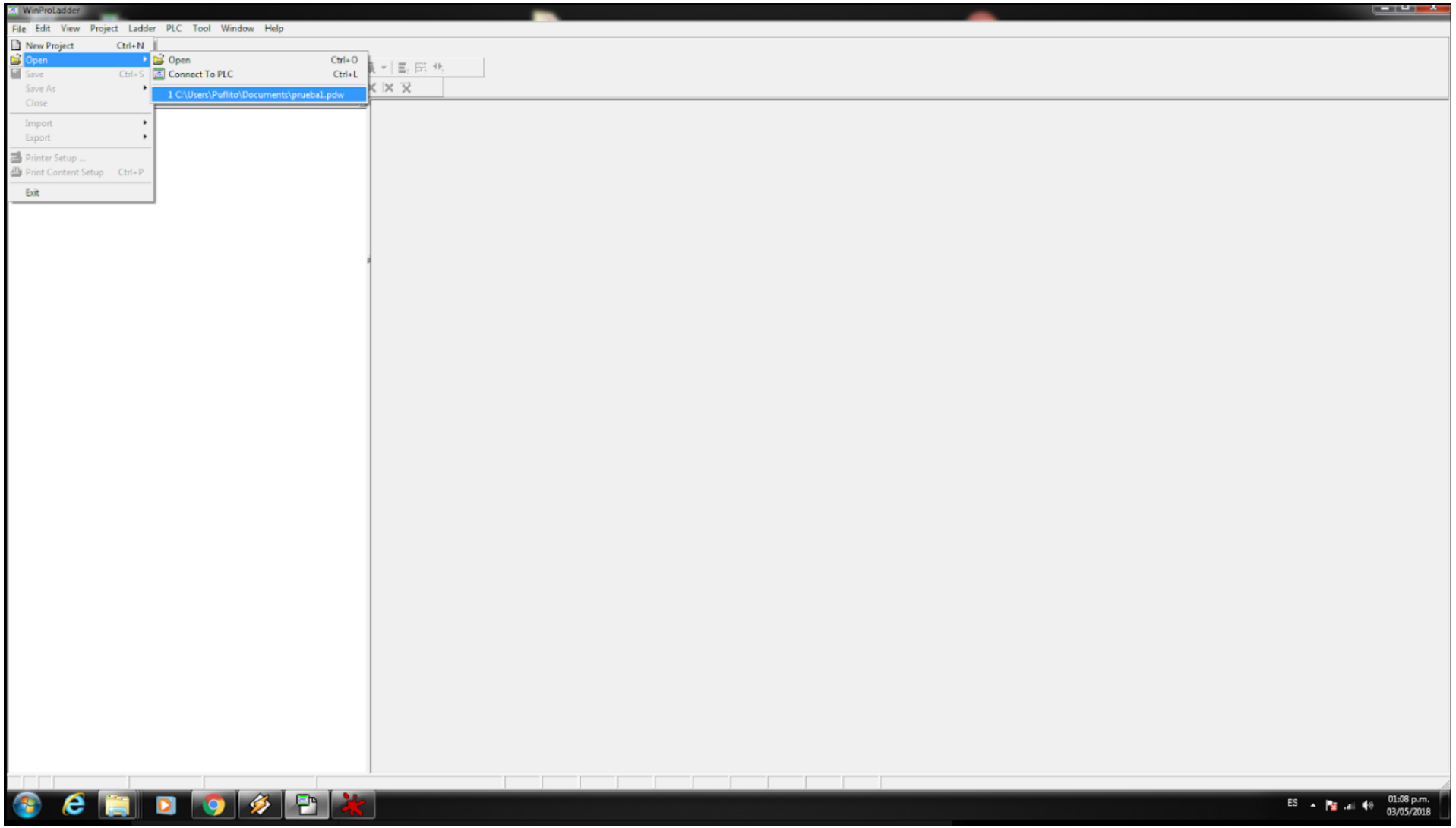
Mở khóa dự án WinProLadder (PLC Fatek)

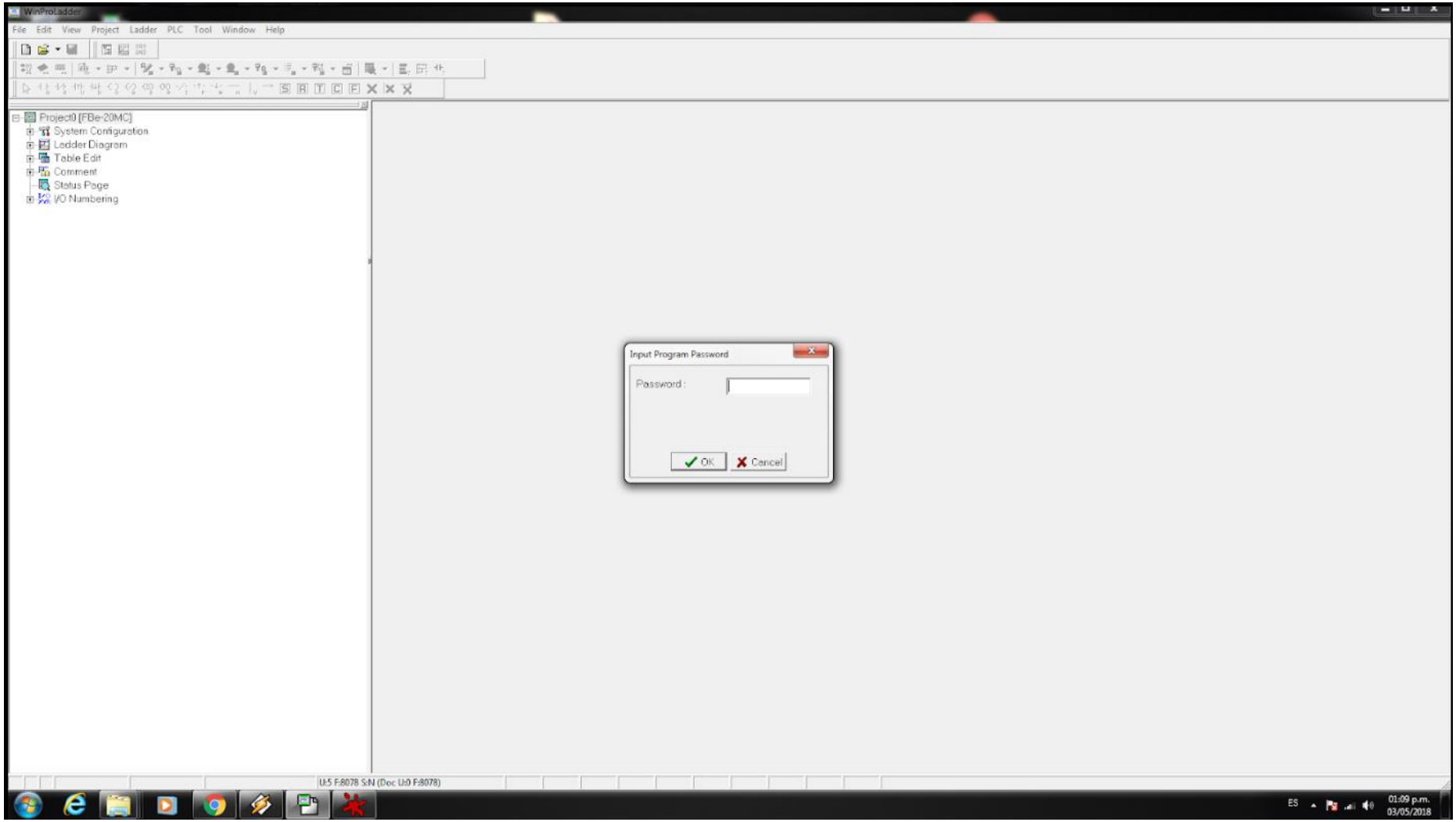
Này các bạn, các bạn thế nào?

Chà, ở đây tôi chỉ cho bạn cách mở khóa dự án WinProLadder được bảo vệ bằng mật khẩu. Dự án này có thể là một dự án đã lưu hoặc đã được lưu/tải lên PLC, như đã được biết đến từ thương hiệu Fatek.

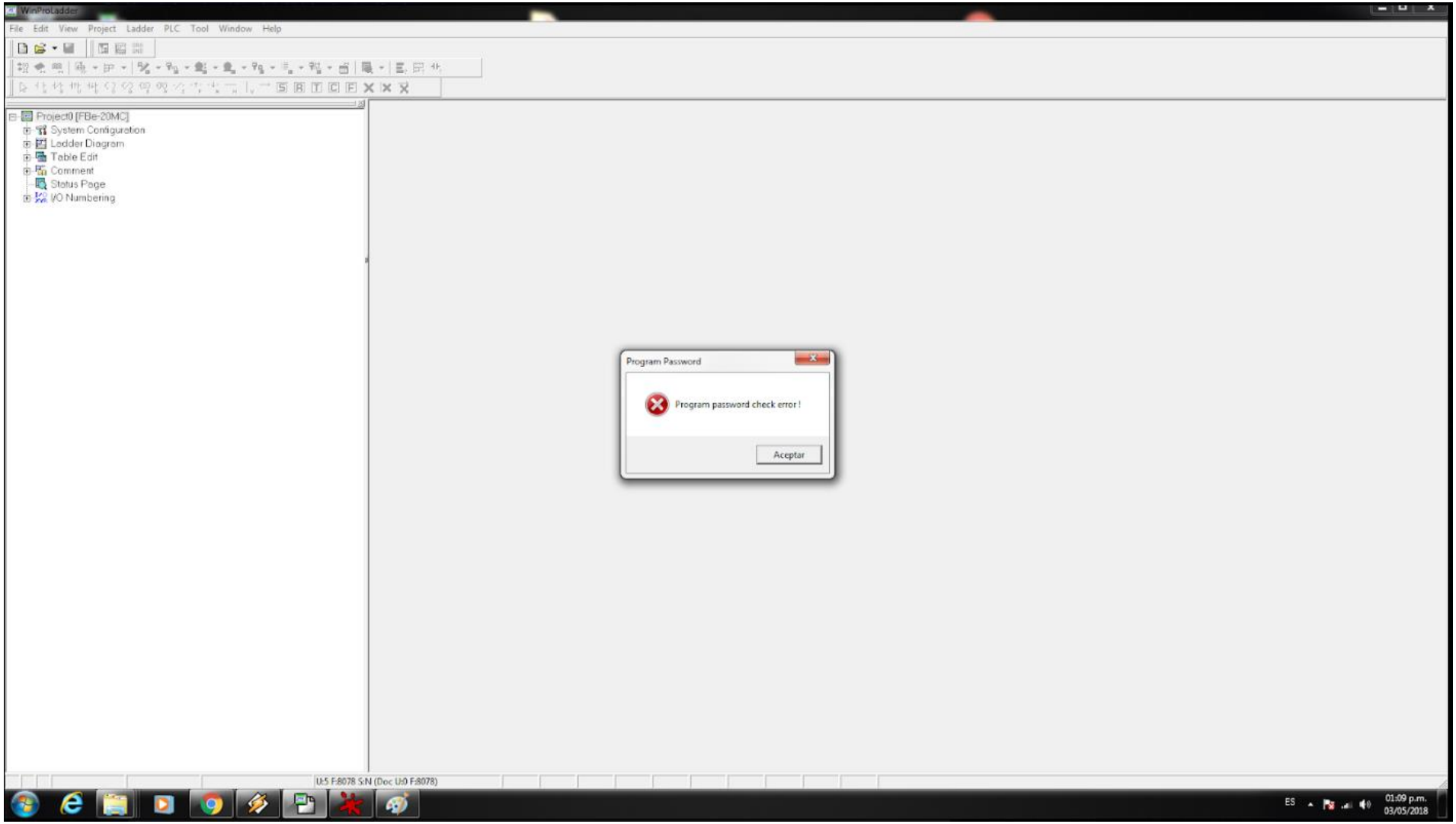
Chà, để bắt đầu, hãy mở chương trình, tải dự án hoặc kết nối với plc và thử tải xuống



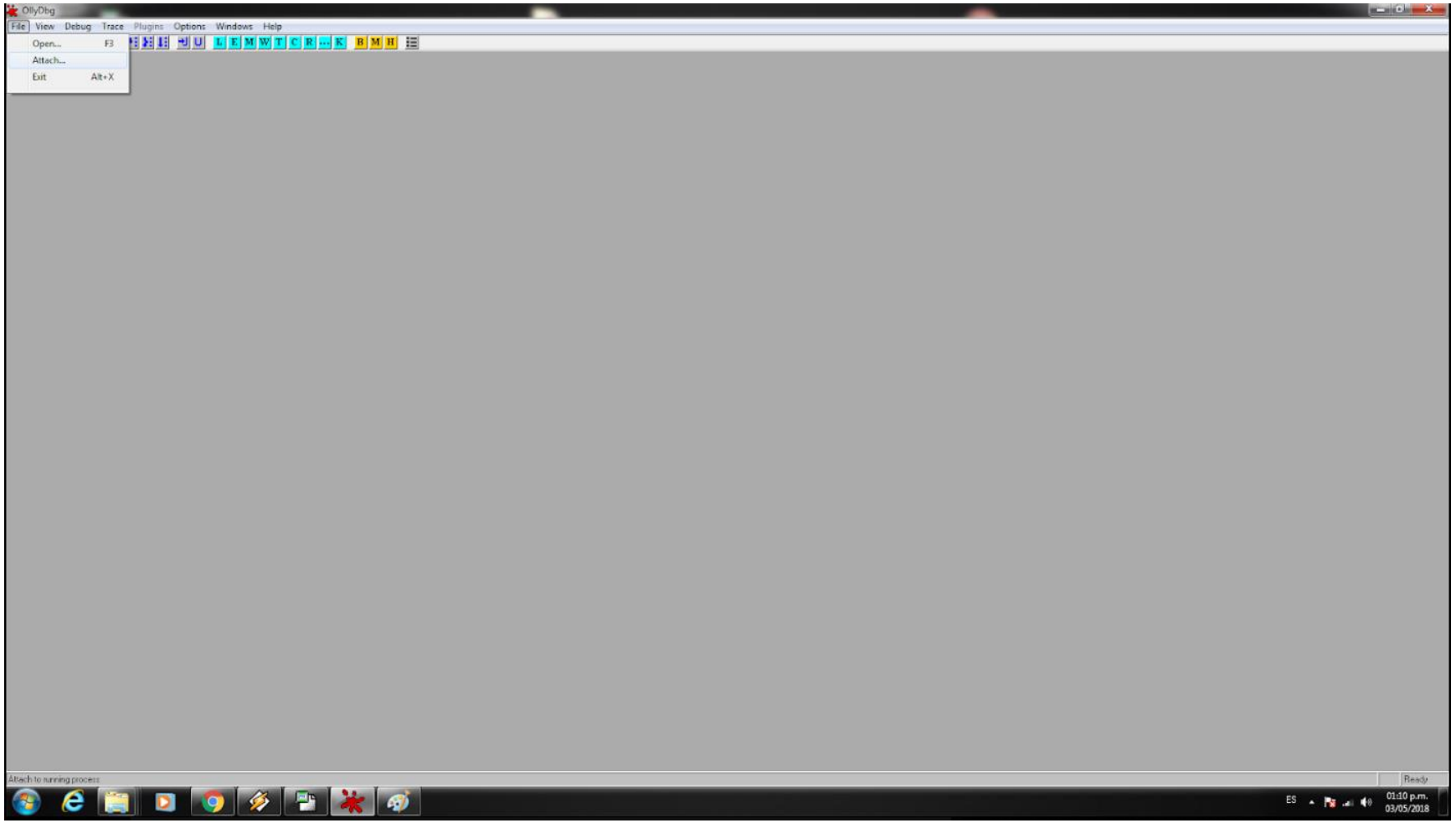
Sau khi mở/tải xuống, nó sẽ yêu cầu mật khẩu:



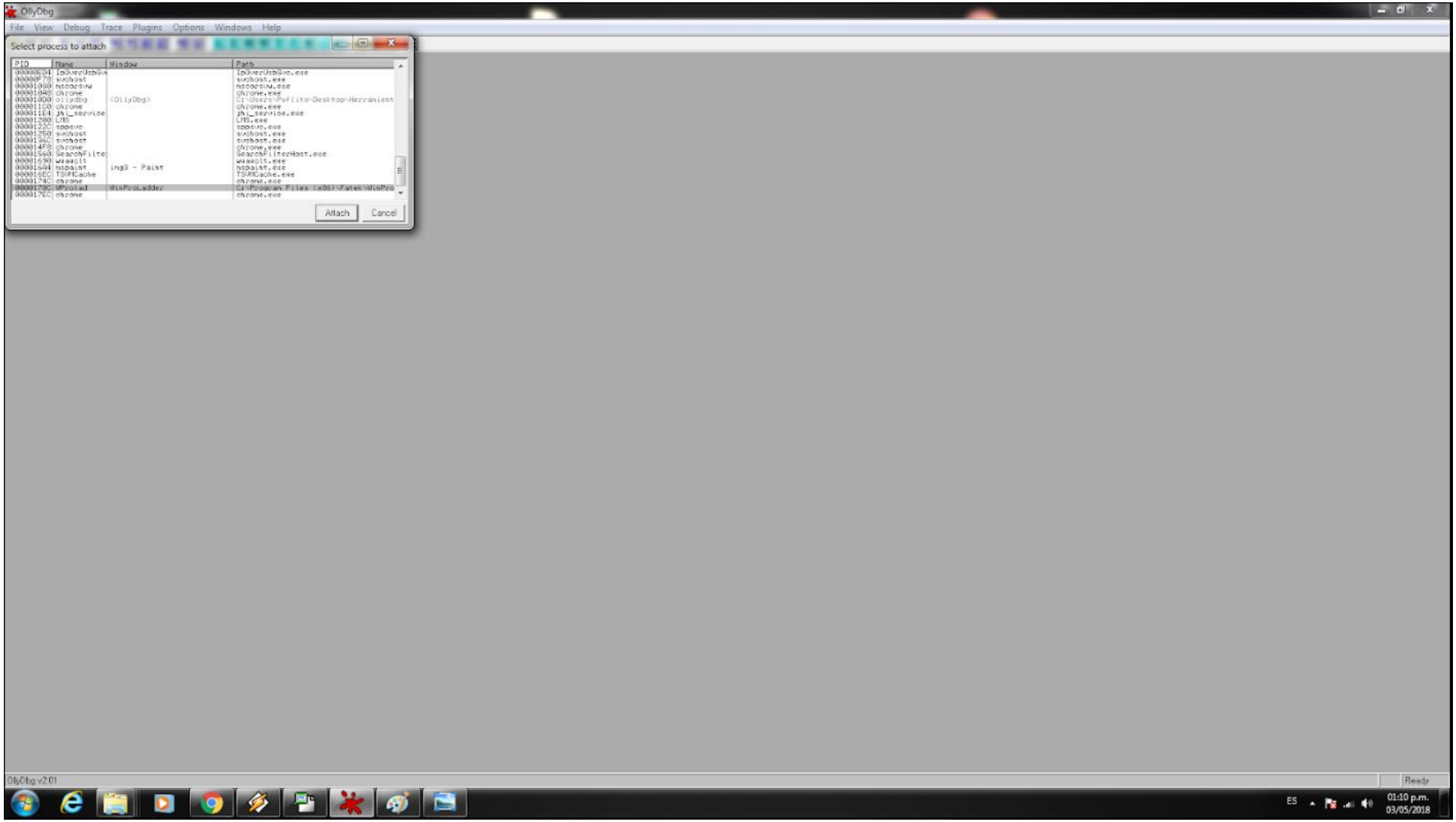
Ở đây chúng ta viết số bất kỳ và cho là ok.
Chúng ta sẽ thấy thông báo sau (Chúng tôi không nhấp vào Chấp nhận và chúng tôi mở OllyDbg):



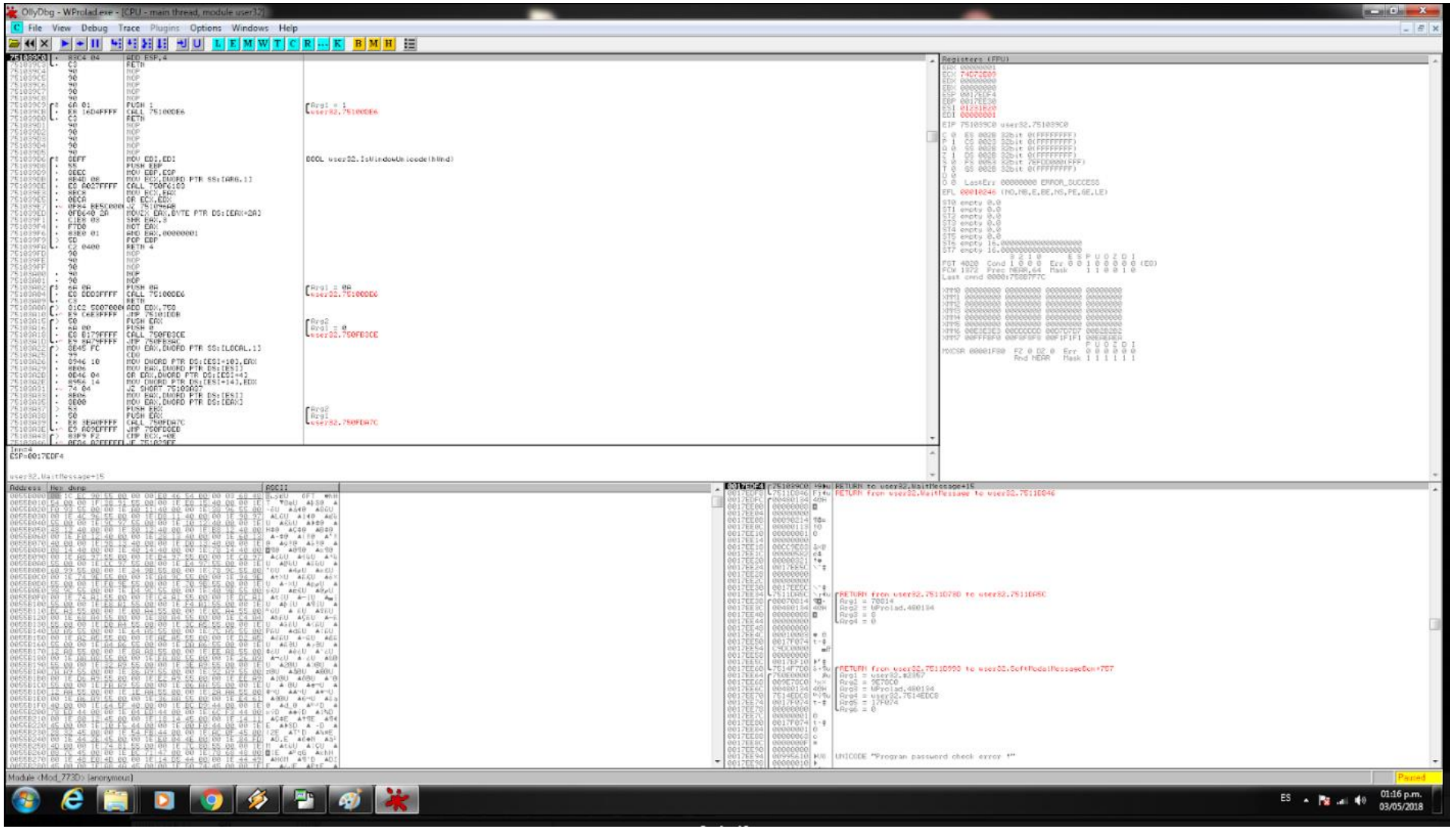
Khi Olly được mở, chúng tôi sẽ đính kèm quy trình, để thực hiện việc này, chúng tôi đi tới tùy chọn Tệp->đính kèm



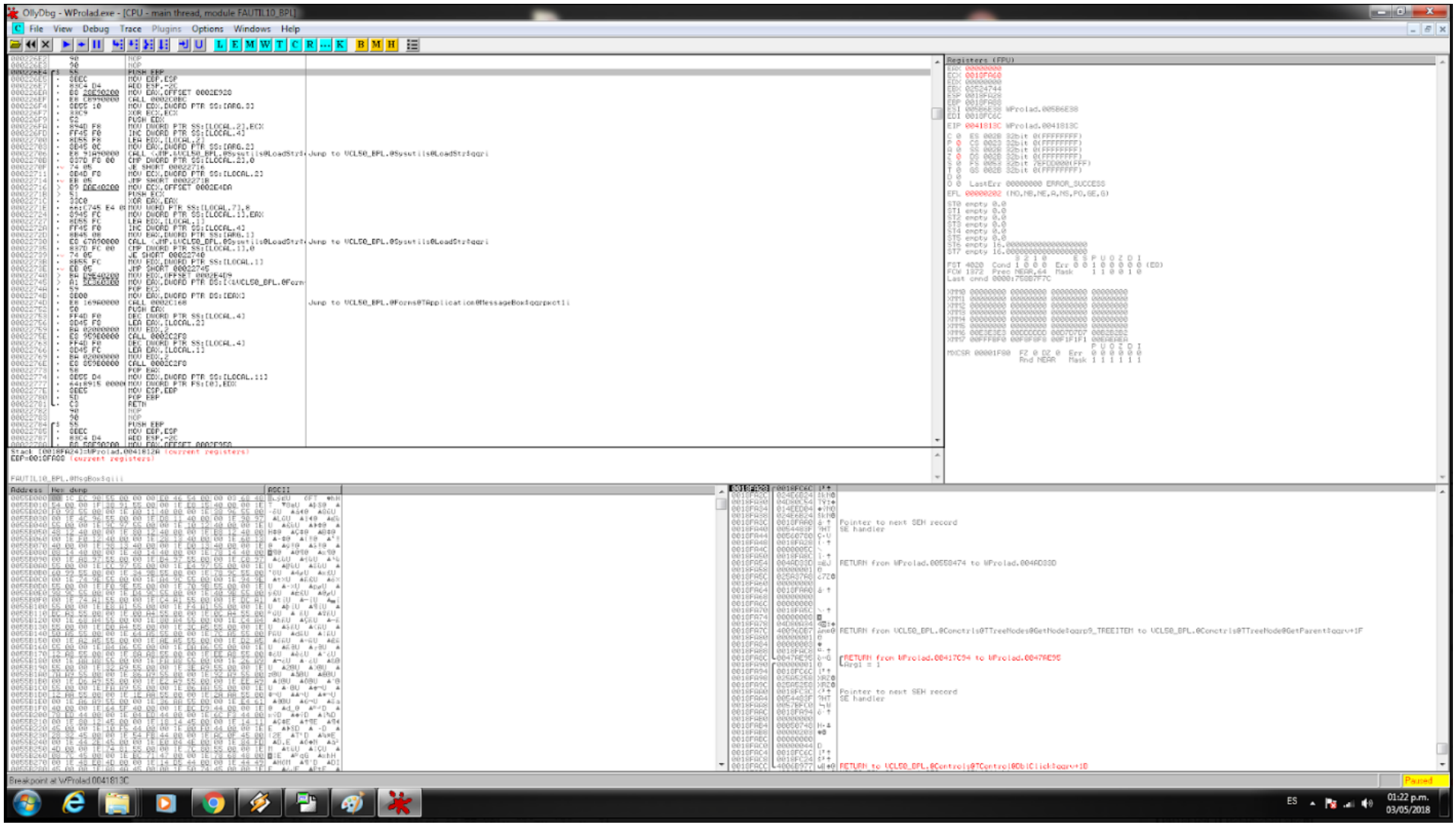
Hộp thoại sau sẽ xuất hiện, nơi chúng tôi tìm kiếm danh sách phiên bản của quy trình WinProLadder và chúng tôi đính kèm nó:

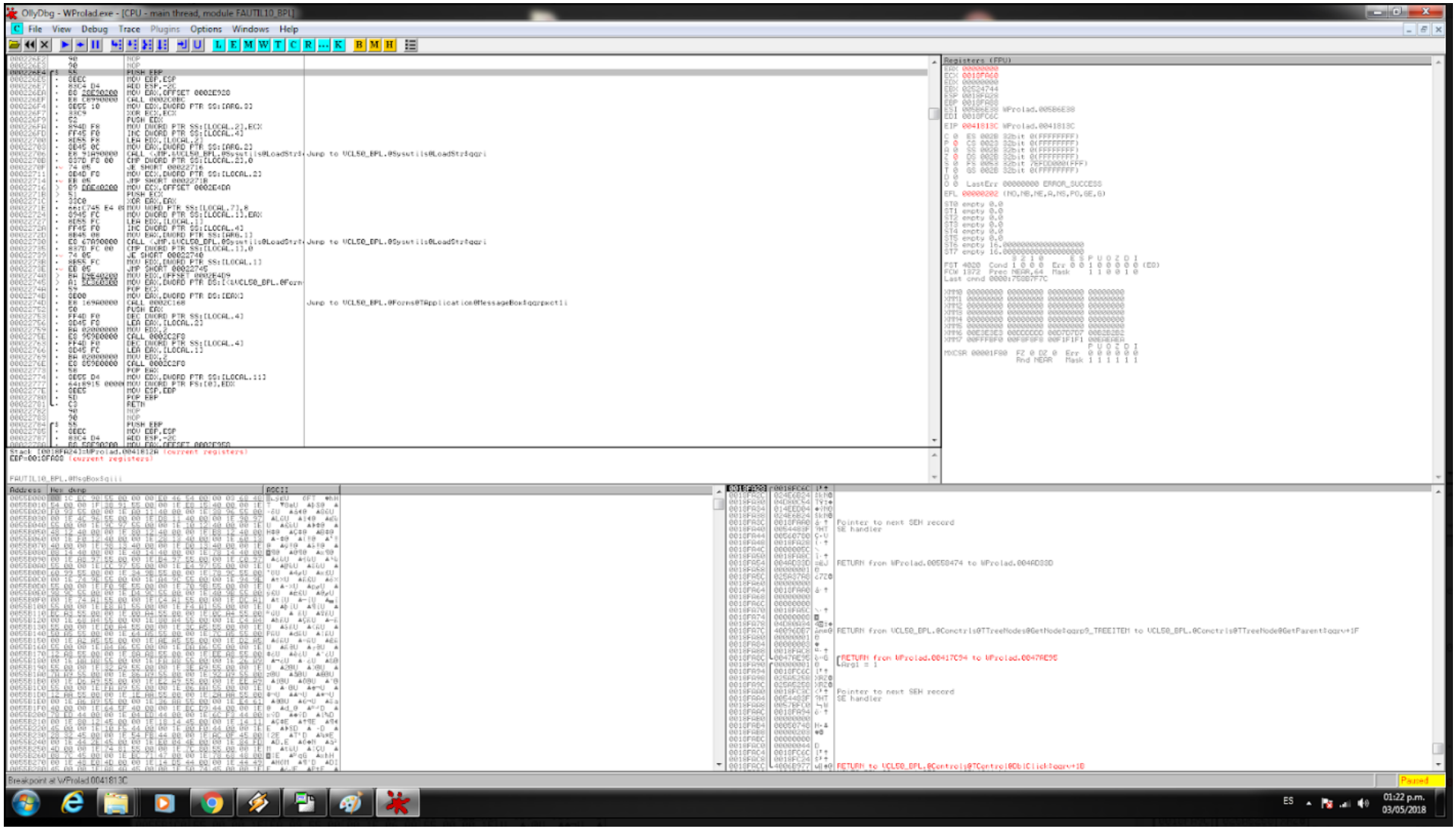


Sau khi được đính kèm, quá trình này sẽ bị tạm dừng theo hướng dẫn sau:

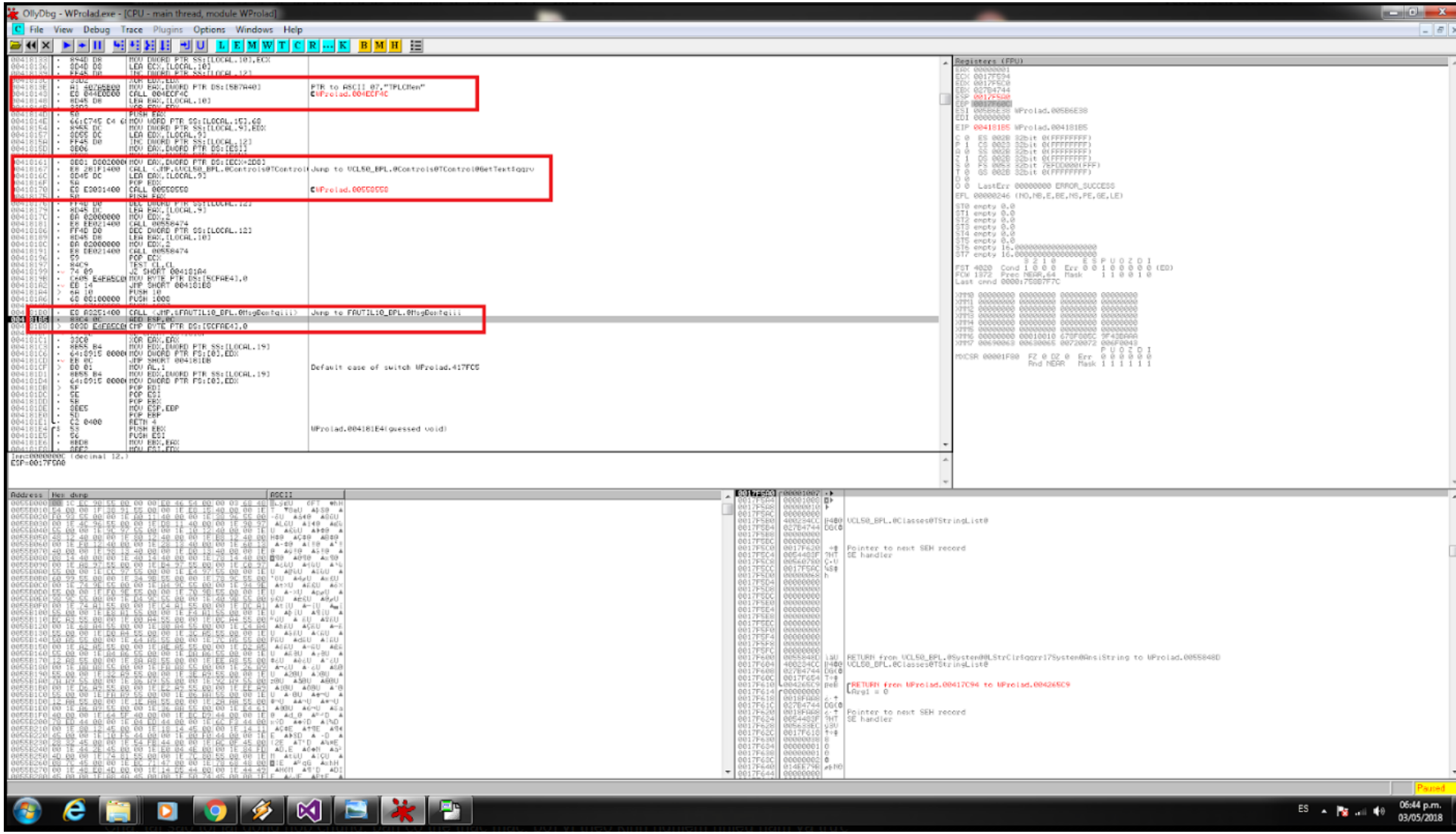


Ở đây chúng tôi bắt đầu nhấp vào Ctrl + F9 cho đến khi đạt được đoạn mã sau:


OllyDbg - WProlad.exe - [CPU - main thread, module FAUTIL10_BPL]
File View Debug Trace Plugins Options Windows Help
Registers (FPU)
Paused
ES
01:22 p.m.
03/05/2018

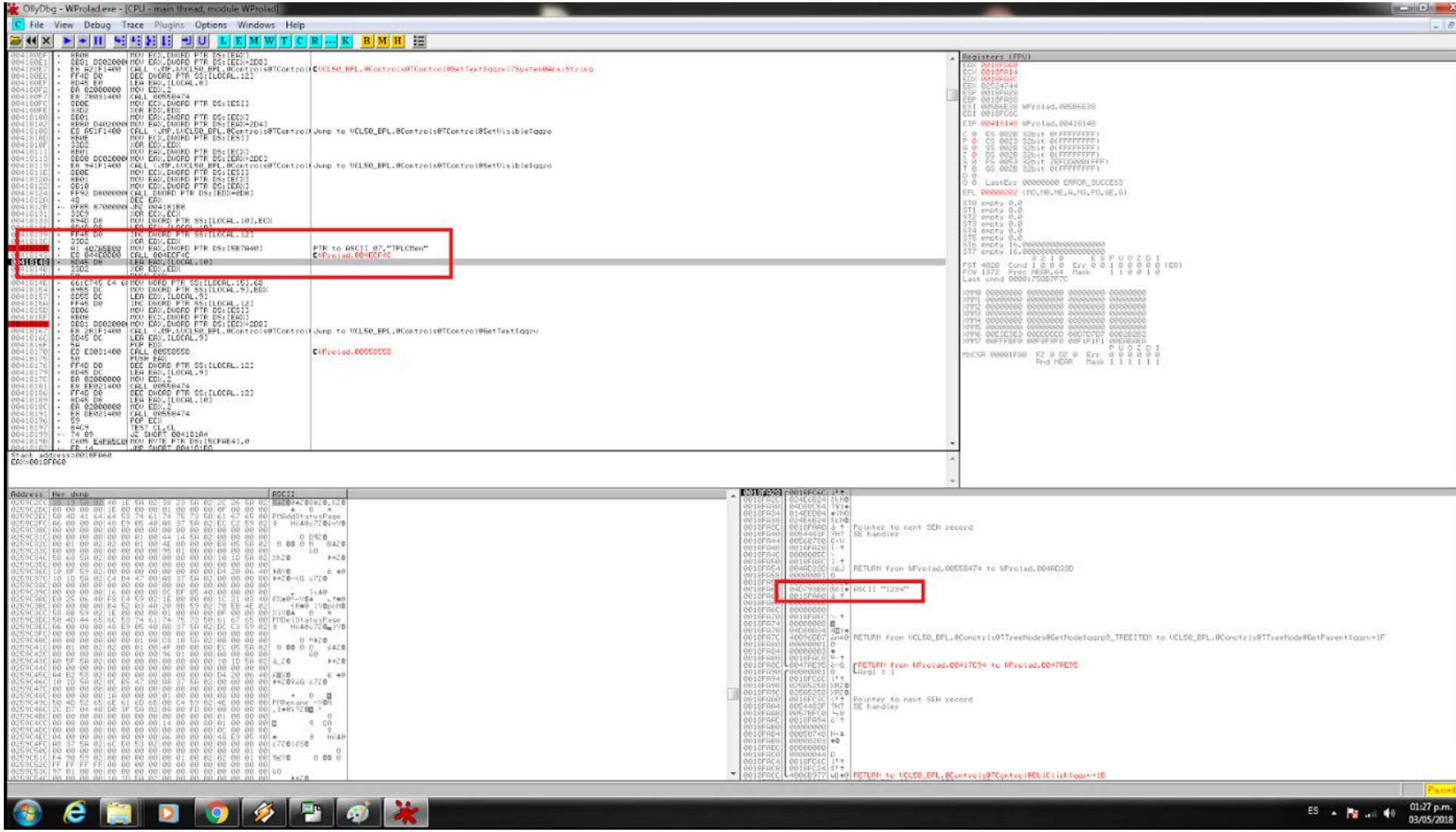


Phân tích đoạn mã trước, chúng tôi đi đến kết luận rằng hàm này là hàm hiển thị thông báo lỗi kiểm tra, nhưng nó không kiểm tra bất cứ thứ gì nên tôi tiếp tục nhấn Ctrl+F9 để thoát khỏi nó và đạt được đoạn mã sau:

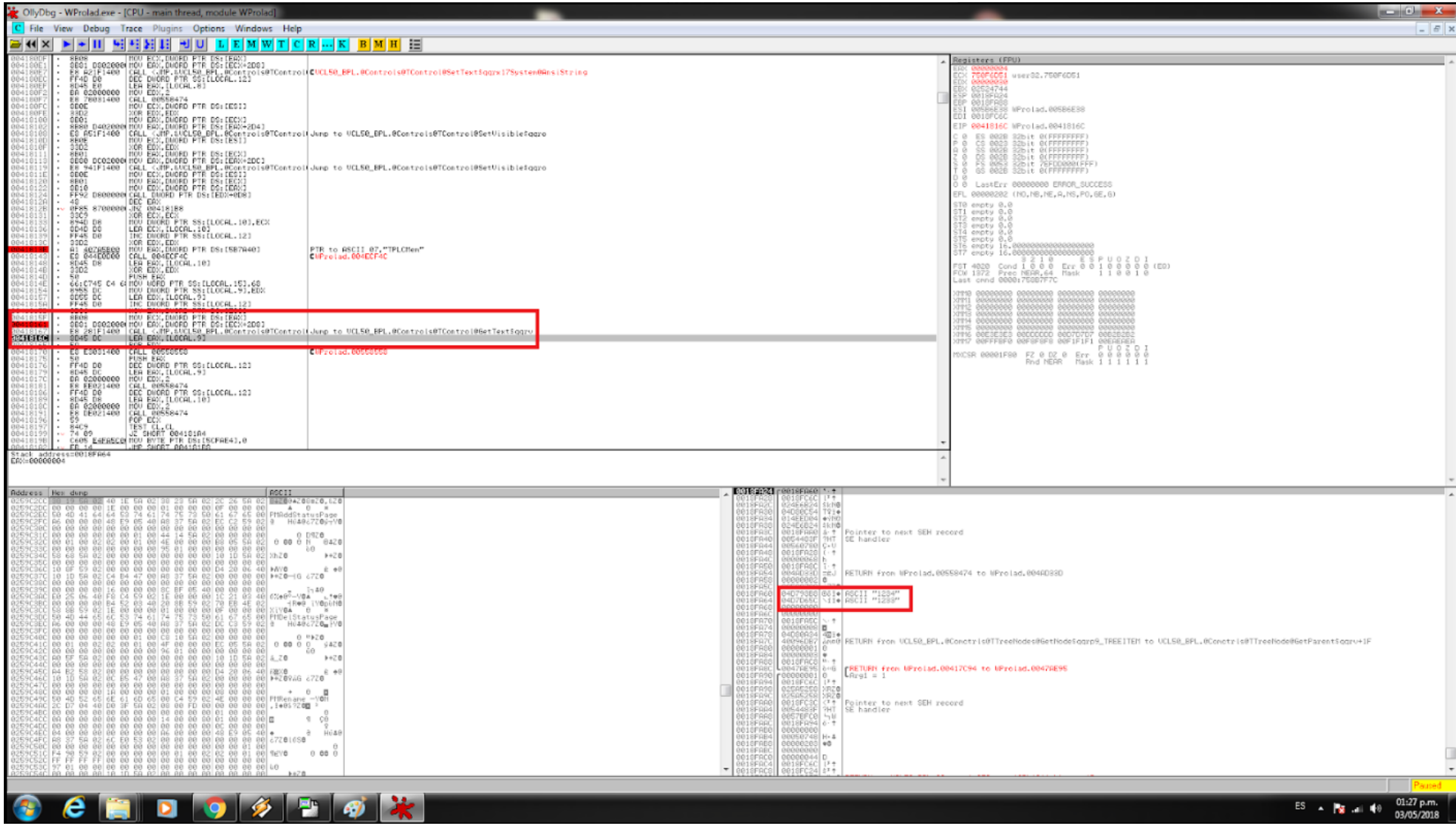


Sau khi quay lại, chúng tôi sẽ tìm thấy mã trong hình ảnh trước đó, như bạn có thể thấy, tôi đã liệt kê ba lệnh gọi hàm. Đây là những lệnh gọi khiến tôi chú ý, lệnh đầu tiên đề cập đến "TPLCMem", lệnh gọi thứ hai là "@Controls @TControl@ GetText$qqrv" và cái thứ ba là cái chúng tôi đã quay lại.

Chà, tại sao tôi lại đóng hộp chúng, bạn có thể thắc mắc, bởi vì theo kinh nghiệm nhiều năm và trực giác của tôi, họ cho tôi biết rằng hai chức năng trước tin nhắn đó là chức năng thu thập dữ liệu kiểm tra và các lệnh gọi sau dành cho nhiều loại kiểm tra khác nhau , và như có thể thấy ngay trước lệnh gọi mà chúng ta quay lại, có một đoạn mã nhỏ với hai lần nhảy, một JZ và một JMP, như bạn biết, JZ là một bước nhảy có điều kiện nếu nó bằng 0 và JMP là một bước nhảy vô điều kiện, trong Nếu đường chuyền không chính xác, so sánh sẽ cho kết quả bằng 0 và JZ được kích hoạt, đưa chúng ta đến thông báo lỗi kiểm tra, nếu không, nó sẽ đi qua JMP và cho phép chúng ta truy cập vào dự án để chỉnh sửa.
Dù sao, tôi thích lắng nghe trực giác của mình hơn (và không làm phức tạp mọi thứ bằng quá nhiều phân tích), vì vậy tôi đặt hai BP, một vào chức năng đầu tiên và một cái khác vào chức năng thứ hai trong số ba chức năng mà tôi đã đánh dấu, tôi nhấn chạy trên olly, Tôi chấp nhận lỗi tin nhắn Tôi nhập sai pass một lần nữa và tôi chấp nhận, tại thời điểm chấp nhận phá sản ở BP đầu tiên:



Sau khi tôi chuyển cuộc gọi đầu tiên bằng F8 (được đóng hộp trong hình ảnh trước đó ở bên trái), bạn có thể thấy trong cửa sổ ở phía dưới bên phải (Ngăn xếp) một chuỗi ký tự số nhỏ mà tôi cũng đã đánh dấu bằng hộp màu đỏ.
Tôi tiếp tục gỡ lỗi cho đến khi vượt qua BP khác và thực hiện chức năng bí ẩn thứ hai:



Giống như hàm trước, nó trả về một chuỗi khác được lưu ngay bên dưới chuỗi trước (cả hai đều được đánh dấu trong hộp màu đỏ ở dưới cùng bên phải), chuỗi thứ hai này có vẻ quen thuộc với tôi, vì đó là mật khẩu mà tôi đã nhập nhầm. thực hiện kiểm tra, vì vậy chuỗi đầu tiên phải là mật khẩu ban đầu của dự án, chúng tôi thực hiện kiểm tra và đúng như mong đợi, chúng tôi đã đúng.

Chúng ta đã đạt được mục tiêu của mình là có thể truy cập vào dự án, vì vậy hướng dẫn nhỏ này kết thúc ở đây.

Đừng ngần ngại hỏi nếu bạn có bất kỳ câu hỏi nào!

Khi có thời gian và nguồn lực, tôi sẽ thực hiện nhiều hướng dẫn hơn về các hệ thống khác.

Lời chào hỏi!!!