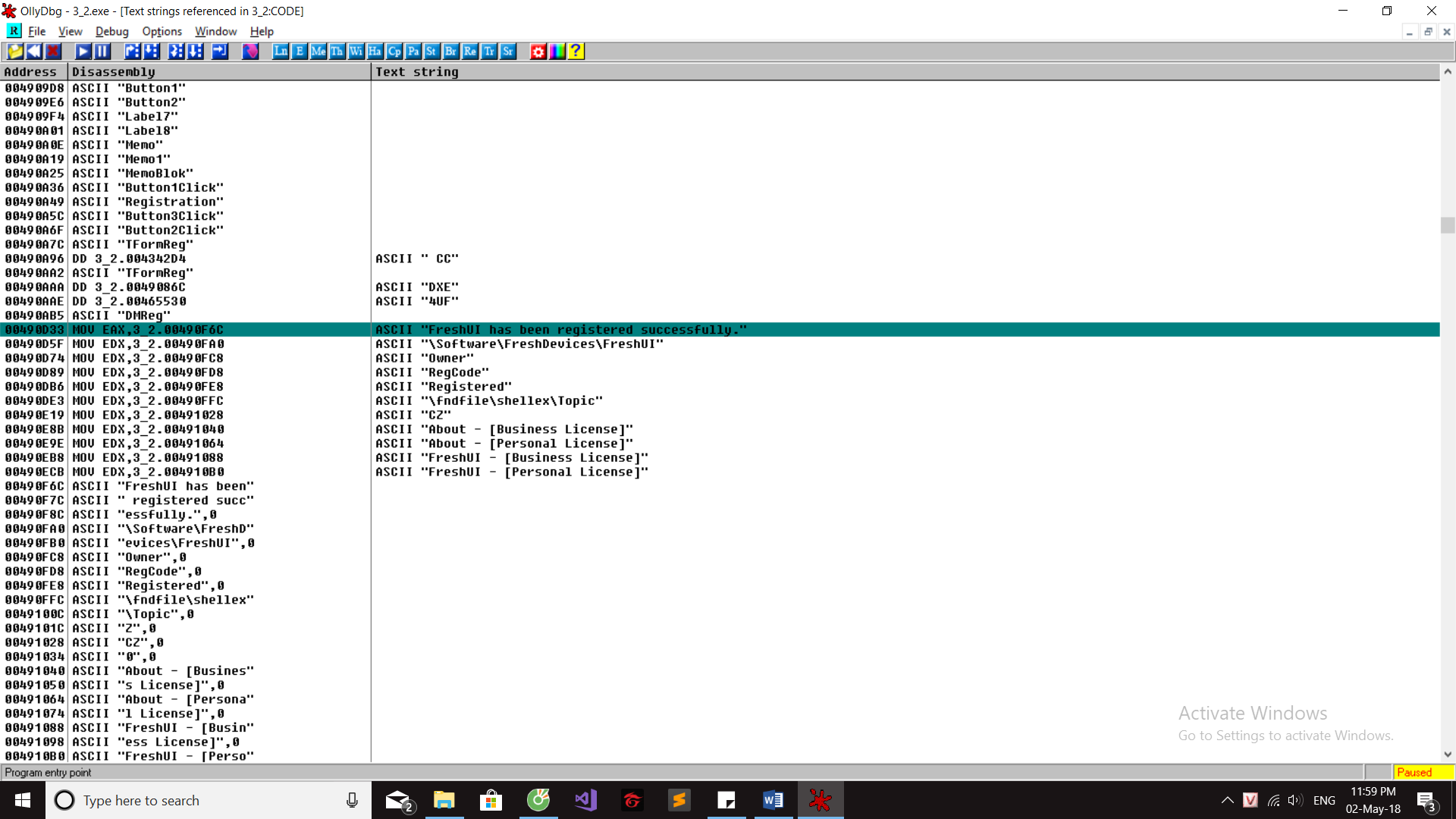
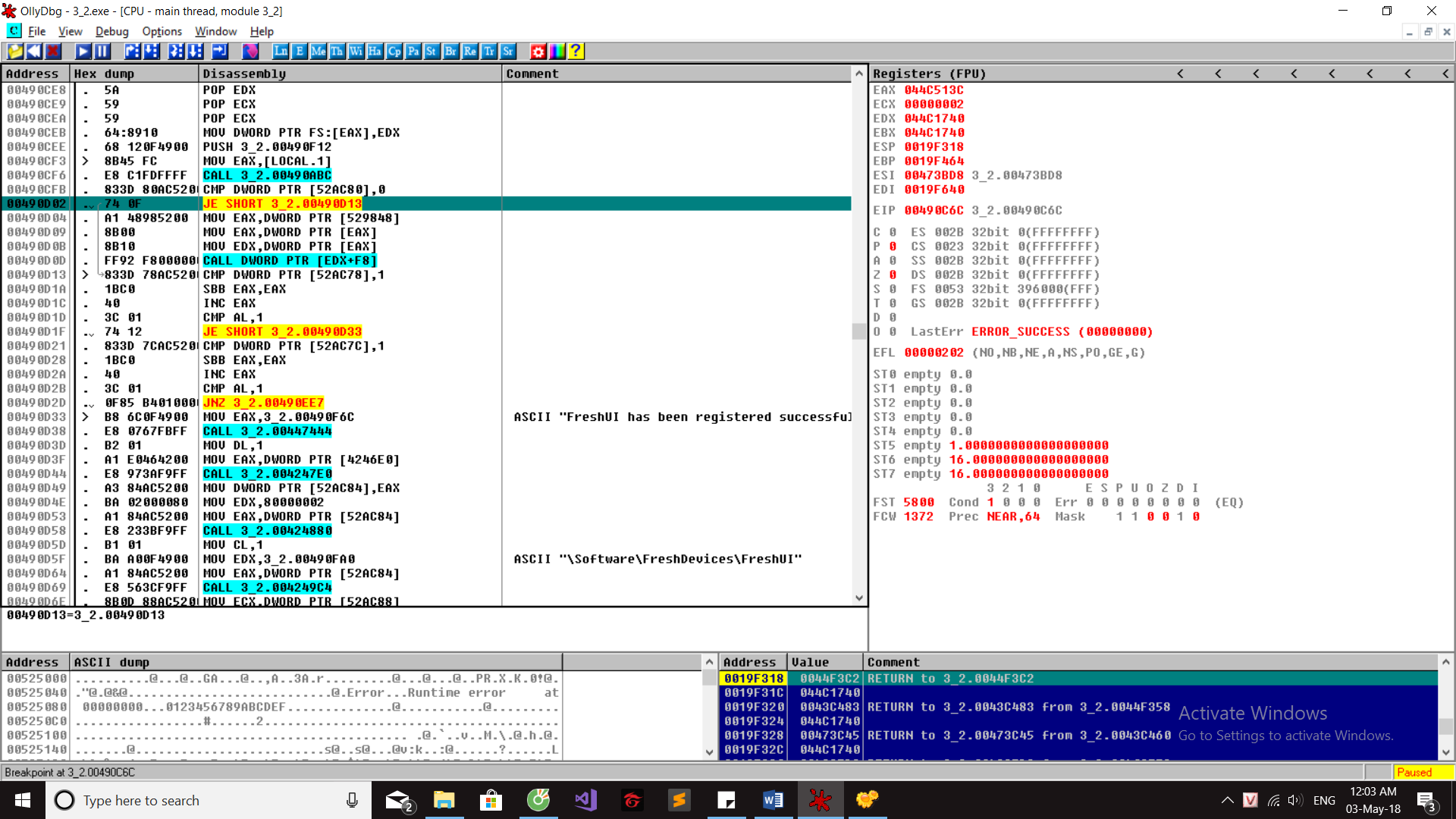
CrackMe 3\_2:

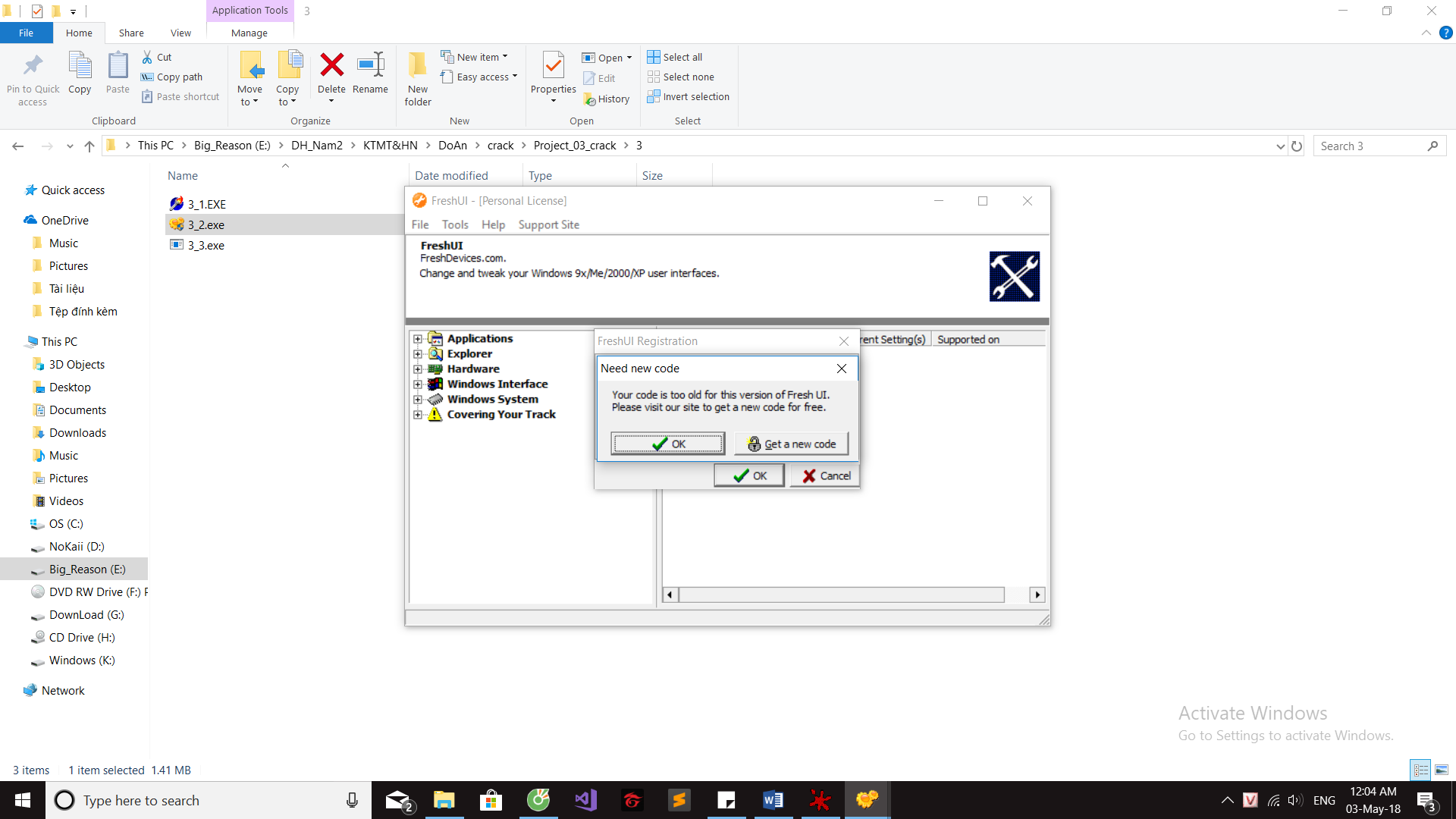
Tìm key: Trước hết ta tìm goodboy là một chuỗi có dạng như sau (Không có badboy).



Ta nhận thấy trước goodboy có 2 lệnh CALL.

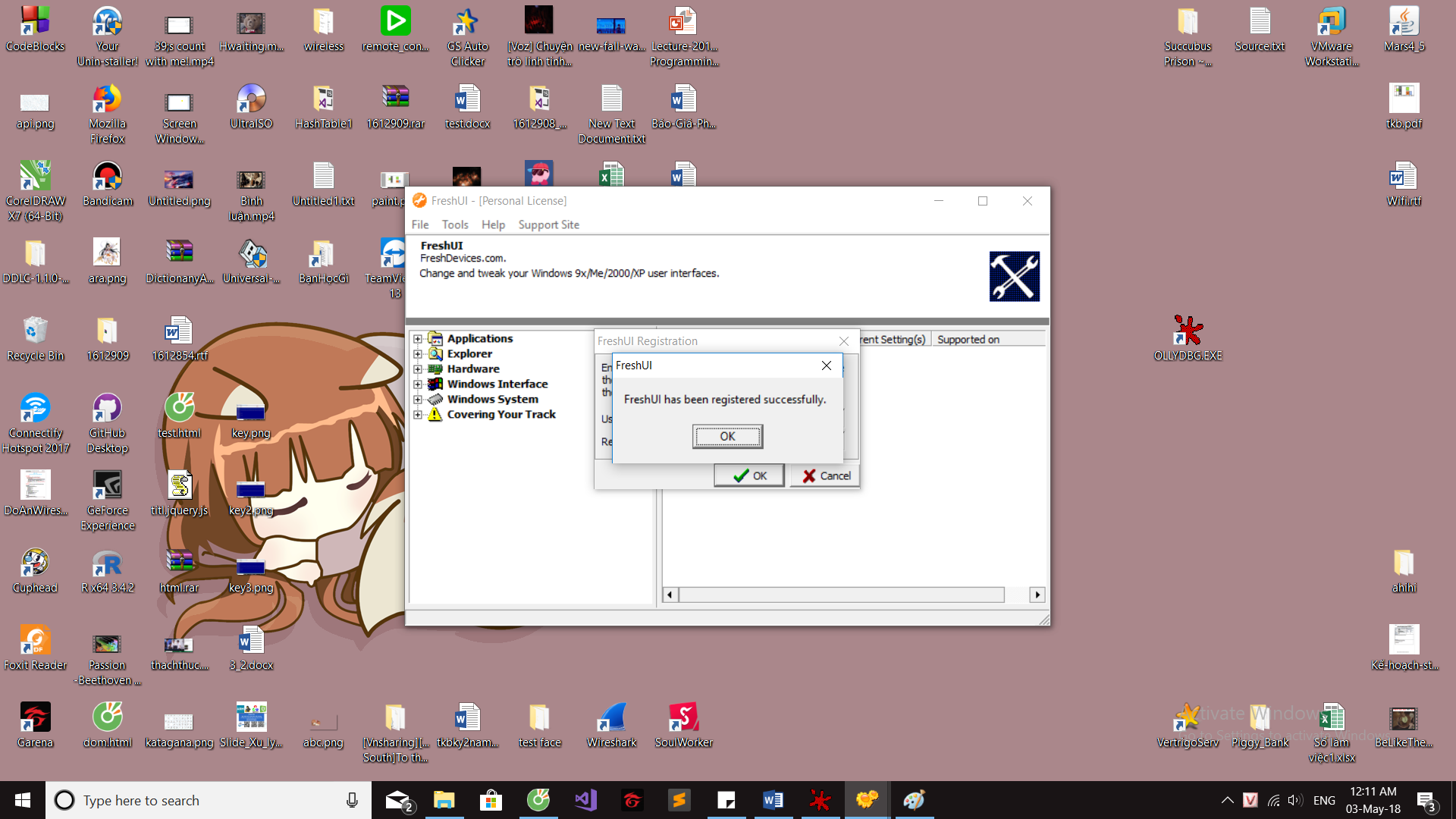


Lệnh gần GoodBoy nhất là lệnh để khi nhập OldKey thì sẽ nhảy vào và xuất ra thông báo Key đã Cũ.

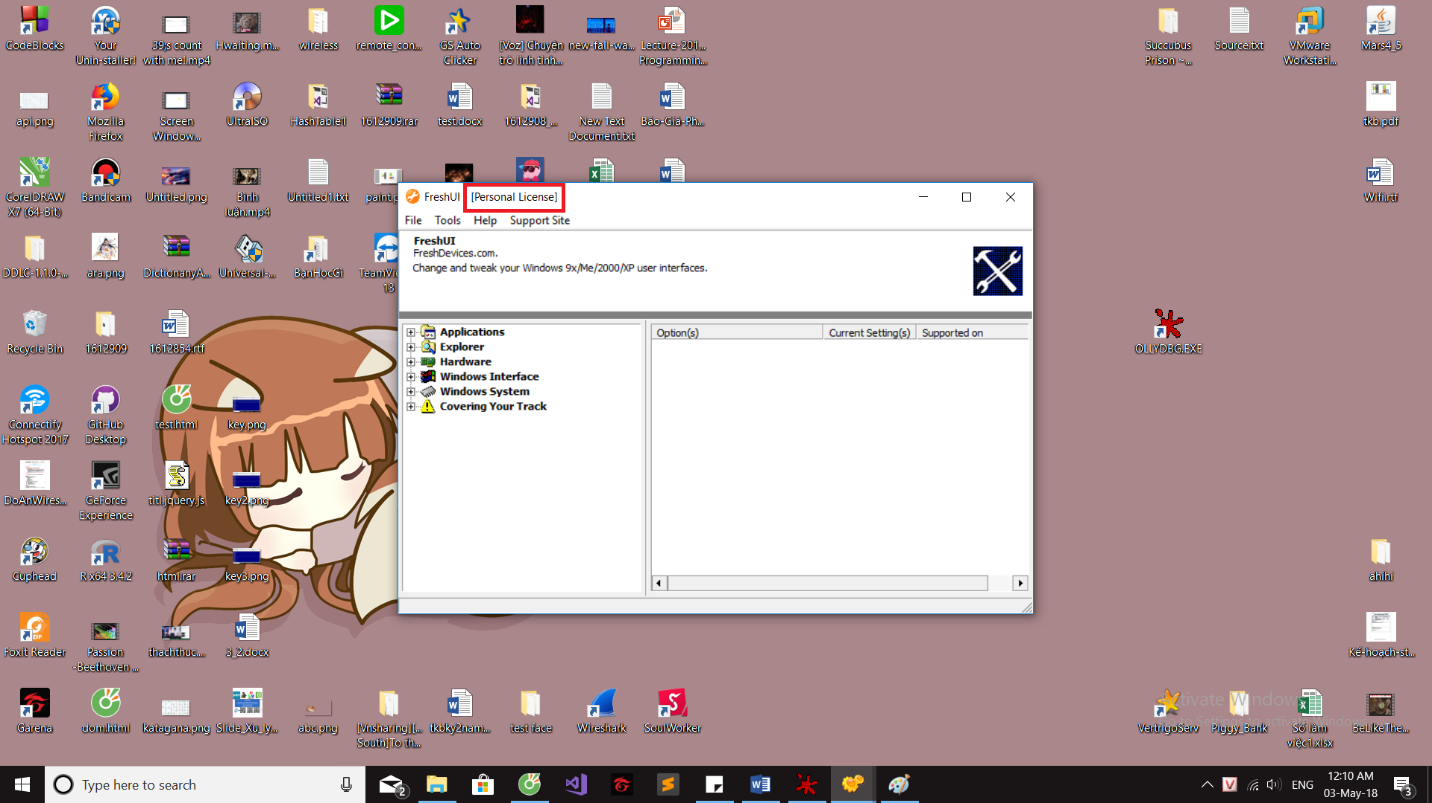


Còn hàm CALL ở trên thì tách 3 loại key ra riêng biệt (dùng 3 vòng for) và so sánh key mình nhập vào với 3 loại key đó.

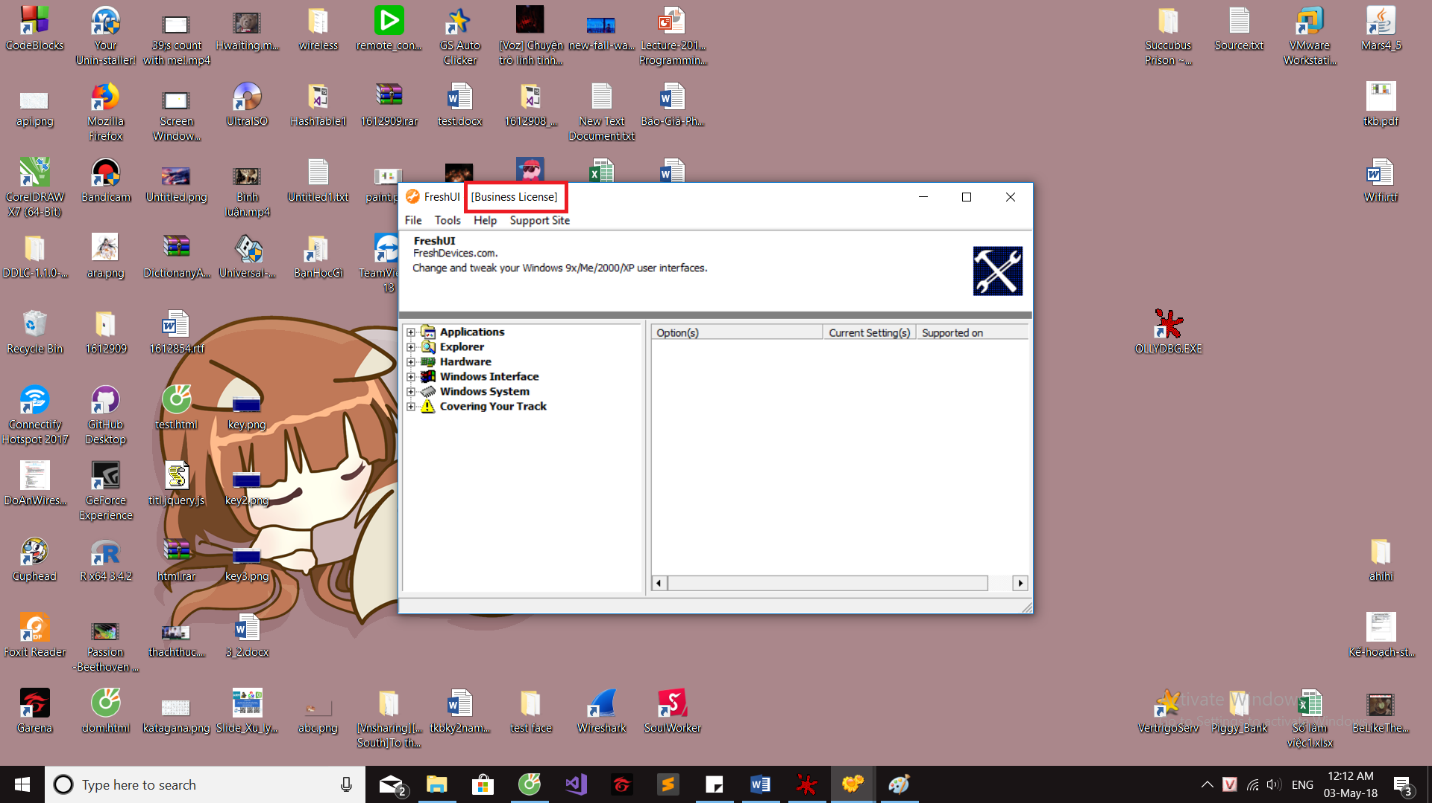
Khi nhập vào key đúng (Hai loại key còn lại – Trừ OldKey) ta sẽ thấy goodboy.



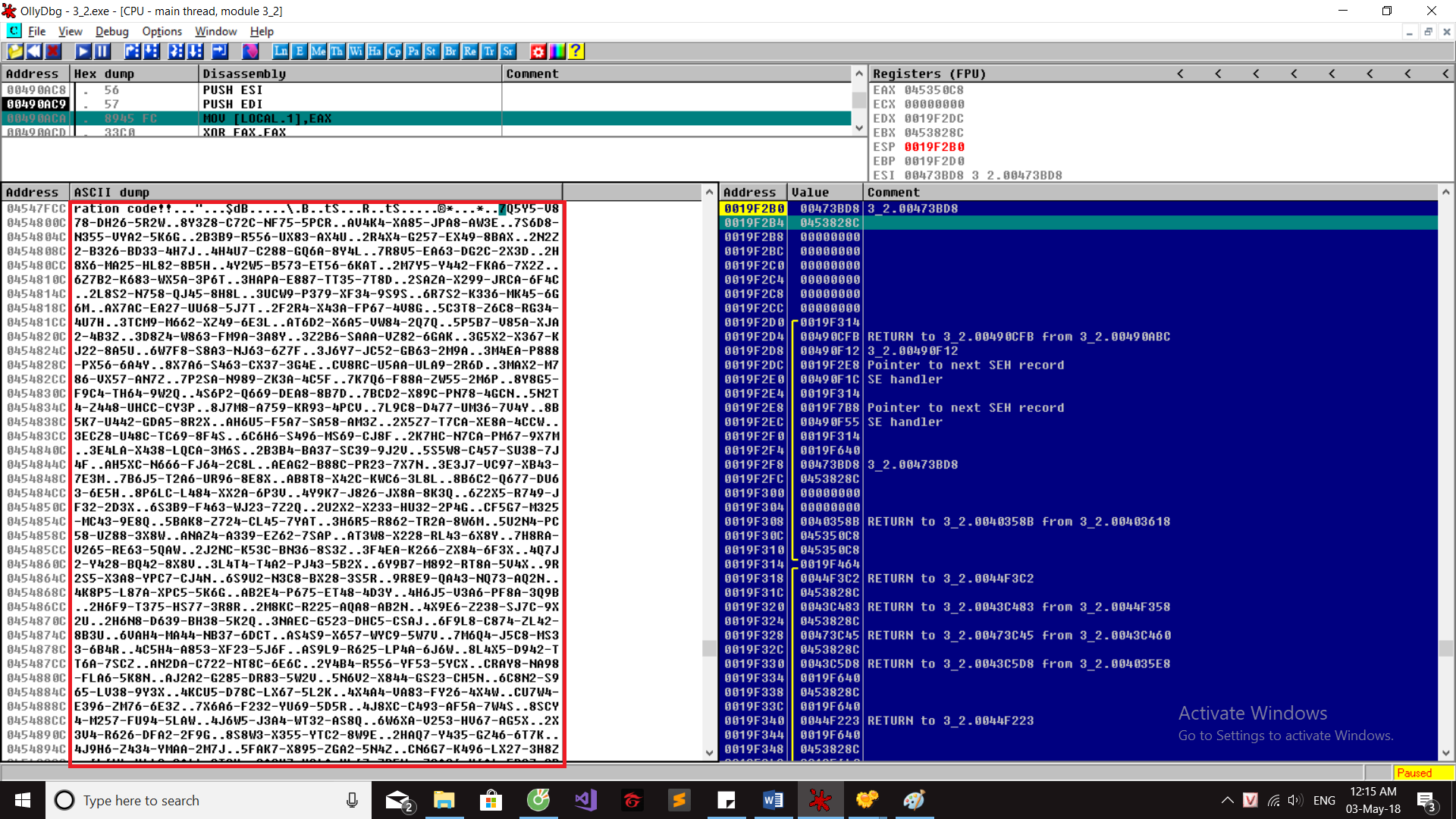
Với personal key:



Với business key:



Đoạn phát sinh key: Nghi vấn key có sẵn trong file vì khi “follow in dump” tại khoảng địa chỉ 04xxxxxx ta có thể thấy hết key.



Key hiện trong dump tại địa chỉ 004422FF0. Nên không có hàm phát sinh.

Tại vùng nhớ này key xếp lần lượt theo thứ tự Personal Key, Business Key và Old Key.

Trong chương trình này có 3 loại key:

1. Personal Key: Định dạng gồm các chữ in và số, và có dấu gạch nối. Personal key có 21 ký tự.

Ví dụ về một personal key: 7Q5Y5-V878-DH26-5R2W.

1. Business key: Định dạng gồm các chữ thường và số, dấu gạch nối. Business key có ký tự.

Ví dụ về một business key: bv2c3r-4x4bu2b3-6f5t44.

1. Old Key: Định dạng giống như Pesonal Key, trong chương trình này có 4 Old Key.

Ví dụ về một Old Key: 7B9X8-Z523-KV67-6T5U.