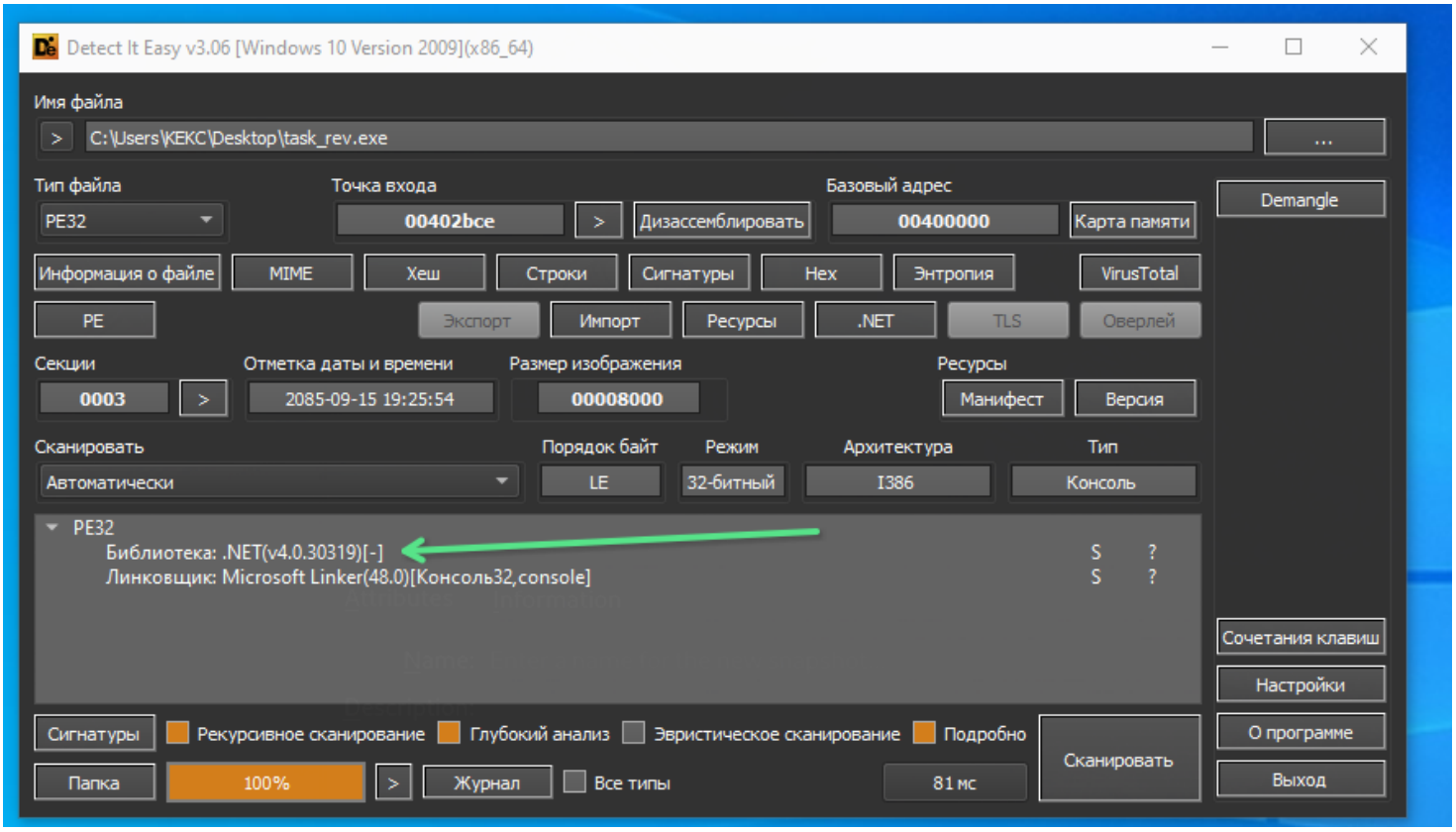
Разминка

Краткая информация
Название: Разминка
Описание: Перед боем нужно и размяться!
Категория: Реверс-инжинирнг
Сложность: Лёгкая
Очки: 150
Подсказка 1: Как насчёт использовать DnSpy и CyberChef
Подсказка 2: Дешифруй какой-то массив через AES

Райтап

1. Изучаем файлы через DIE.



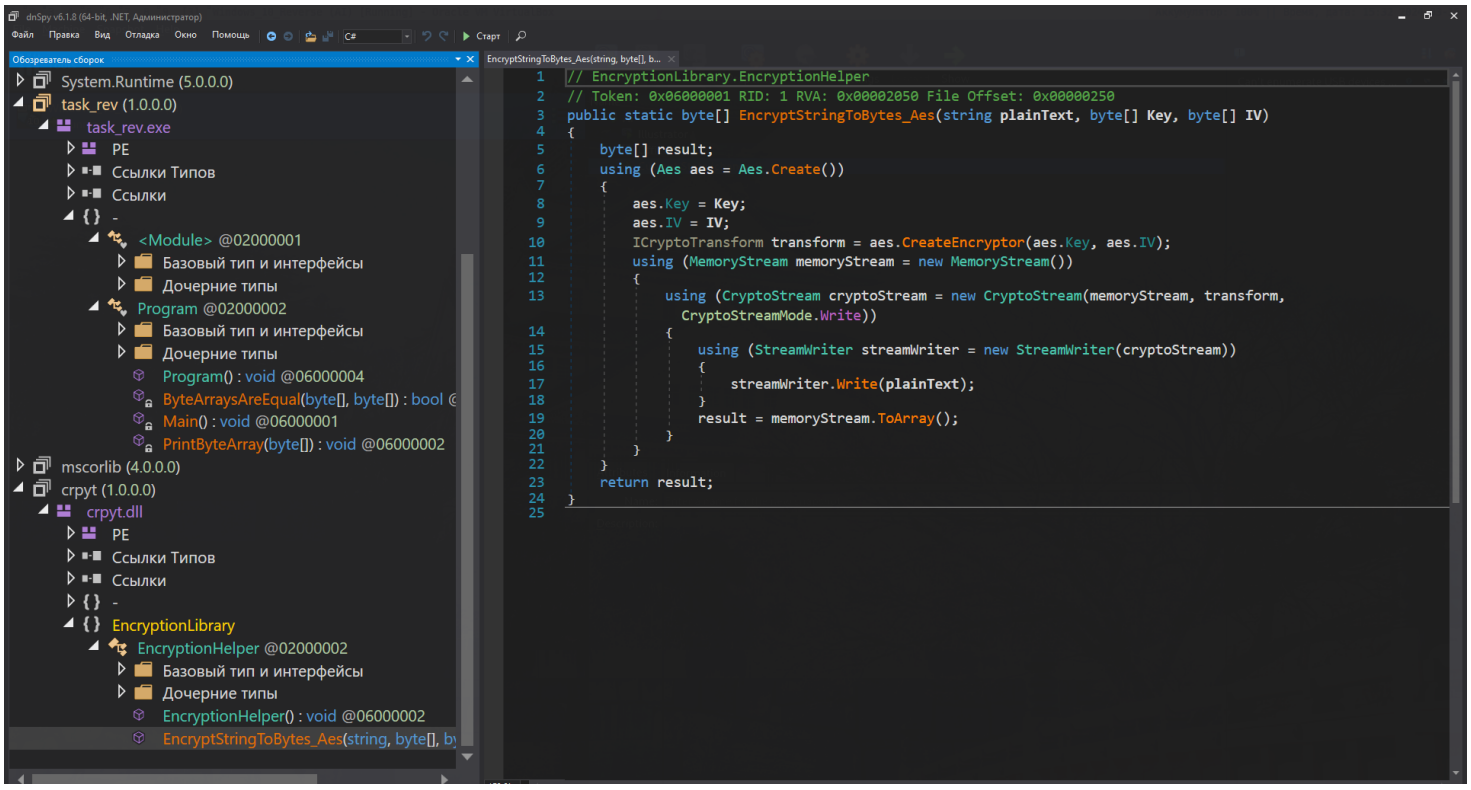
2. Изучаем их в DnSpy.

```
// Program
// Token: 0x06000001 RID: 1 RVA: 0x00002050 File
Offset: 0x00000250
private static void Main() {
  byte[] a = new byte[] {
    90,
    90,
    131,
    173,
    3,
    108,
    139,
    21,
    101,
    136,
    11,
    35,
    101,
    154,
    191,
    222,
    178,
    128,
    45,
    197,
    220,
    65,
    122,
    138,
    18,
    173,
```

```
    210,
    128,
    16,
    101,
    247,
    74
  };
  Console.Write("Введите пароль для шифрования: ");
  string plainText = Console.ReadLine();
  byte[] bytes =
Encoding.UTF8.GetBytes("CODEBY__PASSWORD");
  byte[] bytes2 =
Encoding.UTF8.GetBytes("IV82941840912841");
  byte[] a2 =
EncryptionHelper.EncryptStringToBytes_Aes(plainText,
bytes, bytes2);
  bool flag = Program.ByteArraysAreEqual(a2, a);
  if (flag) {
    Console.WriteLine("Размялся? А теперь серьёзные
таски! :)");
  } else {
    Console.WriteLine("Попробуй ещё, ты точно
справишься! UwU");
  }
  Console.WriteLine("\n(Нажмите Enter для выхода)");
  Console.ReadLine();
}
```

Даже без изучуния DLL можно понять, что ввод юзера шифруется через AES с ключом `"CODEBY__PASSWORD"` и IV `IV82941840912841`. А затем сравнивается с массивом байт `a`.

Сам алгоритм получение зашифрованной строки находится в DLL.



Тогда можно просто дешифровать `a`:

https://cyberchef.org/#recipe=From_Decimal('Comma',false)AES_Decrypt(%7B'option':'UTF8','string':'CODEBY_PASSWORD'%7D,%7B'option':'UTF8','string':'IV82941840912841'%7D,'CBC','Raw','Raw',%7B'option':'Hex','string':''%7D,%7B'option':'Hex','string':''%7D)&input=CQk5MCwKCQk5MCwKCQkxMzEsCgkJMTczLAoJCTMsCgkJMTA4LAoJCTEzOSwKCQkyMSwKCQkxMDEsCgkJMTM2LAoJCTExLAoJCTM1LAoJCTEwMSwKCQkxNTQsCgkJMTkxLAoJCTIyMiwKCQkxNzgsCgkJMTI4LAoJCTQ1LAoJCTE5NywKCQkyMjAsCgkJMTIyLAoJCTEzOCwKCQkxMDEsCgkJMjEwLAoJCTEyOCwKCQkxNzMsCgkJMjEwLAoJCTEyOCwKCQkxNiwKCQkxMDEsCgkJMjQ3LAoJCTc0

Флаг: `CODEBY{p@sSw0rd_1n_EXE_anD_DLL}`