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 _____ Камакин Д.В.

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.

TETR_TO_HEX — перевод значения 4-ёх младших битов в регистре AL в цифру 16-ой СС (остаётся в регистре AL).

BYTE_TO_HEX — перевод значения байта из регистра AL в число 16-ой СС. Результат записывается в AL и AH.

WRD_TO_HEX — перевод значения слова в регистре AX в число 16-ой СС и запись в виде 4 символов по адресу, записанному в регистре DI.

BYTE_TO_DEC — перевод байта в регистре AL в 10-ую СС. Символы записываются по адресу, записанному в регистре SI.

OUTPUT — вызов функции 09h прерывания int 21h (посылает строку на стандартный вывод).

Последовательность действий.

Вызываем функцию 30h прерывания int 21h для получения текущего номера версии DOS. Затем переводим результат работы функции в 16/10 СС и записываем в соответствующие строки. Для этого используем функции BYTE_TO_DEC и BYTE_TO_HEX, а также WRD_TO_HEX.

Для вывода информации о типе PC читаем содержимое предпоследнего байта ROM BIOS и, сравнивая его значение с табличными, получаем строковое представление названия модели.

Выводим все полученные строки при помощи функции OUTPUT и завершаем программу.

Результаты исследования проблем.

Отличия исходных текстов COM и EXE программ

1) Сколько сегментов должна содержать COM-программа?

Только один.

2) EXE-программа?

Не менее одного.

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

ORG 100H, поскольку в начале COM-программы определён 256-байтовый PSP (префикс программного сегмента), а значит необходимо обеспечить смещение на 100h байт от начала.

Директива ASSUME необходима для проверки допустимости каждого обращения к именованной ячейке памяти с учётом значения текущего сегментного регистра. Кроме того, требуется использования директивы END для завершения программы.

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

Нельзя использовать seg из-за отсутствия таблицы настройки.

Отличия форматов файлов COM и EXE модулей

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

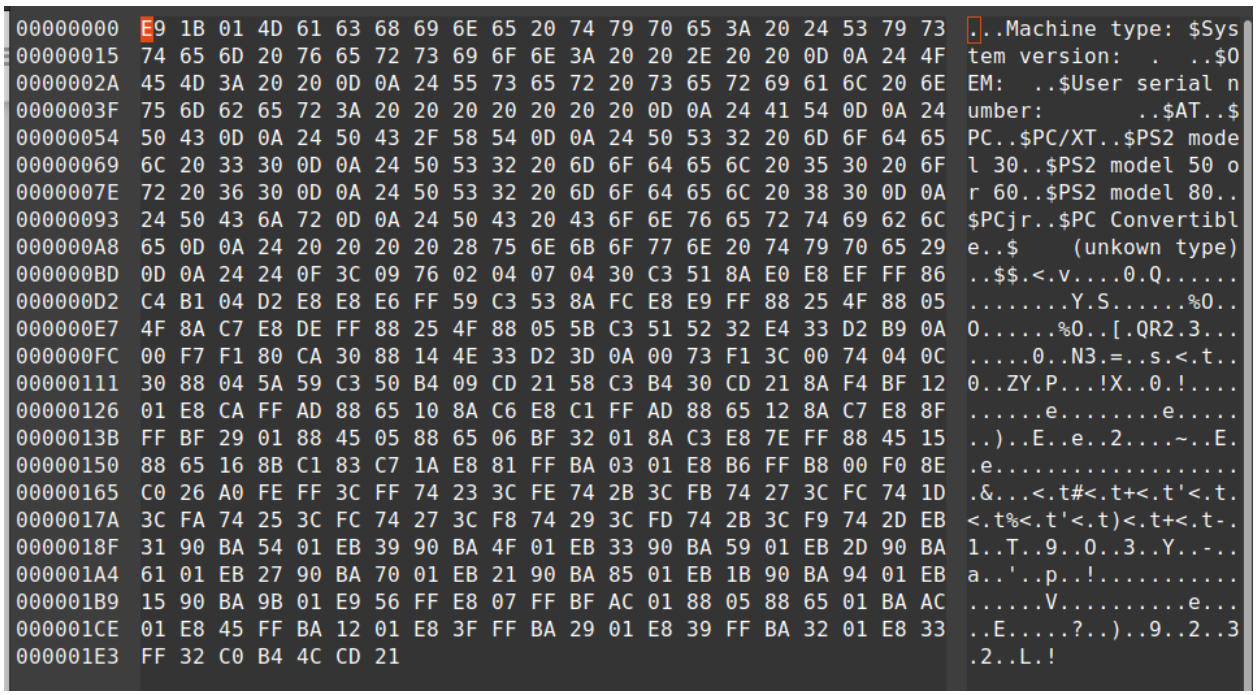

Рис. 1. COM файл в шестнадцатеричной форме.

В файле COM содержится только код и данные программы. Код располагается с 0 адреса.

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

Код и данные расположены в одном сегменте, начиная с адреса 300h. С адреса 0 расположена таблица настроек и заголовок.

Рис. 2. «Плохой» EXE файл в шестнадцатеричной форме.

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

В «хорошем» EXE код и данные разделены по сегментам, таблица настроек корректна (начинается с адреса 0). У «хорошего» и «плохого» EXE файла код начинается с разных смещений, поскольку у первого нет директивы ORG 100h.

Рис. 3. «Хороший» EXE файл в шестнадцатеричной форме.

Загрузка COM модуля в основную память

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

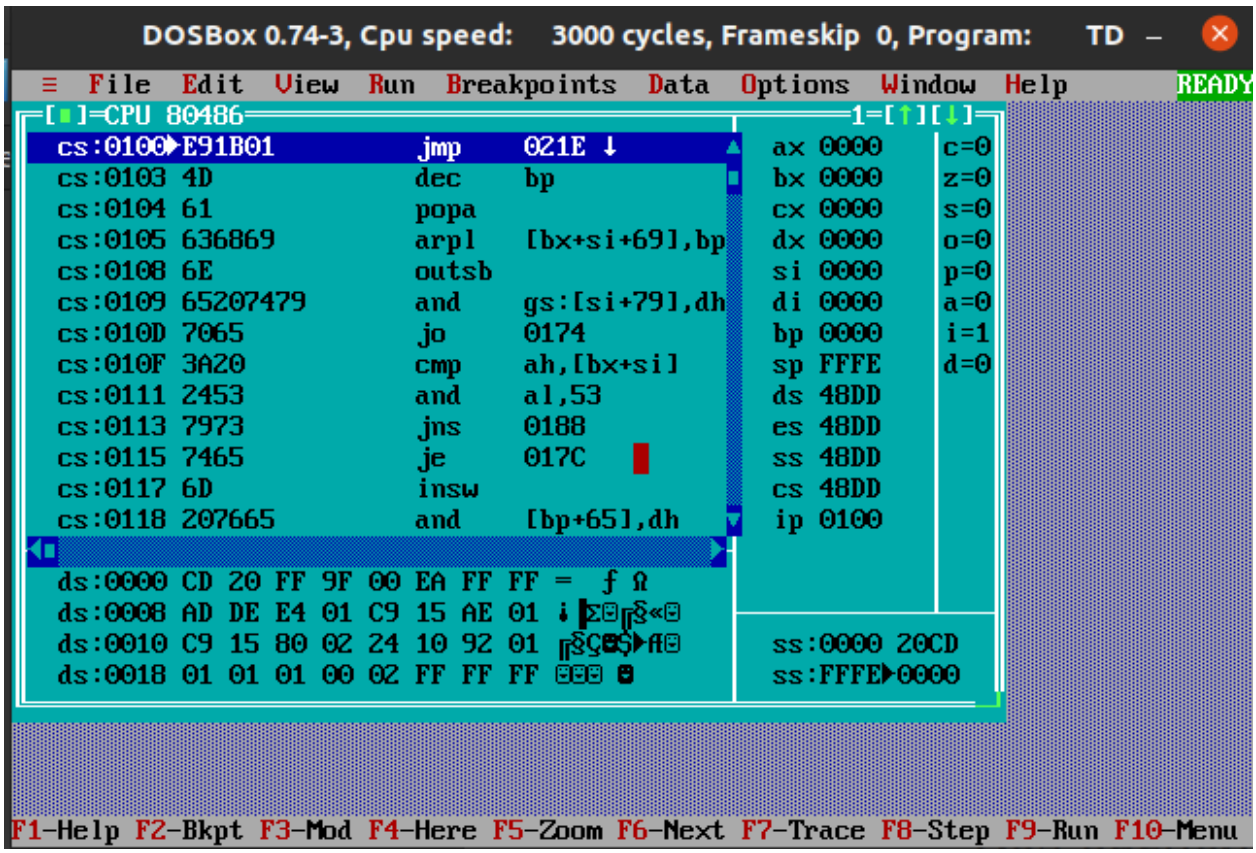

Рис. 4. Результат работы программы TD для COM файла.

Сначала помещается PSP в подходящее по размеру место, а затем сам код (значит он расположен с адреса 100h).

2) Что располагается с адреса 0?

PSP

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

DS,ES,CS и SS указывают на PSP

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

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

Загрузка «хорошего» EXE модуля в основную память

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

Считывается информация из заголовков EXE, в IP загружается смещение точки входа. CS — начало сегмента кода, DS и ES — начало блока PSP, SS — начало стека.

2) На что указывают регистры DS и ES?

На начало блока PSP

3) Как определяется стек?

Директивой .stack, SS будет указывать на начало, SS:SP на конец.

4) Как определяется точка входа?

Директивой END (метка указывает на точку входа)

План загрузки модуля .COM в основную память

1. В основной памяти ищется свободный сегмент, в который будет загружена программа.
2. В начало сегмента загружается блок PSP (100h), после которого идёт COM модуль.

Заключение

Исследованы различия в структурах исходных текстов модулей типов .COM и .EXE, структуры файлов загрузочных модулей и способы их загрузки в основную память.