### 第1章介绍

長日 1.1. 什么是 Wireshark <u>1.1.1. 主要应用</u> <u>1.1.2. 特性</u> 1.1.3. 捕捉多种网络接口 1.1.4. 支持多种其它程序捕捉的文件 1.1.5. 支持多格式输出 1.1.6. 对多种协议解码提供支持 <u>1.1.7. 开源软件</u> <u>1.1.8. Wireshark 不能做的事</u> 1.2. 系通需求 <u>1.2.1. 一般说明</u> 1.2.2. Microsoft Windows 1.2.3. Unix/Linux 1.3. 从哪里可以得到 Wireshark <u>1.4. Wiresahrk 简史</u> 1.5. Wireshark 开发维护 1.6. 汇报问题和获得帮助 <u>1.6.1. 网站</u> 1.6.2. 百科全书 <u>1.6.3. FAQ</u> <u>1.6.4. 邮件列表</u> 1.6.5. 报告问题 <u>1.6.6. 在 UNIX/Linux 平台追踪软件错误</u> 1.6.7. 在 Windows 平台追踪软件错误

### 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 通过过滤以多种色彩显示包 创建多种统计分析 ...还有许多

### 不管怎么说,要想真正了解它的强大,您还得使用它才行 图 1.1. Wireshark **捕捉包并允许您检视其内容**

🗹 test. pcap - Wireshark								
<u>Eile E</u> dit	<u>V</u> iew <u>G</u> o	⊆apture <u>A</u> nalyz	e Statistics !	Help				
	oi oi	🕷   🖻	🗶 🗙 🖓	• ≞ [	9	⇔ ¢0		
Eilter:						- 🕂 E	xpression 🦢 ⊆lear 🖋 Apply	
No. +	Time	Source	[	estination)		Protocol	Info	^
1	0.000000	192.168.0.2	E	Proadcast		ARP	Who has 192.168.0.2? Gratuitous /	
2	0.299139	192.168.0.1	1	.92.168.0.2		NBNS	Name query NBSTAT *<00><00><00><0(	
3	0.299214	192.168.0.2		.92.168.0.1		ICMP	Destination unreachable (Port unre	
4	1.025659	192.168.0.2	4	24.0.0.22		IGMP	V3 Membership Report	
6	1.044366	192.168.0.2		.92.168.U.1 170 755 755	250	UND	Source port: 3193 Destination por	
7	1.050784	192.168.0.2		92 168 0 1	.250	DNS	Standard query SOA ph10061d we004	
8	1.055053	192.168.0.1	1	92.168.0.2		UDP	Source port: 1900 Destination por	
9	1.082038	192.168.0.2	1	.92.168.0.2	55	NBNS	Registration NB NB10061D<00>	
10	1.111945	192.168.0.2		.92.168.0.1		DNS	Standard guery A proxyconf.ww004.:	
11	1.226156	192.168.0.2	1	.92.168.0.1		TCP	3196 > http [SYN] Seq=0 Len=0 MSS	
12	1.227282	192.168.0.1	1	.92.168.0.2		TCP	http > 3196 [SYN, ACK] Seq=0 Ack=:	¥
<								
🕀 Erame	11 (62 byt	es on wire.	62 bytes car	otured)				~
Ethern	et II Src	· 192 168 0	2 (00 • 0h • 5 d	20.cd.02)	Dst. Neto	ear 2d.7	75.9a (00.09.5h.2d.75.9a)	-
Totors	et Brotoco	1 Sec. 103		169 0 3)	Det: 103	169 0 1	(103 169 0 1)	
Therefore Control Destand, Sec. 2412(192.166.0.2), DST: 192.168.0.1 (192.168.0.1)								
- Transm	iission Con	trol Protoco	I, SPC Port	: 2130 (212	16), DST PC	ort: nttp	0 (80), Sed: 0, Len: 0	=
Sour	rce port: 3	3196 (3196)						-
Dest	tination po	ort: http (80	)					
- Seqi	uence numbe	er:0 (rel	ative seque	nce number)	)			
Head	der length:	: 28 bytes						
🕀 Flag	15: 0x0002	(SYN)						
Wind	dow size: P	54240						~
	30W 312C. C							-
0000 00	09 5b 2d 7	'5 9a 00 0b	5d 20 cd 02	08 00 45 (	)0[-u.	]	E.	
0020 00	01 0c 7c 0	0 00 80 06	95 f8 00 00		10 .U.H@. 12	a,	- n-	
0030 fa	f0 27 e0 0	0 00 02 04	05 b4 01 01	04 02				
File: "D:/tes	t.pcap" 14 KB (	00:00:02					P: 120 D: 120 M: 0	.:

### 1.1.3. 捕捉多种网络接口

Wireshark 可以捕捉多种网络接口类型的包,哪怕是无线局域网接口。想了解支持的所有网络接口类型,可以在我们的网站上找到 <u>http://wiki.wireshark.org/CaptureSetup/NetworkMedia.</u>

### 1.1.4. 支持多种其它程序捕捉的文件

Wireshark 可以打开多种网络分析软件捕捉的包,详见???

### 1.1.5. 支持多格式输出

Wieshark 可以将捕捉文件输出为多种其他捕捉软件支持的格式,详见???

### 1.1.6. 对多种协议解码提供支持

可以支持许多协议的解码(在 Wireshark 中可能被称为解剖)???

### 1.1.7. 开源软件

Wireshark 是开源软件项目,用 GPL 协议发行。您可以免费在任意数量的机器上使用它,不用担心授权和付费问题,所有的源代码在 GPL 框架下都可以免费使用。因为以上原因,人们可以很容易在 Wireshark 上添加新的协议,或者将其作为插件整合到您的程序里,这种应用十分广泛。

### 1.1.8. Wireshark 不能做的事

Wireshark 不能提供如下功能

Wireshark 不是入侵检测系统。如果他/她在您的网络做了一些他/她们不被允许的奇怪的事情,Wireshark 不会警告您。但是 如果发生了奇怪的事情,Wireshark 可能对察看发生了什么会有所帮助。<sup>[3]</sup> Wireshark 不会处理网络事务,它仅仅是"测量"(监视)网络。Wireshark 不会发送网络包或做其它交互性的事情(名称解析除 外,但您也可以禁止解析)。

[1] 译者注:因为不是入侵检测之用,所以不会将入侵检测和普通通信区别对待,但是都会体现在网络包里面,如果您有足够的经验,或许能通过监视网络包发现入侵检测

### 1.2. 系通需求

想要安装运行 Wireshark 需要具备的软硬件条件...

### 1.2.1. 一般说明

给出的值只是最小需求,在大多数网络中可以正常使用,但不排除某些情况下不能使用。[4]

在繁忙的网络中捕捉包将很容塞满您的硬盘!举个简单的例子:在100MBIT/s全双工以太网中捕捉数据将会产生750MByties/min的数据!在此类网络中拥有高速的 CPU,大量的内存和足够的磁盘空间是十分有必要的。

如果 Wireshark 运行时内存不足将会导致异常终止。可以在 <u>http://wiki.wireshark.org/KnownBugs/OutOfMemory</u> 察看详细介 绍以及解决办法。

Wireshark 作为对处理器时间敏感任务,在多处理器/多线程系统环境工作不会比单独处理器有更快的速度,例如过滤包就 是在一个处理器下线程运行,除了以下情况例外:在捕捉包时"实时更新包列表",此时捕捉包将会运行在一个处理下,显 示包将会运行在另一个处理器下。此时多处理或许会有所帮助。<sup>[2]</sup>

### 1.2.2. Microsoft Windows

Windows 2000,XP Home 版,XP Pro 版,XP Tablet PC, XP Media Center, Server 2003 or Vista(推荐在 XP 下使用) 32-bit 奔腾处理器或同等规格的处理器(建议频率: 400MHz 或更高),64-bit 处理器在 WoW64仿真环境下-见一般说明 128MB 系统内存(建议256Mbytes 或更高)

75MB 可用磁盘空间(如果想保存捕捉文件,需要更多空间) 800\*600(建议1280\*1024或更高)分辨率最少65536(16bit) 色,(256色旧设备安装时需要选择"legacy GTK1")

网卡需求:

以太网: windows 支持的任何以太网卡都可以

无线局域网卡:见 MicroLogix support list,不捕捉802.11包头和无数据桢。

其它接口见: <u>http://wiki.wireshark.org/CaptureSetup/NetworkMedia</u>

说明

基于以下三点原因,将不会对旧版 Windows 提供支持:没有任何开发人员正在使用那些操作系统,这将使支持变得更加困难,Wireshark 运行所依赖的库文件(如 GTK, WinPCap 等)也放弃对它们的支持。同样,微软也放弃了对它们的技术支持。

Windows 95,98和 ME 不能运行 Wireshark。已知的最后一个可以运行在以上平台的版本是 Ethereal0.99.0(需要安装 WinPCap3.1),你依然可以使用从: <u>http://ethereal.com/download.html</u>获得。顺便提一下: 微软于2006年1月11日停止对98/ME 支持。

Windows NT 4.0今后将无法运行 Wireshark.最有一个已知版本是 Wireshark0.99.4(需安装自带的 WinPCap3.1),你依然可以从: <u>http://prdownloads.sourceforge.net/wireshark/wireshark-setup-0.99.4.exe</u>得到它。顺便提一下:微软于2005年12月31日停止对 NT 4.0的支持。

Windows CE 及嵌入版 windows (NT/XP) 不被支持。

64-bit 处理器运行 Wireshark 需要在32bit 仿真环境下(称作 WoW64),最低需要安装 WinPCap4.0。 支持多显示(不知道是显示其还是监视器)安装,但会遇到一些不可预料的问题。

### 1.2.3. Unix/Linux

Wireshark 目前可以运行在许多 UNIX 平台,系统可以对照上面 Windows 下的指标。 二进制包最少在以下平台可用: APPle Mac OSX Debian GNU/Linux FreeBSD NetBSD OpenPKG Red Hat Fedora/Enterprise Linux rPath Linux Sun Solaris/i386 Sun Solaris/Sparc 如果二进制包在您的平台无法使用,你可以下载源文件并尝试编译它。希望您能发送邮件到 wireshark-dev[AT]wireshark.org.分享您的经验。

(4) 译者注: 原文 "The values below are the minimum requirements and only "rules of thumb" for use on a moderately used network",其中"rules of thumb"中译名应该是拇指规则,但网上关于拇指规则解释莫衷一是,大致意思是说:大多数情况下适用,但并非所有情况。这里翻译的有点别扭

<sup>[5]</sup> 译者注:我对这句话的理解是,正如播放电影一样,高性能的处理器只会增强显示效果,您并不需要将原来30分钟的影 片10分钟之内看完。当然,对减少延时还是有作用的。但是感觉这句有点阅读困难,可能翻译的有点问题.

### 1.3. 从哪里可以得到 Wireshark

你可以从我们的网站下载最新版本的 Wireshark http://www.wireshark.org/download.html.网站上您可以选择适合您的镜像站点。

Wireshark 通常在4-8周内发布一次新版本

如果您想获得 Wireshark 发布的消息通知,你可以订阅 Wireshark-announce 邮件列表。详见<u>第 1.6.4 节 "邮件列表"</u>

### 1.4. Wiresahrk 简史<sup>6</sup>

1997年以后,Gerald Combs 需要一个工具追踪网络问题并想学习网络知识。所以他开始开发 Ethereal (Wireshark 项目以前 的名称) 以解决以上的两个需要。

Ethereal 是第一版,经过数次开发,停顿,1998年,经过这么长的时间,补丁,Bug 报告,以及许多的鼓励,0.2.0版诞生了。 Ethereal 就是以这种方式成功的。

此后不久, Gilbert Ramirez 发现它的潜力,并为其提供了底层分析

1998年10月, Guy Harris 正寻找一种比 TcpView 更好的工具,他开始为 Ethereal 进行改进,并提供分析。

998年以后,正在进行 TCP/IP 教学的 Richard Sharpe 关注了它在这些课程中的作用。并开始研究该软件是否他所需要的协议。如果不行,新协议支持应该很方便被添加。所以他开始从事 Ethereal 的分析及改进。

从那以后,帮助 Ethereal 的人越来越多,他们的开始几乎都是由于一些尚不被 Ethereal 支持的协议。所以他们拷贝了已有的解析器,并为团队提供了改进回馈。

2006年项目 Moved House (这句不知道怎么翻译)并重新命名为: Wireshark.

⑥本段因为有很多协议,程序开发方面的术语,翻译得比较糟糕

### 1.5. Wireshark 开发维护

Wireshark 最初由 Gerald Combs 开发。目前由 Wireshark team 进行进一步开发和维护。Wireshark team 是一个由修补 bug 提高 Wireshark 功能的独立成员组成的松散组织。

有大量的成员为 Wireshark 提供协议分析。同时我们也希望这些活动能持续机芯。通过查看 Wireshark 帮助菜单下的 About,你可以找到为 Wireshark 提供代码的人员名单,或者你也可以通过 Wireshark 网站的 <u>authors</u>页面找到。

Wireshark 是开源软件项目,发布遵循 GNU General Public Licence (GPL 协议),所有源代码可以在 GPL 框架下免费使用。欢 迎您修改 Wireshark 以便适合您的需要,如果您可以提供您的改进给 Wireshark team ,我们将不胜感激。

为 Wireshark Team 提供您的改进建议,有以下益处:

如果其他人发现您提供的改进十分有用会肯定它们的价值,您将会得知你曾像 Wireshark team 一样帮助过他人

The developers of Wireshark might improve your changes even more, as there's always room for improvement. Or they may implement some advanced things on top of your code, which can be useful for yourself too.

The maintainers and developers of Wireshark will maintain your code as well, fixing it when API changes or other changes are made, and generally keeping it in tune with what is happening with Wireshark. So if Wireshark is updated (which is done often), you can get a new Wireshark version from the website and your changes will already be included without any effort for you.

Wireshar 源代码和二进制 kits (二进制工具包?) 可以根据自己的平台对应下载, 网站是: <u>http://www.wireshark.org/download.html.</u>

### 1.6. 汇报问题和获得帮助

如果您在使用中碰到了问题,或者您需要 Wireshark 的帮助,有以下几种可能让您有兴趣的方法(当然,还包括这本书)。

### 1.6.1. 网站

通过访问 http://www.wireshark.org 你将会发现关于 Wireshark 许多有用的信息。

#### 1.6.2. 百科全书

Wireshark Wiki (<u>http://wiki.wireshark.org</u>)提供广泛的跟 Wireshark 以及捕捉包有关信息。你将会发现一些没有被包括在本书 内信息,例如:wiki 上有解释如何在交换网络捕捉包,同时我们正努力建立协议参考,等等。 最好的事情是,如果对某些知识有独到见解(比如您精通某种协议),您可以通过浏览器编辑它。

#### 1.6.3. FAQ

最经常被问到的问题"Frequently Asked Questions"提供一个经常被问到的问题以及答案的列表。

#### **Read The FAQ**

在您发送任何邮件到邮件列表之前,确信您已经阅读了FAQ,因为这里面很可能已经提供了您想问的问题,答案。这将大大节约您的时间(记住,有很多人提交了大量的邮件)。

#### 1.6.4. 邮件列表

下面的几个几个邮件列表,分别属于不同的主题:

Wireshark-users

这是一个 Wireshark 用户的列表,大家提交关于安装和使用 Wireshark 的问题,其它人(非常有用)提供的答案。(译者注: 其他人当然也是指用户?)

#### wireshark-announce

这是一个关于程序发布信息的列表,通常每4-8周出现一次。

#### wireshark-dev

这是一个关于 Wireshark 开发的邮件列表,如果开始开发协议分析,可以从加入该列表

你可以通过网站 <u>http://www.wireshark.org</u> 订阅每个邮件列表.简单点击网站左手边的邮件列表链接就可以。邮件同样在网站上可以看到存档。

#### 提示

你可以搜索存档看看有没有人问过跟你一样的问题,或许您的问题已经有了答案。这样 您就不必提交邮件以等待别人答复您了。

#### 1.6.5. 报告问题

#### 注意

在您提交任何问题之前,请确定您安装的是最新版本的 Wireshark。

当您提交问题的时候,如果您提供如下信息将会对解决问题很有帮助。

Wireshark 的版本,及其依赖的库的版本,如GTK+,等等。你可以通过 Wireshark –v 命令获得版本号。(估计是 UNIX/Linux 平台)。

运行 Wireshark 的平台信息。

关于问题的详细描述。

如果您得到错误或者警告信息,拷贝错误信息的文本(以及在此之前或之后的文本,如果有的话),这样其他人可能会发现 发生问题的地方。请不要发送诸如: "I got a warning while doing x"四,因为这样看起来不是个好主意。

#### 不要发送大文件

不要发送过大的文件(>100KB)到邮件列表,在邮件中附加一个能提供足够数据的记事 本就可以。大文件会让很多邮件列表里的那些对您的问题不感兴趣的用户感到恼怒。如 果需要,你可以单独发送那些数据给对您问题真正感兴趣,要求您发送数据的人。

#### 不要发送机密信息!

如果您发送捕捉数据到邮件列表,请确定它们不包含敏感或者机密信息,比如密码或者 诸如此类的。

### 1.6.6. 在 UNIX/Linux 平台追踪软件错误

如果您发送捕捉数据到邮件列表,请确定它们不包含敏感或者机密信息,比如密码或者诸如此类的。 你可以通过如下命令获得追踪信息:

\$ gdb `whereis wireshark | cut -f2 -d: | cut -d' ' -f2` core >&bt.txt

backtrace

 $^{D}$ 

\$

```
注意
在逐字输入第一行的字符!<sup>[8]</sup>
注意
追踪是一个 GDB 命令。你可以在输完第一上以后输入它,但是会没有相应,^D 命令
(CTL+D)将会退出 GDB 命令。以上命令让你在当前目录得到一个名为 bt.txt 的文本文
件,它包含您的 bug 报告。
注意
如果您缺少 GDB,您必须检查您的操作系统的调试器。
你可以发送追踪邮件到 wireshark-dev[AT]wireshark.org 邮件列表
```

### 1.6.7. 在 Windows 平台追踪软件错误

Windows下无法包含符号文件(.pdb),它们非常大。因此不太可能创建十分有意义的追踪文件。你将汇报软件错误就像前面描述的其他问题一样。(这句不尽人意)

[2] 译者注:那句话的意思是,我在 XX 时碰到一个警告信息
[8] 译者注:原文是: "Type the characters in the first line verbatim! Those are back-tics there!",Those are back-tics there!不知道是 什么意思,back-tics=后勤抽搐?熟悉 Linux 的或许知道

### 第2章编译/安装Wireshark

### 目录

2.1. 须知 2.2. 获得源 2.3. 在 UNIX 下安装之前 2.4. 在UNIX 下编译 Wireshark 2.5. 在 UNIX 下安装二进制包 2.5.1. 在 Linux 或类似环境下安装 RPM 包 <u>2.5.2.</u> 在 Debian 环境下安装 Deb 包 2.5.3. 在 Gentoo Linux 环境下安装 Portage 2.5.4. 在 FreeBSD 环境下安装包 2.6. 解决 UNIX 下安装过程中的问题 2.7. 在 Windows 下编译源 2.8. 在 Windows 下安装 Wireshark 2.8.1. 安装 Wireshark 2.8.2. 手动安装 WinPcap 2.8.3. 更新 Wireshark 2.8.4. 更新 WinPcap 2.8.5. 卸载 Wireshark 2.8.6. 卸载 WinPcap

### 2.1. 须知

万事皆有开头,Wireshark也同样如此。要想使用Wireshark,你必须: 获得一个适合您操作系统的二进制包,或者 获得源文件为您的操作系统编译。 目前,只有两到三种 Linux 发行版可以传送 Wireshark,而且通常传输的都是过时的版本。至今尚未有 UNIX 版本可以传输 Wireshark .Windows 的任何版本都不能传输 Wireshark.基于以上原因,你需要知道从哪能得到最新版本的 Wireshark 以及如 何安装它。 本章节向您展示如何获得源文件和二进制包,如何根据你的需要编译 Wireshark 源文件。 以下是通常的步骤: 下载需要的相关包,例如:源文件或者二进制发行版。

将源文件编译成二进制包(如果您下载的是源文件的话)。这样做做可以整合编译和/或安装其他需要的包。 安装二进制包到最终目标位置。

### 2.2. 获得源

你可以从 Wireshark 网站 <u>http://www.wireshark.org</u>.同时获取源文件和二进制发行版。选择您需要下载的链接,然后选择源文件或二进制发行包所在的镜像站点(尽可能离你近一点的站点)。

### 下载所有需要的文件!

一般来说,除非您已经下载 Wireshark,如果您想编译 Wireshark 源文件,您可能需要下载 多个包。这些在后面章节会提到。

#### 注意

当你发现在网站上有多个二进制发行版可用,您应该选择适合您平台的版本,他们同时 通常会有多个版本紧跟在当前版本后面,那些通常时拥有那些平台的用户编译的。

基于以上原因,您可能想自己下载源文件自己编译,因为这样相对方便一点。

### 2.3. 在 UNIX 下安装之前

在编译或者安装二进制发行版之前,您必须确定已经安装如下包: GTK+, The GIMP Tool Kit. 您将会同样需要 Glib.它们都可以从 <u>www.gtk.org</u> 获得。 Libpcap, Wireshark 用来捕捉包的工具 您可以从 <u>www.tepdump.org</u> 获得。 根据您操作系统的不同,您或许能够安装二进制包,如 RPMs.或许您需要获得源文件并编译它。 如果您已经下载了 GTK+源文件,<u>例 2.1 "从源文件编译 GTK+"</u>提供的指令对您编译有所帮助。 **例 2.1. 从源文件编译 GTK+** gzip -dc gtk+-1.2.10.tar.gz | tar xvf -<much output removed> ./configure <much output removed> make install <much output remove> test------

#### 注意

您可能需要修改例 2.1 "从源文件编译 GTK+" 中提供的版本号成对应您下载的 GTK+版本。如果 GTK 的目录发生变更,您同样需要修改它。,tar xvf 显示您需要修改的目录。 注意

如果您使用 Linux,或者安装了 GUN tar,您可以使用 tar zxvfgtk+-1.2.10.tar.gz 命令。同 样也可能使用 gunzip -c 或者 gzcat 而不是许多 UNIX 中的 gzip -dc

### 注意

如果您在 windows 中下载了 gtk+ 或者其他文件。您的文件可能名称为: gtk+-1\_2\_8\_tar.gz 如果在执行<u>例 2.1"从源文件编译 GTK+"</u>中的指令时有错误发生的话,你可以咨询 GTK+网站。 如果您已经下载了 libpcap 源,一般指令如<u>例 2.2"编译、安装 libpcap"</u>显示的那样会帮您完成编译。同样,如果您的操作 系统不支持 **tcpdump**,您可以从 <u>tcpdump</u> 网站下载安装它。

### 例 2.2. 编译、安装 libpcap

gzip -dc libpcap-0.9.4.tar.Z | tar xvf -<much output removed> cd libpcap-0.9.4 ./configure <much output removed> make <much output removed> make install <much output removed>

### 注意

Libpcap 的目录需要根据您的版本进行修改。tar xvf 命令显示您解压缩的目录。

RedHat 6.x 及其以上版本环境下(包括基于它的发行版,如 Mandrake),您可以直接运行 RPM 安装所有的包。大多数情况 下的 Linux 需要安装 GTK+和 Glib.反过来说,你可能需要安装所有包的定制版。安装命令可以参考例 2.3 "在 RedHat Linux 6.2或者基于该版本得发行版下安装需要的 RPM 包"。如果您还没有安装,您可能需要安装需要的 RPMs。

#### 例 2.3. 在 RedHat Linux 6.2或者基于该版本得发行版下安装需要的 RPM 包

cd /mnt/cdrom/RedHat/RPMS rpm -ivh glib-1.2.6-3.i386.rpm rpm -ivh glib-devel-1.2.6-3.i386.rpm rpm -ivh gtk+-1.2.6-7.i386.rpm rpm -ivh gtk+-devel-1.2.6-7.i386.rpm rpm -ivh libpcap-0.4-19.i386.rpm

#### 注意

如果您使用 RedHat 6.2之后的版本,需要的 RMPs 包可能已经变化。您需要使用正确的 RMPs 包。 在 Debian 下您可以使用 apt-ge 命令。apt-get 将会为您完成所有的操作。参见<u>例 2.4 "在 Deban 下安装 Deb"</u> **例 2.4. 在 Deban 下安装 Deb** apt-get install wireshark-dev

### 2.4. 在 UNIX 下编译 Wireshark

如果在 Unix 操作系统下可以用如下步骤编译 Wireshark 源代码: 如果使用 Linux 则解压 gzip'd tar 文件,如果您使用 UNIX,则解压 GUN tar 文件。对于 Linux 命令如下: tar zxvf wireshark-0.99.5-tar.gz 对于 UNIX 版本, 命令如下 gzip -d wireshark-0.99.5-tar.gz tar xvf wireshark-0.99.5-tar 注意 使用管道命令行 gzip -dc Wireshark-0.99.5-tar.gz|tar xvf 同样可以<sup>12</sup> 注意 如果您在 Windows 下下载了 Wireshark,你会发现文件名中的那些点变成了下划线。 将当前目录设置成源文件的目录。 配置您的源文件以编译成适合您的 Unix 的版本。命令如下: ./configure 如果找个步骤提示错误, 您需要修正错误, 然后重新 configure.解决编译错误可以参考<u>第 2.6 节 "解决 UNIX 下安装过程中</u> <u>的问题</u>" 使用 make 命令将源文件编译成二进制包, 例如: make 安装您编译好的二进制包到最终目标,使用如下命令: make install 一旦您使用 make install 安装了 Wireshark,您就可以通过输入 Wireshark 命令来运行它了。

[2] 译者注:看到别人翻译 Pipelin 之类的,似乎就是叫管道,不知道是否准确

### 2.5. 在 UNIX 下安装二进制包

一般来说,在您的 UNIX 下安装二进制发行包使用的方式根据您的 UNIX 的版本类型而各有不同。例如 AIX 下,您可以使用 smit 安装,Tru64 UNIX 您可以使用 setld 命令。

### 2.5.1. 在 Linux 或类似环境下安装 RPM 包

使用如下命令安装 Wireshark RPM 包 rpm -ivh wireshark-0.99.5.i386.rpm 如果因为缺少 Wireshark 依赖的软件而导致安装错误,请先安装依赖的软件,然后再尝试安装。REDHAT 下依赖的软件请 参考例 2.3 "在 RedHat Linux 6.2或者基于该版本得发行版下安装需要的 RPM 包"

### 2.5.2. 在 Debian 环境下安装 Deb 包

使用下列命令在 Debian 下安装 Wireshark

apt-get install Wireshark apt-get 会为您完成所有的相关操作

### 2.5.3. 在 Gentoo Linux 环境下安装 Portage

使用如下命令在 Gentoo Linux 下安装 wireshark 以及所有的需要的附加文件 USE="adns gtk ipv6 portaudio snmp ssl kerberos threads selinux" emerge wireshark

### 2.5.4. 在 FreeBSD 环境下安装包

使用如下命令在 FreeBSD 下安装 Wireshark pkg\_add -r wireshark pkg\_add 会为您完成所有的相关操作

### 2.6. 解决 UNIX 下安装过程中的问题 11

安装过程中可能会遇到一些错误信息。这里给出一些错误的解决办法:

如果 configure 那一步发生错误。你需要找出错误的原因,您可以检查日志文件 config.log(在源文件目录下),看看都发生了哪些错误。有价值的信息通常在最后几行。

一般原因是因为您缺少 GTK+环境,或者您的 GTK+版本过低。configure 错误的另一个原因是因为因为缺少 libpcap(这就是前面提到的捕捉包的工具)。

另外一个常见问题是很多用户抱怨最后编译、链接过程需要等待太长时间。这通常是因为使用老式的 sed 命令(比如 solaris 下传输)。自从 libtool 脚本使用 sed 命令建立最终链接命令,常常会导致不可知的错误。您可以通过下载最新版本的 sed 解 决该问题 <u>http://directory.fsf.org/GNU/sed.html</u>.

如果您无法检测出错误原因。发送邮件到 <u>wireshark-dev</u>说明您的问题。当然,邮件里要附上 config.log 以及其他您认为对 解决问题有帮助的东西,例如 make 过程的追踪。

[19] 译者注:本人不熟悉 UNIX/LINUX,这一段翻译的有点云里雾里,可能大家通过这部分想安装 Wireshark 会适得其反, 那就对不住了。下面个人说一下 UNIX/LINUX 下安装方法。 UNIX/LINUX 下安装时,有两种安装方式,1是下载源码包自 己编译,这种方式的好处是因为下载源码包是单一的,可以自行加以修改,编译就是适合自己平台的了。2、是利用已经 做好的发行包直接安装,这种方法的好处是只要下载到跟自己平台对应的就可以,但缺点也在这里,不是每个平台都能找 到合适的。不管是编译安装,还是使用发行包安装,都需要有一些有些基本基本支持。比如 Linux 下的 GTK+支持,捕捉 包时需要用的 libpcap.这一点可以参考<u>第 2.3 节 "在 UNIX 下安装之前"</u>。编译的一般步骤是解压,编译,安装(**tar zxvf** Wireshark-0.99.5-tar.gz;make;make install).直接安装则是根据各自平台安装的特点。

### 2.7. 在 Windows 下编译源

在 Windows 平台下,我们建议最好是使用二进制包直接安装,除非您是从事 Wireshark 开发的。如果想了解关于 Windows 下编译安装 Wireshark,请查看我们的开发 WIKI 网站 <u>http://wiki.wireshark.org/Development</u>来了解最新的开发方面的文档。

### 2.8. 在 Windows 下安装 Wireshark

本节将探讨在 Windows 下安装 Wireshark 二进制包。

### 2.8.1. 安装 Wireshark

您获得的 Wireshark 二进制安装包可能名称类似 Wireshark-setup-x.y.z.exe. Wireshark 安装包包含 WinPcap,所以您不需要单独 下载安装它。

您只需要在 <u>http://www.wireshark.org/download.html#releases</u>下载 Wireshark 安装包并执行它即可。除了普通的安装之外,还有几个组件供挑选安装。

**提示:尽量保持默认设置** 如果您不了解设置的作用的话。

### 选择组件[11]

Wireshark(包括 GTK1和 GTK2接口无法同时安装): 如果您使用 GTK2的 GUI 界面遇到问题可以尝试 GTK1,在 Windows 下256色(8bit)显示模式无法运行 GTK2.但是某些高级分析统计功能在 GTK1下可能无法实现。 Wireshark GTK1-Wireshark 是一个 GUI 网络分析工具
Wireshark GTK2-Wireshark 是一个 GUI 网络分析工具(建议使用 GTK2 GUI 模组工具)
GTK-Wimp-GTKWimp 是诗歌 GTK2窗口模拟(看起来感觉像原生 windows32程序,推荐使用)
TSshark-TShark 是一个命令行的网络分析工具
插件/扩展(Wireshark,TShark 分析引擎):
Dissector Plugins-分析插件:带有扩展分析的插件
Tree Statistics Plugins-树状统计插件:统计工具扩展
Mate - Meta Analysis and Tracing Engine (experimental):可配置的显示过滤引擎,参考 http://wiki.wireshark.org/Mate.

SNMP MIBs: SNMP, MIBS 的详细分析。 Tools/工具(处理捕捉文件的附加命令行工具

User's Guide-用户手册-本地安装的用户手册。如果不安装用户手册,帮助菜单的大部分按钮的结果可能就是访问 internet. • Editcap - Editcap is a program that reads a capture file and writes some or all of the packets into another capture file. /Editcap 是一个读取捕捉文件的程序,还可以将一个捕捉文件力的部分或所有信息写入另一个捕捉文件。(文件合并 or 插入?)

**Text2Pcap** - Text2pcap is a program that reads in an ASCII hex dump and writes the data into a libpcap-style capture file./Tex2pcap 是一个读取 ASCII hex,写入数据到 libpcap 个文件的程序。

**Mergecap** - Mergecap is a program that combines multiple saved capture files into a single output file. / Mergecap 是一个可以将 多个播捉文件合并为一个的程序。

Capinfos - Capinfos is a program that provides information on capture files. /Capinfos 是一个显示捕捉文件信息的程序。

### "Additional Tasks"页

Start Menu Shortcuts-开始菜单快捷方式-增加一些快捷方式到开始菜单 Desktop Icon-桌面图标-增加 Wireshark 图标到桌面 Quick Launch Icon-快速启动图标-增加一个 Wireshark 图标到快速启动工具栏 Associate file extensions to Wireshark-Wireshark 文件关联-将捕捉包默认打开方式关联到 Wireshark

#### Install WinPcap?"页

Wireshark 安装包里包含了最新版的 WinPcap 安装包。 如果您没有安装 WinPcap 。您将无法捕捉网络流量。但是您还是可以打开以保存的捕捉包文件。 **Currently installed WinPcap version**-当前安装的 WinPcap 版本 **Install WinPcap x.x** -如果当前安装的版本低于 Wireshark 自带的,该选项将会是默认值。 **Start WinPcap service "NPF" at startup**-将 WinPcap 的服务 NPF 在启动时运行-这样其它非管理员用户就同样可以捕捉包 了。 更多关于 WinPcap 的信息:

更多天于 WmPcap 的信息: Wireshark 相关 <u>http://wiki.wireshark.org/WinPcap</u> WinPcap 官方网站: <u>http://www.winpcap.org</u>

### 安装命令选项

您可以直接在命令行运行安装包,不加任何参数,这样会显示常用的参数以供交互安装。 在个别应用中,可以选择一些参数定制安装:
/NCRC 禁止 CRC 校检
/S 静默模式安装或卸载 Wireshark.注意:静默模式安装时不会安装 WinPcap!
/desktopicon 安装桌面图标,/desktopicon=yes 表示安装图标,反之则不是,适合静默模式。
/quick launchicon 将图标安装到快速启动工具栏,=yes-安装到工具栏,=no-不安装,不填按默认设置。
/D 设置默认安装目录(\$INSTDIR),首选安装目录和安装目录注册表键值,该选项必须设置到最后。即使路径包含空格
/9 2.5.

wireshark-setup-0.99.5.exe /NCRC /S /desktopicon=yes /quicklaunchicon=no /D=C:\Program Files\Foo

### 2.8.2. 手动安装 WinPcap

### 注意

事先声明,Wireshark 安装时会谨慎对待 WinPcap 的安装,所以您通常不必担心 WinPcap。 下面的 WinPcap 仅适合您需要尝试未包括在 Wireshark 内的不同版本 WinPcap。例如一个新版本的 WinPcap 发布了,您需 要安装它。 单独的 WinPcap 版本(包括 alpha or beta 版)可以在下面地址下载到 WinPcap 官方网站: <u>http://www.winpcap.org</u> Wiretapped.net 镜像站点: <u>http://www.mirrors.wiretapped.net/security/packet-capture/winpcap</u> 在下载页面您将会发现 WinPcap 的安装包名称通常类似于"auto-installer"。它们可以在 NT4.0/2000/XP/vista 下安装。

### 2.8.3. 更新 Wireshark

有时候您可能想将您的 WinPcap 更新到最新版本,如果您订阅了 Wireshark 通知邮件,您将会获得 Wireshark 新版本发布的 通知,见<u>第 1.6.4 节 "邮件列表"</u>

新版诞生通常需要8-12周。更新 Wireshark 就是安装一下新版本。下载并安装它就可以。更新通常不需要重新启动,也不会更改过去的默认设置

### 2.8.4. 更新 WinPcap

WinPcap 的更新不是十分频繁,通常一年左右。新版本出现的时候您会收到 WinPcap 的通知。更新 WinPcap 后需要重新启动。

警告

在安装新版 WinPcap 之前,如果您已经安装了旧版 WinPcap,您必须先卸载它。最近版本的 WinPcap 安装时会自己卸载旧版。

#### 2.8.5. 卸载 Wireshark

你可以用常见方式卸载 Wireshark,使用添加/删除程序,选择"Wireshark"选项开始卸载即可。 Wireshark 卸载过程中会提供一些选项供您选择卸载哪些部分,默认是卸载核心组件,但保留个人设置和 WinPcap. WinPcap 默认不会被卸载,因为其他类似 Wireshark 的程序有可能同样适用 WinPcap

### 2.8.6. 卸载 WinPcap

你可以单独卸载 WinPcap,在添加/删除程序选择"WinPcap"卸载它。

#### 注意

卸载 WinPcap 之后您将不能使用 Wireshark 捕捉包。 在卸载完成之后最好重新启动计算机。

Ш 涉及到过多的名次,软件又没有中文版,这里及以后尽量不翻译名称

### 第3章用户界面

#### 目录

3.1. 须知 3.2. 启动 Wireshark <u>3.3. 主窗口</u> 3.3.1. 主窗口概述 <u>3.4. 主菜单</u> <u>3.5. "File" 菜单</u> <u>3.6. "Edit"菜单</u> <u>3.7. "View"菜单</u> <u>3.8. "Go" 菜单</u> <u>3.9. "Capture"菜单</u> <u>3.10. "Analyze" 菜单</u> 3.11. "Statistics"菜单 <u>3.12. "Help" 菜单</u> <u>3.13. "Main"工具栏</u> <u>3.14. "Filter"工具栏</u> <u>3.15. "Pcaket List"面板</u> <u>3.16. "Packet Details"面板</u> <u>3.17. "Packet Byte"面板</u> 3.18. 状态栏

### 3.1. 须知

```
现在您已经安装好了Wireshark,几乎可以马上捕捉您的一个包。紧接着的这一节我们将会介绍:
Wireshark的用户界面如何使用
如何捕捉包
如何查看包
如何过滤包
......以及其他的一些工作。
```

### 3.2. 启动 Wireshark

你可以使用 Shell 命令行或者资源管理器启动 Wireshark.

提示

开始 Wireshark 时您可以指定适当的参数。参见<u>第 9.2 节"从命令行启动 Wireshark"</u> 注意 在后面的章节中,将会出现大量的截图,因为 Wireshark 运行在多个平台,并且支持多 个 GUI Toolkit(GTK1.x/2x),您的屏幕上显示的界面可能与截图不尽吻合。但在功能上不会

有实质性区别。尽管有这些区别,也不会导致理解上的困难。

### 3.3. 主窗口

先来看看图 <u>3.1"主窗口界面"</u>,大多数打开捕捉包以后的界面都是这样子(如何捕捉/打开包文件随后提到)。

图 3	.1. 主	窗口	界面
-----	-------	----	----

🖊 test. pcap - Wireshark					
Eile Edit ⊻iew Go Capture	Analyze Statistics	Help			
	🖻 🔀 🗙	♥	🔿 🗢 🧎		
Eilter:				ssion 💩 ⊆lear 🖋 Apply	
No Time Source	э	Destination	Protocol Info	0	^
1 0.000000 192.:	168.0.2	Broadcast	ARP Who	o has 192.168.0.2? Gratuitous /	
3 0 299214 192	168 0 2	192.168.0.1	TCMP Des	stination unreachable (Port unre	
4 1.025659 192.3	168.0.2	224.0.0.22	IGMP V3	Membership Report	
5 1.044366 192.3	168.0.2	192.168.0.1	DNS Sta	andard query SRV _ldaptcp.nbgr	
6 1.048652 192.:	168.0.2	239.255.255.250	UDP Sou	urce port: 3193 Destination por	
	168.0.2	192.168.0.1	DNS Sta	andard query SOA nb10061d.ww004. unce popt: 1900 Destination po	
9 1.082038 192.	168.0.2	192.168.0.255	NBNS Rec	distration NB NB10061D∠00>	
10 1.111945 192.3	168.0.2	192.168.0.1	DNS Sta	andard query A proxyconf.ww004.s	
11 1.226156 192.3	168.0.2	192.168.0.1	TCP 319	96 > http [SYN] Seq=O Len=O MSS	
12 1.227282 192.3	168.0.1	192.168.0.2	TCP htt	tp > 3196 [SYN, ACK] Seq=0 Ack=:	~
<					ļ
⊕ Frame 11 (62 bytes on	wire, 62 bytes ca	ptured)			~
⊞ Ethernet II, Src: 192.	168.0.2 (00:0b:50	1:20:cd:02), Dst: Netg	ear_2d:75:9	9a (00:09:5b:2d:75:9a)	
Internet Protocol, Sra	: 192.168.0.2 (19	2.168.0.2), Dst: 192.	168.0.1 (19	92.168.0.1)	
🖃 Transmission Control F	Protocol, Src Port	: 3196 (3196), Dst Po	rt: http (8	30), Seq: 0, Len: 0	
Source port: 3196 (3	3196)				≡
Destination port: h	ttp (80)				
Sequence number: O	(relative seque	ence number)			
Header length: 28 by	ytes	-			
	- 				
Window size: 64240					~
0000 00 09 5h 2d 75 9a 0	0 0h 5d 20 cd 02	2 08 00 45 00 F-u	1 5		_
	30 06 61 2c c0 at	3 00 02 c0 a8 .0.H@.	a		
0020 00 01 0c 7c 00 50 3	3c 36 95 f8 00 00	00 00 70 02 .P	<6p.		
0030 ta to 27 eo 00 00 0	02 04 05 64 01 01	. 04 02'	•••••••		
File: "D:/test.pcap" 14 KB 00:00:02				P: 120 D: 120 M: 0	.:

和大多数图形界面程序一样, Wireshark 主窗口由如下部分组成: 菜单(见<u>第 3.4 节"主菜单</u>")用于开始操作。 主工具栏(见<u>第 3.13 节 ""Main"工具栏"</u>)提供快速访问菜单中经常用到的项目的功能。

Fiter toolbar/过滤工具栏(见<u>第 3.14 节 ""Filter"工具栏"</u>)提供处理当前显示过滤得方法。(见6.3:"浏览时进行过滤") Packet List 面板(见<u>第 3.15 节 ""Pcaket List"面板"</u>)显示打开文件的每个包的摘要。点击面板中的单独条目,包的其他情 况将会显示在另外两个面板中。

Packet detail 面板(见<u>第 3.16 节 ""Packet Details"面板"</u>)显示您在 Packet list 面板中选择的包德更多详情。 Packet bytes 面板(见<u>第 3.17 节 ""Packet Byte"面板"</u>)显示您在 Packet list 面板选择的包的数据,以及在 Packet details 面 板高亮显示的字段。

状态栏(见<u>第 3.18 节"状态栏"</u>)显示当前程序状态以及捕捉数据的更多详情。

#### 注意

主界面的三个面版以及各组成部分可以自定义组织方式。见<u>第 9.5 节"首选项"</u>

### 3.3.1. 主窗口概述

Packet list 和 Detail 面版控制可以通过快捷键进行。<u>表 3.1 "导航快捷键"</u>显示了相关的快捷键列表。<u>表 3.5 ""GO"菜单项"</u> 有关于快捷键的更多介绍

#### 表 3.1. 导航快捷键 快捷键

描述

Tab,Shift+T ab	在两个项目间移动,例如从一个包列表移动到下一个
Down	移动到下一个包或者下一个详情
Up	移动到上一个包或者上一个详情
Ctrl-Down, F8	移动到下一个包,即使焦点不在 Packet list 面版
Ctrl-UP,F7	移动到前一个报,即使焦点不在 Packet list 面版
Left	在 Pactect Detail 面版,关闭被选择的详情树状分支。如果以关闭,则返回到父 分支。
Right	在 Packet Detail 面版,打开被选择的树状分支.
Backspace	Packet Detail 面版,返回到被选择的节点的父节点
Return,Ente r	Packet Detail 面版,固定被选择树项目。

另外,在主窗口键入任何字符都会填充到 filter 里面。

### 3.4. 主菜单

Wireshark 主菜单位于 Wireshark 窗口的最上方。图 3.2"主菜单"提供了菜单的基本界面。

图 3.2. 主菜单

Help

<u>File Edit View Go Capture Analyze Statistics Help</u>

主菜单包括以下几个项目: File 包括打开、合并捕捉文件, save/保存, Print/打印, Export/导出捕捉文件的全部或部分。以及退出 Wireshark 项. 见<u>第 3.5 节</u> ""File"菜单" Edit 包括如下项目:查找包,时间参考,标记一个多个包,设置预设参数。(剪切,拷贝,粘贴不能立即执行。)见第 3.6 节 ""Edit" 菜单" View 控制捕捉数据的显示方式,包括颜色,字体缩放,将包显示在分离的窗口,展开或收缩详情面版的地树状节点,.....见第 3.7 <u>节""View"菜单"</u> GO 包含到指定包的功能。见<u>第 3.8 节 ""Go"菜单"</u> Capture 允许您开始或停止捕捉、编辑过滤器。见<u>第 3.9 节 ""Capture"菜单"</u> Analvze 包含处理显示过滤,允许或禁止分析协议,配置用户指定解码和追踪 TCP 流等功能。见<u>第 3.10 节 ""Analyze"菜单"</u> Statistics 包括的菜单项用户显示多个统计窗口,包括关于捕捉包的摘要,协议层次统计等等。见<u>第 3.11 节 ""Statistics"菜单"</u>

```
包含一些辅助用户的参考内容。如访问一些基本的帮助文件,支持的协议列表,用户手册。在线访问一些网站,"关于"等等。见<u>第 3.12 节 ""Help"菜单"</u>
```

本章链接介绍菜单的一般情况,更详细的介绍会出现在后续章节。

#### 提示

你可以直接点击访问菜单项,也可以使用热键,热键显示在菜单文字描述部分。例如:您可以使用 CTR+K 打开捕捉对话框。

### 3.5. "File"菜单

WireSharkFile 菜单包含的项目如表<u>表 3.2 "File 菜单介绍"</u>所示 **图 3.3. File 菜单** 

🗹 test. pcap - Wireshark								
<u>File Edit V</u> iew	<u>Go</u> <u>C</u> apture <u>4</u>	Analyze Statistics	Help					
Den Open <u>R</u> ecent	Ctrl+O	🖻 🖪 🗙	°, 📇 🖸	\$ \$	● 否	₽ [■	<b>.</b> 0, 6	6
Merge ≭ ⊆lose	Ctrl+W			•	🕂 Expressio	n ‱⊆lear	🖋 Apply	
Save	Ctrl+S Shift+Ctrl+S	.0.2	Destination	Pro	tocol Info > Who h	as 192.168.0.	27 Gratuitou	
File Set	•	.0.1	192.168.0.2 192.168.0.1		NS Name AP Desti	query NBSTAT nation unread	*<00><00><00> hable (Port u	
Export	 Ctrl+P	as "Plain <u>T</u> ext" file as " <u>P</u> ostScript" file	 			mbership керо ard query SRV e port: 3193 ard query SOA	rt / _ldaptcp.r Destination / nh10061d.ww0	por por
Quit	Ctrl+Q 945 192.168	as XML - "PSML" (r	Separated values pack backet summary) file	ket summary) ri	lle	e port: 1900 tration NB NE ard query A p	Destination 10061D<00> proxyconf.ww00	por 14.:
11 1.226 12 1.227	156 192.168 282 192.168	Selected Packet B	ytes		Ctrl+H	> http [SYN] > 3196 [SYN,	Seq=0 Len=0 M ACK] Seq=0 Ac	.k=: ₩
<								>
<ul> <li>Frame 11 (62 bytes on wire, 62 bytes captured)</li> <li>Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a)</li> <li>Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)</li> <li>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: 38 bytes</li> </ul>								
	0002 (SYN)	:5						
Window si	ze: 64240							*
0000 00 09 5b 0010 00 30 18 0020 00 01 0c 0030 fa f0 27	2d 75 9a 00 48 40 00 80 7c 00 50 3c e0 00 00 02	0b 5d 20 cd ( 06 61 2c c0 36 95 f8 00 ( 04 05 b4 01 (	D2 08 00 45 00 a8 00 02 c0 a8 D0 00 00 70 02 D1 04 02	[-u .0.H@  .P<6	]E. a,p. p.			
File: "D:/test.pcap"	File: "D:/test.pcap" 14 KB 00:00:02 P: 120 M: 0							

### 表 3.2. File 菜单介绍

菜单项	快捷键	描述
		显示打开文件对话框,让您載入捕捉文件用
Open	Ctr+O	以浏览。见 <u>第 5.2.1 节 "打开捕捉文件对话</u>
		框"
One Description		弹出一个子菜单显示最近打开过的文件供
Open Recent		选择。
		显示合并捕捉文件的对话框。让您选择一个
Merg		文件和当前打开的文件合并。见 <u>第 5.4 节</u>
		"合并捕捉文件"
		关闭当前捕捉文件,如果您未保存,系统将
Close	Ctrl+W	提示您是否保存(如果您预设了禁止提示保
		存,将不会提示)
Sama	Cr1+ S	保存当前捕捉文件,如果您没有设置默认的
Save	Cri+S	保存文件名,Wireshark 出现提示您保存文

		件的对话框。详情 <u>第 5.3.1 节 ""save</u>
		Capture File As/保存文件为"对话框"
		注意
		如果您已经保
		存文件,该选
		项会是灰色不
		可选的。
		注意
		你不能保存动
		<b>杰</b> 捕捉的文
		心,而,从 前,久
		F. 心见须知 市场切时后才
		米油远以户7 能进行保存
		让您将当前文件保存为另外一个文件面,将
Save As	Shift+Ctrl+S	会出现一个另存为的对话框(参见 <u>第 5.3.1</u>
	Shirt+Ctr+5	<u>节""save Capture File As/保存文件为"对话</u>
		<u>稚"</u> ) 金许你目示立 <u>供</u> 集会的 <u>利</u> 害,救会 <u>确</u> 山一个
		九日志亚小文什朱百的列衣。村云坪山 1
File Set>List Files		对 站框並小 □ 打 丌 又 针 的 列 衣, 参 见 <u>另 □.5</u> 节 " 文 件 集 合"
		如果当前載入文件是文件集合的一部分,将
		会跳转到下一个文件。如果不是,将会跳转
File Set>Next File		到最后一个文件。这个文件选项将会是灰
		A A A A A A A A A A A A A A A A A A A
		亡。 加里当前立供具立供集合 的一部分 收合
		如禾当前又什定又什朵百 的 即方, 村云 调到它诉左位罢的前一个文件 加里不具则
File set>Previous Files		则到口川在世里的的 一又下。如木不足则 则 到立供集合的第一合文供 同时亦武五
		成到又什朱言的弟 <sup>一</sup> 个又针,问时变成灰 在
		巴。
		这个来早几许您将捕捉又件中所有的现有
Export> as "Plain Text" File		前方的包寻出为 plain ASCII text 格式。 匕将
		会弹出一个 Wireshark 导出对话框,见 <u>弗</u>
		5.6.1 节 ""Export as Plain Text File"对话框"
		将捕捉又件的全部或部分导出为 PostScrit
Export >as "PostScript" Files		文件。将会出现导出文件对话框。参见第
		5.6.2 节 "''Export as PostScript File'' 对估
		<u>框"</u>
Export > as "CVS" (Comma		导出文件全部或部分摘要为.cvs格式(可用
Senarated Values Packet		在电子表格中)。将会弹出导出对话框,见 <u>第</u>
Summary)File		<u>5.6.3 节 ""Export as CSV (Comma</u>
~		<u>Separated Values) File"对话框"</u> 。
		导出文件的全部或部分为 PSML 格式(包摘
Fyport > as "PSML" File		要标记语言)XML 文件。将会弹出导出文
Export = as I SML FIE		件对话框。见 <u>第 5.6.4 节 ""Export as PSML</u>
		<u>File"对话框"</u>
		导出文件的全部或部分为 PDML(包摘要标
Fundat an HERRAL H. F.		记语言)格式的 XML 文件。将会弹出一个导
Export as "PDML" File		出文件对话框,见 <u>第 5.6.5 节 ""Export as</u>
		PDML File"对话框"
		导出当前在 Packet byte 面版选择的字节为
Export > Selected Packet		二进制文件。将会弹出一个导出对话框。见
Bytes		<u>第 5.6.6 节 ""Export selected packet bytes"</u>
-		对话框"
	_	打印捕捉包的全部或部分,将会弹出打印对
Print	Ctr+P	话框。见第 5.7 节 "打印包"
		退出 Wireshark,如果未保存文件, Wireshark
Quit	Ctrl+Q	会提示是否保存。

## 3.6. "Edit"菜单

Wireshark 的"Edit"菜单包含的项目见表 3.3 "Edit 菜单项"

### 图 3.4. "Edit"菜单

🗖 te	st.cap - Wireshark				
Eile	Edit View Go Capture And	alyze <u>S</u> tatistics <u>H</u>	elp		
	Сору	• @			Ð, Q,
Eilter	Eind Packet Find Next Find Previous	Ctrl+F Ctrl+N Ctrl+B	▼ Expre:	ssion Clear Apply	
140. 4	<u>M</u> ark Packet (toggle) Find Next Mark Find Previous Mark Mark <u>A</u> ll Packets	Ctrl+M 02 Shift+Ctrl+N Shift+Ctrl+B	Broadcast 192.168.0.2 192.168.0.1 224.0.0.22 192.168.0.1	ARP Gratuitous A NBNS Name query M ICMP Destination IGMP V3 Membersh DNS Standard que	ARP for E NBSTAT Unreac ip Repo erv SRV
	Unmark All Packets Set Time Reference (toggle) Find Next Reference Find Previous Reference	Ctrl+T	239.255.255.250 192.168.0.1 192.168.0.2 192.168.0.255 192.168.0.1	SSDP M-SEARCH * 1 DNS Standard que SSDP HTTP/1.1 200 NBNS Registration DNS Standard que	TTP/1. Pry SOA O OK NB NB Pry A p
	★ Preferences 15 1.227523 192.3 14 1.227451 192.3 15 1.229309 192.1	Shift+Ctrl+P	192.168.0.1 192.168.0.2 192.168.0.1 192.168.0.1 192.168.0.1	TCP 3196 > http TCP http > 3196 TCP 3196 > http HTTP SUBSCRIBE /0 TCP http > 3196	LSYNJ [SYN, [ACK] Jpnp/se
<	16         1.232421         192.1           17         1.248355         192.1	168.0.1 168.0.1	192.168.0.2 192.168.0.2 192.168.0.2	TCP [TCP window TCP 1025 > 5000	Update [SYN]
	Hardware type: Ethern Protocol type: IP (0:	net (0x0001) x0800)	, , , , , ,		
<	Haruware Size. o				) <b>&gt;</b>
00000 0010 0020	) <del>ff ff ff ff ff ff ff ff 0</del> 0 <u>08 00</u> 06 04 00 01 0 00 00 00 00 00 00 00 c	00 0b 5d 20 0 00 0b 5d 20 0 0 a8 00 02	d 02 08 06 00 01 d 02 c0 a8 00 02 		
Protoc	ol type (arp.proto.type), 2 bytes		P: 120 D: 120 M: 0		

### 表 3.3. Edit 菜单项 菜单项 快捷键

Copy>As Filter Shift+C trl+C		使用详情面版选择的数据作为显示过滤。显示过滤将会拷贝到剪贴板。				
Find Packet	Ctr+F	打开一个对话框用来通过限制来查找包,见???				
Find Next Ctrl+N		在使用 Find packet 以后,使用该菜单会查找匹配规则的下一个 包				
<b>Find Previous</b>	Ctr+B	查找匹配规则的前一个包。				
Mark Packet(toggle)		标记当前选择的包。见 <u>第 6.9 节 "标记包"</u>				
Find Next Mark	Shift+C trl+N	查找下一个被标记的包				
Find Previous	Ctrl+Sh	杏状前—-个被标记的句				
Mark	ift+B					
Mark ALL Packets		标记所有包				
Unmark All		取消低力扫描				
Packet		<b>状</b> 相用有你吃				
Set Time	Ctrl+T	以当前句时间作为会考 圓笋 6101 节 "句会考时间"				
Reference(toggle)	Cuiti	以コ曲已町町1F刀穸写,尤 <u>另 0.10.1 p 巴穸写时间</u>				

Find Next		壮刻下
Reference		我到下一个时间参考也
Find Previous Refrence		找到前一个时间参考包
Preferences	Shift+C trl+P	打开首选项对话框,个性化设置 Wireshark 的各项参数,设置后的参数将会在每次打开时发挥作用。详见 <u>第 9.5 节"首选项"</u>

## 3.7. "View"菜单

<u>表 3.4 ""View"菜单项"</u>显示了 Wireshar View 菜单的选项

图 3.5. "View"菜单

🗹 test. pcap - Wireshark						
Eile Edit View Go Capture Analyze Statistics Help						
✓ Main Toolbar         ✓ Eilter Toolbar         ✓ Statusbar						
Filter:     Packet List       No     Packet Details       1 (     Packet Bytes	∑⊆lear ♥ Apply					
2 (       Ime Display Format       Date and Time of Day: 1970-01-01 01:02:03.123         3 (       Name Resolution       Time of Day: 01:02:03.123456         4 :       Name Resolution       Seconds Since Beginning of Capture: 123.123456         5 :       ✓ Colorize Packet List       Seconds Since Previous Packet: 1.123456         7 :       ✓ Auto Scroll in Live Capture       Seconds Since Previous Packet: 1.123456	<pre>HBSTAT * &lt;00&gt; &lt;00&gt; &lt;00&gt; &lt;00 unreachable (Port unre ip Report s ery SRV _ldaptcp.nbgr s 3193 Destination por ery SOA nb10061d.ww004.</pre>					
8       Q Zoom In       Ctrl++         9       200m Qut       Ctrl+-         10       Q Zoom Qut       Ctrl+-         11       Q Normal Size       Ctrl+=         12       Resize All Columns       Centiseconds: 0.1         Expand Subtrees       Milliseconds: 0.123	: 1900 Destination por 1 NB NB10061D<00> ery A proxyconf.ww004.: [SYN] Seq=0 Len=0 MSS [SYN, ACK] Seq=0 Ack=: >					
Frame Expand All Nanoseconds: 0.123456     Expand All Nanoseconds: 0.123456789     Collapse <u>A</u> ll     Intern     Transm ➡ Coloring Rules     Intern	5b:2d:75:9a) 68.0.1) Seg: 0. Len: 0					
Sour Dest Show Packet in New <u>W</u> indow Sequ <u>Reload</u> <u>Ctrl+R</u> uence number) Header length: 28 bytes						
Flags: 0×0002 (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<6p. 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 .:					

```
表 3.4. "View"菜单项
```

菜单项	快捷键	描述
Main Taalban		显示隐藏 Main toolbar(主工具栏),见 <u>第</u>
Main 100ibar		<u>3.13 节""Main"工具栏"</u>
Elter Teelber		显示或隐藏 Filter Toolbar(过滤工具栏)见
Filter Iooidar		<u>第 3.14 节 ""Filter"工具栏"</u>
Statushar		显示或隐藏状态栏,见 <u>第 3.18 节 "状态</u>
Statusbar		<u>栏"</u>
De als at I int		显示或隐藏 Packet List pane(包列表面板),
racket List		见 <u>第 3.15 节 ""Pcaket List"面板"</u>
Paals at Dataila		显示或隐藏 Packet details pane(包详情面
racket Details		板).见 <u>第 3.16 节 ""Packet Details"面板"</u>
Pack et Bytes		显示或隐藏 packet Bytes pane(包字节面

Time Display Fromat>Date and Time of Day: 1970-01-01 01:02:03.123456

Time Display Format>Time of Day: 01:02:03.123456

Time Display Format > Seconds Since Beginning of Capture: 123.123456 Time Display Format > Seconds

Since Previous Captured Packet: 1.123456

Time Display Format > Seconds Since Previous Displayed Packet: 1.123456

Time Display Format > -----

Time Display Format > Automatic (File Format Precision)

Time Display Format > Seconds: 0

TimeDisplayFormat>...seconds: 0....

Name Resolution > Resolve Name

Name Resolution > Enable for

板),见<u>第 3.17 节 ""Packet Byte"面板"</u> 选择这里告诉 Wireshark 将时间戳设置为 绝对日期-时间格式(年月日,时分秒),见 <u>第 6.10 节 "时间显示格式及参考时间"</u>

### 注意

这里的字段 "Time of Day", "Date and Time of Day", "Second s Since Beginning of Capture", "Sec onds Since Previous Captured Packet"和 "Seconds Since Previous Displayed Packet"几个 选项是互斥 的,换句话 说,一次同时 有一个被选 中。

将时间设置为绝对时间-日期格式(时分秒 格式),见<u>第 6.10 节"时间显示格式及参</u> <u>考时间"</u>

将时间戳设置为秒格式,从捕捉开始计时,见<u>第 6.10 节"时间显示格式及参考时间"</u>

将时间戳设置为秒格式,从上次捕捉开始 计时,见<u>第 6.10 节"时间显示格式及参考</u> 时间"

将时间戳设置为秒格式,从上次显示的包 开始计时,见<u>第 6.10 节"时间显示格式及</u> 参考时间"

根据指定的精度选择数据包中时间戳的显示方式,见<u>第 6.10 节"时间显示格式及参考时间"</u>

#### 注意

"Automatic"," Seconds"和 "...seconds"是 互斥的

设置精度为1秒,见<u>第 6.10 节"时间显示 格式及参考时间"</u> 设置精度为1秒,0.1秒,0.01秒,百万分之 一秒等等。见<u>第 6.10 节"时间显示格式</u> <u>及参考时间"</u> 仅对当前选定包进行解析<u>第 7.6 节"名称</u> <u>解析"</u> 是否解析 Mac 地址

MAC Layer		
Name Resolution > Enable for		是否解析网络层地址(ip 地址),见 <u>第 7.6 节</u>
Network Layer		"名称解析"
Name Resolution > Enable for		是否解析传输层地址 <u>第 7.6 节 "名称解</u>
Transport Layer		<u>析"</u>
		是否以彩色显示包
		注意
		以彩色方式
		显示包会降
Colorize Packet List		低捕捉再如
		包文件的速
		度
		控制在实时捕捉时是否自动滚屋, 加里诜
		择了该项,在有新数据进入时,面板会项
Auto Scrooll in Live Conture		上滚动。你始终能看到最后的数据。反之
Auto Scroon in Live Capture		工农场。芯茄、配有均取用的废店。 (人名)
		态元14日对两开50日的数据,两中心150 密屋
Zoom In	Ctal	依/开 
Zoom In Zoom Out	Ctrl++	增入于(P) 统小艺体
Zoom Out	Ctrl+-	细小于冲 恢复工学士小
Normai Size	Ctri+=	恢复止市入小
		恢复所有列克 <b>计本</b>
Resiz All Columnus		际非数据包
		非吊人、一枚
		会立刻更改
Even and Suckture of		展开之八主
Expend Subtrees		成开了刀又 手工所方公士 这类顶入屋工你选择的句
Expand All		有开所有方义, 该远坝会展开忽远拜的已 的近去公式
		的周有万义。
Conapse An		收缩所有它的所有万文
		打开一个对话框,让您可以通过过滤衣达
Coloring Rulues		米用小问的颜色亚小包。这项功能对定位
		特定关型的包非常有用。见 <u>弗 9.3 节 "包</u> 在实目二识罢"
Show Packet in New Window		任 新 茵 凵 显示 当 則 包, (新 茵 凵 仪 包 含
		View,Byte View 两个面极)
Reload	Ctrl+R	重新冉如当丽捕捉又件

## **3.8. "Go"**菜单

Wireshark "GO"菜单的内容见<u>表 3.5 ""GO"菜单项"</u> **图 3.6. "GO"菜单** 

🗹 test. pcap - Wireshark			
<u>File Edit View Go</u> Capture <u>A</u> nalyze Statistics	Help		
Image: Section of the section of	ight 🖉 🖉 🗢	* * T 1 🗐 🗐 🔍 Q	
Eilter: Go to Corresponding Packet	I+G		
No         Time         Time         First Packet           1         0.0000 <u>L</u> ast Packet               2              0.299139               192.168.0.1               1            3         0.299214          192.168.0.2               1               1               1               1 <td>ation dcast 192.168.0.2</td> <td>Protocol Info ARP Who has 192.168.0.2? Gratuitous NBNS Name query NBSTAT *&lt;00&gt;&lt;00&gt;&lt; ICMP Destination unreachable (Port un</td> <td></td>	ation dcast 192.168.0.2	Protocol Info ARP Who has 192.168.0.2? Gratuitous NBNS Name query NBSTAT *<00><00>< ICMP Destination unreachable (Port un	
4       1.025659       192.168.0.2       2         5       1.044366       192.168.0.2       2         6       1.048652       192.168.0.2       2         7       1.050784       192.168.0.2       2         8       1.055053       192.168.0.1       1         9       1.082038       192.168.0.2       1         10       1.111945       192.168.0.2       1	224.0.0.22 192.168.0.1 239.255.255.250 192.168.0.1 192.168.0.2 192.168.0.2 192.168.0.255	IGMP V3 Membership Report DNS Standard query SRV _ldaptcp.nb UDP Source port: 3193 Destination p DNS Standard query SOA nb10061d.ww00 UDP Source port: 1900 Destination p NBNS Registration NB NB10061D<00> DNS Standard query A proxyconf.ww004	gr ot 4.
11 1.226156 192.168.0.2 1 12 1.227282 192.168.0.1 1	192.168.0.1 192.168.0.2	TCP 3196 > http [SYN] Seq=0 Len=0 MS TCP http > 3196 [SYN, ACK] Seq=0 Ack	5
<ul> <li>Frame 11 (62 bytes on wire, 62 bytes cap</li> <li>Ethernet II, Src: 192.168.0.2 (00:0b:5d</li> <li>Internet Protocol, Src: 192.168.0.2 (19)</li> <li>Transmission Control Protocol, Src Port Source port: 3196 (3196) Destination port: http (80) Sequence number: 0 (relative seque Header length: 28 bytes</li> <li>Flags: 0×0002 (SYN) Window size: 64240</li> <li>0000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 0010 00 30 18 48 40 00 80 06 61 2c c0 a8 0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 0030 fa f0 27 e0 00 00 02 04 05 b4 01 01</li> </ul>	08 00 45 00[-u. 00 02 c0 a8 .0.H@. 00 02 c0 a8 .0.H@. 00 02 c0 a8 .0.H@. 00 02 c0 a8 .0.H@. 00 00 70 02	<pre>gear_2d:75:9a (00:09:5b:2d:75:9a) 168.0.1 (192.168.0.1) ort: http (80), Seq: 0, Len: 0 ]E a, &gt;&lt;6p.</pre>	
File: "D:/test.pcap" 14 KB 00:00:02		P: 120 D: 120 M: 0	.:

# 表 3.5. "GO"菜单项

菜单项	快捷 键	描述
Back	Alt+L eft	跳到最近浏览的包,类似于浏览器中的页面历史纪录
ForWard	Alt+Ri ght	跳到下一个最近浏览的包, 跟浏览器类似
Go to Packet	Ctrl+ G	打开一个对话框,输入指定的包序号,然后跳转到对应的包,见 <u>第 6.8 节"到指定的包"</u>
Go to		
Corresponding		跳转到当前包的应答包,如果不存在,该选项为灰色
Packet		
Previous Pack et	Ctrl+ UP	移动到包列表中的前一个包,即使包列表面板不是当前焦点, 也是可用的
Next Pack et	Ctrl+ Down	移动到包列表中的后一个包,同上
First Packet		移动到列表中的第一个包
Last Packet		移动到列表中的最后一个包

## 3.9. "Capture"菜单

"Capture"菜单的各项说明见<u>表 3.6 ""Capture"菜单项"</u> 图 3.7. "Capture"菜单

🖪 test. po	ap - W	ires	hark						×
<u>Eile E</u> dit	⊻iew	Go	Capture Analyze	Statistics	Help				
	0		Interfaces Options	Ctrl+K	°, 占	Q 🗢	🕸 🕸		
Eilter:			Stop	Ctrl+E			- 4	Expression 🗞 Clear 🛛 Apply	
No	Time 0.0000	00	Restart Capture Filters.		Destination Broadcast		Protocol ARP	Info Who has 192.168.0.2? Gratuitous /	^
2 3 4	0.2991 0.2992 1.0256	.39 14 59	192.168.0.1 192.168.0.2 192.168.0.2		192.168.0.3 192.168.0.3 224.0.0.22	2 1	NBNS ICMP TGMP	Name query NBSTAT *<00><00><00><00 Destination unreachable (Port unre V3 Membershin Report	
5	1.0443	66 52	192.168.0.2 192.168.0.2		192.168.0.1 239.255.255	1 5.250	DNS UDP DNS	Standard query SRV _ldaptcp.nbgr Source port: 3193 Destination por Standard query SOA ph10061d pr004	
8	1.0550	53 38	192.168.0.2 192.168.0.1 192.168.0.2		192.168.0.1	2	UDP NBNS	Source port: 1900 Destination por Registration NB NB10061D<00>	
10 11 12	1.111 1.2261 1.2272	45 56 82	192.168.0.2 192.168.0.2 192.168.0.1		192.168.0.1 192.168.0.1 192.168.0.1	1 1 2	TCP TCP	Standard query A proxyconf.ww004.: 3196 > http [SYN] Seq=0 Len=0 MSS http > 3196 [SYN, ACK] Seq=0 Ack=:	~
<									_
<ul> <li>              Frame          </li> <li>             Etherr              Interr      </li> </ul>	11 (62 net II, net Pro	2 by Sri otoco	tes on wire, 62 c: 192.168.0.2 ol, Src: 192.10	9 bytes c (00:0b:5 58.0.2 (1	aptured) d:20:cd:02) 92.168.0.2)	, Dst: Net , Dst: 192	tgear_2d:; 2.168.0.1	75:9a (00:09:5b:2d:75:9a) (192.168.0.1)	^
Sour Sour Dest Sequ	nssion rce po tinatio uence	rt: on p numb	atrol Protocol, 3196 (3196) ort: http (80) er: 0 (rela	tive sequ	ience number	96), Dst (	ort: http	p (80), Seq: 0, Len: 0	Ш
Head ⊕ Flag	der le gs: Ox	ngth 0002	: 28 bytes (SYN)						
Wind	dow si:	ze:	64240			5.5 F		-	<u>×</u>
0000 00 0010 00 0020 00 0030 fa	09 56 30 18 01 0c f0 27	2d 48 - 7c - e0 -	75 9a 00 06 5 40 00 80 06 6 00 50 3c 36 9 00 00 02 04 0	1 20 cd 0 L 2c c0 a 5 f8 00 0 5 b4 01 0	2 08 00 45 8 00 02 c0 0 00 00 70 1 04 02	00[-  a8 .0.H 02  	u ] a a, .P<6	E.  p. 	
File: "D:/tes	t.pcap":	14 KB	00:00:02					P: 120 D: 120 M: 0	.:

### 表 3.6. "Capture"菜单项

菜单项	快捷	说明
Interface		在弹出对话框选择您要进行捕捉的网络接口,见 <u>第 4.4 节"捕捉接口</u> <u>对话框"</u>
Ontions	Ctrl+	打开设置捕捉选项的对话框,(见 <u>第 4.5 节 "捕捉选项对话框"</u> )并可以
Options	Κ	在此开始捕捉
Start		立即开始捕捉,设置都是参照最后一次设置。
Stop	Ctrl+ E	停止正在进行的捕捉,见 <u>第 4.9.1 节 "停止捕捉"</u>
Restart		正在进行捕捉时,停止捕捉,并按同样的设置重新开始捕捉.仅在您认 为有必要时
Capture		打开对话框,编辑捕捉过滤设置,可以命名过滤器,保存为其他捕捉
Filters		时使用见 <u>第 6.6 节 "定义,保存过滤器"</u>

## 3.10. "Analyze"菜单

"Analyze"菜单的各项见<u>表 3.7 ""analyze"菜单项"</u> 图 3.8. "Analyze"菜单

🛛 test.pcap - Wireshark			×
Eile Edit ⊻iew Go Capture	Analyze Statistics Help		
	Display Filters Apply as Filter	Selected	
Eilter:	Prepare a Filter  Firewall ACL Rules	Not Selected and Selected or Selected or Selected or Selected	
No Time Source 1 0.000000 192.1 2 0.299139 192.1 3 0.299214 192.1		or selected or not Selected or not Selected Ias 192.168.0.2? Gratuitous / query NBSTAT *<00><00><00	
4 1.025659 192.1 5 1.044366 192.1 6 1.048652 192.1 7 1.050784 192.1 8 1.055053 192.1 9 1.082038 192.1	Eollow TCP Stream Eollow SSL Stream Expert Info Expert Info ⊆omposite	IGMP V3 Membership Report DNS Standard query SRV _ldaptcp.nbgr UDP Source port: 3193 Destination por DNS Standard query SOA nb10061d.ww004. UDP Source port: 1900 Destination por NBNS Registration NB NB10061D<00>	
10 1.111945 192.1 11 1.226156 192.1 12 1.227282 192.1	68.0.2         192.168.0.1           68.0.2         192.168.0.1           68.0.1         192.168.0.2           68.0.1         192.168.0.2	DNS Standard query A proxyconf.ww004.: TCP 3196 > http [SYN] Seq=0 Len=0 MSS: TCP http > 3196 [SYN, ACK] Seq=0 Ack=:	*
<ul> <li>✓</li> <li>Frame 11 (62 bytes on</li> <li>Ethernet II, Src: 192.</li> <li>Internet Protocol, Src</li> <li>Transmission Control P Source port: 3196 (3)</li> </ul>	<pre>wire, 62 bytes captured) 168.0.2 (00:0b:5d:20:cd:02), Dst: 192.168.0.2 (192.168.0.2), Dst: rotocol, Src Port: 3196 (3196), D 196)</pre>	<pre>Netgear_2d:75:9a (00:09:5b:2d:75:9a) : 192.168.0.1 (192.168.0.1) Dst Port: http (80), Seq: 0, Len: 0</pre>	< _
Destination port: ht Sequence number: O Header length: 28 by Flags: 0×0002 (SYN) Window size: 64240	tp (80) (relative sequence number) tes		<
0000 00 09 5b 2d 75 9a 0 0010 00 30 18 48 40 00 8 0020 00 01 0c 7c 00 50 3 0030 fa f0 27 e0 00 00 0	0 0b 5d 20 cd 02 08 00 45 00 . 0 06 61 2c c0 a8 00 02 c0 a8 . c 36 95 f8 00 00 00 00 70 02 . 2 04 05 b4 01 01 04 02 .	[-u]E. .0.H@a,p. 	
Transmission Control Protocol (tcp),	28 bytes	P: 120 D: 120 M: 0	11

### 表 3.7. "analyze"菜单项

菜单项	快捷键	说明
Display		打开过滤器对话框编辑过滤设置,可以命名过滤设置,保存为其他
Filters		地方使用,见 <u>第 6.6 节 "定义,保存过滤器"</u>
Apply as		更改当前过滤显示并立即应用。根据选择的项,当前显示字段会被
Filter>		替换成选择在 Detail 面板的协议字段
Prepare a		更改当前显示过滤设置,当不会立即应用。同样根据当前选择项,
Filter>		过滤字符会被替换成 Detail 面板选择的协议字段
		为多种不同的防火墙创建命令行 ACL 规则(访问控制列表),支持
		Cisco IOS, Linux Netfilter (iptables), OpenBSD pf and Windows
FIFEWAII ACL		Firewall (via netsh). Rules for MAC addresses, IPv4 addresses, TCP
Kules		and UDP ports, 以及 IPv4+混合端口
		以上假定规则用于外部接口
Enable	Shift+Ct	目不会次社》2014年,回答 0.41 苯 (@Pashla Paskasah)是任何
Protocols	rl+R	定百兀叶协以万 <u>析,见<u>弗 9.4.1 可 "Enable Protocols"</u>》[话性"</u>

[4] 看样子他们有个关于这部分的章节

## 3.11. "Statistics"菜单

Wireshark "statistics"菜单项见表 3.8 "" 图 3.9. "Statistics"菜单

🖪 test.pcap - Wireshark		
<u> Eile Edit View Go Capture Analyze</u>	Statistics Help	
	Dummary Protocol Hierarchy	◆ ◆ ◆ 주 ⊈ 🗐 🛃 🔍 �
Eilter:	<ul> <li>Conversations</li> <li>Endpoints</li> <li>IO Graphs</li> </ul>	▼ ♣ Expression Soi ⊆lear ♥ Apply
No Time Source 1 0.000000 192.168.0.2 2 0.299139 192.168.0.1	Conversation List	Protocol Info ARP Who has 192.168.0.2? Gratuitous / NBNS Name query NBSTAT *<00><00><00><00<
<pre>3 0.299214 192.168.0.2 4 1.025659 192.168.0.2 5 1.044366 192.168.0.2 6 1.048652 192.168.0.2 7 1.050784 192.168.0.2 8 1.055053 192.168.0.1 9 1.082038 192.168.0.2 10 1.111945 192.168.0.2 11 1.226156 192.168.0.2 12 1.227282 192.168.0.1</pre> ★ Frame 11 (62 bytes on wire, 62 Ethernet II, Src: 192.168.0.2 ★ Internet Protocol, Src: 192.168 ★ Internet Protocol, Src: 192.168 ★ Source port: 3196 (3196) Destination port: http (80) Sequence number: 0 (related the section of the	ANSI ANSI GSM H.225 MTP3 RTP SCTP SCTP SCTP SIP OVIP Calls WAP-WSP BOOTP-DHCP Destinations Flow Graph HTTP	<pre>     AFP     Ination unreachable (Port unre mbership Report     fibre Channel     Fibre Channel     H.225 RAS     te port: 3193 Destination por hArd query SOA nb10061d.ww004. te port: 1900 Destination por bLDAP     stration NB NB10061D&lt;00&gt;     lard query A proxyconf.ww004.: NCP     http [SYN] Seq=0 Len=0 MSS: ONC-RPC     stration SMB     SMB2     (00:09:5b:2d:75:9a)     192.168.0.1 (192.168.0.1)     st Port: http (80), Seq: 0, Len: 0 </pre>
Header Tength: 28 bytes	IP address ISUP Messages Multicast Streams ONC-RPC Programs	.[-u]E. ).H@a,
0030 fa f0 27 e0 00 00 02 04 05	Packec Length Port Type TCP Stream Graph	P: 120 D: 120 M: 0

表 3.8.	
菜单项 快捷 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一	描述
Summary	显示捕捉数据摘要,见 <u>第 8.2 节 "摘要窗口"</u>
Protocol Hierarchy	显示协议统计分层信息,见 <u>第 8.3 节 ""Protocol Hierarchy"窗口"</u>
Conversations/	显示会话列表(两个终端之间的通信),见???
EndPoints	显示端点列表(通信发起,结束地址),见 <u>第 8.4.2 节 ""Endpoints"窗</u> <u>口"</u>
IO Graphs	显示用户指定图表, (如包数量-时间表)见 <u>第 8.6 节 ""IO Graphs"窗</u> 口"
Conversation	通过一个组合窗口,显示会话列表,见 <u>第 8.5.3 节"协议指定</u>
List	<u>"Conversation List/会话列表"窗口"</u>
Endpoint List	通过一个组合窗口显示终端列表,见 <u>第 8.4.3 节 "特定协议的</u> "Endpoint List"窗口"
Service	显示一个请求及其相应之间的间隔时间,见 <u>第 8.7 节"服务相应时</u>
Response Time	间"
ANSI	见 <u>第 8.8 节"协议指定统计窗口"</u>
GSM	见 <u>第 8.8 节"协议指定统计窗口"</u>
H.225	见 <u>第 8.8 节"协议指定统计窗口"</u>
ISUP Message	见 <u>第 8.8 节"协议指定统计窗口"</u>
Types	见 <u>第 8.8 节 "协议指定统计窗口"</u>
MTP3	见 <u>第 8.8 节 "协议指定统计窗口"</u>
RTP	见 <u>第 8.8 节 "协议指定统计窗口"</u>
GSM	见 <u>第 8.8 节 "协议指定统计窗口"</u>
SIP	见第 8.8 节 "协议指定统计窗口"

VOIP Calls	见 <u>第 8.8 节"协议指定统计窗口"</u>
WAP-WSP	见 <u>第 8.8 节 "协议指定统计窗口"</u>
НТТР	HTTP 请求/相应统计,见 <u>第 8.8 节"协议指定统计窗口"</u>
ISUP Messages	见 <u>第 8.8 节"协议指定统计窗口"</u>
ONC-RPC Programs	见 <u>第 8.8 节 "协议指定统计窗口"</u>
TCP Stream Graph	见 <u>第 8.8 节"协议指定统计窗口"</u>

## 3.12. "Help"菜单

### 帮助菜单的内容见表 3.9 "" 图 3.10. 帮助菜单

🗥 test.pcap - Wireshark		
Eile Edit View Go Capture Analyze Statistics	Help	
	Contents F1 Supported Protocols	
Eilter:	Manual Pages	▶ 🕂 🕂 Expression 🦢 Clear 🖋 Apply
	Wireshark Online	🕨 🏦 Home Page 📃 📃
No Time Source 1 0.000000 192.168.0.2	🖪 About Wireshark	🥑 Wiki 192.168.0.2? Gratuitous /
2 0.299139 192.168.0.1	192.168.0.2	ny NBSTAT * <00> <00> <00> <00
3 0.299214 192.168.0.2	192.168.0.1	FAQS fon unreachable (Port unre
4 1.025659 192.168.0.2 5 1 044366 192 168 0 2	224.0.0.22	Downloads rsnip keport
6 1.048652 192.168.0.2	239.255.255.250	Example Files ort: 3193 Destination por
7 1.050784 192.168.0.2	192.168.0.1	DNS Standard guery 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 1.22/282 192.168.0.1	192.168.0.2	TCP - http > 3196 [SYN, ACK] Seq=0 Ack=: 🗸
<		<u>&gt;</u>
표 Frame 11 (62 bytes on wire, 62 bytes 🛛	aptured)	<u>^</u>
Ethernet II, Src: 192.168.0.2 (00:0b:	d:20:cd:02), Dst: Netg	jear_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 Pon	rt: 3196 (3196), Dst Po	ort: http (80), Seg: 0, Len: 0
Source port: 3196 (3196)		
Destination port: http (80)		
Sequence number: 0 (nelative seq	uence number)	
Headen Jonath, 38 hytes	dence number)	
Flager Pages (SMP)		
H Flags: 0x0002 (SYN)		
Window size: 64240		×
0000 00 09 5b 2d 75 9a 00 0b 5d 20 cd ( 0010 00 30 18 48 40 00 80 06 61 2c c0 0 0020 00 01 0c 7c 00 50 3c 36 95 f8 00 ( 0030 fa f0 27 e0 00 00 02 04 05 b4 01 (	02 08 00 45 00[-u. a8 00 02 c0 a8 .0.H@. 00 00 00 70 02] 01 04 02	]E. a,p. p.
Transmission Control Protocol (tcp), 28 bytes		P: 120 D: 120 M: 0 .:

### 表 3.9.

衣 3.9.		
菜单项	快捷使建	描述
Contents	F1	打开一个基本的帮助系统
Supported		打开一个对话框显示支持的协议或工具
Protocols		
Manaul Pages>		打开浏览器,显示安装在本地的手册
Wireshark		按照选择目示在建资源
Online>		汉黑 <b>赵</b> 伟亚小江线页 <i>体</i>
About Wireshark		弹出信息窗口显示 Wireshark 的一些相关信息,如插件,目录等。

注意

有些版本可能不支持调用 WEB 浏览器。如果是这样,可能会隐藏此菜单。 注意

如果调用浏览器错误,检查 Wireshark 首选项关于浏览器设置。

### 3.13. "Main"工具栏

主工具栏提供了快速访问常见项目的功能,它是不可以自定义的,但如果您觉得屏幕屏幕过于狭小,需要更多空间来显示数据。您可以使用浏览菜单隐藏它。

在主工具栏里面的项目只有在可以使用的时候才能被选择,如果不是可用则显示为灰色,不可选(例如:在未载入文件时,保存文件按钮就不可用.)

图 3.11.

### 表 3.10. 主工具栏选项

工具 栏图 标	工具栏项	对应菜单项	描述						
	接口	Capture/Interfaces	打开接口列表对话框,见 <u>第 4.3 节 "开始捕捉"</u>						
<b>3</b>	选项。。。	Capture/Options	打开捕捉选项对话框,见 <u>第 4.4 节"捕捉接口对话</u> <u>框"</u>						
o.	Start	Capture/Start	使用最后一次的捕捉设置立即开始捕捉						
<b>@</b> [	STOP	Capture/Stop	停止当前的捕捉,见 <u>第 4.3 节"开始捕捉"</u>						
	Restar	Caputer/Rstart	停止当前捕捉,并立即重新开始						
è	Open	File/Open	启动打开文件对话框,用于载入文件,详见 <u>第 5.2.1</u> <u>节"打开捕捉文件对话框</u> "						
	Save As	File/Save As	<ul> <li>【休子当前文件》(江急兴起的文件), 记将会评出 一次</li> <li>话框, (见<u>第 5.3.1 节 ""save Capture File As/保存文</u></li> <li><u>件为"对话框</u>"</li> <li><b>注意</b></li> <li>如果当前文件</li> <li>是临时未保存</li> <li>文件, 图标将会</li> <li>显示为</li> </ul>						
×	Close	File/Close	关闭当前文件。如果未保存,将会提示是否保存						
Ċ	Reload	View/Reload	重新载入当前文件						
	Print	File/Print	打印捕捉文件的全部或部分,将会弹出一个打印对话 框(见 <u>第 5.7 节"打印包"</u> )						
	Find packet	Edit/Find Packet	打开一个对话框,查找包。见 <u>第 6.7 节 "查找包"</u>						
4	Go Back	Go/Go Back	返回历史记录中的上一个						
\$	Go Forward	Go/Go Forward	跳转到历史记录中的下一个包						
	Go to Packet	Go/Go to Packet	弹出一个设置跳转到指定的包的对话框						

Ŧ	Go To First Packet	Go/First Packet	跳转到第一包					
₽	Go To Last Packet	Go/Last Packet	跳转到最后一个包					
	Colorize	View/Coloreze	切换是否以彩色方式显示包列表					
	Auto Scroll in Live	View/Auto Scrool in Live Capture	开启/关闭实时捕捉时自动滚动包列表					
Ð,	Zoom in	View/Zoom In	增大字体					
Θ	zoom out	View/Zoom Out	缩小字体					
	Normal Size	View/Normal Size	设置缩放大小为100%					
**	Resize	View/Resize	重置列宽,使内容适合列宽(使包列表内的文字可以					
· <b>· · · · · ·</b>	Columns	Columns	完全显示)					
	Capture	Capture/Capture	打开对话框,用于创建、编辑过滤器。详见 <u>第 6.6 节</u>					
	Filters	Filters	"定义,保存过滤器"					
V	Display Filters	Analyze/ Filters	打开对话框,用于创建、编辑过滤器。详见 <u>第 6.6 节</u> "定义,保存过滤器"					
	Coloring	View/Coloring	定义以色彩方式显示数据包的规则详见 <u>第 9.3 节</u>					
	Rules	Rules	"包色彩显示设置"					
X	Preferenc es	Edit/Preferences	打开首选项对话框, 详见 <u>第 9.5 节 "首选项"</u>					
Ø	Help	Help/Contents	打开帮助对话框					

## 3.14. "Filter"工具栏

过滤工具栏用于编辑或显示过滤器,更多详情见<u>第 6.3 节"浏览时过滤包"</u> 图 3.12. 过滤工具栏

Eilter:		✓ Imply Expression Signal Apply
表 3.11. 工具栏 图标	工具栏项	说明
$\mathbf{V}$	过滤	打开构建过滤器对话框,见 <u>第 6.7 节 "查找包"<sup>[a]</sup></u>
	过 <b>滤输</b> 入 框	在此区域输入或修改显示的过滤字符,见 <u>第 6.4 节</u> "建立显示过滤表达式",在输入过程中会进行语法检 查。如果您输入的格式不正确,或者未输入完成,则 背景显示为红色。直到您输入合法的表达式,背景会 变为绿色。你可以点击下拉列表选择您先前键入的过 滤字符。列表会一直保留,即使您重新启动程序。 <b>注意</b> 做完修改 之后,记 得点击右 边的 Apply(应 用)按钮,

		或者回 车,以使 过滤生 效。 <b>注意</b> 输入框的 内容同时
		也是当前 过滤器的 内容(当
		前过滤器 的内容会 反映在输 入框)
÷	表达式	标签为表达式的按钮打开一个对话框用以从协议字 段列表中编辑过滤器,详见 <u>第 6.5 节 ""Filter</u> Expression/过滤表达式"对话框"
2	清除	重置当前过滤器,清除输入框
¥	应用	应用当前输入框的表达式为过滤器进行过滤 注意 在大文件 里应用显 示过滤可 能要很长 时间

<sup>a</sup> 我看到的 Filter 按钮貌似没有图标,可能只出现在0.99.4版中

### 3.15. "Pcaket List"面板

Packet list/包列表面板显示所有当前捕捉的包 **图 3.13. "Packet list/包列表"面板** 

No. +	Time	Source	Destination	Protocol	Info	^
1	1 0.000000	192.168.0.2	Broadcast	ARP	Who has 192.168.0.2? Gratuitous	
2	2 0.299139	192.168.0.1	192.168.0.2	NBNS	Name query NBSTAT *<00><00><0	
3	3 0.000075	192.168.0.2	192.168.0.1	ICMP	Destination unreachable (Port un	
4	4 0.726445	192.168.0.2	224.0.0.22	IGMP	V3 Membership Report	
5	5 0.018707	192.168.0.2	192.168.0.1	DNS	Standard query SRV _ldaptcp.nb	1
6	5 0.004286	192.168.0.2	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1	
7	7 0.002132	192.168.0.2	192.168.0.1	DNS	Standard query SOA nb10061d.ww00	
8	3 0.004269	192.168.0.1	192.168.0.2	SSDP	HTTP/1.1 200 OK	
9	9 0.026985	192.168.0.2	192.168.0.255	NBNS	Registration NB NB10061D<00>	
10	0.029907	192.168.0.2	192.168.0.1	DNS	Standard query A proxyconf.ww004	
11	1 0.114211	192.168.0.2	192.168.0.1	TCP	3196 > http [SYN] Seq=0 Ack=0 Wi	1
12	2 0.001126	192.168.0.1	192.168.0.2	TCP	http > 3196 [SYN, ACK] Seq=0 Ack	
13	3 0.000043	192.168.0.2	192.168.0.1	TCP	3196 > http [ACK] Seq=1 Ack=1 Wi	1
14	4 0.000126	192.168.0.2	192.168.0.1	HTTP	SUBSCRIBE /upnp/service/Layer3Fo	1
19	5 0.001858	192.168.0.1	192.168.0.2	TCP	http > 3196 [ACK] Seq=1 Ack=256 M	1
10	5 0.003112	192.168.0.1	192.168.0.2	TCP	[TCP Window Update] http > 3196	
17	7 0.015934	192.168.0.1	192.168.0.2	TCP	_1025 > 5000 [SYN] Seq=0 Ack=0 Wi	
18	3 0.000036	192.168.0.2	192.168.0.1	TCP	5000 > 1025 [SYN, ACK] Seq=0 Ack	
1 1 0	9 0 001790	107 160 0 1	107 160 0 7	UTTO	иттр/1 о роо ом	
<					>	

列表中的每行显示捕捉文件的一个包。如果您选择其中一行,该包得更多情况会显示在"Packet Detail/包详情","Packet Byte/ 包字节"面板

在分析(解剖)包时,Wireshark 会将协议信息放到各个列。因为高层协议通常会覆盖底层协议,您通常在包列表面板看到的都是每个包的最高层协议描述。

例如:让我们看看一个包括 TCP 包, IP 包, 和一个以太网包。在以太网(链路层?)包中解析的数据(比如以太网地址),在 IP

分析中会覆盖为它自己的内容(比如 IP 地址),在 TCP 分析中会覆盖 IP 信息。 包列表面板有很多列可供选择。需要显示哪些列可以在首选项中进行设置,见<u>第 9.5 节"首选项</u>" 默认的列如下 No. 包的编号,编号不会发生改变,即使进行了过滤也同样如此 Time 包的时间戳。包时间戳的格式可以自行设置,见<u>第 6.10 节"时间显示格式及参考时间</u>" Source 显示包的源地址。 Destination 显示包的目标地址。 Protocal 显示包的协议类型的简写 Info 包内容的附加信息 右击包,可以显示对包进行相关操作的上下文菜单。见<u>第 6.3 节"浏览时过滤包</u>"

### 3.16. "Packet Details"面板

"Packet Details/包详情"面板显示当前包(在包列表面板被选中的包)的详情列表。

### 图 3.14. "Packet Details/包详情"面板

```
    H Frame 1 (42 bytes on wire, 42 bytes captured)
    H Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Broadcast (ff:ff:ff:ff:ff)
    H Address Resolution Protocol (request/gratuitous ARP)
```

该面板显示包列表面板选中包的协议及协议字段,协议及字段以树状方式组织。你可以展开或折叠它们。 右击它们会获得相关的上下文菜单。见<u>第 6.4 节"建立显示过滤表达式"</u> 某些协议字段会以特殊方式显示

**Generated fields/衍生字段** Wireshark 会将自己生成附加协议字段加上括号。衍生字段是通过该包的相关的其他包结合生成的。例如: Wireshark 在对 TCP 流应答序列进行分析时。将会在 TCP 协议中添加[SEQ/ACK analysis]字段 **Links/链接** 如果 Wireshark 检测到当前包与其它包的关系,将会产生一个到其它包的链接。链接字段显示为蓝色字体,并加有下划线。双击它会跳转到对应的包。

### 3.17. "Packet Byte"面板

Packet Byte/包字节 面板以16进制转储方式显示当前选择包的数据

### 图 3.15. Packet Byte/包字节面板

0000	ff 08	ff 00	ff 06	ff 04	ff 00	ff 01	00	Ob Ob	5d 5d	20	cd cd	02 02	08 c0	06 a8	00 00	01 02	]
0020	00	00	00	00	00	00	CU	ao	00	02							

通常在16进制转储形式中,左侧显示包数据偏移量,中间栏以16进制表示,右侧显示为对应的ASCII字符 根据包数据的不同,有时候包字节面板可能会有多个页面,例如:有时候 Wireshark 会将多个分片重组为一个,见<u>第 7.5 节</u> "重组包",这时会在面板底部出现一个附加按钮供你选择查看

#### 图 3.16. 带选项的"Paket Bytes/包字节"面板

																			-
0000	08	00	06	ab	04	53	08	00	06	6b	7f	bd	08	00	45	00	SkE.	~	
0010	01	48	33	C7	00	00	1e	11	dd	51	bc	a8	08	0a	bc	a8	.H3Q		f
0020	09	32	41	af	07	04	01	34	00	b4	04	00	2e	00	10	00	.2A4		4
0030	00	00	00	00	a0	de	97	6C	d1	11	82	71	00	57	80	fO	lq.w	~	t
Frame	(342	byte	es) [	Rea:	ssem	bled	DCE		(160	I4 by	tes)	Т							

#### 注意

附加页面的内容可能来自多个包。 右击选项按钮会显示一个上下文菜单显示所有可用的页的清单。如果您的面板尺寸过小,这项功能或许有所帮助

### 3.18. 状态栏

状态栏用于显示信息 通常状态栏的左侧会显示相关上下文信息,右侧会显示当前包数目 图 3.17. 初始状态栏

## Ready to load or capture

No Packets

//

该状态栏显示的是没有文件载入时的状态,如: 刚启动 Wireshark 时 图 3.18. 载入文件后的状态栏

File: test.cap 14 KB 00:00:02	P: 120 D: 120 M: 0

左侧显示当前捕捉文件信息,包括名称,大小,捕捉持续时间等。 右侧显示当前包在文件中的数量,会显示如下值 P:捕捉包的数目 D:被显示的包的数目 M: 被标记的包的数目. 图 3.19. 已选择协议字段的状态栏

Opcode (arp.opcode), 2 bytes

P: 120 D: 120 M: 0

如果你已经在"Packet Detail/包详情"面板选择了一个协议字段,将会显示上图

提示

括号内的值(如上图的 app.opcode)可以作为显示过滤使用。它表示选择的协议字段。

### 第4章 实时捕捉数据包

### 長子

4.1. 介绍 4.2. 准备工作 4.3. 开始捕捉 4.4. 捕捉接口对话框 4.5. 捕捉选项对话框 4.5.1. 捕捉桢 4.5.2. 捉数据帧为文件。 <u>4.5.3. 停止捕捉桢</u> 4.5.4. 显示桢选项 4.5.5. 名称解析设置 <u>4.5.6. 按钮</u> 4.6. 捕捉文件格式、模式设置 4.7. 链路层包头类型 4.8. 捕捉时过滤 4.8.1. 自动过滤远程通信 4.9. 在捕捉过程中 4.9.1. 停止捕捉 4.9.2. 重新启动捕捉

### 4.1. 介绍

实时捕捉数据包时Wireshar的特色之一 Wiershark 捕捉引擎具备以下特点 支持多种网络接口的捕捉(以太网,令牌环网,ATM...) 支持多种机制触发停止捕捉,例如:捕捉文件的大小,捕捉持续时间,捕捉到包的数量... 捕捉时同时显示包解码详情 设置过滤,减少捕捉到包的容量。见<u>第 4.8 节"捕捉时过滤"</u> 长时间捕捉时,可以设置生成多个文件。对于特别长时间的捕捉,可以设置捕捉文件大小罚值,设置仅保留最后的N个文 件等手段。见<u>第 4.6 节"捕捉文件格式、模式设置"</u> Wireshark 捕捉引擎在以下几个方面尚有不足 从多个网络接口同时实时捕捉,(但是您可以开始多个应用程序实体,捕捉后进行文件合并) 根据捕捉到的数据停止捕捉(或其他操作)

### 4.2. 准备工作

第一次设置 Wireshark 捕捉包可能会遇到一些小麻烦 **提示** 

关于如何进行捕捉设置的较为全面的向导可以在:<u>http://wiki.wireshark.org/CaptureSetup.</u> 这里有一些常见需要注意的地方 你必须拥有 root/Administrator 特权以开始捕捉<sup>[12]</sup> 必须选择正确的网络接口捕捉数据 如果您想捕捉某处的通信,你必须作出决定:在什么地方可以捕捉到 ......以及许多 如果你碰到设置问题,建议看看前面的那个向导,或许会有所帮助

[12] 记得在 Windows 安装那一节层提到如果作为服务启动可以避免非管理员无法进行捕捉,不知道二者能否相互印证。

### 4.3. 开始捕捉

可以使用下任一方式开始捕捉包

使用 打开捕捉接口对话框,浏览可用的本地网络接口,见<u>图 4.1 ""Capture Interfaces"捕捉接口对话框"</u>,选择您需要进行捕捉的接口启动捕捉

你也可以使用"并提选项"按钮启动对话框开始捕捉,见图 4.2 ""Capture Option/捕捉选项"对话框"

如果您前次捕捉时的设置和现在的要求一样,您可以点击" 并开始捕捉"按钮或者是菜单项立即开始本次捕捉。

如果你已经知道捕捉接口的名称,可以使用如下命令从命令行开始捕捉:

wireshark -i eth0 -k

上述命令会从 eht0接口开始捕捉,有关命令行的介绍参见<u>第 9.2 节 "从命令行启动 Wireshark"</u>

### 4.4. 捕捉接口对话框

如果您从捕捉菜单选择"Interface...",将会弹出如<u>图 4.1 ""Capture Interfaces"捕捉接口对话框"</u>所示的对话框 **警告** 

打开"Capture Interfaces"/捕捉对话框时 同时正在显示捕捉的数据,这将会大量消耗您的系统资源。尽快选择您需要的接口以结束该对话框。避免影响系统性能

#### 注意

这个对话框只显示本地已知的网络接口,Wireshark可能无法检测到所有的本地接口,Wireshark不能检测远程可用的网络接口,Wireshark只能使用列出可用的网络接口

### 图 4.1. "Capture Interfaces"捕捉接口对话框

🖓 Wireshark: Capture Interfaces				
Description	IP	Packets	Packets/s	Stop
🛒. Adapter for generic dialup and VPN capture	unknown	0	0	
🛒. Broadcom NetXtreme Gigabit Ethernet Driver	11	110	1	Start
Elp Help				K ⊆lose

描述

IP

从操作系统获取的接口信息

Wireshark 能解析的第一个 IP 地址,如果接口未获得 IP 地址(如,不存在可用的 DHCP 服务器),将会显示"Unkow",如果有超过一个 IP 的,只显示第一个(无法确定哪一个会显示).

#### **Packets**

打开该窗口后,从此接口捕捉到的包的数目。如果一直没有接收到包,则会显示为灰度

Pack ets/s

最近一秒捕捉到包的数目。如果最近一秒没有捕捉到包,将会是灰度显示

### Stop

停止当前运行的捕捉

### Capture

从选择的接口立即开始捕捉,使用最后一次捕捉的设置。 Options 打开该接口的捕捉选项对话框,见 <u>第 4.5 节 "捕捉选项对话框</u>" Details(仅 Win32系统)

打开对话框显示接口的详细信息

Close

关闭对话框

### 4.5. 捕捉选项对话框

如果您从捕捉菜单选择"start..."按钮(或者从主工具栏选择对应的项目),Wireshark 弹出"Capture Option/捕捉选项"对话框。如 图 4.2 ""Capture Option/捕捉选项"对话框"所示

### 图 4.2. "Capture Option/捕捉选项"对话框

🖸 Wireshark: C	apture (	Options									
Capture	Capture										
Interface: Bro	Interface: Broadcom NetXtreme Gigabit Ethernet Driver: \Device\NPF_{4C4DB8EB-AC95-4B46-9										
IP address: 157.3	163.15.28										
Link-layer header	type: E	ithernet 👻	Buffer size: 1		🗢 megabyte(s)						
🔽 Capture packs	Capture packets in promiscuous mode										
📃 Limit each pac	ket to 68	0	bytes								
Gapture Filte	er:				•						
Capture File(s)					Display Options						
File:			Brows	;e	✓ Update list of packets in real time						
Use <u>m</u> ultiple fil	es				Automatic scrolling in live capture						
Next file every	/ 1		megabyte(s)	~							
Next file every	/ 1		minute(s)	~	Hide capture info dialog						
🗹 Ring buffer wi	th 2		🗘 files		Name Resolution						
Stop capture a	after 1		🗘 file(s)		Epoble M0C pame resolution						
Stop Capture											
🔲 after	1	2	packet(s)		Enable network name resolution						
🔲 after	1	÷	megabyte(s)	~	🔽 Eachta burgeraidh anns an achtáise						
📃 after	1	2	minute(s)	~	Linable transport name resolution						
🔯 <u>H</u> elp					Start 🗶 Cancel						

### 提示

如果你不了解各项设置的意义,建议保持默认。 你可以用对话框中的如下字段进行设置

### 4.5.1. 捕捉桢

#### Interface

该字段指定你想用于进行捕捉的借口。一次只能使用一个接口。这是一个下拉列表,简单点击右侧的按钮,选择你想要使用的接口。默认第一是支持捕捉的 non-loopback(非环回)接口,如果没有这样的接口,第一个将是环回接口。在某些系统中,回借口不支持捕捉包(windows 平台下的环回接口就不支持。) 在命令行使用-i <interface>参数可以替代该选项

### IP address

表示选择接口的 IP 地址。如果系统未指定 IP 地址,将会显示为"unknown"

### Link-layer header type

除非你有些特殊应用,尽量保持此选项默认。想了解更多详情,见 <u>第 4.7 节"链路层包头类型"</u> Buffer size: n megabyte(s) 输入用于捕捉的缓层大小。该选项是设置写入数据到磁盘前保留在核心缓存中捕捉数据的大小,如果你发现丢包。尝试增 大该值。

### 注意

该选项仅适用于 Windows 平台

Capture packets in promiscuous mode

指定 Wireshark 捕捉包时,设置接口为杂收模式(有些人翻译为混杂模式)。如果你**未指定**该选项,Wireshark 将只能捕捉进出你电脑的数据包(不能捕捉整个局域网段的包)<sup>[13]</sup>

#### 注意

如果其他应用程序将网卡设置为杂收模式,即使不选中该选项,也会工作于杂收模式下。

注意

即使在杂收模式下,你也未必能够接收到整个网段所有的网络包。详细解释见

http://www.wireshark.org/faq.html#promiscsniff

Limit each packet to n bytes

指定捕捉过程中,每个包的最大字节数。在某些地方被称为。"snaplen".<sup>[14]</sup>如果禁止该选项,默认值为65535,这适用于大 多数协议,下面是一些大多数情况下都适用的规则(这里又出现了拇指规则,第一章,系统需求时提到过。这里权且翻译作 普适而非绝对的规则))

如果你不确定,尽量保持默认值

如果你不需要包中的所有数据。例如:如果您仅需要链路层、IP和TCP包头,您可能想要选择一个较小的快照长度。这样只需要较少的 cpu 占用时间用于复制包,包需要的缓存也较少。如此在繁忙网络中捕捉时丢失的包也可能会相应少一点。如果你没有捕捉包中的所有数据(适用 snpaplen 截断了包),你可能会发现有时候你想要的包中的数据部分被截断丢弃了。或者因为缺少重要的部分,想对某些包进行重组而发现失败。

Capture Filter

指定捕捉过滤。捕捉过滤器将会在有<u>第 4.8 节"捕捉时过滤"</u>详细介绍,默认情况下是空的。 同样你也可以点击捕捉按钮,通过弹出的捕捉过滤对话框创建或选择一个过滤器,详见<u>第 6.6 节"定义,保存过滤器</u>"

### 4.5.2. 捉数据帧为文件。

捕捉文件设置的使用方法的详细介绍见<u>第 4.6 节"捕捉文件格式、模式设置</u>" File 指定将用于捕捉的文件名。该字段默认是空白。如果保持空白,捕捉数据将会存储在临时文件夹。详见<u>第 4.6 节"捕捉文</u> <u>件格式、模式设置</u>" 你可以点击右侧的按钮打开浏览窗口设置文件存储位置 Use multiple files 如果指定条件达到临界值,Wireshark将会自动生成一个新文件,而不是适用单独文件。 Next file every n megabyte(s) 仅适用选中 Use multiple files,如果捕捉文件容量达到指定值,将会生成切换到新文件 Next file every n minutes(s) 仅适用选中 Use multiple files,如果捕捉文件持续时间达到指定值,将会切换到新文件。 Ring buffer with n files 仅适用选中 Use multiple files,如果捕捉文件持续时间达到指定值,将会切换到新文件。 Stop caputure after n file(s) 仅适用选中 Use multiple files,但生成制定数目的文件。

### 4.5.3. 停止捕捉桢

... after n packet(s)
在捕捉到指定数目数据包后停止捕捉
... after n megabytes(s)
在捕捉到指定容量的数据(byte(s)/kilobyte(s)/megabyte(s)/gigabyte(s))后停止捕捉。如果没有适用"user multiple files",该选项 将是灰色
... after n minute(s)
在达到指定时间后停止捕捉

### 4.5.4. 显示桢选项

Update list of packets in real time

在包列表面板实时更新捕捉数据。如果**未选定**该选项,在Wireshark 捕捉结束之前将不能显示数据。如果选中该选项,Wireshark 将生成两个独立的进程,通过捕捉进程传输数据给显示进程。 Automatic scrolling in live capture

指定 Wireshark 在有数据进入时实时滚动包列表面板,这样您将一直能看到最近的包。反之,则最新数据包会被放置在行

末,但不会自动滚动面板。如果未设置"update list of packets in real time",该选项将是灰色不可选的。 Hide capture info dialog 选中该选项,将会隐藏捕捉信息对话框

### 4.5.5. 名称解析设置

Enable MAC name resolution 设置是否让 Wireshark 翻译 MAC 地址为名称,见<u>第 7.6 节 "名称解析"</u> Enable network name resolution 是否允许 Wireshark 对网络地址进行解析,见<u>第 7.6 节 "名称解析"</u>

### 4.5.6. 按钮

进行完上述设置以后,你可以点击 start 按钮进行捕捉,也可以点击 Cancel 退出捕捉. 开始捕捉以后,在你收集到足够的数据时你可以停止捕捉。见<u>第 4.9 节 "在捕捉过程中"</u>

<sup>[13]</sup> 网卡在局域网内会接到很多不属于自己的包,默认情况下,网卡会不对这些包进行处理。貌似设置为杂收模式,Wireshak 会监听所有的包,但并不作出相应。

<sup>141</sup> 粗略查了一下,未找到该词的合适翻译,多见于 Winpcap 的描述,如果把该单词拆分, snap:单元,快照, len:长度,似乎 就是单位长度,单元大小的意思。在看看该段下面第二个如果中提到的 snapshot length, snaplen 应该是二者的简写形式,快 照长度

### 4.6. 捕捉文件格式、模式设置

在 捕捉时,libpcap 捕捉引擎(linux 环境下)会抓取来自网卡的包存放在(相对来说)较小的核心缓存内。这些数据由 Wireshark 读取并保存到用户指定的捕捉文件中。

保存包数据到捕捉文件时,可采用差异模式操作。

#### 提示

处理大文件(数百兆)将会变得非常慢。如果你计划进行长时间捕捉,或者处于一个高吞吐量的网络中,考虑使用前面提到的"Multiple files/多文件"选项。该选项可以将捕捉包分割为多个小文件。这样可能更适合上述环境。

#### 注意

使用多文件可能会切断上下文关联信息。Wireshark 保留载入包的上下文信息,所以它会 报告上下文关联问题(例如流问题)和关联上下文协议信息(例如:何处数据产生建立阶段, 必须查找后续包)。这些信息仅能在载入文件中显示,使用多文件模式可能会截断这样的 上下文。如果建立连接阶段已经保存在一个文件中,你想要看的在另一个文件中,你可 能无法看到可用的上下文关联信息。

提示

关于捕捉文件的目录信息,可见???

表 4.1. 捕捉文件模式选项

"File "选 项	"Use "Ring buffer multiple with n files"选 files"选项 项		Mode	最终文件命名方式		
-	-	-	Single temporary file	etherXXXXXX (where XXXXXX 是 一个独立值)		
foo.c ap	-	-	Single named file	foo.cap		
foo.c ap	х	-	Multiple files,continu ous	foo_00001_20040205110102.cap, foo_00002_20040205110102.cap,		
foo.c ap	x	x	Multiple files,ring buffer	foo_00001_20040205110102.cap, foo_00002_20040205110102.cap,		

Single temporary file

将会创建并使用一个临时文件(默认选项).捕捉文件结束后,该文件可以由用户指定文件名。

Single named file 使用单独文件,如果你想放到指定目录,选择此模式 Multiple files,continuous 与 single name file 模式类似,不同点在于,当捕捉达到多文件切换临界条件时之一时,会创建一个新文件用于捕捉 Multiple files,ring buffer 与"multiple files continuous"模式类似,不同之处在于,创建的文件数目固定。当达到 ring buffer with n 值时,会替换掉第一 个文件开始捕捉,如此循环往复。 该模式可以限制最大磁盘空间使用量,即使未限制捕捉数据输入,也只能保留最后几个捕捉数据。

### 4.7. 链路层包头类型

在通常情况下,你不需要选择链路层包头类型。下面的段落描述了例外的情况,此时选择包头类型是有必要的,所以你需要知道怎么做:

如果你在某种版本 BSD 操作系统下从某种802.11 设备(无线局域网设备)捕捉数据,可能需要在"802.11"和"Ethernet"中做出选择。"Ethernet"将会导致捕捉到的包带有伪以太网帧头(不知道是不是应该叫伪首部更准确些);"802.11"将会导致他们带有802.11帧头。如果捕捉时的应用程序不支持"802.11帧头",你需要选择"802.11"

如果你使用 Endace DAG card(某种网络监视卡)连接到同步串口线(译者注: E 文为 synchronous serial line,权且翻译作前文 吧,未接触过此卡、未熟稔此线名称),可能会出现"PPP over serial" 或 "Cisco HDLC"(自己 google 去)供选择。根据你自己 的情况选择二者中的一个。

如果你使用 Endace DAG card(同上)连接到 ATM 网络,将会提供"RFC 1483 IP-over-ATM"、"Sun raw ATM"供选择。如果捕捉的通信是 RFC 1483封装 IP(RFC 1483 LLC-encapsulated IP,不翻译为妙),或者需要在不支持 SunATM 帧头的应用程序下捕捉,选择前者。反之选择后者。

如果你在以太网捕捉,将会提供"Ethernet"、"DOCSIS"供选择,如果您是在 Cisco Cable Modem Termination System(CMTS 是思科同轴电缆终端调制解调系统?)下捕捉数据。它会将 DOCSIS(同轴电缆数据服务接口)通信放置到以太网中,供捕捉。此时需要选择"DOCSIS",反之则反之。

### 4.8. 捕捉时过滤

Wireshark 使用 libpcap 过滤语句进行捕捉过滤(what about winpcap?)。在 tcpdump 主页有介绍,但这些只是过于晦涩难懂,所以这里做小幅度讲解。

提示

你可以从 http://wiki.wireshark.org/CaptureFilters 找到捕捉过滤范例.

在 Wireshark 捕捉选项对话(见图 4.2 ""Capture Option/捕捉选项"对话框")框输入捕捉过滤字段。下面的语句有点类似于 tcpdump 捕捉过滤语言。在 tcpdump 主页 <u>http://www.tcpdump.org/tcpdump\_man.html</u>可以看到 tcpdump 表达式选项介绍。 捕捉过滤的形式为:和取值(**and/or**)进行进行基本单元连接,加上可选的,高有限级的 **not**:

[not] **primitive** [and|or [not] **primitive** ...]

例 4.1. 捕捉来自特定主机的 telnet 协议

tcp port 23 and host 10.0.0.5

本例捕捉来自或指向主机10.0.0.5的 Telnet 通信,展示了如何用 and 连接两个基本单元。另外一个例子例 4.2"捕捉所有不是来自10.0.0.5的 telnet 通信"展示如何捕捉所有不是来自10.0.0.5的 telnet 通信。

### 例 4.2. 捕捉所有不是来自10.0.0.5的 telnet 通信

tcp host 23 and not src host 10.0.0.5

此处笔者建议增加更多范例。但是并没有添加。

一个基本单元通常是下面中的一个

[src|dst] host <host>

此基本单元允许你过滤主机 ip 地址或名称。你可以优先指定 src|dst 关键词来指定你关注的是源地址还是目标地址。如果未 指定,则指定的地址出现在源地址或目标地址中的包会被抓取。

ether [src|dst] host <ehost>

此单元允许你过滤主机以太网地址。你可以优先指定关键词 src|dst 在关键词 ether 和 host 之间,来确定你关注的是源地址 还是目标地址。如果未指定,同上。

gateway host<host>

过滤通过指定 host 作为网关的包。这就是指那些以太网源地址或目标地址是 host, 但源 ip 地址和目标 ip 地址都不是 host 的包

[src|dst] net <net $> [{mask < mask >}|{len < len>}]$ 

通过网络号进行过滤。你可以选择优先指定 src|dst 来确定你感兴趣的是源网络还是目标网络。如果两个都没指定。指定网

### 4.8.1. 自动过滤远程通信

### 4.9. 在捕捉过程中

捕捉时,会出现下面的对话框

### 图 4.3. 捕捉信息对话框

Ę	🚹 Wireshark:	Capture f	rom Broadco	. 💶 🗖 🔀	
	Captured Packel	ts			
	Total	148	% of total		
	SCTP	0		0,0%	
	TCP	4		2,7%	
	UDP	102		68,9%	
	ICMP	0		0,0%	
	ARP	24		16,2%	
	OSPF	0		0,0%	
	GRE	0		0,0%	
	NetBIOS	0		0,0%	
	IPX	5		3,4%	
	VINES	0		0,0%	
	Other	13		8,8%	
	Running 00:00:11				
	🤯 Help			Stop	

上述对话框会向你显示捕捉到包的数目,捕捉持续时间。选择的被统计的协议无法更改(什么鸟意思?)

提示

这个对话框可以被隐藏,在前次的捕捉选项对话框设置"Hide capture info dialog box"即可。

### 4.9.1. 停止捕捉

运行中的捕捉线程可以用下列方法停止:

使用捕捉信息对话框上的"Stop"按钮停止。

### 注意

捕捉信息对话框有可能被隐藏,如果你选择了"Hide capture info dialog"

使用菜单项"Capture/ Stop"

使用工具栏项" 🎒 Stop"

使用快捷键:Ctrl+E 如果设置了触发停止的条件,捕捉达到条件时会自动停止。

### 4.9.2. 重新启动捕捉

运行中的捕捉进程可以被重新启动。这将会移出上次捕捉的所有包。如果你捕捉到一些你不感兴趣的包,你不想保留它, 这个功能十分有用。

重新启动是一项方便的功能,类似于停止捕捉后,在很短的时间内立即开始捕捉。以下两种方式可以实现重新启动捕捉:

使用菜单项"Capture/ Restart"

使用工具栏项" 🔐 Restart"

### 第5章 文件输入 / 输出及打印

### 長

<u>5.1. 说明</u> 5.2. 打开捕捉文件 5.2.1. 打开捕捉文件对话框 5.2.2. 输入文件格式 5.3. 保存捕捉包 5.3.1. "save Capture File As/保存文件为"对话框 5.3.2. 输出格式 5.4. 合并捕捉文件 5.4.1. 合并文件对话框 5.5. 文件集合 5.5.1. 文件列表对话框 5.6. 导出数据 5.6.1. "Export as Plain Text File"对话框 5.6.2. "Export as PostScript File" 对话框 5.6.3. "Export as CSV (Comma Separated Values) File"对话框 5.6.4. "Export as PSML File" 对话框 5.6.5. "Export as PDML File" 对话框 5.6.6. "Export selected packet bytes" 对话框 <u>5.6.7. "Export Objects" 对话框</u> 5.7. 打印包 5.7.1. 打印 对话框 5.8. 包范围选项 5.9. 包格式选项

### 5.1. 说明

本章将介绍捕捉数据的输入输出。 打开 / 导入多种格式的捕捉文件 保存 / 导出多种格式的捕捉文件 合并捕捉文件 打印包

### 5.2. 打开捕捉文件

Wireshark 可以读取以前保存的文件。想读取这些文件,只需选择菜单或工具栏的: "File/ **Open**"。Wireshark 将会 弹出 打开文件对话框。详见第 5.2.1 节 "打开捕捉文件对话框"

#### 如果使用拖放功能会更方便

要打开文件,只需要从文件管理器拖动你想要打开的文件到你的 Wireshark 主窗口。但拖

放功能不是在所有平台都支持。

在你载入新文件时,如果你没有保存当前文件,Wireshark 会提示你是否保存,以避免数据丢失。(你可以在首选项禁止提示保存)

除 Wireshark 原生的格式(libpcap 格式,同样被 tcpdump/Windump 和 其他基于 libpcap/WinPcap 使用)外, Wireshark 可以很 好地读取许多捕捉文件格式。支持的格式列表见<u>第 5.2.2 节 "输入文件格式"</u>

### 5.2.1. 打开捕捉文件对话框

打开文件对话框可以用来查找先前保存的文件。表 5.1 "特定环境下的打开文件对话框"显示了一些 Wireshark 打开文件对话框的例子。

#### 对话框的显示方式取决于你的操作系统

对话框的显示方式取决于操作系统,以及GTK+工具集的版本。但不管怎么说,基本功能

都是一样的。

常见对话框行为: 选择文件和目录

点击 Open/OK 按钮,选择你需要的文件并打开它

点击 Cancle 按钮返回 Wireshark 主窗口而不载入任何文件。

Wireshark 对话框标准操作扩展

如果选中文件,可以查看文件预览信息(例如文件大小,包个数。。。)

通过"filter:"按钮、显示字段指定显示过滤器。过滤器将会在打开文件后应用。在输入过滤字符时会进行语法检查。如果输入正确背景色为绿色,如果错误或输入未结束,背景色为绿色。点击 filter 按钮会打开过滤对话框,用于辅助输入显示过滤表达式。(详见<u>第 6.3 节 "浏览时过滤包"</u>)

XXXX-we need a better description of these read filters(貌似说这一段需要更多的做介绍)

通过点击复选框指定那些地址解析会被执行。详见第 7.6 节 "名称解析"

#### 在大文件中节约大量时间

你可以在打开文件后修改显示过滤器,和名称解析设置。但在一些巨大的文件中进行这些操作将会占用大量的时间。在这种情况下建议在打开文件之前就进行相关过滤,解析 设置。

## 表 5.1. 特定环境下的打开文件对话框

### 图 5.1. Windows 下的打开对话框

Wireshark: Open Capture File	
Look in: 🗀 fileset	
Itest1_00001_20050819181503.pcap         Itest1_           Itest1_00002_20050819181505.pcap         Itest1_           Itest1_00003_20050819181505.pcap         Itest1_           Itest1_00004_20050819181506.pcap         Itest1_           Itest1_00005_20050819181507.pcap         Itest1_           Itest1_00006_20050819181507.pcap         Itest1_           Itest1_00006_20050819181507.pcap         Itest1_           Itest1_00006_20050819181507.pcap         Itest1_           Itest1_00006_20050819181507.pcap         Itest1_           Itest1_00004_20050819181507.pcap         Itest1_           Itest1_00004_20050819181507.pcap         Itest1_	Microsoft Windows(GTK2 installed) 此对话框一般都带有一些 wireshark 扩展 此对话框的说明: 如果可用, "help"按钮将会打开本节的用户手册。 "Filter."按钮 在当前版本的 windows 下不可用(我看了- 下,的确不可用,但过滤输入框还是可用的)
Filter:       File         For       For         ✓ MAC name resolution       Siz         ✓ Network name resolution       Par         ✓ Transport name resolution       First Ela	错误提示功能:如果 Wresnark 无法识别选中的捕捉文件 Open 按钮将为灰色不可用□

#### 图 5.2. 新版 GtK 下的打开对话框 Unix/Linux:GTK version >= 2.4

	20000-700-ras	
Effer     Effer     Enable Effect name resolution     Enable getwork name resolution     thable transport name resolution	Planame: Portual: Sider: Podets: Pint Packat: Elapsed tree:	258000-700 Maprias (http: 138685 byte 700 2003-12-09 00:00:32

这是在 Gimp/GNOME 桌面环境下的打开文件对话框

对此对话框的说明。

"+"按钮可以将右侧选中的目录添加到收藏夹。成为预设 目录。

"-" 按钮可以移除左侧目录列表中选中的目录。 ("Home","Desktop","Filesystem"不可以移除)

如果 Wireshark 不能识别选中的捕捉文件, "Open" 按钮将 是灰色不可用。

### 图 5.3. 旧版 GTK 下的打开对话

「日本」			
Wireshark: Open Capture File			
Create Die Delete File Rename File			
	Filmprometer	oubvenion 📖	
Directories ^ - edicari dalbeck/ enrif/ debarn/ Debag, GTRT/ Debag, GTRT/ data/ dat		Here actinolucite m4 actional/flags stiponals_loader ( stiponals_loader ( stiponals_loader ( stiponals_loader ( stiponals) stiponals_loader ( stiponals) stiponals stiponals) stiponals st	<b>Unix/Linux: GTK version &lt; 2.4 / Microsoft Windows</b> (GTK1 installed) gimp/gnome 桌面环境,或 windows gtk1下的的。 该对话框说明 如果未能识别不做文件, Open 按钮将为灰色不可用
Electric 	Filenature Format Size n Packet: First Packet: on Elepted time		

[a] 我测试了一下,无论什么文件,Wireshark都会去尝试打开,更遑论错误检查

### 5.2.2. 输入文件格式

可以打开的捕捉文件格式列表: libpcap, tcpdump and various other tools using tcpdump's capture format Sun snoop and atmsnoop Shomiti/Finisar Surveyor captures Novell LANalyzer captures Microsoft Network Monitor captures AIX's iptrace captures Cinco Networks NetXray captures Network Associates Windows-based Sniffer and Sniffer Pro captures Network General/Network Associates DOS-based Sniffer (compressed or uncompressed) captures AG Group/WildPackets EtherPeek/TokenPeek/AiroPeek/EtherHelp/PacketGrabber captures RADCOM's WAN/LAN Analyzer captures Network Instruments Observer version 9 captures Lucent/Ascend router debug output HP-UX's nettl Toshiba's ISDN routers dump output ISDN4BSD i4btrace utility traces from the EyeSDN USB S0 IPLog format from the Cisco Secure Intrusion Detection System pppd logs (pppdump format) the output from VMS's TCPIPtrace/TCPtrace/UCX\$TRACE utilities

the text output from the DBS Etherwatch VMS utility Visual Networks' Visual UpTime traffic capture the output from CoSine L2 debug the output from Accellent's 5Views LAN agents Endace Measurement Systems' ERF format captures Linux Bluez Bluetooth stack hcidump -w traces Catapult DCT2000 .out files

#### 不正确的包类型可能无法会导致打开错误。

某些类型的捕捉包可能无法读取。以太网环境下捕捉的大部分类型格式一般都等打开。 但有些包类型(如令牌环环包),不是所有的格式都被 wireshark 支持。

### 5.3. 保存捕捉包

你可以通过 File->Save As...菜单保存捕捉文件。在保存时可以选择保存哪些包,以什么格式保存。

保存可能会丢失某些有用的信息

保存可能会少量都是某些信息。例如:已经被丢弃的包会丢失。详见???

### 5.3.1. "save Capture File As/保存文件为"对话框

"Save Capture File As"对话框用于保存当前捕捉数据到文件。???列举了该对话框的一些例子。

#### 对话框的显示方式取决于你的操作系统

对话框的显示方式取决于你的操作系统和 GTK+工具集版本的不同。但大部分基本功能都 是一样的。

#### 表 5.2. 特定环境下的"Save Capture File As"对话框

图 5.4. Windows 下的保存为对话

#### 框

Wireshark: Save file as			
Save jn: 🗀 fileset			
test1_00001_20050819)           test1_00002_20050819)           test1_00003_20050819)           test1_00004_20050819)           test1_00004_20050819)           test1_00005_20050819)           test1_00006_20050819)           test1_00005_20050819)           test1_00005_20050819)           Save as type:           Wireshark./b	81503.pcap (1) 81505.pcap (2) 81505.pcap (2) 81506.pcap (2) 81507.pcap (2) 81507.pcap (2) 81507.pcap (2) 2005081918150 2005081918150	test1_00007_20050 test1_00008_20050 test1_00010_20050 test1_00010_20050 test1_00011_20050 test1_00011_20050 test1_00012_20050 7.pcap p[".pcap,".cap]	Microsoft Windows(GTK2 installed) 此对话框一般都带有一些 wireshark 扩展 此对话框的说明: 如果可用, "help"按钮将会打开本节的用户手册。 如果你未输入文件扩展名-例如.pcap,Wireshark 会自动添 加该文件格式的标准扩展名。
Packet Range			
	<ul> <li>Captured</li> </ul>	<ul> <li>Displayed</li> </ul>	
<ul> <li>All packets</li> </ul>	120		
<ul> <li>Selected packet</li> </ul>	1		
O Marked packets			
<ul> <li>First to last marked</li> </ul>	0		
O Range:	0		

#### Unix/Linux:GTK version >= 2.4

这是在 Gimp/GNOME 桌面环境下的保存文件对话框 "Browse for other flders"前的"+"按钮可以让你指定文件

图 5.5. 新版 GtK 下的保存为对话 对此对话框的说明。 框

保存的位置。。

C Ethereal: S	ave Capture File As		
Name:	1		
Save in <u>f</u> older:	D:1		
Dacket Dange			
Packet Kange	Ca		
<ul> <li><u>All packet</u></li> </ul>	5		
○ <u>S</u> elected ;	packet only		
O From first	to last marked packet		
O Specify a	packet range:		
File type: libpo	ap (tcpdump, Ethereal, etc.)		
₩ Browse for ot	ther folders		
图 5.6. 旧版	GTK 下的保存为对		
	话框		
🔟 Wireshark: Sa	ive Capture File As		
Create Dir	Delete File Rename File		
	C		
<b>E</b>			
Directones	acinclud		
aciocal-fallback\	aclocal-fi airpcap.h		
debian\	arpcap_ airpcap_		
Debug\ Debug_GTK1\	arpcap_ alert_box		
diameter\	aler_box	Univ/Linux: CTK vor	sion $< 2.4$ / Microsoft Windows
	JZ JAOINO	(GTK1 installed)	
Pack	ket Range	gimp/gnome 桌面环境,	或 windows gtk1下的的。
~ /	All packets 1		
÷ 5	- Selected packet only		
\$1	- Marked packets only		
÷1	From first to last marked packet		
\$ S	Specify a packet range:		
File ty	pe: Wireshark/tcpdump/ libpca		
Selection: 🔟 📖	subversion		
	_		

通过这些对话框,你可以执行如下操作: 输入你指定的文件名。 选择保存的目录 选择保存包的范围,见<u>第 5.8 节"包范围选项"</u> 通过点击"File type/文件类型"下拉列表指定保存文件的格式。见??? **可供选中的文件格式可能会没有那么多** 有些类型的捕捉格式可能不可用,这取决于捕捉包的类型。

可以直接保存为另一种格式。

你可以以一种格式读取捕捉文件,保存时使用另外一种格式(这句可能翻译有误。) 点击"Save/OK"按钮保存。如果保存时遇到问题,会出现错误提示。确认那个错误提示以后,你可以重试。 点击"Cancel"按钮退出而不保存捕捉包。

### 5.3.2. 输出格式

可以将 Wireshark 不着的包保存为其原生格式文件(libpcap),也可以保存为其他格式供其他工具进行读取分析。 各文件类型之间的时间戳精度不尽相同

将当前文件保存为其他格式可能会降低时间戳的精度,见第 7.3 节 "时间戳" Wireshark 可以保存为如下格式。 libpcap, tcpdump and various other tools using tcpdump's capture format (\*.pcap,\*.cap,\*.dmp) Accellent 5Views (\*.5vw) HP-UX's nettl (\*.TRC0,\*.TRC1) Microsoft Network Monitor - NetMon (\*.cap) Network Associates Sniffer - DOS (\*.cap,\*.enc,\*.trc,\*fdc,\*.syc) Network Associates Sniffer - Windows (\*.cap) Network Instruments Observer version 9 (\*.bfr) Novell LANalyzer (\*.trl) Sun snoop (\*.snoop,\*.cap) Visual Networks Visual UpTime traffic (\*.\*)

### 5.4. 合并捕捉文件

有时候你需要将多个捕捉文件合并到一起。例如:如果你对多个接口同时进行捕捉,合并就非常有用(Wireshark实际上不 能在同一个实体运行多次捕捉,需要开启多个 Wireshark 实体) 有三种方法可以合并捕捉文件: 从"File"菜单使用, menu item "Merge"(菜单项 "合并"), 打开合并对话框, 见<u>第 5.4.1 节 "合并文件对话框"</u> 使用拖放功能,将多个文件拖放到主窗口。Wireshark 会创建一个临时文件尝试对拖放的文件按时间顺序进行合并。如果你 只拖放一个文件, Wireshark 可能(只是)简单地替换已经打开的文件。 使用 mergecap 工具。该工具是在命令行进行文件合并的。它提供了合并文件的丰富的选项设置。见???

### 5.4.1. 合并文件对话框

通过该对话框可以选择需要合并的文件,并载入合并它们。

首先你会被提示有一个文件未保存

如果当前文件未保存,Wireshark会在启动合并对话框之前提示你是否保存文件。 此处的对话框的大多数内容与"Open Capture Files/打开捕捉文件"对话框类似,参见<u>第 5.2.1 节"打开捕捉文件对话框"</u> 合并对话框中用于合并的控制选项: 将包插入已存在文件前 将选择文件内的包插入到当前已经载入文件之前 按时间顺序合并文件 将当前选择的文件和已载入的文件里的所有包按时间顺序合并 追加包到当前文件 将选择文件的包插入到当前载入文件的末尾 表 5.3. 不同环境下的"Merge Capture File As"对话框

Microsoft Windows(GTK2 installed) 图 5.7. Windows 下的"合并"对话框

此对话框一般都带有一些 wireshark 扩展

Wireshark: Merge with capture fil	
Look jn: 🙆 fileset	~
<pre>test1_00001_20050819181503.pcap test1_00002_20050819181505.pcap test1_00003_20050819181505.pcap test1_00004_20050819181507.pcap test1_00005_20050819181507.pcap test1_00006_20050819181507.pcap test1_00007_20050819181500.pcap</pre>	Atest1_00008_20050819181509,           Atest1_00009_20050819181510.           Atest1_00010_20050819181512.           Atest1_00011_20050819181513.           Atest1_00012_20050819181514.           Atest1_00012_20050819181514.           Atest1_00013_20050819181514.           Atest1_00014_20050819181514.
File name: test1_00007_20050819181	508.pcap
Filter	Filename: test1_00007_2
Prepend packets to existing file     Merge packets chronologically     Append packets to existing file	Format: Wireshark/top Size: 1074 bytes Packets: 11 First Packet: 2005-08-19-18

### 图 5.8. 新版 GtK 下的合并话框

Ethereal: Merge with Captur	e Fil	le l	
Home Oesktop Sei		DA) (all) (main) (manual) (all) Name () (manual) () (concerned) (c	U
Prepend packets to existing file     Marge packets to existing file     Append packets to existing file		Fiename: test.cap Format: libpcap (tcpdump, Bthe Size: 15317 bytes Padiats: 120 First Padiats: 2004-06-22 20:02:48 Elapsed time: 00:00:02	这

### Unix/Linux:GTK version >= 2.4

这是在 Gimp/GNOME 桌面环境下的合并对话框

### 图 5.9. 旧版 GTK 下的合并对话框



### Unix/Linux: GTK version < 2.4 / Microsoft Windows (GTK1 installed)

## 5.5. 文件集合

在进行捕捉时(见: <u>第 4.6 节 "捕捉文件格式、模式设置"</u>)如果设置"Multiple Files/多文件"选项,捕捉数据会分割为多个文件,称为文件集合.

大量文件手动管理十分困难,Wirreshark的文件集合特性可以让文件管理变得方便一点。

### Wireshark 是如何知道一个文件所属的文件集合 t 的?

文件集合中的文件名以前缀号码+"\_"+号码+"\_"+日期时间+后缀的形式生成的。类似于: "test\_00001\_20060420183910.pcap". 文件集合所有的文件都有一个共同的前缀(例如前面的"test")和后缀(例如:".pcap")以及变化的中间部分。

要查找一个文件集合的所有文件。Wireshark 会扫描当前载入文件的目录下的所有文件,找到那些和当前文件名具有相同部分(前缀和后缀)的作为文件集合。

这个简单的机制通常能正常运行,但也有它的弊端。如果几次进行的捕捉具有相同的前缀和后缀,Wireshark会将它们看作同一个文件集合。如果文件被更名或者放在不同的目录下,这样的按文件名查找机制会无法找到文件集合的所有文件。使用"File"菜单项的子菜单"File Set"可以对文件集合集合进行很方便的控制。

List Files 对话框显示一个对话框列出所有被识别出来属于当前文件集合的文件列表。 Next Files 关闭当前文件,打开文件集合列表中的下一个文件。

Previous Files 关闭当前文件,打开文件集合列表中的前一个文件。

### 5.5.1. 文件列表对话框

### 图 5.10. 文件列表对话框

🖉 Wireshark: 17 Files in Set 📃 🗖 🔁						
Filename	Created	Last Modified	Size			
test1_00001_20050819181503.pcap	2005.08.19 18:15:03	2005.08.19 18:15:05	1067 Bytes			
O test1_00002_20050819181505.pcap	2005,08,19 18:15:05	2005,08,19 18:15:05	1108 Bytes			
O test1_00003_20050819181505.pcap	2005,08,19 18:15:05	2005.08.19 18:15:06	1093 Bytes			
O test1_00004_20050819181506.pcap	2005,08,19 18:15:06	2005.08.19 18:15:07	1031 Bytes			
O test1_00005_20050819181507.pcap	2005,08,19 18:15:07	2005.08.19 18:15:07	1070 Bytes			
O test1_00006_20050819181507.pcap	2005,08,19 18:15:07	2005.08.19 18:15:08	1126 Bytes			
O test1_00007_20050819181508.pcap	2005,08,19 18:15:08	2005.08.19 18:15:09	1074 Bytes			
O test1_00008_20050819181509.pcap	2005.08.19 18:15:09	2005.08.19 18:15:10	1037 Bytes			
🔘 test1_00009_20050819181510.pcap	2005,08,19 18:15:10	2005.08.19 18:15:12	1060 Bytes			
🔘 test1_00010_20050819181512.pcap	2005,08,19 18:15:12	2005.08.19 18:15:13	1079 Bytes			
🔘 test1_00011_20050819181513.pcap	2005,08,19 18:15:13	2005.08.19 18:15:14	1029 Bytes			
O test1_00012_20050819181514.pcap	2005.08.19 18:15:14	2005.08.19 18:15:16	1119 Bytes			
🔘 test1_00013_20050819181516.pcap	2005,08,19 18:15:16	2005.08.19 18:15:17	1029 Bytes			
O test1_00014_20050819181517.pcap	2005.08.19 18:15:17	2005.08.19 18:15:18	1085 Bytes			
🔘 test1_00015_20050819181518.pcap	2005.08.19 18:15:18	2005.08.19 18:15:18	1083 Bytes			
🔿 test1_00016_20050819181518.pcap	2005.08.19 18:15:18	2005.08.19 18:15:18	1058 Bytes			
🔘 test1_00017_20050819181518.pcap	2005.08.19 18:15:18	2005.08.19 18:15:18	1386 Bytes			
	n directory: D:/fileset					
			<b>X</b> ⊆lose			

每行包含文件集合中的一个文件的相关信息。

Filename 文件名称。如果你双击文件名称(或者单击单选钮),当前文件会被关闭,同时载入对应的文件。 Created 文件创建时间。 Last Modified 最后一次修改文件的时间。

size 文件的大小。

最后一行"...indirctory:"显示所有文件所在的目录。

在每次捕捉文件被打开、关闭时,对话框的内容会变化。

Close 按钮关闭该对话框。

### 5.6. 导出数据

Wireshark 支持多种方法,多种格式导出包数据,本节描述 Wireshark 常见的导出包数据方法。

注意

个别数据需要使用许多特殊方式导出,在合适的时候我们会对其进行介绍。

XXX - add detailed descriptions of the output formats and some sample output, too./同样需要对导出格式进行介绍,同样也需要一些范例范例

### 5.6.1. "Export as Plain Text File"对话框

导出包数据为"plain Asc II "文本文本见,适合打印包数据。 图 5.11. "Export as Plain Text File"对话框

🕼 Ethereal: Export as "Plain Text" File					
Export to file:					
1					
Packet Range	Packet Format				
	⊆aptured	Displayed	Packet summary line		
⊙ <u>A</u> ll packets	191	191	Packet details:		
Selected packet only	1	1	🔘 All co <u>l</u> lapsed		
O Marked packets only	0	0	<ul> <li>As displayed</li> </ul>		
O From first <u>t</u> o last marked packet	0	0	◯ All e <u>x</u> panded		
Specify a packet <u>range</u> :	0	0	Packet bytes		
			Each packet on a new page		
			<mark>⊘K X ⊆ancel</mark>		

**Export to file:**导出包数据为指定的文件 **Packet Range** 参见<u>第 5.8 节 "包范围选项"</u> **Packet Details** 参见???

#### 5.6.2. "Export as PostScript File" 对话框

导出数据为 PostScript 格式, PostScript 是一种打印格式。

提示

PostScribt 文件可以使用 ghostscrip 转换为 PDF 格式。例如导出文件名为 foo.ps, 然后调用 **ps2pdf foo.ps** 命令就可以进行转换。

#### 图 5.12. "Export as PostScript File" 对话框



Export to file: 导出包数据为指定的文件 Packet Range: 参见<u>第 5.8 节 "包范围选项"</u> Packet Details: 参见???

### 5.6.3. "Export as CSV (Comma Separated Values) File" 对话框

注: 笔者认为此处应该增加截屏,因为我的 xp 下界面与前图风格迥异,这里就不提供了 导出包的摘要为 CVS 格式,可以被电子表格程序使用。 Export to file 导出包数据为指定的文件

#### Packet Range 参见<u>第 5.8 节 "包范围选项"</u>

### 5.6.4. "Export as PSML File" 对话框

导出包数据为 PSML格式,它是一种仅包含包摘要信息的 xml格式。 PSML格式的说明参见: http://www.nbee.org/Docs/NetPDL/PSML.htm.

#### 图 5.13. "Export as PSML File"对话框

C Ethereal: Export as "PSML"	file	
Export to file:		
		6
Packet Range		
	⊆apture	d <u>D</u> isplayed
All packets	191	191
Selected packet only	1	1
O Marked packets only	0	0
<ul> <li>From first to last marked packet</li> </ul>	0	0
Specify a packet range:	0	0
<b>~</b>		🗶 <u>C</u> ancel

Export to file:导出包数据为指定的文件 Packet Range: 参见<u>第 5.8 节 "包范围选项"</u> 上图没有诸如 Packet details 的选项,因为 PSML 文件格式有特殊要求,不包含这些内容。

### 5.6.5. "Export as PDML File" 对话框

导出数据包为 PDML 格式, PDML 是包含包详情的 xml 格式文件。 PDML 文件的说明见:<u>http://www.nbee.org/Docs/NetPDL/PDML.htm</u>

### 注意

PDML 格式还没有发行版, Wireshark 执行 PDML 还处在测试阶段, 期望外来版本会有所 变化。

#### 图 5.14. "Export as PDML File"对话框

C Ethereal: Export as "PDML"	file	
Export to file:		
Packet Range		
	<u>Capture</u>	d Displayed
All packets	191	191
Selected packet only	1	1
Marked packets only	0	0
<ul> <li>From first <u>t</u>o last marked packet</li> </ul>	0	0
Specify a packet range:	0	0
		X Cancel

**Export to file** 将包数据导出到 **Packet Range**: 参见<u>第 5.8 节 "包范围选项"</u> 上述对话框里没有诸如 Packet details 选项,这是由于 PDML 格式约定的内容决定的。

### 5.6.6. "Export selected packet bytes" 对话框

#### 图 5.15. "Export Selected Packet Bytes" 对话框

C Ethereal: E	xport Selected Packet Bytes 📃 🗖 🔀
<u>N</u> ame:	<u> </u>
Save in <u>f</u> older:	Debug_GTK2
Will s	ave 28 bytes of raw binary data to specified file.
<b>I∓</b> <u>B</u> rowse for a	ther folders
	Save X Cancel

Name: 导出数据包为文件 Save in folder:导出数据包到指定目录 Browser for other folders 通过浏览来指定导出数据的目录。

### 5.6.7. "Export Objects" 对话框

这个对话框是用来扫描当前打开包文件或者是正在捕捉中的包文件,将其中的对象,如 HTML 文档,图片文件,可执行文件等等任何可以通过 HTTP 传输的对象进行重组集合,让你可以将他们保存刀磁盘。如果捕捉正在进行中,列表会在发现新对象之后的几秒内立即更新。保存的对象不需要进行额外处理就可以被对应的查看工具打开,或者直接运行(如果它可以在 Wireshark 所在的平台运行的话)。这项功能在 GTK1下的 Wireshark 中无法使用。

### 图 5.16. "Export Objects"对话框

	www.wireshark.org	text/html		www.wireshark.org
	www.wireshark.org	text/css	4243	ws-l.css
	www.wireshark.org			
2488	www.wireshark.org	image/png	26763	front_screen.png
2592	www.wireshark.org			wslogomedblue113.png
2978	www.wireshark.org	image/png	6525	wsiconinst80.png
2987	www.wireshark.org			cg_fade_bg.png
	www.wireshark.org	image/png	296	top_navbar_bg.png
3441	ads. wireshark. org			adlog.php?bannerid=12&clientid=2&zoneid=0&source=front█=0∩
	www.google-analytics.com			&utmac=UA-605389-2&utmcc=utma%3D87653150.554435287.1170449

**各列说明** Packet num 包含该对象数据的包的数目,有时候多个对象可能包含在同一个包里。 Hostname 作为服务器相应 HTTP 请求发送对象的主机的主机名。 Content Type 对象的 HTTP 内容类型 Bytes 对象的字节数 Filename URL 的最后一部分(最后一个"/"之后)。通常这部分是文件名,但有时是一个又常又复杂的字符串,这通常表明该文件是一 个"HTTP POST"请求。(类似于填写表单以后通过 CGI 提交后跳转页面的 URL) 按钮说明: Help 打开本节的用户手册(5.6.7节?) Close 关闭该对话框 Save As 用指定文件名保存当前选择对象。默认文件名是 filename 列中显示的对象文件名。 Save All 将列表中所有对象按 filename 列显示名称保存。系统会提示你选择哪个目录/文件夹保存他们。如果文件名在当前操作系统 或者文件系统下不合法,Wireshark会提示错误,该对象不会被保存(但其他对象会被保存)。

### 5.7. 打印包

要打印包,选择 File 菜单的"Print..."菜单项。这时会弹出如图 5.17" "Print" 对话框"所示的打印对话框。

### 5.7.1. 打印 对话框

#### 图 5.17. "Print" 对话框 🗖 Wireshark: Print Printer 💿 Plain <u>t</u>ext O PostScript d:\ethereal.out Output to file: Browse... Packet Range Packet Format ⊆aptured Displayed 🔽 Packet summary line Packet details: All packets 11 All collapsed Selected packet only 1 As displayed Marked packets only ) From first to last marked packet O All expanded Packet bytes O Specify a packet range: 0 Each packet on a new page 🔯 Help Print 🗶 🖸 ancel

下面的字段在打印对话可用。 Printer 该字段包括一对互斥的单选钮 Print Text 指定包打印为 plain text 格式 PostScript 在打印过程中使用 PostScript 打印软件生成打印输出。[15] Output to file 打印为文件,文件名使用输入的字段或者在浏览按钮选择。 如果你没有选择 Output to file 复选框,你输入字段的地方或 Browse。。按钮都是灰色。 Print command 设置打印时使用的命令

### 注意

打印命令在 Windows 平台不可用。 用于打印的命令通常是 **lpr**. You would change it to specify a particular queue if you need to print to a queue other than the default. 例如: lpr -Pmypostscript 如果没有选中 **Output to file**,该字段将是灰色不可用的。 Packet Range 需要要被打印的包,参见: <u>第 5.8 节 "包范围选项"</u> Packet Format 选择输出文件的格式。你可以选择包以何种方式打印包。见<u>图 5.19 ""Packet Format"选项卡"</u>

<sup>[13]</sup> 译者注:此处需要说明的是,如果没有打印机,或者不想打印,你应该在后面指定 Output to file,指定打印输出未知,另, out put to file 输出的后缀名是.out,如果想用 acrobat 导入,可以考虑将后缀名修改为.ps,这样可以被直接识别,当然,直接把 文件拖放到 Acrobat Distiller 也可以直接生成 PDF 文件。

另:使用 PostScript 输出的文件具有良好的形式,比如在页首会加上列名,而直接打印为 print text 却没有这样的内容。

### 5.9. 包格式选项

包格式选项卡在很多输出对话框都能看到,它可以指定包的那些部分会被输出。

### 图 5.19. "Packet Format"选项卡



 Packet summary line

 导出包的摘要行,就是"Packet List"面板的内容

 Packet Details

 导出 Packet Details 树

 All collaspsed

 "Packet Details"面板在"all collapsed"状态下的所有信息(折叠所有分支)

 As displayed

 "Packet Details"面板当前状态下的信息

 All expanded

 "Packet Details"面板"all expanded"状态下的信息(展开所有分支)

 Packet bytes

 导出包字节,就是"Packet Bytes"面板的内容

 Each Packet on a new page

 输出是每个包单独一页(例如,如果保存/打印成 text 文件,会在包之间加上分节符)

### 第6章处理已经捕捉的包

目录
6.1. 浏览您捕捉的包
6.2. 弹出菜单项
6.2.1. 包列表面板的弹出菜单
6.2.2. 包详情面板的弹出菜单
6.3. 浏览时过滤包
6.4. 建立显示过滤表达式

6.4.1. 显示过滤字段 6.4.2. 比较值 6.4.3. 组合表达式 6.4.4. 常见的错误 6.5. "Filter Expression/过滤表达式"对话框 6.6. 定义,保存过滤器 6.7. 查找包 <u>6.7.1. 查找包对话框</u> <u>6.7.2. "Find Next/查找下一个"命令</u> <u>6.7.3. "Find Previous/查找上一个"命令</u> 6.8. 到指定的包 <u>6.8.1. "GO Back"返回命令</u> 6.8.2. "Go Forward/向前"命令 6.8.3. "Go to Packet/到指定的包"对话框 6.8.4. "Go to Corresponding Packet/到对应的包"命令 6.8.5. "Go to Firest Packet/到第一个包"命令 6.8.6. "Go to Last Packet/到最后一个包"命令 <u>6.9. 标记包</u> 6.10. 时间显示格式及参考时间 <u>6.10.1. 包参考时间</u>

### 6.1. 浏览您捕捉的包

在你已经捕捉完成之后,或者打开先前保存的包文件时,通过点击包列表面版中的包,可以在包详情面板看到关于这个包 树状结构以及字节面版

通过点击左侧"+"标记,你可以展开树状视图的任意部分。你可以在面板点击任意字段来选择它。例如:在下图图 6.1 "Wireshark 选择了一个 TCP 包后的界面"显示的就是选中 TCP 字段。同样可以选择 T C P 包头的应答号(ack:190),同时会 出现在下方的字节浏览面版中。[14]

图 6.1. Wireshark 选择了一个 TCP 包后的界面

🗖 test.pcap - Wireshark		
Eile Edit View Go Capture Analyze Statistics Help		
	3   Q ⇔ ⇔ <del>∞</del> <del>7</del> <del>2</del>	
Eilter:	▼ ♣ Expression	Sear ✔ Apply
No Time Source Destinat	on Protocol Info	
30 1.259654 192.168.0.1 192.16	8.0.2 TCP [TCP Win	dow Update http > 3197
31 1.266628 192.168.0.1 192.16	8.0.2 TCP 1025 > 5	000 [PSH, ACK] Seq=1 Ack=
32 1.266819 192.168.0.2 192.16	8.0.1 TCP 5000 > 1	025 [PSH, ACK] Seq=1 Ack= 📃
34 1.274361 192.168.0.1 192.16	8.0.2 TCP http > 3	197 [PSH, ACK] Seg=1 Ack=
35 1.274447 192.168.0.2 192.16	8.0.1 TCP 3197 > h	ttp [FIN, ACK] Seq=190 Ac
36 1.274987 192.168.0.1 192.16	8.0.2 TCP http > 3	197 [FIN, ACK] Seq=20 Ack
37 1.275018 192.168.0.2 192.16	8.0.1 TCP 3197 > h	ttp [ACK] Seq=191 Ack=21
39 1.281649 192.168.0.1 192.16	8.0.2 TCP FTCP Win	dow Undate] 1025 \$ 5000 [
40 1.282181 192.168.0.1 192.16	8.0.2 TCP 1025 > 5	000 [FIN, ACK] Seq=510 Ac 🗸
		>
🕢 Frame 36 (60 bytes on wire, 60 bytes captured	)	<u>~</u>
Ethernet II, Src: Netgear_2d:75:9a (00:09:5b:	2d:75:9a), Dst: 192.168.0.2 (00:	:0b:5d:20:cd:02)
Internet Protocol, Src: 192.168.0.1 (192.168.	0.1), Dst: 192.168.0.2 (192.168.	.0.2)
🖃 Transmission Control Protocol, Src Port: http	(80), Dst Port: 3197 (3197), Se	eq: 20, Ack: 190, Len: 0 📃
Source port: http (80)		
Destination port: 3197 (3197)		
Sequence number: 20 (relative sequence r	umber)	
Acknowledgement number: 190 (relative ac	k number)	
Header length: 20 bytes		×
<		
0000 00 0b 5d 20 cd 02 00 09 5b 2d 75 9a 08 00 0010 00 28 00 84 00 00 40 06 f8 f8 c0 a8 00 01 0020 00 02 00 50 0c 7d 00 00 68 14 <mark>3c 38 dd 9b</mark> 0030 0c 00 93 ca 00 00 00 00 00 00 00 00	45 00] [-uE. c0 a8 .(@ 50 11P.} h. <mark>≪8</mark> P.	
Acknowledgement number (tcp.ack), 4 bytes	P: 1	120 D: 120 M: 0 .:

在 Wireshark 正在捕捉时, 您也可以进行同样的选择。(前提是您在捕捉选项对话框选择了实时更新列表(update list of packet in real time))

另外,您可以使用分离的窗口浏览单独的数据包,见图 6.2 "在分离窗口浏览包",想要这样做,你只需要在选中包列表面版中您感兴趣的包,菜单 Display->Show Packet in New Windows 。它可以让你很轻松地比较两个或多个包。

### 图 6.2. 在分离窗口浏览包

Л	36 1	.274	987	192	.168	8.0.1	193	2.16	8.0.	2 ТС	Ph	ttp >	31	97 [F	IN, AO	:K] S	eq=2	0 Ack	=19(	) Win	=30	72 Ler	n=0			
E	Fran	1e 36	(60	) by	tes	on v	vire,	60	byt	es c	apt	ured	)													*
Đ	Ethe	rnet	II,	Sr	c: N	etge	ear_2	2d:75	5:9a	(00	:09	:5b:	2d:2	75:9a	), Ds	st: 1	.92.1	68.0.	2 (0	0:0b	:5d:	20:cd	:02)			
Ð	Inte	rnet	Pro	toc	51,	Src	192	2.168	3.0.	1 (1	.92.	168.	0.1)	), Ds	t: 19	92.16	58.0.	2 (19	2.16	8.0.	2)					-
	Thar	ısmi s	sion	i Co	ntro	1 Pr	oto	:01,	Shc	Por	t:	http	(80	D), D	st Po	ort:	3197	(319	7),	Seq:	20,	Ack:	190,	Len:	0	
I	د.			.+.	h+++	. 101	"																		Y	2
<																									>	
00	00	)O Ob	5d	20	cd Q	2 00	) 09	5 b	2d	75 9	9a ()	8 00	45	00	]		. [-u	E.								Τ
00	10 [	0 28	00	84	00 0	0 40	06 (	- f8	f8	c0 a	18 O	0 01	. c0	a8	· (-	@.										
00	20 [	0 02	00	50	0c 7	'd 00	00 (	68	14	3c 3	88 d	ld 9b	50	11		°.}	. h.<	8P.								
00	30 💈	)c 00	93	ca	00 0	0 00	00 (	00	00	00 0	)0															
																		_								

[16] 不甚了解下方的16进制转储怎么表达190的

### 6.2. 弹出菜单项

在包列表面板,包详情面板,包字节面板点击右键,都会出现对应的上下文弹出菜单

### 6.2.1. 包列表面板的弹出菜单

### 图 6.3. 包列表面板弹出菜单

🗖 test.cap - Wireshark							
<u> Edit View Go Capture Analyze Statistics Help</u>							
	Q ⇔ ⇔ ∞ 조 1	L   📃 📑   🔍 🔍 🔍 💌   🗃	4				
<u>Filter:</u>	▼ <u>E</u> xpression <u>C</u> lear <u>/</u>	Apply					
No Time Source Dest	ination Protocol	Info	_ ^				
20 1.250285 192.168.0.2 192	.168.0.1 TCP	3196 > http [FIN, ACK] Seq=256					
	.168.0.2 TCP	http > 3196 [FIN, ACK] Seq=114					
23 1.251868 192.168.0.1 192	.108.0.1 TCP	1025 > 5000 [ACK] Seq=1 Ack=1	w'				
24 1.252826 192.168.0.1 192	Mark Packet (toggle)	http > 3196 [FIN, ACK] Seq=2661	1				
25 1.253323 192.168.0.2 192	Set Time Reference (toggle)	3197 > NTTP [SYN] Seq=0 Len=0 M	MS Ch				
27 1.254532 192.168.0.2 192	Apply as Filter 🔹 🕨	Selected [ACK] Seq=1 Ack=1 V	W"				
	Prepare a Filter	<u>Not Selected</u> /upnp/service/Layer     [ack] seg_1 ack_10(	ni				
30 1.259654 192.168.0.1 192	Conversation Filter	and Selected [ACK] Seq=1 ACK=190 Update http > 3197	7 -				
	Eollow TCP Stream and pot Selected						
Erame 22 (60 butes on wire 60 butes cantu	Follow SSL Stream	or not Selected					
Flame 23 (00 bytes on wrie, 00 bytes capta Fithernet II. Src: Netgear 2d:75:9a (00:09:		20:cd:02 (00:0b:5d:20:cd:02)					
Internet Protocol, Src: 192.168.0.1 (192.1)	Сору	(192.168.0.2)					
Transmission Control Protocol, Src Port: 10	Export Selected Packet Bytes	) (5000), Seq: 1, Ack: 1, Len: 0					
Source port: 1025 (1025)	😪 Decode As						
Destination port: 5000 (5000)	A Print						
Sequence number: 1 (relative sequence	Show Packet in New Window						
Header length: 20 bytes							
	00 45 00 1 5						
0010 00 28 00 7c 00 00 40 06 f9 00 c0 a8 00	00 45 00	····					
0020 00 02 04 01 13 88 00 00 67 81 3c 37 7f	a7 50 10 g. <	7P.					
) File: "D:\Projects\Patchnose\workpackage_dev\wp3_io\docbook\examples	(test.cap" 1 P: 120 D: 120 M: 0		.:				

下表列出了该面版可用弹出菜单项的概述,主菜单能实现同样功能的菜单项,以及简短的描述。

#### 表 6.1. 包列表弹出菜单项

项目	对应主 菜单项	描述
Mark Packet(toggle)	Edit	标记/取消标记包
Set Time Reference(toggle)	Edit	设置/重设时间参考
Apply as Filter	Analyze	用当前选中的项作为过滤显示
Prepare a Filter	Analyze	准备将当前选择项作为过滤器
Conversation Filter	-	将当前选择项的地址信息作为过滤设置。选中该选项以后, 会生成一个显示过滤,用于显示当前包两个地址之间的会 话(不分源目标地址)。(XXX - add a new section describing this better作者似乎建议添加新章节详细描述)
STCP	-	有待补充
Follow TCP Stream	Analyze	浏览两个节点间的一个完整 TCP 流所有数据
Follow SLL Stream	Analyze	同上,将 TCP 替换成 SSL 理解
Copy/Summary(TE XT)	-	将摘要字段复制到剪贴板。(以 tab 分开的文本)
Copy/Summary(CV S)	-	将摘要字段复制到剪贴板,(CVS 格式,逗号分开)
Copy/As Filter Copy/Bytes(Offset	-	以当前选择项,建立一个显示过滤器,复制到剪贴板 以16进制转储格式将包字节复制到剪贴板。

Hex Text)		
Copy/Bytes(Offset		以16进制转储格式将包字节复制到剪贴板。不包括文本部
Text)	-	分。
Copy/ Bytes		
(Printable Text Only)	-	以ASCII 码格式将包字节复制到剪贴板,包括非打印字符。
Copy/ Bytes (HEX Stream)	-	以16进制未分段列表数字方式将包字节复制到剪贴板,(an unpunctuated list of hex digits 应该有专有名词,有兴趣的查一下)
Copy/ Bytes (Binary Stream)	-	以 raw binary 格式将包字节复制到剪贴板。数据在剪贴板 以 "MIME-type application/octet-stream" 存储,该功能在 GTK+1.x 环境下不支持
Export Selected Packet Bytes	File	与文件菜单同名项目功能一样。允许将 Raw packet 字节转换为二进制文件它
Decode As Print	Analyze File	在两个解析之间建立或修改新关联(不知所云) 打印包
Show Packet in New Window	View	在新窗口显示选中的包

### 6.2.2. 包详情面板的弹出菜单

图 6.4. 包详情面板弹出上下文菜单项

🗖 test.cap - Wireshark	
Eile Edit View Go Capture Analyze Statistics Help	
Eilter:	▼ Expression ⊆lear Apply
No Time Source Destination	n Protocol Info
20 1.250285 192.168.0.2 192.168	3.0.1 TCP 3196 > http [FIN, ACK] Seq=256 /
22 1.250810 192.168.0.1 192.168 22 1.250842 192.168.0.2 192.168	3.0.1 TCP 3196 > http [ACK] Seq=114 7
23 1.251868 192.168.0.1 192.168 24 1.252826 192.168.0.1 192.168	8.0.2 TCP 1025 > 5000 [ACK] Seq=1 Ack=1 W1 8.0.2 TCP http > 3196 [FIN. ACK] Seq=26611
25 1.253323 192.168.0.2 192.168 26 1.254502 192.168.0.1 192.168	8.0.1 TCP 3197 > http [SYN] seq=0 Len=0 MS
27 1.254532 192.168.0.2 192.168	3.0.1 TCP 3197 > http [ACK] seq=1 ACK=1 W
28 1.254649 192.168.0.2 192.168 29 1.256388 192.168.0.1 192.168	3.0.1 HTTP UNSUBSCRIBE /upnp/service/Layer: 3.0.2 TCP http > 3197 [ACK] Seq=1 Ack=190
30 1.259654 192.168.0.1 192.168	3.0.2 TCP [TCP window Update] http > 3197 🗸
	>
<ul> <li>Frame 23 (60 bytes on wire, 60 bytes captured)</li> <li>Ethernet II, Src: Netgear_2d:75:9a (00:09:5b:2d</li> <li>Internet Protocol, Src: 192.168.0.1 (192.168.0.)</li> <li>Transmission Control Protocol. Src Port: 1025 (</li> </ul>	d         Expand Subtrees         cd:02 (00:0b:5d:20:cd:02)           .         Expand All         .168.0.2)           Collapse All         00). Seq: 1. Ack: 1. Len: 0
Source port: 1025 (1025)	Сору
Destination port: 5000 (5000) Sequence number: 1 (relative sequence numb	b Export Selected Packet Bytes
Acknowledgement number: 1 (relative ack nu	u Apply as Filter <u>S</u> elected
Header Tength: 20 bytes ∃ Flags: 0x10 (ACK)	Prepare a Filter   Not Selected  Follow TCP Stream  and Selected
Window size: 3072	Follow SSL Stream <u>or</u> Selected
	Wiki Protocol Page     and not Selected     or pot Selected
	Filter Field Reference
1 0000 00 0b 5d 20 cd 02 00 09 5b 2d 75 9a 08 00	Protocol Preferences
0010 00 28 00 7c 00 00 40 06 f9 00 c0 a8 00 01 0020 00 02 04 01 13 88 00 00 67 81 3c 37 7f a7	C C Decode As
0030 0c 00 e7 97 00 00 00 00 00 00 00 00 00	<u>R</u> esolve Name <u>G</u> o to Corresponding Packet
Frame (frame), 60 bytes	P: 120 D: 120 M: 0

下表介绍了包详情列表菜单项的功能描述,及其他可以提供该功能的主菜单

## 表 6.2. 包详情面板弹出上下文菜档项

项目	对应的 主菜单	描述
<b>Expand Subtrees</b>	View	展开当前选择的子树
Expand All	View	展开捕捉文件的所有包的所有子树
Collapse All	View	关闭包中所有已展开的子树
<b>Copy/Description</b>	-	复制选择字段显示的文本到剪贴板
<b>Copy/AS Filter</b>	Edit	将选择项目作为显示过滤内容复制到剪贴板
Copy/Bytes(Offset Hex Text)	-	将包字节以 Hexdump-like 格式存储到剪贴板;类似于包列 表面板中同名的命令,但是拷贝结果仅仅是树分支中被选 中部分(包字节面板中被选中字节)
Copy/Bytes(Offset Hex)	-	以Hexdump-linke 格式保存到剪贴,不包括又本部分。突 似于包列表命令,不同之处在于此处仅拷贝树分支选中部 分(包字节面板选中部分)
COPY/Bytes (printable Text Only)	-	以 ASCII 格式拷贝包字节,非打印字符除外;类似于包列 表面板中同样的命令。不同点在于此处仅拷贝选择的树分 支(包字符被选择部分)
Copy/Bytes(Hex Stream)	-	j 以 unpunctuated list hex digits 形式保存到剪贴板,类似于 包列表面板中的命令,不同之处在于仅复制选中子树部分 (包字节面板选中部分)

Copy/Bytes(Binary Stream)	-	以 raw binary 格式拷贝到剪贴板;类似于包列表面板中的 命令,不同之处在于仅拷贝选中部分子树(包字节面板选中 部分)。数据以 MIME-type"Application/octet-stream"存储在 剪贴板.该功能在 GTK+1.x 下不可用
Export Selected Packet Bytes	File	同文件菜单中的同名项一样。导出 raw packet 字节为二进制文件。
Apply as Filter Preapare a Filter Follow TCP Stream Follow SSL Stream	analyze Analyze Analyze Analyze	将当前选择项作为过滤内容,并应用 将当前选择项作为过滤内容,但不立即应用 追踪两个节点见,被选择包所属 TCP 流的完整数据 同上
 Wiki Protocol Page Filter Field Reference Protocol	-	显示当前选择协议的对应 WIKI 网站协议参考页 显示当前过滤器的 WEB 参考 如果协议字段被选中、点击该选项、打开属性对话框、选
Protocol Preferences  Decode As	- Analyze	如未协议于权极远中,点击该远项,11开腐住对话框,远 择对应协议的页面,???
Resolve Name Go to corresponding Packet	View	对选择的包进行名称解析,不是指所有的包跳到当前选择包的相应包。

TNND,表格让人崩溃

### 6.3. 浏览时过滤包

Wireshark 有两种过滤语法: 一种是捕捉包时使用,另一种是显示包时使用。本节介绍第二种过滤语法: 显示过滤。第一种 过滤语法在<u>第4.8节"捕捉时过滤"</u>提到 显示过滤可以隐藏一些你不感兴趣的包,让你可以集中注意力在你感兴趣的那些包上面。你可以用从以下几个方面选择包: 协议 预设字段 字段值 字段值比较 。。。以及许多 根据协议类型选择数据报,只需要在 **Filter** 框里输入你刚兴趣的协议,然后回车开始过滤。???显示了你输入 tcp 进行过滤 后的图。 **图 6.5. 用 TCP 协议过滤** 

🗖 test	t. pca	up - W	/iresha	rk																		×
<u>F</u> ile [	Edit	⊻iew	<u>G</u> o ⊆	apture	Analy	ze 🕯	5tatistics	Help														
	<b>1</b>	04	<b>8</b>		D	8	×	¢,	_	) [	٩	4	\$	Ŕ	Ŧ	⊉	: [[		•	•	Q	
<u>F</u> ilter:	tcp											•	Ē×p	ression	<u>⊂</u> le	ar <u>é</u>	3pply					
No. +	Т	ïme		Source	э			Dest	inatio	n			Pro	tocol	Info							^
	11 1	.2261	.56	192.3	168.0.	2		192	.168	3.0.3	1		TC	P	3196	> h	ittp	[SYN]	Seq=(	) Len=	⊧O MSS	
	12 1	.2272	282	192.3	168.0.	1		192	.168	3.0.	2		TC	P	http	> 3	196	ESYN,	ACK]	Seq=0	) Ack=	
	13 1		25	192.1	168.0.			192	.168	.0.	1		TC		3196	> h	ittp	[ACK]	Seq=1	L ACK=	=1 Win	
	14 1		100	192.	168.0.	1		192	169	2.0.1	2		- TC		bttp	_KTD	196 /U	EACK1	Seg-1	:/Laye	-756 W	
	16 1	.2324	21	192.	168.0.	1		192	.168	.0.	2		TC	P	TCP	Win	Idow	Updat	el ht		196	
	17 1	.2483	155	192.3	168.0.	1		192	.168	3.0.3	2		TC	Р	1025	> 5	000	[SYN]	Seq=0	) Len=	=O MSS	
	18 1	.2483	91	192.3	168.0.	2		192	.168	3.0.3	1		TC	P	5000	> 1	.025	ĒSYN,	ACK]	Seq=0	) Ack=	
	19 1	. 2501	.71	192.3	168.0.	1		192	.168	3.0.3	2		HT	TP	HTTP/	/1.0	200	OK				
	20 1	. 2502	285	192.3	168.0.	2		192	.168	3.0.	1		TC	P	3196	> h	ittp	[FIN,	ACK]	Seq=2	256 Ac	
	21 1	. 2508	310	192.3	168.0.	1		192	.168	3.0.	2		TC	P	http	> 3	196	LFIN,	ACK]	Seq=1	L14 AC	
	22 1		34Z	192.1	168.0.	2		192	.168	.0.	1		TC	P	3196	> n	ittp	[ACK]	Seq=2	257 AC	1K=115	
	23 1	2510	566	192.	168.0.	1		192	169		2		TC	P	1025	> >	106	[ACK]	Seq=1	Sec-1	•1 W1N 26611	
	24 1	2533	20	192.1	168 0	2		192	168	2 0	1		- TC	r D	3197	÷ h	ttn	ESVNI	Section Section	) Lens	-0 MSS	
	$\frac{25}{26}$ 1	.2545	02	192.1	168.0.	1		192	.168	3.0.1	2		TC	P	httn	5 3	197	ESYN.	ACK1	Sea=0	) Ack=	
	27 1	.2545	32	192.3	168.0.	2		192	.168	3.0.	1		ΤĊ	P	3197	Śĥ	ittp	TACK1	Seg=1	L Ack=	1 Win	V
<																					>	j
🕀 Fra	me 1	1 (6)	2 byte	s on	wire.	62 ł	ovtes d	aptur	ed)													
+ Eth	ierne	t II	. Src:	192.	168.0.	.2 (0	00:0b:5	d:20:	cd:	02).	Dst	: Net	oear	2d:7	5:9a	(00)	:09:5	b:2d:	75:9a	)		
+ Int	erne	t Pro	tocol	. Sec	: 192	168	0.2 (1	92.16	18.0	.21	Dst	: 192	.168	.0.1	(192.	168.	0.1)					
Tra	nem	issio	a Cont	rol P	rotoco	-1 4	Sec Por	+ • 31	96	(310	161	Det P	ort	http	(80)	5001	20.0	) ler				
	LIT SITT	3310	i conc	101 1	. 0 . 0	., .		· · · ·	.50	(51)	<i>,</i> ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	DBC P	0, с.	neep	(00)	, 50	- <b>q</b> . v	, cc,	•••			
0000	00 (	)9 5b	2d 75	9a 0	O Ob	5d ;	20 cd C	2 08	00	45 (	00	[-u		]	.E.							
0010	00	30 18	48 40	00 8	0 06	61 2	2c c0 a	18 00	02	CO (	<u>18</u>	.0.H@		a,	• • •							
0020	00 ( fa 4	JI UC FA 27	- / C 00	50 3	C 36	95 1	F8 00 0 64 01 0	10 00	00	70 (	12		P<6	• • • • •	.p.							
2030	, a	V 2/	20 00	00 0	2 04	05 1	04 OI (	/1 V4	22			•••••	•••		•							
L Files "De		nane"	14 VB 00	.00.02												D.	120 P	102 M	0.[52-4	who Erect		
The: D:	quest.	pcap	14 KD 00	:00:02												JP: .	120 D:	103 14	OLEXD	arci Erro	μŢ	

或许你没有注意到,上图显示的已经仅有 TCP 协议了(从图中可以看到1-10号包已经被隐藏)。因为包的编号是固定不变的,所以第一个包显示的编号是11。

### 注意

当你使用过滤时,所有的包依然保留在捕捉文件里。显示过滤只是更改捕捉文件的显示 方式而非内容。

你只能对 Wireshark 可以识别的协议进行过滤。你也可以对解析器已经添加到树视图的字段进行过滤,但仅限于解析器已 经为字段加上了协议缩写的。在 Add Expression...对话框可以看到可用的字段列表.详见<u>第 6.5 节 ""Filter Expression/过滤</u> 表达式"对话框"

例如: 想要限制包列表面板仅显示来自或指向192.168.0.1的包,可以使用 ip.addr==192.168.0.

注意

点击 Clear 可以移除过滤

### 6.4. 建立显示过滤表达式

Wireshark 提供了简单而强大的过滤语法,你可以用它们建立复杂的过滤表达式。你可以比较包中的值,合并表达式为多个指定表达式。本节介绍了相关操作。

提示

你可以在 Wireshark Wiki Display 页找到发现大量的显示过滤范例。 http://wiki.wireshark.org/DisplayFilters.

### 6.4.1. 显示过滤字段

包详情面板的每个字段都可以作为过滤使用。应用这些作为过滤将会仅显示包含该字段的包。例如:过滤字符串:TCP 将会显示所有包含 TCP 协议的包。

通过"Help/Support Protocals"/帮助/协议支持菜单项访问"Display Filter Fields/显示过滤字段"可以查看完整完整的过滤字段列表。

### 6.4.2. 比较值

你可以通过在许多不同的比较操作建立比较过滤。详见表 6.3 "显示滤镜比较操作符"

提示

你可以使用下表中的英语和比较符(c-link)项达到同样的效果,它们也可以混合使用。

#### 表 6.3. 显示滤镜比较操作符

English	C-linke	描述及范例
22		Equal
eq		ip.addr==10.0.0.5
no	!=	Not equal
ne	:	ip.addr!=10.0.0.5
at		Greate than
gı		frame.pkt_len>10
14	_	Less than
n		frame.pkt_len<128
<u>a</u> 9	>=	Greater than or equal to
ge	/-	frame.pkt_len ge 0x100
le	<=	Equal
	~-	frame.pkt_len <= 0x20

### 6.4.3. 组合表达式

你可以用逻辑操作符将过滤表达式组合在一起使用,见表 6.4 "显示过滤的逻辑操作符"

表 6.4.	显示过	<b>滤</b> 的逻辑操作符
Engli	C-lin	<b>井</b> 法 印英 例
sh	ke	田立です。近ろう
and	&r &r	Logical AND
and	αα	ip.addr==10.0.0.5 and tcp.flags.fin
or	Ш	Logical OR
01	II	ip.addr==10.0.0.5 or ip.addr==192.1.1.1
vor	$\wedge \wedge$	Logical XOR
XOI		tr.dst[0:3] == 0.6.29  xor  tr.src[0:3] == 0.6.29
not	,	Logical Not
not	:	not llc
		Substring Operator
		Wireshark 允许选择一个序列的子序列。在标签后你可以加上一对[]号,在里
		面包含用逗号(是不是冒号?)分离的列表范围。
		eht.src[0:3] == 00:00:83
		上例使用 n:m 格式指定一个范围。在这种情况下,n 是起始位置偏移(0表示
		没有偏移,即是第一位,同理1表示向右偏移一位,便是第二位), m 是从指
		定起始位置的区域长度。
		eth.src[1-2] == 00:83
		上例使用 n-m 格式一个范围。在本例中 n 表示起始位置偏移,m 表示终止位置
[]		偏移
		eth.src[:4]=00:00:83:00
		上例使用:m 格式,表示从起始位置到偏移偏移位置 m。等价于0:m
		eth.src[4:]=20:20
		上例使用 n:格式,表示从最后位置偏移 n 个序列
		eht.src[2] == 83
		上例使用 n 形式指定一个単独的位置。在此例中中序列中的単元已经在偏移
		量 n 中指定。它等价于 n:1
		eth.src[0:3,102,:4,4:,2] == $00:00:83:00:83:00:00:83:00:20:20:83$
		Wireshark 兀计你将多个分亏隔开的列表组合在一起表示复合区域,如上例
		所不

### 6.4.4. 常见的错误

警告

在组合表达式中使用"!="操作符,像eth.addr,ip.addr,tcp.port,udp.port等元素可能会产生非预期效果

经常有人用 ip.addr ==1.2.3.4 表达式来选择所有包含 ip 地址为1.2.3.4的包,

如果有人想用 ip.addr !=1.2.3.4 表达式来排除 ip 地址为1.2.3.4的包,很不幸。它不会像你期待的那样。

相反,那个表达式为真值得条件是源地址或目标地址中的任意一个不等于1.2.3.4即可。因此,那个表达式 **ip.addr !=1.2.3.4** 可 以被读作: "该包包含的 ip 字段值必须不为1.2.3.4"。因为一个 ip 数据报同含源地址和目标地址,只要两个地址有一个不为 1,2,3,4表达式就为真。

接着上面的话题,如果你真想过滤捕捉文件中, ip 地址包含1.2.3.4的包,正确的表达式应该是!(ip.addr==1.2.3.4)。它可以 读作:"显示所有'**字段名为 ip.addr 值存在1.2.3.4**'为非真的包'",换句话说:"筛选所有**字段名 ip.addr 的值中未出现1.2.3.4**的包"

### 6.5. "Filter Expression/过滤表达式"对话框

当你熟悉 Wireshark 过滤系统,并了解你可以用那些标签进行过滤以后,你可以快速简单地输入过滤字符 但如果你是一个 Wireshark 新手,或者处理一些相对陌生的协议,你可能很难通过直接输入字符进行过滤。过滤表达式对 话框会帮你解决这些问题

### 提示

过滤表达式对话框是学习输入表达式的不错的工具。(不知道用不错是不是有点委屈)

### 图 6.6. 过滤表达式对话框

co	resnark: ritter expression			
Fiel	d name		Relation	Value (protocol)
	2dparityfec	^	is present	
Đ	3COMXNS		==	Predefined values:
±	3GPP2 A11		!=	
Ŧ	802.11 MGT		>	
±	802.11 Radiotap		<	
Ŧ	802.3 Slow protocols		>=	
±	9P		<=	
	AAL1		contains	
	AAL3/4		matches	
Đ	AARP			
Ŧ	ACAP			
Đ	ACP133			
Đ	ACSE			
±	ACtrace			
Ŧ	ADP			Range (offset:length)
Ð	AFP	~		
				QK

打开上图的对话框以后。将会显示一个按协议类型分组的树分支列表,一个关系选择框。

Field Name

从协议字段树中选择协议字段。每个可过滤协议都放在第一级。点击+号展开列表,可以获得关于那些协议的可过滤字段。 Relation

从可用关系列表中选择关系。is present 是一元关系,表示如果你选择的字段存在,表达式就为真值。其它关系都为二元关系,需要附加数据(例如:一个值来匹配)来完成。

如果你从字段名列表选择一个字段,并选择一个二元关系(例如等于关系"=="),你可能需要输入值,也有可能是范围信息。 Value

在此输入合适的配置值,输入的值同样要符合你选择的 field name 的属性值类型(例如 字符串).

### Predefined values

有些协议字段包含预设值可用,这一点跟C语言中的枚举变量类似。如果选择的协议有这样的值定义,你可以在此选择。 Range

### 此处作者留空了

OK

如果你已经建立好了表达式,点击 OK 即可创建你的过滤字符串 Cancel 你可以点击 **Cancle** 按钮不做任何修改离开 Add Expression。。。对话框。

### 6.6. 定义,保存过滤器

你可以定义过滤器,并给他们标记以便以后使用。这样可以省去回忆、重新输入某些你曾用过的复杂过滤器的时间。 定义新的过滤器或修改已经存在的过滤器有两种方法:1、在 Capture 菜单选择 **Capture Filters...**;2、在 Analyze 菜单选择 **Display filter...**。Wireshark 将会弹出如图 6.7 ""捕捉过滤器"和"显示过滤器"对话框"所示话框。

#### piay into 注意

因为捕捉和显示滤镜的设定义和保存方式几乎完全一样。所以这里放在一起讲,二者之间的不同点会做标记

警告

你必须用 Save 来保存你的过滤器, OK 或者 Apply 不会保存过滤器。关闭 wireshark 时会 随之消失

### 图 6.7. "捕捉过滤器"和"显示过滤器"对话框

🗖 Wireshark	: Display Filter	
Edit	Filter	
	tpkt_long	
	tpkt_only	
New	ethernet broadcast	
	ip broadcast	
	dcerpc	
	DCERPC Fault	
Delete		
<u> </u>		
Properties		
Filter name: ip	broadcast	
Filter string: ip	.addr == 255.255.255.255	xpression
🔯 Help	QK	X ⊆lose

New

增加一个新的过滤器到列表中。当前输入的 Filter name, Filter string 值将会被使用。如果这些都为空,将会被设置为"new"(是说 filtername 还是说二者都是?)

### Delete

删除选中的过滤器。如果没有过滤器被选中则为灰色 Filter name 修改当前选择的过滤器的名称

### 注意

过滤器名称仅用在此处为了区分方便而已,没有其他用处。你可以将多个过滤器使用同

一个名称,但这样会很不方便

Filter string

修改当前选中过滤器的的内容。仅适用显示过滤: 在输入时进行语法检查。

### Add Expression

仅适用显示过滤:打开增加表达式对话框,辅助创建过滤表达式。详见<u>第 6.5 节 ""Filter Expression/过滤表达式"对话框"</u> OK

仅适用显示过滤:为当前显示应用选择的过滤器,关闭当前对话框。

save

保存当前对话框设置。文件位置和格式见???

Close

### 6.7. 查找包

当你捕捉到一些包以后,或者读取以前存储的包的时候,可以很容易的进行查找。从 Edit 菜单选择 Find Packet...菜单 项.Wireshark 将会弹出图 6.8 ""Find Packet/查找包"对话框"所示对话框.

### 6.7.1. 查找包对话框

### 图 6.8. "Find Packet/查找包"对话框

Wireshark: Fi	ind Packet										
Find By: O Display filter O Hex value O String											
Eilter:											
Search In	String Options	Direction									
🔿 Packet list	Case sensitive	О Цр									
O Packet details	Character set:	⊙ <u>D</u> own									
Packet bytes	ASCII Unicode & Non-Unicode										
	Eind	🗶 Cancel									

首先你需要选择查找方式: Display filter 在 Filter: 输入字段,选择查找方向,点击 OK(过滤器方式) 例如:查找192.168.0.1发起的三步握手建立连接,使用如下字符: ip.addr == 192.168.0.1 and tcp.flags.syn 显示过滤的详情,参见第 6.3 节"浏览时过滤包" Hex Value 在包数据中搜索指定的序列 例如,使用"00:00"查找下一个包含两个空字节的包数据。 String 在包中查找字符串,可以指定多种参数 输入的查找值将会被进行语法检查。如果语法检查无误,输入框背景色会变成绿色,反之则是红色。 你可以指定查找的方向通过: UP 向上查找包列表(包编号递减方式) Down 向下查找包列表(包编号递增方式)

### 6.7.2. "Find Next/查找下一个"命令

适用最后一次的查找设置继续查找

### 6.7.3. "Find Previous/查找上一个"命令

适用最后一次的设置修改查找方向,继续查找。

### 6.8. 到指定的包

通过"Go"菜单可以很轻松跳转到指定的包

### 6.8.1. "GO Back"返回命令

使用 Go back 返回包历史记录,工作方式跟 web 浏览器的页面历史记录类似

### 6.8.2. "Go Forward /向前"命令

### 6.8.3. "Go to Packet/到指定的包"对话框

### 图 6.9. "GO to packet/转到指定包"对话框

🗖 Wireshark:		
Packet number: 1		
🔯 <u>H</u> elp	💫 Jump to	🗶 Cancel

输入包的编号,点击OK,跳转到指定的包(他妈的我怎么看都是 jump to,怎么成了 OK?).

### 6.8.4. "Go to Corresponding Packet/到对应的包"命令

如果被选择协议字段指向文件中的另一个包,该命令将会跳转到那个包。

注意

该协议字段看起来有点像超链接(就像浏览器里的),双击该字段也可以跳转到对应的包。

### 6.8.5. "Go to Firest Packet/到第一个包"命令

跳到第一个包

### 6.8.6. "Go to Last Packet/到最后一个包"命令

跳到最后一个包

### 6.9. 标记包

你可以在包列表面板对包进行标记。被标记的包背景色为黑色,不管原来设置的颜色是怎样的。标记包有助于分析大的包文件时进行查找。

警告

包标记并没有存储在捕捉文件中或任何其他地方,关闭文件后,所有标记将会丢失。 在保存/导出/打印包时,你可以使用包标记控制输出包。标记包以后,可以输出进行区间选择。见<u>第 5.8 节"包范围选项</u>" 对标记包可以进行三项操作 Mark packet(toggle) 冻结以标记的单个包 Mark all packets 标记所有包. Unmark all packets 取消所有标记 这些标记功能出现在"Edit"菜单。"Mark packet(toggle)"功能在弹出包列表面板弹出上下文菜单同样可以找到。

### 6.10. 时间显示格式及参考时间

在捕捉包的过程中,每个包都带有时间戳。时间戳会被保存在捕捉文件中,以备将来分析用。 关于时间戳,时区以及相关的东西的描述介绍,见<u>第 7.3 节"时间戳"</u> 包列表的时间戳格式预设和精度可在浏览菜单选择,见<u>第 3.5 节 ""File"菜单"</u> 可用的预置格式如下: Date and Time of Day: 1970-01-01 01:02:03.123456 包捕捉的绝对日期和时间 Time of Day: 01:02:03.123456 包捕捉的绝对时间 Seconds Since Beginning of Capture: 123.123456 相对与文件开始捕捉的时间或第一个时间参考包的 到这个包之前的时 间。(见<u>第 6.10.1 节"包参考时间"</u>) Seconds Since Previous Captured Packet: 1.123456 相对前一个捕捉包的时间 Seconds Since Previous Displayed Packet: 1.123456 相对前一个显示包的时间(过滤/显示) 可用精度(正如你所致的,数字是以10进制形式的)有: Automatic 使用载入文件格式具有的时间戳精度。(默认选项) Seconds, Deciseconds, Centiseconds, Milliseconds, Microseconds or Nanoseconds 强制使用你指定的精度。如果实际精度比 你指定的低,会在后面自动追加0.如果实际精度比你指定的高。数据会被截尾。 精度距离:如果你有个时间戳,显示时使用:"Seconds Since Previous Packet",:它的值可能是1.123456.默认会采用"Automatic" 精度设置,也就是来自 libpcap 格式文件的固有精度(百万分之一秒)。如果你指定精度为秒,则显示为1,如果你使用。纳 秒(nanoseconds),将会显示为1.123456000.

### 6.10.1. 包参考时间

用户可以为包设置时间参考。时间参考是所有后续包的起算时间。如果你想知道到某一个特定包的时间间隔,会很有用。例如:开始一个新请求。可以在一个包里面设置多个参考时间。

警告

时间参考不能保存到包文件中,关闭文件后就会丢失。

注意

时间参考可能仅仅在时间格式为"Seconds Since Beginning of Capture"模式下比较有用。其

他时间显示形式下可能要么是不能工作,要么是没作用。

要使用时间参考,选择 Edit 菜单下"Time Reference"项中的一个。详见<u>第 3.6 节 ""Edit"菜单"</u>,或者从包列表的右键弹出项选择。

Set Time Refernce(toggle) 切换当前包时间参考状态开关

Find Next 在包列表面板查找下一个时间参考包

Find Previous 在包列表面板查找前一个时间参考包

#### 图 6.10. 时间参考举例

🛾 test. pcap - Wireshark													
<u> Eile Edit View Go Capture Analyze Statist</u>	ics <u>H</u> elp												
	« «» 🖾 🛛 🗢												
Eilter:		<ul> <li>Expression</li> </ul>	n 🏷⊆lear 🖋 <u>A</u> pply										
No Time Source	Destination	Protocol Info		^									
4 1.025659 192.168.0.2	igmp.mcast.net	IGMP V3 Me	mbership Report										
5 1.044366 192.168.0.2	192.168.0.1	DNS Stand	lard query SRV _ldaptcp.nb	9									
6 1.048652 192.168.0.2	239.255.255.250	UDP Sourc	e port: 3193 Destination po	2									
	192.168.0.1	UNS Stand	and query SUA Mb10061d.ww004	4									
9 1.082038 192.168.0.2	192.168.0.255	NBNS Regis	tration NB NB10061D<005	·									
10 *REF* 192.168.0.2	192.168.0.1	DNS Stand	land query A proxycont.ww004										
11 0.114211 192.168.0.2	192.168.0.1	TCP 3196	> http [SYN] Seq=0 Len=0 MS:	s									
12 0.115337 192.168.0.1	192.168.0.2	TCP http	> 3196 [SYN, ACK] Seq=0 Ack										
13 0.115380 192.168.0.2	192.168.0.1	TCP 3196	> http [ACK] Seq=1 Ack=1 Will bether [DSH] ack2 Sec=1 ack	n									
14 0.115506 192.168.0.2	192.168.0.2	TCP 5196	> NTTP [PSH, ACK] SEQ=1 ACK > 3196 [ACK] Seg=1 Ack=256 (										
16 0.120476 192.168.0.1	192.168.0.2	тер Гтер	Window Updatel http > 3196										
17 0.136410 192.168.0.1	192.168.0.2	TCP 1025	> 5000 [SYN] Seq=0 Len=0 MS:	5 🗸									
<													
Identification: 0x1847 (6215)													
🕀 Flags: 0×00													
Fragment offset: O													
Time to live: 128													
Protocol: UDP (0x11)													
Header checksum: 0xa109 [correct]				=									
Source: 192,168.0.2 (192,168.0.2)				-									
Destination: 192.168.0.1 (192.168	.0.1)			~									
		JE.											
0020 00 01 0b d2 00 35 00 35 46 69 00	0 21 01 00 00 015	.5 Fi.!		=									
0030 00 00 00 00 00 00 09 70 72 6f 70	8 79 63 6f 6e 66	.p roxyconf											
	a 65 6e 73 03 6e .ww004	.s iemens.n											
File: "Dultant anne" 14 KB 00:00:00	ec	•	D. 100 D. 100 M. 0										
The: Diftescipcap 14 KB 00:00:02			P: 120 D: 120 M: 0										

作为时间参考的包,在 time 列会有\*REF\*字符串作为标记(见上图第10个包)。所有后续包都会用最后一个时间参考来显示时间。

### 第7章 高级

**目录**7.1. 说明
7.2. "Follow TCP Stream"
7.2.1. "Follow TCP Stream"
7.3. 时间戳
7.3.1. Wireshark 内置

7.3.2. 捕捉文件格式 7.3.3. 准确性 <u>7.4. 时区</u> 7.4.1. 正确设置你的计算机的时区 7.4.2. Wireshark 和时区的关系 7.5. 重组包 7.5.1. 什么是重组包 <u>7.5.2.</u> 如何用 Wireshark 重组包 <u>7.6. 名称解析</u> 7.6.1. 名字解析的流弊 7.6.2. 以太网名字解析(mac 层) 7.6.3. IP 地址解析(网络层) 7.6.4. IPX 名称解析(网络层) 7.6.5. TCP/UDP 端口名解析(传输层) <u>7.7. 校检和</u> 7.7.1. Wireshark 校检和验证 7.7.2. Checksum offloading

### 7.1. 说明

在本节将介绍 Wireshark 的一些高级特性

### 7.2. "Follow TCP Stream"

如果你处理 TCP 协议,想要查看 Tcp 流中的应用层数据,"Following TCP streams"功能将会很有用。如果你项查看 telnet 流中的密码,或者你想尝试弄明白一个数据流。或者你仅仅只需要一个显示过滤来显示某个 TCP 流的包。这些都可以通过 Wireshark 的"Following TCP streams"功能来实现。

在包列表中选择一个你感兴趣的 TCP 包,然后选择 Wireshark 工具栏菜单的"Following TCP Streams"选项(或者使用包列表 鼠标右键的上下文菜单)。然后,Wireshark 就会创建合适的显示过滤器,并弹出一个对话框显示 TCP 流的所有数据。如图 7.1 ""Follow TCP Stream"对话框"所示

注意

值得注意的是: Follow Tcp Stream 会装入一个显示过滤来选择你已经选择的 Tcp 流的所有包。

### 7.2.1. "Follow TCP Stream"对话框

图 7.1. "Follow TCP Stream"对话框

Follow TCP Stream	
<pre>Stream Content SUBSCRIBE /upnp/service/Layer3Forwarding HTTP/1.1 NT: upnp:event Callback: <http: (compatible;="" 0="" 0k="" 1.0="" 1.0;="" 192.168.0.1="" 192.168.0.2:5000="" 200="" 4.0="" 5.1)="" close="" connection:="" content-length:="" host:="" http="" mozilla="" no-cache="" notifys="" nt="" pragma:="" pre="" second="1800" second-1800="" server:="" sid:="" timeout:="" upnp="" upnp-device="Host/1.0" user-agent:="" uuid:cf<="" windows=""></http:></pre>	
Save As Brint Entire conversation (368 bytes)	) Raw
Image: Second secon	; Stream

流的内容出现的顺序同他们在网络中出现的顺序一致。从 A 到 B 的通信标记为红色,从 B 到 A 的通信标记为蓝色。当然,如果你喜欢的话你可以从"Edit/Preferences"菜单项的"Colores"修改颜色。

非打印字符将会被显示为圆点。XXX - What about line wrapping (maximum line length) and CRNL conversions? 在捕捉过程中,TCP 流不能实时更新。想得到最近的内容需要重新打开对话框。 你可以在此对话框执行如下操作: Save As 以当前选择格式保存流数据。 Print 以当前选择格式打印流数据。 Direction 选择流的显示方向("Entire conversation", "data from A to B only" or "data from B to A only"). Filter out this stream 应用一个显示过滤,在显示中排除当前选择的 TCP 流。 Close 关闭当前对话框。移除对当前显示过滤的影响。 你可以用以下格式浏览流数据。 AsCII。在此视图下你可以以 ASCII 凡是查看数据。当然最适合基于 ASCII 的协议用,例如 HTTP. EBCDIC。For the big-iron freaks out there. (不知道这句是什么意思, EBCDIC 是 IBM 公司的字符二进制编码标准。) HEX Dump. 允许你查看所有数据,可能会占用大量屏幕空间。适合显示二进制协议。

CArrays. 允许你将流数据导入你自己的 C 语言程序。

RAW。 允许你载入原始数据到其他应用程序做进一步分析。显示类似与 ASCII 设置。但"save As"将会保存为二进制文件。

### 7.3. 时间戳

时间戳,时间戳的精度,等等是在让人感到困惑。本节将向你介绍介绍 Wireshark 处理时间戳时都发生了什么。 在包被捕捉时,每个包在进入时都被加上时间戳,这个时间戳将会保存在捕捉文件中,所以他们也可以在以后分析时使用。 那么说,时间戳是从哪里来的呢?是捕捉的时候产生的。Wireshark 从 libpcap(WinPcap) libraray(库)中获得时间戳。而 libpcap(winpcap)又是从操作系统内核获得的时间。如果捕捉数据是从捕捉文件载入的,很显然 Wireshark 从文件中获得时 间戳数据。

### 7.3.1. Wireshark 内置

Wireshak 内置的格式使用的时间戳格式由日期(从1.1.1970开始)和时间(从凌晨起,纳秒(10亿分之一秒)为单位)组成。你

可以调整 Wireshark 在包列表的时间戳显示方式。见<u>第 3.7 节 ""View"菜单"</u>的"Time Display Format"项。 当读取或写入捕捉文件时,Wireshark 按需要在内置格式和其他捕捉文件格式间进行时间戳转换。 捕捉时,Wireshark 使用 libpcap(WinPcap)捕捉库(支持纳秒精度)。除非你在专用的捕捉硬件上进行捕捉,一般这样的精度 已经足够了。

### 7.3.2. 捕捉文件格式

Wireshark 支持的捕捉文件格式都带有时间戳。不同的捕捉文件格式的时间戳精度有很大不同,从秒"0"到纳秒 "0.123456789"都有。大多数格式捕捉文件存储的时间戳都是固定精度的,些捕捉文件格式甚至存储了时间戳精度本身(可能是出于方便)。

大多数被 Wireshark(和或多其他工具)使用的 libpcap 捕捉文件格式都仅支持固定的百万分之一固定精度"0.123456" 注意

写入数据到一个实际支持精度比你写入数据精度低的格式文件中,可能会导致数据丢失。

例如:如果你载入一个纳秒精度的捕捉文件,然后将其存储为 libpcap 文件(百万分之一秒

精度)。Wireshark 很明显会将时间精度调整为百万分之一秒。

### 7.3.3. 准确性

经常有人问: "Wireshark 的时间戳的准确性如何? "。实际上, Wireshark 自身不会创建时间戳, 而是通过其他的地方得到时间并显示他们。所以,准确性取决于你实用的捕捉系统(操作系统,性能。。。)。因此以上问题很难通过通常的途径回答。

#### 注意

通常 USB 连接的网络适配器提供的精度非常差。入口的实际上"占用很长的时间和走很曲折的路"才能穿过 USB 数据线到系统内核。而数据包只有被系统内核处理过以后才会打上时间戳,这种时间戳机制将会导致准确性大大降低。 结论:如果你需要精确的时间戳,请不要使用 USB 连接的网卡!(笔者的注脚:有没有网卡在 USB 硬件上提前加上时间戳的?)<sup>[12]</sup>

side bar ceshi

<sup>[12]</sup> 译者注:前文提到,时间戳是 Wireshark 用库获取的时间加在包上的,不知为何有此一问。难道以后要识别硬件是否有时间戳功能。

### 7.4. 时区

当你在各地旅行时,会碰到时区的困扰。如果你从其他时区得到捕捉文件,时区问题会给你带来更大的困扰:-) 首先,下面有两个原因说明你为什么**完全不需要**考虑时区问题:

你仅对两个包的时间戳的差别有兴趣,你并不需要了解捕捉包的实际的日期和时间(通常是这样)。

很可能你不会得到不同与你所在时区的包文件,所以你基本上碰不到时区问题。例如:你的团队的所有都和你工作在一个 时区。

#### 表 7.1.

### 什么是时区?

人们希望时间和日升日落对应。早成应该是6点钟,天黑应该在20:00.这些时间又随着四季变化。如果地球上每个人使用同样的全局时间,将只有一小部分人的日落和时间对应,这将会导致混乱。

因此,人们将地球划分为不同的区域,每个区域都有一个本地时间对应本地的日升日落。 时区基于 UTC(Coordinated Universal Time)或者 Zulu 时间(军事和航空)。旧有的 GTM(格林尼 治时间)已不再使用,因为它有少许误差(与 UTC 相比达到0.9秒)。UTC 起始时区等于0(位于 格林威治,英格兰),所有的时区和它的偏在在-12~+14小时之间!

例如:如果你住在柏林,你的时区将比 UTC 早1小时,所以你的时区应该是"+1"(与 UTC 时间比较的差别,以小时为单位)。柏林的3点和 UTC 的两点钟表示同一个时刻。

有些地区要加以注意,因为那里的时区不是用整小时的。(比如:新德里的时区是 UTC+05:30) 更多相关信息见<u>http://en.wikipedia.org/wiki/time\_zone</u>和 <u>http://en.wikipedia.org/wiki/Coordinated\_Universal\_Time</u>。

### 表 7.2.

什么是时 DST?

Daylight Saving Time(DST),又称为夏令时,目的是在夏天的几个月里"拯救"白天的时间(夏季 白昼较长,如果按照传统的作息时间,比较可惜,不过我不认为)。为了达到这个目的,很多

国家(但不是所有的)增加一个 DST 小时到 UTC 中。所以你还得加个小时(极少数地方甚至 是2小时)的时差来计算你的时区。 不幸的是,DST 并未在全世界范围内被启用。你可能同样注意到,北半球和南半球的夏令时 是刚好相反的(比如:欧洲是夏季时,澳大利亚则是冬季)。 注意:不管 DST 怎样,UTC 在全年都是一致的。 更多相关信息见 <u>http://en.wikipedia.org/wiki/Daylight\_saving</u>.

### 7.4.1. 正确设置你的计算机的时区

7.4.2. Wireshark 和时区的关系

### 7.5. 合并包

### 7.5.1. 什么是合并包

提示

网络协议经常需要传输较大的数据块,在传输时,底层协议可能不支持这样大的数据块(比如网络包大小的限制),或者是 像像 TCP 一样的流数据,TCP 流完全不知道数据分块情况。(原文为:or is stream-based like TCP, which doesn't know data chunks at all.)

在这种情况下,网络协议必须确定数据块分段的边界,并(如果有必要)将数据块分割为多个包。很明显在接受端也需要有 找到数据块分段边界的机制。



在 Wireshark 里面,这个机制/方法被称为**合并/reasembling**,在特定协议的描述可能 不尽相同(例如: desegmentation, defragmentation, ...)

### 7.5.2. 如何用 Wireshark 合并包

对那些可以被 Wireshark 识别的协议, Wireshark 通常处理过程为:查找、解码、显示数据块。Wireshark 会尝试查找数据块 对应的包,在"Packet Bytes"面板的附加页面显示合并以后的数据。(关于"Packet Bytes"面板的详细介绍,见<u>第 4.7 节 ""View"</u> 菜单")

### 图 7.2. 带有合并包附加选项卡 "Packet Bytes 面板"

0000	08	00	06	ab	04	53	08	00	06	6b	7f	bd	08	00	45	00	SkE.	~
0010	01	48	33 41	c7 af	00	00	1e 01	11	dd	51 h4	bc n4	a8 00	08 2e	0a 00	bc 10	a8 00	.H3Q	
0030	ŏŏ	õõ	00	õõ	a0	de	97	6C	d1	11	82	71	õõ	57	80	f0	iq.w	~
			_ C															

Frame (342 bytes) Reassembled DCE/RPC (1604 bytes)



合并可能发生在多个协议层,所以在"Packet Bytes"面板可能会见到多个附加页选项

**注意** 你会

你会在数据块的最后一个包看到合并后的数据。

以 HTTP Get 应答为例:请求数据(例如一个 HTML 页面)返回时。Wireshark 会显示一个16进制转储数据在"Packet Bytes"面板的一个名为"Uncompressed entity body"新选项卡。

默认情况下,首选项中合并功能被设置为允许。在2005年9月之前默认值是不允许。如果你的首选项是在200年9月之前设置的,你得确认一下,合并包选项的设置。合并包对分析网络包作用非常大。

允许和禁止合并包设置对协议来说还有两项要求。

下层的协议(如: TCP)必须支持合并。通常协议支持合并与否都是通过协议的参数设置的。

高层协议协议(如:HTTP)必须使用合并机制来合并分片的数据。这些也同样可以通过协议参数来允许或禁止。 在设置高层协议的时候 tooltip 会提醒你同样需要考虑低层的协议设置。

### 7.6. 名称解析

名字解析尝试将数字地址解析成适合人们阅读格式。有两种方法可以完成这项工作:通过系统/网络服务(例如获取主机名) 和/或 Wireshark 指定的赋值文件。关于通过赋值文件进行解析的详情,可以参见??? 名字解析可以分协议层进行允许,禁止设置。

### 7.6.1. 名字解析的流弊

名字解析在使用 Wireshark 时有重要价值,甚至可以节约大量时间。不幸的是,名字解析也有它自己的缺点。

**名字解析经常会不可用**。服务器可能不知道需要被解析的名字,或者服务器不可用。又或者需要解析的名字在赋值配置文件中找不到。

**名字解析并没有存储在捕捉文件或其他什么地方**。因此你以后打开捕捉文件或者在其他设备上打开文件有可能发现名字解 析不可用。每次打开捕捉文件可能会发现部分地址略微发生变化,也许仅仅是因为无法连接到名字解析服务器(之前还是可 以连接的)

**DNS 可能会增加额外的包到 Wireshark 中**。你会在包文件中看到由 Wireshark 请求 DNS 服务生成的包进出你的机器。 **解析名称被 Wireshark 缓存**。这对设备性能有一定需求。但是,如果名字解析信息在 wireshark 运行时发生变化,wireshark 不会注意到这个变化,因为它是从缓存进行解析的。如果这些信息在 Wireshark 运行时变化了,例如获取一个新 DHCP 租约,Wireshark 不会注意到。(这些是针对 DNS 还是所有信息? 有多少机器使用动态 dns 注册?)



提示

名字解析在包列表填入时已经完成。如果一个包填入包列表以后被解析,包列表的 内容不会立即更改,相反解析结果会被缓存,你可以使用"View/Reload"重建包列表, 来正确显示名字解析结果。但在捕捉过程中这样做没有效果。

### 7.6.2. 以太网名字解析(mac 层)

尝试将 MAC 地址(e.g. 00:09:5b:01:02:03)解析为适合阅读的地址("Human readable")

**ARP 名字解析(系统服务)** Wireshark 会向操作系统发出请求,将以太网地址转换为对应的 IP 地址(e.g. 00:09:5b:01:02:03->192.168.0.1)

**Ethernet codes(ethers file)** 如果 ARP 解析错误, Wireshark 会尝试将以太网地址解析为已知设备名。这种解析需要用户指定 一个 ethers 文件为 mac 地址分配名称。(e.g. 00:09:5b:01:02:03 -> homerouter).

Ethernet manufacturer codes (manuf file) 如果 ARP 解析和 ethers 文件都无法成功解析, Wireshark 会尝试转换 mac 地址的 前三个字节为厂商名的缩写。mac 地址的前三个字节是 IEEE 为各厂商分配的独立地址(通过前三个字节可以得出每个网络 设备的供应商,当然这些也是可以被篡改的。,)(e.g. 00:09:5b:01:02:03 -> Netgear\_01:02:03).

### 7.6.3. IP 地址解析(网络层)

将 IP 地址(e.g. 216.239.37.99)转换为适合阅读的地址/"Human readable"

**DNS/ADNS name resolution(system/library service)**Wireshark 会向操作系统(或 ADSN library 地址-名称解析词典?)请求, 将 IP 地址转换为相关联的主机名(e.g. 216.239.37.99 -> www.l.google.com).此时 DNS 服务正在同步请求 DNS 服务器,所以 Wireshark 会停止相应直到 DNS 请求的响应返回。如果可能的话,你可以考虑使用 ADNS library(这样可以避免等待网络相 应。)



鏊告

如果名称解析服务器不可用,允许网络名称解析使 Wireshark 明显变慢,因为

wireshark 会等待名字解析结果直到超时。在这种情况你应该使用 ADNS。

**DNS vs. ADNS** 这里是一个简短的对比:两个都是用来转换 ip 地址为其他易读的地址"Human readable"(域名)。通常 DNS 用 gethostname()将地址转换为名称。通常首先是查询 hosts 文件(e.g. /etc/hosts,/windows/system32/drivers/etc/hosts)看能否找 到匹配实体。如果找不到,会向指定的 DNS 服务器查询。

DNS 和 ADNS 真正的区别在于等待 DNS 服务器名字解析。gethost()会一直等待知道名字被解析或者返回错误。如果 DNS 服务器不可用,可能会占用很长时间(好几秒)。ADNS 服务会略微有点不同。它也同样向 DNS 服务器发出请求,但不会等 待服务器应答。它会立即相应 Wireshark。此时的地址(和后续地址)在 ADNS 得到结果前不会显示解析名称。如前文书 中说道,解析结果被保存在缓存中,你需要使用"View/Reload"菜单更新这些字段来显示解析名称。

**hosts name resolution(hosts file)** 如果 dns 解析不成功, Wireshark 会尝试使用用户提供的主机文件将 IP 地址转换为对应的 主机名。(e.g. 216.239.37.99 -> www.google.com)

### 7.6.4. IPX 名称解析(网络层)

### ipxnet name resolution (ipxnets file) (笔者未作解释)

### 7.6.5. TCP/UDP 端口名解析(传输层)

翻译 TCP/UDP 端口(e.g.80)为更加易读的玩意"human readable"[15]

**TCP/UDP port conversion (system service)** Wireshark 会向操作系统发出请求,转换 TCP/UDP 端口为已知名称(e.g. 80->http)。 XXX - mention the role of the /etc/services file (but don't forget the files and folders section)!

[15] 应该是指将端口翻译为服务名

7.7. 校检和

很多协议使用校检和来验证数据的完整性/正确性。



应用校检和在这里也被成为 redundancy check(冗余校检?)

### 校检和是做什么的?

提示

校验和是用来验证传输数据或存储数据的数据部分的正确性。一个检验和是数据部分进行摘要计算的出的数字。 网络数据在传输过程中经常会产生错误,例如数据错误,字节重复等。数据接收方可能。

正因为传输过程中会伴随错误,网络协议会经常使用校验和检测这些错误。发送方会对数据进行检验和计算,并将数据和 检验和一起发送。接收方使用同样的方法计算数据部分的校验和,如果收到的校验和计算出来的校验和不匹配,就表示数 据有错误。

有些校验和方法可以通过计算得出发生需要被修复错误的数据位置,并修复(简单的)错误。

如果那些错误无法修复,接收方会丢弃错误的数据包。根据协议的不同,数据丢失会仅仅被丢弃,也有可能发送端会根据 数据丢失情况重传需要的数据包。

使用校验和可以大量减少传输错误数量。但任何检验和算法都无法确保100%检测到所有错误,依然有少量的错误会无法被 检测到。

校验和的算法有很多,例如最经常被使用的检验和算法 CRC32 (循环冗余校验)。特的的网络协议选择的校验算法取决于希望网络媒介达到的出错率上限、错误检测的重要性,处理载入计算的性能,其他方面需要的性能。

关于检验和的更多信息可以参考: http://en.wikipedia.org/wiki/Checksum

### 7.7.1. Wireshark 校检和验证

Wireshark 会对很多协议进行检验和验证,如:TCP、IP。。。

它会和"normal receiver"做一样的计算.然后在包详情面板显示检验和字段的内容, e.g.:[correct], [invalid, must be 0x12345678] 以及其他类似的内容。

如果校验和验证选项被打开或正在进行校验和检测,合并包特性不会被执行。这是为了避免错误的的连接数据扰乱内部数据。

### 7.7.2. Checksum offloading

检验和计算可能由网络网络驱动,协议驱动,甚至是硬件完成。

例如:以太网传输硬件计算以太网循环容易校验,接受硬件验证这个校验。如果接受验证发现错误,Wireshark将不会接收 到这个包,以太网硬件会直接丢弃这个包。

高层校验通常是由协议执行,并将完成后的包转交给硬件。

比较新的网络硬件可以执行一些高级功能,如 IP 检验和计算,这被成为 checksum offloading。网络驱动不会计算校验和,只是简单将校验和字段留空或填入无效信息,交给硬件计算。



注意

Checksum offloading 经常会导致混乱,因为网络包在检验和计算之前转交给

Wireshark。Wireshark 得到包的检验和字段是空的,必然会显示检验和错误,尽管这

个包在从网络硬件发出的时候是带有校验和的。

Checksum offloading 会引起混淆,让你屏幕上看到大量的[invalid]信息,引起你的反感。前面提到过,错误的检验和会导致 包无法合并,更难进行包数据分析。

你可以采取两种方法避免 Checksum offloading 问题

在驱动程序上关闭 checksum offloading 选项,如果可用的话。[16]

通过首选项关闭 Wireshark 上特定协议的校验和验证。

[16] 在 Windows 平台如果驱动支持,应该是计算机管理->设备管理器->网络适配器->对应网卡的属性-高级选项