

5.1.3 使用端点和会话定位最高用量者

端点和会话窗口是排查网络问题的得力助手，特别是当你试图寻找网络中产生巨大流量的源头时。

还是拿*lotsofweb.pcapng*来举例，就像文件名所揭示的那样，该捕获文件含有多个客户端浏览互联网时产生的大量 HTTP 流量。图 5-4 显示了在这个捕获文件中以字节数目排序的端点列表。

你可以注意到：以字节数排序后的第一个地址是 172.16.16.128 本地地址，这是一个内网地址（我们会在第 7 章讲到如何区分）。除此之外，拥有这个地址的设备是数据集中最活跃的信息源（进行了最多通信的主机）。

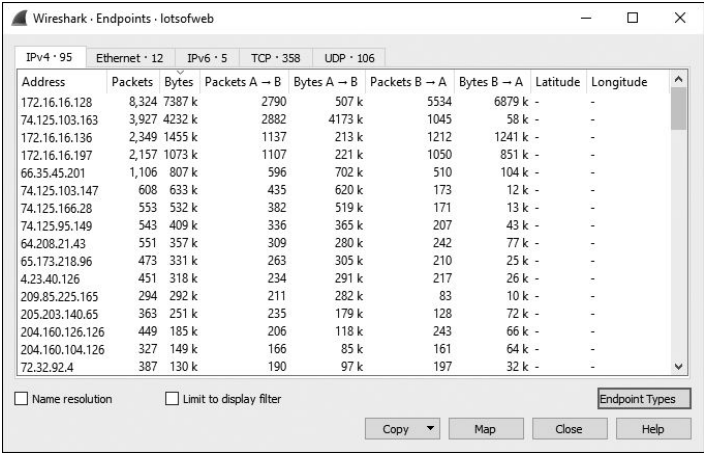


图 5-4 端点窗口显示了哪个主机是最高用量者

第二个地址 74.125.103.163 是一个公网地址。当你对一个公网地址一无所知时，可以使用 WHOIS 来查询它的注册者。在这个例子中该地址属于 Google，如图 5-5 所示。

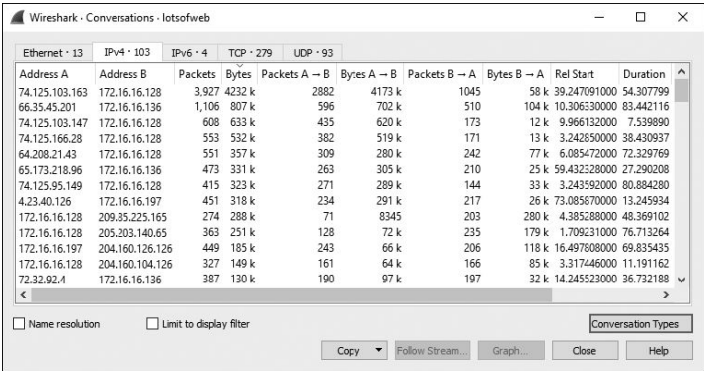
Network	
Net Range	74.125.0.0 - 74.125.255.255
CIDR	74.125.0.0/16
Name	GOOGLE
Handle	NET-74-125-0-0-1
Parent	NET74 (NET-74-0-0-0-0)
Net Type	Direct Allocation
Origin AS	
Organization	Google Inc. (GOGL)
Registration Date	2007-03-13
Last Updated	2012-02-24
Comments	
RESTful Link	<a href="https://whois.arin.net/rest/net/NET-74-125-0-0-1">https://whois.arin.net/rest/net/NET-74-125-0-0-1</a>
See Also	<a href="#">Related organization's POC records.</a>
See Also	<a href="#">Related delegations.</a>

图 5-5 WHOIS 查询结果显示 74.125.103.163 指向谷歌

注意

IP 地址的分配由多个实体根据其地址信息进行管理。美国互联网号码注册中心（ARIN）负责美国（及周边地区）的 IP 地址分配。相似的，非洲互联网络信息中心（AfriNIC）负责非洲的，世界互联网组织（RIPE）负责欧洲的，亚太互联网络信息中心（APNIC）负责亚洲的。一般来说，如果你想对某一个 IP 进行 WHOIS 查询，那么在负责这个 IP 组织的网站上操作即可。当然，如果仅看 IP 地址你并不知道地理信息，那么像 Robtex 这样的网站会帮你搞定。然而即使你在错误的注册中心网站上进行了查询，这个网站也会告诉你正确的查询位置。

有了这些信息，你可以假设：74.125.103.163 和 172.16.16.128 正在各自与很多其他设备进行大量通信，或者这两个 IP 之间在彼此通信。实际上，最大用量者之间的端点通信是比较常见的。要确认这一点，请打开会话窗口并选中 IPv4 选项卡，你就可以通过使用字节数对列表进行排序来验证这一点。在这个例子中，你可以看到这个流量应该是连续的视频下载流量，因为从地址 A(74.125.103.163)发出的数据包比从地址 B(172.16.16.128)发出的要大得多，如图 5-6 所示。



Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
74.125.103.163	172.16.16.128	3,927	4232 k	2882	4173 k	1045	58 k	39.247091000	54.307799
66.35.45.201	172.16.16.136	1,106	807 k	596	702 k	510	104 k	10.306330000	83.442116
74.125.103.147	172.16.16.128	608	633 k	435	620 k	173	12 k	9.966132000	7.539890
74.125.166.28	172.16.16.128	553	532 k	382	519 k	171	13 k	3.242650000	38.430937
64.208.21.43	172.16.16.128	551	357 k	309	280 k	242	77 k	6.085472000	72.329769
65.173.218.96	172.16.16.136	473	331 k	263	305 k	210	25 k	59.432228000	27.290208
74.125.95.149	172.16.16.128	415	323 k	271	289 k	144	33 k	3.243592000	80.884280
4.23.40.126	172.16.16.197	451	318 k	234	291 k	217	26 k	73.085670000	13.245934
172.16.16.128	209.35.225.165	274	288 k	71	8345	203	280 k	4.385288000	48.369102
172.16.16.128	205.203.140.65	363	251 k	128	72 k	235	179 k	1.709231000	76.713264
172.16.16.197	204.160.126.126	449	185 k	243	66 k	206	118 k	16.497808000	69.835435
172.16.16.128	204.160.104.126	327	149 k	161	64 k	166	85 k	3.317446000	11.191162
72.32.92.4	172.16.16.136	387	130 k	190	97 k	197	32 k	14.245523000	36.732188

图 5-6 会话窗口确认这两个最高用量者之间有交互

你可以通过以下显示过滤表达式来检查这个会话：

```
ip.addr == 74.125.103.163 && ip.addr == 172.16.16.128
```

如果往下翻这个列表，那么你将会在 Info 列看到一些到域名为 youtube.com 的 DNS 请求。这和我们之前所查询的 74.125.103.163 属于 Google 是相符的，因为 YouTube 属于 Google。

在此书后面的实战场景中，你还会看到如何使用端点和会话窗口。