

Họ và tên: Trần Trí Dũng

Mã số sinh viên: HE190680

Lớp: IA1901

#### Lab 4:

Install YARA -> Install p7zip-full -> Download package.01.ful.7z -> Download file clam\_to\_yara.py  
-> Install python2

```
dungthe190680@dungthe190680:~$ sudo apt-get install yara
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
yara is already the newest version (4.1.3-1build1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
dungthe190680@dungthe190680:~$ sudo apt-get install p7zip-full p7zip-rar unrar-free
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
p7zip-full is already the newest version (16.02+dfsg-0).
unrar-free is already the newest version (1:0.0.2-0.1).
p7zip-rar is already the newest version (16.02-3build1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
dungthe190680@dungthe190680:~$ ls
daily.cd package.01.ful.7z Test
dungthe190680@dungthe190680:~$ sudo wget https://github.com/mattulm/volgui/blob/master/tools/clamav_to_yara.py
--2025-05-21 07:29:05-- https://github.com/mattulm/volgui/blob/master/tools/clamav_to_yara.py
Resolving github.com (github.com)... 64:ff9b:14cd:f3a6, 20.205.243.166
Connecting to github.com (github.com)[64:ff9b:14cd:f3a6]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'clamav_to_yara.py'

clamav_to_yara.py      [ <=> ] 197.39K  601KB/s   in 0.3s

2025-05-21 07:29:06 (601 KB/s) - 'clamav_to_yara.py' saved [202130]

dungthe190680@dungthe190680:~$ 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,12 CPUs 13th Gen Intel(R) Core(TM) i5-13480P (B06A2),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
dungthe190680@dungthe190680:~$ sudo apt-get install python2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
python2 is already the newest version (2.7.18-3).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Convert file clamav to yara -> Start scanning with the yara:

```
dungthe190680@dungthe190680:~$ ls
BIG_FAT_WARNING.txt  clamscan.exe          COPYING             COPYING.lzma        libclamav.dll
clamav               clamsrch.bat          COPYING.bzrip2      COPYING.regex        libclamav.patch
clamav_to.yara.py    clamsrch.ldb          COPYING.file         COPYING.sha256       package
clamfief.py          clamsrch.ndb          COPYING.getopt       COPYING.unrar        package.01.ful.7z
clameid.ndb          conversion.peid.log   COPYING.lgpl        COPYING.zlib         sigbase.sig
clameid.py           conversion.signsrch.log  COPYING.llvm        daily.cvd            Test
dungthe190680@dungthe190680:~$ 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

dungthe190680@dungthe190680:~$ ls
BIG_FAT_WARNING.txt  clamsrch.bat          COPYING.bzrip2      COPYING.sha256       package.01.ful.7z
clamav               clamsrch.ldb          COPYING.bzrip2      COPYING.unrar        sigbase.sig
clamav_to.yara.py    clamsrch.ndb          COPYING.getopt       COPYING.zlib         Test
clamfief.py          clamsrch.yara         COPYING.lgpl        daily.cvd            libclamav.dll
clameid.ndb          conversion.peid.log   COPYING.llvm        libclamav.dll
clameid.py           conversion.signsrch.log  COPYING.lzma        libclamav.patch
clamscan.exe         COPYING               COPYING.regex        package

dungthe190680@dungthe190680:~$ yara -r clamsrch.yara /home/
PADDINGXXPADDING_8_byt_STR_16_ /home//dungthe190680/clamsrch.yara
anti_debug_IsDebuggerPresent_8_byt_STR_17_ /home//dungthe190680/clamsrch.yara
Simbin_Race_WTCC_files_encryption_version_2_8_byt_STR_16_ /home//dungthe190680/sigbase.sig
GS_SDM_challenge_response_algorithm_default_key_8_byt_STR_32_ /home//dungthe190680/sigbase.sig
anti_debug_WINICE_0R_8_byt_STR_9_ /home//dungthe190680/sigbase.sig
Bzip2_signature_8_byt_STR_6_ /home//dungthe190680/sigbase.sig
anti_debug_SOFTICE1_8_byt_STR_8_ /home//dungthe190680/sigbase.sig
_rotor_German_Enigma_8_byt_STR_26_ /home//dungthe190680/sigbase.sig
GS_SDM_challenge_response_algorithm_soldier_of_anarchy_key_8_byt_STR_32_ /home//dungthe190680/sigbase.sig
PADDINGXXPADDING_8_byt_STR_16_ /home//dungthe190680/clamsrch.yara
PSCFH_Pukall_Stream_Cipher_Hash_Function_8_byt_STR_16_ /home//dungthe190680/sigbase.sig
anti_debug_IsDebuggerPresent_8_byt_STR_17_ /home//dungthe190680/sigbase.sig
anti_debug_WINICE_0R_8_byt_STR_9_ /home//dungthe190680/clamsrch.ndb
anti_debug_SOFTICE1_8_byt_STR_8_ /home//dungthe190680/clamsrch.ndb
PADDINGXXPADDING_8_byt_STR_16_ /home//dungthe190680/clamsrch.ndb
anti_debug_IsDebuggerPresent_8_byt_STR_17_ /home//dungthe190680/clamsrch.ndb
anti_debug_SOFTICE1_8_byt_STR_8_ /home//dungthe190680/clamsrch.yara
PADDINGXXPADDING_8_byt_STR_16_ /home//dungthe190680/clamsrch.yara
anti_debug_IsDebuggerPresent_8_byt_STR_17_ /home//dungthe190680/clamsrch.yara
Adler_CRC32_0x01c26a37_32_lil_1024_ /home//dungthe190680/libclamav.dll
Rar29_InitBinEsc_16_lil_16_ /home//dungthe190680/libclamav.dll
zinflate_lengthExtraBits_32_lil_116_ /home//dungthe190680/libclamav.dll
Zlib_base_length_32_lil_116_ /home//dungthe190680/libclamav.dll
zinflate_distanceExtraBits_16_lil_60_ /home//dungthe190680/libclamav.dll
Adler_CRC32_0x191b31d1_32_lil_1024_ /home//dungthe190680/libclamav.dll
CRC_32_IEEE_802_3_poly_0x04c110b7_32_lil_refl_false_ /home//dungthe190680/libclamav.dll
Zlib_base_dist_32_lil_130_ /home//dungthe190680/libclamav.dll
unlz_table_three_16_lil_32_ /home//dungthe190680/libclamav.dll
Rijndael_Td1_0xf4a75051u_32_lil_1024_ /home//dungthe190680/libclamav.dll
zinflate_lengthExtraBits_8_byt_29_ /home//dungthe190680/libclamav.dll
Rijndael_Te4_0x63636363u_32_big_1024_ /home//dungthe190680/libclamav.dll
```

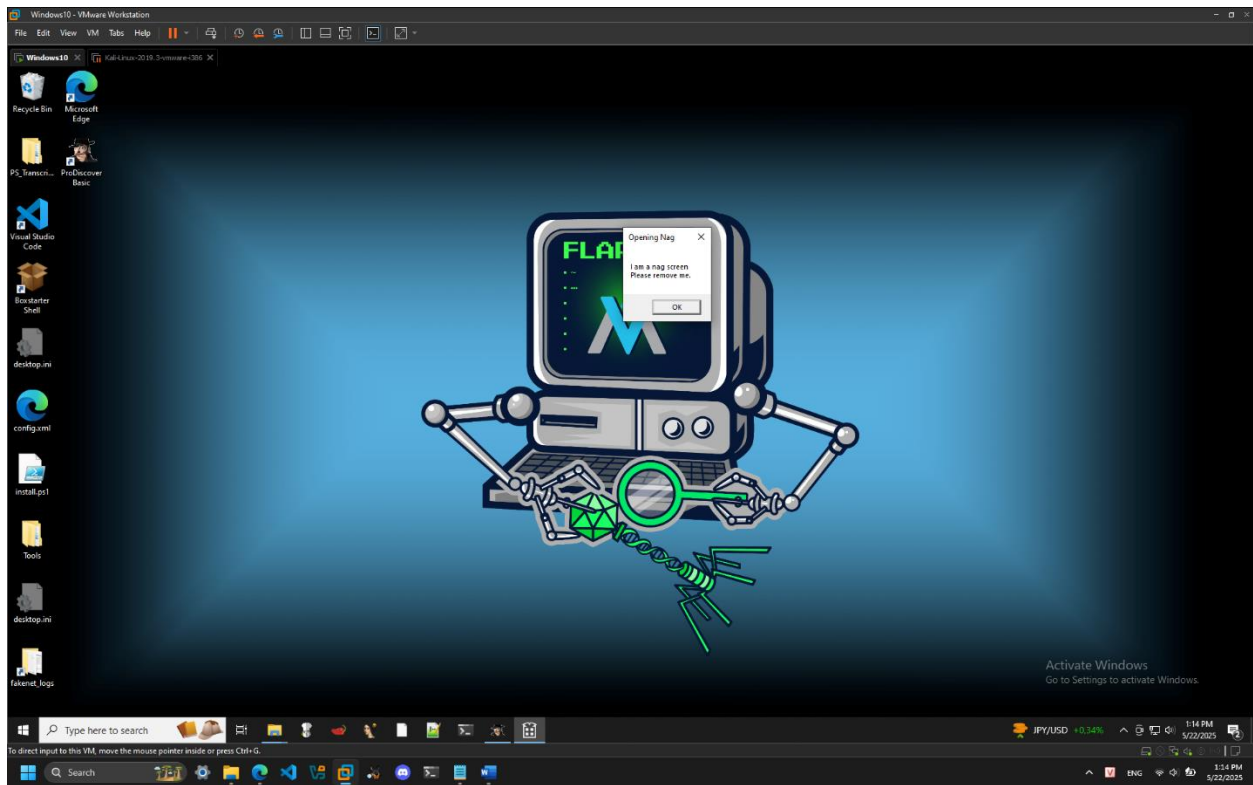
Create a new rule file called custome.yara -> Test yara rules:

```
dungthe190680@dungthe190680:~$ 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 = { 09 50 4e 47 0d 0a 1a 0a }
  condition:
    any of them
}

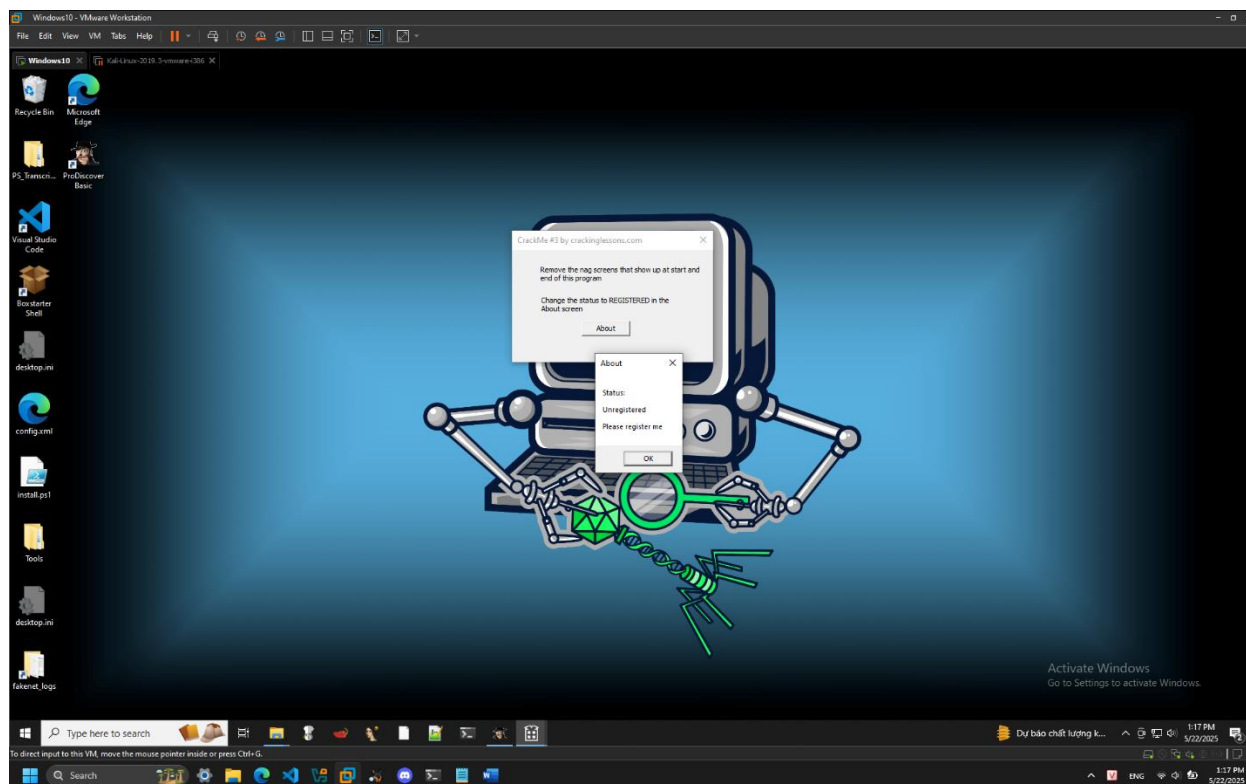
dungthe190680@dungthe190680:~$ yara -r custome.yara /home/dungthe190680/Test/
ConditionsExample /home/dungthe190680/Test//test.txt
GlobalRuleExample /home/dungthe190680/Test//claa_helloWorld.ndb
GlobalRuleExample /home/dungthe190680/Test//test.txt
dungthe190680@dungthe190680:~$
```

### CrackMe #3:

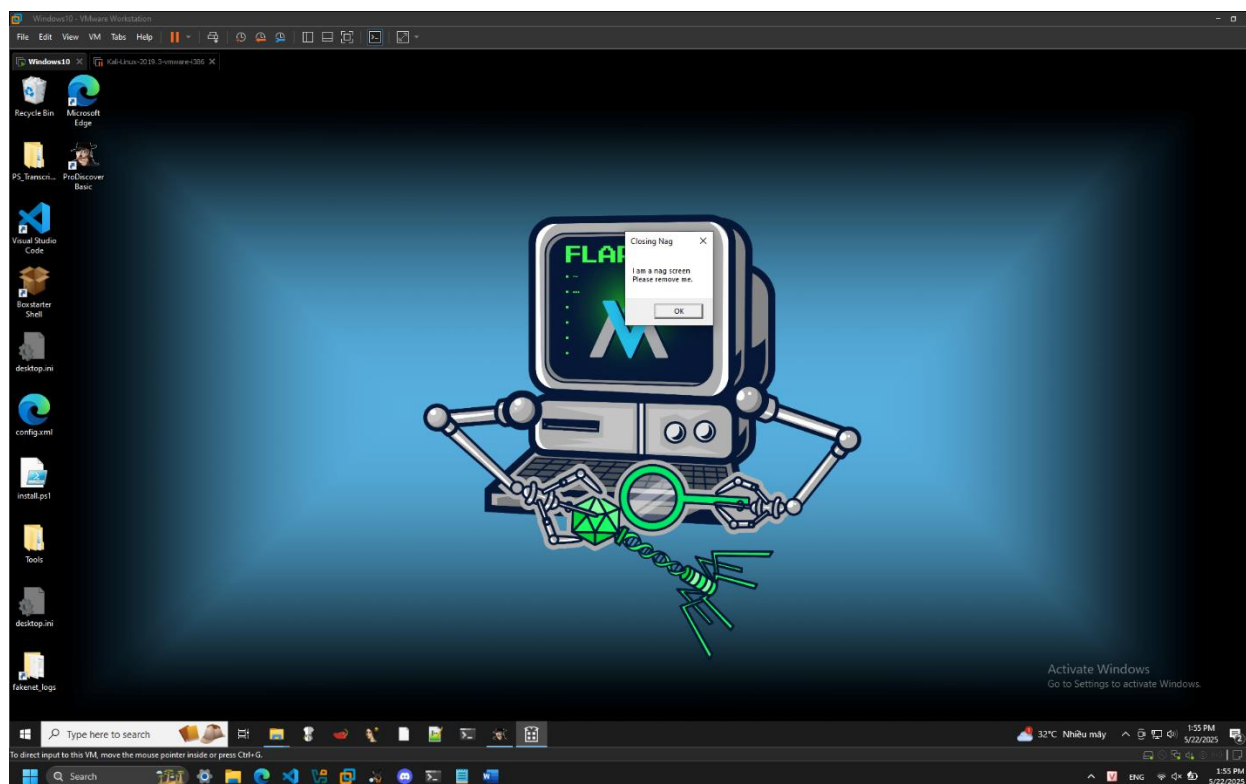
Đầu tiên em thử chạy chương trình và nhận được thông báo có từ khóa “Opening”:



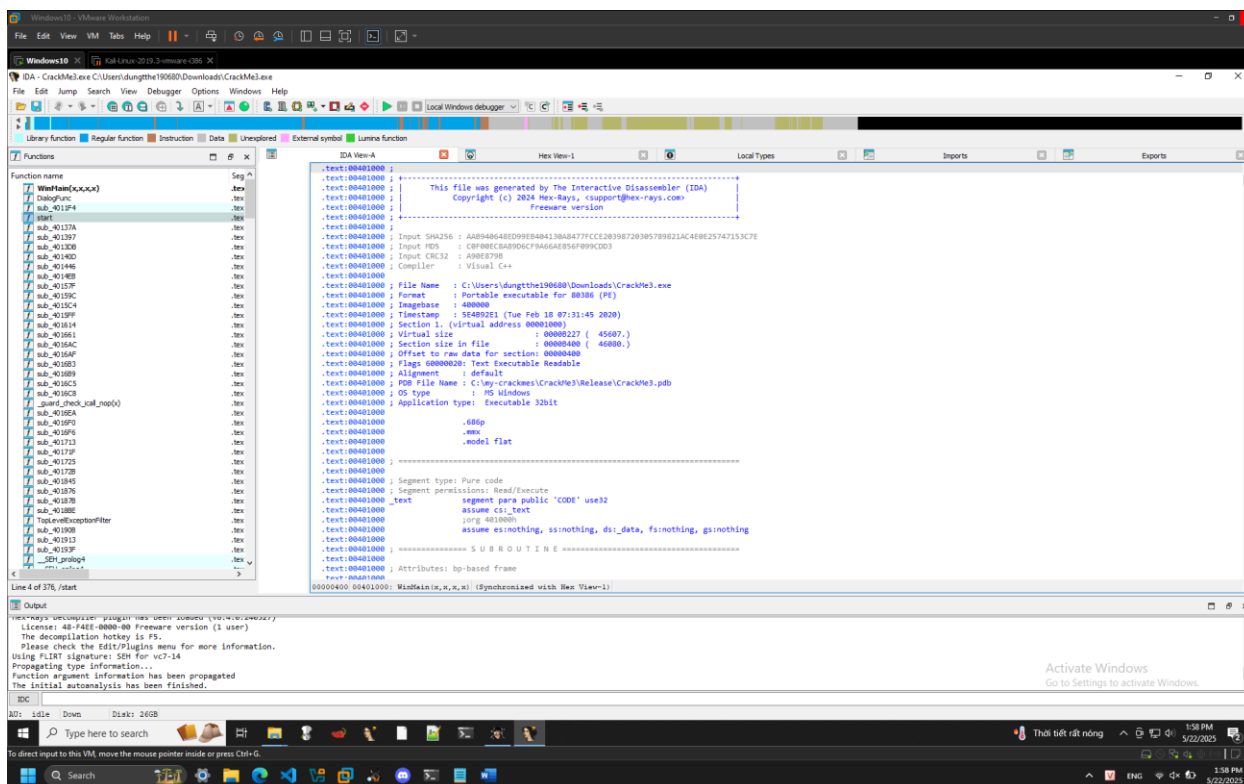
Sau khi tắt thông báo đầu tiên, em nhận được thông báo tiếp theo có từ khóa “Unregistered”:



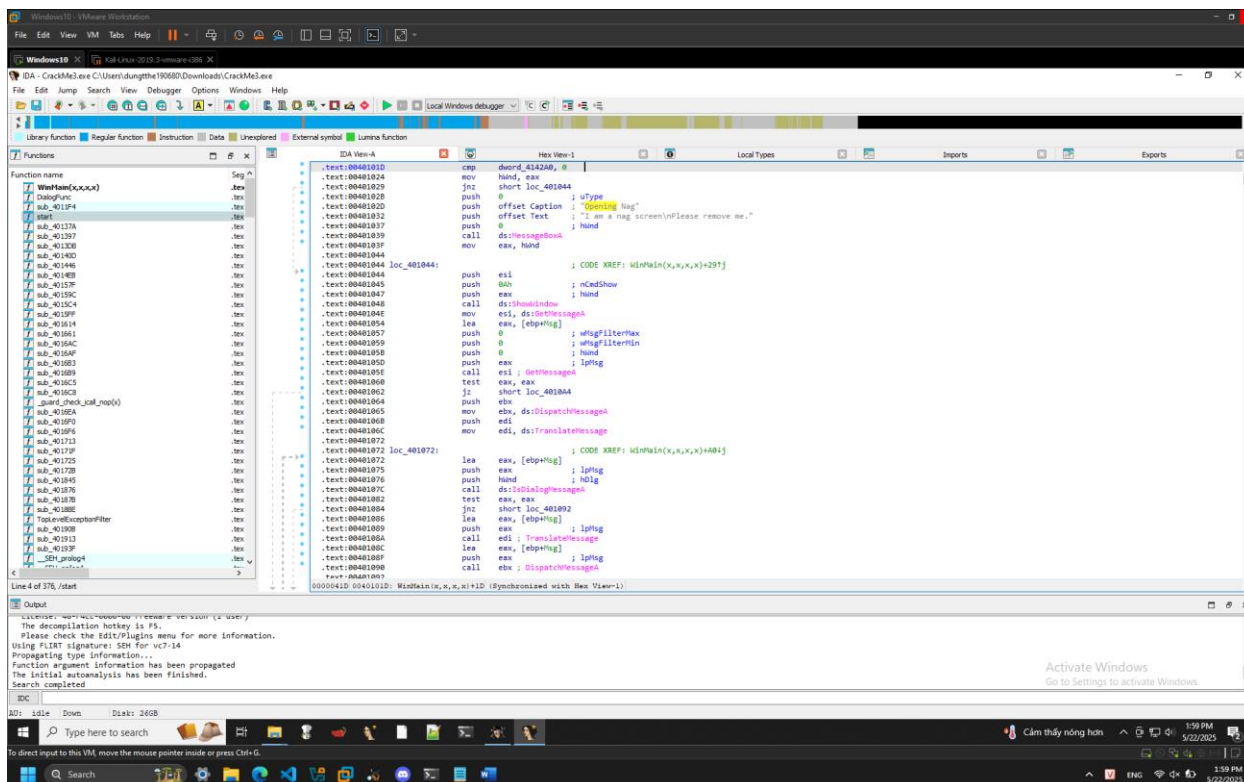
Sau khi tắt thông báo thứ hai, em nhận được thông báo cuối cùng có từ khóa “Closing”:



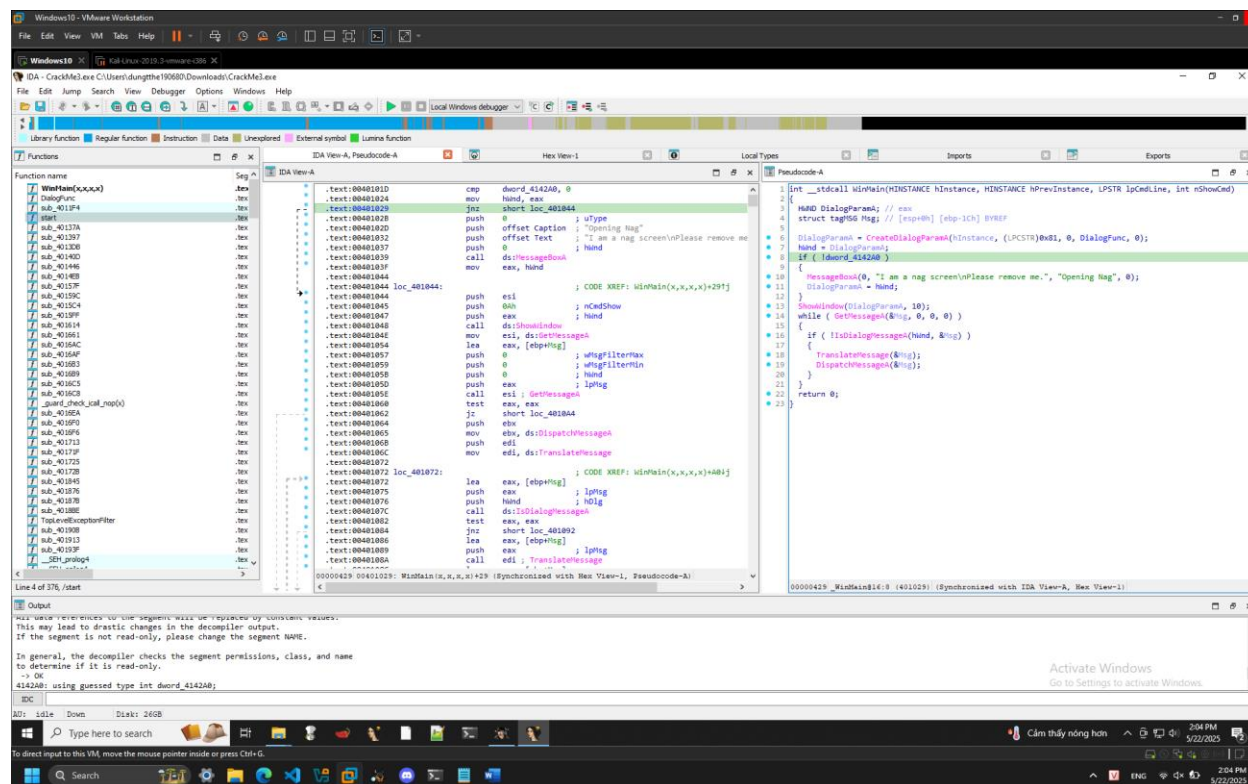
Em mở phần mềm IDA và tiến hành dịch ngược file:



Em search từ khóa “Opening” và được điều hướng đến đoạn code này:

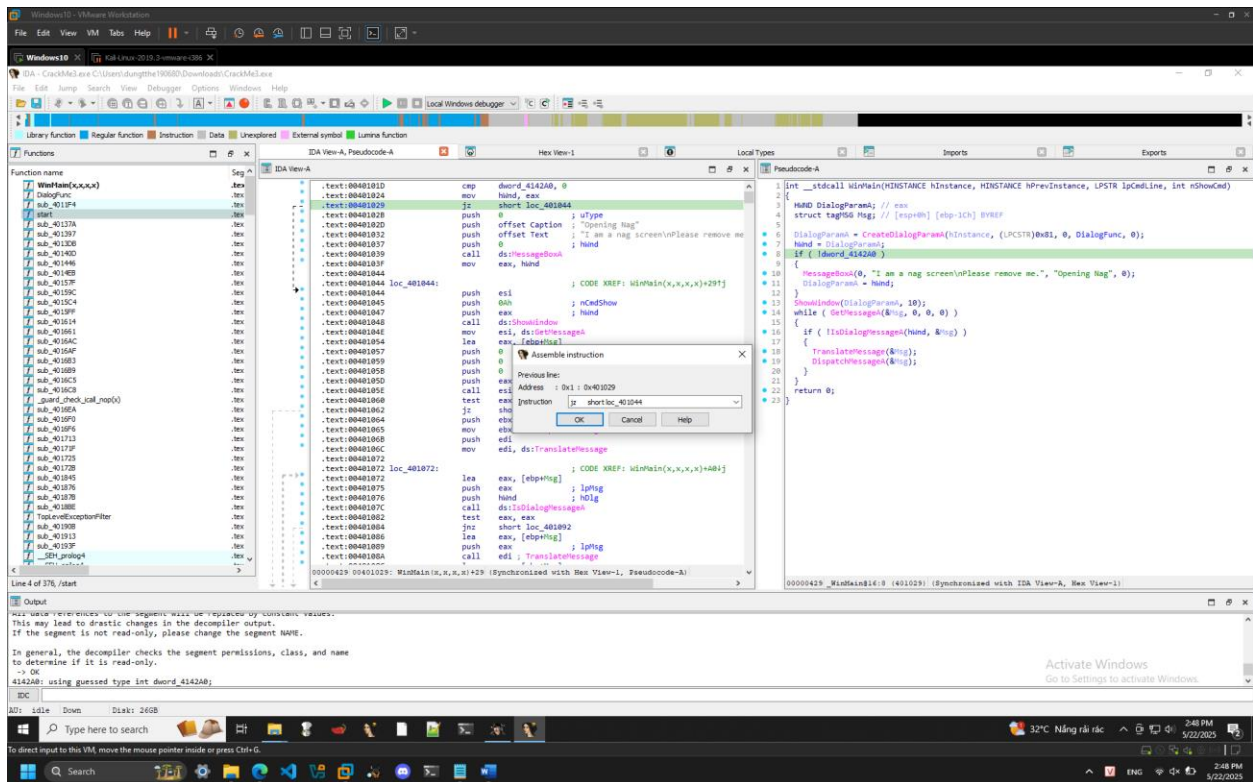


Em bôi đen đoạn code và decompile sang pseudocode thì nhận được đoạn code này:

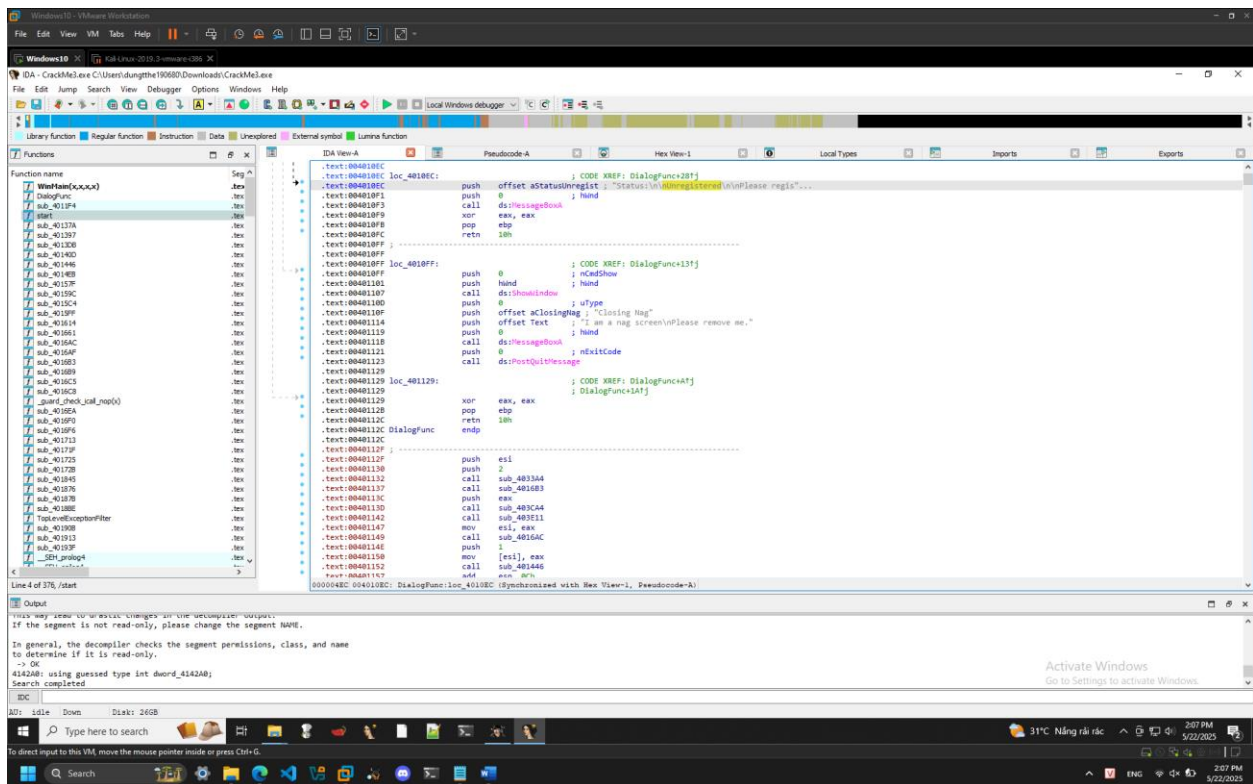


Có thể thấy thông báo đầu tiên được hiển thị nếu giá trị của biến “dword\_4142A0” bằng 0. Vì vậy để ngăn thông báo hiển thị em đảo ngược logic đoạn code bằng cách sửa “jnz” thành “jz”:

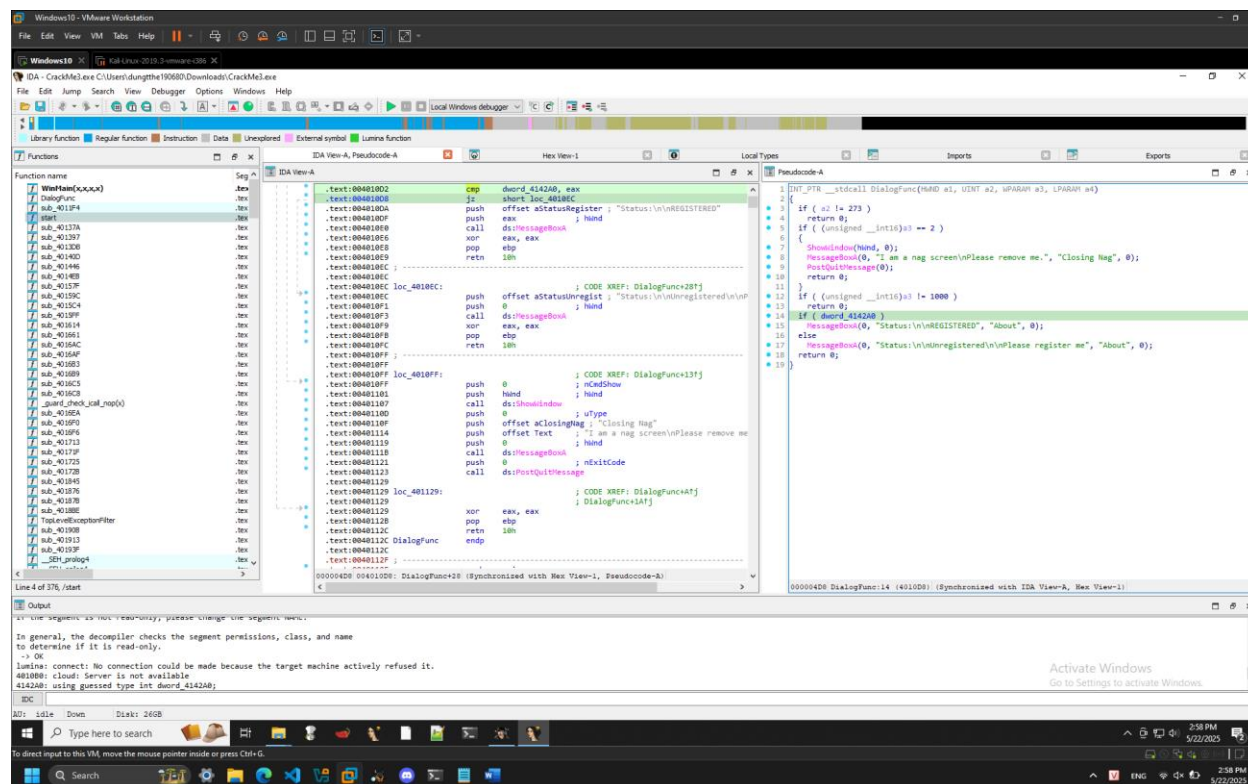




Tiếp theo em search từ khóa “Unregistered” và được điều hướng đến đoạn code này:

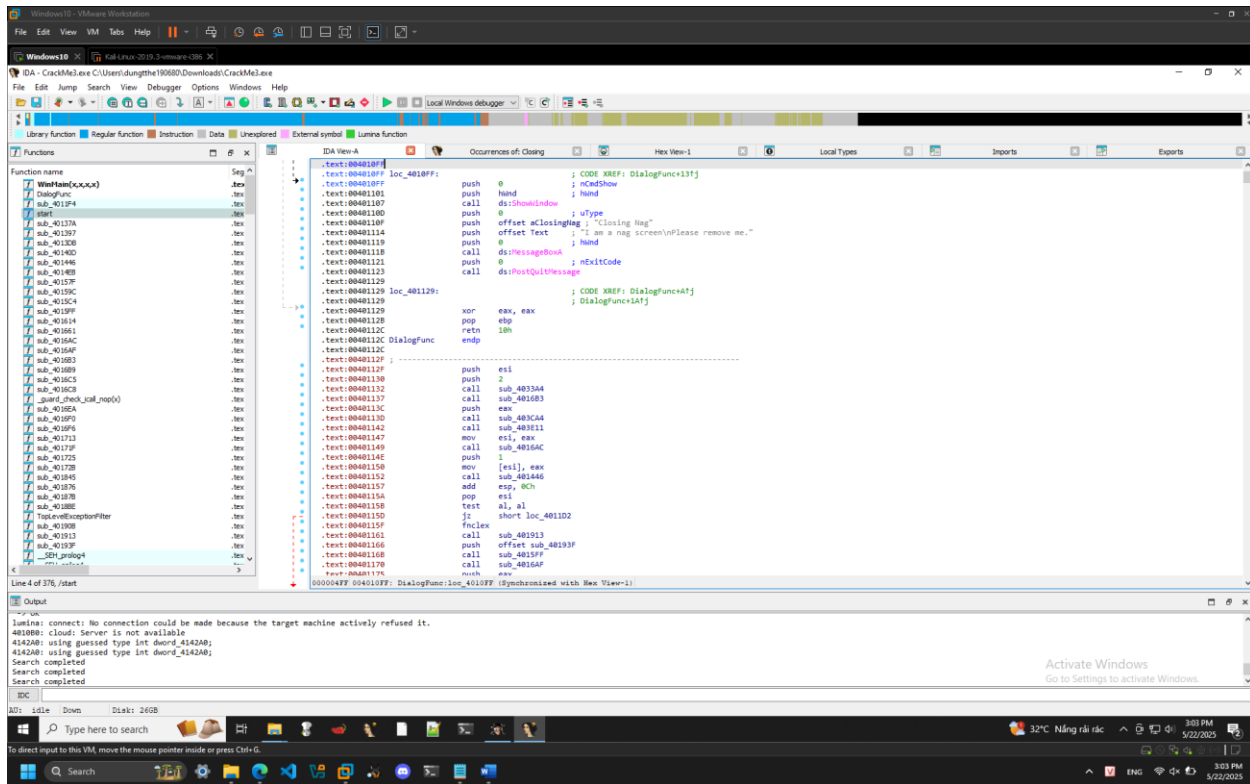
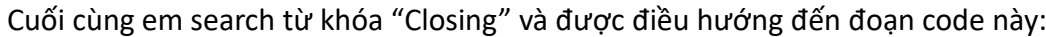


Em bôi đen đoạn code và decompile sang pseudocode thì nhận được đoạn code này:

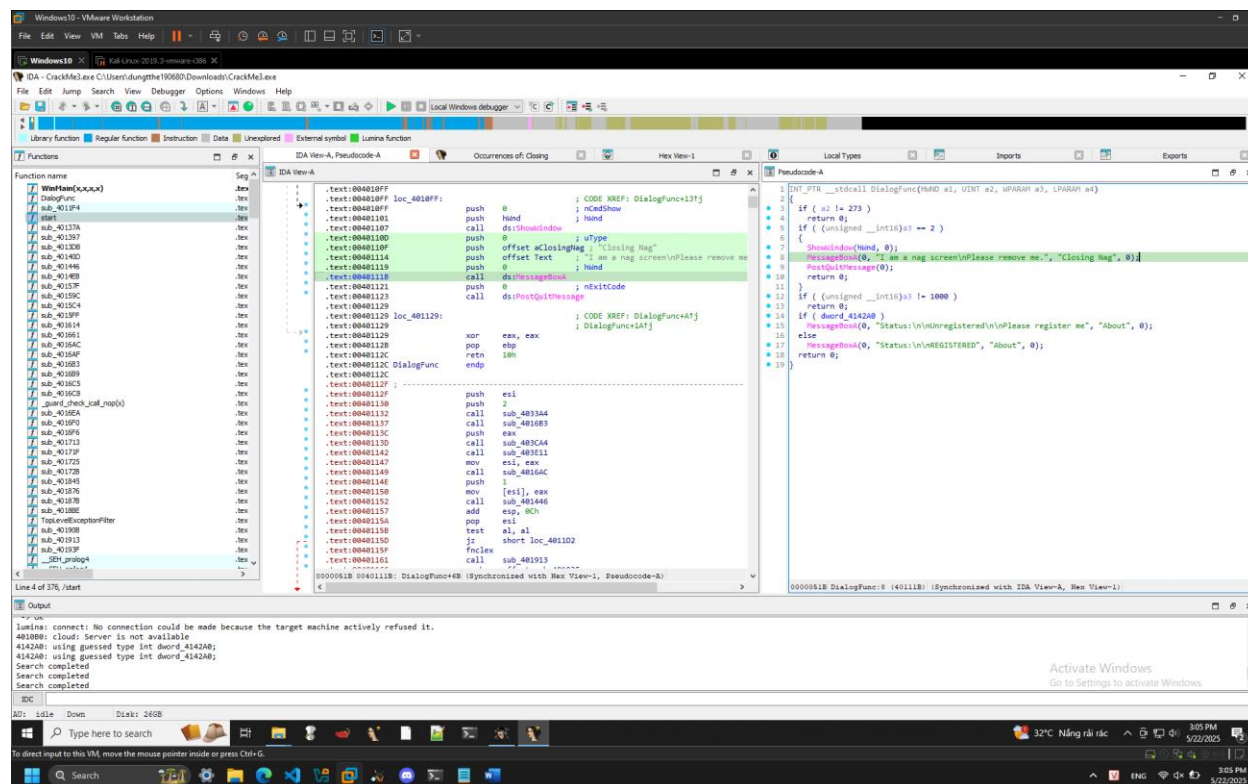


Có thể thấy thông báo chưa đăng ký được hiển thị nếu giá trị của biến “dword\_4142A0” bằng 0. Vì vậy để hiển thị thông báo đã đăng ký em đảo ngược logic đoạn code bằng cách sửa “jz” thành “jnz”:

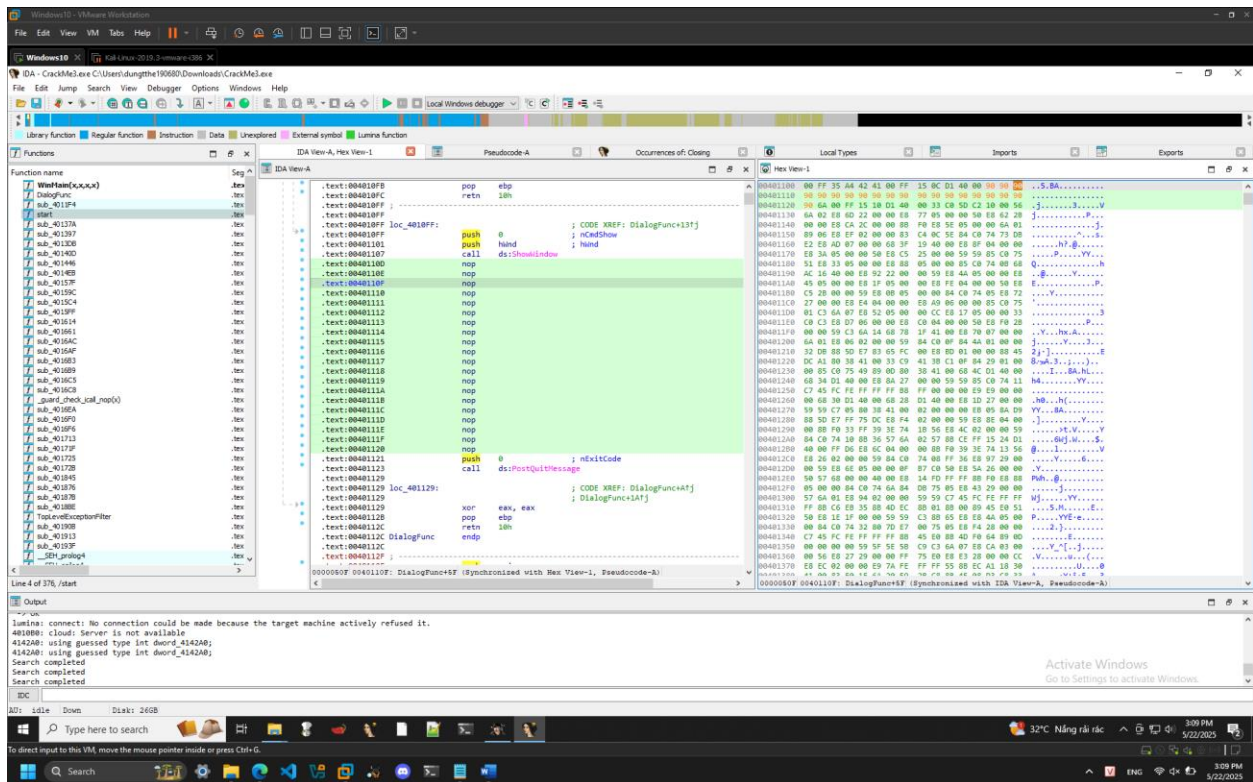




Em bôi đen đoạn code và decompile sang pseudocode thì nhận được đoạn code này:



Có thể thấy thông báo được hiển thị nếu điều kiện của hàm if bằng True, nhưng vì trong hàm if còn gọi các hàm liên quan đến chức năng khác của chương trình nên không thể sửa logic của cả hàm if được. Vì vậy để ngăn thông báo hiển thị em xóa đoạn code gọi hàm hiển thị bằng cách sửa mã hex của chúng thành 90 (nop):



Lưu lại và chạy chương trình sẽ nhận được thông báo đã đăng ký và thông báo khi bắt đầu và kết thúc chương trình sẽ không hiển thị:

