项目1

网络封包分析工具 Wireshark

1.1 Wireshark 简介



Wireshark 是目前流行的网络封包分析工具,可以帮助我们获得网络连接中的各项数据。以前上网、访问网页对于人们来说,只是一个抽象的概念,我们并不知道到底是如何浏览那些网络信息的,而利用 Wireshark 可以将这些概念实体化,各项数据直观地展现了网络连接、网页访问的全过程。这个强大的工具可以捕捉网络中的数据,并为用户提供关于网络和上层协议的各种信息。与其他很多网络工具一样,Wireshark 也使用 Npcap 来进行封包捕捉,并可破解局域网内 QQ、邮箱、MSN 等账号密码。

网络管理员使用 Wireshark 来检测网络问题,网络安全工程师使用 Wireshark 来检查安全的相关问题,开发者使用 Wireshark 来为新的通信协议找错,普通使用者使用 Wireshark 来学习网络协议的相关知识。当然,有的人也会"居心叵测"地用它来寻找一些敏感信息。

1.2 Wireshark 工作流程

(1)确定 Wireshark 的位置。如果没有一个正确的位置, 启动 Wireshark 后会花费 很长的时间捕获一些与自己无关的数据。

(2)选择捕获接口。一般都是选择连接到 Internet 网络的接口,这样才可以捕获到 与网络相关的数据;否则,捕获到的其他数据对自己也没有任何帮助。

(3)使用捕获过滤器。通过设置捕获过滤器,可以避免产生过大的捕获文件。这样 用户在分析数据时,也不会受其他数据的干扰,而且,还可以为用户节约大量的时间。

(4)使用显示过滤器。通常使用捕获过滤器过滤后的数据,往往还是很复杂。为了 使过滤的数据包更细致,此时使用显示过滤器进行过滤。

(5)使用着色规则。通常使用显示过滤器过滤后的数据,都是有用的数据包。如果 想更加突出地显示某个会话,可以使用着色规则高亮显示。

(6)构建图表。如果用户想要更明显地看出一个网络中数据的变化情况,使用图表的形式可以很方便地展现数据分布的情况。

(7) 重组数据。Wireshark 的重组功能,可以重组一个会话中不同数据包的信息,或 者是重组一个完整的图片或文件。由于传输的文件往往较大,所以信息分布在多个数据



网络攻防项目实战(微课视频版)

包中。为了能够查看到整个图片或文件,需要使用重组数据的方法来实现。

1.3 Wireshark 安装

可到官网下载 Wireshark, 网址为 https://www.wireshark.org/download.html, 网站界面如图 1.1 所示。



图 1.1 打开 Wireshark 的官网

选择 3.4.2 版本,单击 Windows Installer(64-bit)下载,可以下载到任意目录,下载的 文件为 Wireshark-win64-3.4.2. exe,执行该文件,显示结果如图 1.2 所示。



图 1.2 安装 Wireshark-win64-3.4.2. exe



单击 Next 按钮,显示许可协议,如图 1.3 所示。

i cense Agreement Diasea raview the licence terms before installin	www.wirechark 3.4	764.64		1
Please review ule idense terms before installi	iy wiresilark 5.4.	2 04-011.		-
Wireshark is distributed under the GNU Genera	al Public License.			
This text consists of three parts:				1
Part I: Some remarks regarding the license give	ven in			
Part II: The actual license that covers Wiresh	ark.			
Part III: Other applicable licenses.				
When in doubt: Part II/III is the legally bindin	g part, Part I is ju	st CPI v2		
there to make it easier for people that are no	t lamilar with the	GPLV2.		
1				
This is not an end user license agreement (EU	A). It is provided	here for inform	ational	
LET CROSSES CETTY.				
Papers (11)				
eshark® Installer				
eshark® Installer				

图 1.3 显示许可协议

单击 Noted 按钮,选择安装的组件,这里将所有的复选框都选中,如图 1.4 所示。

Choose Components			
Choose which features of Wire	shark 3.4.2 64-bit you want to install.		
The following components are	available for installation.		
Select components to install:	Vireshark V TShark V Plugins & Extensions V Documentation		
Space required: 199.6 MB	Description Position your mouse over a component to see I description.	ts	

图 1.4 选择安装的组件

单击 Next 按钮,显示其他任务,默认安装,如图 1.5 所示。

单击 Next 按钮,选择安装的路径,如图 1.6 所示。

单击 Next 按钮, Wireshark 需要 Npcap 或 WinPcap 来捕获实时网络数据,安装 Npcap 和 WinPcap,继续安装,如图 1.7 所示。

单击 Next 按钮,安装 USB Capture,如图 1.8 所示。

单击 Install 按钮,开始安装,如图 1.9 所示。

安装时跳出的窗口如图 1.10 所示,开始安装 Npcap 插件, Npcap 是 WinPcap 的改进版。

单击 I Agree 按钮,继续安装,如图 1.11 所示。

单击 Install 按钮,显示如图 1.12 所示。

网络攻防项目实战(微课视频版)



图 1.5 安装的任务

Wireshark 3.4.2 64-bit Setup	°		×
Choose Install Location			
Choose the folder in which to install Wireshark 3.4.2 64-bit.		1	
Choose a directory in which to install Wireshark.			
Destination Folder			
2:\Program Files\Wireshark	Brow	vse	
Space required: 199.6 MB			
Space available: 179.9 GB			
Wireshark® Installer			
Wireshark® Installer	Next >	Cano	el

图 1.6 选择安装的路径

Dealert Contern		
acket Capture		1
Wireshark requires either Npcap or WinPcap to capture live network	data.	Æ
Currently installed Npcap or WinPcap version		
WinPcap 4.1.3		
Install		
Install Npcap 1.00		
The currently installed WinPcap 4.1.3 may be uninstalled first.		
Get WinPcap		
Learn more about Npcap and WinPcap		
reshark@ Installer		
and the state of the second		

图 1.7 继续安装



Witeshark 5.4.2 04-bit Setup		-		×
USB Capture				-
USBPcap is required to capture USB traff (experimental)?	fic. Should USBPcap be ins	talled	2	
Currently installed USBPcap version				
USBPcap is currently not installed				
Install				
Install USBPcap 1.5.4.0				
(Use Add/Remove Programs first t	to uninstall any undetecte	d old USBPcap	versions)	
Important notice				
In case of issue after installation, plea https://github.com/desowin/usbpcap	ase use the system restor /issues/3	e point create	ed or read	
na ha dan ta kalina				
rresnankig installer				_

图 1.8 安装 USB Capture

stalling			
lease wait while Wireshark 3.4.2 64-bit is being installed.			
ixecute: "C:\Program Files\Wireshark\vcredist_x64.exe" /install /quie	t /norestar	t	
Extract: pdml2html.xsl			^
Extract: ws.css			
Extract: wireshark.html			
Extract: wireshark-filter.html			
Extract: dumpcap.exe			
Extract: dumpcap.html			
Extract: extcap.html			
Extract: ipmap.html			
Extract: vcredist_x64.exe 100%			
Execute: "C:\Program Files\Wireshark\vcredist_x64.exe" /install /qu	iet /norest	art	~
shark® Installer			_
	-	100	-

图 1.9 开始安装

0	License Agreement	talling N	ocan 1.00
NMAP. ORG	Piedse review the intense terms before ins	stalling N	pcap 1.00.
Press Page Down to see	the rest of the agreement.		
NPCAP COPYRIGHT / EN	D USER LICENSE AGREEMENT		^
Npcap is a Windows pad (c) 2013-2020 by Insecu reserved.	ket sniffing driver and library and is copyright re.Com LLC ("The Nmap Project"). All rights		
Even though Npcap sour not open source softwar permission from the Nma limited to installation on	ce code is publicly available for review, it is re and may not be redistributed without specia ip Project. The standard version is also five systems. We fund the Npcap project by	I	
If you accept the terms of agreement to install Npca	of the agreement, dick I Agree to continue. Yo up 1.00.	u must a	ccept the

图 1.10 安装 Npcap 插件





图 1.11 继续安装 Npcap 插件

Npcap 1.00 Setup	Finished Thank you for installing Npcap	-		×
Npcap has been install	ed on your computer. s wizard.			
Nullsoft Install System v2.51	< Back	Finish	Can	cel

图 1.12 完成 Npcap 插件的安装

单击 Finish 按钮,完成 Npcap 的安装。如图 1.13 所示,显示安装完成。

etup was completed successfully.			4
ompleted			
Extract caushade ave			
Extract: rawshark.html			
Output folder: C:\Program Files\Wireshark			
Extract: mmdbresolve.html			
Output folder: C:\Program Files\Wireshark			
Extract: mmdbresolve.exe			
Output folder: C:\Program Files\Wireshark			
Extract: user-guide.chm			
Extract: faq.html			- 11
Completed			~
N ARES STR			

图 1.13 显示安装完成



单击 Next 按钮, Wireshark 安装完成, 重启系统, 如图 1.14 所示。

Wireshark 3.4.2 64-bit Setup	- 🗆 ×
	completing Wireshark 3.4.2 64-bit setup wr computer must be restarted in order to complete the stallation of Wireshark 3.4.2 64-bit. Do you want to reboot w?
•) Reboot now
) I want to manually reboot later
	< Back Finish Cancel

图 1.14 安装完成,重启系统

1.4 Wireshark 基本应用

1. 界面介绍

打开 Wireshark 程序, Wireshark 3.4.2 启动界面如图 1.15 所示。

▲ Wireshark 网络分析器				
文件(F) 编辑(E) 视图(V)	凯特(G) 捕获(C) 分析(A) 统计(S)	电话(V) 无线(W) 工具(T) 幕助(H)		
4		9991		
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□				
	NAMES OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTIONO			
1	XXHURH #ireshark			
	插获			
	"使用这个过滤器: [目]输入拥获过滤器 …		* 显示所有捨口 *	
	本均连接*7 以士師			
	本地连接*8			
	本地连接*6			
	VMware Network Adapter VMnet1			
	VMware Network Adapter VMnet8	mm		
	Adapter for loopback traffic capture			
10	学习			
	User's Guide · Viki · Questions	and Answers · Mailine Lists		
	E在运行 Wireshark3.4.2 (v3.4.2-0-za889c)	[1b1b19] 接受自动更新。		
S 20				
2 已准备好加载或捕获			无分组	RE: Defealt

图 1.15 Wireshark 启动界面



1 号窗口是数据包列表,显示捕获的数据包,第一列为捕获的序列号,第二列为捕获的时间,第三列为源 IP 地址,第四列为目标 IP 地址,第五列为协议,第六列为长度,第七 列为说明信息。

2 号窗口是数据包详细信息,在1 号窗口数据包列表中选择指定数据包,在2 号窗口 数据包详细信息中会显示数据包的所有详细信息内容。数据包详细信息是非常重要的, 可用来查看协议中的每一个字段。各行信息分别说明如下。

(1) Frame: 物理层的数据帧概况。

(2) Ethernet Ⅱ:数据链路层以太网帧头部信息。

(3) Internet Protocol Version 4:网络层 IP 包头部信息。

(4) Transmission Control Protocol: 传输层的数据段头部信息,此处是 TCP。

(5) Hypertext Transfer Protocol:应用层的信息,此处是 HTTP。

3 号窗口是1 号窗口中选定的数据包字节区,其中左侧是十六进制表示,右侧是 ASCII 码表示。另外,在2 号窗口中选中某层或某字段,3 号窗口对应位置也会被高亮。



图 1.16 抓包结果

2. 设置数据列表颜色

从图 1.16 看到,数据包列表中不同的协议功能使用了不同的颜色区分。如需更改颜 色,选择菜单栏"视图(V)"→"着色规则",选择某个规则,使用下面的按钮更改前景色和 背景色,如图 1.17 所示。

3. 设置网卡

如需重新选择网卡,应选择菜单栏"捕获(C)"→"选项",打开"捕获选项"对话框,在 Input 选项卡中选择网卡后,单击"开始"按钮,开始抓包,如图 1.18 所示。



nalysis.flags && Itcp.analysis.window_update && Itcp.analysis.keep_alive && Itcp.analysis.keep_alive_ack state != 8 && hsrp.state != 16 /pe == 0x80 msg != 1
state != 8 && hsrp.state != 16 /pe == 0x80 msg != 1
/pe == 0x80 msg != 1
msg != 1
type eq 3 icmp.type eq 4 icmp.type eq 5 icmp.type eq 11 icmpv6.type eq 1 icmpv6.type eq 2 icmpv6.type
icmpv6
ags.reset eq 1
chunk_type eq ABORT
dst == 224.0.0.0/4 && ip.ttl < 5 && pim && lospf) (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1
:s.status=="Bad" ip.checksum.status=="Bad" tcp.checksum.status=="Bad" udp.checksum.status=="Bad" sctp.
nbss nbns netbios
tcp.port == 80 http2
pc
eigrp ospf bgp cdp vrrp carp gvrp igmp ismp
ags & 0x02 tcp.flags.fin == 1
] & 1
md_journal sysdig
AGRO.
过速器应用

图 1.17 数据包列表中颜色的设置

ξ Π	Traffic	Link-layer Header	混杂	捕获长居	缓冲区(监控机	捕获过清醒	6	
本地连接*7		Ethernet		默认	2	<u></u>			
以太网		Ethernet		默认	2				
本地连接* 8		Ethernet		默认	2	_			
本地连接*6		Ethernet		默认	2				
VMware Network Adapter VMnet1		Ethernet		默认	2				
VMware Network Adapter VMnet8		Ethernet		默认	2	_			
Adapter for loopback traffic capture	re	BSD loopback		默认	2	-			

图 1.18 更换网卡抓包

4. 显示过滤器

在捕获时未设置捕获规则直接通过网卡抓取所有数据包,如图 1.19 所示,可看到抓 取了所有协议的数据包。

显示过滤器用于在抓取数据包后设置过滤条件,从而过滤数据包。通常在抓取数据

▲ "以太月				7	D X
文件图 编辑图 短期区	MALE CHING (A)THE CURRE (D)MA	无线(业) 工具(土) 制物(土)			
	0 • • • · · · · · · · · · · · · · · · ·	e, 11			
■ 应用显示过透器 ··· 《trl-/	0				+
Be. Time	Source	Destination	fratoral 1	length Info	^
11399 1172.150640	192.168.3.2	40.119.211.203	TLSv1.2	153 Application Data	
11400 1172.254998	40.119.211.203	192.168.3.2	TLSv1.2	223 Application Data	
11401 1172.299196	192,168.3.2	40.119.211.203	TCP	54 59757 + 443 [ACK] Seq=2571 Ack=5005 Win=130048 Len=0	
11402 1173.089145	192,168.3.2	124.238.251.101	TCP	55 [TCP Keep-Alive] 59786 + 443 [ACK] Seq=1715 Ack=8504 Win=130048 Len=1	
11403 1173.095502	124.238.251.101	192.168.3.2	TCP	66 [TCP Keep-Alive ACK] 443 - 59786 [ACK] Seq-8504 Ack-1716 Win-16896 Len-0 SLE-1715 SRE-17	16
11404 1174.013248	HummeiTe_2d:b9:55	Spanning-tree-(for-,	STP	68 Conf. Root = 32768/0/e8:cd:2d:2d:59:55 Cost = 0 Port = 0x8001	
11405 1176.013274	HummelTe_2d:b0:55	Spanning-tree-(for	. 5TP	50 Conf. Root = 32768/0/e8:cd:2d:2d:b9:55 Cost = 0 Port = 0x8001	- 8
11486 1176.459685	101.199.113.94	192.168.3.2	TCP	60 [TCP Keep-Alive] 80 + 59782 [ACK] Seq=272 Ack=281 Win=30336 Len=0	
11407 1176.459635	192.168.3.2	101.199.113.94	TCP	54 [TCP Keep-Alive ACK] 59782 + 80 [ACK] Seq-281 Ack-273 Win-130816 Len-0	
11488 1177.186257	192.168.3.2	192.168.3.1	DNS	89 Standard query 0x362e A v10.events.data.microsoft.com	
11409 1177.198773	192.168.3.1	192.168.3.2	DNS	207 Standard query response 0x362e A v10.events.data.microsoft.com CNAME global.asimov.event:	s.data
11410 1177, 199214	192.168.3.2	52.114,133.61	TCP	66 59787 + 443 [SYN] Seq=0 Min=64240 Len=0 MSS=1460 MS=256 SACK_PERM=1	
11411 1177.440212	52.114.133.61	192.168.3.2	TCP	66 443 + 59787 [5YN, ACK] Seq-0 Ack-1 Win-65535 Len-0 M55-1412 W5-256 SACK_PERM-1	
11412 1177.440269	192,168.3.2	52.114.133.61	TCP	54 59787 + 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0	
11413 1177.448522	192.168.3.2	52.114.133.61	TLSv1.2	262 Client Hello	÷
 Ethernet II, Src: H Internet Protocol V Transmission Contro Hypertext Transfer 	P_2f:74:c0 (04:0e:3c:2f:74:c0), Dr Version 4, Src: 192.168.3.2, Dst: 1 al Protocol, Src Port: 59800, Dst F Protocol	st: HuaweiTe_2d:b9:55 (124.238.251.101 Port: 80, Seq: 1, Ack:	(e8:cd:2d: 1, Len: 3	24:99:55) 23	
> GET /t0122249ade	ac950c0b.ico HTTP/1.1\r\n				
Host: p0.qhimg.c	om/r/n				
Connection: keep	-alive\r\n				
User-Agent: Mozi	11a/5.0 (Windows NT 10.0; WOW64) A	ppleWebKit/537.36 (KHT	ML, 11ke 6	ecko) Chrome/78.0.3904.108 Safar1/537.36\r\n	
Doront' Imade/we	An Image/anne Image/* */**AHA Rini				
0050 63 6f 20 48 54	54 50 2f 31 2e 31 6d 8a 48 6f 73	co HTTP/ 1.1 - Pos			^
0050 74 30 20 70 30 0070 31 43 6f 6a 6a	45 53 74 59 56 5e 3e 29 5b 55 55	Connect ion: kee			
0000 78 2d 61 6c 69	76 65 8d 8a 55 73 65 72 2d 41 67	p-alive User-Ag			
0090 65 6e 74 3a 20	4d 6f 7a 69 6c 6c 61 2f 35 2e 30	ent: Moz illa/5.0			
00a0 20 28 57 69 6e	64 6f 77 73 20 4e 54 20 31 30 2e	(Window s NT 10.			
00b0 30 3b 20 57 4f	57 36 34 29 20 41 70 70 6c 65 57	0; WOW64) AppleW			v
O Z MITT Kost Chity hes	st). 20 byte(s)			分组: 25210 · 已豐示: 25210 (108.0%) [23	t Defult

图 1.19 抓取所有数据包

包时设置条件相对宽泛,抓取的数据包内容较多时,使用显示过滤器设置条件过滤,以方 便分析,如果只抓取 TCP 的数据包,则在显示过滤器中输入 TCP,如图 1.20 所示。

2700 MBD MBD <td< th=""><th>A titte</th><th></th><th></th><th></th><th>- 0</th><th>×</th></td<>	A titte				- 0	×
Image Image <t< th=""><th>文件图 编辑图 探测区</th><th>(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)</th><th>无线的 工具① 制物团</th><th></th><th></th><th></th></t<>	文件图 编辑图 探测区	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	无线的 工具① 制物团			
Imp Description Description as Tries Server. Description Description Description 11370 11370.085776 180.163.342.72 192.164.3.2 TCP 166.439 59795 AdX Seqr-3096 Ack-358 Min-30664 Len-9 11372 11372.1317.082541 50.58.2 101.199.113.94 TCP 166.439 59795 AdX Seqr-3096 Ack-358 Min-3066 Len-96 11373 1137.02545 50.99.170.110 192.165.3.2 TCP 60.443 59797 [AdX Seqr-313 Ack-1408 Min-3256 Len-9 11374 11374.02546 50.99.170.110 192.165.3.2 TCP 166.443 59797 [AdX Seqr-313 Ack-1408 Min-3256 Len-94 11375 11374.02546 50.99.170.110 192.166.3.2 TCP 166.443 59797 [AdX Seqr-313 Ack-1408 Min-3256 Len-142 TCP segment of a reassembled POU] 11377 11374.09464 50.99.170.110 192.166.3.2 TCP 1466.443 59797 [AdX Seqr-406 Ack-318 Min-3107 Len-142 TCP segment of a reassembled POU] 11378 1137.09467 50.99.170.110 192.166.3.2 TCP 1466.443 59797 [AdX Seqr-406 Ack-318 Min-31072 Le	A COLOR	B 4 + + G 7 ± 3 ■ 4 4	6, <u>Ⅲ</u>			
Image Description Description <thdescription< th=""> <thdescription< th=""> <thde< th=""><th>tep</th><th></th><th></th><th></th><th>80</th><th>•+</th></thde<></thdescription<></thdescription<>	tep				80	•+
11870 1372,085774 180.16.3,242.72 192.168.3.2 TCP 60.403 595782 + 80 [5%], KAX [Seq=40.84A:-5373 Hun-130864 Len-0 11871 1372,03574 192.168.3.2 156,99.170.110 TCP 55.99782 + 80 [5%], KAX [Seq=47.84A:-5473 Hun-130816 Len-0 11873 1373,042418 192.168.3.2 156,99.170.110 TCP 55.99782 + 80 [5%], KaX [Seq=47.84A:-5478 Hun-130816 Len-0 11875 1317,04545 156,99.170.110 192.168.3.2 TCP 60.43 - 59782 [5%], KaX-577 Hun-15222 Len-0 11875 1317,04457 156,99.170.110 192.168.3.2 TCP 166.43 + 59798 [AX] Seq=47.84 A:-4408 Hun-3225 Len-142 [TCP segment of a reassembled POU] 11875 1317,04467 56,99.170.110 192.168.3.2 TCP 166.43 + 59799 [AX] Seq=7665 A:-1405 Hun-3256 Len-1412 [TCP segment of a reassembled POU] 1187 1317,04467 56,99.170.110 192.168.3.2 TCP 166.43 + 59799 [AX] Seq=7665 A:-1405 Hun-3256 Len-1412 [TCP segment of a reassembled POU] 1187 1317,04457 56,99.170.110 192.168.3.2 TCP 165.431 + 59799 [AX] Seq=7466 A:-1405 Hun-3256 Len-1412 [TCP segment of a reassembled POU] 1187 1317,04457 56,99.170.110 192.168.3.2 TCP 169.431 + 59799 [AX] S	No. Time	Source	Jestination	Protocol.	Length Iafo	~
11871 137, 038572 192,163.2 101,199.113.94 TCP 159 5782+ 480 [Psi, ACX] Seq-409 Ack-337 kin-130616 Len=0 11872 137, 042545 35.99,170.110 192,163.3.2 TCP 60 431 - 5979 [ACX] Seq-409 Ack-4732 kin-130616 Len=0 11873 137, 042545 35.99,170.110 192,163.3.2 TCP 60 431 - 5979 [ACX] Seq-403 [AcX-1408 kin-32356 Len=-0 11873 137, 042545 35.99,170.110 192,163.3.2 TCP 60 431 - 5979 [ACX] Seq-473 [Act-1408 kin-32356 Len=-142 11875 137, 072894 101,199.113.94 192,163.3.2 TCP 166 433 - 5979 [ACX] Seq-473 [Act-1408 kin-32356 Len=-142 11875 137, 09467 35.99,170.110 192,163.3.2 TCP 166 433 - 5979 [ACX] Seq-473 [Act-1408 kin-3256 Len=142 [TCP segment of a reassembled P00] 11875 137, 09467 35.99,170.110 192,163.3.2 TCP 1466 443 - 5979 [ACX] Seq-4703 [Act-1408 kin-3256 Len=142 [TCP segment of a reassembled P00] 11875 137, 09467 35.99,170.110 192,163.3.2 TCP 1456 443 - 5979 [ACX] Seq-498 Act-348 kin-3162 Len=0 11885 137,1704505 192,163.3.2 TCP 1456 443 - 5979 [ACX] Seq-498 Act-318 kin-13107 Len=0 11885 137,11422 192,153.3.2 192,163.3.2 TCP 54 59789 - 443 [ACX] Seq-406 Act-318 kin-13107 Len=0 11885 1337,11422 19	11870 1317.036776	180.163.242.72	192.168.3.2	TCP	60 443 + 59795 [ACK] Seq=5306 Ack=1568 Win=33664 Len=0	
11872 1317,042411 192,168.3.2 36,99.170.110 TCP 54 5979 / 443 [AcX] Seq-1466 Act-4781 Min-120816 Lem-0 11873 1317,066807 110.161.327.176 192,168.3.2 TCP 60 433 - 5979 [AcX] Seq-178 (AcX) Seq-178	11871 1317.038572	192.168.3.2	101.199.113.94	TCP	150 59782 + 80 [PSH, ACK] Seg=409 Ack=337 Win=130816 Len=96	
11873 137,04254 36.99,170.10 192.168.3.2 TCP 60 433 - 9379 [ACK] Seq-473 Act-1408 Min-3235 Lem-0 11874 137,07284 101.199.113.34 192.168.3.2 TCP 60 433 - 9379 [ACK] Seq-473 Act-1408 Min-3235 Lem-12 11875 137,07284 101.199.113.34 192.168.3.2 TCP 60 433 - 9379 [ACK] Seq-473 Act-1408 Min-3255 Lem-142 11875 137,07284 101.199.113.34 192.168.3.2 TCP 166 433 - 9379 [ACK] Seq-473 Act-1408 Min-3255 Lem-142 11875 137,09447 36.99,170.10 192.168.3.2 TCP 1466 433 - 9379 [ACK] Seq-473 Act-1408 Min-3255 Lem-142 [TCP segment of a reassembled POU] 11875 137,09447 36.99,170.10 192.168.3.2 TCP 1466 433 - 9379 [ACK] Seq-473 Act-1408 Min-3256 Lem-142 [TCP segment of a reassembled POU] 11878 137,09446 36.99,170.10 192.168.3.2 TCP 1466 433 - 9379 [ACK] Seq-4708 Act-1408 Min-3256 Lem-142 [TCP segment of a reassembled POU] 1187 137,09446 36.99,170.10 192.168.3.2 TCP 1466 433 - 9379 [ACK] Seq-4708 Act-1408 Min-31072 Lem-0 1188 137,17097 192.168.12 100.157 137.061 1188 137,14229 192.168.3.2 190.161.262.72 150.12 100.157 137.061 100.157 137.061 1188 137,714620 192.168.3.2 191.199.113.94 TCP 54 59789 - 40 [ACK] Seq-40 Act-318 Min-1306 Lem-0 155.146 Min 140.146 Min 140.146 Min 140.146 Min 140.146 Min 140.146 M	11872 1317.042418	192.168.3.2	36.99.170.110	TCP	54 59799 - 443 [ACK] Seg-1406 Ack-4781 Win-130816 Len-0	
1187 1317,0060007 100.163.27.776 192.163.3.2 TCP 60.43 - 59708 [DK] Seq-157 Ack-57 Win-15222 Len-0 11875 1317,004467 36.99,170.110 192.163.3.2 TCP 106.64 03 + 59708 [DK] Seq-157 Ack-56 Win-32056 Len-142 [TC segment of a reassembled POU] 11876 1317,004467 36.99,170.110 192.163.3.2 TCP 1066 43 + 59708 [DK] Seq-053 Ack-160 Win-32256 Len-142 [TC segment of a reassembled POU] 11877 1317,004467 36.99,170.110 192.163.3.2 TCP 1066 43 + 59708 [DK] Seq-053 Ack-1405 Win-32256 Len-142 [TC segment of a reassembled POU] 11879 1317,004467 36.99,170.110 192.163.3.2 TCP 1666 431 + 59708 [DK] Seq-053 Ack-1405 Win-32256 Len-142 [TC segment of a reassembled POU] 11879 1317,004467 36.99,170.110 TCP 54 59709 ACK] Seq-0466 Ack-9188 Win-131072 Len-0 1182 1317.102477 123.163.12 105.124.272 TLS/1.2 128 Application Data 1188 1317,104237 192.166.3.2 108.152.24 101.199.113.34 TCP 56 5980 + 5080 [SM] Seq-04 Min-54240 Len-0 MS5-1460 K5-555 SACK (FSM-1 1188 1317,104237 192.166.3.2 108.199.133.34 TCP 56 9980 + 508 [SM] Seq-04 Min-54240 Len-0 MS5-1412 SACK (FSM-1 108.199.112.04 108.199.112.04 108.199.113.04 108.199.11	11873 1317.042545	36.99.170.110	192.168.3.2	TCP	60 443 + 59799 [ACK] Seq-4781 Ack-1405 Win-32256 Len-0	
1187:137.072894 101.197.131.94 192.168.3.2 TCP 16.00.04 + 0.00.0000 (Lem-122) 1187:0137.072894 101.097.113.94 192.168.3.2 TCP 16.00.04 + 0.0000 (Lem-122) 101.07.01.0000 (Lem-122) 1187:0137.094467 36.99.170.110 192.168.3.2 TCP 16.00.04 + 0.0000 (Lem-122) 100.0000 (Lem-122) </td <td>11874 1317.060807</td> <td>180.163.237.176</td> <td>192.168.3.2</td> <td>TCP</td> <td>60 443 + 59798 [ACK] Seg=157 Ack=577 Win=15232 Len=0</td> <td></td>	11874 1317.060807	180.163.237.176	192.168.3.2	TCP	60 443 + 59798 [ACK] Seg=157 Ack=577 Win=15232 Len=0	
1187:137.094467 36:09.170.10 192.168.3.2 TCP 1466 43 + 9799 [ACK] Seq-4781 Act-1408 Min-3225 Lem-142 [TCP segment of a reassembled POU] 1187:7137.094467 36:09.170.10 192.168.3.2 TCP 1466 43 + 9799 [ACK] Seq-4781 Act-1408 Min-3225 Lem-142 [TCP segment of a reassembled POU] 1187:7137.094467 36:09.170.10 192.168.3.2 TCP 1466 43 + 9799 [ACK] Seq-1608 Act-1408 Min-3225 Lem-1412 [TCP segment of a reassembled POU] 1187:7137.094467 36:09.170.10 192.168.3.2 TCP 1466 43 + 9799 [ACK] Seq-160 Act-0188 Min-3225 Lem-1412 [TCP segment of a reassembled POU] 1189:137.109457 192.168.3.2 1157.122.72 125.40.1.2 180 Application Data 1188:137.109457 192.168.3.2 100.157.242.77 175.1.2 180 Application Data 1188:137.11023 192.168.3.2 101.199.113.94 TCP 56 39900 + 80 [SVR] Seq-408 Kin-5428 (Lem-40 KS-1412 SACK /PEM+1 KS-512 1188:137.11024 192.383.251.101 TCP 56 39900 + 80 [SVR] Seq-478 KAC3-69 Min-308016 Lem-0 1188:137.11024 192.383.251.101 TCP 56 39900 + 80 [SVR] Seq-478 KAC3 Seq-478 KAC3 (Seq-142 SACK /PEM+1 KS-512 1188:137.11024 192.168.3.2, DT: 124.238.251.101 TCP 56 39 5900 (Se 0 KT /STR) /SE (Se 0 KT /STR) /SE (SE (SE /STR) /SE (SE /STR) /SE (SE /STR) /SE	11875 1317.072894	101.199.113.94	192.168.3.2	TCP	86 88 + 59782 [PSH, ACK] Seq=337 Ack=585 Win=38336 Len=32	
11877 1317,094467 36.99,170.110 192.168.3.2 TCP 1466 431 + 9799 [ACK] Seq-705 3A ct-1468 Min-32256 Lem-1412 [TCP segment of a reassembled POU] 11878 1317,094467 36.99,170.110 192.168.3.2 TCP 1466 431 + 9799 [ACK] Seq-705 Act-1468 Min-32256 Lem-1412 [TCP segment of a reassembled POU] 11889 1317,094467 36.99,170.110 192.168.3.2 TCP 1466 431 + 9799 [ACK] Seq-705 Act-1468 Min-32256 Lem-1412 [TCP segment of a reassembled POU] 11880 1317,09550 192.168.3.2 159.970.10 192.168.3.2 TCP 1466 431 + 9799 [ACK] Seq-706 Act-1408 Min-32256 Lem-1412 [TCP segment of a reassembled POU] 11880 1317,09550 192.168.3.2 109.170.10 TCP 54 59792 + 043 [ACK] Seq-106 Act-108 Min-11072 Lem-0 11885 1317,14621 192.168.3.2 110.199.113.94 TCP 54 59702 + 043 [ACK] Seq-106 Act-306 Min-310821 Lem-0 11885 1317,11822 192.168.3.2 TCP 166 80 = 59800 [SN, ACK] Seq-06 Act-306 Min-310821 Lem-0 155.101 11885 1317,11822 192.168.3.2 TCP 56 80 = 59800 [SN, ACK] Seq-06 Act-306 Min-310821 Lem-0 155.102 165.123 LSA 2SI 100 11885 1317,11824 192.168.3.2 TCP 168 80 = 59800 [SN, ACK] Seq-06 Act-306 Min-310821 Lem-0 155.102 SACK_PEM+1 Mc-512 1186 1317,11626 192	11876 1317.094467	36.99.170.110	192.168.3.2	TCP	1466 443 + 59799 [ACK] Seq-4781 Ack-1406 Win-32256 Len-1412 [TCP segment of a reassembled PDU]	10 A
11879 1317,094467 36.99.170.10 192.168.3.2 TCP 1466 434 - 90.979 [Ack] Seq-7468 Ac-1405 Min-32256 Lem-1412 [TCP segment of a reassembled PDU] 11879 1317,09457 192.168.3.2 TCP 165 431 - 90.979 [Ack] Seq-7468 Ac-1405 Min-32256 Lem-1412 [TCP segment of a reassembled PDU] 11880 1317,09457 192.168.3.2 TCP 154 5979 - 441 [Ack] Seq-1406 Act-9188 Min-32256 Lem-1412 [TCP segment of a reassembled PDU] 11880 1317,109457 192.168.3.2 TCP 54 5979 - 441 [Ack] Seq-1406 Act-9188 Min-32256 Lem-1412 [Ack PEB+1 11880 1317,109477 192.168.3.2 TCP 56 309 - 90 [SNR] Seq-0 Min-6428 Lem-0 MS-1464 Kd-855 SGK [FEB+1 11885 1317,11240 120.168.3.2 101.199.113.94 TCP 56 309 - 900 [SNR] Seq-0 Min-300816 Lem-0 11885 1317,11240 120.120.3.2 101.199.113.94 TCP 56 00 + 59002 (SNR, Ack] Seq-046 Kd-85 SGK [FEB+1 11885 1317,11240 120.120.3.2 102.168.3.2 TCP 56 00 + 59002 (SNR, Ack] Seq-046 Kd-85 SGK [FEB+1 11885 1317,11240 120.120 (Min-32), ST Dytes captured (MB16 bits) on Interface (Dev/CoVMF_[189627F8-F08F-4752-8378-62F9077IAC6E], 1d 0 1 11885 1317,11240 120 (Min-32), SC Dyte: 124,238,251.101 Termintsion famme/fox data data data data data data data dat	11877 1317.094467	36.99.170.110	192.168.3.2	TCP	1466 443 + 59799 [ACK] Seq=6193 Ack=1486 Win=32256 Len=1412 [TCP segment of a reassembled POU]	
11879 137,094440 96.99.170.10 192.168.3.2 TLSN.1.2 225 Application Data 11880 137,095320 192.168.3.2 TLSN.1.2 225 Application Data 11880 137,095320 192.168.3.2 TLSN.1.2 128 Application Data 11880 137,095320 192.168.3.2 TLSN.1.2 188 Application Data 11881 137,146230 192.168.3.2 118.151,242.72 TLSN.1.2 188 Application Data 11881 1317,146240 192.168.3.2 118.151,341 TCP 55 59800 + 20 (XS) Seq-04 Kn-45240 Len-0 MS5-1460 K5-256 SACK PEBH-1 11885 1317,146240 192.168.3.2 119.199.113.94 TCP 55 59800 (SN, ACK) Seq-04 Kn-45240 Len-0 MS5-1462 KoC, PEBH-1 K5-512 11885 1317,146240 192.168.3.2 TCP 56 80 = 59800 (SN, ACK) Seq-04 Kn-45240 Len-0 MS5-1462 KoC, PEBH-1 K5-512 11885 1317,116240 192.168.3.2 TCP 56 80 = 59800 (SN, ACK) Seq-04 Kn-4528 Min-138051 Len-0 11885 1317,116240 192.174.60 (Mides)::::::::::::::::::::::::::::::::::::	11878 1317.094467	36.99.170.110	192.168.3.2	TCP	1466 443 + 59799 [ACK] Seg-7605 Ack-1405 Win-32256 Len-1412 [TCP segment of a reassembled PDU]	
11880 1317,094552 192,168.3.2 106,99.170.110 TCP 54 59799 - 443 [Ack] Seq-1486 Act-9188 Min-318672 Len-0 11882 1317,109477 192,168.3.2 106,1242,72 115,124,22 TLSY,12 1188 Application Data 11884 1317,109477 192,168.3.2 124,238,251.101 TCP 65 59800 + 80 [SMR] Seq-06 Min-30861 Len-0 HSS-1460 Ke-255 SACK PE8H-1 11885 1317,1172421 129,218.3.2 124,238,251.101 TCP 65 59800 + 59000 [SMR, ACK] Seq-06 Min-30861 Len-0 11885 1317,117240 124,238,251.101 192.165.3.2 TCP 65 80 + 59000 [SMR, ACK] Seq-06 Act-308 Min-30861 Len-0 11895 1317,117640 144,238,251.101 192.165.3.2 TCP 65 80 + 59000 [SMR, ACK] Seq-06 Act-308 Min-30861 Len-0 11895 1317,117640 144,238,251.101 192.165.3.2 TCP 65 80 + 59000 [SMR, ACK] Seq-06 Act-3186 Len-0 11895 1317,21021 192,165.3.2 Dsr: 124,238,251.101 192.165.3.2 192.168.1.2 1 Transmission Control Protocol, Scr Dert: 59000, Dsr Dert: 80, Seq: 1, Ack: 1, Len: 323 Yhpertext Transfer Protocol. Yhpertext Transfer Protocol. Yhpertext Transfer Protocol. Seq: 41,445,459,27,315,400 TCP 148 Get 6, 65 50 76, 96 Get 6, 17 7,36 Get 6, 17 7,37,36 (GHR, 11 Me, 14,400 Safar1/537,36/r/n	11879 1317.094467	36.99.170.110	192.168.3.2	TLSv1.2	225 Application Data	
11882 1317,105386 190,168.3.2 180,163,242.72 TLSY.1.2 180 Application Data 11884 1317,119477 102,168.3.2 120,168.3.2 120,168.3.2 120,168.3.2 11885 1317,114629 102,168.3.2 120,168.3.2 120,169.4 120,169.4 120,169.4 11885 1317,114629 102,268.3.2 101,199,113.94 TCP 56 59800 + 50 [SN, ACK)56 Him-16260 Lem-0 HSS-1460 LSS (K, PERH-1 11885 1317,114629 104,238.251.101 192,168.3.2 TCP 56 80 - 59800 [SN, ACK)56 Him-1660 Lem-0 HSS-1412 SACK PERH-1 KS-512 1 Termer TLR Sec: H2,268.3.2 102,159.5 (Ei:cd:22:25:1.0) Sec=0 Min-16200 Lem-10 HSS-1412 SACK PERH-1 KS-512 1 Termer TLR Sec: H2,268.3.2, Det: 120,268.3.2, Det: 120,268.3.2, Det: 120,268.3.2, Det: 120,268.3.2, Det: 120,268.3.2, Det: 120,278.4.2.3.2, Det: 120,278.4.2.3.2.3.1.101 Paramission Control Perstool, Sec Pert: 59800, Det Pert: 80, Seq: 1, ACK: 1, Len: 323 * paratission Control Perstool, Isson Paris Seq: 1, ACK: 1, Len: 323 * * * paratission Control Perstool, Isson Paris Seg: 1, ACK: 1, Len: 323 * * * paratission Control Perstool, Isson Paris Seg: 1, ACK: 1, Len: 323 * * * * Sef: roble: 20,070,070,070,070,070,070,070,070,070,0	11880 1317.094552	192.168.3.2	36.99.170.110	TCP	54 59799 + 443 [ACK] Seg=1406 Ack-9188 Win~131072 Len=0	
1184 1317, 198477 192,168.3.2 124,238,251.101 TCP 66 59808 - 98 [SMR] Seq=6 Min-42046 Len-0 HSS-1466 HS-255 SACK PE8H-1 1185 1317,117640 124,238,251.101 192.168.3.2 TCP 66 59808 - 59808 [SMR] Seq=6 Min-32081 En-0 11886 1317,117640 124,238,251.101 192.168.3.2 TCP 66 8980 - 59808 [SMR] Seq=6 Min-32081 En-0 11886 1317,117640 124,238,251.101 192.168.3.2 TCP 66 80 - 59808 [SMR] Seq=6 Min-32081 En-0 11886 1317,117640 124,238,251.101 192.168.3.2 TCP 66 80 - 59808 [SMR] Seq=6 Min-32081 En-0 11886 1317,117640 124,238,251.101 192.168.3.2 TCP 66 80 - 59808 [SMR] Seq=6 Min-32081 En-0 11886 1317,117640 124,238,251.101 192.168.3.2 Nit 124,238,251.101 192.168.2718-7887-425907714G61; 14 0 11886 1317,117640 Seq.11,2,2,38,251.101 192.168.3.2 Nit 124,238,251.101 192.168.2718-425907714G61; 14 0 11886 1317,117640 Seq.11,2,2,38,251.101 192.168.3.2 Nit 124.238,251.101 192.168.2718-425907714G61; 14 0 11885 1387,1187,1187 International International Internation International Internation International Internation Intern	11882 1317.105306	192.168.3.2	180.163.242.72	TLSv1.2	180 Application Data	
11885 1337.114620 192.168.3.2 101.199.113.94 TCP 54 59782 Ack-369 Min-138816 Lem-0 11886 1337.114640 124.238.251.101 192.168.3.2 TCP 56 80 = 59900 [SNH, ACK] Seq-0 Ack-369 Min-138816 Lem-0 11886 1337.114640 124.238.251.101 192.168.3.2 TCP 56 80 = 59900 [SNH, ACK] Seq-0 Ack-369 Min-138816 Lem-0 1 Thream 1188: 377 bytes on wire (3016 bits), 377 bytes captured (3016 bits) on interface (Device/WPF_[18962776-780-742-8376-62900771AC66], 16 0 10 1 Thream 1188: 377 bytes on wire (3016 bits), 377 bytes captured (3016 bits) on interface (Device/WPF_[18962776-780-742-8376-62900771AC66], 16 0 10 1 Thream 1188: 377 bytes on wire (3016 bits), 377 bytes captured (3016 bits) on interface (Device/WPF_[18962776-780-782-8376-62900771AC66], 16 0 10 1 Thream 1186 tem-0 TCP 56 80 - 59000 [SNH, ACK] Seq-0 Ack-10 Min-1366-12500771AC66], 16 0 1 Thream 1285: 377 bytes on wire (3016 bits), 377 bytes captured (3016 bits) on interface (Device/WPF_[18962776-780-786-62900771AC66], 16 0 10 1 Thream 1285: 100 Threat for Protocol, Scc Prot: 59800, Dt Prot: 80, Seq: 1, ACk: 1, Len: 32 TCP 10 1 Start and proting capture (Coll Coll Coll Coll Coll Coll Coll Col	- 11884 1317.109477	192.168.3.2	124.238.251.101	TCP	66 59800 + 80 [SYN] Seg-0 Win-64240 Len-0 MSS-1460 WS-256 SACK PERM-1	
11886 1317.117640 124.238.251.101 192.168.3.2 TCP 66 80 - 59000 [51%, ACK] Seque A.ck-1 Min-14600 Lem-0 MSS-1412 SACK_FEM-1 MS-512 > Frame 11888: 377 bytes on wire (3816 bits), 377 bytes captured (3016 bits) on interface \Device\Dev	11885 1317.114232	192.168.3.2	101.199.113.94	TCP	54 59782 + 80 [ACK] Seg=505 Ack=369 Win=130816 Len=0	
<pre>> Frame 11888: 377 bytes on wire (3816 bits), 377 bytes captured (3816 bits) on interface \Device\UPF[189627F8-F88F-4752-8378-62F90771AC66], 18 8 > (thermet Ti, Src: 19, 246.7Ac6 (04:0e); 2;;77:7A:00), Dst: HammalTi_23109:55 (ds:(ds:2d:2d:2d:09:55))) Internet Frotocol Version 4, Src: 192.168.7As, Dst: 12.23.82.32.31.81 > Internation Control Protocol, Src Port: 59680, Dst Port: 88, Seq: 1, Ack: 1, Len: 323 >> (ds: 120248/selex.596c08.Lice MTP/1.1v/n Nost: pd:_pdimg.com\v/n Connection: keep-alive\v/n Connection: keep-alive</pre>	11886 1317.117640	124.238.251.101	192.168.3.2	TCP	66 80 + 59800 [SYN, ACK] Seg=0 Ack=1 Win=14600 Len=0 MSS=1412 SACK PERM=1 WS=512	ų
Connection: kees-alive\r\n User-Agent: (kindows NF 10,0;) k00454) ApplekiebK1r5/37.36 (0H704, 11ke Gecko) Chrome/78.0.3904.108 Safar1/537.36 (r\n 056: 36:57:06 24:55:45:05:07 26:07 Connection: kee 0000 70:24:05:16:07:00 07:27:16:07 06:06:17 Connection: kee 0000 70:24:05:16:07:00 07:27:16:07 06:05:17 Connection: kee 0000 70:24:05:16:07:00 07:27:16:07 06:00:17 Connection: kee 0000 70:24:05:16:07:00 07:25:20:01 Connection: kee 0000 70:24:05:16:07:20:01 07:25:20:01 Connection: kee 0000 70:26:16:07:05:00:01 07:20:01:07:00 07:20:01:07:00 07:20:01:07:00 0000 70:26:05:07:05:00:01:07:01:00:01 07:00:01:00:01 07:00:00:00:01 07:00:00:00:00:00:00 0000 70:20:05:07:07:00:00:00:00:00:00:00:00:00:00:00:	 > Frame 11888: 377 by > Ethernet II, Src: F > Internet Protocol V > Transmission Contre > Hypertext Transfer > GET /t0122249ade Host: p0.qhimg.c 	<pre>/tes on wire (3016 bits), 37/ byte (P_2f;74:c0), D fersion 4, Src: 192.168.3.2, Dst:)] Protocol, Src Port: 59800, Dst (Protocol ac598c0b.ico HTTP/1.1\r\n om\r\n</pre>	: captured (3016 bits) it: HuaweITe_2d:b9:55 (124.238.251.101 'ort: 80, Seq: 1, Ack:	on interf (e8:cd:2d: 1, Len: 3	ace (Device(WPF_[11992/H=H08+-4752-8578-62H90/71AC6E], 18 0 2019555) 223	
User-Agent: Nor111a/5.0 (Hindows NT 10.6; NOR64) AppleWebK1(75)7.3 (DHTM, 11ke Gecko) Chrome/78.8.3904.108 Safar1/537.36\r\n Accent: Tassachenh Tassachen T	Connection: keep	-alive\r\n				
International Control Internation (Free Action of Control Internati	User-Agent: Mozi	11a/5.0 (Windows NT 10.0; WOW64) A	ppleWebKit/537.36 (KHT	ML, like	Gecko) Chrome/78.0.3904.108 Safari/537.36\r\n	
00596 63 67 20 45 54 59 7 31 04 64 54 57 7	Accent: image/we	hn image/anne image/* */*-o=A Riri	n			~
1000 20 20 20 20 20 20 20 20 20 20 20 20	0050 63 6f 20 48 54 0060 74 3a 20 70 30 0070 3a 43 6f 6e 6e 0080 70 2d 6f 6e 6e 0090 65 6e 74 3a 20 0090 65 6e 74 3a 20 0090 65 6e 74 3a 20	54 50 2f 31 2e 31 0d 0a 48 6f 73 2e 71 88 69 5d 67 2e 63 6f 6d 0d 65 63 74 69 6f 6e 3a 20 6b 65 67 76 65 0d 0a 55 73 65 72 2d 41 67 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 46 66 77 32 8d 4c 42 31 38 2e	co HTTP/ 1.1 los t: p0.qh ing.com- Connect ion: kee p-alive -User-Ag ent: Moz illa/5.0 (block - NT 10			-
● 2 Transistin Catrol Protocl: Poteol: Poteol	00b0 30 3h 20 57 4f	57 36 34 29 28 41 78 78 66 65 57	8: NDM64) Annlew			
	O 7 Transistion Contra	d Protocol: Protocol	of monor / uppress		(3)明 25748 - 戸野子 20078 (79 98) P2等: 5-	failt

图 1.20 显示过滤器中输入 TCP 抓包

1.4.1 数据链路层过滤

按照 MAC 地址进行筛选:

格式: eth.src == MAC 地址

【例 1-1】 如筛选 MAC 地址为 e0:d5:5e:ac:eb:71 的数据包,则应该在显示过滤器 中输入 eth. src == e0:d5:5e:ac:eb:71,然后单击右侧的箭头按钮,如图 1.21 所示。



A NEED						
文件(F) 鋼櫃(E) 视题(V)	跳转(G) 捕获(C) 分析(A) 统计(S) 电运(Y)	无间(W) 工具(T) 和助(H)				
4840 28	C 4 + + S 7 ± 🛄 Q Q	Q. 11				
oth size = +0: d5 5+ ar ob	71					S == +
No. Ties	Source	Pestination	Protocal	Length Info		
6308 901.860675	202.206.96.131	239.255.255.250	SSDP	219 M-SEARCH * HTTP/1.1		
6320 984.319814	fe80::e128:b77e:7f20:4c9f	ff02::c	UDP	714 50907 + 3702 Len=652		
6321 984.319944	202.206.96.131	239.255.255.250	UDP	694 50906 + 3702 Len=652		
6322 984.439998	fe80::e128:b77e:7f20:4c9f	ff02::c	UDP	714 50907 + 3702 Len=652		
6323 984.525987	202.206.96.131	239.255.255.250	UDP	694 50906 + 3702 Len=652		
6324 984.678939	fe80::e128:b77e:7f20:4c9f	ff02::c	UDP	714 50907 + 3702 Len=652		
6325 984.935528	202.206.96.131	239.255.255.250	UDP	694 50906 - 3702 Len=652		
6326 905.155213	fe80::e128:b77e:7f20:4c9f	ff02::c	UDP	714 50907 + 3702 Len=652		
6329 985.758884	202.206.96.131	239.255.255.250	UDP	694 58986 + 3782 Len=652		
6330 986.106927	fe80::e128:b77e:7f20:4c9f	ff02::c	UDP	714 50907 + 3702 Len=652		
6336 907.383498	202.206.96.131	239.255.255.250	UDP	694 50906 + 3702 Len=652		
6342 908.011053	fe80::e128:b77e:7f20:4c9f	ff02::c	UDP	714 58987 + 3782 Len=652		
6348 989.384839	202.206.96.131	239.255.255.250	UDP	694 50906 + 3702 Len=652		
6359 910.011937	fe80::e128:b77e:7f20:4c9f	ff02::c	UDP	714 58987 + 3782 Len=652		
6367 911.384028	202,206,96,131	239.255.255.250	UDP	694 58986 + 3782 Len=652		
6381 916.103353	202.206.96.131	239.255.255.250	SSDP	219 M-SEARCH * HTTP/1.1		
6384 917.184776	202.206.96.131	239.255.255.250	SSDP	219 M-SEARCH * HTTP/1.1		
6394 918, 105974	202,206,96,131	239,255,255,250	SSDP	219 M-SEARCH * HTTP/1.1		
6400 919.107869	202.206.96.131	239.255.255.250	SSDP	219 M-SEARCH * HTTP/1.1		
S						· · · ·
> Frame 5787: 92 byte	es on wire (736 bits), 92 bytes ca	optured (736 bits) on	interface	\Device\NPF_{1B9E27F0-F08F-4752-83	378-62F9D771AC6E}, 1d 0	
> Ethernet II, Src: 6	iga-Byt_ac:eb:71 (e0:d5:5e:ac:eb:	71), Dst: IPv4mcast_f	b (01:00:5	5e:00:00:fb)		
> Internet Protocol V	Version 4, Src: 202.206.96.131, D	it: 224.0.0.251				
> User Datagram Proto	ocol, Src Port: 5353, Dst Port: 53	153				
> Multicast Domain Na	ame System (response)					
0000 01 00 Se 00 00	fb e8 d5 5e ac eb 71 88 88 45 8	a				
0010 00 4e 1e 07 00	00 ff 11 91 4a ca ce 60 83 e0 0	N				
0020 00 fb 14 e9 14	e9 00 3a 3c ed 00 00 84 00 00 00					
0030 00 01 00 00 00	00 0b 5f 74 65 61 6d 76 69 65 7	7 teamview				
0040 65 72 04 5f 74	63 70 05 6c 6f 63 61 6c 00 00 0	ertcp. local				
0050 00 01 00 00 00	00 00 04 01 30 c0 0c					
@ Z Ethernet (ath), 14	byte(s)				分頃 6410 ・ 已費余 605 (9.4%)	DPE: Defealt

图 1.21 按照 MAC 地址筛选

注意:等号必须输入两个,如果输入一个等号则语法错误。输入框为红色表示错误, 为绿色表示正确,可以执行过滤器。

1.4.2 网络层过滤

1. 按照 IP 地址筛选

格式: ip.addr == IP 地址

【例 1-2】 如想要过滤出目的地址或源地址为 202. 206. 96. 52 的数据包,则应在过滤器中输入 ip. addr == 202. 206. 96. 52,然后单击右侧的箭头按钮,如图 1. 22 所示。

ip. addr=202.206.96.52				[×] →
Tine	Source	Destination	Protocol	Length Info
192 0.142568	222.199.191.43	202.206.96.52	HTTP	1466 Continuation
193 0.142688	222.199.191.43	202.206.96.52	HTTP	1466 Continuation
194 0.142695	202.206.96.52	222.199.191.43	TCP	54 1477 → 80 [ACK] Seq=1 Ack=110721 Win=512 Len=0
195 0.142808	222.199.191.43	202.206.96.52	HTTP	1466 Continuation
196 0.142927	222.199.191.43	202.206.96.52	HTTP	1466 Continuation
197 0.142939	202.206.96.52	222.199.191.43	TCP	54 1477 → 80 [ACK] Seg=1 Ack=113545 Win=512 Len=0
198 0.143047	222.199.191.43	202.206.96.52	HTTP	1466 Continuation
199 0.143432	222.199.191.43	202.206.96.52	HTTP	1466 Continuation
200 0.143444	202.206.96.52	222.199.191.43	TCP	54 1477 → 80 [ACK] Seq=1 Ack=116369 Win=512 Len=0
201 0.143550	222.199.191.43	202.206.96.52	HTTP	1466 Continuation
202 0.143670	222.199.191.43	202.206.96.52	HTTP	1466 Continuation
203 0.143678	202.206.96.52	222.199.191.43	TCP	54 1477 → 80 [ACK] Seq=1 Ack=119193 Win=512 Len=0
204 0.143789	222.199.191.43	202.206.96.52	HTTP	1466 Continuation

图 1.22 按照 IP 地址筛选

2. 按照源 IP 地址筛选

格式: ip.src == 源 IP 地址

【例 1-3】 如想要过滤源地址为 202. 206. 96. 180 的数据包,根据语法规则,在过滤器 中输入 ip. src == 202. 206. 96. 180,然后单击右侧的箭头按钮,就可以进行过滤了,如

图 1.23 所示。

「北北市					
文件(F) 編編(E) 税图(V) 跳時(G) 捕获(C) 分析(A) 统计(5) 电话(V) 无间(W	() 工具(T) 制能	04	
▲ ■ △ ● □ □ □ 1	x E 4 + + 2 8 3				8 CT + +
Yo. Time	Source	Destination	Protocol	Length Info	
56 3.513320	202.206.96.180	121.51.139.184	TCP.	54 [TCP Retransmission] 52022 + 80 [FIN, ACK] Seg=1 Ack=1 Win=32650 Len=0	
				54 [TCP Retransmission] 52013 - 80 [FIN, ACK] Seg=1 Ack=1 Win=32768 Len=0	
					_
				54 [TCP Retransmission] 52013 = 80 [FIN, ACK] Seq=1 Ack=1 Win=32768 Len=0	
66 4.462513	202,206.96.180	121.51.77.101	TCP	441 62051 + 8080 [PSH, ACK] Seq=1 Ack=1 Win=517 Len=387	
69 4.552246	202.205.96.180	121.51.77.101	TCP	54 62051 → 8080 [ACK] Seq=388 Ack=91 Win=516 Len=0	
71 5.314550	202.205.96.180			54 [TCP Retransmission] 52022 → 80 [FIN, ACK] Seq=1 Ack=1 Win=32650 Len=0	
72 5.314550	202.206.96.180	220.194.91.69		54 [TCP Retransmission] 52017 + 80 [FIN, ACK] Seq=1 Ack=1 Win=32255 Len=0	
73 5,314566	202.206.96.180	220.194.91.69	TCP	54 [TCP Retransmission] 52013 + 80 [FIN, ACK] Seq=1 Ack=1 Min=32768 Len=0	
84 6.800649	202.205.96.180	8.129.59.224	UDP	42 62680 → 8200 Len+0	
107 7.715255	202.206.96.180	182,254,57,124		54 [TCP Retransmission] 52008 → 80 [FIN, ACK] Seq=1 Ack=1 Win=32005 Len=0	-
108 7.715299	202.206.96.180	228.194.91.69		54 [TCP Retransmission] 52017 + 80 [FIN, ACK] Seq=1 Ack=1 Win=32255 Len+0	=
109 7.715303	202.205.95.180	121.51.139.184		54 [TCP Retransmission] 52022 → 80 [FIN, ACK] Seq=1 Ack=1 Win=32650 Len=0	_
110 7.715312	202.206.96.180	220.194.91.69	TCP	54 [TCP Retransmission] 52013 + 80 [FIN, ACK] Seq=1 Ack=1 Win=32768 Len=0	
126 9.273520	282,286,96,188	58.251.121.55	TCP	66 52025 + 8000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1	
128 9.338419	202.206.96.180	58.251.121.55	TCP	54 52025 + 8000 [RST] Seq=0 Win=0 Len=0	
 > Frame 128: 54 by > Ethernet II, Src > Internet Protoco > Transmission Con 	tes on wire (432 bits) : HP_2f:74:c0 (04:0e: 1 Version 4, Src: 202 trol Protocol, Src Por), 54 bytes captured 3c:2f:74:c0), Dst: Ci .206.96.180, Dst: 58. rt: 52025, Dst Port:	(432 bits) on sco_23:44:c3 251.121.55 8000, Seq: 0,	interface \Device\NFF_(189E27F0-F08F-4752-8378-62F90771AC6E}, 1d 0 (08:17:35:23:44:c3) Len: 0	
0000 08 17 35 23 0010 00 28 ca al	44 c3 84 8e 3c 2f 74	c0 08 00 45 005	#D · · · <td>54 </td> <td></td>	54 	
0020 79 37 cb 39 0030 00 00 df cf	1f 40 eb 32 e1 26 eb 00 00	32 e1 26 50 04 y7-	9-0-2 -8-2-8		
O Z Source Address	IPv4 address			分類:168 + 已算示:54 (32.1%) + 已丢弃	: 0 (0.0%) 228: Defualt
And an owner of the Party of th					

图 1.23 按照源 IP 地址筛选

3. 按照目的 IP 地址筛选

格式: ip.dst == IP 地址

【例 1-4】 如果要过滤目的地址为 202. 206. 96. 180 的数据包,则根据语法规则在过 滤器中输入 ip. dst == 202. 206. 96. 180,然后单击右侧的箭头按钮,就可以进行过滤了, 结果如图 1. 24 所示。

10.10R				
4(F) 編編(E) 模型(V)	期時(G) 捕获(C) 分析(A)	统计(5) 电运(Y) 无线(W)	工具(T) 科批	040
	0 9 + + ST	TERRET		
. dat -002 206 96 100				S
Tiee	Source	Destination	Protocol	Length Info
12 1.119706	180.163.249.3	202.206.96.180	TCP	66 80 → 51542 [ACK] Seq=1 Ack=2 Win=864 Len=0 SLE=1 SRE=2
16 1.575133	61.151.178.213	202.206.96.180	UDP	105 8000 + 4000 Len=63
18 1.838124	8.129.59.224	202.206.96.180	ADP	99
21 2.090576	42.56.76.76	202.206.96.180	TLSv1.2	85 Encrypted Alert
22.2.090576	42.56.76.76	202.206.96.180	TCP	60 443 + 52012 [FIN, ACK] Seq=32 Ack=1 Nin=265 Len=0
35 3.215654	202.206.100.36	202.206.96.180	DNS	435 Standard query response 0xd0f0 A pub.idqqimg.com CNAME pub.idqqimg.com.tc.qq.com CNAME pub.idq.
36 3.216140	202.206.100.36	202.206.96.180	DNS	221 Standard query response 0x95b3 AAAA pub.idqqimg.com CNAME pub.idqqimg.com.tc.qq.com CNAME pub
38 3.227574	182.254.52.196	202,206,96.180	TCP	66 443 + 52024 [5YN, ACK] Seq-0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=128
41 3.238325	182.254.52.196	202.206.96.180	TCP	60 443 → 52024 [ACK] Seq=1 Ack=318 Win=15744 Len=0
42 3.238916	182.254.52.196	202.206.96.180	TL5v1.2	1514 Server Hello
43 3.238916	182.254.52.196	202.206.96.180	TCP	1514 443 → 52024 [ACK] Seq=1461 Ack=318 Win=15744 Len=1460 [TCP segment of a reassembled POU]
44 3,238916	182.254.52.196	202.206.96.180	TCP	1230 443 + 52024 [PSH, ACK] Seq=2921 Ack=318 Win=15744 Len=1176 [TCP segment of a reassembled PDU]
46 3.248822	182.254.52.196	202.206.96.180	TLSv1.2	642 Certificate, Server Key Exchange, Server Hello Done
49 3.268546	182.254.52.196	202.206.96.180	TLSv1.2	312 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
51 3.271858	182.254.52.196	202.206.96.180	TLSv1.2	736 Application Data
52 3.273297	61.151.178.213	202.206.96.180	UDP	89 8000 + 4000 Len=47
53 3.281785	182.254.52.196	202.206.95.180	TCP	736 [TCP Retransmission] 443 - 52024 [PSH, ACK] Seq-4943 Ack-717 Win-16768 Len-682
68 4.511784	121.51.77.101	202.206.96.180	TCP	144 8080 + 62051 [PSH, ACK] Seq=1 Ack=388 Win=331 Len=90
115 7.877402	61.151.178.213	202.206.96.180	OICQ	129 OICQ Protocol
127 9.330385	\$8.251.121.55	202.206.96.180	TCP	66 8000 + 52025 [SYN, ACK] Seq=0 Ack=0 MIn=64240 Len=0 MSS=1460 MS=256 SACK_PERM=1
name 127: 66 byte thernet II, Src: nternet Protocol ransmission Contr	es on wire (528 bits) Cisco_23:44:c3 (08:1 Version 4, Src: 58.2 rol Protocol, Src Por	, 66 bytes captured (7:35:23:44:c3), Dst: 151.121.55, Dst: 202.2 t: 8000, Dst Port: 52	528 bits) on HP_2f:74:c0 86.96.180 025, Seq: 0,	interface UpericeUMF[189627F0-F08F-4752-8378-62F90771ACGE}, id 0 (04:0e:3c:2f:74:0) Ack: 0, Len: 0
0 84 8e 3c 2f 74	4 c0 08 17 35 23 44 0 00 71 05 55 50 30	c3 08 00 45 00 ··· </td <td>t 5#D8</td> <td>4</td>	t 5#D8	4
0 68 b4 1f 40 c	b 39 fe ff 7b ff eb	32 e1 26 80 12	9. 1.2.8	
0 fa f0 62 87 0	0 00 02 04 05 64 01	03 03 08 01 01 ··b·		
0 04 02				
				The second
· Destination Addre	II. LIVE LOUVESS			77년 168 · 已五水 24 (14.36) · 已五井 0 (0.06)] 配置 De

图 1.24 按照目的地址筛选

4. 按照指定的源地址和目的地址进行筛选数据包

格式: ip.src == IP地址 && IP.dst == IP地址

【例 1-5】 如果想要筛选源地址为 202. 206. 96. 180,目的地址为 58. 205. 218. 18 的数据 包,只需要根据语法规则在过滤器中输入 ip. src == 202. 206. 96. 180 & & ip. dst == 58. 205. 218. 18,然后单击右侧的箭头按钮,就可以进行过滤了,结果如图 1. 25 所示。

18/17) HENRICE (71.81					0.0
+(r) seess(c) scale(r)	题[46(G) 14(程(C) 13(45(A) 14(1+(S)	电运(Y) 无线(W) 工具(T) 制助()	-0		
	B 9 + + S 7 ±				
ip uns = 202 206 96 180	0 An ip dat -68 205 218 18				8 - I •
Tine	Searce	Destination.	Pretoral 1	Longth Islo	
2657 40.914687	202.206.96.180	58.205.218.18	TEP	66 63375 - 443 [SYN] Seg-0 Min+64240 Len+0 MSS-1460 MS-256 SACK_PERM+1	
2659 40.920916	202.206.96.180	58,205,218,18	TCP	54 63375 - 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0	
2660 40.921244	202.206.96.180	58.205.218.18	TLSv1.2	571 Client Hello	
2665 40.930537	202.206.96.180	58.205.218.18	TCP	54 63375 → 443 [ACK] Seq=518 Ack=4381 Win=131328 Len=0	
2668 40.931150	202.206.96.180	58.205.218.18	TCP	54 63375 - 443 [ACK] Seq=518 Ack=6049 Win=131328 Len=0	
2669 40.935743	202,205,95,180	58.205.218.18	TLSv1.2	180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
2670 40.936115	202.206.96.180	58.205.218.18	TLSv1.2	147 Application Data	
2671 40.936727	202.206.96.180	58.205.218.18	TLSv1.2	566 Application Data	
2675 40.942339	202.206.96.180	58.205.218.18	TCP	54 63375 - 443 [ACK] Seq=1249 Ack=6385 Win=130816 Len=0	
2676 48.942688	202.206.96.180	58,205,218,18	TLSv1.2	92 Application Data	
2679 40.984368	202.205.96.180	58.205.218.18	TCP	54 63375 - 443 [ACK] Seg=1287 Ack=6769 Win=130560 Len=0	
rame 2657: 66 by ithernet II. Src:	tes on wire (528 bits), 66 by HP 2f:74:c0 (04:0e:3c:2f:74:	tes captured (528 bits) on c0). Dst: Cisco 23:44:c3 (interface \\ 08:17:35:23:	Device\WF[159E27F8-F08F-4752-8378-62F90771AC6E], 1d 0 44:c1)	_
Frame 2657: 66 by Ethernet II, Src: Internet Protocol	tes on wire (528 bits), 66 by HP_2f:74:c0 (04:0e:3c:2f:74: Version 4. Src: 202.206:96.1	tes captured (528 bits) on c0), Dst: Cisco_23:44:c3 (80. Dst: 58.205:218.18	interface V 08:17:35:23:	Device\MPF_{189E27F0-F08F-4752-8378-62F90771AC6E}, id 0 44:c3)	_
Frame 2657: 66 byt Ethernet II, Src: Internet Protocol Transmission Cont	tes on wire (528 bits), 66 by HP_2f:74:c0 (04:0e:3c:2f:74: Version 4, 5rc: 702.206.96. T01 Protoc0, 5rc Port 63.7	tes captured (528 bits) on c0), Dst: Cisco_23:44:c3 (80, Dst: 58.205.218.18 Det Port: 443.5eg: 0.1	interface V 08:17:35:23:-	Device\WPF_(189E27F0-F08F-4752-8378-62F90771AC6E}, 1d 0 44:c3)	_
Frame 2657: 66 by Ethernet II, Src: Internet Protocol Transmission Contr	tes on wire (528 bits), 66 by HP_2f:74:c0 (04:0e:3c:2f:74: Version 4, Src: 202.266:96.1 nol Protocol, Src Port: 63375	tes captured (528 bits) on c8), Dst: Cisco_23:44:3 80, Dst: 58.205:218.18 9, Dst Port: 443, Seq: 9, L	en: 0	Device(NPF_(189E2770-F08F-4752-8378-62F90771AC6E), id @ 44:c3)	_
Frame 2657: 66 by Ethernet II, Src: Internet Protocol Transmission Contr	tes on wire (528 bits), 66 by HP_2f:74:c0 (04:0e:3c:2f:74 Version 4, 5rc: 202.206.96.1 Fol Protocol, 5rc Port: 63375	tes captured (528 bits) on c0), Dst: Cisco 23:44:c3 (80, Dst: 58.205.218.18 , Dst Post: 443, Seq: 0, L	interface \ 08:17:35:23: en: 0	Device\MPF_{189E27F0-F08F-4752-8378-62F90771AC6E}, id 0 44:c3)	_
Frame 2657: 66 by Ethernet II, Src: Internet Protocol Framsmission Contr 90 08 17 35 23 4	tes on wire (528 bits), 66 by H0_2f;74:00 (04:00:30:2f;74: Version 4, Src: 202.206.96.1 H03 Protocol, Src Port: 83375 4 c3 04 00 32 2f 74 c0 08 00	tes captured (528 bits) on c0), Dst: Cisco 23:44:c3 (80, Dst: 58.205.218.18 , Dst Port: 443, Seq: 0, L 9 45 00540 45 00540	iinterface ↓ 08:17:35:23: en: 0	Device\MPF_{189E27F0-F08F-4752-8378-62F90771AC6E}, id 0 44:c3)	
Frame 2657: 66 by thernet II, Src: Internet Protocol framsmission Contr 00 08 17 35 23 4 10 00 34 83 35 4 10 00 34 83 35 4	tes on wire (528 bits), 66 by HP_2f:74:00 (04:0e:3c:2f:74 Version 4, Src: 202.206.96.1 On Protocol, Src Port 6337 4 c3 04 0e 3c 2f 74 c0 08 00 0 00 50 06 00 00 ca c6 6b 0	tes captured (528 bits) on c0), Dst: Cisco_21:44:C3 (80, Dst: 58.205.218.18), Dst Port: 443, See: 0, L 45 500 \$40 \$70 \$71 3a 6d -4.78 \$71 \$75	interface \ 08:17:35:23: en: 0	Device\MPF_(189E27F0-F08F-4752-8378-62F90771AC6E), id 0 44:c3)	
Frame 2657: 66 by Ethernet II, Src: Internet Protocol Transmission Contr 00 08 17 35 23 4 0 00 34 83 3f 4 28 da 12 f7 8f 6 5 fa 60 48 80 0	tes on vire (528 bits), 66 by HP_2f:74:c0 (04:0e:3:c2f:74: Version 4, 5:c2 a02.06.9c3 nol Protocol, Snc Port: 63375 4 c3 04 0e: 3c 2f 74 c0 08 00 08 08 00 60 00 00 ca ce 60 bi 08 00 20 00 55 c4 00 10 ca	tes captured (528 bits) on c0), Dat: Cisco_23:44:c1 (80, Dat: 58:505-218:18 , Dat Pont: 443, Seq: 0, L 145 00580 145 00580 145 00 - 145 00 - 15 00 - 16 00 -	interface \ 08:17:35:23: en: 0	Device\WFf_(189E27F0-F08F-4752-8378-62F90771AC6E), id 0 44:c3)	_
Frame 2657: 66 byt Ethernet II, Src: Internet Protocol Transmission Contr 00 08 17 35 23 4 10 00 34 83 3f 4 20 4a 12 7 8f 0 30 fa f0 40 89 0 0 04 0	tes on wire (528 bits), 66 by HP_2f:74:00 (04:0e:3c:2f:74) Version 4, Src: 202.206.96.1 on Protocol, Src Port 1075 4 -3 04 0e 3.2f 74 +0 08 00 00 08 06 00 00 ca cc 66 bi 1 b 6: 27 00 55 00 00 00 0 08 08 05 00 00 ca cc 66 bi 1 b 6: 27 00 55 00 00 00 00 0 00 02 04 05 b4 01 03 03 03	tes captured (528 bits) on c0), Dst: Cisco_23:44:2) (80, Dst: 58.265.218.18), Dst Port: 43.3, See: 0, L. E 38.40 - 4.7g	08:17:35:23:4	Device\MPF_(189E27F0-F08F-4752-8378-62F90771AC6E), 1d 0 44:c3)	_
rame 2657: 66 by thermet II, Srci framstration Contr framstission Contr 0 08 17 35 23 4 0 09 34 83 37 4 0 da 12 f7 8 f 0 16 fa f0 40 89 00 10 04 02	tes on vire (528 bits), 66 by HP_2f:74:00 (04:0e:3:c:2f:74: Version 4, 5:c: 202.06.96.16 nol Protocol, Snc Porti 63375 4 c3 04 0e: 3c 2f 74 c0 08 00 00 08 00 06 00 00 ca c6 bi bi bi c3 20 03 56 000 00 ca 00 00 00 00 00 00 ca c6 bi bi bi c3 20 03 56 000 00 ca 00 00 02 04 05 bi d 01 03 00 00	tes captured (528 bits) on c0), Dat: Cisco_23:44:c1 (80, Dat: 58:505-218:18 , Dat Port: 443, Seq: 0, L 145 005#0 - 45 005#0 145 00 5#0 0 00 02 00 02 01 01	interface \ 08:17:35:23: en: 0	Device\MPF_(159E27F0-F08F-4752-8378-62F90771AC6E), id 0 44:c3)	_
Frame 2657: 66 byth Ethernet II, Src: Internet Protocol Transmission Contr 00 08 17 35 23 4 10 00 34 83 37 6 40 40 27 6 10 fa f0 40 89 0 10 64 02	tes on vire (528 bits), 66 by 10°_21:74;c0 (04:0e:3c:2f:74: Version 4, 5rc: 202,266.96: 100 Protocol, 5rc Revit 1372 4 c3 04 0e: 3c 2f 74 c0 08 00 0 08 80 06 00 00 ca c6 04 1 b 61 20 0 25 60 00 00 00 0 08 00 00 00 00 ca c6 04 0 00 00 00 00 00 00 ca c6 04 0 00 00 00 00 00 00 00 00 00 0 00 00 00	tes captured (528 bits) on c0), Dst: Cisco_23:44:c3 (80, Dst: 58.205.218.18 , Dst Nort 443, See; 0. L 145 00 -580 - 145 00 -580 - 180 02	interface \ 08:17:35:21: en: 0	Device\WF_{189E27F0-F08F-4752-8378-62F90773AC6E}, id 0 44:c3)	_

图 1.25 按照指定的源地址和目的地址筛选

1.4.3 传输层过滤

1. 筛选 TCP 的数据包

格式:tcp

【例 1-6】 在过滤器中输入规则 TCP,这样就可以过滤出所有协议为 TCP 的数据 包,如图 1.26 所示。

top				\times
Tine	Source	Destination	Protocol	Length Info
1 0.000000	222.199.191.43	202.206.96.52	HTTP	1466 Continuation
2 0.000118	222.199.191.43	202.206.96.52	HTTP	1466 Continuation
3 0.000126	202.206.96.52	222.199.191.43	TCP	54 1476 → 80 [ACK] Seq=1 Ack=2825 Win=512 Len=0
4 0.000178	222.199.191.43	202.206.96.52	HTTP	638 Continuation
5 0.010364	222.199.191.43	202.206.96.52	HTTP	1466 Continuation
6 0.010480	222.199.191.43	202.206.96.52	HTTP	1466 Continuation
7 0.010504	202.206.96.52	222.199.191.43	TCP	54 1477 → 80 [ACK] Seg=1 Ack=2825 Win=512 Len=0
8 0.010602	222.199.191.43	202.206.96.52	HTTP	1466 Continuation
9 0.010722	222.199.191.43	202.206.96.52	HTTP	1466 Continuation
10 0.010743	202.206.96.52	222.199.191.43	TCP	54 1477 → 80 [ACK] Seq=1 Ack=5649 Win=512 Len=0
11 0.010840	222.199.191.43	202.206.96.52	HTTP	1466 Continuation

图 1.26 筛选 TCP 的数据包

2. 筛选不是 TCP 的数据包

格式:!tcp

【例 1-7】 在过滤器中输入规则! tcp,过滤出所有不是 TCP 的数据包,如图 1.27 所示。 注意:在英文状态下输入感叹号。

1	法用					
文件	(F) 鋼腦(E) 视图(V)	調時(G) 捕获(C) 分析(A) 统计(S) 电运(Y)	无间(W) 工具(T) 解助(H)			
1		C 4 + + S 7 ±	ц			
110	tep					S +
No.	Ties	Source	Pestination	Protocal	Length Infs	^
	447 43.534038	8.129.59.224	202.206.95.180	ADP	99	
	448 43.577117	Cisco_7b:f6:05	PVST+	STP	64 Canf. Root = 32768/406/08:17:35:23:44:88 Cost = 2 Port = 0x8006	
	449 43.718509	Universa_df:60:93	Broadcast	ARP	60 Who has 202.206.96.1? Tell 202.206.96.223	
	450 43.772440	NewH3CTe_07:4c:38	Huawe1Te_2d:6c:05	ARP	68 Who has 202.206.96.195? Tell 202.206.96.49	
	451 43.783631	KYOCERAD_8c:cd:c0	Broadcast	ARP	60 Gratuitous ARP for 202.206.96.219 (Request)	
	452 43.795067	202.206.96.163	239.255.255.250	SSDP	219 M-SEARCH * HTTP/1.1	
	453 43.877928	202.206.96.15	202.206.96.255	NBNS	92 Name query NB WPAD<00>	
	454 44.003631	202.206.96.205	239,255,255,250	SSDP	139 M-SEARCH * HTTP/1.1	
	455 44.795471	202.206.96.163	239.255.255.258	SSDP	219 M-SEARCH * HTTP/1.1	
	461 45.469165	202.206.96.188	202.206.95.255	NBNS	92 Name query NB LX46TAIFU83<1c>	
	462 45,576949	Cisco_7b:f6:06	PVST+	STP.	64 Conf. Root = 32768/406/88:17:35:23:44:80 Cost = 2 Port = 0x8006	
	463 46.218991	202.206.96.188	202.206.96.255	NBNS	92 Name query NB LX46TAIFU03<1c>	
	464 46.888415	HuaweiTe_9d:28:08	Broadcast	ARP	60 ARP Announcement for 202.206.96.139	
	465 46.880415	HuaweiTe_9d:28:08	Broadcast	ARP	60 ARP Announcement for 202.206.96.139	
	466 46.888415	HuaweiTe_9d:28:08	Broadcast	ARP	60 ARP Announcement for 202.206.96.139	
	467 46.968988	202.206.96.188	202.206.96.255	NBNS	92 Name query NB LX46TAIFU03<1c>	
-	468 47.003877	202.206.96.205	239.255.255.250	SSDP	139 M-SEARCH * HTTP/1.1	
	469 47.581794	Cisco_7b:f6:06	PVST+	STP	64 Conf. Root = 32768/406/08:17:35:23:44:80 Cost = 2 Port = 0x8006	
	470 47.632776	202.206.96.13	239.255.255.258	SSDP	219 M-SEARCH * HTTP/1.1	
<		*** *** ** ***				
> F > E > I > U > D 000 001 002 003 004 005 006	rame 17: 132 byte thernet II, Src: ntermet Protocol ser Datagram Prot 0 04 0e 3c 2f 74 0 00 76 bb 40 00 6 06 b4 00 35 F9 0 06 06 00 00 00 0 65 72 02 71 71 0 00 06 00 10 00 0 6c 31 c0 18 09	s on wire (1056 bits), 132 bytes ca (15x_0_2):44:(1), 132 bytes (15x_0):44:(2), 1 Version 4, 5rc: 202.206.100.36, 0st occl, Src Port: 53, 0st Port: 63015 (response) 000 3 16 16 cl: ca cc 64 24 ca cc a 600 3 17 35 23 44 cl 08.00 45 00 000 3 16 cl: ca cc 64 24 ca cc a 600 3 17 35 00 07 67 18 08 00 01 0.00 3 51 6f 64 00 00 1c 00 01 co 10 00 01 52 00 2a 07 66 73 24 77 73 77 65 62 64 61 73 74 65 72 co 18	ptured (1856 bits) or Dst: HP_2f;74:c0 (84 : 202.206.96.180 	interfac	e UDevice\NFF_(189E27F0-F00F-4752-8378-62F90771AC6E), id 0 :74:c0)	
0	2 Transmission Contr	al Protocol Protocol			分壇: 477 - 已世示: 318 (66.7%)	配置: Defwalt

图 1.27 筛选不是 TCP 的数据包

3. 筛选端口是 80 的数据包

格式:tcp.port == 80

【例 1-8】 输入规则 tcp. port == 80,过滤出所有经过 80 端口的数据包,如图 1.28 所示。

tep.per	t -00					X
	Tine	Source	Destination	Protocol L	ength Info	
2	6 3.211725	202.206.96.180	121.51.139.184	TCP	54 52022 + 80 [FIN, ACK] Seq=1 Ack=1 Win=32650 Len=0	
2	7 3.211827	202.206.96.180	182.254.57.124	TCP	54 52008 + 80 [FIN, ACK] Seq=1 Ack=1 Win=32085 Len=0	
2	8 3.211898	202.206.96.180	220.194.91.69	TCP	54 52017 + 80 [FIN, ACK] Seq=1 Ack=1 Win=32255 Len=0	
2	9 3.211963	202.205.96.180	220.194.91.69	TCP	54 52013 → 80 [FIN, ACK] Seq=1 Ack=1 Win=32768 Len=0	
	5 3.513299	202.206.96.180	220.194.91.69		54 [TCP Retransmission] 52017 + 80 [FIN, ACK] Seq=1 Ack=1 Win=32255 Len=0	
		202,206.96.180	121.51.139.184		54 [TCP Retransmission] 52022 + 80 [FIN, ACK] Seq=1 Ack=1 Win=32650 Len=0	
	7 3.513340	202.206.96.180	228,194,91,69		54 [TCP Retransmission] 52013 + 80 [FIN, ACK] Seq=1 Ack=1 Win=32768 Len=0	
	8 3.513344	202.205.96.180	182,254,57,124		54 [TCP Hetransmission] 52008 - 80 [FIN, ACK] Seq=1 Ack=1 Win=32085 Len=0	
	9 4.114116	202.205.96.180	182.254.57.124		54 [TCP Retransmission] 52008 + 80 [FIN, ACK] Seq=1 Ack=1 Win=32085 Len=0	
6	0 4.114118	202.206.96.180	121.51.139.184		54 [TCP Retransmission] 52022 + 88 [FIN, ACK] Seg=1 Ack=1 Win=32650 Len=0	
1	1 4.114117	202,206,96,180	220.194.91.69		54 [TCP Retransmission] 52017 + 80 [FIN, ACK] Seq=1 ACK=1 Min=32255 Len=0	
	0.5 314550	202.200.90.100	103 354 53 134		54 [ICP Retransmission] 52015 4 00 [FIN, ACK] Seq=1 ACK+1 Min+32700 Len+0	
	9 5.314330	202.200.20.100	102-234-37-124		54 [177] Referencesization] 52000 + 00 [Fill, ACK] Sedel Ackel Min-52005 Loneo	
	1 3.314330	202.200.30.100	220 104 01 60		54 [TCP Retransmission] 52022 + 00 [Fin, Ack] Seq=1 Ack+1 Win+32050 Len+0	
	2 3.314330	202.200.90.100	220,194,91,09		S4 [107 Retransmission] S2017 + 80 [119, ACK] Seqei Acket Min-32255 Len-0	
10	7 7 715355	202 206 06 100	102 254 57 124		54 [TCP Reteasemicsion] 52013 + 00 [FTH_ACK] Seget Acket Min-32005 Len-0	
10	8 7 715299	202.205.96.180	220 104 91 69		54 [TCP Retransmission] 52017 # 80 [ETM_ACK] Sevel Ackel Mine32255 Land	
10	9 7 715181	202.206.96.180			54 [TCP Retransmission] 52022 + 80 [FTN, ACK] Senvi Arist Mins 2650 Lens0	
11	0 7.715312	202.286.96.188	228 194.91.69		54 [TCP Retransmission] 52013 + 60 [FIN_ACK] Sac+1 Ark+1 kin+32768 Lan+0	
Frame Ether Inter Trans	0 7.715112 110: 54 byte net II, Src: net Protocol mission Contr	202.206.96.100 es on wire (432 bits) HP_2f:74:c0 (04:0e:3 Version 4, Src: 202. Protocol, Src Por	220.194.91.69 , 54 bytes captured (ic:2f:74:c0), Dst: Cis 206.96.180, Dst: 220. t: 52013, Dst Port: 8	432 bits) on co_23:44:c3 (194.91.69 8, Seq: 1, Ac	54 [[CP Retranssission] 52013 - 00 [FU9, ACC] 5eg-1 Ack-1 Min-12268 Len-0 interface \Device\WPF_[189E27F0-F08F-4752-8378-62F90771AC6E}, id 0 00:17:35:32:44:c3) k: 1, Len: 0	
00 6	18 17 35 23 44	1 c3 04 0e 3c 2f 74	c0 08 00 45 00 ··5#	0 <td></td> <td></td>		
00 5	ib 45 cb 2d 86	50 51 cc d5 26 71	74 17 75 50 11 [E	·PQ· -&qt-uP·		

图 1.28 筛选端口是 80 的数据包

4. 筛选指定的源 IP 地址并且端口是 80 的数据包

格式: tcp.port == 80 && IP.src == 源 IP 地址

【例 1-9】 输入规则 tcp. port == 80 & & ip. src == 202. 206. 96. 180, 筛选源 IP 地址为 202. 206. 96. 180 并且端口是 80 的数据包, 如图 1. 29 所示。

	Time	Source	Destination	Protocol	Length Info
12481	1675.975068	202.206.96.180	180.163.249.3	TCP	54 60438 → 80 [ACK] Seq=217 Ack=209 Win=131840 Len=0
12588	1691.009290	202.206.96.180	180.163.249.3	TCP	54 [TCP Keep-Alive ACK] 60438 → 80 [ACK] Seq=217 Ack=209 Win=131840 Len=0
12591	1691.426854	202.206.96.180	36.110.231.9	TCP	55 [TCP Keep-Alive] 51522 + 80 [ACK] Seg=81 Ack=97 Win=509 Len=1
12629	1702.737603	202.206.96.180	180.163.237.176	TCP	55 [TCP Keep-Alive] 60430 → 80 [ACK] Seq=869 Ack=5959 Win=132096 Len=1
12641	1706.043511	202.206.96.180	180.163.249.3	TCP	54 [TCP Keep-Alive ACK] 60438 → 80 [ACK] Seq=217 Ack=209 Win=131840 Len=0
12645	1706.912175	202.206.96.180	182.254.52.87	TCP	54 60439 → 80 [ACK] Seg=232 Ack=205425 Win=65536 Len=0
12703	1720.935284	202.206.96.180	180.163.249.3	TCP	55 [TCP Keep-Alive] 60438 + 80 [ACK] Seg=216 Ack=209 Win=131840 Len=1
12788	1735.936089	202.206.96.180	180.163.249.3	TCP	70 60438 + 80 [PSH, ACK] Seq=217 Ack=209 Win=131840 Len=16
12791	1736.011003	202.206.96.180	180.163.249.3	TCP	54 60438 → 80 [ACK] Seg=233 Ack=225 Win=131840 Len=0
12792	1736.197194	202.206.96.180	36.110.231.9	TCP	70 51522 - 80 [PSH, ACK] Seg=82 Ack=97 Win=509 Len=16
12795	1736.241977	202.206.96.180	36.110.231.9	TCP	54 51522 + 80 [ACK] Seq=98 Ack=113 Win=509 Len=0
13005	1749.306028	202.206.96.180	222.28.152.253	TCP	66 60452 + 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
13007	1749.311983	202.206.96.180	222.28.152.253	TCP	54 60452 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0

图 1.29 筛选指定的源 IP 地址并且端口是 80 的数据包

注意:逻辑运算符"&&"表示与,"|]"表示或,"!"表示非,用于规则之间的连接。

1.4.4 应用层过滤

(1) 在过滤器中输入 http. request 表示请求,从图 1.30 看到源 IP 地址都为 192.168.3.2。

http.red	quest																								
	Time			So	urce											Destination			Protocol	Length	Info				
2828	3 171.42	2396	0	19	92.1	168.3	3.2	2								202.205.1	.09.205	6	HTTP	521	GET	/images	/inde	x/edu	2011/
3139	172.57	7272	7	19	92.1	168.3	3.2									239.255.2	55.250	1	SSDP	179	M-S	EARCH *	HTTP/	1.1	
3209	9 175.68	3312	4	19	92.1	168.3	3.2									124.236.2	6.47		HTTP	321	GET	/favico	n.ico	HTTP,	/1.1
3238	3 175.78	8516	2	19	92.1	168.3	3.2									1.71.150.	167		HTTP	319	GET	/favico	n.ico	HTTP,	/1.1
3248	3 175.86	5496	3	19	92.1	168.3	3.2									106.75.77	.239		HTTP	319	GET	/favico	n.ico	HTTP,	/1.1
3268	8 175.89	9286	7	19	92.1	168.3	3.2	5								119.18.19	3.144		HTTP	317	GET	/favico	n.ico	HTTP,	/1.1
3286	175.95	5771	2	19	92.1	168.3	3.2									211.144.8	0.103		HTTP	318	GET	/favico	n.ico	HTTP,	/1.1
3345	5 181.46	5049	8	19	92.1	168.3	3.2									202.205.1	.09.205	i.	HTTP	474	GET	/favico	n.ico	HTTP,	/1.1
3417	7 187.26	0134	2	19	92.1	168.3	3.2	2								39.105.58	.72		HTTP	316	GET	/favico	n.ico	HTTP,	/1.1
3425	5 187.23	3944	4	19	92.1	168.3	3.2									223.15.17	7.248		HTTP	319	GET	/favico	n.ico	HTTP,	/1.1
3434	1 187.28	3383	3	19	92.1	168.3	3.2	2								223.15.17	7.243		HTTP	316	GET	/favico	n.ico	HTTP,	/1.1
3463	3 190.49	9649	2	19	92.1	168.3	3.2	È.								239.255.2	55.250)	SSDP	179	M-S	EARCH *	HTTP/	1.1	
3477	7 192.48	3854	2	19	92.1	168.3	3.2	£								202.205.1	09.205	i.	HTTP	396	GET	/favico	n.ico	HTTP,	/1.1
3522	2 193.49	9662	3	19	92.1	168.3	3.2	į.								239.255.2	55.250	1	SSDP	179	M-S	EARCH *	HTTP/	1.1	
Interr Transm Hypert	net Promission text Tra	toco Cor ansf	ol V ntro fer	Vers: 01 Pi Pro	ion roto	4, 9 ocol ol	Src , S	irc	Por	168 t:	3.3 614	.2,	Ds , D	t: St	202 Por	.205.109 t: 80, 50	.205 eq: 1,	Ack:	1, Len:	407					
000 e8	B cd 2d	2d	b9	55	04	0e	3c	2f	74	c0	08	00	45	00	,	· · · U · ·	<th>E٠</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>	E٠							
010 01	1 bf 2c	2d	40	00	80	06	00	00	c0	a8	03	02	ca	cd		···,-@····									
820 60	d cd f0	08	00	50	83	11	b8	36	29	93	f9	4a	50	18		mP	.6)	JP.							
930 ta	a +0 +d	10	00	00	4/	45	54	20	21	20	48	54	54	50		/1 1 He	1 / н	IP							
040 Z	5 64 7E	20	63	60	40	OT On	13	74	58	20	65	62	11	Ze		/1.1. HO	Connor	w.							
a60 B	f 6e 3a	20	6b	65	65	70	2d	61	66	69	76	65	ed.	09		on: keen	-alive								
7	irerbark	11+5	odey?	410 -			2.0	01	U.C.	0.0	13		00	0.5		one weep	GIIVE								
- 100 · *	a cana A_	SAACP	- Josep	-nv.)	abi																				

图 1.30 http. request 请求

网络攻防项目实战(微课视频版)

16

注意:从图 1.30 可以看到,协议(protocol)列显示 HTTP 和 SSDP,SSDP 是简单服务发现协议,此协议为网络客户提供一种无须任何配置、管理和维护网络设备服务的机制,设备查询通过 HTTP 协议扩展 M-SEARCH 方法实现。

(2) 输入 http. response 表示响应,如图 1.31 所示。从图 1.31 中可以看到,目的 IP 地址都为 192.168.3.2 接收响应。

- い太月					- 🗆 X
文件(图 编辑(图) 视图(3)	期時(G) 開閉(C) 分析(A) 统计(S) 电场(0 无线000 工具(1) 解助(1)			
	N A A A A A A A A A A A A A A A A A A A				(10) (10) (1)
http.response	12				
a. Tine	Source	Destination .	Fratacal	Length Info	
2123 165.641814	124.225.213.208	192.168.3.2	HIIP	608 HIIP/1.1 404 Not Found (text/ntml)	
2133 165.855209	180.163.242.116	192.168.3.2	HIIP	136 HTTP/1.1 404 Not Found	
2141 166.045651	202.200.100.34	192.168.3.2	HIIP	603 HTTP/1.1 404 Not Found (text/ntml)	
2154 100.252210	42.01.120.01	192.100.3.2		200 HTTP/1.1 302 Found (text/html)	
2150 100.290509	42.01.120.01	192.100.3.2	ATTP	1033 HTTP/1.1 200 UK (text/html)	
2109 100, 390023	42,01.0.40	102 168 2 2	UTTR	1052 http:// 1 301 hoved Permanently (text/html)	
2202 100.470737	100.103.242.110	102.168.3.2	ccne	100 HTTP/1.1 404 HOL FOUND	
2210 100.373274	303 305 100 34	103 169 3 3	UTTR	502 HTTP/1 1 404 Net Found (text/html)	
22214 100.003430	199 163 242 116	102 168 3 3	HTTP	136 HTTP/1.1 404 Not Found (CEXC/ICHL)	
2222 100.024304	202 205 100 34	192.100.3.2	HTTP	603 HTTP/1.1 404 Not Found (text/html)	
22/2 167 719896	110 43 83 1	192 168 3 2	HTTP	523 HTTP/1 1 307 Temporary Redirect (text/html)	
2278 167 893365	202 206 100 34	192 168 3 2	HTTP	603 HTTP/1 1 404 Not Found (text/html)	
2291 169 576925	192, 168, 3, 1	192,168,3,2	SSOP	380 HTTP/1,1 200 OK	
ELSE IOST JOSEJ	152.100,3.1	19211001912	3301	300 mm/111 200 0K	
 Ethernet II, Src: I Internet Protocol User Datagram Prot Simple Service Dis 	HuaweiTe_2d:b9:55 (e8:cd:2d:2d:b Version 4, Src: 192.168.3.1, Dst ocol, Src Port: 1900, Dst Port: covery Protocol	9:55), Dst: HP_2f:74:c0 (0 : 192.168.3.2 50252	4:0e:3c	:2f:74:c0)	
0000 04 0e 3c 2f 74	c0 e8 cd 2d 2d b9 55 88 00 45	00 ··· <td></td> <td></td> <td></td>			
3020 01 02 00 00 40	Ac 01 5a 1b ab 48 54 54 50 26	311.1.7HTTP/1			
0030 2e 31 20 32 30	30 20 4f 4b 0d 0a 4c 4f 43 41	54 .1 200 0 KLOCAT			
0040 49 4f 4e 3a 20	68 74 74 70 3a 2f 2f 31 39 32	2e ION: htt p://192.			
0050 31 36 38 2e 33	2e 31 3a 33 37 32 31 35 2f 75	70 168.3.1: 37215/up			
0060 6e 70 64 65 76	2e 78 6d 6c 0d 0a 53 45 52 56	45 npdev.xm 1SERVE			
O Z vireshark Ut 1968	2410. propng			分组: 607125 + 已豊余: 583 (0.1	(S) 配置: Defailt

图 1.31 http. response 响应

(3) 输入 http. request. method == "GET", 请求指定的页面信息, 显示 HTTP GET 方法的请求, 如图 1.32 所示。

CHARGE HEBMIN Rinking Rinking <thrinking< th=""> <thrinking< th=""> <thrin< th=""><th>###(C) 9##(A) #(H(S) #0.5(Y) ● ⊕ 螢 筆 ≟ ⊒ @ @ @ @ 58.3.2 58.3.2</th><th>无近(1) 1月(1) 年初(1) 日 Destination Protoc 202, 206, 100, 34 HTTP 180, 163, 247, 162 HTTP</th><th>ol Length Info 401 GET 319 GET</th><th>/favicon.ico HTTP/1.1</th><th></th><th>ä - •</th></thrin<></thrinking<></thrinking<>	###(C) 9##(A) #(H(S) #0.5(Y) ● ⊕ 螢 筆 ≟ ⊒ @ @ @ @ 58.3.2 58.3.2	无近(1) 1月(1) 年初(1) 日 Destination Protoc 202, 206, 100, 34 HTTP 180, 163, 247, 162 HTTP	ol Length Info 401 GET 319 GET	/favicon.ico HTTP/1.1		ä - •
Time Scarce 2104 165.410089 192.10 2110 165.493079 192.10 2113 165.893360 192.10 2131 165.893360 192.10	● ⇔ ≌ ∓ ≟ ⊒ ⊒ Q, Q, Q 58.3.2 58.3.2 58.3.2	Destination Protoc 202.206.100.34 HTTP 180.163.247.162 HTTP	ol Length Info 401 GET 319 GET	/favicon.ico HTTP/1.1		8
[http:request sethed="GRT" Time Source 2104 165.410089 192.10 2110 165.493079 192.10 2118 165.597398 192.110 2131 165.830360 192.10	58.3.2 58.3.2 58.3.2	Destination Protoc 202.206.100.34 HTTP 180.163.247.162 HTTP	ol Length Info 401 GET 319 GET	/favicon.ico HTTP/1.1		3 -
Time Source 2104 165.410089 192.10 2110 165.493079 192.10 2118 165.597398 192.10 2131 165.830360 192.10	58.3.2 58.3.2 58.3.2	Destination Protoc 202.206.100.34 HTTP 180.163.247.162 HTTP	al Length Info 401 GET 319 GET	/favicon.ico HTTP/1.1		
2104 165.410089 192.10 2110 165.493079 192.10 2118 165.597398 192.10 2131 165.830360 192.10	58.3.2 58.3.2 58.3.2	202.206.100.34 HTTP 180.163.247.162 HTTP	401 GET 319 GET	/favicon.ico HTTP/1.1		
2110 165.493079 192.10 2118 165.597398 192.10 2131 165.830360 192.10	58.3.2 58.3.2	180.163.247.162 HTTP	319 GET	(Faulton Les HTTD/1 1		
2118 165.597398 192.10 2131 165.830360 192.10	58.3.2			/1441001.100 0017/1.1		
2131 165.830360 192.10		124.225.213.208 HTTP	319 GET	/favicon.ico HTTP/1.1		
	58.3.2	180.163.242.116 HTTP	644 GET	/s?q=http://w&src=se HTTP/1.1		
2139 166.011555 192.10	58.3.2	202.206.100.34 HTTP	401 GET	/favicon.ico HTTP/1.1		
2152 166.191927 192.16	58.3.2	42.81.120.61 HTTP	318 GET	/favicon.ico HTTP/1.1		
2155 166.253847 192.10	58.3.2	42.81.120.61 HTTP	322 GET	/error/error.htm HTTP/1.1		
2166 166.382775 192.10	58.3.2	42.81.8.40 HTTP	317 GET	/favicon.ico HTTP/1.1		
2191 166.452187 192.10	58.3.2	180.163.242.116 HTTP	645 GET	/s?q=http://wwfsrc=se HTTP/1.1		
2211 166.628222 192.10	58.3.2	202.206.100.34 HTTP	401 GET	/favicon.ico HTTP/1.1		
2220 166.799156 192.10	58.3.2	180.163.242.116 HTTP	646 GET	/s?q-http://wwwBsrc-se HTTP/1.1		
2229 167.229217 192.10	58.3.2	202.206.100.34 HTTP	401 GET	/favicon.ico HTTP/1.1		
2240 167.708284 192.10	58.3.2	110.43.83.1 HTTP	316 GET	/favicon.ico HTTP/1.1		
- 2267 167.846265 192.10	58.3.2	202.206.100.34 HTTP	401 GET	/favicon.ico HTTP/1.1		
Ethernet II, Src: HP_2f:74 Internet Protocol Version Transmission Control Proto Hypertext Transfer Protoco	:c0 (04:0e:3c:2f:74:c0), Dst 4, Src: 192.168.3.2, Dst: 20 col, Src Port: 55796, Dst Po 1	: HuawelTe_2d:b9:55 (e8:cd 2.206.100.34 mt: 80, Seq: 7982, Ack: 45	:2d:2d:b9:55) 104, Len: 347		, or , i we a	

图 1.32 HTTP GET 方法的请求

(4) 在过滤器输入 http. request. uri contains ". php",筛选 URL HTTP 中包含. php 的数据包,如图 1.33 所示。

▲ 102大月						
文件(F) 编辑(E) 视题(V)	新時(G) 捕获(C) 分析(A) 统计(S) 电运(Y)	无间(W) 工具(T) 和助(H)				
AIDO DER	B 9 + + = = = = = = = 0 0 0	A II				
A http. request uri contain	ns fi php f	Con Fill			8	-+
So. Ties	Source	Pestination 1	Protocal	Longth Info		
+ 3551 364.980451	202.206.96.180	36.110.237.161	ITTP	1328 POST	/wdinfo.php HTTP/1.1	
4018 376.507865	202.206.96.180	36.110.237.161	ITTP	1508 POST	/wdinfo.php HTTP/1.1	
4460 377.060903	202.206.96.180	36.110.237.161	ITTP	1376 POST	/wdinfo.php HTTP/1.1	
6485 400.182135	202.206.96.180	111.206.60.52	ITTP	644 P0ST	/wdinfo.php HTTP/1.1	
6486 400.182137	202.206.96.180	111.206.60.52	ITTP	652 P0ST	/wdinfo.php HTTP/1.1	
6531 400.214937	202.206.96.180	111.206.60.52	ITTP	572 POST	/wdinfo.php HTTP/1.1	
6536 400.219360	202.206.96.180	111.206.60.52	ITTP	588 POST	/wdinfo.php HTTP/1.1	
8079 401.246396	202.206.96.180	111.206.60.52	ITTP	716 P05T	/wdinfo.php HTTP/1.1	
10221 407.516125	202.206.96.180	111.206.60.52	ITTP	988 P05T	/wdinfo.php HTTP/1.1	
10233 407.525312	202.206.96.180	111.206.60.52	ITTP	788 P05T	/wdinfo.php HTTP/1.1	
11133 414.187673	202.206.96.180	36.110.213.230	ITTP	585 GET /	intf.php?method=ExtUpdate.query&os=win&arch=x86&os_arch=x86_64&nac1_arch=x	86-648pt
11246 415.670798	202.206.96.180	111.206.60.52	ITTP	1188 P05T	/wdinfo.php HTTP/1.1	
11253 415.678571	202,206.96.180	111.206.60.52	ITTP	836 P0ST	/wdinfo.php HTTP/1.1	
c > Frame 3551: 1328 b > Ethernet II, Src: \Internet Partecel	bytes on wire (10624 bits), 1328 byt HP_2f:74;c0 (04:0e:3c:2f:74:c0), 05 Varies 4, 5ex: 103, 264 6€ 108 Det	es captured (10624 bits) t: Cisco_23:44:c3 (08:1) t: 36 110 227 161) on in 7:35:23	terface \De :44:c3)	rice\MPf_{189E27F0-F00F-4752-8378-62F90771AC6E}, id 0	
Internet Protocol	Version 4, SPC: 202.200.90.100, USC	: 30.110.237.101				
> Transmission Contr	Comments (2000 butes): #3540(155)	#3550/1460) #3551/137	: 1, Le	n: 12/4		
2 [5 Reassembled for	segments (2003 bytes): #3349(133),	*3330(1400), *3331(127	•/]			_
0000 08 17 35 23 44	4 c3 04 0e 3c 2f 74 c0 08 00 45 00	EE				
0010 05 22 a5 90 40	0 00 80 06 00 00 ca ce 60 b4 24 6e	-"@"-\$n				
0020 ed a1 fb f3 00	0 50 d5 a9 d6 6f da 39 c3 c7 50 18	·····P·· ·o·9··P·				
0030 04 00 42 a7 00	0 00 26 12 ad d9 73 2e dd f4 a9 f7	- B & - + 5				
0040 ua 6/ 68 5/ a6	5 A6 a7 86 23 AA 86 a8 18 8a a3 ad	strikt Cy those .				
toose or at ab us us	realled TTP (2000 letter)	8				
O Z alashah (1+0as	10000				1 All man - 2004 in (n m)	
C = HIRDRY SOAPSY	county bushed				3746 - 14420 - EEG(1: 13 (0.14) BEE	C. PELGUE

图 1.33 筛选包含.php 的数据包

1.4.5 抓包实例

【例 1-10】 使用 ICMP 协议并抓取百度的数据包,步骤如下。

(1) 在 cmd 下执行 ping www.baidu.com -t 命令,如图 1.34 所示,显示百度的 IP 地 址为 182.61.200.7。

C:\windows\system32>ping www.baidu.com -t
正在 Ping www.a. shifen.com [182.61.200.7] 具有 32 字节的数据: 来自 182.61.200.7 的回复: 字节=32 时间=7ms TTL=51 来自 182.61.200.7 的回复: 字节=32 时间=7ms TTL=51 182.61.200.7 的回复: 字节=32 时间=7ms TTL=51 来自 182.61.200.7 的回复: 字节=32 时间
182.61.200.7 的 Ping 统计信息: 数据包: 已发送 = 19, 已接收 = 19, 丢失 = 0 (0% 丢失), 往返行程的估计时间(以毫秒为单位): 最短 = 7ms, 最长 = 10ms, 平均 = 7ms Control-C

图 1.34 执行 ping 操作

(2) 回到桌面,在过滤器中,输入 ip. addr == 182.61.200.7 and icmp,如图 1.35 所示。

1 4	+8dr - 102 61 200 7	and imp					6
Ro.	Tine	Source	Destination	Protocal 1	sugth Info		
-10	715 23.762121	202.206.96.154	182.61.200.7	ICHP	74 Echo (ping) request	1d=0x0001, seq=2/512, ttl=128 (reply in 716)	
+	716 23.769504	182.61.200.7	202.206.96.154	IOW	74 Echo (ping) reply	id=0x0001, seq=2/512, ttl=51 (request in 715)	
	749 24.774231	202.206.96.154	182.61.200.7	ICMP	74 Echo (ping) request	id=0x0001, seq=3/768, ttl=128 (reply in 750)	
	750 24.782084	182.61.200.7	202.206.96.154	ICMP	74 Echo (ping) reply	id=0x0001, seq=3/768, ttl=51 (request in 749)	
	754 25.777327	202.206.96.154	182.61.200.7	ICMP	74 Echo (ping) request	id=0x0001, seq=4/1024, ttl=128 (reply in 755)	
	755 25.785671	182.61.200.7	202.206.96.154	ICMP	74 Echo (ping) reply	id=0x0001, seq=4/1024, ttl=51 (request in 754)	
	765 26.782494	202.206.96.154	182.61.200.7	ICMP	74 Echo (ping) request	id-0x0001, seq-5/1200, ttl-128 (reply in 766)	
	765 26.793100	182.61.200.7	202.206.96.154	ICMP	74 Echo (ping) reply	id=0x0001, seq=5/1280, ttl=51 (request in 765)	
	775 27.785966	202.206.96.154	182.61.200.7	ICMP	74 Echo (ping) request	id=0x00001, seq=6/1536, ttl=128 (reply in 776)	
	776 27.793179	182.61.200.7	202.206.96.154	ICMP	74 Echo (ping) reply	id=0x0001, seq=6/1536, ttl=51 (request in 775)	
	788 28.791487	202.206.96.154	182.61.200.7	ICMP	74 Echo (ping) request	id=0x0001, seq=7/1792, ttl=128 (reply in 781)	
	781 28.798797	182.61.200.7	202.206.96.154	ICMP	74 Echo (ping) reply	id=0x0001, seq=7/1792, ttl=51 (request in 780)	
	785 29.797424	202.206.96.154	182.61.200.7	ICMP	74 Echo (ping) request	id-0x0001, seq-8/2048, ttl=128 (reply in 787)	
	787 29.806129	182.61.200.7	202.206.96.154	ICMP	74 Echo (ping) reply	id-0x0001, seg-8/2048, ttl-51 (request in 786)	
€							_
> E > I > I	thernet II, Src: sternet Protocol sternet Control M	HP_24:74:c0 (04:0e:3c:24:74:c0), Version 4, Src: 202.206.96.154, essage Protocol	Dst: Cisco_23:44:c3 (6 Dst: 182.61.200.7	88:17:35:23:4	μiε3)		
	08 17 35 23 44	c3 04 0e 3c 2f 74 c0 08 00 45	00 ···5#0··· <td></td> <td></td> <td></td> <td></td>				

图 1.35 抓取百度数据包

(3)选中图 1.35 中 1 号窗口的第一行的数据包,在 2 号窗口数据包详细信息中显示 这个数据包的所有详细信息内容,包括 Frame、Ethernet II、Internet Protocol Version 4、 Internet Control Message Protocol。单击 2 号窗口左侧三角,可显示抓到的数据包的详 细信息,如图 1.36 所示。

II ip. eddr - 102 61 20	0.7 and imp					
Bo, Tine	Seurce	Destination	Fratocal	Length Info		
- 715 23.76212	1 202.206.96.154	182.61.200.7	ICMP	74 Echo	(ping) request	id=0x0001, seq=2/512, ttl=128 (reply in 716)
s				1	[40073370 F007	
 Frame 715: 74 b 	ytes on wire (592 bits), 74 b	ytes captured (592 bits) on	interface \	Device\NPF_	{189E27F0-F08F	4752-B378-62F9D771AC6E}, 1d 0
> Interface 1d	: A (/DeArce/Mb+_{IBAFS/HB-HA	1F-4/52-83/8-62F90//1AL6E})				
Encapsulatio	type: Ethernet (1)	and the Water				
Arrival lime	: Apr 5, 2021 15:38:44.36603	1000 中国标准时间				
Ench Time	161769334 366030000 cocoods	aeconus J				
Time delta	from operations contineed fromes	0 006063000 seconds]				
Time delta	from previous captured trame:	0.000000000 seconds]				
[Time cinca	rom previous displayed frame.	(2121000 seconds]				
Ecome Number	- 715	vozizioou seconusi				
France Longth	74 hutos (502 hits)					
Capture Length	th: 74 butes (592 bits)					
Erame is ma	rked: Falsel					
[Frame is in	word Falsel					
[Protocols i	frame: eth:ethectype:in:icm	a:data]				
[Coloring Ru	le Name: ICMP]					
[Coloring Ru	le String: ican icany6]					
~ Ethernet II. Sr	c: HP 2f:74:c0 (04:0e:3c:2f:7	4:c0), Dst: Cisco 23:44:c3	(08:17:35:23)	(44:c3)		
> Destination:	Cisco 23:44:c3 (08:17:35:23:4	14:c3)	(
> Source: HP 2	f:74:c0 (04:0e:3c:2f:74:c0)					
Type: IPv4 (9×9899)					
v Internet Protoc	ol Version 4, Src: 202.206.96	.154, Dst: 182.61.200.7				
0100 1	Version: 4					
0101 = 1	Header Length: 20 bytes (5)					
> Differentiat	ed Services Field: 0x00 (DSCP:	CS0, ECN: Not-ECT)				
Total Length	: 60					
Identificati	on: 0x66d9 (26329)					
> Flags: 0x00						
Fragment Off	set: 0					
Time to Live	: 128					
Protocol: IC	4P (1)					
Header Check	sum: 0x0000 [validation disab]	led]				
[Header check	<pre>ksum status: Unverified]</pre>					
Source Addre	ss: 202.206.96.154					
Destination	Address: 182.61.200.7					
✓ Internet Contro	1 Message Protocol					
Type: 8 (Ech	o (ping) request)					
Code: 0						
Checksum: 0x	1d59 [correct]					
[Checksum Sta	atus: Good]					
Identifier (3E): 1 (0x0001)					
Idantifian /	E1. 256 (0-0100)					

图 1.36 数据包的详细信息

1.5 网络安全分析实例



19

1.5.1 ARP 欺骗原理

ARP 协议是 Address Resolution Protocol(地址解析协议)的缩写,在以太网环境中,数据的传输所依赖的是 MAC 地址而非 IP 地址,而将已知 IP 地址转换为 MAC 地址的工作是由 ARP 协议来完成的。

ARP欺骗就是一种典型的中间人攻击方式,中间人攻击就是 A 机器和 B 机器在进行正常的网络通信时,Hacker实施中间人攻击,监听 A 机器和 B 机器的通信,在这个过程中 Hacker 作为中间人会处理转发它们的数据信息,也就是说 A 机器和 B 机器之间依然可以正常通信,并且它们也不会发现通信过程中多了一个人。A 机器以为自己是在和 B 机器通信,然而实际上多了一个 Hacker 正在默默地监听 A 机器和 B 机器之间的通信。

ARP协议的缺点是没有任何认证机制。当主机A收到一个发送方IP地址为192.168.157.142的ARP请求包时,主机A并不会对这个数据包做任何的真伪校验,无论这个数据包是否来自192.168.157.142,它都会将其添加到ARP缓存表中,Hacker 正是利用这一点来冒充网关等主机的。

【例 1-11】 在 VMware 中分别创建两台虚拟机, Kali 机器的 IP 地址为 192.168.157.142, Windows 7 机器的 IP 地址为 192.168.157.170。

(1) 在 Kali 下执行"09-嗅探/欺骗"下的 Wireshark 程序,如图 1.37 所示。 说明: 创建虚拟机和 Kali 系统的详细安装步骤可以参考项目 5。



图 1.37 在 Kali 下执行 Wireshark

(2) 在 Kali 下进入终端模式,执行 ping 192.168.157.170 命令,如图 1.38 所示。

<pre>(root@ kali)-[/home/malimei]</pre>
-# ping 192.168.157.170
PING 192.168.157.170 (192.168.157.170) 56(84) bytes of data.
64 bytes from 192.168.157.170: icmp seg=1 ttl=128 time=0.606 ms
64 bytes from 192.168.157.170: icmp seg=2 ttl=128 time=0.423 ms
64 bytes from 192.168.157.170; icmp seg=3 ttl=128 time=1.23 ms
64 bytes from 192,168,157,170; icmp_seq=4 ttl=128 time=0,720 ms
64 bytes from 192.168.157.170; icmp_seg=5 ttl=128 time=0.625 ms
64 bytes from 192.168.157.170: icmp_seq=6 ttl=128 time=0.325 ms
64 bytes from 192,168,157,170: jcmp seq=7 ttl=128 time=0.553 ms
64 bytes from 192.168.157.170: icmp_seq=8 ttl=128 time=0.479 ms
64 hytes from 192,168,157,170: icmn seq=9 ttl=128 time=0.522 ms
AC
102 168 157 170 ping statistics
0 packate transmitted 0 received 0% packat loss time 9129ms
st min / aug/max/mday _ 0 225/0 608/1 227/0 2/4 mc
rtt min/avg/max/muev = 0.323/0.000/1.22//0.244 ms
(marked health) (there in the state of the
(root & kati)-[/nome/matimel]

图 1.38 Kali 机器 ping Windows 7

(3) Kali 机器 192.168.157.142 和 Windows 7 机器 192.168.157.170 进行通信时, 会先在 ARP 缓存表查找 192.168.157.170 对应的 ARP 表项(即 192.168.111.170 对应 的 MAC 地址),如果没有找到则会发送 ARP 请求。IP 为 192.168.157.142 的主机首先 会以广播方式发送一个 ARP 请求包获取 192.168.157.170 主机的 MAC 地址,其内容为 who has 192.168.157.170? Tell 192.168.157.142,如图 1.39 所示。



图 1.39 抓取到的广播内容

(4)当 IP为 192.168.157.170的主机收到这个 ARP 请求包时并不会做任何的真伪 校验, 而是直接回复一个 ARP 响应包, 把自己的 MAC 地址告诉 192.168.157.142的主机, 如图 1.40 所示。

ar ar	þ													\times		+
No.	Time	Sourc	Destination	Protocol	Length	Info										
	141 24.273790145	VMw	Broadcast	ARP	42	Who I	as :	192.1	168.	157.	170?	Tell :	192.16	8.157	.142	
	142 24.274054283	VMw	VMware_5a:4a:c7	ARP	60	192.1	168.1	157.2	170	is a	: 00:	0c:29	:04:00	1:9d		_
	182 29.265158865	VMw	VMware_5a:4a:c7	ARP	60	Who I	as :	192.1	168.	157.3	142?	Tell :	192.16	8.157	.170	
	183 29.265186602	VMw	VMware_04:00:9d	ARP	42	192.1	168.3	157.1	42	is a	: 00:	0c:29	:5a:4a	:c7		
L. Fr	ama 142: 60 hutas	00.14	re (400 bits) (0 butos	contur	nd 11	00 1	itel	00	inte	rfac	oth	h id	0		
Fr	ame 142: 60 bytes hernet II, Src: V	on wi Mware_	Lre (480 bits), 6 04:00:9d (00:0c:	50 bytes :29:04:0	captur 9:9d),	ed (4 Dst:	80 t VMwa	its) are_5	on a:4	inte :c7	rface (00:0	e eth@ 0c:29:), 1d 5a:4a	0 :c7)		
Fr Et	ame 142: 60 bytes hernet II, Src: V iress Resolution	on wi Mware_ Protoc	<pre>Lre (480 bits), 6 _04:00:9d (00:0c: col (reply) t (1)</pre>	60 bytes 29:04:0	captur 9:9d),	ed (4 Dst:	180 t VMwa	its) are_5	on a:4	inte :c7	rface (00:0	e ethe Dc:29:), id 5a:4a	0 :c7)	_	
Fr Et	ame 142: 60 bytes hernet II, Src: V iress Resolution Hardware type: E Protocol type: I	on wi Mware_ Protoc therne Pv4 (0	lre (480 bits), (04:00:9d (00:0c: col (reply) t (1) x0800)	60 bytes 29:04:0	captur 9:9d),	ed (4 Dst:	180 t VMwa	oits) are_5	on a:4	inte :c7	rfac (00:0	e ethe Oc:29:), 1d 5a:4a	0 :c7)		
Fr Et	ame 142: 60 bytes hernet II, Src: V iress Resolution Hardware type: E Protocol type: I Hardware size: 6	on wi Mware_ Enclose therne Pv4 (0	re (480 bits), 6 04:00:9d (00:0c: col (reply) tt (1) x0800)	60 bytes 29:04:0	captur 9:9d),	ed (4 Dst:	180 t VMwa	oits) are_5	on a:4	inte :c7	(00:0	e ethe Oc:29:), 1d 5a:4a	0 :c7)		
Fr Et	ame 142: 60 bytes hernet II, Src: V fress Resolution Hardware type: E Protocol type: I Hardware size: 6 Protocol size: 4	ON WI Mware Protoc therne Pv4 (6	lre (480 bits), 6 04:00:9d (00:0c: col (reply) tt (1) x0800)	60 bytes 29:04:0	captur 9:9d),	ed (4 Dst:	180 t VMwa	oits) are_5	on a:4	inte 1:c7	(00:0	e eth@ 0c:29:), 1d 5a:4a	0 :c7)		
Fr Et	ame 142: 60 bytes mernet II, Src: V Fress Resolution Hardware type: E Protocol type: I Hardware size: 6 Protocol size: 4 Opcode: reply (2	on wi Mware Proto Proto therne Pv4 (6)	ire (480 bits), 6 04:00:9d (00:0c: col (reply) tt (1) x0800)	60 bytes 29:04:00	captur 9:9d),	ed (4 Dst:	180 t VMwa	oits) are_5	on ia:4	inte :c7	(00:0	e ethe 9c:29:), 1d 5a:4a	0 :c7)		
 Fr Et Ad 	ame 142: 60 bytes hernet II, Src: V fress Resolution Hardware type: E Protocol type: I Hardware size: 6 Protocol size: 4 Opcode: reply (2 Sender MAC addre	on wi Mware_ Enote therne Pv4 (6) ss: VM	<pre>Lre (480 bits), 6 04:00:9d (00:0c: col (reply) t (1) xx8800) Ware_04:00:9d (00 </pre>	50 bytes :29:04:00	captur 9:9d),	ed (4 Dst: 9d)	80 t VMwa	oits) are_5	on a:4	inte 1:c7	(00:0	e ethé 0c:29:), 1d 5a:4a	0 :c7)		
 Fr Et Ad 	ame 142: 60 bytes hernet II, Src: V fress Resolution Hardware type: E Protocol type: I Hardware size: 6 Protocol size: 4 Opcode: reply (2 Sender MAC addre Sender IP addres	on wi Mware Proto therne Pv4 (6) ss: VM s: 192	Lre (480 bits), 6 04:00:9d (00:0c: col (reply) t (1) x0800) ware_04:00:9d (6 :168.157.170	50 bytes 29:04:00	captur 9:9d),	ed (4 Dst: 9d)	180 t VMwa	oits) are_5	on a:4	inte i:c7	(00:(e eth0 0c:29:), 1d 5a:4a	0 :c7)		

图 1.40 回复响应包