04.Basic+aesthetic patching

2012년 1월 28일 토요일

오전 10:11

기본문

Hello everybody.

Welcome to this Part 4 in my series about reversing for newbies/beginners.

This "saga" is intended for complete starters in reversing, also for those without any programming experience at all.

Lena151 (2006)

1. **Abstract**

In this Part 4, we will reverse a 'real" application. That is because indeed, the best practice is found in the real applications.

As always, the goal is NOT to study this particular case but to try to teach some basic techniques. This series is purely meant to bring you the ideas for continued reversing, to give you the basics from where you can start exploring and developing your skills.

In my search not to harm anybody, I came across Pixtopianbook. This is a program not updated since 1/2001 and thus probably abandoned. This application is targeted because it is ideal for this tutorial in reversing and as such is targeted for educational purposes only. I hope you will exploit your newly acquired knowledge in a positive way.

In this matter, I also want to refer to Part 1.

**이것도 똑같음**

Set your screen resolution to 1152\*864 and press F11 to see the movie full screen !!!

Again, I have made this movie interactive. So, if you are a fast reader and you want to continue to the next screen, just click here on this invisible hotspot. You don't see it, but it IS there on text screens. Then the movie will skip the text and continue with the next screen. If something is not clear or goes too fast, you can always use the control buttons and the slider below on this screen.

He, try it out and click on the hotspot to skip this text and to go to the next screen now !!!

Click here as soon as you finished reading (on each screen!)

During the whole movie you can click this spot to leave immediately

1. **Tools and Target**

**이것도 똑같음**

The tools for today are : Ollydebug and… your brain.

The first can be obtained for free at

<http://www.ollydbg.de>

Like always, the second is your responsibility ;)

Todays target is a program called Pixtopianbook v1.07. It is some kind of phonebook. Probably due to the upcoming broadband internet connections, the program seems to have set back in interest due to its dial-up connection working?

For your convenience and because the downloadsite can only be accessed using a certain browser, I included it in this package.

1. **A word about exceptions**

Todays application gives me the opportunity to tell you the little you need to know for now about exceptions.

오늘 application은 나에게 약간의 네가 필요한 것을 알아가기 위해 예외들을 말할 수 있는 기회를 주었다.

The program has the SEH(structured exception handler) to handle wanted or not wanted exceptions.

Program은 원하는 것과 원하지 않는 예외들을 handle 하기 위해 SEC가 있다.

Olly has difficulties handling these exceptions but gives us the possibility to let the program deal with these.

Olly는 어려운 이것들의 예외적인 handling을 한다. 그러나 우리에게 program과 협상 할 가능성을 준다.

So, that's what we will do for now. But for completeness, just remember for later that we use the exceptions, thrown at Olly by protectors, to easily get close to OEP.

그래서 우리는 이제 해야 한다. 그러나 완벽하기 위해, 기억해라. Olly에서 protectors에 의해 우리가 쓸 예외들을 OEP를 쉽게 얻기 위해서 던진다.

So, to find OEP in an easy way. That's all for now, I will explain this better when we deal with protectors. Don't worry yet :)

그래서 OEP를 쉬운 방법으로 찾자. 그것은 현재 모든 것이다. 우리가 protector와 거래할 때 나는 좀 더 좋게 설명할 것이다. 아직 걱정하지마 :)

SEH are also important when we come to anti-debugging and the likes. Again, see later

우리가 anti-debugging과 강은 것들을 할 경우 SEH는 또한 중요하다. 다시 보자.

So, let me show you first what happens if an exception occurs… BTW, I suppose you understand an exception occurs when something is not very good, right? ;))

그래서, 나는 너에게 첫번째로 exception이 발생할 때 무슨 일이 발생하는지 보여줄 것이다. By the way, 어떤 것은 매우 좋지 않다. 그렇죠? 네가 exception이 발생하는 것을 이해했을 거라 생각한다.

Like you can see, I have already opened the application in Olly. Let's run and see…

너처럼 보겠다. 나는 이미 application을 Olly에 열어 놓았다. 실행하고 보자.

시스템 생성 대체 텍스트: 미CP【j-耐inthread
RETtI4
【29】
F7
■■
■■■■■■■■■■■■■■■■
''IFfltj,
EIP
7CgBEBRCntd【1.Rt1Ra($eEㅐ。e
..800000
00】2E984
ee0000Oe
e012E978
0012E9D4
0012ER14
0012ER14
0e33084E
X니丹U八XPPt'1
H脾睡恪瑨
스－三-
CO ESOa근332b쵱to驢FFFFFFFF)
Pe CS001B32bit이FFFFFFFF)
Rl SS002332bi鸞O(FFFFFFFF〕
Ze DSO蝕2832bL零O(FFFFFFFF)
51 「S003B32bLt7FFDF00e(FFF
TO GSOO90HLjLL
D0
00 La$tErr티驪ofL珊뱁〔kELHOT--
EFL.0e0e0292〔NO.NB.NE,n,S,PO.ㄴ
STee"pt,1.4445416드0255413'320
STIehpt,-4.9585297144드2839707
STZehpt,＋바刃R"00180800e03B
ST3e"pty＋야刃R"oe3B001ZF180
ST4ehpt'一UHOR"F178e00002e2
ST드ehpt,＋바刃R"6098aaO0e28O
ST6.npt,+UHOR"29BEOOe0000e
ST7enot,9.읽19275395358870020
광2!0 E3
FST488e COnd!000 Erreo
F이Je온7F PrecHERR.53 "a$k
밌離離RL離円離離離離亂離亂亂亂
체J체J체J에■J맥■Jf.J쫴JIJ체JIJf.Jf■Jf.Jf.JIJ
U죠XX닌nXXUA닢AVCXXkK넋凸V凸
ETRTRTRTRTRTRTRTRTRTRTRTRTRTRTRTRTRTRTRTRTRTRTRTRTRTRTRTRTRTRTRTRTRTRTRTRTRTR
TPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPPP
V
BEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE
'TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT
H모부UTUTUTVVVV부부UTVYUT무V모부VVUTUTVV부UTUTVUγ부UT모UTVVVV
CBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
.Lr흩ㅗ
ㄴF7
CZe4e6
3RZD29000000
ae00
離離離亂離RL離離円離亂離Pl
낚Xk닢凸X나nXXXU쵸XVCX
nHnnHCHnHCHRCHnHCHCHnHn
EEEEEEEEEEEEF
DSDSDSDSDSDSDSDSDSDSDSDSm
圈硼RDORDORDOROO隅ROOPDOPDDqDD隅RDO刪qDDRDDRDOROOPDD刪隅翩
nonUdUeaUn룅dononpdUn킵nonpnUn디OO0enD0npnonodpnUnUnU0n
nO00doaO白pdpaoaodp쵸pnpd다npao白OeeaO白O白Odpaoenpaodonon
腑的盼ee騁盼盼盼盼盼盼的盼盼盼ee卵盼沁盼盼盼盼盼盼ee盼觸朋
003300드9
OO338OSB
OO3300SD
0033005F
O033eO61
00330063
OO33eO65
00330067
00330069
0033006B
0093006D
0033906F
00330071
00330073
0033007드
00330077
00330079
0033007B
0033e07D
Oe33007F
00330e81
0033Oe83
0033eO85
00330087
00330089
00330e8B
OO33008D
0033008「
00330091
00330093
00330095
00330097
00330099
0033009B
0033009D
0033009F
OO3300RI
nn요요nnn으
eo닝
000
ChP
ROO
RDD
RDD
姃勵
Bam!
이lybreaks...
PTRDS:
DS:[En
DS:〔En
DS:tER
05:[ER
DS:tER
05:tER
DS:tEn
DS:tER
DS:〔ER
DS:LER
DS.[En
DS.tEn
05:[En
DS:[ER
DS:tER
D요‘U乙
Ofcourseweco미drlowruntheprㅇgram
pressingShift+Fgbutl'msurethatyㅇu
understandthis15anannoyingthing.〕ust
IookhㅇwwecandealWithit...
RVTFPTR
《 '''l
R슨tUrn
to7C81EB33(kerne【32.7C81EB331
；鱗1匕ㅂ
'·1닐.J*
UH「ㅓ …lㅏ「I嘴＜·rL
더4f ...1nan
exceptionandtellsuswhattㅇdo
topasstheexcePtiontotheprogram
논－ㄱ’「貶尸∼－-－∼－
“「
Fl
가
f
[…
BTW
dㅇn'tforgetthat
r 」E춈느E뇨．'‘흽sese-se｀一一‘－一｀횹욜
yㅇucanalways
cliCkhereifyoufinishedreadingand
긴쁘뗄뺌쌜쀼墺
｀蝕丁丁l-
41빡4ㅓ낙l-4
COmman(1
ExceP聃nEO
戚欌
스l
·u沁shifbF뀨FS/Fg山Passexc햐나i예山Program

Bam! Olly breaks…

Olly가 예외에서 멈췄다.

…in an exception and tells us what to do to pass the exception to the program

그리고 우리에게 이것이 program에서 exception을 pass하기 위해 어떻게 해야 하는지 말한다.

Of course we could now run the program pressing Shift+F9 but I'm sure that you understand this is an annoying thing. Just look how we can deal with it…

물론 우리는 Shift+F9를 눌러 program을 실행한다. 그러나 물론 네가 짜증나는 것을 이해했을 것이라고 생각한다.

BTW, don't forget that you can always click here if you finished reading and want to continue to the next screen

By the way, 잊지 말아라,네가 읽는 것을 다 마치고 next screen을 진행하고 싶을 때 항상 click 하라.

시스템 생성 대체 텍스트: 낀」■뻐．■
F뻐e W8w
Debug더메恥s『르
쌔ㅃ에HelP{That'sit!
Rmn螂구
「囹뾔즈L」
더CpU-m茁nthread
00330051
003300드7
003300드9
날》戚》츱츱a냘》「O
CZe4ee
3RZD29O000e
0000
0000
a냘）r》戚》
勿야aranCe 』〃鱗－
DebugglngOP汝ns Alt緘）
知st衲·出난debugging
取뉩toEX休xer
7
離勵B부TEPTR
RDDBVTEPTR
r노『놀『놀 O('7rr o체「O
DS:tEn＞招,
DS:【EpX],
『노C·『『rr눔｀』1
「札
RL
rㅐ

The exceptions can be handled under options here

That's it

Exceptions은 이 아래 option에서 handle 된다.

이곳이야

Unless when dealing with protectors, leave all these checked

우리가 protector와 거래하지 않는 한 check를 해라.

시스템 생성 대체 텍스트: 目DebLlggingoPb
Commands-Disasm
OnS
-cPu
Regis'efsㅣ
E麟이沁ns
staCk
sel겼Jri砂-Debugㅣ
Ever낚s
Tlace
飾헤粃
-s以
因
1-An＊粃ZIAnalvs枋기
-s眈뻬。-Addlesses-
LL石너UUUU匕rb
EDX008e0000
ESX더0L:10000O
ESP8812自O3C
EBPe012R138
ES100000000
ED100000000
EIP7C90EB94ntd!l.K'f
尸ㅣgnorememo汐acce枋vd輛아繃inKERNEL32
l笙ㅉe鱗as糾OPloglafn】foIl애刪g태ce拗勵s;
「INT3bleaks
FS써始·샀epbfe하치
ES002332b1tOlr
CS001B32bit이f
55002332bit이f
DS002332bLto(f
「S003B32bit7FI
650000HULL
EFL
STO
La$tErr
0000e202
ERR0fLS넋
댜뱁0.NB.m
80e0e00no
CPnH핫LSTDO
여여이여
FMem이yaC이’55.,1야＆bn
F―楸egel바楙IOn야0
F-nvaiid01Plivi텨edin功ucl
FAllFPUexce댜10『．5
e衲p'、一？令7「「FF
--.｀《「FF
이이｀'
白U
FF 凸U
Frleseseskb
Ifyouwant,youco미daddth이ast
ocCuredeXCePtiㅇntothe
"passtotheprogram니istbycliCkinghere·
「-gnoreals。foI―輛ng。ustomexce丙O纛茄輛醇r
'000
.r근1
쨌oe
F이jetr「
-no
rr손C
HㅌnR,驪
AddIast戚閔01始n
A（多dlange
래■
..J
Deleteselection】祗、」 一xl
Butletmeshㅇwyouhㅇwtoaddal-
poSSibleexceptiㅇnsatonce

If you want, you could add the last occurred exception to the "pass to the program" list by clicking here.

만약에 네가 원한다면, 너는 마지막 exception 상황을 여기에서 click하여 "pass to the program" list에 더할 수 있다.

But let me show you how to add all possible exceptions at once

그러나 나는 너에게 가능한 exception을 어떻게 추가하는지 보여준다.

시스템 생성 대체 텍스트: - _■■■■·■
l놈J놉룝■욥'-‘■·｀ㅏ. 졈■．』 一
^一괘．
■■.
미b ■■
·■■·_
훤·－
■■■■■■■■■■■■■■■· --
Corrlmands
seCu,i砂l
-Disasm
Deb'Jgl
CPU
EvenIS
IR
AddingthecomPlete
rang타frㅇmzero
An따s枋3
AddleS零es
'
Flgnolem
Ig凹柏脯a＄ㅇ
隱lN
Fsi·
FM(
Rlnl
^d(lran伊ofexc벱조
Fils。。xc繃癬綴
000D00
L枇texcept沁ninfang비Inc勵ded)
什fff'f「
.....ti∥FFFFFFFF
- 嫩 ㅣ cancel
Ad(llast하（e야刃n
a …
e -
O ㅡ
n -! -
g
F
쁘-Und。-Cance디
■■■

Adding the complete range, from zero

Zero에서 완벽하게 추가했다.

00000000 ~ ffff ffff

….. Till FFFFFFFF

시스템 생성 대체 텍스트: ■.■■■■■．뱃춈여딩■■ㄱ■■■변」■■’』■■■‘■탬．뀁■■변’■·rJ■■■■■·I
Addlesses
ses읽걷I-aj s
－댜m琿es枋媤
目Debug輧ngoptions
COfnmands-DisasmICPu
secu'i砂1Debug1Evenl,
ㅣReg嫩螂sㅣ以ackl
Excep（미：IT『ace
粃니A떼
如헤粃
ㅣs〃
粃ZIAnalv
sl"ngs
녹IlesesesㅓHl-
ㅡ
Fㅣgnorememo汐ac閃ss났괘＆ionsinKERNEL32
Ig凹祗鱗as기OPIO아柳U혀跏hg饌졔出ns:
FINT3嵋毓： 颱
FS너緘삵ePbfeak
F附颱汐。凶eㅎ＂盼故物n
F臟빙“di麻眈놀蝕0
巨-nyaiid01pliv■너出．功以六硼
FAllFPUex閔翩ons
巨-gnorealsofol아納gl＞盤山mexcePtions騈fa띠醜：
:)
呼
..FF"FFFF
Addlaste）媤햐낙刃。
D00
「石「〕Undo1Canc키

Ignore also following custom exceptions or ranges:

또한 조정된 exceptions이나 범위를 무시해라.

So, that will deal with the exceptions except when stepping, see later.

Now, we can run the program normally and study its behaviour. Restart.

그래서, 우리는 stepping 할 때를 제외하고 예외처리 된다. 나중에 보자.

이제, 일반적으로 program을 실행할 수 있다. 그리고 행동을 배우자. 재시작.

*번역 주) 나도 잘 이해가 안됨*

1. **Behaviour of the program**

I told already that I can't emphasize enough the importance from the study of the target.

내가 이미 말했다. 나는 목표물의 공부에서 충분히 중요한 것을 강조할 수 없다.

It can very often give you detailed info on how to start the attack. Good research of the application can drastically reduce the time you spend on it afterwards.

이것은 매우 자주 너에게 어떻게 공격을 시작해야 할지 자세한 정보를 준다. 좋은 application 연구는 네가 나중에 보내야 할 시간을 많이 줄여준다.

So, let's do that together and run the application in Olly.

같이 해보자. Olly에서 application을 실행하자.

Aha, That's nice!

We get a warm welcome here!

However, after a little while …

아하. 좋아!

우리는 따뜻한 인사를 여기에서 받았다.

그러나, 잠시 후...

Huh ???

으잉 ???

시스템 생성 대체 텍스트: … F一一一一一一一겯＝르뜨블므난｝"“뺨r''「＇U
睹血涵柳胸就二
EntryGr。up
(UHf汪GI玖rER〔獵v[R듸灌줬
r겨「肉幅nk沁「。
- [·Uull妙1pU00U4 _ _
…노－-=－닐9C4R38SHELL32.7C9C4R38
跏
V'ewo丙or1Help
因圓嚼嚼
D00000
12R09C
12R130
a0000O
a00000
9OE994ntdtl.K'Fa뜨tsy숫tㅌ여C·t【卜ㅌt
J幻rㅡ胞
？軫건ㅡ태
Dele驢e Plint
■一1．써욉- a
■囊、념”의-츤b
GroupN祈 」除AddGroo쟈eleleGrOUP晩Renl
FaVOrite
;002죤32bLte(FFFFFF「FI
.OOIB32bi零0(FFFFFFFF)
.002332bite(FFFFFF「F)
002프32bLto(FFFFFFFF)
,003B32bit7FFOEO0e(FF「）
.OO00HULL
cali
-脯‘ITalkIHangunl쓰l
騙tErr타騙0f헵하CS－휴E(HQT-FOL】＂寧
a0e202tHO.NB,NE,p,HS.PO,GE,이
니JU7yU7
수Ltt수차
Thls欠한냇얀뻗畛헨쌘rsion이Pixt0PianBI【끄自」죕魯끄
헥QuickS삐ch
-??gFFFFe00OFF0000OOFFOO
-???FFFFO00ee0000e00FF00
-???FFFF0000FF000000FF00
·孚학9FFFF000Oe0e00000FF00
+UHOR"'847e00e00ee88S4BI도
Nalne
Mmmm,that'5someaestheticfeaturewe
dislikesomewhat.PerhapSwecantryㅇut
이』rreversingcapabilitiesandloㅇkwhatit
wㅇulcllool<likeifwepurchasetheprㅇgram?
瘢섬令섬瘢섬瘢섭
ntd【t.7C．키0738
쑈_
,38
:FF
〕eo
SED
「Ce
커판0
rF「
End。fSEH야놀aIn
겨니I
걀찧we

Mmmm, that's some aesthetic feature we dislike somewhat. Perhaps we can try out our reversing capabilities and look what it would look like if we purchase the program?

음, 약간 심미적인 특성은 우리가 좋아하지 않는다. 아마 우리는 reversing 능력으로 도전했다. 그리고 우리가 구매한 program은 어떨까 생각해봐.

시스템 생성 대체 텍스트: 珊．r5 U
U3
- OR
- U4
- 너eeIL
－귀·1ee긔」
殃勵仇
(UNf汪GIS'TFR〔DV[RsION)
ACtion USt 닝
Help
〃－--.-－겨
卜■■■■■■눕미
口回因
Gr。up
O繭야1
圈磻嘔
劃釀
D000O
12n09
12R13
De0Oe
〕0000
9OE99
Call E·Mail
D하ete
Groupl：쩜g繭
「aVOrite
이al미andthis?
Mmm,let'5haveabetterloㅇkinthe
innersoftheapPliCationtoo·..
- - - -+''뱁＾·‘
U7、∥7y、、U7、
tt t t tt ' '
isisanunre中Steredversi0nofPixtoPianB0ok.PIeasere小ste『
QuickSealch
땐헥
瘢섬令섬瘢섬瘢섬
《
》
夕F3
E]
S
뜸紛댜的乙굻柏FF

Olala, and this?

Mmm, let's have a better look in the inners of the application too…

얼라 그리고 이거는?

음, Application 안에서 좀 더 좋게 하자.

:)

시스템 생성 대체 텍스트: 珊粗
C．헤－
回磻
Call E·Ma"
因圓颯
Delete Print
Groupㅏ볍g祗
一 －ㅋ탸AddGrOUPX
」쟈蔿轉艇］
J-갭｀六슬枓개ㄷ『/
긱／---'-－ㅣ…／ 무楓）II
祉J錢凶쎈
Pll굼rplP驪In표무무r)I
V es l iJW냐-ㅡ
a … a -H니-一 눌
rr es LJ esFlll-一、빽
卜一一一一→、
·［。。。.쟝Ctn님겨裙깝O인
U"e伊삵eledvelsiorlvl.07
WeCouldmakesㅇme
otheraestheticglitches...
麻·瘢섬令섭瘢섭瘢섭
.

We could make some other aesthetic glitches …

우리는 약간의 심미적인 작은 문제가 있다

시스템 생성 대체 텍스트: 수驪7 硼描
_ 』··탭■■· 냅■■■■■■b
티즙탸．' ·．次．小
跏回磻因圓隊
E·Mail Dele〔e Print
Group
Call
1볍祈
긔團
AddG『어’X【）eI이e
FaVOrite
Calㅣ-
孔＝＝쑈Pleasere戚Ste「머넜oPjan盼＂k
■I■■콥■겹驪．■」
O
You'vereackdthelimitof4entriesPergrou恪
Pleasere며sterP瀷眈柏r政딤（tO（始y'
겼갼
e -
陶－瘢섬瘢“瘢섭瘢섭

Oops!

웁스!

I had already made 4 entries

나는 이미 4 entries를 만들었다.

시스템 생성 대체 텍스트: 口―
ㅍI汕r- H쓸r
因圓嚼呱
Delete Pfint Find Exit
-L터7군'■ a
-더7蔘－M
'긔듄 b굼rL
:BP.ESP
一l
PLH탭OpLa.
PLHtOOia.
:RX,DUORL)
ERX
l니ORDPTR
:SP,58
EBX
ESI
EDI
LOCnL.'],
미JORDPTR
:DX,EDX
IL.RH
IUORDPTR
:CX,ER×
:CX,OFF
IUORDPTR
:CX.:i:
:CX.EDX
뺨비O효rLPI묘닌
뾔코끄趣
티춈吹난, Gyl:'-
跏回
Add Call
Groupl탭勢 - 」탸AddGfouPx脯eleGrouP心IRe
「aVOrite
CaI
맥碑무re戚ster더았。PianB이傘
After3grㅇups
drrr프7뗀r맥·「eses〔JO『＇’驪．a江lres
H쌘uP.I쑈l
，。se『eiji뇨라l
:Cx
ERX,ERX
;HORTP요xt
1l:
PLㅐ첩。OLa.
:CX
P乙ㅐt。pLa.
ERX.E와＜
;HORTPLㅐt
1L.f
PLㅐt。OL..
:CX
:S1,ESI
■n「01·11-
You'verea巾e배klimitof3gro뱌恪．
p논aser려rter더Xtt덥ar1BOok嫩始y.
00［拓!
_ 겯－、
( 꺼L___』－(-－一―
1 . '':-J ' ' ∼
-_'／ㅋ｝.*^.●
u ∼ㅗee권닐》一＇노γㄱr－·
G
희-
p· 卜
―陶효灌爐湧嘴―勵
0·UnUO엥ea킵ea
n-·Unpsea긷ap什
'br규64612L
4444444·
n3736Fir
R凸OBDC드ㅌ·
n죠飇m·

Oops !

After 3 groups

3groups 후에

Ok. So, this is a good example of a "restricted" program. It restricts the trial to 4 entries and 3 groups.

Ok. 그래서, 이것은 좋은 "제한된" 예제 program 이다. 이것은 4명과 3그룹에서 제한된 trial 이다.

1. **Patching the "Group" restriction**

Let's try to reverse the "crippled" application into the full version.

"불구된" application를 full version으로 reverse 하기 위해 도전하자.

How to do this? I told in previous parts that we could now grab to the string searches and try to find our way like that.

어떻게 하냐? 나는 이미 전 part 에서 이야기 했다. 우리가 문자열 검색으로 잡자. 그리고 우리들만의 방법을 찾다.

Don't … or you will get lost as soon as you are confronted with more difficult stuff.

좀 더 어려운 문제에 직면했을 때 너는 곧바로 잃을 것이다.

There are other ways to do this that also work in i.e. encrypted files !!! (See later).

그곳에는 이것을 할 다른 방법이 있다. 또한 암호화된 file에서 일한다 !!! (나중에 보자).

For example : here we want to know where this messagebox is created and called from.

예를 들어 : 여기 우리는 어디에서 messagebox가 생성되는지, 어디에서 호출되는지 알기를 원한다.

Use this simple trick: pause Olly first…

간단한 trick을 사용하자 : 먼저 Olly를 멈춰라.

시스템 생성 대체 텍스트: P쳤』sed
틔뾔최늬꾀뾔」蠟뾔뾔쫴」」희꾀긔흐1브1의」즈
더CP【j,
17C9eEB94
＂녔inthread,"x》d미entdl·
55:tESP】
55:[E얏》】
55=LESP+8〕
RR R
TT T
PP P
7C兮OEBgC
7CgOEE:gC
7CgOEBRO
7C90EBRI
7C90EBR욘
7C·）OEBg드：
7C90EBR4
7C90EBR드
7C，캬正卜ng
7C·키〕EBCB
7C90EBpC
7―〕이仟bR[I
7C90EBnF
7CgOEBBe
7CgOEBB6
7C90EBBC
7C90EBCZ
7C90EBCS
7CgOESCS
7C90EBCB
7CgOEBDI
7CgOEBD7
7C90EBDD
7C90EE:E3
7C90EBEg
7CgOEBEF
7C90EBFZ
7C90EBFS
7cgeEBFB
7C90ㅌCoi
7CgeEC04
C3
8DR42400e00000
8D6424Oe
90
9e
9e
90
9e
8DS42408
CDZE
C3
드드
SBEC
9C
slECDOOZOeoe
8985DCFDFFFF
898DDSFDFFFF
8B4508
SB4D04
8948OC
8D85ZcFDFFFF
8988BSOeeeeo
8998q400Oeee
899eR80000e0
89BeR000O000
89B89C0000ee
SD4DOC
8988C400000e
SB4Doe
8988B4Oeoe00
SB4DFC
8988C000O000
RETN
LEpESP.D너ORD
LEF놈ESP.DUORD
rloP
HOP
NOP
HOP
99
SS
:rEBP-2241.EP묘
EBP-228],E(>
55졈【EBP+8】
PTR55=tEBP+4】
DS:〔ER묘＋Cl,ECZ
PTR〃尸닙‘="‘。．
USER32.77D7E
USER32.77D2E
USER32.77D7E
Now,pressAlt-Fg
(====retumtouser)
77D7E
iFa힁t
聊轍PTR
·탭」믹」．닙r훨r.r'r노r팀
05:[ERX+C4],ECX
PTR55'tEBP]
DS:［탸강X+B’홍」,EO《
PTR55:tE鮮’-4]
DS:[EF겹X+CO】.ECX
USER32.77D7E
USER32.77D7E
USER32.77D7E
L RR··R·RRRRROR·R·R
R TTRRTRTTTTTRTRTRTH
U P 슭、PPOOPOPPPPPOPOPOP'
U S D U뻐 U U U U C
D E 쟈一000DDDODDDDODDDOD
' P· 요NR''R'RRRRR·R'R'R'
X BP POOXXOX00000XOXOU쵸On
Dㅌ EBDS닒니쀼nHC닒nHI.IW닒U니밋UCUC니맣Cl.l빌丹
E·J EFEOOEEDEDDDDDEDEDㅌD"
HH H
NOPLEP緞PUs驟緇騶騶LEP騶騶hOULEP騶騶뺏
디·……PL$··············……
r빡esesesesesesesesesesse---

Now, press Alt-F9

(==return to user)

이제, Alt-F9 누른다.(==user로 돌아간다)

And notice that Olly promises he will return to user as soon as you let him ;)

그리고 알린다. Olly는 약속을 했다. 그가 곧 user로 갈 때 알려주며 돌아간다.

Remark : if Olly would simply pause again here, then it means this trick fails in that case

주목 : 만약에 Olly는 다시 간단히 멈추면, 이번 case에서 그것은 trick이 실패했다는 것이다.

Hehe, we will let him :)

헤헤, 우리는 알려준다.

Olly kept his promise !!!

He breaks right after ….

(scroll up)

Olly는 그의 약속을 지켰다.

그는 실행 후에 멈췄다.

스크롤 올려봐.

… the messagebox. This little trick works in about 80% of all cases. Of course we could also have used the universal applicable API's (MessageBoxA, etc)

Messagebox. 작은 trick은 80% 정도로 성공된다. 물론 우리는 일반적으로 해당하는 API를 사용할 때 쓸 수 있다.(MessageBoxA, etc)

So, all that is needed now is some backtracking to see where this messagebox was called from. Step F8

그래서, 그것이 필요해졌다. 모든 것은 추적하는 것이다. Messagebox가 어디에서 불러지는지 보기 위해 F8을 눌러

Aha. A command we have not discussed yet.

아하! 아직 의논하지 않았다.

시스템 생성 대체 텍스트: OOH녑맬욥미I
004드6〕IF
004E6광Ze
0더4F':길궁2
00456925
004드6324
00456327
eO4드632R
004드6330
004드639.
004牙터》
뎨14「ㅑ H
.1'ldll …
〔’ - ㄷ
0045633F
eO456341
0e4드6343
00456346
00456349
004드634R
004드634F
0e4563드i
00456353
nn4FRgF7
,J...l
L:
OCOO
EC
RE대O죠
PUSHEBP
ASSㅌMBLERINF○:
畔
e8
RO554700
24드드4700
E
r구r댜rDD062
77.'魯구FF
노콩一SB67FFFBBr구46Fr댜4FFZO8rpr구3'
·CrO8r긍rpFFF8887r걀F87FF5E878F
.
·V
·
·
·
·V
RET(Return)
Syntax:RㅌT
RETdigit
O7
C0
l0
7510
7드OC
DOFFFFFF
Ce
3F
7D1000
RETdoesnothingbutreturnfromapartㅇf
cㅇdethatwasreachedusingaCALL
instrUCtiㅇn.
RETdigitcleansthestackbefㅇreitretur『15.

ASSEMBLER INFO :

RET (Return)

Syntax: RET

|  |  |
| --- | --- |
| RET | Digit |

RET does nothing but return from a part of code that was reached using a CALL instruction. RET digit cleans the stack before it returns.

RET는 아무것도 실행하지 않는다. 그러나 이 부분의 code가 call이 사용됐던 곳으로 돌려준다. 그것을 돌려준 다음에 RET 숫자는 stack을 깨끗이 한다.

So, also step the return to.

그래서, step을 return 한다.

시스템 생성 대체 텍스트: 뎌cPu,颱inthread,飇d미ePi功pi。
겯」 I ’·
> 64:n10O0O0000
6RFF
-sagEF94BOe
rl이）탸媤．아DRDPTRFS:〔0〕
F'l』SH-l
PUSHPLㅐ零卯ka.OO46F995
饗F
ntd1I.7C910드6D
3?
-->Arethere
groupsalready
00 、｀
83R40000
너너
460100ee
ERX
D닒ORD
Indeed,theteXt
fromthemessagebox
TR05:t《各USER32.S聊冠HF륭튱耳룝
》eh．노겨탕엥엥楡q뺨
JLSHOR
R烙H10
슝떼。t。이a.0e4e8B34
P길“t。p{a.ee48F70O
Piㅐt。pLa.OO48F6B4
ECX.EBX
nSC11"P1easereg杜＄terP렁ㅐt。야anBol
nSCll버큰에'vereachedtl난l'hitOf
_PL怜駐畛죙a.eO4562ED
E룝．겨닐
EBr 찍논、
PUSHPUSH刪一P0P
POP騶姻釀於
날어）40슝n
100408R
［菰
100408R
100408R
100408R
100408R
1004eSR
100408R
100408B
100408B
100408B
10p4인SB
曜二
….1'1.1니:ㅑ
15【n56470e
FSe3
2R
l0
0eF74800
B4F64eoe
CB
DOD7O4es
OO40eE요F
.:10·10尸BZ(
00408B2D
00408B33
00408BS4
O04OSB36
00408B3n
OO40eB3F
OO40eB41
00408B45
00408BSe
00408B5드
슭습솥“깁瑤눕드그
BC2434elee00
잽89eoe00ee08
·，몌예p》귄（55·【E驪’+134]
미OROPTRFSN3치ECX
SP.140 、C、｀
Butmoreimportantly:
해8B해68騶FF的7c胡秘688BESSE騶8B64
8!C440018000
C3
> 6Ree
8D4C2424
ESZIEZeleo
6R00
8D4C2424
C784244801000
ES8BSO0200
앤맸「，．겯、r'^/
dㅇyoureCognizethis???
e
ECk
PL
n0U
驛LL
PUSH
0
ECX
OUO
NㅇtiCethatthisWaSthemainCal-
totriggerthemessageboxca∥
Afterthereturrl,weland
에theneXtlineㅇfCㅇdeOfCOUrse
RSCll" H．닐Gr에P''
RSC11"P楡tㅇp'anBOOk''
RSC11"Gr。uDnane"
驪’+3e]
Stack[0012F7901=e04761E8(PIHt。pLa.
ESI竅）04汪．1ㅌ8(Pi님tㅇDLa.004761E8),
4
I
76lE8),R驪［11＂이G"
''OLG"

Now, scroll up to see what was the caller

이제, 스크롤 올려서 caller가 무엇인지 봐.

Notice that this was the main call to trigger the messagebox call

After the return, we land on the next line of code of course

But more importantly : do you recognize this ???

알린다. 이것은 messagebox를 call하기 위한 mail call 이었다.

Return 후에, 우리는 code의 다음 line에 도착했다.

그러나 엄청 중요하다 : 이것을 알아볼 수 있겠어?

Indeed, the text from the messagebox

정말, messagebox에서 나온 text다.

--> Are there 3 groups already ?

--> 이미 3groups 비교한다.

If not, then …

만약에 작다면,

시스템 생성 대체 텍스트: 더cPu,mainthread,飇dule머馳脯。
너너4너谷HU너
0040SnD6
OO40SpD요
> 64:n100000000
6RFF
-5요95F34BO0
『1이．,티媤．DUORDPㅜRFS:〔0〕
PUSH-i
PUSHPLㅐ零。0La.Oa46F99S
X燧HERX
튑DUOROPTRFS:〔e〕,ESP
E아）'134
HEBX
EB닝，ECX
ntd1I.7Cgle드60
3?
-->Arethere
groupsalready
OO408RLF
OO408FIFI
OO40SRF7
00408RF9
0040슝R「E
004이뜨니FF
004이［E:l:l딩
0．媤eD.e
004이크EeR
00408B0C
거더4뎨「쵸1
,1。14너:f:·
U너小1:.f1
밉甄J∥졉미긺펩뱁
00 、｀
83R40000
ee
46010釀蹈
一一― ∼、
Ifnot,then
販珊ㄿ八朋
444444
00內U00乙U
on찬白U00白긴
Indeed,thetext
fromthemessagebox
Plllp노LP
15DO5647ee
FSa3
2R
i0
00F74800
B4F648Oe
CB
D0D70480
霹L「헉
C"PE
ERX
O닐ORD
'ROS:t《各USER32.S羈하恪륭륭茗薛
》eh毓꽝르르〕·〕르
JLSHORT
LㅐtOOLa.ee408BS4
...jumppast
themessagebox
RSC11"P【ea$eregL룔terPLx
RSCll버군。u'v.re술Chedth슨
tㅇpianB。．
ILhitO「
l:l더큭이크EIE
oa극이프EIF
0一各08BaE.
00408B2D
0아408833
00408B34
00408BS6
0040SB3n
00408B3F
OO408B41
00408B45
00408850
0040SB드드
010000
POP
r1聊）
RBnH8eF3Cp88BSES
6866r댜F876668E8긍r규
＇卜890D000000
8!C4400le0e0
C3
6Ree
8D4C2424
ESZIEZeieo
6R00
8D4C2424
C784244801000
Ee8B500200
6Roe /
시DUORD》否
OROPTRFS
55·tESF略134]
A그.EC낭
낟∼ㄴㅍu^J沮盛뇨나t一一一一一一一一一一一一一一
Butmoreimportantly:
SP.140
dㅇyoureCOgnizethis???
J'―久珊
니n·｀ y:0'
L'CP l．ㄴUP
r.lesesweweseeswe‘졈es·쟁we
J
· · · · · · · … …노Z
NㅇtiCethatthisWaSthemainCal-
totriggerthemessageboxcal-
CRLL
PUSH
Aftertheretum'weland
에theneXtlineㅇfCㅇdeOfCㅇUrse
RSC11
RSC11
RSC拓
H．닐Gr에P''
iㅐt。OtanB。。k"
'.GrO니p
nane
+3e그
Junp'$taken
00408B34:P＂뱁tOOia.ee4e8834
anddㅇWhat
15askedl니

...jump past the messagebox

지나간 Messagebox를 jump 한다.

And do what is asked !!!

그리고 무엇을 물었는지 봐라.

시스템 생성 대체 텍스트: bU
'4:89290000000
EC348lO00e
D9
0O
83습4000080
0e
46010釀蹈
→-========스－_닙鷺＝=======＝∼
^SSembleat【》04（》SBOS _
IJmpSH매Tolj4田B겨
一」琿
」
FFi∥嫩hNOPs
-Assembleㅣcance'-
-U
eeN
-l=
11=
it-1
eel=
→S
6
ㄴa$tErrㅌR
0e00a298〔"
'a긴－너a킬
긍TOO
ppDppppp
hhhhhhhh
eeeeeeee
柏TITZ柏T4瑤T6T7
55555555
나나댜UbHUU
00408RDE
00408nE5
00408REB
00408nEC
00408nEE
0040邵긔EF
00488nFI
004ee自F7
0040아졉Fg
00408RFE
*lit4螂HF卜
*:ld4이뜨〔：e딩
．·媤eDOe
004이프EeG
00408BeC
더.-1'4rl:F그l
.1。1미1:1]。
U"4너：.fl
騙볍j聊’1.
0더40；크EIE
0a40:SEIF
00408B26
0·40882D
00408833
00408B:34
00408836
00408B9n
0940883F
00408841
00408B45
0a4088드0
00408B드드
00408857
00408B드C
00408861
Oa408B66
“吾4nRRF.p
《 ,,lI
15DO56470e
FS03
2R
lO
eeF74800
B4F648Oe
CB
DeD7O4eO
8C2434e10000
'89000e0000e
C440010000
rU魯HLHK
nOUDUORDPTRFS:to】'ESP
SUBESP,134
PUSHEBX
戚시EBX.ECX
PUSHESI
PUSHO
戚시ERX,DUORDPTRDS:tE하宅＋n4]
Pt鸞SHI:l
댔르SH1'46
PUSHERX
이LL미j0RDPTRDS:【＜各USER32.S'ndn●＄＄슬gen》］
C"PEn지〕
JLSHORTPLHtㅇpLa.00408B34
PUSH10
PUSHP춈Ht。pLa.e048F7ee
댔JSHP룁ㅐt。p杜a.OO4eF6B4
戚치「CX.EBX
댜괘LLPLㅒt。pL..ee4562ED
POPESI
P아》EBX
臘시ECX.D너아극DPTR55:tESF》＋134]
＂以jDUORDPTRFS:to」.ECk
RDDESP.쵸40
ㅒ크＂
RSC11"P【ease
nSC11버군。u.u.
regi$tetPLx
re毓十손dth.
零p야an오
I。mt냐
EFL
P'Htop'a.004761E8
PLㅐtop(a.ee4761ES
PLHtㅇ이a.oe4드6R드E
ntd【l.7CglO드6D
ee
4C2424
ZIEZO100
00
4C2424
842448ei0000
SBS082ee
e8
RSF648ee
0CF64800
9CF648e0
4C2430
「1「夕더Inn
PUSH.
LEnECX.머袒ROPTR
驪LLPIHt。pLa.oe42
PUSHe
55:tE얏샤24]
6D6e
55:tE얏’+24]
ESP+148].0
낙섬卜
댔꺼叩
－수수수
孔卜O뒤
孔翩OR
꿱卜0尸
눼꺼OR
꿱꺼（m
LEn
『loU
댜LL
PUSH
PUSH
PL烙H
PUSH
LEn
「r뀁I
EO<，미쫠매p
OUORDPTR
PTR
55:t
FST
FCU
0000
827F
COnd
PreC
P쵱ㅐt。Ola.OO42DBEO
ixt。p딩a.0048F'RS
Htop
H鷺00
a.00
a.00
48F68C
RSC11" 『ㅓ·닐Gr이．r.''
RSC11''Pi낚t。p【arlBOㅇ「－
RSCll''6ro너0nahe--
너PPP
EO枓며柏R【》P
Pi닛tnnij-n
TR
n4
F6
SS
9C
딩tE얏’+3e】
夕R「八n
''3B6pBnHenOF3Cp88DpeEB84i히JRDSCHD78CH888DR
SSSL댜6866L큐FS무‘6668EU날58rO8C68E68CE66668F
rllesseweseeses졈weseeswe,.
、
· · ■ · · · · · · · · · · · · · · … …노Z · … … ■ · …
JullpLstak슨n
00488B34=PiH眈pLa.8e408834

I trust it's clear for everybody what is needed here. Let's assemble it

나는 이것이 여기에서 필요해진 모두를 위해 명확하다고 믿는다. Assemble 하자.

So, the JMP will always jump the messagebox and continue doing what we want!

JMP는 항상 meesagebox를 jump하고 우리가 원하는 것을 계속 한다.

Now, let's see what else is needed…

이제, 무엇이 필요한지 봐라.

1. **Patching the "Entries" restriction**

Oh, yeah, we couldn't add a fifth entry

오, 우리는 fifth entry를 추가하지 않았다.

:(

Let's do exactly the same as before to find the messagebox creation : pause Olly first. Press Alt+F9 and click the OK button ….

정확히 전과 같다. Messagebox가 만들어진 곳을 찾기 위해 : 먼저 Olly를 멈추자. Press Alt + F9 와 OK button을 누르자.

시스템 생성 대체 텍스트: ---------－솥－
더cPU,颱inth『ead,飇dule어馳脯d
n04드6〕1E功
O驪추드631C
0045631F
0045B32e
004드6322
00456323
004드6324
004드6327
004드632R
004드6330
00455336
00455338
OO45633n
0045633C
0045633D
004드633F
00456341
00456343
00456346
004드6349
0045634n
OO45634F
Oe455351
004드6353
004드5357
004드635e
004563Sn
嶼）45535F
00456361
00456366
004F6368
0045636n
0045536D
004드6S6F
004드6371
00456373
00455375
00456378
004드637B
004드537C
nn4FR요Rl
0C00
EC
75eC
75es
1드no드드47ee
3D245547e0
F0
F6
2E
D7
C0
i0
7510
75eC
DOFFFFFF
Ce
3F
7D1000
:Ontrol!D
卜．:.1;.」
t뛸各US티국32.G순tD【glt.h>1
05:t（馭略ER32.GetT야엡Lnd
G숩t미9
USER32
Iten
.6etTOOU｀『b니
hParent=009DS324
BetTcpULndO닒
rRr93
l枕92
Igrgl
'PLHt
=ee9D5324
Opla.004563lF
07
OCESFFFF
3l
ZCESFFFF
C0
28
7508
D7
「0
F6
lB
75!0
75OC
gEFFFFFF
[
qr93
nr92
Rrgi=009D5324
PLㅐtOOL술，O04S63lF
· l a a · t t ·t · t t ·
I LU t t · Xn삡 HaH· H IH'J'J '‘닙乃
- 녹·Z rrr nn t'H 잉nH'''J ·t딩衲·‘· ·｀·｀;'·t닙귀·｀'J 딩n츤q·｀졉J뱁乙 Op
· ■■ ｀·7 L닙닢n.C'1 LH··｀의결터F LILHnLIJ LLn1DLㅁnHnL꿸흩 nHL'.r · · aLL
· 〃·｀ ＂너nrLJㄷnr rU.F · · CrF 뼙q C CrF · r' ' 仁U仁U 수첫 ·
- ＇■■ nㄴr드 · · ao컨U 수황 '＇· · 쨍·t맣·수一 ＇쨍■尸O ·＇'쨍·nn.nt'ㅐ닝
- L、 '·맣‘멩·＇■‘＇쵸닙n썅■.r.nt1H닌n.r.qtl"nㅐ.nHLn.n.nt'랗‘컨gbnn"n"仁q·솔‘nH
까 sEb1ESIEsHDREsED태H0R데대ESPi태SHatqRESSHOPISHOPi태sH0데EDEsTEsH0nn任나댜
니r *- 7·尸OH·J7·eOHHUn■JT H ■J ■JT H·JU슨0 SCO츤O·노츤겨
r쌩눼 눙'lseeseseses·．1冶·L卜차L닐.q 尸겹■느컨C 仁g컨g컨C■J컨g쨋J.F츤q,'·LnF·J컨섭''Cq·J．닙rㄷrㄷL닙L닙L닙"rF
EZrOB67FFFSBr04'Frr)4FF68r0rr)36rD8Dp8r0InFFBrD4FF60무
rpCrD85SFFF88875F87FFrOES'fsrD7EEES떻rFF887FFSE
RFnn
■零··……■J…갼··…갼＞·갼·갼＞·갼＞。＞·갼··…
ㅡr■■·■·■■■■■■■■■■
《 'I
Stack【0013EF70〕：009D4D드91009D4D58),nSCll"Dve.
ESI=009DS爻［4

:)

Scroll up

스크롤 올려.

시스템 생성 대체 텍스트: 더cpU.mainthr洲d,飇dule더馳脯a
U‘맣4Fㅏ.EF
004562E7
004드62E9
004드62EB
004드62EC
OO4S62ED
004562FI
004드62F2
004드62F4
OO4552F6
eO4552F8
004562FD
004563ee
004563e2
OO4563e4
004드6306
004드63e8
004드630B
0045630F
004드63!0
004딧〕14
.1니4t'、1【
田祗녑·［휘
.:104드E프1'
004드63lF
004드6320
004드6322
00456329
00456324
004드6슝2-'
.:l〔14드63요R
004드68힛〕
004드6386
01:14드6크광：〕
00456二jㅓ
0045E.33〔
00456〕3D
004드633F
0045齪＝41
O毓홍드684광
nn4FF덕4「
匪시ECX,티拐
J"PSHORTP嫩眈》이a.ee4562Dn
戚시Enk.ESI
P아》ESI
009D4D드S
REV거
廉시ER닝，D너아刃PTR55:tESP+8]
PIHtopLa.8848FC68
1C
24
24
l0
i0
04564700
PUSH
TEST
nOU
JIZ
邙LL
n0U
TEST
·J"Z
kOR
J"P
r10I,I
PI-I·크H
PUSH
PUSㅐ
PL,SH
이LL
HP
REYㅐ
PUSH
n0U
POSH
PUSH
ESI
EnX,EF枕
ESI.E댜＜
SHORTPLㅐtOPLa.O04563Oe
Piㅐ＝。pLa.OO46nEC6
ERX,Dl.ORDPTRDS:【E따＜+10】
ESI,ESI
SHORTPLㅒtopia.00456308
ECX.ECX
SHORTPLxtopia.OO4563OB
EC:<,DUORDPㅜF:DS:〔ESI+IC】
ntd【L.7C91056D
ntdlL.7Cgis드6D
觸
田 4
몌0
1 24 894143
8F6 4 e뱀laOC06egap
C C 4 CF 4F C
ORDPTR55:tESP+leJ
X
ORO
X
ORD
P꽈감55:[ESP+101
Style:hB-OK:Na-ICONHnllD:h〔nPPLhl
Tt'【e=ee00eeel???
T=n수=O00ee010수층층
ho닐ner=7C91056D
ESI
0C
EBP
EBP,ESP
ESI
EDI
PTRDS:t＜各USER32.".''*9●抉ㅄ
ㅣ
綸硼騙애”
몌태며Ec얘
E4 4 r구
47 7 쨈‘
SBEBSB또臼SBS6邵8B花E88B8s花盼EBSBFFseFFSIFFSECZ弱8B恥S7
'＾·＞··＄…갼··＞갼·갼＞>……＄
.．■·■．■Lr■■··■■··■l■■■．· r
Allright.Samestuffhere'
Here15thecreatiㅇnofthemessagebo》．
Let'$seewhereitwascal-ecl.StepFS
[
…：.:．「．t'.:.IID
논．:llr,」
연쁘腹I브n_
UbbK驪＜.bet·OOU나놀。。닐
.F'ar'「．t=009DS324
GetT。pULndㅇ닐
8드CO
.v7410
FF7510
FF7Fn「
ㅜESTEnk,ERX
JESHORTPLㅐtㅇpia.ee4563S3
PUSH[RRG.3]
Pl.gH rpRR'21
St.ck【0012EF7O]=0e9D4D58(00904D58).RSC!I''o、'l3''
ESI:OOgDS324

All right. Same stuff here.

좋아. 이곳은 같은 구성이다.

Here is the creation of the messagebox.

이곳은 messagebox가 만들어진 곳이다.

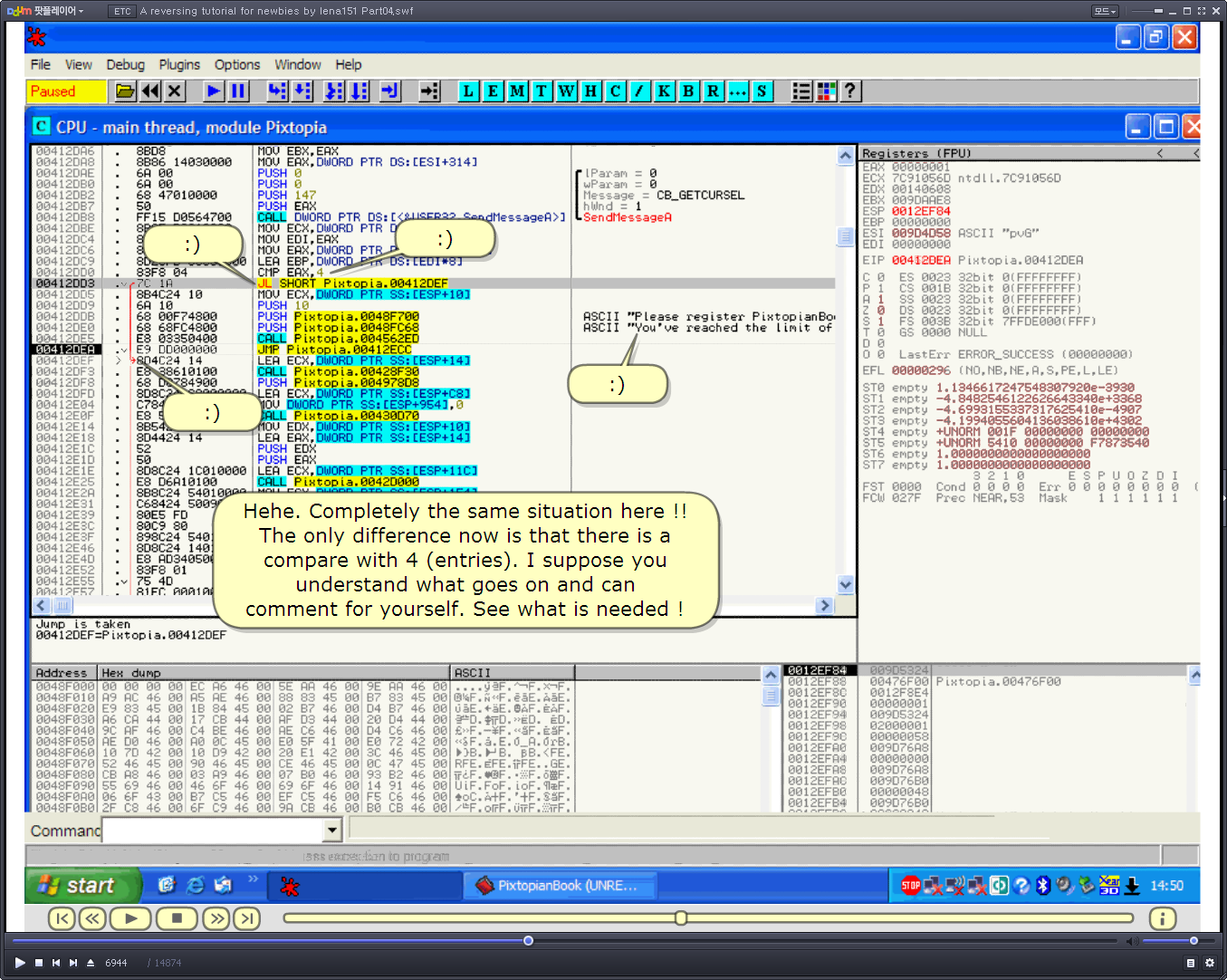
Let's see where it was called. Step F8

어디에서 불러졌는지 F8 눌러보자.

시스템 생성 대체 텍스트: 디cPtj-耐inth隅비爬dule어纖脯a
n더41：》「「p
*:l041之DEFㅗ
0041ZDF3
004!ZDFS
004!ZDFD
004!2E04
0041ZEOF
0041ZE14
0041ZE18
0041ZEiC
0041ZEID
e04!ZE!E
004!2E25
0()4!ZEZR
0041ZE31
004!2E39
004i2E3C
004!ZE3F
00412E46
004!ZE4D
004!ZESZ
004!ZESS
00412E57
004!ZE드D
004!2E64
00412E66
004!ZE6D
004!ZE6E
004!2E73
0驪흥i2E79
004!2ㅌ7B
0041ZE7D
00412E82
004!2E88
004!ZESE
004!ZESF
004!ZEge
0041ZEgl
004!2E93
00412E98
더더4IPFgn
<'ㅐ-
赫ㄲ古菰l
--[-
JP
LE요
。LL
六巴H
LER
廉지
댜LL
戚지
LEn
PUSH
PUSH
LER
댜LL
ㅒ以k
Ptxt。p.a.e0412ECC
ECX.DUORDPTR55:tESP+14]
Piㅐ탭叩'a.OO428F30
PIHr。p〔a.004978D8
ECX.Dl.ORDPTR55:tESF'+C81
미蹈ROPTR55.[ESP+954],.
PiㅐtㅇpLa.ee430D7O
E마＜'DU아랙DPTRSS:tESP+lel
E냐겸，미J하극OPTRSS=【ESP+14]
EDX
ERX
ECX,DUORDPTR55:tESP+1IC그
Piㅐt。。.a.0042D000
-. 〕 ＿… -- -
一날노一一ㅋ
Scr이―uptㅇtakealook
atthesitUationhere....
ntd【L.7C91056D
LE自、
驛LL
CnP
J"Z
딧勵
LEn
廉쟈
姃시
PUSH
댜LL
"OU
PUSH
RDO
댜LL
戚쟈
hOU
Pt炤H
PUSH
PLBH
咸시
驛LL
PUSH
"nU
P(Ht。Ota.OO4662「「
EnX,1
SHORTPixtopL..oe412ER4
ESP.100
EDX.DU여괵DPTR55:tESP+114]
EOqESP
OUOROPTR
EDX
P료ㅒt。pia.
ECX,DIJORD
1
E（》，EBP
PiㅐtㅇOLa.
551「ESP+1101,ESP
Oe428FBO
PTR05:tㅌ51+IBC〕
ER
EC
X,DUORD
畛
PT
40딩eZ
,DIJORDPTR
X
I
X
略
DS
ESI+18C]
ESI+IBC]
d킬rLrL
[
Rr93=eeseee01
qr92=oeeoeeeo
Rrg!:7C9!e56［》
RDC
EEE
ECX,EBX
PLㅐ덕。OLa.0040E490
PIH零叩La.O048FC50
「n낫．「gT
PLHtㅇpLa.004eE490
RSC11"Rne뷰entr,15added."
=P［∥t。p(a.00412ECC

Scroll up to take a look at the situation here…

스크롤 올려서 이 상황을 가져봐.



:)

:)

:)

:)

Hehe. Completely the same situation here !!

헤헤. 완벽히 같은 상황이다. !!

The only difference now is that there is a compare with 4 (entries). I suppose you understand what goes on and can comment for yourself. See what is needed!

오직 다른 것은 4와 비교하는 것이다. 네가 무엇이 동작하고 너에게 comment를 남기는지 이해했을 거라 생각한다. 무엇이 필요한지 봐라.

Right. Now, we will always jump past the messagebox to continue the job.

Save all the changes in the usual way.

맞아. 이제, 우리는 항상 과거의 meessagebox를 jump 하면서 진행 한다.

시스템 생성 대체 텍스트: 더cPU'mainthread,飇d미e어馳pid
LSt솥＇
'｀■．J츱r.'겯굿놈r盼띰r■‘rr
19191白pg白p
CO쇼peapo白p
H70Oea다d다白U
U凸XPPt'''
DBSBSD
EEEEEE
■■■■■■■■■■■■탭탭
ㅡㅡ-
vv－수iㅗ낱nC'
0驪홈12DR8
OO4laDnE
O公41aOBO
O兮412DB2
0a412。B7
0041ZDBS
00412DBE
00412。C4
OO41aOCS
OO4iZDCg
004으ED【：l0
004뱃ZDDS
．뺘1됴뜨［탭5
004版【．．〔9
.:104la〔〔E
01:141ZDEO
0盼41요DE드
0041윱DER
0041ZDEF
00412。F3
0041ZDFS
0041ZDFD
00412E04
004laEeF
004흰ZE14
00412E18
0041aEIC
0041ZEID
0驪홍iZEIE
00412ㅌ2드
0兮41aEZn
0041aㅌ키
004조aE39
0a412E3C
OO412EgF
00412E46
00412E4D
00412E52
0公4쵸ZESS
n야41夕FF7
O8
e6140300e0
00
00
47010e80
15D0564700
SEBcei0O0e
Fe
e4Fg
ZCFD0ee00O00
FS04
1q
4C24!O
lO
OOF74e0O
68FC48e0
033驪나00
DD000000
4C2414
3861e100
087849e0
8C24CSOO0eee
842454e90888
드CDF0leo
드42410
442414
＂이．'
no나
PUSH
PUSH
PUSㅐ
PUSH
댜LL
nOU
蹴지
盼OU
LER
CnP
」nP
ㅒOU
PUSH
PUSH
PUSH
螂뵙L
J"P
LER
驛LL.
PUSH
LEn
炡p
야LL
咸지
LER
더JSH
PUSH
LER
E앉＜,ERK
ERX,OLll0RDPTRDS:tESI+314〕
0
0
147
ERX
D닒ORDPTR
ECX.DUORD
EDI.ERX
EnX.DI탤ORD
EBP.DUORD
ERX,4
DS:t＜各USER32.Sendhe''ageR＞】-
PㅜRDS:tESI+IBCI
-
ntdll.RtlRaiseEㅐc'ptE.n
!Para衿=0
닐Paran=0
제e$$age=CB_GETCURSEL
hUn．」=7CgeEBRC
Sendn·＄$ageR
ntd【I.RtLRa료＄eE님c.pti。n
태논
EcX
4 555555
매--EcsDF6
PTRDS:tECX+EDI톨81
PTRDS:[EDI를8〕
EIP
eii.pln긴aUap
伊PRzSTno
홉H
EC
국－
RScll"Pl.a5Ereg枋terP‘ㅐtop'anBo.
RSC11"VOu'v.rtaCh.dth.【in(tOf
EFL
L．뱀
eo啖
······……v차··…큰＞·
솔｀●｀O'솥｀엥｀솥｀춈멩｀스맣｀
ppDppppp
衲hh【nHnn
eeeee·순e
a긴1234r규67
무■TTTTTT7·
55555555
ntdll.RttRai‘。E닝。’pt쵸。n
8C24ICO!oeoe
D‘습leloe
8C24드4ei0000
84a450090e00
ESFD
Cg80
eC245401000e
SC2414el0e80
RD34O드Oe
FS01
4D
ORTPlㅐt。pta.00412DEF
X,0．여乙PTR55:tㅌ驪눌＋leJ
Backup
C。py
많녑ry
ASSefn비e SPace
Label :
Comment ;
Brealpo「t
H沈traCe
RUrltraC.
FSTe00E
FCU027F
New。nglnhere
GOto
갸lread
F헤owirl以＇np
Ctrl졌女ay'
SB886R胡輜SeFF888B88印83EB輜胡秘卵대E9卽E8盼SDC7태8B卯덧騁SDEe88C6秘8e898DE8的花
Rl「「nnnlnnnn
야LL
戚지E
댜OUB
R∥DC
0RCL
"oUO
LERE
螂LL
CtIPE
J"25
의『RF
쎄
3븐脯汁篩唜纛宖尸篩韶盤聊
X＝갔珊！e56D〔ntdll.7C91056D)
se驪ch拓r
Wemade2changes
atdifferentOffsetS.
R넌re눋renC슨sto
跳탄W
Analy,s
S비e功아l
聊「”汗i
-＾·緇
00
00
laEF；깃「
12EF80
12EFge
·■日‘욉
ee47〔FF
eolZFSE
e0Oeo姃

We made 2 changes at different offsets.

우리는 2가지 변화된 점을 다른 offsets에서 만들었다.

Saving under a different name

다른 이름으로 저장해라.

Load the newly saved application and run it to see what else need fixing :)

새롭게 저장된 application을 load 하고 무엇을 바꿔야 하는지 보기 위해 실행하라.

1. **Some aesthetical patches**

시스템 생성 대체 텍스트: EBP,ESP
一1
Piㅐ탭OpL.
Piㅒt。pia
ERX,DUORL》
ERX
7팀』군첵콘밍.·■｀콘훨
l r=fl f下rZ71 떱르1 놀 rrr죠외L一rF一Fl rl힌잿긷
There15arelatiVelybigchancethis15inthe
RD。r×ㄴ
OPBS
USEE
OE
n J翩
e 、져
勵 s
dataOFresㅇUrCeSSeCtiㅇnandCar1'tbefㅇUnd
inthecodesectio『1.Let'simmediatelyskip
searchingstringsinCod윅butIookforthisin
thememㅇrymㅇd미e·BTW,O∥ysearches
onlyincodesectiㅇnforstrings.ㅜhi$15alsㅇ
why1adVisedyㅇuthellAnalyseThiSI"Plugin
inPartZ(oredit이ly'sㅇptio『155ㅇthatyㅇucan
alsㅇsearchtheseseCtions).(Gㅇtㅇthat
secti아、nrst,rightcliCkinCPUWindowand
analyse)
xit
臘
Up
Ln1PCS·
S EEr
쵸
효
쵸
- - - l - l 걋꺽
noapnO88n따aodoaO。p
6rO64612rO66
4444444444
麗的B7D3C6또El拓Be6F
EseFE:e오：El7후
■■■■■

Mmmm, see this?

이게 보여?

There is a relatively big chance this is in the data or resources section and can't be found in the code section.

그것은 data와 resource section에서 비교적 큰 change다. 그리고 우리는 code section에서 찾지 못했다.

Let's immediately skip searching strings in code, but look for this in the memory module.

즉시 code에서 searching strings을 skip 한다. 그러나 이것을 위한 memory module을 봐라.

BTW, Olly searches only in code section for strings. This is also why i advised you the "Analyze This" plugin in Part2 (or edit Olly's options so that you can also search these sections).

By the way, Olly는 strings을 위해 code section에서 찾는다. 이것은 내가 Part 2에서 너에게 충고했던 "Analyze This" plugin이다.(또는 Olly's option을 수정해. 그래서 너는 these section을 찾을 수 있다.)

(Go to that section first, rightclick in CPU window and analyze)

(먼저 section의 처음으로 가서, CPU window 에서 오른쪽 클릭하고 분석해라)

시스템 생성 대체 텍스트: Running
뾔뾔씌의꾀蛔쫴多ㅗ흰
‘딩】
回표］매
Enterbinary
ngtose。rchfor
詠叩긔
EBP
EBP.ES
솨毓
L＄첩ers
戚oIUNICODE
-
ECX
EDk
EBX
ESP
EBP
ESI
EDI
ee.e6o여
eeF400며
7CgeEB)
ee00eo어
e012F78(
e012F8혀
e00000여
80e000이
·ㅗ·｀'딩凸
0044036F
OO44e371
00440373
0044e378
OO44037D
00440383
0044〔）384
oa닐숌섬狙
SBㅌC
sn「「
68B00448鱗〕
'8'O鮮枓4.B
64요R10aaOBBee
Se
'4:8925SBBB88
PUSH一
PUSHP
R炤HP
庶지ER
PUSHE
庶p야‘
HE×+00
YㅇUCanaSWellsearChin
UniCodeaSinASCllasinHEX.
Let'5tryour-uckinuniCodefirst....
EIP7C90EB잇
.:l며．'.=’ㄷ
004403R4
004403「16
004403RC
004403B2
0044e3B5
OO44e3B7
OO44e3BD
004403C0
e04403C5
e04403C7
釀）4403CC
004403CD
004403CF
e044O3Di
0044e3D3
004403D8
004403D9
004403DE
0〔）4403E0
004403E2
0044e3E4
OO44O3Eg
004403ER
여n44n요「「
CS ESOOZ돈
Pi CS00n
E
이:I∥
81E효FF
89eoRg
CIEI08
e3CR
89eo댜추
CIES10
n3自agE
'Pel
E87自33
59
85C.
75e8
'nlC
ESC3OO
5'
ESCE各＇
85CB
75BS
sn!e
ESBZOO
59
33F'
R97F「n
Rddre츨츨15죙큘e
죠」닙」
「兩ㄱcance't
RCCe츌츌
Vㅡ
RRRRRRRRPRRRRRRF:RRRRRRRRR
e10000e0OeleeO
02000000001000
11E00000001000
!IFOOe00e쵸1000
130000e000300e
14Oeoeoe.6eaoe
IR1000e00tOO00
IB4OeO00001000
IBB000Oe003000
24000000006000
2드000000003000
00021
뉴障‘『’
잿E亡Fr/
Ft
Pr
Pr
冬t슬Okㅇ「"aLnthr슨츱d Pr
"a
Pr
Pr
Pt
Pr
Pr
"a
ha
"a
ha
"a
Pr
Pt
Pr
Pr
Pr
".
Pr
"a
Pt
"a
i!04
l!04
F*IV
RU 톤
RU Gua戱늦d
R닒 Gua戱늦d
R
RU
RU
RU …
R니
R"I …
Rbj
B
R '
R
R
RUE
RUE
R닒 l
RU
R· -
R
R닒
R
RU
R
244444422勺드20aO44424242
ea킹eeeeeo길白킵ee44d긴Opea킹eaoee
eeeeedO0ap白pee000OpeodOOee
츨■춈맬홈뱀홑뱁춈．홑．홑.'．■춈
一一一一一一一一一一一
.．춈뱀‘．흽뱀‘·■룔·■‘··욥‘■춈뱀홉．홑·‘··룔·■욥
4442222242424
刪刪喊刪eee吸慨0ee刪0Oe刪刪刪
VVVV VVVVV VVVVV V V
·‘'t'、‘p·‘'l·｀＇쵱‘poppp''11·멩·lp''p·｀D
柵縕漑鄒刪一
22233333333
12F33
3900Oe
3R0000
3B0000
」■■■．1
.0016000
0003D()00
ee84쵸釀衲
00e08000
000OIOaO
00001000
00801000
0e80!鹹珀
e000B000
eoe03aoe
000e4000
00002000
00003000
00002000
n킵仕킹dUn탭a밍a따aon긷apenUO길O띵eaod킵eno·apn킵eeeno
餞킵ap白Oe麴p·ea딩ap白pdDap·e·eeaOg仕Ue白OodoaO
V l 》 '
· · · · … … 。 · … …횔Z … …노Z ·
탑■■■■■■■■■■■■■■■
1ㄴ■■■■■■■■■■■■■■■
「’'닛r.｀『、i令_:『lr．빼ㅓu1.「n'l'.

You can as well search in Unicode as in ASCII as in HEX.

Let's try our luck in unicode first…

너는 ASCII, HEX, Unicode를 찾을 수 있다.

우리의 운을 믿고 unicode 먼저 찾자.

INFO : ASCII :

Stands for the American Standard Code for Information Interchange, pronounced as "ask-ee".

정보 교환에 사용되기 위해 미국에서 만든 표준 code다. "아스키" 라고 불린다.

ASCII is a way of defining a set of characters which can be displayed by a computer on a screen, as well as some control characters which have special functions.

ASCII는 character set을 정의한 방법. 그것은 컴퓨터의 screen 이나, 제어 character를 보여줄 때, 특별한 function을 가지는 것을 보여준다.

INFO : Unicode :

Fundamentally, computers just deal with numbers. They store letters and other characters by assigning a number for each one. The Unicode Standard provides a unique number for every character, no matter what the platform, no matter what the program, no matter what the language.

기본적으로, computer는 숫자를 처리한다. 그들은 할당된 숫자에 의해 각각 letters와 다른 character를 저장한다. Unicode Standard는 모든 character를 위해 유일한 number를 제공한다. 어떤 platform 이든지 문제 없다. 어떤 program이든지 상관없다, 어떤 language든지 상관없다.

시스템 생성 대체 텍스트: 004403BD
OO44e3CO
004403C드
004483C7
004403CC
004403CD
004403CF
O044e3DI
004403D3
OO44e3DS
00440SD9
004403DE
00440SEe
0()4403E2
0044e3E4
004403E9
OO44e3ER
nn44n숙F「
0ei30000
eei400Oe
eoiR10Oe
.01B400e
eolBBOOe
.0240000
1:10003000
00e68令＇-
"ap 01:1041002 R
000
00e
INF○:
HEX
YouknowbynowwhatHEXmeans,right?
Ifnot,yㅇusho미ddefinatelygoogleforsome
moreirlformatiㅇnlInthisspecificcas티it's
theopcodesthatthecomputerunderstands.
ThㅇSeareheXadeCimalnotatiㅇns.
劫蔘－'/＇…‘「苾赫r껑‘
클脇 /// 낍v넣狐指離 뿌
·1..''j긔jl·긔．·｀■ eaoaonD
00乙UoeOOdpdp^Usapeedoapaoap
秘屹盼盼盼ee的腑騁e6卵eeee騁盼騁ee
柵柵縕漑漑柵溫
2222333333a규333
ee·aoa·dpenpopeeeaodO
eno·e·e仕OaOg仕컁eaO0aO
’꿎1硼휸刪EZFS翰翩
-sq·7 eB쨈‘C C·e뱀‘B 'F
-ㅌ C C F7
허Pa6PES臼邵7S胡EssgE88S花얘Essg貂斛
·……갼…＞·六…＞·
걋찧
12F39
003B0000
《
p'Htㅇ
a그SCe48Ce48COp4^
CCCDDDDEEEEFFL
FFFFFFFFFFFFFP
FFFFFFFFFFFFF·
2222222222222(
00000eO000Oa킵0^
00色pa긷dp00000aUO0(
^ 르
Heㅒ벼Jn
쵸춈E.
슬쵸F.
손D.
흐춈F.
f馹姃卽r
^lr·O沁"
0048F「꽈드
004흰.-l·
0「 …,:
OU댜UㅑU櫛너
0048F040
OO48FOSe
0048F06e
OO48Fe70
0048F0Se
0048F090
0048F0p0
0048FeB0
嶼｀F.竇“「．츤
05E.＋눙E.·
루魯D.흙「D.''
요，,F.一驪F。
“용F.욜．E.LR.drs.
*)B.PB.pB.(FE.
RFE.蠟FE．름옭FE..GE.
臘：轢纘纘'
鱗轢씨緻癬기
Oeo仕긴n킵oe000OO
eedO0eapedoaononoe
656462r댜r긍6666
444444444444
m的r며c6724647B29lC6CB
冗B7D4泌D4Ee沈eC9314円몌
騁開朋帥eeeese騁卵盼Beee
'564'뱁‘Zr댜6666
444444444444
옛汕B7閔C6SFEI拓Be6FCSCB
E효jrFE00E79Fn
r큐80rICIEZC·6E9
a딩白p0IU000e仕OnDaps
a턍心pnp'p쇼Un따쇼p仁peseao
6'r구46r긍2rO666'
444444444444
鱗麗S4C88EecD946貯6FCSCg
CU)B74eee367F
ECHllCCHigaO4B6
O08aO08eeO8eo
eeeeoeeeeeedo
觸46貂4446拓42貂4646柏46
ee麗SSmRFD67D拓舵696FC8
盼貯E9飇9C姃柏덧CB騶B62F

INFO : HEX

You know by now what HEX means, right?

여기에서 말하는 HEX의 뜻을 알지? 그렇지?

If not, you should definitely google for some more information! In this specific case, it's the opcodes that the computer understands. Those are hexadecimal notations.

만약에 모른다면 분명히 좀더 많은 정보를 google 해라. 이런 특정한 경우에, opcode는 computer가 이해한다. 그것들은 16진수로 표기되었다.

시스템 생성 대체 텍스트: ，틔l뾔크희츠희
．탭탭■긔■■【T』．탭■■·차새■驪■■탭■·『』■-：익■■즘，■「‘＇탬「＇맥
르희」뾔」희
nX》dulepi
EnterbinaryStringtosearchfor
"OUEBP.ES
PUSH一1
PUSHPLㅒ탭O
PUSHPLㅐto
廉시ERX,DU
PLtSHERX
i꿸t슬r휴
UNICODE
n000e8
0·0
800
D이： 밌RD
R 'Vn'1쨍ㅗCO
OPBSDOU
니맣SEEELD
OE rL
HHH
UBSSS
閔SUPUPUPU
HE×尸2匯『驪驪乙〔驪〔商
I''pp뗀.pZ꿸
164BBZEI더더?6
7200'500
'5
'5
72
72
67
'5
'H＇、UU닐옵Ua
EQ《oeF4Oe
EDX7C98EB
ES><.80000
ESPes12F7
EBPe012F8
ES!e000eo
EDI000000
EIP7C90EB
크247ee
Ce ESOO
PI CS00
FEn盼ebk(k
「Casesensitive
죠」‘」
「記ㄱcanc시
뗀E
攫勳
■■■·■‘ ｀■■■■■■날-
RCO．별별
니we
텄Rt댔RRtRtRt댔Rt댔RRRR
StaokOr"ainthr솥魯d
，■．．··■믹·탭띱·탭今 ■■딥 ■■밉
RRRRRRRRR
2드O00e
26000e
2800e0
ZC0000
3100ee
3200Oe
33000e
34000e
3드0000
3600ee
370aee
38000e
39000e
3nO00e
3BO00e
F‘·힁딨00021004
PtiV0002lee4
PrLv驪떵21!04
Pr1v0002!184
"aD 0004!eeZ
Priv00021004
Pr1v00021ee4
PrLVe0OZle04
PriV00021084
Pr1V0002le04
"aD 0004!004
"ap 0004'eeZ
"ap 000410e2
"ap 00041002
"ap 0004leeZ
PrLV00021040
Pr1V00021040
Pr쵸VO0021004
PrtV0002!004
PrLV00021ee4
hap OOe4leeZ
PrLv0002lee4
hap 00041082
Pr1V00021004
"ao 0004!e02
RIIl
RU
RU Gu蠟戱늦d
R닒 Guaㅍ늦d
R
RU
RU
RU
RU
RU
RU
R
R
R
R
R너E
RIJE
RkI
RU
RU
R
R'I
R
RU
R
硼觸螂觸螂觸騁開에凶觸Oe的ee舵觸馝Oe觸Oe開醜觸硼朋
SOOlap6inU0eol34O0n킬aonU仕Uee000
O쵸p白pap白paonO00白OnUnpe6aponU8e仕peeo쵸OaO
盼e0盼卵盼eees卵eO盼Oe卵00騁00醱00ee00eoee腑에騁애
nU色Uapd타伋팅ea컁dpa'e
n디乙U櫓UdU鐄깊Dpa킹白U松paU
n길a긴dUnon깊白pnoapapap
n길apEFO白p｀ㅗ4Bap
121134nBB4
白Uaoil'11ㅓㅗi솔‘2
eapnonpen따dpa긷apnononpeapn따apnonO·eeap白OapnO
OdoaUeapaU0apoape白paoaoaO0aoa000OeeoaO白O
》
----．…－-．눕．

:)

시스템 생성 대체 텍스트: 프Dump-어났。跡驃。祗rc0049【）（》（》（》．。004匹snH=
圓厦風
^…
R.gL를ter$
E뎨〔00000〔l〔
ECyOOF400〔
eseeo匿
e012F7E
eoiZFeE
e00000E
e00e00E
U凸U八PF'II
DBSBSD
EEEEEE
涵희－‘午蠶嘴화一4「汶쐐－49
:i：諛魔새d，。r．。S。a。。a。。。n
5.1.O.H.).....
····……P.L.
t.。．0.L.a.n.B.
111-I"I·너－a뷩
-Ulrll自｀白U
nUq'dpnLJ
즙J心습np凸U
腑觸醜腑
444E애eO
apea길e
白Oeoe
004E4C5
004E4C6
004ㄷ닉bㄷ
004E4BF
004E4C0
004E4
004E4
e04E4
004E4
引욕나驪U덕聊u札l」치닭L
Ok.Fㅇund
ㅇ．o.k.우．R.e.a.d.
,.....··........
EIP7CgeEB드
00슭1．溜ll
0櫓U自·n겸탬．
004E4C76
e04E4C
004E4C
:：섯『rr노1:i: ■＿___.. .
,''P"r'으’9'r'·” ［요요므뜨쑈르드헵뜨
象t:t：緘：읫r：公 ■■■■■■
CO ES
Pl CS
첵｀ -_趨츰
짓'－∼珊트
^ 【 V·
낙댔櫻끝닐尸飡櫻欌肉惻汾脚R嘴洲肉댔澈澈嘴>
444422220白O
dU습Uapdoe。긴nUe44
nUnO000。긴noeonO
A乙224444422
"W"“。pppp·＂lv
功盼PrPr曲胸h．內內Pr라
nn·I나t·｀
·a.r.o.·ㄴ·＂
n yb솥＇pn
Orpn·｀p요
'eo·U츱·｀
룔bCtC닙 →또
rn h4e昌
eUdgthn
역織6Dee柵6E8e쌔74eO69ee
匯Les泌卵舵湘卵騁卵盼騁盼
난샌F-Inr너·心一가、깁－匕넋」『즌砥「
eo6FOe67ee72
eo66Oe6F0072
886E00ZC00Ze
006F006EeeZe
eo72Oe200061
007e0079oe72
ee41Oe62se6F
oe69Oe7400Ze
0070Oe7eoe6c
墟貂4F卵卵花鬱엾枋726E6F“邵6F얘騙
O0騁에卵觸ee觸OOee盼ee盼ee朋脯朋閔에ee
E'J心70eFBnp仕p4e9932341o
4ㄷ구40e66e仕04뺑r667667r구2
祇驪더een·l넌eeapoaoeeesaO0aoeaOO
副겡nUIU■l-lnoenO。Oaodoeaoaoapnoenoaoe
驪販開觸746Feeee3F2e2e7472印2e68카
004E4D061680065
驪뱁4E쨋旺峰＼《抑－釀二蝴l
殮Clo盼騁開腑腑開閔閔腑開舵腑開閔開嵋腑
SFgnO89D솥‘r댜r댜4748
767aoaO7rO66떻r6676
004E4Cn6
004E4CB6
OO4E4CC6
004E4CD6
OO4E4CE6
OO4E4CF6
Op74釀ㅣO묶呱］驪「O聊O트⑦聊且D④聊琢―上釀
144e9C0
14408CC
따4e3C7
1440돈：lI
I44e3CD
뺘403CF
14403Di
144e3D3
녘403D8
14403D9
따403DE
14403Ee
14403E2
14403E4
14403E9
144eSER
I44n슉「「
R또놉E’펩80
01 180
纛겸33예00
.00
ZSaaeO
ZC000e
310Oae
32000e
Ce
08
lC
C3O
00330000
e034000O
0e3드O00e
oe83DOOe
00041000
eee0600e
00001000
00001000
0e00lO00
0000!000
ㅌ
RRRRRR
一PEcO出
CEZF
C0
e8
l0
B200
요q7F「「
;P=0012F830
oe3600aeoeeeBOOe
803700Oeoe8O30Oe
0e380000ee004000
e039000000002000
oe3pOO00000e3000
003B000000802000
003CO00000803000
oe400O00000el0O0
00401Oe0oee7400e
00475000008lF겹000
0048FOO0eoe0E000
004900000004CO00
004「Ooeel00006000
《
ROCe룝를
RU
R뻐
RU
RU
R
R
R
R
R닒E
RkjE
Rbj
...the
Seeit
make
露e"'>
reSOUrceSSeCtiorl.Let'S
inthedumpwindowand
thenecessarychanges.
·t．甘t
.rdata
.data
·r룝rC
pㅇrtj즐tXOOrt륭
data군「
re룔에rCe룝
Iha90!0el002
lh.g0lO010e2
IhageloeloeZ
I"ag01001e02
Ihagei0010eZ
"aO O啖｝4[020
3p895r0CI898r0r구nH893
n6ES87ZOErDE876ErO3
·…■J…＞·갼…＞
..．·Pi' ,H^극．.1'「”뱀눕.,

Ok. Found in …

… the resources section. Let's see it in the dump window and make the necessary changes.

Ok. 찾았다.

Resource section. Dump window와 변화가 필요한 것을 수정해.

역자 주) resource 범위가 49D000 부터 시작해서 size가 4C000다. 즉, 49D000 ~ 4E9000 까지다. 현재 unregistered version을 찾은 주소가 4E4BE6 이므로 resource 범위에 포함된다.

시스템 생성 대체 텍스트: 딤·EDID
' ·R 、R
XXOXO
l:1044e궁Pb
0044寸：:P'-
0044嫩＜E.
"04411::tE'.
,I't44「-:E
긔044〔正…E
El｝ㅗ4e프E〔
UO죡40슬LS
ee4483C7
004403CC
00수泌3CD
OO44O3CF
0044e3o!
004403D3
OO44e3D3
004403D9
00440．〕DE
004403Ee
OO4403E2
004403E4
0044e3E9
004403ER
nn44n究「n
<빼
bH Ul
ES7R330eO0
59
85Ce
7508
'niC
ESC30000OO
59
ESCE2F0000
85Ce
75es
6Rle
ESBZ000O00
S9
33F6
요q7F「n
R"DEC
嫩지DU
SHLEC
RDDEC
ㅒ以룔DU
SHREn
廉쟈DU
P(JSHI
댜LLP
POPEC
X.OF=
ORDp
ㅌuhm...whatdㅇyㅇu
Wantittㅇ
abㅇUtthe
say?Hㅇw
f이lㅇWing
Lㅐto
><
ASD-
uNIc0DE眈瞰REGI“매EDuERsl恥IJ一一一
…
··9
?r구3
44r구
…
…
..52..4드
..펠5..52
..'5..52
E4'
펠55
…
…
rJ3·
rjrJZ
8·e
··0
8、펠-
2펠·!
TESTERX,E냐省
J裙SHORTPixt。pL..004403L】
PUSHI-:
驛룁LPIH첩。OLa.OO44O49B
P아》ECX
댜LLPiㅒt。pLa.e04433nC
TESTERX.E야＜
JHZSHORTPLㅒt。pL..0e4403E
PUSH10
여LLPiㅐt。pLa·0e44049B
P아》ECX
넜RESI,ESI
"nUrln「aI·11.F르T
HEX＋開
V V ·
· · · · · · … …노Z … …노Z ·
■■■■■■■·■．.．·■■■
- ■■■■■므．를＇＇흽■．■■■
ㅋ「功rTr쿳
巨Kee따눈e
P［거h'Dta. lo．中』:'Fr.tn,「
觸騁舵嵋盼옛
체
r…'·
뻐··솥卄O
a길Ooeeed긷
藕U·l.InDnoeaUap
=：·r콥8e924
ㄷ·1맥e·646
馝：i:esee騁騁騁
49孔閔觸騶6E61
긺닌·JO00a뱁ap
凸l·l.IOIU00더l
7、·너a?apDlrp
ㅓ낙-．·卜分‘OOzprO
畔맺凶蹄盼卯卵
朽444E韶e86952
0·O白paoeap
·견·IJ趨p內쌥肉뱁凸p
도部4F舵騁柏貂
盼·盼盼卵卵盼
ES욜90습빕FB
4='l4乙긴06'b
e·너e솔U自－슭·白찬
··UO－너000
瞞礪앗舵騁746F
ee函：邯油盼［l00o
-티·41'乙p08F
功-U'lU')-U白09''L.
Rddre슝S
004E4卜醜
004E4BF6
004E4C06
OO4E4C16
O04E4Ca6
004E4CS6
004E’홍C46
HeXdUn
-OKlc紬
[.U.l넌．F;.E.
T.E.R.E.D.
.1.5.
.뱃）.E.
R.5.1
궁．우
.0.꺼．)..
눕'··J.··
·.··…P
t.。．p.토...n.B.
0.k.'.R.츨．a.d.
ZFFCC
ZFFDe
ZFFD4
ZFFDS
ZFFDC
2「FEO
FFFFF
7FFD(
000鱗
00i2F
8516F
「「「FF

Hum … what do you want it to say? How about the following ?

무엇을 원하는지 찾았어? 따라가니 어때?

Understand that these changes were only made in memory. Now, we still have to save these changes to file.

메모리에서 바뀐 점들을 이해하기 바란다. 이제, 우리는 바뀐 점을 file로 저장해야 한다.

:)

So far, all good I hope :)

But there is more work to be done.

Load newly saved application and run till you drop ….

지금까지 좋았다고 생각한다.

그러나 많은 것을 더 해야 한다.

새로 저장된 application을 저장하고 drop할 때까지 실행하라.

시스템 생성 대체 텍스트: ============================ ∼→=＝극一一一一一＝一、－一
더났。PianBOOkRe섧sterellversi。n
EntryGroupACb。nLls,뇨W야山。n
Fi뇬
Help
國回楓鷗圓嚼呱
Aㅃ
CaII
r衙獅
E'Mail
D히e
Pri앉
Find
Exit
jGroup
ㅌuhm,
曰F견坐。嘲Ren
Favorite
「一－－一－一一 一Dia'ITalkIH씨빼
S비t
·＇,．■
Q여ck5earch
a 놀
C ■ 、꺼
r-
Name
...her텨(RemㅇveclfrㅇmmoVieforSize).
蠱섬驪섭驪섭슭섬驪섭
\
■■■■■■■■■■

...here. (Removed from movie for size).

Euhm, …. LOL

여기 (movie를 위해 삭제됐다)

Remember ??

Right ! Let's go for this one too ….

기억해?

올바르게! 이것을 위해 하자.

:)

Same recipe !!!

같은 방법 !!!

And once more found in …

:)

...the resources section.

한 번 더 resources section에서 찾았다.

INFO:

There are more advanced ways to achieve the same but we will discuss these in later Parts in this series.

같은 걸 달성하기 위해 진보적인 방법들이 많다. 그러나 우리는 이 series에서 나중에 의논할 것이다.

Common rule: use strings only as confirmation of the searched on your path, not as the main means of finding stuff!

공통 rule: 경로를 검색에서 확인하고, 찾는 주요 수단이 없을 때, strings를 사용한다.

!

:)

So, this is what the application could look like when buying. :)

그래서, 이 application은 우리가 구입했을 때와 같이 보여준다.

Well, it's again the same, right?

Save the changes, start the new saved application and run it till you land …

… here. (Again removed from movie to reduce its size)

같은 방법을 다시 해봐, 그렇지?

바뀐 것을 저장하고, 새로 저장된 application을 시작하고 여기를 도착할 때까지 실행하라.

Now, do you remember this and how it changes after a short while ? Look …

잠시 동안 어떻게 바뀐 건지 기억해? 봐 …

시스템 생성 대체 텍스트: 늬꾀늬」
刪離
Emerbinarystringto刪rchfor
늬劉최
괘뱁·．·．--
쵸1
PUSㅐEBP
＂아』EBP,ES
PUSH-l
ASCI- 「a「I「콰n떼
Lt청솥r일
1800 1PUSH
1480 1PUSH
UNICODE
0000090
匯IV
PUSH
戚IU
SUB
PUSH
PIJSH
PIJSH
麟OV
댜LL
■■■■■■■
蠱寒■［닒
PIHtO
PLHtO
ERY,DU
ERk
DUORD
ESP.띵〕
ESX
ESI
EDI
[LOCnL
D닒ORD
HEX＋沁 l ［』Rn97
7732더616E2더?5
Fl기 77드CR드7
ECX8ea00C7
ED><e00e000
E마《e000000
ESPe0i2P09
EBP0ei2R13
ES!oe000OO
EDI00e0000
EIP7CgeEBg
24700
巨Ent盼敬乙k
Rddr숱룔릉
眄표硼拓
＂녑pl「츤 .'K
一一」뜨一」 · UaseSensl《k탭
·탭 겨〕
죠」」」
「祈그Cance.ㅣ
CO ESO02
Pe CS00i
I하 r팀 r'r' r노r一-.
ROOe륭S
＊트 V、
·欌댔댔R戱댔戱댔댔RRRR있있RIRI댔R댔R댔RRI
EE
니네니빙니밀닒 니맞m냐m빚너쀼니밍 U닒니빙UU따 U맣 니쀼 니따
RRRRRRRRRRRRRRRRRRRRRRRRR
20000
鷺t쟈Okㅇr"a【nthr슨ad
n킵enUnUnUn찝白pn킹d띱a킹nUn킵d띵nUnpd킵a긴aUn힙nUn찝nUa킵d긴aU
欄lee擺F0O鄒鄒擺leO68O漂槌溫甥鄒300
oeaole42npaoe1340e松pnodonUea.aoe白OnU
仕킵enpdo仕p쵸p白p白Uoaoeapee白On띱凸O白pap仕pe白poao白O
odpap00np白O白긴00enpeaO00凸p白p00aO00np凸O
oaU凸Ooaoa따aoaUOap仕Osa컁eo白pedp白OeapaO0a긴ao
一一一一脈一一
11349B
nl-''뱁‘뱁‘뱀‘ㅓ‘
nll,1-IUeeen킵
肉－더－UesaO白딩
e024
002드0000
00260000
280000
ZCO0eo
310000
320000
330000
340000
3드000e
0000
0000
3800Oe
39000e
3슴000e
3BOO00
3C0000
Pri딨00021004
PriV00021004
PrLVe釀뇨21!04
Pr1u00021le4
".p 0004leeZ
Pr(v00021004
Pr1V000210e4
PrtV00021004
PriVaOO210e4
"ap e0041004
"aD 00041002
"ap 00041002
"ap 000410e2
"ap 00041002
Pr1v0002le48
PrLV00021040
Pr1V00021004
PrLu00021004
Pr1V00021004
hap 0004ieeZ
PriV00e210e4
＂술p 0004iee2
PrLV000210e4
hap 00041002
PrLv00021004
noenoa따apdodO8enpnpapdDn
oeea긷ap仕OeOO08aoe쵸Oq
땝쵭썹뱀

Let's go get it. Let's find this one in two ways, use whichever you prefer …

얻으러 가자. 이것을 찾는 것에는 2가지 방법이 있다. 먼저 사용했다.

시스템 생성 대체 텍스트: 더DumP-어xtoPi。：．曲功어껴8F毓m..oo49cFFF
口回因
낍驪絡認r聊驢g^
。fPixt。pi聊炚pk
Ptea'eregi't.
rt。dag슝....ClnL
EIP7CgeE鱗
CO ES002
PO CSO이
tDLat。gBar.
nCCe룔별
OrhULe닐·
.CLe「
.NOte
.Enai
7eBrOg'-
626666'
r콥EF4Erp·
/D667ZO6-
松6F6F紛49饉
E92939-
664'44·
rO3E7eo-
、·76'e仕Dl
口U21'roee-
히乙7ZO60dO-
Er규92dU2一
-b·b67仕U7-
61祗沁沈騁壑
白UapFrot'2-
즐JZ'624·
측a44397-
7677뺑｀20·
朽朽786161壑
泌泛69朽64壑
76변규6곤첵 '
9괘뺑aUa닉노닐
βb7a'뻑닐rro
8勺규딕Lbe4
6r驢I노224
FE24
'2쨍r7
V
댔댔있댔敞RRRR댔댔댔댔밌RRIR밌R밌밌翩댔刪댔
m비니씨UU니밉
RRRRRRRRR
닢p''v.겻rq
0048F984
e048F닷94
0048F9R4
OO48FgB4
.:IO48FI?l꽈手
.-lr149F｀否굳
.1114딤
004E
.:l려4：ㅌ
.:104：프
,1l04드
긔．-14프
1.ㅓl'
004;_
0048
Heh익thisㅇne15inthedata
seCtio『1.BTW,do1needtosaythat
youneedtoverifyeachtimefor
doubleappearanCeS?Ihㅇpe『lot...
dre5s
an,Na衿ㅎ
니밉니밋닒 니쀼 닒 니빚
RRRRRRRRRRRRRR
Z,Setting卜...
눌＊B'gHead..Or.9
anddrㅇpth·en
rgt0theFavor.'
:〔':-'긺: 길：」－二녹걋
tebartoadd냥 '
00021004
00021004
0002!004
0002!0e4
000410e4
0004le02
00041e02
00041eeZ
00041002
eO021e40
OOaZ!04e
00021084
0002!004
00021004
00041002
00021004
00041eeZ
00021004
000410e2
00a21ee4
oloeleeZ
ol00leeZ
OIO010eZ
01001002
olO0ieeZ
eUE
R놈IE
E29
rO77
rOFO
662
秘花64
rD14
乙066
86''
646
4ee
722
沈邵邵
花6874
F4O
672
2e2
,r27
헤6F히
042
276
4eap
622
Egr규
乙O렇rZO
124
6떻＇7
aO49
2떻r6
e048F댜h·
0048FR84
0048FR94
3O4SFnn4
닢 V Vggggg
p·｀p·｀p·｀aaaaa
ararar"nH【h
nPHllPnPllllT
'bLL匕ㅏL
SSCO
75es
6R10
ESB200E
드9
33F6
요q7<FI
0038000000004000
.e89000o00002000
e03P000000003000
ee3B000驪：1oee〔12000
oe3C00Oee00e3e0o
e0400Oeeeeee10OePIXt
0040100000074000PIHt
oe47EOOOe00iR000Piㅐt
0048F0000000E0O0Piㅐt
0049D0啖）e0e4C000P（ㅐt
PEhe옰눕r
帥de
L"D。rt冬．슬ㅐport룔
.data
re룝。UrO슬S
·
ttaC
Hatr
슬da룔
trdr
· …
솔aaaa
·‘'＾■··＊'·슬■·..'
ppDpp
00000
螺 一一－---－一

Hehe, this one is in the data section. BTW, do I need to say that you need to verify each time for double appearances ? I hope not …

헤헤, 이것은 data section에 있다. By the way, 네가 2번 appearances를 위해 매번 검증하는 것이 필요한가? 나는 바라지 않는다 ...

I'm sure you know by now what needs to be done !!!

무론 네가 끝내기 위해 어떤 것이 필요한지 알고 있을 거라고 생각한다.

Saving also these changes to a new file

바뀐 것들을 new file로 저장해라.

Let's see what this looks like !

어떻게 됐는지 봐라.

Still a nice welcome, and then …

좋은 환영인사야.

Mmmmmm. I don't like it. Let's always keep the nice welcome and skip this from appearing …

음. 나는 좋아하지 않는다. 항상 환영 인사를 유지하고 보여주는 것에서 이것을 skip 하자.

Where was that again ? Hehe, I forgot the exact address …

어디였지? 헤헤, 정확한 주소를 잃어 버렸다.

Aha, right, there it is. Now, let's see if Olly knows where this address is pushed

아하, 맞다. 저기에 있다. 이제 봐라. 만약에 Olly가 address를 어디에 넣었는지 안다면.

Olly "knows" where this address is pushed. So, if you doubleclick this address, you will land in this string

Olly는 어디에 주소를 넣었는지 안다. 그래서, 우리는 이 address를 doubleclick 한다면 이 string이 있는 곳에 도착한다.

Ok. Here, the string is pushed on the stack == preparing to write it on window

But also notice the compare just above == am I registered

Ok. 이곳이야. String은 stack에 넣어졌다. == 그것을 window에 쓰기 위해 준비했다.

그러나 위에서 비교되는 것을 알린다 == 나는 등록됐다.

And if registered … jump this routine == don't write it on the window !!!

그리고 만약에 등록됐다면...routine을 jump 한다 == window에 쓸 수 없다.

Mmmm, so that means in this application : unregistered

if EBP == 907

음, 그래서 등록되지 않았다는 뜻이야.

만약에 EBP == 907 이라면

Let's see when we are registered

우리가 등록됐을 때 봐라.

Scroll up to follow the jump leading here

스크롤 올려봐. Jump가 이끄는 곳이 이곳이야.

Are we registered?

906 == registered

등록됐어?

906 == 등록

If not, jump to the place where we were before to put the string on the window

만약에 우리가 전에 왔던 곳으로 jump를 하지 않는다면 그러고나서 string을 window에 넣었다.

Do understand that this is a splendid indication to verify where the registration is set.

Find the place where is decided about

이해했어? 이것은 훌륭한 말이야. registration이 set되는 곳을 검증하기 위한 곳.

결정되는 곳을 찾아라

EBP == 906 (registered)

Or

EBP == 907 (unregistered)

Changing this to always EBP == 906

---> always registered

EBP == 906 (등록)

Or

EBP == 907(미등록)

항상 EBP를 바꿔라 == 906

---> 항상 등록

However, we know enough for this application.

Let's do this kind of stuff later in another example program.

Scroll down

그러나, 우리는 이 application에 대해서 충분하다는 것을 안다.

여러종류를 다른 예제 프로그램에서 보자.

스크롤 내려봐.

Yep, assemble this JNZ to jump always.

It will keep the lovely welcome message on the window until we buy the application

예, assemble 해. JNZ는 항상 jump 한다.

우리가 application을 살 때까지 항상 window에서 따뜻한 환영의 message를 유지해.

Because you know how to do it, I have removed from this tutorial the saving of the changes to file, the restarting and running of the new saved application till we land ….

… here. The only thing that rests now is

그래서 우리는 어떻게 해야 되는지 알고 있다. 나는 바뀐점을 file로 저장하는 movie를 tutorial에서 삭제했다. 재시작하고 새로 저장된 application을 실행하면 우리는 여기에 도착한다.

여기. 오직 있다. 그것은 쉰다.

1. **Testing the program**

OK

OK

OK

Ok. It keeps the welcome message

Ok. 이것은 환영 메시지를 유지한다.

Ok. We can make more then 4 entries !

Let's enter an empty one

Ok. 우리는 4 entries 보다 더 많이 만들 수 있다.

Right !

All right, we can enter more then 3 groups.

Let's make one …

맞아!

모두 맞아, 우리는 3groups 보다 더 많이 만들 수 있어.

하나 만들어 봐.

Ok.

Ok

And so we end with a full working program.

우리는 가득 찬 full program을 끝냈다.

1. **Conclusion**

In this part 4, we learned to kill some restrictions in a "crippled" application. There are more possibilities and other solutions to do this of course.

이번 Part4 에서는, 우리는 "불구" program에서 약간의 제한된 것을 kill 하기 위해 배웠다. 그것은 많은 가능성이 있고 다른 해결책들도 있다.

We also studied some other basic stuff. I hope you understood everything fine and I also hope someone somewhere learned something from this.

우리는 또한 다른 기본적인 자료들에 대해서 공부했다. 네가 모든 것을 이해했기를 바라고 누구나 누구든지 여기에서 무언가를 배웠으면 좋겠다.

See me back in part 05 ;)

Part 05에서 돌아올께.

The other parts are available at

다른 parts는 사용 가능하다.

<http://tinyurl.com/27dzdn> (tuts4you)

<http://tinyurl.com/r89zq> (SnD Filez)

<http://tinyurl.com/l6srv> (fixdown)

Regards to all and especially to you for taking the time to look at this tutorial.

Lena151 (2006, updated 2007)

모두에게 안부를 전하고 특별히 이 tutorial에 시간을 투자해준 너에게 감사한다.