1. 分析工具能够解读哪种类型的报文？

2. 分析工具为什么能够解读不同协议的报文？

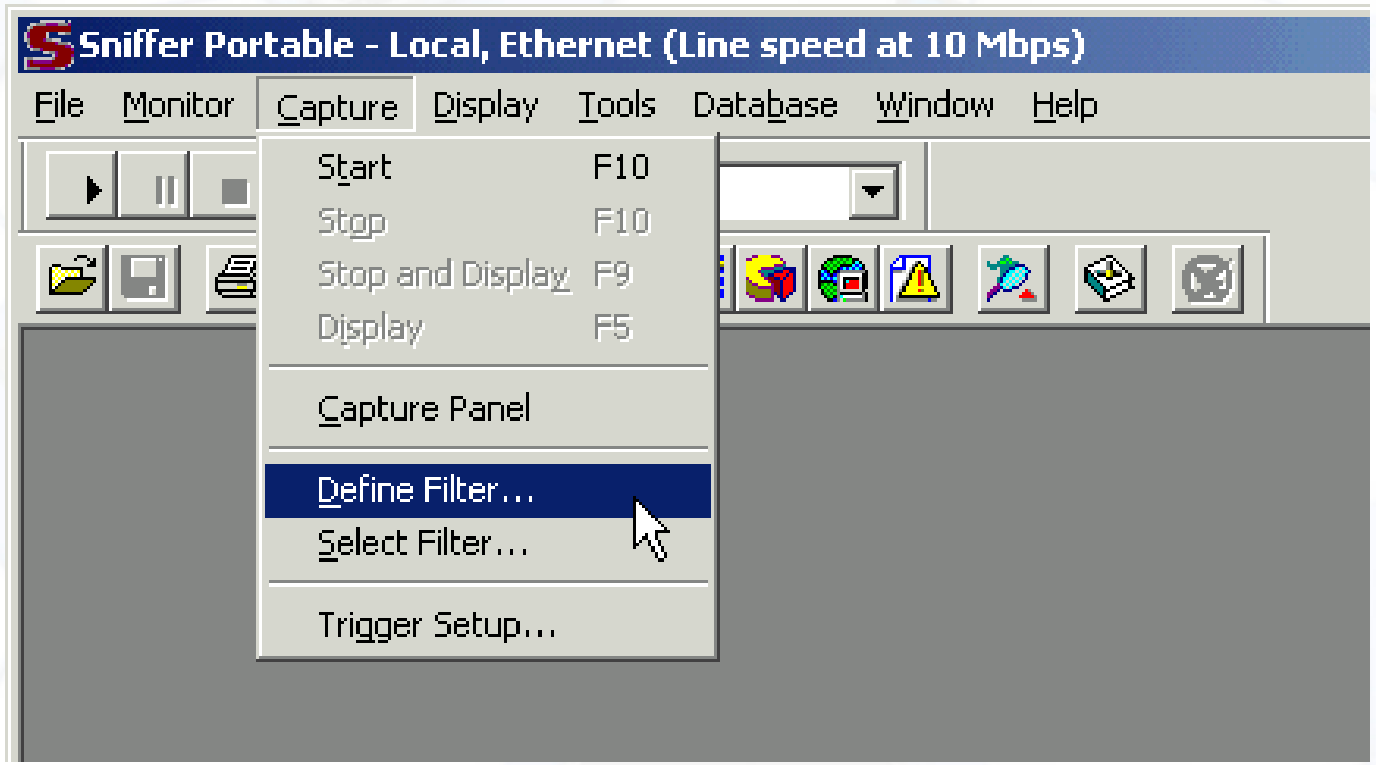
3. 怎样可以在交换网络中嗅探数据？

一、 网络数据分析（嗅探）工具

- 数据监听原理：在局域网中与其他计算机进行数据交换的时候，采用的是共享介质的广播方式传输
- 只有与数据帧中目标地址一致的主机才会接收数据，其他的机器都会将帧丢弃。
- 当主机工作在监听模式时，无论接收到的数据包中目标地址是什么，主机都将其接收下来。对数据包进行分析，就得到了局域网中通信的数据
- 一台计算机可以监听同一网段所有的数据包，不能监听不同网段的计算机传输的信息
- 由于现在普遍使用交换机，监听数据没有使用集线器时那么容易

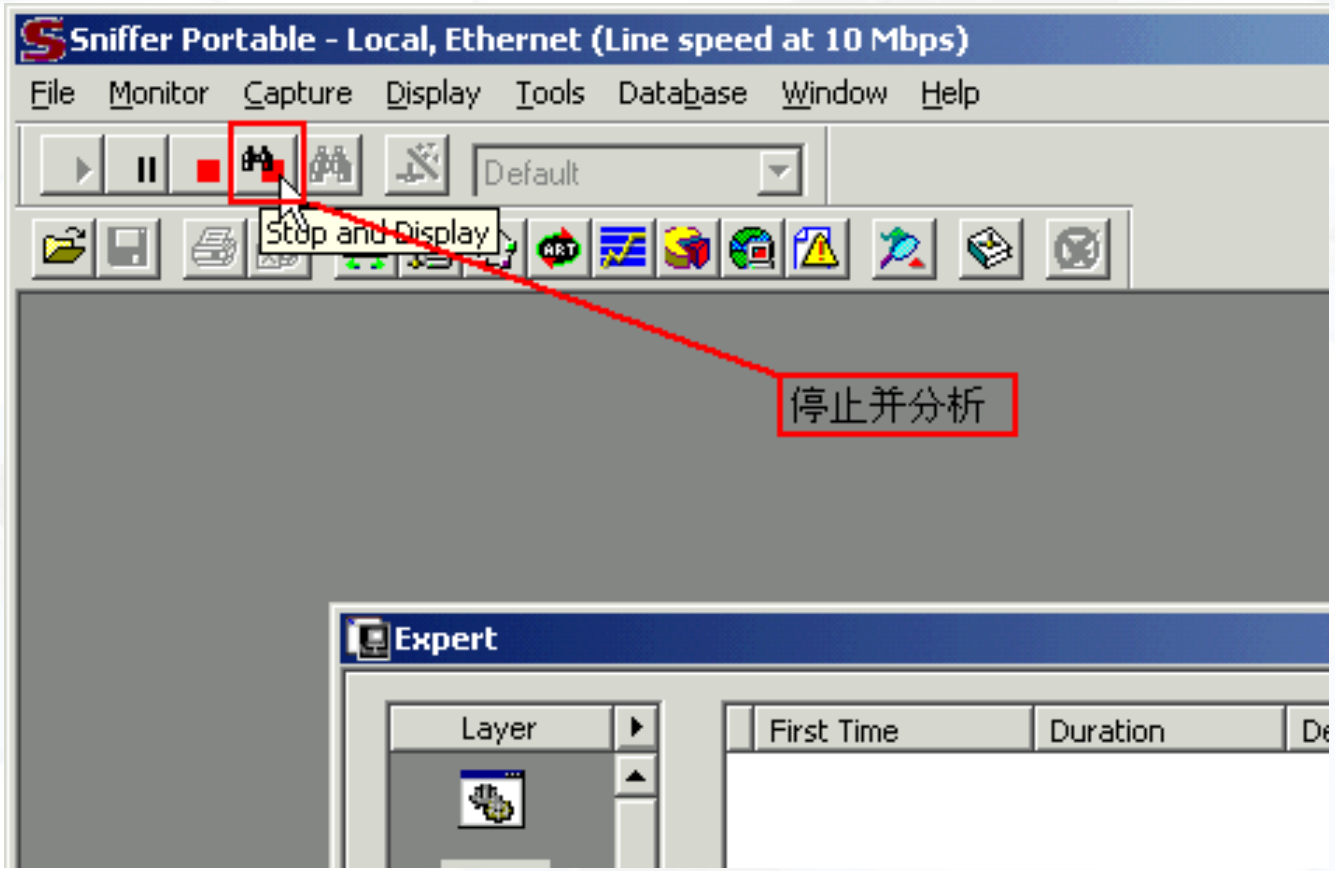
1. 商业工具软件Sniffer

- 进入Sniffer主界面，抓包之前必须首先设置要抓取数据包的类型。选择主菜单Capture下的Define Filter菜单



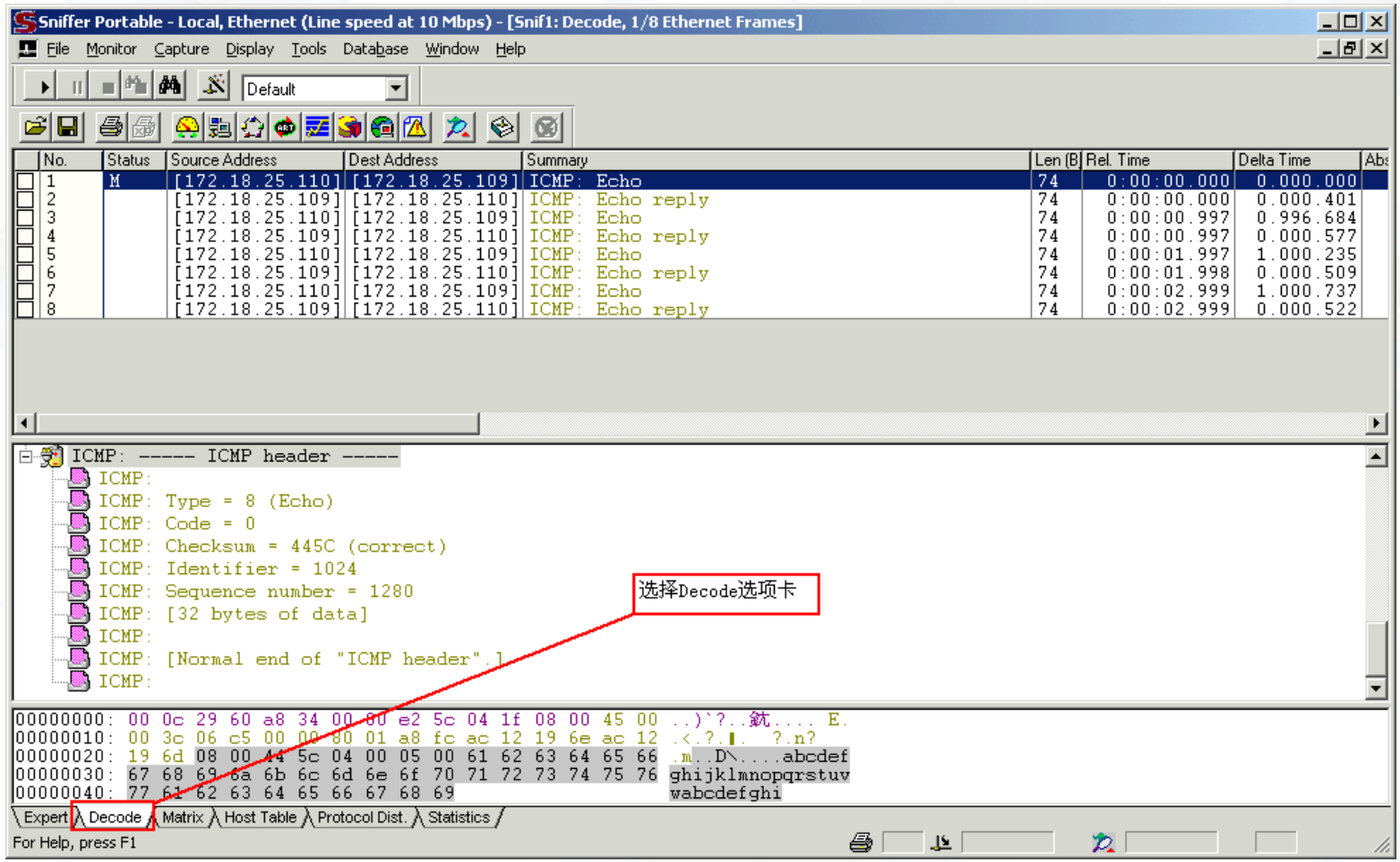
1） 停止捕获并分析

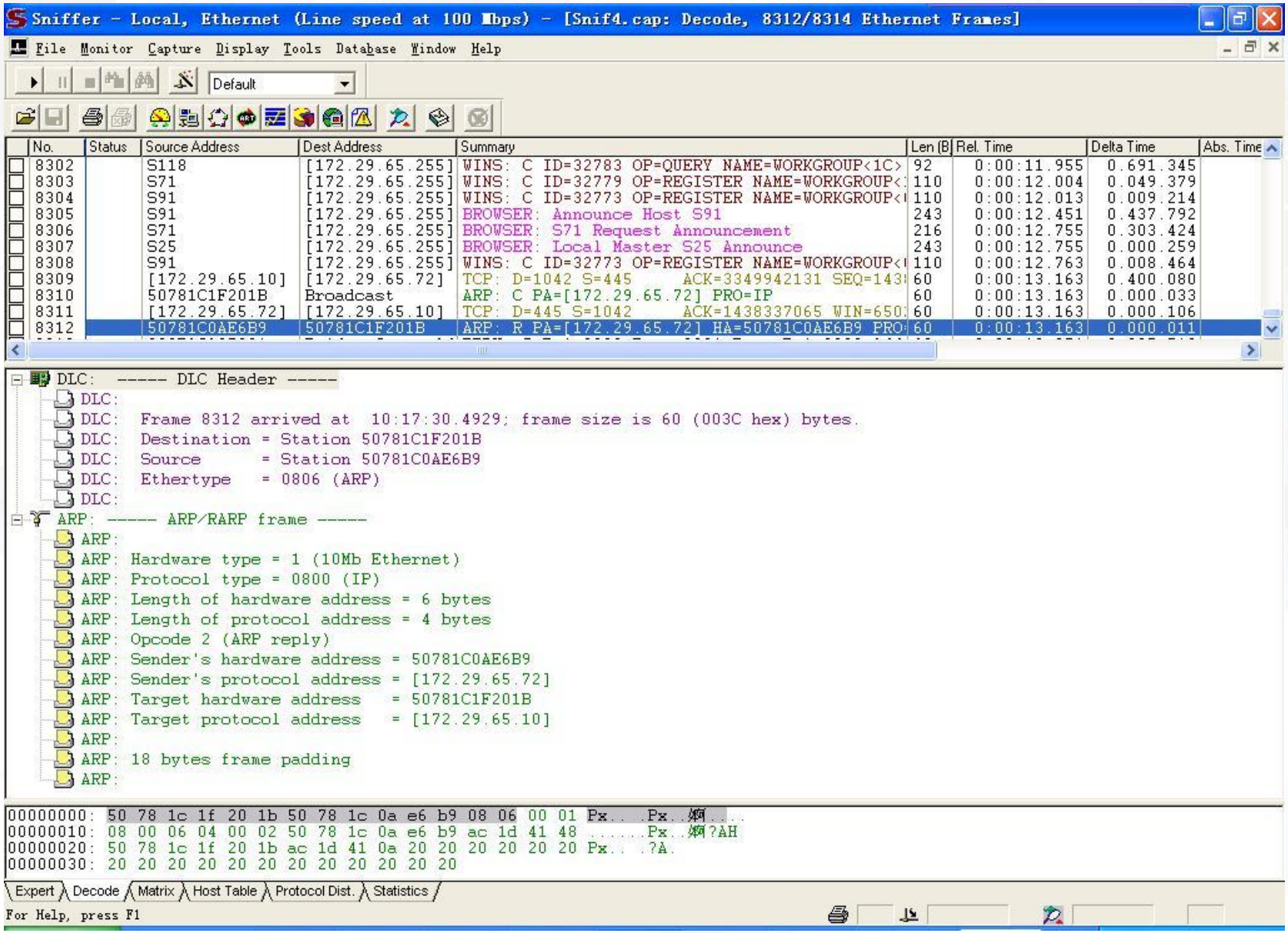
- 等指令执行完毕后，点击工具栏上的停止并分析按钮



2） 对数据包解码分析

- 在出现的窗口选择Decode选项卡，可以看到数据包在两台计算机间的传递过程




Sniffer - Local, Ethernet (Line speed at 100 Mbps) - [Snif4.cap: Decode, 8312/8314 Ethernet Frames]
File Monitor Capture Display Tools Database Window Help
Default
No. Status Source Address Dest Address Summary Len (B) Rel. Time Delta Time Abs. Time
8302 S118 [172.29.65.255] WINS: C ID=32783 OP=QUERY NAME=WORKGROUP<1C> 92 0:00:11.955 0.691.345
8303 S71 [172.29.65.255] WINS: C ID=32779 OP=REGISTER NAME=WORKGROUP< 110 0:00:12.004 0.049.379
8304 S91 [172.29.65.255] WINS: C ID=32773 OP=REGISTER NAME=WORKGROUP< 110 0:00:12.013 0.009.214
8305 S91 [172.29.65.255] BROWSER: Announce Host S91 243 0:00:12.451 0.437.792
8306 S71 [172.29.65.255] BROWSER: S71 Request Announcement 216 0:00:12.755 0.303.424
8307 S25 [172.29.65.255] BROWSER: Local Master S25 Announce 243 0:00:12.755 0.000.259
8308 S91 [172.29.65.255] WINS: C ID=32773 OP=REGISTER NAME=WORKGROUP< 110 0:00:12.763 0.008.464
8309 [172.29.65.10] [172.29.65.72] TCP: D=1042 S=445 ACK=3349942131 SEQ=143 60 0:00:13.163 0.400.080
8310 50781C1F201B Broadcast ARP: C PA=[172.29.65.72] PRO=IP 60 0:00:13.163 0.000.033
8311 [172.29.65.72] [172.29.65.10] TCP: D=445 S=1042 ACK=1438337065 WIN=650 60 0:00:13.163 0.000.106
8312 50781C0AE6B9 50781C1F201B ARP: R PA=[172.29.65.72] HA=50781C0AE6B9 PRO 60 0:00:13.163 0.000.011
DLC: ----- DLC Header -----
DLC:
DLC: Frame 8312 arrived at 10:17:30.4929; frame size is 60 (003C hex) bytes.
DLC: Destination = Station 50781C1F201B
DLC: Source = Station 50781C0AE6B9
DLC: Ethertype = 0806 (ARP)
DLC:
ARP: ----- ARP/RARP frame -----
ARP:
ARP: Hardware type = 1 (10Mb Ethernet)
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 2 (ARP reply)
ARP: Sender's hardware address = 50781C0AE6B9
ARP: Sender's protocol address = [172.29.65.72]
ARP: Target hardware address = 50781C1F201B
ARP: Target protocol address = [172.29.65.10]
ARP:
ARP: 18 bytes frame padding
ARP:
00000000: 50 78 1c 1f 20 1b 50 78 1c 0a e6 b9 08 06 00 01 Px.. .Px.
00000010: 08 00 06 04 00 02 50 78 1c 0a e6 b9 ac 1d 41 48 ....Px.?AH
00000020: 50 78 1c 1f 20 1b ac 1d 41 0a 20 20 20 20 20 20 Px.. .?A.
00000030: 20 20 20 20 20 20 20 20 20 20 20 20
Expert Decode Matrix Host Table Protocol Dist. Statistics
For Help, press F1

数据分析窗口示例

2. 免费工具软件WireShark

1.1. 什么是Wireshark

Wireshark 是网络包分析工具。网络包分析工具的主要作用是尝试捕获网络包， 并尝试显示包的尽可能详细的情况。

你可以把网络包分析工具当成是一种用来测量有什么东西从网线上进出的测量工具，就好像使电工用来测量进入电信的电量的电度表一样。（当然比那个更高级）

过去的此类工具要么是过于昂贵，要么是属于某人私有，或者是二者兼顾。 Wireshark出现以后，这种现状得以改变。

Wireshark可能算得上是今天能使用的最好的开元网络分析软件。

1.1.1. 主要应用

下面是Wireshark一些应用的举例：

- 网络管理员用来解决网络问题
- 网络安全工程师用来检测安全隐患
- 开发人员用来测试协议执行情况
- 用来学习网络协议

除了上面提到的，Wireshark还可以用在其它许多场合。

1.1.2. 特性

- 支持UNIX和Windows平台
- 在接口实时捕捉包
- 能详细显示包的详细协议信息
- 可以打开/保存捕捉的包
- 可以导入导出其他捕捉程序支持的包数据格式
- 可以通过多种方式过滤包
- 多种方式查找包

1) WireShark 简史

- Wireshark（前称Ethereal）是一个网络封包分析软件。使用者可以免费取得软件与其代码，并拥有针对其原码修改及定制化的权利。
- 1997年底，Gerald Combs开始撰写Ethereal软件。1998年7月第一个版本 v0.2.0。此后，Combs收到了来自全世界的修补程式、错误回报与鼓励信件。Ethereal的发展就此开始
- Gilbert Ramirez 开始参予低阶程式的开发
- 1998年10月，来自 Network Appliance 公司的 Guy Harris 参与Ethereal的开发工作
- 1998年底， TCP/IP 课程讲师 Richard Sharpe开始参与开发与加入新协定的功能。他开始在Ethereal上新增的封包撷取功能，几乎包含了当时所有通讯协议
- 2006年6月，因为商标的问题，Ethereal更名为Wireshark

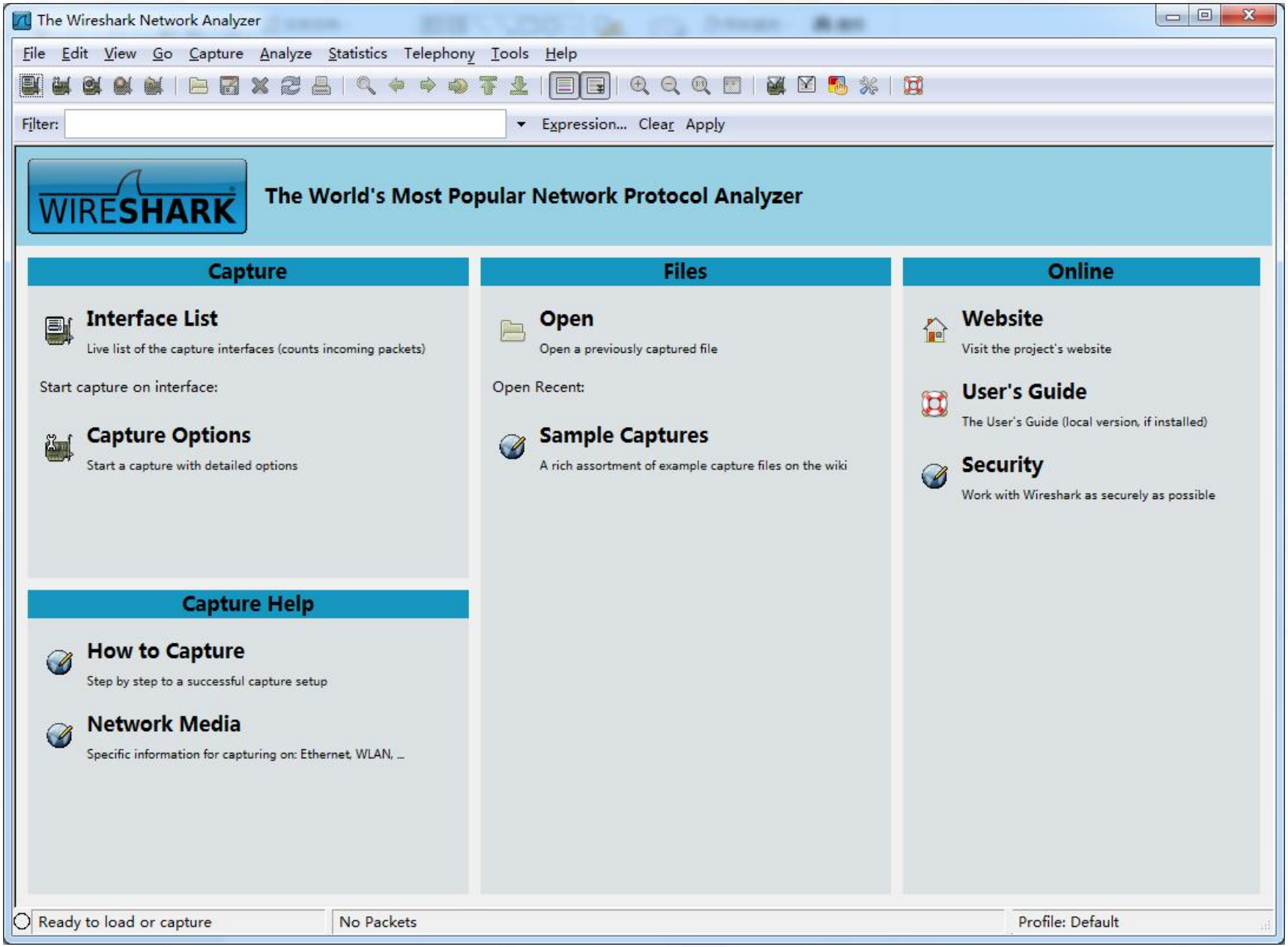
2) WireShark 特点

- 网络管理员使用Ethereal来检测网络问题
- 网络安全工程师使用Ethereal来检查资讯安全相关问题
- 开发者使用Ethereal来为新的通讯协定除错
- 普通使用者使用Ethereal来学习网络协定的相关知识

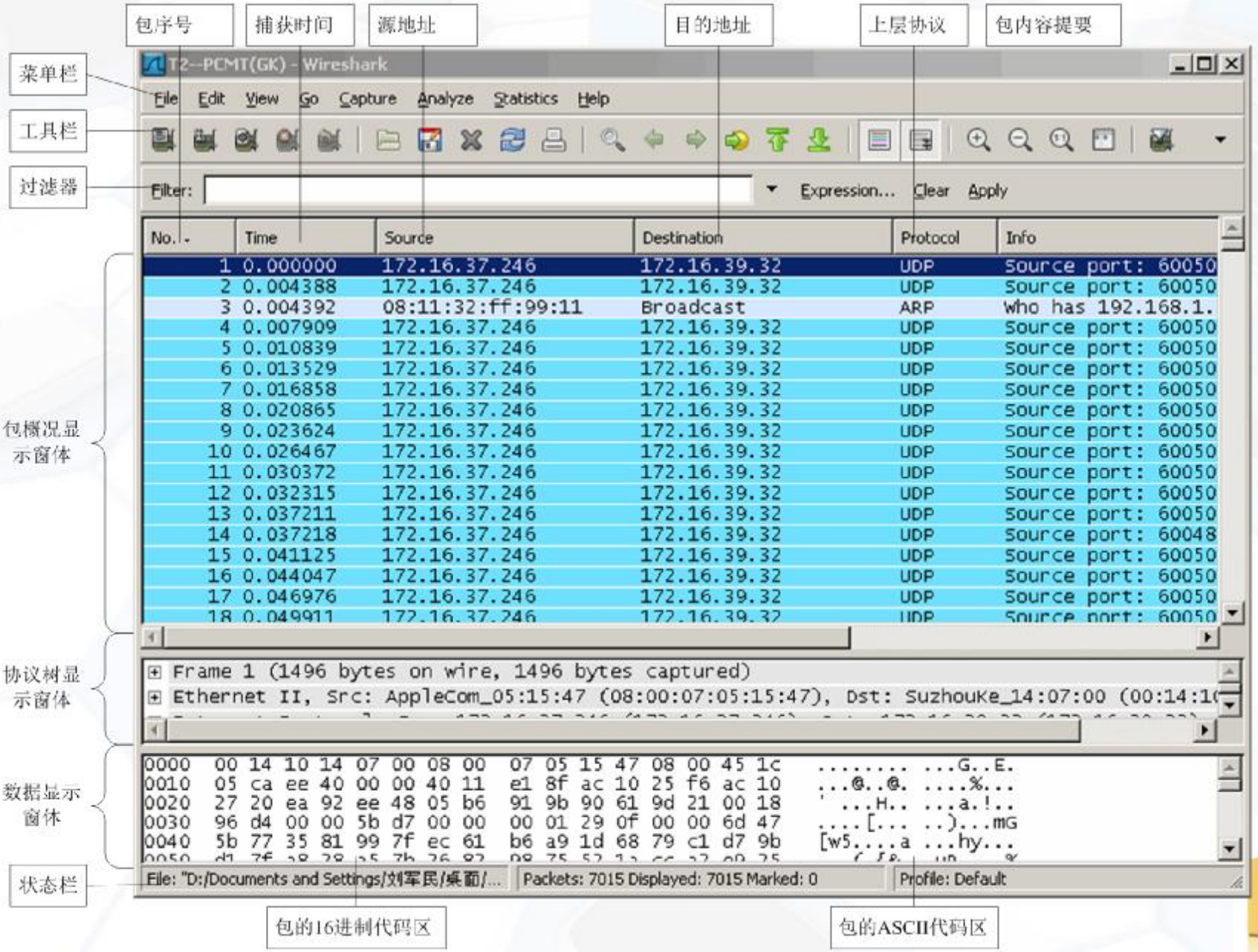
- Ethereal不会对网络封包产生内容的修改 - 它只会反映出目前流通的封包资讯。 Ethereal本身也不会送出封包至网络上
- Wireshark用户手册中文版网络版地址

http://man.lupaworld.com/content/network/wireshark/

可以从网站下载最新版本的Wireshark http://www.wireshark.org/download.html。Wireshark通常在4-8周内发布一次新版

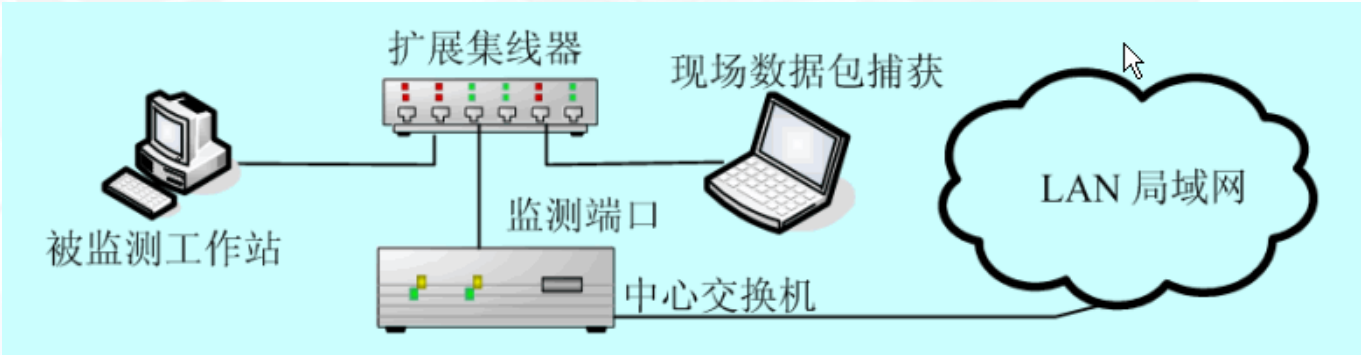

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Capture
Interface List
Live list of the capture interfaces (counts incoming packets)
Start capture on interface:
Capture Options
Start a capture with detailed options
Files
Open
Open a previously captured file
Open Recent:
Sample Captures
A rich assortment of example capture files on the wiki
Online
Website
Visit the project's website
User's Guide
The User's Guide (local version, if installed)
Security
Work with Wireshark as securely as possible
Capture Help
How to Capture
Step by step to a successful capture setup
Network Media
Specific information for capturing on: Ethernet, WLAN, ...
Ready to load or capture
No Packets
Profile: Default

3) 主窗口

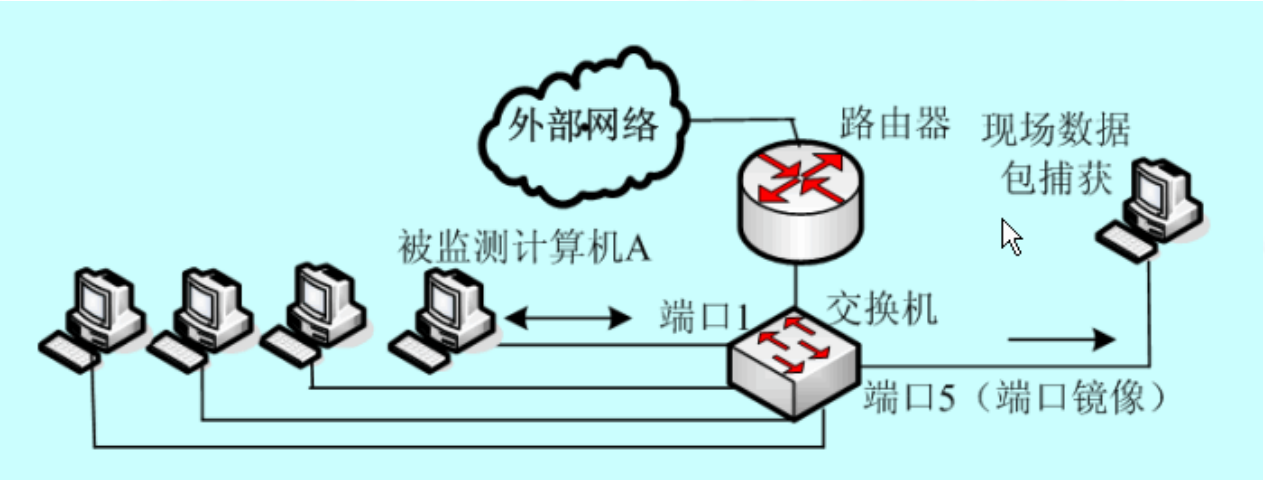

包序号
捕获时间
源地址
目的地址
上层协议
包内容提要
菜单栏
工具栏
过滤器
T2--PCMT(GK) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 172.16.37.246 172.16.39.32 UDP Source port: 60050
2 0.004388 172.16.37.246 172.16.39.32 UDP Source port: 60050
3 0.004392 08:11:32:ff:99:11 Broadcast ARP Who has 192.168.1.
4 0.007909 172.16.37.246 172.16.39.32 UDP Source port: 60050
5 0.010839 172.16.37.246 172.16.39.32 UDP Source port: 60050
6 0.013529 172.16.37.246 172.16.39.32 UDP Source port: 60050
7 0.016858 172.16.37.246 172.16.39.32 UDP Source port: 60050
8 0.020865 172.16.37.246 172.16.39.32 UDP Source port: 60050
9 0.023624 172.16.37.246 172.16.39.32 UDP Source port: 60050
10 0.026467 172.16.37.246 172.16.39.32 UDP Source port: 60050
11 0.030372 172.16.37.246 172.16.39.32 UDP Source port: 60050
12 0.032315 172.16.37.246 172.16.39.32 UDP Source port: 60050
13 0.037211 172.16.37.246 172.16.39.32 UDP Source port: 60050
14 0.037218 172.16.37.246 172.16.39.32 UDP Source port: 60048
15 0.041125 172.16.37.246 172.16.39.32 UDP Source port: 60050
16 0.044047 172.16.37.246 172.16.39.32 UDP Source port: 60050
17 0.046976 172.16.37.246 172.16.39.32 UDP Source port: 60050
18 0.049911 172.16.37.246 172.16.39.32 UDP Source port: 60050
包概况显示窗体
Frame 1 (1496 bytes on wire, 1496 bytes captured)
Ethernet II, Src: AppleCom_05:15:47 (08:00:07:05:15:47), Dst: SuzhouKe_14:07:00 (00:14:1
协议树显示窗体
0000 00 14 10 14 07 00 08 00 07 05 15 47 08 00 45 1c ....G..E.
0010 05 ca ee 40 00 00 40 11 e1 8f ac 10 25 f6 ac 10 ...@..@. ....%...
0020 27 20 ea 92 ee 48 05 b6 91 9b 90 61 9d 21 00 18 ' ...H.. ...a.!..
0030 96 d4 00 00 5b d7 00 00 00 01 29 0f 00 00 6d 47 ....[... ..)...mG
0040 5b 77 35 81 99 7f ec 61 b6 a9 1d 68 79 c1 d7 9b [w5....a ...hy...
数据显示窗体
File: "D:/Documents and Settings/刘军民/桌面/... Packets: 7015 Displayed: 7015 Marked: 0 Profile: Default
状态栏
包的16进制代码区
包的ASCII代码区

4) 网络数据流的监测接入点

- 在被监测计算机上直接捕获；
- 利用集线器将被检测端口的数据分为多路进行捕获

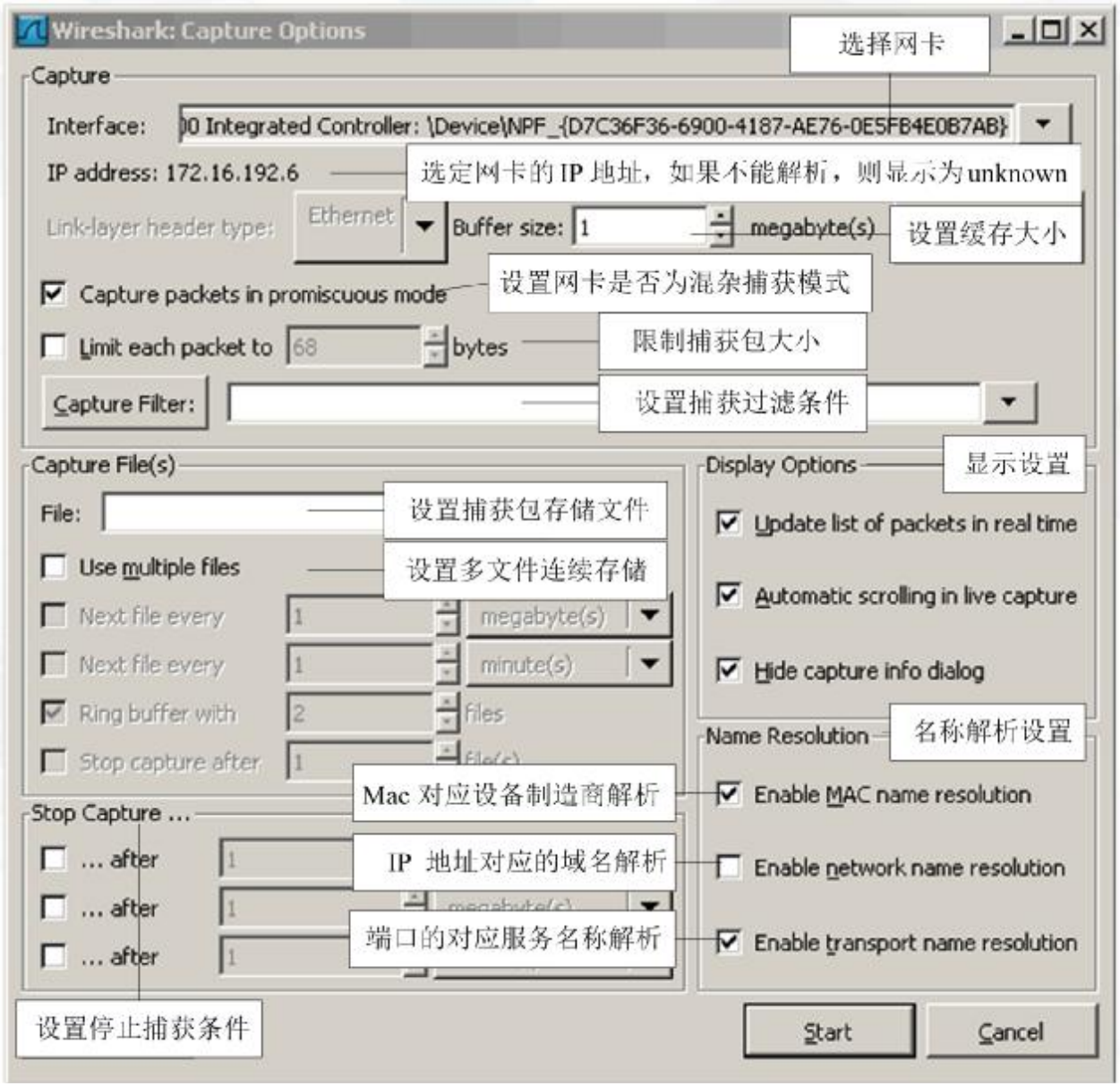


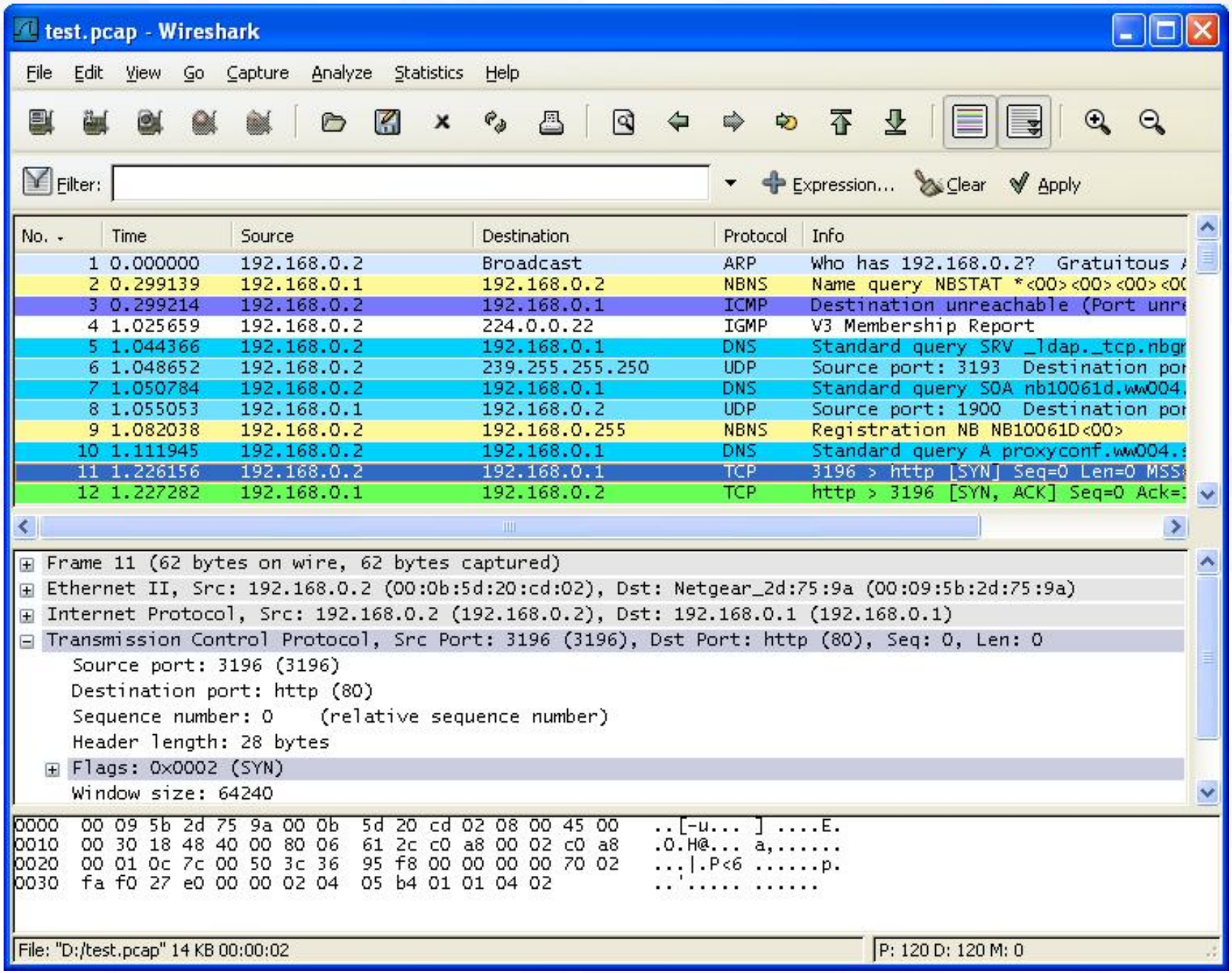
- 利用交换机的端口数据映射功能进行捕获



5) 实时捕获数据包

- 使用按钮”Capture Options“开始捕获取 对话框，选择正确的NIC进行捕获



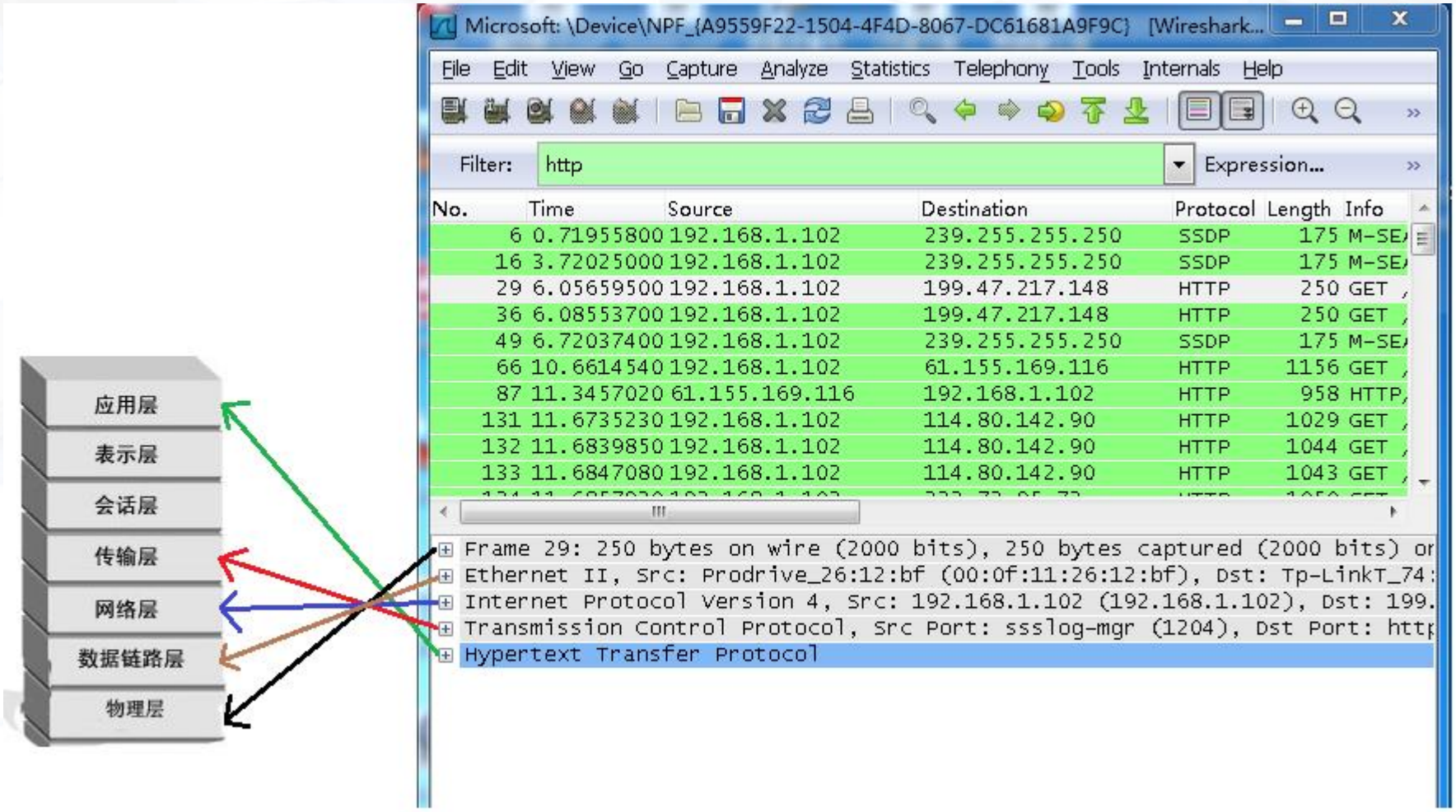

test.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 192.168.0.2 Broadcast ARP Who has 192.168.0.2? Gratuitous
2 0.299139 192.168.0.1 192.168.0.2 NBNS Name query NBSTAT *<00><00><00><00>
3 0.299214 192.168.0.2 192.168.0.1 ICMP Destination unreachable (Port unr
4 1.025659 192.168.0.2 224.0.0.22 IGMP V3 Membership Report
5 1.044366 192.168.0.2 192.168.0.1 DNS Standard query SRV _ldap._tcp.nbg
6 1.048652 192.168.0.2 239.255.255.250 UDP Source port: 3193 Destination por
7 1.050784 192.168.0.2 192.168.0.1 DNS Standard query SOA nb10061d.ww004.
8 1.055053 192.168.0.1 192.168.0.2 UDP Source port: 1900 Destination por
9 1.082038 192.168.0.2 192.168.0.255 NBNS Registration NB NB10061D<00>
10 1.111945 192.168.0.2 192.168.0.1 DNS Standard query A proxyconf.ww004.
11 1.226156 192.168.0.2 192.168.0.1 TCP 3196 > http [SYN] Seq=0 Len=0 MSS
12 1.227282 192.168.0.1 192.168.0.2 TCP http > 3196 [SYN, ACK] Seq=0 Ack=
Frame 11 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a)
Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
Transmission Control Protocol, Src Port: 3196 (3196), Dst Port: http (80), Seq: 0, Len: 0
Source port: 3196 (3196)
Destination port: http (80)
Sequence number: 0 (relative sequence number)
Header length: 28 bytes
Flags: 0x0002 (SYN)
Window size: 64240
0000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00 ..[-u...] ....E.
0010 00 30 18 48 40 00 80 06 61 2c c0 a8 00 02 c0 a8 .0.H@... a,.....
0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 00 70 02 ...|.P<6 ......p.
0030 fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02 ..'..... ......
File: "D:/test.pcap" 14 KB 00:00:02
P: 120 D: 120 M: 0

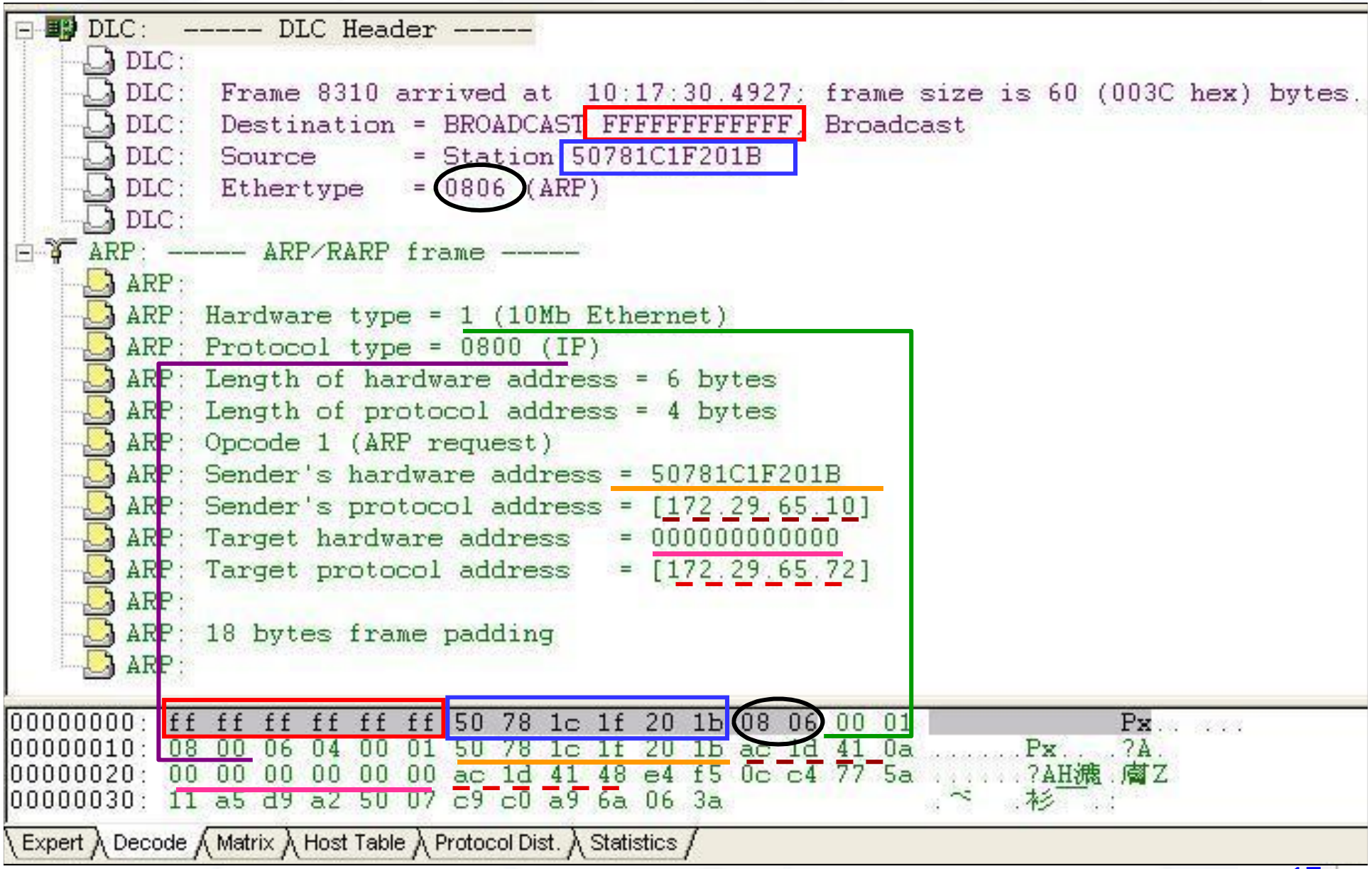
二、 数据分析有什么用？

- 网络管理员会使用wireshark来检查网络问题
- 软件测试工程师使用wireshark抓包，来分析自己测试的软件
- 从事socket编程的工程师会用wireshark来调试
- 网络工程师（华为/中兴/思科）都会用到wireshark

http://www.cnblogs.com/tankxiao/archive/2012/10/10/2711777.html

1. 理解网络的层次


Microsoft: \Device\NPF_{A9559F22-1504-4F4D-8067-DC61681A9F9C} [Wireshark...
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http
Expression...
No. Time Source Destination Protocol Length Info
6 0.71955800 192.168.1.102 239.255.255.250 SSDP 175 M-SE
16 3.72025000 192.168.1.102 239.255.255.250 SSDP 175 M-SE
29 6.05659500 192.168.1.102 199.47.217.148 HTTP 250 GET
36 6.08553700 192.168.1.102 199.47.217.148 HTTP 250 GET
49 6.72037400 192.168.1.102 239.255.255.250 SSDP 175 M-SE
66 10.6614540 192.168.1.102 61.155.169.116 HTTP 1156 GET
87 11.3457020 61.155.169.116 192.168.1.102 HTTP 958 HTTP/
131 11.6735230 192.168.1.102 114.80.142.90 HTTP 1029 GET
132 11.6839850 192.168.1.102 114.80.142.90 HTTP 1044 GET
133 11.6847080 192.168.1.102 114.80.142.90 HTTP 1043 GET
Frame 29: 250 bytes on wire (2000 bits), 250 bytes captured (2000 bits) or
Ethernet II, Src: Prodrive_26:12:bf (00:0f:11:26:12:bf), Dst: Tp-LinkT_74:
Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: 199.
Transmission Control Protocol, Src Port: ssslog-mgr (1204), Dst Port: http
Hypertext Transfer Protocol
应用层
表示层
会话层
传输层
网络层
数据链路层
物理层


DLC: ----- DLC Header -----
DLC:
DLC: Frame 8310 arrived at 10:17:30.4927; frame size is 60 (003C hex) bytes.
DLC: Destination = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source = Station 50781C1F201B
DLC: Ethertype = 0806 (ARP)
DLC:
ARP: ----- ARP/RARP frame -----
ARP:
ARP: Hardware type = 1 (10Mb Ethernet)
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 1 (ARP request)
ARP: Sender's hardware address = 50781C1F201B
ARP: Sender's protocol address = [172.29.65.10]
ARP: Target hardware address = 000000000000
ARP: Target protocol address = [172.29.65.72]
ARP:
ARP: 18 bytes frame padding
ARP:
00000000: ff ff ff ff ff ff 50 78 1c 1f 20 1b 08 06 00 01
00000010: 08 00 06 04 00 01 50 78 1c 1f 20 1b ac 1d 41 0a
00000020: 00 00 00 00 00 00 ac 1d 41 48 e4 f5 0c c4 77 5a
00000030: 11 a5 d9 a2 50 07 c9 c0 a9 6a 06 3a
Expert
Decode
Matrix
Host Table
Protocol Dist.
Statistics

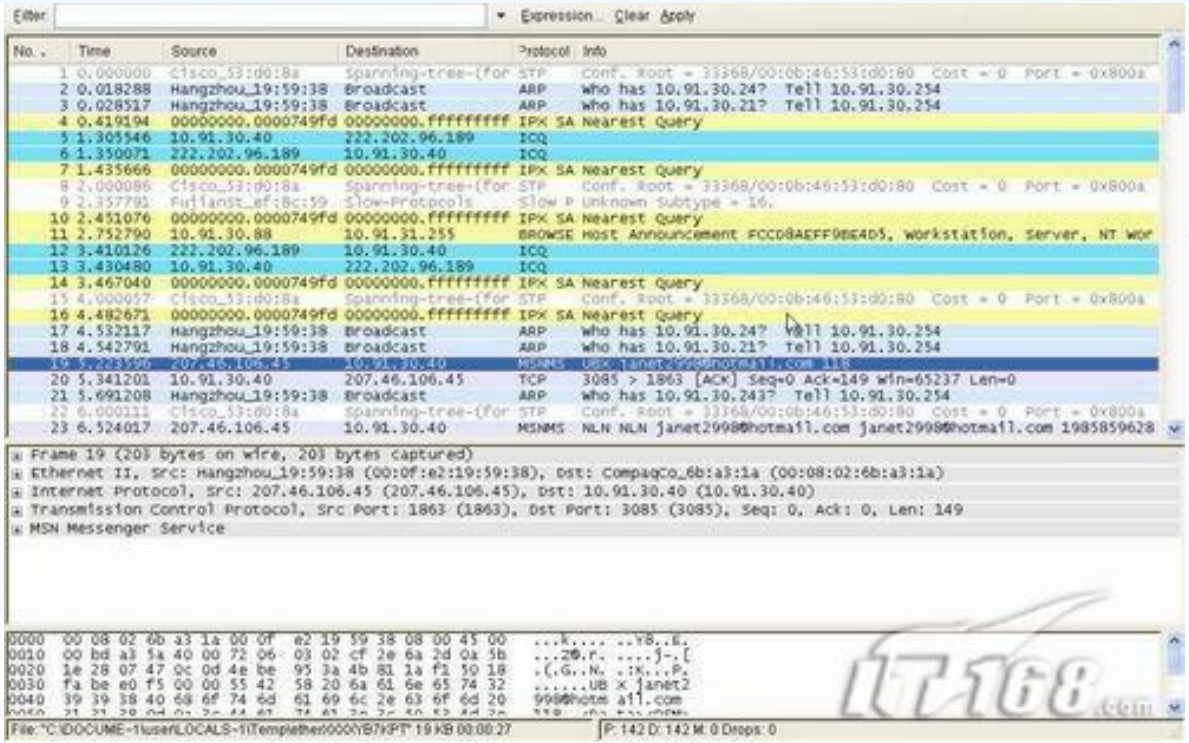
数据内容分析举例

2. 了解网络中的活动

（1）检测网中是否有MSN或QQ在使用

有的时候我们企业不希望员工在上班时通过MSN或QQ聊天，并针对这些IM交流软件进行了封锁，但是封锁和突破总是对立的，很多员工会找到代理工具或者其他方法来突破限制。不过不管他采用何种方法都无法逃避Wireshark的火眼金睛。

我们打开Wireshark并设置好监控网卡，之后扫描网络中的数据，收集一段时间后停止捕获来查看数据包，如果网络中有MSN或者QQ在使用，Wireshark会记录这些数据通话，在protocol协议处显示为ICQ的通讯就是OICQ，而显示为MSNMS的话则说明此数据包是MSN发送接收的，并且通过具体内容我们还可以看到MSN的通话对象的邮件地址（如图7）。



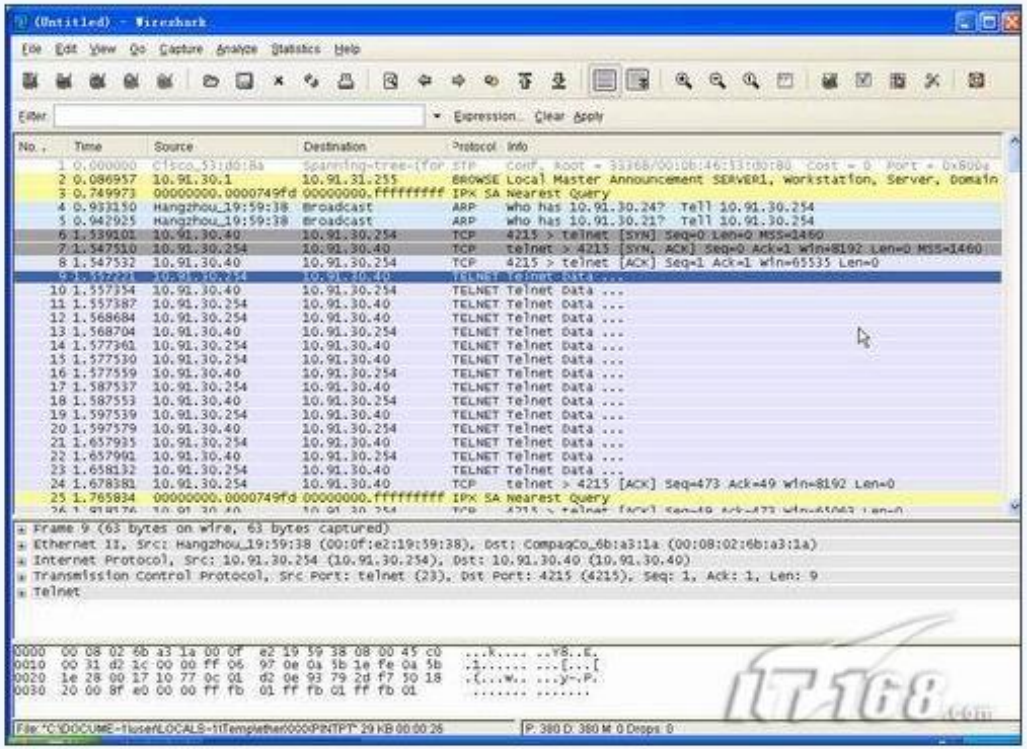
http://publish.it168.com/2007/0328/20070328016603.shtml

3. 窃取用户信息

（3）检测明文数据包

正如前面所说Wireshark可以针对网络中的明文数据包内容进行分析，例如我们在使用telnet来管理路由交换设备时所有的传输数据都是基于明文的，这样通过Wireshark可以将telnet输入的指令分析出来。

首先检测网络数据包，如果在检测过程中有人进行telnet操作，那么在数据包显示窗口中会看到对应的telnet协议，以及通讯双方的IP地址信息（如图10）。



4. 了解网络应用开发的细节

前一段时间接了一个任务，把目前主流的应用市场请求响应全抓出来分析一下，出个报告。至于分析这些应用的目的就不直说了。然后在邮件后面列出了一个长长的应用列表，包括：91、360、机锋、应用汇、安智、安卓...等等，以致于我把这些应用都装测试机上发现手机内存不够用了。

不过加班加点昨天可算弄完，分析结果就不贴出来了，这里只记录一下方法。

一、需要使用如下软件：

android sdk （我装的2.1）

抓包：tcpdump

分析包：Wireshark Version 1.6.2

二、抓包(需要root过的手机)：

首先进入android sdk中的platform-tools路径，执行：

adb push D:/tcpdump /data/local/tcpdump //把tcpdump放在data/local路径下

执行adb shell，进入android的shell环境，执行su切换到root用户。

最后执行：/data/local/tcpdump -p -vv -s 0 -w /sdcard/capture.pcap

这时抓包就开始了，可以在手机上使用你需要分析的应用进行抓包。

抓完之后按ctrl+c停止抓包，然后退出android shell环境，执行：

adb pull /sdcard/capture.pcap

获取刚才抓到的文件到本机。

三、分析包：

用wireshark打开刚才获取到的pcap文件：

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco_e8:51:cb	Broadcast	ARP	60	who has 10.18.123.80? Tell 10.18.123.254
2	0.000223	Cisco_e8:51:cb	Broadcast	ARP	60	who has 10.18.123.178? Tell 10.18.123.254
3	0.000175	Cisco_e8:51:cb	Broadcast	ARP	60	who has 10.18.120.114? Tell 10.18.123.254
4	0.000500	Cisco_e8:51:cb	Broadcast	ARP	60	who has 10.18.120.154? Tell 10.18.123.254
5	0.000795	Cisco_e8:51:cb	Broadcast	ARP	60	who has 10.18.123.208? Tell 10.18.123.254
6	0.001160	Cisco_e8:51:cb	Broadcast	ARP	60	who has 10.18.123.152? Tell 10.18.123.254
7	0.102966	IntelCor_03:32:d2	Broadcast	ARP	42	who has 10.18.121.138? Tell 10.18.121.211
8	0.306033	Cisco_e8:51:cb	Broadcast	ARP	60	who has 10.18.120.15? Tell 10.18.123.254
9	0.306493	Cisco_e8:51:cb	Broadcast	ARP	60	who has 10.18.120.220? Tell 10.18.123.254
10	0.306918	LiteonTe_95:f5:28	Broadcast	ARP	42	who has 10.18.121.159? Tell 10.18.123.153
11	0.511253	10.18.121.114	10.18.123.255	BJNP	58	Scanner Command: Discover
12	0.715933	74:de:2b:8d:4c:ba	Broadcast	ARP	42	who has 10.18.121.159? Tell 10.18.121.29

下载

http://shensy.iteye.com/blog/1904118