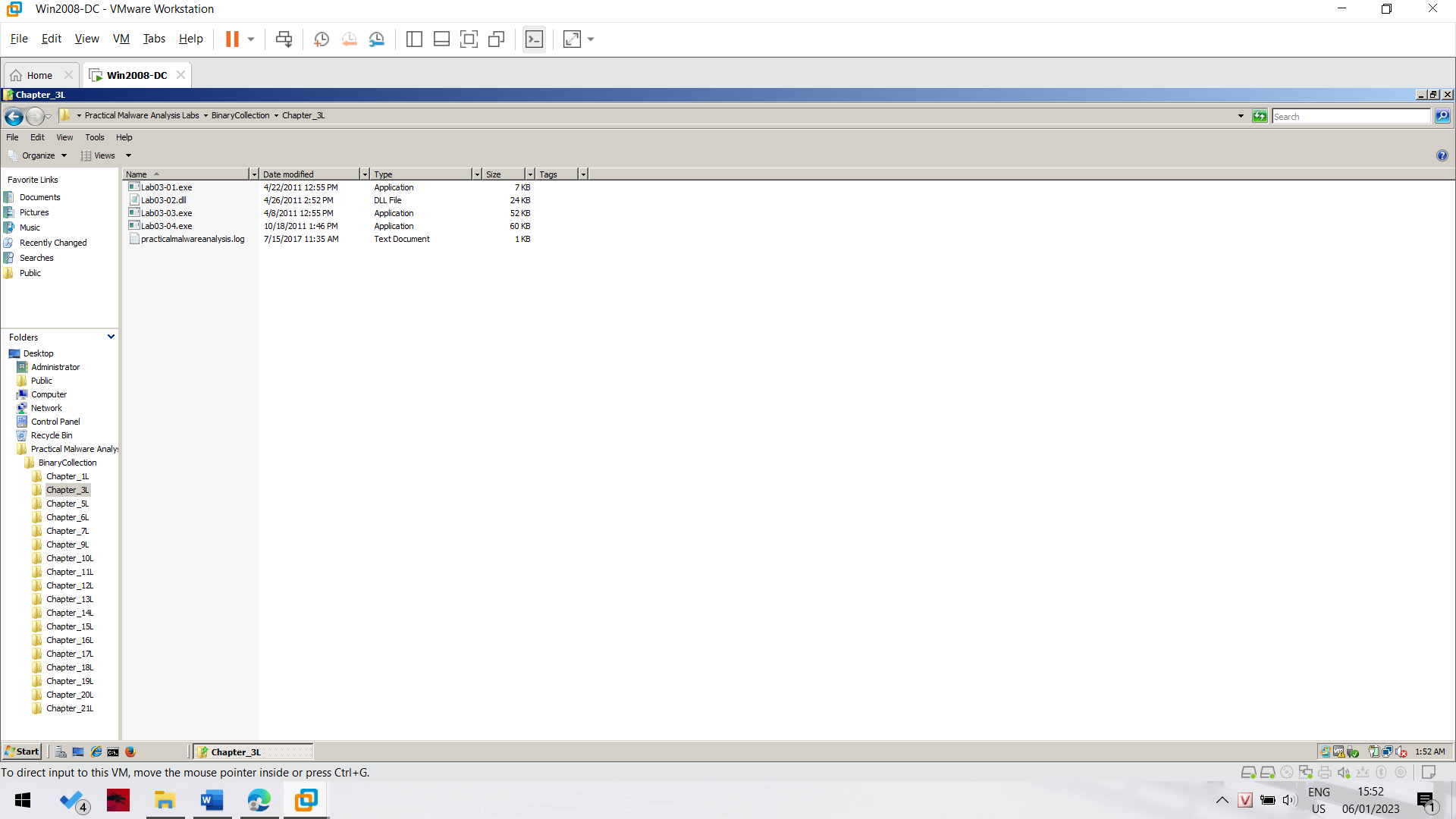
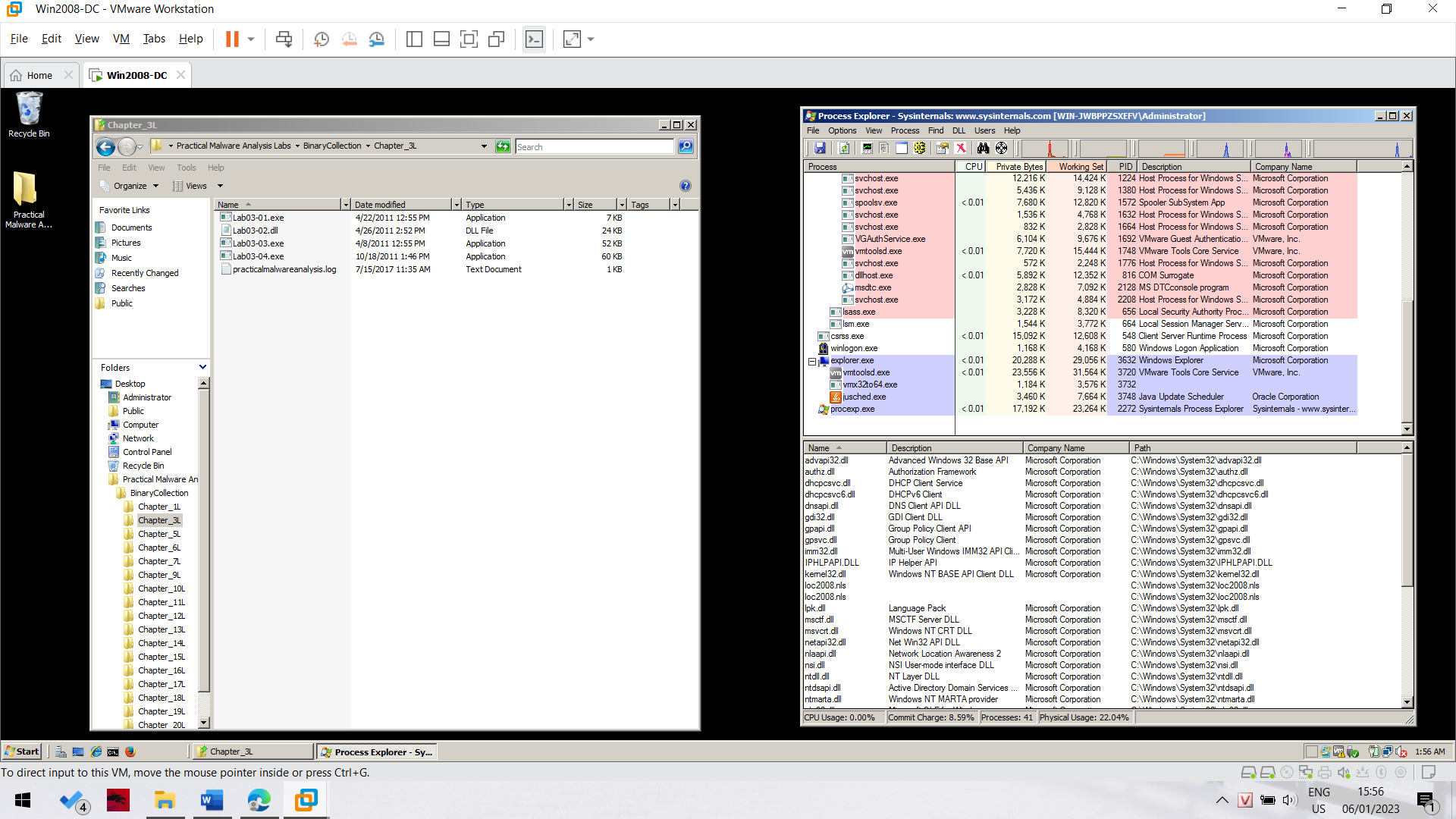
**Lab 6: Keylogger**

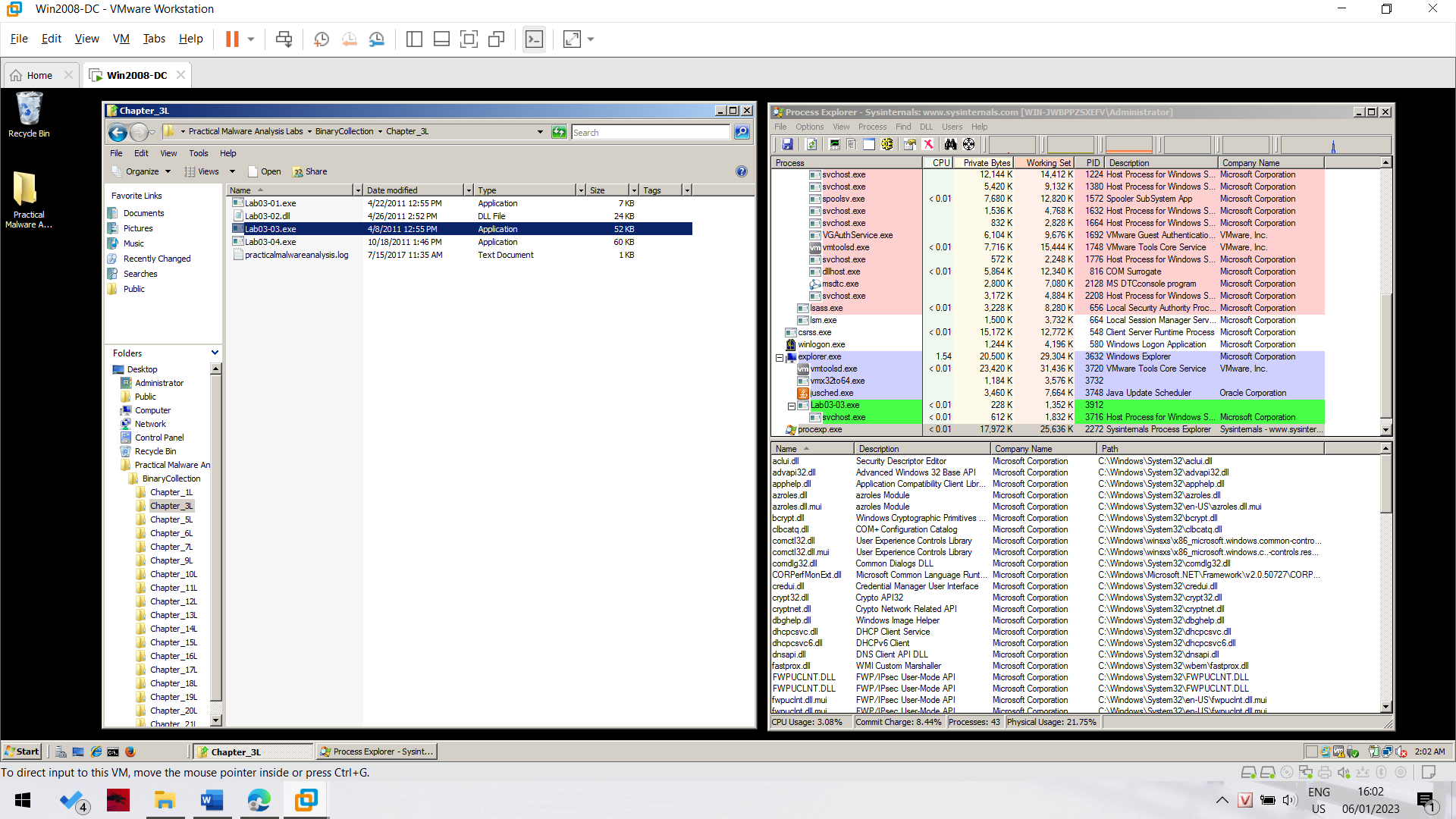
Ở bài này chúng ta sẽ tiến hành phân tích một con malware keylogger có tên là Lab03-03.exe.



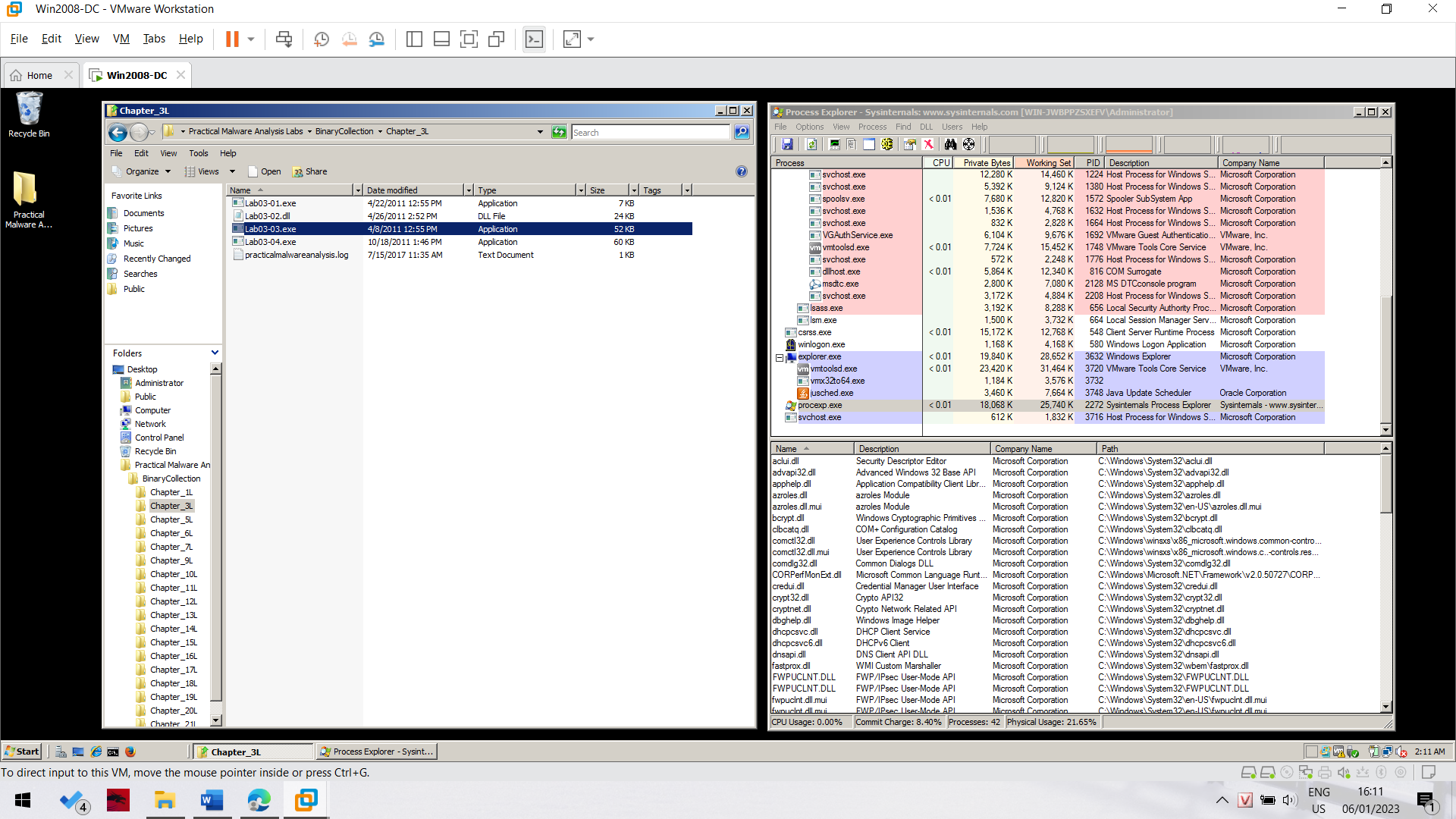
Đầu tiên ta sẽ khởi động Process Explorer để xem coi trong quá trình runtime, con malware này sẽ thực hiện những hành vi như thế nào.



Bây giờ ta đã sẵn sàng để chạy thử con malware này ngay trên máy của mình.

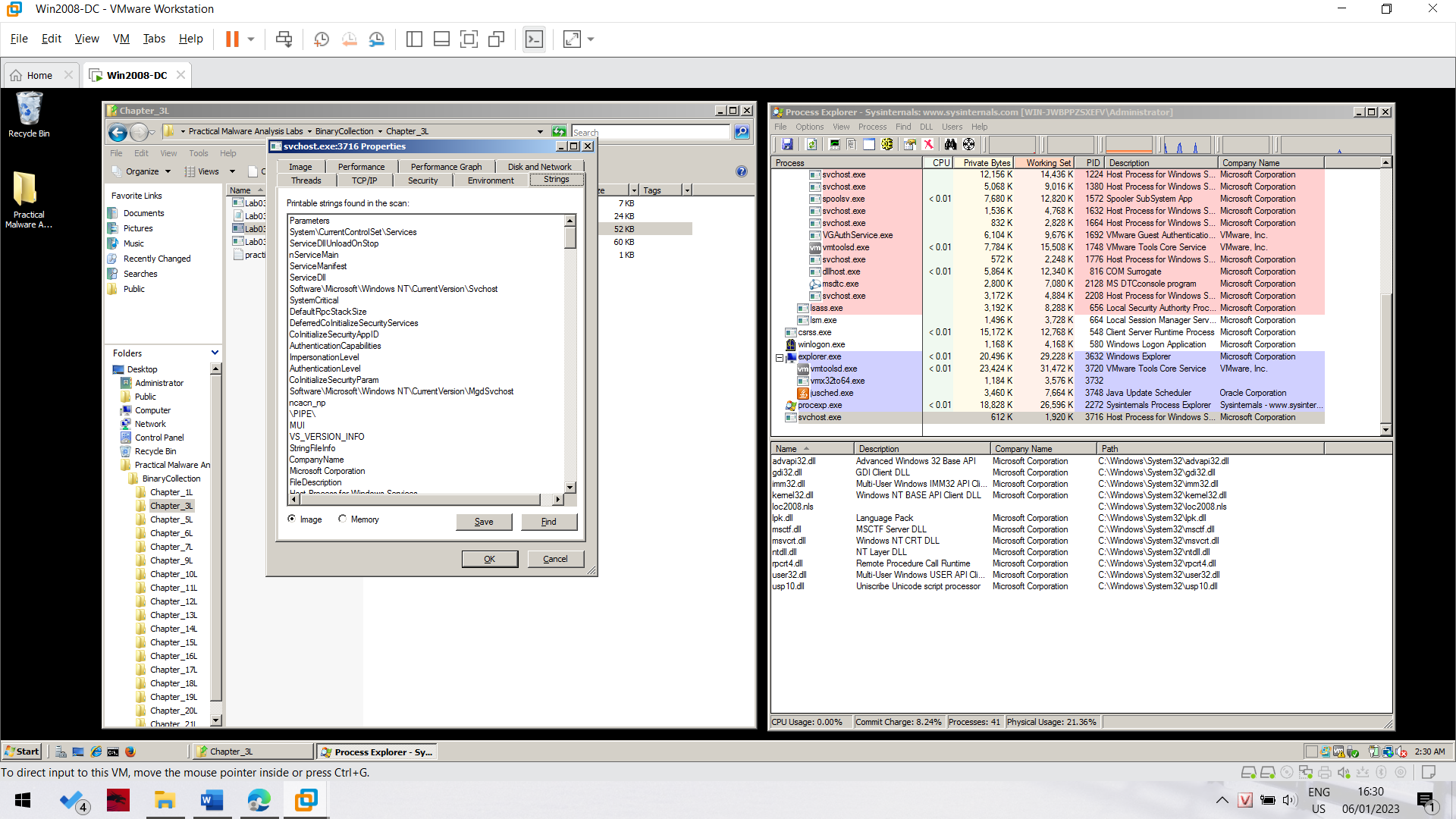


Khi chạy con malware sẽ có hai tiến trình được tạo ra lần lượt là Lab03-03.exe sinh ra tiến trình con mang tên svchost.exe. Tuy nhiên chỉ sau tầm 1 2 giây gì đó, process Lab03-03.exe tự động terminate chính mình đi và chỉ để lại tiến trình con của nó là svchost.exe như hình dưới đây.



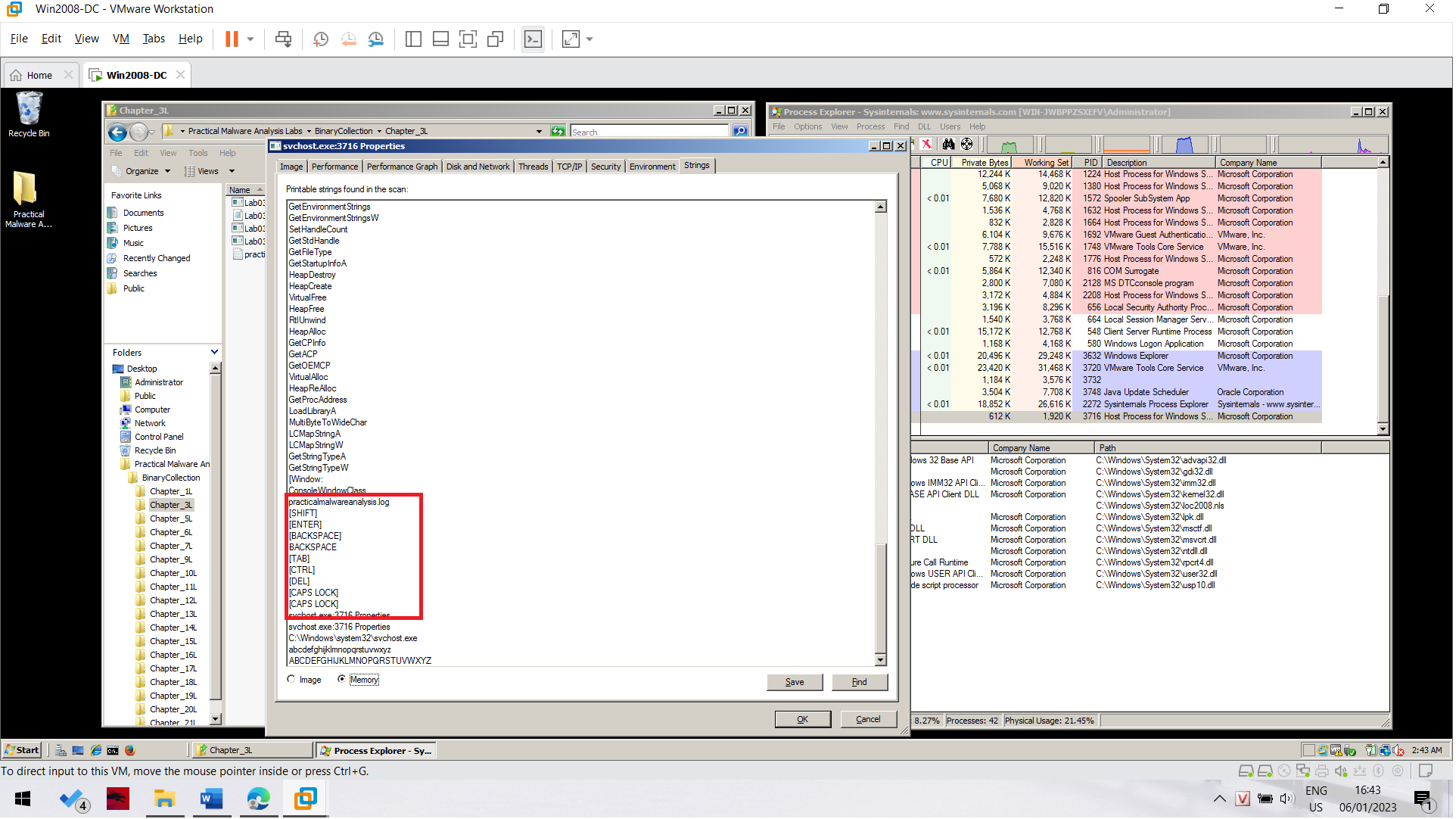
Quả là một hành vi đáng ngờ đến từ con malware Lab03-03.exe này. Theo dự đoán của em tiến trình scvhost.exe này mới chính là con keylogger thật của bài này. Cái tên Lab03-03 chỉ là cái tên giả làm che mắt người phân tích chứ con malware này đã giả tên một tiến trình hệ thống tên svchost để khi mà người dùng có check task manager thì không phát hiện ra có điều gì đáng ngờ.

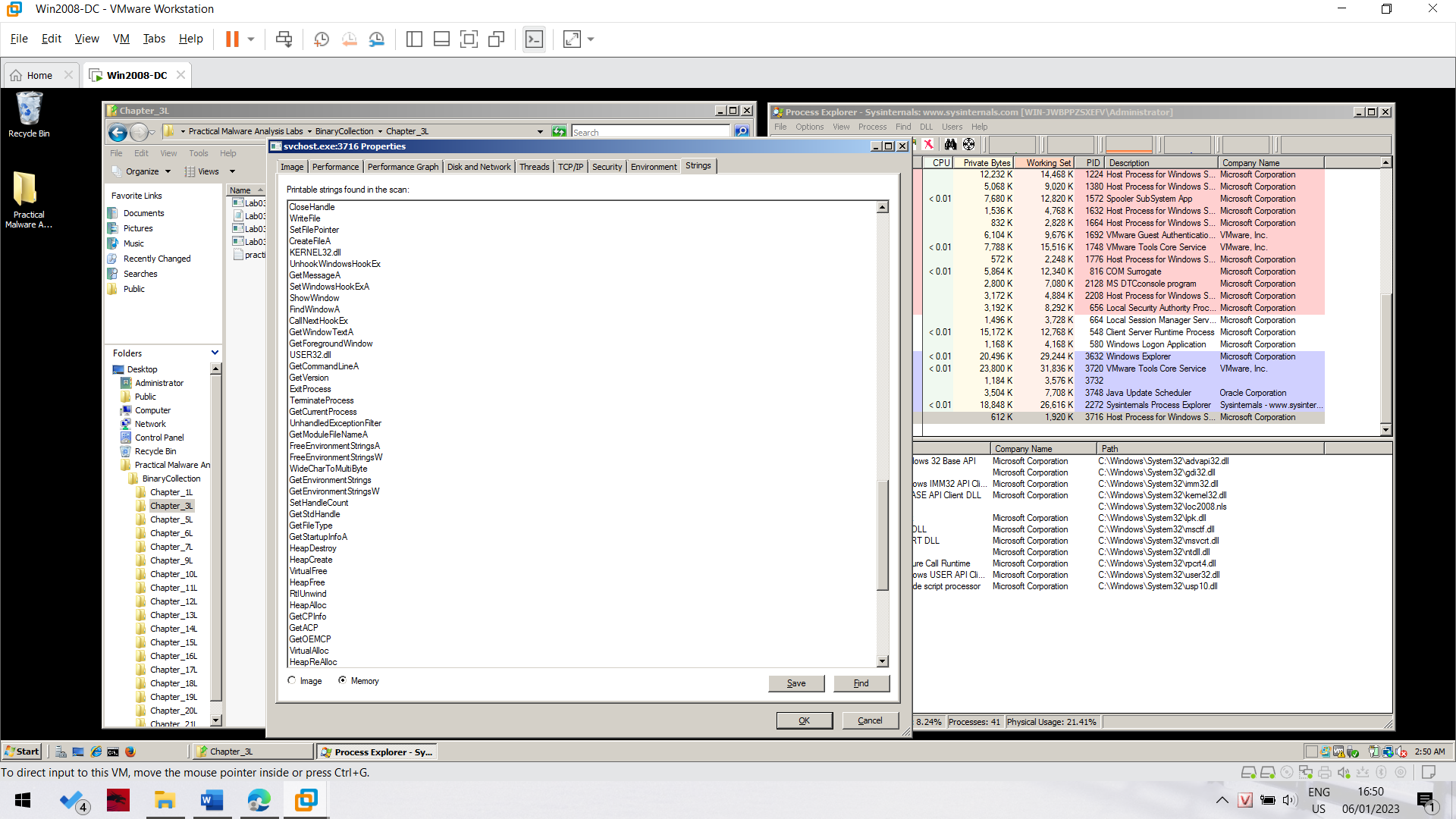
Bây giờ ta sẽ tiến hành phân tích hành vi của tiến trình mang tên svchost này.

Ta nhấn chuột phải vào process này, chọn Properties rồi chuyển qua tab strings. 

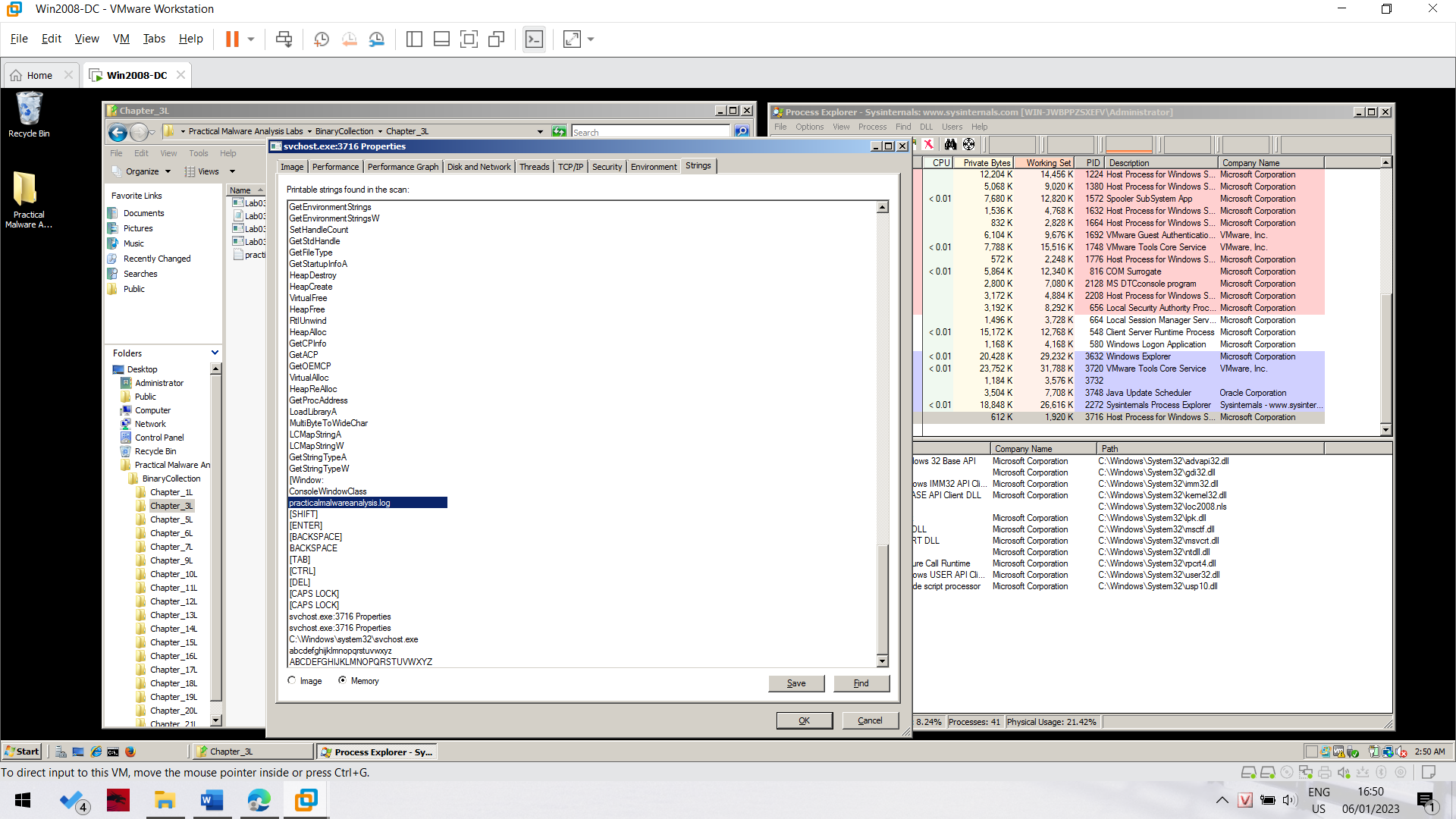
Ở đây, process explorer cung cấp cho ta hai chế độ xem strings. Một là xem strings của file thực thi này trên ổ cứng hay file thực thi gốc. Hai là chế độ memory để xem string của file thực thi này khi chương trình đang chạy.

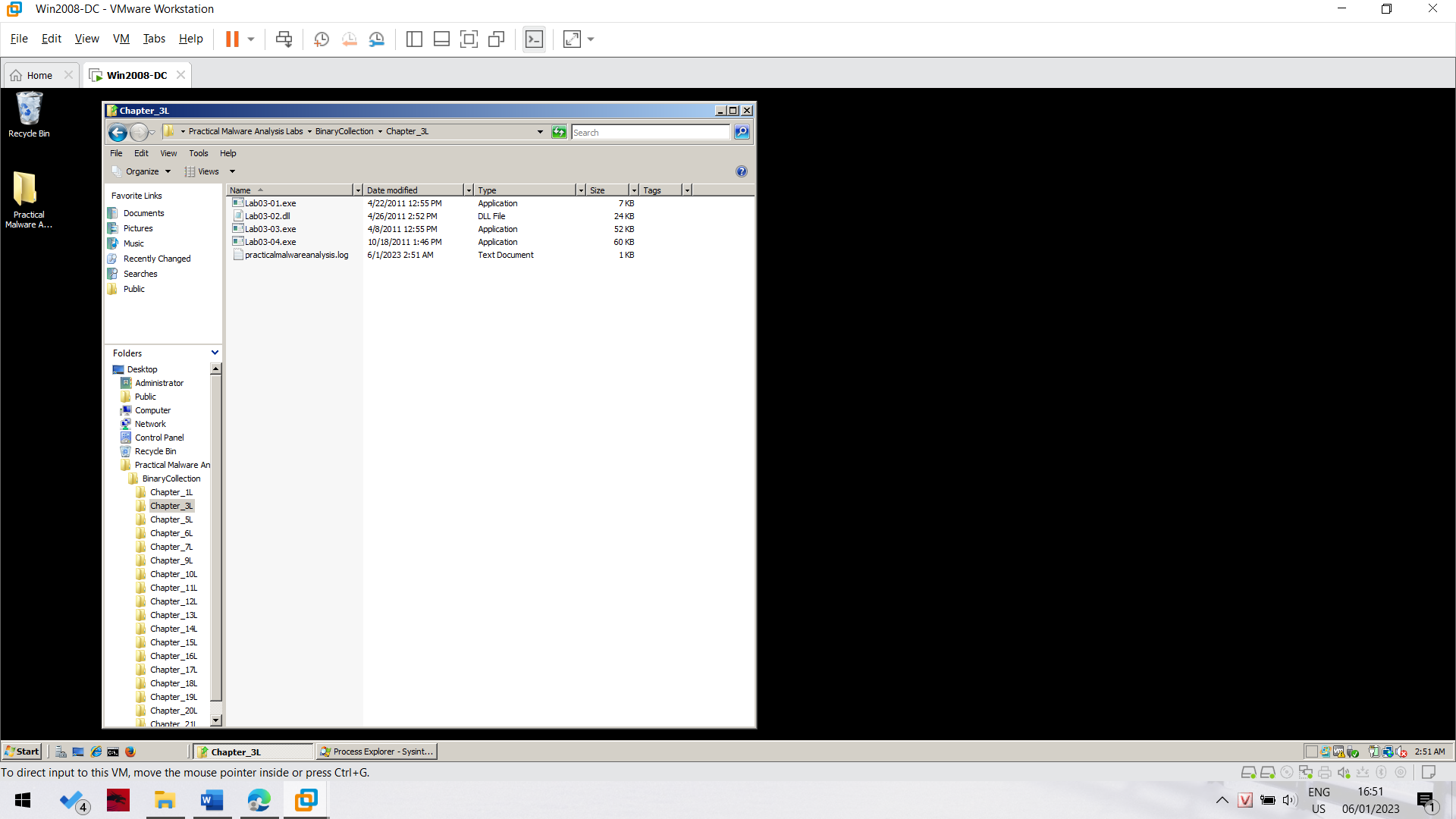
Vì đây là một con keylogger đang chạy ngầm trên hệ thống nên ta sẽ xem string trong chế độ memory để xem có điều gì khả nghi hay không.



Như ta có thể thấy những đoạn chuỗi khả nghi như hình trên là các phím gõ trên bàn phím. 

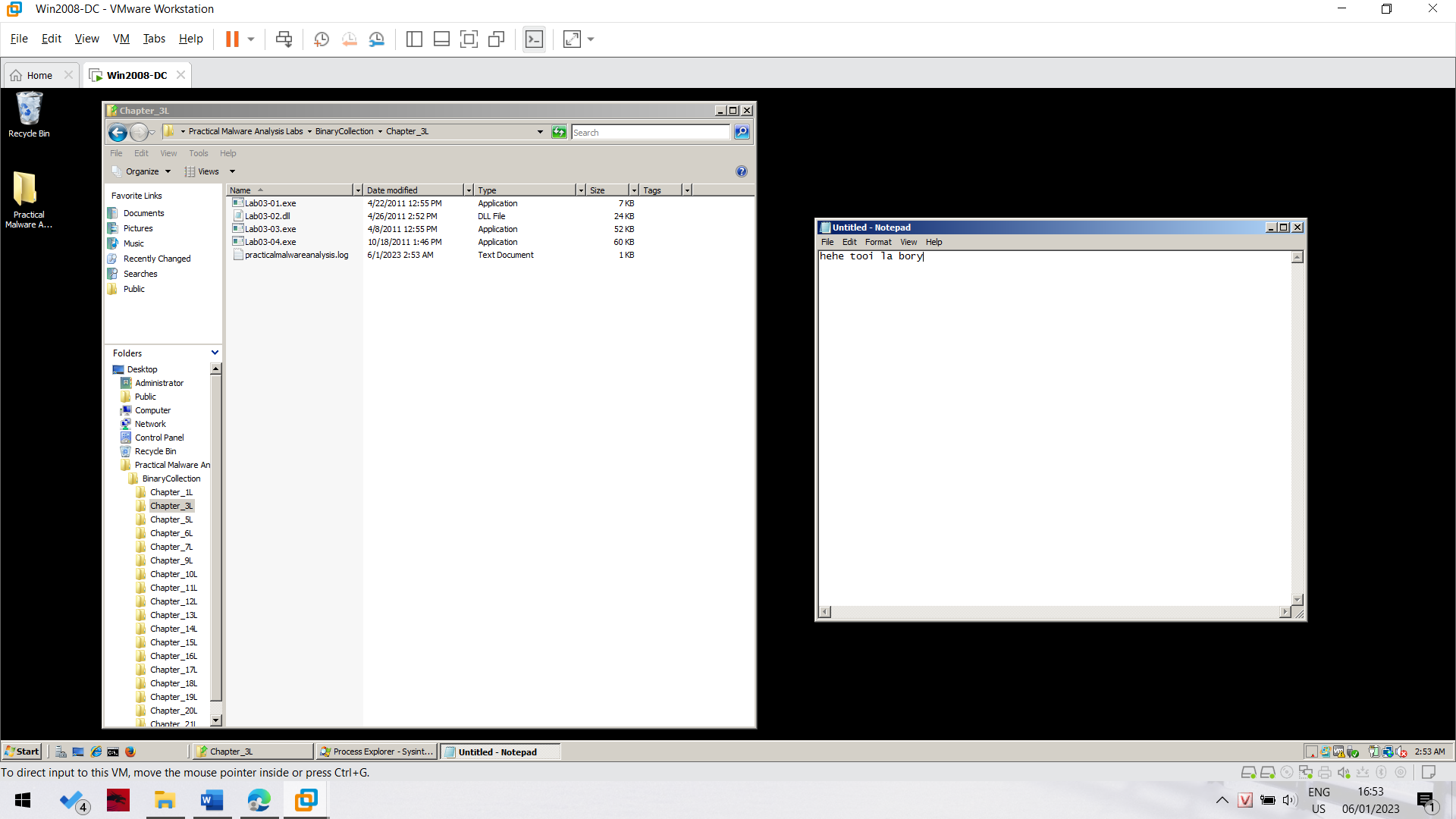
Ngoài ra còn có các hàm để tạo tiến trình giả lấy từ kernel32.dll.



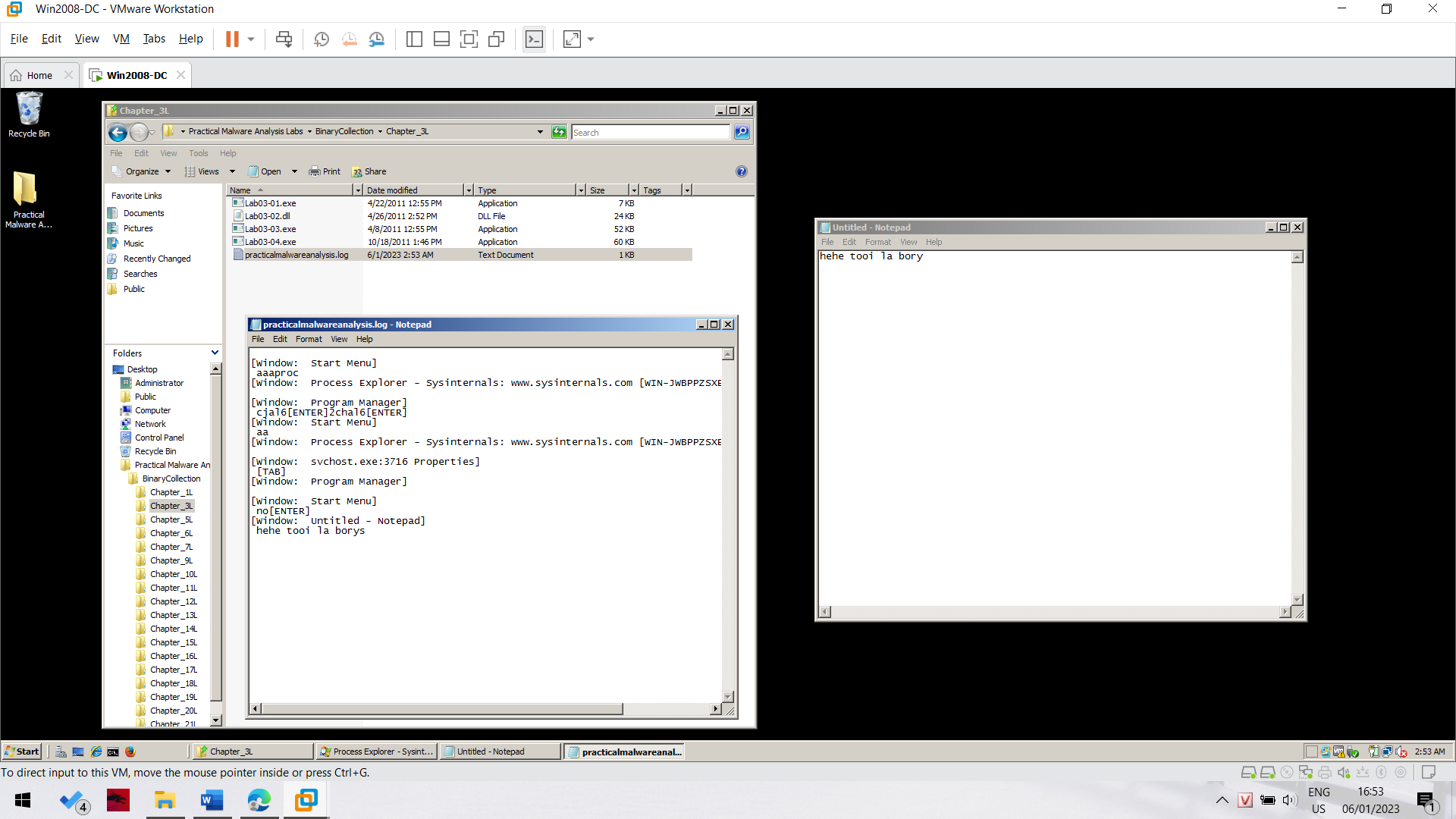
Thứ đáng lưu ý nhất ở đây có lẽ là dòng practicalmalwareanalysis.log này. 

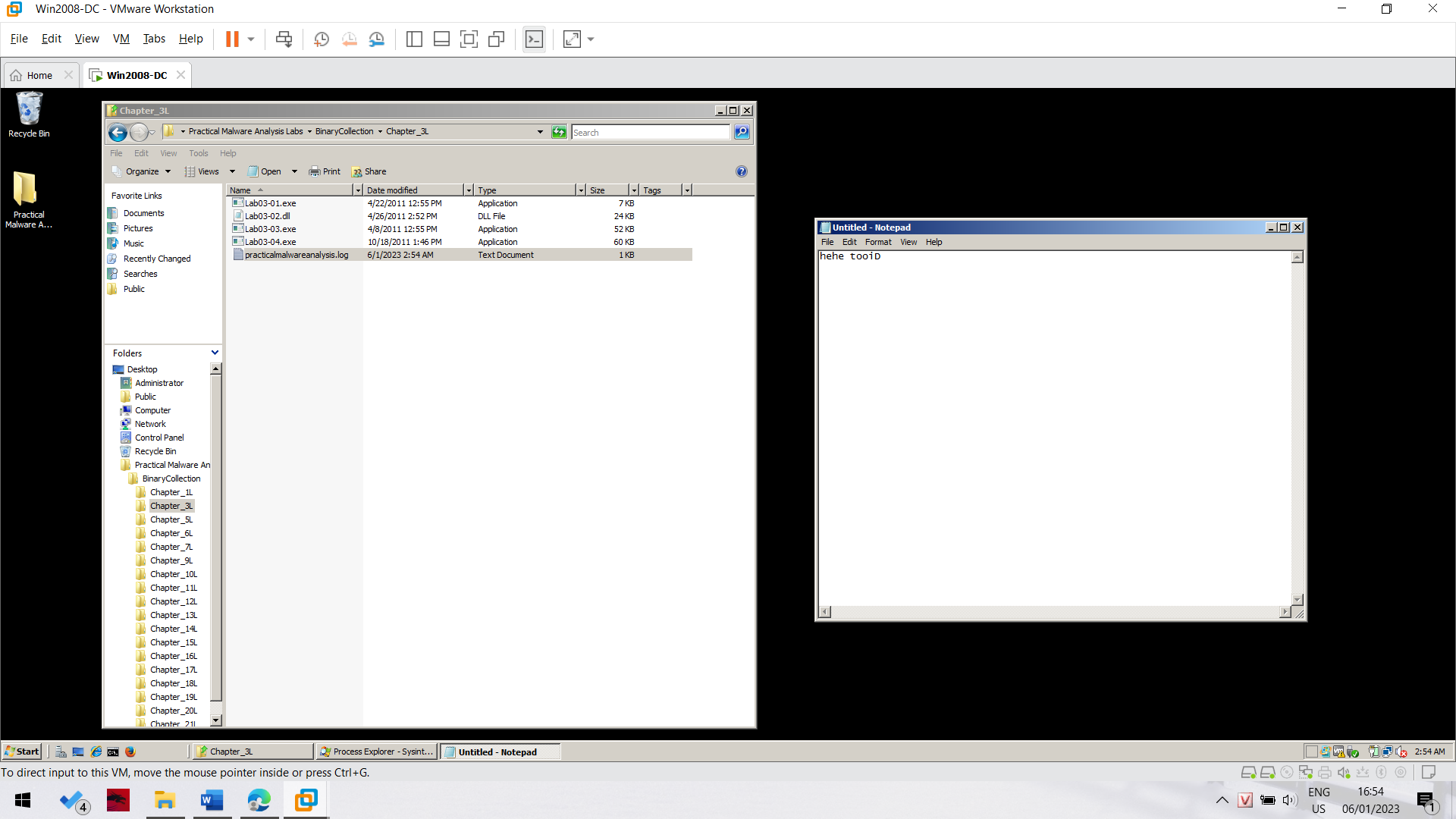
Nó nằm ở ngay tại chỗ nơi chứa con malware này luôn, đây là một file log ghi lại những keystroke mỗi khi ta gõ bàn phím, những phím này sẽ ghi lại vào file log này.

Bây giờ ta sẽ tiến hành test thử coi con keylogger này hoạt động như thế nào.

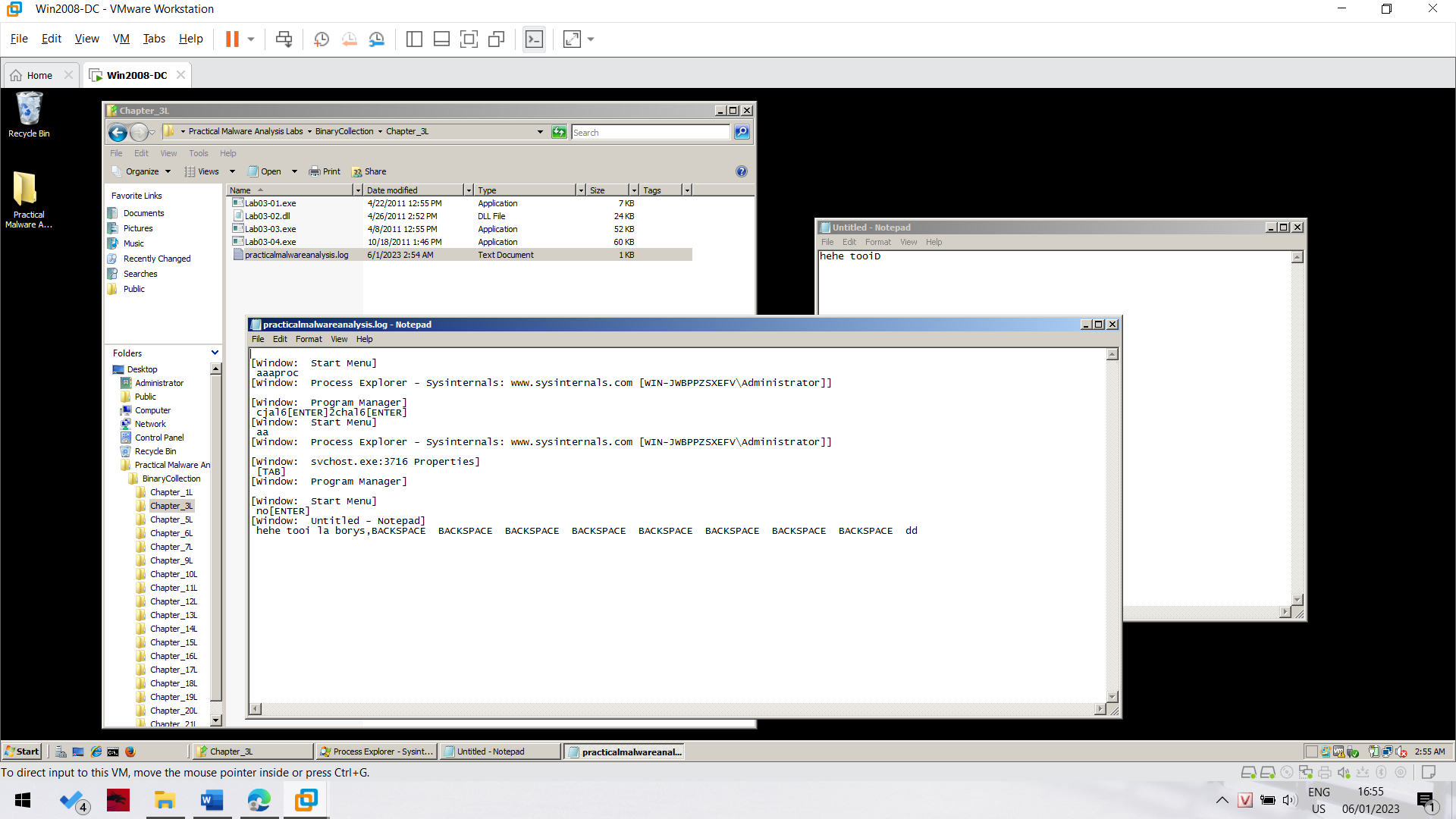


Mở một file notepad và ghi nội dung như bên trên.



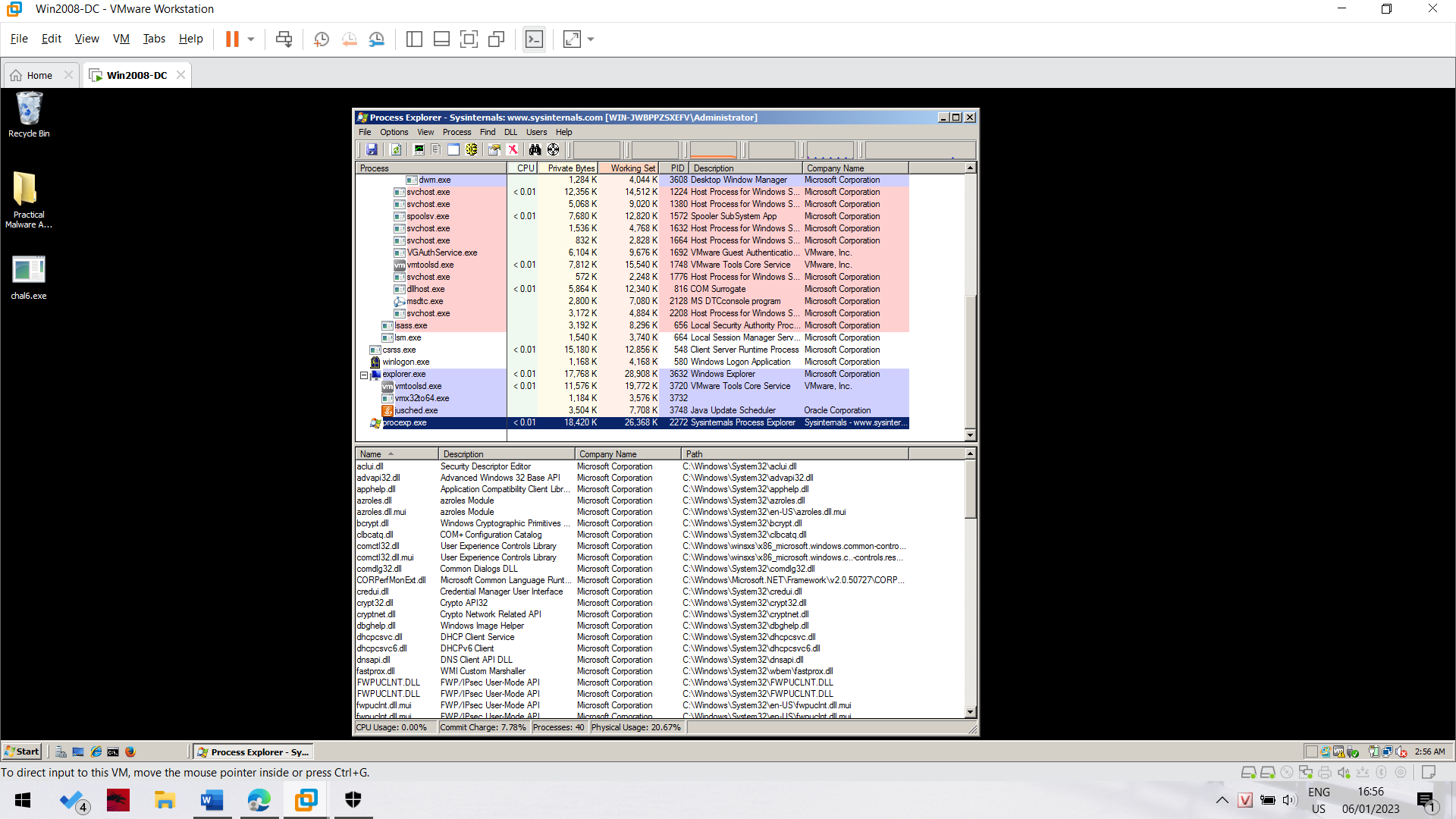
Mở file log lên check thì thấy dòng chữ mà ta gõ trên notepad được ghi lại trên file log này. 

Thử xóa vài chữ bằng phím backspace, nhấn phím ctrl và nhấn phím shift.

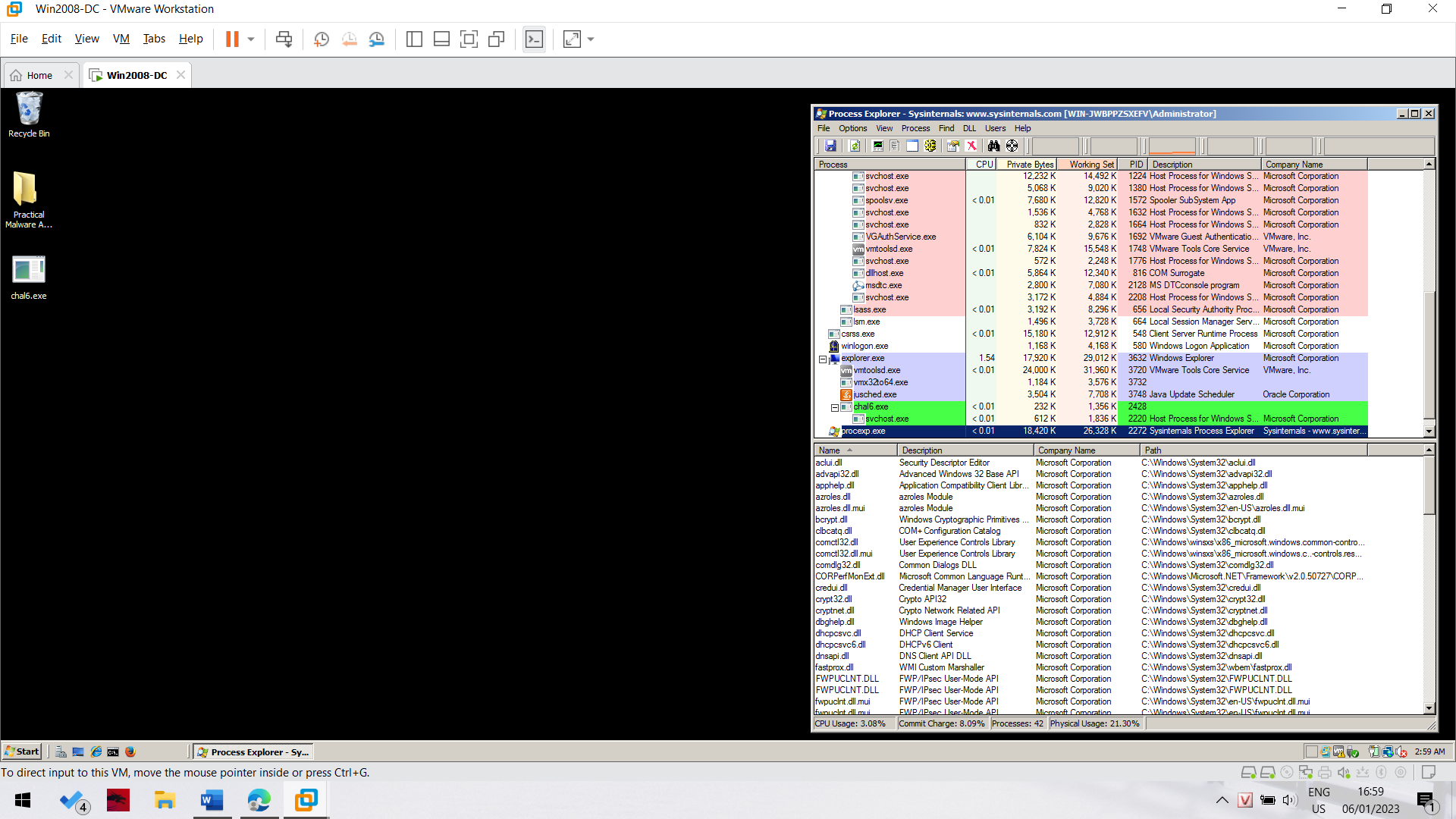


Ok file log đã ghi lại các keystroke của chúng ta. Vậy là ta đã hiểu hành vi của con malware này rồi.

Ở phần tiếp theo ta sẽ thực hiện những bước tương tự để phân tích một con keylogger khác.

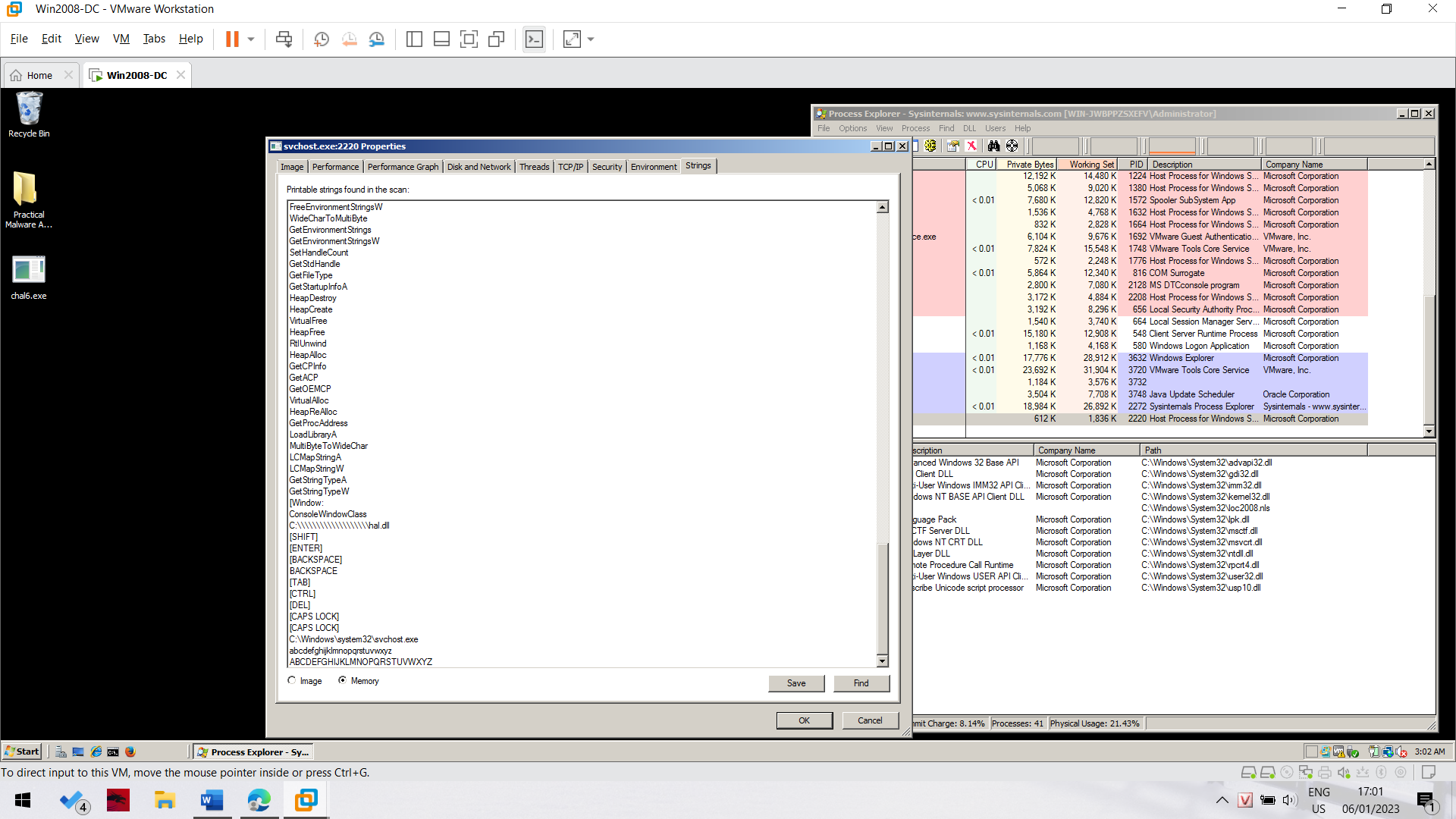


Con malware này tên là chal6.exe, em sẽ để nó ở trên desktop.



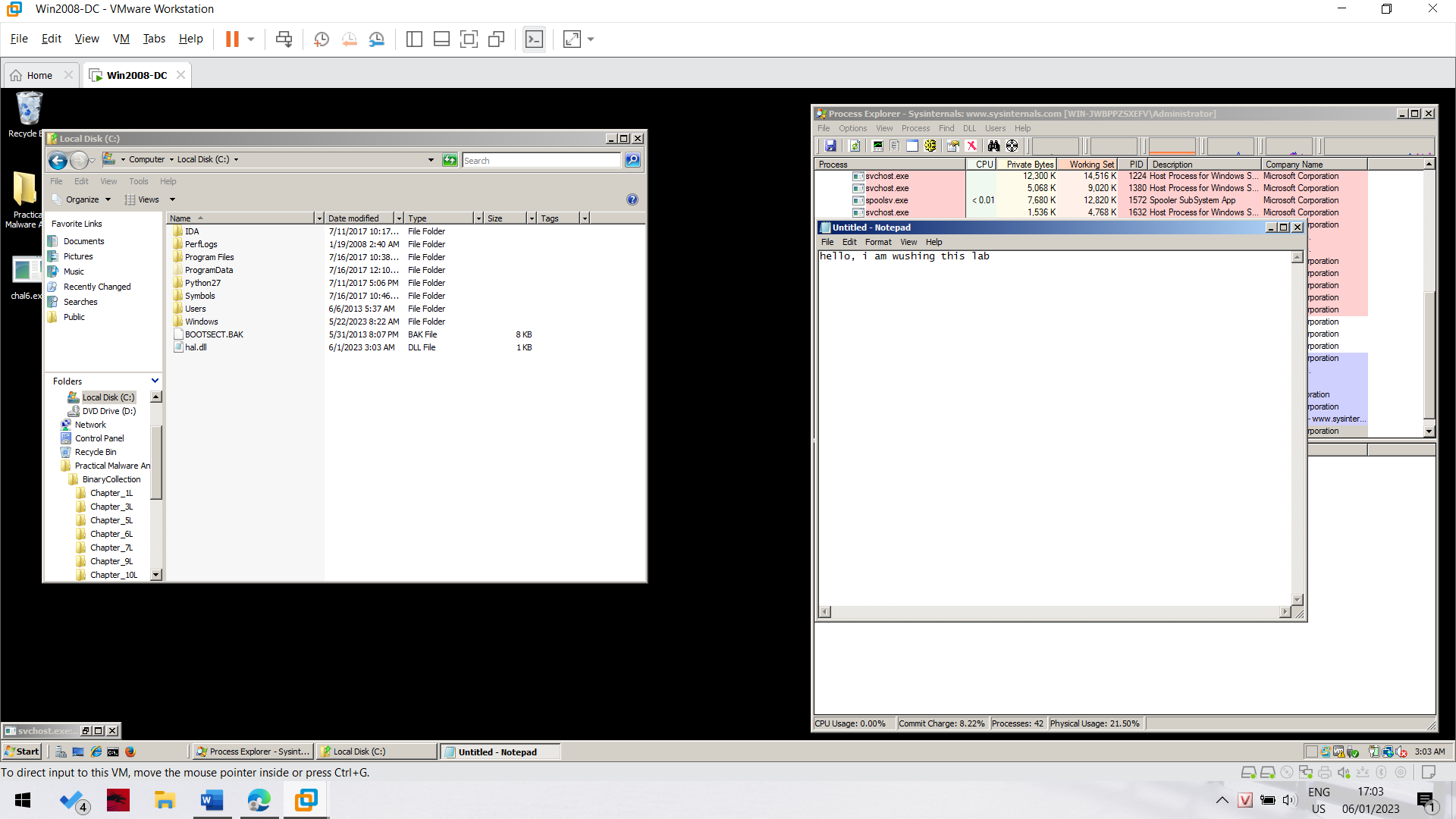
Hành vi của con này cũng tương tự như con trước, nó cũng tạo ra 2 process và process của con malware chính mang tên svchost.exe. Sau tầm 1 2 giây nó cũng tự động terminate tiến trình và chỉ để lại tiến trình chính bị giả tên ở lại để ghi log keystroke.

Ta cũng sẽ xem string của tiến trình này trên memory khi runtime.

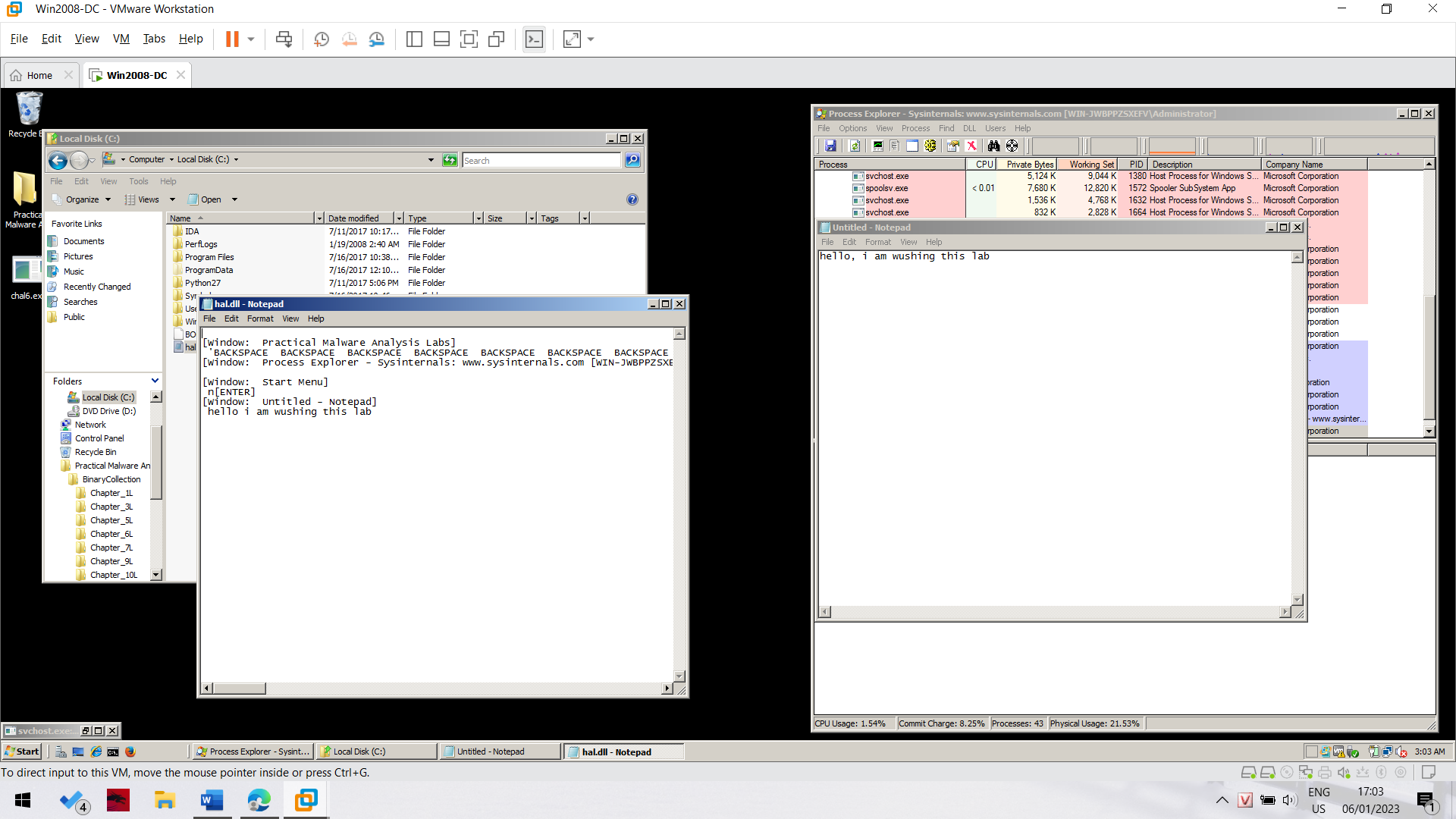


Ở đây có một dòng siêu khả nghi. C:\\\\\\\hal.dll.

Chắc hẳn đây là file mà con keylogger này ghi log lại.



Mở notepad lên test file log coi nó có ghi lại được keystroke không.



Ok con malware đã ghi lại thành công các phím mà mình gõ vào.

Vậy là ta đã thành công phân tích hai con keylogger này ^^