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. 9382 _____ Сорочина М.В.

Преподаватель _____ Ефремов М.А.

Санкт-Петербург

2021

Цель.

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

Сведения, использованные для составления программы.

Тип IBM PC хранится в байте по адресу 0F000:0FFFEh, в предпоследнем байте ROM BIOS. Соответствие кода и типа представлены в табл. 1.

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

Табл. 1

Для определения версии MS DOS существует функция 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
- BL:CX - 24-битовый серийный номер пользователя.

Ход работы.

На основе шаблона был написан текст исходного .COM модуля, который определяет тип PC, версию системы, серийный номер OEM и серийный номер пользователя и выводит эту информацию на экран. Таким образом были получены “плохой” EXE и “хороший” COM модули.

На основе текста исходного COM модуля был написан текст исходного EXE модуля, выполняющего те же функции. Так был получен “хороший” EXE модуль.

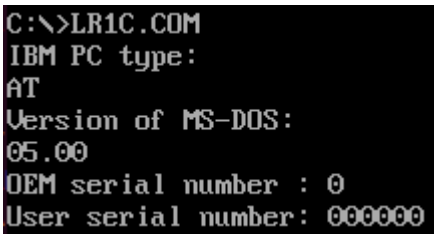

Рис. 1. Вывод COM модуля

Рис. 2. Вывод “плохого” EXE модуля

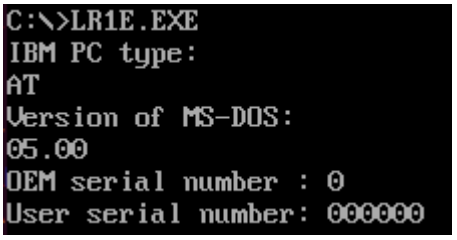

Рис. 3. Вывод “хорошего” EXE модуля.

Ответы на контрольные вопросы.

Отличия исходных текстов COM и EXE программ

1. Сколько сегментов должна содержать COM-программа?

COM-программа должна содержать 1 сегмент.

2. Сколько сегментов должна содержать EXE-программа?

Не менее одного.

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

org 100h и assume

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

Нельзя использовать команды вида mov *регистр*, seg *имя сегмента*, тк в COM- программе в отличие от EXE нет таблицы настроек, содержащей описание необходимого адреса, зависящего от размещения модуля в памяти.

Отличия форматов файлов COM и EXE модулей

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

Файл COM содержит 1 сегмент. Код располагается с 0.

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

В плохом exe стек, данные и код в одном сегменте.

Данные располагаются с адреса 300h (видно на рис. 4). До данных располагается управляющая информация и 100h, выделенные командой org 100h.

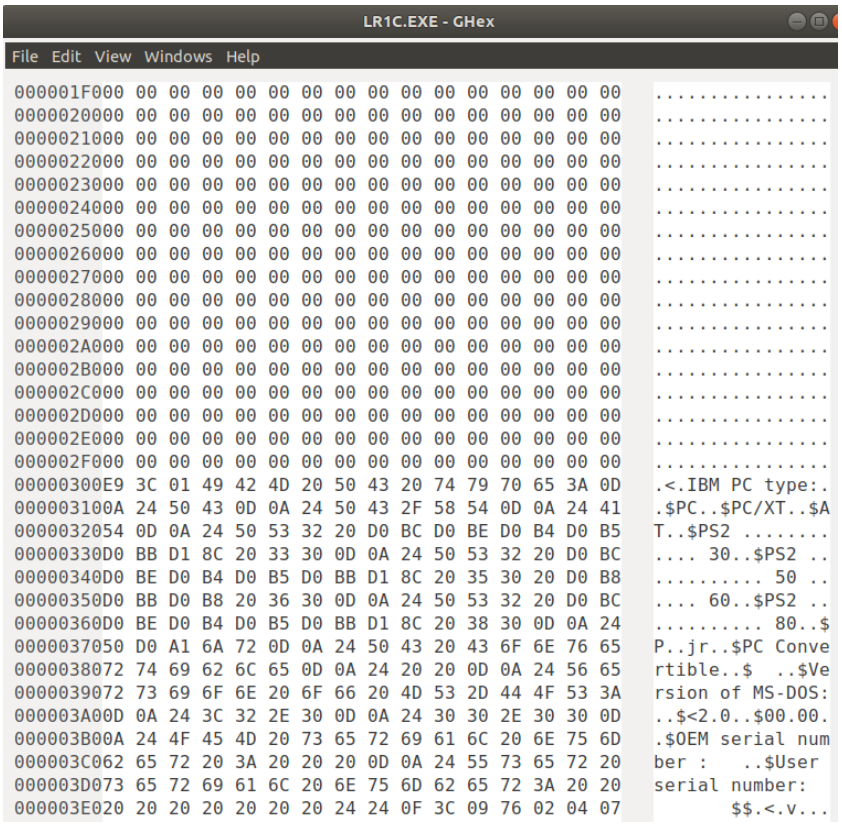

рис. 4. “плохой” exe в шестнадцатеричном виде

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

В хорошем exe, в отличие от плохого, есть 3 сегмента - стек, код и данные. Данные располагаются с адреса 400h. До данных располагаются управляющая информация и стек, под который выделено 200h.

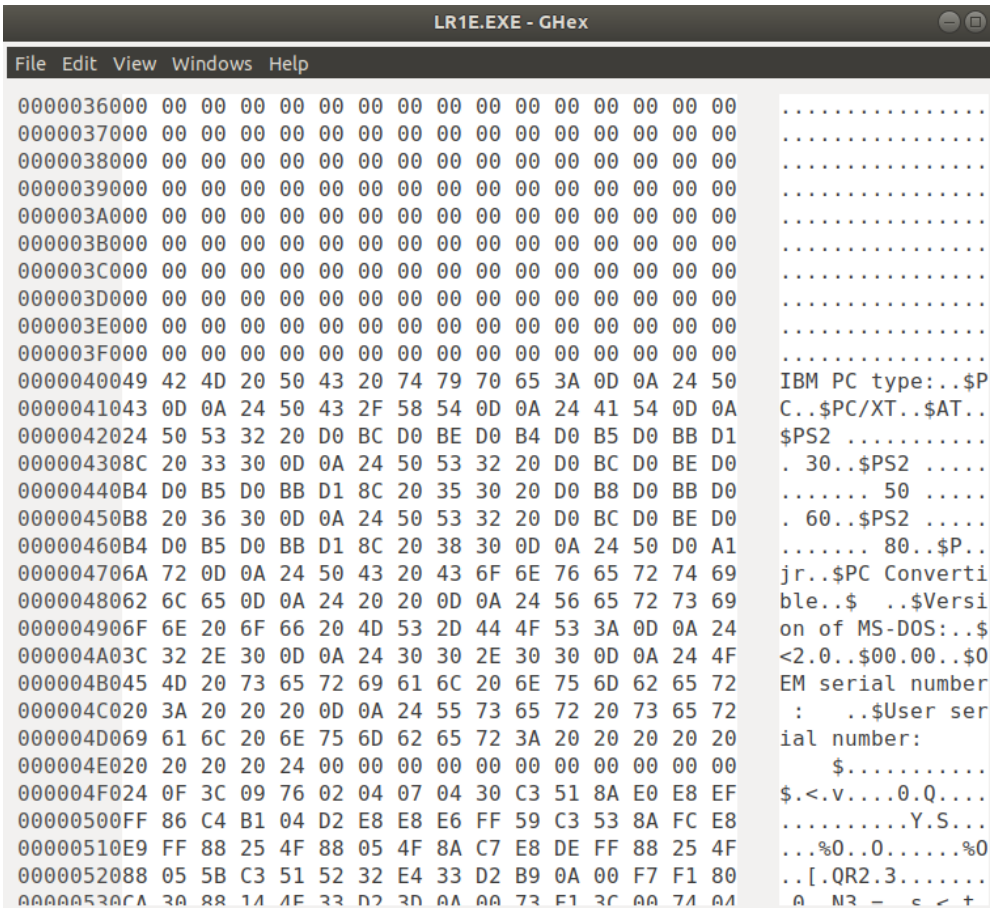

рис. 5.”хороший” exe в шестнадцатеричном виде

Загрузка COM модуля в основную память.

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

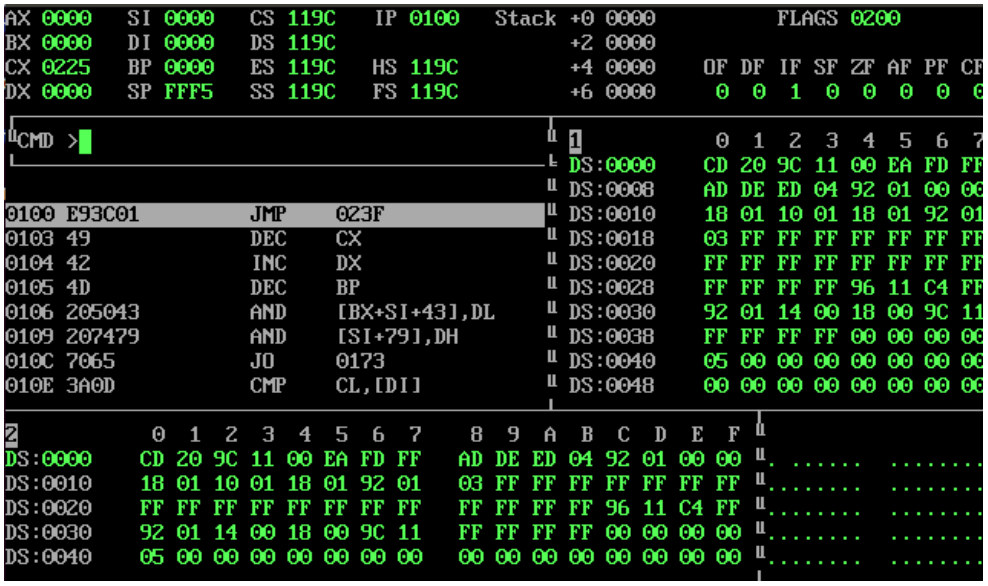

рис. 6. Запуск COM файла при помощи afd

Как можно заметить по рис. 6 при запуске COM программы, код располагается с адреса 100h, ip имеет значение 100h, а сегментные регистры указывают на начало PSP.

2. Что располагается с адреса 0?

PSP

3. Какие значения имеют сегментные регистры?

Сегментные регистры имеют одинаковое значение (119C)

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

Стек определяется автоматически и занимает свободную от PSP и кода память. Его адреса идут от больших к меньшим

Загрузка “хорошего” EXE модуля в основную память.

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

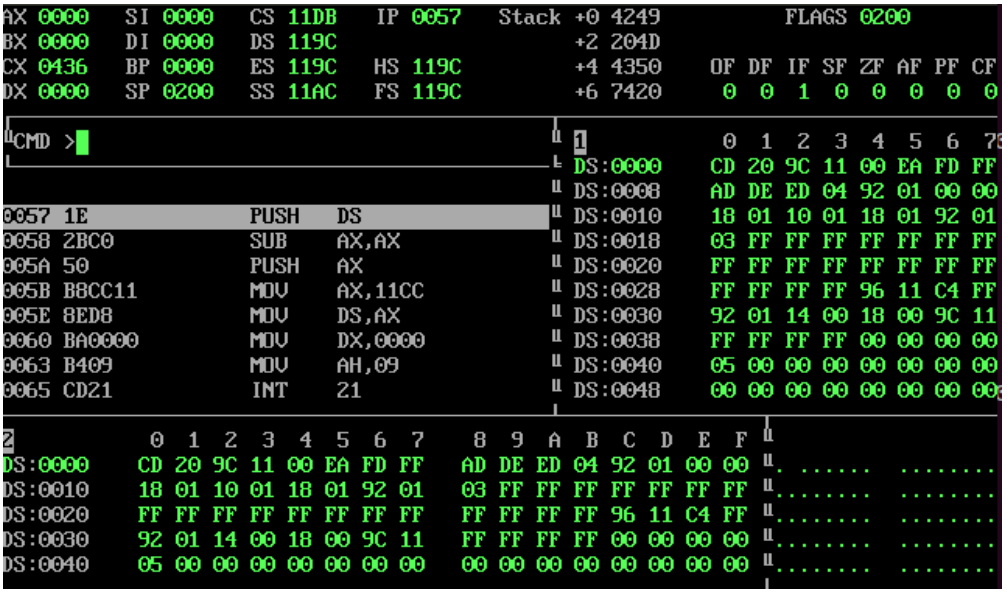

рис. 7. Запуск EXE файла при помощи afd

Как можно заметить по рис. 7 при запуске exe программы, DS и ES равны 119C (начало PSP), CS равен 11DB.

2. На что указывают регистры DS и ES?

На начало PSP.

3. Как определяется стек?

При помощи директив SEGMENT и ASSUME.

4. Как определяется точка входа?

Директивой END, после нее пишется точка входа

Выводы.

В ходе выполнения данной работы были изучены COM и EXE файлы и их ключевые отличия.