云演长安战役re复盘（2）

原创

cainiao78777 于 2022-01-18 19:24:53 发布 94 收藏

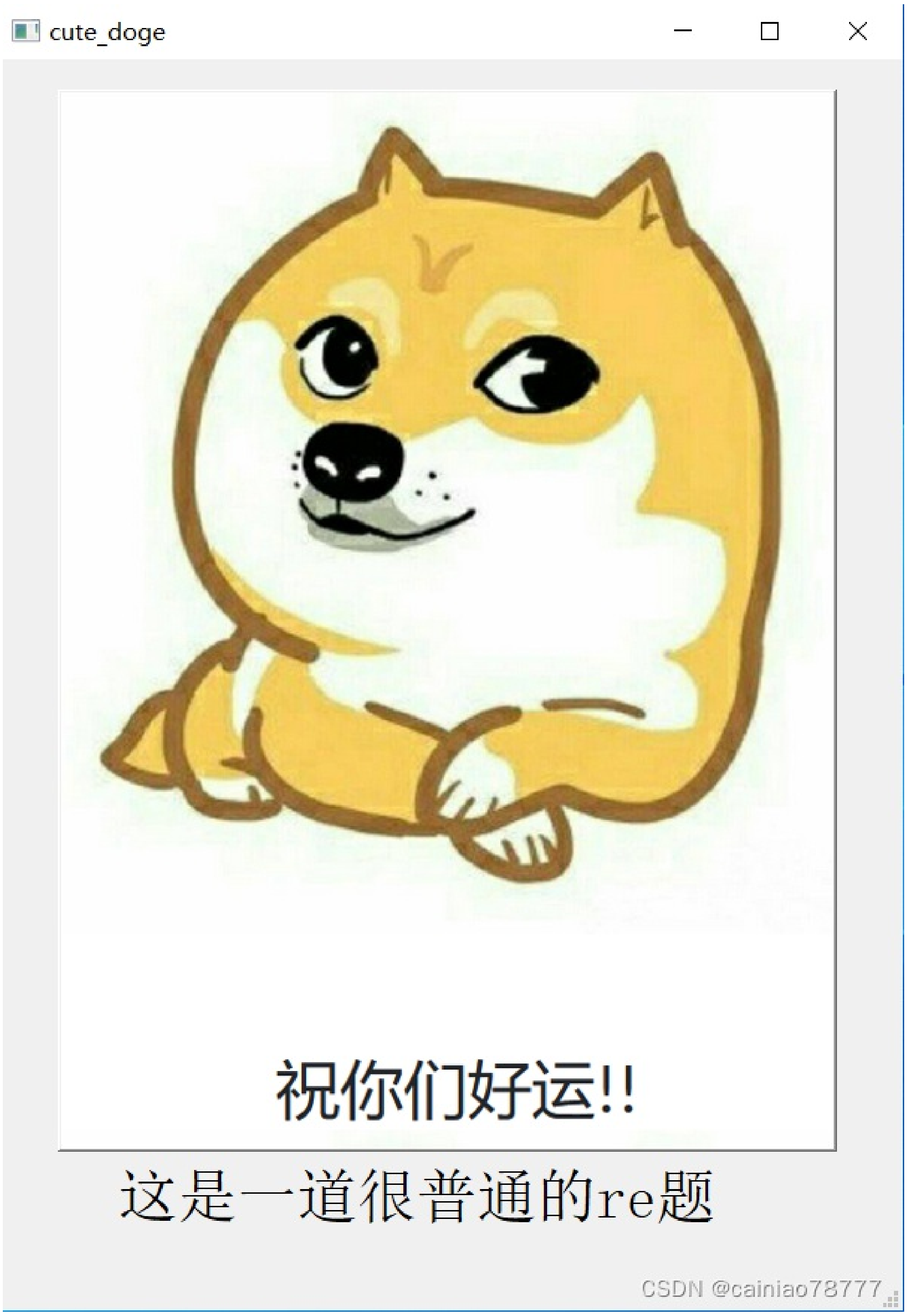
文章标签： 测试工具

本文链接：https://blog.csdn.net/cainiao78777/article/details/122565765

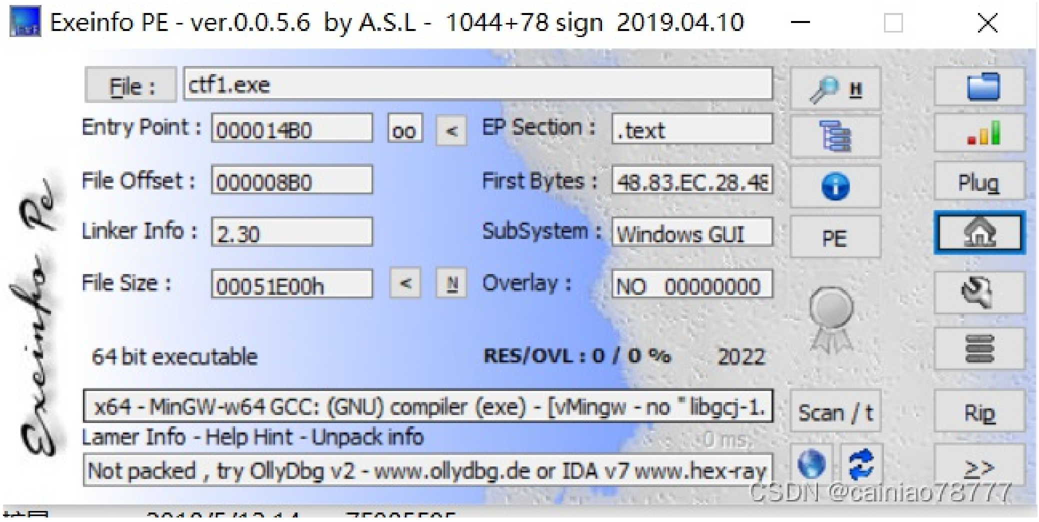
版权

re3：cute_doge

附件打开如下



查壳



Exeinfo PE - ver.0.0.5.6 by A.S.L - 1044+78 sign 2019.04.10

File : ctf1.exe

Entry Point : 000014B0

EP Section : .text

File Offset : 000008B0

First Bytes : 48.83.EC.28.48

Linker Info : 2.30

SubSystem : Windows GUI

File Size : 00051E00h

Overlay : NO 00000000

64 bit executable

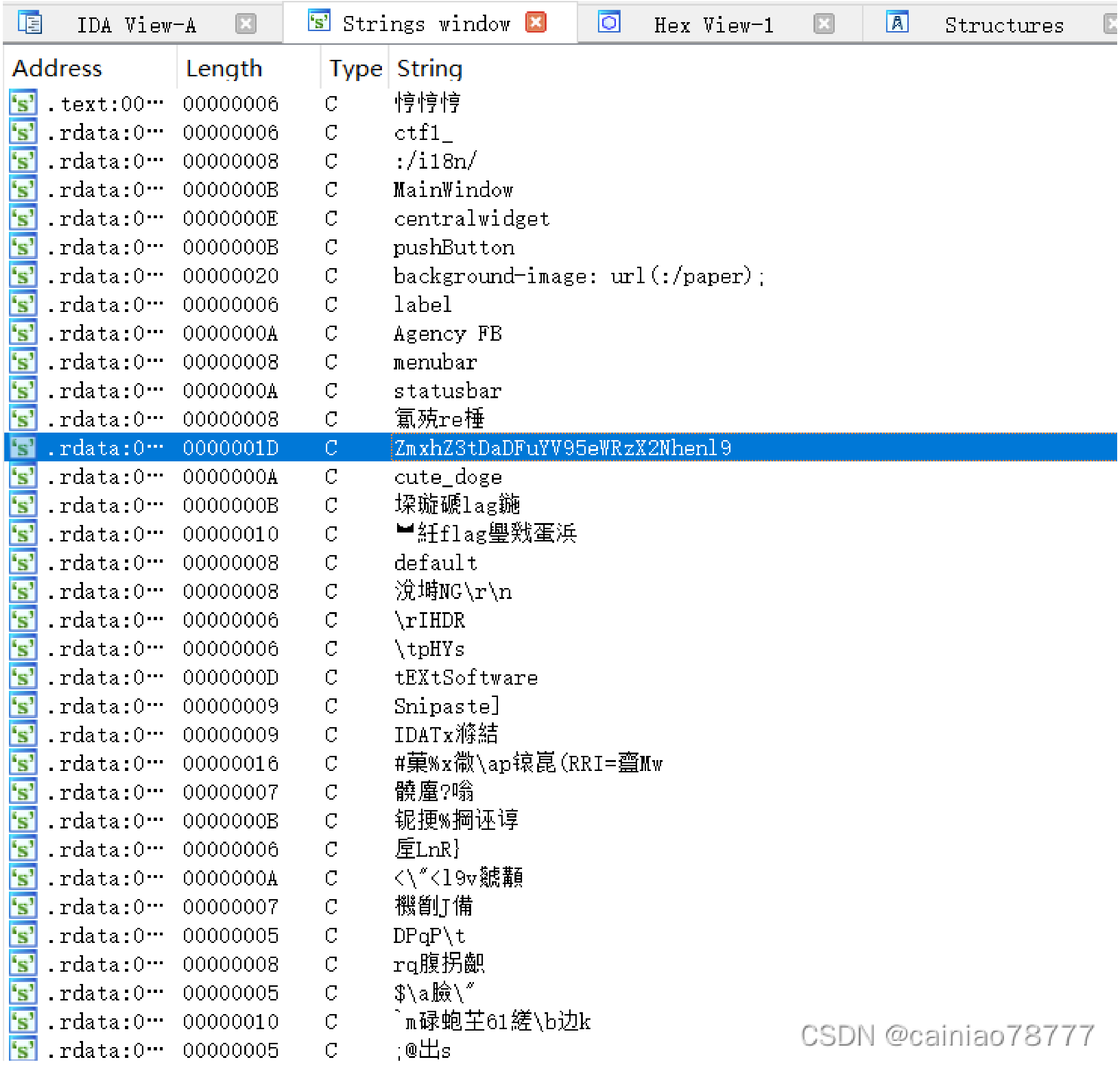
RES/OVL : 0 / 0 % 2022

x64 - MinGW-w64 GCC: (GNU) compiler (exe) - [vMingw - no " libgcj-1.

Lamer Info - Help Hint - Unpack info

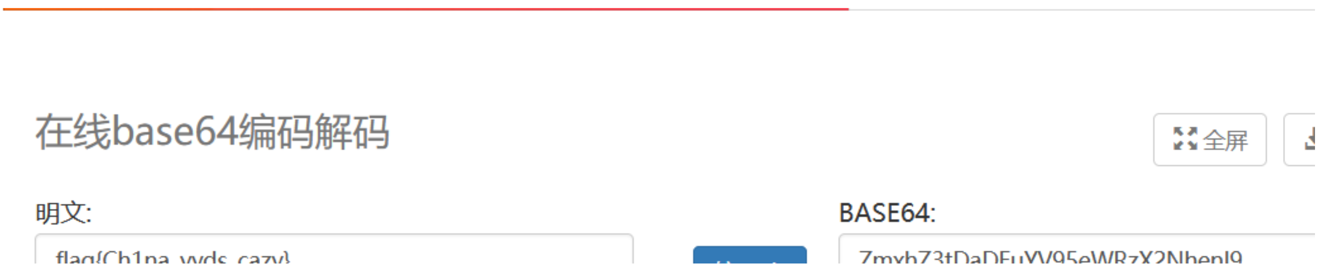
Not packed , try OllyDbg v2 - www.ollydbg.de or IDA v7 www.hex-ray

x64,用ida64分析



Address	Length	Type	String
.text:00···	00000006	C	悖悖悖
.rdata:0···	00000006	C	ctf1_
.rdata:0···	00000008	C	:/i18n/
.rdata:0···	0000000B	C	MainWindow
.rdata:0···	0000000E	C	centralwidget
.rdata:0···	0000000B	C	pushButton
.rdata:0···	00000020	C	background-image: url(:/paper);
.rdata:0···	00000006	C	label
.rdata:0···	0000000A	C	Agency FB
.rdata:0···	00000008	C	menubar
.rdata:0···	0000000A	C	statusbar
.rdata:0···	00000008	C	氯殑re棰
.rdata:0···	0000001D	C	ZmxhZ3tDaDFuYV95eWRzX2Nhenl9
.rdata:0···	0000000A	C	cute_doge
.rdata:0···	0000000B	C	垛璇磃lag鍦
.rdata:0···	00000010	C	▀紝flag璺戝埌浜
.rdata:0···	00000008	C	default
.rdata:0···	00000008	C	涗墒NG\r\n
.rdata:0···	00000006	C	\rIHDR
.rdata:0···	00000006	C	\tpHYs
.rdata:0···	0000000D	C	tEXtSoftware
.rdata:0···	00000009	C	Snipaste]
.rdata:0···	00000009	C	IDATx滌結
.rdata:0···	00000016	C	#菓%x黴\ap锿崑(RRI=齏Mw
.rdata:0···	00000007	C	髒廛?嗡
.rdata:0···	0000000B	C	鋃捙%搁诬谆
.rdata:0···	00000006	C	厔LnR}
.rdata:0···	0000000A	C	<\"<19v虢顜
.rdata:0···	00000007	C	櫗剳J備
.rdata:0···	00000005	C	DPqP\t
.rdata:0···	00000008	C	rq腹拐齠
.rdata:0···	00000005	C	$\a臉\"
.rdata:0···	00000010	C	`m碌蚫芏61縒\b边k
.rdata:0···	00000005	C	;@出s

base64解码



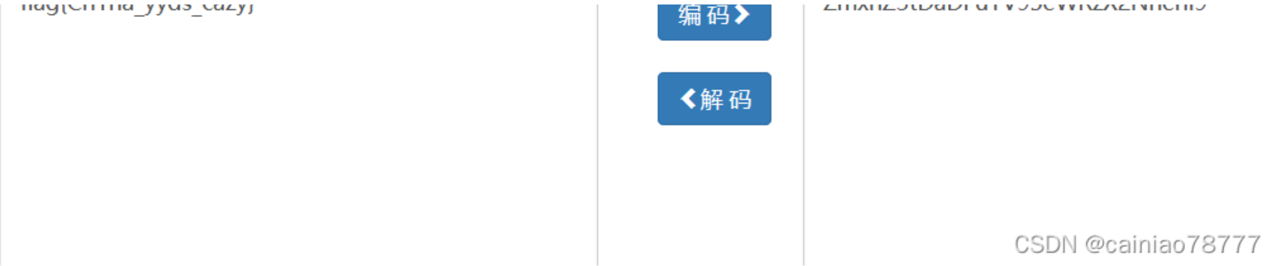
在线base64编码解码

明文:

flag{Ch1na_yyds_cazy}

BASE64:

ZmxhZ3tDaDFuYV95eWRzX2Nhenl9

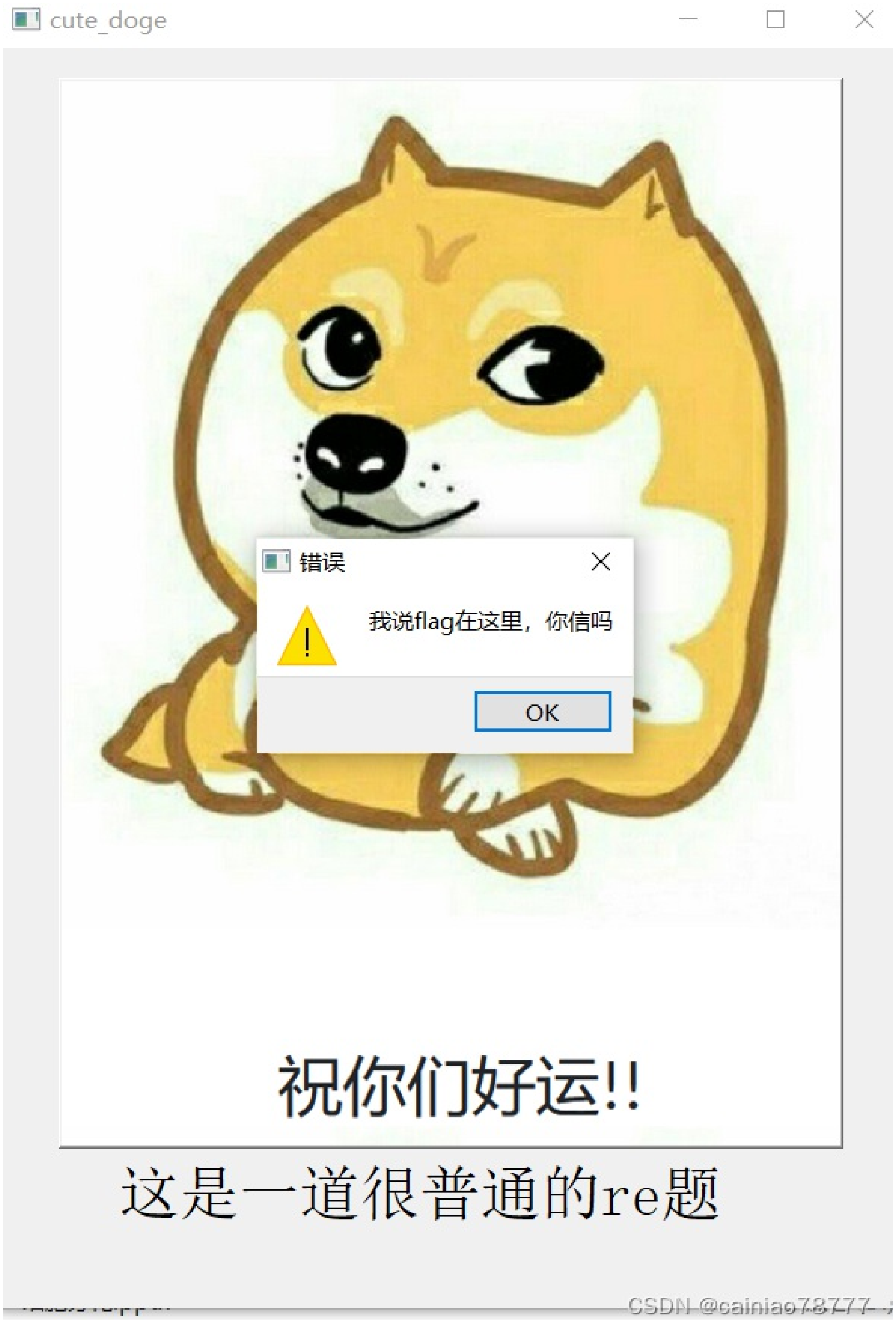


flag{Ch1na_yyds_cazy}

ZmxhZ3tDaDFuYV95eWRzX2NhenI9

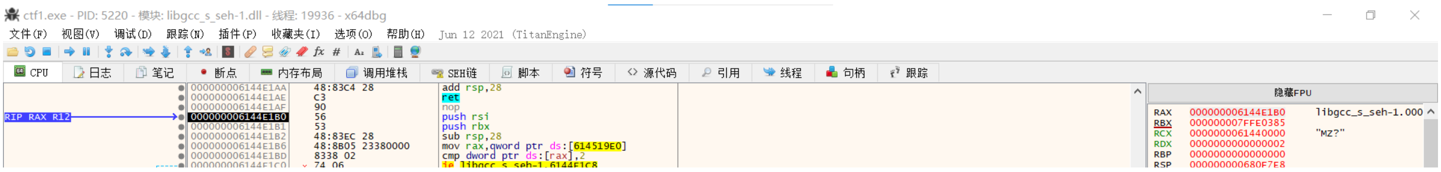
flag{Ch1na_yyds_cazy}

总结： 在看到x64时，想到的是用x64dbg



我说flag在这里，你信吗

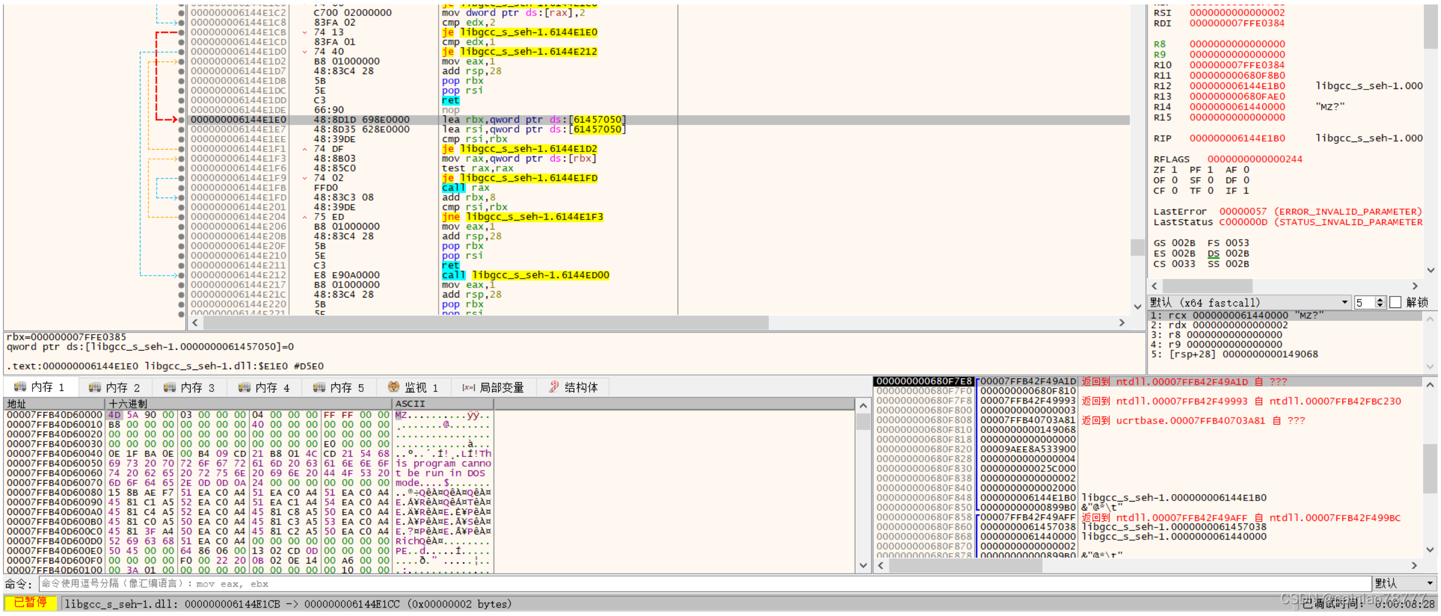
想用x64dbg调试一下，如下



ctf1.exe - PID: 5220 - 模块: libgcc_s_seh-1.dll - 线程: 19936 - x64dbg
文件(F) 视图(V) 调试(D) 跟踪(N) 插件(P) 收藏夹(I) 选项(O) 帮助(H) Jun 12 2021 (TitanEngine)
CPU 日志 笔记 断点 内存布局 调用堆栈 SEH链 脚本 符号 源代码 引用 线程 句柄 跟踪
隐藏FPU

```
RIP RAX R12 → 000000006144E1AA  48:83C4 28         add rsp,28
              000000006144E1AE  C3                 ret
              000000006144E1AF  90                 nop
              000000006144E1B0  56                 push rsi
              000000006144E1B1  53                 push rbx
              000000006144E1B2  48:83EC 28         sub rsp,28
              000000006144E1B6  48:8B05 23380000   mov rax,qword ptr ds:[614519E0]
              000000006144E1BD  8338 02            cmp dword ptr ds:[rax],2
              000000006144E1C0  74 06              je libgcc_s_seh-1.6144E1C8

RAX  000000006144E1B0   libgcc_s_seh-1.000
RBX  000000007FFE0385
RCX  0000000061440000   "MZ?"
RDX  0000000000000002
RBP  0000000000000000
RSP  00000000680F7E8
```



```
000000006144E1C2   C700 02000000      mov dword ptr ds:[rax],2
000000006144E1C8   83FA 02            cmp edx,2
000000006144E1CB   74 13              je libgcc_s_seh-1.6144E1E0
000000006144E1CD   83FA 01            cmp edx,1
000000006144E1D0   74 40              je libgcc_s_seh-1.6144E212
000000006144E1D2   B8 01000000        mov eax,1
000000006144E1D7   48:83C4 28         add rsp,28
000000006144E1DB   5B                 pop rbx
000000006144E1DC   5E                 pop rsi
000000006144E1DD   C3                 ret
000000006144E1DE   66:90              nop
000000006144E1E0   48:8D1D 698E0000   lea rbx,qword ptr ds:[61457050]
000000006144E1E7   48:8D35 628E0000   lea rsi,qword ptr ds:[61457050]
000000006144E1EE   48:39DE            cmp rsi,rbx
000000006144E1F1   74 DF              je libgcc_s_seh-1.6144E1D2
000000006144E1F3   48:8B03            mov rax,qword ptr ds:[rbx]
000000006144E1F6   48:85C0            test rax,rax
000000006144E1F9   74 02              je libgcc_s_seh-1.6144E1FD
000000006144E1FB   FFD0               call rax
000000006144E1FD   48:83C3 08         add rbx,8
000000006144E201   48:39DE            cmp rsi,rbx
000000006144E204   75 ED              jne libgcc_s_seh-1.6144E1F3
000000006144E206   B8 01000000        mov eax,1
000000006144E20B   48:83C4 28         add rsp,28
000000006144E20F   5B                 pop rbx
000000006144E210   5E                 pop rsi
000000006144E211   C3                 ret
000000006144E212   E8 E90A0000        call libgcc_s_seh-1.6144ED00
000000006144E217   B8 01000000        mov eax,1
000000006144E21C   48:83C4 28         add rsp,28
000000006144E220   5B                 pop rbx
```

```
RSI    0000000000000002
RDI    000000007FFE0384

R8     0000000000000000
R9     0000000000000000
R10    000000007FFE0384
R11    00000000680F8B0
R12    000000006144E1B0     libgcc_s_seh-1.000
R13    00000000680FAE0
R14    0000000061440000     "MZ?"
R15    0000000000000000

RIP    000000006144E1B0     libgcc_s_seh-1.000

RFLAGS   0000000000000244
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError  00000057 (ERROR_INVALID_PARAMETER)
LastStatus C000000D (STATUS_INVALID_PARAMETER

GS 002B  FS 0053
ES 002B  DS 002B
CS 0033  SS 002B
```

默认 (x64 fastcall) 5 □ 解锁

```
1: rcx 0000000061440000 "MZ?"
2: rdx 0000000000000002
3: r8 0000000000000000
4: r9 0000000000000000
5: [rsp+28] 0000000000149068
```

```
rbx=000000007FFE0385
qword ptr ds:[libgcc_s_seh-1.0000000061457050]=0

.text:000000006144E1E0 libgcc_s_seh-1.dll:$E1E0 #D5E0
```

```
地址              十六进制                                          ASCII
00007FFB40D60000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
00007FFB40D60010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ,.......@.......
00007FFB40D60020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00007FFB40D60030  00 00 00 00 00 00 00 00 00 00 00 00 E0 00 00 00  ............à...
00007FFB40D60040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º..´.Í!¸.LÍ!Th
00007FFB40D60050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
00007FFB40D60060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS 
00007FFB40D60070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
00007FFB40D60080  15 8B AE F7 51 EA C0 A4 51 EA C0 A4 51 EA C0 A4  ..®÷QêÀ¤QêÀ¤QêÀ¤
00007FFB40D60090  45 81 C1 A5 52 EA C0 A4 51 EA C1 A4 54 EA C0 A4  E.Á¥RêÀ¤QêÁ¤TêÀ¤
00007FFB40D600A0  45 81 C4 A5 52 EA C0 A4 45 81 C8 A5 50 EA C0 A4  E.Ä¥RêÀ¤E.È¥PêÀ¤
00007FFB40D600B0  45 81 C0 A5 50 EA C0 A4 45 81 C3 A5 53 EA C0 A4  E.À¥PêÀ¤E.Ã¥SêÀ¤
00007FFB40D600C0  45 81 3F A4 50 EA C0 A4 45 81 C2 A5 50 EA C0 A4  E.?¤PêÀ¤E.Â¥PêÀ¤
00007FFB40D600D0  52 69 63 68 51 EA C0 A4 00 00 00 00 00 00 00 00  RichQêÀ¤........
00007FFB40D600E0  50 45 00 00 64 86 06 00 13 02 CD 0D 00 00 00 00  PE..d.....Í.....
00007FFB40D600F0  00 00 00 00 F0 00 22 20 0B 02 0E 14 00 A6 00 00  ....ð." .....¦..
```

```
000000000680F7E8  00007FFB42F49A1D  返回到 ntdll.00007FFB42F49A1D 自 ???
000000000680F7F0  000000000680F810
000000000680F7F8  00007FFB42F49993  返回到 ntdll.00007FFB42F49993 自 ntdll.00007FFB42FBC230
000000000680F800  0000000000000003
000000000680F808  00007FFB40703A81  返回到 ucrtbase.00007FFB40703A81 自 ???
000000000680F810  0000000000149068
000000000680F818  0000000000000000
000000000680F820  00009AEE8A533900
000000000680F828  0000000000000004
000000000680F830  000000000025C000
000000000680F838  0000000000000002
000000000680F840  0000000000002000
000000000680F848  000000006144E1B0  libgcc_s_seh-1.000000006144E1B0
000000000680F850  00000000000899B0  &"@*\t"
000000000680F858  00007FFB42F49AFF  返回到 ntdll.00007FFB42F49AFF 自 ntdll.00007FFB42F499BC
000000000680F860  0000000061457038  libgcc_s_seh-1.0000000061457038
000000000680F868  0000000061440000  libgcc_s_seh-1.0000000061440000
000000000680F870  0000000000000002
```

命令: 命令使用逗号分隔（像汇编语言）: mov eax, ebx

默认

已暂停 libgcc_s_seh-1.dll: 000000006144E1CB -> 000000006144E1CC (0x00000002 bytes)

已调试时间: 0:00:08:28

但是我被没有发现什么，后来wp别人是有的，有点不懂。