Отчет

По лабораторной работе №1

По дисциплине "Операционные системы"

Тема: Исследование структур загрузочных модулей

Студент гр. 8382		Гордиенко А.М.
Преподаватель		Ефремов М.А.

Санкт-Петербург

2020

Цель работы.

Исследование различий структур исходных модулей типов .com и .exe, структур файлов загрузочных модулей и способов загрузки в основную память.

Необходимые сведения.

Тип IBM PC хранится в байте по адресу 0F000:0FFFEh, в предпоследнем байте ROM BIOS. Соответствие кода и типа в таблице:

PC	**FF**
PC/XT	**FE, FB**
AT	**FC**
PS2 модель 30	**FA**
PS2 модель 50 или 60	**FC**
PS2 модель 80	**F8**
PCjr	**FD**
PC Convertible	**F9**

Для определения версии MS DOS следует воспользоваться функцией 30h прерывания 21h. Входным параметром является номер функции в AH:

mov ah, 30h

int 21h

Выходными параметрами являются:

AL - номер основной версии. Если 0, то <2.0

AH - номер модификации

BH - серийный номер OEM(Original Equipment Manufacturer)

BL:CX – 24-битовый серийный номер пользователя.

Постановка задачи.

Требуется реализовать текст исходного .com модуля, который определяет тип PC и версию системы. 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.
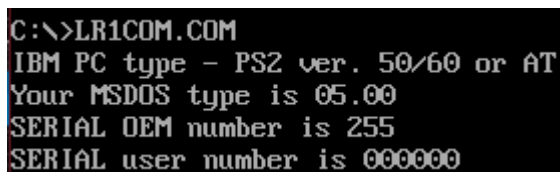
Далее необходимо отладить полученный исходный модуль и получить "хороший" .com модуль, а также необходимо построить "плохой" .exe, полученный из исходного текста для .com модуля.

Затем нужно написать текст "хорошего" .exe модуля, который выполняет те же функции, что и модуль .com, далее его построить, отладить и сравнить исходные тексты для .com и .exe модулей.

Выполнение работы.

Для определения типа PC и версии были написаны тексты .com и .exe модулей. Для определения версии MS DOS была использована функция 30h прерывания 21h. После ее вызова версия системы определяется значением регистров al, ah. В регистре bh - серийный номер OEM, в bl:cx – 24-битовый серийный номер пользователя.

Результат выполнения .com модуля виден на рис. 1. Результат выполнения "плохого" .exe модуля, полученного из исходного текста для .com модуля, виден на рис. 2. Результат выполнения "хорошего" .exe модуля - на рис. 3.

Рисунок 1 - Результат работы lr1com.com

Рисунок 2 - Результат lr1com.exe

Рисунок 3 - Результат работы lr1exe.exe

Представление исходных файлов в шестнадцатеричном виде представление исходных файлов в шестнадцатеричном виде:

Рисунок 4 – lr1com.com в шестнадцатеричном виде.

```
0000000000:  4D 5A CB 00 03 00 00 00   20 00 00 00 FF FF 00 00   MZË ♥     ÿÿ
0000000010:  00 00 A4 0F 00 01 00 00   1E 00 00 00 01 00 00 00   Hо ☺     ▲    ☺
0000000020:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000030:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000040:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000050:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000060:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000070:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000080:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000090:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000000A0:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000000B0:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000000C0:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000000D0:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000000E0:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000000F0:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000100:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000110:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000120:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000130:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000140:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000150:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000160:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000170:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000180:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000190:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000001A0:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000001B0:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000001C0:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000001D0:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000001E0:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000001F0:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000200:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000210:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000220:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000230:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000240:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000250:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000260:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000270:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000280:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000290:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000002A0:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000002B0:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000002C0:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000002D0:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000002E0:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000002F0:  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000300:  E9 0E 01 49 42 4D 20 50   43 20 74 79 70 65 20 2D   é♫☺IBM PC type -
0000000310:  20 24 50 43 0A 0D 24 50   43 2F 58 54 0A 0D 24 50    $PC♪$PC/XT♪$P
0000000320:  53 32 20 76 65 72 2E 20   33 30 0A 0D 24 50 53 32   S2 ver. 30☒♪$PS2
0000000330:  20 76 65 72 2E 20 35 30   2F 36 30 20 6F 72 20 41    ver. 50/60 or A
0000000340:  54 0A 0D 24 50 53 32 20   76 65 72 2E 20 38 30 0A   T☒♪$PS2 ver. 80☒
0000000350:  0D 24 50 43 6A 72 0A 0D   24 50 43 20 43 6F 6E 76   ♪$PCjr☒♪$PC Conv
0000000360:  65 72 74 69 62 6C 65 0A   0D 24 59 6F 75 72 20 4D   ertible☒♪$Your M
0000000370:  53 44 4F 53 20 74 79 70   65 20 69 73 20 24 3C 32   SDOS type is $<2
0000000380:  2E 30 0A 0D 24 30 78 2E   30 79 0A 0D 24 53 45 52   .0☒♪$0x.0y☒♪$SER
0000000390:  49 41 4C 20 4F 45 4D 20   6E 75 6D 62 65 72 20 69   IAL OEM number i
00000003A0:  73 20 24 0A 0D 53 45 52   49 41 4C 20 75 73 65 72   s $☒♪SERIAL user
00000003B0:  20 6E 75 6D 62 65 72 20   69 73 20 24 51 52 E8 1C    number is $QRèL
00000003C0:  00 8A EC 8A D0 B4 02 CD   21 8A D5 B4 02 CD 21 5A   šìŠÐ´☻Í!ŠÕ´☻Í!Z
00000003D0:  59 C3 24 0F 3C 09 76 02   04 07 04 30 C3 51 8A E0   YÃ$☼<○v☻♦•♦0ÃQŠà
00000003E0:  E8 EF FF 86 C4 B1 04 D2   E8 E6 FF 59 C3 51 52       èïÿ†Ä±♦Òèæ ÿYÃQR
00000003F0:  32 E4 33 D2 B9 0A 00 F7   F1 80 CA 30 88 14 4E 33   2ä3Ò¹☒ ÷ñ€Ê0ˆ¶N3
0000000400:  D2 3D 0A 00 73 F1 3C 00   74 04 0C 30 88 04 5A 59   Ò=☒ sñ< t♦♀0ˆ♦ZY
0000000410:  C3 B8 00 F0 8E C0 26 A0   FE FF BA 03 01 B4 09 CD   Ã, ðŽÀ& þÿº☺´○Í
0000000420:  21 BA 12 01 3C FF 74 31   BA 17 01 3C FE 74 2A 3C   !º‡☺<ÿt1º‡☺<þt*<
0000000430:  FB 74 26 BA 2D 01 3C FC   74 1F BA 1F 01 3C FA 74   ût&º-☺<üt▼º☼<út
0000000440:  18 BA 44 01 3C F8 74 11   BA 52 01 3C FD 74 0A BA   ↑ºD☺<øt◄☺R☺<ýt☒º
0000000450:  59 01 3C F9 75 00 E8 63   FF B4 09 CD 21 BA 6A 01   Y☺<ùu èc ´○Í!ºj☺
0000000460:  B4 09 CD 21 B4 30 CD 21   3C 00 75 07 BA 7E 01 B4   ´○Í!´0Í!< u•º~☺´
0000000470:  09 CD 21 BE 85 01 83 C6   01 E8 72 FF 83 C6 04 8A   ○Í!¾…☺fÆèrÿfÆ♦Š
0000000480:  C4 E8 6A FF BA 85 01 B4   09 CD 21 B4 30 CD 21 BA   Äèjÿ…☺´○Í!´0Í!º
0000000490:  8D 01 B4 09 CD 21 8A C7   E8 53 FF 8A 14 B4 02 CD   ☒☺´○Í!ŠÇèSÿŠ¶´☻Í
00000004A0:  21 8A 54 01 CD 21 8A 54   02 CD 21 B4 30 CD 21 BA   !ŠT☺Í!ŠT☻Í!´0Í!º
00000004B0:  A3 01 B4 09 CD 21 8A C3   E8 01 FF 8A C5 E8 FC FE   £☺´○Í!ŠÃè☺ÿŠÅèüþ
00000004C0:  8A C1 E8 F7 FE 32 C0 B4   4C CD 21                   ŠÁè÷þ2À´LÍ!
```

Рисунок 5 – lr1com.exe в шестнадцатеричном виде.

```
0000000000: 4D 5A D4 01 03 00 01 00   20 00 00 00 FF FF 00 00   MZÔ♥ ☺        ÿÿ
0000000010: 00 02 DC D6 55 00 2C 00   1E 00 00 00 01 00 56 00    ☻ÜÖU , ▲    ☺ V
0000000020: 2C 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ,
0000000030: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000040: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000050: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000060: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000070: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000080: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000090: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000000A0: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000000B0: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000000C0: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000000D0: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000000E0: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000000F0: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000100: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000110: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000120: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000130: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000140: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000150: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000160: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000170: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000180: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000190: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000001A0: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000001B0: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000001C0: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000001D0: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000001E0: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000001F0: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000200: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000210: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000220: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000230: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000240: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000250: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000260: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000270: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000280: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000290: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000002A0: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000002B0: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000002C0: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000002D0: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000002E0: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000002F0: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000300: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000310: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000320: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000330: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000340: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000350: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000360: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000370: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000380: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000390: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000003A0: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000003B0: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000003C0: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000003D0: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000003E0: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
00000003F0: 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00
0000000400: 49 42 4D 20 50 43 20 74   79 70 65 20 2D 20 24 50   IBM PC type - $P
0000000410: 43 0A 0D 24 50 43 2F 58   54 0A 0D 24 50 53 32 20   C♪$PC/XT☒♪$PS2
0000000420: 76 65 72 2E 20 33 30 0A   0D 24 50 53 32 20 76 65   ver. 30☒♪$PS2 ve
0000000430: 72 2E 20 35 30 2F 36 30   20 6F 72 20 41 54 0A 0D   r. 50/60 or AT☒♪
0000000440: 24 50 53 32 20 76 65 72   2E 20 38 30 0A 0D 24 50   $PS2 ver. 80☒♪$P
0000000450: 43 6A 72 0A 0D 24 50 43   20 43 6F 6E 76 65 72 74   Cjr☒♪$PC Convert
0000000460: 69 62 6C 65 0A 0D 24 59   6F 75 72 20 4D 53 44 4F   ible☒♪$Your MSDO
0000000470: 53 20 74 79 70 65 20 69   73 20 24 3C 32 2E 30 0A   S type is $<2.0☒
0000000480: 0D 24 30 78 2E 30 79 0A   0D 24 53 45 52 49 41 4C   ♪$0x.0y☒♪$SERIAL
0000000490: 20 4F 45 4D 20 6E 75 6D   62 65 72 20 69 73 20 24    OEM number is $
00000004A0: 0A 0D 53 45 52 49 41 4C   20 75 73 65 72 20 6E 75   ☒♪SERIAL user nu
00000004B0: 6D 62 65 72 20 69 73 20   24 00 00 00 00 00 00 00   mber is $
00000004C0: 51 52 E8 1C 00 8A EC 8A   3C 09 76 02 04 07 04 30   QRèL ŠìŠĐ ´θÍ!ŠÕ´
00000004D0: 02 CD 21 5A 59 C3 24 0F   θÍ!ZYÃ$¤<ov☒♦•♦0
00000004E0: C3 51 8A E0 E8 EF FF 86   C4 B1 04 D2 E8 E8 E6 FF   ÃQŠàèïÿ�†Ä±♦Òèèæÿ
00000004F0: 59 C3 51 52 32 E4 33 D2   B9 0A 00 F7 F1 80 CA 30   YÃQR2ä3Ò¹☒ ÷ñÊ0
0000000500: 88 14 4E 33 D2 3D 0A 00   73 F1 3C 00 74 04 0C 30   ˆ¶N3Ò=☒ sñ< t♦♀0
0000000510: 88 04 5A 59 C3 B8 20 00   8E D8 B8 00 F0 8E C0 26   ˆ♦ZYÃ¸  ŽØ¸ ðŽÀ&
0000000520: A0 FE FF BA 00 00 B4 09   C0 21 BA 0F 00 3C FF 74   þÿº    ´oÍ!º¤ <ÿt
0000000530: 31 BA 14 00 3C FE 74 2A   3C FB 74 26 BA 2A 00 3C   1º¶ <þt*<ût&º* <
0000000540: FC 74 1F BA 1C 00 3C FA   74 18 BA 41 00 3C F8 74   üt▼L <út↑ºA <øt
0000000550: 11 BA 4F 00 3C FD 74 0A   ◄ºO <ýt☒ºV <ùu è
0000000560: 5E FF B4 09 CD 21 BA 67   00 B4 09 CD 21 B4 30 CD   ^ÿ´oÍ!ºg ´oÍ! ´oÍ
0000000570: 21 3C 00 75 07 BA 7B 00   B4 09 CD 21 BE 82 00 83   !< u•º{ ´oÍ!¾‚ ƒ
0000000580: C6 01 E8 6D FF 83 C6 04   8A C4 E8 65 FF BA 82 00   Æ☺èmÿƒÆ♦ŠÄèeÿº‚
0000000590: B4 09 CD 21 B4 30 CD 21   BA 8A 00 B4 09 CD 21 8A   ´oÍ! ´oÍ!ºŠ ´oÍ!Š
00000005A0: C7 E8 4E FF 8A 14 B4 02   CD 21 8A 54 01 CD 21 8A   ÇèNÿŠ¶´θÍ!ŠTθÍ!Š
00000005B0: 54 02 CD 21 B4 30 CD 21   FE 8A C1 E8 F2 FE 32 C0   Tθ́Í! ´oÍ!º   ´oÍ!Š
00000005C0: C3 E8 FC FE 8A C5 E8 F7   FE 8A C1 E8 F2 FE 32 C0   ÃèüþŠÅè÷þŠÁèòþ2À
00000005D0: B4 4C CD 21                                         ´LÍ!
```

Рисунок 6 – lr1exe.exe в шестнадцатеричном виде.

Рассмотреть файлы модулей .com и .exe можно в отладчике.

Рисунок 7 – lr1com.com в td.exe отладчике.

Рисунок 8 – lr1exe.exe в td.exe отладчике.