Лабораторна робота № 3
Дослідження структури програм формату EXE.

Мета роботи

Ознайомлення із специфікацією **COFF** (Common Object File Format). Вивчення прийомів дослідження структури файлів **PE**-формату.

Порядок виконання роботи

1. Вивчити структуру програм формату **EXE** [1].
2. Розробити програму на мові Асемблер, за допомогою якої у віконному інтерфейсі по введеному паролю виводяться персональні дані студента – ПІБ, дата народження, номер залікової книжки тощо (див. лаб. роботу 1).
3. Виконати компіляцію розробленого файлу у формат **EXE**.
4. Перевірити роботу програми шляхом введення як правильного, так і невірного паролів.
5. Отриманий виконавчий файл дослідити за допомогою програми **HEX**-редактора **HIEW32** (див. лаб. роботу 2) або **WinHex** (http://rainbowsky.ru/system/winhex/ - trial версия*) [2]
6. На скріншоте перших 25 рядків вмісту файлу обвести кольоровим олівцем або фломастером області MS-DOS заголовка (**DOS_HEADER**), PE заголовка (**PE_HEADER**) і таблиці секцій (**SECTION_HEADERS**). Скріншот привести в звіті по лабораторній роботі.
7. Відповідно до опису секцій [1] скласти таблицю, в яку занести параметри свого файлу, вказані в розділах 3.3.1, 3.4.1 і 4 (перша таблиця).
8. У останньому стовпчику таблиці розшифрувати виписані значення полів заголовка файлу. Таблицю привести в звіті по лабораторній роботі.
9. Провести дослідження того ж файлу за допомогою меню "**PE Editor**" безкоштовної програми **PE Tools** (http://soft.mydiv.net/win/download-PE-Tools.html*). Все скріншоти вікон програми з даними, відповідними раніше побудованій таблиці, привести в звіті по лабораторній роботі.
10. Дослідити таблицю імпорту (**Import Directory**) даного файлу і визначити, які саме функції використовуються з бібліотек, що підключаються. Скріншоти вікон **Import Directory** з функціями, що імпортуються, з кожного бібліотечного файлу привести в звіті по лабораторній роботі.
11. Знайти в тексті файлу по зсуву, узятому з побудованої таблиці, секцію з даними і переконатися, що текст оригінала пароля, що міститься в тексті програми, може бути легко виявлений за допомогою **HEX**-редактора. Привести скріншот цього фрагмента програми у вигляді **HEX** - коду в звіті по лабораторній роботі.
12. Виконати шифрування пароля за допомогою функції **XOR**, знову скомпілювати **EXE** - файл і переконатися, що тепер вони не виявляються явним чином в тексті виконуваного **EXE** - файлу. Привести скріншоти цієї програми в режимах «**Hex**» і «**Text**» в звіті по лабораторній роботі.
13. Зробити висновки по лабораторній роботі.

Література, що рекомендується:

1. Microsoft Portable Executable and Common Object File Format Specification. (http://www.osdever.net/documents/PECOFF.pdf)
2. PE Format . https://docs.microsoft.com/en-us/windows/win32/debug/pe-format
3. WinHex. Материал из Википедии. https://ru.wikipedia.org/wiki/WinHex.

* ***вказані ресурси є орієнтовними, студент має право самостійно вибрати який-небудь інший ресурс для завантаження вказаних програм***.