**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**

|  |  |  |
| --- | --- | --- |
| Студентка гр. 6381 |  | Вероха В. Н. |
| Преподаватель |  | Губкин А. Ф. |

Санкт-Петербург

2018

**Постановка задачи**

1. Цель работы:

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

1. Описание функций:

|  |  |
| --- | --- |
| Название | Назначение |
| TETR\_TO\_HEX | перевод половины байта в 16-ую систему счисления |
| BYTE\_TO\_HEX | перевод байта регистра AL в 16-ую систему счисления в AX |
| WRD\_TO\_HEX | перевод двух байт регистра AX в 16-ую систему счисления в DI |
| BYTE\_TO\_DEC | перевод байта регистра AL в 10-ую систему счисления, помещая результат в SI |
| PC\_INFO | определяет тип IBM PC |
| SYSTEM\_INFO | определяет версию MS DOS |
| OEM\_INFO | определяет серийный номер OEM |
| USER\_INFO | определяет серийный номер пользователя |
| Write\_msg | вывод на экран |

1. Описание данных:

|  |  |
| --- | --- |
| Наименование | Назначение |
| TYPE\_PC | Тип IBM PC |
| SYS\_VER | Версия системы |
| OEM\_NUM | Номер OEM |
| USER\_NUM | Серийный номер пользователя |

1. Общие сведения:

Тип IBM PC хранится в байте по адресу 0F000:0FFFE, 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;

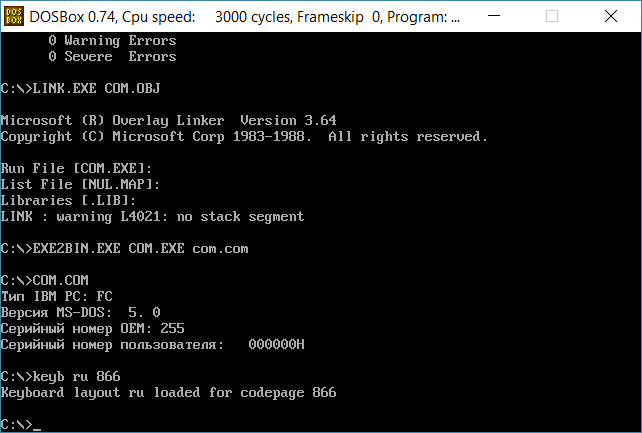
BH – серийный номер OEM (Original Equipment Manufacturer);

BL: CX – 24-битовый серийный номер пользователя.

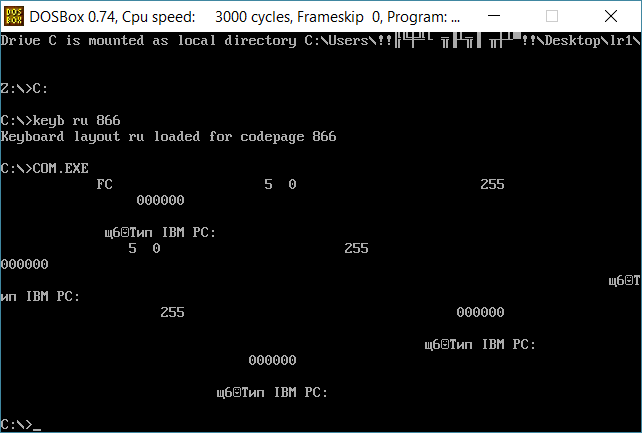
**Ход работы**

Шаг 1.

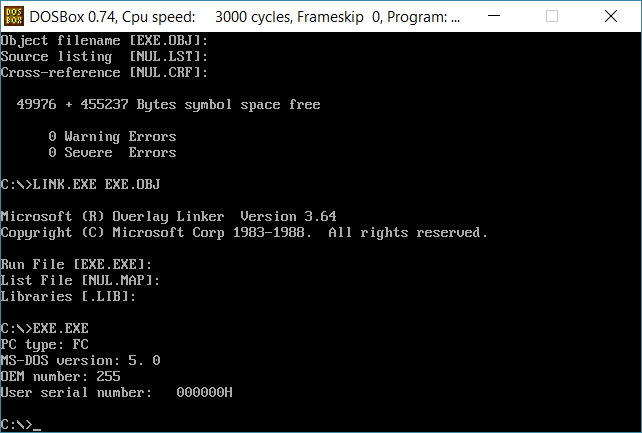
Запуск «хорошего» .COM модуля:



Запуск «плохого» .EXE модуля:



Шаг 2. Запуск «хорошего» .EXE модуля:



Шаг 3. Ответы на контрольные вопросы.

Отличия исходных текстов COM и EXE программ:

1. *Сколько сегментов должна содержать COM-программа?*

COM-программа может содержать только один сегмент (сегмент кода).

1. *EXE программа?*

EXE-программа может содержать более одного сегмента. В таких программах могут быть сегменты и для кода, и для данных, и для стека.

1. *Какие директивы должны обязательно быть в тексте COM- программы?*

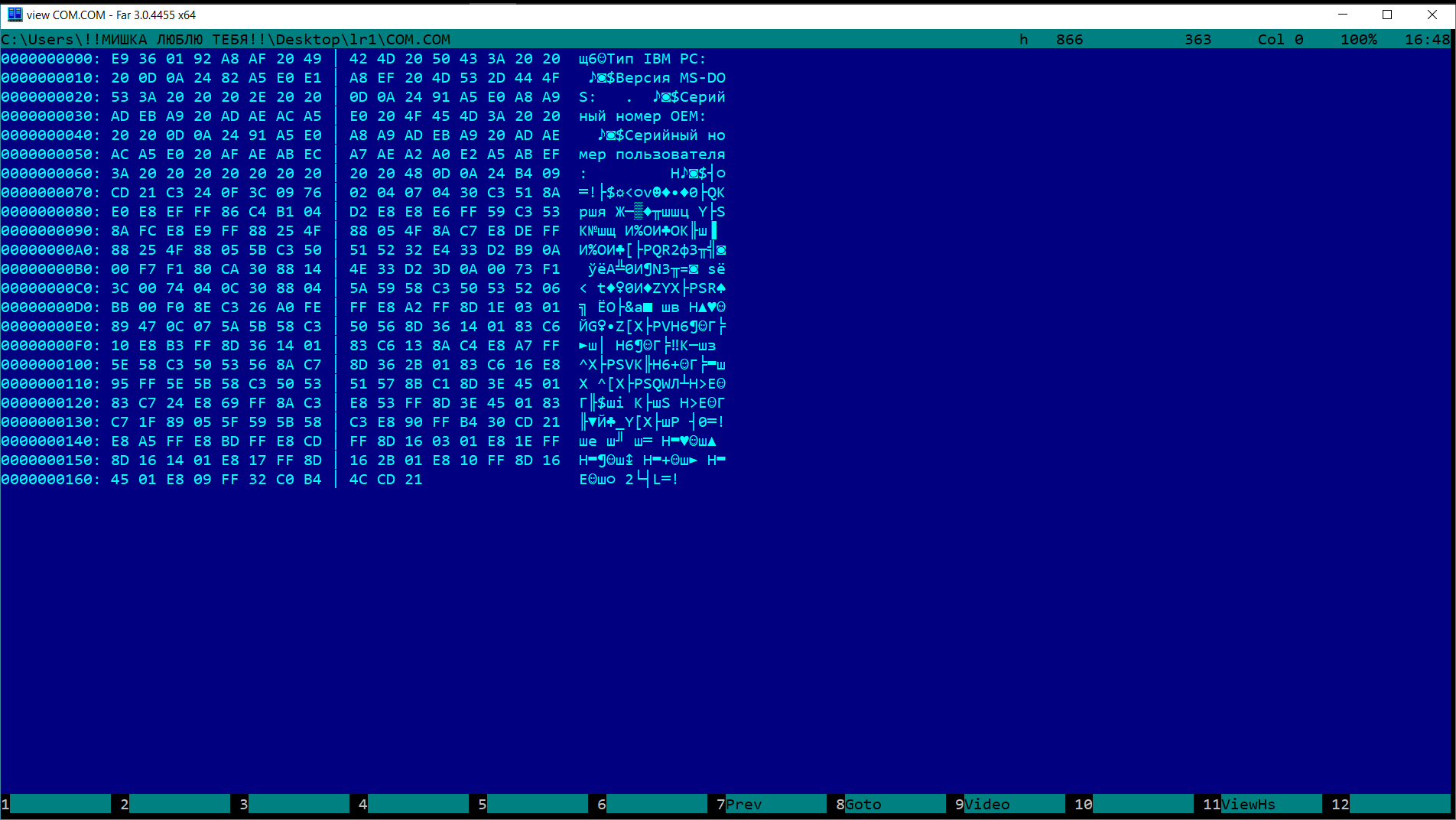
В тексте COM-программы должна обязательно быть директива ORG 100h (смещение 100h), так как при загрузке СОМ файла в память DOS занимает первые 256 байт (100h) блоком данных PSP, после него располагает код программы.

1. *Все ли форматы команд можно использовать в COM-программе?*

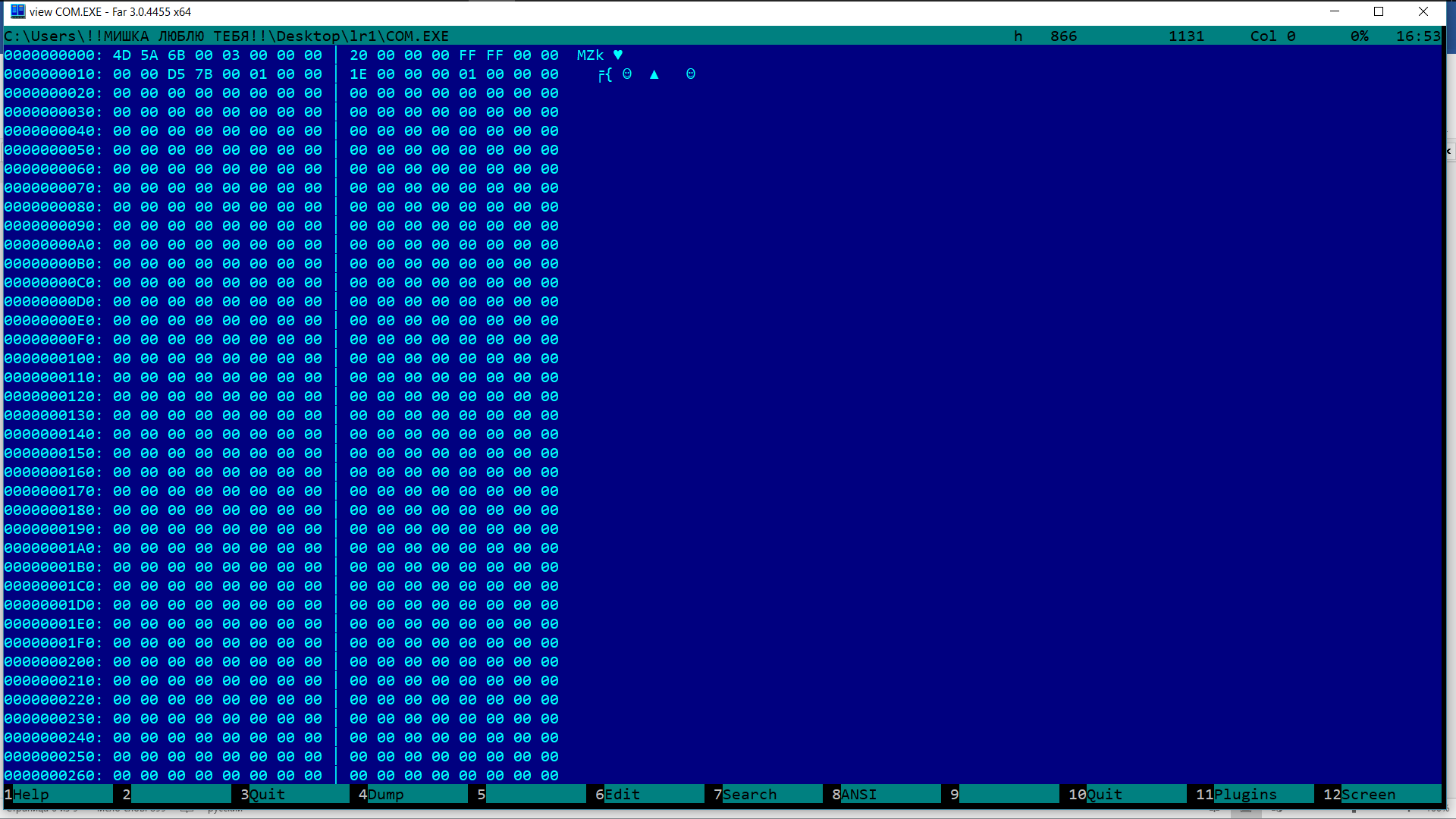
Нельзя использовать команды, связанные с адресом сегмента, ибо до загрузки адрес сегмента неизвестен (так как в COM-программе не содержится таблица настроек (Relocation Table), которая содержит описание адресов, зависящих от размещения загрузочного модуля в ОП, поскольку подобные адреса в нем запрещены), поэтому загрузчик не сможет его определить. Также нельзя использовать оператор far: переход на метку возможен только в результате межсегментной передачи управления, а в COM-файле только один сегмент, следовательно, такие переходы невозможны.

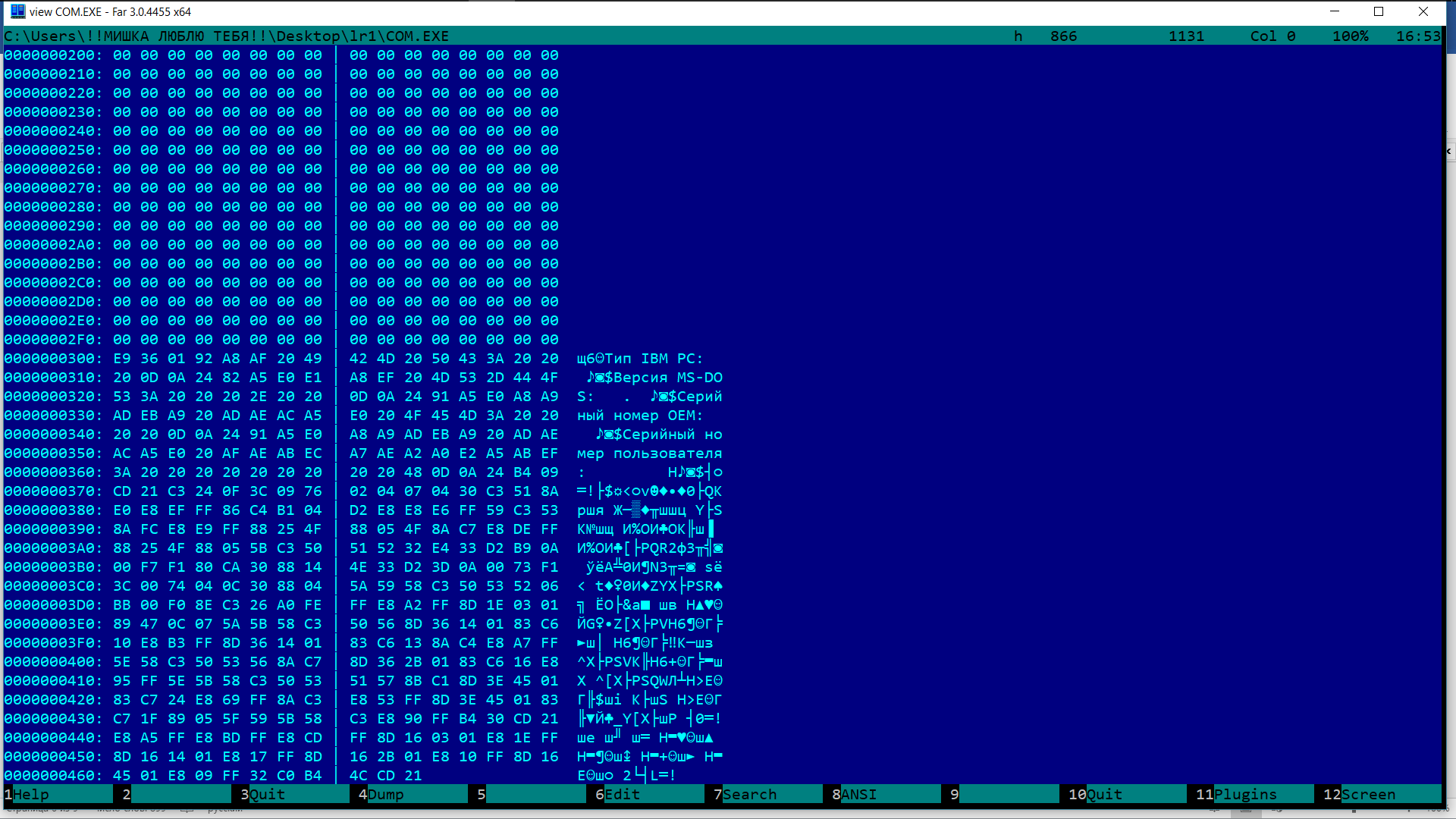
Шаг 4.

COM-модуль в 16-ричном виде:

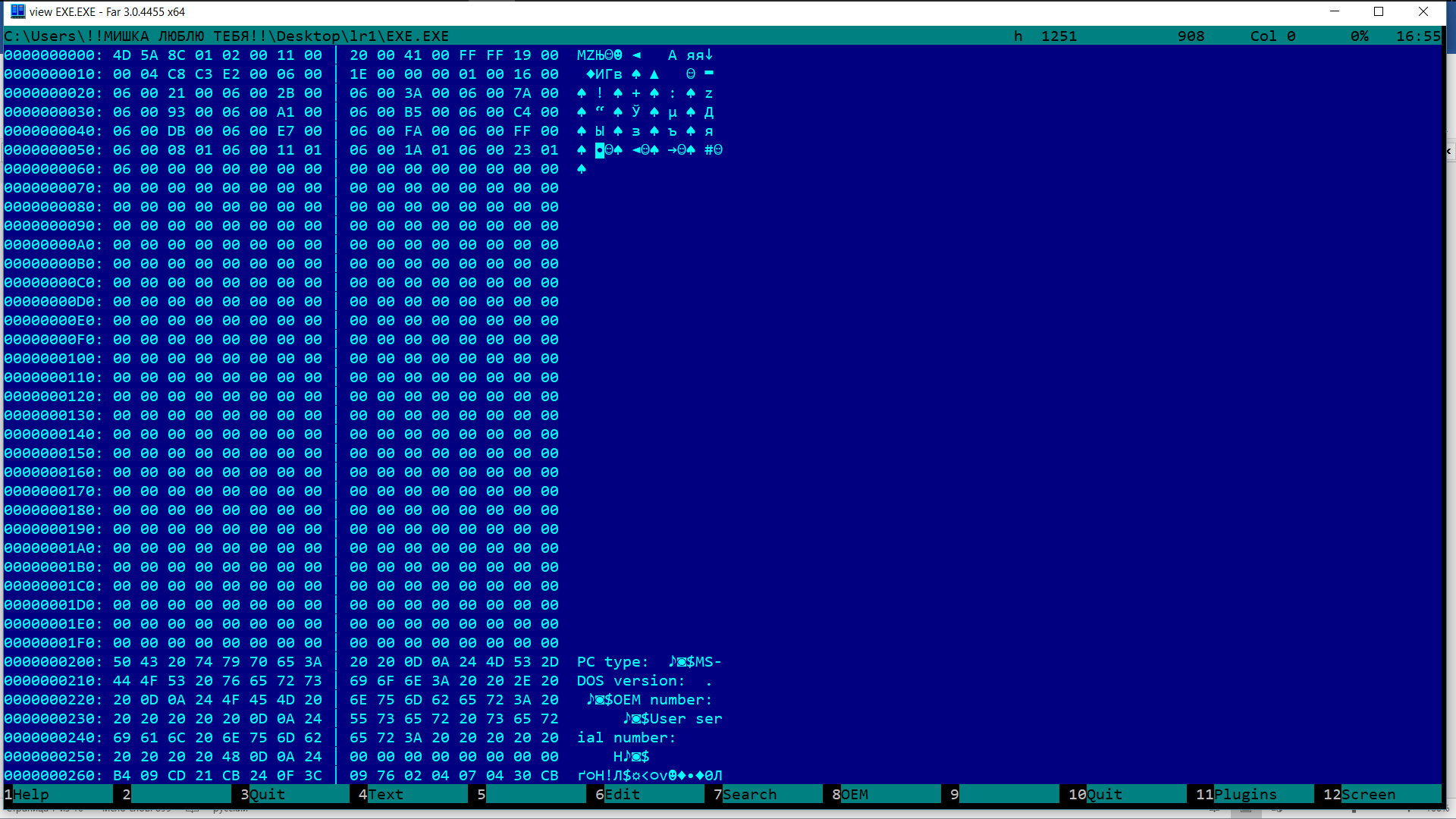


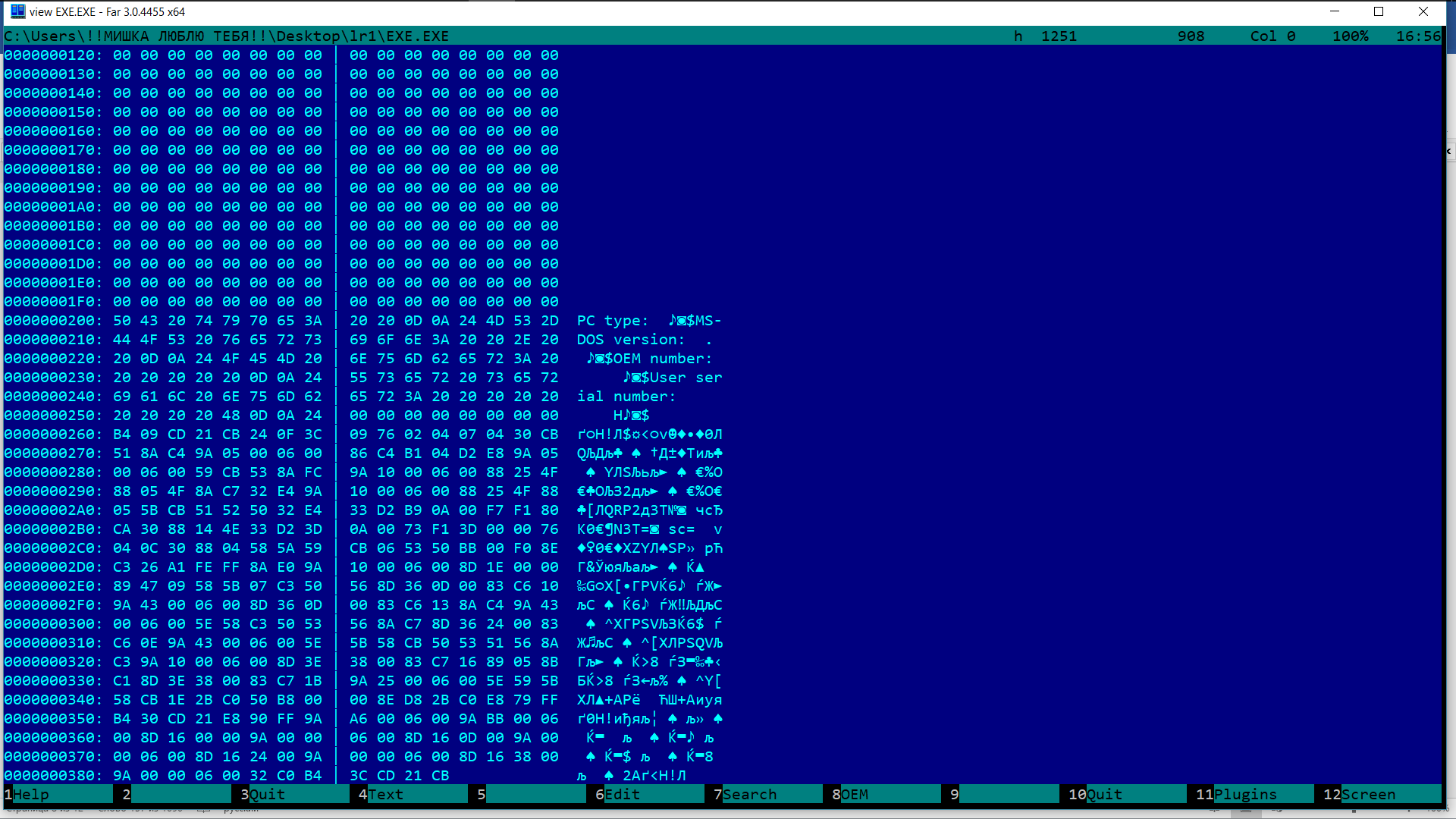
«Плохой» .EXE модуль в 16-ричном виде:





«Хороший» .EXE модуль в 16-ричном виде:





Ответы на контрольные вопросы.

Отличия форматов файлов COM и EXE программ:

1. *Какова структура файла COM? С какого адреса располагается код?*

COM-файл состоит из команд, процедур и данных, используемых в программе. Код начинается с адреса 0h, но при загрузке модуля устанавливается смещение в 100h.

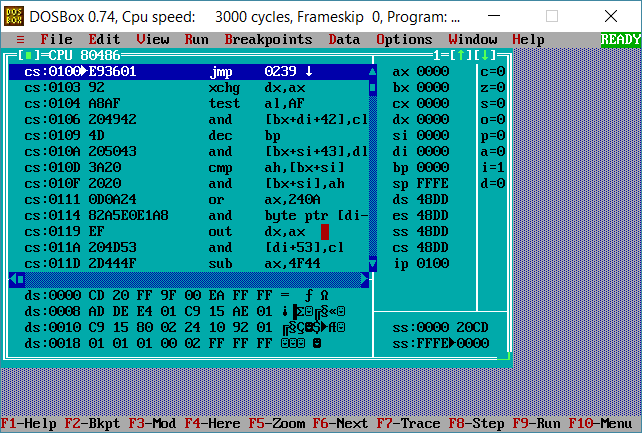
1. *Какова структура файла «плохого» EXE? С какого адреса располагается код? Что располагается с 0 адреса?*

В «плохом» EXE файле данные и код располагаются в одном сегменте. С адреса 0h располагается Relocation Table (таблица разметки), а код - с адреса 300h.

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

В «хорошем» файле EXE содержится информация для загрузчика, сегмент стека, сегмент данных и сегмент кода, то есть 3 сегмента в отличии от одного в «плохом».EXE. Код располагается с адреса 200h, а не с 300h.

Шаг 5. Загрузка COM модуля в основную память.



Ответы на контрольные вопросы.

Загрузка COM модуля в основную память:

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

После загрузки COM-программы в память сегментные регистры указывают на начало PSP. Код располагается с адреса 100h.

1. *Что располагается с 0 адреса?*

С нулевого адреса располагается заголовок PSP.

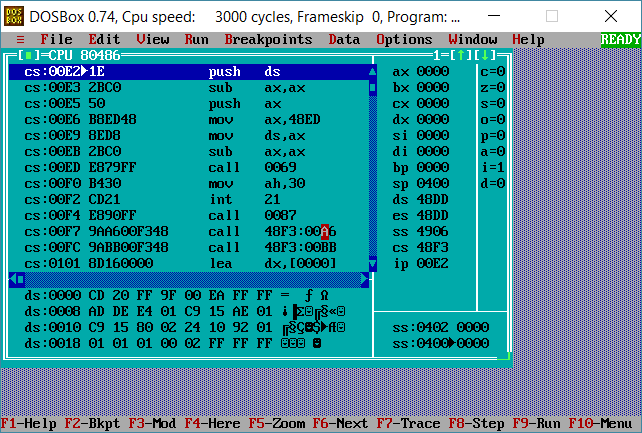
1. *Какие значения имеют сегментные регистры? На какие области памяти они указывают?*

48DD. Они указывают на начало PSP.

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

Стек определяется автоматически, указатель стека устанавливается на конец сегмента. Если для программы размер сегмента в 64КБ является достаточным, то DOS устанавливает в регистре SP адрес конца сегмента – FFFEh. Если 64К байтовый сегмент не имеет достаточно места для стека, то DOS устанавливает стек в конце памяти. Адреса расположены в диапазоне 0000h-FFFEh.

Шаг 6. Загрузка «хорошего» EXE модуля в память.



Ответы на контрольные вопросы.

Загрузка «хорошего» EXE модуля в память:

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

В области памяти строится PSP, считывается стандартная часть заголовка в память, определяется длина тела загрузочного модуля, начальный сегмент, загрузочный модуль считывается в начальный сегмент, таблица настройки считывается в рабочую память, определяются значения сегментных регистров. DS и ES устанавливаются на начало PSP, SS - на начало стека, CS - на начало сегмента кода.

1. *На что указывают регистры DS и ES?*

Изначально DS и ES указывают на начало PSP.

1. *Как определяется стек?*

Регистры SS и SP принимают значения, указанные в заголовке, потом к SS прибавляется сегментный адрес начального сегмента.

1. *Как определяется точка входа?*

Смещение точки входа в программу загружается в указатель команд IP. IP, а именно адрес, с которого начинается выполнение программы, определяется операндом директивы END, который называется точкой входа.

**Заключение:**

В ходе работы было проведено исследование различий в структурах исходных текстов модулей .COM и .EXE, структур файлов загрузочных модулей и способов их загрузки в основную память.