



- 맨 밑에 Number of trials 8 이라면  
서 남은 실행횟수를 알려준다.
- 체험판이라 이 남은 횟수만큼 실행  
할 수 있도록 하고, 남은 횟수만큼  
다 사용하면 original판을 구매하라  
고 나온다.

00489310	. 6A FF	push FFFFFFFF	sub_489310
00489312	. 64:A1 00000000	mov eax,dword ptr fs:[0]	eax:"뽕"
00489318	. 68 BC7C4C00	push <visualsite designer.sub_4C7CBC>	4C7CBC:"뽕>N"
0048931D	. 50	push eax	eax:"뽕"
0048931E	. B8 60870000	mov eax,8760	eax:"뽕"
00489323	. 64:8925 00000000	mov dword ptr fs:[0],esp	
0048932A	. E8 E13F0300	call <visualsite designer.sub_4BD310>	
0048932F	. 53	push ebx	
00489330	. 55	push ebp	

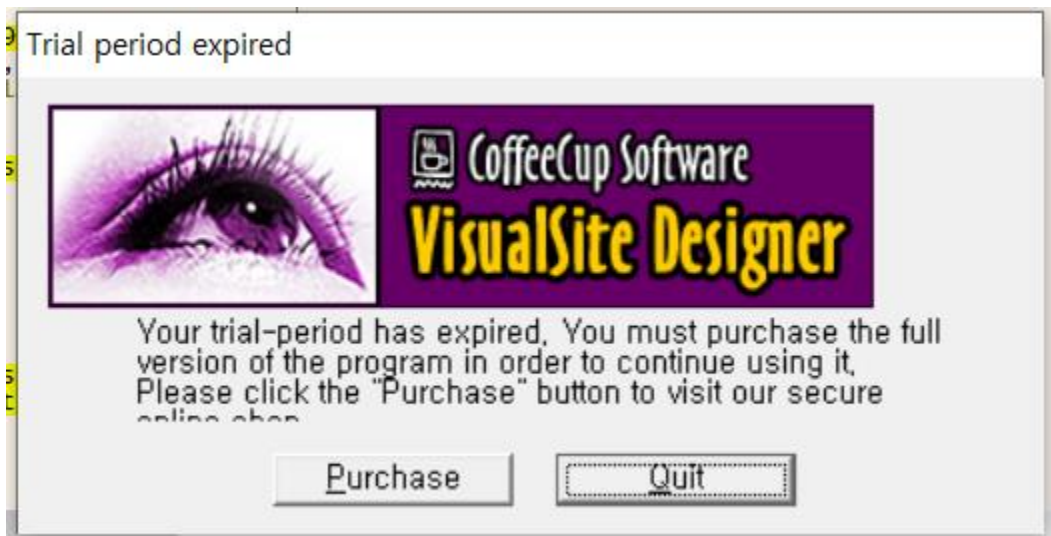
004898ED	. 6A 00	push 0	
004898EF	. 85C0	test eax,eax	
004898F1	. 0F8E A1000000	jle visualsite designer.489998	
004898F7	. 8D8C24 10020000	lea ecx,dword ptr ss:[esp+210]	
004898FE	. E8 6D240200	call <visualsite designer.sub_4ABD70>	
00489903	. 8D8C24 0C020000	lea ecx,dword ptr ss:[esp+20C]	
0048990A	. C68424 78870000 0B	mov byte ptr ss:[esp+8778],B	
00489912	. E8 132B0300	call <JMP.&Ordinal#2514>	
00489917	. 83F8 01	cmp eax,1	
0048991A	. 74 40	je visualsite designer.48995C	
0048991C	. 8BCF	mov ecx,edi	
0048991F	. 58 00F65555	call <visualsite designer.sub_489520>	

- ctrl + 8을 눌러 첫 실행 화면이 나올 때까지 실행한다. 그러면 실행할 때마다 call한 부분에서 멈추고, 실행하는데, 하나 하나 call 명령을 따라가다보니 해당 부분에서 최종적으로 함수를 불러 프로그램을 실행하는 것을 볼 수 있다.
- 그리고 이 부분에서 또 ctrl + 8을 눌러 실행하면 해당 부분에서 멈추고 프로그램을 실행하는걸 볼 수 있다.

004898CC	. E8 AFF0FFFF	call <visualsite designer.sub_488980>
004898D1	. 84C0	test al,al
004898D3	. 0F84 FF000000	je visualsite designer.4899D8
004898D9	. 8A87 E0000000	mov al,byte ptr ds:[edi+E0]
004898DF	. 84C0	test al,al
004898E1	. 0F85 42010000	jne visualsite designer.489A29
004898E7	. 8B87 E4000000	mov eax,dword ptr ds:[edi+E4]
004898ED	. 6A 00	push 0
004898EF	. 85C0	test eax,eax
004898F1	. 0F8E A1000000	jle visualsite designer.489998
004898F7	. 8D8C24 10020000	lea ecx,dword ptr ss:[esp+210]
004898FE	. E8 6D240200	call <visualsite designer.sub_4ABD70>
00489903	. 8D8C24 0C020000	lea ecx,dword ptr ss:[esp+20C]
0048990A	. C68424 78870000 0B	mov byte ptr ss:[esp+8778],B

004898ED	. 6A 00	push 0
004898EF	. 85C0	test eax,eax
004898F1	. 0F8E A1000000	jle visualsite designer.489998
004898F7	. 8D8C24 10020000	lea ecx,dword ptr ss:[esp+210]

- 그럼 그전에 실행 횟수를 제어하는 코드가 있을것으로 예상돼 함수가 호출되기 전 코드를 살펴본다.
- 비교 구문 test를 위주로 살펴봤다. 4898EF부분에 bp를 걸고 실행한다.test eax, eax를 하여 결과 값이 0보다 같거나 작은지 비교한다. 작거나 같으면 489998 부분으로 점프한다.(아니면 그대로 실행해 아까처럼 제한 횟수 창이 뜬다.)
- ZF=1로 설정해 점프하게 만든 후 실행 결과를 본다.




004898D3	0F84 FF000000	jle visualsite designer.4899D8
004898D9	8A87 E0000000	mov al,byte ptr ds:[edi+E0]
004898DF	84C0	test al,al
004898E1	0F85 42010000	jne visualsite designer.489A29
004898E7	8B87 E4000000	mov eax,dword ptr ds:[edi+E4]
004898ED	6A 00	push 0
004898EF	85C0	test eax,eax
004898F1	0F8E A1000000	jle visualsite designer.489998
004898F7	8B87 E4000000	mov eax,dword ptr ds:[edi+E4]

- 점프하면 이렇게 체험판이 끝났으면서, 살건지 아니면 끝낼건지 물어보는 창이 나온다. 이 부분도 우회해 프로그램을 바로 실행할 수 있도록 한다.
- 아까 test문 위에 보면 또 test 부분이 있는데, 이 부분에 bp를 걸고 실행했다. ZF=1로 설정되어 있는걸 Z=0으로 설정하니 프로그램이 바로 실행되는걸 볼 수 있었다.
- 해당 부분은 0이냐 1이냐에 따라 해 체험판인지 아닌지를 구분하는 것 같다. 같으면 체험판이고, 아니면 오리지널 버전으로 실행한다는 의미인것 같다.

- 그리고 마지막으로 우회할 것은 프로그램 종료시 실행되는 광고창이다.
- 이 부분을 안뜨게 우회한다.
- 프로그램을 종료하고, F12를 눌러 일시정지 시킨 후, 콜 스택을 확인한다.

CoffeeCup VisualSite Designer

 **Please check out our other great services for your Website:**



**Submit your Website to over  
3,000 Search Engines & Directories  
for only \$7.95/mo !**


 Sign up now & get **1 year** of Search Engine Submission for only \$79.  
That's 2 months for free !

[Click Here](#)



**Great Web Hosting starting at \$9.95/mo.**

Host a New Website or Transfer your current Website & get over  
**\$300 of CoffeeCup Software Free !**

 **No Setup Fees  
24/7 Live Support  
99.9% Uptime**

[Click Here](#)

0019EB30	6AB44425	7741106C	44	win32u.7741106C	시스템
0019EB74	6AB70ADD	6AB44425	48	mfc42.6AB44425	시스템
0019EBBC	00480C29	6AB70ADD	78	mfc42.6AB70ADD	사용자
0019EC34	6AB3C51B	00480C29	98	visualsite designer_dump.00480C29	시스템
0019ECCC	6AB43B84	6AB3C51B	28	mfc42.6AB3C51B	시스템
0019ECF4	6AB3BD7B	6AB43B84	80	mfc42.6AB43B84	시스템

00480C13	E8 2855FEFF	call visualsite designer_dump.403F40
00480C18	8D4C24 00	lea ecx,dword ptr ss:[esp]
00480C1C	C74424 68 00000000	mov dword ptr ss:[esp+68],0
00480C24	E8 01B80300	call <JMP.&ordinal#2514>
00480C29	8D4C24 00	lea ecx,dword ptr ss:[esp]
00480C2D	C74424 68 FFFFFFFF	mov dword ptr ss:[esp+68],FFFFFFFF
00480C35	E8 DEBA0300	call <JMP.&ordinal#641>
00480C3A	8B4C24 60	mov ecx,dword ptr ss:[esp+60]
00480C3E	64:890D 00000000	mov dword ptr [es:[0]],ecx
00480C45	83C4 6C	add esp,6C

00480C18	8D4C24 00	lea ecx,dword ptr ss:[esp]
00480C1C	C74424 68 00000000	mov dword ptr ss:[esp+68],0
00480C24	90	nop
00480C25	90	nop
00480C26	90	nop
00480C27	90	nop
00480C28	90	nop
00480C29	8D4C24 00	lea ecx,dword ptr ss:[esp]
00480C2D	C74424 68 FFFFFFFF	mov dword ptr ss:[esp+68],FFFFFFFF
00480C35	E8 DEBA0300	call <JMP.&ordinal#641>
00480C3A	8B4C24 60	mov ecx,dword ptr ss:[esp+60]

- 프로그램을 종료하고, 광고가 나오면 F12를 눌러 일시 정지 후, 콜스택을 본다.
- 가장 상단에 있는 visualsite designer가 보인다. 해당 부분에서 call했을 것이다.
- 해당 부분으로 이동하면, 바로 위에 call 명령이 보인다. 이 부분에서 광고를 호출하는 것 같다.
- 해당 부분을 NOP으로 채워준 후 실행하면 이제 광고창이 안 뜨는걸 볼 수 있다.