# Analizador de Tráfico de Red

**Ericka Barahona Delgado**

**Paola Gellibert López**

# Objetivos del Proyecto

- El objetivo principal es diseñar e implementar un software que analice el tráfico en una red LAN, con la finalidad de:
  - Brindar seguridad a la red.
  - Conocer  a fondo los posibles problemas de la red.
  - Establecer correcciones o permisos.
  - Filtrar los paquetes de acuerdo a la necesidad de cada usuario.
  - Realizar capturas en tiempo real, control estadístico de los protocolos.
- Además tenemos como objetivo realizar un análisis comparativo entre tres analizadores de red para determinar cual posee el mejor rendimiento.
- Nuestro proyecto tiene como finalidad diseñar esta aplicación para su uso en el ámbito estudiantil.

# Problema

- Con el paso de los años el acceso a las redes crece con más usuarios y estos a su vez, tienen más requerimientos tanto para cargar o descargar información, haciendo que cada día exista más tráfico.

- Debido a este gran incremento de usuarios se deben adoptar soluciones relacionadas con las redes ya que estas sufren de frecuentes congestionamientos, colapsos, o pérdidas de información.

# Redes de Datos

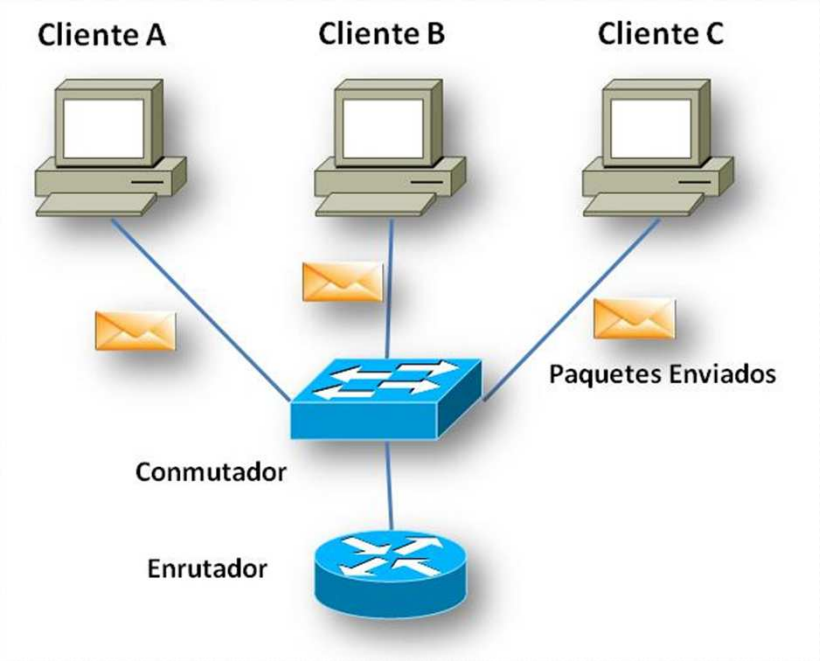
- A diferencia de los circuitos tradicionales de telefonía, las redes de computadores son canales de comunicación compartidos que pueden recibir información de diversos dispositivos.

# Analizador de Tráfico de Red

- En informática es un programa especializado en monitoreo y análisis, que captura tramas o paquetes de una red de datos.
- Software informático que puede interceptar y registrar tráfico de paquetes sobre una red de datos.
- Tiene varios usos como por ejemplo detección de cuello de botella, análisis de falencias en la red, o fines maliciosos.

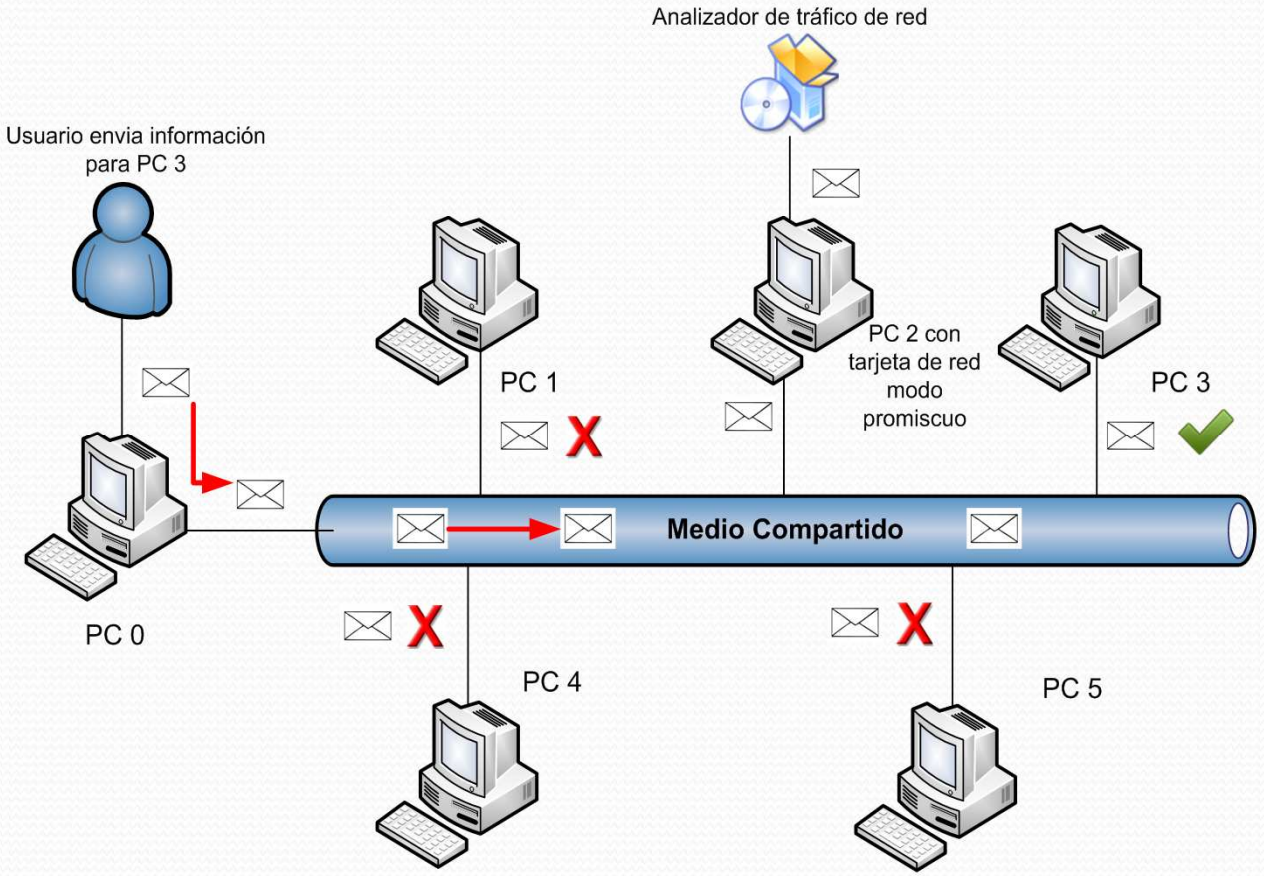
# Funcionamiento de un Analizador de Red

- Una red de datos esta conformada por varias computadoras conectadas entre sí por un medio cableado o inalámbrico, que a su vez están interconectadas a otros dispositivos.




Conexión de una red LAN

# Funcionamiento de un Analizador de Red



# Analizadores de Tráfico en el Mercado

- **TCPDUMP:** Su fuerte son los filtros.
- **Darkstat:** Crea resumen y gráficos por periodos de tiempo.
- **Traffic – VIS:** Convierte información en código ASCII, HTML o PostScript.
- **SNORT:** Sistema de detección de intrusos.
- **NWATCH**: Analizador de puertos pasivos de tráfico IP.
- **Wireshark**: Potente analizador libre de protocolos, soporta mas de 300 protocolos.
- **Ettercap**: Interceptor para redes LAN, soporta muchos protocolos.
- **Kismet**: Analizador de tráfico en Linux para redes inalámbricas.

# Requerimientos de la Aplicación

- Protocolos capturados mediante el analizador ErPa.

| Capas Analizadas por ERPA | Protocolos a capturar |
|---|---|
| Capa Aplicación: | SSH<br>Telnet<br>FTP<br>HTTP<br>POP3<br>SMTP |
| Capa de Transporte: | TCP<br>UDP |
| Capa de Acceso a la red: | Información del paquete<br>Trama de los paquetes Ethernet |

# Diseño del Analizador ErPa

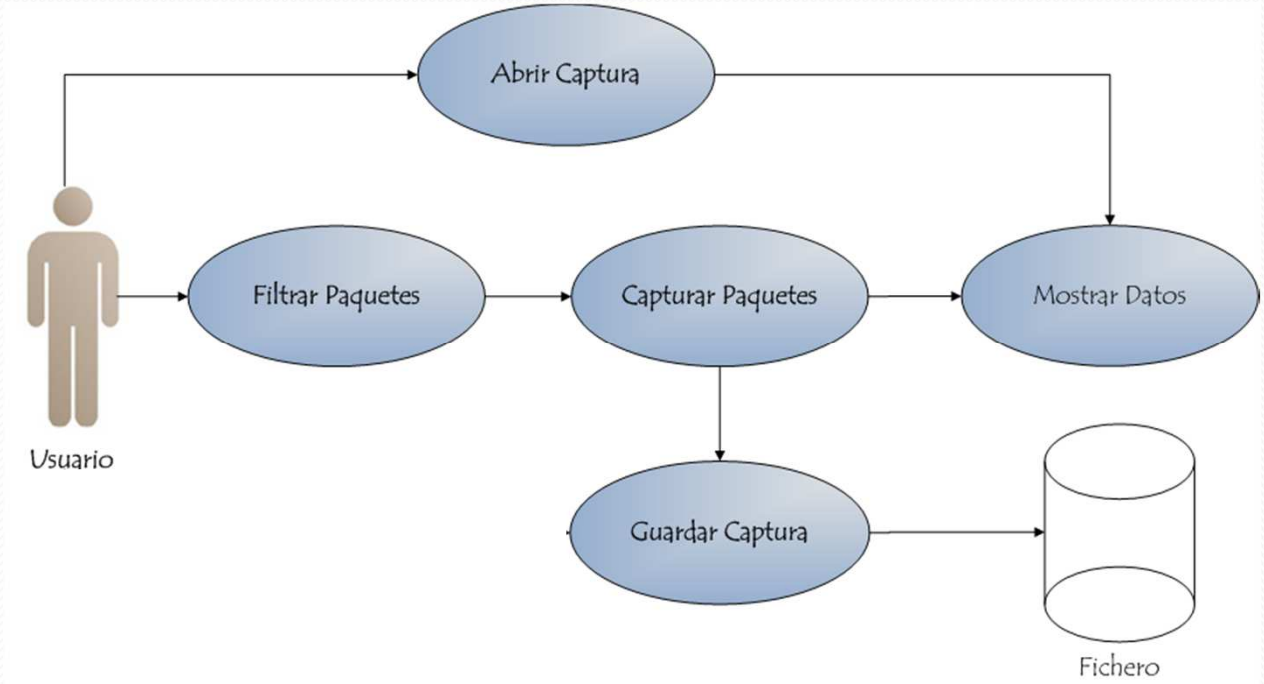


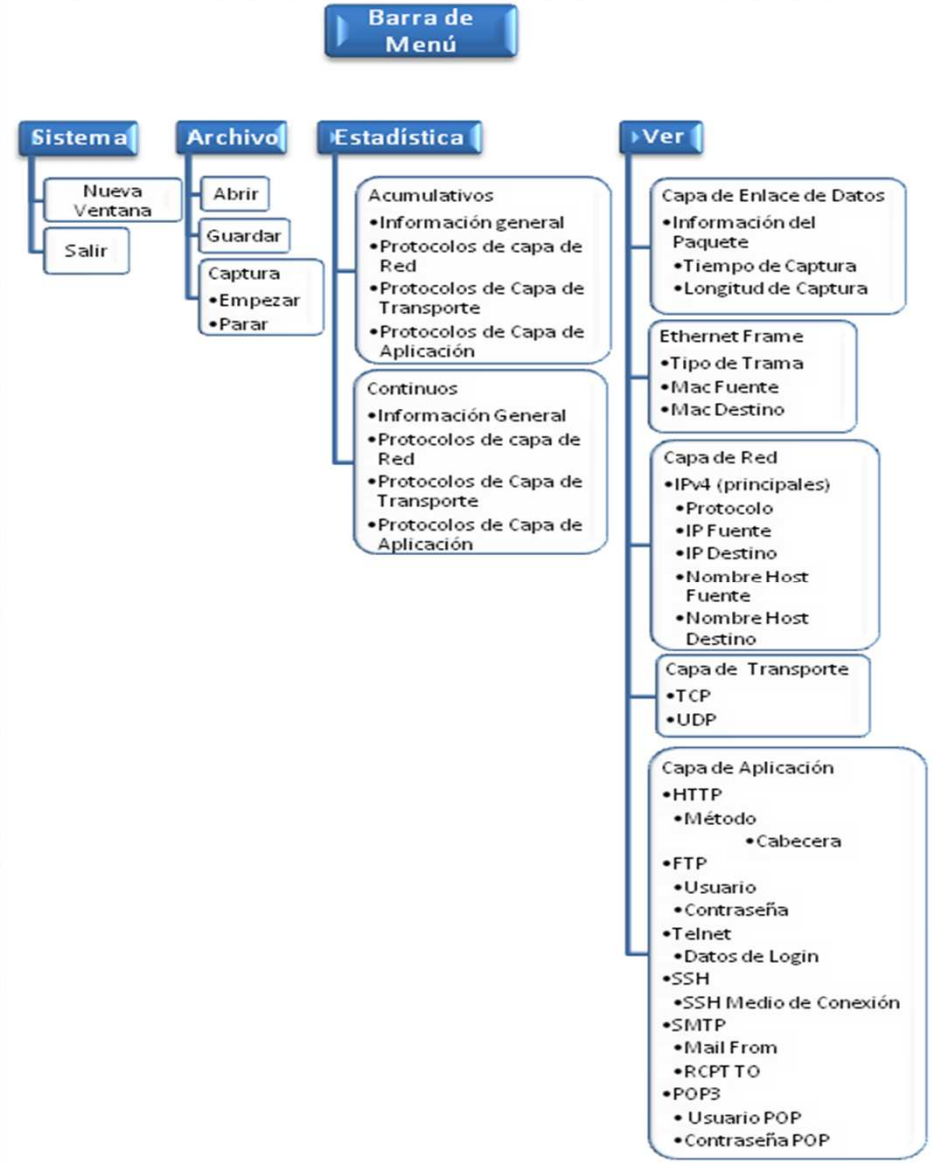

Gráfico del Diagrama UML

# Diseño del analizador ErPa

***Capturar Paquetes***

- El actor es el usuario conectado a una red, debe haber seleccionado la tarjeta de red.
- Selecciona Captura y luego Empezar de la barra de menú.
- Después se pueden visualizar paquetes enteros, solo encabezados o seleccionar el tamaño máximo de la captura.
- El actor presiona OK y los paquetes obtenidos se van mostrando en la pantalla de acuerdo a las opciones de visualización del usuario.
- El sistema comprueba la validez del tamaño máximo de la captura, regresando un mensaje de error en caso de estar incorrecto.
- Los datos se pueden visualizar en pantalla o grabarla en un fichero para posterior análisis.

# Diseño del analizador ErPa



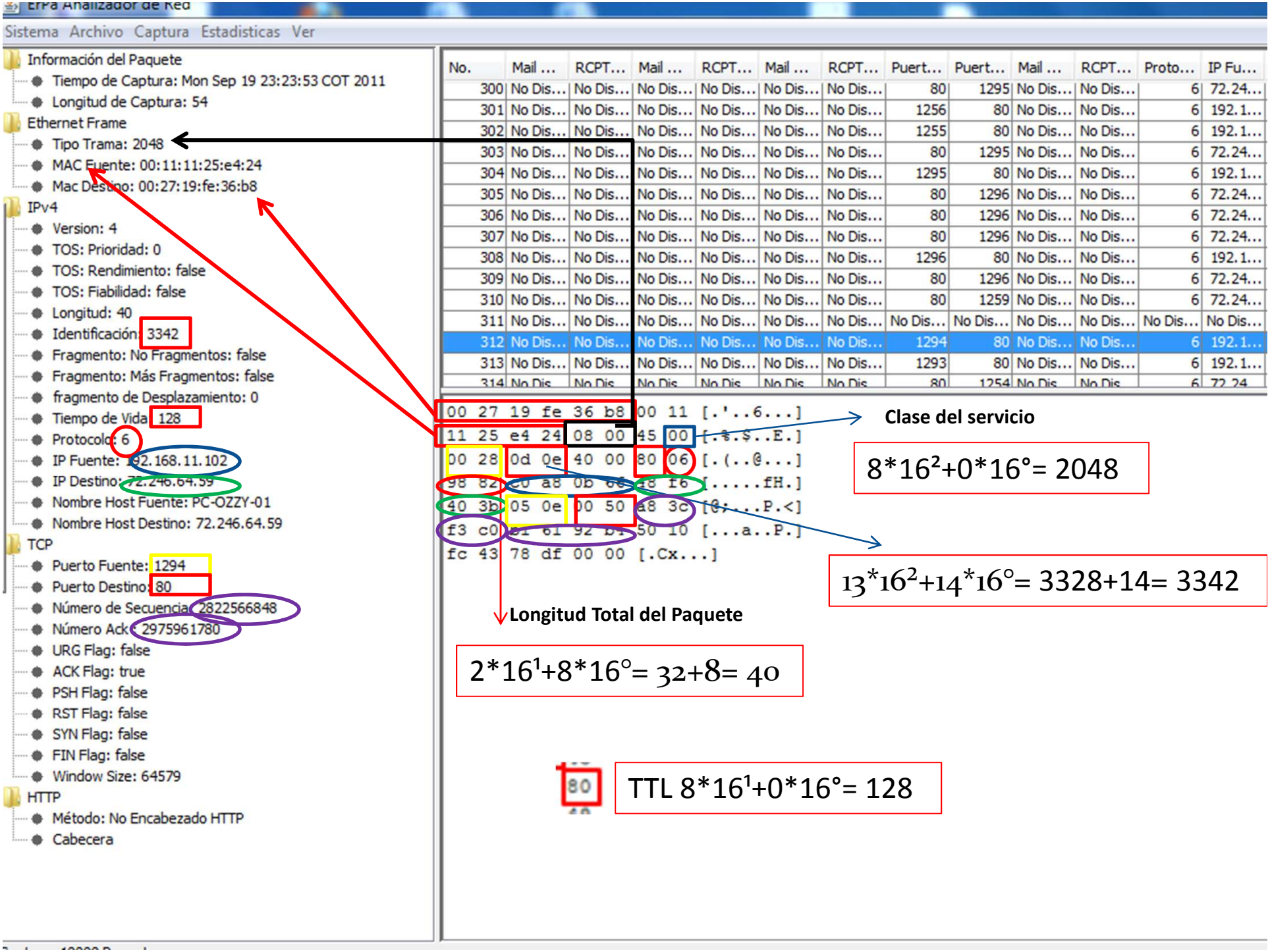
# Requerimientos Mínimos de ErPa

- Intel ® Pentium ® 4, procesador de 2.80 GHz, 1Gb de memoria RAM, con sistema operativo Microsoft Windows XP Profesional, versión 2002, Service Pack3.
- Las librerías Winpcap, Jpcap, y JRE 6.
- ErPa ha sido probado en sistema operativo Windows XP SP3 y Windows 7 32 bits y debe ser ejecutado con permisos de administrador, junto con JRE 6 o superior.

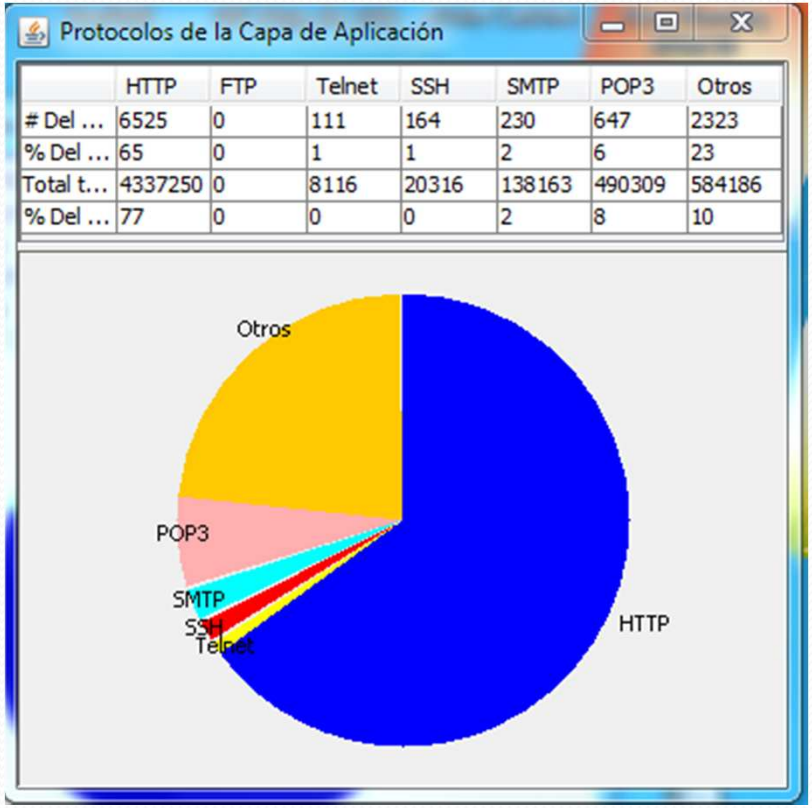
# ErPa

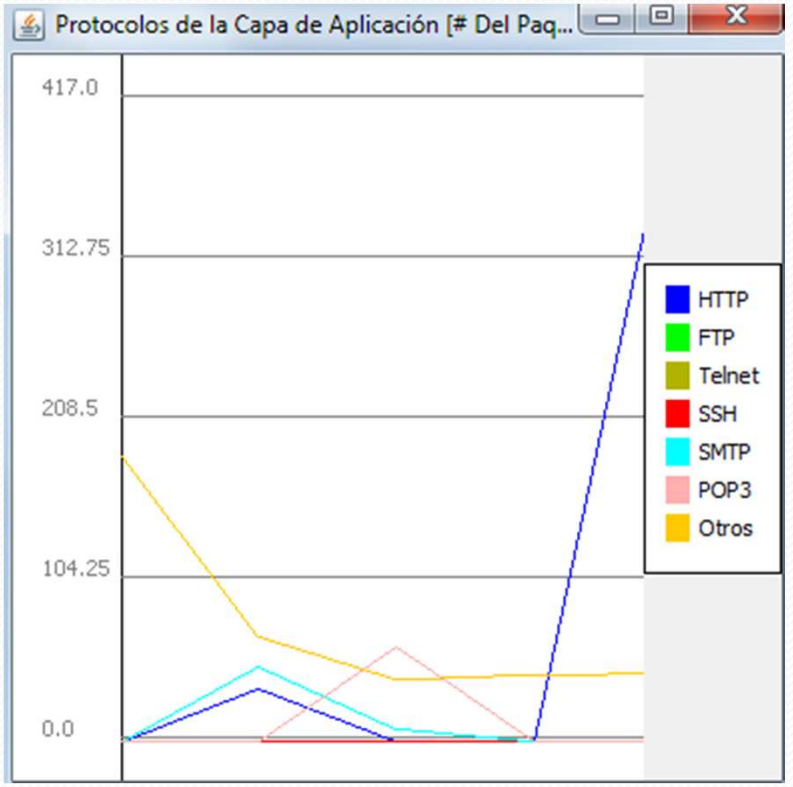
# DEMO

# Capturas


Sistema Archivo Captura Estadisticas Ver
Información del Paquete
Tiempo de Captura: Mon Sep 19 23:23:53 COT 2011
Longitud de Captura: 54
Ethernet Frame
Tipo Trama: 2048
MAC Fuente: 00:11:11:25:e4:24
Mac Destino: 00:27:19:fe:36:b8
IPv4
Version: 4
TOS: Prioridad: 0
TOS: Rendimiento: false
TOS: Fiabilidad: false
Longitud: 40
Identificación: 3342
Fragmento: No Fragmentos: false
Fragmento: Más Fragmentos: false
fragmento de Desplazamiento: 0
Tiempo de Vida: 128
Protocolo: 6
IP Fuente: 192.168.11.102
IP Destino: 72.246.64.59
Nombre Host Fuente: PC-OZZY-01
Nombre Host Destino: 72.246.64.59
TCP
Puerto Fuente: 1294
Puerto Destino: 80
Número de Secuencia: 2822566848
Número Ack: 2975961780
URG Flag: false
ACK Flag: true
PSH Flag: false
RST Flag: false
SYN Flag: false
FIN Flag: false
Window Size: 64579
HTTP
Método: No Encabezado HTTP
Cabecera
No. Mail ... RCPT... Mail ... RCPT... Mail ... RCPT... Puert... Puert... Mail ... RCPT... Proto... IP Fu...
300 No Dis... No Dis... No Dis... No Dis... No Dis... No Dis... 80 1295 No Dis... No Dis... 6 72.24...
301 No Dis... No Dis... No Dis... No Dis... No Dis... No Dis... 1256 80 No Dis... No Dis... 6 192.1...
302 No Dis... No Dis... No Dis... No Dis... No Dis... No Dis... 1255 80 No Dis... No Dis... 6 192.1...
303 No Dis... No Dis... No Dis... No Dis... No Dis... No Dis... 80 1295 No Dis... No Dis... 6 72.24...
304 No Dis... No Dis... No Dis... No Dis... No Dis... No Dis... 1295 80 No Dis... No Dis... 6 192.1...
305 No Dis... No Dis... No Dis... No Dis... No Dis... No Dis... 80 1296 No Dis... No Dis... 6 72.24...
306 No Dis... No Dis... No Dis... No Dis... No Dis... No Dis... 80 1296 No Dis... No Dis... 6 72.24...
307 No Dis... No Dis... No Dis... No Dis... No Dis... No Dis... 80 1296 No Dis... No Dis... 6 72.24...
308 No Dis... No Dis... No Dis... No Dis... No Dis... No Dis... 1296 80 No Dis... No Dis... 6 192.1...
309 No Dis... No Dis... No Dis... No Dis... No Dis... No Dis... 80 1296 No Dis... No Dis... 6 72.24...
310 No Dis... No Dis... No Dis... No Dis... No Dis... No Dis... 80 1259 No Dis... No Dis... 6 72.24...
311 No Dis... No Dis... No Dis... No Dis... No Dis... No Dis... No Dis... No Dis... No Dis... No Dis... No Dis... No Dis...
312 No Dis... No Dis... No Dis... No Dis... No Dis... No Dis... 1294 80 No Dis... No Dis... 6 192.1...
313 No Dis... No Dis... No Dis... No Dis... No Dis... No Dis... 1293 80 No Dis... No Dis... 6 192.1...
00 27 19 fe 36 b8 00 11 [.'..6...]
11 25 e4 24 08 00 45 00 [.%.$..E.]
00 28 0d 0e 40 00 80 06 [.(..@...]
f3 c0 b1 61 92 b4 50 10 [...a..P.]
fc 43 78 df 00 00 [.Cx...]
Clase del servicio
8*16²+0*16°= 2048
13*16²+14*16°= 3328+14= 3342
Longitud Total del Paquete
2*16¹+8*16°= 32+8= 40
80
TTL 8*16¹+0*16°= 128

# Presentación de los datos



# Capturas de los protocolos

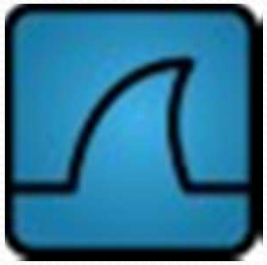
- SSH
- Telnet
- FTP
- POP3 y SMTP
- HTTP

# Comparativa


ErPa

# Comparación entre analizadores de red licenciados y no licenciados

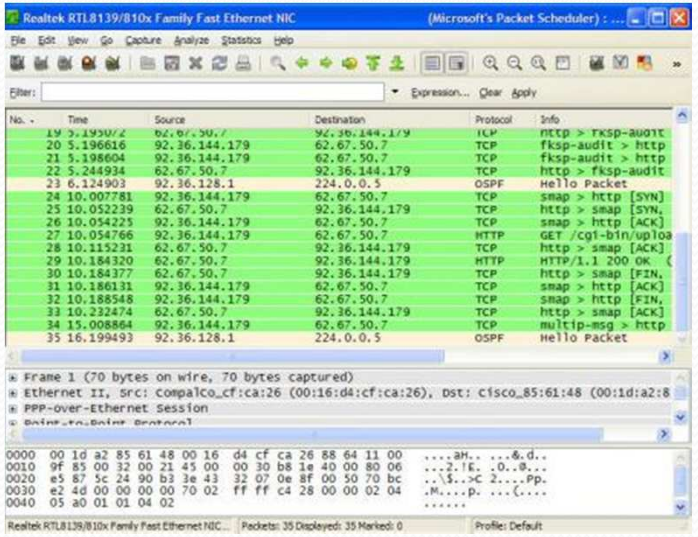
- El análisis y monitoreo de redes se ha convertido en una labor cada vez más importante y de carácter proactivo para evitar problemas.
- Las herramientas que se ofrecen hoy en día, le permiten, al administrador de red, realizar el análisis del tráfico de red por cuenta propia, y manejar un sistema experto que ayude a la interpretación de los resultados obtenidos y facilitándole el análisis de la red.




ErPa

# Analizador Wireshark

- Pertenece a los analizadores de red de software libre .
- Posee una interfaz agradable al usuario,  tiene muchas opciones de organización  y filtrado de la información.
- Es compatible con otro tipos de redes no solo LAN.
- Examina datos en tiempo real y de capturas anteriores.
- Da detalles, sumarios y un lenguaje completo para el filtrado y análisis de los paquetes.

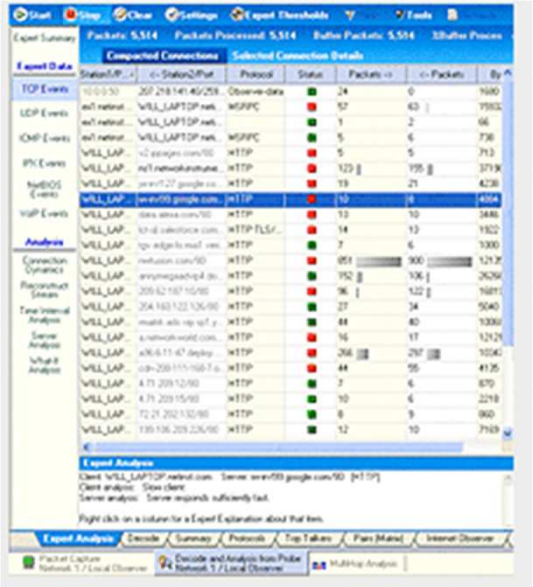



# Analizador Observer

- Se ubica en la categoría de analizadores licenciados.
- Puede ser usado para redes inalámbricas o alámbricas.
- Software desarrollado por National Instruments, tiene diferentes versiones, en nuestra tesis utilizamos la versión Observer Trial de 15 días.
- Ofrece diversos modos de análisis para aislar problemas específicos y concentrarse en la solución más optima de la red.

OBSERVER EXPERT

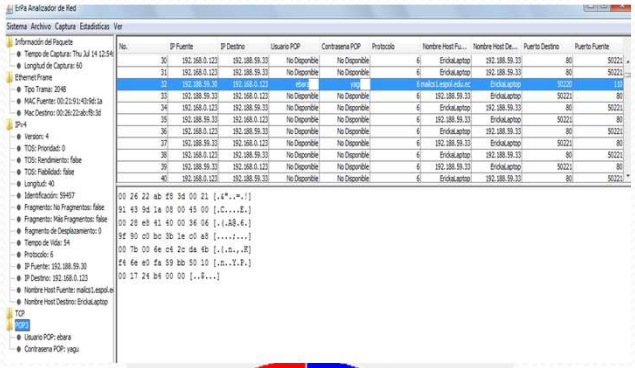
NETWORK INSTRUMENTS

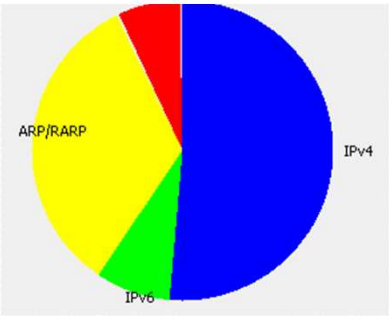


# Analizador ErPa

- El analizador de red ErPa fue diseñado con propósitos estudiantiles.
- Filtra ,captura y realiza diagramas estadísticos de los protocolos básicos como FTP, SSH, Telnet, HTTP, POP3, SMTP.
- Tiene una interfaz gráfica amigable y puede ser utilizada por personas con los conocimientos básicos sobre redes de datos.
- Limitante en la captura de paquetes que se ha fijado en 10.000.

ErPa






| | IPv4 | IPv6 | ARP/RARP | Otros |
|---|---|---|---|---|
| # Del Paquete | 5147 | 817 | 3343 | 693 |
| % Del Paquete | 26 | 4 | 17 | 3 |
| Total del Ta... | 727646 | 154892 | 187728 | 59062 |
| % Del Tam. | 64 | 13 | 16 | 5 |

# Ventajas y Desventajas de un analizador de código libre

- Una de las principales ventajas es la parte económica lo que permite a pequeñas y a medianas empresas obtener soluciones de bajo costo para los problemas de redes.

- El analizador de código libre nos da la libertad de utilizar el programa para el fin que mejor nos convenga, pudiendo instalar el software en cualquier PC sin necesidad de licencias.

- Una desventaja es que el analizador de código libre no posee una garantía de proveedor, ni de autores que respalden esa tecnología.

# Diseño Experimental

- En este análisis comparativo vamos a usar Wireshark como analizador de tráfico de red de software libre versus Observer Analizador de tráfico de red como software licenciado, y nuestro analizador ErPa.
- Utilizamos tres computadores portátiles con diferentes características.
- La captura se la realizo durante tres días, con tres equipos diferentes y cada uno con el mismo analizador de red.

# Análisis de la captura de tráfico

## Día A

| Observer | Intervalo de tiempo | Paquetes Capturados |
|---|---|---|
| Equipo A | 10:00 – 11:00 | 24450 |
| Equipo B | 10:00 – 11:00 | 34294 |
| Equipo C | 10:00 – 11:00 | 30828 |

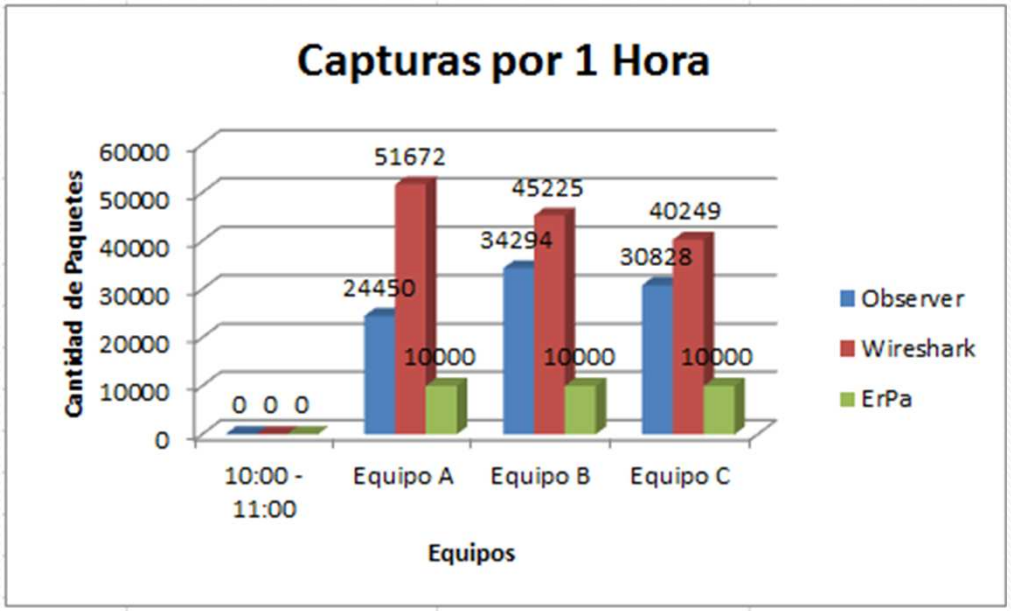
| | Observer | Wireshark | ErPa |
|---|---|---|---|
| 10:00 - 11:00 | Paquetes Capturados | Paquetes Capturados | Paquetes Capturados |
| Equipo A | 24450 | 51672 | 10000 |
| Equipo B | 34294 | 45225 | 10000 |
| Equipo C | 30828 | 40249 | 10000 |

## Día B

| Wireshark | Intervalo de tiempo | Paquetes Capturados |
|---|---|---|
| Equipo A | 10:00 – 11:00 | 51672 |
| Equipo B | 10:00 – 11:00 | 45225 |
| Equipo C | 10:00 – 11:00 | 40249 |

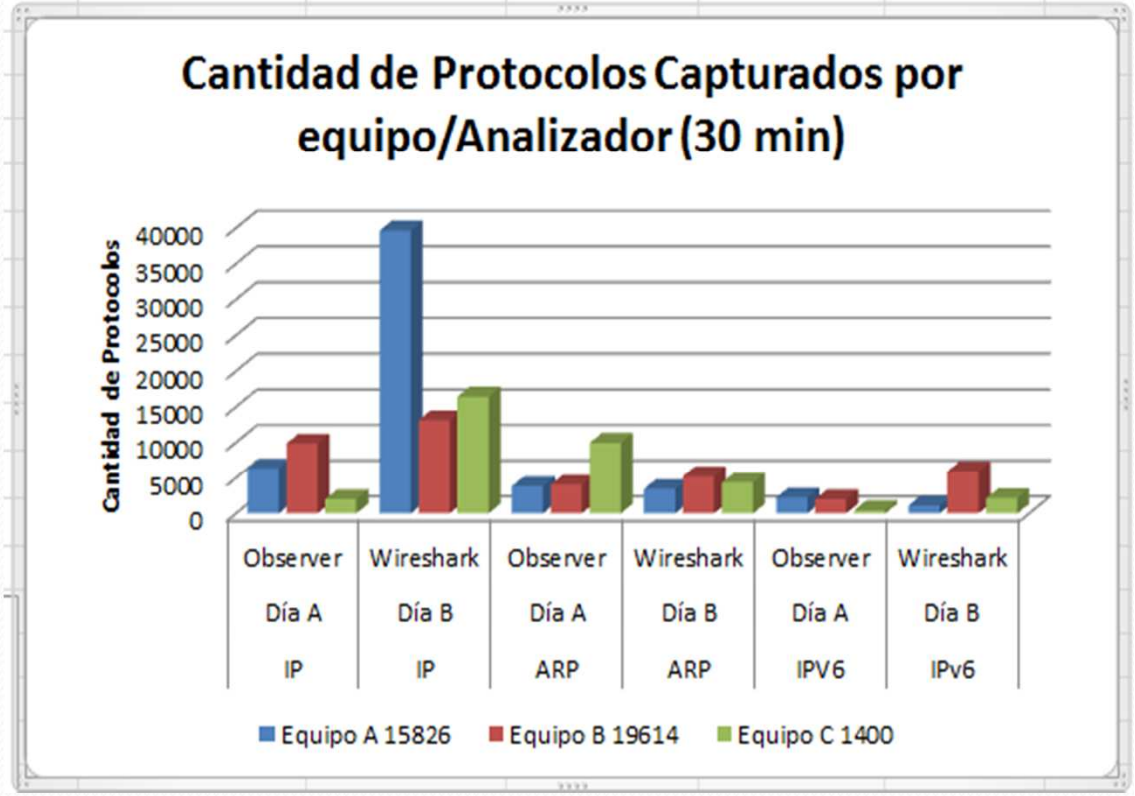
## Día C

| ErPa | Intervalo de tiempo | Paquetes Capturados |
|---|---|---|
| Equipo A | 10:00 – 11:00 | 10000 |
| Equipo B | 10:00 – 11:00 | 10000 |
| Equipo C | 10:00 – 11:00 | 10000 |



# Análisis de la captura de tráfico

| | | | Equipo A 15826 | Equipo B 19614 | Equipo C 1400 |
|---|---|---|---|---|---|
| IP | Día A | Observer | 6341 | 9871 | 2026 |
| IP | Día B | Wireshark | 39656 | 13134 | 16440 |
| ARP | Día A | Observer | 3844 | 4054 | 9968 |
| ARP | Día B | Wireshark | 3465 | 5240 | 4354 |
| IPV6 | Día A | Observer | 2259 | 2026 | 455 |
| IPv6 | Día B | Wireshark | 1108 | 5927 | 2162 |



# Conclusiones

- Se observó que el tráfico de red capturado durante todo el proceso siempre se mantuvo constante.
- Para elegir el tipo de analizador de red debemos determinar :
  - Problema que tenemos.
  - Saber con cuanto detalle y cuán completo necesitamos el análisis.
  - Instalación del analizador en el segmento de red que creemos tiene alguna falencia.

# Conclusiones

- ErPa puede generar graficas estadísticas acumulativas y continuas de los protocolos capturados.
- ErPa es un analizador que puede ser usado por los estudiantes para entender el comportamiento de una red.
- ErPa captura protocolos como Telnet, POP3, SHH, FTP, HTTP, SMTP, TCP y UDP, que son los más comunes en la red.

# Recomendaciones

- Determinar el punto correcto para analizar el comportamiento del tráfico en la red.
- Para todo tipo de red, se recomienda que cada cierto tiempo se realice un análisis de tráfico.
- Para realizar una captura con un analizador de red, el lugar preciso es en un conmutador, haciendo un espejo del puerto para luego capturar los paquetes con el analizador de redes.

# ¡Gracias por su Atención!