

Làm thế nào để biết có ai đó đã truy cập và sử dụng máy tính của bạn?

Nhiều người dùng không có thói quen đặt mật khẩu cho máy tính của mình, nhất là khi làm việc ở văn phòng. Tuy nhiên điều này cũng gây ra một số rắc rối vì người lạ có thể truy cập trái phép máy tính của bạn để lấy cắp thông tin hoặc sử dụng máy tính của bạn cho những mục đích khác.

Nếu đang nghi ngờ có ai đó truy cập và sử dụng trái phép máy tính của mình, bạn có thể áp dụng một số thủ thuật dưới đây để xác nhận và khẳng định lại điều đó.

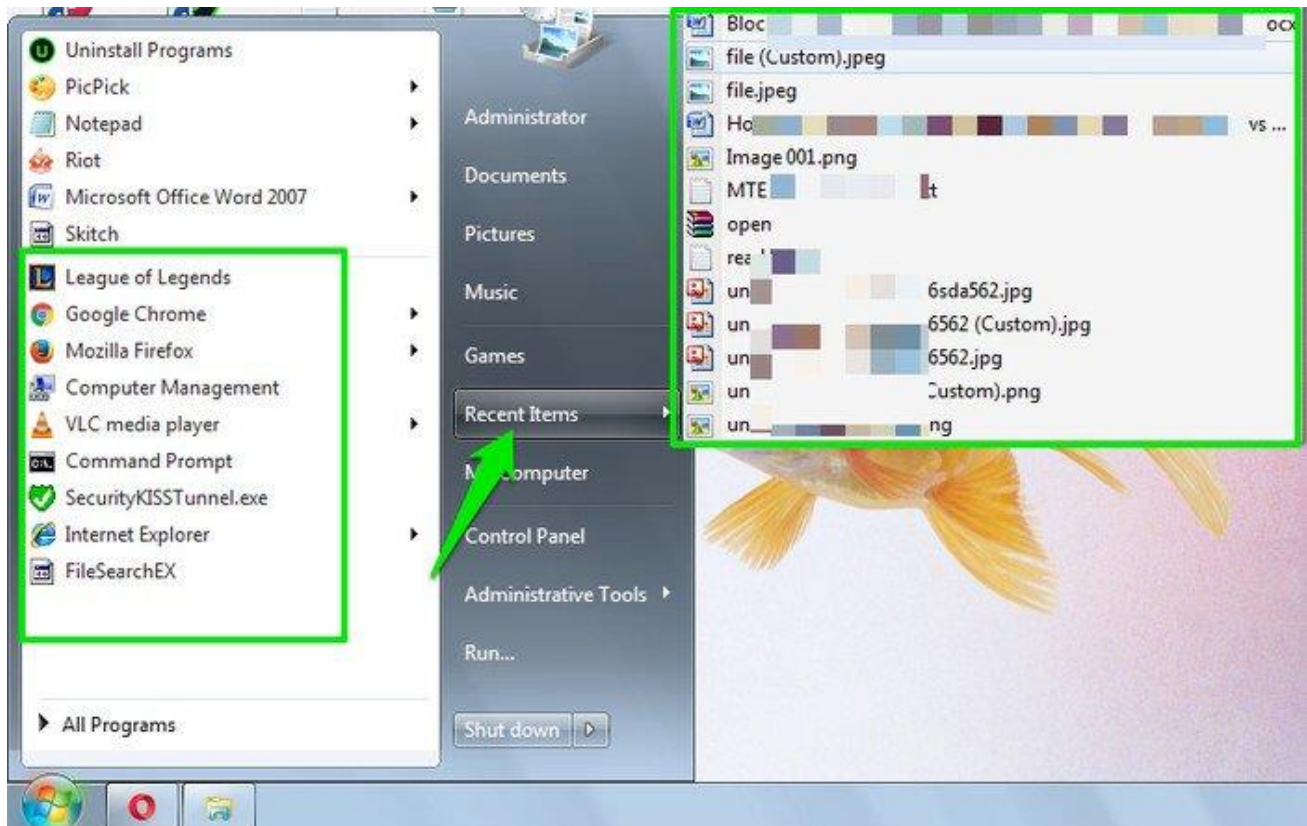
Phần 1: Trên máy tính Windows

1. Kiểm tra các hoạt động gần đây (Recent Activity)

Nếu có ai đó truy cập máy tính Windows của bạn, chắc hẳn họ sẽ sử dụng và thực hiện một số thao tác, khi đó bạn cần kiểm tra xem các hoạt động gần đây trên máy tính của bạn có gì thay đổi hay không?

Mục đầu tiên mà bạn cần kiểm tra là các chương trình gần đây (Recent Program) trên Start Menu. Click vào **Start Menu**, và bạn sẽ nhìn thấy danh sách tất cả các chương trình đã mở gần đây và bạn có thể biết được máy tính của mình có bị ai đó truy cập trái phép và sử dụng hay không?

Ngoài ra khi bạn di chuột qua mục **Recent Items** ở phía bên phải Start Menu, bạn cũng sẽ nhìn thấy danh sách các tập tin đã mở gần đây.



Cách phát hiện người lạ mở máy tính

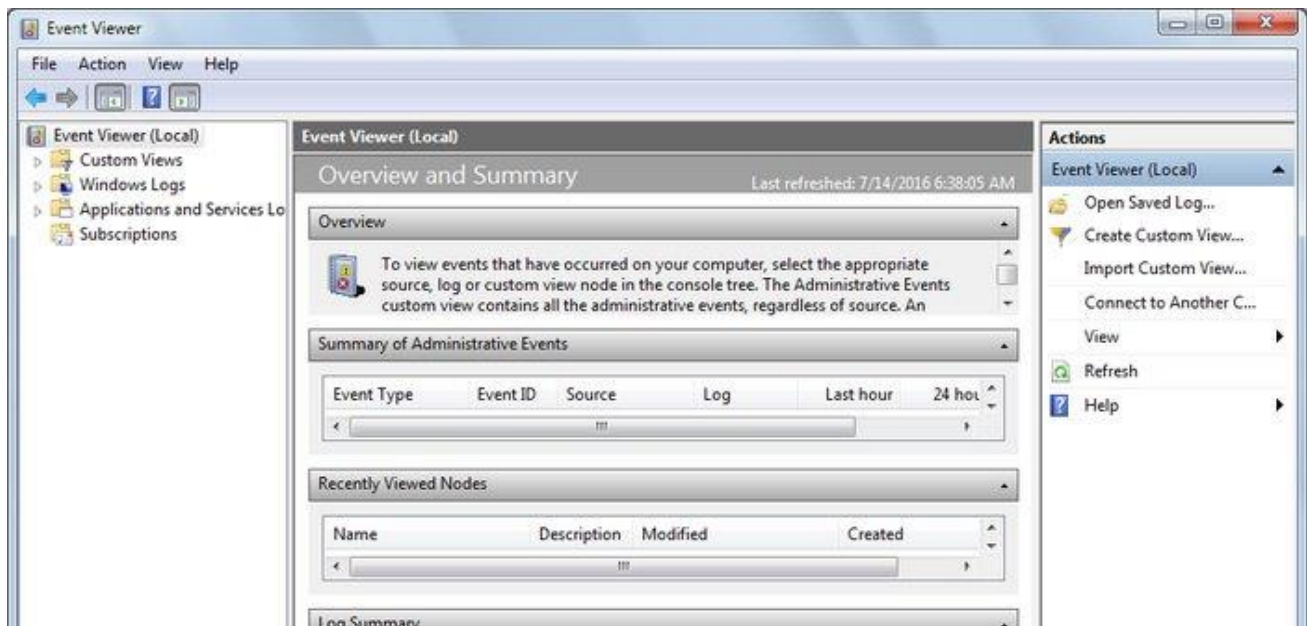
Tuy nhiên điểm hạn chế của giải pháp này là nếu người truy cập trái phép máy tính của bạn đủ thông minh, họ có thể xóa các hoạt động gần đây và xóa các tập tin đã mở gần đây, do đó bạn khó có thể mà phát hiện được máy tính của mình có bị ai đó truy cập và sử dụng hay không?

2. Kiểm tra Windows Event Viewer

Windows sẽ lưu trữ một bản đầy đủ các lần đăng nhập thành công cũng như đăng nhập thất bại. Bạn có thể tận dụng điểm này để kiểm tra xem có ai đó đã truy cập máy tính của bạn hay không?

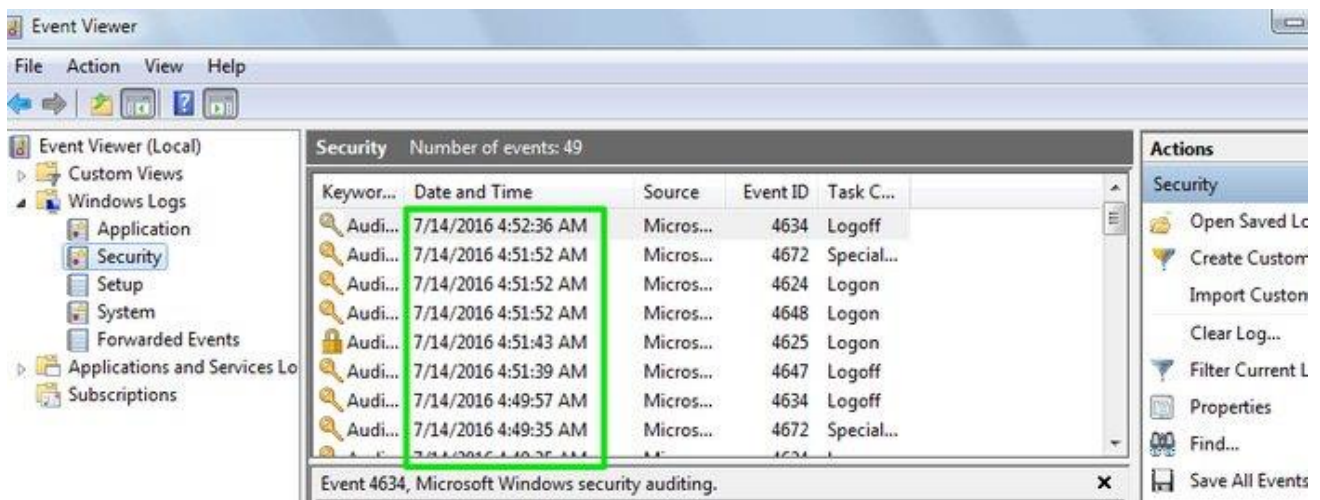
Để xem các lần đăng nhập thành công hay thất bại, bạn truy cập Windows Event Viewer.

Để truy cập Windows Event Viewer, đầu tiên bạn nhấn tổ hợp phím **Windows + R** để mở cửa sổ lệnh Run, sau đó nhập **eventvwr.msc** vào đó rồi nhấn **Enter** hoặc click chọn **OK** để mở cửa sổ Event Viewer.

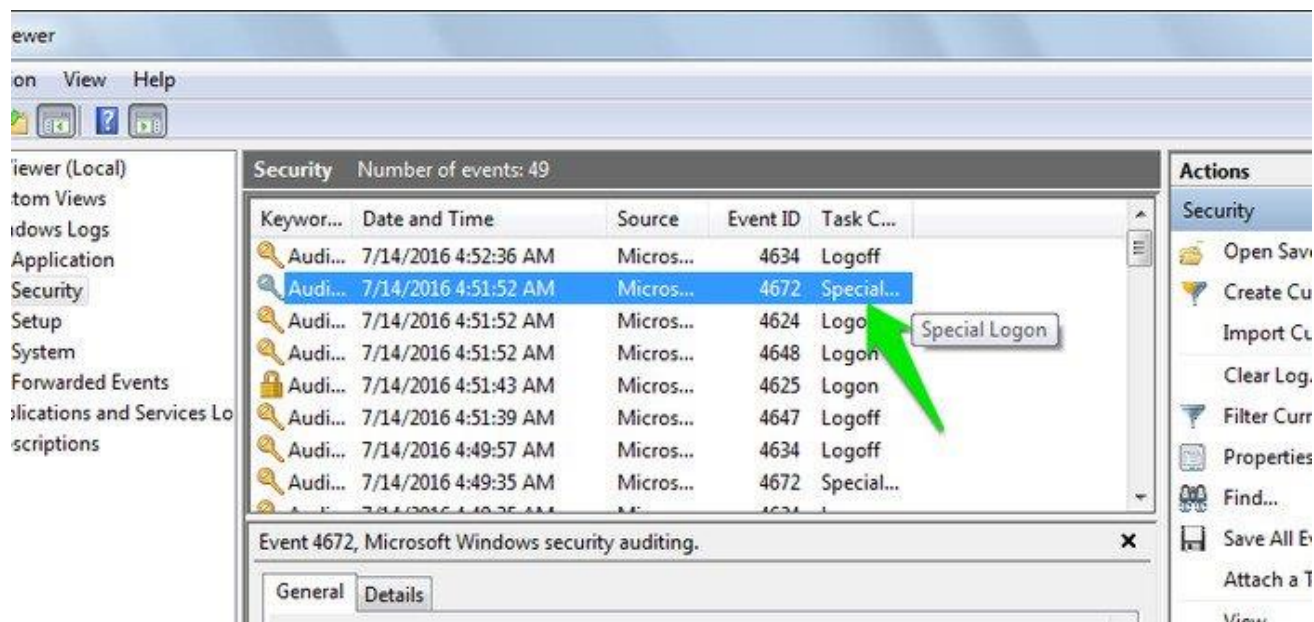


Theo dõi máy tính khi bạn vắng mặt

Tại đây bạn kích đúp chuột vào nút **Windows Logs**, sau đó click chọn **Security**. Ở giữa bảng danh sách bạn sẽ nhìn thấy các lần đăng nhập kèm theo ngày và giờ đăng nhập. Mỗi lần bạn đăng nhập, Windows sẽ ghi lại các lần đăng nhập trong khoảng thời gian trước đó khoảng 2 đến 4 phút.



Ngoài ra bạn có thể kiểm tra cụ thể tài khoản đã truy cập máy tính của bạn trước đó (trường hợp nếu có nhiều tài khoản). Để kiểm tra, bạn kích đúp chuột vào lần đăng nhập cụ thể, lúc này trên màn hình sẽ xuất hiện cửa sổ Event Properties. Và bạn sẽ nhìn thấy tên tài khoản nằm kế bên **Account Name**.



3. Hiện thị chi tiết lần đăng nhập cuối cùng

Giải pháp cuối cùng bạn có thể nghĩ đến là thiết lập hiện thị chi tiết thông tin đăng nhập khi máy tính khởi động. Thao tác này sẽ hiện thị tài khoản bạn sử dụng trong lần đăng nhập cuối cùng, dù thành công hay thất bại.

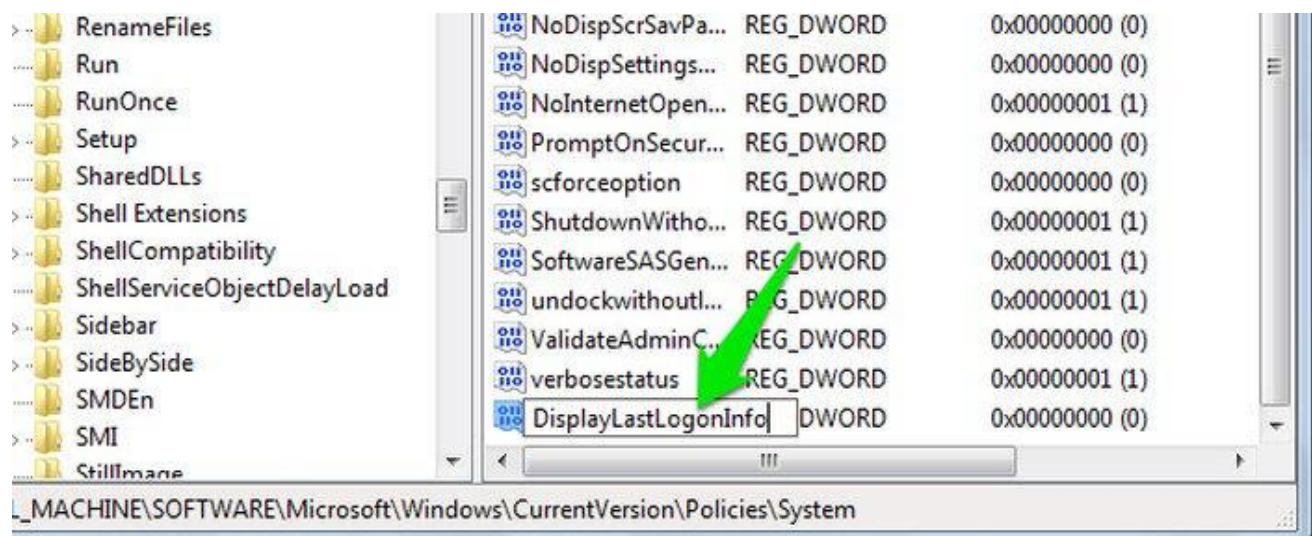
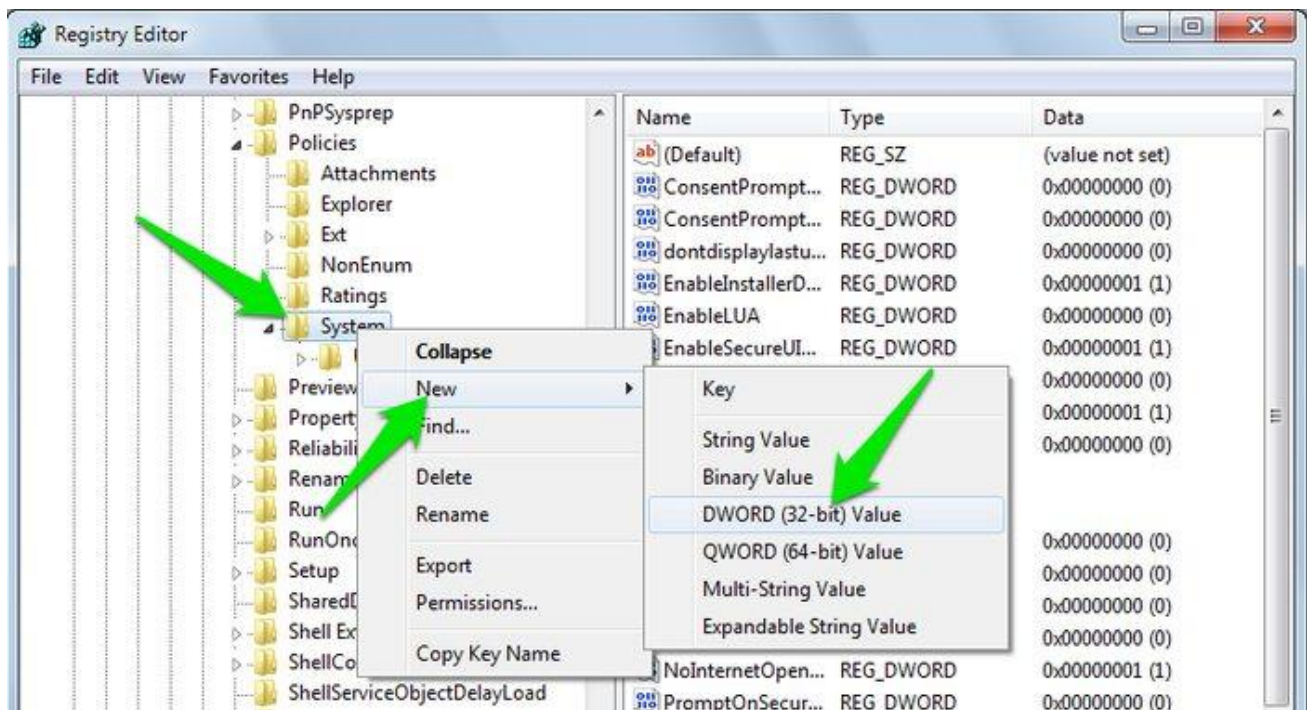
Bạn sẽ phải chỉnh sửa Windows Registry, do đó trước khi thực hiện bạn nên tiến hành tạo một bản sao lưu trước tiên.

Nhấn tổ hợp phím **Windows + R** để mở cửa sổ lệnh Run, sau đó nhập **regedit** vào cửa sổ lệnh Run rồi nhấn **Enter** hoặc click chọn **OK** để mở Windows Registry.

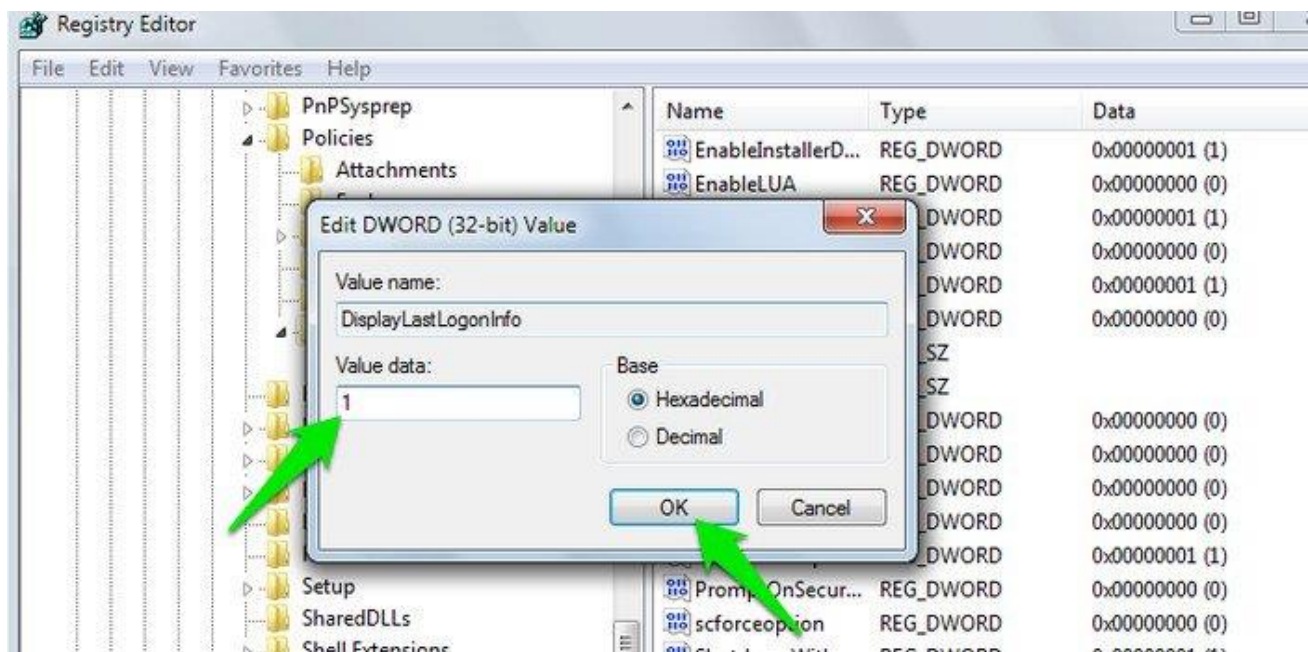
Trên cửa sổ Registry Editor, bạn điều hướng theo key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Tiếp theo kích chuột phải vào thư mục System chọn **New => DWORD value** để tạo một DWORD mới và đặt tên cho DWORD này là **DisplayLastLogonInfo**.



Kích đúp chuột vào **DisplayLastLogonInfo** và thiết lập giá trị trong khung **Value Data** là **1**.



Từ giờ bất cứ khi nào đăng nhập máy tính, bạn sẽ nhìn thấy thông tin chi tiết lần đăng nhập cuối cùng và bất kỳ lần đăng nhập thất bại.

4. Kích hoạt Logon Auditing

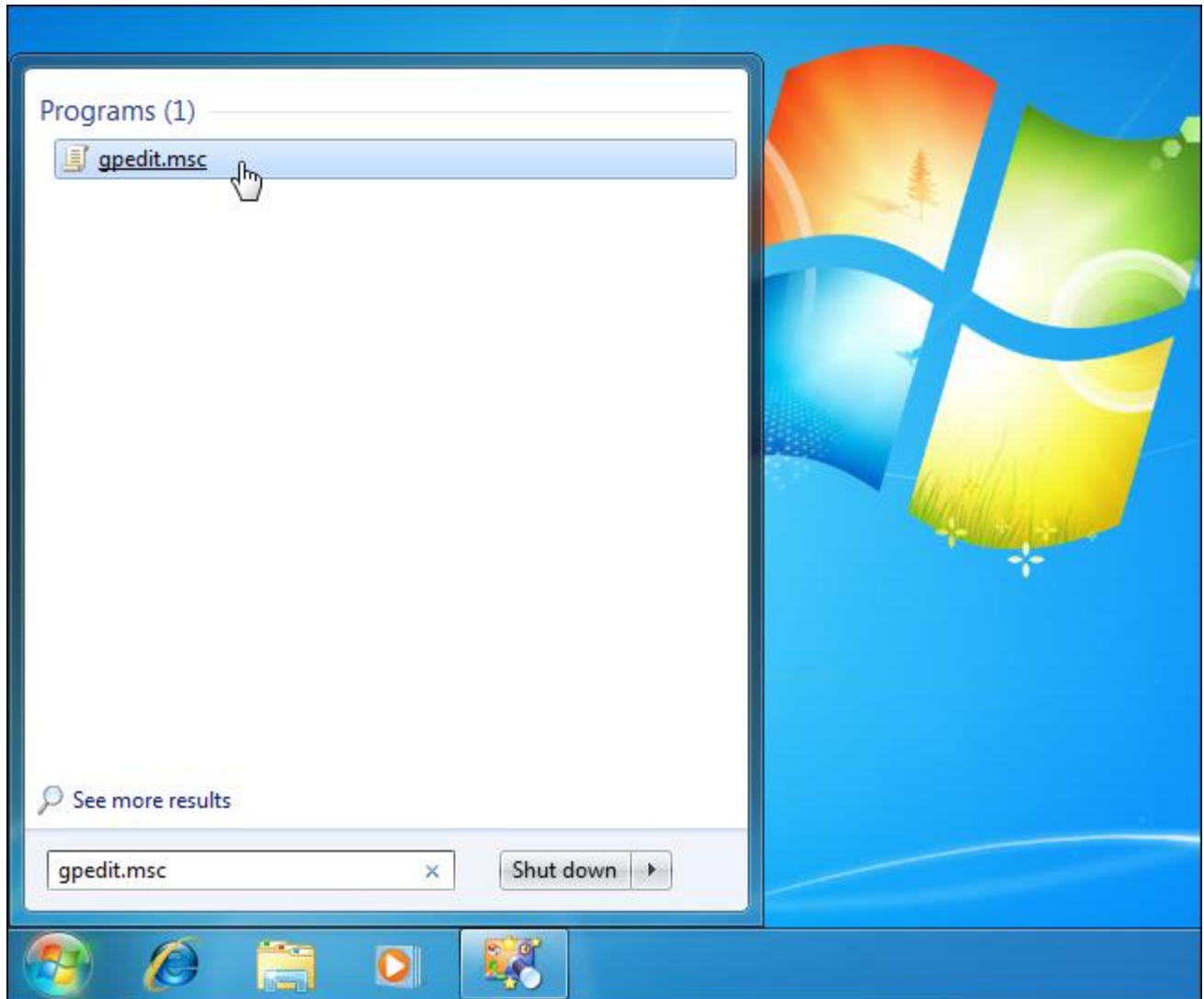
Lưu ý: Logon Auditing chỉ hoạt động trên phiên bản Professional của Windows 7, 8 và Windows 10 và KHÔNG hoạt động trên phiên bản Home.

Để kích hoạt Logon Auditing, đầu tiên bạn mở Local Group Policy Editor. Nhấn tổ hợp phím **Windows + R** để mở cửa sổ lệnh Run, sau đó nhập **gpedit.msc** vào đó rồi nhấn **Enter** để mở Local Group Policy Editor.

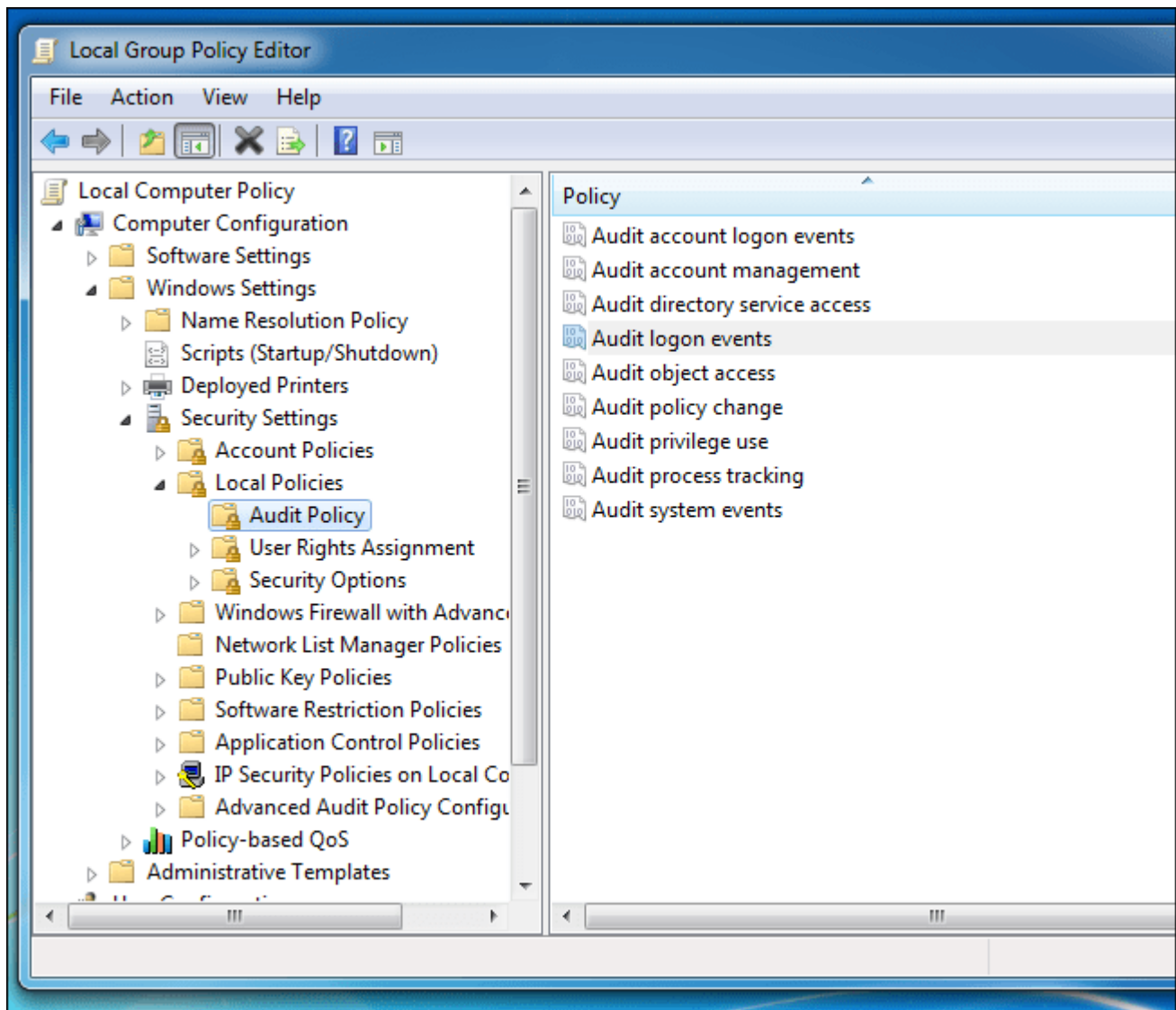
Hoặc cách khác là nhập **gpedit.msc** vào khung Search trên Start Menu rồi nhấn **Enter**.

Tiếp theo trên cửa sổ Local Group Policy Editor, bạn điều hướng theo key:

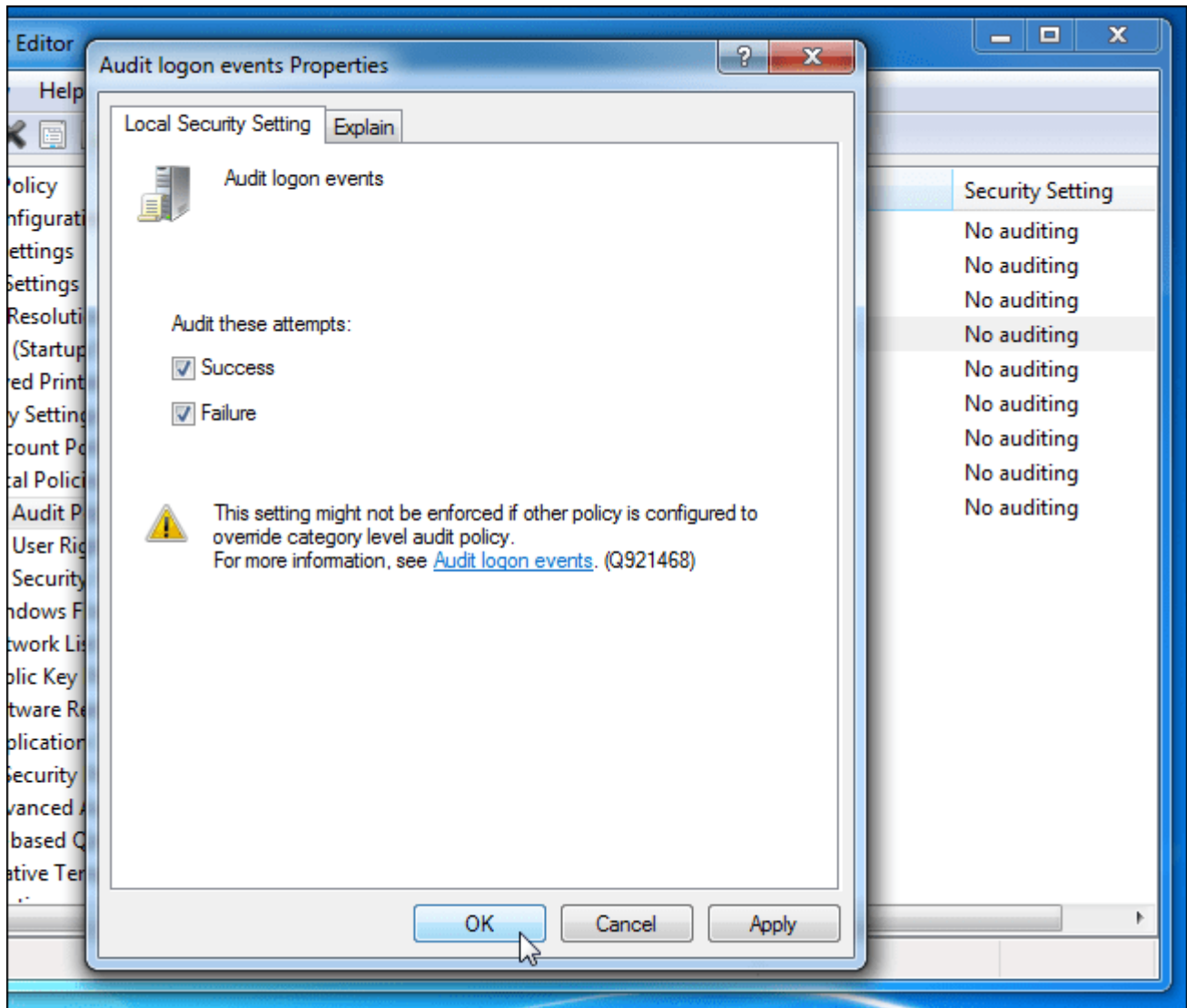
Local Computer Policy => Computer Configuration => Windows Settings => Security Settings => Local Policies => Audit Policy



Kích đúp chuột vào thiết lập policy **Audit logon events** ở khung bên phải để điều chỉnh tùy chọn.

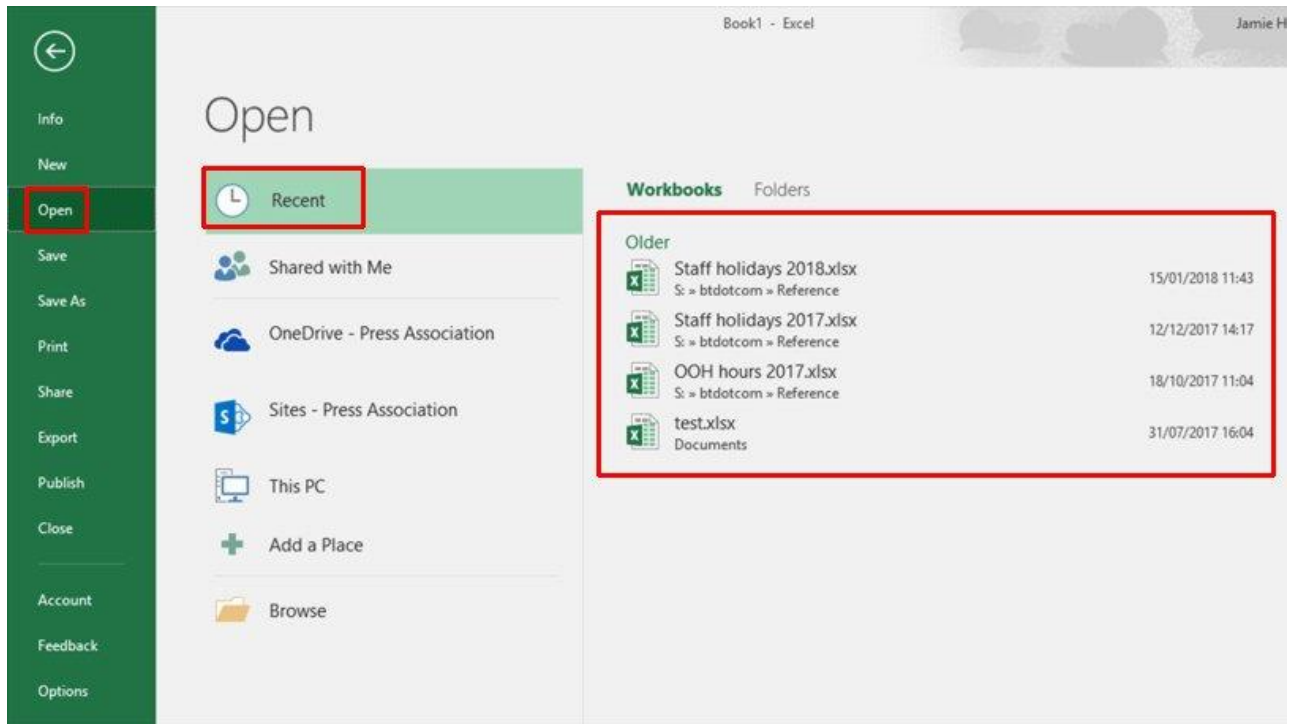


Tiếp theo trên cửa sổ Properties, bạn đánh tích chọn mục **Success** để hiển thị đăng nhập thành công. Ngoài ra bạn có thể đánh tích chọn **Failure** để hiển thị lần đăng nhập thất bại.

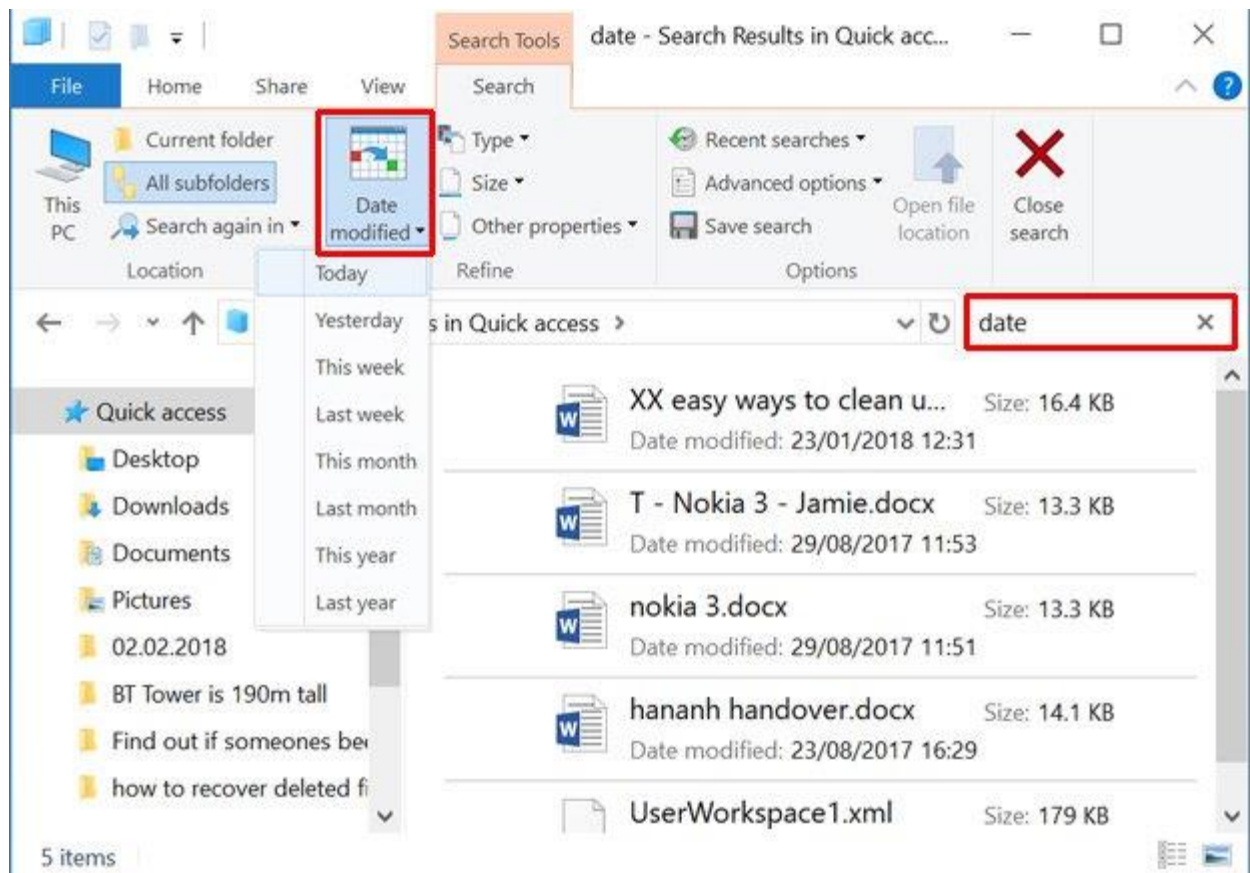


5. Kiểm tra các file được sử dụng gần đây

Để kiểm tra các file được sử dụng gần đây, mở bất kỳ ứng dụng nào bạn sử dụng thường xuyên và kiểm tra tùy chọn **Open recent** (hoặc tương tự) trong menu **File**. Không phải ứng dụng nào cũng có tùy chọn này, nhưng nó sẽ hiển thị cho người dùng những file được mở gần đây, tìm kiếm những file mà bạn không nhận ra.

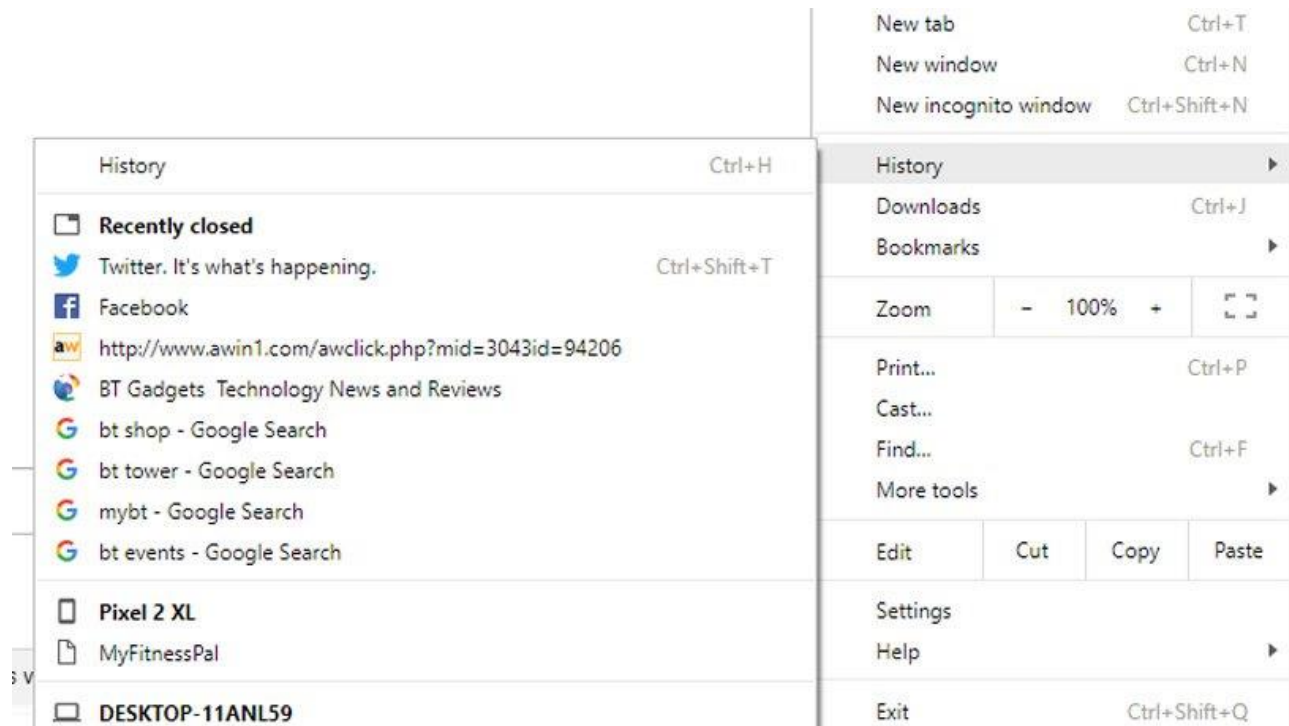


Bạn cũng có thể tìm kiếm các file đã được sửa đổi vào những ngày đã xác định. Mở cửa sổ và nhập một từ có liên quan ở bên trái của sổ, sau đó chọn tùy chọn **Date modified** và chọn một ngày trên lịch xuất hiện.



Windows sau đó sẽ tìm kiếm tất cả các file trong thư mục Library được thay đổi trong ngày đó. Bạn có thể thực hiện tương tự trong ổ C: nhưng Windows thay đổi nhiều file để sử dụng với mục đích thông thường, do đó việc làm này có thể không thu được kết quả tương tự.

6. Kiểm tra lịch sử trình duyệt web



Cuối cùng, đừng quên kiểm tra lịch sử trình duyệt web của bạn. Nó sẽ hiển thị danh sách tất cả các trang web được mở gần đây và duyệt theo ngày. Nhưng một điều bạn cần lưu ý là lịch sử duyệt web có thể bị xóa một cách dễ dàng nhưng bạn hoàn toàn có thể truy tìm lịch sử duyệt web đã bị xóa.

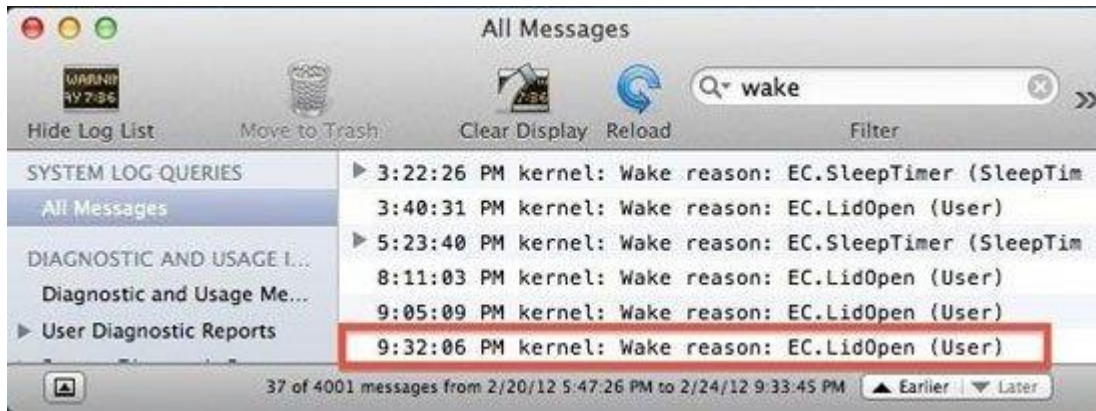


Cách tốt nhất để phòng ngừa ai đó sử dụng máy tính của bạn là đặt mật khẩu tài khoản người dùng Windows. Sau đó bất cứ khi nào bạn rời khỏi máy tính nhưng không muốn tắt nó, hãy nhấn **Windows + L** để khóa màn hình.

Phần 2: Trên Mac

Trên máy tính sử dụng hệ điều hành Mac OS, bạn chỉ có thể kiểm tra xem có ai sử dụng máy tính của mình khi bạn rời đi và đang để máy ở chế độ **Sleep**, nghĩa là nó chỉ lưu lại các hoạt động đánh thức máy tính từ chế độ **Sleep**. Bạn có thể thực hiện theo các bước sau:

Mở hộp thoại **Console** bằng cách nhấn **Command + Spacebar**, hoặc click vào biểu tượng **Spotlight** và tìm kiếm nó. Gõ từ "**wake**" vào thanh tìm kiếm, sau đó kéo xuống phần dưới cùng của danh sách, bạn sẽ tìm thấy những hoạt động đăng nhập gần đây nhất.



Một vài thủ thuật đơn giản, nhưng hiệu quả giúp bạn kiểm tra những người sử dụng máy tính của mình khi bạn không ở đó. Việc này khá hữu ích để kiểm soát việc sử dụng máy tính của con cái bạn hoặc các em nhỏ, tuy nhiên trong các trường hợp khác bạn nên đặt một mật khẩu cho máy tính của mình để đảm bảo sự an toàn.