

2.4 网络监听原理

网络嗅探（Network Sniffer）是指利用计算机的网络接口截获其他计算机的数据报文的一种手段。

网络嗅探的基础是数据捕获,目的是对数据进行分析,挑选出重点关注的数据。



2.4.1 网卡的工作原理

01

直接模式

02

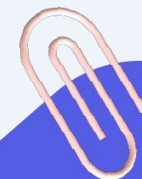
广播模式

嗅探的步骤

混杂模式：更改网卡工作模式

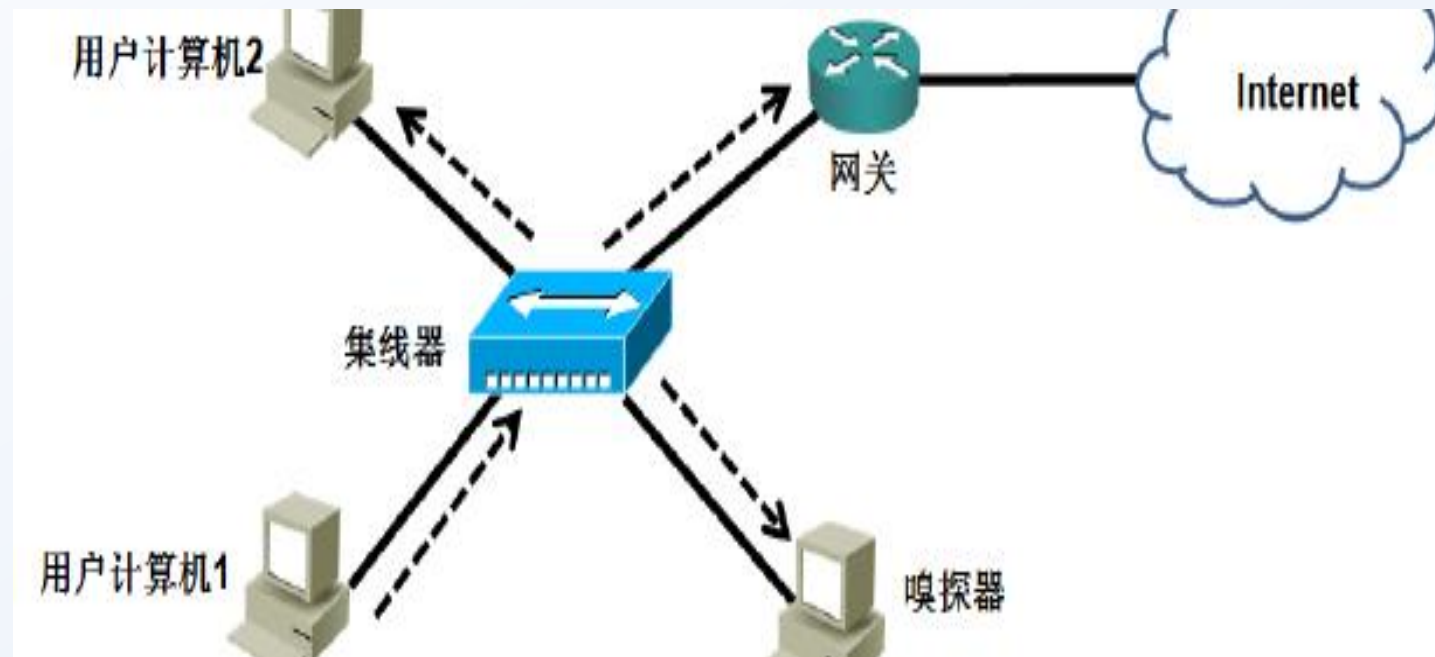
协议分析软件：捕获数据包

人工或智能：分析数据包



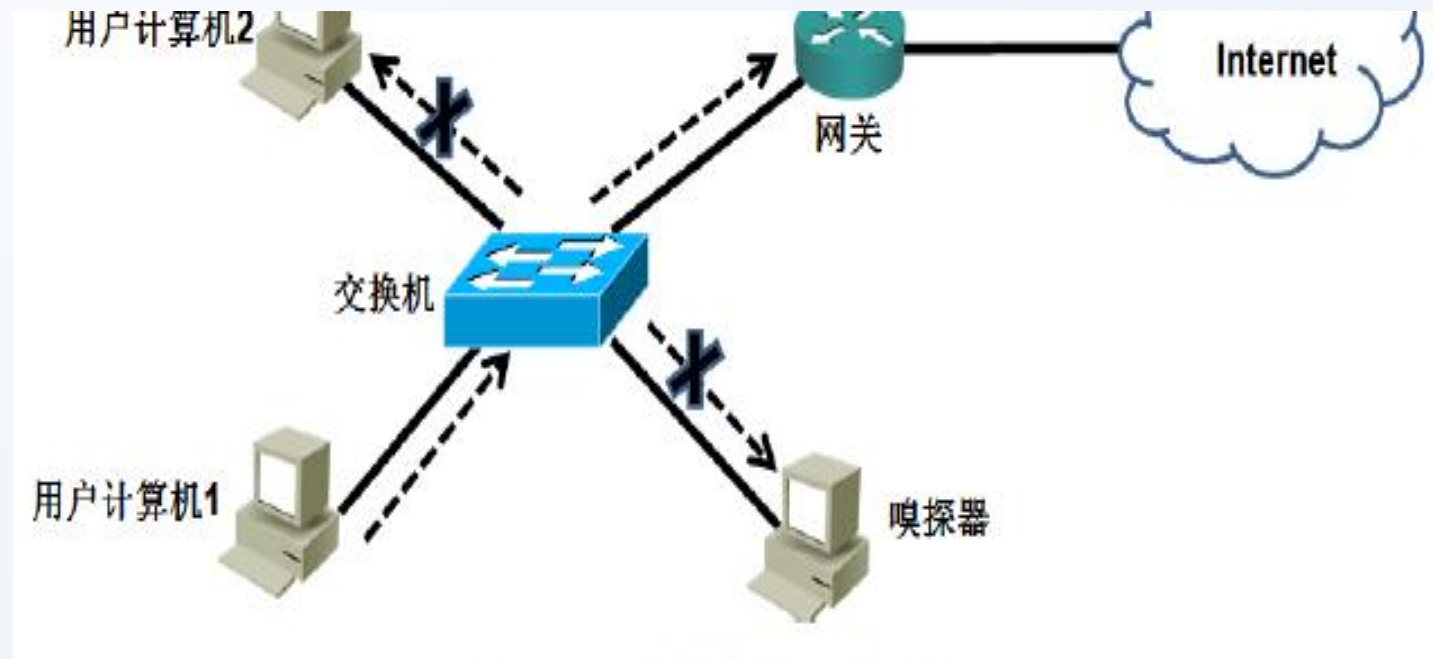
网络嗅探的工作环境1 - HUB

2.4.2 嗅探的步骤



集线器 (Hub) 是物理层设备，它从一个接口收到数据，会把数据位从其他全部接口发送出去。

2.4.2 嗅探的步骤

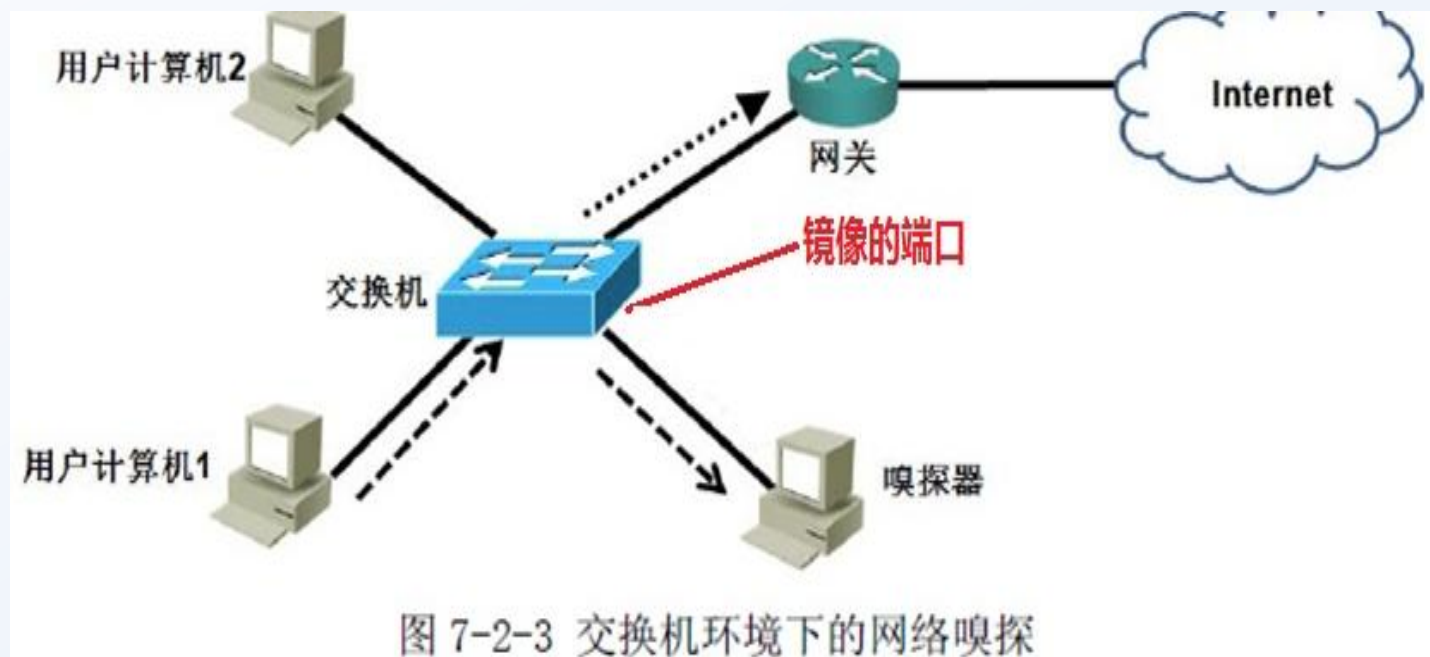


网络嗅探的工作环境2-
交换机

交换机 (switch) 是数据链路层设备，正常情况下，交换机只把转发给接收者所在的接口。

2.4.2 嗅探的步骤

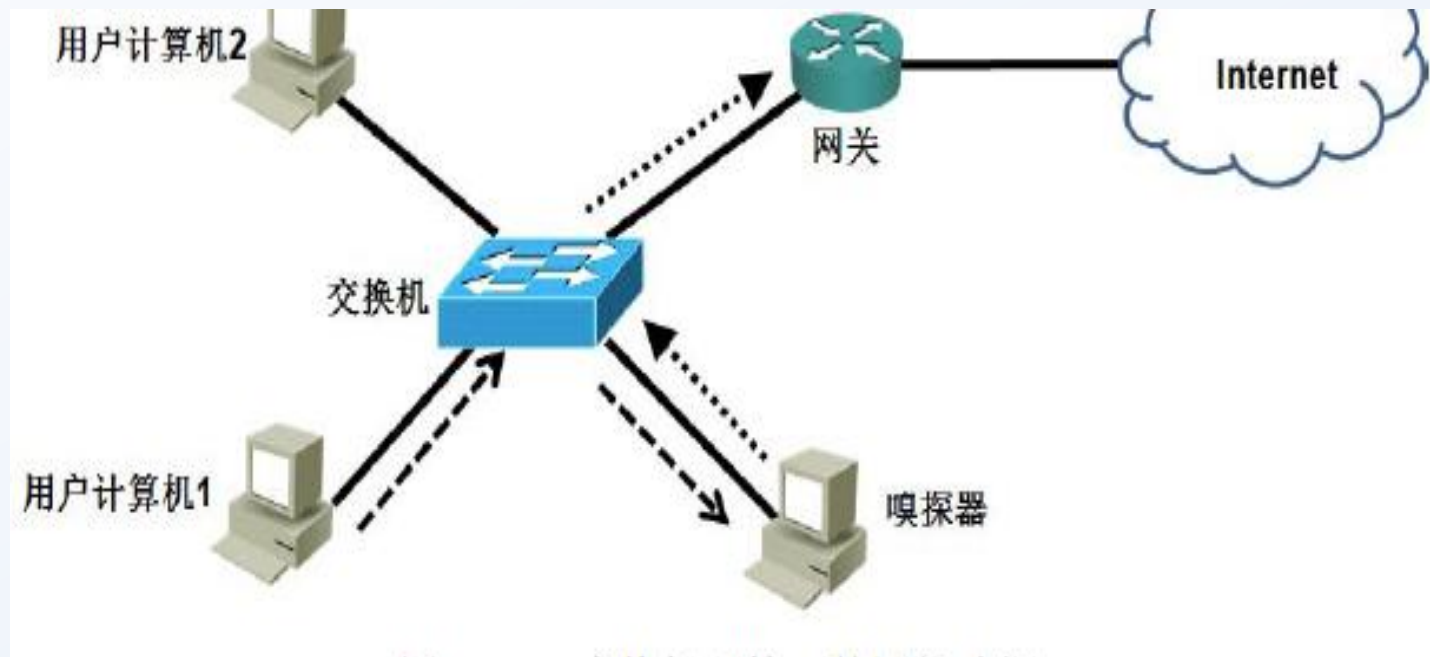
交换环境下的网络嗅探 1-端口镜像



如果嗅探者是交换机的管理员，则可以在交换机上配置端口镜像，把需要嗅探的接口上的收和发的流量，镜像到嗅探器所连接的接口。

2.4.2 嗅探的步骤

交换环境下的网络嗅探
2-结合ARP欺骗



在交换机上配置端口镜像，把需要嗅探的接口上的收和发的流量，镜像到嗅探器所连接的接口。

2.4.2

嗅探的步骤



嗅探软件介绍

Wireshark (Ethereal)

1

2

Sniffer Pro

EffTech HTTP Sniffer

4

3

Iris



2.4.2 嗅探的步骤

嗅探的防御

01

尽量工作在交换网络中

02

对传输的关键数据加密

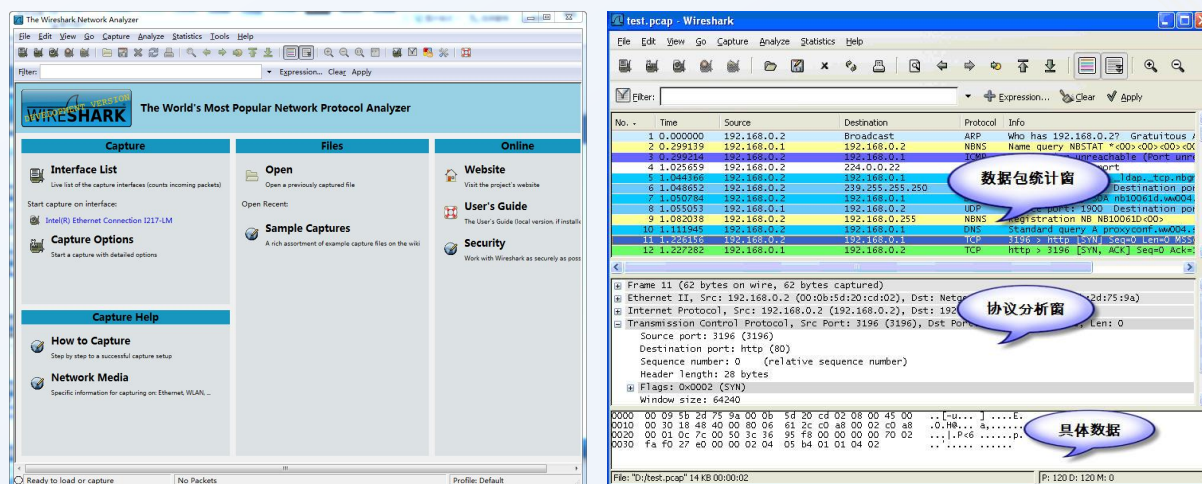
03

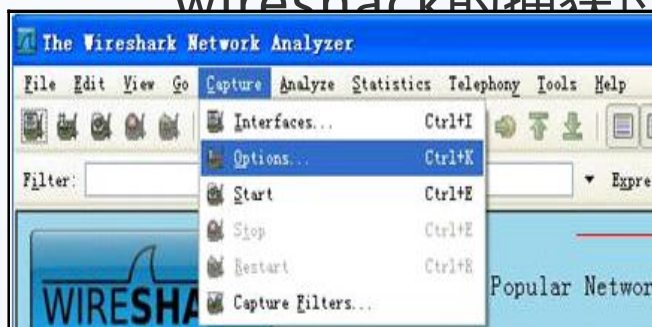
在网络中布置入侵检测系统 (IDS)

2.4.3 wireshack的应用

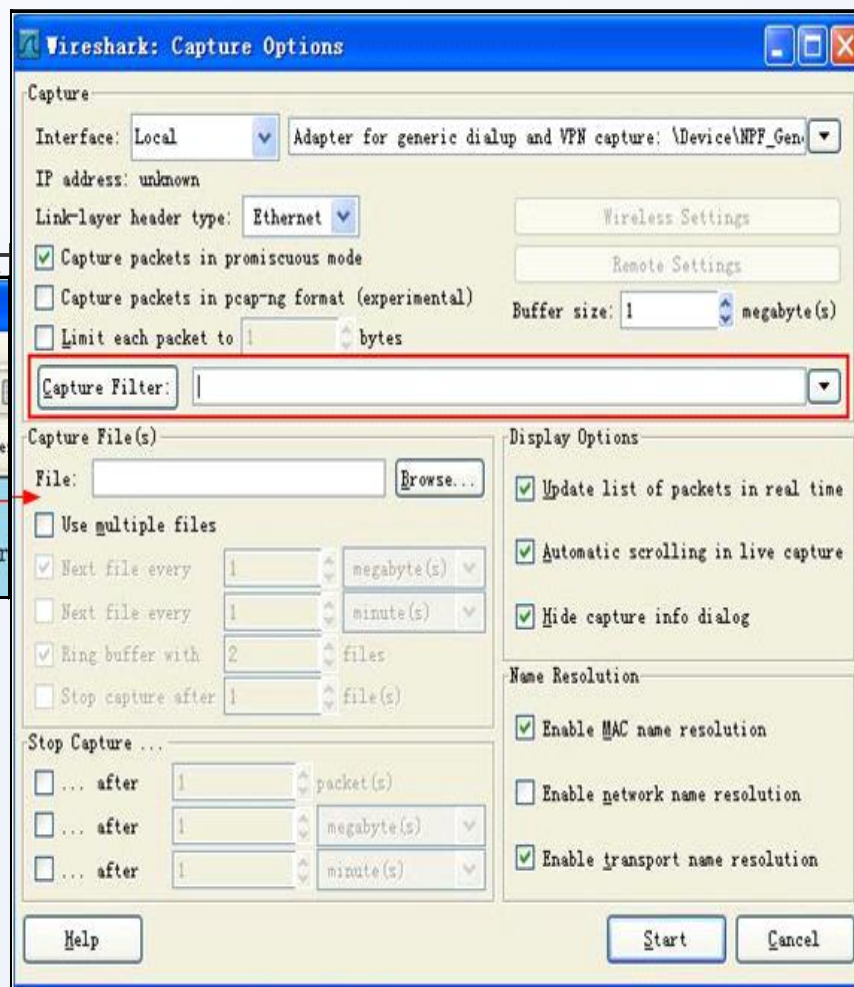
wireshack的应用

wireshack的窗口





wireshark的捕获选项



2.4.3

wireshack的应用

语法:

Protocol	Direction	Host(s)	Value	Logical Operations	Other expression
----------	-----------	---------	-------	--------------------	------------------

例子: tcp dst 10.1.1.1 80 and tcp dst 10.2.2.2 3128

英文写法:	C语言写法:	含义:
eq	==	等于
ne	!=	不等于
gt	>	大于
lt	<	小于
ge	>=	大于等于
le	<=	小于等于

英文写法:	C语言写法:	含义:
and	&&	逻辑与
or		逻辑或
xor	^^	逻辑异或
not	!	逻辑非

wireshack捕获过
滤的语法

Logical
e-xpressions (逻辑
运算符)

2.4.3 wireshack的应用



语法	备注
udp dst port 139	目的UDP端口为139的数据包
not icmp	除icmp以外的数据包
src host 172.17.12.1 and dst net 192.168.2.0/24	显示来源IP地址为 172.17.12.1，并且目的地址是 192.168.2.0/24的数据包
(src host 10.4.1.12 or src net 10.6.0.0/16) and tcp dst portrange 200-1000 and dst net 10.0.0.0/8	IP为10.4.1.12或者源网络为10.6.0.0/16，目的地TCP端口号在200至1000之间，并且目的位于网络10.0.0.0/8内的所有数据包。

2.4.3 wireshack的 应用

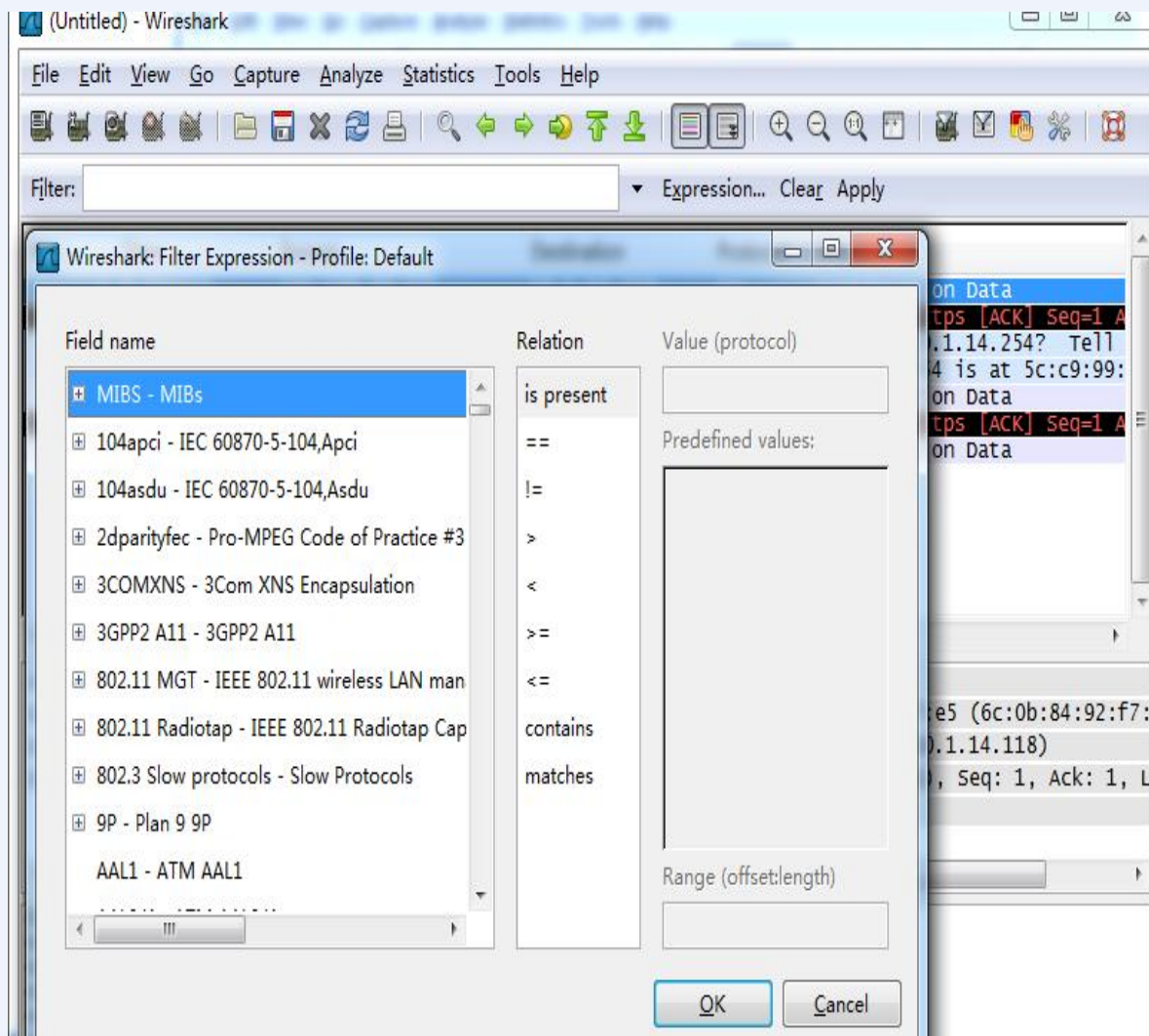
wireshack的显示过滤



2.4.3 wireshack的应用

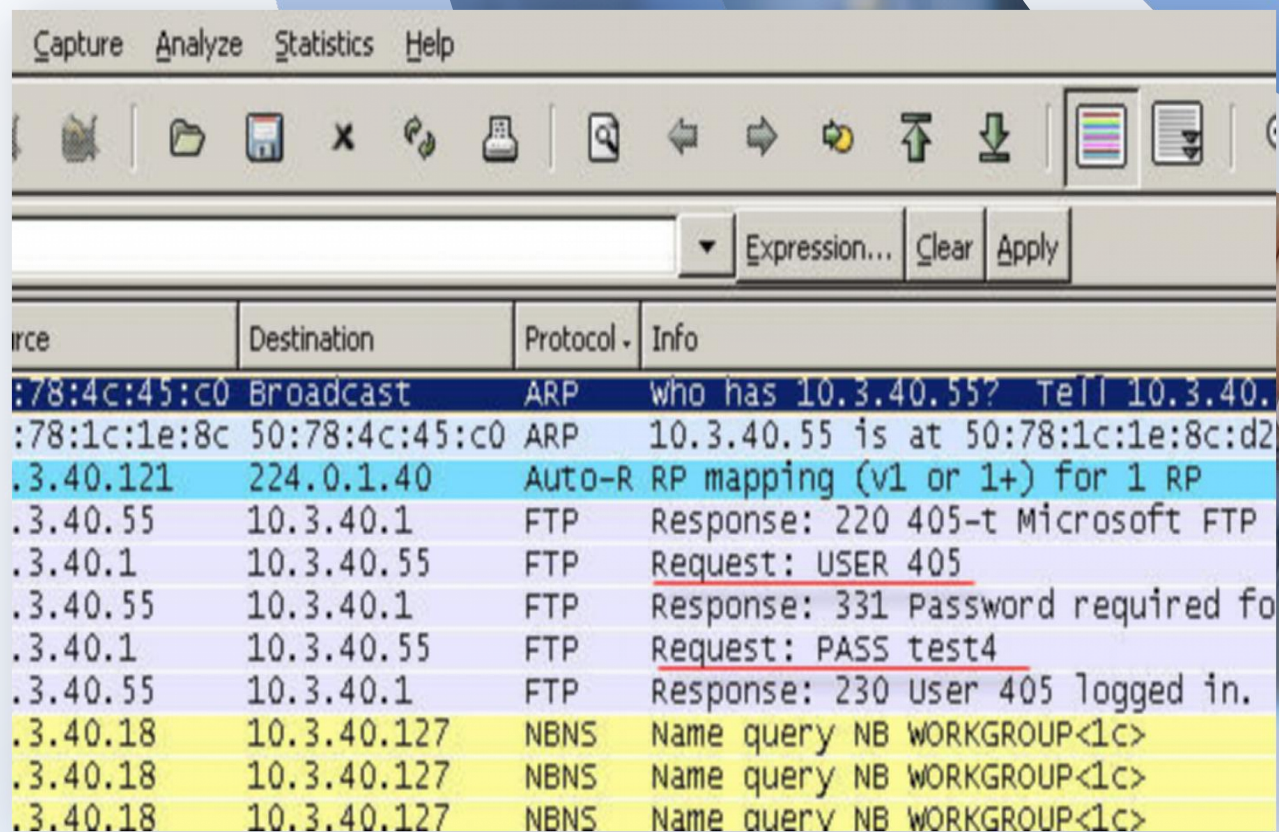
语法	备注
eth.addr==5c:99:63:21:33:54	指定物理地址
ip.addr==10.1.1.1	指定IP（不区分源或者目的）
ip.dst ==10.3.42.1 and tcp.dstport==80	指定目的IP和目的端口
ip.src 10.1.1.0/24 and tcp.dstport 300-500	指定源IP为网络地址并且目的端口的范围
not arp	不显示ARP协议
http.request.method=="GET"	显示HTTP协议请求中的get方法
http.date contains "789"	显示HTTP协议中的具体内容

2.4.3 wireshack的应用



≡ 2.4.3 wireshack的应用

WIRESHACK的案例1



The image shows a screenshot of the Wireshark network traffic capture tool. The interface includes a menu bar (Capture, Analyze, Statistics, Help), a toolbar with various icons, and a packet list table. The table has columns for Source, Destination, Protocol, and Info. The captured traffic includes ARP requests, FTP sessions, and NBNS name queries.

Source	Destination	Protocol	Info
50:78:4c:45:c0	Broadcast	ARP	who has 10.3.40.55? Tell 10.3.40.55
50:78:1c:1e:8c	50:78:4c:45:c0	ARP	10.3.40.55 is at 50:78:1c:1e:8c:d2
10.3.40.121	224.0.1.40	Auto-RP	RP mapping (v1 or 1+) for 1 RP
10.3.40.55	10.3.40.1	FTP	Response: 220 405-t Microsoft FTP
10.3.40.1	10.3.40.55	FTP	Request: <u>USER 405</u>
10.3.40.55	10.3.40.1	FTP	Response: 331 Password required for
10.3.40.1	10.3.40.55	FTP	Request: <u>PASS test4</u>
10.3.40.55	10.3.40.1	FTP	Response: 230 User 405 logged in.
10.3.40.18	10.3.40.127	NBNS	Name query NB WORKGROUP<1c>
10.3.40.18	10.3.40.127	NBNS	Name query NB WORKGROUP<1c>
10.3.40.18	10.3.40.127	NBNS	Name query NB WORKGROUP<1c>

