

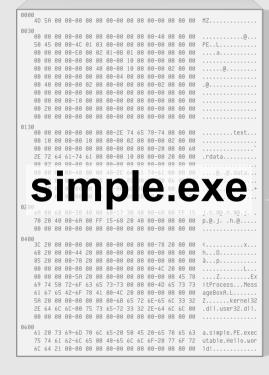
PE101 пошаговое руководство к исполняемым файлам (EXE) Windows

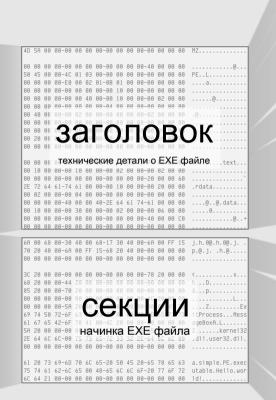
Ange Albertini corkami.com

версия 1.00 RU, 03.07.2012

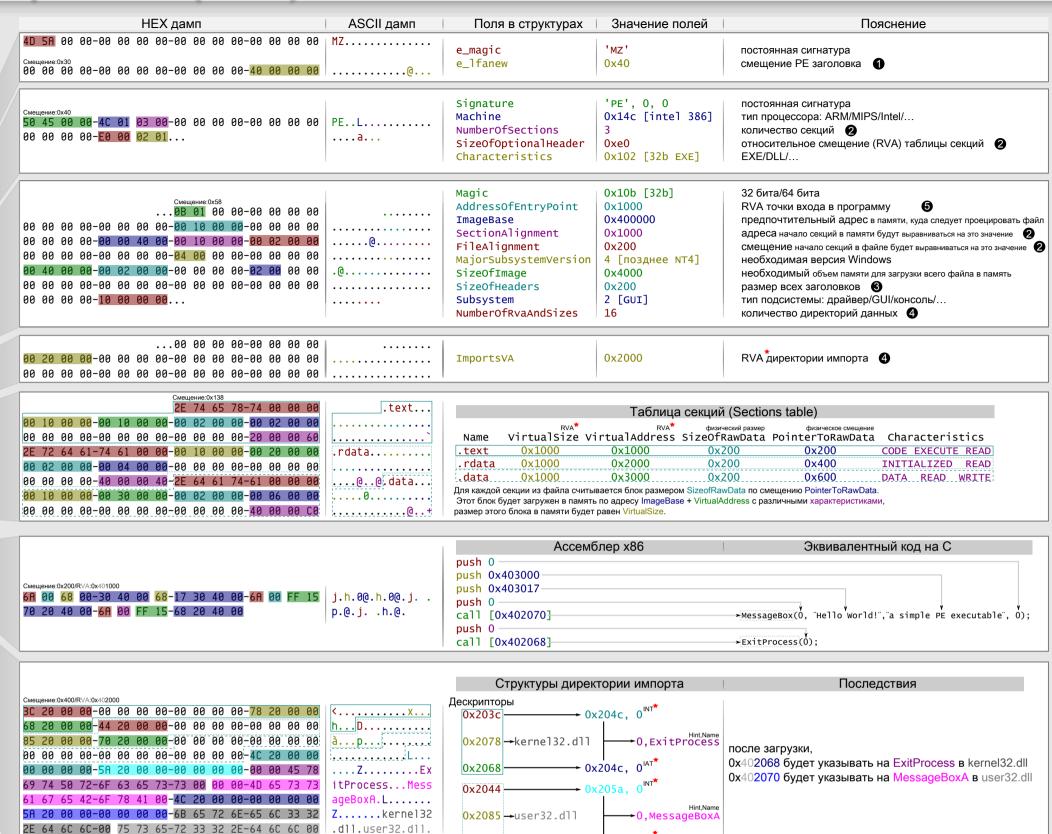
Разобранный РЕ











0x2070 -

Строки

a simple PE executable\0

переведено Lyr1k

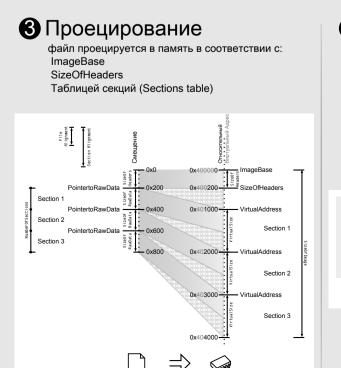
Процесс загрузки

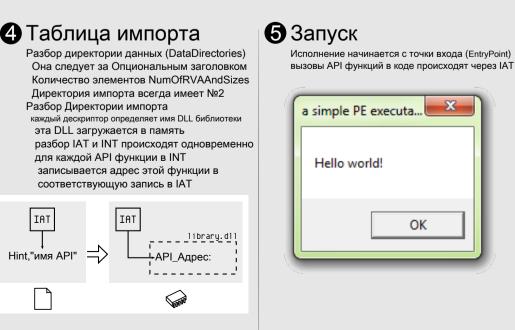
1 Заголовки

разбор РЕ заголовка (поле e_lfanew в DOS заголовке указывает на PE заголовок) (он следует сразу за РЕ заголовком)

2 Таблица секций

Разбор Таблицы секций она содержит NumberOfSections элементов она проверяется на корректность выравнивания: FileAlignments и SectionAlignments



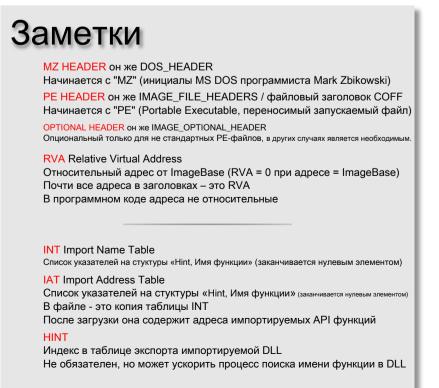


6C 64 21 00

61 20 73 69-6D 70 6C 65-20 50 45 20-65 78 65 63 a.simple.PE.exec

75 74 61 62-6C 65 00 48-65 6C 6C 6F-20 77 6F 72 utable.Hello.wor

Это полноценный РЕ-файл, однако, большинство РЕ-файлов содержат большее количество элементов. Для простоты объяснения опущены



Здесь все адреса записаны в RVA