«Тулзы» для Revers'а

Основные инструменты: IDA Pro + Ghidra

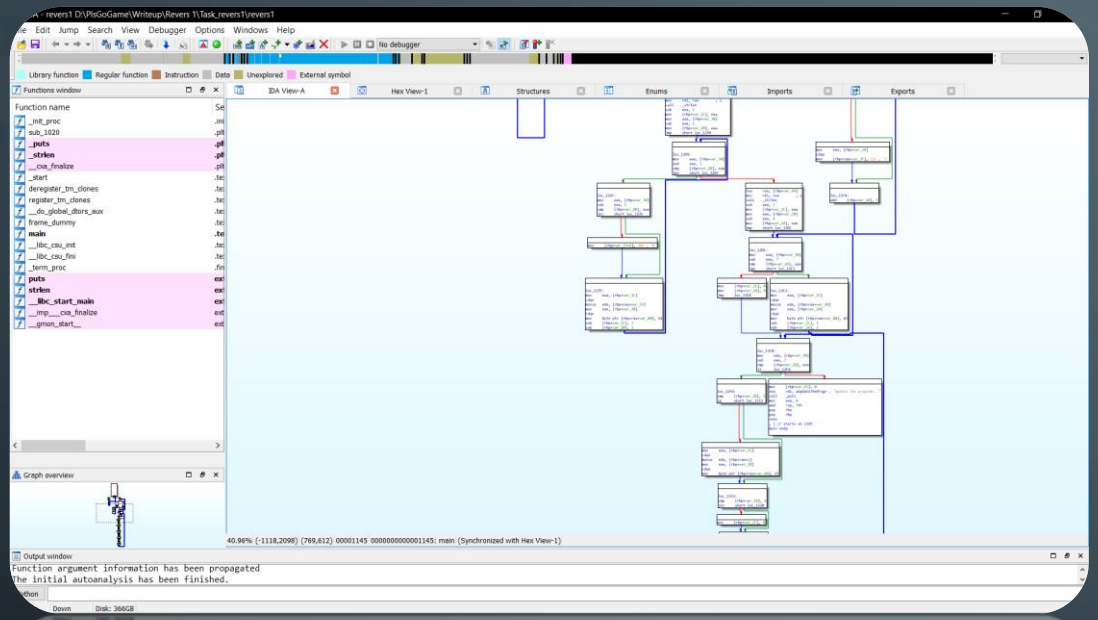
Понятия:

Обратная разработка – процесс, при котором группа разработчиков исследует машинный код готового продукта.

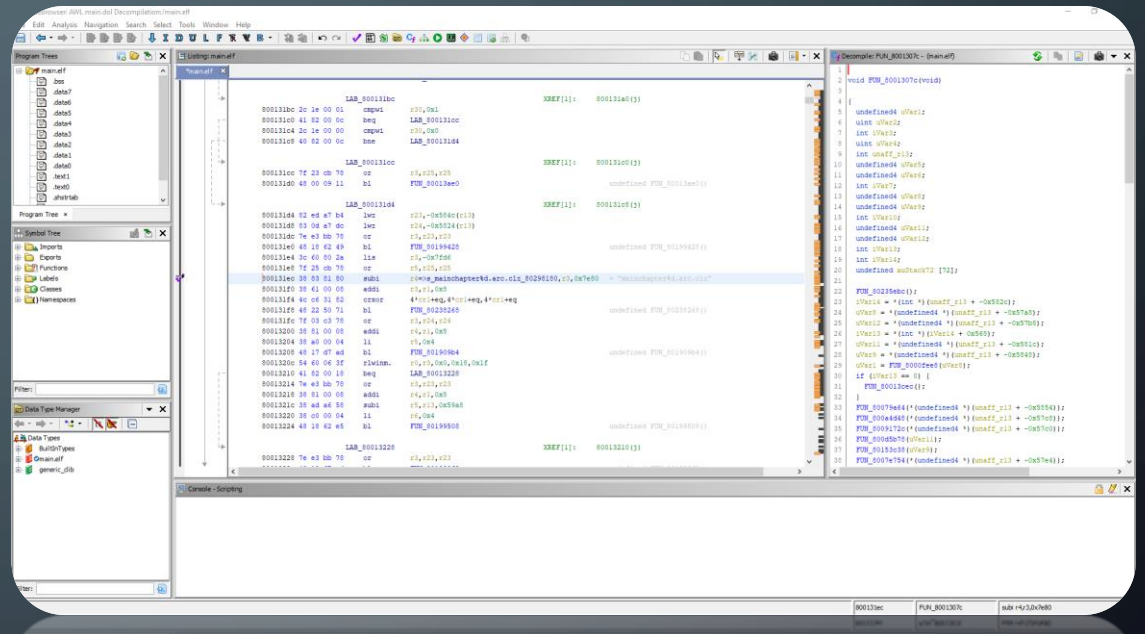
Дизассемблер - транслятор, преобразующий машинный код, объектный файл или библиотечные модули в текст программы на языке ассемблера.

Декомпилятор - это программа, транслирующая исполняемый модуль в эквивалентный исходный код на языке программирования высокого уровня.

Основные инструменты:



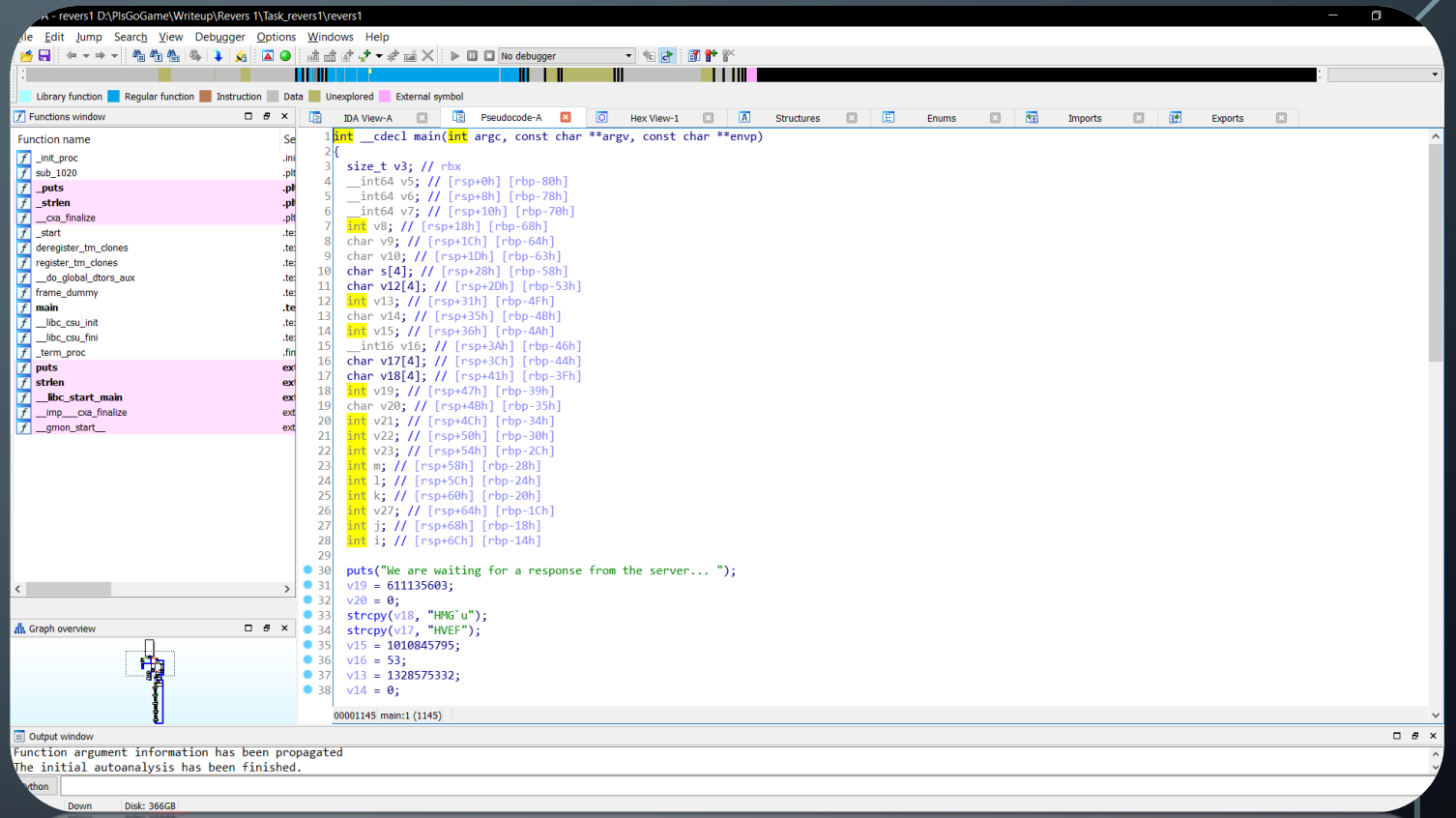
IDA Pro – Hex Rays

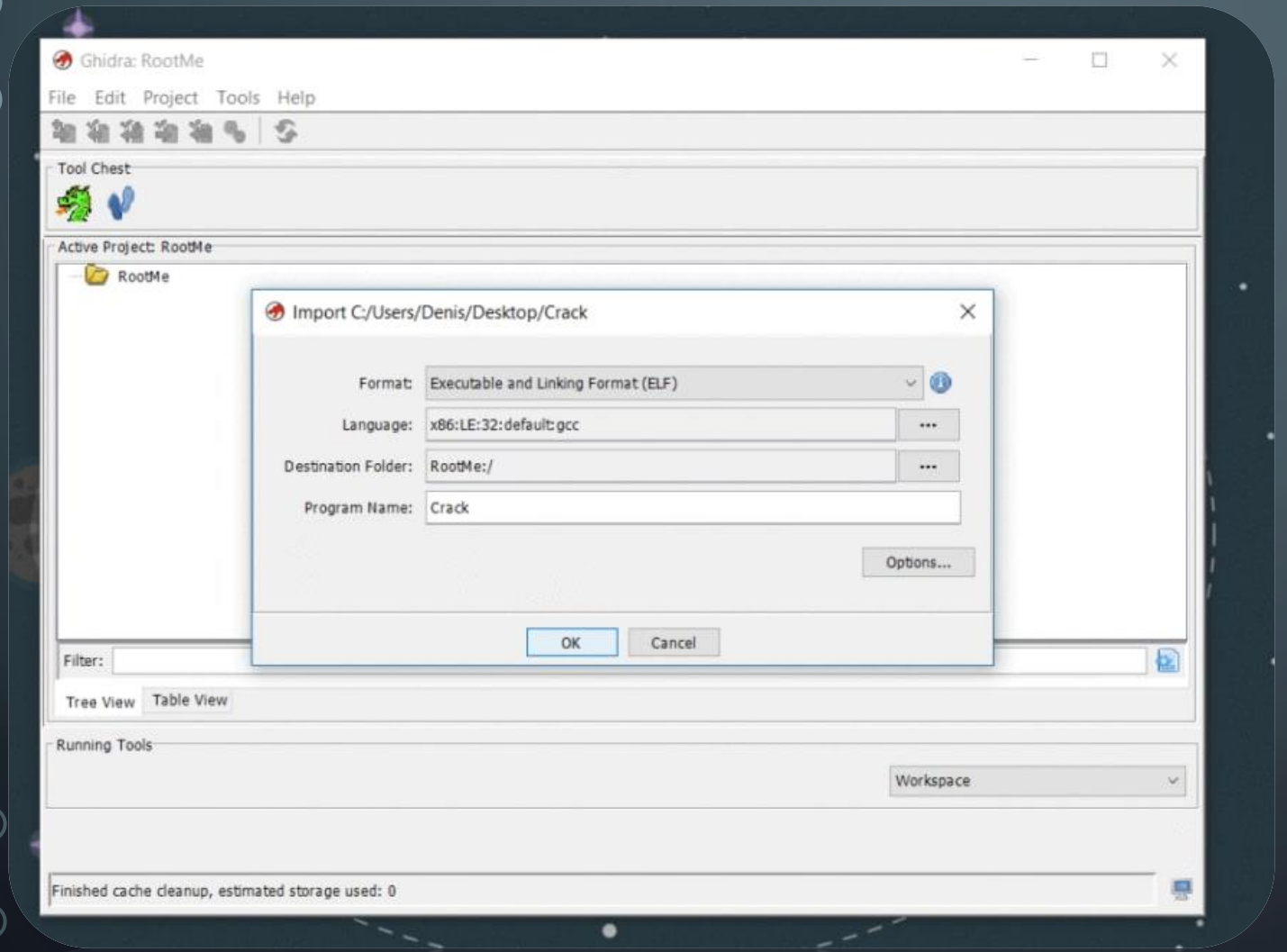


GHIDRA

Преимущества IDA Pro:

1) *Широкий список поддерживаемых форматов;*
2) *Большое количество поддерживаемых процессоров;*
3) *Небольшое количество мусора в выводе;*
4) *Удобный интерфейс.*





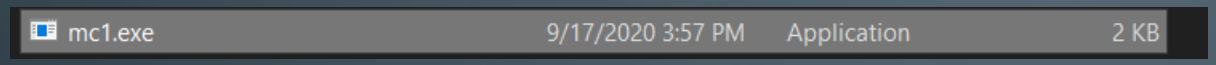
Преимущества GHIDRA:

1) *Регулярность выпуска новых версий;*
2) *Бесплатный доступ;*
3) *Совместная работа над проектом;*
4) *Преимущество в реверсе IoT-устройств.*

DEMO:

Порядок действий:

1) *У нас есть исполняемый файл .exe*



2) *Отправляем его в IDA*

```
1  void __noreturn start()
2  {
3    int v0; // eax
4    int v1; // [esp+0h] [ebp-14h]
5    int Code; // [esp+4h] [ebp-10h]
6    int v3; // [esp+8h] [ebp-Ch]
7    int v4; // [esp+Ch] [ebp-8h]
8    int v5; // [esp+10h] [ebp-4h]
9
10   v1 = 0;
11   controlfp(0x10000u, 0x30000u);
12   _set_app_type(1);
13   _getmainargs(&v5, &v4, &v3, 0, &v1);
14   v0 = sub_401000();
15   Code = v0;
16   exit(v0);
17 }
```

3) *Просматриваем функции*

4) *Находим флаг*

```
.data:00402016 aS              db '%s',0               ; DATA XREF: sub_401000+1F↑o
.data:00402019 ; char Str2[]
.data:00402019 Str2            db 'f1rst_FLAG',0       ; DATA XREF: sub_401000+2D↑o
.data:00402024 ; char aYesCorrectFlag[]
.data:00402024 aYesCorrectFlag db 'Yes! Correct flag is %s',0Ah,0
.data:00402024                                         ; DATA XREF: sub_401000+52↑o
```

Спасибо за внимание!