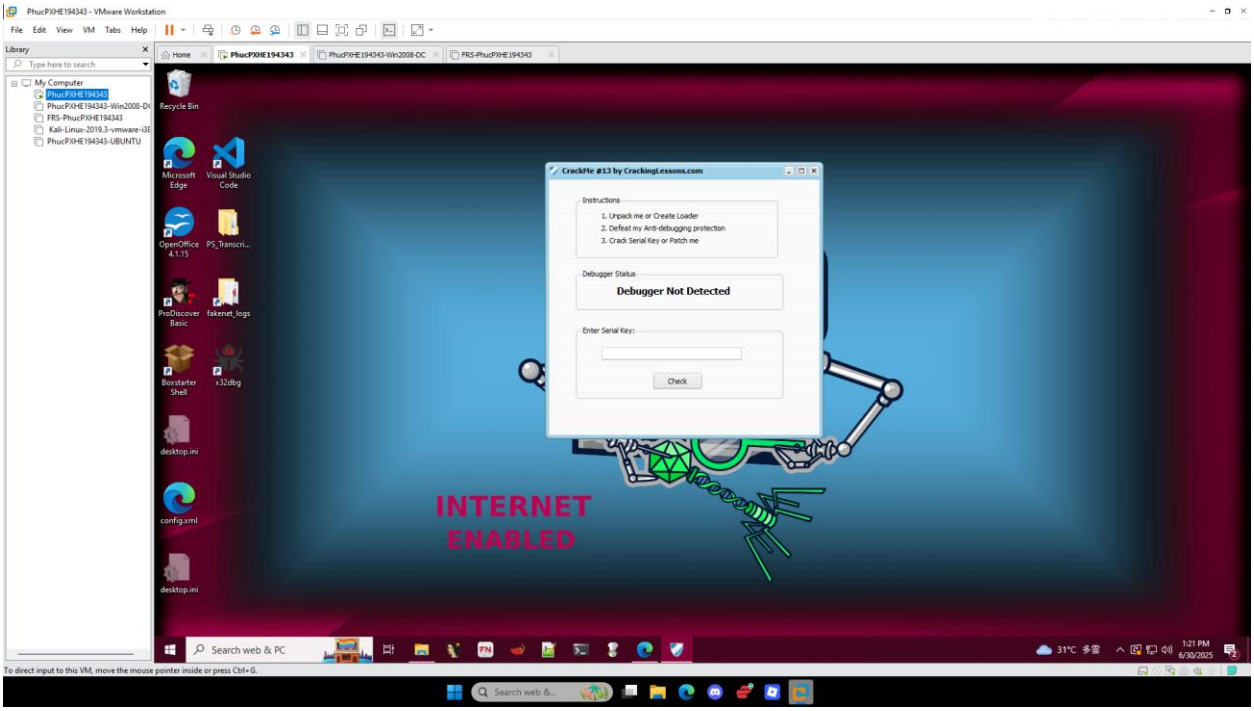
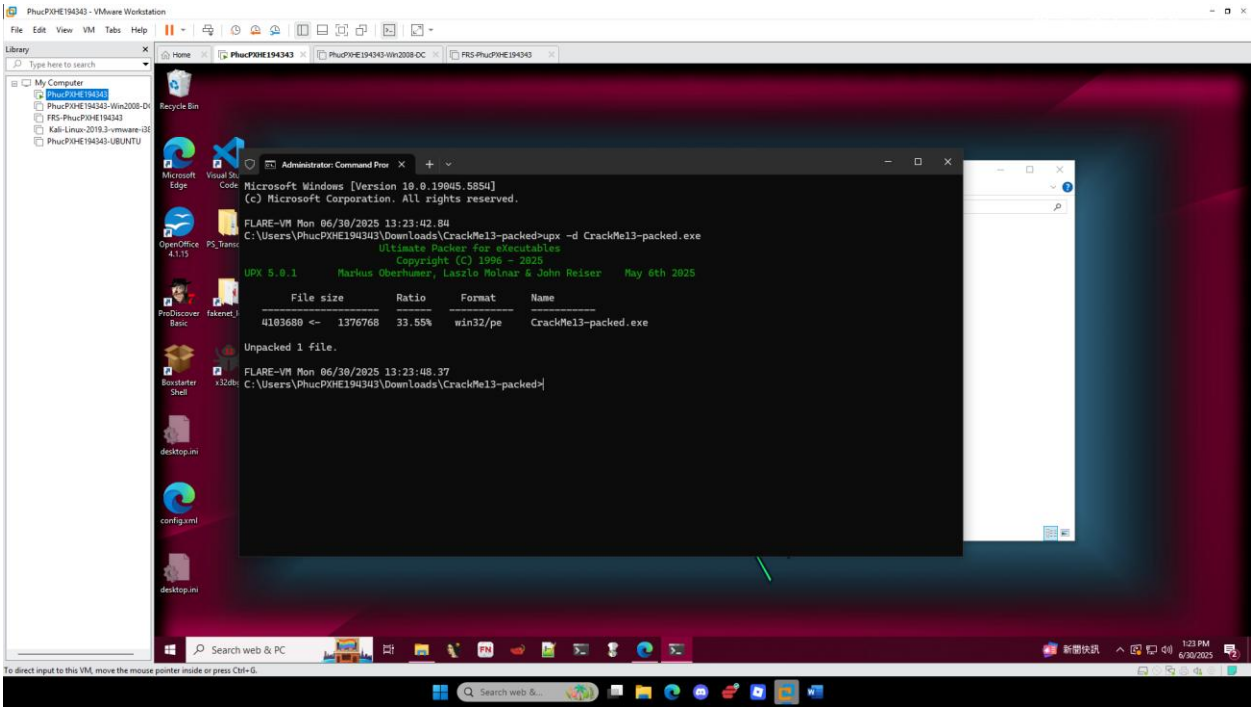
Crack Me 13

Part 1: Unpack

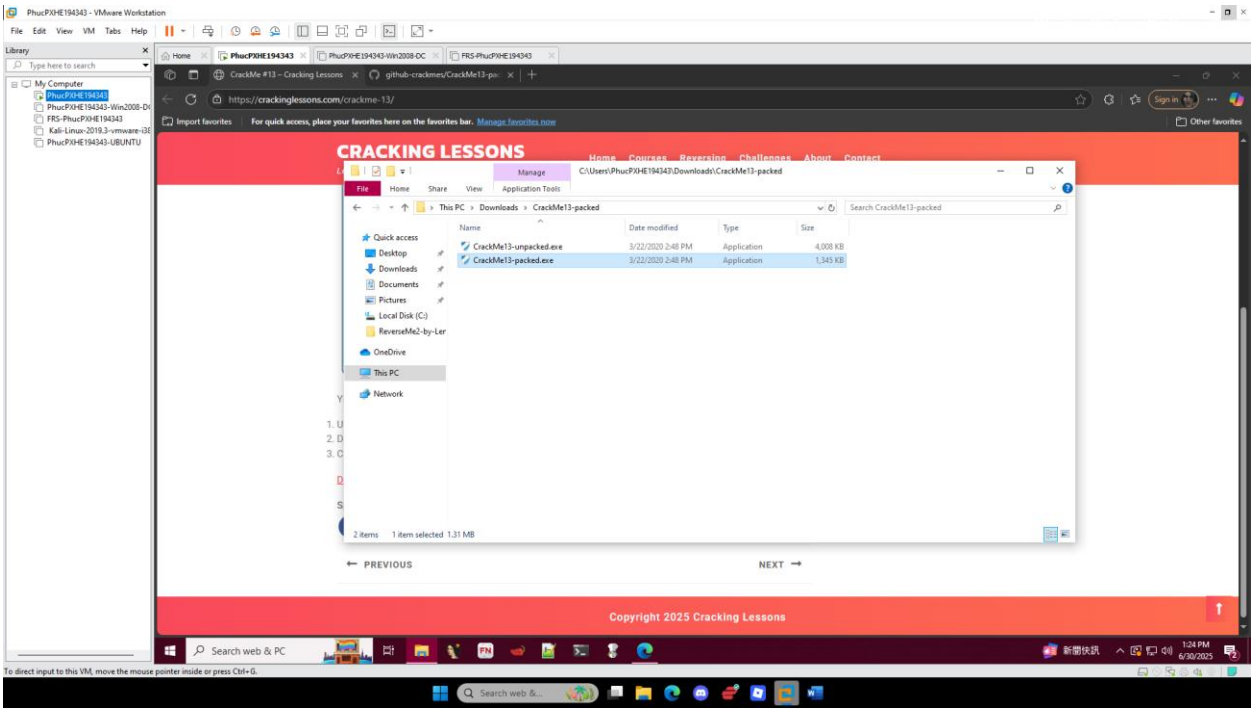
Step 1: Mở phần mềm lên để xem có những yêu cầu nào



Step 2: Unpack phần mềm bằng UPX

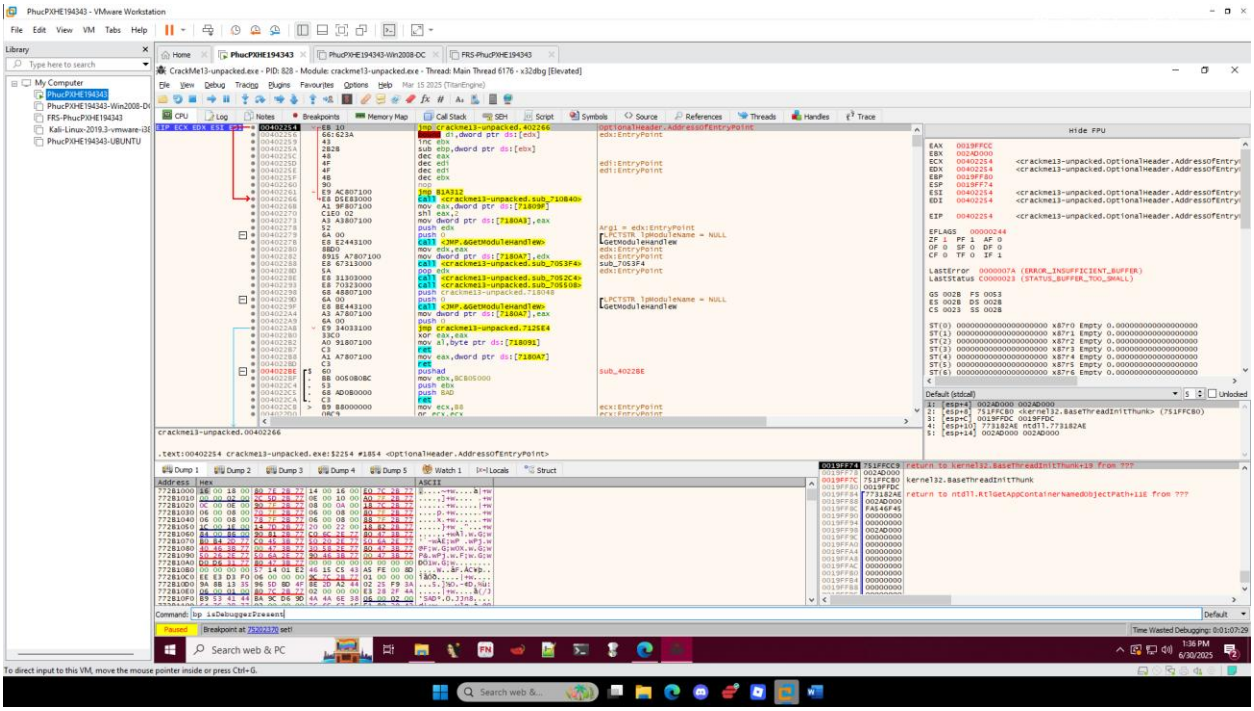


Step 3: So sánh giữa packed với unpacked

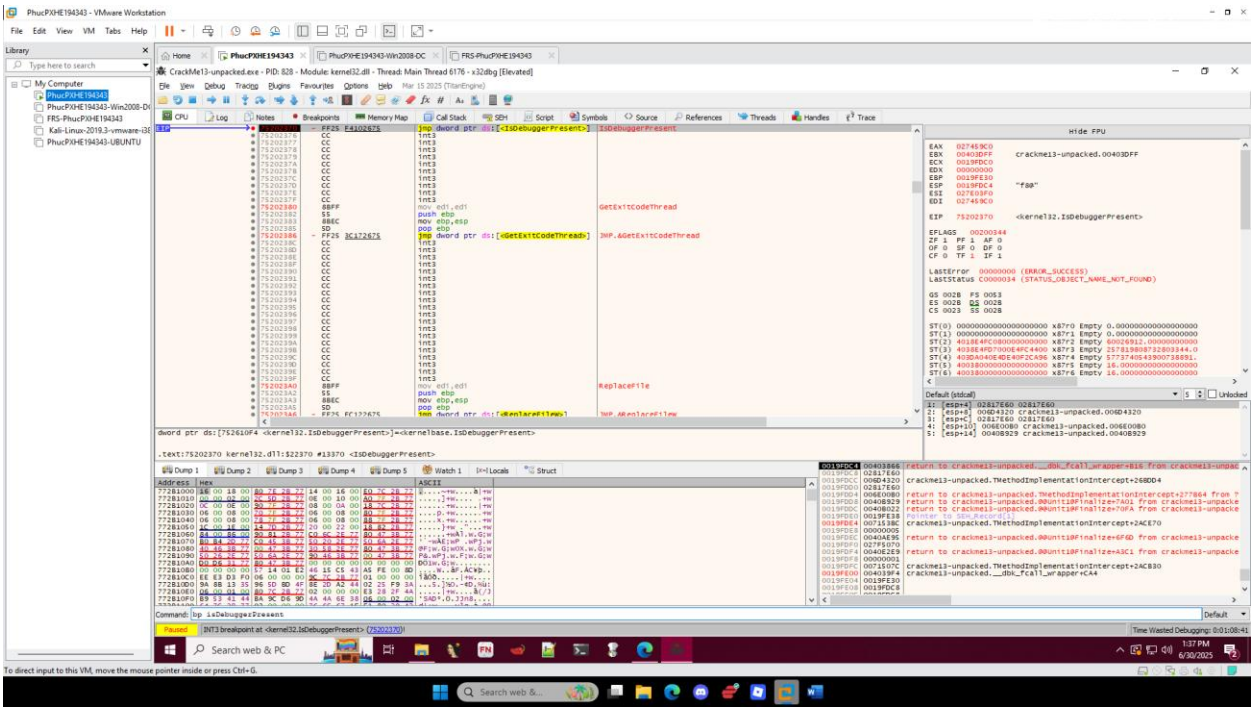


Part 2: Anti anti debugger

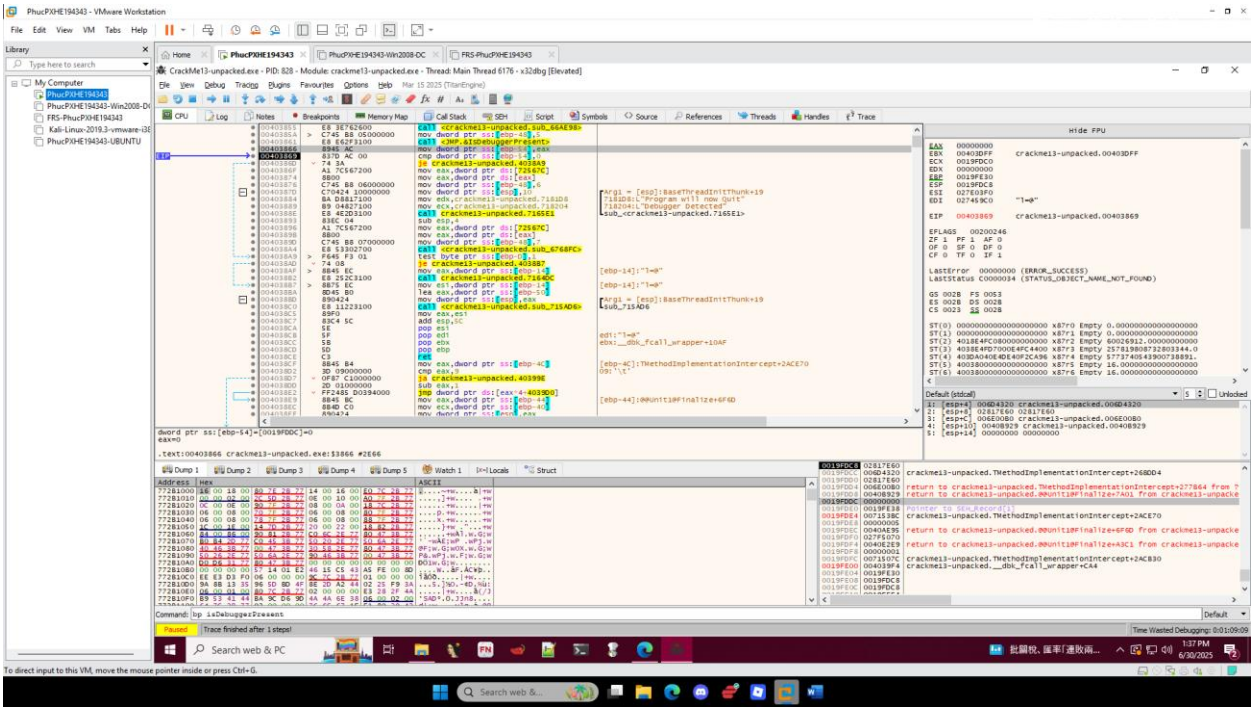
Step 1: Load phần mềm vào x32DBG em sử dụng command bp isDebuggerPresent để tìm kiếm debugger tampered trong phần mềm



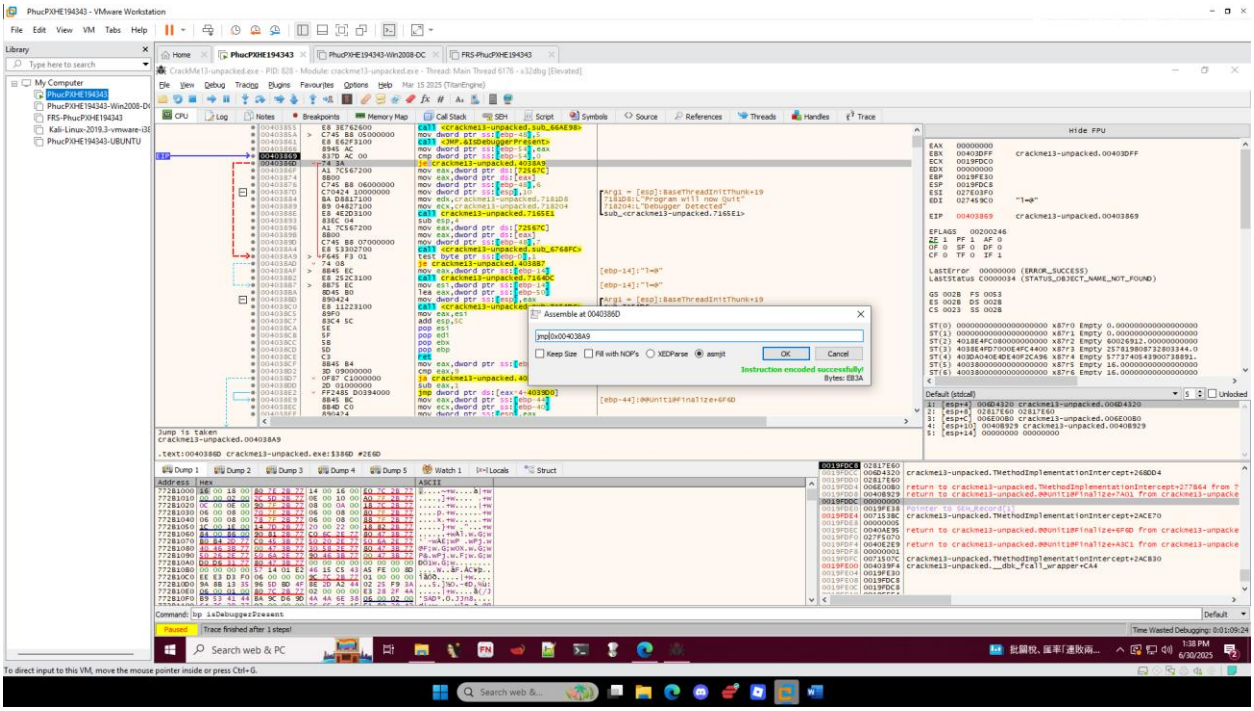
Step 2: Sử dụng command xong thì chương trình đã đặt cho chúng ta 1 cái breakpoint nơi debugger tampered xuất hiện ở trong system module



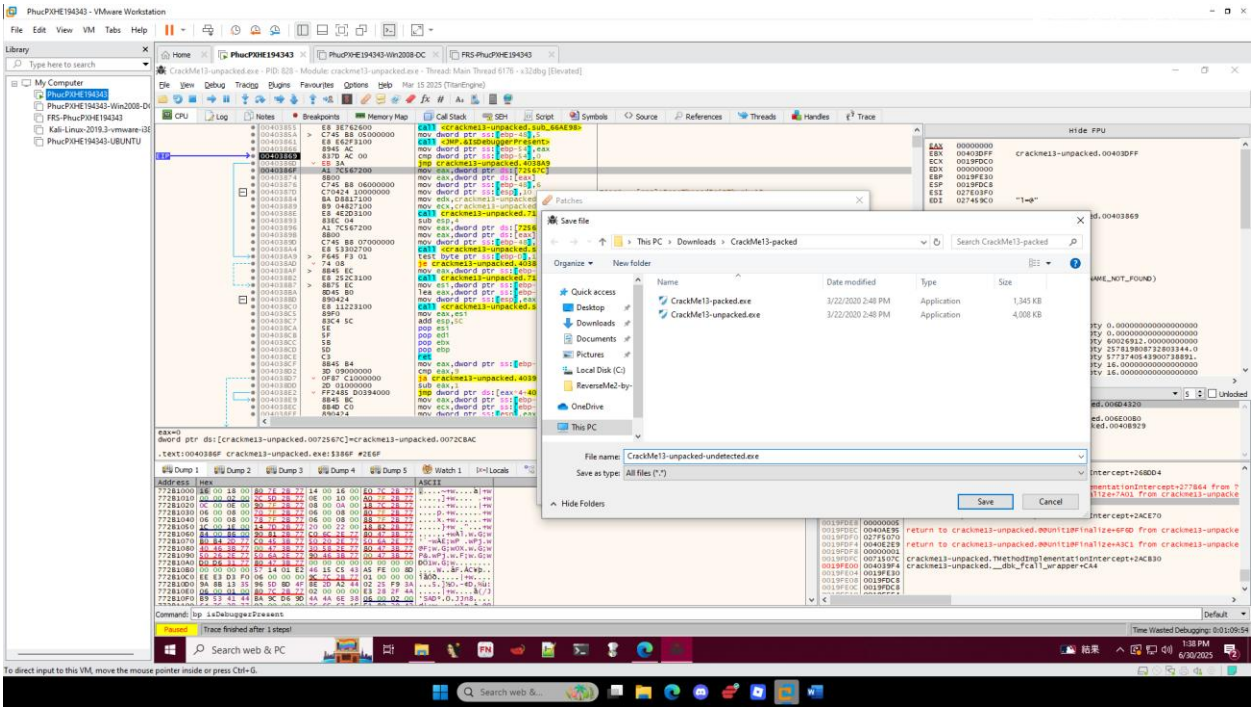
Step 3: Chuyển về user module chúng ta đã thấy đoạn code chứa debugger tampered



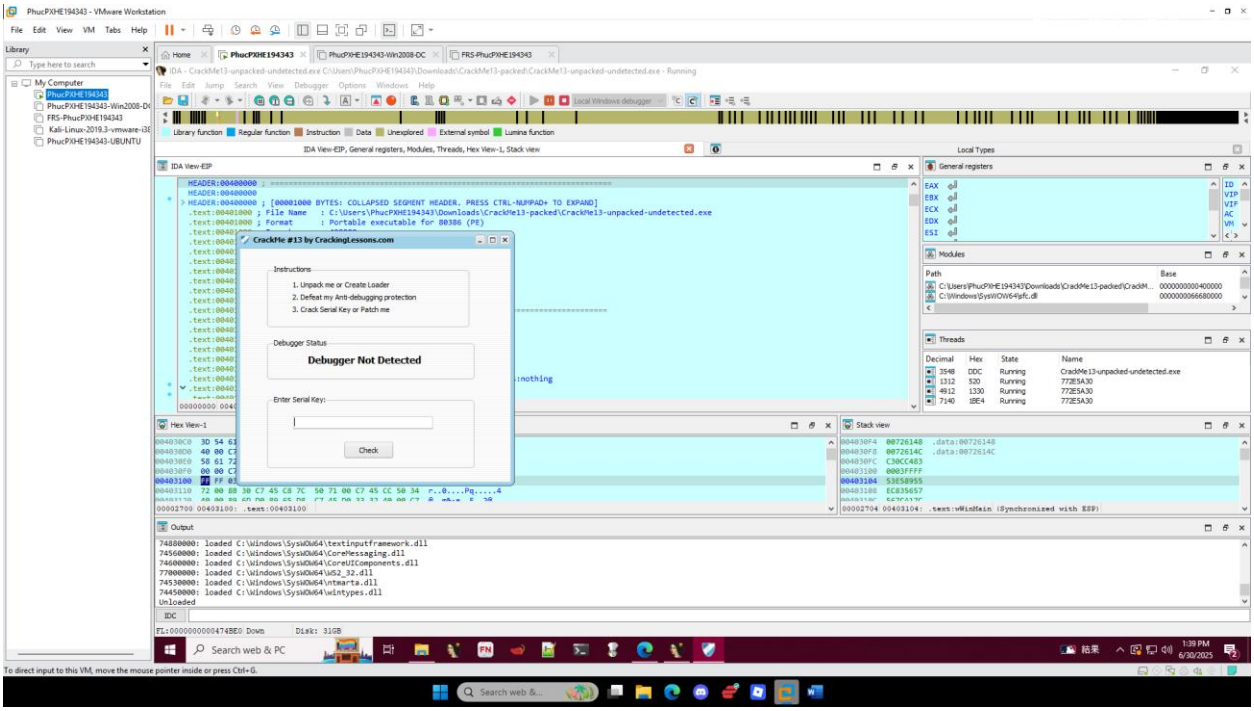
Step 4: Em chuyển lệnh je thành jmp để bypass vòng lặp chứa debugger tampered



Step 5: Patched chương trình

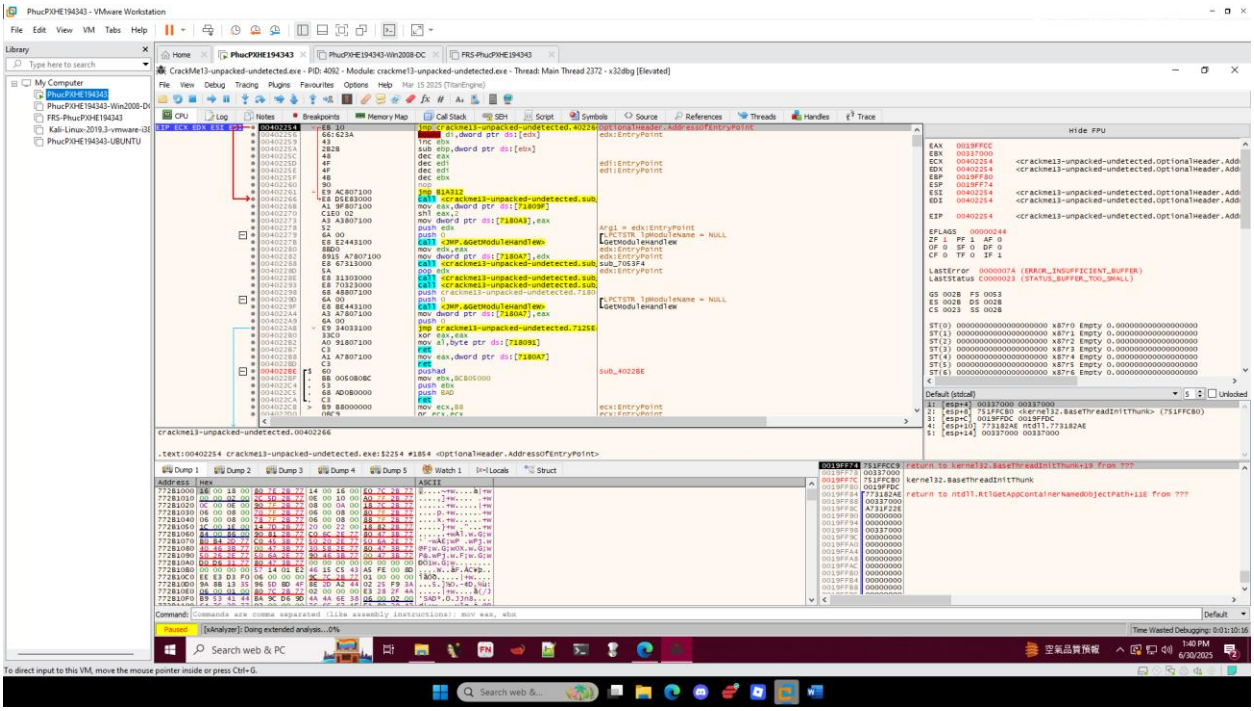


Step 6: Thử file đã patched

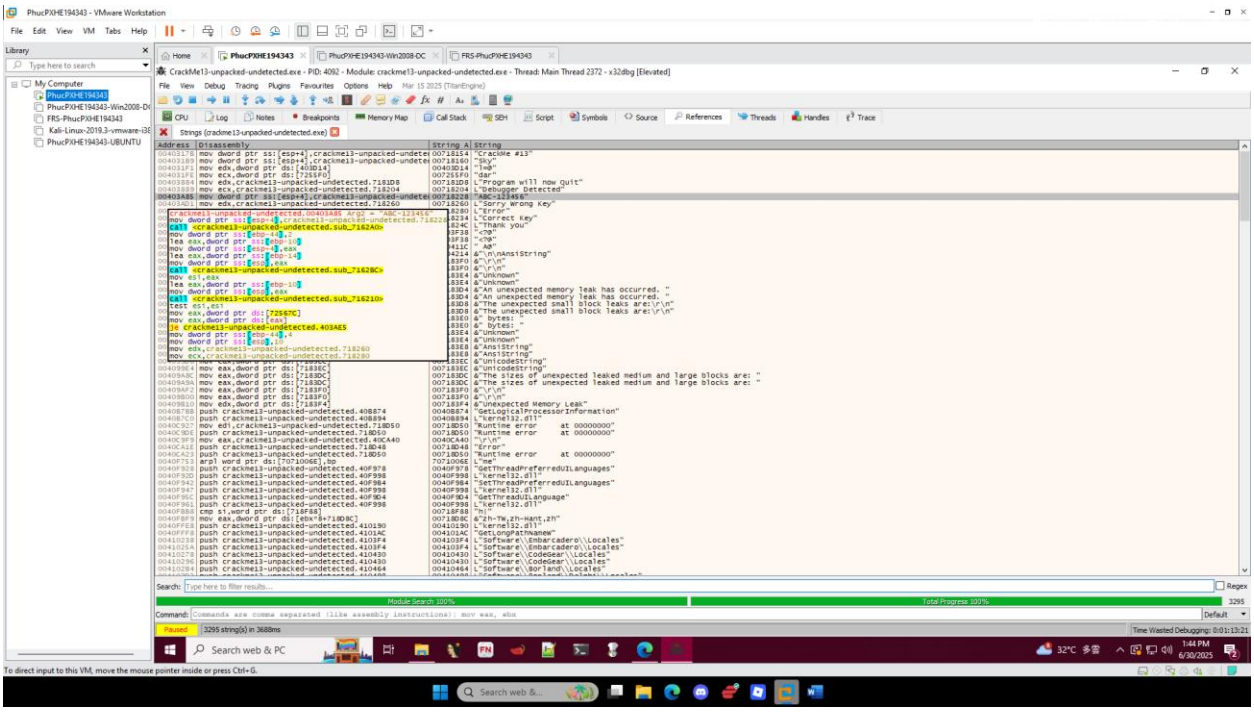


Part 3: Crack serial key

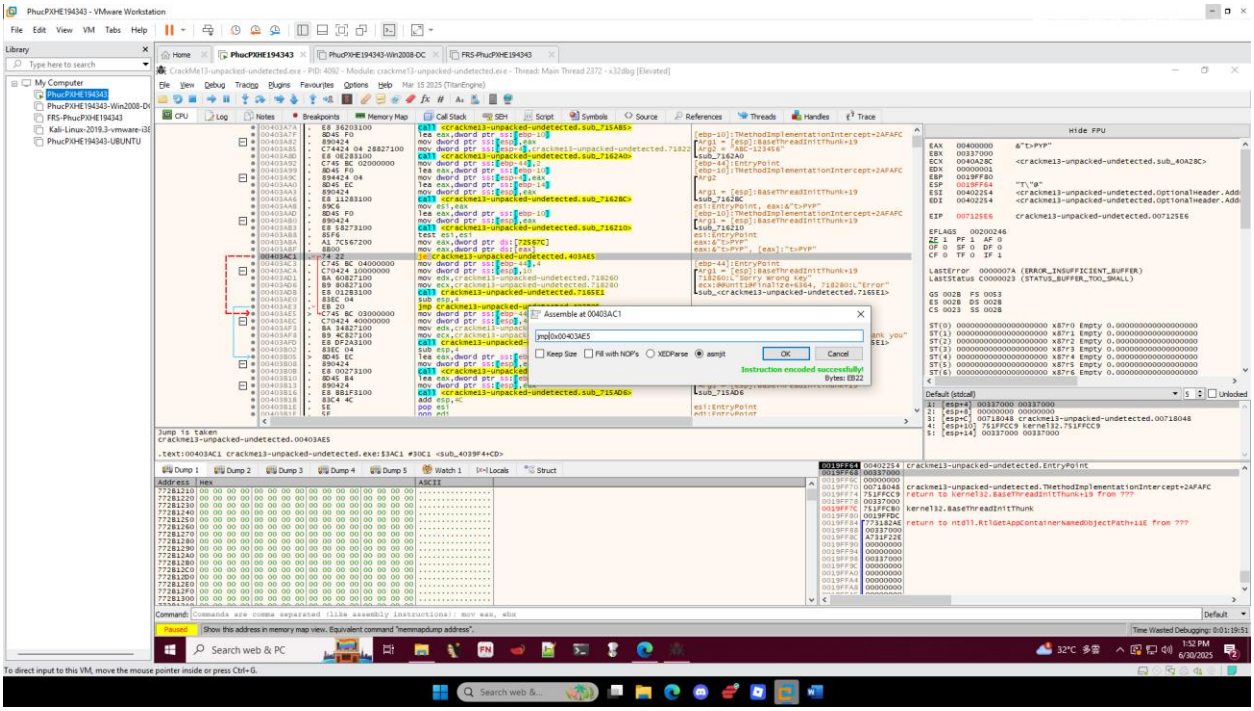
Step 1: Load phần mềm vào x32debugger



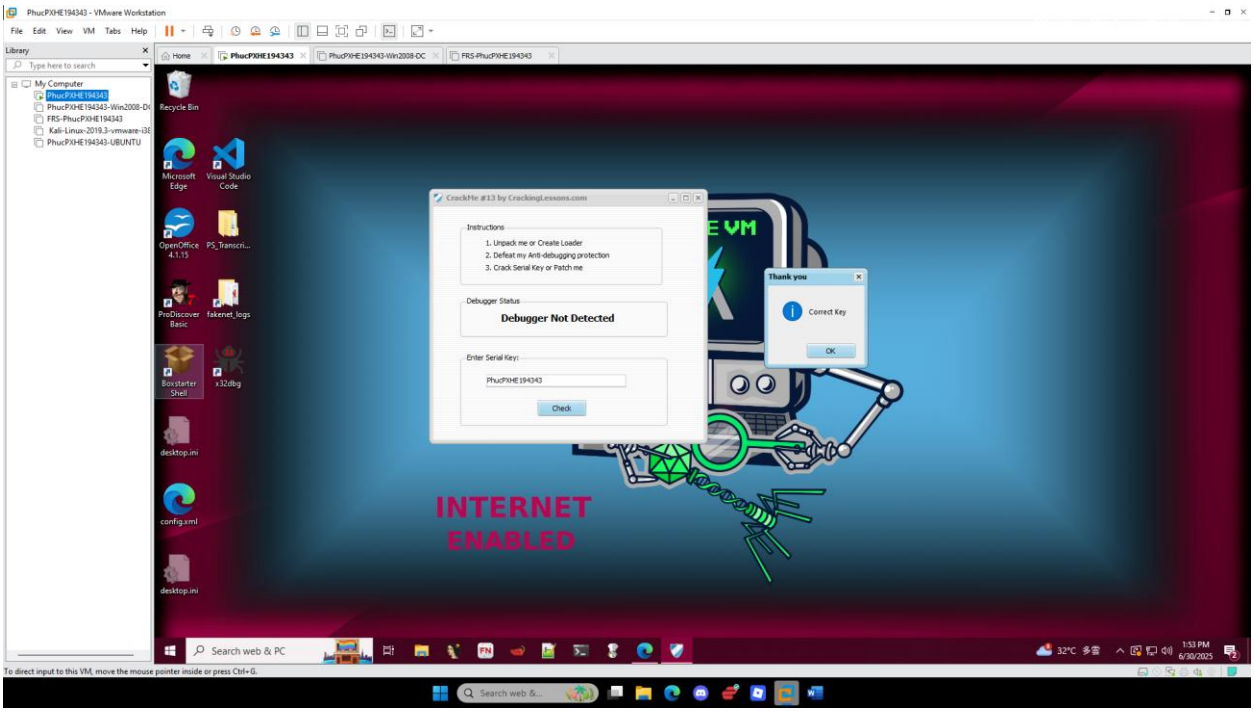
Step 2: Em search strings trong user module này, và tìm thấy đoạn hiển thị màn hình chứa bad message



Step 3: Em sửa lệnh je thành jmp để bypass vòng lặp chứa đoạn mã hiện thị popup chứa bad message

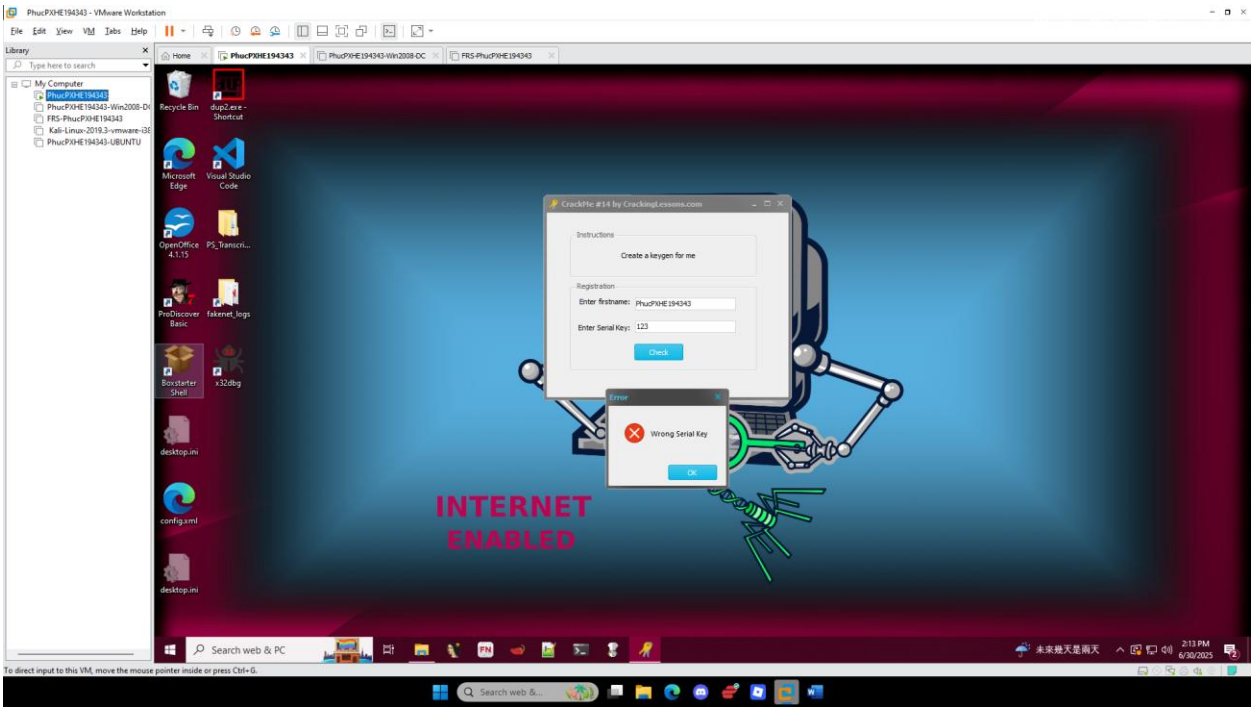


Step 5: Em patched file và kiểm thử lại

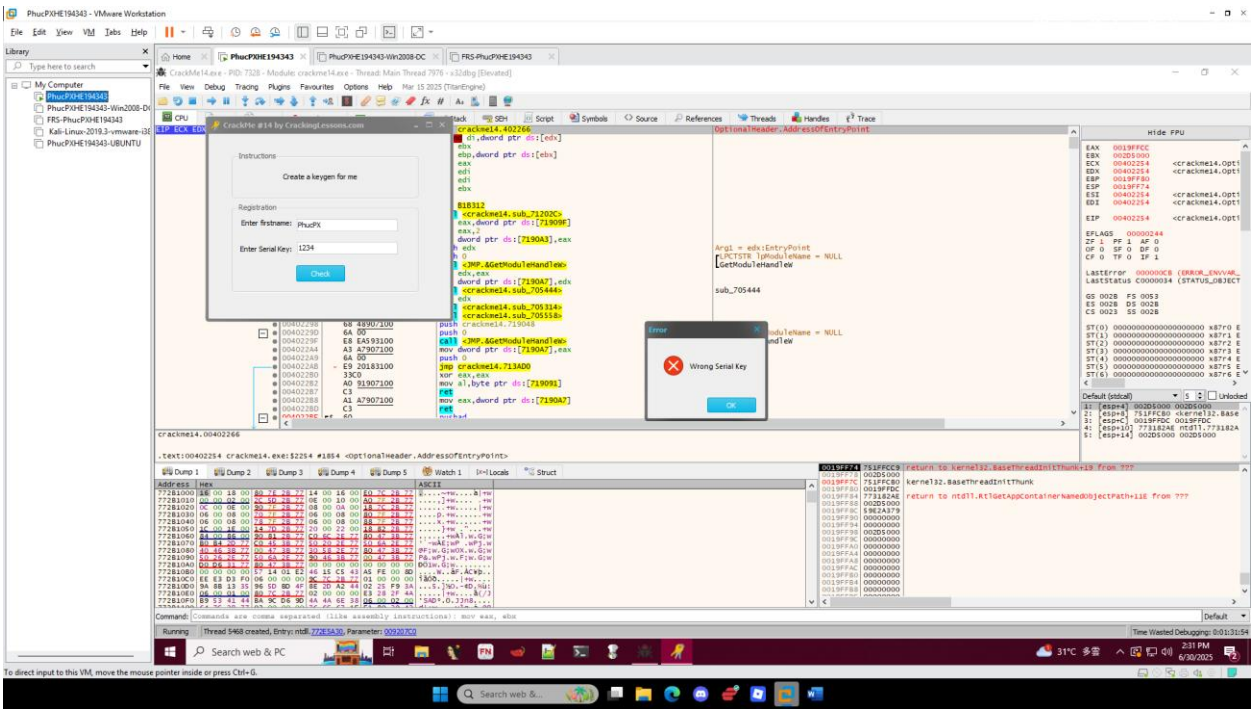


Crack Me 14

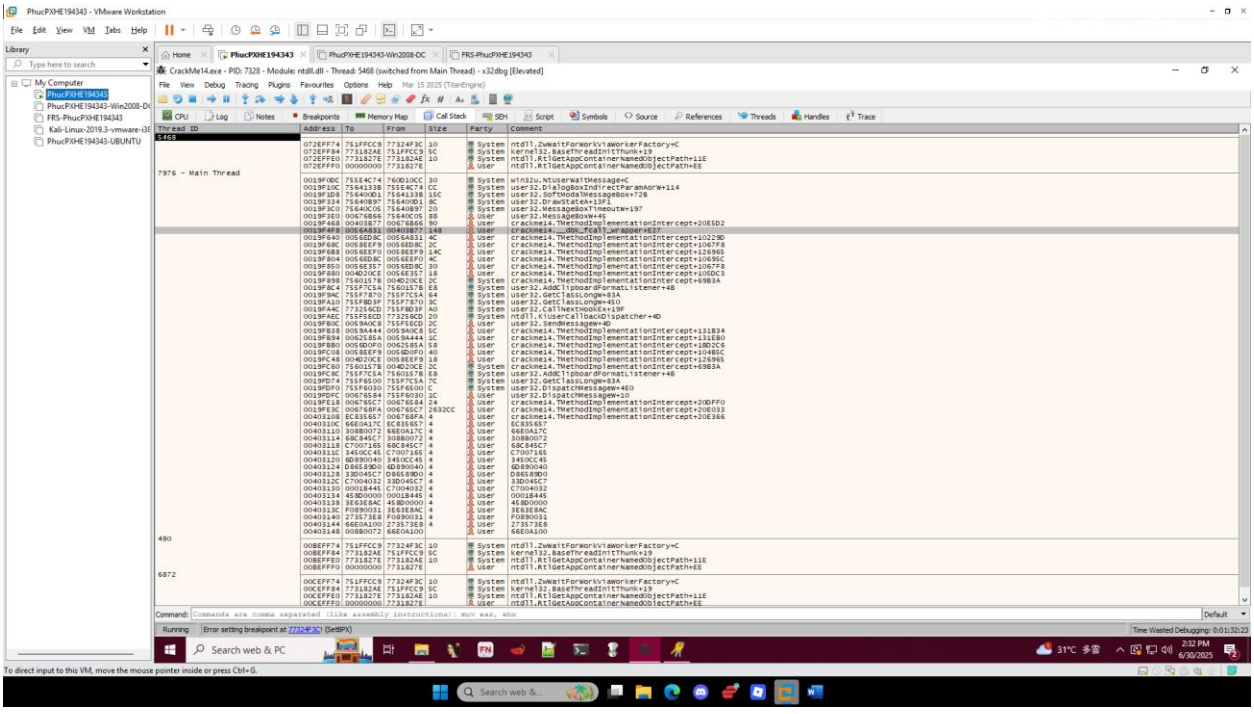
Step 1: Mở phần mềm ra và check xem có requirement nào không



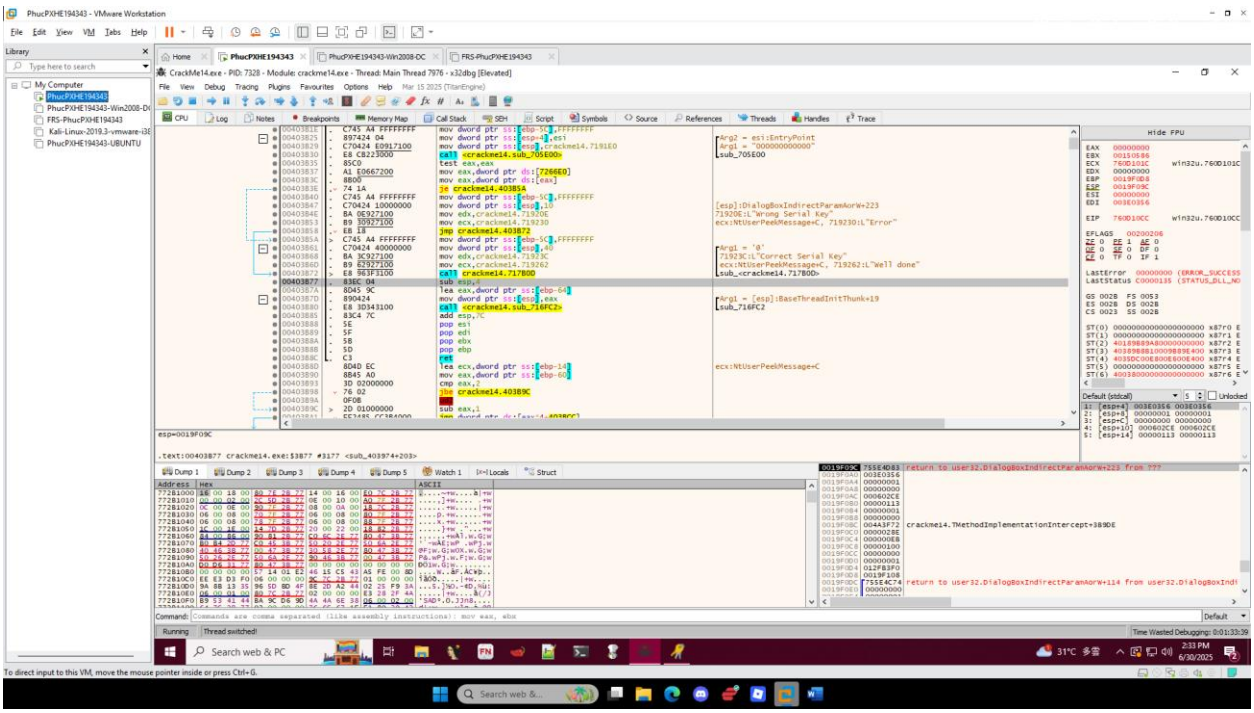
Step 2: Load phần mềm vào x32dbg chạy đến entry point nhập username và serial key để check



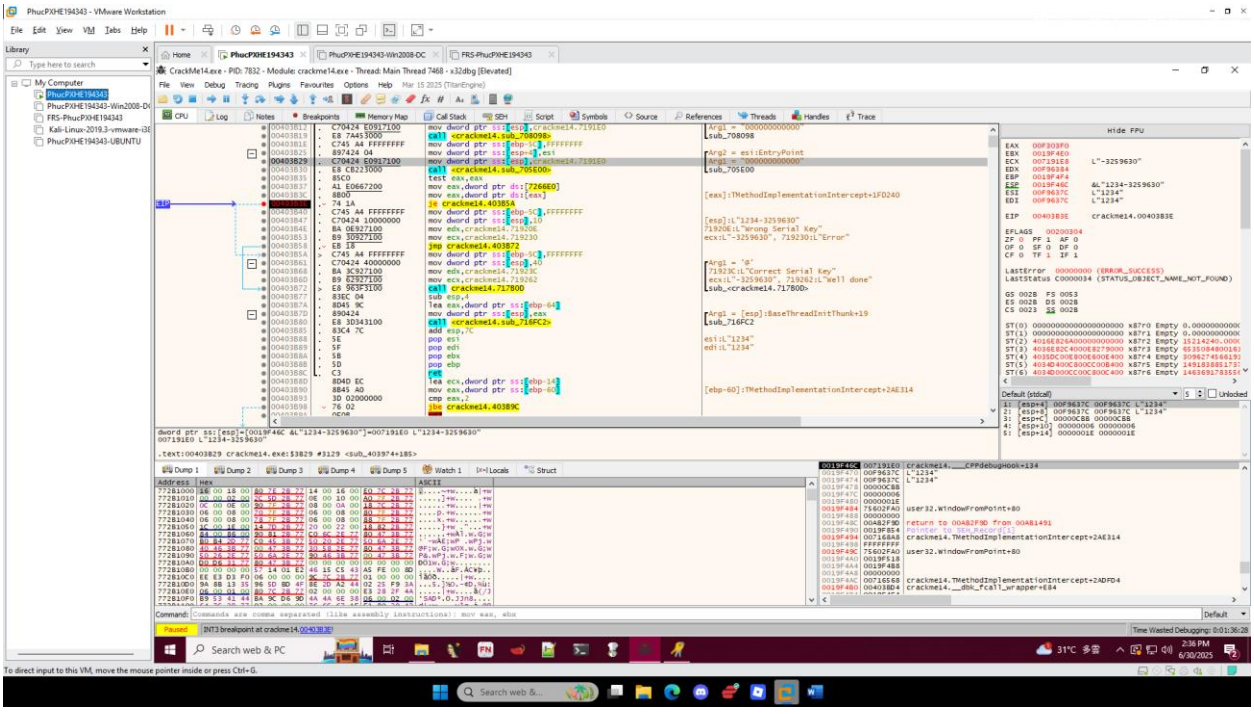
Step 3: Pause chương trình và vào call stack đi đến địa chỉ của phần như trong hình



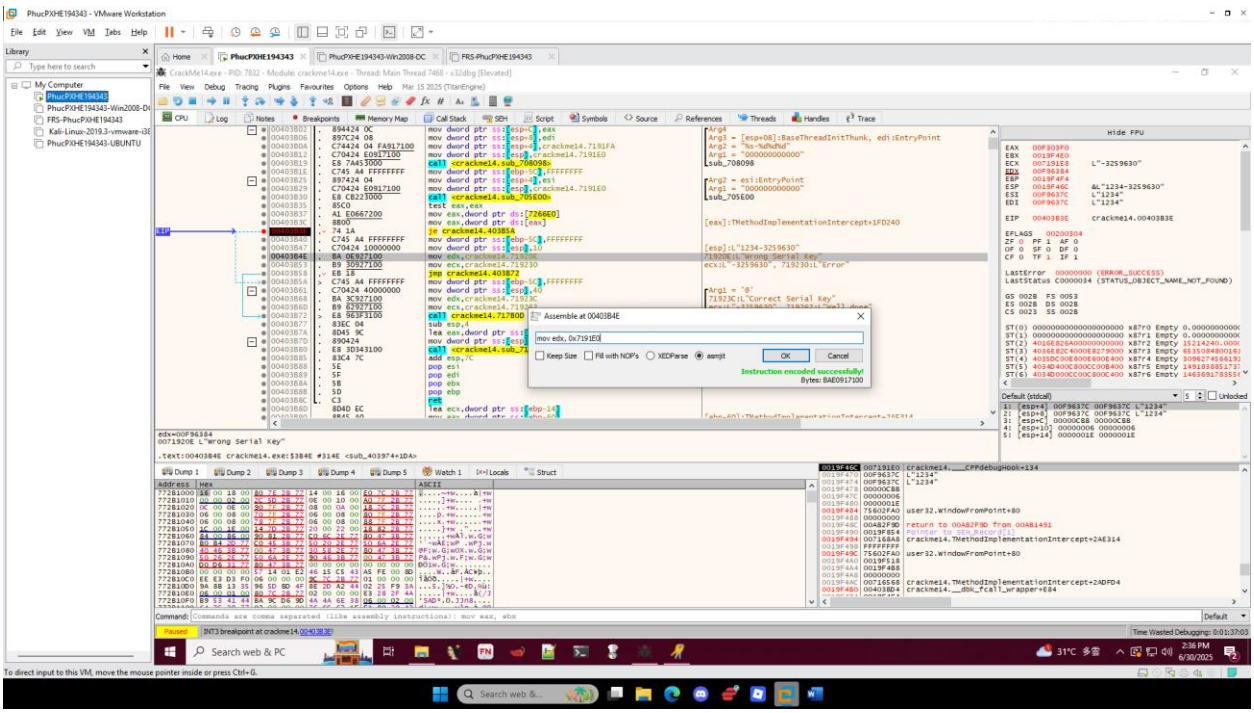
Step 4: Follow from địa chỉ từ call stack về user module



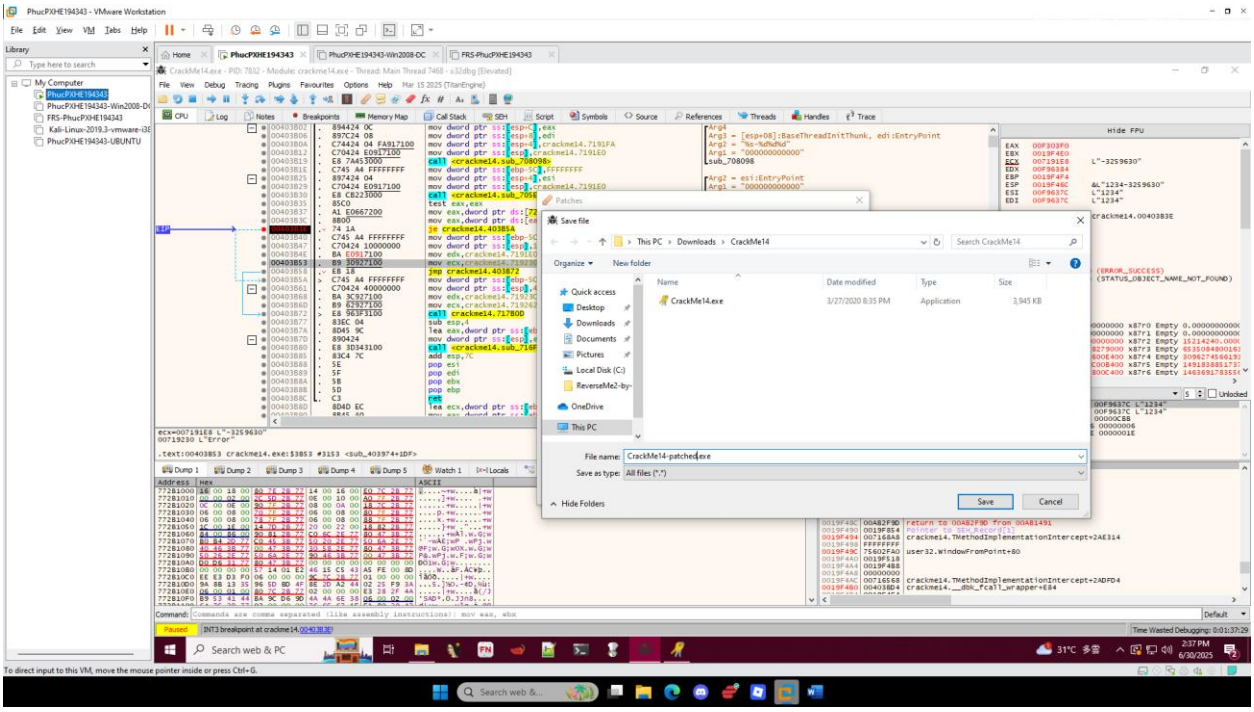
Step 5: Đọc code và ta thấy được địa chỉ được highlight ở trong hình là địa chỉ chứa keygen



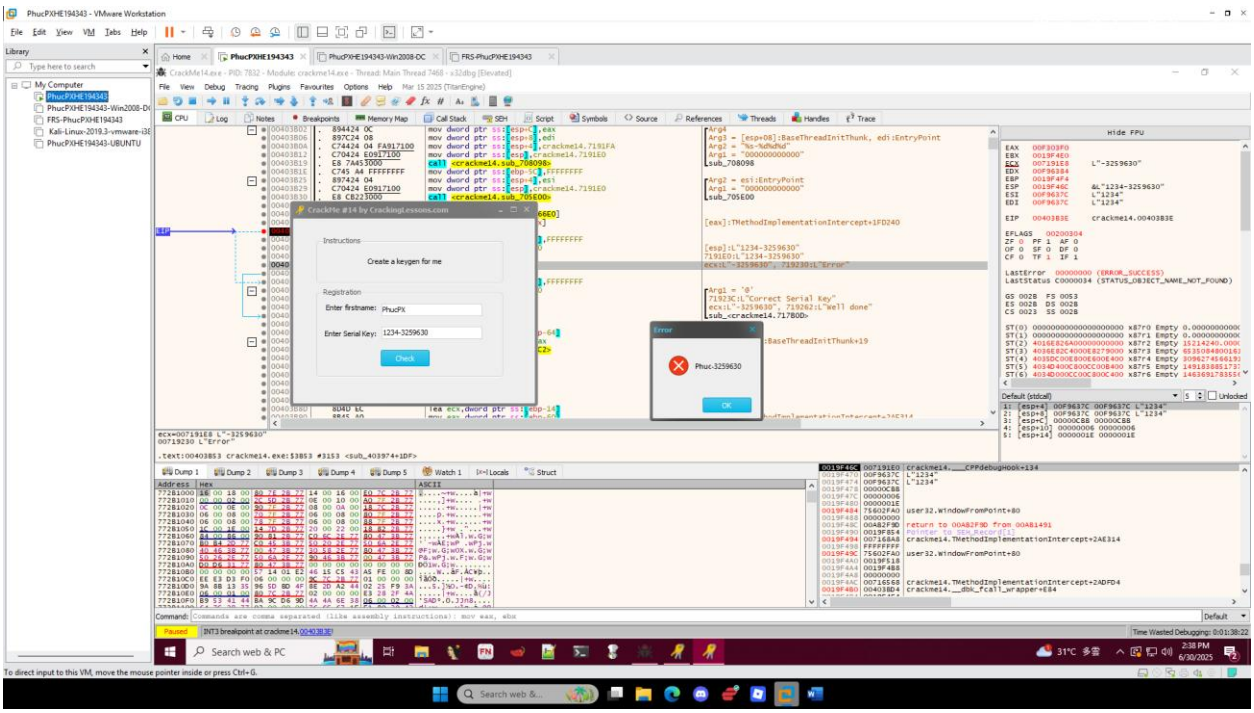
Step 6: Ta thay địa chỉ chứa bad message thành địa chỉ của keygen, khi mà ta nhập sai thì nó sẽ hiện ra key được generated từ keygen



Step 7: Tiến hành patched chương trình



Step 8: Chạy thử chương trình đã patched, nhập vào 1 key bất kì thì chương trình sẽ hiện ra key đúng



Step 9: Nhập thử key đúng vào phần mềm