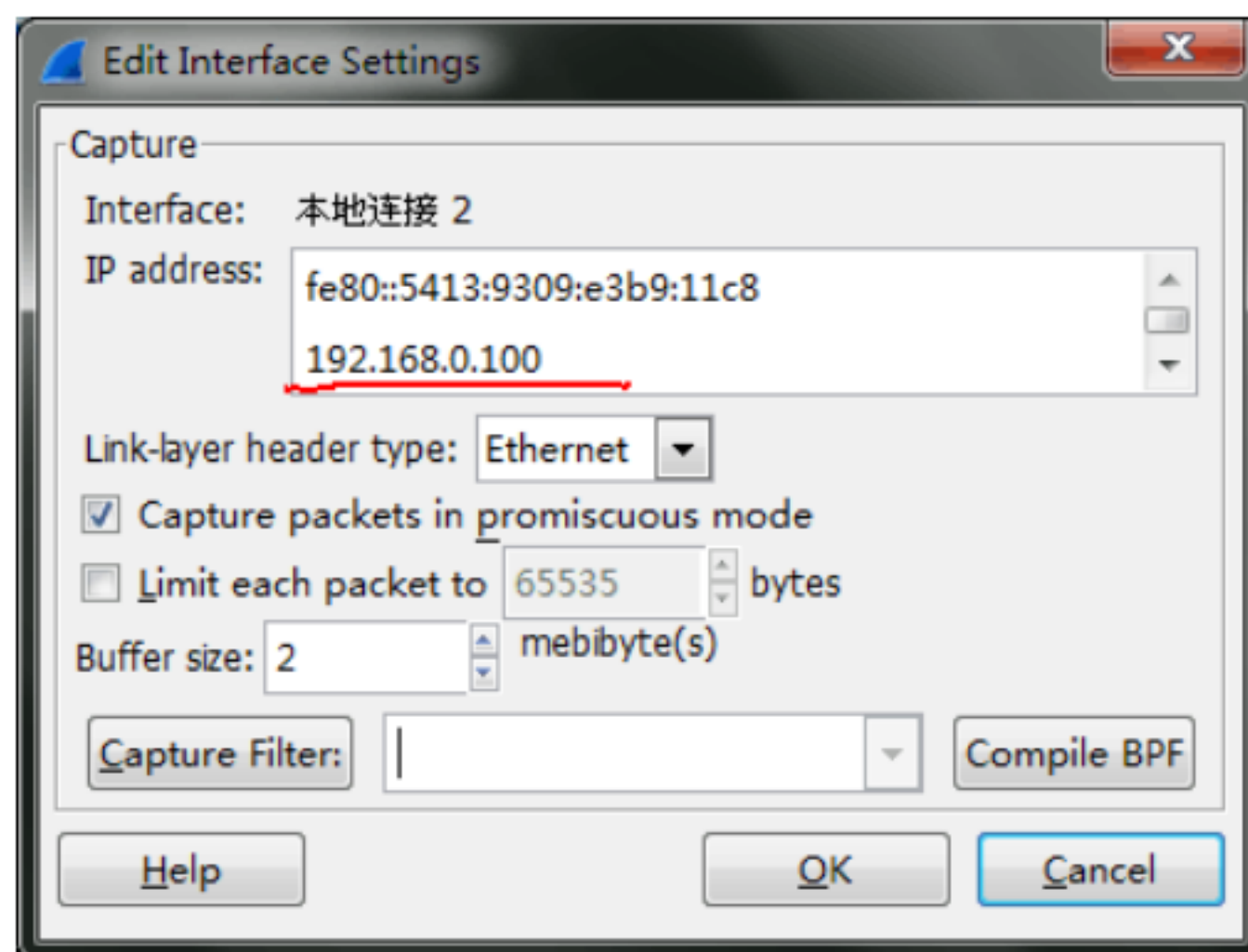
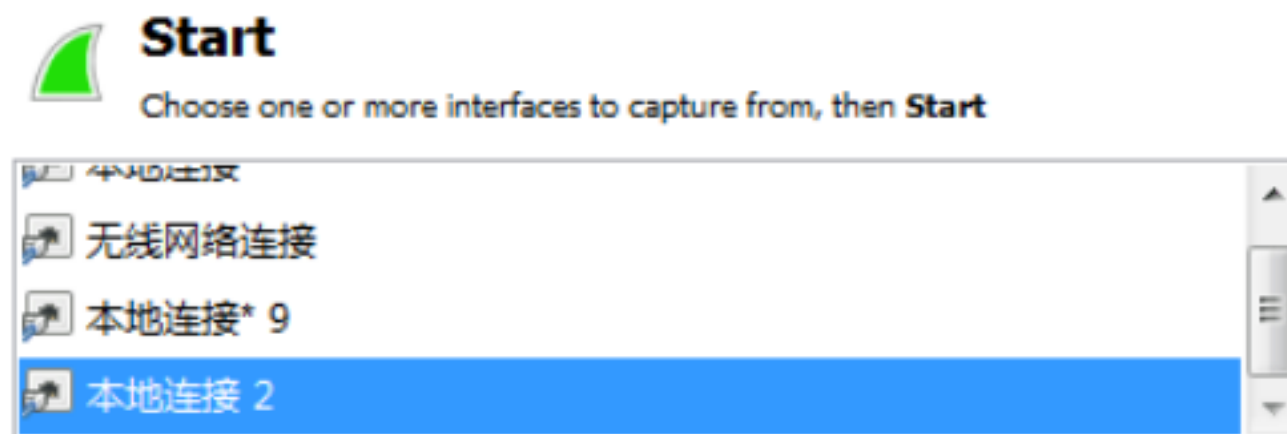


wireshark 抓包简明教程

- wireshark 抓包简明教程 1
 - 1、找到需要抓包的接口 2
 - 2、wireshark 窗口说明 3
 - 3、过滤窗口的使用 3
 - 3.1 按协议过滤 3
 - 3.2 按地址过滤 4
 - 3.3 按 tcp 或 udp 端口过滤 5
 - 3.4 过滤条件组合 6

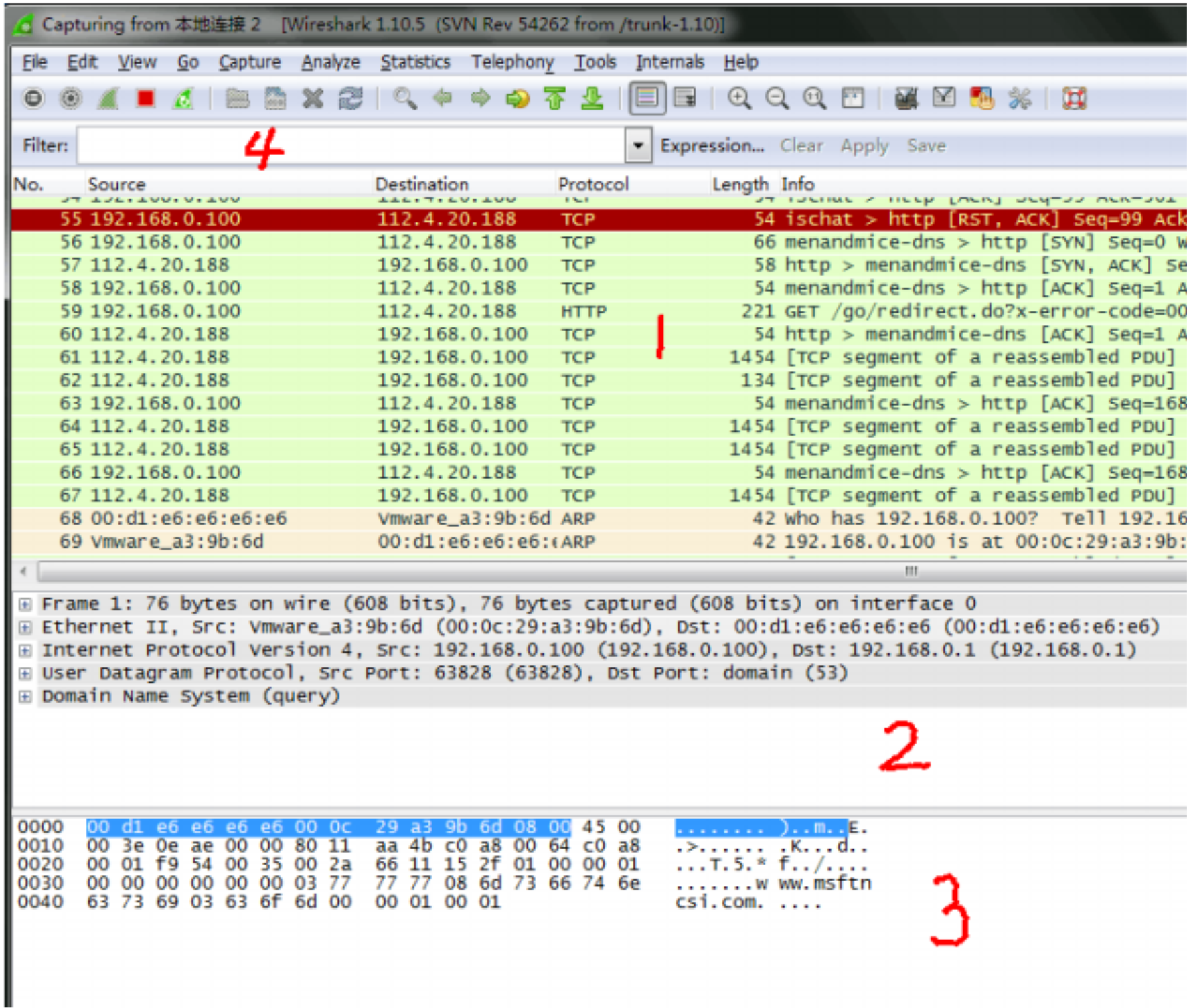
1、找到需要抓包的接口

打开 wireshark 软件，找到相应的网络接口，可能存在多个连接，此时双击某个网络连接看起 IP 地址，如与上张图的地址一样，即要查看的接口。



点击 ok 回到之前窗口，选中接口，点击 Start 开始抓包。

2、wireshark 窗口说明



- 窗口 1 是包列表，可以看到每个包的源、目的地址、协议类型、长度和信息等。
- 窗口 2 是点选某条包的详细信息，详细给出该包的 mac 层、IP 层、传输层和应用层信息。
- 窗口 3 是包内容的文本信息及字节信息。
- 窗口 4 是过滤窗口，可以过滤出需要的内容。

3、过滤窗口的使用

3.1 按协议过滤

在过滤窗口内输入协议类型，回车（或点 apply），可过滤对应类型的包。若不许可要过滤，再点 clear 清除过滤条件即可。下图以 http 为例。

Filter:	http	▼	Expression...	Clear	Apply
No.	Source	Destination	Protocol	Length	Info
13	221.176.30.196	192.168.0.100	HTTP	311	Continuat
17	221.176.30.196	192.168.0.100	HTTP	371	Continuat
25	221.176.30.196	192.168.0.100	HTTP	371	Continuat
29	221.176.30.196	192.168.0.100	HTTP	377	Continuat
47	192.168.0.100	112.4.20.188	HTTP	152	GET /ncsi
52	112.4.20.188	192.168.0.100	HTTP	134	[TCP out-
59	192.168.0.100	112.4.20.188	HTTP	221	GET /go/r
85	77.234.44.53	192.168.0.100	HTTP	217	HTTP/1.1
86	192.168.0.100	77.234.44.53	HTTP	288	GET /R/A0
93	192.168.0.100	112.4.20.188	HTTP	152	GET /ncsi
98	112.4.20.188	192.168.0.100	HTTP	134	[TCP out-
105	192.168.0.100	112.4.20.188	HTTP	221	GET /go/r
132	123.58.182.30	192.168.0.100	HTTP	284	HTTP/1.1
133	192.168.0.100	123.58.182.30	HTTP	974	Continuat
134	123.58.182.30	192.168.0.100	HTTP	285	HTTP/1.1
135	192.168.0.100	123.58.182.30	HTTP	1401	Continuat

+ Frame 13: 311 bytes on wire (2488 bits), 311 bytes captured (2488 bits) on
 + Ethernet II, Src: 00:d1:e6:e6:e6:e6 (00:d1:e6:e6:e6:e6), Dst: Vmware_a3:9b:6d
 - Internet Protocol Version 4, Src: 221.176.30.196 (221.176.30.196), Dst: 192.168.0.100

3.2 按地址过滤

ip.addr : 源或者目的地址过滤

ip.src : 源地址过滤

ip.dst : 目的地址过滤

Filter:	ip.dst == 192.168.0.100	▼	Expression...	Clear	Apply	Save
No.	Source	Destination	Protocol	Length	Info	
5907	192.168.0.1	192.168.0.100	DNS	433	Standard query re	
5909	23.76.204.57	192.168.0.100	TCP	66	http > timbuku-s	
5912	23.76.204.57	192.168.0.100	TCP	66	[TCP Retransmissi	
5916	123.58.182.30	192.168.0.100	HTTP	284	HTTP/1.1 200 OK	
5917	123.58.182.30	192.168.0.100	HTTP	285	HTTP/1.1 200 OK	
5920	123.58.182.30	192.168.0.100	TCP	54	http > fuscrypt [
5921	123.58.182.30	192.168.0.100	TCP	54	http > capioverla	
5922	23.76.204.57	192.168.0.100	TCP	54	http > timbuku-s	
5923	23.76.204.57	192.168.0.100	TCP	54	[TCP Previous seg	
5925	23.76.204.57	192.168.0.100	HTTP	233	[TCP Fast Retrans	
5930	112.4.20.188	192.168.0.100	TCP	58	http > timbuku-s	
5933	112.4.20.188	192.168.0.100	TCP	54	http > timbuku-s	
5934	112.4.20.188	192.168.0.100	TCP	54	[TCP Previous seg	
5936	112.4.20.188	192.168.0.100	TCP	473	[TCP out-Of-order	
5937	112.4.20.188	192.168.0.100	HTTP	134	[TCP out-Of-order	
5942	112.4.20.188	192.168.0.100	TCP	58	http > timbuku-s	

⊕

Frame 9: 326 bytes on wire (2608 bits), 326 bytes captured (2608 bits) on interface

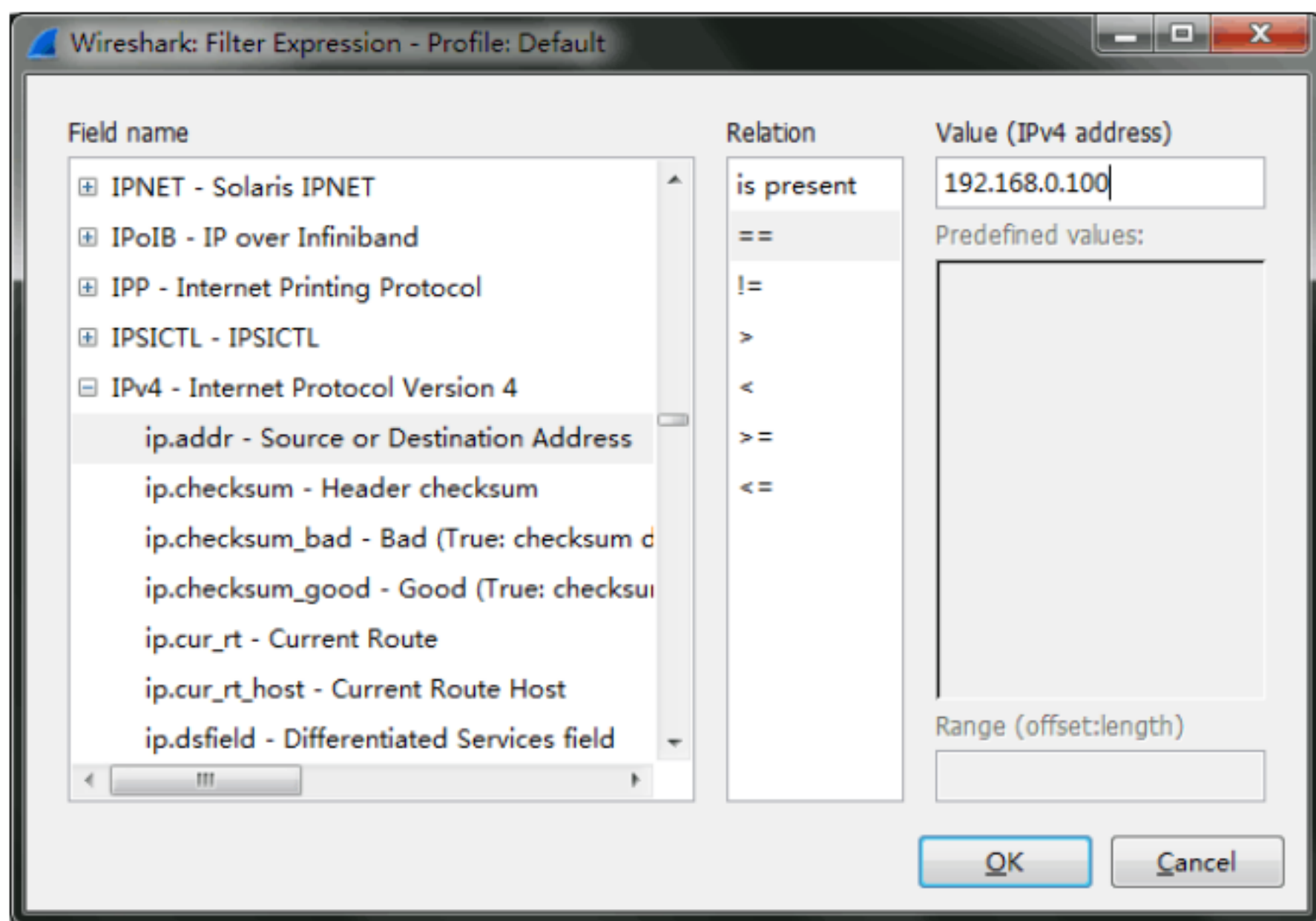
⊕

Ethernet II, Src: 00:d1:e6:e6:e6:e6 (00:d1:e6:e6:e6:e6), Dst: Vmware_a3:9b:6d (00:

⊖

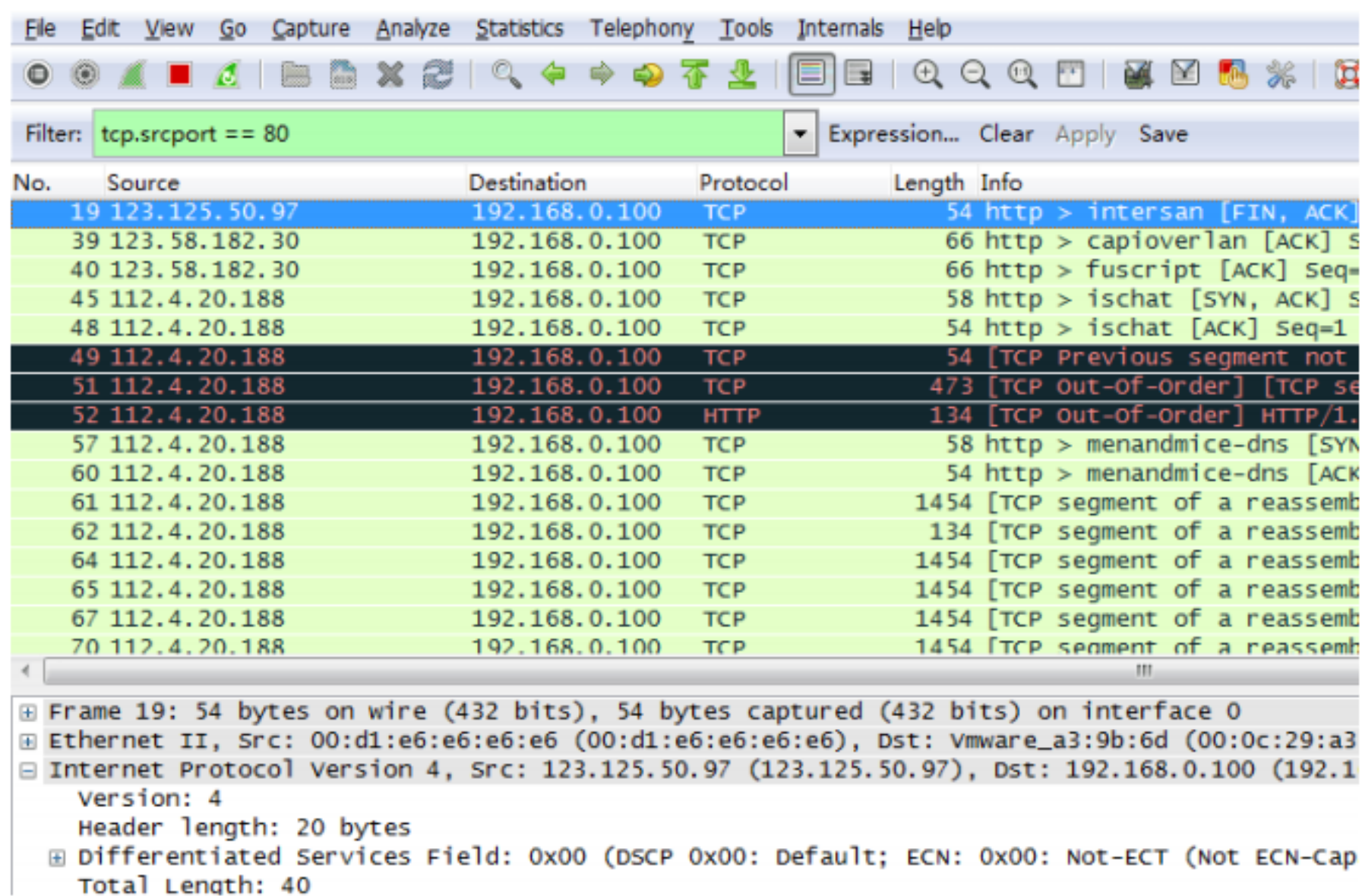
Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.100 (C

可以在过滤窗口直接输入，也可点击 Expression，可以看到所有过滤条件列表，选择需要的过滤条件即可。



3.3 按 tcp 或 udp 端口过滤

以 tcp 源端口 80 为例，如下图所示。

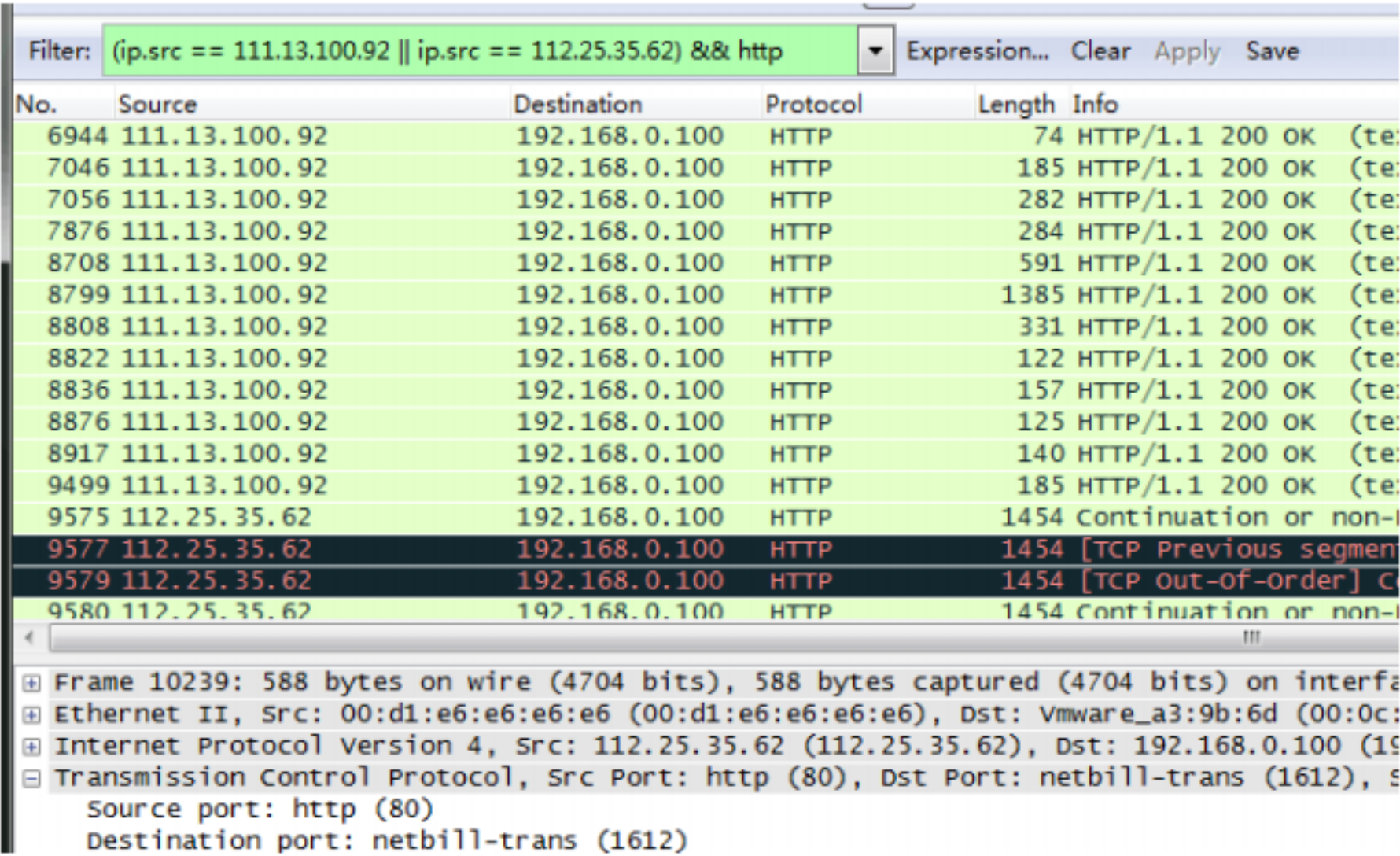


3.4 过滤条件组合

与：&&

或：||

举例，要查看百度或网易发过来的 http 消息。用 ping 或 nslookup 查看百度地址为 111.13.100.92，网易地址为 112.25.35.62，按下面的图进行过滤。



The screenshot shows the Wireshark interface with a filter applied: `(ip.src == 111.13.100.92 || ip.src == 112.25.35.62) && http`. The packet list displays several HTTP packets. The first 14 packets are from 111.13.100.92, and the next 4 are from 112.25.35.62. The details pane shows the structure of a selected packet: Frame 10239 (588 bytes on wire, 588 bytes captured), Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol.

No.	Source	Destination	Protocol	Length	Info
6944	111.13.100.92	192.168.0.100	HTTP	74	HTTP/1.1 200 OK (te:)
7046	111.13.100.92	192.168.0.100	HTTP	185	HTTP/1.1 200 OK (te:)
7056	111.13.100.92	192.168.0.100	HTTP	282	HTTP/1.1 200 OK (te:)
7876	111.13.100.92	192.168.0.100	HTTP	284	HTTP/1.1 200 OK (te:)
8708	111.13.100.92	192.168.0.100	HTTP	591	HTTP/1.1 200 OK (te:)
8799	111.13.100.92	192.168.0.100	HTTP	1385	HTTP/1.1 200 OK (te:)
8808	111.13.100.92	192.168.0.100	HTTP	331	HTTP/1.1 200 OK (te:)
8822	111.13.100.92	192.168.0.100	HTTP	122	HTTP/1.1 200 OK (te:)
8836	111.13.100.92	192.168.0.100	HTTP	157	HTTP/1.1 200 OK (te:)
8876	111.13.100.92	192.168.0.100	HTTP	125	HTTP/1.1 200 OK (te:)
8917	111.13.100.92	192.168.0.100	HTTP	140	HTTP/1.1 200 OK (te:)
9499	111.13.100.92	192.168.0.100	HTTP	185	HTTP/1.1 200 OK (te:)
9575	112.25.35.62	192.168.0.100	HTTP	1454	Continuation or non-l
9577	112.25.35.62	192.168.0.100	HTTP	1454	[TCP Previous segmen
9579	112.25.35.62	192.168.0.100	HTTP	1454	[TCP out-of-order] C
9580	112.25.35.62	192.168.0.100	HTTP	1454	Continuation or non-l

Frame 10239: 588 bytes on wire (4704 bits), 588 bytes captured (4704 bits) on interface
Ethernet II, Src: 00:d1:e6:e6:e6:e6 (00:d1:e6:e6:e6:e6), Dst: Vmware_a3:9b:6d (00:0c:
Internet Protocol Version 4, Src: 112.25.35.62 (112.25.35.62), Dst: 192.168.0.100 (19
Transmission Control Protocol, Src Port: http (80), Dst Port: netbill-trans (1612), s
Source port: http (80)
Destination port: netbill-trans (1612)