

МИНОБРНАУКИ РОССИИ
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)
Кафедра МО ЭВМ

ОТЧЕТ
по лабораторной работе №1
по дисциплине «Операционные системы»
Тема: Исследование структур загрузочных модулей

Студент гр. 9382

Савельев И.С.

Преподаватель

Ефремов М.А.

Санкт-Петербург

2021

Цель работы.

Исследование различий в структурах исходных текстов модулей типов .COM и .EXE, структур файлов загрузочных модулей и способов их загрузки в основную память.

Задание.

Шаг 1. Напишите текст исходного .COM модуля, который определяет тип РС версию системы. Это довольно простая задача и для тех, кто уже имеет опыт программирования на ассемблере, это будет небольшой разминкой. Для тех, кто раньше не сталкивался с программированием на ассемблере, это неплохая задача для первого опыта. За основу возьмите шаблон, приведенный в разделе «Основные сведения». Необходимые сведения о том, как извлечь требуемую информацию, представлены в следующем разделе. Ассемблерная программа должна читать содержимое предпоследнего байта ROM BIOS, по таблице, сравнивая коды, определять тип РС и выводить строку с названием модели. Если код не совпадает ни с одним значением, то двоичный код переводиться в символьную строку, содержащую запись шестнадцатеричного числа и выводиться на экран в виде соответствующего сообщения. Затем определяется версия системы. Ассемблерная программа должна по значениям регистров AL и AH формировать текстовую строку в формате xx.yy, где xx - номер основной версии, а yy - номер модификации в десятичной системе счисления, формировать строки с серийным номером OEM и серийным номером пользователя. Полученные строки выводятся на экран. Отладьте полученный исходный модуль. Результатом выполнения этого шага будет «хороший» .COM модуль, а также необходимо построить «плохой» .EXE, полученный из исходного текста для .COM модуля.

Шаг 2. Напишите текст исходного .EXE модуля, который выполняет те же функции, что и модуль в Шаге 1 и постройте и отладьте его. Таким образом, будет получен «хороший» .EXE.

Шаг 3. Сравните исходные тексты для .COM и .EXE модулей. Ответьте на контрольные вопросы «Отличия исходных текстов COM и EXE программ».

Шаг 4. Запустите FAR и откройте (F3/F4) файл загрузочного модуля .COM и файл «плохого» .EXE в шестнадцатеричном виде. Затем откройте (F3/F4) файл загрузочного модуля «хорошего» .EXE и сравните его с предыдущими файлами. Ответьте на контрольные вопросы «Отличия форматов файлов COM и EXE модулей».

Шаг 5. Откройте отладчик TD.EXE и загрузите .COM. Ответьте на контрольные вопросы «Загрузка COM модуля в основную память». Представьте в отчете план загрузки модуля .COM в основную память.

Шаг 6. Откройте отладчик TD.EXE и загрузите «хороший» .EXE. Ответьте на контрольные вопросы «Загрузка «хорошего» EXE модуля в основную память».

Шаг 7. Оформление отчета в соответствии с требованиями. В отчете необходимо привести скриншоты. Для файлов их вид в шестнадцатеричном виде, для загрузочных модулей – в отладчике

Ход работы.

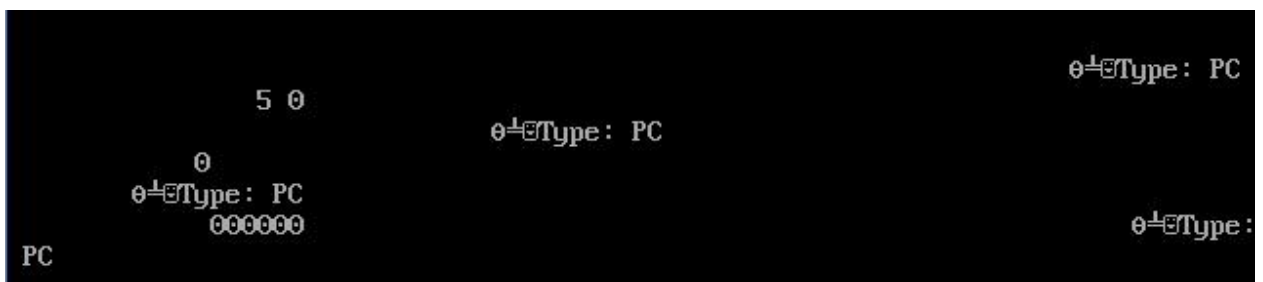
В обеих программах в начале были объявлены константные строки для вывода информации о ПК и версии MS DOS. Также были написаны собственные функции MYPRINT - для вывода строк, DEFINE_PC_TYP - для определения типа ПК и DEFINE_OS_VER - для определения версии MS DOS.

Запуск хорошего .com модуля

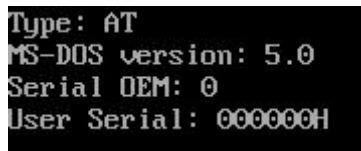


```
Type: AT
MS-DOS version: 5.0
Serial OEM: 0
User Serial: 0000000H
```

Запуск плохого .exe модуля



Запуск хорошего .exe модуля



Вывод.

В результате выполнения лабораторной работы были написаны программы для определения версии PC и MS DOS. Исследованы различия в структурах исходных текстовых модулей типов .COM и .EXE, структурах файлов загрузочных модулей и способов их загрузки в основную память.

Ответы на контрольные вопросы.

Отличия исходных текстов COM и EXE программ

1) Сколько сегментов должна содержать COM-программа?

У COM-программы 1 сегмент.

2) Сколько сегментов должна содержать EXE-программа?

У EXE-программы может быть больше одного сегмента, отдельные сегменты для данных, кода и стека.

3) Какие директивы должны обязательно быть в тексте COM программы?

В тексте COM-программы обязательно должна быть директива ORG 100h, так как в первых 256(100h) байтах находится PSP, а код программы располагается после него. Также обязательно должна присутствовать директива ASSUME, которая сообщает о том, какой сегмент к какому сегментному регистру привязан.

4) Все ли форматы команд можно использовать в COM-программе?

Нет, не все. Например в COM-программе нельзя использовать команды вида `mov register, segment`, так как в COM-программе отсутствует таблица настроек, которая содержит адреса, зависящие от расположения загрузочного модуля в оперативной памяти.

Отличия форматов файлов COM и EXE модулей

1) Какова структура файла COM? С какого адреса располагается код?

Структура состоит из одного сегмента размером не больше 64КБ. В файле код располагается с нулевого адреса, но при загрузке модуля смещается на 100h.

| | | | | |
|----------|-------------------------|-------------------------|-------------------------|---------------------|
| 00000000 | E9 | CF 01 54 79 70 65 3A | 20 50 43 0D 0A 24 54 79 | 01.Type: PC..\$Type |
| 00000010 | 70 65 3A 20 50 43 2F 58 | 54 0D 0A 24 54 79 70 65 | pe: PC/XT..\$Type | |
| 00000020 | 3A 20 41 54 0D 0A 24 54 | 79 70 65 3A 20 50 53 32 | : AT..\$Type: PS2 | |
| 00000030 | 20 6D 6F 64 65 6C 20 33 | 30 0D 0A 24 54 79 70 65 | model 30..\$Type | |
| 00000040 | 3A 20 50 53 32 20 6D 6F | 64 65 6C 20 35 30 20 6F | : PS2 model 50 o | |
| 00000050 | 72 20 36 30 0D 0A 24 54 | 79 70 65 3A 20 50 53 32 | r 60..\$Type: PS2 | |
| 00000060 | 20 6D 6F 64 65 6C 20 38 | 30 0D 0A 24 54 79 70 65 | model 80..\$Type | |
| 00000070 | 3A 20 50 D0 A1 6A 72 0D | 0A 24 54 79 70 65 3A 20 | : Pijr..\$Type: | |
| 00000080 | 50 43 20 43 6F 6E 76 65 | 72 74 69 62 6C 65 0D 0A | PC Convertible.. | |
| 00000090 | 24 4D 53 2D 44 4F 53 20 | 76 65 72 73 69 6F 6E 3A | \$MS-DOS version: | |
| 000000A0 | 20 20 2E 20 20 0D 0A 24 | 53 65 72 69 61 6C 20 4F | . ..\$Serial 0 | |
| 000000B0 | 45 4D 3A 20 20 0D 0A 24 | 55 73 65 72 20 53 65 72 | EM: ..\$User Ser | |
| 000000C0 | 69 61 6C 3A 20 20 20 20 | 20 20 20 48 0D 0A 24 24 | ial: H..\$\$ | |
| 000000D0 | 0F 3C 09 76 02 04 07 04 | 30 C3 51 8A E0 E8 EF FF | .<.v....0 Qèαφη | |
| 000000E0 | 86 C4 B1 04 D2 E8 E8 E6 | FF 59 C3 53 8A FC E8 E9 | â-...тФФμ Y Sè^nФ0 | |
| 000000F0 | FF 88 25 4F 88 05 4F 8A | C7 E8 DE FF 88 25 4F 88 | è%0è.0è Ф è%0è | |
| 00000100 | 05 5B C3 51 52 32 E4 33 | D2 B9 0A 00 F7 F1 80 CA | .[QR2Σ3т ..≈±çL | |
| 00000110 | 30 88 14 4E 33 D2 3D 0A | 00 73 F1 3C 00 74 04 0C | 0è.N3т=..s±<.t.. | |
| 00000120 | 30 88 04 5A 59 C3 B4 09 | CD 21 C3 B8 00 F0 8E C0 | 0è.ZYт =! т.≡ÄL | |
| 00000130 | 26 A0 FE FF 3C FF 74 1C | 3C FE 74 1E 3C FB 74 1A | &â. < t.< t.<√t. | |
| 00000140 | 3C FC 74 1C 3C FA 74 1E | 3C F8 74 26 3C FD 74 28 | <^nt.< t.<^nt&<^2t(| |
| 00000150 | 3C F9 74 2A BA 03 01 EB | 2B 90 BA 0E 01 EB 25 90 | < t* ..δ+É ..δ%É | |
| 00000160 | BA 1C 01 EB 1F 90 BA 27 | 01 EB 19 90 BA 3C 01 EB | ..δ.É '.δ.É <.δ | |
| 00000170 | 13 90 BA 57 01 EB 0D 90 | BA 6C 01 EB 07 90 BA 7A | .É w.δ.É L.δ.É z | |
| 00000180 | 01 EB 01 90 E8 9F FF C3 | B4 30 CD 21 50 BE 91 01 | .δ.ÉФf т 0=!Pδæ. | |
| 00000190 | 83 C6 10 E8 6D FF 58 8A | C4 83 C6 03 E8 64 FF BA | âт.Фm Xè-âт.Фd | |
| 000001A0 | 91 01 E8 81 FF BE A8 01 | 83 C6 0C 8A C7 E8 53 FF | æ.Фü тζ.âт.è ФS | |
| 000001B0 | BA A8 01 E8 70 FF BF B8 | 01 83 C7 12 8B C1 E8 2A | ζ.Фp тт.âт.îLФ* | |
| 000001C0 | FF 8A C3 E8 14 FF 83 EF | 02 89 05 BA B8 01 E8 55 | èт. ân.è. т.ФU | |
| 000001D0 | FF C3 E8 56 FF E8 B0 FF | 32 C0 B4 4C CD 21 | тV Ф 2тL=! | |

2) Какова структура файла «плохого» EXE? С какого адреса располагается код? Что располагается с адреса 0?

В «плохом» EXE файле данные и код содержатся в одном сегменте. Код располагается с адреса 300h. С адреса 0h располагается заголовок и таблица настроек.

| | | | | | | | | | | | | | | | | | | | | |
|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|-------|---|-------|----|
| 00000000 | 4D | 5A | DE | 00 | 03 | 00 | 00 | 00 | 20 | 00 | 00 | 00 | FF | FF | 00 | 00 | MZ | . | | .. |
| 00000010 | 00 | 00 | 04 | 89 | 00 | 01 | 00 | 00 | 1E | 00 | 00 | 00 | 01 | 00 | 00 | 00 | ... | ě | | |
| 00000020 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | |
| 00000030 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | |
| 00000040 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | |
| 00000050 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | |
| 00000060 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | |
| 00000070 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | |
| 00000080 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | |
| 00000090 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | |
| 000000A0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | |
| 000000B0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | |
| 000000C0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | |
| 000000D0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | |
| 000000E0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | |
| 000000F0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | |
| 00000100 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | |
| 00000110 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | |
| 00000120 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | |
| 00000130 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | |
| 00000140 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | |
| 00000150 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | |
| 00000160 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | |
| 00000170 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | |
| 00000180 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | |
| 00000190 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | |
| 000001A0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | |
| 000001B0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | |
| 000001C0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | |
| 000001D0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | |
| 000001E0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | |
| 000001F0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | | | | |

| | | | |
|----------|-------------------------|-------------------------|---------------------|
| 000002E0 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 | |
| 000002F0 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 | |
| 00000300 | E9 CF 01 54 79 70 65 3A | 20 50 43 0D 0A 24 54 79 | 0=..Type: PC..\$Ty |
| 00000310 | 70 65 3A 20 50 43 2F 58 | 54 0D 0A 24 54 79 70 65 | pe: PC/XT..\$Type |
| 00000320 | 3A 20 41 54 0D 0A 24 54 | 79 70 65 3A 20 50 53 32 | : AT..\$Type: PS2 |
| 00000330 | 20 6D 6F 64 65 6C 20 33 | 30 0D 0A 24 54 79 70 65 | model 30..\$Type |
| 00000340 | 3A 20 50 53 32 20 6D 6F | 64 65 6C 20 35 30 20 6F | : PS2 model 50 o |
| 00000350 | 72 20 36 30 0D 0A 24 54 | 79 70 65 3A 20 50 53 32 | r 60..\$Type: PS2 |
| 00000360 | 20 6D 6F 64 65 6C 20 38 | 30 0D 0A 24 54 79 70 65 | model 80..\$Type |
| 00000370 | 3A 20 50 D0 A1 6A 72 0D | 0A 24 54 79 70 65 3A 20 | : P\ijr..\$Type: |
| 00000380 | 50 43 20 43 6F 6E 76 65 | 72 74 69 62 6C 65 0D 0A | PC Convertible.. |
| 00000390 | 24 4D 53 2D 44 4F 53 20 | 76 65 72 73 69 6F 6E 3A | \$MS-DOS version: |
| 000003A0 | 20 20 2E 20 20 0D 0A 24 | 53 65 72 69 61 6C 20 4F | . ..\$Serial 0 |
| 000003B0 | 45 4D 3A 20 20 0D 0A 24 | 55 73 65 72 20 53 65 72 | EM: ..\$User Ser |
| 000003C0 | 69 61 6C 3A 20 20 20 20 | 20 20 20 48 0D 0A 24 24 | ial: H..\$\$ |
| 000003D0 | 0F 3C 09 76 02 04 07 04 | 30 C3 51 8A E0 E8 EF FF | .<.v....0 Qèαφη |
| 000003E0 | 86 C4 B1 04 D2 E8 E8 E6 | FF 59 C3 53 8A FC E8 E9 | â- .тФФμ γ SèⁿΦθ |
| 000003F0 | FF 88 25 4F 88 05 4F 8A | C7 E8 DE FF 88 25 4F 88 | ê%0ê.0è Φ ê%0ê |
| 00000400 | 05 5B C3 51 52 32 E4 33 | D2 B9 0A 00 F7 F1 80 CA | .[QR2Σ3т ..≈±ç± |
| 00000410 | 30 88 14 4E 33 D2 3D 0A | 00 73 F1 3C 00 74 04 0C | 0ê.N3т=.s±<.t.. |
| 00000420 | 30 88 04 5A 59 C3 B4 09 | CD 21 C3 B8 00 F0 8E C0 | 0ê.ZY .!= γ.≡Ä L |
| 00000430 | 26 A0 FE FF 3C FF 74 1C | 3C FE 74 1E 3C FB 74 1A | &â. < t.<·t.<√t. |
| 00000440 | 3C FC 74 1C 3C FA 74 1E | 3C F8 74 26 3C FD 74 28 | <ⁿt.<·t.<°t&<²t(|
| 00000450 | 3C F9 74 2A BA 03 01 EB | 2B 90 BA 0E 01 EB 25 90 | <·t* ..δ+É ..δ%É |
| 00000460 | BA 1C 01 EB 1F 90 BA 27 | 01 EB 19 90 BA 3C 01 EB | ..δ.É '.δ.É <.δ |
| 00000470 | 13 90 BA 57 01 EB 0D 90 | BA 6C 01 EB 07 90 BA 7A | .É w.δ.É λ.δ.É z |
| 00000480 | 01 EB 01 90 E8 9F FF C3 | B4 30 CD 21 50 BE 91 01 | .δ.ÉΦf 0= P æ. |
| 00000490 | 83 C6 10 E8 6D FF 58 8A | C4 83 C6 03 E8 64 FF BA | â .Φm Xè-â .Φd |
| 000004A0 | 91 01 E8 81 FF BE A8 01 | 83 C6 0C 8A C7 E8 53 FF | æ.Φü ↓¿.â .è ΦS |
| 000004B0 | BA A8 01 E8 70 FF BF B8 | 01 83 C7 12 8B C1 E8 2A | ¿.Φp γγ.â .î↓Φ* |
| 000004C0 | FF 8A C3 E8 14 FF 83 EF | 02 89 05 BA B8 01 E8 55 | è Φ. ân.ë. γ.ΦU |
| 000004D0 | FF C3 E8 56 FF E8 B0 FF | 32 C0 B4 4C CD 21 | ΦV Φ\\ 2 L L=! |

3) Какова структура файла «хорошего» EXE? Чем он отличается от файла «плохого» EXE?

В «хорошем» EXE, код, стек и данные выделены в отдельные сегменты в отличие от «плохого», который не имеет деления на сегменты. В «хорошего» EXE адресация кода начинается с 300h (200h под заголовок и таблицу, 100h под стек).

| | | | | | | | | | | | | | | | | | |
|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|-------------|
| 00000000 | 4D | 5A | E7 | 00 | 03 | 00 | 01 | 00 | 20 | 00 | 00 | 00 | FF | FF | 00 | 00 | MZt..... .. |
| 00000010 | 00 | 01 | 2F | 99 | 03 | 01 | 1D | 00 | 1E | 00 | 00 | 00 | 01 | 00 | 07 | 01 | .. /Ö..... |
| 00000020 | 1D | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000030 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000040 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000050 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000060 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000070 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000080 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000090 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000000A0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000000B0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000000C0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000000D0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000000E0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000000F0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | .. /Ö..... |
| 00000100 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000110 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000120 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000130 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000140 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000150 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000160 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000170 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000180 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000190 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000001A0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000001B0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000001C0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000001D0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 000001E0 | 00 | 00 | 00 | | | | | | | | | | | | | | |

| | | | |
|----------|-------------------------|-------------------------|-----------------------|
| 000002F0 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 | |
| 00000300 | 54 79 70 65 3A 20 50 43 | 0D 0A 24 54 79 70 65 3A | Type: PC..\$Type: |
| 00000310 | 20 50 43 2F 58 54 0D 0A | 24 54 79 70 65 3A 20 41 | PC/XT..\$Type: A |
| 00000320 | 54 0D 0A 24 54 79 70 65 | 3A 20 50 53 32 20 6D 6F | T..\$Type: PS2 mo |
| 00000330 | 64 65 6C 20 33 30 0D 0A | 24 54 79 70 65 3A 20 50 | del 30..\$Type: P |
| 00000340 | 53 32 20 6D 6F 64 65 6C | 20 35 30 20 6F 72 20 36 | S2 model 50 or 6 |
| 00000350 | 30 0D 0A 24 54 79 70 65 | 3A 20 50 53 32 20 6D 6F | 0..\$Type: PS2 mo |
| 00000360 | 64 65 6C 20 38 30 0D 0A | 24 54 79 70 65 3A 20 50 | del 80..\$Type: P |
| 00000370 | D0 A1 6A 72 0D 0A 24 54 | 79 70 65 3A 20 50 43 20 | lir..\$Type: PC |
| 00000380 | 43 6F 6E 76 65 72 74 69 | 62 6C 65 0D 0A 24 4D 53 | Convertible..\$MS |
| 00000390 | 2D 44 4F 53 20 76 65 72 | 73 69 6F 6E 3A 20 20 2E | -DOS version: . |
| 000003A0 | 20 20 0D 0A 24 53 65 72 | 69 61 6C 20 4F 45 4D 3A | ..\$Serial OEM: |
| 000003B0 | 20 20 0D 0A 24 55 73 65 | 72 20 53 65 72 69 61 6C | ..\$User Serial |
| 000003C0 | 3A 20 20 20 20 20 20 20 | 48 0D 0A 24 00 00 00 00 | : H..\$.... |
| 000003D0 | 24 0F 3C 09 76 02 04 07 | 04 30 C3 51 8A E0 E8 EF | \$.<.v....0 QèαΦη |
| 000003E0 | FF 86 C4 B1 04 D2 E8 E8 | E6 FF 59 C3 53 8A FC E8 | â-ΠΦμ Y Sè^nΦ |
| 000003F0 | E9 FF 88 25 4F 88 05 4F | 8A C7 E8 DE FF 88 25 4F | θ è%0è.Oè Φ è%0 |
| 00000400 | 88 05 5B C3 51 52 32 E4 | 33 D2 B9 0A 00 F7 F1 80 | è. [QR2Σ3Π ..≈±Ç |
| 00000410 | CA 30 88 14 4E 33 D2 3D | 0A 00 73 F1 3C 00 74 04 | ⌚0è.N3Π=..s±<.t. |
| 00000420 | 0C 30 88 04 5A 59 C3 B4 | 09 CD 21 C3 B8 00 F0 8E | .0è.ZY =! γ.≡Ä |
| 00000430 | C0 26 A0 FE FF 3C FF 74 | 1C 3C FE 74 1E 3C FB 74 | L&á. < t.<.t.<√t |
| 00000440 | 1A 3C FC 74 1C 3C FA 74 | 1E 3C F8 74 26 3C FD 74 | .<^t.<.t.<^t&<^t |
| 00000450 | 28 3C F9 74 2A BA 00 00 | EB 2B 90 BA 0B 00 EB 25 | (<.t* ..δ+É ..δ% |
| 00000460 | 90 BA 19 00 EB 1F 90 BA | 24 00 EB 19 90 BA 39 00 | É ..δ.É \$.δ.É 9. |
| 00000470 | EB 13 90 BA 54 00 EB 0D | 90 BA 69 00 EB 07 90 BA | δ.É T.δ.É i.δ.É |
| 00000480 | 77 00 EB 01 90 E8 9F FF | C3 B4 30 CD 21 50 BE 8E | w.δ.ÉΦf 0= P Ä |
| 00000490 | 00 83 C6 10 E8 6D FF 58 | 8A C4 83 C6 03 E8 64 FF | .â .Φm Xè-â .Φd |
| 000004A0 | BA 8E 00 E8 81 FF BE A5 | 00 83 C6 0C 8A C7 E8 53 | Ä.Φü N.â .è ΦS |
| 000004B0 | FF BA A5 00 E8 70 FF BF | B5 00 83 C7 12 8B C1 E8 | N.Φp γ .â .i Φ |
| 000004C0 | 2A FF 8A C3 E8 14 FF 83 | EF 02 89 05 BA B5 00 E8 | * è Φ. ân.ë. .Φ |
| 000004D0 | 55 FF C3 2B C0 50 B8 10 | 00 8E D8 E8 4E FF E8 A8 | U Lpγ ..Ä ΦN Φz |
| 000004E0 | FF 32 C0 B4 4C CD 21 | + | 2 L=! |

Загрузка COM модуля в основную память.

DOSBox 0.74-3, Cpu speed: ...eskip 0, Program: AFDPRO

| | | | | | |
|---------|---------|---------|---------|---------------|-------------------------|
| AX 0000 | SI 0000 | CS 19F5 | IP 0100 | Stack +0 0000 | Flags 7202 |
| BX 0000 | DI 0000 | DS 19F5 | | +2 20CD | |
| CX 01DE | BP 0000 | ES 19F5 | HS 19F5 | +4 9FFF | OF DF IF SF ZF AF PF CF |
| DX 0000 | SP FFFE | SS 19F5 | FS 19F5 | +6 EA00 | 0 0 1 0 0 0 0 |

CMD >

| | | |
|-------------|------|-------------|
| 0100 E9CF01 | JMP | 02D2 |
| 0103 54 | PUSH | SP |
| 0104 7970 | JNS | 0176 |
| 0106 65 | DB | 65 |
| 0107 3A20 | CMP | AH, [BX+SI] |
| 0109 50 | PUSH | AX |
| 010A 43 | INC | BX |
| 010B 0D0A24 | OR | AX, 240A |

| | |
|---------|-------------------------|
| DS:0000 | CD 20 FF 9F 00 EA F0 FE |
| DS:0008 | AD DE 1B 05 C5 06 00 00 |
| DS:0010 | 18 01 10 01 18 01 92 01 |
| DS:0018 | 01 01 01 00 FF 00 01 FF |
| DS:0020 | FF FF FF FF FF FF FF FF |
| DS:0028 | FF FF FF FF EB 19 C0 11 |
| DS:0030 | A2 01 14 00 18 00 F5 19 |
| DS:0038 | FF FF FF FF 00 00 00 00 |
| DS:0040 | 05 00 00 00 00 00 00 00 |
| DS:0048 | 00 00 00 00 00 00 00 00 |

| | | |
|---------|-------------------------|-------------------------|
| DS:0000 | CD 20 FF 9F 00 EA F0 FE | AD DE 1B 05 C5 06 00 00 |
| DS:0010 | 18 01 10 01 18 01 92 01 | 01 01 01 00 FF 00 01 FF |
| DS:0020 | FF FF FF FF FF FF FF FF | FF FF FF FF EB 19 C0 11 |
| DS:0030 | A2 01 14 00 18 00 F5 19 | FF FF FF FF 00 00 00 00 |
| DS:0040 | 05 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 |

1 Step 2ProcStep 3Retrieve 4Help ON 5BRK Menu 6 7 ↑ 8 ↓ 9 ← 10 ⇒

- 1) Какой формат загрузки COM модуля? С какого адреса располагается код?

В начале определяется адрес сегмента оперативной памяти, в котором хватит места для загрузки программы, после чего система отводит первые 256 байт для PSP, а COM файл помещается в память со смещением 100h. Затем инициализируются сегментные регистры, которые все указывают на начало PSP. SP при этом будет указывать на конец PSP, IP станет равным 100h, в стек будет помещено 0000h. Код будет располагаться со смещением в 100h.

- 2) Что располагается с 0 адреса?

Сегмент PSP.

- 3) Какие значения имеют сегментные регистры? На какие области памяти они указывают?

Сегментные регистры будут иметь одинаковые значения. И будут указывать на начало PSP.

4) Как определяется стек? Какую область памяти он занимает? Какие адреса?

Стек определяется автоматически. Регистр SS указывает на начало сегмента, а SP=FFFEh – на его конец.

Загрузка «хорошего» EXE модуля в основную память

| | | | | | |
|---------|---------|---------|---------|---------------|-------------------------|
| AX 0000 | SI 0000 | CS 1A22 | IP 0103 | Stack +0 7954 | Flags 7202 |
| BX 0000 | DI 0000 | DS 19F5 | | +2 6570 | |
| CX 02E7 | BP 0000 | ES 19F5 | HS 19F5 | +4 203A | OF DF IF SF ZF AF PF CF |
| DX 0000 | SP 0100 | SS 1A05 | FS 19F5 | +6 4350 | 0 0 1 0 0 0 0 0 |

| | | | | | | | | | | | | | | | | | | | |
|-------|--|--|--|---|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| CMD > | | | | <div>10 1 2 3 4 5 6 7</div> <div>DS:0000 CD 20 FF 9F 00 EA F0 FE</div> <div>DS:0008 AD DE 1B 05 C5 06 00 00</div> <div>DS:0010 18 01 10 01 18 01 92 01</div> <div>DS:0018 01 01 01 00 FF 00 01 FF</div> <div>DS:0020 FF FF FF FF FF FF FF FF</div> <div>DS:0028 FF FF FF FF EB 19 C0 11</div> <div>DS:0030 A2 01 14 00 18 00 F5 19</div> <div>DS:0038 FF FF FF FF 00 00 00 00</div> <div>DS:0040 05 00 00 00 00 00 00 00</div> <div>DS:0048 00 00 00 00 00 00 00 00</div> | | | | | | | | | | | | | | | |
|-------|--|--|--|---|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|

| | | | | | | | | | | | | | | | | |
|---------------------------------|--|--|--|-------------------------|--|--|--|--|--|--|--|--|--|--|--|--|
| 20 1 2 3 4 5 6 7 | | | | 8 9 A B C D E F | | | | | | | | | | | | <div>= f. n = i . + . .</div> <div>.....f.</div> <div>. L .</div> <div>6 J</div> <div>.....</div> |
| DS:0000 CD 20 FF 9F 00 EA F0 FE | | | | AD DE 1B 05 C5 06 00 00 | | | | | | | | | | | | |
| DS:0010 18 01 10 01 18 01 92 01 | | | | 01 01 01 00 FF 00 01 FF | | | | | | | | | | | | |
| DS:0020 FF FF FF FF FF FF FF FF | | | | FF FF FF FF EB 19 C0 11 | | | | | | | | | | | | |
| DS:0030 A2 01 14 00 18 00 F5 19 | | | | FF FF FF FF 00 00 00 00 | | | | | | | | | | | | |
| DS:0040 05 00 00 00 00 00 00 00 | | | | 00 00 00 00 00 00 00 00 | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | | | |
|---|------|---|----------|---|----------|---|---------|---|----------|---|--|---|---|---|---|---|---|----|---|
| 1 | Step | 2 | ProcStep | 3 | Retrieve | 4 | Help ON | 5 | BRK Menu | 6 | | 7 | ↑ | 8 | ↓ | 9 | ← | 10 | → |
|---|------|---|----------|---|----------|---|---------|---|----------|---|--|---|---|---|---|---|---|----|---|

1) Как загружается «хороший» EXE? Какие значения имеют сегментные регистры?

Сначала считывается информация с заголовка EXE. Затем инициализируются сегментные регистры. SS будет указывать на начало сегмента стека, PS на конец сегмента стека, CS на начало сегмента кода. В IP запишется точка входа в программу.

2) На что указывают регистры DS и ES ?

ES и DS будут указывать на начало PSP.

3) Как определяется стек?

В программе с помощью специальной директивы .STACK с указанием размера.

4) Как определяется точка входа?

Точка входа в программу определяется с помощью директивы END.