

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

ОТЧЕТ
по лабораторной работе №1
по дисциплине «Операционные системы»

Тема: Исследование структур загрузочных модулей

Студент гр. 0381

Павлов Е. А.

Преподаватель

Ефремов М. А.

Санкт-Петербург

2022

Цель работы.

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

Задание.

Ассемблерная программа должна читать содержимое предпоследнего байта ROM BIOS, по таблице, сравнивая коды, определять тип PC 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.

Результатом выполнения этого шага будет «хороший» .COM модуль, а также необходимо построить «плохой» .EXE, полученный из исходного текста для .COM модуля.

Напишите текст исходного .EXE модуля, который выполняет те же функции и постройте его. Таким образом будет получен хороший .EXE модуль. Сравните исходные тексты для .COM и .EXE модулей. Сравните файлы .COM, «плохого» и «хорошего» .EXE модулей в шестнадцатеричном виде.

Выполнение работы.

Для написания исходного текста .COM модуля был использован шаблон из методических указаний. Были добавлены строки с названиями моделей для последующего вывода на экран.

Для получения информации о версии DOS используется функция 30h прерывания 21h. Полученные значения переводятся в требуемый формат и выводятся на экран.

```
F:\>exe2bin lb1.exe lb1.com

F:\>lb1.com
IBM PC type: AT
MS DOS version: 05.0
OEM: 0
User: 000000H

F:\>
```

```
F:\>1b1.exe
= Я Ъ Н ll Ë ↑▶↑↑↑↑↑↑ 0      H@W B@M ↑ T@      ♠

                                     ш?@IBM PC type: PC

                    5 0
                ш?@IBM PC type: PC

0                                     ш?@IBM PC typ
e: PC

                                ш?@IBM PC type: PC

F:\>
```

```
F:\>lb1_exe.exe
IBM PC type: AT
MS DOS version: 05.0
OEM:240
User: 0000000H
F:\>_
```

Ответы на вопросы см. в разделе «Вопросы».

Выводы.

Были исследованы различия в структуре исходных текстов для модулей .COM и .EXE, структура загрузочных файлов этих типов и способы загрузки их в основную память.

Такой файл содержит заголовок, таблицу настройки адресов и один сегмент, в котором находятся данные и код. Код располагается с адреса 300h, потому что 200h – заголовок и таблица настроек, а 100h – смещение ORG 100h. С адреса 0h располагается заголовок EXE файла, который содержит сигнатуру EXE файла, длину образа программы, размер таблицы настройки, сегментный адрес стека, адрес точки входа, а также ряд других параметров, необходимых для загрузки.

Address	Hex	ASCII
00000000	5A CA 00	MZ.....
00000001	00 00 00 00
00000002	00 00 00 00
00000003	00 00 00 00
00000004	00 00 00 00
00000005	00 00 00 00
00000006	00 00 00 00
00000007	00 00 00 00
00000008	00 00 00 00
00000009	00 00 00 00
0000000A	00 00 00 00
0000000B	00 00 00 00
0000000C	00 00 00 00
0000000D	00 00 00 00
0000000E	00 00 00 00
0000000F	00 00 00 00
00000010	00 00 00 00
00000011	00 00 00 00
00000012	00 00 00 00
00000013	00 00 00 00
00000014	00 00 00 00
00000015	00 00 00 00
00000016	00 00 00 00
00000017	00 00 00 00
00000018	00 00 00 00
00000019	00 00 00 00
0000001A	00 00 00 00
0000001B	00 00 00 00
0000001C	00 00 00 00
0000001D	00 00 00 00
0000001E	00 00 00 00
0000001F	00 00 00 00
00000020	00 00 00 00
00000021	00 00 00 00
00000022	00 00 00 00
00000023	00 00 00 00
00000024	00 00 00 00
00000025	00 00 00 00
00000026	00 00 00 00
00000027	00 00 00 00
00000028	00 00 00 00
00000029	00 00 00 00
0000002A	00 00 00 00
0000002B	00 00 00 00
0000002C	00 00 00 00
0000002D	00 00 00 00
0000002E	00 00 00 00
0000002F	00 00 00 00
00000030	2F 58 54 0D
00000031	0A 24 49 42
00000032	40 20 50 43
00000033	50 43 20 43
00000034	65 3A 20 41
00000035	54 00 0A 24
00000036	49 42 40 20
00000037	50 43 20 43
00000038	6F 0E 70 65
00000039	72 74 09 62
0000003A	6C 65 00 0A
0000003B	24 49 42 40
0000003C	20 50 43 20
0000003D	74 79 70 65
0000003E	0A 24 49 42
0000003F	40 20 50 43
00000040	20 74 79 70
00000041	65 3A 20 50
00000042	43 6A 72 0D
00000043	0A 24 49 42
00000044	40 20 50 43
00000045	20 74 79 70
00000046	6C 6F 64 65
00000047	6C 20 33 30
00000048	00 0A 24 49
00000049	42 4D 20 50
0000004A	3A 20 50 43
0000004B	74 79 70 65
0000004C	20 50 43 20
0000004D	74 79 70 65
0000004E	00 00 00 00
0000004F	00 00 00 00
00000050	00 00 00 00
00000051	00 00 00 00
00000052	00 00 00 00
00000053	00 00 00 00
00000054	00 00 00 00
00000055	00 00 00 00
00000056	00 00 00 00
00000057	00 00 00 00
00000058	00 00 00 00
00000059	00 00 00 00
0000005A	00 00 00 00
0000005B	00 00 00 00
0000005C	00 00 00 00
0000005D	00 00 00 00
0000005E	00 00 00 00
0000005F	00 00 00 00
00000060	00 00 00 00
00000061	00 00 00 00
00000062	00 00 00 00
00000063	00 00 00 00
00000064	00 00 00 00
00000065	00 00 00 00
00000066	00 00 00 00
00000067	00 00 00 00
00000068	00 00 00 00
00000069	00 00 00 00
0000006A	00 00 00 00
0000006B	00 00 00 00
0000006C	00 00 00 00
0000006D	00 00 00 00
0000006E	00 00 00 00
0000006F	00 00 00 00
00000070	00 00 00 00
00000071	00 00 00 00
00000072	00 00 00 00
00000073	00 00 00 00
00000074	00 00 00 00
00000075	00 00 00 00
00000076	00 00 00 00
00000077	00 00 00 00
00000078	00 00 00 00
00000079	00 00 00 00
0000007A	00 00 00 00
0000007B	00 00 00 00
0000007C	00 00 00 00
0000007D	00 00 00 00
0000007E	00 00 00 00
0000007F	00 00 00 00
00000080	00 00 00 00
00000081	00 00 00 00
00000082	00 00 00 00
00000083	00 00 00 00
00000084	00 00 00 00
00000085	00 00 00 00
00000086	00 00 00 00
00000087	00 00 00 00
00000088	00 00 00 00
00000089	00 00 00 00
0000008A	00 00 00 00
0000008B	00 00 00 00
0000008C	00 00 00 00
0000008D	00 00 00 00
0000008E	00 00 00 00
0000008F	00 00 00 00
00000090	00 00 00 00
00000091	00 00 00 00
00000092	00 00 00 00
00000093	00 00 00 00
00000094	00 00 00 00
00000095	00 00 00 00
00000096	00 00 00 00
00000097	00 00 00 00
00000098	00 00 00 00
00000099	00 00 00 00
0000009A	00 00 00 00
0000009B	00 00 00 00
0000009C	00 00 00 00
0000009D	00 00 00 00
0000009E	00 00 00 00
0000009F	00 00 00 00
000000A0	00 00 00 00
000000A1	00 00 00 00
000000A2	00 00 00 00
000000A3	00 00 00 00
000000A4	00 00 00 00
000000A5	00 00 00 00
000000A6	00 00 00 00
000000A7	00 00 00 00
000000A8	00 00 00 00
000000A9	00 00 00 00
000000AA	00 00 00 00
000000AB	00 00 00 00
000000AC	00 00 00 00
000000AD	00 00 00 00
000000AE	00 00 00 00
000000AF	00 00 00 00
000000B0	00 00 00 00
000000B1	00 00 00 00
000000B2	00 00 00 00
000000B3	00 00 00 00
000000B4	00 00 00 00
000000B5	00 00 00 00
000000B6	00 00 00 00
000000B7	00 00 00 00
000000B8	00 00 00 00
000000B9	00 00 00 00
000000BA	00 00 00 00
000000BB	00 00 00 00
000000BC	00 00 00 00
000000BD	00 00 00 00
000000BE	00 00 00 00
000000BF	00 00 00 00
000000C0	00 00 00 00
000000C1	00 00 00 00
000000C2	00 00 00 00
000000C3	00 00 00 00
000000C4	00 00 00 00
000000C5	00 00 00 00
000000C6	00 00 00 00
000000C7	00 00 00 00
000000C8	00 00 00 00
000000C9	00 00 00 00
000000CA	00 00 00 00
000000CB	00 00 00 00
000000CC	00 00 00 00
000000CD	00 00 00 00
000000CE	00 00 00 00
000000CF	00 00 00 00
000000D0	00 00 00 00
000000D1	00 00 00 00
000000D2	00 00 00 00
000000D3	00 00 00 00
000000D4	00 00 00 00
000000D5	00 00 00 00
000000D6	00 00 00 00
000000D7	00 00 00 00
000000D8	00 00 00 00
000000D9	00 00 00 00
000000DA	00 00 00 00
000000DB	00 00 00 00
000000DC	00 00 00 00
000000DD	00 00 00 00
000000DE	00 00 00 00
000000DF	00 00 00 00
000000E0	00 00 00 00
000000E1	00 00 00 00
000000E2	00 00 00 00
000000E3	00 00 00 00
000000E4	00 00 00 00
000000E5	00 00 00 00
000000E6	00 00 00 00
000000E7	00 00 00 00
000000E8	00 00 00 00
000000E9	00 00 00 00
000000EA	00 00 00 00
000000EB	00 00 00 00
000000EC	00 00 00 00
000000ED	00 00 00 00
000000EE	00 00 00 00
000000EF	00 00 00 00
000000F0	00 00 00 00
000000F1	00 00 00 00
000000F2	00 00 00 00
000000F3	00 00 00 00
000000F4	00 00 00 00
000000F5	00 00 00 00
000000F6	00 00 00 00
000000F7	00 00 00 00
000000F8	00 00 00 00
000000F9	00 00 00 00
000000FA	00 00 00 00
000000FB	00 00 00 00
000000FC	00 00 00 00
000000FD	00 00 00 00
000000FE	00 00 00 00
000000FF	00 00 00 00

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

«Хороший» содержит заголовок и таблицу настройки адресов, общая длина которых 200h. В отличие от «плохого» EXE файла после таблицы идет три отдельных сегмента: сегмента стека, сегмента данных и сегмент кода.

Загрузка COM модуля в основную память

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

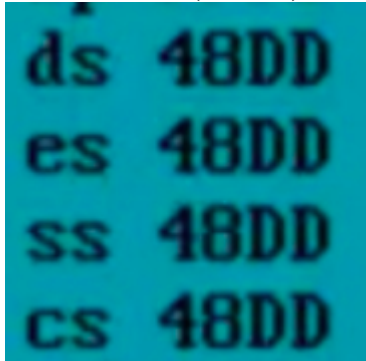
Происходит выделение свободного сегмента памяти, адрес заносится в сегментные регистры. В первые 256 байт этого сегмента записывается PSP, далее происходит подгрузка COM-файла без изменений. В стек записывается адрес возврата, SP указывает на конец сегмента.

2. Что располагается с адреса 0?

Префикс программного сегмента.

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

Одинаковое(48DD). Указывают на начало PSP.



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

Автоматически. Перед PSP. В диапазоне FFFEh-0h

Загрузка «хорошего» EXE модуля в основную память

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

Построение PSP, определение сегментного адреса, обработка таблицы настройки адресов

2. На что указывают регистры DS и ES?

На PSP.

3. Как определяется стек?

Стек задается парой регистров SS:SP. При запуске программы в SS помещается смещение сегмента стека относительно начального сегмента программы, который содержится в заголовке, плюс адрес начального сегмента. В SP же помещается значение напрямую из заголовка.

4. Как определяется точка входа?

С помощью директивы END