Wireshark

Wireshark前称是“Ethereal”是一个网络抓包和分析软件。广泛流行在计算机取证、网络安全、计算机、计算机网络等领域。

[典型范例]:

在计算机取证领域中，取证人员可以查看Wireshark抓取的数据包而进行判断攻击者的IP地址及攻击时间等。

而在计算机领域，主要是涉及计算机网络的和相关专业的，比如计算机应用、计算机网络等方向的，教师可用Wireshark来演示相关协议的数据包信息，比如TCP三次握手等。

一，基本过滤规则

类型	名称	实例	描述
IP	ip.dst	ip.dst==1	查找目的地址为1的包
	ip.src	ip.src==1	查找源地址为1的包
MAC	eth.dst	eth.dst==MAC	过滤目标MAC
		ech.src==MAC	过滤来源MAC
端口	tcp.port	tcp.port==1	只查找端口为1的包
	tcp.dstport	tcp.dstport==1	查找目的端口为1的包
	tcp.srcport	tcp.srcport==1	查找源端口为1的包
协议	SSDP	SSPD	过滤SSDP包
and	and	ip.src==1 and SSDP	过滤源地址为1且协议类型为SSDP是数据包