

МИНОБРНАУКИ РОССИИ
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
“ЛЭТИ” ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)
Кафедра математического обеспечения и применения ЭВМ

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:CH – 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.

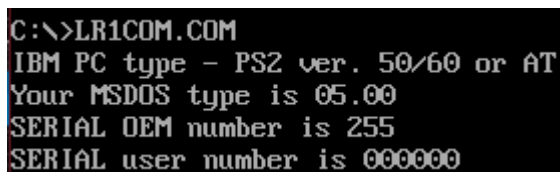
Далее необходимо отладить полученный исходный модуль и получить “хороший” .com модуль, а также необходимо построить “плохой” .exe, полученный из исходного текста для .com модуля.

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.



```
C:\>LR1COM.COM
IBM PC type - PS2 ver. 50/60 or AT
Your MSDOS type is 05.00
SERIAL OEM number is 255
SERIAL user number is 000000
```

Рисунок 1 - Результат работы lr1com.com

```
C:\>LR1COM.EXE

      00IBM PC type -

00IBM PC type -

      00IBM PC type - 5 0

pe -                                00IBM PC ty

                                00IBM PC type - 255

PC type - 000000                                00IBM
```

Рисунок 2 - Результат lr1com.exe

```
C:\>LR1EXE.EXE
IBM PC type - PS2 ver. 50/60 or AT
Your MSDOS type is 05.00
SERIAL OEM number is 255
SERIAL user number is 000000
```

Рисунок 3 - Результат работы lr1.exe.exe

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

0000000000: E9 0E 01 49 42 4D 20 50	43 20 74 79 70 65 20 2D	ÉIBM PC type
0000000010: 20 2A 50 43 0A 0D 24 50	43 2F 58 54 0A 0D 24 50	\$PC\$PC/XT\$
0000000020: 53 32 20 76 65 72 2E 20	33 30 0A 0D 24 50 53 32	S2 ver. 30\$PS
0000000030: 20 76 65 72 2E 20 35 30	2F 36 30 20 6F 72 20 41	ver. 50/60 or
0000000040: 54 0A 0D 24 50 53 32 30	76 65 72 2E 20 38 30 0A	T\$PS2 ver. 80
0000000050: 0D 24 50 43 6A 72 0A 0D	24 50 43 20 43 6F 6E 76	\$PCjr\$PC Con
0000000060: 65 72 74 69 62 6C 65 0A	0D 24 59 6F 75 72 20 4D	ertible\$Your M
0000000070: 53 44 4F 53 20 74 79 70	65 20 69 73 20 24 3C 32	SDOS type is <\$
0000000080: 2E 30 0A 0D 24 30 78 2E	30 79 0A 0D 24 53 45 52	.0\$0x.0y\$SE
0000000090: 49 41 4C 20 4F 45 4D 20	6E 75 6D 62 65 72 20 69	IAL OEM number
00000000A0: 73 20 24 0A 0D 53 45 52	49 41 4C 20 75 73 65 72	s \$SERIAL user
00000000B0: 20 6E 75 6D 62 65 72 20	69 73 20 24 51 52 E8 1C	number is \$QR
00000000C0: 00 8A EC 8A D0 B4 02 CD	21 8A D5 B4 02 CD 21 5A	ŠiŠ0'0iŠ0'0iŠ
00000000D0: 59 C3 24 0F 3C 09 76 02	04 07 04 30 C3 51 8A E0	Y\$soxov0+00AQŠ
00000000E0: E8 EF FF 86 C4 B1 04 D2	E8 E8 E6 FF 59 C3 51 52	eiŸtÄ+0deæŸŸAQ
00000000F0: 32 EF 33 D2 B9 0A 00 F7	F1 80 CA 30 88 14 4E 33	2ä30Š+ ñE0'JN
0000000100: D2 3D 0A 00 73 F1 3C 00	74 04 0C 30 88 04 5A 59	0= šn< t#0'Z
0000000110: C3 B8 00 F0 E8 0C 26 A0	FE FF BA 03 01 B4 09 CD	Ä, öŽÄ& pŸ♥0'o
0000000120: 21 BA 12 01 3C FF 74 31	BA 17 01 3C FE 74 2A 3C	lŸt0<Ÿt1Ÿt0<bt*
0000000130: FB 74 26 BA 2D 01 3C FF	74 1F BA 1F 01 3C FA 7A	üt&=0<ütŸŸ♥0'o
0000000140: 18 BA 44 01 3C F8 74 11	BA 52 01 3C FD 74 0A BA	†D0<0t+R0<Ÿt0'o
0000000150: 59 01 3C F9 75 00 E8 63	FF B4 09 CD 21 BA 6A 01	Ÿ0<üu èŸŸ'0iŸŸj
0000000160: B4 09 CD 21 B4 30 CD 21	3C 00 75 07 BA 7E 01 B4	'0iŸ'0iŸ< u=æ~0
0000000170: 09 CD 21 BE 85 01 83 C6	01 E8 72 FF 83 C6 04 8A	0iŸŸ.0of0æŸŸŸŸ&+
0000000180: C4 E8 6A FF BA 85 01 B4	09 CD 21 B4 30 CD 21 BA	ÄejŸŸ...0'0iŸ'0iŸŸ
0000000190: 8D 01 B4 09 CD 21 8A C7	E8 53 FF 8A 14 B4 02 CD	00'0iŸŠčesŸŸŸŸŸŸŸ
00000001A0: 21 8A 54 01 CD 21 8A 54	02 CD 21 B4 30 CD 21 BA	lŠt0iŸŠt0iŸ'0iŸŸ
00000001B0: A3 01 B4 09 CD 21 8A C3	E8 01 FF 8A C5 E8 FC FE	Ÿ0'0iŸŠÄeŸŸŠÄeŸŸŸ
00000001C0: 8A C1 E8 F7 FE 32 C0 B4	4C CD 21	ŠÄe=þ2Ä'ŸŸŸŸŸŸŸ

Рисунок 4 – lr1com.com в шестнадцатеричном виде.

0000000000: 4D 5A CB 06 03 00 00 00 00	20 00 00 00 FF FF 00 00 MZE ♥ yy
0000000010: 00 00 A4 0F 00 01 00 00 00	1E 00 00 00 01 00 00 00 Re @ ▲ 0
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
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 éIBM 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 type. 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 7E \$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 \$<
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 \$QR&
00000003C0: 00 8A EC 8A 0D B4 02 CD	21 8A D5 B4 02 CD 21 5A ŠiŠD o'iŠD o'iLZ
00000003D0: 59 C3 24 0F 3C 09 76 02	0A 07 0A 30 C3 51 8A E YÄ\$<ov0\$+0AQŠ
00000003E0: E8 EF FF 86 C4 B1 04 D2	E8 E8 E6 FF 59 C3 51 52 ëÿtÄ+0ëëÿYAQR
00000003F0: 32 E4 33 D2 B9 0A 00 F7	F1 80 CA 30 88 14 4E 33 2ä30\$ ÷ñë0'0N3
0000000400: D2 3D 0A 00 73 F1 3C 00	74 04 0C 30 88 04 5A 5D ð= sñ< t00'0ZY
0000000410: C3 B8 00 F0 8E 0C 26 A0	FE FF BA 03 01 B4 09 CD Ä. äZ& þÿ0'0f
0000000420: 21 BA 12 01 3C FF 74 31	BA 17 01 3C FE 74 2A 3C !00<y't100<pt*<
0000000430: FB 74 26 BA 2D 01 3C FC	74 1F BA 1F 01 3C FA 74 üt00<0<üt0'0<üt
0000000440: 18 BA 44 01 3C F8 74 11	BA 52 01 3C FD 74 0A BA üD0<0t0'0R0<y't00
0000000450: 59 01 3C F9 75 00 E8 63	FF B4 09 CD 21 BA 6A 01 Y0küu ëcÿ'o'i!0j0
0000000460: B4 09 CD 21 B4 30 CD 21	3C 00 75 07 BA 7E 01 B4 'o'i!'0'i!< u00<0'
0000000470: 09 CD 21 BE 85 01 83 C6	01 E8 72 FF 83 C6 04 8A o'i!%0f0ëÿÿf0Š
0000000480: CA E8 6A FF BA 85 01 B4	09 CD 21 B4 30 CD 21 BA Äëÿÿ00'o'i! o'i!0
0000000490: 8D 01 B4 09 CD 21 8A C7	E8 53 FF 8A 14 B4 02 CD 00'o'i!ŠcäÿŠÿ0i
00000004A0: 21 8A 54 01 CD 21 8A 54	02 CD 21 B4 30 CD 21 BA !ŠtëiŠtëi! o'i!0
00000004B0: A3 01 B4 09 CD 21 8A C3	E8 01 FF 8A C5 E8 FC FE ë0'o'i!ŠÄëÿŠÄëÿ
00000004C0: 8A C1 E8 F7 FE 32 0C B4	4C CD 21 ŠÄëÿb2Ä'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	MZ00 00 00 00 00 00 00 00
0000000010: 00 02 DC D6 55 00 2C 00	1E 00 00 00 01 00 56 00	0000 00 00 00 00 00 00 00
0000000020: 2C 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000030: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000040: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000050: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000060: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000070: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000080: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000090: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000000A0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000000B0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000000C0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000000D0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000000E0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000000F0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000100: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000110: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000120: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000130: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000140: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000150: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000160: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000170: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000180: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000190: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000001A0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000001B0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000001C0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000001D0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000001E0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000001F0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000200: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000210: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000220: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000230: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000240: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000250: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000260: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000270: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000280: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000290: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000002A0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000002B0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000002C0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000002D0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000002E0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000002F0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000300: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000310: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000320: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000330: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000340: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000350: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000360: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000370: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000380: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
0000000390: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000003A0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000003B0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000003C0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000003D0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000003E0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 00 00 00 00 00 00 00
00000003F0: 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0000 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	CM\$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	D0 B4 02 CD 21 8A D5 B4	QReL \$iSD `oiIS0`
00000004D0: 02 CD 21 5A 59 C3 24 0F	3C 09 76 02 04 07 04 30	0iIZYA\$<ov0\$0
00000004E0: C3 51 8A E0 E8 EF FF 86	C4 B1 04 D2 E8 E8 E6 FF	AQSaaiYtA±00eey
00000004F0: 59 C3 51 52 32 E4 33 D2	B9 0A 00 F7 F1 80 CA 30	YQR2A30±\$ ÷n€E0
0000000500: 88 14 4E 33 D2 3D 0A 00	73 F1 3C 00 74 04 0C 30	`gN30=\$ sn< t+q0
0000000510: 88 04 5A 59 C3 B8 20 00	8E D8 B8 00 F0 8E C0 26	`+ZYA. Ž0. dŽA&
0000000520: A0 FE FF BA 00 00 B4 09	CD 21 BA 0F 00 3C FF 74	bÿa `oi!o<ÿt
0000000530: 31 BA 14 00 3C FE 74 2A	3C FB 74 26 BA 2A 00 3C	1\$g <pt*<ut&* <
0000000540: FC 74 1F BA 1C 00 3C FA	74 18 BA 41 00 3C F8 74	ÿt\$0L <ut†A <øt
0000000550: 11 BA 4F 00 3C FD 74 0A	BA 56 00 3C F9 75 00 E8	→00 <ÿt\$0V <uu è
0000000560: 5E FF B4 09 CD 21 BA 67	00 B4 09 CD 21 B4 30 CD	^ÿ`oi!eg `oi!`0i
0000000570: 21 3C 00 75 07 BA 7B 00	B4 09 CD 21 BE 82 00 83	!< u+0{ `oi!%, f
0000000580: C6 01 E8 6D FF 83 C6 04	8A C4 E8 65 FF BA 82 00	A0emÿfA+SÀeey0,
0000000590: B4 09 CD 21 B4 30 CD 21	BA 8A 00 B4 09 CD 21 8A	`oi!`oi!0\$ `oi!\$
00000005A0: C7 E8 4E FF 8A 14 B4 02	CD 21 8A 54 01 CD 21 8A	CaNy\$g`oi!Stoi!\$
00000005B0: 54 02 CD 21 B4 30 CD 21	BA A0 00 B4 09 CD 21 8A	T0i!`oi!0 `oi!\$
00000005C0: C3 E8 FC FE 8A C5 E8 F7	FE 8A C1 E8 F2 FE 32 C0	Aeüp\$Ae±p\$Aeöp2A
00000005D0: B4 4C CD 21		`Li!

Рисунок 6 – lr1exe.exe в шестнадцатеричном виде.

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

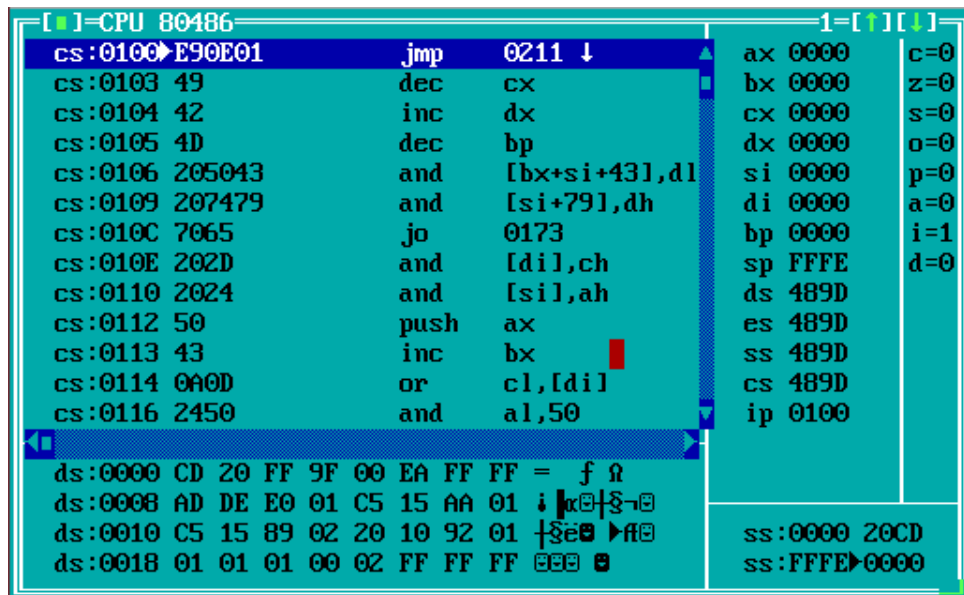


Рисунок 7 – lrlcom.com в td.exe отладчике.

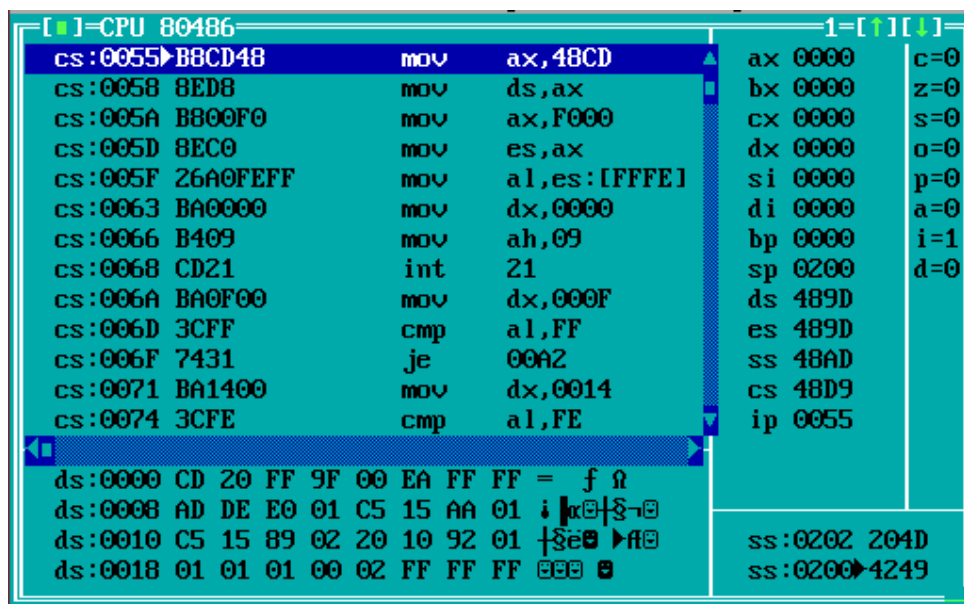


Рисунок 8 – lrl.exe в td.exe отладчике.

Контрольные вопросы.

Отличие исходных текстов com и exe программ:

1. Сколько сегментов должна содержать com-программа?

Представляет собой один сегмент и его размер не превышает 64кб памяти, ровно как размер одного сегмента.

2. ... exe-программа

Сама exe-программа на уровень сложнее com-программы ввиду того, что может содержать несколько сегментов: сегмент кода, сегмент стека, и несколько сегментов данных.

3. Какие директивы должны обязательно быть в тексте com-программы?

Assume для установления соответствующих сегментных регистров. Org 100h для установки смещения в psp, то есть резервирует память под psp.

4. Все ли форматы команд можно использовать в com-программе.

В .com программе нет таблицы настроек, поэтому загрузчик файла не сможет настроить адреса сегментов. В виду чего нельзя будет использовать команды такого формата.

Отличие форматов файлов com и exe модулей:

1. Какова структура файла com? С какого адреса располагается код?

Располагается по адресу 0h и состоит из одного сегмента.

2. Какова структура файла “плохого” exe? С какого адреса располагается код? Что располагается с адреса 0?

“Плохой” exe состоит из одного сегмента. Сам код начинается с адреса 300h, а перед ним идет заголовок файла, включающий в себя сигнатуру файла, число элементов и адрес таблицы настроек адресов, длину заголовка. Сама таблицы настроек состоит из длинных указателей вида смещение:сегмент на слова в загрузочном модуле, которые содержат настраиваемые сегментные адреса.

3. Какова структура файла “хорошего” exe? Чем он отличается от файла “плохого” exe?

“Хороший” ехе теперь имеет три сегмента. Код смещен на величину 100h, то есть размер сегмента стека, и теперь расположен по адресу 0400h.

Загрузка com модуля в основную память:

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

Код расположен с адреса 100h, так как перед ним расположен psp такого размера.

2. Что располагается с адреса 0h?

Psp, так как мы в начале программы выделяем под него память.

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

Значение регистров можно посмотреть в TD отладчике. Регистры указывают на адреса 489Dh.

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

Стек расположен в конце основного сегмента. SP указывает на FFFEh, а в самом стеке лежит адрес возврата(0000h).

Загрузка “хорошего” ехе модуля в основную память:

1. Как загружается “хороший” ехе? Какие значения имеют сегментные регистры?

SS - начало стека, DS - начало psp, CS - сегмент кода соответственно. SS = 0200h, DS = 489Dh, CS = 48D9h, ES = 489Dh.

2. На что указывают регистры DS и ES?

Оба имеют значение 489Dh и указывают на psp.

3. Как определяется стек?

При использовании директивы assume значению ss присваивается значение начала сегмента стека.

4. Как определяется точка входа?

Ехе-программа может содержать несколько функций, и ,чтобы определить, с какой должна начать выполняться работа, применяется

директива END func, где func - метка, с которой программа должна начинать работу.

Выводы.

В ходе работы были получены навыки по созданию и работе с com и exe файлами. Были реализованы программы, определяющие тип РС, а также версию системы.