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 _____ Пя С.

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.

Сведения о функциях и структурах.

TETR_TO_HEX: процедура перевода из 10-ой сс в символы

BYTE_TO_HEX: процедура перевода байта из 16-ой сс в символы

WRD_TO_HEX: перевод слова из 16-ой сс в символы

BYTE_TO_DEC: перевод байта из 16-ой сс в 10-юю и символы

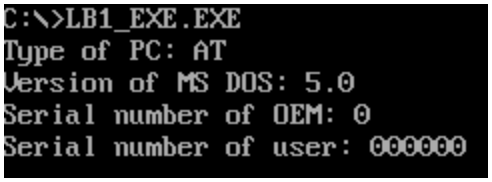
print_string: процедура вывода строки на экран

print_type_of_PC: процедура вывода типа IBM PC на экран

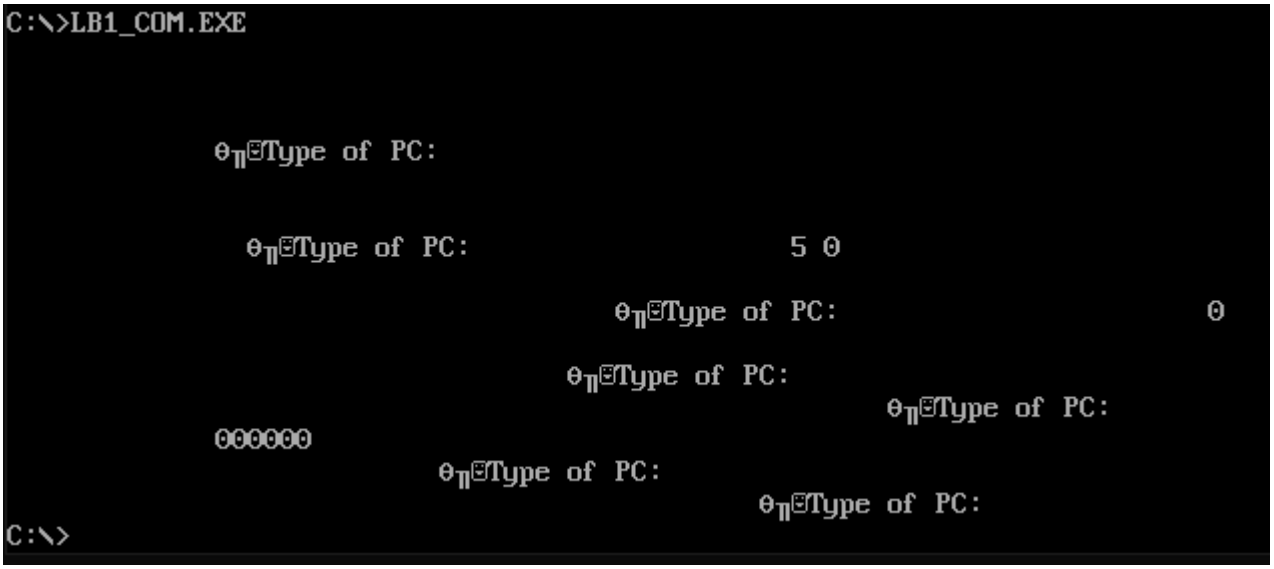
print_version_of_PC: процедура вывода версии MS DOS на экран

Последовательность действий, выполняемых утилитой.

1. Определяется тип PC путем считывания содержимого предпоследнего байта ROM BIOS с представленной таблицей в методических указаниях, и выводится строка, содержащая название соответствующего типа.
2. Определяется версия PC. Выводится строка в определенном формате, содержащая номер основной версии и номер модификации в десятичной системе счисления, затем выводится серийный номер OEM и серийный номер пользователя. Путь их определения написан в методических указаниях. Вывод «правильного» файла EXE:



Вывод «плохого» EXE файла:



Вывод COM файла:

Выводы.

В ходе выполнения лабораторной работы была написана программа для определения типа и версии PC, изучены различия в структурах исходных текстов модулей типов .COM и .EXE, структур файлов загрузочных модулей и способов их загрузки в основную память.

Ответы на контрольные вопросы по лабораторной работе №1.

Отличия исходных текстов COM и EXE программ

1) Сколько сегментов должна содержать COM-программа?

COM-программа должна содержать только один сегмент, стек генерируется автоматически, а привычные сегменты кода и данных содержатся в одном сегменте.

2) EXE-программа?

EXE-программа должна содержать более одного сегмента. Код, данные и стек будут храниться в отдельных сегментах.

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

В тексте COM-программы обязательно должны быть директивы ORG 100h и ASSUME, так как при загрузке модуля в начале определяется 100h префикс программного сегмента, так что адресация должна быть смещена на столько же и вторая для того, чтобы указать один сегмент как сегмент данных и кода.

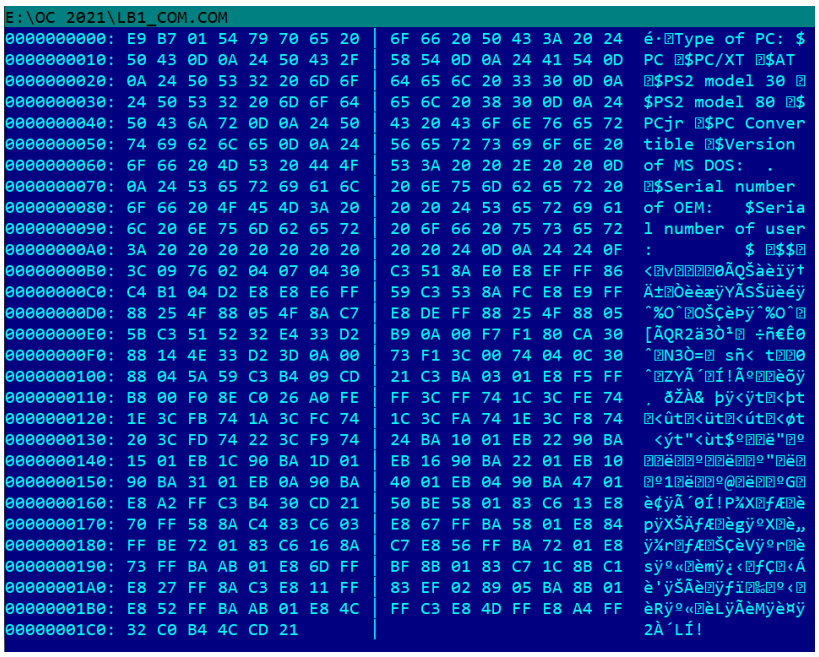
4) Все ли форматы команд можно использовать в COM-программе?

Не все форматы команд можно использовать в COM-программе, а именно команды типа mov (регистр), seg (наименование сегмента). COM-программы имеют один сегмент, поэтому сегментные регистры имеют одни и те же значения. А EXE-программы могут быть больше 64КБ, поэтому загрузчик ОС распределяет содержимое по нескольким сегментам.

Отличия форматов файлов COM и EXE модулей

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

Файл COM состоит из одного сегмента и может быть размером не больше 64КБ. Код располагается с 0h, но при загрузке модуля смещается на 100h.



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

У файла «плохого» EXE код и данные будут располагаться в одном сегменте, код будет располагаться с адреса 300h, с адреса 0h будет таблица настроек.

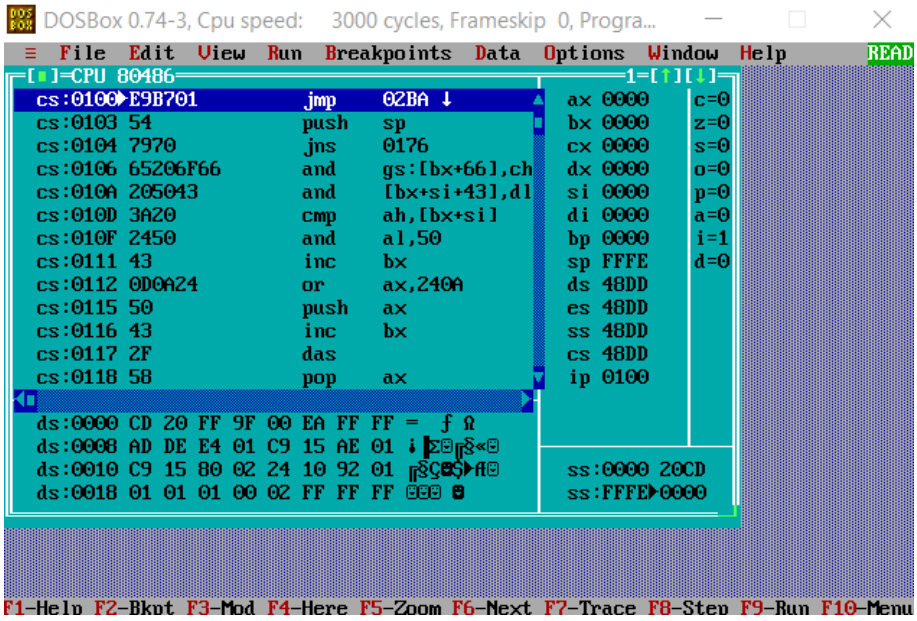
3) Какова структура файла «хорошего» EXE? Чем он отличается от файла «плохого» EXE?

У файла «хорошего» EXE данные, код и стек размещены в разных сегментах, и файл может быть большего размера, чем 64КБ. У «плохого» файла EXE код начинается с 300h, так как он получается из файла COM, в котором код смещен на 100h, а 200h – это размер PSP модуля, а у «хорошего» EXE выделяется память под стек между PSP и кодом.

Загрузка COM модуля в основную память

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

Сначала определяется сегментный адрес участка ОП, способного вместить загрузку программы, затем создается блок памяти для PSP и программы, COM-файл считывается помещается в память с 100h. После сегментные регистры устанавливаются на начало PSP. SP устанавливается на конец PSP, 0000h помещается в стек, в IP записывается 100h. Код располагается с адреса 100h.



2) Что располагается с адреса 0?

PSP сегмент располагается с адреса 0.

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

Сегментные регистры имеют значения 48DD и указывают на PSP.

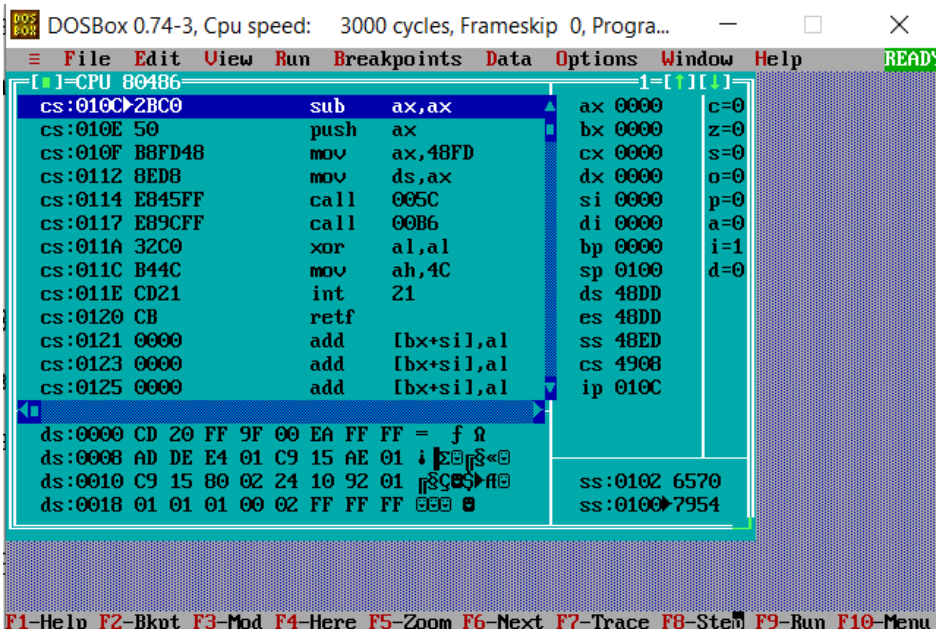
4) Как определяется стек? Какую область памяти он занимает? Какие адреса?

Стек генерируется автоматически. SP указывает на конец стека, а SS – на начало. Адреса расположены в диапазоне 0h–FFFEh (потому что это последний адрес, который кратен двум).

Загрузка «хорошего» EXE модуля в основную память

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

Загружается «хороший» EXE со считыванием информации заголовка EXE, выполняется перемещение адресов сегментов, ES и DS устанавливаются на начало PSP, SS – на начало сегмента стека, а CS – на начало сегмента команд.



2) На что указывают регистры DS и ES?

ES и DS указывают на начало PSP.

3) Как определяется стек?

Стек определяется с помощью директивы .stack с указанием размера стека. SS указывает на начало сегмента стека, а SP – на конец.

4) Как определяется точка входа?

Точка входа определяется директивой END.