Lab #4: ClamAV - Yara

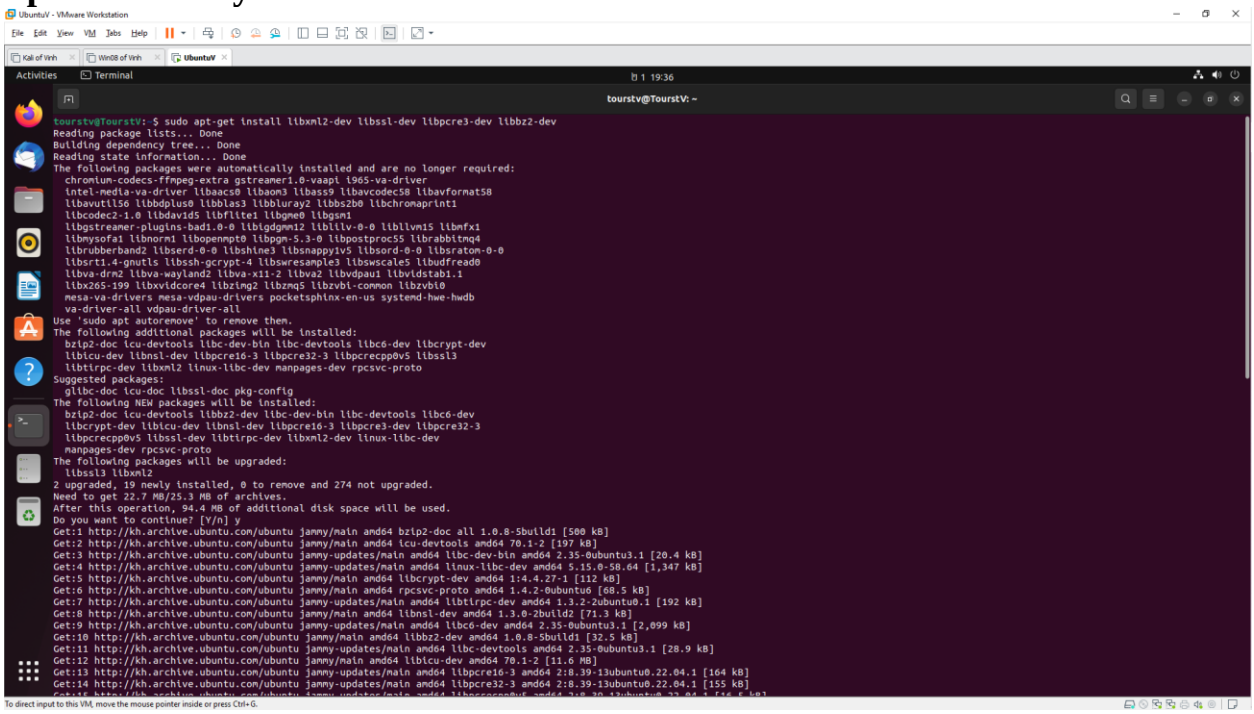
Course Name: Malware Analysis and Reverse Engineering (IAM302)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 1/2/2023

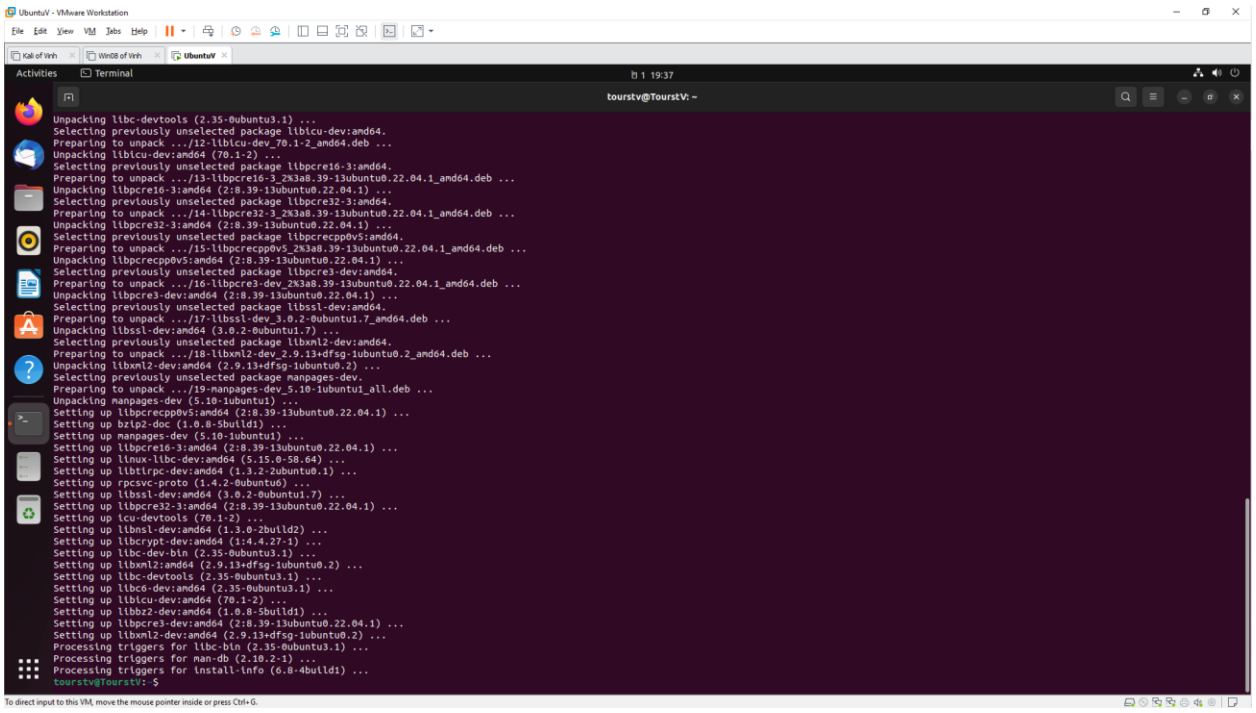
Purpose

Install ClamAV, Yara and scan file

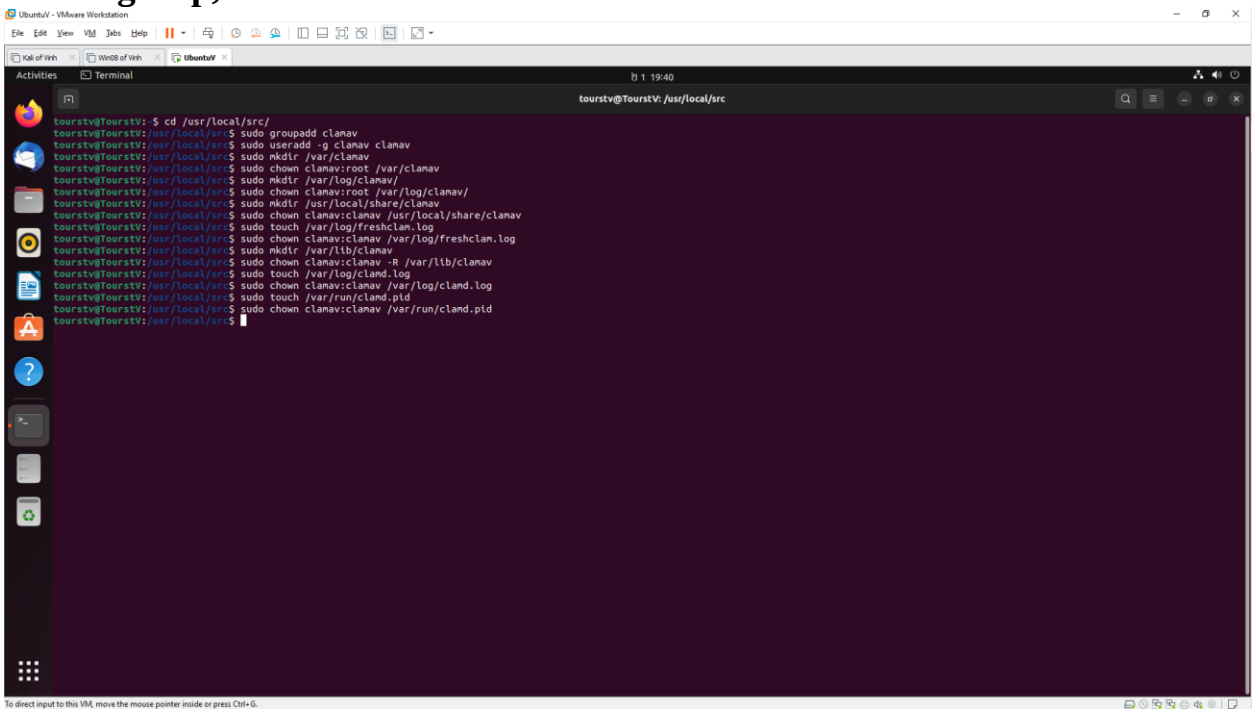
PART 1: ClamAV

Update Library:

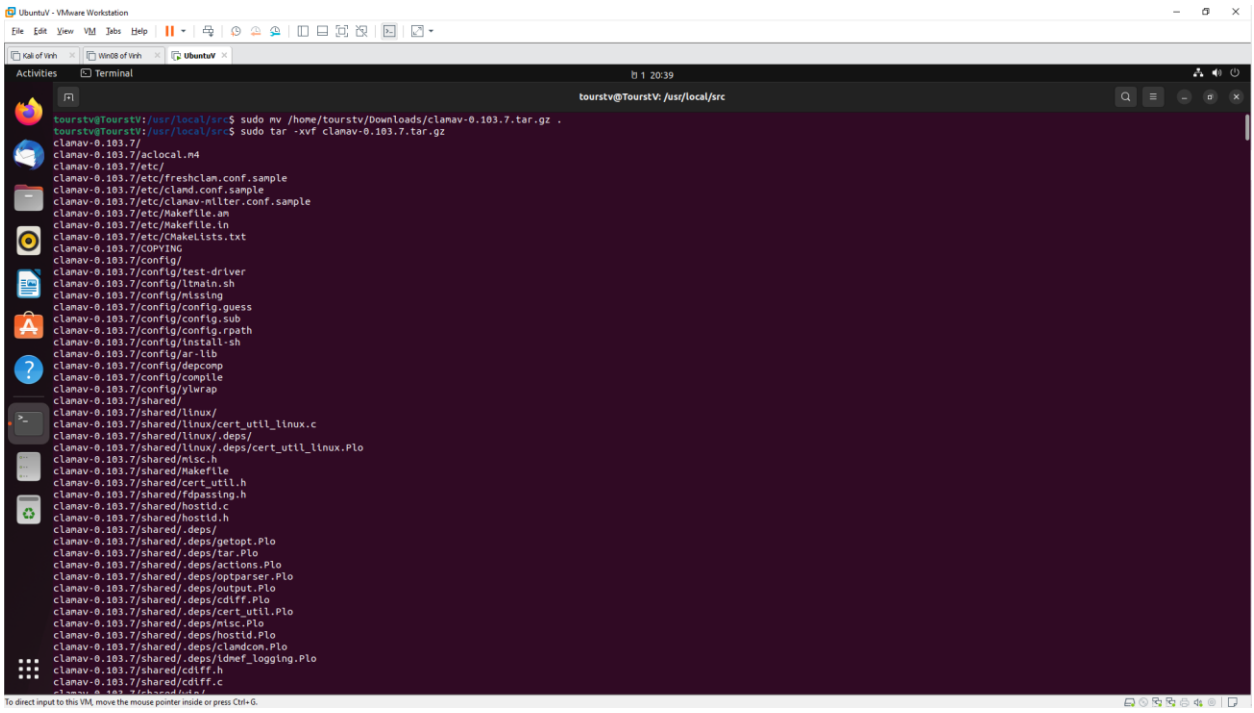




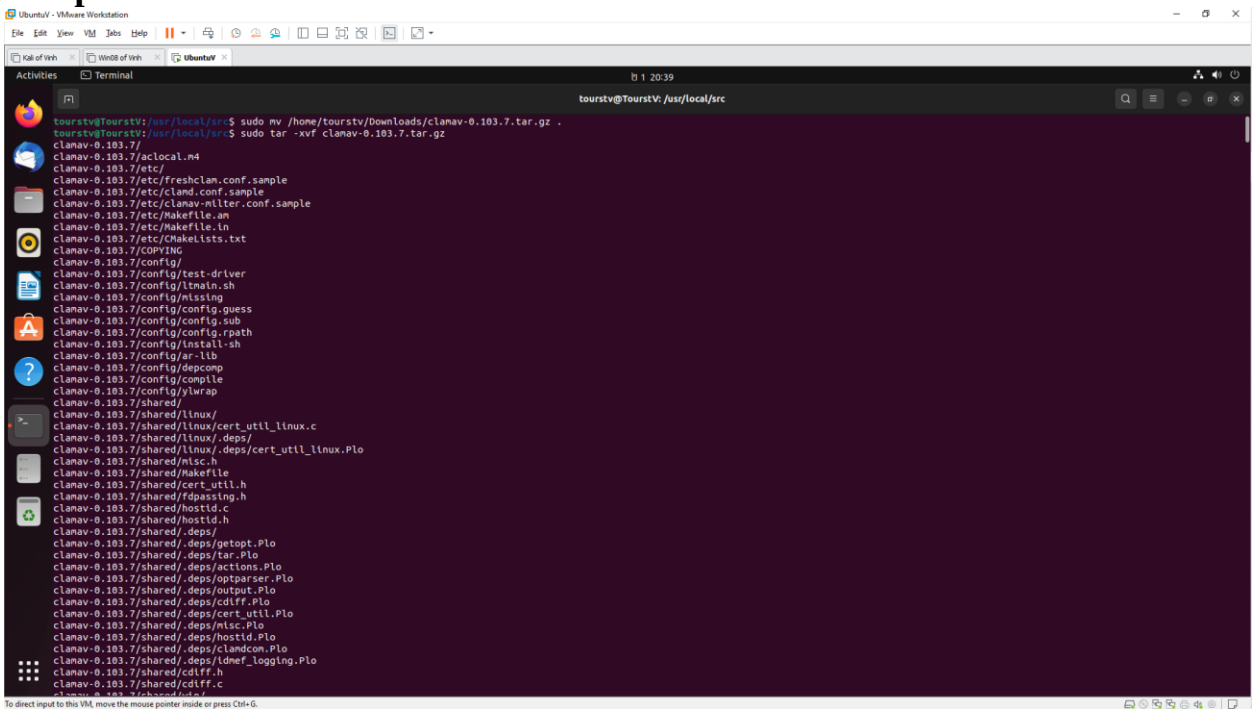
Create group, user and folder:

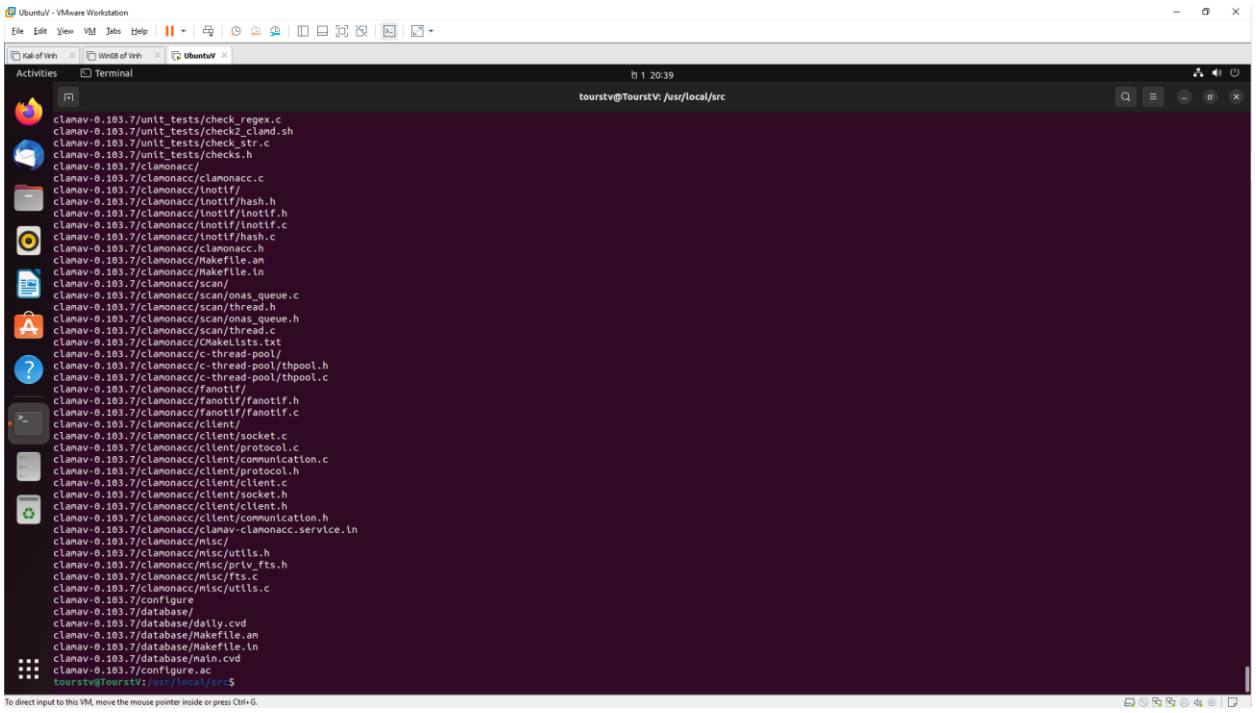


Move file clamav-0.103.7.tar.gz from /home/touristv/Download to /usr/local/src

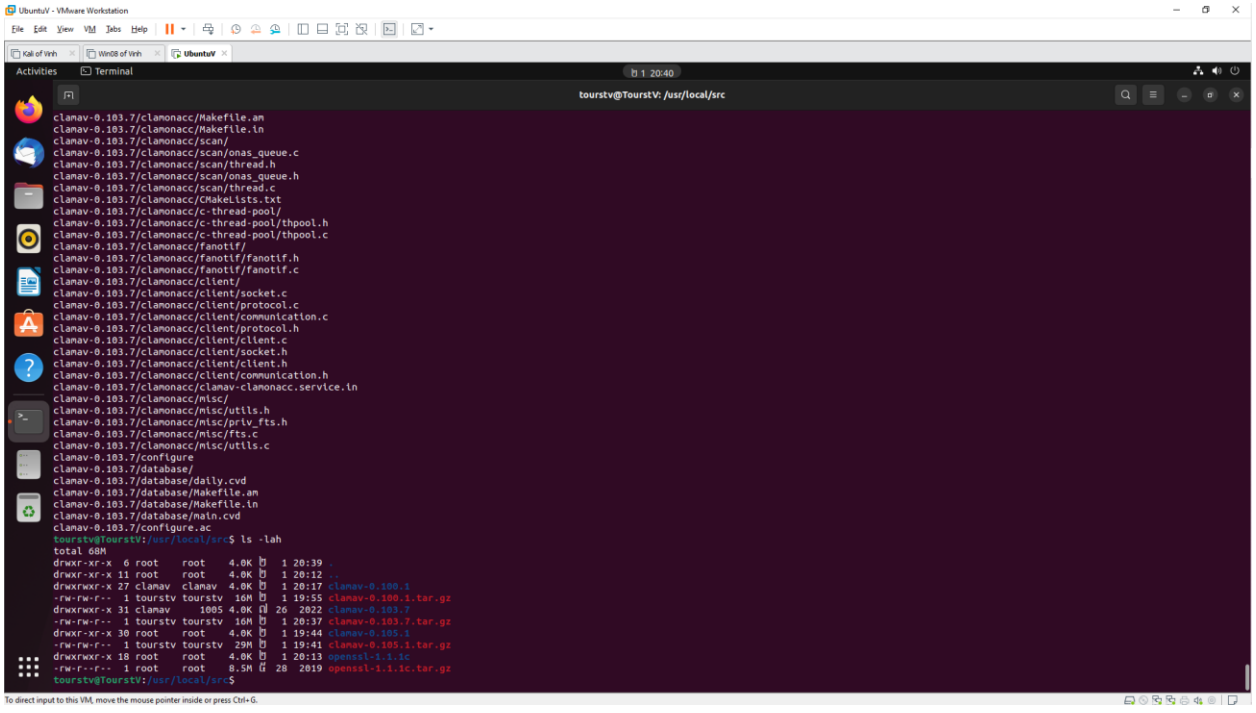

UbuntuV - VMware Workstation
File Edit View VM Tabs Help
Kali of Vinh
Win08 of Vinh
UbuntuV
Activities
Terminal
1 20:39
tourstv@TourstV: /usr/local/src
tourstv@TourstV:/usr/local/src$ sudo mv /home/tourstv/Downloads/clamav-0.103.7.tar.gz .
tourstv@TourstV:/usr/local/src$ sudo tar -xvf clamav-0.103.7.tar.gz
clamav-0.103.7/
clamav-0.103.7/aclocal.m4
clamav-0.103.7/etc/
clamav-0.103.7/etc/freshclam.conf.sample
clamav-0.103.7/etc/clamd.conf.sample
clamav-0.103.7/etc/clamav-milter.conf.sample
clamav-0.103.7/etc/Makefile.am
clamav-0.103.7/etc/Makefile.in
clamav-0.103.7/etc/CMakeLists.txt
clamav-0.103.7/COPYING
clamav-0.103.7/config/
clamav-0.103.7/config/test-driver
clamav-0.103.7/config/ltmain.sh
clamav-0.103.7/config/missing
clamav-0.103.7/config/config.guess
clamav-0.103.7/config/config.sub
clamav-0.103.7/config/config.rpath
clamav-0.103.7/config/install-sh
clamav-0.103.7/config/ar-lib
clamav-0.103.7/config/depcomp
clamav-0.103.7/config/compile
clamav-0.103.7/config/ylwrap
clamav-0.103.7/shared/
clamav-0.103.7/shared/linux/
clamav-0.103.7/shared/linux/cert_util_linux.c
clamav-0.103.7/shared/linux/.deps/
clamav-0.103.7/shared/linux/.deps/cert_util_linux.Plo
clamav-0.103.7/shared/misc.h
clamav-0.103.7/shared/Makefile
clamav-0.103.7/shared/cert_util.h
clamav-0.103.7/shared/fdpassing.h
clamav-0.103.7/shared/hostid.c
clamav-0.103.7/shared/hostid.h
clamav-0.103.7/shared/.deps/
clamav-0.103.7/shared/.deps/getopt.Plo
clamav-0.103.7/shared/.deps/tar.Plo
clamav-0.103.7/shared/.deps/actions.Plo
clamav-0.103.7/shared/.deps/optparser.Plo
clamav-0.103.7/shared/.deps/output.Plo
clamav-0.103.7/shared/.deps/cdiff.Plo
clamav-0.103.7/shared/.deps/cert_util.Plo
clamav-0.103.7/shared/.deps/misc.Plo
clamav-0.103.7/shared/.deps/hostid.Plo
clamav-0.103.7/shared/.deps/clamdcom.Plo
clamav-0.103.7/shared/.deps/idmef_logging.Plo
clamav-0.103.7/shared/cdiff.h
clamav-0.103.7/shared/cdiff.c
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Unzip file

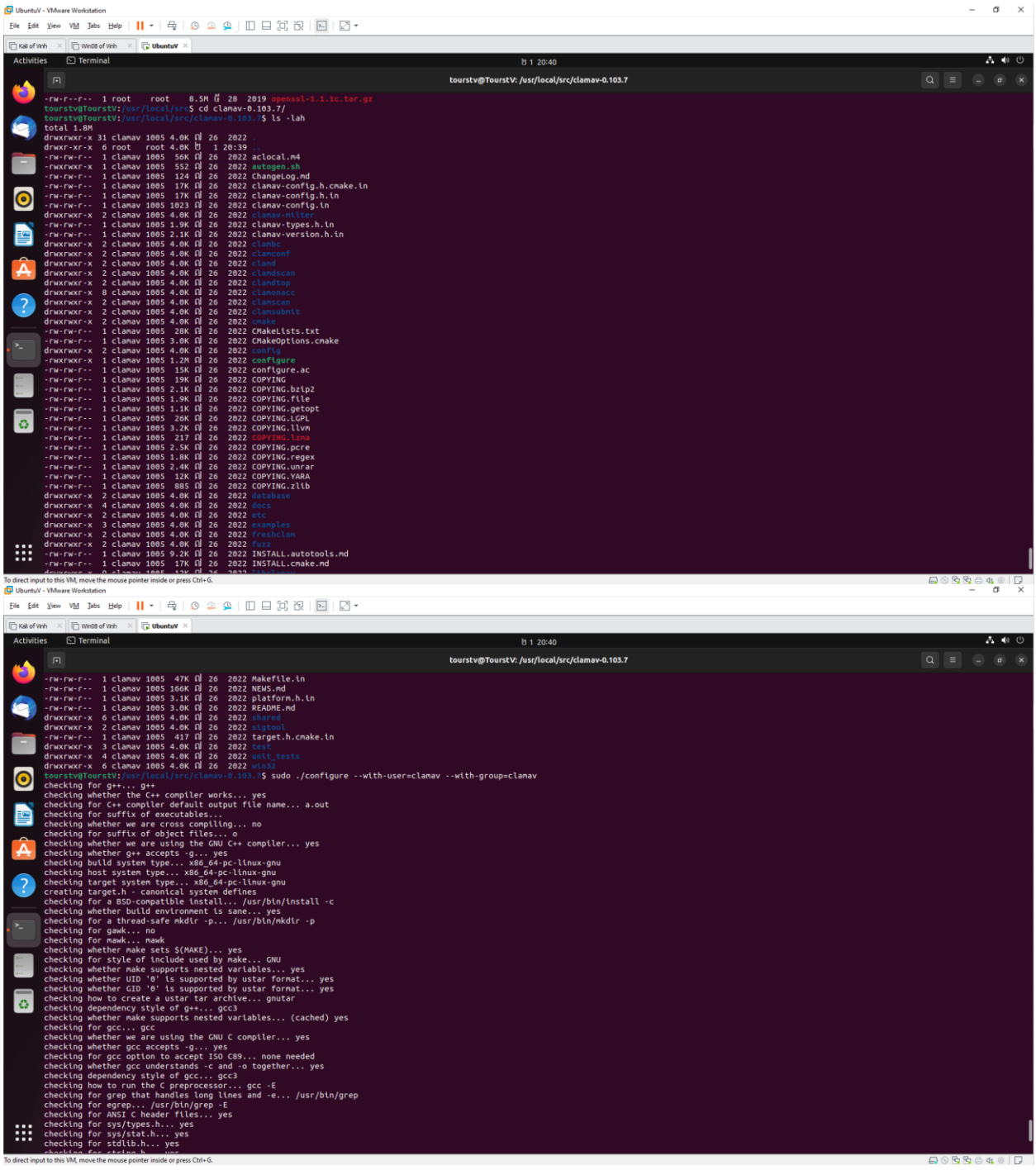

UbuntuV - VMware Workstation
File Edit View VM Tabs Help
Kali of Vinh
Win08 of Vinh
UbuntuV
Activities
Terminal
1 20:39
tourstv@TourstV: /usr/local/src
tourstv@TourstV:/usr/local/src$ sudo mv /home/tourstv/Downloads/clamav-0.103.7.tar.gz .
tourstv@TourstV:/usr/local/src$ sudo tar -xvf clamav-0.103.7.tar.gz
clamav-0.103.7/
clamav-0.103.7/aclocal.m4
clamav-0.103.7/etc/
clamav-0.103.7/etc/freshclam.conf.sample
clamav-0.103.7/etc/clamd.conf.sample
clamav-0.103.7/etc/clamav-milter.conf.sample
clamav-0.103.7/etc/Makefile.am
clamav-0.103.7/etc/Makefile.in
clamav-0.103.7/etc/CMakeLists.txt
clamav-0.103.7/COPYING
clamav-0.103.7/config/
clamav-0.103.7/config/test-driver
clamav-0.103.7/config/ltmain.sh
clamav-0.103.7/config/missing
clamav-0.103.7/config/config.guess
clamav-0.103.7/config/config.sub
clamav-0.103.7/config/config.rpath
clamav-0.103.7/config/install-sh
clamav-0.103.7/config/ar-lib
clamav-0.103.7/config/depcomp
clamav-0.103.7/config/compile
clamav-0.103.7/config/ylwrap
clamav-0.103.7/shared/
clamav-0.103.7/shared/linux/
clamav-0.103.7/shared/linux/cert_util_linux.c
clamav-0.103.7/shared/linux/.deps/
clamav-0.103.7/shared/linux/.deps/cert_util_linux.Plo
clamav-0.103.7/shared/misc.h
clamav-0.103.7/shared/Makefile
clamav-0.103.7/shared/cert_util.h
clamav-0.103.7/shared/fdpassing.h
clamav-0.103.7/shared/hostid.c
clamav-0.103.7/shared/hostid.h
clamav-0.103.7/shared/.deps/
clamav-0.103.7/shared/.deps/getopt.Plo
clamav-0.103.7/shared/.deps/tar.Plo
clamav-0.103.7/shared/.deps/actions.Plo
clamav-0.103.7/shared/.deps/optparser.Plo
clamav-0.103.7/shared/.deps/output.Plo
clamav-0.103.7/shared/.deps/cdiff.Plo
clamav-0.103.7/shared/.deps/cert_util.Plo
clamav-0.103.7/shared/.deps/misc.Plo
clamav-0.103.7/shared/.deps/hostid.Plo
clamav-0.103.7/shared/.deps/clamdcom.Plo
clamav-0.103.7/shared/.deps/idmef_logging.Plo
clamav-0.103.7/shared/cdiff.h
clamav-0.103.7/shared/cdiff.c
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



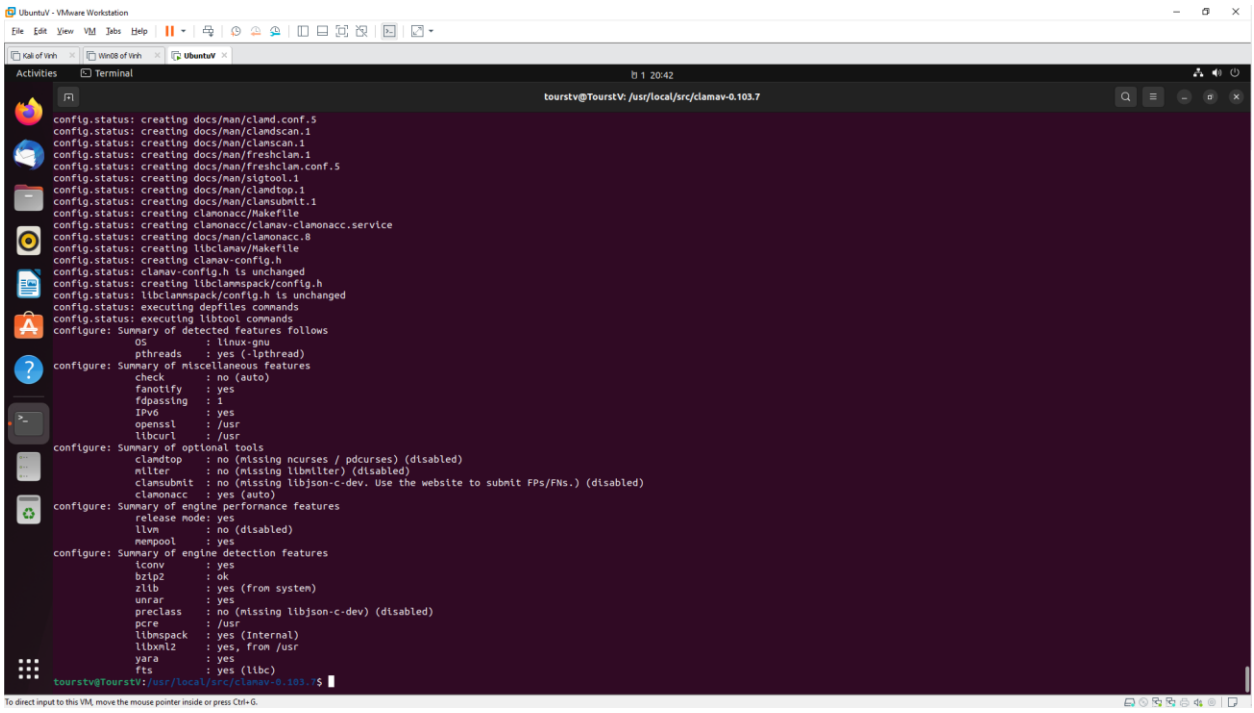
List all file



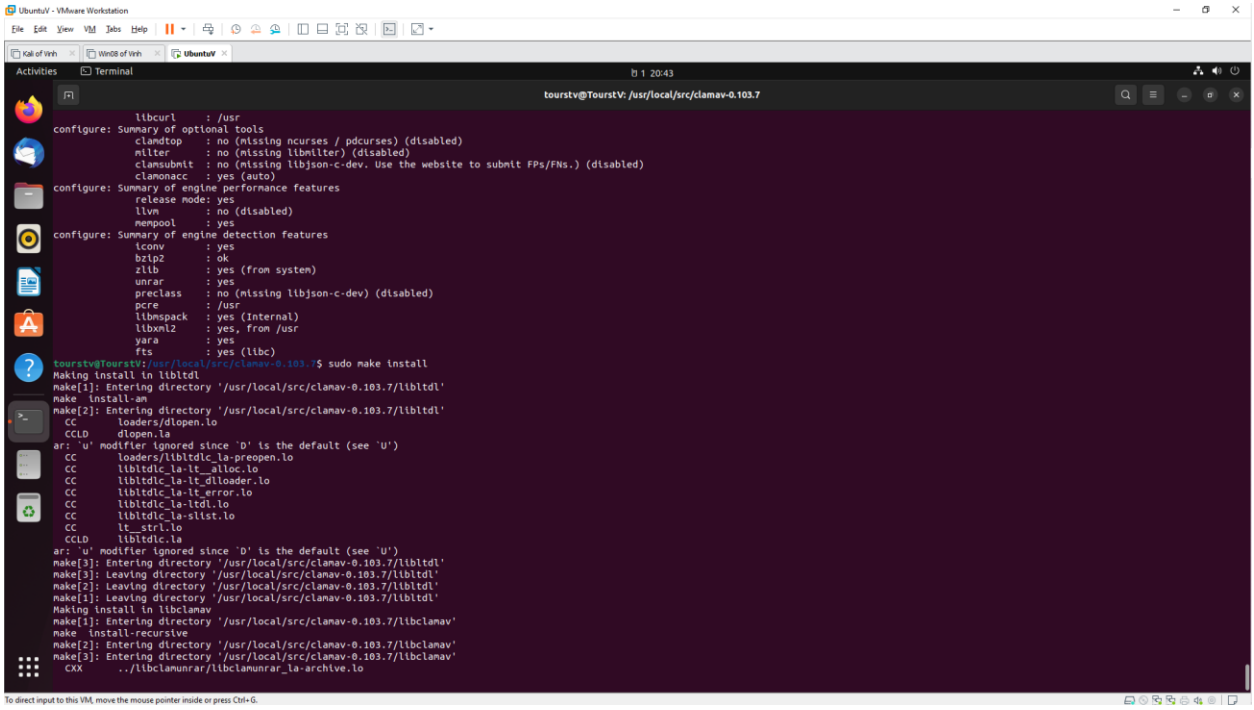
Go into folder and configure


UbuntuV - VMware Workstation
File Edit View VM Tabs Help
Kali of Vnh
Win08 of Vnh
UbuntuV
Activities
Terminal
1 20:40
tourstv@TourstV: /usr/local/src/clamav-0.103.7
-rw-r--r-- 1 root root 8.5M 月 28 2019 openssl-1.1.1c.tar.gz
tourstv@TourstV:/usr/local/src$ cd clamav-0.103.7/
tourstv@TourstV:/usr/local/src/clamav-0.103.7$ ls -lah
total 1.8M
drwxrwxr-x 31 clamav 1005 4.0K 月 26 2022 .
drwxr-xr-x 6 root root 4.0K 下 1 20:39 ..
-rw-rw-r-- 1 clamav 1005 56K 月 26 2022 aclocal.m4
-rwxrwxr-x 1 clamav 1005 552 月 26 2022 autogen.sh
-rw-rw-r-- 1 clamav 1005 124 月 26 2022 ChangeLog.md
-rw-rw-r-- 1 clamav 1005 17K 月 26 2022 clamav-config.h.cmake.in
-rw-rw-r-- 1 clamav 1005 17K 月 26 2022 clamav-config.h.in
-rw-rw-r-- 1 clamav 1005 1023 月 26 2022 clamav-config.in
drwxrwxr-x 2 clamav 1005 4.0K 月 26 2022 clamav-milter
-rw-rw-r-- 1 clamav 1005 1.9K 月 26 2022 clamav-types.h.in
-rw-rw-r-- 1 clamav 1005 2.1K 月 26 2022 clamav-version.h.in
drwxrwxr-x 2 clamav 1005 4.0K 月 26 2022 clambc
drwxrwxr-x 2 clamav 1005 4.0K 月 26 2022 clamconf
drwxrwxr-x 2 clamav 1005 4.0K 月 26 2022 clamd
drwxrwxr-x 2 clamav 1005 4.0K 月 26 2022 clamdscan
drwxrwxr-x 2 clamav 1005 4.0K 月 26 2022 clamdtop
drwxrwxr-x 8 clamav 1005 4.0K 月 26 2022 clamonacc
drwxrwxr-x 2 clamav 1005 4.0K 月 26 2022 clamscan
drwxrwxr-x 2 clamav 1005 4.0K 月 26 2022 clamsubmit
drwxrwxr-x 2 clamav 1005 4.0K 月 26 2022 cmake
-rw-rw-r-- 1 clamav 1005 28K 月 26 2022 CMakeLists.txt
-rw-rw-r-- 1 clamav 1005 3.0K 月 26 2022 CMakeOptions.cmake
drwxrwxr-x 2 clamav 1005 4.0K 月 26 2022 config
-rwxrwxr-x 1 clamav 1005 1.2M 月 26 2022 configure
-rw-rw-r-- 1 clamav 1005 15K 月 26 2022 configure.ac
-rw-rw-r-- 1 clamav 1005 19K 月 26 2022 COPYING
-rw-rw-r-- 1 clamav 1005 2.1K 月 26 2022 COPYING.bzip2
-rw-rw-r-- 1 clamav 1005 1.9K 月 26 2022 COPYING.file
-rw-rw-r-- 1 clamav 1005 1.1K 月 26 2022 COPYING.getopt
-rw-rw-r-- 1 clamav 1005 26K 月 26 2022 COPYING.LGPL
-rw-rw-r-- 1 clamav 1005 3.2K 月 26 2022 COPYING.llvm
-rw-rw-r-- 1 clamav 1005 217 月 26 2022 COPYING.lzma
-rw-rw-r-- 1 clamav 1005 2.5K 月 26 2022 COPYING.pcre
-rw-rw-r-- 1 clamav 1005 1.8K 月 26 2022 COPYING.regex
-rw-rw-r-- 1 clamav 1005 2.4K 月 26 2022 COPYING.unrar
-rw-rw-r-- 1 clamav 1005 12K 月 26 2022 COPYING.YARA
-rw-rw-r-- 1 clamav 1005 885 月 26 2022 COPYING.zlib
drwxrwxr-x 2 clamav 1005 4.0K 月 26 2022 database
drwxrwxr-x 4 clamav 1005 4.0K 月 26 2022 docs
drwxrwxr-x 2 clamav 1005 4.0K 月 26 2022 etc
drwxrwxr-x 3 clamav 1005 4.0K 月 26 2022 examples
drwxrwxr-x 2 clamav 1005 4.0K 月 26 2022 freshclam
drwxrwxr-x 2 clamav 1005 4.0K 月 26 2022 fuzz
-rw-rw-r-- 1 clamav 1005 9.2K 月 26 2022 INSTALL.autotools.md
-rw-rw-r-- 1 clamav 1005 17K 月 26 2022 INSTALL.cmake.md
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

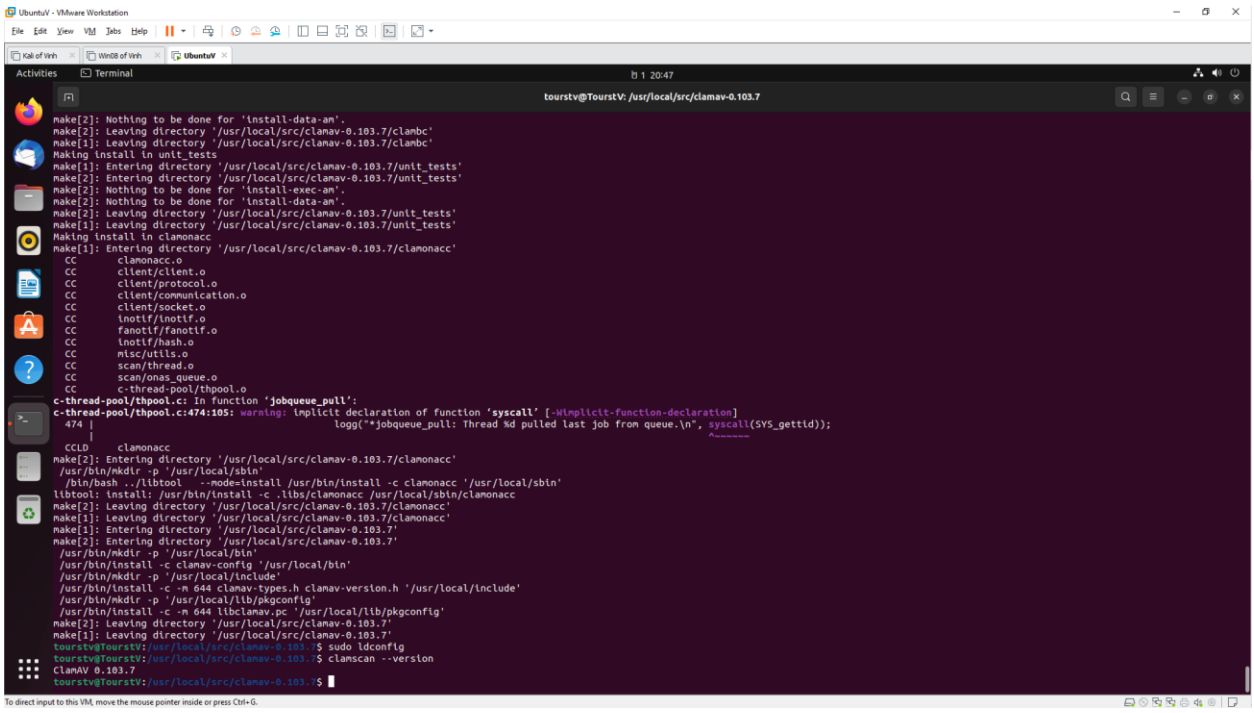
UbuntuV - VMware Workstation
File Edit View VM Tabs Help
Kali of Vnh
Win08 of Vnh
UbuntuV
Activities
Terminal
1 20:40
tourstv@TourstV: /usr/local/src/clamav-0.103.7
-rw-rw-r-- 1 clamav 1005 47K 月 26 2022 Makefile.in
-rw-rw-r-- 1 clamav 1005 166K 月 26 2022 NEWS.md
-rw-rw-r-- 1 clamav 1005 3.1K 月 26 2022 platform.h.in
-rw-rw-r-- 1 clamav 1005 3.0K 月 26 2022 README.md
drwxrwxr-x 6 clamav 1005 4.0K 月 26 2022 shared
drwxrwxr-x 2 clamav 1005 4.0K 月 26 2022 sigtool
-rw-rw-r-- 1 clamav 1005 417 月 26 2022 target.h.cmake.in
drwxrwxr-x 3 clamav 1005 4.0K 月 26 2022 test
drwxrwxr-x 4 clamav 1005 4.0K 月 26 2022 unit_tests
drwxrwxr-x 6 clamav 1005 4.0K 月 26 2022 win32
tourstv@TourstV:/usr/local/src/clamav-0.103.7$ sudo ./configure --with-user=clamav --with-group=clamav
checking for g++... g++
checking whether the C++ compiler works... yes
checking for C++ compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C++ compiler... yes
checking whether g++ accepts -g... yes
checking build system type... x86_64-pc-linux-gnu
checking host system type... x86_64-pc-linux-gnu
checking target system type... x86_64-pc-linux-gnu
creating target.h - canonical system defines
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... no
checking for mawk... mawk
checking whether make sets $(MAKE)... yes
checking for style of include used by make... GNU
checking whether make supports nested variables... yes
checking whether UID '0' is supported by ustar format... yes
checking whether GID '0' is supported by ustar format... yes
checking how to create a ustar tar archive... gnutar
checking dependency style of g++... gcc3
checking whether make supports nested variables... (cached) yes
checking for gcc... gcc
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking whether gcc understands -c and -o together... yes
checking dependency style of gcc... gcc3
checking how to run the C preprocessor... gcc -E
checking for grep that handles long lines and -e... /usr/bin/grep
checking for egrep... /usr/bin/grep -E
checking for ANSI C header files... yes
checking for sys/types.h... yes
checking for sys/stat.h... yes
checking for stdlib.h... yes
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



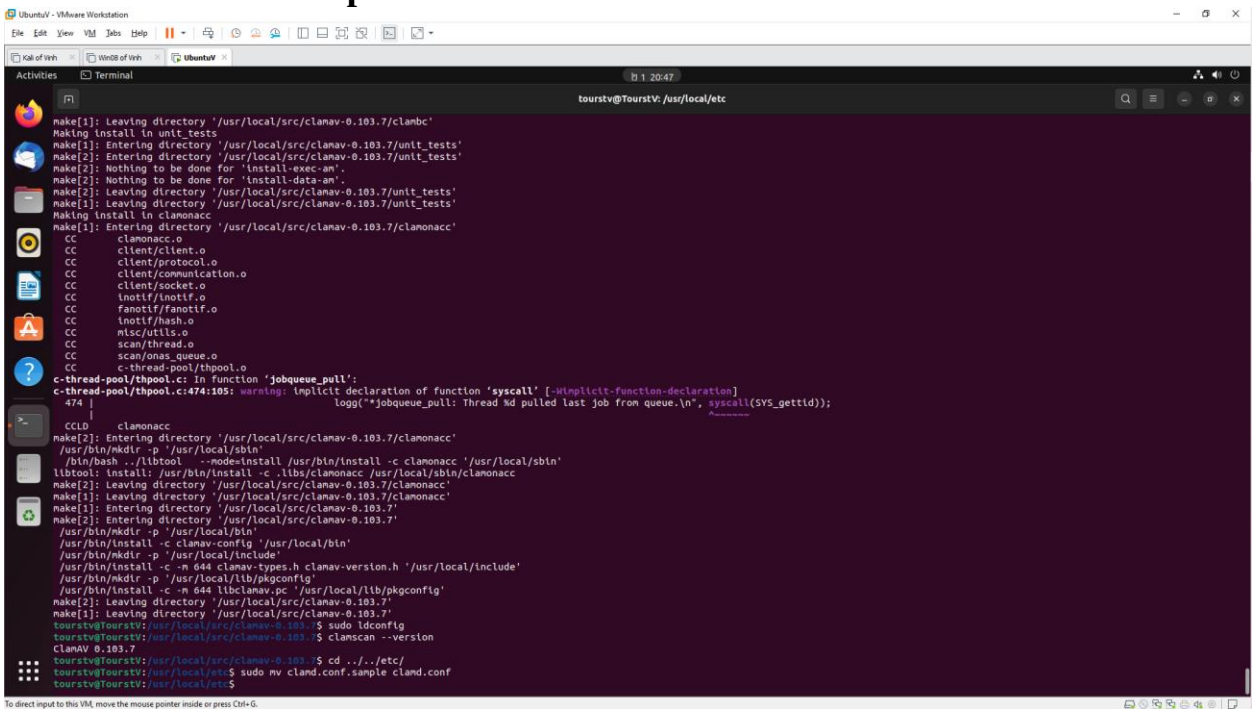
Sudo make command



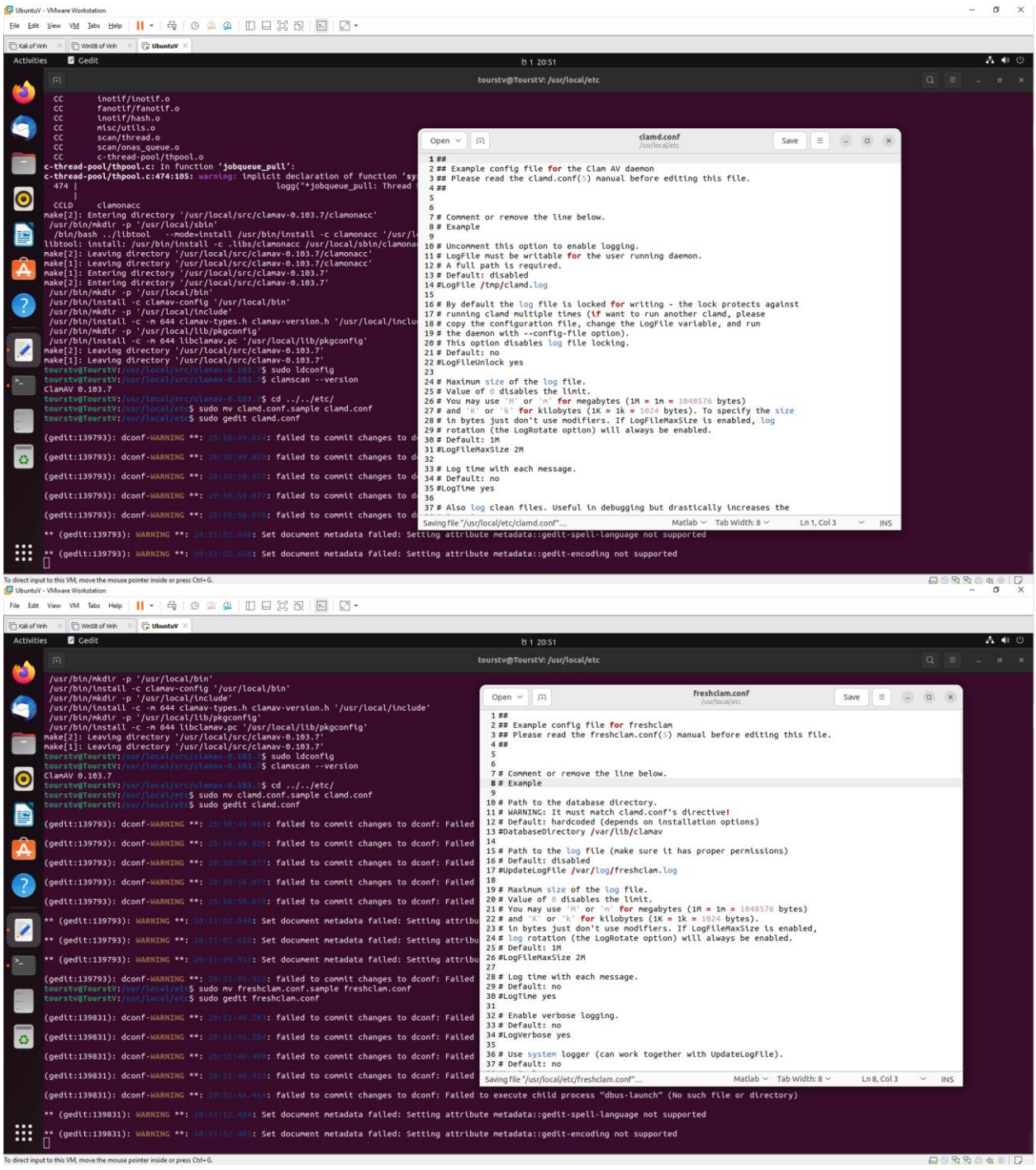
Check version



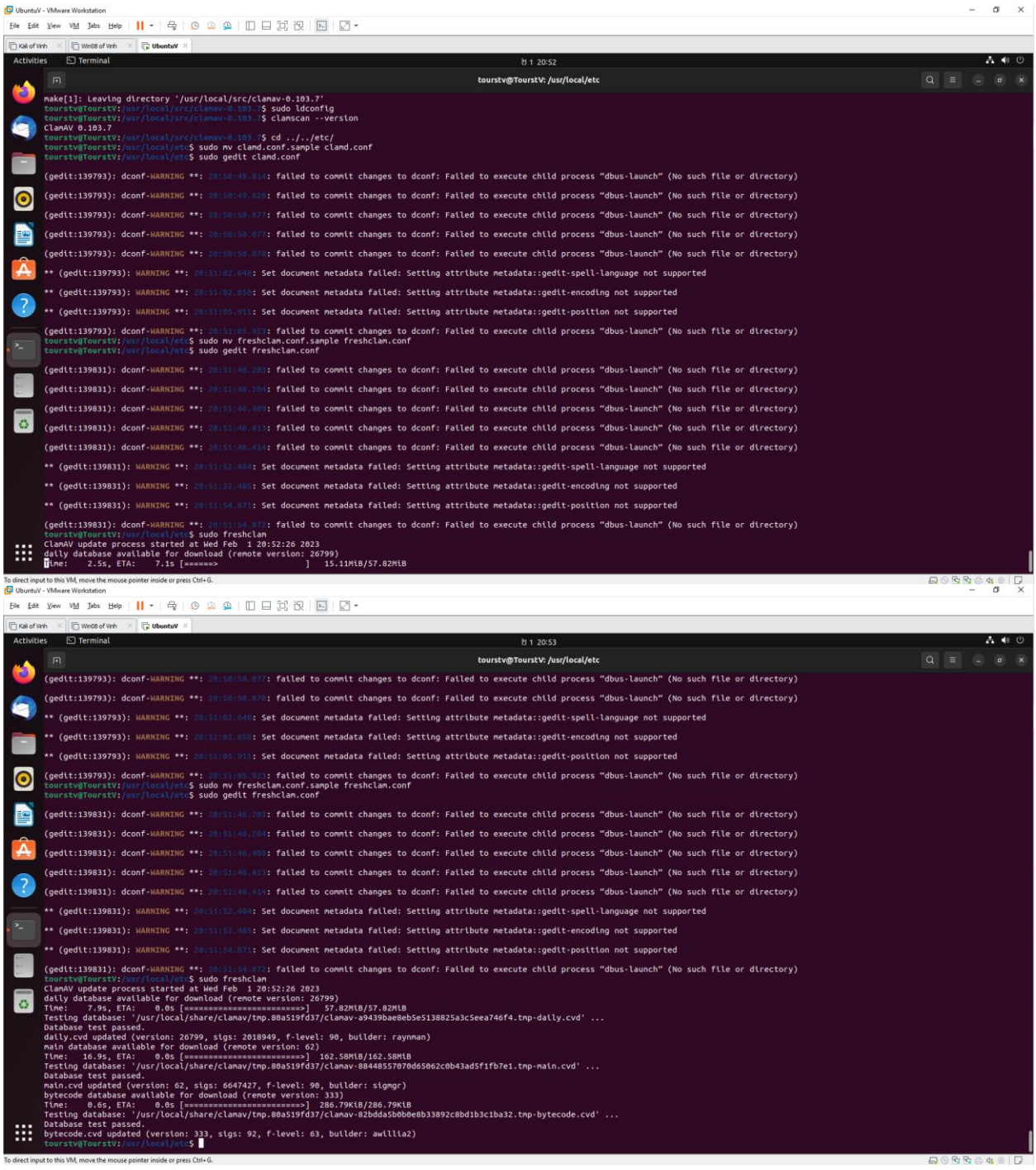
Move clamd.conf.sample to clamd.conf



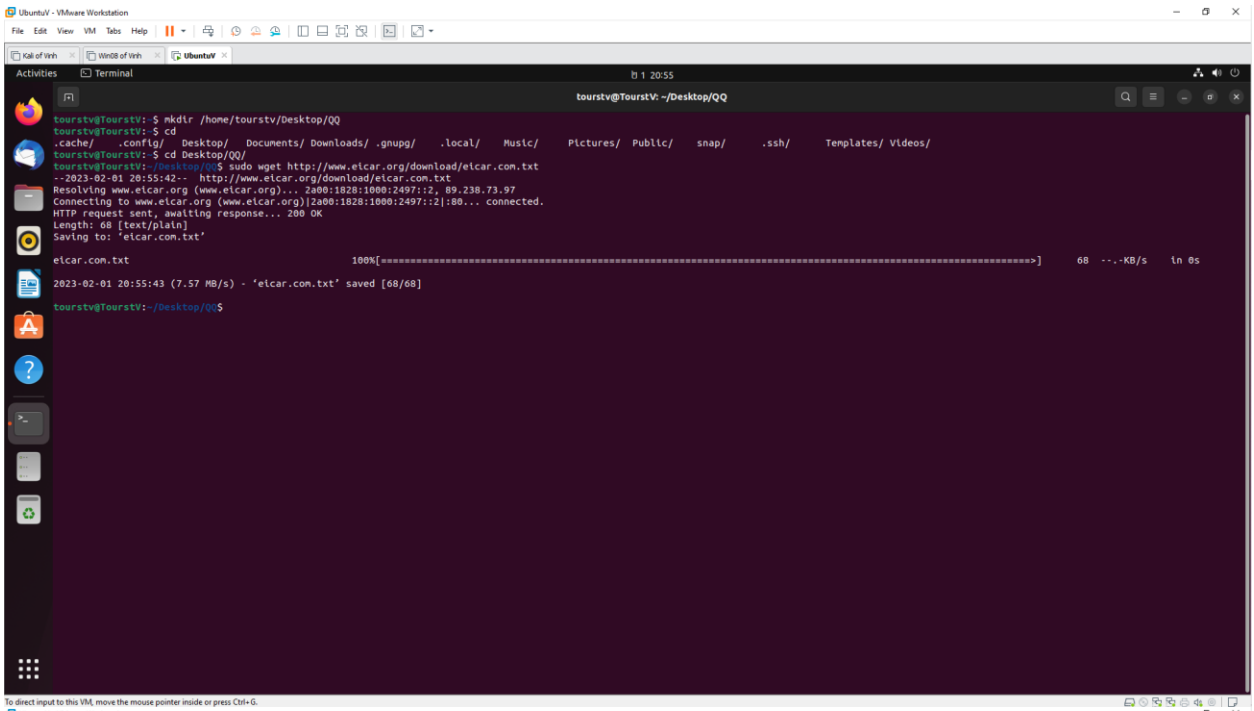
Delete example

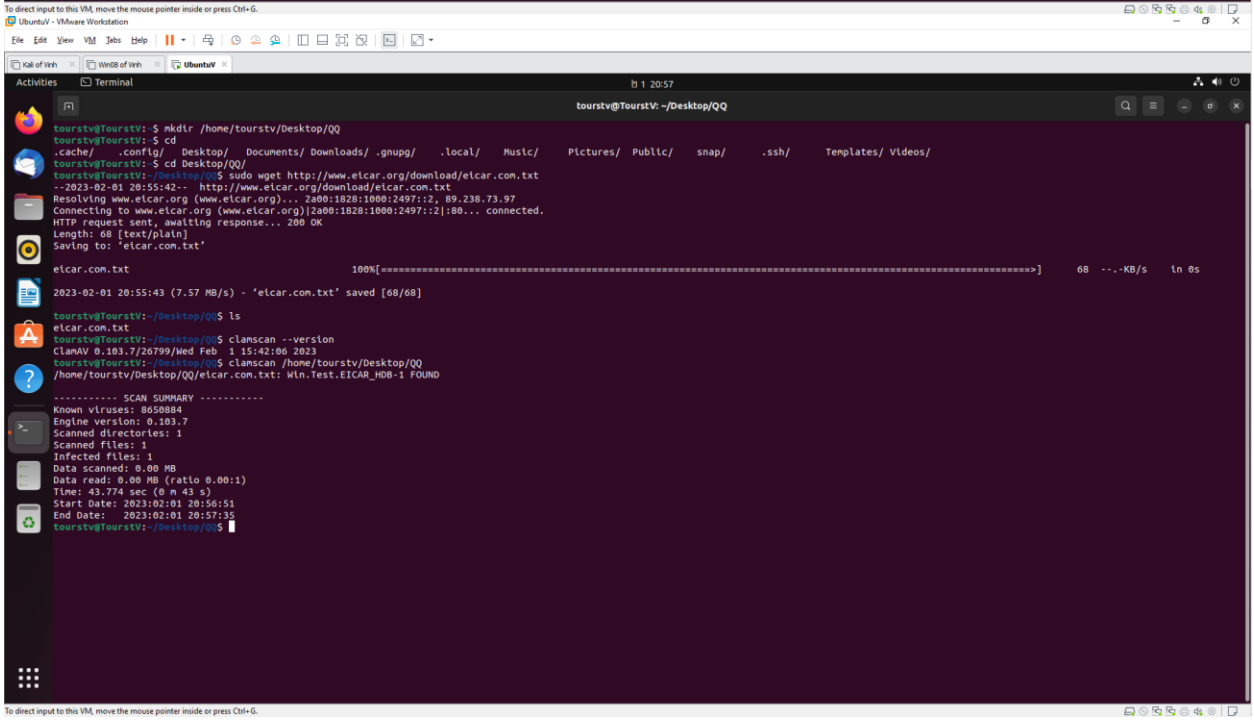


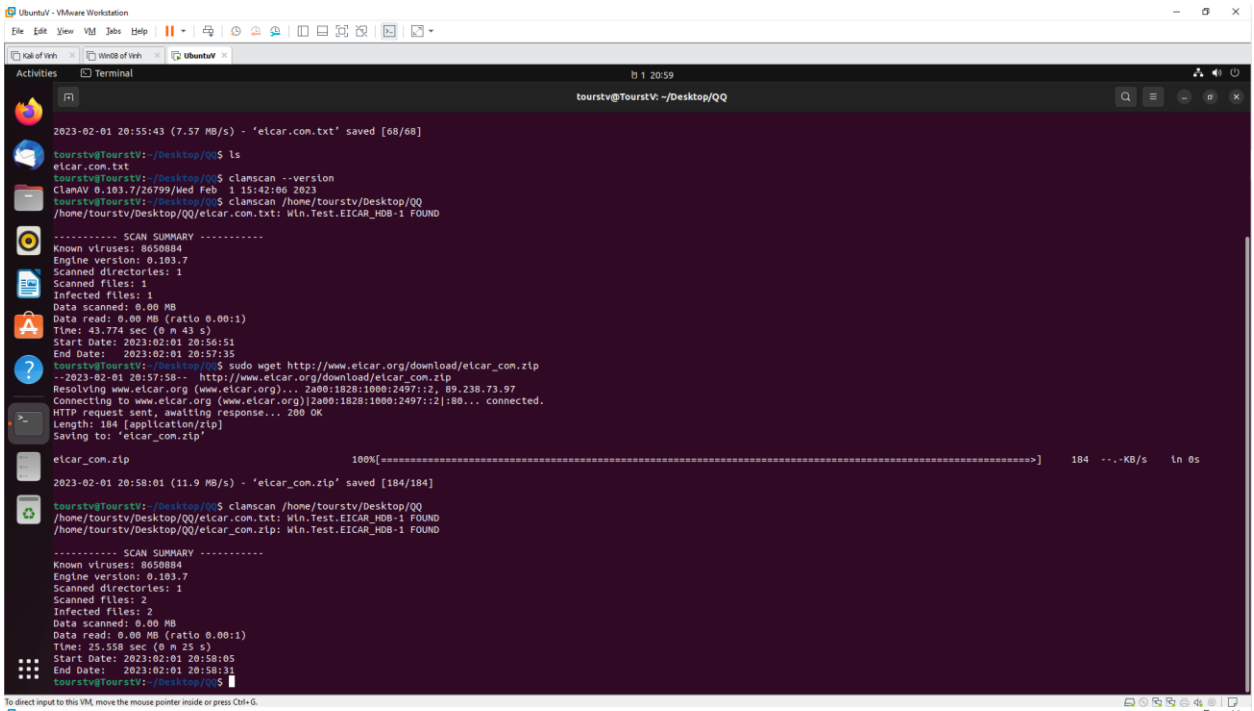
Install freshclam

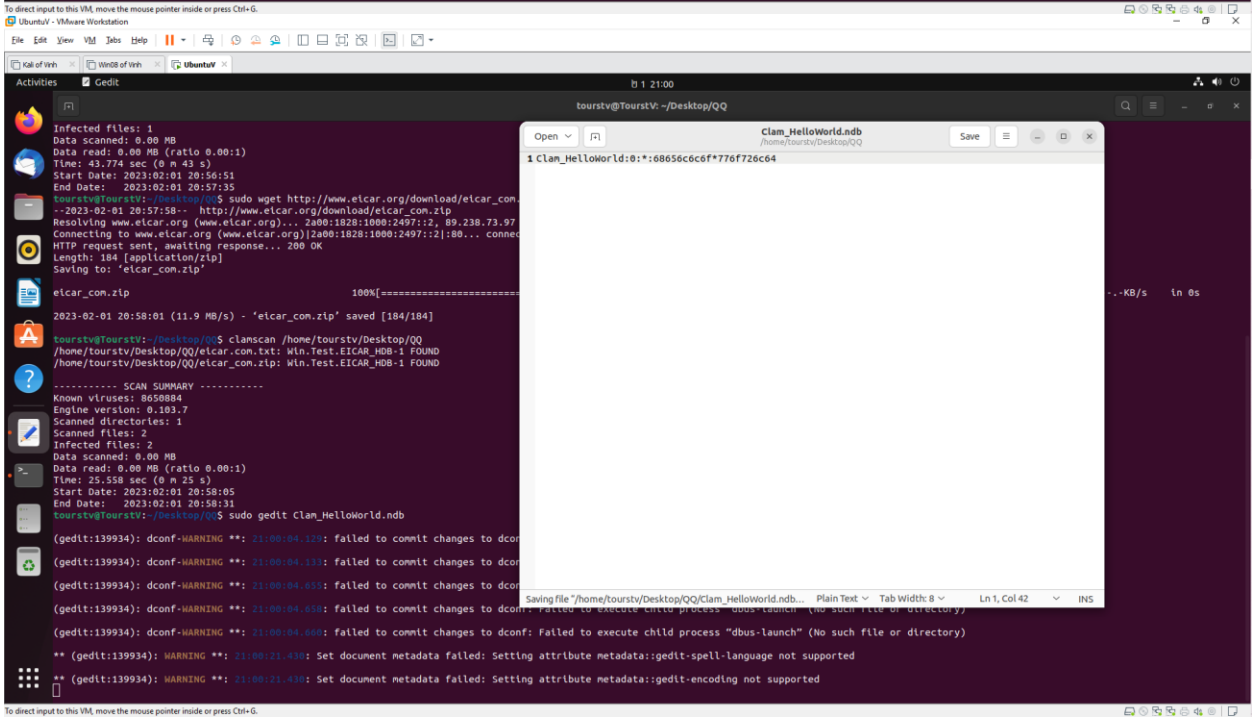

UbuntuV - VMware Workstation
File Edit View VM Tabs Help
Kali of Vmh
Win08 of Vmh
UbuntuV
Activities
Terminal
1 20:52
tourstv@TourstV: /usr/local/etc
make[1]: Leaving directory '/usr/local/src/clamav-0.103.7'
tourstv@TourstV:/usr/local/src/clamav-0.103.7$ sudo ldconfig
tourstv@TourstV:/usr/local/src/clamav-0.103.7$ clamscan --version
ClamAV 0.103.7
tourstv@TourstV:/usr/local/src/clamav-0.103.7$ cd ../../etc/
tourstv@TourstV:/usr/local/etc$ sudo mv clamd.conf.sample clamd.conf
tourstv@TourstV:/usr/local/etc$ sudo gedit clamd.conf
(gedit:139793): dconf-WARNING **: 20:50:49.814: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139793): dconf-WARNING **: 20:50:49.820: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139793): dconf-WARNING **: 20:50:50.077: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139793): dconf-WARNING **: 20:50:50.077: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139793): dconf-WARNING **: 20:50:50.078: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
** (gedit:139793): WARNING **: 20:51:02.648: Set document metadata failed: Setting attribute metadata::gedit-spell-language not supported
** (gedit:139793): WARNING **: 20:51:02.658: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:139793): WARNING **: 20:51:05.911: Set document metadata failed: Setting attribute metadata::gedit-position not supported
(gedit:139793): dconf-WARNING **: 20:51:05.923: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
tourstv@TourstV:/usr/local/etc$ sudo mv freshclam.conf.sample freshclam.conf
tourstv@TourstV:/usr/local/etc$ sudo gedit freshclam.conf
(gedit:139831): dconf-WARNING **: 20:51:46.203: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139831): dconf-WARNING **: 20:51:46.204: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139831): dconf-WARNING **: 20:51:46.409: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139831): dconf-WARNING **: 20:51:46.413: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139831): dconf-WARNING **: 20:51:46.414: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
** (gedit:139831): WARNING **: 20:51:52.484: Set document metadata failed: Setting attribute metadata::gedit-spell-language not supported
** (gedit:139831): WARNING **: 20:51:52.485: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:139831): WARNING **: 20:51:54.871: Set document metadata failed: Setting attribute metadata::gedit-position not supported
(gedit:139831): dconf-WARNING **: 20:51:54.872: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
tourstv@TourstV:/usr/local/etc$ sudo freshclam
ClamAV update process started at Wed Feb 1 20:52:26 2023
daily database available for download (remote version: 26799)
Time: 2.5s, ETA: 7.1s [======>] 15.11MiB/57.82MiB
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
UbuntuV - VMware Workstation
File Edit View VM Tabs Help
Kali of Vmh
Win08 of Vmh
UbuntuV
Activities
Terminal
1 20:53
tourstv@TourstV: /usr/local/etc
(gedit:139793): dconf-WARNING **: 20:50:50.077: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139793): dconf-WARNING **: 20:50:50.078: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
** (gedit:139793): WARNING **: 20:51:02.648: Set document metadata failed: Setting attribute metadata::gedit-spell-language not supported
** (gedit:139793): WARNING **: 20:51:02.658: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:139793): WARNING **: 20:51:05.911: Set document metadata failed: Setting attribute metadata::gedit-position not supported
(gedit:139793): dconf-WARNING **: 20:51:05.923: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
tourstv@TourstV:/usr/local/etc$ sudo mv freshclam.conf.sample freshclam.conf
tourstv@TourstV:/usr/local/etc$ sudo gedit freshclam.conf
(gedit:139831): dconf-WARNING **: 20:51:46.203: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139831): dconf-WARNING **: 20:51:46.204: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139831): dconf-WARNING **: 20:51:46.409: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139831): dconf-WARNING **: 20:51:46.413: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139831): dconf-WARNING **: 20:51:46.414: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
** (gedit:139831): WARNING **: 20:51:52.484: Set document metadata failed: Setting attribute metadata::gedit-spell-language not supported
** (gedit:139831): WARNING **: 20:51:52.485: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:139831): WARNING **: 20:51:54.871: Set document metadata failed: Setting attribute metadata::gedit-position not supported
(gedit:139831): dconf-WARNING **: 20:51:54.872: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
tourstv@TourstV:/usr/local/etc$ sudo freshclam
ClamAV update process started at Wed Feb 1 20:52:26 2023
daily database available for download (remote version: 26799)
Time: 7.9s, ETA: 0.0s [========================>] 57.82MiB/57.82MiB
Testing database: '/usr/local/share/clamav/tmp.80a519fd37/clamav-a9439bae8eb5e5138825a3c5eea746f4.tmp-daily.cvd' ...
Database test passed.
daily.cvd updated (version: 26799, sigs: 2018949, f-level: 90, builder: raynman)
main database available for download (remote version: 62)
Time: 16.9s, ETA: 0.0s [========================>] 162.58MiB/162.58MiB
Testing database: '/usr/local/share/clamav/tmp.80a519fd37/clamav-88448557070d65062c0b43ad5f1fb7e1.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: 333)
Time: 0.6s, ETA: 0.0s [========================>] 286.79KiB/286.79KiB
Testing database: '/usr/local/share/clamav/tmp.80a519fd37/clamav-82bdda5b0b0e8b33892c8bd1b3c1ba32.tmp-bytecode.cvd' ...
Database test passed.
bytecode.cvd updated (version: 333, sigs: 92, f-level: 63, builder: awillia2)
tourstv@TourstV:/usr/local/etc$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

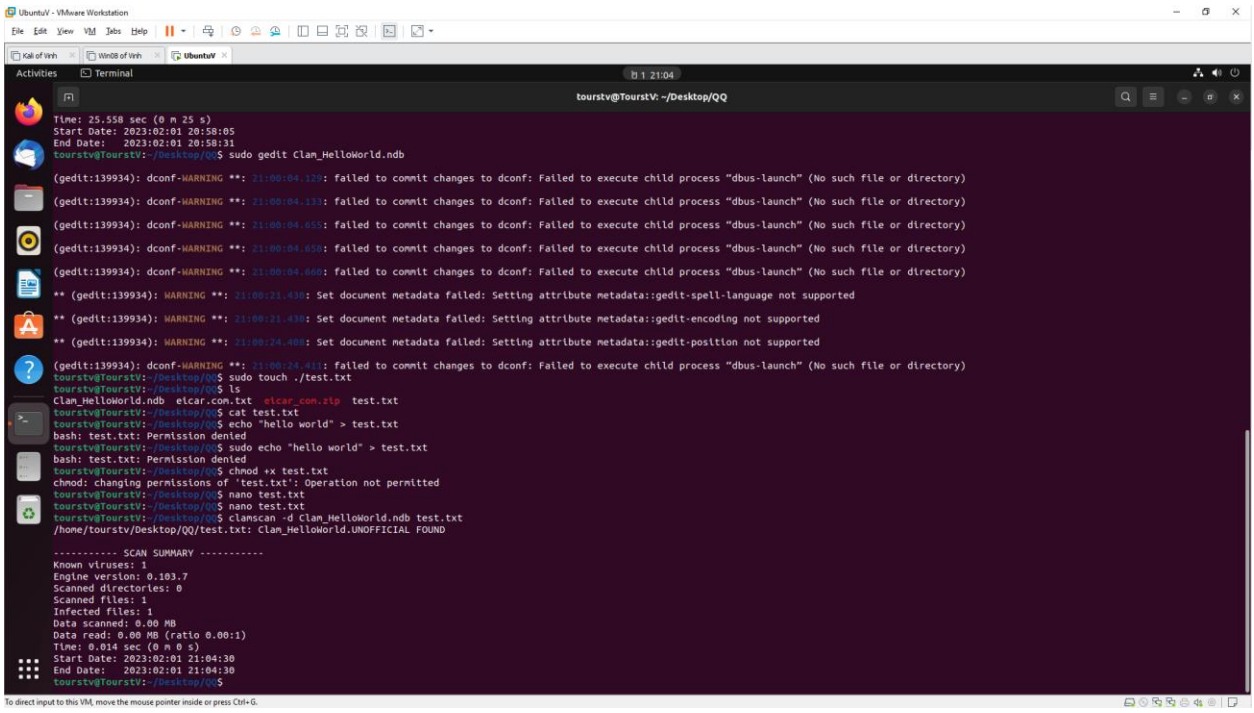
Test


UbuntuV - VMware Workstation
File Edit View VM Tabs Help
Kali of Vinh
Win08 of Vinh
UbuntuV
Activities
Terminal
1 20:55
tourstv@TourstV: ~/Desktop/QQ
tourstv@TourstV:~$ mkdir /home/tourstv/Desktop/QQ
tourstv@TourstV:~$ cd
.cache/ .config/ Desktop/ Documents/ Downloads/ .gnupg/ .local/ Music/ Pictures/ Public/ snap/ .ssh/ Templates/ Videos/
tourstv@TourstV:~$ cd Desktop/QQ/
tourstv@TourstV:~/Desktop/QQ$ sudo wget http://www.eicar.org/download/eicar.com.txt
--2023-02-01 20:55:42-- http://www.eicar.org/download/eicar.com.txt
Resolving www.eicar.org (www.eicar.org)... 2a00:1828:1000:2497::2, 89.238.73.97
Connecting to www.eicar.org (www.eicar.org)|2a00:1828:1000:2497::2|:80... 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
2023-02-01 20:55:43 (7.57 MB/s) - 'eicar.com.txt' saved [68/68]
tourstv@TourstV:~/Desktop/QQ$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


UbuntuV - VMware Workstation
File Edit View VM Tabs Help
Kali of Vinh
Win08 of Vinh
UbuntuV
Activities
Terminal
1 20:57
tourstv@TourstV: ~/Desktop/QQ
tourstv@TourstV:~$ mkdir /home/tourstv/Desktop/QQ
tourstv@TourstV:~$ cd
.cache/ .config/ Desktop/ Documents/ Downloads/ .gnupg/ .local/ Music/ Pictures/ Public/ snap/ .ssh/ Templates/ Videos/
tourstv@TourstV:~$ cd Desktop/QQ/
tourstv@TourstV:~/Desktop/QQ$ sudo wget http://www.eicar.org/download/eicar.com.txt
--2023-02-01 20:55:42-- http://www.eicar.org/download/eicar.com.txt
Resolving www.eicar.org (www.eicar.org)... 2a00:1828:1000:2497::2, 89.238.73.97
Connecting to www.eicar.org (www.eicar.org)|2a00:1828:1000:2497::2|:80... 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
2023-02-01 20:55:43 (7.57 MB/s) - 'eicar.com.txt' saved [68/68]
tourstv@TourstV:~/Desktop/QQ$ ls
eicar.com.txt
tourstv@TourstV:~/Desktop/QQ$ clamscan --version
ClamAV 0.103.7/26799/Wed Feb 1 15:42:06 2023
tourstv@TourstV:~/Desktop/QQ$ clamscan /home/tourstv/Desktop/QQ
/home/tourstv/Desktop/QQ/eicar.com.txt: Win.Test.EICAR_HDB-1 FOUND
---------- SCAN SUMMARY ----------
Known viruses: 8650884
Engine version: 0.103.7
Scanned directories: 1
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 43.774 sec (0 m 43 s)
Start Date: 2023:02:01 20:56:51
End Date: 2023:02:01 20:57:35
tourstv@TourstV:~/Desktop/QQ$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

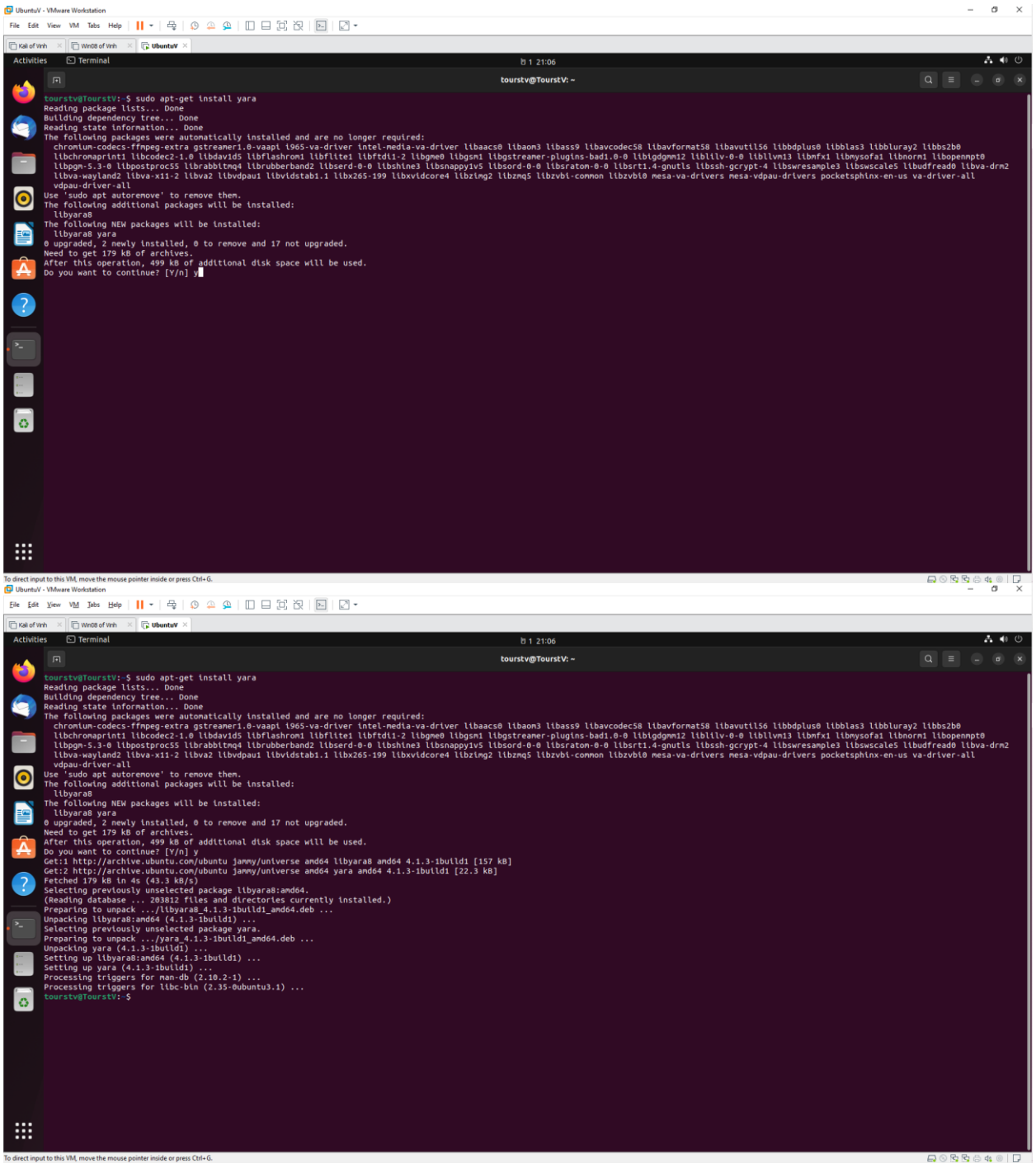

UbuntuV - VMware Workstation
File Edit View VM Tabs Help
Kali of Vnh
Win08 of Vnh
UbuntuV
Activities
Terminal
1 20:59
tourstv@TourstV: ~/Desktop/QQ
2023-02-01 20:55:43 (7.57 MB/s) - 'eicar.com.txt' saved [68/68]
tourstv@TourstV:~/Desktop/QQ$ ls
eicar.com.txt
tourstv@TourstV:~/Desktop/QQ$ clamscan --version
ClamAV 0.103.7/26799/Wed Feb 1 15:42:06 2023
tourstv@TourstV:~/Desktop/QQ$ clamscan /home/tourstv/Desktop/QQ
/home/tourstv/Desktop/QQ/eicar.com.txt: Win.Test.EICAR_HDB-1 FOUND
----------- SCAN SUMMARY -----------
Known viruses: 8650884
Engine version: 0.103.7
Scanned directories: 1
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 43.774 sec (0 m 43 s)
Start Date: 2023:02:01 20:56:51
End Date: 2023:02:01 20:57:35
tourstv@TourstV:~/Desktop/QQ$ sudo wget http://www.eicar.org/download/eicar_com.zip
--2023-02-01 20:57:58-- http://www.eicar.org/download/eicar_com.zip
Resolving www.eicar.org (www.eicar.org)... 2a00:1828:1000:2497::2, 89.238.73.97
Connecting to www.eicar.org (www.eicar.org)|2a00:1828:1000:2497::2|: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
2023-02-01 20:58:01 (11.9 MB/s) - 'eicar_com.zip' saved [184/184]
tourstv@TourstV:~/Desktop/QQ$ clamscan /home/tourstv/Desktop/QQ
/home/tourstv/Desktop/QQ/eicar.com.txt: Win.Test.EICAR_HDB-1 FOUND
/home/tourstv/Desktop/QQ/eicar_com.zip: Win.Test.EICAR_HDB-1 FOUND
----------- SCAN SUMMARY -----------
Known viruses: 8650884
Engine version: 0.103.7
Scanned directories: 1
Scanned files: 2
Infected files: 2
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 25.558 sec (0 m 25 s)
Start Date: 2023:02:01 20:58:05
End Date: 2023:02:01 20:58:31
tourstv@TourstV:~/Desktop/QQ$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


UbuntuV - VMware Workstation
File Edit View VM Tabs Help
Kali of Vnh
Win08 of Vnh
UbuntuV
Activities
Gedit
1 21:00
tourstv@TourstV: ~/Desktop/QQ
Open
Clam_HelloWorld.ndb
/home/tourstv/Desktop/QQ
Save
1 Clam_HelloWorld:0:*:68656c6c6f*776f726c64
Saving file "/home/tourstv/Desktop/QQ/Clam_HelloWorld.ndb... Plain Text Tab Width: 8 Ln 1, Col 42 INS
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 43.774 sec (0 m 43 s)
Start Date: 2023:02:01 20:56:51
End Date: 2023:02:01 20:57:35
tourstv@TourstV:~/Desktop/QQ$ sudo wget http://www.eicar.org/download/eicar_com.
--2023-02-01 20:57:58-- http://www.eicar.org/download/eicar_com.zip
Resolving www.eicar.org (www.eicar.org)... 2a00:1828:1000:2497::2, 89.238.73.97
Connecting to www.eicar.org (www.eicar.org)|2a00:1828:1000:2497::2|:80... connec
HTTP request sent, awaiting response... 200 OK
Length: 184 [application/zip]
Saving to: 'eicar_com.zip'
eicar_com.zip 100%[=
-.-KB/s in 0s
2023-02-01 20:58:01 (11.9 MB/s) - 'eicar_com.zip' saved [184/184]
tourstv@TourstV:~/Desktop/QQ$ clamscan /home/tourstv/Desktop/QQ
/home/tourstv/Desktop/QQ/eicar.com.txt: Win.Test.EICAR_HDB-1 FOUND
/home/tourstv/Desktop/QQ/eicar_com.zip: Win.Test.EICAR_HDB-1 FOUND
----------- SCAN SUMMARY -----------
Known viruses: 8650884
Engine version: 0.103.7
Scanned directories: 1
Scanned files: 2
Infected files: 2
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 25.558 sec (0 m 25 s)
Start Date: 2023:02:01 20:58:05
End Date: 2023:02:01 20:58:31
tourstv@TourstV:~/Desktop/QQ$ sudo gedit Clam_HelloWorld.ndb
(gedit:139934): dconf-WARNING **: 21:00:04.129: failed to commit changes to dcon
(gedit:139934): dconf-WARNING **: 21:00:04.133: failed to commit changes to dcon
(gedit:139934): dconf-WARNING **: 21:00:04.633: failed to commit changes to dcon
(gedit:139934): dconf-WARNING **: 21:00:04.688: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139934): dconf-WARNING **: 21:00:04.688: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
** (gedit:139934): WARNING **: 21:00:21.430: Set document metadata failed: Setting attribute metadata::gedit-spell-language not supported
** (gedit:139934): WARNING **: 21:00:21.430: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

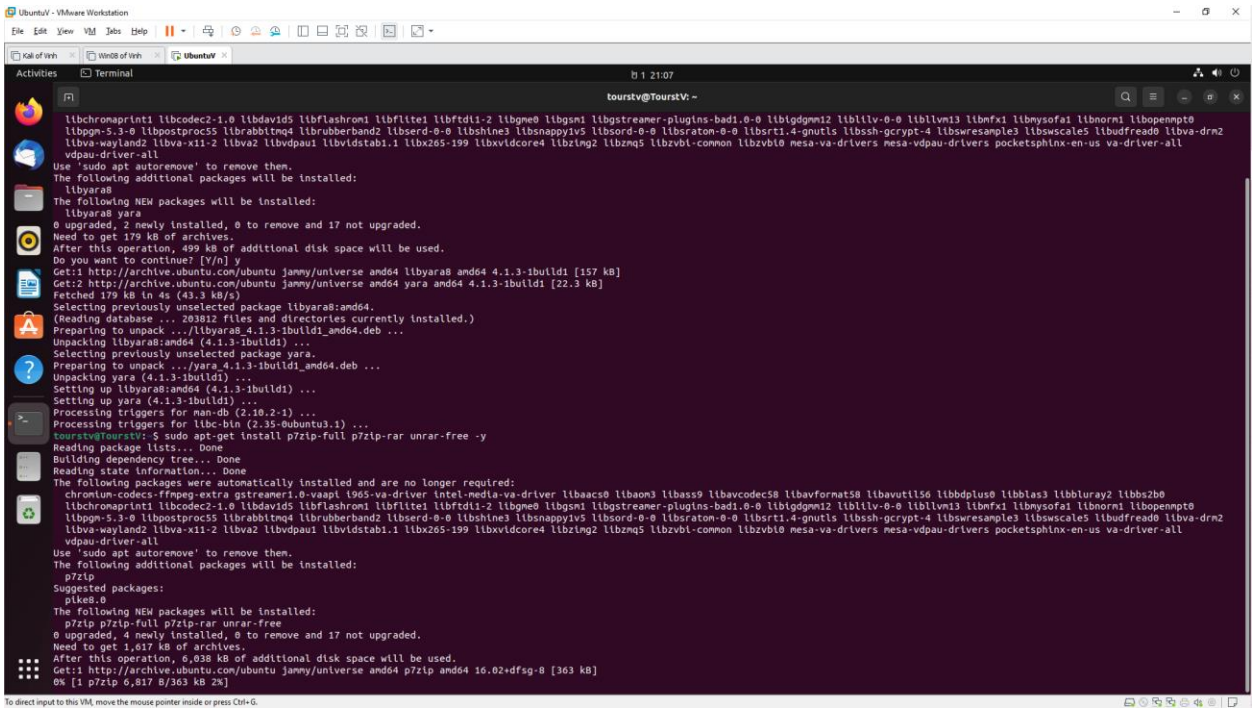


PART 2: YARA

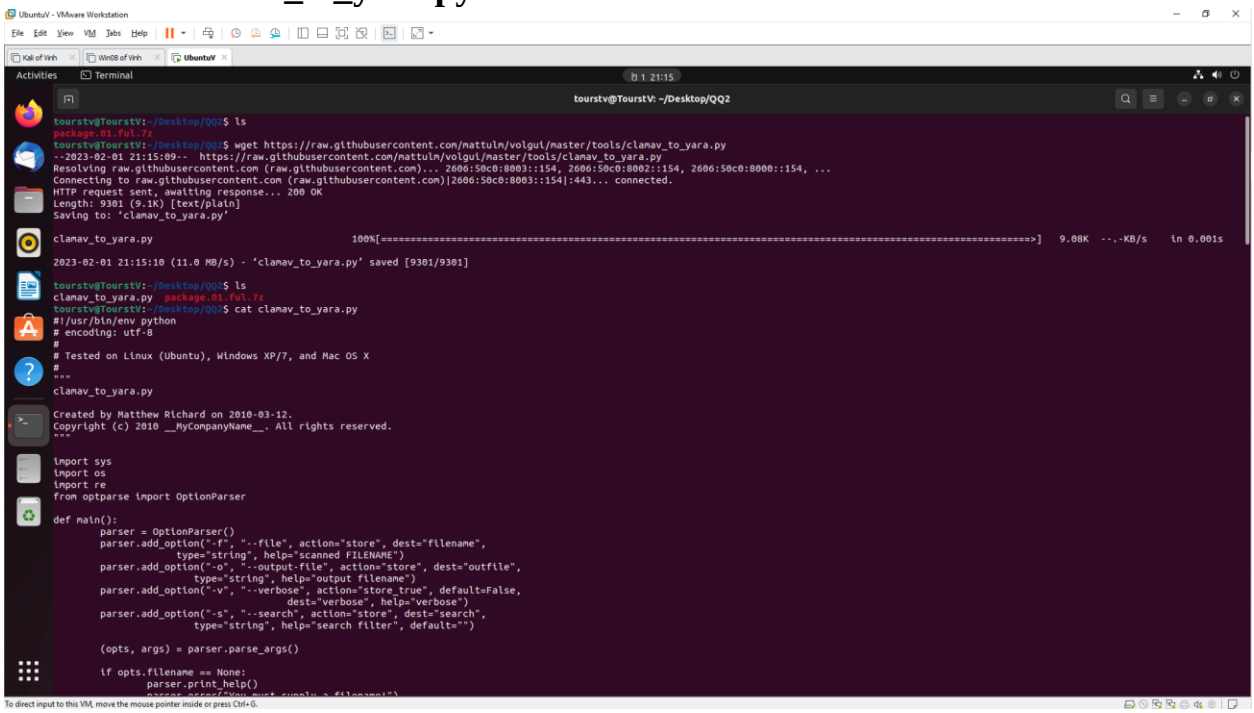
Install Yara



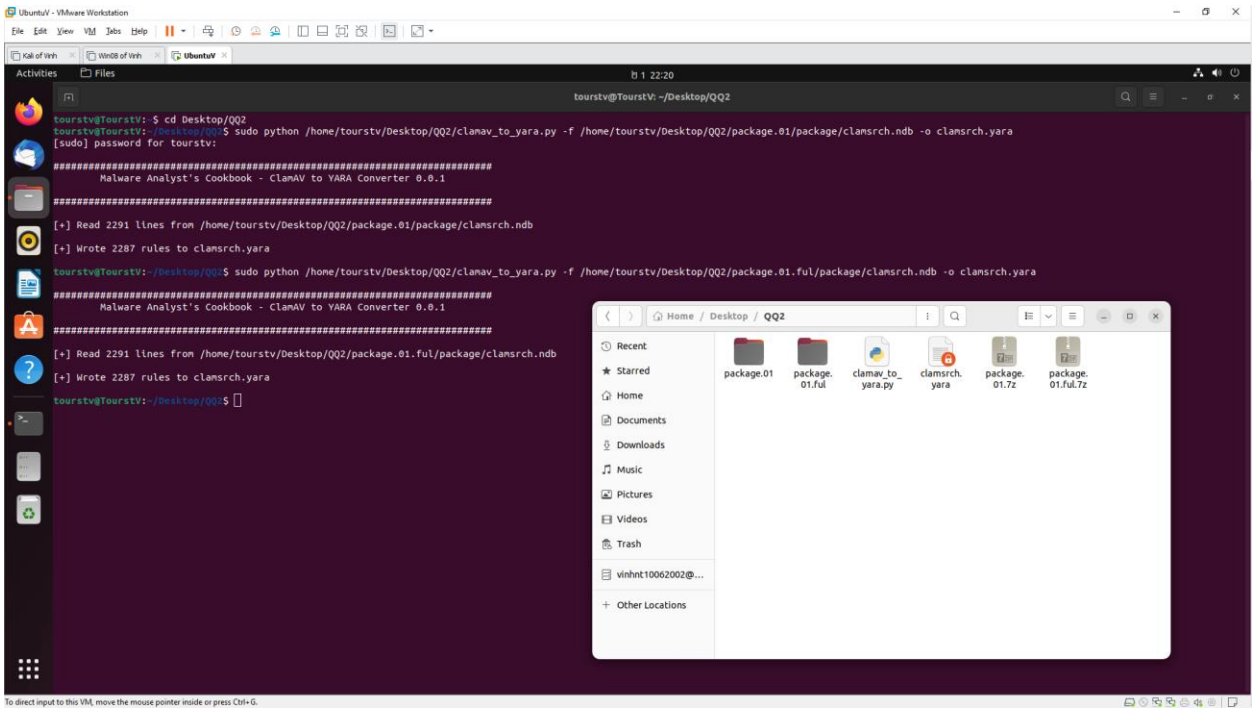
Install p7zip-full



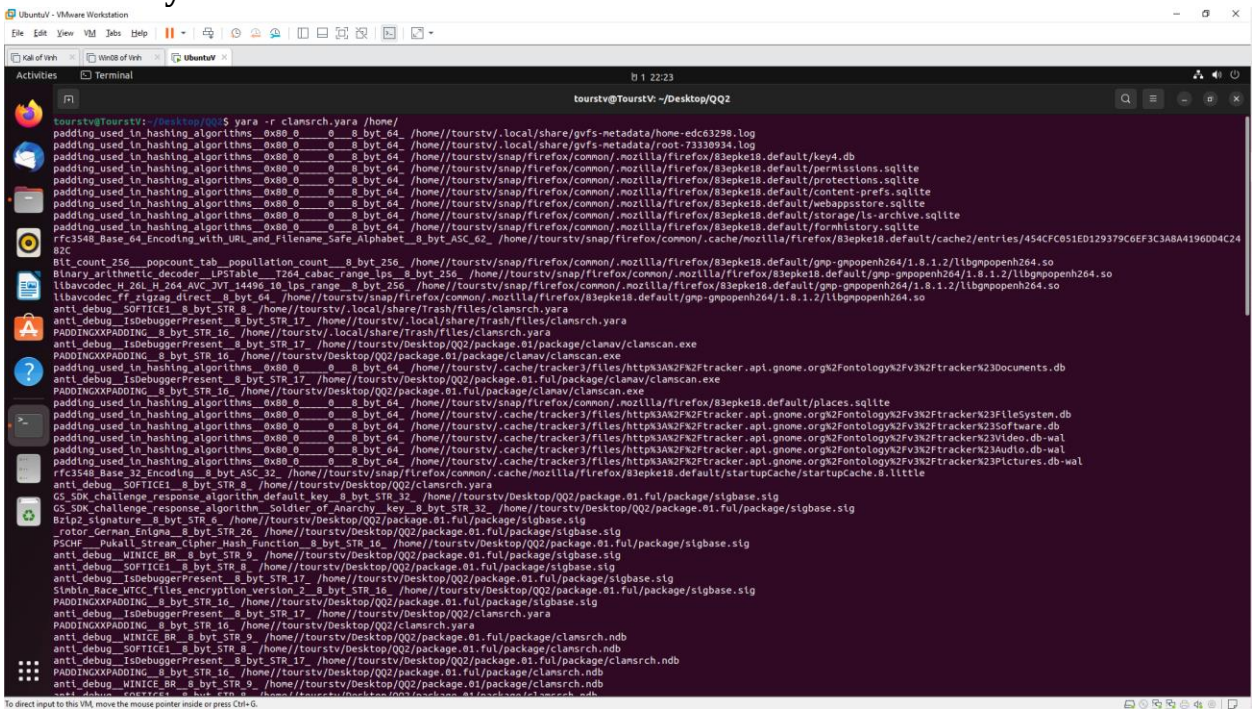
Download clamav_to_yara.py



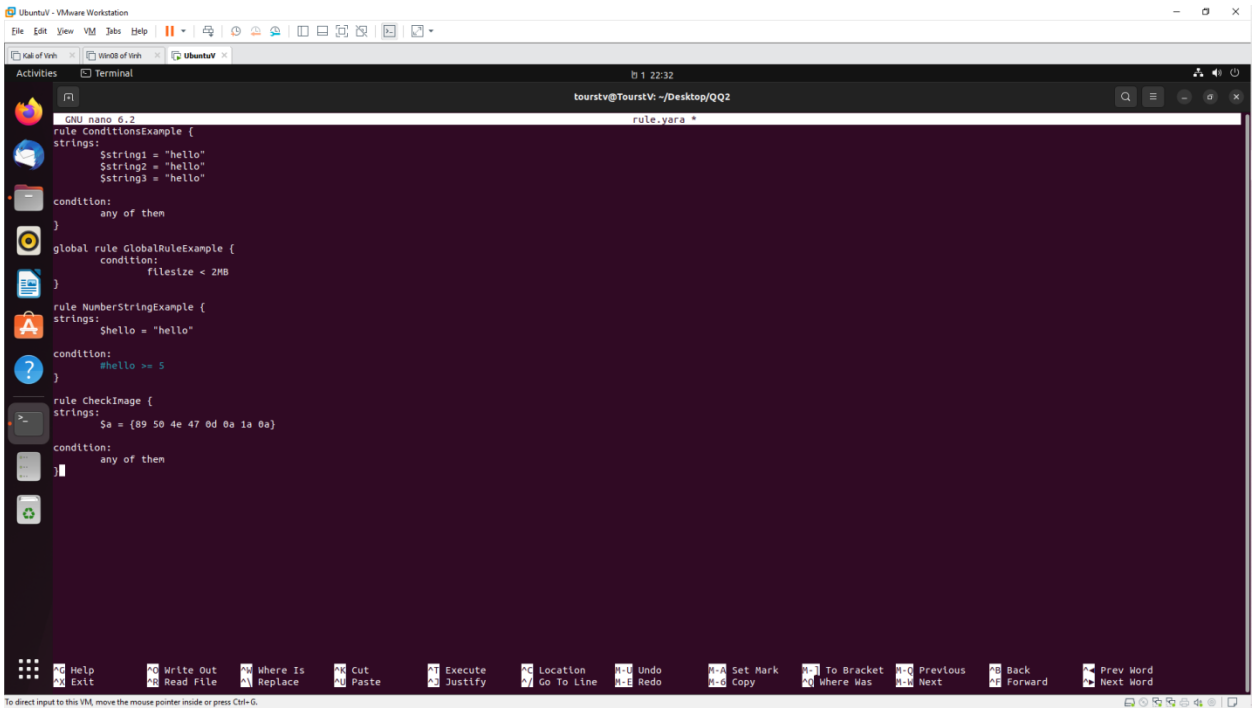
Convert file clamav to yara:



Scan with yara:



Yara rule:



Test yara rule