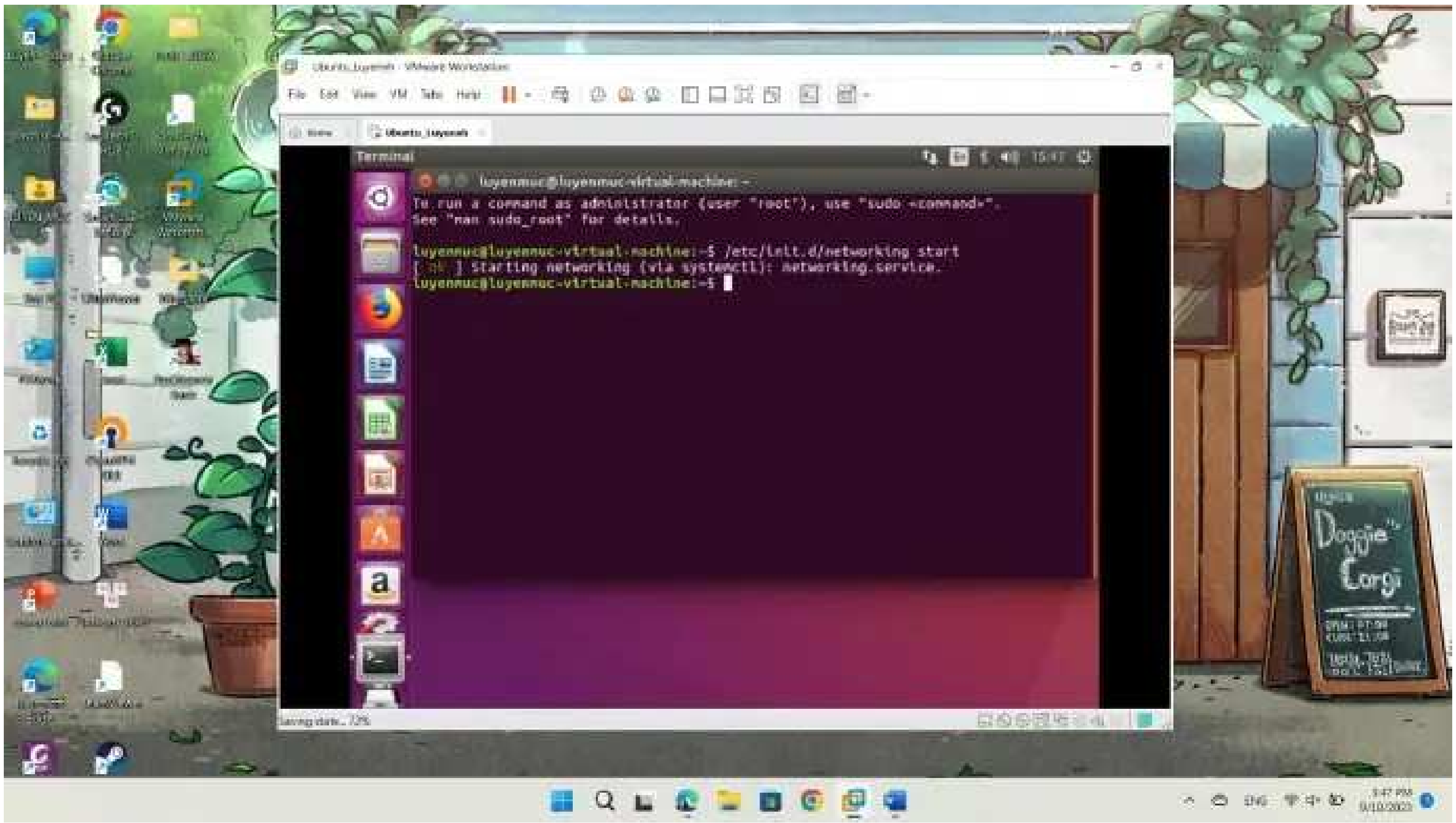
LAB 4

Nguyễn Hồng Luyến_SE172617

Lab 4.1

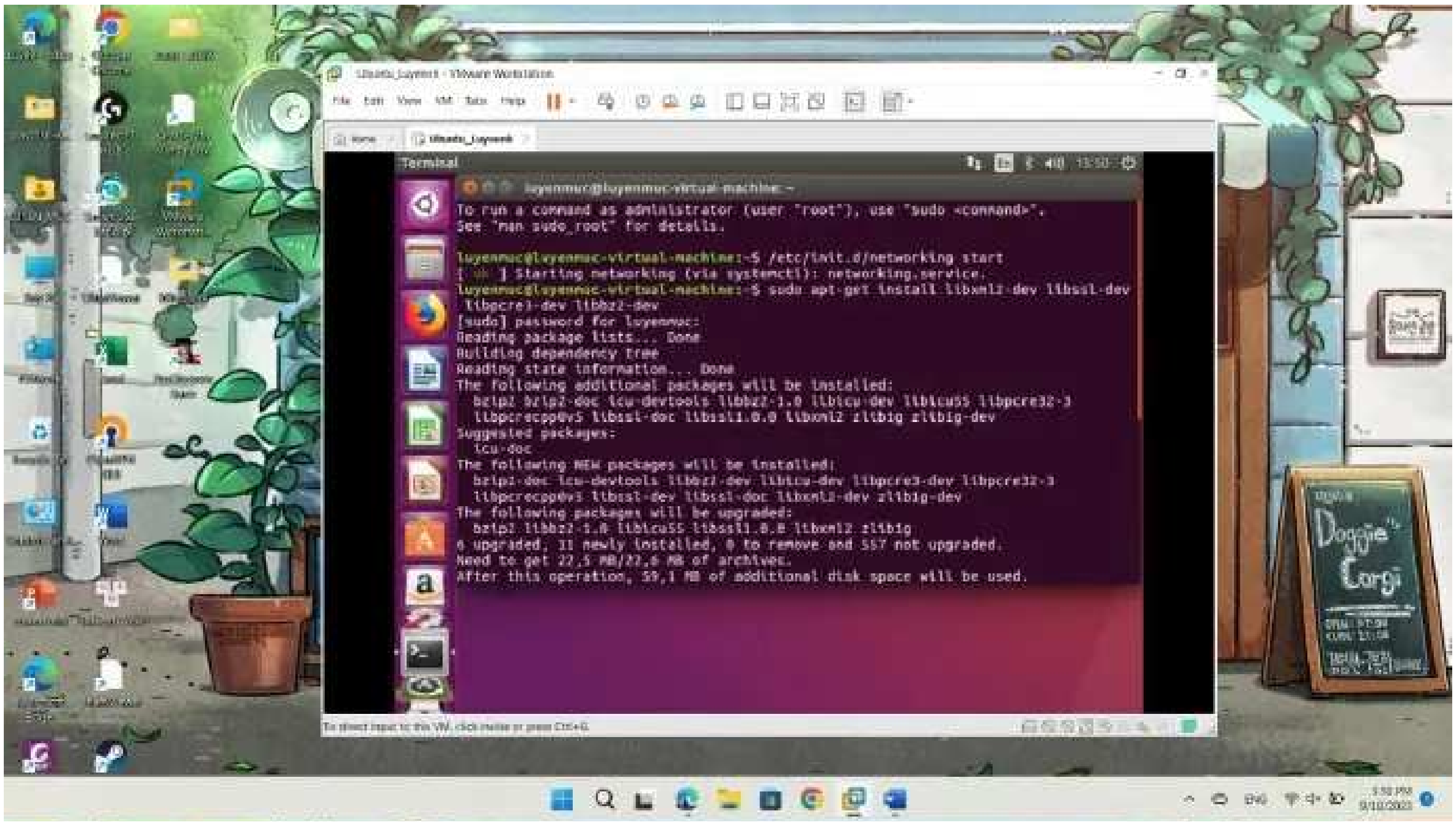
Khởi động card mạng trong ubuntu lại trong máy ảo:



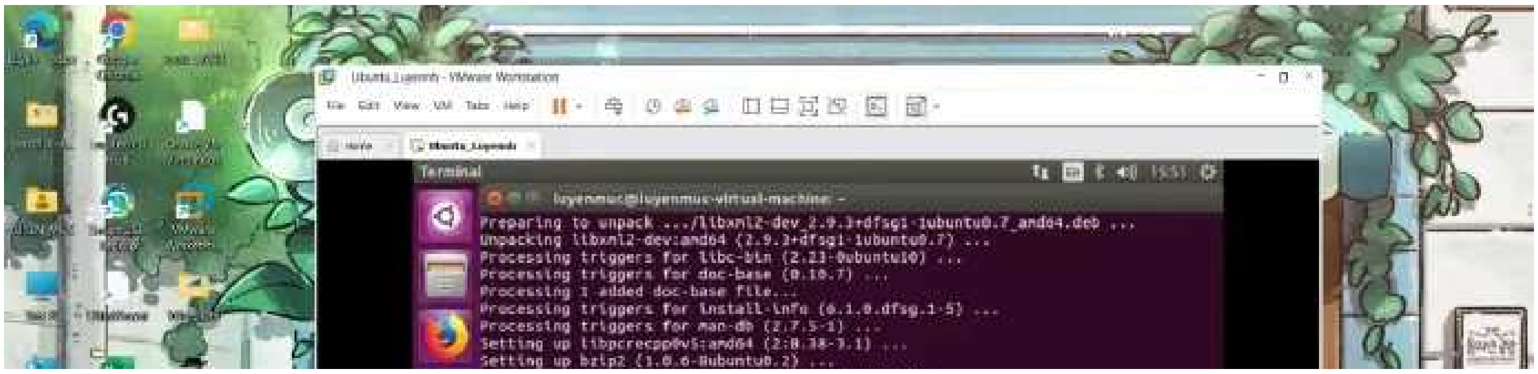
```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

luyenmuc@luyenmuc-virtual-machine:~$ /etc/init.d/networking start
[ ok ] Starting networking (via systemctl): networking.service.
luyenmuc@luyenmuc-virtual-machine:~$ 
```

Ubuntu_Luyenmh - VMware Workstation
File
Edit
View
VM
Tabs
Help
Home
Ubuntu_Luyenmh
Terminal
luyenmuc@luyenmuc-virtual-machine: ~

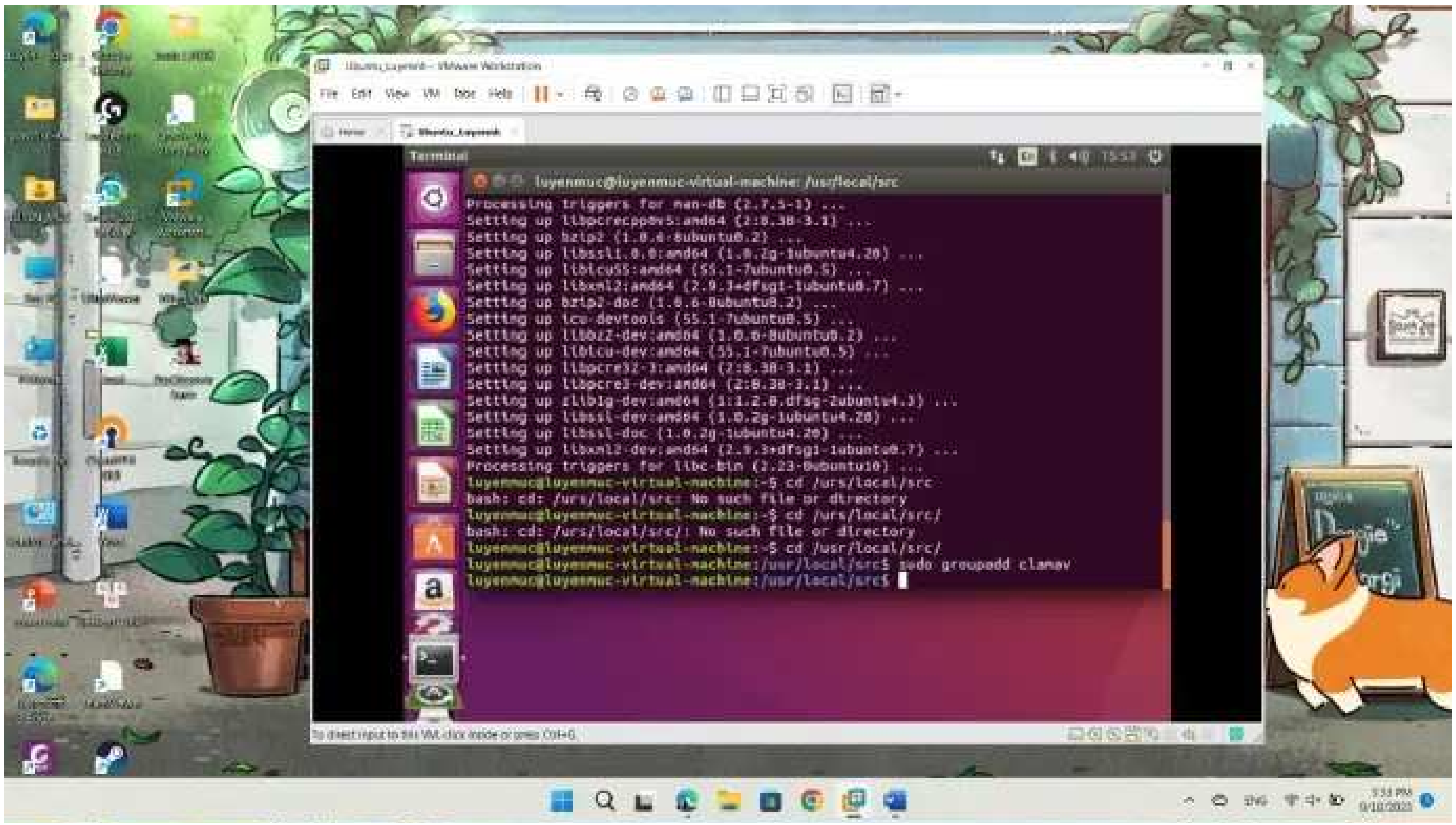
Cập nhật và cài các thư viện cần thiết cho cài đặt ClamAV:



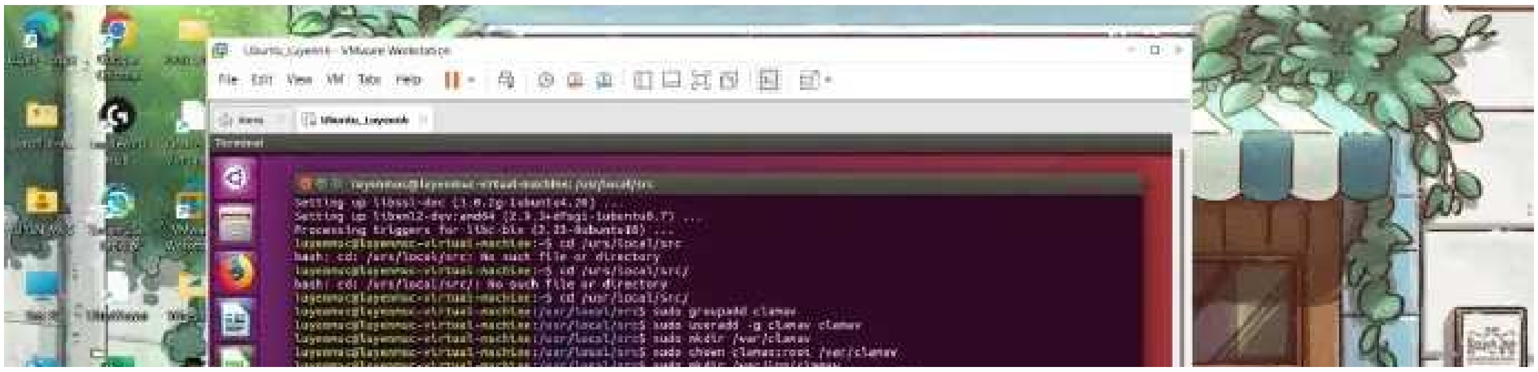
```
luyenmuc@luyenmuc-virtual-machine: ~
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

luyenmuc@luyenmuc-virtual-machine:~$ /etc/init.d/networking start
[ ok ] Starting networking (via systemctl): networking.service.
luyenmuc@luyenmuc-virtual-machine:~$ sudo apt-get install libxml2-dev libssl-dev
 libpcre3-dev libbz2-dev
[sudo] password for luyenmuc:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  bzip2 bzip2-doc icu-devtools libbz2-1.0 libicu-dev libicu55 libpcre32-3
  libpcrecpp0v5 libssl-doc libssl1.0.0 libxml2 zlib1g zlib1g-dev
Suggested packages:
  icu-doc
The following NEW packages will be installed:
  bzip2-doc icu-devtools libbz2-dev libicu-dev libpcre3-dev libpcre32-3
  libpcrecpp0v5 libssl-dev libssl-doc libxml2-dev zlib1g-dev
The following packages will be upgraded:
  bzip2 libbz2-1.0 libicu55 libssl1.0.0 libxml2 zlib1g
6 upgraded, 11 newly installed, 0 to remove and 557 not upgraded.
Need to get 22,5 MB/22,6 MB of archives.
After this operation, 59,1 MB of additional disk space will be used.
```



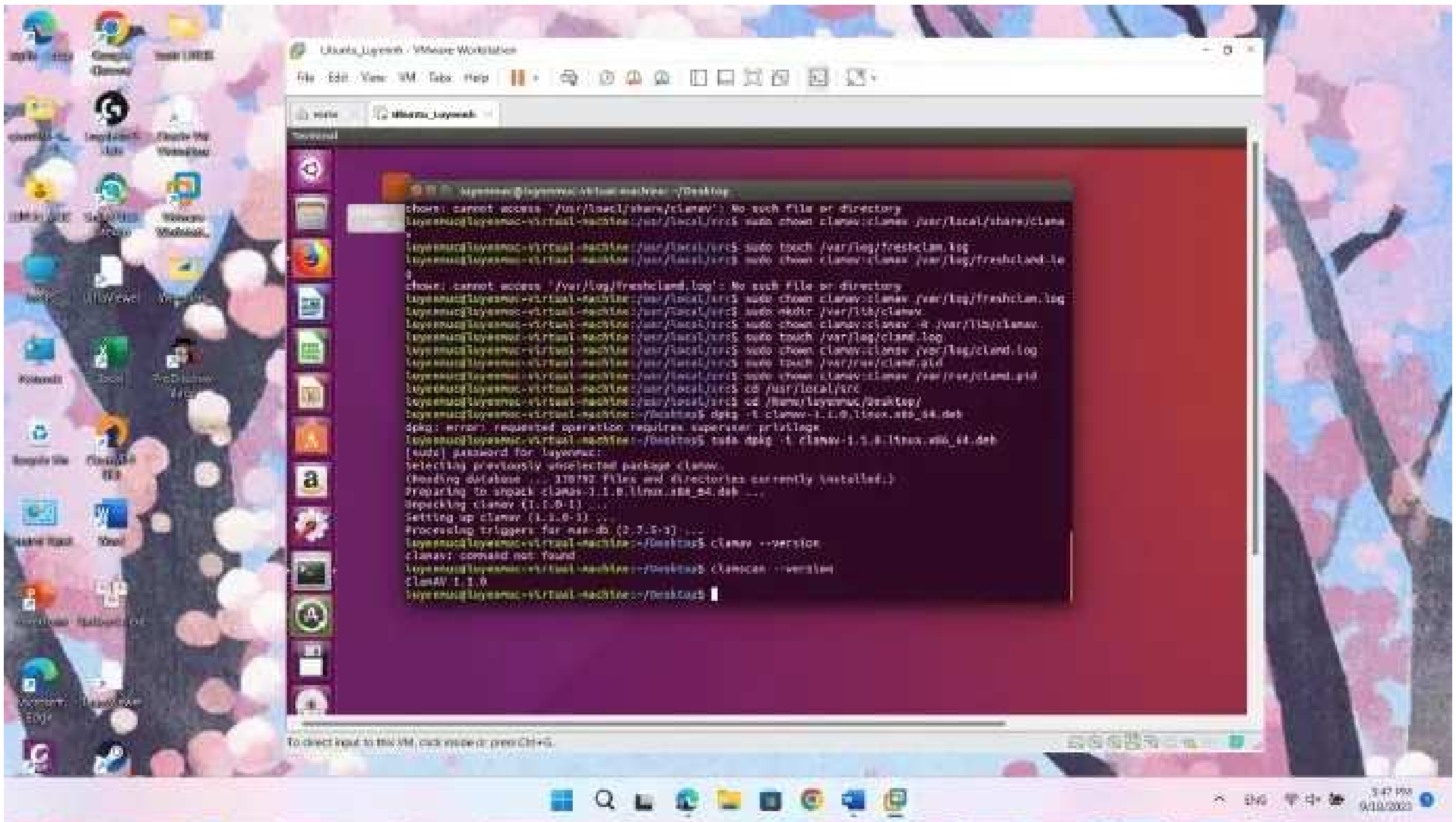
```
luyenmuc@luyenmuc-virtual-machine: ~
Preparing to unpack .../libxml2-dev_2.9.3+dfsg1-1ubuntu0.7_amd64.deb ...
Unpacking libxml2-dev:amd64 (2.9.3+dfsg1-1ubuntu0.7) ...
Processing triggers for libc-bin (2.23-0ubuntu10) ...
Processing triggers for doc-base (0.10.7) ...
Processing 1 added doc-base file...
Processing triggers for install-info (6.1.0.dfsg.1-5) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up libpcrecpp0v5:amd64 (2:8.38-3.1) ...
Setting up bzip2 (1.0.6-0ubuntu0.2) ...
```


Ubuntu_Luyenmk - VMware Workstation
File Edit View VM Tabs Help
Home
Ubuntu_Luyenmk
Terminal
15:53
luyenmuc@luyenmuc-virtual-machine: /usr/local/src
To direct input to this VM, click inside or press Ctrl+G.
3:53 PM
9/10/2023

```
Processing triggers for man-db (2.7.5-1) ...
Setting up libpcrecpp0v5:amd64 (2:8.38-3.1) ...
Setting up bzip2 (1.0.6-8ubuntu0.2) ...
Setting up libssl1.0.0:amd64 (1.0.2g-1ubuntu4.20) ...
Setting up libicu55:amd64 (55.1-7ubuntu0.5) ...
Setting up libxml2:amd64 (2.9.3+dfsg1-1ubuntu0.7) ...
Setting up bzip2-doc (1.0.6-8ubuntu0.2) ...
Setting up icu-devtools (55.1-7ubuntu0.5) ...
Setting up libbz2-dev:amd64 (1.0.6-8ubuntu0.2) ...
Setting up libicu-dev:amd64 (55.1-7ubuntu0.5) ...
Setting up libpcre32-3:amd64 (2:8.38-3.1) ...
Setting up libpcre3-dev:amd64 (2:8.38-3.1) ...
Setting up zlib1g-dev:amd64 (1:1.2.8.dfsg-2ubuntu4.3) ...
Setting up libssl-dev:amd64 (1.0.2g-1ubuntu4.20) ...
Setting up libssl-doc (1.0.2g-1ubuntu4.20) ...
Setting up libxml2-dev:amd64 (2.9.3+dfsg1-1ubuntu0.7) ...
Processing triggers for libc-bin (2.23-0ubuntu10) ...
luyenmuc@luyenmuc-virtual-machine:~$ cd /urs/local/src
bash: cd: /urs/local/src: No such file or directory
luyenmuc@luyenmuc-virtual-machine:~$ cd /urs/local/src/
bash: cd: /urs/local/src/: No such file or directory
luyenmuc@luyenmuc-virtual-machine:~$ cd /usr/local/src/
luyenmuc@luyenmuc-virtual-machine:/usr/local/src$ sudo groupadd clamav
luyenmuc@luyenmuc-virtual-machine:/usr/local/src$ 
```


Ubuntu_Luyenmk - VMware Workstation
File Edit View VM Tabs Help
Home
Ubuntu_Luyenmk
Terminal
luyenmuc@luyenmuc-virtual-machine: /usr/local/src

```
Setting up libssl-doc (1.0.2g-1ubuntu4.20) ...
Setting up libxml2-dev:amd64 (2.9.3+dfsg1-1ubuntu0.7) ...
Processing triggers for libc-bin (2.23-0ubuntu10) ...
luyenmuc@luyenmuc-virtual-machine:~$ cd /urs/local/src
bash: cd: /urs/local/src: No such file or directory
luyenmuc@luyenmuc-virtual-machine:~$ cd /urs/local/src/
bash: cd: /urs/local/src/: No such file or directory
luyenmuc@luyenmuc-virtual-machine:~$ cd /usr/local/src/
luyenmuc@luyenmuc-virtual-machine:/usr/local/src$ sudo groupadd clamav
luyenmuc@luyenmuc-virtual-machine:/usr/local/src$ sudo useradd -g clamav clamav
luyenmuc@luyenmuc-virtual-machine:/usr/local/src$ sudo mkdir /var/clamav
luyenmuc@luyenmuc-virtual-machine:/usr/local/src$ sudo chown clamav:root /var/clamav
luyenmuc@luyenmuc-virtual-machine:/usr/local/src$ sudo mkdir /var/lib/clamav
```



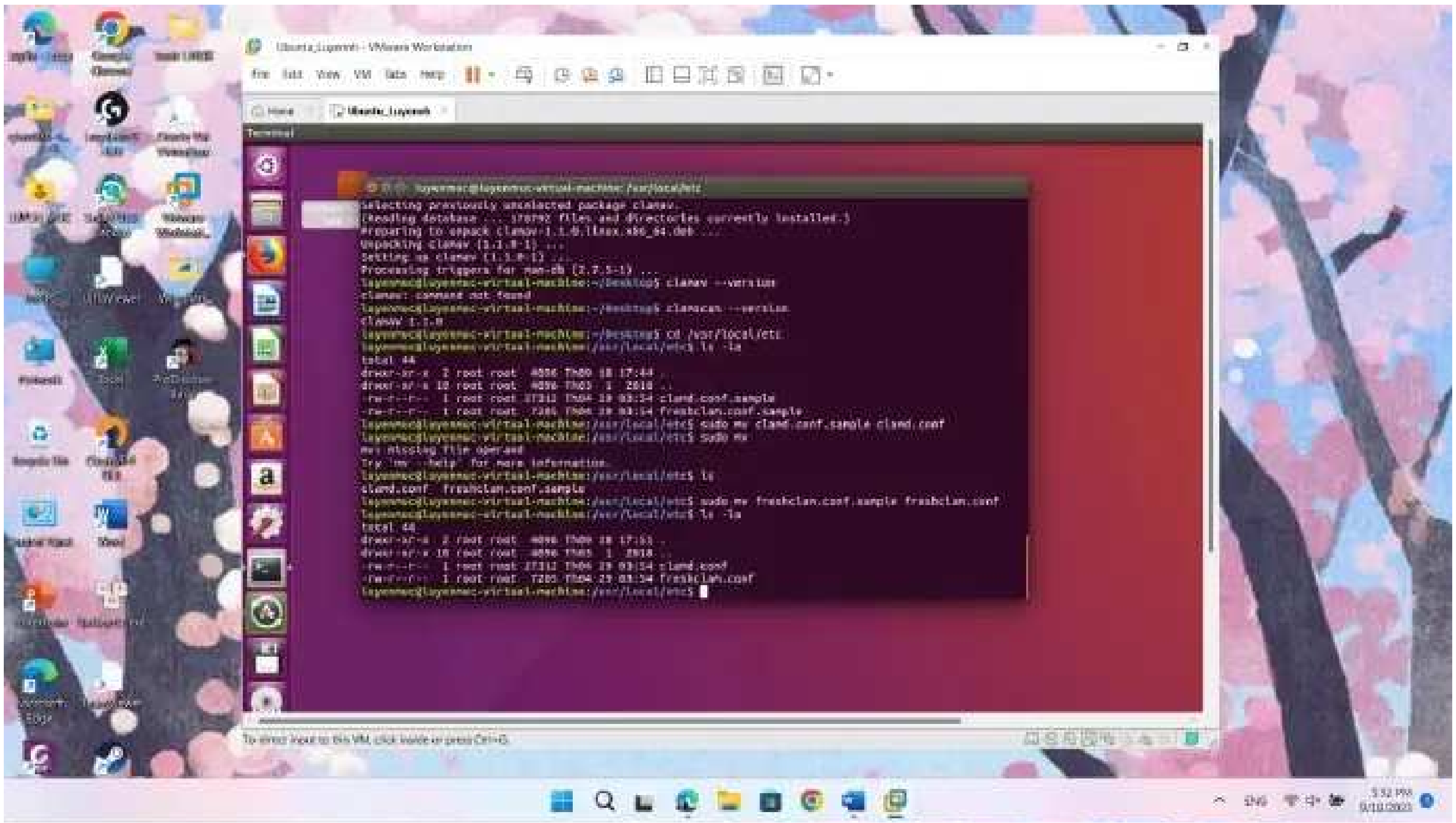
Ubuntu_Luyenmh - VMware Workstation
File Edit View VM Tabs Help
Home
Ubuntu_Luyenmh
Terminal
luyenmuc@luyenmuc-virtual-machine: ~/Desktop
To direct input to this VM, click inside or press Ctrl+G.
ENG

```
chown: cannot access '/usr/local/share/clamav': No such file or directory
luyenmuc@luyenmuc-virtual-machine:/usr/local/src$ sudo chown clamav:clamav /usr/local/share/clama
v
luyenmuc@luyenmuc-virtual-machine:/usr/local/src$ sudo touch /var/log/freshclam.log
luyenmuc@luyenmuc-virtual-machine:/usr/local/src$ sudo chown clamav:clamav /var/log/freshcland.lo
g
chown: cannot access '/var/log/freshcland.log': No such file or directory
luyenmuc@luyenmuc-virtual-machine:/usr/local/src$ sudo chown clamav:clamav /var/log/freshclam.log
luyenmuc@luyenmuc-virtual-machine:/usr/local/src$ sudo mkdir /var/lib/clamav
luyenmuc@luyenmuc-virtual-machine:/usr/local/src$ sudo chown clamav:clamav -R /var/lib/clamav
luyenmuc@luyenmuc-virtual-machine:/usr/local/src$ sudo touch /var/log/clamd.log
luyenmuc@luyenmuc-virtual-machine:/usr/local/src$ sudo chown clamav:clamav /var/log/clamd.log
luyenmuc@luyenmuc-virtual-machine:/usr/local/src$ sudo touch /var/run/clamd.pid
luyenmuc@luyenmuc-virtual-machine:/usr/local/src$ sudo chown clamav:clamav /var/run/clamd.pid
luyenmuc@luyenmuc-virtual-machine:/usr/local/src$ cd /usr/local/src
luyenmuc@luyenmuc-virtual-machine:/usr/local/src$ cd /home/luyenmuc/Desktop/
luyenmuc@luyenmuc-virtual-machine:~/Desktop$ dpkg -i clamav-1.1.0.linux.x86_64.deb
dpkg: error: requested operation requires superuser privilege
luyenmuc@luyenmuc-virtual-machine:~/Desktop$ sudo dpkg -i clamav-1.1.0.linux.x86_64.deb
[sudo] password for luyenmuc:
Selecting previously unselected package clamav.
(Reading database ... 170792 files and directories currently installed.)
Preparing to unpack clamav-1.1.0.linux.x86_64.deb ...
Unpacking clamav (1.1.0-1) ...
Setting up clamav (1.1.0-1) ...
Processing triggers for man-db (2.7.5-1) ...
luyenmuc@luyenmuc-virtual-machine:~/Desktop$ clamav --version
clamav: command not found
luyenmuc@luyenmuc-virtual-machine:~/Desktop$ clamscan --version
ClamAV 1.1.0
luyenmuc@luyenmuc-virtual-machine:~/Desktop$ 
```

Di chuyển tới thư mục /usr/local/etc bằng câu lệnh cd /usr/local/etc, sau đó kiểm tra bằng câu lệnh ls -la ta có thể thấy hai file là clamd.conf.sample và clamd.conf.sample

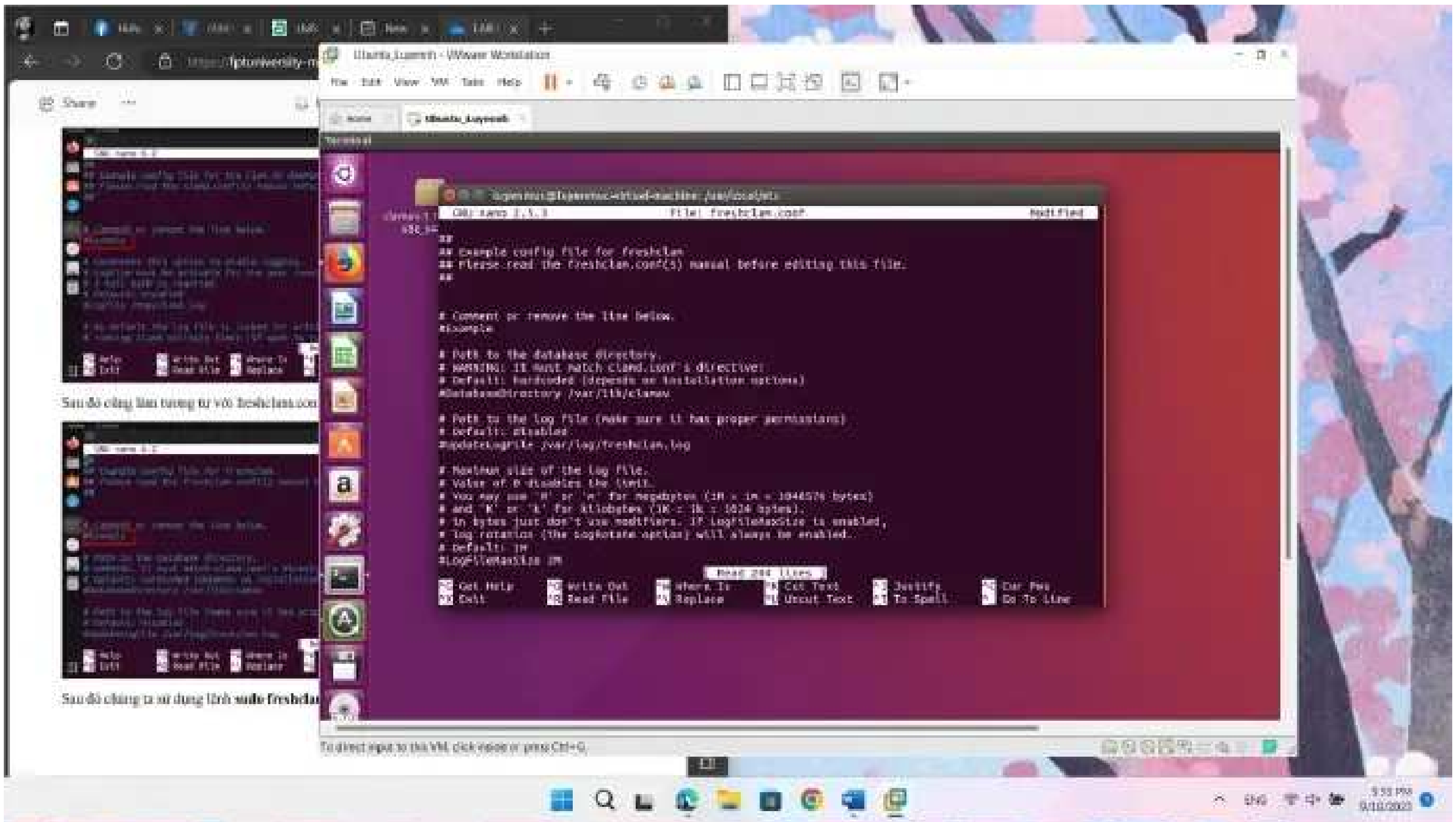
Ubuntu_Luyenmh - VMware Workstation
File Edit View VM Tabs Help
Home
Ubuntu_Luyenmh
Terminal

file cũ> <tên file mới>



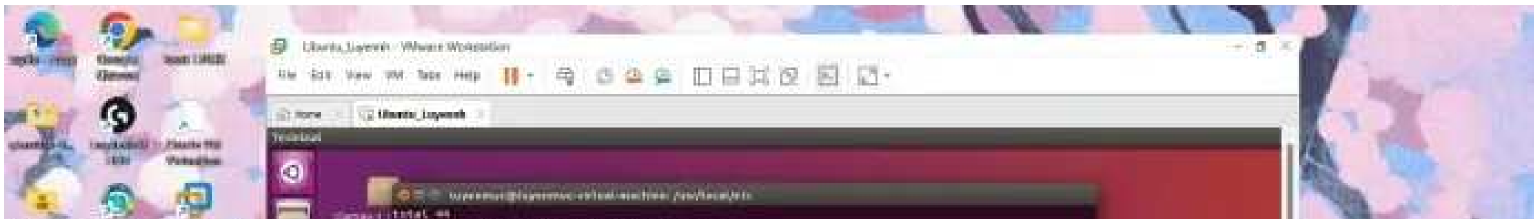
```
Selecting previously unselected package clamav.
(Reading database ... 170792 files and directories currently installed.)
Preparing to unpack clamav-1.1.0.linux.x86_64.deb ...
Unpacking clamav (1.1.0-1) ...
Setting up clamav (1.1.0-1) ...
Processing triggers for man-db (2.7.5-1) ...
layenmac@layenmac-virtual-machine:~/Desktop$ clamav --version
clamav: command not found
layenmac@layenmac-virtual-machine:~/Desktop$ clamscan --version
ClamAV 1.1.0
layenmac@layenmac-virtual-machine:~/Desktop$ cd /usr/local/etc
layenmac@layenmac-virtual-machine:/usr/local/etc$ ls -la
total 44
drwxr-xr-x  2 root root  4096 Th09 18 17:44 .
drwxr-xr-x 10 root root  4096 Th03  1  2018 ..
-rw-r--r--  1 root root 27312 Th06 19 03:34 clamd.conf.sample
-rw-r--r--  1 root root  7205 Th06 19 03:34 freshclam.conf.sample
layenmac@layenmac-virtual-machine:/usr/local/etc$ sudo mv clamd.conf.sample clamd.conf
layenmac@layenmac-virtual-machine:/usr/local/etc$ sudo mv
mv: missing file operand
Try 'mv --help' for more information.
layenmac@layenmac-virtual-machine:/usr/local/etc$ ls
clamd.conf  freshclam.conf.sample
layenmac@layenmac-virtual-machine:/usr/local/etc$ sudo mv freshclam.conf.sample freshclam.conf
layenmac@layenmac-virtual-machine:/usr/local/etc$ ls -la
total 44
drwxr-xr-x  2 root root  4096 Th09 18 17:51 .
drwxr-xr-x 10 root root  4096 Th03  1  2018 ..
-rw-r--r--  1 root root 27312 Th06 29 03:34 clamd.conf
-rw-r--r--  1 root root  7205 Th06 29 03:34 freshclam.conf
layenmac@layenmac-virtual-machine:/usr/local/etc$ 
```

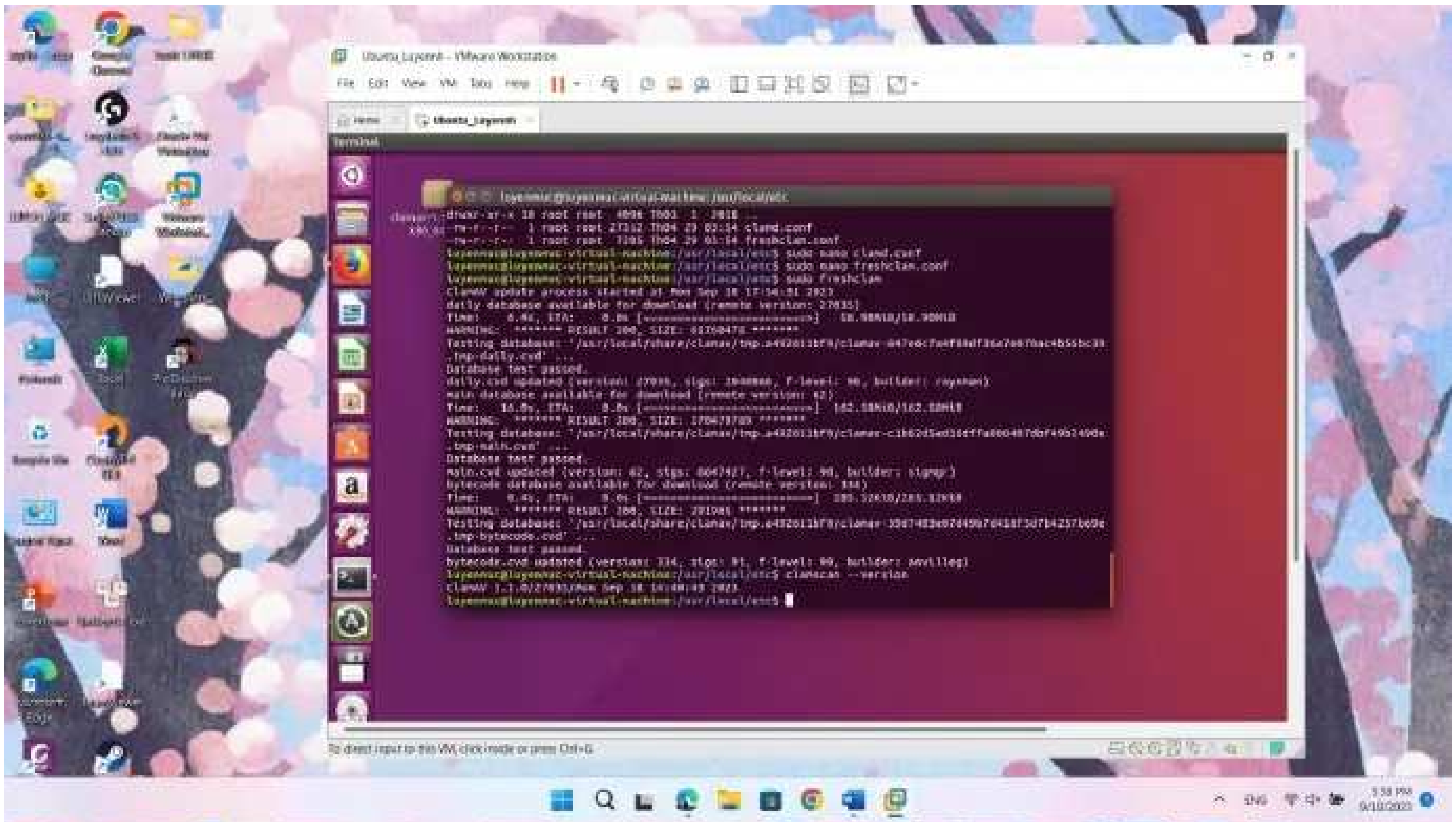
Dùng lệnh sudo nano clamd.conf (xóa example hoặc thêm hastag trước example) Sau đó nhấn Ctrl S rồi Ctrl X để thoát:



```
  GNU nano 2.5.3              File: freshclam.conf                      Modified

##
## Example config file for freshclam
## Please read the freshclam.conf(5) manual before editing this file.
##


# Comment or remove the line below.
#Example

# Path to the database directory.
# WARNING: It must match clamd.conf's directive!
# Default: hardcoded (depends on installation options)
#DatabaseDirectory /var/lib/clamav

# Path to the log file (make sure it has proper permissions)
# Default: disabled
#UpdateLogFile /var/log/freshclam.log

# Maximum size of the log file.
# Value of 0 disables the limit.
# You may use 'M' or 'm' for megabytes (1M = 1m = 1048576 bytes)
# and 'K' or 'k' for kilobytes (1K = 1k = 1024 bytes).
# in bytes just don't use modifiers. If LogFileMaxSize is enabled,
# log rotation (the LogRotate option) will always be enabled.
# Default: 1M
#LogFileMaxSize 2M
                                  [ Read 204 lines ]
^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line
```

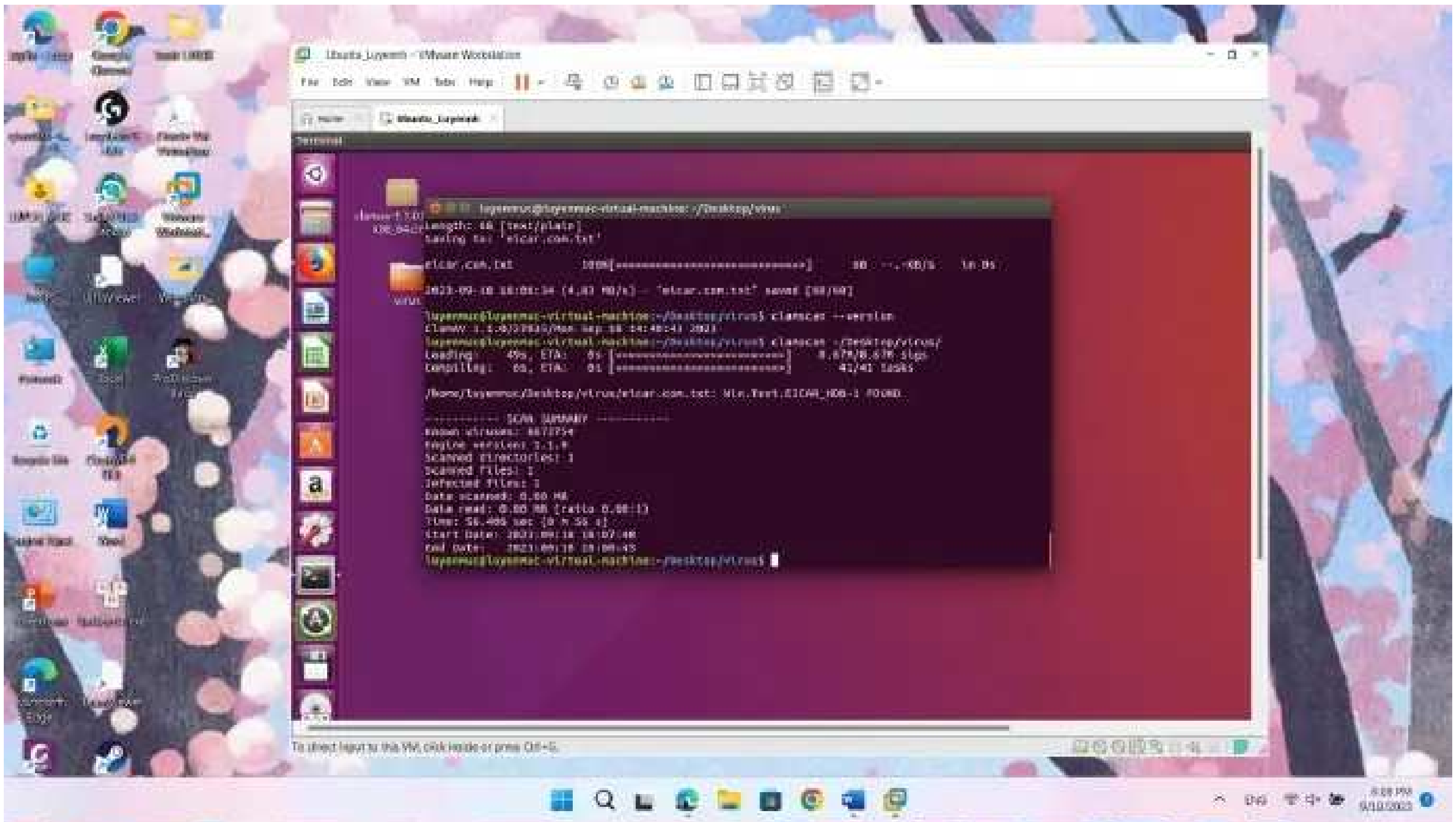
Sau đó chúng ta sử dụng lệnh sudo freshclam để download các file cài đặt ClamAV





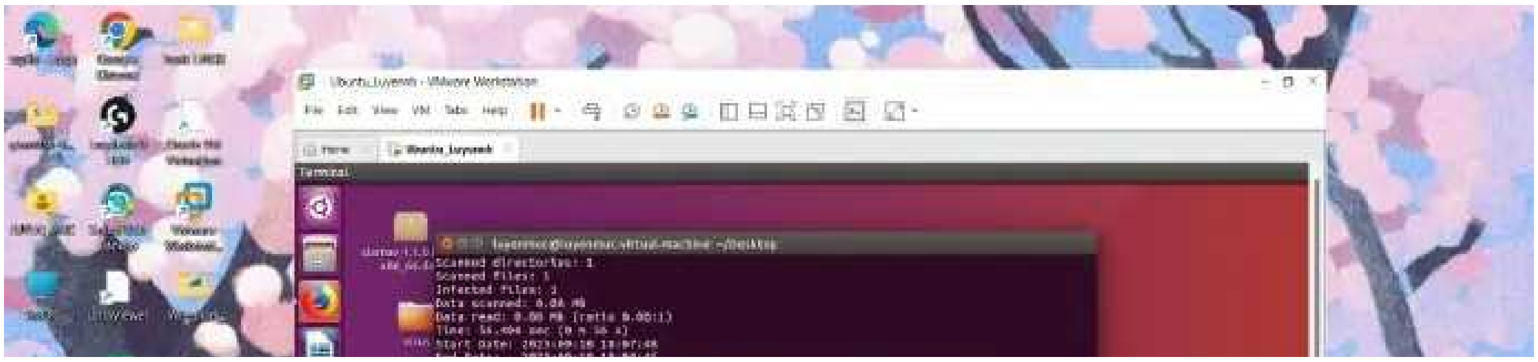
```
drwxr-xr-x 10 root root  4096 Th01  1  2018 ..
-rw-r--r--  1 root root 27312 Th04 29 01:54 clamd.conf
-rw-r--r--  1 root root  7205 Th04 29 01:54 freshclam.conf
layenmac@layenmac-virtual-machine:/usr/local/etc$ sudo nano clamd.conf
layenmac@layenmac-virtual-machine:/usr/local/etc$ sudo nano freshclam.conf
layenmac@layenmac-virtual-machine:/usr/local/etc$ sudo freshclam
ClamAV update process started at Mon Sep 18 17:36:31 2023
daily database available for download (remote version: 27035)
Time:    6.4s, ETA:    0.0s [========================>]   58.98MiB/58.98MiB
WARNING:  ******* RESULT 200, SIZE: 61768478 *******
Testing database: '/usr/local/share/clamav/tmp.a4920113f9/clamav-047edcfa0f88df36a7e07bac4b55bc39
.tmp-daily.cvd' ...
Database test passed.
daily.cvd updated (version: 27035, sigs: 2048066, f-level: 90, builder: raynman)
main database available for download (remote version: 62)
Time:   16.0s, ETA:    0.0s [========================>]  162.58MiB/162.58MiB
WARNING:  ******* RESULT 200, SIZE: 170479789 *******
Testing database: '/usr/local/share/clamav/tmp.a4920113f9/clamav-c1b62d5ed16ffa0b0487dbf49b2490e
.tmp-main.cvd' ...
Database test passed.
main.cvd updated (version: 62, sigs: 6647427, f-level: 90, builder: sigmgr)
bytecode database available for download (remote version: 334)
Time:    0.4s, ETA:    0.0s [========================>]  285.32KiB/285.32KiB
WARNING:  ******* RESULT 200, SIZE: 291961 *******
Testing database: '/usr/local/share/clamav/tmp.a4920113f9/clamav-35d7483e07449b7d418f3d7b4257b60e
.tmp-bytecode.cvd' ...
Database test passed.
bytecode.cvd updated (version: 334, sigs: 91, f-level: 90, builder: anvilleg)
layenmac@layenmac-virtual-machine:/usr/local/etc$ clamscan --version
ClamAV 1.1.0/27035/Mon Sep 18 16:40:49 2023
layenmac@layenmac-virtual-machine:/usr/local/etc$
```

Tiếp theo. chúng ta sẽ thử download một con virus xem có chạy hay không. Vào trong desktop, tạo một thư mục bất kỳ, sau đó dung câu lệnh wget để có thể download file về.



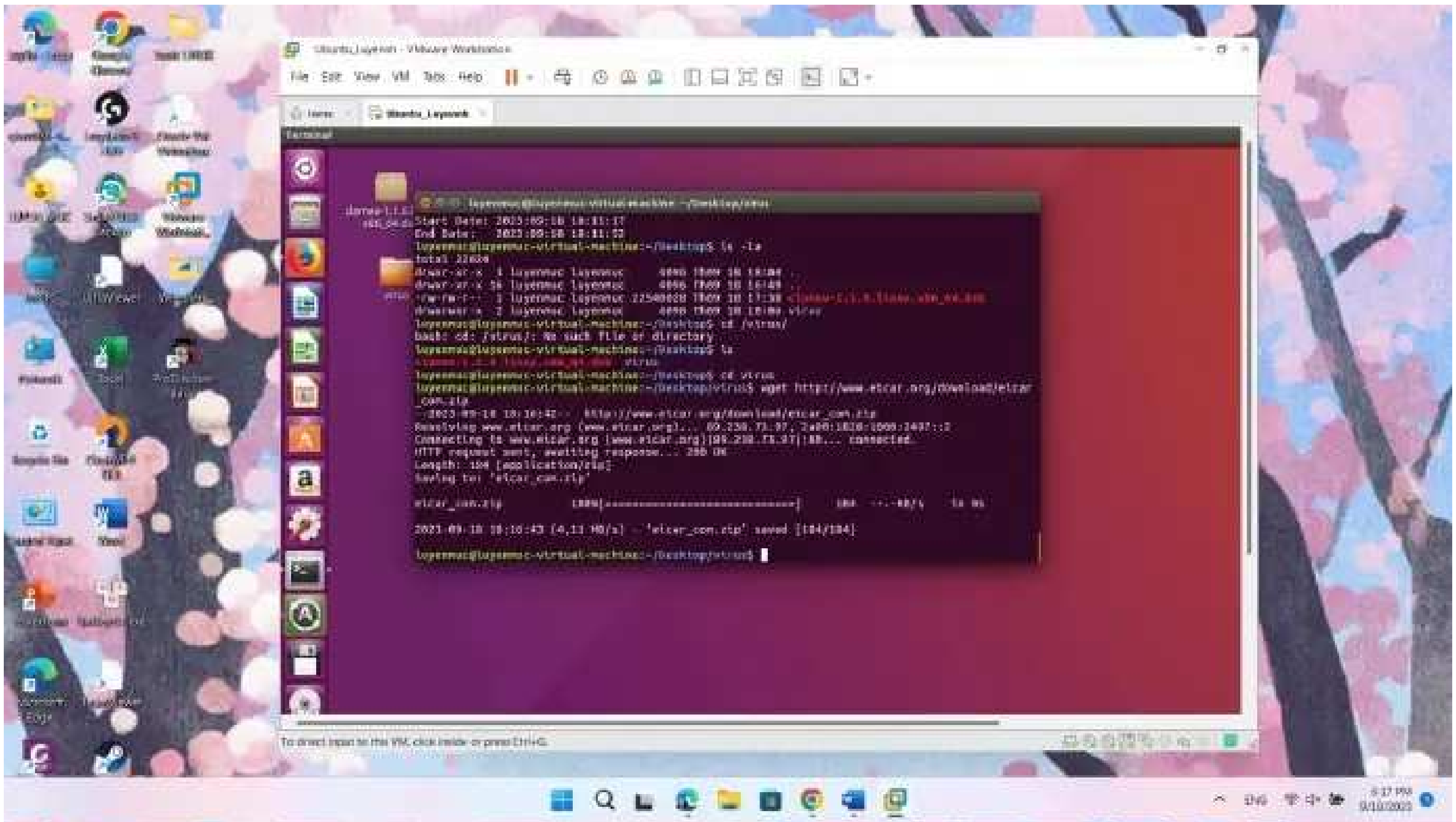
Ubuntu_Luyenmh - VMware Workstation
File Edit View VM Tabs Help
Home
Ubuntu_Luyenmh
Terminal
luyenmuc@luyenmuc-virtual-machine: ~/Desktop/virus
To direct input to this VM, click inside or press Ctrl+G.

```
Length: 68 [text/plain]
Saving to: 'eicar.com.txt'

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

2023-09-18 18:06:34 (4.83 MB/s) - 'eicar.com.txt' saved [68/68]

luyenmuc@luyenmuc-virtual-machine:~/Desktop/virus$ clamscan --version
ClamAV 1.1.0/27036/Mon Sep 18 14:40:43 2023
luyenmuc@luyenmuc-virtual-machine:~/Desktop/virus$ clamscan ~/Desktop/virus/
Loading:    49s, ETA:   0s [========================>]    8.67M/8.67M sigs
Compiling:   6s, ETA:   0s [========================>]       41/41 tasks

/home/luyenmuc/Desktop/virus/eicar.com.txt: Win.Test.EICAR_HDB-1 FOUND

----------- SCAN SUMMARY -----------
Known viruses: 8672754
Engine version: 1.1.0
Scanned directories: 1
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 56.408 sec (0 m 56 s)
Start Date: 2023:09:18 18:07:48
End Date:   2023:09:18 18:08:45
luyenmuc@luyenmuc-virtual-machine:~/Desktop/virus$
```



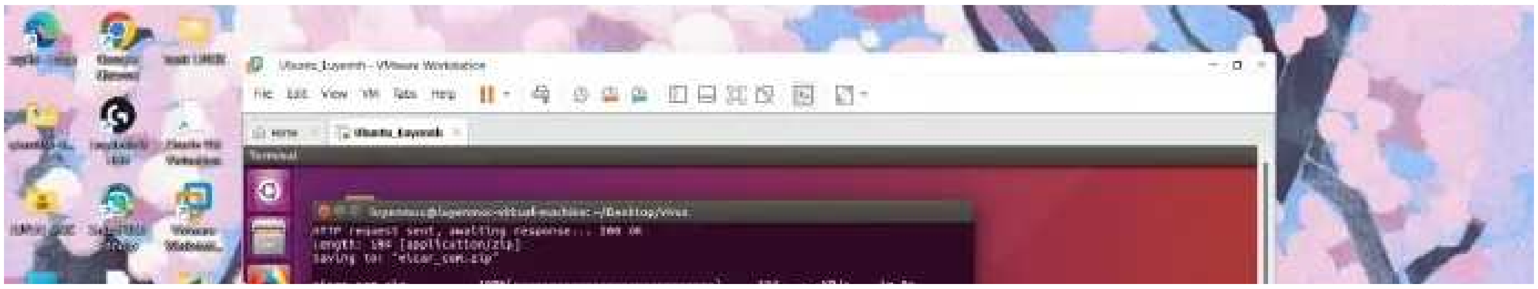
Ubuntu_Luyenmh - VMware Workstation
File Edit View VM Tabs Help
Home
Ubuntu_Luyenmh
Terminal
luyenmuc@luyenmuc-virtual-machine: ~/Desktop

```
Scanned directories: 1
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 56.404 sec (0 m 56 s)
Start Date: 2023:09:18 18:07:48
```

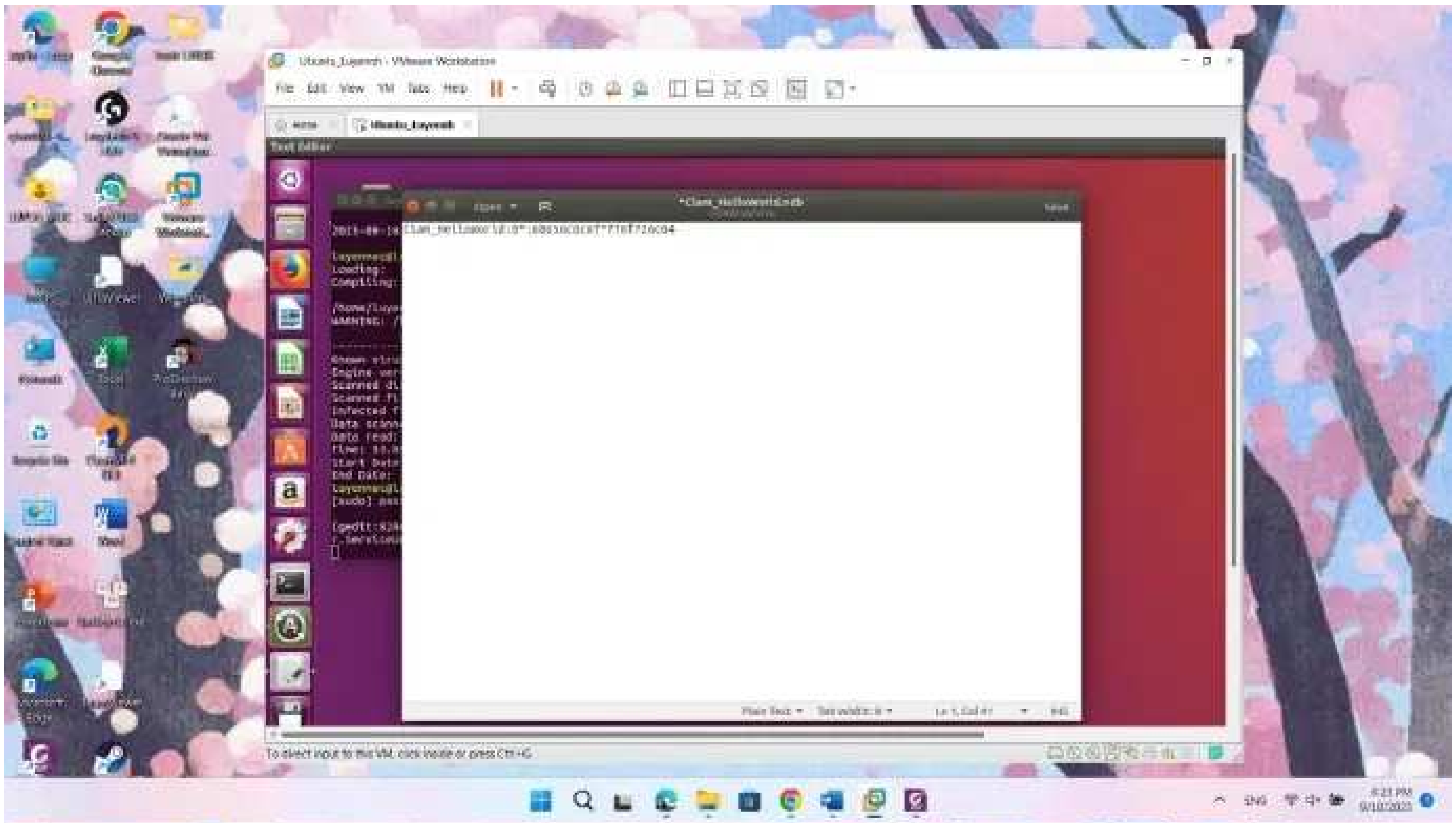


```
luyennuc@luyennuc-virtual-machine: ~/Desktop/virus
Start Date: 2023:09:18 18:11:17
End Date:   2023:09:18 18:11:52
luyennuc@luyennuc-virtual-machine:~/Desktop$ ls -la
total 22024
drwxr-xr-x  3 luyennuc luyennuc     4096 Th09 18 18:04 .
drwxr-x--- 16 luyennuc luyennuc     4096 Th09 18 16:49 ..
-rw-rw-r--  1 luyennuc luyennuc 22540028 Th09 18 17:38 clamav-1.1.0.linux.x86_64.deb
drwxrwxr-x  2 luyennuc luyennuc     4096 Th09 18 18:08 virus
luyennuc@luyennuc-virtual-machine:~/Desktop$ cd /virus/
bash: cd: /virus/: No such file or directory
luyennuc@luyennuc-virtual-machine:~/Desktop$ ls
clamav-1.1.0.linux.x86_64.deb  virus
luyennuc@luyennuc-virtual-machine:~/Desktop$ cd virus
luyennuc@luyennuc-virtual-machine:~/Desktop/virus$ wget http://www.eicar.org/download/eicar
_com.zip
--2023-09-18 18:16:42--  http://www.eicar.org/download/eicar_com.zip
Resolving www.eicar.org (www.eicar.org)... 89.238.73.97, 2a00:1828:1000:2497::2
Connecting to www.eicar.org (www.eicar.org)|89.238.73.97|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 184 [application/zip]
Saving to: 'eicar_com.zip'

eicar_com.zip           100%[===================================>]     184  --.-KB/s    in 0s

2023-09-18 18:16:43 (4,13 MB/s) - 'eicar_com.zip' saved [184/184]

luyennuc@luyennuc-virtual-machine:~/Desktop/virus$
```

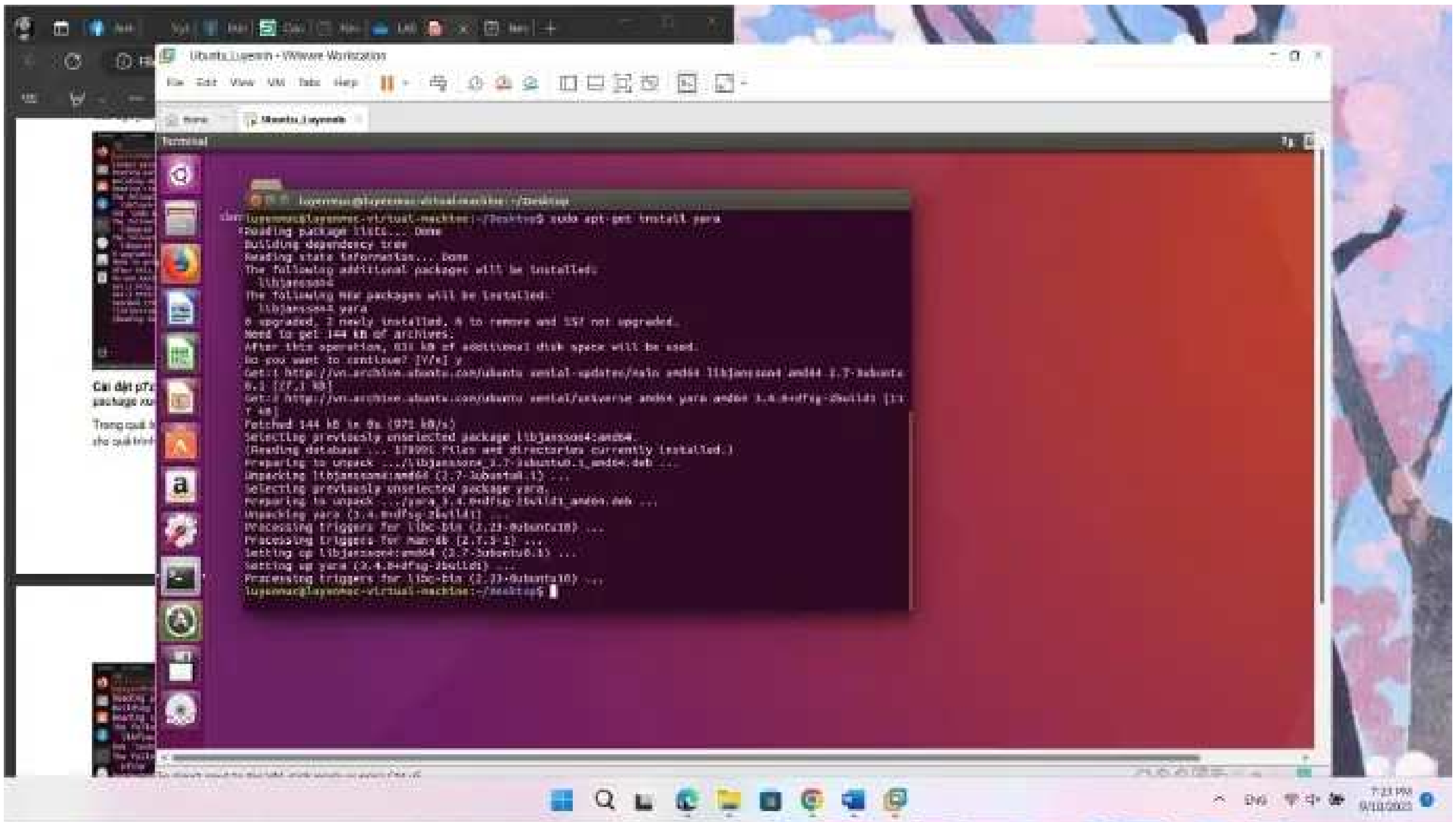
Bây giờ chún ta sẽ tạo một rule để có thể test với clamav.



```
luyennuc@luyennuc-virtual-machine: ~/Desktop/virus
HTTP request sent, awaiting response... 200 OK
Length: 184 [application/zip]
Saving to: 'eicar_com.zip'
```

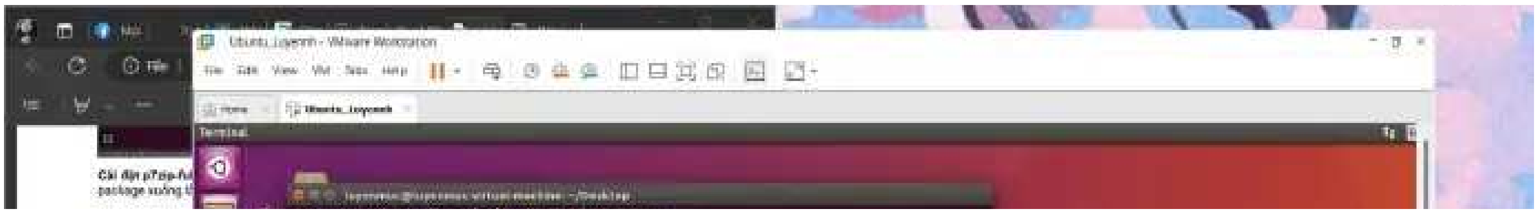


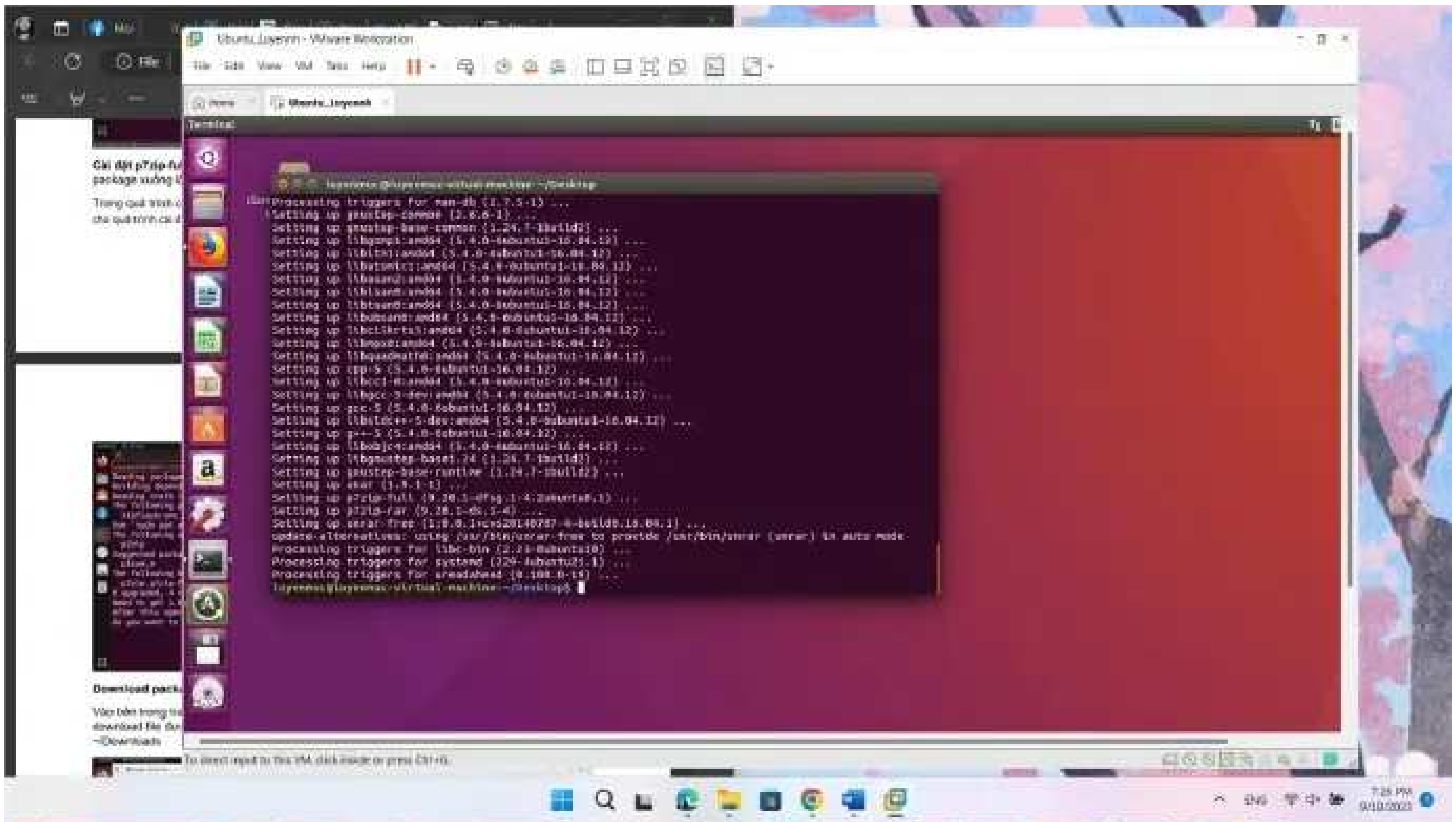
Tiếp đến, ta tạo file test.txt bằng lệnh sudo touch ./test.txt, trong file này có sẽ chứa 2 từ “hello world”. Sau đó là ta dùng lệnh này để scan:



```
luyenmac@luyenmac-virtual-machine:~/Desktop$ sudo apt-get install yara
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libjansson4
The following NEW packages will be installed:
  libjansson4 yara
0 upgraded, 2 newly installed, 0 to remove and 557 not upgraded.
Need to get 144 kB of archives.
After this operation, 631 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://vn.archive.ubuntu.com/ubuntu xenial-updates/main amd64 libjansson4 amd64 2.7-1ubuntu
0.1 [27.1 kB]
Get:2 http://vn.archive.ubuntu.com/ubuntu xenial/universe amd64 yara amd64 3.4.0+dfsg-2build1 [11
7 kB]
Fetched 144 kB in 0s (971 kB/s)
Selecting previously unselected package libjansson4:amd64.
(Reading database ... 178991 files and directories currently installed.)
Preparing to unpack .../libjansson4_2.7-1ubuntu0.1_amd64.deb ...
Unpacking libjansson4:amd64 (2.7-1ubuntu0.1) ...
Selecting previously unselected package yara.
Preparing to unpack .../yara_3.4.0+dfsg-2build1_amd64.deb ...
Unpacking yara (3.4.0+dfsg-2build1) ...
Processing triggers for libc-bin (2.23-0ubuntu10) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up libjansson4:amd64 (2.7-1ubuntu0.1) ...
Setting up yara (3.4.0+dfsg-2build1) ...
Processing triggers for libc-bin (2.23-0ubuntu10) ...
luyenmac@luyenmac-virtual-machine:~/Desktop$
```

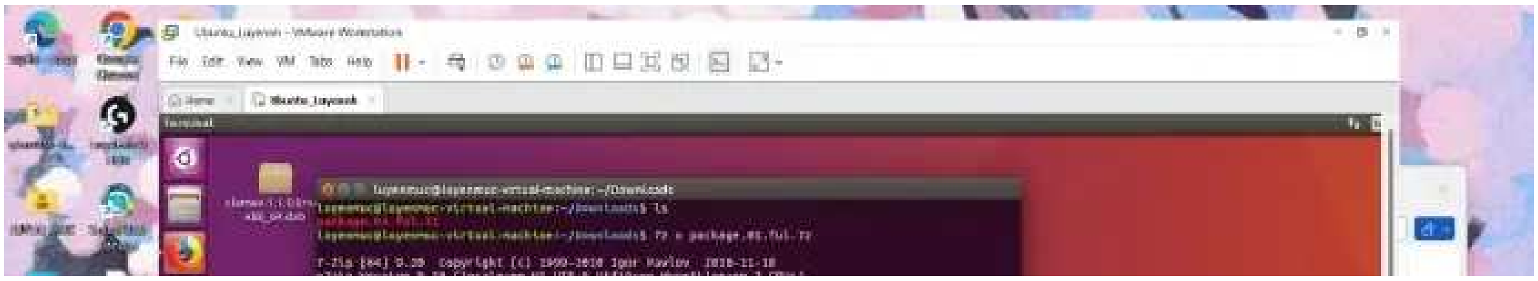
Cài đặt p7zip-full:



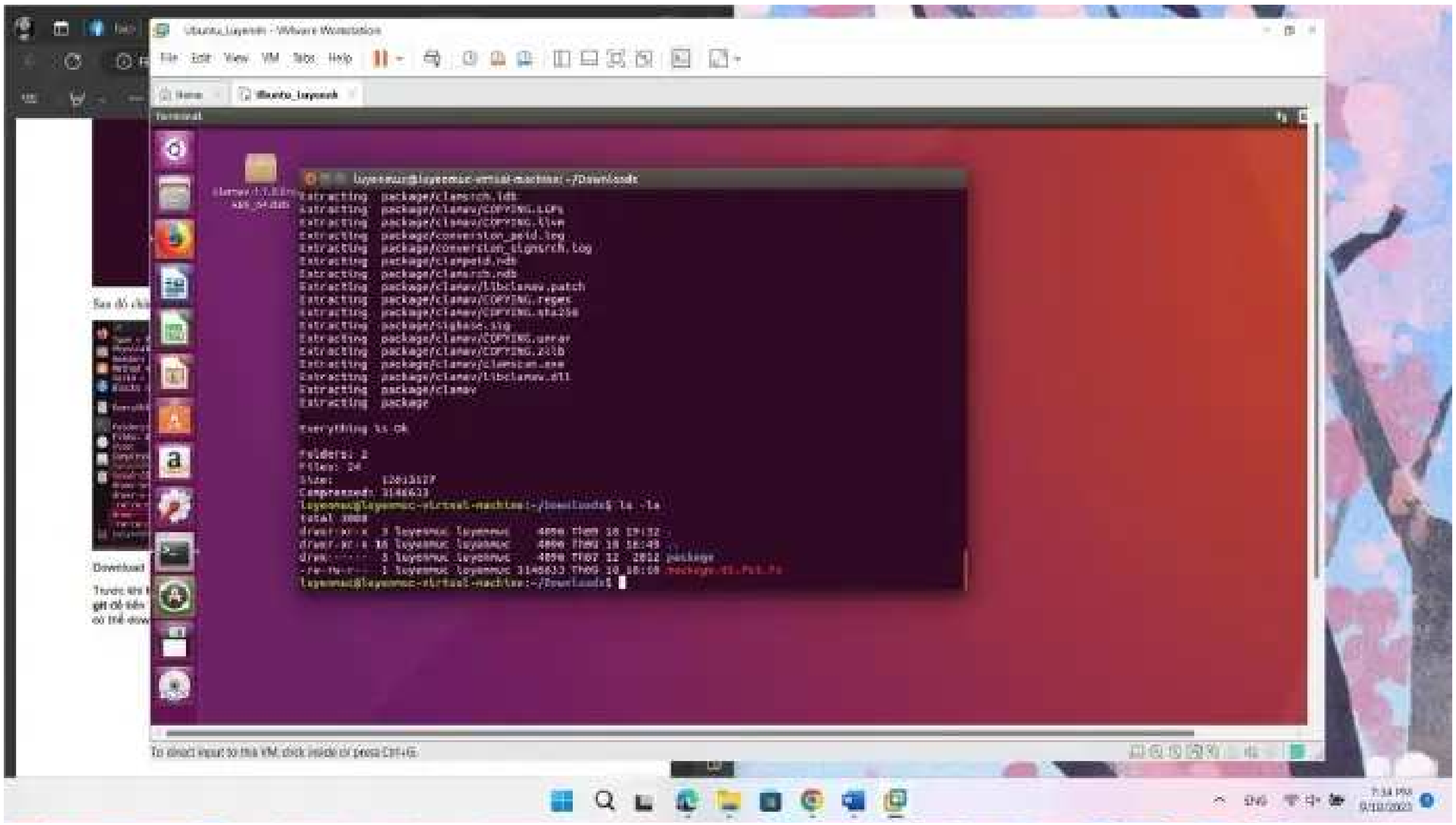


```
luyenmuc@luyenmuc-virtual-machine: ~/Desktop
Processing triggers for man-db (2.7.5-1) ...
Setting up gnustep-common (2.6.6-1) ...
Setting up gnustep-base-common (1.24.7-1build2) ...
Setting up libgomp1:amd64 (5.4.0-6ubuntu1~16.04.12) ...
Setting up libitm1:amd64 (5.4.0-6ubuntu1~16.04.12) ...
Setting up libatomic1:amd64 (5.4.0-6ubuntu1~16.04.12) ...
Setting up libasan2:amd64 (5.4.0-6ubuntu1~16.04.12) ...
Setting up liblsan0:amd64 (5.4.0-6ubuntu1~16.04.12) ...
Setting up libtsan0:amd64 (5.4.0-6ubuntu1~16.04.12) ...
Setting up libubsan0:amd64 (5.4.0-6ubuntu1~16.04.12) ...
Setting up libcilkrts5:amd64 (5.4.0-6ubuntu1~16.04.12) ...
Setting up libmpx0:amd64 (5.4.0-6ubuntu1~16.04.12) ...
Setting up libquadmath0:amd64 (5.4.0-6ubuntu1~16.04.12) ...
Setting up cpp-5 (5.4.0-6ubuntu1~16.04.12) ...
Setting up libcc1-0:amd64 (5.4.0-6ubuntu1~16.04.12) ...
Setting up libgcc-5-dev:amd64 (5.4.0-6ubuntu1~16.04.12) ...
Setting up gcc-5 (5.4.0-6ubuntu1~16.04.12) ...
Setting up libstdc++-5-dev:amd64 (5.4.0-6ubuntu1~16.04.12) ...
Setting up g++-5 (5.4.0-6ubuntu1~16.04.12) ...
Setting up libobjc4:amd64 (5.4.0-6ubuntu1~16.04.12) ...
Setting up libgnustep-base1.24 (1.24.7-1build2) ...
Setting up gnustep-base-runtime (1.24.7-1build2) ...
Setting up akor (1.9.1-1) ...
Setting up p7zip-full (9.20.1~dfsg.1-4.2ubuntu0.1) ...
Setting up p7zip-rar (9.20.1-ds.1-4) ...
Setting up unrar-free (1:0.0.1+cvs20140707-4-build0.16.04.1) ...
update-alternatives: using /usr/bin/unrar-free to provide /usr/bin/unrar (unrar) in auto mode
Processing triggers for libc-bin (2.23-0ubuntu10) ...
Processing triggers for systemd (229-4ubuntu21.1) ...
Processing triggers for ureadahead (0.100.0-19) ...
luyenmuc@luyenmuc-virtual-machine:~/Desktop$ 
```

Sau khi download, chúng ta sẽ tiến hành phân giải chúng:

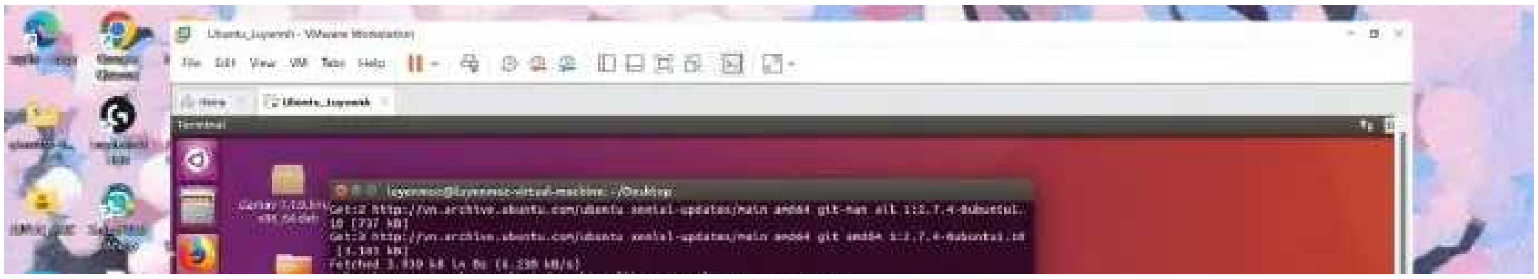


```
luyenmuc@luyenmuc-virtual-machine:~/Downloads
luyenmuc@luyenmuc-virtual-machine:~/Downloads$ ls
package.01.full.7z
luyenmuc@luyenmuc-virtual-machine:~/Downloads$ 7z x package.01.full.7z

7-Zip [64] 9.20  Copyright (c) 1999-2010 Igor Pavlov  2010-11-18
```

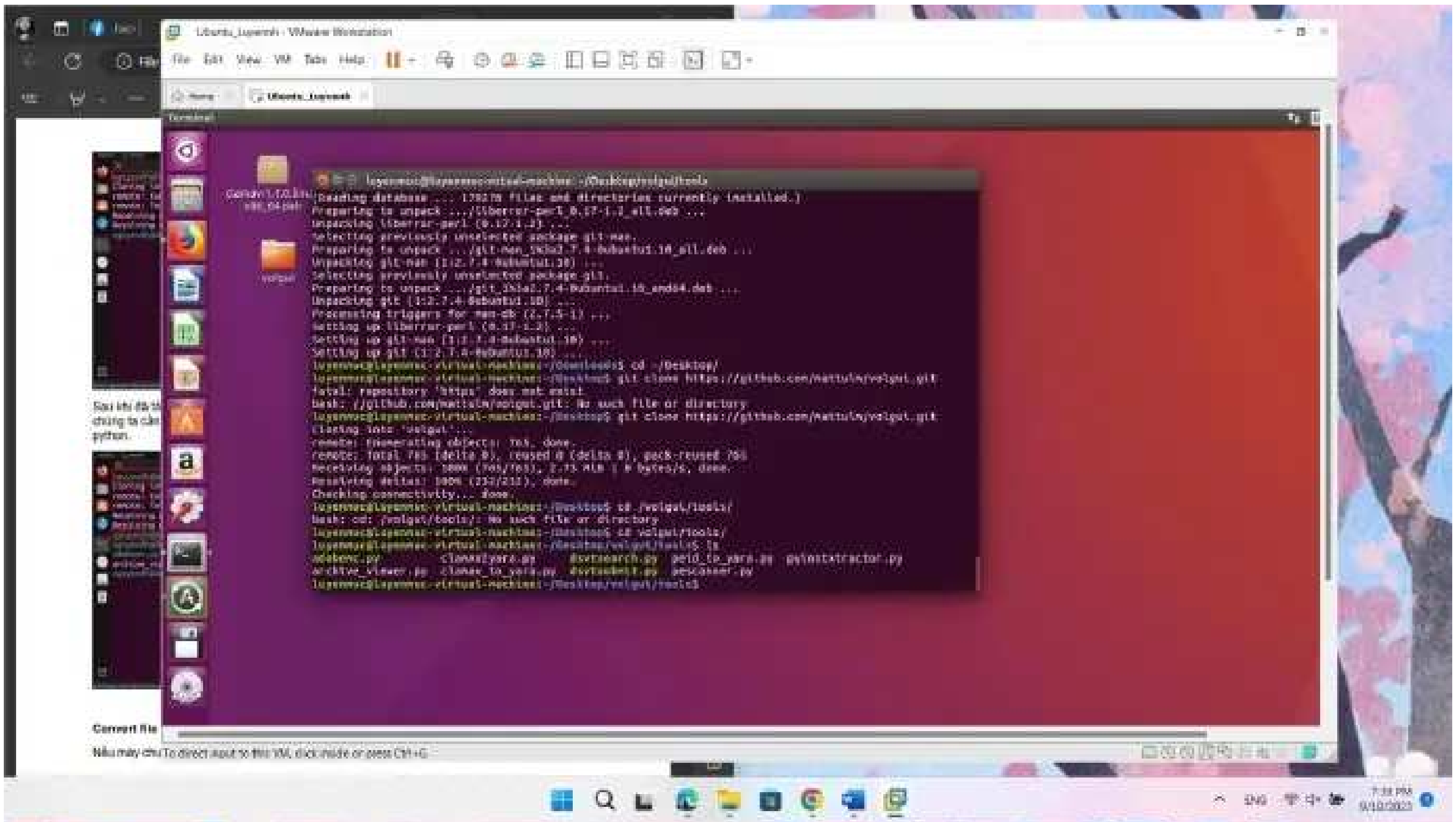


```
luyenmuc@luyenmuc-virtual-machine: ~/Downloads
Extracting  package/clamsrch.ldb
Extracting  package/clamav/COPYING.LGPL
Extracting  package/clamav/COPYING.llvm
Extracting  package/conversion_peid.log
Extracting  package/conversion_signsrch.log
Extracting  package/clampeid.ndb
Extracting  package/clamsrch.ndb
Extracting  package/clamav/libclamav.patch
Extracting  package/clamav/COPYING.regex
Extracting  package/clamav/COPYING.sha256
Extracting  package/sigbase.sig
Extracting  package/clamav/COPYING.unrar
Extracting  package/clamav/COPYING.zlib
Extracting  package/clamav/clamscan.exe
Extracting  package/clamav/libclamav.dll
Extracting  package/clamav
Extracting  package

Everything is Ok

Folders: 2
Files: 24
Size:       12813127
Compressed: 3146633
luyenmuc@luyenmuc-virtual-machine:~/Downloads$ ls -la
total 3088
drwxr-xr-x  3 luyenmuc luyenmuc    4096 Th09 10 19:32 .
drwxr-xr-x 16 luyenmuc luyenmuc    4096 Th09 10 16:49 ..
drwx------  3 luyenmuc luyenmuc    4096 Th07 12  2012 package
-rw-rw-r--  1 luyenmuc luyenmuc 3146633 Th09 10 18:08 package.01.Pc5.7z
luyenmuc@luyenmuc-virtual-machine:~/Downloads$ 
```

Download file clam_to_yara.py:



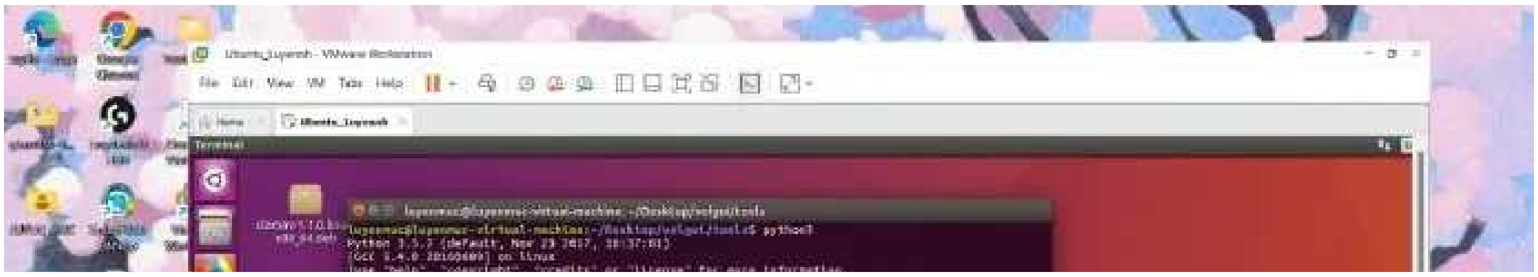
```
luyenmuc@luyenmuc-virtual-machine: ~/Desktop
Get:2 http://vn.archive.ubuntu.com/ubuntu xenial-updates/main amd64 git-man all 1:2.7.4-0ubuntu1.
10 [737 kB]
Get:3 http://vn.archive.ubuntu.com/ubuntu xenial-updates/main amd64 git amd64 1:2.7.4-0ubuntu1.10
 [3,103 kB]
Fetched 3,839 kB in 0s (4,238 kB/s)
```



```
luyennmc@luyennmc-virtual-machine: ~/Desktop/volgui/tools
(Reading database ... 170278 files and directories currently installed.)
Preparing to unpack .../liberror-perl_0.17-1.2_all.deb ...
Unpacking liberror-perl (0.17-1.2) ...
Selecting previously unselected package git-man.
Preparing to unpack .../git-man_1%3a2.7.4-0ubuntu1.10_all.deb ...
Unpacking git-man (1:2.7.4-0ubuntu1.10) ...
Selecting previously unselected package git.
Preparing to unpack .../git_1%3a2.7.4-0ubuntu1.10_amd64.deb ...
Unpacking git (1:2.7.4-0ubuntu1.10) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up liberror-perl (0.17-1.2) ...
Setting up git-man (1:2.7.4-0ubuntu1.10) ...
Setting up git (1:2.7.4-0ubuntu1.10) ...
luyennmc@luyennmc-virtual-machine:~/Downloads$ cd ~/Desktop/
luyennmc@luyennmc-virtual-machine:~/Desktop$ git clone https://github.com/mattulm/volgui.git
fatal: repository 'https' does not exist
bash: //github.com/mattulm/volgui.git: No such file or directory
luyennmc@luyennmc-virtual-machine:~/Desktop$ git clone https://github.com/mattulm/volgui.git
Cloning into 'volgui'...
remote: Enumerating objects: 765, done.
remote: Total 765 (delta 0), reused 0 (delta 0), pack-reused 765
Receiving objects: 100% (765/765), 2.73 MiB | 0 bytes/s, done.
Resolving deltas: 100% (232/232), done.
Checking connectivity... done.
luyennmc@luyennmc-virtual-machine:~/Desktop$ cd /volgui/tools/
bash: cd: /volgui/tools/: No such file or directory
luyennmc@luyennmc-virtual-machine:~/Desktop$ cd volgui/tools/
luyennmc@luyennmc-virtual-machine:~/Desktop/volgui/tools$ ls
adobenc.py        clamavtyara.py     dsvtsearch.py   peid_to_yara.py  pytextractor.py
archive_viewer.py  clamav_to_yara.py  dsvtsubmit.py   pescanner.py
luyennmc@luyennmc-virtual-machine:~/Desktop/volgui/tools$
```

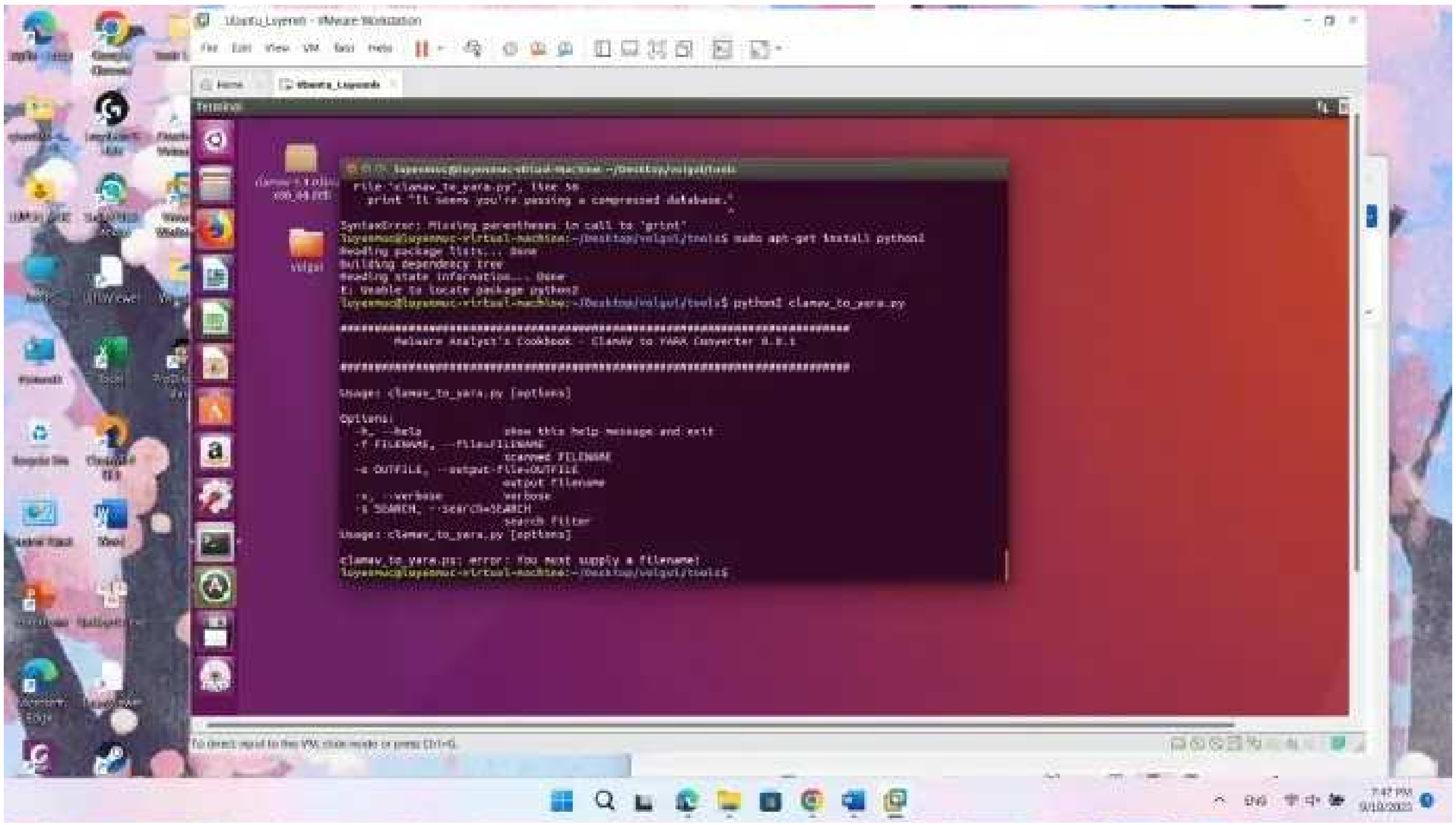
Ubuntu_Luyennh - VMware Workstation
File Edit View VM Tabs Help
Home
Ubuntu_Luyennh
Terminal
volgui
Convert file
To direct input to this VM, click inside or press Ctrl+G.
ENG
7:33 PM
9/10/2023

Convert file clamav sang yara



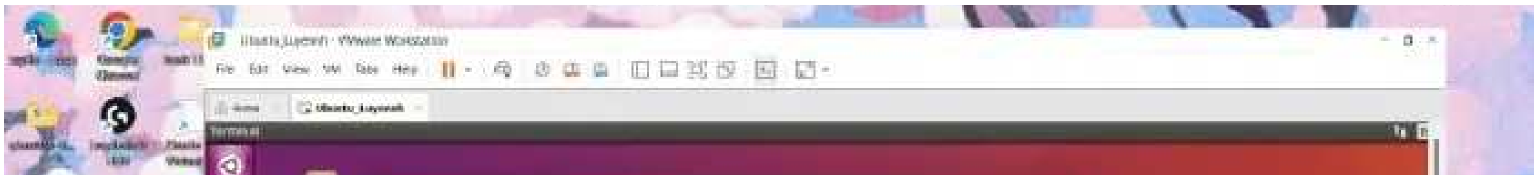
```
luyennmc@luyennmc-virtual-machine: ~/Desktop/volgui/tools
luyennmc@luyennmc-virtual-machine:~/Desktop/volgui/tools$ python3
Python 3.5.2 (default, Nov 23 2017, 16:37:01)
[GCC 5.4.0 20160609] on linux
Type "help", "copyright", "credits" or "license" for more information.
```

Google Chrome
Ubuntu_Luyennh - VMware Workstation
File Edit View VM Tabs Help
Home
Ubuntu_Luyennh
Terminal



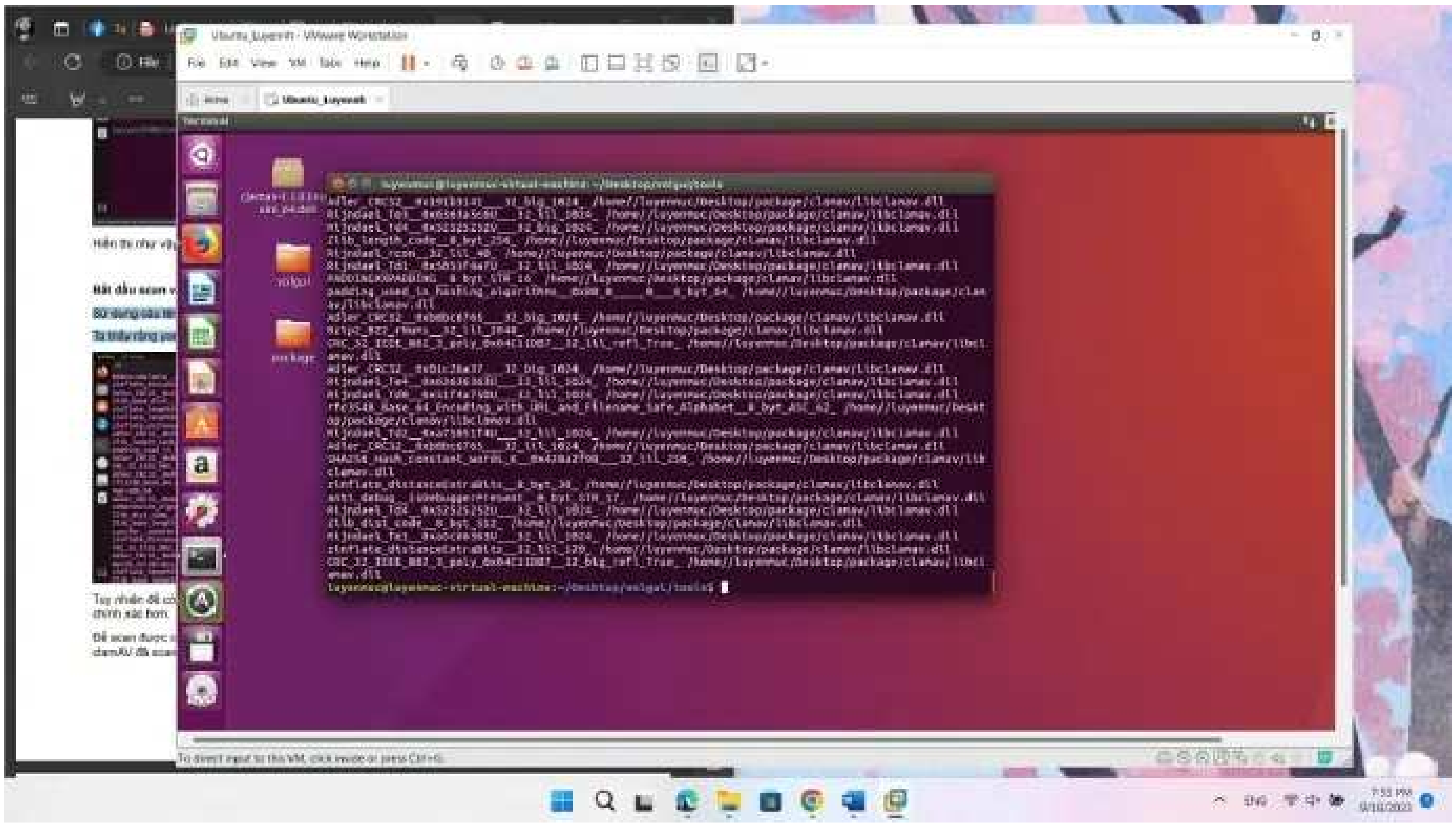
```
File "clamav_to_yara.py", line 56
    print "It seems you're passing a compressed database."
                                                          ^
SyntaxError: Missing parentheses in call to 'print'
luyenmuc@luyenmuc-virtual-machine:~/Desktop/volgui/tools$ sudo apt-get install python2
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package python2
luyenmuc@luyenmuc-virtual-machine:~/Desktop/volgui/tools$ python2 clamav_to_yara.py

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

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

Usage: clamav_to_yara.py [options]

Options:
  -h, --help            show this help message and exit
  -f FILENAME, --file=FILENAME
                        scanned FILENAME
  -o OUTFILE, --output-file=OUTFILE
                        output filename
  -v, --verbose         verbose
  -s SEARCH, --search=SEARCH
                        search filter
Usage: clamav_to_yara.py [options]

clamav_to_yara.py: error: You must supply a filename!
luyenmuc@luyenmuc-virtual-machine:~/Desktop/volgui/tools$
```

Ở đây nó sẽ hiện ra một số cách dung cơ bản của file này như là -f để hiện file, -o là file output. Vì thế full command của chúng ta sẽ là: sudo python clamav_to_yara.py -f ~/Desktop/package/clamsrch.ndb -o clamsrch.yara



Bắt đầu scan với yara:

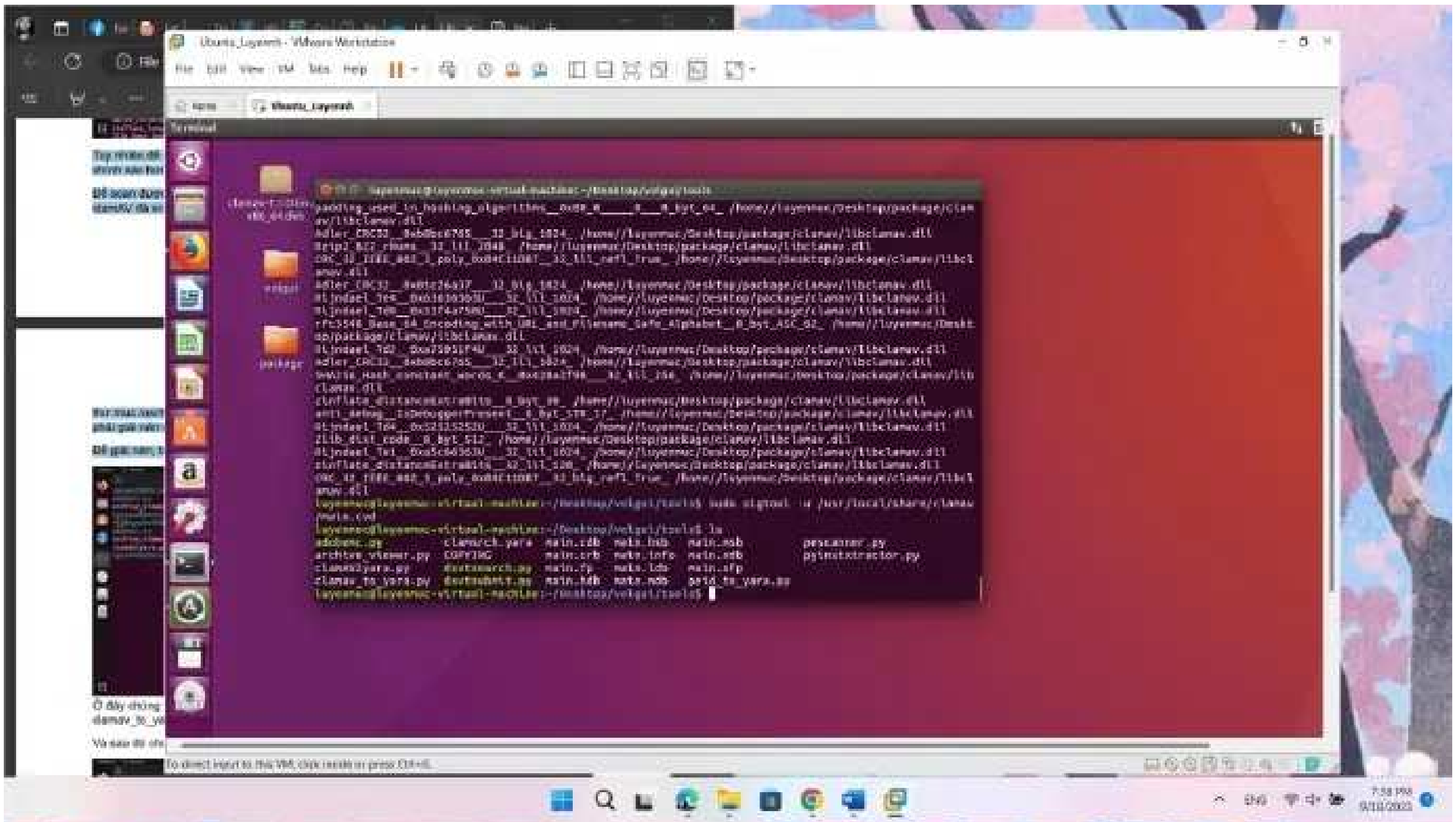
Sử dụng câu lệnh: yara -r clamsrch.yara /home/ để test xem có chuyện gì xảy ra không Ta thấy rằng yara đã scan ra rất nhiều thứ được biểu thị ở hình dưới đây



Ubuntu_Luyenmh - VMware Workstation
File Edit View VM Tabs Help
Home
Ubuntu_Luyenmh
luyenmuc@luyenmuc-virtual-machine: ~/Desktop/nsigat/tools

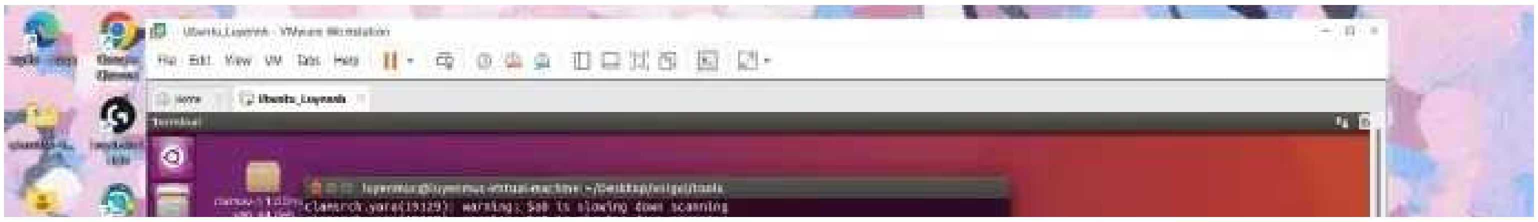
```
Adler_CRC32__0x[illegible]__32_big_1024_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
Rijndael_Td1__0x[illegible]__32_lit_1024_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
Rijndael_Td4__0x52525252U__32_big_1024_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
Zlib_length_code__8_byt_256_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
Rijndael_rcon__32_lit_40_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
Rijndael_Td1__0x5053f0a7U__32_lit_1024_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
[illegible]__8_byt_STR_16_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
padding_used_in_hashing_algorithms__0x80_0____0___0_byt_64_ /home//luyenmuc/Desktop/package/clam
av/libclamav.dll
Adler_CRC32__0xb0bc6765__32_big_1024_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
[illegible]__32_lit_2048_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
CRC_32_IEEE_802_3_poly_0x04C11DB7__32_lit_refl_True_ /home//luyenmuc/Desktop/package/clamav/libcl
amav.dll
Adler_CRC32__0x01c[illegible]__32_big_1024_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
Rijndael_Te4__0x63636363U__32_lit_1024_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
Rijndael_Td0__0x51f4a750U__32_lit_1024_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
rfc3548_Base_64_Encoding_with_URL_and_Filename_Safe_Alphabet__8_byt_ASC_62_ /home//luyenmuc/Deskt
op/package/clamav/libclamav.dll
Rijndael_Td2__0xa75051f4U__32_lit_1024_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
Adler_CRC32__0xb0bc6765__32_lit_1024_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
SHA256_Hash_constant_words_K__0x428a2f98__32_lit_256_ /home//luyenmuc/Desktop/package/clamav/lib
clamav.dll
zinflate_distanceExtraBits__8_byt_30_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
anti_debug__IsDebuggerPresent__8_byt_STR_17_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
Rijndael_Td3__0x52525252U__32_lit_1024_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
zlib_dist_code__8_byt_512_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
Rijndael_Te1__0xa5c66363U__32_lit_1024_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
zinflate_distanceExtraBits__32_lit_120_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
CRC_32_IEEE_802_3_poly_0x04C11DB7__32_big_refl_True_ /home//luyenmuc/Desktop/package/clamav/libcl
amav.dll
luyenmuc@luyenmuc-virtual-machine:~/Desktop/nsigat/tools$
```

Tuy nhiên để có thể chính xác hơn thì ta sẽ dung data của clamav để làm để scan một cách chính xác hơn.



```
padding_used_in_hashing_algorithms__0x80_0______0___0_byt_64_ /home//luyenmuc/Desktop/package/clam
av/libclamav.dll
Adler_CRC32__0xb0bc6785___32_big_1024_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
Bzip2_BZ2_rNums__32_lil_2048_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
CRC_32_IEEE_802_3_poly_0x04C11DB7__32_lil_refl_true_ /home//luyenmuc/Desktop/package/clamav/libcl
amav.dll
Adler_CRC32__0x0tc26a37___32_big_1024_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
Rijndael_Te6__0x6163636363U___32_lil_1024_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
Rijndael_Td0__0x33f4a7500___32_lil_1024_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
rfc3548_Base_64_Encoding_with_URL_and_Filename_Safe_Alphabet__8_byt_ASC_62_ /home//luyenmuc/Deskt
op/package/clamav/libclamav.dll
Rijndael_Td2__0xa75051f4U___32_lil_1024_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
Adler_CRC32__0xb0bc6785___32_lil_1024_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
SHA256_Hash_constant_words_K__0x428a2f98___32_lil_256_ /home//luyenmuc/Desktop/package/clamav/lib
clamav.dll
zinflate_distanceExtraBits__8_byt_30_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
anti_debug__IsDebuggerPresent__8_byt_STR_17_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
Rijndael_Te4__0x52525252U___32_lil_1024_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
Zlib_dist_code__8_byt_512_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
Rijndael_Te1__0xa5c66363U___32_lil_1024_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
zinflate_distanceExtraBits__32_lil_120_ /home//luyenmuc/Desktop/package/clamav/libclamav.dll
CRC_32_IEEE_802_3_poly_0x04C11DB7__32_big_refl_true_ /home//luyenmuc/Desktop/package/clamav/libcl
amav.dll
luyenmuc@luyenmuc-virtual-machine:~/Desktop/volgai/tools$ sudo sigtool -u /usr/local/share/clamav
/main.cvd
luyenmuc@luyenmuc-virtual-machine:~/Desktop/volgai/tools$ ls
adobemc.py         clamsrch.yara  main.cdb  main.hdb   main.mdb        pescanner.py
archive_viewer.py  COPYING        main.crb  main.info  main.ndb        pyinstxtractor.py
clamav2yara.py     dextsearch.py  main.fp   main.ldb   main.sfp
clamav_to_yara.py  dextsubmit.py  main.hdb  main.mdb   peid_to_yara.py
luyenmuc@luyenmuc-virtual-machine:~/Desktop/volgai/tools$ 
```

Ở đây chúng ta có thể thấy rằng file đã được giải nén ra là main.ndb. Sau đó sử dụng clamav_to_yara.py để chuyển đổi file thành file yara. Và sau đó chúng ta chúng ta



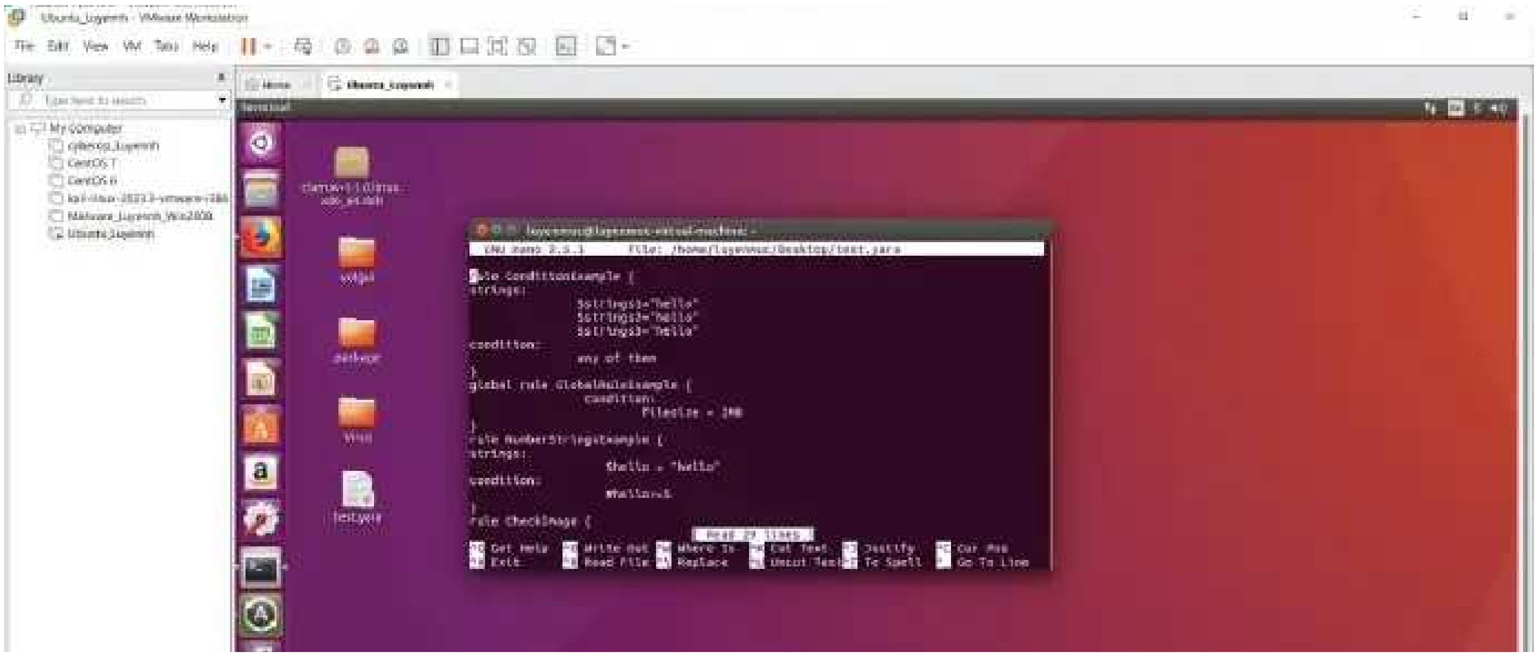
```
clamsrch.yara(19129): warning: $a0 is slowing down scanning
```

rule ConditionsExample { strings: $strings1="hello" $strings2="hello" $strings3="hello" condition: any of them }

Câu lệnh này sẽ check xem là trong file có chữ hello hay không, nếu có chữ hello thì sẽ match rule global rule GlobalRuleExample { condition: filesize < 2MB }, rule này sẽ bắt buộc yêu cầu filesize < 2MB, nếu bé hơn 2MB thì sẽ match

rule NumberStringsExample { strings: $hello ="hello" condition: #hello>=5 }, rule này thiết lập một điều kiện rằng một biến chuỗi có tên "$hello" phải xuất hiện trong tệp đang được quét, cụ thể là nó tìm kiếm chuỗi "hello".

rule CheckImage { strings: $a ={89 50 4e 47 0d 0a 1a 0a} condition: any of them } rule này dung để check một file png



```
  GNU nano 2.5.3        File: /home/luyenmuc/Desktop/test.yara

rule ConditionsExample {
strings:
                $strings1="hello"
                $strings2="hello"
                $strings3="hello"
condition:
                any of them
}
global rule GlobalRuleExample {
                condition:
                        filesize < 2MB
}
rule NumberStringsExample {
strings:
                $hello = "hello"
condition:
                #hello>=5
}
rule CheckImage {
                          [ Read 29 lines ]
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Spell ^_ Go To Line
```