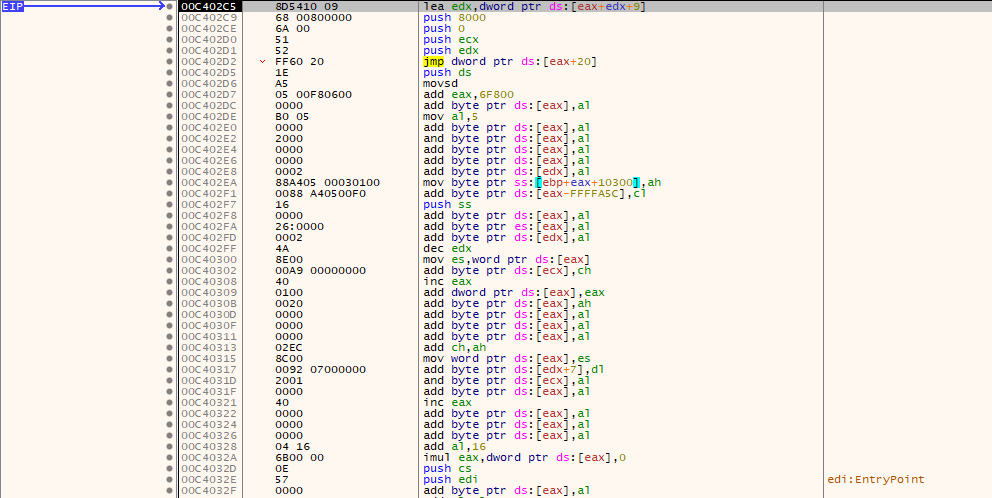
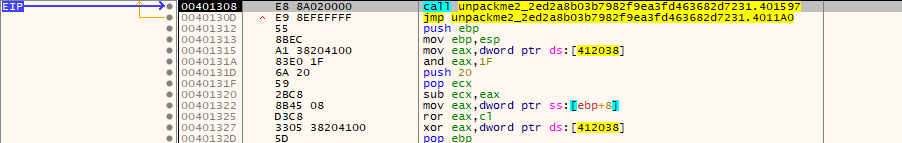
Sử dụng detect it easy xem thông tin thấy unpack2 được pack bằng petie

Graphical user interface

Description automatically generated

Làm tương tự như bài 1 cho tới hardware breakpoint

Trace 1 hồi thì sẽ tới OEP của bài là 0x401308.



Dump và fix bằng Scylla, file dump không chạy được nhưng load vào ida đã detect được WinMain, nguyên nhân là do IAT có những hàm không tự scan được phải sửa bằng tay. Cái này em không biết làm như nào nên trước hết cứ dump ra đã