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

Студент гр. 9381 _____ Аухадиев А.А.

Преподаватель _____ Ефремов М.А.

Санкт-Петербург

2021

Цель работы.

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

Функции и структуры данных.

Название	Назначение
TETR_TO_HEX	Перевод 4-х младших битов AL в цифру 16 с/с, представление в виде символа и запись в AL
BYTE_TO_HEX	Байт в AL переводится в два символа шестн. числа в AX
WRD_TO_HEX	Перевод в 16 с/с 16-ти разрядного числа в AX число, DI - адрес последнего символа
BYTE_TO_DEC	Перевод в 10 с/с, SI - адрес поля младшей цифры
PRINT_MESSAGE	Вывод строки на экран (функция 09h)
BEGIN	Поиск всей необходимой информации о компьютере, её обработка и вывод на экран с помощью функций выше

Последовательность действий программы.

Вызов процедуры BEGIN, которая находит и выводит на экран тип PC, серийные номера OEM и пользователя, версию ОС. Для получения необходимых данных используется информация из последнего байта ROM BIOS по адресу 0F000:0FFFEh для получения типа ПК, а также функция 30h прерывания 21h.

Выполнение работы.

1. Написание текста исходного .COM модуля lab_com.asm, его компиляция в "плохой" .EXE модуль lab_com.exe. При помощи EXE2BIN.EXE по плохому .EXE модулю был построен хороший .COM модуль lab_com.com.

2. Создание .EXE модуля lab_exe.asm, его компиляция в хороший .EXE модуль lab_exe.exe.

3. Сравнение исходных текстов lab_com.asm и lab_exe.asm.

4. Сравнение загрузочных модулей с помощью программы hexyl.

5. Исследование загрузочных модулей .COM и .EXE при помощи отладчика AFD.

Ответы на контрольные вопросы.

I. Отличия исходных текстов COM и EXE программ

1) Сколько сегментов должна содержать COM-программа?

Ответ: один сегмент

2) EXE-программа?

Ответ: Один и более сегментов

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

Ответ:

1. Директива ORG 100h, которая задаёт смещение адресации в 256 байт от нулевого адреса для PSP.

2. Директива ASSUME необходима для проверки допустимости каждого обращения к именованной ячейке памяти с учётом значения текущего сегментного регистра.

3. Директива END, по метке которой определяется первая команда программы.

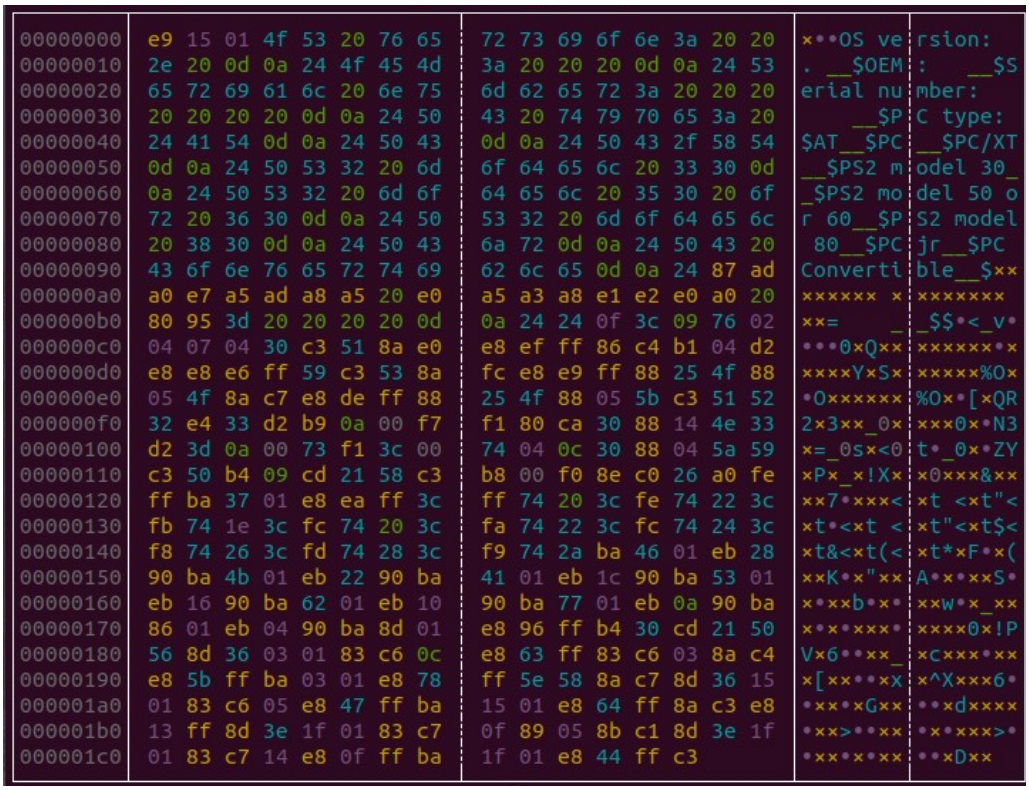
4) Все ли форматы команд можно использовать в COM-программе?

Ответ: Невозможно использование команд вида mov <регистр>, seg <имя сегмента>, так как в COM-программе отсутствует таблица настройки, содержащая описание адресов, зависящих от размещения загрузочного модуля в оперативной памяти. Таким образом, адрес сегмента COM-файла до загрузки неизвестен, в отличие от EXE-файлов, у которых все адреса прописаны в таблице нстроек.

II. Отличие форматов COM и EXE программ

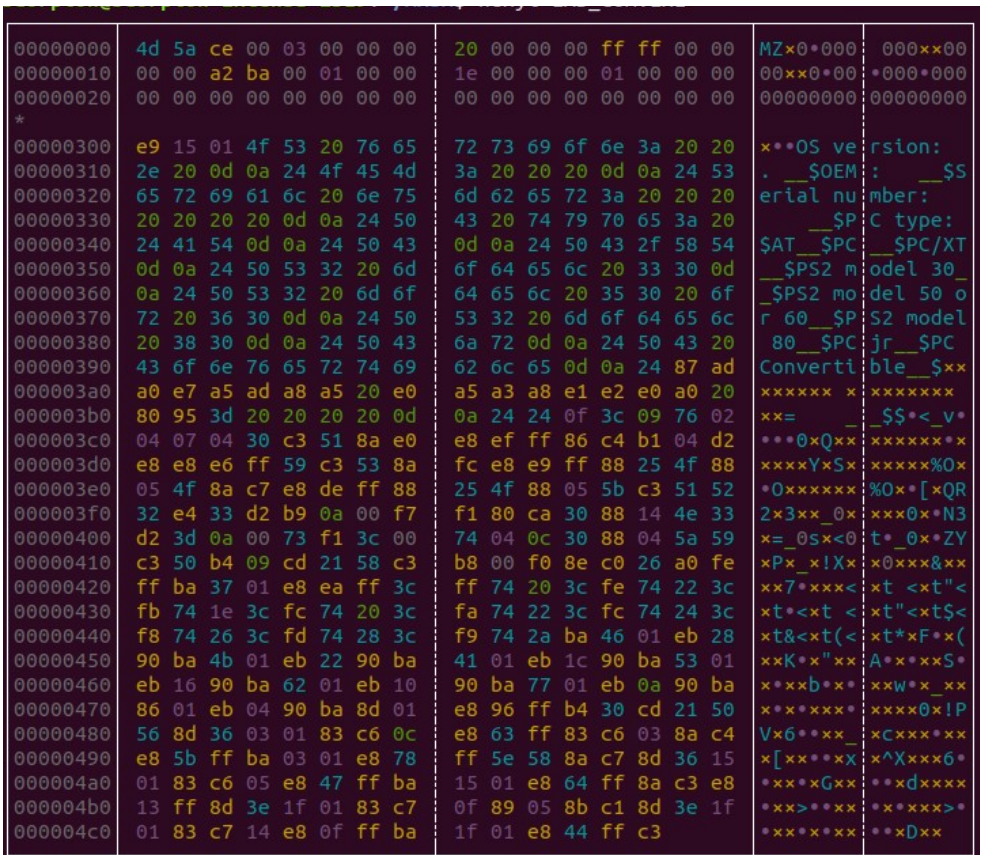
1) Какова структура файла COM? С какого адреса располагается код?

Ответ: COM-файл содержит данные и машинные команды. Код начинается с адреса 0h, но при загрузке модуля устанавливается смещение в 100h.



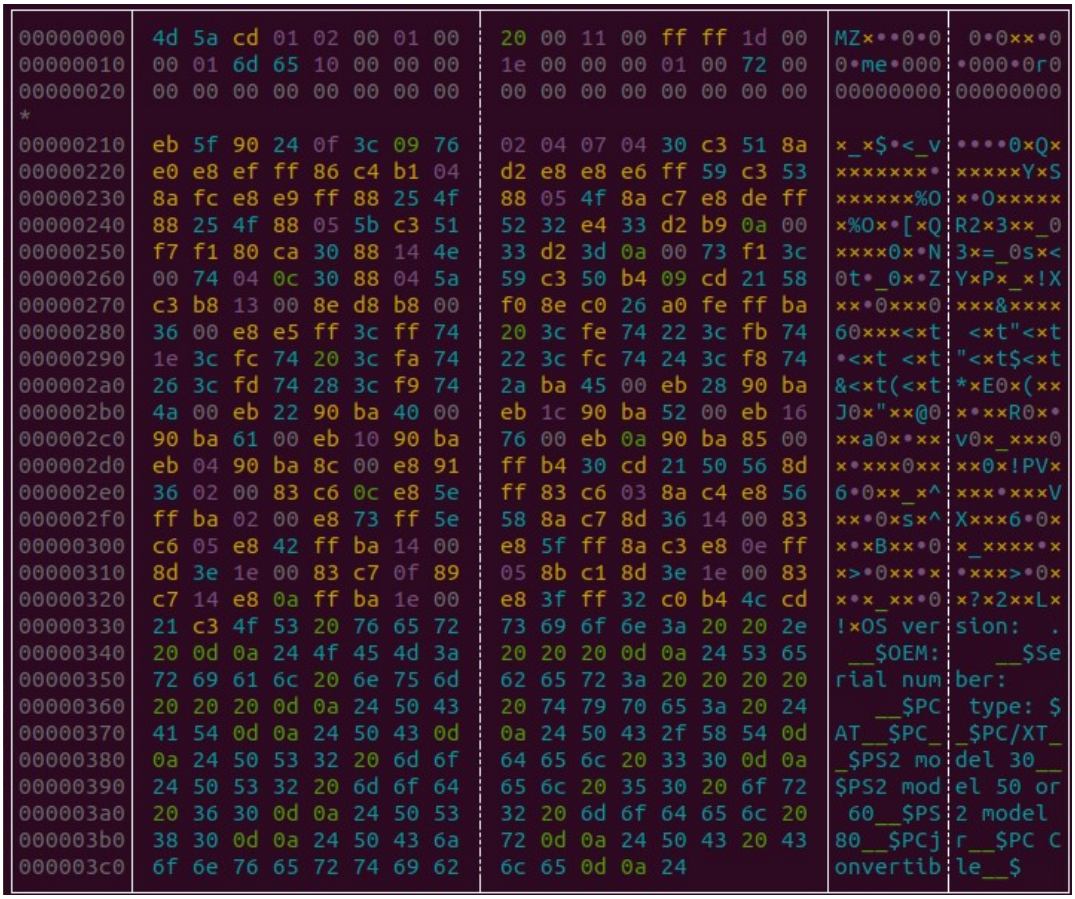
2) Какова структура файла "плохого" EXE? С какого адреса располагается код? Что располагается с адреса 0?

Ответ: В "плохом" EXE файле данные и код содержатся в одном сегменте. С адреса 0h идёт заголовок, содержащий необходимую информацию для загрузки программы в память и специальную таблицу перемещения (relocation table), необходимую для настройки ссылок на сегменты программы. MZ - первое 2-байтовое поле заголовка, в которое компоновщик устанавливает значение для идентификации правильного EXE-файла. Код располагается с адреса 300h.



3) Какова структура "хорошего" EXE? Чем он отличается от файла "плохого" EXE?

Ответ: В "хорошем" EXE данные, стек и код находятся в разных сегментах. Код начинается с адреса 210h, а не с 300h, как в "плохом" EXE-файле, так как не происходит выделения дополнительной памяти под PSP.



III. Загрузка COM модуля в основную память

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

Ответ:

1. Определяется сегментный адрес участка ОП, у которого достаточно места для загрузки программы

2. Создаётся блок памяти для PSP и программы

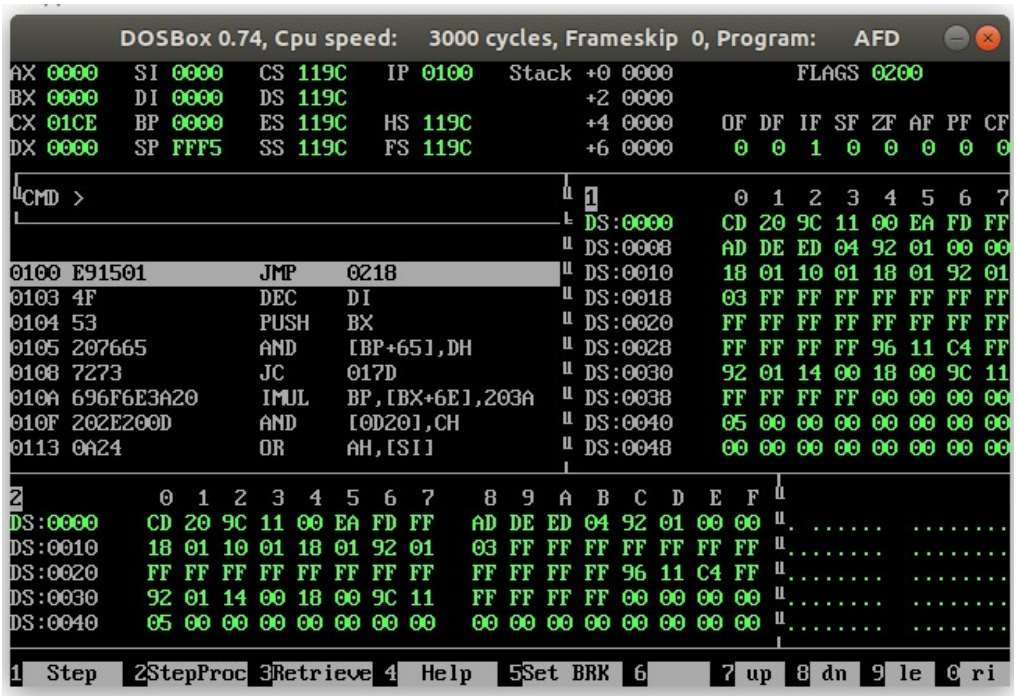
3. Загружается COM-файл с адреса 100h

4. Сегментные регистры CS, DS, ES, SS устанавливаются на начало PSP (0h)

5. Регистр SP устанавливается на конец PSP (FFh)

6. В стек записывается значение 0000

7. В регистр IP записывается значение 100h. С такого же адреса и начинается код.



2) Что располагается с адреса 0?

Ответ: Сегмент PSP

3) Какие значения имеют сегментные регистры? На какие области памяти ни указывают?

Ответ: При загрузке программы они указывают на начало PSP

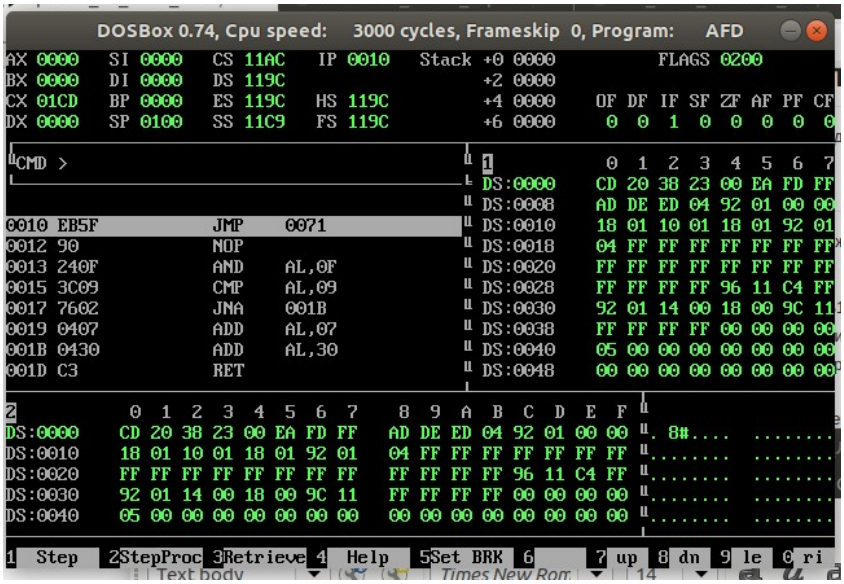
4) Как определяется стек? Какую область памяти он занимает? Какие адреса?

Ответ: Стек расположен между адресами SS:0000h и SS:FFFFh

IV. Загрузка "хорошего" EXE модуля в основную память

1) Как загружается "хороший" EXE? Какие значения имеют сегментные регистры?

Ответ: Регистры DS и ES указывают на начало блока PSP, регистр CS указывает на начало сегмента кода, а регистр SS - на начало сегмента стека.



2) На что указывают регистры DS и ES?

Ответ: На начало блока PSP

3) Как определяется стек?

Ответ: SS - начало сегмента, SS:SP - конец

4) Как определяется точка входа?

Ответ: параметром после директивы END, в качестве которого нужно передать метку, с которой программа начнёт выполнение команд.

Заключение.

Были изучены различия в структурах исходных текстов модулей .COM и .EXE, структур файлов загрузочных модулей и способов их загрузки в основную память.