
K-LAB®
GENERADOR DE INTELIGENCIA

FUNCIONAMIENTO DE K-LAB®

Captura, procesa y almacena la actividad de los usuarios en la red de la organización.

Permite la búsqueda, reconstrucción y visualización de los datos auditados a través de una interfaz gráfica amigable, con el fin de generar inteligencia oportuna que permita mitigar riesgos.

PROTOCOLOS CAPTURADOS

MENSAJERÍA INSTANTÁNEA
Soporte para MSN Messenger, IRC y XMPP

CORREOS SALIENTES (SMTP)
Mensajes y archivos adjuntos

CORREOS ENTRANTES (POP3 e IMAP4)
Mensajes, contraseñas y archivos adjuntos

SESIONES TELNET (TN3270, entre otros)
Sesiones de usuario bi-direccionales con AS400

HTTP (Navegación Páginas Web)

SSL (Secure Socket Layer)
Utilizando una implementación específica en la red

DATAGRAMAS IP PUROS
Para la detección de amenazas de distintos tipos

CAPTURA EN FORMATO PCAP
Configurable para cumplir con regulaciones

MOTORES DE BÚSQUEDA WEB
google.com, altavista.com ,yahoo.com, entre otros.

DIFERENCIADORES COMERCIALES

•Reglas de captura que disparan automáticamente otras reglas (preestablecidas por el usuario).

• Mapa relacional gráfico de la actividad capturada en la red. (actualizado en tiempo casi- real)

• Reconstrucción y visualización amigable de la información almacenada.

• Búsquedas interactivas sobre los datos capturados

• Motor para la generación de expresiones regulares que permiten detectar palabras mal escritas o patrones de textos alterado a propósito

• Modelos teóricos para la generación y análisis de inteligencia.

• Herramienta pasiva indetectable en la red.

•Captura distribuida posible mediante “probes” o sondas ubicadas remotamente

•Arquitectura cliente-servidor

CARACTERÍSTICAS TÉCNICAS K-LAB®

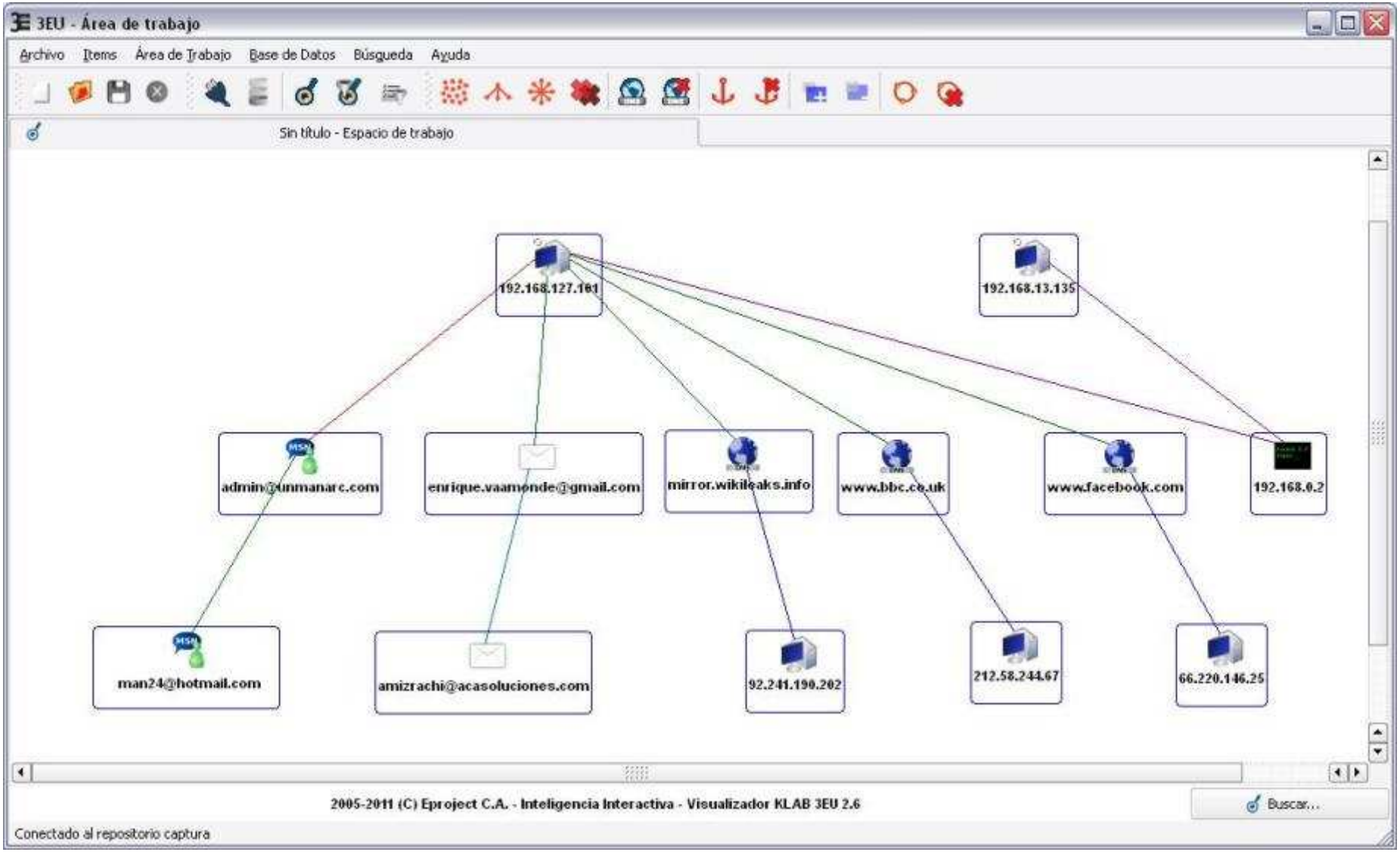
Dispositivo rack-mountable con soporte de 3 Hasta 6 NICs Gigabit Ethernet

Versión GNU/Linux y Windows del Software cliente ThirdEye Utility (3EU).

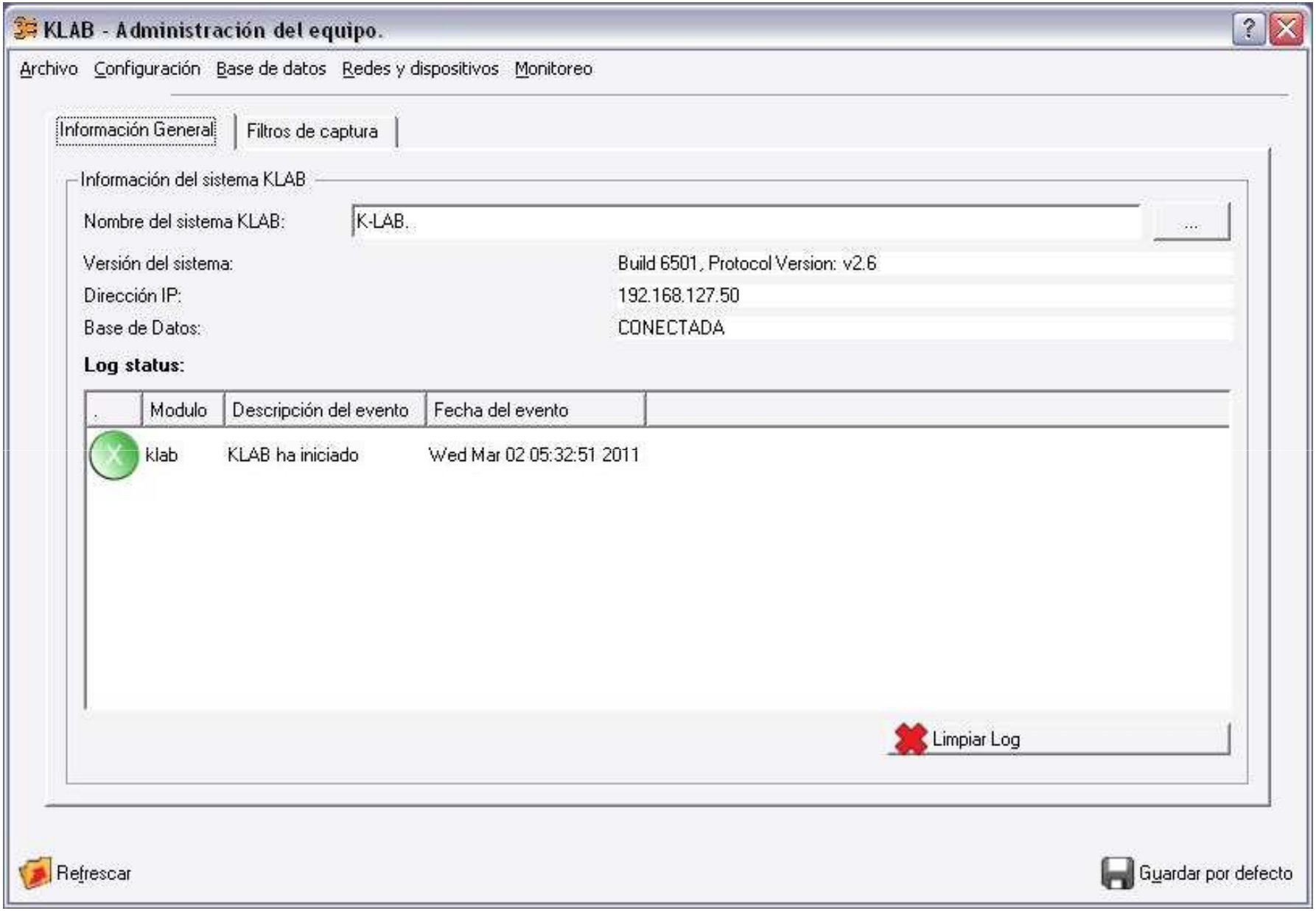
Arquitectura modular permite fácil instalación de actualizaciones y mejoras (por ejemplo: protocolos adicionales de captura).

CAPTURAS DE PANTALLA DE K-LAB®

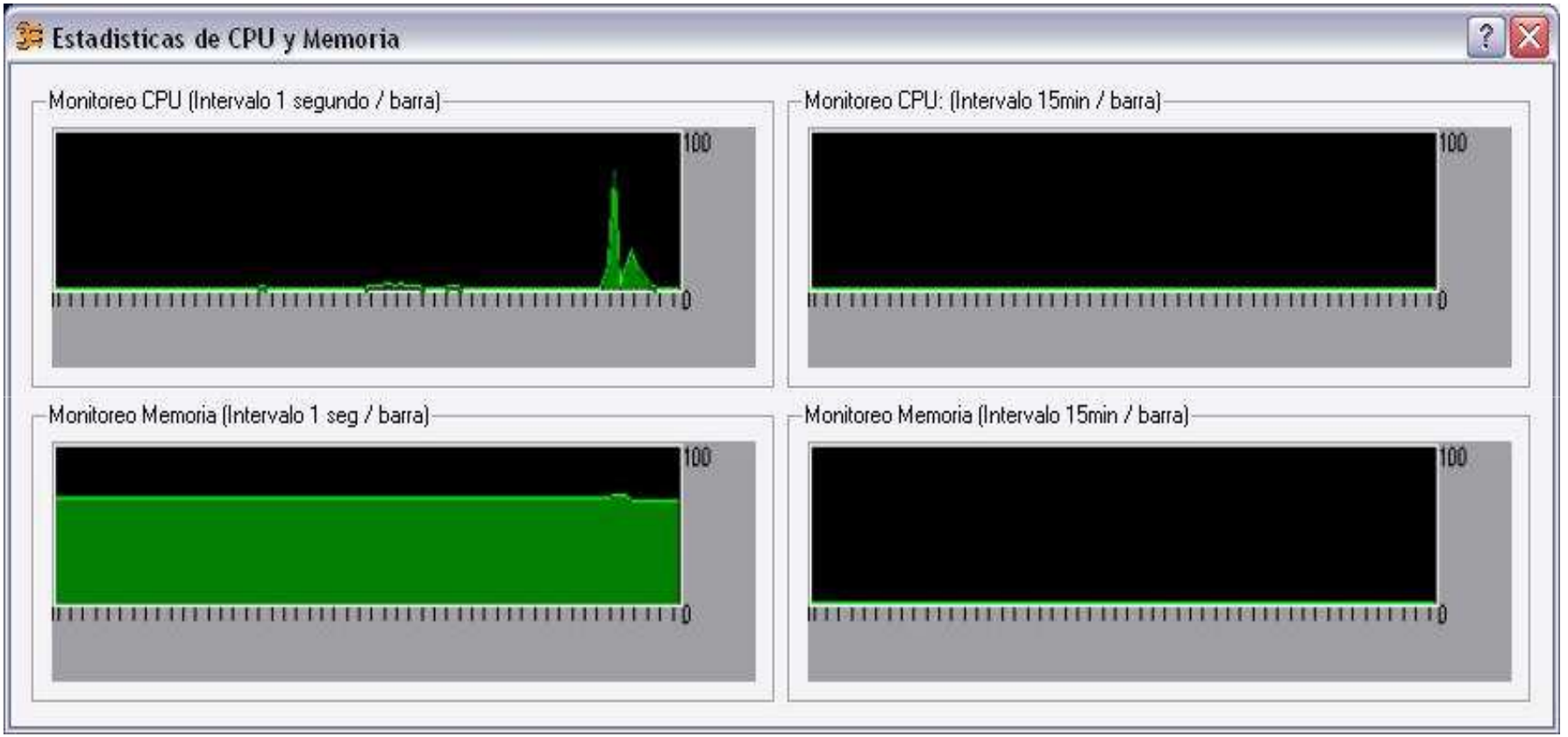
CAPTURAS DE PANTALLA DE K-LAB®



CAPTURAS DE PANTALLA DE K-LAB®

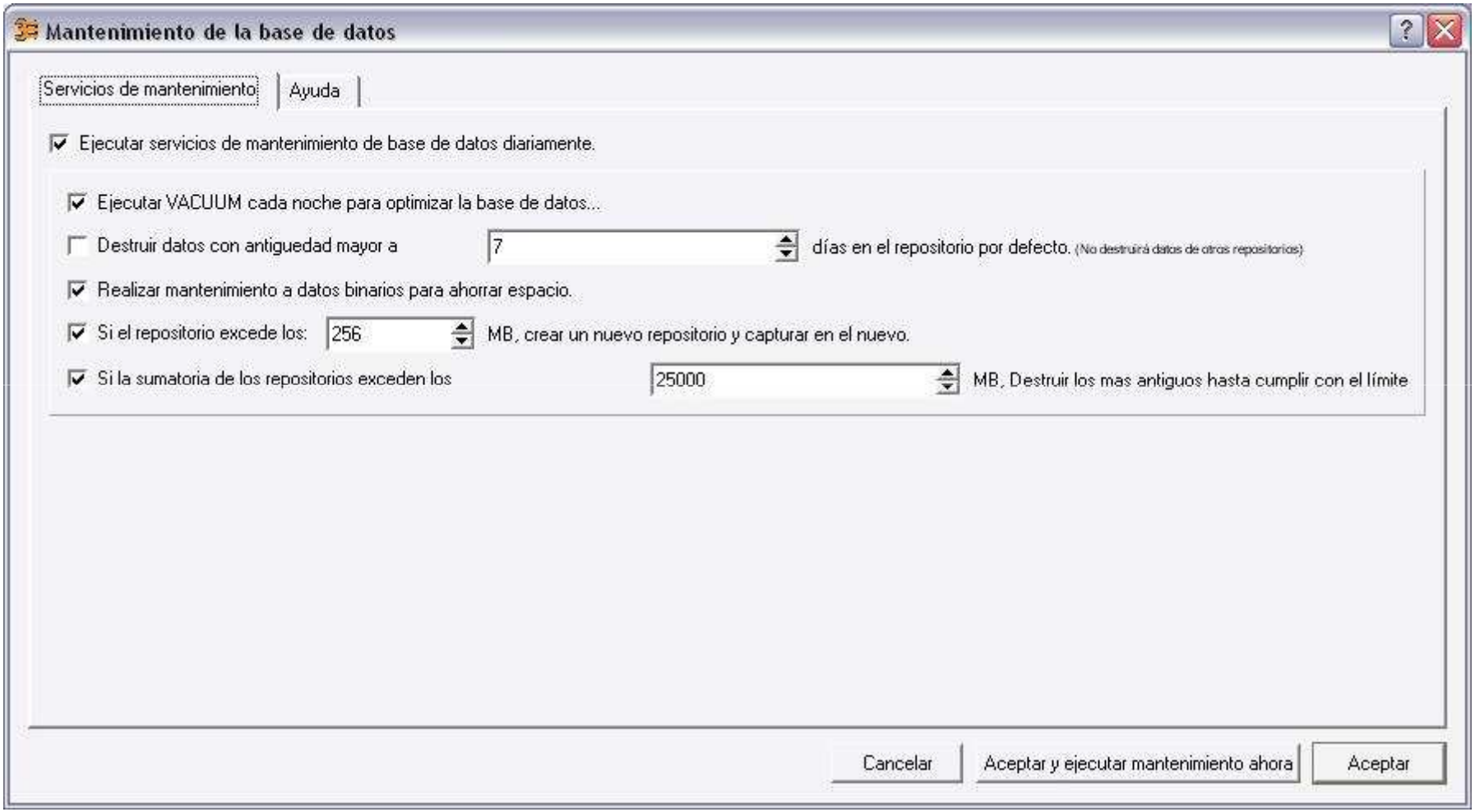


CAPTURAS DE PANTALLA DE K-LAB®

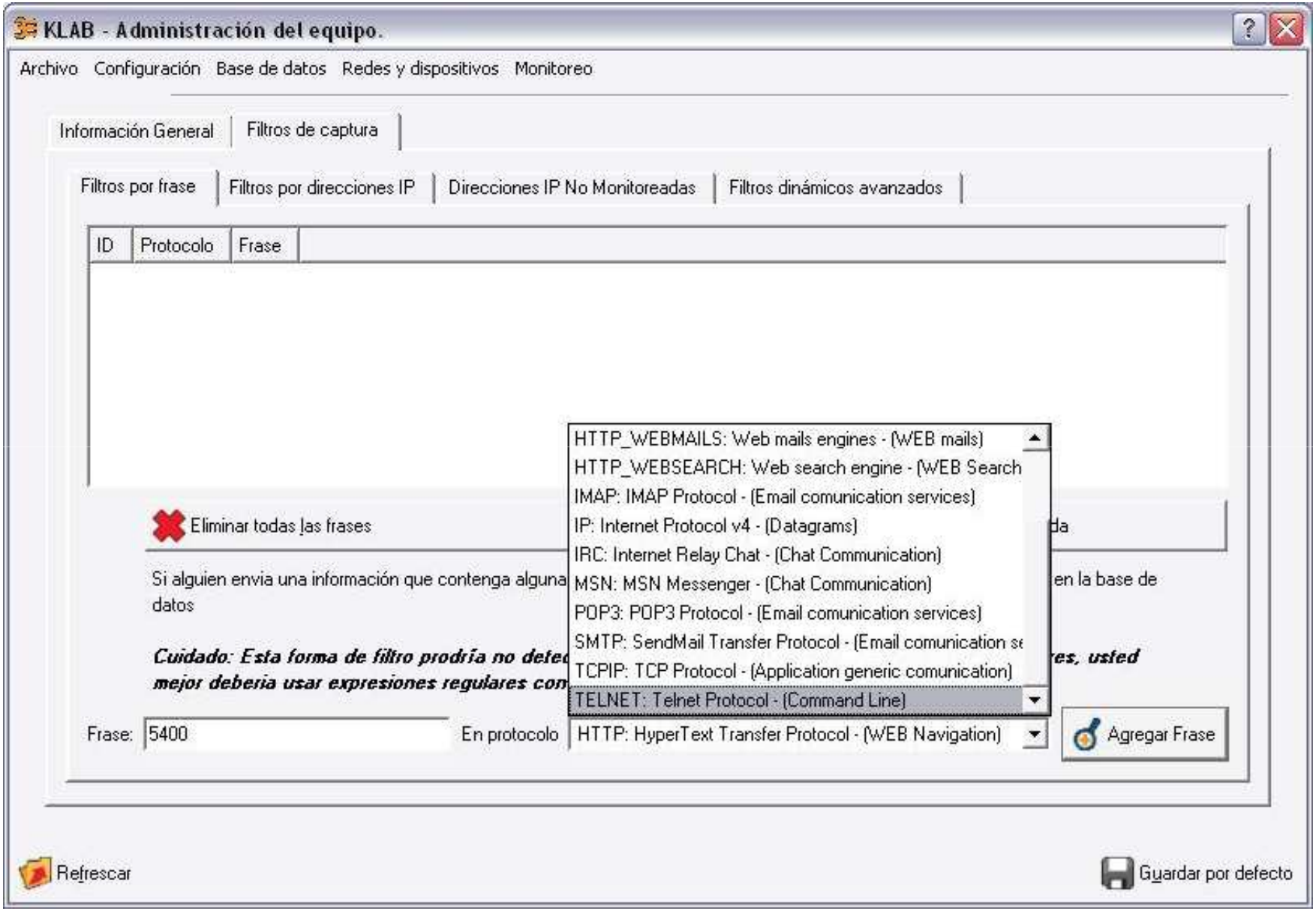


CAPTURAS DE PANTALLA DE K-LAB®

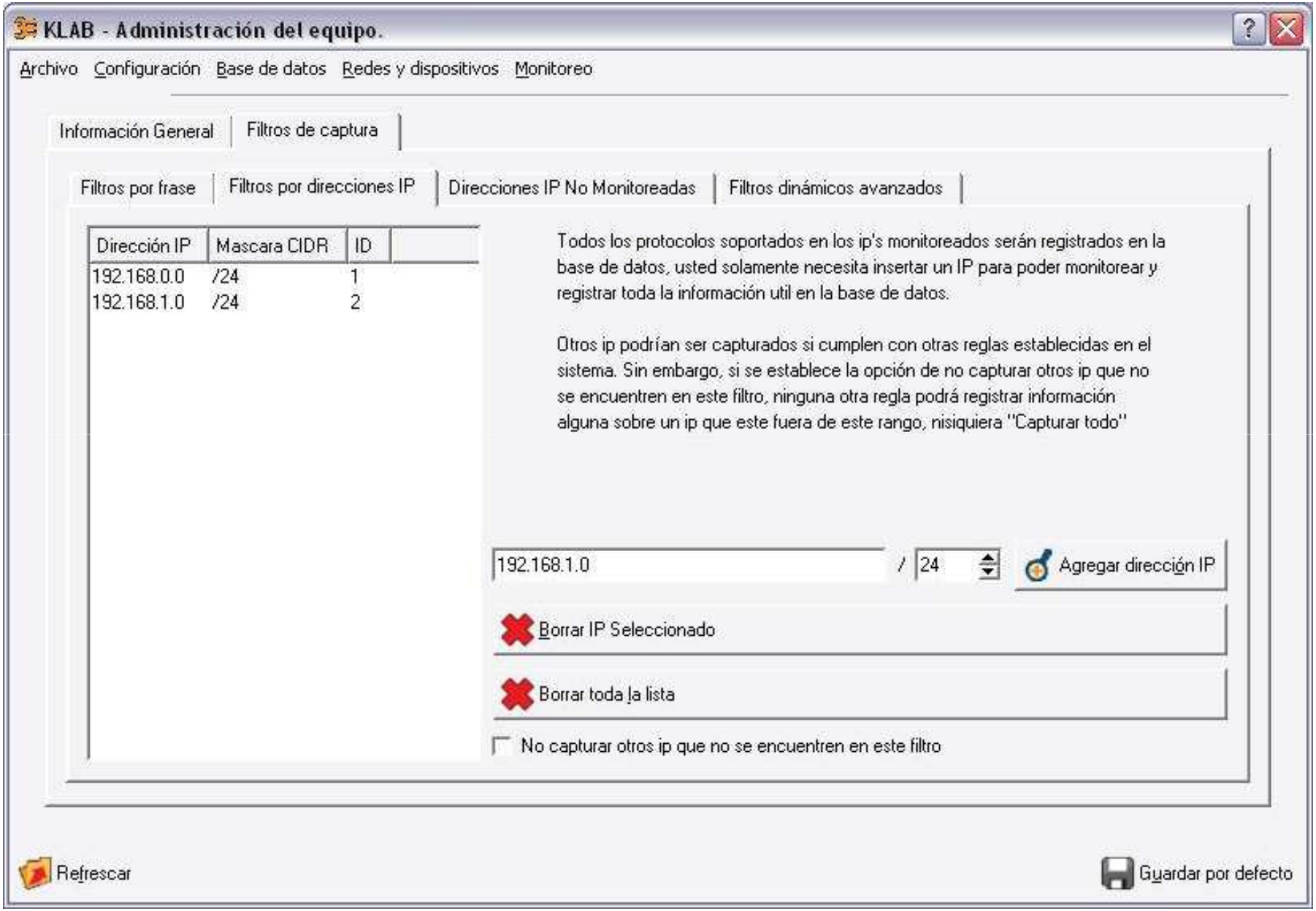
CAPTURAS DE PANTALLA DE K-LAB®



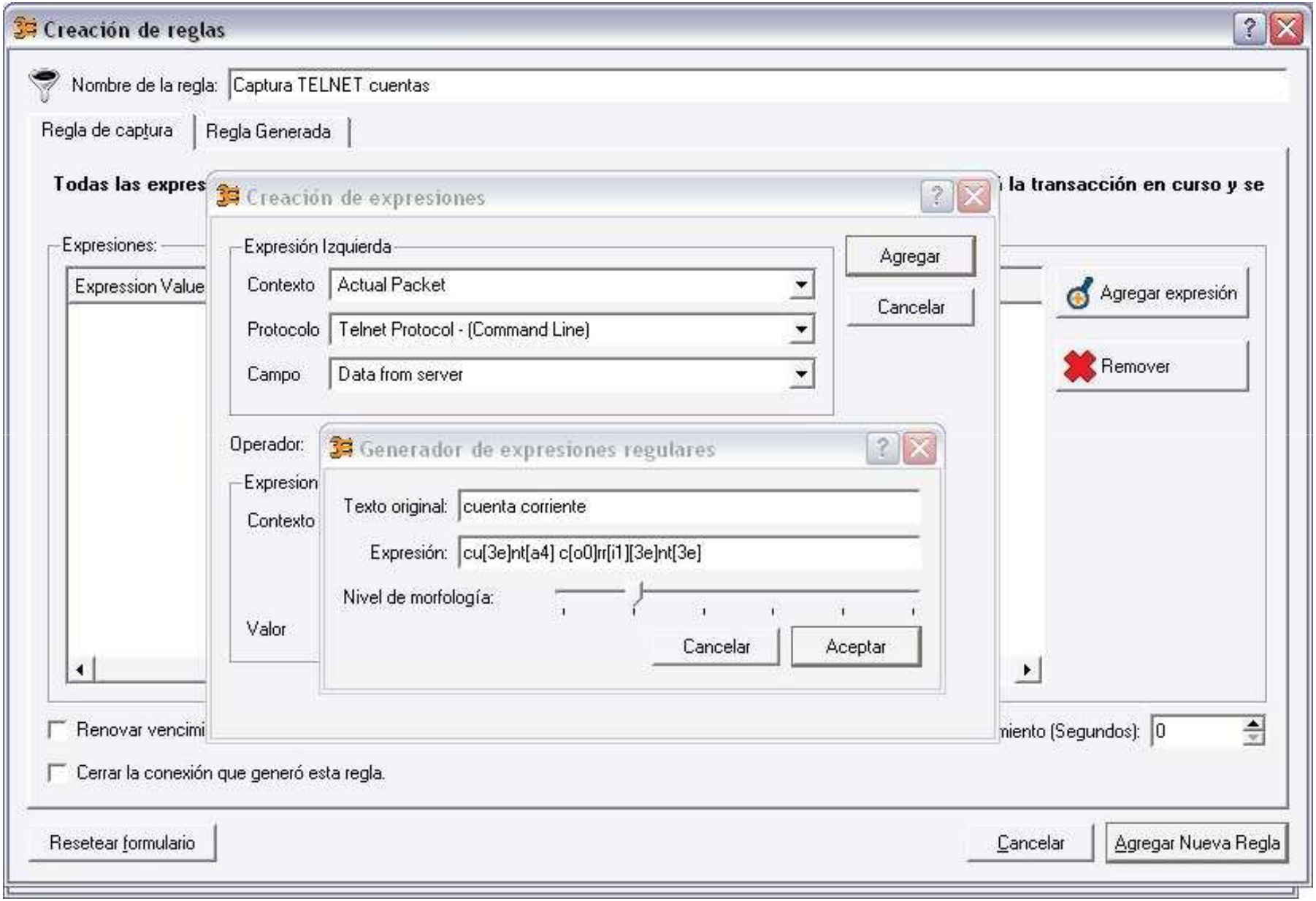
CAPTURAS DE PANTALLA DE K-LAB®



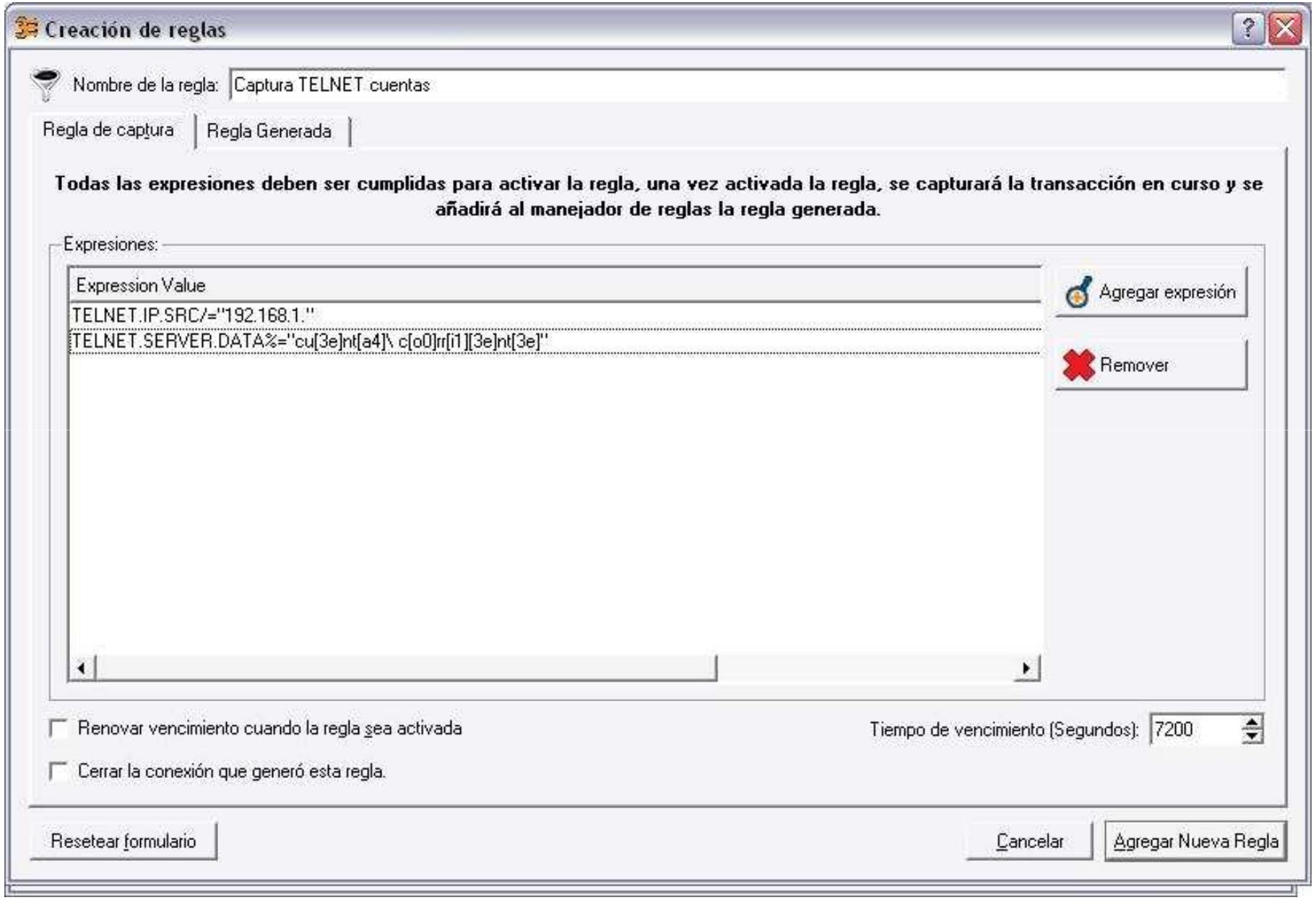
CAPTURAS DE PANTALLA DE K-LAB®



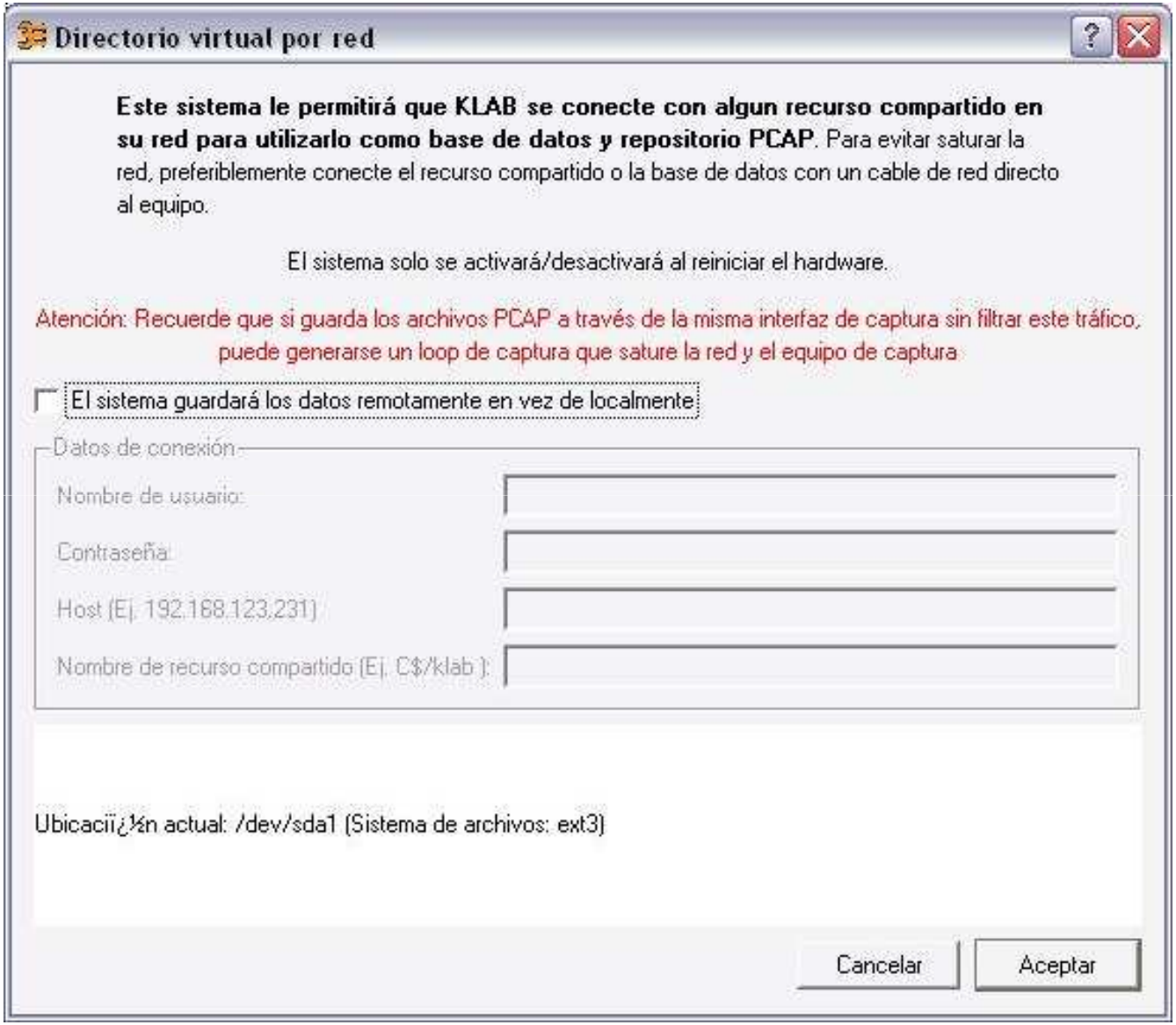
CAPTURAS DE PANTALLA DE K-LAB®



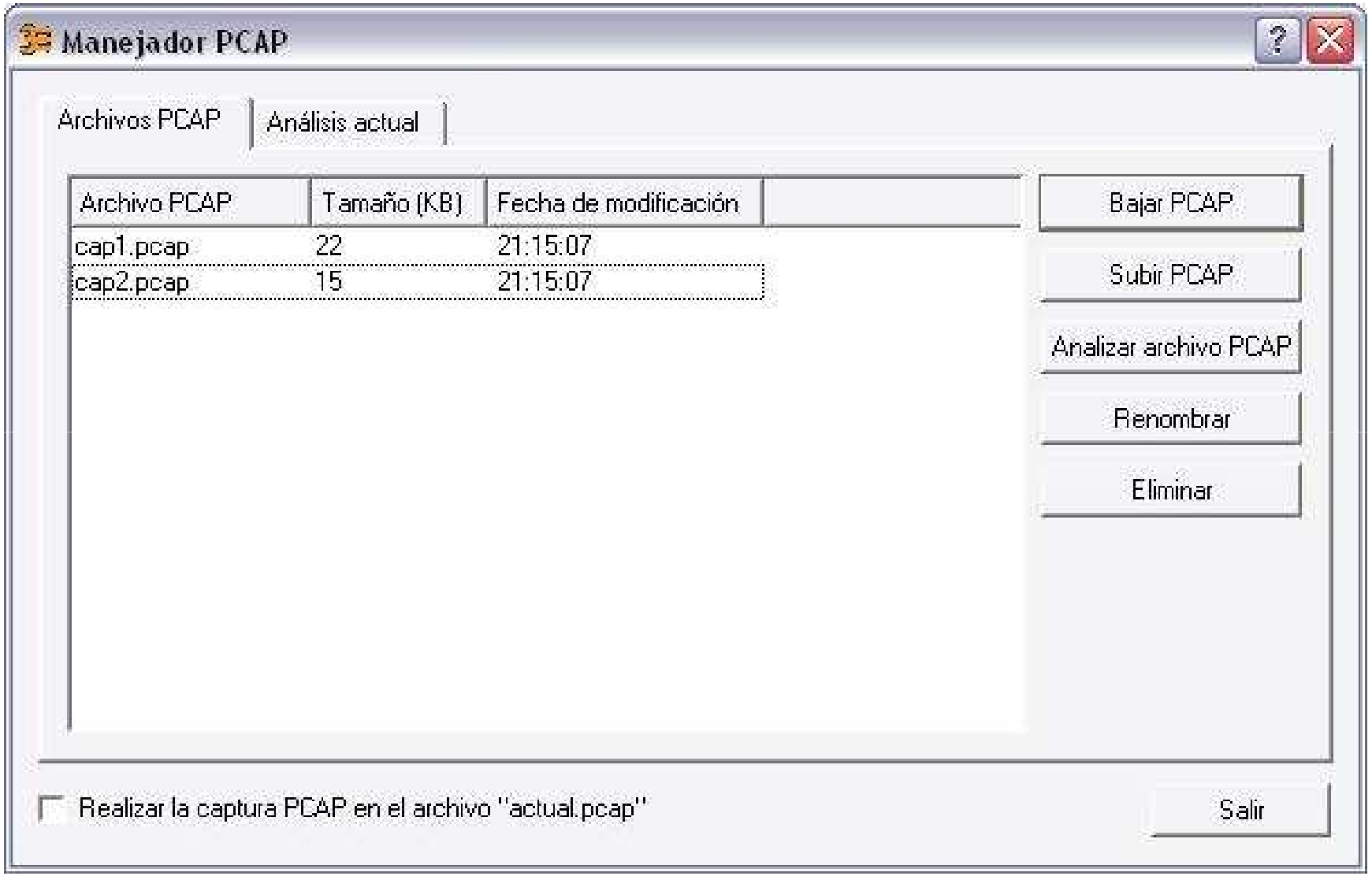
CAPTURAS DE PANTALLA DE K-LAB®



CAPTURAS DE PANTALLA DE K-LAB®

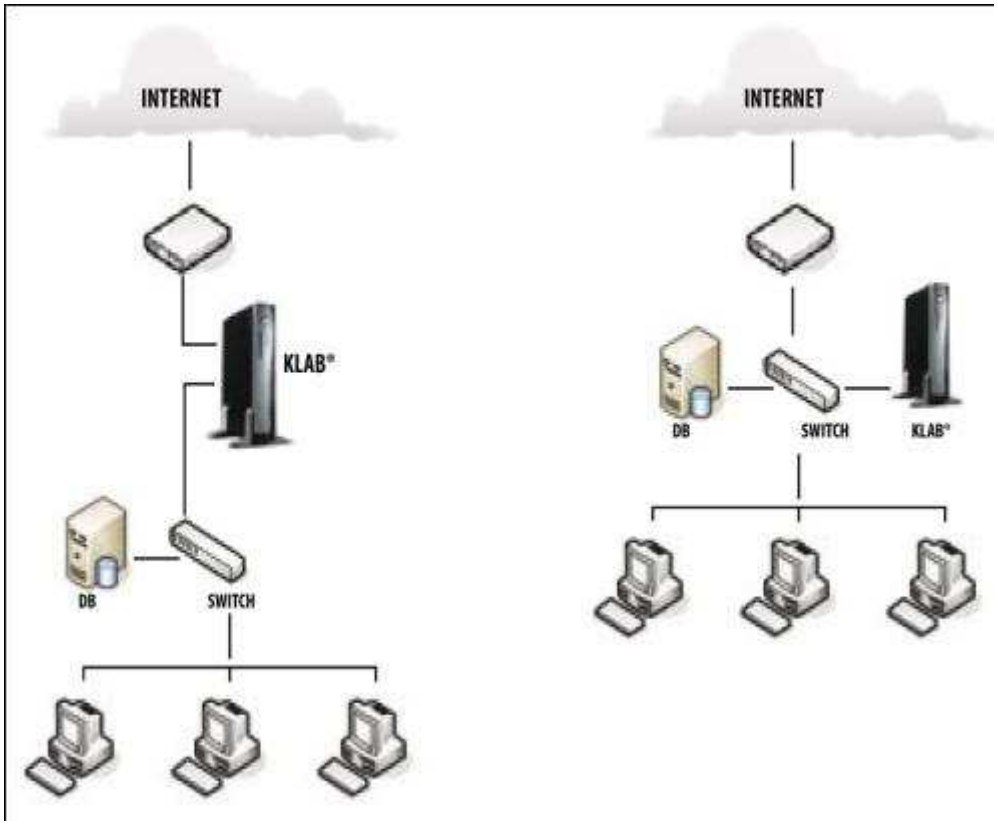


CAPTURAS DE PANTALLA DE K-LAB®



IMPLEMENTACIÓN DE K-LAB® EN LA RED DE LA ORGANIZACIÓN

MODO "BRIDGE"



MODO PUERTO SPAN O UTILIZANDO UN NETWORK TAP

Modo "Bridge" (almacenamiento interno)

Modo puerto SPAN o en segmento de red (almacenamiento interno)


GRACIAS
POR
SU TIEMPO