal_2.7.18-13ubuntu1.2_amd64.deb ...
Unpacking python2.7-minimal (2.7.18-13ubuntu1.2) ...
Selecting previously unselected package python2-minimal.
Preparing to unpack .../2-python2-minimal_2.7.18-3_amd64.deb ...
Unpacking python2-minimal (2.7.18-3) ...
Selecting previously unselected package libpython2.7-stdlib:amd64.
Preparing to unpack .../3-libpython2.7-stdlib_2.7.18-13ubuntu1.2_amd64.deb ...
Unpacking libpython2.7-stdlib:amd64 (2.7.18-13ubuntu1.2) ...
```



```
nquangit@nquangit-iam:~$ ls
BIG_FAT_WARNING.txt  clampeid.ndb  clamsrch.ndb             COPYING.file    COPYING.regex   Desktop         Music              sigbase.sig  Videos
clamav               clampeid.py   conversion_peid.log      COPYING.getopt  COPYING.sha256  Documents       package            snap
clamav_to_yara.py    clamscan.exe  conversion_signsrch.log  COPYING.LGPL    COPYING.unrar   Downloads       package.01.ful.7z  Templates
Clam_HelloWorld.ndb  clamsrch.bat  COPYING                  COPYING.llvm    COPYING.zlib    libclamav.dll   Pictures           Test
clamifier.py         clamsrch.ldb  COPYING.bzip2            COPYING.lzma    daily.cvd       libclamav.patch Public             test.txt
nquangit@nquangit-iam:~$ sudo python2 clamav_to_yara.py -f clamsrch.ndb -o clamsrch.yara

###########################################################################
        Malware Analyst's Cookbook - ClamAV to YARA Converter 0.0.1

###########################################################################

[+] Read 2291 lines from clamsrch.ndb

[+] Wrote 2287 rules to clamsrch.yara

nquangit@nquangit-iam:~$
```

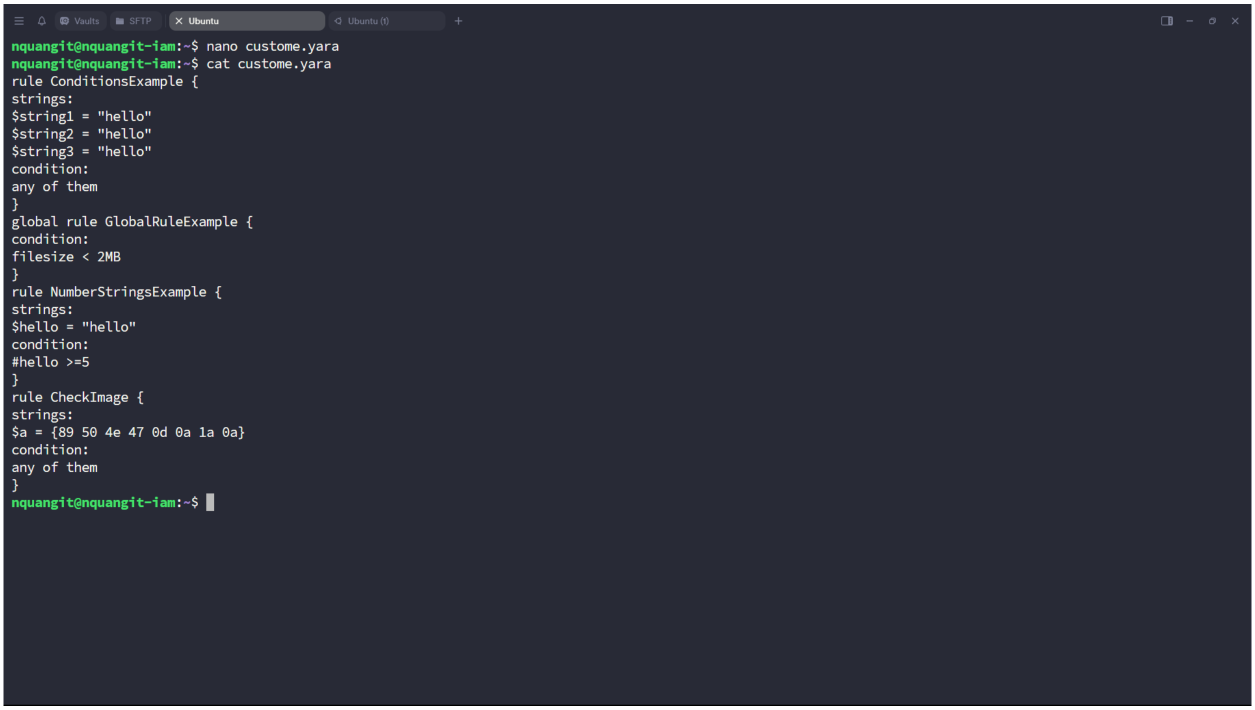


```
nquangit@nquangit-iam:~$ ls
BIG_FAT_WARNING.txt  clampeid.ndb  clamsrch.ndb             COPYING.bzip2   COPYING.lzma    daily.cvd      libclamav.patch    Public       test.txt
clamav               clampeid.py   clamsrch.yara            COPYING.file    COPYING.regex   Desktop        Music              sigbase.sig  Videos
clamav_to_yara.py    clamscan.exe  conversion_peid.log      COPYING.getopt  COPYING.sha256  Documents      package            snap
Clam_HelloWorld.ndb  clamsrch.bat  conversion_signsrch.log  COPYING.LGPL    COPYING.unrar   Downloads      package.01.ful.7z  Templates
clamifier.py         clamsrch.ldb  COPYING                  COPYING.llvm    COPYING.zlib    libclamav.dll  Pictures           Test
nquangit@nquangit-iam:~$
```



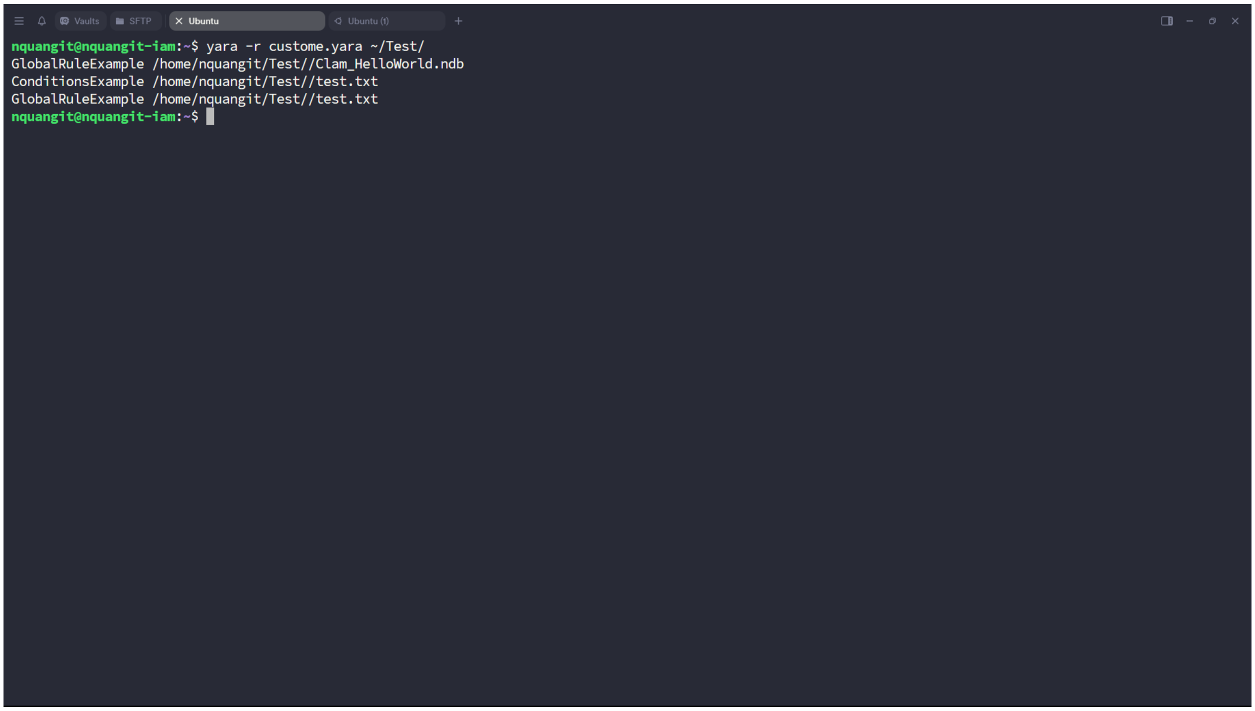
```
nquangit@nquangit-iam:~$ yara -r clamsrch.yara /home/
Simbin_Race_WTCC_files_encryption_version_2__8_byt_STR_16_ /home//nquangit/sigbase.sig
GS_SDK_challenge_response_algorithm_default_key__8_byt_STR_32_ /home//nquangit/sigbase.sig
anti_debug__WINICE_BR__8_byt_STR_9_ /home//nquangit/sigbase.sig
Bzip2_signature__8_byt_STR_6_ /home//nquangit/sigbase.sig
anti_debug__SOFTICE1__8_byt_STR_8_ /home//nquangit/sigbase.sig
_rotor_German_Enigma__8_byt_STR_26_ /home//nquangit/sigbase.sig
GS_SDK_challenge_response_algorithm__Soldier_of_Anarchy__key__8_byt_STR_32_ /home//nquangit/sigbase.sig
PADDINGXXPADDING__8_byt_STR_16_ /home//nquangit/sigbase.sig
PSCHF___Pukall_Stream_Cipher_Hash_Function__8_byt_STR_16_ /home//nquangit/sigbase.sig
anti_debug__IsDebuggerPresent__8_byt_STR_17_ /home//nquangit/sigbase.sig
anti_debug__WINICE_BR__8_byt_STR_9_ /home//nquangit/clamsrch.ndb
anti_debug__SOFTICE1__8_byt_STR_8_ /home//nquangit/clamsrch.ndb
PADDINGXXPADDING__8_byt_STR_16_ /home//nquangit/clamsrch.ndb
anti_debug__IsDebuggerPresent__8_byt_STR_17_ /home//nquangit/clamsrch.ndb
padding_used_in_hashing_algorithms__0x80_0_____0___8_byt_64_ /home//nquangit/.local/share/gvfs-metadata/root-f184ce05.log
padding_used_in_hashing_algorithms__0x80_0_____0___8_byt_64_ /home//nquangit/.local/share/gvfs-metadata/home-c7017972.log
PADDINGXXPADDING__8_byt_STR_16_ /home//nquangit/clamscan.exe
anti_debug__IsDebuggerPresent__8_byt_STR_17_ /home//nquangit/clamscan.exe
anti_debug__SOFTICE1__8_byt_STR_8_ /home//nquangit/clamsrch.yara
PADDINGXXPADDING__8_byt_STR_16_ /home//nquangit/clamsrch.yara
anti_debug__IsDebuggerPresent__8_byt_STR_17_ /home//nquangit/clamsrch.yara
padding_used_in_hashing_algorithms__0x80_0_____0___8_byt_64_ /home//nquangit/.cache/tracker3/files/http%3A%2F%2Ftracker.api.gnome.org%2Fontology%2Fv3%2Ftracke
r%23Software.db-wal
padding_used_in_hashing_algorithms__0x80_0_____0___8_byt_64_ /home//nquangit/.cache/tracker3/files/http%3A%2F%2Ftracker.api.gnome.org%2Fontology%2Fv3%2Ftracke
r%23FileSystem.db-wal
anti_debug__SOFTICE1__8_byt_STR_8_ /home//nquangit/.cache/tracker3/files/http%3A%2F%2Ftracker.api.gnome.org%2Fontology%2Fv3%2Ftracker%23Documents.db-wal
padding_used_in_hashing_algorithms__0x80_0_____0___8_byt_64_ /home//nquangit/.cache/tracker3/files/http%3A%2F%2Ftracker.api.gnome.org%2Fontology%2Fv3%2Ftracke
r%23Documents.db-wal
Adler_CRC32__0x01c26a37___32_lil_1024_ /home//nquangit/libclamav.dll
Rar29_InitBinEsc__16_lil_16_ /home//nquangit/libclamav.dll
zinflate_lengthExtraBits__32_lil_116_ /home//nquangit/libclamav.dll
Zlib_base_length__32_lil_116_ /home//nquangit/libclamav.dll
zinflate_distanceExtraBits__16_lil_60_ /home//nquangit/libclamav.dll
Adler_CRC32__0x191b3141___32_lil_1024_ /home//nquangit/libclamav.dll
CRC_32_IEEE_802_3_poly_0x04C11DB7__32_lil_refl_False_ /home//nquangit/libclamav.dll
Zlib_base_dist__32_lil_120_ /home//nquangit/libclamav.dll
```

Create a new rule file called custome.yara



```
nquangit@nquangit-iam:~$ nano custome.yara
nquangit@nquangit-iam:~$ cat custome.yara
rule ConditionsExample {
strings:
$string1 = "hello"
$string2 = "hello"
$string3 = "hello"
condition:
any of them
}
global rule GlobalRuleExample {
condition:
filesize < 2MB
}
rule NumberStringsExample {
strings:
$hello = "hello"
condition:
#hello >=5
}
rule CheckImage {
strings:
$a = {89 50 4e 47 0d 0a 1a 0a}
condition:
any of them
}
nquangit@nquangit-iam:~$
```

Test yara rules:



```
nquangit@nquangit-iam:~$ yara -r custome.yara ~/Test/
GlobalRuleExample /home/nquangit/Test//Clam_HelloWorld.ndb
ConditionsExample /home/nquangit/Test//test.txt
GlobalRuleExample /home/nquangit/Test//test.txt
nquangit@nquangit-iam:~$
```