Nguyen Nam Khanh – HE191159 – IA1902

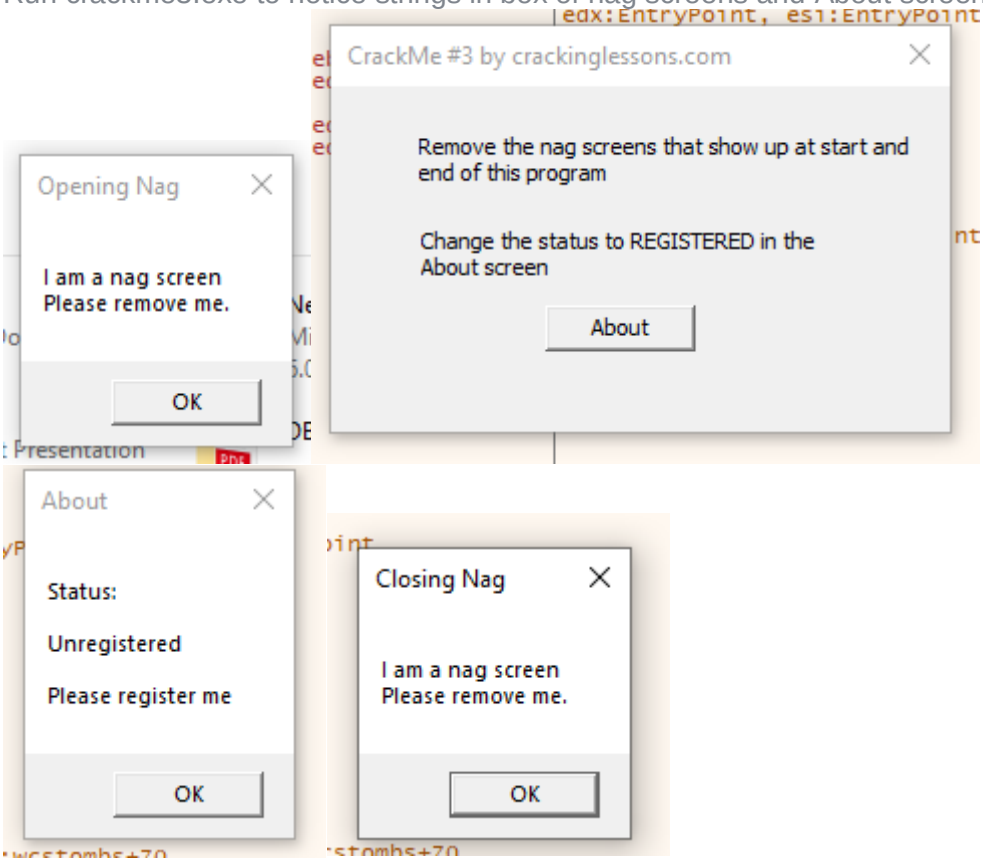
Crack me 3:

Objective:

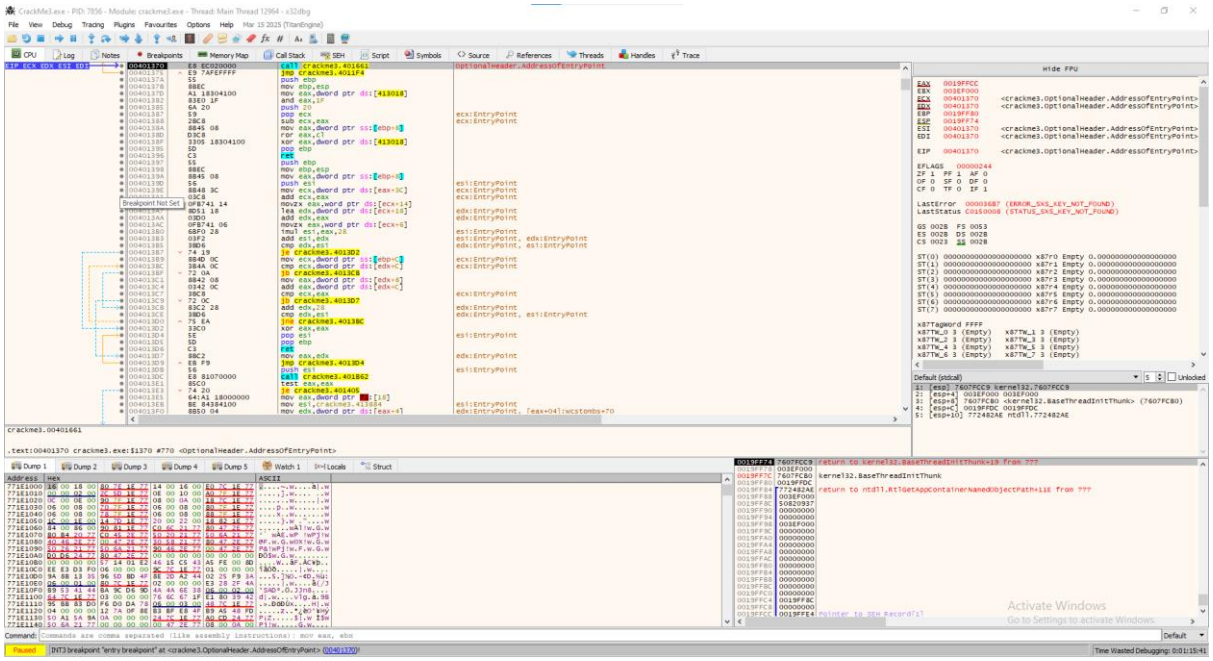
1. Remove the 2 nag screens – one at startup and one at close of program.
2. In the About screen – change status to Registered.

Solution:

Run crackme3.exe to notice strings in box of nag screens and About screen.

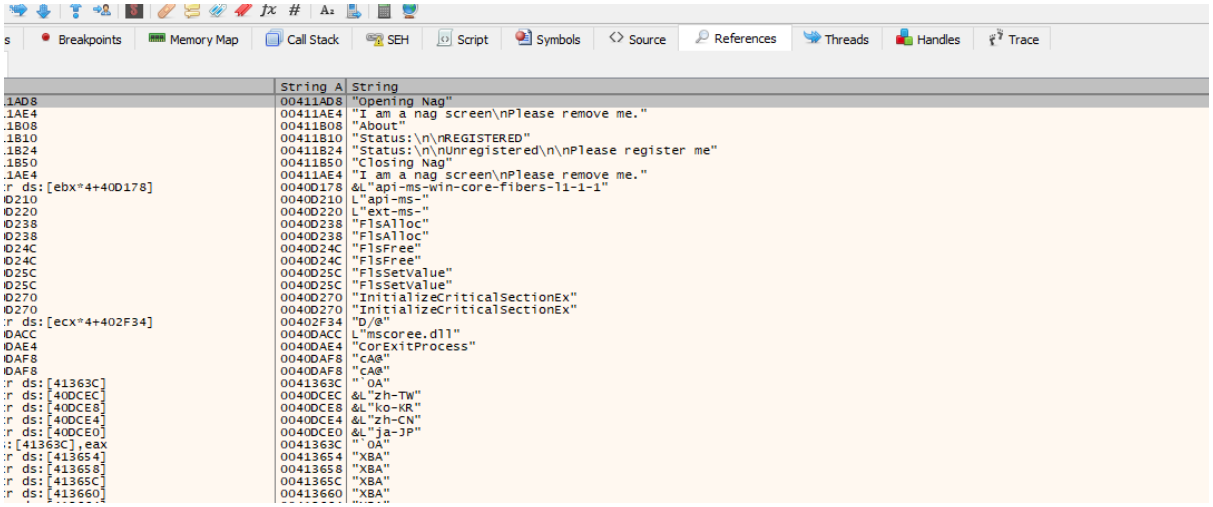


Open crackme3.exe in x32dbg tool.

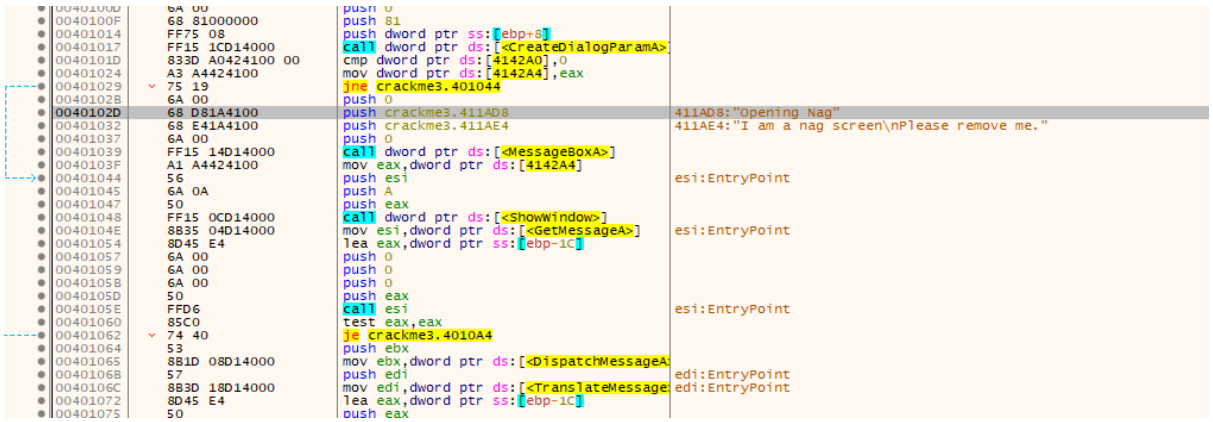


Opening nag:

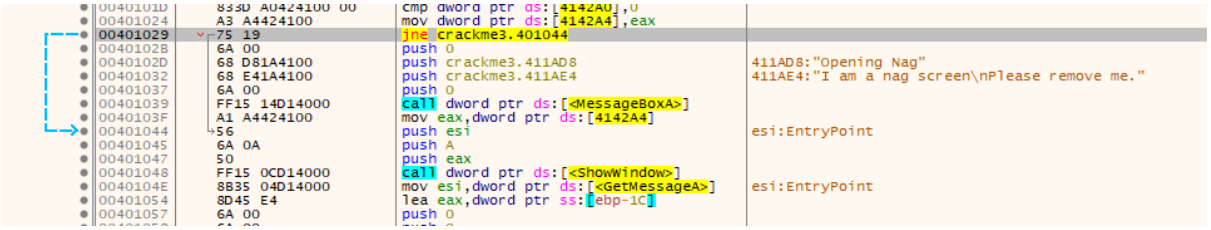
Find Opening Nag in String references



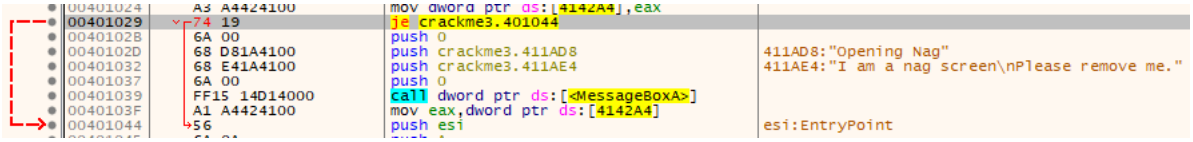
Double click to see code in CPU:



Trace code above and below, pay attention on this line ‘jne crackme3.401044’, this code is jump not equal through MessageBoxA of string “Opening Nag, I am a nag…” to address 00401044.

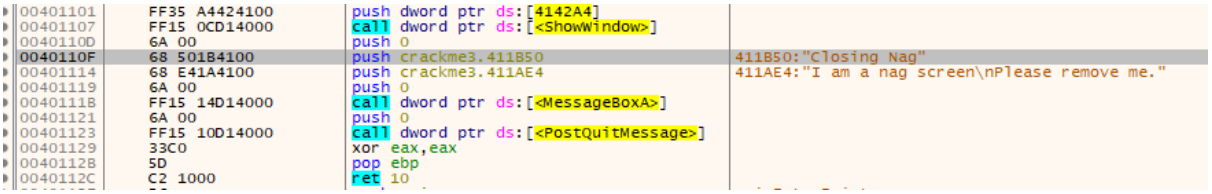


Need to change this one to je – jump equal to 00401044 ignoring these opening nag.

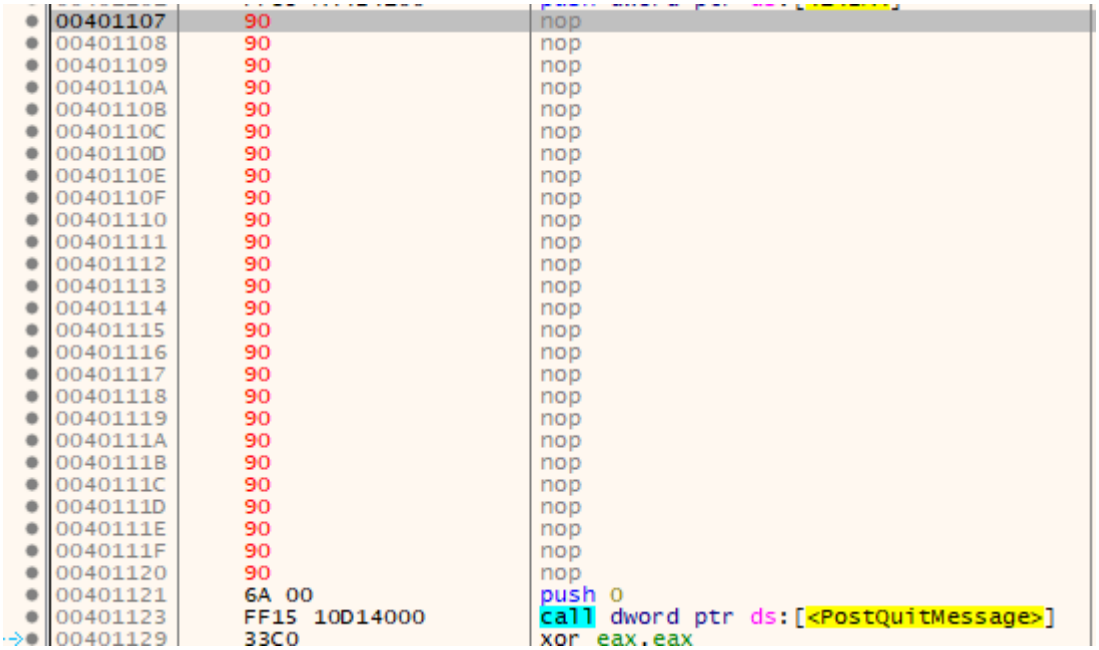


Closing nag:

Do it again with Closing nag



Trace code above and below to find the line jump, but no line has comparison to jump so we need to highlight 00401107 to 0040111BB (content of MessageBoxA of Closing nag) and fill with NOPs (no operation) to ignore Closing nag.



About screen:

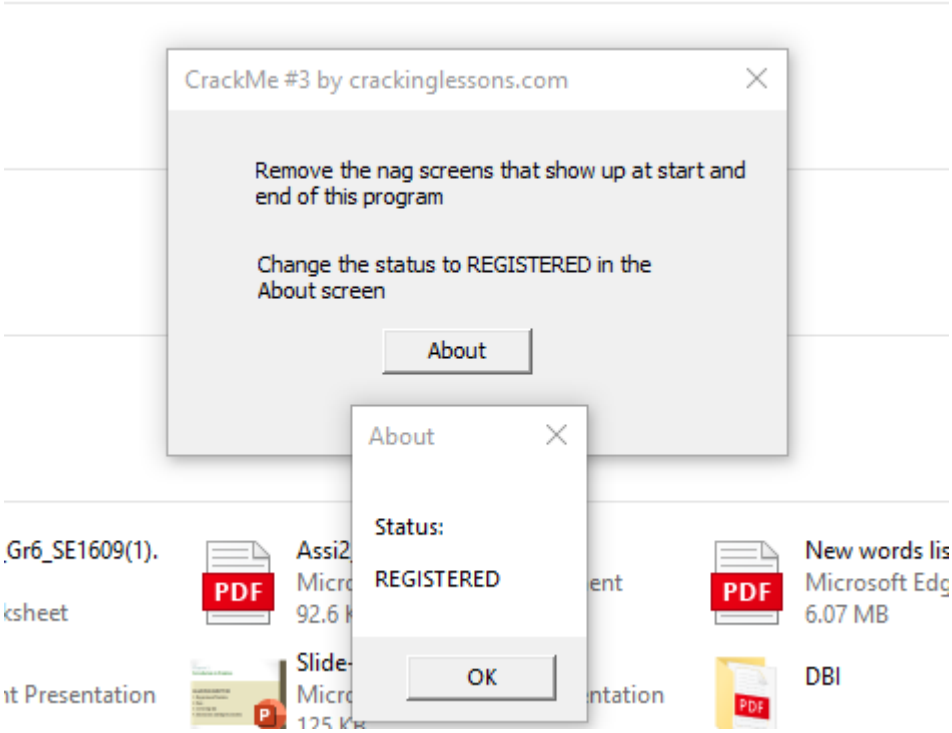
Then trace to About screen:

```
004010CD    68 081B4100     push crackme3.411B08            411B08:"About"
004010D2    3905 A0424100   cmp dword ptr ds:[4142A0],eax
004010D8    74 12           je crackme3.4010EC
004010DA    68 101B4100     push crackme3.411B10            411B10:"Status:\n\nREGISTERED"
004010DF    50              push eax
004010E0    FF15 14D14000   call dword ptr ds:[<MessageBoxA>]
004010E6    33C0            xor eax,eax
004010E8    5D              pop ebp
004010E9    C2 1000         ret 10
004010EC    68 241B4100     push crackme3.411B24            411B24:"Status:\n\nUnregistered\n\nPlease register me"
004010F1    6A 00           push 0
004010F3    FF15 14D14000   call dword ptr ds:[<MessageBoxA>]
```

Notice line “je crackme3.4010EC”, this mean jump equal to push string “Unregistered…” and call MessageBoxA, while we find out address 004010DA has string “Registered”. We need to change “je crackme3.4010EC” to “je crackme3.4010DA” to display Registered status.

```
004010CD    68 081B4100     push crackme3.411B08            411B08:"About"
004010D2    3905 A0424100   cmp dword ptr ds:[4142A0],eax
004010D8    74 00           je crackme3.4010DA
004010DA    68 101B4100     push crackme3.411B10            411B10:"Status:\n\nREGISTERED"
004010DF    50              push eax
004010E0    FF15 14D14000   call dword ptr ds:[<MessageBoxA>]
```

After change 3 objective, we patch file and run again to check the consequence.

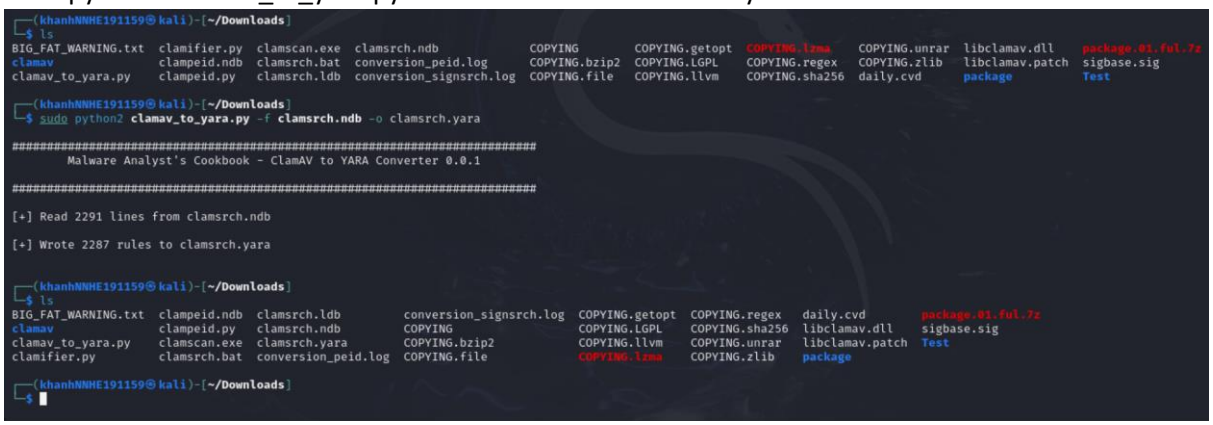


Done!

LAB 4:Detect Malware Capabilities with YARA

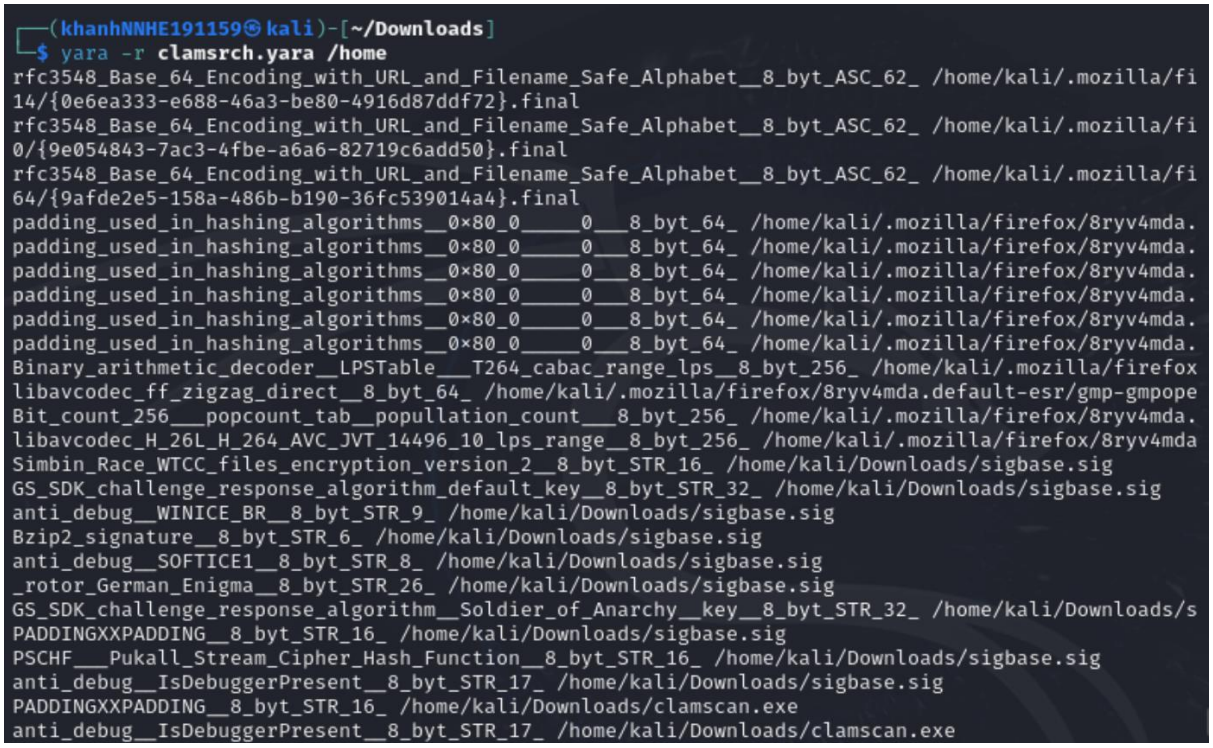
Convert file clamav to yara with the command:

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



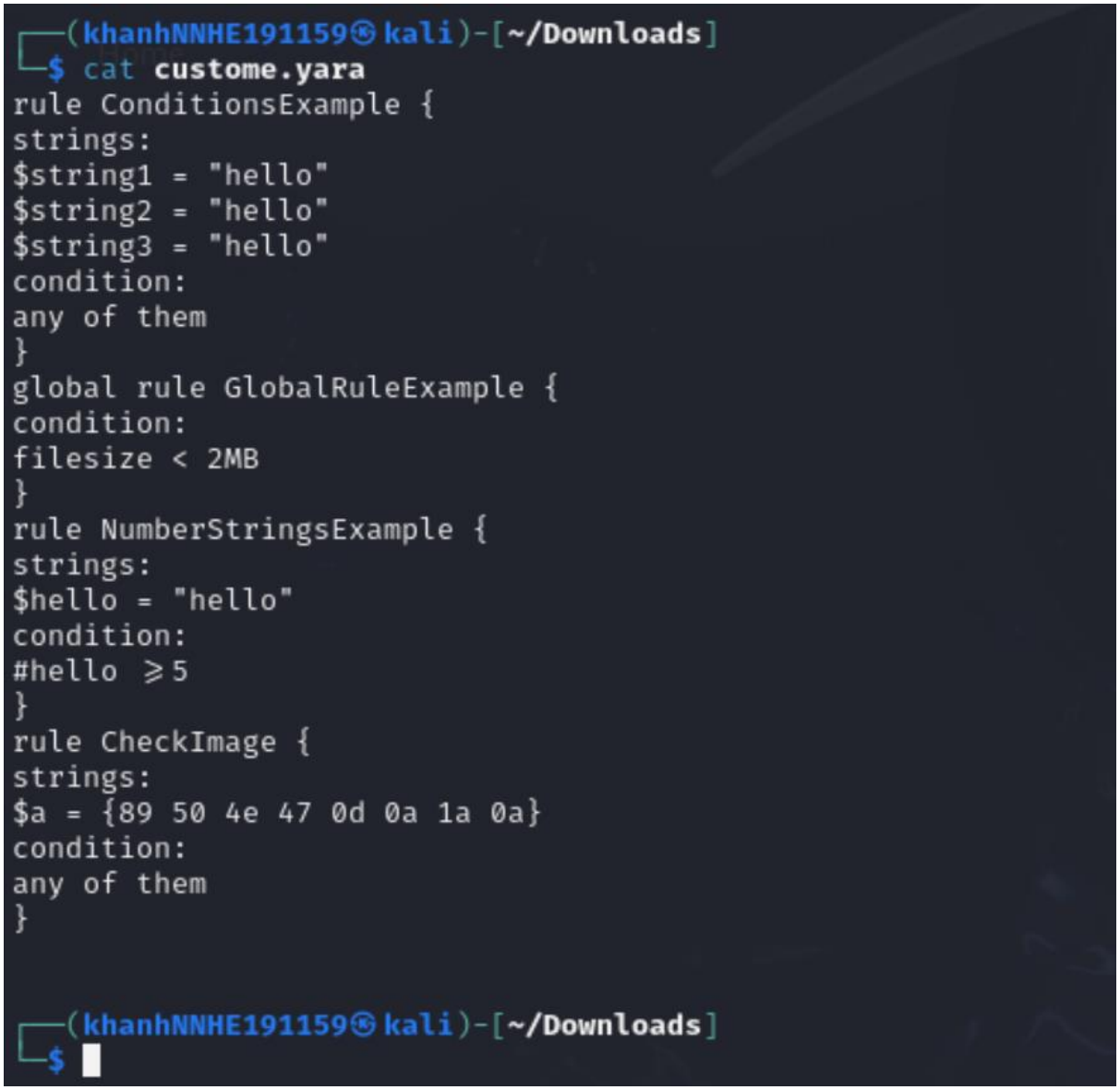
```
┌──(khanhNNHE191159㉿kali)-[~/Downloads]
└─$ ls
BIG_FAT_WARNING.txt  clamifier.py  clamscan.exe  clamsrch.ndb             COPYING        COPYING.getopt  COPYING.lzma    COPYING.unrar  libclamav.dll    package.01.ful.7z
clamav               clampeid.ndb  clamsrch.bat  conversion_peid.log      COPYING.bzip2  COPYING.LGPL    COPYING.regex   COPYING.zlib   libclamav.patch  sigbase.sig
clamav_to_yara.py    clampeid.py   clamsrch.ldb  conversion_signsrch.log  COPYING.file   COPYING.llvm    COPYING.sha256  daily.cvd      package          Test

┌──(khanhNNHE191159㉿kali)-[~/Downloads]
└─$ 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


┌──(khanhNNHE191159㉿kali)-[~/Downloads]
└─$ ls
BIG_FAT_WARNING.txt  clampeid.ndb  clamsrch.ldb         conversion_signsrch.log  COPYING.getopt  COPYING.regex   daily.cvd        package.01.ful.7z
clamav               clampeid.py   clamsrch.ndb         COPYING                  COPYING.LGPL    COPYING.sha256  libclamav.dll    sigbase.sig
clamav_to_yara.py    clamscan.exe  clamsrch.yara        COPYING.bzip2            COPYING.llvm    COPYING.unrar   libclamav.patch  Test
clamifier.py         clamsrch.bat  conversion_peid.log  COPYING.file             COPYING.lzma    COPYING.zlib    package

┌──(khanhNNHE191159㉿kali)-[~/Downloads]
└─$ █
```

Start scanning with the yara:

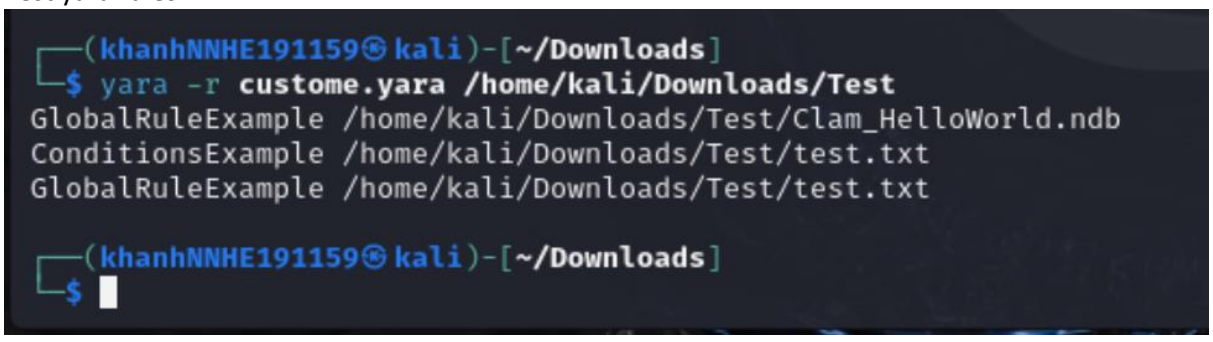


```
┌──(khanhNNHE191159㉿kali)-[~/Downloads]
└─$ yara -r clamsrch.yara /home
rfc3548_Base_64_Encoding_with_URL_and_Filename_Safe_Alphabet__8_byt_ASC_62_ /home/kali/.mozilla/fi
14/{0e6ea333-e688-46a3-be80-4916d87ddf72}.final
rfc3548_Base_64_Encoding_with_URL_and_Filename_Safe_Alphabet__8_byt_ASC_62_ /home/kali/.mozilla/fi
0/{9e054843-7ac3-4fbe-a6a6-82719c6add50}.final
rfc3548_Base_64_Encoding_with_URL_and_Filename_Safe_Alphabet__8_byt_ASC_62_ /home/kali/.mozilla/fi
64/{9afde2e5-158a-486b-b190-36fc539014a4}.final
padding_used_in_hashing_algorithms__0×80_0_____0___8_byt_64_ /home/kali/.mozilla/firefox/8ryv4mda.
padding_used_in_hashing_algorithms__0×80_0_____0___8_byt_64_ /home/kali/.mozilla/firefox/8ryv4mda.
padding_used_in_hashing_algorithms__0×80_0_____0___8_byt_64_ /home/kali/.mozilla/firefox/8ryv4mda.
padding_used_in_hashing_algorithms__0×80_0_____0___8_byt_64_ /home/kali/.mozilla/firefox/8ryv4mda.
padding_used_in_hashing_algorithms__0×80_0_____0___8_byt_64_ /home/kali/.mozilla/firefox/8ryv4mda.
padding_used_in_hashing_algorithms__0×80_0_____0___8_byt_64_ /home/kali/.mozilla/firefox/8ryv4mda.
Binary_arithmetic_decoder__LPSTable___T264_cabac_range_lps__8_byt_256_ /home/kali/.mozilla/firefox
libavcodec_ff_zigzag_direct__8_byt_64_ /home/kali/.mozilla/firefox/8ryv4mda.default-esr/gmp-gmpope
Bit_count_256___popcount_tab__popullation_count___8_byt_256_ /home/kali/.mozilla/firefox/8ryv4mda.
libavcodec_H_26L_H_264_AVC_JVT_14496_10_lps_range__8_byt_256_ /home/kali/.mozilla/firefox/8ryv4mda
Simbin_Race_WTCC_files_encryption_version_2__8_byt_STR_16_ /home/kali/Downloads/sigbase.sig
GS_SDK_challenge_response_algorithm_default_key__8_byt_STR_32_ /home/kali/Downloads/sigbase.sig
anti_debug__WINICE_BR__8_byt_STR_9_ /home/kali/Downloads/sigbase.sig
Bzip2_signature__8_byt_STR_6_ /home/kali/Downloads/sigbase.sig
anti_debug__SOFTICE1__8_byt_STR_8_ /home/kali/Downloads/sigbase.sig
_rotor_German_Enigma__8_byt_STR_26_ /home/kali/Downloads/sigbase.sig
GS_SDK_challenge_response_algorithm__Soldier_of_Anarchy__key__8_byt_STR_32_ /home/kali/Downloads/s
PADDINGXXPADDING__8_byt_STR_16_ /home/kali/Downloads/sigbase.sig
PSCHF___Pukall_Stream_Cipher_Hash_Function__8_byt_STR_16_ /home/kali/Downloads/sigbase.sig
anti_debug__IsDebuggerPresent__8_byt_STR_17_ /home/kali/Downloads/sigbase.sig
PADDINGXXPADDING__8_byt_STR_16_ /home/kali/Downloads/clamscan.exe
anti_debug__IsDebuggerPresent__8_byt_STR_17_ /home/kali/Downloads/clamscan.exe
```

Create a new rule file called custome.yara and cat to see:



Test yara rules:



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.