

Họ và tên: Trần Trí Dũng

Mã số sinh viên: HE190680

Lớp: IA1901

Lab 2:

Update the Repository -> Install ClamAV -> Verify ClamAV -> Download Updates Using freshclam:

```
dungthe190680@dungthe1:~$ sudo apt update
Hit:1 http://vn.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://vn.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://vn.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu jammy-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
dungthe190680@dungthe1:~$ sudo apt install clamav clamav-daemon
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
clamav is already the newest version (0.103.12+dfsg-0ubuntu0.22.04.1).
clamav-daemon is already the newest version (0.103.12+dfsg-0ubuntu0.22.04.1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
dungthe190680@dungthe1:~$ clamscan -v
ClamAV 0.103.12/27641/Sun May 18 08:31:14 2025
dungthe190680@dungthe1:~$ sudo systemctl stop clamav-freshclam
dungthe190680@dungthe1:~$ sudo freshclam
Mon May 19 06:22:48 2025 -> ClamAV update process started at Mon May 19 06:22:48 2025
Mon May 19 06:22:49 2025 -> *Your ClamAV installation is OUTDATED!
Mon May 19 06:22:49 2025 -> *Local version: 0.103.12 Recommended version: 1.0.8
Mon May 19 06:22:49 2025 -> DOWNT PAMIC! Read https://docs.clamav.net/manual/Installing.html
Mon May 19 06:22:49 2025 -> daily.cvd database is up-to-date (version: 27641, sigs: 2974857, f-level: 90, builder: rayman)
Mon May 19 06:22:49 2025 -> main.cvd database is up-to-date (version: 62, sigs: 6647427, f-level: 90, builder: sigmgr)
Mon May 19 06:22:49 2025 -> bytecode.cvd database is up-to-date (version: 336, sigs: 83, f-level: 90, builder: nrandolp)
dungthe190680@dungthe1:~$ sudo systemctl start clamav-freshclam
dungthe190680@dungthe1:~$
```

Download Updates Using Official Website:

```
dungtthe190680@dungtthe190680:~$ ls
daily.cvd
dungtthe190680@dungtthe190680:~$ sudo cp daily.cvd /var/lib/clamav/
[sudo] password for dungtthe190680:
dungtthe190680@dungtthe190680:~$ ls /var/lib/clamav/
bytecode.cvd  daily.cvd  freshclam.dat  main.cvd
dungtthe190680@dungtthe190680:~$ clamscan --help

Clam AntiVirus: Scanner 0.103.12
By The ClamAV Team: https://www.clamav.net/about.html#credits
(C) 2022 Cisco Systems, Inc.

clamscan [options] [file/directory/-]

--help                -h          Show this help
--version             -V          Print version number
--verbose             -v          Be verbose
--archive-verbose     -a          Show filenames inside scanned archives
--debug               -d          Enable libclamav's debug messages
--quiet               -q          Only output error messages
--stdout              -s          Write to stdout instead of stderr. Does not affect 'debug' messages.
--no-summary          -S          Disable summary at end of scanning
--infected             -i          Only print infected files
--suppress-ok-results -o          Skip printing OK files
--bell                -b          Sound bell on virus detection

--tempdir=DIRECTORY   Create temporary files in DIRECTORY
--leave-temp[yes/no(*)] Do not remove temporary files
--gen-json[yes/no(*)]  Generate JSON description of scanned file(s). JSON will be printed and also-
                        dropped to the temp directory if --leave-temp is enabled.
--database=FILE/DIR   -d FILE/DIR Load virus database from FILE or load all supported db files from DIR
--official-db-only[yes/no(*)] Only load official signatures
--log=FILE             -l FILE      Save scan report to FILE
--recursive[yes/no(*)] -r          Scan subdirectories recursively
--allmatch[yes/no(*)]  -z          Continue scanning within file after finding a match
--cross-fs[yes/no(*)]  -x          Scan files and directories on other filesystems
--follow-dir-symlinks[0/1(*)/2] Follow directory symlinks (0 = never, 1 = direct, 2 = always)
--follow-file-symlinks[0/1(*)/2] Follow file symlinks (0 = never, 1 = direct, 2 = always)
--file-list=FILE       -f FILE      Scan files from FILE
--remove[yes/no(*)]    -R          Remove infected files. Be careful!
--move=DIRECTORY       -M          Move infected files into DIRECTORY
--copy=DIRECTORY       -C          Copy infected files into DIRECTORY
--exclude=REGEX         -E          Don't scan file names matching REGEX
--exclude-dir=REGEX     -ED         Don't scan directories matching REGEX
--include=REGEX         -I          Only scan file names matching REGEX
--include-dir=REGEX     -ID         Only scan directories matching REGEX

--bytecode[yes/no]     -b          Load bytecode from the database
--bytecode-unsigned[yes/no(*)] Load unsigned bytecode
                        **Caution**: You should NEVER run bytecode signatures from untrusted sources.
                        Doing so may result in arbitrary code execution.
--bytecode-timeout=N    Set bytecode timeout (in milliseconds)
--statistics[none(*)/bytecode/pcr] Collect and print execution statistics
--detect-pua[yes/no(*)] Detect Possibly Unwanted Applications
--exclude-pua=CAT       Skip PUA signs of category CAT
--include-pua=CAT       Load PUA signs of category CAT
--detect-structured[yes/no(*)] Detect structured data (SSN, Credit Card)
--structured-ssn-format=X SSN format (0=normal,1=stripped,2=both)
--structured-ssn-count=N Min SSN count to generate a detect
--structured-cc-count=N  Min CC count to generate a detect
--structured-cc-mode=X   CC mode (0=credit debit and private label, 1=credit cards only)
--scan-mail[yes/no]     -m          Scan mail files
--phishing-sig[yes/no]  -P          Enable email signature-based phishing detection
--phishing-scan-urls[yes/no] Enable URL signature-based phishing detection
--heuristic-alerts[yes/no] Heuristic alerts

----- SCAN SUMMARY -----
Known viruses: 8796351
Engine version: 0.103.12
Scanned directories: 1
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 31.591 sec (0 m 31 s)
Start Date: 2025:05:19 07:00:32
End Date: 2025:05:19 07:01:04
dungtthe190680@dungtthe190680:~$
```

Scan a Directory:

```
dungtthe190680@dungtthe190680:~$ sudo mkdir Test
dungtthe190680@dungtthe190680:~$ ls
daily.cvd  Test
dungtthe190680@dungtthe190680:~$ cd Test/
dungtthe190680@dungtthe190680:~/Test$ sudo curl -O https://secure.eicar.org/eicar.com.txt
% Total % Received % Xferd Average Speed Time Time Current
           Dload Upload Total Spent Left Speed
100 68 100 68 0 0 54 0 0:00:01 0:00:01 --:--:-- 54
dungtthe190680@dungtthe190680:~/Test$ cd
dungtthe190680@dungtthe190680:~$ ls
daily.cvd  Test
dungtthe190680@dungtthe190680:~$ sudo clamscan --infected --remove --recursive Test/
/home/dungtthe190680/Test/eicar.com.txt: Win.Test.EICAR_HDB-1 FOUND
/home/dungtthe190680/Test/eicar.com.txt: Removed.

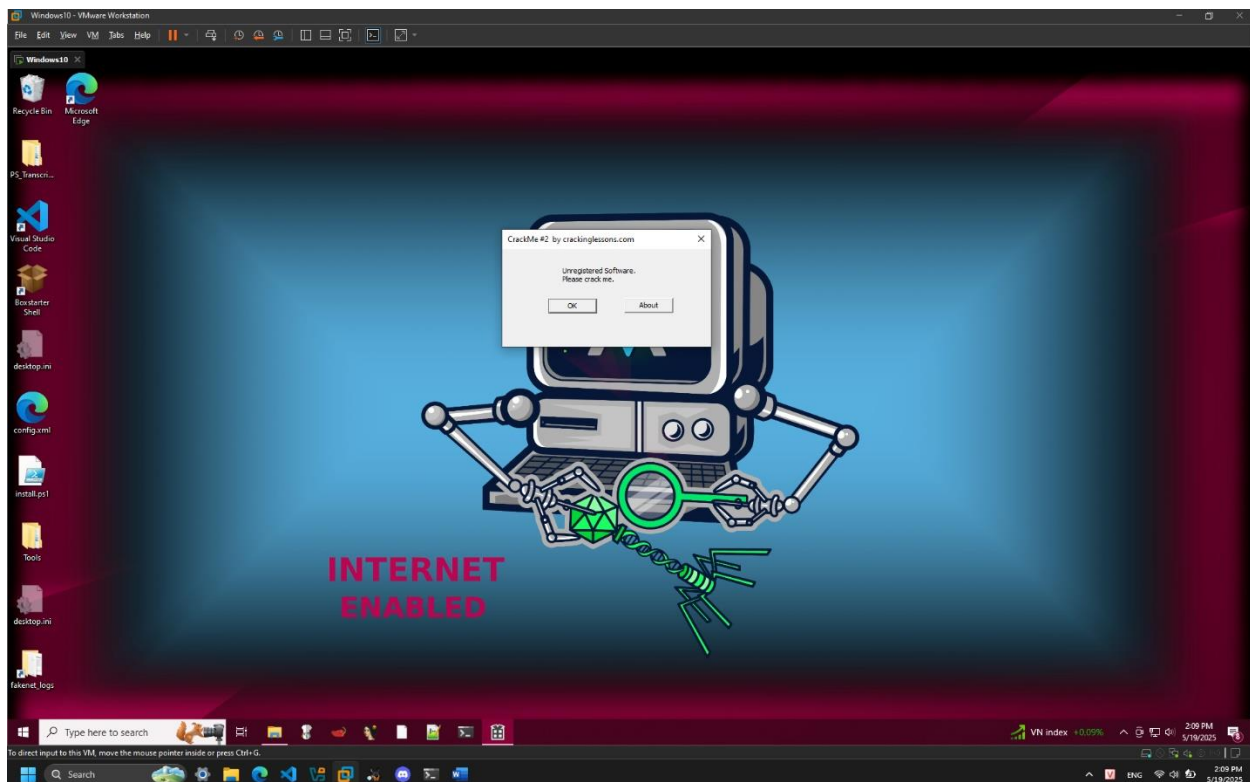
----- SCAN SUMMARY -----
Known viruses: 8796351
Engine version: 0.103.12
Scanned directories: 1
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 31.591 sec (0 m 31 s)
Start Date: 2025:05:19 07:00:32
End Date: 2025:05:19 07:01:04
dungtthe190680@dungtthe190680:~$
```

```
dungthe190680@dungthe15:~$ sudo vi Clam_HelloWorld.ndb
dungthe190680@dungthe15:~$ cat Clam_HelloWorld.ndb
Clam_HelloWorld:0:*:68656c6cf*776f726c64
dungthe190680@dungthe15:~$ sudo vi test.txt
dungthe190680@dungthe15:~$ cat test.txt
hello world
dungthe190680@dungthe15:~$ clamscan -d Clam_HelloWorld.ndb test.txt
/home/dungthe190680/test.txt: Clam_HelloWorld.UNOFFICIAL FOUND

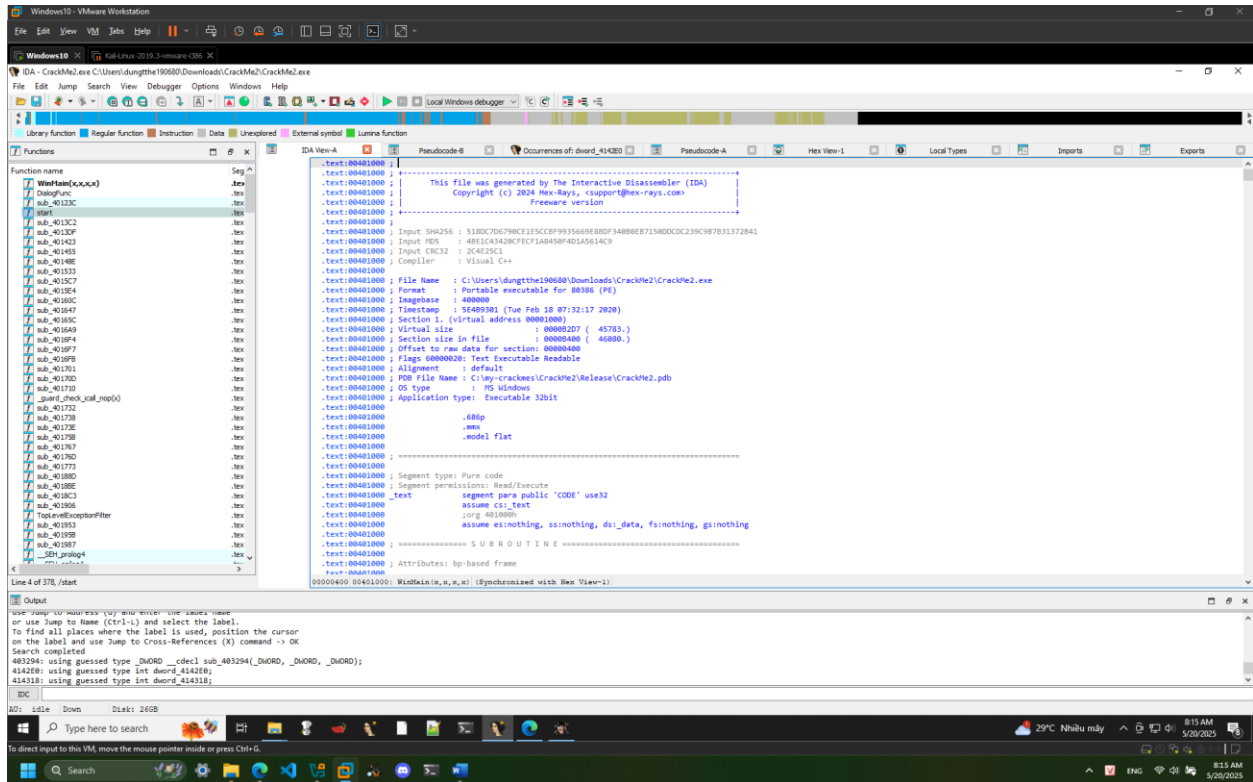
----- SCAN SUMMARY -----
Known viruses: 1
Engine version: 0.103.12
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.08 MB
Data read: 0.08 MB (ratio 0.00:1)
Time: 0.014 sec (0 m 0 s)
Start Date: 2025:05:19 07:05:41
End Date: 2025:05:19 07:05:41
dungthe190680@dungthe15:~$
```

CrackMe #2

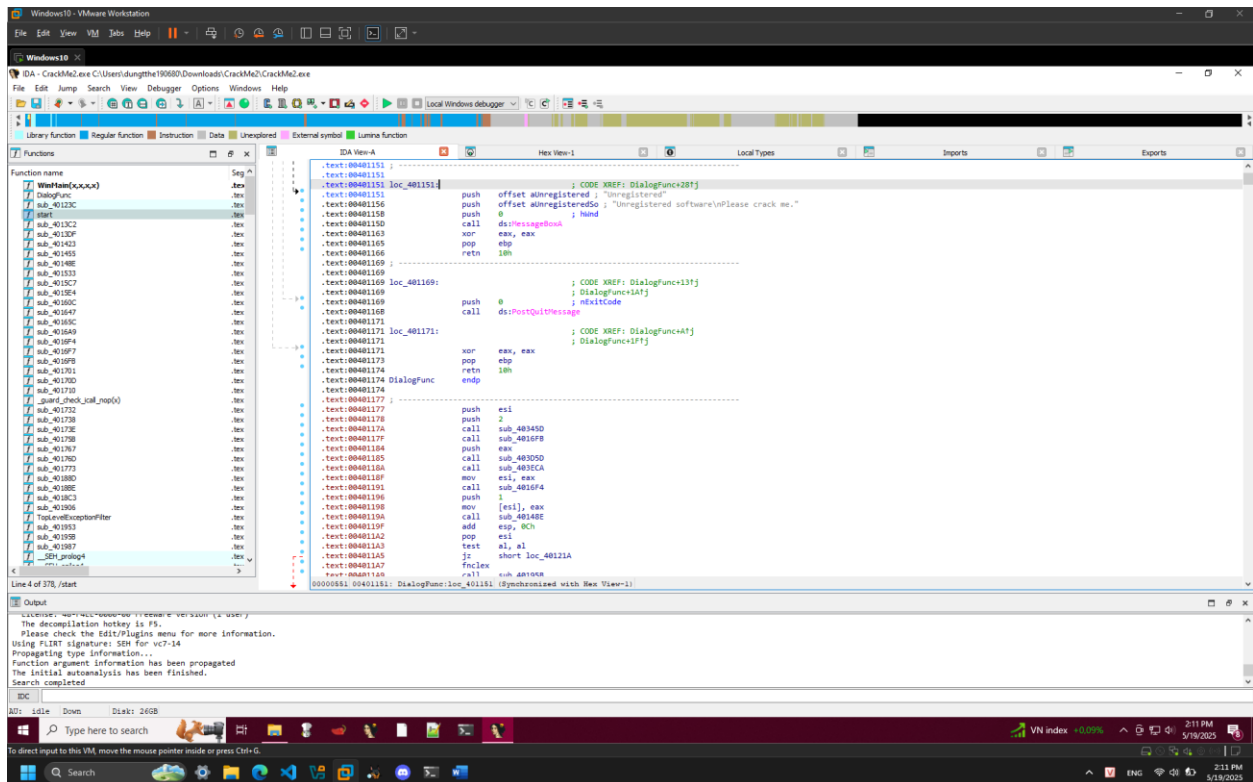
Đầu tiên em thử chạy chương trình và nhận được thông báo có từ khóa “Unregistered”:



Sau đó em mở phần mềm IDA và tiến hành dịch ngược file:



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



The screenshot shows a Windows 10 desktop with a Windows VM running. The VM is named 'Windows10' and is running a debugger (IDA Pro) on a file named 'CrackMe2.exe'. The debugger is in the 'Pseudocode-A' view, showing a function named 'DialogFunc' with assembly and pseudocode. The pseudocode shows a loop that checks if a3 is 2 or 1000, and if not, it calls MessageBox with the text 'About'. The assembly view on the left shows the corresponding assembly instructions. The output window at the bottom shows the message 'About' being displayed.

File Edit Jump Search View Debugger Options Windows Help

Library function Regular function Instruction Data Unexplored External symbol Lumina function

Functions

Function name

WinMain@x64

DialogFunc

sub_40123C

start

sub_4013C2

sub_4013D0

sub_401421

sub_401455

sub_40148E

sub_401533

sub_4015C7

sub_40160C

sub_401647

sub_40169C

sub_4016A9

sub_4016F4

sub_4016F7

sub_4016F8

sub_401701

sub_40170D

sub_401719

_guard_check_icall_nop

sub_401722

sub_401728

sub_40173E

sub_401758

sub_401767

sub_40176D

sub_401773

sub_40180D

sub_40186C

sub_4018C3

sub_401908

TlsEventListenerFilter

sub_401913

sub_401939

sub_401987

_JTI_000004

sub_4019C4

sub_4019C5

sub_4019C6

sub_4019C7

sub_4019C8

sub_4019C9

sub_4019CA

sub_4019CB

sub_4019CC

sub_4019CD

sub_4019CE

sub_4019CF

sub_4019D0

sub_4019D1

sub_4019D2

sub_4019D3

sub_4019D4

sub_4019D5

sub_4019D6

sub_4019D7

sub_4019D8

sub_4019D9

sub_4019DA

sub_4019DB

sub_4019DC

sub_4019DD

sub_4019DE

sub_4019DF

sub_4019E0

sub_4019E1

sub_4019E2

sub_4019E3

sub_4019E4

sub_4019E5

sub_4019E6

sub_4019E7

sub_4019E8

sub_4019E9

sub_4019EA

sub_4019EB

sub_4019EC

sub_4019ED

sub_4019EE

sub_4019EF

sub_4019F0

sub_4019F1

sub_4019F2

sub_4019F3

sub_4019F4

sub_4019F5

sub_4019F6

sub_4019F7

sub_4019F8

sub_4019F9

sub_4019FA

sub_4019FB

sub_4019FC

sub_4019FD

sub_4019FE

sub_4019FF

sub_401A00

sub_401A01

sub_401A02

sub_401A03

sub_401A04

sub_401A05

sub_401A06

sub_401A07

sub_401A08

sub_401A09

sub_401A0A

sub_401A0B

sub_401A0C

sub_401A0D

sub_401A0E

sub_401A0F

sub_401A10

sub_401A11

sub_401A12

sub_401A13

sub_401A14

sub_401A15

sub_401A16

sub_401A17

sub_401A18

sub_401A19

sub_401A1A

sub_401A1B

sub_401A1C

sub_401A1D

sub_401A1E

sub_401A1F

sub_401A20

sub_401A21

sub_401A22

sub_401A23

sub_401A24

sub_401A25

sub_401A26

sub_401A27

sub_401A28

sub_401A29

sub_401A2A

sub_401A2B

sub_401A2C

sub_401A2D

sub_401A2E

sub_401A2F

sub_401A30

sub_401A31

sub_401A32

sub_401A33

sub_401A34

sub_401A35

sub_401A36

sub_401A37

sub_401A38

sub_401A39

sub_401A3A

sub_401A3B

sub_401A3C

sub_401A3D

sub_401A3E

sub_401A3F

sub_401A40

sub_401A41

sub_401A42

sub_401A43

sub_401A44

sub_401A45

sub_401A46

sub_401A47

sub_401A48

sub_401A49

sub_401A4A

sub_401A4B

sub_401A4C

sub_401A4D

sub_401A4E

sub_401A4F

sub_401A50

sub_401A51

sub_401A52

sub_401A53

sub_401A54

sub_401A55

sub_401A56

sub_401A57

sub_401A58

sub_401A59

sub_401A5A

sub_401A5B

sub_401A5C

sub_401A5D

sub_401A5E

sub_401A5F

sub_401A60

sub_401A61

sub_401A62

sub_401A63

sub_401A64

sub_401A65

sub_401A66

sub_401A67

sub_401A68

sub_401A69

sub_401A6A

sub_401A6B

sub_401A6C

sub_401A6D

sub_401A6E

sub_401A6F

sub_401A70

sub_401A71

sub_401A72

sub_401A73

sub_401A74

sub_401A75

sub_401A76

sub_401A77

sub_401A78

sub_401A79

sub_401A7A

sub_401A7B

sub_401A7C

sub_401A7D

sub_401A7E

sub_401A7F

sub_401A80

sub_401A81

sub_401A82

sub_401A83

sub_401A84

sub_401A85

sub_401A86

sub_401A87

sub_401A88

sub_401A89

sub_401A8A

sub_401A8B

sub_401A8C

sub_401A8D

sub_401A8E

sub_401A8F

sub_401A90

sub_401A91

sub_401A92

sub_401A93

sub_401A94

sub_401A95

sub_401A96

sub_401A97

sub_401A98

sub_401A99

sub_401A9A

sub_401A9B

sub_401A9C

sub_401A9D

sub_401A9E

sub_401A9F

sub_401AA0

sub_401AA1

sub_401AA2

sub_401AA3

sub_401AA4

sub_401AA5

sub_401AA6

sub_401AA7

sub_401AA8

sub_401AA9

sub_401AAA

sub_401AAB

sub_401AAC

sub_401AAD

sub_401AAE

[illegible]

The screenshot shows a Windows 10 desktop with a debugger (IDA Pro) open. The main window displays the assembly code for the 'WinMain@xx' function. The code includes standard Windows API calls like 'MessageBox' and 'CreateDialogParam'. The user has set a breakpoint at the start of the function, and the 'Registers' window shows the 'eax' register containing the value 00004211. The 'Output' window shows the results of the debugger's analysis, including the address of the 'WinMain@xx' function.

Assembly code snippet:

```

1 int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nShowCmd)
2 {
3     HANDLE hFile; // eax
4     void *v5; // esi
5     struct tagMSG Msg; // [esp+4h] [ebp-1ch] BYREF
6
7     hDlg = CreateDialogParam(hInstance, (LPCSTR)hInstance, 0, DialogFunc, 0);
8     ShowWindow(hDlg, 1);
9     hFile = CreateFile("keyfile.txt", 0x00000000, 1, 0, 3u, 0x00000000, 0);
10    v5 = hFile;
11    if (hFile != INVALID_HANDLE_VALUE)
12    {
13        if (!ReadFile(hFile, &Msg, 0x100, &v5, 0))
14        {
15            dword_414208 = 1;
16            sub_401204(Msg, 64, &Msg);
17            SetDlgItemText(hDlg, -1, Text);
18        }
19        CloseHandle(hFile);
20    }
21    for (dword_414318 = GetMessage(&Msg, 0, 0, 0); dword_414318 < GetMessage(&Msg, 0, 0, 0);)
22    {
23        if (!IsDialogMessage(hDlg, &Msg))
24        {
25            TranslateMessage(&Msg);
26            DispatchMessage(&Msg);
27        }
28    }
29    return 0;
30 }

```

Registers window:

Register	Value
eax	00004211
ecx	00000000
edx	00000000
ebx	00000000
esi	00000000
edi	00000000
eip	00401000

Output window:

```

user 'jump to address (or) enter the label name
or use jump to Name (Ctrl-L) and select the label.
To find all places where the label is used, position the cursor
on the label and use jump to Cross-References (X) command -> OK
Search completed
401204: using guessed type dword_401204 (dword_401204, dword_401204);
414208: using guessed type int dword_414208;
414318: using guessed type int dword_414318;

```

The screenshot shows a Windows File Explorer window with the address bar set to 'C:\Users\dungtt\Downloads\CrackMe2'. The left sidebar shows the 'Downloads' folder selected. The main pane displays a list of files in the 'CrackMe2' folder:

Name	Date modified	Type	Size
CrackMe2.exe	2/18/2025 2:32 PM	Application	164 KB
CrackMe2.exe.id0	5/19/2025 2:10 PM	ID0 File	16 KB
CrackMe2.exe.id1	5/19/2025 2:10 PM	ID1 File	288 KB
CrackMe2.exe.id2	5/19/2025 2:10 PM	ID2 File	1 KB
CrackMe2.exe.nam	5/19/2025 2:10 PM	NAM File	0 KB
CrackMe2.exe.til	5/19/2025 2:10 PM	TL File	1 KB
keyfile.txt	5/19/2025 2:30 PM	Text Document	1 KB

A Notepad window titled 'keyfile.txt - Notepad' is open, showing the contents of the 'keyfile.txt' file. The text in the Notepad window is:

```
File Edit Format View Help
dungttthe198688
```

The status bar at the bottom of the Notepad window indicates 'Ln 1, Col 15', '100%' zoom, 'Windows (CRLF)' encoding, and 'UTF-8' file type.

Chạy lại chương trình sẽ nhận được kết quả đã đăng ký thành công:

