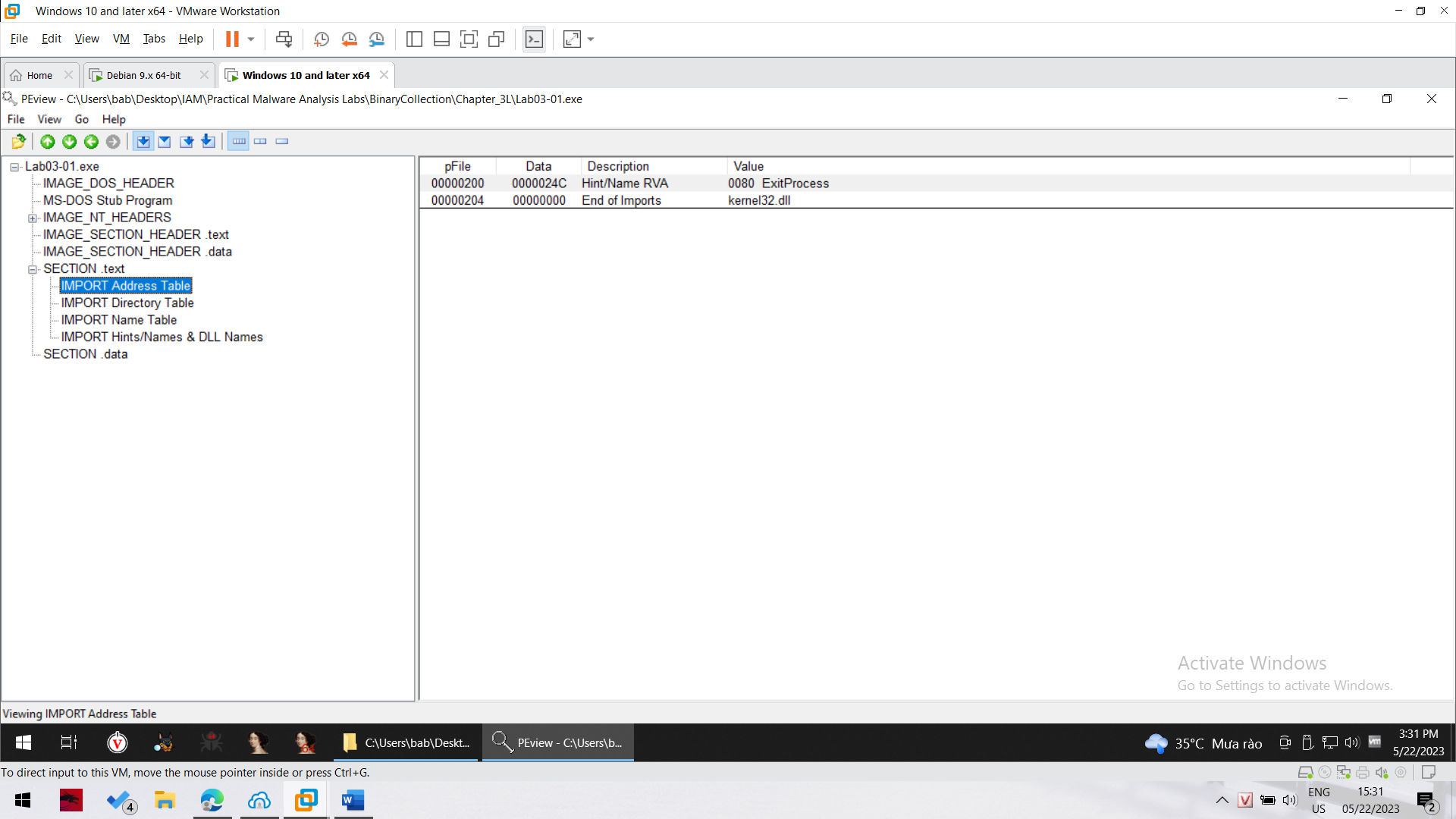
Proj 4: Basic Dynamic Techniques (Lab 3-1)

Ở bài lab này ta sẽ tiến hành phân tích trên con malware.

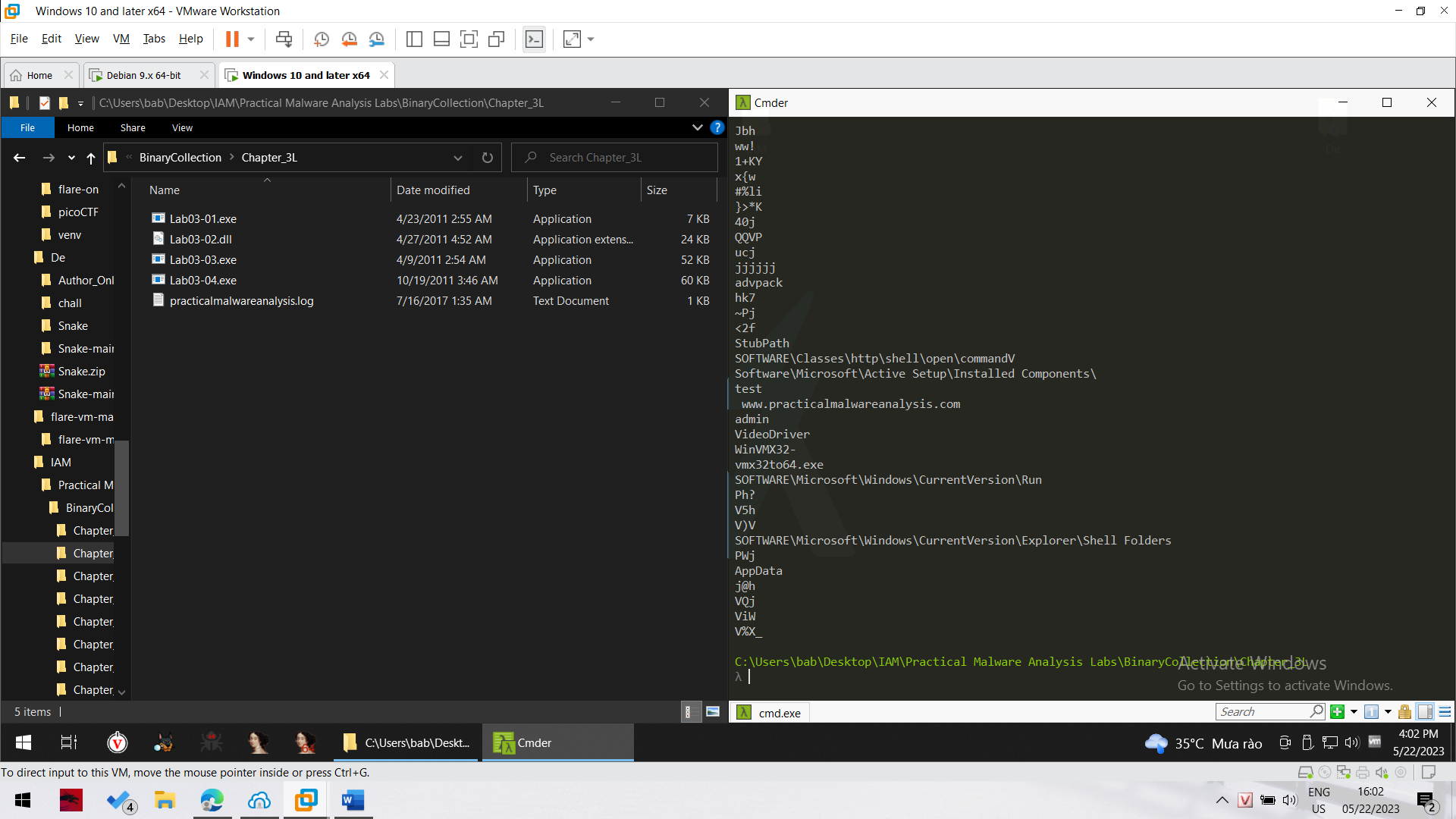
**Using PEview**

Đầu tiên ta sẽ ném file Lab03-01.exe vào trong PEview.

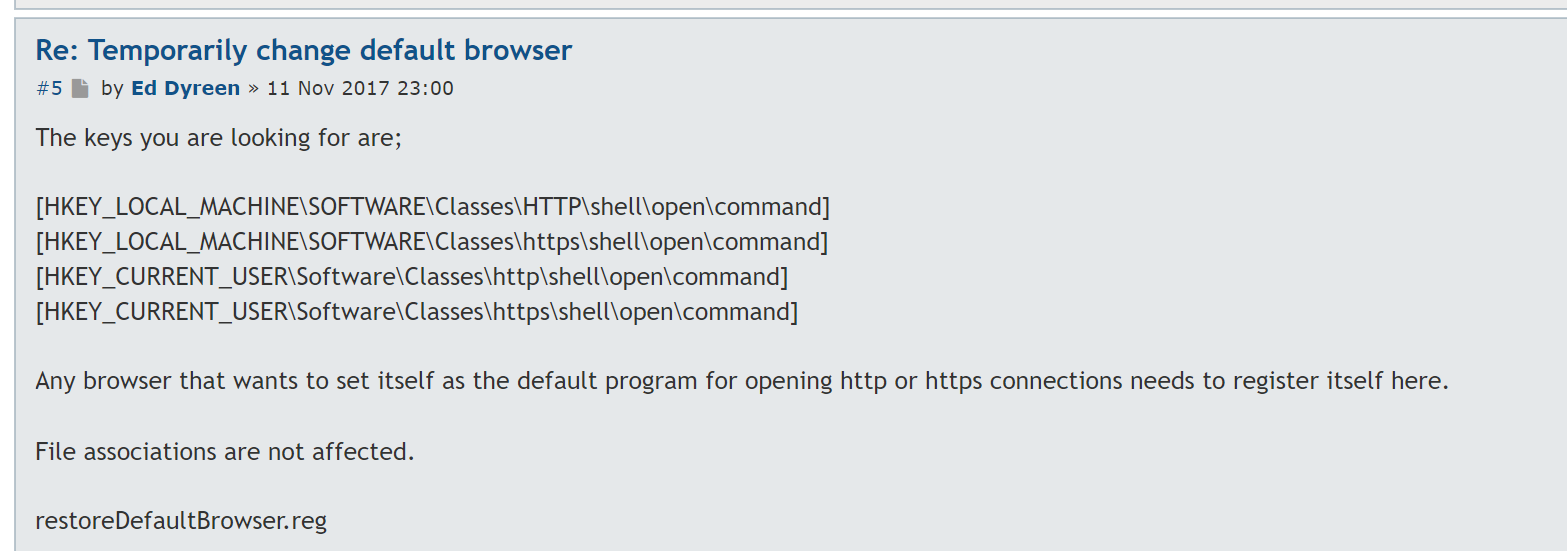


Ta thấy con malware này chỉ import mỗi thư viện kernel32.dll và xài mỗi function ExitProcess của thư viện này. Điều này thật vô lý, vì chỉ xài mỗi API ExitProcess thì chẳng làm được gì cả. Rất có thể file malware này đang bị pack và ẩn đi mã nguồn mà vì thế tất cả thư viện được import có thể đucợ bung ra khi chương trình đang chạy.

Kế tiếp ta thực hiện thêm một bước static nữa trước khi thực hiện dynamic. Sử dụng strings để xem một số chuỗi có trong file binary này.



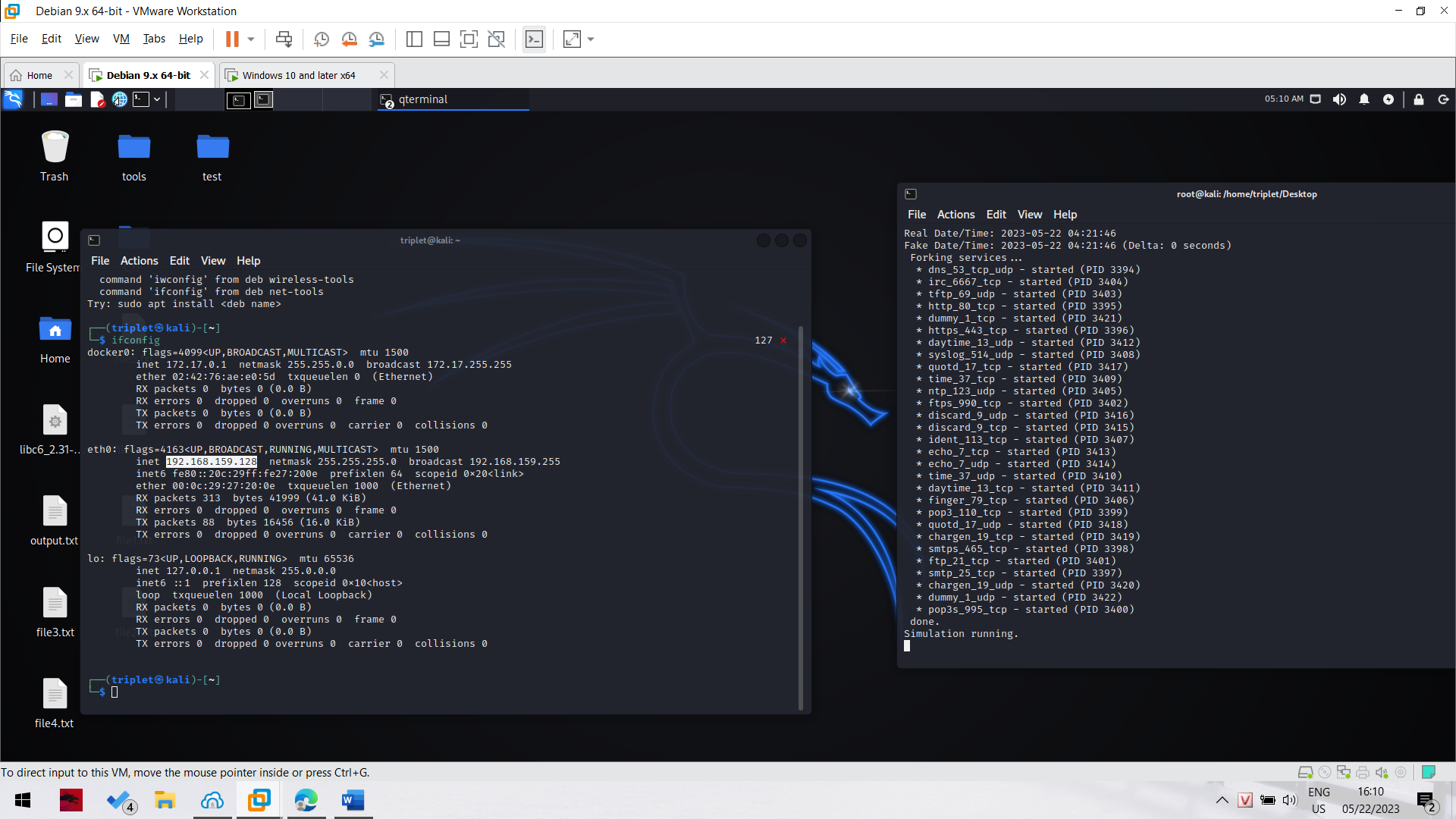
Ta thấy có khá nhiều đoạn strings khả nghi ở đây.

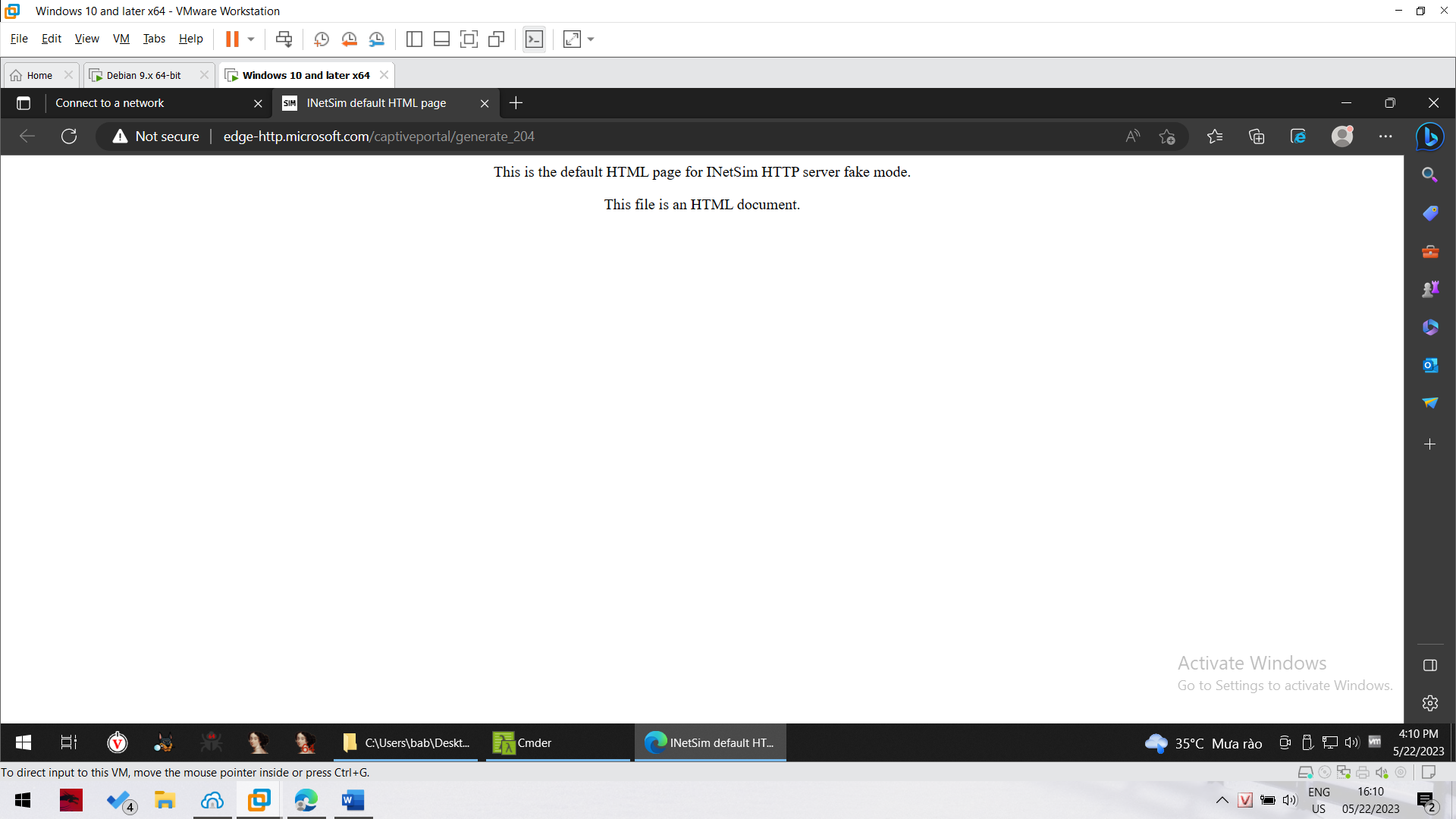
Em đặc biệt chứ ý đến đoạn “SOFTWARE\Classes\http\shell\open\commandV” nên thực hiện google một chút. Ta được kết quả như sau

Có một điều kỳ lạ ở đây so với phỏng đoán ban đầu của chúng ta. Nếu file bị pack thì không thể nào mà ta coi được các đoạn strings rõ như thế này được.

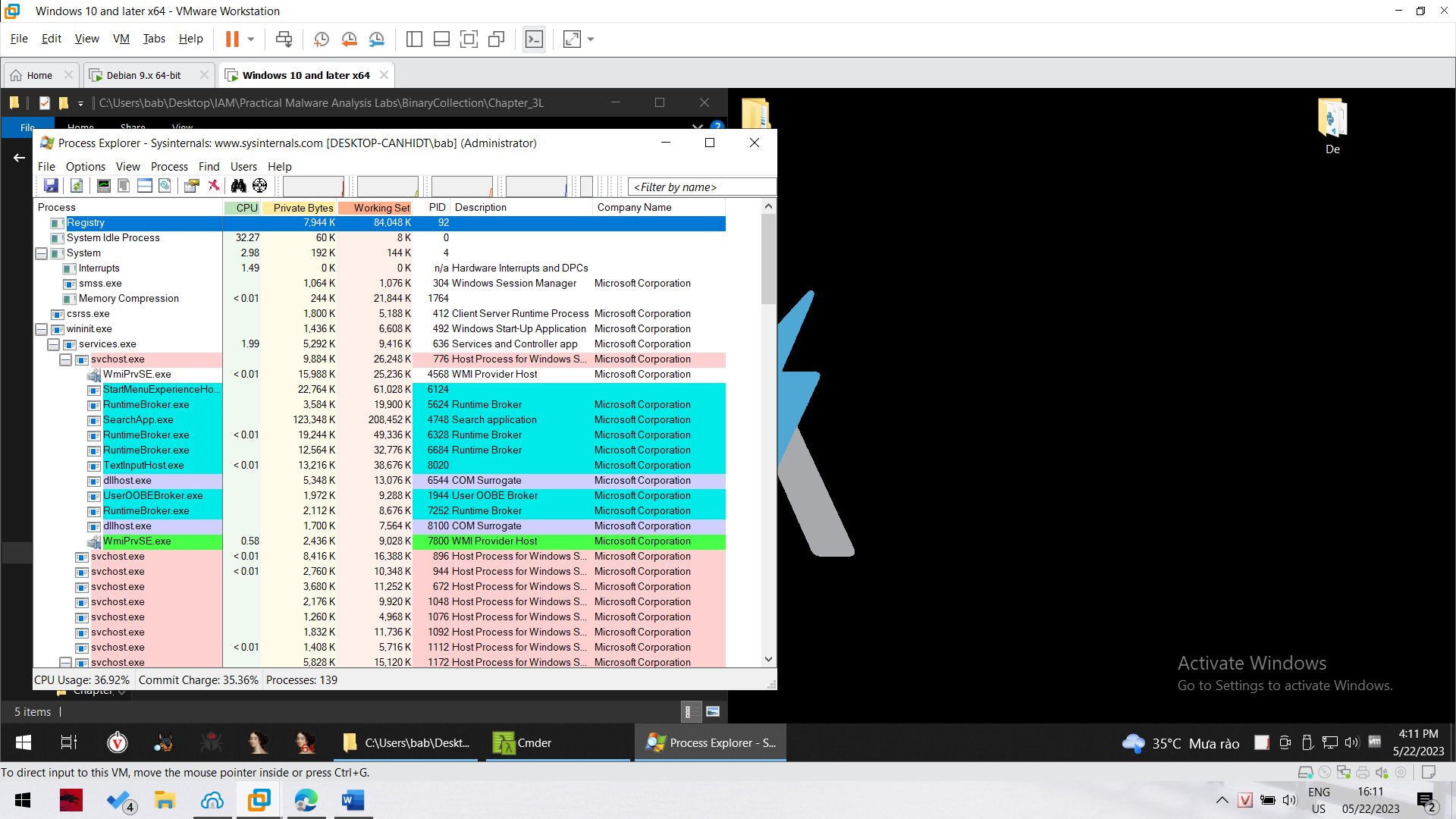
Bây giờ ta sẽ tiến hành chuẩn bị cho quá trình basic dynamic analysis.

Đầu tiên bật inetsim lên.

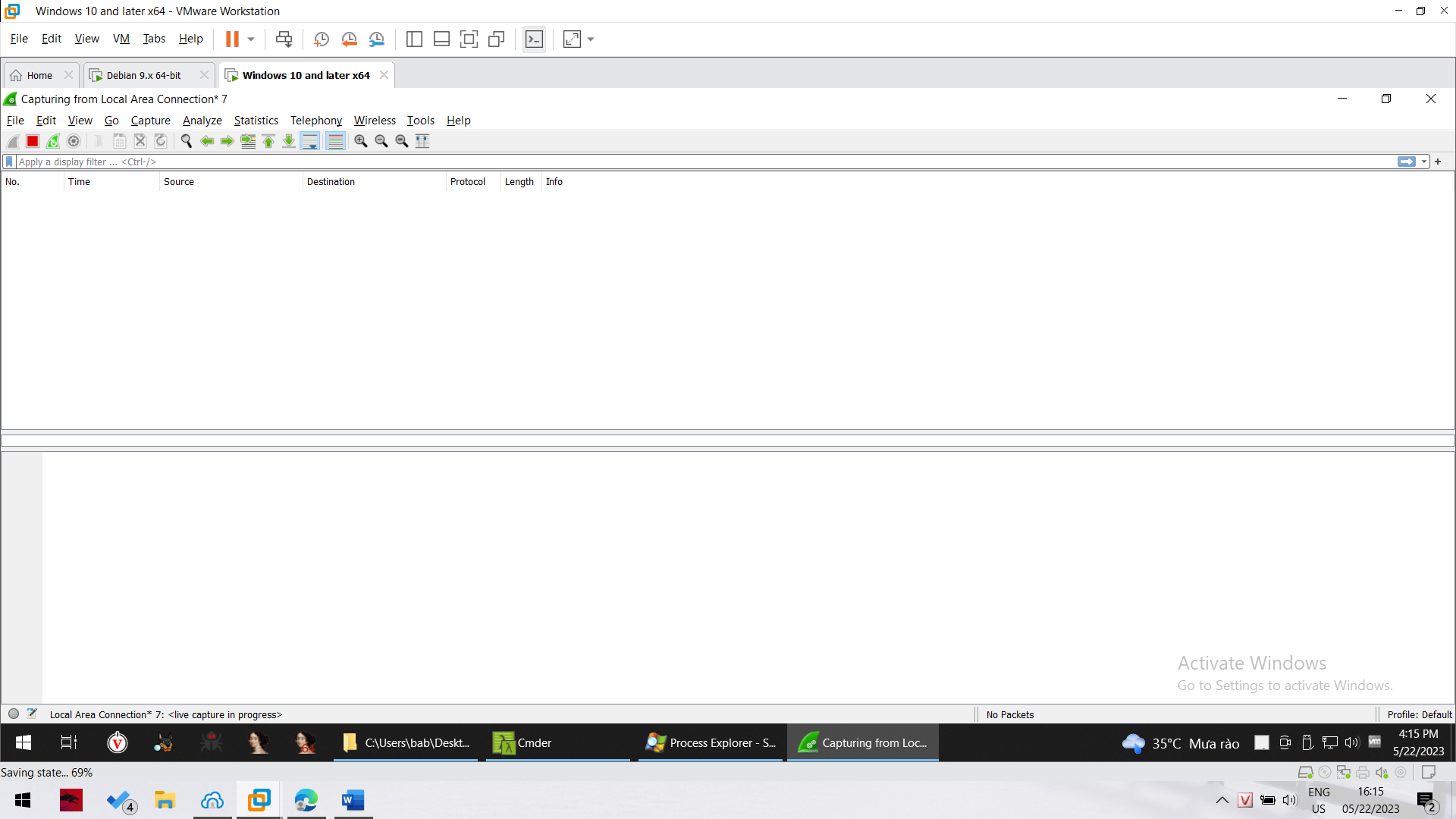




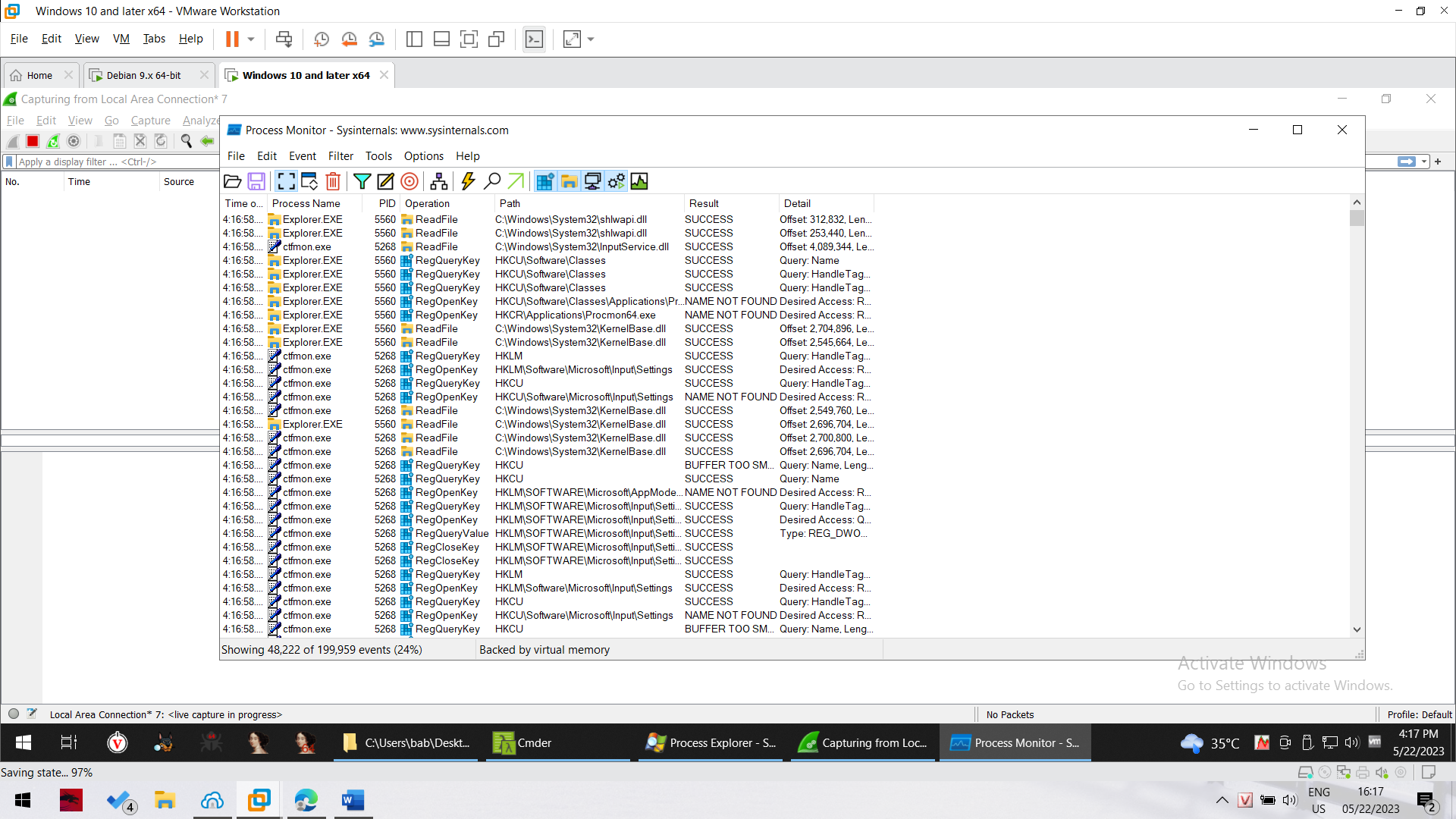
Tiếp theo ta chạy process explorer.



Tiếp theo ta chạy wireshark và thực hiện capture trên “Local Area Connection”



Tiếp theo ta bật Process Monitor



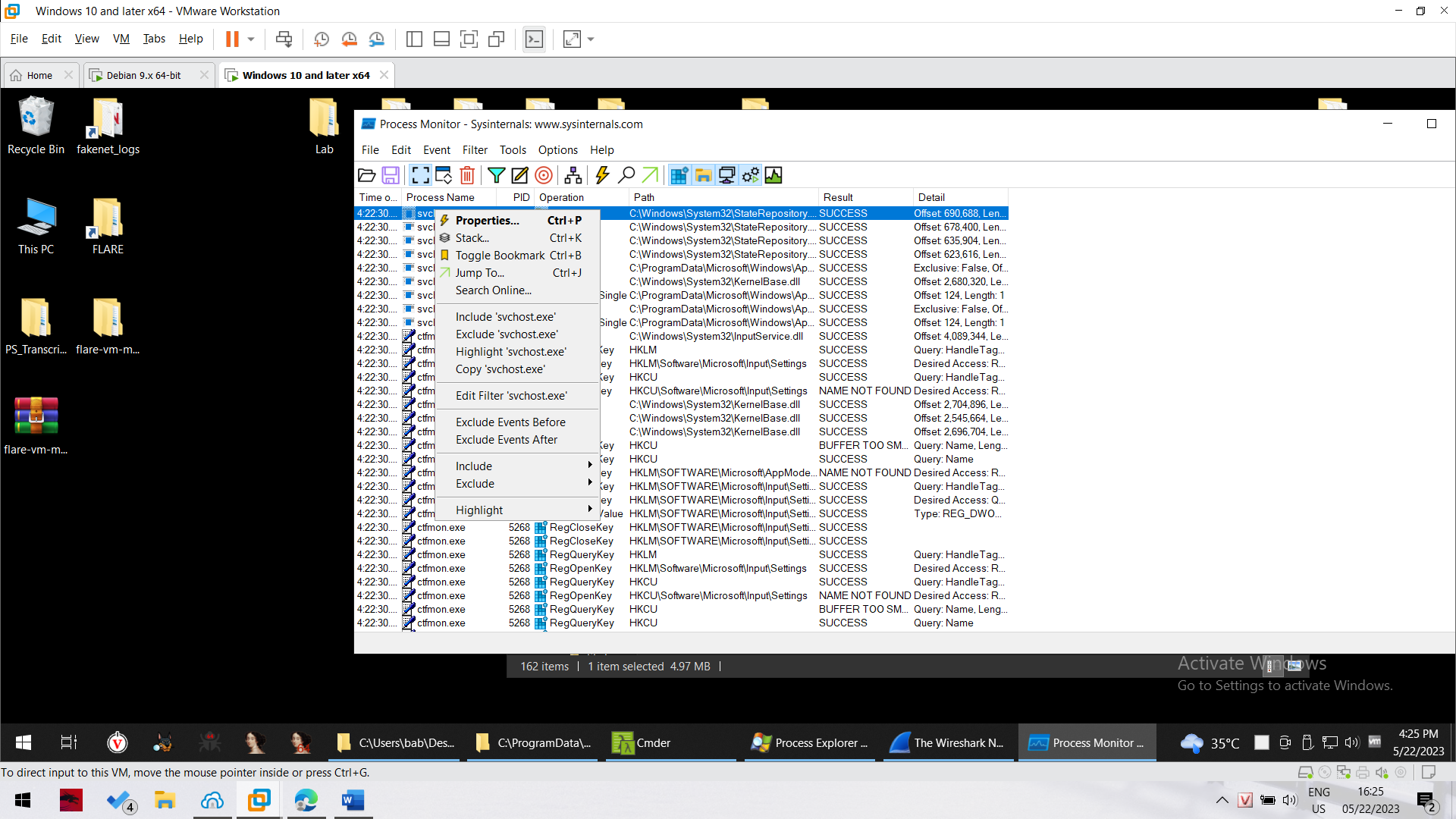
Bây giờ ta sẽ loại bỏ các tiến trình phụ, đã chạy sẵn trước khi chạy con malware này để dễ dàng thực hiện quá trình phân tích này hơn.

Những process sẽ thực hiện exclude là csrss.exe, explorer.exe, services.exe,

vmtoolsd.exe, iexplore.exe, VMwareTray.exe, verclsid.exe, winlogon.exe, wmiprvse.exe, wuauclt.exe, regshot.exe, spoolsv.exe, alg.exe, rundll.exe, WMIADAP.EXE,

GoogleUpdate.exe, GoogleCrashHandler.exe, chromeinstaller.exe, and setup.exe.

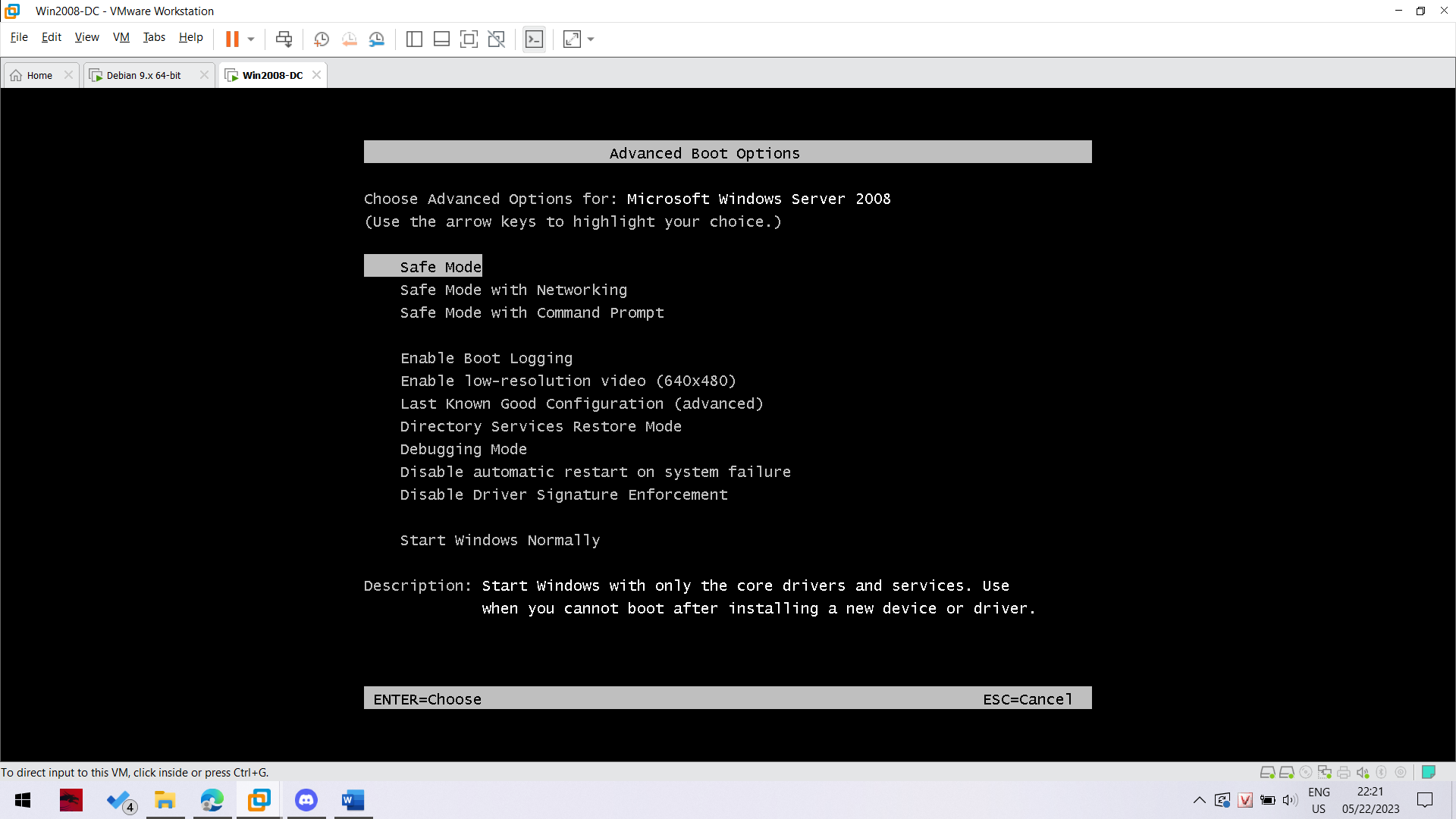
Vậy là ta đã filter hết tất cả những process không cần thiết.

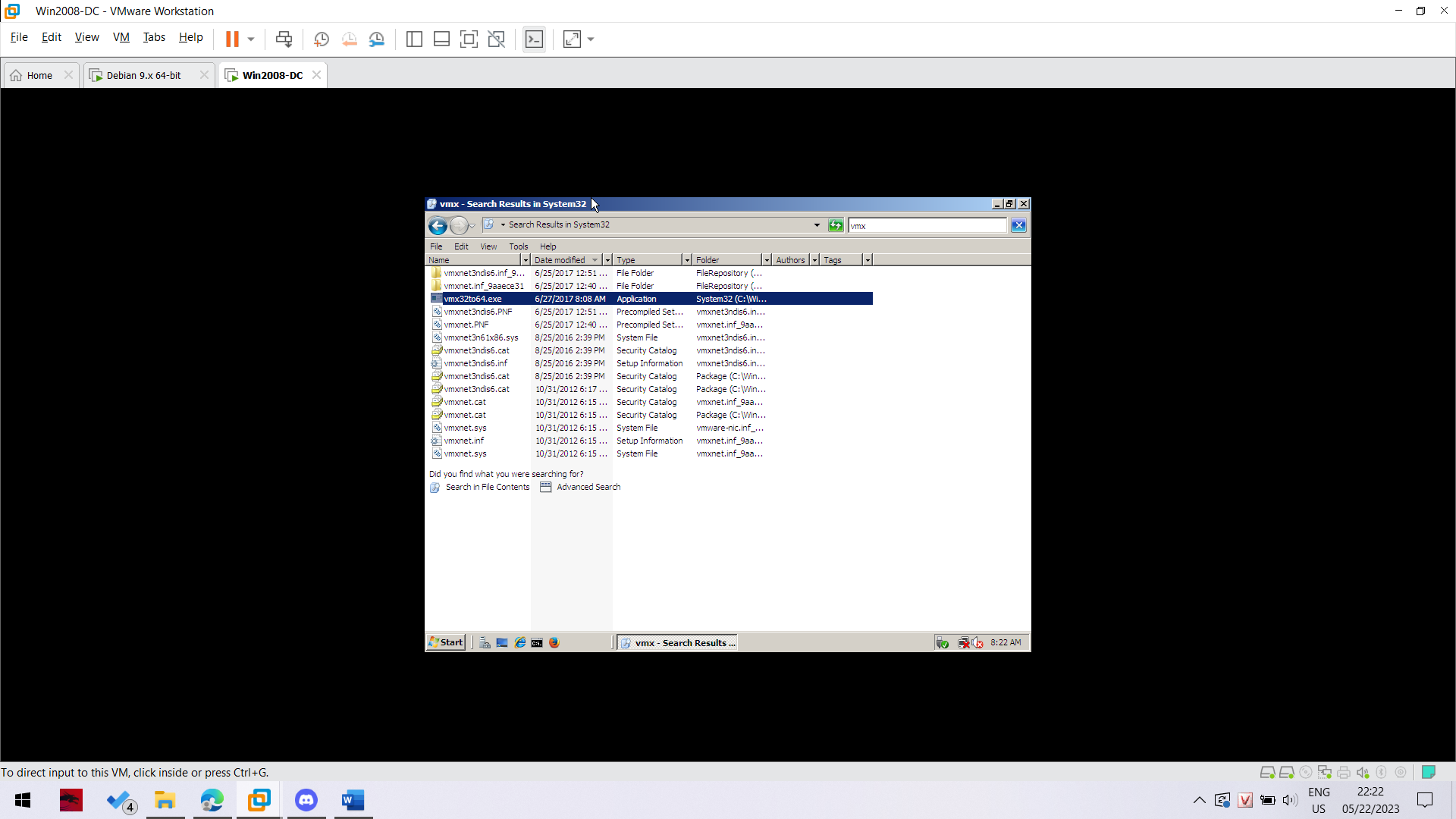


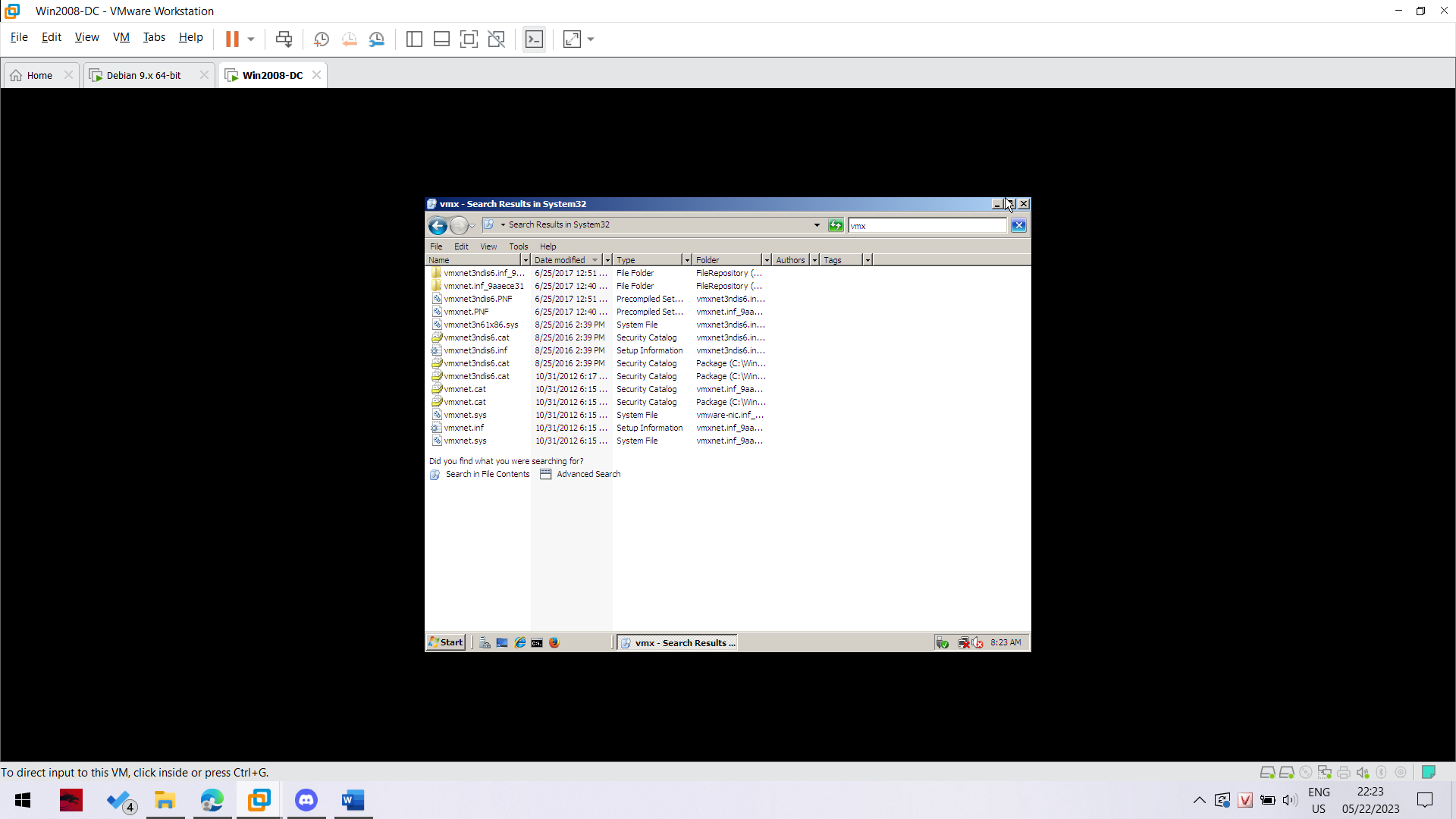


Bây giờ ta sẽ tiến hành xóa file vmx32to64.exe để nó hiện file malware này lên màn hình process monitor.

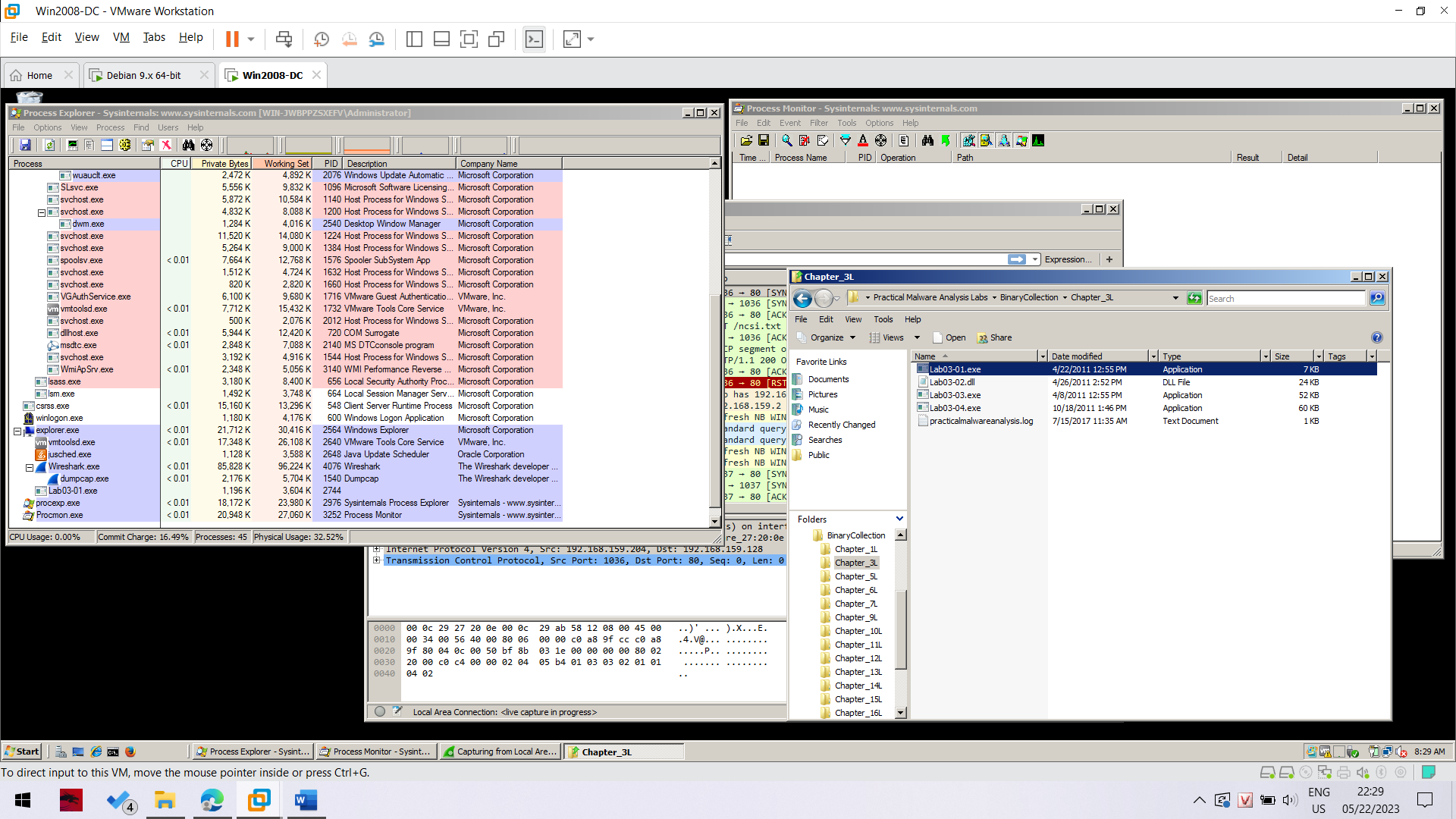
Tuy nhiên trên máy windows 2008 này ta không làm vậy được mà phải vào safe mode của máy để xóa



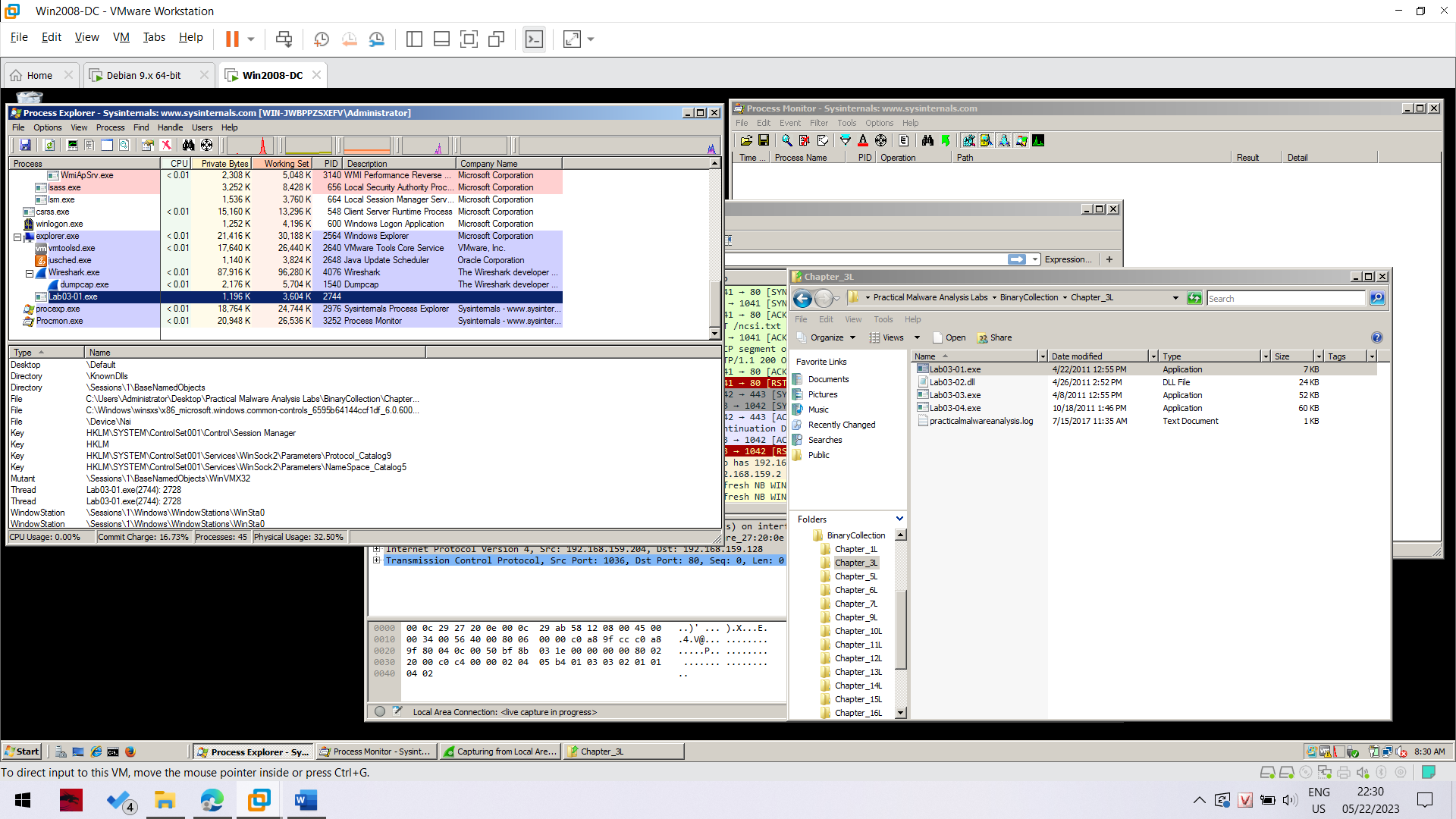


Ta sẽ tiến hành xóa file này đây. Rồi sau đó khởi động lại máy với normal mode như bình thường. 

Chuẩn bị sẵn sàng bộ công cụ để tiến hành phân tích động malware.

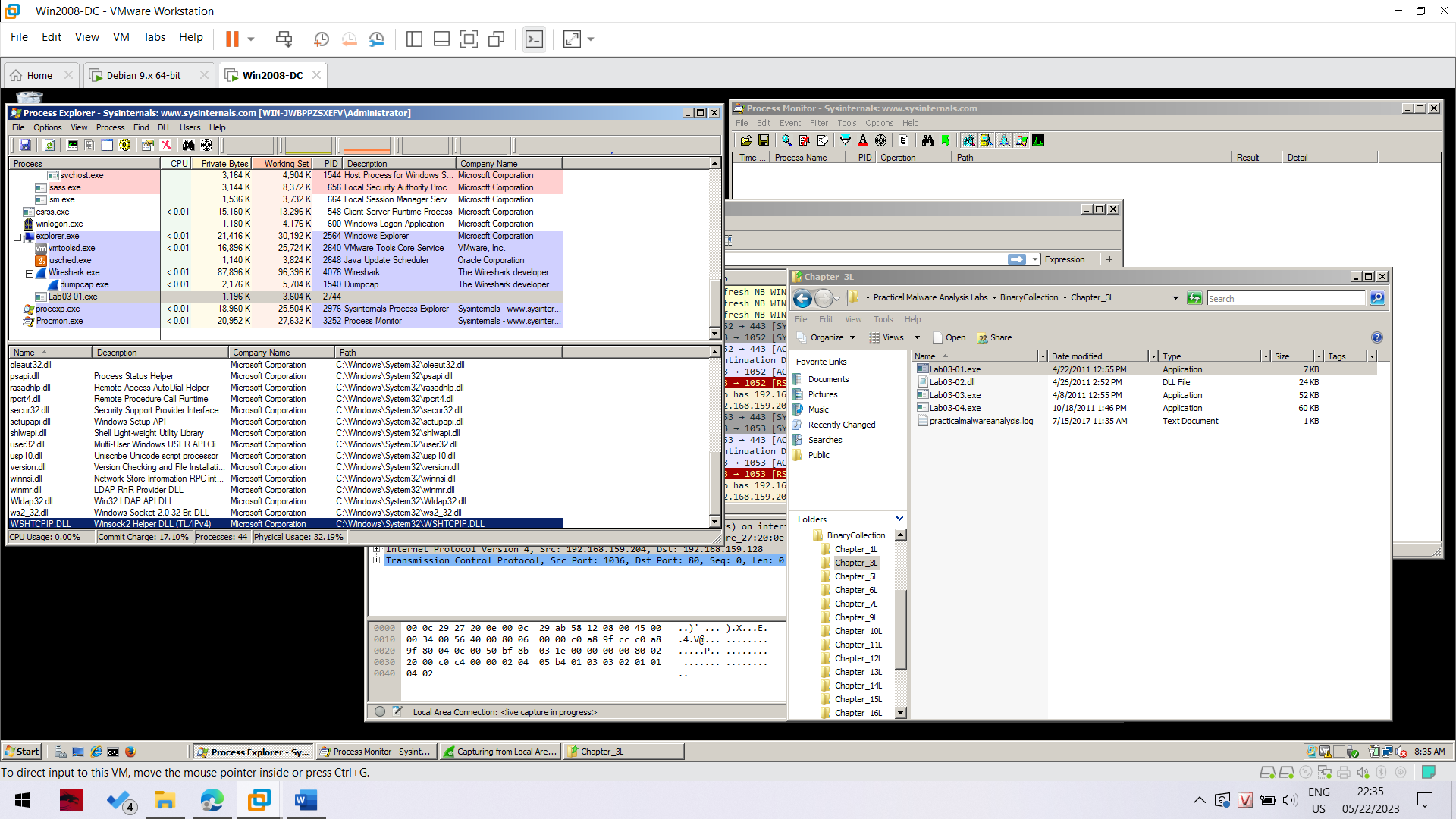


Ta có thể thấy sau khi chạy con malware này thì Process Monitor đã bắt được thông tin của process Lab03-01.exe này.

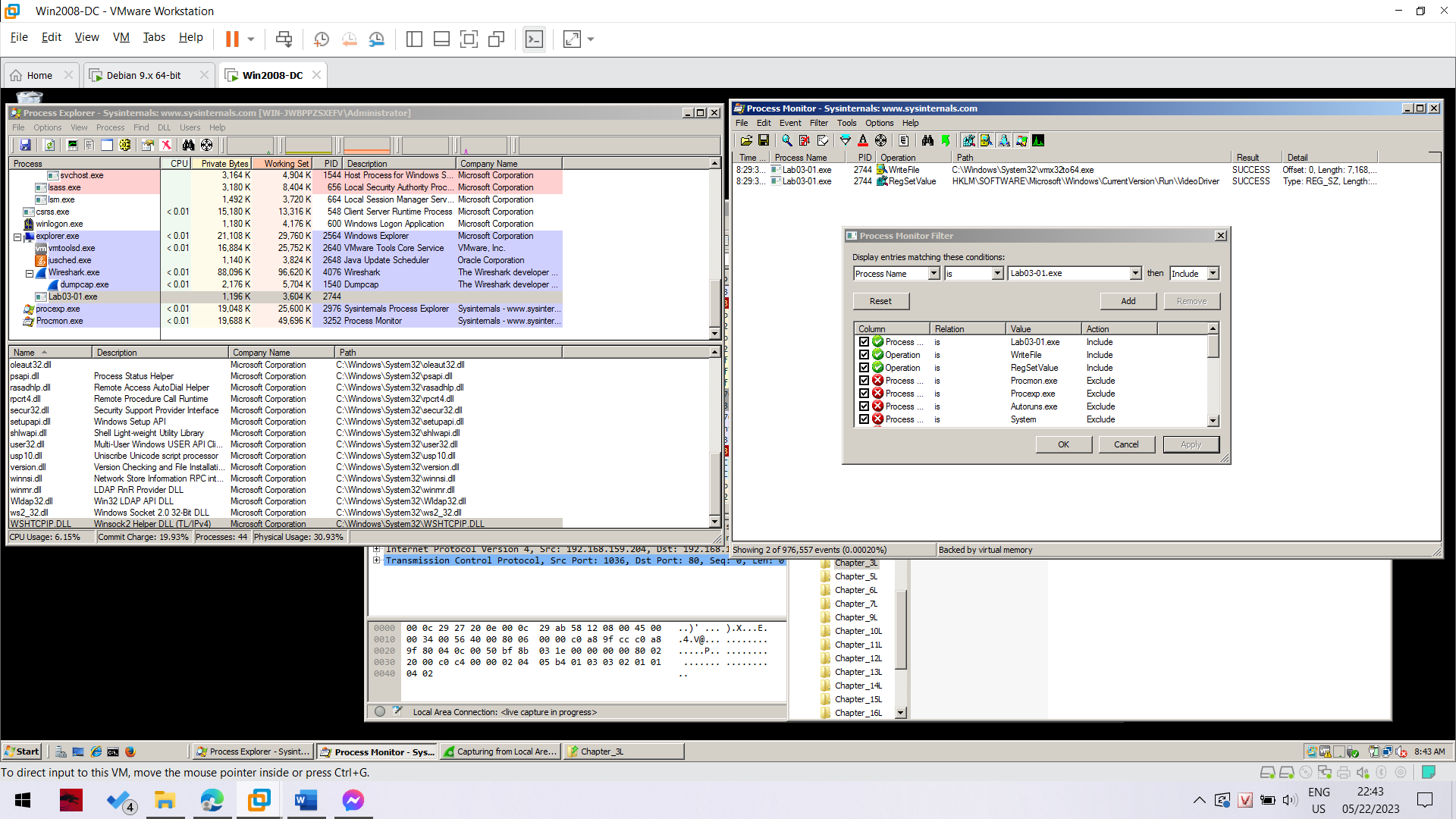


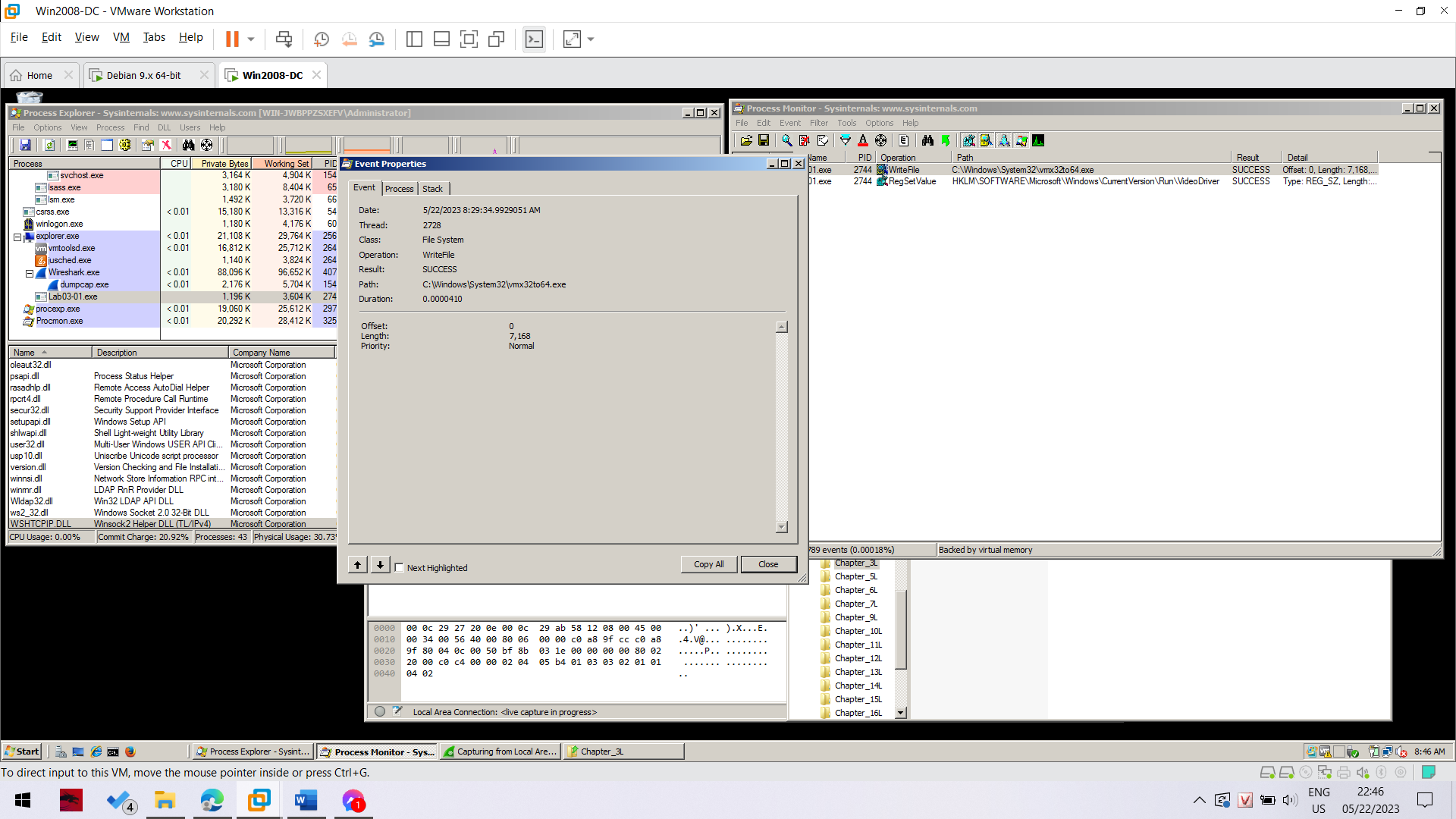
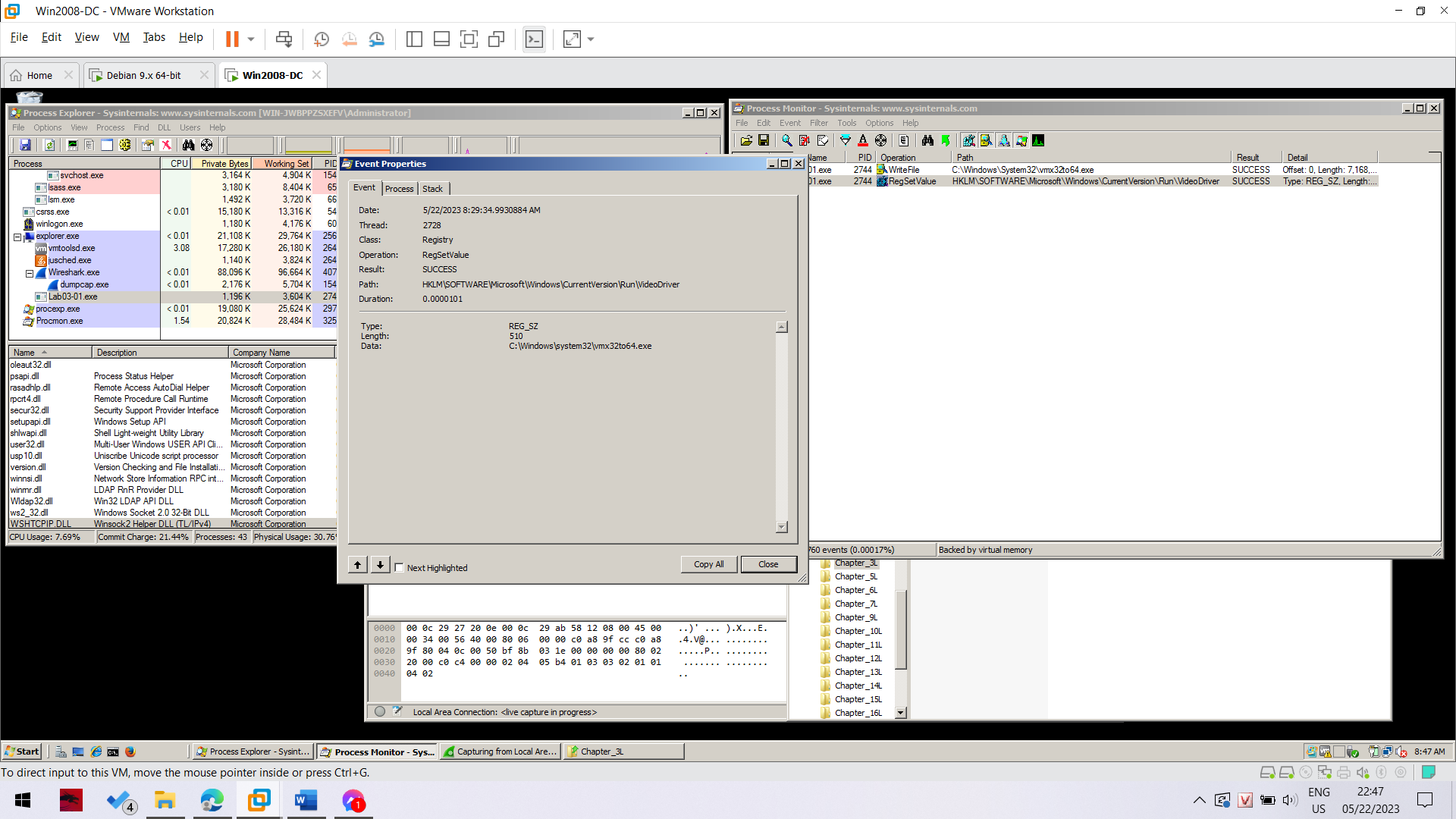
Nhấn vào xem Handles của con malware này, ta có thể thấy ở phần mutant có name là WinVMX32. Có nghĩa là con malware này nó đang giả tên WinVMX32.

Chuyển sang xem chế độ DLLs.



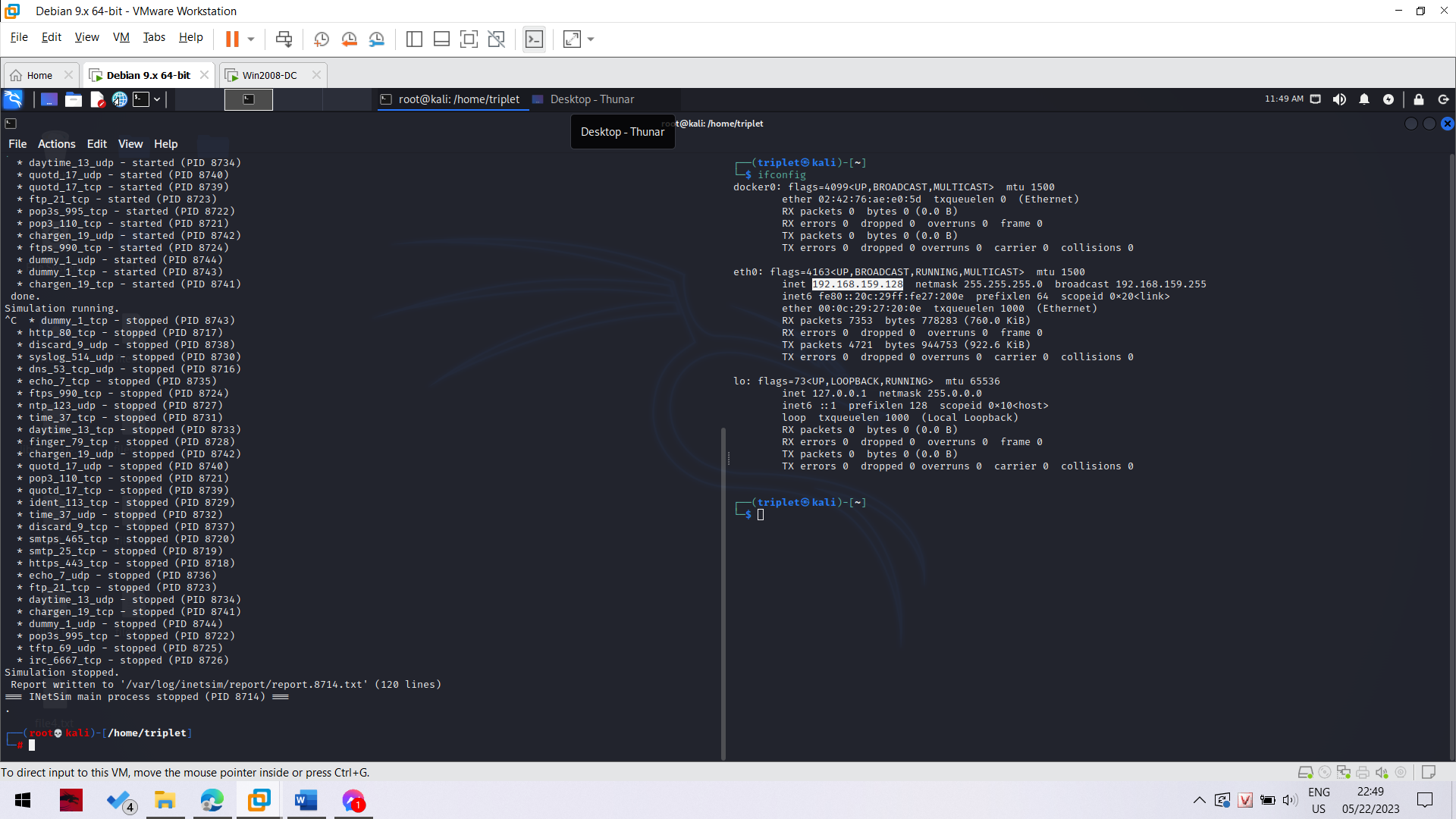
Ở cửa sổ này ta có thể thấy tất cả các DLLs được con malware này sử dụng khi runtime. Ở đây ta đã lý giải được lý do ban đầu tại sao mà chỉ có kernel32.dll. Bây giờ ta có thể thấy khi chạy chương trình, con malware này đã bung ra hết những DLLs gốc mà nó cần để chạy chương trình.

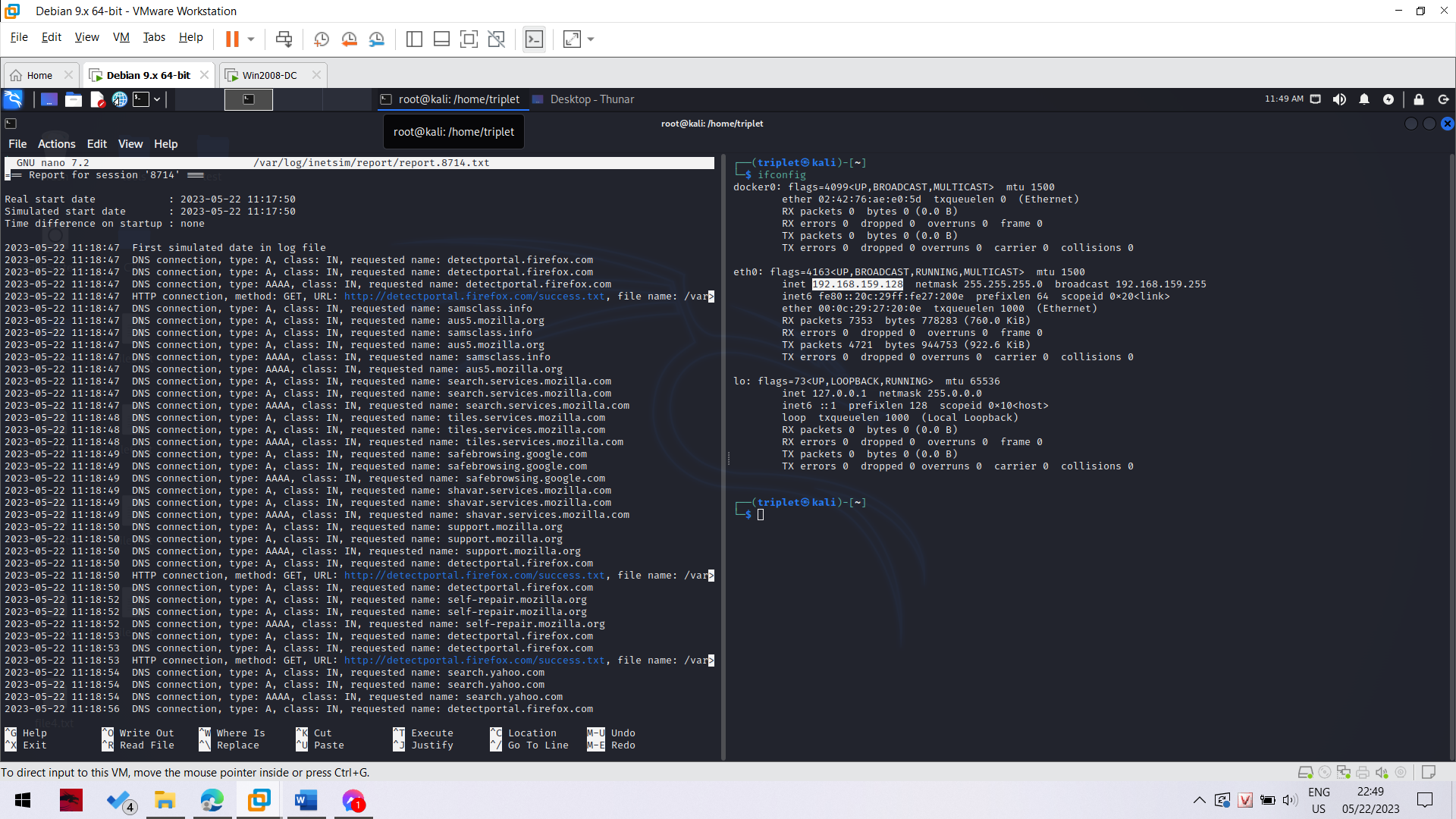
Bây giờ ta chuyển sang xem process này qua process monitor. Ta sử dụng một số filter như hình trên. Apply filter là ra được 2 record của tiến trình Lab03-01.exe.

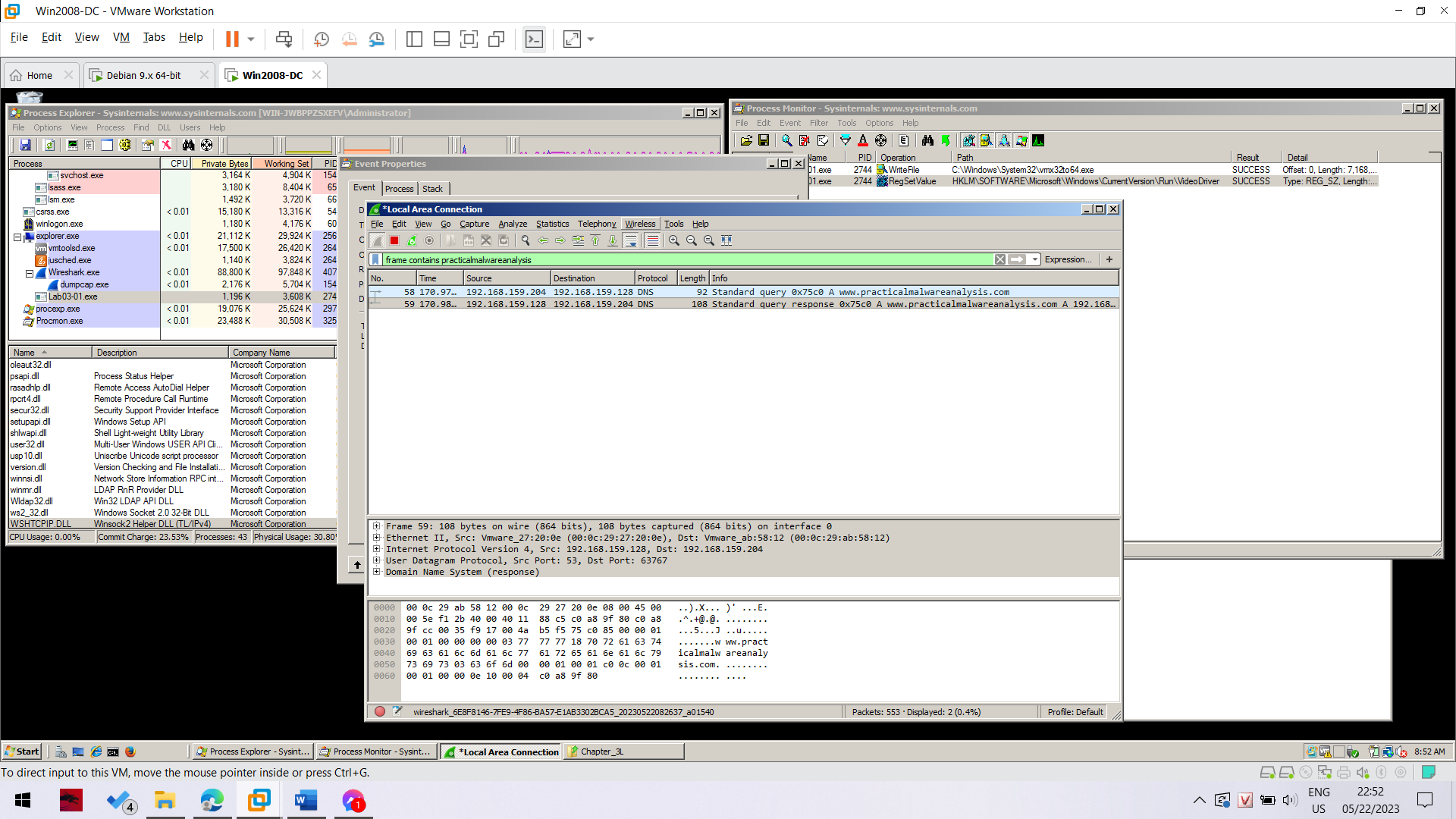
Bấm vào nó ta có thể xem được thông tin chi tiết thằng malware này nó làm cái gì. Có thể thấy ở operation đầu tiên nó đã tạo một file tên là vmx32to64.exe vào system32 như lúc nãy chúng ta troubleshoot. 

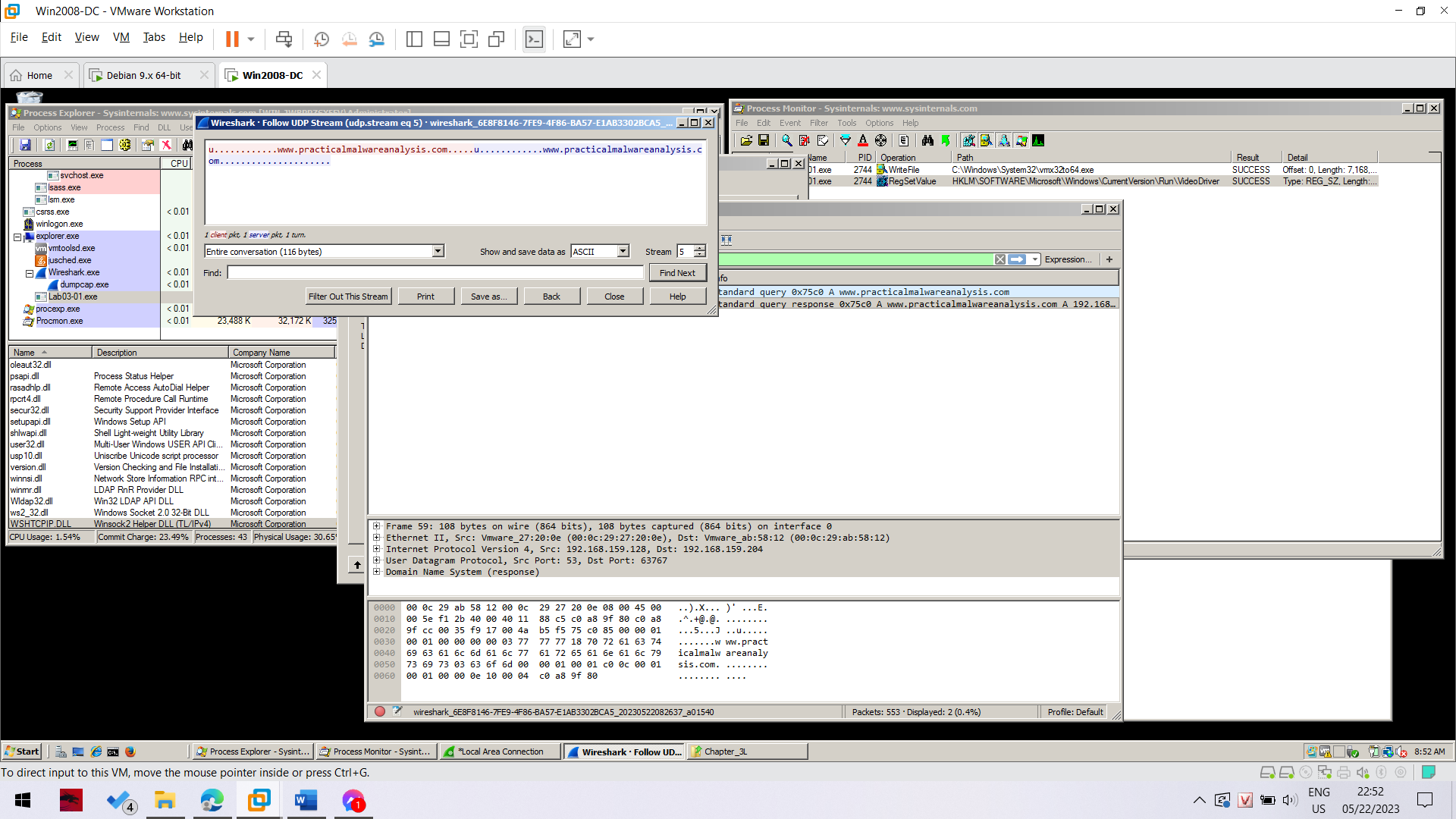
Xem đến operation thứ hai, ta có thể thấy con malware này đang tính gắn một giá trị vào registry.

Phân tích như vậy đã được tương đối. Ta qua xem log của inetsim để phân tích network base trông như thế nào.

Report được lưu vào file 8714, ta dùng nano mở nó lên.

Ok và đây là rất nhiều lưu lượng mạng ra inetsim đã được ghi lại.

Tiếp theo ta quay lại với máy windows. Tại đây ta check wireshark xem có capture được gì hay ho không. Thì đúng như dự đoán sử dụng filter frame contains practicalmalwareanalysis thì ta thu được 2 packet DNS. 

Xuất hiện một tên miền lạ.

Vậy là ta đã phân tích hoàn thành bài lab này rồi!!!