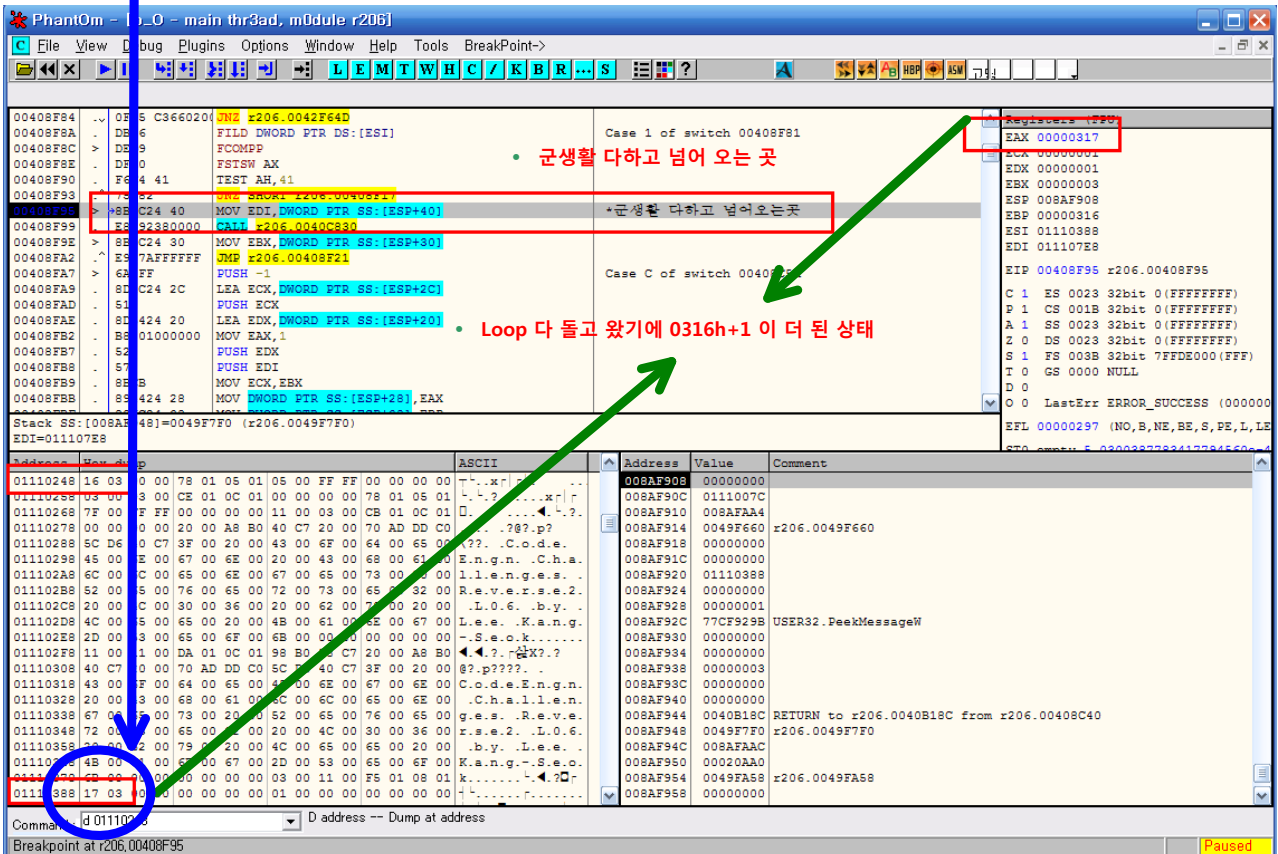
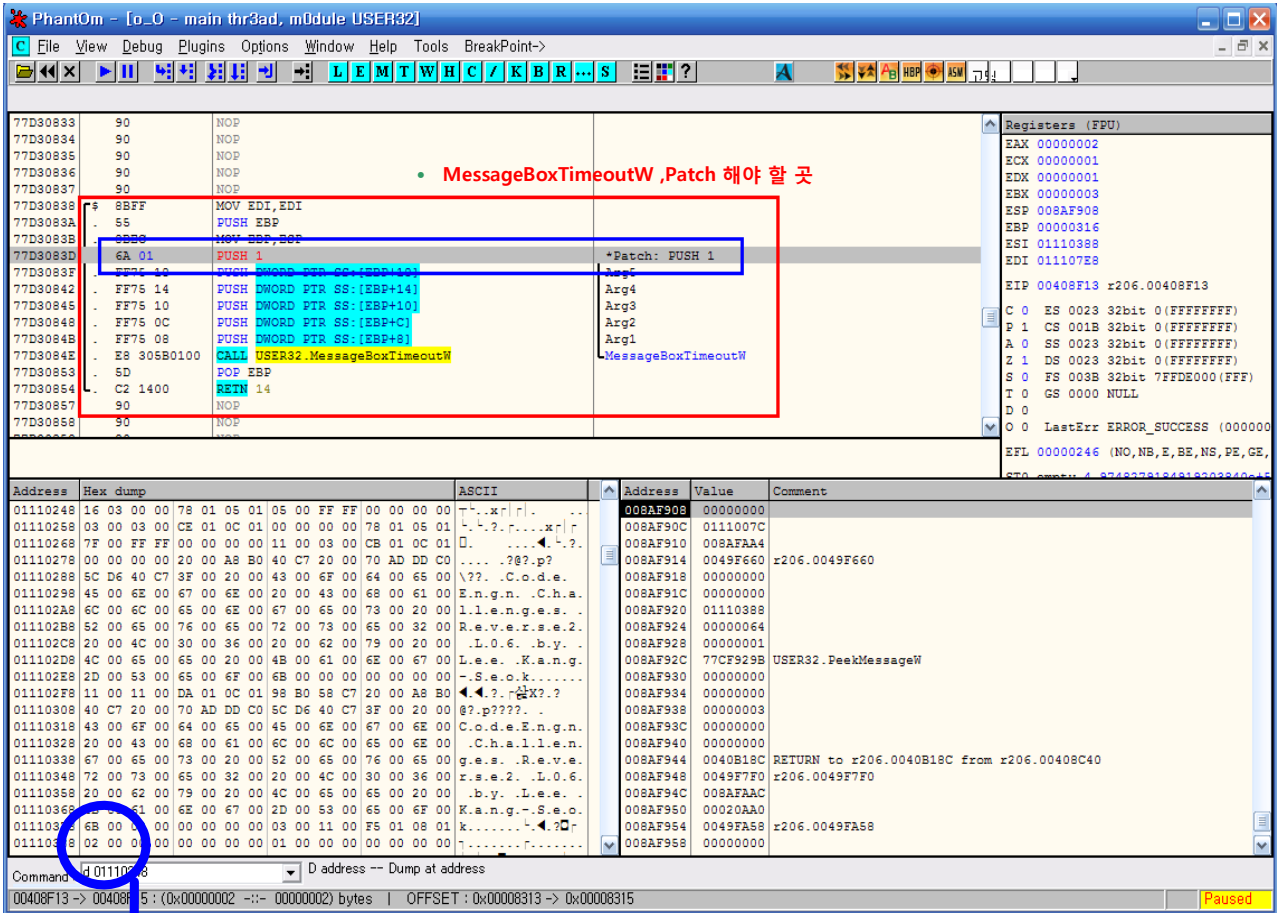


- **MessageBoxTimeoutW 형식**

MessageBoxTimeoutW(HWND hWnd, LPCWSTR lpText, LPCWSTR lpCaption,
UINT uType, WORD wLanguageId, **DWORD dwMilliseconds**)



Phantom - [o_O - main thr3ad, module r206]

File View Debug Plugins Options Window Help Tools BreakPoint->

LEMTWHCKBR...S

0040B446	53	PUSH EBX			
0040B447	E8 2460FFFF	JMP r206.00401470			
0040B44C	6A 00	PUSH 0			
0040B44E	FF15 ECD670	CALL DWORD PTR DS:[<USER32.LockWindowUpdate>]	hWnd = NULL		
0040B454	8B0D 08E9480	MOV ECX, DWORD PTR DS:[48E908]	LockWindowUpdate		
0040B45A	51	PUSH ECX			
0040B45B	FF15 DCD570	CALL DWORD PTR DS:[<USER32.DestroyWindow>]	hWnd => 009A03E8 ('AutoIt v3', class='AutoIt v3')		
0040B461	8B35 E8D670	MOV ESI, DWORD PTR DS:[<USER32.GetMessageW>]	*참 달하는 곳		
0040B467	6A 00	PUSH 0	USER32.GetMessageW		
0040B469	6A 00	PUSH 0	MsgFilterMax = 0		
0040B46B	6A 00	PUSH 0	MsgFilterMin = 0		
0040B46D	8D9424 40010	LEA EDI, DWORD PTR SS:[ESP+140]	hWnd = NULL		
0040B474	52	PUSH EDI			
0040B475	FFD6	CALL ESI	pMsg		
0040B477	85C0	TEST EAX, EAX	GetMessageW		
0040B479	0FBF 0056020	JNZ r206.004030A7F			
0040B47F	33C0	XOR EAX, EAX			
0040B481	5F	POP EDI			
0040B482	5E	POP ESI			

Registers (FPU)

EAX 00000000
ECX 009A03E8
EDX 7C93E4F4 ntdll.KiFastSystemCal
EBX 0049F660 r206.0049F660
ESP 008AF94C
EBP 008AF94C
ESI 77CF929B USER32.PeekMessageW
EDI 00000001
EIP 0040B45B r206.0040B45B
C 0 ES 0023 32bit 0 (FFFFFFFF)
P 1 CS 001B 32bit 0 (FFFFFFFF)
A 1 SS 0023 32bit 0 (FFFFFFFF)
Z 0 DS 0023 32bit 0 (FFFFFFFF)
S 0 FS 003B 32bit 7FFDE000 (FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_INVALID_PARAMET
EFL 00000216 (NO, NB, NE, A, NS, PE, GE,
ETO error 5 0200327282417284560e4

DS:[0047D5DC]=77D0B19C (USER32.DestroyWindow)

Address	Hex dump	ASCII	Address	Value	Comment
01110248	16 03 00 00 78 01 05 01 05 00 FF FF 00 00 00 00x.....	008AF94C	009A03E8	hWnd = 009A03E8 ('AutoIt v3', class='AutoIt v3')
01110258	03 00 03 00 CE 01 0C 01 00 00 00 00 78 01 05 01x.....	008AF950	00020AA0	
01110268	7F 00 FF FF 00 00 00 00 11 00 03 00 CB 01 0C 01?.....	008AF954	0049FA58	r206.0049FA58
01110278	00 00 00 00 20 00 A8 B0 40 C7 20 00 70 AD DD C0?p?	008AF958	00000000	
01110288	5C D6 40 C7 3F 00 20 00 43 00 6F 00 64 00 65 00	...C.o.d.e.	008AF95C	00000000	
01110298	45 00 6E 00 67 00 6E 00 20 00 43 00 68 00 61 00	E.n.g.n..C.h.a.	008AF960	00000000	
011102A8	6C 00 6C 00 65 00 6E 00 67 00 65 00 73 00 20 00	l.l.e.n.g.e.s.	008AF964	01110F28	
011102B8	52 00 65 00 76 00 65 00 72 00 73 00 65 00 32 00	R.e.v.e.r.s.e.2.	008AF968	01110F28	
011102C8	20 00 4C 00 30 00 36 00 20 00 62 00 79 00 20 00	.L.O.6..b.y..	008AF96C	00000000	
011102D8	4C 00 65 00 65 00 20 00 4B 00 61 00 6E 00 67 00	L.e.e..K.a.n.g.	008AF970	00000003	
011102E8	2D 00 53 00 65 00 6F 00 6B 00 00 00 00 00 00 00	-S.e.o.k.....	008AF974	00000000	
011102F8	11 00 11 00 DA 01 0C 01 98 B0 58 C7 20 00 A8 B0X?..?	008AF978	00000000	
01110308	40 C7 20 00 70 AD DD C0 5C D6 40 C7 3F 00 20 00	?p????	008AF97C	00000000	
01110318	43 00 6F 00 64 00 65 00 45 00 6E 00 67 00 6E 00	C.o.d.e.E.n.g.n.	008AF980	00000000	
01110328	20 00 43 00 68 00 61 00 6C 00 6C 00 65 00 6E 00	.C.h.a.l.l.e.n.	008AF984	00000000	
01110338	67 00 65 00 73 00 20 00 52 00 65 00 76 00 65 00	g.e.s..R.e.v.e.	008AF988	00492278	ASCII "GyF"
01110348	72 00 73 00 65 00 32 00 20 00 4C 00 30 00 36 00	r.s.e.2..L.O.6.	008AF98C	01110F70	
01110358	20 00 62 00 75 00 20 00 4C 00 65 00 65 00 20 00	.b.y..L.e.e..	008AF990	00000000	
01110368	48 00 61 00 6E 00 67 00 2D 00 53 00 65 00 6F 00	K.a.n.g.-S.e.o.	008AF994	00000004	
01110378	68 00 00 00 00 00 00 00 03 00 11 00 F5 01 08 01	k.....?...	008AF998	00000000	
01110388	17 03 00 00 00 00 00 00 01 00 00 00 00 00 00 00	008AF99C	00000000	

Command: d 01110248 D address -- Dump at address

Breakpoint at r206.0040B45B

Paused

- 남은 군생할 : 0316h => 790 => 2DACE78F80BC92E6D7493423D729448E
- -끝-