09.Explaining the Visual Basic concept, introduction to SmartCheck and configuration

2012년 1월 29일 일요일

오전 11:51

Hello everybody.

모두들 안녕.

Welcome to this Part 9 in my series about reversing for newbies/beginners.

나의 초보자 reversing series Part 9에 온 것을 환영해.

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

이 "saga"는 완벽히 reversing 초보자를 맞춰서 만들어졌다. 또한 어떠한 programming 경험이 없어도 된다.

Lena151 (2006)

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

Again, I have made this movie interactive.

You screen 해상도를 1152\*864로 설정해 그리고 full screen으로 movie를 보기 위해 F11를 눌러

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.

그래서, 네가 이것을 빨리 읽고 다음 screen을 보고 싶다면, 보이는 hotspot 여기를 눌러. 보고 싶지 않을 때는 여기에 두지마.

Then the movie will skip the text and continue with the next screen.

Movie는 text와 다음 screen을 skip할 수 있다.

If something is not clear or goes too fast, you can always use the control buttons and the slider below on this screen.

무언가 명확하지 않거나 빨리 넘기고자 할 때, 항상 control button과 이 screen 밑에 있는 slider 바를 사용해.

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

도전해봐. 그리고 이 text와 다음 screen을 보기 위해 hotspot을 click해.

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

이 movie 어디에서나 즉시 떠나기 위해 이 spot을 click 할 수 있다.

1. **Abstract**

In this Part 9, we will reverse a "real" application to learn something about Visual Basic programs(VB), while studying the reversing of a registration scheme.

이 Part 9에서, registration scheme을 reversing 공부할 때, 우리는 "real" application을 Visual Basic에 대하여 배우기 위해 reverse 할 것이다.

That is because indeed, the best practice is found in real applications.

Real application에서 가장 좋은 연습 방법을 찾았다.

This registration scheme will also differ from previous parts because it is rather unusual : the program installs a unique key specific for your PC at first startup.

Registration scheme는 또한 이전 part와 다르다. 왜냐하면 꽤 일반적이지 않다 : 너의 컴퓨터에 처음 시작할 때 program은 명확하고 유일한 key를 install 했다.

For better comprehension and if you are a newbie, I advise you to first see the previous parts in this series before seeing this movie.

좀 더 좋은 이해력을 위해 네가 초보자라면, 이 series의 첫번째 part부터 보고 이 movie를 보라고 충고를 한다.

The goal of this tutorial is to teach you something about a program's behaviour.

이 tutorial의 목표는 너에게 program's의 behaviour를 가르치는 것이다.

In my search not to harm authors, I found an old version of PC to Answering machine(v2.0.0.4).

나의 연구는 제작자에게 해가 되지 않는다. 나는 PC의 old version인 Answering machine(v2.0.0.4)을 찾았다.

Taking a look in the specialized media, I also found this application to be "cracked" already.

특별한 media에 관심을 가져, 이미 "crack"된 application을 발견했다.

Here, this application is only chosen because it is ideal for this tutorial in reversing and it is targeted for educational purposes only.

여기, 이 application은 오직 선택됐다. 왜냐하면 이것은 reversing tutorial에 이상적이다. 그리고 이것은 오직 교육적인 목적이다.

I hope you will exploit your newly acquired knowledge in a positive way.

너는 너의 새롭게 얻은 지식으로 긍정적인 방향으로 이용할 수 있다.

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

이 문제는, Part 1을 참고하길 바란다.

1. **Tools and Target**

**이것도 똑같음**

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

이 tools은 ollydebug와 너의 두뇌다.

The first can be obtained for free at

먼저 free로 얻을 수 있다.

<http://www.ollydbg.de>

Numega Technologies' SmartCheck was a software company that was acquired by Compuware in 1997.

Numega Technologies' SmartCheck는 Compuware에서 1997년에 얻은 software company다.

Compuware only continued development of SmartCheck till late 2001. Then it was discontinued.

Compuware는 오직 SmartCheck를 2001년까지 만들었다. 이것은 비연결적이다.

SmartCheck was old as shareware.

SmartCheck는 shareware로 오래됐다.

However now, it can still be found on internet as freeware. Just google for it.

I'm using version 6.20 here.

그러나 이제, 이것은 아직 freeware로써 흥미를 끄는 점이 있다. Google로 검색해 봐.

나는 6.20 version을 사용했다.

As usual, the brain is your responsibility ;)

보통, 두뇌는 너의 책임감이다.

Todays target is the program called PC2Answering Machine Pro v2.0.0.4 For your research, I have included a DIFFERENT old version of this program(v2.0.8.2) in this package

오늘 target program은 너의 연구에서 PC2Answering Machine Pro v.2.0.0.4로 불린다. 이 package에 다른 옛날 version program(v2.0.8.2)를 첨부했다.

1. **Behaviour of the program**

As you can see, I have already loaded the application in Olly and in PEiD.

네가 볼 때, 나는 이미 이 application을 Olly와 PEiD에 load 했다.

Starters should always load a program in PEiD first(or similar like RDG Packer Detector, etc) to see what language it was made in or if/which packer/protector was used.

초보자는 항상 program을 PEiD에서 먼저 load 해라.(비슷한 program인 RDG Packer Detector, etc) 어떤 언어로 만들어졌는지 또는 어떤 packer/protector가 사용되었는지 보기 위해

More will be explained about this as soon as we deal with those (see later Parts).

We are here at the EP(entry point) of the program.

나는 좀 더 이것에 대해서 바로 설명할 것이다. 우리는 이것과 거래를 했다.(나중 part에서 보자)

우리는 program의 EP(entry point)에 있다.

Today, this is what I want you to nice

Because this part will deal with Visual Basic concepts

오늘, 이것은 내가 원하는 것이 무엇인지 보여준다.

왜냐하면 이 part는 Visual Basic 개념을 거래한다.

INFO :

VISUAL BASIC is a high level programming language (HLL) evolved from the earlier DOS version called BASIC.

VISUAL BASIC은 DOS version에서는 BASIC이라고 불리었던 진화 된 high level program language다.

BASIC stands for "Beginners All-purpose Symbolic Instruction Code".

BASIC은 "초보자용 상징 명령 코드" 을 나타냅니다.

VISUAL BASIC is a VISUAL and events driven Programming Language: the programming is done in a graphical environment.

VISUAL BASIC은 시각적이고 events 중심 Programming Language : programming은 graphic 환경에서 실행된다.

Programmers may click on a certain object randomly, hence each object has to be programmed independently to be able to response to those actions (events).

Programmer는 정확한 object를 랜덤으로 click 할 수 있다. 그리하여 각 object는 그들의 action(events)에 반응할 수 있게 독립적으로 programmed 됐다.

Therefore, a VISUAL BASIC Program is made up of many "subprograms", each has its own program codes, and each can be executed independently and at the same time each can be linked together in one way or another.

그러므로, VISUAL BASIC program은 많은 "subprograms"들로 만들어졌다. 각각은 그 program code와 각각 독립적으로 실행될 수 있다. 같은 시간에 한 가지 방법이나 다른 방법으로 각 link가 될 수 있다.

Keep your mouse pointer here and click whenever you are ready reading(on each textscreen)

너의 mouse pointer를 여기에 유지하고 네가 다음 textscreen을 읽기 위해 준비가 되었다면 click 해

INFO :

VB Application are fully compiled applications, but have a specific behaviour which complicates OllyDbg's job.

VB Application은 완전히 compile 된 application 이다. 그러나 특정한 behavior를 가지고 있다. 그것은 OllyDbg's의 복잡한 일이다.

Olly is a debugger for compiled languages but is far from ideally constituted to handle VB and as such works far better with languages such as C/C++.

Olly는 compiled된 language debugger다. VB를 handle하기 위해 C/C++로 짠 것보다 이상적으로 구성되어 있다.

The VB behaviour looks very efficient by the language and the programmer's point of view: VB programmers can focus on the specific applications' events and behaviors.

VB behaviour는 language와 programmer's의 관점에서 충분히 볼 수 있다. : VB programmer는 명확한 application events와 behaviors에 집중할 수 있다.

INFO :

All VB programs rely on an external dynamic link library (dll) (MSVBVM60.DLL for VB v6.0 and similar dll's for other versions). This dll implements all the APIs and the events.

모든 VB program은 외부적인 dll에 신뢰한다.(MSVBVM60.DLL은 VB v6.0이고 다른 version도 비슷한 dll이다.) 이 dll은 모든 APIs와 events를 시행한다.

Because all the VB APIs are implemented into the dll, the executed code is almost all the time inside this dll or jumps in and out constantly.

왜냐하면 모든 VB APIs는 dll에서 시행됐다. 실행된 code는 거의 모든 시간 dll안에 있거나 jump한다. 그리고 끊임없이 있다.

This results into a problem for OllyDbg, and as such, the call stack won't be able to help us further.

이 결과는 OllyDbg를 위한 문제다. 그리고 그러한 call stack은 우리를 도와주지 않는다.

This is very important when reversing: the call stack is seldom a help in Olly exactly because the application is almost continuously inside the VB specific dll.

이것은 reversing 할 때 매우 중요하다 : call stack은 Olly에서 좀처럼 도와주지 않는다. 왜냐하면 application은 거의 끊임없이 VB의 명확한 dll에 있다.

BTW, the application is mostly the event handlers, used as callbacks from the Dll to answer to specific events/messages.

By the way, application은 주로 event handler다. Dll에서 명확한 events/message에 대해 대답 하기위해 Callbacks일 때 사용했다.

The rest of the VB application are the resources, the variables and the functions used to associate event-handlers.

다른 VB application은 resource가 있다. 다양하고 기능을 event-handlers와 연관시켜 사용했다.

INFO :

VB is stack-based, meaning that it uses the system stack for virtually all its operations.

VB는 stack base다. 그것은 가상으로 그 명령을 실행하기 위해 system stack을 사용한다.

This in contrast to most other languages who use registers for most of the operations and use the stack primarily to perform function call mechanics.

거의 다른 language는 거의 모든 명령을 등록하여 사용한다. 그리고 주로 function call을 실행하기 위해 stack을 사용한다.

Application created in Visual Basic are compiled as interpreted or p-code executables. At run time, the instructions are translated or interpreted by a run-time dynamic-link library.

Visual Basic으로 만들어진 Application은 interpreted나 p-code가 실행되게 compile 됐다. 실행 시간에, 명령들은 번역되거나 실행 시간에, dynamic-link library에 의해 해석 된다.

If used, the p-code engine is a simple machine that processes the opcodes.

사용할 때, p-code engine은 간단한 machine 이다. 그것은 opcode를 처리한다.

All operands used by p-code instructions are stored on the stack.

모든 operand는 p-code 명령에 의해 stack에 저장된다.

시스템 생성 대체 텍스트: 흐희꾀긔꾀꾀의죄희희꾀」희셥1최
COh衿슴ht
..lee>
냠」.RL
INFO:
RememberthatyㅇucanacCess
thecal-stackhere(orAlt-K)
LHLLLL
nDRRRn-
' ' ' ' 、 '
IJIJIJIJIJIJI
나門나內나n나內니門니內·

INFO :

Remember that you can access the call stack here (or Alt-K)

기억해. 너는 call stack을 access 할 수 있다. (또는 Alt-K)

시스템 생성 대체 텍스트: 닙급·』 ■'。'' 「'.'·'''＇、'。··
INF○;
Whilethe(system)
StaCk15here
SFOa룅80찧
73FF盼64FcgF
10FFDO觸ZFE7
gFFa킹18
沈FF芥에開83FF沈沈開觸eeee騁
FZnE쩌청O翩떼
ntdll.7C91O73e
「『臣万乙「乙百‘
FFFFFF
EndOFSEㅐOhaLn
SEhand【er
kerne【32.7C818D드8
386n킵n팁
9F嵋舵eO開
PCZnhZ一P.＜敞업u【eEn零r,P。int>
的l6閔예觸田開
8808e40
닝C。U48Cnp48Ce48C
一r·DDDDEEEEFFFF
下H汗円汗FF麗FFFFFFFFFF麗
J、업즐논Jl녑22222222
JUen킵npo킬dUnpnpaDeaUa긷aU
IU0ap柏U白p。pap仕pnpoapa빕0

INFO :

While the (system) stack is here

Stack은 여기 있다.

INFO :

In general, a dynamic link library (DLL) is a (collection of) small "program(s)" which can be called upon when needed by the executable program (exe) that is running.

보통, dynamic link library 는 작은 (집합체) "program" 이다. Executable program에 의해서 필요할 때 불려질 수 있다. Exe는 실행되고 있다.

Mostly, the DLL lets the executable communicate with a specific device such as a printer or may contain source code to do particular functions.

대부분, dll은 executable의 특정한 device와 함께 전달된다. Printer나 특정한 function을 하기 위해 source code가 들어있다.

INFO :

An example would be if the program (exe) needs to get the free space of your hard drive.

Program이(exe) hard drive의 자유로운 공간을 얻기 위해서 필요하다. Example이 있다.

The program can call the DLL file that contains the function with parameters and a call function.

Program은 dll file을 call 한다. 그것은 parameter function과 call function을 포함하고 있다.

The DLL will then tell the executable the free space.

이 dll은 executable free space를 전할 수 있다.

This allows the executable to be small in size : no need to rewrite the function that was already written in the DLL.

이 executable은 size가 작아야 한다 : function을 재 작성할 필요없다. 이미 DLL에 작성되어져 있다.

This allows any program to obtain the information about the free space without the author having to rewrite all the source code.  
모든 program은 저작자가 source code를 재 작성 할 필요 없이 여유공간에 대한 정보를 얻을 수 있다.

It also saves space on your hard drive.

너의 hard drive 공간에 저장할 수 있다.

INFO :

The advantage of DLL files is that, because they do not get loaded into random access memory (RAM) together with the main program, space is saved in RAM.

진화된 dll file이 있다, RAM의 공간을 절약하기 위해 main program과 함께 RAM에 load 되지 않는다.

When and if a DLL file is called, then it is loaded.

Dll file은 그것들이 load 된 후에 불려졌다.

For example, you are editing a Microsoft Word document, the printer DLL file does not need to be loaded into RAM.

예를 들어, 우리가 Microsoft Word document를 수정할 때, printer DLL file은 RAM에 load될 필요가 없다.

If you decide to print the document, then the printer DLL file is loaded and run.

Document를 print할 **때** Printer dll file이 load되고 실행된다.

INFO :

All in all a DLL is an executable file that cannot run on its own, it can only run from inside an executable file.

모든 DLL 파일은 executable file 이다. 그것은 그들 스스로 실행할 수 없다. 그것은 오직executable file의 안에서 실행된다.

To do this, an executable needs to declare the DLL function, then when needed the call is made with required parameters.

이것을 하려면, Executable은 DLL function을 선언해야 한다. Call이 필요할 때 필수 parameter와 함께 만든다.

Now, for VB and its language specific DLL, all said on this page is also true, except that the DLL is loaded all the time of course.

이제, VB와 명확한 DLL language를 위해, 이 page에서 모든 것을 말했다. 이것은 진실이다. 예외적으로 dll은 모든 시간에 load된다.

이제, VB 및 언어 특정 DLL language를 위해 예외적으로 dll은 모든 시간에 load 되는 것이 있다. 이것은 진실이다.

Perhaps you think now that VB will be a very difficult to handle language?

아마 VB는 handle 하기 매우 어렵다.

Well, it's more the contrary because we have some very useful tools for this which I will explain in the next Parts in this tutorial series.

좋아, 꽤 정반대 된다. 왜냐하면 우리는 이것을 위한 매우 유용한 tool이 있다. 그것을 이 series의 다음 part에서 설명할 것이다.

So, stay tuned ;)

계속 지켜봐 주시기 바랍니다.

However, don't think that Olly is completely useless in VB either : after all, each language is translated to assembly …

그러나, 생각하지 말자. Olly는 VB에서 완벽히 유용하지 않다. : 결국, 각 language를 assembly로 번환 한다.

But let's talk about the behaviour of this program.

Program의 behaviour에 대하여 이야기 하자.

Well, I kept my eyes wide open and remarked this: at first startup after installing, the program asks for some time and states it is calculating and install "a unique key" for your computer.

좋아, 나의 눈을 넓게 유지하겠다. 그리고 이것을 발언했다 : install 후에 첫번째로 startup 한다. Program은 약간의 시간과 계산하는 상태와 install 할 때 너의 computer의 "a unique key"에 대해 묻는다.

Now, this is rather unusual but it gives us already a good hint: it means the program has made a registration code from some ID(for example a hard disk ID).

이제, 이것은 꽤 일반적이지 않다. 우리에게 좋은 hint를 준다. Program은 약간의 ID(예를 들면 hard disk ID)에서 registration code를 만들었다.

But … this also states that the program needs to keep this code somewhere so it can verify at each startup if it is registered or not!

그러나 … 이것은 program이 code를 유지할 때 필요하다는 걸 명시한다. 등록되었든지 아니든지 각 startup에서 검증할 수 있다.

Let's exploit this as in fact, we know enough already.

이 사실을 이용하자. 우리는 이미 충분히 알았다.

1. **Finding the serial**

I said we know enough already, hence, let me explain what we will do.

우리는 이미 충분히 알았다고 말했다. 그리하여 우리가 무엇을 할 지 설명하겠다.

The program needs to verify at each startup if it is registered or not.

등록되었는지 아닌지 Program은 각 startup을 검증하기 위해 필요하다.

Verifying this naturally includes a compare "Am I registered ?" in the code somewhere.

자연스럽게 비교하는 "등록되었어?" 것을 code의 어디엔가 첨부했다.

Well, in VB, this is done in the API's in the DLL.

좋아, VB, API와 DLL에서 됐다.

시스템 생성 대체 텍스트: 묘蜀緘
"tdll.k
eeee7
ZbZbZbZbZb∥
333公구3N
心JB33Ba긷
e2이貶02떠oo
aoapaoapa딩0
555555
ECSDF6
a틸뱁‘ao뱁‘n
CPpZq
훨7
eL LHLLLLL
eR nDnnRRR
.얹h렁沿U"60.ㅎl
PTRDS:〔ERX】,
PTRDS:
PTRDS:
PTRDS:
PTRDS:
PTRDS:
PTRDS:
PTRDS:
37!19e6F
ThemㅇSt
importantare:
EL므001ZFFBO
EDX7CgOEB94
EBN7FFDD00e
E슝Pee!ZFFC4
EBoOe1ZFFFO
E二!「FFr「F「FF
ED】7C9i0738
E!P004i0178
ntdLt.7《
PC鮮눕n〔F
洲耀rE''rErErErErErErE
｀뻑낟J여
執．ESX
拓C
r』 빽볍볍볍볍졉볍졉볍뗀
깽pEIDvo.93
논뾔뻐出
F넓e:IC：뿌rogramF＊논‘PCZAnswer찌MaChnePr아《기배2--F핏o.exe
□
La'tErrERROR－딧
0000024'《HO.HB,E
순hpt부weUHOR"BSB〔
래p차겯0.0
ehpt닛0.0
걔 刀
rp밉
4''｀난－ ·
_vbaVarTstEq
VbaVarTStNe
_vbaVarCmpEq
_vbastrCmp
_vbastrComp
_vbastrCㅇmpVar
n 빼一 "
O 덥礪 e
力 Y 탰
X 타 뱀
e E 洲rj
S 沈 즈
·· S Jㄴ
nr r U
E F S
M亡。酵t읽S뱌딧Ba,CS·0/6.0
'Pc래＂乙PRo'''"I陋。scan--Task梗臟1ㅣ여bons-I About- E離 l
巨Sbyontop
느」느」
-―迪닉
RemaFI이thefirst
에eineaChCC)IUmn
arebyfarmㅇstused
p《겯 UO U《， 《P.1pU Op po 《rp
00000000100On0000
·····……J체『닙
,〔껸끄그휄컫이
l흐비솥ㄸ坐―쁘鑒Z王으l_

The most important are :

가장 중요한 것은

\_\_vbaVarTstEq

\_\_vbaVarTstNe

\_\_vbaVarCmpEq

\_\_vbaStrCmp

\_\_vbaStrComp

\_\_vbaStrCompVar

*번역 주)vba Variable Test Equal, Negative, Compare, String*

Remark : the first one in each column are by far most used

각 열의 첫번째는 가장 많이 사용되어졌다.

So, let's try the first API and place a breakpoint on it.

First close PEiD, then follow how this can be done …

첫번째 API다. Breakpoint를 설정할 수 있다.

첫번째로 PEiD를 닫자. 어떻게 끝낼 수 있는지 봐.

And we are at the OEP now

So, press Ctrl-N to show the names module

우리는 OEP에 있다.

그래서, name module을 보기 위해 Ctrl-N을 눌러.

And press vbavartst on the keyboard

…. To easily find the right API Also notice that all AP's are in the DLL

Keyboard의 Vbavartst를 눌러.

쉽게 올바른 API를 찾을 수 있다. DLL에 모든 API가 있다.

시스템 생성 대체 텍스트: nFind:V-그꺼
口回因”
Rddr순홍씽
tIOn」--T
"ane
』卜
.t숱st
J=＇닛t
ItCan
騙7<-
be
「ㄷ＇「－
댑가·－익잇
fo∥owedhere
Ca11
RddR.f
＂『’－陝”r目”r爵탰긴G·tIO'OfN刪ㅎ’
"glB。ill60.EUENT--SINK-Invok.
"SV「n60.타ENT--SINf입Ou슨r,Inter「욥。e
n힛l:'r10·타，ENT--SINK-Re·e糾．
d니【eEn
프乙낍拓
tttt수‘
HHHHㅐ
'e욘eee
'ttttt
… …
.teㅐt
.te님t
.teㅐt
.t·닝t
·teHt
.teHt
.teHt
.teHt
.teHt
·_Vb.n
.__ub'R
._VbaR
r,
耽mt업r닙O첩a
O순륭trUCt
rVLOck
r，汝싸．
－驟跡T'
CmR
팝1以JB
"SUB
h무」B
＂孰룔B
.__"ba습r,Un【。。k
._vbaBO。tErH,ar
.___VbaBOO【Str
._Ub.BOO【Uar
.__VbaDOO〔UarNu【l
m·댄6e6e6e秘6e6e6e
뻐llr1배배배배배배硼
l'EBBB
蘭楡溜呱
"sl)BUr160. UbaC슬＄tobj
rrrr''rrrrrrrrr
PODOPOPO艸a畔aPOa鱗a釀DO
nhnHI..hLhH衿hhhn
''랗‘''E=''It'I'L''''''''
嶼lC8刪l84懈刪吸ID81B8178倒6C82D4e24刪O88eD4llc陝924
11111'11101111111111
nIO더1OUdUdUedUd팅.'0ao8aUa댜aoaOO쵸Ud깅
44444444444444444444
:i：엣배帥脯盼卵腑盼에盼腑ee盼腑ee脯卵盼卵

시스템 생성 대체 텍스트: 탤r밴「
口回因
^
던）r16軌＿vbaVar야pEq
’톄새16이＿_vbaUarCnp6e
르쁘뜨뜨ㄴ－꼬b슬UarCnp6t
h-· 一
纏
헨）P憮
nr느OP,
〕rU니p
argUarC。pg
다
；나n60.＿니baUarqUa까bve
：륭jnbU.-Vb솥V.r1OU,
,뗘60._vbaU枇Hov.
l저60._.vbaUaror
니n60.
_vbaUatsub
_"b얽눕，Ttt數l
익여헝g읽
l1"""n
OO4OleZO
004012EC
OO401eCOI
a040!1RCㅣ
HSVB나160._vbaVarT$t6t
"SUB바160.__vbaUarT'tLt
HSVBU"60._vbaVarT$tH.
"SUB바160._vbaUarUar삶Iofree
h무）B녜160._vbaU.rifyVarobJ
nsl」던／뼈60.2。“b힁e.GetT,peIn「。
＂딧盼니r160。Z。衲b1._GetTg。eln「OC。니nt
녹걋

It can be followed here

Now place a BP

이것은 따라갈 수 있다.

이제 BP를 설치해.

시스템 생성 대체 텍스트: inPCZAㅆZp
珊轍무무뺐JLI『님》
曆暄仄
arCnp〔q
'rCn0GE
홑rC'p6t
arC"pNe
뻐baUbaUbaU
빼勵ft
"pOXt
뻐port
nport
nport
hport
np。rt
hport
衿p。rt
hport
hport
hpott
＇뱀prt
hport
"port
hport
hport
nport
nport
nDOrt
쑈르坐L一－■·ㄴ
;爲닌slvlt姃0._v
119)BU"'e._v
11St)gUh6e._V
"SUBU"60._v
t.Ht
t손ㅐt
teHt
teHt
teHt
nSUB녜16e._vb.Ua.COp,
"SVB나16e._vb.UatO니p
"SUB나160._vbaUatgUarC。p,
"SUBU"60._vb.UatqUa난byㅎ
n놉VbVnbU.-VO.Vat10"*
nspB아160._vbaUatNO"e
"g」BU"6e._vbaVator
nSVB아160. vb'UatS"b
te눠
teㅐ
零ISU테，t16o.
ACtUa놉Ze
t·님t
＂의』
＂읽」
＂以』
BUh60.
004012C0.teHt
Oe40le20.te남t
e040!ZEC.t.Ht
OO401eCO.te"t
e04el!RC.teHt
BU"60._vb
BUh60.__vb
＝窕仄F
一vb Ft엠OW
in【）isaSS톄軟聊
겨es ·844Oe4884CC408C
게es엣－乙eC14e83eZEeB14e4ellsee"ee12
-目ㅡ命we紛柏盼柏牝柏柏柏牝牝牝犯’e柏柏
-ㅁㅡ언we盼騁恥觸盼盼애舵盼盼ee盼Be盼騁
Eh눈f
＂딩」B（버60._Vb
＂以夕BUh
"9.＇던j너
60.2
60.2
。nb
O矜b
Fo跡wl叫＂rtlnUsasse祉尨r
肉룝이｀inDUmp
Findr이눙ences
V빈빙대［tr슨e
Hebons얜令히넌name
＇욥뺑홉맬홉＇■춈7lt홑7홑f'7홑썅‘우‘썅‘쟁홉7'＇■솥7쵸f홑7홑f'f'
C히용Fl
elee觸的盼舵
BBBBBB
ODDDDD
BPoneveryreference
『『－珊궁r'r7一댜r닥芬「rr一一「「견’｀큰F갑대「r-rr
功凶논노ea너oint
Co〃公出m」노ea楙덞t
COnc느bon님Iogbrd畛ht
F2
sh즐ft수FZ
Sh漱수F4
·泮「－
窯執
tonev비re慽enㄸ■
＂「toneveryre돋renc횬
觸ee騁騁
bOBBB
ODDD
elseeeee에的觸r뵤鞠ee卵eeee鰍
RBCDE큰re뱁‘234Fe쫠‘20
nnnnHnnBBBBBBCCC츤
自自41n「．:
Remove려1bre써mints
J-IHeH山醱． . 二r
COpyto야軟）ard
SOrtby
勿畛aranCe

시스템 생성 대체 텍스트: O''a'$.nbl,
PU驪「P乙Zn匿
COh杓슝nt
041067
inP(i2＾ㅆZp
떼回國
O업老On
nSUBU서60._vb솝parChpEq
＂읽沿Uh6e._vbaU.rCnpG'
"SUB아160._vbaVarCnp6t
"SUBUh60. vbaUarCnON·
"SUJ챠16e._vbaUarC여）y
HSUB바1
쫴gIDlj"
'니E:ll"
''IIE;llrl
6e._vbaUatD니p
60._vbaVa'gUarC。p넛
._vbaUar
._vb'Var
밴젯肋飇
IOIV
Cl、뗘50._vbaUarNove
··니E;l）셔6e.__vbaVaror
_딴111150._vb.U홀tsub
■■■·‘별．_vb.U쟁，Ttt嫩쟁
hSUBUr160._vbaV슬rT't6t
"g」e나160. ubaU.rㅜ’tLt
"SUB야160._vbaUarT．댜솔e
hSVBUn6e. vbaUarUar삶Iorree
"St)BUn60._vb.U.rL仲Var()bJ
"SVB나I6e.20"b1e.GetT,peln주。
"SUBUr16e.Z。衲b'e_aetT”。eln「OC。unt
el00000000000000000000
四叩叩叩叩叩叩叩叩叩叩叩叩쎄畛叩叩叩叩叩閃
"PCZn＂乙．이국0".e
rtrtrtrtttrtrtrtttrtrtrtrtrtrtttrtrtrt炸·el盼硼騁애飇卵ee觸Oe＝盼硼開朋
BBBBBBBBBBSCBBBB
ODDDDD一UDODRDDDO
ㄷ 궉 r'r---11111111-111-!l---------· 4
O 汀ee섬一CC480EB4418O멩reZCZECn·l色Uee·eea긷a긷dpapa길쇼poe
U 쾨ee흔－Z쵸ple32elee10·‘012e2OI·e仕peeeeoeee드eseo
' r톼·ㅡR-000eoeeoee쇼컁e·00eap0Oe'ClbOCDEFei234FelZ
r굳-r■F■■■■■■■■■■■■■ nHnHRpnHnHBBBBBBCCC
梧Uoap00np00eap洲뱀驪뱁蝦힁apa무bpoapoapeo일eaUapa긷00apapeoeea킬0ap000
술홑뱀‘1'1홑1'ㅓ홑뱀‘뱀횹뱀쵸ㅓ홑뱀‘1홑ㅓ횹1홑'.'·‘｀흩1'ㅓ홑1'뱀‘ㅕ홑｀홑ㅓ‘1'멩홑1'멩홑''ㅓ‘뺑‘뱁홑1'뱀‘뱀‘뺑홑ㅓ홑ㅓ‘ㅓ‘1'’홑
444크－f4444444444444444444444444444444444444
dpd긴oe000000dpdpapon긷000仕UdpoeeeaOOe000O00eoe000eo
凸p00eoaUOeoa틸dU00000白UOa긴od탭oa깊0仕Uea긷白OOd긴ea긷eeapapaoa깊eo白긷
HZP.OO4i
e''IH’盼L地l"P-
’→…
I78BP'Sha
R혀그I
beenSet니!
홑에 너'1 너.
COmma
絿SSe蠟

BP on every reference

78 BP's have been set !!!

모든 reference에 BP가 있다.

78 BP가 set 됐다.

BTW, there are other methods to do this, for example using command bar plugin.

We'll see that in later parts.

By the way, 그곳에는 그 일을 할 다른 method가 있다. 예를 들어 command bar plugin을 사용할 수 있다.

좋아 이것은 다음 parts에서 보자.

And run or F9

실행하거나 F9를 눌러.

시스템 생성 대체 텍스트: 더
- 계【．찧'- 一 一一―‘一-
Cp【j-颱inthrea비m여lulePCZAㅆ치．P
-.__.＿「－―一l一一∼
「즈］
勉넙畛슨흖훰'H.X
00SFIF4FR
00드RF4FD
山』hp
「FIS7el14lae
66:gB「8
SD4D80
CC,r·，nent
l1s昞지蘭JJC
00드nF태
08또E7
eo또태
005RF驢
nSUB네160._vbaFr..U.
이lybreaks
緞邵纖祈祝否而麻玩緬눠
"OUDI,RX
LEnECX,DUORDPTR55:[E아》一80〕
댜LLO볍，0Pn극DS.［《‘hSUBVn6e._Vb'Fr卄·
CㅒPDI.SI
'gEr구O巴D128
뱀‘33
닝e8Fbpgrp88
·66F83766
닝7CI
UnUeed룅eeee
"-→UdUa틸n긴000白p
〕OFnF드
PCZqnaeeP.OO드nF621
DUQRDPTRD하〔드C9990〕.D〕I
SH()RTPC쵸놈＂2一F.이〕드RF드27
「드i
「드l
F드2
e99드COO
eO94200
7C!2400e
9e995C0e
28835Cee
0
8835C0e
e9241ee
PUSHPC라놈H긱P.OOSC’夕）令O
PUSHFC라겸U흽e,OO42D3ES
댜LㄴD볍芬【PTR05.[＜긺恪（8바拓0.＿아》샅뺑。날2'
h0UEDI.DUORDPTRDS:[SC99901
CNP以닐야극DPTRDS:[5Ce328】,ESI
JHZSㅐORTPCZRhZ-P.OOSRF54S
PUSHPC즈놈H〔P.Oa5C8328
PUSHPC하궈nZ一P.8驪홍19280
nSCll"T.쿠"
"SUBU"60._vbaHe닐2
inthefirst
_vbaVarTStEq
itenCOUnterS
>·갼··
빽rD3rpCI
竇·2勺규3츱9
드rorpr규r규
FFFFF
nHCHhHnCHCHCHCH
r길rpr구r큐Srpr구rp

Olly breaks

In the first \_\_vbaVarTstEq it encounters

Olly는 멈췄다.

처음 \_\_vbaVarTstEq에 맞닥뜨렸다.

Mmmm, there is not much to see in the code.

음, 그곳은 code를 보기 위해 충분하지 않다.

Nor above this screen : I scrolled up but removed it from movie

이 위의 screen : 나는 scroll up 했다. 그러나 이것을 movie에서 삭제했다.

Now, step with F8 to get an overview of the program

이제, F8을 눌러 program의 관점을 얻자.

Hehe, that's interesting but first let's jump and look further on

헤헤, 이것은 매우 흥미롭다. 그러나 먼저 jump 하고 더 멀리 봐라.

Now, take a look in this piece of code. Do you remark something ?

이제, code 조각을 봐라. 무언가를 주목했어?

시스템 생성 대체 텍스트: 더Cp【j,mainthre繃，驟넌uleP(i걔ㅆ2--P
dUhp
OL룝a''enb【，
C이브빰쵸L____^
IJr4II:l:IDF"PC2qn＄닐ering"acf,ine2.0一P'.-,F'츤
rUCD
EEE
며」
OU
,:--F슥＂a-P.eO4967n요
자「ㅣ죠：叩깁P,e05C80B4
1,D니）RDPTRDS:〔＜各hSUB아陋e._vbas
"H니H니
驛LLㅌ01
HOUEDX,PCZ
h읽긔BU"'e._vbastrCOp,
《얇媤pBVH60._ubastrCop,>
UH1CI)DE'.2.0.0.4"
HOV印닝。PCZ
CFILLEOI
R「t〔．P.00436770
R『tLP.O05C827C
re一뻐·－나l측ㄱO닢n니·r
룝es 흽뱁닙ktrr'L·卜－겸．
竺丹聊珊鮮
츤논ee 履볕r.蝦띰蝦．乙LnL··
009긔F644
00囊경F649
009슴「64B
00드n「6드드
00SRF65B
eesnF6드D
005qF662
ee驪괘F667
00驪극F66D
OOSRF673
00하겹F675
00驪긔F678
00驪겸F679
00驪긔F67n
00딧경F67D
ee驪겹F67F
ee驪IF681
oe하겸F683
ee5RF685
ee드RF88n
00SqF68B
e05RF68C
00驪놈F692
eo드nF'94
00驪놈F696
00드qF69C
OeSRF69F
00드습F6nl
00SRF6n3
oeSRF6ng
00드nF6RR
OeSRF6RB
00야겸F6RE
'1.·「」뎨'{.1
■一，길[一■〔'【:
ER.,.：깁r一4:p더
BgB4805C00
SB3D술012400e
「FD7
BR7a67430e
Bg7C825CO0
「FD7
BR84石74300
BgeO82히二ee
더l:lt·ED>:.PCZR"(P.00436784
NOUECX,PCZRH乙．P.OOSC8280
FFI)7
C7OS
邙LLEDI
배II:13DE"r嶝로’－貶’'
39
.v7s
68
68
FF
8畛略CO이ㅒ
9e995c00lC
머JORDPTRDS:[CCSZ
DUORDPTRDS:〔SC99
85긔IE
ge],ㅌ51
ie
90995C00
SH0RTP(:2Rn乙P.이〕이눼F66D
HPCZRnZ一P.005C9990
HUh끄뀨
D34200
7C124eee
9099드coe
E8D342
CnLL
邵棚누癩
0042D3E8 .
OS:t＜各서SUB아恪e.＿야’냠눋닒의
RSCll"T.
hSUBU"'0.
에際附嵋US
JPP
》SB3D
SBO7
SD4O
5l
드7
FF5814
OBEZ
3BC6
.v7D13
'R14
68D80342ee
57
5e
SBIDnCle4O00
「FD3
.vEBe6
》SB10nC1e4O0e
>8B4드94
SBFS
SBle
8【）SDSCFEF「FF
5l
5e
FF52'8
DBEZ
3BC'
H야』EDI,DUORDPTRDS.:【SC9990】
HOUER자D배）ROPTRDS:tEDIJ
ㄸREC닝，DUORDPTR55:[E마》一“）】
PUSHEO二
PUSHEDI
댜LLD닝ORDPTR05:tEp<+141
FCLEX
C"PERX.ESI
JGESHORTPCZnh乙P.e05nF696
P냐SH14
PUSHPCZRH〔P.00420308
PL夕SHEDI
P냐SHERk
HOUEBX.D뺘ORDPTRDS:【＜各hSUBU
댜LLE탸蝦
J"PSH이괵TPC즈긔HZ一P.oe릉nF'gC
HOUEBX,D뺘ORDPTRDS:【（蝦HSU6U
HOUERX,D驢）RDPTR55:[EBF》一잇）】
"OUEDI,ERk
NOUEDX,O뺘OROPTRDS:[E댜＜」
LEnECX,OUORDPTR55:tEBF'-17쎄
P냐SHECX
PUSHE댜《
댜LL미蹈RDPTR。S:tED닝＋58〕
FCLEX
CrIPERX,ESI
Wel-,here
Isuspected
lS
tO
What
finclo
咀鑽넌鯉’ㅜvb뛴奴잇It뎬擊k맥Z。，、
｀致긔J魯V켭V「（'U.-VO려nr뺨SU[r닙n'C駁UOJZ
"SUBU"'0._vbaHr.'u1tChe。kotU

Well, here is what I suspected to find :)

좋아, 이것을 찾기 위해 의심했다.

Continue stepping to see a little further

조금 더 멀리 보기 위해 계속 가보자.

시스템 생성 대체 텍스트: …－ㄴ．一－-－」」lleeee→「11111一
r두＝>/ㄷ준7처rrwe닙
I.' I「1,-11L匈－7
亡」亡솨t스긷
.^낸르
i$ter룝《FPU) < < <
刀訂胛巨r硏兀閔r긔치猫「4…
00e0O000
阪，4〕6기크4UHICODE"k」hd-546-Lu'-82"
태P
EBP
ESI
EDI
EIP
00008000
.e1ZFBC쎄
0012FD94
oeeee800
''eE'1．ㅌ
005自F644
씨‘兀誦兩
XXXX
톄ECEDES
＂읽沿U"'0._vbastrCOP,
PCZnHLP.0e5RF644
ES0a2332bLtel「「FFFFF「）
CSOe1B32bLtelFFFF댜’FF)
55eB2332bttelFFFFF「FF)
050B2332bite(FFFFFFFF)
FS.e3B32b't7FFDFeeO(FFF,
65eO00HLjLL
La$tErrEf攪OR-S度鷺CESS(eee0O0eO)
08e08246 ._.느니콰1.'?.노∼＿닌.L_·
e뱀‘aOin낑eaOS
CPnH쌩LSTDO
EFL
貂Oe8217e6
eell'e
aeeeFo
STOehpt,
STI콱hpt,
STZehpt닛
ST3e"pt,
ST4ehpt닛
STSe"ot,
ST6'npt,
ST7'"pty
FST00e0
FCU137F
a.．드6드8498397恪OIOF42Oe-4933
－나【R"F3BO000006
＋나【댜lee3BOB12F6
－나【댜멩FSEC0e20a2
e.000000Oe78484483
＋나【R"2679000000
4.eee000aoaoaa009e
e.ZS0000BBOSO000OO
B7C38680
e00000.o
e08000!B
e송－4슬33
400e1372
*'O킬쵱욥
rl·1
1 0펩‘
e''
UO뱀‘
PO뱀‘
너O
!e
''O
3O
COnd
Pr'c
NERR,64
Err
ha'k
〔GT)

Mmmm

All right, try it out

First remove all BP's

음

좋아, 해보자.

모든 BP's를 삭제하자.

시스템 생성 대체 텍스트: 홰CpU·α넌inthread,"x》dulePCZAㅆZ_p
쁘뽁隱군
미므뜨뻐비L一一一一一一一一一一一
110UEOX,P嚥〕n텨a一P.e0435709
.hent
繭乙硼E
芯꾜職nNa一inPCㅆㅆ긴P
_ 口回因
緞翩驢＝匕騶零b馮읗
UHI竄j
l鑒鑽뻔했·一v
볍獵꿇騈盤甕
arC써）Gt
arCnpHe
argp,
솥rU나O
갇C
댜n
J
qX
臘존맺組’一앵뱄ar뱄ar坐p,
n놉냉，切ㄱ컨꿴ㄴ_v。av'r'U.rn。ve
H앉珊（功ICO._Vb'U솥rldiv
,_vb콤V쵭rnov룝
._VD솝VarUr
._VbaU슴꽈sub
._gb옭汕rTtt탸3
"SUBUh'U.__vbaU숩rT룔t6t
HSUBUh6e. ubaUarㅜ’tLt
"SUB야1'e._vbaUarT륭th슬
HSUBUh6e._vbaUarVat삶욜ofr.e
"St)B나1'0._vbaU.rLf,VarobJ
"SUBUn6e.Z。＂b딩e.GetT닛peln주。
"Sl)BU터60.20衲bi순一GetT，。슬InfOCo니nt
n8Cr
H以l驢
UVUUUUU
bababab.b.b.b.
l수튕욜｀t수흼t솥룅tt수밍t수눙수놈솥b수튕t수랗t수딩t수힁
-frrrrrrrrrrrrrrrrrrr
묘hh鞠鞠鞠鞠鞠鞠什鞠鞠鞠1.h汁鞠h鞠鞠什
S층Ct흰On
.t순Ht
쬐‘글춈욜驪l
닐'e빵’욘ㄴ
·teHt
輟ㅜ：·
…긷 rp누p
긔싸雕넙、
驢＇＊夕츱八’r쨍눙
騙敭切簾騙
수혹헝：'닙황
· · ‘、·
닐珊몇욜훵궁r
닐르1…
0.-r＝ㅓ댜
llUSㅗㅓ一·
0·）以F'
니ㄷ려＝'
".’「니‘-'
以－「궈＝'
I-IUSHㅏ며
OOFRFf
oe5RF'
oe5RF'
00드RF덕
00gRF변
이〕SRF貶
00CRF一
005RF'
이〕SnF'
00드RF'
00gIF'
00드RF'
oeg自F,
匯눔듸긔F'
00401
Oe4el
OO4el
OO4el
004el
.多우님t
.t앙혐t
·七eㅐt
.零eㅐt
·t盼님t
■L·휘옭l흩P.LpE휘팝z爭tㅏ수rrㅏf·-
蠟曦1l4瓏擺瀣攫槨
d-444444444444떼
tttt
·t·H
.teH
媛徹稷
매E
SRF
00401醵이.t애
OO4eltnC'.teㅐ
驪눕F'SR
드RF'SB
snF68C
드nF'92
드RF694
드q「696
弓RF'gC
SRF69F
snF6nl
드RF6n3
SRF6ng
SRF6RR
SRF6nB
snF6RE
드RF6BO
「O「‘D》
드7
5e
PUSH
PUgH
EDI
Em《
SBIO
「FD3
pC!040e0
nCie46ee
94
SL下邸FFF
태
LE
낚．D냐ORDPTR
뱌《
ORTPCZn＂乙
乙，DUORDPTR
X,D뺘DRDPTR
DS:t＜얇ISUB아盼e._vbaH극
P.ee驪nF'gC I
n있j6나垢오
＜읨HSUBU「
.vESe'
》eelD
》8츨45
seFS
e白le
SD6O
Si
5e
FF드2
"SUEU"5尸
I,E슴k
X.D뺘ORO
ECX,DUORD
ECX
E댜＜
O냈累OPTR
PTF
PTF
Ds'〔（蝦HSUB아佑e·＿VbaHI
55:tEBF》一sc】 1
05:tE아‘1
55:[EBP-174]
乙pseㅐDh니
EEEE
에인l1P0(JOU에에태USuS
hCJhㅒ"hLPP
댜LL
08:tE마＜수恪8]
DBEZ
38C6
FCLEX
CnPER났，ESI
nUnpeenUeedonoeeeeeeen긴
Ueapeea긴dpapa밍eeapdpap쇼pa킵쇼U
ED놉0.000000
峰
Rddre엥｀1HeH改』h
RSCll
쎄...0.E.O.......
.5···.0......4...
0.枉．0.......’石■··
.O..........D＊···
0.拓0....
…
· · ■
· ·떽r
·＂뱃U
· · ■
....p합■.........
........-．■··....
·····.......p수·.
..·.-X…,····.·
卯盼盼沁盼盼盼盼開盼盼盼盼盼叩勵
b白룅a컁6600色딩odO6aOO00n
凸UOO.'ㅓ‘O白pO00.'dO00ap功
凸UnUO6닢＾d긷eeeesa킵eoen
‘니八닌O31dpapoeoleoeO슈
｀니-U18UO4000UapaoaUaUap盼
白！npll7d컁ee007eoee仇
凸U楡길od긷onp츨‘eeaoapaO0ea긷功
O－너008eea긷oeoeodoe白
구0000d컁200'oeoeo功
汕UOa깅뎌U09仕UO뱀‘Oap00荏pa
·aUd킵。킵nod딩3070e0eea
白UOU0aUO0la긷ap00en
、－山的盼ㅃ冊이E9開円開開eoee開勵
l:lcl脯開腑洲四開ee開脯eeee觸ee애鹹
舶騙）的脯盼0O盼槌le盼盼도ee盼盼鹹
卽螂이盼배卵恥幻盼盼eegEOe盼ee鹹
아e6이배에매柏70
걔盼卵배盼盼盼韶
'bZU0apeo
ㅓㅗd70dp白pa다趨U
仇貂騁비腑恥開舵Zr-'
-''O뺑‘OOa딩on긴nUd긴ao色U色U轟다n
V*'aoeapeeO00O000ap白
a팅aUaUn디npon딩n킵nUaUnUnUaUn딩n터l
ㅔ鄒猥舞鄒鄒跳驪
··t.I-：미·맛恥切父닷닷螂駝駝卽
·-UU·Ueoeeeeap습
거너I-UoaUa긴aUnpnpdU蠱
COmman(
沔b;e心諭솟；，奇戱“

Ok

1. **Registering the program**

시스템 생성 대체 텍스트: ［탄＇’륵
Fie E’뉼t
ㅌ O
드 On
-- - . - we
』뻐■．■，·■탬매．'
】 ''。
〔그口回찌
■·■
Last
H뻐p
녹
EVentS
Registratio
。
쟈．nk取빕H낱山hqPCZ鞠團활레닒qHㄽ公·肥Z』
＿희
U「nal
PCZAnswering"achinertlllS始
lim沈vers馴fo『3O-day'
7EI
F----―닐
Re휴沁nsem。de
Hh노샐
rMan
! 호
QD
Last
功day
LOg
Saved
Recydebi「
다
l)305ec。찼hme55agebmit
기3αmtactsatn날恪t''''
InordertoconbnUeer醵ylngthe
so轍白rey。uneedpurchasea
竇cense.PCZAn跳燈ringM＇贓ne
2.0-Pr아님sslonalEditjonisn。w
아눈redatgreat床媤e:35USD
拓rakense-Indu（노ng헤the
徒atore',賑찬恥넌叩曲t"and
낵聊rades.
Theappknowsatstartupthat
wearenotregistered
―麟
BTW,th1515
askingtㅇ
anagSCreerl,
register..。.
1f누om30daysofuse.
Reastrabon卜눈y:
- Try -IR에匕ter" 이（ ㅣ
3l蹈512005-O十S9
OltemS
Unels아번n·ready拓rrec터venewcall$

And run …

The app knows at startup that we are not registered

BTW, this is a nag scree, asking to register ….

실행하자…

처음 시작할 때 이 app은 등록되지 않은걸 알고 있다.

By the way, 이 nag scree은 등록됐는지 물어본다…

시스템 생성 대체 텍스트: ．一■■■■■■■■卜
써미騙
V빈W
TO하s H러p
Z 녹
RegistratiO
勵怜찬erI이구 ㅌvents
Llrn
亡ueeㅓ더
「Han
QLast
DTI업ay
稷LoQ
聊Wsav出
닝Recy蘆노n
호
PCZAnswerin0Hachinerull'袖
．·m枕vers馴fo『3O·山·y'
1)305ec。ㅆ요sme55agebmit
고）3contactsatn날》st
InordertoconthueenJQ"ngthe
so轍恪reyouneedpurchasea
竇cense.PC2AnS'l찮eringMaC練ne
2.0-Prof님s돠。rlaIEditjon眈n어｀
Of什戚e山六greatpr匕e=35USD
拓rahcense크ndLJdlng레the
돋atures,卜돋址泌叩datesand
嚥빙rades.
흴hb汕
Andthere15only
(nonam익
One
nO
Regkeyaskedfor
nothing·．.)
1f누帆3【】daysofuse.
쟈瞭夔트옛“y:
Try
-R에匕ter" 氓 ㅣ
31蹈
...that15
ir1Stal1edat
the"
first
uniquekey
program's
"calc미atedand
Startupofcourse
erlewCallS
뗀뺏＇무뗀「변뗀·므
印〕汪.r이
더尸'-:-

And there is only one Reg key asked for (no name, no nothing…)

...that is the "unique key" calculated and installed at first program's startup of course

그곳은 오직 하나의 reg key가 묻는다.(no name, no nothing)

그것은 "unique key"로 계산됐다. 그리고 첫번째 program이 startup 될 때 install 됐다.  
*번역 주)즉, 딱 한 개의 key만 있다는 뜻이다. 예를 들자면 사용자에게 이름과 주소 등을 변수에 넣어서 unique key를 만든다면 이름이 영향을 주는 요인이 되겠지만 여기에서는 영향을 줄 수 없다. 왜냐하면 이름과 주소를 받는 변수가 없기 때문이다.*

Go for registration :)

Try the key!!!

등록하기 위해 가자 :)

Key를 찾자.

시스템 생성 대체 텍스트: 風PCIAnsweri
ㅆ邵hine1.0·p『OfeSSIOnalEditiofl
1■■■■【
F렙e EI査t V'ew TO하s
[ 。 ,璲
i on 삽怜wenng
墜竺夔느／= ｀뗀크즈
－으쁘【쁘브쓰쁘으쁘뜨－坐변인으－-
rMan
QLast
DTOday
「르Log
미W勿v出
냥R띠蘆b「
PCZ^"sweri미결Hachinertjllsh
Iim沈vers沁nfo『3O-day'
l)3osec아넌smessagebm枕
Z)3contactsat尸－-
Re휴沁rlsemㅇde
PCZAnswehng糾achine2.0-Professi
50,whatdoyou
thinkabOUtthat?
!-- J．··■■·．．■．■
·· :후
Its ·、
L엥en
紮Reg伽勸SucCesS
Let'5re$tartthe
apPlicatiㅇnand
Seeifit'5Sti∥
re91stered
1f山m30daysofuse.
Re며，tr비＇onK뇬y:
********솥L솔*****
I Trv HRegister」l oK I
O:（》《》：O《）10：《》《）:（》《》
3110512005·04:S9
O!tems
Unets。pen·ready拓rreceivenewc혀15
미

So, what do you think about that?

Let's restart the application and see if it's still registered

너는 이것에 어떻게 생각해?

Application을 restart 해. 그리고 여전히 등록됐는지 봐.

1. **Testing the registration**

Ctrl-F2 to restart or click here…

Restart 하기 위해 Ctrl-F2를 click 해.

And run or F9

Run이나 F9를 눌러.

시스템 생성 대체 텍스트: 며PcZAn＂尸ring物chineZ·0-ProfeSSionai［出b에
.＂떼더
F렙． Edt V반w
Toa눕 H轍
r 녹
An孰enng EventS
閤
Nofke ACCeSS
驪
익
S.arCh
0
COntaCtS
ㅇOPbonS
巾
」Ourn님
' 후 D
From
Re《e'ved
듸）On冬e
Re繁）On引
mㅇde
卜＇ff ㅡ
八뱀O ㅡIn
I ( ㅡa
ㅡM
Last
功day
LOQ
Saved
Recydebi「
NOitemS
나
HehelNomore
nagscreer닌!!
杖UpJ나
甘卜4XDD넒臼
H-
O:（》0：이》10:（》《》：（》《》
31蹈512()()5-O十S9
OltemS
녜녜려

Hehe! No more nagscreen !!!

헤헤! 더 이상 nagscreen이 없다 !!!

:)

:)

시스템 생성 대체 텍스트: 「독〔p「一一一一一一一一一一一一一겸‘「一一一一一一一一 一一一一一一一一一一一一一一一一 一一一一一一＝ㅌ＝7르
〕．PC1Answe∥예麻hine2．ㅑPr酵es爽na'tditi。n
,一J戇， ,－、一,
욥r一一一一一一컨」
∼ '' 닒
Too柚 H뻐p
鮮 녹
I쵸一－盧L 團 蠟 'a
샬많werlnO
Even佐ㅣ며戱沁ut
－喙，
Last
〔Han
QLast
DTI업ay
變Log
刪臘sav出
닝Recy蘆b
Teley
PC
.· 0...0. …000.. 0·O
ReS床msem。de
Okl!!Everythingworks
fineㄴThatbringsustothe
seCondpartinthistutㅇrial:
reVersingaVBtargetwith
NuMega'sSmartCheck
미루Wenng
m■ne
..ProfessionalEdition
COOvr냠ItD20（》ST뇬논y-T뇬뇬山onyAD이icabons
httn：什www.te논v，α驢n
O:（》（》：《》（)10:（》《》：《》《）
뱀■■
3l蹈512005·O수59
OltemS
Une.。pen-ready拓rrecefvenewc혀15

Ok!!! Everything works fine.

That brings us to the second part in this tutorial : reversing a VB target with NuMega's SmartCheck

Ok!!! 모든 게 잘 됐어.

이 tutorial의 2번째 part를 가져온다. : VB target을 reversing를 할 때 NuMega's SmartCheck를 사용한다.

1. **Configuration of SmartCheck**

Hence, we come to this new "old" program: SmartCheck from NuMega.

그리하여, 우리는 새로운 "old" program을 가져온다 : NuMega에서 SmartCheck

This program was made specifically for VB debugging and reversing.

이 program은 VB debugging과 reversing에 특화되어 만들어졌다.

After installing, SmartCheck is not well configured.

Install 후에, SmartCheck는 잘 된 설정이 필요없다.

It needs some finetuning in the settings and the configuration, and that can be rather annoying.

Setting과 configuration에서 약간의 미세조정이 필요하다. 그리고 꽤 짜증스럽다.

That's why I will show you here how to do it. So, install SmartCheck first and then load a program in the tool.

SmartCheck install 후 이 tool에서 program을 load 했을 때 제일 먼저 어떻게 하는지 너에게 보여줄 것이다.

I have chosen the same target as in the first part in this tutorial.

이 tutorial의 첫번째 part에서 비슷한 target을 선택했다.

Remark: I am doing this on a different Computer: on the first computer, PC 2 Answering Machine is registered :)

주목 : 나는 다른 computer에서 하고 있다. : 첫번째 computer에서, PC 2 Answering Machine은 등록됐다 :)

Loading PC 2 Answering Machine Pro

PC 2 Answering Machine Pro을 Loading 해.

Loaded but automatically minimized

Load 됐다. 그러나 자동으로 최소화 되어있다.

시스템 생성 대체 텍스트: 섶Nu練伊s颱rtchec〔PcZ새2-PRo.exe-programT"ns
秧Edet勸戚·windo*Heb
브의희*沙t FS一7크꼬희그
Event醜여xting
傘嫩쟈’...

:)

시스템 생성 대체 텍스트: ^dvancedS6tbn鱗
―너Repoltefl여5caused야며helellofs
巨Re［沁l·eflofsevenifno釵시Icecodeisava괘able
혀庶｀'.
타DrDete
S
a楙肥tc
Sehnds
球珊ofe。
蹶l
EventR얘uPS
「ROllUP轉｛cateef慨＄
「R애uPdu야開柚Ieaks
「S叩Pr이sdu山cateerro"an이e
Usernu祗이echecklngalgo"thm
Seetheright
corlfiguration
．」‘옵춈눕‘
【군APla
Checka"heapbk(k"meach薩紬聊硼醜「히
ov히w楸e飇mo며w洲f비pjtelnuPOndeailoc찮Ion
rrr
「ReP아t
Guald聊es FIIcharaclet
「긔 Iox8F 麟ol:'
ed
빼
「Savet
Pefformanceo翩麻za劤ns
FCachePlogl柳eyenls
「SuPPles＂艸始mAPI예d0LECJb
「Defel〃。以am＇야녜sun테proglarnlelmhjes
S嫩bngs
H히p
Canc미
H히p
■■■탭■■

See the right configuration !

Configuration을 봐.

시스템 생성 대체 텍스트: PCZAㅆ2--PRo.exe-NuㅆegdSmdrtChecksettin苧
師瞰嫩，on跡嫩凶―태est。∼ㅣ帥r勿飇∥。n-恥阿I쟎。―
回回
SmartCheCeckw래n呱히盼be鑒nrepeftirlgeverltsanand毓rofshlmediat냠yafteratafbngt닝
PrDgrafn.麗youwou너ㅣ敷et。여）nt繃wheneventrepoft．이戚비5.deartheSett「9bel。w.
巨StafteverltreP아bngwhenstafbngtNsㄵDg闡
飇凶dadditionatevents
Inf。rmatiOnab（씨ttheeverlts
。r’胛沈珊寸叭n醜aseth,
Selecttheev軾ItSyouwou紀
ㅜhisarethe
settingsherel
IiagrD'ng財뻐ems.恥【
;a뙤tnportseverltS
rePOltS.
FRePOlt劤n（펴edVtsㅃIBa鄒띠山me一
巨PeffOㅃan아出afhan래ed切suaIBa'c띠山mee而B
「RepeltMo"eMoyeeventsf山mOCX。넜따15
巨RepeftWhdowsmessa야s
巨RePortca沁ackandhook釉祉力on$

This are the settings here !

이 setting처럼 해.

시스템 생성 대체 텍스트: PCZAㅆ2--PRo.e粉-NuㅆegaSmdrtCheckse苗n鱗
囹因
師瞰嫩．on跡吻―ㅐest。
I飾r勳飇轍on-綸胛ml珊。-
Sm鹹Chececkw미n아malfybe)nrepeftrge
한Dg關．驢yt지woL」dl余et。여）ntrol뻐쑨
sand卽아s紬油硼atelyafterstafbngt닝
\-－∼ㅂ－써山e괬「gbel。w.
巨＿一evr璽맨enstM
一f'tㄻ매Ion히eV헤’ \
InfofmatiㅇnabOLlttheevefltsbe紬W
LeaVethistab
alone:it15not
importantforus
財。비em$.恥t
can＇胛祉珊寸聊n醜asethedISk叩aceused嫩SmaftCheCkasit懲Po劤ever曲
SeleCttheev軾ItSyouwou陋耿eSmㄼtCheckt이ndUdeinhrePOfts.
F
飇凶d砧n（최edVtsuaIB해c띠ntlme一
FPelf師an아出afha祗led切suaIBa'c띠山mee而躇
RepeltMou,eMㅇveeventsf出InocX이蠟祇s
RepeftWilldowsmeSSages
RePOltcallbackandhookfunctlon$
rF巨
「－--－仇I繃ujerenl ㅃp-

Leave this tab alone: it is not important for us

이 tab은 건드리지마 : 이것은 우리에게 중요하지 않아.

시스템 생성 대체 텍스트: l
PCZAㅆ2_PRo.e騁-NuㅆegdSlndrtChecksettings
Onlythe3thatyㅇu
SeehereneeCltO
beCheCked
끼因L--
勖r瞰出．onI腕嫩삐紬to∼勖rsuo畔騶onHro"m雨-
Avaiiablesup庠e騶。nlib闡es
난벵더쬘뱀닙탭■■■■■■■■■■■■■．■
E써찌JBaK6.ORun卄陋凶．y써SVB＼여60.DLL)
M새su닒Basic6．【》R嶼卄油凶faly斗eedEflhanc柳“胸
Su야D＂。mtems
lT辦e l眈ati굶
lscoPe
C。mm슨m
-
漱」dAPIFLIn功On...
싸rule砲n

Only the 3 that you see here need to be checked

오직 보이는 3개만 check 해.

시스템 생성 대체 텍스트: PCZAㅆ치－pRo.exe-HuㅆegdSmdrtChecksettin鱗
回因
飾r瞰緘．onI跡嫩凶IFlesto∼枷rsuo幟緻onl綸嶼雨-
Avai:a以esup댜郞휘。미心nfie$
l·「焚村命尸－---
탬새利aIBa鷺6.ORUnT’臘나》m·신SVB＼여60.DLL)
FM헤alBas￡6.1)RLjn卄船U)rary瘢eedEr슭anc뻬ent$
AnClleaVethis
tabalㅇnetㅇㅇ．
Sup댜·＂。mtems
-TvDe ㅣLocatI0n
SCope
-一 一 一 一 一 一 n
功mment l
- oKI肋ujeren-__ㅃp-

And leave this tab alone too.

그리고 이 tab은 건드리지마.

시스템 생성 대체 텍스트: FㅐeEI노tyiewPr여r勸Wi沁。wHeb
브의희
－크브꾀꽤히최홰고」희ㅍ
Atthispoint,youneedtorunaVB
eXetㅇchangetheothersettingS.lf
yㅇudon't,sㅇmeoftheConfiguration
isgreyeclout,henceimpossi비e

At this point, you need to run a VB exe to change the other settings.

이 point, 다른 설정을 바꾸기 위해서는 VB.exe를 실행해야 됩니다.

If you don't some of the configuration is greyed out, hence impossible

그렇지 않으면 구성의 일부가 회색으로 됩니다. 그러면 불가능하게 됩니다.

시스템 생성 대체 텍스트: ^
fN。山柚lsl

Right. PC 2 Answering Machine is running. First of all, make the "Details" window visible if hidden.

좋아. PC 2 Answering Machine은 실행 중이다. 첫번째로, "Details" window이 감춰져 있다면 보게 만들자.

시스템 생성 대체 텍스트: 젱츄츄홀츄
'·*춈*
<,JU
2738
2746
2754
2花2
277n
<.11
니nelnpulf'Um"n【e며밧：니
r淅石죠福딩。U。。eFile;':'wind。w
butfㅇr
reversing,wese-domlyneedthat:)
n한표여Um『眈e嶼『
．츄lin써n대ll勵Imlㅣ않。r'.1
녹갇l
굽鶯돛李
』Ul
」1 》
'닐｀ㅡ-O
'J一-N
Fo[H이pPr醜sFI

This is the "Source File" window, but for reversing, we seldomly need that :)

이것은 "Source File" window다. 그러나 reversing을 위해 좀처럼 필요하지 않다.

The event summary window gives you useful info

Event 요약 window는 우리에게 유용한 정보를 준다.

시스템 생성 대체 텍스트: P〔Z춈ㅐZ＿며眈》·ex.-hoqramkest．眈｀-Ev레tSUm耐rV.a
22X
0.
0枋
El『이s
Resource,mefno汐，andOLElea盼
Han래edefforS
rL P'
0
1058
7
16
6145
2
20
12457
113
1
1
206
0
1
onElrolsandRes내ne숑
TheeventsummaryWindow
giVesyㅇuusef미1info
切糊히B邵始해凸써沁owsAP!lurlCti예s
obiecteven盼『‘ck,Load,ACtiv楸e..]
M남h出s,댜OP텨砂getsandPI叩el砂sets
Va勵ecoef改m
FofmCleal沁n
COr山olclea出n
APIcahf'omCC++andSystemcode
OLEme小odc래15frolrIS忖emcode
Thre.d랐헤s酌dfe戮〃r"s
Ev레hep이＊샀art／삵OPe臘祉s
Wind。wanddial에mes拓ges
HOokS
COmme祉s
or:Hetgegevensgebieddata예eerlsy
07F
ErisgeP『Obeerd糖vefwi脾卽naareen
D:00盼0000,D닢t)RD:00020이9,PTR:
egerl,InI텨Xr:1023.1楸톄e「이
RD:0000()0()0,PTR:0이2FB78,PTR:00
轟균β'^다=◆콴數넣버J7
ger:1,In聰畔「5000,―쟎e鱗l：이
M뻬아yu裙d［聊郞】

The goal for you is to see all these exactly like this.

너의 목표는 이것들을 정확히 보는 것이다.

BTW, I'm using SmartCheck v6.20 here.

By the way, 나는 SmartCheck v6.20을 사용한다.

If your version is different, it doesn't matter: you will easily find your way too because since version 6, there are no big differences.

너의 version이 다르다면, 문제없다. : 너는 쉽게 너의 방법을 찾을 수 있다. 왜냐하면 version 6 이후로, 크게 다른 점이 없다.

Notice also that I have the "Sequence Numbers" checked. I find this useful to find my way in the code later.

"Sequence Numbers"를 check 했다는 것을 알린다. 나중에 Code에서 나만의 방법으로 이것의 유용한 점을 찾았다.

We will see further that it is really easy to drown in the tens of thousands of lines of code without it ….

수 많은 code에서 쉽게 구별할 수 있다.

시스템 생성 대체 텍스트: 殼씁踪큰樑쁜夔쁘
브뾔壅ㅌYent一y
會닷期｀탑rorsandLe괌s毓캬
飾메＇째Events
孰아＇Errorsand象eof裙
勵희희
轍爾짊
192
380
388
419
1514
19겨
2327
2339
2427
2431
2491
2496
2521
2536
2559
2581
2636
2678
2683
2689
2691
2701
2708
2716
a'a괘
훤山仗Evenb，··
낟Ar화洲ents
궂SegpenceNufnbers
낟훤叩ressedErrors
내陋샀1,O닛【
0x00000()00.
d嚥0CD0000〔
石FL
Jmen叱1,LOD:-
』山盼00000()00ㅣ
Co岬banceR력＂rt...
Ver＇에In뇨ma敏＂
betUfnsB00L
虛섭--!1!I겨놈눕눕겨눕·*·*솔
B
이‘래’l:Tl니e
alx:0이66DE4,
氓nZFBAalon
틈＝터，and魅
麻pa며Brㄺch
노以腕燈ㅆ
여．Ia陟e6ran出
TO혀山rs...
7Status申r
6F24
8.1아、
닐이1
[".1·ㅣOng:'j
··…*…*··
.
-k·乙
Pref눙ences...
l衲」""솥kl..mn"'‘∼·＊1】

Go here

가자.

시스템 생성 대체 텍스트: 跡ecifiC[yents
隣兩祗珊而困俎百盼菰〔…－」J츠ET긔
더거andedeffolspnEI＇驪』R爵Ume] ^
MV轉uaIBa쐬cand닢ind이새ㅎAPI柏nct沁nㅎ
넌obiec〔evenl$【Di改，Lo毓】，ACtiv레e...]
-－肱lgeㅣ
-
MM戚h。巾，PI。p이
MValuecoel嫩m
MFαmclea山n
MCO∥lola늉汕에
U昉aks
砂getsa
Checl이ikethis.Theseare
臘聊I theonlytobe。hecked
alsㅇWhen
I디API閃Isfl帆C,C++and하stemcode
「勿山山alnew兩崗。麟
scrollingdown
노낟

Check like this. These are the only to be checked also when scrolling down

이렇게 check 해. 이것들은 오직 scrolling down 할 때 check 됐다.

시스템 생성 대체 텍스트: EI꾀츠I쐬끄汀r」」희표
뜨＂ \\
v겼’邯19：∥「43 :______\'
ㅆafgumeLnt珊H뻔D:山「FF「FF「믹
‘毓gUmentl·미呱汨D:0x0000005시
『redox00t刃0[)oaLa샀E"0「Kan。며蹈
u『ned（殃0C000000.Las[I『o「H비畔9
＇여艸ㅛㄴc皿』m凶山7∼－
mentmu혔bebetweenoxo()000000and0x00()()00
빈뻔坐vlㅃenll짇 」
힁geDIeO00【aaneen왱읽eemaan【Oep·5OOOIgDg.
Sㅇfar,ifyㅇuchangedeverythinglikeshㅇwrl,
allShㅇ미dWOrkfinE'CIOSeSmartCheCkand
10
restartandruntheapPlicatiㅇninit.yㅇu
Shㅇ미dther1SeethesameasmEㄴㅜhese
buttonsaboveshㅇ미dbeVISi비eforyㅇutoo.
Bl』

So far, if you changed everything like shown, all should work fine. Close SmartCheck and restart and run the application in it.

멀리 보자, 만약에 네가 이것처럼 모든 것을 바꿨다면, 모든 것은 괜찮을 것이다. SmartCheck를 닫고 restart 해. Application을 실행하자.

You should then see the same as me. These buttons above should be visible for you too.

너는 나와 같은 걸 보게 될 것이다. 이 buttons은 너를 위해 보여줄 수 있다.

Finally, SmartCheck is configured.

Let's reverse the application now.

Take an overview and scroll down.

마지막으로, SmartCheck 설정을 했다.

Application을 reverse 하자.

관점을 가지고 scroll down 하자.

1. **Fishing the serial in SmartCheck**

시스템 생성 대체 텍스트: 쐰r曄畔泡呱啣E璉獅蕭珊碗繡碼닙홑■닙』■■■■■탭「■．
닙」F눈Edit
YiewPr여nmw眈lowH轍
맨．■■．톄괘겹
- 芬X
뾔씌택
의꾀꾀뻬끄邸r그」미코
10618
10626
1【）634
10642
10650
10658
10666
10674
10682
10690
10698
10706
10겨4
10753
10758
10775
10790
10807
10B29
10874
10903
10908
109:25
10940
10957
10979
11020
11050
11062
11()67
11084
11099
11116
11138
11167
11172
1llPq
<
．츄Lin버nPUtNumlㅣ앉egelll
.4Line4nPUtNum(―앉비蹈l：치
．츄LinelnPUtNum［ㅣ않egel:1)
．轟LinelnPUtNum(―앉egel:1l
．츄LinelnPUtNumlㅣ앉이”l·치
＊츄LinelnP야Num［ㅣ샀egell】
．홀LinelnPu刪um（ㅣ않이蹈1.1]
．츄UnelnmtNumll많e塋l·치
．츄LinelnPUtNumlㅣ않egel치
.4LinelnPUtNumll앉egel.1】
．츄LinelnPUtNu삐l않egel:1)
．홀LinelnPUtNuml―않e畔1:11
．츄다。se(―쟎터衿f:1)
．츄onE"olllong:.1)
泗。d戚a蘇］
Quitea-otof"useless"
COdeabOVe.
．흩．洲醜빼여새IANT：세騁四）let녜帆Boolean:Tlue
．츄Re여penK톄以이HKEY:8000()()02.ch鄒x:00166DE4,D\VORD:0000000()00,미〃0RD:00020이9,PTR:0012FB98】，이unsLONG:0
．츄Re氏rnIFLAGs·【）0어）00B0,IOrlg:1,PTR：戚nZFBAO,Iona:1지楸egef:1,Integel:1D23,Inte酸r:0l
．츄Re胛uelyValueE甬【HKEY:00驥】0174,chal'D017EC4CDw0RD:00000凹0,PTR.0012F878,PTR:0여7ED40,PTR:0012F87Cjletur帆LONG:0
＊츄Sp聊e$l跡蟬4】
．홀RegCI이eK래HKEY:OD000174llet내mLONG:0
onElroltbng：·1]
bMissmg여ARIJ식NT:MㄶsfngjletㄵnsBoolean:True
Re胛penK톄E댐떠KEY;8000메D2.chal.:0016앉
Re助m!FLAGS'00()00080,ㅣ아빙·1,PTR：凹1ZFB써
Reaouervva勵eE甬lHKEY:0（勵00174.아녑l쬔001
Space$1bng24] I
ReaooseKevfHKEY:000001741『바u『nsLONG：이
R·嫩陟日ㅣANT,B,Ref하Iing’·2-750402...'I,ㅣon쇼
OnE"ollbng：·1]
Forthetimebeing,
PTR:0012FBgS】媤山msLONG:0
neVermindtheCod타
I'l-tel-yㅇumㅇreabout
R:0[n7ED40,PTR:0이ZFB7C】l이u『nsLONG;0
theCOdeintheneXt
partinthisseries:)
hMissr聊AR닙NT[M鱗山h비嗽5soolean:Tfue
RegopenK하E얌HKEY:8000凹02,아ㄶ1.:00166DE4,D\V0RD:0000000氓）0,D\VOR以0D020019,PTR:0012FB98】letor
Re腕n[FLAGs·凹000080,I떼：1,PTR：凹1芥BAO'I예912.nlegerl，ㅣnteg하：1023.Inlegel：이 /
RecI0ue『vValueE甬IHKEY:00000174.하ㅒl첫0이7EC4C.뎨V0RD:00000000.PTROD12FB78JPTFLO이7ED40,PTRI
ReOCIos야길evflㅓKEY.00000174lle蠟umsLONG:o l
OnErr。r【IonC-11 [
IsMiss．卵蠟RIANT;M椽輧놀g]＇비JnsBoolean:T『ue 、
Seehㅇweasyit15todrownin
theamOUntOf22840eVentS!
REMARK:1pressedthe·。
p。nn灐hr허下v쇼f니K「V·요床n饉놀n夕사pr勵nnlRRn「4n＼緘nPnnnnnnnflnn以Inpn·汀贓IX놀nlqpTP·nrll夕「R年n『츨h'n*In시nn
츄츄轟츄츄츄츄轟轟츄轟츄츄轟츄츄轟
수·…수…수+··+··、
x。eSU嚥zjㄿD- 一
l 》
→‘욥홑홑＝‘■■．－·－-
FofHeb,Pr郞sFI
Prog『柳Blent驢22840

Quite a lot of "useless" code above.

꽤 "유용하지 않은" code가 있다.

But here is the start of the "real" code.

그러나 이곳은 "real" code의 시작이다.

For the time being, never mind the code, I'll tell you more about the code in the next part in this series :)

시작하는 사람이라면, code에 대해서 걱정하지마. 너에게 이 series의 다음 part에서 code에 대해 많은 것을 말할 것이다.

See how easy it is to drown in the amount of 22840 events !

얼마나 쉽게 22840 events를 보여주는지 봐라.

REMARK : I pressed the …..

주목 : 나는 눌렀다.

시스템 생성 대체 텍스트: 희희쐬희可r스l－시미큐
...''Endprogram"buttonwhich15here·
Ididthis(butremㅇveditfrㅇmmㅇVie)
because1onlyneedthebeginning
ofthecodeforthisapPlicatio『1.
ir『lot,itCo미dhavebeenasmuch
as1.5m∥＂에eVentSn!

… "End program" button which is here.

"End program" button은 이곳에 있다.

I did this (but removed it from movie)

나는 했다.(그러나 movie에서 삭제했다)

Because I only need the beginning of the code for this application.

왜냐하면 오직 이 application의 시작하는 code가 필요하다.

If not, it could have been as much as 1.5 million events !!!

아니라면, 나는 1.5 million events를 봐야 한다.

시스템 생성 대체 텍스트: 10618
10626
10634
10642
10650
10658
10666
10674
10682
10690
10698
107D6
10겨4
10753
10758
10775
10790
10807
10829
10874
10903
10908
10925
10940
10957
10979
11020
11050
11062
11067
11084
11099
11116
11139
11167
11172
1llRq
《
훵7
걘닙
n邙
4츄츄轟츄츄츄츄츄4츄츄츄츄
··*·수··춈·춈수…
令穫―洲灘mqL'ID칡。∥．]m祗】」lelu帆Boolean;T'ue
빅∼ →劇 n_-r、－__'_‘「..^"·L.「u.^^nnr낢、n'-L__'.n^,츤「＾「』
AndSeethatalleVentS
are『lotyet
disPlayecl!Seethe
"gaps"betweenthelines.
DW0RU00000000()0,미V0RD:00020이9,PTR:0012FBgB)I이unsLONG:0
＼지nlegef:1,Inlegef:1023,Inleger：이
W0RD:00000凹0,PTR.0012F878,PTR；嶼n7ED40.PTR:0이ZFB7C】le山mㅎLONG:0
느ㄷ e p e n
hCRCJRO
츄츄츄츄츄
수·*··
．츄―洲躇鏑嫩一何一”刪卵∼祇祇一－。「→／
．츄Re胛penK톄E삐H旺Y:80대）嶼】02,chal.:00166DE4,D＼硼〕RD:00叩000며）0，야田R以叩020019,PTR:0012FB95】廠mLONG:0
．츄ReD빼FLAGS:00000田D,ㅣ아빕：1,PTR：咳nZFBAO.ㅣ예Q:1져톄eg이1,ㅣ楸eger:102치nleger이
．츄Re蝦ue따lalueE觸HKEY:00000174,야녑l댓）이IC4C,恥VOR以00미）()000,PTR:0012F878,PTR:0Q17ED40,PTR:0012FB7Cll이urnsLON以0
＋츄SPace＄嫩叩：241
．츄Re聊O裙K하IHKEYㅍ000001741，비urnsLONG:0
.4R·ght陟떼ANrB거ef하liny'2-750402·．.'I,Iong:7]
＊츄onElrol【bng:.1]
．츄hMissrglvARIANT:Mlss凶］fe＇ㄵn$BOolean:Tfue
．轟Re胛penK톄E댐떠旺Y:8000凹02chal.:00166DE4,D＼艇m以0000000凹0,眺｀0RD:00D20019,PTR:0012FB9B】letu帆LONG:0
．츄ReD빼FLAGs0000000盼0,I아빙1,PTR【）D1芥BAO,lono:1지nlegerl,ㅣnteg히：1023.Inlegel:0l
．츄RegQue뗘IaILIeE殲HKEY：匯勵（)0174,래鄒첫0017EC4C,恥VOR以00며）0000,PTR0012FB78,PTR:0이7ED4D,PTR:0012FB7CjleturnsLONaZ…
．츄RegClos야q톄IH旺쪼0嶼）001741letur帆LONG:0
．츄onE。rol【bng-1)
.415세“．聊ARIANT；恥驪．삐let曠nsB祇ea庶Tfue
'4p아。灐굻숴下v酊니K「v箴mn汀m)사ㄵ，'nn1R戚『4n닙InPn·nnnfmnnnnwnpn汀n게mqpT.nnl夕「R驢、，이．,n,In"G.n v
l 》
n^^.1수·

And see that all events are not yet displayed! See the "gaps" between the lines.

모든 events는 아직 display 되지 않은 것을 봐. Line 사이에 있는 "gaps"을 봐.

시스템 생성 대체 텍스트: 빽치U〔긔＿」미J
That15becauseonly''Errorsand
SPecificevents''areshㅇw『ㅏ

That is because only "Errors and specific events" are shown.

오직 "Errors and specific events"가 있다.

*번역 주)10758과 10775 사이에 있는 차이를 보세요. 그 안에 엄청 많은 event와 error가 있겠죠?*

시스템 생성 대체 텍스트: 뾔뾔택
프그一l쬐’」調。」」희ㅍ.'
_l[
겯닙
놈■■J 令■．구 훰·■구 ｀■■J 님■■겯 겨■·J ｀■·■r
10658
10666
10674
1()682
10690
10698
10706
10714
10겨8
10719
10720
1이91
10732
10737
10745
10750
11)753
10758
10759
10762
10763
10764
10765
10766
10767
10775
10776
10779
10790
10796
10799
10507
10808
10811
10821
10824
InR夕q
《
X
Un이야시씨um
Un이야시여um
Uneln凶礪um
Uneln
Uneln
며여um
PU며um
Unel야빕一Num
Uneㅣn헨〔Nuln
Intege
Inbge
디osellnte畔rl】
＿祉n돠［m며Shing;''RT
＿祉n티嫩Ploct】『버uln퀴
田曰田田田田田田
Ok.AI-eventsareshow『1.
_vbaFleeSI心샀D『etvfn
vbaFleeobLPINTER
Weknㅇwfrㅇmstartupthattheprogram
verifiesthellca-cu-ateduniqueker.
vba하l
祉n잇I
Co炚
Co아I
余linr”·，LP
slringl”·，LPBSTR:00158)C】'etur帆D\VORD:17EC64
沁aFlee孰f.PBSTR:OD12FBB4jlet내鬧미VOR以10
vba닷rC아聊（Strin『’SPaceK톄”',LPSSTR:O이2F880】retuf帆D\VORD:16F花C
-ㅡㅡㅡㅡ
onElfolllong:.1]
-sMi驪h刪결R-ANT；쎄驪hgjrehansBoo始a庶True
ltclm閥珝Jel「什ARIANT·Bo허eanrT『ue'W떠ㅣANT:ErnP砂，vARIANT:Misslng】媤h'ns盼VOR[)12FB40
＿沁WefM。ve泌식R너NT;Emp砂，vARIANT:E呻抄）retulnsD\VOR【）:12FB88
_vba하ICaUS輛ng:’삿．,S驕여r’드OFT＼曄隅E.,.'')feI驪nㅎD\VORD:16F65C
_vba딧IMQve【gnng:'80FT\W'RE.”·，LPBSTR：凹12FB68】retu『ns미頀】RD:16F65C
＿沁ba하ICatlSlflng'”·，잇＇.y.SOFTWARE...'1『이urnsD\VOR【）:16F7B4
_vba닷IMove【S輛어r'SOFTWAR〔.‘·，LPBSTR：凹12FB64lreturnsD\VORD:16F7B4
＿沁ba하IT쑈ns빼Strlng:''SOFTWARE...”힝LPSTR一0이2FB60】retuns미VORD166DE4
츄轟츄츄轟츄4츄 츄츄
·…춈·춈····……수
巴 떠田田田田
*+·***·
曰 田
．轟Re胛penK태E삐HKEY:80（〕00002,charx:0이66DE4,대VORD:00凹00叩，미VR以00020019,PTR:0012FBg히re眈nsLONG:0
円. _vbasetS뾰tefnElfo『0『戚ul帆미VOR以153258
녠◆ _vbaFleest心510『이ulnsD\VOR［떠0
디．츄ReD빼FLAGS:00()00080,―예g:1,PTR：暝nZFBAO.Ion이7,Integef:1,―톄예ef:102하―비eg軾이
미. _Vb펴砂Lock【lre柏InsD\VORD:17E이8
田. _vba하IT섐nsiIStl豹g:''Spac軾하’·，LPSTR·：0012FB68】l戚내ns마旺mD:17EC4C
．츄R테QuelvvalueE댐IHKEY·叩000174,ch히x:D017EC4CD\VORD:0000000qPTR:0여2FB78,PTR:0017ED4aPTR:0012FB7ClretIJmsLON
V
일r
m+ ＿沁as비S螂뻬Elro心let내ns미V0RD:153258
田. _vbaSllToUnlcodelchal쬔0017EC4C,LPSSTR:0012FB80)letUfnsD\VORD:16F78C
m. _vbaA聊」nbckmetumsD\VORD:0
田. ＿沁祈『ees벼LPBSTR:0이ZFB6히rel녜nsD\VORD:10
m‘轟qn力＾츨劇卜－）시
Re'UltS
臘F［聊르；「－

Ok. All events are shown.

We know from startup that the program verifies the "calculated unique key".

Ok. 모든 events를 보여준다.

우리는 startup을 알고 있다. Program이 "계산된 unique key"를 검증한다.

시스템 생성 대체 텍스트: 뾔뾔희「
긔
旦꾀꾀끄F브」」」미큐
10658
10666
10674
10682
10690
10698
．츄Unel먀시tNumllnte醉l:1]
．轟Un이n凶tNumtlnt이渗r:1】
．轟UnelnPUINumt＞논－놉
unelnPUtNu야
Un비nPUtNu뼈
UnelnDU(Numl
SO,
SearCh
-et'sSimPly
fㅇrtheAPI....
4츄츄
…
떠디田田田田

So, let's simply search for the API ….

그래서, API를 간단히 검색하자.

시스템 생성 대체 텍스트: _vba'V驪T：텨
첵츠―翩竺
프F'
스니희J
Uneln헨며umtlnteger:1
Lin이n凶여umt―야
Lineln헨tNumt―어
Lineln凶뗘umf-m
AnCISearCh
fㅇrtheAPI
:-｀·－∼.''..．∼lI一트∼→一ㅏ
츄轟4홉蠟

And search for the API

API를 검색하자.

시스템 생성 대체 텍스트: 녜뾔홱．·圃廠驪’
-－고삐繃삐끄百副」」희J
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
190B
1909
1910
1911
1912
2318
2326
2327
2333
2334
2339
2344
2345
2350
2353
2358
2361
2362
2363
2364
2365
2373
2374
2375
2376
2377
)17R
v畝u비ProtecqDW매以01761)00qD＼써〕R以凹0[)6000,맸GE_FLAGSO()000()04PAGEeeREAD\VR댜E,PTRO[nZFE30)漱u＇祇BOD너 ^i
G비Cull예tPfoc야솨】fetufnsHANDLE:FFFFFFFF
RushlnstIudionCachefHPR0CESS:FFFFFFFF,PTR01760000.D눠IORD:0며〕0600이＇려u'nsB00LI
V畝u긷』oc(DW0RD:0176이）oqD\VORD:()()007000,MEM_FLAGS：이）0이000:MEM_COMMIT,PAGEesFLAGS:0000()(）【）4；댜、GEeeREA［略IRIT
V畝u瓣내oc【邙V0RD:0176驥）()0,미VOR以00008000,M다쎄＿FLAGS00001OO［】：MEM_COMMIT,PAGE_FLAGs:00【）00004:R垢E_REA［山．IRIT
He쑤학Ioc(HANDLE:01620000,FLAGS:t)00며）叩8,미V0RD.000000D4h아ufn$LF쩍l미D:1634C30
V嫩u頀Joc【미V0RD:01760000,미V()RD；여）009000,MEM_FL섬一Sㅍ叩0이【）oaMEM_COMM-T,PAGE_FLAGs:00며）0田4：앉心EeeREAD\VRIT I
v"u小‘ㄸ【Dw0RD:0176刪qDw0RD：예仄념000,ME시weFL시拓「叩00100αMEMeeCOMMIT,PAGEee汕Gs‘凹叩0004'PAGE-READwRIT -
v"uaIPr야eCqDw0RD:0176000qD＼戚꺼u凹ㄸh000·PAGE--FLAGs:00000020:PAGE-.E×EcUTEeeREA［기PTR「oo1芥E3미I바urnsB00L:1 -
G비Cu"entP『oc螂s(lfeI내nsHANDLE:FFFFFFFF I
Rushㅣnshu이ionCach터HPROCESs:FFFFFFFF,PTR.01760000,函VOR以000야노（)0이lelum$B00L:1
Hea벼IoclHANDLE:01620000,FLAGs:0()000008,미V0RD:000023EC)『비ulnsLP낟01以1634이0
Hea出Ioc
Hea翩I여
吻Regi做
AndWelandin
thefirstenCOUntered
YORD:o
VORD:0
嶼）0003C)『etU＇鬧LPV0ID:1637108
()000020】letu『mLPVOID:163겨50
S邰Vind軸贓껴r
Re여p卽K卽섯HK
c一ㄺdt] /
汕멩＊BF84.cF138505漱2마，LPINTERFA旺：이63겨54,F며GS:00叩凹01,FLAGs:ot)01
A4]『elㄵnsB00L:1
0()000Zch&쬔66이gFEC'PTR：이겨ZFDSC】retumsLONG:2
*··…수·*·+··*+수·
田田
田．轟
◆ _vba\I毓Ts[qM尸臘NT.strmg"I...vARIANT;COn샀앗兩r＂勿副嘴nsD\VOR以0
田+ ＿沁aF＇締V＆釀汨IANT.5茁ng:'"'l『비내nsD\VOR以10
田．츄CO翩n례배
. ＿沁W〃T쇠Eq陟尸며NT：닷＇mg:'''',VARIANT:COns一닷Ilny"'jlet嘴ns아VOR【）:0
曰. _vbaFI枕V驪M떠tANT:Stling:'''lfet내nsD\VORD:10
田. ＿沁ba하rCo아（軌“이r'PCZAns,‘·，LPBSTR:（】05D80B4]retur鬧D\V0RD:16218C
田. _vba하凸마Flrlng''2.l】．8.2",LPBSTR：咳】SDS414hetulmD\VORD:16D94C
田. _vba璥（螂礪出ng기oe",564...”·，LPBSTR:00508418]letu『帆미V0RD:166泌C
. Hea出Ioc떠ANDLE·01620()t)0,FLAGS：田000008、騶VOR以000仄刃FCI『飾〃nsLPV미D:1637180
. G비Velsi예b씩mTRI)()1ZFA4ClletulnsB00L:1
. G비K하bo'dL斗ouUDWORD:00이）0000】lelumsHKL:8130813
. He쑤새。떠ANDLE:01620驪）0,FLAGS:m000000,盼V0RD:0000000B)『etU『야LFV미11637298
田. 5톄葯ndowT해몌勖刪D：며）碼（)494,LPSTR01637288llet내帆B00너
수 H閔出Ioc떠ANDLE：이620()00,FLAG요며）00000q이V0RD:00000001】letulnsLPV미―16372A0
. Hea出＂oc떠ANDLE；이620驪）0,FLAG요【）0000000.DW0R以卯00000B).etufnsLPV이D1637280
수 Hea벼Ioc떠ANDLE：이620【）00,FLAG도0()000000.D\V0R[X00（〕0000B】＇비ulmLPV0ID:16372C8
수 Hea벼110이HANDLE:01620000.FLAG兮凹0여）008,미VOR以0凹에015jreturnsLPV미―16372E0
. ＿沁aFreeob鱗PINTERFAcE.：驪】12FDZcJ
円' nll「·．츤卜nn「ㅋlf겨rpfl.h층n닙Inpn다괭）「4pPq
괏
X
Resu-t'
송 Evem드

And we land in the first encountered

그리고 우리는 첫번째로 맞닥뜨렸다.

시스템 생성 대체 텍스트: 뾔뙤희同「祉］
긔꾀꾀쐬끄耳희*I.1희큐
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
2318
2326
2327
2333
2334
2339
2344
2345
2350
2353
2358
2361
2362
2363
2364
2365
2373
2374
2375
2376
2377
）슥7n
v畝u히PIOtecqDW매以이760000,미礪mD：凹006()00.P시死＿FLAGS000()0()04PAGE-,READ\VR-TE7PTRO이ZFE30)畛tUf帆B00L:1 즈느
G비Cul『헤＇P『oces헤）re*ufnsHANDLE:FFFFFFFF
RushlnstluCti에Cach러HPROCESS：「FF「「F「F,PTR이760마）0,D\VORD:0【）00600미＇너u『nsB00LI
V畝ua쌔I。c【DWORD:01760D0댜D닢OR以0()007000,MEM_FLAGS：叩0이이）0:MEM..COM빼T,PAGE-FLAGS;00000004：만心E-REA［洲IRW
V戮轍＾"oc【D\VOR［〔이7600t)0,邙VORU以）008000,MEM_FL獻〕S：叩001000MEM_COMMIT,PAGEeeFL시〕S:000【）0釀）4：댜汨E_READ\VRIT
Hea出Ioc(HANDLE:016200DO,FLAG요0()000008,聊VOR以000仄刃D4)felufnㅎLFV미―:1634C30
V낡u瓣새oc【DWORD：이花叩00,미｀0RD.00009000.MEM＿「LAGS.00001000:MEM_COMMIT,PAGE＿「LAUS:O叩00004：탸、UE_REA［羚ZRIT
V옰uJJoc(DWORD：이76Ot)oqDWOR以며）0며0D0,MEM_FL시〕S:0000100以MEM_COMMIT,PAGEseFLAGS:00()()()004·PAGEeeR댜〔）WRIT
V畝uaIP『이ectfD\VORD：여760000,D＼艇IRI>00（心헉000,PAGEeeFLAGS:000（】0020:PAGEeeE×ECUTEeeR티헉〔PTR:0012FE3이＇바u『nsB00L:1
G瓠〕ul『예［P『oc螂솨】leturnsHANDLE:FFFFFFFF
Flushln삵Iu（力예다（h러HPROCESS:FFFFFFFF,PTR;01760【）00,D\VORD:00()0A()00】『비u『nsB00L:1
HeaㅄIoc(HANDLE:0162000【）,FLAGS:0()0()0009,미VOR【）:000023EClle驢내nsLP70ID:1634D10
AndWelandin
thefirstenCOUntered
y0RD:0000003C)'etUl帆LPV이D:1쁘108
胛RD:0凹000zojretulns볜olDI"7150
』0탸누BF84.CF138505〕녹2마＿LPINTERFA다
毓0咳）0()0이，FLAGs:000I
S에Vind軸贓떼m
Re벼penK래치HK댜
〃口醜｀'""m醜沁A4)re眈n
0()0002.ch&뜬6601gFEC,PTR:0(nZF
Studythecodeher텨
··수…수·…수··*수·
田디
□◆츄c一ㄺ배/
. _vbalV毓T삵Eq陟尸념HT：딧ling:‘∥’.VARIANT[COn샀slrinr"1
田. _vbaFI泌7＆眸RㅣANT．恥i凹：'’휜et내帆미VOR以10
田．츄댜mman배
沁W〃T삵EqM汨녀NT：하『．9:''’딩VARIANT:C0n삵하『Iny"1『
vbaFI沈V＆盼RIANT:Stfing걋＂】let내nsD\VORD:10
INFO:
WeW∥1SeeaIOtmㅇreㅇn
VB"COde"intheneXtPart
沁ba앗rCOPI朽trinrPCZAr略．'I,【．PBSTR刀（)5D80B41retur鬧머V0RD:16218C
ㅡ-ㅡ
＿沁as眈Co마（String:''z0.8.Z',LPBSTR:005DS414)let내nsD\VORD:16D94C
_vbastrCOPI朽輛nroeiu·珊4...'',LPBSTR:0()508418】retu隧D\VORD:166沁C
Hea벼IoclHANDLE=0162000驪
G쨋花fsion티轉［PTR.oo12FA4두
G비K水oal艸므岬쯔맥으r
Hea벼Ioc떠ANDLE:01620。이
s棚ㅃowTex며ImvN岬시
Hea벼locIHAN뜨트016젯이
He秘■oclHAN뜨트미6곈0믹
Hea벼lㅇ이HANDLE:0162000헥
GS凹000008,미VORD:000000FCI『et네帆LFV미D:1637180
Butthere15『lotmuch
studyingneCessaryin
thiscase·...Dㅇesn't
this-ookimmediately
verysusPICious:)
ms【．더心ID:1637288
Hea出Ioc떠ANDLE：이620000，枕계「n戚뾰
_vbaFleeob鱗PINTERFAcE";0012FD2c)
nll「．．츤「＾'rㅋIr겸rPh朔죽n＼緘npn·다긔）「4ppq
hsLFvoID:163媤切
麗淵믐擺擢I
山msL더10ID16372E【】
솜·'··…수··*…
田디田田 田
囚 닐b

Study the code here.

여기 Code를 공부하자.

INFO:

We will see a lot more on VB "code" in the next Part

우리는 다음 part에서 VB "code" 에 대한 많은 정보를 볼 수 있다.

But there is not much studying necessary in this case….

그러나 이번 경우에는 더 이상 공부가 필요하지 않다.

Doesn't this look immediately very suspicious :)

매우 의심스럽다.

Mmmm. Expanding the tree doesn't give us more info.

음. Tree를 확장해도 정보를 더 이상 주지 않는다.

Let's highlight the line and look in the details window.

Highlight line을 details window에서 보자.

시스템 생성 대체 텍스트: 키TE'PTRIXn2FE30】le山InsB00너 ^
PC껴MZ-PROE×EIO이BBFE미nodebug
츠uns跡ed功驪tㅎ閃。嘴ce.00438（》98
AndWhatdoWeSee7?
RemaFI<:ar10therSerial
'oaLj-564。qel숑r
d軌art**山est.ooSD8418
ed軌Ort··NL】LL
rLrL
:1心凸
.GE쵯becausea『lothercomDuter
心나느’''''-’뺙슥∼
EREAD,PTR;oo12FE3미『etur鬧B00LI ,-

And what do we see??

Remark : another serial because another computer

우리는 무엇을 봤는가?

주목 : 다른 computer 이기 때문에 다른 serial 이다.

Because of movie size, I am not testing the serial in this movie. I suppose you believe me that it IS the serial :)

Movie size를 줄이기 위해 이 movie에서 serial을 test 하지 않는다. 이 serial과 나를 믿을 거라고 생각한다.

REMARK :

This was a rather unusual reversing for SmartCheck because of the comparing at startup.

SmartCheck is very convenient for fishing a serial in a "normal" registration scheme.

We will do that in next Part. See me there!

주목 :

이것은 SmartCheck를 위한 꽤 일반적이지 않은 reversing 이다. 왜냐하면 startup 할 때 비교한다.

SmartCheck는 "normal" registration scheme에서 serial을 얻을 때 매우 간편하다.

우리는 다음 Part에서 할 수 있다. 그곳에서 보자.

REMARK :

There exist a number of possible anti-SmartCheck tricks. One of them consists in that the application looks if it finds the name "NuMega SmartCheck".

Anti-SmartCheck trick의 많은 가능성이 존재한다. "NuMega SmartCheck"를 찾는 Application으로 구성되어져 있다.

I have not tested this application for it because I had no problems, possibly because my SmartCheck had a "Re-pair0.6" cure :)

그것을 위해 이 application을 test하지 않는다. 나는 문제없다, 나의 SmartCheck는 "Re-pair0.6" cure이기 때문에 가능하다.

I have included this tool just in case you should have problems with this. Big thanks to the author(s) !

나는 이번에 이 tool을 첨부했다. 너는 문제가 있을 것이다. 제작자들에게 정말 고맙다.

1. **Conclusion**

We have learned a little about a program made in Visual Basic. In this part 9 of this reversing series, the primary goal was to study the behaviour of a program compiled in VB.

우리는 Visual Basic에서 program을 어떻게 만드는지 배웠다. 이번 reversing series의 Part 9에서는, 주요한 목표는 VB에서 compile된 program의 behaviour를 공부하는 것이다.

We have also reversed the same program as well in Olly as in SmartCheck.

우리는 같은 program을 Olly와 SmartCheck에서 reverse 했다.

In this Visual Basic program, due to the calculation of a registration key at startup, it was really easy to find the registration key.

이 Visual Basic program은 startup 할 때 registration key를 계산 덕분에 필요하다. 그것은 정말로 registration key를 찾기 쉽다.

Next Parts in this series will bring you some more difficult VB reversing, also introducing another tool.

이 series의 다음 part에서 너에게 약간 어려운 VB reversing을 가져올 것이다. 또한 다른 tool도 소개할 것이다.

I hope you understood everything fine and I also hope someone somewhere learned something from this. See ma back in part 10 ;)

네가 모든 것을 좋게 이해했기를 희망한다. 또한 누구든지 어디서든지 이것에서 무언가를 배웠으면 좋겠다. Part 10에서 보자.

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.