Лабораторна робота №9—12

РЕВЕРС ІНЖЕНЕРІНГ ДИНАМІЧНИХ БІБЛІОТЕК

**Мета**: здобути практичних навичок реверсного програмування.

**Індивідуальне завдання:** використовучи зовнішню динамічну бібліотеку виконати наступні завдання:

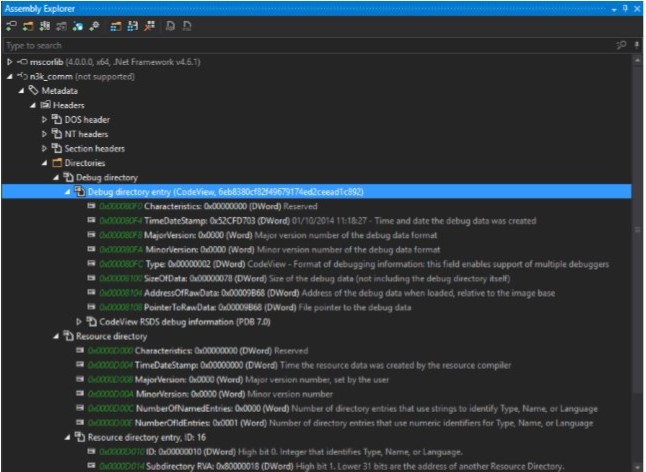
* визначити якою мовою написано бібліотеку
* визначити список функцій та їх сігнатури, якими можна користуватися
* декомпілювати та нормалізувати функції getIV, getIVDB, getK, getKDB
* декомпілювати/переписати функцію CRC\_16\_IBM
* декомпілювати/переписати функції dec / enc.

ХІД РОБОТИ

Розробка програми проводилася у сфері розробки Eclipse IDE для С++.

Декомпіляцію динамічної бібліотеки було виконано у декомпіляторі dotPeek.

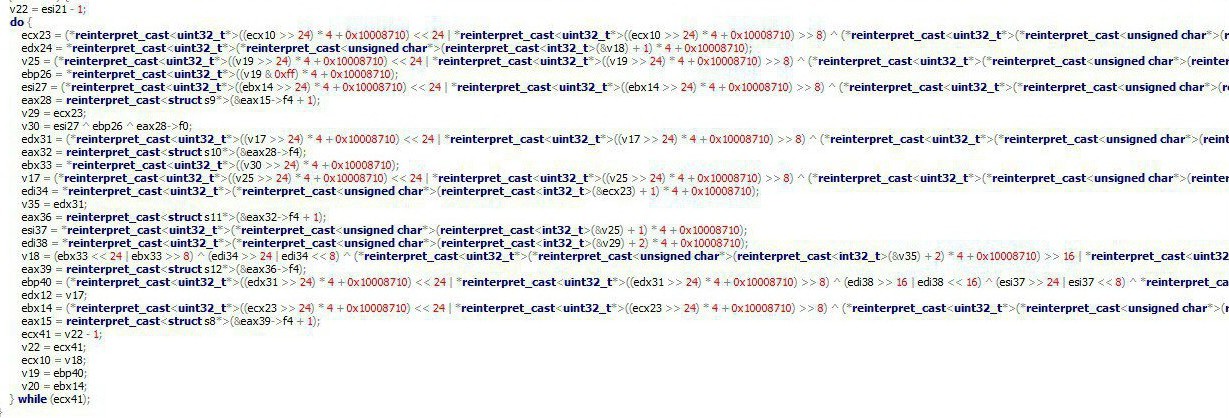
Першим чином було завантажено динамічну бібліотеку з Google диску. Бібліотека має назву n3k\_comm.dll, яка написана мовою С++. Структуру декомпільованої бібліотеки можна побачити далі.



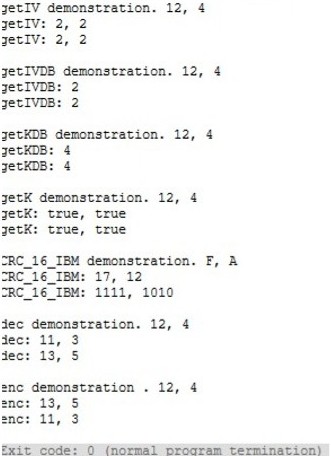
Зі скріну можна побачити, що бібліотеку було створено 01.10.2014 у 11:18:27. Оскільки динамічна бібліотека має нестандартний вигляд без приєднаних ресурсних пакетів, основна переробка програми буде виконана у сфері розробки Eclipse. Натискаючи кнопку



проект із бібліотеки стає істівним у Visual Studio. Далі копіюємо у Eclipse.

Оскільки бібліотека має вставки з чистого асемблеру декомпілюємо ще раз у x64dbg. Результат можна побачити далі.

Для кожної функції отримуємо новий вигляд. Результат компіляції в Eclipse можна побачити далі.



ВИСНОВКИ

В результаті виконання лабораторної роботи ми здобули практичних навичок з декомпілювання динамічних бібліотек.