## Wireshark配置

可以配置网卡

## 分析协议的过程

分析的范围:HTTP TCP IP Ethernet DNS UDP ARP

确定某种行为能够产生某些数据,比如一次连接能够产生TCP连接,HTTP请求等;

然后进行该行为,过滤头部.

## HTTP

浏览器访问某个特殊网站,然后过滤特定的网站

## TCP

同样的是一个浏览器请求,过滤特定的网站和远程端口

## IP

Ping应用程序使用的ICMP协议,这个协议是封装