МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

Ордена Трудового Красного Знамени федеральное государственное

бюджетное образовательное учреждение

высшего образования

«Московский технический университет связи и информатики»

(МТУСИ)

Отчет

по лабораторной работе №1

по дисциплине «Защита информации в глобальных сетях»

на тему: Составление РЕ файла и внедрение сигнатуры

Выполнил: студент группы МБД2031

Морозов М.Е.

Проверил: Барков В.В.

Москва

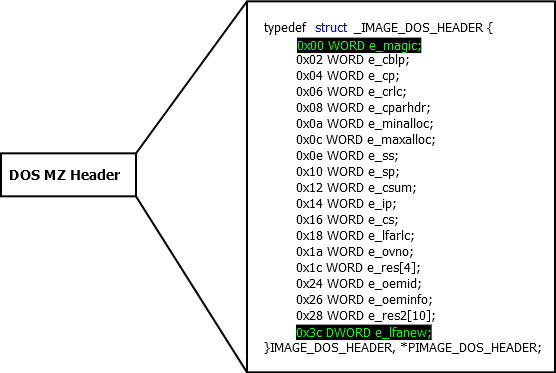
2022

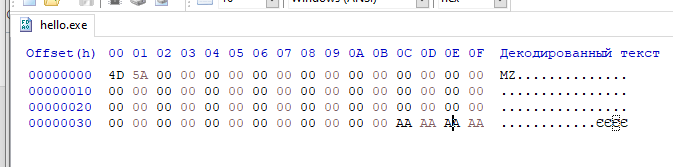
**Цель работы:** изучить принципы работы и получить навыки составления РЕ файла.

**Инструментарий:**

HxD Hex Editor.

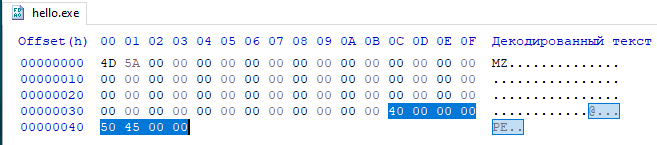
PE Explorer.



*e\_magic*: WORD — сигнатура находящаяся по смещению 0 от начала файла и равная “MZ”. Если данная сигнатура не равна MZ, то файл не загрузится. 

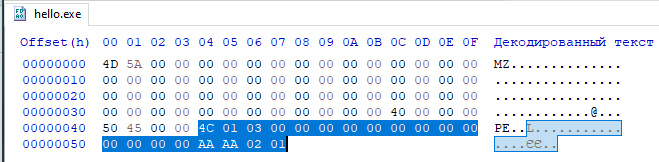
*e\_lfnew*: DWORD — смещение PE заголовка относительно начала файла. PE заголовок должен начинаться с сигнатуры PE\x0\x0. PE заголовок может располагаться в любом месте файла. Если посмотреть на структуру, то можно увидеть, что *e\_lfnew* находится по смещению 0x3C (60 байт). То есть чтобы прочитать это значение, мы должны от указателя на начало файла прибавить 60 байт и тогда мы встанем перед e\_lfnew. Читаем это значение и плюсуем к указателю начала файла это значение. Это должен быть PE заголовок.

В данной лабораторной работе задаём смещение в 0x40, пусть РЕ заголовок следует сразу за *e\_lfnew.* Его длинна 4 байта.



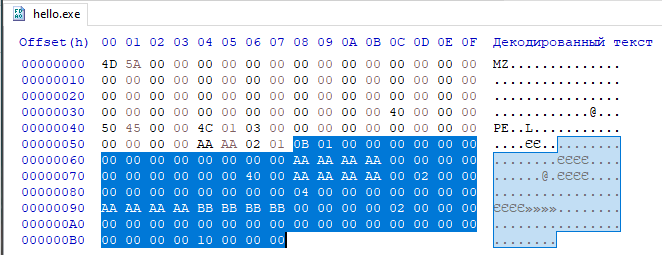
Так как Dos-Header я заполнил, далее заполняю File-Header, где начиная с адреса 0х44 по порядку буду использовать следующие значения:

* Архитектура процессора 32 бита (2 байта) – 0х014с
* Количество секций – 3 (2 байта) – 0х03
* Временная метка (4 байта) – NULL
* Указатель на таблицу символов (4 байта) – NULL
* Количество символов (4 байта) – NULL
* Размер дополнительного заголовка (2 байта) - ?? ААAA
* Характеристика файла (2 байта) – 0х0102 где 0х0002 – исполняемый файл, а 0х0100 – 32х битная поддержка

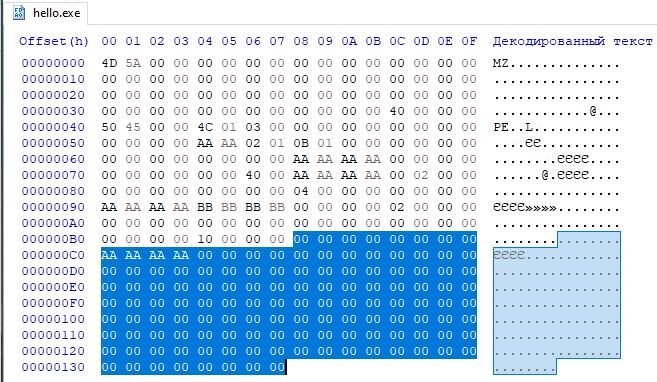


Затем заполняю опциональный заголовок, он будет состоять из:

* Magic (2 байта) – 0х01b указывает на 32 битность программы
* AddressOfEntryPoint (4 байта) - ?? АААААААА
* ImageBase (4 байта) – 0х004 значение по умолчанию
* SectionAlignment (4 байта) - ?? ААAAАААА
* FileAlignment (4 байта) – 0х200 значение по умолчанию
* MajorSubsystemVersion – 0х0004 Windows NT
* SizeOfImage – AAAAAAAA кратно SectionAlignment
* SizeOfHeaders – BBBBBBBB кратно FileAlignment
* Subsystem – 0x0002 т.к. программа является графической программой Windows
* NumberOfRvaAndSizes – 0x10 значение по умолчанию



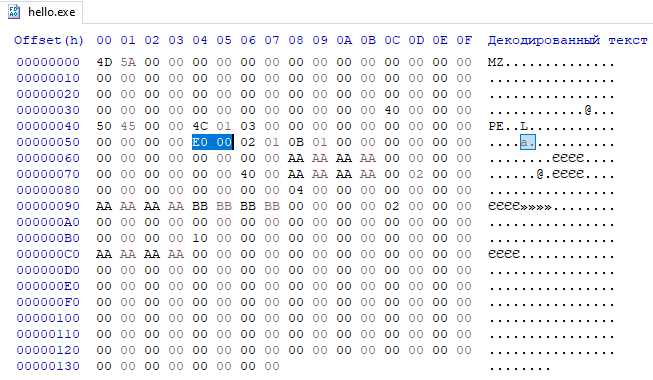
Далее в DataDirectory возмём IMAGE\_DIRECTORY\_ENTRY\_IMPORT где секцию VirtualAddress заполним АААААААА, а Size заполним NULL



После заполнения опционального заголовка, вычисляем его размер и он составил:

0х137 – 0х58 + 0х1 = 0хЕ0

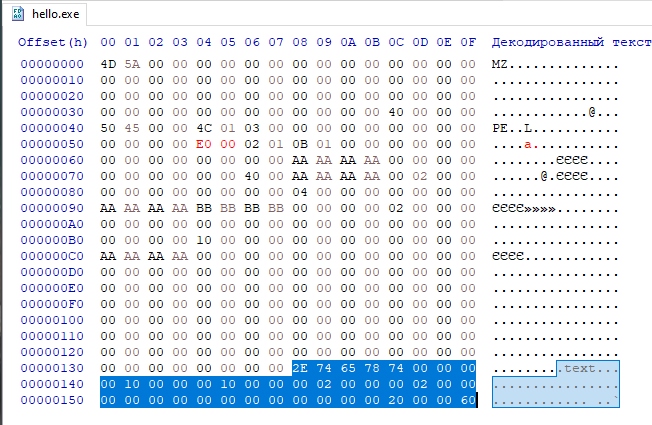
Запишем это значение в SizeOfOptionalHeader:



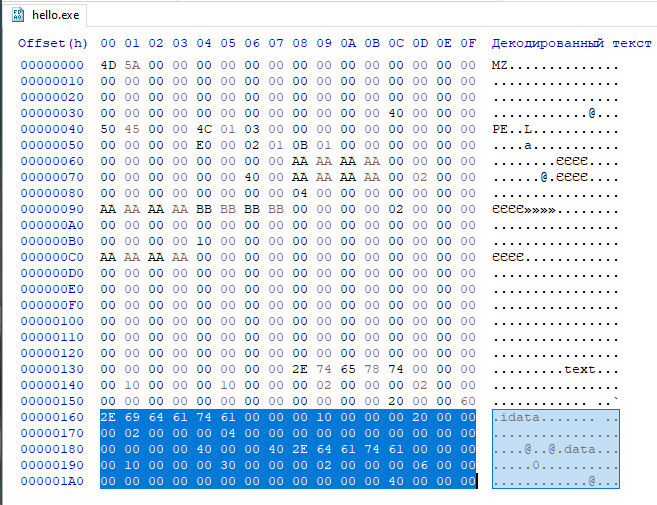
Далее заполняем IMAGE\_SECTION\_HEADER, где:

* Name - .text
* VirtualSize – 0x1000
* VirtualAddress – 0x1000
* SizeOfRawData – 0x200
* PointerToRawData – 0x200
* Characteristics – 0x60000020

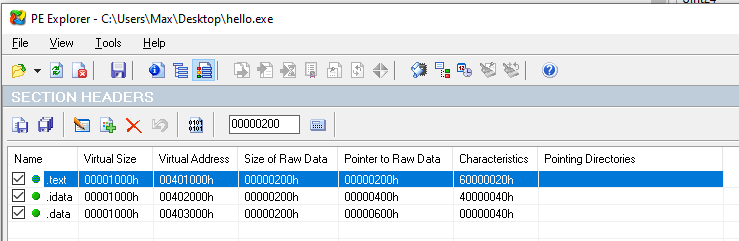
Остальные заполним NULL.



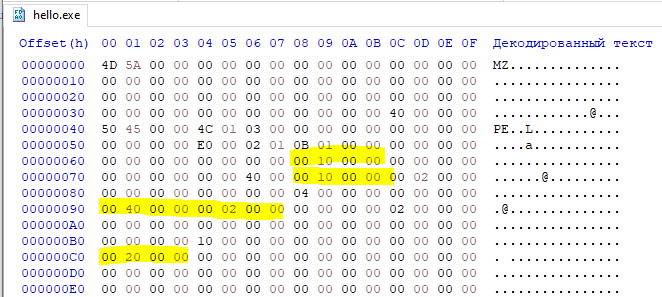
Аналогично заполним секции .idata и .data

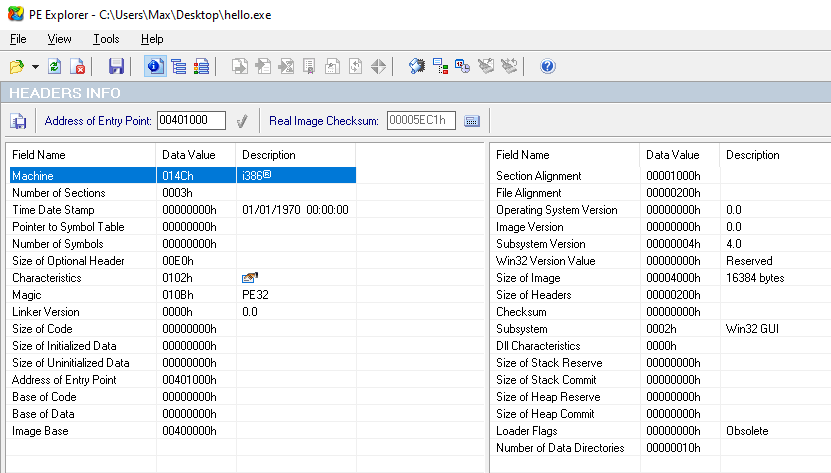


Далее открываем получившийся файл в программе PE Explorer, где уже можно определить виртуальный адрес загрузки секции кода .text:

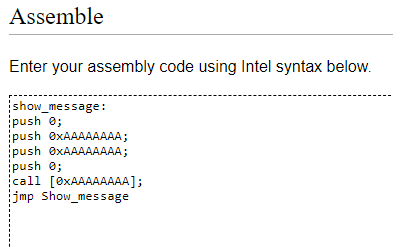


После чего можем заменить значения в AddressOfEntryPoint, SectionAllignment, SizeOfImage, SizeOfHeaders и виртуальный адрес таблицы импорта.

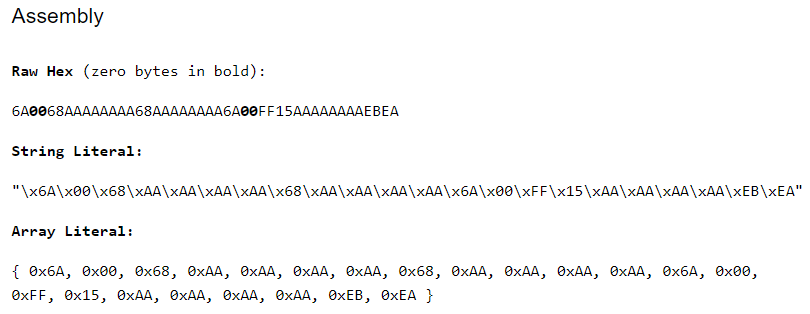




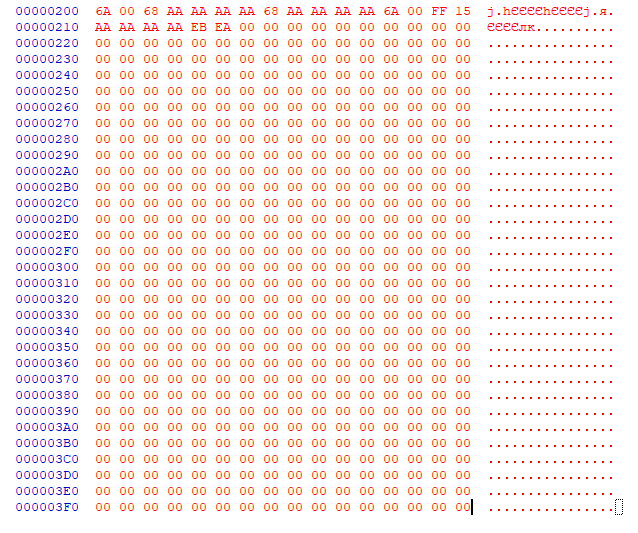
Для секции кода наша процедура отображения сообщения выглядит так:



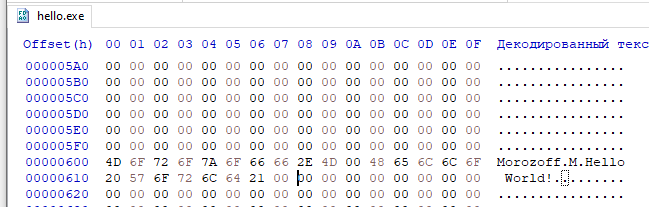
В коде выглядит так:



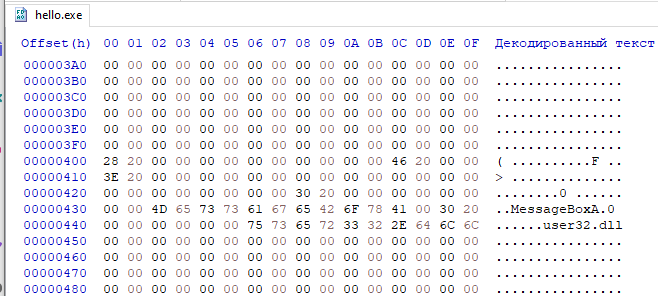
Внесем в секцию .text с учетом корректировки адреса:



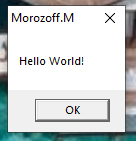
В секции данных ввел Morozoff.М Hello World! и выровнял размер секции до 0х200:



Далее в секцию Import List внес функцию и имя библиотеки:



Сохранил. Программа готова и работает:



**Выводы**

В данной лабораторной работе я изучил принципы работы и составления РЕ файла, получил навыки построения РЕ файла с помощью НЕХ - редактора.