В этот раз я решил сначала посмотреть на дизассемблированный код и провести статический анализ. Надо приучать себя к тому, что нельзя сходу запускать никакое ПО на неизолированной машине, особенно на своей основной (пусть мы и понимаем, что задачи учебные и это не малварь)

Нашел практически сразу main()

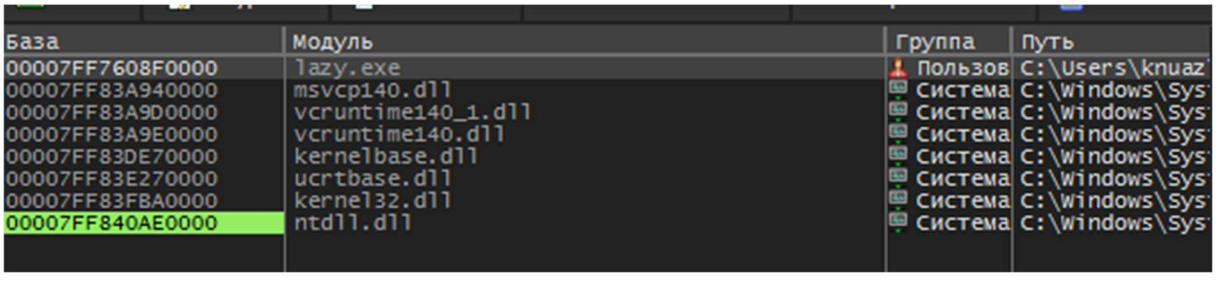
И взгляд зацепился за следующие несколько конструкций:

```
hFindFile = FindFirstFileA("???.jpeg",&local_198);
if (hFindFile == (HANDLE)0xffffffffffffffff) {
  FUN_140012410((basic_ostream<> *)cerr_exref,"umm....try again\n");
  pFVar27 = (FILE *)local_310[0]._ptr;
}

 if (((bVar18 == 0) || (bVar19 == 0)) || (bVar25 == 0)) {
   FUN_140012410((basic_ostream<> *)cerr_exref,"umm....try again\n");
   uVar24 = local_310[0]._24_8_;
   pFVar27 = (FILE *)local_310[0]._ptr;
 }

if ((local_1d8._base == pcVar23) &&
   ((local_1d8._base == (char *)0x0 ||
    (iVar14 = memcmp(pFVar20,pFVar22,(size_t)local_1d8._base), iVar14 == 0)))) {
  pcVar23 = "dayummm\n";
}
else {
  pcVar23 = "umm....try again\n";
}

pbVar17 = FUN_140012410((basic_ostream<> *)cerr_exref,"umm....try again");
pauVar21 = (undefined1 (*) [32])&local_200;
if (0xf < local_1e8) {
  pauVar21 = local_200;
}
```

Выглядит так, что сначала программа пытается посмотреть, есть ли в её директории файл формата .jpeg, а потом уже проверяет название.

Посмотрим что происходит в рантайме

Перейдем в модуль .exe



Найдем в нём ссылки на строки

```
00007FF760901F5F  lea rax,qword ptr ds:[7FF760906960]   00007FF760906960  "can't fopen"
00007FF760902041  lea rdx,qword ptr ds:[7FF760907098]   00007FF760907098  "umm....try again"
00007FF760902295  lea rdx,qword ptr ds:[7FF7609070B0]   00007FF7609070B0  "dayummm\n"
00007FF76090229E  lea rdx,qword ptr ds:[7FF760907080]   00007FF760907080  "umm....try again\n"
00007FF7609022FF  lea rdx,qword ptr ds:[7FF760907080]   00007FF760907080  "umm....try again\n"
00007FF76090231C  lea rdx,qword ptr ds:[7FF760907080]   00007FF760907080  "umm....try again\n"
```

И на требуемые нам поставим брейкпоинты по адресам

```
00007FF760901F5F  lea rax,qword ptr ds:[7FF760906960]   00007FF760906960  "can't fopen"
00007FF760902041  lea rdx,qword ptr ds:[7FF760907098]   00007FF760907098  "umm....try again"
00007FF760902295  lea rdx,qword ptr ds:[7FF7609070B0]   00007FF7609070B0  "dayummm\n"
00007FF76090229E  lea rdx,qword ptr ds:[7FF760907080]   00007FF760907080  "umm....try again\n"
00007FF7609022FF  lea rdx,qword ptr ds:[7FF760907080]   00007FF760907080  "umm....try again\n"
00007FF76090231C  lea rdx,qword ptr ds:[7FF760907080]   00007FF760907080  "umm....try again\n"
```

На всякий случай поставим брейкпоинт на cant fopen

Видим раз:

```
RAX   0000000000000001
RBX   000000000000000F
RCX   0000000539AFFC30   "~~~"
RDX   00007FF760907080   "umm....try again\n"
RBP   0000000539AFFBB0
RSP   0000000539AFFAB0
RSI   00000000007E7E7E
RDI   0000000000636261
```

Вроде как вот оно и название, но надо удостовериться – проверок несколько, попробуем изменить один символ на символ из этой строки.

```
RAX   0000000000000001
RBX   000000000000000F
RCX   00000029AF97F971   "~~"
RDX   FFFFFFFFFFFFFEC8
RBP   00000029AF97F8F0
RSP   00000029AF97F7F0   "Рщ-Ї)"
RSI   00000000007E7E7E
RDI   000000000063627E

R8    0000000000000002
R9    00007FF83A9F09DF   vcruntime140.00007FF83A9F09DF
R10   00007FF83A9E0000   "MZђ"
R11   000000000000007E   '~'
R12   00000000011966CD
R13   0000000000000000
R14   000000000000000F
R15   0000000000000001
```

Наверное, я где-то пропустил конструкцию сравнения, надо подняться повыше вывода строк, на которые я ставил брейкпоинты.

```
00007FF760902276  4C:8B85 90000000  mov r8,qword ptr ss:[rbp+90]   moves data from src to ds
00007FF76090227D  6648:0F7EF0       movq rax,xmm6                 move quadword
00007FF760902282  4C:3BC0           cmp r8,rax                    compare two operands
00007FF760902285  75 17             jne lazy.7FF76090229E         jump short if not equal/r
```

```
RAX   0000000000000003
RBX   000000000000000F
RCX   00000051D9CFF750   "~~~"
RDX   00000051D9CFF618   "~bc"
```

Вот оно! Требуемое название файла – “~~~.jpeg”