

**THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
KHOA CÔNG NGHỆ THÔNG TIN**



Trần Đại Chí - 18127070

Trần Huy Vũ - 18127257

ĐỀ TÀI

Crack

Chuyên ngành: Công nghệ thông tin

Môn: Kiến trúc máy tính và hợp ngữ

Thành phố Hồ Chí Minh - 2019

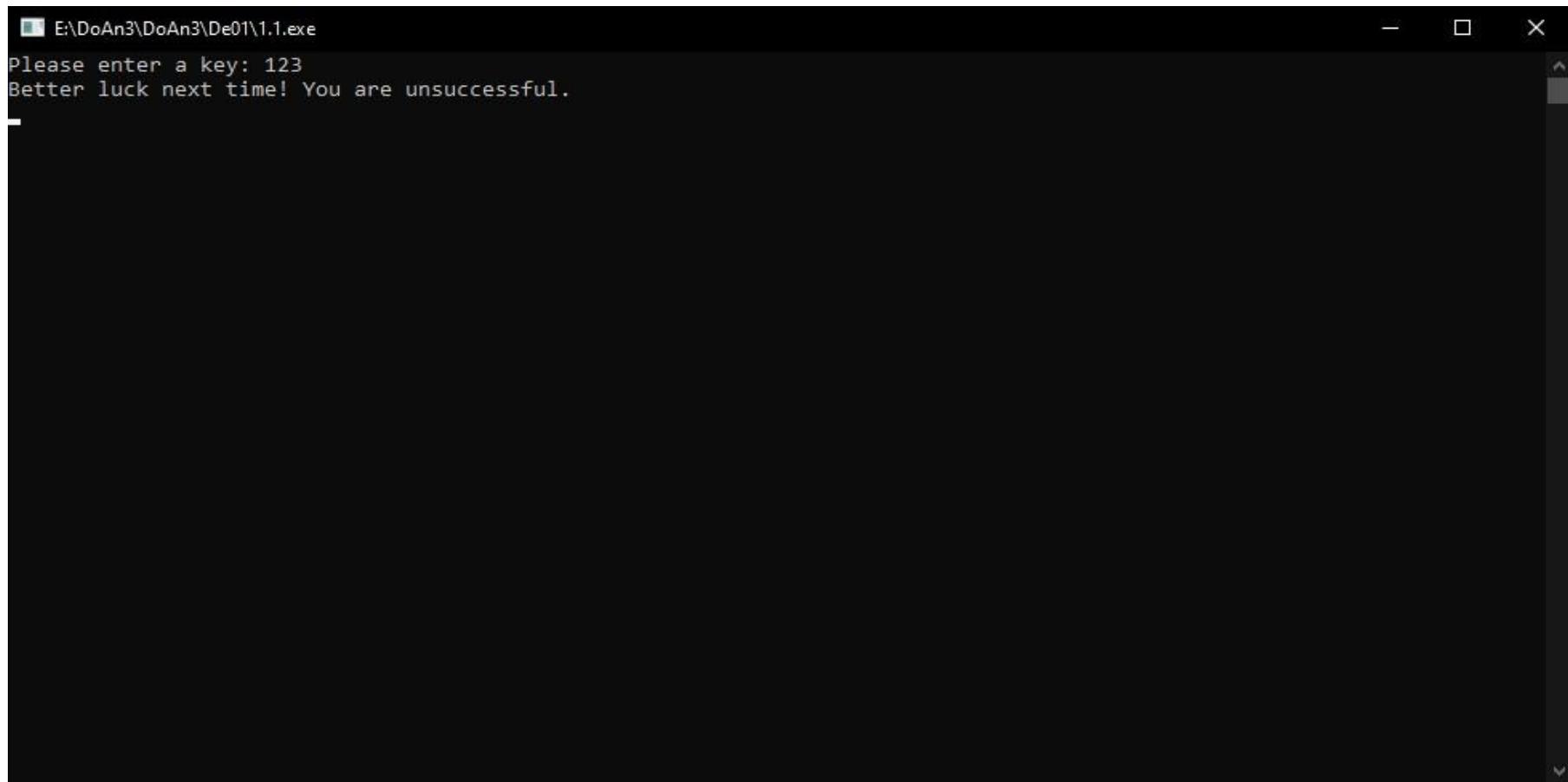
THÔNG TIN THÀNH VIÊN NHÓM

STT	Họ tên	MSSV
1	Trần Đại Chí	18127070
2	Trần Huy Vũ	18127257

I. BẢNG PHÂN CÔNG CÔNG VIỆC

Trần Đại Chí	1.2, 1.5, viết keygen
Trần Huy Vũ	1.1, 1.3, 1.4

1.1



A screenshot of a terminal window titled "E:\DoAn3\DoAn3\De01\1.1.exe". The window contains the following text:
Please enter a key: 123
Better luck next time! You are unsuccessful.

Đầu tiên ta chạy chương trình và nhập vào 1 số bất kì chương trình sẽ hiện thông báo “Better luck next time! You are unsuccessful”

OllyDbg - 1.1.exe - [Text strings referenced in 1_1.text]

The screenshot shows the OllyDbg interface with the 'Text strings' search results window open. The window has three columns: Address, Disassembly, and Text string. The 'Text string' column contains several ASCII strings related to CPU selection and shared pointer assertions.

Address	Disassembly	Text string
00401220	PUSH EBP	(Initial CPU selection)
00401302	MOV DWORD PTR SS:[ESP],1_1.00403000	ASCII "Please enter a key: "
00401316	MOV DWORD PTR SS:[ESP],1_1.00403015	ASCII "%d"
00401330	MOV DWORD PTR SS:[ESP],1_1.00403018	ASCII "Congratulation! You are successful."
0040133E	MOV DWORD PTR SS:[ESP],1_1.00403040	ASCII "Better luck next time! You are unsuccessful."
00401517	MOV ECX,1_1.00403094	ASCII "w32_sharedptr->size == sizeof(W32_EH_SHARED)"
00401529	MOV DWORD PTR SS:[ESP],1_1.004030C1	ASCII "%s:%u: failed assertion '%s'"
00401530	MOV EAX,1_1.004030E0	ASCII ".../gcc/gcc/config/i386/w32-shared-ptr.c"
0040153E	MOV EAX,1_1.0040310C	ASCII "GetAtomNameA (atom, s, sizeof(s)) != 0"

Sau đó ta mở OllyDbg, mở 1.1.exe, chuột phải chọn search for -> All preferred text strings, ta thấy được hai chuỗi hiện ra thông báo khi ta nhập key đúng và khi nhập sai. Sau đó nhấn vào đi đến đoạn mã chưa chuỗi đó

OllyDbg - 1.1.exe - [CPU - main thread, module 1_1]

File View Debug Plugins Options Window Help

L E M T W H C / K B R ... S ?

004012F8	. E8 A3040000	CALL 1_1.004017A0	
004012FD	. E8 3E010000	CALL 1_1.00401440	
00401302	. C70424 00304000	MOV DWORD PTR SS:[ESP],1_1.00403000	ASCII "Please enter a key: "
00401309	. E8 A2050000	CALL <JMP.&msvcrt.printf>	printf
0040130E	. C74424 04 1040	MOV DWORD PTR SS:[ESP+4],1_1.00404010	ASCII "%d"
00401316	. C70424 15304000	MOV DWORD PTR SS:[ESP],1_1.00403015	scanf
0040131D	. E8 7E050000	CALL <JMP.&msvcrt.scprintf>	
00401322	. E8 69FFFFFF	CALL 1_1.00401290	
00401327	. 893D 10404000	CMP DWORD PTR DS:[404010],1	
0040132E	.~ 75 0E	JNZ SHORT 1_1.0040133E	
00401330	. C70424 18304000	MOV DWORD PTR SS:[ESP],1_1.00403018	ASCII "Congratulation! You are successful."
00401337	. E8 74050000	CALL <JMP.&msvcrt.printf>	printf
0040133C	.~ EB 0C	JMP SHORT 1_1.0040134A	
0040133E	> C70424 40304000	MOV DWORD PTR SS:[ESP],1_1.00403040	ASCII "Better luck next time! You are unsuccessful."
00401345	. E8 66050000	CALL <JMP.&msvcrt.printf>	printf
0040134A	> E8 D1040000	CALL <JMP.&msvcrt._getch>	_getch
0040134F	. B8 00000000	MOV EAX,0	
00401354	. C9	LEAVE	
00401355	. C3	RETN	
00401356	90	NOP	
00401357	90	NOP	
00401358	90	NOP	
00401359	90	NOP	
0040135A	90	NOP	
0040135B	90	NOP	
0040135C	90	NOP	
0040135D	90	NOP	
0040135E	90	NOP	
0040135F	90	NOP	
00401360	\$ 55	PUSH EBP	
00401361	. B9 50314000	MOV ECX,1_1.00403150	
00401362	. C3	RETN	
00401363	00403018=1_1.00403018	(ASCII "Congratulation! You are successful.")	

00401316 ASCII "%d"

0040131D scanf

Hai dòng trên gọi hàm scanf yêu cầu người dùng nhập key vào

00401322 CALL 1_1.00401290: đi tới dòng lệnh có địa chỉ 00401290

0040128B	90	NOP	
0040128C	90	NOP	
0040128D	90	NOP	
0040128E	90	NOP	
0040128F	90	NOP	
00401290	\$ 55	PUSH EBP	
00401291	. 89E5	MOV EBP,ESP	
00401293	. 83EC 04	SUB ESP,4	
00401296	. C745 FC C80000	MOV DWORD PTR SS:[EBP-4],0C8	
0040129D	. 8B55 FC	MOV EDX,DWORD PTR SS:[EBP-4]	
004012A0	. 8900	MOV EAX,EDX	
004012A2	. C1E0 02	SHL EAX,2	
004012A5	. 01D0	ADD EAX,EDX	
004012A7	. 8945 FC	MOV DWORD PTR SS:[EBP-4],EAX	
004012AA	. 8D45 FC	LEA EAX,DWORD PTR SS:[EBP-4]	
004012AD	. 8330 64	XOR DWORD PTR DS:[EAX],64	
004012B0	. 8D45 FC	LEA EAX,DWORD PTR SS:[EBP-4]	
004012B3	. F710	NOT DWORD PTR DS:[EAX]	
004012B5	. A1 10404000	MOV EAX,DWORD PTR DS:[404010]	
004012BA	. 3B45 FC	CMP EAX,DWORD PTR SS:[EBP-4]	
004012BD	. 75 0C	JNZ SHORT 1_1.004012CB	
004012BF	. C705 10404000	MOV DWORD PTR DS:[404010],1	
004012C9	. EB 0A	JMP SHORT 1_1.004012D5	
004012CB	> C705 10404000	MOV DWORD PTR DS:[404010],0	
004012D5	> C9	LEAVE	
004012D6	. C3	RETN	
004012D7	90	NOP	
004012D8	\$ 55	PUSH EBP	
004012D9	. 89E5	MOV EBP,ESP	
004012DB	. 83EC 18	SUB ESP,18	
004012DE	. 83E4 F0	AND ESP,FFFFFFF0	

Ta đi tới dòng lệnh tương ứng địa chỉ đó
00401296 MOV DWORD PTR SS:[EBP-4].0C8: lưu giá trị 0C8 vào địa chỉ EBP-4

0040129D MOV EDX.DWORD PTR SS:[EBP-4]

004012A0 MOV EAX.EDX

Hai dòng trên có nghĩa lưu giá trị của EBP-4 vào thanh ghi EDX rồi EAX = EDX = 0C8

004012A2 SHL EAX,2: dịch trái EAX 2 lần

004012A5 ADD EAX,EDX: EAX = EAX + EDX = 3E8

004012A7 MOV DWORD PTR[EBP-4], EAX: lưu EAX vào EBP-4

004012A2 LEA EAX, DWORD PTR[EBP-4]: gán EAX vào EBP-4 (EBP = 0023FF08) -> EAX = 0023FF04

004012AD XOR DWORD PTR[EAX], 64: phép XOR EAX với 64 -> 38C

004012B3 NOT DWORD PTR[EAX]: phép NOT với EAX -> FFFFFC73, đổi ra decimal ta được kết quả là -909

004012B5 MOV EAX, DWORD PTR[404010]: gán EAX bằng giá trị vùng nhớ có địa chỉ 404010 -> EAX = 4D2

004012BA CMP EAX, DWORD PTR[EBP-4]

004012BD JNZ SHORT 1_1.004012CB

004012BF MOV DWORD PTR[404010], 1

004512C9 JMP SHORT 1_1.004012D5

004012CB MOV DWORD PTR[404010], 0

004012D5 LEAVE

004012D6

So sánh EAX với EBP-4(= -909). Nếu bằng thì gán giá trị ở vùng nhớ 404010 bằng 1, ngược lại gán bằng 0. Sau đó quay về dòng lệnh 00401327 (nếu bằng 1 thì in ra thông báo successful, ngược lại bằng 0 thì là unsuccessful). Như vậy key cần tìm ở đây là -909

E:\DoAn3\DoAn3\De01\1.1.exe

Please enter a key: -909

Congratulation! You are successful.

1.3

Address	Disassembly	Text string
00416F71	ASCII "TObject"	
00416F79	ASCII "String"	
00416FA8	DD 1_3.00417016	ASCII 0A,"THKStreams"
00417017	ASCII "THKStreams"	
0041702A	ASCII "THKStreams"	
0041703F	ASCII "HKStreamCol"	
00417067	ASCII "Compressed"	
0041708C	ASCII "Encrypted"	
004170B0	ASCII "Key"	
004170CE	ASCII "OnAskForKey"	
004170F4	ASCII "OnCorrupt"	
00417226	MOV ECX,1_3.00417248	ASCII "File is corrupt."
00417248	ASCII "File is corrupt."	
00417258	ASCII 0	
00417C98	MOV ECX,1_3.00417EB8	ASCII "Compressed file is corrupt"
00417EB8	ASCII "Compressed file "	
00417EC8	ASCII "is corrupt",0	
00418958	ASCII "\",0	
00418CDE	MOV EAX,1_3.00418D90	ASCII "TMP"
00418CFA	MOV EAX,1_3.00418D9C	ASCII "TEMP"
00418D20	MOV EAX,1_3.00418DAC	ASCII "USERPROFILE"
00418D90	ASCII "TMP",0	
00418D9C	ASCII "TEMP",0	
00418DAC	ASCII "USERPROFILE",0	
004190E0	PUSH EBP	(Initial CPU selection)
004191E8	MOV EAX,1_3.00419734	ASCII "MYFILES"
0041922B	MOV EDX,1_3.00419744	ASCII "Quick Batch File Compiler"
004192DC	MOV EDX,1_3.00419768	ASCII "BAT"
004192F1	MOV EDX,1_3.00419774	ASCII "FILES"
00419417	PUSH 1_3.00419790	ASCII "bt"
00419470	PUSH 1_3.0041979C	ASCII ".bat"
00419484	MOV ECX,1_3.004197AC	ASCII "@shift 1"
00419517	MOV ECX,1_3.004197D0	ASCII "^&"
00419571	PUSH 1_3.004197E8	ASCII "cmd.exe /c "
00419599	PUSH 1_3.004197FC	ASCII "command.com /c "
00419734	ASCII "MYFILES",0	
00419744	ASCII "Quick Batch File"	
00419754	ASCII " Compiler",0	
00419768	ASCII "BAT",0	

Khi mở chương trình lên, tìm trong chương trình ta không thấy đoạn string khi mở chương trình lên để nhập password -> vùng nhớ không thể truy xuất khi chương trình chưa chạy

OllyDbg - 1.5.exe - [CPU - main thread, module _1_>]

File View Debug Plugins Options Window Help

L E M T W H C / E B R . S ?

```

00419460 . E8 BF9A0EFF CALL 1_3.004102F24
00419465 . 8D55 C0 LEA EDX,DWORD PTR SS:[EBP-40]
00419468 . E8 CBDFFEFF CALL 1_3.004107438
0041946D . FF75 C0 PUSH DWORD PTR SS:[EBP-40]
00419470 . 68 9C974100 PUSH 1_3.0041979C
00419475 . 8B DCE84100 MOV EAX,1_3.0041E8DC
00419478 . BA 00000000 MOV EDX,6
0041947F . E8 38B1FEFF CALL 1_3.0041045BC
00419484 . B9 AC974100 MOV ECX,1_3.004197AC
00419489 . 33D2 XOR EDX,EDX
0041948B . A1 70E84100 MOV EAX,DWORD PTR DS:[41E870]
00419490 . 8B18 MOV EBX,DWORD PTR DS:[EAX]
00419492 . FF53 60 CALL DWORD PTR DS:[EBX+60]
00419495 . 8D45 BC LEA EAX,DWORD PTR SS:[EBP-44]
00419498 . 8B0D DCE84100 MOV ECX,DWORD PTR DS:[41E8DC]
0041949L . 8B15 D4E84100 MOV EDX,DWORD PTR DS:[41E8D4]
004194A4 . E8 9FB0FEFF CALL 1_3.004104548
004194A9 . 8B55 BC MOV EDX,DWORD PTR SS:[EBP-44]
004194AC . A1 70E84100 MOV EAX,DWORD PTR DS:[41E870]
004194B1 . 8B08 MOV ECX,DWORD PTR DS:[EAX]
004194B3 . FF51 74 CALL DWORD PTR DS:[ECX+74]
004194B6 . 8D45 B8 LEA EAX,DWORD PTR SS:[EBP-48]
004194B9 . 8B0D DCE84100 MOV ECX,DWORD PTR DS:[41E8DC]
004194BE . 8B15 D4E84100 MOV EDX,DWORD PTR DS:[41E8D4]
004194C5 . E8 7EB0FEFF CALL 1_3.004104548
004194C8 . 8B45 B8 MOV EAX,DWORD PTR SS:[EBP-48]
004194CD . BA 02000000 MOV EDX,2
004194D2 . E8 E1E3FEFF CALL 1_3.0041078B8
004194D7 . 8D85 B4FFFFF LEA EAX,DWORD PTR SS:[EBP-14C]
004194D0 . 8B15 9CB854100 MOV EDX,DWORD PTR DS:[41B59C]
004194E3 . 8B12 MOV EDX,DWORD PTR DS:[EDX]

```

Registers (FPU)

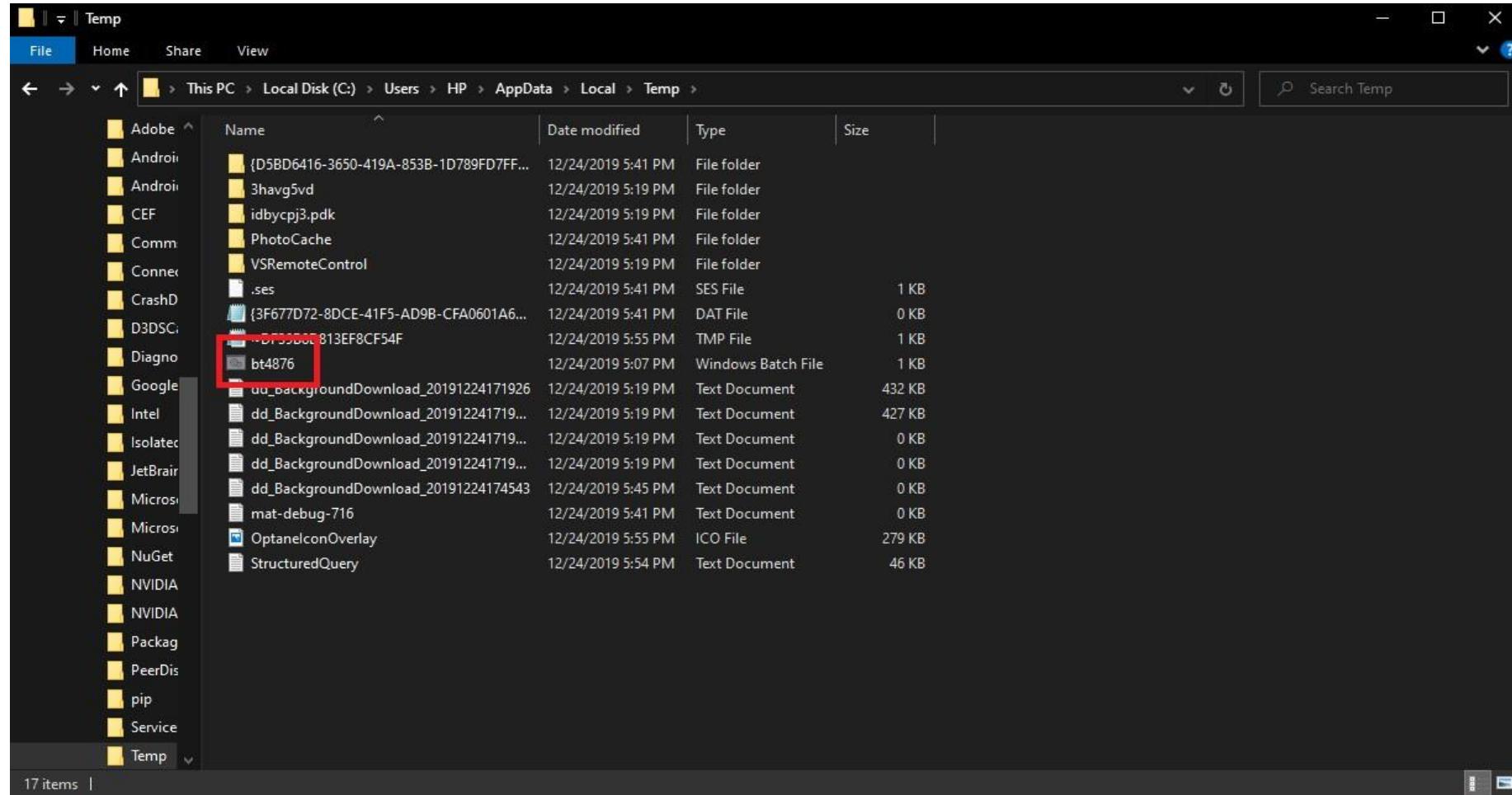
^

rax	00000000
rcx	00000000
rdx	021B1470 ASCII "C:\Users\HP\AppData\Local\Temp\bt5378.bat"
rbx	00410AC4 1_3.00410AC4
rsp	0019FD8
rbp	0019FF70
rsi	004190E0 1_3.<ModuleEntryPoint>
rdi	004190E0 1_3.<ModuleEntryPoint>
rip	004194AC 1_3.004194AC
c0	es 002B 32bit 0(FFFFFFFF)
p1	cs 0023 32bit 0(FFFFFFFF)
a1	ss 002B 32bit 0(FFFFFFFF)
z0	ds 002B 32bit 0(FFFFFFFF)
s0	fs 0053 32bit 378000(FFF)
t0	gs 002B 32bit 0(FFFFFFFF)
d0	0 0 LastErr ERROR_SUCCESS (00000000)
e0	EFL 00000216 (NO,NB,NE,A,NS,PE,GE,G)
st0	empty 0.0
st1	empty 0.0
st2	empty 0.0
st3	empty 0.0
st4	empty 0.0
st5	empty 0.0
st6	empty 0.0
st7	empty 0.0

FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)
FCW 1372 Prec NEAR,64 Mask 1 1 0 0 1 0

DS:10041E870=021B0BE8
FAX=00000000

Ta tiến hành debug và thấy được một đường dẫn xuất hiện ở 5 dòng sau “C:\HP\AppData\Local\Temp\bt5378.bat”



Ta tiến hành mở đường dẫn và có một file bt4876.bat như trong chương trình

C:\WINDOWS\system32\cmd.exe
ts the first time i give someone try 2 crack this kind of CM.
good luck! - N3tRAt aka V[i]RuS
Enter Password:

Ta tiến hành mở file lên và thấy xuất hiện những dòng như giống như chương trình chính -> ta có thể đoán được file .bat này hoạt động tương tự như chương trình chính nên ta tiến hành edit file .bat này để có thể thấy được password của nó

bt4876 - Notepad

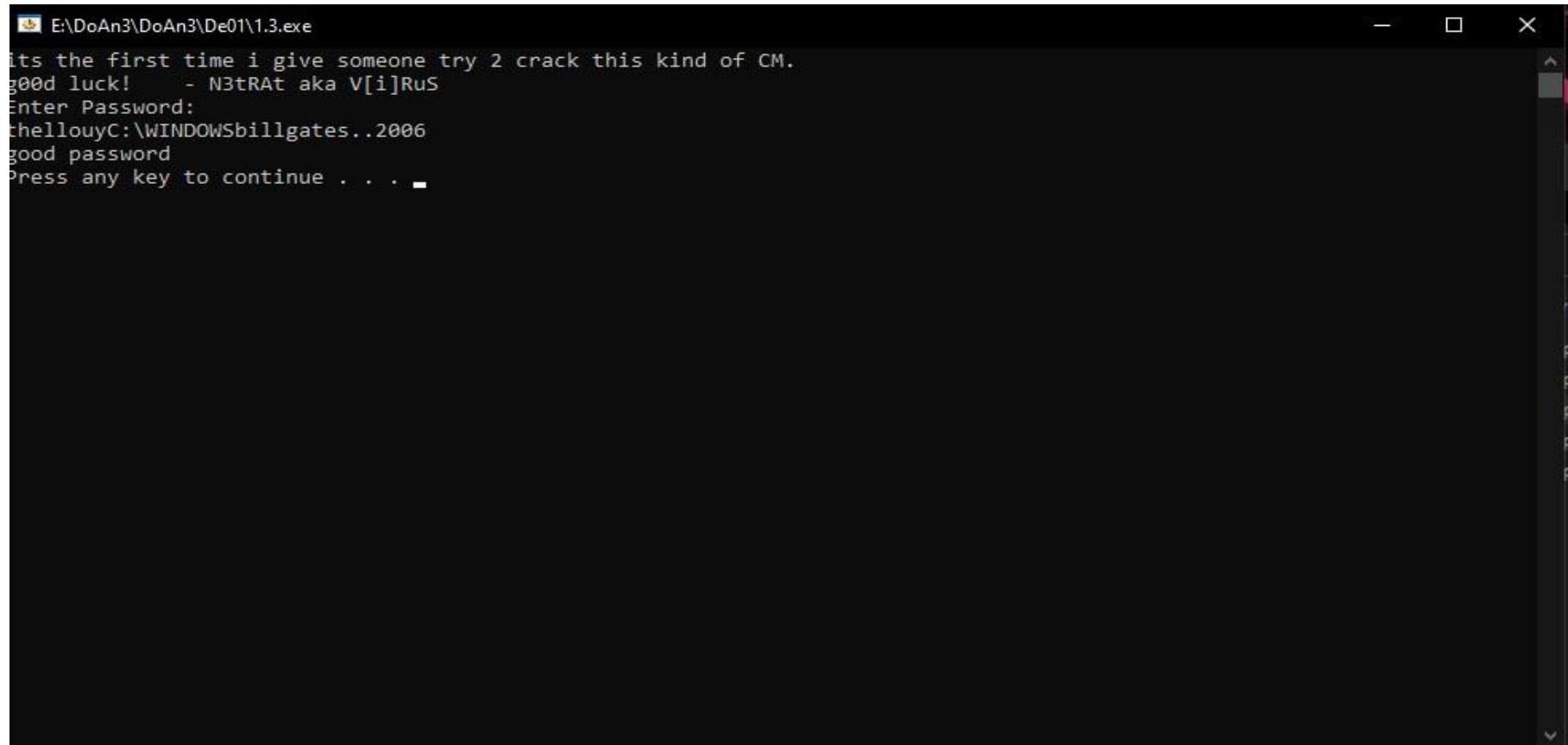
File Edit Format View Help

```
@shift 1
ECHO OFF
cls
REM title crackme - Batch or not?
set r=o
set o=t
set llo=he
set t=y
set h=u
set j=w
set he=llo
echo its the first time i give someone try 2 crack this kind of CM.
echo g00d luck!      - N3tRAt aka V[i]RuS

echo Enter Password:
set /p password=
if "%password%"=="%o%%llo%%he%%h%%t%%windir%billgates..2006" goto good
if not "%password%"=="%o%%llo%%he%%h%%t%%windir%billgates..2006" goto bad
:good
echo good password
pause
exit
:bad
echo bad password
```

Ln 1, Col 1 | 100% | Windows (CRLF) | UTF-8

Sau khi ta edit file này và có được password của chương trình là thellouyC:\WINDOWSbillgates..2006



E:\DoAn3\DoAn3\De01\1.3.exe

its the first time i give someone try 2 crack this kind of CM.
g00d luck! - N3tRAt aka V[i]RuS

Enter Password:

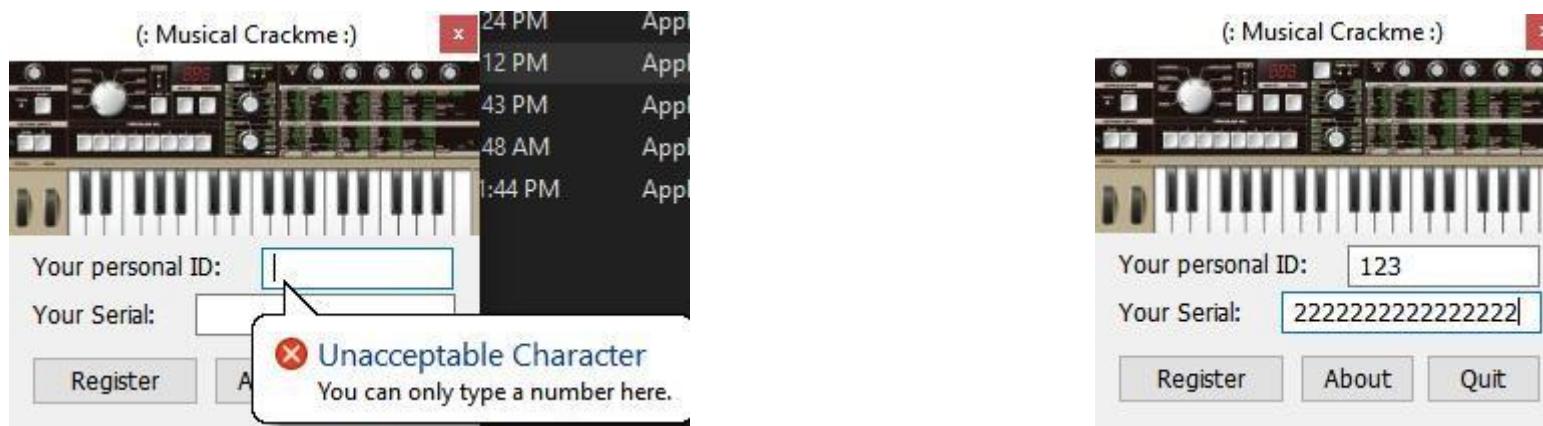
thellouyC:\WINDOWSbillgates..2006

good password

Press any key to continue . . .

Ta thử lại chương trình với password trên và kết quả là thành công

1.2



Đầu tiên mở chương trình lên ta nhập thử số vào ID thì thấy báo lỗi -> ID chỉ có thể nhập số

Tiếp đó đến nhập serial ta thấy chỉ có thể nhập tối đa là 16 chữ số -> không nhập gì cũng được

The image shows a screenshot of the OllyDbg debugger. The menu bar includes File, View, Debug, Plugins, Options, Window, and Help. The assembly pane shows the following assembly code:

Address	Disassembly	Text string
00401000	PUSH 0	(Initial CPU selection)
004010EE	PUSH 1_2.00405063	ASCII "About"
004010F9	PUSH 1_2.00405000	ASCII "Musical Crackme" Rules: - No debugging - No patching - Make a keygen wt0vrenr@gmail.com"

Mở ollydbg lên vào search tìm string thì ta chỉ thấy có chuỗi về about

OllyDbg - 1.2.exe - [Found intermodular calls]

File View Debug Plugins Options Window Help

Address	Disassembly	Destination
00401000	PUSH 0	(Initial CPU selection)
00401002	CALL <JMP.&kernel32.GetModuleHandleA>	KERNEL32.GetModuleHandleA
0040100C	CALL <JMP.&comctl32.InitCommonControls>	comctl32.InitCommonControls
00401022	CALL <JMP.&user32.DialogBoxParamA>	user32.DialogBoxParamA
00401029	CALL <JMP.&kernel32.ExitProcess>	KERNEL32.ExitProcess
0040103E	CALL <JMP.&kernel32.FindResourceA>	KERNEL32.FindResourceA
0040104B	CALL <JMP.&kernel32.SizeofResource>	KERNEL32.SizeofResource
0040105D	CALL <JMP.&kernel32.LoadResource>	KERNEL32.LoadResource
00401063	CALL <JMP.&kernel32.LockResource>	KERNEL32.LockResource
00401075	CALL <JMP.&kernel32.GlobalAlloc>	KERNEL32.GlobalAlloc
004010CD	CALL <JMP.&user32.SendDlgItemMessageA>	user32.SendDlgItemMessageA
004010FB	CALL <JMP.&user32.MessageBoxA>	user32.MessageBoxA
00401120	CALL <JMP.&user32.GetDlgItemInt>	user32.GetDlgItemInt
00401142	CALL <JMP.&user32.GetDlgItemInt>	user32.GetDlgItemInt
00401166	CALL <JMP.&user32.GetDlgItem>	user32.GetDlgItem
0040116E	CALL <JMP.&user32.EnableWindow>	user32.EnableWindow
0040117B	CALL <JMP.&user32.GetDlgItem>	user32.GetDlgItem
00401183	CALL <JMP.&user32.EnableWindow>	user32.EnableWindow
00401190	CALL <JMP.&user32.GetDlgItem>	user32.GetDlgItem
00401198	CALL <JMP.&user32.EnableWindow>	user32.EnableWindow
004011BD	CALL <JMP.&user32.EndDialog>	user32.EndDialog
00401241	CALL <JMP.&winmm.waveOutRestart>	winmm.waveOutRestart
00401246	CALL <JMP.&kernel32.ResumeThread>	KERNEL32.ResumeThread
0040124D	CALL <JMP.&kernel32.SuspendThread>	KERNEL32.SuspendThread
00401258	CALL <JMP.&winmm.waveOutPause>	winmm.waveOutPause
004012C5	CALL <JMP.&winmm.waveOutReset>	winmm.waveOutReset
004012D0	CALL <JMP.&winmm.waveOutClose>	winmm.waveOutClose

Sau đó ta vào search -> all intermodular calls thì phát hiện thấy có 2 dòng màu đỏ như trong hình là 2 dòng cho phép nhập ID và serial

0040111F	. 53	PUSH EBX
00401120	. 50	PUSH EAX
00401121	. 6A 01	PUSH 1
00401123	. 6A 00	PUSH 0
00401125	. 68 EC030000	PUSH 3EC
0040112A	. FF75 08	PUSH DWORD PTR SS:[EBP+8]
0040112D	. E8 D8000000	CALL <JMP.&user32.GetDlgItemInt>
00401132	. 8BD8	MOV EBX,EAX
00401134	. 33C0	XOR EAX,EAX
00401136	. 6A 01	PUSH 1
00401138	. 6A 00	PUSH 0
0040113A	. 68 ED030000	PUSH 3ED
0040113F	. FF75 08	PUSH DWORD PTR SS:[EBP+8]
00401142	. E8 C3000000	CALL <JMP.&user32.GetDlgItemInt>
00401147	. 8BC8	MOV ECX,EAX
00401149	. E8 40FFFFFF	CALL 1_2.0040109B
0040114E	. 3BC9	CMP EAX,EBX
00401150	. 74 0C	JE SHORT 1_2.0040115E
00401152	. BB 00000000	MOV EBX,0
00401157	. BA 00000000	MOV EDX,0

Đi đến dòng đó và ta phát hiện sau khi nhập ID và serial xong ở dòng 00401149 Call 1_2.0040109B chương trình sẽ nhảy tới dòng 0040109B

* OllyDbg - 1.2.exe - [CPU - main thread, module 1_2]

File View Debug Plugins Options Window Help

Registers (FPU)

EAX	0019FFCC
ECX	00401000 1_2.<ModuleEntryPoint>
EDX	00401000 1_2.<ModuleEntryPoint>
EBX	00401000
ESP	0019FF74
EBP	0019FF80
ESI	00401000 1_2.<ModuleEntryPoint>
EDI	00401000 1_2.<ModuleEntryPoint>
EIP	00401000 1_2.<ModuleEntryPoint>
C	0 ES 002B 32bit 0(FFFFFFFF)
P	1 CS 0023 32bit 0(FFFFFFFF)
A	0 SS 002B 32bit 0(FFFFFFFF)
Z	1 DS 002B 32bit 0(FFFFFFFF)
S	0 FS 0053 32bit 3A4000(FFF)
T	0 GS 002B 32bit 0(FFFFFFFF)
D	0 LastErr ERROR_SUCCESS (00000000)
EFL	00000246 (NO,NB,E,BE,NS,PE,GE,LE)

IPParam = 0
wParam = 4
Message = EM_LIMITTEXT
ControlID = 3EC (1004.)
hWnd = SendDlgItemMessage@

FST 0000 Cond 0 0 0 Err 0 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1

Address Hex dump ASCII

00405000	4D 75 73 69 63 61 6C 20	Musical
00405008	43 72 61 63 6B 6D 65 00	Crackme.
00405010	00 0D 00 52 75 6C 65 73	...Rules
00405018	3A 0D 00 20 2D 20 4E 6F	... - No
00405020	20 64 65 62 69 67 67 69	debuggi
00405028	6E 67 0D 0A 20 2D 20 4E	ng.. N
00405030	6F 20 70 61 74 63 68 69	o patchi
00405038	6E 67 0D 00 2D 20 2D 4D	ng.. - M
00405040	61 6B 65 20 61 20 6B 65	ake a ke
00405048	79 67 65 6E 00 0A 0D 0A	ygen....
00405050	77 74 30 76 72 65 6D 72	w0vremr
00405058	40 67 6D 61 69 6C 2E 63	@gmail.c
00405060	6F 6D 00 41 62 6F 75 74	om.About
00405068	00 00 00 00 00 00 80 3FC?
00405070	00 00 7A 44 6F 12 83 3A	zDotâ:

^ 0019FF74 767CF989 RETURN to KERNEL32.767CF989

0019FF78 003A1000
0019FF7C 767CF970 KERNEL32.BaseThreadInitThunk
0019FF80 0019FFDC
0019FF84 7715DE4 RETURN to ntdll.7715DE4
0019FF88 003A1000
0019FF8C 1553C457
0019FF90 00000000
0019FF94 00000000
0019FF98 003A1000
0019FF9C 00000000
0019FFA0 00000000
0019FFA4 00000000
0019FFB8 00000000
0019FAC 00000000
0019FB0 00000000
0019FCD 00000000

Program entry point

Paused

11:54 AM ENG 12/27/2019

Đi đến địa chỉ đó và ta thấy được những dòng màu đỏ trong hình là phát sinh ra serial từ ID ta đã nhập

UillyDbg - I_2.exe - [CPU - main thread, module I_2]

File View Debug Plugins Options Window Help

The screenshot shows the UillyDbg debugger interface. The assembly code window displays the following instructions:

Address	Instruction	Description
0040109B	\$ 83C3 4C	ADD EBX, 4C
0040109E	. 83C2 03	ADD EDX, 3
004010A1	. 43	INC EBX
004010A2	. 81C3 8B030000	ADD EBX, 38B
004010A8	. 03DB	ADD EBX, EBX
004010AA	. 0FAFDA	IMUL EBX, EDX
004010AD	. 4B	DEC EBX
004010AE	C3	RETN
004010AF	. 55	PUSH EBP
004010B0	. 8BEC	MOV EBP, ESP
004010B2	. 8B45 0C	MOV EAX, DWORD PTR SS:[EBP+C]
004010B5	. 3D 10010000	CMP EAX, 110

The registers window shows the following values:

Register	Value
EAX	22ED614F
ECX	22ED614F
EDX	0019F785
EBX	22ED614F
ESP	0019F848
EBP	0019F858
ESI	001C03FA
EDI	00000111
EIP	004010AE 1_2.004010AE
C	1 FS 002R 32bit @{FFFFFF}

Ta thử nhập ID là 1712 và debug những dòng trên để tìm serial và ta có được kết quả EBX là 22ED614F đổi ra hệ 10 là 585982287

ADD EBX, 4C -> EBX = EBX + 76

ADD EDX, 3 -> EDX = EDX + 3

INC EBX -> EBX++

ADD EBX, 38B -> EBX = EBX + 907

ADD EBX, EBX -> EBX = EBX + EBX

IMUL EBX, EDX -> EBX = EBX * EDX

DEC EBX -> EBX--

Tóm lại ta có công thức tổng quát cho serial như sau: Serial = 3 * (2 * ID + 1968) - 1

OllyDbg - 1.2.exe - [CPU - main thread, module 1_2]

File View Debug Plugins Options Window Help

Address	Hex dump	ASCII
00401098	4D 75 73 69 63 61 6C 20	Musical
0040109E	00 03	ADD EDX, 3
004010A1	. 43	INC EBX
004010A2	. 81C9 8B030000	ADD EBX, 38B
004010A8	. 03DB	ADD EBX, EBX
004010A9	. 0FAFDA	IMUL EBX, EDX
004010AD	. 4B	DEC EBX
004010AL	. C3	RETN
004010AF	. 55	PUSH EBP
004010B0	. 8BEC	MOV EBP, ESP
004010B2	. 8B45 0C	MOV EAX,DWORD PTR SS:[EBP+C]
004010B5	. 3D 10010000	CMP EAX,110
004010B8	. 75 1B	JNZ SHORT 1_2.004010D7
004010BC	. 60 00	PUSH 0
004010BE	. 60 04	PUSH 4
004010C0	. 68 C5000000	PUSH 0C5
004010C5	. 68 EC030000	PUSH 3EC
004010CA	. FF75 08	PUSH DWORD PTR SS:[EBP+8]
004010CD	. E8 44010000	CALL <JMP.&user32.SendMessageA>
004010D2	. E9 EB000000	JMP 1_2.004011C2
004010D7	> 3D 11010000	CMP EAX,111
004010DC	. 0F85 D1000000	JNZ 1_2.004011B3
004010E2	. 8B45 10	MOV EAX,DWORD PTR SS:[EBP+10]
004010E5	. 3D EA030000	CMP EAX,3EA
004010EA	. 75 19	JNZ SHORT 1_2.00401105
004010EC	. 60 00	PUSH 0
004010EE	. 68 63504000	PUSH 1_2.00405063
004010F3	. 68 00504000	PUSH 1_2.00405000
004010F8	. FF75 08	PUSH DWORD PTR SS:[EBP+8]
004010FB	. E8 10010000	CALL <JMP.&user32.MessageBoxA>
00401100	. E9 BD000000	JMP 1_2.004011C2

lParam = 0
wParam = 4
Message = EM_LIMITTEXT
ControlID = 3EC (1004.)
hWnd

SendDlgItem (: Musical Crackme :)

Style = M Your personal ID: 1712
Title = " Your Serial: 585982287
Text = " Register About Quit
es: M - N

MessageBoxA

Registers (FPU)

EAX	00000000
ECX	00000000
EDX	00000000
EBX	0072B7F0
ESP	0019F528
EBP	0019F598
ESI	00000000
EDI	00000388

EIP 77120EFC ntdll.77120EFC

C 0	ES 002B 32bit 0(FFFFFFFF)
P 1	CS 0023 32bit 0(FFFFFFFF)
A 0	SS 002B 32bit 0(FFFFFFFF)
Z 0	DS 002B 32bit 0(FFFFFFFF)
S 0	FS 0053 32bit 270000(FFF)
T 0	GS 002B 32bit 0(FFFFFFFF)
D 0	
O 0	LastErr ERROR_SUCCESS (00000000)
EFL 00000206	(NO,NB,NE,A,NS,PE,GE,G)
ST0	empty 0.0
ST1	empty 0.0
ST2	empty 0.0
ST3	empty 0.0
ST4	empty 1.0000000000000000000000000000000
ST5	empty 0.5000000000000000000000000000000
ST6	empty 16.0000000000000000000000000000000
ST7	empty 16.0000000000000000000000000000000

FST 4020 Cond 1 0 0 0 Err 0 0 1 0 0 0 0 0
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1 1 1

Sau đó ta thử lại với ID và Serial ở trên thì thấy chương trình bị mờ và có tiếng nhạc phát lên -> ta đã nhập đúng ID và Serial

1.5

The screenshot shows the OllyDbg debugger interface with the 'Disassembly' tab selected. The 'Address' column lists memory addresses, and the 'Destination' column lists the API functions being called. A specific address, 004014A0, is highlighted in red and has a yellow arrow pointing to it from the left margin. The destination for this call is 'USER32.GetDlgItemTextA'. Other visible calls include USER32.SendMessageA, USER32.CreateWindowExA, and various USER32 and GDI32 functions like GetDlgItem, SetTextColor, and CreateBrushIndirect.

Address	Disassembly	Destination
0040115E	CALL <JMP.&user32.GetItem>	USER32.GetItem
00401193	CALL <JMP.&user32.SendDlgItemMessageA>	USER32.SendDlgItemMessageA
004011B0	CALL <JMP.&user32.SendDlgItemMessageA>	USER32.SendDlgItemMessageA
004011BF	CALL <JMP.&comctl32.InitCommonControls>	comctl32.InitCommonControls
004011EF	CALL <JMP.&user32.CreateWindowExA>	USER32.CreateWindowExA
0040121B	CALL <JMP.&user32.GetWindowRect>	USER32.GetWindowRect
0040122C	CALL <JMP.&user32.EnumChildWindows>	USER32.EnumChildWindows
00401240	CALL <JMP.&user32.SendDlgItemMessageA>	USER32.SendDlgItemMessageA
00401260	CALL <JMP.&user32.SendDlgItemMessageA>	USER32.SendDlgItemMessageA
00401287	CALL <JMP.&user32.CreateDialogParamA>	USER32.CreateDialogParamA
004012BD	CALL <JMP.&user32.SendMessageA>	USER32.SendMessageA
004012BA	CALL <JMP.&user32.GetDlgItem>	USER32.GetDlgItem
004012CC	CALL <JMP.&user32.GetDlgItem>	USER32.GetDlgItem
004012DE	CALL <JMP.&user32.EnableWindow>	USER32.EnableWindow
004012F4	CALL <JMP.&user32.SendDlgItemMessageA>	USER32.SendDlgItemMessageA
00401320	CALL <JMP.&gdi32.CreateBrushIndirect>	gdi32.CreateBrushIndirect
00401332	CALL <JMP.&user32.GetClientRect>	USER32.GetClientRect
00401341	CALL <JMP.&user32.FillRect>	USER32.FillRect
00401360	CALL <JMP.&user32.GetDlgCtrlID>	USER32.GetDlgCtrlID
0040137C	CALL <JMP.&gdi32.SetTextColor>	gdi32.SetTextColor
00401384	CALL <JMP.&user32.GetDlgCtrlID>	USER32.GetDlgCtrlID
00401390	CALL <JMP.&gdi32.SetTextColor>	gdi32.SetTextColor
004013B7	CALL <JMP.&gdi32.SetBkColor>	gdi32.SetBkColor
004013BE	CALL <JMP.&user32.GetStockObject>	gdi32.GetStockObject
004013EF	CALL <JMP.&kernel32.GetModuleHandleA>	KERNEL32.GetModuleHandleA
0040140E	CALL <JMP.&user32.GetStockObject>	USER32.DialogBoxParamA
00401400	CALL <JMP.&user32.GetDlgItemTextA>	USER32.GetDlgItemTextA
004014E9	CALL <JMP.&user32.MessageBoxA>	USER32.MessageBoxA
004014F6	CALL <JMP.&user32.EnableWindow>	USER32.EnableWindow
00401556	CALL <JMP.&user32.EnableWindow>	USER32.EnableWindow
00401563	CALL <JMP.&user32.EnableWindow>	USER32.EnableWindow
00401579	CALL <JMP.&user32.SendMessageA>	USER32.SendMessageA
00401594	CALL <JMP.&user32.SendDlgItemMessageA>	USER32.SendDlgItemMessageA
004015B8	CALL <JMP.&user32.EndDialog>	USER32.EndDialog
004015D7	CALL <JMP.&user32.SetTimer>	USER32.SetTimer
00401630	CALL <JMP.&user32.SetTimer>	USER32.SetTimer
00401651	CALL <JMP.&user32.SendDlgItemMessageA>	USER32.SendDlgItemMessageA
00401660	CALL <JMP.&user32.SendDlgItemMessageA>	USER32.SendDlgItemMessageA
00401689	CALL <JMP.&user32.SendDlgItemMessageA>	USER32.SendDlgItemMessageA
004016B5	CALL <JMP.&user32.SendDlgItemMessageA>	USER32.SendDlgItemMessageA
004016C1	CALL <JMP.&user32.SendDlgItemMessageA>	USER32.SendDlgItemMessageA
004016D0	CALL <JMP.&user32.SendDlgItemMessageA>	USER32.SendDlgItemMessageA
004016F9	CALL <JMP.&user32.SendDlgItemMessageA>	USER32.SendDlgItemMessageA
00401715	CALL <JMP.&user32.SendDlgItemMessageA>	USER32.SendDlgItemMessageA
00401731	CALL <JMP.&user32.SendDlgItemMessageA>	USER32.SendDlgItemMessageA
0040174A	CALL <JMP.&user32.SendDlgItemMessageA>	USER32.SendDlgItemMessageA
00401766	CALL <JMP.&user32.SendDlgItemMessageA>	USER32.SendDlgItemMessageA
0040177F	CALL <JMP.&user32.SendDlgItemMessageA>	USER32.SendDlgItemMessageA
0040179B	CALL <JMP.&user32.SendDlgItemMessageA>	USER32.SendDlgItemMessageA

Đầu tiên mở chương trình lên vào search for -> all intermodular calls

Tại địa chỉ 4014A0 (ô màu đỏ như trong hình) là nơi để ta lấy key của chương trình, ta nhấn vào đó để đến địa chỉ đó.

CMP EAX, 1 trên địa chỉ 004014A5 sẽ kiểm tra nếu có bất kỳ thứ gì đã được nhập vào hộp văn bản. Nếu không có gì được nhập thì sẽ nhận được hộp thông báo của ở địa chỉ 004014DB cho biết "Tên của bạn phải có ít nhất một byte".

OllyDbg - 1.5.exe - [CPU - main thread, module 1_5]

File View Debug Plugins Options Window Help

L E M T W H C / K B R ... S ⌂ ?

```

004014A8 .~ 7D 56 JGE SHORT 1_5.00401500
004014AA .. EB 2F JMP SHORT 1_5.004014DB
004014AC .. EB 25 JMP SHORT 1_5.004014D3
004014AE .~ 59 6F 75 72 20 ASCII "Your name must b"
004014BE .. 65 20 61 74 20 ASCII "e at least one b"
004014CE .~ 79 74 65 21 00 ASCII "yle!" 0
004014D3 > EB 06 JMP SHORT 1_5.004014DB
004014D5 .~ 45 72 72 6F 72 ASCII "Error",0
004014DB > 6A 40 PUSH 40
004014DD .. 68 D5144000 PUSH 1_5.004014D5
004014E2 .. 68 AE144000 PUSH 1_5.004014AE
004014E7 .. 6A 00 PUSH 0
004014E9 .. E8 30080000 CALL <JMP.&user32.MessageBoxA>
004014EE .. 6A 00 PUSH 0
004014F0 .. FF35 60304000 PUSH DWORD PTR DS:[403060]
004014F6 .. E8 D3070000 CALL <JMP.&user32.EnableWindow>
004014FB .. E9 99000000 JMP 1_5.00401599
00401500 > 50 PUSH EAX
00401501 .. E8 55040000 CALL 1_5.0040195B
00401506 .. 01 3B344000 MOV EAX,DWORD PTR DS:[40333D]
0040150B .. 8B1D 41334000 MOV EBX,DWORD PTR DS:[403341]
00401511 .. 03 E4324000 MOV DWORD PTR DS:[4032E1],EBX
00401516 .. 891D E8324000 MOV DWORD PTR DS:[4032E81],EBX
0040151C .. E8 C0040000 CALL 1_5.004019E1
00401521 .. 33C0 XOR EAX,EAX
00401523 .. 33DB XOR EBX,EBX
00401525 .. 66:A1 3B334000 MOV AX,WORD PTR DS:[40333B]
00401528 .. 66:8B5F 08 MOV BX,WORD PTR DS:[EDI+8]
0040152F .. 66:2BC3 SUB AX,BX
00401532 .. 35 3F1B0000 XOR EAX,1B3F
00401537 .. 2D 23010000 SUB EAX,123
0040153C .. EB 03 JMP SHORT 1_5.00401541
0040153E .. 01 DB 01
0040153F .. 44 DB 44

```

Registers (FPU)

EAX	0019FFCC
ECX	00401065 1_5.<ModuleEntryPoint>
EDX	00401065 1_5.<ModuleEntryPoint>
EBX	002C6000
ESP	0019FF74
EBP	0019FF80
ESI	00401065 1_5.<ModuleEntryPoint>
EDI	00401065 1_5.<ModuleEntryPoint>
EIP	00401065 1_5.<ModuleEntryPoint>
C 0	ES 002B 32bit 0(FFFFFF)
P 1	CS 0023 32bit 0(FFFFFF)
A 0	SS 002B 32bit 0(FFFFFF)
Z 1	DS 002B 32bit 0(FFFFFF)
S 0	FS 0053 32bit 2C9000(FFF)
T 0	GS 002B 32bit 0(FFFFFF)
D 0	0 0 LastErr ERROR_MOD_NOT_FOUND (0000007E)
EFL	00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0	empty 0.0
ST1	empty 0.0
ST2	empty 0.0
ST3	empty 0.0
ST4	empty 0.0
ST5	empty 0.0
ST6	empty 0.0
ST7	empty 0.0
FST	0000 Cond 0 0 0 Err 0 0 0 0 0 0 (GT)
FCW	027F Prec NEAR,53 Mask 1 1 1 1 1 1

CHAR 'D'

Address Hex dump ASCII

00403000	00 00 00 00 00 00 00 00 00 00 00
00403008	00 00 00 00 00 00 00 00 00 00 00
00403010	00 00 00 00 00 00 00 00 00 00 00
00403018	00 00 00 00 00 00 00 00 00 00 00
00403020	00 00 00 00 00 00 00 00 00 00 00
00403028	00 00 00 00 00 00 00 00 00 00 00
00403030	00 00 00 00 00 00 00 00 00 00 00
00403038	00 00 00 00 00 00 00 00 00 00 00
00403040	00 00 00 00 00 00 00 00 00 00 00
00403048	00 00 00 00 00 00 00 00 00 00 00
00403050	00 00 00 00 00 00 00 00 00 00 00
00403058	00 00 00 00 00 00 00 00 00 00 00
00403060	00 00 00 00 00 00 00 00 00 00 00
00403068	54 6F 6F 6C 74 69 70 73	Tooltips

Program entry point

Windows Taskbar: File Explorer, Internet Explorer, File, Start, Task View, Taskbar Buttons, Taskbar Icons.

Paused

5:58 PM ENG 12/30/2019

Tiếp đó nhấn f8 chương trình sẽ đi tới địa chỉ 00401501 (dòng màu đỏ đầu tiên trong hình), bắt đầu giai đoạn đoạn để lấy key

File View Debug Plugins Options Window Help

L E M T W H C / K B R S ?

```

00401951 . C9 LEAVE
00401952 . C2 1000 RETN 10
00401953 . 33C0 XOR EAX,EAX
00401954 . C9 LEAVE
00401955 . C2 1000 RETN 10
00401956 . 55 PUSH EBP
00401957 . 8BEC MOV EBP,ESP
00401958 . BE 1C334000 MOV ESI,1_5.0040331C
00401959 . BF 3B334000 MOV EDI,1_5.0040333B
00401960 . B9 10000000 MOV ECX,10
00401961 > 0FB606 MOVZX EAX,BYTE PTR DS:[ESI]
00401970 . 51 PUSH ECX
00401971 . 50 PUSH EAX
00401972 . E8 08000000 CALL 1_5.0040197F
00401973 . 8907 MOV DHWORD PTR DS:[EDI],EAX
00401974 . 47 INC EDI
00401975 . 46 INC ESI
00401976 . E2 F0 LOOP SHORT 1_5.0040196D
00401977 . C9 LEAVE
00401978 . C3 RETN
00401979 . 55 PUSH EBP
00401980 . 8BEC MOV EBP,ESP
00401981 . 83C4 FC ADD ESP,-4
00401982 . 33C0 XOR EAX,EAX
00401983 . BB 56141200 MOV EBX,121456
00401984 . 05 11100001 ADD EAX,1001011
00401985 . C645 FC 2D MOV BYTE PTR SS:[EBP-4],2D
00401986 . 8A50 FC MOV BL,BYTE PTR SS:[EBP-4]
00401987 . 02C3 ADD AL,BL
00401988 . C645 FD 3F MOV BYTE PTR SS:[EBP-31],3F
00401989 . 8A50 FD MOV BL,BYTE PTR SS:[EBP-31]
0040198A . 02C3 ADD AL,BL
0040198B . C645 FE 3F MOV BYTE PTR SS:[EBP-21],3F
0040198C . 8A50 FE MOV BL,BYTE PTR SS:[EBP-21]

```

Registers (FPU)

ERX	0019FFCC
ECX	00401065 1_5.<ModuleEntryPoint>
EDX	00401065 1_5.<ModuleEntryPoint>
EBX	002C6000
ESP	0019FF74
EBP	0019FF80
ESI	00401065 1_5.<ModuleEntryPoint>
EDI	00401065 1_5.<ModuleEntryPoint>
EIP	00401065 1_5.<ModuleEntryPoint>
C 0	ES 002B 32bit 0(FFFFFFFF)
P 1	CS 0023 32bit 0(FFFFFFFF)
A 0	SS 002B 32bit 0(FFFFFFFF)
Z 1	DS 002B 32bit 0(FFFFFFFF)
S 0	FS 0053 32bit 2C9000(FFF)
T 0	GS 002B 32bit 0(FFFFFFFF)
D 0	0 0 LastErr ERROR_MOD_NOT_FOUND (0000007E)
EFL	00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0	empty 0.0
ST1	empty 0.0
ST2	empty 0.0
ST3	empty 0.0
ST4	empty 0.0
ST5	empty 0.0
ST6	empty 0.0
ST7	empty 0.0
FST	0000 Cond 0 0 0 Err 0 0 0 0 0 0 0 (GT)
FCW	027F Prec NEAR,53 Mask 1 1 1 1 1

Address Hex dump ASCII

00403000	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00403001	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00403010	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00403018	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00403020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00403028	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00403030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00403038	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00403040	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00403048	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00403050	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00403058	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00403060	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00403068	54 6F 6F 6C 74 69 70 73	Tooltips

0019FF74 7614F989 RETURN to KERNEL32.7614F989

0019FF78	002C6000
0019FF7C	7614F970 KERNEL32.BaseThreadInitThunk
0019FF80	0019FFDC
0019FF84	77495DE4 RETURN to ntdll.77495DE4
0019FF88	002C6000
0019FF8C	31DAB079
0019FF90	00000000
0019FF94	00000000
0019FF98	002C6000
0019FF9C	00000000
0019FFA0	00000000
0019FFA4	00000000
0019FFA8	00000000
0019FFAC	00000000

Paused

6:03 PM ENG 12/30/2019

Tiếp tục nhấn f7 để di chuyển đến địa chỉ như trong hình

OllyDbg - 1.5.exe - [CPU - main thread, module 1_5]

File View Debug Plugins Options Window Help

L E M T W H C / K B R . S ?

```

0040199E . 8A5D FD MOV BL,BYTE PTR SS:[EBP-3]
004019A1 . 02C3 ADD AL,BL
004019A3 . C645 FE 3F MOV BYTE PTR SS:[EBP-21],3F
004019A7 . 8A5D FE MOV BL,BYTE PTR SS:[EBP-2]
004019A8 . 32C3 XOR AL,BL
004019A9 . C645 FF 02 MOV BYTE PTR SS:[EBP-11],2
004019B0 . 005D FF ADD BYTE PTR SS:[EBP-11],BL
004019B3 . F7E3 MUL EBX
004019B5 . 93 XCHG EAX,EBX
004019B6 . 29C3 AND EAX,EBX
004019B8 . 86F8 XCHG AL,BH
004019B9 . 32C3 XOR AL,BL
004019BC . 83E8 09 SUB EAX,9
004019BF . 8B45 08 MOV EAX,DWORD PTR SS:[EBP+8]
004019C2 . 83C0 01 ADD EAX,1
004019C5 . 8B45 08 MOV EAX,DWORD PTR SS:[EBP+8]
004019C8 . 03C1 ADD EAX,ECX
004019CA . 83F8 21 CMP EAX,21
004019CD . 73 03 JNB SHORT 1_5.004019D2
004019CF . 83C0 21 ADD EAX,21
004019D2 > 83F8 7B CMP EAX,7B
004019D5 . 7E 02 JLE SHORT 1_5.004019D9
004019D7 . D1E8 SHR EAX,1
004019D9 > 8945 08 MOV DWORD PTR SS:[EBP+8],EAX
004019DC . 8B45 08 MOV EAX,DWORD PTR SS:[EBP+8]
004019DF . C9 LEAVE
004019E0 . C3 RETN
004019E1 $ 8B3D E4324000 LEA EDI,DWORD PTR DS:[4032E4]
004019E7 . 6A 00 PUSH 0
004019E9 . 6A 00 PUSH 0
004019EB . 50 PUSH EAX
004019EC . DF2C24 FILD QWORD PTR SS:[ESP]
004019F1 . DF3424 FBSTP TBYTE PTR SS:[ESP]
004019F2 . 59 POP ECX

```

Registers (FPU)

EAX	0019FFCC
ECX	00401065 1_5.<ModuleEntryPoint>
EDX	00401065 1_5.<ModuleEntryPoint>
EBX	002C6000
ESP	0019FF74
EBP	0019FF80
ESI	00401065 1_5.<ModuleEntryPoint>
EDI	00401065 1_5.<ModuleEntryPoint>
EIP	00401065 1_5.<ModuleEntryPoint>
C 0	ES 002B 32bit 0(FFFFFFFF)
P 1	CS 0023 32bit 0(FFFFFFFF)
A 0	SS 002B 32bit 0(FFFFFFFF)
Z 1	DS 002B 32bit 0(FFFFFFFF)
S 0	FS 0053 32bit 2C9000(FFF)
T 0	GS 002B 32bit 0(FFFFFFFF)
D 0	
O 0	LastErr ERROR_MOD_NOT_FOUND (0000007E)
EFL	00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0	empty 0.0
ST1	empty 0.0
ST2	empty 0.0
ST3	empty 0.0
ST4	empty 0.0
ST5	empty 0.0
ST6	empty 0.0
ST7	empty 0.0

FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1

Address Hex dump ASCII

00403000	00 00 00 00 00 00 00 00 00 00 00
00403008	00 00 00 00 00 00 00 00 00 00 00
00403010	00 00 00 00 00 00 00 00 00 00 00
00403018	00 00 00 00 00 00 00 00 00 00 00
00403020	00 00 00 00 00 00 00 00 00 00 00
00403028	00 00 00 00 00 00 00 00 00 00 00
00403030	00 00 00 00 00 00 00 00 00 00 00
00403038	00 00 00 00 00 00 00 00 00 00 00
00403040	00 00 00 00 00 00 00 00 00 00 00
00403048	00 00 00 00 00 00 00 00 00 00 00
00403050	00 00 00 00 00 00 00 00 00 00 00
00403058	00 00 00 00 00 00 00 00 00 00 00
00403060	00 00 00 00 00 00 00 00 00 00 00
00403068	54 6F 6F 6C 74 69 70 73	Tooltips

Program entry point

Paused

Windows Taskbar icons

604 PM ENG 12/30/2019

Tiếp tục di chuyển ta sẽ nhảy đến địa chỉ 0040197F, tuy nhiên từ địa chỉ 004019C5 đến 004019DC mới là đoạn mã hóa chính. Giá trị ascii (tương đương ở dạng hexa) của mỗi chữ cái/ kí tự của key vừa nhập được đặt ở EAX. Sau đó nó được cộng với giá trị ở ECX. Nếu EAX lớn hơn 21 sẽ nhảy tới địa chỉ 004019CC. Sau đó giá trị được so sánh với 7B thì sẽ thực hiện thao tác SHR EAX, 1. Giá trị này sau đó được lưu trữ. (SHL = shift logical right). Kí tự tiếp theo của chữ số đó được lấy ra và đặt ở EAX, ECX bị giảm và cứ thế lặp lại cho đến khi ECX = 0

OllyDbg - 1.5.exe - [CPU - main thread, module 1_5]

File View Debug Plugins Options Window Help

Registers (FPU)

```

EAX 0019FFCC
ECX 00401065 1_5.<ModuleEntryPoint>
EDX 00401065 1_5.<ModuleEntryPoint>
EBX 002C6000
ESP 0019FF74
EBP 0019FF80
ESI 00401065 1_5.<ModuleEntryPoint>
EDI 00401065 1_5.<ModuleEntryPoint>
EIP 00401065 1_5.<ModuleEntryPoint>
C 0 ES 002B 32bit 0(FFFFFFFF)
P 1 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
Z 1 DS 002B 32bit 0(FFFFFFFF)
S 0 FS 0053 32bit 2C9000(FFFF)
T 0 GS 002B 32bit 0(FFFFFFFF)
D 0
0 0 LastErr ERROR_MOD_NOT_FOUND (0000007E)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
3 2 1 0 E S P U O Z D I
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1

```

Registers (CPU)

```

0019FF74 7614E989 RETURN to KERNEL32.7614E989
0019FF78 002C6000
0019FF7C 7614E970 KERNEL32.BaseThreadInitThunk
0019FF80 0019FFDC
0019FF84 77495DE4 RETURN to ntdll.77495DE4
0019FF88 002C6000
0019FF8C 31DAB879
0019FF90 00000000
0019FF94 00000000
0019FF98 002C6000
0019FF9C 00000000
0019FFA0 00000000
0019FFA4 00000000
0019FFA8 00000000
0019FFAC 00000000

```

Stack Dump

Address	Hex dump	ASCII
00403000	00 00 00 00 00 00 00 00 00 00 00
00403008	00 00 00 00 00 00 00 00 00 00 00
00403010	00 00 00 00 00 00 00 00 00 00 00
00403018	00 00 00 00 00 00 00 00 00 00 00
00403020	00 00 00 00 00 00 00 00 00 00 00
00403028	00 00 00 00 00 00 00 00 00 00 00
00403030	00 00 00 00 00 00 00 00 00 00 00
00403038	00 00 00 00 00 00 00 00 00 00 00
00403040	00 00 00 00 00 00 00 00 00 00 00
00403048	00 00 00 00 00 00 00 00 00 00 00
00403050	00 00 00 00 00 00 00 00 00 00 00
00403058	00 00 00 00 00 00 00 00 00 00 00
00403060	00 00 00 00 00 00 00 00 00 00 00
00403068	54 6F 6F 6C 74 69 70 73	Tooltips

Program entry point

Paused

6:16 PM ENG 12/30/2019

Sau lần gọi cuối đó chúng ta sẽ quay lại 6 dòng như trong hình

OllyDbg - 1.5.exe - [CPU - main thread, module 1_5]

File View Debug Plugins Options Window Help

L E M T W H C / K B R ... S ?

```

0040190F . C9 LEAVE
004019E0 . C3 RETN
004019E1 $ 8D3D E4324000 LER EDI,DWORD PTR DS:[4032E4]
004019E7 . 6A 00 PUSH 0
004019E9 . 6A 00 PUSH 0
004019EB . 50 PUSH EAX
004019EC . DF2C24 FILD QWORD PTR SS:[ESP]
004019F1 DF3424 FBSTP TBYTE PTR SS:[ESP]
004019F2 . 59 POP ECX
004019F3 . 58 POP EAX
004019F4 . 8BD1 MOV EDX,ECX
004019F6 . 8BD8 MOV EBX,ECX
004019F8 . C1E9 04 SHR ECX,4
004019F9 . C1E9 04 SHL EHX,4
004019FE . 83E3 0F AND EBX,0F
00401A01 . 81E2 0F0F0F0F AND EDX,0F0F0F0F
00401A07 . 81E1 0F0F0F0F AND ECX,0F0F0F0F
00401A0D . 81C2 30303030 ADD EDX,30303030
00401A13 . 81C1 30303030 ADD ECX,30303030
00401A19 . 83C0 30 ADD EAX,30
00401A1C . 83C3 30 ADD EBX,30
00401A1F . 8807 MOV BYTE PTR DS:[EDI],AL
00401A21 . 885F 01 MOV BYTE PTR DS:[EDI+1],BL
00401A24 . 884F 08 MOV BYTE PTR DS:[EDI+8],CL
00401A27 . 8857 09 MOV BYTE PTR DS:[EDI+9],DL
00401A2A . 886F 06 MOV BYTE PTR DS:[EDI+6],CH
00401A2D . 8877 07 MOV BYTE PTR DS:[EDI+7],DH
00401A30 . 0FC9 BSADP ECX
00401A32 . 0FC9 BSADP EDX
00401A34 . 884F 02 MOV BYTE PTR DS:[EDI+2],CL
00401A37 . 8857 03 MOV BYTE PTR DS:[EDI+3],DL
00401A3A . 886F 04 MOV BYTE PTR DS:[EDI+4],CH
00401A3D . 8877 05 MOV BYTE PTR DS:[EDI+5],DH
00401A40 . 58 POP EAX

```

Registers (FPU)

EAX	0019FFCC
ECX	00401065 1_5.<ModuleEntryPoint>
EDX	00401065 1_5.<ModuleEntryPoint>
EBX	002C6000
ESP	0019FF74
EBP	0019FF80
ESI	00401065 1_5.<ModuleEntryPoint>
EDI	00401065 1_5.<ModuleEntryPoint>
EIP	00401065 1_5.<ModuleEntryPoint>
C 0	ES 002B 32bit 0(FFFFFF)
P 1	CS 0023 32bit 0(FFFFFF)
A 0	SS 002B 32bit 0(FFFFFF)
Z 1	DS 002B 32bit 0(FFFFFF)
S 0	FS 0053 32bit 2C9000(F)
T 0	GS 002B 32bit 0(FFFFFF)
D 0	
O 0	LastErr ERROR_MOD_NOT_FOUND (0000007E)
EFL	00000026 (NO,NB,E,BE,NS,PE,GE,LE)
ST0	empty 0.0
ST1	empty 0.0
ST2	empty 0.0
ST3	empty 0.0
ST4	empty 0.0
ST5	empty 0.0
ST6	empty 0.0
ST7	empty 0.0

3 2 1 0 E S P U O Z D I
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1 1

Address Hex dump ASCII

00403000	00 00 00 00 00 00 00 00
00403008	00 00 00 00 00 00 00 00
00403010	00 00 00 00 00 00 00 00
00403018	00 00 00 00 00 00 00 00
00403020	00 00 00 00 00 00 00 00
00403028	00 00 00 00 00 00 00 00
00403030	00 00 00 00 00 00 00 00
00403038	00 00 00 00 00 00 00 00
00403040	00 00 00 00 00 00 00 00
00403048	00 00 00 00 00 00 00 00
00403050	00 00 00 00 00 00 00 00
00403058	00 00 00 00 00 00 00 00
00403060	00 00 00 00 00 00 00 00
00403068	54 6F 6C 74 69 70 73	Tooltips

Program entry point

Paused

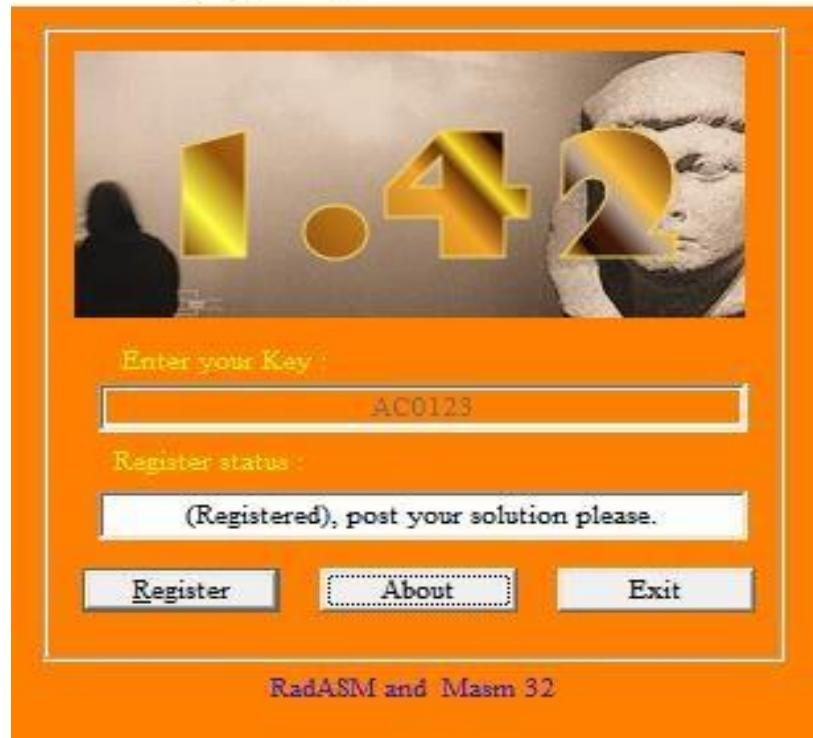
621 PM ENG 12/30/2019

Sau đó nó sẽ nhảy tới địa chỉ 004019E1. Ở địa chỉ 004019EF sẽ chuyển đổi 4 bytes được lưu của key được mã hóa đến giá trị decimal. Phần mã còn lại định dạng thập phân, vd 123456789 thì giá trị decimal là 3938 được lưu trữ sau khi định dạng.

00401521	. 33C0	XOR EAX,EAX
00401523	. 33DB	XOR EBX,EBX
00401525	. 66:A1 3B334000	MOV AX,WORD PTR DS:[40333B]
0040152B	. 66:8B5F 08	MOV BX,WORD PTR DS:[EDI+8]
0040152F	. 66:2BC9	SUB AX,BX
00401532	. 35 3F1B0000	XOR EAX,1B3F
00401537	. 2D 23010000	SUB EAX,123
0040153C	FR 03	IMP SHORT 1 5 00401541

Hai bytes đầu tiên của key mã hóa được lưu ở địa chỉ 00401977 thì di chuyển đến EAX. Phần định dạng được chuyển đến EBX. Sau đó lấy EAX – EBX. Kết quả có được thực hiện phép xor với 1B3F và trừ cho 123. Nếu kết quả cuối cùng là 0 sẽ không nhảy tới địa chỉ 00401543 mà sẽ nhận được thông báo đăng ký thành công.

Ribbere 1.42 (Registered)



1.4

Đầu tiên mở chương trình lên, vào serach for -> all referenced text strings

Address	Disassembly	Text String
004031ED	PUSH 1 4 .0047B048	ASCII "RES-REGGED.txt"
004031F0	PUSH 1 4 .0047B034	ASCII "RES-VALIDATE.diz"
004032E1	PUSH 1 4 .0047B05C	ASCII "EDIT"
004033D0	PUSH 1 4 .0047B05C	ASCII "EDIT"
00403408	PUSH 1 4 .0047B07C	ASCII "Validate"
0040340D	PUSH 1 4 .0047B074	ASCII "BUTTON"
00403440	PUSH 1 4 .0047B06C	ASCII "About"
0040344F	PUSH 1 4 .0047B074	ASCII "BUTTON"
0040348C	PUSH 1 4 .0047B064	ASCII "Exit"
00403491	PUSH 1 4 .0047B074	ASCII "BUTTON"
004035E0	PUSH 1 4 .0047B18C	ASCII "VERBATIM :: Keygenme"
00403623	PUSH 1 4 .0047B164	ASCII "Enter a name and press validate!"
004037JB	PUSH 1 4 .0047B160	ASCII "XIX"
004037C9	PUSH 1 4 .0047B15C	ASCII "x0"
004037CE	PUSH 1 4 .0047B148	ASCII "Serial Accepted"
004037E0	PUSH 1 4 .0047B13C	ASCII ":: STATUS
004037EF	PUSH 1 4 .0047B120	ASCII "Key/Keys not accepted!"
0040380F	PUSH 1 4 .0047B110	ASCII ":: VERBATIM"
00403814	PUSH 1 4 .0047B088	ASCII "Coded by Amasazi//RESiSTANCE Greetz fly out to Shub, hex0101, the mUTABLE, 0x87k, Potassium, lena151 and Ank83"
004087F3	PUSH 1 4 .0047B254	ASCII "missing locale facet"
004089F3	PUSH 1 4 .0047B254	ASCII "missing locale facet"
00408960	PUSH 1 4 .0047B254	ASCII "missing locale facet"
00408ECD	PUSH 1 4 .0047B278	ASCII "0123456789abcdefHBCDEF"
0040BF73	PUSH 1 4 .0047B254	ASCII "missing locale facet"
0040D36D	MOV EAX,1 4 .0047B294	ASCII "false"
0040D3AD	MOV EAX,1 4 .0047B29C	ASCII "true"
0040D0DF	ASCII "'c'" ,0	
0040E000	ASCII "'c'" ,0	
0040E067	ASCII "'c'" ,0	
0040E130	ASCII "'c'" ,0	
00412264	MOV DWORD PTR SS:[EBP-110],1 4 .0047B320	ASCII "Extended Module: "
004138B3	PUSH 1 4 .0047B420	ASCII ".CrtCheckMemory()"
004138C1	PUSH 1 4 .0047B414	ASCII "dbgheap.c"
00413924	PUSH 1 4 .0047B3DC	ASCII "Client hook allocation failure at file %hs line %d."
00413947	PUSH 1 4 .0047B3B8	ASCII "Client hook allocation failure."
0041394C	PUSH 1 4 .0047B3B4	ASCII "%s"
00413908	PUSH 1 4 .0047B390	ASCII "Invalid allocation size: %u bytes."
004139F0	PUSH 1 4 .0047B35C	ASCII "Error: memory allocation: bad memory block type."
004139FF	PUSH 1 4 .0047B3B4	ASCII "%s"
00413CEB	PUSH 1 4 .0047B420	ASCII ".CrtCheckMemory()"
00413CF7	PUSH 1 4 .0047B414	ASCII "dbgheap.c"
00413D5C	PUSH 1 4 .0047B59C	ASCII "Client hook re-allocation failure at file %hs line %d."
00413D7F	PUSH 1 4 .0047B578	ASCII "Client hook re-allocation failure."
00413D84	PUSH 1 4 .0047B3B4	ASCII "%s"
00413DB6	PUSH 1 4 .0047B548	ASCII "Allocation too large or negative: %u bytes."
00413E00	PUSH 1 4 .0047B35C	ASCII "Error: memory allocation: bad memory block type."
00413E05	PUSH 1 4 .0047B3B4	ASCII "%s"
00413E36	PUSH 1 4 .0047B524	ASCII ".CrtIsValidHeapPointer(pUserData)"
00413E42	PUSH 1 4 .0047B414	ASCII "dbgheap.c"

Ta thấy ở địa chỉ 004037CE là chuỗi thông báo serial accepted, ta tiếp tục nhấn vào dòng đó để đi đến địa chỉ đó

OllyDbg - 1.4.exe - [CPU - main thread, module 1_4]

File View Debug Plugins Options Window Help

L E M T W H C / K B R ... S ?

00403696	. 8BF4	MOV ESI,ESP
00403698	. 6A 14	PUSH 14
0040369A	. 8D45 EC	LEA EAX,DWORD PTR SS:[EBP-14]
0040369D	. 50	PUSH EAX
0040369E	. 6A 6A	PUSH 6A
004036A0	. 8B4D 08	MOV ECX,DWORD PTR SS:[EBP+8]
004036A3	. 51	PUSH ECX
004036A4	FF15 98144A00	CALL DWORD PTR DS:[4A1498]
004036A6	. 3BF4	CMP ESI,ESP
004036AC	. E8 8F1F0100	CALL 1_4.00415640
004036B1	. 8D55 EC	LEA EDX,DWORD PTR SS:[EBP-14]
004036B4	. 52	PUSH EDX
004036B5	. E8 86290100	CALL 1_4.00416040
004036B8	. 89C4 04	ADD ESP,4
004036BD	. 8BF4	MOV ESI,ESP
004036BE	. 6A 14	PUSH 14
004036C1	. 8D45 D8	LEA EAX,DWORD PTR SS:[EBP-28]
004036C4	. 50	PUSH EAX
004036C5	. 6A 6B	PUSH 6B
004036C7	. 8B4D 08	MOV ECX,DWORD PTR SS:[EBP+8]
004036CA	. 51	PUSH ECX
004036CB	FF15 98144A00	CALL DWORD PTR DS:[4A1498]
004036D1	. 3BF4	CMP ESI,ESP
004036D3	. E8 681F0100	CALL 1_4.00415640
004036D8	. 8D55 D8	LEA EDX,DWORD PTR SS:[EBP-28]
004036DB	. 52	PUSH EDX
004036DC	. E8 5F290100	CALL 1_4.00416040
004036E1	. 89C4 04	ADD ESP,4
004036E4	. 8D45 EC	LEA EAX,DWORD PTR SS:[EBP-14]
004036E7	. 50	PUSH EAX
004036E8	. E8 D3280100	CALL 1_4.00415FC0
004036ED	. 89C4 04	ADD ESP,4
004036F0	. 8945 C0	MOV DWORD PTR SS:[EBP-40],EAX
004036F3	. 8B4D B8	MOV ECX,DWORD PTR SS:[EBP-48]

Count = 14 (20.)

Buffer ControlID = 6A (106.)

hWnd GetDlgItemTextA

Count = 14 (20.)

Buffer ControlID = 6B (107.)

hWnd GetDlgItemTextA

Registers (FPU)

EAX 0019FFCC ECX 00417DC0 1_4.<ModuleEntryPoint> EDX 00417DC0 1_4.<ModuleEntryPoint> EBX 002EC000 ESP 0019FF74 EBP 0019FF80 ESI 00417DC0 1_4.<ModuleEntryPoint> EDI 00417DC0 1_4.<ModuleEntryPoint> EIP 00417DC0 1_4.<ModuleEntryPoint>

C 0 ES 002B 32bit 0{FFFFFF}

P 1 CS 0023 32bit 0{FFFFFF}

A 0 SS 002B 32bit 0{FFFFFF}

Z 1 DS 002B 32bit 0{FFFFFF}

S 0 FS 0053 32bit 2EF000(FFF)

T 0 GS 002B 32bit 0{FFFFFF}

D 0

O 0 LastErr ERROR_SXS_KEY_NOT_FOUND (000036B7)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty 0.0 ST1 empty 0.0 ST2 empty 0.0 ST3 empty 0.0 ST4 empty 0.0 ST5 empty 0.0 ST6 empty 0.0 ST7 empty 0.0

3 2 1 0 E S P U O Z D I
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,59 Mask 1 1 1 1 1 1

Sau đó ta kéo lên trên thấy được tại hai dòng đỏ như trong hình là dòng cho người dùng nhập Name và Serial

OllyDbg - 1.4.exe - [CPU - main thread, module 1_4]

File View Debug Plugins Options Window Help

Registers (FPU)

EAX 0019FFCC
 ECX 00417DC0 1_4.<ModuleEntryPoint>
 EDX 00417DC0 1_4.<ModuleEntryPoint>
 EBX 002EC000
 ESP 0019FF74
 EBP 0019FF80
 ESI 00417DC0 1_4.<ModuleEntryPoint>
 EDI 00417DC0 1_4.<ModuleEntryPoint>
 EIP 00417DC0 1_4.<ModuleEntryPoint>

C 0 ES 002B 32bit 0(FFFFFFF)
 P 1 CS 0023 32bit 0(FFFFFFF)
 A 0 SS 002B 32bit 0(FFFFFFF)
 Z 1 DS 002B 32bit 0(FFFFFFF)
 S 0 FS 0053 32bit 2E000(F)
 T 0 GS 002B 32bit 0(FFFFFFF)
 D 0
 0 0 LastErr ERROR_SXS_KEY_NOT_FOUND (000036B7)
 EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty 0.0
 ST1 empty 0.0
 ST2 empty 0.0
 ST3 empty 0.0
 ST4 empty 0.0
 ST5 empty 0.0
 ST6 empty 0.0
 ST7 empty 0.0

3	2	1	0	E	S	P	U	O	Z	D	I	
FST	0000	Cond	0	0	0	0	Err	0	0	0	0	(GT)
FCW	027F	Prec	NEAR,53	Mask	1	1	1	1	1	1	1	

^ Registers (FPU)

004036E8 . E8 D3280100 CALL 1_4.00415FC0
 004036ED . 83C4 04 ADD ESP,4
 004036F0 . 8945 C0 MOV DWORD PTR SS:[EBP-40],EAX
 004036F3 . 8B4D B8 MOV ECX,DWORD PTR SS:[EBP-48]
 004036F6 . 334D B8 XOR ECX,DWORD PTR SS:[EBP-48]
 004036F9 . 8940 B8 MOV DWORD PTR SS:[EBP-48],ECX
 004036FC . C745 AC 000000 MOV DWORD PTR SS:[EBP-54],0
 00403703 . EB 09 JMP SHORT 1_4.0040370E
00403705 > 8B55 AC MOV EDX,DWORD PTR SS:[EBP-54]
 00403708 . 89C2 01 ADD EDX,1
0040370B > 8955 AC MOV DWORD PTR SS:[EBP-54],EDX
0040370E > 8B45 AC MOV EAX,DWORD PTR SS:[EBP-54]
00403711 . 3B45 C0 CMP EAX,DWORD PTR SS:[EBP-40]
00403714 . 7D 1F JGE SHORT 1_4.00403735
00403716 . 8B4D AC MOV ECX,DWORD PTR SS:[EBP-54]
00403719 . 0FBE540D EC MOVSS EDX,BYTE PTR SS:[EBP-ECX-14]
0040371E . 8955 BC MOV DWORD PTR SS:[EBP-44],EDX
00403721 . 8B45 BC MOV EAX,DWORD PTR SS:[EBP-44]
00403724 . 89E8 20 SUB EAX,20
00403727 . 8945 BC MOV DWORD PTR SS:[EBP-44],EAX
0040372B . 8B4D B8 MOV ECX,DWORD PTR SS:[EBP-48]
0040372D . 2B4D BC SUB ECX,DWORD PTR SS:[EBP-44]
00403730 . 894D B8 MOV DWORD PTR SS:[EBP-48],ECX
00403733 ^ EB D0 JMP SHORT 1_4.00403705
00403735 > 8BF4 MOV ESI,ESP
00403737 . 8B55 B8 MOV EDX,DWORD PTR SS:[EBP-48]
0040373B . 52 PUSH EDX
0040373B . 68 60B14700 PUSH 1_4.0047B160
00403740 . 8D45 C4 LEA EAX,DWORD PTR SS:[EBP-3C]
00403743 . 50 PUSH EAX
00403744 . FF15 94144A00 CALL DWORD PTR DS:[4A1494]
00403748 . 83C4 0C ADD ESP,0C
0040374D . 3BF4 CMP ESI,ESP
0040374F . E8 EC1E0100 CALL 1_4.00415640

<%IX>
 Format = "%IX"
 S **wprintfA**

Tiếp tục kéo xuống dưới ta thấy được từ địa chỉ 00403705 -> 00403733 là đoạn phát ra Serial từ Name ta đã nhập

004036D8 8D55 D8 LEA EDX,DWORD PTR SS:[EBP-28] → serial chuyển đến EDX

004036DB 52 PUSH EDX → lưu serial

004036E4 8D45 EC LEA EAX,DWORD PTR SS:[EBP-14] → đảo ngược Name đến EAX

004036E7 50 PUSH EAX → lưu tên đảo ngược

004036F3 8B4D B8 MOV ECX,DWORD PTR SS:[EBP-48] → đảo ngược tên đến ECX

Về phần phát sinh key những dòng màu đỏ như trong hình có thể giải thích ngắn gọn như sau: ban đầu từ chuỗi nam người dùng nhập vào chương trình sẽ đảo ngược chuỗi Name, sau đó dùng vòng lặp với biến đếm là EDX để lấy ra từng ký tự của chuỗi Name đã bị đảo ngược gán vào EAX rồi trừ cho 20 ở hệ Hexa và lưu kết quả. Sau đó lấy ECX trừ cho kết quả đó. Sau khi chạy vòng lặp ta có được kết quả ở Hexa kiểu 8 bits, đảo ngược lại kết quả đó ta có được Serial, vd với Name nhập vào là “a” thì ta có được Serial tương ứng sau khi đảo ngược là: “FBFFFFFF”. Tuy nhiên đến đây tuy ta đã có được Name và Serial của chương trình những nếu nhập vào thì vẫn bị báo là sai.

The screenshot shows the OllyDbg debugger interface with the assembly window on the left and the registers window on the right.

Registers (FPU)

```

EAX 0019FFCC
ECX 00417DC0 1_4.<ModuleEntryPoint>
EDX 00417DC0 1_4.<ModuleEntryPoint>
EBX 002EC000
ESP 0019FF74
EBP 0019FF80
ESI 00417DC0 1_4.<ModuleEntryPoint>
EDI 00417DC0 1_4.<ModuleEntryPoint>
EIP 00417DC0 1_4.<ModuleEntryPoint>
C 0 ES 002B 32bit 0{FFFFFF}
P 1 CS 0023 32bit 0{FFFFFF}
A 0 SS 002B 32bit 0{FFFFFF}
Z 1 DS 002B 32bit 0{FFFFFF}
S 0 FS 0053 32bit 2EF000(F)
T 0 GS 002B 32bit 0{FFFFFF}
D 0
O 0 LastErr ERROR_SXS_KEY_NOT_FOUND (000036B7)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0

```

FST 0000 Cond 0 0 0 Err 0 0 0 0 0 0 0 (GT)

FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1

ASCII "RES-REGGED.txt"

```

00402EDA: 6A 01    PUSH 1
00402EDC: . 8D8D C0FEFFFF LEA ECX,DWORD PTR SS:[EBP-140]
00402EE2: . E8 4AE2FFFF CALL 1_4.00401191
00402EE7: . C645 FC 02 MOV BYTE PTR SS:[EBP-41],2
00402EEB: . 6A 01    PUSH 1
00402F00: . 68 48B84700 PUSH 1_4.00401226
00402F2: . 8D8D 50FFFFFF LEA ECX,DWORD PTR SS:[EBP-B0]
00402F8: . E8 6BE2FFFF CALL 1_4.00401168
00402FD: . 8B80 50FFFFFF MOV ECX,DWORD PTR SS:[EBP-B0]
00402F03: . 8B51 04    MOV EDX,DWORD PTR DS:[ECX+4]
00402F06: . 8D8C15 50FFFFFF LEA ECX,DWORD PTR SS:[EBP+EDX-B0]
00402F00: . E8 14E3FFFF CALL 1_4.00401226
00402F12: . 25 FF000000 AND EAX,0FF
00402F17: . 85C0    TEST EAX,EAX
00402F19: . 74 0C    JE SHORT 1_4.00402F27
00402F1B: > C705 F0624900 MOV DWORD PTR DS:[4962F0],0
00402F25: . EB 0A    JMP SHORT 1_4.00402F31
00402F27: > C705 F0624900 MOV DWORD PTR DS:[4962F0],1
00402F31: > 8D45 E0    LEA EAX,DWORD PTR SS:[EBP-B0]
00402F34: . 50      PUSH EAX
00402F35: . 8D8D 50FFFFFF LEA ECX,DWORD PTR SS:[EBP-B0]
00402F3B: . E8 8FE4FFFF CALL 1_4.004013CF
00402F40: > 8D80 50FFFFFF LEA ECX,DWORD PTR SS:[EBP-B0]
00402F46: . 85C9    TEST ECX,ECX
00402F48: . 75 0C    JNZ SHORT 1_4.00402F56
00402F4A: . C785 B8FEFFFF MOV DWORD PTR SS:[EBP-148],0
00402F54: . EB 16    JNP SHORT 1_4.00402F6C
00402F56: > 8B95 50FFFFFF MOV EDX,DWORD PTR SS:[EBP-B0]
00402F5C: . 8B42 04    MOV EAX,DWORD PTR DS:[EDX+4]
00402F5F: . 8D8C05 50FFFFFF LEA ECX,DWORD PTR SS:[EBP+EDX-B0]
00402F66: . 8980 B8FEFFFF MOV DWORD PTR SS:[EBP-148],ECX
00402F6C: > 8B80 B8FEFFFF MOV ECX,DWORD PTR SS:[EBP-148]
00402F72: . E8 16E5FFFF CALL 1_4.0040148D
00402F77: . 85C0    TEST EAX,EAX

```

Đến đây ta kéo lên trên và phát hiện ở địa chỉ 00402EF2 chương trình sẽ kiểm tra file RES-REGGED.txt

OllyDbg - 1.4.exe - [CPU - main thread, module 1_4]

File View Debug Plugins Options Window Help

Registers (FPU)

```

EAX 0019FFCC
ECX 00417DC0 1_4.<ModuleEntryPoint>
EDX 00417DC0 1_4.<ModuleEntryPoint>
EBX 002EC000
ESP 0019FF74
EBP 0019FF80
ESI 00417DC0 1_4.<ModuleEntryPoint>
EDI 00417DC0 1_4.<ModuleEntryPoint>
EIP 00417DC0 1_4.<ModuleEntryPoint>

```

C 0 ES 002B 32bit 0(FFFFFFFF)
P 1 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
Z 1 DS 002B 32bit 0(FFFFFFFF)
S 0 FS 0053 32bit 2EF000(F)
T 0 GS 002B 32bit 0(FFFFFFFF)
D 0

0 0 LastErr ERROR_SXS_KEY_NOT_FOUND (000036B7)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0

3 2 1 0 E S P U O Z D I
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1

ASCII "RES-VALIDATE.diz"

Address Hex dump ASCII

```

0040000C 50 45 00 00 4C 01 03 00 PE..L0V.
00400014 00 00 00 00 00 00 00 00 .....
0040001C 00 00 00 00 E0 00 F0 01 .....0.00
00400024 0B 01 00 00 00 02 00 00 <0.....0..
0040002C 00 00 00 00 00 00 00 00 .....
00400034 C0 7D 81 00 00 10 00 00 l]0...>.
0040003C 0C 00 00 00 00 00 40 00 .....e.
00400044 00 10 00 00 00 10 00 00 >....>.
0040004C 04 00 00 00 00 00 00 00 <.....>.
00400054 00 00 00 00 00 00 00 00 <.....>.
0040005C 00 D0 12 00 00 02 00 00 <.....>.
00400064 00 00 00 00 02 00 00 00 <.....>.
0040006C 00 00 10 00 00 10 00 00 <.....>.
00400074 00 00 10 00 00 10 00 00 <.....>.

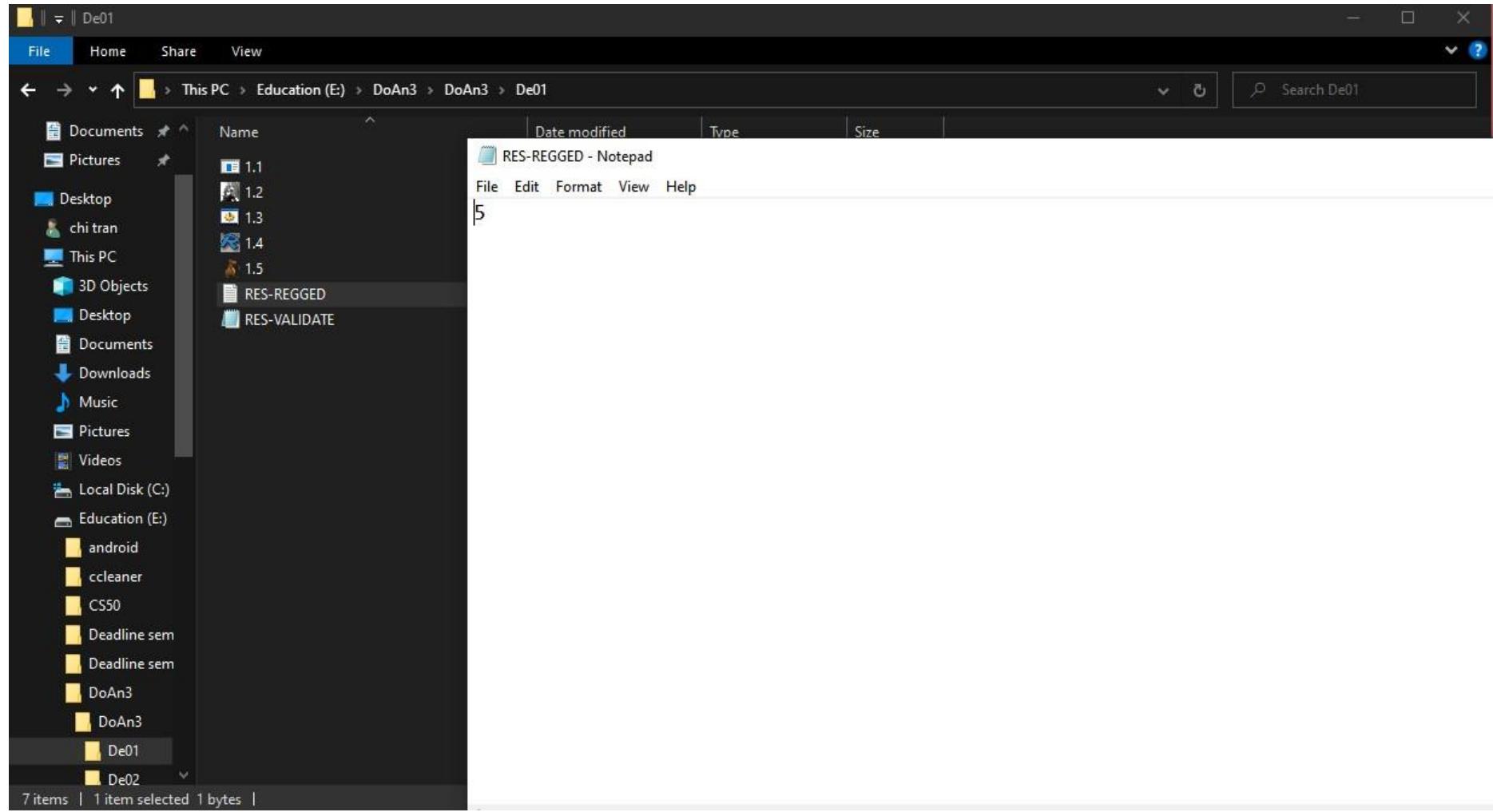
```

0019FF74 761BF989 RETURN to KERNEL32.761BF989

002EC000
0019FF78 761BF970 KERNEL32.BaseThreadInitThunk
0019FF80 0019FFDC
0019FF84 77775DE4 RETURN to ntdll.77775DE4
0019FF88 002EC000
0019FF8C C180A31B
0019FF90 00000000
0019FF94 00000000
0019FF98 002EC000
0019FF9C 00000000
0019FFA0 00000000
0019FFA4 00000000
0019FFA8 00000000
0019FFAC 00000000

Paused 11:55 AM 12/31/2019

Sau đó từ địa chỉ 00402F7F -> 00402F87 sẽ kiểm tra xem số trong file đó < 1 hoặc > 5, tiếp theo ở địa chỉ 00402F93 chương trình sẽ kiểm tra tiếp 1 file có tên là RES-VALIDATE.diz. Ta có nhận xét file RES-VALIDATE.diz chỉ cần được đặt chung trong folder với file crack còn lại ko có dữ liệu gì trong đó còn file RES-REGGED.txt sẽ có 1 con số trong khoảng từ 1 → 5



Ta cũng tạo 2 file như vậy và nhập vào thử số 5 trong file RES-REGGED.txt và debug chương trình lại 1 lần nữa với Name và Serial ta đã có được ở trên và kết quả là chương trình hiện thông báo thành công

OllyDbg - 1.4.exe - [CPU - main thread, module 1_4]

File View Debug Plugins Options Window Help

L E M T W H C / K B R ... S ☰ ?

```

00402FF1 > 8D80 50FFFFFF LEA ECX,DWORD PTR SS:[EBP-B0]
00402FF7 . E8 97E3FFFF CALL 1_4.00401393
00402FFC . C645 FC 01 MOV BYTE PTR SS:[EBP-4],1
00403000 . 8D8D C0FEFFFF LEA ECX,DWORD PTR SS:[EBP-140]
00403006 . E8 2CE5FFFF CALL 1_4.00401537
0040300B . C645 FC 00 MOV BYTE PTR SS:[EBP-4],0
0040300F . 8D8D 50FFFFFF LEA ECX,DWORD PTR SS:[EBP-B0]
00403015 . E8 1DE5FFFF CALL 1_4.00401537
0040301A . C745 FC FFFFFF MOV DWORD PTR SS:[EBP-4],-1
00403021 . 8D4D E4 LEA ECX,DWORD PTR SS:[EBP-1C]
00403024 . E8 68E5FFFF CALL 1_4.00401591
00403029 . 8B4D F4 MOV ECX,DWORD PTR SS:[EBP-C]
0040302C 64:890D 000000 MOV DWORD PTR FS:[0],ECX
00403033 . 5F POP EDI
00403034 . 5E POP ESI
00403035 . 5B POP EBX
00403036 . 81C4 88010000 ADD ESP,188
0040303C . 3BEC CMP EBP,ESP
0040303E . E8 FD250100 CALL 1_4.00415640
00403043 . 8BE5 MOV ESP,EBP
00403045 . 5D POP EBP
00403046 . C3 RETN
00403047 CC INT3
00403048 CC INT3
00403049 CC INT3
0040304A CC INT3
0040304B CC INT3
0040304C CC INT3
0040304D CC INT3
0040304E CC INT3
0040304F CC INT3
00403050 CC INT3
00403051 CC INT3
00403052 CC INT3

```

Registers (FPU)

EAX 0019F664
ECX 0019F7D8
EDX 0019F664
EBX 00000001
ESP 0019F4EC
EBP 0019F680
ESI 0019F688
EDI 0019F674
EIP 0040302C 1_4.0040302C

C 0 ES 002B 32bit 0(FFFFFFFF)
P 1 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
Z 1 DS 002B 32bit 0(FFFFFFFF)
S 0 FS 0053 32bit 2EF000(FFF)
T 0 GS 002B 32bit 0(FFFFFFFF)
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty -256.000000000000000000000000000000
ST1 empty -3328.000000000000000000000000000000
ST2 empty -1055.0546569347980040
ST3 empty -215.21396553516387940
ST4 empty 1.00000000000000000000000000000000
ST5 empty 16.00000000000000000000000000000000
ST6 empty 16.00000000000000000000000000000000
ST7 empty 16.00000000000000000000000000000000

3 2 1 0 E S P U O Z D I
FST 4020 Cond 1 0 0 0 Err 0 0 1 0 0 0 0 0 (EQ)
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1

II. Mức độ hoàn thành

- Đánh giá mức độ hoàn thành: 100%