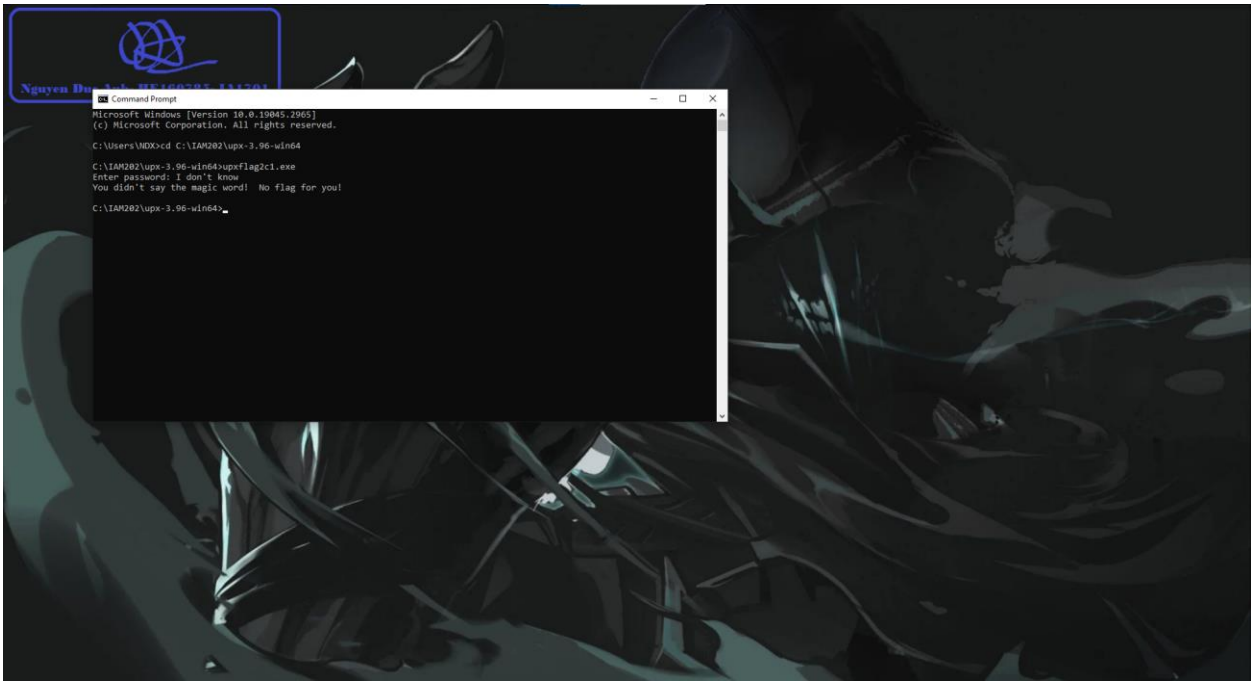
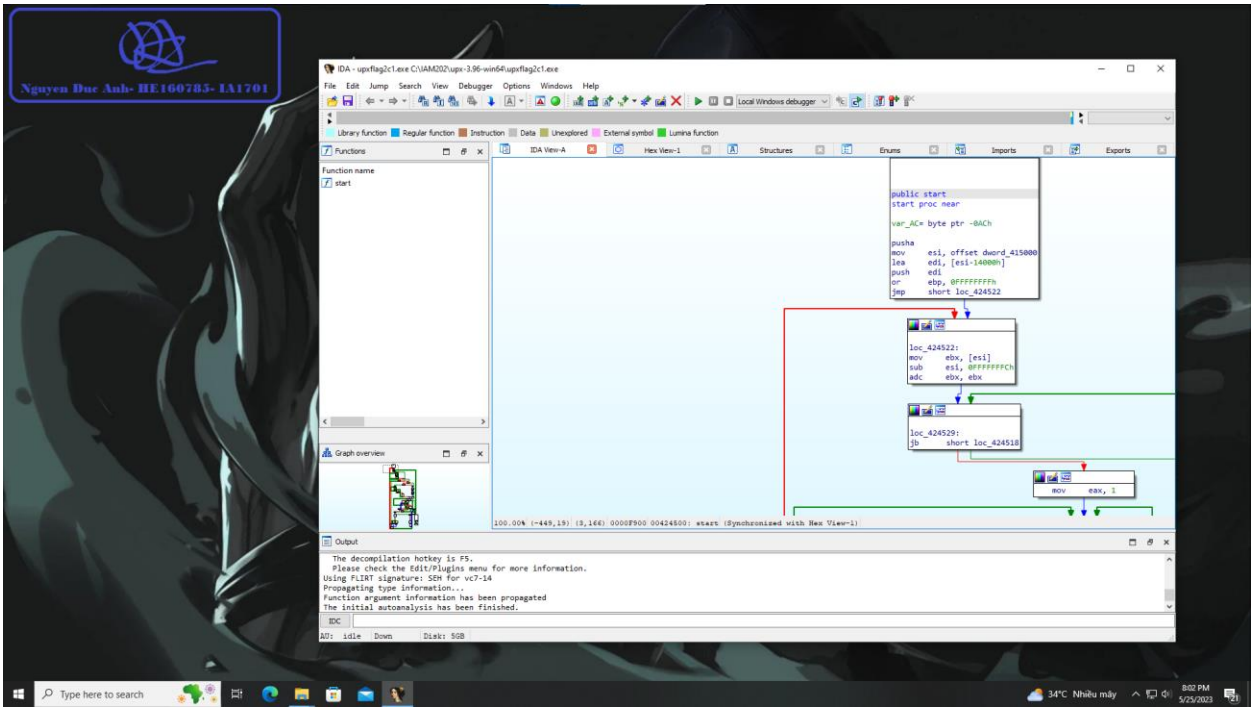
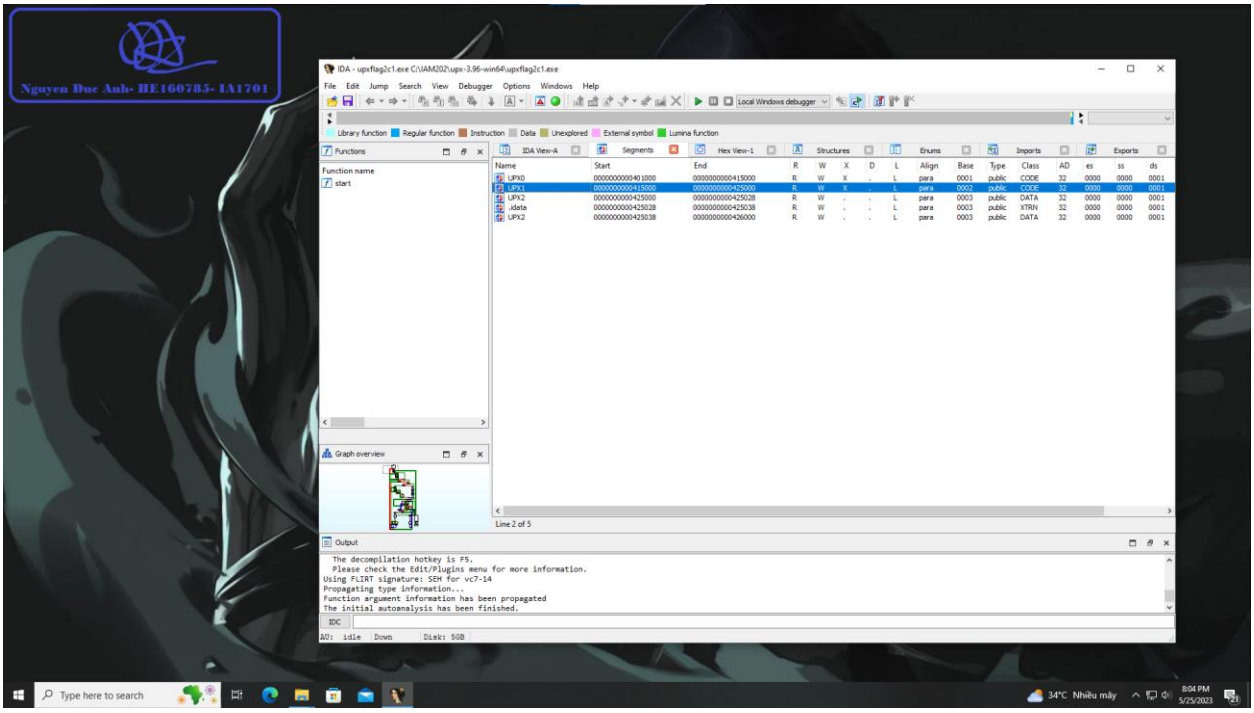
Đầu tiên ta sẽ chạy thử file upxflag2c1.exe



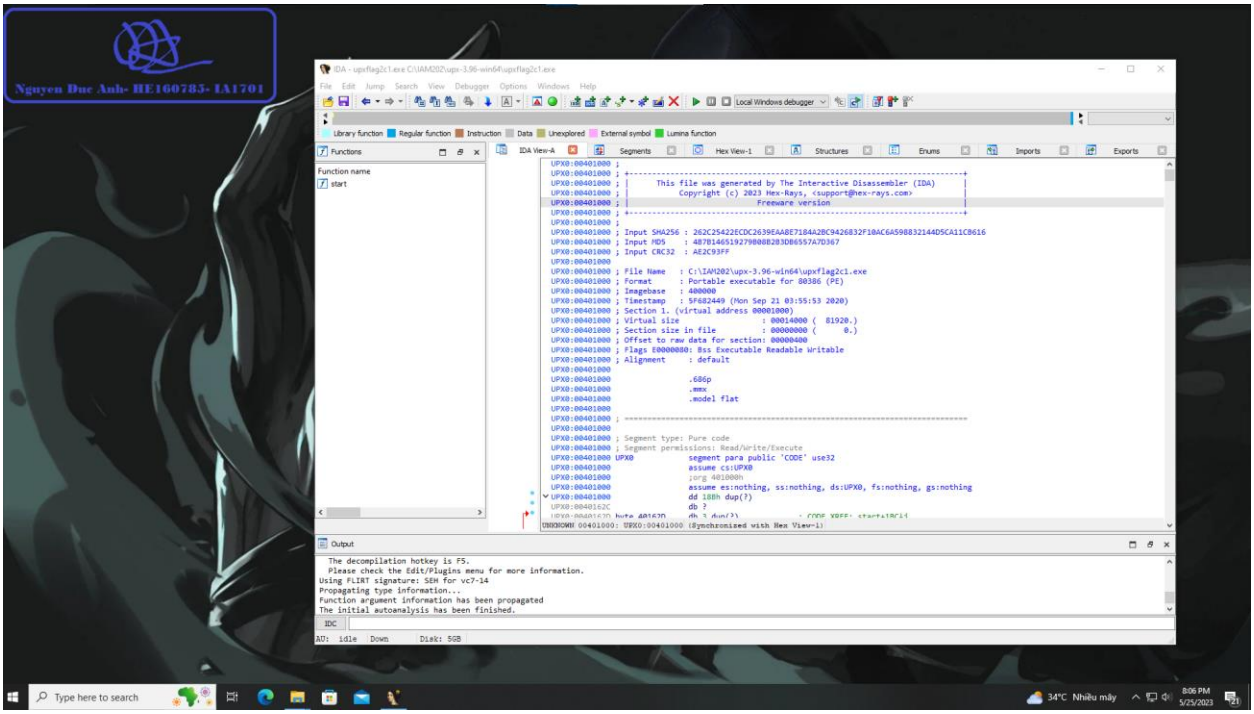
Ta thấy nó bắt điền password mà chúng ta chưa biết password là gì nên sẽ phải đi kiểm tra file này mở file upxflag2c1.exe bằng IDA



Đầu tiên thì chúng ta sẽ kiểm tra các section trong file này

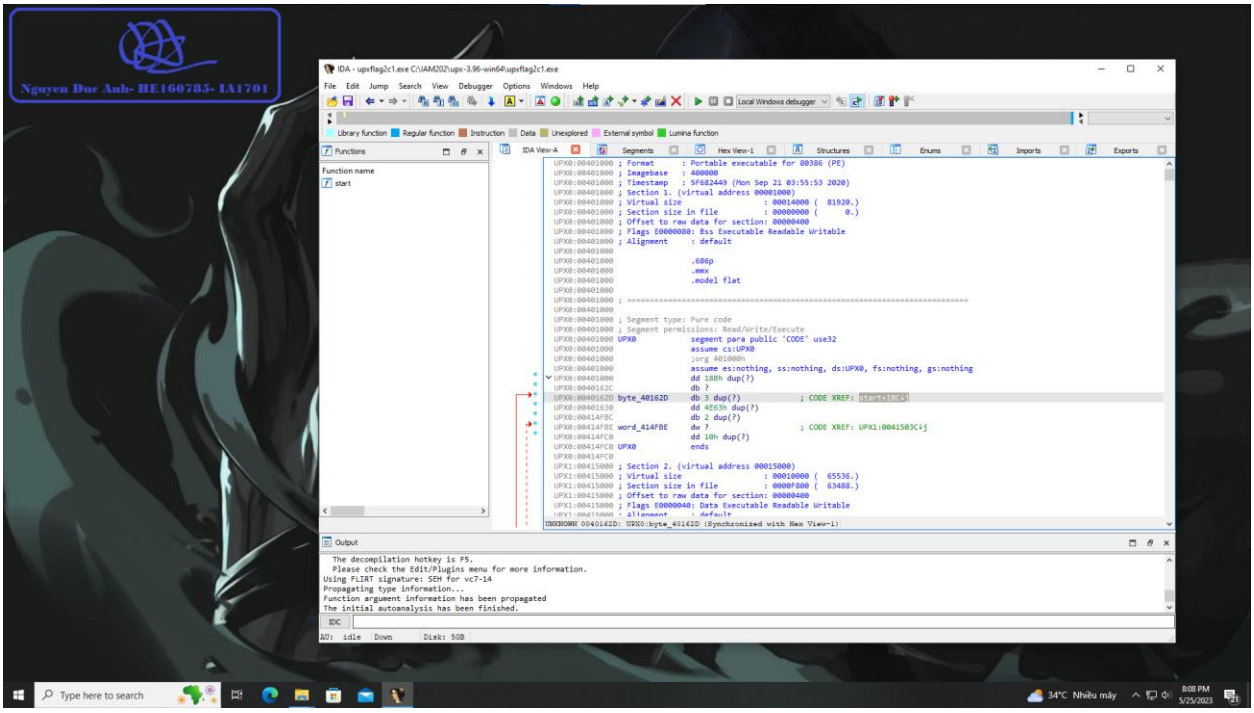


Trước hết ta sẽ kiểm tra section UPX0

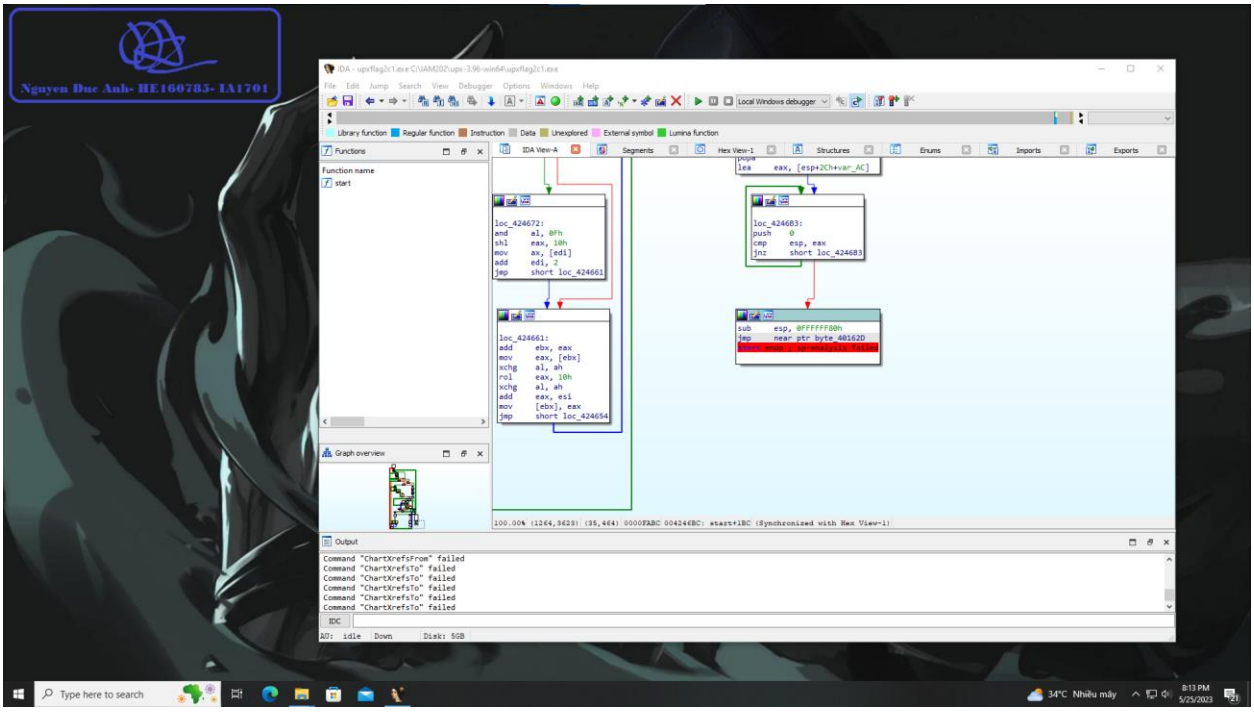


Ta thấy được code bắt đầu của section UPX0 địa chỉ bắt đầu của nó là 0040100

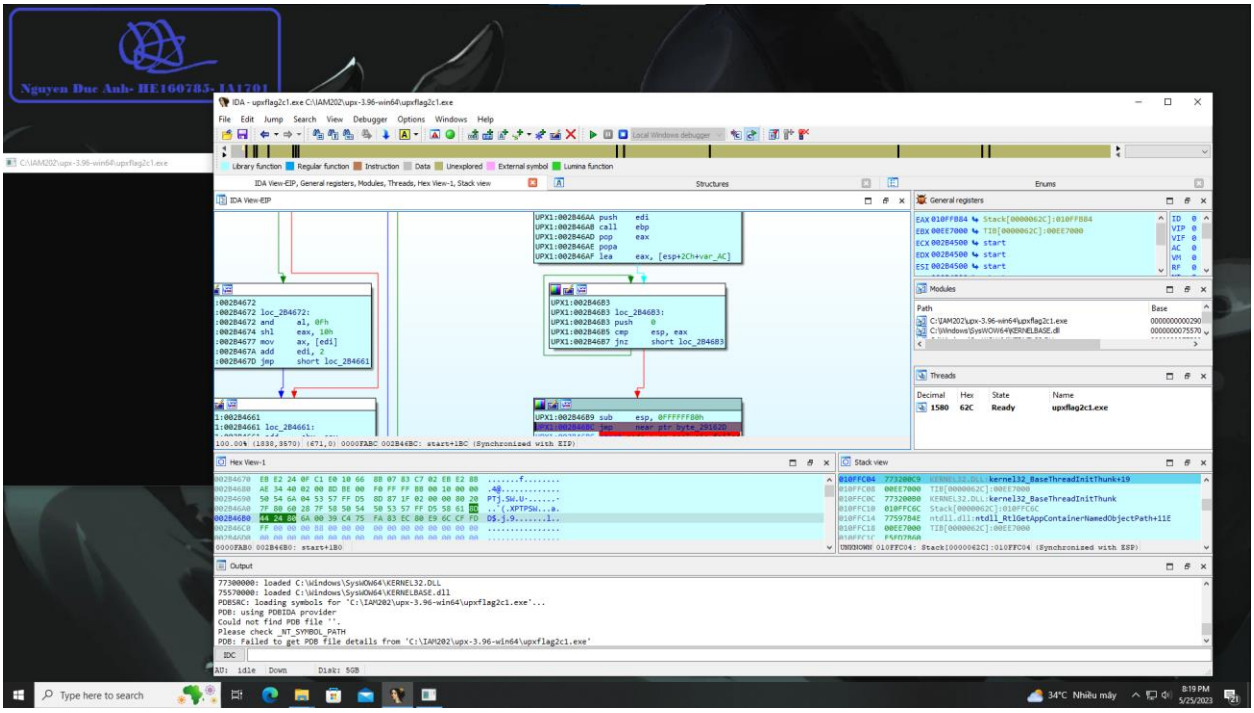
Sau đó xem tiếp tại địa chỉ 0040162D ta thấy có CODE XREF: start+1BC ↓ j, đây là tham chiếu của mã thực thi đến entrypoint của file upxflag2c1.exe



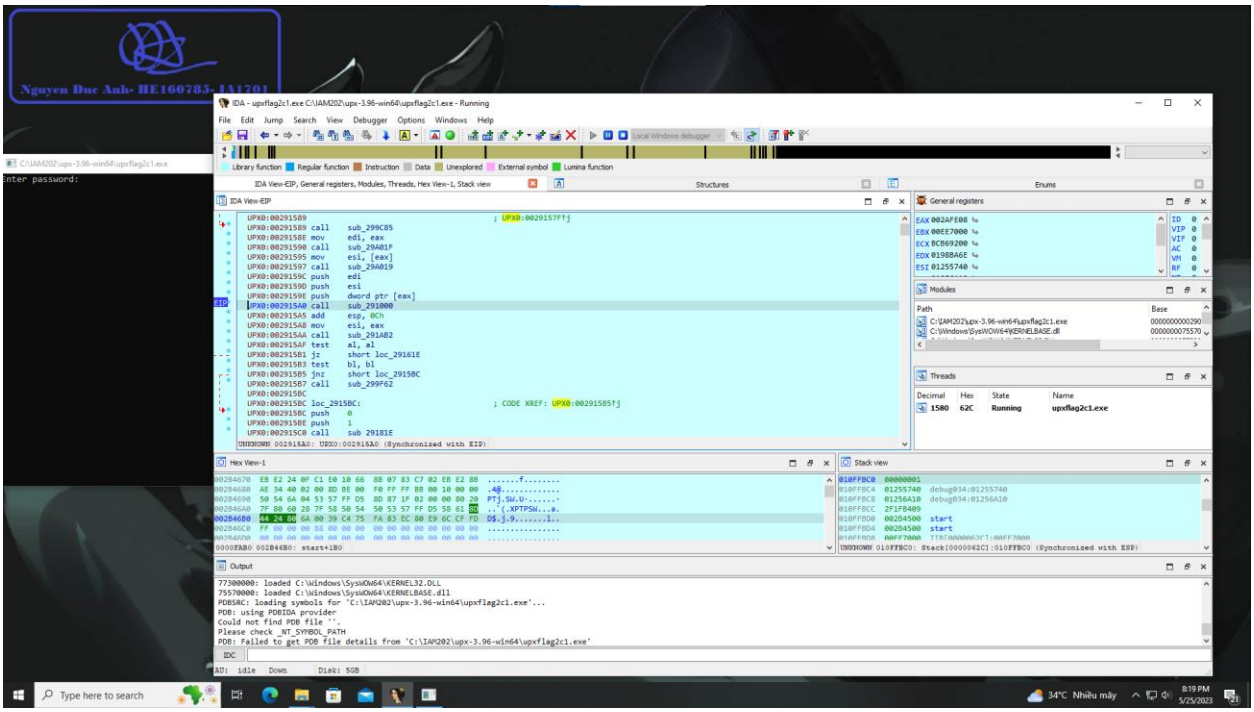
Giờ ta sẽ trỏ đến nơi được tham chiếu



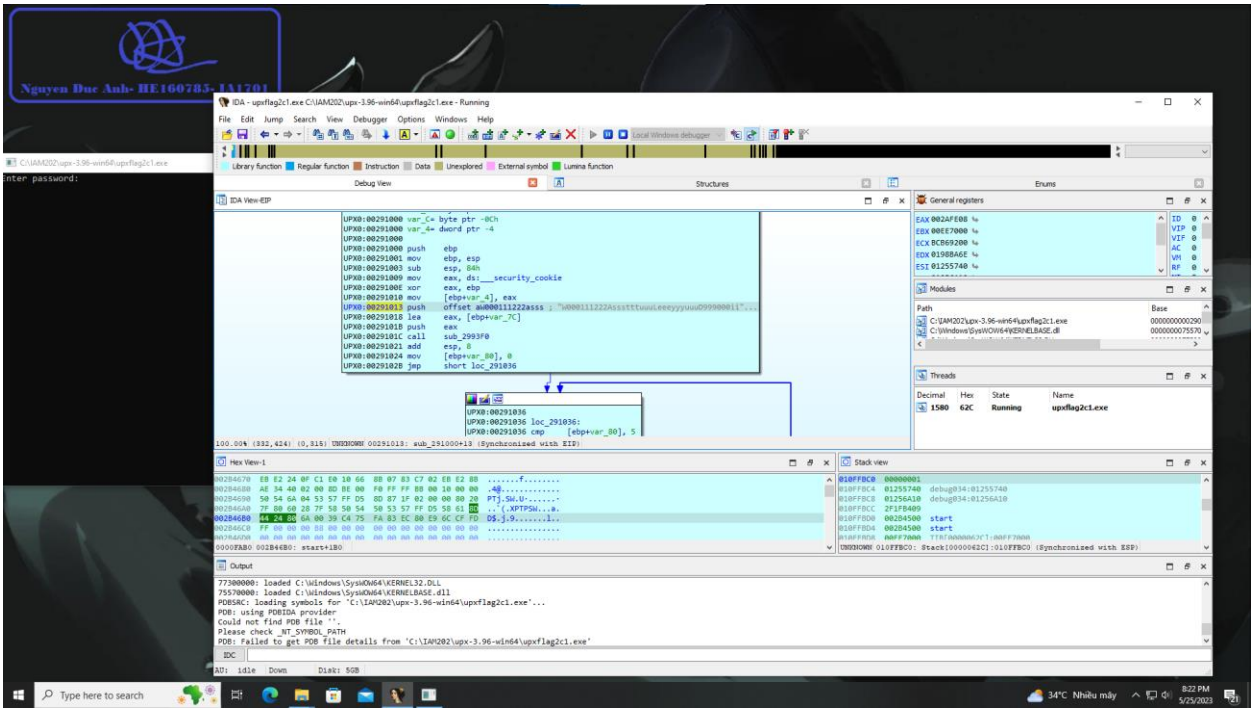
Ta thấy được jmp near ptr byte_40162D đây là entrypoint của Stub chứ không phải của OEP, nên ta sẽ Debug chương trình từ lệnh này

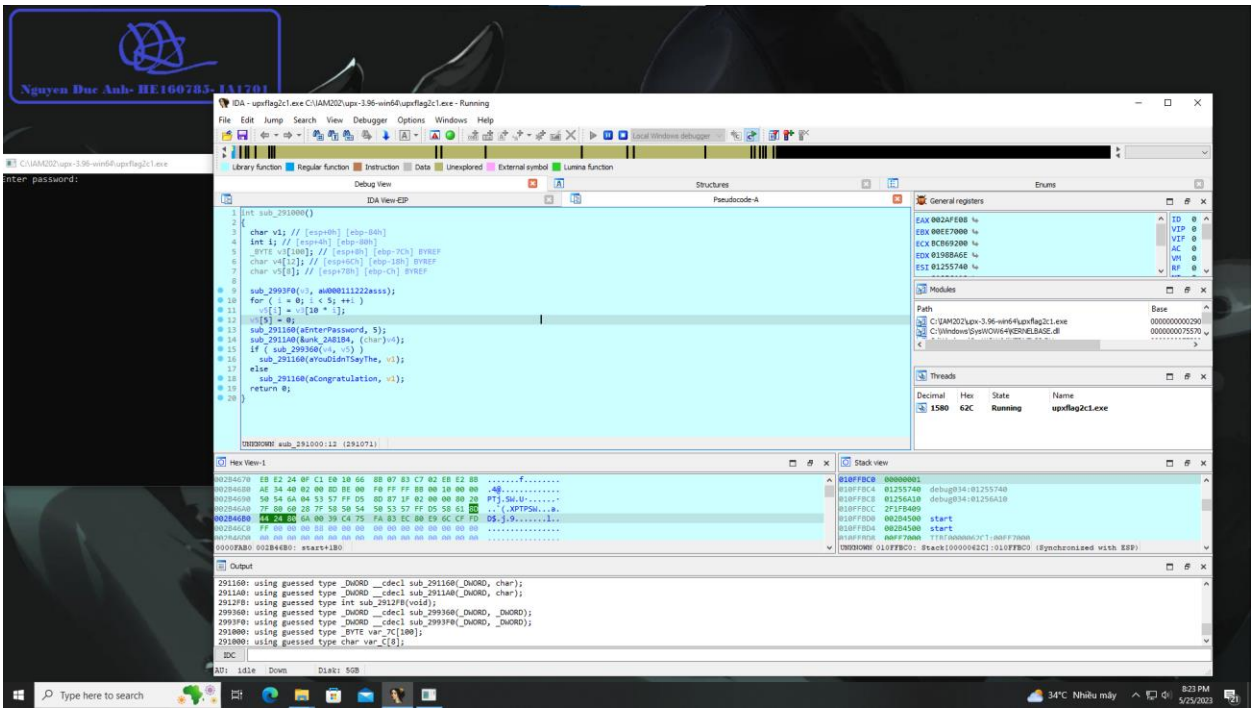


Sau khi debug ta thấy chương trình dừng lại ở lệnh call sub_291000 và trên cmd hiện Enter password:



Ta sẽ đi vào hàm sub_291000





Ở đây ta sẽ thấy được code mà chương trình dùng để tạo ra password cho file upxflag2c1.exe

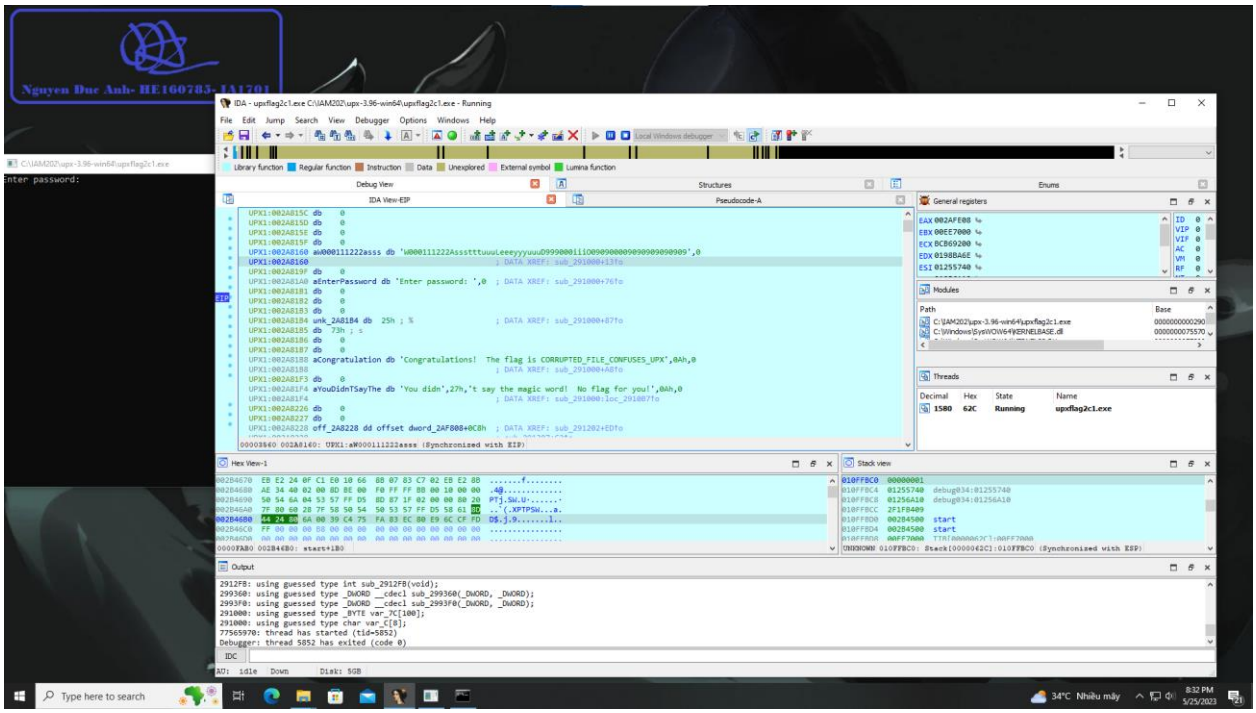
Ta thấy code if (sub_299360(v4, v5)) đây là câu lệnh so sánh giữa 2 biến v4 và v5

Nếu v4 giống v5 thì nó đúng và hiển thị ra flag còn không thì không hiển thị vậy nhiệm vụ của ta là đi tìm v5

```
sub_2993F0(v3, aW000111222asss);
for ( i = 0; i < 5; ++i )
  v5[i] = v3[10 * i];
v5[5] = 0;
```

Ở đây ta thấy được v5 được tạo ra từ biến v3 là một chuỗi String với công thức 10* i

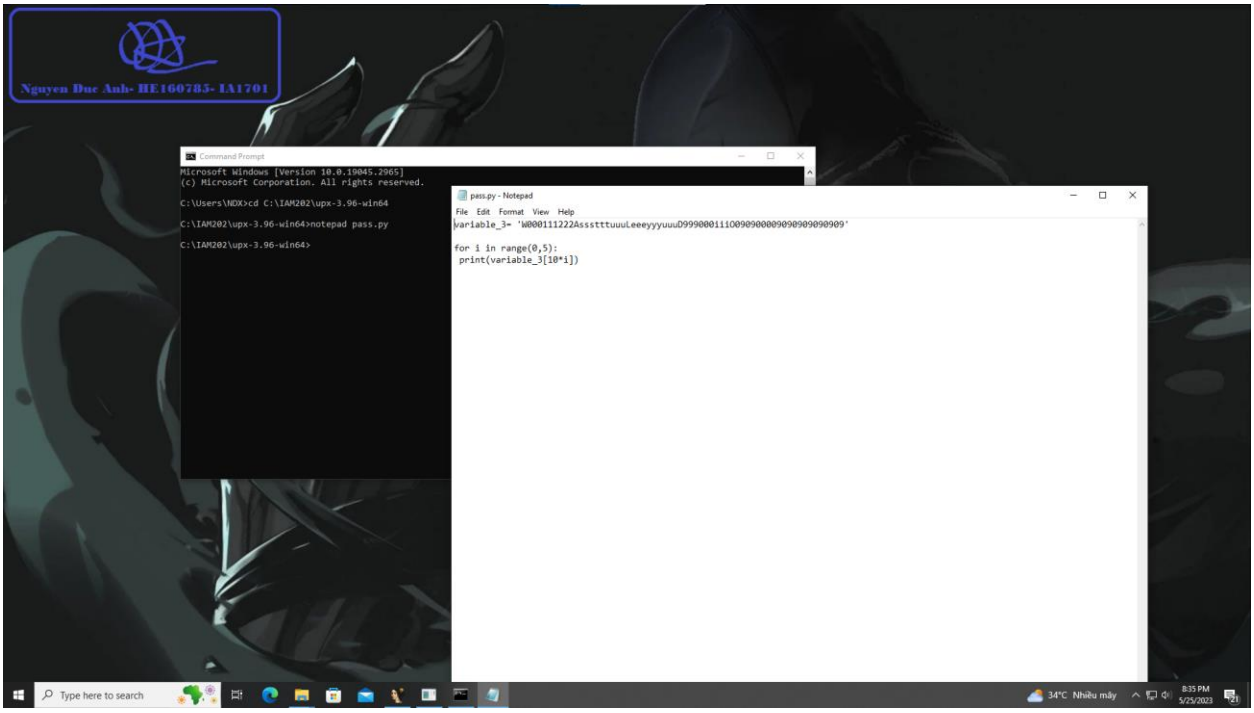
Mà v3 đang được trỏ đến aW000111222asss nên ta nó đang nằm ở đâu



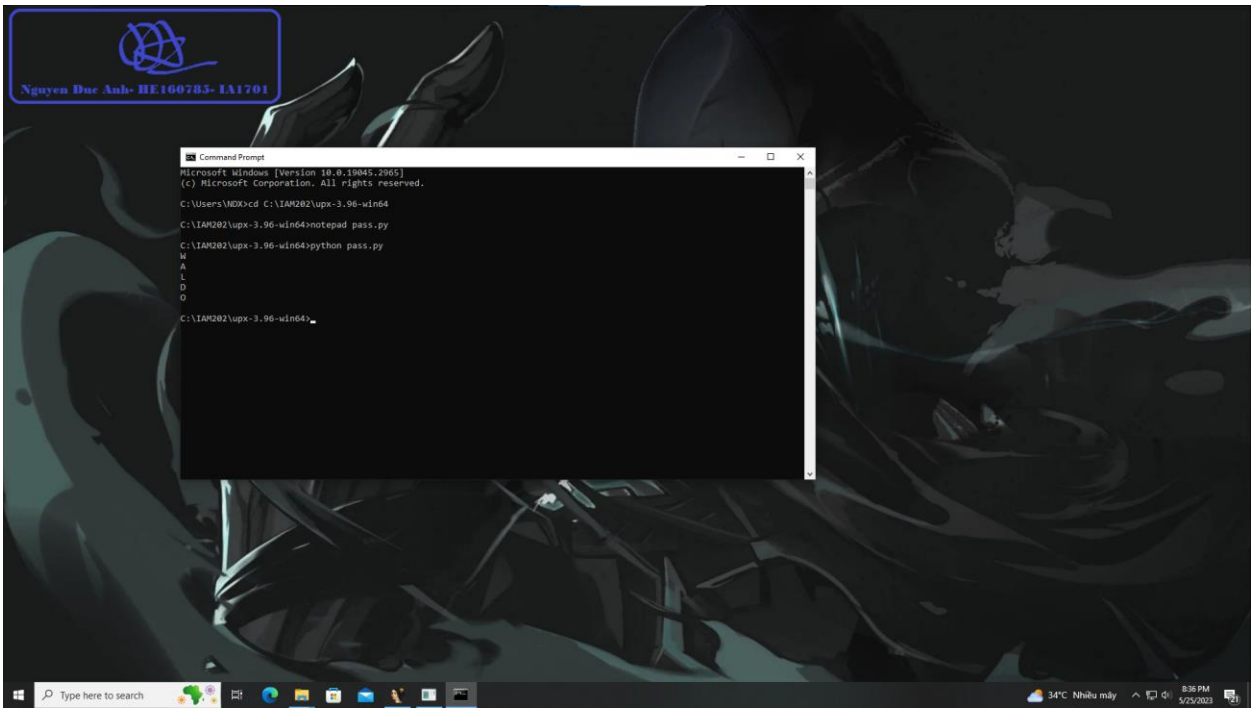
Vậy đây là biến v3 của file upxflag2c1.exe là W000111222AsssttuuuLeeeyyyuuuD999000iiiO0909000090909090909

Và ở ngay dưới ta có thể nhìn thấy luôn flag của file là CORRUPTED_FILE_CONFUSES_UPX

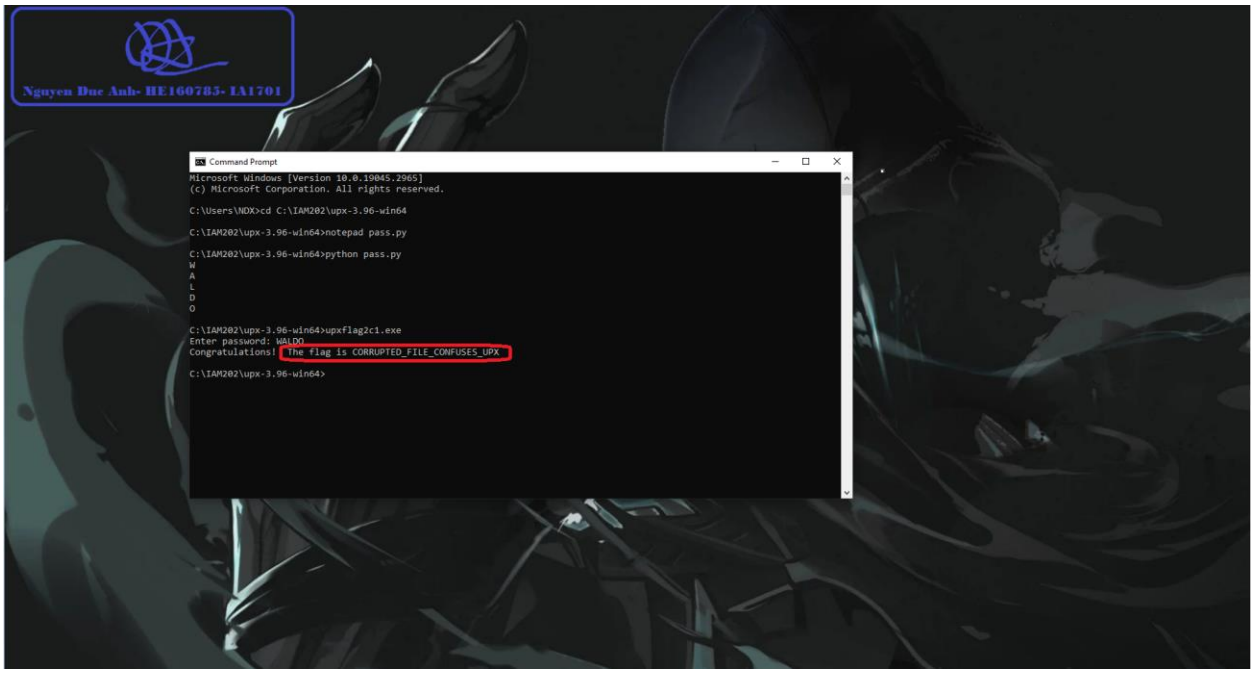
Giờ từ công thức và biến v3 cho sẵn ta sẽ đi tìm ra v5 bằng một file python có code như hình dưới đây



Giờ ta sẽ chạy file Python



File Python in ra password là “WALDO” việc chúng ta cần làm bây giờ là kiểm tra xem password này có đúng hay không



Với password đúng ta đã tìm ra được flag của bài là CORRUPTED_FILE_CONFUSES_UPX