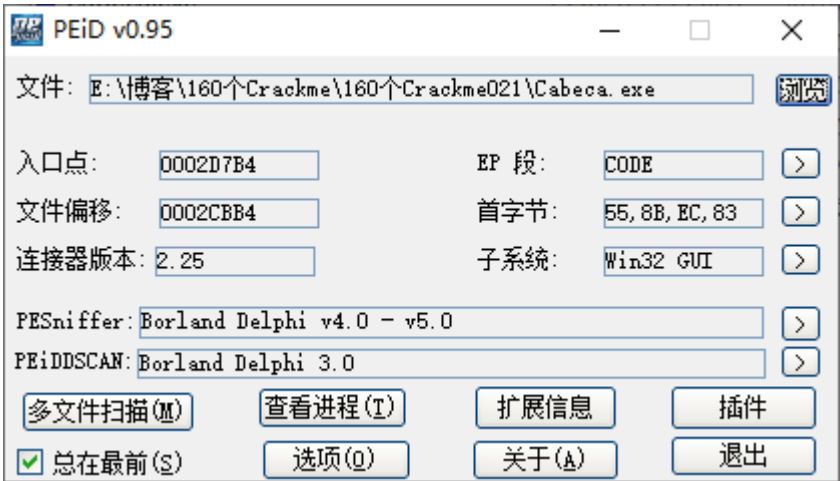


查壳
导出符号
分析程序
关键算法分析
结论

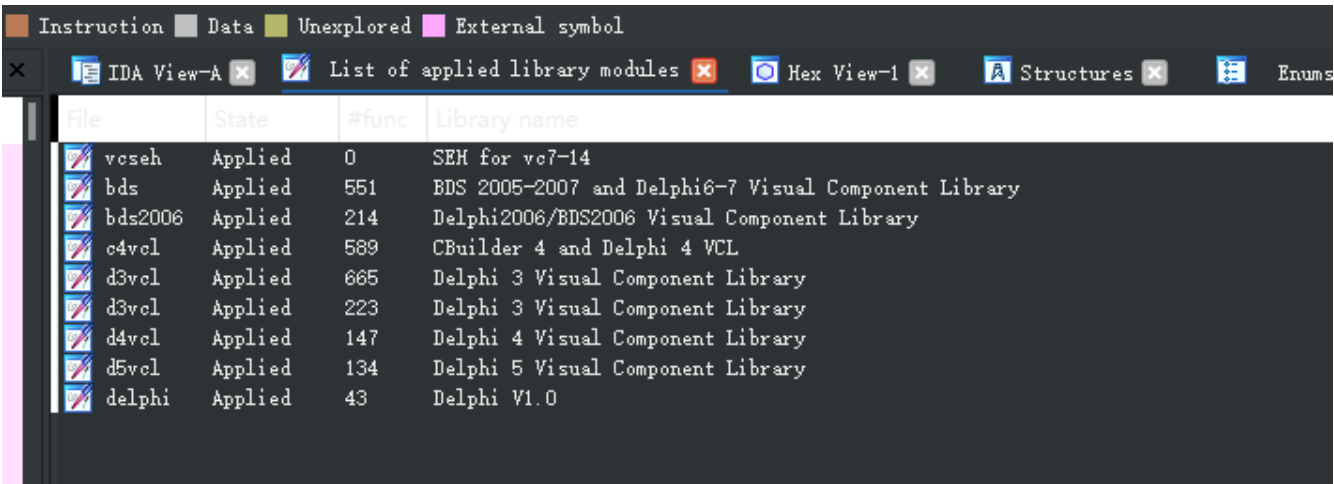
查壳



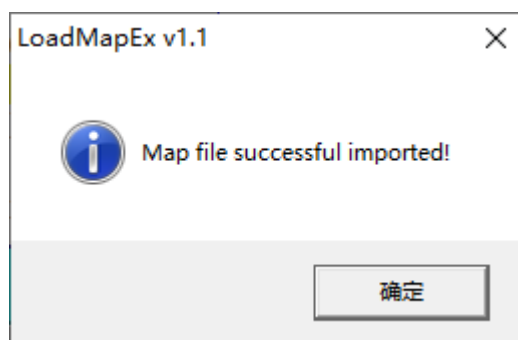
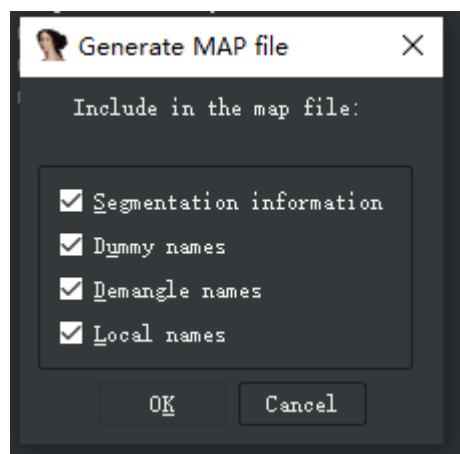
是Delphi写的，没有壳

导出符号

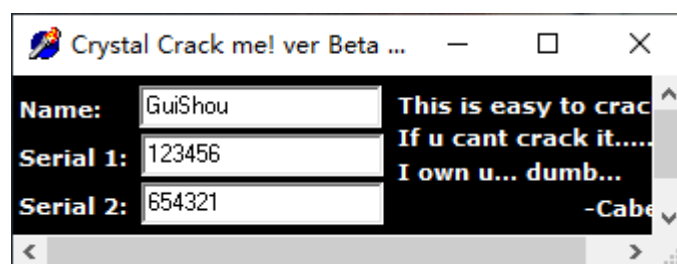
直接拖到IDA里，添加所有的Delphi签名



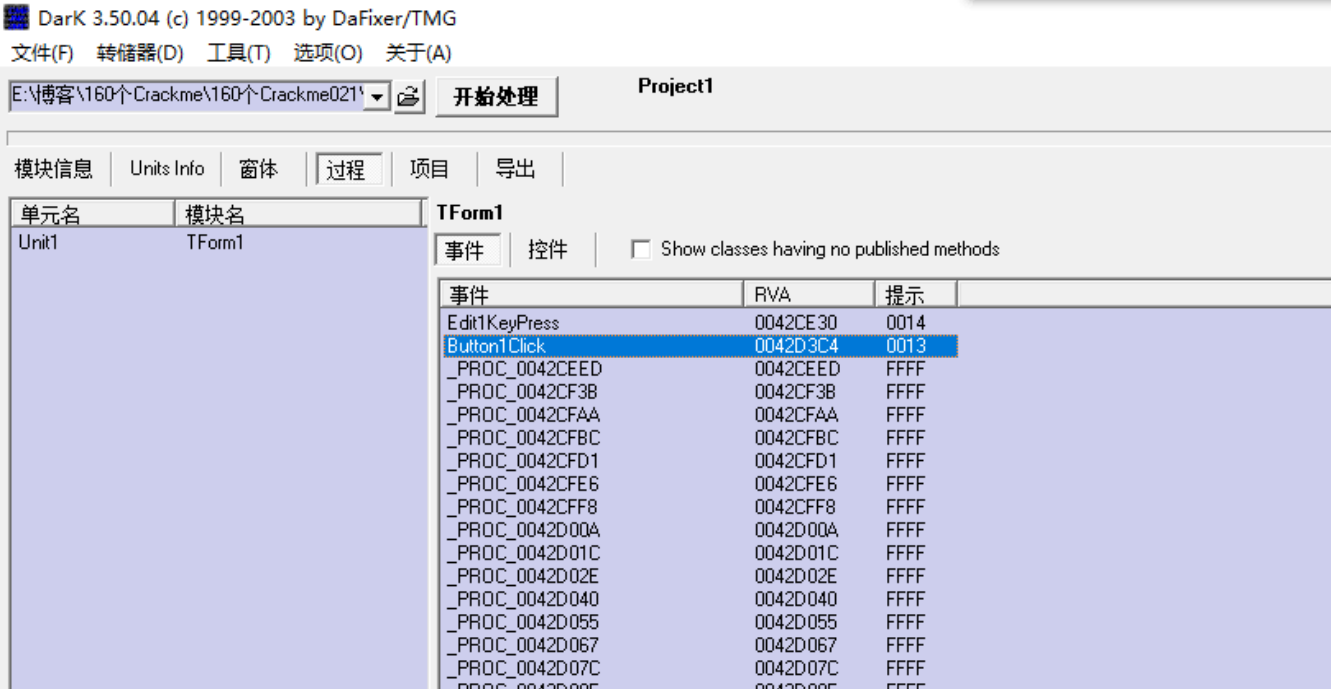
然后导出为map文件，再导入到OD，能加快分析速度



分析程序



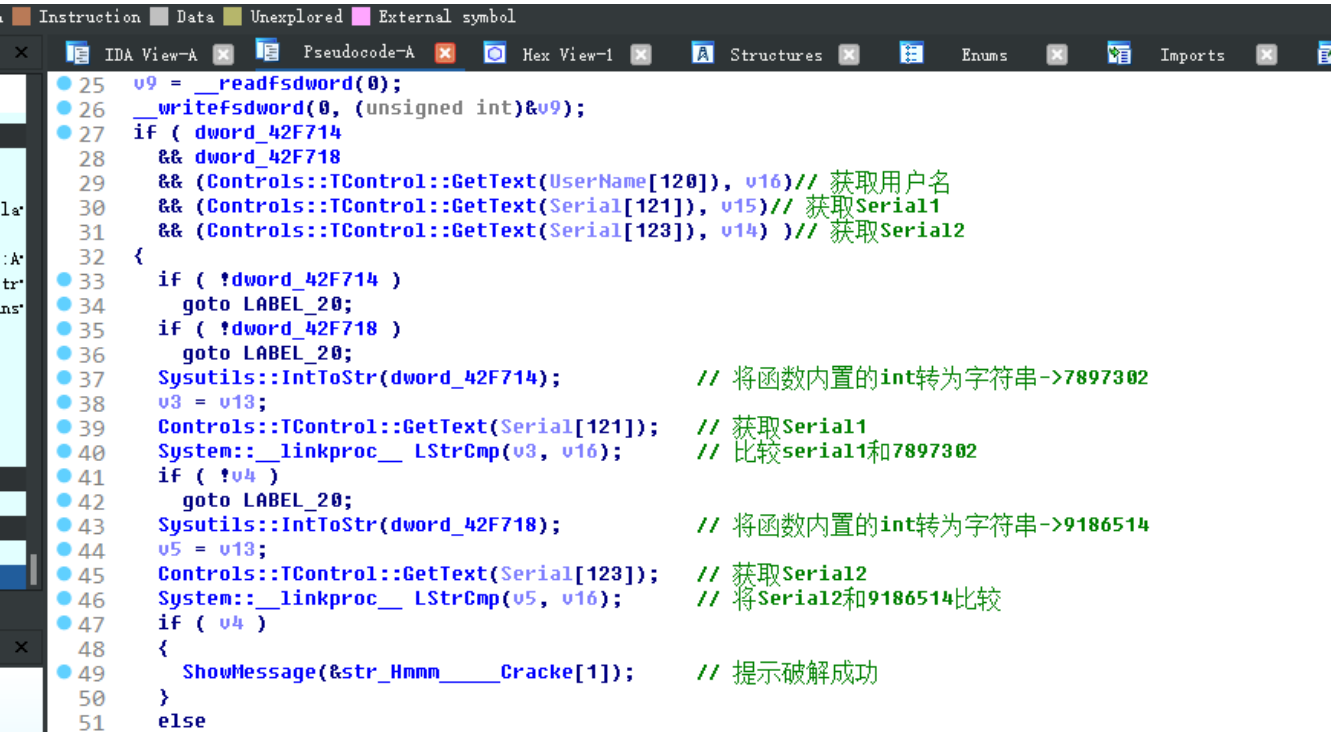
这个程序有两个序列号，



直接通过DarkDe，找到按钮事件，开始分析算法，管他有几个序列号呢~

关键算法分析

整个校验过程如下



1. 获取用户名 序列号1 序列号2

查看(V) 调试(D) 插件(P) 选项(O) 窗口(W) 帮助(H) [+]
文件(F) 查看(V) 调试(D) 插件(P) 选项(O) 窗口(W) 帮助(H) [+]
暂停 文件(F) 查看(V) 调试(D) 插件(P) 选项(O) 窗口(W) 帮助(H) [+]
l e m t w h c p k b r ... s 三 四 五 六 七 八 九 十 十一 十二 十三 十四 十五 十六 十七 十八 十九 二十 二十一 二十二 二十三 二十四 二十五 二十六 二十七 二十八 二十九 三十 三十一 三十二 三十三 三十四 三十五 三十六 三十七 三十八 三十九 四十 四十一 四十二 四十三 四十四 四十五 四十六 四十七 四十八 四十九 五十 五十一 五十二 五十三 五十四 五十五 五十六 五十七 五十八 五十九 六十 六十一 六十二 六十三 六十四 六十五 六十六 六十七 六十八 六十九 七十 七十一 七十二 七十三 七十四 七十五 七十六 七十七 七十八 七十九 八十 八十一 八十二 八十三 八十四 八十五 八十六 八十七 八十八 八十九 九十 九十一 九十二 九十三 九十四 九十五 九十六 九十七 九十八 九十九 一百

地址	HEX 数据	反汇编	注释	寄存器	
0042D3F0	. 8D55 FC	lea edx,[local.1]		EAX (
0042D3F3	. 8B83 E001000	mov eax,dword ptr ds:[ebx+0x1E0]		ECX :	
0042D3F9	. E8 E2C9FEFF	call <Cabeca.Controls::TControl::GetText(void)>		EDX	
0042D3FE	. 837D FC 00	cmp [local.1],0x0		EBX (
0042D402	. 74 28	je short <Cabeca.loc_42D42C>		ESP (
0042D404	. 8D55 F8	lea edx,[local.2]		EBP (
0042D407	. 8B83 E401000	mov eax,dword ptr ds:[ebx+0x1E4]		ESI (
0042D40D	. E8 CEC9FEFF	call <Cabeca.Controls::TControl::GetText(void)>		EDI (
0042D412	. 837D F8 00	cmp [local.2],0x0		EIP (
0042D416	. 74 14	je short <Cabeca.loc_42D42C>		C 0	
0042D418	. 8D55 F4	lea edx,[local.3]		P 1	
0042D41B	. 8B83 EC01000	mov eax,dword ptr ds:[ebx+0x1EC]		A 0	
0042D421	. E8 BAC9FEFF	call <Cabeca.Controls::TControl::GetText(void)>		Z 0	
0042D426	. 837D F4 00	cmp [local.3],0x0		S 0	
0042D42A	. 75 44	jnz short <Cabeca.loc_42D470>		T 0	
0042D42C	> B8 C4D54200	mov eax,Cabeca.0042D5C4	loc_42D42C	D 0	
0042D431	. F8 58C9FEFF	call <Cabeca._@ShdwMessage>		O 0	
堆栈 ss:[0019F694]=02254DC8, (ASCII "654321")					
地址	数值	注释	地址	数值	注释
0019F690	00000000		0019F680	0019F788	指向下一个 SEH
0019F694	02254DC8	ASCII "654321"	0019F684	0042D5AD	SE处理程序
0019F698	02254DB4	ASCII "123456"	0019F688	0019F6A0	
0019F69C	02255E8C	ASCII "GuiShou"	0019F68C	022519B8	
0019F6A0	0019F710		0019F690	00000000	

2. 将函数内置的int变量转成字符串和序列号1比较

0042D480 . 74 63 je short <Cabeca.loc_42D4E5>						注释						寄存器 (FPU)											
0042D482 . 8D55 F0 lea edx,[local.4]												EAX 02254DDC ASCII "7897302"											
0042D485 . A1 14F74200 mov eax,dword ptr ds:[<dword 42F714>]												ECX 3F5848B9											
0042D48A . E8 C190FDFE call <Cabeca.Sysutils::_IntToStr(int)>												EDX 02254DF0 ASCII "123456"											
0042D48F . 8B45 F0 mov eax,[local.4]												EBX 022549C0 ASCII "继B"											
0042D492 . 50 push eax												ESP 0019F680											
0042D493 . 8D55 FC lea edx,[local.1]												EBP 0019F6A0											
0042D496 . 8B83 E4010000 mov eax,dword ptr ds:[ebx+0x1E4]												ESI 022519B8											
0042D49C . E8 3FC9FEFF call <Cabeca.Controls::TControl::GetText(void)>												EDI 022519B8											
0042D4A1 . 8B55 FC mov edx,[local.1]												EIP 0042D4A5 Cabeca.0042D4A5											
0042D4A4 . 58 pop eax						0019F788						C 0 ES 002B 32位 0(FFFFFFFF)											
0042D4A5 . E8 2664FDFE call <Cabeca.System::_linkproc__LStrCmp(void)>												P 0 CS 0023 32位 0(FFFFFFFF)											
0042D4AA . 75 39 jnz short <Cabeca.loc_42D4E5>												A 0 SS 002B 32位 0(FFFFFFFF)											
0042D4AC . 8D55 F0 lea edx,[local.4]												Z 0 DS 002B 32位 0(FFFFFFFF)											
0042D4AF . A1 18F74200 mov eax,dword ptr ds:[<dword 42F718>]												S 0 FS 0053 32位 291000(FFF)											
0042D4B4 . E8 9790FDFE call <Cabeca.Sysutils::_IntToStr(int)>												T 0 GS 002B 32位 0(FFFFFFFF)											
0042D4B9 . 8B45 F0 mov eax,[local.4]												D 0											
004038D0=<Cabeca.System::_linkproc__LStrCmp(void)>												O 0 LastErr ERROR_SUCCESS (0000)											
地址 数值 注释												地址 数值 注释											
0019F690 02254DDC ASCII "7897302"												0019F680 0019F788 指向下一个 SEH 记录的指针											
0019F694 02254DC8 ASCII "654321"												0019F684 0042D5AD SE处理程序											
0019F698 02254DB4 ASCII "123456"												0019F688 0019F6A0											
0019F69C 02254DF0 ASCII "123456"												0019F68C 022519B8											
0019F6A0 0019F710												0019F690 02254DDC ASCII "7897302"											
0019F6A4 0041A7D7 返回到 Cabeca.Db::TDataSet::DoAfterOpen(void)+1B												0019F694 02254DC8 ASCII "654321"											

3. 将函数内置的int变量转成字符串和序列号2比较

吾爱破解 - Cabeca.exe - [LCG - 主线程, 模块 - Cabeca]

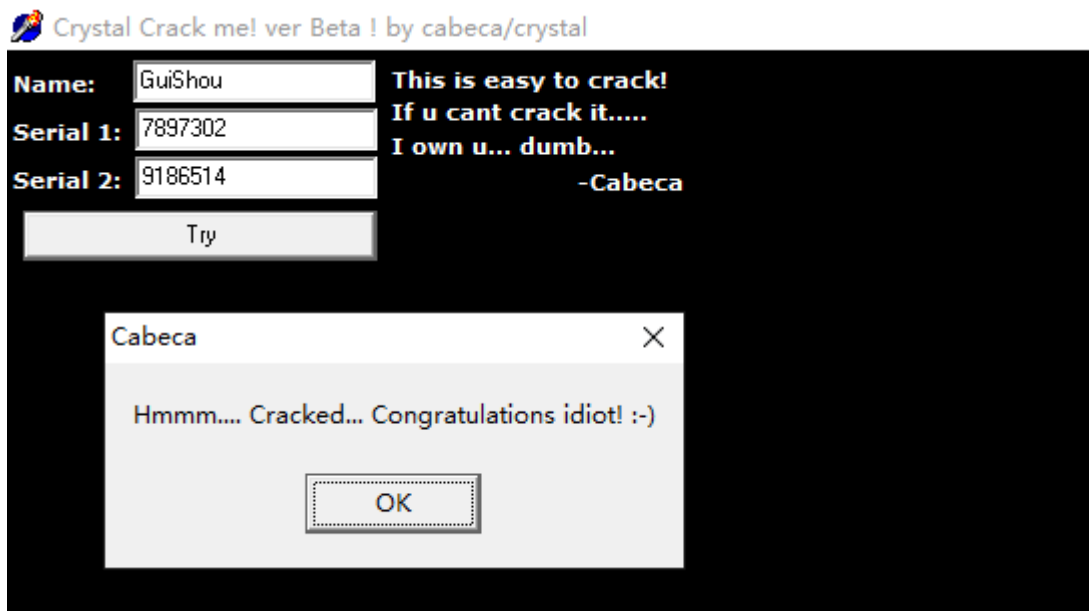
文件(F) 查看(V) 调试(D) 插件(P) 选项(O) 窗口(W) 帮助(H) [+]
 暂停 1 e m t w h c p k b r ... s 反汇编 寄存器(FPU)

地址	HEX	数据	反汇编	注释
0042D4EC	74 33		je short <Cabeca.loc_42D521>	
0042D4EE	83 3D 18 F7 42 00		cmp dword ptr ds:[<dword_42F718>], 0x0	
0042D4F5	74 2A		je short <Cabeca.loc_42D521>	
0042D4F7	8D 55 F0		lea edx, [local.4]	
0042D4FA	A1 14 F7 42 00		mov eax, dword ptr ds:[<dword_42F714>]	
0042D4FF	E8 4C 90 FD FF		call <Cabeca.Sysutils::IntToStr(int)>	
0042D504	8B 45 F0		mov eax, [local.4]	
0042D507	50		push eax	
0042D508	8D 55 FC		lea edx, [local.1]	
0042D50B	8B 83 E4 01 00 00		mov eax, dword ptr ds:[ebx+0x1E4]	
0042D511	E8 CAC 8FE FF		call <Cabeca.Controls::TControl::GetText(void)>	
0042D516	8B 55 FC		mov edx, [local.1]	
0042D519	58		pop eax	0019F788
0042D51A	E8 B1 63 FD FF		call <Cabeca.System::_linkproc__LStrCmp(void)>	
0042D51F	75 2A		jnz short <Cabeca.loc_42D54B>	
0042D521	8D 55 F0		lea edx, [local.4]	loc_42D521
004038D0	<Cabeca.System::_linkproc__LStrCmp(void)>			

地址	数值	注释
0019F688	0019F6A0	
0019F68C	022519B8	
0019F690	02255E8C	ASCII "7897302"
0019F694	02254DC8	ASCII "654321"
0019F698	02254DB4	ASCII "123456"

地址	数值	注释
0019F680	0019F788	指向下一个 SEH 记录的指针
0019F684	0042D5AD	SE处理程序
0019F688	0019F6A0	
0019F68C	022519B8	
0019F690	02255E8C	ASCII "7897302"

比较成功则提示正确



结论

- Name为任意值 无校验
- Serial1等于7897302
- Serial2等于9186514

需要相关文件的可以到我的Github下载: <https://github.com/TonyChen56/160-Crackme>