Captura de Paquetes

con tcpdump, libpcap y wireshark

Software para análisis de tráfico en la red:

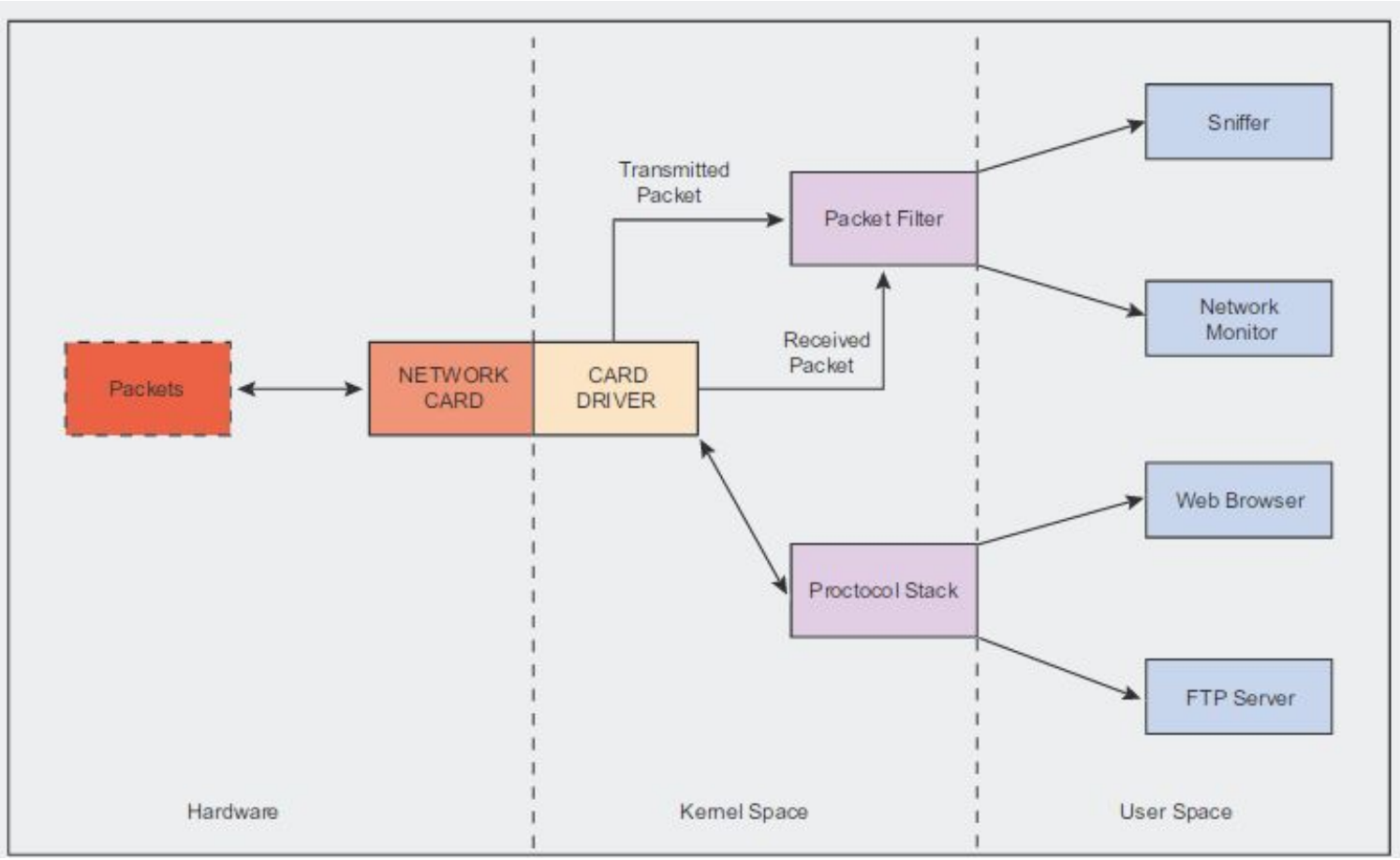
Cómo empezaron? En el principio no había nada...

Un verano de 1988...

Steve McCanne
linkedin

Van Jacobson
Network Research Group en U.C Berkeley
control de congestion TCP en Arpanet

Especificación:



Filtrar paquetes antes de que sean procesados por el stack de protocolos.

Introdujo un módulo del kernel (Packet filter) para hacer esta tarea.

Tcpdump

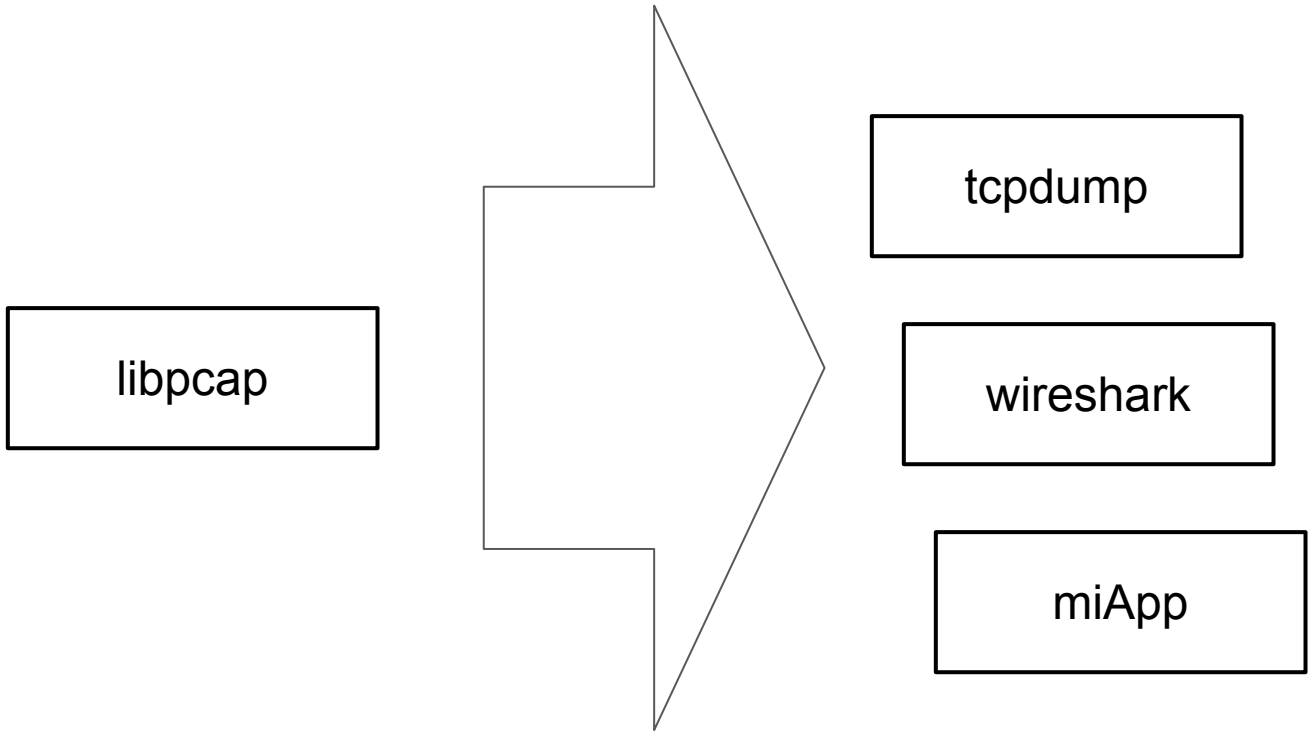
es un analizador de paquetes de línea de comandos. Permite al usuario ver paquetes TCP/IP que se transmiten sobre una red. Ver www.tcpdump.org

Ejemplo para ver el tráfico en la interfaz de red wlan0 (wireless) y guardarla en el archivo captura:

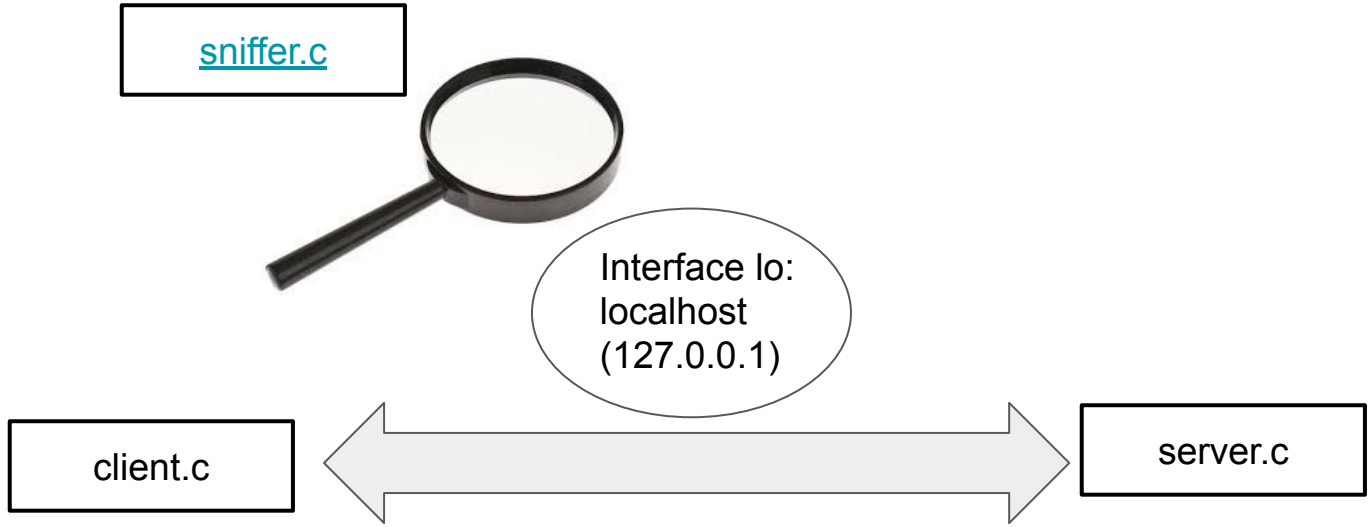
```
ifconfig -a

sudo tcpdump -i wlan0 -w captura
```

Una API, una librería reutilizable: libpcap



Programando con pcap.h



Bibliografía

Historia de tcpdump
https://msahputra.wordpress.com/2016/02/20/history-of-tcpdump-and-libpcap/

Manual de pcap
http://www.tcpdump.org/pcap.html

Tutorial de libpcap
http://recursos.aldabaknocking.com/libpcapHakin9LuisMartinGarcia.pdf

Geoip libreria
https://github.com/maxmind/geoip-api-c/blob/master/INSTALL