# LAB 06

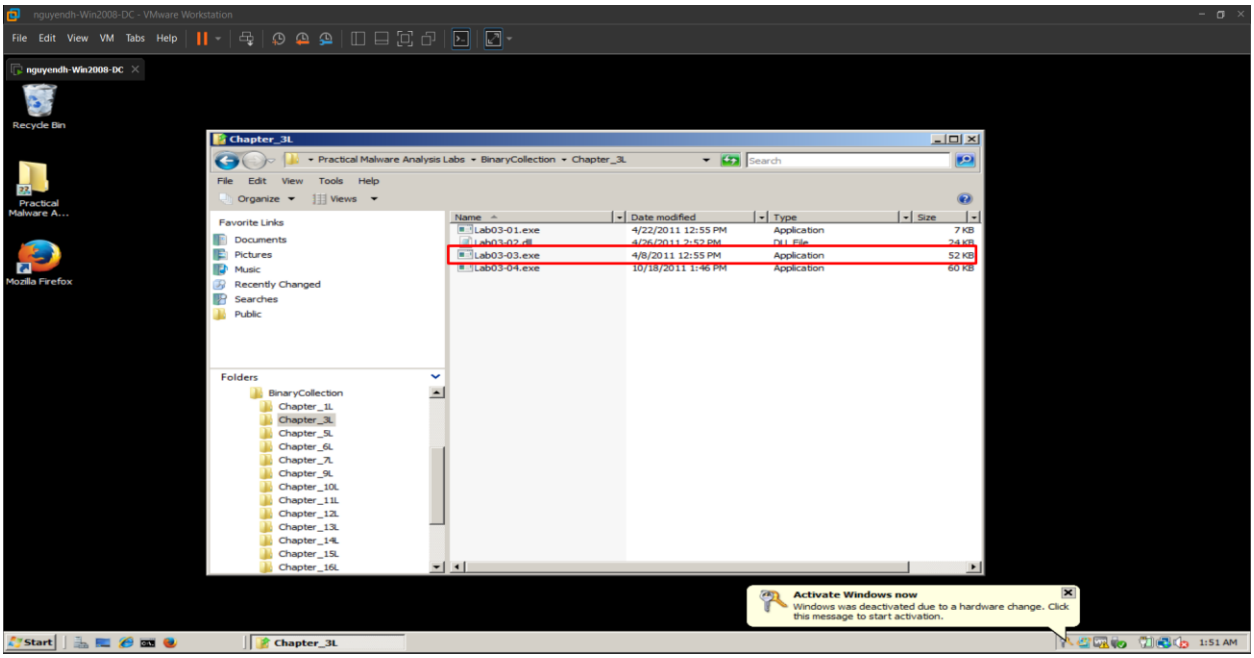
Thầy Mai Hoàng Đỉnh
Trường đại học FPT

Người thực hiện

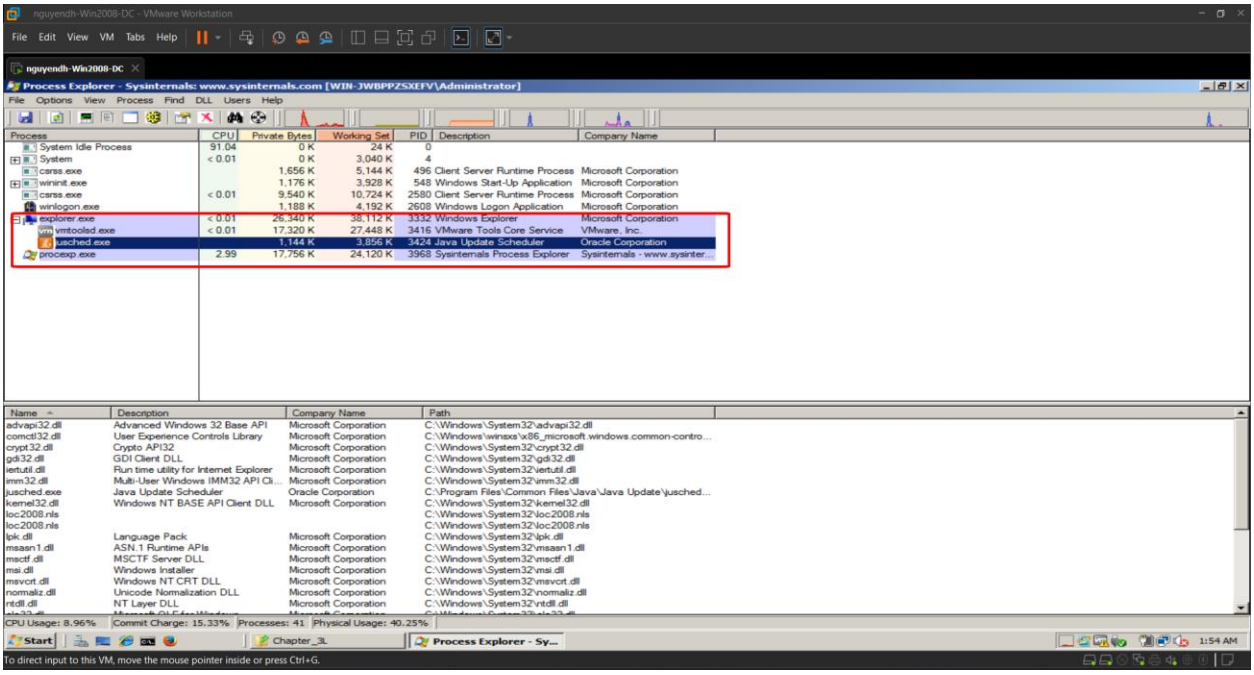
Đặng Hoàng Nguyên

# Keylogger

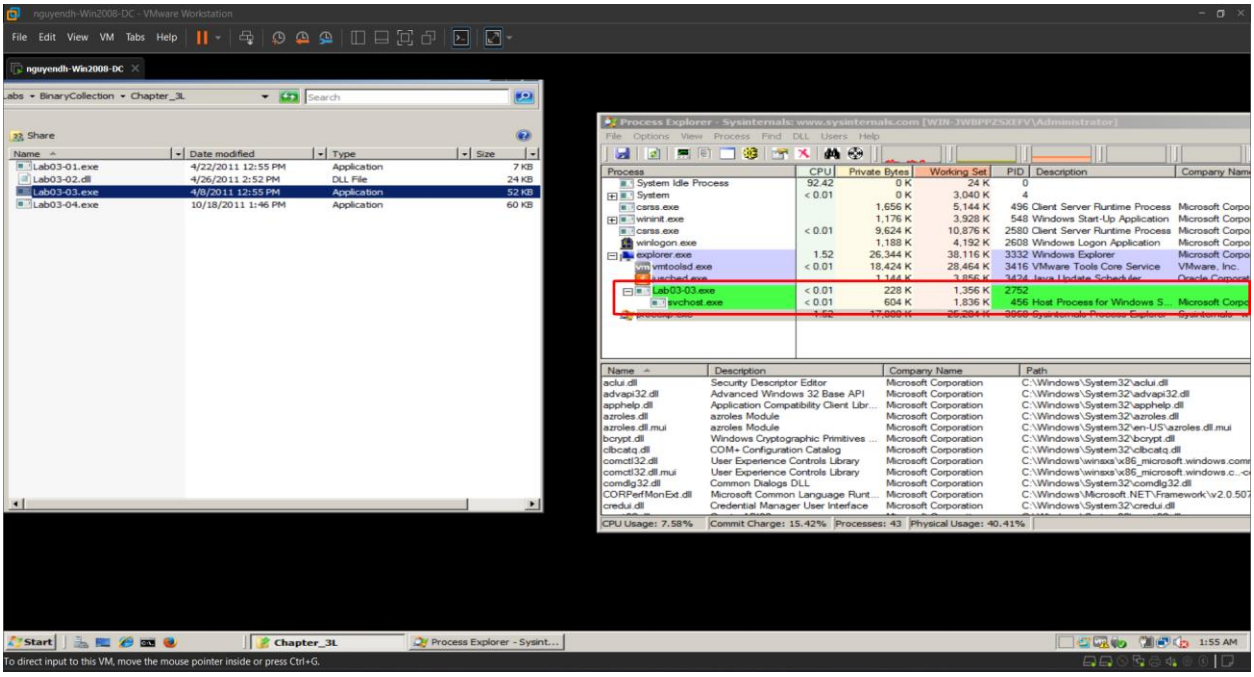
Bước đầu ta cần chuẩn bị con malware, vào bên trong Window Server 2008, mở file "Practical Malware Analysys Labs". Mở "Binary Collection" và Chapter_3L, sau đó ta sẽ thấy một file **Lab3-03.**



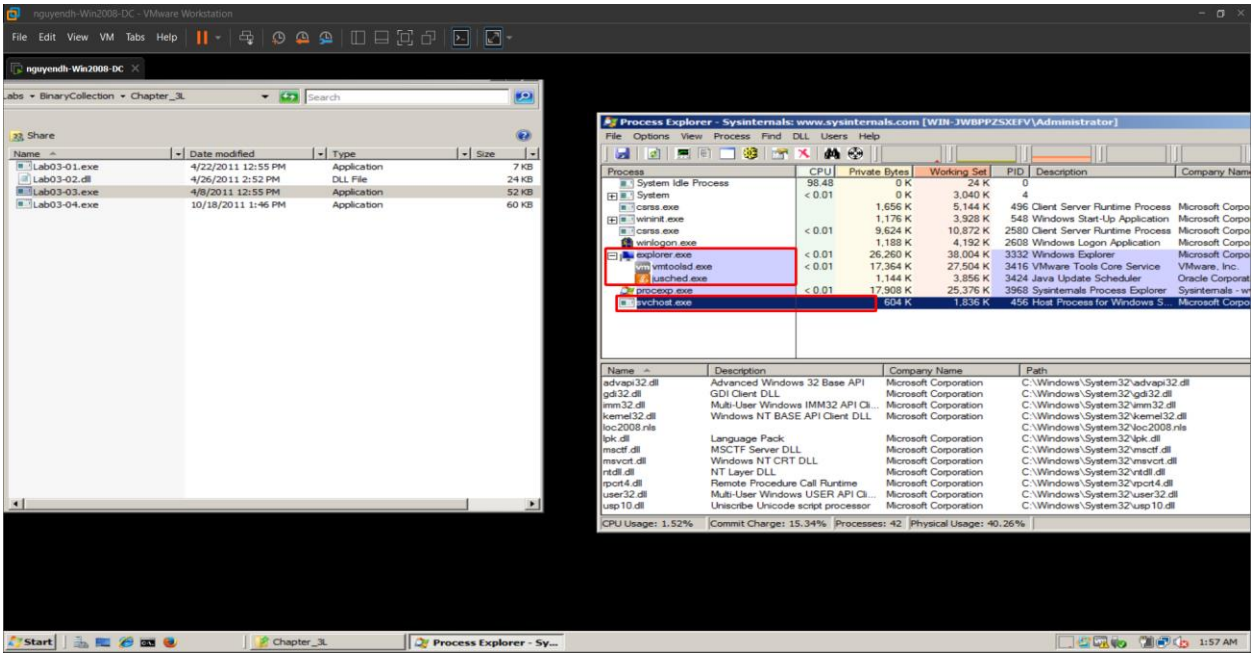

Sau đó mở **Process explorer** để xem các tiến trình đang chạy trước khi mở con virus lên




Sau khi mở Lab03-03.exe ta có thể thấy được rằng nó đã tạo ra một tiến trình con là **svchost.exe**

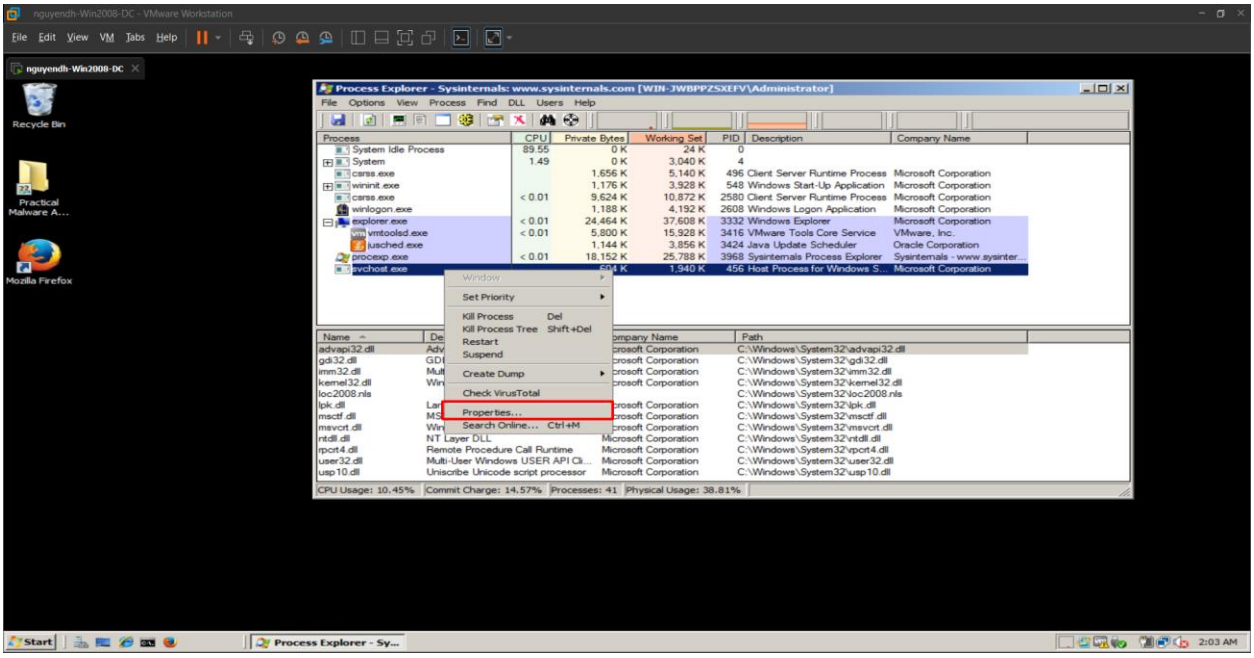


Sau khi tạo ra tiến trình xong, Lab3-03.exe bị terminate ngay lập tức, nhưng thay vì bình thường nếu PPID bị terminate thì PID cũng bị terminate nốt nhưng thay vì đó, svchost.exe được tách ra thành một tiến trình riêng

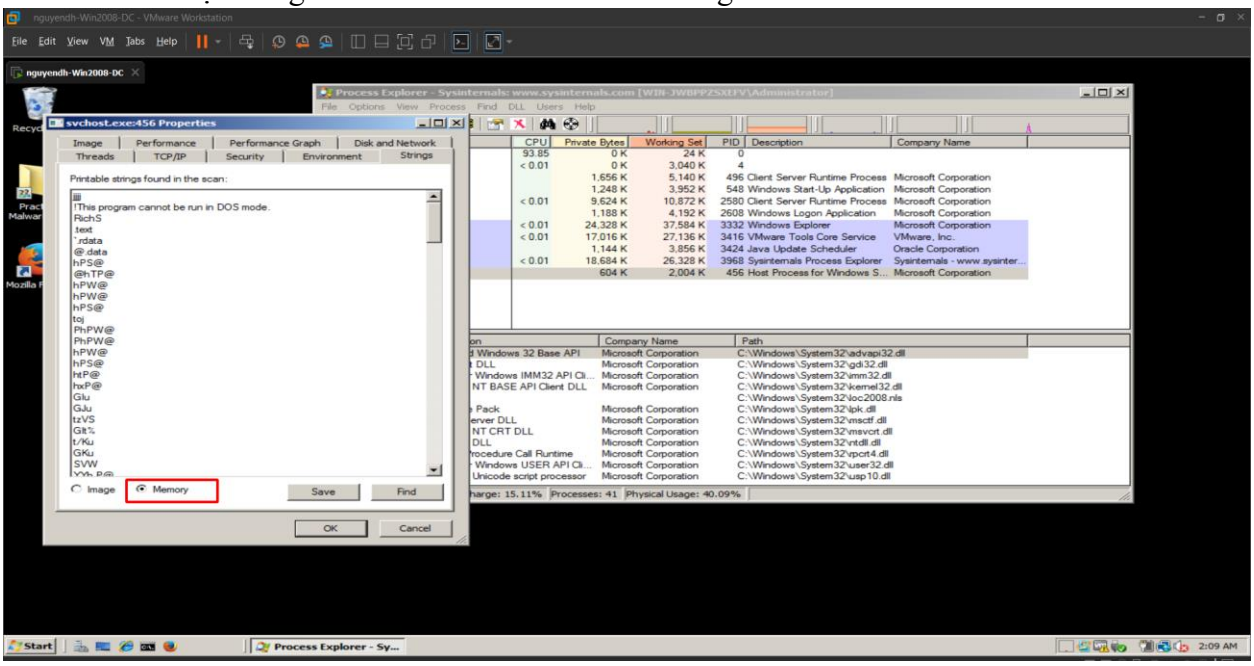


**Observing Process Replacement**

Chúng ta sẽ tiến hành phân tích trên strings của nó bằng cach nhấn **chuột phải vào svchost.exe → chọn vào properties**

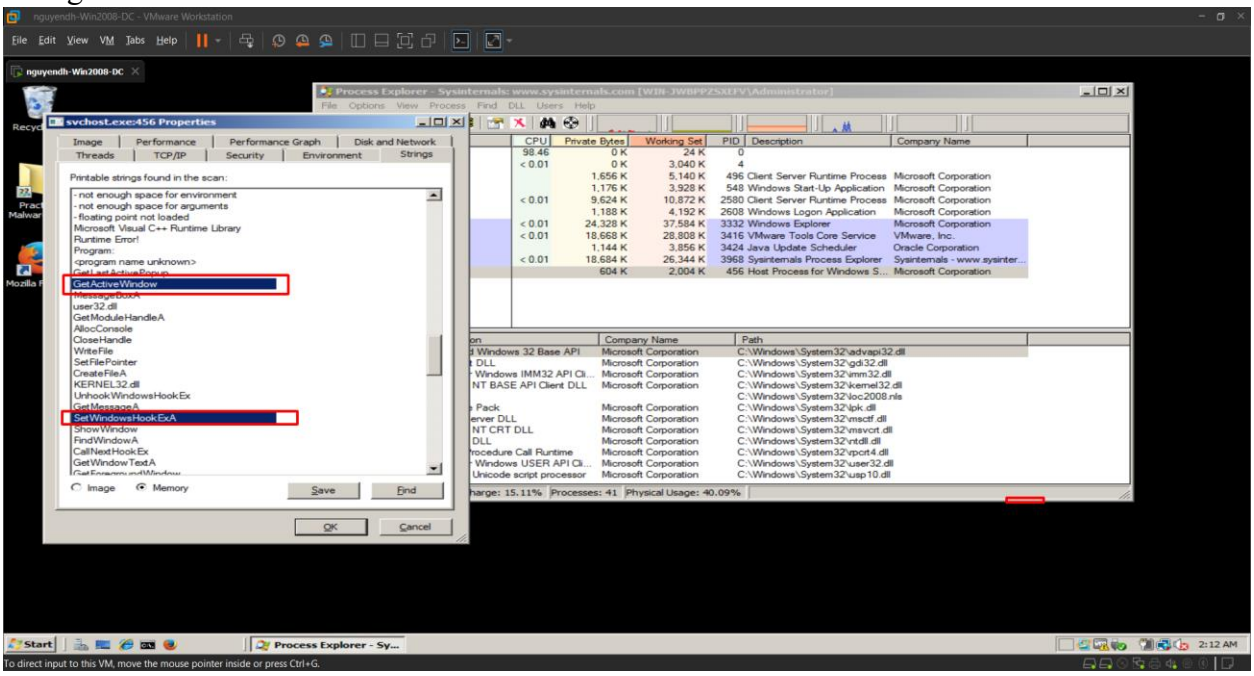



Sau đó nhấn chọn Image ở bên dưới để có thể xem strings của tiến trình

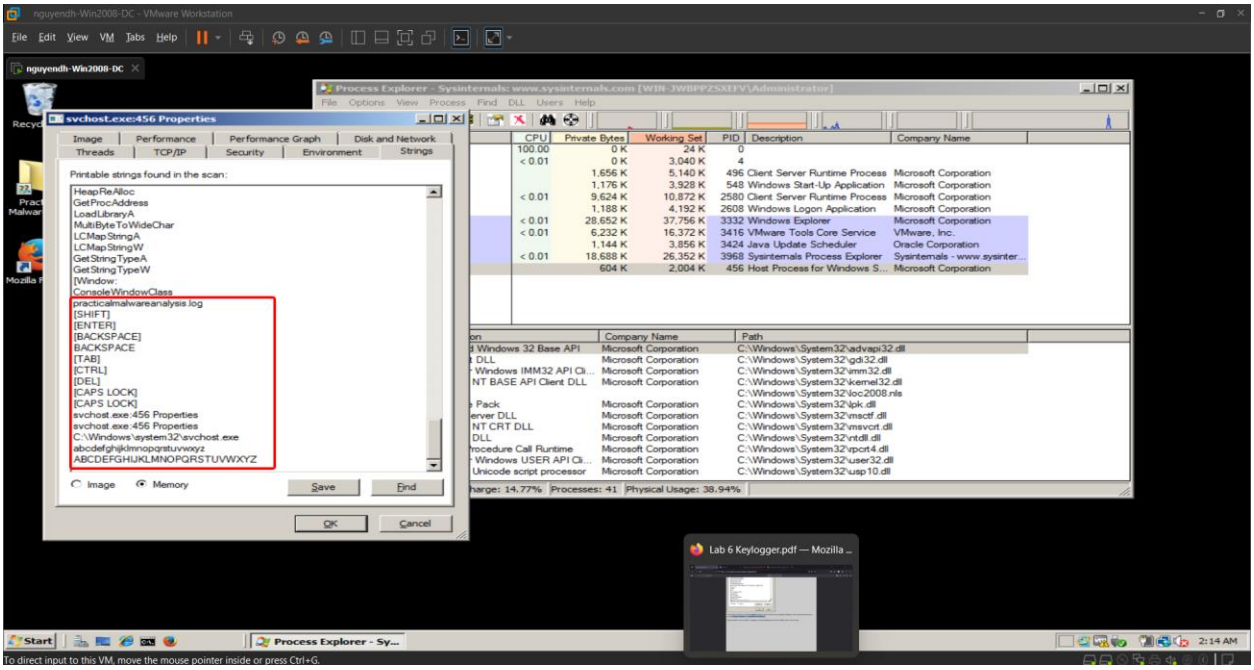



Ở đây chúng ta sẽ quan tới một số thứ như là **GetActiveWindow và SetWindowsHookExA.** Hai hàm này hay được sử dụng trong việc tạo malware keylogger. Đây chỉ là phỏng đoán, chúng ta tiếp tục xem các strings khác để xem có những gì hơn để có thể kết luận đây là keylogger

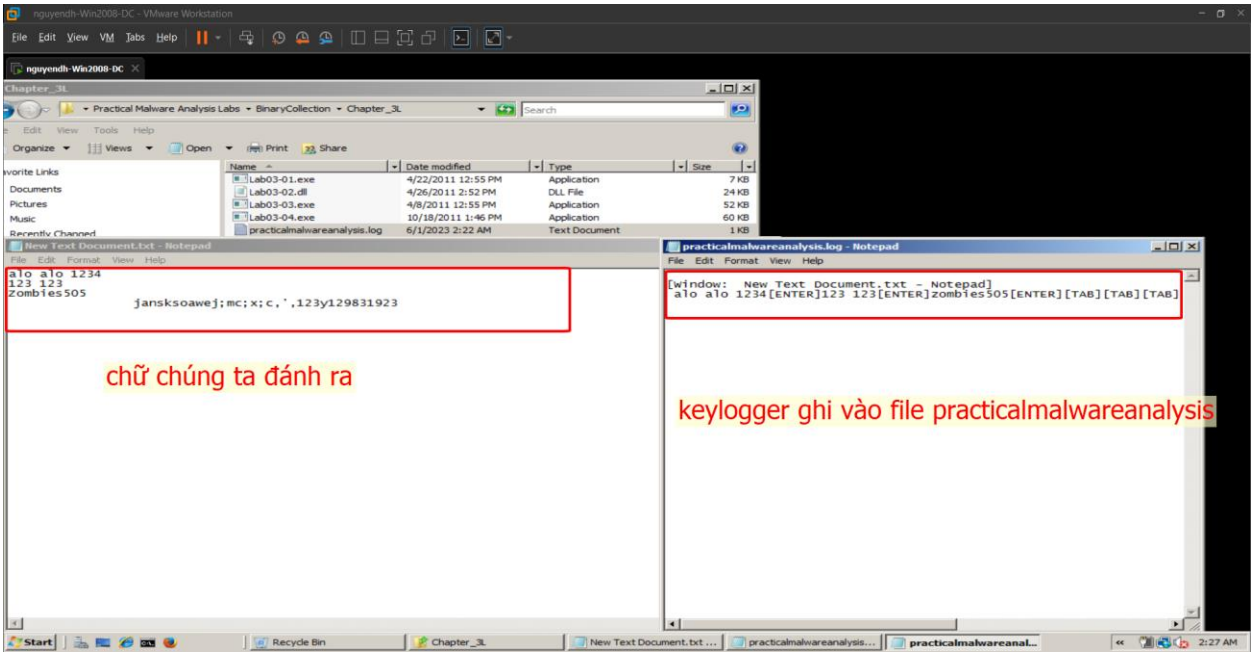
không.




Quả như là chúng ta dự đoán, ở dưới có những thông tin bao gồm những phím trên keyboard như abcdef, các phím chức năng như là shift, tab, cap lock,… và tất cả sẽ được lưu vào bên trong một file được gọi là practicalmalwareanalysis.log

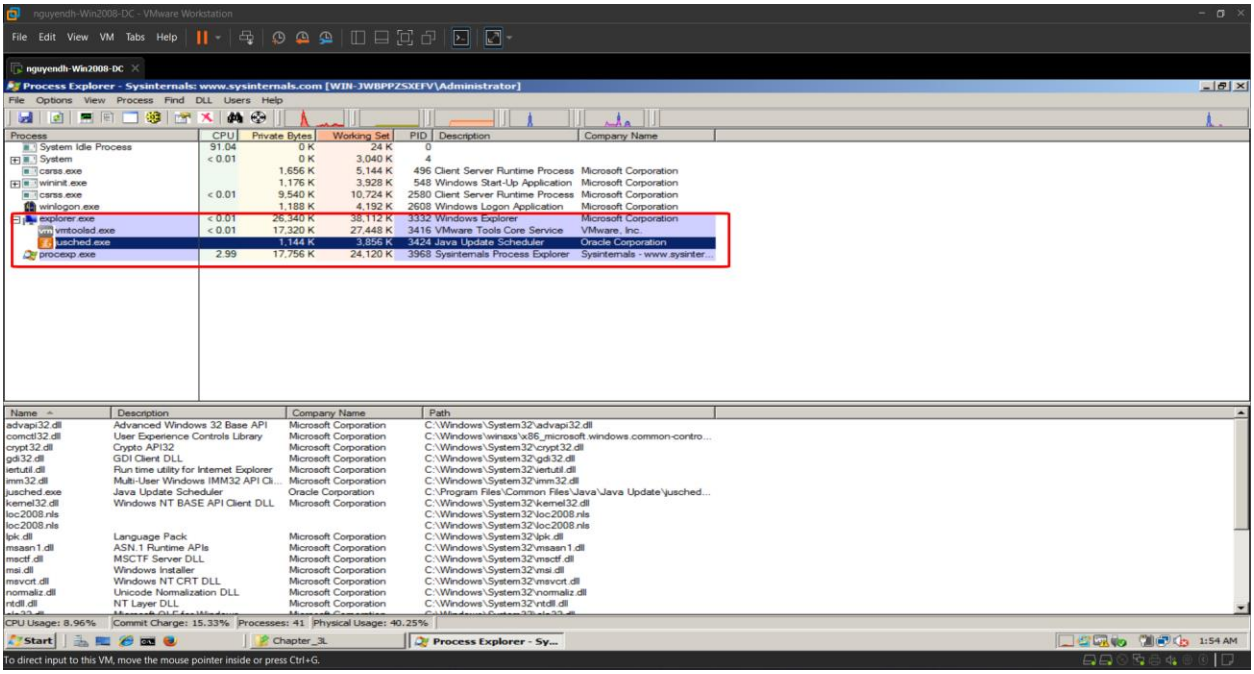



Sau đây là những gì mà diễn ra bên trong file log mà keylogger ghi lại (bên phải)

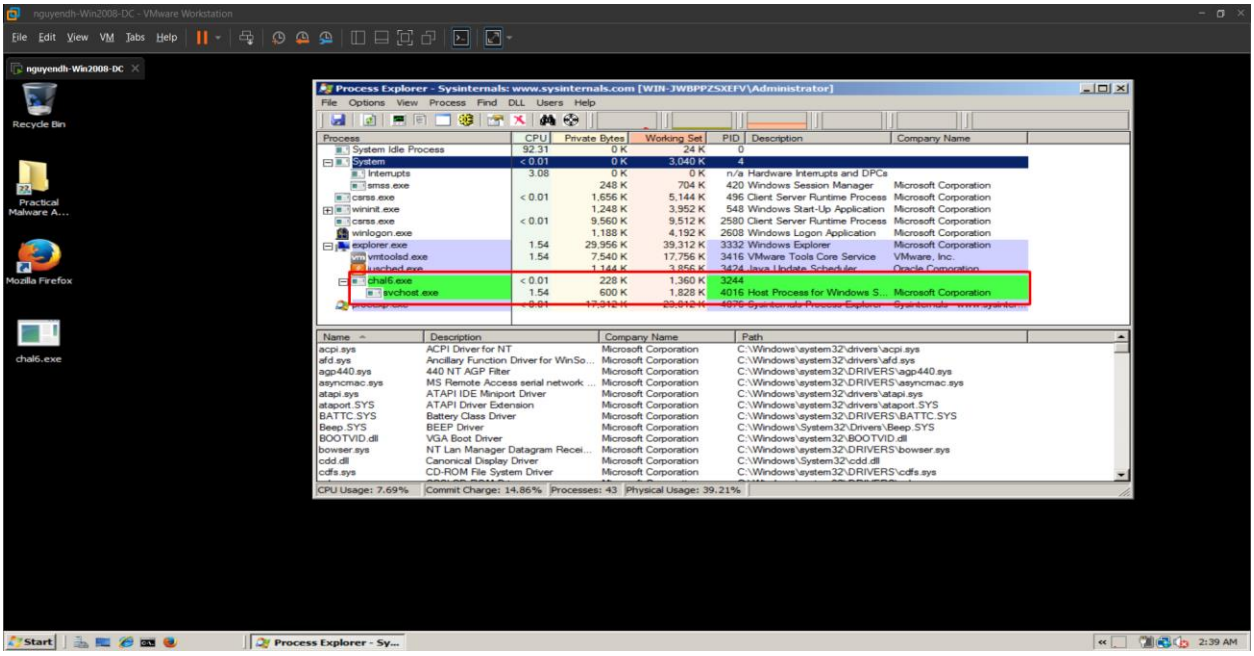



## Find the Logfile

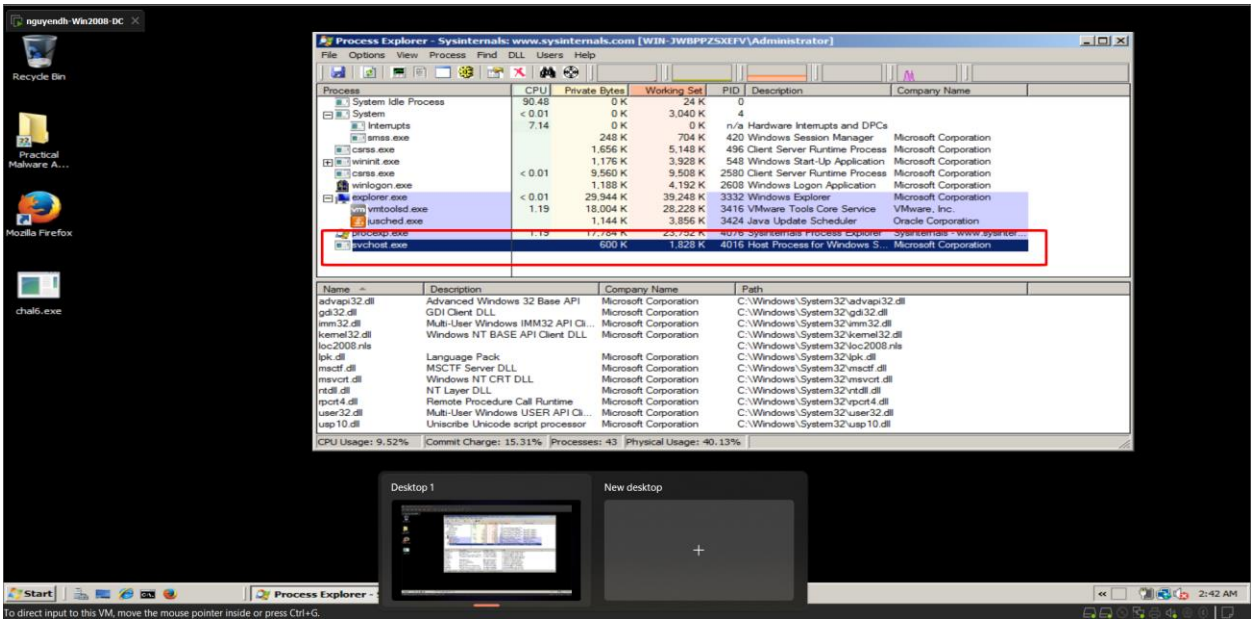
Mở process explorer lên trước để xem các tiến trình trên máy đang chạy bao gồm những gì. Ở đây, ta chỉ cần để ý tới những process được tao ra bởi explorer.exe



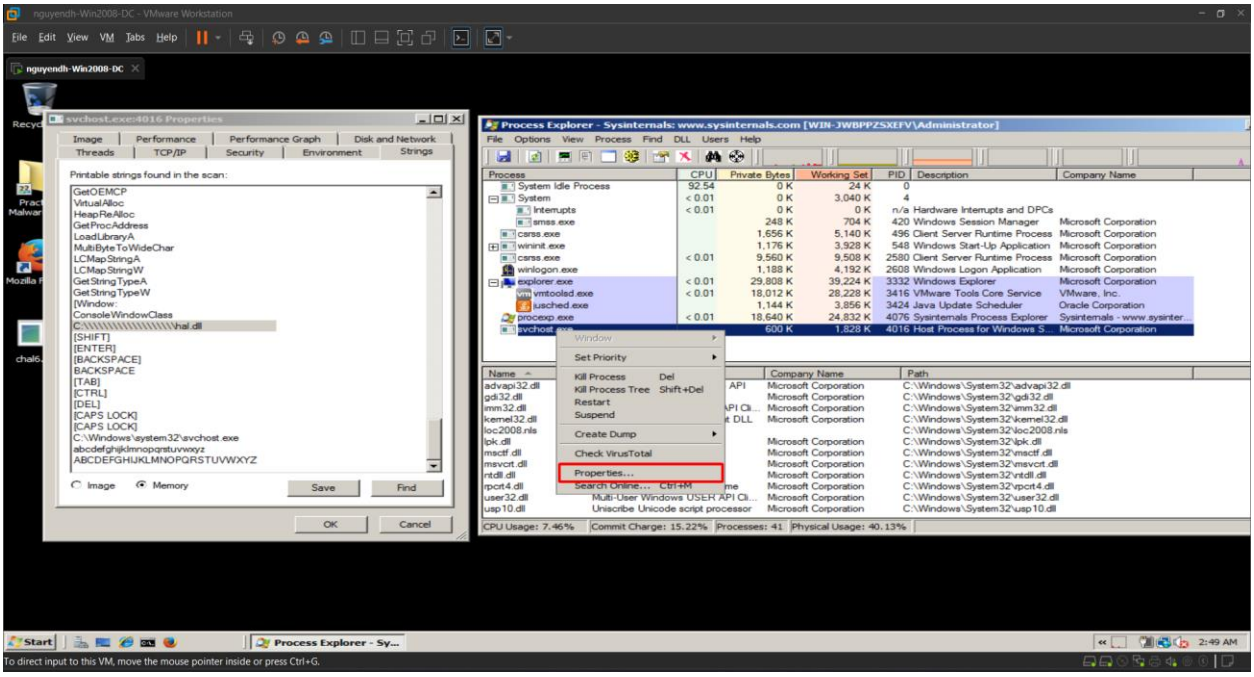
Xét ở đây ta thấy rằng đây cũng giống như thằng keylogger ở trên, nó cũng tạo ra một process con ở đây vẫn là svchost.exe từ PPID là thằng chal6.exe.



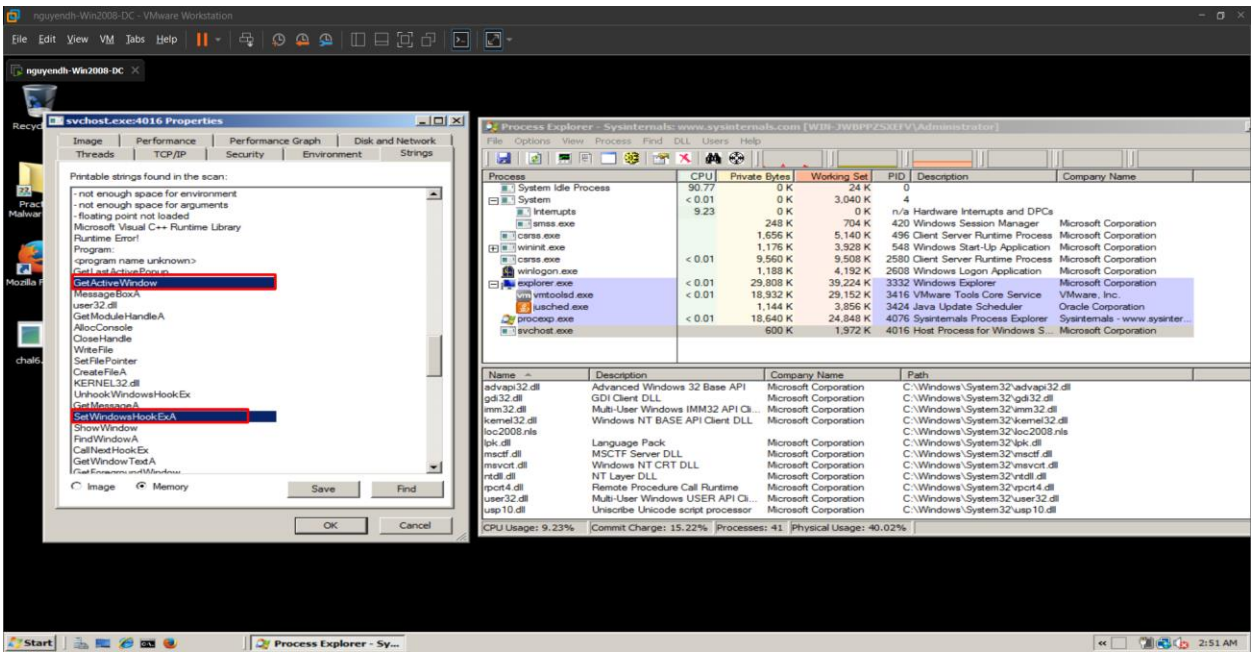

Hành vi của nó cũng giống như con keylogger bên trên, khi bắt đầu khởi động, nó sẽ tạo ra tiến trình con và sau đó tiến trình con đó trở thành tiến trình độc lập,




Click chuột phải và chonj vào phần properties, để xem được strings của nó, như lúc ban nãy, chúng ta sẽ vào phần image để xem strings của nó có những gì.

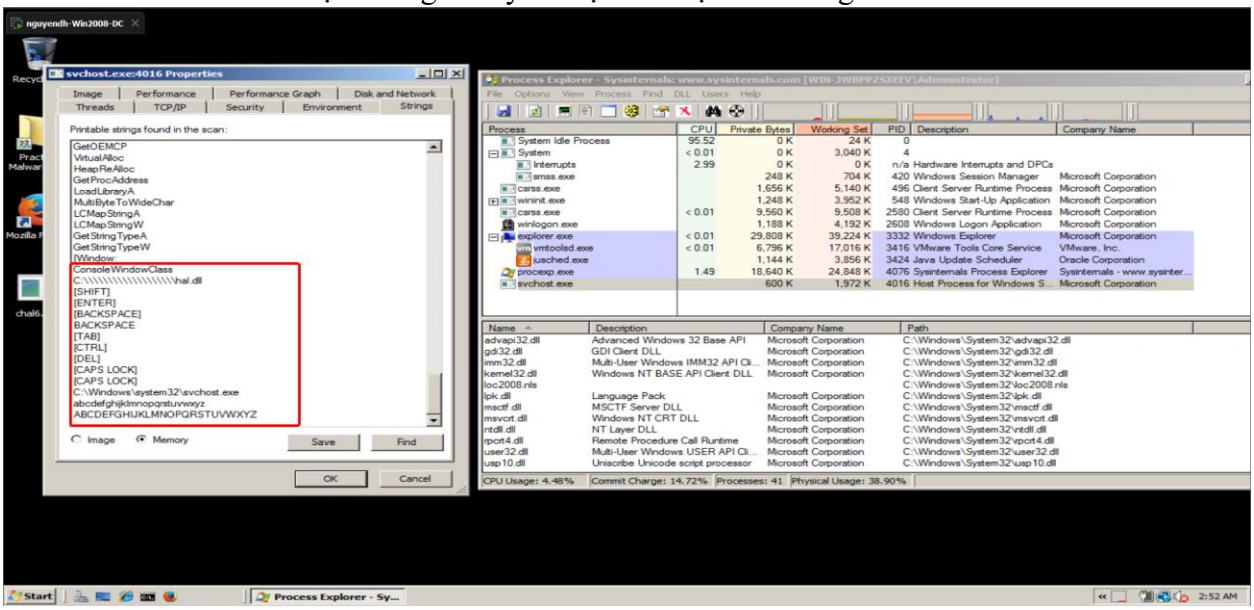



Tại đây các hàm cũng không khác gì mấy với con keylogger bên trên, sử dụng hai hàm là **GetActiveWindow và SetWindowsHookExA.**



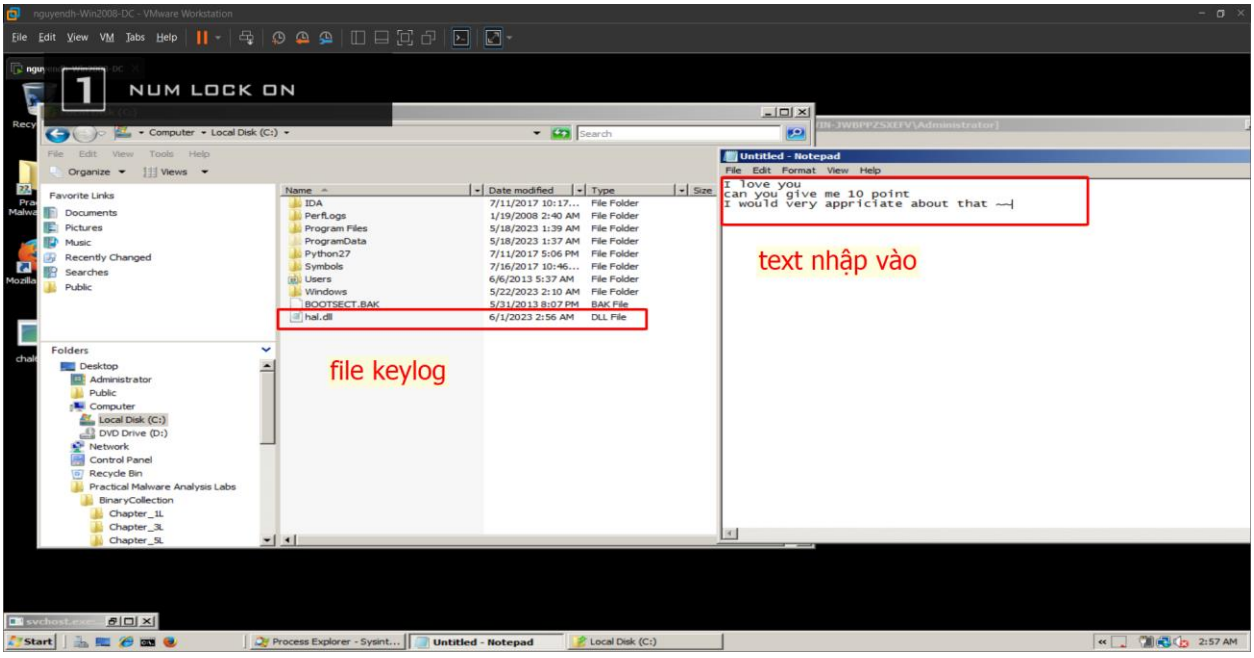

Kéo xuống bên dưới, không khác gì với co keylogger ban đầu, con này cũng ghi nhận những chữ cái ghi từ bàn phím, thay vì như con ở trên, nó lưu log tại thư mục nơi chứa con malware đó, tại đây nó sẽ lưu tại C:\\hal.dll. Thay vì là một log file, nó sẽ lưu dưới dạng là một dynamic link

nhằm có thể đánh lừa được chúng ta đây là một thư viện bên trong Windows

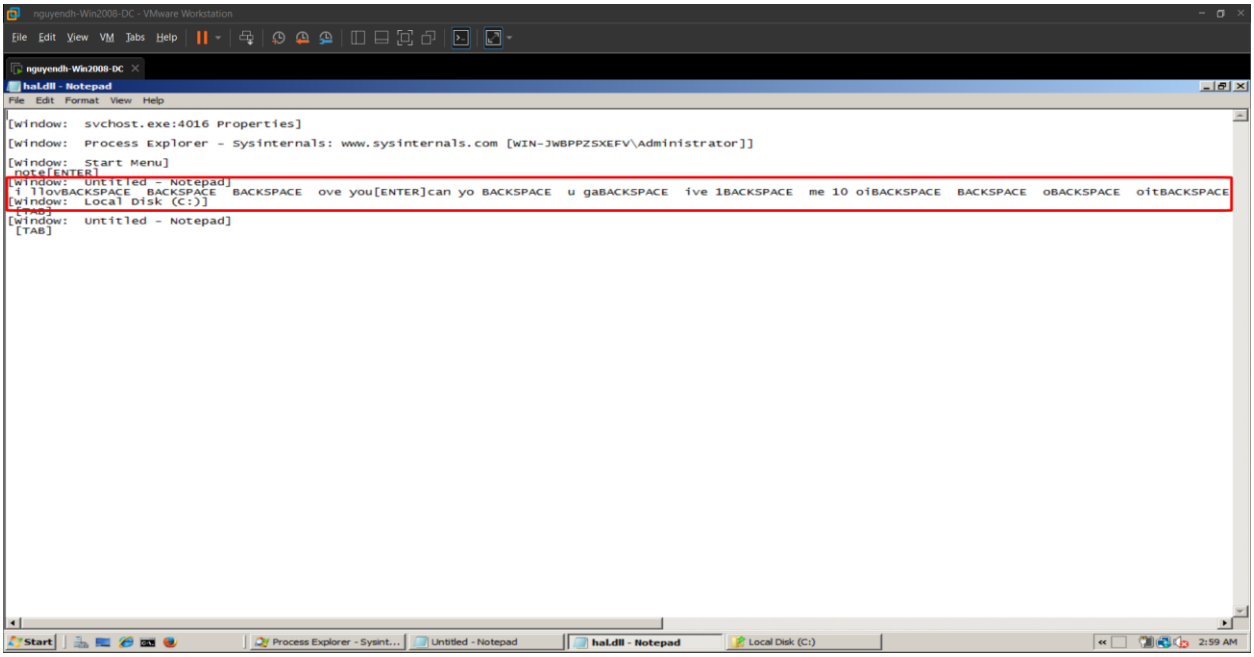



Giờ chúng ta sẽ bắt đầu mở notepad ra và chạy thử xem có file keylogger nào được ghi bên trong thư mục C:\\ không.

Đúng như chúng ta nghĩ thì file log đã được lưu vào bên trong hal.dll ở bên trong ổ C




Ta có thể thấy rằng là khi mở file keylogger tên là hal.dll lên thì ta sẽ thấy được bên trong đó đã ghi lại những gì.


nguyendh-Win2008-DC - VMware Workstation
File Edit View VM Tabs Help
nguyendh-Win2008-DC
haLdll - Notepad
File Edit Format View Help
[window: svchost.exe:4016 Properties]
[window: Process Explorer - Sysinternals: www.sysinternals.com [WIN-JWBPPZSXEFV\Administrator]]
[window: Start Menu]
note[ENTER]
[window: Untitled - Notepad]
i llovBACKSPACE BACKSPACE BACKSPACE ove you[ENTER]can yo BACKSPACE u gaBACKSPACE ive 1BACKSPACE me 10 oiBACKSPACE BACKSPACE oBACKSPACE oitBACKSPACE
[window: Local Disk (C:)]
[TAB]
[window: Untitled - Notepad]
[TAB]
Start
Process Explorer - Sysint...
Untitled - Notepad
haLdll - Notepad
Local Disk (C:)
2:59 AM