NetResident®

Documentación de Ayuda

Introducción

Acerca de NetResident

NetResident es un programa avanzado de monitoreo de contenido de red que captura, almacena, analiza, y reconstruye eventos de red tales como mensajes de correo electrónico, páginas Web, archivos descargados, mensajes instantáneos y conversaciones de voz. NetResident usa tecnología avanzada de monitoreo para capturar los datos requeridos desde la red, guardarlos en una base de datos, reconstruirlos, y mostrar este contenido en un formato fácil de comprender.

Mientras que NetResident es similar a los analizadores de red en muchos aspectos, se enfoca en protocolos de alto nivel que son usados para transferir contenidos sobre Internet o LAN. Con NetResident, no necesita un conocimiento profundo de tecnologías de red, tener que usar complejos software de análisis y captura de paquetes, o ahondar entre paquetes de red para reconstruir los datos actuales; NetResident hace todo el trabajo por usted y le presenta solo las páginas Web, correos electrónicos, mensajes instantáneos, o archivos descargados según se requiera. NetResident es usado por administradores de red para ejecutar políticas de IT, padres para monitorear las comunicaciones sobre Internet de sus hijos, y por expertos legales para obtener información crucial.

Si es uno de los muchos profesionales de red que usa soluciones de monitoreo de red de TamoSoft, CommView o CommView para WiFi, NetResident procesará los archivos de registro generados por su programa de monitoreo de paquetes y recuperará mensajes de correo electrónico, páginas Web, y otros tipos de contenido para análisis rápido.

Novedades

Versión 1.4

- Nuevo y mejorado motor de alto rendimiento de base de datos
- Soporte mejorado para VoIP
- Soporte mejorado para ICQ
- Herramienta opcional PromiSwitch para monitoreo en ambientes de redes basadas en switches
- Nuevos tipos de licencia: Pro y Lite
- Soluciones a algunos problemas

Versión 1.3

- Soporte mejorado para VoIP
- Ahora son posibles conexiones al servicio NetResident
- Detalles adicionales de eventos (números de puerto e impresión de hora)
- Soporte de Windows Vista
- Soluciones a algunos problemas

Versión 1.2

- Soporte para protocolo IRC (Internet Relay Chat)
- Soporte para protocolo Telnet
- Soporte para VoIP (Voz sobre IP)
- Importación y exportación de Bases de Datos
- Soluciones a algunos problemas

Versión 1.1

- Suporte para protocolos de mensajes instantáneo Yahoo y Jabber
- Importación de registro mejorada que soporta muchos formatos de archivos de captura de terceros
- Administrador de tamaño de base de datos configurable que puede ser usado para borrar automáticamente eventos viejos.
- Soluciones a algunos problemas

Como Usar el Programa

Antes de Comenzar: Visibilidad de Red

La clave de un monitoreo de red satisfactorio es la visibilidad de tráfico de red. Si necesita monitorear sólo una computadora en la red, no hay preguntas de visibilidad de red: puede simplemente instalar y correr NetResident en la computadora. Sin embargo, si necesita monitorear múltiples computadoras en una LAN, es importante que comprenda como lograr visibilidad de red, por ejemplo la habilidad de “ver” tráfico de red de otras estaciones desde un único punto de observación.

En resumen, para monitorear otras computadoras en su LAN, necesita instalar NetResident en una computadora compuerta, o usar un switch con facilidad de “espejado de puerto”, o usar un hub. Hay muchos diseños posibles de red, por lo que si es nuevo en monitoreo de red, le recomendamos que lea el documento detallado e ilustrado de TamoSoft, Promiscuous Monitoring in Ethernet and Wi-Fi Networks (También está disponible la versión en PDF).

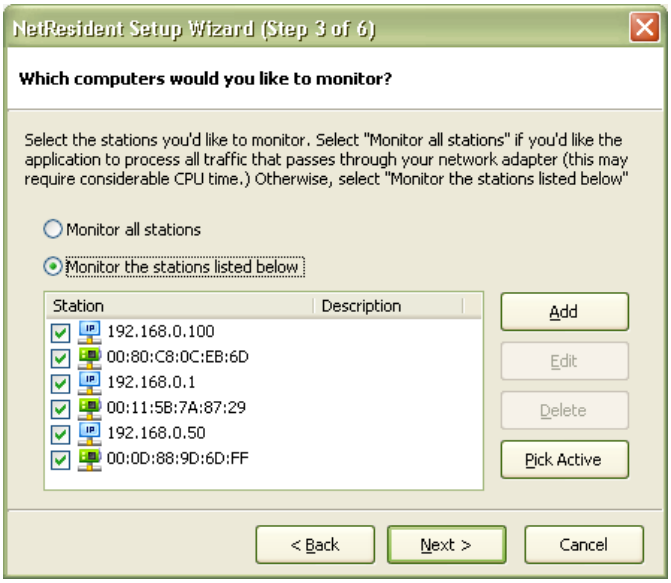
Hay disponible un utilitario opcional para monitoreo de redes Ethernet basadas en switches. Por favor vea el capítulo Herramienta PromiSwitch para más información.

Asistente de Configuración

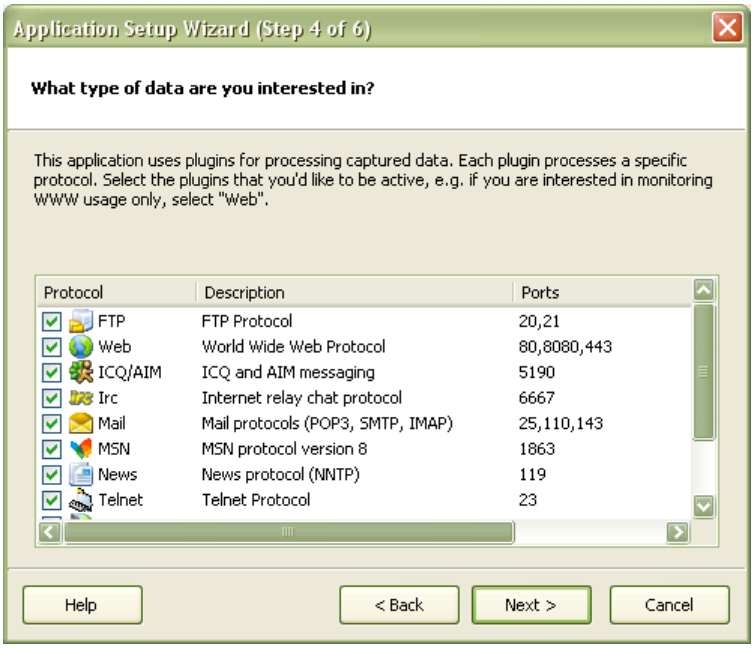
Antes que pueda comenzar a monitorear su red, debe configurar NetResident. El Asistente de Configuración le ayudará a configurar NetResident con solo algunos clic del ratón. Si no inicio el asistente cuando arrancó el programa por primera vez, puede hacerlo siempre pulsando **Herramientas =>Asistente de Configuración**.

Pulse **Siguiente** en la pantalla de bienvenida y vaya a la pantalla de selección de adaptador. La pantalla de selección de adaptador tuene una lista desplegable que le permite especificar el adaptador de red correcto para monitorear. Si su computadora tiene una conexión discada o está conectada a una LAN vía un adaptador Ethernet, tendrá un solo adaptador en el menú. Selecciónelo. Si su computadora sirve como portal de acceso a Internet para la LAN o tiene más de un adaptador de red, necesita seleccionar el adaptador que desea que NetResident monitoree. Algunos adaptadores de red no pueden funcionar en modo promiscuo. Si usa tal adaptador, por favor marque la casilla **Use modo no promiscuo**. Esta opción debe seleccionarse siempre para adaptadores inalámbricos (802.11). Para adaptadores discados y VPN, por favor seleccione el adaptador **minipuerto WAN.** Pulse **Siguiente** para ir a la pantalla de selección de estaciones.

El programa tratará de descubrir las estaciones de trabajo en su red y proveerá una lista de nodos que podría desear monitorear. La forma más fácil de configurar esta opción es seleccionar el botón **Monitorear todas las estaciones**. Esto hará que NetResident recoja todos los datos de la red. Siempre puede configurar este comportamiento y especificar cuales estaciones desea monitorear más adelante. Por favor vea el capítulo Estaciones Monitoreadas para más información.



Pulse el botón **Siguiente** para ir a la pantalla de selección de plugins. NetResident procesa tráfico de red usando módulos de protocolo de plugin. Si no necesita ver los datos transmitidos sobre un protocolo de red particular, podría desactivar el plugin correspondiente desmarcando la casilla junto al nombre del protocolo. Por favor lea el capítulo Plugins para más información.



La siguiente pantalla le permite configurar el comportamiento de monitoreo de red del programa. Seleccione la opción **Al inicio de Windows** si desea que el programa arranque monitoreando la red en cuanto se inicia Windows, o seleccione la opción **Al inicio de NetResident** si desea monitorear la red solo cuando está corriendo NetResident. Pulse **Siguiente** y luego **Finalizar** en la siguiente pantalla para guardar las preferencias de configuración.

Visión general de la Interfaz

NetResident puede mostrar información actual usando vistas que pueden cambiarse usando el ítem de menú **Eventos => Vistas** o pulsando el botón correspondiente en la barra de herramientas. El aspecto del programa podría variar dependiendo de la vista seleccionada, pero básicamente, la ventana de aplicación principal tiene tres secciones que presenta los datos en un formato estructurado y le permite filtrar y ordenar eventos de red y accederlos rápidamente.

La vista de **Grupos** muestra eventos agrupados por las fechas en que ocurrieron, protocolos de red, y hosts involucrados en las comunicaciones. Marcando o desmarcando las casillas junto al grupo incluirá/excluirá los eventos que pertenecen al grupo a/desde la sección **Lista de Eventos**. Los host son agrupados en **Partes** que representan las partes involucradas en el proceso de comunicación. El Parte A incluye todas las direcciones IP/Nombres de host del lado local de la comunicación. Si solo unas una interfaz de red para conectar a Internet, generalmente tiene solo una entrada bajo este Parte. Sin embargo, si usa su adaptador de LAN como el método principal de conexión a Internet, pero también usa ocasionalmente un adaptador de discado, o tiene una dirección IP asignada dinámicamente a su computadora cada vez que se conecta, tendrá varias entradas en este Parte. El Parte B incluye todos los host remotos que se han comunicado con el/los host/(s) local(es). Por favor refiérase a Disposición de Datos para más información.

La Vista **Explorador** es similar la Vista de Grupo excepto que muestra los eventos de red agrupados solo por protocolos de red. Sugerimos que use esta vista si desear ver los eventos para un protocolo especificado: por ejemplo, todos los mensajes ICQ para un determinado período de tiempo. Pulsando en el signo de suma expandirá los nodos, permitiéndole seleccionar y ver los eventos de red deseados. Por favor refiérase a Disposición de Datos para más información.

La sección **Lista de Eventos** muestra una lista de eventos disponibles para ver bajo las siguientes columnas:

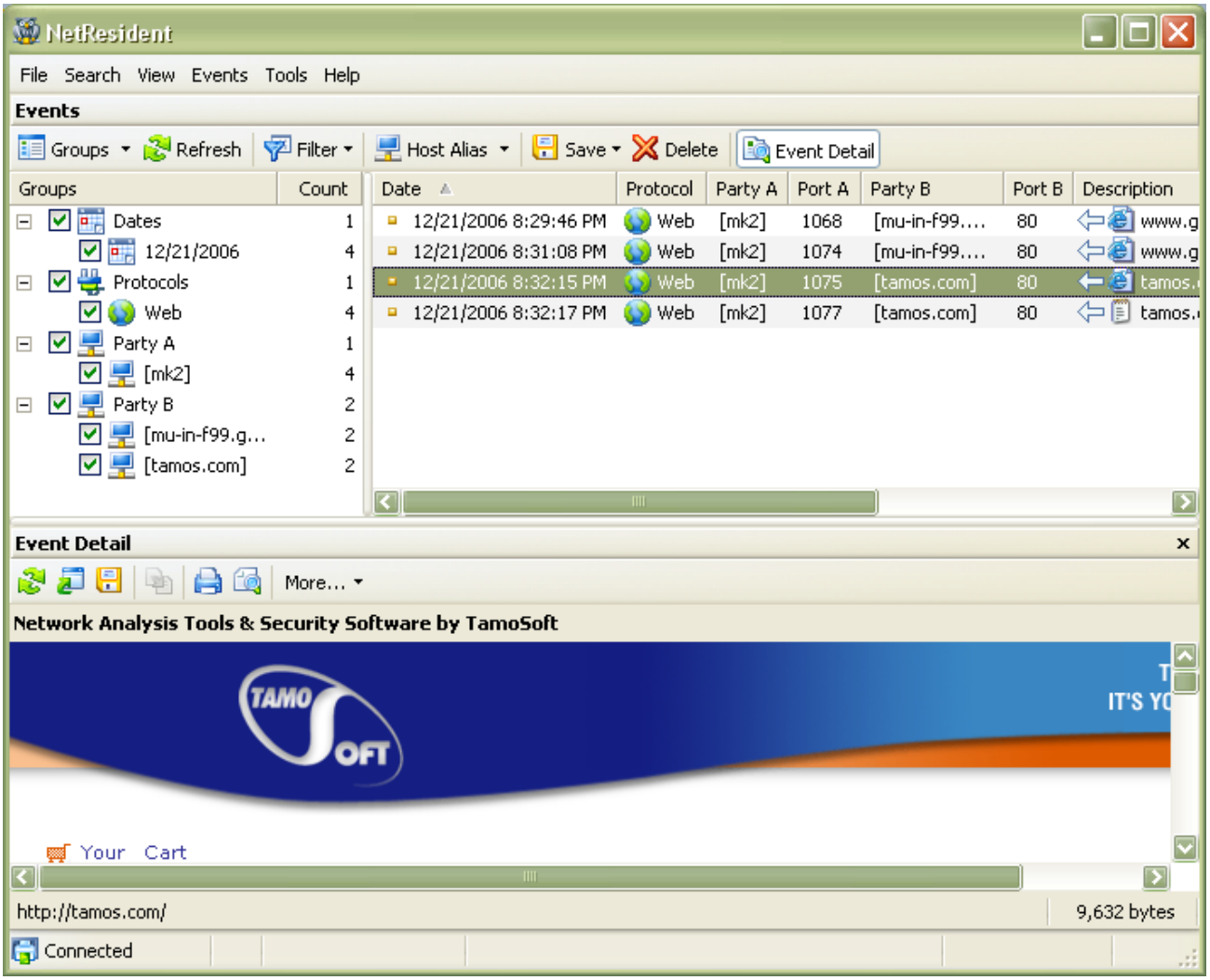
Fecha – la fecha en que se produjo el evento
Protocolo – El protócolo usado para la transmisión de datos
Parte A, Parte B – indica los host que enviaron y recibieron datos
Puerto A, Puerto B – Los puertos usados para la transmisión de datos
Última Actualización – la fecha y hora en que se actualizó por última vez el evento
Descripción – muestra el resumen de eventos

La sección **Detalle de eventos** muestra los contenidos reales de los eventos seleccionados en la sección **Lista de Eventos**. Puede mostrar solo un evento a la vez.

La ventana principal también tiene una sección **Estado** para mostrar mensajes del sistema producidos por el programa.

NetResident consiste de dos partes: La consola NetResident que se conecta al servicio NetResident, procesa los datos, los agrupa, y los presenta al usuario y el servicio NetResident que monitorea la red, captura los datos, y los almacena en la base de datos para procesamiento y vista.

NetResident use módulos de plugin de protocolos de red para procesar los datos recolectados. Puede activar y desactivar determinados plugins para asegurarse que ve solo los datos deseados.



Menú Principal	
Archivo	
Conectar	Hace una conexión al Servicio NetResident
Desconectar	Desconecta del Servicio NetResident
Administrar Base de Datos	Inicia el Asistente de Administrador de Base de Datos
Importar Registros	Inicia el Asistente de Importación de Registro
Salir	Cierra el programa
Buscar	
Encontrar	Busca los eventos para la búsqueda especificada
Encontrar de Nuevo	Repite la búsqueda
Ver	
Ventana de Estado	Muestra/oculta la Ventana de Estado
Barra de Estado	Muestra/oculta la Barra de Estado
Eventos	
Actualizar/Detener Actualizar	Actualiza todos los eventos/detiene el proceso de renovación

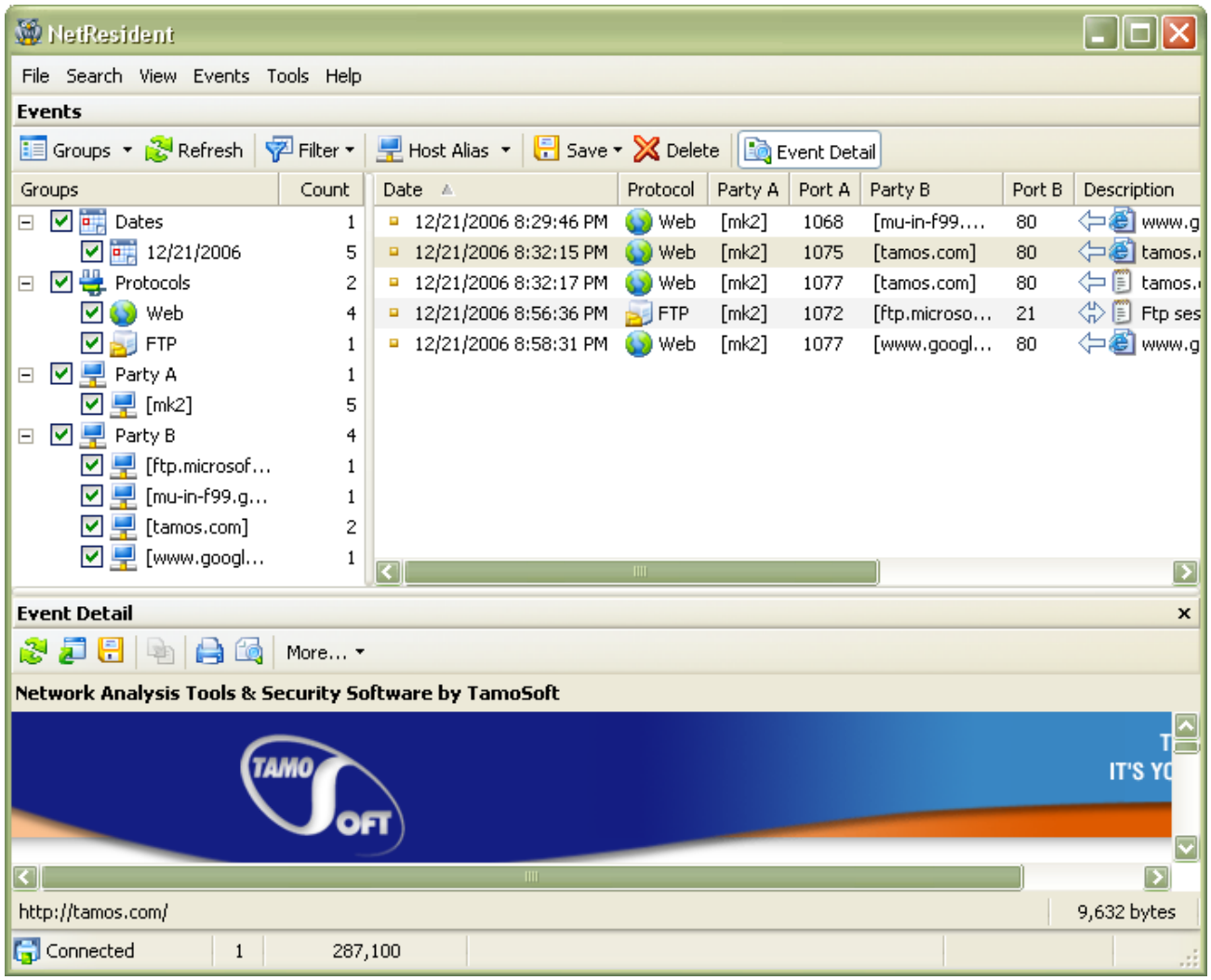
Filtro	Le permite fijar filtros de eventos
Guardar	Guarda la lista de eventos actual o los detalle de eventos a un archivo
Borrar	Borra los eventos seleccionados de la base de datos
Detalle de Evento	Muestra/oculta la sección de Detalle de eventos
Vistas	Intercambia las vistas de la ventana principal
Modo Muestra de Host	Cambia el modo de mostrar los host en las secciones Vista Grupos y Lista de Eventos
Herramientas	
Alias	Muestra el diálogo de Alias
Opciones	Muestra el diálogo de Opciones
Asistente de Configuración	Inicia el Asistente de Configuración
Herramienta Anti-Switch	Inicia la aplicación PromiSwitch
Idiomas	Le permite seleccionar el Idioma de la Interfaz de Usuario
Ayuda	
Contenido	Inicia la ayuda de NetResident
Buscar Ayuda Sobre...	Muestra el índice de ayuda de NetResident
Verificar por actualizaciones en la Web...	Busca una actualización en el sitio Web de TamoSoft
Acerca de	Muestra la ventana Acerca de

Como Organizar los Datos

NetResident es una ponderosa aplicación de monitoreo de red que presenta una figura detallada de actividades de usuarios de red. En una red cargada, puede ver cientos de miles de eventos de redes tales como mensajes de correos electrónicos, páginas Web, mensajes instantáneos, etc. El organizar los datos en una forma que le permita encontrar los eventos que está buscando es esencial cuando usa NetResident. Hemos implementado varias opciones de filtrado que le permitirá mostrar los datos en que está interesado.

NetResident tiene las vistas **Explorador** y **Grupos** que agrupa los eventos de red en forma distinta. Le sugerimos que mire ambos y luego elija uno que sea más conveniente para sus necesidades.

La sección **Vista de Grupos** en el lado izquierdo de la ventana principal del programa le permite filtrar los eventos de red por fecha, Parte de comunicación de red, o Host de red.



- **Fecha** – Marque la casilla al lado de las fechas de los eventos de red en los que está interesado. Los eventos que se producen en otras fechas serán ignorados y no serán mostrados en la sección **Vista de Evento**. Por favor advierta que las casillas no marcadas en la sección **Vista de Grupos** no borrará los datos de la base de datos. Puede configurar la sección **Vista de Grupos** para mostrar otros eventos que han sido registrados.

- **Protocolos** – marque la casilla al lado de protocolos que desea ver. Por ejemplo, si desea ver mensajes de correo electrónico, entonces seleccione el protocolo **Correo**.

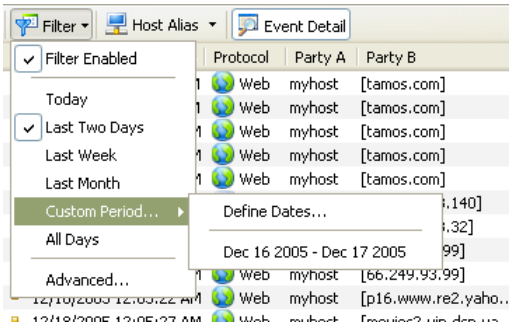
- **Parte A / Parte B** – le permite filtrar eventos de red por Parte de la comunicación de red. Encontrará hosts de red específicos bajo la Parte a o Parte B. Marque o desmarque las casillas al lado de ellos para monitorear eventos de red generados por estos hosts.

Por favor advierta que puede combinar filtros: por ejemplo, si deseara ver solo las páginas Web descargadas de un servidor en particular en determinado día, por favor seleccione la fecha en la sección **Fechas**, seleccione **Web** en la sección **Protocolos**, y especifique el host en la sección **Parte B**. Todos los demás eventos que no coinciden con el criterio serán ignorados.

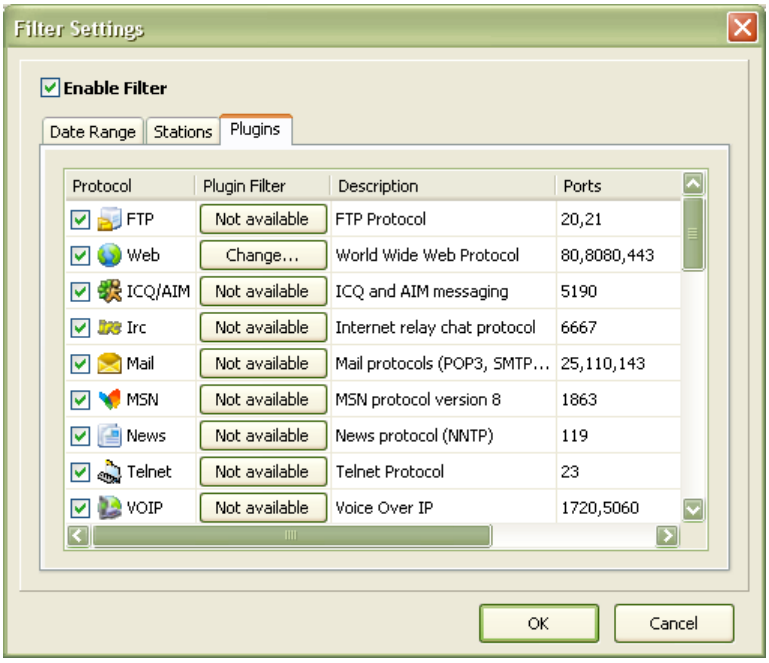
Un filtro de fechas más flexible está disponible en el menú **Eventos =>Filtro** o pulsando el botón de la barra de herramientas **Filtro**. Puede especificar un período predefinido:

- **Hoy** – Muestra todos los eventos de red que se produjeron hoy
- **Dos Últimos Días** – Muestra todos los eventos de red que se produjeron durante los dos últimos días
- **Última Semana** – Muestra todos los eventos de red que se produjeron durante la última semana
- **Último Mes**– Muestra todos los eventos que se produjeron durante el último mes

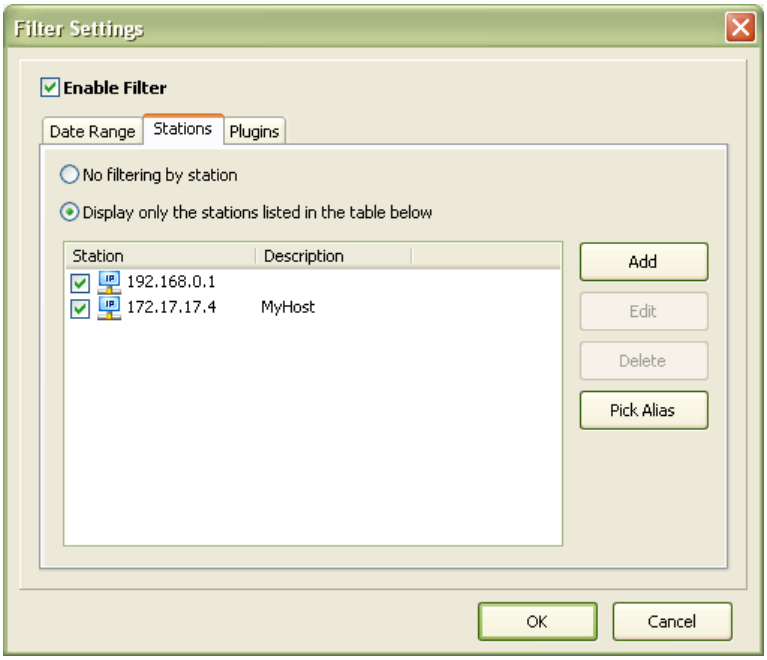
Seleccionando **Todos los Días** del menú hará que el programa muestre eventos para todo el período monitoreado. También puede especificar el rango de fechas bajo el ítem de menú **Período Personalizado,** seleccionando las fechas **Desde** y **Hasta** en las listas desplegadas correspondientes.



Hay disponibles más opciones avanzadas de filtrado bajo el menú **Eventos => Filtro => Avanzado**. También puede filtrar los eventos por plugins de protocolos de red o por estaciones.



La página **Plugins** muestra todos los plugins instalados actualmente. Los plugins activos tienen casillas marcadas junto a sus nombres. Si necesita determinados plugins (por ejemplo, necesita ver páginas Web y correos electrónicos solamente), desactive los plugins innecesarios desmarcando las casillas correspondientes. Si el plugin especificado soporta filtrado adicional, puede cambiar este filtro pulsando el botón Cambio en la columna correspondiente. Por favor refiérase al capítulo Plugins para una detallada descripción de plugin.



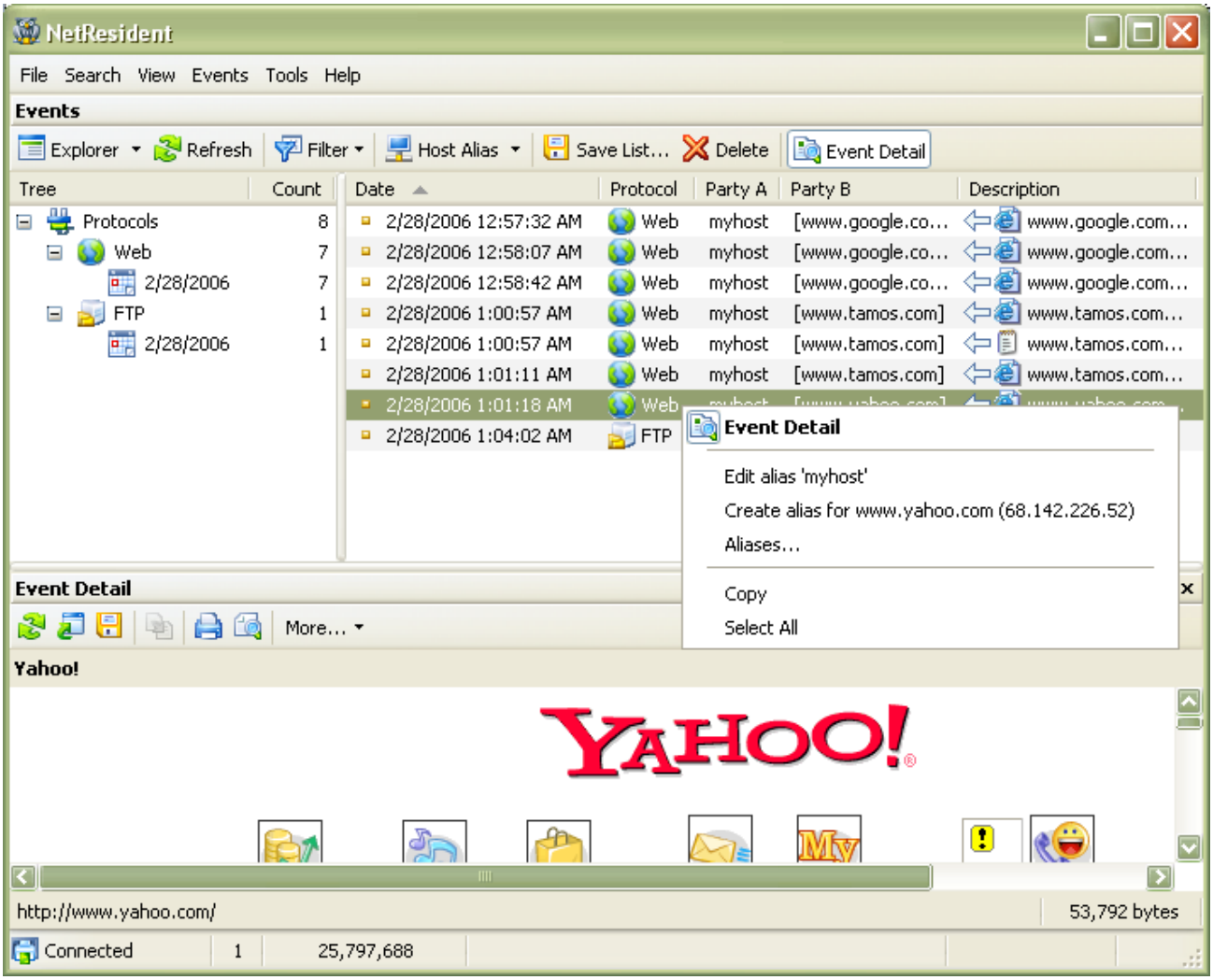
NetResident le permite mostrar los datos recibidos solo de estaciones seleccionadas (computadoras, routers, o demás dispositivos conectados a su LAN). En ese caso, NetResident solo mostrará los datos desde/hacia computadoras listadas en la tabla de la sección **Estaciones**. Puede agregar otras estaciones seleccionando **Mostrar solo estaciones listadas en la tabla siguiente**, pulsando el botón **Agregar** y especificando la dirección IP, Rango de direcciones IP, o dirección física (MAC) de la estación. Si ha asignado previamente alias a hosts, puede pulsar el botón **Elegir Alias** y elegir una estación de la lista de alias. También puede ingresar una descripción opcional para cada estación agregada. Edite una estación seleccionándola y pulsando el botón **Edit (Editar)**. Si desea quitar una estación de la lista, selecciónela y pulse el botón **Borrar.**

Pulse **OK** para guardar la configuración de filtro o pulse **Cancelar** para desechar la preferencia.

Si desea desactivar temporalmente el filtro sin desechar la preferencia de filtro, desmarque la casilla **Activar Filtro**.

Importante: La preferencia de filtro solo afecta los datos mostrados en la ventana principal del programa. La preferencia de filtro no cambia la recolección de datos o comportamiento de almacenamiento de datos del programa. Las preferencias de recolección de datos está descriptas en el capítulo Configurar NetResident de este manual, y las opciones de almacenamiento de datos están descriptas en el capítulo Administración de Base de Datos.

La sección **Vista de Explorador** en el lado izquierdo de la ventana principal del programa le permite filtrar eventos de red por protocolos de red.

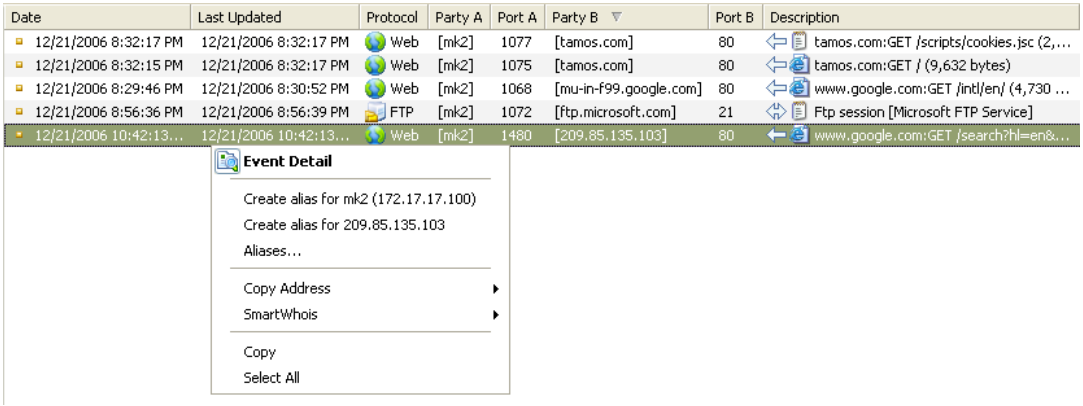


Expanda los nodos deseados pulsando el signo suma (+) a la izquierda del nodo. Si desea ver páginas web, expanda el nodo Web. El nodo expandido le permite ver los eventos de red del protocolo especificado agrupados por fecha. Si desea ver los eventos de red que ocurrieron en un día específico, seleccione el grupo deseado en la izquierda y ver los eventos de red mismos a la derecha. La vista de Explorador es similar a la Vista de Grupo excepto por la forma en que se agrupan los eventos de red.

Como Navegar Eventos de Red

NetResident muestra intercambio de datos sobre la red en la forma de eventos de red. Ejemplos de eventos incluyen un mensaje de correo electrónico, un archivo descargado vía FTP, Una página Web descargada, o un mensaje instantáneo de ICQ. Después de haber configurado las opciones de filtrado de datos, la sección **Lista de Eventos** muestra la lista cruda de eventos que NetResident ha filtrado de la base de datos.

Cada línea en la tabla de Lista de Eventos representa un evento de red.



La tabla tiene las siguientes columnas:

- **Fecha** – La fecha y hora en que comenzó el evento.
- **Última Actualización** – la fecha y hora en que el evento fue actualizado por última vez.
- **Protocolo** – El protocolo de red usado para la transmisión de datos. El nombre del protocolo corresponde al nombre del módulo plugin responsable para procesar el evento en particular.
- **Parte A / Parte B** – Partes emisores y receptores en el intercambio de datos de red. Un ejemplo de Partes podría ser una computadora descargando una página Web y un servidor Web que aloja la página, o una computadora que recibe correos electrónicos y el servidor de correo que aloja a la casilla de correo.
- **Puerto A/Puerto B** – los puertos usados para transmisión de datos.
- **Descripción** – Una breve descripción del evento de red que incluye el tamaño del objeto transmitido.

Las Partes A y B participantes en una conexión podrían ser mostradas por sus direcciones IP o Físicas (MAC) o por los nombres de host asociados con la dirección IP de la Parte. Las opciones de muestra pueden configurarse en el menú **Eventos => Modo Muestra de Host**.

Puede sustituir las direcciones IP o Físicas (MAC) con nombres leíbles por humanos y fáciles de recordar (alias). Pulsando el botón derecho sobre cualquier evento de red y seleccione la dirección del menú desplegado para crear un alias para los host Parte A y Parte B, o para abrir la lista de alias.

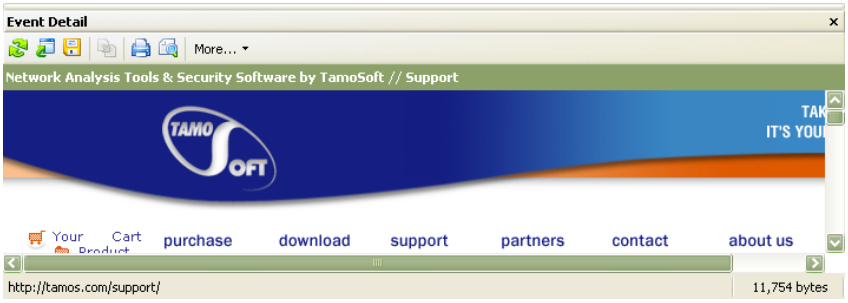
Guardar la lista de eventos a un archivo HTML seleccionando **Eventos => Guardar Lista...** o pulsando el botón correspondiente en la barra de herramientas.

Para ver un evento de red en la sección Detalle de evento, pulse en la línea de evento en la **(Lista de Eventos**. Pulsando el botón derecho en un evento y seleccionando **Detalle de Evento** del menú desplegado ocultará la sección Detalle de Evento.

Importante: Algunas columnas podrían faltar en la Vista de Explorador (dependiendo del grupo de registro seleccionado). Por ejemplo, si el protocolo especificado es seleccionado, la columna correspondiente con el nombre del protocolo faltará.

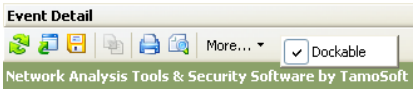
Como Ver Detalle de eventos

La sección **Detalle de Evento** de la pantalla principal muestra el evento de red reconstruido. Para mostrar la sección **Detalle de Evento,** pulse **Eventos => Detalle de eventos** o pulse el botón derecho en un evento de red en la sección **Vista de Evento** y seleccione **Detalle de Evento** del menú desplegado. Alternativamente, puede pulsar el botón correspondiente en la barra de herramientas para mostrar la sección **Detalle de Evento**. Los plugins de protocolo de NetResident procesan los datos y reconstruyen la página Web completa, mensajes de correo electrónico, sesiones de Chat de mensajería instantánea, etc.



Una vez que un evento de red es seleccionado en la sección **Vista de Eventos** de la ventana principal, NetResident consultará la base de datos reconstruyendo los detalle de evento, mostrando los resultados en la sección **Detalle de evento**. Además de mostrar el evento en si mismo, el programa muestra información útil de servicio acerca del evento, tales como los encabezados HTTP para páginas Web, Encabezados de Correo Electrónico para mensajes de correo electrónico, y registros de sesión FTP para sesiones de transferencia de archivos FTP.

La sección **Vista de Eventos** tiene una barra de herramientas y un menú que ofrece distintas opciones, dependiendo del tipo de evento seleccionado.



Puede arrastrar la sección **Vista de Eventos** y colocarlo en cualquier lugar de la ventana principal del programa. Para traer de nuevo el panel, arrástrelo sobre la ventana principal hasta que se adose el mismo a un lado de la ventana. Para desactivar la ubicación automática, pulse el botón derecho sobre en encabezado y desmarque la casilla **Ubicable**.

El menú de sección **Detalle de Eventos** ofrece las siguientes opciones:

Preferencias de Interfaz – Le permite configurar la preferencia de fuente para el evento mostrado
Copiar – copia los datos seleccionados al portapapeles
Seleccionar todo – selecciona todos los datos relativos al evento de red

Además a las opciones generales mencionadas arriba, cada plugin de NetResident plugin ofrece opciones específicas del plugin (dependiendo del tipo de evento de red) que puede ver en este menú. Por ejemplo, la opción **Mostrar Autenticación/Contraseña** muestra la autenticación y contraseña usada para sesiones de correo (para mensajes de correo electrónico solamente); La opción **Ver Encabezados** muestra encabezados de Sesión HTTP (para páginas Web solamente), etc.

Como Configurar NetResident

Las opciones de configuración NetResident están disponibles bajo el menú **Herramientas => Opciones**. Si es un usuario novel o no familiarizado con redes, le sugerimos que inicie el Asistente de Configuración para guiarlo a través del proceso de configuración.

La ventana **Opciones** le permite configurar NetResident para cubrir sus necesidades. Seleccione una categoría del menú en el lado izquierdo de la ventana para configurar las opciones disponibles para cada ítem menú.

Interfaz: General

Le permite cambiar la preferencia de fuente de la interfaz y configurar el modo actualización.

Por favor marque la casilla **Activar actualizaciones automáticas** para activar actualizaciones, También, puede configurar el intervalo en que NetResident verificará por actualizaciones; ingrese el valor deseado en el campo **Intervalo entre verificaciones, días**. Pulsando el botón **Verificar Ahora** hará que NetResident verifique inmediatamente por actualizaciones.

Red: Inicio

Le permite configurar la función de monitoreo de red realizado por Servicio NetResident.

Si necesita monitorear su red constantemente, seleccione la opción **Al Inicio de Windows**. Cuando este botón es seleccionado, El Servicio NetResident se iniciará al inicio de Windows y comenzará a monitorear la red. Puede iniciar NetResident y ver los resultados de monitoreo en cualquier momento.

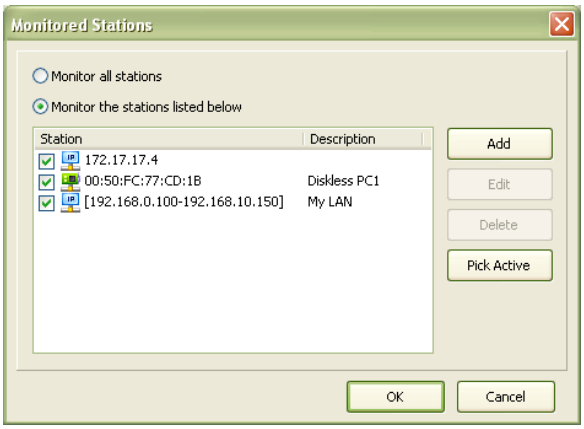
Si usa NetResident periódicamente y no necesita monitorear su red en todo momento, le sugerimos que seleccione **Al inicio de NetResident**. Esto le permitirá ahorrar espacio en disco y reducir la carga de CPU. Seleccionando esta opción, el Servicio NetResident inicia con la aplicación NetResident y comienza a monitorear la red. La recolección de datos de red se detendrá una vez que cierre la aplicación.

Red: Objetivos

La opción de menú **Objetivos** tiene una lista desplegada que le permite especificar el adaptador de red correcto para monitorear la red. Si su computadora tiene una conexión discada o está conectada a la LAN por un adaptador Ethernet, tendrá solo un adaptador a la lista; selecciónelo. Si su computadora sirve como portal de acceso a Internet para la LAN o tiene más de un adaptador de red, necesitará seleccionar el adaptador que desea para monitorear con NetResident. Algunos adaptadores de red no pueden funcionar en modo promiscuo; si usa tal adaptador marque la casilla **Use modo no promiscuo**. Esta opción debe ser seleccionada siempre para adaptadores inalámbricos, para adaptadores discados y VPN, seleccione el adaptador **Minipuerto WAN**.

Para analizar datos de todas las computadoras en la red, active la opción **Monitorear todas las Estaciones**. Si está en una red muy cargada, podría desear angostar el rango de estaciones que monitorea NetResidents.Pulse el botón **Avanzado** y seleccione el botón **Monitorear las estaciones listadas a continuación**. Marque las casillas junto a las estaciones seleccionadas. Si el botón **Avanzado** está grisado, desactive la opción **Monitorear Todas las Estaciones** y el botón se hará disponible.

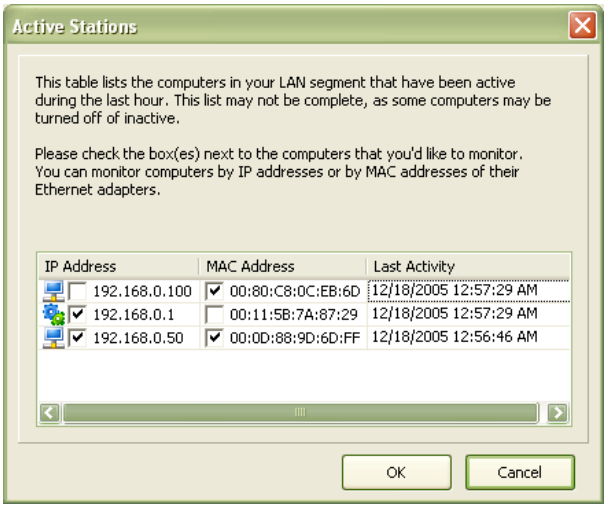
Estaciones Monitoreadas



Puede agregar una nueva estación pulsando el botón **Agregar** e ingresando las direcciones IP o física MAC o un rango de direcciones IP. El campo **Descripción** es usado para ingresar cualquier información acerca de la(s) estación(es) agregada(s). Este campo es optativo.

Pulse **OK** para guardar las preferencias o **Cancelar** para desechar los cambios. Use los botones **Editar** y **Borrar** para cambiar o quitar las estaciones en la lista. Si desea desactivar el monitoreo de una estación en particular temporalmente. Sin quitarla de la lista, desmarque la casilla al lado de esta.

También podría desear agregar las estaciones activas pulsando el botón **Tomar Activa** y marcando las estaciones activas descubiertas por NetResident:



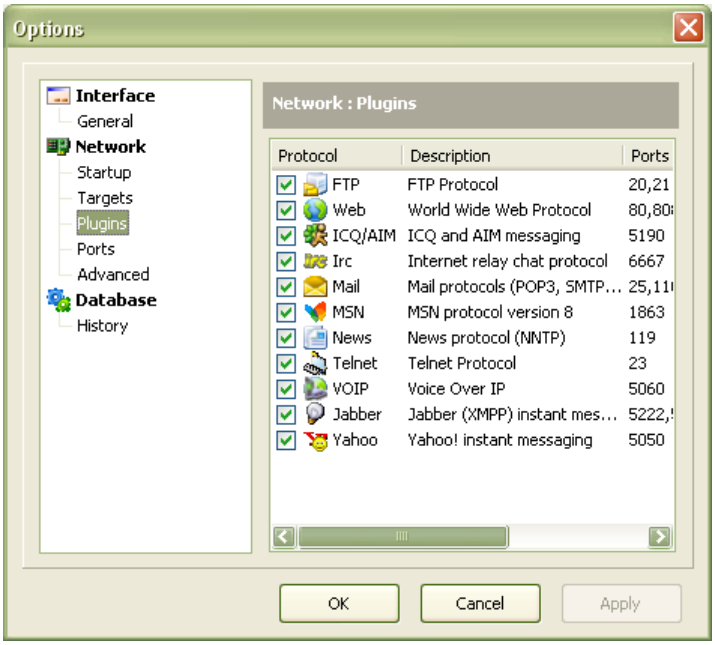
Seleccione las direcciones deseadas marcando las casillas correspondientes y pulsando **OK**. Las direcciones seleccionadas se agregarán a la lista de estaciones para monitorear.

Por favor advierta que la lista de estaciones puede estar incompleta, dado que algunas estaciones podrían estar apagadas o haber cambiado sus direcciones. También, algunas estaciones podrían estar ocultas detrás de firewalls. Por favor use esta lista solo como su referencia.

Si no está seguro si debería elegir direcciones IP o Físicas (MAC) para identificar las estaciones monitoreadas, por favor refiérase al capitulo Preguntas Frecuentes.

Red: Plugins

Esta página muestra la lista de los plugins actualmente instalados usados por NetResident. Si no usa algunos plugins, le sugerimos que los deshabilite anulando la selección en sus respectivas casillas para reducir la carga de CPU y la utilización de espacio en disco.


Options
Interface
General
Network
Startup
Targets
Plugins
Ports
Advanced
Database
History
Network : Plugins
Protocol
Description
Ports
FTP
FTP Protocol
20,21
Web
World Wide Web Protocol
ICQ/AIM
ICQ and AIM messaging
5190
Irc
Internet relay chat protocol
6667
Mail
Mail protocols (POP3, SMTP...
MSN
MSN protocol version 8
1863
News
News protocol (NNTP)
119
Telnet
Telnet Protocol
23
VOIP
Voice Over IP
5060
Jabber
Jabber (XMPP) instant mes...
Yahoo
Yahoo! instant messaging
5050
OK
Cancel
Apply

Red: Puertos

Esta página le permite configurar los números de puertos usados por NetResident para monitoreo de tráfico.

Por defecto, el Servicio NetResident está configurado para monitorear tráfico sobre todos los puertos posibles (1-65535). Esto asegura que todos los datos de red posibles podrían ser interceptados. Sin embargo, se requiere mucho tiempo de CPU para procesar todos los paquetes de red interceptados (incluso los no deseados). Si experimenta problemas relativos a rendimiento, trate de angostar el número de puertos usados para intercepción de datos. Por ejemplo, si monitorea tráfico sobre una red de oficina local donde la mayoría del tráfico es generado por transferencia de archivos de una computadora a otra por medios de Microsoft Windows, podría desear excluir este tráfico ingresando la siguiente línea:

139,445

La línea de arriba desactiva el monitoreo de los puertos 139 y 445. Si no sabe cuales son los puertos o no experimenta ninguna dificultad relativa a rendimiento cuando corre NetResident, no cambie ningún valor de esta página.

Puede especificar uno o varios puertos separados por comas o un rango de puertos. Por favor advierta que la exclusión de puertos será aplicada a los puertos de origen y de destino

Red: Conexiones Remotas

Esta página le permite configurar conexiones remotas al servicio NetResident. Por favor vea el capítulo Conexiones Remotas al Servicio NetResident para más información.

Red: Avanzado

Esta página le permite configurar el comportamiento de autenticación del programa. La opción de autenticación **activar servicio** está activada por defecto y la autenticación está fijada al nivel **Silencioso**. Si experimenta problemas con NetResident, el equipo de soporte de TamoSoft podría solicitarle que cambie el nivel de servicio de autenticación si se requiere información adicional. Los mensajes del servicio NetResident son escritos al archivo DebugCWS.log ubicado en la carpeta de la aplicación y el equipo de soporte de TamoSoft podría requerirle que nos envíe este archivo por correo electrónico. Por favor advierta que este archivo podría tener un tamaño considerable si la opción **detallado** está seleccionada. Siempre comprima (zip) el archivo de registro antes de enviarlo a soporte a cliente.

Base de Datos: Historial

Dado que la base de datos contiene registros de todos los eventos capturados por NetResident, el tamaño de la base de datos se incrementa con el tiempo. Para reducir el espacio ocupado por estos registros e incrementar el rendimiento del programa, podría querer activar el modo de limitación de tamaño de base de datos marcando la casilla **Limitar Tamaño de Base de Datos**. El campo **Borrar los eventos mas viejos que** contiene el número de días que NetResident mantendrá los registros. Los registros más antiguos serán borrados automáticamente.

Puede vaciar la base de datos automáticamente cada vez que termina de trabajar con el programa marcando la casilla **limpiar la base de datos al salir**.

Alias

Los Alias son nombres leíbles por humanos y fáciles de recordar que pueden sustituir las direcciones IP y Físicas (MAC) mostradas en las secciones **Vista de Grupo** y V**ista de Eventos** de la ventana principal del programa. Esto puede hacer más fácil reconocer y analizar eventos de red.

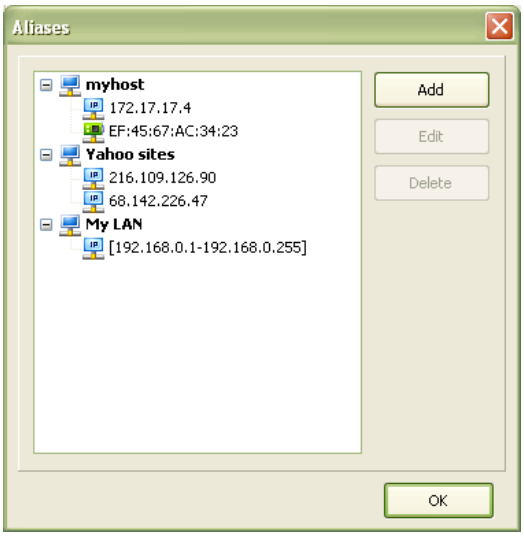
Una vez que un Alias es asignado a una dirección IP o Física (MAC), se reemplazarán las direcciones correspondientes en las secciones **Vista de Grupo)** y **(Vista de Eventos** de la ventana principal. Puede elegir como son mostrados los host participantes de las comunicaciones: por **Dirección IP**, por **Dirección Física (MAC)**, o por **Alias de Host**. Configure como son mostrados los hosts en el menú **Eventos =>Modo Muestra de Host**.

El programa tiene capacidad de resolver las direcciones IP en nombres de host. Marque el ítem **Resolver direcciones IP Numéricas a Nombres de Host** en el menú **Eventos =>Modo de Muestra de Host** para activar la resolución de direcciones IP.

También se podría asignar un alias a un rango de direcciones IP. Esto es muy conveniente, dado que le permite tener solo un nombre para un grupo de dispositivos de red – por ejemplo, todas las computadoras en una LAN.

Cada Alias es único. Sin embargo, puede asignar el mismo alias a varias direcciones IP o Físicas (MAC), formando de esta forma un grupo. Esto es útil si una computadora tiene varias direcciones de red y desea identificarlas con un nombre.

Puede agregar, editar, o borrar alias pulsando **Herramientas=> Alias**



Pulse el botón **Agregar** para agregar una estación. Ingrese un nombre de alias y pulse el botón **Agregar**. Una ventana de diálogo se abrirá solicitándole que ingrese la dirección para el alias y seleccione su tipo: **Dirección IP, Rango de Dirección IP**, o **Dirección MAC**. Si desea agregar un rango de direcciones IP, seleccione el botón **Rango de Dirección IP** e ingrese las direcciones IP de comienzo y final para el rango en los campos correspondientes.

Pulse el botón **OK** para actualizar la lista de alias o pulse **Cancelar** para desechar los cambios. Puede editar un alias seleccionando y pulsando los botones **Editar** o **Borrar.**

También podría asignar alias a hosts pulsando el botón derecho sobre un evento de red en la sección **Event View (Vista de Eventos)** de la ventana principal y eligiendo el ítem correspondiente del menú desplegado.

Como Importar Archivos de Registro de Paquetes

NetResident usa sus capacidades de monitoreo y registro para análisis y presentación de datos de red. También le permite importar archivos de captura de paquetes guardados por otros programas de monitoreo de red de TamoSoft: CommView y CommView para WiFi, así como algunas otras aplicaciones de monitoreo de red de terceros.

Inicie el Asistente de Importación de Registros pulsando **Archivo => Importar Registros**. Se le solicitará que seleccione el archivo a importar y configurar las opciones de importación. El archivo importado podría haberse grabado un tiempo atrás y podría desear importar el archivo con la fecha actual asignada a todos los eventos en el registro. En contrario, todos los datos serán importados con su fecha original de acuerdo con la fecha estampada en el archivo de registro.

Nota: Esta opción no está disponible para todos los tipos de archivos de registro.

Importante: Alguno o todos los eventos en el archivo de registro podrían borrarse de la base de datos justo después de importarse debido a que la aplicación podría estar configurada para borrar eventos antiguos. Si las fechas estampadas en el archivo de registro son más antiguas que el número de días especificado en las opciones de la aplicación, considere usar la fecha actual cuando importa archivos de registro, o incremente el lapso de tiempo de eventos en las opciones de la aplicación. Por favor vea la descripción de la opción Base de Datos: Historial para más información.

Podría importar solo los eventos de su interés en lugar de importar el archivo el registro completo. Marque la **Usar filtros de servicios actuales mientras importa los datos**. El asistente de importación usará entonces las preferencias de filtro actual para el servicio NetResident.

Por favor asegúrese que el **Vista de Grupo** actual y las preferencias de filtro le permiten a NetResident para mostrar los datos que se están importando. De otro modo, no podrá verlos en la ventana principal, incluso si los datos están importados satisfactoriamente dentro de la base de datos, hasta que cambie estas preferencias.

Pulse el botón **Siguiente** para importar el archivo seleccionado. Puede esperar hasta que se complete la importación o pulse el botón **Finalizar** para continuar importando en segundo plano. En este caso, el programa notificará cuando se haya completado la importación. La importación puede cancelarse en cualquier momento pulsando el botón **Cancelar**.

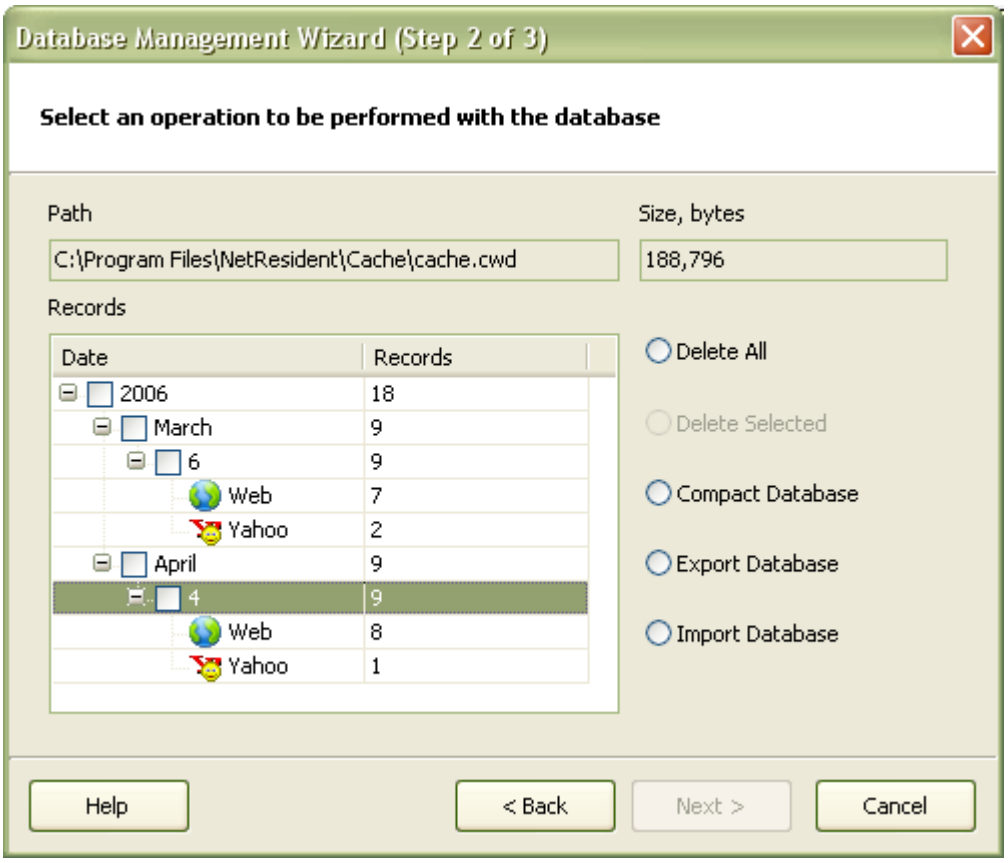
Nota: No está disponible la importación de archivos de registro para usuarios de licencia Lite.

Administración de Base de Datos

Toda la información de red capturada y analizada es guardada en la base de datos de NetResident. La base de datos puede crecer eventualmente a un tamaño tal que afectará el rendimiento del programa. Los registros podrían hacerse obsoletos con el tiempo. En estas instancias, le sugerimos que quite los registros innecesarios usando el **Asistente de Administración de Base de Datos**.

Pulse **Archivo=> Administrar Base de Datos** para iniciar el **Asistente de Administración de Base de Datos**.

Pulse el botón **Siguiente** para ver el estado actual de la base de datos, su tamaño y el número de registros. También, seleccione la operación a realizar con la base de datos.



Ver los eventos de red actuales guardados en la base de datos NetResident sobre esta página. La columna **Fecha,** le permite encontrar registros por su fecha (año, mes, día) en que se produjeron los eventos de red grabados. Las columnas **Registros** muestran el número de eventos de red para el período, seleccionado en la columna **Fecha**. Para borrar todos los eventos de red en la base de datos, seleccione la opción **Borrar Todo**, o para borrar registros para un período de tiempo especificado (día, mes, año), marque la casilla correspondiente y seleccione la opción **Borrar Seleccionado**.

Importante: ¡Los registros serán borrados permanentemente y no se pueden recuperar!

Si desea guardar la base de datos para mayor uso en otra computadora, seleccione **Exportar Base de Datos**. NetResident guardará la base de datos en un archivo que puede ser visto más tarde seleccionando la opción **Importar Base de Datos**.

Nota: ¡Importar la base de datos borra todos los registros en su base de datos actual!

Elija la operación deseada y pulse el botón **Siguiente**. Cuando selecciona las opciones Importar o Exportar se le solicitará el nombre de archivo de la base de datos. El mantenimiento de la base de datos podría tomar una cantidad de tiempo significativa. El monitoreo y registro de datos será pausada mientras los cambios están ingresándose en la base de datos.

Servicio NetResident

El servicio NetResident corre en segundo plano capturando tráfico de red, analizándolo, y agregándolo a la base de datos. El servicio arranca automáticamente al inicio de Windows y está activo en todo momento. Dependiendo de la configuración del programa, captura el tráfico en todo momento o solo cuando es iniciado NetResident. Este comportamiento es configurado en la ventana **Herramientas => Opciones, Red => Inicio** en el menú. Por favor refiérase a la sección Red: Inicio del manual para más información.

Normalmente, no necesita arrancar o detener manualmente el Servicio NetResident. Si necesitara hacerlo, el servicio puede ser controlado desde el grupo de programa NetResident (ítems **Stop NetResident Service** / **Start NetResident)** o en **Panel de Control => Herramientas Administrativas => Servicios.**

Conexiones Remotas a Servicio NetResident

Como se mencionó anteriormente, NetResident consiste de dos partes: La consola NetResident que se conecta al servicio NetResident, procesa los datos, los agrupa. Y los presenta al usuario y el Servicio NetResident que monitorea la red, captura los datos, y los almacena en la Base de Datos para procesamiento y vista. La conexión entre el servicio y la consola se hace sobre TCP/IP, lo que significa que puede conectarse al servicio NetResident corriendo en cualquier computadora, mientras se pueda conectar sobre TCP/IP y conozca la contraseña.

Cuando inicia NetResident, este inicia una conexión al servicio NetResident al que se conectó por última vez (por defecto, esta es la PC local). Para conectarse a otro servicio NetResident, haga lo siguiente:

- Pulse **Archivo => Desconectar** para desconectarse del servicio NetResidental cual está conectado actualmente.
- Pulse **Archivo=> Conectar**.
- Seleccione la opción **Conectar al servicio local** si desea conectarse al servicio NetResident que corre en la computadora que está usando actualmente. Si quisiera conectarse a una computadora remota que corre NetResident, seleccione la opción **Conectar a servicio remoto**.
- Si seleccionó la opción **Conectar a servicio remoto**, especifique la dirección IP de la computadora a la que quiere conectarse y la contraseña en los campos **Servicio remoto** y **Contraseña** respectivamente.
- Pulse **OK**.

Por favor advierta que las conexiones remotas al servicio NetResident están desactivadas por defecto por razones de seguridad. Para activar esta opción, el servicio NetResident debería estar adecuadamente configurado en la computadora a la que desea conectarse. Para configurar NetResident, inicie el programa y seleccione **Herramientas => Opciones => Red => Conexión remota**. Marque la casilla **Permitir conexiones remotas a este servicio** y especifique la contraseña para conectarse a este servicio en el campo **Contraseña**. Confirme la contraseña ingresándola nuevamente en el campo **Confirmar contraseña** y pulsando **OK**.

Nota: Nunca se le solicitará la contraseña cuando se conecta localmente al servicio NetResident.

Plugins

NetResident usa un sistema de plugin de modulo de protocolo para procesar y mostrar eventos de red. Cada plugin es responsable del procesamiento de un protocolo o varios protocolos de red. El paquete de instalación de NetResident viene con los siguientes plugins de protocolos:

- **Web** – procesa los datos transmitidos sobre protocolo HTTP. Este plugin es responsable de mostrar páginas Web.
- **Mail** – procesa los datos transmitidos sobre protocolos POP3, SMTP, e IMAP. Estos protocolos son usados por software de clientes y servidores de correo electrónico para intercambios de mensajes de correo electrónico.
- **News** – procesa los datos transmitidos sobre protocolo NNTP. Este protocolo es usado para publicar y ver mensajes de newsgroup.
- **ICQ/AIM –** procesa los datos transmitidos sobre protocolos de mensajería instantánea ICQ y AOL.
- **MSN** – procesa los datos transmitidos sobre protocolo de mensajería instantánea MSN versión 8.
- **FTP** – procesa los datos transmitidos sobre protocolos FTP usados para descargar/subir archivos desde/hacia servidores FTP.
- **Yahoo –** procesa los datos transmitidos sobre el protocolo de mensajería instantánea de Yahoo.
- **Jabber** – procesa los datos transmitidos sobre protocolo XMPP. Este protocolo es usado para mensajería instantánea por distintos clientes Jabber, incluyendo Google Talk. Por favor advierta que el plugin **Jabber** no puede capturar mensajes codificados en SSL.
- **IRC** – procesa los datos transmitidos sobre protocolo Internet Relay Chat.
- **Telnet** – procesa los datos transmitidos sobre protocolo Telnet.
- **VoIP** – procesa los datos transmitidos sobre protocolo SIP usando flujo de voz RTP.

Nota: La reproducción de voz capturada no está disponible para usuarios de licencia Lite.

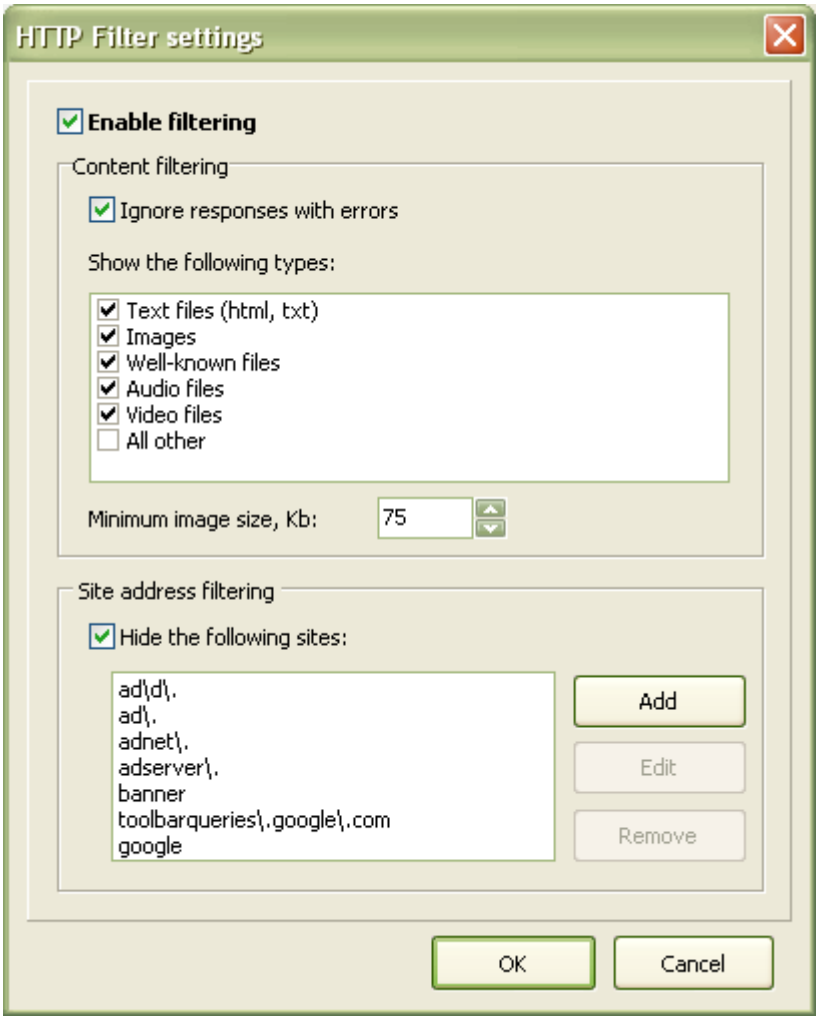
Los módulos Plugin están ubicados en la subcarpeta Plugins en la carpeta de la aplicación. Por defecto, todos los plugins están activados, por ejemplo, procesan datos de red y los guardan en la base de datos. Si no está interesado en procesar y almacenar los datos transmitidos sobre determinados protocolos, puede desactivar los plugins correspondientes para disminuir la carga de CPU y la utilización de espacio en disco.

Pueden agregarse plugin adicionales desde TamoSoft a NetResident a medida que estén disponibles. Coloque el archivo de módulo plugin en la subcarpeta Plugins en la carpeta de la aplicación. Después de agregar un plugin, reinicie el servicio NetResident para cargar el nuevo módulo. Pulse los ítems de menú **Stop NetResident Service** / **Start NetResident** en el grupo de programa NetResident para reiniciar el servicio.

Algunos Plugins NetResident podrían configurarse. Para configurar un plugin, Seleccione **Eventos => Filtro => Avanzado**. Vaya a la pestaña **Plugins**. Seleccione el plugin deseado y pulse el botón **Cambiar**. En este momento el plugin HTTP soporta configuración:

Filtro de Plugin HTTP

Mostrar una página Web requiere una gran cantidad de archivos auxiliares a ser cargados por el navegador automáticamente cuando abre la página Web. El propósito de este filtro es ocultar todos los archivos auxiliares para reducir la cantidad de registros mostrados.



Por favor marque la casilla **Activar filtrado** para activar el filtro HTTP. Si desea desactivar temporalmente el filtro, desmarque la casilla.

La lista **Mostrar los siguientes tipos** le permite especificar los tipos de archivo que serán (o no serán, dependiendo de las preferencias) mostrados como eventos de red.

- **Archivos de Texto** – Archivos de texto y html (páginas Web)
- **Imágenes** – imágenes
- **Archivos Conocidos** –archivos (.zip, .rar, .arj, etc.), documentos MS Office (.doc, .xls) y otros archivos bien conocidos no serían mostrados cuando esta casilla está marcada
- **Archivos de Audio** – archivos de audio
- **Archivos de Video** – archivos de video
- **Todos los demás** – cualquier otro tipo de archivo

Desmarcando las casillas correspondientes hará que NetResident oculte los archivos respectivos de la lista de eventos. Por ejemplo, si desmarca la casilla **Imágenes**, no podrá ver ninguna imagen en la lista. Desmarcando las casillas correspondientes hará que NetResident quite los respectivos tipos de archivo de la lista. Si desmarca todas las casillas, no vería ningún evento HTTP de red.

Tamaño mínimo de imagen, kb – Esta opción fija el tamaño mínimo que la imagen debe tener para ser mostrada. La mayoría de las imágenes en la Web (excepto las fotos) son bastante pequeñas. Si desea que NetResident muestre imágenes, pero no desea ver publicidad y elementos de página, fije el valor deseado en este campo.

Ignorar respuestas con errores – Cuando está activada, esta opción oculta errores de solicitud/respuesta (la mayoría de los usuarios debería activar esta opción para reducir la cantidad de registros basura)

Otra parte del filtro HTTP es filtrado por dirección de sitio. Le permite ocultar sitios específicos usando sus nombres como criterio de filtro.

Ocultar los siguientes sitios – activa/desactiva el filtrado de dirección de sitio.

Cuando está activado el filtro de dirección de filtro oculta todos los sitios que cumplen con el criterio de filtrado (especificado en el marco **Filtro de dirección de sitio**. Por favor use la siguiente sintaxis para especificar los criterios de filtro

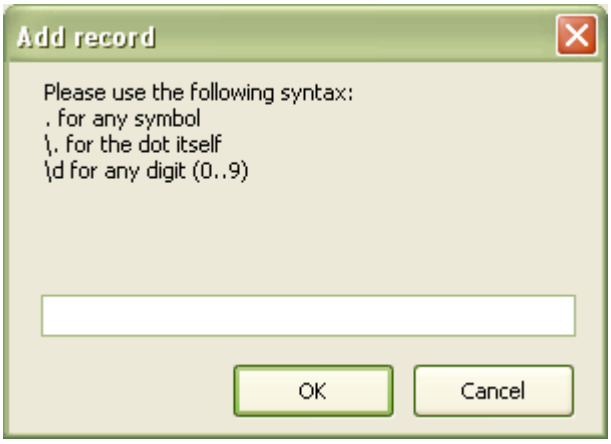
. – Cualquier símbolo
\. – El símbolo punto
\d – Un dígito (de 0 a 9)

Ejemplos de criterio:

Google\.com – oculta sitios que contengan "google.com" en el nombre de dominio
www\.google\.com – oculta "www.google.com"
\.org$– oculta todos los sitios del dominio .ORG
\d – oculta todos los sitios que tienen un dígito en su nombre de dominio.

Nota: Si solo especifica el dominio como criterio (.org, .com, etc.), debería colocarse el carácter **$** al final de la cadena de caracteres.

Para agregar un criterio de filtro, por favor pulse el botón **Agregar** en el lado derecho de la ventana.



Se abrirá la ventana **Agregar registro**. Por favor especifique un criterio deseado y pulse el botón **OK**. Esta ventana se cerrará y el registro respectivo se agregará a la lista de criterios de filtro.

Para quitar un registro, por favor selecciónelo en la lista y pulse el botón **Eliminar**. Para editar un registro, seleccione el registro deseado y pulse el botón **Editar**.

Herramienta PromiSwitch

Nota: Use esta herramienta a su propio riego. Nunca use esta herramienta salvo que sea el administrador de red de la LAN a la cual está conectado. El uso de esta herramienta podría entorpecer la conectividad de red. No hay disponible soporte técnico para esta herramienta.

La Herramienta PromiSwitch está diseñada para proveer visibilidad de red en redes basadas en switches donde no está disponible la opción de espejado de puerto en los switches que se están usando. Por favor refiérase a nuestro documento técnico, Monitoreo Promiscuo en Redes Ethernet y Wi-Fi para más información sobre este tema. Esta herramienta intentará asegurar visibilidad de red aprovechando las debilidades del protocolo ARP. Recomendamos fuertemente el uso de espejado de puerto en lugar de PromiSwitch siempre que sea posible.

Iniciar PromiSwitch y seleccionar el adaptador de red deseado que será usado para estación de monitoreo. Indicar el rango de IP deseado completando los campos **Explorar desde:** y **Explorar a:**, luego pulsar el botón **Iniciar Exploración.** Para abortar el proceso de exploración, pulsar el botón **Detener exploración**. Después que se completa la exploración, se mostrarán las terminales descubiertas (incluyendo sus direcciones IP y Físicas (MAC)) en la lista.

Marcar las casillas junto a las estaciones que desea monitorear y pulse el botón **Iniciar**. La herramienta PromiSwitch enviará periódicamente paquetes de red especiales a las estaciones seleccionadas. Esto redirigirá el tráfico entre el puerto de entrada y las estaciones seleccionadas, proveyendo visibilidad de red. También puede tener el tráfico interno entre dos estaciones redirigidas a su estación, lo cual puede lograrse seleccionando **Interno** en la lista desplegada de **Tráfico** y seleccionando dos estaciones.

La ventana **Opciones** le permite cambiar algunas opciones de programa, tales como limpiar la lista de estaciones en nueva exploración, envío automático de paquetes en el inicio, y el intervalo entre paquetes.

Referencia

Preguntas Frecuentes

En este capítulo puede encontrar respuestas a las preguntas más frecuentemente hechas. Las últimas preguntas frecuentes están disponibles siempre en http://www.tamos.com/products/netresident/faq.php.

P. Mi plugin HTTP no siempre muestra las páginas HTML correctamente. Por ejemplo, algunas imágenes no son mostradas ¿Por qué es así?

R. Una página HTML típica representa una colección de una docena de objetos independientes –códigos HTML, imágenes, estilos CSS, y demás. Un navegador solicita cada uno de estos objetos; sin embargo, la mayoría de estos objetos están en caché (guardados en el disco duro de la computadora para accesos futuros) y por lo tanto no requerido de la red cada vez que la página web es vista. NetResident no tiene acceso al cache del navegador; Por lo tanto no puede "ver" este objeto. No es un problema NetResident; siempre puede recargar la página Web en su navegador (necesita realizar una recarga completa, MSIE esto se logra pulsando en el botón actualizar mientras mantiene apretada la tecla Cambio (Shift). Esto permitirá a NetResident registrar y almacenar todos los elementos de la página Web.

P. ¿Cuál dirección IP o física (MAC)) debería usar para identificar una estación que deseo monitorear?

R**.** Si tiene activado DHCP en su computadora, cada computadora con una dirección física (MAC) exclusiva tiene asignada una dirección IP distinta para cada sesión. En este caso, debería identificar sus estaciones por las direcciones físicas (MAC). Esto hará que el programa asigne todos los eventos de red donde esté presente la dirección física (MAC) especificada a una estación en particular y evitar que la lista de estaciones se transforme en superpoblada. En algunos casos, podría encontrar una dirección física (MAC) distinta para cada host. Si tiene asignada una dirección IP estática a su adaptador de red y otras estaciones en su LAN, debería usar direcciones IP para identificar estaciones. Recomendamos usar alias para direcciones Físicas (MAC) e IP dado que hace el reconocimiento y el análisis de eventos de red mucho más fácil.

P. Cuando trato de importar archivos de registro de CommView o CommView para WiFi, no puedo mostrar los contenidos de algunos archivos. Creo que tengo todos los parámetros definidos correctamente en relación a vista y filtrado de eventos.

R. Es importante comprender que el procedimiento de importación tiene sus propios filtros y el mecanismo de muestra de contenido tiene sus propios filtros. Cuando está importando un archivo, el contenido fue posiblemente filtrado durante la fase de importación si aplicó filtros. Una vez que pasó la fase de importación, la aplicación usa los filtros de muestra para mostrar los contenidos. Hay una posibilidad que la aplicación esté configurada para mostrar solo los datos recolectados durante los dos últimos días, mientras que las sesiones contenidas en los registros estaban fuera del período de tiempo. Podría desear desactivar el filtro de muestra para hacer que la aplicación muestre los datos.

P. ¿Por qué el servicio NetResident insiste en iniciar si solo deseo revisar archivos LOG y no capturar datos actuales?

R. La base de datos es mantenida por el servicio. El GUI es simplemente una consola que "habla" con el servicio. Todo el procesamiento y filtrado de datos es realizado pro el servicio también, por lo que tiene que estar funcionando.

P. Tengo definido a NetResident para iniciar solo cuando la aplicación está funcionando, y no iniciar con Windows. Advertí que después de apagar NetResident, el proceso de servicio, "tfsnrs.exe" continua funcionando en el Administrador de Tareas. ¿Por qué continúa funcionando?

R. Correr el servicio y monitorear son cosas distintas. El servicio debe estar activo en todo momento para poder "hablar" con el GUI. Esto no significa que el servicio está capturando datos en todo momento. Captura datos solamente a pedido. En teoría, si la aplicación está configurada para capturar datos solo cuando está funcionando el GUI, Uno podría iniciar el servicio cuando el GUI inicia y se detiene cuando el GUI se detiene, pero iniciar el servicio es un poco lento y, lo más importante, no puede hacerse en forma remota, cuando el servicio y GUI están corriendo en máquinas distintas. Esto es algo que pensamos implementar en el futuro. El hecho que el servicio esté corriendo en segundo plano no debería preocupar porque cuando no está monitoreando la red no consume recursos de sistema en forma considerable.

P. ¿Podrían darme algunas mediciones de rendimiento cuando se está usando NetResident para monitorear una red fuertemente cargada?

R. El rendimiento del programa depende de la velocidad de la CPU y el tamaño de la RAM. Si usa las preferencias de monitoreo por defecto, por ejemplo cuando todos los plugins están habilitados y todos los puertos están siendo monitoreados, una PC Pentium4 de 3Ghz con 512 Mbytes de RAM puede monitorear un enlace de 100 Mbit utilizado totalmente. Para monitorear enlaces de red más rápidos, debería configurar filtrado por estación, limitar los puertos ha monitorear, y desactivar los plugins innecesarios. El rendimiento también depende del tipo de tráfico a monitorear, por lo que filtros adicionales deberían aplicarse solo si experimenta problemas de rendimiento.

P. Para algunas sesiones de chat de ICQ y AIM, uno de los números de Identificación de parte es mostrado como "no detectado". ¿Por qué no es detectado?

R. Esto sucede cuando una sesión de Chat ICQ o AIM (incluyendo la fase de autenticación) comienza antes que NetResident comience a capturar paquetes de red. Si la captura es iniciada en el medio de una sesión de Chat. La identificación a veces puede ser encontrada (dado que es encontrada en algunos paquetes de servicio, que son enviados intermitentemente), aunque esto no puede garantizarse.

P. ¿Puede su módulo VoIP usarse para registrar conversaciones Skype?

R. No, lo siento. Skype usa un cifrado robusto; es imposible descifrar conversaciones Skype.

P. ¿Porqué NetResident no muestra la cantidad de datos transferidos en términos de bytes?

R. NetResident no siempre almacena los datos transferidos en su forma original. En cambio, los procesa para una presentación más conveniente. No es extraño para sesiones únicas de red que sean divididas en varios eventos separados, o varias sesiones de red a combinarse dentro de un evento. Además, algunos datos transferidos simplemente no están soportados para ser procesados por los plugins actuales de NetResident. Dicho eso, NetResident no puede y no está pensado para mostrar confiables datos estadísticos de red. Si está interesado en estadísticas de tráfico de red, podría desear otro producto TamoSoft, CommTraffic.

P. Use WireShark y advertí que no puede capturar más paquetes después que se ha instalado.

A. Hay un conflicto conocido entre WinPcap, el controlador usado en WireShark y muchos productos similares, y el controlador usado en NetResident. Hay una circunvención simple: Inicie la captura de paquetes con WireShark **Antes** de comenzar a capturar paquetes con NetResident. En este caso, ambos productos podrán capturar datos simultáneamente. Si comienza a capturar primero con NetResident, WinPcap fallará al capturar cualquier paquete por una razón desconocida por nosotros.

Información

Como Comprar NetResident

Este programa es una versión de evaluación de 30 días. Si desea continuar usándolo después de 30 días, debe comprarlo. Hay disponible dos tipos de licencia para NetResident: Lite y Pro.

- Pro: Están disponibles todas las funciones.
- Lite: Están disponibles todas las funciones excepto el soporte de VoIP y la capacidad de importar archivos de registros de paquetes desde otras aplicaciones.

Como cliente registro tiene derecho a:

- Actualizaciones gratuitas que serán liberadas dentro del 1 año de la fecha de compra;
- Información sobre actualizaciones y nuevos productos;
- Soporte Técnico gratuito.

Aceptamos órdenes de tarjetas de crédito, órdenes por teléfono y fax, cheques, y cables de transferencia. Los precios, términos, y condiciones están sujetos a cambio sin notificación previa; por favor verifique nuestro sitio Web por nuestros más recientes ofrecimientos de productos y precios.

http://www.tamos.com/order/

Contáctenos

Web

http://www.tamos.com

Correo Electrónico

sales@tamos.com (Preguntas relativas a ventas)
support@tamos.com (Todas las demás preguntas)

Correo y Fax

Dirección de Correo:

PO Box 1385
Christchurch 8140
New Zealand

Fax: +64 3 359 0392 (New Zealand)
Fax: +1 917 591 6567 (USA)

Otros Productos por TamoSoft

CommView

CommView es un programa para el monitoreo de actividad de Internet y Redes de Área Local (LAN) capaz de capturar y analizar paquetes de red. Recoge información acerca de datos que pasan por su conexión discada o tarjeta de Ethernet y decodifica los datos analizados. Con CommView puede ver la lista de conexiones de red y estadísticas de IP vitales y examina paquetes individuales. Los paquetes son decodificados hasta la capa más baja con un análisis completo de la mayoría de los protocolos difundidos. Acceso completo a los datos crudos también es provisto en tiempo real. CommView es una útil herramienta para administradores de LAN, profesionales de seguridad, programadores de red, o cualquiera que desea tener un panorama complete del tráfico que pasa por la PC de uno o un segmento de LAN.

Más información

CommView para WiFi

CommView para WiFi es un poderoso analizador y monitor de red inalámbrica para redes 802.11 a/b/g. Provisto con muchas funciones fáciles de usar, CommView para WiFi combina rendimiento y flexibilidad con una facilidad de uso incomparable en la industria. CommView para WiFi captura cada paquete en el aire para mostrar información importante tales como la lista de puntos y estaciones de acceso. Estadísticas por nodo y por canal, Fortaleza de señal, una lista de paquetes y conexiones de red, gráficos de distribución de protocolos, etc. Proveyendo esta información, CommView para WiFi puede ayudarle a ver y examinar paquetes, determinar con precisión problemas de red, realizar investigaciones del sitio, y hacer determinación de problemas de software y hardware

Más información

CommTraffic

CommTraffic es un utilitario de red para recolectar, procesar, y mostrar estadísticas de tráfico y utilización de red para conexiones de red, incluyendo LAN y discadas. Este muestra estadísticas de tráfico y utilización de red para cada computadora en el segmento. El software provee una muy interfaz atractiva y personalizable, con un icono de menú de bandeja adicional que muestra estadísticas generales de red. Puede también generar informes que reflejan los volúmenes de tráfico y los costos de conexión a Internet (si hay alguno). CommTraffic soporta virtualmente cualquier plan de cuenta que su ISP pueda usar, tales como uno basado en tiempo de conexión, volumen de tráfico, hora del día, y otras mediciones. Puede fijar alarmas que le informarán cuando determinados criterios (por ejemplo cantidad de tráfico, gastos) son alcanzados. Un asistente de configuración lo guiará a través de la configuración y detectará automáticamente sus preferencias de red o conexión.

Más información

CountryWhois

CountryWhois es un utilitario para identificar la ubicación geográfica de una dirección IP. CountryWhois puede ser utilizado para analizar registros de servidor, verificar encabezados de direcciones de email, identificar fraudes en línea de tarjetas de crédito, o cualquier otra instancia donde necesita rápida y exactamente determinar el país de origen por la dirección IP. Lo que hace a CountryWhois distinto de herramientas similares es su muy alta exactitud (más del 98%), velocidad de procesamiento sin precedentes (un archivo de registros de 100 MB es procesado en menos de un segundo), actualizaciones regulares que mantienen las siempre cambiantes bases de datos de dirección IP actualizadas, y una variedad de formatos soportados de importación exportación, modo de línea de comandos, y una cómoda interfaz.

Más información

SmartWhois

SmartWhois es un utilitario útil para obtener información acerca de cualquier dirección IP, nombre de host, o dominio en el mundo. A diferencia de los utilitarios estándares Whois, este muestra información asociada con una dirección IP o domino no importando donde se encuentre registrada geográficamente. En cuestión de segundos, usted puede obtener todo lo que desea acerca de un usuario: domino, nombre de red, país, estado o provincia y ciudad. Incluso si la dirección IP no puede ser resuelta a nombre de host, ¡SmartWhois no fallara!

Más información

Essential NetTools

Essential NetTools es un conjunto de herramientas de red útiles para el diagnostico de redes y el monitoreo de las conexiones de redes de su computadora. Es un cortaplumas para cada persona interesada en un conjunto de herramientas de redes poderosas para el uso diario. El programa incluye la utilidad NetStat que muestra las conexiones de red de su computadora y abre los puertos y hace un mapeo con la aplicación dueña. Otra de sus funciones son un rápido explorador de NetBIOS , una herramienta de auditoria de Netbios para comprobar la seguridad de su LAN, y un "monitor" de las conexiones externas a sus recursos compartidos, como también un monitor de procesos que muestra la información acerca de todos los programas y servicios ejecutándose en su computadora. Otras herramientas útiles como Ping, TraceRoute, y NSLookup. Las funciones adicionales incluyen la generación de reportes en formatos HTML, textos, y delimitados por comas y una interfaz configurable. Este programa es fácil de utilizar y un poderoso reemplazo para utilitarios de Windows como nbstat, nettat, y Netwatcher. El mismo incorpora muchas funciones avanzadas que las herramientas de Windows no ofrecen.

Más información

DigiSecret

DigiSecret es una herramienta fácil de utilizar, segura, y una poderosa aplicación para encriptar y compartir archivos. Esta utiliza algoritmos fuertes y probados a través del tiempo para la creación de archivos encriptados, Archivos EXE autoexpandibles, y compartir archivos con asociados y amigos. DigiSecret también incluye una compresión poderosa e inteligente de archivos; no necesitara más archivos .zip dado que puede tener archivos Digisecret encriptados y comprimidos. Este programa está integrado con la interfaz de Windows, y usted puede realizar operaciones sobre sus archivos solo haciendo clic con el botón derecho sobre ellos. También incluye soporte de operaciones de arrastrar y soltar.

Más información