



Курс: «АРХИТЕКТУРА ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ» (АВС)

проф. Легалов А.И., проф. Панфилов П.Б.

Программа «Программная инженерия»

Осенний семестр, 2020-2021 учебный год

Семинар 2 – 19.09.2020

АРХИТЕКТУРА ВС:

семинар №2

Цель: Самостоятельная работа по отладке программ на языке ассемблера

- Погружение в среду отладки
- Освоение среды, ее функционала
- Решение практической задачи:
 - разработка программы, использующей динамическое выделение памяти под массив, которая вводит одномерный массив $A[N]$, формирует из элементов массива A новый массив B и выводит его.

Материалы курса ABC

SoftCraft

разноликое программирование

ОТПРАВНАЯ ТОЧКА

ПРОЕКТИРОВАНИЕ

ПАРАДИГМЫ

СИСТЕМЫ
ПРОГРАММИРОВАНИЯ

ТЕХНИКА
КОДИРОВАНИЯ

ИСКУССТВЕННЫЙ
ИНТЕЛЛЕКТ

ТЕОРИЯ

УЧЕБНЫЙ ПРОЦЕСС

РАЗНОЕ

ОБ АВТОРЕ

Архитектура вычислительных систем

Содержание раздела

Об этом разделе

Лекции

1. Архитектура ВС. Основные понятия
2. Архитектура ВС. Уровень набора команд

Семинары

1. Разработка программ на Ассемблере
2. Отладка ассемблерных программ

Источники информации по дисциплине

1. Ассемблер процессоров Intel
2. Отладка программ, написанных на Ассемблере (для различных архитектур ВС)

Веб-сайт проф. Легалова А.И.: <http://www.softcraft.ru/>

Материалы семинара: 2-я неделя

SoftCraft

разноликое программирование

ОТПРАВНАЯ ТОЧКА

ПРОЕКТИРОВАНИЕ

ПАРАДИГМЫ

СИСТЕМЫ
ПРОГРАММИРОВАНИЯ

ТЕХНИКА
КОДИРОВАНИЯ

ИСКУССТВЕННЫЙ
ИНТЕЛЛЕКТ

ТЕОРИЯ

УЧЕБНЫЙ ПРОЦЕСС

РАЗНОЕ

ОБ АВТОРЕ

Отладка ассемблерных программ

Начальная страница курса

Содержание занятия

1. Отладчик OllyDbg. Особенности использования.
2. Знакомство с регистрами процессора Intel.
3. Разработка и отладка программ, написанных на Ассемблере.

Задание для самостоятельной работы

1. Установить отладчик (OllyDbg) на рабочий компьютер.
Примечание. По согласованию с преподавателем выполнение самостоятельной работы допускается с использованием иных современных архитектур ВС, ОС, а также компиляторов с языка программирования Ассемблер.
2. В соответствии с вариантом задания разработать программу, осуществляющую обработку одномерных массивов. При создании программы использовать подпрограммы для отдельных подзадач (ввода, вывода массивов, обработки данных).
3. Выложить программу и скриншоты на Git в качестве отчета о выполненной работе, предоставляемого преподавателю. Сообщить о выполненной работе. Срок выполнения задания: 2 недели.
Примечание. Для второго задания внутри ранее сформированного проекта создать отдельный каталог с названием task02. Размещение данных внутри этого каталога произвольное.

Задание для самостоятельной работы на 2-й неделе

- Установить отладчик (OllyDbg) на рабочий компьютер.
 - Примечание. По согласованию с преподавателем выполнение самостоятельной работы допускается с использованием иных современных архитектур ВС, ОС, а также компиляторов с языка программирования Ассемблер.
- В соответствии с вариантом задания **разработать программу, осуществляющую обработку одномерных массивов.**
 - При создании программы использовать подпрограммы для отдельных подзадач (ввода, вывода массивов, обработки данных).
- **Выложить программу и скриншоты** на Git в качестве отчета о выполненной работе, предоставляемого преподавателю.
- **Сообщить о выполненной работе.** Срок выполнения задания: **2 недели.**
 - Примечание. Для второго задания внутри ранее сформированного проекта создать отдельный каталог с названием **task02**. Размещение данных внутри этого каталога произвольное.

Инструментарий для семинара №2

ОТПРАВНАЯ ТОЧКА

ПРОЕКТИРОВАНИЕ

ПАРАДИГМЫ

СИСТЕМЫ ПРОГРАММИРОВАНИЯ

ТЕХНИКА КОДИРОВАНИЯ

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

ТЕОРИЯ

УЧЕБНЫЙ ПРОЦЕСС

РАЗНОЕ

ОБ АВТОРЕ

SoftCraft

разноликое программирование

Информация об отладке программ и отладчиках

Начальная страница курса

Отладчик OllyDbg

OllyDbg. Статья в википедии

OllyDbg. Интернет

1. Официальный сайт OllyDbg

2. Цикл статей-переводов по книге «Введение в крэкинг с нуля, используя OllyDbg»

OllyDbg. Каналы на youtube

Канал "Яша Добрый Хакер". Введение в отладку с нуля используя OllyDbg

57 уроков, сделанных по книге «Введения в крэкинг с нуля, используя OllyDbg»

РАЗНОЕ

OllyDbg. Ка

Инструментарий для семинара №2

Olly Debugger в Вики: <https://ru.wikipedia.org/wiki/OllyDbg>

OllyDbg — [shareware](#) 32-битный [отладчик](#) уровня третьего [кольца защиты](#) ([англ. ring-3](#)) для операционных систем [Windows](#), предназначенный для анализа и модификации откомпилированных [исполняемых файлов](#) и [библиотек](#), работающих в режиме пользователя (ring-3).

OllyDbg выгодно отличается от классических отладчиков (таких, как [SoftICE](#)) интуитивно понятным [интерфейсом](#), подсветкой специфических структур кода, простотой в установке и запуске.

В октябре 2013 года была анонсирована 64-битная версия отладчика.

Интерфейс пользователя OllyDbg



Olly Debugger в Вики: <https://ru.wikipedia.org/wiki/OllyDbg>

OllyDbg - PEB.exe - [CPU - main thread, module PEB]

File View Debug Plugins Options Window Help

LEMTWHC/KBR...S

00401231: 55 PUSH EBP
00401232: 8BEC MOV EBP, ESP
00401234: 83C4 F8 ADD ESP, -8
00401237: 68 PUSHAD
00401238: 8B75 08 MOV ESI, DWORD PTR SS:[EBP+8]
00401239: 8B0D LEA EDI, DWORD PTR DS:[403370]
00401241: 33C0 XOR EAX, EAX
00401243: 8A06 MOV AL, BYTE PTR DS:[ESI]
00401245: 8B07 MOV EAX, BYTE PTR DS:[EDI], AL
00401247: 47 INC EDI
00401248: 83C6 02 ADD ESI, 2
0040124E: 8B0E MOV EAX, BYTE PTR DS:[ESI], 0
00401250: 75 F3 JNZ 00401254
00401251: 66C707 0008 MOV WORD PTR DS:[EDI], 0A00
00401255: 83C7 02 ADD EDI, 2
00401258: 66C707 0008 MOV WORD PTR DS:[EDI], 0A00
0040125D: 33C0 XOR EAX, EAX
0040125F: 8B0D LEA EDI, DWORD PTR DS:[403370]
00401265: B9 FFFFFFFF MOV ECX, -1
0040126A: F2AE REPNE SCAS BYTE PTR ES:[EDI]
0040126C: F7D1 NOT ECX
0040126E: 49 DEC ECX
0040126F: 894D FC MOV DWORD PTR SS:[EBP-4], ECX
00401272: 6A 02 PUSH 2
00401274: 6A 00 PUSH 0
00401276: 6A 00 PUSH 0
00401278: FF35 6D324000 PUSH DWORD PTR DS:[40326D]
0040127E: E8 4B000000 CALL JMP, <kernel32.SetFilePointer>
00401283: 6A 00 PUSH 0
00401285: 8D45 F8 LEA EAX, DWORD PTR SS:[EBP-8]
00401288: 50 PUSH EAX
00401289: 68 F75 FC MOV DWORD PTR SS:[EBP-4]
0040128C: 68 70334000 MOV PEB, 00403370
00401291: FF35 6D324000 PUSH DWORD PTR DS:[40326D]
00401293: E8 3B000000 CALL JMP, <kernel32.WriteFile>
0040129C: 68 FF000000 PUSH OFF
004012A1: 68 70334000 MOV PEB, 00403370
004012A6: E8 1D000000 CALL JMP, <kernel32.RtlZeroMemory>
004012AB: 61 POPAD
004012AC: C9 LEAVE
004012AD: C2 0400 RETN 4
004012B0: FF25 00204000 JMP DWORD PTR DS:[<kernel32.CloseHandle>]
004012B6: FF25 04204000 JMP DWORD PTR DS:[<kernel32.CreateFileA>]
004012BC: FF25 08204000 JMP DWORD PTR DS:[<kernel32.ExitProcess>]
004012C2: FF25 0C204000 JMP DWORD PTR DS:[<kernel32.GetCommandLineA>]
004012C8: FF25 10204000 JMP DWORD PTR DS:[<kernel32.RtlZeroMemory>]
004012CE: FF25 14204000 JMP DWORD PTR DS:[<kernel32.SetFilePointer>]
004012D4: FF25 18204000 JMP DWORD PTR DS:[<kernel32.WriteFile>]
004012DA: FF25 1C204000 JMP DWORD PTR DS:[<kernel32.lstrcatA>]
004012E0: FF25 20204000 JMP DWORD PTR DS:[<kernel32.lstrcpyA>]
004012E6: FF25 24204000 JMP DWORD PTR DS:[<user32.wsprintfA>]
004012EC: FF25 28204000 JMP DWORD PTR DS:[<user32.MessageBoxA>]
004012F2: FF25 2C204000 JMP DWORD PTR DS:[<shell32.ShellExecuteA>]
004012F8: DB 00
004012FA: DB 00
004012FB: DB 00
004012FC: DB 00
004012FD: DB 00
004012FE: DB 00
004012FF: DB 00
00401300: DB 00
00401301: DB 00
00401302: DB 00
00401303: DB 00
EBP=0012FFBC
Local calls from 00401131, 004011AC

Registers (FPU)
EAX 00241EBC
ECX 7C91056D ntdll.7C91056D
EDX 00140609
EBX 00400000 PEB.00400000
ESP 0012FFBC
EBP 0012FFBC
ESI 7FFD4000
EDI 0040316D PEB.0040316D
EIP 00401231 PEB.00401231
C 0 ES 0023 32bit 0(FFFFFFFF)
P 0 CS 001B 32bit 0(FFFFFFFF)
S 0 SS 0023 32bit 0(FFFFFFFF)
D 0 DS 0023 32bit 0(FFFFFFFF)
F 0 FS 003B 32bit 7FFDF000(FFF)
T 0 GS 0000 NULL
D 0
0 0 LastErr ERROR_ALREADY_EXISTS (000000B7)
EFL 00000202 (NO, NB, NE, R, NS, PO, GE, G)
ST0 empty 6.4522409303522723840e-4932
ST1 empty -UNORM EAD0 0012FF38 00000000
ST2 empty 6.697353337766765920e+1824
ST3 empty -UNORM 0020 0000003B F5A553F0
ST4 empty -UNORM 003B 0012FF3C 00000000
ST5 empty -UNORM F9D4 00000202 0000001B
ST6 empty 1.00000000000000000000
ST7 empty 1.00000000000000000000
S 2 I 0 E S P U O Z D I
FST 4000 Cond I 0 0 0 Err 0 0 0 0 0 0 0 0 (E0)
FCW 027F Prec NEAR, SS Mask I 1 I 1 I 1

00401291: 55 PUSH EBP
00401292: 8BEC MOV EBP, ESP
00401294: 83C4 F8 ADD ESP, -8
00401297: 68 PUSHAD
00401298: 8B75 08 MOV ESI, DWORD PTR SS:[EBP+8]
00401299: 8B0D LEA EDI, DWORD PTR DS:[403370]
004012A1: 33C0 XOR EAX, EAX
004012A3: 8A06 MOV AL, BYTE PTR DS:[ESI]
004012A5: 8B07 MOV EAX, BYTE PTR DS:[EDI], AL
004012A7: 47 INC EDI
004012A8: 83C6 02 ADD ESI, 2
004012AE: 8B0E MOV EAX, BYTE PTR DS:[ESI], 0
00401250: 75 F3 JNZ 00401254
00401251: 66C707 0008 MOV WORD PTR DS:[EDI], 0A00
00401255: 83C7 02 ADD EDI, 2
00401258: 66C707 0008 MOV WORD PTR DS:[EDI], 0A00
0040125D: 33C0 XOR EAX, EAX
0040125F: 8B0D LEA EDI, DWORD PTR DS:[403370]
00401265: B9 FFFFFFFF MOV ECX, -1
0040126A: F2AE REPNE SCAS BYTE PTR ES:[EDI]
0040126C: F7D1 NOT ECX
0040126E: 49 DEC ECX
0040126F: 894D FC MOV DWORD PTR SS:[EBP-4], ECX
00401272: 6A 02 PUSH 2
00401274: 6A 00 PUSH 0
00401276: 6A 00 PUSH 0
00401278: FF35 6D324000 PUSH DWORD PTR DS:[40326D]
0040127E: E8 4B000000 CALL JMP, <kernel32.SetFilePointer>
00401283: 6A 00 PUSH 0
00401285: 8D45 F8 LEA EAX, DWORD PTR SS:[EBP-8]
00401288: 50 PUSH EAX
00401289: 68 F75 FC MOV DWORD PTR SS:[EBP-4]
0040128C: 68 70334000 MOV PEB, 00403370
00401291: FF35 6D324000 PUSH DWORD PTR DS:[40326D]
00401293: E8 3B000000 CALL JMP, <kernel32.WriteFile>
0040129C: 68 FF000000 PUSH OFF
004012A1: 68 70334000 MOV PEB, 00403370
004012A6: E8 1D000000 CALL JMP, <kernel32.RtlZeroMemory>
004012AB: 61 POPAD
004012AC: C9 LEAVE
004012AD: C2 0400 RETN 4
004012B0: FF25 00204000 JMP DWORD PTR DS:[<kernel32.CloseHandle>]
004012B6: FF25 04204000 JMP DWORD PTR DS:[<kernel32.CreateFileA>]
004012BC: FF25 08204000 JMP DWORD PTR DS:[<kernel32.ExitProcess>]
004012C2: FF25 0C204000 JMP DWORD PTR DS:[<kernel32.GetCommandLineA>]
004012C8: FF25 10204000 JMP DWORD PTR DS:[<kernel32.RtlZeroMemory>]
004012CE: FF25 14204000 JMP DWORD PTR DS:[<kernel32.SetFilePointer>]
004012D4: FF25 18204000 JMP DWORD PTR DS:[<kernel32.WriteFile>]
004012DA: FF25 1C204000 JMP DWORD PTR DS:[<kernel32.lstrcatA>]
004012E0: FF25 20204000 JMP DWORD PTR DS:[<kernel32.lstrcpyA>]
004012E6: FF25 24204000 JMP DWORD PTR DS:[<user32.wsprintfA>]
004012EC: FF25 28204000 JMP DWORD PTR DS:[<user32.MessageBoxA>]
004012F2: FF25 2C204000 JMP DWORD PTR DS:[<shell32.ShellExecuteA>]
004012F8: DB 00
004012FA: DB 00
004012FB: DB 00
004012FC: DB 00
004012FD: DB 00
004012FE: DB 00
004012FF: DB 00
00401300: DB 00
00401301: DB 00
00401302: DB 00
00401303: DB 00

Address Hex dump ASCII
00403000 47 61 64 68 65 72 65 64 20 69 6E 66 6F 72 6D 61 Gathered information: OK...rep
00403010 74 69 6F 6E 3A 20 4F 48 00 00 00 00 72 65 70 ort:txt,PEB - ge
00403020 6F 72 74 2E 74 78 74 00 50 45 42 20 20 47 65 t all OI's, open
00403030 74 20 61 6C 6F 44 6C 6E 27 70 65 6F 79 65 6F .PEB address is at:
00403040 00 50 45 42 20 61 64 72 65 73 70 61 74 3A 2081X.Ldr is at
00403050 20 25 30 38 6C 58 00 4C 64 72 20 69 79 20 61 74 2081X.LIST_E
00403060 20 64 20 25 30 38 6C 58 00 5F 4C 49 5A 5F 45 5F NTRV at 2081
00403070 4E 54 2E 69 6E 68 20 61 74 20 30 20 58 00 3C 00 NTRV at 2081
00403080 49 6D 61 67 65 42 61 73 65 20 3A 20 25 30 38 6C ImageBase : 2081
00403090 58 00 46 6C 69 6E 68 20 61 74 3A 20 25 30 38 6C X.Flink at: 2081
004030A0 58 00 42 69 6E 68 20 61 74 3A 20 25 30 38 6C X.Blink at: 2081
004030B0 58 00 44 6C 6C 20 62 61 73 65 20 3A 20 25 30 38 X.Dll base : 2081
004030C0 6C 58 00 45 6E 74 72 79 50 6F 69 6E 74 20 3A 20 IX.EntryPoint :
004030D0 25 30 38 6C 58 00 53 69 70 65 6F 6D 61 6F 2081X.SizeOfInag
004030E0 65 20 3A 20 25 30 38 6C 58 00 50 72 6F 63 65 73 e : 2081X.Proces
004030F0 73 20 64 65 62 75 6F 67 65 64 00 50 72 6F 63 65 s debugged,Proce
00403100 73 20 6E 6F 74 20 64 65 62 75 6F 64 00 50 72 6F 63 65 s not debugged.
00403110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00403120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Command:
Breakpoint at PEB.00401231

0012FFBC 00400000 RETURN to PEB.00401136 from PEB.00401231
0012FFB0 00400000 PEB.00400000
0012FFB4 00241E00
0012FFB8 00241EBC
0012FFBC 00241EBC
0012FFC0 00401046 RETURN to PEB.<ModuleEntryPoint>+46 from PEB.00401067
0012FFC4 7C81604F RETURN to kernel32.7C81604F
0012FFC8 7C910738 ntdll.7C910738
0012FFCC FFFFFFFF
0012FFD0 7FFD4000
0012FFD4 00049958
0012FFD8 0012FFC8
0012FFDC 84D128B0
0012FFE0 FFFFFFFF
0012FFE4 7C8999F3
0012FFE8 7C816058
0012FFFC 00000000
0012FFF0 00000000
0012FFF4 00000000
0012FFF8 00401000
0012FFFC 00000000
00000000 PEB.<ModuleEntryPoint>

Paused

OllyDbg – для загрузки

Веб-сайт проекта: <http://www.ollydbg.de/>



Progress in [OllyDbg 64](#) (05-Feb-2014)

[VERSION 2.01](#) (27-Sep-2013)

+ Disassembler v2.01, preliminary version (GPL v3)

Off-topic 1: [PaperBack](#) - backups on the paper (v1.10 22-Jul-2013)

Off-topic 2: [Jason](#) - graphical interface to the Hercules S/370 emulator

 Softpedia Clean Award

OllyDbg is a 32-bit assembler level analysing debugger for Microsoft® Windows®. Emphasis on **binary code analysis** makes it particularly useful in cases where source is unavailable. OllyDbg is a shareware, but you can [download](#) and use it **for free**. Special highlights are:

- Intuitive user interface, no cryptical commands
- Code analysis - traces registers, recognizes procedures, loops, API calls, switches, tables, constants and strings
- Directly loads and debugs DLLs
- Object file scanning - locates routines from object files and libraries
- Allows for user-defined labels, comments and function descriptions
- Understands debugging information in Borland® format
- Saves patches between sessions, writes them back to executable file and updates fixups
- Open architecture - many third-party plugins are available

Index

[Main page](#)
[What's new](#)
[Requirements](#)
[Privacy](#)
[Download](#)
[Quick start](#)
[PDK](#)
[Schemes](#)
[FAQs](#)
[Sources](#)

Files

[Odbg200.zip](#)
[Odbg110.zip](#)
[Odbg108b.zip](#)
[Plug110.zip](#)
[Disasm.zip](#)
[Cmdline.zip](#)

Tutorials

[Run trace \(zip\)](#)
[Load DLL \(zip\)](#)

OllyDbg – для загрузки

Веб-сайт проекта: <https://www.softpedia.com/get/Programming/Debuggers-Decompilers-Dissassemblers/OllyDbg.shtml>

SOFTPEDIA®

WINDOWS DRIVERS GAMES MAC ANDROID APK LINUX NEWS & REVIEWS

Softpedia > Windows > Programming > Debuggers/Decompilers/Dissassemblers > OllyDbg

FREE TRIAL ⚠ Driver Booster 6 PRO (60% OFF when you buy)

**DOWNLOAD NOW**124,860 downloads · Updated: July 1, 2019 · **FREWARE** ?

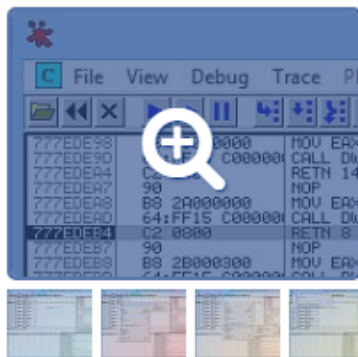
★★★★☆ 4.2/5 111

OllyDbg 2.01

ADD TO WATCHLIST

SEND US AN UPDATE

25 SCREENSHOTS:



RUNS ON:

Windows All

REVIEW

FREE DOWNLOAD

SPECIFICATIONS



100% CLEAN



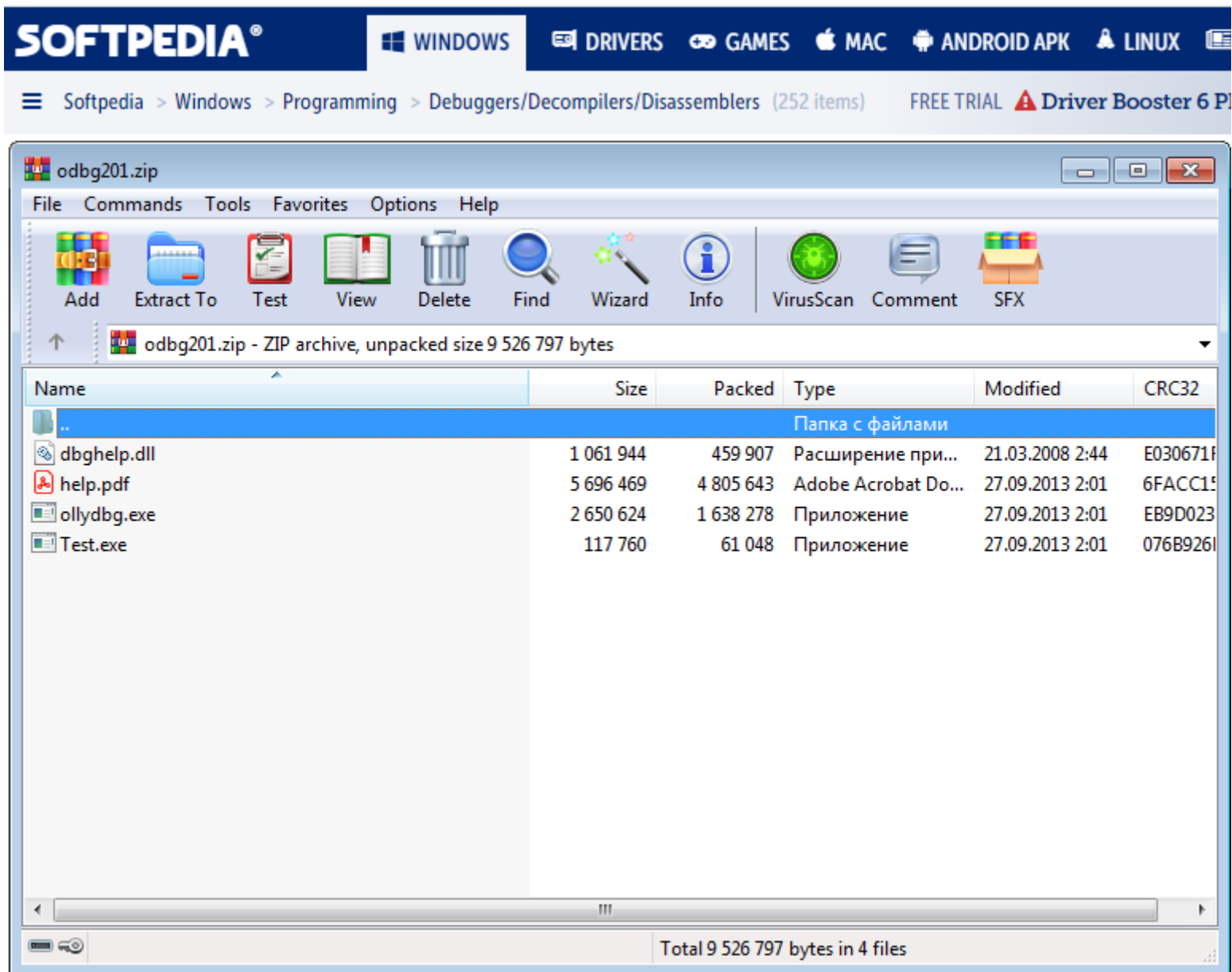
REPORT MALWARE

A handy and reliable assembler level analyzing debugger worth having when you need to examine and modify program executions, as well as to set breakpoints

OllyDbg is a software solution built specifically for debugging multi-thread programs. The application is able to perform code analysis and to display information about registers, loops, API calls, switches and many others. It focuses on binary code analysis, and can reveal important data, especially when the source is unavailable.

It sports a clean interface, and you can easily access

OlyDbg для Windows zip-файл



OllyDbg на вашем компьютере

Quick start - version 1.10

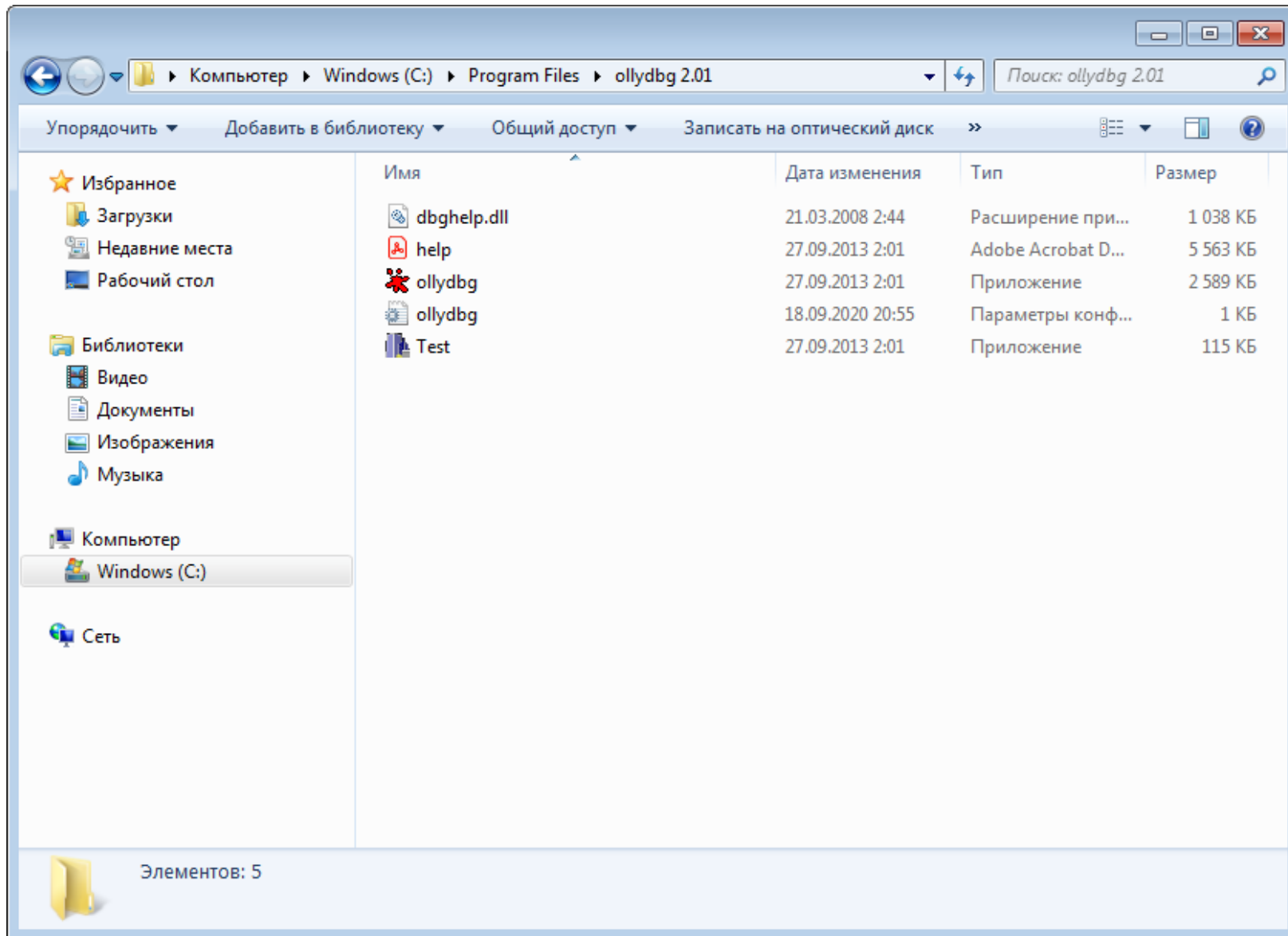
Read this for quick start. Consult help file for details and more features.

Installation is not necessary. Create new directory and unpack odbg110.zip - now you can start!

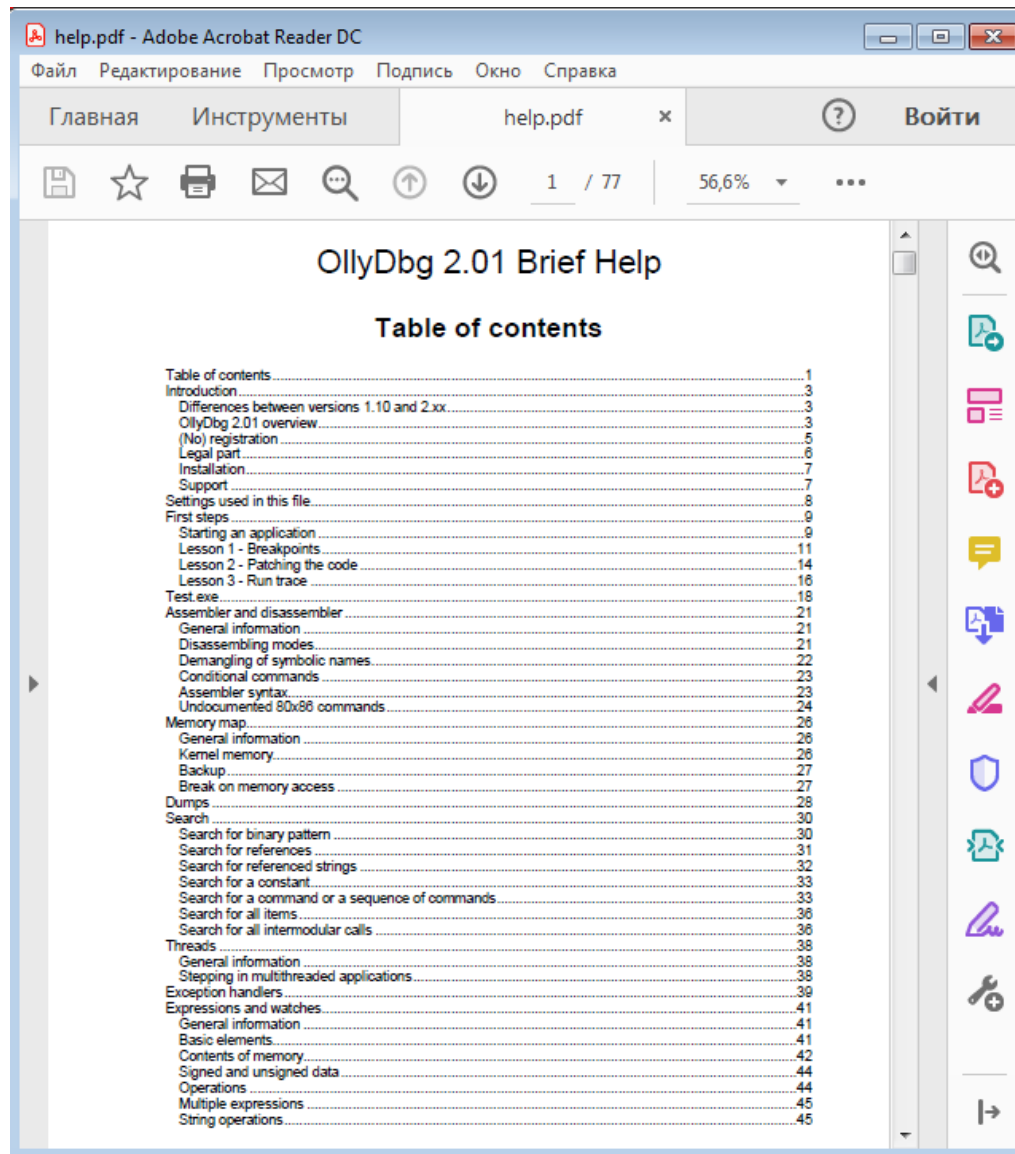
Pop-up menus display only items that apply. Frequently used menu functions:

Function	Window	Menu command	Shortcut
Edit memory as binary, ASCII or UNICODE string	Disassembler, Stack Dump	Binary Edit	Ctrl+E
Undo changes	Disassembler, Dump Registers	Undo selection Undo	Alt+BkSp
Run application	Main	Debug Run	F9
Run to selection	Disassembler	Breakpoint Run to selection	F4
Execute till return	Main	Debug Execute till return	Ctrl+F9
Execute till user code	Main	Debug Execute till user code	Alt+F9
Set/reset INT3 breakpoint	Disassembler Names, Source	Breakpoint Toggle Toggle breakpoint	F2
Set/edit conditional INT3 breakpoint	Disassembler Names, Source	Breakpoint Conditional Conditional breakpoint	Shift+F2
Set/edit conditional logging breakpoint (logs into the Log window)	Disassembler Names, Source	Breakpoint Conditional log Conditional log breakpoint	Shift+F4
Temporarily disable/restore INT3 breakpoint	Breakpoints	Disable Enable	Space

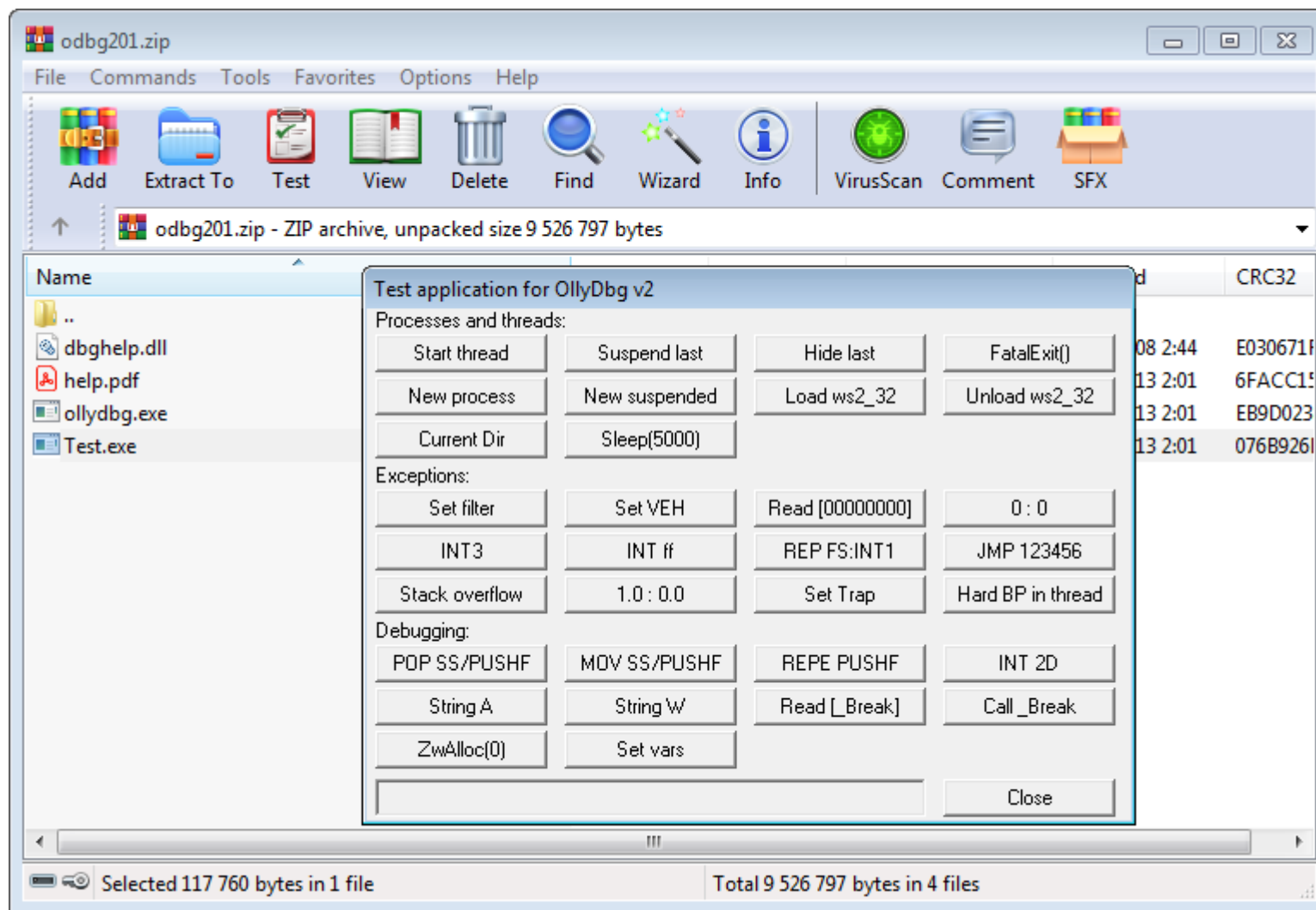
OllyDbg на вашем компьютере



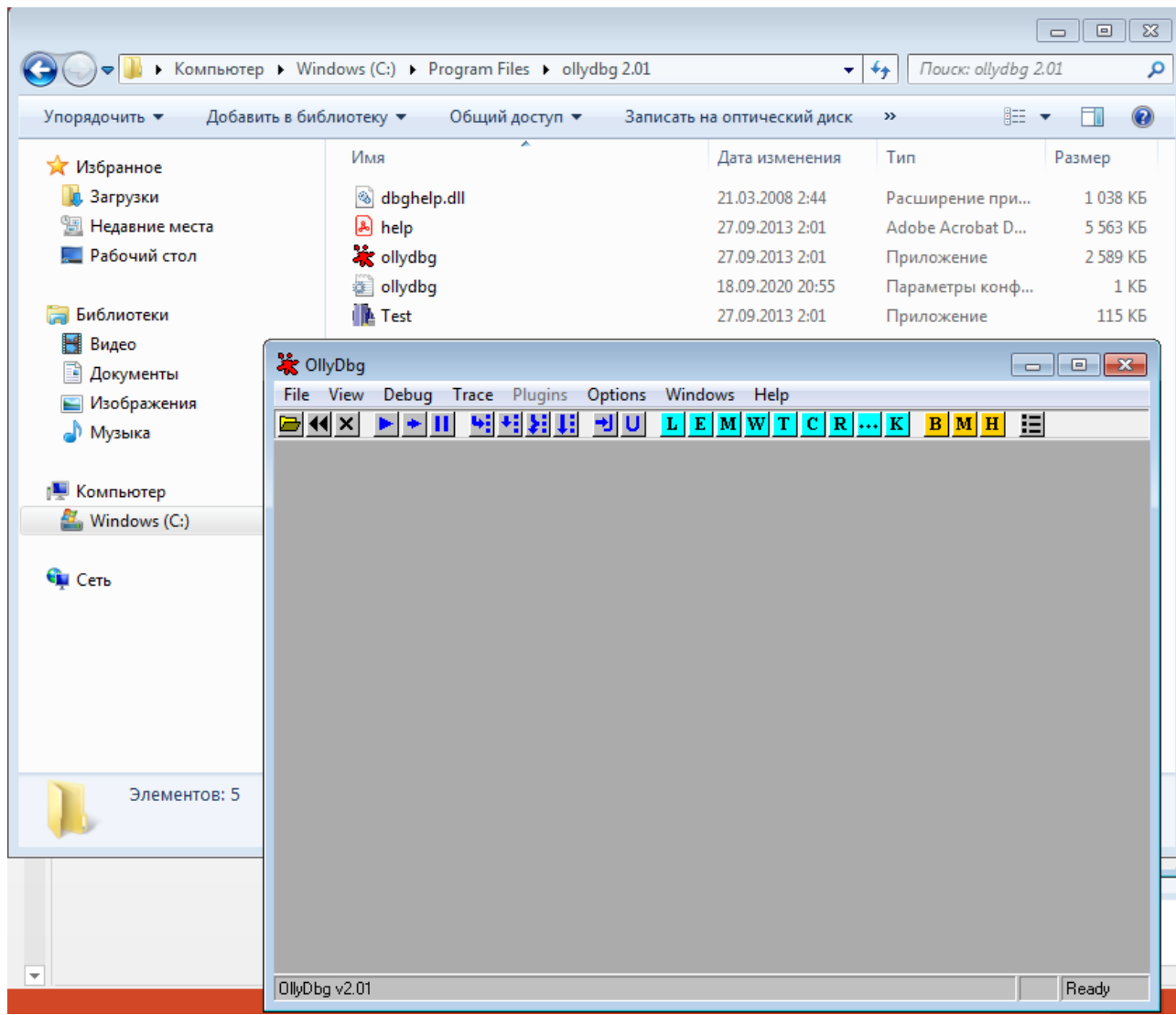
OllyDbg на вашем компьютере



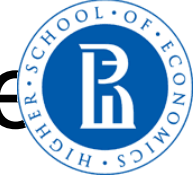
Пример: тестовое приложение для OllyDbg



Запуск ollydbg.exe – среда отладчика



Пример: приложение calculator.exe в OllyDbg



OllyDbg - calculator.exe - [CPU - main thread, module calculator]

File View Debug Trace Plugins Options Windows Help

00402000 68 00104000 PUSH OFFSET 00401000
00402005 FF15 88304000 CALL DWORD PTR DS:[<msvsort.printf>]
00402010 68 43104000 PUSH OFFSET 00401043
00402015 68 32104000 PUSH OFFSET 00401032
00402020 FF15 8C304000 CALL DWORD PTR DS:[<msvsort.scanf>]
00402025 68 09104000 PUSH OFFSET 00401009
00402030 FF15 88304000 CALL DWORD PTR DS:[<msvsort.printf>]
00402035 68 47104000 PUSH OFFSET 00401047
00402040 68 32104000 PUSH OFFSET 00401032
00402045 FF15 8C304000 CALL DWORD PTR DS:[<msvsort.scanf>]
00402050 68 12104000 PUSH OFFSET 00401012
00402055 FF15 88304000 CALL DWORD PTR DS:[<msvsort.printf>]
00402060 FF15 90304000 CALL DWORD PTR DS:[<msvsort._getch>]
00402065 75 2B JNE SHORT 00402069
00402069 8B0D 43104000 MOV ECX, DWORD PTR DS:[401043]
00402070 8B0D 47104000 ADD ECX, DWORD PTR DS:[401047]
00402075 51 PUSH ECX
00402080 68 23104000 PUSH OFFSET 00401023
00402085 FF15 88304000 CALL DWORD PTR DS:[<msvsort.printf>]
00402090 E9 29010000 JMP 00402192
00402095 83F8 2D CMP EAX, 2D
004020A0 75 1D JNE SHORT 004020B8
004020A5 8B0D 43104000 MOV ECX, DWORD PTR DS:[401043]
004020B0 2B0D 47104000 SUB ECX, DWORD PTR DS:[401047]
004020B5 51 PUSH ECX
004020C0 68 23104000 PUSH OFFSET 00401023
004020C5 FF15 88304000 CALL DWORD PTR DS:[<msvsort.printf>]
004020D0 75 2B JNE SHORT 004020E8
004020D5 8B0D 43104000 MOV ECX, DWORD PTR DS:[401043]
004020E0 0F4F0D 47104000 INVL ECX, DWORD PTR DS:[401047]
004020E5 51 PUSH ECX
004020F0 68 23104000 PUSH OFFSET 00401023
004020F5 FF15 88304000 CALL DWORD PTR DS:[<msvsort.printf>]
00402100 E9 E4000000 JMP 00402192

Format = "Enter A:"
MSVCRT.printf
<Xd> = calculator.401043 -> 0
Format = "%d"
MSVCRT.scanf
Format = "Enter B:"
MSVCRT.printf
<Xd> = calculator.401047 -> 0
Format = "%d"
MSVCRT.scanf
Format = "Enter operation:"
MSVCRT.printf
MSVCRT._getch
CONST 2B => '+'

<Xd>
Format = "Result: %d"
MSVCRT.printf

<Xd>
Format = "Result: %d"
MSVCRT.printf

<Xd>
Format = "Result: %d"
MSVCRT.printf

Stack [000CFF88]=0
Imm=calculator.00401000, ASCII "Enter A:"

calculator.<ModuleEntryPoint>

Address Hex dump ASCII (ANSI) - w

00401000 45 6E 74 65 72 20 41 3A Enter A: Enter B:
00401010 3A 00 45 6E 74 65 72 20 6F 70 65 72 61 74 69 6F : Enter operation:
00401020 6E 3A 00 52 65 73 75 6C 74 3A 20 25 64 00 2F 25 n: Result: %d %
00401030 64 00 25 64 00 25 64 00 69 6E 69 6E 69 6E 69 6E d %d %d Infinity
00401040 00 2C 00 00 00 00 00 00 00 00 00 00 00 00 00
00401050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
004010A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
004010B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
004010C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
004010D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
004010E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
004010F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
004011A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Registers (FPU)

EAX 7555342B kernel32.BaseThreadInitThunk
ECX 00000000 calculator.<ModuleEntryPoint>
EDX 00402000
EBX 7EFD0000
ESP 000CFF8C ASCII "=4eu"
EBP 000CFF34
ESI 00000000
EDI 00000000
EIP 00402000 calculator.<ModuleEntryPoint>

C 0 ES 002B 32bit 0 (FFFFFFFF)
P 1 CS 0023 32bit 0 (FFFFFFFF)
A 0 SS 002B 32bit 0 (FFFFFFFF)
Z 1 DS 002B 32bit 0 (FFFFFFFF)
S 0 FS 0053 32bit 7EFD0000 (FFF)
T 0 GS 002B 32bit 0 (FFFFFFFF)
D 0
O 0 LastErr 00000000 ERROR_SUCCESS
EFL 00000246 (NO,NB,E,BS,NS,PE,GE,LE)
ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)
FCW 027F Prec NEAR, 53 Mask 1 1 1 1 1 1
Last cmd 0000:00000000
XMM0 00000000 00000000 00000000 00000000
XMM1 00000000 00000000 00000000 00000000
XMM2 00000000 00000000 00000000 00000000
XMM3 00000000 00000000 00000000 00000000
XMM4 00000000 00000000 00000000 00000000
XMM5 00000000 00000000 00000000 00000000
XMM6 00000000 00000000 00000000 00000000
XMM7 00000000 00000000 00000000 00000000

000CFF8C 7555343D =4eu RETURN to kernel32.BaseThreadInitThunk+12
000CFF90 7EFD0000
000CFF94 000CFF04
000CFF98 770F9812 RETURN to ntdll.770F9812
000CFF9C 7EFD0000
000CFFA0 743759F0 EV7t
000CFFA4 00000000
000CFFA8 00000000
000CFFAC 7EFD0000
000CFFB0 00000000
000CFFB4 76F37C4F 0!ev RETURN from 76F378F0 to 76F37C4F
000CFFB8 00000000
000CFFBC 000CFFA0
000CFFC0 00000000
000CFFC4 FFFFFFFF End of SEH chain
000CFFC8 77134DCD =M!w SE handler
000CFFCC 03550554 T!5
000CFFD0 000CFFD0
000CFFD4 000CFFEC
000CFFD8 770F97E5 b 5xw
000CFFDC 00402000 @ calculator.<ModuleEntryPoint>
000CFFE0 000CFFC4
000CFFE4 7EFD0000
000CFFE8 00000000
000CFFEC 00000000
000CFFF0 00000000
000CFFF4 00402000
000CFFF8 7EFD0000

Module (Mod_76FD) (anonymous)

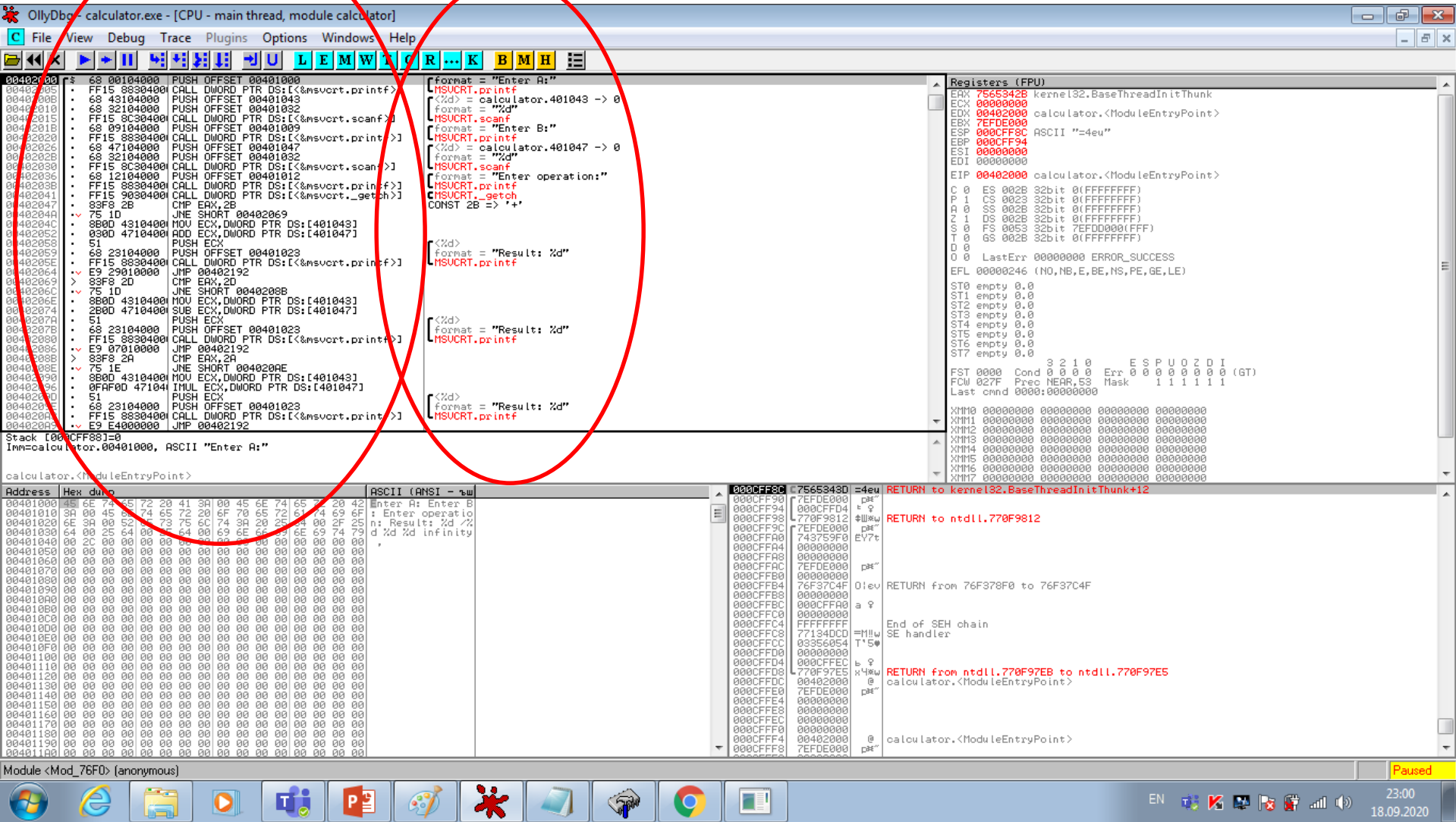
Paused

23:00 18.09.2020

Особенности среды OllyDbg

Листинг: дизассемблированный код

Анализ кода программы: анализ по всем форматам



OllyDbg - calculator.exe - [CPU - main thread, module calculator]

File View Debug Trace Plugins Options Windows Help

Address Hex dump ASCII (ANSI) - w

00401000 68 00104000 PUSH OFFSET 00401000
 00401005 FF15 88304000 CALL DWORD PTR DS:[<msvort.printf>
 00401008 68 43104000 PUSH OFFSET 00401043
 00401010 68 32104000 PUSH OFFSET 00401032
 00401015 FF15 8C304000 CALL DWORD PTR DS:[<msvort.scanf>
 00401018 68 09104000 PUSH OFFSET 00401009
 00401020 FF15 88304000 CALL DWORD PTR DS:[<msvort.printf>
 00401025 68 47104000 PUSH OFFSET 00401047
 00401028 68 32104000 PUSH OFFSET 00401032
 00401035 FF15 8C304000 CALL DWORD PTR DS:[<msvort.scanf>
 00401038 68 12104000 PUSH OFFSET 00401012
 00401040 FF15 88304000 CALL DWORD PTR DS:[<msvort.printf>
 00401045 FF15 90304000 CALL DWORD PTR DS:[<msvort._getch>
 00401048 8BFB 2B CMP EBX, 2B
 0040104A 75 1D JNE SHORT 00402069
 0040104C 8B0D 43104000 MOV ECX, DWORD PTR DS:[401043]
 00401052 8B0D 47104000 MOV ECX, DWORD PTR DS:[401047]
 00401055 51 PUSH ECX
 00401058 68 23104000 PUSH OFFSET 00401023
 0040105A FF15 88304000 CALL DWORD PTR DS:[<msvort.printf>
 0040105D E9 29010000 JMP 00402192
 00401060 8BFB 2D CMP EBX, 2D
 00401062 75 1D JNE SHORT 0040206B
 00401064 8B0D 43104000 MOV ECX, DWORD PTR DS:[401043]
 0040106A 2B0D 47104000 SUB ECX, DWORD PTR DS:[401047]
 0040106D 51 PUSH ECX
 00401070 68 23104000 PUSH OFFSET 00401023
 00401072 FF15 88304000 CALL DWORD PTR DS:[<msvort.printf>
 00401075 E9 07010000 JMP 00402192
 00401078 8BFB 2A CMP EBX, 2A
 0040107A 75 1E JNE SHORT 004020AE
 0040107C 8B0D 43104000 MOV ECX, DWORD PTR DS:[401043]
 00401082 0FAD 47104000 INVL ECX, DWORD PTR DS:[401047]
 00401085 51 PUSH ECX
 00401088 68 23104000 PUSH OFFSET 00401023
 0040108A FF15 88304000 CALL DWORD PTR DS:[<msvort.printf>
 0040108D E9 E4000000 JMP 00402192

Stack [00CFF8B]=0
 Imm=calculator.00401000, ASCII "Enter A:"

calculator.<ModuleEntryPoint>

Registers (FPU)

EAX 755342B kernel32.BaseThreadInitThunk
 ECX 00000000 calculator.<ModuleEntryPoint>
 EDI 00402000
 EBX 76FDE000
 ESP 000CFF8C ASCII "=4eu"
 EBP 000CFFB4
 ESI 00000000
 EDI 00000000
 EIP 00402000 calculator.<ModuleEntryPoint>

C 0 ES 002B 32bit 0(FFFFFFFF)
 P 1 CS 0023 32bit 0(FFFFFFFF)
 A 0 SS 002B 32bit 0(FFFFFFFF)
 Z 1 DS 002B 32bit 0(FFFFFFFF)
 S 0 FS 0053 32bit 7EFD0000(FFF)
 T 0 GS 002B 32bit 0(FFFFFFFF)
 D 0
 O 0 LastErr 00000000 ERROR_SUCCESS
 EFL 00000246 (NO,NB,EB,NS,PE,GE,LE)
 ST0 empty 0.0
 ST1 empty 0.0
 ST2 empty 0.0
 ST3 empty 0.0
 ST4 empty 0.0
 ST5 empty 0.0
 ST6 empty 0.0
 ST7 empty 0.0
 FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)
 FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1
 Last cmd 0000:00000000

XMM0 00000000 00000000 00000000 00000000
 XMM1 00000000 00000000 00000000 00000000
 XMM2 00000000 00000000 00000000 00000000
 XMM3 00000000 00000000 00000000 00000000
 XMM4 00000000 00000000 00000000 00000000
 XMM5 00000000 00000000 00000000 00000000
 XMM6 00000000 00000000 00000000 00000000
 XMM7 00000000 00000000 00000000 00000000

000CFF90 76FDE000 =4eu RETURN to kernel32.BaseThreadInitThunk+12
 000CFF94 000CFFD4
 000CFF98 770F9812
 000CFF9C 76FDE000
 000CFFA0 743759F0 EV7t
 000CFFA4 00000000
 000CFFA8 00000000
 000CFFAC 76FDE000
 000CFFB0 00000000
 000CFFB4 76F37C4F 01ev RETURN from 76F378F0 to 76F37C4F
 000CFFB8 00000000
 000CFFBC 000CFFB0
 000CFFC0 00000000
 000CFFC4 FFFFFFFF
 000CFFC8 77134DCD =MIIw SE handler
 000CFFCC 03356054 T'S
 000CFFD0 00000000
 000CFFD4 000CFFEC
 000CFFD8 770F97E5 b 9
 000CFFDC 00402000 x4w
 000CFFE0 76FDE000
 000CFFE4 00000000
 000CFFE8 00000000
 000CFEFC 00000000
 000CFFF0 00000000
 000CFFF4 00402000
 000CFFF8 76FDE000
 000CFFFC 76FDE000

RETURN to ntdll.770F9812
 RETURN from 76F378F0 to 76F37C4F
 End of SEH chain
 SE handler
 RETURN from ntdll.770F97E5 to ntdll.770F97E5
 calculator.<ModuleEntryPoint>

Module (Mod_76FD) (anonymous)

23:00
 18.09.2020

Настройка анализатора кода

OllyDbg - calculator.exe - [CPU - main thread, module calculator]

File View Debug Trace Plugins Options Windows Help

Registers: EAX 7565342B, ECX 00000000, EDX 00402000, EBX 7EFD0000

Options

Analysis options

Recognition of procedures:

- ☐ Strict
- ☒ Fuzzy

Automatical module analysis:

- ☐ Off
- ☐ Main module
- ☐ Non-system modules
- ☒ All modules

☒ Show predicted register values

☐ Don't predict register contents for system DLLs

☒ Show recognized ARGs and LOCALs in disassembly

☒ Show recognized ARGs and LOCALs in comments

☐ Use symbolic names for ARGs, if known

OK Cancel

Code

- Mnemonics
- Operands
- Dump
- Strings

Debugging

- Debugging data
- Start
- Events
- Exceptions
- Run trace
- Hit trace
- SFX
- Just-in-time

Analysis

- Advanced
- Invalid commands

Search

- CPU
- More CPU
- Directories
- Errors and warnings
- Appearance
- Defaults
- Startup
- Fonts
- Colours
- Code highlighting
- Text-to-speech
- Miscellaneous

Im=0000002D (decimal 45.)
EAX=7565342B (kernel32.BaseThreadInitThunk) (current registers)
Jump from <ModuleEntryPoint>+4A
calculator.<ModuleEntryPoint>+69

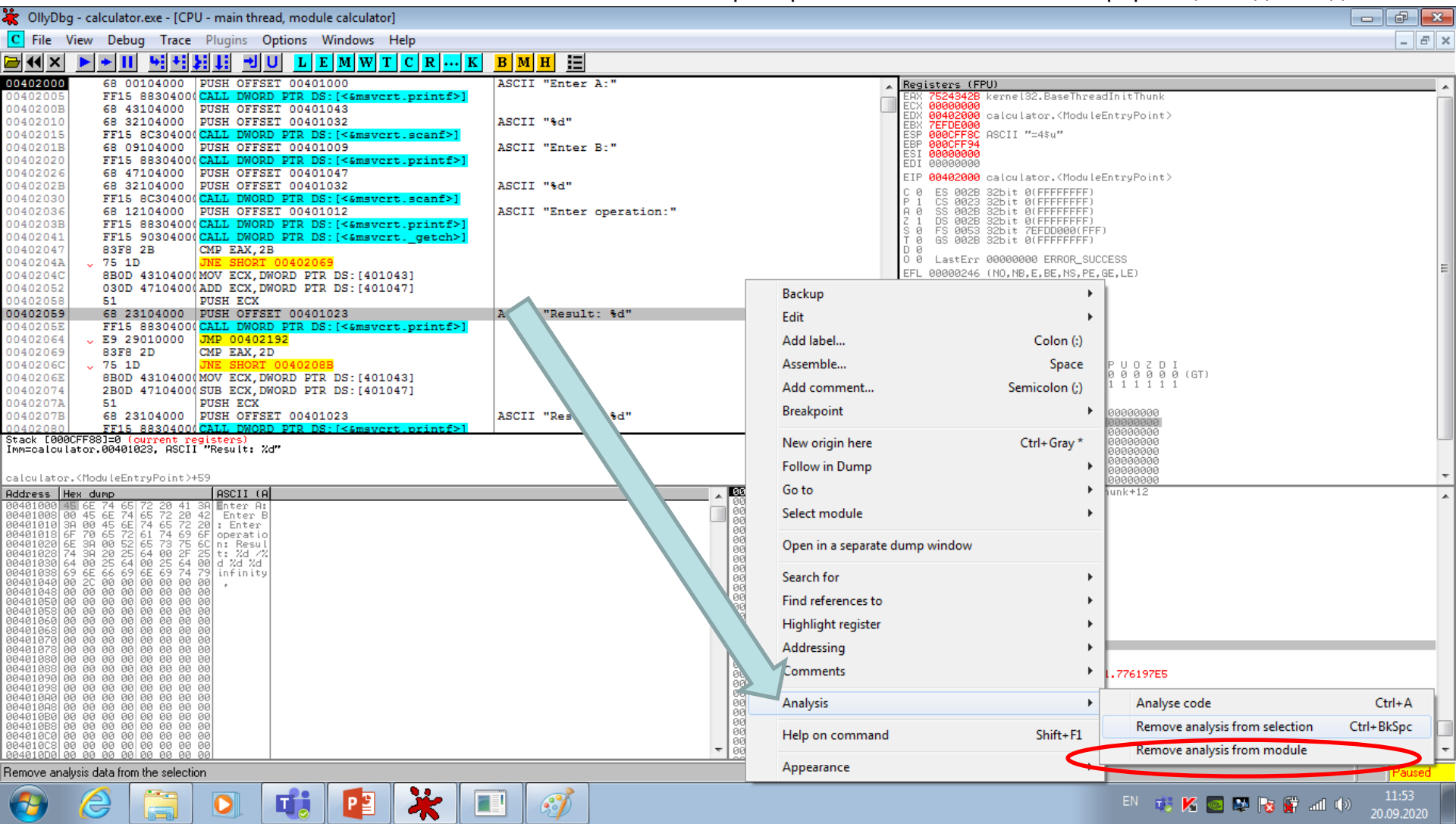
Address	Hex	dump	ASCII (ANSI - 7B)
00401000	45 6E 74 65	72 20 41 3A 00 45 6E 74	Enter A: Enter B
00401010	3A 00 45 6E	74 65 72 20 6F 70 65 72	: Enter operation
00401020	6E 3A 00 52	65 73 75 6C 74 3A 20 25	n: Result: %d / %
00401030	64 00 25 64	00 25 64 00 69 6E 66 69	d %d %d infinity
00401040	00 2C 00 00	00 00 00 00 00 00 00 00	
00401050	00 00 00 00	00 00 00 00 00 00 00 00	
00401060	00 00 00 00	00 00 00 00 00 00 00 00	
00401070	00 00 00 00	00 00 00 00 00 00 00 00	
00401080	00 00 00 00	00 00 00 00 00 00 00 00	
00401090	00 00 00 00	00 00 00 00 00 00 00 00	
004010A0	00 00 00 00	00 00 00 00 00 00 00 00	

Настройка анализатора кода

Полезная опция: Убрать анализ кода программы

«правый клик» на зоне кода - «анализ» - «off»

Например: ошибочный анализ - интерпретация кода как данные.



Полезная опция: подсветка кода

OllyDbg - calculator.exe - [CPU - main thread, module calculator]

File View Debug Trace Plugins Options Windows Help

OllyDbg interface showing assembly code and registers.

```

00402000 68 00104000 PUSH OFFSET 00401000
00402005 FF15 88304000 CALL DWORD PTR DS:[<&msvcrt.printf>]
00402008 68 43104000 PUSH OFFSET 00401043
00402010 68 32104000 PUSH OFFSET 00401032
00402015 FF15 8C304000 CALL DWORD PTR DS:[<&msvcrt scanf>]
00402018 68 09104000 PUSH OFFSET 00401009
00402020 FF15 88304000 CALL DWORD PTR DS:[<&msvcrt.printf>]
00402026 68 47104000 PUSH OFFSET 00401047
00402028 68 32104000 PUSH OFFSET 00401032
00402030 FF15 8C304000 CALL DWORD PTR DS:[<&msvcrt scanf>]
00402036 68 12104000 PUSH OFFSET 00401012
00402038 FF15 88304000 CALL DWORD PTR DS:[<&msvcrt.printf>]
00402041 FF15 90304000 CALL DWORD PTR DS:[<&msvcrt.printf>]
00402047 83F8 2B CMP EAX, 2B
0040204A 75 10 JNE SHORT 0040205C
0040204C 8B00 43104000 MOV ECX, DWORD PTR DS:[43104000]
00402052 0300 47104000 ADD ECX, DWORD PTR DS:[47104000]
00402058 51 PUSH ECX
00402059 68 23104000 PUSH OFFSET 00401023
0040205E FF15 88304000 CALL DWORD PTR DS:[<&msvcrt.printf>]
00402064 E9 29010000 JMP 00402195
00402069 83F8 2D CMP EAX, 2D
0040206C 75 10 JNE SHORT 0040207C
0040206E 8B00 43104000 MOV ECX, DWORD PTR DS:[43104000]
00402074 2B00 47104000 SUB ECX, DWORD PTR DS:[47104000]
0040207A 51 PUSH ECX
0040207B 68 23104000 PUSH OFFSET 00401023
00402080 FF15 88304000 CALL DWORD PTR DS:[<&msvcrt.printf>]
00402086 E9 07010000 JMP 00402195
0040208B 83F8 2A CMP EAX, 2A
0040208E 75 1E JNE SHORT 004020A4
00402090 8B00 43104000 MOV ECX, DWORD PTR DS:[43104000]
00402096 0FAF00 47104000 IMUL ECX, DWORD PTR DS:[47104000]
0040209D 51 PUSH ECX
0040209E 68 23104000 PUSH OFFSET 00401023
004020A3 FF15 88304000 CALL DWORD PTR DS:[<&msvcrt.printf>]
004020A9 E9 E4000000 JMP 00402195
  
```

Backup

Edit

Add label...

Assemble...

Add comment...

Breakpoint

New origin here

Follow in Dump

Go to

Select module

Open in a separate dump window

Search for

Find references to

Highlight register

Addressing

Comments

Analysis

Help on command

Appearance

Colon (:)

Space

Semicolon (;)

Ctrl+Gray *

Shift+F1

Выделить переходы в коде:
«правый клик» на листинге -
«отображение» -
«подсветка» -
«переходы и вызовы»

Always on top

Show bar

Show horizontal scroll

Default columns

Font

Colours

Highlighting

No highlighting

Christmas tree

Jumps and calls

Memory access

Hilite 4

Hilite 5

Hilite 6

Hilite 7

Особенности среды OllyDbg



Три режима отображения: FPU, MMX, 3DNow!

OllyDbg - calculator.exe - [CPU - main thread, module calculator]

File View Debug Trace Plugins Options Windows Help

Registers (FPU)

Область регистров

Address Hex dump ASCII (ANSI) - w

Module (Mod_76FD) (anonymous)

Paused

23:00 18.09.2020

Особенности среды OllyDbg



Режим отображения ESP по умолчанию

OllyDbg - calculator.exe - [CPU - main thread, module calculator]

File View Debug Trace Plugins Options Windows Help

Address Hex dump ASCII (ANSI) - w

00401000 45 6E 74 65 72 20 41 3A Enter A: Enter B:
00401010 3A 00 45 6E 74 65 72 20 6F 70 65 72 61 74 69 6F : Enter operation:
00401020 6E 3A 00 52 65 73 75 6C 74 3A 20 25 64 00 2F 65 n: Result: %d %
00401030 00 2C 00 00 00 00 00 00 00 00 00 00 00 00 00 d %d %d Infinity
00401040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
004010A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
004010B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
004010C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
004010D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
004010E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
004010F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
004011A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stack [000CFF88]=0
Imm=calculator.00401000, ASCII "Enter A:"
calculator.<ModuleEntryPoint>

Registers (FPU)
EAX 755342B kernel32.BaseThreadInitThunk
ECX 00000000 calculator.<ModuleEntryPoint>
EDX 00402000
EBX 7FDE0000
ESP 000CFF8C ASCII "=4eu"
EBP 000CFF84
ESI 00000000
EDI 00000000
EIP 00402000 calculator.<ModuleEntryPoint>
C 0 ES 002B 32bit 0(FFFFFFFF)
P 1 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
Z 1 DS 002B 32bit 0(FFFFFFFF)
S 0 FS 0053 32bit 7EFD0000(FFF)
T 0 GS 002B 32bit 0(FFFFFFFF)
D 0
O 0 LastErr 00000000 ERROR_SUCCESS
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1
Last cmd 0000:00000000
XMM0 00000000 00000000 00000000 00000000
XMM1 00000000 00000000 00000000 00000000
XMM2 00000000 00000000 00000000 00000000
XMM3 00000000 00000000 00000000 00000000
XMM4 00000000 00000000 00000000 00000000
XMM5 00000000 00000000 00000000 00000000
XMM6 00000000 00000000 00000000 00000000
XMM7 00000000 00000000 00000000 00000000

000CFF8C 755342B =4eu RETURN to kernel32.BaseThreadInitThunk+12
000CFF90 7FDE0000 000CFF94
000CFF98 000CFF9C 7FDE0000 000CFF9C
000CFFA0 743759F0 EV7t
000CFFA4 00000000
000CFFA8 00000000
000CFFAC 7FDE0000
000CFFB0 00000000
000CFFB4 76F37C4F 01ev RETURN from 76F378F0 to 76F37C4F
000CFFB8 00000000
000CFFBC 000CFFB0
000CFFC0 00000000
000CFFC4 FFFFFFFF
000CFFC8 77134DCD =MIIw SE handler
000CFFCC 03356054 T'S
000CFFD0 000CFFD0
000CFFD4 000CFFEC b 9
000CFFD8 770F97E5 x4w
000CFFDC 00402000 @ calculator.<ModuleEntryPoint>
000CFFE0 7FDE0000
000CFFE4 00000000
000CFFE8 00000000
000CFFEC 00000000
000CFFF0 00000000
000CFFF4 00000000
000CFFF8 7FDE0000

Область стека

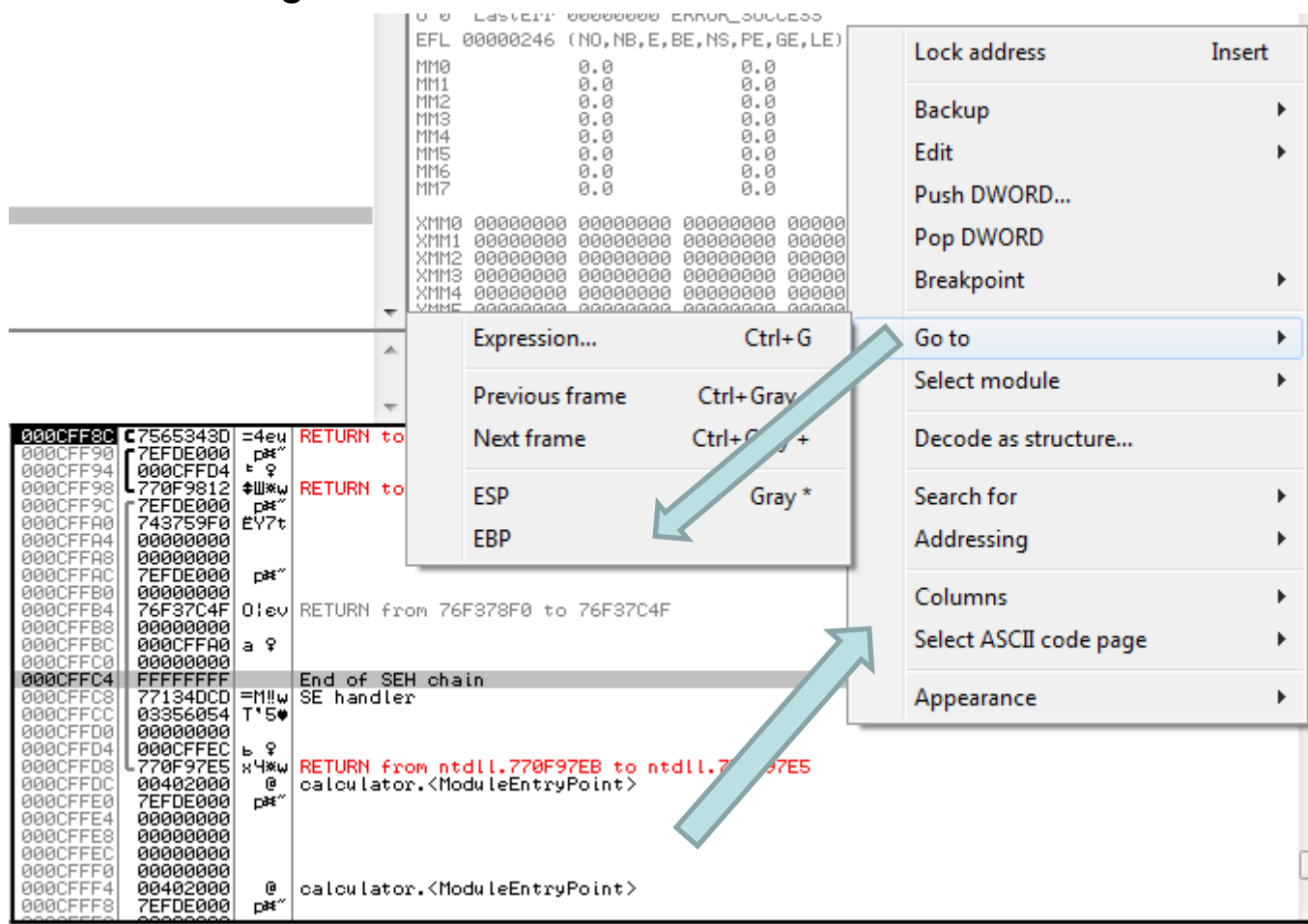
Module (Mod_76FD) (anonymous)

Paused

23:00
18.09.2020

Настройка отображения стека

Полезная опция: Переключить на режим отображения стека EBP
«правый клик» на зоне стека - «go to» - «EBP»



Особенности среды OllyDbg

Режим отображения по умолчанию – 8-байтовый и ASCII

OllyDbg - calculator.exe [CPU - main thread, module calculator]

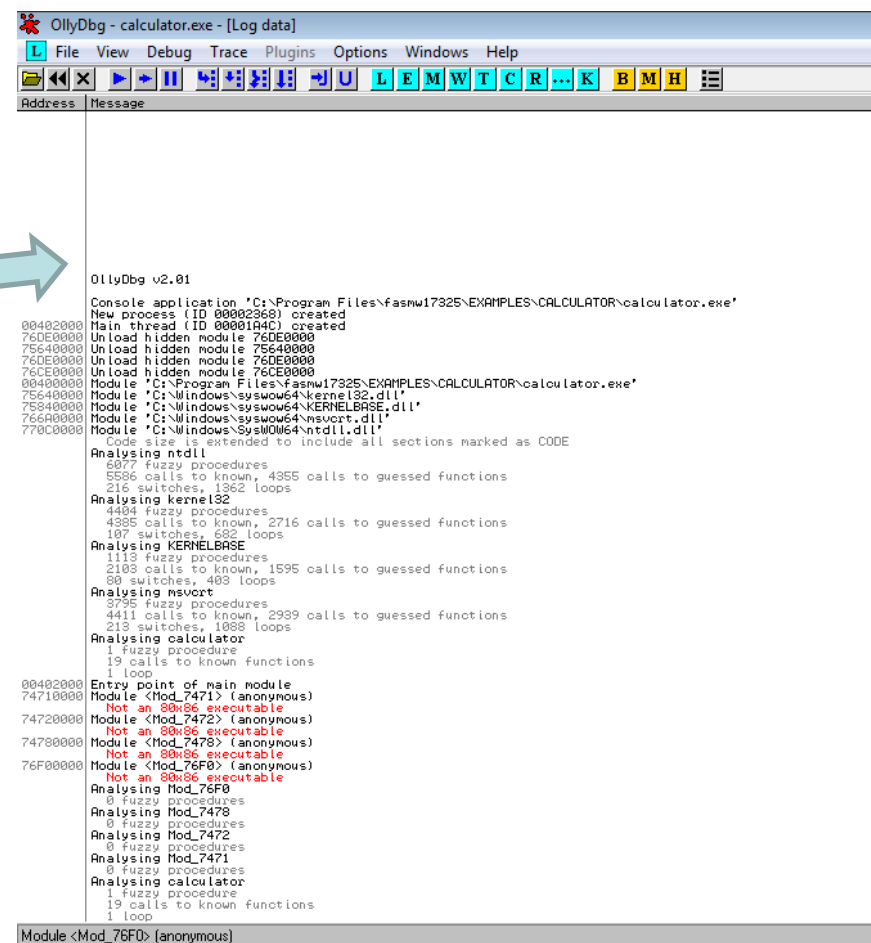
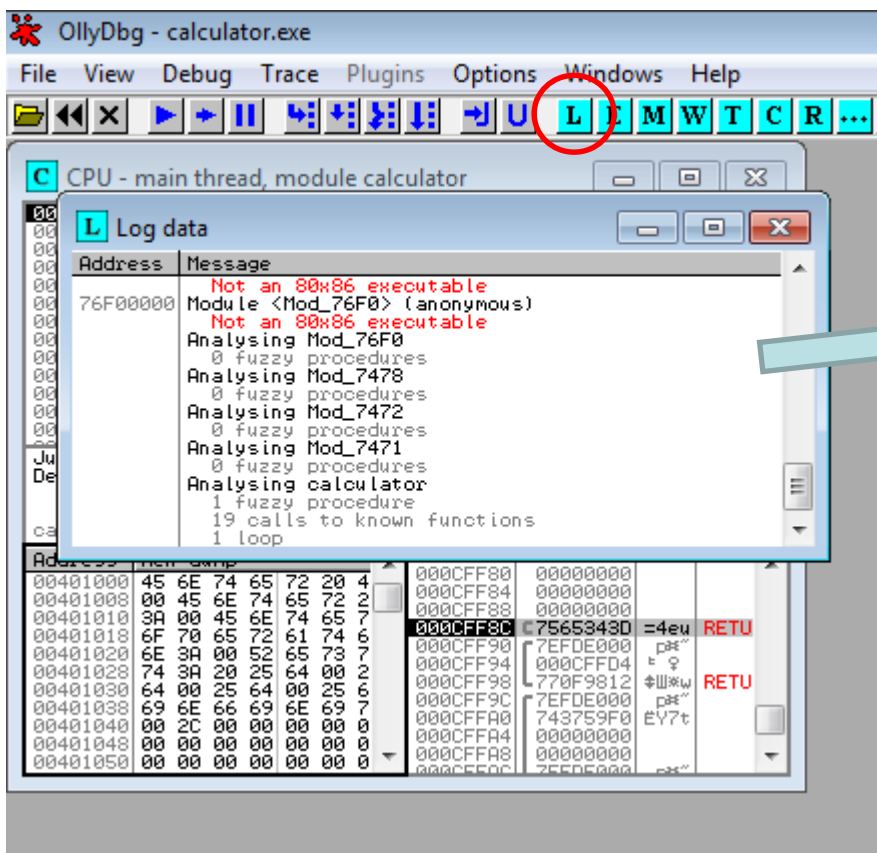
File View Debug Trace Plugins Options Windows Help

Address Hex dump ASCII (ANSI - w)

00401000 45 6E 74 65 72 20 41 3A 00 00 00 00 00 00 00 00 Enter A: Enter B
 00401004 3A 00 45 6E 74 65 72 20 5F 70 65 72 61 74 69 6F : Enter operatio
 00401008 5F 70 65 72 61 74 69 6F 00 00 00 00 00 00 00 00 n: Result: %d %d
 0040100C 64 00 25 64 00 25 64 00 69 6E 66 69 6E 69 74 79 d %d %d infinity
 00401010 00 2C 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00401014 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00401018 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0040101C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00401020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00401024 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00401028 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0040102C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00401030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00401034 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00401038 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0040103C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00401040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00401044 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00401048 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0040104C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00401050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00401054 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00401058 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0040105C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00401060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00401064 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00401068 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0040106C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00401070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00401074 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00401078 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0040107C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00401080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00401084 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00401088 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0040108C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00401090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00401094 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00401098 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0040109C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 004010A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 004010A4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 004010A8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 004010AC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 004010B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 004010B4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 004010B8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 004010BC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 004010C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 004010C4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 004010C8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 004010CC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 004010D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 004010D4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 004010D8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 004010DC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 004010E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 004010E4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 004010E8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 004010EC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 004010F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 004010F4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 004010F8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00401100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

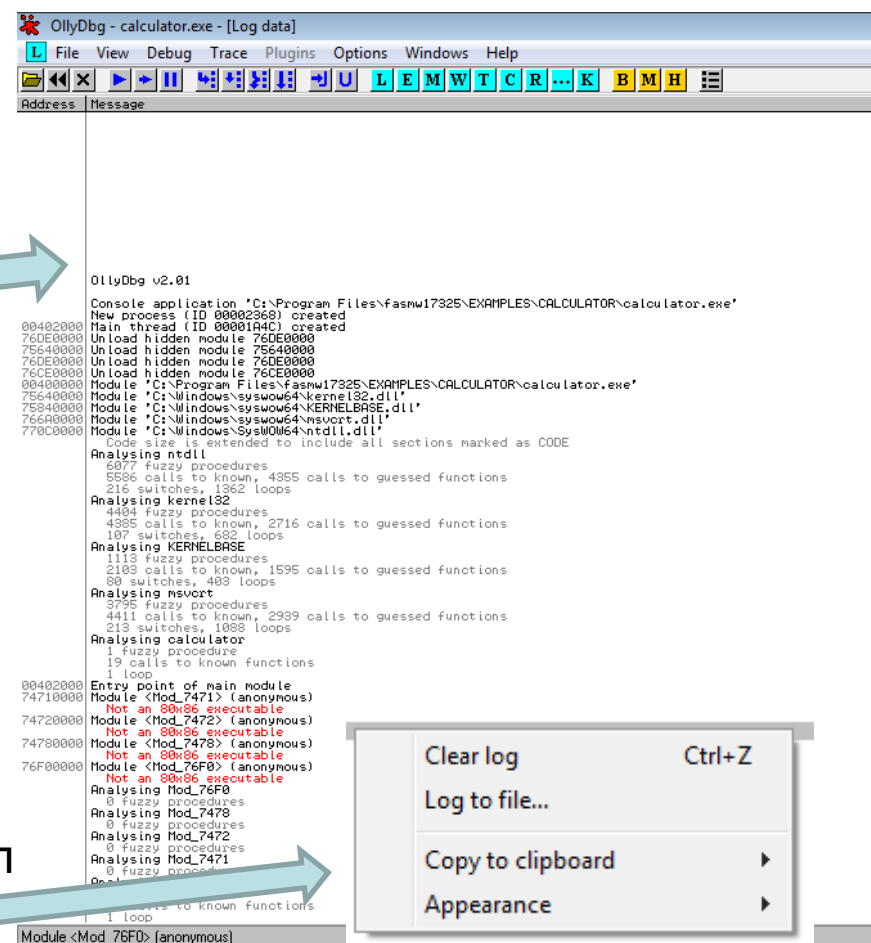
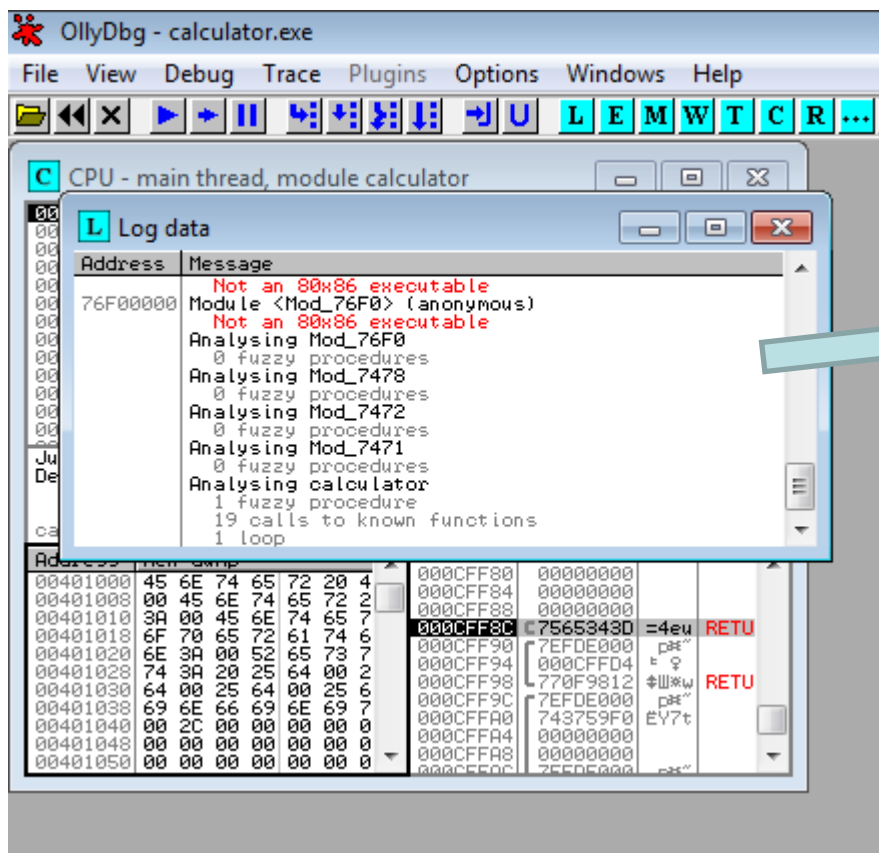
Особенности OllyDbg

Кнопка “L” - Окно Лога: информация о запуске и условных точках останова



Особенности OllyDbg

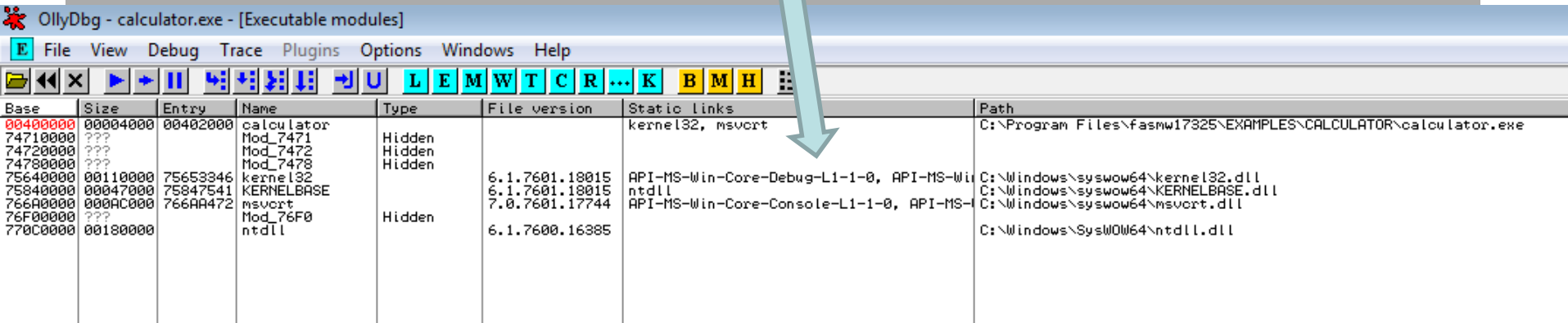
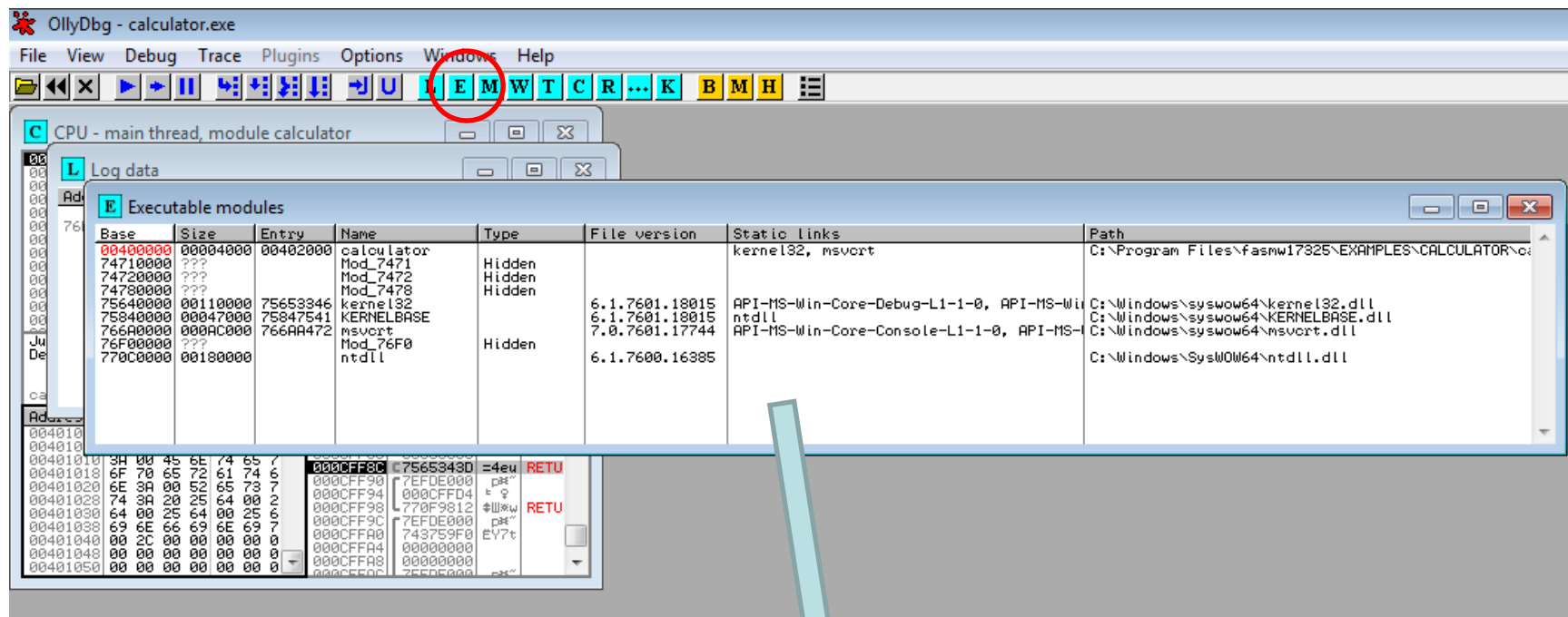
Кнопка “L” - Окно Лога: информация о запуске и условных точках останова



Полезная опция: вывод лога в файл
«правый клик» на логе - «Log to file»

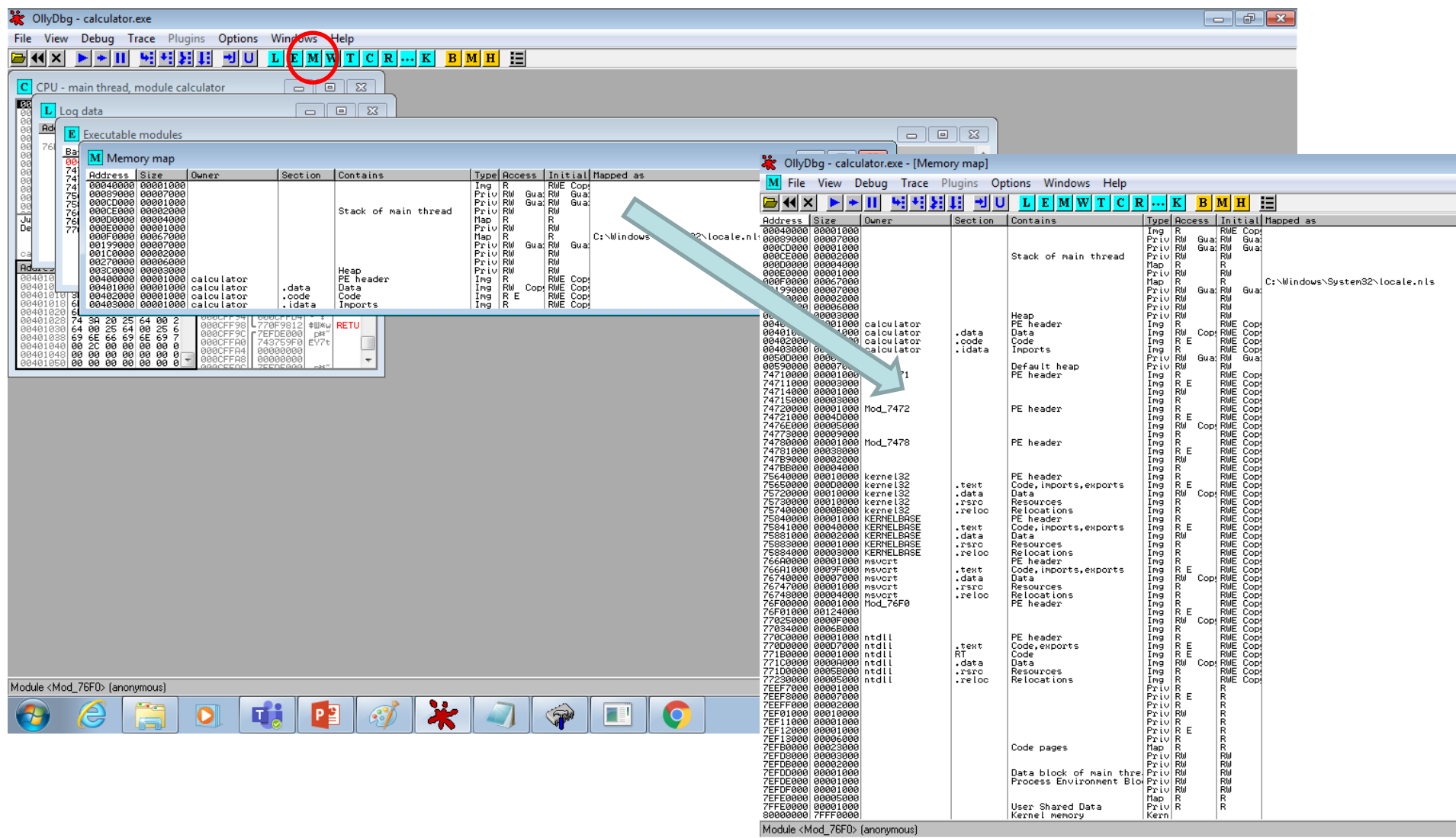
Особенности OllyDbg

Кнопка “Е” – Исполняемые Модули: информация о модулях программы



Особенности OllyDbg

Кнопка “М” – Память: карта памяти приложения



OllyDbg - calculator.exe

File View Debug Trace Plugins Options Windows Help

Log data

Executable modules

Memory map

Address	Size	Owner	Section	Contains	Type	Access	Initial	Mapped as
00040000	00001000				Ing	R	RWE	Cop
00050000	00007000				Priv	RM	Gua	Gua
00060000	00001000				Priv	RM	Gua	Gua
00070000	00002000				Map	R	R	
00080000	00007000				Priv	RM	Gua	Gua
00090000	00001000				Map	R	R	
000A0000	00007000				Priv	RM	Gua	Gua
000B0000	00002000				Priv	RM	Gua	Gua
000C0000	00003000				Priv	RM	Gua	Gua
000D0000	00001000				Ing	R	RWE	Cop
000E0000	00007000				Priv	RM	Gua	Gua
000F0000	00002000				Priv	RM	Gua	Gua
00100000	00002000				Priv	RM	Gua	Gua
00110000	00003000				Priv	RM	Gua	Gua
00120000	00001000				Ing	R	RWE	Cop
00130000	00007000				Priv	RM	Gua	Gua
00140000	00002000				Priv	RM	Gua	Gua
00150000	00003000				Priv	RM	Gua	Gua
00160000	00001000				Ing	R	RWE	Cop
00170000	00007000				Priv	RM	Gua	Gua
00180000	00002000				Priv	RM	Gua	Gua
00190000	00003000				Priv	RM	Gua	Gua
001A0000	00001000				Ing	R	RWE	Cop
001B0000	00007000				Priv	RM	Gua	Gua
001C0000	00002000				Priv	RM	Gua	Gua
001D0000	00003000				Priv	RM	Gua	Gua
001E0000	00001000				Ing	R	RWE	Cop
001F0000	00007000				Priv	RM	Gua	Gua
00200000	00002000				Priv	RM	Gua	Gua
00210000	00003000				Priv	RM	Gua	Gua
00220000	00001000				Ing	R	RWE	Cop
00230000	00007000				Priv	RM	Gua	Gua
00240000	00002000				Priv	RM	Gua	Gua
00250000	00003000				Priv	RM	Gua	Gua
00260000	00001000				Ing	R	RWE	Cop
00270000	00007000				Priv	RM	Gua	Gua
00280000	00002000				Priv	RM	Gua	Gua
00290000	00003000				Priv	RM	Gua	Gua
002A0000	00001000				Ing	R	RWE	Cop
002B0000	00007000				Priv	RM	Gua	Gua
002C0000	00002000				Priv	RM	Gua	Gua
002D0000	00003000				Priv	RM	Gua	Gua
002E0000	00001000				Ing	R	RWE	Cop
002F0000	00007000				Priv	RM	Gua	Gua
00300000	00002000				Priv	RM	Gua	Gua
00310000	00003000				Priv	RM	Gua	Gua
00320000	00001000				Ing	R	RWE	Cop
00330000	00007000				Priv	RM	Gua	Gua
00340000	00002000				Priv	RM	Gua	Gua
00350000	00003000				Priv	RM	Gua	Gua
00360000	00001000				Ing	R	RWE	Cop
00370000	00007000				Priv	RM	Gua	Gua
00380000	00002000				Priv	RM	Gua	Gua
00390000	00003000				Priv	RM	Gua	Gua
003A0000	00001000				Ing	R	RWE	Cop
003B0000	00007000				Priv	RM	Gua	Gua
003C0000	00002000				Priv	RM	Gua	Gua
003D0000	00003000				Priv	RM	Gua	Gua
003E0000	00001000				Ing	R	RWE	Cop
003F0000	00007000				Priv	RM	Gua	Gua
00400000	00002000				Priv	RM	Gua	Gua
00410000	00003000				Priv	RM	Gua	Gua
00420000	00001000				Ing	R	RWE	Cop
00430000	00007000				Priv	RM	Gua	Gua
00440000	00002000				Priv	RM	Gua	Gua
00450000	00003000				Priv	RM	Gua	Gua
00460000	00001000				Ing	R	RWE	Cop
00470000	00007000				Priv	RM	Gua	Gua
00480000	00002000				Priv	RM	Gua	Gua
00490000	00003000				Priv	RM	Gua	Gua
004A0000	00001000				Ing	R	RWE	Cop
004B0000	00007000				Priv	RM	Gua	Gua
004C0000	00002000				Priv	RM	Gua	Gua
004D0000	00003000				Priv	RM	Gua	Gua
004E0000	00001000				Ing	R	RWE	Cop
004F0000	00007000				Priv	RM	Gua	Gua
00500000	00002000				Priv	RM	Gua	Gua
00510000	00003000				Priv	RM	Gua	Gua
00520000	00001000				Ing	R	RWE	Cop
00530000	00007000				Priv	RM	Gua	Gua
00540000	00002000				Priv	RM	Gua	Gua
00550000	00003000				Priv	RM	Gua	Gua
00560000	00001000				Ing	R	RWE	Cop
00570000	00007000				Priv	RM	Gua	Gua
00580000	00002000				Priv	RM	Gua	Gua
00590000	00003000				Priv	RM	Gua	Gua
005A0000	00001000				Ing	R	RWE	Cop
005B0000	00007000				Priv	RM	Gua	Gua
005C0000	00002000				Priv	RM	Gua	Gua
005D0000	00003000				Priv	RM	Gua	Gua
005E0000	00001000				Ing	R	RWE	Cop
005F0000	00007000				Priv	RM	Gua	Gua
00600000	00002000				Priv	RM	Gua	Gua
00610000	00003000				Priv	RM	Gua	Gua
00620000	00001000				Ing	R	RWE	Cop
00630000	00007000				Priv	RM	Gua	Gua
00640000	00002000				Priv	RM	Gua	Gua
00650000	00003000				Priv	RM	Gua	Gua
00660000	00001000				Ing	R	RWE	Cop
00670000	00007000				Priv	RM	Gua	Gua
00680000	00002000				Priv	RM	Gua	Gua
00690000	00003000				Priv	RM	Gua	Gua
006A0000	00001000				Ing	R	RWE	Cop
006B0000	00007000				Priv	RM	Gua	Gua
006C0000	00002000				Priv	RM	Gua	Gua
006D0000	00003000				Priv	RM	Gua	Gua
006E0000	00001000				Ing	R	RWE	Cop
006F0000	00007000				Priv	RM	Gua	Gua
00700000	00002000				Priv	RM	Gua	Gua
00710000	00003000				Priv	RM	Gua	Gua
00720000	00001000				Ing	R	RWE	Cop
00730000	00007000				Priv	RM	Gua	Gua
00740000	00002000				Priv	RM	Gua	Gua
00750000	00003000				Priv	RM	Gua	Gua
00760000	00001000				Ing	R	RWE	Cop
00770000	00007000				Priv	RM	Gua	Gua
00780000	00002000				Priv	RM	Gua	Gua
00790000	00003000				Priv	RM	Gua	Gua
007A0000	00001000				Ing	R	RWE	Cop
007B0000	00007000				Priv	RM	Gua	Gua
007C0000	00002000				Priv	RM	Gua	Gua
007D0000	00003000				Priv	RM	Gua	Gua
007E0000	00001000				Ing	R	RWE	Cop
007F0000	00007000				Priv	RM	Gua	Gua
00800000	00002000				Priv	RM	Gua	Gua
00810000	00003000				Priv	RM	Gua	Gua
00820000	00001000				Ing	R	RWE	Cop
00830000	00007000				Priv	RM	Gua	Gua
00840000	00002000				Priv	RM	Gua	Gua
00850000	00003000				Priv	RM	Gua	Gua
00860000	00001000				Ing	R	RWE	Cop
00870000	00007000				Priv	RM	Gua	Gua
00880000	00002000				Priv	RM	Gua	Gua
00890000	00003000				Priv	RM	Gua	Gua
008A0000	00001000				Ing	R	RWE	Cop
008B0000	00007000				Priv	RM	Gua	Gua
008C0000	00002000				Priv	RM	Gua	Gua
008D0000	00003000				Priv	RM	Gua	Gua
008E0000	00001000				Ing	R	RWE	Cop
008F0000	00007000				Priv	RM	Gua	Gua
00900000	00002000				Priv	RM	Gua	Gua
00910000	00003000				Priv	RM	Gua	Gua
00920000	00001000				Ing	R	RWE	Cop
00930000	00007000				Priv	RM	Gua	Gua
00940000	00002000				Priv	RM	Gua	Gua
00950000	00003000				Priv	RM	Gua	Gua
00960000	00001000				Ing	R	RWE	Cop
00970000	00007000				Priv	RM	Gua	Gua
00980000	00002000				Priv	RM	Gua	Gua
00990000	00003000				Priv	RM	Gua	Gua
009A0000	00001000				Ing	R	RWE	Cop
009B0000	00007000				Priv	RM	Gua	Gua
009C0000	00002000				Priv	RM	Gua	Gua
009D0000	00003000							

Особенности OllyDbg

Кнопка “М” – Память: карта памяти приложения

The screenshot displays the OllyDbg interface with the 'Memory map' window open. The memory map shows various memory segments including the stack of the main thread, heap, and various modules like calculator.exe and kernel32.dll. A search dialog is open in the foreground, and a right-click context menu is visible over the memory map table, with the 'Search...' option highlighted. Arrows indicate the workflow: clicking 'Search...' in the menu opens the search dialog, and the search is performed on the memory map data.

Enter search pattern

ASCII (1251)

UTF-8

UNICODE

HEX +00

INS

☐ Ignore case

<< Prev Next >>

Search Cancel

Right-click context menu options:

- Update (Ctrl+R)
- Create backup
- Dump in CPU
- Dump (Enter)
- Search... (Ctrl+B)
- Show free memory (Space)
- Set break-on-access (F2)
- Set access
- Copy to clipboard
- Sort by
- Appearance

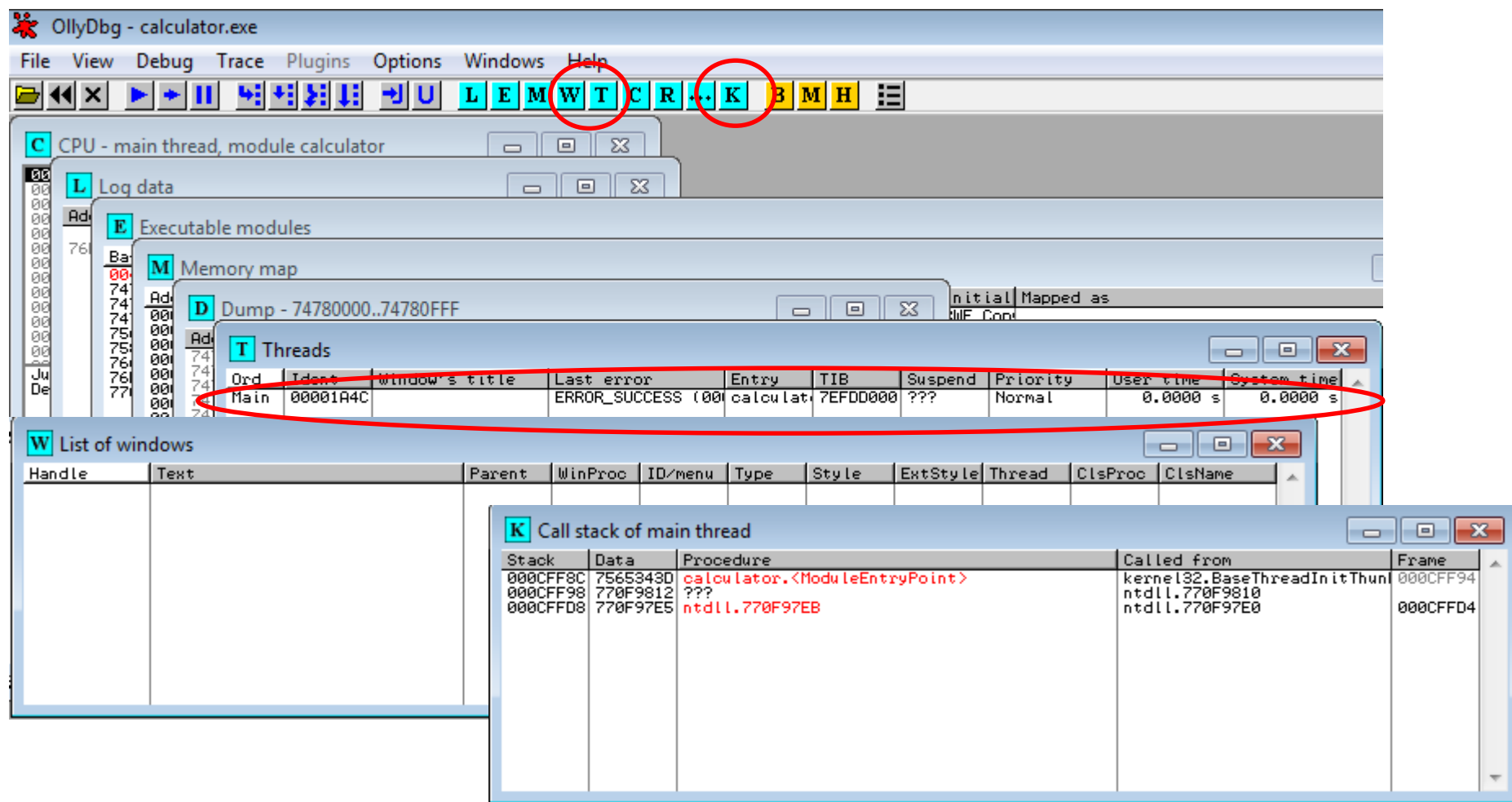
Полезная опция: Поиск в карте памяти
«правый клик» на карте памяти - «Search» - шаблон поиска

Особенности OllyDbg

Кнопка “T” – треды: список «нитей» в потоковой программе;

Кнопка “W” – список окон в программе;

Кнопка “K” – список (стек) вызовов основного потока вычислений



OllyDbg - calculator.exe

File View Debug Trace Plugins Options Windows Help

Buttons: L E M W T C R K B M H

Windows:

- CPU - main thread, module calculator
- Log data
- Executable modules
- Memory map
- Dump - 74780000..74780FFF
- Threads
- List of windows
- Call stack of main thread

Threads window details:

Ord	Ident	Window's title	Last error	Entry	TIB	Suspend	Priority	User time	System time
0	00001A4C		ERROR_SUCCESS (00000000)	calculator.7EFD0000	7EFD0000	???	Normal	0.0000 s	0.0000 s

Call stack of main thread window details:

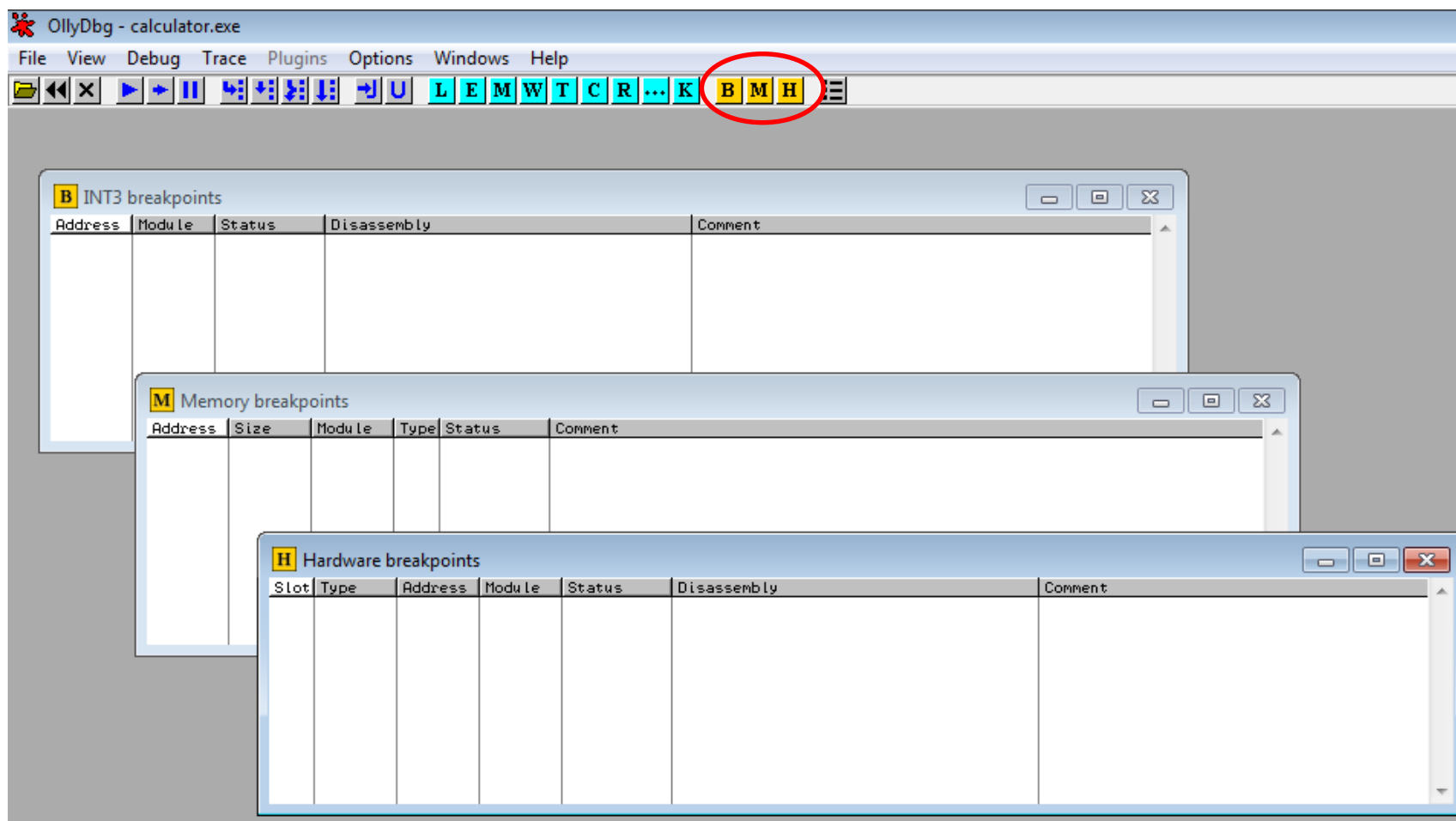
Stack	Data	Procedure	Called from	Frame
000CFF8C	7565343D	calculator.<ModuleEntryPoint>	kernel32.BaseThreadInitThunk	000CFF94
000CFF98	770F9812	???	ntdll.770F9810	
000CFFD8	770F97E5	ntdll.770F97E5	ntdll.770F97E0	000CFFD4

Особенности OllyDbg

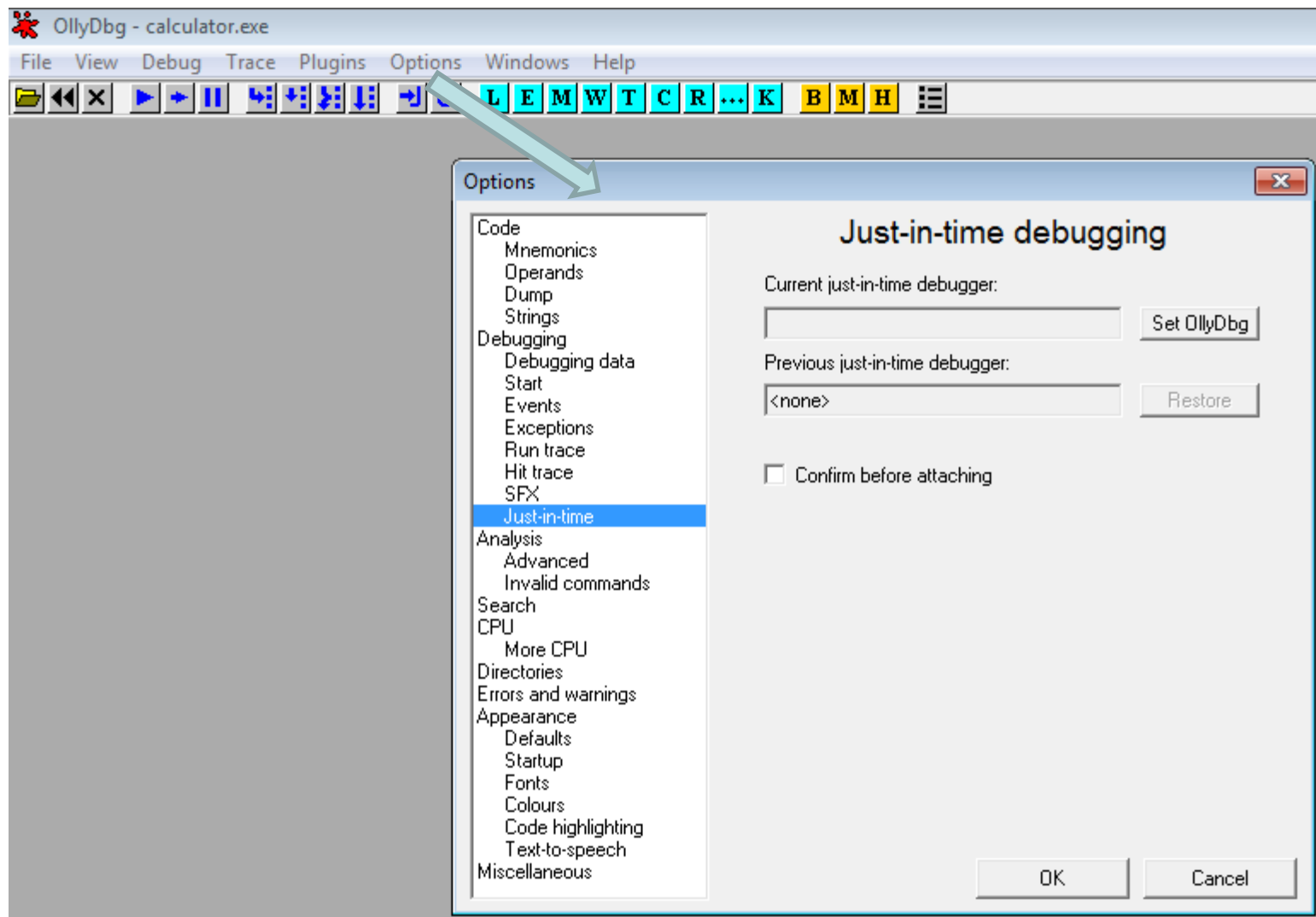
Кнопка “В” – внутренние очки останова (контрольные точки) в программе;

Кнопка “М” – список точек останова в памяти;

Кнопка “Н” – список аппаратных точек останова.



OlllyDbg как JIT-отладчик



Особенности OllyDbg

Наиболее полезные клавиши:

F7 – выполняет одну строку кода. Если мы находимся на строке “call”, то переходим внутрь выделенного участка.

По **F8** мы «ходим» по программе, не заходя внутрь участка кода, если попадаем на call.

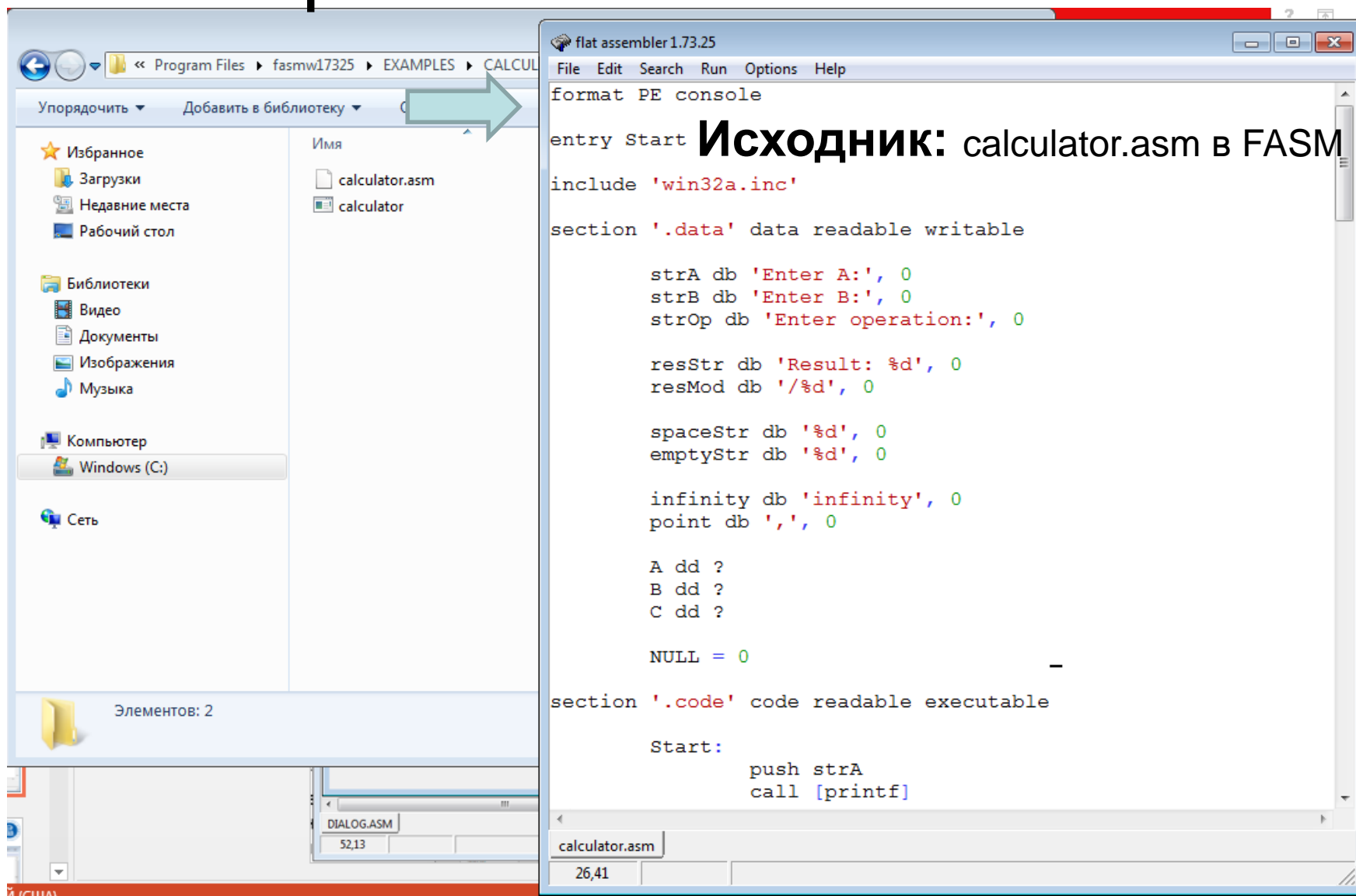
Это два вида ручной трассировки.

F2 – устанавливает «точку останова» на отмеченной линии.

F9 – запускает программу, которая будет выполняться пока не встретит «точку останова» или не прекратит работу.

F12 - чтобы прекратить выполнение программы.

Пример: отладка консольного приложения calculator



Пример: отладка консольного приложения calculator

OllyDbg - calculator.exe - [CPU - main thread, module calculator]

File View Debug Trace Plugins Options Windows Help

Address Hex dump Disassembly Comment

00402000 68 00104000 PUSH OFFSET 00401000
 00402005 FF15 88304000 CALL DWORD PTR DS:[&msvort.printf]>
 00402008 68 43104000 PUSH OFFSET 00401043
 0040200B 68 32104000 PUSH OFFSET 00401032
 0040200E FF15 8C304000 CALL DWORD PTR DS:[&msvort.scanf]>
 00402011 68 09104000 PUSH OFFSET 00401009
 00402014 FF15 88304000 CALL DWORD PTR DS:[&msvort.printf]>
 00402017 68 47104000 PUSH OFFSET 00401047
 0040201A 68 32104000 PUSH OFFSET 00401032
 0040201D FF15 8C304000 CALL DWORD PTR DS:[&msvort.scanf]>
 00402020 68 12104000 PUSH OFFSET 00401012
 00402023 FF15 88304000 CALL DWORD PTR DS:[&msvort.printf]>
 00402026 68 32104000 PUSH OFFSET 00401032
 00402029 FF15 8C304000 CALL DWORD PTR DS:[&msvort.scanf]>
 0040202C 68 12104000 PUSH OFFSET 00401012
 0040202F FF15 88304000 CALL DWORD PTR DS:[&msvort.printf]>
 00402032 68 32104000 PUSH OFFSET 00401032
 00402035 FF15 8C304000 CALL DWORD PTR DS:[&msvort.scanf]>
 00402038 68 12104000 PUSH OFFSET 00401012
 0040203B FF15 88304000 CALL DWORD PTR DS:[&msvort.printf]>
 0040203E 68 32104000 PUSH OFFSET 00401032
 00402041 FF15 8C304000 CALL DWORD PTR DS:[&msvort.scanf]>
 00402044 75 1D JNE SHORT 00402069
 00402047 8B0D 43104000 MOV ECX, DWORD PTR DS:[401043]
 0040204A 8B0D 47104000 MOV ECX, DWORD PTR DS:[401047]
 0040204D 51 PUSH ECX
 0040204E FF15 88304000 CALL DWORD PTR DS:[&msvort.printf]>
 00402051 68 23104000 PUSH OFFSET 00401023
 00402054 FF15 88304000 CALL DWORD PTR DS:[&msvort.printf]>
 00402057 E9 29010000 JMP 00402192
 0040205A 83F8 2D CMP EAX, 2D
 0040205D 75 1D JNE SHORT 004020B8
 00402060 8B0D 43104000 MOV ECX, DWORD PTR DS:[401043]
 00402063 8B0D 47104000 MOV ECX, DWORD PTR DS:[401047]
 00402066 51 PUSH ECX
 00402067 68 23104000 PUSH OFFSET 00401023
 0040206A FF15 88304000 CALL DWORD PTR DS:[&msvort.printf]>
 0040206D E9 07010000 JMP 00402192
 00402070 83F8 2A CMP EAX, 2A
 00402073 75 1E JNE SHORT 0040209E
 00402076 8B0D 43104000 MOV ECX, DWORD PTR DS:[401043]
 00402079 8B0D 47104000 MOV ECX, DWORD PTR DS:[401047]
 0040207C 51 PUSH ECX
 0040207D 68 23104000 PUSH OFFSET 00401023
 00402080 FF15 88304000 CALL DWORD PTR DS:[&msvort.printf]>
 00402083 E9 44000000 JMP 00402192

Stack [000CFF88]=0
 Imm=calculator.00401000, ASCII "Enter A:"

calculator.<ModuleEntryPoint>

Address Hex dump Disassembly Comment

000CFF88 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFF90 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFF94 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFF98 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFF9C 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFA0 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFA4 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFA8 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFAC 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFB0 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFB4 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFB8 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFBC 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFC0 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFC4 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFC8 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFCC 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFD0 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFD4 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFD8 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFDC 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFE0 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFE4 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFE8 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFEC 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFF0 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFF4 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFF8 7FDE0000 7FDE0000 7FDE0000 7FDE0000

Registers (FPU)

EAX 755342B kernel32.BaseThreadInitThunk
 ECX 00000000 calculator.<ModuleEntryPoint>
 EDI 00000000
 ESI 00000000
 EBP 000CFF8C ASCII "=4eu"
 ESP 000CFF8C
 EIP 00402000 calculator.<ModuleEntryPoint>

C 0 ES 002B 32bit 0(FFFFFFFF)
 P 1 CS 0023 32bit 0(FFFFFFFF)
 A 0 SS 002B 32bit 0(FFFFFFFF)
 Z 1 DS 002B 32bit 0(FFFFFFFF)
 S 0 FS 0053 32bit 7EFD0000(FFF)
 T 0 GS 002B 32bit 0(FFFFFFFF)

D 0
 0 0 LastErr 00000000 ERROR_SUCCESS
 EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty 0.0
 ST1 empty 0.0
 ST2 empty 0.0
 ST3 empty 0.0
 ST4 empty 0.0
 ST5 empty 0.0
 ST6 empty 0.0
 ST7 empty 0.0

FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)
 FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1
 Last cmd 0000:00000000

XMM0 00000000 00000000 00000000 00000000
 XMM1 00000000 00000000 00000000 00000000
 XMM2 00000000 00000000 00000000 00000000
 XMM3 00000000 00000000 00000000 00000000
 XMM4 00000000 00000000 00000000 00000000
 XMM5 00000000 00000000 00000000 00000000
 XMM6 00000000 00000000 00000000 00000000
 XMM7 00000000 00000000 00000000 00000000

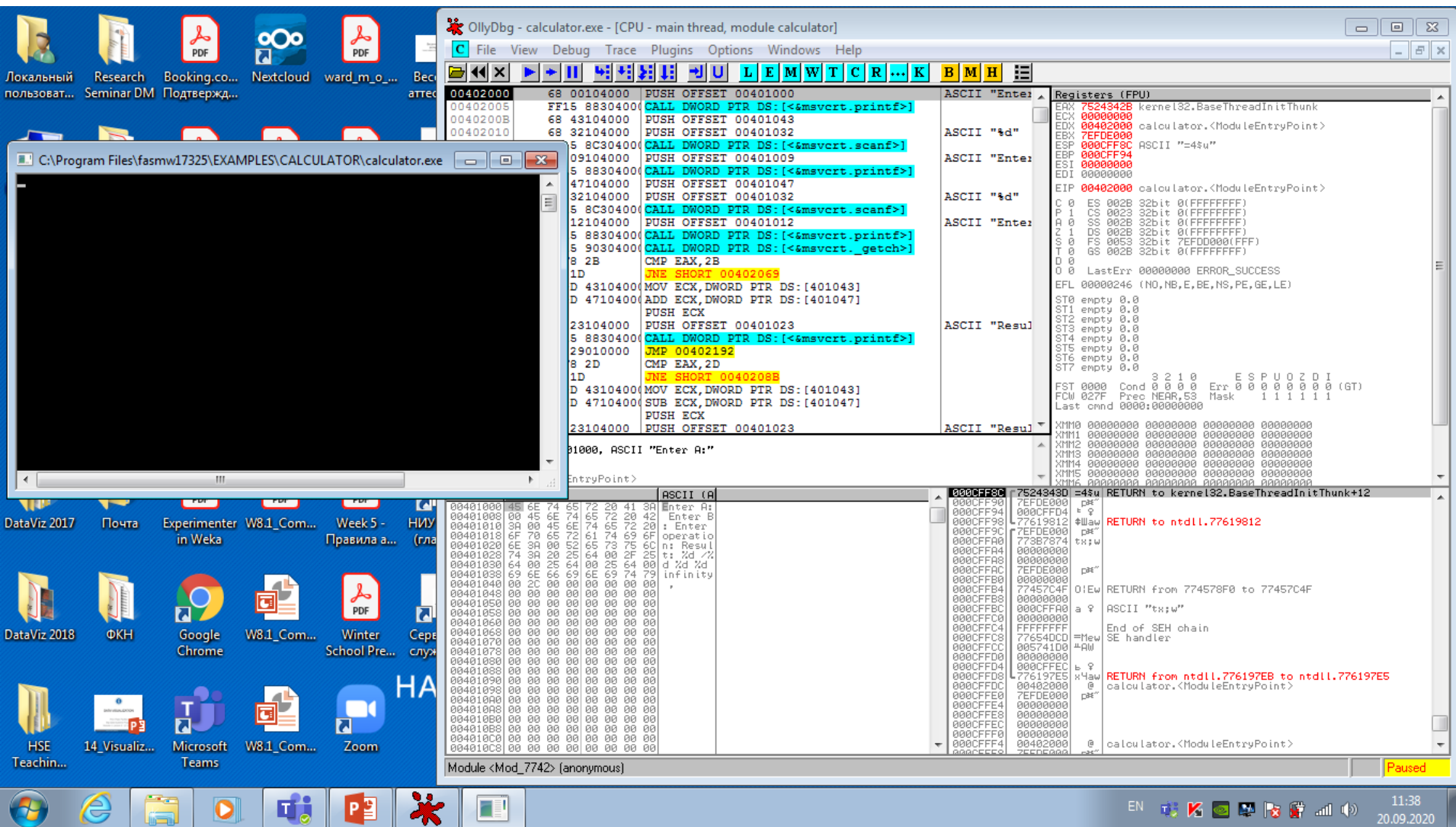
000CFF8C 755343D0 =4eu RETURN to kernel32.BaseThreadInitThunk+12
 000CFF90 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFF94 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFF98 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFF9C 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFA0 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFA4 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFA8 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFAC 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFB0 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFB4 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFB8 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFBC 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFC0 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFC4 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFC8 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFCC 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFD0 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFD4 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFD8 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFDC 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFE0 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFE4 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFE8 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFEC 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFF0 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFF4 7FDE0000 7FDE0000 7FDE0000 7FDE0000
 000CFFF8 7FDE0000 7FDE0000 7FDE0000 7FDE0000

Module (Mod_76FD) (anonymous)

Paused

23:00
 18.09.2020

Пример: отладка консольного приложения calculator



Задание для самостоятельной работы на 2-й неделе

- Установить отладчик (OllyDbg) на рабочий компьютер.
 - Примечание. По согласованию с преподавателем выполнение самостоятельной работы допускается с использование иных современных архитектур ВС, ОС, а также компиляторов с языка программирования Ассемблер.
- В соответствии с вариантом задания **разработать программу, осуществляющую обработку одномерных массивов.**
 - При создании программы использовать подпрограммы для отдельных подзадач (ввода, вывода массивов, обработки данных).
- **Выложить программу и скриншоты** на Git в качестве отчета о выполненной работе, предоставляемого преподавателю.
- **Сообщить о выполненной работе.** Срок выполнения задания: **2 недели.**
 - Примечание. Для второго задания внутри ранее сформированного проекта создать отдельный каталог с названием **task02**. Размещение данных внутри этого каталога произвольное.

Особенности задания для самостоятельной работы

- **Разработать программу**, использующую динамическое выделение памяти под массив, которая
 1. вводит одномерный массив $A[N]$,
 2. формирует из элементов массива A новый массив B по правилам, указанным в таблице, и
 3. выводит его.
- **Разбить решение задачи на функции** следующим образом:
 1. *Ввод и вывод массивов оформить как процедуры.*
 2. *Выполнение задания по варианту оформить как процедуру.*
 3. *Указанные процедуры могут использовать данные напрямую (имитация процедур без параметров).*

Варианты заданий для самостоятельной работы

Вариант	Массив B из...
1	положительных элементов A
2	элементов A , значение которых не совпадает с первым и последним элементами A
3	сумм соседних элементов A ($\{A[0] + A[1], A[1] + A[2], \dots\}$)
4	элементов $B[i] = \begin{cases} 1, & \text{если } A[i] > 0; \\ -1, & \text{если } A[i] < 0; \\ 0, & \text{если } A[i] = 0. \end{cases}$
5	элементов A , значение которых не совпадает с введённым числом x
6	элементов A , значение которых кратно введённому числу x
7	индексов положительных элементов A
8	элементов $B[i] = \begin{cases} A[i] + 5, & \text{если } A[i] > 5; \\ A[i] - 5, & \text{если } A[i] < -5; \\ 0, & \text{иначе.} \end{cases}$
9	нечётных элементов A
10	элементов A в обратном порядке

Варианты заданий для самостоятельной работы

Вариант	Массив B из...
11	за исключением первого положительного
12	за исключением последнего отрицательного
13	за исключением элементов, значения которых совпадают с минимальным элементом A
14	с заменой всех отрицательных элементов значением максимального
15	с заменой всех нулевых элементов значением минимального
16	значения которых больше среднего арифметического
17	расположенных после последнего положительного элемента
18	с уменьшением всех элементов до первого положительного на 5
19	с заменой нулевых элементов, предшествующих первому отрицательному, единицей
20	с перестановкой местами минимального и первого элемента

КОНТАКТЫ

преподавателя

- Проф. Панфилов Петр Борисович
- Персональная страница на сайте университета:
<https://www.hse.ru/org/persons/14608534>
- e-mail для сообщений по семинару курса ABC:
ppanfilov210@gmail.com
- e-mail для прочих вопросов:
ppanfilov@hse.ru