CommView®
For WiFi

Monitor y Analizador de Redes inalámbricas para MS Windows

Documentación de Ayuda

Introducción

Acerca de CommView for WiFi

CommView for WiFi es una edición especial de CommView diseñado para capturar y analizar paquetes de red sobre redes inalámbricas 802.11a/b/g. CommView for WiFi recoge información del adaptador inalámbrico y decodifica los datos analizados.

Con CommView for WiFi puede ver la lista de conexiones de red y estadísticas vitales de IP y examinar paquetes individuales. Los paquetes son decodificados utilizando claves WEP o WPA-PSK definidas por el usuario y 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 for WiFi posee decodificación completa de los siguientes protocolos: 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.

CommView es una herramienta valiosa para administradores de WLAN, profesionales de seguridad, programadores de redes, o cualquiera que quiera tener una visión completa de su tráfico WLAN. Esta aplicación funciona bajo Windows 2000/XP/2003 y requiere un adaptador de red inalámbrica compatible. Para la lista de adaptadores soportados, por favor visite nuestro Sitio Web.

Novedades

Versión 5.4

- Suporte para CommView Remote Agent para WiFi.

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.
- Colorización de Marcos de Administración dependiendo de su tipo
- Alarmas mejoradas le permiten fácilmente detectar estaciones Ad Hoc y enviar e-mails de alerta personalizables.
- Soporte para adaptadores Intel PRO/Wireless 2200BG y 2915ABG (versión beta).
- Soporte para nuevos canales 802.11a en el dominio regulatorio JP.
- Ventana de “Estadísticas” modificable en tamaño.
- Diálogo de “Encontrar” mejorado.
- Líneas de grillas opcionales para una mejor visibilidad de paquetes.

Otras mejoras menores.

Versión 5.2

- Filtros rápidos que le permiten crear fácilmente nuevas vistas de paquetes para paquetes similares basado en direcciones físicas (MAC), direcciones IP, o puertos.
- Identificación de tipo de codificación.
- Una nueva herramienta de Reasociación de Nodo que puede ayudarlo a re-iniciar intercambio de clave WPA-PSK.
- Soporte para nuevos canales Europeos 802.11a.
- Lista de proveedores MAC actualizada.
- Es soportado un nuevo adaptador: TRENDnet TEW-501PC.
- Aplicación automática de actualizaciones.

Muchas otras mejoras.

Versión 5.1

- Varios nuevos adaptadores ahora están soportados: 3Com OfficeConnect Wireless a/b/g PC Card (3CRWE154A72), D-Link AirPlus G DWL-G630 Wireless Cardbus Adapter (Rev. C), D-Link AirPremier DWL-AG530 Wireless PCI Adapter, NETGEAR WG511U Double 108 Mbps Wireless PC Card.
- El controlador ha sido actualizado para asegurar compatibilidad con las últimas versiones de un número de adaptadores D-Link.
- Han sido solucionados problemas menores relativos a capturar archivos de Importación/Exportación y decodificación de protocolo

Versión 5.0

- Exploración pro-activa usando paquetes PROBE REQUEST (requiere un adaptador basados en el conjunto de chips Atheros).
- Ahora está disponible el Generador de Paquetes (requiere un adaptador basados en el conjunto de chips Atheros).
- Nuevas reglas avanzadas que permite a usuario filytar paquetes basados en tipos de marcos, subtipos de marcos, reintentos, duración, etc.
- Estampado de tiempo de alta precisión (hasta microsegundos).
- Nuevo formato 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.
- Los informes HTML pueden incluir gráficos.
- Nuevos tipos de alarmas.
- Menor uso de CPU.

Versión 4.2

- Las nuevas Pestañas Nodos y Canales le brindan estadísticas detalladas por nodo y por canal: Tasa de transferencia de datos, fuerza de señal, errores ICV y CRC, etc.
- Decodificación al vuelo de paquetes codificados WPA en modo de Claves Pre Compartidas (Pre-Shared Key (PSK)). Esta es una función exclusiva no disponible en ningún otro analizador de red inalámbrica.
- Mejoras importantes de rendimiento que le permiten monitorear una WLAN fuertemente utilizada y decodificar tráfico al vuelo sin usar el 100% del tiempo de CPU.

- Una alarma de detección de AP corrupto ha sido agregada.

Las nuevas versiones de los controladores ofrecen estabilidad mejorada

Versión 4.1

- El programa ahora soporta adaptadores inalámbricos 802.11g y 802.11a.
- Funcionalidad de exploración mejorada.
- El programa puede registrar URLs. visitadas.
- Nuevos módulos de decodificación de protocolos han sido agregados: IMAP, NNTP, SSH, TLS.
- Una interfaz de plug-in abierta 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).
- Puede tener el programa generando estadísticas sobre datos precapturados adicionalmente a estadísticas en tiempo real.
- La funcionalidades de alarma mejoradas le permiten pasar variables a aplicaciones arrancadas o mensajes de alarma.
- Otras mejoras menores.

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. 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.

Actualizaciones
Este Acuerdo no le concede ningún derecho para ninguna mejora, actualizaciones, o versiones nuevas para este software (colectivamente, “Actualizaciones”). TamoSoft puede o no, a su sola determinación, ofrecer tales actualizaciones a usuarios licenciados. TamoSoft no garantiza que tales actualizaciones estarán disponibles, o que tales actualizaciones ofrecerán cualquier mejora en compatibilidad con los últimos estándares de la industria, incluyendo, pero no limitándose a, nuevos dispositivos de Hardware, protocolos de red, o algoritmos de codificación.

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
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.

Utilización del Programa

Instalación del Controlador

CommView for WiFi es una herramienta para monitorear redes inalámbricas 802.11a/b/g. para usar este producto, **debe** tener un adaptador inalámbrico compatible. Para activar las funciones de monitoreo de su adaptador inalámbrico. Necesita usar el controlador especial que viene con el producto. Dependiendo del modelo de adaptador y sistema operativo, el controlador provisto funcionará en uno de los siguientes modos:

- **Modo Dual (Conectividad + Monitoreo):** Cuando CommView for WiFi no está funcionando, su adaptador podrá comunicarse con otros hosts inalámbricos o puntos de acceso, igual que cuando está usando el controlador original provisto por el fabricante del adaptador. Cuando CommView for WiFi está funcionando, su adaptador será puesto en modo de monitoreo pasivo y promiscuo.
- **Modo de Solo Monitoreo:** Su adaptador será usado solo para monitoreo. No podrá usarlo para comunicarse con otros hosts inalámbricos o puntos de acceso. Para restablecer las funciones estándar de su adaptador, debería volver al controlador original del adaptador provisto por el fabricante.

Para usar el adaptador en modo dual, debe estar usando Windows XP, su adaptador debe ser un adaptador 802.11b/g o 802.11a/b/g (no funcionará con los viejos adaptadores 802.11b), y debe desinstalar cualquier utilitario de configuración de adaptador provisto por el fabricante y permitir que Windows use el utilitario incorporado de configuración inalámbrica. Si no se cumplen estas condiciones, está disponible el modo de solo monitoreo.

Antes de instalar el nuevo controlador para su adaptador inalámbrico, asegúrese que su adaptador es compatible con el producto. La lista de adaptadores compatibles puede encontrarse en la siguiente URL:

http://www.tamos.com/products/commwifi/

CommView for WiFi podría soportar otros adaptadores. Si su adaptador no está listado arriba, por favor refiérase al capítulo Preguntas Frecuentes para información actualizada.

Para instrucciones de instalación de controlador detalladas e ilustradas, por favor inicie el programa, pulse **Ayuda => Guía de Instalación de Dispositivos** en el menú del programa, y muévase hasta la parte inferior de la ventana.

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, haga clic en el botón **Iniciar Captura** o seleccione **Archivo => Iniciar Captura** en el menú.

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 4ta pestaña.
Guardar Nodo Como – le permite guardar el contenido de la pestaña Nodos.
Guardar las Últimas Conexiones IP Como – le permite guardar el contenido de la pestaña Últimas Conexiones IP.
Guardar Registro de Paquetes como – Le permite guardar el contenido de la pestaña de Paquetes. Utilice la pestaña de registros para las opciones avanzadas de guardar.
Visor de Registros – Abre una nueva ventana de Visor de registro.
Borrar Nodos – Borra la tabla de Nodos (1ra pestaña).
Borrar Canales – Borra la tabla de Canales (2da pestaña).
Borrar Últimas Conexiones IP – Borra la tabla de Últimas Conexiones IP (3ra pestaña).
Borrar Buffer de Paquetes – Borra el contenido del buffer del programa y la lista de paquetes en la 4da pestaña
Datos de Rendimiento –Muestra las estadísticas de rendimiento del programa: El número de paquetes capturados y perdidos por el controlador de dispositivo.
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.
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 Nodos – Muestra/oculta las pestañas de columnas de Nodos.
Columnas de Canales – Muestra/oculta las pestañas de columnas de Canales.
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.
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.
Reasociación de Nodo – Abre la ventana de Reasociación de Nodo

Preferencias

Fuentes – Muestra el submenú para fijar los caracteres fuente de los elementos de la interfaz.
Claves WEP/WPA – abre una ventana que le permite ingresar Claves WEP/WPA.
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 for WiFi 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.

Reglas

Capturar Paquetes de Datos – marque o desmarque este ítem para activar/desactivar la captura de paquetes del tipo “Datos.”
Capturar Paquetes de Administración – – marque o desmarque este ítem para activar/desactivar la captura de paquetes del tipo "Administración."
Capturar Paquetes de Control – – marque o desmarque este ítem para activar/desactivar la captura de paquetes del tipo "Control."
Ignorar Balizas - – marque o desmarque este ítem para activar/desactivar la captara de paquetes del tipo "Balizas."
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 de Instalación de Controlador ... – Muestra instrucciones de instalación de controlador detalladas.
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 for 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 puntos de acceso y estaciones activos. para más información vea Nodos

La segunda pestaña es usada para mostrar las estadísticas por canal. Para más información vea Canales

La tercera pestaña es usada para mostrar información detallada acerca de las conexiones de red WLAN (solo protocolos IP). Para mayor información vea Últimas Conexiones IP.

La cuarta 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 quinta pestaña le permite guardar los paquetes capturados en archivos. Para mayor información vea Registro.

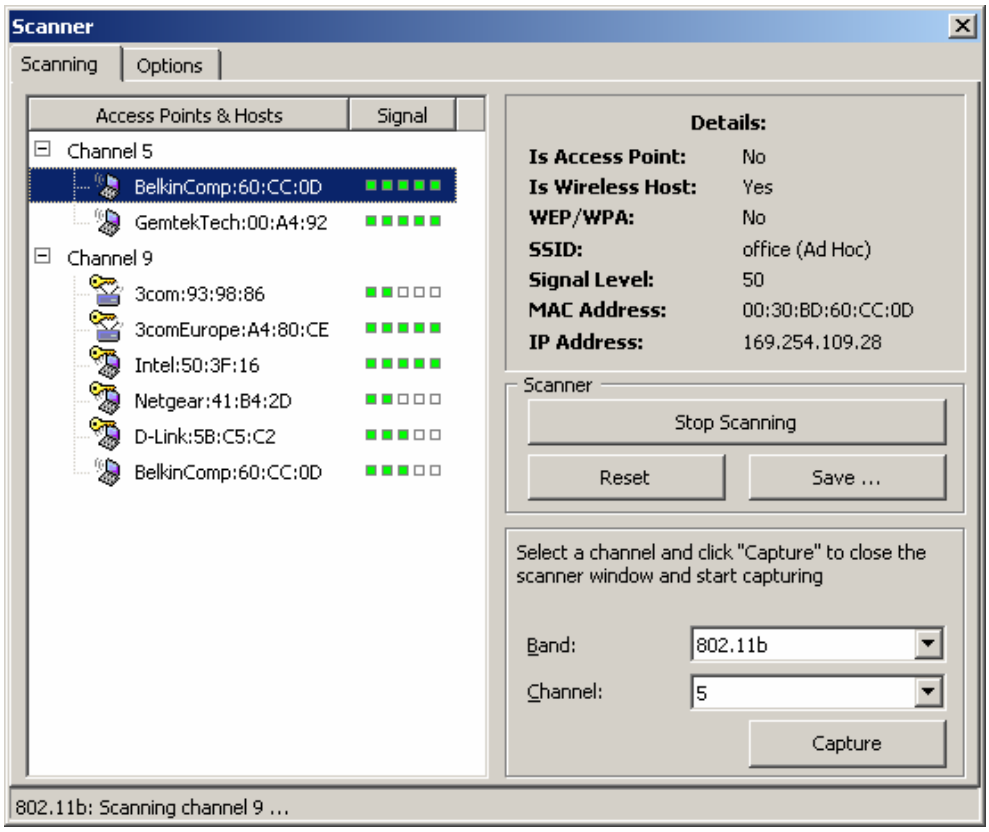
La sexta pestaña es para configurar reglas que le permiten capturar/ignorar paquetes basándose en diferentes criterios, tales como la dirección IP o el número de Puerto, para mayor información vea Reglas.

La séptima 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.

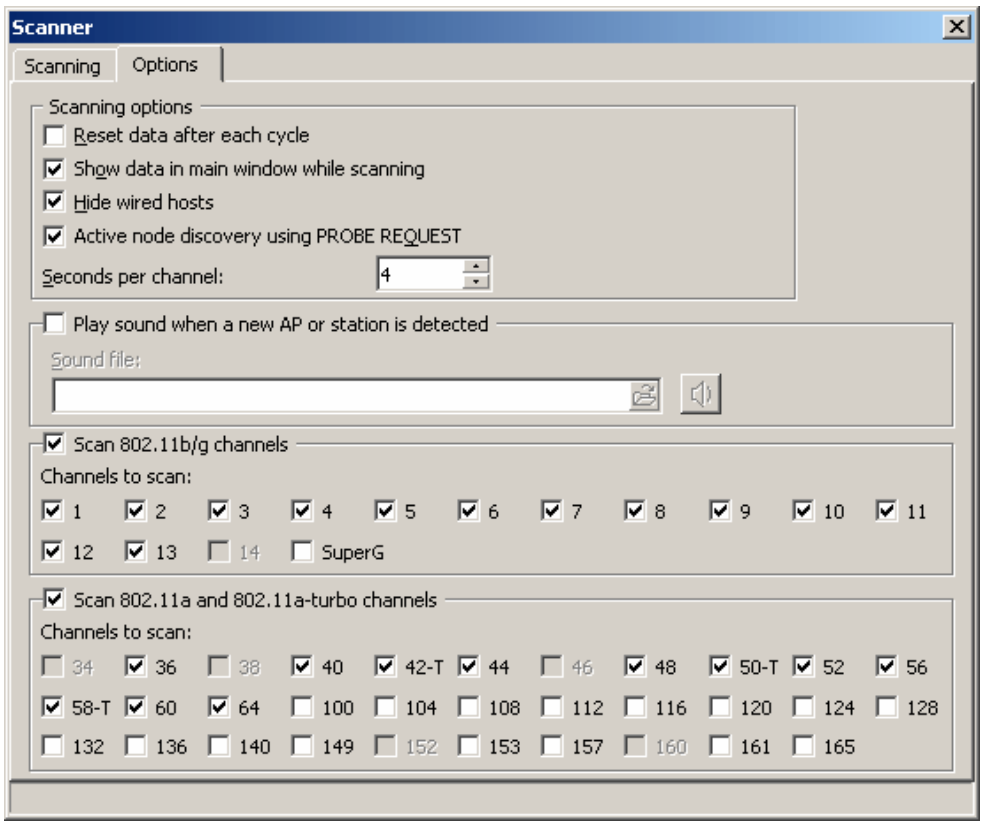
Usted puede cambiar algunas de las preferencias, como fuentes, colores, y tamaño de buffer seleccionando **Preferencias** desde el menú. Para más información vea Preferencias Opciones.

Explorador

La ventana Explorador le permite explorar el aire por señales WiFi y seleccionar un canal para monitorear. Para comenzar a escanear, simplemente pulse el botón **Iniciar Exploración**. El proceso de exploración es cíclico, por ejemplo, el programa "escuchará" por señales en el primer canal, luego cambiará al canal siguiente, y así sucesivamente, hasta que alcance al último canal, luego del cual comienza un nuevo ciclo de exploración. El proceso de exploración no se detendrá hasta que sea pulsado **Detener Exploración**. Para limpiar los datos que han sido recogidos, pulse **Restaurar**. Para guardar el informe de exploración en formato HTML, pulse **Guardar**. Cuando haya finalizado con el exploración y/o si conoce el canal sobre el cual desea que el programa capture paquetes, seleccione una banda de la lista desplegada **Banda** (dependiendo de su adaptador, la lista podría contener hasta tres bandas distintas: 802.11a, 802.11a-turbo, y 802.11b/g), luego seleccione un canal de la lista desplegada **Canal** y pulse **Capturar**.



La pestaña **Opciones** le permite configurar un número de opciones de exploración. Las siguientes opciones de exploración están disponibles:



Restaurar datos después de cada ciclo – marque esta casilla si desea que el programa limpie los datos que ha recolectado antes de comenzar un nuevo ciclo de exploración. Esta opción tiene ventajas y desventajas. La ventaja es que restaurando los datos le dará un panorama más actualice del éter. Por ejemplo, si una determinada estación no envía más datos, no aparecerá de nuevo en la lista. Sin embargo, la desventaja es que si una determinada estación no envía datos activamente, por ejemplo lo hace unas pocas veces por minuto, el explorador podría no "reconocer" a la estación cada vez que escanea un determinado canal. Es más, esta estación será quitada de la lista.

Mostrar datos en la ventana principal mientras escanea – marque esta casilla si desea que el programa muestre los paquetes que están siendo capturados durante el exploración en la ventana principal del programa (en las pestañas **Nodos, Canales, Paquetes** y **Últimas Conexiones IP**). Si esta casilla no está marcada, los paquetes que son capturados mientras el explorador está funcionando no serán mostrados o registrados en ningún lado.

Ocultar Hosts Conectados – Marque esta casilla si desea que el programa muestre solamente hosts inalámbricos y puntos de acceso. Si esta casilla no está marcada, el explorador mostrará tanto hosts inalámbricos como conectados en el segmento a ser escaneado. Advierta que activando esta opción podría a veces ocultar incluso hosts inalámbricos, dado que el programa necesita capturar varios paquetes de datos para determinar si un host es inalámbrico o está conectado.

Descubrir nodo Activo usando PROBE REQUEST – si esta casilla está marcada, el programa envía periódicamente paquetes PROBE REQUEST. Tales paquetes facilitan el descubrimiento de aquellos Puntos de Acceso que no emiten sus SSID. Advierta que usando esta opción podría hacer que el adaptador transmita paquetes, por lo que dejará de ser completamente sigiloso. Está opción no está disponible para las Viejas tarjetas 802.11b.

Segundos por canal – determina el intervalo de tiempo que el explorador escuchará por datos en cada canal que está siendo escaneado.

Ejecutar sonido cuando un nuevo PA o estación es detectado – Marque esta casilla y seleccione un archivo WAV si desea que el programa le notifique acerca de puntos de acceso o estaciones son encontradas. Puede probar el archivo WAV seleccionado pulsando el botón junto al campo de selección de archivo.

Escanear canales 802.11b/g y **Escanear Canales 802.11a** –Estas casillas le permiten seleccionar los canales a ser escaneados. Necesita seleccionar al menos un canal. Dependiendo de su país, su adaptador de red inalámbrica podría no soportar todos los canales mostrados en la ventana. Si un canal no está soportado por su adaptador, la casilla correspondiente estará Griseado. Lo mismo se aplica a marcos de **Escanear Canales 802.11a**: estarán griseados si su adaptador no soporta 802.11a. Si su adaptador no soporta 802.11g, el marco **Escanear Canales 802.11b/g** estará nombrado **Escanear Canales 802.11b**.

Dependiendo del país y el dominio regulatorio fijado en su adaptador, la lista de canales soportados podría variar. Esto es discutido en detalle en el capítulo Preguntas Frecuentes.

Acerca de SuperG y SuperAG

SuperG/SuperAG es una tecnología de mejora propietaria introducida por Atheros Communications y soportada por varios proveedores de hardware (visite www.super-ag.com para más información). SuperG/SuperAG usa quiebre de paquetes, "marcos rápidos," compresión/descompresión en el aire, y unión dual de canales para proveer mejoras de salida hasta 108 Mbps. Dependiendo del hardware usado, su WLAN podría trabajar parcial o completamente en modo SuperG/SuperAG. El Hardware activado SuperG- y SuperAG funciona típicamente en varios modos: Modo Súper Sin Turbo, Modo Súper con Turbo Estático, y Modo Súper con Turbo Dinámico.

En la banda 802.11g, la transmisión en modo Súper con Turbo Estático y Modo Súper con Turbo Dinámico es realizado sobre el canal 6 de 802.11g. Sin embargo, CommView for WiFi podría ser incapaz de capturar el tráfico inalámbrico si selecciona el canal 6 de 802.11g para monitorear. Esto es porque tiene la opción de seleccionar SuperG para monitorear, en cuyo caso CommView for WiFi podrá capturar este tipo especial de marcos. Advierta que el hardware podría cambiar dinámicamente, dependiendo de la carga de red y otros factores, lo que hace problemático el monitoreo.

En la banda 802.11a, la transmisión de datos en modo Súper con Turbo Estático y Modo Súper con Turbo Dinámico es realizado sobre canales turbo especiales. Si su adaptador usado para monitoreo soporta el modo turbo 802.11a, simplemente seleccione la banda y canal adecuados en la lista desplegada. Este modo usa un conjunto de canales separados, por ejemplo los canales 42, 50, y 58 son generalmente canales turbo, mientras que otros canales 802.11a son no turbo. Hay excepciones a esta regla; por ejemplo, en Japón, los canales 34, 38, 42, y 46 son canales no turbo. Para poder monitorear esos canales en Japón, es necesario construir un controlador específico de país. Puede contactarnos si necesita tal controlador para Japón o cualquier otro país con conjunto de canales no estándar.

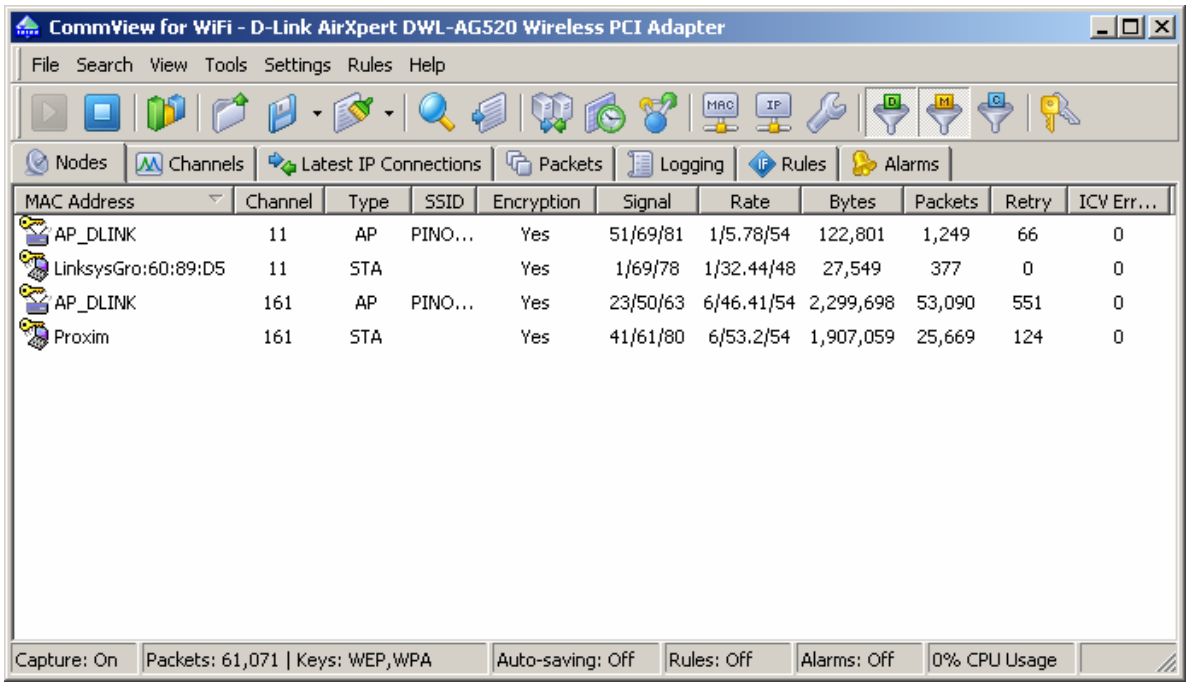
IMPORTANTE: Debido a que SuperG/SuperAG es una tecnología propietaria y no estándar, no podemos dar ninguna garantía de la capacidad de nuestro producto para capturar, decodificar, y descifrar los paquetes que están siendo transmitidos en el modo SuperG/SuperAG.

Diferencias Entre la Ventana de Explorador y la Pestaña de Nodos

Mientras que la ventana de Explorador se parece a la pestaña **Nodos** de la ventana principal de la aplicación, hay una diferencia importante entre ellas. El Explorador es una cómoda herramienta para una evaluación de sitio rápida y la detección de puntos de acceso y estaciones. No provee estadísticas detalladas por nodo y podría incluir incluso host no inalámbricos (si la casilla **Ocultar Hosts Conectados** no está marcada), para brindarle una mejor comprensión de la topología de la red.

Nodos

Esta pestaña es usada para mostrar información detallada sobre los nodos inalámbricos activos, por ejemplo los puntos de acceso y estaciones asociadas que transmite datos sobre el(los) canal(es) que están monitoreándose. Una vez que haya seleccionado un canal para monitorear usando el Explorador, El programa comenzará a poblar esta tabla con nodos inalámbricos detectados. El mecanismo de análisis de paquetes empleados en el programa listará los puntos de acceso encontrados sobre el canal dado, estaciones en modo ad hoc, así como las estaciones asociadas en modo infraestructura. Aquellas estaciones que no están asociadas y no envían datos no serán listadas.



Es importante comprender que el radio usado en un adaptador inalámbrico puede recibir datos solo sobre un canal a la vez. Por lo tanto, cuando ha seleccionado un determinado canal para monitorear, esta tabla contendrá datos sobre los PAs y estaciones que transmiten datos solo sobre el canal seleccionado. Puede, sin embargo, seleccionar un canal distinto y reiniciar la captura en cualquier momento sin restaurar datos e la tabla, o incluso dejar que el Explorador barra entre los canales para que pueda ver los nodos activos en distintos canales (asegúrese de marcar la casilla **Mostrar datos en la ventana principal mientras escanea** en las opciones de Explorador si desea que la pestaña Nodos Se pueble mientras escanea).

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

Dirección Física (MAC) – La direcciones físicas (MAC) y/o alias de los puntos de acceso y estaciones. El ícono junto a la dirección física (MAC) representa el tipo de nodo. Una casilla con dos antenas es un punto de acceso, mientras que una computadora portátil representa una estación en modo infraestructura o ad hoc La llave dorada es mostrada cuando está usándose cifrado de datos.
Canal – El canal sobre la cual determinada PA o estación está transmitiendo datos.
Tipo – tipo de nodo. Los valores posibles son AP (para puntos de acceso),STA (para estaciones en modo infraestructura) y AD HOC (para estaciones en modo ad hoc).
SSID – Conjunto Identificador de Servicio (Service Set Identifier), una serie única que diferencia una WLAN de otra.
Cifrado – Muestra si el nodo está usando cifrado WEP o WPA. Para puntos de acceso esta columna muestra los métodos de cifrado disponibles que están siendo "anunciados" por el punto de acceso.
Señal – nivel de señal en el formato mín/promedio/máx. El valor promedio es calculado desde que los datos fueron restaurados por última vez en la tabla.
Ritmo – Ritmo de transferencia de datos en el formato mín/promedio/máx. El valor promedio es calculado desde que los datos fueron restaurados por última vez en la tabla.
Bytes –el número de bytes enviados y recibidos por el nodo.
Paquetes – el número de paquetes enviados y recibidos por el nodo.
Reintentos – El número de paquetes donde el indicador de Reintento estaba presente.
Errores ICV – El número de paquetes con errores ICV. Vea Comprendiendo Errores CRC e ICV para una explicación detallada.

Puede mostrar u ocultar columnas individuales pulsando botón derecho sobre la lista de encabezados o usando el menú **Ver** => **Columnas de Nodos**. El orden de las columnas puede ser cambiado arrastrando el encabezado de la columna a su nueva ubicación.

Comandos de Menú

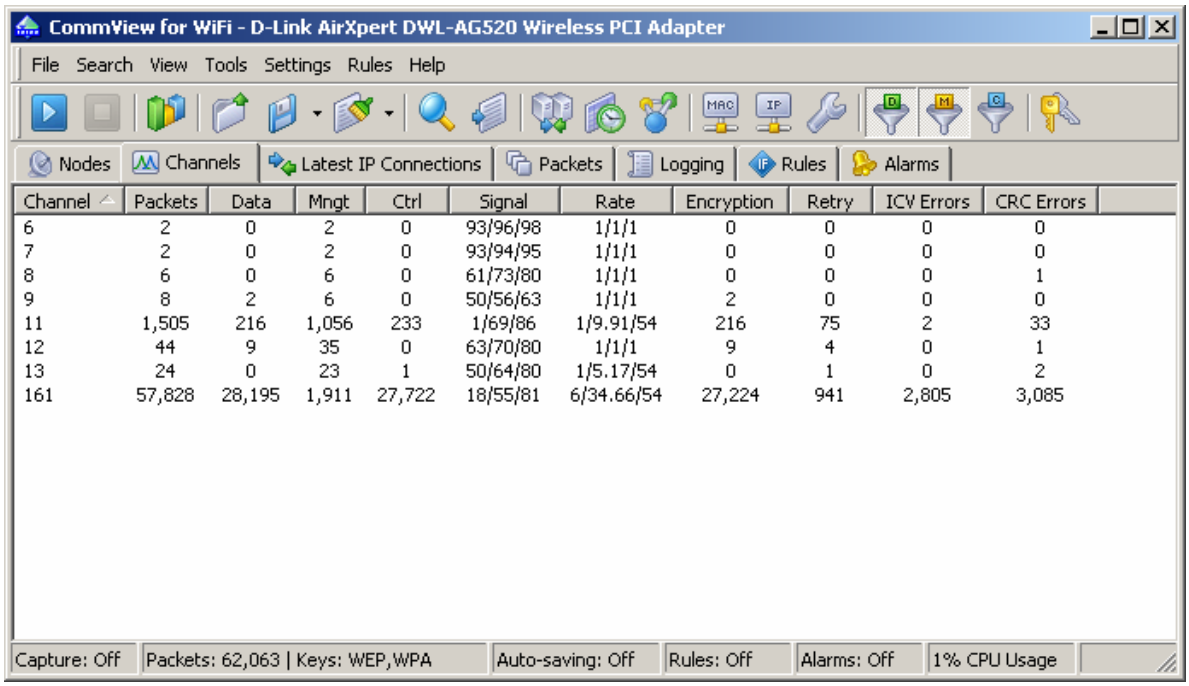
Haciendo Clic sobre la lista Últimas Conexiones IP trae un menú con los siguientes comandos:

Copiar Dirección Física (MAC) – copia la dirección IP local, la dirección IP remota, o el nombre de host al portapapeles.

Crear Alias – Abre una ventana donde puede asignar un alias fácil de recordar para la dirección física (MAC) seleccionada.
Guardar Nodos Como – le permite guardar el contenido de la pestaña Nodos como un informe HTML.
Limpiar Nodos – Limpia la tabla.
Más Estadísticas – muestra una ventana con Estadísticas de transferencia de datos y distribución de protocolos.

Canales

Esta pestaña muestra estadísticas por canal que han sido o están monitoreándose. El número de canales mostrados en esta pestaña depende de la forma en que usa CommView for WiFi. Normalmente, cuando monitorea un solo canal usado por su WLAN, la tabla contendrá datos solo sobre el canal seleccionado, dado que la radio usada en un adaptador inalámbrico puede recibir datos de solo un canal por vez. Una vez que haya seleccionado un canal distinto para monitorear, otro canal será agregado a la tabla. Alternativamente, si usa el Explorador para barrer entre los canales y la casilla **Mostrar datos en la ventana principal mientras escanea** está marcada en las opciones de Explorador, la tabla contendrá datos sobre todos los canales escaneados para el cual al menos un paquete ha sido capturado. Esto a veces es un método conveniente de relevar un sitio.



Channel	Packets	Data	Mngt	Ctrl	Signal	Rate	Encryption	Retry	ICV Errors	CRC Errors
6	2	0	2	0	93/96/98	1/1/1	0	0	0	0
7	2	0	2	0	93/94/95	1/1/1	0	0	0	0
8	6	0	6	0	61/73/80	1/1/1	0	0	0	1
9	8	2	6	0	50/56/63	1/1/1	2	0	0	0
11	1,505	216	1,056	233	1/69/86	1/9.91/54	216	75	2	33
12	44	9	35	0	63/70/80	1/1/1	9	4	0	1
13	24	0	23	1	50/64/80	1/5.17/54	0	1	0	2
161	57,828	28,195	1,911	27,722	18/55/81	6/34.66/54	27,224	941	2,805	3,085

Dado que el estándar 802.11b/g usa solapamiento de frecuencias de canal, puede advertir que incluso si su WLAN está configurada para usar solo un canal, por ejemplo el 6, seguirá viendo valores distintos de cero para los canales adyacentes. A diferencia de los canales 802.11b/g, los canales 802.11a no se superponen.

El significado de las columnas de las tablas está explicado a continuación:

Canal – El número de canal.
Paquetes – El número total de paquetes transmitidos (Datos + Administración + Control).
Datos – El número de paquete de Datos transmitidos.
Admin – El número de paquetes de Administración transmitidos.
Ctrl – El número de los paquetes de Control transmitidos.
Señal – El nivel de señal en el formato mín/promedio/máx. El valor promedio es calculado desde que los datos fueron restaurados por última vez en la tabla.
Ritmo – Ritmo de transferencia de datos en el formato mín/promedio/máx. El valor promedio es calculado desde que los datos fueron restaurados por última vez en la tabla.
Cifrado – el número de paquetes de Datos para los cuales el indicador de cifrado estaba presente.
Reintentos – El número de paquetes donde el indicador de Reintento estaba presente.
Errores ICV – El número de paquetes con errores ICV. Vea Comprendiendo Errores CRC e ICV para una explicación detallada
Errores CRC – El número de paquetes con errores CRC. Vea Comprendiendo Errores CRC e ICV para una explicación detallada.

Puede mostrar u ocultar columnas individuales pulsando botón derecho sobre la lista de encabezados o usando el menú **Ver** => **Columnas de Canales**. El orden de las columnas puede ser cambiado arrastrando el encabezado de la columna a su nueva ubicación.

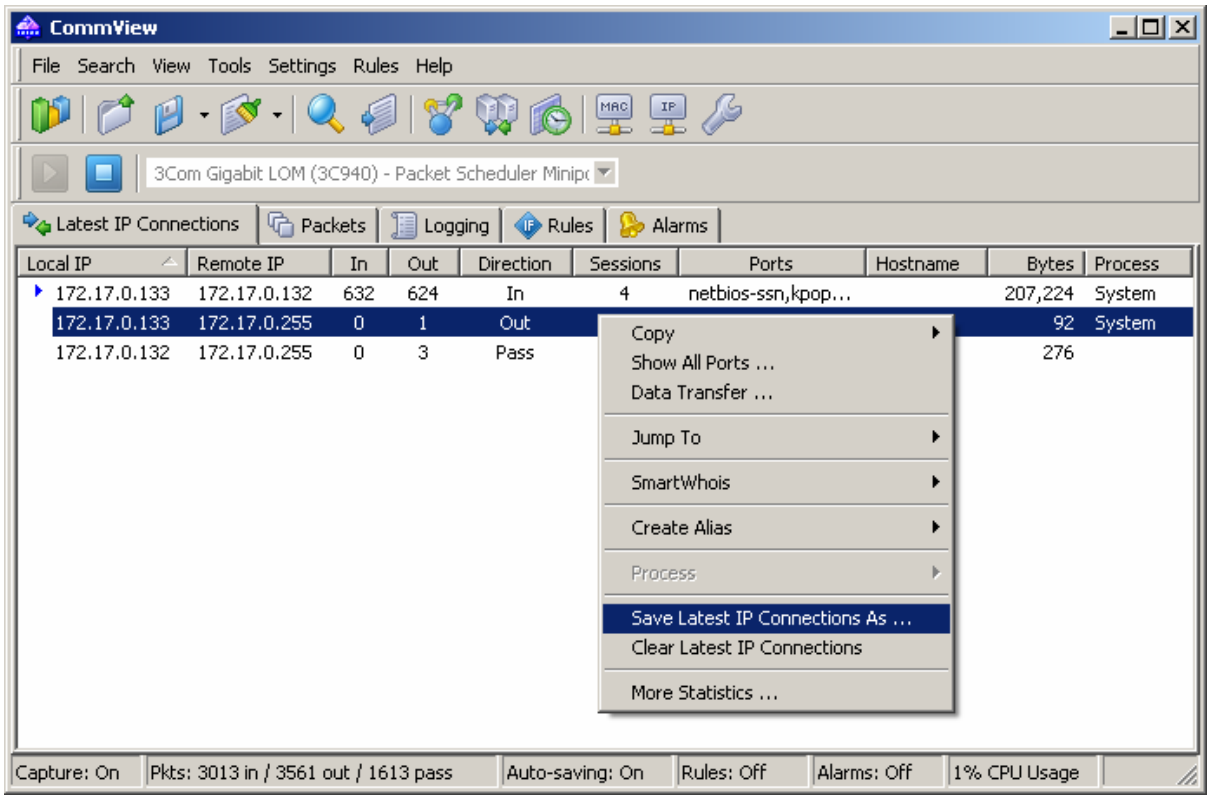
Comandos de Menú

Haciendo Clic sobre la lista Últimas Conexiones IP trae un menú con los siguientes comandos:

Guardar Nodos Como – le permite guardar el contenido de la pestaña Canales como un informe HTML.
Limpiar Nodos – Limpia la tabla.
Más Estadísticas – muestra una ventana con Estadísticas de transferencia de datos y distribución de protocolos.

Últimas Conexiones IP

Esta pestaña es utilizada para mostrar información detallada acerca de las conexiones WLAN (solo protocolos IP). 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. Por favor advierta que esta pestaña **no** se poblará a menos que el programa pueda descifrar tráfico WLAN cifrado WEP/WPA. Si su WLAN usa cifrado WEP, todos los paquetes de datos que so enviados están cifrados, y es imposible obtener información acerca de sus direcciones IP a menos que haya ingresado las claves WEP p WPA correctas, seleccionando **Preferencias => Claves WEP/WPA** en el menú



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

IP Fuente, IP Destino – Muestra el par de direcciones IP entre las cuales está siendo enviado el paquete. 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.
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.

Puede mostrar u ocultar columnas individuales haciendo 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

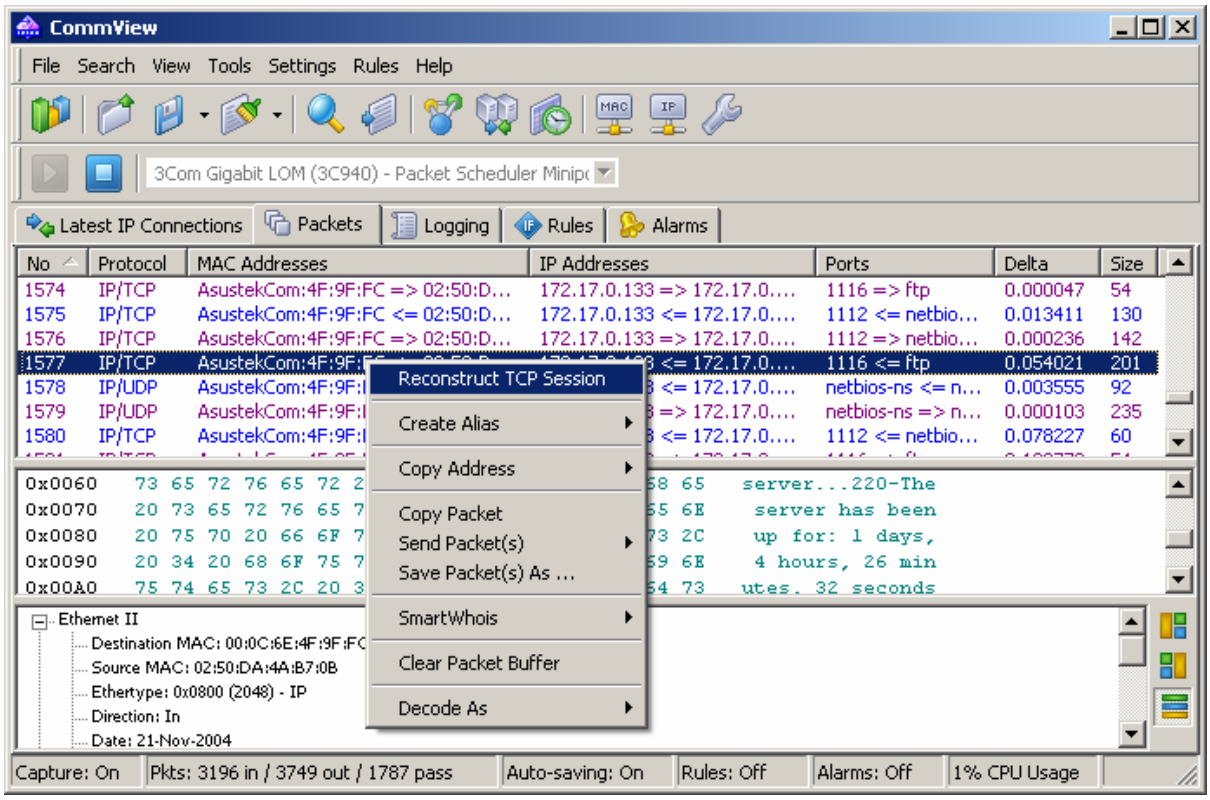
Haciendo clic en el botón derecho de Últimas Conexiones IP muestra un menú de acceso directo con los siguientes comandos:

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.
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
Señal – Muestra la fuerza de la señal en formato de percentil
Ritmo – Muestra el ritmo de transferencia de datos en Megabits por segundo.
Más Detalles – Muestra información adicional sobre algunos tipos de paquetes.
Errores – Muestra información de errores. Vea Comprendiendo Errores CRC e ICV para una explicación detallada. Esta columna por defecto no está visible
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 crudo 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.
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

CommView le permite dos tipos de reglas.

El primer tipo (**reglas inalámbricas**) le permite filtrar paquetes basados en el tipo de paquete inalámbrico: paquetes de **Datos**, **Administración**, y **Control**. Para activar o desactivar la captura de estos tipos de paquetes, use el comando **Reglas** del menú del programa, o los botones correspondientes de la barra de herramientas. Además, el comando de menú **Ignorar Balizas** le permite activar o desactivar los paquetes balizas.

El Segundo tipo (**reglas convencionales**) le permite filtrar paquetes en muchos criterios, tales como número de puerto o dirección física (MAC). Para usar este tipo de regla, cambia la pestaña **Reglas** de la ventana principal del programa. Si se fija una o más reglas, el programa filtra paquetes basado en el conjunto de reglas y muestra solamente los paquetes que cumplen con esas reglas. Si una regla es fijada, el nombre de la página correspondiente es mostrado en negrita.

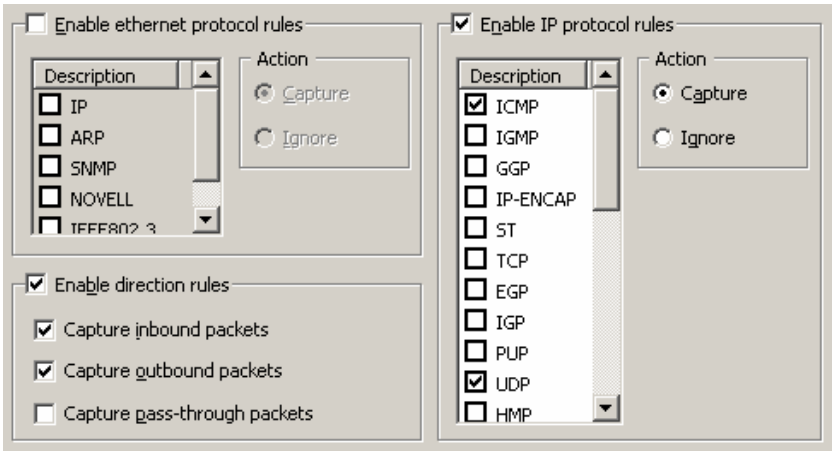
La barra de estado del programa muestra el número de reglas convencionales que están activas actualmente. Advierta que **no** muestra el número de reglas inalámbricas activas, como lo indican los botones de la barra de herramientas (arriba o abajo) claramente indican si alguna de las reglas inalámbricas están activadas o desactivadas. También advierta que las reglas inalámbricas tienen preeminencia sobre las reglas convencionales. Cualquier paquete capturado primero debe pasar las reglas inalámbricas antes de que siga procesándose. Si, por ejemplo, ninguno de los tres botones de reglas inalámbricas de la barra de herramientas es presionado, el programa no mostrará ningún paquete.

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

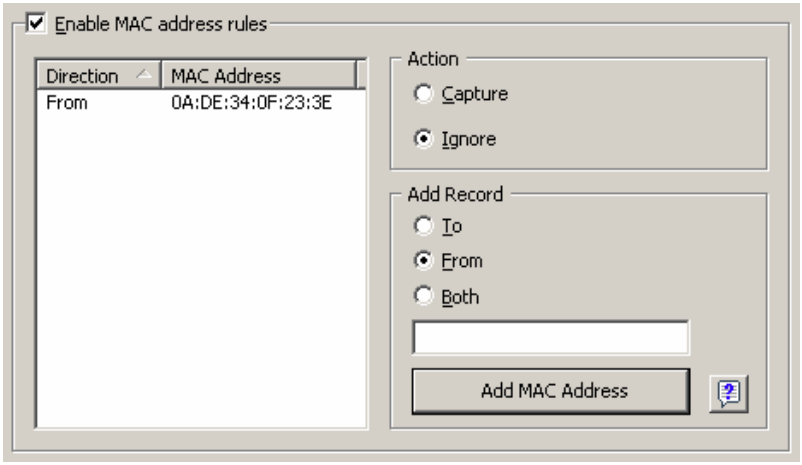
Le permite ignorar o capturar paquetes basados en protocolos de Ethernet (Capa 2) e IP (Capa 3),



Este ejemplo muestra como hacer que el programa capture solamente los paquetes ICMP y UDP. Todos los otros paquetes en la familia IP van a ser ignorados.

Direcciones Físicas

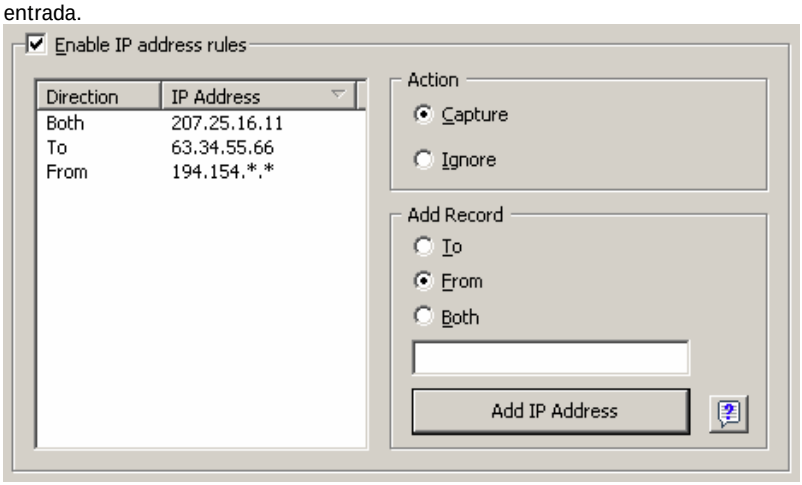
Le permite ignorar o capturar paquetes basados en la dirección física (MAC). Ingrese una dirección física (MAC) en el cuadro **Agregar Registro,** seleccione la dirección (**Desde, Hacia, Ambas)**, y haga clic en **Agregar Dirección Física**. La nueva regla será mostrada. Ahora puede seleccionar la acción 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

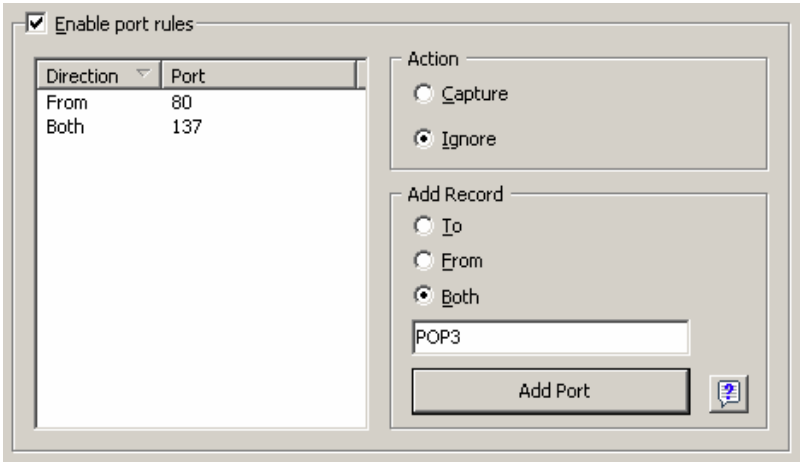
Le permite ignorar o capturar paquetes basados en las direcciones IP. Ingrese una dirección IP en la sesión **Agregar Registro,** seleccione la dirección (**Desde, Hacia, o Ambos**), y haga clic en **Agregar Dirección IP**. Puede usar comodines para especificar bloques de direcciones IP. Esta nueva regla 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

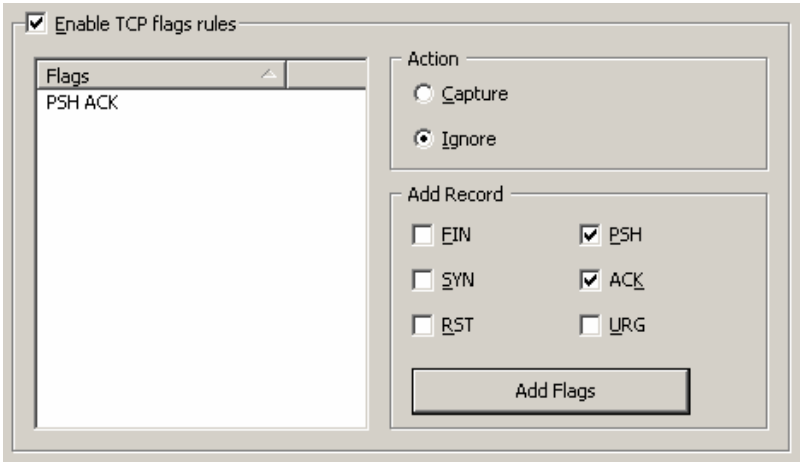
Le permite ignorar o capturar paquetes basados en el Puerto. Ingrese un número de puerto en el cuadro **Agregar Registro**, seleccione la dirección (**Desde, Hacia, o Ambos**), y haga clic en **Agregar Puerto.** La nueva regla será mostrada. Ahora puede seleccionar la acción a ser tomada cuando un nuevo 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

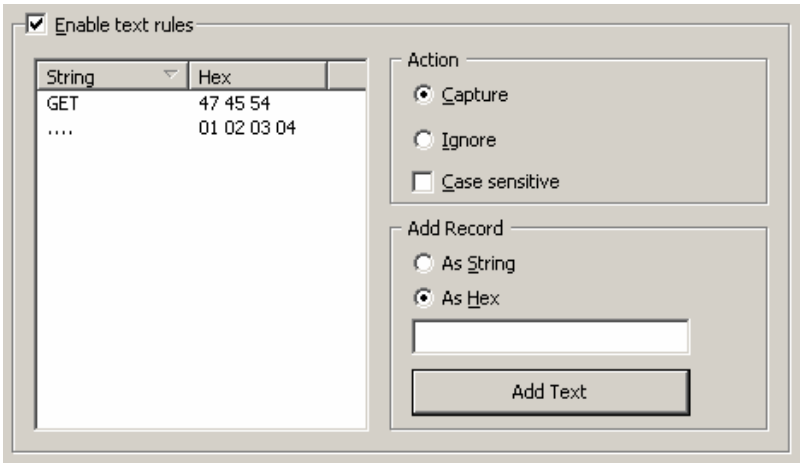
Le permite ignorar o capturar paquetes basados en indicadores de TCP, Controle un indicador o una combinación de indicadores en el cuadro **Agregar Registro**, haga clic en **Agregar Indicadores**. La nueva regla será mostrada. Ahora puede seleccionar la acción a ser tomada cuando un nuevo paquete con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



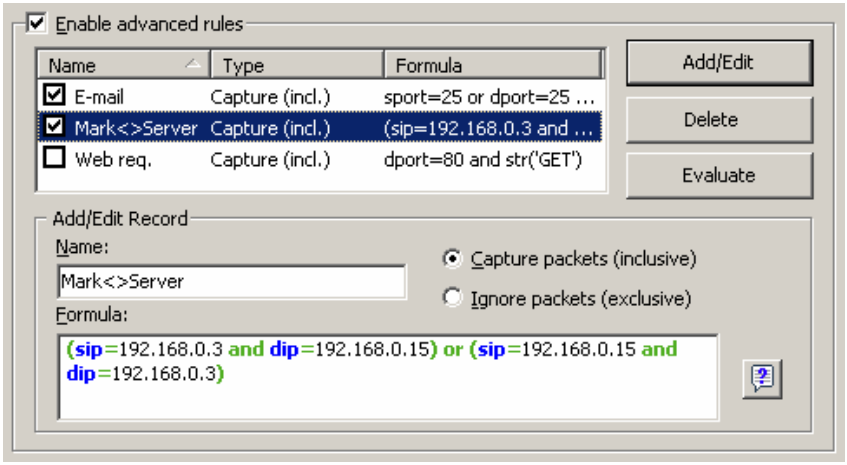
Este ejemplo muestra como hacer que el programa capture solo los paquetes que contiene tanto "GET" o los datos hexadecimales 01 02 03 04. Marque la casilla **Coincidir MAYÚSCULAS/minúsculas** si quiere que las reglas utilicen la comparación en Texto Exacto. Todos los otros paquetes que no contengan el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

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).*

ToDS, FromDS, MoreFrag, Retry, Power, MoreData, WEP, Order, Ftype, FsubType, Duration, FragNum, SeqNum – le permite usar campos de encabezados de paquete 802.11 en reglas avanzadas. Los nombres de los operadores corresponden completamente a los campos de encabewzado de paquete como se describe en la especificación del estándar 802.11. Los valores aceptables para ToDS, FromDS, MoreFrag, Retry, Power, MoreData, WEP, y Order son 0 o 1. Para los operadores Ftype, FsubType, Duration, FragNum, y SeqNum son aceptables otros valores numéricos.

Por favor refiérase a las especificaciones de estándar 802.11 para la información detallada acerca de campos de encabezado de paquetes 802.11 y sus valores aceptables

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.

- **(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.
- **not(ftype=0 and fsubtype=8)** // Ignorar paquetes de administración del tipo baliza
- **ftype=2 and wep=1** // Capturar paquetes de datos cifrados

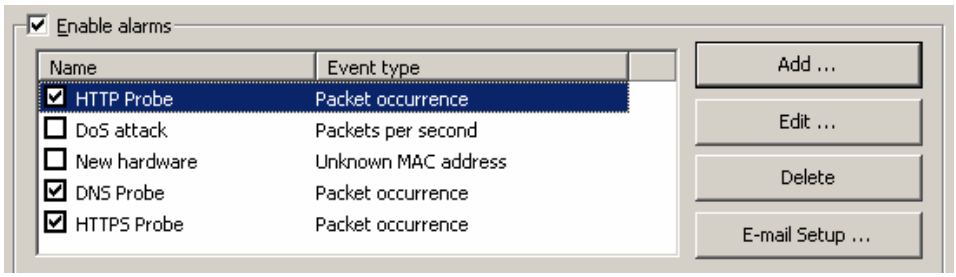
MoreFrag=0 and FragNum=0 // Capturar paquetes no fragmentados

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.

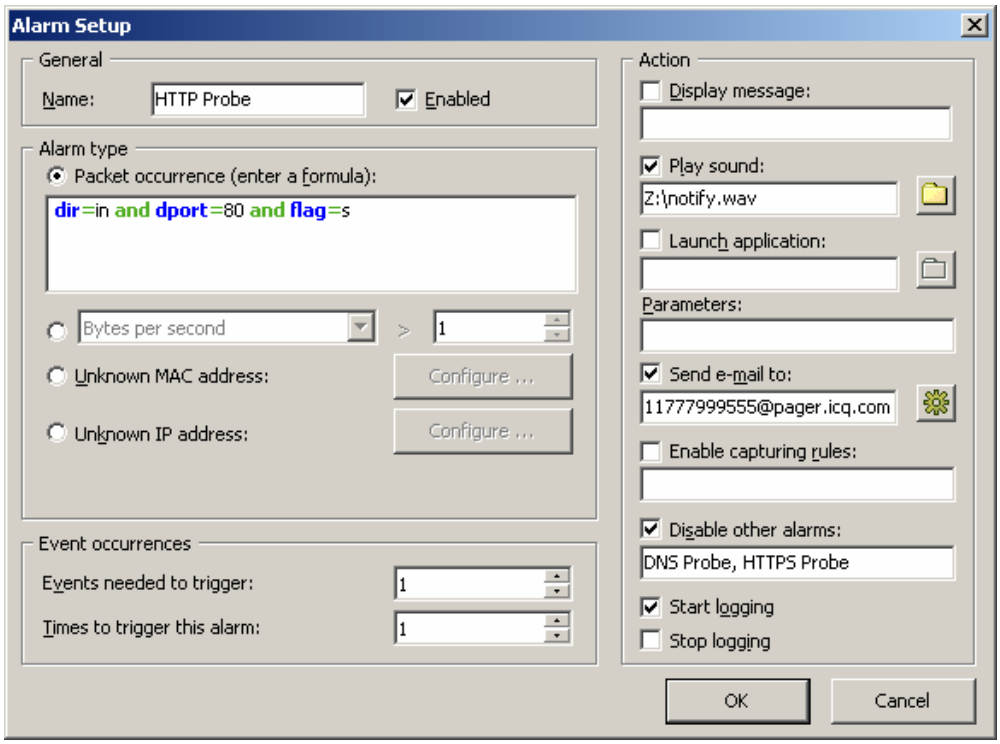
Importante: Las alarmas pueden ser disparadas solo por aquellos paquetes que han pasado los filtros del programa. Si, por ejemplo, configuró el programa para filtrar paquetes UDP creando la regla correspondiente, mientras una de sus alarmas se supone que sea disparada por un paquete UDP, tal alarma nunca será disparada.

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.

- **Errores CRC por segundo** – La alarma será disparada una vez que el número de errores CRC por Segundo ha excedido (o caído por debajo) del valor especificado.

- **Reintentos por segundo** – La alarma será disparada una vez que el número de reintentos por Segundo haya excedido (o caído por debajo) del valore 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.

- **PAs Corruptas** – La alarma será disparada una vez que CommView ha capturado un paquete baliza desde un punto de acceso desconocido. Use el botón **Configurar** para ingresar direcciones físicas (MAC) de puntos de acceso conocidos. este tipo de alarmas es útil para detectar puntos de acceso no autorizados.

- **Redes Ad Hoc –** La alarma será disparada una vez que CommView ha capturado un paquete baliza desde una estación Ad Hoc desconocida. Use el botón **Configurar** para ingresar las direcciones físicas (MAC) de estaciones Ad Hoc conocidas, si hay alguna. Este tipo de alarmas es útil para detector uso no autorizado de redes Ad Hoc.

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.

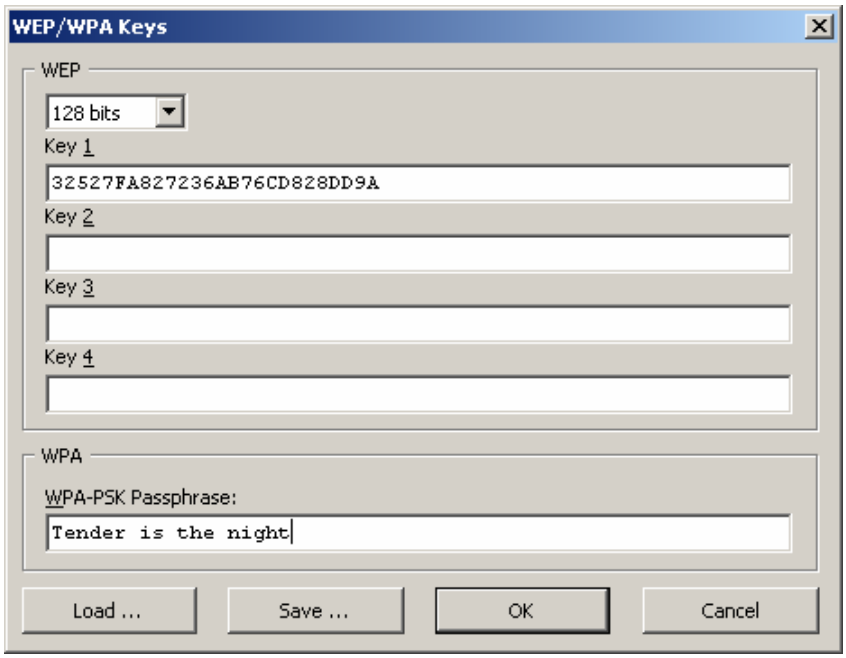
Claves WEP/WPA

La ventana de **Claves WEP/WPA** permite que claves WEP o WPA sean ingresadas para el descifrado de paquetes capturados. Sin estas claves, el programa no podrá descifrar paquetes de datos que están trasmitiéndose sobre su WLAN, dado que algunas WLANs usan modo de cifrado mixto, donde clientes WEP y WPA activos pueden autenticarse, puede usar claves WEP y frases WPA simultáneamente.

WEP
El estándar permite usar hasta cuatro claves WEP, por lo que puede especificar una, dos, tres o cuatro claves. La lista desplegada de longitud de clave le permite seleccionar la longitud de clave. Las longitudes soportadas son 64, 128, 152, y 256 bits, y debería ingresar una secuencia hexadecimal que es de 10, 26, 32, o 58 caracteres de largo respectivamente.

WPA
El estándar de Acceso Protegido a Wi-Fi (WPA) define un número de modos de autenticación y cifrado, No todos ellos están soportados por CommView for WiFi debido a las restricciones del modelo de seguridad subyacente. CommView for WiFi soporta descifrado de WPA o WPA2 en modo de Claves Pre-Compartidas (PSK) usando el Protocolo de Integridad de Clave Temporal (TKIP) o el cifrado de datos Estándar de Cifrado Avanzado/Protocolo Contador CBC-MAC (AES/CCMP). Puede ingresar tanto una frase contraseña o una clave hexadecimal que tiene 64 caracteres de largo.

Importante: Por favor refiérase al capítulo comprendiendo el cifrado WPA para información detallada relativa a la forma en que CommView for WiFi procesa el tráfico cifrado en WPA. También podría desear usar la herramienta reasociación de Nodo una vez que haya ingresado una nueva frase contraseña WPA.

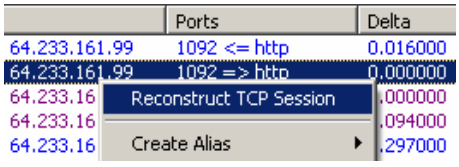


Para guardar el conjunto actual de claves, pulse **Guardar** ....para cargar un conjunto de claves previamente guardado, pulse **Cargar ...**.

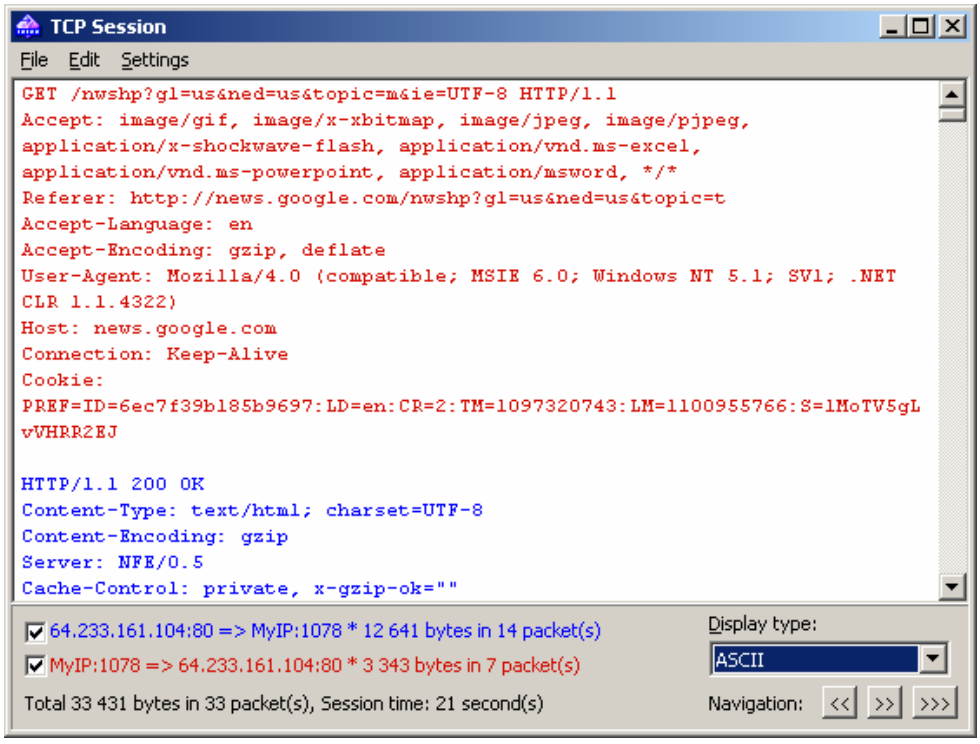
El conjunto de claves que puede ingresar o cargar usando esta ventana de diálogo se aplicará a paquetes capturados en tiempo real, así como a cualquier archivo de captura NCF que podría haber sido guardado previamente, cuando los paquetes capturados son guardados en un archivo de captura NCF, aquellos paquetes que fueron descifrados satisfactoriamente serán guardados en forma descifrada, mientras aquellos paquetes que no pudieron ser descifrados serán guardados en el formato original sin modificar.

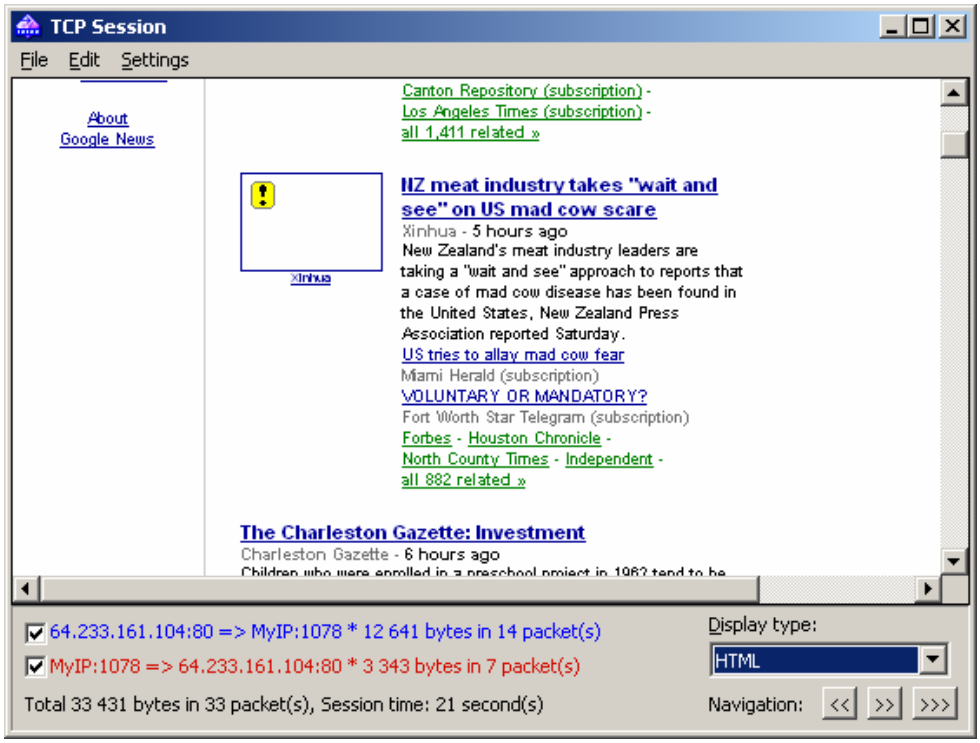
Reconstruir sesión TCP

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:

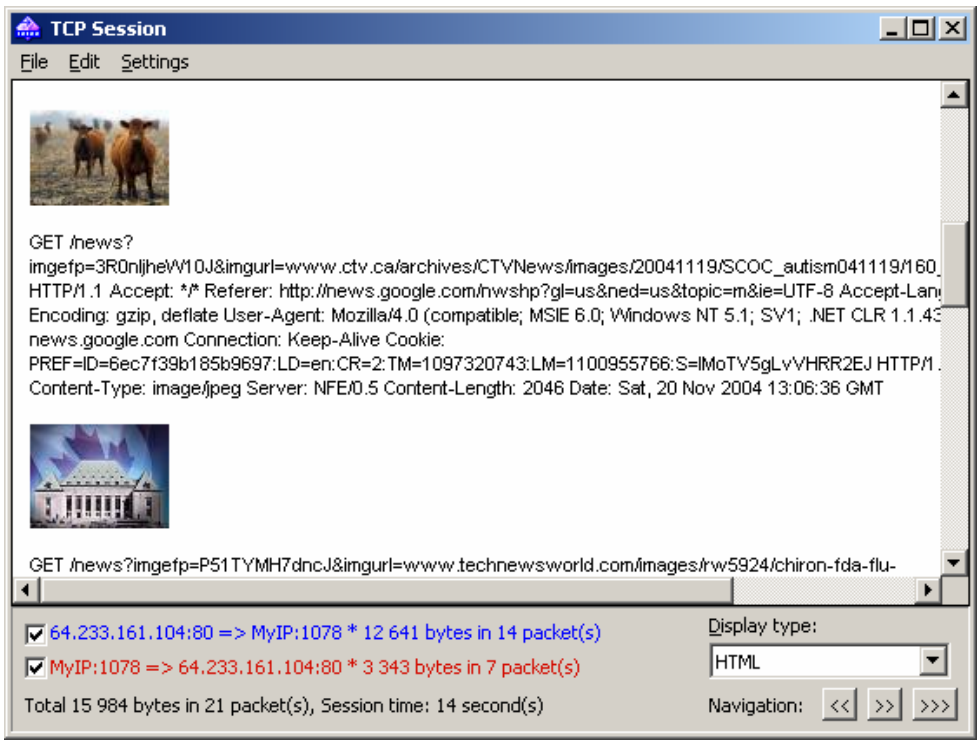


La reconstrucción de sesiones funciona mejor para protocolos basados en texto, como POP3, Telnet, o HTTP. Por supuesto, puede también reconstruir la descarga de un archivo grande comprimido, pero puede llevarle a CommView mucho tiempo reconstruir varios megabytes de datos, y la información obtenida será 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. Si su WLAN usa cifrado WEP o WPA, debe configurar las claves WEP o WPA correctamente para poder descifrar tráfico de red; de otro modo este gráfico estará vacío.

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. Si su WLAN usa cifrado WEP o WPA, debe configurar las claves WEP o WPA correctamente para poder descifrar tráfico de red; de otro modo este gráfico estará vacío.

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. Si su WLAN usa cifrado WEP o WPA, debe configurar las claves WEP o WPA correctamente para poder descifrar tráfico de red; de otro modo este gráfico estará vacío.

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. Si su WLAN usa cifrado WEP o WPA, debe configurar las claves WEP o WPA correctamente para poder descifrar tráfico de red; de otro modo este gráfico estará vacío.

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**.

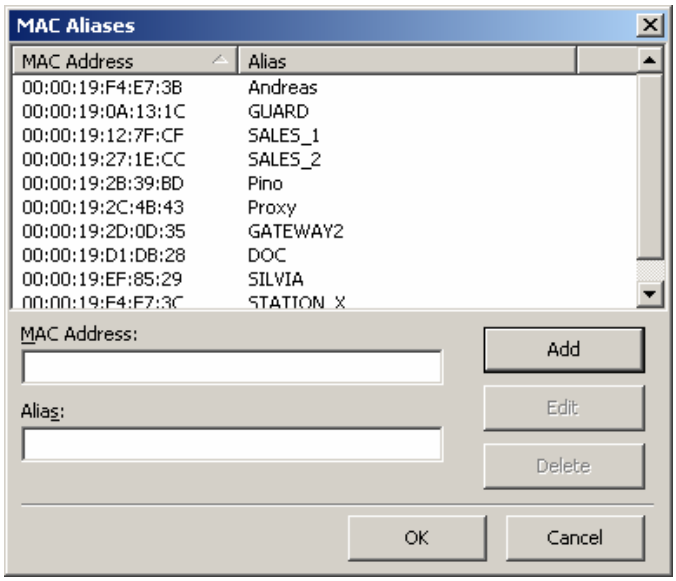
Reporte
Esta pestaña permite a CommView la generación automática de reportes definibles en formato HTML (incluyendo imágenes de gráficos) o de texto delimitados por coma.

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.

Uso de Alias

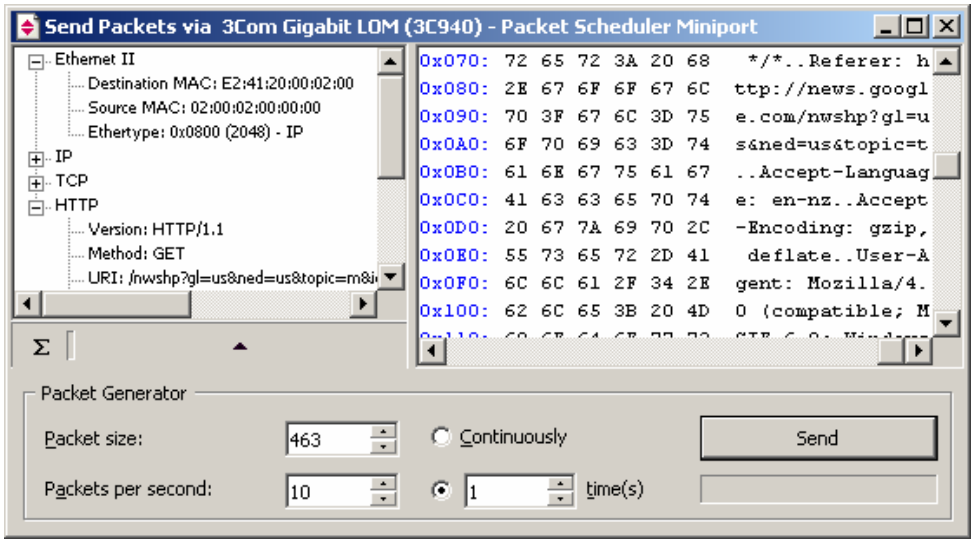
Los Alias son nombres fáciles de recordar y capaces de ser leídos por el ser humano que CommView va a sustituir por una dirección física (MAC) o dirección IP cuando se muestran los paquetes en las pestañas de Paquetes y Estadísticas. Esto permite que los paquetes sean más fáciles de reconocer y analizar. 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 su adaptador inalámbrico de red. Para abrir el 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 Paquete**.



Por favor lea la siguiente información importante acerca de las limitaciones y peculiaridades de usar el Generador de Paquetes con adaptadores inalámbricos:

- No use el Generador de Paquetes a menos que sepa exactamente que efecto desea lograr. Enviar paquetes podría producir resultados impredecibles, y recomendamos fuertemente evitar usar esta herramienta a menos que sea un experimentado administrador de red.
- El Generador de Paquetes no funcionará cn los viejos adaptadores 802.11b.
- Determinados campos en el encabezado del paquete son modificados por la lógica del adaptador antes que el paquete sea enviado. Por ejemplo, los valores de Duración y Número de secuencia son reescritos por la lógica del adaptador, y el bit “More Fragments” será fijado siempre en 0.
- La lógica de su adaptador podría fallar al enviar determinados paquetes, o podría enviar determinados paquetes varias veces. Esta conducta es totalmente controlada por la lógica y está más allá de nuestro control.
- La lógica de su adaptador podría imposibilitarle enviar paquetes a un ritmo arbitrario. Es muy posible que cuando seleccione el ritmo de 1000 paquetes por segundo, la lógica realmente enviará los paquetes a un ritmo mucho menor.

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

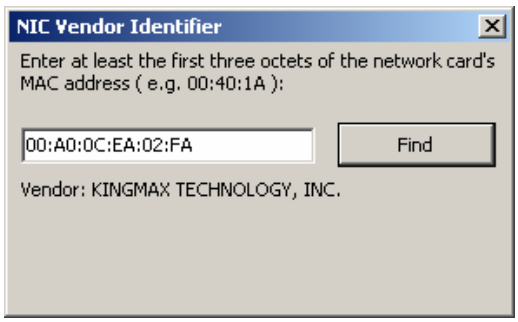
Puede usar el Generador de Paquetes para enviar múltiples paquetes al mismo tiempo. Para hacer esto, solo seleccione los paquetes de la lista que quiere enviar e invoque el generador de paquetes utilizando el menú de clic derecho, o arrastrar y soltar los paquetes seleccionados en la ventana del Generador 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.

Identificar el Fabricante de la Tarjeta

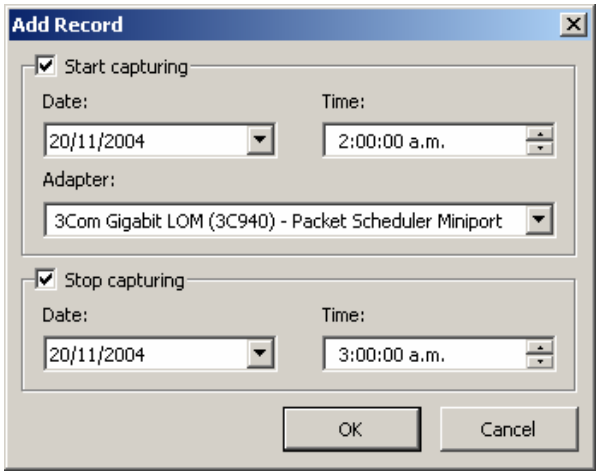
Los primeros 24 bits de la dirección física de una tarjeta de red identifican al fabricante de la misma. Este número de 24-bit es llamado OUI ("Organizationally Unique Identifier"). Identificar el Fabricante de la Tarjeta es una herramienta que permite buscar el nombre de fabricante por la dirección 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.

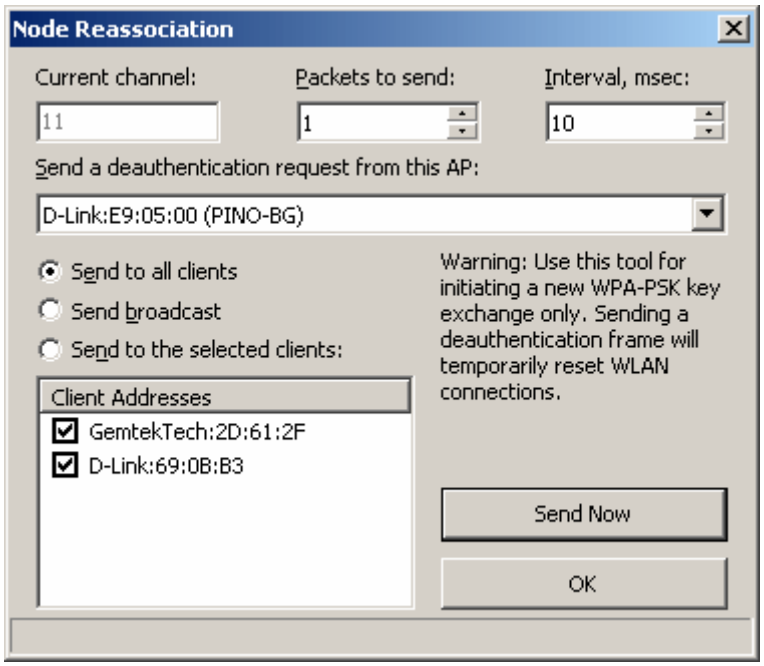
Si CommView está ya capturando paquetes al mismo tiempo que la tarea programada comienza y si el adaptador que especificó es distinto de la que está siendo monitoreada, CommView detendrá la captura, cambiará de adaptador al especificado en la tarea y reiniciará la captura.

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

Reasociación de Nodo

Dada la naturaleza dinámica del cifrado WPA, conocer la frase contraseña WPA solamente no le permite descifrar tráfico inmediatamente después de ingresar la frase contraseña correcta. Para poder descifrar tráfico cifrado WPA, CommView for WiFi debe estar funcionando y capturando paquetes durante la fase de intercambio de clave (el intercambio de clave es llevado a cabo usando el protocolo EAPOL). Por favor refiérase al capítulo comprendiendo el descifrado WPA para información detallada.

La herramienta Reasociación de Nodo puede ser usada para iniciar un nuevo intercambio de clave:



Esta herramienta simplemente envía una solicitud de des-autenticación a la estación seleccionada en nombre del punto de acceso. Esto provoca que la estación se re-asocie con el punto de acceso. El proceso de reasociación dura generalmente un Segundo y le permite a CommView for WiFi capturar paquetes EAPOL necesarios para el descifrado WPA-PSK. No use esta herramienta a menos que necesite descifrar tráfico WPA-PSK sobre su WLAN.

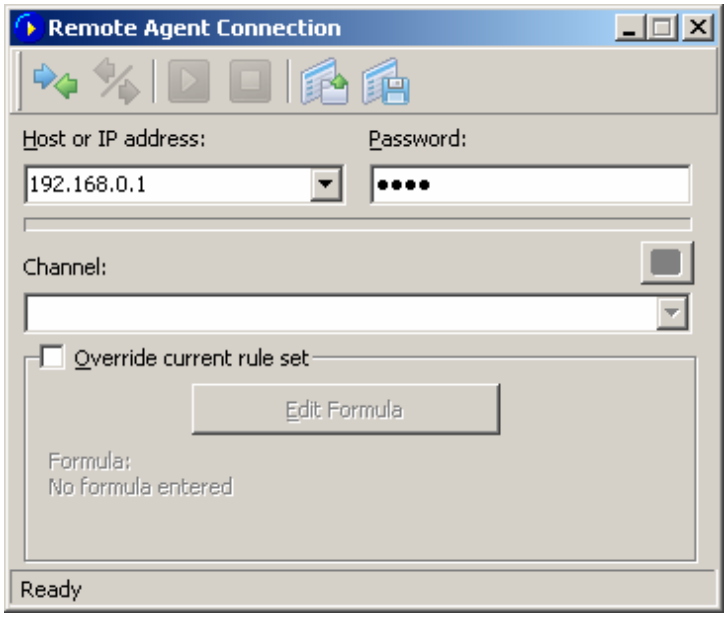
Para iniciar una reasociación, seleccione un punto de acceso desde la lista desplegada, seleccione las estaciones, y pulse **Enviar**. Las opciones **Enviar a todos los clientes** y **Enviar a clientes seleccionados** envía paquetes unicast a todos o a clientes seleccionados. La opción **Enviar broadcast** envía un paquete de broadcast a la dirección FF:FF:FF:FF:FF:FF. Mientras esta opción cubre estaciones no detectadas, algunas estaciones podrían ignorar la solicitud de desautenticación emitida. Podría desear enviar varios paquetes usando las casillas **Enviar Paquetes** e **Intervalo**.

Uso de Remote Agent para WiFi

CommView Remote Agent para WiFi es un producto adicional que puede ser usado para monitorear tráfico de red en forma remota. Todo lo que tiene que hacer es instalar Remote Agent para WiFi en la computadora objetivo, y luego usar CommView for WiFi para conectarse a Remote Agent. Una vez que está conectado y autenticado, puede comenzar a monitorear como si estuviera allí.

Importante: Este capítulo describe como usar CommView for WiFi para conectarse a Remote Agent y capturar tráfico en forma remota. Para información detallada sobre la instalación y configuración de Remote Agent, por favor refiérase al archivo de ayuda que viene con Remote Agent. Se recomienda fuertemente que lea cuidadosamente la documentación de Remote Agent antes de usarlo. CommView Remote Agent para WiFi puede descargarse de nuestro sitio Web.

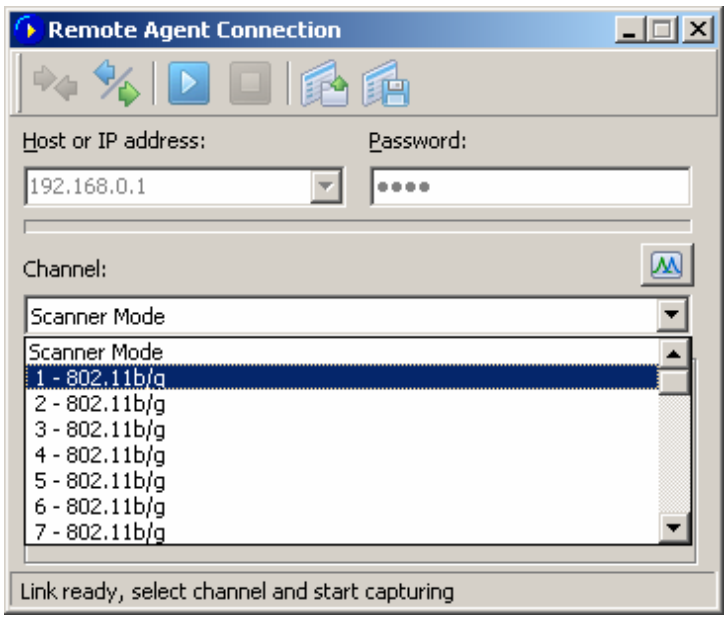
Para cambiar al modo de monitoreo remoto, pulse **Archivo** => **Modo de Monitoreo Remoto**. Aparecerá una barra de herramientas adicional en la ventan principal de CommView for WiFi junto a la barra de herramientas principal. Si está detrás de un firewall o servidor proxy, o usando un puerto de Remote Agent no estándar, podría necesitar pulsar el botón **Preferencias Avanzadas de Red** para cambiar el número de puerto y/o ingrese preferencias para el servidor Proxy SOCKS5. El diálogo **Preferencias Avanzadas de Red** también le permite definir si Remote Agent aplicará las reglas de filtrado localmente, o enviará el tráfico capturado a CommView for WiFi; esto será discutido en detalle más adelante en este capítulo.



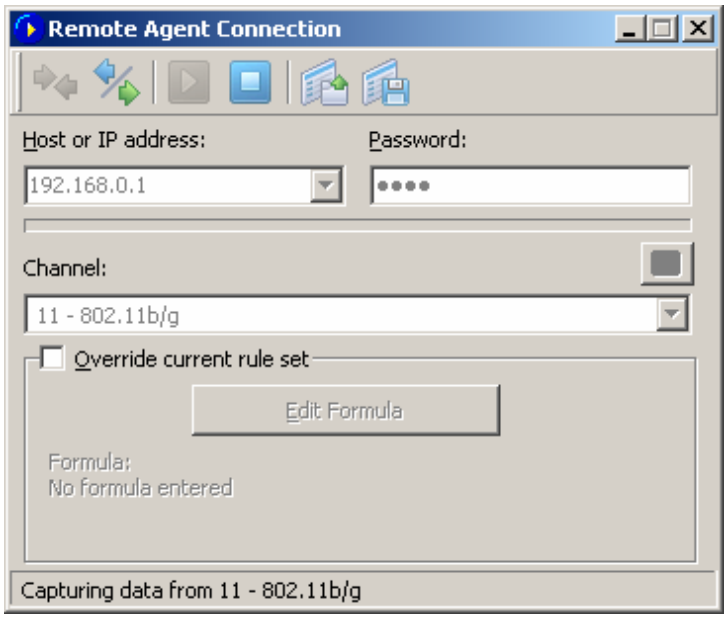
Pulse sobre el botón **Nueva Conexión de Remote Agent** para establecer una nueva conexión, o pulse en el botón de la barra de herramientas **Cargar Perfil de Remote Agent** para cargar un perfil de conexión de Remote Agent previamente guardadas. Un perfil previamente guardado también podría haber sido cargado desde la ventana de Nueva Conexión de Remote Agent.

Aparecerá una ventana de Conexión de Remote Agent. Ingrese la dirección IP de la computadora que está ejecutando CommView Remote Agent para WiFi dentro del área de ingreso de dirección IP, ingrese la contraseña de conexión y pulse el botón **Conectar**. Si la contraseña es correcta, se establecerá una conexión. Entonces, podrá ver el mensaje *Enlace Listo* en la barra de estado y la casilla de selección de canal listará los canales soportados por el adaptador inalámbrico instalado en la computadora remota. Además de las listas de canales, un ítem especial **Modo Exploración** se agregará como el primer ítem de la lista.

Si selecciona el **Modo Exploración**, el adaptador inalámbrico remoto ciclará por los canales disponibles, capturando datos de cada uno de ellos por varios segundos. El pequeño botón ubicado en el lado derecho de la ventana, justo arriba de la casilla de selección de canal, le permite ajustar las preferencias de escaneo. Pulse este botón para seleccionar los canales a ser monitoreados en Modo Escaneo y fije el intervalo, por ejemplo, el número de segundos por canal. Advierta que para adaptadores inalámbricos Intel, el intervalo no puede estar por debajo de los 4 segundos debido a limitaciones técnicas.



Ahora es el mejor momento para configurar las reglas de captura usando la pestaña **Reglas** en la pantalla principal de CommView for WiFi. También puede aplicar un conjunto personalizado de reglas de captura para esta conexión y sobrescribir las reglas actuales definidas en CommView marcando el cuadro **Sobrescribir conjunto de reglas actuales**, pulsando en el botón **Editar Formula** e ingresando las reglas de formula en el campo de abajo. La sintaxis de formula es la misma usada en Reglas Avanzadas. Una vez que esté listo para comenzar a monitorear, seleccione el canal desde la lista y pulse el botón de la barra de herramientas **Comenzar Captura**. CommView for WiFi le permite guardar las preferencias de Conexión de Remote Agent como un perfil de conexión para un rápido y fácil acceso en el futuro. Pulse el botón de la barra de herramientas **Guardar Perfil de Remote Agent** en la ventana de nueva conexión de Remote Agent e ingrese un nombre para el archivo.



CommView for WiFi comenzará a capturar el tráfico de adaptador remoto como si fuera tráfico de su red local; Virtualmente no hay diferencia entre usar CommView for WiFi local o en forma remota. Cuando haya finalizado con monitoreo remoto, simplemente pulse botón de barra de herramienta **Detener Captura**. Luego puede cambiar el canal o desconectarse de Remote Agent pulsando el botón de la barra de herramientas **Desconectar**. Para volver al modo estándar, pulse **Archivo** => **Modo de Monitoreo Remoto**, y la barra de herramientas adicional desaparecerá.

Por favor advierta que CommView for WiFi puede trabajar con múltiples Remote Agents simultáneamente. Puede abrir varias conexiones remotas, cada una con sus propias preferencias y an conjunto independiente de reglas y recolectar el tráfico de WLANs remotas en una instancia de CommView for WiFi.

Como Usar CommView Remote Agent para WiFi Eficientemente

La clave para el uso eficiente de Remote Agent es asegurarse que hay suficiente ancho de banda disponible para transferir los datos recolectados por Remote Agent a CommView for WiFi. Como se mencionó anteriormente, Remote Agent debería instalarse sobre una computadora que tiene un adaptador inalámbrico compatible (para ser usado para monitorear) y un adaptador Ethernet adapter (para ser usados por la conexión entre Remote Agent y CommView for WiFi).

Por omisión, Remote Agent envía los paquetes recolectados hacia CommView for WiFi, sin importar las reglas de captura que podrían configurarse en CommView for WiFi. Esto se realiza proveyendo los datos estadísticos y el descifrado correctos, así como las formas de identificación correcta de nodos inalámbricos. Dado que una red WiFi completamente cargada tiene un ancho de banda de 54 Mbit/s (o incluso 108 Mbit/s con algún hardware propietario), Es importante que el enlace cableado entre Remote Agent y CommView for WiFi sea capaz de manejar este ancho de banda. En un ambiente de oficina moderno, donde son comunes redes de Gigabits, un solo adaptador Gigabit puede fácilmente recibir datos desde una docena de Remote Agents.

Hay situaciones donde una conexión rápida es problemática. Por ejemplo, una conexión de ancho de banda podría no estar disponible si está monitoreando una WLAN remota sobre Internet. Incluso una conexión T3 (4.5 Mbit/s) es insuficiente para transferir todos los paquetes de una WLAN moderadamente cargada. En tales situaciones, puede cambiar las preferencias por omisión y hacer que Remote Agent filtre los paquetes antes que sean transferidos a CommView for WiFi. El botón de Preferencias Avanzadas de Red en la barra de herramientas adicional de monitoreo remoto en la ventana principal de CommView for WiFi le permite activar la opción de Minimizar ancho de banda. Cuando esta opción está activada, el conjunto de reglas actuales de CommView for WiFi es enviada periódicamente al Remote Agent. El conjunto de reglas es así aplicado localmente, de forma tal que solo aquellos paquetes que pasan las reglas son enviados hacia CommView for WiFi. En este modo, los Nodos podrían no mostrar ningún nodo, y la pestaña Canales no mostrará estadísticas por canal completas, por lo que use este modo solo cuando tiene ancho de banda limitados, pero sigue necesitando acceso a los paquetes de una WLAN remota.

Por las mismas razones de ancho de banda, se recomienda NO usar conexiones inalámbricas para intercambiar datos entre Remote Agent y CommView for WiFi. También es una mala idea dado que el monitoreo del adaptador inalámbrico está siendo usado para comunicar con CommView for WiFi si funciona sobre el mismo, o canales cercanos. Esto simplemente provocará el efecto bola de nieve.

Si CommView Remote Agent para WiFi captura más datos de los que puede enviar a CommView for WiFi, usa un buffer interno para almacenar paquetes que no pueden enviarse inmediatamente. El tamaño del buffer es de 5 Mbytes. El indicador de utilización del Buffer en la ventana de Remote Agent muestra el estado actual del buffer. Por ejemplo, el programa tiene almacenados 2.5 Mbytes de datos, la utilización del buffer es del 50%. Si/cuando la utilización del buffer alcanza el 100%, el programa para de almacenar datos y descargar paquetes capturados hasta que se libere espacio en el buffer.

Seguridad

CommView Remote Agent para WiFi fue hecho con la seguridad en mente. Puede ser accedido solamente usando una contraseña que nunca es transmitida en texto plano y que está asegurada usando un protocolo desafío-respuesta. Con una función arbitraria segura. Si la autenticación es satisfactoria, todo el tráfico transmitido es comprimido y luego cifrado con la misma contraseña. Por favor tome precauciones para mantener su contraseña en secreto. Una vez que es revelada a una persona no autorizada, esa persona tendrá amplias facultades para estudiar su red e interceptar tráfico de red sobre la computadora remota.

Configuración de 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.

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 marcada, 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. lo puede encontrar 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.

Descifrado WEP forzado – debería marcar esta casilla si su adaptador inalámbrico informa erróneamente que los paquetes capturados no están cifrados (el indicador WEP en el encabezado 802.11 está fijado en 0). Este es el caso con algunos adaptadores, por ejemplo, fabricados por Belkin. Para hacer que CommView descifre tales paquetes, esta opción debería estar activada.

Capturar Paquetes Dañados – debido a la distancia, la interferencia de radio, y otros fenómenos físicos, algunos paquetes recibidos por su adaptador inalámbrico podrían estar dañados. Por ejemplo contener datos parcial o totalmente inválidos. Marque esta casilla si desea que el programa capture y muestre tales paquetes. Esta opción tiene ventajas y desventajas. La ventaja es que si está ubicado lejos de las estaciones y/o puntos de acceso WLAN, un alto porcentaje de paquetes podrían estar rotos, y activando esta opción le permitiría ver más datos, a pesar que los datos podrían estar parcialmente dañados. Por ejemplo, podría ver paquetes IP enviados a direcciones IP inexistentes. También, cuando esta casilla está marcada, el programa tratará de descifrar aquellos paquetes cifrados WEP o WPA en el cual el Valor de Verificación de Integridad es incorrecto, pero el encabezado parece ser válido.

Descartar paquetes dañados en el explorador – cuando esta opción es activada, CommView ignorará paquetes dañados mientras escanea canales y solo listará nodos que transmiten paquetes válidos.

Descubrir nodos activos usando PROBE REQUEST – si esta casilla está marcada, el programa envía paquetes PROBE REQUEST periódicamente, Tales paquetes facilitan el descubrimiento de aquellos Puntos de Acceso que no difunden su SSID, Advierta que usando esta opción hace que su adaptador transmita paquetes, por lo que no estará más completamente sigiloso. Esta opción no está disponible par alas antiguas tarjetas 802.11b.

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 - 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 WLAN con muchos paquetes pasantes y una mezcla de direcciones IP internas y externas. En una situación como esta CommView for WiFi 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**.

Colores

Color de los Paquetes - Define el color de los distintos tipos de paquetes (Normal, CRC Malo, ICV Malo) en la pestaña de **paquetes**

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.

Color de Marco de Administración – fija el color para dos tipos distintos de marcos de Administración. El color es usado en la columna **Protocolo** de la pestaña **Paquetes** para mostrar los tipos de marcos correspondientes.

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 el mapeo 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 fresca 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.

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. Puede localizarlo en la carpeta **\system32\drivers\etc**. Puede editar manualmente este archivo si desea agregar más puertos/nombres de servicio. CommView for WiFi 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 capítulo puede escuchar respuestas a algunas de las preguntas hechas más frecuentemente. Las últimas preguntas frecuentes siempre están disponibles en http://www.tamos.com/products/commwifi/faq.php

P. Estoy en una red inalámbrica, y deseo monitorear mis propios paquetes entrantes y salientes. ¿Cuál producto necesito: la edición estándar y no inalámbrica de CommView, o CommView for WiFi?

R. Necesita la edición estándar, no inalámbrica de CommView. Esto le permitirá monitorear su propio tráfico, pero no podrá ver el tráfico de otras estaciones WLAN. A diferencia de la edición estándar de CommView, CommView for WiFi le permite monitorear otras estaciones inalámbricas.

P. ¿Necesito un hardware especial para usar CommView for WiFi?

R. necesita un adaptador inalámbrico compatible. La lista de adaptadores compatibles puede encontrarse en http://www.tamos.com/products/commwifi/. Debe instalar un controlado especial para su adaptador. Este controlador viene con CommView for WiFi. Una vez que el controlador ha sido instalado, su adaptador será puesto en modo de monitoreo pasivo y no podrá comunicarse con hosts inalámbricos o puntos de acceso. Para reestablecer las funciones estándar de su adaptador, deberá volver a su controlador original del adaptador provisto por el fabricante. Sin embargo, este no siempre es el caso, y dependiendo del modelo del adaptador y el sistema operativo, podría usar el controlador en modo dual (modo pasivo cuando CommView para WiFi está funcionando y modo activo cuando CommView no está funcionando). Por favor refiérase a las notas técnicas para encontrar si el modo dual es posible en su caso. Si no es posible, y desea preservar su conectividad inalámbrica mientras usa este producto, considere instalar dos adaptadores inalámbricos, uno que puede ser usado para monitoreo, mientras que el otro podría realizar las funciones estándar de red.

Advierta que si decide usar dos adaptadores como se sugiere arriba, y uno está basado en el conjunto de chips Atheros, es altamente recomendado que el otro adaptador este basado en un conjunto de chips distinto, dado que si usa dos adaptadores basados en Atheros, uno de ellos no estará operativo. Otra consideración es relativa a las dimensiones de su adaptador: si está usando una portátil y quisiera usar dos adaptadores, y su portátil no tienen un adaptador inalámbrico incorporado, necesitará usar sus dos ranuras de tarjetas de su portátil. Esto podría ser difícil dado que una tarjeta inalámbrica típica es muy gruesa, y dos tarjetas podrían no entrar. Si desea evitar este problema, considere usar una Proxim ORiNOCO 802.11ag ComboCard. Estas tarjetas tienen una cubierta fina, y si inserta esta tarjeta en la ranura inferior, le permitirá instalar cualquier tarjeta en la ranura superior.

P. Mi tarjeta no está en su lista de hardware soportado. ¿Cuáles son mis opciones?

R. En primer lugar, la información sobre los tipos de adaptadores que no soportaremos:

- Adaptadores USB.
- Adaptadores 802.11b, excepto aquellos que ya están soportados. Cada vez menos proveedores hacen nuevos modelos de adaptadores 802.11b, han sido reemplazados por adaptadores 802.11g, 802.11a, y combinados 802.11a/b/g.
- Adaptadores basados en conjunto de chips Broadcom, hasta y al menos que Broadcom sea más cooperativo.

En Segundo lugar, nuestra lista de compatibilidad de hardware incluye solo aquellas tarjetas que hemos probado en nuestro laboratorio de pruebas. Hay varios fabricantes que usan conjuntos de chips Atheros (actualmente soportamos principalmente este conjunto de chips). Naturalmente, no podemos probar todas estas tarjetas. Si su tarjeta 802.11g o 802.11a/b/g CardBus o tarjeta PCI está basada en el conjunto de chips Atheros, hay buenas posibilidades de que su tarjeta funcione con el controlador existente. Descargue nuestro Utilitario de Prueba de Adaptador y ejecútelo en su computadora, si un adaptador compatible está instalado, el utilitario mostrará su nombre. Advierta que un adaptador compatible podría mostrarse bajo un nombre genérico, "Adaptador Inalámbrico de Red Atheros". Esto es normal. Si un adaptador compatible ha sido detectado, puede instalar CommView for WiFi. Por favor háganos saber si ha probado satisfactoriamente CommView for WiFi con un adaptador que no está soportado oficialmente por nosotros.

Si su tarjeta NO está basada en el conjunto de chip Atheros, podría desear esperar hasta que soportemos otros conjuntos de chip, sin embargo no podemos dar ninguna garantía o tiempos estimados. Por último, podría desear compara una tarjeta compatible, dado que no son terriblemente caras en estos días.

P. ¿Qué adaptador recomiendan para usar con su aplicación?

R. Si ya tiene un adaptador que esta en nuestra lista de hardware compatible, no hay razón para cambiarlo. Algunos son un poco mejores que otros en términos de sensibilidad y capacidad para descartar marcos malformados, pero estas diferencias no son críticas. Si está por comprar un nuevo adaptador, no le recomendaríamos comprar una tarjeta 802.11b, dado que los estándares 802.11g y 802.11a se están haciendo más y más populares. La mejor opción sería un adaptador CardBus de banda dual y de tres modos, tales como D-Link AirPremier DWL-AG660, NETGEAR WG511U, o Proxim ORiNOCO ComboCard 8480. Generalmente, los adaptadores CardBus muestran mejor rendimiento que los adaptadores PCI.

P. ¿Cuáles adaptadores soportados tienen conectores de antena externa?

R. por lo que sabemos, el único adaptador soportado que tiene un conector es el Proxim ORiNOCO 802.11b/g ComboCard Gold 8470. No sabemos de ninguna tarjeta a/b/g con conectores.

Q. Estoy tratando de instalar el controlador de CommView for WiFi para mi adaptador, pero la ventana de instalación muestra el siguiente mensaje de error: El nombre ya está en uso tanto como nombre de servicio o un nombre de muestra de servicio." ¿Podrían ayudarme?

A. Si. Este mensaje podría aparecer cuando está tratando de instalar el controlador CommView for WiFi para más de un adaptador, o cuando reemplaza un Viejo adaptador por uno nuevo (por ejemplo tiene una tarjeta 802.11b, y ahora desea usar CommView for

WiFi con una nueva tarjeta 802.11g). Debe asegurarse que el controlador es usado solamente por una tarjeta. La siguiente respuesta le dirá como.

P. he estado usando mi adaptador con CommView for WiFi por un tiempo, pero ahora compré un nuevo adaptador y deseo reemplazar el Viejo. ¿Cómo lo hago?
R. Debe asegurarse que su controlador es usado por solamente una tarjeta. Por favor siga los siguientes pasos:

- Abra el registro con REGEDIT.
- Ubique la siguiente rama de registros: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.
- Busque las siguientes claves en esta rama: COMMCS, COMMPR, COMMIPW, COMMIWI, y COMMSYM. Borre estas claves si las encuentra (normalmente debería encontrar solo una de ellas).
- Reinicie la computadora.

Ahora puede seguir adelante con la instalación del controlador de CommView for WiFi, como lo indica la Guía de Instalación del Controlador.

P. ¿Soporta el programa el modo 802.11a Turbo?
R. Si, si su adaptador lo soporta. Algunos de los adaptadores que soportan el modo 802.11a Turbo son Linksys WPC55AG y NETGEAR WAG511.

P. Algunos de los canales en la ventana de opciones de explorador está griseado. ¿Es esto normal? ¿Qué sucede si deseo monitorear estos canales?
R. Dependiendo de su país, su adaptador inalámbrico podría no soportar todos los canales mostrados en la ventana. Los canales que están disponibles para usar en un país determinado difieren de acuerdo a las regulaciones de ese país. En los Estados Unidos, por ejemplo, las regulaciones FCC solo permiten que los canales 1 a 11 sean usados en la banda 802.11b/g. La lógica de los adaptadores inalámbricos que se venden en USA están típicamente configurados para deshabilitar los canales 12 y 13. Esto no siempre es conveniente, dado que si tiene que viajar a otras partes del mundo y podría monitorear canales disponibles localmente con CommView for WiFi. Podría desear comprar un adaptador localmente, pero también puede usar el utilitario que le permite cambiar el dominio regulatorio y el código de país para algunos adaptadores. Antes de descargar y usar el utilitario, por favor advierta:

- Sobrescribir el dominio regulatorio y las preferencias de país podría dañar permanentemente el dispositivo. Proceda a su propio riesgo.
- Cambiando el dominio regulatorio t las preferencias de país podría no ser legal en su país. Consulte al departamento legal de su compañía.
- No hay soporte técnico disponible para este utilitario.
- Este utilitario SOLO funciona con adaptadores 802.11 b/g y 802.11 a/b/g basados en el conjunto de chips Atheros.

Para descargar el utilitario, pulse aquí.

P. Cuando monitoreo una WLAN, puedo estar seguro que el programa capturará cada paquete que se envía o recibe?
R. No, y aquí está el porqué. Cuando una estación inalámbrica esta conectada y autenticada, la estación y el(los) punto(s) de acceso emplean un mecanismo que les permite reenviar los paquetes que no fueron recibidos por la otra parte o dañados en el camino por alguna razón (por ejemplo interferencia de radio). En el caso de CommView for WiFi, el adaptador inalámbrico es colocado en modo pasivo de monitoreo. Por lo tanto, el adaptador no puede enviar “pedidos” para que los paquetes sean reenviados, ni puede informar la recepción satisfactoria de paquetes. Esto lleva a la pérdida de algunos paquetes. El porcentaje de paquetes perdidos podría variar. Generalmente, cuanto más cerca está de otras estaciones o puntos de acceso, menos paquetes perderá.

P. ¿Puede el programa descifrar paquetes cifrados WPA?
R. Si, en el modo WPA-PSK (son soportados TKIP y AES (a.k.a. CCMP)). CommView for WiFi es el primero y el único analizador de red inalámbrica que soporta descifrado WPA/WPA2. Otros productos solo pueden descifrar WEP.

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, seleccionado el canal, comenzado la Captura, pero ningún paquete es mostrado. ¡¡¡Ayuda!!!
R. Primero, cambie a la pestaña **Paquetes**. La pestaña **Últimas Conexiones IP** podrían estar vacías si no ingresa las claves WEP correctas, y su WLAN usa cifrado WEP. Si la pestaña **Paquetes** también está vacía, mire la barra de estado del programa. Si el contador de paquetes está incrementándose, entonces tiene reglas activas que impiden que el programa muestre paquetes. Pulse **Reglas => Restaurar Todo**, y luego presione tres botones de la barra de herramientas: **Capturar Paquetes de Datos**, **Capturar Paquetes de Administración,** y **Capturar Paquetes de Control.** Si el contador de paquetes en la barra de estado no se está incrementando, entonces probablemente no hay estaciones inalámbricas o puntos de acceso activos disponibles/detectados. Si está absolutamente seguro que hay estaciones inalámbricas o puntos de acceso, infórmenos el problema.

P. ¿Puede CommView for WiFi leer archivos de registro NCF generados por la edición estándar no inalámbrica de CommView? ¿Y al revés?
R. Si, CommView for WiFi puede leer archivos de registro NCF generados por la versión estándar, no inalámbrica de CommView. La edición estándar, no inalámbrica de CommView puede leer archivos de registro NCF generados por CommView for WiFi, pero (a)

necesita CommView 4.0 Build 321 o superior, y (b) no podrá ver columnas específicas de l inalámbrico, tales como fuerza de señal, o número de clave WEP.

P. ¿Funciona CommView for WiFi en computadoras con procesadores múltiples?
R. Si, funciona.

P. Mi software de firewall me alerta que CommView for WiFi 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 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.

Q. ¿Podrían guiarme a Buenos recursos en línea sobre redes inalámbricas, su seguridad y configuración?
A. a continuación encontrará algunos Buenos enlaces. Algunos serán interesantes para usuarios principiantes, mientras que otros proveen información profunda para profesionales:

Wireless Ethernet LAN - General 802.11/802.11b FAQ
http://support.intel.com/support/network/wireless/sb/CS-008409.htm
Wi-Fi Planet Tutorials
http://www.wi-fiplanet.com/tutorials/
IEEE Wireless Standards Zone
http://standards.ieee.org/wireless/
WPA Wireless Security for Home Networks
http://www.microsoft.com/WindowsXP/expertzone/columns/bowman/03july28.asp
Configuring Windows XP IEEE 802.11b Wireless Networks for the Home and Small Business
http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/wifisoho.mspx
The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards
http://www.sans.org/rr/papers/68/1109.pdf
SAFE: Wireless LAN Security in Depth
http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.pdf

Temas Avanzados

Comprendiendo Errores CRC e ICV

Errores CRC

Cada marco inalámbrico consiste de los siguientes componentes básicos:

- Un encabezado MAC que incluye el protocolo del marco, duración, dirección, e información de control de secuencia.
- Un cuerpo de marco de longitud variable que contiene información específica del tipo de marco.
- Una secuencia de verificación de marco (FCS) que contiene un código de redundancia cíclica de 4 bytes (CRC).

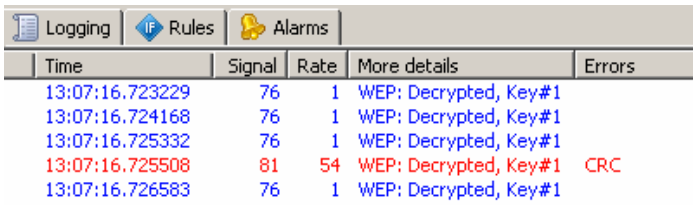
El último componente, FCS, es usado para verificar la integridad del paquete del lado receptor. El lado receptor calcula el valor del CRC sobre el marco recibido y compara el valor calculado con los cuatro bytes reales al final del paquete. Si los valores no coinciden, el paquete es considerado dañado.

La forma en que CommView for WiFi maneja tales marcos corrompidos depende de preferencias definidas por el usuario. Por omisión, tales marcos son ignorados por la aplicación con las siguientes excepciones:

- Incrementan los contadores generales de paquetes y bytes.
- Incrementan el contador de Errores CRC en la pestaña **Canales**.
- Son incluidos en el gráfico Tamaño de Paquete en la ventana de **Estadísticas**.

Los marcos dañados no son contados en otros gráficos y tablas por una razón obvia: Ninguna parte de un marco con un valor CRC erróneo es creíble. Podría tener una dirección IP totalmente equivocada, datos erróneos, etc., a pesar que en la vida real tales marcos soportan un parecido con el original. Por la misma razón los Errores CRC no pueden ser atribuidos a un PA o estación inalámbrica en particular, por lo que es imposible determinar la real dirección física (MAC) del emisor.

Sin embargo, el usuario podría marcar la casilla **Capturar marcos dañados** en las opciones, en cuyo caso los marcos dañados también serán mostrados en la lista de paquetes, por defecto, tales marcos están marcados en rojo y tienen el identificador de "CRC" ,mostrado en la columna **Errores** de la pestaña **Paquetes**:



Es importante comprender que un marco recibido con un error CRC por CommView for WiFi podría haber sido recibido por el nodo de destino sin error. Pese al hecho que los marcos dañados se supone que sean desechados por el nodo destino sin más procesamiento, CommView for WiFi intentará decodificador e incluso descifrar tales marcos.

No todos los adaptadores inalámbricos son capaces de pasar marcos dañados a nivel aplicación. Tal funcionalidad está garantizada solo en los nuevos adaptadores 802.11g y 802.11a/b/g soportados por CommView for WiFi.

Errores ICV

El valor de Verificación de Integridad (Integrity Check Value (ICV)) es un cálculo de verificación de 4 bytes usados en marcos cifrados en WEP- y WPA para verificar los resultados del cifrado. El lado receptor calcula el valor ICV sobre la porción de datos del marco recibido y compara el valor calculado con los cuatro bytes reales en el final de la porción de datos del paquete. Si los valores no coinciden, el descifrado es considerado insatisfactorio.

CommView for WiFi es capaz de descifrado en el aire de WEP y WPA, siempre que las correctas Clave(s) WEP/WPA hayan sido ingresadas por el usuario, el programa mostrara información relativa al ICV en tres lugares distintos: sobre las pestañas **Nodos** y **Canales** y en la columna **Errores** de la pestaña **Paquetes**. La forma en que los errores ICV son mostrados y contados por el programa depende si la clave ha sido ingresada así como en su exactitud, hay distintos casos posibles:

1. Una clave ha sido ingresada por el usuario, y es correcta para la WLAN dada.
2. Una clave a sido ingresada por el usuario, pero es incorrecta para la WLAN dada.
3. No ha sido ingresada ninguna clave.

En el primer caso, debería ver muy pocos errores ICV informados por el programa. En el segundo caso, todos los marcos de datos capturados estarán marcados con el indicador de error ICV dado que los valores de ICV calculados y reales no coinciden si la clave equivocada es usada para el descifrado. En el tercer caso, ningún marco tendrá errores ICV debido a que no se hará ningún intento de descifrar.

Como se explicó arriba, a diferencia de los “fuertes” errores CRC, los errores ICV son “suaves” que dependen de la clave de descifrado. Su WLAN podría estar perfectamente sana, pero si ingresa la clave WEP errónea en CommView for WiFi, observará muchos errores ICV, debido a su “Suavidad”, los paquetes con errores ICV son, por omisión, mostrados en el mismo color que los demás paquetes. Esto puede ser cambiado usando el diálogo Opciones del programa.

Si los marcos tienen un error CRC, detector un error ICV no es un problema. Por lo tanto, CommView for WiFi nunca fija un indicador de error ICV para marcos con errores CRC.

Comprendiendo Descifrado WPA

Como ha sido mencionado a lo largo de esta documentación del producto, CommView for WiFi es capaz de descifrar tráfico de red cifradas en WEP- y WPA en el aire. Para aprovechar totalmente esta funcionalidad, debería tener un buen conocimiento de los principios criptográficos subyacentes.

WEP (**Wired Equivalent Privacy (Privacidad equivalente a conectado)**) es un mecanismo usado para proveer seguridad de datos en redes inalámbricas. WEP le permite al administrador definir un conjunto de claves (o solo una clave) para la WLAN. Estas claves son compartidas entre los clientes y puntos de acceso y son usados para cifrar datos antes de transmitirse. Si un cliente no tiene la clave WEP correcta, no puede descifrar los paquetes recibidos o enviar datos a otros clientes. Lo cual evita el acceso no autorizado de la red y escuchas furtivas. El descifrado WEPT es más que directo si tiene la clave correcta. El WEP es un sistema de cifrado estático y sin nacionalidad, lo que significa que una vez que ingreso la clave correcta en el diálogo Claves WEP/WPA, CommView for WiFi será capaz inmediatamente de descifrar paquetes.

WPA (Wi-Fi Protected Access (Acceso WiFi Protegido)) viene como un reemplazo para el menos seguro estándar WEP, WAP soluciona muchos de los problemas de seguridad y privacidad WEP, incrementa significativamente el nivel de protección de datos y control de acceso para WLANs. A diferencia de WEP, WPA es un sistema de cifrado dinámico que usa la re-clave, clave exclusiva por estación, y un número de otras medidas para mejorar la seguridad. WPA posee dos modos, PSK (Pre-Shared Key (clave pre-compartida)) y Corporativa, la cual difiere en varias formas. CommView for WiFi soporta descifrado de WPA en modo PSK.

Dada la naturaleza dinámica del cifrado WPA, solo conociendo la frase contraseña WPA no le permite descifrar tráfico inmediatamente después de ingresar la frase contraseña correcta. Para poder descifrar tráfico cifrado en WPA, CommView for WiFi debe estar funcionando y capturando datos durante la fase de intercambio de clave (El intercambio de clave se lleva a cabo usando el protocolo EAPOL). Es importante que todos los paquetes EAPOL de intercambio de claves sean capturados satisfactoriamente. Un paquete EAPOL dañado o faltante hará imposible para CommView for WiFi descifrar paquetes que serán enviados/recibidos de la estación dada, y podría requerirse capturar la siguiente conversación EAPOL entre una PA y una estación. Esta es una diferencia importante entre las formas en que los tráficos WEP y WPA son descifrados.

Los principios explicados arriba significan que una vez que ha ingresado la frase contraseña WPA, cerrado el diálogo Claves WEP/WPA, y comenzado a capturar paquetes, necesitará esperar hasta la siguiente autenticación y evento de intercambio de clave antes que los paquetes puedan ser descifrados para la estación que ha sido autenticada. Naturalmente, no es raro que el programa pueda descifrar paquetes desde/hacia un cliente, pero no desde hacia otro, dado que podría no haber capturado todavía paquetes EAPOL para todos los clientes.

La Re-autenticación podría ser disparada usando la herramienta Reasociación de Nodo, reiniciando el PA (para todas las estaciones autenticadas) o reconectando a la red (para el cliente dado).

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.

Ejecución CommView for WiFi 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 NT/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 for WiFi 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 for 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.

Una versión completamente funcional, irrestricta del programa puede ser comprada por US$499.

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

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

Más información

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.

Más información

DigiSecret

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

Más información

CommTraffic

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

Más información