http://youtu.be/AcVTF1HfTb8

Исследование было проведено в Cnc3:Tiberium Wars (7.33.017), Brave Videogame(8.01.10?), PES 2014 (8.03.12), последняя версия на данным момент). Возможно тянется еще с Homeworld 2 (5.00.03).

Суть: 2х уровневый патчинг ключевых развязок по определению лицензионного диска модуля проверки SecuROM. Все было разобрано с помощью оригинально образа с алкоголем и diff_trace на 7.33.017, для остальных – развязки были найдены **в слепую (по аналогии).**

Инструкция (гайд, мануал, F.A.Q.) по правильному поиску инструкций:

ПОДГОТОВИТЕЛЬНАЯ ЧАСТЬ

1. Берется абсолютно любой диск (рекомендуется все-таки DVD)[1] и вставляется в физический или виртуальный привод.
2. Запускаем **target.exe** под отладчиком[2]
3. Дожидаемся когда секуром выплюнет сообщение "Wrong disc inserted. Please insert the original %GAME_NAME% CD/DVD." – весь код защиты распакован.

УРОВЕНЬ 1 [3] [4]

1. Сигнатурная проверка. Ищем последовательность **83E0 1F 3C 1F**[5] т.е. две инструкции и ставим Hardware Breakpoint №1
   AND EAX,0000001F
   CMP AL,1F
   В AL/EAX заносим 0x1F(31).

Проверка: правильно угаданное местоположение и патчинг только этой разводки заставляет секуром выплюнуть сообщение: *Cannot authenticate the original disc. Your disc may require a different software version.*
Please contact the manufacturer of your application or visit http://www.securom.com/message.asp?m=disc for further information.

2. Ищем последовательность **84 98 C0 07 00 00** и ставим Hardware Breakpoint №2
   Инструкция: **TEST BYTE PTR DS:[EAX+7C0],BL** //BL = 1
   В *EAX+0x7C0* любое число от 2 до 10 (В идеале там должна быть 9.) Какие-то спец байты структуры, которая задает кол-во проходов. Для левака: меньше – быстрее проверяется.
3. **Возможны <u>два</u> варианта.**
   3.1 Для 7й версии ищем последовательность **80BF F2070000**, инструкция
   CMP BYTE PTR DS:[EDI+7F2],0
   3.2 Для 8й версии ищем последовательность **80 78 02 00**
   CMP BYTE PTR DS:[EAX+2],0
   и ставим Hardware Breakpoint №3
   Какой-то множитель для интервала. В *EDI+7F2/EAX+2* в идеале должна стоять 2. (по факту – любое число, не равное нулю. Рекомендуется от 5 – 1 чтоб попасть в интервал с первого раза)
4. **<u>Исправление ошибки 2fix</u>**. Если **<u>НЕ</u>** исправить – процесс аварийно завершится (секуром неправильно обсчитывает свои данные с диска)!
   Ищем конструкцию, в [CONST]***(АДРЕС)*** для левого диска всегда будет 0. Тут придется немного погадать:
   CMP BYTE PTR DS:[*CONST*],0
   PUSHFD
   PUSH *CONST*
   JBE SHORT ADDRESS

ставим Hardware Breakpoint №4. В [CONST] в идеале должна быть 2.

ЕСЛИ ВСЕ СДЕЛАНО ПРАВИЛЬНО, ЗАПУСКАЕТСЯ ВТОРАЯ ЧАСТЬ – ГЕОМЕТРИЧЕСКАЯ ПРОВЕРКА: КУРСОР ВНЕЗАПНО МЕНЯЕТСЯ НА КРУТЯЩИЙСЯ ДИСК(temp.ani в TEMP директории). После смены обратно начинается контрольный подсчет попадания в заданный интервал. Внутри проверки геометрии (когда курсор-диск) важных разводок нет!

УРОВЕНЬ 2.

Найти и запатчить 3 (три)[6] раза разводки[7] типа:[4]

```
FLD QWORD PTR DS:[CONST]
FSUB QWORD PTR DS:[CONST]
FMUL QWORD PTR DS:[CONST]
FCOMP QWORD PTR DS:[CONST]
FSTSW AX
TEST AH,05
```

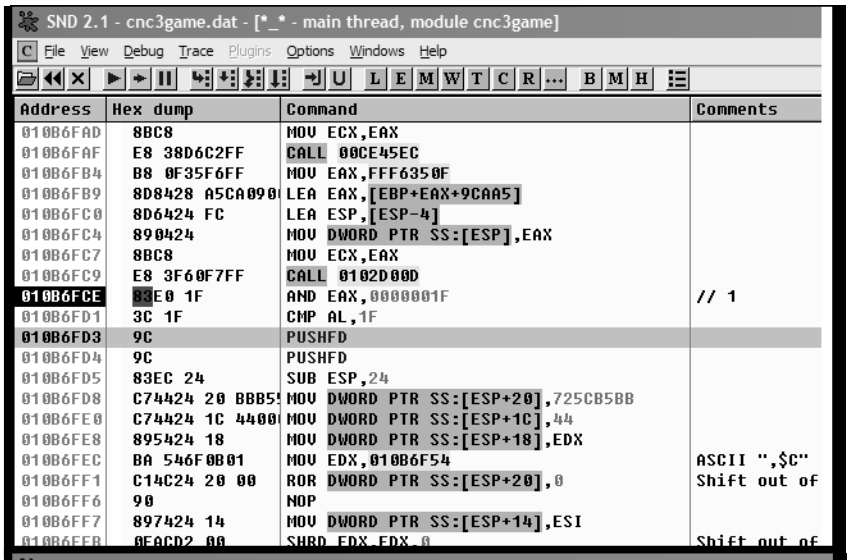
Адрес в *FLD QWORD PTR DS:[адрес]* всегда один и тот же во всех трех. Находим и ставим точку останова на память. Патчится регистр AH

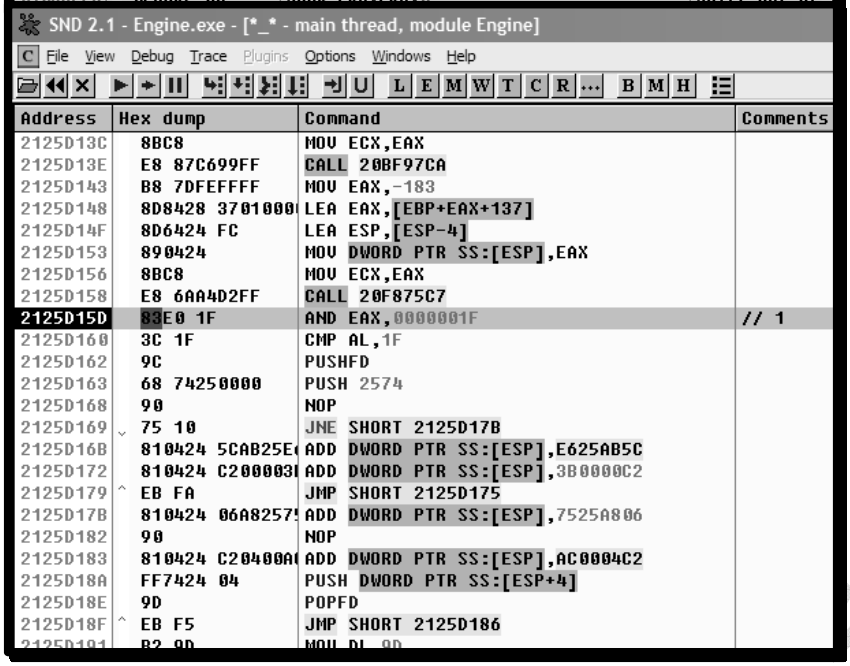
	Для geometry-1	Для geometry-2	Для geometry-3
Значение регистра **AH**	**0**	**1**	**1**

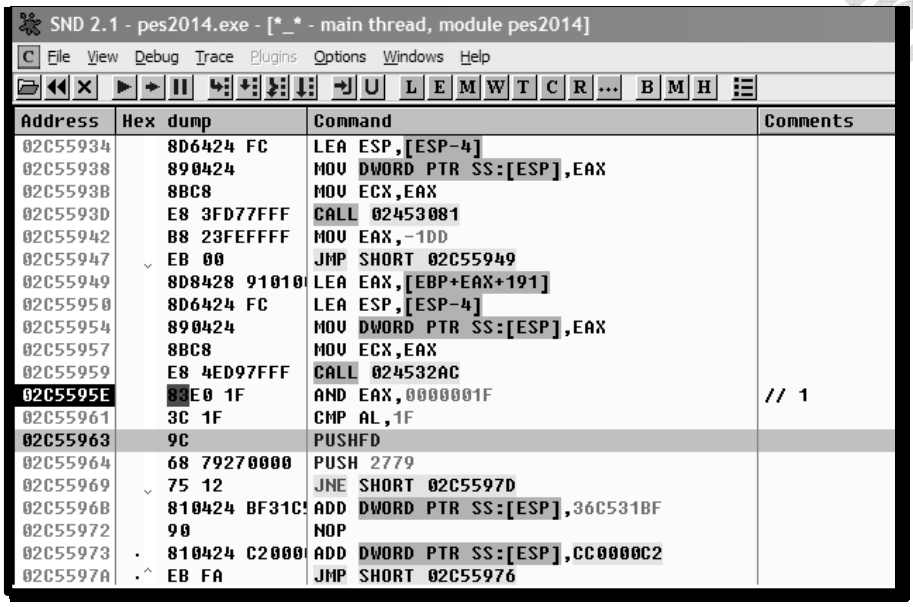
ЕСЛИ ВСЕ СДЕЛАНО ПРАВИЛЬНО, ВЫХОДИМ НА ВТОРИЧНУЮ ПРОВЕРКУ АППАРАТНЫХ ТОЧЕК ОСТАНОВА. НЕ ЗАБУДЬТЕ СНЯТЬ ВСЕ Hardware Breakpoints, иначе ошибка 3000.

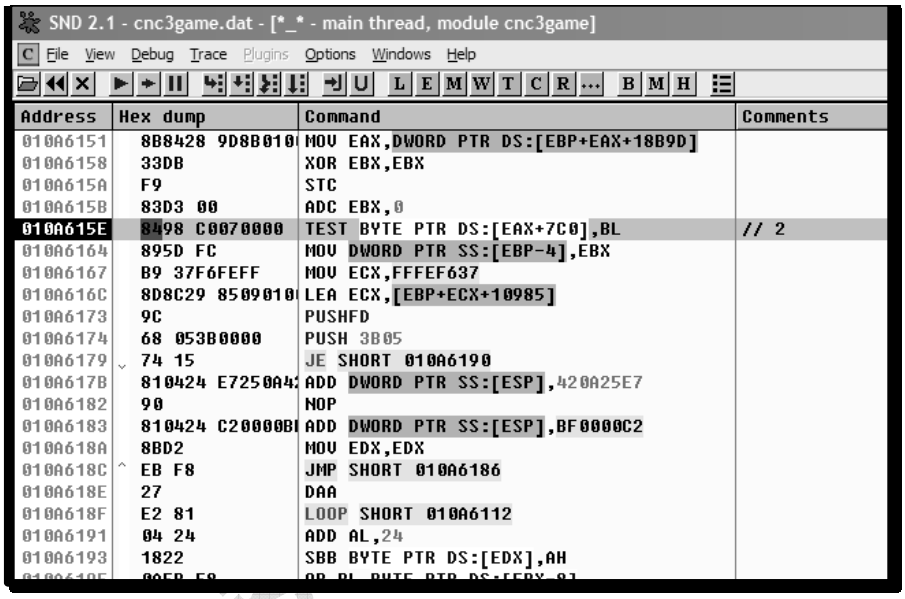
ВАЖНЫЕ ЗАМЕЧАНИЯ:

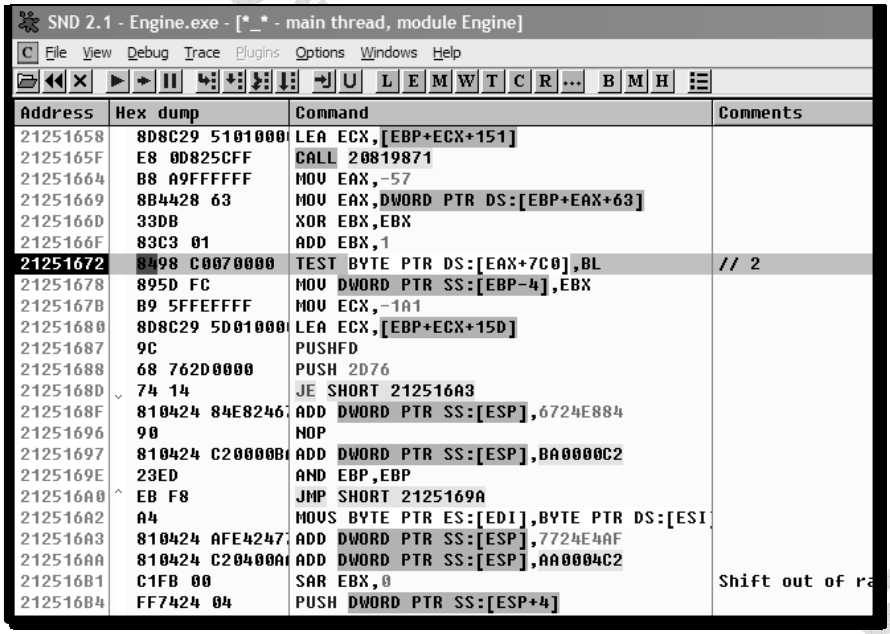
1. Для любого другого диска с секуромом (т.е. от другой защищенной игры) достаточно выполнение пункта 1 в уровне-1 и уровня 2(иногда по необходимости).
2. При наличии рук - сойдет простой ollydbg с оф. сайта, ибо там сбросить BeingDebugged и условная точка останова на ZwQueryInformationProcess с ProcessInfoClass = 7 или 0x1F, ну и переименовать ollydbg.exe в elf.exe
3. После ключевых инструкций на уровне 1 всегда идет PUSHFD(9C)
4. Все развязки находится в коде с обфускацией. Похожие инструкции в коде без обфускации(и вообще типичный код генерируемых компиляторами) можно смело отсекать.
5. Вверху перед инструкциями всегда расположен CALL на какую-то статическую C++ процедуру с одним аргументом.
6. Если не патчить самую первую разводку, вылезет сообщение “Please insert the original disc instead of a backup (1000)”. После нажатия OK, SecuROM, все равно, подстраховывается и переходит на вторую разводку, которую, как и последнюю третью можно спокойно запатчить и успешно пройти уровень 2.
7. В идеале, после этого, путь на OEP открыт! Помешать может код ошибки **9000**, который свидетельствует о применении технологии *SecuROM DATA File Activation*. Нужно достать файл **dfe**

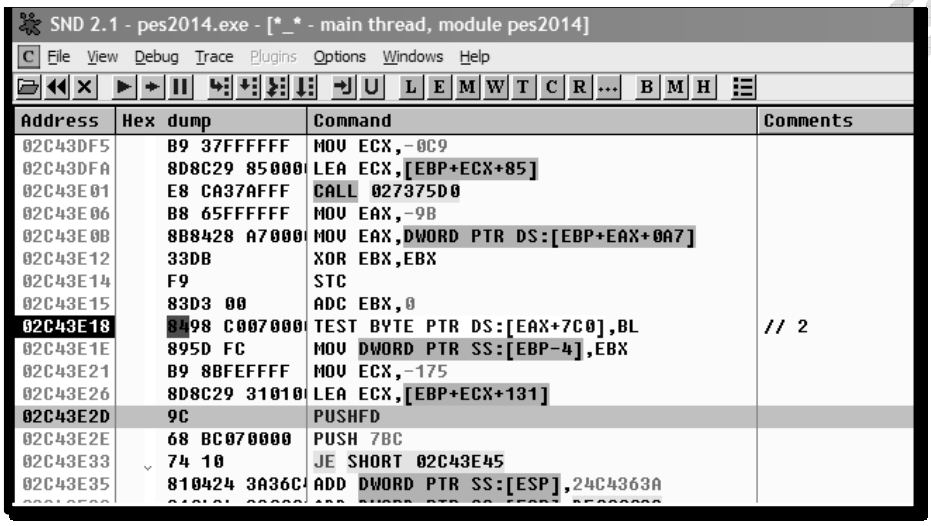

SND 2.1 - cnc3game.dat - [*_* - main thread, module cnc3game]
File View Debug Trace Plugins Options Windows Help
Address Hex dump Command Comments
010B6FAD 8BC8 MOV ECX,EAX
010B6FAF E8 38D6C2FF CALL 00CE45EC
010B6FB4 B8 0F35F6FF MOV EAX,FFF6350F
010B6FB9 8D8428 A5CA090 LEA EAX,[EBP+EAX+9CAA5]
010B6FC0 8D6424 FC LEA ESP,[ESP-4]
010B6FC4 890424 MOV DWORD PTR SS:[ESP],EAX
010B6FC7 8BC8 MOV ECX,EAX
010B6FC9 E8 3F60F7FF CALL 0102D00D
010B6FCE 83E0 1F AND EAX,0000001F // 1
010B6FD1 3C 1F CMP AL,1F
010B6FD3 9C PUSHFD
010B6FD4 9C PUSHFD
010B6FD5 83EC 24 SUB ESP,24
010B6FD8 C74424 20 BBB5 MOV DWORD PTR SS:[ESP+20],725CB5BB
010B6FE0 C74424 1C 4400 MOV DWORD PTR SS:[ESP+1C],44
010B6FE8 895424 18 MOV DWORD PTR SS:[ESP+18],EDX
010B6FEC BA 546F0B01 MOV EDX,010B6F54 ASCII ",$C"
010B6FF1 C14C24 20 00 ROR DWORD PTR SS:[ESP+20],0 Shift out of
010B6FF6 90 NOP
010B6FF7 897424 14 MOV DWORD PTR SS:[ESP+14],ESI
010B6FFB 0FACD2 00 SHRD EDX,EDX,0 Shift out of

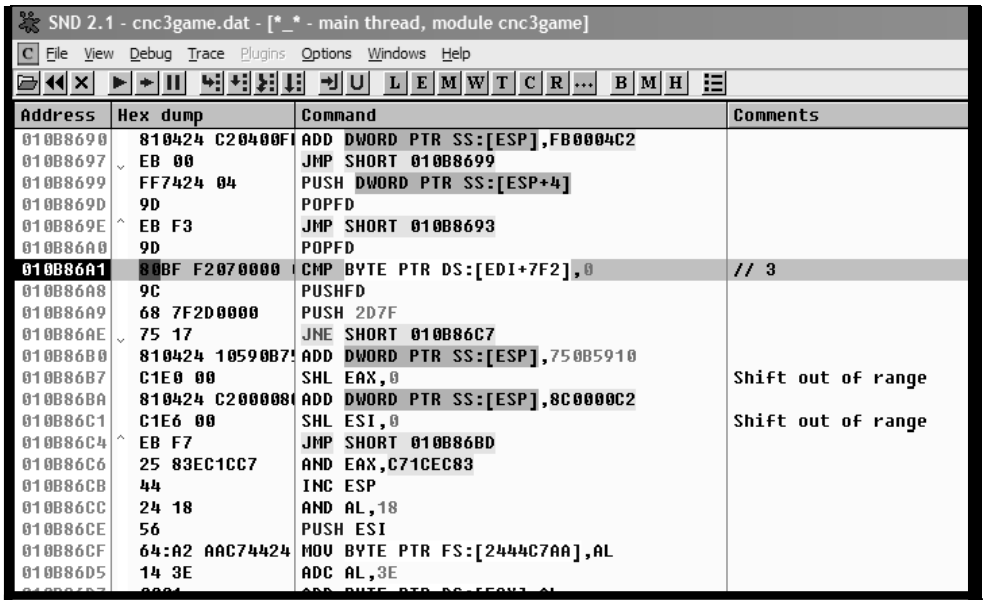

SND 2.1 - Engine.exe - [*_* - main thread, module Engine]
File View Debug Trace Plugins Options Windows Help
Address Hex dump Command Comments
2125D13C 8BC8 MOV ECX,EAX
2125D13E E8 87C699FF CALL 20BF97CA
2125D143 B8 7DFEFFFF MOV EAX,-183
2125D148 8D8428 3701000 LEA EAX,[EBP+EAX+137]
2125D14F 8D6424 FC LEA ESP,[ESP-4]
2125D153 890424 MOV DWORD PTR SS:[ESP],EAX
2125D156 8BC8 MOV ECX,EAX
2125D158 E8 6AA4D2FF CALL 20F875C7
2125D15D 83E0 1F AND EAX,0000001F // 1
2125D160 3C 1F CMP AL,1F
2125D162 9C PUSHFD
2125D163 68 74250000 PUSH 2574
2125D168 90 NOP
2125D169 75 10 JNE SHORT 2125D17B
2125D16B 810424 5CAB25E ADD DWORD PTR SS:[ESP],E625AB5C
2125D172 810424 C200003 ADD DWORD PTR SS:[ESP],3B0000C2
2125D179 EB FA JMP SHORT 2125D175
2125D17B 810424 06A8257 ADD DWORD PTR SS:[ESP],7525A806
2125D182 90 NOP
2125D183 810424 C20400A ADD DWORD PTR SS:[ESP],AC0004C2
2125D18A FF7424 04 PUSH DWORD PTR SS:[ESP+4]
2125D18E 9D POPFD
2125D18F EB F5 JMP SHORT 2125D186

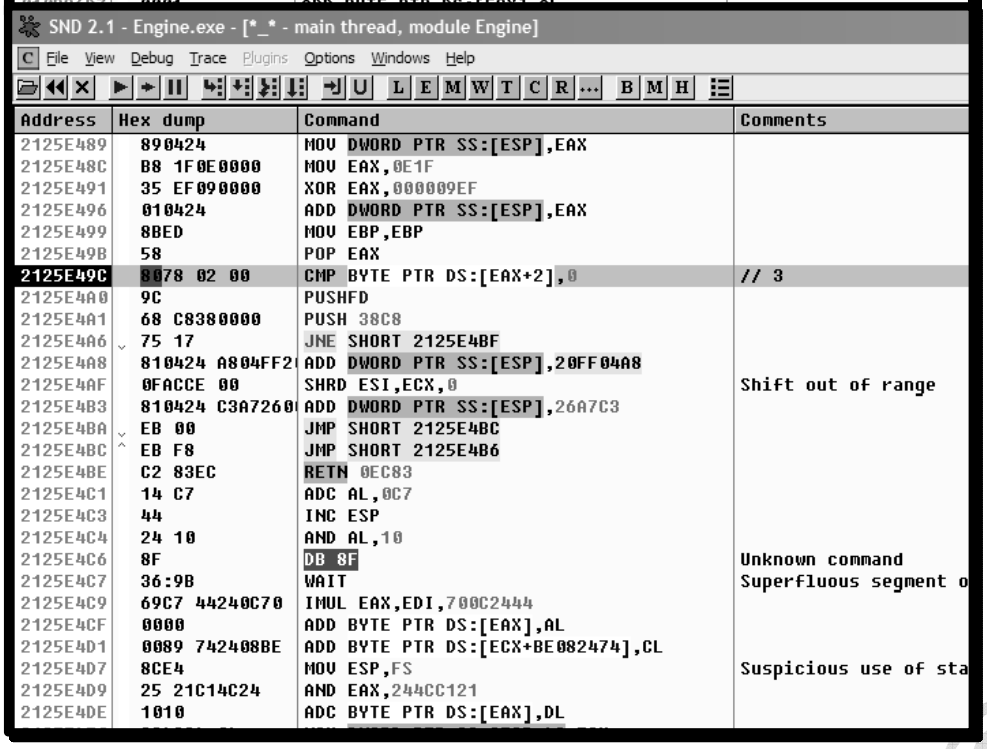

SND 2.1 - pes2014.exe - [*_* - main thread, module pes2014]
File View Debug Trace Plugins Options Windows Help
Address Hex dump Command Comments
02C55934 8D6424 FC LEA ESP,[ESP-4]
02C55938 890424 MOV DWORD PTR SS:[ESP],EAX
02C5593B 8BC8 MOV ECX,EAX
02C5593D E8 3FD77FFF CALL 02453081
02C55942 B8 23FEFFFF MOV EAX,-1DD
02C55947 EB 00 JMP SHORT 02C55949
02C55949 8D8428 91010 LEA EAX,[EBP+EAX+191]
02C55950 8D6424 FC LEA ESP,[ESP-4]
02C55954 890424 MOV DWORD PTR SS:[ESP],EAX
02C55957 8BC8 MOV ECX,EAX
02C55959 E8 4ED97FFF CALL 024532AC
02C5595E 83E0 1F AND EAX,0000001F // 1
02C55961 3C 1F CMP AL,1F
02C55963 9C PUSHFD
02C55964 68 79270000 PUSH 2779
02C55969 75 12 JNE SHORT 02C5597D
02C5596B 810424 BF31C ADD DWORD PTR SS:[ESP],36C531BF
02C55972 90 NOP
02C55973 810424 C2000 ADD DWORD PTR SS:[ESP],CC0000C2
02C5597A EB FA JMP SHORT 02C55976

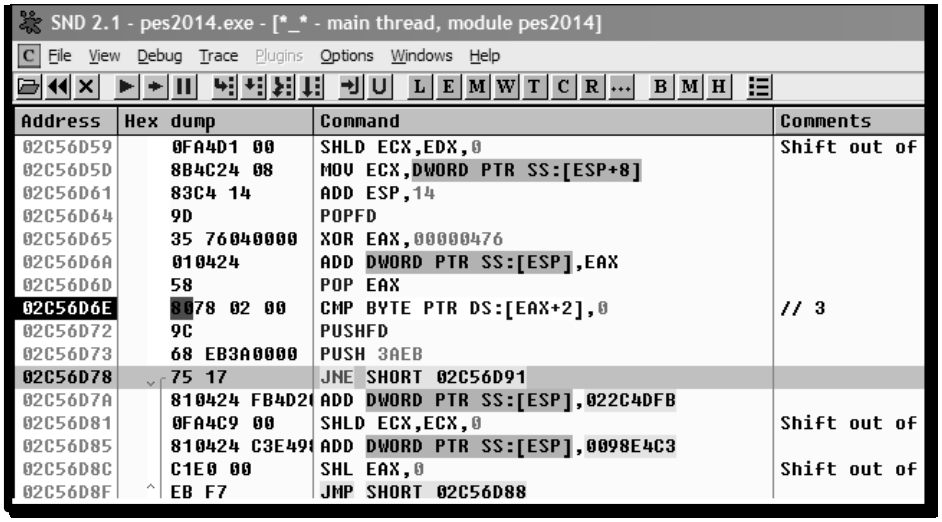

SND 2.1 - cnc3game.dat - [*_* - main thread, module cnc3game]
File View Debug Trace Plugins Options Windows Help
Address Hex dump Command Comments
010A6151 8B8428 9D8B010(MOV EAX,DWORD PTR DS:[EBP+EAX+18B9D]
010A6158 33DB XOR EBX,EBX
010A615A F9 STC
010A615B 83D3 00 ADC EBX,0
010A615E 8498 C0070000 TEST BYTE PTR DS:[EAX+7C0],BL // 2
010A6164 895D FC MOV DWORD PTR SS:[EBP-4],EBX
010A6167 B9 37F6FEFF MOV ECX,FFFEF637
010A616C 8D8C29 8509010(LEA ECX,[EBP+ECX+10985]
010A6173 9C PUSHFD
010A6174 68 053B0000 PUSH 3B05
010A6179 74 15 JE SHORT 010A6190
010A617B 810424 E7250A4 ADD DWORD PTR SS:[ESP],420A25E7
010A6182 90 NOP
010A6183 810424 C20000B(ADD DWORD PTR SS:[ESP],BF0000C2
010A618A 8BD2 MOV EDX,EDX
010A618C EB F8 JMP SHORT 010A6186
010A618E 27 DAA
010A618F E2 81 LOOP SHORT 010A6112
010A6191 04 24 ADD AL,24
010A6193 1822 SBB BYTE PTR DS:[EDX],AH

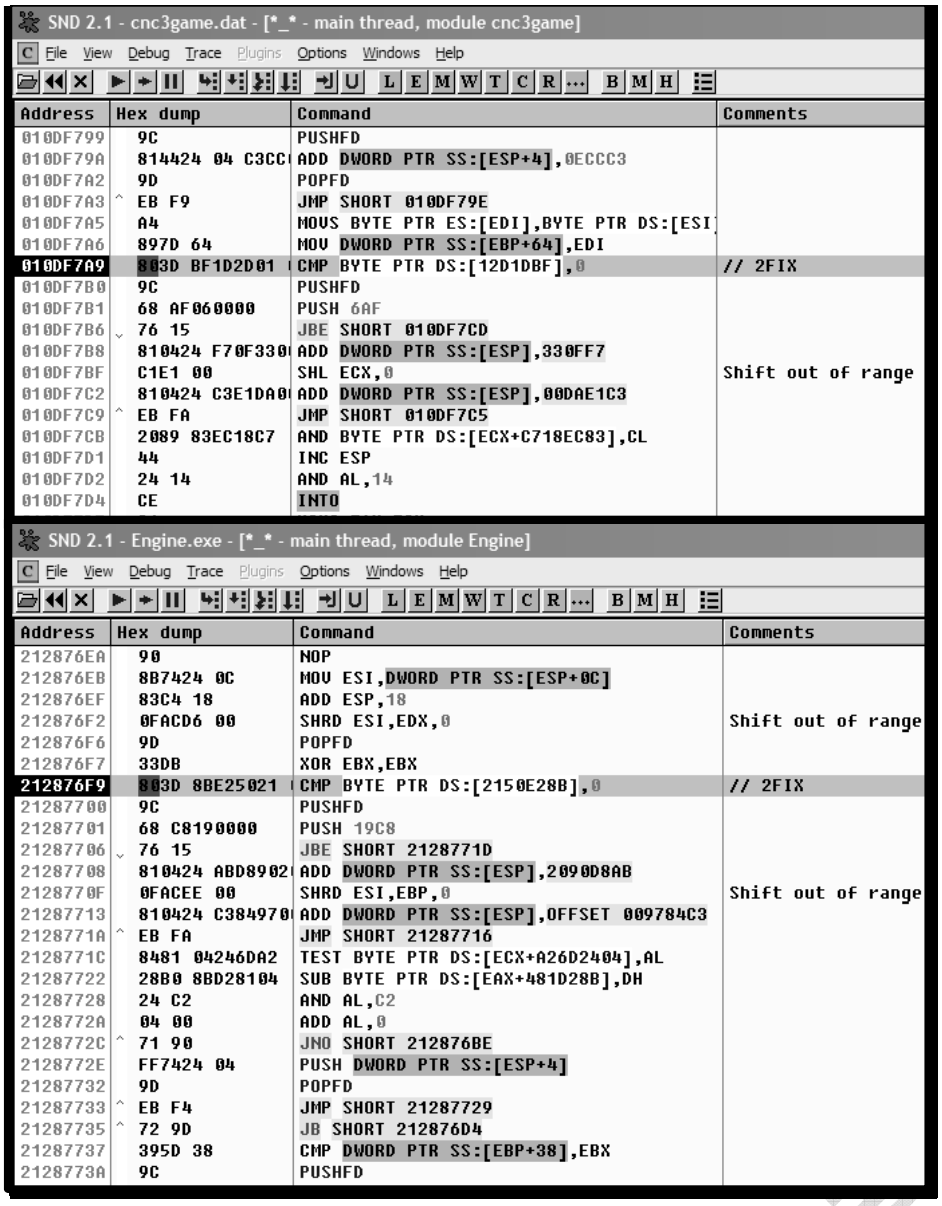

SND 2.1 - Engine.exe - [*_* - main thread, module Engine]
File View Debug Trace Plugins Options Windows Help
Address Hex dump Command Comments
21251658 8D8C29 5101000(LEA ECX,[EBP+ECX+151]
2125165F E8 0D825CFF CALL 20819871
21251664 B8 A9FFFFFF MOV EAX,-57
21251669 8B4428 63 MOV EAX,DWORD PTR DS:[EBP+EAX+63]
2125166D 33DB XOR EBX,EBX
2125166F 83C3 01 ADD EBX,1
21251672 8498 C0070000 TEST BYTE PTR DS:[EAX+7C0],BL // 2
21251678 895D FC MOV DWORD PTR SS:[EBP-4],EBX
2125167B B9 5FFEFFFF MOV ECX,-1A1
21251680 8D8C29 5D01000(LEA ECX,[EBP+ECX+15D]
21251687 9C PUSHFD
21251688 68 762D0000 PUSH 2D76
2125168D 74 14 JE SHORT 212516A3
2125168F 810424 84E8246 ADD DWORD PTR SS:[ESP],6724E884
21251696 90 NOP
21251697 810424 C20000B(ADD DWORD PTR SS:[ESP],BA0000C2
2125169E 23ED AND EBP,EBP
212516A0 EB F8 JMP SHORT 2125169A
212516A2 A4 MOVS BYTE PTR ES:[EDI],BYTE PTR DS:[ESI]
212516A3 810424 AFE4247 ADD DWORD PTR SS:[ESP],7724E4AF
212516AA 810424 C20400A(ADD DWORD PTR SS:[ESP],AA0004C2
212516B1 C1FB 00 SAR EBX,0 Shift out of ra
212516B4 FF7424 04 PUSH DWORD PTR SS:[ESP+4]


SND 2.1 - pes2014.exe - [*_* - main thread, module pes2014]
File View Debug Trace Plugins Options Windows Help
Address Hex dump Command Comments
02C43DF5 B9 37FFFFFF MOV ECX,-0C9
02C43DFA 8D8C29 85000(LEA ECX,[EBP+ECX+85]
02C43E01 E8 CA37AFFF CALL 027375D0
02C43E06 B8 65FFFFFF MOV EAX,-9B
02C43E0B 8B8428 A7000(MOV EAX,DWORD PTR DS:[EBP+EAX+0A7]
02C43E12 33DB XOR EBX,EBX
02C43E14 F9 STC
02C43E15 83D3 00 ADC EBX,0
02C43E18 8498 C007000(TEST BYTE PTR DS:[EAX+7C0],BL // 2
02C43E1E 895D FC MOV DWORD PTR SS:[EBP-4],EBX
02C43E21 B9 8BFEFFFF MOV ECX,-175
02C43E26 8D8C29 31010(LEA ECX,[EBP+ECX+131]
02C43E2D 9C PUSHFD
02C43E2E 68 BC070000 PUSH 7BC
02C43E33 74 10 JE SHORT 02C43E45
02C43E35 810424 3A36C(ADD DWORD PTR SS:[ESP],24C4363A


SND 2.1 - cnc3game.dat - [*_* - main thread, module cnc3game]
File View Debug Trace Plugins Options Windows Help
Address Hex dump Command Comments
010B8690 810424 C20400FI ADD DWORD PTR SS:[ESP],FB0004C2
010B8697 EB 00 JMP SHORT 010B8699
010B8699 FF7424 04 PUSH DWORD PTR SS:[ESP+4]
010B869D 9D POPFD
010B869E EB F3 JMP SHORT 010B8693
010B86A0 9D POPFD
010B86A1 80BF F2070000 CMP BYTE PTR DS:[EDI+7F2],0 // 3
010B86A8 9C PUSHFD
010B86A9 68 7F2D0000 PUSH 2D7F
010B86AE 75 17 JNE SHORT 010B86C7
010B86B0 810424 10590B7 ADD DWORD PTR SS:[ESP],750B5910
010B86B7 C1E0 00 SHL EAX,0 Shift out of range
010B86BA 810424 C200008 ADD DWORD PTR SS:[ESP],8C0000C2
010B86C1 C1E6 00 SHL ESI,0 Shift out of range
010B86C4 EB F7 JMP SHORT 010B86BD
010B86C6 25 83EC1CC7 AND EAX,C71CEC83
010B86CB 44 INC ESP
010B86CC 24 18 AND AL,18
010B86CE 56 PUSH ESI
010B86CF 64:A2 AAC74424 MOV BYTE PTR FS:[2444C7AA],AL
010B86D5 14 3E ADC AL,3E


SND 2.1 - Engine.exe - [*_* - main thread, module Engine]
File View Debug Trace Plugins Options Windows Help
Address Hex dump Command Comments
2125E489 890424 MOV DWORD PTR SS:[ESP],EAX
2125E48C B8 1F0E0000 MOV EAX,0E1F
2125E491 35 EF090000 XOR EAX,000009EF
2125E496 010424 ADD DWORD PTR SS:[ESP],EAX
2125E499 8BED MOV EBP,EBP
2125E49B 58 POP EAX
2125E49C 8078 02 00 CMP BYTE PTR DS:[EAX+2],0 // 3
2125E4A0 9C PUSHFD
2125E4A1 68 C8380000 PUSH 38C8
2125E4A6 75 17 JNE SHORT 2125E4BF
2125E4A8 810424 A804FF2 ADD DWORD PTR SS:[ESP],20FF04A8
2125E4AF 0FACCE 00 SHRD ESI,ECX,0 Shift out of range
2125E4B3 810424 C3A7260 ADD DWORD PTR SS:[ESP],26A7C3
2125E4BA EB 00 JMP SHORT 2125E4BC
2125E4BC EB F8 JMP SHORT 2125E4B6
2125E4BE C2 83EC RETN 0EC83
2125E4C1 14 C7 ADC AL,0C7
2125E4C3 44 INC ESP
2125E4C4 24 10 AND AL,10
2125E4C6 8F DB 8F Unknown command
2125E4C7 36:9B WAIT Superfluous segment o
2125E4C9 69C7 44240C70 IMUL EAX,EDI,700C2444
2125E4CF 0000 ADD BYTE PTR DS:[EAX],AL
2125E4D1 0089 742408BE ADD BYTE PTR DS:[ECX+BE082474],CL
2125E4D7 8CE4 MOV ESP,FS Suspicious use of sta
2125E4D9 25 21C14C24 AND EAX,244CC121
2125E4DE 1010 ADC BYTE PTR DS:[EAX],DL


SND 2.1 - pes2014.exe - [*_* - main thread, module pes2014]
File View Debug Trace Plugins Options Windows Help
Address Hex dump Command Comments
02C56D59 0FA4D1 00 SHLD ECX,EDX,0 Shift out of
02C56D5D 8B4C24 08 MOV ECX,DWORD PTR SS:[ESP+8]
02C56D61 83C4 14 ADD ESP,14
02C56D64 9D POPFD
02C56D65 35 76040000 XOR EAX,00000476
02C56D6A 010424 ADD DWORD PTR SS:[ESP],EAX
02C56D6D 58 POP EAX
02C56D6E 8078 02 00 CMP BYTE PTR DS:[EAX+2],0 // 3
02C56D72 9C PUSHFD
02C56D73 68 EB3A0000 PUSH 3AEB
02C56D78 75 17 JNE SHORT 02C56D91
02C56D7A 810424 FB4D2 ADD DWORD PTR SS:[ESP],022C4DFB
02C56D81 0FA4C9 00 SHLD ECX,ECX,0 Shift out of
02C56D85 810424 C3E49 ADD DWORD PTR SS:[ESP],0098E4C3
02C56D8C C1E0 00 SHL EAX,0 Shift out of
02C56D8F EB F7 JMP SHORT 02C56D88



SND 2.1 - cnc3game.dat - [*_* - main thread, module cnc3game]

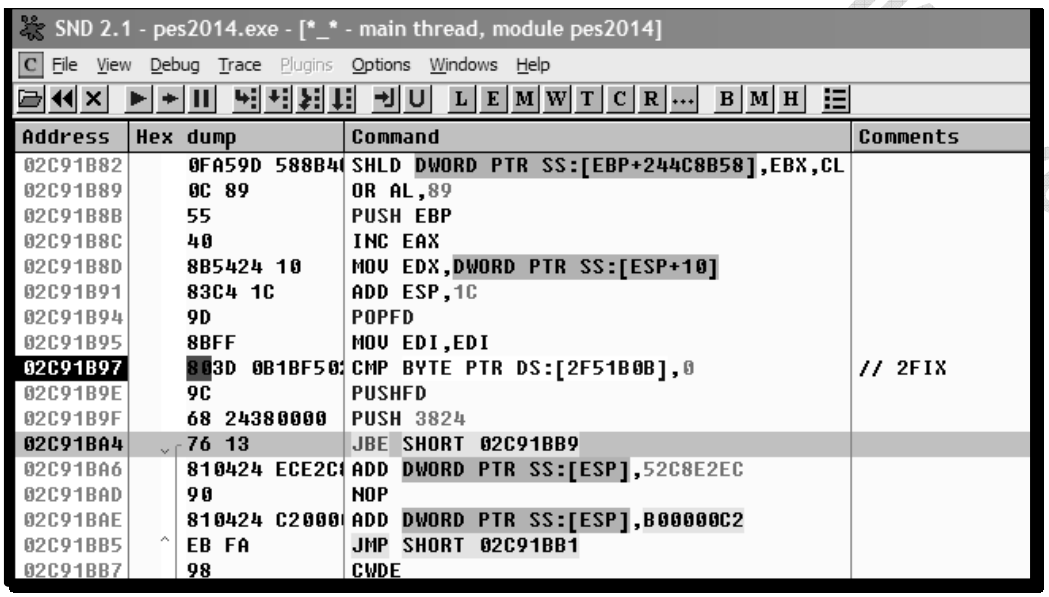
File View Debug Trace Plugins Options Windows Help

Address	Hex dump	Command	Comments
010DF799	9C	PUSHFD	
010DF79A	814424 04 C3CC(	ADD DWORD PTR SS:[ESP+4],0ECCC3	
010DF7A2	9D	POPFD	
010DF7A3	EB F9	JMP SHORT 010DF79E	
010DF7A5	A4	MOVS BYTE PTR ES:[EDI],BYTE PTR DS:[ESI]	
010DF7A6	897D 64	MOV DWORD PTR SS:[EBP+64],EDI	
010DF7A9	803D BF1D2D01 (	CMP BYTE PTR DS:[12D1DBF],0	// 2FIX
010DF7B0	9C	PUSHFD	
010DF7B1	68 AF060000	PUSH 6AF	
010DF7B6	76 15	JBE SHORT 010DF7CD	
010DF7B8	810424 F70F330(	ADD DWORD PTR SS:[ESP],330FF7	
010DF7BF	C1E1 00	SHL ECX,0	Shift out of range
010DF7C2	810424 C3E1DA0(	ADD DWORD PTR SS:[ESP],00DAE1C3	
010DF7C9	EB FA	JMP SHORT 010DF7C5	
010DF7CB	2089 83EC18C7	AND BYTE PTR DS:[ECX+C718EC83],CL	
010DF7D1	44	INC ESP	
010DF7D2	24 14	AND AL,14	
010DF7D4	CE	INTO	

SND 2.1 - Engine.exe - [*_* - main thread, module Engine]

File View Debug Trace Plugins Options Windows Help

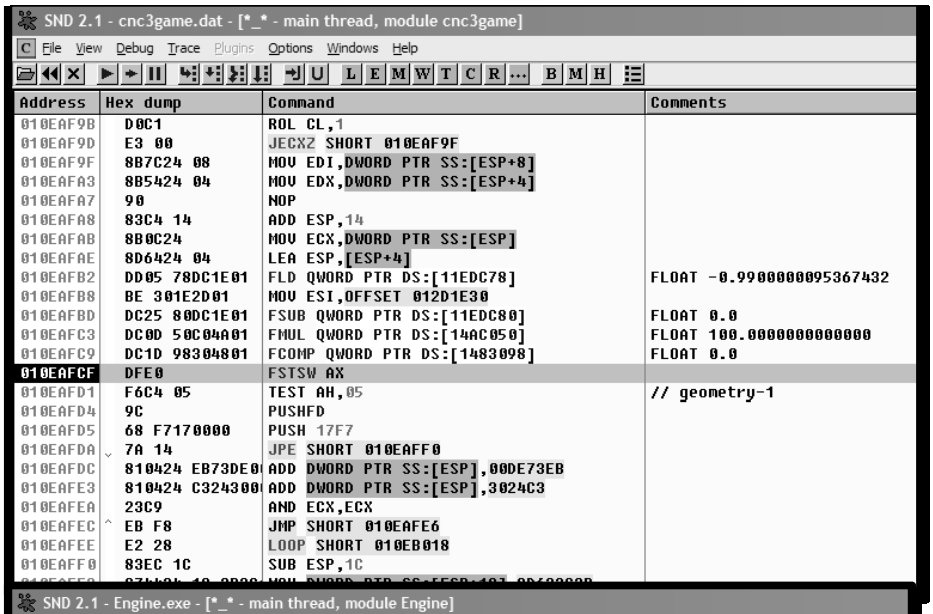
Address	Hex dump	Command	Comments
212876EA	90	NOP	
212876EB	8B7424 0C	MOV ESI,DWORD PTR SS:[ESP+0C]	
212876EF	83C4 18	ADD ESP,18	
212876F2	0FACD6 00	SHRD ESI,EDX,0	Shift out of range
212876F6	9D	POPFD	
212876F7	33DB	XOR EBX,EBX	
212876F9	803D 8BE25021 (	CMP BYTE PTR DS:[2150E28B],0	// 2FIX
21287700	9C	PUSHFD	
21287701	68 C8190000	PUSH 19C8	
21287706	76 15	JBE SHORT 2128771D	
21287708	810424 ABD8902(	ADD DWORD PTR SS:[ESP],2090D8AB	
2128770F	0FACEE 00	SHRD ESI,EBP,0	Shift out of range
21287713	810424 C384970(	ADD DWORD PTR SS:[ESP],OFFSET 009784C3	
2128771A	EB FA	JMP SHORT 21287716	
2128771C	8481 04246DA2	TEST BYTE PTR DS:[ECX+A26D2404],AL	
21287722	28B0 8BD28104	SUB BYTE PTR DS:[EAX+481D28B],DH	
21287728	24 C2	AND AL,C2	
2128772A	04 00	ADD AL,0	
2128772C	71 90	JNO SHORT 212876BE	
2128772E	FF7424 04	PUSH DWORD PTR SS:[ESP+4]	
21287732	9D	POPFD	
21287733	EB F4	JMP SHORT 21287729	
21287735	72 9D	JB SHORT 212876D4	
21287737	395D 38	CMP DWORD PTR SS:[EBP+38],EBX	
2128773A	9C	PUSHFD	

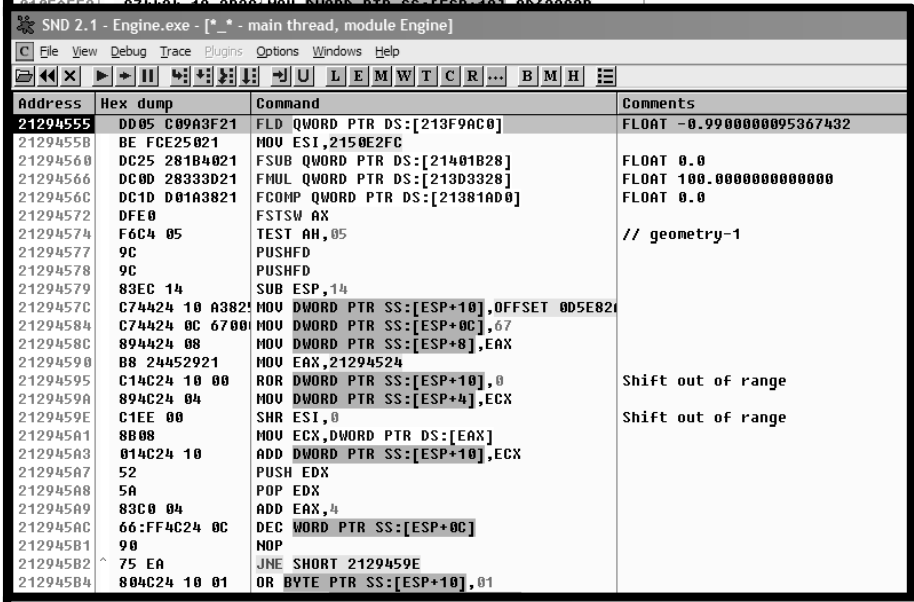


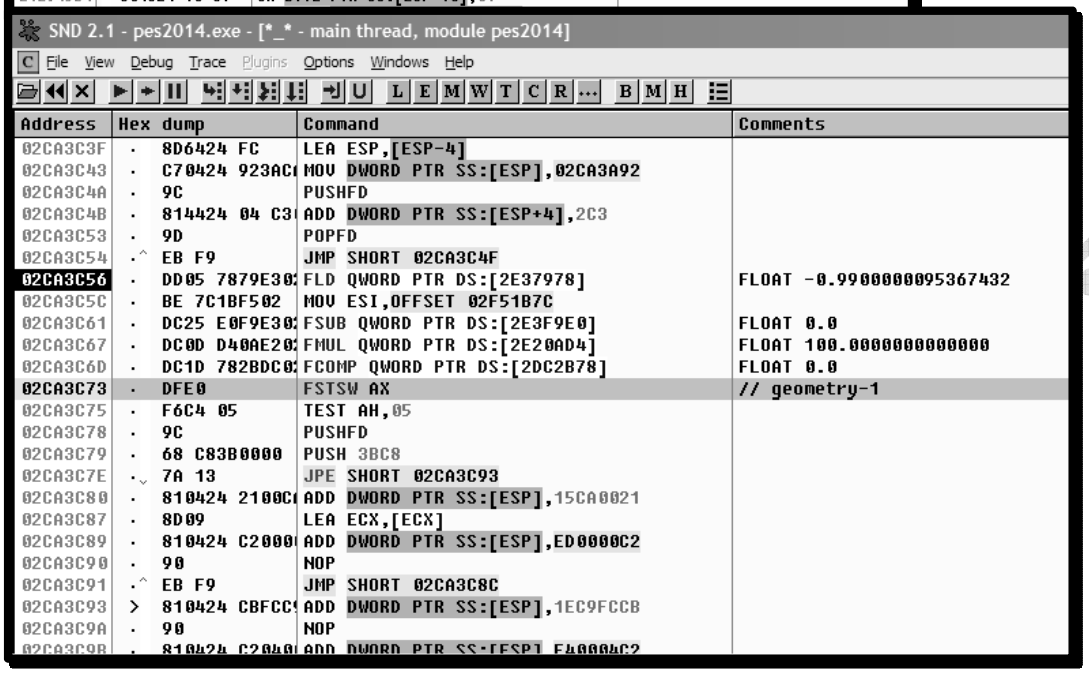
SND 2.1 - pes2014.exe - [*_* - main thread, module pes2014]

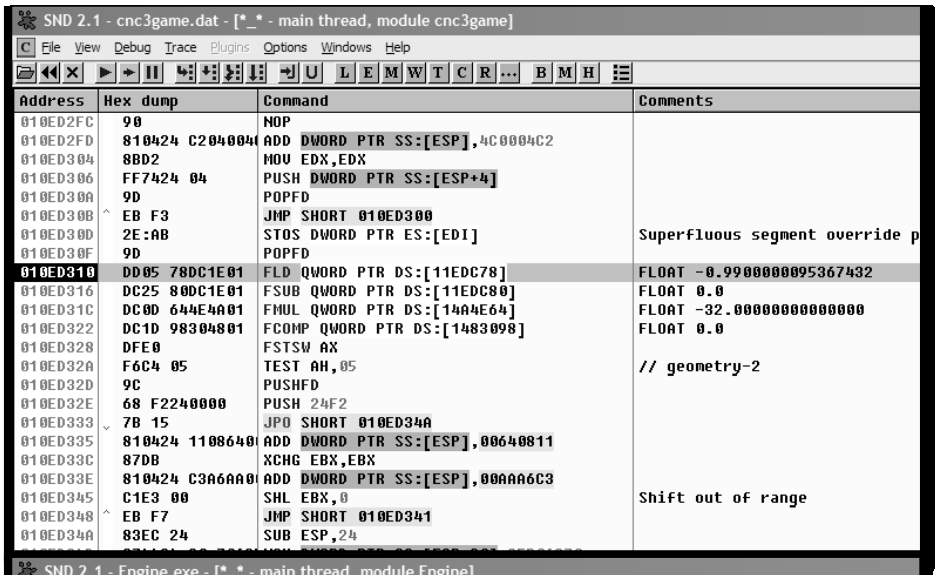
File View Debug Trace Plugins Options Windows Help

Address	Hex dump	Command	Comments
02C91B82	0FA59D 588B4(	SHLD DWORD PTR SS:[EBP+244C8B58],EBX,CL	
02C91B89	0C 89	OR AL,89	
02C91B8B	55	PUSH EBP	
02C91B8C	40	INC EAX	
02C91B8D	8B5424 10	MOV EDX,DWORD PTR SS:[ESP+10]	
02C91B91	83C4 1C	ADD ESP,1C	
02C91B94	9D	POPFD	
02C91B95	8BFF	MOV EDI,EDI	
02C91B97	803D 0B1BF50(	CMP BYTE PTR DS:[2F51B0B],0	// 2FIX
02C91B9E	9C	PUSHFD	
02C91B9F	68 24380000	PUSH 3824	
02C91BA4	76 13	JBE SHORT 02C91BB9	
02C91BA6	810424 ECE2C(	ADD DWORD PTR SS:[ESP],52C8E2EC	
02C91BAD	90	NOP	
02C91BAE	810424 C2000(	ADD DWORD PTR SS:[ESP],B00000C2	
02C91BB5	EB FA	JMP SHORT 02C91BB1	
02C91BB7	98	CWDE	


SND 2.1 - cnc3game.dat - [*_* - main thread, module cnc3game]
File View Debug Trace Plugins Options Windows Help
Address Hex dump Command Comments
010EAF9B D0C1 ROL CL,1
010EAF9D E3 00 JECXZ SHORT 010EAF9F
010EAF9F 8B7C24 08 MOV EDI,DWORD PTR SS:[ESP+8]
010EAFA3 8B5424 04 MOV EDX,DWORD PTR SS:[ESP+4]
010EAFA7 90 NOP
010EAFA8 83C4 14 ADD ESP,14
010EAFAB 8B0C24 MOV ECX,DWORD PTR SS:[ESP]
010EAFAE 8D6424 04 LEA ESP,[ESP+4]
010EAFB2 DD05 78DC1E01 FLD QWORD PTR DS:[11EDC78] FLOAT -0.9900000095367432
010EAFB8 BE 301E2D01 MOV ESI,OFFSET 012D1E30
010EAFBD DC25 80DC1E01 FSUB QWORD PTR DS:[11EDC80] FLOAT 0.0
010EAFC3 DC0D 50C04A01 FMUL QWORD PTR DS:[14AC050] FLOAT 100.0000000000000
010EAFC9 DC1D 98304801 FCOMP QWORD PTR DS:[1483098] FLOAT 0.0
010EAFCF DFE0 FSTSW AX
010EAFD1 F6C4 05 TEST AH,05 // geometry-1
010EAFD4 9C PUSHFD
010EAFD5 68 F7170000 PUSH 17F7
010EAFDA 7A 14 JPE SHORT 010EAFF0
010EAFDC 810424 EB73DE0 ADD DWORD PTR SS:[ESP],00DE73EB
010EAFE3 810424 C324300 ADD DWORD PTR SS:[ESP],3024C3
010EAFEA 23C9 AND ECX,ECX
010EAFEC EB F8 JMP SHORT 010EAFE6
010EAFEE E2 28 LOOP SHORT 010EB018
010EAFF0 83EC 1C SUB ESP,1C


SND 2.1 - Engine.exe - [*_* - main thread, module Engine]
File View Debug Trace Plugins Options Windows Help
Address Hex dump Command Comments
21294555 DD05 C09A3F21 FLD QWORD PTR DS:[213F9AC0] FLOAT -0.9900000095367432
2129455B BE FCE25021 MOV ESI,2150E2FC
21294560 DC25 281B4021 FSUB QWORD PTR DS:[21401B28] FLOAT 0.0
21294566 DC0D 28333D21 FMUL QWORD PTR DS:[213D3328] FLOAT 100.0000000000000
2129456C DC1D D01A3821 FCOMP QWORD PTR DS:[21381AD0] FLOAT 0.0
21294572 DFE0 FSTSW AX
21294574 F6C4 05 TEST AH,05 // geometry-1
21294577 9C PUSHFD
21294578 9C PUSHFD
21294579 83EC 14 SUB ESP,14
2129457C C74424 10 A382 MOV DWORD PTR SS:[ESP+10],OFFSET 0D5E82
21294584 C74424 0C 6700 MOV DWORD PTR SS:[ESP+0C],67
2129458C 894424 08 MOV DWORD PTR SS:[ESP+8],EAX
21294590 B8 24452921 MOV EAX,21294524
21294595 C14C24 10 00 ROR DWORD PTR SS:[ESP+10],0 Shift out of range
2129459A 894C24 04 MOV DWORD PTR SS:[ESP+4],ECX
2129459E C1EE 00 SHR ESI,0 Shift out of range
212945A1 8B08 MOV ECX,DWORD PTR DS:[EAX]
212945A3 014C24 10 ADD DWORD PTR SS:[ESP+10],ECX
212945A7 52 PUSH EDX
212945A8 5A POP EDX
212945A9 83C0 04 ADD EAX,4
212945AC 66:FF4C24 0C DEC WORD PTR SS:[ESP+0C]
212945B1 90 NOP
212945B2 75 EA JNE SHORT 2129459E
212945B4 804C24 10 01 OR BYTE PTR SS:[ESP+10],01

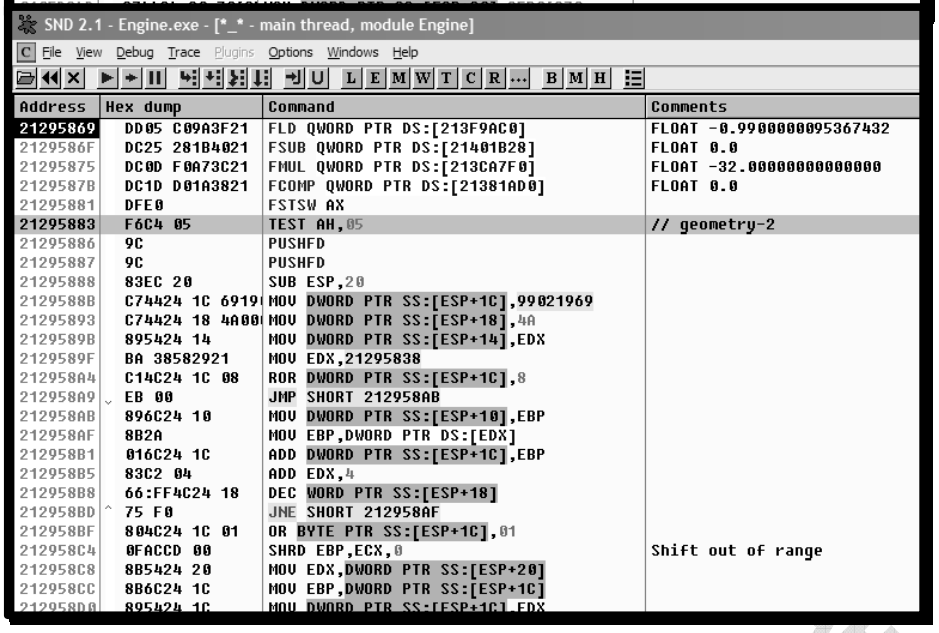

SND 2.1 - pes2014.exe - [*_* - main thread, module pes2014]
File View Debug Trace Plugins Options Windows Help
Address Hex dump Command Comments
02CA3C3F 8D6424 FC LEA ESP,[ESP-4]
02CA3C43 C70424 923AC MOV DWORD PTR SS:[ESP],02CA3A92
02CA3C4A 9C PUSHFD
02CA3C4B 814424 04 C3 ADD DWORD PTR SS:[ESP+4],2C3
02CA3C53 9D POPFD
02CA3C54 EB F9 JMP SHORT 02CA3C4F
02CA3C56 DD05 7879E30 FLD QWORD PTR DS:[2E37978] FLOAT -0.9900000095367432
02CA3C5C BE 7C1BF502 MOV ESI,OFFSET 02F51B7C
02CA3C61 DC25 E0F9E30 FSUB QWORD PTR DS:[2E3F9E0] FLOAT 0.0
02CA3C67 DC0D D40AE20 FMUL QWORD PTR DS:[2E20AD4] FLOAT 100.0000000000000
02CA3C6D DC1D 782BDC0 FCOMP QWORD PTR DS:[2DC2B78] FLOAT 0.0
02CA3C73 DFE0 FSTSW AX // geometry-1
02CA3C75 F6C4 05 TEST AH,05
02CA3C78 9C PUSHFD
02CA3C79 68 C83B0000 PUSH 3BC8
02CA3C7E 7A 13 JPE SHORT 02CA3C93
02CA3C80 810424 2100C ADD DWORD PTR SS:[ESP],15CA0021
02CA3C87 8D09 LEA ECX,[ECX]
02CA3C89 810424 C2000 ADD DWORD PTR SS:[ESP],ED0000C2
02CA3C90 90 NOP
02CA3C91 EB F9 JMP SHORT 02CA3C8C
02CA3C93 810424 CBFCC ADD DWORD PTR SS:[ESP],1EC9FCCB
02CA3C9A 90 NOP



SND 2.1 - cnc3game.dat - [*_* - main thread, module cnc3game]

File View Debug Trace Plugins Options Windows Help

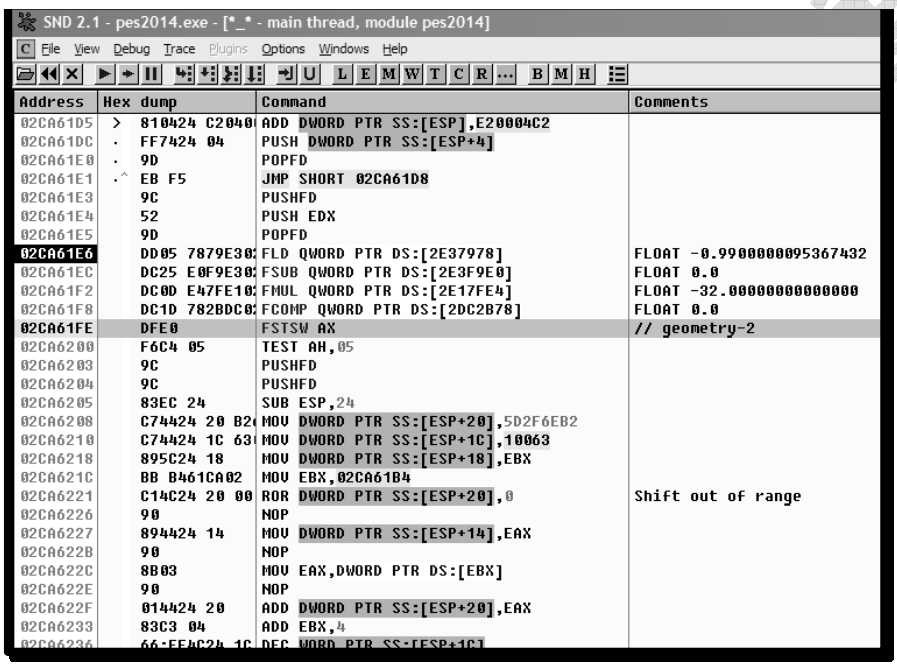
Address	Hex dump	Command	Comments
010ED2FC	90	NOP	
010ED2FD	810424 C204004(	ADD DWORD PTR SS:[ESP],4C0004C2	
010ED304	8BD2	MOV EDX,EDX	
010ED306	FF7424 04	PUSH DWORD PTR SS:[ESP+4]	
010ED30A	9D	POPFD	
010ED30B ^	EB F3	JMP SHORT 010ED300	
010ED30D	2E:AB	STOS DWORD PTR ES:[EDI]	Superfluous segment override p
010ED30F	9D	POPFD	
010ED310	DD05 78DC1E01	FLD QWORD PTR DS:[11EDC78]	FLOAT -0.9900000095367432
010ED316	DC25 80DC1E01	FSUB QWORD PTR DS:[11EDC80]	FLOAT 0.0
010ED31C	DC0D 644E4A01	FMUL QWORD PTR DS:[14A4E64]	FLOAT -32.00000000000000
010ED322	DC1D 98304801	FCOMP QWORD PTR DS:[1483098]	FLOAT 0.0
010ED328	DFE0	FSTSW AX	
010ED32A	F6C4 05	TEST AH,05	// geometry-2
010ED32D	9C	PUSHFD	
010ED32E	68 F2240000	PUSH 24F2	
010ED333 v	7B 15	JPO SHORT 010ED34A	
010ED335	810424 1108640(	ADD DWORD PTR SS:[ESP],00640811	
010ED33C	87DB	XCHG EBX,EBX	
010ED33E	810424 C3A6AA0(	ADD DWORD PTR SS:[ESP],00AAA6C3	
010ED345	C1E3 00	SHL EBX,0	Shift out of range
010ED348 ^	EB F7	JMP SHORT 010ED341	
010ED34A	83EC 24	SUB ESP,24	



SND 2.1 - Engine.exe - [*_* - main thread, module Engine]

File View Debug Trace Plugins Options Windows Help

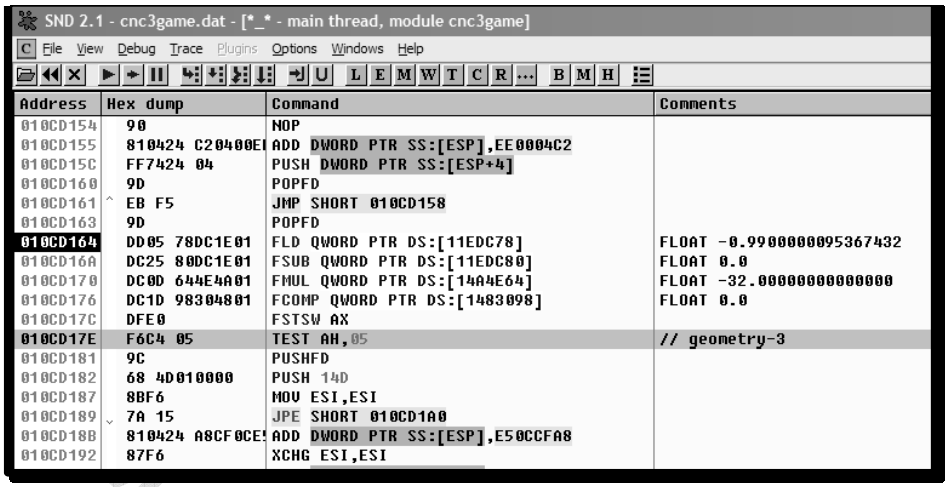
Address	Hex dump	Command	Comments
21295869	DD05 C09A3F21	FLD QWORD PTR DS:[213F9AC0]	FLOAT -0.9900000095367432
2129586F	DC25 281B4021	FSUB QWORD PTR DS:[21401B28]	FLOAT 0.0
21295875	DC0D F0A73C21	FMUL QWORD PTR DS:[213CA7F0]	FLOAT -32.00000000000000
2129587B	DC1D D01A3821	FCOMP QWORD PTR DS:[21381AD0]	FLOAT 0.0
21295881	DFE0	FSTSW AX	
21295883	F6C4 05	TEST AH,05	// geometry-2
21295886	9C	PUSHFD	
21295887	9C	PUSHFD	
21295888	83EC 20	SUB ESP,20	
2129588B	C74424 1C 6919(	MOV DWORD PTR SS:[ESP+1C],99021969	
21295893	C74424 18 4A00(	MOV DWORD PTR SS:[ESP+18],4A	
2129589B	895424 14	MOV DWORD PTR SS:[ESP+14],EDX	
2129589F	BA 38582921	MOV EDX,21295838	
212958A4	C14C24 1C 08	ROR DWORD PTR SS:[ESP+1C],8	
212958A9 v	EB 00	JMP SHORT 212958AB	
212958AB	896C24 10	MOV DWORD PTR SS:[ESP+10],EBP	
212958AF	8B2A	MOV EBP,DWORD PTR DS:[EDX]	
212958B1	016C24 1C	ADD DWORD PTR SS:[ESP+1C],EBP	
212958B5	83C2 04	ADD EDX,4	
212958B8	66:FF4C24 18	DEC WORD PTR SS:[ESP+18]	
212958BD ^	75 F0	JNE SHORT 212958AF	
212958BF	804C24 1C 01	OR BYTE PTR SS:[ESP+1C],01	
212958C4	0FACCD 00	SHRD EBP,ECX,0	Shift out of range
212958C8	8B5424 20	MOV EDX,DWORD PTR SS:[ESP+20]	
212958CC	8B6C24 1C	MOV EBP,DWORD PTR SS:[ESP+1C]	
212958D0	895424 1C	MOV DWORD PTR SS:[ESP+1C],EDX	

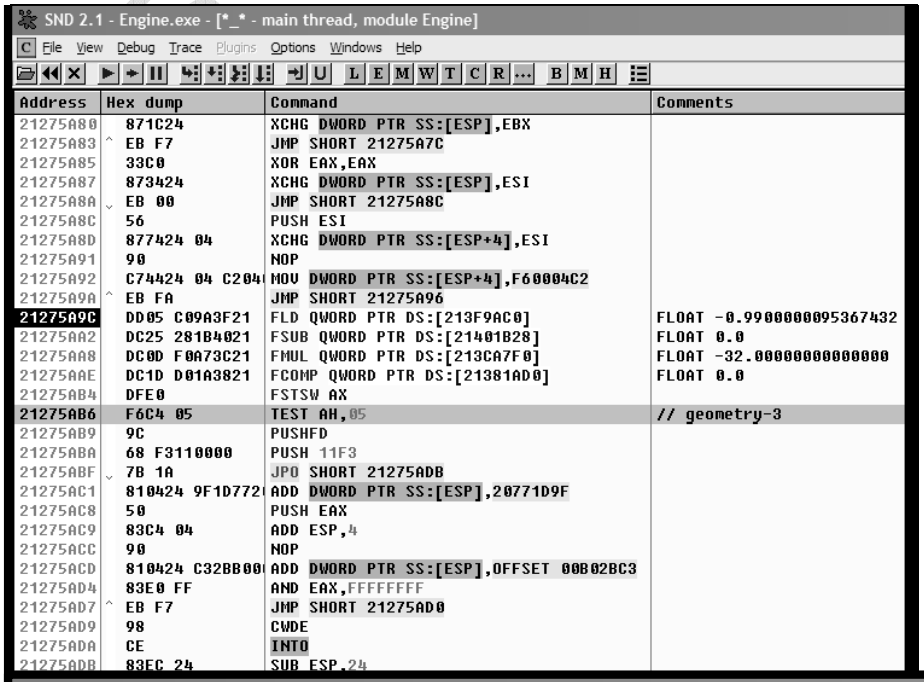


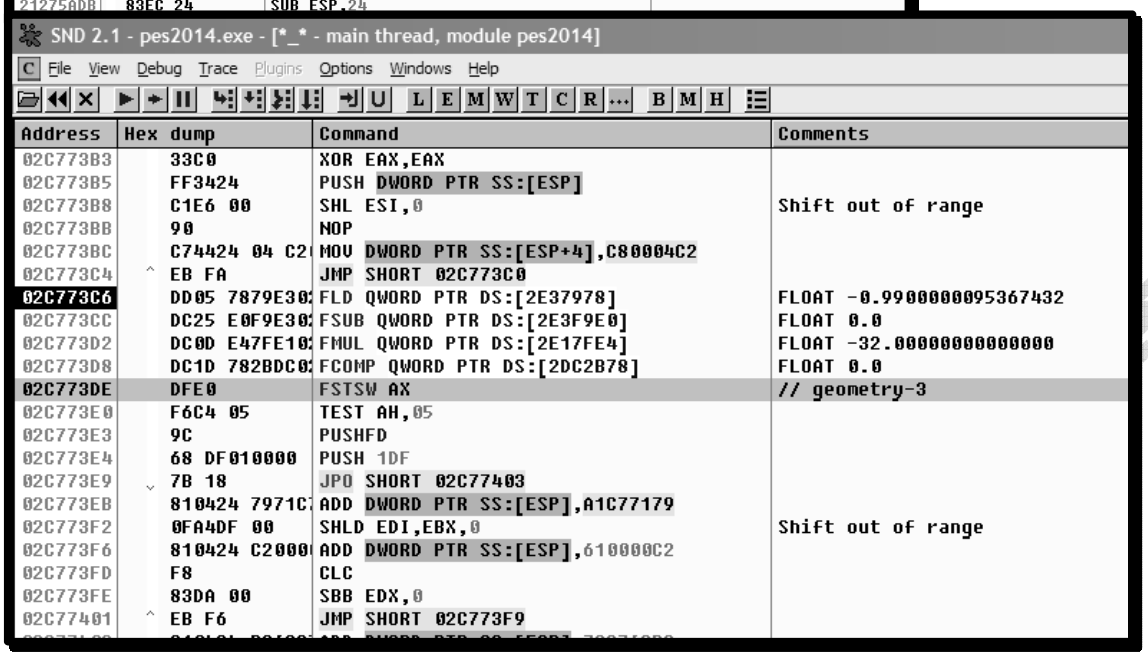
SND 2.1 - pes2014.exe - [*_* - main thread, module pes2014]

File View Debug Trace Plugins Options Windows Help

Address	Hex dump	Command	Comments
02CA61D5 >	810424 C2040(	ADD DWORD PTR SS:[ESP],E2004C2	
02CA61DC .	FF7424 04	PUSH DWORD PTR SS:[ESP+4]	
02CA61E0 .	9D	POPFD	
02CA61E1 .^	EB F5	JMP SHORT 02CA61D8	
02CA61E3	9C	PUSHFD	
02CA61E4	52	PUSH EDX	
02CA61E5	9D	POPFD	
02CA61E6	DD05 7879E30(	FLD QWORD PTR DS:[2E37978]	FLOAT -0.9900000095367432
02CA61EC	DC25 E0F9E30(	FSUB QWORD PTR DS:[2E3F9E0]	FLOAT 0.0
02CA61F2	DC0D E47FE10(	FMUL QWORD PTR DS:[2E17FE4]	FLOAT -32.00000000000000
02CA61F8	DC1D 782BDC0(	FCOMP QWORD PTR DS:[2DC2B78]	FLOAT 0.0
02CA61FE	DFE0	FSTSW AX	// geometry-2
02CA6200	F6C4 05	TEST AH,05	
02CA6203	9C	PUSHFD	
02CA6204	9C	PUSHFD	
02CA6205	83EC 24	SUB ESP,24	
02CA6208	C74424 20 B2(	MOV DWORD PTR SS:[ESP+20],5D2F6EB2	
02CA6210	C74424 1C 63(	MOV DWORD PTR SS:[ESP+1C],10063	
02CA6218	895C24 18	MOV DWORD PTR SS:[ESP+18],EBX	
02CA621C	BB B461CA02	MOV EBX,02CA61B4	
02CA6221	C14C24 20 00	ROR DWORD PTR SS:[ESP+20],0	Shift out of range
02CA6226	90	NOP	
02CA6227	894424 14	MOV DWORD PTR SS:[ESP+14],EAX	
02CA622B	90	NOP	
02CA622C	8B03	MOV EAX,DWORD PTR DS:[EBX]	
02CA622E	90	NOP	
02CA622F	014424 20	ADD DWORD PTR SS:[ESP+20],EAX	
02CA6233	83C3 04	ADD EBX,4	
02CA6236	66:FF4C24 1C	DEC WORD PTR SS:[ESP+1C]	


SND 2.1 - cnc3game.dat - [*_* - main thread, module cnc3game]
File View Debug Trace Plugins Options Windows Help
Address Hex dump Command Comments
010CD154 90 NOP
010CD155 810424 C20400E ADD DWORD PTR SS:[ESP],EE0004C2
010CD15C FF7424 04 PUSH DWORD PTR SS:[ESP+4]
010CD160 9D POPFD
010CD161 EB F5 JMP SHORT 010CD158
010CD163 9D POPFD
010CD164 DD05 78DC1E01 FLD QWORD PTR DS:[11EDC78] FLOAT -0.9900000095367432
010CD16A DC25 80DC1E01 FSUB QWORD PTR DS:[11EDC80] FLOAT 0.0
010CD170 DC0D 644E4A01 FMUL QWORD PTR DS:[14A4E64] FLOAT -32.00000000000000
010CD176 DC1D 98304801 FCOMP QWORD PTR DS:[1483098] FLOAT 0.0
010CD17C DFE0 FSTSW AX
010CD17E F6C4 05 TEST AH,05 // geometry-3
010CD181 9C PUSHFD
010CD182 68 4D010000 PUSH 14D
010CD187 8BF6 MOV ESI,ESI
010CD189 7A 15 JPE SHORT 010CD1A0
010CD18B 810424 A8CF0CE ADD DWORD PTR SS:[ESP],E50CCFA8
010CD192 87F6 XCHG ESI,ESI


SND 2.1 - Engine.exe - [*_* - main thread, module Engine]
File View Debug Trace Plugins Options Windows Help
Address Hex dump Command Comments
21275A80 871C24 XCHG DWORD PTR SS:[ESP],EBX
21275A83 EB F7 JMP SHORT 21275A7C
21275A85 33C0 XOR EAX,EAX
21275A87 873424 XCHG DWORD PTR SS:[ESP],ESI
21275A8A EB 00 JMP SHORT 21275A8C
21275A8C 56 PUSH ESI
21275A8D 877424 04 XCHG DWORD PTR SS:[ESP+4],ESI
21275A91 90 NOP
21275A92 C74424 04 C204 MOV DWORD PTR SS:[ESP+4],F60004C2
21275A9A EB FA JMP SHORT 21275A96
21275A9C DD05 C09A3F21 FLD QWORD PTR DS:[213F9AC0] FLOAT -0.9900000095367432
21275AA2 DC25 281B4021 FSUB QWORD PTR DS:[21401B28] FLOAT 0.0
21275AA8 DC0D F0A73C21 FMUL QWORD PTR DS:[213CA7F0] FLOAT -32.00000000000000
21275AAE DC1D D01A3821 FCOMP QWORD PTR DS:[21381AD0] FLOAT 0.0
21275AB4 DFE0 FSTSW AX
21275AB6 F6C4 05 TEST AH,05 // geometry-3
21275AB9 9C PUSHFD
21275ABA 68 F3110000 PUSH 11F3
21275ABF 7B 1A JPO SHORT 21275ADB
21275AC1 810424 9F1D772 ADD DWORD PTR SS:[ESP],20771D9F
21275AC8 50 PUSH EAX
21275AC9 83C4 04 ADD ESP,4
21275ACC 90 NOP
21275ACD 810424 C32BB00 ADD DWORD PTR SS:[ESP],OFFSET 00B02BC3
21275AD4 83E0 FF AND EAX,FFFFFFFF
21275AD7 EB F7 JMP SHORT 21275AD0
21275AD9 98 CWDE
21275ADA CE INTO
21275ADB 83EC 24 SUB ESP,24


SND 2.1 - pes2014.exe - [*_* - main thread, module pes2014]
File View Debug Trace Plugins Options Windows Help
Address Hex dump Command Comments
02C773B3 33C0 XOR EAX,EAX
02C773B5 FF3424 PUSH DWORD PTR SS:[ESP]
02C773B8 C1E6 00 SHL ESI,0 Shift out of range
02C773BB 90 NOP
02C773BC C74424 04 C2 MOV DWORD PTR SS:[ESP+4],C80004C2
02C773C4 EB FA JMP SHORT 02C773C0
02C773C6 DD05 7879E30 FLD QWORD PTR DS:[2E37978] FLOAT -0.9900000095367432
02C773CC DC25 E0F9E30 FSUB QWORD PTR DS:[2E3F9E0] FLOAT 0.0
02C773D2 DC0D E47FE10 FMUL QWORD PTR DS:[2E17FE4] FLOAT -32.00000000000000
02C773D8 DC1D 782BDC0 FCOMP QWORD PTR DS:[2DC2B78] FLOAT 0.0
02C773DE DFE0 FSTSW AX // geometry-3
02C773E0 F6C4 05 TEST AH,05
02C773E3 9C PUSHFD
02C773E4 68 DF010000 PUSH 1DF
02C773E9 7B 18 JPO SHORT 02C77403
02C773EB 810424 7971C ADD DWORD PTR SS:[ESP],A1C77179
02C773F2 0FA4DF 00 SHLD EDI,EBX,0 Shift out of range
02C773F6 810424 C2000 ADD DWORD PTR SS:[ESP],610000C2
02C773FD F8 CLC
02C773FE 83DA 00 SBB EDX,0
02C77401 EB F6 JMP SHORT 02C773F9