# SetUnhanledExceptionFilter()

Load file vào Ida 32bit, thực hiện debug thì gặp exception Integer divide by zero.

Graphical user interface, text, application

Description automatically generated

Exception này gây ra tại “div eax”

Graphical user interface, application

Description automatically generated

Đây là ý đồ của chương trình vì ở phía trên chương trình có gọi API SetUnhandledExceotionFilter để đăng kí handle exception với handler là TopLevelExceptionFilter.

Graphical user interface, text, application

Description automatically generated và flow của chương trình sẽ được tiếp tục khi exception này được handle (khi chương trình handle exception thì hàm này sẽ được call, và nếu có debuger thì exception này được handle bởi debuger chứ không phải chương trình, do vậy hàm kia không được call và chương trình không tiếp tục).

Để bypass trick này, ta patch program jump thẳng tới TopLevelExceptionFilter.

2.

F5 để decompiler update lại chương trình.

Text

Description automatically generated

Sau đó chương trình tạo 1 dialog box với procedure là DialogFunc.