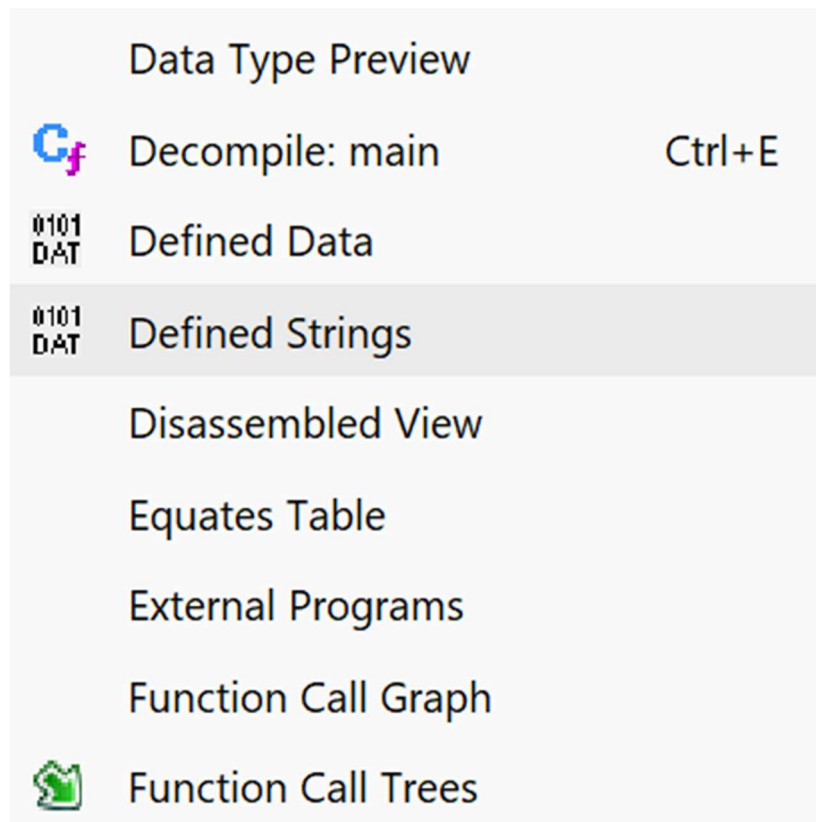


Запускаем программу в Ghidra. Попробую изменить подход к анализу, и не запускать программу в самом начале.

Посмотрю, какие вообще строки содержатся в бинарнике



Видим стандартные сообщения

00488000	secret123	"secret123"	ds
0048800a	Enter passwo...	"Enter passw...	ds
0048801b	Correct pass...	"Correct pass...	ds
0048802d	Incorrect pas...	"Incorrect pa...	ds
00488041	pause	"pause"	ds

И одно интересное – secret123

Можно уже понять по смыслу строки, что это наверняка и есть пароль, тем более что можно сразу его попробовать ввести и получить строку Correct password

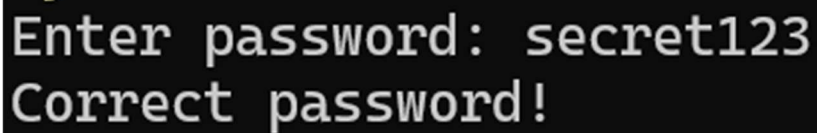
Но посмотрим внутрь функции, которая эти строки использует

```

std::string::string(pwd,"secret123");
std::allocator<char>::~~allocator();
std::operator<<(&std::cout,"Enter password: ",output);
std::getline<>(&std::cin,input);
status = std::operator==(input,pwd);
if ((char)status == '\0') {
    output = std::operator<<(&std::cout,"Incorrect password!",output);
    std::ostream::operator<<(output,std::endl<>);
}
else {
    output = std::operator<<(&std::cout,"Correct password!",output);
    std::ostream::operator<<(output,std::endl<>);
}

```

Да, изначальное предположение оказалось точно достоверным – secret123 и есть искомый пароль



```

Enter password: secret123
Correct password!

```