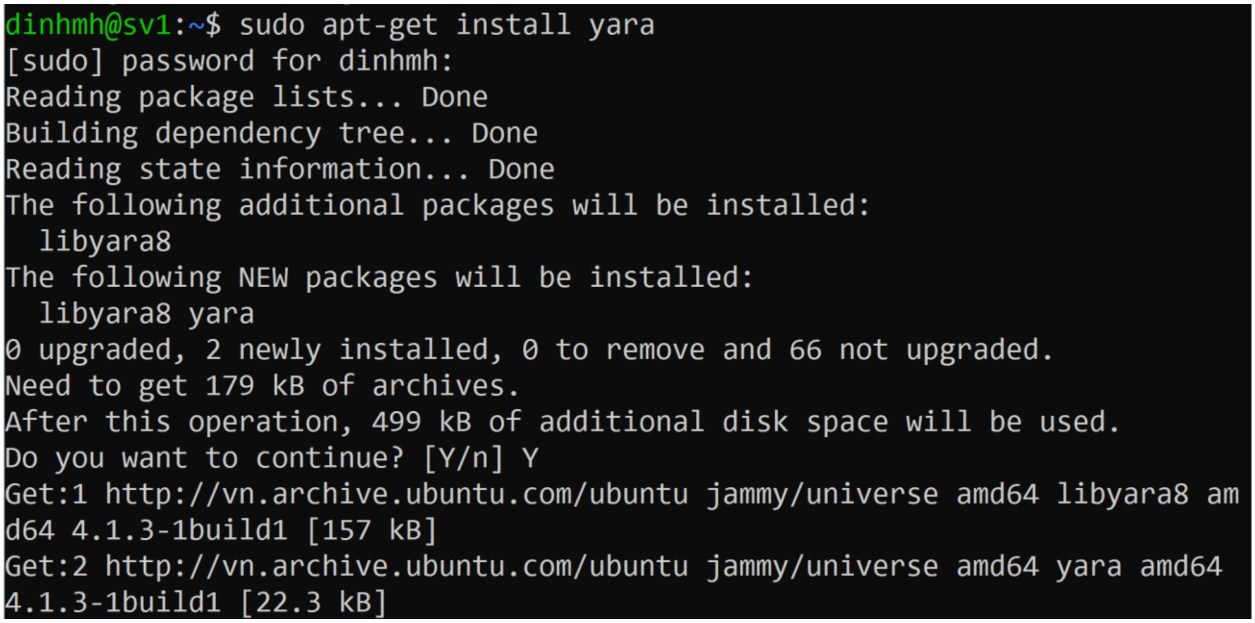
LAB 4:Detect Malware Capabilities with YARA

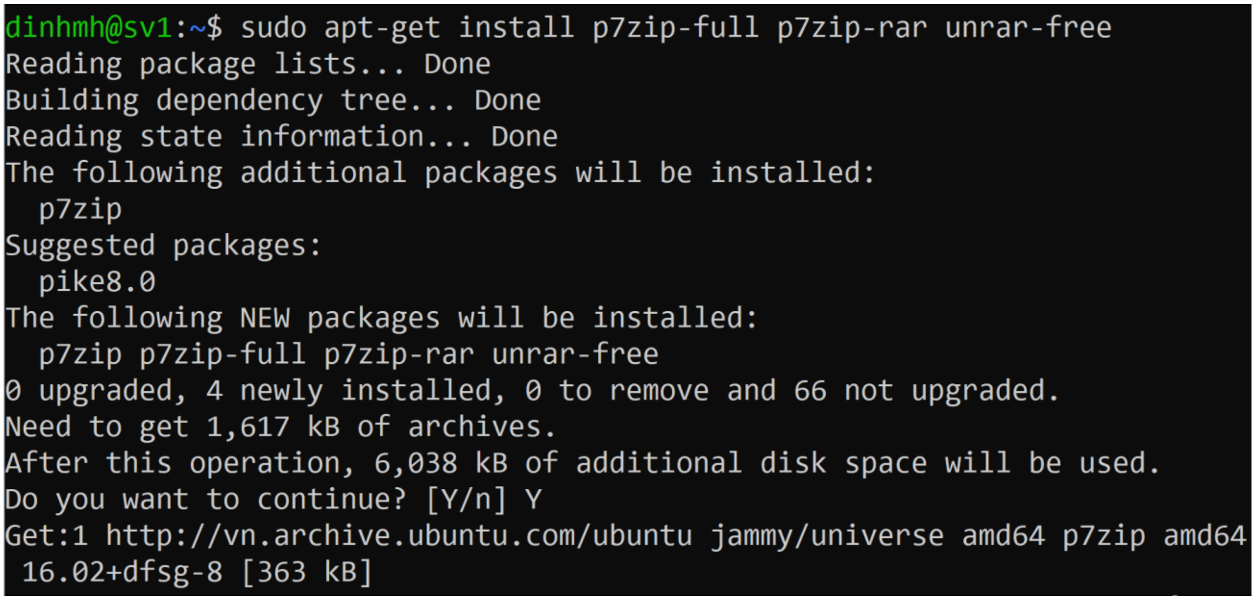
- YARA is a popular tool that provides a robust language.
- It is used to examine the suspected files/directories and match strings as is defined in the YARA rules with the file.

Install YARA



```
dinhmh@sv1:~$ sudo apt-get install yara
[sudo] password for dinhmh:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
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 66 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 am
d64 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]
```

Install p7zip-full:

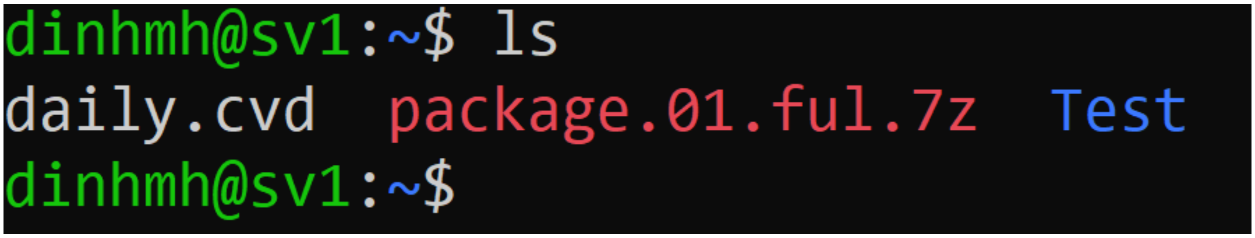


```
dinhmh@sv1:~$ sudo apt-get install p7zip-full p7zip-rar unrar-free
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  p7zip
Suggested packages:
  pike8.0
The following NEW packages will be installed:
  p7zip p7zip-full p7zip-rar unrar-free
0 upgraded, 4 newly installed, 0 to remove and 66 not upgraded.
Need to get 1,617 kB of archives.
After this operation, 6,038 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 p7zip amd64
 16.02+dfsg-8 [363 kB]
```

Download package.01.ful.7z:

https://code.google.com/archive/p/clamsrch/downloads

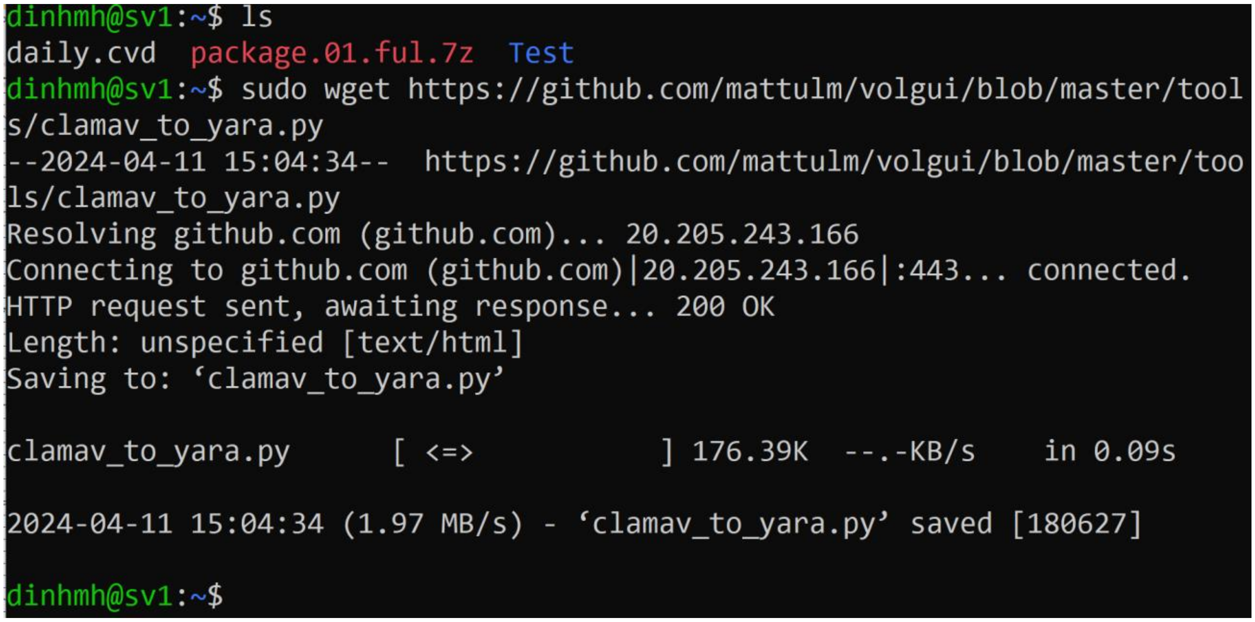
(https://storage.googleapis.com/google-code-archive-downloads/v2/code.google.com/clamsrch/package.01.ful.7z)



```
dinhmh@sv1:~$ ls
daily.cvd  package.01.ful.7z  Test
dinhmh@sv1:~$
```

Download file clam_to_yara.py:

sudo wget https://github.com/mattulm/volgui/blob/master/tools/clamav_to_yara.py

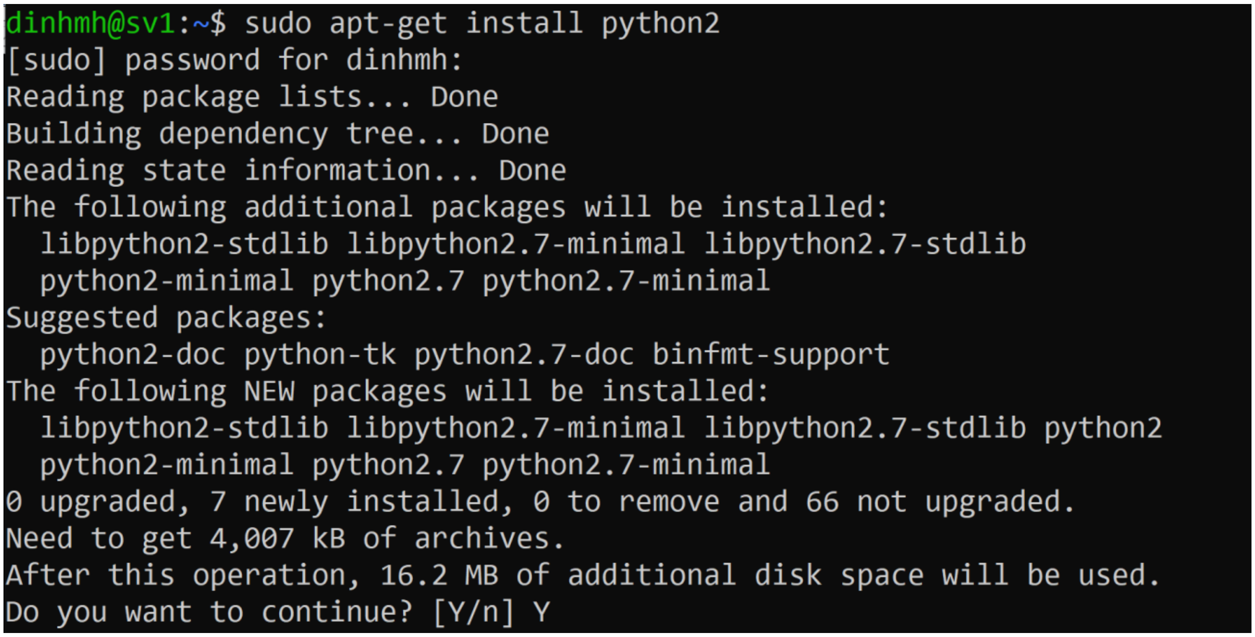


```
dinhmh@sv1:~$ ls
daily.cvd  package.01.ful.7z  Test
dinhmh@sv1:~$ sudo wget https://github.com/mattulm/volgui/blob/master/tool
s/clamav_to_yara.py
--2024-04-11 15:04:34--  https://github.com/mattulm/volgui/blob/master/too
ls/clamav_to_yara.py
Resolving github.com (github.com)... 20.205.243.166
Connecting to github.com (github.com)|20.205.243.166|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: ‘clamav_to_yara.py’

clamav_to_yara.py      [ <=>           ] 176.39K  --.-KB/s    in 0.09s

2024-04-11 15:04:34 (1.97 MB/s) - ‘clamav_to_yara.py’ saved [180627]

dinhmh@sv1:~$
```

Convert file clamav sang yara:

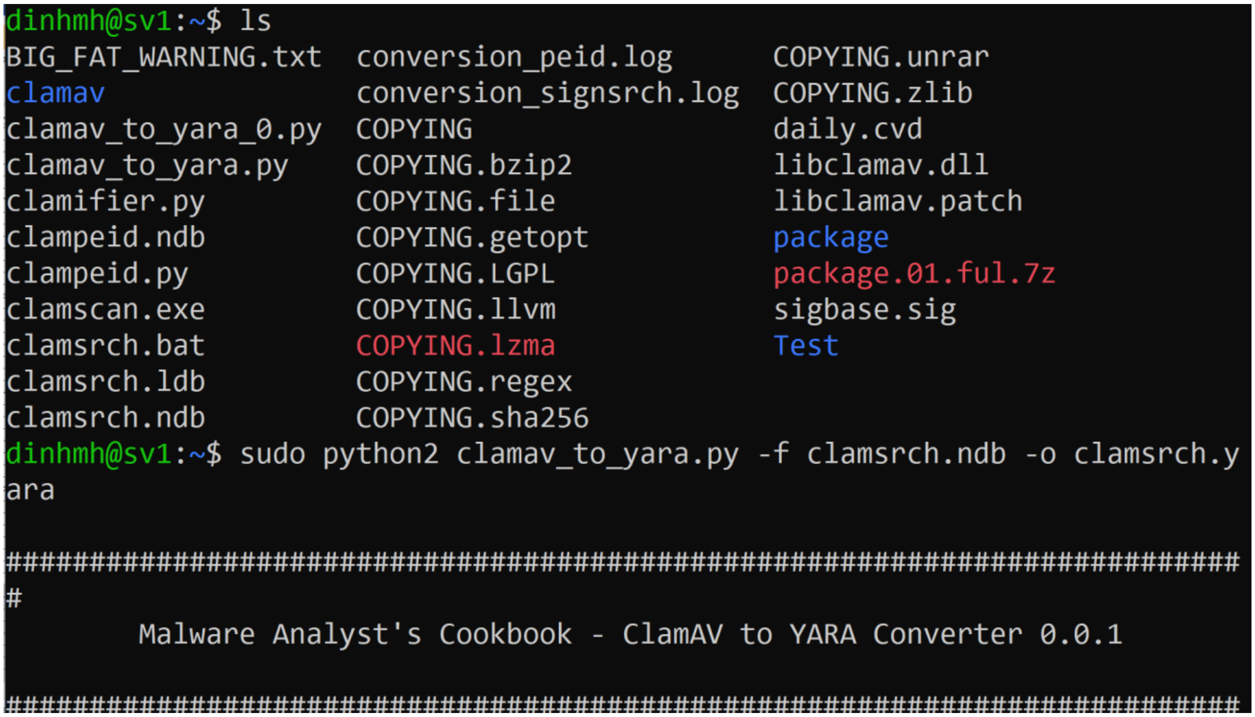
Unzip the **package.01.ful.7z** file with the command: **sudo 7z e package.01.ful.7z**

You must first install python2 because the clamav_to_yara.py file is written in python2.

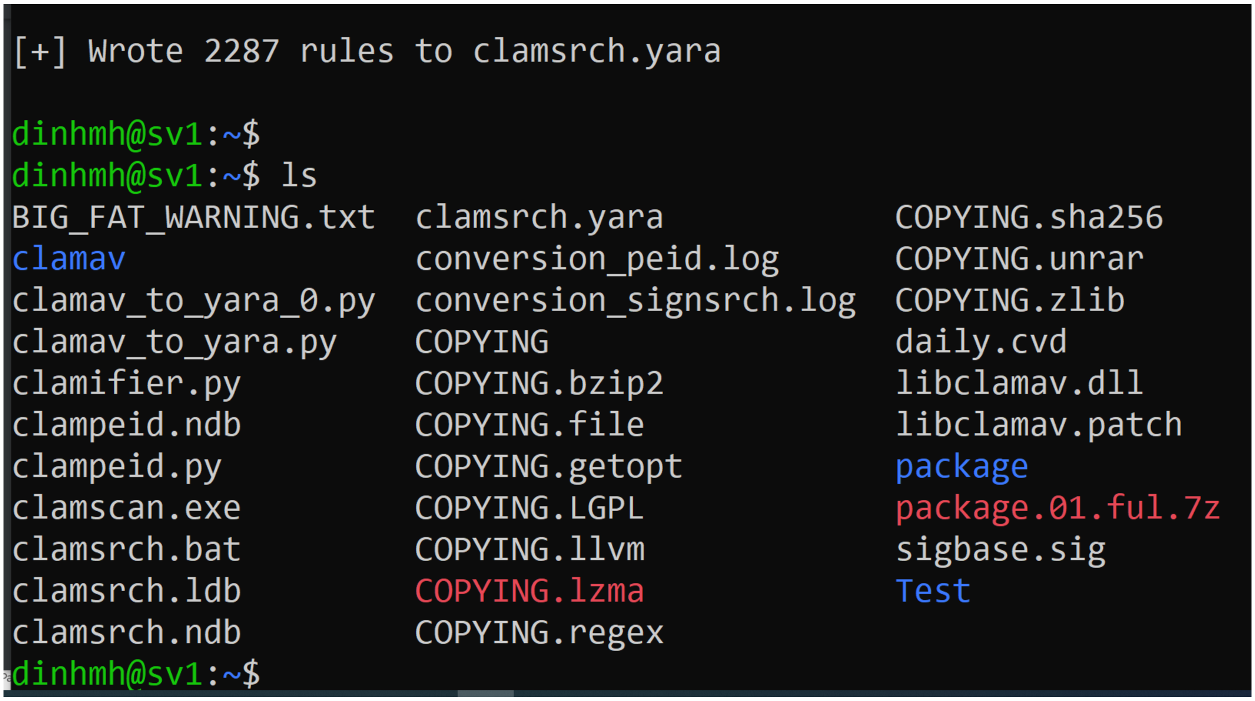


```
dinhmh@sv1:~$ sudo apt-get install python2
[sudo] password for dinhmh:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libpython2-stdlib libpython2.7-minimal libpython2.7-stdlib
  python2-minimal python2.7 python2.7-minimal
Suggested packages:
  python2-doc python-tk python2.7-doc 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 66 not upgraded.
Need to get 4,007 kB of archives.
After this operation, 16.2 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

sudo python2 clamav_to_yara.py -f clamsrch.ndb -o clamsrch.yara

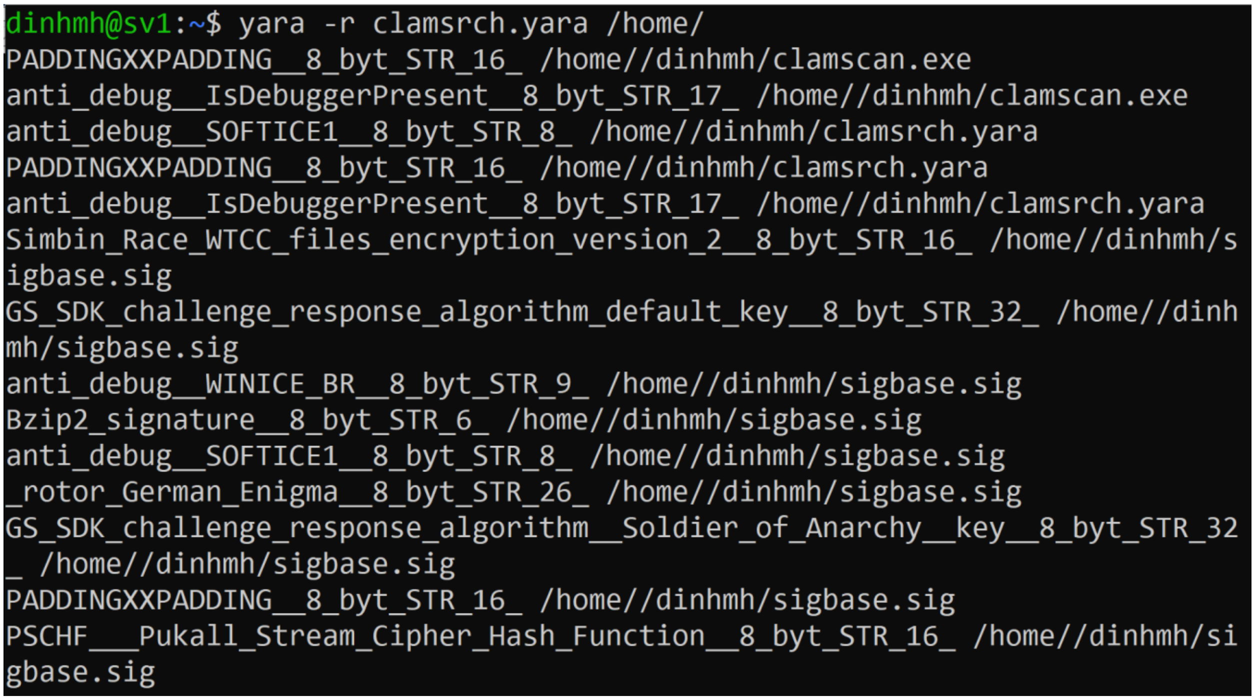


```
dinhmh@sv1:~$ ls
BIG_FAT_WARNING.txt  conversion_peid.log      COPYING.unrar
clamav               conversion_signsrch.log  COPYING.zlib
clamav_to_yara_0.py  COPYING                  daily.cvd
clamav_to_yara.py    COPYING.bzip2            libclamav.dll
clamifier.py         COPYING.file             libclamav.patch
clampeid.ndb         COPYING.getopt           package
clampeid.py          COPYING.LGPL             package.01.ful.7z
clamscan.exe         COPYING.llvm             sigbase.sig
clamsrch.bat         COPYING.lzma             Test
clamsrch.ldb         COPYING.regex
clamsrch.ndb         COPYING.sha256
dinhmh@sv1:~$ sudo python2 clamav_to_yara.py -f clamsrch.ndb -o clamsrch.y
ara

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

############################################################################
```



```
[+] Wrote 2287 rules to clamsrch.yara

dinhmh@sv1:~$
dinhmh@sv1:~$ ls
BIG_FAT_WARNING.txt  clamsrch.yara            COPYING.sha256
clamav               conversion_peid.log      COPYING.unrar
clamav_to_yara_0.py  conversion_signsrch.log  COPYING.zlib
clamav_to_yara.py    COPYING                  daily.cvd
clamifier.py         COPYING.bzip2            libclamav.dll
clampeid.ndb         COPYING.file             libclamav.patch
clampeid.py          COPYING.getopt           package
clamscan.exe         COPYING.LGPL             package.01.ful.7z
clamsrch.bat         COPYING.llvm             sigbase.sig
clamsrch.ldb         COPYING.lzma             Test
clamsrch.ndb         COPYING.regex
dinhmh@sv1:~$
```

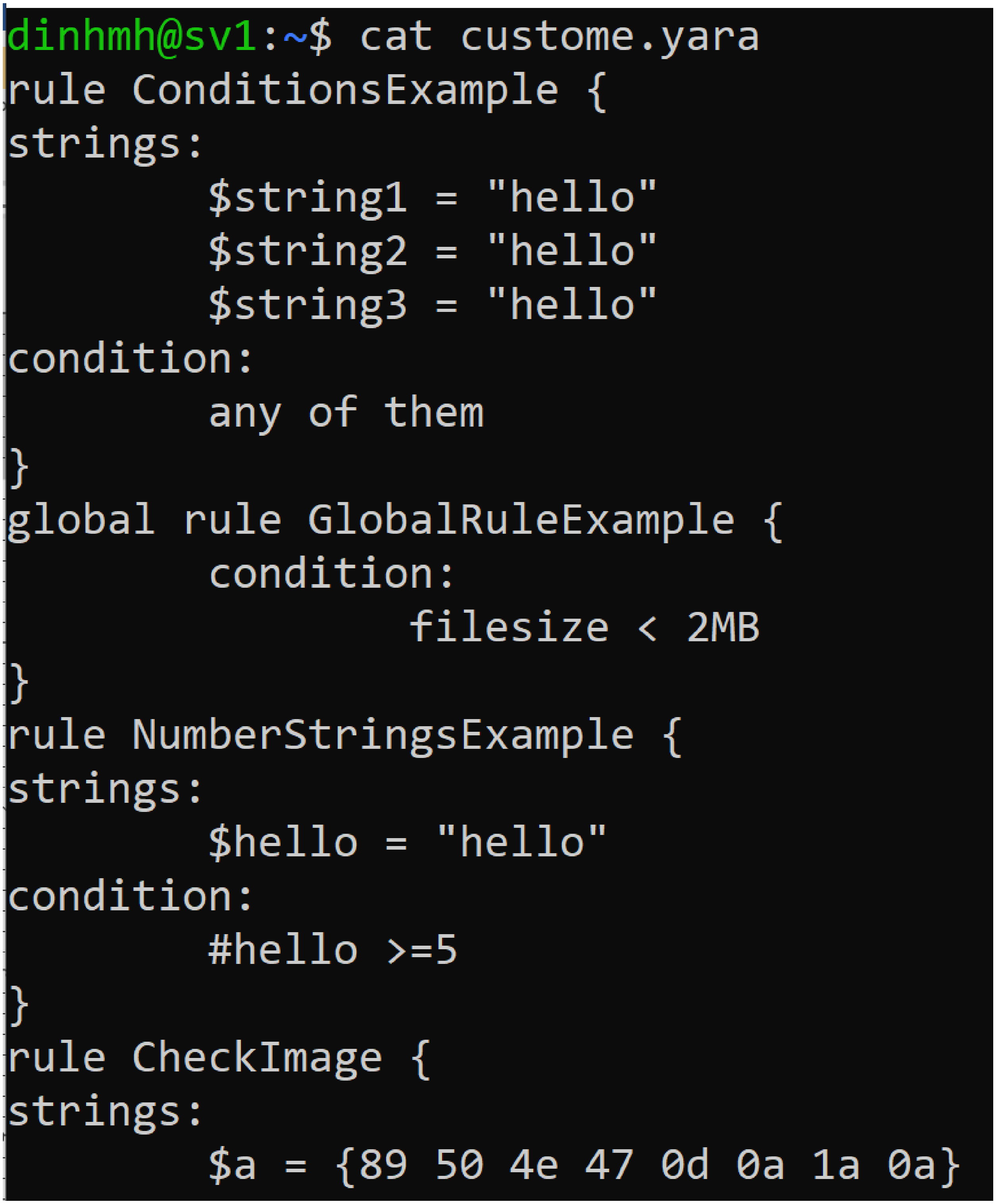
Start scanning with the yara



```
dinhmh@sv1:~$ yara -r clamsrch.yara /home/
PADDINGXXPADDING__8_byt_STR_16_ /home//dinhmh/clamscan.exe
anti_debug__IsDebuggerPresent__8_byt_STR_17_ /home//dinhmh/clamscan.exe
anti_debug__SOFTICE1__8_byt_STR_8_ /home//dinhmh/clamsrch.yara
PADDINGXXPADDING__8_byt_STR_16_ /home//dinhmh/clamsrch.yara
anti_debug__IsDebuggerPresent__8_byt_STR_17_ /home//dinhmh/clamsrch.yara
Simbin_Race_WTCC_files_encryption_version_2__8_byt_STR_16_ /home//dinhmh/s
igbase.sig
GS_SDK_challenge_response_algorithm_default_key__8_byt_STR_32_ /home//dinh
mh/sigbase.sig
anti_debug__WINICE_BR__8_byt_STR_9_ /home//dinhmh/sigbase.sig
Bzip2_signature__8_byt_STR_6_ /home//dinhmh/sigbase.sig
anti_debug__SOFTICE1__8_byt_STR_8_ /home//dinhmh/sigbase.sig
_rotor_German_Enigma__8_byt_STR_26_ /home//dinhmh/sigbase.sig
GS_SDK_challenge_response_algorithm__Soldier_of_Anarchy__key__8_byt_STR_32
_ /home//dinhmh/sigbase.sig
PADDINGXXPADDING__8_byt_STR_16_ /home//dinhmh/sigbase.sig
PSCHF___Pukall_Stream_Cipher_Hash_Function__8_byt_STR_16_ /home//dinhmh/si
gbase.sig
```

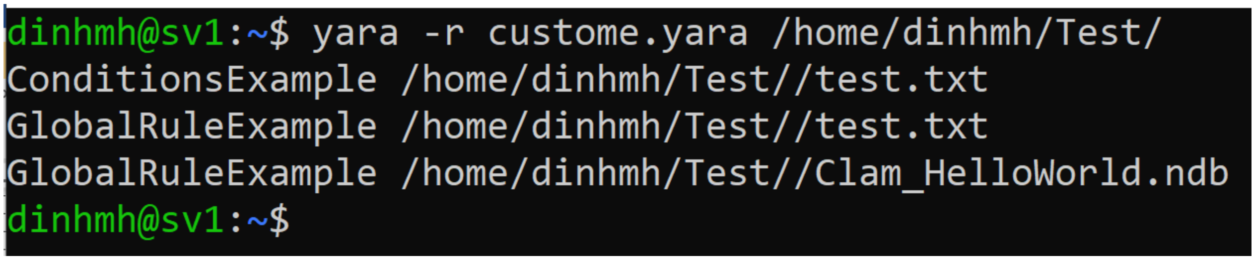
Create a new rule file called custome.yara

```
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
}
```



```
dinhmh@sv1:~$ 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}
```

Test yara rules:



```
dinhmh@sv1:~$ yara -r custome.yara /home/dinhmh/Test/
ConditionsExample /home/dinhmh/Test//test.txt
GlobalRuleExample /home/dinhmh/Test//test.txt
GlobalRuleExample /home/dinhmh/Test//Clam_HelloWorld.ndb
dinhmh@sv1:~$
```

Here we see yara's report for the rule we created as follows: ConditionExample means that yara has detected that the test.txt file matches the rule we provided and contains the string “hello” in there. In addition, other files will match yara's GlobalRuleExample