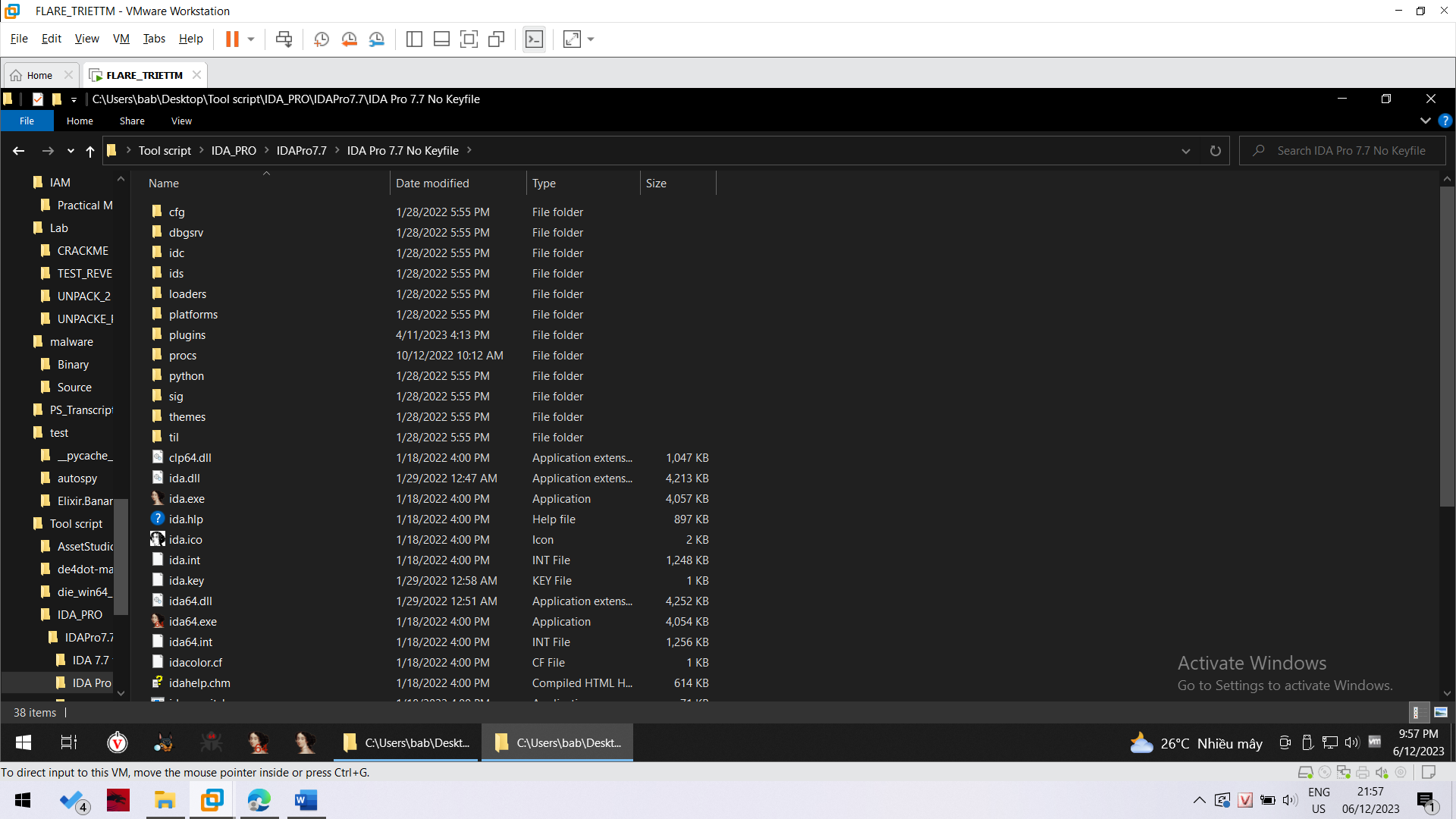
**Lab 9.1: IDA PRO**

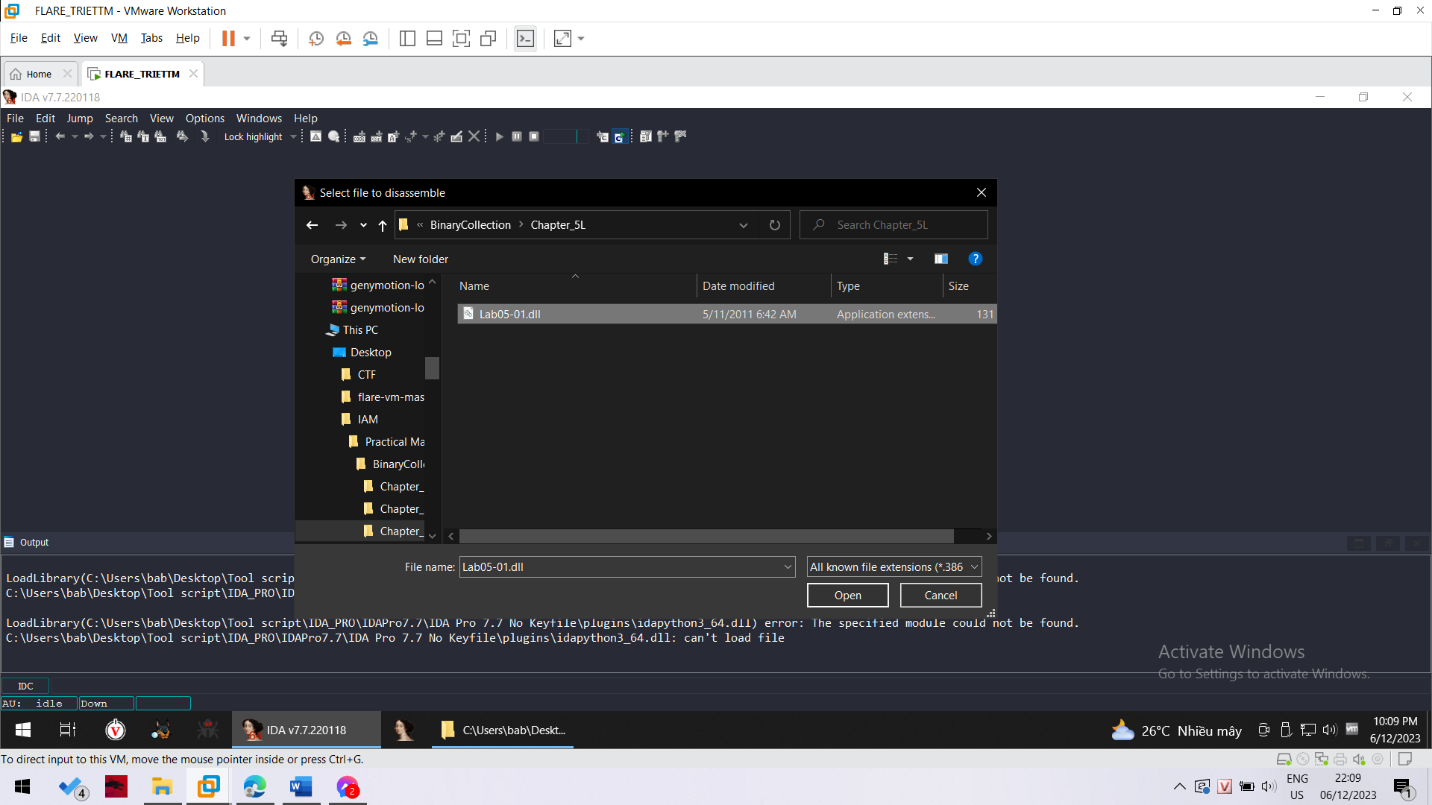
Ở bài lab này chúng ta sẽ thực hành cài đặt IDA rồi sử dụng công cụ IDA này, thử một vài thao tác cũng như chức năng của IDA.



Em đã cài đặt thành công IDA pro.

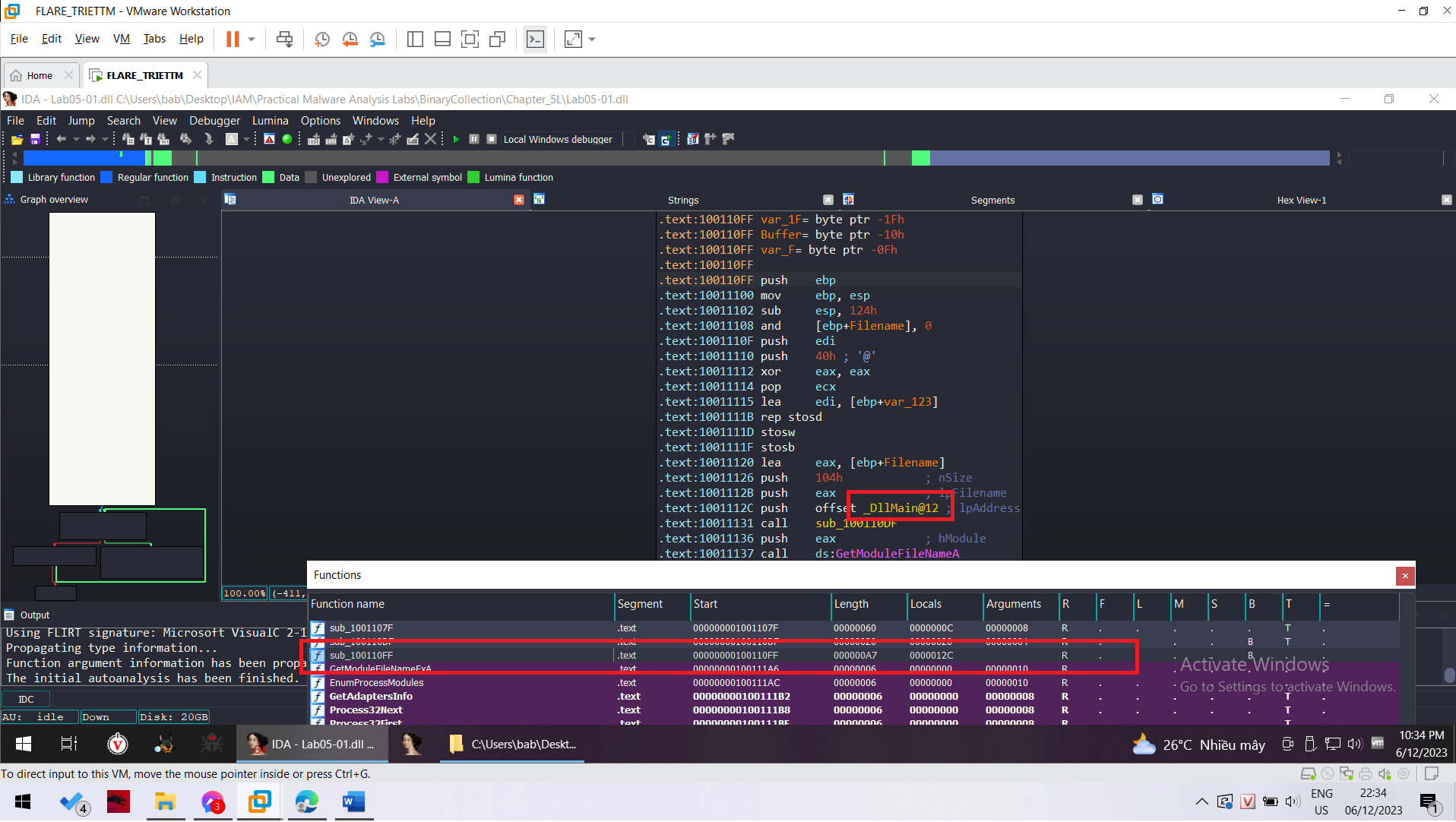
**Opening Lab05-01.dll in IDA Pro**

Bây giờ ta sẽ mở file Lab05-01.dll trong IDA.



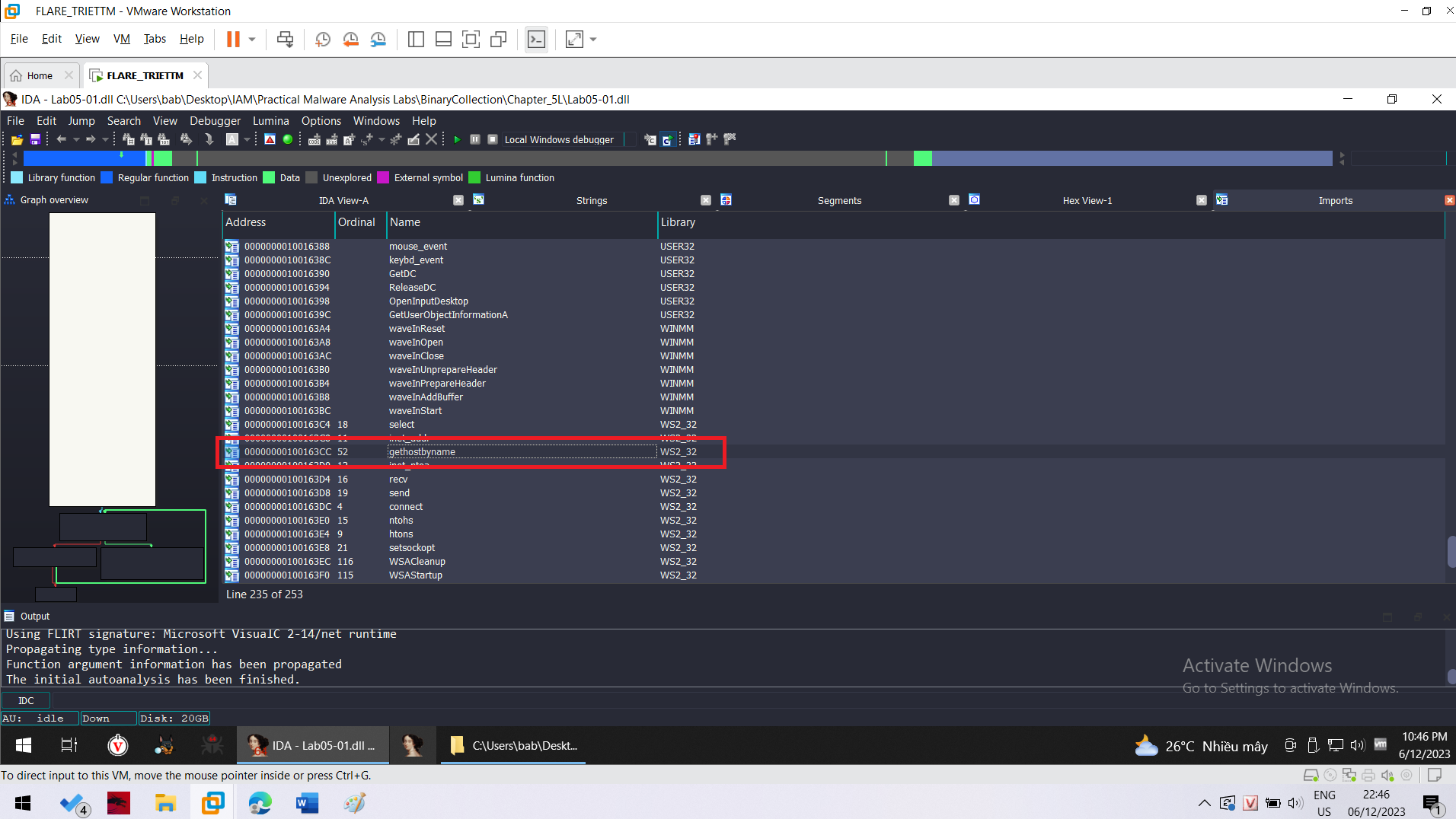
Q 1: Finding the Address of DLLMain

Ta vào View -> Sub view -> Fucntion để xem trọn cửa sổ các hàm của chương trình.



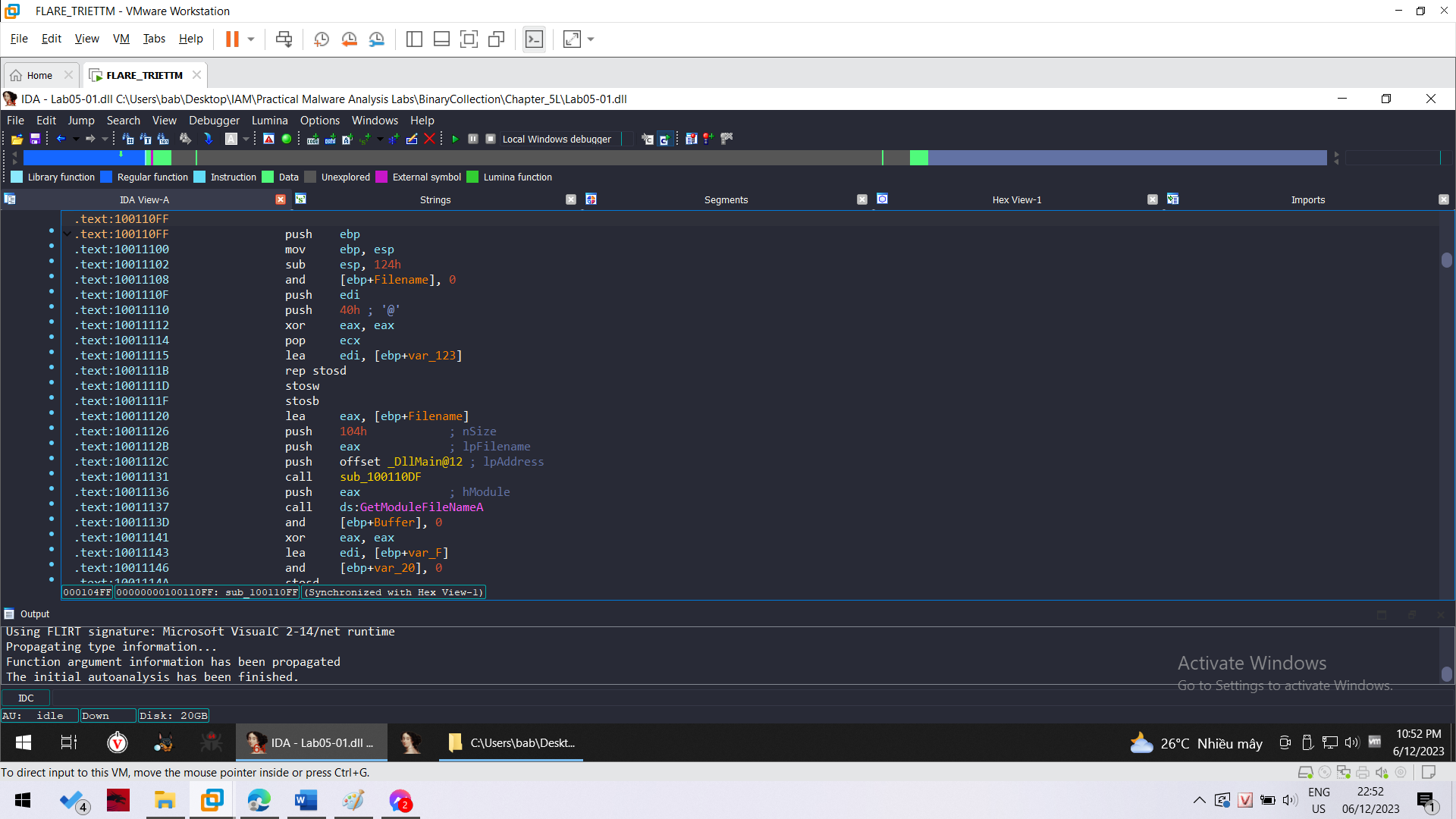
Hàm DLLMain ở địa chỉ 0x100110FF

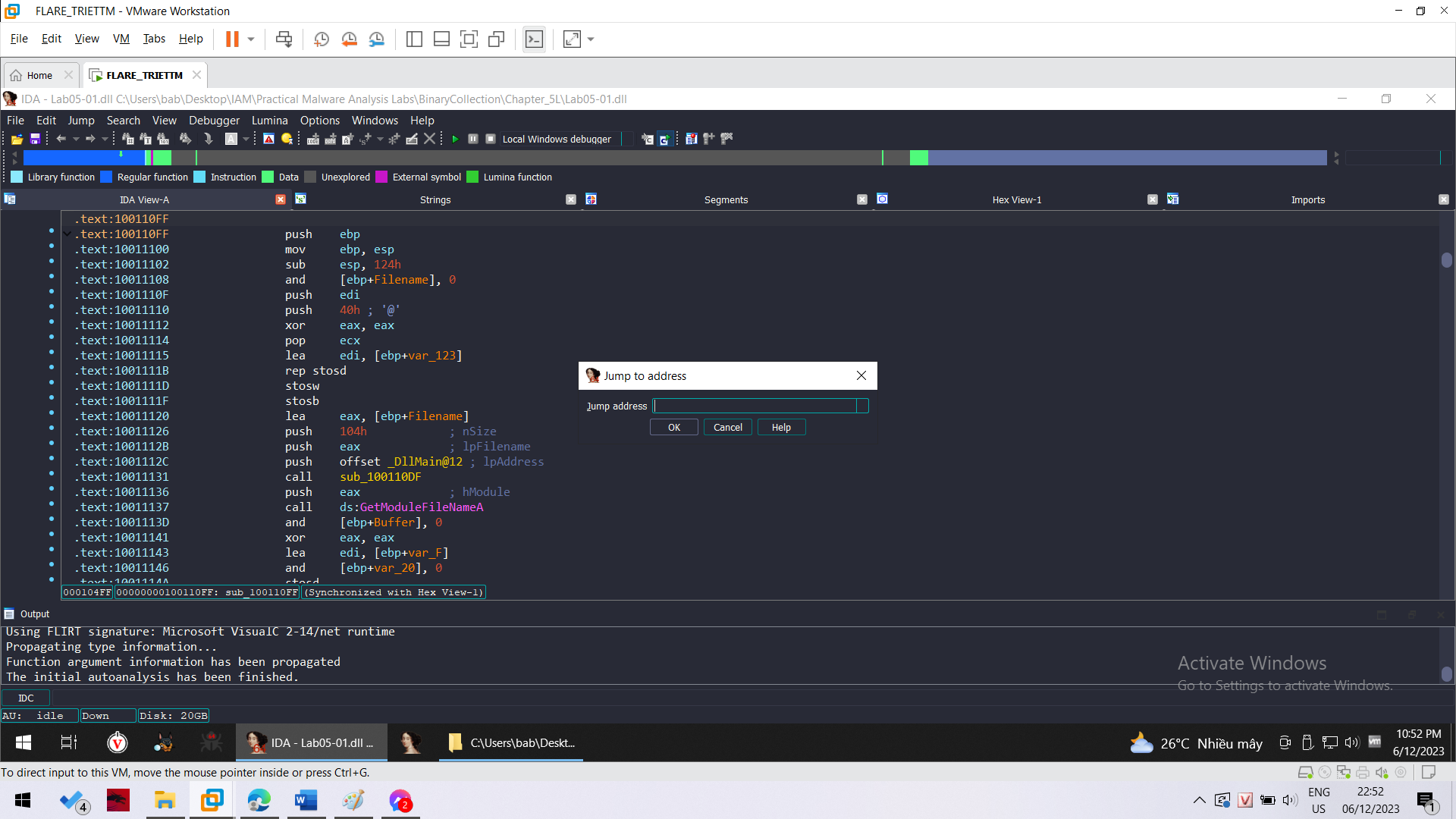
**Q 2: Find the import for gethostbyname**



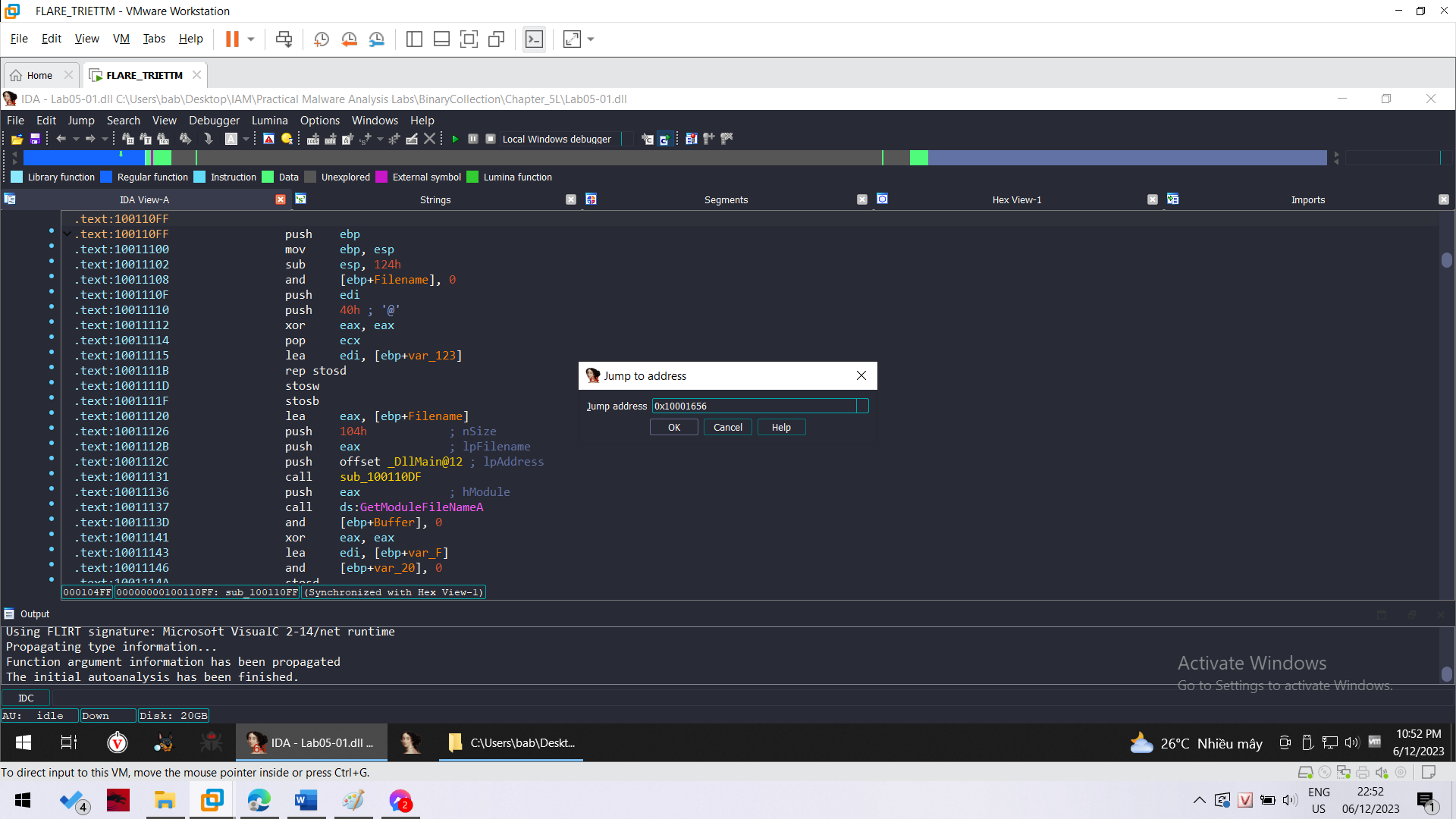
**Q5: Count Local Variables for the Subroutine at 0x10001656**

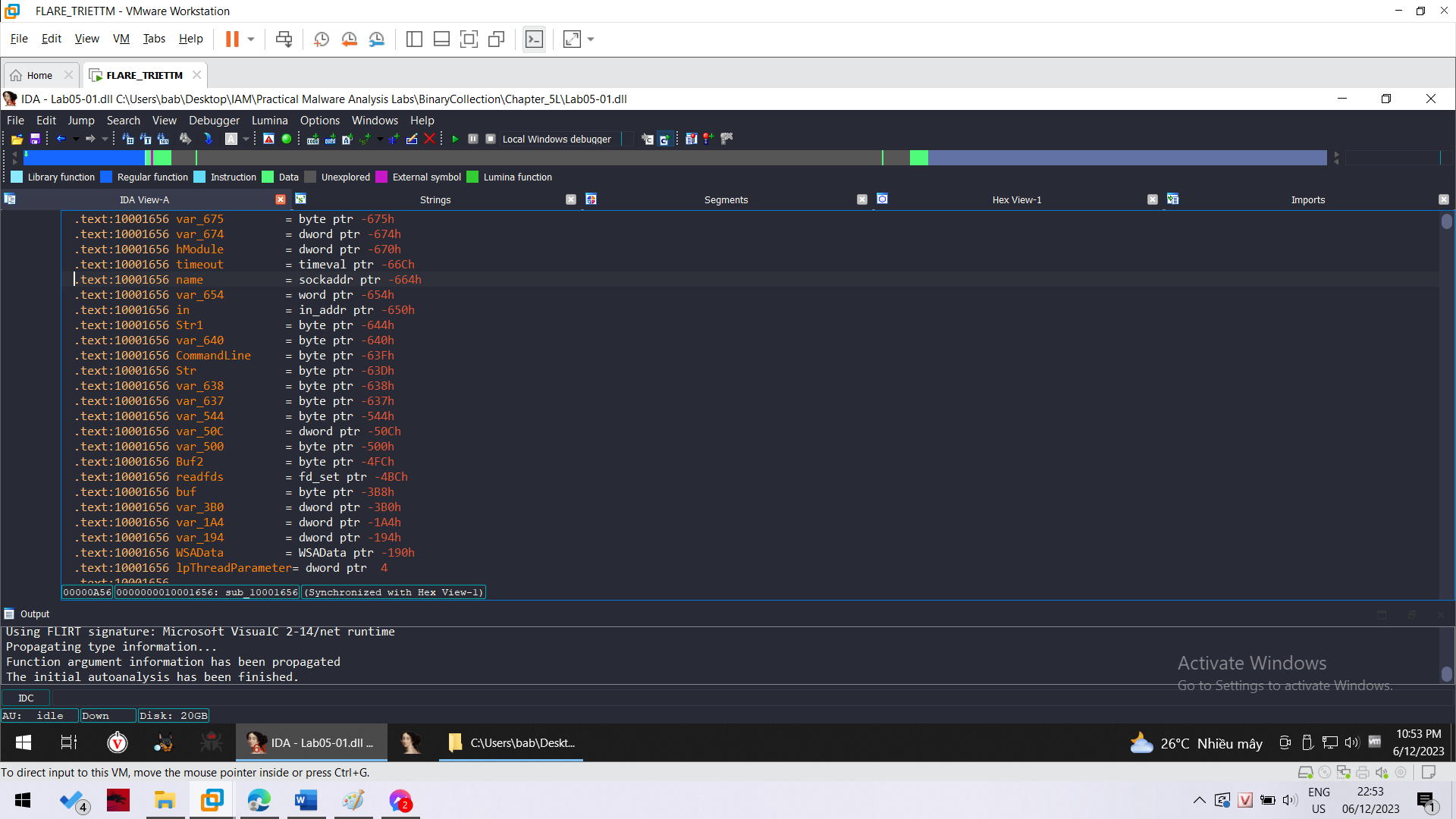
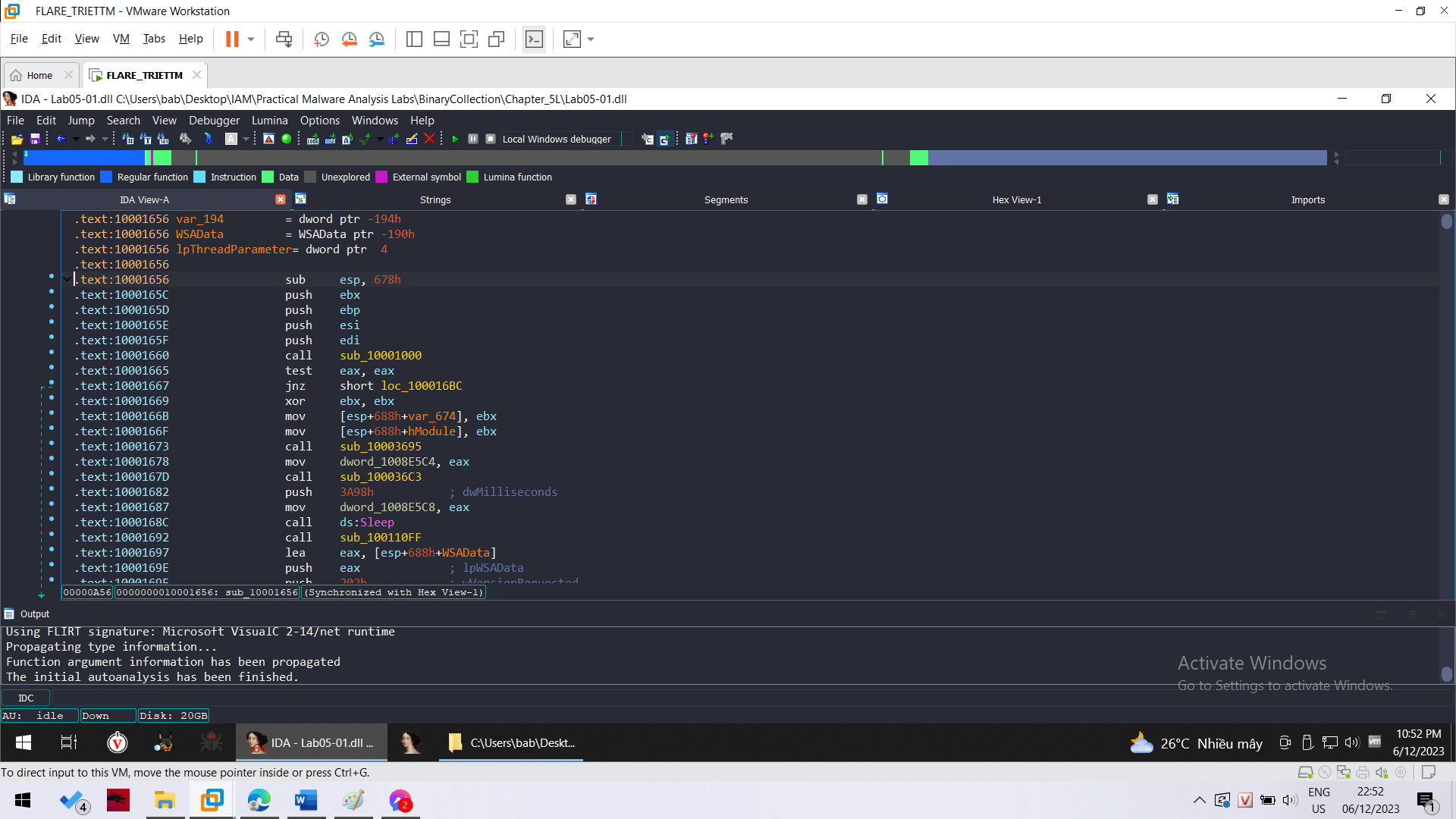
Bấm nút space để chuyển từ graph view sang text view





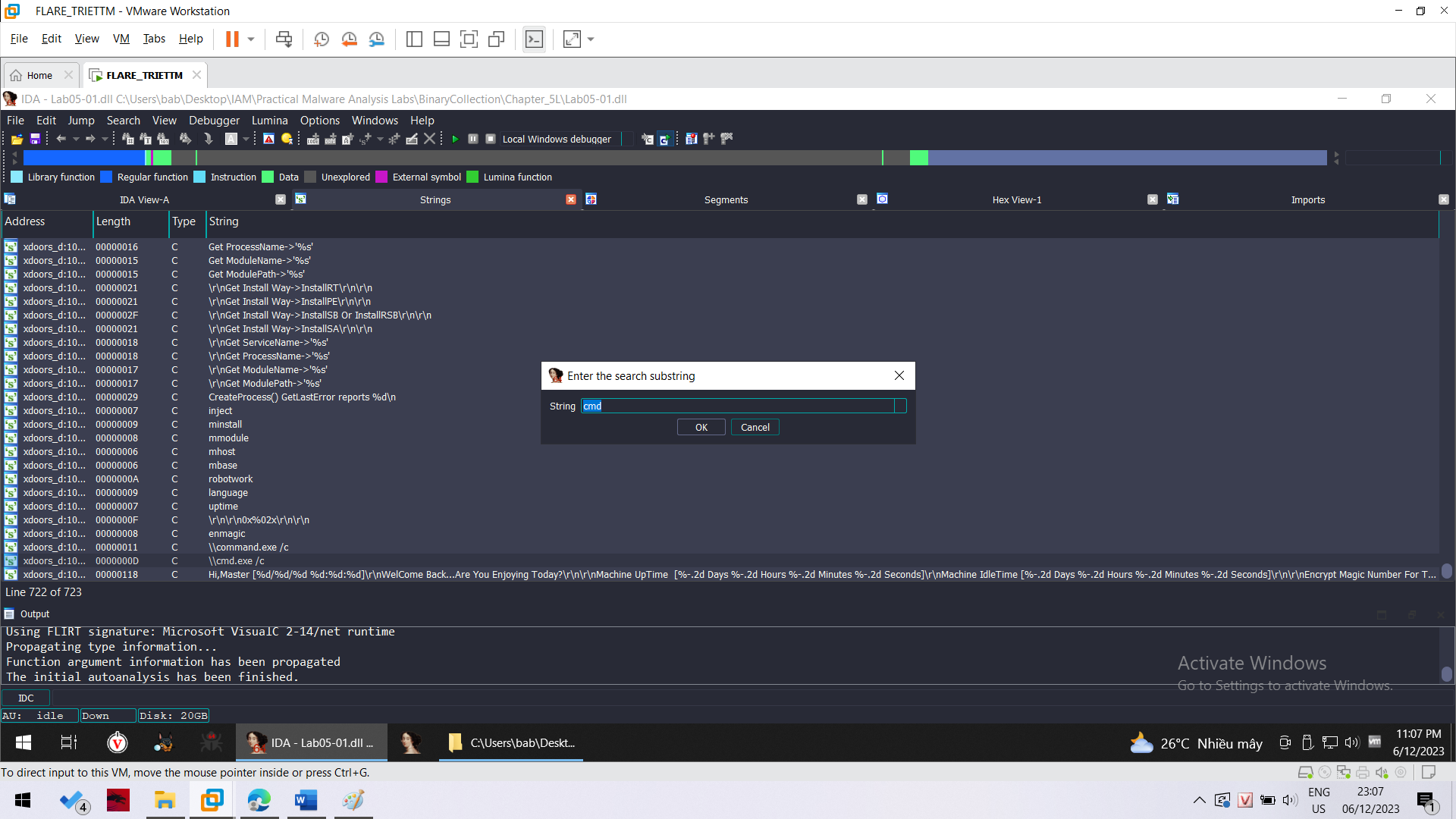
Bấm nút G để thực hiện nhảy tới address mình muốn

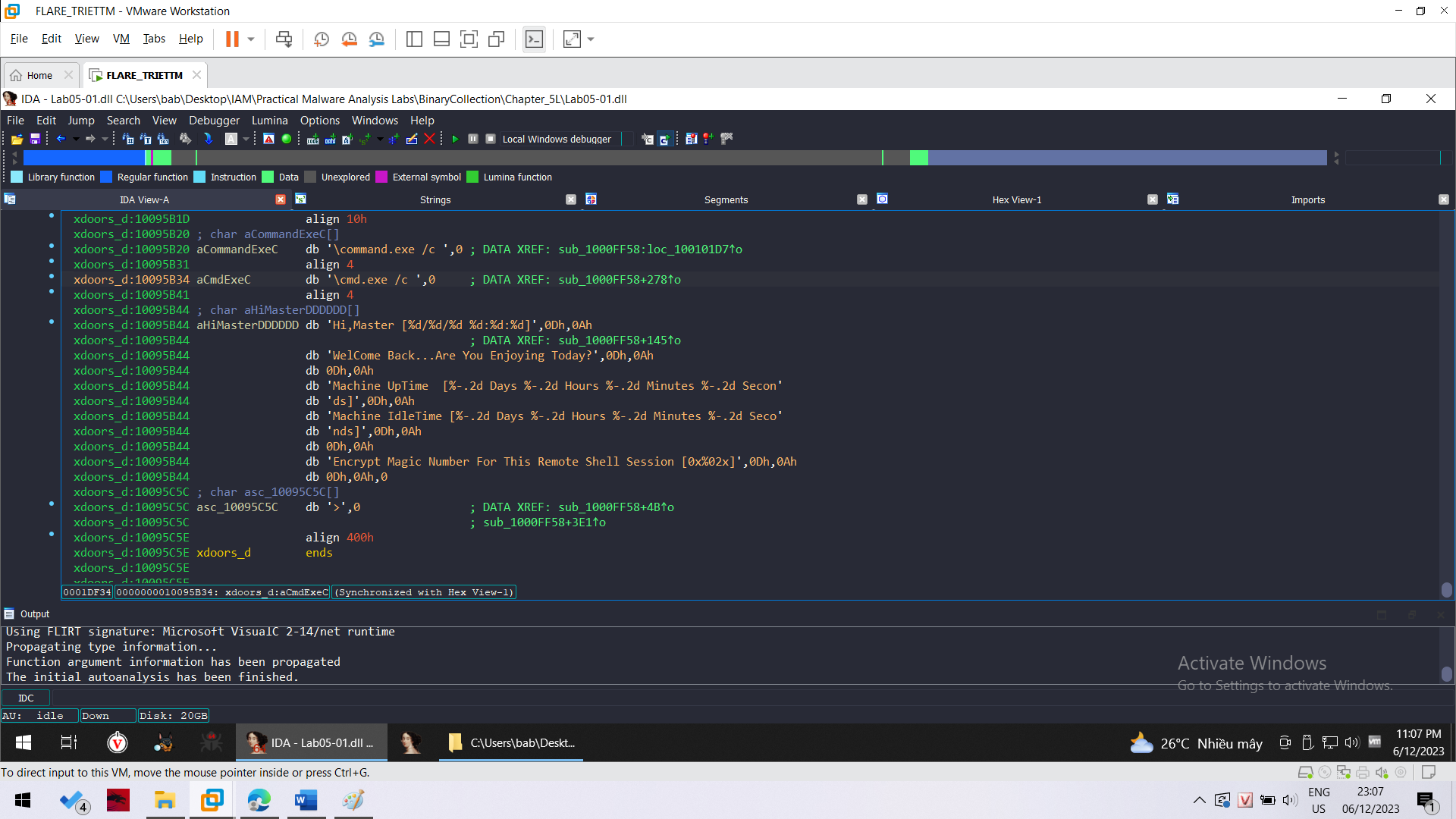




Có rất nhiều biến nội bộ được khai báo ở hàm này.

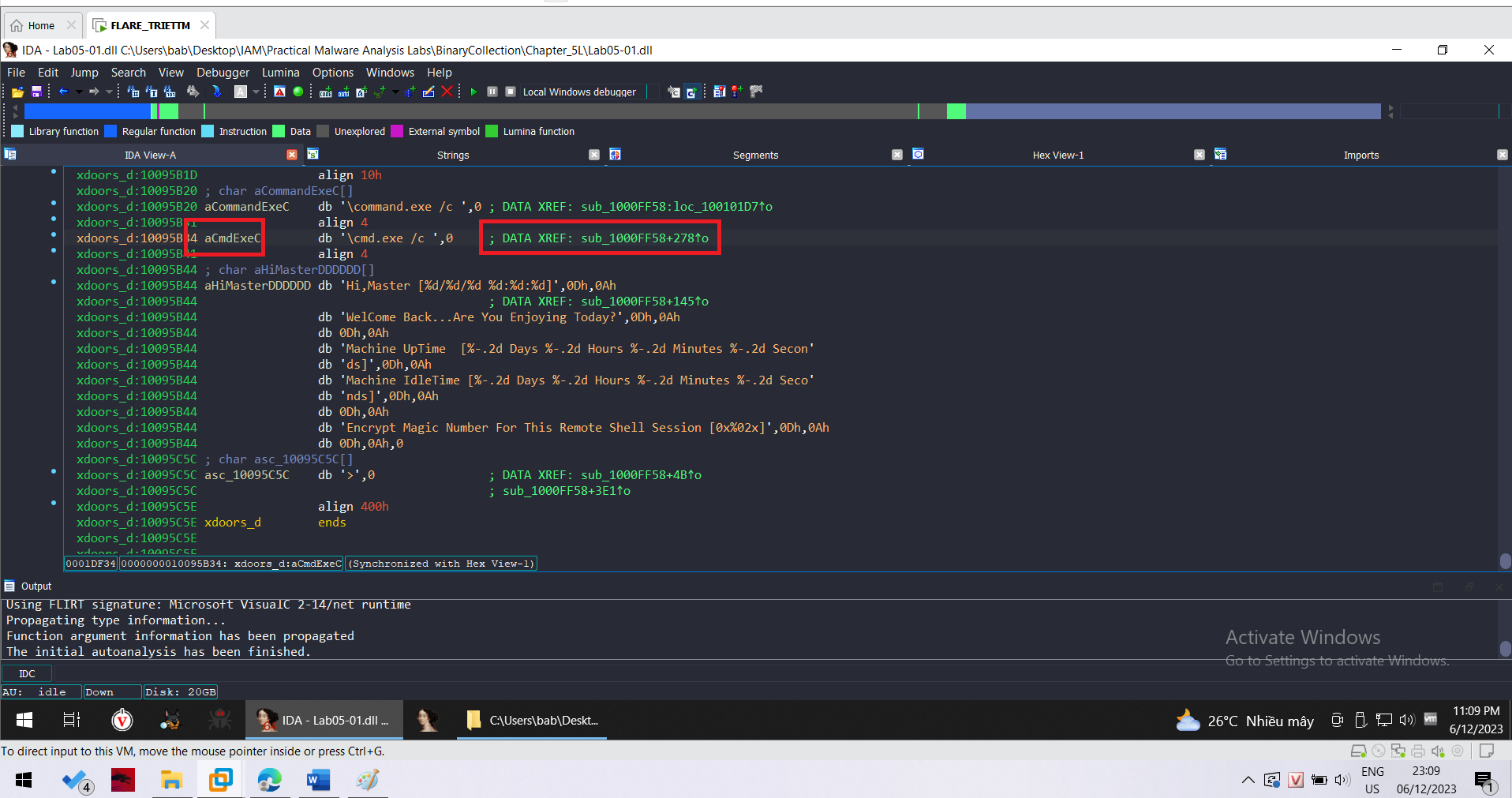
**Q 8: Finding the Purpose of the Code that References \cmd.exe /c**





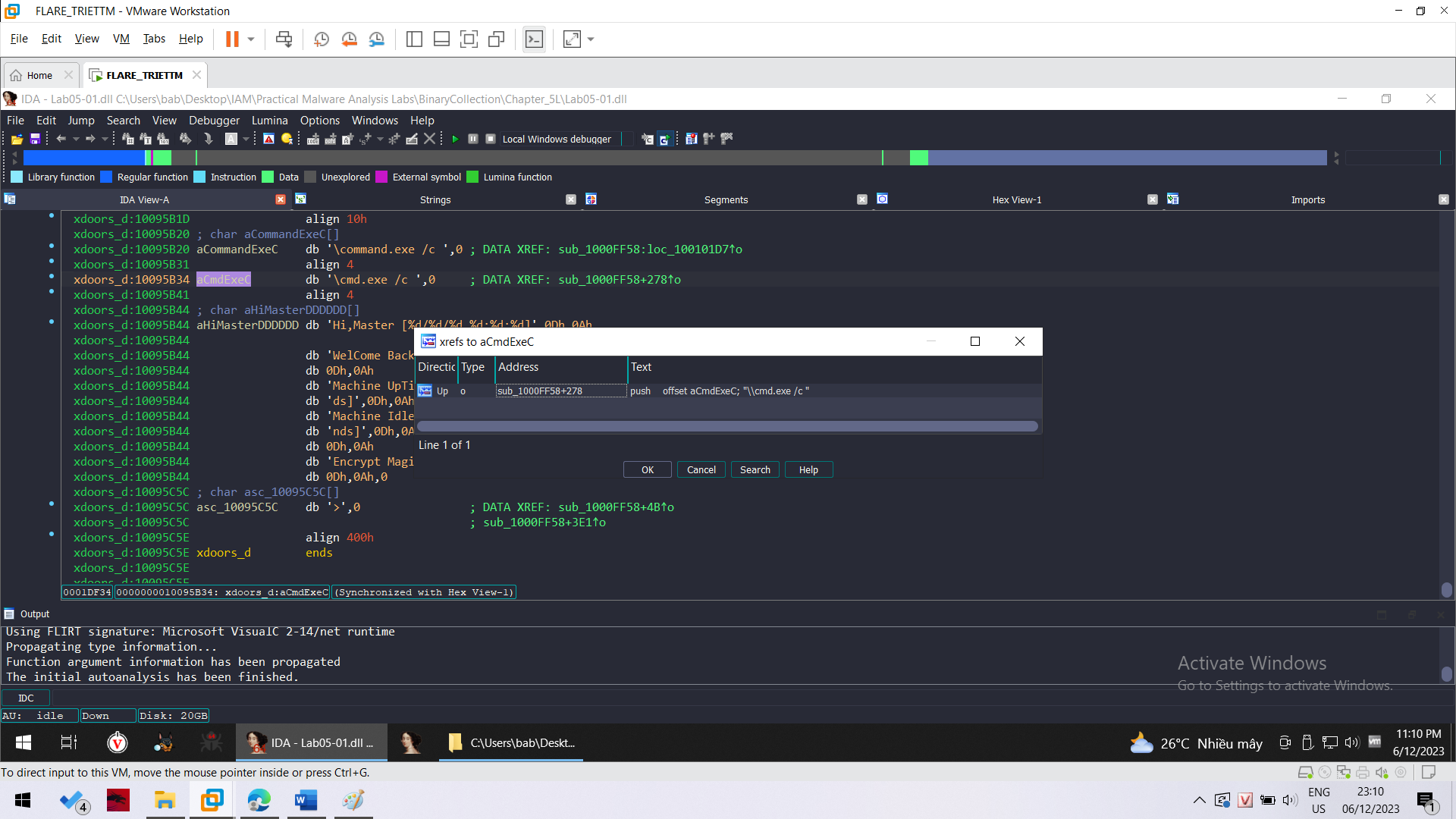
Ta thực hiện search ở ô cửa sổ string để tìm nơi có chứa chuỗi cmd

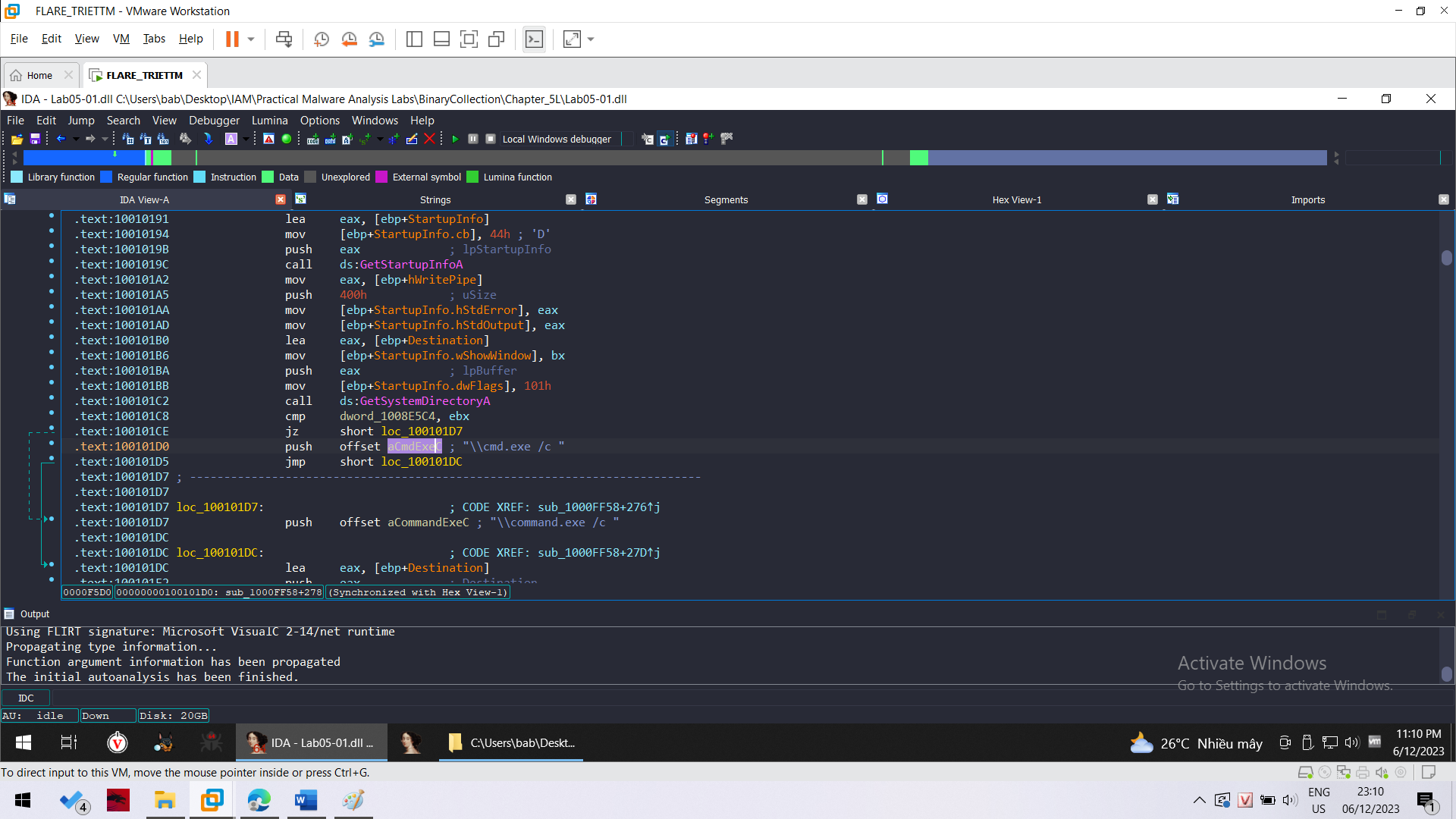
Bây giờ ta sẽ tìm hiểu về chức năng refference của IDA. Chức anngw này cho phép ta di chuyển đến vùng code có sử dụng đoạn chuỗi này.



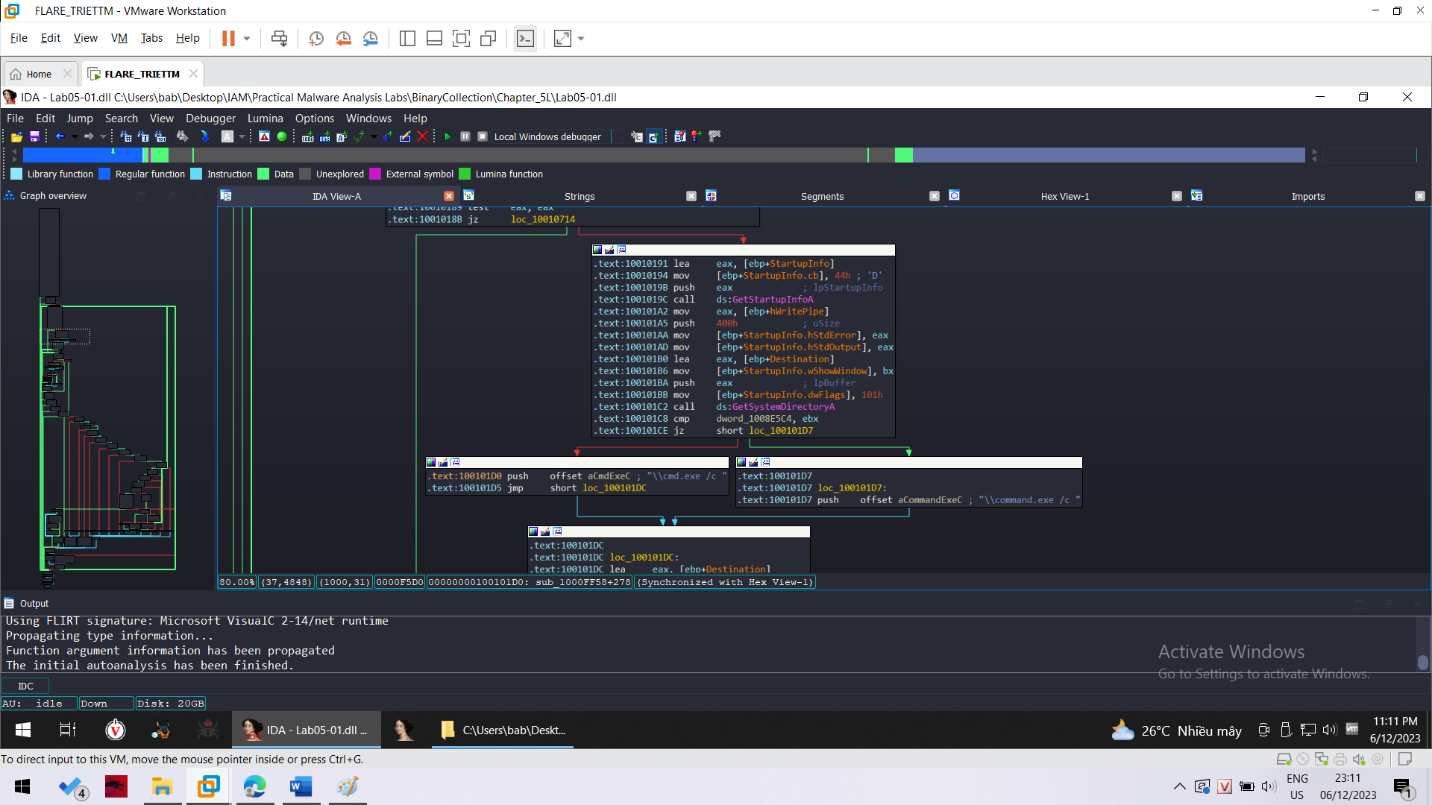
Ta có hai cách để thực hiện tham chiếu.

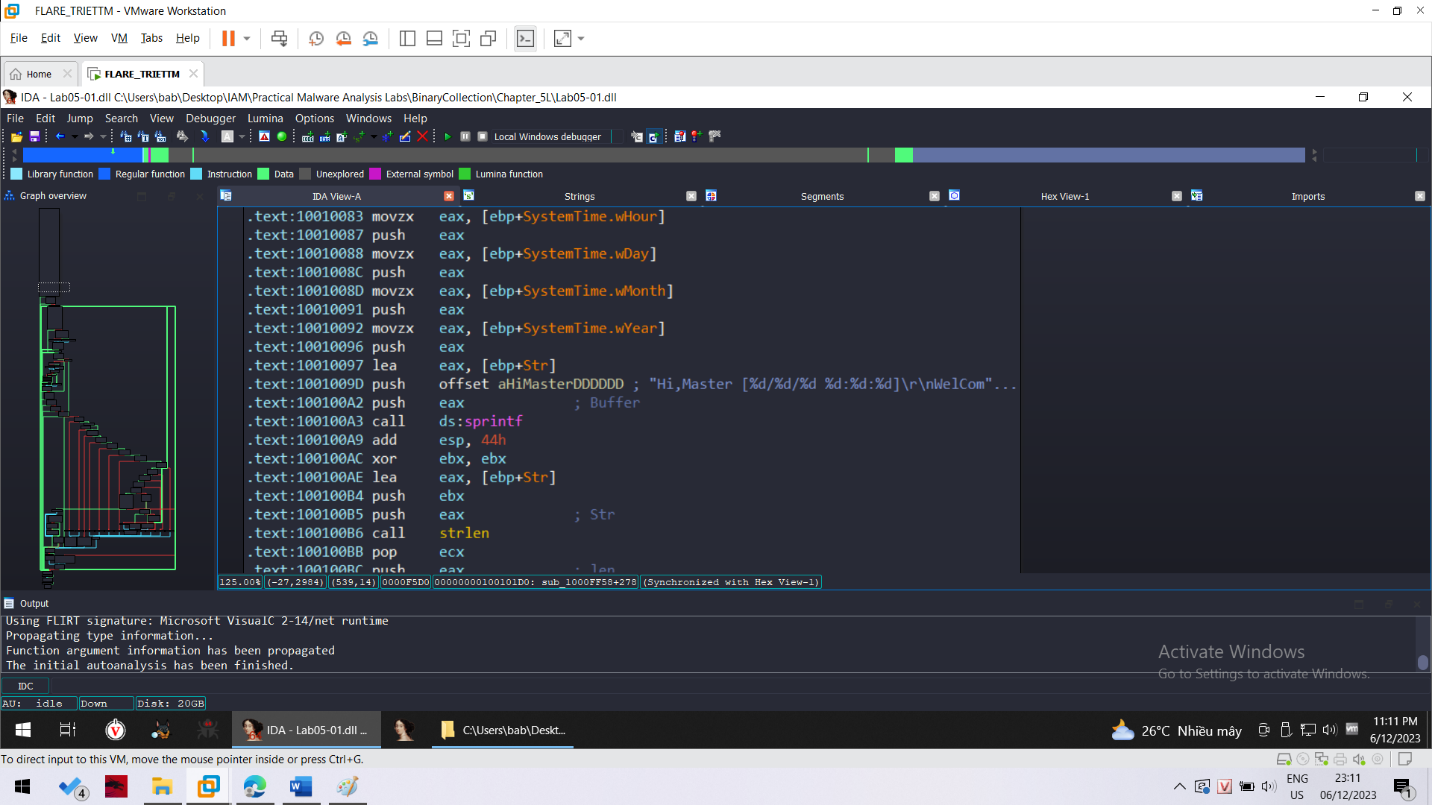
Có thể bấm vào DATA XREF bên tay phải hoặc nhấn vào tên biến bên tay trái rồi nhấn phím x



Chọn vào function cần nhảy tới

Đây ta có thể thấy đây là nơi cmd được gọi.





Ta đi tìm chuỗi master rồi có thể nhấn vào để em vị trí của nó trên memory như khi nãy.

