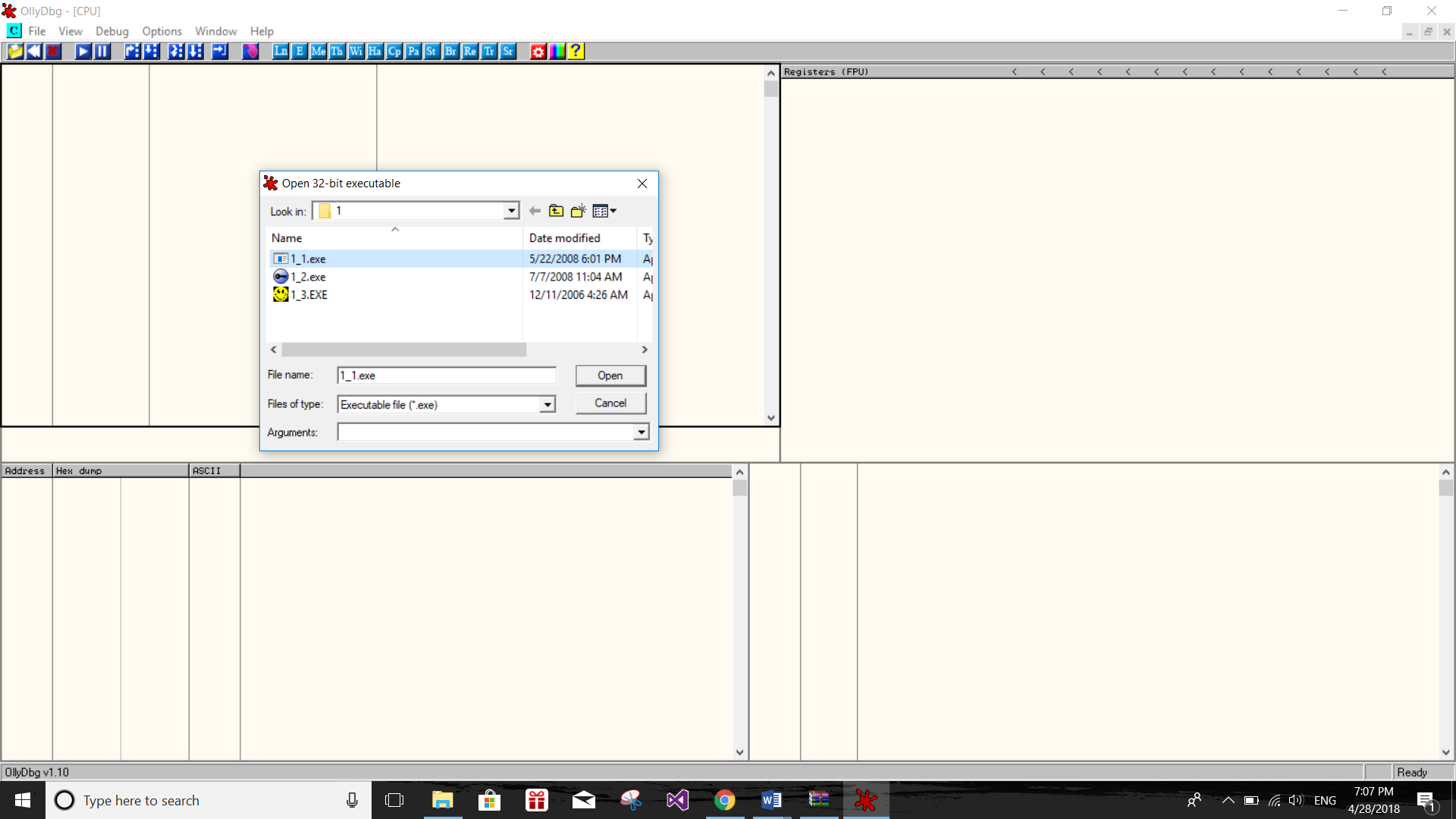
Báo cáo đồ án file 1.1 đề 1.

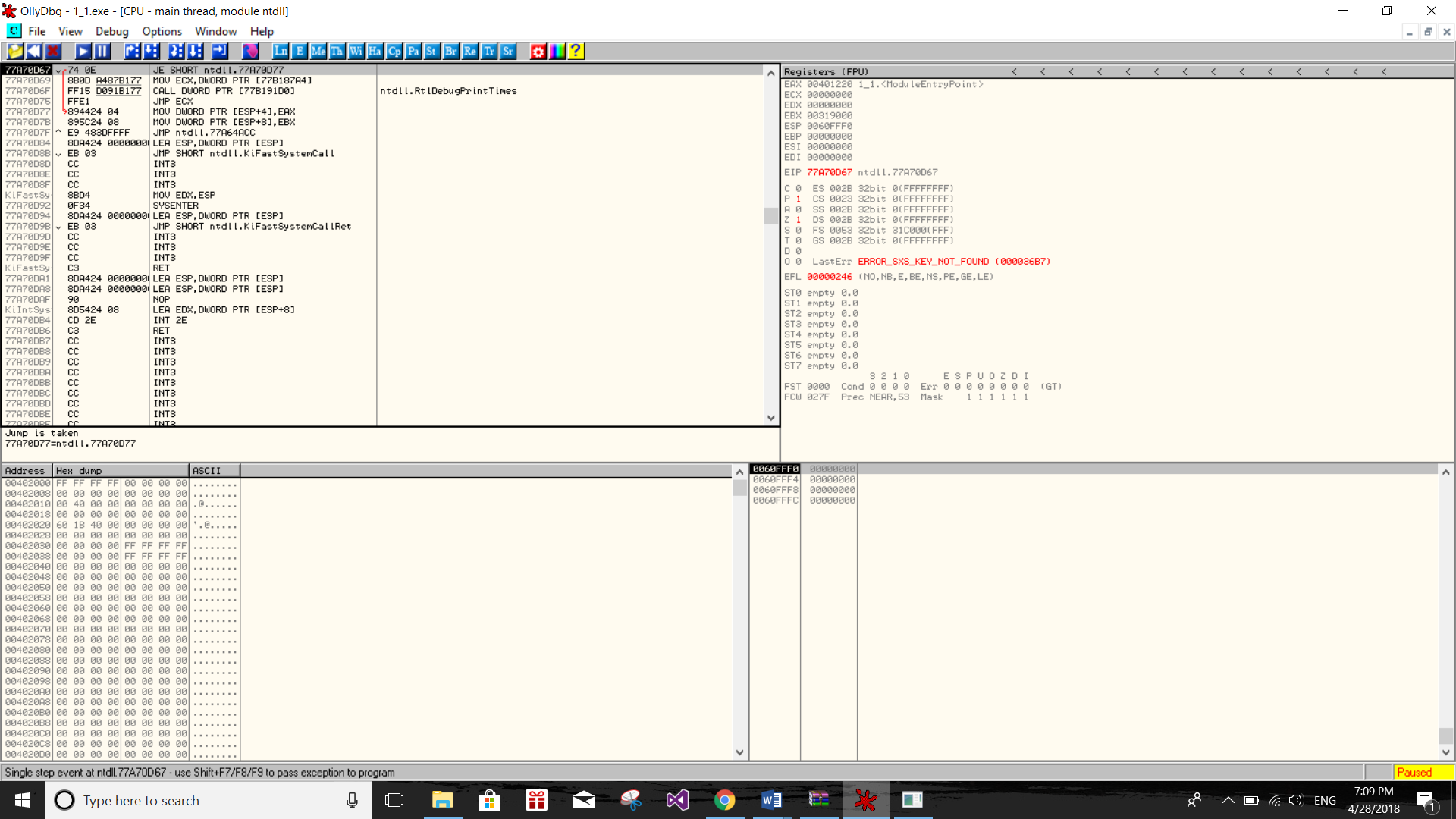
Sử dụng phần mềm OLLDBG để thực hiện quá trình Crack phân mềm.

Bước 1: Load phần mềm cần Crack để lấy Key.

File 🡪 Open 🡪 ( tìm đến địa chỉ lưu phần mềm cần Crack)



Bước 2: Sau khi Load phần mềm sẽ có giao diện như hình.



**5**

**4**

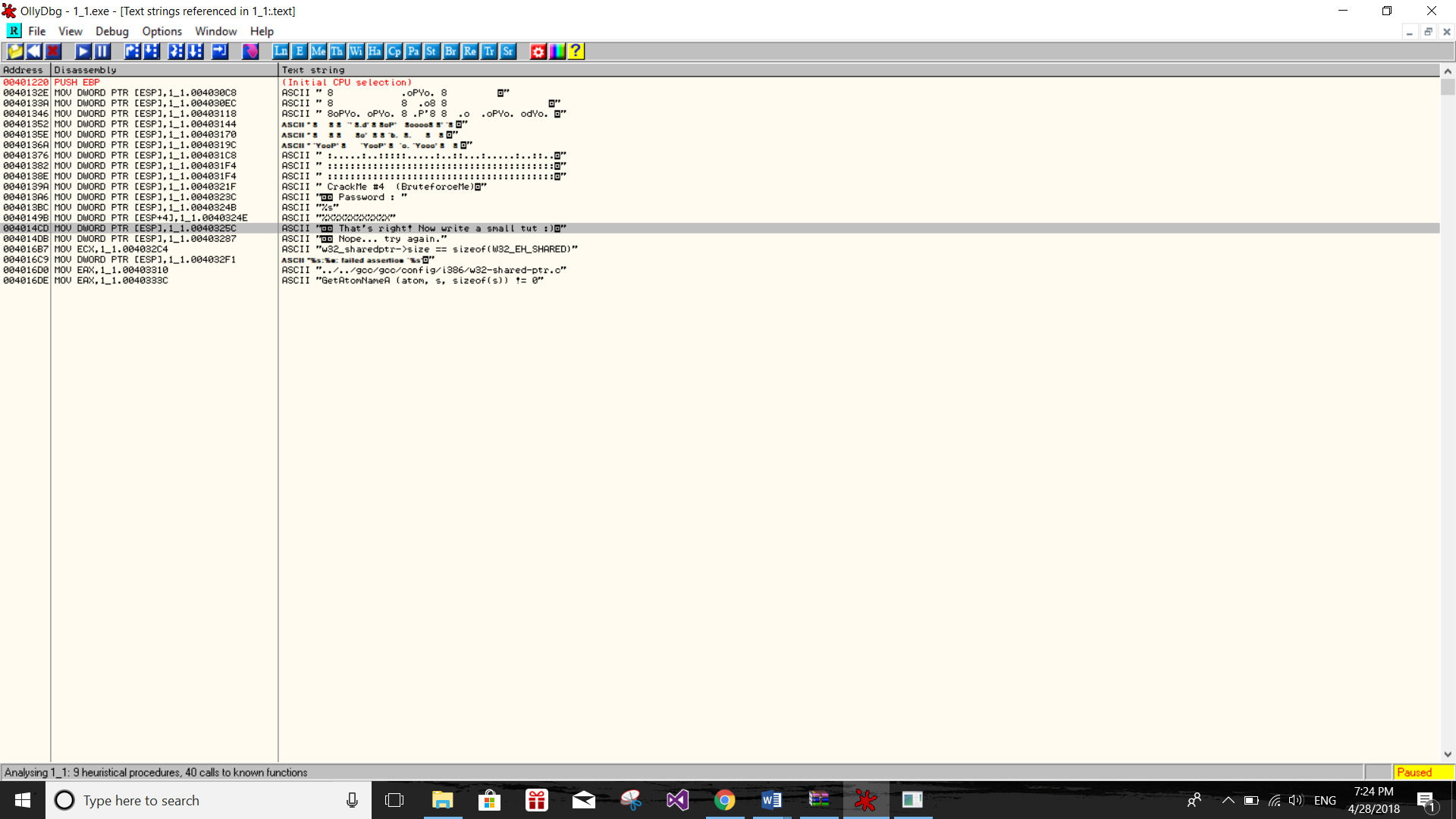
**3**

**2**

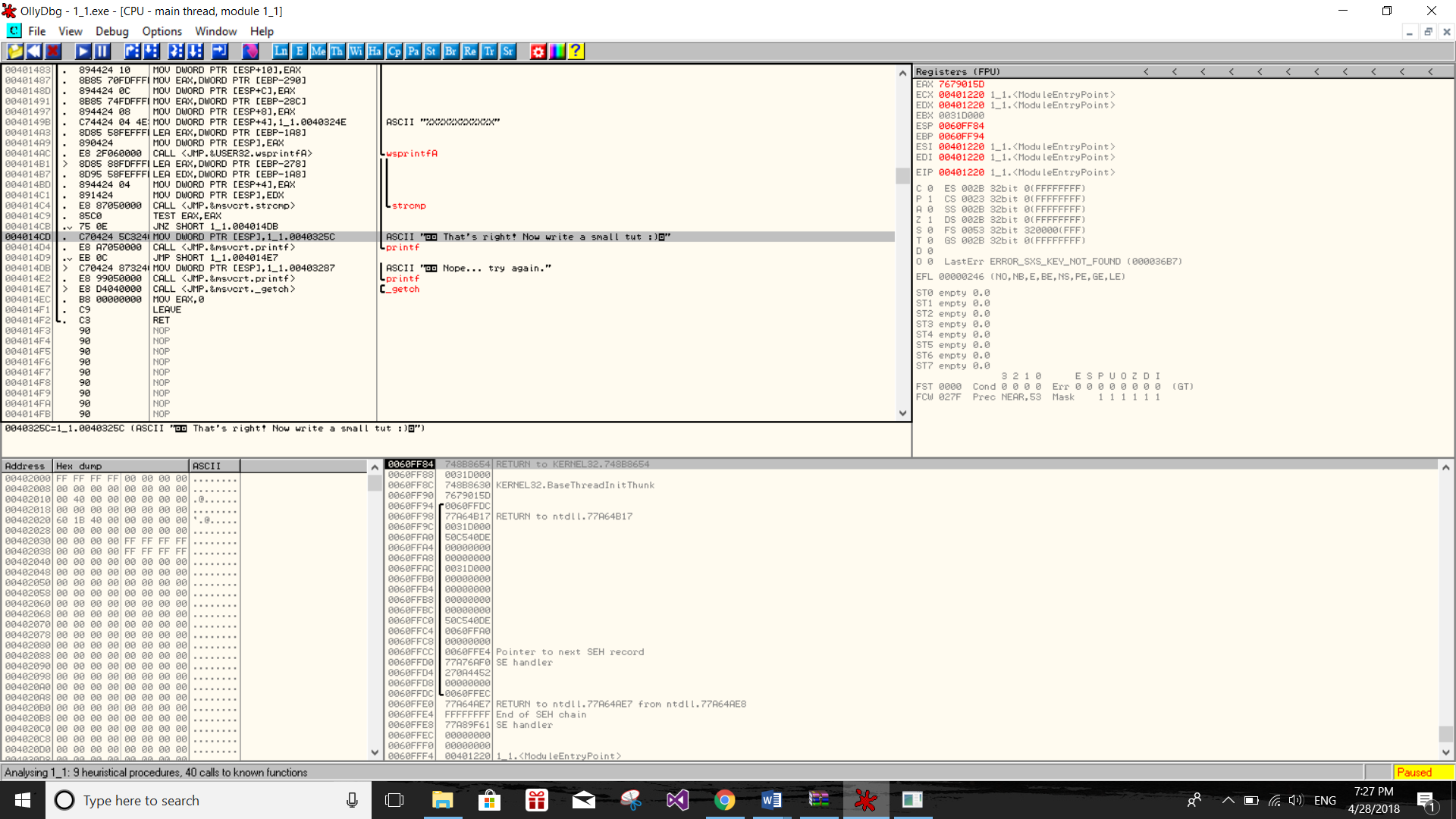
**1**

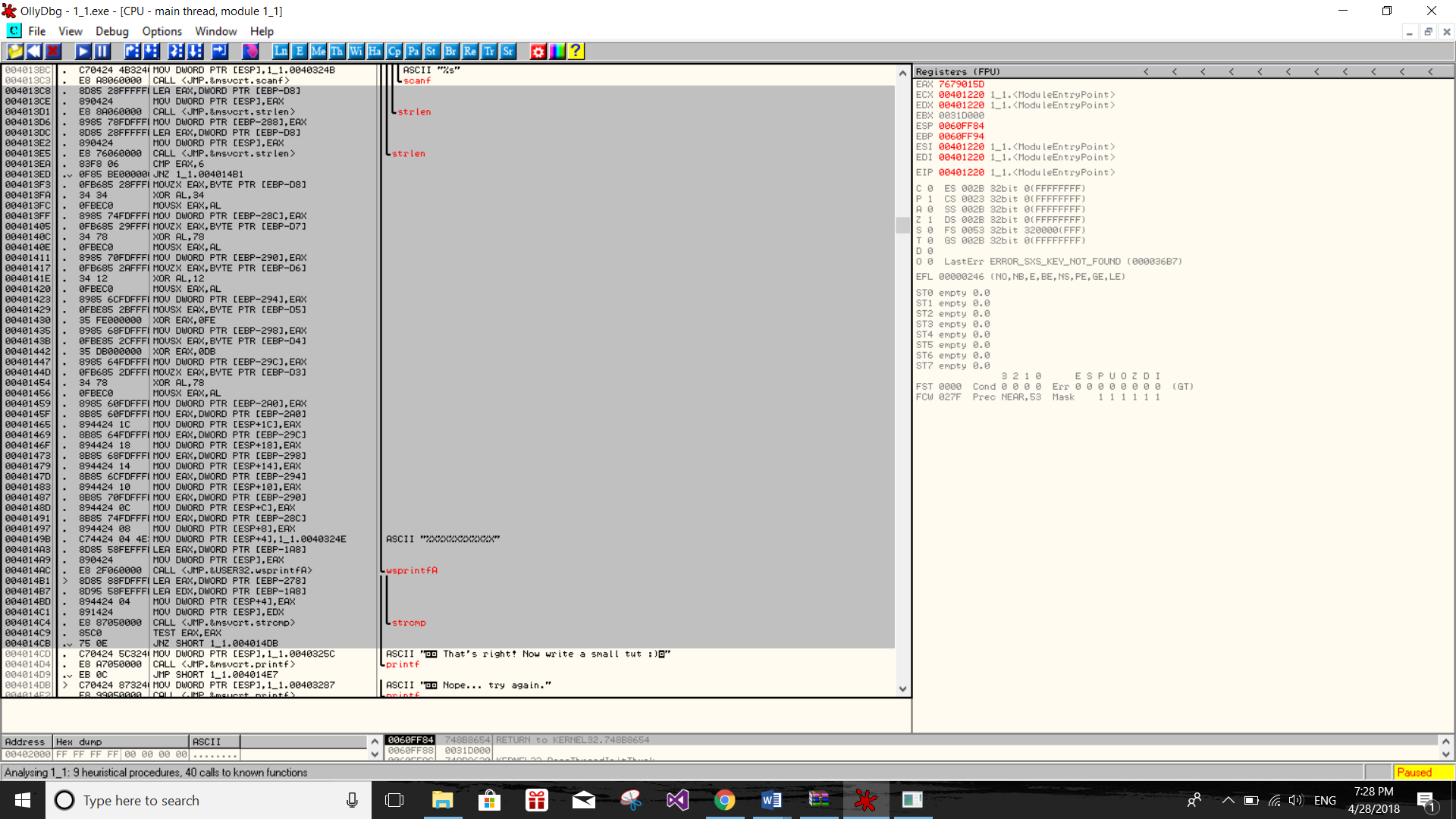
Cửa sổ OllyDBG được chia ra làm 5 cửa sổ con :  
  
1: Disassembler window: Các đoạn mã của chương trình dưới dạng code assembly và các comment tại các dòng code đó.  
2: Register window: Các thanh ghi và giá trị của chúng.  
3: Tip window: Các thông tin bổ sung cho 1 dòng code. Các thông tin này khá hữu ích trong quá trình debug.  
4: Dump window: Cho phép người sử dụng xem và chỉnh sửa các giá trị trong bộ nhớ của chương trình đang được debug.  
5: Stack window: Thông tin về stack của chương trình.

Bước 3: Ta chạy chương trình bằng cách nhấn F9 🡪 nhấn chuột phải vào disassembler window 🡪 chọn Search for 🡪 All referenced text strings



Chọn dòng text tô đậm như trong hình. Sau đó sẽ chuyển đến địa chỉ của dòng text này.

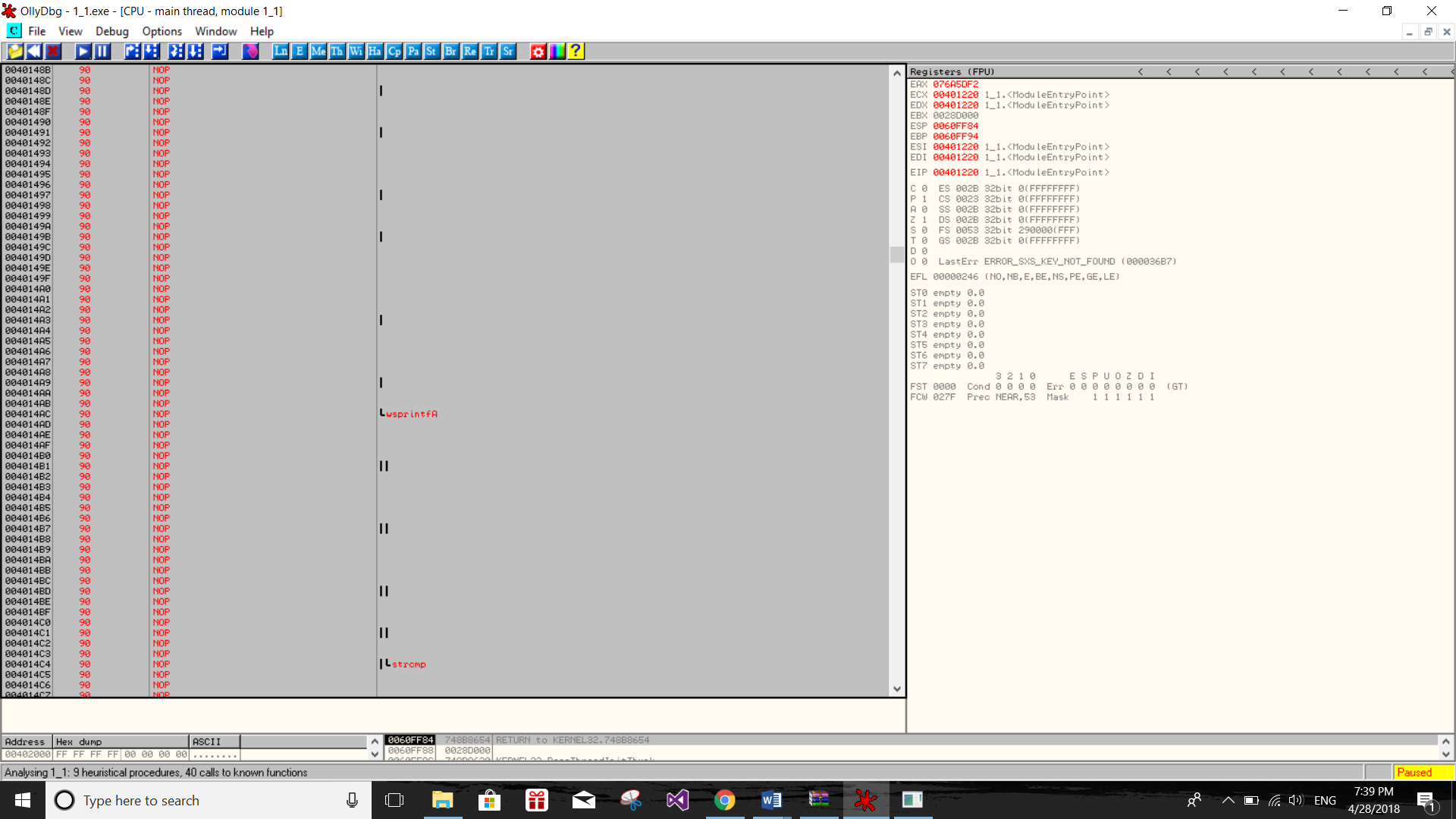




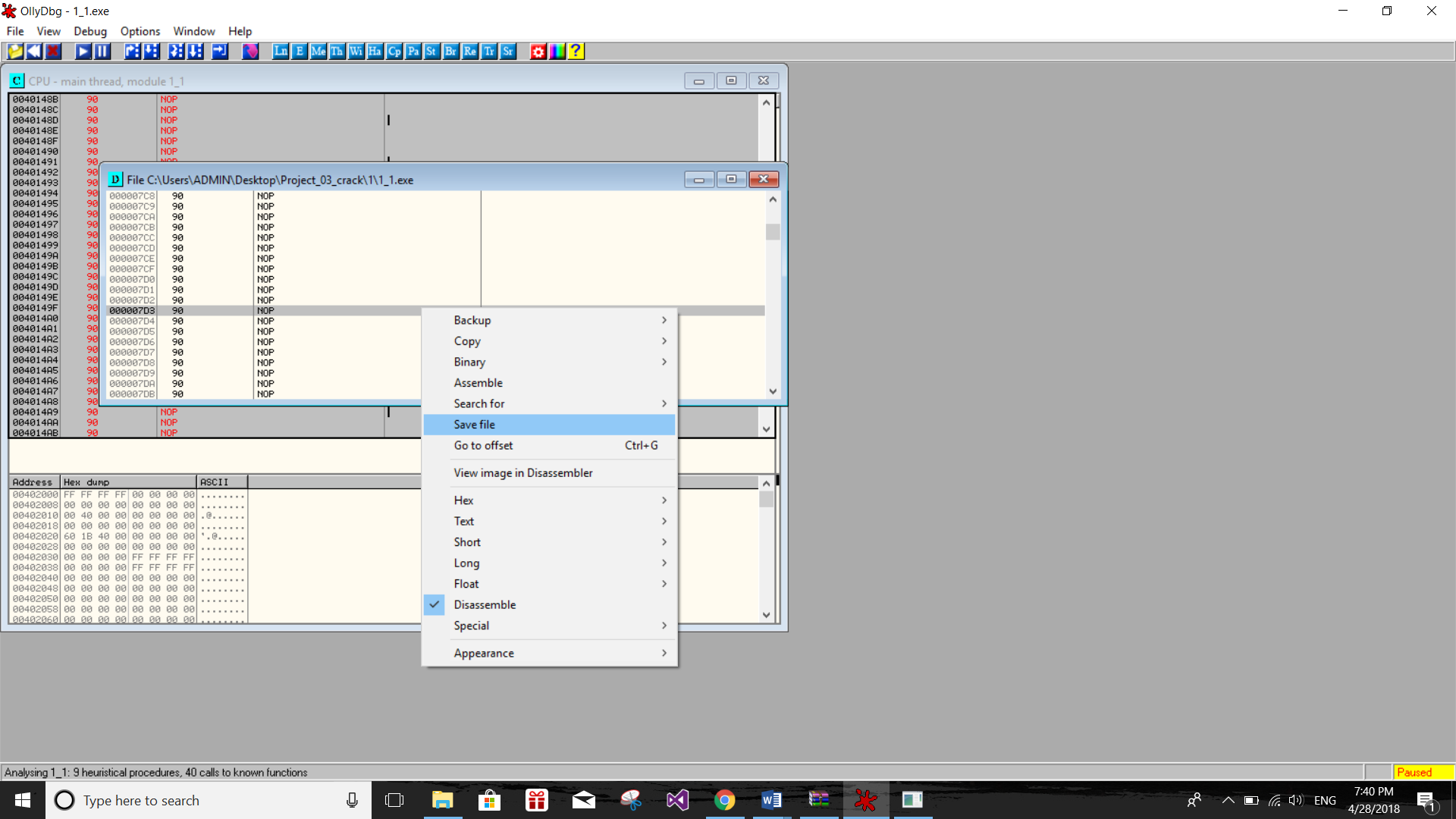
Phần tô đậm trên hình là phần phát sinh key để đăng nhập vào phần mềm.

Ta tiến hành tô đậm và đóng băng đoạn lệnh này để tránh quá trình phát sinh key của phần mềm.

Nhấn chuột phải 🡪 Binary 🡪 Fill with NOPs



Sau đó ta chọn Copy to executable 🡪 Selection.



Sau đó ta lưu lại File vừa crack xong. Nhấn chuột phải 🡪 save file.