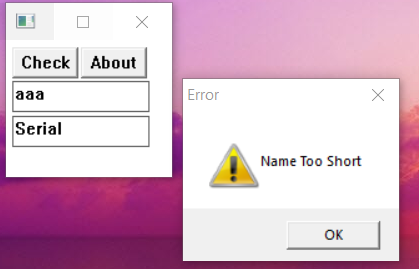
Ta mở chương trình 3\_3.exe

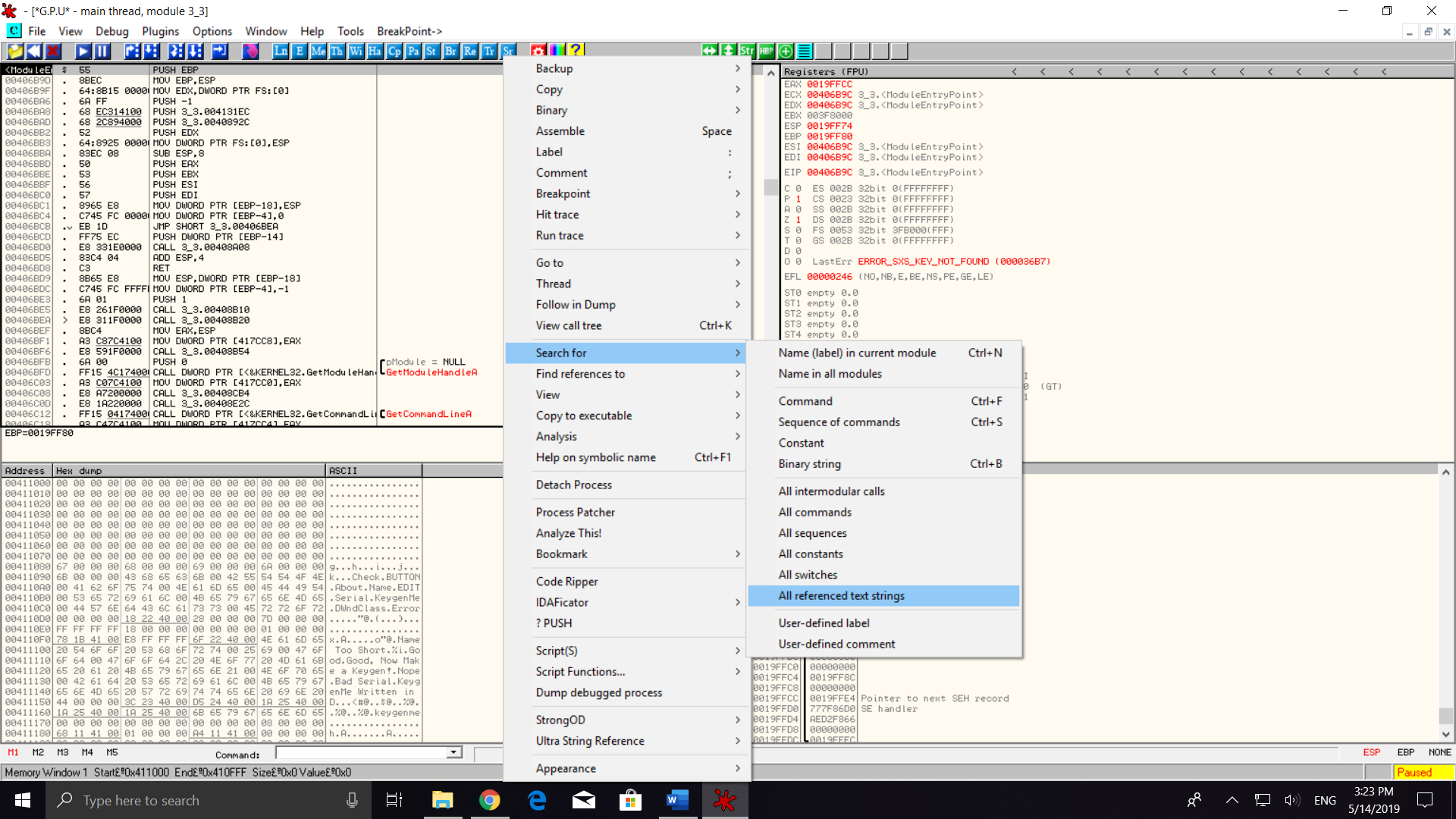
Chạy với một user và serial bất kỳ ta thấy

Hình dưới ta thấy với user là aaa hiện ra lỗi error Name Too Short

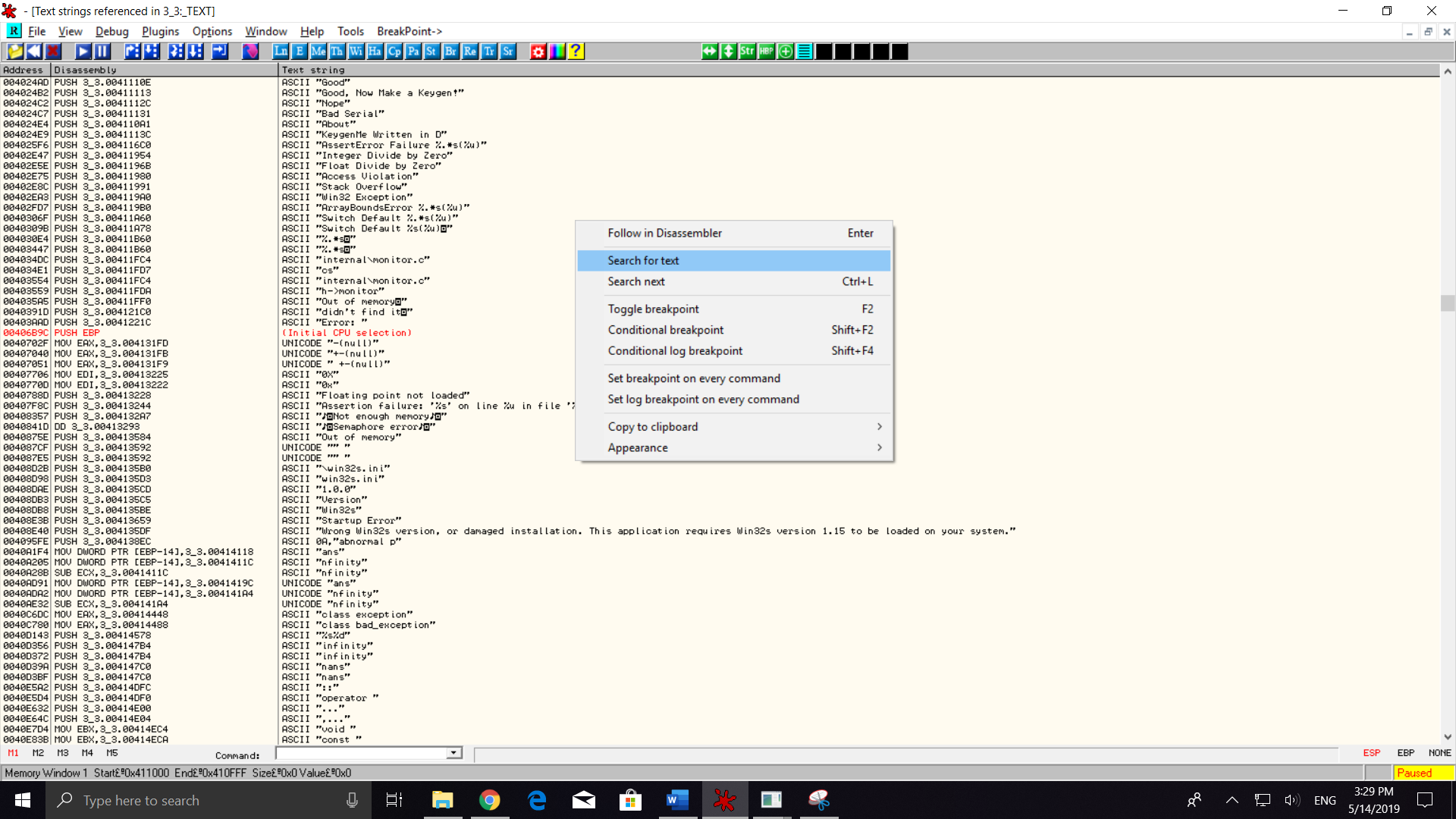


Mở OllyDbg lên

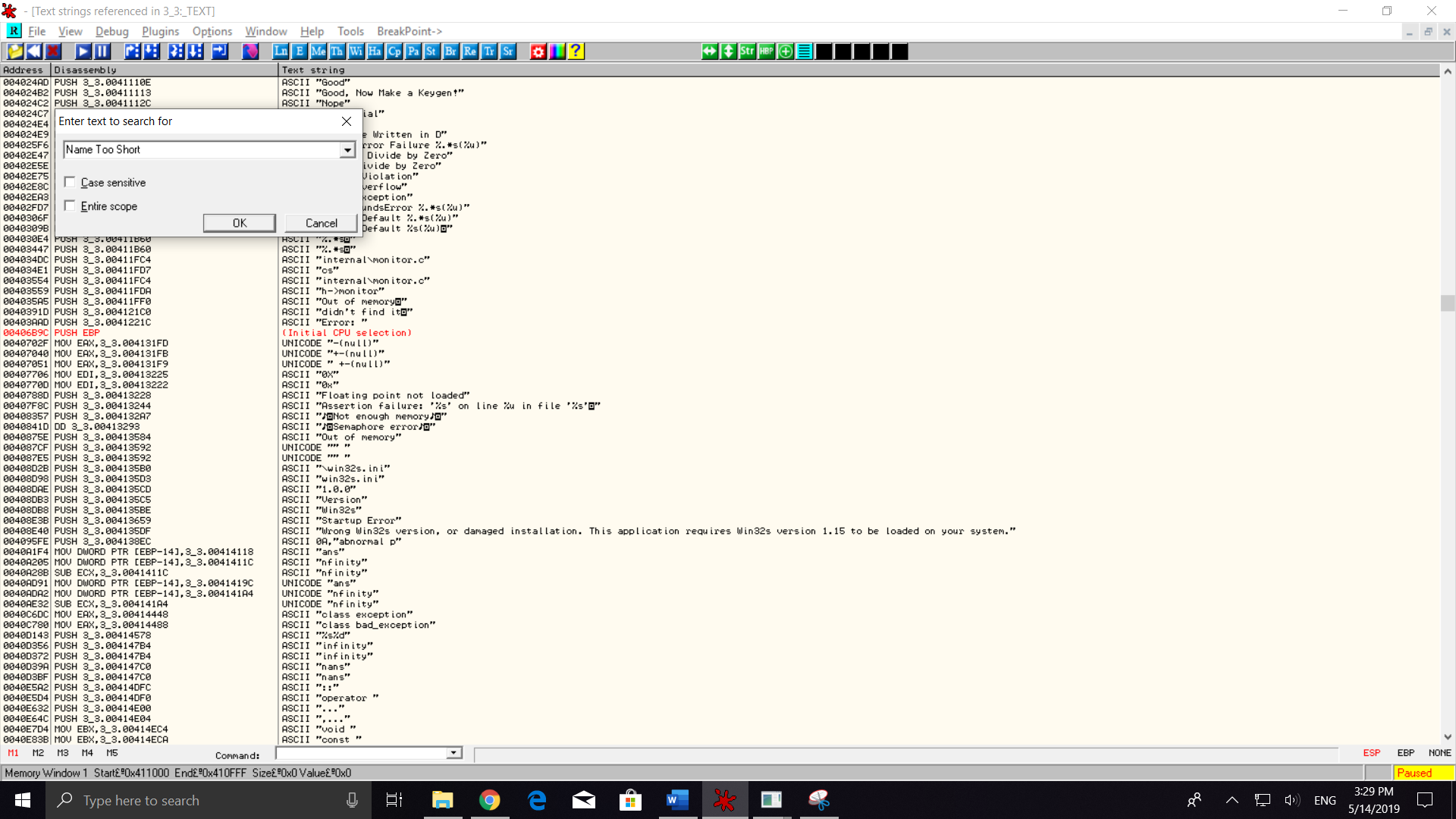
Chuột phải chọn Search for\All referencer text strings



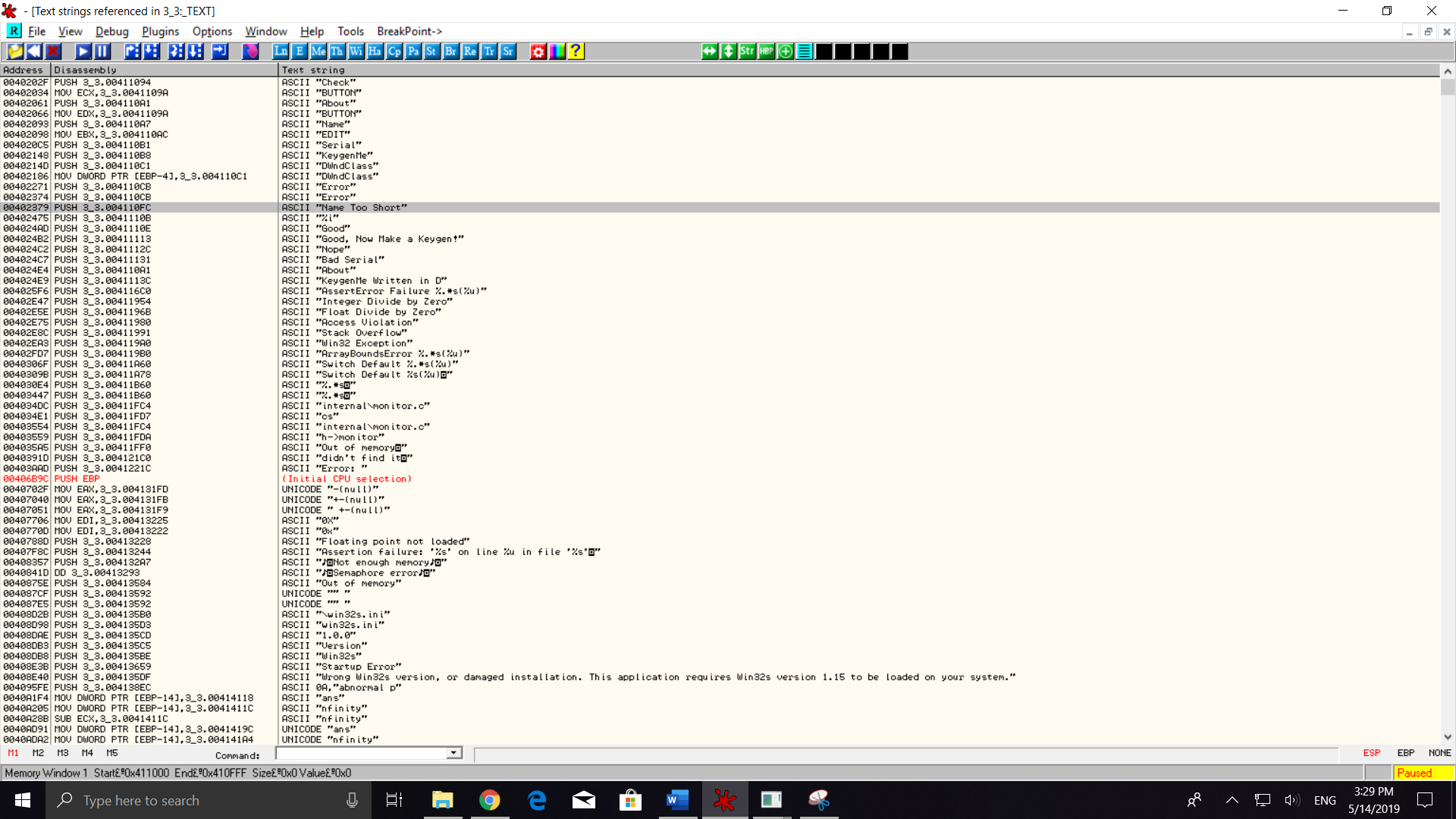
Ta nhấn chuột phải vào bảng chọn Search for text



Tìm kiếm với từ khoá là Name Too Short



nhấn dúp vào đó



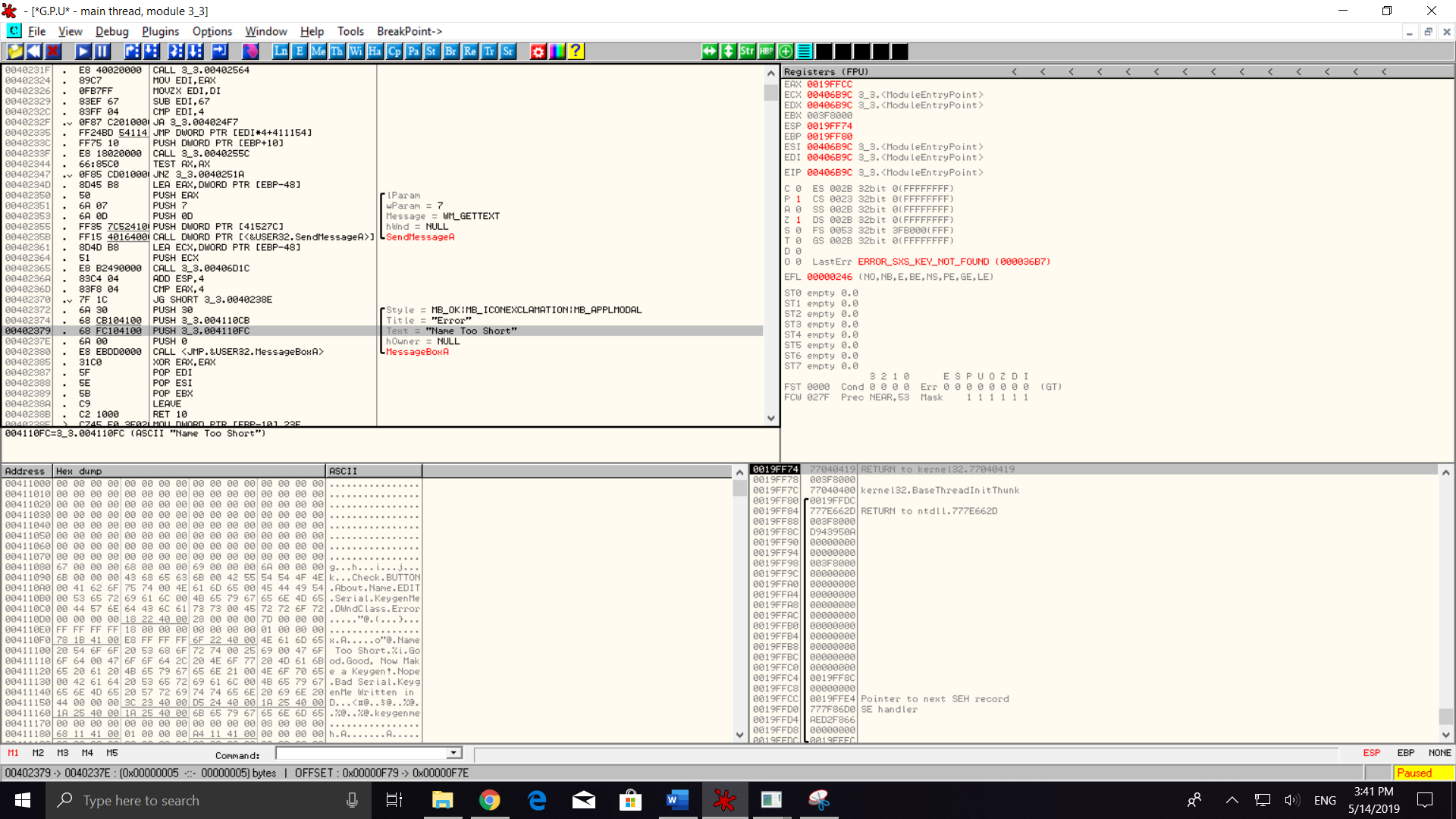
Ta tiềm kiếm các mã trên và thấy đoạn mã

0040236D CMP EAX,4

00402370 JG SHORT 3\_3.0040238E

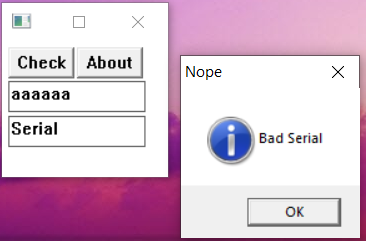
Ta thấy lệnh so sánh CMP nó sẽ nhãy tới 0040238E khi EAX < 4

Vậy tức là user phải có hơn 4 ký tự

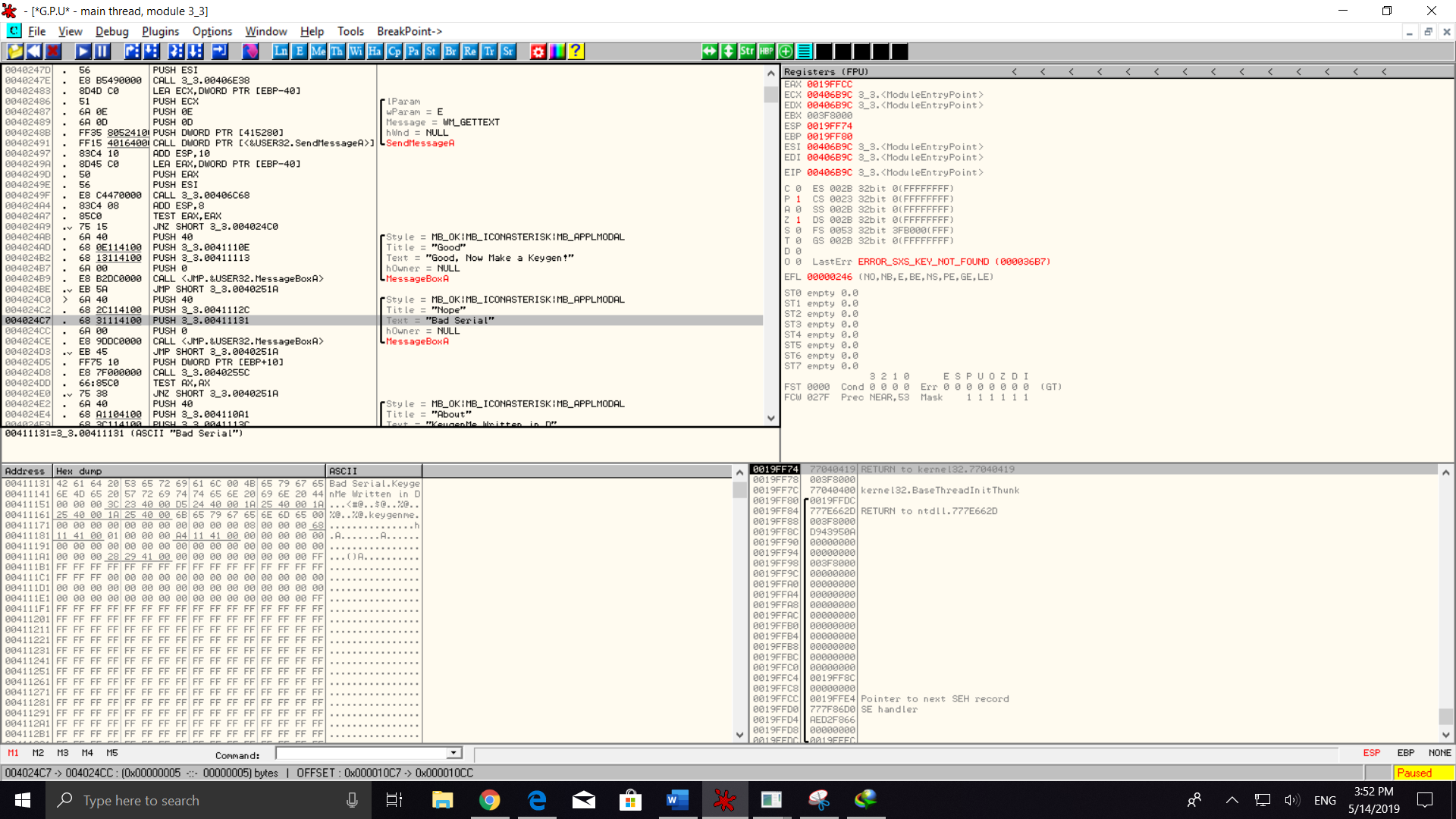


Ta check lại với dòng user là aaaaaa

T thấy hiện ra bản nope

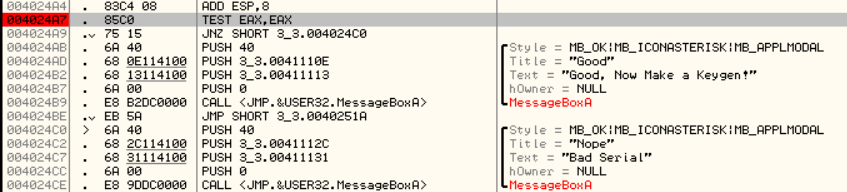


Mở OllyDbg lên và tiềm kiếm từ khoá Bab Serial



thấy lệnh nhảy JNZ tới địa chỉ 004024C0

set breakpiont dòng đó là F9 chạy chương trình

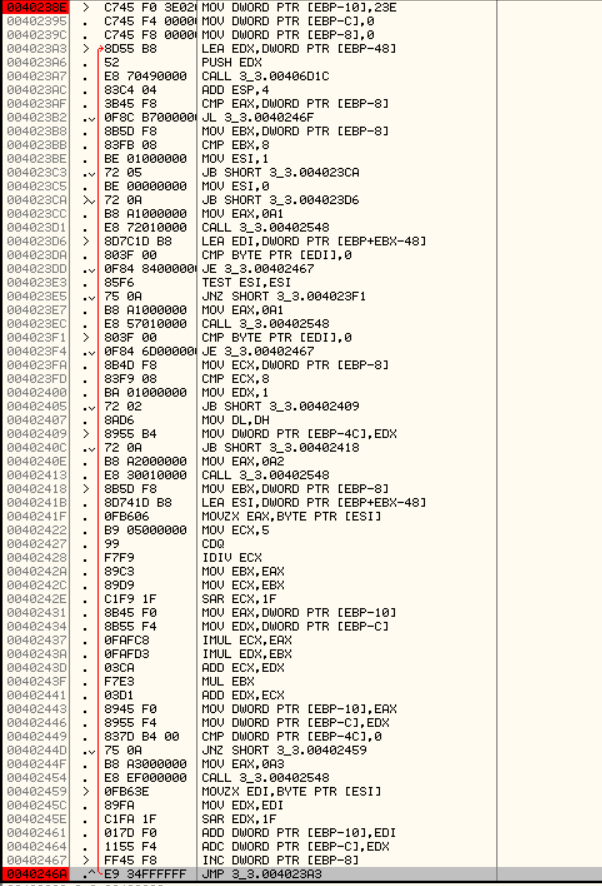


T thấy dóng ECX là key tương ừng với user aaaaaa

Và Serial là key ta nhập lúc nãy

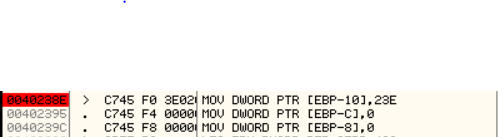


Tìm kiếm gần đó và ta thấy được đoạn code về tạo key từ user



Giải thích đoạn mã

Tạo biến khởi đầu cho vòng lặp



DWORD PRT [EBP-8] là i

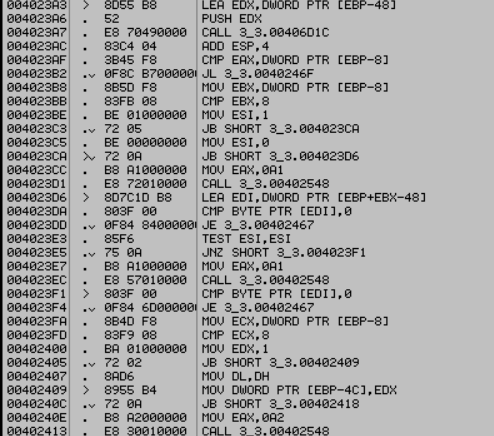
Lấy chuổi từ user người dùng nhập vào

Lấy phần tử đầu của chuổi gán vào ESI

Xoá phần từ vừa lấy ra từ chuổi user

EAX là độ dài của chuổi (4<EAX<=6)

Lệnh CMP EAX,DWORD PTR [EBP-8] (thoát khỏi vòng lắm khi i=EAX)

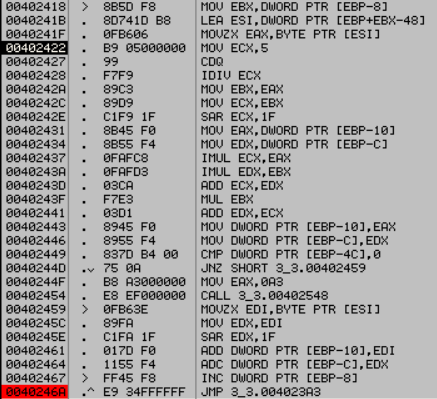


Gán EBX=i

ESI= chuổi sau khi tách phần tử đầu

EAX = ký tự vừa lấy ra từ user

ECX = 5



IDIV ECX là EAX=EAX / ECX

(ví dụ như user aaaaaa, EAX= 61 theo mã ascii hệ 16

Phép chia ở hệ 16 thì 61 / 5 = 13)

Gán EBX=EAX , ECX=EBX

SAR ECX,1F (dịch ECX sang phải 31 bit)

Gán EAX = DWORD PRT [EPB-10]

Gán EDX = DWORD PRT [EPB-C]

IMUL ECX,EAX (ECX=ECX\*EAX)

IMUL EDX,EBX (EDX=EDX\*EBX)

ADD ECX,EDX (ECX=ECX+EDX)

MUL EBX (EAX=EAX\*EBX)

ADD EDX,ECX (EDX=EDX+ECX)

Lưu EAX vào DWORD PTR [EBP-10]

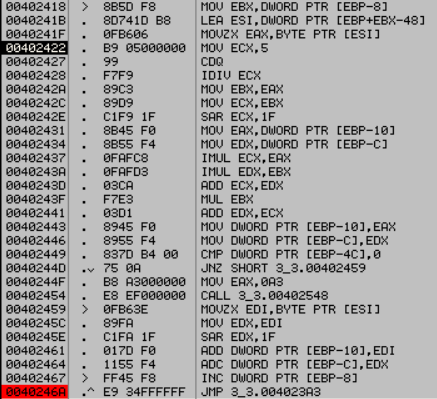
Lưu EDX vào DWORD PTR [EBP-C]

MOVZX EDI,BYTE PTR [ESI] gán EDI = ký tự đầu chuổi ESI

MOV EDX,EDI (địa chỉ EDX= EDI)

dịch EDX sang phải 31 bit sau đó Lưu vào EBP-C

[EBP-10]= [EBP-10]+EDI



Tăng biến đếm i++

Quay lại vòng lặp

