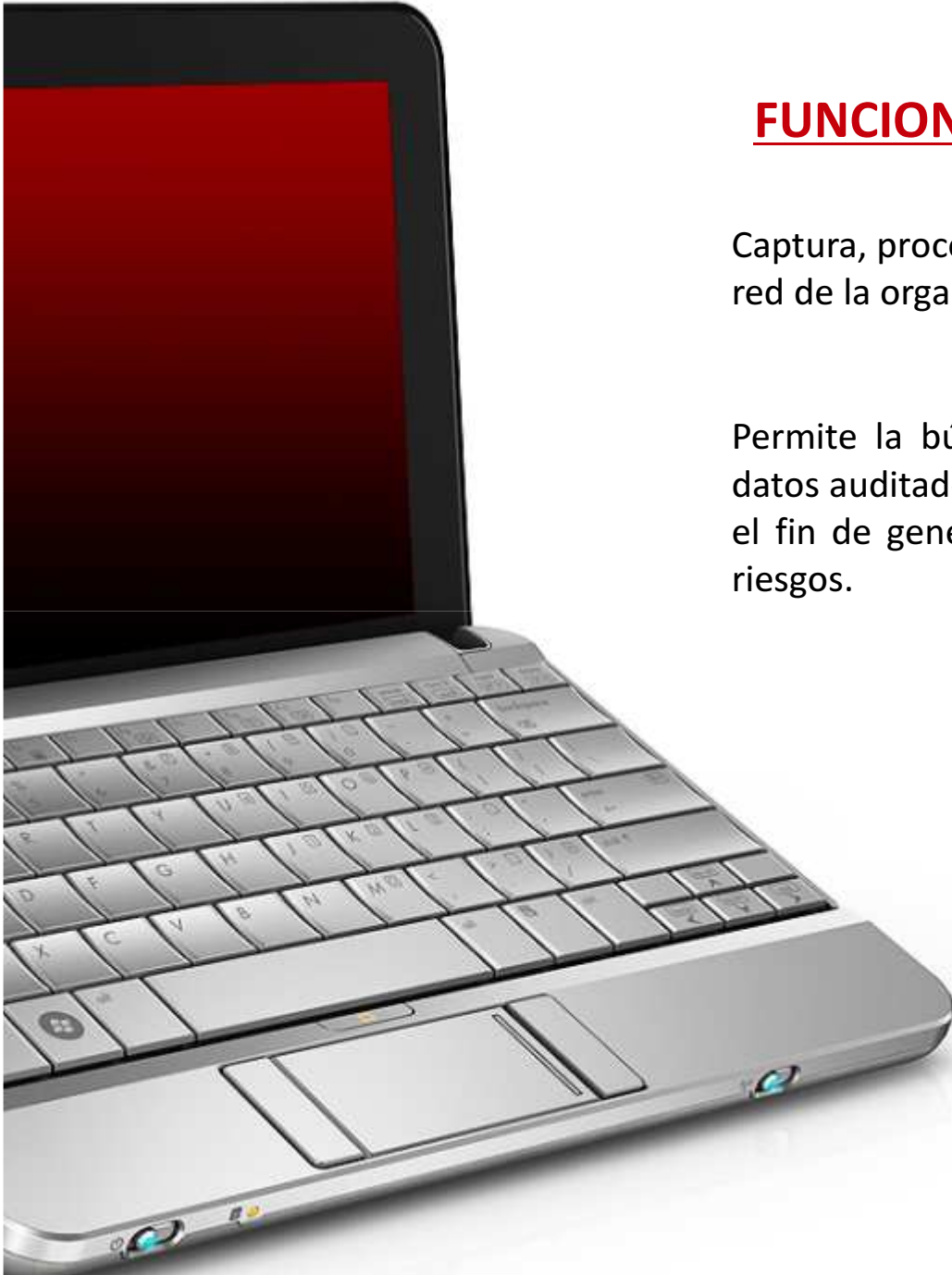


A close-up photograph of a human eye, looking directly at the camera. The eye is the central focus, with the iris and pupil clearly visible. The pupil contains a reflection of a camera lens. The entire image is overlaid with a semi-transparent red filter. The background behind the eye shows fine skin texture and eyelashes.

**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

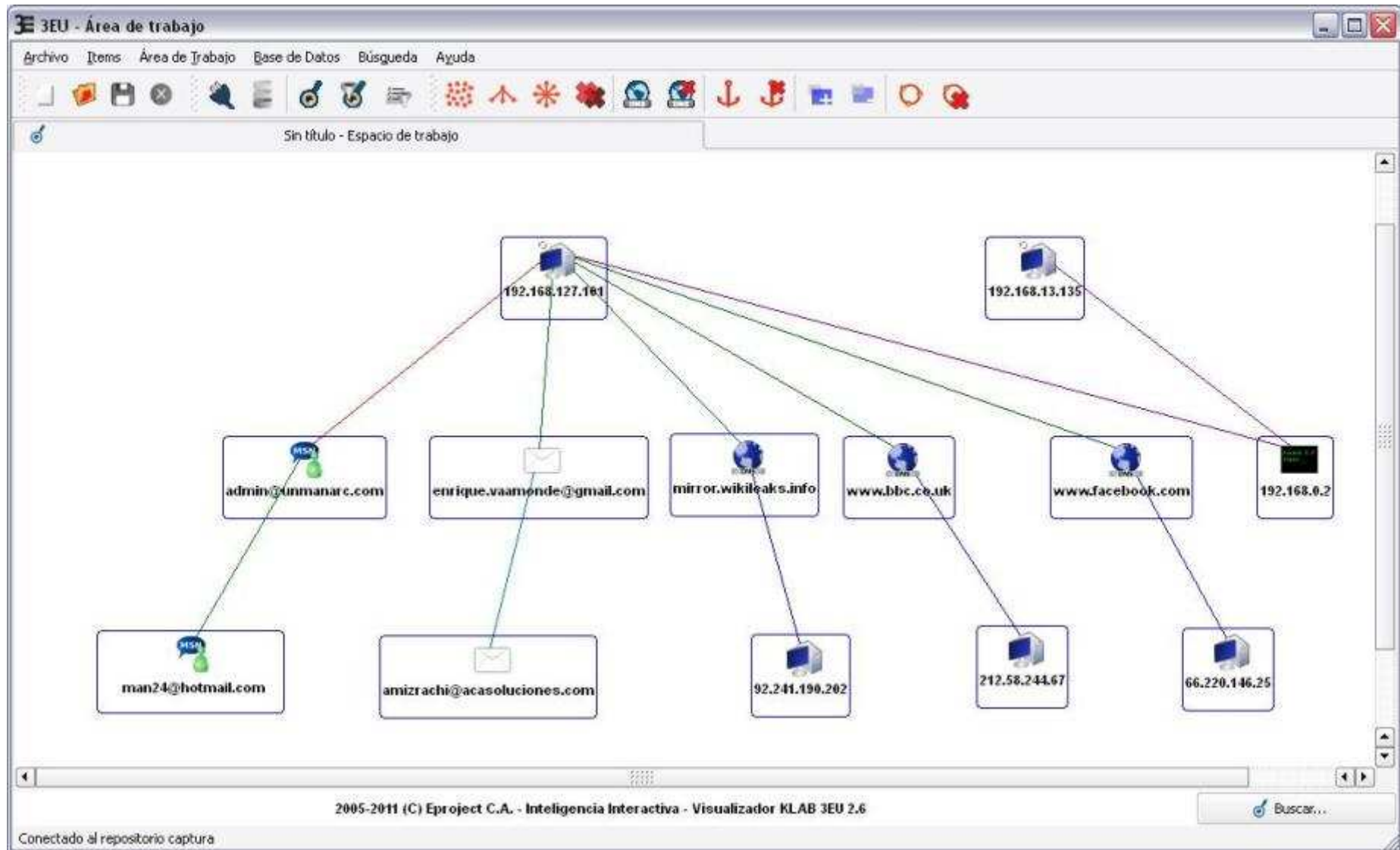
Versión GNU/Linux y Windows del Software cliente ThirdEye Utility (3EU).

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®

Información General | Filtros de captura

Información del sistema KLAB

Nombre del sistema KLAB: K-LAB.

Versión del sistema: Build 6501, Protocol Version: v2.6

Dirección IP: 192.168.127.50

Base de Datos: CONECTADA

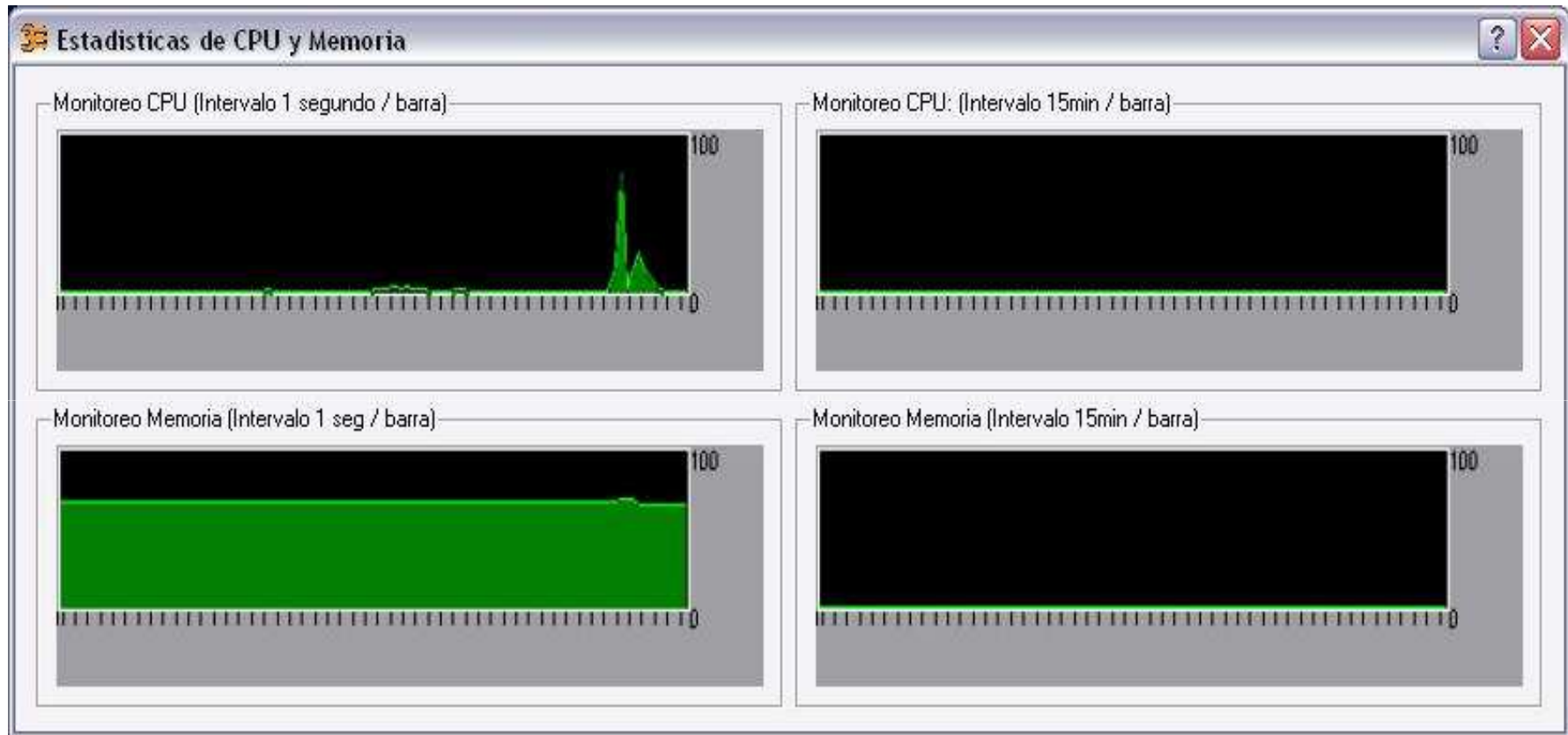
**Log status:**

	Modulo	Descripción del evento	Fecha del evento
	klab	KLAB ha iniciado	Wed Mar 02 05:32:51 2011

Limpiar Log

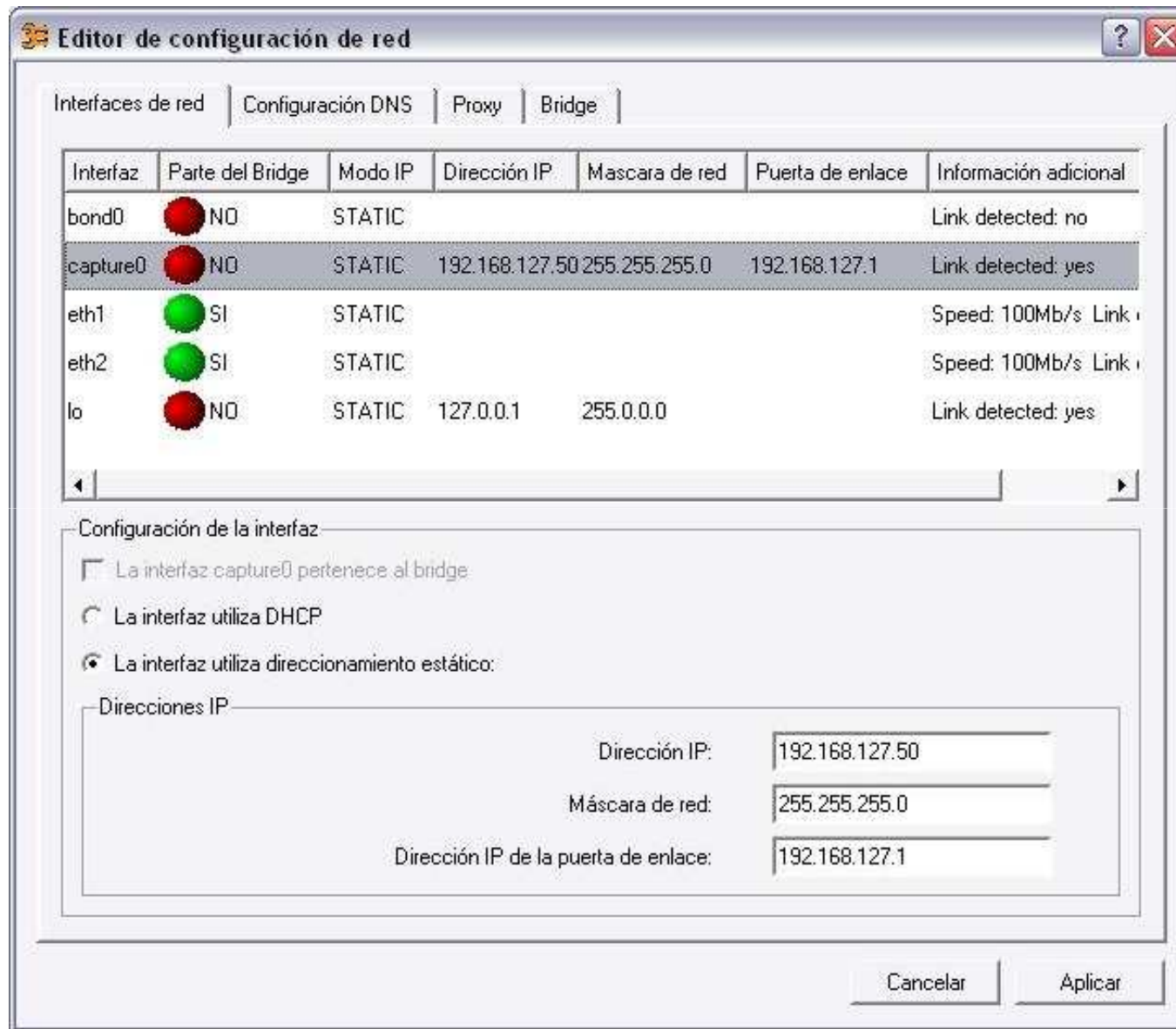
Refrescar Guardar por defecto

# CAPTURAS DE PANTALLA DE K-LAB®





# CAPTURAS DE PANTALLA DE K-LAB®



## CAPTURAS DE PANTALLA DE K-LAB®

**Mantenimiento de la base de datos**

Servicios de mantenimiento | Ayuda

- Ejecutar servicios de mantenimiento de base de datos diariamente.
- Ejecutar VACUUM cada noche para optimizar la base de datos...
- Destruir datos con antigüedad mayor a  días en el repositorio por defecto. (No destruirá datos de otros repositorios)
- Realizar mantenimiento a datos binarios para ahorrar espacio.
- Si el repositorio excede los:  MB, crear un nuevo repositorio y capturar en el nuevo.
- Si la sumatoria de los repositorios exceden los  MB, Destruir los mas antiguos hasta cumplir con el límite

Cancelar | Aceptar y ejecutar mantenimiento ahora | Aceptar

# CAPTURAS DE PANTALLA DE K-LAB®

The screenshot shows the 'KLAB - Administración del equipo' application window. The main menu includes 'Archivo', 'Configuración', 'Base de datos', 'Redes y dispositivos', and 'Monitoreo'. The 'Filtros de captura' tab is active, with sub-tabs for 'Filtros por frase', 'Filtros por direcciones IP', 'Direcciones IP No Monitoreadas', and 'Filtros dinámicos avanzados'. A table with columns 'ID', 'Protocolo', and 'Frase' is present but empty. A dropdown menu is open, listing protocols such as HTTP\_WEBMAILS, HTTP\_WEBSEARCH, IMAP, IP, IRC, MSN, POP3, SMTP, TCP/IP, TELNET, and HTTP. Below the table, there is a red 'X' icon and the text 'Eliminar todas las frases'. A warning message reads: 'Si alguien envía una información que contenga algunos datos. Cuidado: Esta forma de filtro podría no detectar mejor debería usar expresiones regulares con'. At the bottom, there is a 'Frase:' input field containing '5400', an 'En protocolo:' dropdown menu, and an 'Agregar Frase' button. The bottom of the window features a 'Refrescar' button and a 'Guardar por defecto' button.

KLAB - Administración del equipo.

Archivo Configuración Base de datos Redes y dispositivos Monitoreo

Información General Filtros de captura

Filtros por frase Filtros por direcciones IP Direcciones IP No Monitoreadas Filtros dinámicos avanzados

ID	Protocolo	Frase
----	-----------	-------

Eliminar todas las frases

Si alguien envía una información que contenga algunos datos

**Cuidado: Esta forma de filtro podría no detectar mejor debería usar expresiones regulares con**

Frase: 5400 En protocolo

- HTTP\_WEBMAILS: Web mails engines - (WEB mails)
- HTTP\_WEBSEARCH: Web search engine - (WEB Search
- IMAP: IMAP Protocol - (Email communication services)
- IP: Internet Protocol v4 - (Datagrams)
- IRC: Internet Relay Chat - (Chat Communication)
- MSN: MSN Messenger - (Chat Communication)
- POP3: POP3 Protocol - (Email communication services)
- SMTP: SendMail Transfer Protocol - (Email communication se
- TCP/IP: TCP Protocol - (Application generic communication)
- TELNET: Telnet Protocol - (Command Line)
- HTTP: HyperText Transfer Protocol - (WEB Navigation)

Agregar Frase

Refrescar Guardar por defecto

# CAPTURAS DE PANTALLA DE K-LAB®

**KLAB - Administración del equipo.**

Archivo Configuración Base de datos Redes y dispositivos Monitoreo


Información General | Filtros de captura


Filtros por frase | Filtros por direcciones IP | Direcciones IP No Monitoreadas | Filtros dinámicos avanzados


Dirección IP	Mascara CIDR	ID	
192.168.0.0	/24	1	
192.168.1.0	/24	2	

Todos los protocolos soportados en los ip's monitoreados serán registrados en la base de datos, usted solamente necesita insertar un IP para poder monitorear y registrar toda la información util en la base de datos.



Otros ip podrían ser capturados si cumplen con otras reglas establecidas en el sistema. Sin embargo, si se establece la opción de no capturar otros ip que no se encuentren en este filtro, ninguna otra regla podrá registrar información alguna sobre un ip que este fuera de este rango, niquiera "Capturar todo"

192.168.1.0 / 24  Agregar dirección IP

 Borrar IP Seleccionado

 Borrar toda la lista

No capturar otros ip que no se encuentren en este filtro

 Refrescar  Guardar por defecto

# CAPTURAS DE PANTALLA DE K-LAB®

**Creación de reglas**

Nombre de la regla:

Regla de captura | Regla Generada

Todas las expresiones

Expresiones:

- Expression Value

**Creación de expresiones**

Expresión Izquierda:

Contexto:

Protocolo:

Campo:

Agregar

Cancelar

**Generador de expresiones regulares**

Expresión

Contexto

Texto original:

Expresión:

Nivel de morfología:

Valor

Cancelar

Aceptar

Renovar vencimi...

Cerrar la conexión que generó esta regla.

Resetear formulario

Cancelar

Agregar Nueva Regla

tiempo (Segundos):

# CAPTURAS DE PANTALLA DE K-LAB®



**Creación de reglas**

Nombre de la regla:

Regla de captura | Regla Generada

**Todas las expresiones deben ser cumplidas para activar la regla, una vez activada la regla, se capturará la transacción en curso y se añadirá al manejador de reglas la regla generada.**

Expresiones:

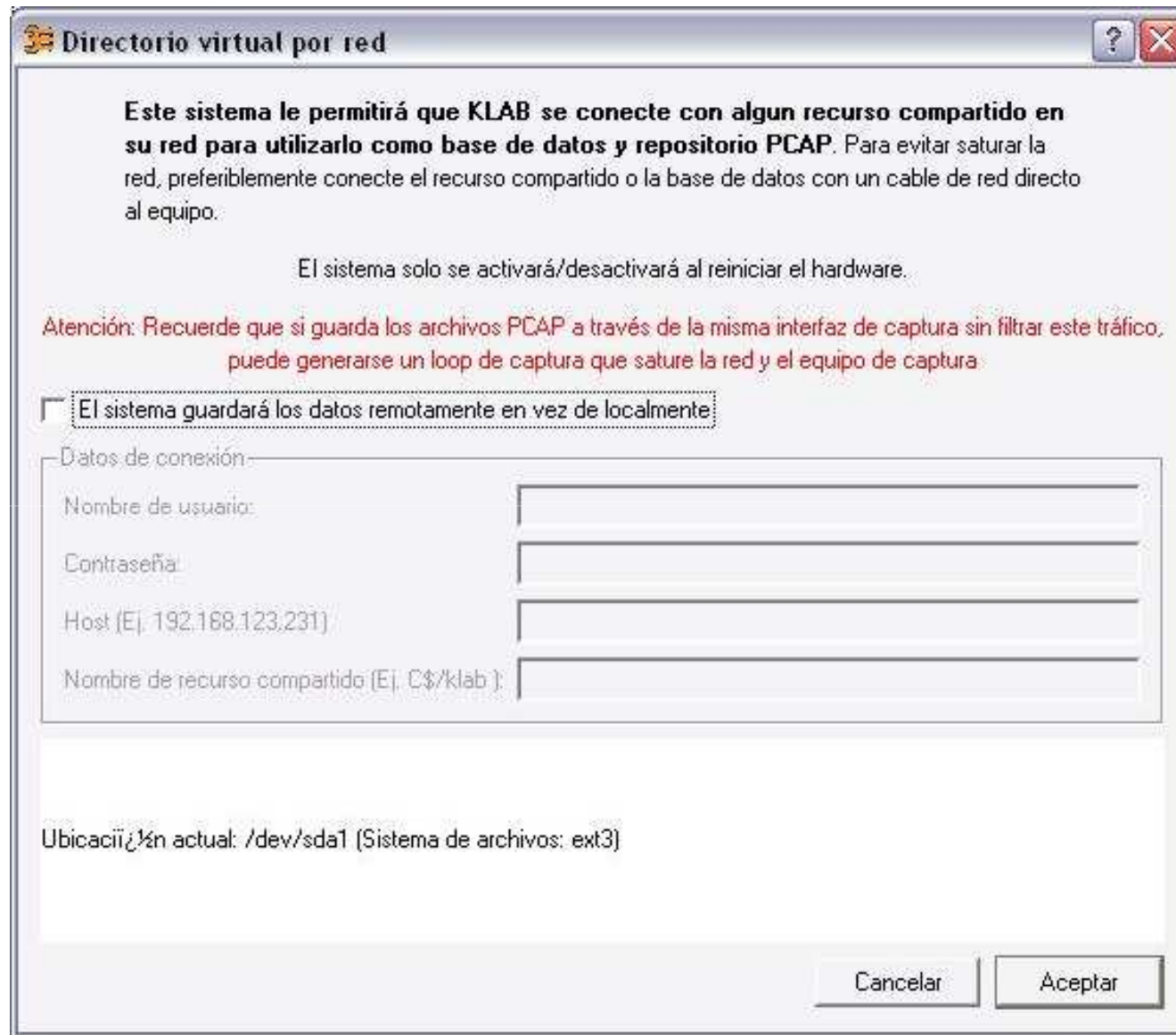
Expression Value	
TELNET.IP.SRC/="192.168.1."	 Agregar expresión
TELNET.SERVER.DATA%="cu[3e]nt[a4]\ c[o0]rr[ri ][3e]nt[3e]"	 Remove

Renovar vencimiento cuando la regla sea activada

Cerrar la conexión que generó esta regla.

Tiempo de vencimiento (Segundos):

## CAPTURAS DE PANTALLA DE K-LAB®



**Directorio virtual por red**

Este sistema le permitirá que KLAB se conecte con algún recurso compartido en su red para utilizarlo como base de datos y repositorio PCAP. Para evitar saturar la red, preferiblemente conecte el recurso compartido o la base de datos con un cable de red directo al equipo.

El sistema solo se activará/desactivará al reiniciar el hardware.

Atención: Recuerde que si guarda los archivos PCAP a través de la misma interfaz de captura sin filtrar este tráfico, puede generarse un loop de captura que sature la red y el equipo de captura.

El sistema guardará los datos remotamente en vez de localmente

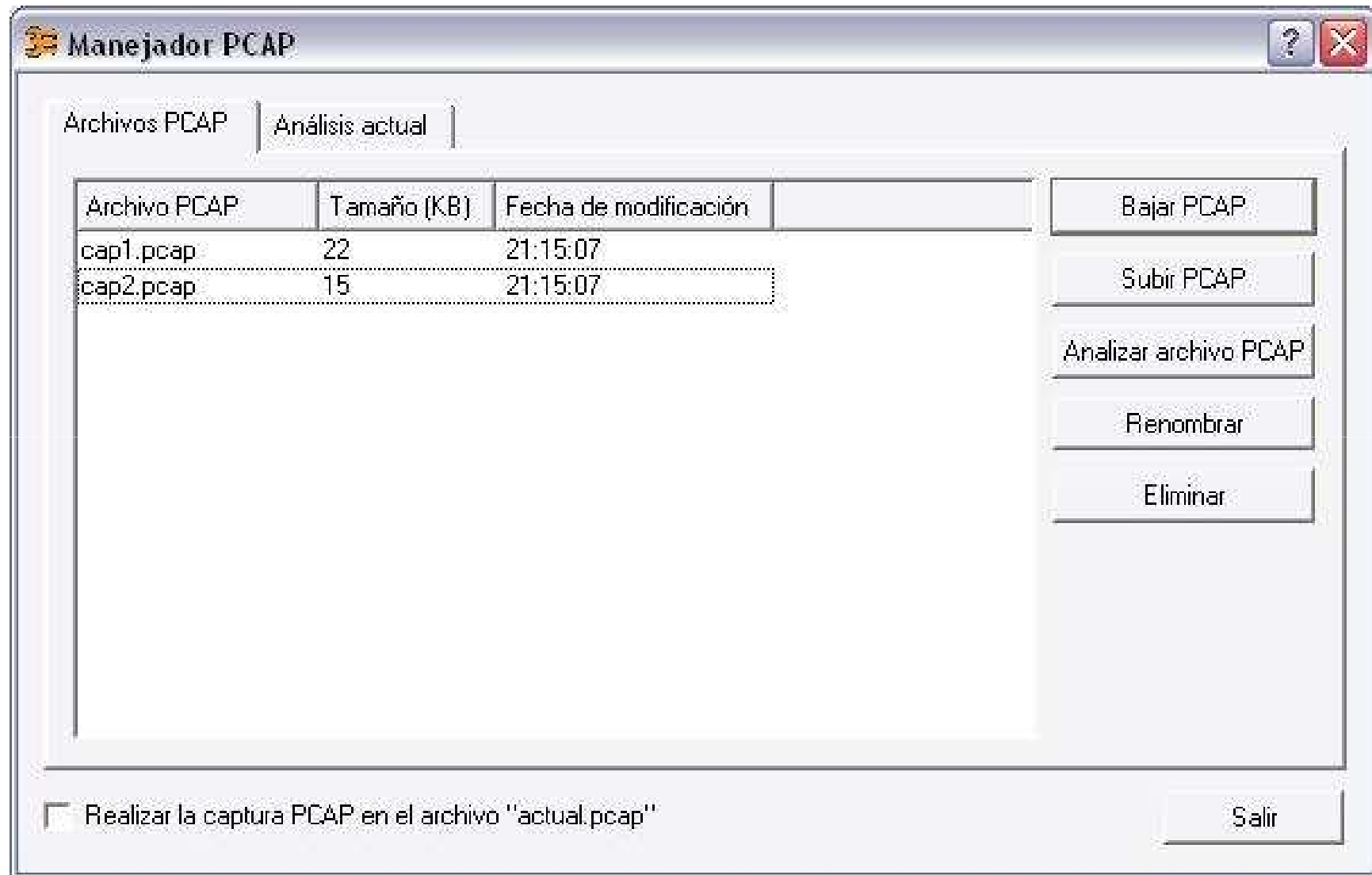
Datos de conexión:

Nombre de usuario:	<input type="text"/>
Contraseña:	<input type="password"/>
Host (Ej. 192.168.123.231):	<input type="text"/>
Nombre de recurso compartido (Ej. C\$/klab):	<input type="text"/>

Ubicación actual: /dev/sda1 (Sistema de archivos: ext3)

Cancelar    Aceptar

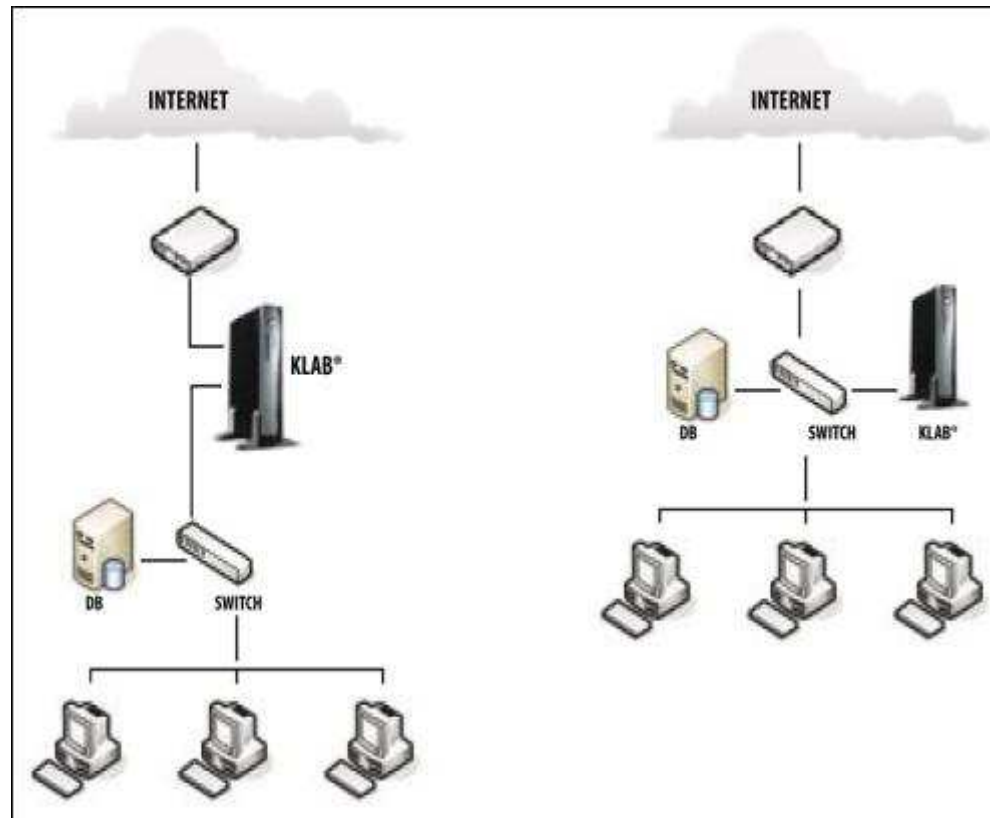
## CAPTURAS DE PANTALLA DE K-LAB®





## 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**