**Bài thực hành 1: Ẩn/ Hiện ổ đĩa trong máy tính dùng DiskPart:**

- Ẩn ổ đĩa:

Bước 1: Chạy cmd dưới quyền Admin

Bước 2: Dùng lệnh Diskpart

Bước 3: Dùng lệnh List Volume

Bước 4: Select Volume 3

Bước 5: Remove letter D

Bước 6: My computer kiểm tra ổ D đã được ẩn ?

- Hiện ổ đĩa:

Bước 1: Chạy cmd dưới quyền Admin

Bước 2: Dùng lệnh Diskpart

Bước 3: Dùng lệnh List Volume

Bước 4: Select Volume 3

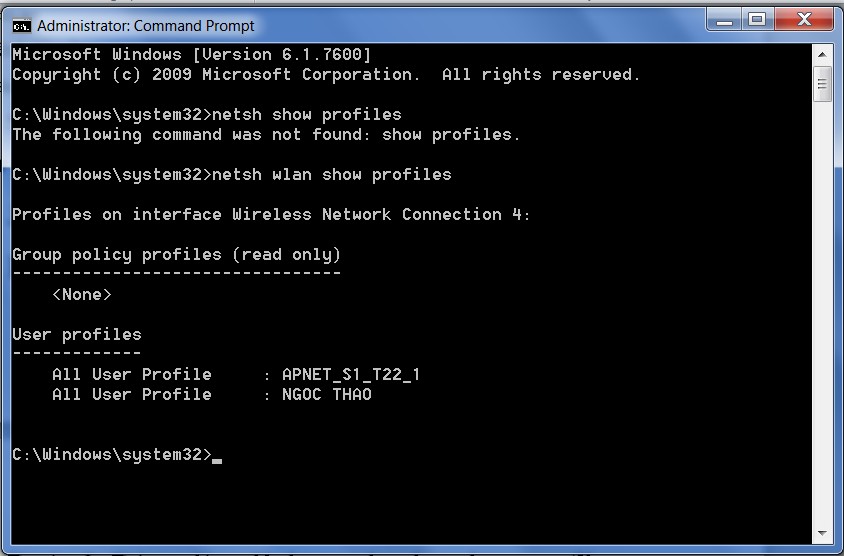
Bước 5: Assign Letter D

**Lab 2: Làm việc với CMD:**

**2.1 Hiển thị những WIFI đã được kết nối;tìm pass**

Bước 1: Mở cmd với quyền admin

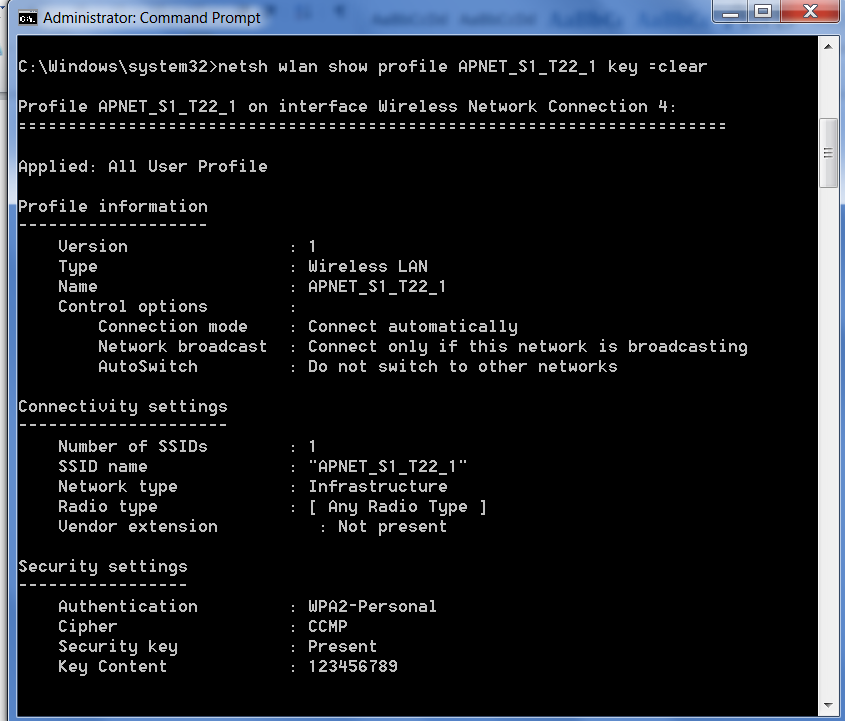
Bước 2: Dùng dòng lệnh: netsh wlan show profiles



Bước 3: Kiểm tra mật khẩu của Wifi

netsh wlan show profile tên-mạng-muốn-xem key=clear

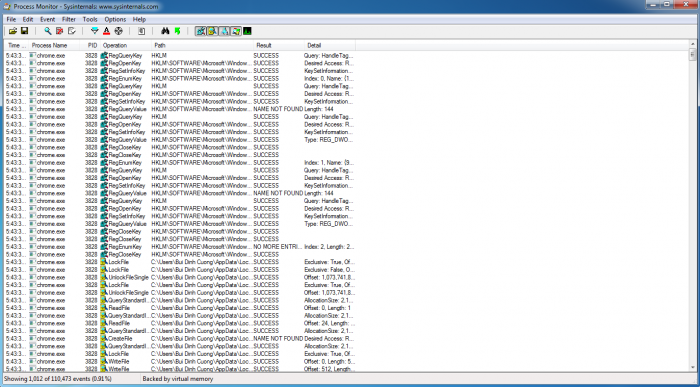
VD: netsh wlan show profile APNET\_S1\_T22\_1 key=clear

s

Bai 3: **Lab 3: Sử dụng công cụ Process Monitor**

1. Giới thiệu

Process Monitor (ProcessMon) là công cụ giám sát và theo dõi giành cho hệ điều hành Windows bằng cách ghi lại các hành động liên quan tới file hệ thống, registry, process/thread trong thời gian thực. Đây là công cụ rất hữu ích hỗ trợ quá trình phát hiện Malware, phần mềm độc hại hoặc muốn theo dõi hành vi của bất kỳ một chương trình nào đang tác động tới hệ thống. ProcessMon cung cấp các cơ chế lọc cho phép tập trung vào việc theo dõi các đối tượng cụ thể theo nhiều tiêu chí khác nhau: Tên chương trình, Process ID …

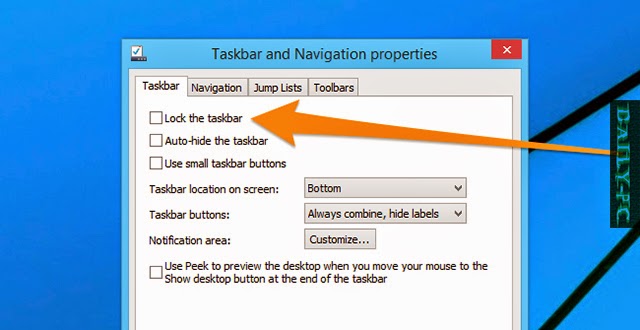
[](http://securitydaily.net/wp-content/uploads/2014/07/main_gui.png)

ProcessMon có tính năng giám sát và khả năng lọc rất mạnh mẽ:

* Khả năng bắt thông tin qua các tham số vào/ra
* Quá trình lọc (filter) không làm mất dữ liệu
* Bắt các thông tin của stack trong các luồng cho từng hành động, do đó dễ dàng phát hiện ra gốc của hành động
* Đưa ra các thông tin tin cậy về chi tiết sản phẩm: đường dẫn, command line, người dùng, session ID
* Khả năng cấu hình các cột linh hoạt
* Khả năng filter được thiết lập tới tất cả các trường dữ liệu
* Khả năng ghi log và capture dữ liệu rất lớn: khoảng 10 triệu sự kiện được capture với khoảng 10 triệu GB dữ liệu
* Process Tree chỉ ra mối quan hệ giữa các tiến trình liên quan trong cùng một nhánh
* Dễ dàng xem thông tin về process thông qua tool tip
* Ghi log các thao tác, hành động thời gian boot

1. Dùng Process Monitor để tìm khóa Registry cho những cấu hình thông thường.

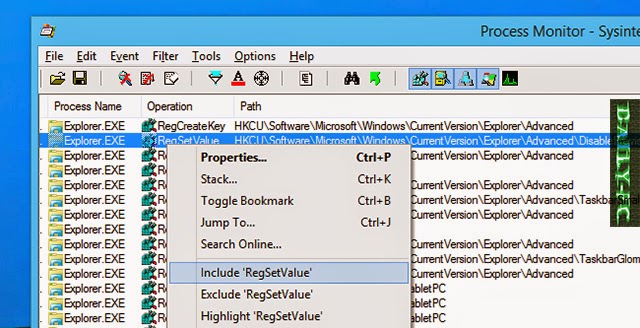
Hẳn ai cũng đã từng click vào một checkbox hoặc thay đổi giá trị của một box bằng một giá trị nào đó, nhưng bạn có bao giờ tự hỏi những giá trị này thực sự được lưu giữ ở đâu hay không? Nhiều ứng dụng và hầu như mọi thứ trong Windows đều lưu giữ cấu hình tại một nơi nào đó trong Registry.Trong ví dụ sẽ sử dụng tùy chọn đầu tiên trong tab đầu tiên của 'Taskbar and Navigation Properties'. Nhiệm vụ của chúng ta là tìm xem cấu hình 'Lock the taskbar' này được lưu giữ ở nơi nào trong registry.

[](http://2.bp.blogspot.com/-HeRFp1ZuhBQ/VDQF2VTGouI/AAAAAAAABA4/en0BM2q3TR0/s1600/2.jpg)

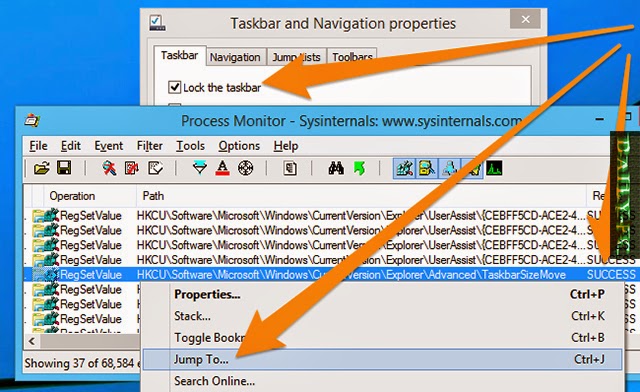
Mỗi khi được bật, Process Monitor sẽ ghi chép lại các sự kiện xảy ra trên hệ thống theo thời gian thực, vì vậy công việc của chúng ta là:

*1.Chạy Process Monitor (bắt đầu theo dõi hệ thống).  
2. Thay đổi cấu hình chúng ta muốn thử nghiệm (ở đây là cấu hình 'Lock the Taskbar').  
3. Ra lệnh cho Process Monitor dừng theo dõi hệ thống để danh sách sự kiện không kéo dài thêm nữa. (Capture (Ctrl+E) trong menu File hoặc icon thứ 3 từ trái sang trên toolbar của P.M)*

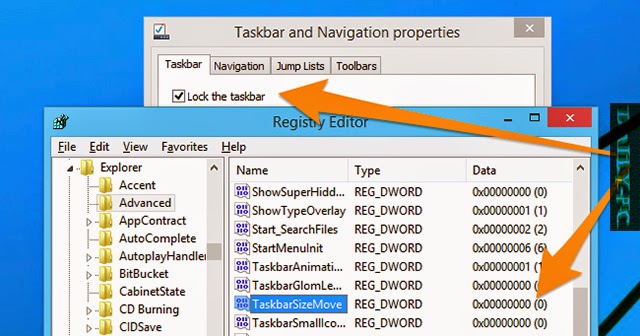
Dù thời gian chỉ trôi qua vài giây nhưng chúng ta sẽ có cả một đống dữ liệu ở trong danh sách, giờ là lúc để tiến hành lọc danh sách và giảm số hàng mà bạn phải tìm kiếm. Bởi vì chúng ta đang tìm kiếm một giá trị registry được thay đổi, chúng ta sẽ cần lọc ra tác vụ (operation) "RegSetValue", nó là loại tác vụ mà Windows sử dụng để đặt một cấu hình mới cho một khóa registry. Sử dụng tùy chọn "Include" để hiển thị những sự kiện loại này.

[](http://2.bp.blogspot.com/-3bA3Iu284gY/VDQGLSMHXXI/AAAAAAAABBA/AwKg9qckIsU/s1600/3.jpg)

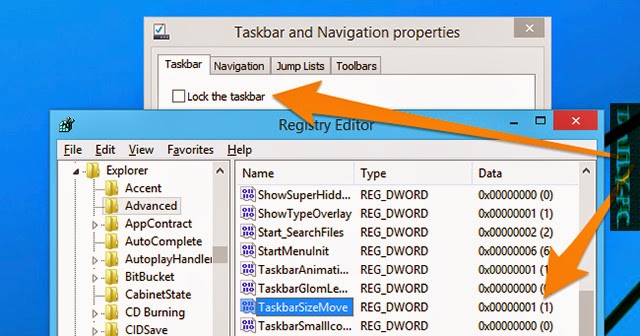
Danh sách của bạn bây giờ đã được giới hạn, chỉ bao gồm những khóa registry đã thay đổi, vì vậy đây là lúc để xem xét các sự kiện và thử tìm ra đâu là khóa registry mà chúng ta đang tìm kiếm. Và do chúng ta đang thử cấu hình "Lock the Taskbar", và một trong những khóa registry được cài đặt có chứa từ "Taskbar" trong tên, thế nên, đây sẽ là một nơi khá tốt để chúng ta bắt đầu. Right-Click lên đường dẫn và chọn tùy chọn "Jump to"

[](http://3.bp.blogspot.com/-ue5YMH1_Kl4/VDQGg2KrZbI/AAAAAAAABBI/6dFK6syrLXY/s1600/4.jpg)

Process Monitor sẽ mở 'Registry Editor' lên và đánh dấu khóa đó trong danh sách. Bây giờ chúng ta cần kiểm tra lại để chắc chắn rằng đây thực sự là khóa phải tìm. Hãy để ý vào cả cấu hình hiện thời và giá trị của khóa. Bây giờ, cấu hình được bật, và khóa được đặt giá trị là 0.

[](http://3.bp.blogspot.com/-EbfOegFHu4k/VDQGp_LvNVI/AAAAAAAABBQ/Hgy_2tmtC8Y/s1600/5.jpg)

Rồi thay đổi cấu hình, bấm Apply trên hộp thoại, và dùng phím F5 trong cửa sổ Registry Editor. Trong trường hợp này, chúng ta đã chọn được cấu hình đúng, bởi vì, bạn có thể thấy giá trị TaskbarSizeMove đã được đặt lại thành 1.

[](http://1.bp.blogspot.com/-WpqSQzFlG70/VDQGw9md_JI/AAAAAAAABBY/mIsZSnOU880/s1600/6.jpg)