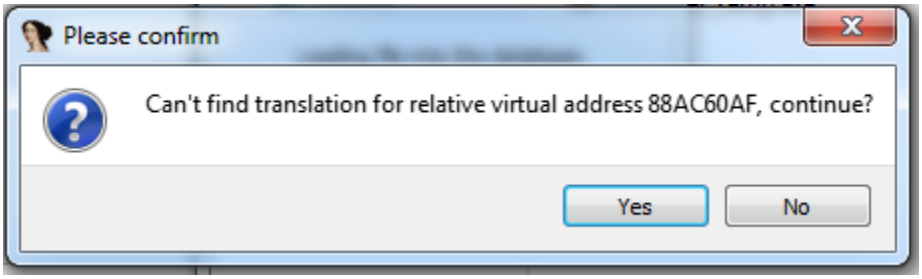
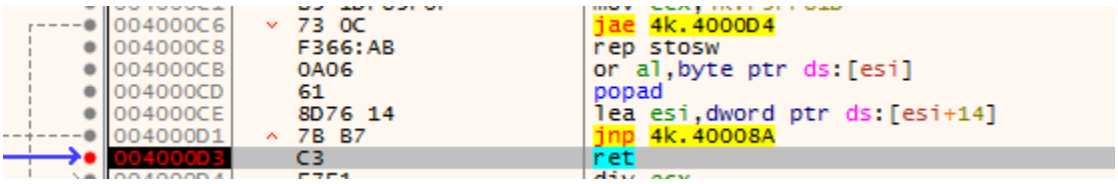
Demo

Chạy thử chương trình ta thấy:

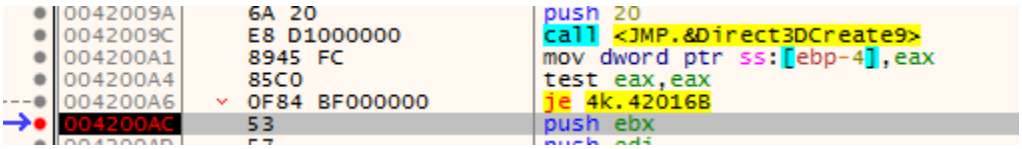
Mở chương trình bằng IDA Pro thì có vẻ như chương trình đã bị packed



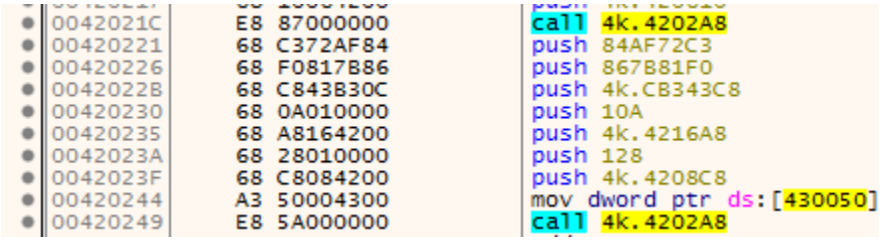
Chạy chương trình bằng x64dbg, chương trình sau khi chạy đến instruction return thì chương trình chính đã được unpack xong



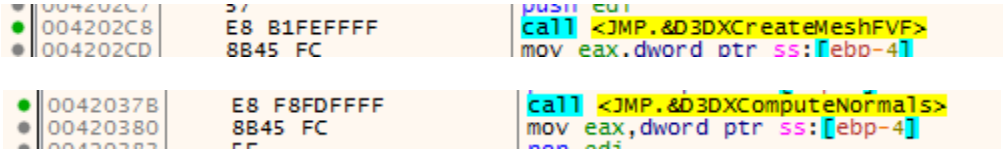
Chương trình sử dụng thư viện DirectX 9 để render



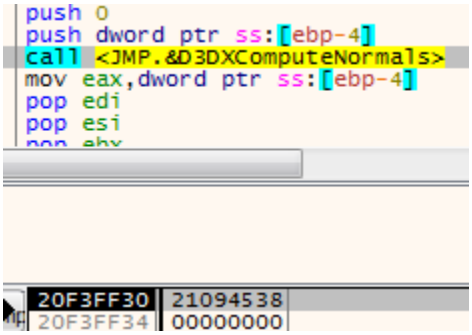
Trong hàm 4201FF có gọi đến hàm 4202A8 hai lần:



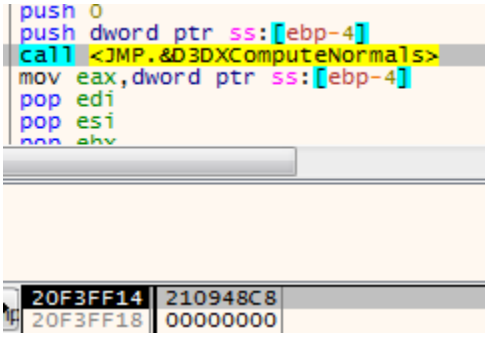
Trong hàm 4202A8 có gọi đến hai hàm trong thư viện DirectX là



Hàm D3DXComputeNormals sẽ trả ra địa chỉ chứa object được render

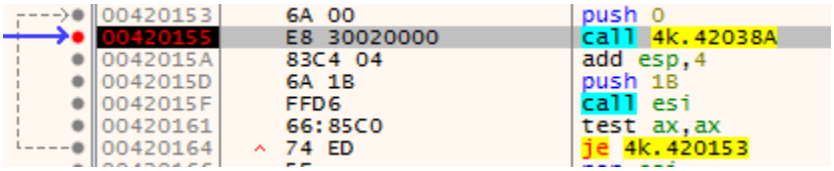


Object đầu tiên có địa chỉ 0x21094538



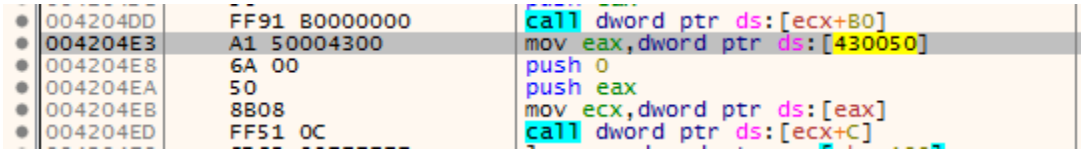
Object thứ 2 có địa chỉ 0x210948C8

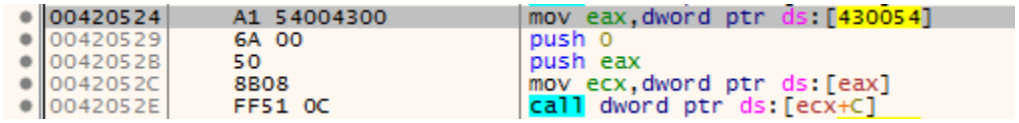
Tiếp theo ta sẽ gặp được một vòng lặp



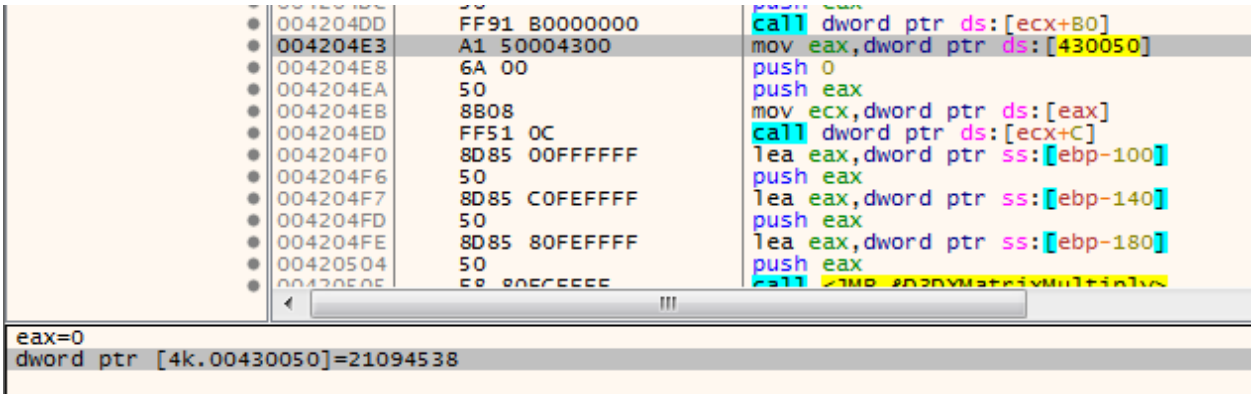
Đây là vòng lặp dùng để render từng frame của chương trình

Debug hàm 42038A ta sẽ thấy

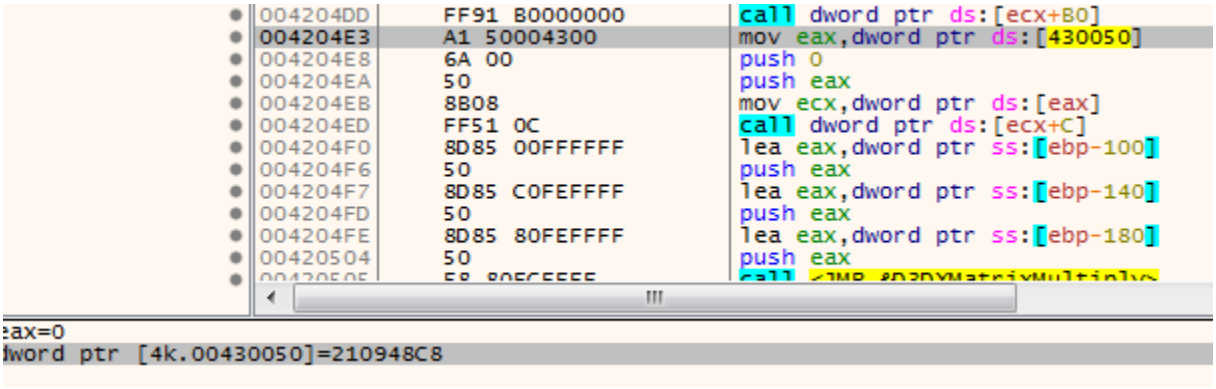




2 địa chỉ này được load vào hàm chứa trong ecx+C



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



Ta có được Flag