# 第3章 捕获过滤器技巧

捕获过滤器用于决定将什么样的信息记录在捕获文件中。在使用 Wireshark 捕获数据 时,捕获过滤器是数据经过的第一层过滤器,它用来控制捕获数据的数量。通过设置捕获 过滤器,可以避免产生过大的捕获文件。本章将介绍使用捕获过滤器的技巧。

## 3.1 捕获过滤器简介

使用 Wireshark 的默认设置捕获数据时,会产生大量的冗余信息,导致用户很难找到 自己需要的部分。这时可以使用捕获过滤器来控制捕获数据的数量。捕获过滤器的设置界 面如图 3.1 所示。

📕 Wireshark: Capture Opt	tions					
Capture	1					
Capture Ir	nterface	Link-layer he	ader Prom. Mod	e Snaplen (B) But	ffer [MiB] Cap	ture Filter 🔺
本地连接 2 fe80:c5a2:72ce:4 0.0.0.0	40bb:6005	Ethernet	enabled	default	2	
本地连接 ☑ fe80:40fa:dfed:94 192.168.0.108	4b:f9db	Ethernet	enabled	default	2	
<						•
Capture on all inter Use promiscuous n	faces node on all inter	faces			2 Mana	ge Interfaces
Capture Filter:		(	3	-	Compile se	elected BPFs
Capture Files				Display Options	6	
File: D:\traces\captur	e.pcapng		Browse	<b>☑</b> <u>U</u> pdate list	of packets in	real time
✓ Use <u>m</u> ultiple files		☑ Use pcap-ng	format	✓ Automatica	Ily scroll durin	g live capture
Next file every	100	megabyte(s)	-			
Next file every	10	minute(s)	-	Hide captu	re into dialog	
Ring buffer with	5	files		Name Resolution	7	
Stop capture after	1	file(s)		✓ Resolve M	AC addresses	
Stop Capture Automatica	lly After 🌀	)		Resolve <u>n</u> e	twork-layer na	mes
□ 1 pi	acket(s) negabyte(s) 👻	1		🔽 Resolve <u>t</u> ra	insport-layer r	ame
	ninute(s) 🔻	]		Use <u>e</u> xterna	al network nar	ne resolver
Help					<u>S</u> tart	Close

图 3.1 捕获选项

在该图中,每部分的含义如下所示。

□ Interface 列表:选择一个或多个接口(捕获多个适配器)。

- □ Manage Interfaces 按钮:单击该按钮可以添加或删除接口。
- □ Capture Filter 下拉列表:显示被应用的捕获过滤器(双击可以修改、删除或添加捕获过滤器)。
- □ Capture File(s)选项框:设置保存多个文件、循环缓冲区大小和基于文件数量自动 停止的条件。
- □ Display Options 选项框:设置捕获数据时,自动滚动显示捕获的数据包。
- □ Stop Capture 选项框:设置自动停止条件,如基于包数、数据捕获的数量或运行时间。
- □ Name Resolution 选项框:为 MAC 地址、IP 地址和端口号启动/禁用名称解析。

当以上捕获选项设置完成后,就可以单击 Start 按钮捕获数据了。捕获数据保存时,Wireshark 的图标显示为绿色,如图 3.2 所示。

8	<b>d</b> 0	apturing	from 2	本地连持	妾 (port	53)	[Wire	esharl	k 1.1	0.7 (\	/1.10.7	-0-g6b	931a1 fro	m mas	ter-1.	10)]			_		~
	Eile	Edit 1	/iew g	<u>Go C</u> a	apture	Analy	ze	<u>S</u> tatis	tics	Telep	ohony	Tools	Internals	<u>H</u> elp	)						- (
	0	•		1   8		* :	2	0	4	<b>\$</b> 1	ې 🔇	2		⊕	Q	Q	e	4 🗹	-	36	E.
	<b>X</b> ,		<u>-</u>			bee-t	to_file	ЧÇН.	(sr.e)	A DA	NI~1	-			⊶dr⊸i	- C.,		"tot		Prof	il

图 3.2 Wireshark 运行界面

### 3.2 选择捕获位置

使用 Wireshark 分析网络数据时,首先要确认 Wireshark 捕获数据的正确位置。如果没 有在正确的位置启动 Wireshark,则导致用户可能花费很长的时间处理一些与自己无关的数 据。所以在使用 Wireshark 之前,需要确认它的位置。

如图 3.3 所示,该图代表了一个简单的网络环境。在捕获过程中,可以检测到往返延迟时间、丢包、错误信息及其他主机之间传输的问题。如果在捕获过程中,发现访问网页 速度慢,则说明 Wireshark 捕获工具可能是来自客户端。



图 3.3 捕获工具的位置

当出现以上的情况时,就需要考虑将 Wireshark 捕获工具移动到其他位置。如发现大

量丢包时,可以在路由器或交换机上开启 Wireshark 工具,以确定哪个设备存在大量丢包。

### 3.3 选择捕获接口

在使用 Wireshark 捕获数据前,首先要选择捕获接口。在一台计算机上可能存在多个 网卡,包括有线和无线网卡。Wireshark 可能无法检测到所有的本地接口和远程可用的网络 接口,只能列出可用的网络接口。本节将介绍如何选择捕获接口。

#### 3.3.1 判断哪个适配器上的数据

在工具栏中单击 • 按钮或在菜单栏中依次选择 Capture Interfaces 命令,可以快速地判断哪个接口捕获数据和每个接口连接的网络。捕获接口界面,如图 3.4 所示。

Wireshark: Capture	Interfaces				
Device 回	Description VMware Virtual Ethernet Adapter	IP fe80::ad44:d27f:44bb:8416	Packets 0	Packets/s	Details
<ul> <li>一 過 本地连接 4</li> <li>一 通 本地连接 2</li> </ul>	VMware Virtual Ethernet Adapter Realtek RTL8139/810x Family Ft NIC	fe80::7cf6:f806:deb1:d42a fe80::c5a2:72ce:40bb:6005	5 0	0 0	<u>D</u> etails <u>D</u> etails
🔽 🔊 本地连接	Realtek PCIe GBE Family Controller	fe80::40fa:dfed:94b:f9db	96	1	<u>D</u> etails
<u>H</u> elp		Start Stop	<u>O</u> ptior	IS	<u>C</u> lose

图 3.4 捕获接口

如果主机使用了双协议栈(IPv4 和 IPv6),Wireshark 默认将显示每个适配器的 IPv6 地址。如果存在 IPv4 地址,单击 IPv6 地址将可以看到 IPv4 地址(以本地连接为例),如 图 3.5 所示。

Wireshark: Capture In	nterfaces				
Device	Description	IP	Packets	Packets/s	
📃 🛃 本地连接 3	VMware Virtual Ethernet Adapter	fe80::ad44:d27f:44bb:8416	11	5	Details
🔲 🛃 无线网络连接	Microsoft	fe80::686f:67f8:4c51:d0ec	0	0	Details
📄 🚰 本地连接 4	VMware Virtual Ethernet Adapter	fe80::7cf6:f806:deb1:d42a	23	6	Details
📄 述 本地连接 2	Realtek RTL8139/810x Family Ft NIC	fe80::c5a2:72ce:40bb:6005	0	0	Details
🔽 述 本地连接	Realtek PCIe GBE Family Controller	192.168.0.105	43	7	Details
Help		<u>Start</u> Stop	<u>Option</u>	IS S	<u>C</u> lose

图 3.5 IPv4 地址显示

从该界面可以看到本地连接接口的 IP 由 IPv6 的地址(fe80::40fa:dfed:94b:f9db)变成 了 IPv4 地址(192.168.0.105)。

• 58 •

如果想捕获某个接口上的数据,只需将图 3.4 中设备前面的复选框勾上,然后单击 Start 按钮,将开始捕获该接口上的数据。

#### 3.3.2 使用多适配器捕获

从 Wireshark 1.8 开始,可以同时捕获两个或更多个接口。如果想要同时捕获有线和无 线网络数据,这个功能是有用的。例如,如果用户正试图解决在网络上的 WLAN 客户端的 问题,可以同时捕获客户端的 WLAN 适配器和无线网络,如图 3.6 所示。



图 3.6 同时捕获有线和无线数据

### 3.4 捕获以太网数据

用户可以使用多种方法来捕获以太网上的数据。尽管有多种方法,但并不都是最有效的方法。最有效的捕获方法有3种,分别是直接在主机上捕获数据、映射主机的交换端口和设置一个测试访问点。下面将分别介绍这3种方法。

第1种:直接在主机上捕获数据

如果在主机上安装捕获工具,这可能是最好的选择。这样用户可以不用安装 Wireshark, 使用一个简单的包捕获工具(如 tcpdump)就可以了,如图 3.7 所示。

第2种:端口映射

如图 3.8 所示,该图中的交换机支持端口映射,并且用户有权配置交换机和设置交换 机来复制所有数据到用户交换端口下的 Wireshark 端口。然而,需要注意的一个问题是, 交换机不会向链路层发送错误数据包,所以可以不看性能相关的所有数据。



图 3.7 在主机捕获数据



图 3.8 映射主机的交换端口

第3种:设置一个测试访问点(TAP)

测试访问点是全双工设备,它安装在主机和交换机之间,如图 3.9 所示。默认情况下,测试访问点向前发送所有网络数据,包括链路层错误。尽管测试访问点可能是昂贵的,如 果用户想监听所有流量或来自一个主机的流量,它们可以节约大量的时间。



图 3.9 设置测试访问点

### 3.5 捕获无线数据

使用 Wireshark 捕获无线网络数据,可以帮助用户了解无线网络怎样工作和分析家庭 网络性能慢的原因。如果要捕获无线网络数据,捕获之前需要做些准备工作。例如,确定 无线局域网适配器是否正运行在 Wireshark 上。本节将介绍捕获无线网络数据。

#### 3.5.1 捕获无线网络数据的方式

无线网络数据捕获方式类似于以太网数据捕获,只是端口选择不同。下面简要介绍一下。

【实例 3-1】捕获无线局域网适配器数据。具体操作步骤如下所示。

(1) 在工具栏中依次选择 Capture Interfaces 命令,将显示如图 3.10 所示的界面。

Wireshark: Capture Ir	nterfaces				
Device	Description VMware Virtual Ethernet Adapter Microsoft	IP fe80::ad44:d27f:44bb:8416 fe80::686f:67f8:4c51:d0ec	Packets 1 5	Packets/s 1 4	Details
🔲 🚰 本地连接 4	VMware Virtual Ethernet Adapter	fe80::7cf6:f806:deb1:d42a	1	1	<u>D</u> etails
🔲 🛃 本地连接 2	Realtek RTL8139/810x Family Ft NIC	fe80::c5a2:72ce:40bb:6005	0	0	<u>D</u> etails
🔲 🛃 本地连接	Realtek PCIe GBE Family Controller	fe80::40fa:dfed:94b:f9db	45	8	<u>D</u> etails
<u>H</u> elp		Stop	<u>Option</u>	IS	<u>C</u> lose

图 3.10 捕获接口

(2)从该界面可以看到有一个无线网络适配器,在该界面选择无线网络连接接口的复选框,如图 3.10 所示。然后单击 Start 按钮,开始捕获数据,如图 3.11 所示。

• 60 •

Eile	Edit View Go	Capture Analyze	<u>Statistics</u> Telephony	ools Internals H	elp	
0	• 🖌 🔳 🔬	📄 🛅 🗶 🛃	। 🔍 🗢 🔶 🚡 ।	<u>↓</u>   🗐 🖬   🤆	Ð, Q, Q, 🖭	🏽 🗹 🥵 %   🕱
F	ilter:			- Exp	ression Clear	Apply
No.	Time	Source	Destination	Protocol L	ength Info	
	1 0.000000000	192.168.4.10	5 224.0.0.252	IGMPV2	46 Members	nip Report group 2
	2 0.000116000	192.168.4.10	5 224.0.0.251	IGMPV2	46 Membersh	nip Report group 2
	3 2.167098000	fe80::686f:6	7f8:4(ff02::c	SSDP	208 M-SEARCH	H * HTTP/1.1
	4 0.000547000	fe80::686f:6	7f8:4 ff02::1:ffa3:b	3a6 ICMPv6	86 Neighbor	Solicitation for
	5 0.000042000	fe80::686f:6	7f8:4(ff02::1:ff11:f	390 ICMPv6	86 Neighbor	Solicitation for
	6 0.832238000	fe80::686f:6	7f8:4 ff02::1:ffa3:b	3a6 ICMPv6	86 Neighbor	Solicitation for
	7 0.000065000	fe80::686f:6	7f8:4 ff02::1:ff11:f	390 ICMPv6	86 Neighbor	Solicitation for
	8 1.000204000	fe80::686f:6	7f8:4(ff02::1:ffa3:b)	3a6 ICMPv6	86 Neighbor	Solicitation for
	9 0.000051000	fe80::686f:6	7f8:4.ff02::1:ff11:f	390 ICMPv6	86 Neighbor	Solicitation for
1	0 1.166851000	fe80::686f:6	7f8:4.ff02::c	SSDP	208 M-SEARCH	H * HTTP/1.1
1	1 0.833038000	192.168.4.10	5 239.255.255.25	0 IGMPV2	46 Membersh	nip Report group 2
1	2 0.604083000	192.168.4.10	5 224.0.0.251	MDNS	285 Standard	d query response (
. 1	0 00154000	00.10.76.40.	clied procedurant	400	40 Who had	100 160 4 10 Tol
C			"			•

图 3.11 无线网络数据

(3) 该捕获文件中捕获的数据都是来自无线接口上的数据。

#### 3.5.2 使用 AirPcap 适配器

AirPcap 适配器是专门设计用于捕获所有类型的 WLAN 数据,应用 WLAN 解密密钥, 并添加捕获数据帧的元数据。AirPcap 适配器可以捕获 802.11 控制、管理和数据帧。此外, 这些适配器运行在监听模式(也称为射频监控或 RFMON 模式)下,使适配器捕获所有数 据,而不必结合特定的访问点。这意味着 AirPcap 适配器可以捕获任何 802.11 网络流量, 而不仅仅是一个本地主机接口上的数据。

#### 3.6 处理大数据

在 Wireshark 的默认设置情况下,将会捕获各种协议的数据。当用户分析时,这样的 大数据将会带来很大的困扰。本节将介绍如何处理这些大数据。

#### 3.6.1 捕获过滤器

捕获过滤器是数据经过的第一层过滤器,它用于控制捕捉数据的数量,可以避免产生 过大的捕获文件。这样在使用 Wireshark 捕获之前,就可以通过指定捕获过滤器获取到自 己需要的数据。下面将介绍捕获过滤器的使用。

在菜单栏中依次选择 Capture|Options...命令,打开捕获选项窗口。打开界面,如图 3.12 所示。

pture							-
Capture	Interface	Link-layer hea	der Prom. Mode	Snaplen [B] E	Suffer [MiB]	Capture Filter	
	本地连接 fe80:116:521c:83b5:7a9c 0.0.0.0	Ethernet	enabled	default	2		
	VMware Network Adapter fe80:18d3:3b24:9fc9:9781 192.168.52.1	V Ethernet	enabled	default	2		-
	本地连接 2 fe80:b8f6:ee8a:54fc:b228 192.168.0.104	Ethernet	enabled	default	2		

图 3.12 捕获窗口

在该界面可以看到捕获过滤器列是空白的。这是因为默认情况下没有使用任何的过滤器。此时,双击选择接口行的任何一处,启动编辑接口设置窗口,如图 3.13 所示。

在该界面单击 Capture Filter 按钮,可以查看并选择捕获过滤器。这里选择 port 53,如 图 3.13 所示。从该界面可以看到设置捕获过滤器后,背景颜色为绿色。通过该背景色可以 判断使用的语法是否正确,如果语法错误,则背景为红色;如果正确,背景为绿色。然后 单击 OK 按钮,将显示如图 3.14 所示的界面。

Edit Interface Settings	Capture	e Interface 本地连接 2	Link-layer head	der Prom. Mode	Snaplen [B] E	uffer [MiB]	Capture Filter	
lapture Interface: P address: fe80::40fa:dfed:94b:f9db 192.168.0.108	Captu	ure Interface 本地连接 2	Link-layer head	der Prom. Mode	Snaplen [B] E	uffer [MiB]	Capture Filter	
IP address: fe80::40fa:dfed:94b:f9db		本地连接 2					capta c filler	^
192.100.0.100		0.0.0.0	Ethernet	enabled	default	2		
Link-layer header type: Ethernet		本地连接 fe80::40fa:dfed:94b:f9db 192.168.0.108	Ethernet	enabled	default	2	port 53	ļ
Limit each packet to 65535 bytes Buffer size: 2	< 📃	apture on all interfaces	m			ſ	Manage Interfa	COS.
Capture Filter: port 53 Compile BPF	Vs	se <u>p</u> romiscuous mode on all in	terfaces			Ľ	nanage internat	,es
Help QK Cancel	Capt	ture Filter: port 53				Com	pile selected BP	Fs

图 3.13 编辑接口设置

图 3.14 捕获选项

在该界面的 Capture filter 列可以看到,设置的捕获过滤器为 port 53。Wireshark 捕获过 滤器使用的是伯克利数据包过滤器 (Berkeley Packet Filtering) 语法。用户也可以直接在捕 获过滤器区域,输入捕获过滤器的语法。然后单击 Start 按钮,开始捕获数据。

#### 3.6.2 捕获文件集

文件集就是多个文件的组合。在 Wireshark 中,使用文件集的方法可以将一个大数据 文件分成好几个小文件。在捕获选项窗口中,可以设置每个文件的大小及每隔多长时间保 存一个文件。这样也可以帮助用户快速地处理数据。下面将介绍捕获文件集。

【实例 3-2】 捕获文件集。具体操作步骤如下所示。

(1) 在主菜单栏中单击 (显示捕获选项) 按钮, 将打开如图 3.15 所示的界面。

(2) 在该界面的 Capture 选项框中,选择连接到 Internet 网络适配器前的复选框。这里选择"本地连接"接口。

(3) 在 Capture Files 部分,单击 Browse 按钮选择保存捕获文件的路径和文件名。这里 设置文件名为 capture.pcapng,如图 3.16 所示。然后单击 OK 按钮,将返回到捕获选项 界面。

(4) 在捕获界面的 Capture Files 部分,将看到上面指定的捕获文件的路径和文件名, 如图 3.17 所示。在该界面选择启用 Use multiple files 选项,并定义生成的捕获文件每个大 小为 1MB、每 10 秒生成一个文件及捕获 4 个文件后自动停止捕获。以上信息设置完后, 单击 Start 按钮,开始数据捕获。

▲注意: 捕获选项窗口中的 Stop Capture after 选项,在某些版本中存在 Bug。在 1.10.7 版本中,选择该选项后,将无法发挥它的作用。

(5) 现在通过访问 www.openoffice.org 网站,产生流量。大概访问几秒,然后返回到

• 62 •

Wireshark 查看状态栏的文件区域。将会看到文件名发送了变化,文件名后面添加了文件编号(本例中是\_00004)、时间和时间戳,如图 3.18 所示。

Wireshark: Capture Options							
Capture							
Capture Interface 192.168.41.1	Link-layer header Prom. Mo	ode Snaplen (B) Buffer (MiB) Cap	ture Filter				
本地连接 2 fe80::c5a2:72ce:40bb:6005 0.0.0.0	Ethernet enabled	d default 2					
本地连接 ☑ fe80:40fa:dfed.94b:f9db 192.168.0.105	Ethernet enabled	d default 2	H I				
•	m						
Capture on all interfaces		Manag	ge Interfaces				
Use promiscuous mode on all interfa	aces						
Capture Filter:		- Compile se	elected BPFs				
apture Hies		Display Options					
File:	<u>B</u> rowse	Update list of packets in	real time	📕 Wireshark: Sp	pecify a Cap	ture File	ł
Use <u>m</u> ultiple files	✓ Use pcap-ng format	Automatically scroll durin	g live capture				
✓ Next file every 1 *	megabyte(s) 👻			<u>N</u> ame:	caputer.	pcapng	
Next file every	minute(s) 👻	✓ Hide capture info dialog		Save in folder:	traces		Create Fo
Ring buffer with 2	fles	Name Resolution		Save in Torger.			
Stop capture after 1	file(s)	Resolve MAC addresses		D			A 10 10 1
Stop Capture Automatically After		Resolve <u>n</u> etwork-layer na	mes	Recently Us	sed	http.pcapng	- Modified 星期三
1         v         packet(s)           1         v         megabyte(s)         v		✓ Resolve transport-layer n	ame	🖻 Administrat	tor +	http-error.pcapng tcp.pcapng	星期五 2012/10/2
1 minute(s) v		Use <u>e</u> xternal network nar	ne resolver				
Help		Start	Close				<u>O</u> K <u>C</u> ance

图 3.15 捕获选项界面



/ Wiror	thark Capture Opt	tions			
Villes	shark: Capture Opt	uons			
Captur	e Files				Display Options
File:	D:\traces\Captur	re.pcapng		Browse	☑ Update list of packets in real time
V U	Jse <u>m</u> ultiple files			✓ Use pcap-ng format	Automatically scroll during live capture
<b>V</b> N	lext file every	1	* *	megabyte(s) 💌	
▼ Next file every 10				second(s)	☑ <u>H</u> ide capture info dialog
🕅 R	ling buffer with	2	×	files	Name Resolution
V S	top capture after	4	*	file(s)	☑ Resolve <u>M</u> AC addresses
Stop C	Capture Automatica	lly After			Resolve network-layer names
	1 × p	acket(s)			
$\checkmark$	1 × n	megabyte(s)	Ŧ		☑ Resolve <u>t</u> ransport-layer name
	1 minute(s) v		Ŧ		☑ Use <u>e</u> xternal network name resolver
He	elp				<u>Start</u>

图 3.17 设置文件集

	Ca	pture	_00004	4_201	407011	82455	i.pcapr	ng [Wires	hark 1.8.	15 (vi	1.8.15	-0-g50a18	2c fror	n maste	er-1.8)	1			×
	ile	Edit	View	<u>G</u> o	<u>Captu</u>	re <u>A</u> r	nalyze	Statistics	Teleph	ony	<u>T</u> ools	Internals	<u>H</u> elp						
		<b>.</b>	M 🕅				1	$\mathbb{B} \mid \mathbb{Q}$	\\$ \$	· 🍛	<b>T</b> :	⊈   🗐		€ Θ		•	<b>¥</b>	¥ !	<u> </u>
Ų	Filter			-	~	-	~	~	-	-	-	Expre	ssion	Clear	Арр	olv Sa	ve	5	5
C	) 🕑	File:	"D:\tra	aces\0	Capture	0000	4_2014	07011824	55.pcapn	g" 89.	. P	ackets: 36 I	Display	e P	rofile:	Default	t		

图 3.18 文件名变化

(6) 用户也可以通过在工具栏中依次选择 File|File Set|List Files 命令, 查看文件集中的 所有文件, 如图 3.19 所示。

Wireshark: 4 Files in Set			
Filename	Created	Last Modified	Size
Capture_00001_20140701182425.pcapng	2014.07.01 18:24:25	2014.07.01 18:24:35	52344 Bytes
© Capture_00002_20140701182435.pcapng	2014.07.01 18:24:35	2014.07.01 18:24:45	13976 Bytes
Capture_00003_20140701182445.pcapng	2014.07.01 18:24:45	2014.07.01 18:24:55	5916 Bytes
Capture_00004_20140701182455.pcapng	2014.07.01 18:24:55	2014.07.01 18:25:05	8960 Bytes
in (	directory: D:\traces		
Help		(	<u>C</u> lose

图 3.19 文件集

(7)从该界面可以看到生成的4个小文件。

### 3.7 处理随机发生的问题

在捕获数据时,用户可能会遇到一些特殊的问题。但是这些问题,并不是在每次捕获 数据时都可以捕获到。所以,这些随机发生的问题常常给用户带来一定的困扰。在 Wireshark 中有一些特殊的功能,可以捕获到这些烦人的、难以捉摸的数据包。本节将介绍处理这些 随机发生的问题。

在 Wireshark 中可以通过设置使用文件集,并且使用循环缓冲区的功能来处理随机发生的问题。设置该功能后,Wireshark 会持续地捕获数据,直到问题再次出现。下面介绍设置循环缓冲区的方法。

在菜单栏中依次选择 Capture|Options 命令,打开捕获选项窗口。在该界面即可设置缓冲区文件,如图 3.20 所示。

Wireshark: Capture Opti	ons				
Capture					
Capture In	terface	Link-layer he	eader Prom. Mo	de Snaplen [B] Buff	er [MiB] Capture Filter 🔺
本地连接 2 fe80:c5a2:72ce:44 0.0.0.0	066.6005	Ethernet	enabled	l d <del>e</del> fault	2
本地连接 「e80:40fa:dfed:94 192.168.0.108	b:f9db	Ethernet	enabled	default	2
< [					Þ
Capture on all interf	aces ode on all inte	rfaces			Manage Interfaces
⊆apture Filter:				•	Compile selected BPFs
apture Files				Display Options	
File: D:\traces\roamin	gprob.pcapng		Browse	☑ Update list of	of packets in real time
Use <u>m</u> ultiple files		💟 Use pcap ng	g format	Automatical	y scroll during live capture
Next file every	100 🗘	megabyte(s)	-		
Next file every	10	minute(s)	Ŧ	☑ <u>H</u> ide capture	e info dialog
Ring buffer with	5	files		Name Resolution	
Stop capture after	1	file(s)		Resolve MA	C addresses
top Capture Automatical	y After			Resolve <u>n</u> etv	vork-layer names
1 × pa	cket(s)	-		✓ Resolve tran	sport-layer name
√ 100 m	egabyte(s) 🔻				network name recolver
m	inute(s)			Se <u>e</u> xternal	network name resolver
Help					<u>Start</u> <u>C</u> lose

图 3.20 设置缓冲区

以上的设置表示当 Wireshark 完成捕获第 5 个 100MB 的文件后,将删除第一个 100MB 的文件,并创建第 6 个文件,使 Wireshark 继续运行。

【实例 3-3】 使用设置循环缓冲区的方法节约磁盘空间。具体操作步骤如下所示。

(1) 在主菜单栏中单击 (显示捕获选项) 按钮。

(2) 在该界面的 Capture 部分,选择连接到 Internet 网络适配器前的复选框。这里选择 "本地连接"接口。

(3) 在 Capture Files 部分,单击 Browse 按钮选择保存捕获文件的路径和文件名。这里 设置文件名为 capturese.pcapng,如图 3.16 所示。然后单击 OK 按钮,将返回到捕获选项 界面。

(4) 在捕获界面的 Capture Files 部分,将看到上面指定的捕获文件的路径和文件名。 在该界面选择启用 Use multiple files 选项,设置生成文件集中的每个文件大小为 10MB、每 30 秒生成一个文件、缓冲区最多保存 3 个文件,如图 3.21 所示。以上信息设置完后,单 击 Start 按钮,将开始数据捕获。

📕 Wires	hark: Capture Opt	tions		
Capture	e Files			Display Options
File:	D:\traces\stopat	problem.pcapng	<u>B</u> rowse	☑ Update list of packets in real time
<b>V</b> U	se <u>m</u> ultiple files		✓ Use pcap-ng format	Automatically scroll during live capture
V N	ext file every	10	megabyte(s)	
V N	ext file every	30	second(s)	☑ <u>H</u> ide capture info dialog
🗸 Ri	ing buffer with	3	files	Name Resolution
🗖 St	op capture after	2	file(s)	☑ Resolve MAC addresses
Stop Ca	apture Automatica	lly After		Resolve network-layer names
	1 × p	acket(s)		Parahya transport layar nama
7	40 × k	cilobyte(s) 👻		V Resolve transport-layer name
	1 × n	ninute(s) 🔍		✓ Use <u>e</u> xternal network name resolver
He	lp			<u>Start</u> <u>Close</u>

图 3.21 捕获选项

(5)此时打开浏览器,访问 www.wireshark.org 网站产生流量。大概访问 30 秒该网站。 然后再访问一下 www.chappellu.com/nothere.html 网站,将会出现 404 错误,因为该网站不 存在。当出现 404 错误后,快速返回到 Wireshark 界面,单击■(停止捕获)按钮。

(6) 查看 Wireshark 状态栏的文件区域,将看到许多文件编号已经被分配。当查看保存捕获文件目录或查看文件集时,仅能看到3个文件,如图3.22所示。因为在前面的循环缓存区设置了仅保存最后3个文件。

Wireshark: 3 Files in Set			
Filename	Created	Last Modified	Size
stopatproblem_00002_20140701152912.pcapng	2014-07-01 15:29:12	2014-07-01 15:29:42	33024 Bytes
stopatproblem_00003_20140701152942.pcapng	2014-07-01 15:29:42	2014-07-01 15:30:12	21148 Bytes
stopatproblem_00004_20140701153012.pcapng	2014-07-01 15:30:12	2014-07-01 15:30:26	18732 Bytes
, in direc	ctory: D:\traces		
Help		[	<u>C</u> lose

图 3.22 文件集

(7)在该界面从文件名的编号(\_00002、\_00003、\_00004)可以看出目前保存的3个文件。由于缓存文件设置仅能保存3个文件,所以第1个文件(编号为\_00001)被删除了。这样就可以节约磁盘空间。现在单击 Close 按钮,返回到 Wireshark 主界面。将能够快速地找出 404 的错误信息,如图 3.23 所示。

📕 sto	patproblem_0	0004_20140701153012.p	capng [Wireshark 1.1	0.7 (v1.10.7-	0-g6b931a1 from master 🗖 🗖 🗙
Eile	Edit View (	o <u>C</u> apture <u>A</u> nalyze <u>S</u>	tatistics Telephony	ools Intern	als <u>H</u> elp
0	ءَ 📕 🗴	(   🖻 🗟 🗙 🔁	् 🗢 🛸 🍛 🚡	⊻   🔳 🗉	3] ( Q, Q, 🖭   🎬 🗹 🐔 🛛 »
Filter	:			▼ Exp	pression Clear Apply Save
No.	Time	Source	Destination	Protocol L	ength Info
33	2.8902860	00 192.168.0.104	123.125.125.86	тср	54 11882 > http [ACK] Seq=119
34	2.8928530	00 192.168.0.104	123.125.125.86	HTTP	703 POST /q HTTP/1.1
35	2.8928760	00 192.168.0.104	123.125.125.86	HTTP	601 Continuation or non-HTTP 1
36	5 2.9041570	00 123.125.125.86	192.168.0.104	TCP	60 http > 11882 [ACK] Seq=20!
37	2.9194640	00 Giga-Byt_Ob:00	:4 Broadcast	ARP	60 who has 192.168.0.111? TO
38	2.9196990	00 fe80::1914:a44	0:ff02::1:ffbc:1	CICMPV6	86 Neighbor Solicitation for
39	2.9272440	00 123.125.125.86	192.168.0.104	HTTP	394 HTTP/1.1 404 Not Found (1
40	2.9272700	00 192.168.0.104	123.125.125.86	TCP	54 11882 > http [ACK] Seq=23
41	3.6747960	00 fe80::1914:a44	0:ff02::1:2	DHCPv6	147 Solicit XID: 0x7bf798 CID
42	3.9197880	00 Giga-Byt_Ob:00	:4 Broadcast	ARP	60 who has 192.168.0.111? To
43	4.3108060	00 Giga-Byt_9d:e7	:4 Broadcast	ARP	60 who has 192.168.0.104? To
44	4.3108290	00 Giga-Byt_c8:4c	:8Giga-Byt_9d:e7	ARP	42 192.168.0.104 is at 1c:6f
4	1 2110260	102 100 0 2	102 100 0 104		A 1997 Complete State 1
0 🕅	File: "D:\trace	s\stopatproblem_00004_2	2014 Packets: 89 · C	isplayed: 89	(100.0%) Profile: Default

图 3.23 404 错误信息

(8)从该界面可以看到, 39帧中的数据中包含 404 Not Found 信息。

### 3.8 捕获基于 MAC/IP 地址数据

在使用 Wireshark 捕获过滤器时,可以设置只捕获 MAC/IP 地址数据的过滤器。本节 将介绍捕获基于 MAC/IP 地址数据的方法。

#### 3.8.1 捕获单个 IP 地址数据

IP 地址是 IP 协议提供的一种统一的地址格式,它为互联网上的每一个网络和每一台 主机分配了一个逻辑地址。通常 IP 地址分为 IPv4 和 IPv6 两大类。现在大部分使用的都是 IPv4 地址,该地址是一个 32 位的二进制数。通常在捕获数据时,用户会通过 IP 地址的方 式来判断是哪台主机上的数据。下面将介绍捕获单个 IP 地址数据的方法。

下面看几个 IP 地址捕获过滤器的例子。

- □ host 10.3.1.1: 捕获到达/来自 10.3.1.1 主机的数据。
- □ host 2406:da00:ff00::6b16:f02d: 捕获到达/来自 IPv6 地址 2406:da00:ff00::6b16:f02d 的数据。
- □ not host 10.3.1.1: 捕获除了到达/来自 10.3.1.1 主机的所有数据。
- □ src host 10.3.1.1: 捕获来自 10.3.1.1 主机上的数据。
- □ dst host 10.3.1.1: 捕获到达 10.3.1.1 主机上的数据。
- □ host 10.3.1.1 or host 10.3.1.2: 捕获到达/来自 10.3.1.1 主机上的数据,和到达/来自 10.3.1.2 主机的数据。

• 66 •

□ host www.espn.com: 捕获解析 www.espn.com 的 IP 地址上的数据。

【实例 3-4】 仅捕获到达/来自 192.168.0.112 主机的数据包。具体操作步骤如下所示。 (1) 在工具栏中单击 ⑥按钮,打开捕获选项界面,如图 3.24 所示。

pture							
Capture	Interface	Link-layer hea	der Prom. Mode	Snaplen [B] E	uffer [MiB]	Capture Filter	
	<b>本地连接 2</b> fe80::c5a2:72ce:40bb:6005 0.0.0.0	Ethernet	enabled	default	2		[
	<b>本地连接</b> fe80:40fa:dfed:94b:f9db 192.168.0.108	Ethernet	enabled	default	2		

图 3.24 捕获选项

(2)在该界面的捕获区域,选择捕获数据的接口(本地连接)的复选框。在这个捕获 区域双击选择接口行的任何一处,启动编辑接口设置窗口,如图 3.25 所示。

📕 Edit Interfa	ce Settings
Capture	
Interface:	<b>本地连接</b>
IP address:	fe80::40fa:dfed:94b:f9db
	192.168.0.108
Link-layer he	ader type: Ethernet 💌
Capture	packets in promiscuous mode
🔲 Limit eac	h packet to 65535
Buffer size: 2	mebibyte(s)
Capture File	ter: host 192.168.0.112   Compile BPF
<u>H</u> elp	<u>O</u> K <u>C</u> ancel

图 3.25 编辑接口设置

(3) 从该界面可以看到本地连接接口的 IP 地址,此时就可以根据该地址信息创建相应的捕获过滤器。在该界面的捕获过滤器区域,输入 host x.x.x.x (x.x.x 表示指定捕获的 IP 地址,本例中使用的地址是 192.168.0.112)来过滤 IPv4 地址的数据。如果捕获 IPv6 地址的话,则输入 host xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx. 然后单击 OK 按钮,将看到如图 3.26 所示的界面。

Capture	Interface	Link-layer bea	der Prom. Mode	Snaplen (B) F	luffer (Mil	31 Capture Filter	
本地 了 fe80- 192.1	连接 40fa:dfed:94b:f9db 68.0.108	Ethernet	enabled	default	2	host 192.168.0.112	1
Capture o	n all interfaces					Manage Interfac	es
✓ Use prom Capture Filte	iscuous mode on all in host 192.168.0.112	terfaces			-	Compile selected BP	Fs

图 3.26 捕获过滤器

(4) 从该界面可以看到,本地连接接口的捕获过滤器中显示了一条信息。在该界面不要启动 Use multiple files,此时就可以捕获数据了。单击 Start 按钮,将开始捕获过程,如 图 3.27 所示。

	*本	地连	接 (hos	t 192.	168.0.1	12)	[Wi	iresha	rk 1.1(	0.7	(v1.1	.0.7-0-	g6b93	31a1 fro	om n	naster-	1.10)]		l			x
E	ile	<u>E</u> dit	View	<u>G</u> o	<u>C</u> aptu	ire	<u>A</u> nał	yze ş	<u>S</u> tatist	ics	Tele	ephony	Too	ols Int	ernal	s <u>H</u> elp	)					
		٤ (	( III	6		a10	×	2	0	\$	\$	ې 💫	F 2		] 🖬	) Đ		0	3   6	4	2 🖪	>>
	Filt	er:													•	Expres	ssion	C	lear			**
No	<b>D</b> .	Time	•		Source	е			D	estir	natio	n		Protoc	ol L	ength	Info					~
	1	0.0	00000	0000	192.	168.	0.1	112	1	92.	168	.0.1		DNS		77	Stan	ndard	que	ry (	0x9a11	1
	2	0.0	00114	000	192.	168.	0.1	112	1	92.	168	.0.1		DNS		77	Stan	ndar d	que	ry (	0xc71	e
	3	1.0	21917	000	192.	168.	.0.1	L	1	92.	168	.0.11	.2	DNS		93	Stan	ndard	que	ry i	respoi	ns
	4	0.0	12027	000	192.	168.	0.1	L	1	92.	168	.0.11	.2	DNS		146	Stan	ndard	que	ry i	espor	ns
	5	0.0	00412	2000	192.	168.	.0.1	112	1	98.	66.	239.1	46	TCP		74	6024	7 >	http	[S	YN] S	eq
	6	0.2	50239	000	192.	168.	.0.1	112	1	92.	168	.0.1		DNS		77	Stan	ndar d	que	ry (	0x3724	4
	7	0.4	43976	5000	192.	168.	.0.1	L	1	92.	168	.0.11	.2	DNS		93	Stan	ndard	que	ry i	respoi	ns
	8	0.0	00321	000	192.	168.	.0.1	112	1	98.	66.	239.1	.46	TCP		74	6024	8 >	http	[5]	YN] S	eq
	9	0.3	03372	2000	192.	168.	.0.1	112	1	98.	66.	239.1	L46	TCP		74	[TCP	'Ret	rans	nis	sion]	6
	10	0.6	96015	5000	192.	168.	.0.1	112	1	98.	66.	239.1	L46	TCP		74	[TCP	P Ret	rans	nis:	sion]	6
	11	1.3	08080	0000	192.	168.	.0.1	112	1	98.	66.	239.1	L46	TCP		74	[TCP	P Ret	rans	nis:	sion]	6
	12	0.6	95992	2000	192.	168.	.0.1	L12	1	98.	66.	239.1	L46	TCP		74	[TCP	'Ret	rans	nis:	sion]	6
	17	1 7	07460	2000	To I	d miles			-0 1			07.20		100		60	Who	har	107	1 6 0	A 11	12
1		_																				·
0	) 💅	File	"C:\Us	ers\Al	DMINI~	1\Ap	pDa	ta\Loc	al\Ter	np\v	vires	hark_p	capn <u>g</u>	_807BB	CAF-	BDB3-4	B97-91	139-DF	5		Profile	: D

图 3.27 捕获数据过程

(5) 在 IP 地址为 192.168.0.112 的主机上访问网络(如访问网站 www.chappellu.com), 以产生数据。所有的数据,都将显示在图 3.27 中。

(6)返回到 Wireshark 中查看捕获文件,所有的数据都是来自/到达 192.168.0.112 主机。

#### 3.8.2 捕获 IP 地址范围

IP 地址一共分为 A、B、C、D、E 五类。其中,最常用的是前三类地址。IP 地址根据 网络位和主机位,将其分为五类。为了节约地址,CIDR(Classless Interdomain Routing) 将好几个 IP 网络结合在一起。通过使用掩码值,表示了一个 IP 地址范围。

下面看几个 IP 地址范围捕获过滤器的例子。

- □ net 192.168.0.0/24: 捕获到达/来自 192.168.0.0 网络中任何主机的数据。
- □ net 192.168.0.0 mask 255.255.255.0: 捕获到达/来自 192.168.0.0 网络中任何主机的 数据。
- □ ip6 net 2406:da00:ff00::/64: 捕获到达/来自 2406:da00:ff00:0000 (IPv6) 网络中任 何主机的数据。
- □ not dst net 192.168.0.0/24: 捕获除目的 IP 地址是 192.168.0.0 网络外的所有数据。
- □ dst net 192.168.0.0/24: 捕获到达 IP 地址为 192.168.0.0 网络内的所有数据。

□ src net 192.168.0.0/24: 捕获来自 IP 地址为 192.168.0.0 网络内的所有数据。

【实例 3-5】 捕获 192.168.0.0 网络中所有主机的数据。具体操作步骤如下所示。

(1) 启动 Wireshark 捕获工具。在该界面的菜单栏中依次选择 Capture|Options 选项, 打开捕获选项窗口, 如图 3.28 所示。

(2) 在该界面过滤器区域输入捕获过滤器 net 192.168.0.0/24。如果要保存该捕获文件,则单击 Browse 按钮选择保存捕获文件的位置和文件名。设置完后,如图 3.29 所示。

• 68 •

🚄 Wireshark: Capture Opti	ions		
Capture			
Capture In	terface	Link-layer header Pro	om. Mode Snaplen [B] Buffer [MiB] Capture Filter 📩
本地连接 「e80:95c2:84b3:b 192.168.0.110			enabled default 2
•		III	E and
Capture on all inter	faces		Manage Interfaces
✓ Use promiscuous m	node on all inte	rfaces	
<u>Capture Filter:</u>			Compile selected BPFs
Capture Files			Display Options
File:		Brows	e ☑ Update list of packets in real time
Use <u>m</u> ultiple files		✓ Use pcap-ng format	Automatically scroll during live capture
✓ Next file every	1 *	megabyte(s) 👻	
Next file every	1	minute(s) v	I Hide capture info dialog
Ring buffer with	2 *	files	Name Resolution
Stop capture after	1 *	file(s)	☑ Resolve MAC addresses
Stop Capture Automatical	ly After		Resolve <u>n</u> etwork-layer names
	icket(s)	1	Resolve transport-layer name
1 v m	ninute(s)	]	☑ Use <u>e</u> xternal network name resolver
Help			<u>Start</u> <u>Close</u>

图 3.28 捕获选项窗口

Wireshark: Capt	ure Options					
Capture						
Capture	Interface	Link-layer hea	der Prom. Mode	Snaplen [B] Bi	uffer (Mi	B] Capture Filte 🔺
本地连 「fe80:95 19216	接 6c2:84b3:b1fe:7828 8.0.110	Ethernet	disabled	default	2	net 192.168.0.0
<						- F
Use promis	cuous mode on all int net 192.168.0.0/24	erfaces		·	Con	npile selected BPFs
Capture Files			D	isplay Options		
File: D:\traces	i∖ip-range.pcapng	PC	Browse	✓ Update lis	t of pack	kets in real time
<u>H</u> elp					Sta	art <u>C</u> lose

图 3.29 设置过滤器

(3)从该界面可以看到目前设置的过滤器及文件保存位置。然后单击 Start 按钮,将开始捕获数据,如图 3.30 所示。

📕 ip	-rang	e.pcap	ng [\	Wireshar	k 1.10.7 (v	1.10.7-0	g6b931a1 from	n master	-1.10)]				x
Eile	Edit	View	<u>G</u> o	Capture	e <u>A</u> nalyze	Statist	cs Telephon <u>y</u>	Tools	Internals	<u>H</u> elp			
0	۲	4	Ø		<b>X</b> 🔁	Q	🗢 🛸 🌍 🖣	2		⊕,⊖,©	Q 🖭	<u>الله</u>	>>
Filte	er:								- Express	ion Clea	r Apply	Save	
No.	Tim	e	S	ource		Desti	nation	Protoc	ol Length	Info			
2	3 14	2254	270 G	iga-By	t_0b:00	4f Broa	dcast	ARP	60	who has	192.16	8.0.11	1
2	4 14	8007	300 1	92.168	.0.110	192.	168.0.1	DNS	77	Standard	d query	0x8b7	'c
2	5 14	98574	4301	92.168	.0.1	192.	168.0.110	DNS	109	Standard	d query	respo	or E
2	6 14	9863	5901	92.168	.0.110	162.	159.242.165	TCP	66	49335 >	http [	SYN] S	ie -
2	7 15	1924	900 1	62.159	.242.16	5 192.	168.0.110	TCP	66	http > 4	19335 [	SYN, A	AC
2	8 1 5	1925	380 1	92.168	.0.110	162.	159.242.165	TCP	54	49335 >	http [	ACK] S	se
2	9 1 5	1927	<b>500 1</b>	92.168	.0.110	162.	159.242.165	HTTP	476	GET / HT	<pre>FTP/1.1</pre>		
3	0 15	2393	690 G	iga-By	t_0b:00	4fBroa	dcast	ARP	60	Who has	192.16	8.0.11	1
3	1 15	3978	0401	62.159	.242.16	5 192.	168.0.110	TCP	60	http > 4	19335 [	ACK] S	ie i
3	2 1 5	4402	800 1	62.159	.242.16	5 192.	168.0.110	TCP	1293	[TCP sec	ament d	fare	28
3	3 1 5	4452	350 1	62.159	.242.16	5 192.	168.0.110	TCP	394	[TCP sec	, gment c	fare	28
3	4 15	4452	360 1	62.159	.242.16	5 192.	168.0.110	TCP	1087	[TCP sec	gment o	fare	ea -
3	5 1 5	4452	3701	62.159	.242.16	5 192.	168.0.110	TCP	1494	[TCP sed	ament c	fare	ea
3	6 1 5	4452	380 1	62.159	.242.16	5 192.	168.0.110	TCP	847	[TCP sed	, iment c	fare	- 6
٠ 📄						11							•
0	Fra	me (fra	me), (	60 bytes			Packets: 161	Displayee	d: 161 (100	.0 Profile	e: Default		

图 3.30 捕获的数据包

• 69 •

(4) 该捕获文件中所有的数据包, 都是 192.168.0.0/24 网络中主机的数据。

#### 3.8.3 捕获广播或多播地址数据

当 IP 地址的网络和主机位全为1时,广播地址就是 255.255.255.255。该地址应用于网络内的所有主机。该地址通常用在向局域网内所有主机发送广播包时,其目的地址就是广播地址。

多播地址即组播地址,是一组主机的表示符。在以太网中,多播地址是一个 48 位的标示符。在 IPv4 中,它在历史上被叫做 D 类地址,它的范围是 224.0.0.0~239.255.255.255。 广播地址全为 1 的 48 位地址,也属于多播地址。

通过监听广播和多播,可以在 Wireshark 中了解到关于网络上主机的数据。下面列出 几个常用的例子,如下所示。

□ ip broadcast: 捕获到 255.255.255.255 的数据。

□ ip multicast: 捕获通过 239.255.255~224.0.0.0 的数据。

□ dst host ff02::1: 捕获所有主机到 IPv6 多播地址的数据。

□ dst host ff02::2: 捕获所有路由到 IPv6 多播地址的数据。

如果只想捕获所有 IP 或 IPv6 的数据,使用 IP 或 IPv6 捕获过滤器。

【实例 3-6】 捕获广播地址数据。具体操作步骤如下所示。

(1) 启动 Wireshark 捕获工具。

(2) 在捕获窗口中设置捕获过滤器为 ip 255.255.255.255, 如图 3.31 所示。

apture						
Capture	Interface	Link-layer hea	der Prom. Mode	Snaplen [B] Bu	ffer [Mi	B] Captur ^
<b>V</b>	<b>本地连接</b> fe80::95c2:84b3:b1fe:7828 192.168.0.110	Ethernet	disabled	default	2	ip broadcast
•						•
Use <u>p</u>	romiscuous mode on all in Filter: ip broadcast	terfaces		Ŧ	Con	npile selected BPFs
apture File	25		D	splay Options		
File: D:\	traces\ip-broadcast.pcapn		Browse	✓ Update list	of pac	kets in real time
<u>H</u> elp					Sta	art <u>C</u> lose

图 3.31 设置广播地址过滤器

(3) 从该界面可以看到指定的过滤器和捕获文件的位置。此时单击 Start 按钮,将开始 捕获数据,如图 3.32 所示。

(4) 从该界面可以看到所有数据包,都是发送给255.255.255.255 主机的。

#### 3.8.4 捕获 MAC 地址数据

当想要捕获到达/来自一个主机 IPv4 或 IPv6 的数据时,可以创建一个基于主机的 MAC

• 70 •

地址捕获过滤器。由于 MAC 头部被剥去,并且通过路由器的路径被应用。这样确保了网络片段和目标主机片段一样。

	(ip-	broad	lcast.pcap	ong [Wire	shark 1.10	.7 (v1.10.7-	0-g6b931a	1 from m	aster-1.10	)]			
E	ile	<u>E</u> dit	View G	o <u>C</u> aptur	e <u>A</u> nalyze	Statistics	Telephon	<u>y T</u> ools	<u>I</u> nternals	<u>H</u> elp			
	D	۷ (	( 🔳 🖉		) X 2	Q, ¢	🔶 🧼	7 L		⊕,⊝	0	1   🌌	🗹 畅 »
F	ilter	:							- Expre	ession (	Clear A	pply Sa	ve
N	о.	Time		Source		Destinatio	n	Protoco	l Length	Info			~
		0.00	0000000	)192.168	.0.102	255.255	.255.255	UDP	508	Source	port:	58274	Destina
	2	30.0	0088730	192.168	.0.102	255.255	.255.255	UDP	508	Source	port:	58274	Destina =
	3	31.7	7193260	192.168	.0.108	255.255	.255.255	DHCP	342	DHCP In	nform	– Tra	nsactior
	4	40.0	0510450	192.168	.0.102	255.255	.255.255	UDP	508	Source	port:	58275	Destina —
	5	41.4	4338510	192.168	.0.104	255.255	.255.255	DHCP	342	DHCP In	nform	– Tra	nsactior
	6	70.0	0602220	192.168	.0.102	255.255	.255.255	UDP	508	Source	port:	58275	Destina
	- 7	100.	. 069057	192.168	.0.102	255.255	.255.255	UDP	508	Source	port:	58275	Destina
	8	130.	074696	5192.168	.0.102	255.255	.255.255	UDP	508	Source	port:	58275	Destina
	9	130.	.110494	192.168	.0.104	255.255	.255.255	DHCP	342	DHCP In	nform	– Tra	nsactior
	10	160.	.081700	192.168	.0.102	255.255	.255.255	UDP	508	Source	port:	58275	Destina
	11	166.	205064	192.168	.0.106	255.255	.255.255	UDP	355	Source	port:	53855	Destina
	12	166.	225063	192.168	.0.106	255.255	.255.255	UDP	397	Source	port:	53856	Destina
	10	166	245002	107 169	0 106	755 755	755 755	linn	264	Source	nort ·	52957	Doctin
1		_	_			ni		_					•
C	) 💅	File:	"D:\trace	s\ip-broadc	ast.pcapng	" 18 k 🖡	ackets: 38	Displayed	d: 38 (100	.0%) · Dr.	Prof	ile: Defau	t

图 3.32 捕获的广播地址数据

□ ether host 00:08:15:00:08:15: 捕获到达/来自 00:08:15:00:08:15 主机的数据。

- □ ether src 02:0A:42:23:41:AC: 捕获来自 02:0A:42:23:41:AC 主机的数据。
- □ ether dst 02:0A:42:23:41:AC: 捕获到达 02:0A:42:23:41:AC 主机的数据。
- □ not ether host 00:08:15:00:08:15: 捕获到达/来自除了 00:08:15:00:08:15 的任何 MAC 地址的流量。

【实例 3-7】 仅捕获到达/来自其他 MAC 地址的数据。具体操作步骤如下所示。

- (1) 使用 ipconfig 或 ifconfig 命令, 查看活跃接口的 MAC 地址。
- (2) 在工具栏中单击 ④按钮, 打开捕获选项界面, 如图 3.33 所示。

pture							
Capture	Interface	Link-layer hea	der Prom. Mode	Snaplen [B] B	uffer [MiB]	Capture Filter	
	<b>本地连接 2</b> fe80:c5a2:72ce:40bb:6005 0.0.0.0	Ethernet	enabled	default	2		[
	<b>本地连接</b> fe80:40fa:dfed:94b:f9db 192 168.0 108	Ethernet	enabled	default			

图 3.33 捕获选项

(3)在该界面的捕获区域,勾选捕获数据的接口(本地连接)的复选框。在这个捕获 区域双击选择接口行的任何一处,启动编辑接口设置窗口,如图 3.34 所示。

(4) 在该界面输入 not ether host xx.xx.xx.xx.xx (以太网地址), 如图 3.34 所示。

(5)为了方便以后使用该过滤器,这里将保留此过滤器。单击 Capture Filter 按钮,将显示如图 3.35 所示的界面。

(6) 在该界面修改过滤器名字,设置为 NotMyMAC。然后单击 New 按钮,该过滤器 创建成功,如图 3.36 所示。

• 71 •

	📕 Wireshark: Capture Filter - Profile: Default
	Edit Capture Filter
	new
Edit Interface Settings	udp only
Capture	
Interface: 本地连接	
IP address: fe80::40fa:dfed:94b:f9db	
192.168.0.108 -	Delete
Link-layer header type: Ethernet 💌	
Capture packets in promiscuous mode	
Limit each packet to 65535 A bytes	Properties
Buffer size: 2 mebibyte(s)	Filter name: New filter
Compile BPF	Filter string: not ether host 00-0C-29-56-BD-21
Help         QK         Cancel	Help         QK         Cancel

- 图 3.34 编辑接口设置
- 图 3.35 保存捕获过滤器

📕 Wiresha	rk: Capture Filter - Profile: Default
Edit	Capture Filter
	new
	udp only
New	NotMyMAC
Delete	
Properties	
Filter name	e: NotMyMAC
Filter string	r not ether host 00-0C-29-56-BD-21
Help	<u>Q</u> K <u>C</u> ancel

图 3.36 创建捕获过滤器

(7) 从该界面可以看到 NotMyMAC 捕获过滤器被成功地创建。此时单击 OK 按钮,将看到如图 3.37 所示的界面。

Capture	Interface 本冊法辞 2	Link-layer head	der Prom. Mode	Snaplen [B] B	Buffer [MiB]	] Capture Filter	^
	fe80:c5a2:72ce:40bb:6005 0.0.0.0	Ethernet	enabled	default	2		
<b>V</b>	本地连接 fe80:40fa:dfed:94b:f9db 192.168.0.108	Ethernet	enabled	default	2	not ether host 00-0C-29-56-BD-21	<u>ן</u>
۰.							P.
Capt	ure on all interfaces promiscuous mode on all int	erfaces				Manage Inter	faces

图 3.37 创建的捕获过滤器

(8)从该界面可以看到新创建的捕获过滤器。现在单击 Start 按钮,将开始捕获。

• 72 •

(9)此时,用户可以在非 MAC 地址为 00-0C-29-56-BD-21 的所有主机上进行操作。 通过访问各种网站、登录服务器或发生邮件,产生主机间的数据流量。

(10) 返回到 Wireshark 主界面,单击■(停止捕获)按钮。捕获到的数据如图 3.38 所示。

	Capt	ure_mac.pca	png [Wires	hark 1.10.7 (v1	.10.7-0-g6b931a1	from master-1	1.10)]	
E	ile <u>E</u>	dit <u>V</u> iew	<u>Go</u> <u>C</u> apture	<u>Analyze</u> <u>S</u> tat	tistics Telephony	<u>T</u> ools <u>I</u> nterr	nals <u>H</u> elp	
			1 🖻 🔓	🗶 🔁   Q	、 🗢 🔿 🐴	• 👱   🔳 🛙	🗐 ( O, O, O, 🖺 ) 🌌 🗹 🕵 % (	1
	Filter	:					Expression Clear Apply	Save New Label
No	о. Т	ime	Source		Destination	Protocol	Length Info	*
	1 (	.0000000	00 Giga-By	/t_68:24:58	Broadcast	ARP	60 who has 192.168.0.3? Tel	1 192.168.0.110 🦳
	2 0	.2985300	00 Giga-By	/t_0b:00:4f	Broadcast	ARP	60 who has 192.168.0.111? T	ell 192.168.0.105
	3 (	.3358610	00 192.168	8.0.112	74.125.136.1	01 TCP	74 41514 > http [SYN] Seq=0	Win=29200 Len=0 MS5
	4 (	.0001850	00 192.168	8.0.112	74.125.136.1	39 TCP	74 52398 > http [SYN] Seq=0	Win=29200 Len=0 MSS
	5 0	.1649580	00 192.168	8.0.112	74.125.136.1	38 TCP	74 38863 > http [SYN] Seq=0	Win=29200 Len=0 MSS
	6 (	.0639570	00 192.168	8.0.112	74.125.136.1	00 ТСР	74 37243 > http [SYN] Seq=0	Win=29200 Len=0 MSS
	7 0	.0000810	00 192.168	8.0.112	74.125.136.1	38 TCP	74 secrmmsafecopya > http [S	YN] Seq=0 Win=29200
	8 (	.0797350	00 Giga-By	/t_c8:4c:89	Broadcast	ARP	42 who has 192.168.0.1? Tel	1 192.168.0.108
	9 (	.0002380	00 Tp-Link	кт_f9:3c:c0	Giga-Byt_c8:	4c:8ARP	60 192.168.0.1 is at 6c:e8:7	3:f9:3c:c0
	10 0	.0564090	00 Giga-By	/t_68:24:58	Broadcast	ARP	60 Who has 192.168.0.3? Tel	1 192.168.0.110
	11 (	.1845010	00 Giga-By	/t_0b:00:4f	Broadcast	ARP	60 who has 192.168.0.111? T	ell 192.168.0.105
	12 (	.4470740	00 192.168	8.0.112	74.125.136.1	01 ТСР	74 [TCP Retransmission] 4151	4 > http [SYN] Seq=
	13 (	0000850	00 192.168	8.0.112	74.125.136.1	39 ТСР	74 [TCP Retransmission] 5239	8 > http [SYN] Seq=
	14 (	.3649570	00 Giga-By	/t_c8:4c:89	Broadcast	ARP	42 Who has 192.168.0.3? Tel	1 192.168.0.108
	15 0	.1862280	00 Giga-By	/t_0b:00:4f	Broadcast	ARP	60 Who has 192.168.0.111? T	ell 192.168.0.105 🗸
4					····			4
0	1	File: "D:\trac	es\Capture_m	ac.pcapng" 306	4 kB 00:01:10		Packets: 5448 · Dis	played: 5448 Profile: D

图 3.38 捕获的数据

(11)在该界面通过滚动鼠标,查看捕获的所有数据。在该捕获文件中,将不会出现 MAC 地址为 00-0C-29-56-BD-21 主机的数据。

### 3.9 捕获端口应用程序数据

在 Wireshark 中想要使用捕获过滤器捕获应用程序的数据时,需要使用端口过滤器。 本节将介绍捕获端口应用程序数据。

#### 3.9.1 捕获所有端口号的数据

在网络中,大部分的应用程序都有相应的端口号,如 DNS、HTTP、FTP。下面列出了 一些最常用的应用程序捕获过滤器,如下所示。

□ port 53: 捕获到达/来自端口号为 53 的 UDP/TCP 数据(典型的 DNS 数据)。

□ not port 53: 捕获除到达/来自端口号为 53 的所有 UDP/TCP 数据。

□ port 80: 捕获到达/来自端口号为 80 的 UDP/TCP 数据(典型的 HTTP 数据)。

□ udp port 67: 捕获到达/来自端口号为 67 的 UDP 数据(典型的 DHCP 数据)。

□ tcp port 21: 捕获到达/来自端口号为 21 的 TCP 数据(典型的 FTP 命令行)。

□ portrange 1-80: 捕获到达/来自 1~80 端口号的 UDP/TCP 数据。

□ tcp portrange 1-80: 捕获到达/来自 1~80 端口号的 TCP 数据。

【实例 3-8】 捕获端口为 80 的所有数据包。具体操作步骤如下所示。

• 73 •

- (1) 启动 Wireshark 工具。
- (2) 在捕获选项窗口中设置捕获 80 端口数据的过滤器,并保存该文件,如图 3.39 所示。

📕 Wireshark: Capt	ure Options						• X			
Capture										
Capture	Interface	Link-layer head	der Prom. Mode	Snaplen [B] But	fer (MiB	] Capture F	ilter 🔺			
本地连 又 fe80:95 192.168	接 5c2:84b3:b1fe:7828 8.0.110	Ethernet	disabled	default	2	port 80				
٠							Þ			
✓ Capture on ✓ Use promision	Capture on all interfaces     Manage Interfaces     Use promiscuous mode on all interfaces									
Capture Filter:	port 80			-	Com	pile selected	BPFs			
Capture Files			Di	splay Options						
File: D:\traces	http-port.pcapng		Browse	✓ Update list	of pack	ets in real ti	me			
Help				[	<u>S</u> tar	rt 📄	<u>C</u> lose			

图 3.39 设置端口过滤器

(3)从该界面可以看到设置的捕获过滤器和文件保存位置。设置完后单击 Start 按钮,将显示如图 3.40 所示的界面。

	http-	-port.pcap	ong [Wireshark	1.10.7 (v	/1.10.7-0-g	5b931a1 f	rom maste	er-1.10)]			x
Eile	e <u>E</u> o	dit <u>V</u> iew	<u>G</u> o <u>C</u> apture	<u>A</u> nalyze	Statistics	Telephor	i <u>y T</u> ools	<u>I</u> nternals <u>H</u> elp			
0	۲		🔏   🖻 🤷	* 2	0, ቀ	🧼 🏟	₮ 👱		Q. Q. 🖪	3	>>
Filt	ter:							Expression	Clear A	oply	~~
No.	Т	ime	Source		Destination		Protocol	l Length Info			~
	1 0	0.00000	000 192.168.	0.110	61.135.1	69.125	тср	54 49363	> http	[RST	
	2 0	0.452284	00 192.168.	0.110	61.135.1	69.125	TCP	66 49366	> http	[SYN]	1 E
	3 0	).461451	100 61.135.1	69.125	192.168.	0.110	TCP	66 http	> 49366	[SYN	, ,
	4 0	).461517	700 192.168.	0.110	61.135.1	.69.125	TCP	54 49366	> http	[ACK]	
	5 0	).465234	00 192.168.	0.110	61.135.1	.69.125	HTTP	589 GET /	' HTTP/1.	1	
	6 0	).491559	00 61.135.1	69.125	192.168.	0.110	TCP	60 http	> 49366	[ACK]	
	70	0.495069	00 61.135.1	69.125	192.168.	0.110	TCP	586 [TCP	segment	of a	r
	8 0	.496037	00 61.135.1	69.125	192.168.	0.110	TCP	1494 [TCP	segment	of a	r
	9 0	).496038	300 61.135.1	69.125	192.168.	0.110	TCP	1494 [TCP	segment	of a	r
	10 0	).496039	00 61.135.1	69.125	192.168.	0.110	TCP	1494 [TCP	segment	of a	r
	11 0	.496040	000 61.135.1	69.125	192.168.	0.110	TCP	1494 [TCP	segment	of a	r
	12 0	0.496041	100 61.135.1	69.125	192.168.	0.110	TCP	1494 [TCP	segment	of a	r
	1 7 0	106047	000 61 175 1	CO 105	100 160	0 110	TCD	1404 Erch	coment	of o	
1											
	1	File: "D:\tr	aces\http-port.p	capng" 23	9 kB Pa	ackets: 40	<ul> <li>Displayed</li> </ul>	i: 40 (10 Pro	file: Default		

图 3.40 捕获 80 端口的数据

(4) 从该捕获文件的 Protocol 列可以看到所有的协议都为 TCP 和 HTTP。这两种协议 的数据包,都是来自 80 端口的。

#### 3.9.2 结合基于端口的捕获过滤器

当用户想要捕获到达/来自各种非连续端口号的数据,可以通过组合各种逻辑运算符来 实现,如下所示。

□ port 20 or port 21: 捕获到达/来自 20 或 21 端口号的所有 UDP/TCP 数据。

• 74 •

- □ host 10.3.1.1 and port 80: 捕获到达/来自端口号为 80, 并且是到达/来自 10.3.1.1 主 机的 UDP/TCP 数据。
- □ host 10.3.1.1 and not port 80: 捕获到/来自 10.3.1.1 主机,并且是非 80 端口的 UDP/TCP 数据。
- □ udp src port 68 and udp dst port 67: 捕获来自端口为 68, 目标端口号为 67 的所有 UDP 数据(典型的 DHCP 客户端到 DHCP 服务器的数据)。
- □ udp src port 67 and udp dst port 68: 捕获来自端口号为 67, 目标端口号为 68 的所有 UDP 数据(典型的 DHCP 服务器到 DHCP 客户端的数据)。
- ●提示:尽可能不要使用捕获过滤器。当捕获大量的数据时,可以通过使用显示过滤器过 滤特定的数据。

【实例 3-9】 捕获 192.168.0.110 主机上非 80 端口的数据。具体操作步骤如下所示。

(1) 启动 Wireshark 工具。

(2) 在捕获选项窗口中设置捕获主机 192.168.0.110 上非 80 端口数据的过滤器,并保存该文件,如图 3.41 所示。

🚄 Wireshark: Ca	apture Options										
Capture											
Capture	Interface	Link-layer head	der Prom. Mode	Snaplen (B) Bu	ffer [MiB]	Cap 🔺					
本批 ▼ fe80 192	<b>b连接</b> )::95c2:84b3:b1fe:7828 .168.0.110	Ethernet	disabled	default	2 host	192.168.0					
٠		III				Þ					
✓ Capture ✓ Use pror	Image: Capture on all interfaces       Manage Interfaces         Image: Use promiscuous mode on all interfaces       Image: Capture on all interfaces										
Capture Filt	er: host 192.168.0.110	and not port 80		•	Compile se	elected BPFs					
Capture Files Capture Files			Di Di	isplay Options isplay Options							
File: D:\tra Help	ces\http-noport.pcapng		Browse	Vodate list	of packets in <u>S</u> tart	real time <u>C</u> lose					

图 3.41 设置的过滤器

(3) 在捕获过滤器区域设置捕获过滤器后,单击 Start 按钮,将显示如图 3.42 所示的 界面。

<u> </u>	ttp-noj	port.pc	apng	[Wiresh	ark 1.10.7	(v1.10	.7-0-g6b	931a1 <del> </del>	from m	aster-1.10	)] 🕒		x
<u>F</u> ile	<u>E</u> dit	View	<u>G</u> o	<u>Capture</u>	<u>A</u> nalyze	<u>S</u> tatis	tics Tele	phon <u>y</u>	<u>T</u> ools	Internals	<u>H</u> elp		
0	0		Ø		* 2	Q	<b>\$</b>	4) 7	<b>1</b>		⊕,⊝		~~
Filte	er:									- Expre	ession	Clear	**
No.	Time		So	urce		Destina	tion		Protoco	l Length	Info		
	1 0.0	00000	100 Vn	nware_7	2:ff:21	Broad	cast		ARP	42	Who ha	5 192.	168.0
	2 0.0	00698	00 тр	o-Link⊤	_f9:3c:	Vmwar	e_72:f1	:21	ARP	60	192.16	8.0.1	is a
	3 2.4	09270	00 19	92.168.	0.110	192.1	68.0.1		DNS	73	Standa	rd que	ry 0
	4 2.4	16292	00 19	92.168.	0.1	192.1	68.0.1	LO	DNS	132	Standa	rd que	ry r
	5 2.5	63982	00 19	92.168.	0.110	192.1	68.0.1		DNS	78	Standa	rd que	ry 0
	62.5	67076	00 19	92.168.	0.1	192.1	68.0.1	L <b>O</b>	DNS	126	Standa	rd que	ry r
	7 2.5	69428	00 19	92.168.	0.110	192.1	68.0.1		DNS	80	Standa	rd que	ry 0
	8 2.5	73074	00 19	92.168.	0.1	192.1	68.0.1	L <b>O</b>	DNS	130	Standa	rd que	ry re
٠.					III								P.
0 🖢	File:	"D:\tra	ces\ht	ttp-nopor	t.pcapng"	126	Packets	: 8 · Di	splayed	: 8 Pro	file: Defau	lt	

图 3.42 捕获的数据

(4)此时,在该捕获文件中的 Protocol 列,将不会看到有 TCP 和 HTTP 的数据。因为 TCP 和 HTTP 协议的数据包,端口号是 80。

【实例 3-10】 创建、保存并应用一个 DNS 捕获过滤器。具体操作步骤如下所示。 (1) 在工具栏中单击 ④按钮,打开捕获选项界面,如图 3.43 所示。

apture							
Capture	Interface	Link-layer hea	der Prom. Mode	Snaplen [B] B	Buffer [MiB]	Capture Filter	^
	<b>本地连接 2</b> fe80:c5a2:72ce:40bb:6005 0.0.0.0	Ethernet	enabled	default	2		
V	本地连接 fe80:40fa:dfed:94b:f9db 192.168.0.108	Ethernet	enabled	default	2		

图 3.43 捕获选项

(2) 在该界面的捕获区域,勾选捕获数据的接口(本地连接)的复选框。在这个捕获 区域双击选择接口行的任何一处,启动编辑接口设置窗口,如图 3.44 所示。

(3) 在该界面 Capture Filter 对应的文本框中输入 port 53, 如图 3.44 所示。此时通过单 击 Capture Filter 按钮添加该捕获过滤器, 如图 3.45 所示。

📕 Edit Interfa	ce Settings	Wiresha	urk: Canture Filter - Profile: Default
Capture Interface:	本地连接	Edit	Capture Filter
IP address:	fe80::40fa:dfed:94b:f9db		udp only
	192.168.0.108	New	NotMyMAC
Link-layer he	ader type: Ethernet		DNS
✓ Capture ■ Limit eac	h packet to 65535  bytes	Delete	
Buffer size: 2	mebibyte(s)	Properties	
Capture File	ter: port 53 Compile BPF	Filter nam Filter strin	e: DNS g: port 53
Help	<u>Q</u> K <u>C</u> ancel	Help	<u>QK</u> <u>Cancel</u>

图 3.44 接口设置界面

图 3.45 创建捕获过滤器

(4)从该界面可以看到,添加的过滤器名称为 DNS。然后单击 OK 按钮,将显示如图 3.46 所示的界面。

(5)从该界面可以看到创建的捕获过滤器。在该界面指定捕获文件的位置,单击 Browse 按钮,选择并保存捕获文件。本例中设置的捕获文件为 mydns.pcapng。然后设置使用多个 文件,并定义下一个生成的文件为每 10 秒生成一个 1MB 的文件,如图 3.46 所示。单击 Start 按钮,开始捕获数据。

(6)此时通过访问互联网上不同的网站,查看数据。最好访问最近没有访问过的网站, 以确保 DNS 信息不是从缓存中加载的。

(7) 返回到 Wireshark 界面,单击■(停止捕获)按钮。显示界面,如图 3.47 所示。

apture						
Capture In	terface	Link-layer header P	rom. Mode Snaplen [B] Buffer [MiB] Capt 🔨			
本地连接 ✓ fe80:40fa:dfed:94 192.168.0.108	b:f9db	Ethernet	enabled default 2 port 53			
•		m	•			
Capture on all interf Use promiscuous m	aces ode on all inte	rfaces	Manage Interfaces			
Capture Filter: port 5	i3		▼ Compile selected BPFs			
apture Files Display Options						
File: D:\traces\mydns.pcapng						
✓ Use <u>multiple</u> files ✓ Use pcap-ng format			at 🔄 Automatically scroll during live capture			
Next file every	1	megabyte(s)	•			
Next file every	10	minute(s)	✓ <u>H</u> ide capture info dialog			
Ring buffer with	2 *	files	Name Resolution			
Stop capture after	1	file(s)	Resolve MAC addresses			
top Capture Automatical	y After		Resolve <u>n</u> etwork-layer names			
	cket(s)	_	Resolve transport-layer name			
1 m	egabyte(s) 🔻					
🔲 1 🗎 m	inute(s)	,	Use <u>external network name resolver</u>			

图 3.46 捕获选项

	🕻 mydns_00001_20140618155128.pcapng [Wireshark 1.10.7 (v1.10.7-0-g6b931a1 from master-1.10)]							
Eile	<u>E</u> dit	<u>V</u> iew <u>G</u> o	<u>Capture</u> Analyze	Statistics Telephon	<u>y T</u> ools	Internals Help		
0	۲	1 🔳 🔬	🕒 🛅 🗶 🔁	् 🔶 🔿	₮ ⊻	🗐 🖬   9, 9, 9, 17   👪 🗹 🥵 🔆   🕱	1	
	Filter:					Expression Clear Apply	»»	
No.	Tim	e	Source	Destination	Protocol	Length Info	*	
	1 0.0	000000000	192.168.0.108	8.8.8.8	DNS	73 Standard query Oxfebf A www.leca	-	
	2 0.2	221143000	8.8.8.8	192.168.0.108	DNS	246 Standard query response Oxfebf (		
	3 1. 5	509150000	192.168.0.114	192.168.0.1	DNS	73 Standard query Oxf521 A www.baid		
	4 0.0	000079000	192.168.0.114	192.168.0.1	DNS	73 Standard query 0x2412 AAAA www.b		
	5 0.0	001998000	192.168.0.1	192.168.0.114	DNS	132 Standard query response 0xf521 0	1	
	6 0.0	000457000	192.168.0.1	192.168.0.114	DNS	157 Standard query response 0x2412 (	1	
	7 0.0	037207000	192.168.0.114	192.168.0.1	DNS	75 Standard query 0x4cbd A s1.bdsta		
	8 0.0	000073000	192.168.0.114	192.168.0.1	DNS	75 Standard query 0x537d AAAA s1.bo		
	9 0.0	001695000	192.168.0.114	192.168.0.1	DNS	72 Standard query 0x98fe A t1.baidu	1	
	10 0.0	000042000	192.168.0.114	192.168.0.1	DNS	72 Standard query Oxdfa0 AAAA t1.ba		
	11 0.0	000429000	192.168.0.114	192.168.0.1	DNS	72 Standard query 0x1669 A t2.baid		
	12 0.0	000034000	192.168.0.114	192.168.0.1	DNS	72 Standard query 0x5376 AAAA t2.ba		
	13 0.0	00096000	192.168.0.1	192.168.0.114	DNS	122 Standard query response 0x4cbd 0	1	
	14 0.0	000000000	192.168.0.1	192.168.0.114	DNS	169 Standard query response 0x537d (		
	15 0.0	000748000	192.168.0.114	192.168.0.1	DNS	72 Standard query 0xb281 A t3.baidu	Ŧ	
۲.				"		•		
0	⑦ File: "D:\traces\mydns_00001_20140618155128.pcapng" 54 kB 00:00:39 Packets: Profile: D							

图 3.47 捕获的数据

(8)从该界面可以看到,所有的数据都是 DNS。此时可以通过滚动鼠标,查看捕获文件过程中访问过的网站。

# 3.10 捕获特定 ICMP 数据

互联网控制消息协议(ICMP)是一种协议。当一个网络中出现性能或安全问题时,将

• 77 •

会看到该协议。在这种情况下,用户必须使用一个偏移量来表示在一个 ICMP 中字段的位

- 置。偏移量为0表示是ICMP字段类型;偏移量为1表示ICMP的位置代码字段。
  - 下面将列出几个 ICMP 捕获过滤器的结构。
  - □ icmp: 捕获所有 ICMP 数据包。
  - □ icmp[0]=8: 捕获所有 ICMP 字段类型为 8(Echo Request)的数据包。
  - □ icmp[0]=17: 捕获所有 ICMP 字段类型为 17 (Address Mask Request)的数据包。
  - □ icmp[0]=8 or icmp[0]=0: 捕获所有 ICMP 字段类型为 8 (Echo Request) 或 ICMP 字段类型为 0 (Echo Reply) 的数据包。
  - □ icmp[0]=3 and not icmp[1]=4: 捕获所有 ICMP 字段类型为 3 (Destination Unreachable)的包,除了 ICMP 字段类型为 3/代码为 4 (Fragmentation Needed and Don't Fragment was Set)的数据包。

【实例 3-11】 捕获 ICMP 协议数据包。具体操作步骤如下所示。

(1)在工具栏中单击 ③按钮,打开捕获选项界面,如图 3.48 所示。

apture							
Capture	Interface	Link-layer hea	der Prom. Mode	Snaplen [B] B	Buffer [Mi	iB] Capture Filte	r 1
	本地注按 2 fe80:548b:a761:b6e:5c5c 192:168.0.104	Ethernet	enabled	default	2		
	<b>本地连接</b> fe80:744c:a0ee:dbfd:769 192168.6101	Ethernet	enabled	default	2		

图 3.48 捕获选项

(2) 在该界面的捕获区域,勾选捕获数据的接口(本地连接)的复选框。在这个捕获 区域双击选择接口行的任何一处,启动编辑接口设置窗口,如图 3.49 所示。

(3) 在该界面的 Capture Filter 文本框中输入 icmp,如图 3.49 所示。如果用户在后面 还要使用该过滤器,可以通过单击 Capture Filter 按钮,来添加该捕获过滤器,如图 3.50 所示。

Capture	
Interface:	本地连接
IP address:	fe80::744c:a0ee:dbfd:769
	192.168.6.101 +
Link-layer he	ader type: Ethernet
Limit ead	ch packet to 65535 🖉 bytes
Buffer size:	2 mebibyte(s)
Capture Fi	ter: icmp  Compile BPF

图 3.49 接口设置界面

Wireshark	:: Capture Filter - Profile: Default					
Edit C	apture Filter					
	IP only					
	IP address 192.168.0.1					
New	IPX only					
	TCP only					
	UDP only					
	TCP or UDP port 80 (HTTP)					
	HTTP TCP port (80)					
<u>D</u> elete	No ARP and no DNS					
	Non-HTTP and non-SMTP to/from www.wireshark.org					
	ICMP only					
roperties						
Filter name:	ICMP only					
Filter string:	icmp					
<u>H</u> elp	<u>Q</u> K <u>C</u> ancel					

图 3.50 创建捕获过滤器

• 78 •

(4) 在该界面设置过滤器的名称(这里设置名称为 ICMP only),单击 New 按钮添加 该过滤器。然后单击 OK 按钮,将显示如图 3.51 所示的界面。

Wireshark: Captu	re Options				
Capture					
Capture	Interface	Link-layer hea	der Prom. Mode	e Snaplen [B] Buff	er [MiB] Capture Filter 🔺
本地连接 「fe80:744 192.168」	<b>登</b> ic:a0ee:dbfd:769 5.101	Ethernet	enabled	default	2 icmp
∢ [		"	1		Þ
Capture on a	II interfaces				Manage Interfaces
✓ Use promisc	uous mode on all i	nterfaces			
	icmp			Ţ	Compile selected BPFs
Capture Files			(	Display Options	
File: H:\traces\	icmp.pcapng		Browse	<b>☑</b> <u>U</u> pdate list o	of packets in real time
<b>▼</b> Use <u>m</u> ultiple	files	Use pcap-ng	format	✓ <u>A</u> utomatical	y scroll during live capture
Next file even	ry 1	megabyte(s)	-		
Vext file even	ry 10	minute(s)	•	Hide capture	e info dialog
🔲 Ring buffer v	vith 2	∱ files		Name Resolution	
Stop capture	after 1	file(s)		▼ Resolve <u>M</u> A	C addresses
top Capture Auto	matically After			Resolve <u>n</u> et	vork-layer names
1	packet(s)				
1	megabyte(s)	-		Resolve tran	sport-layer name
1	minute(s)	~		☑ Use <u>e</u> xterna	network name resolver

图 3.51 捕获选项

(5)从该界面可以看到创建的捕获过滤器。在该界面指定捕获文件的位置,单击 Browse 按钮,选择并保存捕获文件。本例中设置的捕获文件为 icmp.pcapng。然后设置使用多个文件,并定义下一个生成的文件为每 10 秒生成一个 1MB 的文件,如图 3.51 所示。单击 Start 按钮,开始捕获数据。

(6) 此时通过执行 ping 命令,以产生供 Wireshark 捕获的数据。

(7) 返回到 Wireshark 界面,单击■(停止捕获)按钮。显示界面,如图 3.52 所示。

	🧹 icmp_00001_20140822145618.pcapng [Wireshark 1.10.7 (v1.10.7-0-g6b931a1 from master-1.10)]								
Eik	e <u>E</u> dit <u>V</u> ie	ew <u>G</u> o <u>C</u> apture <u>/</u>	<u>A</u> nalyze <u>S</u> tatistics Telephor	n <u>y T</u> ools <u>I</u> ntern	als <u>H</u> elp				
0	◉ ◉ ∡ ■ ∅   ⊨ ≞ ೫ ∅   ੧, ⇔ ⇔ ⇔ 7 ⊻   🗐 🗐 ! ୧, ୧, ୧, 🗉   ₩ № 🥵 %   छ								
Fil	ter:			- Ex	pression Clear Apply	Save			
No.	Time	Source	Destination	Protocol L	ength Info				
	1 0.0000	00000 192.168.6.	101 192.168.6.1	ICMP	74 Echo (ping) r	equest id=0x0001, seq=1/256,			
	2 0.0001	4700 192.168.6.	1 192.168.6.101	ICMP	74 Echo (ping) r	eply id=0x0001, seq=1/256, 1			
	3 1.0011	1500 192.168.6.	101 192.168.6.1	ICMP	74 Echo (ping) r	equest id=0x0001, seq=2/512,			
	4 1.0012	29100 192.168.6.	1 192.168.6.101	ICMP	74 Echo (ping) r	eply id=0x0001, seq=2/512, i			
	5 2.0024	5100 192.168.6.	101 192.168.6.1	ICMP	74 Echo (ping) r	equest id=0x0001, seq=3/768,			
	6 2.0026	55400 192.168.6.	1 192.168.6.101	ICMP	74 Echo (ping) r	eply id=0x0001, seq=3/768,			
	7 3.0035	59900 192.168.6.	101 192.168.6.1	ICMP	74 Echo (ping) r	equest id=0x0001, seq=4/1024,			
	8 3.0037	6800 192.168.6.	1 192.168.6.101	ICMP	74 Echo (ping) r	eply id=0x0001, seq=4/1024,			
•	_					•			
0	💅 File: "H:	\traces\icmp_00001_	2 Packets: 8 · Displayed:	8 (100.0%) · Dr	opped: 0 (0.0%) · Load tin	ne: 0:00.000 Profile: Default			

图 3.52 捕获的 ICMP 数据包

(8) 从该界面可以看到, 捕获的所有数据包的 Protocol 列为 ICMP。