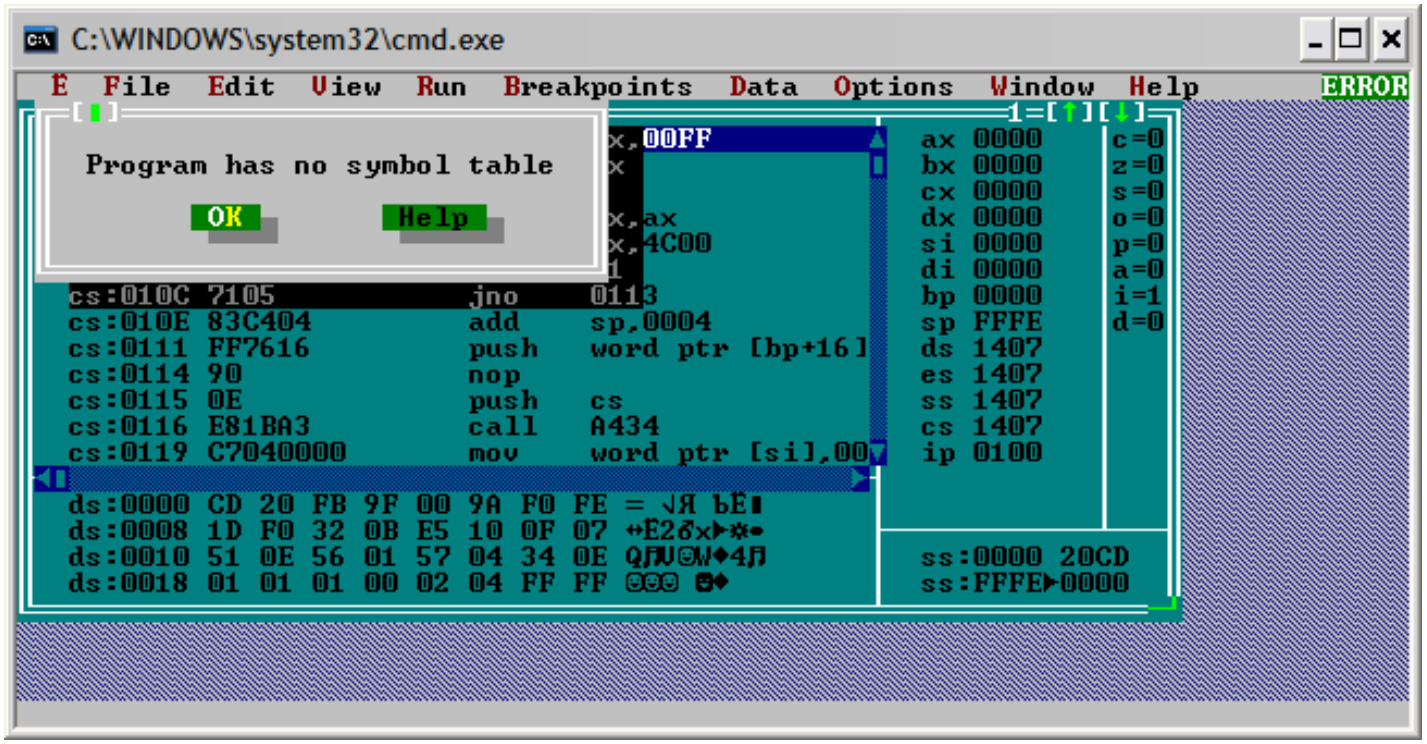
Учебный курс. Часть 3. Turbo Debugger

Автор: xrnd | Рубрика: Учебный курс | 12-03-2010 | Распечатать запись

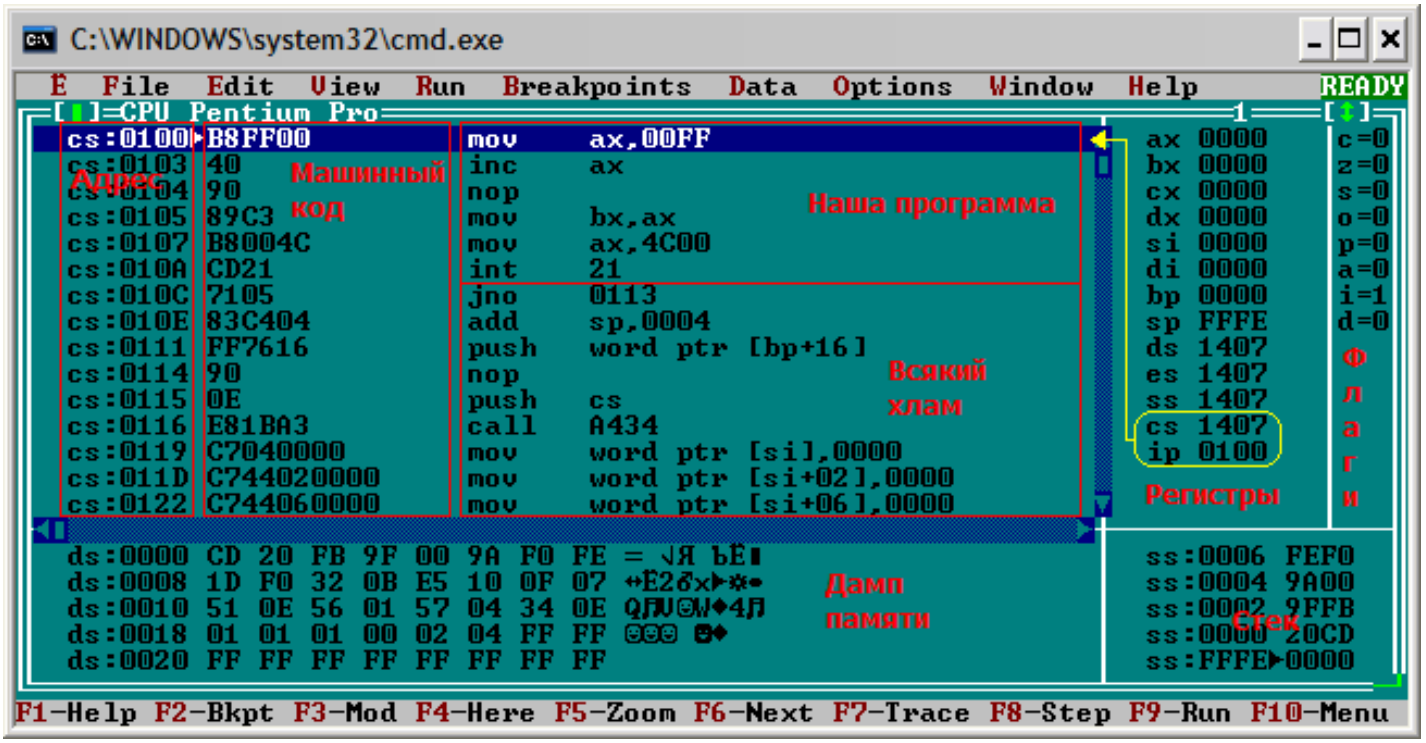
Прежде всего необходимо запустить отладчик. Для этого удобно использовать bat-файл. Создайте в каталоге программы текстовый файл, назовите его, например, «debug.bat». В него надо записать всего одну строку:

```
1 C:\TD\td.exe <файл_программы>.com
```

После запуска этого bat-файла вы увидите примерно такое окно:



Сообщение означает, что в исполняемом файле нет специальных данных для отладки. Но нам эти данные и не нужны, потому что программа простая и понятная. Нажимаем OK. Turbo Debugger отображает окно CPU, в котором можно увидеть, как выполняется программа.

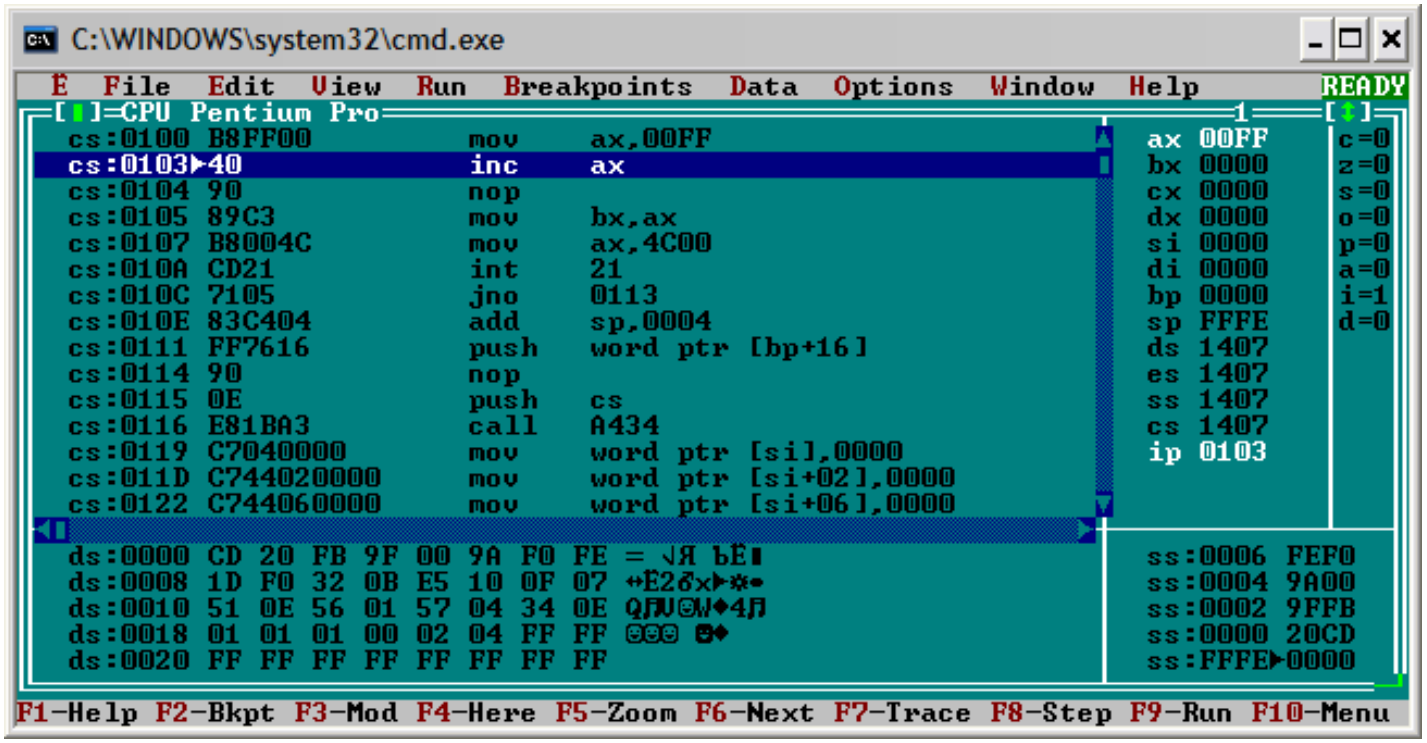


В большой области мы видим код нашей программы. Самый левый столбец — адреса, правее отображаются байты машинного кода, а ещё правее — символическое обозначение команд. Программа размещается в памяти, начиная с адреса 0100h в сегменте кода. В нашей программе всего 6 машинных команд, а за ними в памяти находится случайный мусор (точные значения неизвестны).

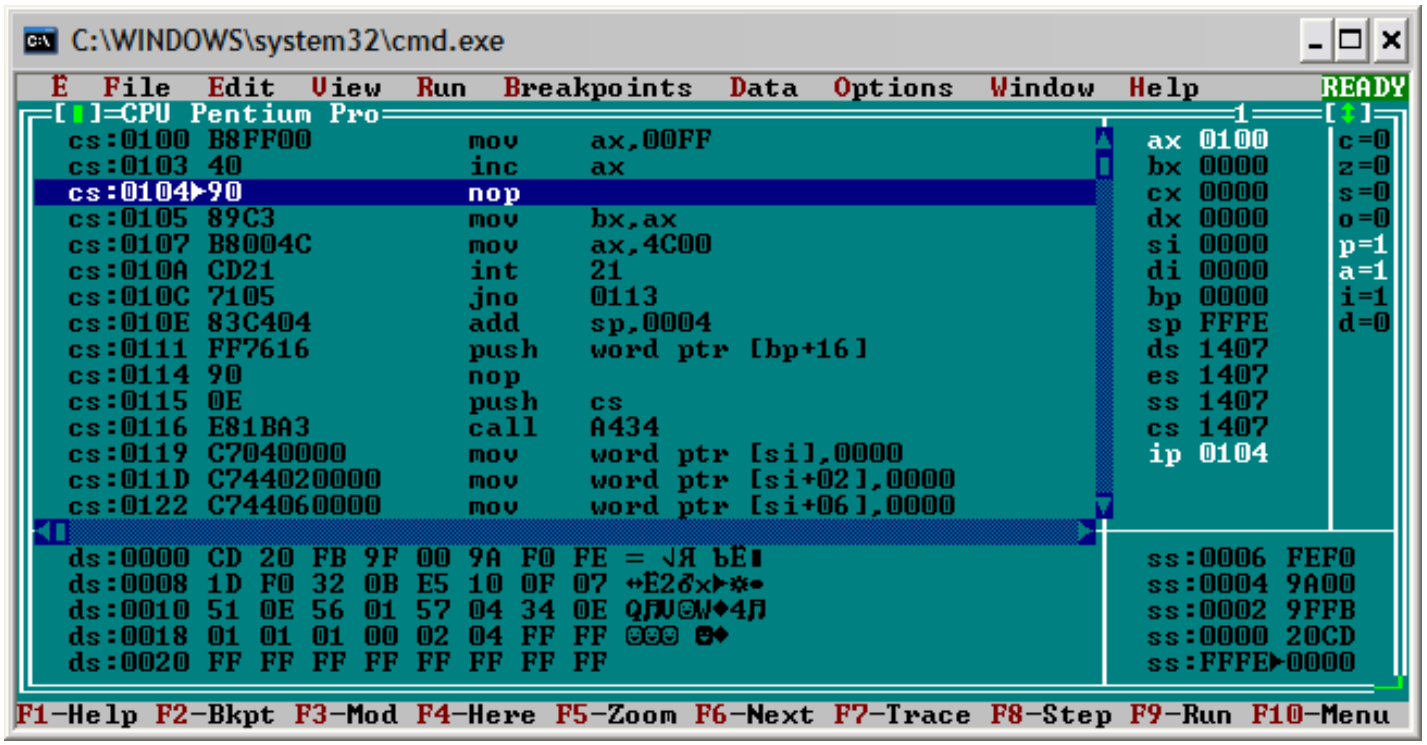
Обратите внимание, что отладчик показывает адреса и значения в шестнадцатеричном виде. Если вы ещё плохо разбираетесь в системах счисления, советую прочитать сразу 7-ю часть учебного курса «Системы счисления».

В правой части окна CPU отображаются регистры процессора и флаги. В нижней части можно увидеть дамп области памяти и стек. Стек — это специальная структура данных, с которой работают некоторые команды процессора.

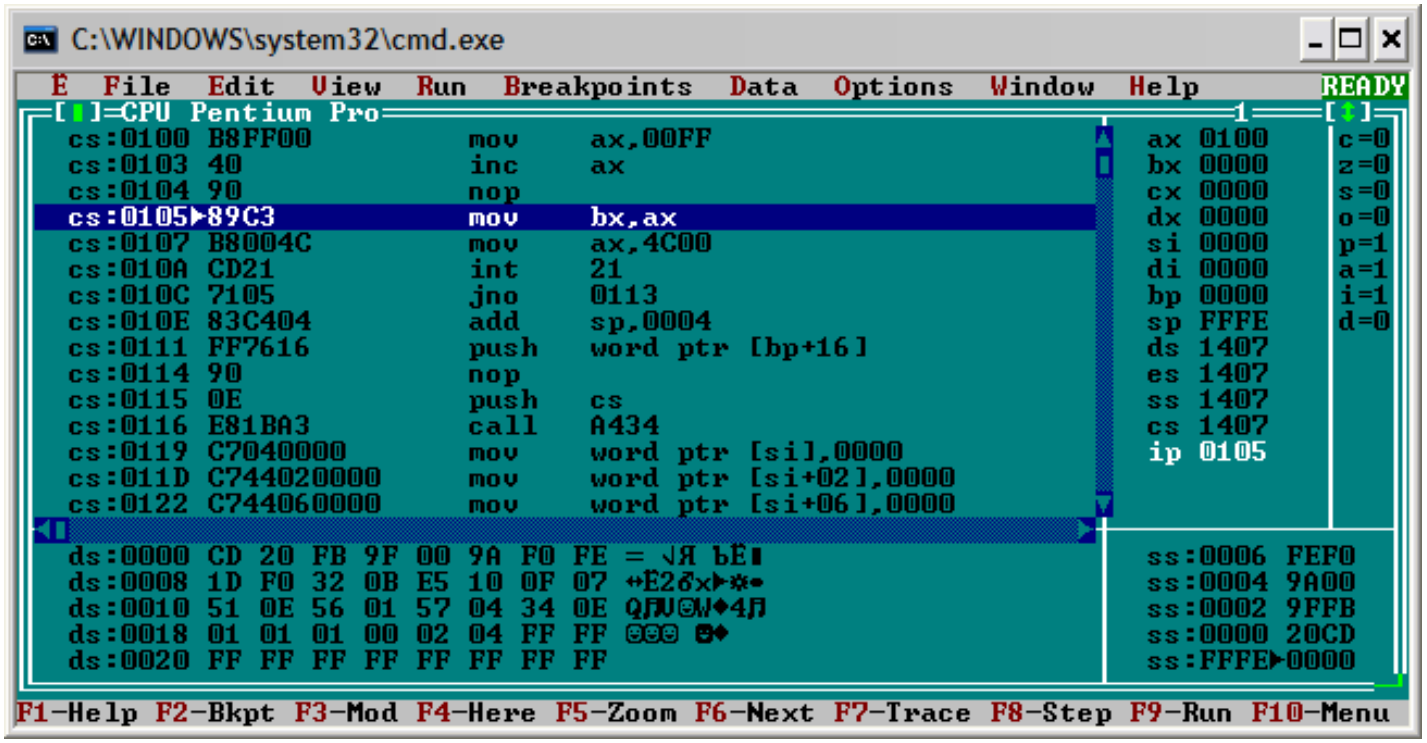
Адрес текущей машинной команды определяется регистрами CS и IP, эта команда показана выделенной строкой и стрелкой. Теперь нажмите F8, чтобы выполнить первую команду.



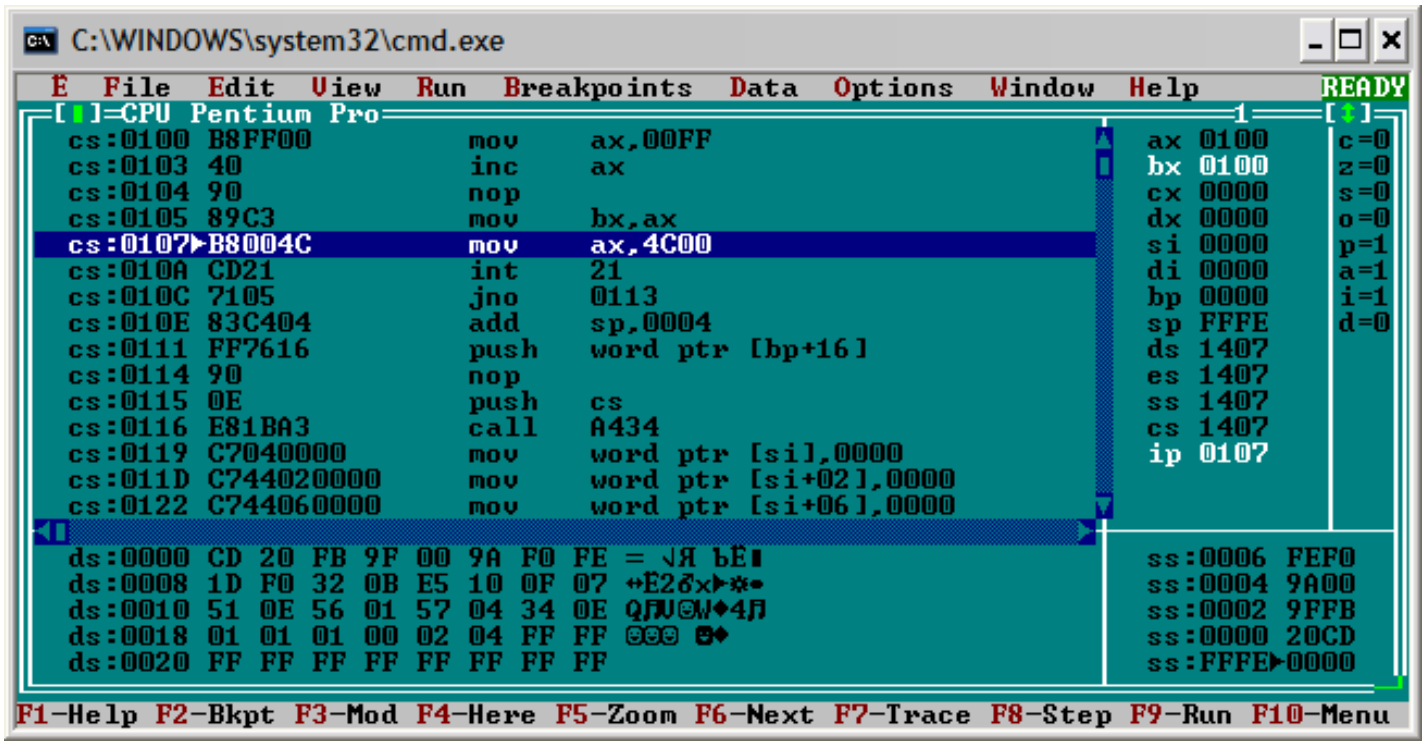
Теперь стрелка указывает на вторую команду. Изменившиеся регистры выделены белым цветом. Регистр AX теперь содержит значение 00FFh (то есть 255, чего мы и хотели от команды «mov ax,255»). Также изменилось значение регистра IP — оно увеличилось на размер выполненной машинной команды, а именно на 3. Теперь CS:IP указывает на следующую команду. Снова нажимаем F8.



Значение регистра AX увеличилось на 1 и стало равным 0100h (256). Значение IP тоже увеличилось на 1, потому что длина команды «inc ax» — 1 байт. Процессор выполняет программу последовательно, одну команду за другой. Ещё раз нажимаем F8.



Команда NOP ничего не делает. Меняется только значение IP — снова увеличивается на 1. Снова F8.



Значение BX становится равным AX. После ещё двух нажатий F8 программа завершается. Закрыть отладчик можно с помощью меню *File->Quit*.

Следующая часть »

Комментарии:

bebe
27-03-2010 09:45

Спасибо, многие моменты стали понятны 🙂
Но хотелось, чтобы отладчик использовался и в других примерах.
Благодарю за Ваш труд!

[Ответить]

xrnd
27-03-2010 20:56

В 9-й части будет ещё немного про отладчик 🙂

[Ответить]

Linked
20-03-2013 09:21

потрясный сайт!Самый лучший из всех что я видел по асме.. СПАСИБО АВТОРУ!!!

[Ответить]

mc-black
08-05-2010 20:58

Классно, все понятно предельно и без длинны нудных отступлений от темы. Пиши обязательно ещё! Конечно, кому-то неясно может быть про систему счисления, почему 255 — это FF, но тут правда не стоит отвлекаться — можно отослать ссылкой на приложение — маленькую свою или можно даже чужую статью о системах счисления.

[Ответить]

xrnd
09-05-2010 16:57

О системах счисления подробно рассказывается в 7-й части.

[Ответить]

levinter
13-06-2010 10:15

спасибо огромное !!!) давно ищу вот такую понятную статью по работе с отладчиком

[Ответить]

xrnd
14-06-2010 14:30

Пожалуйста 🙂 Правда эта статься не претендует на полноту, это только основы.

[Ответить]

Petersvi
26-06-2010 17:36

На недавно приобретеной Win 7 64 дебургер не запустился (файл утановлен не на C: , но пробл видимо в 64-й винде — не хочется заморачиваться с вирт машиной — как быть?)

[Ответить]

xrnd
26-06-2010 23:57

К сожалению, помочь не могу, с Win 7 я не работал 😕

[Ответить]

levinter
27-06-2010 23:20

нет у меня тоже стоит семерка и все пашет просто ты может чето не правельно делаешь

[Ответить]

Petersvi
28-06-2010 00:49

levinter, собсно дело не в семерке, а в 64-й битности помноженной на семерку… Проще говоря не идут проги и всё…

[Ответить]

Гена Борщ
19-10-2010 17:30

На втором скрине «всякий хлам», это то, что осталось в памяти от выполнения прошлых программ?

[Ответить]

xrnd
19-10-2010 23:54

Если программа запускается в чистом DOSe то да, именно так.

Под Windows Turbo Debugger будет работать в эмуляторе реального режима, поэтому трудно точно сказать, что там остаётся в памяти.

Тут главное понимать, что если память специально не инициализируется, то в ней могут быть любые значения.

[Ответить]

IgorKing
24-10-2010 10:24

Что означает такое сообшение: «NMI Interrupt» ? Я всё рвусь поработать с графикой EGA не попёрло, проверяю другой режим (вроде как SVGA) и не пойму он включен или нет. Слышал, что DOS программы вообще вроде как не могут использовать гафику это правда?

Вот собственно код:

```
use16
org 100h
mov ah,4fh
mov al,02h
mov bx,115h
int 02h
mov ax,4c00h
int 21h
```

[Ответить]

xrnd
24-10-2010 18:31

Сообщение о каком-то прерывании 🙂
Графику в DOS использовать можно. Я не очень знаком с этой темой,
но могу посоветовать книгу:
http://www.xserver.ru/computer/computer/video/2/

[Ответить]

Philin
07-12-2010 13:59

Привет… начинаю изучать программирование с ноля… и хочу попросить помочь…
создал текстовый файл как было описано, в папке с программой TD, но он не запускается как в иллюстрации… может не так и не там…? у меня XP…

[Ответить]

xrnd
07-12-2010 14:08

Текстовый файл надо скомпилировать.
Возможно, проблема в том, что имя файла должно быть не длиннее 8 символов (+3 символа расширение). Turbo Debugger — досовская программа, она не понимает длинные имена файлов.

[Ответить]

Philin
07-12-2010 14:57

ну вроде что то похожее получилось, вот только при запуске не вышло окошко с *в исполняемом файле нет специальных данных для отладки* и еще, данные о программке котор. на вашем рис. и в моём отладчике должны быть идентичны…? спасибо…!

[Ответить]

xrnd
07-12-2010 15:26

Код программы должен быть таким же. «Всякий хлам» и значения в регистрах могут быть другими.

Если не вышло окошко, скорее всего, отладчик запустился пустой, без программы.
Проверь, правильно ли имя файла написано. Либо можно через меню TD открыть программу.

[Ответить]

Philin
07-12-2010 16:14

имя файла — причина… спс…
по всем пунктам правильно, вот единственное: последняя строчка *int 21*
int 21 _____ вместо 21* в TD отображает 15* … ?
извини если отвлекаю…

[Ответить]

xrnd
07-12-2010 16:20

Должно быть int 21h (шестнадцатеричное число).
Если без буквы h, то оно считается десятичным.
Turbo Debugger показывает в шестнадцатеричном виде 15(h) = 21.

[Ответить]

Philin
07-12-2010 16:24

точно… спасибо…!

[Ответить]

Amator
31-12-2010 01:24

при вводе строки мне пишет Program not found, подскажите пожалуйста, что я делаю не правильно

[Ответить]

Amator
02-01-2011 17:27

подскажите пожалуйста, у меня в Turbo Debugger в место — C:\WINDOS\sistem32\cdm.exe
пишет — C:\DOKUME-1\B523-1\C316-1\D4422-1\td\td.exe
Может быть это влияет на работу TD

[Ответить]

xrnd
02-01-2011 18:28

Скорее всего, td.exe просто не находится. Дело в том, что Turbo Debugger — старая досовская программа. В досе имена файлов и папок не больше 8 символов и должны содержать только английские буквы, цифры и некоторые символы.

Если в Windows папка называется «C:\Documents and settings», то для дос-программ она сокращается так: «C:\DOCUME~1» — 6 первых символов, затем тильда и номер файла, если их несколько с похожими именами. Папки с кириллическими названиями вообще преобразуются в абракадабру.

Чтобы не было проблем, положи TD.EXE в папку C:\TD или другую.
Программа на ассемблере тоже должна иметь не более 8 символов в имени файла.

[Ответить]

Amator
03-01-2011 22:40

спасибо за подсказку, я переложил папку TD отдельно на диск C, теперь падпись немого сократилась C:\D4422-1\td\td.exe
Будет ли програма работать коректно?

[Ответить]

xrnd
10-01-2011 22:49

Странно, что такой путь. Вероятно, папка TD оказалась не в самом корне диске.

Вообще, корректно работать должно из любой папки. Просто труднее указывать такой корявый путь к файлу 🙂

[Ответить]

exbbrat
17-01-2011 16:40

что может быть если не запускается TD у мя XP пробовал многое

[Ответить]

xrnd
18-01-2011 17:52

Не знаю, в чём дело. Тут кто-то уже писал, что на 64-битной XP он не хочет работать.
У меня 32-битный процессор и винда тоже 32-битная 🙁

[Ответить]

Ne_Ice
02-07-2011 12:55

Под 64-битной Windows td отлично запускается через DOSBox)

[Ответить]

RT >> Falcon
26-01-2011 20:07

Короче всяким способом попробовал открыть, или хотя б найти турбо дебаггер в своём виндоусе но так и не удалось. Скачал себе турбо дебаггер, оно безусловно затормозило несколько секунд а потом выдаёт СИНИЙ ЭКРАН СМЕРТИ !!! (В общем, такое постоянно случается когда я пытаюсь развернуть любую 16-битную досовскую программу на полный экран с помощью Alt+Enter). Перезапустил комп, запустил дебаггер через DOSBox-07.4 … слава богу всё работает))
Спасибо за понятную статью))

[Ответить]

xrnd
26-01-2011 22:54

Может дело в винде или каком-то драйвере 🙂
Тогда действительно проще в эмуляторе запускать.
Все программы в примерах очень простые, должны быстро работать.

[Ответить]

4reddie
21-04-2011 00:58

Может я тупой канеш)))
Но что писать в эти в строке, которую вы указали написать в debug.bat???

[Ответить]

magi
13-06-2012 10:29

Да не мучайтесь с батником, если не понимаете его. Просто запустите td.exe и через меню откройте скомпилированный файл. File->Open->Browse (только учтите, что там по умолчангию стоит маска *.exe, а вам нужна маска *.com). Для простоты навигации проще всего скопировать бинарный файл в папку с td.

[Ответить]

4reddie
21-04-2011 00:59

C:\TD\td.exe .com

вместо этого: файл_программы что следует написать?

[Ответить]

xrnd
21-04-2011 01:05

Имя файла. Например, если файл с текстом программы называется proga.asm, то скомпилированная программа будет называться proga.com

В bat-файл надо написать:
C:\TD\td.exe proga.com

[Ответить]

Ne_Ice
02-07-2011 12:58

Если дебагер и программа в разных каталогах то надо прописывать полный путь.

[Ответить]

Nelexis
29-09-2011 21:48

Статьи супер =) моя благодарность

[Ответить]

Денис
08-11-2011 17:23

А как узнать с какой строки начинается всякий хлам когда отлаживаешь другую программу?

И мне бы хотелось по подробнее узнать об отладчике Что такое дамп, флаги, регистры, и стек и что с ними нужно делать? адрес это номера строк так я понял?

И почему при отладке программы у меня выскакивает окно No programm loaded?

И почему бы не запускать программу через меню File\open? так я думаю гораздо удобнее. Зачем создавать какой то бетник и через него запускать?

[Ответить]

T86
09-11-2011 07:23

http://www.wasm.ru Введение в крэкинг с нуля, используя OllyDbg

[Ответить]

Алексей
19-11-2011 18:53

спасибо все понятно

[Ответить]

Ammator
09-01-2012 05:16

я создал текстовый файл, скопировал в него C:\TD\td.exe .com и присвоил ему имя debug.bat , но он почему-то не запускается

[Ответить]

vv20
11-01-2012 21:15

Очень хороший учебник. Все просто и понятно. Спасибо Вам за Ваш труд. Очень надеюсь что Вы не бросите это дело в дальнейшем. А теперь по делу… Может я
что-то не так понял, но зачем все эти сложности с bat-файлами. Не проще бы было просто перетащить «proga.com» на ярлык «TD» или напрямую на сам «TD». Так быстрее и удобнее и bat-файлов ни каких не надо . Объясните пожалуйста.

[Ответить]

Тимур
03-04-2012 12:14

Добрый день. И еще вопрос, хотя перед тем как задать вопрос я бы просил не очень смеяться над моими вопросами, я совсем на начальном этапе нахожусь.
Но ладно, вопрос, отладчик он нужен только для того чтобы пронаблюдать как работает программа? и если мы напишем программу для какой-либо микросхемы, то его можно вшивать не используя отладчик, я правильно мыслю?
Спасибо.

[Ответить]

metalizator
01-05-2012 10:56

Для тех, кто работает в win7 и т.д.

1. Убедитесь, что Вы запустили FASMW.exe, т.е. fasmwindows.

2.Создайте, как описано, proga.com

3.Скопируйте proga.com в каталог C:\Td

4.Запустите td.exe выберите File>open>C:\Td\proga.com — в окне C:\Td\td.exe будет текст proga.com
5. Если нужно в окне C:\windows\system32 запустите debug.bat(C:\Td\td.exe proga.com) из C:\fasm

[Ответить]

metalizator
01-05-2012 12:46

Изменение к предыдущему:
5.5. Если нужно в окне C:\windows\system32
запустите debug.bat(C:\Td\td.exe) можно из C:\debug.bat, выберите File>open>C:\Td\proga.com
Автору спасибо за уроки!

[Ответить]

magi
13-06-2012 10:09

Для своего времени td был хорошим отладчиком. Но реально его сейчас не получиться приминить кроме как в учебных целях. Поэтому лучше сразу использовать современный вроде OllyDbg.

[Ответить]

asmL
15-06-2012 22:16

интересно, данным дебаггером любые проги можно отлаживать. к примеру прошивки устройств на arm процессорах?

[Ответить]

shoker
14-10-2012 21:51

«В нашей программе всего 6 машинных команд, а за ними в памяти находится случайный мусор»

так это мусор? А я на одном сайте читал, что это команды, которые выполняются после завершения нашей программы.

[Ответить]

Мария
22-01-2013 21:22

Ребят, если у кого батник не компилится, оставаясь текстовым файлом, введите расширение .BAT, т.е. заглавными буквами. У меня на семерке тока из за этого не работало.

[Ответить]

Ваш комментарий

Имя *

Почта (скрыта) *

Сайт

Добавить

- [ ] Уведомить меня о новых комментариях по email.
- [ ] Уведомлять меня о новых записях почтой.