

6.8 TShark 中的总结统计

TShark 的另一个有用的功能（也是比 Tcpdump 先进的功能），是它可以从捕获的文件中生成统计的一个子集。很多这些统计功能在 Wireshark 中都能找到影子，但是 TShark 提供了简单的命令方式来进行访问。使用 -z 参数加上输出的名字可以生成统计信息。你可以使用以下命令查看所有可用的统计：

```
C:\Program Files\Wireshark>tshark -z help
```

很多我们之前学过的功能都可以用 -z 参数实现。这其中包括了输出端点和会话的命令：

```
C:\Program Files\Wireshark>tshark -r packets.pcap -z conv,ip
```

这个命令从 packets.pcap 中打印出了有关 IP 会话的信息的统计图表，如图 6-3 所示。

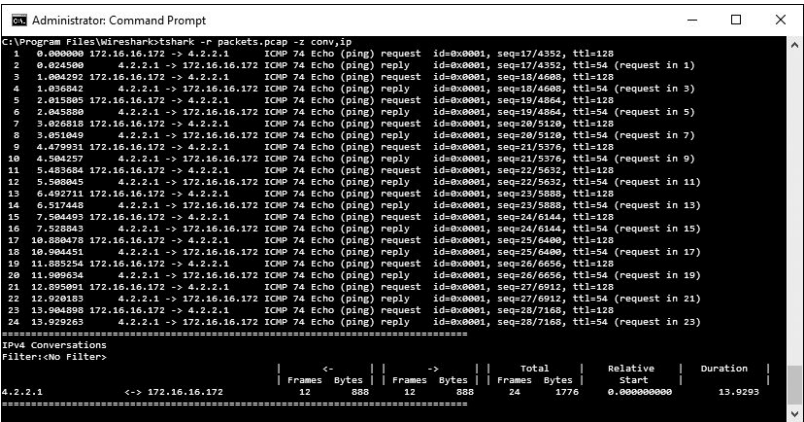


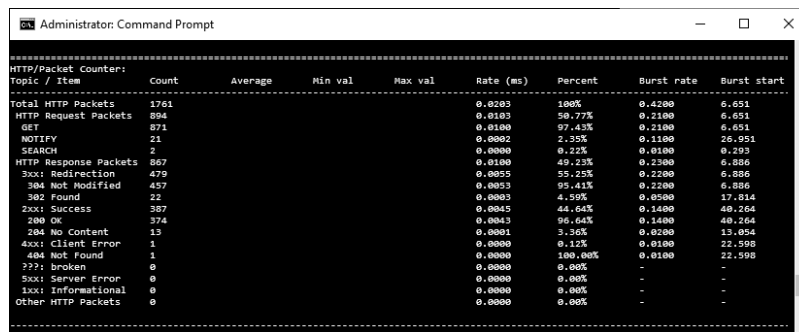
图 6-3 使用 TShark 来查看会话统计

你也可以使用这个参数来查看特定协议的信息，如图 6-4 所示。你可以使用 http, tree 选项，以表的形式来分解 HTTP 的请求和返回数据包。

```
C:\Program Files\Wireshark>tshark -r packets.pcap -z http,tree
```

另一个非常有用的功能是查看已完成排序的输出流，就像之前我们在 Wireshark 里先右键单击一个数据包然后选择「跟随 TCP 流」一样。要想获得这个输出，我们需要使用 follow 选项，并且指明流的类型、输出模式和我们想显示出的流。你可以通过会话统计最左列的序号来表示一段流，类似命令如下所示：

```
C:\Program Files\Wireshark>tshark -r http_google.pcap -z follow,tcp,ascii,0
```



Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Total HTTP Packets	1761				0.0203	100%	0.4200	6.651
HTTP Request Packets	804				0.0103	58.72%	0.2100	6.651
GET	871				0.0100	97.43%	0.2100	6.651
NOTIFY	21				0.0002	2.35%	0.1100	26.951
SEARCH	2				0.0000	0.22%	0.0100	0.299
HTTP Response Packets	867				0.0100	49.13%	0.2300	6.886
3xx: Redirection	479				0.0055	55.25%	0.2200	6.886
304 Not Modified	457				0.0053	95.41%	0.2200	6.886
302 Found	22				0.0003	4.59%	0.0500	12.814
2xx: Success	387				0.0045	44.64%	0.1400	40.264
200 OK	374				0.0043	96.64%	0.1400	40.264
204 No Content	13				0.0001	3.36%	0.0200	13.054
4xx: Client Error	1				0.0000	0.12%	0.0100	22.598
404 Not Found	1				0.0000	100.00%	0.0100	22.598
???: broken	0				0.0000	0.00%	-	-
5xx: Server Error	0				0.0000	0.00%	-	-
1xx: Informational	0				0.0000	0.00%	-	-
Other HTTP Packets	0				0.0000	0.00%	-	-

图 6-4 使用 TShark 来查看 HTTP 请求和返回统计

这条命令还会以 ASCII 形式将 http_google.pcap 的 0 号 TCP 流打印到屏幕上。这个命令的输出如下所示：

```
C:\Program Files\Wireshark>tshark -r http_google.pcap -z
--snip--
=====
Follow: tcp,ascii
Filter: tcp.stream eq 0
Node 0: 172.16.16.128:1606
Node 1: 74.125.95.104:80
627
GET / HTTP/1.1
Host: www.google.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.
Gecko/20091221 Firefox/3.5.7
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: PREF=ID=257913a938e6c248:U=267c896b5f39fb0b:FF=4:LD=e
n:NR=10:TM=1260730654:LM=1265479336:GM=1:S=h1UBGonTuWU3D23L;
NID=31=Z-nhWMjUP63e0tYMTp-3T1igMSPnNS1eM1kN1_DUrN02zW1cPM4JE3AJec9b
vG-YFibFXszOApfbhBA1B0X4dKx4L8ZDdeiKwqekgP5_kzELtC2mUHx7RHx3PittcuZ

1406
HTTP/1.1 200 OK
Date: Tue, 09 Feb 2010 01:18:37 GMT
Expires: -1

Cache-Control: private, max-age=0
Content-Type: text/html; charset=UTF-8
Content-Encoding: gzip
Server: gws
Content-Length: 4633
X-XSS-Protection: 0
```

你也可以通过提供地址细节，来指明想要查看哪个数据流。例如，下面的命令会获取一个指明端点和端口的 UDP 流：

```
C:\Program Files\Wireshark>tshark -r packets.pcap -z follow,udp,ascii,192.168.1.5:23429①,4.2.2.1:53②
```

这条命令会打印 packets.pcap 中端口 23429 上的 192.168.1.5 端点和端口 53 上的 4.2.2.1 端点的 UDP 流。

以下是我个人最爱的统计选项。

ip_hosts,tree：在一段捕获中显示每个 IP 地址，并统计每个 IP 地址在所占流量的比率。

io, phs：分层级统计在捕获文件中找到的所有协议。

http,tree：显示关于 HTTP 请求和回应的统计。

http_req,tree：显示每个 HTTP 请求的统计。

smb,srt：显示关于 Windows 会话的 SMB 命令的统计。

endpoints,wlan：显示无线端点。

expert：从捕获中显示专家信息（对话、错误等）。

当你使用 -z 参数时会有很多有用的选项，把它们都描述一遍会占用大量的篇幅。但是如果你经常使用 TShark，我还是建议你在官方文档上花点时间学习一下所有可用的选项。