CommView®

Monitor y Analizador de Redes para MS Windows

Manual del Usuario

Derechos Reservados © 1999-2006 TamoSoft

Introducción

Acerca de CommView

CommView es un programa que permite monitorear la actividad de Internet y redes de área local (Local Area Network (LAN)) siendo capaz de capturar y analizar paquetes de red. El mismo recoge información acerca del tráfico de datos a través de su conexión telefónica o su tarjeta Ethernet y decodifica los datos analizados.

Con CommView usted puede ver la lista de conexiones de red y estadísticas vitales de IP y examinar paquetes individuales. Los paquetes son decodificados hasta el nivel mas bajo con un análisis profundo de los protocolos más difundidos. También provee un completo acceso a datos sin depurar. Los paquetes capturados pueden ser guardados en archivos de registro para análisis futuros. Un sistema flexible de filtros hace posible eliminar paquetes que no necesita, o capturar solo aquellos paquetes que desea. Alarmas configurables pueden notificar eventos importantes, tales como paquetes sospechosos, utilización excesiva del ancho de banda, o direcciones desconocidas.

CommView es una herramienta valiosa para administradores de LAN, profesionales de seguridad, programadores de redes, o cualquiera que quiera tener una visión completa del tráfico que pasa a través de una PC o segmento de LAN. Esta aplicación esta diseñada para usuarios de Internet y redes de tamaño pequeño o mediano y puede ejecutarse en cualquier sistema Windows 98/Me/NT/2000/XP/2003 o la edición Windows XP 64-bit sobre procesadores AMD. Este requiere una tarjeta de red Ethernet, Wireless Ethernet o Token Ring que soporte el estándar de controlador de dispositivo NDIS 3.0, o un adaptador telefónico estándar.

Los siguientes protocolos son decodificados completamente por las funciones de CommView: ARP, BCAST, BGP, BMP, CDP, DAYTIME, DDNS, DHCP, DIAG, DNS, EIGRP, FTP, G.723, GRE, H.225, H261, H.263, H.323, HTTP, HTTPS, ICMP, ICQ, IGMP, IGRP, IMAP, IPsec, IPv4, IPv6, IPX, HSRP, LDAP, MS SQL, NCP, NDS, NetBIOS, NFS, NLSP, NNTP, NTP, OSPF, POP3, PPP, PPPoE, RARP, RADIUS, RDP, RIP, RIPX, RMCP, RPC, RSVP, RTP, RTCP, RTSP, SAP, SER, SIP, SMB, SMTP, SNA, SNMP, SNTP, SOCKS, SPX, SSH, TCP, TELNET, TFTP, TIME, TLS, UDP, VTP, WAP, WDOG, YMSG, 802.1Q, 802.1X.

Adicionalmente, nuestra nueva tecnología de monitoreo remoto permite a los usuarios de CommView capturar tráfico de red sobre cualquier computadora donde el Remote Agent se esté ejecutando, sin importar la ubicación física de la computadora. Para acceder a las ventajas de esta función única, es necesaria la utilización de CommView Remote Agent, un producto adicional a CommView a un precio accesible.

Novedades

Versión 5.3

- Asignación IP-país para direcciones IP provee geolocalización en tiempo real para todas las direcciones IP mostradas por la aplicación.
- Columnas rediseñadas en la pestaña “Paquetes” y el “Visor de registro” para hacerlos más cómodos para usar. El orden de columna en todas las pestañas de la ventana principal de la aplicación ahora es personalizable.
- Capacidad para crear cualquier número de instantáneas del buffer actual de paquetes, lo que hace mucho más fácil trabajar con paquetes bajo una carga pesada de red. Ahora puede examinar el buffer en ventanas separadas, sin el riesgo de perder paquetes viejos y la necesidad de buscar paquetes que fueron quitados de la vista.
- Alarmas mejoradas que le permiten enviar e-mails de alerta personalizables.
- Ventana de “Estadísticas” modificable en tamaño.
- Cuadro de Diálogo de “Búsqueda” mejorado.
- Líneas de grillas opcionales para una mejor visibilidad de paquetes.

Otras mejoras menores.

Versión 5.1

- Filtros rápidos que le permiten crear fácilmente nuevas vistas de paquetes para paquetes similares basado en direcciones físicas (MAC), direcciones IP, o puertos.
- Ahora está disponible el filtrado por nombre de proceso.
- Lista de Proveedores de MAC actualizada.
- Aplicación Automática de actualizaciones.
- Muchas otras mejoras y corrección de errores

Versión 5.0

- Los paquetes son asignados a la aplicación que los envía o recibe (esta característica está disponible bajo Windows 2000/XP/2003).
- Estampado de tiempo de alta precisión (hasta microsegundos, disponible bajo Windows NT/2000/XP/2003).
- Nuevo ormato de registro abierto y compacto.
- Matrices gráficas que representan conversaciones entre hosts.
- Han sido agregados nuevos módulos de decodificación: MS SQL, LDAP, y YMSG. la decodificación de SMB e ICQ han sido mejoradas.
- Ahora está soportada la Edición Windows XP 64-bit sobre procesadores AMD Opteron y Athlon64.
- Ahora están soportadas múltiples conexiones de Remote Agent simultáneas.
- Generador de paquetes mejorado conteniendo un cómodo acceso a las plantillas.
- Los informes HTML pueden incluir gráficos.
- Nuevos tipos de alarmas.
- Menor uso de CPU.

Versión 4.1

- Ahora puede capturar paquetes loopback enviados desde/hacia direcciones IP locales, por ejemplo 127.0.0.1 (esta funcionalidad está disponible bajo Windows NT/2000/XP/2003).
- El programa puede registrar URLs. visitadas.
- Nuevos módulos de decodificación han sido agregados: IMAP, NNTP, SSH, TLS.
- Una interfaz de plug-in le permite implementar su propio protocolo de decodificación.
- La ventana de Reconstruir Sesión TCP ahora puede descomprimir contenidos web GZIP, así como mostrar imágenes que se envían sobre las sesiones HTTP.
- La ventana de Reconstruir Sesión TCP ahora le permite ir a la próxima sesión TCP entre dos Hosts cualquiera (en la versión anterior, podía saltar a la próxima sesión solo entre aquellos dos Host que fueron seleccionados inicialmente).
- El programa lo notificará acerca de cambios en la lista de adaptadores de red.
- La captura es reiniciada automáticamente después de la hibernación o suspensión de Windows.
- Están soportados los adaptadores Token Ring (esta funcionalidad está disponible sobre Windows 2000/XP/2003).
- Están soportados frames Jumbo.
- Puede tener el programa generando estadísticas sobre datos precapturados adicionalmente a estadísticas en tiempo real.
- La funcionalidades de alarma mejoradas le permite pasar variables a aplicaciones arrancadas o mensajes de alarma.
- Otras mejoras menores.

Versión 4.0

- Alarmas: Puede configurar el programa para notificar acerca de ciertas ocurrencias de paquetes, direcciones físicas (MAC) desconocidas, etc.
- Han sido agregados nuevos módulos de decodificación de protocolos: DAYTIME, DDNS, H.323 (H.225, Q.850, Q.931, Q932), HTTPS, NTP, RMCP, RTP/RTCP (G.723, H.261, H.263), SNTP, TIME.
- Interfaz en Múltiples Idiomas.
- Un módulo de decodificación personalizado puede ser utilizado con el programa.

- Nuevos parámetros de línea de comandos que le permite cargar conjunto de reglas automáticamente y/o abrir adaptadores.
- La ventana de Reconstrucción de sesión TCP ahora tiene la función “Buscar”.
- Las plantillas de paquetes TCP, UDP, e ICMP en el Generador de Paquetes.
- Una nueva función “Decodificar Como” que puede ser utilizada para decodificar protocolos soportados utilizando puertos no estándar.
- Nuevas opciones configurables.

Versión 3.4

- Han sido agregados nuevos módulos de decodificación de protocolos: BGP, CDP, EIGRP, IGRP, IPsec, HSRP, NFS, OSPF, RADIUS, RIP, RPC, SNA, VTP, WAP, 802.1Q, 802.1X.
- Ha sido agregada una nueva herramienta de manejo de registros que permite separar/concatenar archivos CCF.
- La ventana de Reconstrucción de Sesión TCP ahora permite saltar a la siguiente sesión entre dos hosts.
- Nuevas funciones en la ventana de Estadísticas: cambiar entre bits y bytes por Segundo, un indicador de utilización de ancho de banda, gráficos de protocolos IP y sub-protocolos por número de bytes o por número de paquetes.
- Opción de modo no promiscuo.
- Importación de archivos capturados en MS NetMon y NAI Sniffer para Windows.
- Sintaxis resaltada en la ventana de formulas avanzadas.
- Mejoras en el soporte de temas de Windows XP.
- Solución a un importante problema en la función de reglas avanzadas hex; esta función no trabajaba correctamente para los patrones de bytes que incluían 0x00.

Versión 3.3

- Reglas avanzadas que permiten crear filtros complejos Utilizando lógica booleana y sintaxis simple y fácil de entender.
- Han sido agregados nuevos módulos de decodificación de protocolos: FTP, TFTP, SOCKS (v. 4,5), TELNET.
- Nueva mejora de rendimiento
- Nuevos dispositivos en Generador de Paquetes: soporte de "arrastrar-y-soltar" para muchos formatos de paquetes, generación de paquetes a alta velocidad (hasta 5,000 paquetes/seg), y la habilidad de enviar muchos paquetes distintos con un simple "clic".
- Archivos de registros pueden ser concatenados opcionalmente dentro de un único archivo cuando el programa detiene la captura.
- Nuevos formatos de exportación: archivos delimitados por coma, con y sin datos Hexadecimales.
- Puede guardar directamente diferentes formatos (CCF, ENC, etc.), sin primero cargar los archivos de registro en el Visor de Registro.
- Ahora las Tablas de LAN de Hosts pueden manejar hasta 1,000 direcciones físicas (MAC) & IP.
- Está disponible opcionalmente la Columna "Tamaño" en la lista de paquetes.
- Puede definir direcciones de red y máscaras de subnet para las direcciones IP que UD. Quiere que el programa trate como locales.
- Muchas mejoras menores y corrección de errores.

Versión 3.2

- Han sido agregados nuevos módulos de decodificación de protocolos: SNMP (v. 1,2,3), IPv6, ICQ, GRE, RDP.
- Importante mejora de rendimiento cuando abre/importa archivos de captura: Los archivos son cargados hasta 25 veces más rápido.
- Menor uso de CPU.
- Están disponibles Estadísticas NIC ampliadas, tales como colisión y errores de CRC.
- Puede aplicar reglas a datos pre-capturados en Visor de Registros.
- Cuadro de diálogo de "Buscar Paquete" mejorada.

Versión 3.1

- Han sido agregados nuevos módulos de decodificación de protocolos: DHCP, DNS, HTTP, POP3, RTSP, SMTP.
- Una nueva, exclusiva, tecnología de monitoreo remoto.
- Puede agregar hasta 4 protocolos personalizados al diagrama de sub-protocolos de IP.
- Puede importar archivos capturados en formato Tcpdump (libcap).
- Han sido agregadas más opciones de configuración.
- Muchas mejoras menores y corrección de errores.

Versión 3.0

- Un nuevo decodificador de protocolos; ahora soporta: ARP, BCAST, BMP, DIAG, ICMP, IGMP, IPv4, IPX, NCP, NDS, NetBIOS, NLSP, PPP, PPPoE, RARP, RIPX, RSVP, SAP, SER, SMB, SPX, TCP, UDP, WDOG. más protocolos próximamente.
- Soporte de adaptadores Ethernet (802.11b).
- El programa está listo para Windows XP (probado con RC1).
- El Generador de Paquetes puede ahora mandar paquetes utilizando el adaptador de discado telefónico de Windows 2000/XP.
- Un decodificador de protocolo y un corrector de checksum fue agregado al Generador de Paquetes.
- Puede, opcionalmente, ejecutarse en múltiples instancias de CommView para monitorear varios adaptadores simultáneamente.
- Pueden ser incluidas Estadísticas de IP en los Reportes Estadísticos.
- Una nueva tabla de LAN Hosts por IP ha sido agregada a la ventana de estadísticas.
- La ventana de reconstrucción de TCP le permite excluir/incluir datos basados en la dirección del paquete.
- Ahora puede filtrar paquetes basado en indicadores TCP.
- El programa puede ejecutarse en modo invisible.
- Ahora puede compartir datos de CommView con su propia aplicación utilizando una simple interfase TCP/IP.
- La pestaña de paquetes le permite seleccionar paquetes múltiples.

Versión 2.6

- Pueden ser asignados Alias a direcciones IP.
- Las reglas actuales pueden ser aplicadas a las ventanas de estadísticas y reportes.
- Decodificador PPPoE.
- La ventana de Reconstruir Sesión TCP, ahora sin modalidad, permite tener varias ventanas abiertas con diferentes sesiones.
- Mejoras menores y corrección de errores.

Versión 2.5

- Soporte completo de “arrastrar y soltar”: ahora puede arrastrar estadísticas de IP, paquetes individuales, y gráficos y soltarlos en el escritorio o en cualquier carpeta. Puede arrastrar archivos capturados (CCF, ENC, o BFR) y soltarlos en la aplicación.
- El diagrama de Distribución de tamaño de paquete y la Tabla de Hosts de LAN han sido agregados a la ventana de Estadísticas.
- Generación de informes automáticos o manuales: todos los datos estadísticos pueden ser guardados como HTML o reportes delimitados por punto y coma, (ver la pestaña “reporte” en la ventana de Estadísticas).
- La ventana de Reconstruir Sesión TCP ahora permite ver datos como HTML y EBCDIC adicionalmente a ASCII y HEX.

Versión 2.4

- Reconstrucción de sesiones TCP.
- Pueden ser asignados Alias a direcciones físicas (MAC).
- identificador NIC del fabricante.
- Más columnas están disponibles en las pestañas "Estadísticas IP" y "Paquetes".
- Las columnas en las pestañas "Paquetes" e "Estadísticas IP" pueden ser ocultadas.
- Los paquetes ARP/RARP son decodificados.
- Comodines pueden ser utilizados en reglas de direcciones IP.
- La opción ambas en reglas de captura está disponible adicionalmente a las de desde y hacia.
- Pestañas con reglas activas se muestran en negrita.
- El envío de Paquetes puede ser suspendido/reanudado.
- Están disponibles distintas alternativas de presentación de estadísticas IP.
- Otras mejoras menores.

Versión 2.3

- Soporte de discado telefónico bajo Windows 2000.

Versión 2.2

- Encabezados coloreados de direcciones físicas, direcciones IP, y TCP/UDP/ICMP.
- El contenido de la pestaña de estadísticas IP puede ser guardado en formato HTML.
- La nueva función Generador de Paquetes permite enviar paquetes.
- Las reglas de configuración pueden ser guardadas/cargadas.
- Ahora las Reglas de texto permiten Mayúsculas o minúsculas.
- Cuadro de diálogo Buscar Contenidos de Paquetes mejorado.
- Falla arreglada: Problema cuando arranca el controlador localizado en un sistema Windows 2000 ha sido resuelto.

Versión 2.1

- Visor de Registro: Ahora puede cargar y explorar archivos de captura tal como lo hace con datos capturados en tiempo real.
- Puede importar y exportar archivos de captura desde/hacia los formatos NI Observer o NAI Sniffer.
- Los números de Puerto pueden ser mostrados como nombres de servicio.
- Una nueva función “Ir a” permite buscar rápidamente los paquetes provenientes/dirigidos a una cierta dirección IP.
- Unas pocas mejoras en la interfaz.
- Falla arreglada: La versión previa mostraba un chequeo incorrecto de UDP.

Version 2.01

- Soporte Windows 2000

Versión 2.0 Final

- Mejora en el desempeño bajo Windows NT.
- Los errores encontrados en la versión Beta 2.0 fueron arregladas.

Version 2.0 Beta

- Soporte Windows NT
- Mayor información estadística.

Versión 1.0 Final

- Nuevas funciones: Buscar Paquete e Ir a Paquete Número.
- Nuevos Filtros: Capturar/Ignorar paquetes basados en las direcciones físicas y dirección de paquetes.
- Estadísticas: Histogramas de Paquetes por Segundo y Bytes por Segundo, Gráficos de distribución de protocolos y subprotocolos de IP.
- Falla Arreglada: El filtro de texto en v.1.0 Beta podría algunas veces capturar paquetes que no contenían el texto especificado; este problema ya ha sido resuelto.

Acuerdo de Licencia

Por favor lea los siguientes términos y condiciones cuidadosamente antes de utilizar este software. La utilización de este software indica que usted ha aceptado el acuerdo de licencia. Si no está de acuerdo con los términos de está licencia, debe eliminar este software de sus dispositivos de almacenamiento y cesar la utilización de este producto.

Derechos de autor
Los derechos registrados del software 1999-2006 por TamoSoft. CommView es una marca registrada de TamoSoft. La utilización y los derechos de autor de este software se encuentran gobernados por los tratados internacionales de derechos de autor. TamoSoft. Retiene el pleno titulo y derechos de este programa y la documentación, y de ninguna manera la licencia otorgada disminuye los derechos de propiedad intelectual de TamoSoft. No debe redistribuir códigos de registro provistos – en papel, de forma electrónica o de cualquier otra forma.

Versión de Evaluación
Este no es un software gratuito. Usted está obligado a utilizar este software para el propósito de su evaluación sin cargo por un periodo de 30 días. La utilización de este software después del periodo de evaluación viola las leyes de propiedad intelectual y puede derivar en severas penas civiles y criminales.

Versión Registrada (Licenciada)
Una copia registrada de este software puede ser utilizada por una sola persona que utiliza este software de forma personal y en una o más computadoras, o puede ser instalado en una sola computadora y utilizado de forma no simultánea por más de una persona, pero nunca en ambos supuestos simultáneamente. La Home License para este software limita su uso y funciones. La lista de limitaciones está sujeta a cambios sin previo aviso. La lista actual de limitaciones está disponible en el sitio web de TamoSoft. Este software puede ser instalado en un servidor de red, proveyendo una licencia apropiada otorgada por Tamosoft. para cada computadora que tenga acceso a este software.

Responsabilidad
TAMOSOFT NO GARANTIZA QUE EL PRODUCTO ESTÉ LIBRE DE ERRORES. ESTE PROGRAMA SE ENTREGA "TAL CUAL" SIN GARANTÍA DE NINGÚN TIPO, NI EXPRESA, NI IMPLÍCITA, INCLUSO LAS GARANTÍAS EXCEPTUALES DERIVADAS DEL COMERCIO O DESARROLLO PARA FINES ESPECÍFICOS. EN NINGÚN CASO TAMOSOFT. SERÁ CULPABLE DE LOS DAÑOS, DE CUALQUIER CARACTERÍSTICA, DERIVADOS DE LA UTILIZACIÓN DE ESTE PROGRAMA, INCLUSO HABIENDO SIENDO ADVERTIDO DE LA POSIBILIDAD DE TALES DAÑOS. USTED RECONOCE QUE HA LEÍDO ESTA LICENCIA, LA HA COMPRENDIDO Y ACUERDA ACEPTAR SUS ESTIPULACIONES.

Leyes que gobiernan este acuerdo
Este acuerdo está gobernado bajo las leyes de Nueva Zelanda.

Distribución
Este software puede ser distribuido libremente en su forma original sin modificaciones ni registros. La distribución tiene que incluir todos los archivos de la distribución original. Los distribuidores no pueden percibir dinero por ella. Cualquiera que distribuya este software por cualquier tipo de remuneración debe primero contactarnos para recibir la correspondiente autorización.

Otras Restricciones
Usted no puede modificar, aplicar ingeniería reversa, de-compilar, o de-codificar este software bajo ningún concepto, incluyendo cambiar o eliminar cualquier mensaje o ventana del mismo.

Windows es una marca registrada de Microsoft Corporation. Todas las demás marcas registradas son propiedad, de sus respectivos dueños

Utilización del Programa

Perspectiva General

La interfaz del programa consiste de cinco pestañas que le permiten ver los datos y realizar diversas acciones sobre los paquetes capturados. Para comenzar la captura de paquetes, seleccione un adaptador de red desde la lista del menú en la barra de herramientas, haga clic en el botón **Iniciar Captura** o seleccione **Archivo => Iniciar Captura** en el menú. Si el tráfico de red pasa a través del adaptador seleccionado, CommView comenzara a mostrar la información.

Menú Principal

Archivo

Iniciar/Detener Captura – inicia/detiene la captura de paquetes.
Suspender/Reanudar Salida de Paquetes – suspende/reanuda la salida de paquetes en la 2da pestaña.
Modo de Monitoreo Remoto – Muestra/Oculta la barra de herramientas de Monitoreo remoto.
Guardar las Últimas Conexiones IP Como – le permite guardar el contenido de la pestaña Últimas Conexiones IP como un reporte HTML o un reporte delimitado por comas (CSV).
Guardar Registro de Paquetes como – Le permite guardar el contenido de la pestaña de Paquetes en formatos diferentes. Utilice la pestaña de registros para las opciones avanzadas de guardar.
Visor de Registros – Abre una nueva ventana de Visor de registro.
Borrar Estadísticas IP – Borra la tabla de estadísticas de IP 1er pestaña
Borrar Buffer de Paquetes – Borra el contenido del buffer del programa y la lista de paquetes en la 2da pestaña
Datos de Rendimiento –Muestra las estadísticas de rendimiento del programa: El número de paquetes capturados y perdidos por el controlador de dispositivo. Este comando no está disponible bajo Windows 95/98/Me.
Salir – Cierra el programa.

Buscar

Buscar Paquete – Muestra un cuadro de diálogo que le permite Buscar paquetes. que coincidan con un texto especificado
Ir a Paquete Número – Muestra un cuadro de diálogo que le permite saltar a un paquete con un número especificado.

Ver

Estadísticas – Muestra una ventana con estadísticas de transferencias de datos y distribución de protocolos.
Información de Referencia de Puertos – muestra una ventana con Información de referencia sobre el puerto.
Directorio de Registros – abre un directorio donde son guardados por omisión los registros.
Columnas de Últimas Conexiones IP – Muestra/oculta las pestañas de columnas de Últimas Conexiones IP.
Columnas de Paquetes – Muestra/oculta las pestañas de columnas de paquetes.

Herramientas

Generador de Paquetes – abre la ventana del Generador de Paquetes. (No disponible bajo Windows 95/98/Me)
Reconstruir Sesión TCP – Le permite reconstruir una sesión de TCP. Comenzando desde el paquete seleccionado; abre una ventana que muestra la conversación completa entre dos hosts.
Identificar el Fabricante de la Tarjeta – Abre una ventana donde puede identificar el fabricante de un adaptador de red. por la dirección física (MAC) especificada.
Planificador – le permite agregar o remover tareas de captura programada.

Preferencias

Fuentes – Muestra el submenú para fijar los caracteres fuente de los elementos de la interfaz.
Alias de Direcciones Físicas (MAC) – Crea una ventana donde se puede asignar un alias. Fácil de recordar, a las direcciones físicas (MAC).
Alias de IP – Crea una ventana donde se puede asignar un alias. Fácil de recordar, a las direcciones IP.
Opciones – crea una ventana de opciones donde se pueden definir opciones avanzadas del programa.
Idioma – Le permite cambiar el idioma de la interfaz. Asegúrese de reiniciar el programa una vez que haya cambiado el idioma. El paquete de instalación de CommView puede no incluir todos los archivos de idioma disponibles para la interfaz. Haciendo clic en el ítem del menú **Otros Idiomas** abre la página para descargar idiomas adicionales desde nuestro sitio Web donde puede descargar su archivo de idioma si está disponible para la versión actual.
Instalar Controlador de Discado – instala un controlador para capturar paquetes sobre adaptadores de discado telefónico. Este ítem está disponible bajo Windows 2000/XP/2003 solamente; Windows 98/ME no requieren este controlador. Este ítem está invisible si el controlador ha sido instalado.
Instalar Controlador Token Ring – instala un controlador para capturar paquetes sobre adaptadores Token Ring. Este ítem está disponible bajo Windows 2000/XP/2003 solamente. Bajo Windows 98/ME, CommView no soporta adaptadores Token Ring. Este ítem está invisible si el controlador ha sido instalado.

Reglas

Guardar Reglas Actuales Como – Le permite guardar las reglas actuales de configuración en un archivo.
Cargar Reglas Desde – Le permite cargar las reglas de configuración guardadas desde un archivo.
Borrar Todo – Borra todas las reglas existentes (si hay alguna).

Ayuda

Contenido – inicia la ayuda de CommView.
Buscar ayuda sobre – Muestra el índice de ayuda de CommView.
Guía en Línea – Inicia una ventana de navegador y abre la Guía en Línea de CommView.
Verificación de una Actualización en la Web ... – abre el asistente de actualización. Por favor siga las instrucciones sobre la pantalla para descargar e instalar la última actualización para CommView para WiFi del sitio Web de TamoSoft.
Acerca de – Muestra información acerca del programa.

Casi todos los elementos de la interfaz tienen un menú sensible al contexto que puede ser invocado haciendo clic en el botón derecho del mouse, y muchos comandos están disponibles solamente a través de estos menús.

La primera pestaña es utilizada para mostrar información detallada acerca de las conexiones de red de su computadora (solo protocolos IP). Para mayor información vea Últimas Conexiones IP.

La segunda pestaña es utilizada para ver los paquetes de red capturados y mostrar la información detallada acerca de un paquete seleccionado. Para mayor información vea Paquetes.

La tercera pestaña le permite guardar los paquetes capturados en archivos. Para mayor información vea Registro.
La cuarta pestaña es para configurar reglas que le permiten capturar/ignorar paquetes basándose en diferentes criterios, tales como la dirección IP o el número de Puerto, para mayor información vea Reglas.

La quinta pestaña le permite crear alarmas que le pueden notificar acerca de eventos importantes, tales como paquetes sospechosos, utilización elevada del ancho de banda, etc. Para mayor información vea Alarmas.

Usted puede cambiar algunas de las preferencias, como fuentes, colores, y tamaño de buffer seleccionando **Preferencias** desde el menú. Para más información vea Preferencias Opciones.

Seleccionar Interfaz de Red para Monitoreo

El monitoreo de su conexión de red comienza seleccionando la interfaz de red que desea monitorear. La selección de la interfaz correcta de red es fundamental para lograr los resultados de monitoreo deseados. Tratamos de hacer CommView tan simple y fácil de usar como sea posible, todo lo que necesita hacer para iniciar el monitoreo de su red es seleccionar un adaptador en el menú contextual en la barra de herramientas y hacer clic en el botón **Iniciar Captura**.

A medida que la tecnología de red se desarrolla más y más, distintos tipos de adaptadores están disponibles en el mercado. Adaptadores WiFi, xDSL, usted los menciona. CommView soporta muchos de ellos; Sin embargo, cada tipo de conexión de red tiene sus propias particularidades que necesita conocer para obtener los resultados de monitoreo adecuados.

Permítanos revisar los tipos más comunes de adaptadores de red y ver cómo funciona CommView con ellos y cómo debería ser configurado.

Durante la Instalación, CommView detecta los adaptadores de red disponibles en su sistema. En algún punto, el script de instalación le solicitará instalar el controlador de su adaptador de discado. Necesita hacer clic sobre **Si** si planea monitorear su red discada o su conexión xDSL, o usar PPPoE/VPN sobre otros tipos de conexiones de red. Si dice **No** en este punto, siempre podrá instalar el adaptador de discado más tarde haciendo clic sobre **Preferencias** => **Instalar el Controlador de Discado**. Durante la instalación del controlador de discado sus enlaces de red serán desconectados por un momento.

Una vez que es completada la instalación, inicie CommView y haga clic sobre el menú contextual en la barra de herramientas, verá el adaptador Loopback (no disponible en Windows 98/ME), su adaptador de Red Local (si tiene uno), y el adaptador de discado (si ha hecho clic sobre **Si** cuando se le solicitó instalar el controlador de discado).

Permítanos ver cómo estos registros corresponden al hardware actual en su computadora y los tipos de conexión de red.

Si está conectado e la red vía un **Adaptador Ethernet** común, sólo selecciónelo de el menú contextual e inicie el monitoreo. CommView soporta virtualmente cualquier adaptador Ethernet de 10, 100, o 1000 Mbit disponible en el mercado.

Si su discado para conectarse a la red es vía módem, seleccione su **Adaptador de Discado** para monitorear. Por favor advierta que sólo ve los paquetes salientes y entrantes (y no los paquetes que pasan) en CommView. Esta no es una limitación de CommView. Dada la naturaleza de una conexión punto a punto; sólo dos hosts, el local y el remoto participan en la conexión. Si usa ICS, podrá capturar todos los paquetes desde y hacia el cliente ICS.

Cuando usa CommView para monitorear redes inalámbricas 802.11 a, b, o g, seleccione su **Adaptador Wi-Fi** para monitorear. Los controladores de propósitos generales no pueden poner a los adaptadores Wi-Fi en modo promiscuo; CommView mostrará los paquetes entrantes y salientes, así como los paquetes multicast y broadcast. Los encabezados de paquetes 802.11 no serán mostrados, si está buscando una solución de monitoreo de modo promiscuo para redes 802.11 a/b/g, tenga en cuenta CommView para WiFi que realmente coloca su adaptador inalámbrico en modo de monitoreo y le permite capturar tráfico desde otras estaciones inalámbricas y Puntos de Acceso. CommView para WiFi puede ser descargado del sitio Web de TamoSoft.

Si su conexión de red es vía un módem **xDSL** con **Interfaz USB**, puede monitorearlo con CommView. Oficialmente, no soportamos interfaces USB en CommView, por lo que lo mejor es intentarlo. En muchos casos la conexión de red real será establecida sobre un enlace PPPoE, en estos casos necesitará seleccionar el adaptador de discado para monitorear y podrá capturar el tráfico de red.

Si su **módem xDSL** tiene **Interfaz de Ethernet**, pero la conexión real se realiza sobre un enlace PPPoE, seleccione el adaptador de discado para monitorear el tráfico de red desde/hacia su computadora, y los paquetes broadcast y multicast. Si selecciona su adaptador Ethernet para monitorear, podrá capturar todos los paquetes sobre su segmento de LAN, sin embargo estarán encapsulados en PPPoE y pueden estar encriptados.

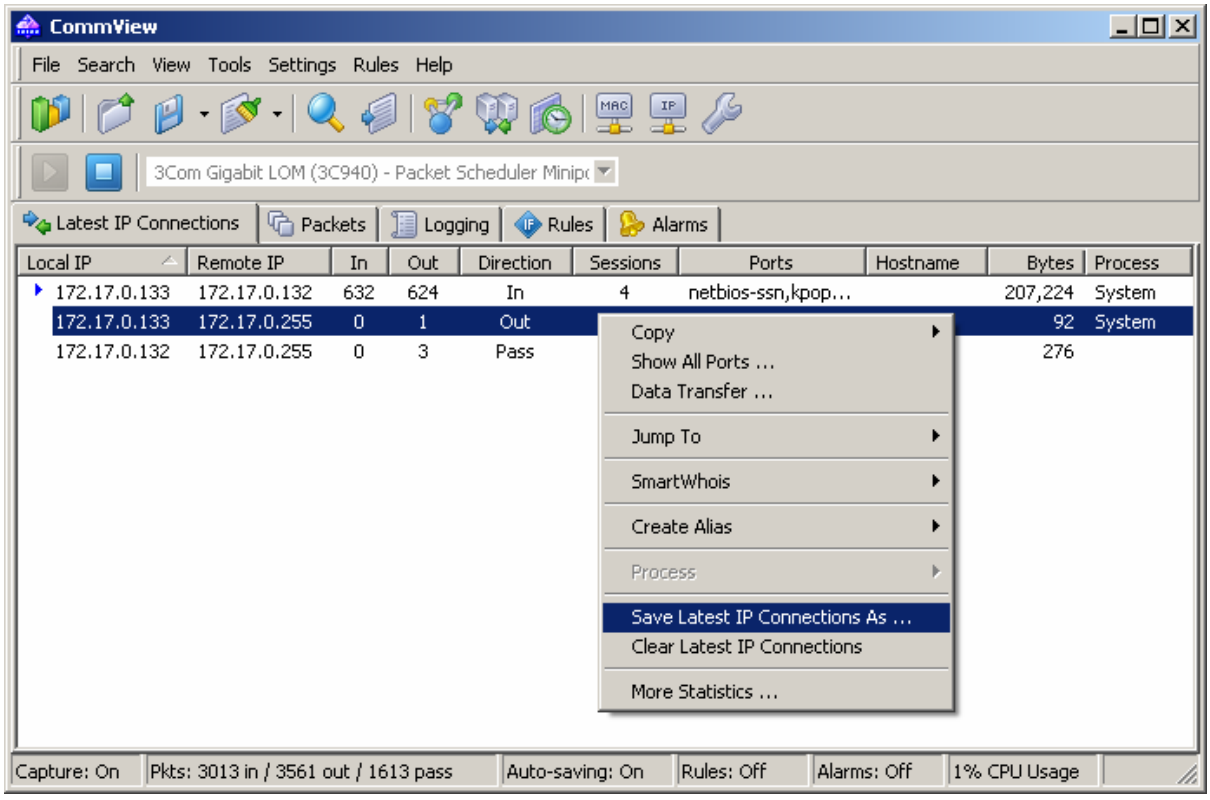
Si está conectado a la red vía un enlace **VPN seguro**, el monitoreo de su adaptador de red Ethernet sólo le permitirá capturar paquetes encriptados, en este caso necesita monitorear el adaptador de discado para capturar los datos que están siendo transmitidos realmente.

Si tiene dos o más adaptadores de red en su computadora que están "**Bridged" (Puenteados)**, el monitoreo del "bridge" (Puente) mostrará el tráfico entrante y saliente para cada adaptador en el Bridge, los paquetes broadcast y multicast, y los paquetes que están re-dirigidos a otro adaptador de red bridged.

El monitoreo de **Adaptador Loopback** mostrará el tráfico enviado o recibido sobre TCP/IP por programas que están corriendo en su computadora. Si no tiene programas corriendo que intercambien datos localmente, no verá ningún tráfico cuando monitorea el adaptador Loopback. Por favor advierta que la función Generador de Paquete no funcionará con el adaptador Loopback. Para mayor información vea el capítulo Capturando tráfico de Loopback .

Últimas Conexiones IP

Esta pestaña es utilizada para mostrar información detallada acerca de las conexiones de red (solo protocolos IP) de su computadora. Para comenzar la captura de paquetes, seleccione **Archivo => Iniciar Captura** en el menú, o haga clic en el botón correspondiente de la barra de herramientas.



El significado de las columnas de la tabla está explicado a continuación:

IP Local – Muestra la dirección IP local. Para los paquetes que llegan, esta es la dirección IP de destino; Para los paquetes que salen o pasantes, esta es la dirección IP de origen.
IP Remota – muestra la dirección IP remota, para los paquetes que arriban, esta es la dirección IP de origen; Para los paquetes que salen o pasantes, esta es la dirección IP de destino.

El programa automáticamente determina la ubicación de cualquier dirección IP, y dependiendo de sus preferencias de geolocalización, podría mostrar el nombre o bandera del país junto a la dirección IP. Para mayor información vea Determinar Opciones.

Entrada – Muestra el número de paquetes recibidos.
Salida – Muestra el número de paquetes enviados.
Dirección– Muestra la dirección de la sesión. La dirección está determinada por la dirección del primer paquete recibido-de o enviado-a la dirección IP remota.
Sesiones – Muestra el número de sesiones TCP/IP establecidas. Si no fueron establecidas conexiones TCP (fallo de conexión, o el protocolo es UDP/IP o ICMP/IP), este valor es cero.
Puertos – Muestra los puertos de computadoras remotas utilizados durante la conexión TCP/IP o intentos de conexión. Esta lista puede estar vacía si el protocolo no es TCP/IP. Los puertos pueden ser mostrados tanto como valores numéricos o como el correspondiente nombre de servicio. Para más información vea opciones de configuración.
Nombre de Host – Muestra el nombre de host de la computadora remota. Si el nombre de host no puede ser resuelto, esta columna estará vacía.
Bytes – Muestra el número de Bytes transmitidos durante la sesión.
Último Paquete – Muestra el tiempo del último paquete enviado /recibido durante esta sesión.
Proceso – Muestra el proceso sobre su computadora que envía o recibe paquetes en la sesión. Esta columna sólo está disponible en Windows 2000/XP/2003. La asignación de paquetes sólo funciona para paquetes entrantes y salientes, dado que CommView no puede estar al tanto de los procesos que corren sobre otras computadoras que envían o reciben paquetes. Naturalmente, puede haber varias aplicaciones sobre la computadora local intercambiando datos con una computadora remota, por lo que la pestaña **Últimas conexiones IP** sólo muestra las últimos procesos que envían o reciben datos para este particular par de direcciones IP. si desea mapear un proceso a un paquete determinado, puede ver la información en el árbol de paquete decodificado en la pestaña **Paquetes**. CommView puede mostrar el paso completo al proceso que envía o recibe paquetes, marque la casilla **Mostrar la ruta completa del proceso** en la pestaña **Preferencias** => **Opciones**, **General** para activar esta función.

Puede mostrar u ocultar columnas individuales haciendo clic en el ítem correspondiente en el menú **Ver => Columnas de Últimas Conexiones IP**

Puede mostrar u ocultar columnas individuales hacienda clic derecho en la lista de encabezado o usando el menú **Ver** => **Columnas de Últimas Conexiones IP**. El orden de columnas puede ser cambiado arrastrando el encabezado de la columna a la nueva ubicación.

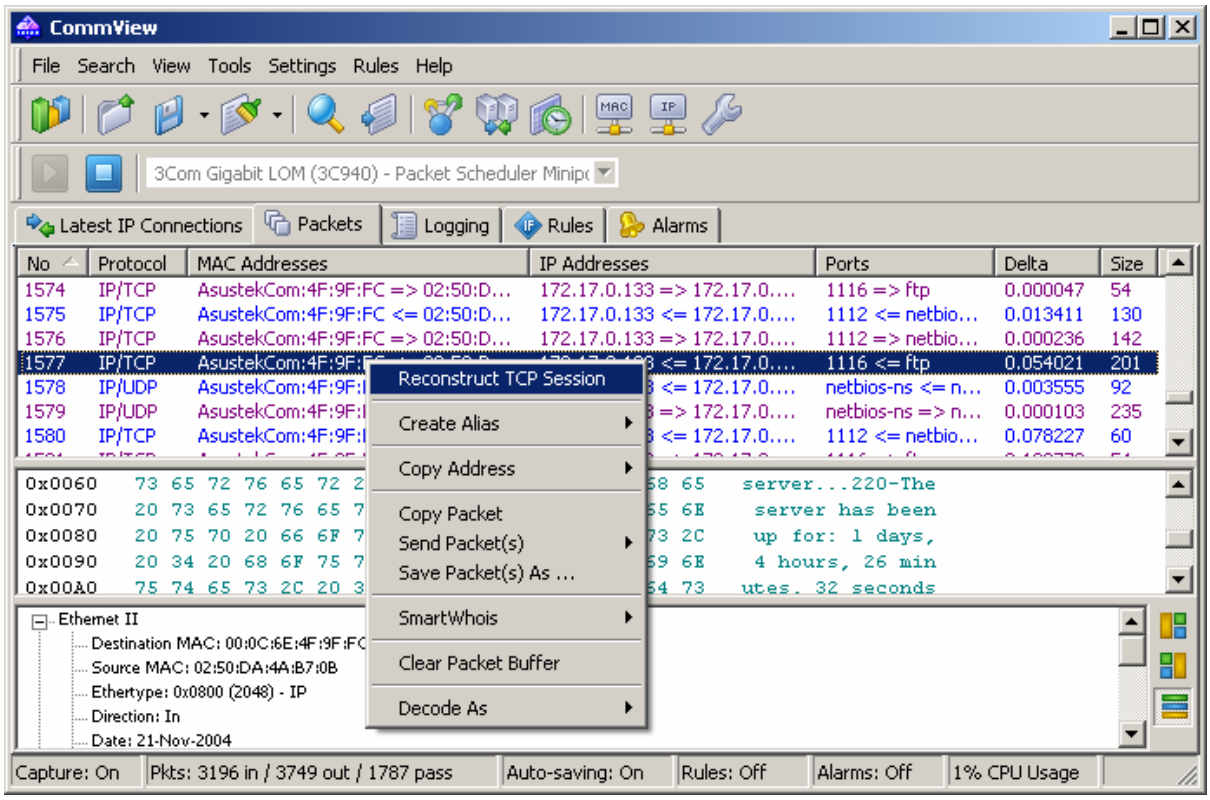
Menú de Comandos

Haciendo clic en el botón derecho de Últimas Conexiones IP muestra un menú de acceso directo con los siguientes comandos:

Filtro Rápido – Encuentra los paquetes enviados entre las direcciones IP seleccionadas y los muestra en una nueva ventana. La misma acción es realizada cuando hace doble clic sobre esta ventana.
Copiar – copia la dirección IP local, la dirección IP remota, o el nombre del host al portapapeles.
Mostrar Todos los Puertos – muestra una ventana con la lista completa de puertos utilizados en la comunicación entre el par de direcciones IP seleccionadas. Esto es útil cuando fueron utilizados muchos puertos, y ellos exceden la columna correspondiente.
Transferencia de Datos – muestra una ventana con información sobre el volumen de datos transferidos entre el par de direcciones IP seleccionadas y la hora del último paquete.
Ir A – permite que usted vaya al primer/último paquete de una dirección IP seleccionada de origen/destino; El programa le mostrará la pestaña de paquetes y moverá el cursor del mouse hacia el paquete que coincida con el criterio elegido.
SmartWhois – envía la dirección IP fuente o destino remota seleccionada a SmartWhois, si se encuentra instalado en su sistema. SmartWhois es una aplicación desarrollada por nuestra empresa capaz de obtener información acerca de cualquier dirección IP o nombre de host en el mundo. Esta provee automáticamente información asociada con la dirección IP como dominio, nombre de red, país, estado o provincia, ciudad. Este programa puede ser descargado desde nuestro sitio.
Crear Alias – Le Provee una ventana donde puede asignar un alias fácil de recordar, para la dirección IP seleccionada.
Proceso – Le permite obtener información adicional acerca, o realizar acciones, con el proceso que envía o recibe paquetes en la sesión seleccionada (sólo en Windows 2000/XP/2003). Puede **Terminar** un proceso, ver el diálogo de **Propiedades de Archivo**, o hacer al programa **Mostrar la ruta completa** al archivo ejecutable del proceso.
Guardar Últimas Conexiones IP Como – le permite guardar el contenido de la pestaña de Últimas Conexiones IP como un reporte HTML o delimitado por coma (CSV).
Borrar Últimas Conexiones IP – Borra la tabla.
Estadísticas Adicionales – Muestra una ventana con estadísticas sobre transferencia de datos y distribución de protocolos.

Paquetes

Esta etiqueta es utilizada para mostrar todos los paquetes de red capturados y mostrar la información detallada acerca de un paquete seleccionado.



La **tabla superior** muestra la lista de paquetes capturados. Utilice esta lista para seleccionar un paquete que desee ver y analizar. Cuando selecciona un paquete haciendo clic en él, los otros paneles mostraran información acerca del paquete seleccionado.

El significado de las columnas de esta tabla está explicado a continuación:

No – un número único de paquete.
Protocolo – Muestra el protocolo del paquete.
MAC Fnt, MAC Dest – muestra las direcciones MAC de Fuente y Destino.
IP Fnt, IP Dest – Muestra las direcciones IP de Fuente y Destino (Según se aplique).
Puerto Fnt, Puerto Dest – Muestra los puertos de fuente y destino (Según se aplique). Los puertos pueden ser mostrados tanto como valores numéricos como con el correspondiente nombre de servicio. Para más información, vea Configurando Opciones.
Tiempo / Diferencia – Muestra el valor absoluto o la variación de tiempo del paquete. La variación del tiempo es la diferencia entre los tiempos absolutos de los dos últimos paquetes. Usted puede elegir entre tiempo absoluto y variación haciendo clic en **Ver=> Columnas de Paquetes=>Mostrar Tiempo Como.**
Tamaño – Muestra el tamaño del paquete en bytes. Esta columna no se encuentra visible por omisión

Puede mostrar u ocultar columnas individuales hacienda clic derecho en la lista de encabezado o usando el menú **Ver** => **Columnas de Paquetes**. El orden de columnas puede ser cambiado arrastrando el encabezado de la columna a la nueva ubicación.

El envío de paquetes puede ser suspendido haciendo clic en **Archivo=>Suspender salida de paquetes**. En el modo suspendido los paquetes son capturados, pero no mostrados, en la pestaña **Paquetes.** Este modo es útil cuando está interesado solo en las estadísticas más que en los paquetes individuales. Para reanudar la muestra de los paquetes en tiempo real haga clic en **Archivo=>Reiniciar Salida de Paquetes**.

El **Panel Medio** muestra el contenido de las filas del paquete, en notación hexadecimal y en texto. En la parte de texto los caracteres no representables son reemplazados por puntos. Cuando son seleccionados paquetes múltiples en la **tabla superior**, el **Panel Medio** muestra el número total de paquetes seleccionados, el tamaño total, y la hora impresa entre el primer y el último paquete.

El **Panel inferior** muestra la información decodificada del paquete para un paquete seleccionado. Esta información incluye datos esenciales que pueden ser utilizados por los profesionales de red. Haciendo clic en el botón derecho sobre el panel invoca el menú de contexto que le permite colapsar/expandir todos los nodos, copiar el nodo seleccionado o todos ellos.

La pestaña paquetes también incluye una pequeña barra de herramientas mostrada a continuación:

Puede cambiar la posición de la ventana del decodificador haciendo clic sobre uno de los tres botones sobre esta barra de herramientas (puede tener la ventana del decodificador alineada abajo, a la izquierda o la derecha). El cuarto botón hace que la lista de paquetes se displace automáticamente hasta el último paquete recibido. El quinto botón mantiene el paquete que seleccionó en la lista visible (por ejemplo: no dejará el área visible a medida que arriban nuevos paquetes). El sexto botón le permite abrir el contenido de buffer de paquete actual en una nueva ventana. Esta funcionalidad es muy útil bajo una carga pesada de red, cuando la lista de paquetes es movida rápidamente y es difícil examinar paquetes antes que se mueva fuera del área visible. Haciendo clic en este botón crea una instantánea del buffer por lo que puede cómodamente examinarlo en una ventan separada. Puede tomar tantas instantáneas como desee.

Comandos del Menú

Haciendo clic en el botón derecho de la lista de paquetes muestra un menú con los siguientes comandos:

Reconstruir Sesión TCP – Le permite reconstruir una sesión TCP Comenzando desde el paquete seleccionado; Este abre una ventana que muestra la conversación completa entre dos Hosts. La misma acción es realizada cuando hace doble clic sobre esta ventana.
Filtro Rápido – Encuentra los paquetes enviados entre las direcciones físicas (MAC), direcciones IP, o puertos seleccionadas y las muestra en una nueva ventana.
Abrir Paquete(s) en Nueva Ventana – le permite abrir uno o varios paquetes seleccionados en una nueva ventana para un lcómoda investigación
Crear Alias – muestra una ventana donde puede asignar un alias fácil de recordar para las direcciones físicas o IP seleccionada.
Copiar Dirección – copia la dirección física de origen, la dirección física de destino, la dirección IP de origen, o la dirección IP destino al portapapeles.
Copiar Paquete – copia la fila de datos del paquete seleccionado al portapapeles.
Enviar Paquete(s) – muestra la ventana Generador de Paquetes que le permite re-enviar el paquete seleccionado o un grupo de paquetes. También puede modificar el contenido del paquete antes de enviarlo.
Guardar Paquete(s) Como – Guarda el contenido del(los) paquete(s) seleccionados a un archivo. El cuadro de diálogo le permite seleccionar el formato a ser utilizado salvándolos desde la lista mostrada.
SmartWhois – Envía la dirección IP de origen o destino para el paquete seleccionado a SmartWhois si éste está instalado sobre su sistema. SmartWhois es una aplicación autónoma desarrollada por nuestra compañía capaz de obtener información acerca de cualquier dirección IP o Nombre de Host en el mundo. Automáticamente provee información asociada con una dirección IP, tales como el dominio, nombre de red, país, estado o provincial, y ciudad. El programa puede ser descargado desde nuestro sitio.
Borrar Buffer de Paquetes – Borra el contenido del buffer del programa. La lista de paquetes será borrada y no será capaz de ver los paquetes previamente capturados por el programa.
Decodificar Como – Para paquetes TCP y UDP, le permite decodificar protocolos soportados que utilizan puertos No estándar. Por ejemplo, si su servidor SOCKS corre sobre el puerto 333 en lugar del 1080, puede seleccionar un paquete que pertenece a la sesión SOCKS y mediante este comando de menú hacer que CommView decodifique todos los paquetes sobre el puerto 333 como paquetes SOCKS. Tal reasignación de Puerto-protocolo no es permanente y permanece hasta que el programa se cierre. Advierta que no puede superponerse a pares de puerto-protocolo estándar, por ejemplo no puede hacer que CommView decodifique paquetes sobre el puerto 80 como paquetes TELNET.
Fuente – le permite aumentar o disminuir el tamaño de fuente usado para mostrar paquetes si afectar el tamaño de fuente de todos los demás elementos de la interfaz.
También puede arrastrar y soltar el/los paquete(s) seleccionados al escritorio.

Registro

Esta pestaña se utiliza para guardar los paquetes capturados en un archivo en el disco. CommView guarda los paquetes en su propio formato con la extensión .NCF. El antiguo formato (CCF) es soportado debido a la compatibilidad de versiones anteriores; sin embargo no puede volver a guardar los paquetes capturados. Puede abrir y ver estos archivos en cualquier momento utilizando el Visor de Registro, o haciendo doble-clic sobre cualquier archivo NCF o CCF para que este se abra y decodifique.

NCF es un formato abierto; por favor refiérase al capítulo Formatos de Archivo de Registro de CommView para una descripción detallada del formato NCF

Guardar y Administrar

Utilice este cuadro para guardar manualmente los paquetes capturados en un archivo y para concatenar/dividir archivos capturados.

Puede guardar todos los paquetes almacenados actualmente en el buffer o guardar solo una parte de ellos en un rango dado. Los campos **Hacia y Desde** le permiten definir el rango buscado basado en los números de paquetes como se muestra en la pestaña de paquetes. Haga clic en **Guardar como...** para seleccionar el nombre del archivo.

Para concatenar archivos múltiples NCF, dentro de un único archivo grande, haga clic sobre el botón **Concatenar Registros**. Para dividir archivos NCF que son muy grandes en porciones de menor tamaño, haga clic en el botón **Dividir Registros**. Luego el programa lo guiará a través del proceso, y será capaz de ingresar el tamaño deseado de los archivos de salida.

Guardar Automáticamente

Marque esta opción para que el programa guarde los paquetes de forma automática mientras estos arriben. Utilice el campo **Tamaño máximo del directorio** para limitar el tamaño total de los archivos de captura almacenados en el **Directorio de Registros**. Si el tamaño total de los archivos de captura excede este limite, el programa elimina automáticamente los archivos más antiguos de esta carpeta. El campo **Tamaño promedio de Archivo de Registro** le permite especificar el tamaño aproximado deseado de cada archivo de registro. Cuando el archivo de registro alcanza el tamaño especificado, es creado automáticamente un nuevo archivo de registro. Para cambiar la carpeta por omisión del **Directorio de Registros,** haga clic sobre la casilla **Guardar registros en** y seleccione una carpeta diferente.

IMPORTANTE: Si desea conservar un archivo almacenado que considere importante por un largo período, no lo mantenga en el Directorio de Registro por omisión: es posible que éste sea automáticamente borrado cuando sean guardados nuevos archivos. Mueva ese archivo a una carpeta diferente para preservarlo.

Observe por favor que el programa no guarda cada paquete de forma individual inmediatamente de su captura. Esto significa que si usted ve el archivo de registros en tiempo real, éste puede no contener los últimos paquetes. Para hacer que el programa inmediatamente escriba el contenido del buffer en el archivo de registro, haga clic en **Detener Captura** o deseleccione **Guardar automáticamente.**

Registro de acceso WWW

Marque este cuadro para activar el registro de sesiones HTTP. Utilice el campo **Tamaño Máximo de Archivo** para limitar el tamaño del archivo de registro. Si el tamaño del archivo de registro excede el límite, el programa automáticamente borra los registros mas viejos en el archivo. Para cambiar el nombre y la ruta por omisión del archivo, haga clic sobre el cuadro **Guardar archivos en** y seleccione un nombre de archivo diferente. Los archivos de registro pueden ser generados en formato **HTML** o **TXT.** Haga clic en **Configurar** para cambiar las opciones por omisión de registro. Puede cambiar el número de puerto que es usado para acceso http (el valor por omisión es 80 y puede no funcionar para usted si está detrás de un servidor proxy), y excluir cierto tipo de datos (generalmente registrando cualquier cosa distinta a páginas HTML es casi inútil, por lo tanto es una buena idea excluir URLs o imágenes del archivo de registro).

Visor de Registros

Visor de Registros es una herramienta para ver y explorar archivos de captura creados por CommView y otros analizadores de paquetes. Tiene la funcionalidad de la pestaña Paquetes de la ventana del programa principal, pero a diferencia de la pestaña Paquetes, Visor de Registros muestra los paquetes provenientes de los archivos en el disco en lugar de los paquetes capturados en tiempo real.

Para abrir Visor de Registros, haga clic en **Archivo => Visor de Registros** del menú principal del programa, o solo haga doble clic sobre cualquier archivo de captura CommView que halla previamente guardado. Puede abrir tantas ventanas de Visor de Registros como usted quiera, y cada una de ellas puede ser utilizada para explorar uno o varios archivos capturados.

Visor de Registros puede ser utilizado para explorar archivos de captura creados por otros analizadores de paquetes y firewalls personales. La versión actual puede importar en los formatos de Network Instruments Observer®, Network General Sniffer® para DOS/Windows, Microsoft NetMon, WildPackets EtherPeek™ y AiroPeek™, y Tcpdump (libcap). Estos formatos también son utilizados por numerosas aplicaciones de terceros. Visor de Registros es capaz de exportar datos de paquetes mediante la creación de archivos en los formatos Network Instruments Observer®, Network General Sniffer® para DOS/Windows, Microsoft® NetMon, WildPackets EtherPeek™ y AiroPeek™, y Tcpdump (libcap) también como en el formato nativo de CommView.

La utilización de Visor de Registros es similar a utilizar la pestaña de **Paquetes** de la ventana principal; por favor refiérase al capitulo Paquetes si necesita información detallada.

Menú del Visor de Registros

Archivo

Abrir Registros CommView – abre y carga uno o varios archivos de captura CommView.
Importar Registros – le permite importar archivos de captura creados por otro analizador de paquetes.
Exportar Registros – le permite exportar los paquetes mostrados a archivos de captura en formatos diferentes.
Borrar Ventana – borra la lista de paquetes.
Generar Estadísticas – hace que CommView genere estadísticas sobre los paquetes cargados en Visor de Registros. Opcionalmente, es posible restaurar datos estadísticos colectados previamente mostrados en el la ventana **Estadísticas**. Por favor advierta que esta función no mostrará la distribución de paquetes a lo largo de una línea de tiempo. Se limita a mostrar totales, gráficos de protocolos, y tablas de host de LAN.
Cerrar Ventana – cierra la ventana.

Buscar

Buscar Paquete – Muestra un cuadro de diálogo que le permite Buscar paquetes que coincidan con un texto específico.
Ir a Paquete Número – Muestra un cuadro de dialogo que le permite ir a un paquete con un número específico.

Reglas

Aplicar - Aplica el conjunto de reglas actuales a los paquetes mostrados en Visor de Registros. Como resultado, cuando utiliza este comando el programa borrará los paquetes que no concuerden con el conjunto de reglas actuales. Tenga en cuenta que esto no modifica el archivo en el disco.
Desde Archivo... – Produce los mismos resultados que el comando **Aplicar** pero le permite utilizar el conjunto de reglas desde un archivo .RLS previamente guardado, en lugar del conjunto de reglas actuales.

Reglas

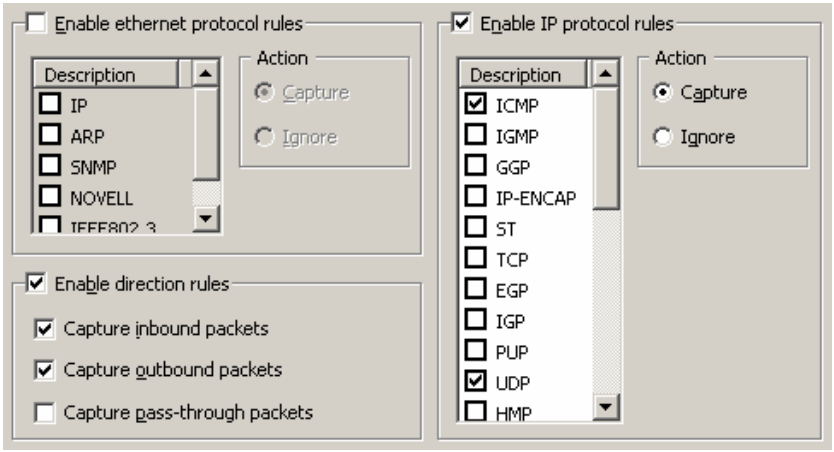
Esta pestaña le permite definir reglas para la captura de paquetes. Si una o más reglas son definidas, el programa filtra paquetes basándose en esas reglas y muestra solo los paquetes que cumplen con las reglas especificadas. Tenga en cuenta que CommView No es un firewall, y cuando define las reglas, los paquetes siguen siendo procesados por el sistema operativo; ellos solamente no seran mostrados y almacenados por CommView. Si una regla es definida, el nombre de la pestaña correspondiente es mostrado en negrita.

Usted puede guardar la(s) definición(es) de reglas en un archivo y abrirlas mediante la utilización del comando **Reglas** en el menú del programa.

Ya que el tráfico de red puede generar frecuentemente gran cantidad de paquetes es recomendable la utilización de reglas para el filtrado de los paquetes innecesarios. Esto puede reducir la cantidad de recursos del sistema consumidos por el programa. Si quiere habilitar/deshabilitar una regla, seleccione la rama apropiada en el lado izquierdo de la ventana (ejemplo. **Direcciones IP** o **Puertos**), y seleccione o deseleccione (**Habilitar Reglas Direcciones IP** o **Habilitar Reglas de Puerto**). Existen ocho tipos diferentes de reglas que se pueden utilizar:

Protocolos y Direcciones

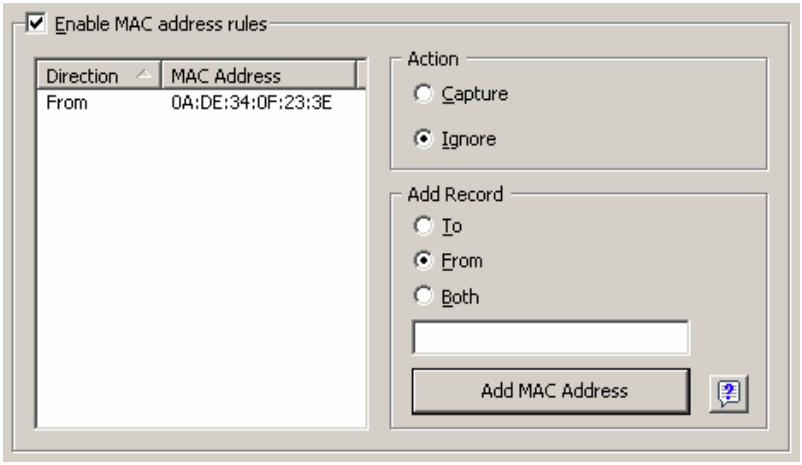
Le permite ignorar o capturar paquetes basados en protocolos de Ethernet (Capa 2) e IP (Capa 3), como también basado en la dirección del paquete.



Este ejemplo muestra como hacer que el programa capture solamente los paquetes ICMP y UDP entrantes y salientes. Todos los otros paquetes en la familia IP van a ser ignorados; También van a ser ignorados todos los paquetes que sean pasantes.

Direcciones Físicas

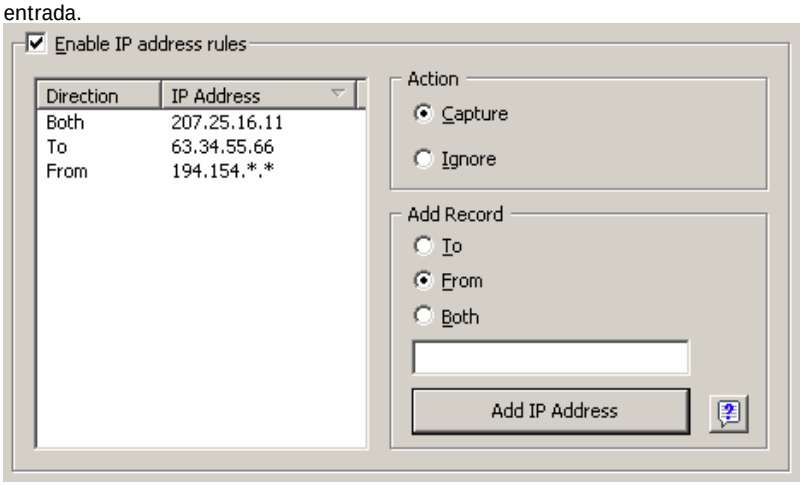
Le permite ignorar o capturar paquetes basados en la dirección física (MAC). Ingrese una dirección física (MAC) en el cuadro **Agregar Registro,** seleccione la dirección **Desde, Hacia, Ambas**, y haga clic en **Agregar Dirección Física**. La nueva regla será mostrada. Ahora puede seleccionar la acción a ser tomada cuando un nuevo paquete sea procesado; El paquete puede ser tanto capturado como ignorado. También puede hacer clic sobre el botón de Alias de la dirección física para tener la lista de Alias; Haga doble clic sobre el alias que quiere agregar, y la dirección física (MAC) correspondiente aparecerá en el cuadro de entrada.



Este ejemplo muestra como hacer que el programa ignore los paquetes provenientes desde 0A:DE:34:0F:23:3E. Todos los paquetes que provengan de otras direcciones físicas serán capturados.

Direcciones IP

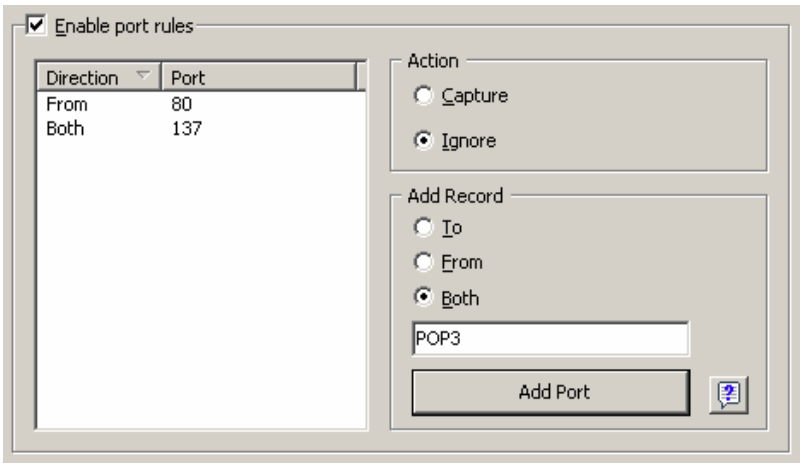
Le permite ignorar o capturar paquetes basados en las direcciones IP. Ingrese una dirección IP en la sesión **Agregar Registro,** seleccione la dirección **Desde, Hacia, o Ambos**), y haga clic en **Agregar Dirección IP**. Puede usar comodines para especificar bloques de direcciones IP. Esta nueva regla será mostrada. Ahora puede seleccionar que esta acción se lleve a cabo cuando un paquete es procesado: el paquete puede ser capturado o ignorado. Puede también hacer clic en el botón IP Alias para obtener la lista de alias, haga doble-clic sobre el alias que usted desea agregar y la dirección correspondiente aparecerá en el cuadro de entrada.



Este ejemplo muestra como hacer que el programa capture los paquetes que se dirigen a la dirección 63.34.55.66, y se dirigen / provienen de la dirección 207.25.16.11 y provienen de todas las direcciones entre 194.154.0.0 y 194.154.255.255. Todos los paquetes que provienen de otras direcciones y van hacia otras direcciones serán ignorados. Ya que las direcciones IP solamente son utilizadas en el protocolo IP, esta definición automáticamente hará que el programa ignore todos los paquetes no-IP.

Puertos

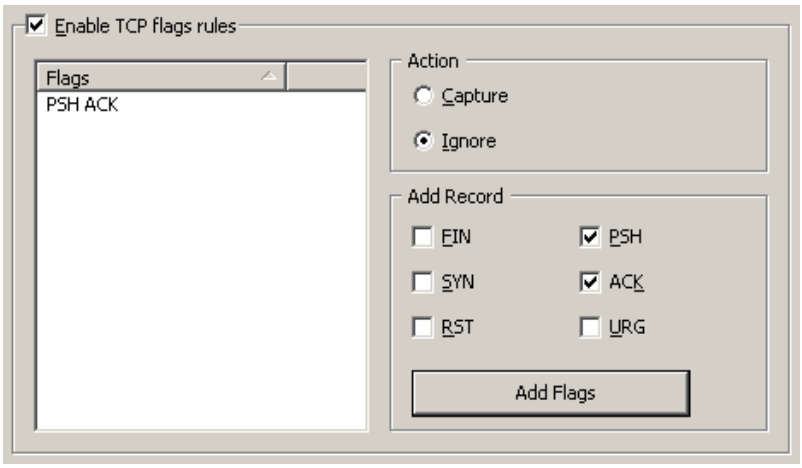
Le permite ignorar o capturar paquetes basados en el Puerto. Ingrese un número de puerto en el cuadro **Agregar Registro**, seleccione la dirección (**Desde, Hacia, o Ambos**), y haga clic en **Agregar Puerto.** La nueva regla será mostrada. Ahora puede seleccionar la acción a ser tomada cuando un nuevo paquete sea procesado; El paquete puede ser tanto capturado como ignorado. También puede hacer clic sobre el botón de **Información sobre Puertos** para tener una lista de todos los puertos conocidos; Haga doble clic sobre el puerto que quiera agregar y su número aparecerá en el cuadro de entrada. Los puertos también pueden ser introducidos como texto; por ejemplo, puede ingresar *http* o *pop3*, y el programa convertirá el Nombre del Puerto a un valor numérico.



Este ejemplo muestra como hacer que el programa ignore los paquetes que provienen del Puerto 80 y los que provienen y salen del Puerto 137. Esta regla previene que CommView muestre el tráfico entrante http, como también el tráfico entrante/saliente "Nombre de Servicios de NetBIOS". Todos los paquetes entrantes y salientes de otros puertos serán capturados.

Indicadores TCP

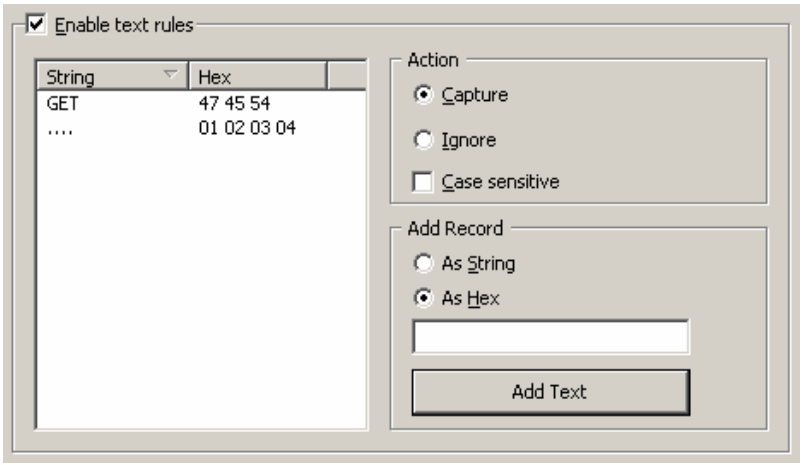
Le permite ignorar o capturar paquetes basados en indicadores de TCP, Controle un indicador o una combinación de indicadores en el cuadro **Agregar Registro**, haga clic en **Agregar Indicadores**. La nueva regla será mostrada. Ahora puede seleccionar la acción a ser tomada cuando un nuevo paquete con los indicadores de TCP sea procesado; El paquete puede ser tanto procesado como ignorado.



Este ejemplo muestra como hacer que el programa ignore los paquetes TCP con el indicador PSH ACK. Todos los paquetes con otros indicadores TCP serán capturados

Texto

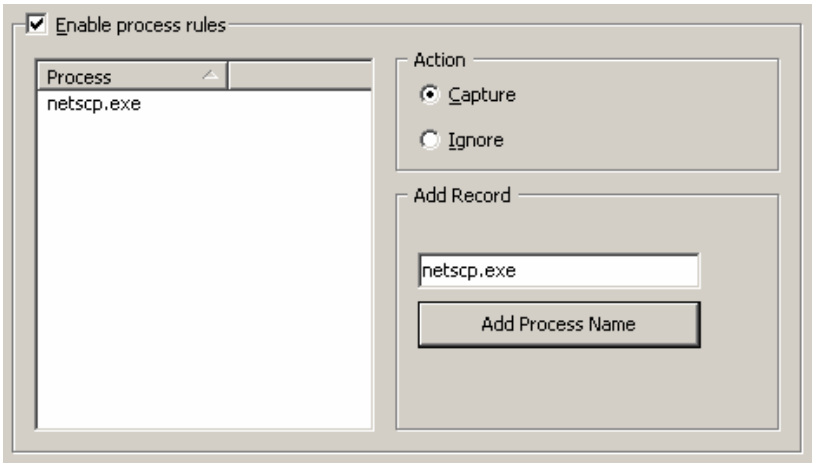
Le permite capturar paquetes que contengan determinado texto. Introduzca una cadena de caracteres en el cuadro **Agregar Registro** seleccione el tipo de información ingresada (**Como Cadena de Caracteres o Como Hexadecimal**), y haga clic en **Agregar Texto.** La nueva regla será mostrada. Puede ingresar texto como una cadena de caracteres, o como un valor hexadecimal, este último debería ser utilizado cuando quiere ingresar caracteres no imprimibles; Solo ingrese los valores de caracteres hexadecimales separados por espacios, como se muestra a continuación. Ahora puede seleccionar la acción ha ser realizada cuando un nuevo paquete sea procesado; el paquete puede ser tanto capturado como ignorado.



Este ejemplo muestra como hacer que el programa capture solo los paquetes que contiene tanto "GET" o los datos hexadecimales 01 02 03 04. Marque la casilla Coincidir MAYÚSCULAS/minúsculas **si quiere que las reglas utilicen la comparación en Texto Exacto. Todos los otros paquetes que no contengan el texto mencionado arriba serán ignorados**

Proceso

Le permite capturar paquetes basado en el nombre del proceso (esta funcionalidad no está disponible bajo Windows 98/Me). Ingrese el nombre del proceso en el cuadro **Agregar Registro** y haga clic en **Agregar Nombre de Proceso**. La nueva regla será mostrada. Ahora puede seleccionar la acción a ser tomada cuando un nuevo paquete es procesado: el paquete puede ser tanto capturado como ignorado. Puede ingresar nombres de procesos parciales, por ejemplo *netscp* o *net*; cualquier nombre de proceso que contenga tal cadena de caracteres coincidirá con la regla. Los nombres de proceso no son sensibles a mayúsculas.



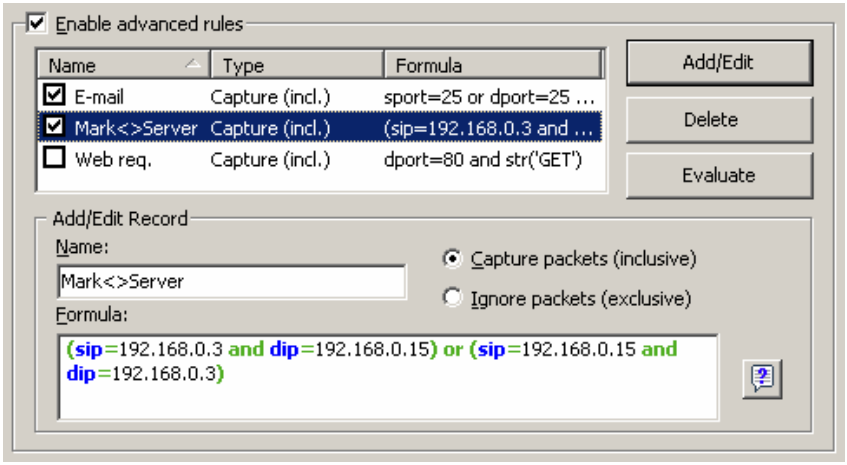
Este ejemplo muestra como hacer que el programa capture solo los paquetes que fueron enviados o recibidos por *netscp.exe*. Los paquetes enviados por otros procesos serán ignorados.

Avanzado

Las reglas avanzadas son las reglas más poderosas y flexibles que le permitirán crear filtros complejos utilizando la Lógica Booleana. Para una detallada ayuda de cómo usar las reglas avanzadas, por favor refiérase al capitulo Reglas Avanzadas.

Reglas Avanzadas

Las reglas avanzadas son reglas que poseen mayor flexibilidad y son más poderosas. Las mismas le permiten crear filtros complejos utilizando lógica Booleana. La utilización de reglas avanzadas requiere un entendimiento básico de lógica y matemáticas, pero la sintaxis de las reglas es fácil de comprender.



Perspectiva **General**

Para agregar una nueva regla, deberá ingresar un nombre a elección en el campo **Nombre,** seleccionar la acción **Capturar / Ignorar**, ingresar una **Formula** utilizando la sintaxis descripta a continuación, y hacer clic en **Agregar / Editar.** Su nueva regla será agregada a la lista y se activara de forma inmediata. Puede agregar todas las reglas que desee, pero solo aquellas reglas que tienen marcado la casilla contigua al nombre de la regla estarán actualmente activas. Puede activar/desactivar reglas marcando/desmarcando las casillas correspondientes o eliminar completamente las reglas seleccionadas utilizando el botón **Eliminar.** Si más de una regla está activa, puede evaluar la regla combinada resultante haciendo clic en **Evaluar**. Por favor observe que múltiples reglas activas estarán combinadas utilizando el operador lógico OR, por ejemplo si tiene tres reglas activas, RULE1, RULE2, y RULE3, la regla resultante será RULE1 OR RULE2 OR RULE3.

Puede utilizar las reglas avanzadas en conjunción con las reglas básicas descriptas en el capitulo previo, sin embargo, si se siente confortable con la lógica booleana, es buena idea utilizar solamente reglas avanzadas, ya que ofrecen mayor flexibilidad. Las reglas básicas se combinan con reglas avanzadas utilizando el operador lógico AND.

Descripción de la sintaxis

dir - Dirección del paquete. Los valores posibles son *in* (entrante), *out* (saliente), y *pass* (pasante).

etherproto - Protocolo Ethernet, el 13vo y 14vo Bytes del paquete. Los valores aceptables son numéricos (ejemplo *etherproto=0x0800* para IP) o alias utilizados comúnmente (ejemplo *etherproto=ARP*, que es equivalente a 0x0806).

ipproto - Protocolo IP. Los valores aceptables son numéricos (ejemplo *ipproto!=0x06* para TCP) o alias utilizados comúnmente (ejemplo *ipproto=UDP*, que es equivalente a 0x11).

smac - Dirección física de origen. Los valores aceptables de las direcciones físicas se deben expresar en notación hexadecimal (ejemplo *smac=00:00:21:0A:13:0F*) o alias definido por el usuario.

dmac - Dirección física de destino.

sip - Dirección IP de origen. Los valores aceptables son direcciones IP en notación puntuada (e.g. *sip=192.168.0.1*), direcciones IP con comodines (e.g. *sip!=*.*.*.255*), direcciones de red y máscaras de subnet (e.g. *sip=192.168.0.4/255.255.255.240* o *sip=192.168.0.5/28*), rangos de IP (e.g. *sip from 192.168.0.15 to 192.168.0.18* o *sip in 192.168.0.15 .. 192.168.0.18*), o Alias definidos por el usuario.

dip - Dirección IP de destino.

sport - Puertos de origen para paquetes de TCP y UDP. Los valores aceptables son numéricos (ejemplo *sport=80* para HTTP), rangos (ejemplo *sport from 20 to 50* o *sport in 20..50* para cualquier número de Puerto entre 20 y 50) o alias definidos por el sistema operativo (ejemplo *sport=ftp*, que es equivalente a 21). Para la lista de alias soportados por su sistema operativo haga clic en **Ver => Información de Referencia de Puertos**

dport - Puerto de destino para los paquetes TCP y UDP.

flag - Indicador TCP. Los valores aceptables son numéricos (ejemplo *0x18* para PSH ACK) o uno o varios de los siguientes caracteres: *F* (FIN), *S* (SYN), *R* (RST), *P* (PSH), *A* (ACK), y *U* (URG), o la clave *has*, que significa que el indicador contiene un valor cierto. Ejemplos de uso: *flag=0x18*, *flag=SA*, *flag has F*.

size - Tamaño del paquete. Los valores aceptados son numéricos (ej: size*=1514*) o rangos (ej. *size from 64 to 84* o *size in 64..84* para cualquier tamaño entre 64 y 84).

str - Contenido del paquete. Utilice esta función para indicar que el paquete debe contener una cadena de caracteres. Esta función tiene tres argumentos: cadena de caracteres, posición y MAYÚSCULAS/minúsculas. El primer argumento es una cadena de caracteres, por ejemplo *'GET'*. El segundo argumento es un número que indica el desplazamiento de la posición de la cadena de caracteres en el paquete. La primera posición para medir el desplazamiento es CERO, por ejemplo si está buscando por el primer Byte en el paquete, el valor del desplazamiento debe ser *0*. Si el valor del desplazamiento no es importante, utilice *-1*. El tercer argumento es MAYÚSCULAS/minúsculas y puede ser *false* (no sensible a MAYÚSCULAS/minúsculas) o *true* (sensible a MAYÚSCULAS/minúsculas). El segundo y el tercer argumento son opcionales, si se omiten, el desplazamiento por omisión es *-1* y la sensibilidad a MAYÚSCULAS/minúsculas por omisión es *false*. Ejemplos de uso: *str('GET',-1,false)*, *str('GET',-1)*, *str ('GET')*.

hex - Contenido del paquete. Utilice esta función para indicar que el paquete debe contener un cierto patrón hexadecimal. Esta función tiene dos argumentos: patrón hex y posición. El primer argumento es un valor hexadecimal, ejemplo *0x4500*. El segundo argumento es un número indicando el desplazamiento del patrón en el paquete. El desplazamiento está basado en cero, ejemplo. Si usted está buscando por el primer byte de un paquete, el valor del desplazamiento debe ser *0*. Si el desplazamiento no es importante, utilice *-1*. El segundo argumento es opcional; si es omitido, el valor del desplazamiento será *-1*. Ejemplo de uso: *hex(0x04500, 14)* , *hex(0x4500, 0x0E)*, *hex (0x010101)*.

bit – Contenido del paquete. Use esta función para determinar si el bit especificado en el desplazamiento especificado está fijado a 1. En este caso, la función da como resultado *verdadero* (*true)*. Si el bit especificado está fijado a 0 o el byte especificado está más allá del límite del paquete, la función da como resultado *falso (false)*. Esta función tiene dos argumentos índices de bit y posición de byte. El primer argumento es el índice de bit en el byte; Los valores permitidos son 0-7. El índice está basado en 0, por ejemplo si está buscando por el octavo bit en el byte, el valor de índice debe ser *7*. El segundo argumento es un número que indica la posición del byte (desplazamiento) en el paquete. El desplazamiento está basado en cero, por ejemplo si está buscando el primer byte en el paquete, el valor del desplazamiento debe ser *0*. Ambos argumentos son obligatorios, Ejemplos de Uso: *bit(0, 14)* , *bit(5, 1).*

Las palabras clave descriptas a continuación pueden ser utilizadas con los siguientes operadores:

and - Conjunción Booleana.
or - Disyunción Booleana.
not - Negación Booleana.
= - Igualdad aritmética.
!= - desigualdad aritmética.
< > - desigualdad aritmética.
> - Aritmética mayor-que.
< - Aritmética menor-que.
( ) - paréntesis, operador de control precedente de las reglas.

Todos los números pueden encontrarse en notación decimal o hexadecimal. Si usted desea utilizar notación hexadecimal, el número debe estar precedido de *0x*, ejemplo usted puede utilizar tanto el *15* o el *0x0F*.

Ejemplos

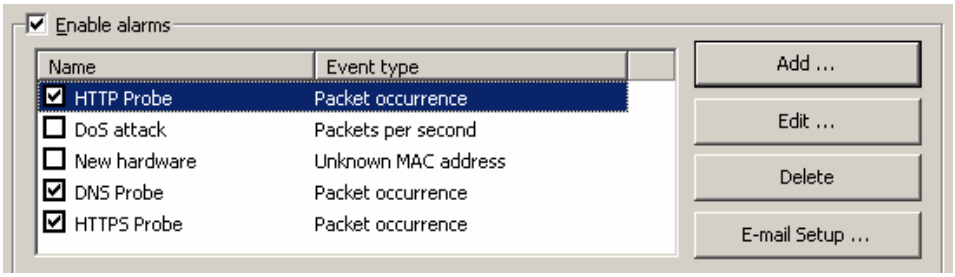
A continuación encontrará un número de ejemplos ilustrando las reglas de sintaxis. Cada regla esta seguida por nuestros comentarios acerca de lo que realiza cada regla. Las reglas son mostradas en rojo. Los comentarios están separados de la regla actual por dos barras.

- **dir**!**=**pass // Capturar solamente paquetes entrantes y salientes. Los paquetes pasantes que son enviados por otras computadoras en la LAN son ignorados.
- **(smac=00:00:21:0A:13:0E or smac=00:00:21:0A:13:0F) and etherproto=arp** // Captura puertos ARP enviados por dos computadoras, 00:00:21:0A:13:0E y 00:00:21:0A:13:0F.
- **ipproto=udp and dport=137** // Captura paquetes UDP/IP enviados al Puerto número 137.
- **dport=25 and str('RCPT TO:', -1, true)** // Captura paquetes TCP/IP o UDP/IP que contengan "'RCPT TO:" y donde el Puerto de destino es 25.
- **not (sport>110)** // Captura todo excepto los paquetes donde el Puerto de origen es mayor a 110
- **(sip=192.168.0.3 and dip=192.168.0.15) or (sip=192.168.0.15 and dip=192.168.0.3)** // Captura solamente los paquetes IP que están siendo enviados entre las maquinas, 192.168.0.3 y 192.168.0.15. Todos los demás paquetes serán descartados.
- **((sip from 192.168.0.3 to 192.168.0.7) and (dip = 192.168.1.0/28)) and (flag=PA) and (size in 200..600)** // Capturar los paquetes TCP cuyo tamaño esté entre 200 y 600 bytes provenientes de las direcciones IP cuyo rango sea 192.168.0.3 - 192.168.0.7, cuya dirección IP de destino se encuentre en el segmento 192.168.0.1/255.255.255.240 , y cuando su indicador TCP es PSH ACK.
- **Hex(0x0203, 89) and (dir<>in)**// Capturar los paquetes que contienen 0x0203 y el desplazamiento 89, donde la dirección del paquete no sea entrante.

Alarmas

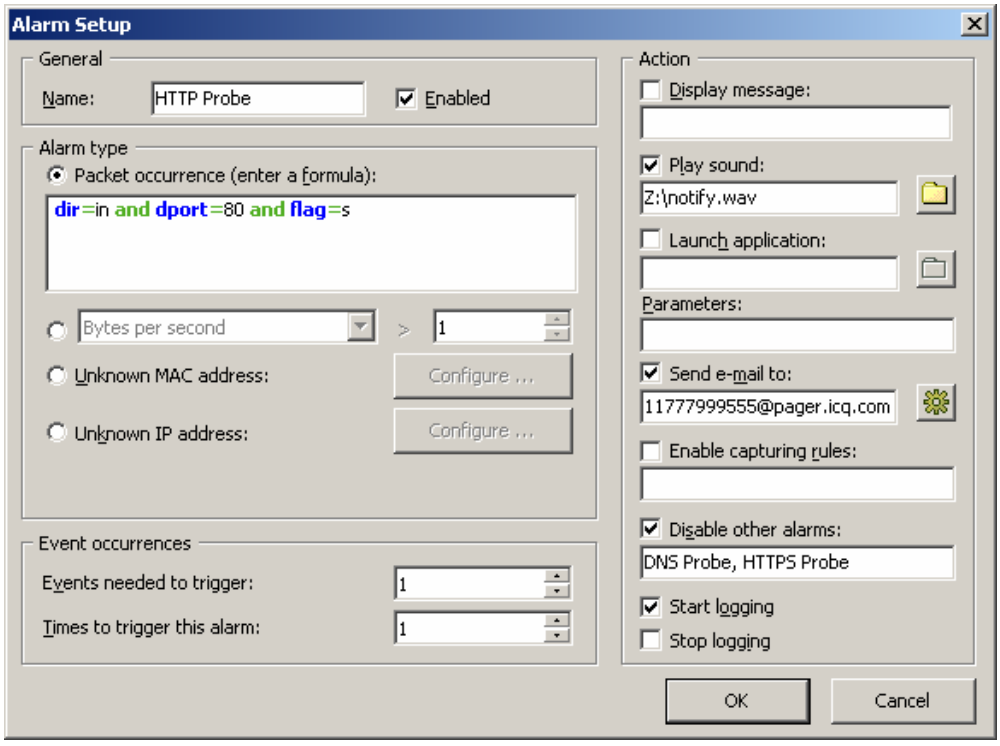
Esta pestaña le permite crear alarmas que le pueden informar sobre eventos importantes, tales como paquetes sospechosos, excesiva utilización de ancho de banda, direcciones desconocidas, etc. Las alarmas son muy útiles en situaciones donde necesite observar la red por algún evento sospechoso, por ejemplo patrones de bytes distintivos en paquetes capturados, rastreo de puertos, o conexiones de dispositivos de hardware inesperados.

Las Alarmas son administradas utilizando la lista de alarmas mostrada a continuación.



Cada línea representa una alarma distinta, y el cuadro marcado al lado de la alarma indica si la alarma esta actualmente activada. Cuando una alarma es disparada, la marca desaparece. Para reactivar una alarma desactivada, marque el cuadro próximo a su nombre. Para desactivar todas las alarmas, desmarque el cuadro **Activar Alarmas.** Para agregar una nueva alarma o edite o borre una existente, utilice los botones a la derecha de la lista de alarmas. El botón **Configurar E-mail.** Debería ser utilizado para ingresar información acerca de su servidor SMTP si planifica utilizar la opción de notificación de E-mail (vea a continuación)

La ventana de configuración de Alarma se muestra a continuación**.**



El campo **Nombre** debería ser utilizado para describir la función de la alarma. Marque el cuadro **Activado** si desea que la alarma que esta agregando/editando sea activada cuando finalice la configuración. Esta marca de cuadro es equivalente al mostrado en la lista de alarmas. El marco **Tipo de Alarma** le permite seleccionar uno de los siete tipos de alarma:

- **Ocurrencia del Paquete**: La alarma será ejecutada una vez que CommView haya capturado un paquete que coincide con la fórmula dada. La sintaxis de formula es la misma que la sintaxis utilizada en las Reglas Avanzadas y están descriptas en detalle en el capítulo Reglas Avanzadas.

- **Bytes por Segundo**: La alarma será ejecutada una vez que el número de bytes por segundo haya excedido (o caído por debajo de) el valor especificado. Advierta que debe ingresar el valor en bytes, así si desea que la alarma se ejecute cuando el ritmo de transferencia exceda 1Mbyte por segundo, el valor debería ser ingresado como 1000000.

- **Paquetes por Segundo**: la alarma será ejecutada una vez que el número paquetes ha excedido (o caído por debajo de) el valor especificado.

- **Paquetes broadcast por segundo**: La alarma será ejecutada una vez que el número de paquetes broadcast ha excedido (o caído por debajo de) el valor especificado.

- **Paquetes multicast por segundo**: La alarma será ejecutada una vez que el número de paquetes multicast haya excedido (o caído por debajo de) el valor especificado.

- **Dirección Física Desconocida**: La alarma será ejecutada una vez que CommView ha capturado un paquete con una dirección física de fuente o destino desconocida. Utilice el botón **Configurar** para ingresar las direcciones físicas conocidas. Este tipo de alarma es útil para detectar dispositivos de hardware no autorizados a conectarse a su LAN.

- **Dirección IP Desconocida**: La alarma será ejecutada una vez que CommView ha capturado un paquete con una dirección IP fuente o de destino desconocida. Utilice el botón **Configurar** para ingresar las direcciones de IP conocidas. Este tipo de alarma es útil para detectar conexiones de IP no autorizadas, mas alla del firewall corporativo.

El campo **Eventos necesarios para ejecutar** le permite especificar el número de veces que el evento esperado debe ocurrir antes de que la alarma sea ejecutada. Por ejemplo, si especifica el valor 3, la alarma no se ejecutara hasta que el evento ocurra tres veces. Si edita una alarma existente, el contador interno de eventos se restaurará.

El campo **Veces para ejecutar esta alarma** le permite especificar el número de veces que la alarma sea ejecutada antes de la desactivación. Por omisión, este valor es de 1, de tal forma que la alarma se desactivará después que el primer evento ocurre. Incrementando este valor, hará que CommView ejecute la alarma múltiples veces. Si edita una alarma existente, el contador interno de disparo se restaurará.

El cuadro de **Acción** le permite seleccionar la acción a ser realizada cuando ocurra el evento de alarma. Las siguientes opciones se encuentran disponibles:

- **Mostrar Mensaje**: Muestra un cuadro de mensajes con el texto especificado. Esta acción permite el uso de variables a ser reemplazadas por los correspondientes parámetros del paquete que ha disparado la alarma. Estas variables están enumeradas a continuación:
  %SMAC% -- Dirección física (MAC) origen.
  %DMAC% -- Dirección física (MAC) destino.
  %SIP% -- Dirección IP origen.
  %DIP% -- Dirección IP destino.
  %SPORT% -- Puerto origen.
  %DPORT% -- Puerto destino.
  %ETHERPROTO% --Protocolo Ethernet.
  %IPPROTO% --Protocolo IP.
  %SIZE% -- Tamaño de paquete.
  %FILE% -- La ruta a un archivo temporario que contiene el paquete capturado.

Por ejemplo, si su mensaje es “Paquete SYN recibido desde %SIP%", en la ventana actual que aparece el texto %SIP% será reemplazado por la dirección IP origen del paquete que disparo la alarma. Si utiliza la variable %FILE%, un archivo .NCF será creado en la carpeta temporaria. Es su responsabilidad borrar el archivo después de que ha sedo procesado; CommView no hace ningún intento de borrarlo. No debería utilizar variables si la alarma es disparada por valores de **Bytes por Segundo** o **Paquetes por segundo**, dado que estos tipos de alarmas no son disparados por paquetes individuales.

- **Reproducir Sonido**: reproduce el archivo WAV especificado.

- **Iniciar Aplicación**: Corre el EXE especificado o archivo COM. Utilice el campo opcional **Parámetros** para ingresar las opciones de línea de comando. Puede utilizar las variables descriptas en la sección **Mostrar Mensaje** de arriba como parámetros de línea de comandos si desea que su aplicación reciba y procese información acerca de paquetes que dispararon alarmas.

- **Enviar E-mail a**: Envía e-mail a la dirección especificada de e-mail. Debe configurar CommView para utilizar su servidor SMTP antes de enviar el e-mail. Utilice el botón **Configurar E-mail** al lado de la lista de alarma para ingresar su configuración de servidor SMTP y enviar un e-mail de prueba. Usualmente, un mensaje de e-mail puede ser utilizado para enviar alertas a su aplicación de mensajes instantáneos. Por ejemplo, para enviar un mensaje a un usuario ICQ, debería ingresar la dirección de e-mail como ICQ_USER_UIN@pager.icq.com, donde ICQ_USER_UIN es el número único de identificación de usuario ICQ, y permitir mensajes de EmailExpress en las opciones de ICQ. Remítase a la documentación de su aplicación de mensajes instantáneos u operador de telefonía celular para obtener mayor información. El campo **Agregar texto** puede ser usado para agregar un mensaje arbitrario a la notificación de e-mail. Puede usar las variables descritas en la sección **Mostrar mensaje** en el texto de mensaje.

- **Habilitar Reglas de Captura**: activa Reglas Avanzadas; debería ingresar el(los) nombre(s) de reglas. Si existen reglas múltiples deben ser activadas, sepárelas con comas o punto y coma.

- **Desactivar otras alarmas**: Desactiva otras alarmas; debería ingresar el(los) nombre(s) de alarma. Si alarmas múltiples deben ser desactivada, sepárelas con coma o punto y coma.

- **Iniciar Registro**: Activa el guardado automático (vea el capítulo Registro) ; CommView comenzará a volcar paquetes al disco rígido.

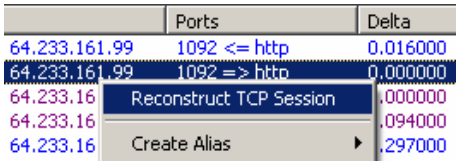
- **Detener registro**: desactiva el guardado automático.

Haga clic en **OK** para guardar sus definiciones y cerrar el cuadro de diálogo de configuración de alarma.

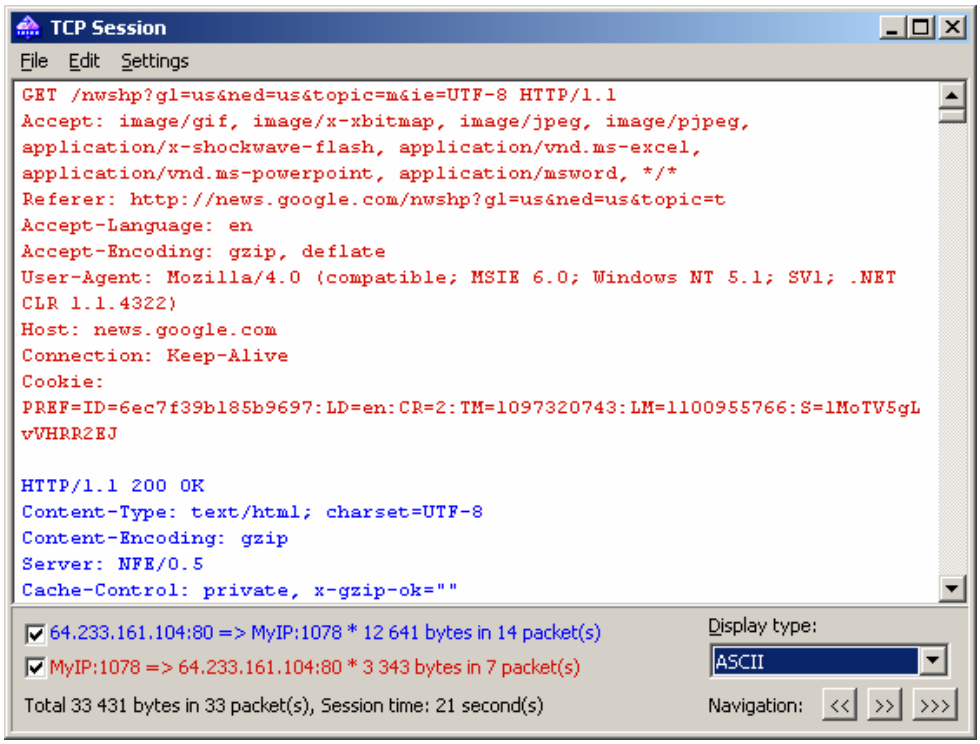
Todos los eventos y acciones relativas a las alarmas serán listados en la ventana **Registro de Eventos** debajo de la lista de alarma.

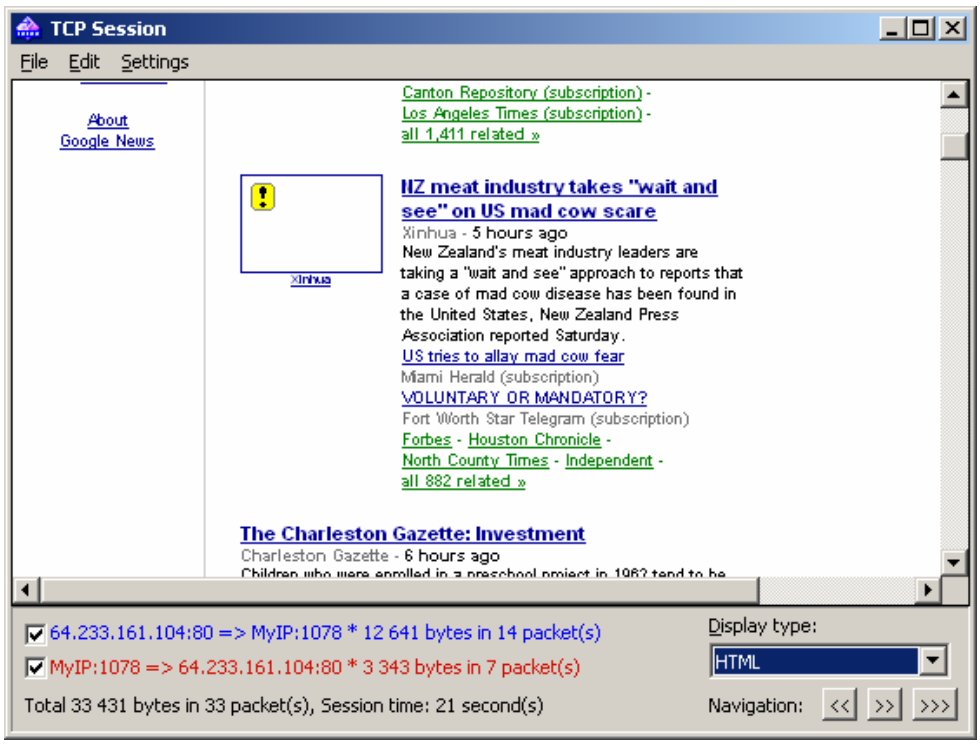
Reconstruir sesión TCP

Esta herramienta permite ver la conversación TCP entre dos Hosts. Para reconstruir una sesión debe seleccionar primero un paquete TCP en la pestaña Paquetes. Si desea reconstruir la sesión entera. Le recomendamos que seleccione el primer paquete en la sesión, de otra manera, la reconstrucción puede empezar en el medio de la "conversación". Después de ubicar y seleccionar el paquete, haga clic con el botón derecho, y seleccione **Reconstruir Sesión TCP** desde el menú de acceso directo como se muestra a continuación:

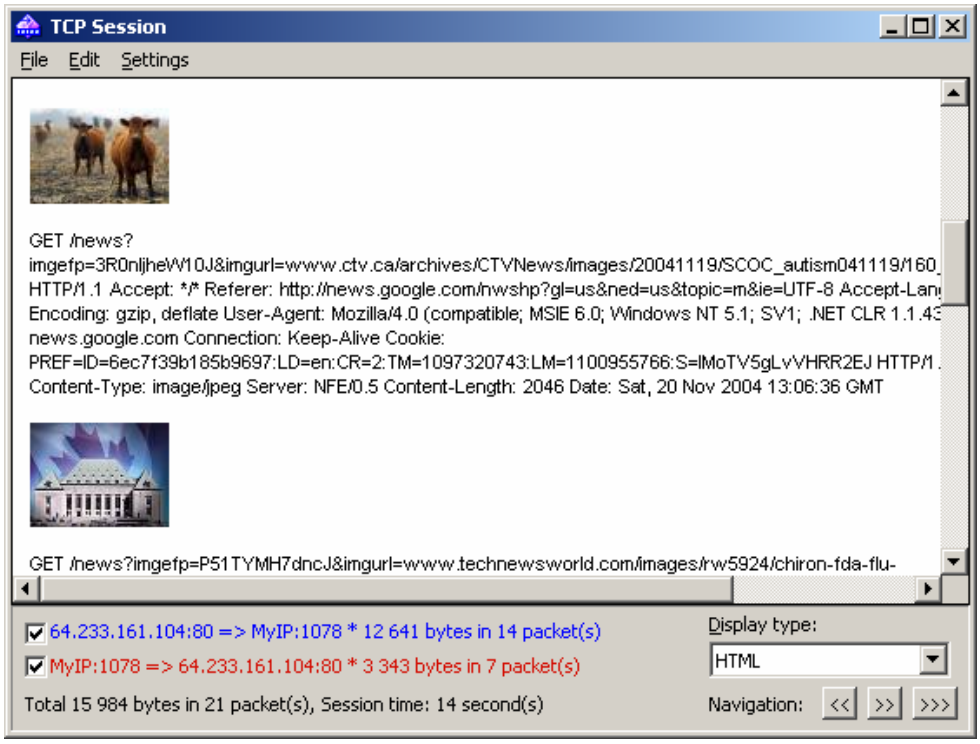


La reconstrucción de sesiones funciona mejor para protocolos basados en texto, como POP3, Telnet, o HTTP. Por supuesto, puede también reconstruir la descarga de un archivo grande comprimido, pero puede llevarle a CommView mucho tiempo reconstruir varios megabytes de datos, y la información obtenida será inútil en la mayoría de los casos. Una sesión HTTP de ejemplo que contiene datos HTML en los modos ASCII y HTML se muestra a continuación:





En modo mostrar HTML, las páginas HTML nunca incluyen gráficos interiores, dado que en el protocolo HTTP las imágenes son transferidas separadamente de los datos. Para ver las imágenes, generalmente es necesario navegar a la siguiente sesión TCP. Un ejemplo de sesión HTTP que contiene imagen de datos mostrados en modo HTML se muestra a continuación:



Por omisión, CommView intenta descomprimir contenido web GZIP y reconstruir imágenes desde cadenas de caracteres binarios. Si desea desactivar esta funcionalidad, use la pestaña **Decodificando** del cuadro de dialogo de **Opciones** del programa.

Puede filtrar los datos que vienen de una de las direcciones eliminando la marca de una de las casillas en el panel de botones. Los datos entrantes y salientes están marcados por diferentes colores para su comodidad. Si quiere cambiar uno de los colores, haga clic en **Preferencias => Colores** y elija un color diferente. Puede habilitar o deshabilitar ajuste de texto a la ventana utilizando el ítem **Ajuste de Texto a la Ventana** en el menú **Preferencias.**

El menú contextual **Mostrar Tipo** le permite ver datos en formatos **ASCII** (datos de texto plano), **HEX** (datos hexadecimales), **HTML** (Páginas web e imágenes), y **EBCDIC** (código de datos de mainframes IBM). Por favor, observe que los datos vistos como HTML no necesariamente producen exactamente el mismo resultado como aquel que puede ver en un Navegador de Internet (por ejemplo no podrá ver gráficos en línea); Sin embargo, le dará una buena idea de como se verá la pagina original.

Puede elegir el tipo de muestra por omisión para la ventana de reconstrucción de Sesión TCP en la pestaña **Decodificar** del cuadro de diálogo de **Opciones** del programa.

Los botones de **Navegación** le permiten buscar el buffer para la sesión TCP previa o siguiente. El primer botón de avance (>>) buscará por la próxima sesión entre estos dos Hosts que estaban involucrados en la primera sesión de reconstrucción. El segundo botón de avance (>>>) buscará por la siguiente sesión entre dos hosts cualquiera. Si tiene sesiones TCP múltiples entre los dos Hosts en el buffer y quiere verlas una por una, se recomienda arrancar la reconstrucción desde la primera sesión, dado que el botón de retroceso (<<) no puede navegar mas allá de la sesión TCP que fue reconstruida primero

Los datos obtenidos pueden ser guardados como archivos de datos binarios, texto, o texto enriquecido, haciendo clic en **Archivo => Guardar Como...**. También puede buscar por una cadena de caracteres haciendo clic en **Editar => Buscar...**

Estadísticas y Reportes

Esta ventana **Ver => Estadísticas** muestra estadísticas esenciales de red de su PC o segmento de LAN, tales como cantidad de paquetes por segundo, cantidad de bytes por Segundo, protocolos de Ethernet y gráficos de distribución de protocolos y subprotocolos de IP. Puede copiar cualquiera de los gráficos al portapapeles haciendo doble clic sobre el gráfico. Los gráficos de torta de protocolos Ethernet; protocolos y subprotocolos de IP pueden girarse utilizando los pequeños botones en la esquina inferior derecha para una mejor visibilidad de las porciones.

Los datos mostrados en cada página pueden ser guardados como un bitmap o un archivo de texto delimitado por comas utilizando el menú de contexto o arrastrando y soltando. La página **Reporte** le permite obtener de forma automática informes definibles generados por CommView en formatos HTML o texto delimitados por coma.

Las estadísticas de red pueden ser recolectadas utilizando tanto todos los datos que pasan a través de su adaptador de red como utilizando las reglas que estén actualmente fijadas. Si quiere solo los conteos estadísticos para procesar solo los datos (paquetes) que coinciden con el conjunto de reglas actuales e ignorar todos los otros datos, debería marcar la casilla **Aplicar reglas actuales**

General
Muestra histogramas de paquetes por segundo y Bytes/Bits por segundo, un indicador de utilización de ancho de banda (tráfico por segundo dividido por el NIC o velocidad de enlace de MODEM), así como contadores totales de Paquetes y Bytes. Haciendo doble clic sobre el indicador trae una ventana de diálogo que le permite configurar manualmente la velocidad del adaptador a ser usado en los cálculos de utilización del ancho de banda.

Protocolos
Muestra la distribución de protocolos Ethernet, tales como ARP, IP, SNAP, SPX, etc. Use el menú de contexto **Gráfico Por** para seleccionar uno de los dos métodos de cálculo disponibles: por número de paquetes o por el número de bytes

Protocolos IP
Muestra la distribución de los protocolos IP. Utilice el menú contextual **Gráfico por** para seleccionar uno de los dos métodos disponibles de cálculo: por número de paquetes o por número de bytes.

Subprotocolos IP
Muestra la distribución de los principales subprotocolos IP a nivel de aplicación: HTTP, FTP, POP3, SMTP, Telnet, NNTP, NetBIOS, HTTPS, y DNS. Para agregar más protocolos, haga clic sobre el botón **Personalizar**. Este cuadro de diálogo permite definir hasta 8 protocolos personalizados. Puede ingresar el nombre del protocolo, seleccionar el tipo de protocolo (TCP/IP), y el número de puerto.
Utilice el menú contextual **Gráfico por** para seleccionar uno de los dos métodos disponibles de cálculo: por número de paquetes o por número de bytes

Tamaño
Muestra el gráfico de distribución de tamaño de paquetes.

Hosts por Direcciones Físicas
Lista los Hosts de LAN activos por dirección física y muestra las estadísticas de transferencia de datos. Se pueden asignar alias a las direcciones físicas. Si tiene demasiados paquetes multicast sobre su red y la tabla de Hosts por dirección física esta superpoblada, puede querer agrupar las direcciones multicast en una línea que será llamada GroupedMulticast. Puede activar esta función marcando la casilla **Agrupar Direcciones multicast**. Por favor advierta que sólo los paquetes que llegan después de que la opción ha sido seleccionada serán agrupados: los paquetes recibidos previamente no serán afectados por esta opción.

Host por Direcciones IP
Lista los Hosts de LAN activos por dirección IP y muestra las estadísticas de transferencia de datos. Dado que el paquete de IP capturado por el programa puede ser originado por un número ilimitado de direcciones IP (tanto de su LAN interna como externa), por omisión esta pestaña no muestra ninguna estadística. Para tener las estadísticas desplegadas, debería primero definir el rango de direcciones IP a ser monitoreados, haciendo clic en **Agregar/Definir Rangos.** Normalmente, estos rangos deben pertenecer a su LAN, y definiéndole al programa que monitoree cierto rango de direcciones IP, le permite obtener estadísticas de utilización. Puede definir cualquier número de rangos, pero el número total de direcciones IP que se encuentran bajo monitoreo no puede exceder de 1.000. Para borrar un rango, haga clic con el botón derecho sobre la lista de rangos y seleccione el comando apropiado del menú. Usted puede asignar alias a las direcciones IP. Además, puede marcar la casilla **Todas** para hacer que el programa liste todas las direcciones IP; sin embargo esta opción no es recomendada por razones de utilización de RAM y CPU.

Matriz por Dirección Física
Esta página muestra la matriz gráfica de conversación entre hosts basados en direcciones físicas. Los hosts representados por su dirección física son colocados sobre el círculo, y las sesiones entre ellos son mostradas como líneas que conectan los hosts. Moviendo el ratón sobre un host resalta todas las conexiones que este host hace con otros hosts. Puede cambiar el número de los pares más activos de hosts que son mostrados en la matriz cambiando el valor en el campo **Pares más activos**. Para cambiar el número de los últimos pares de dirección examinados por el programa, modifique el valor en el campo **Últimos pares a contar**. Si su segmento de red tiene demasiados paquetes broadcast o multicast que sobre pueblan la matriz, puede ignorar tales paquetes marcando las casillas **Ignorar Broadcast** e **Ignorar multicast**.

Matriz por Dirección IP
Esta página muestra la matriz gráfica de conversación entre host basado en sus direcciones IP. Los host representados por sus direcciones IP son colocados sobre el círculo, y las sesiones entre ellos son mostradas como líneas que conectan los hosts. Moviendo el ratón sobre un host resalta todas las conexiones que este host hace con otros hosts. Puede cambiar el número de los pares mas activos de hosts que son mostrados en la matriz cambiando el valor en el campo **Pares más activos**. Para cambiar el

número de los últimos pares de dirección examinados por el programa, modifique el valor en el campo **Últimos pares a contar**. Si su segmento de red tiene demasiados paquetes broadcast o multicast que sobre pueblan la matriz, puede ignorar tales paquetes marcando las casillas **Ignorar Broadcast** e **Ignorar multicast**.

Errores

Muestra la información de Ehternet obtenida directamente desde el adaptador. A continuación están las explicaciones de los tipos de errores.

Rx CRS Errors
El número de frames recibidos con errores de control de redundancia circular (circular redundancy check) (CRC) o control de secuencia de frame (frame check sequense) (FCS)
Rx Alignment Errors
El número de frames recibidos con errores de alineamiento (alignment errors).
Rx Overrun
El número de frames no recibidos debido a errores de saturación sobre el NIC.
Tx One Collision
El número de frames transmitidos satisfactoriamente exactamente después de una colisión
Tx More Collisions
El número de frames transmitidos satisfactoriamente después de más de una colisión
Tx Deferred
El número de frames transmitidos satisfactoriamente después de una transmisión diferida de NIC al menos una vez.
Tx Max Collisions
El número de frames no transmitidos debido al exceso de colisiones.
Tx Underrun
El número de frames no transmitidos debido a la baja de errores sobre el NIC.
Tx Heartbeat Failure
El número de frames transmitidos satisfactoriamente sin la detección de pulsos de colisión.
Tx Times CRS Lost
El número de veces que la señal CRS se ha perdido durante la transmisión de paquetes.
Tx Late Collisions
El número de colisiones detectadas después de una ventana normal.
Rx Frames w/Errors
El número de frames que un NIC recibe, no indica a que protocolos debido a los errores.
Rx Frames w/o Errors
El número de frames que recibe un NIC sin errores e indica que están asociadas con un protocolo
Tx Frames w/Errors
El número de frames que un NIC falla al transmitir.
Tx Frames w/o Errors
El número de frames que son transmitidos sin errores.

Por favor observe que:

- No se encuentran soportados Adaptadores de acceso telefónico, solamente tarjeta de hardware de Ethernet.
- Su tarjeta puede no soportar todos los campos. Algunos fabricantes producen sus tarjetas y proveen toda la información requerida, otros no.
- A diferencia de otros datos en la ventana de Estadísticas, los datos en la pestaña de **Errores** no pueden ser reiniciados si usted hace clic en el botón de **Reiniciar**. Este contador se reinicia cuando su computadora se reinicia.
- Esta pestaña no se encuentra soportada bajo Windows 95.

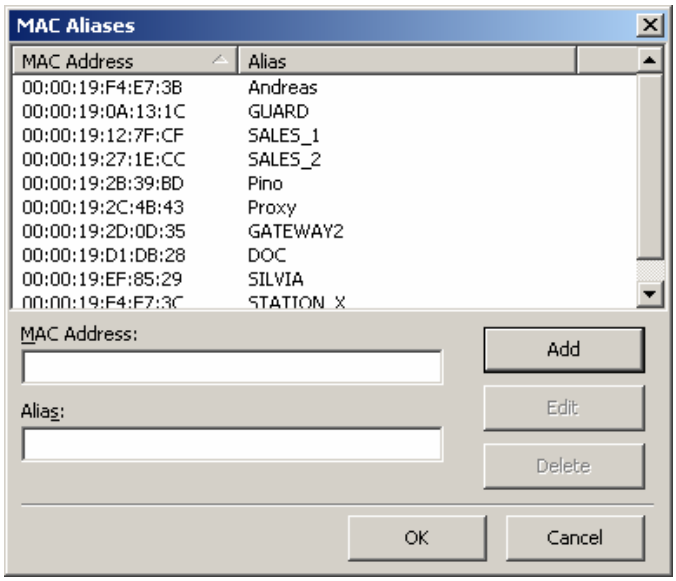
Reporte
Esta pestaña permite a CommView la generación automática de reportes definibles en formato HTML (incluyendo imágenes de gráficos) o de texto delimitados por coma.

Es posible tener al programa generando estadísticas sobre datos pre-capturados adicionalmente a las estadísticas en tiempo real. Para hacer esto, cargue un archivo capturado en Visor de Registro y haga clic en **Archivo => Generar Estadísticas.** Puede opcionalmente restaurar estadísticas recolectadas previamente mostradas en la ventana de **Estadísticas**. Por favor advierta que esta función no mostrará la distribución de paquetes a lo largo de una línea de tiempo, está limitada a mostrar totales, gráficos de protocolos, y tablas de hosts de LAN.

Utilizando Alias

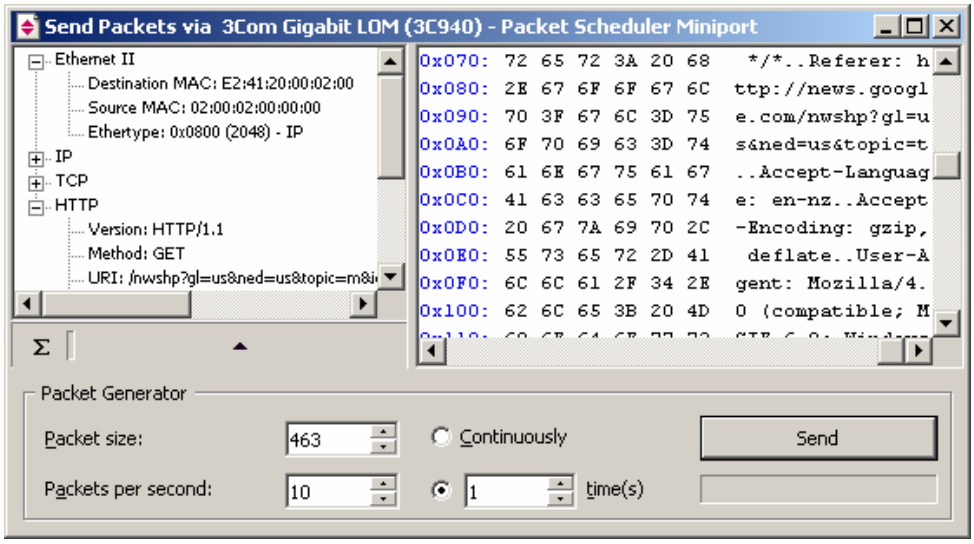
Los Alias son nombres fáciles de recordar y capaces de ser leídos por el ser humano que CommView va a sustituir por una dirección física (MAC) o dirección IP cuando se muestran los paquetes en las pestañas de Paquetes y Estadísticas. Esto permite que los paquetes sean más fáciles de reconocer y analizar. Por ejemplo, 00:00:19:2D:0D:35 se convierte en GATEWAY2, y ns1.earthlink.com se convierte en MyDNS.

Para agregar un alias de una dirección física, haga clic con el botón derecho sobre el paquete y seleccione **Crear Alias Utilizando Dirección Física de Origen** o **Utilizando la Dirección Física de Destino** desde el menú de acceso directo. Una ventana le aparecerá donde la Dirección Física ya está ingresada, y solo tiene que completar en ella el alias. Alternativamente, usted puede hacer clic sobre **Preferencias => Direcciones Físicas => Alias** y completar los campos de dirección física y Alias manualmente. Para eliminar un alias o borrar la lista de alias de forma completa, haga clic con el botón derecho sobre la ventana de alias y seleccione **Eliminar Registro o Borrar todo**. Lo mismo se aplica a la creación de alias IP.
Cuando se crea un nuevo alias IP, haciendo clic derecho sobre un paquete, el campo de alias se completa automáticamente con el nombre de Host correspondiente(si está disponible) y luego puede ser editado por el usuario.



Generador de Paquetes

Esta herramienta permite editar y enviar paquetes a través de una tarjeta de red. Se encuentra disponible solo bajo Windows 2000/XP/2003. Para abrir la herramienta del Generador de Paquetes, haga clic en **Herramientas => Generador de Paquetes**, o seleccione un paquete desde la pestaña Paquetes, haga clic con el botón derecho sobre él, y seleccione el comando **Enviar**.



Por favor advierta que el Generador de Paquetes no puede y no debería ser usado para mandar flujos TCP a niveles de aplicación, por ejemplo, este no tiene cuidado de incrementar los valores de SEQ o ACK automáticamente, ajustar checksums y tamaños de paquetes y así sucesivamente. Si necesita mandar un flujo de TCP, debería utilizar una aplicación basada en Winsock especialmente diseñada para ese propósito. El Generador de Paquetes es una herramienta para responder datos pre-capturados, probar firewalls y sistemas de detección de intrusión, así como realizar otras tareas específicas que requieren el armado manual de paquetes.

El Generador de paquetes le permite cambiar el contendido del paquete y tener el paquete decodificado mostrado en la ventana izquierda a medida que lo edita. Puede crear paquetes de cualquier tipo; tiene total control sobre el contenido del paquete. Para paquetes IP, TCP, UDP, y ICMP, puede corregir automáticamente el checksum(s) apretando el botón **sigma**.

También puede hacer clic sobre los botones con una flecha para mostrar la lista de plantillas de paquetes disponibles. El programa viene con plantillas de paquetes **TCP**, **UDP**, e **ICMP;** usarlas es mucho más rápido que ingresar los códigos Hex en la ventana de edición. Esas plantillas contienen paquetes típicos TCP, UDP, e ICMP, pero muy probablemente deseará editar varios campos de paquetes y utilizar valores significativos para cubrir sus necesidades, tales como direcciones reales físicas y de IP, número de puerto, números de SEQ y ACK, etc. Puede utilizar sus propias plantillas en lugar de las provistas. Puede arrastrar y soltar un paquete desde la pestaña de Paquetes de CommView a la sección Plantillas en la ventana del Generador de Paquetes. Si arrastra varios paquetes dentro de la sección Plantillas, sólo el primer paquete será usado como una plantilla. Una entrada llamada Nueva Plantilla aparecerá en la lista de plantillas. Puede renombrar una plantilla haciendo clic derecho sobre este en la lista y seleccionar **Renombrar**. Si necesita renombrar una plantilla, haga clic derecho sobre ésta y seleccione **Borrar** desde el menú contextual. Al seleccionar una plantilla en la lista cargará el paquete que contiene en la ventana de edición donde puede ser editado antes de enviar.

También puede colocar archivos NCF con las plantillas de su elección a la sub-carpeta TEMPLATES en la carpeta de la aplicación. Si CommView encuentra archivos NCF (o al menos uno de ellos) en la subcarpeta TEMPLATES, los listará junto con las plantillas disponibles en el menú contextual. Estos archivos NCF deberían contener sólo un paquete por archivo, pero si usa un archivo que contienen varios paquetes, CommView cargará sólo el primero.

Una vez que haya editado un paquete, utilice los controles explicados abajo para enviarlo:

Tamaño de paquete - modifica el tamaño de paquete.
Paquetes por Segundo - controla la velocidad a la cual lo paquetes son enviados. Asegúrese de no enviar los paquetes demasiado rápido si tiene una conexión lenta. Por ejemplo, si envía un paquete de 1.000 bytes 5.000 veces es más de lo que puede manejar una tarjeta de red de 10 Mbits.
Continuamente - seleccione esta opción si usted desea que el Generador de Paquetes envié paquetes de forma continua hasta que usted haga clic en **Detener**.
Veces - seleccione esta opción si quiere que el Generador de Paquetes envíe un paquete un número dado de veces.
Enviar / Detener- haga clic en este botón cuando esté listo para enviar paquetes o quiera parar de enviarlos.

Trabajando con múltiples paquetes

Puede usar el Generador de Paquetes para enviar múltiples paquetes al mismo tiempo. Para hacer esto, solo seleccione los paquetes de la lista que quiere enviar e invoque el generador de paquetes utilizando el menú de clic derecho, o arrastrar y soltar los paquetes seleccionados en la ventana del Generador de Paquetes. Alternativamente, puede arrastrar y soltar archivos capturados en todos los formatos soportados directamente desde la ventana del generador de paquetes. Cuando están enviándose múltiples paquetes, el árbol de editor de paquetes y decodificador se hacen visibles.

Guardando Paquetes editados

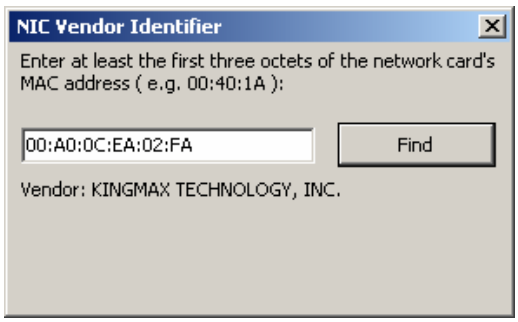
Si editó un paquete y lo desea guardar, solamente arrastre el árbol decodificador hacia el escritorio o cualquier carpeta, será creado un nuevo archivo en el formato CCF conteniendo el paquete. El nombre del archivo siempre será PACKET.NCF. También puede arrastrar el paquete a la ventana de plantillas. Si necesita editar y enviar paquetes múltiples, edítelos uno por uno, arrastrando por vez un nuevo paquete al escritorio y renombrándolo. Después, abra una nueva ventana de Visor de Registro, arrastre y suelte el paquete editado desde el escritorio al Visor de Registro, selecciónelos usando el botón de cambio, e invoque al Generador de Paquetes usando el menú de contexto.

ADVERTENCIA:

1. No utilice el Generador de Paquetes a menos que sepa exactamente que efecto desea alcanzar. El envío de paquetes puede producir resultados no previstos, y nosotros recomendados fuertemente no utilizar esta herramienta, al menos que usted sea un administrador de redes experimentado.
2. Debe encontrarse al menos otra computadora trabajando en la red además de la suya cuando utilice esta herramienta. De otra manera, experimentará demoras severas en el envío de paquetes.

Identificar el Fabricante de la Tarjeta

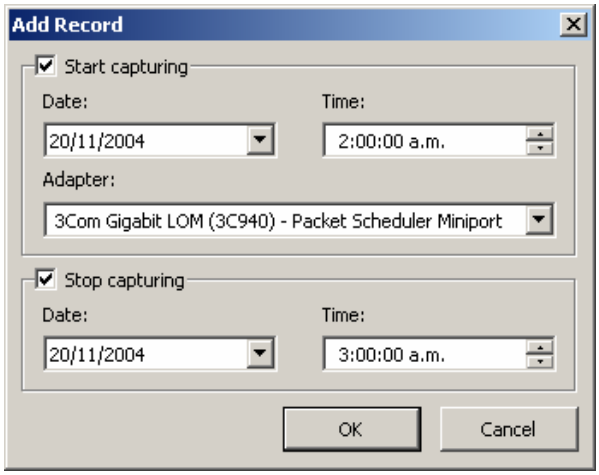
Los primeros 24 bits de la dirección física de una tarjeta de red identifican al fabricante de la misma. Este número de 24-bit es llamado OUI ("Organizationally Unique Identifier"). Identificar el Fabricante de la Tarjeta es una herramienta que permite buscar el nombre de fabricante por la dirección física. Para buscar el nombre del fabricante, haga clic en **Herramientas=> Identificar el Fabricante de la Tarjeta,** ingrese la dirección física y haga clic en **Buscar**. El nombre del fabricante será mostrado. Por omisión, CommView reemplaza los tres primeros octetos de la dirección física por el nombre del fabricante del adaptador en la pestaña **Paquetes**. Esta conducta puede ser cambiada desmarcando la casilla **Mostrar nombre de fabricante en direcciones Físicas** en la pestaña **General** del diálogo de **Opciones** del programa



La lista de fabricantes se encuentra en el archivo MACS.TXT en la carpeta de la aplicación CommView. Usted puede editar manualmente esta lista para agregar/modificar información.

Planificador

Puede utilizar esta herramienta para crear y editar una tarea de captura programada. Esto es útil cuando quiere comenzar y/o detener la captura de CommView cuando no está en la máquina, por ejemplo, a la noche o en fines de semana. Para agregar una nueva tarea, haga clic en **Herramientas => Planificador**, y luego haga clic en el botón **Agregar.**



Utilice el cuadro **Iniciar Captura** para especificar la fecha y hora de cuando CommView comenzará la captura. Utilice el menú contextual de **Adaptador** para especificar el adaptador que debería ser utilizado. Utilice el cuadro **Detener Captura** para especificar fecha y hora de cuando CommView detendrá la captura. No tiene necesariamente que marcar ambos cuadros **Iniciar Captura** y **Detener Captura**. Si sólo marca el primer cuadro, la captura continuará hasta que manualmente lo detenga. Si marca sólo el segundo cuadro, debe comenzar la captura manualmente, pero CommView automáticamente detendrá la captura en el momento especificado.

Si CommView está ya capturando paquetes al mismo tiempo que la tarea programada comienza y si el adaptador que especificó es distinto de la que está siendo monitoreada, CommView detendrá la captura, cambiará de adaptador al especificado en la tarea y reiniciará la captura.

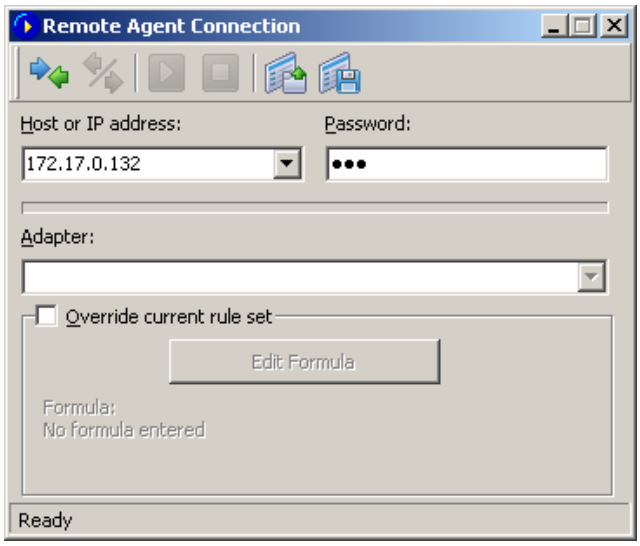
Es importante tener en cuenta que las tareas programadas solo pueden ser realizadas si CommView está corriendo.

Utilizando Remote Agent

CommView Remote Agent es un producto complementario que puede ser utilizado para monitorear tráfico de red remotamente. Todo lo que tiene que hacer es instalar Remote Agent sobre la computadora objeto, y luego usar CommView para conectarse al Remote Agent. Una vez que está conectado y autenticado, pede comenzar el monitoreo como si usted estuviera allí.

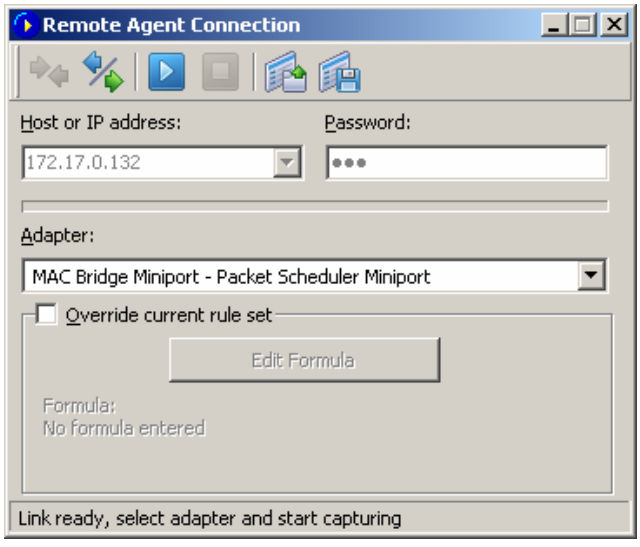
Importante: Este capítulo describe como utilizar CommView para conectarse a Remote Agent y capturar tráfico de forma remota. Para mayor información sobre la instalación de Remote Agent y su configuración, por favor consulte el archivo de ayuda que viene con Remote Agent. Es altamente recomendado que usted lea cuidadosamente la documentación de Remote Agent antes de utilizarlo. CommView Remote Agent puede descargarse de nuestro sitio.

Para cambiar al modo de monitoreo remoto, haga un clic en **Archivo => Modo de Monitoreo Remoto**. Una barra adicional aparecerá en la ventana de CommView próxima a la barra principal. Si está detrás de un firewall o servidor proxy, o utilizando un puerto no estándar de Remote Agent, puede necesitar hacer un clic en el botón **Opciones de Red Avanzadas** para cambiar el número de puerto y/o ingresar las preferencias del servidor SOCKS5.

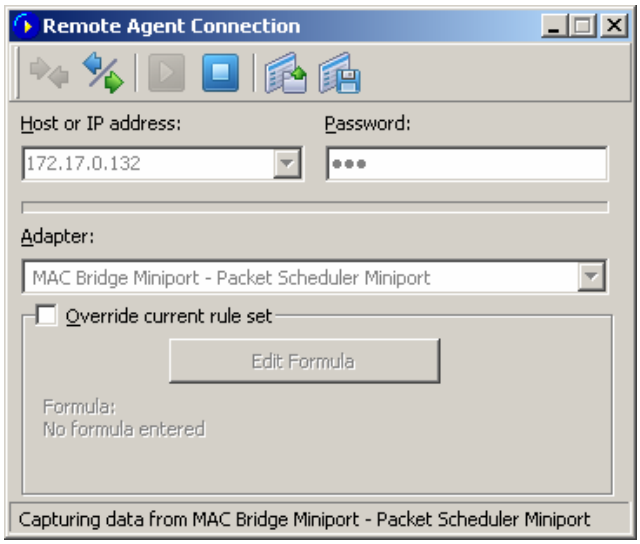


Haga clic sobre el botón **Nueva Conexión de Remote Agent** para establecer una nueva conexión, o haga clic sobre el botón de la barra de herramientas **Cargar Perfil de Remote Agent** para cargar un perfil de conexión de Remote Agent previamente guardado. Un perfil guardado previamente podría también ser cargado desde la ventana de conexión de Nuevo Remote Agent.

Aparecerá una ventana de Conexión de Remote Agent donde puede ingresar la dirección IP de la computadora que corre el Remote Agent de CommView dentro del área de ingreso de la dirección IP, ingrese la contraseña de conexión y haga clic sobre el botón **Conectar,** y si la contraseña es correcta, se establecerá una conexión. Luego verá el mensaje *Enlace Listo* en la barra de estado, y la casilla de selección de adaptador listará los adaptadores de la computadora remota.



Ahora es el mejor momento de definir las reglas de captura utilizando la pestaña **Reglas**. Es muy importante definir las reglas correctamente para que el tráfico entre el Remote Agent y CommView no exceda el límite de ancho de banda en cualquiera de los lados de la conexión, o experimentará un retraso considerable. Asegúrese de descartar los paquetes innecesarios (vea más de este tema a continuación). También puede aplicar un conjunto de reglas de captura personalizadas a esta conexión y sobrescribir las reglas actuales definidas en CommView marcando la casilla **Sobrescribir el conjunto de reglas actuales**, haciendo clic en el botón **Editar Fórmula** e ingresando la fórmula de reglas en el campo de abajo. La sintaxis de fórmula es la misma que la usada en Reglas Avanzadas. Cuando esté listo para comenzar el monitoreo, seleccione el adaptador de red de la lista y haga clic en el botón **Iniciar Captura** de la barra de herramientas. CommView le permite guardar las definiciones de Conexión de Remote Agent como un perfil de conexión para un rápido y fácil acceso en el futuro. Haga clic sobre el botón de la barra de herramientas **Guardar perfil de Remote Agent** en la ventana de Conexión de Nuevo Remote Agent e ingrese un nombre para el archivo



CommView va a comenzar a capturar el tráfico de la computadora remota como si este fuera su tráfico local; no existe virtualmente diferencia entre la utilización de CommView de forma local o remota. Cuando usted quiera finalizar el monitoreo remoto, solamente haga clic en el botón **Detener Captura** de la barra de herramientas. Luego podrá cambiar la tarjeta o desconectar con solamente hacer clic en el botón **Desconectar** de la barra de herramientas. Para volver al modo estándar, haga clic en **Archivo => Modo de Monitoreo Remoto**, y la barra adicional desaparecerá.

Por favor advierta que CommView puede trabajar con múltiples Remote Agents simultáneamente. Puede abrir varias conexiones remotas, cada una teniendo sus propias definiciones y juegos independientes de reglas y recolectar tráfico desde segmentos de red remotos en una sola ejecución de CommView.

Capturar Tráfico Loopback

CommView le permite capturar tráfico sobre la interfaz loopback. Esta funcionalidad está disponible bajo Windows 2000/XP/2003. Para iniciar el monitoreo de la interfaz loopback, selecciónelo desde el menú contextual en la barra de herramientas.

Los paquetes Loopback son los paquetes enviados/recibidos dentro de la misma computadora, por ejemplo paquetes dirigidos a si mismo. Típicamente, virtualmente no hay ningún tráfico sobre la PC estándar. Sin embargo, el tráfico loopback es ampliamente usado por desarrolladores de software para analizar aplicaciones relativas a redes. Así, la funcionalidad de capturar loopback de CommView apunta primariamente a este grupo.

Cuando captura tráfico loopback, los paquetes se ven exactamente como cualquier otro paquete de red, excepto que el checksum no está calculado. Por favor ponga atención en las siguientes peculiaridades cuando captura tráfico loopback:

- CommView captura tráfico loopback sobre todas las direcciones IP locales. Esto incluye siempre 127.0.0.1/255.0.0.0, pero puede también incluir direcciones IP de sus adaptadores Ethernet por ejemplo 192.168.0.1.
- Los paquetes ICMP no pueden ser capturados. Se pueden capturar otros protocolos IP (TCP, UDP, etc.).
- Solo los paquetes enviados/recibidos satisfactoriamente son capturados. Por ejemplo, si un intento de conexión falla debido a que el Puerto de destino está cerrado, no verá ningún paquete SYN / RST.
- Las Sesiones son cerradas silenciosamente; no son capturados paquetes FIN.

Configurando Opciones

Puede configurar alguna de las opciones de programa seleccionando en el menú **Preferencias**.

Fuentes

Utilice este ítem del menú para definir la fuente de la interfaz, el texto del paquete y el decodificador de paquete. Para cambiar los colores del texto del paquete, utilice el menú **Opciones** (a continuación).

Opciones

General

Inicio Automático de la Captura - Marque esta casilla si quiere que CommView comience a capturar paquetes inmediatamente después de iniciado el programa. Para sistemas con múltiples adaptadores, también podrá seleccionar el adaptador a ser utilizado desde el menú contextual.

Red

Deshabilitar resolución DNS - seleccione esta opción si no desea que CommView realice búsquedas DNS de las direcciones IP. Si selecciona esta opción, la columna de **Nombre de Host** en la pestaña **Últimas Conexiones IP** estará en blanco.

Convertir valores numéricos de puertos en nombres de servicios - marque esta casilla si quiere que CommView muestre nombres de servicios en lugar de números. Por ejemplo, si esta casilla esta marcado, el puerto **21** es mostrado como **ftp**, y el puerto **23** como **telnet**. El programa convierte valores numéricos a nombre de servicios utilizando el archivo SERVICES instalado por Windows. Dependiendo de su versión de Windows, el archivo SERVICES está localizado en diferentes carpetas: en Windows 95/98/Me lo puede buscar en la carpeta \Windows, y en Windows 2000/XP/2003, lo puede buscar en la carpeta \Winnt\system32\drivers\etc. Si quiere agregar más nombres de puerto o servicio puede manualmente editar este archivo.

Convertir Direcciones Físicas a alias - sustituir las direcciones físicas por los alias en la pestaña **Paquetes**. Los Alias pueden asignarse a las direcciones físicas utilizando el comando de menú **Preferencias => Alias de Direcciones Físicas**

Convertir Direcciones IP en alias - sustituir las direcciones IP por alias en las pestañas **Paquetes y Estadísticas**. pueden ser asignados Alias a las direcciones IP utilizando el comando de menú **Preferencias => Alias IP.**

Convertir Direcciones IP a Nombres de Host en la pestaña "Paquetes" – marque este cuadro si desea que CommView muestre nombres de host resueltos en lugar de direcciones IP en la pestaña **Paquetes** si el cuadro está marcado, CommView primero intentará encontrar el alias para la dirección IP dada. Si no se encuentra el alias o el cuadro anterior **Convertir Direcciones IP a Alias** no esta marcado, CommView consultará el caché interno de DNS por el nombre de host. Si no se encuentra un nombre de host, la dirección IP será mostrada en forma numérica.

Mostrar nombres de fabricantes en las direcciones físicas – por omisión, CommView reemplaza los tres primeros octetos de la dirección física por el nombre del fabricante del adaptador sobre la pestaña **Paquetes**. Desmarque esta casilla si desea cambiar esta conducta.

Utilizar modo no promiscuo - Por omisión, CommView, configura el adaptador de red en modo promiscuo, lo que significa que el programa captura todo el tráfico en el segmento local de LAN. Marcando este cuadro, cambia CommView a modo no promiscuo, el cual puede querer utilizar alguna vez, por ejemplo si la política de IT de su compañía no permite monitorear paquetes promiscuos, o para reducir la utilización de CPU, si está interesado solamente en sus propios paquetes de entrada y salida y quiere filtrar los paquetes pasantes.

Notificar cuando la lista de controladores ha cambiado – Marque este cuadro si desea que CommView muestre un globo de mensaje en el área de la bandeja del sistema una vez que el número de adaptadores de red activos ha cambiado.

Mostrar la ruta completa del proceso – marque esta casilla si desea ver el directorio completo al proceso enviar/recibir proceso en la pestaña **Últimas conexiones IP**, así como en el árbol de decodificación de paquetes en la pestaña **Paquetes** (por ejemplo. "C:\Files\Program.exe" es una ruta completa, mientras que "Program.exe" es una ruta corta).

Mostrar nombres amigables de adaptador – marcando esta opción hará que CommView muestre los nombres de adaptador en el menú contextual en la barra de herramientas como ellos aparecen en la página de Conexiones de Red de Windows.

Mostrar Líneas de Grilla – hace que el programa dibuje líneas en todas las listas de paquete.

Utilización de Memoria

Mostrar

Máximo de paquetes en el buffer - define el número máximo de paquetes que el programa almacena en la memoria y puede mostrar en la lista de paquetes (2da pestaña). Por ejemplo, si define este valor como 3000, solo los últimos 3000 paquetes serán almacenados en la memoria y mostrados en la lista de paquetes. Cuanto más alto es este valor, el programa consume más recursos de computadora.

Tenga en cuenta que si desea acceder a un gran número de paquetes, es recomendable que utilice los dispositivos de guardado automático (vea Registro para más información): Esto le permite volcar todos los paquetes a un archivo de registros sobre el disco.

Máximo de Líneas en Últimas Conexiones IP - define el número de líneas que el programa mostrara en la pestaña de Últimas conexiones IP. Cuando el número de conexiones excede el límite, las conexiones que han sido mantenidas por los más largos periodos son removidas de la lista.

Buffer del Controlador (solamente Windows 2000/XP/2003) - define el tamaño del buffer del controlador. Esta definición afecta el rendimiento del programa: a mayor memoria asignada al buffer del Controlador , el programa perderá menor cantidad de paquetes. Para LANs de poco tráfico y conexiones telefónicas, el tamaño del buffer no es critico. Para LANs de elevado tráfico, si el programa pierde paquetes, puede incrementar el tamaño del buffer para minimizar esto. Para verificar el número de paquetes perdidos, utilice el comando de menú **Archivo=> Datos de Rendimiento** cuando la captura está activada.

Últimas Conexiones IP

Lógica de Visualización - Le permite seleccionar la disposición de las Últimas Conexiones IP que mejor cubran sus necesidades. Seleccionando un ítem de la lista mostrara la descripción de la lógica seleccionada. En muchos casos es recomendable usar la lógica **Smart** por omisión.

Definir direcciones de IP locales - Debe utilizar esta herramienta si monitorea tráfico de LAN con muchos paquetes pasantes y una mezcla de direcciones IP internas y externas. En una situación como esta CommView no "sabe" que direcciones IP deben ser tratadas como locales y podría llegar a revertir las direcciones IP en las columnas Local e IP Remota. Esta herramienta permite que defina las direcciones locales de red y las máscaras de subred para asegurarse que la ventana Últimas Conexiones IP funcione correctamente. Esto funcionará si solo usa la opción por omisión lógica **Smart**.

Agregar PID numérico a nombres de procesos – marque esta casilla si desea que el ID del proceso (PID) se muestre al lado del nombre del proceso en la columna **Proceso**.

Colores

Color de los Paquetes - Define el color de los paquetes que se muestran en la pestaña de paquetes basándose sobre la dirección del paquete (entrante, saliente, pasante). Para cambiar el color, seleccione la dirección del paquete de la lista y haga clic sobre el rectángulo coloreado.

Colorear Encabezamiento de Paquetes - Marque esta casilla si desea que CommView coloree el contenido de los paquetes. Si esta casilla esta marcada, el programa muestra los ocho primeros niveles de paquete utilizando diferentes colores. Para cambiar un color, seleccione el tipo de encabezamiento para el cual desea cambiar el color y haga clic sobre el rectángulo coloreado.

Sintaxis de Formula Resaltado - define los colores para resaltar las palabras claves en las formulas en la ventana de Reglas Avanzadas.

Color de secuencia de byte seleccionada – fije el color de fuente y fondo para mostrar la secuencia de byte que fue seleccionada en el árbol decodificador. Por ejemplo, cuando selecciona el árbol de nodo "TCP", la parte correspondiente del paquete será resaltada utilizando estos colores.

Decodificando

Expandir siempre todos los nodos en la ventana del decodificador. - Marque esta casilla si quiere tener todos los nodos expandidos automáticamente en la ventana del decodificador cuando seleccione un nuevo paquete en la lista de paquetes.

Decodificar hasta el primer nivel, solamente en exportaciones de ASCII - esta opción afecta el formato de decodificación utilizado cuando exporta un archivo de registros de paquetes o un paquete individual como un archivo ASCII con decodificación. Si esta casilla esta marcada, solo los nodos de alto nivel serán guardados, por ejemplo, si guarda un paquete de TCP/IP cuando esta opción está desactivada, serán guardados todos los subnodos de *tipos de servicios,* cuando esta opción está activada esos subnodos no son guardados, marcando esta casilla, usted selecciona que el archivo de salida ASCII tenga menor detalle y por lo tanto sea más compacto.

Ignorar checksums incorrectos cuando se reconstruyen sesiones TCP - esta opción afecta la manera en que CommView trata paquetes TCP/IP malformados cuando reconstruye secciones TCP. Por omisión, esta opción está activa, los paquetes con checksums incorrectos no serán descartados en el proceso de reconstrucción. Si desactiva esta opción los paquetes con checksum

incorrectos serán descartados y no serán mostrados en la ventana de reconstrucción de TCP. Alerta para usuarios de tarjetas Gigabit: todos los paquetes salientes tendrán un checksum incorrecto si el dispositivo "checksum offload" está presente. Si desactiva esta opción, solamente vera la mitad de los conjuntos de TCP reconstruidos. Lo mismo se aplica a la reconstrucción de sesiones loopback, dado que los paquetes loopback tienen cero checksum.

Descomprimir contenido de GZIP – marque este cuadro si desea que CommView convierta contenidos HTTP comprimidos en GZIP en texto legible el la ventana de Reconstrucción de Sesión TCP. El contenido GZIP es descomprimido solo cuando el tipo de muestra en la ventana está fijado "ASCII".

Reconstruir imágenes – Marque este cuadro si desea que CommView convierta flujos binarios HTTP que representan imágenes en imágenes visibles JPG, BMP, PNG, y GIF en la ventana de Reconstrucción de Sesión TCP. Las imágenes son solamente mostradas cuando el tipo de muestra en la ventana está fijado como "HTML". Las imágenes nunca son mostradas dentro de las páginas HTML a la cual pertenecen, dado que ellas son transferidas por el servidor en una sesión HTTP separada.

Tipo de visualización por omisión – seleccione el valor de tipo de visualización desde el menú contextual que desea fijar por omisión para la función de reconstrucción de sesión TCP. Los valores disponibles son ASCII, HEX, HTML, y EBCDIC

Geolocalización

La Geolocalización es la asignación de IP-País para direcciones IP. Cuando esta funcionalidad está habilitada, CommView verifica la base de datos interna para proveer información sobre el país de cualquier dirección IP que le pertenece. Puede configurar el programa para mostrar el **Código ISO de país,** o la **Bandera de País** junto a cualquier dirección IP. También puede desactivar la geolocalización, Para algunas direcciones IP, tales como las reservadas (por ejemplo 192.168.*.* o 10.*.*.*) no puede proveerse información sobre el país. En tales casos, el nombre del país no es mostrado, o si usa la opción **Bandera de País**, se muestra una bandera con un signo de interrogación.

Dado que la asignación de IP está cambiando constantemente, es importante que siempre tenga una versión actualizada de CommView. Una Base de datos fresca y actualizada está incluida con cada modificación CommView. Una base de datos actualizada tiene un 98% de exactitud. Sin actualizaciones, los porcentajes de exactitud caen aproximadamente el 15% cada año.

Misceláneos

Ocultar desde la barra de tareas al minimizarse - Marque esta casilla si no quiere ver los botones del programa en la ventana de barra de tareas cuando minimiza el programa. Si esta casilla esta marcada, la utilización de los sistemas del programa tratan de restaurar el icono después de la minimización.

Permitir múltiples instancias de aplicación - Marque esta casilla si quiere tener múltiples instancias de CommView corriendo simultáneamente para poder capturar tráfico que está pasando por distintos adaptadores. Esta opción está ahora disponible bajo Windows 95.

Confirmar al salir de la aplicación - Marque esta casilla si quiere que el programa le pregunte por una confirmación cuando lo cierra.

Desplazamiento automático de los datos de paquetes - Si esta casilla está marcada, el programa mueve el texto de los datos del paquete cuando selecciona un nuevo paquete desde la lista de paquetes (pero solo si el texto no encuadra dentro de la ventana). Esto es útil cuando quiere ver el contenido de un paquete largo sin tener que mover manualmente la ventana.

Desplazamiento de la lista de paquetes hasta el último paquete – si este cuadro está marcado, el programa automáticamente desplaza la lista de paquetes en la pestaña **Paquetes** hasta el último paquete recibido.

Ordenar automáticamente registros nuevos en Últimas Conexiones IP - si esta casilla está marcada, el programa ordenará automáticamente los nuevos registros en la pestaña de Últimas conexiones IP basado en el criterio de ordenamiento definido por el usuario (por ejemplo, en orden ascendente de la dirección IP remota)

Control inteligente de utilización de CPU - si esta casilla está marcada, el programa trata de disminuir la utilización de CPU cuando captura altos volúmenes de tráfico disminuyendo la calidad y frecuencia de las actualizaciones de pantallas.

Ejecutar desde el arranque de Windows - si esta casilla está marcada, el programa es automáticamente iniciado cada vez que Windows se inicia.

Ejecutar minimizado - si este casilla esta marcada, el programa es iniciado minimizado y la ventana principal no es desplegada hasta que haga clic en el icono o en el botón de la barra de tareas.

Activar aplicación automática de actualizaciones – marque esta casilla para permitirle al programa conectarse al sitio Web de TamoSoft periódicamente y verificar por actualizaciones. Use la casilla **Intervalos entre verificaciones** para configurar cuan a menudo deberían realizarse las verificaciones.

Plug-ins

Esta pestaña es utilizada por Plug-Ins de terceros para realizar tareas de configuración. Por favor vea Intercambiando Datos con Su Aplicación para mayor información.

Buscar Paquete

Este cuadro de diálogo **Buscar => Buscar Paquete** le permite buscar paquetes que coincidan con un texto especificado. Ingrese una cadena de caracteres, seleccione el tipo de la información ingresada (**Cadena** o **Hex**), y haga clic en **Buscar Siguiente**. El programa va a buscar los paquetes que coincidan con el criterio de búsqueda y los mostrará en la pestaña Paquetes.

Usted puede ingresar el valor como texto, valor hexadecimal, dirección IP o MAC. Una secuencia hexadecimal debe ser utilizada cuando quiera ingresar caracteres no imprimibles: solamente ingrese valores hexadecimales separados por espacios, ejemplo. AD0A027804.

Marque **Coincidir MAY/min** para una búsqueda sensitiva de MAYÚSCULAS/minúsculas. Marque **desplazamiento** para buscar un texto que tenga un determinado desplazamiento. Observe que el indicador desplazamiento es hexadecimal y comienza en cero (ejemplo: si usted está buscando el primer byte de un paquete, el valor de desplazamiento es 0).

Información de Referencia de Puertos

Esta ventana muestra una tabla con los números de Puerto y sus correspondientes nombres de servicios. Esta referencia es obtenida desde el archivo SERVICES instalado por Windows. Dependiendo de su versión de Windows, el archivo SERVICES puede localizarse en diferentes carpetas: En Windows 95/98/Me, lo puede buscar en la carpeta **\Windows**, y en Windows 2000/XP/2003, lo puede encontrar en la carpeta **\system32\drivers\etc**. Puede editar manualmente este archivo si desea agregar más puertos/nombres de servicio. CommView lee este archivo en el inicio, por lo tanto sus cambios en el archivo se mostraran solamente cuando reinicie el programa.

Respuestas a Preguntas Frecuentes

En este capitulo, usted puede encontrar respuestas a algunas de las preguntas más frecuentes. Las últimas respuestas a las preguntas más frecuentes se encuentran disponibles en la dirección http://www.tamos.com/products/commview/faq.php.

P. ¿Puede CommView ser utilizado para capturar tráfico de adaptadores telefónicos?
R. Si, Windows 98/Me/2000/XP/2003.

P.¿Que es lo que "ve" exactamente CommView cuando está instalado en una PC conectada a una LAN?
R. CommView habilita el modo promiscuo de la tarjeta de red y puede capturar el tráfico de red en su segmento local de la LAN. En otras palabras, normalmente él mismo captura y analiza los paquetes dirigidos hacia todos los computadores en ese segmento, no solo al de la computadora que está ejecutándose. Existen ciertas limitaciones para adaptadores Wireless Ethernet (puede solo monitorear tráfico entrante/saliente) y redes switcheadas (vea la siguiente pregunta acerca de switches).

P. Estoy conectado a una LAN mediante un switch, y cuando inicio CommView, este captura solo los paquetes enviados a y desde mi maquina. No puedo ver el tráfico de otras maquinas. ¿Por qué sucede esto?
R. A diferencia de los Hubs, Los switches previenen capturas promiscuas. En un ambiente de red con swiches, CommView (u otros analizadores de paquetes) están limitados a capturar paquetes broadcast o multicast y el tráfico enviado o recibido por la PC donde CommView está corriendo. Sin embargo, los switches más modernos soportan port mirroring "espejado de puertos", el cual es un dispositivo que le permite configurar el switch para redireccionar el tráfico que pasa por alguno o todos los puertos al que sea designado puerto de monitoreo sobre el switch. Utilizando esta función, será capaz de monitorear el segmento entero de la LAN. Hemos escrito un informe técnico, Monitoreo Promiscuo en Redes Ethernet y Wi-Fi (Disponible en Inglés), que cubre estos temas en detalle

P. Bueno, Estoy conectado a la LAN a través de un Hub, pero no puedo ver tráfico de otras máquinas, de nuevo, si este no es un switch. ¿Por qué pasa esto?
R. Hay dos razones posibles: o tiene un hub que dice solo Hub, pero interiormente es un switch (algunos fabricantes como Linksys hacen esto) o tiene un hub multi-velocidad, en cuyo caso no puede ver el tráfico desde las estaciones que operan a una velocidad diferente de la velocidad de su NIC (por ejemplo si tiene una NIC de 10 Mbit, no puede ver trafico generado por NICs de 100 Mbit.

P. Tengo una LAN hogareña conectada a Internet mediante un router de banda ancha, y solo puedo ver mi propio tráfico. ¿Es posible capturar el tráfico de otras maquinas sobre mi LAN Hogareña?
A. En resumen, si. Hay algunos métodos que pueden ayudar a resolver este problema. Para más información y diseños de redes de muestra, por favor refiérase a nuestro documento, Monitoreo Promiscuo en Redes Ethernet y Wi-Fi (disponible en Inglés)

P. Puede CommView capturar datos desde una tarjeta de red que no tiene una dirección IP?
R. Sí. De hecho, una tarjeta de red no necesita estar asociada con TCP/IP o cualquier otro protocolo. En esa situación donde está tratando de solucionar problemas en la red puede ser necesario tener la capacidad de conectar la computadora ejecutándose CommView en un puerto disponible de un hub. En estos casos no necesita adivinar una dirección IP disponible en este segmento de LAN, todo lo que necesita es desasociar el adaptador de red de TCP/IP y comenzar la captura. En Windows 2000/XP/2003 abra el Panel de Control => Conexiones de Red, apriete el botón derecho en el icono de la conexión, seleccione propiedades, y desmarque los elementos correspondientes a los protocolos que usted quiere que no estén asociados con su adaptador de red. En Windows 9x Panel de Control => Red, seleccione TCP/IP => su adaptador de Red, haga clic en Eliminar, y luego reinicie.

P. Estoy sobre una LAN con alto volumen de tráfico, y es difícil examinar paquetes individuales cuando la aplicación está recibiendo cientos de miles de paquetes por segundos, dado que los paquetes viejos son rápidamente quitados del buffer circular. ¿Hay algo que pueda hacer?
R. Si, puede usar el botón **Abrir el buffer actual en ventana nueva** sobre la pequeña barra de herramientas en la pestaña **Paquetes**. Esto le permitirá hacer instantáneas del buffer actual tantas veces como desea, en cualquier intervalo. Luego podrá explorar los paquetes en esta nueva ventana a su ritmo.

P. Yo he iniciado el programa e hice clic sobre "Iniciar Captura", pero ningún paquete es mostrado. ¿Por qué?
R. Hay dos causas posibles: Seleccionó un adaptador de red que no se encuentra utilizado, o cometió un error cuando definió las reglas de captura. Desactive las reglas y vea que pasa. En cualquier caso, incluso cuando las reglas de captura están activas, la barra de estado del programa debería mostrar el número total de paquetes, por lo tanto revíselo antes de entrar en pánico.

P. He notado que el checksum de IP/TCP/UDP en los paquetes salientes es incorrecto. ¿Por qué sucede esto?.
R. Los nuevos adaptadores de red Gigabit tienen un dispositivo llamado TCP/UDP/IP "checksum offload", el cual le permite al adaptador de red calcular el checksum de los paquetes, de esta manera aumenta el rendimiento del sistema y disminuye la utilización de CPU. Dado que CommView intercepta los paquetes antes de que alcancen el adaptador de red, el checksum parece ser incorrecto. Esto es normal y la única cosa que puede estar afectada es la reconstrucción de sesiones TCP y solo si cambia la opción por omisión "Ignorar checksums incorrectos cuando se reconstruyen sesiones TCP", (para mayor información vea Opciones de Configuración).

P. CommView, ¿Corre en computadoras múlti-procesador?
R. Si, lo hace.

P. Mi conexión de red es utilizando un MODEM cable/xDSL. ¿CommView será capaz de monitorear el tráfico sobre el?
R. Si su MODEM tiene una interfaz dual USB/Ethernet y puede conectar este a la tarjeta Ethernet, CommView ciertamente capturará tráfico sobre él. Si esta tiene solo interfaz USB, lo mejor que puede hacer es tratar.

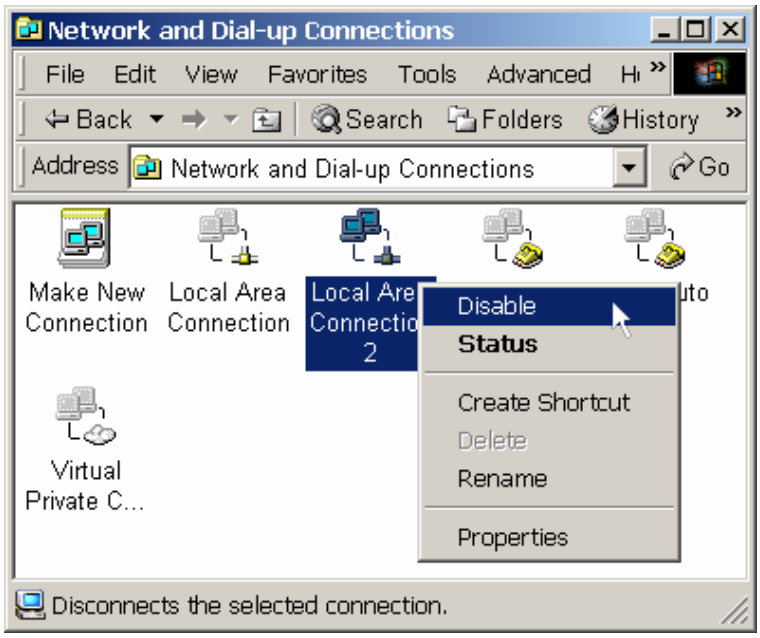
P. Mi software de firewall me alerta que CommView está "tratando de acceder a Internet" Sé que algunos sitios son capaces de rastrear usuarios recolectando la información enviada por sus programas sobre Internet. ¿Por qué CommView "intenta acceder a Internet"?

R. Dos actividades podrían estar alertando a su firewall. Primero, podría ser un intento de resolver direcciones IP en nombres de host. Dado que CommView tiene que contactar su servidor DNS para hacer una consulta DNS, este inevitablemente activará la alarma. Puede desactivar este dispositivo (Preferencias=> Opciones=> desactivar resolución DNS), pero en este caso, la pestaña de Últimas Conexiones IP no va a ser capaz de mostrar los nombres de Host. Segundo, podría tener configurado que el programa verifique si hay disponibles actualizaciones o nuevas versiones. Para hacer esto, CommView tiene que conectarse a www.tamos.com. Puede desactivar este dispositivo (Preferencias=> Opciones=> Misc. => Activar aplicación automática de actualizaciones). Estas son los dos únicos tipos de conexiones que CommView puede potencialmente hacer. No hay otras actividades ocultas. No vendemos spyware

P. Bajo Windows 2000/XP/2003 Estoy generalmente registrado como un usuario sin privilegios de administrador. ¿Tengo que cerrar la sesión y volver a iniciar la sesión como administrador para poder ejecutar CommView?

R. No, usted puede abrir la carpeta de CommView, apretar el botón derecho del mouse sobre el archivo CV.exe mientras mantiene apretada la tecla "Shift", y seleccione "Ejecutar como" desde el menú que aparece. Ingrese el usuario administrador y la contraseña en la ventana que aparece y seleccione OK para ejecutar el programa.

P. Tengo Windows 2000, y cuando desinstalo el programa, recibo el mensaje: "CommView ahora desinstalará los controladores. Haga clic en "OK" para continuar. Esto puede tomar entre 10 y 60 segundos." ¡Pero después nada ocurre!
R. Esto puede suceder si existen conexiones activas de red cuando intentaba desinstalar su programa. Usted debería deshabilitar temporalmente todas las conexiones activas como se muestra a continuación:



Tan pronto como la(s) conexión(es) se deshabiliten, CommView continuará con el proceso de desinstalación. Una vez que la desinstalación se haya completado, usted puede habilitar estas conexiones.

P. Tengo Windows 2000 Server, y CommView no me permite seleccionar ningún otro adaptador a no ser "Loopback".
R. Esto sucede si instala CommView sobre una conexión Terminal Services. La solución es simple: Reinicie el servidor, y todos los adaptadores de red estarán disponibles en la casilla de selección de adaptador de CommView.

P. Tengo Windows 2000/2003 Terminal Server, y tengo un problema corriendo CommView desde un Cliente de Terminal Services.
R.La única limitación es que el adaptador puede ser abierto por un usuario al mismo tiempo. En otras palabras, dos usuarios (locales o remotos) no pueden capturar tráfico desde el mismo adaptador mediante la ejecución de dos instancias de CommView bajo el mismo servidor.

Q. ¿Puede CommView monitorear un adaptador de red cuando corre bajo Microsoft Virtual PC?
A. Sí. La única limitación es que el modo promiscuo no está disponible para adaptadores virtuales, por lo que estará limitado a capturar sólo sus propios paquetes y los paquetes broadcast.

P. Cuando monitoreo mi conexión telefónica, no veo ningún paquete PPP durante la sesión set up (CHAP, LCP, etc). ¿Es esto normal?
R. Lo lamentamos, los paquetes de protocolo PPP solo pueden ser capturados bajo Windows 98/ME, CommView no puede capturar ese tipo de paquetes bajo Windows 2000/XP/2003. Advierta que todos los otros paquetes PPP que siguen al proceso de conexión inicial son capturados.

P. ¿Puedo intercambiar tarjetas de PC en mi notebook mientras CommView está ejecutándose?
R. No, es más seguro cerrar CommView, luego cambiar su tarjeta, y reiniciar el programa. La lista de adaptadores será actualizada automáticamente.

P. ¿Hay conflictos conocidos con otros programas?
Actualmente conocemos sobre conflictos con los siguientes programas:

- SoftIce de Numega: Puede provocar un posible colapso del sistema
- PGPNet 7.0 by NAI: Hay un conflicto de "controlador de dispositivo de bajo nivel" resultando en la pantalla azul de error fatal bajo Windows 2000 si PGPNet está contiguo al adaptador telefónico.
- Sygate Personal Firewall: Un conflicto de controlador de dispositivo resultando en la Pantalla Azul de Error Fatal bajo Windows 2000/XP si está tratando de monitorear un adaptador de discado y utilizando CommView 3.3 o anteriores. Si está monitoreando una tarjeta Ethernet , no será afectado, este problema fue solucionado en CommView 3.4.
- McAfee Personal Firewall: Posible caída del sistema. También, McAfee Personal Firewall podría nunca más asginar tráfico a apliicaciones.

Si piensa que ha descubierto un conflicto con una aplicación no listada precedentemente, estaremos muy agradecidos si nos lo informa.

P. ¿Tengo que ser profesional para utilizar este programa?
R. No. Nosotros esperamos que incluso los usuarios inexperimentados lo encuentren útil. Usted no tiene que usar todas las funciones. Por ejemplo, incluso principiantes pueden estar interesados en tener un panorama completo de las conexiones de Internet y LAN desde y hacia sus PCs, o encontrar que el programa instalado ayer era de hecho un Troyano que envía contraseñas de acceso remoto hacia ciertas direcciones de e-mail.

P. ¿Donde puedo encontrar un buen "preguntas frecuentes" sobre captura de paquetes y análisis de protocolos?
R. Revise estos sitios:

Sniffing (network wiretap, sniffer) Preguntas Frecuentes

Protocols.com

Guía de CommView

Temas Avanzados

Captura de un volumen elevado de tráfico

Cuando realiza una captura de datos en un segmento de una red, de gran tamaño, sujeto a una gran utilización, debe tener en cuenta que el procesamiento de miles de paquetes por segundo pueden incrementar considerablemente el uso del procesador y hacer que la aplicación pierda capacidad de respuesta. La mejor forma de lograr un mejor desempeño es mediante la utilización de reglas para el filtrado de paquetes que no necesiten ser monitoreados. Por ejemplo, el envío de un archivo de 50 Megabytes entre dos maquinas en una LAN puede generar aproximadamente alrededor de 40.000 paquetes de NetBIOS con una velocidad de transferencia de datos del orden de 1 Megabyte por segundo, lo cual puede ser una carga muy grande para una aplicación. Pero normalmente no necesita ver cada paquete de NETBIOS que se esté enviando, con lo cual usted puede configurar CommView para capturar solamente paquetes de IP. CommView posee un sistema flexible de filtros, que puede seleccionar para que la aplicación muestre solamente los paquetes que realmente necesita. A su vez, si está interesado solo en la información estadística (histogramas verdes, gráficos de torta, y tablas de hosts), puede utilizar el comando del menú “Suspender salida de paquetes”, que le permite tener datos estadísticos sin la muestra de los paquetes en tiempo real.

Los factores que mejoran el desempeño de la aplicación son:

- Un Procesador rápido (Pentium IV recomendado)
- Cantidad de Memoria (128 o superior recomendado)
- Un sistema operativo basado en tecnología NT (Windows 2000/XP/2003 recomendado)
- La utilización de reglas para descartar el tráfico innecesario.

Trabajando con Múltiples Instancias

CommView puede capturar paquetes desde diferentes adaptadores de red simultáneamente. Esta función se activa cuando marca **Permitir múltiples instancias de la aplicación en (Preferencias => Opciones => Misc.)**. Por favor observe que no puede abrir el mismo adaptador en dos instancias diferentes del programa. Esta limitación también se aplica a Terminal Server: dos usuarios (local o remoto) no pueden capturar tráfico del mismo adaptador mediante la ejecución de dos instancias de CommView en el mismo servidor.

Ejecutando CommView en Modo Oculto

Existen dos formas de ejecutar CommView como un proceso oculto:

1. Inicie CommView con el parámetro de oculto:

   CV.EXE hidden

2. Si CommView se encuentra ejecutando, puede ocultar/mostrar la aplicación utilizando esta combinación de teclas: Para ocultar la aplicación, presione ALT+SHIFT+h. para mostrar la aplicación, presione ALT+SHIFT+u.

Recuerde que no puede ocultar completamente cualquier aplicación de Windows. Cuando se ejecuta en modo invisible, CommView no se muestra en la lista de tareas (la cual es invocada presionando ALT+CTRL+Supr) bajo Windows 98/ME, pero uno puede aun ver la aplicación si usa cualquier aplicación que liste los procesos que se encuentran ejecutándose. Bajo Windows 2000/XP/2003 esta herramienta es parte del Administrador de Tareas.

Parámetros de Línea de Comandos

Puede utilizar parámetros en la línea de comandos para realizar las siguientes operaciones cuando el programa está siendo iniciado:

- Cargar y activar un conjunto de reglas desde un archivo. Utilice el indicador "/ruleset" seguido del nombre y el paso de archivo completo, por ejemplo:

  CV.EXE /ruleset "C:\Program Files\CommView\Rules\POP3Rules.rls"

  Si un nombre de archivo o un paso contienen espacios, este debe ser enmarcado entre comillas (“ ”).

- Abrir un adaptador y comenzar captura. Utilice el indicador "/adapter" seguido por el nombre del adaptador, por ejemplo:

  CV.EXE /adapter "Intel(R) PRO/1000 T Desktop Adapter"

  El nombre del adaptador debe ser enmarcado entre comillas (" "). Dado que los nombres de adaptador son típicamente largos, puede querer copiar el nombre del adaptador desde el cuadro de selección de adaptadores del programa en lugar de escribirlos. Para copiar el nombre del adaptador, seleccione el adaptador en el cuadro de selección de adaptador y presione Ctrl-C.

- Use la carpeta especificada para almacenar archivos de registro. Use el parámetro /logdir seguido por el directorio completo de la carpeta, por ejemplo:

  CV.EXE /logdir "C:\Archivos de Programas\CommView\Logs"

Puede utilizar todos estos parámetros simultáneamente.

Intercambiando datos con su aplicación

CommView provee una interfaz TCP/IP simple que le permite procesar paquetes capturados por CommView usando su propia aplicación en tiempo real. Comenzando con la versión 5.0 también puede usar esta interfaz para enviar paquetes (similar a la función de Generador de Paquete en CommView).

Por favor advierta que el formato ha cambiado comparado con las versiones previas de CommView. El parámetro TS también ha sido eliminado dado que toda la información acerca del paquete incluyendo el horario es enviado ahora en el encabezamiento.

Cómo Funciona
Debe iniciar CommView con un parámetro especial de línea de comando, "MIRROR" diciéndole al programa que espeje los paquetes capturados hacia una dirección IP y el puerto TCP de su elección.

Ejemplos:
CV.EXE mirror:127.0.0.1:5555 // espeja los paquetes a la dirección loopback, puerto TCP 5555
CV.EXE mirror:192.169.0.2:10200 // espeja los paquetes a la dirección 192.169.0.2, TCP puerto 10200

Cuando CommView es iniciado como un parámetro como ese, el mismo trata de establecer una sesión TCP de conexión a la dirección IP y el número de Puerto especificado. Esto significa que ya debería tener funcionando su aplicación y escuchando en el puerto especificado. Si CommView falla en establecer la conexión, seguirá intentando conectarse cada 15 segundos. Lo mismo sucede si la conexión se rompe: CommView va a tratar de restablecerla cada 15 segundos. Si la conexión se establece satisfactoriamente, CommView envía los paquetes que captura hacia la dirección IP establecida a medida que arriben en tiempo real.

Formato de Datos

Los datos son transmitidos en formato NCF. Por favor refiérase al capítulo Formato de Archivos de registro de CommView para la descripción del formato

Enviar Paquetes

Los paquetes pueden no sólo ser recibidos por su aplicación, sino también enviar como si estuviera usando el Generador de Paquetes. Los datos pueden ser enviados a CommView usando la misma conexión TCP sobre la cual está recibiendo datos. El formato de datos es simple: Debería enviar el largo del paquete (un entero sin signo de dos bytes en el orden de byte little-endian estándar) seguido por el paquete en sí. Si el adaptador no es abierto o no soporta inyección de paquete, el paquete es desechado silenciosamente

Proyectos de Ejemplo
Dos aplicaciones sencillas para demostración, que escuchan conexiones entrantes, extraen paquetes del flujo y muestran los datos sin procesar, están disponibles en:

- http://www.tamos.com/products/commview/samp_mirr_c5.zip. Este es un proyecto de Visual Studio cuyo código fuente es C++
- http://www.tamos.com/products/commview/samp_mirr_d5.zip. Este es un proyecto de Delphi cuyo código fuente es Pascal. Si usted desea compilar el proyecto. Va a necesitar la suite popular de componentes ICSI desarrollados por François Piette disponibles en http://overbyte.be

Ancho de banda
Cuando esté espejando datos a una computadora remota, asegúrese que el vínculo entre CommView y la otra computadora a la cual los datos se envían sea lo suficiente rápido para transferir los datos que están siendo capturados. Si CommView captura 500 Kbytes/sec, y su vínculo solo puede manipular 50 Kbytes/sec, inevitablemente tendrá "embotellamientos de tráfico", que puede resultar en varios problemas (ejemplo, Winsock puede parar de enviar datos bajo algunas versiones de Windows). Si usted está buscando una solución más flexible esa será la función de smart buffering (Utilización del buffer de forma inteligente) y remote control (Control Remoto), considere utilizar CommView Remote Agent.

Decodificación Personalizada

CommView le permite dos tipos de sus decodificadores personalizados.

Decodificador Simple

Si implementa este tipo de decodificador, la salida de su decodificador será mostrada en una columna adicional en la pestaña **Paquetes**. Su decodificador debe ser un archivo DLL de 32-bit llamado "Custom.dll" que exporta solamente el procedimiento llamado "Decode". El prototipo de este procedimiento es mostrado abajo en C y Pascal:

```
extern "C" {
  void __stdcall Decode(unsigned char *PacketData, int PacketLen, char *Buffer, int BufferLen);
}

procedure Decode (PacketData: PChar; PacketLen: integer; Buffer: PChar; BufferLen: integer); stdcall;
```

La DLL debe estar localizada en la carpeta de la aplicación CommView. Cuando se inicia CommView, este busca por "Custom.dll" en la carpeta de la aplicación y lo carga en la memoria. Si la entrada "Decode" se encuentra, CommView agrega una nueva columna llamada "Custom" a la lista de paquetes.

Cuando un nuevo paquete es capturado y va a ser mostrado, CommView llama al procedimiento "Decode" y pasa el contenido del paquete a la DLL. El procedimiento "Decode" debe procesar los datos del paquete y copiar el resultado en el buffer suministrado. El primer argumento es el puntero a los datos del paquete, el segundo argumento es la longitud de los datos, el tercer argumento es el puntero al buffer donde los resultados de su decodificación deben ser copiados, y el cuarto argumento es el tamaño del buffer (actualmente siempre es de 1024 bytes). El buffer es fijado y liberado por CommView, por lo tanto no trate de reasignarlo o liberarlo. El resultado que copió al buffer es mostrado como una cadena de caracteres en la columna "Custom".

Su procedimiento debe ser lo suficientemente rápido para manejar cientos de paquetes por Segundo.; de otra manera este podría demorar la aplicación. No olvide utilizar la convención de llamadas STDCALL.

Dos DLLs de muestra se encuentran disponibles. Ellas muestran una muy simple operación: la salida de la función de "Decode" es el código hex del último byte del paquete. Su decodificador puede ser tan complejo como desee.

- http://www.tamos.com/products/commview/cust_decoder_c.zip. Este es un proyecto de Visual Studio con código fuente de C++.
- http://www.tamos.com/products/commview/cust_decoder_d.zip. Este es un proyecto Delphi con código fuente Pascal.

Decodificador Complejo

Si implementa este tipo de decodificador, la salida de su decodificador será mostrada como ítems adicionales en el árbol de decodificador de paquetes. Para más información sobre este decodificador, por favor descargue el siguiente archivo:

http://www.tamos.com/products/commview/complex_decoder_c6.zip

Este tipo de decodificador puede ser escrito en Microsoft Visual C++ solamente, dado que este esta construido usando C++ classes.

Soporte Técnico

El soporte técnico para decodificadores personalizados se provee en la base “del mejor esfuerzo”. Puede ser que no podamos responder sus preguntas relacionadas a programación.

Formato de Archivos de Registro de CommView

CommView y CommView para WiFi usa el formato de datos descrito abajo para escribir paquetes capturados a archivos .NCF. Este es un formato de datos abierto que puede ser usado para procesar archivos de registro generados por CommView en sus aplicaciones, así como para intercambiar datos directamente con sus aplicaciones (este método es descrito en este archivo de ayuda).

Los paquetes son grabados consecutivamente. Un encabezado de 24 bytes (la estructura del cual es mostrada abajo) precede cada cuerpo de paquete. Todos los campos de encabezado con una longitud que exceda 1 byte usa orden de byte little-endian.

<table>
<tr><th>Nombre del Campo</th><th>Longitud (bytes)</th><th>Descripción</th></tr>
<tr><td>Longitud de Datos</td><td>2</td><td>La longitud del cuerpo del paquete que sigue el encabezado</td></tr>
<tr><td>Longitud de datos fuente</td><td>2</td><td>La longitud original del cuerpo del paquete que sigue al encabezado (sin compresión). Si la compresión no es usada, el valor de este campo es igual al valor del campo previo.</td></tr>
<tr><td>Versión</td><td>1</td><td>Versión de formato de paquete (0 para la implementación actual)</td></tr>
<tr><td>Año</td><td>2</td><td>Fecha del paquete (año)</td></tr>
<tr><td>Mes</td><td>1</td><td>Fecha del paquete (mes)</td></tr>
<tr><td>Día</td><td>1</td><td>Fecha del paquete (día)</td></tr>
<tr><td>Horas</td><td>1</td><td>Horario del paquete (horas)</td></tr>
<tr><td>Minutos</td><td>1</td><td>Horario del paquete (minutos)</td></tr>
<tr><td>Segundos</td><td>1</td><td>Horario del paquete (segundos)</td></tr>
<tr><td>Microsegundos</td><td>4</td><td>Horario del paquete (microsegundos)</td></tr>
<tr><td>Indicadores</td><td>1</td><td>Bit de Indicadores:
<table>
<tr><td>Medio</td><td>0...3</td><td>Tipo de medio para el paquete (0 - Ethernet, 1 - WiFi, 2 - Token Ring)</td></tr>
<tr><td>Desencriptado</td><td>4</td><td>El paquete ha sido desencriptado (aplicable sólo a paquetes WiFi)</td></tr>
<tr><td>Roto</td><td>5</td><td>El paquete estaba corrupto, por ejemplo tiene incorrecto el valor de CRC (aplicable sólo a paquetes WiFi)</td></tr>
<tr><td>Comprimido</td><td>6</td><td>El paquete es almacenado en forma comprimida</td></tr>
<tr><td>Reservado</td><td>7</td><td>Reservado</td></tr>
</table></td></tr>
<tr><td>Nivel de Señal</td><td>1</td><td>Nivel de señal en porcentaje (aplicable sólo a paquetes WiFi)</td></tr>
<tr><td>Tasa</td><td>1</td><td>Tasa de transmisión de la fecha en Mbps multiplicado por 2 (aplicable sólo a paquetes WiFi)</td></tr>
<tr><td>Banda</td><td>1</td><td>Banda de transmisión. 0x01 para 802.11a, 0x02 para 802.11b, 0x04 para 802.11g, 0x08 para 802.11a-turbo, 0x10 para 802.11 SuperG. (aplicable sólo a paquetes WiFi)</td></tr>
<tr><td>Canal</td><td>1</td><td>Número de canal (aplicable sólo a paquetes WiFi)</td></tr>
<tr><td>Dirección</td><td>1</td><td>Dirección del paquete. 0x00 para pasantes, 0x01 para entrantes, 0x02 para salientes (no aplicable a paquetes WiFi)</td></tr>
<tr><td>Reservado</td><td>2</td><td>Reservado</td></tr>
<tr><td>Datos</td><td>...</td><td>Cuerpo del paquete (sin modificar, como fueron transmitidos sobre el medio). Si la marca de compresión está fijada, los datos están comprimidos usando la librería públicamente disponible Zlib 1.1.4. la longitud de este campo está grabada en Longitud de Datos.</td></tr>
</table>

La longitud del encabezado es de 24 bytes.
Si los paquetes son almacenados en forma comprimida, el campo de Longitud de Datos contiene la longitud de datos después de la compresión, mientras que el campo Longitud de Fuente contiene la longitud original de datos. Si el paquete está sin comprimir, ambos campos contienen el mismo valor.

Información

Como Adquirir CommView

Este programa es una evaluación de 30 días. A continuación está el precio de la versión completamente funcional, irrestricta del programa:

Tipo de licencia	Precio, US$
CommView Enterprise License 1 usuario (para uso comercial & profesional)	499.00
CommView Home License 1 usuario (para uso privado, no comercial)	99.00

- La licencia más costosa **Enterprise License** le da derecho a la utilización de programa en cualquier lugar para propósitos comerciales y no comerciales

- La licencia menos costosa **Home License** le da derecho a la utilización del programa en su hogar para propósitos no comerciales. Si usted utiliza CommView para el monitoreo de su red hogareña, el número máximo de hosts en su LAN que puede monitorear con esta licencia no puede exceder diez. La Home license no le permitiría conectar a CommView Remote Agents. La Home license no le permitiría capturar tráfico loopback.

Una copia licenciada de CommView puede ser utilizada por una sola persona quien utilice el software personalmente en una o más computadoras , o puede ser instalada en una sola computadora utilizándose de forma no-simultanea por más de una persona, pero no ambas. Verifique nuestro sitio web para el precio de licencias multi-usuario si necesita comprar el producto para más de un usuario.

Como un usuario registrado, usted recibirá:

- Una copia irrestricta, totalmente funcional de este software.
- Actualizaciones gratuitas por el plazo de 1 año a partir de la fecha de compra del producto.
- Información sobre actualizaciones y nuevos productos
- Soporte Técnico Gratuito

Nosotros aceptamos tarjetas de crédito, ordenes por teléfono y fax, cheques, ordenes de compra y giros telegráficos. Los precios, términos y condiciones están sujeto a cambio sin previo aviso: Por favor visite nuestro sitio para ver los últimos productos que ofrecemos y los precios.

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

Contáctenos

Web

http://www.tamos.com

E-mail

sales@tamos.com (Preguntas relacionadas con ventas)
support@tamos.com (Otras preguntas)

Correo y Fax

Dirección Postal:

PO Box 1385
Christchurch 8140
New Zealand

Fax: +64 3 359 0392 (Nueva Zelanda)
Fax: +1 917 591-6567 (EEUU)

Otros productos por TamoSoft

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

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

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.

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.

Mas 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.

Mas 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.

Mas información