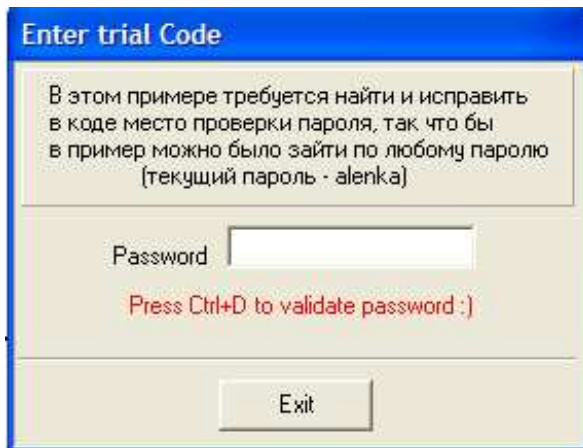
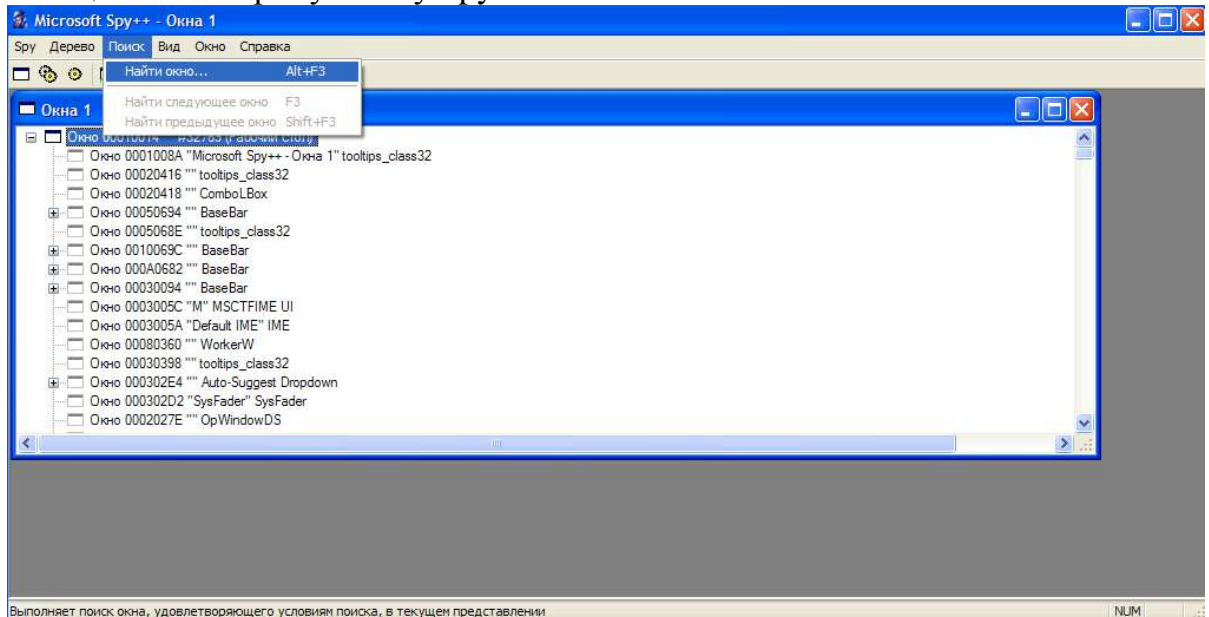


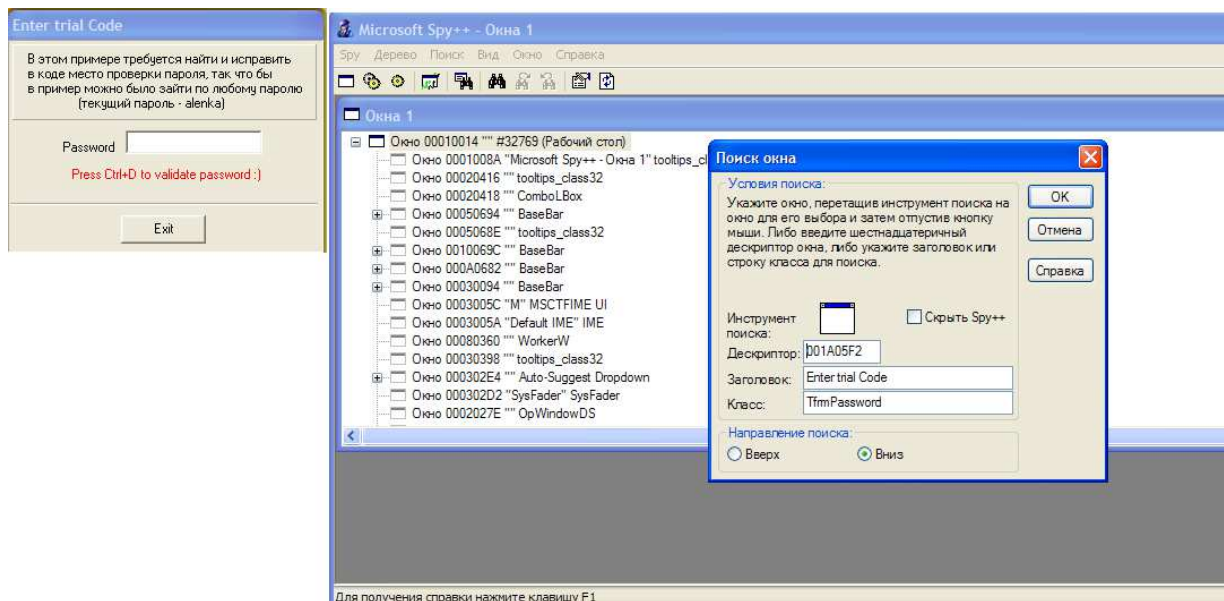
1. Запустили под отладчиком.



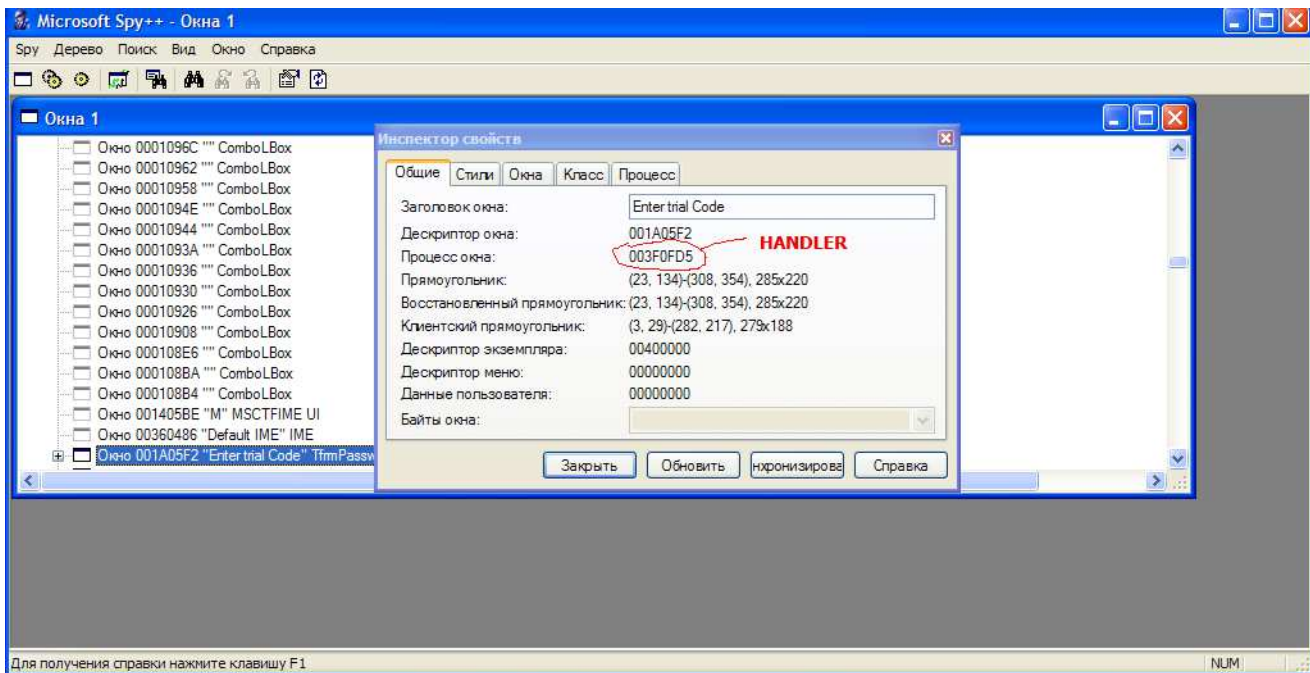
2. Ищем окно через утилиту Spy++.



3. Вот как это делается:



4. Целью поиска является обработчик сообщений окна. (WndProc).



5. Нашли его, так он выглядит в отладчике. Ставим на него брейкпоинт.

003F0FD5	E8 2AF0FFFF	CALL 003F0004
003F0FDA	88BF 41002C55	MOV BYTE PTR DS:[EDI+0x552C0041],BH
003F0FE0	93	XCHG EAX,EBX
003F0FE1	00E8	ADD AL,CH
003F0FE3	1D F0FFFF88	SBB EAX,0x88FFFFFFF0
003F0FEB	BF 41000C52	MOV EDI,0x520C0041
003F0FED	93	XCHG EAX,EBX
003F0FEE	00E8	ADD AL,CH
003F0FF0	10F0	ADC AL,DH

6. Теперь переведём фокус ввода на окно крямки, что коно получило какое-то сообщение и брейкпоинт сработал. Протрассируем пару инструкций, и мы попадаем в обработчик такого вида. Далее нашей задачей является поиск метаобъектной информации.

004229E0	. 55	PUSH EBP
004229E1	. 8BEC	MOV EBP,ESP
004229E3	. 31C0	XOR EAX,EAX
004229E5	. 50	PUSH EAX
004229E6	. FF75 14	PUSH DWORD PTR SS:[EBP+0x14]
004229E9	. FF75 10	PUSH DWORD PTR SS:[EBP+0x10]
004229EC	. FF75 0C	PUSH DWORD PTR SS:[EBP+0x0C]
004229EF	. 89E2	MOV EDX,ESP
004229F1	. 8B41 04	MOV EAX,DWORD PTR DS:[ECX+0x4]
004229F4	. FF11	CALL DWORD PTR DS:[ECX]
004229F6	. 83C4 0C	ADD ESP,0xC
004229F9	. 58	POP EAX
004229FA	. 5D	POP EBP
004229FB	. C2 1000	RETN 0x10

7. Стоя на адресе из скриншота (который ниже), видим, что в eax ложится адрес с этой самой метаобъектной инфой.

Address	Value	Comment
004229E1	. 8BEC	MOV EBP, ESP
004229E3	. 31C0	XOR EAX, EAX
004229E5	. 50	PUSH EAX
004229E6	. FF75 14	PUSH DWORD PTR SS:[EBP+0x14]
004229E9	. FF75 10	PUSH DWORD PTR SS:[EBP+0x10]
004229EC	. FF75 0C	PUSH DWORD PTR SS:[EBP+0xC]
004229EF	. 89E2	MOV EDX, ESP
004229F1	. 8B41 04	MOV EAX, DWORD PTR DS:[ECX+0x4]
004229F4	. FF11	CALL DWORD PTR DS:[ECX]
004229F6	. 83C4 0C	ADD ESP, 0xC
004229F9	. 58	POP EAX
004229FA	. 5D	POP EBP
004229FB	. C2 1000	RETN 0x10
004229FE	. 8BC0	MOV EAX, EAX
00422A00	. 83C0 05	ADD EAX, 0x5
00422A03	. 2BD0	SUB EDX, EAX
00422A05	. 8BC2	MOV EAX, EDX
00422A07	. C3	RETN
00422A08	. 55	PUSH EBP
00422A09	. 8BEC	MOV EBP, ESP
00422A0B	. 53	PUSH EBX
00422A0C	. 56	PUSH ESI
00422A0E	. 57	PUSH EDI
00422A0F	. BF DC464300	MOV EDI, HACKME1.004346DC

Registers (FPU)

Register	Value
EAX	0093552C
ECX	003F0FDA
EDX	0012FD48
EBX	00000000
ESP	0012FD48
EBP	0012FD58
ESI	003F0FD5
EDI	0012FE84

DS: [003F0FDA]=0041BF88 (HACKME1.0041BF88)

Address	Value	Comment
0093552C	004313F0	HACKME1.004313F0
00935530	009350B4	
00935534	009369D8	ASCII "frmPassword"
00935538	00000000	
0093553C	00936B74	
00935540	00000000	
00935544	00000000	
00935548	00000000	
0093554C	00000100	
00935550	00000000	
00935554	00424460	HACKME1.00424460
00935558	0093552C	

8. По первому двойному слову читаем значение и переходим по прочитанному адресу:

Address	Value	Comment
004313CF	00	DB 00
004313D0	. F9144300	DD HACKME1.004314F9
004313D4	FC	DB FC
004313D5	01	DB 01
004313D6	00	DB 00
004313D7	00	DB 00
004313D8	. D81A4200	DD HACKME1.00421AD8
004313DC	. 10FA4000	DD HACKME1.0040FA10
004313E0	. 40524200	DD HACKME1.00425240
004313E4	. 40284000	DD HACKME1.00402840
004313E8	. 54284000	DD HACKME1.00402854
004313EC	. 38384200	DD HACKME1.00423838
004313F0	. 24864000	DD HACKME1.00408624
004313F4	. 043F4200	DD HACKME1.00423F04
004313F8	. 20B54000	DD HACKME1.0040B520
004313FC	. 603C4200	DD HACKME1.00423C60
00431400	. 983C4200	DD HACKME1.00423C98
00431404	. 203D4200	DD HACKME1.00423D20
00431408	. 389E4100	DD HACKME1.00419E38
0043140C	. 24444200	DD HACKME1.00424424
00431410	. 84F64000	DD HACKME1.0040F684
00431414	. 9C384200	DD HACKME1.0042389C
00431418	. CCDC4100	DD HACKME1.0041DCCC
0043141C	. 78414200	DD HACKME1.00424178

ASCII 0C, "TfrmPassword"

Entry address

Entry address

Entry address

Address	Value	Comment
0093552C	004313F0	HACKME1.004313F0
00935530	009350B4	

Здесь мы видим обработчики формы. Но нас интересует обработчик нажатия на Ctrl+D. Элементы на форме всегда располагаются в виде дерева. Т.е. главная форма, на ней всякие кнопки, менюшки и т.д. с различной вложенностью. Каждый из таких элементов сам может иметь разные обработчики. Для их поиска просто прокрутим окно кода чуток ниже.

9. Прокрутили вот сюда:

004314E5	. 44154300	DD HACKME1.00431544
004314E9	. 0F	DB 0F
004314EA	. 43 6F 64 65 45	ASCII "CodeEditKeyDown"
004314F9	. 0C	DB 0C
004314FA	. 54 66 72 6D 50	ASCII "TfrmPassword"

А вот и наш заветный адресок 00431544. За сим всё.