

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего
образования
**«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)**

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
КАФЕДРА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Отчет по домашнему заданию № 1

Выполнила: студентка 4 курса
Группы 171-341
Решетникова Дарья Алексеевна

Преподаватель:
Недогарок Антон Александрович

Куратор проекта: _____ / _____, _____ /
подпись ФИО, уч. звание и степень

Студент: _____ / _____, _____ /
подпись ФИО, группа

Москва 2020 г.

Вариант №13

DOS-заглушка. (границы начала и конца)

HxD - [D:\Krita_x64_Rus_Setup.exe]

Файл Правка Поиск Вид Анализ Инструменты Окно Справка

16 Windows (ANSI) hex

Krita_x64_Rus_Setup.exe

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Текст декодирован
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZб.....ая..
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	ё.....@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	C8	00	00	00И...
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	..е..р.Н!ё.LH!Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode....\$.....
00000080	AD	31	38	81	E9	50	56	D2	E9	50	56	D2	E9	50	56	D2	.18ГйPVTйPVTйPVT
00000090	2A	5F	09	D2	EB	50	56	D2	E9	50	57	D2	4D	50	56	D2	*..ТлPVTйPWTMPVT
000000A0	2A	5F	0B	D2	E6	50	56	D2	BD	73	66	D2	E3	50	56	D2	*..ТжPVTSSfTrPVT
000000B0	2E	56	50	D2	E8	50	56	D2	52	69	63	68	E9	50	56	D2	.VPтиPVTRichйPVT
000000C0	00	00	00	00	00	00	00	00	50	45	00	00	4C	01	05	00PE...L...
000000D0	ED	D4	F6	5D	00	00	00	00	00	00	00	00	E0	00	0F	01	н#ц].....а...
000000E0	0B	01	06	00	00	66	00	00	00	2A	02	00	00	08	00	00f...*.....
000000F0	0D	35	00	00	00	10	00	00	00	80	00	00	00	00	40	00	.5.....Ъ.....@.
00000100	00	10	00	00	00	02	00	00	04	00	00	00	06	00	00	00
00000110	04	00	00	00	00	00	00	00	00	80	06	00	00	04	00	00Ъ.....
00000120	FF	EB	EF	07	02	00	40	85	00	00	10	00	00	10	00	00	ялп...@.....
00000130	00	00	10	00	00	10	00	00	00	00	00	00	10	00	00	00
00000140	00	00	00	00	00	00	00	00	04	85	00	00	A0	00	00	00
00000150	00	10	06	00	80	65	00	00	00	00	00	00	00	00	00	00Ъе.....
00000160	C0	C8	EF	07	E0	1E	00	00	00	00	00	00	00	00	00	00	АИп.а.....
00000170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001A0	00	80	00	00	AC	02	00	00	00	00	00	00	00	00	00	00	.Ъ...~.....
000001B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001C0	2E	74	65	78	74	00	00	00	00	7B	64	00	00	10	00	00	.text...{d.....
000001D0	00	66	00	00	00	04	00	00	00	00	00	00	00	00	00	00	.f.....
000001E0	00	00	00	00	20	00	00	60	2E	72	64	61	74	61	00	00`..rdata..
000001F0	84	13	00	00	00	80	00	00	00	14	00	00	00	6A	00	00Ъ.....j..
00000200	00	00	00	00	00	00	00	00	00	00	00	00	40	00	00	40@...@
00000210	2E	64	61	74	61	00	00	58	03	02	00	00	A0	00	00	00	.data...X....
00000220	00	06	00	00	00	7E	00	00	00	00	00	00	00	00	00	00~.....
00000230	00	00	00	00	40	00	00	C0	2E	6E	64	61	74	61	00	00@...A.ndata..
00000240	00	60	03	00	00	B0	02	00	00	00	00	00	00	00	00	00	`.....

PE-заголовок (дополнительный). DllCharacteristics (значение + расшифровка)

HxD - [D:\Krita_x64_Rus_Setup.exe]

Файл Правка Поиск Вид Анализ Инструменты Окно Справка

16 Windows (ANSI) hex

Krita_x64_Rus_Setup.exe

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Текст декодирован
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZб.....ая..
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	ё.....@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	C8	00	00	00И...
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	..е..р.Н!ё.LH!Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode....\$.....
00000080	AD	31	38	81	E9	50	56	D2	E9	50	56	D2	E9	50	56	D2	.18ГйPVTйPVTйPVT
00000090	2A	5F	09	D2	EB	50	56	D2	E9	50	57	D2	4D	50	56	D2	*..ТлPVTйPWTMPVT
000000A0	2A	5F	0B	D2	E6	50	56	D2	BD	73	66	D2	E3	50	56	D2	*..ТжPVTSSfTrPVT
000000B0	2E	56	50	D2	E8	50	56	D2	52	69	63	68	E9	50	56	D2	.VPтиPVTRichйPVT
000000C0	00	00	00	00	00	00	00	00	50	45	00	00	4C	01	05	00PE...L...
000000D0	ED	D4	F6	5D	00	00	00	00	00	00	00	00	E0	00	0F	01	н#ц].....а...
000000E0	0B	01	06	00	00	66	00	00	00	2A	02	00	00	08	00	00f...*.....
000000F0	0D	35	00	00	00	10	00	00	00	80	00	00	00	00	40	00	.5.....Ъ.....@.
00000100	00	10	00	00	00	02	00	00	04	00	00	00	06	00	00	00
00000110	04	00	00	00	00	00	00	00	00	80	06	00	00	04	00	00Ъ.....
00000120	FF	EB	EF	07	02	00	40	85	00	00	10	00	00	10	00	00	ялп...@.....
00000130	00	00	10	00	00	10	00	00	00	00	00	00	10	00	00	00
00000140	00	00	00	00	00	00	00	00	04	85	00	00	A0	00	00	00
00000150	00	10	06	00	80	65	00	00	00	00	00	00	00	00	00	00Ъе.....
00000160	C0	C8	EF	07	E0	1E	00	00	00	00	00	00	00	00	00	00	АИп.а.....

От 0B 01 смещение (dec) 70.

Расшифровка:

Специальные редакторы

Анализ данных

◀ ▶ 🔍

Двоичный (8 бит)	01000000
Int8	перейти к: 40
UInt8	перейти к: 40
Int16	перейти к: -7AC0
UInt16	перейти к: 8540
Int24	перейти к: Недействительно
UInt24	перейти к: Недействительно
Int32	перейти к: Недействительно
UInt32	перейти к: Недействительно
Int64	перейти к: Недействительно
UInt64	перейти к: Недействительно
AnsiChar / char8_t	@
WideChar / char16_t	𐤀
Точка кода UTF-8	@ (U+0040)
Single (float32)	Недействительно
Double (float64)	Недействительно
OLETIME	Недействительно
FILETIME	Недействительно
Дата DOS	Недействительно
Время DOS	16:42:00
Время и дата DOS	Недействительно
time_t (32-бит)	Недействительно
time_t (64-бит)	Недействительно
GUID	Недействительно
Дизассемблирование (x86-16)	inc ax
Дизассемблирование (x86-32)	inc eax
Дизассемблирование (x86-64)	test [rax],eax

Порядок байт
☒ Little endian ☐ Big endian

☒ Показывать целые числа в hex-виде

0x8000

Terminal Server aware.

PE-заголовок (дополнительный). BaseOfCode (значение)

File Edit View Analysis Instruments Window Help

16 Windows (ANSI) hex

Krita_x64_Rus_Setup.exe

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Текст декодирован
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	МЗъ.....ая..
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	ё.....ё.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00И.....
00000030	00	00	00	00	00	00	00	00	00	00	00	00	C9	00	00	00Д.....
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68ё.г.Нё.ЛHth
00000050	68	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program cannot
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	be run in DOS
00000070	6D	6F	64	65	2E	0D	0A	24	00	00	00	00	00	00	00	00	mode.....ё.....
00000080	AD	31	38	81	E9	50	56	D2	E9	50	56	D2	E9	50	56	D2	...18йPVTйPVTйPVT
00000090	2A	5F	09	D2	EB	50	56	D2	E9	50	57	D2	4D	50	56	D2	*...TлPVTйPVTйPVT
000000A0	2A	5F	0B	D2	E6	50	56	D2	BD	73	66	D2	E3	50	56	D2	*...TлPVTйSsfTлPVT
000000B0	2E	56	50	D2	E8	50	56	D2	52	69	63	68	E9	50	56	D2	...VPтйPVTриchйPVT
000000C0	00	00	00	00	00	00	00	00	50	45	00	00	4C	01	05	00FE...L...
000000D0	ED	D4	F6	5D	00	00	00	00	00	00	00	00	00	00	0F	01	нщ].....а...
000000E0	0B	01	06	00	00	66	00	00	00	2A	02	00	00	08	00	00ё.....*
000000F0	0D	35	00	00	10	00	00	00	80	00	00	00	00	40	00	00	...5.....ъ.....ё.
00000100	00	10	00	00	00	02	00	00	04	00	00	00	06	00	00	00ё.....
00000110	0F	00	00	00	00	00	00	00	80	06	00	00	00	04	00	00ё.....
00000120	FF	EB	EF	07	02	00	00	00	40	85	00	10	00	00	10	00	ялп...@.....
00000130	00	00	10	00	00	10	00	00	00	00	00	10	00	00	00	00
00000140	00	00	00	00	00	00	00	00	04	85	00	00	A0	00	00	00
00000150	00	10	06	00	80	65	00	00	00	00	00	00	00	00	00	00	...ё.....
00000160	C0	C8	EF	07	E0	1E	00	00	00	00	00	00	00	00	00	00	АЙп.а.....
00000170	00	00	00	00													

РЕ-заголовок (основной). *NumberOfSections* (значение)

[illegible]

Таблица секций. `.data`. `VirtualSize`, `VirtualAddress`, `SizeOfRawData`, `PointerToRawData` (значения + проверка по файлу `SizeOfRawData`, `PointerToRawData`).

```

HxD - [D:\Krita_x64_Rus_Setup.exe]
Файл Правка Поиск Вид Анализ Инструменты Окно Справка
16 Windows (ANSI) hex
Krita_x64_Rus_Setup.exe
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Текст декодирован
00000000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZб.....яя..
00000010 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ё.....@.....
00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000030 00 00 00 00 00 00 00 00 00 00 00 00 C8 00 00 00 .....И...
00000040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ..e..r.H!ё.LH!Th
00000050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno
00000060 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS
00000070 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode....$.
00000080 AD 31 38 81 E9 50 56 D2 E9 50 56 D2 E9 50 56 D2 .18ГйРVТйРVТйРVТ
00000090 2A 5F 09 D2 EB 50 56 D2 E9 50 57 D2 4D 50 56 D2 *_.ТлРVТйРWТлРVТ
000000A0 2A 5F 0B D2 E6 50 56 D2 BD 73 66 D2 E3 50 56 D2 *_.ТжРVТSsfТлРVТ
000000B0 2E 56 50 D2 E8 50 56 D2 52 69 63 68 E9 50 56 D2 .VРТлРVТRichйРVТ
000000C0 00 00 00 00 00 00 00 00 50 45 00 00 4C 01 05 00 .....FE..L...
000000D0 ED D4 F6 5D 00 00 00 00 00 00 00 00 E0 00 0F 01 нѳu].....a...
000000E0 0B 01 06 00 00 66 00 00 00 2A 02 00 00 08 00 00 .....f...*.
000000F0 0D 35 00 00 00 10 00 00 00 80 00 00 00 00 40 00 .5.....Ъ.....@.
00000100 00 10 00 00 00 02 00 00 04 00 00 00 06 00 00 00 .....
00000110 04 00 00 00 00 00 00 00 80 06 00 00 04 00 00 .....Ъ.....
00000120 FF EB EF 07 02 00 40 85 00 00 10 00 00 10 00 00 ялп...@.....
00000130 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 .....
00000140 00 00 00 00 00 00 00 00 04 85 00 00 A0 00 00 00 .....
00000150 00 10 06 00 80 65 00 00 00 00 00 00 00 00 00 00 ....Ъe.....
00000160 C0 C8 EF 07 E0 1E 00 00 00 00 00 00 00 00 00 00 АИп.a.....
00000170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000001A0 00 80 00 00 AC 02 00 00 00 00 00 00 00 00 00 00 .Ъ..-.....
000001B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000001C0 2E 74 65 78 74 00 00 00 7B 64 00 00 00 10 00 00 .text...(d....
000001D0 00 66 00 00 00 04 00 00 00 00 00 00 00 00 00 00 .f.....
000001E0 00 00 00 00 20 00 00 60 2E 72 64 61 74 61 00 00 ....`..rdata..
000001F0 84 13 00 00 00 80 00 00 00 14 00 00 00 6A 00 00 „....Ъ.....j..
00000200 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 .....@...@...
00000210 2E 64 61 74 61 00 00 00 58 03 02 00 00 A0 00 00 .data...X....
00000220 00 06 00 00 00 7E 00 00 00 00 00 00 00 00 00 00 .....~.....
00000230 00 00 00 00 40 00 00 C0 2E 6E 64 61 74 61 00 00 ....@...A.ndata..
00000240 00 60 03 00 00 B0 02 00 00 00 00 00 00 00 00 00 .`...°.....
00000250 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 C0 .....Ъ..A
00000260 2E 72 73 72 63 00 00 80 65 00 00 00 10 06 00 .rsrc...Ъe.....
00000270 00 66 00 00 00 84 00 00 00 00 00 00 00 00 00 00 .f.....
00000280 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 ....@...@.....

```

Проверка:

.data

`VirtualSize` 20358

`VirtualAddress` A000

`SizeOfRawData` 600

`PointerToRawData` 7E00

Переходим по `PointerToRawData` (7E00):

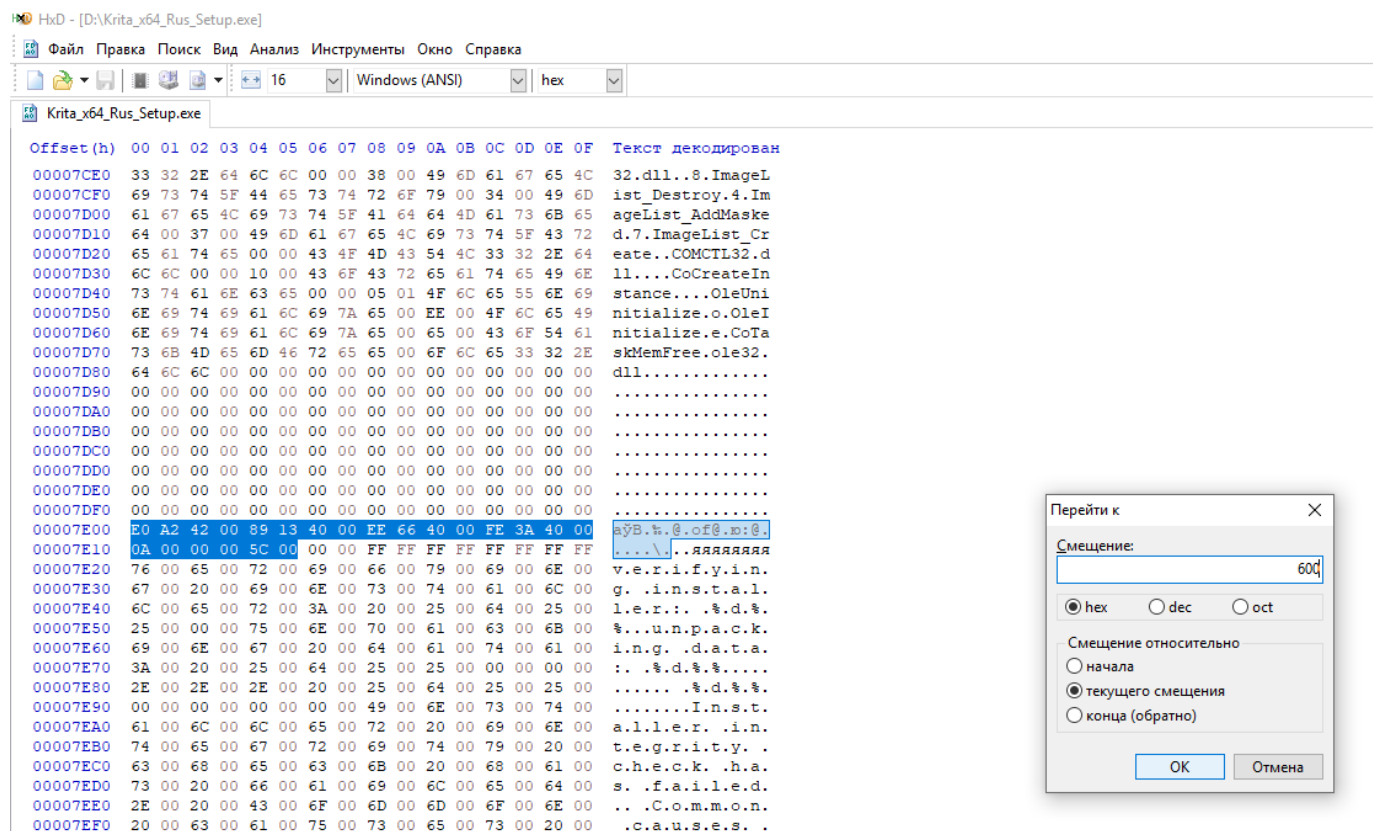
HxD - [D:\Krita_x64_Rus_Setup.exe]

Файл Правка Поиск Вид Анализ Инструменты Окно Справка																	
Krita_x64_Rus_Setup.exe																	
Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Текст декодирован
00007D70	73	6B	4D	65	6D	46	72	65	65	00	6F	6C	65	33	32	2E	skMemFree.ole32.
00007D80	64	6C	6C	00	00	00	00	00	00	00	00	00	00	00	00	00	dll.....
00007D90	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00007DA0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00007DB0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00007DC0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00007DD0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00007DE0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00007DF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00007E00	E0	A2	42	00	89	13	40	00	EE	66	40	00	FE	3A	40	00	аўВ.к. @.of @.м: @.
00007E10	0A	00	00	00	5C	00	00	00	FF	FF	FF	FF	FF	FF	FF	FF\...яяяяяяяя
00007E20	76	00	65	00	72	00	69	00	66	00	79	00	69	00	6E	00	v.e.r.i.f.y.i.n.
00007E30	67	00	20	00	69	00	6E	00	73	00	74	00	61	00	6C	00	g. .i.n.s.t.a.l.
00007E40	6C	00	65	00	72	00	3A	00	20	00	25	00	64	00	25	00	l.e.r.:. %.d.%.
00007E50	25	00	00	00	75	00	6E	00	70	00	61	00	63	00	6B	00	%.u.n.p.a.c.k.
00007E60	69	00	6E	00	67	00	20	00	64	00	61	00	74	00	61	00	i.n.g. .d.a.t.a.
00007E70	3A	00	20	00	25	00	64	00	25	00	25	00	00	00	00	00	:. %.d.%.%.
00007E80	2E	00	2E	00	2E	00	20	00	25	00	64	00	25	00	25	00 %.d.%.%.
00007E90	00	00	00	00	00	00	00	00	49	00	6E	00	73	00	74	00I.n.s.t.
00007EA0	61	00	6C	00	6C	00	65	00	72	00	20	00	69	00	6E	00	a.l.l.e.r. .i.n.
00007EB0	74	00	65	00	67	00	72	00	69	00	74	00	79	00	20	00	t.e.g.r.i.t.y. .
00007EC0	63	00	68	00	65	00	63	00	6B	00	20	00	68	00	61	00	c.h.e.c.k. .h.a.
00007ED0	73	00	20	00	66	00	61	00	69	00	6C	00	65	00	64	00	s. .f.a.i.l.e.d.
00007EE0	2E	00	20	00	43	00	6F	00	6D	00	6D	00	6F	00	6E	00	.. .C.o.m.m.o.n.
00007EF0	20	00	63	00	61	00	75	00	73	00	65	00	73	00	20	00	.c.a.u.s.e.s. .
00007F00	69	00	6E	00	63	00	6C	00	75	00	64	00	65	00	0A	00	i.n.c.l.u.d.e...
00007F10	69	00	6E	00	63	00	6F	00	6D	00	70	00	6C	00	65	00	i.n.c.o.m.p.l.e.
00007F20	74	00	65	00	20	00	64	00	6F	00	77	00	6E	00	6C	00	t.e. .d.o.w.n.l.
00007F30	6F	00	61	00	64	00	20	00	61	00	6E	00	64	00	20	00	p.a.d. .a.n.d. .
00007F40	64	00	61	00	6D	00	61	00	67	00	65	00	64	00	20	00	d.a.m.a.g.e.d. .
00007F50	6D	00	65	00	64	00	69	00	61	00	2E	00	20	00	43	00	m.e.d.i.a... .C.
00007F60	6F	00	6E	00	74	00	61	00	63	00	74	00	20	00	74	00	p.n.t.a.c.t. .t.
00007F70	68	00	65	00	0A	00	69	00	6E	00	73	00	74	00	61	00	h.e...i.n.s.t.a.
00007F80	6C	00	6C	00	65	00	72	00	27	00	73	00	20	00	61	00	l.l.e.r.'s. .a.
00007F90	75	00	74	00	68	00	6F	00	72	00	20	00	74	00	6F	00	u.t.h.o.r. .t.o.
00007FA0	20	00	6F	00	62	00	74	00	61	00	69	00	6E	00	20	00	.o.b.t.a.i.n. .
00007FB0	61	00	20	00	6E	00	65	00	77	00	20	00	63	00	6F	00	a. .n.e.w. .c.o.
00007FC0	70	00	79	00	2E	00	0A	00	0A	00	4D	00	6F	00	72	00	p.y.....M.o.r.
00007FD0	65	00	20	00	69	00	6E	00	66	00	6F	00	72	00	6D	00	e. .i.n.f.o.r.m.
00007FE0	61	00	74	00	69	00	6F	00	6E	00	20	00	61	00	74	00	a.t.i.o.n. .a.t.
00007FF0	3A	00	0A	00	68	00	74	00	74	00	70	00	3A	00	2F	00	:...h.t.t.p.:./.
00008000	2F	00	6E	00	73	00	69	00	73	00	2E	00	73	00	66	00	/n.s.i.s...s.f.
00008010	2E	00	6E	00	65	00	74	00	2F	00	4E	00	53	00	49	00	..n.e.t./N.S.I.
00008020	53	00	5F	00	45	00	72	00	72	00	6F	00	72	00	00	00	S_.E.r.r.o.r...
00008030	45	00	72	00	72	00	6F	00	72	00	20	00	77	00	72	00	E.r.r.o.r. .w.r.
00008040	69	00	74	00	69	00	6E	00	67	00	20	00	74	00	65	00	i.t.i.n.g. .t.e.

[illegible]

Тут что-то начинается.

Далее переходим к `SizeOfRawData`:



После чего перебрасывает в строку 00008400

```
HxD - [D:\Krita_x64_Rus_Setup.exe]
Файл Правка Поиск Вид Анализ Инструменты Окно Справка
16 Windows (ANSI) hex
Krita_x64_Rus_Setup.exe
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Текст декодирован
00008310 65 4B 65 79 45 78 57 00 41 44 56 41 50 49 33 32 eKeyExW.ADVAPI32
00008320 00 00 00 00 47 65 74 55 73 65 72 44 65 66 61 75 ....GetUserDefau
00008330 6C 74 55 49 4C 61 6E 67 75 61 67 65 00 00 00 00 ltUILanguage....
00008340 47 65 74 44 69 73 6B 46 72 65 65 53 70 61 63 65 GetDiskFreeSpace
00008350 45 78 57 00 53 65 74 44 65 66 61 75 6C 74 44 6C ExW.SetDefaultDl
00008360 6C 44 69 72 65 63 74 6F 72 69 65 73 00 00 00 00 lDirectories....
00008370 4B 45 52 4E 45 4C 33 32 00 00 00 00 5C 00 2A 00 KERNEL32....\.*
00008380 2E 00 2A 00 00 00 00 00 6E 00 73 00 61 00 00 00 ..*.....n.s.a...
00008390 0A 5B 00 00 5B 52 65 6E 61 6D 65 5D 0D 0A 00 00 .[.[Rename]....
000083A0 25 6C 73 3D 25 6C 73 0D 0A 00 00 00 2A 00 3F 00 %ls=%ls.....*?.
000083B0 7C 00 3C 00 3E 00 2F 00 22 00 3A 00 00 00 00 00 |.<.>./.".:.....
000083C0 25 00 73 00 25 00 53 00 2E 00 64 00 6C 00 6C 00 %s.%S...d.l.l.
000083D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000083E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000083F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00008400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 06 00 .....
00008410 02 00 00 00 40 00 00 80 03 00 00 00 58 00 00 80 ....@..Ъ...Х..Ъ
00008420 05 00 00 00 A0 00 00 80 0E 00 00 00 70 01 00 80 .... ..Ъ...р..Ъ
00008430 10 00 00 00 88 01 00 80 18 00 00 00 A0 01 00 80 ....€..Ъ... ..Ъ
00008440 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 .....
00008450 6E 00 00 00 B8 01 00 80 00 00 00 00 00 00 00 00 п...ё..Ъ.....
00008460 00 00 00 00 00 00 07 00 01 00 00 00 D0 01 00 80 .....Р..Ъ
00008470 02 00 00 00 E8 01 00 80 03 00 00 00 00 02 00 80 ....и..Ъ.....Ъ
00008480 04 00 00 00 18 02 00 80 05 00 00 00 30 02 00 80 .....Ъ...О..Ъ
00008490 06 00 00 00 48 02 00 80 07 00 00 00 60 02 00 80 ....Н..Ъ...`..Ъ
000084A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 .....
000084B0 66 00 00 00 78 02 00 80 67 00 00 00 90 02 00 80 f...х..Ъg...ђ..Ъ
000084C0 68 00 00 00 A8 02 00 80 69 00 00 00 C0 02 00 80 h...ё..Ъi...А..Ъ
000084D0 6A 00 00 00 D8 02 00 80 6B 00 00 00 F0 02 00 80 j...ш..Ъk...р..Ъ
000084E0 6D 00 00 00 08 03 00 80 6F 00 00 00 20 03 00 80 m.....Ъo... ..Ъ
000084F0 CA 00 00 00 38 03 00 80 CB 00 00 00 50 03 00 80 K...8..ЪЛ...Р..Ъ
00008500 CC 00 00 00 68 03 00 80 CD 00 00 00 80 03 00 80 M...h..ЪH...Ъ..Ъ
00008510 CE 00 00 00 98 03 00 80 CF 00 00 00 B0 03 00 80 O.....ЪП...°..Ъ
00008520 D1 00 00 00 C8 03 00 80 D3 00 00 00 E0 03 00 80 C...И..ЪУ...а..Ъ
00008530 2E 01 00 00 F8 03 00 80 2F 01 00 00 10 04 00 80 ....ш..Ъ/.....Ъ
00008540 30 01 00 00 28 04 00 80 31 01 00 00 40 04 00 80 0...(..Ъl...@..Ъ
00008550 32 01 00 00 58 04 00 80 33 01 00 00 70 04 00 80 2...Х..Ъ3...р..Ъ
00008560 35 01 00 00 88 04 00 80 37 01 00 00 A0 04 00 80 5...€..Ъ7... ..Ъ
00008570 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 .....
00008580 67 00 00 00 B8 04 00 80 00 00 00 00 00 00 00 00 г...ё..Ъ.....
00008590 00 00 00 00 00 00 01 00 01 00 00 00 D0 04 00 80 .....Р..Ъ
000085A0 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 .....
000085B0 01 00 00 00 F8 04 00 80 00 00 00 00 00 00 00 00 ..Ъ
```

До данной позиции шли 0 (тут думаю небольшой сбой из-за выравнивания), но с 00008410 можем отчетливо видеть некую структуру.

PE-заголовок (дополнительный). *SizeOfHeapCommit* (значение)

Файл 0B 01 - PE32:

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Текст декодирован

00000000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZђ.....яя..

00000010 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ё.....ё.....

00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00И.....

00000030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00И.....

00000040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ..е..г.Н!ё.LH!Th

00000050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno

00000060 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS

00000070 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode....\$......

00000080 AD 31 38 81 E9 50 56 D2 E9 50 56 D2 E9 50 56 D2 .18ГйРVТйРVТйРVТ

00000090 2A 5F 09 D2 EB 50 56 D2 E9 50 57 D2 4D 50 56 D2 *_.ТлРVТйРWТМРVТ

000000A0 2A 5F 0B D2 E6 50 56 D2 BD 73 66 D2 E3 50 56 D2 *_.ТлРVТSsfТлРVТ

000000B0 2E 56 50 D2 E8 50 56 D2 52 69 63 68 E9 50 56 D2 .VРТйРVТRchйРVТ

000000C0 00 00 00 00 00 00 00 00 50 45 00 00 4C 01 05 00PE..L...

000000D0 ED D4 F6 5D 00 00 00 00 00 00 00 00 E0 00 0F 01 нфц].....а...

000000E0 0B 01 06 00 00 66 00 00 00 2A 02 00 00 08 00 00f...*.....

000000F0 0D 35 00 00 00 10 00 00 00 80 00 00 00 00 40 00 .5.....Ъ.....ё..

00000100 00 10 00 00 00 02 00 00 04 00 00 00 06 00 00 00Ъ.....

00000110 04 00 00 00 00 00 00 00 00 80 06 00 00 04 00 00Ъ.....

00000120 FF EB EF 07 02 00 40 85 00 00 10 00 10 00 00 00 ялп...@.....

00000130 00 00 10 00 00 10 00 00 00 00 10 00 10 00 00 00SizeOfHeapCommit

00000140 00 00 00 00 00 00 00 00 04 85 00 00 A0 00 00 00а.....

00000150 00 10 06 00 80 65 00 00 00 00 00 00 00 00 00 00Ъе.....

00000160 C0 C8 EF 07 E0 1E 00 00 00 00 00 00 00 00 00 00 АИп.а.....

00000170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00а.....

00000180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00а.....

00000190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00а.....

000001A0 00 80 00 00 AC 02 00 00 00 00 00 00 00 00 00 00 .Ъ...т.....

PE-заголовок (дополнительный). *AddressOfEntryPoint* (значение + проверка по файлу)

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Текст декодирован

00000000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZђ.....яя..

00000010 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ё.....ё.....

00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00И.....

00000030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00И.....

00000040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ..е..г.Н!ё.LH!Th

00000050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno

00000060 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS

00000070 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode....\$......

00000080 AD 31 38 81 E9 50 56 D2 E9 50 56 D2 E9 50 56 D2 .18ГйРVТйРVТйРVТ

00000090 2A 5F 09 D2 EB 50 56 D2 E9 50 57 D2 4D 50 56 D2 *_.ТлРVТйРWТМРVТ

000000A0 2A 5F 0B D2 E6 50 56 D2 BD 73 66 D2 E3 50 56 D2 *_.ТлРVТSsfТлРVТ

000000B0 2E 56 50 D2 E8 50 56 D2 52 69 63 68 E9 50 56 D2 .VРТйРVТRchйРVТ

000000C0 00 00 00 00 00 00 00 00 50 45 00 00 4C 01 05 00PE..L...

000000D0 ED D4 F6 5D 00 00 00 00 00 00 00 00 E0 00 0F 01 нфц].....а...

000000E0 0B 01 06 00 00 66 00 00 00 2A 02 00 00 08 00 00f...*.....

000000F0 0D 35 00 00 00 10 00 00 00 80 00 00 00 00 40 00 .5.....Ъ.....ё..

00000100 00 10 00 00 00 02 00 00 04 00 00 00 06 00 00 00Ъ.....

00000110 04 00 00 00 00 00 00 00 00 80 06 00 00 04 00 00Ъ.....

00000120 FF EB EF 07 02 00 40 85 00 00 10 00 10 00 00 00 ялп...@.....

00000130 00 00 10 00 00 10 00 00 00 00 10 00 10 00 00 00SizeOfHeapCommit

00000140 00 00 00 00 00 00 00 00 04 85 00 00 A0 00 00 00а.....

00000150 00 10 06 00 80 65 00 00 00 00 00 00 00 00 00 00Ъе.....

00000160 C0 C8 EF 07 E0 1E 00 00 00 00 00 00 00 00 00 00 АИп.а.....

00000170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00а.....

00000180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00а.....

00000190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00а.....

000001A0 00 80 00 00 AC 02 00 00 00 00 00 00 00 00 00 00 .Ъ...т.....

000001B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00а.....

Проверка:

0D 35 00 00 = 35 0D 00 00

IDA - Krita_x64_Rus_Setup.exe D:\Krita_x64_Rus_Setup.exe

File Edit Jump Search View Debugger Options Windows Help

Library function Regular function Instruction Data Unexplored External symbol

Functions window

Function name	Segment	Start
sub_402D6C	.text	0000000000402D6C
sub_402D81	.text	0000000000402D81
DialogFunc	.text	0000000000402E60
sub_402EDF	.text	0000000000402EDF
sub_402EFB	.text	0000000000402EFB
sub_402F9D	.text	0000000000402F9D
sub_40323E	.text	000000000040323E
sub_403346	.text	0000000000403346
sub_4034AF	.text	00000000004034AF
sub_4034C5	.text	00000000004034C5
sub_4034DC	.text	00000000004034DC
start	.text	000000000040350D
sub_403A4E	.text	0000000000403A4E
sub_403A90	.text	0000000000403A90
sub_403AAB	.text	0000000000403AAB
sub_403AE0	.text	0000000000403AE0
sub_403AFE	.text	0000000000403AFE
sub_403B40	.text	0000000000403B40
sub_403E16	.text	0000000000403E16
sub_403ECF	.text	0000000000403ECF
sub_403EEE	.text	0000000000403EEE
sub_4043A0	.text	00000000004043A0
sub_4043C7	.text	00000000004043C7
sub_4043E9	.text	00000000004043E9
sub_4043FC	.text	00000000004043FC
sub_404413	.text	0000000000404413
sub_40442E	.text	000000000040442E
sub_4044FD	.text	00000000004044FD
sub_404537	.text	0000000000404537
sub_404586	.text	0000000000404586
sub_404811	.text	0000000000404811
sub_404835	.text	0000000000404835
sub_404871	.text	0000000000404871
sub_404888	.text	0000000000404888

Line 27 of 106

IDA View-A Hex View-1 Structures Enums Imports Exports

Attributes: noreturn

```
public start
start proc near

var_2D4= dword ptr -2D4h
uExitCode= dword ptr -2D0h
TokenHandle= dword ptr -2CCh
Buffer= dword ptr -2C8h
NewState= _TOKEN_PRIVILEGES ptr -2C4h
psfi= SHFILEINFORM ptr -2B4h

sub esp, 2D4h
push ebx
push esi
push edi
push 20h
pop edi
xor ebx, ebx
push 8001h ; uMode
mov [esp+2E4h+uExitCode], ebx
mov [esp+2E4h+var_2D4], offset aErrorWritingTe ; "Error writing temporary file. Make sure"...
mov [esp+2E4h+Buffer], ebx
call ds:SetErrorMode
call ds:GetVersion
and eax, 0BFFFFFFFh
cmp ax, 6
mov dword_42A24C, eax
jz short loc_40355D
```

push ebx
call sub_406834
cmp eax, ebx
jz short loc_40355D

sub_4034C5	.text	00000000004034C5
sub_4034DC	.text	00000000004034DC
start	.text	000000000040350D
sub_403A4E	.text	0000000000403A4E
sub_403A90	.text	0000000000403A90
sub_403AAB	.text	0000000000403AAB

```
; Attributes: noreturn

public start
start proc near

var_2D4= dword ptr -2D4h
uExitCode= dword ptr -2D0h
TokenHandle= dword ptr -2CCh
Buffer= dword ptr -2C8h
NewState= _TOKEN_PRIVILEGES ptr -2C4h
psfi= SHFILEINFORM ptr -2B4h

sub esp, 2D4h
push ebx
push esi
push edi
push 20h
pop edi
xor ebx, ebx
push 8001h ; uMode
mov [esp+2E4h+uExitCode], ebx
mov [esp+2E4h+var_2D4], offset aErrorWritingTe ; "Error writing temporary file. Make sure"...
mov [esp+2E4h+Buffer], ebx
call ds:SetErrorMode
call ds:GetVersion
and eax, 0BFFFFFFFh
cmp ax, 6
mov dword_42A24C, eax
jz short loc_40355D
```

```

.text:0040350C sub_4034DC     endp
.text:0040350C
.text:0040350D ; ===== S U B R O U T I N E =====
.text:0040350D ; Attributes: noreturn
.text:0040350D
.text:0040350D     public start
.text:0040350D start      proc near
.text:0040350D
.text:0040350D var_2D4      = dword ptr -2D4h
.text:0040350D uExitCode    = dword ptr -2D0h
.text:0040350D TokenHandle  = dword ptr -2CCh
.text:0040350D Buffer       = dword ptr -2C8h
.text:0040350D NewState    = _TOKEN_PRIVILEGES ptr -2C4h
.text:0040350D psfi       = SHFILEINFOW ptr -2B4h
.text:0040350D
.text:0040350D     sub     esp, 2D4h
.text:00403513     push    ebx
.text:00403514     push    esi
.text:00403515     push    edi

```

Адрес start (точки входа) = 350D - сходится

Name	Address	Ordinal
start	000000000040350D	[main entry]

Путём перехода от *DataDirectories* и таблицы секций, путём преобразований *RVA* в *raw*-адреса, найти в файле таблицу импорта, а в ней название библиотеки, которая подключена под номером 2 и функции из неё, которая подключена под номером 4. Все действия задокументировать, сопроводить снимками экрана с выделением нужной информации.

Библиотека $N = 2$, функция $M = 4$

1. Выяснить, на какую секцию попадает таблица импорта:

а. Выписать виртуальный адрес Import Table из *DataDirectories*

Address	Hex	ASCII
000000F0	0D 35 00 00 00 10 00 00 00 80 00 00 00 00 40 00	.5.....Ъ.....@.
00000100	00 10 00 00 00 00 02 00 00 04 00 00 00 06 00 00
00000110	04 00 00 00 00 00 00 00 00 80 06 00 00 04 00 00Ъ.....
00000120	FF EB EF 07 02 00 40 85 00 00 10 00 00 10 00 00	ялп...@.....
00000130	00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00
00000140	00 00 00 00 00 00 00 00 04 85 00 00 A0 00 00 00
00000150	00 10 06 00 80 65 00 00 00 00 00 00 00 00 00 00Ъe.....
00000160	C0 C8 EF 07 E0 1E 00 00 00 00 00 00 00 00 00 00	Имп.а.....
00000170	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000180	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000190	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000001A0	00 80 00 00 AC 02 00 00 00 00 00 00 00 00 00 00	.Ъ... ..
000001B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Import Table

04 85 00 00 A0 00 00 00

Size = A0 (A0 00 00 00) - это размер Import Table

VirtualAddress = 04 85 00 00 = 8504 - RVA таблицы импорта

Resource Table

00 10 06 00 80 65 00 00

Size = 6580 (80 65 00 00) - это размер Resource Table

VirtualAddress = 00 10 06 00 = 61000

- b. Выписать виртуальные и raw-адреса сегментов из таблицы секций

.rdata

VirtualSize 1384 (84 13 00 00)

VirtualAddress 8000 (00 80 00 00)

SizeOfRawData 1400 (00 14 00 00)

PointerToRawData 6A00 (00 6A 00 00)

- c. Определить между адресами каких секций попадает адрес Import Table (на .rdata)

Виртуальный адрес Import Table из DataDirectories 8504 попадает в .rdata.

RVA(начала секции .data)=8000

RAW(начала секции .data)=6A00

2. По формуле рассчитать RAW-адрес начала Import Table в файле
 $RAW = RVA(\text{относительно начала секции .rdata}) - RVA(\text{начала секции .rdata}) + RAW(\text{начала секции .rdata})$

$$RAW = 0x8504 - 0x8000 + 0x6A00 = 0x6F04$$

Получаем адрес 6F04, по которому должна быть расположена таблица. По нему можно перейти в hex-редакторе, потому что это число из файла. Переходим от начала файла (от нуля) абсолютным смещением на этот адрес.

Курсор оказывается здесь:

```
HxD - [D:\Krita_x64_Rus_Setup.exe]
Файл Правка Поиск Вид Анализ Инструменты Окно Справка
16 Windows (ANSI) hex
Krita_x64_Rus_Setup.exe
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Текст декодирован
00006D20 45 00 64 00 69 00 74 00 32 00 30 00 57 00 00 00 E.d.i.t.2.0.W...
00006D30 52 69 63 68 45 64 33 32 00 00 00 00 52 69 63 68 RichEd32....Rich
00006D40 45 64 32 30 00 00 00 00 2E 00 44 00 45 00 46 00 Ed20.....D.E.F.
00006D50 41 00 55 00 4C 00 54 00 5C 00 43 00 6F 00 6E 00 A.U.L.T.\.C.o.n.
00006D60 74 00 72 00 6F 00 6C 00 20 00 50 00 61 00 6E 00 t.r.o.l. .P.a.n.
00006D70 65 00 6C 00 5C 00 49 00 6E 00 74 00 65 00 72 00 e.l.\.I.n.t.e.r.
00006D80 6E 00 61 00 74 00 69 00 6F 00 6E 00 61 00 6C 00 n.a.t.i.o.n.a.l.
00006D90 00 00 00 00 00 00 00 00 43 00 6F 00 6E 00 74 00 .....C.o.n.t.
00006DA0 72 00 6F 00 6C 00 20 00 50 00 61 00 6E 00 65 00 r.o.l. .P.a.n.e.
00006DB0 6C 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 l.\.D.e.s.k.t.o.
00006DC0 70 00 5C 00 52 00 65 00 73 00 6F 00 75 00 72 00 p.\.R.e.s.o.u.r.
00006DD0 63 00 65 00 4C 00 6F 00 63 00 61 00 6C 00 65 00 c.e.L.o.c.a.l.e.
00006DE0 00 00 00 00 00 00 00 00 02 00 34 00 02 00 00 00 .....4.....
00006DF0 00 03 18 00 00 00 00 00 10 01 02 00 00 00 00 05 .....
00006E00 20 00 00 00 20 02 00 00 00 03 14 00 41 00 13 00 ... ..A...
00006E10 01 01 00 00 00 00 00 01 00 00 00 00 FF FE 00 00 .....яю..
00006E20 25 00 64 00 00 00 00 00 53 00 6F 00 66 00 74 00 %d....S.o.f.t.
00006E30 77 00 61 00 72 00 65 00 5C 00 4D 00 69 00 63 00 w.a.r.e.\.M.i.c.
00006E40 72 00 6F 00 73 00 6F 00 66 00 74 00 5C 00 57 00 r.o.s.o.f.t.\.W.
00006E50 69 00 6E 00 64 00 6F 00 77 00 73 00 5C 00 43 00 i.n.d.o.w.s.\.C.
00006E60 75 00 72 00 72 00 65 00 6E 00 74 00 56 00 65 00 u.r.r.e.n.t.V.e.
00006E70 72 00 73 00 69 00 6F 00 6E 00 00 00 00 00 00 00 r.s.i.o.n.....
00006E80 5C 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 \.M.i.c.r.o.s.o.
00006E90 66 00 74 00 5C 00 49 00 6E 00 74 00 65 00 72 00 f.t.\.I.n.t.e.r.
00006EA0 6E 00 65 00 74 00 20 00 45 00 78 00 70 00 6C 00 n.e.t. .E.x.p.l.
00006EB0 6F 00 72 00 65 00 72 00 5C 00 51 00 75 00 69 00 o.r.e.r.\.Q.u.i.
00006EC0 63 00 6B 00 20 00 4C 00 61 00 75 00 6E 00 63 00 c.k. .L.a.u.n.c.
00006ED0 68 00 00 00 F9 14 02 00 00 00 00 00 C0 00 00 00 h...ш.....A...
00006EE0 00 00 00 46 01 14 02 00 00 00 00 00 C0 00 00 00 ...F.....A...
00006EF0 00 00 00 46 0B 01 00 00 00 00 00 00 C0 00 00 00 ...F.....A...
00006F00 00 00 00 46 14 86 00 00 00 00 00 00 00 00 00 00 ...F|+.....
00006F10 A6 8C 00 00 70 80 00 00 38 87 00 00 00 00 00 00 |Б..рБ..8+.....
00006F20 00 00 00 00 C0 90 00 00 94 81 00 00 F0 85 00 00 ...АБ..Т..р...
00006F30 00 00 00 00 00 00 00 00 52 91 00 00 4C 80 00 00 .....R'.LB...
00006F40 1C 87 00 00 00 00 00 00 00 00 00 00 E0 91 00 00 .+.....a'.
00006F50 78 81 00 00 A4 85 00 00 00 00 00 00 00 00 00 00 xГ..м.....
00006F60 DA 92 00 00 80 80 00 00 DC 85 00 00 00 00 00 00 Б'...Б..b.....
00006F70 00 00 00 00 26 83 00 00 38 80 00 00 3C 88 00 00 ....&"..8Б..<€..
00006F80 00 00 00 00 00 00 00 00 7A 93 00 00 98 82 00 00 .....z".....
00006F90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00006FA0 00 00 00 00 60 92 00 00 C8 92 00 00 B8 92 00 00 .....И'..Е'..
00006FB0 A4 92 00 00 90 92 00 00 78 92 00 00 EC 91 00 00 и'..ђ'..х'..м'..
00006FC0 50 92 00 00 3E 92 00 00 30 92 00 00 1E 92 00 00 Р'..>'..0'..'..
00006FD0 0A 92 00 00 FC 91 00 00 00 00 00 00 12 93 00 00 .'..ь'....."
00006FE0 FC 92 00 00 11 00 00 80 E8 92 00 00 00 00 00 00 Б'.....Би'.....
00006FF0 CC 90 00 00 DC 90 00 00 EC 90 00 00 F8 90 00 00 МБ..бБ..мБ..шБ..
00007000 0E 91 00 00 24 91 00 00 34 91 00 00 44 91 00 00 ..$.4'..D'..
00007010 00 00 00 00 C8 8A 00 00 48 8A 00 00 5E 8A 00 00 ....ИБ..НБ..^Б..
00007020 66 8A 00 00 76 8A 00 00 84 8A 00 00 92 8A 00 00 фБ..vБ..„Б..'Б..
```

Видно, что здесь начинается какая-то регулярная табличная структура действительно. Энтропия низкая, значит тут лежит что-то таблица-образное. Мы нашли какую-то таблицу, но мы пока точно не можем сказать, правильно ли мы перешли по адресу.

3. По формуле рассчитать Raw-адрес имени DLL-файла (поле Name в одном из элементов Import Table)

Для каждой библиотеки указан адрес на следующую таблицу, дата время и имя от начала таблицы. Ссылка на имя указана со смещением десятичным 12 (ОТ НАЧАЛА ТАБЛИЦЫ!):

Начало таблицы (14 86 00 00)+12 смещение в 10 ричной системе = виртуальный адрес

Это адрес, где расположена строка с названием dll библиотеки. Но это виртуальный адрес, адрес в виртуальной памяти. Перейдя по нему в файле, мы ничего путного не обнаружим, потому что это не raw-адрес.

00006EA0	6E 00 65 00 74 00 20 00 45 00 78 00 70 00 6C 00	n.e.t. .E.x.p.l.
00006EB0	6F 00 72 00 65 00 72 00 5C 00 51 00 75 00 69 00	o.r.e.r.\.Q.u.i.
00006EC0	63 00 6B 00 20 00 4C 00 61 00 75 00 6E 00 63 00	s.k. .L.a.u.n.c.
00006ED0	68 00 00 00 F9 14 02 00 00 00 00 00 C0 00 00 00	h...щ.....А...
00006EE0	00 00 00 46 01 14 02 00 00 00 00 00 C0 00 00 00	...F.....А...
00006EF0	00 00 00 46 0B 01 00 00 00 00 00 00 C0 00 00 00	...F.....А...
00006F00	00 00 00 46 14 86 00 00 00 00 00 00 00 00 00 00	...F.†.....
00006F10	A6 8C 00 00 70 80 00 00 38 87 00 00 00 00 00 00	!Б..рЪ..8†.....
00006F20	00 00 00 00 C0 90 00 00 94 81 00 00 F0 85 00 00АЪ..”Г..р....
00006F30	00 00 00 00 00 00 00 00 52 91 00 00 4C 80 00 00R\..LЪ..
00006F40	1C 87 00 00 00 00 00 00 00 00 00 00 E0 91 00 00	.†.....a\..
00006F50	78 81 00 00 A4 85 00 00 00 00 00 00 00 00 00 00	xГ’..я.....
00006F60	DA 92 00 00 00 80 00 00 DC 85 00 00 00 00 00 00	Ъ’...Ъ..Ъ.....
00006F70	00 00 00 00 26 93 00 00 38 80 00 00 3C 88 00 00&”..8Ъ..<€..
00006F80	00 00 00 00 00 00 00 00 7A 93 00 00 98 82 00 00z”...,,..
00006F90	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

С помощью формулы рассчитываем RAW-адрес:

RAW = RVA(относительно начала секции .rdata) - RVA(начала секции .rdata) + RAW(начала секции .rdata)

RAW = 0x8CA6 - 0x8000 + 0x6A00 = 0x76A6

Переходим и видим:


```

000075E0 44 69 72 65 63 74 6F 72 79 57 00 00 C3 03 6C 73 DirectoryW...r.is
000075F0 74 72 63 6D 70 69 41 00 D4 01 47 65 74 54 65 6D trcmpiA.4.GetTem
00007600 70 46 69 6C 65 4E 61 6D 65 57 00 00 A4 03 57 72 pFileNameW...я.Wr
00007610 69 74 65 46 69 6C 65 00 C6 03 6C 73 74 72 63 70 iteFile.Ж.1strcp
00007620 79 41 00 00 70 02 4D 6F 76 65 46 69 6C 65 45 78 yA..p.MoveFileEx
00007630 57 00 BE 03 6C 73 74 72 63 61 74 57 00 00 C2 01 W.s.1strcatW..B.
00007640 47 65 74 53 79 73 74 65 6D 44 69 72 65 63 74 6F GetSystemDirecto
00007650 72 79 57 00 A0 01 47 65 74 50 72 6F 63 41 64 64 ryW. .GetProcAdd
00007660 72 65 73 73 00 00 7F 01 47 65 74 4D 6F 64 75 6C ress....GetModul
00007670 65 48 61 6E 64 6C 65 41 00 00 5A 01 47 65 74 45 eHandleA..Z.GetE
00007680 78 69 74 43 6F 64 65 50 72 6F 63 65 73 73 00 00 xitCodeProcess..
00007690 90 03 57 61 69 74 46 6F 72 53 69 6E 67 6C 65 4F h.WaitForSingleO
000076A0 62 6A 65 63 74 00 4B 45 52 4E 45 4C 33 32 2E 64 bject.KERNEL32.c
000076B0 6C 6C 00 00 C8 00 45 6E 64 50 61 69 6E 74 00 00 l...И.EndPaint..
000076C0 BF 00 44 72 61 77 54 65 78 74 57 00 E2 00 46 69 i.DrawTextW.в.Fi
000076D0 6C 6C 52 65 63 74 00 00 FF 00 47 65 74 43 6C 69 llRect...я.GetCli
000076E0 65 6E 74 52 65 63 74 00 0D 00 42 65 67 69 6E 50 entRect...BeginP
000076F0 61 69 6E 74 00 00 8F 00 44 65 66 57 69 6E 64 6F aint..Ц.DefWindo
00007700 77 50 72 6F 63 57 00 00 40 02 53 65 6E 64 4D 65 wProcW...@.SendMe
00007710 73 73 61 67 65 57 00 00 93 01 49 6E 76 61 6C 69 ssageW...".Invali
00007720 64 61 74 65 52 65 63 74 00 00 C4 00 45 6E 61 62 dateRect...Д.Enab
00007730 6C 65 57 69 6F 64 6F 77 00 00 2A 02 52 65 6C 65 leWindow * Data

```

- это 1 библиотека.

Найдем виртуальный адрес 2 библиотеки (каждая библиотека имеет размер 20 - <https://docs.microsoft.com/en-us/windows/win32/debug/pe-format#import-directory-table>, поэтому к смещению 12 прибавляем 20). От данного местоположения курсора:

```

00006EA0 6E 00 65 00 74 00 20 00 45 00 78 00 70 00 6C 00 n.e.t. .E.x.p.l.
00006EB0 6F 00 72 00 65 00 72 00 5C 00 51 00 75 00 69 00 o.r.e.r.\.Q.u.i.
00006EC0 63 00 6B 00 20 00 4C 00 61 00 75 00 6E 00 63 00 c.k. .L.a.u.n.c.
00006ED0 68 00 00 00 F9 14 02 00 00 00 00 00 00 00 00 h...щ.....A...
00006EE0 00 00 00 46 01 14 02 00 00 00 00 00 00 00 00 ...F.....A...
00006EF0 00 00 00 46 0B 01 00 00 00 00 00 00 00 00 00 ...F.....A...
00006F00 00 00 00 46 14 86 00 00 00 00 00 00 00 00 00 ...F.t.....
00006F10 A6 8C 00 00 70 80 00 00 38 87 00 00 00 00 00 00 Б...рБ..8±.....
00006F20 00 00 00 00 C0 90 00 00 94 81 00 00 F0 85 00 00 ....Аб.."Г..p....
00006F30 00 00 00 00 00 00 00 00 52 91 00 00 4C 80 00 00 .....R'\..ЛБ..
00006F40 1C 87 00 00 00 00 00 00 00 00 00 00 00 00 00 .±.....a'..
00006F50 78 81 00 00 A4 85 00 00 00 00 00 00 00 00 00 00 хГ...я.....
00006F60 DA 92 00 00 00 80 00 00 DC 85 00 00 00 00 00 00 Ъ'...Б..б.....
00006F70 00 00 00 00 26 93 00 00 38 80 00 00 3C 88 00 00 ....&"..8Б..<€..
00006F80 00 00 00 00 00 00 00 00 7A 93 00 00 98 82 00 00 .....z"...,,...
00006F90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

Смещение 20:

Перейти к

Смещение:

20

☐ hex ☒ dec ☐ oct

Смещение относительно

☐ начала

☒ текущего смещения

☐ конца (обратно)

OK Отмена

Местоположение курсора:

```

00006D50 41 00 55 00 4C 00 54 00 5C 00 43 00 6F 00 6E 00 A.U.L.T.\.C.o.n.
00006D60 74 00 72 00 6F 00 6C 00 20 00 50 00 61 00 6E 00 t.r.o.l. .P.a.n.
00006D70 65 00 6C 00 5C 00 49 00 6E 00 74 00 65 00 72 00 e.l.\.I.n.t.e.r.
00006D80 6E 00 61 00 74 00 69 00 6F 00 6E 00 61 00 6C 00 n.a.t.i.o.n.a.l.
00006D90 00 00 00 00 00 00 00 00 43 00 6F 00 6E 00 74 00 .....C.o.n.t.
00006DA0 72 00 6F 00 6C 00 20 00 50 00 61 00 6E 00 65 00 r.o.l. .P.a.n.e.
00006DB0 6C 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 l.\.D.e.s.k.t.o.
00006DC0 70 00 5C 00 52 00 65 00 73 00 6F 00 75 00 72 00 p.\.R.e.s.o.u.r.
00006DD0 63 00 65 00 4C 00 6F 00 63 00 61 00 6C 00 65 00 c.e.L.o.c.a.l.e.
00006DE0 00 00 00 00 00 00 00 00 02 00 34 00 02 00 00 00 .....4.....
00006DF0 00 03 18 00 00 00 00 10 01 02 00 00 00 00 00 05 .....
00006E00 20 00 00 00 20 02 00 00 00 03 14 00 41 00 13 00 ... .....A...
00006E10 01 01 00 00 00 00 00 01 00 00 00 00 FF FE 00 00 .....яю..
00006E20 25 00 64 00 00 00 00 00 53 00 6F 00 66 00 74 00 %d.....S.o.f.t.
00006E30 77 00 61 00 72 00 65 00 5C 00 4D 00 69 00 63 00 w.a.r.e.\.M.i.c.
00006E40 72 00 6F 00 73 00 6F 00 66 00 74 00 5C 00 57 00 r.o.s.o.f.t.\.W.
00006E50 69 00 6E 00 64 00 6F 00 77 00 73 00 5C 00 43 00 i.n.d.o.w.s.\.C.
00006E60 75 00 72 00 72 00 65 00 6E 00 74 00 56 00 65 00 u.r.r.e.n.t.V.e.
00006E70 72 00 73 00 69 00 6F 00 6E 00 00 00 00 00 00 00 r.s.i.o.n.....
00006E80 5C 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 \.M.i.c.r.o.s.o.
00006E90 66 00 74 00 5C 00 49 00 6E 00 74 00 65 00 72 00 f.t.\.I.n.t.e.r.
00006EA0 6E 00 65 00 74 00 20 00 45 00 78 00 70 00 6C 00 n.e.t. .E.x.p.l.
00006EB0 6F 00 72 00 65 00 72 00 5C 00 51 00 75 00 69 00 o.r.e.r.\.Q.u.i.
00006EC0 63 00 6B 00 20 00 4C 00 61 00 75 00 6E 00 63 00 c.k. .L.a.u.n.c.
00006ED0 68 00 00 00 F9 14 02 00 00 00 00 00 C0 00 00 00 h...щ.....A...
00006EE0 00 00 00 46 01 14 02 00 00 00 00 00 C0 00 00 00 ...F.....A...
00006EF0 00 00 00 46 0B 01 00 00 00 00 00 00 C0 00 00 00 ...F.....A...
00006F00 00 00 00 46 14 86 00 00 00 00 00 00 00 00 00 00 ...F.t.....
00006F10 A6 8C 00 00 70 80 00 00 38 87 00 00 00 00 00 00 |E...pБ..8+.
00006F20 00 00 00 00 C0 90 00 00 94 81 00 00 F0 85 00 00 ....Ab.. "Г..p....
00006F30 00 00 00 00 00 00 00 00 52 91 00 00 4C 80 00 00 .....R'\.LБ..
00006F40 1C 87 00 00 00 00 00 00 00 00 00 00 E0 91 00 00 .+. .....a\..
00006F50 78 81 00 00 A4 85 00 00 00 00 00 00 00 00 00 00 xГ...я.....
00006F60 DA 92 00 00 00 80 00 00 DC 85 00 00 00 00 00 00 00 Ъ'...Б..Б.....
00006F70 00 00 00 00 26 93 00 00 38 80 00 00 3C 88 00 00 ....&"..8Б..<€..
00006F80 00 00 00 00 00 00 00 00 7A 93 00 00 98 82 00 00 .....з".....

```

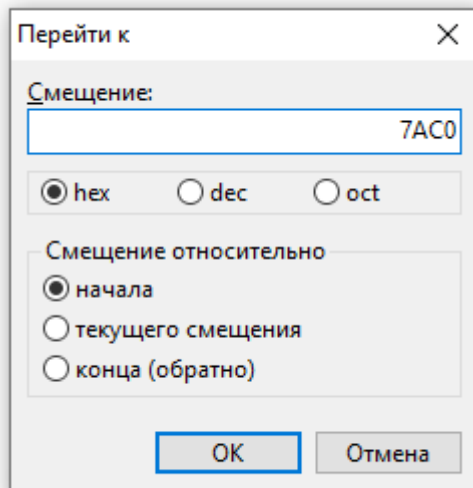
C0 90 00 00 = 90C0

Это виртуальный адрес, а нам нужно найти Raw-адрес, поэтому:

RAW = RVA(относительно начала секции .rdata) - RVA(начала секции .rdata) + RAW(начала секции .rdata)

RAW = 0x90C0 - 0x8000 + 0x6A00 = 0x7AC0

Переходим:



Видим:

```
00007910 49 73 57 69 6E 64 6F 77 45 6E 61 62 6C 65 64 00 IsWindowEnabled.
00007920 83 02 53 65 74 57 69 6E 64 6F 77 50 6F 73 00 00 f.SetWindowPos...
00007930 5A 01 47 65 74 53 79 73 43 6F 6C 6F 72 00 6F 01 Z.GetSysColor.o.
00007940 47 65 74 57 69 6E 64 6F 77 4C 6F 6E 67 57 00 00 GetWindowLongW..
00007950 4D 02 53 65 74 43 75 72 73 6F 72 00 BD 01 4C 6F M.SetCursor.S.Lo
00007960 61 64 43 75 72 73 6F 72 57 00 38 00 43 68 65 63 adCursorW.8.Chec
00007970 6B 44 6C 67 42 75 74 74 6F 6E 00 00 3C 01 47 65 kDlgButton...<.Ge
00007980 74 4D 65 73 73 61 67 65 50 6F 73 00 1C 00 43 61 tMessagePos...Ca
00007990 6C 6C 57 69 6E 64 6F 77 50 72 6F 63 57 00 B1 01 llWindowProcW.±.
000079A0 49 73 57 69 6E 64 6F 77 56 69 73 69 62 6C 65 00 IsWindowVisible.
000079B0 42 00 43 6C 6F 73 65 43 6C 69 70 62 6F 61 72 64 B.CloseClipboard
000079C0 00 00 4A 02 53 65 74 43 6C 69 70 62 6F 61 72 64 ..J.SetClipboard
000079D0 44 61 74 61 00 00 C1 00 45 6D 70 74 79 43 6C 69 Data..B.EmptyCli
000079E0 70 62 6F 61 72 64 00 00 F6 01 4F 70 65 6E 43 6C pboard..ц.OpenCl
000079F0 69 70 62 6F 61 72 64 00 A4 02 54 72 61 63 6B 50 ipboard.».TrackP
00007A00 6F 70 75 70 4D 65 6E 75 00 00 09 00 41 70 70 65 opupMenu....Appe
00007A10 6E 64 4D 65 6E 75 57 00 5E 00 43 72 65 61 74 65 ndMenuW.^.Create
00007A20 50 6F 70 75 70 4D 65 6E 75 00 5D 01 47 65 74 53 PopupMenu.].GetS
00007A30 79 73 74 65 6D 4D 65 74 72 69 63 73 00 00 54 02 ystemMetrics..T.
00007A40 53 65 74 44 6C 67 49 74 65 6D 54 65 78 74 57 00 SetDlgItemTextW.
00007A50 14 01 47 65 74 44 6C 67 49 74 65 6D 54 65 78 74 ..GetDlgItemText
00007A60 57 00 E3 01 4D 65 73 73 61 67 65 42 6F 78 49 6E W.r.MessageBoxIn
00007A70 64 69 72 65 63 74 57 00 2F 00 43 68 61 72 50 72 directW./.CharPr
00007A80 65 76 57 00 2A 00 43 68 61 72 4E 65 78 74 41 00 evW.*.CharNextA.
00007A90 D7 02 77 73 70 72 69 6E 74 66 41 00 A2 00 44 69 %wsprintfA.ÿ.Di
00007AA0 73 70 61 74 63 68 4D 65 73 73 61 67 65 57 00 00 spatchMessageW..
00007AB0 01 02 50 65 65 6B 4D 65 73 73 61 67 65 57 00 00 ..PeekMessageW..
00007AC0 55 53 45 52 33 32 2E 64 6C 6C 00 00 0E 02 53 65 USER32.dll....Se
00007AD0 6C 65 63 74 4F 62 6A 65 63 74 00 00 3C 02 53 65 lectObject...<.Se
00007AE0 74 54 65 78 74 43 6F 6C 6F 72 00 00 16 02 53 65 tTextColor....Se
00007AF0 74 42 6B 4D 6F 64 65 00 3D 00 43 72 65 61 74 65 tBkMode.=.Create
00007B00 46 6F 6E 74 49 6E 64 69 72 65 63 74 57 00 29 00 FontIndirectW.).
00007B10 43 72 65 61 74 65 42 72 75 73 68 49 6E 64 69 72 CreateBrushIndir
00007B20 65 63 74 00 8F 00 44 65 6C 65 74 65 4F 62 6A 65 ect.Û.DeleteObje
00007B30 63 74 00 00 6B 01 47 65 74 44 65 76 69 63 65 43 ct...k.GetDeviceC
00007B40 61 70 73 00 15 02 53 65 74 42 6B 43 6F 6C 6F 72 aps...SetBkColor
00007B50 00 00 47 44 49 33 32 2E 64 6C 6C 00 9B 00 53 48 ..GDI32.dll.>.SH
00007B60 46 69 6C 65 4F 70 65 72 61 74 69 6F 6E 57 00 00 FileOperationW..
00007B70 AD 00 53 48 47 65 74 46 69 6C 65 49 6E 66 6F 57 ..SHGetFileInfoW
00007B80 00 00 7A 00 53 48 42 72 6F 77 73 65 46 6F 72 46 ..z.SHBrowseForF
00007B90 6F 6C 64 65 72 57 00 00 BD 00 53 48 47 65 74 50 olderW...S.SHGetP
00007BA0 61 74 68 46 72 6F 6D 49 44 4C 69 73 74 57 00 00 athFromIDListW..
00007BB0 0A 01 53 68 65 6C 6C 45 78 65 63 75 74 65 45 78 ..ShellExecuteEx
```

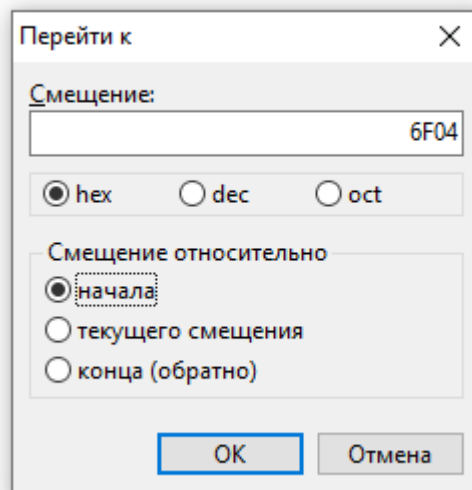
Это и есть 2 библиотека, которая мне нужна по условию.

Далее находим необходимые функции.

4. По формуле рассчитать Raw-адрес Image Thunk Data

Возвращаемся во 2 шаг (обнаружение таблицы). И берем имя не по смещению 12, а самый первый адрес.

Перейдем на начало таблицы:



Берем адрес с самого начала таблицы:

00006EA0	6E 00 65 00 74 00 20 00 45 00 78 00 70 00 6C 00	n.e.t. .E.x.p.l.
00006EB0	6F 00 72 00 65 00 72 00 5C 00 51 00 75 00 69 00	o.r.e.r.\.Q.u.i.
00006EC0	63 00 6B 00 20 00 4C 00 61 00 75 00 6E 00 63 00	s.k. .L.a.u.n.c.
00006ED0	68 00 00 00 F9 14 02 00 00 00 00 00 C0 00 00 00	h...ш.....A...
00006EE0	00 00 00 46 01 14 02 00 00 00 00 00 C0 00 00 00	...F.....A...
00006EF0	00 00 00 46 0B 01 00 00 00 00 00 00 C0 00 00 00	...F.....A...
00006F00	00 00 00 46 14 86 00 00 00 00 00 00 00 00 00 00	...F...+.....
00006F10	A6 8C 00 00 70 80 00 00 38 87 00 00 00 00 00 00	!B..pB..8+.....
00006F20	00 00 00 00 C0 90 00 00 94 81 00 00 F0 85 00 00Ah.."T..p....
00006F30	00 00 00 00 00 00 00 00 52 91 00 00 4C 80 00 00R'\.LT...
00006F40	1C 87 00 00 00 00 00 00 00 00 00 00 E0 91 00 00	..+.....a'...
00006F50	78 81 00 00 A4 85 00 00 00 00 00 00 00 00 00 00	xT'..я.....
00006F60	DA 92 00 00 00 80 00 00 DC 85 00 00 00 00 00 00	Ъ'...Ъ..Ъ.....
00006F70	00 00 00 00 26 93 00 00 38 80 00 00 3C 88 00 00&"..8Ъ..<€..
00006F80	00 00 00 00 00 00 00 00 7A 93 00 00 98 82 00 00z"...,,...
00006F90	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00006FA0	00 00 00 00 60 92 00 00 C8 92 00 00 B8 92 00 00`...И'..ë'...
00006FB0	A4 92 00 00 90 92 00 00 78 92 00 00 EC 91 00 00	я'..ђ'..x'..м'...
00006FC0	50 92 00 00 3E 92 00 00 30 92 00 00 1E 92 00 00	P'..>'..0'...'...
00006FD0	0A 92 00 00 FC 91 00 00 00 00 00 00 12 93 00 00	..'..ъ'....."
00006FE0	FC 92 00 00 11 00 00 80 E8 92 00 00 00 00 00 00	ь'.....Ъи'.....
00006FF0	CC 90 00 00 DC 90 00 00 EC 90 00 00 F8 90 00 00	Mђ..bђ..mђ..шђ..

$$14\ 86\ 00\ 00 = 8614$$

RVA следующей таблицы ILT и ссылками на имена функций 0x8614

RAW с ILT и ссылками на имена функций = $0x8614 - 0x8000 + 0x6A00 = 0x7014$

Получаем адрес для шага 4. Здесь хранится ссылка на имя функции, переходим:

```
00006F40 1C 87 00 00 00 00 00 00 00 00 00 00 00 00 E0 91 00 00 .#.....a'..
00006F50 78 81 00 00 A4 85 00 00 00 00 00 00 00 00 00 00 00 00 xГ'...я.....
00006F60 DA 92 00 00 00 80 00 00 DC 85 00 00 00 00 00 00 00 00 Ъ'...Ъ..Ъ.....
00006F70 00 00 00 00 26 93 00 00 38 80 00 00 3C 88 00 00 ....&"..8Ъ..<€..
00006F80 00 00 00 00 00 00 00 00 7A 93 00 00 98 82 00 00 .....z"...
00006F90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00006FA0 00 00 00 00 60 92 00 00 C8 92 00 00 B8 92 00 00 ....`'..И'..ë'..
00006FB0 A4 92 00 00 90 92 00 00 78 92 00 00 EC 91 00 00 я'..ђ'..х'..м'..
00006FC0 50 92 00 00 3E 92 00 00 30 92 00 00 1E 92 00 00 P'..>'..0'...'..
00006FD0 0A 92 00 00 FC 91 00 00 00 00 00 00 12 93 00 00 .'..Ъ'..'.."..
00006FE0 FC 92 00 00 11 00 00 80 E8 92 00 00 00 00 00 00 00 00 00 Ъ'.....Ъи'.....
00006FF0 CC 90 00 00 DC 90 00 00 EC 90 00 00 F8 90 00 00 МЪ..ЪЪ..мЪ..шЪ..
00007000 0E 91 00 00 24 91 00 00 34 91 00 00 44 91 00 00 ..'..$'..4'..D'..
00007010 00 00 00 00 C8 8A 00 00 48 8A 00 00 5E 8A 00 00 ....ИЪ..НЪ..^Ъ..
00007020 66 8A 00 00 76 8A 00 00 84 8A 00 00 92 8A 00 00 fЪ..vЪ..,,Ъ..'Ъ..
00007030 A8 8A 00 00 1A 8A 00 00 32 8A 00 00 D6 8A 00 00 EЪ..Ъ..2Ъ..ЦЪ..
00007040 F0 8A 00 00 08 8B 00 00 18 8B 00 00 2A 8B 00 00 pЪ...<...<..*<..
00007050 38 8B 00 00 48 8B 00 00 54 8B 00 00 BC 8A 00 00 8<...Н<..Т<...jЪ..
00007060 0E 8A 00 00 84 8B 00 00 92 8B 00 00 A2 8B 00 00 ..Ъ..,,<..'<...ÿ<..
00007070 B2 8B 00 00 C6 8B 00 00 D8 8B 00 00 EC 8B 00 00 I<...Ж<..Ш<..м<..
00007080 F8 8B 00 00 0C 8C 00 00 18 8C 00 00 24 8C 00 00 ш<...Б...Ъ..$Ъ..
00007090 32 8C 00 00 3E 8C 00 00 54 8C 00 00 66 8C 00 00 2Ъ..>Ъ..ТЪ..fЪ..
000070A0 7A 8C 00 00 90 8C 00 00 9E 89 00 00 92 89 00 00 zЪ..ђЪ..h%..'%.
000070B0 FA 89 00 00 E6 89 00 00 D8 89 00 00 C6 89 00 00 ь%.ж%.Ш%.Ж%.
000070C0 B8 89 00 00 AA 89 00 00 76 89 00 00 68 89 00 00 ë%.С%.v%.h%.
000070D0 74 8B 00 00 60 8B 00 00 5A 89 00 00 5A 88 00 00 t<..'<..Z%.Z€..
000070E0 68 88 00 00 7A 88 00 00 8A 88 00 00 96 88 00 00 h€..z€..Ъ€...€..
000070F0 A8 88 00 00 50 88 00 00 CA 88 00 00 D6 88 00 00 E€..P€..K€..Ц€..
```

Видим повторяющуюся табличную структуру. На месте курсора следующий адрес - виртуальный. Преобразовываем его к RAW-адресу, чтобы найти в файле что он кодирует.

$C8\ 8A\ 00\ 00 = 8AC8$

Для 2 библиотеки:

Берем первый адрес по смещению 20 (первый адрес от обнаруженной нами таблицы):

Перейти к

Смещение:

6F04

☒ hex ☐ dec ☐ oct

Смещение относительно

☒ начала

☐ текущего смещения

☐ конца (обратно)

OK Отмена

- смещение, чтобы найти таблицу.

Перейти к

Смещение:

20

☐ hex ☒ dec ☐ oct

Смещение относительно

☐ начала

☒ текущего смещения

☐ конца (обратно)

OK Отмена

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Текст декодирован
00006E70	72	00	73	00	69	00	6F	00	6E	00	00	00	00	00	00	00	r.s.i.o.n.....
00006E80	5C	00	4D	00	69	00	63	00	72	00	6F	00	73	00	6F	00	\.M.i.c.r.o.s.o.
00006E90	66	00	74	00	5C	00	49	00	6E	00	74	00	65	00	72	00	f.t.\.I.n.t.e.r.
00006EA0	6E	00	65	00	74	00	20	00	45	00	78	00	70	00	6C	00	n.e.t. .E.x.p.l.
00006EB0	6F	00	72	00	65	00	72	00	5C	00	51	00	75	00	69	00	o.r.e.r.\.Q.u.i.
00006EC0	63	00	6B	00	20	00	4C	00	61	00	75	00	6E	00	63	00	c.k. .L.a.u.n.c.
00006ED0	68	00	00	00	F9	14	02	00	00	00	00	00	C0	00	00	00	h...щ.....A...
00006EE0	00	00	00	46	01	14	02	00	00	00	00	00	C0	00	00	00	...F.....A...
00006EF0	00	00	00	46	0B	01	00	00	00	00	00	00	C0	00	00	00	...F.....A...
00006F00	00	00	00	46	14	86	00	00	00	00	00	00	00	00	00	00	...F.t.....
00006F10	A6	8C	00	00	70	80	00	00	38	87	00	00	00	00	00	00	!B..pB..8+..
00006F20	00	00	00	00	C0	90	00	00	94	81	00	00	F0	85	00	00	...Ah.."T..p...
00006F30	00	00	00	00	00	00	00	00	52	91	00	00	4C	80	00	00R'\..LB..
00006F40	1C	87	00	00	00	00	00	00	00	00	00	00	E0	91	00	00	.+......a\'..
00006F50	78	81	00	00	A4	85	00	00	00	00	00	00	00	00	00	00	xT'..я.....
00006F60	DA	92	00	00	00	80	00	00	DC	85	00	00	00	00	00	00	Ъ'...Ъ..b.....
00006F70	00	00	00	00	26	93	00	00	38	80	00	00	3C	88	00	00&"..8Ъ..<€..
00006F80	00	00	00	00	00	00	00	00	7A	93	00	00	98	82	00	00z^.....
00006F90	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00006FA0	00	00	00	00	60	92	00	00	C8	92	00	00	B8	92	00	00'..И'..é'..
00006FB0	A4	92	00	00	90	92	00	00	78	92	00	00	EC	91	00	00	я'..ђ'..x'..м'..
00006FC0	50	92	00	00	3E	92	00	00	30	92	00	00	1E	92	00	00	P'...>'..0'....'
00006FD0	0A	92	00	00	FC	91	00	00	00	00	00	00	12	93	00	00	.'...ь'....."
00006FE0	FC	92	00	00	11	00	00	80	E8	92	00	00	00	00	00	00	ь'.....Би'.....
00006FF0	CC	90	00	00	DC	90	00	00	EC	90	00	00	F8	90	00	00	Mђ..bђ..mђ..шђ..
00007000	0E	91	00	00	24	91	00	00	34	91	00	00	44	91	00	00	..\$.4'.D'..
00007010	00	00	00	00	C8	87	00	00	48	87	00	00	5F	87	00	00	иБ иБ ^Б

RVA следующей таблицы ILT и ссылками на имена функций 0x8738

RAW с ILT и ссылками на имени функций = $0x8738 - 0x8000 + 0x6A00 = 0x7138$

5. По формуле рассчитать RAW-адрес имени первой функции, импортируемой из Name

RVA имени первой функции из первой DLL 0x8AC8

$RAW = 0x8AC8 - 0x8000 + 0x6A00 = 0x74C8$

Переходим по этому RAW-адресу и видим:

```
00007360  61 6C 41 6C 6C 6E 63 00 FF 01 47 6C 6F 62 61 6C  aiAlloc.Я.Global
00007370  46 72 65 65 00 00 BD 00 45 78 70 61 6E 64 45 6E  Free..S.ExpandEn
00007380  76 69 72 6F 6E 6D 65 6E 74 53 74 72 69 6E 67 73  vironmentStrings
00007390  57 00 C1 03 6C 73 74 72 63 6D 70 57 00 00 C4 03  W.E.lstrcmpW..Д.
000073A0  6C 73 74 72 63 6D 70 69 57 00 34 00 43 6C 6F 73  lstrcmpiW.4.Clos
000073B0  65 48 61 6E 64 6C 65 00 1F 03 53 65 74 46 69 6C  eHandle...SetFil
000073C0  65 54 69 6D 65 00 39 00 43 6F 6D 70 61 72 65 46  eTime.9.CompareF
000073D0  69 6C 65 54 69 6D 65 00 DC 02 53 65 61 72 63 68  ileTime.b.Search
000073E0  50 61 74 68 57 00 B6 01 47 65 74 53 68 6F 72 74  PathW.f.GetShort
000073F0  50 61 74 68 4E 61 6D 65 57 00 6A 01 47 65 74 46  PathNameW.j.GetF
00007400  75 6C 6C 50 61 74 68 4E 61 6D 65 57 00 00 71 02  ullPathNameW..q.
00007410  4D 6F 76 65 46 69 6C 65 57 00 0B 03 53 65 74 43  MoveFileW...SetC
00007420  75 72 72 65 6E 74 44 69 72 65 63 74 6F 72 79 57  urrentDirectoryW
00007430  00 00 61 01 47 65 74 46 69 6C 65 41 74 74 72 69  ..a.GetFileAttri
00007440  62 75 74 65 73 57 00 00 1A 03 53 65 74 46 69 6C  butesW....SetFil
00007450  65 41 74 74 72 69 62 75 74 65 73 57 00 00 56 03  eAttributesW..V.
00007460  53 6C 65 65 70 00 DF 01 47 65 74 54 69 63 6B 43  Sleep.f.GetTickC
00007470  6F 75 6E 74 00 00 56 00 43 72 65 61 74 65 46 69  ount..V.CreateFi
00007480  6C 65 57 00 63 01 47 65 74 46 69 6C 65 53 69 7A  leW.c.GetFileSiz
00007490  65 00 7E 01 47 65 74 4D 6F 64 75 6C 65 46 69 6C  e..GetModuleFil
000074A0  65 4E 61 6D 65 57 00 00 42 01 47 65 74 43 75 72  eNameW..B.GetCur
000074B0  72 65 6E 74 50 72 6F 63 65 73 73 00 46 00 43 6F  rentProcess.F.Co
000074C0  70 79 46 69 6C 65 57 00 B9 00 45 78 69 74 50 72  pyFileW.f.ExitPr
000074D0  6F 63 65 73 73 00 14 03 53 65 74 45 6E 76 69 72  ocess...SetEnvir
000074E0  6F 6E 6D 65 6E 74 56 61 72 69 61 62 6C 65 57 00  onmentVariableW.
000074F0  F4 01 47 65 74 57 69 6E 64 6F 77 73 44 69 72 65  f.GetWindowsDire
00007500  63 74 6F 72 79 57 00 00 D6 01 47 65 74 54 65 6D  ctoryW..Ц.GetTem
00007510  70 50 61 74 68 57 00 00 11 01 47 65 74 43 6F 6D  pPathW....GetCom
00007520  6D 61 6E 64 4C 69 6E 65 57 00 E8 01 47 65 74 56  mandLineW.и.GetV
00007530  65 72 73 69 6F 6E 00 00 15 03 53 65 74 45 72 72  ersion....SetErr
00007540  6F 72 4D 6F 64 65 00 00 CD 03 6C 73 74 72 6C 65  orMode..H.lstrle
00007550  6E 57 00 00 CA 03 6C 73 74 72 63 70 79 6E 57 00  nW..K.lstrcpyW.
-----
```

Видим строковое имя - читабельная строка с именем функции. Имя узнаваемое, однако появились лишний префикс. Скорее всего компилятор добавил к функции что-то свое.

Проверяем с помощью IdaPro:

0000000000408080	CreateFileW	KERNEL32
00000000004080D0	CreateProcessW	KERNEL32
00000000004080C4	CreateThread	KERNEL32
0000000000408138	DeleteFileW	KERNEL32
0000000000408070	ExitProcess	KERNEL32
0000000000408124	ExpandEnvironmentStringsW	KERNEL32
0000000000408144	FindClose	KERNEL32
000000000040813C	FindFirstFileW	KERNEL32
0000000000408140	FindNextFileW	KERNEL32
0000000000408164	FreeLibrary	KERNEL32
00000000004080A4	GetCommandLineW	KERNEL32

Для 2 библиотеки:

- 1 функция

Перейти к

Смещение:

7138

☒ hex

☐ dec

☐ oct

Смещение относительно

☒ начала

☐ текущего смещения

☐ конца (обратно)

OK

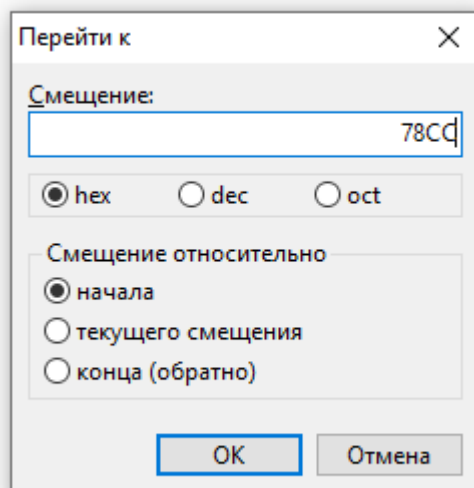
Отмена

00006FD0	0A 92 00 00 FC 91 00 00 00 00 00 00 12 93 00 00	.'...Б'......"
00006FE0	FC 92 00 00 11 00 00 80 E8 92 00 00 00 00 00 00	Б'.....Би'.....
00006FF0	CC 90 00 00 DC 90 00 00 EC 90 00 00 F8 90 00 00	Мђ..бђ..мђ..мђ..
00007000	0E 91 00 00 24 91 00 00 34 91 00 00 44 91 00 00	.'...\$'....4'....D'..
00007010	00 00 00 00 C8 8A 00 00 48 8A 00 00 5E 8A 00 00ИЉ..НЉ..^Љ..
00007020	66 8A 00 00 76 8A 00 00 84 8A 00 00 92 8A 00 00	fЉ..vЉ..„Љ..'Љ..
00007030	A8 8A 00 00 1A 8A 00 00 32 8A 00 00 D6 8A 00 00	ЕЉ...Љ..2Љ..ЦЉ..
00007040	F0 8A 00 00 08 8B 00 00 18 8B 00 00 2A 8B 00 00	pЉ...<...<...*<..
00007050	38 8B 00 00 48 8B 00 00 54 8B 00 00 BC 8A 00 00	8<...H<...T<...jЉ..
00007060	0E 8A 00 00 84 8B 00 00 92 8B 00 00 A2 8B 00 00	.Љ...„<...'<...Ÿ<..
00007070	B2 8B 00 00 C6 8B 00 00 D8 8B 00 00 EC 8B 00 00	I<...Ж<...Ш<...м<..
00007080	F8 8B 00 00 0C 8C 00 00 18 8C 00 00 24 8C 00 00	м<...Б...Б...\$Б..
00007090	32 8C 00 00 3E 8C 00 00 54 8C 00 00 66 8C 00 00	2Б..>Б..ТБ..fБ..
000070A0	7A 8C 00 00 90 8C 00 00 9E 89 00 00 92 89 00 00	zБ..ђБ..h%..'%....
000070B0	FA 89 00 00 E6 89 00 00 D8 89 00 00 C6 89 00 00	ъ%..ж%..ш%..ж%...
000070C0	B8 89 00 00 AA 89 00 00 76 89 00 00 68 89 00 00	ѐ%..е%..v%..h%...
000070D0	74 8B 00 00 60 8B 00 00 5A 89 00 00 5A 88 00 00	t<...'<...Z%..Z€..
000070E0	68 88 00 00 7A 88 00 00 8A 88 00 00 96 88 00 00	h€..z€..Љ€...-€..
000070F0	A8 88 00 00 50 88 00 00 CA 88 00 00 D6 88 00 00	Ė€...P€..K€..Ц€..
00007100	B4 88 00 00 08 89 00 00 26 89 00 00 EC 88 00 00	r€...%..&%..м€..
00007110	46 89 00 00 34 89 00 00 00 00 00 00 B0 91 00 00	F%..4%.....°'\..
00007120	98 91 00 00 C2 91 00 00 70 91 00 00 5C 91 00 00	.'...B'\..p'\..\'....
00007130	82 91 00 00 00 00 00 00 CC 8E 00 00 EE 8E 00 00	, '\.....МѢ..оѢ..
00007140	FE 8E 00 00 0E 8F 00 00 20 8F 00 00 30 8F 00 00	юѢ...Ц...Ц...ОЦ..
00007150	3E 8F 00 00 50 8F 00 00 5C 8F 00 00 6A 8F 00 00	>Ц..PЦ..\Ц..jЦ..
00007160	7C 8F 00 00 8C 8F 00 00 9E 8F 00 00 B0 8F 00 00	Ц..БЦ..hЦ..°Ц..
00007170	C2 8F 00 00 D6 8F 00 00 E8 8F 00 00 F8 8F 00 00	ВЦ..ЦЦ..иЦ..мЦ..
00007180	BA 8E 00 00 DC 8E 00 00 6E 8D 00 00 3E 90 00 00	еѢ..бѢ..nĲ..>ђ..
00007190	50 90 00 00 62 90 00 00 78 90 00 00 84 90 00 00	Pђ..bђ..xђ..„ђ..
000071A0	90 90 00 00 9C 90 00 00 B0 90 00 00 46 8D 00 00	ђђ..њђ..°ђ..FK..
000071B0	3A 8D 00 00 2A 8D 00 00 18 8D 00 00 08 8D 00 00	:Ĳ..*Ĳ...Ĳ...Ĳ..
000071C0	F6 8C 00 00 E8 8C 00 00 D8 8C 00 00 CC 8C 00 00	цѢ..иѢ..шѢ..мѢ..
000071D0	84 8E 00 00 AE 8E 00 00 9C 8E 00 00 50 8E 00 00	..Ѣ..ѦѢ..њѢ..PѢ..

RVA имени первой функции из второй DLL 0x8ECC

RAW = 0x8ECC - 0x8000 + 0x6A00 = 0x78CC

Переходим:



Видим:

```
000077F0 87 02 53 65 74 57 69 6E 64 6F 77 54 65 78 74 57 #.SetWindowTextW
00007800 00 00 7A 02 53 65 74 54 69 6D 65 72 00 00 56 00 ..z.SetTimer..V.
00007810 43 72 65 61 74 65 44 69 61 6C 6F 67 50 61 72 61 CreateDialogPara
00007820 6D 57 00 00 99 00 44 65 73 74 72 6F 79 57 69 6E mW..".DestroyWin
00007830 64 6F 77 00 E1 00 45 78 69 74 57 69 6E 64 6F 77 dow.6.ExitWindow
00007840 73 45 78 00 2C 00 43 68 61 72 4E 65 78 74 57 00 sEx.,.CharNextW.
00007850 9F 00 44 69 61 6C 6F 67 42 6F 78 50 61 72 61 6D u.DialogBoxParam
00007860 57 00 F9 00 47 65 74 43 6C 61 73 73 49 6E 66 6F W.m.GetClassInfo
00007870 57 00 61 00 43 72 65 61 74 65 57 69 6E 64 6F 77 W.a.CreateWindow
00007880 45 78 57 00 9A 02 53 79 73 74 65 6D 50 61 72 61 ExW.m.SystemPara
00007890 6D 65 74 65 72 73 49 6E 66 6F 57 00 19 02 52 65 metersInfoW...Re
000078A0 67 69 73 74 65 72 43 6C 61 73 73 57 00 00 C6 00 gisterClassW..X.
000078B0 45 6E 64 44 69 61 6C 6F 67 00 31 02 53 63 72 65 EndDialog.l.Scre
000078C0 65 6E 54 6F 43 6C 69 65 6E 74 00 00 74 01 47 65 enToClient..t.Ge
000078D0 74 57 69 6E 64 6F 77 52 65 63 74 00 C2 00 45 6E tWindowRect.B.En
000078E0 61 62 6C 65 4D 65 6E 75 49 74 65 6D 00 00 5C 01 ableMenuItem..\
000078F0 47 65 74 53 79 73 74 65 6D 4D 65 6E 75 00 48 02 GetSystemMenu.H.
00007900 53 65 74 43 6C 61 73 73 4C 6F 6E 67 57 00 AE 01 SetClassLongW.@.
00007910 49 73 57 69 6E 64 6F 77 45 6E 61 62 6C 65 64 00 IsWindowEnabled.
00007920 83 02 53 65 74 57 69 6E 64 6F 77 50 6F 73 00 00 f.SetWindowPos..
00007930 5A 01 47 65 74 53 79 73 43 6F 6C 6F 72 00 6F 01 Z.GetSysColor.o.
00007940 47 65 74 57 69 6E 64 6F 77 4C 6F 6E 67 57 00 00 GetWindowLongW..
00007950 4D 02 53 65 74 43 75 72 73 6F 72 00 BD 01 4C 6F M.SetCursor.S.Lo
00007960 61 64 43 75 72 73 6F 72 57 00 38 00 43 68 65 63 adCursorW.8.Chec
00007970 6B 44 6C 67 42 75 74 74 6F 6E 00 00 3C 01 47 65 kDlgButton.<.Ge
00007980 74 4D 65 73 73 61 67 65 50 6F 73 00 1C 00 43 61 tMessagePos...Ca
00007990 6C 6C 57 69 6E 64 6F 77 50 72 6F 63 57 00 B1 01 llWindowProcW.±.
000079A0 49 73 57 69 6E 64 6F 77 56 69 73 69 62 6C 65 00 IsWindowVisible.
000079B0 42 00 43 6C 6F 73 65 43 6C 69 70 62 6F 61 72 64 B.CloseClipboard
```

Компилятор добавил к функции что-то свое.

Проверяем с помощью IdaPro:

0000000000408178	ShellExecuteExW	SHELL32
000000000040817C	SHGetPathFromIDListW	SHELL32
0000000000408180	SHGetSpecialFolderLocation	SHELL32
0000000000408184	SHGetFileInfoW	SHELL32
0000000000408188	SHFileOperationW	SHELL32
000000000040818C	SHBrowseForFolderW	SHELL32
0000000000408194	GetWindowRect	USER32
0000000000408198	GetSystemMenu	USER32
000000000040819C	SetClassLongW	USER32
00000000004081A0	IsWindowEnabled	USER32
00000000004081A4	SetWindowPos	USER32
00000000004081A8	GetSysColor	USER32
00000000004081AC	GetWindowLongW	USER32
00000000004081B0	SetCursor	USER32
00000000004081B4	LoadCursorW	USER32
00000000004081B8	CheckDlgButton	USER32
00000000004081BC	GetMessagePos	USER32
00000000004081C0	CallWindowProcW	USER32
00000000004081C4	IsWindowVisible	USER32
00000000004081C8	CloseClipboard	USER32
00000000004081CC	SetClipboardData	USER32
00000000004081D0	EmptyClipboard	USER32
00000000004081D4	OpenClipboard	USER32

```

.idata:00408190
.idata:00408194 ;
.idata:00408194 ; Imports from USER32.dll
.idata:00408194 ;
.idata:00408194 ; BOOL __stdcall GetWindowRect(HWND hWnd, LPRECT lpRect)
.idata:00408194 extrn GetWindowRect:dword
.idata:00408194 ; CODE XREF: sub_403EEE+40E↑p
.idata:00408194 ; sub_405601+2C1↑p
.idata:00408194 ; DATA XREF: ...
.idata:00408198 ; HMENU __stdcall GetSystemMenu(HWND hWnd, BOOL bRevert)
.idata:00408198 extrn GetSystemMenu:dword
.idata:00408198 ; CODE XREF: sub_403EEE+2F2↑p
.idata:00408198 ; DATA XREF: sub_403EEE+2F2↑p
.idata:0040819C ; DWORD __stdcall SetClassLongW(HWND hWnd, int nIndex, LONG dwNewLong)
.idata:0040819C extrn SetClassLongW:dword
.idata:0040819C ; CODE XREF: sub_403EEE+197↑p
.idata:0040819C ; DATA XREF: sub_403EEE+197↑p
.idata:004081A0 ; BOOL __stdcall IsWindowEnabled(HWND hWnd)
.idata:004081A0 extrn IsWindowEnabled:dword
.idata:004081A0 ; CODE XREF: sub_403EEE+C5↑p
.idata:004081A0 ; DATA XREF: sub_403EEE+C5↑p
.idata:004081A4 ; BOOL __stdcall SetWindowPos(HWND hWnd, HWND hWndInsertAfter, int X, int Y, int cx, int cy, UINT uFlags)
.idata:004081A4 extrn SetWindowPos:dword
.idata:004081A4 ; CODE XREF: sub_403EEE+3C↑p
.idata:004081A4 ; sub_403EEE+433↑p
.idata:004081A4 ; DATA XREF: ...
.idata:004081A8 ; DWORD __stdcall GetSysColor(int nIndex)
.idata:004081A8 extrn GetSysColor:dword ; CODE XREF: sub_40442E+5B↑p
.idata:004081A8 ; sub_40442E+86↑p ...
.idata:004081AC ; LONG __stdcall GetWindowLongW(HWND hWnd, int nIndex)
.idata:004081AC extrn GetWindowLongW:dword
.idata:004081AC ; CODE XREF: sub_40442E+1D↑p
.idata:004081AC ; sub_404E34+23E↑p
.idata:004081AC ; DATA XREF: ...
.idata:004081B0 ; HCURSOR __stdcall SetCursor(HCURSOR hCursor)
.idata:004081B0 extrn SetCursor:dword ; CODE XREF: sub_404586+202↑p
.idata:004081B0 ; sub_404586+21E↑p
.idata:004081B0 ; DATA XREF: ...

```

● 2 функция

```

00007090 32 8C 00 00 3E 8C 00 00 54 8C 00 00 66 8C 00 00 2B..>B..TB...fB..
000070A0 7A 8C 00 00 90 8C 00 00 9E 89 00 00 92 89 00 00 zB...hB...h%...'%..
000070B0 FA 89 00 00 E6 89 00 00 D8 89 00 00 C6 89 00 00 %%...x%...Ш%...Ж%..
000070C0 B8 89 00 00 AA 89 00 00 76 89 00 00 68 89 00 00 ë%...C%...v%...h%..
000070D0 74 8B 00 00 60 8B 00 00 5A 89 00 00 5A 88 00 00 t<...`<...Z%...Z€..
000070E0 68 88 00 00 7A 88 00 00 8A 88 00 00 96 88 00 00 h€...z€...b€...-€..
000070F0 A8 88 00 00 50 88 00 00 CA 88 00 00 D6 88 00 00 È€...P€...K€...Ц€..
00007100 B4 88 00 00 08 89 00 00 26 89 00 00 EC 88 00 00 r€...%...&%...M€..
00007110 46 89 00 00 34 89 00 00 00 00 00 00 B0 91 00 00 F%...4%.....°'\..
00007120 98 91 00 00 C2 91 00 00 70 91 00 00 5C 91 00 00 .'\.B'\.p'\.\'\..
00007130 82 91 00 00 00 00 00 00 CC 8E 00 00 EE 8E 00 00 ,'. ....Mh..õh..
00007140 FE 8E 00 00 0E 8F 00 00 20 8F 00 00 30 8F 00 00 юh...U...U...0U..
00007150 3E 8F 00 00 50 8F 00 00 5C 8F 00 00 6A 8F 00 00 >U...PU...\U...jU..
00007160 7C 8F 00 00 8C 8F 00 00 9E 8F 00 00 B0 8F 00 00 |U...hU...hU...°U..
00007170 C2 8F 00 00 D6 8F 00 00 F8 8F 00 00 F8 8F 00 00 RU IIII wII mII

```

RVA имени второй функции из второй DLL 0x8EEE

RAW = 0x8EEE - 0x8000 + 0x6A00 = 0x78EE

Переходим:


```

000077D0 65 67 72 6F 75 6E 64 57 69 6E 64 6F 77 00 04 02 egroundWindow...
000077E0 50 6F 73 74 51 75 69 74 4D 65 73 73 61 67 65 00 PostQuitMessage.
000077F0 87 02 53 65 74 57 69 6E 64 6F 77 54 65 78 74 57 #.SetWindowTextW
00007800 00 00 7A 02 53 65 74 54 69 6D 65 72 00 00 56 00 ...z.SetTimer..V.
00007810 43 72 65 61 74 65 44 69 61 6C 6F 67 50 61 72 61 CreateDialogPara
00007820 6D 57 00 00 99 00 44 65 73 74 72 6F 79 57 69 6E mW...DestroyWin
00007830 64 6F 77 00 E1 00 45 78 69 74 57 69 6E 64 6F 77 dow.6.ExitWindow
00007840 73 45 78 00 2C 00 43 68 61 72 4E 65 78 74 57 00 sEx...CharNextW.
00007850 9F 00 44 69 61 6C 6F 67 42 6F 78 50 61 72 61 6D u.DialogBoxParam
00007860 57 00 F9 00 47 65 74 43 6C 61 73 73 49 6E 66 6F W.m.GetClassInfo
00007870 57 00 61 00 43 72 65 61 74 65 57 69 6E 64 6F 77 W.a.CreateWindow
00007880 45 78 57 00 9A 02 53 79 73 74 65 6D 50 61 72 61 ExW...SystemPara
00007890 6D 65 74 65 72 73 49 6E 66 6F 57 00 19 02 52 65 metersInfoW...Re
000078A0 67 69 73 74 65 72 43 6C 61 73 73 57 00 00 C6 00 gisterClassW...Ж.
000078B0 45 6E 64 44 69 61 6C 6F 67 00 31 02 53 63 72 65 EndDialog.1.Scre
000078C0 65 6E 54 6F 43 6C 69 65 6E 74 00 00 74 01 47 65 enToClient...t.Ge
000078D0 74 57 69 6E 64 6F 77 52 65 63 74 00 C2 00 45 6E tWindowRect.B.En
000078E0 61 62 6C 65 4D 65 6E 75 49 74 65 6D 00 00 5C 01 ableMenuItem...\.
000078F0 47 65 74 53 79 73 74 65 6D 4D 65 6E 75 00 48 02 GetSystemMenu.H.
00007900 53 65 74 43 6C 61 73 73 4C 6F 6E 67 57 00 AE 01 SetClassLongW.®.
00007910 49 73 57 69 6E 64 6F 77 45 6E 61 62 6C 65 64 00 IsWindowEnabled.
00007920 83 02 53 65 74 57 69 6E 64 6F 77 50 6F 73 00 00 f.SetWindowPos..
00007930 5A 01 47 65 74 53 79 73 43 6F 6C 6F 72 00 6F 01 Z.GetSysColor.o.
00007940 47 65 74 57 69 6E 64 6F 77 4C 6F 6E 67 57 00 00 GetWindowLongW..
00007950 4D 02 53 65 74 43 75 72 73 6F 72 00 BD 01 4C 6F M.SetCursor.S.Lo
00007960 61 64 43 75 72 73 6F 72 57 00 38 00 43 68 65 63 adCursorW.8.Chec
00007970 6B 44 6C 67 42 75 74 74 6F 6E 00 00 3C 01 47 65 kDlgButton...<.Ge
00007980 74 4D 65 73 73 61 67 65 50 6F 73 00 1C 00 43 61 tMessagePos...Ca

```

● 3 функция

```

000070D0 74 8B 00 00 60 8B 00 00 5A 89 00 00 5A 88 00 00 t<...`<...Z%...Z€..
000070E0 68 88 00 00 7A 88 00 00 8A 88 00 00 96 88 00 00 h€...z€...Ђ€...-€..
000070F0 A8 88 00 00 50 88 00 00 CA 88 00 00 D6 88 00 00 Ё€...P€...K€...Ц€..
00007100 B4 88 00 00 08 89 00 00 26 89 00 00 EC 88 00 00 r€...%...&%...m€..
00007110 46 89 00 00 34 89 00 00 00 00 00 00 B0 91 00 00 F%...4%.....°\..
00007120 98 91 00 00 C2 91 00 00 70 91 00 00 5C 91 00 00 .\..B\..p\..\..
00007130 82 91 00 00 00 00 00 00 CC 8E 00 00 EE 8E 00 00 ,\.....MЂ...оЂ..
00007140 FE 8E 00 00 0E 8F 00 00 20 8F 00 00 30 8F 00 00 оЂ...Ц...Ц...0Ц..
00007150 3E 8F 00 00 50 8F 00 00 5C 8F 00 00 6A 8F 00 00 >Ц...ПЦ...\Ц...jЦ..
00007160 7C 8F 00 00 8C 8F 00 00 9E 8F 00 00 B0 8F 00 00 |Ц...ЂЦ...hЦ...°Ц..
00007170 C2 8F 00 00 D6 8F 00 00 E8 8F 00 00 F8 8F 00 00 БЦ...ЦЦ...иЦ...мЦ..
00007180 BA 8E 00 00 DC 8E 00 00 6E 8D 00 00 3E 90 00 00 еЂ...БЂ...nK...>ђ..
00007190 50 80 00 00 62 80 00 00 78 80 00 00 84 80 00 00 нЂ  бЂ  ..Ђ  Ђ

```

RVA имени третьей функции из второй DLL 0x8EFE

RAW = 0x8EFE - 0x8000 + 0x6A00 = 0x78FE

Переходим:

```

000078A0 67 69 73 74 65 72 43 6C 61 73 73 57 00 00 C6 00 gisterClassW...А.
000078B0 45 6E 64 44 69 61 6C 6F 67 00 31 02 53 63 72 65 EndDialog.1.Scre
000078C0 65 6E 54 6F 43 6C 69 65 6E 74 00 00 74 01 47 65 enToClient...t.Ge
000078D0 74 57 69 6E 64 6F 77 52 65 63 74 00 C2 00 45 6E tWindowRect.B.En
000078E0 61 62 6C 65 4D 65 6E 75 49 74 65 6D 00 00 5C 01 ableMenuItem...\.
000078F0 47 65 74 53 79 73 74 65 6D 4D 65 6E 75 00 48 02 GetSystemMenu.Ђ.
00007900 53 65 74 43 6C 61 73 73 4C 6F 6E 67 57 00 AE 01 SetClassLongW.®.
00007910 49 73 57 69 6E 64 6F 77 45 6E 61 62 6C 65 64 00 IsWindowEnabled.
00007920 83 02 53 65 74 57 69 6E 64 6F 77 50 6F 73 00 00 f.SetWindowPos..

```


- 4 функция

```

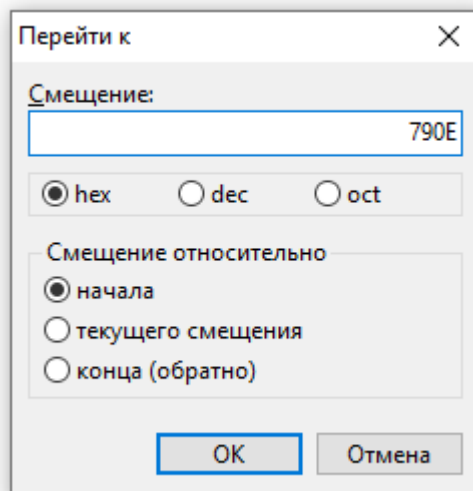
00007110 46 89 00 00 34 89 00 00 00 00 00 00 B0 91 00 00 F%...4%.....°\..
00007120 98 91 00 00 C2 91 00 00 70 91 00 00 5C 91 00 00 .\..B\..p\..\..
00007130 82 91 00 00 00 00 00 00 CC 8E 00 00 EE 8E 00 00 ,\.....M%..o%..
00007140 FE 8E 00 00 0E 8F 00 00 20 8F 00 00 30 8F 00 00 ю%...%.. %..O%..
00007150 3E 8F 00 00 50 8F 00 00 5C 8F 00 00 6A 8F 00 00 >%..P%..\%..j%..
00007160 7C 8F 00 00 8C 8F 00 00 9E 8F 00 00 B0 8F 00 00 |%..%..%..°%..
00007170 C2 8F 00 00 D6 8F 00 00 E8 8F 00 00 F8 8F 00 00 B%..%..и%..m%..
00007180 BA 8E 00 00 DC 8E 00 00 6E 8D 00 00 3E 90 00 00 e%..b%..n%..>%..
00007190 50 90 00 00 62 90 00 00 78 90 00 00 84 90 00 00 P%..b%..x%..%..

```

RVA имени четвертой функции из второй DLL 0x8F0E

$$RAW = 0x8F0E - 0x8000 + 0x6A00 = 0x790E$$

Переходим:


















```

00007890 6D 65 74 65 72 73 49 6E 66 6F 57 00 19 02 52 65 metersInfoW...Re
000078A0 67 69 73 74 65 72 43 6C 61 73 73 57 00 00 C6 00 gisterClassW...Ж.
000078B0 45 6E 64 44 69 61 6C 6F 67 00 31 02 53 63 72 65 EndDialog.1.Scre
000078C0 65 6E 54 6F 43 6C 69 65 6E 74 00 00 74 01 47 65 enToClient...t.Ge
000078D0 74 57 69 6E 64 6F 77 52 65 63 74 00 C2 00 45 6E tWindowRect.B.En
000078E0 61 62 6C 65 4D 65 6E 75 49 74 65 6D 00 00 5C 01 ableMenuItem...\
000078F0 47 65 74 53 79 73 74 65 6D 4D 65 6E 75 00 48 02 GetSystemMenu.H.
00007900 53 65 74 43 6C 61 73 73 4C 6F 6E 67 57 00 AE 01 SetClassLongW.%
00007910 49 73 57 69 6E 64 6F 77 45 6E 61 62 6C 65 64 00 IsWindowEnabled.
00007920 83 02 53 65 74 57 69 6E 64 6F 77 50 6F 73 00 00 f.SetWindowPos..
00007930 5A 01 47 65 74 53 79 73 43 6F 6C 6F 72 00 6F 01 Z.GetSysColor.o.
00007940 47 65 74 57 69 6E 64 6F 77 4C 6F 6E 67 57 00 00 GetWindowLongW..
00007950 4D 02 53 65 74 43 75 72 73 6F 72 00 BD 01 4C 6F M.SetCursor.S.Lo
00007960 61 64 43 75 72 73 6F 72 57 00 38 00 43 68 65 63 adCursorW.8.Chec
00007970 6B 44 6C 67 42 75 74 74 6F 6E 00 00 3C 01 47 65 kDlgButton...<.Ge

```

Проверяем с помощью IdaPro:

 0000000000408180	SHGetSpecialFolderLocation	SHELL32
 0000000000408184	SHGetFileInfoW	SHELL32
 0000000000408188	SHFileOperationW	SHELL32
 000000000040818C	SHBrowseForFolderW	SHELL32
 0000000000408194	GetWindowRect	USER32
 0000000000408198	GetSystemMenu	USER32
 000000000040819C	SetClassLongW	USER32
 00000000004081A0	IsWindowEnabled	USER32
 00000000004081A4	SetWindowPos	USER32
 00000000004081A8	GetSysColor	USER32
 00000000004081AC	GetWindowLongW	USER32
 00000000004081B0	SetCursor	USER32
 00000000004081B4	LoadCursorW	USER32
 00000000004081B8	CheckDlgButton	USER32
 00000000004081BC	GetMessagePos	USER32

Ответ: 2 библиотека - **USER32.dll**, 4 функция - **IsWindowEnabled**.