Ver Los Sitios Que Secretamente Realizan Conexiones En Nuestra Computadora

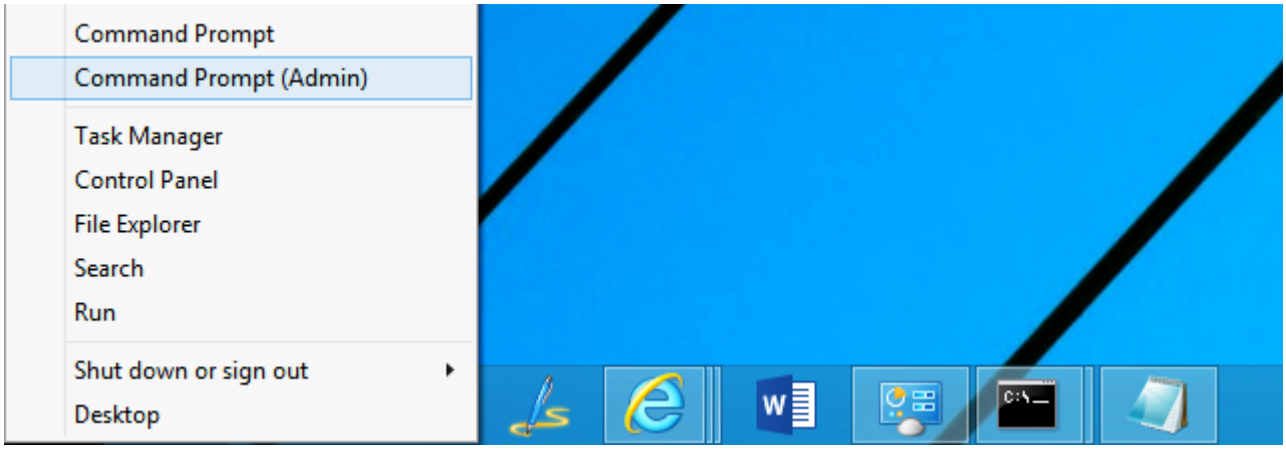
En la web se podrá encontrar material para enseñar como realizar penetraciones en las redes wifi, con eso podrán robar las contraseñas de las redes inalámbricas y usar ancho de banda de nuestra red. Es por esto que muchas veces es util conocer las medidas y métodos para saber si alguien mas esta realizando una conexión. Existen herramientas especializadas como **WireShark**, pero en esta oportunidad usaremos la line de comando de Windows.

Cómo Comprobar Las Conexiones Que Realiza El Computador

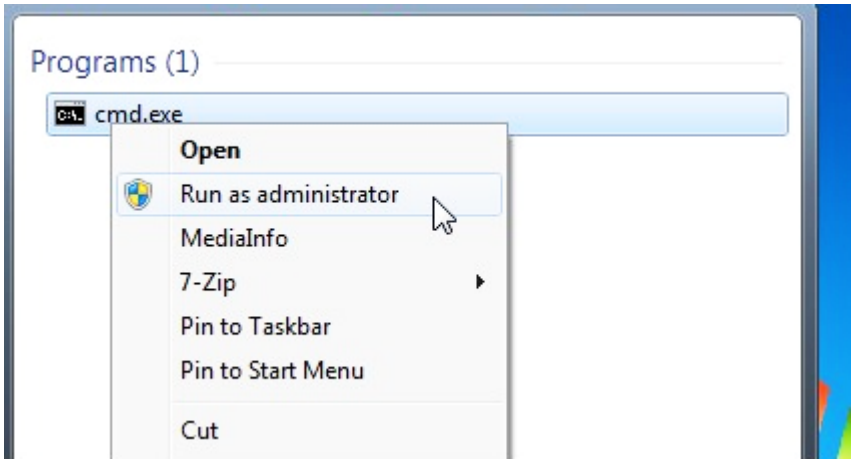
¿Cómo encontrar cuál es el problema? Para esta ardua tarea, usaremos el comando netstat, no es tan complicado, ni necesitas ser todo un experto en la consola de comando, solo

seguir los siguientes pasos :) Esto funciona con Windows 8, 7, Vista y XP. Vamos a **utilizar el comando netstat para generar una lista** de todo lo que ha hecho una conexión a Internet en un período de tiempo especificado. Para utilizar el comando netstat, debe **ejecutar la ventana de símbolo del sistema como administrador**.

Si está utilizando 8.x de Windows puede hacer clic derecho sobre el botón Inicio y seleccione la opción Símbolo del sistema (administrador).

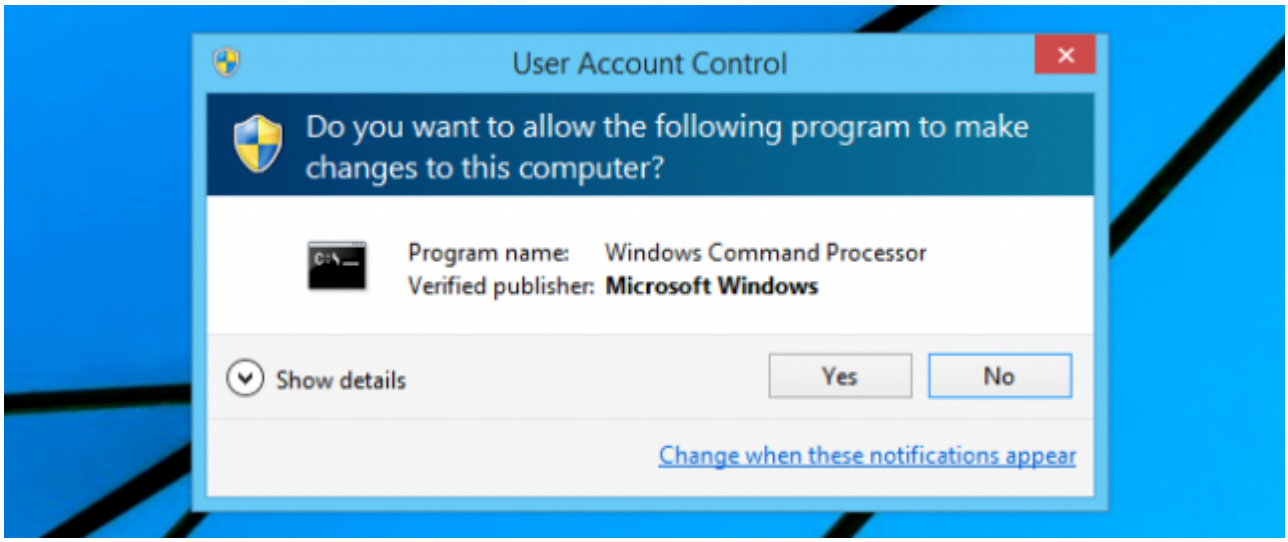


Si se encuentra en Windows 7 ó Vista, abra el menú Inicio y escriba «cmd.exe» en el cuadro de búsqueda. Cuando se muestre la pantalla de resultados, haga clic en cmd.exe y seleccione Ejecutar como administrador en el menú emergente.



Si el cuadro de diálogo de Control de cuentas de usuario, haga clic en Sí para continuar. **Nota**: No se puede ver este cuadro de diálogo, dependiendo de la configuración de Control de

cuentas de usuario.

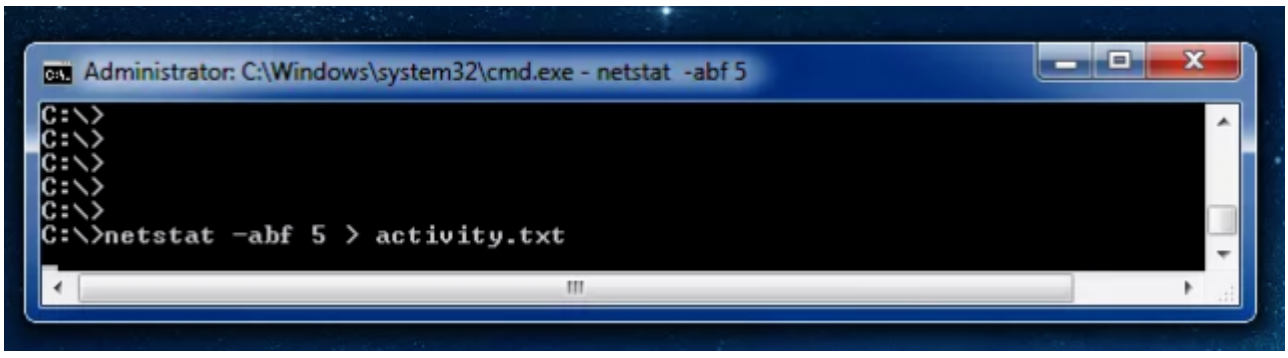


En el símbolo del sistema, escriba el siguiente comando y presione Intro.

[bash]netstat -abf 5 > activity.txt[/bash]

La opción -a muestra todas las conexiones y puertos de escucha, la opción -b muestra qué aplicación está haciendo la conexión, y la opción -f muestra el nombre DNS completo para cada opción de conexión para facilitar la comprensión de donde se están realizando las conexiones. También puede utilizar la opción -n si sólo desea mostrar la dirección IP. La opción 5 sondeará cada 5 segundos para las conexiones para que sea más fácil seguir lo que está pasando, y los resultados se almacenan en el archivo **activity.txt**.

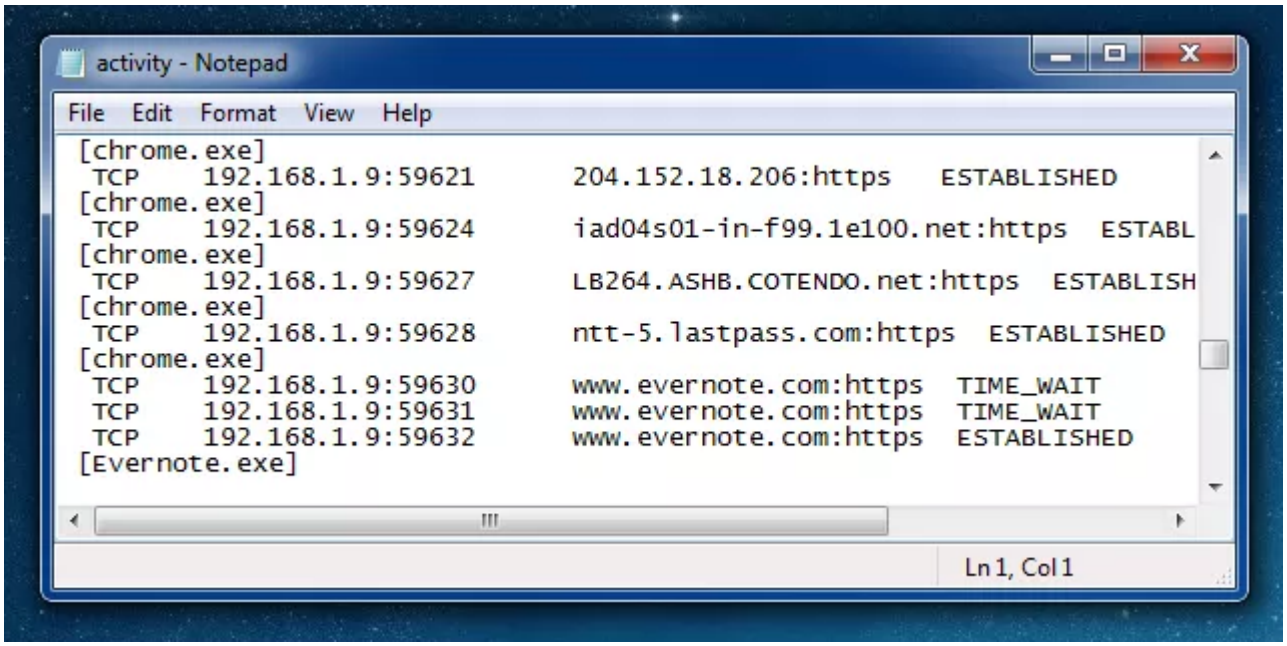
Espere unos dos minutos y luego presione **Ctrl + C** para detener la grabación de datos.



Una vez que haya terminado la grabación de datos, sólo tiene que abrir el archivo **activity.txt** en su editor favorito para ver los resultados, o puede escribir activity.txt en la línea de comandos para abrirlo en el Bloc de notas.

El archivo resultante mostrará todos los procesos en su ordenador (navegadores, clientes de mensajería instantánea, programas de correo electrónico, etc) que han hecho una conexión a Internet en el tiempo que esperó antes de pulsar **Ctrl + C**. También enumera que procesa conectado a los sitios web.

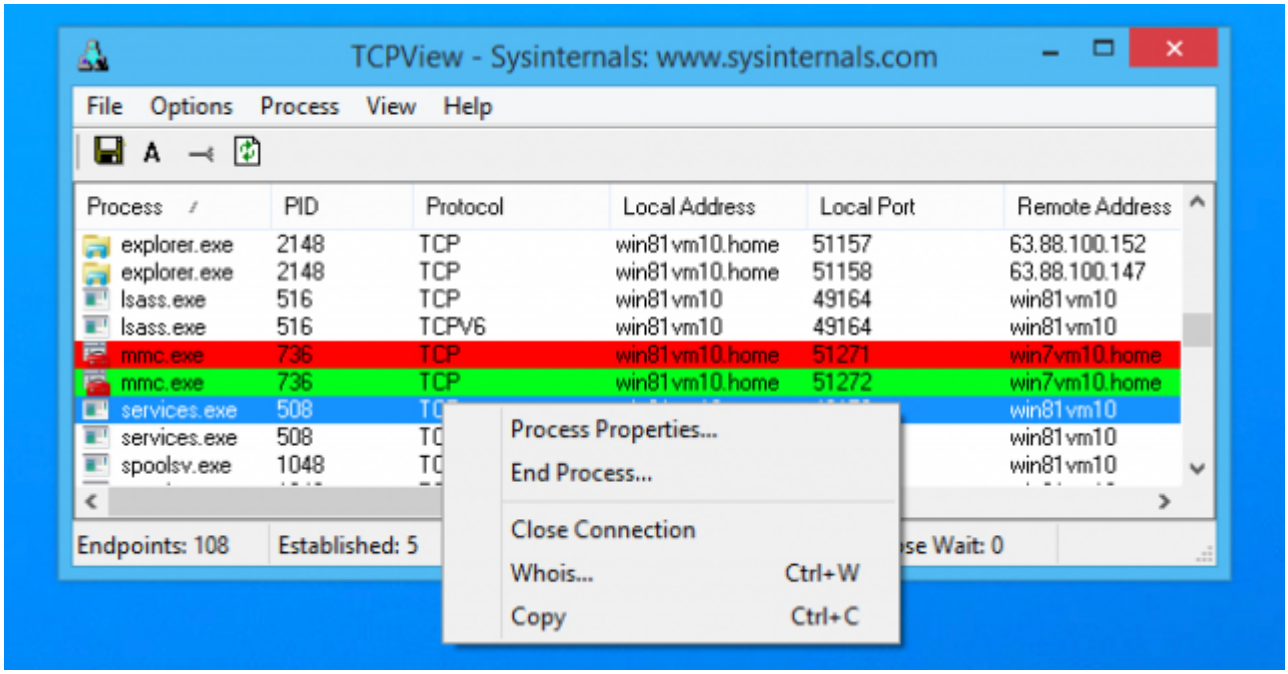
Si ves los nombres de procesos ó direcciones de sitios web con los que no está familiarizado, puede buscar el nombre en Google y ver lo que es. Puede ser una función del sistema que no conoces ó de uno de sus programas en ejecución. Sin embargo, si parece un mal sitio, puede utilizar Google de nuevo para encontrar la manera de deshacerse de él.



Bueno, y si no te gusta la linea de comandos y estas mal acostumbrado a las interfaces gráficas, no te preocupes, también te compartimos una herramienta que hará lo mismo pero con una interfaz gráfica.

Usar TCPView Ver Las Conexiones

La utilidad **TCPView** que viene en el kit de herramientas **SysInternals,** este le permitirá ver rápidamente exactamente qué procesos se están conectando a qué recursos en Internet, e incluso permitir que termines el proceso, cierres la conexión, o hacer una búsqueda Whois rápida para darle más información . Es, definitivamente, nuestra primera opción cuando se trata de diagnosticar problemas o simplemente tratando de obtener más información sobre su ordenador.



Nota: La primera vez que TCPView carga, es posible que vea un montón de conexiones de [Procesos de Sistema] para todo tipo

de direcciones de Internet, pero esto no suele ser un problema. Si todas las conexiones están en el estado TIME_WAIT, eso significa que la conexión se está cerrando, y no hay un proceso para asignar la conexión, por lo que se debe a que le sean asignadas PID 0 ya que no hay PID para asignarlo.