11.01.2024

Курс:

Практическая работа к уроку № Lesson_8

--
Антиотладочные приемы

Задание:

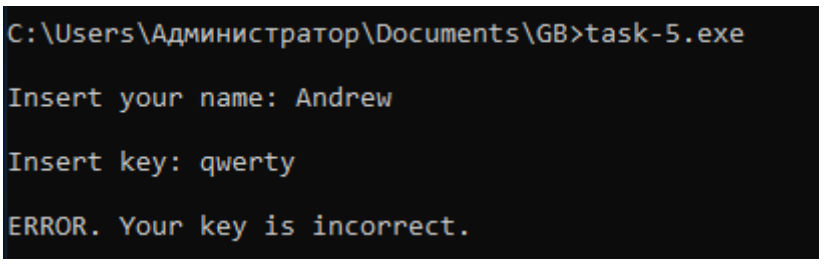
Дана программа task-5. Необходимо получить ключ для вашего имени, который успешно примет программа.
Пример запуска программы:
task-5.exe

```
Name: <your name>
License Key: <license key>
```

Антиотладочный прием – это способ обнаружения того, что программа выполняется под
управлением отладчика. Основной целью является замедление или предотвращение процесса реверс - инжиниринга.

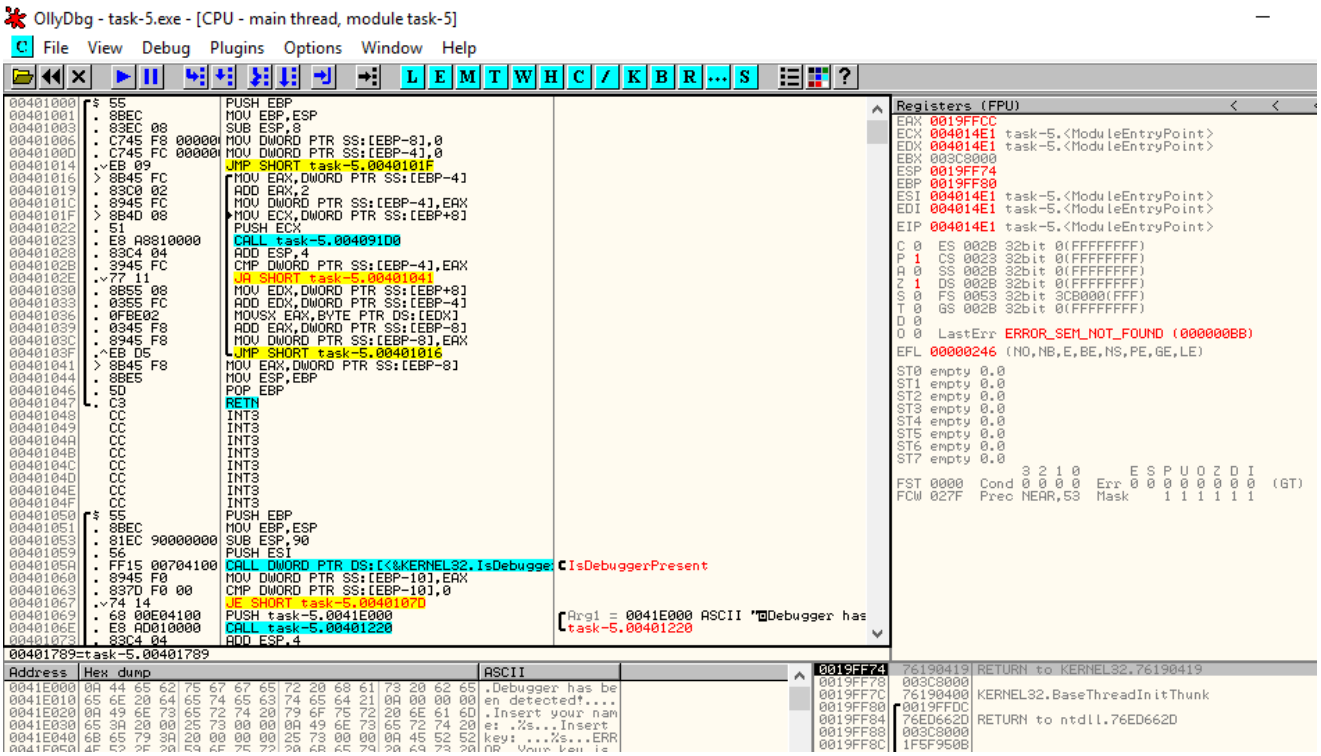
Запускаем в CMD *task-5.exe*

Insert name: Andrew
License key: aaaabbbbccccdddd

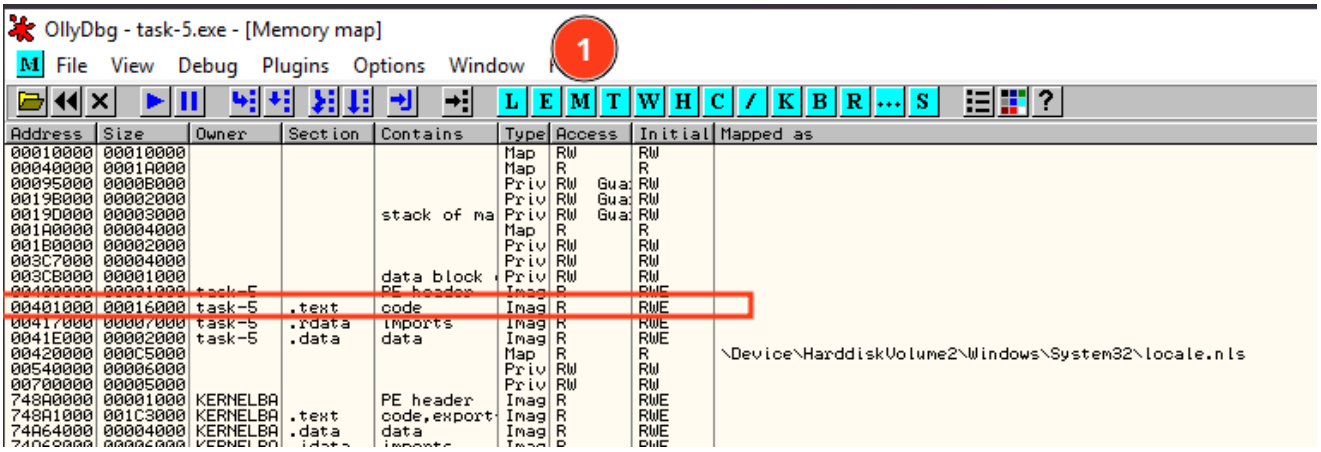


License key: **aaaabbbbccccdddd**

Запускаем *task-5.exe* под отладчиком в OllyDbg



Окно ***Memory***



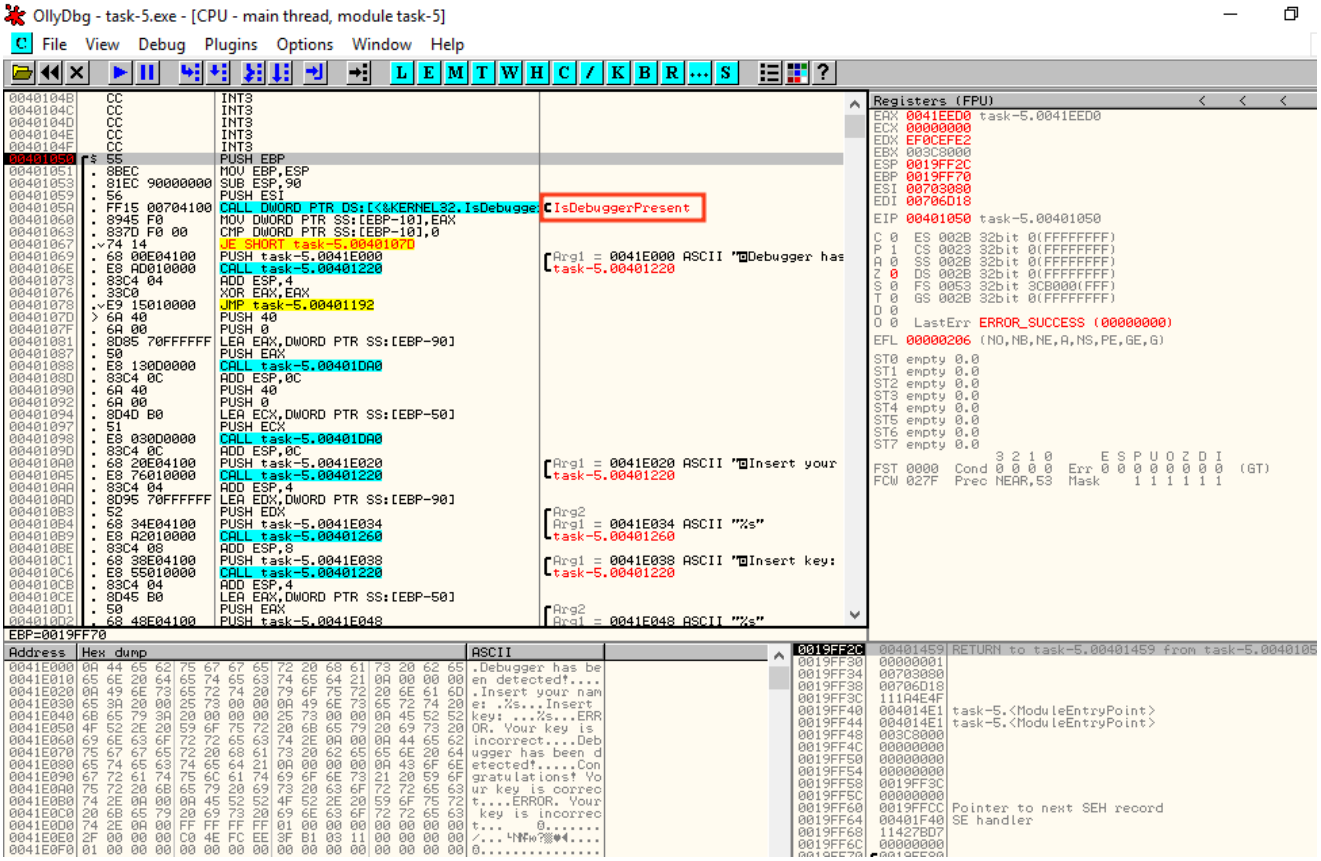
Секция кода находится по адресу 00401000

Переходим по этому адресу (C)

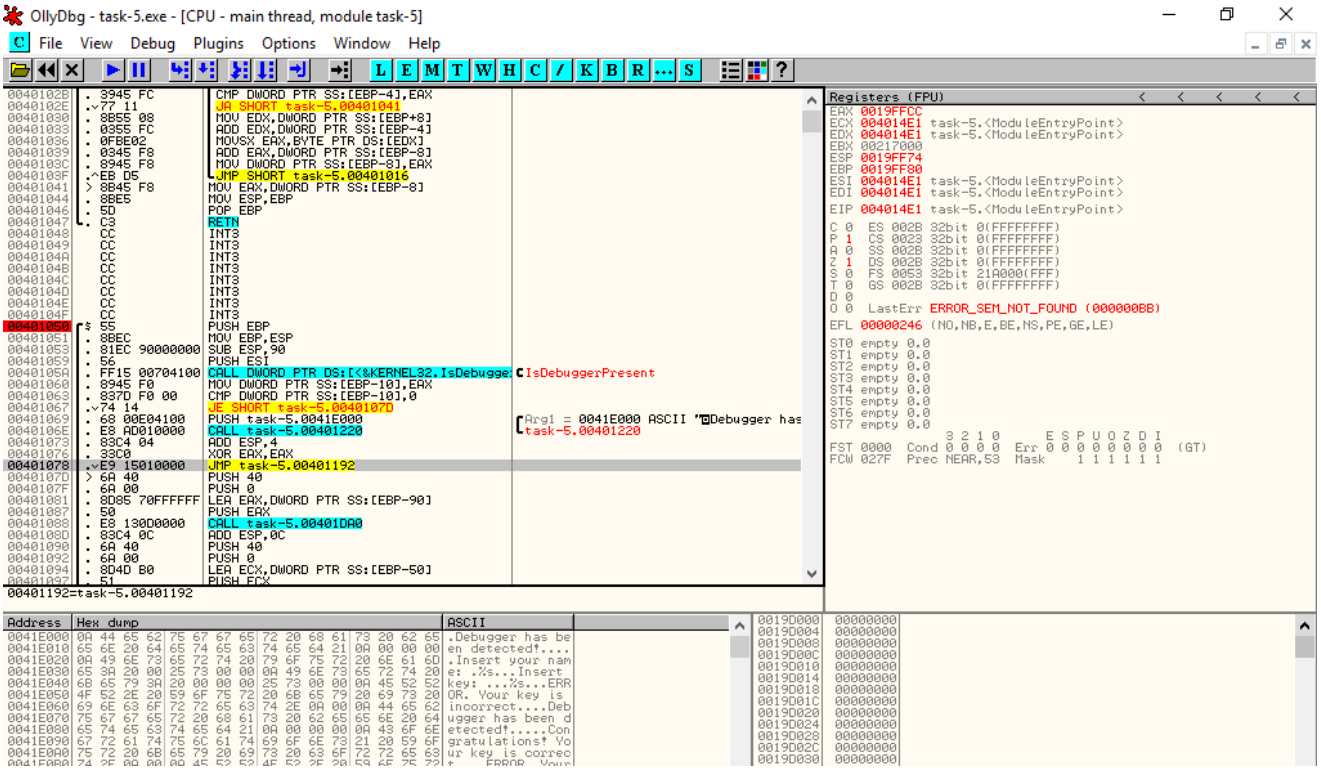
Ctrl+G 00401000

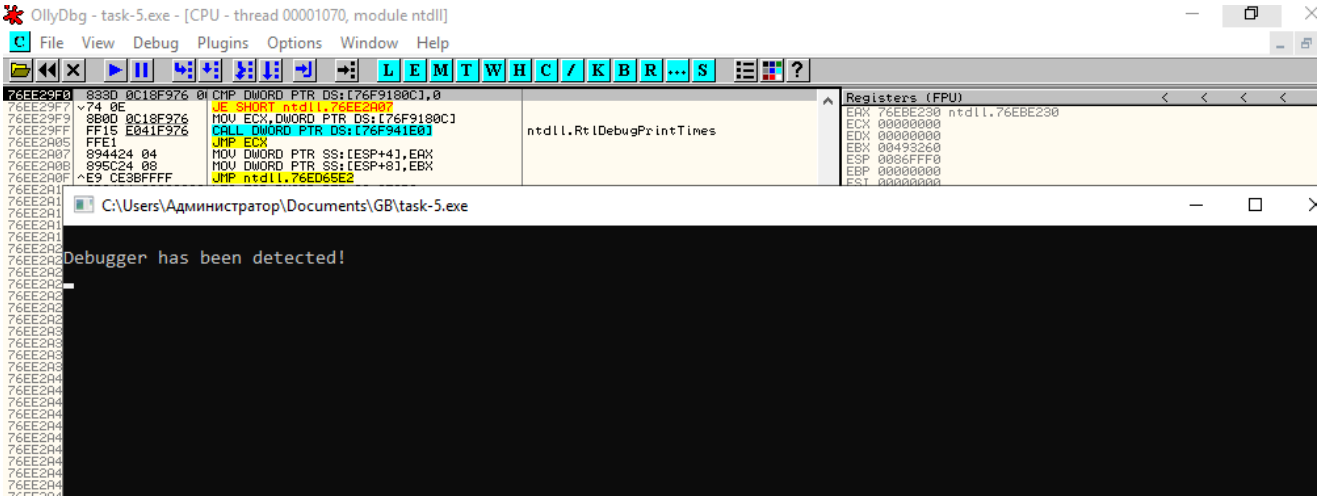
Переходим в фунцию main и ставим точку остановы - break point (F2) 0040105

и запускаем программу (F9)



DebbugerPresent - определение наличия отладчика. Применяем здесь несколько инструкций...

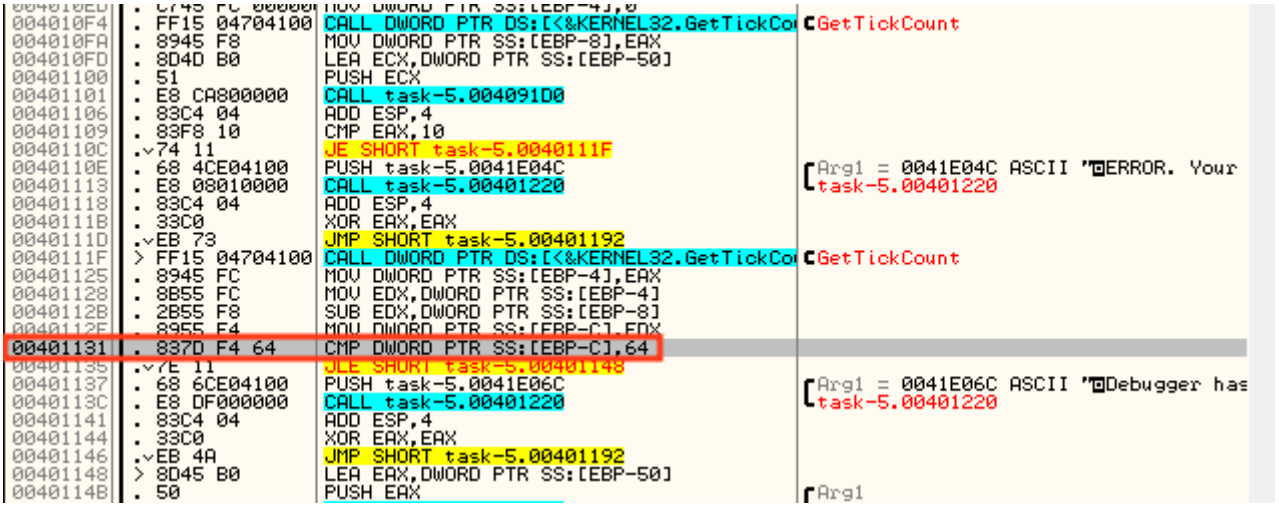




Будем для обхода использовать плагин *HideOD*

Option
-> Auto Run HideOD
-> HideNrDebugBit

Видим, вызывается дважды $GetTickCount$
Проходит проверка на длину ключа *CMP EAX, 10*
Далее видим *CMP , 64* (число 100), т.е. если разница более 100 мили сек., должен сработать отладчик



Enter expression to follow in Dump (local 3)

- видим содержится число $B1770000$, больше 64, следовательно проверку не проходим.

Ставим точку останова на втором $GetTickCount$
Проверяем содержимое ячейки, оно равно 0.

Смотрим регистры.
Для корректировки нужно меньше на 1C байт.
меняем первый байт на E (большое = 14)

License key: **Eaaabbbbccccdddd**
проходит проверку

Использование специальных плагинов
https://github.com/JackAston/OllyDbg1plugins/tree/master/
.DLL скачать и поместить в директорию Plugins
https://at0m2k.narod.ru/soft.html
• ScyllaHide https://github.com/x64dbg/ScyllaHide
• HideOD https://www.aldeid.com/wiki/OllyDbg/HideOD
• HideDebugger https://www.aldeid.com/wiki/OllyDbg/HideDebugger

Выполнил: AndreiM