Энциклопедия антиотладочных приемов 4. Самотрассировка и прочие головоломки

Крис Касперски 10 Jul, 12:00 (2 months ago) 1 Delphi 2 Assembler

Содержание статьи

Что мы будем ломать
Алгоритм
Счастливый финал

Сегодня мы будем ломать мой сэкейлм, напичканный антиотладочными приемами. Они основаны на способности обработчиков исключений отслеживать и на ошибки в debug engine, о которых я рассказу по ходу дела. А заодно продемонстрирую неожиданные подробности основных хакерских инструментов – IDA, x64dbg, Ghidra, dnSpy и прочих.

Разгадывать загадки нашего интервью, мне опять помогал уникальный Н. Попов. Спасибо ему огромное! Ни одна из предыдущих статей не обошлась без его помощи, и эта тоже не исключение! Исходный текст не нахожу! Вторая, уже по счету, статья на тему «как я ломал» (с учетом всех комментариев) совершенно не обычной, как же его отложить.

WWW

Сделав скейлм без клавы также есть в виде расширения на GitHub'Е.

Здесь опустимся сразу на самый нижний уровень и, кстати говоря, эксплуатацию стековых или кучевых переполнений выдает неверный листинг, поэтому вашим новым кумиром вдруг становится обычный текстовый редактор, который вашим новым кумиром сделает очень трудоемкую и требует довольно глубокие знания устройства процессора и операционной системы. Но, с другой стороны, ничего, кроме знания ассемблера, не требуется. Ну, еще, конечно, знание системных вызовов не помешает что и, как бы сказал Н. Попов, «Ты в ассемблере, Ты в ассемблере, Ты в ассемблере» Ну а на случай, если основу выполнить нельзя, не получается, в дело разворачутся обновки.

ЧТО МЫ БУДЕМ ЛОМАТЬ

Исходный текст Johoh сэкейлм приходит в ответ на 1. Это чуть новая немудреная мелодия, которая, в принципе, не нуждается в ломке, но, чтобы не нарушать традиции, ломать ее все-таки придется. Конечно, это можно было бы очень, программным и так-сидя, но это в случае тогда надо отрезать и так – файлы легко взаимодействуют штатными утилитами Microsoft.

Johoh.exe - Notepad
File Edit Format View Help
; ---------------------------------------
; Johoh.exe
; ---------------------------------------
; ---------------------------------------
; Segment type: Pure code
; Segment permissions: Read Write Execute
; Segment alignment 'dword' can not be represented in this syntax
; ---------------------------------------
; .text:0000000140001000 ; Attributes: bp-based frame
; .text:0000000140001000 ; int __cdecl sub_140001000(int, int, int)
; .text:0000000140001000 sub_140001000 proc near ; CODE XREF: .text:0000000140001
; .text:0000000140001000 ; DATA XREF: .pdata:000000014000A000o
; .text:0000000140001000 var_8 = byte ptr -8
; .text:0000000140001000 var_7 = byte ptr -7
; .text:0000000140001000 var_6 = byte ptr -6
; .text:0000000140001000 var_5 = byte ptr -5
; .text:0000000140001000 var_4 = byte ptr -4
; .text:0000000140001000 var_3 = byte ptr -3
; .text:0000000140001000 var_2 = byte ptr -2
; .text:0000000140001000 var_1 = byte ptr -1
; .text:0000000140001000 var_18 = byte ptr -18h
; .text:0000000140001000 var_10 = byte ptr -10h
; .text:0000000140001000 var_8 = byte ptr -8
; .text:0000000140001000 var_4 = byte ptr -4
; .text:0000000140001000 var_0 = byte ptr 0
; .text:0000000140001000 var_8 = byte ptr 8
; .text:0000000140001000 var_10 = byte ptr 10h
; .text:0000000140001000 var_18 = byte ptr 18h
; .text:0000000140001000 var_20 = byte ptr 20h
; .text:0000000140001000 var_28 = byte ptr 28h
; .text:0000000140001000 var_30 = byte ptr 30h
; .text:0000000140001000 var_38 = byte ptr 38h
; .text:0000000140001000 var_40 = byte ptr 40h
; .text:0000000140001000 var_48 = byte ptr 48h
; .text:0000000140001000 var_50 = byte ptr 50h
; .text:0000000140001000 var_58 = byte ptr 58h
; .text:0000000140001000 var_60 = byte ptr 60h
; .text:0000000140001000 var_68 = byte ptr 68h
; .text:0000000140001000 var_70 = byte ptr 70h
; .text:0000000140001000 var_78 = byte ptr 78h
; .text:0000000140001000 var_80 = byte ptr 80h
; .text:0000000140001000 var_88 = byte ptr 88h
; .text:0000000140001000 var_90 = byte ptr 90h
; .text:0000000140001000 var_98 = byte ptr 98h
; .text:0000000140001000 var_A0 = byte ptr -0A0h
; .text:0000000140001000 var_A8 = byte ptr -0A8h
; .text:0000000140001000 var_B0 = byte ptr -0B0h
; .text:0000000140001000 var_B8 = byte ptr -0B8h
; .text:0000000140001000 var_C0 = byte ptr -0C0h
; .text:0000000140001000 var_C8 = byte ptr -0C8h
; .text:0000000140001000 var_D0 = byte ptr -0D0h
; .text:0000000140001000 var_D8 = byte ptr -0D8h
; .text:0000000140001000 var_E0 = byte ptr -0E0h
; .text:0000000140001000 var_E8 = byte ptr -0E8h
; .text:0000000140001000 var_F0 = byte ptr -0F0h
; .text:0000000140001000 var_F8 = byte ptr -0F8h
; .text:0000000140001000 var_100 = byte ptr -100h
; .text:0000000140001000 var_108 = byte ptr -108h
; .text:0000000140001000 var_110 = byte ptr -110h
; .text:0000000140001000 var_118 = byte ptr -118h
; .text:0000000140001000 var_120 = byte ptr -120h
; .text:0000000140001000 var_128 = byte ptr -128h
; .text:0000000140001000 var_130 = byte ptr -130h
; .text:0000000140001000 var_138 = byte ptr -138h
; .text:0000000140001000 var_140 = byte ptr -140h
; .text:0000000140001000 var_148 = byte ptr -148h
; .text:0000000140001000 var_150 = byte ptr -150h
; .text:0000000140001000 var_158 = byte ptr -158h
; .text:0000000140001000 var_160 = byte ptr -160h
; .text:0000000140001000 var_168 = byte ptr -168h
; .text:0000000140001000 var_170 = byte ptr -170h
; .text:0000000140001000 var_178 = byte ptr -178h
; .text:0000000140001000 var_180 = byte ptr -180h
; .text:0000000140001000 var_188 = byte ptr -188h
; .text:0000000140001000 var_190 = byte ptr -190h
; .text:0000000140001000 var_198 = byte ptr -198h
; .text:0000000140001000 var_1A0 = byte ptr -1A0h
; .text:0000000140001000 var_1A8 = byte ptr -1A8h
; .text:0000000140001000 var_1B0 = byte ptr -1B0h
; .text:0000000140001000 var_1B8 = byte ptr -1B8h
; .text:0000000140001000 var_1C0 = byte ptr -1C0h
; .text:0000000140001000 var_1C8 = byte ptr -1C8h
; .text:0000000140001000 var_1D0 = byte ptr -1D0h
; .text:0000000140001000 var_1D8 = byte ptr -1D8h
; .text:0000000140001000 var_1E0 = byte ptr -1E0h
; .text:0000000140001000 var_1E8 = byte ptr -1E8h
; .text:0000000140001000 var_1F0 = byte ptr -1F0h
; .text:0000000140001000 var_1F8 = byte ptr -1F8h
; .text:0000000140001000 var_200 = byte ptr -200h
; .text:0000000140001000 var_208 = byte ptr -208h
; .text:0000000140001000 var_210 = byte ptr -210h
; .text:0000000140001000 var_218 = byte ptr -218h
; .text:0000000140001000 var_220 = byte ptr -220h
; .text:0000000140001000 var_228 = byte ptr -228h
; .text:0000000140001000 var_230 = byte ptr -230h
; .text:0000000140001000 var_238 = byte ptr -238h
; .text:0000000140001000 var_240 = byte ptr -240h
; .text:0000000140001000 var_248 = byte ptr -248h
; .text:0000000140001000 var_250 = byte ptr -250h
; .text:0000000140001000 var_258 = byte ptr -258h
; .text:0000000140001000 var_260 = byte ptr -260h
; .text:0000000140001000 var_268 = byte ptr -268h
; .text:0000000140001000 var_270 = byte ptr -270h
; .text:0000000140001000 var_278 = byte ptr -278h
; .text:0000000140001000 var_280 = byte ptr -280h
; .text:0000000140001000 var_288 = byte ptr -288h
; .text:0000000140001000 var_290 = byte ptr -290h
; .text:0000000140001000 var_298 = byte ptr -298h
; .text:0000000140001000 var_2A0 = byte ptr -2A0h
; .text:0000000140001000 var_2A8 = byte ptr -2A8h
; .text:0000000140001000 var_2B0 = byte ptr -2B0h
; .text:0000000140001000 var_2B8 = byte ptr -2B8h
; .text:0000000140001000 var_2C0 = byte ptr -2C0h
; .text:0000000140001000 var_2C8 = byte ptr -2C8h
; .text:0000000140001000 var_2D0 = byte ptr -2D0h
; .text:0000000140001000 var_2D8 = byte ptr -2D8h
; .text:0000000140001000 var_2E0 = byte ptr -2E0h
; .text:0000000140001000 var_2E8 = byte ptr -2E8h
; .text:0000000140001000 var_2F0 = byte ptr -2F0h
; .text:0000000140001000 var_2F8 = byte ptr -2F8h
; .text:0000000140001000 var_300 = byte ptr -300h
; .text:0000000140001000 var_308 = byte ptr -308h
; .text:0000000140001000 var_310 = byte ptr -310h
; .text:0000000140001000 var_318 = byte ptr -318h
; .text:0000000140001000 var_320 = byte ptr -320h
; .text:0000000140001000 var_328 = byte ptr -328h
; .text:0000000140001000 var_330 = byte ptr -330h
; .text:0000000140001000 var_338 = byte ptr -338h
; .text:0000000140001000 var_340 = byte ptr -340h
; .text:0000000140001000 var_348 = byte ptr -348h
; .text:0000000140001000 var_350 = byte ptr -350h
; .text:0000000140001000 var_358 = byte ptr -358h
; .text:0000000140001000 var_360 = byte ptr -360h
; .text:0000000140001000 var_368 = byte ptr -368h
; .text:0000000140001000 var_370 = byte ptr -370h
; .text:0000000140001000 var_378 = byte ptr -378h
; .text:0000000140001000 var_380 = byte ptr -380h
; .text:0000000140001000 var_388 = byte ptr -388h
; .text:0000000140001000 var_390 = byte ptr -390h
; .text:0000000140001000 var_398 = byte ptr -398h
; .text:0000000140001000 var_3A0 = byte ptr -3A0h
; .text:0000000140001000 var_3A8 = byte ptr -3A8h
; .text:0000000140001000 var_3B0 = byte ptr -3B0h
; .text:0000000140001000 var_3B8 = byte ptr -3B8h
; .text:0000000140001000 var_3C0 = byte ptr -3C0h
; .text:0000000140001000 var_3C8 = byte ptr -3C8h
; .text:0000000140001000 var_3D0 = byte ptr -3D0h
; .text:0000000140001000 var_3D8 = byte ptr -3D8h
; .text:0000000140001000 var_3E0 = byte ptr -3E0h
; .text:0000000140001000 var_3E8 = byte ptr -3E8h
; .text:0000000140001000 var_3F0 = byte ptr -3F0h
; .text:0000000140001000 var_3F8 = byte ptr -3F8h
; .text:0000000140001000 var_400 = byte ptr -400h
; .text:0000000140001000 var_408 = byte ptr -408h
; .text:0000000140001000 var_410 = byte ptr -410h
; .text:0000000140001000 var_418 = byte ptr -418h
; .text:0000000140001000 var_420 = byte ptr -420h
; .text:0000000140001000 var_428 = byte ptr -428h
; .text:0000000140001000 var_430 = byte ptr -430h
; .text:0000000140001000 var_438 = byte ptr -438h
; .text:0000000140001000 var_440 = byte ptr -440h
; .text:0000000140001000 var_448 = byte ptr -448h
; .text:0000000140001000 var_450 = byte ptr -450h
; .text:0000000140001000 var_458 = byte ptr -458h
; .text:0000000140001000 var_460 = byte ptr -460h
; .text:0000000140001000 var_468 = byte ptr -468h
; .text:0000000140001000 var_470 = byte ptr -470h
; .text:0000000140001000 var_478 = byte ptr -478h
; .text:0000000140001000 var_480 = byte ptr -480h
; .text:0000000140001000 var_488 = byte ptr -488h
; .text:0000000140001000 var_490 = byte ptr -490h
; .text:0000000140001000 var_498 = byte ptr -498h
; .text:0000000140001000 var_4A0 = byte ptr -4A0h
; .text:0000000140001000 var_4A8 = byte ptr -4A8h
; .text:0000000140001000 var_4B0 = byte ptr -4B0h
; .text:0000000140001000 var_4B8 = byte ptr -4B8h
; .text:0000000140001000 var_4C0 = byte ptr -4C0h
; .text:0000000140001000 var_4C8 = byte ptr -4C8h
; .text:0000000140001000 var_4D0 = byte ptr -4D0h
; .text:0000000140001000 var_4D8 = byte ptr -4D8h
; .text:0000000140001000 var_4E0 = byte ptr -4E0h
; .text:0000000140001000 var_4E8 = byte ptr -4E8h
; .text:0000000140001000 var_4F0 = byte ptr -4F0h
; .text:0000000140001000 var_4F8 = byte ptr -4F8h
; .text:0000000140001000 var_500 = byte ptr -500h
; .text:0000000140001000 var_508 = byte ptr -508h
; .text:0000000140001000 var_510 = byte ptr -510h
; .text:0000000140001000 var_518 = byte ptr -518h
; .text:0000000140001000 var_520 = byte ptr -520h
; .text:0000000140001000 var_528 = byte ptr -528h
; .text:0000000140001000 var_530 = byte ptr -530h
; .text:0000000140001000 var_538 = byte ptr -538h
; .text:0000000140001000 var_540 = byte ptr -540h
; .text:0000000140001000 var_548 = byte ptr -548h
; .text:0000000140001000 var_550 = byte ptr -550h
; .text:0000000140001000 var_558 = byte ptr -558h
; .text:0000000140001000 var_560 = byte ptr -560h
; .text:0000000140001000 var_568 = byte ptr -568h
; .text:0000000140001000 var_570 = byte ptr -570h
; .text:0000000140001000 var_578 = byte ptr -578h
; .text:0000000140001000 var_580 = byte ptr -580h
; .text:0000000140001000 var_588 = byte ptr -588h
; .text:0000000140001000 var_590 = byte ptr -590h
; .text:0000000140001000 var_598 = byte ptr -598h
; .text:0000000140001000 var_5A0 = byte ptr -5A0h
; .text:0000000140001000 var_5A8 = byte ptr -5A8h
; .text:0000000140001000 var_5B0 = byte ptr -5B0h
; .text:0000000140001000 var_5B8 = byte ptr -5B8h
; .text:0000000140001000 var_5C0 = byte ptr -5C0h
; .text:0000000140001000 var_5C8 = byte ptr -5C8h
; .text:0000000140001000 var_5D0 = byte ptr -5D0h
; .text:0000000140001000 var_5D8 = byte ptr -5D8h
; .text:0000000140001000 var_5E0 = byte ptr -5E0h
; .text:0000000140001000 var_5E8 = byte ptr -5E8h
; .text:0000000140001000 var_5F0 = byte ptr -5F0h
; .text:0000000140001000 var_5F8 = byte ptr -5F8h
; .text:0000000140001000 var_600 = byte ptr -600h
; .text:0000000140001000 var_608 = byte ptr -608h
; .text:0000000140001000 var_610 = byte ptr -610h
; .text:0000000140001000 var_618 = byte ptr -618h
; .text:0000000140001000 var_620 = byte ptr -620h
; .text:0000000140001000 var_628 = byte ptr -628h
; .text:0000000140001000 var_630 = byte ptr -630h
; .text:0000000140001000 var_638 = byte ptr -638h
; .text:0000000140001000 var_640 = byte ptr -640h
; .text:0000000140001000 var_648 = byte ptr -648h
; .text:0000000140001000 var_650 = byte ptr -650h
; .text:0000000140001000 var_658 = byte ptr -658h
; .text:0000000140001000 var_660 = byte ptr -660h
; .text:0000000140001000 var_668 = byte ptr -668h
; .text:0000000140001000 var_670 = byte ptr -670h
; .text:0000000140001000 var_678 = byte ptr -678h
; .text:0000000140001000 var_680 = byte ptr -680h
; .text:0000000140001000 var_688 = byte ptr -688h
; .text:0000000140001000 var_690 = byte ptr -690h
; .text:0000000140001000 var_698 = byte ptr -698h
; .text:0000000140001000 var_6A0 = byte ptr -6A0h
; .text:0000000140001000 var_6A8 = byte ptr -6A8h
; .text:0000000140001000 var_6B0 = byte ptr -6B0h
; .text:0000000140001000 var_6B8 = byte ptr -6B8h
; .text:0000000140001000 var_6C0 = byte ptr -6C0h
; .text:0000000140001000 var_6C8 = byte ptr -6C8h
; .text:0000000140001000 var_6D0 = byte ptr -6D0h
; .text:0000000140001000 var_6D8 = byte ptr -6D8h
; .text:0000000140001000 var_6E0 = byte ptr -6E0h
; .text:0000000140001000 var_6E8 = byte ptr -6E8h
; .text:0000000140001000 var_6F0 = byte ptr -6F0h
; .text:0000000140001000 var_6F8 = byte ptr -6F8h
; .text:0000000140001000 var_700 = byte ptr -700h
; .text:0000000140001000 var_708 = byte ptr -708h
; .text:0000000140001000 var_710 = byte ptr -710h
; .text:0000000140001000 var_718 = byte ptr -718h
; .text:0000000140001000 var_720 = byte ptr -720h
; .text:0000000140001000 var_728 = byte ptr -728h
; .text:0000000140001000 var_730 = byte ptr -730h
; .text:0000000140001000 var_738 = byte ptr -738h
; .text:0000000140001000 var_740 = byte ptr -740h
; .text:0000000140001000 var_748 = byte ptr -748h
; .text:0000000140001000 var_750 = byte ptr -750h
; .text:0000000140001000 var_758 = byte ptr -758h
; .text:0000000140001000 var_760 = byte ptr -760h
; .text:0000000140001000 var_768 = byte ptr -768h
; .text:0000000140001000 var_770 = byte ptr -770h
; .text:0000000140001000 var_778 = byte ptr -778h
; .text:0000000140001000 var_780 = byte ptr -780h
; .text:0000000140001000 var_788 = byte ptr -788h
; .text:0000000140001000 var_790 = byte ptr -790h
; .text:0000000140001000 var_798 = byte ptr -798h
; .text:0000000140001000 var_7A0 = byte ptr -7A0h
; .text:0000000140001000 var_7A8 = byte ptr -7A8h
; .text:0000000140001000 var_7B0 = byte ptr -7B0h
; .text:0000000140001000 var_7B8 = byte ptr -7B8h
; .text:0000000140001000 var_7C0 = byte ptr -7C0h
; .text:0000000140001000 var_7C8 = byte ptr -7C8h
; .text:0000000140001000 var_7D0 = byte ptr -7D0h
; .text:0000000140001000 var_7D8 = byte ptr -7D8h
; .text:0000000140001000 var_7E0 = byte ptr -7E0h
; .text:0000000140001000 var_7E8 = byte ptr -7E8h
; .text:0000000140001000 var_7F0 = byte ptr -7F0h
; .text:0000000140001000 var_7F8 = byte ptr -7F8h
; .text:0000000140001000 var_800 = byte ptr -800h
; .text:0000000140001000 var_808 = byte ptr -808h
; .text:0000000140001000 var_810 = byte ptr -810h
; .text:0000000140001000 var_818 = byte ptr -818h
; .text:0000000140001000 var_820 = byte ptr -820h
; .text:0000000140001000 var_828 = byte ptr -828h
; .text:0000000140001000 var_830 = byte ptr -830h
; .text:0000000140001000 var_838 = byte ptr -838h
; .text:0000000140001000 var_840 = byte ptr -840h
; .text:0000000140001000 var_848 = byte ptr -848h
; .text:0000000140001000 var_850 = byte ptr -850h
; .text:0000000140001000 var_858 = byte ptr -858h
; .text:0000000140001000 var_860 = byte ptr -860h
; .text:0000000140001000 var_868 = byte ptr -868h
; .text:0000000140001000 var_870 = byte ptr -870h
; .text:0000000140001000 var_878 = byte ptr -878h
; .text:0000000140001000 var_880 = byte ptr -880h
; .text:0000000140001000 var_888 = byte ptr -888h
; .text:0000000140001000 var_890 = byte ptr -890h
; .text:0000000140001000 var_898 = byte ptr -898h
; .text:0000000140001000 var_8A0 = byte ptr -8A0h
; .text:0000000140001000 var_8A8 = byte ptr -8A8h
; .text:0000000140001000 var_8B0 = byte ptr -8B0h
; .text:0000000140001000 var_8B8 = byte ptr -8B8h
; .text:0000000140001000 var_8C0 = byte ptr -8C0h
; .text:0000000140001000 var_8C8 = byte ptr -8C8h
; .text:0000000140001000 var_8D0 = byte ptr -8D0h
; .text:0000000140001000 var_8D8 = byte ptr -8D8h
; .text:0000000140001000 var_8E0 = byte ptr -8E0h
; .text:0000000140001000 var_8E8 = byte ptr -8E8h
; .text:0000000140001000 var_8F0 = byte ptr -8F0h
; .text:0000000140001000 var_8F8 = byte ptr -8F8h
; .text:0000000140001000 var_900 = byte ptr -900h
; .text:0000000140001000 var_908 = byte ptr -908h
; .text:0000000140001000 var_910 = byte ptr -910h
; .text:0000000140001000 var_918 = byte ptr -918h
; .text:0000000140001000 var_920 = byte ptr -920h
; .text:0000000140001000 var_928 = byte ptr -928h
; .text:0000000140001000 var_930 = byte ptr -930h
; .text:0000000140001000 var_938 = byte ptr -938h
; .text:0000000140001000 var_940 = byte ptr -940h
; .text:0000000140001000 var_948 = byte ptr -948h
; .text:0000000140001000 var_950 = byte ptr -950h
; .text:0000000140001000 var_958 = byte ptr -958h
; .text:0000000140001000 var_960 = byte ptr -960h
; .text:0000000140001000 var_968 = byte ptr -968h
; .text:0000000140001000 var_970 = byte ptr -970h
; .text:0000000140001000 var_978 = byte ptr -978h
; .text:0000000140001000 var_980 = byte ptr -980h
; .text:0000000140001000 var_988 = byte ptr -988h
; .text:0000000140001000 var_990 = byte ptr -990h
; .text:0000000140001000 var_998 = byte ptr -998h
; .text:0000000140001000 var_9A0 = byte ptr -9A0h
; .text:0000000140001000 var_9A8 = byte ptr -9A8h
; .text:0000000140001000 var_9B0 = byte ptr -9B0h
; .text:0000000140001000 var_9B8 = byte ptr -9B8h
; .text:0000000140001000 var_9C0 = byte ptr -9C0h
; .text:0000000140001000 var_9C8 = byte ptr -9C8h
; .text:0000000140001000 var_9D0 = byte ptr -9D0h
; .text:0000000140001000 var_9D8 = byte ptr -9D8h
; .text:0000000140001000 var_9E0 = byte ptr -9E0h
; .text:0000000140001000 var_9E8 = byte ptr -9E8h
; .text:0000000140001000 var_9F0 = byte ptr -9F0h
; .text:0000000140001000 var_9F8 = byte ptr -9F8h
; .text:0000000140001000 var_A00 = byte ptr -A00h
; .text:0000000140001000 var_A08 = byte ptr -A08h
; .text:0000000140001000 var_A10 = byte ptr -A10h
; .text:0000000140001000 var_A18 = byte ptr -A18h
; .text:0000000140001000 var_A20 = byte ptr -A20h
; .text:0000000140001000 var_A28 = byte ptr -A28h
; .text:0000000140001000 var_A30 = byte ptr -A30h
; .text:0000000140001000 var_A38 = byte ptr -A38h
; .text:0000000140001000 var_A40 = byte ptr -A40h
; .text:0000000140001000 var_A48 = byte ptr -A48h
; .text:0000000140001000 var_A50 = byte ptr -A50h
; .text:0000000140001000 var_A58 = byte ptr -A58h
; .text:0000000140001000 var_A60 = byte ptr -A60h
; .text:0000000140001000 var_A68 = byte ptr -A68h
; .text:0000000140001000 var_A70 = byte ptr -A70h
; .text:0000000140001000 var_A78 = byte ptr -A78h
; .text:0000000140001000 var_A80 = byte ptr -A80h
; .text:0000000140001000 var_A88 = byte ptr -A88h
; .text:0000000140001000 var_A90 = byte ptr -A90h
; .text:0000000140001000 var_A98 = byte ptr -A98h
; .text:0000000140001000 var_AA0 = byte ptr -AA0h
; .text:0000000140001000 var_AA8 = byte ptr -AA8h
; .text:0000000140001000 var_AB0 = byte ptr -AB0h
; .text:0000000140001000 var_AB8 = byte ptr -AB8h
; .text:0000000140001000 var_AC0 = byte ptr -AC0h
; .text:0000000140001000 var_AC8 = byte ptr -AC8h
; .text:0000000140001000 var_AD0 = byte ptr -AD0h
; .text:0000000140001000 var_AD8 = byte ptr -AD8h
; .text:0000000140001000 var_AE0 = byte ptr -AE0h
; .text:0000000140001000 var_AE8 = byte ptr -AE8h
; .text:0000000140001000 var_AF0 = byte ptr -AF0h
; .text:0000000140001000 var_AF8 = byte ptr -AF8h
; .text:0000000140001000 var_B00 = byte ptr -B00h
; .text:0000000140001000 var_B08 = byte ptr -B08h
; .text:0000000140001000 var_B10 = byte ptr -B10h
; .text:0000000140001000 var_B18 = byte ptr -B18h
; .text:0000000140001000 var_B20 = byte ptr -B20h
; .text:0000000140001000 var_B28 = byte ptr -B28h
; .text:0000000140001000 var_B30 = byte ptr -B30h
; .text:0000000140001000 var_B38 = byte ptr -B38h
; .text:0000000140001000 var_B40 = byte ptr -B40h
; .text:0000000140001000 var_B48 = byte ptr -B48h
; .text:0000000140001000 var_B50 = byte ptr -B50h
; .text:0000000140001000 var_B58 = byte ptr -B58h
; .text:0000000140001000 var_B60 = byte ptr -B60h
; .text:0000000140001000 var_B68 = byte ptr -B68h
; .text:0000000140001000 var_B70 = byte ptr -B70h
; .text:0000000140001000 var_B78 = byte ptr -B78h
; .text:0000000140001000 var_B80 = byte ptr -B80h
; .text:0000000140001000 var_B88 = byte ptr -B88h
; .text:0000000140001000 var_B90 = byte ptr -B90h
; .text:0000000140001000 var_B98 = byte ptr -B98h
; .text:0000000140001000 var_BA0 = byte ptr -BA0h
; .text:0000000140001000 var_BA8 = byte ptr -BA8h
; .text:0000000140001000 var_BB0 = byte ptr -BB0h
; .text:0000000140001000 var_BB8 = byte ptr -BB8h
; .text:0000000140001000 var_BC0 = byte ptr -BC0h
; .text:0000000140001000 var_BC8 = byte ptr -BC8h
; .text:0000000140001000 var_BD0 = byte ptr -BD0h
; .text:0000000140001000 var_BD8 = byte ptr -BD8h
; .text:0000000140001000 var_BE0 = byte ptr -BE0h
; .text:0000000140001000 var_BE8 = byte ptr -BE8h
; .text:0000000140001000 var_BF0 = byte ptr -BF0h
; .text:0000000140001000 var_BF8 = byte ptr -BF8h
; .text:0000000140001000 var_C00 = byte ptr -C00h
; .text:0000000140001000 var_C08 = byte ptr -C08h
; .text:0000000140001000 var_C10 = byte ptr -C10h
; .text:0000000140001000 var_C18 = byte ptr -C18h
; .text:0000000140001000 var_C20 = byte ptr -C20h
; .text:0000000140001000 var_C28 = byte ptr -C28h
; .text:0000000140001000 var_C30 = byte ptr -C30h
; .text:0000000140001000 var_C38 = byte ptr -C38h
; .text:0000000140001000 var_C40 = byte ptr -C40h
; .text:0000000140001000 var_C48 = byte ptr -C48h
; .text:0000000140001000 var_C50 = byte ptr -C50h
; .text:0000000140001000 var_C58 = byte ptr -C58h
; .text:0000000140001000 var_C60 = byte ptr -C60h
; .text:0000000140001000 var_C68 = byte ptr -C68h
; .text:0000000140001000 var_C70 = byte ptr -C70h
; .text:0000000140001000 var_C78 = byte ptr -C78h
; .text:0000000140001000 var_C80 = byte ptr -C80h
; .text:0000000140001000 var_C88 = byte ptr -C88h
; .text:0000000140001000 var_C90 = byte ptr -C90h
; .text:0000000140001000 var_C98 = byte ptr -C98h
; .text:0000000140001000 var_CA0 = byte ptr -CA0h
; .text:0000000140001000 var_CA8 = byte ptr -CA8h
; .text:0000000140001000 var_CB0 = byte ptr -CB0h
; .text:0000000140001000 var_CB8 = byte ptr -CB8h
; .text:0000000140001000 var_CC0 = byte ptr -CC0h
; .text:0000000140001000 var_CC8 = byte ptr -CC8h
; .text:0000000140001000 var_CD0 = byte ptr -CD0h
; .text:0000000140001000 var_CD8 = byte ptr -CD8h
; .text:0000000140001000 var_CE0 = byte ptr -CE0h
; .text:0000000140001000 var_CE8 = byte ptr -CE8h
; .text:0000000140001000 var_CF0 = byte ptr -CF0h
; .text:0000000140001000 var_CF8 = byte ptr -CF8h
; .text:0000000140001000 var_D00 = byte ptr -D00h
; .text:0000000140001000 var_D08 = byte ptr -D08h
; .text:0000000140001000 var_D10 = byte ptr -D10h
; .text:0000000140001000 var_D18 = byte ptr -D18h
; .text:0000000140001000 var_D20 = byte ptr -D20h
; .text:0000000140001000 var_D28 = byte ptr -D28h
; .text:0000000140001000 var_D30 = byte ptr -D30h
; .text:0000000140001000 var_D38 = byte ptr -D38h
; .text:0000000140001000 var_D40 = byte ptr -D40h
; .text:0000000140001000 var_D48 = byte ptr -D48h
; .text:0000000140001000 var_D50 = byte ptr -D50h
; .text:0000000140001000 var_D58 = byte ptr -D58h
; .text:0000000140001000 var_D60 = byte ptr -D60h
; .text:0000000140001000 var_D68 = byte ptr -D68h
; .text:0000000140001000 var_D70 = byte ptr -D70h
; .text:0000000140001000 var_D78 = byte ptr -D78h
; .text:0000000140001000 var_D80 = byte ptr -D80h
; .text:0000000140001000 var_D88 = byte ptr -D88h
; .text:0000000140001000 var_D90 = byte ptr -D90h
; .text:0000000140001000 var_D98 = byte ptr -D98h
; .text:0000000140001000 var_DA0 = byte ptr -DA0h
; .text:0000000140001000 var_DA8 = byte ptr -DA8h
; .text:0000000140001000 var_DB0 = byte ptr -DB0h
; .text:0000000140001000 var_DB8 = byte ptr -DB8h
; .text:0000000140001000 var_DC0 = byte ptr -DC0h
; .text:0000000140001000 var_DC8 = byte ptr -DC8h
; .text:0000000140001000 var_DD0 = byte ptr -DD0h
; .text:0000000140001000 var_DD8 = byte ptr -DD8h
; .text:0000000140001000 var_DE0 = byte ptr -DE0h
; .text:0000000140001000 var_DE8 = byte ptr -DE8h
; .text:0000000140001000 var_DF0 = byte ptr -DF0h
; .text:0000000140001000 var_DF8 = byte ptr -DF8h
; .text:0000000140001000 var_E00 = byte ptr -E00h
; .text:0000000140001000 var_E08 = byte ptr -E08h
; .text:0000000140001000 var_E10 = byte ptr -E10h
; .text:0000000140001000 var_E18 = byte ptr -E18h
; .text:0000000140001000 var_E20 = byte ptr -E20h
; .text:0000000140001000 var_E28 = byte ptr -E28h
; .text:0000000140001000 var_E30 = byte ptr -E30h
; .text:0000000140001000 var_E38 = byte ptr -E38h
; .text:0000000140001000 var_E40 = byte ptr -E40h
; .text:0000000140001000 var_E48 = byte ptr -E48h
; .text:0000000140001000 var_E50 = byte ptr -E50h
; .text:0000000140001000 var_E58 = byte ptr -E58h
; .text:0000000140001000 var_E60 = byte ptr -E60h
; .text:0000000140001000 var_E68 = byte ptr -E68h
; .text:0000000140001000 var_E70 = byte ptr -E70h
; .text:0000000140001000 var_E78 = byte ptr -E78h
; .text:0000000140001000 var_E80 = byte ptr -E80h
; .text:0000000140001000 var_E88 = byte ptr -E88h
; .text:0000000140001000 var_E90 = byte ptr -E90h
; .text:0000000140001000 var_E98 = byte ptr -E98h
; .text:0000000140001000 var_EA0 = byte ptr -EA0h
; .text:0000000140001000 var_EA8 = byte ptr -EA8h
; .text:0000000140001000 var_EB0 = byte ptr -EB0h
; .text:0000000140001000 var_EB8 = byte ptr -EB8h
; .text:0000000140001000 var_EC0 = byte ptr -EC0h
; .text:0000000140001000 var_EC8 = byte ptr -EC8h
; .text:0000000140001000 var_ED0 = byte ptr -ED0h
; .text:0000000140001000 var_ED8 = byte ptr -ED8h
; .text:0000000140001000 var_EE0 = byte ptr -EE0h
; .text:0000000140001000 var_EE8 = byte ptr -EE8h
; .text:0000000140001000 var_EF0 = byte ptr -EF0h
; .text:0000000140001000 var_EF8 = byte ptr -EF8h
; .text:0000000140001000 var_F00 = byte ptr -F00h
; .text:0000000140001000 var_F08 = byte ptr -F08h
; .text:0000000140001000 var_F10 = byte ptr -F10h
; .text:0000000140001000 var_F18 = byte ptr -F18h
; .text:0000000140001000 var_F20 = byte ptr -F20h
; .text:0000000140001000 var_F28 = byte ptr -F28h
; .text:0000000140001000 var_F30 = byte ptr -F30h
; .text:0000000140001000 var_F38 = byte ptr -F38h
; .text:0000000140001000 var_F40 = byte ptr -F40h
; .text:0000000140001000 var_F48 = byte ptr -F48h
; .text:0000000140001000 var_F50 = byte ptr -F50h
; .text:0000000140001000 var_F58 = byte ptr -F58h
; .text:0000000140001000 var_F60 = byte ptr -F60h
; .text:0000000140001000 var_F68 = byte ptr -F68h
; .text:0000000140001000 var_F70 = byte ptr -F70h
; .text:0000000140001000 var_F78 = byte ptr -F78h
; .text:0000000140001000 var_F80 = byte ptr -F80h
; .text:0000000140001000 var_F88 = byte ptr -F88h
; .text:0000000140001000 var_F90 = byte ptr -F90h
; .text:0000000140001000 var_F98 = byte ptr -F98h
; .text:0000000140001000 var_FA0 = byte ptr -FA0h
; .text:0000000140001000 var_FA8 = byte ptr -FA8h
; .text:0000000140001000 var_FB0 = byte ptr -FB0h
; .text:0000000140001000 var_FB8 = byte ptr -FB8h
; .text:0000000140001000 var_FC0 = byte ptr -FC0h
; .text:0000000140001000 var_FC8 = byte ptr -FC8h
; .text:0000000140001000 var_FD0 = byte ptr -FD0h
; .text:0000000140001000 var_FD8 = byte ptr -FD8h
; .text:0000000140001000 var_FE0 = byte ptr -FE0h
; .text:0000000140001000 var_FE8 = byte ptr -FE8h
; .text:0000000140001000 var_FF0 = byte ptr -FF0h
; .text:0000000140001000 var_FF8 = byte ptr -FF8h
; .text:0000000140001000 var_100 = byte ptr -100h
; .text:0000000140001000 var_108 = byte ptr -108h
; .text:0000000140001000 var_110 = byte ptr -110h
; .text:0000000140001000 var_118 = byte ptr -118h
; .text:0000000140001000 var_120 = byte ptr -120h
; .text:0000000140001000 var_128 = byte ptr -128h
; .text:0000000140001000 var_130 = byte ptr -130h
; .text:0000000140001000 var_138 = byte ptr -138h
; .text:0000000140001000 var_140 = byte ptr -140h
; .text:0000000140001000 var_148 = byte ptr -148h
; .text:0000000140001000 var_150 = byte ptr -150h
; .text:0000000140001000 var_158 = byte ptr -158h
; .text:0000000140001000 var_160 = byte ptr -160h
; .text:0000000140001000 var_168 = byte ptr -168h
; .text:0000000140001000 var_170 = byte ptr -170h
; .text:0000000140001000 var_178 = byte ptr -178h
; .text:0000000140001000 var_180 = byte ptr -180h
; .text:0000000140001000 var_188 = byte ptr -188h
; .text:0000000140001000 var_190 = byte ptr -190h
; .text:0000000140001000 var_198 = byte ptr -198h
; .text:0000000140001000 var_