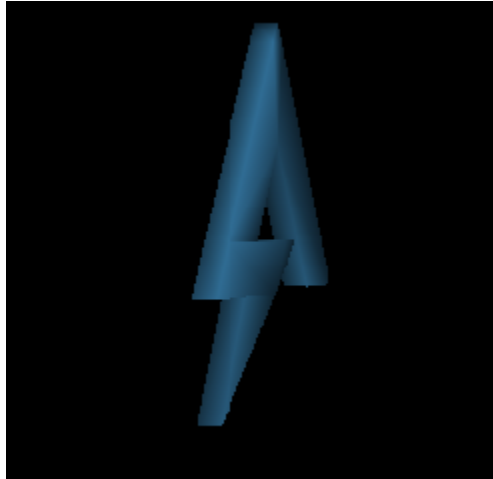
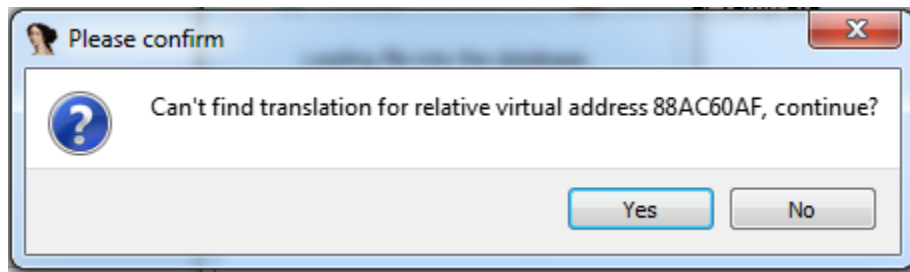


Demo

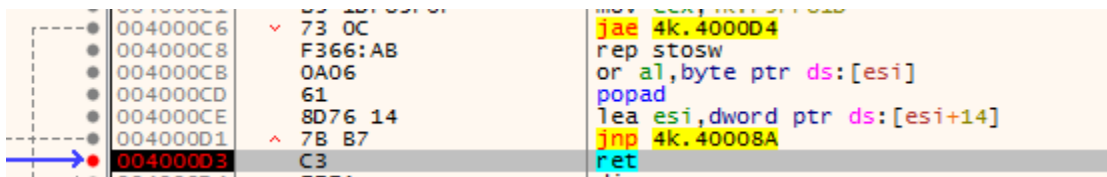
Chạy thử chương trình ta thấy:



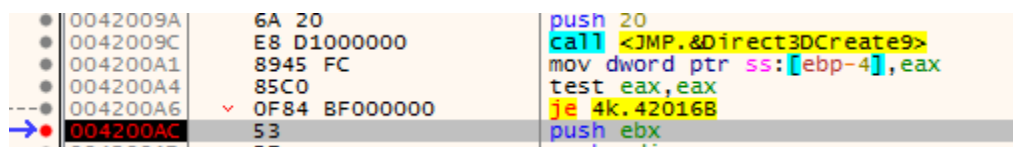
Mở chương trình bằng IDA Pro thì có vẻ như chương trình đã bị packed



Chạy chương trình bằng x64dbg, chương trình sau khi chạy đến instruction return thì chương trình chính đã được unpack xong



Chương trình sử dụng thư viện DirectX 9 để render



Trong hàm 4201FF có gọi đến hàm 4202A8 hai lần:

0042021C	E8 87000000	call 4k.4202A8
00420221	68 C372AF84	push 84AF72C3
00420226	68 F0817B86	push 867B81F0
0042022B	68 C843B30C	push 4k.CB343C8
00420230	68 0A010000	push 10A
00420235	68 A8164200	push 4k.4216A8
0042023A	68 28010000	push 128
0042023F	68 C8084200	push 4k.4208C8
00420244	A3 50004300	mov dword ptr ds:[430050]
00420249	E8 5A000000	call 4k.4202A8

Trong hàm 4202A8 có gọi đến hai hàm trong thư viện DirectX là

004202C7	57	push esi
004202C8	E8 B1FEFFFF	call <JMP.&D3DXCreateMeshFVF>
004202CD	8B45 FC	mov eax,dword ptr ss:[ebp-4]
00420378	E8 F8FDFFFF	call <JMP.&D3DXComputeNormals>
00420380	8B45 FC	mov eax,dword ptr ss:[ebp-4]
00420383	FF	pop edi

Hàm D3DXComputeNormals sẽ trả ra địa chỉ chứa object được render

push 0
push dword ptr ss:[ebp-4]
call <JMP.&D3DXComputeNormals>
mov eax,dword ptr ss:[ebp-4]
pop edi
pop esi
pop ebx
20F3FF30 21094538
20F3FF34 00000000

Object đầu tiên có địa chỉ 0x21094538

push 0
push dword ptr ss:[ebp-4]
call <JMP.&D3DXComputeNormals>
mov eax,dword ptr ss:[ebp-4]
pop edi
pop esi
pop ebx
20F3FF14 210948C8
20F3FF18 00000000

Object thứ 2 có địa chỉ 0x210948C8

Tiếp theo ta sẽ gặp được một vòng lặp

00420153	6A 00	push 0
00420155	E8 30020000	call 4k.42038A
0042015A	83C4 04	add esp,4
0042015D	6A 1B	push 1B
0042015F	FFD6	call esi
00420161	66:85C0	test ax,ax
00420164	74 ED	je 4k.420153

Đây là vòng lặp dùng để render từng frame của chương trình

Debug hàm 42038A ta sẽ thấy

004204DD	FF91 80000000	call dword ptr ds:[ecx+80]
004204E3	A1 50004300	mov eax,dword ptr ds:[430050]
004204E8	6A 00	push 0
004204EA	50	push eax
004204EB	8B08	mov ecx,dword ptr ds:[eax]
004204ED	FF51 0C	call dword ptr ds:[ecx+C]
00420524	A1 54004300	mov eax,dword ptr ds:[430054]
00420529	6A 00	push 0
0042052B	50	push eax
0042052C	8B08	mov ecx,dword ptr ds:[eax]
0042052E	FF51 0C	call dword ptr ds:[ecx+C]

2 địa chỉ này được load vào hàm chứa trong ecx+C

004204DD	FF91 80000000	call dword ptr ds:[ecx+80]
004204E3	A1 50004300	mov eax,dword ptr ds:[430050]
004204E8	6A 00	push 0
004204EA	50	push eax
004204EB	8B08	mov ecx,dword ptr ds:[eax]
004204ED	FF51 0C	call dword ptr ds:[ecx+C]
004204F0	8D85 00FFFFFF	lea eax,dword ptr ss:[ebp-100]
004204F6	50	push eax
004204F7	8D85 C0FFFFFF	lea eax,dword ptr ss:[ebp-140]
004204FD	50	push eax
004204FE	8D85 80FFFFFF	lea eax,dword ptr ss:[ebp-180]
00420504	50	push eax
00420505	58 80CCEEEE	call 4k.420505

eax=0
dword ptr [4k.00430050]=21094538

Sau khi thay đổi địa chỉ chứa trong 430050 thành địa chỉ chứa trong 430054

004204DD	FF91 80000000	call dword ptr ds:[ecx+80]
004204E3	A1 50004300	mov eax,dword ptr ds:[430050]
004204E8	6A 00	push 0
004204EA	50	push eax
004204EB	8B08	mov ecx,dword ptr ds:[eax]
004204ED	FF51 0C	call dword ptr ds:[ecx+C]
004204F0	8D85 00FFFFFF	lea eax,dword ptr ss:[ebp-100]
004204F6	50	push eax
004204F7	8D85 C0FFFFFF	lea eax,dword ptr ss:[ebp-140]
004204FD	50	push eax
004204FE	8D85 80FFFFFF	lea eax,dword ptr ss:[ebp-180]
00420504	50	push eax
00420505	EB 80FFFFFF	call <MP_8030VMatrixMultiply>

eax=0
dword ptr [4k.00430050]=210948C8

Ta có được Flag

