Đây là một ứng dụng có giao diện sử dụng winapi. Chương trình sẽ bắt đầu từ hàm WinMain.

Graphical user interface, text, application, email

Description automatically generated

Đoạn đầu của WinMain thực hiện check quyền admin, do vậy ta phải chạy IDA bằng quyền admin để có thể debug được.

WinMain không có gì đặc biệt, chỉ cho biết function nào được sử dụng làm Procedure

Có hàm TLSCallback\_0, hàm này sẽ được gọi trước khi chương trình bắt đầu hàm main, malicious program có thể sử dụng để kiểm tra debugger hoặc làm gì đó trước khi breakpoint ở trong.