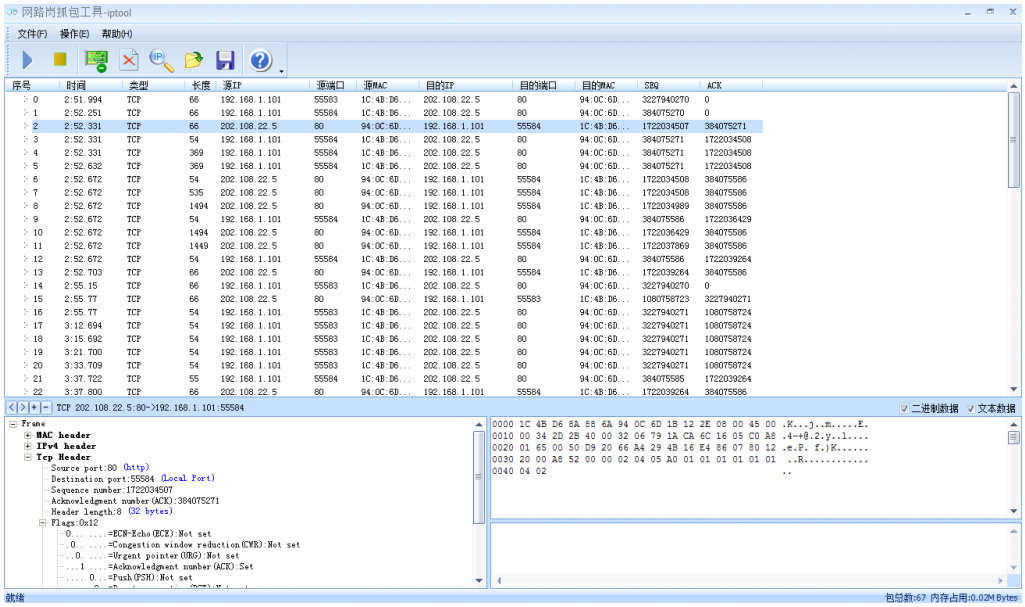
IPtool 抓包工具的使用与体验

1. 下载 IPTool

   下载该工具 http://www.duote.com/soft/18571.html

2. 运行该工具



3. 配置网卡以及 IP 过滤

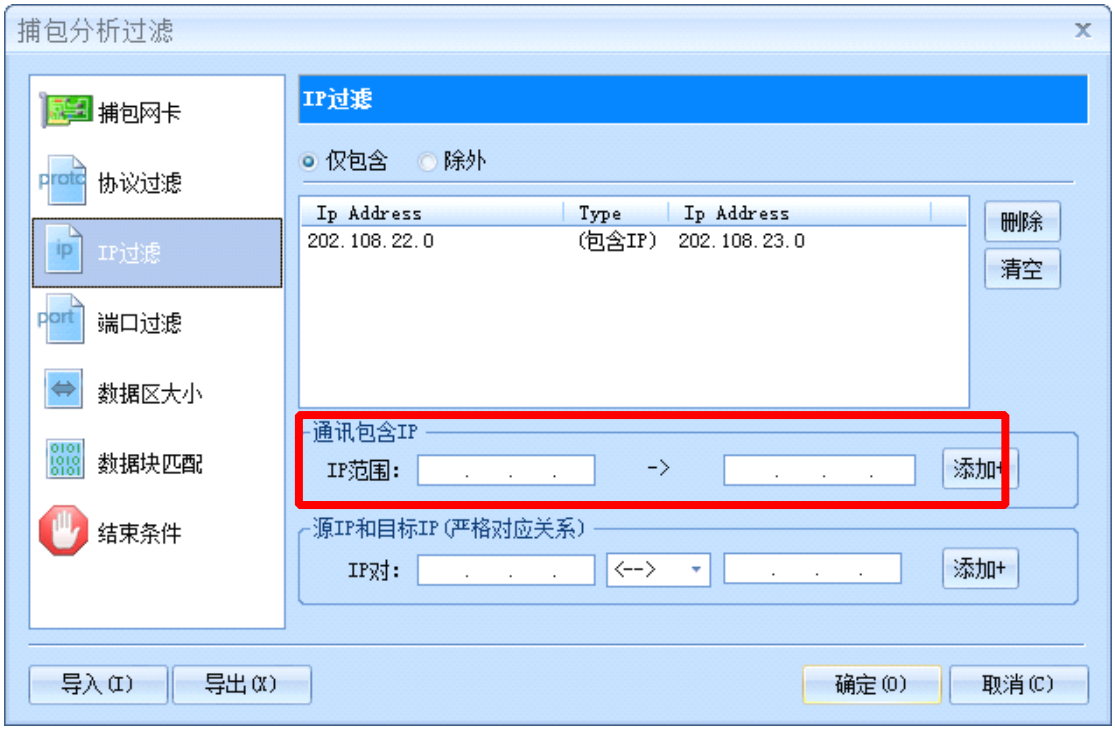
由于 IP 过多，可以通过 IP 过滤。这边使用百度的 IP 来作为目的 IP。

通过 ipconfig 查看主机的源 IP 来选定网卡。

选择网卡

配置 IP 过滤

百度的 IP 为 202.108.22.5

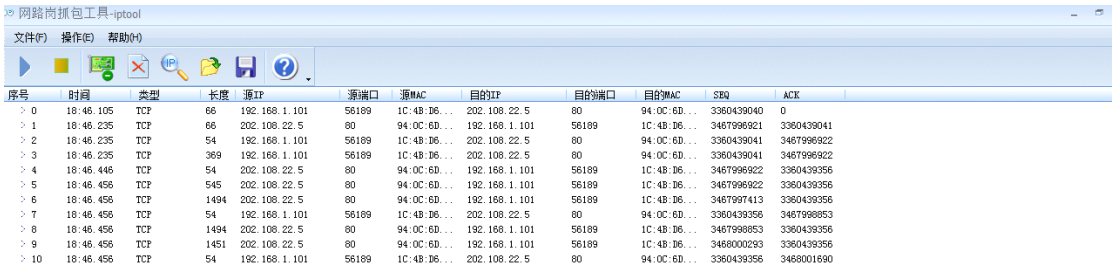


设定范围 202.108.22.0->202.108.23.0，添加。

4. 运行该工具

5. 在浏览器中输入百度 ip

得到结果如下图：



分析捕捉的结果：

0	18:46.105	TCP	66	192.168.1.101	56189	1C:4B:D6...	202.108.22.5	80	94:0C:6D...	3360439040	0
1	18:46.235	TCP	66	202.108.22.5	80	94:0C:6D...	192.168.1.101	56189	1C:4B:D6...	3467996921	3360439041
2	18:46.235	TCP	54	192.168.1.101	56189	1C:4B:D6...	202.108.22.5	80	94:0C:6D...	3360439041	3467996922
3	18:46.235	TCP	369	192.168.1.101	56189	1C:4B:D6...	202.108.22.5	80	94:0C:6D...	3360439041	3467996922
4	18:46.446	TCP	54	202.108.22.5	80	94:0C:6D...	192.168.1.101	56189	1C:4B:D6...	3467996922	3360439356
5	18:46.456	TCP	545	202.108.22.5	80	94:0C:6D...	192.168.1.101	56189	1C:4B:D6...	3467996922	3360439356
6	18:46.456	TCP	1494	202.108.22.5	80	94:0C:6D...	192.168.1.101	56189	1C:4B:D6...	3467997413	3360439356
7	18:46.456	TCP	54	192.168.1.101	56189	1C:4B:D6...	202.108.22.5	80	94:0C:6D...	3360439356	3467998853
8	18:46.456	TCP	1494	202.108.22.5	80	94:0C:6D...	192.168.1.101	56189	1C:4B:D6...	3467998853	3360439356
9	18:46.456	TCP	1451	202.108.22.5	80	94:0C:6D...	192.168.1.101	56189	1C:4B:D6...	3468000293	3360439356
10	18:46.456	TCP	54	192.168.1.101	56189	1C:4B:D6...	202.108.22.5	80	94:0C:6D...	3360439356	3468001690

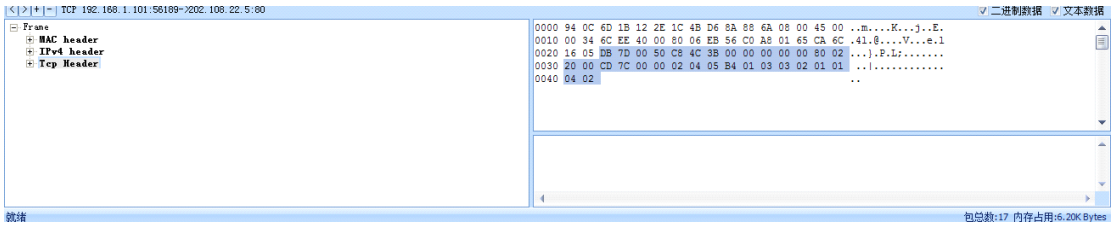
由上图可以看到，请求的协议类型是 TCP，并且能够从图中看到源 IP 和目的 IP，同时是遵循 TCP 三次握手协议的：

第一次握手：主机发送位码 SYN=1，Sequence Number 为 SEQ=3360439040 的数据包到服务器，服务器由 SYN=1 知道主机请求建立连接。

第二次握手：服务器接收到请求后确认连接请求，向主机发送 ACK Number= SEQ+1 =3360439041，SYN=1，ACK=1 随机产生 SEQ=3467996921 的包。

第三次握手：主机收到后检查 ACK Number 是不是 SEQ+1，以及位码 ack 是否为 1，若验证正确，则会再发送 ACK Number= SEQ+1=3467996922，ack=1 的包，服务器收到后，确认 SEQ 值与 ACK=1 则连接建立成功。

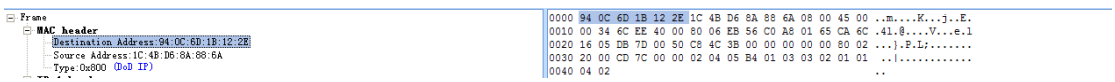
6. 观察头部内容



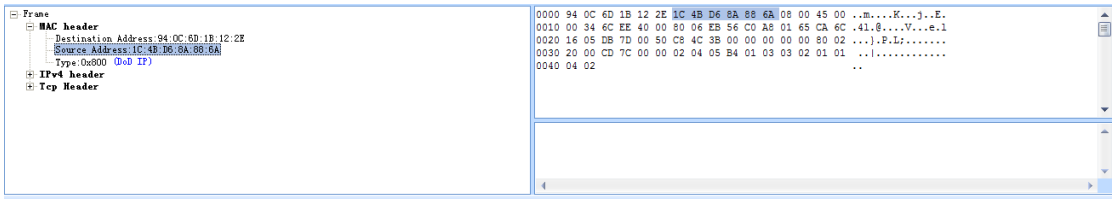
上图右边显示的是整个 Header 部分的具体内容，可以对照左边观看。颜色加深部分即为对应的部分：

首先 mac header 部分

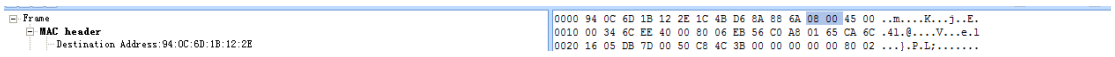
1) 目的地 mac 地址 48bit



2) 源 mac 地址 48bit



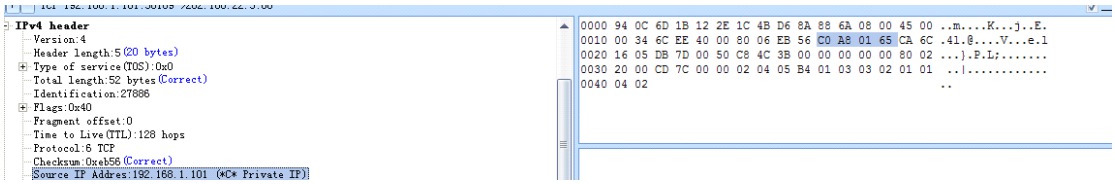
3) 数据包的协议类型 16bit



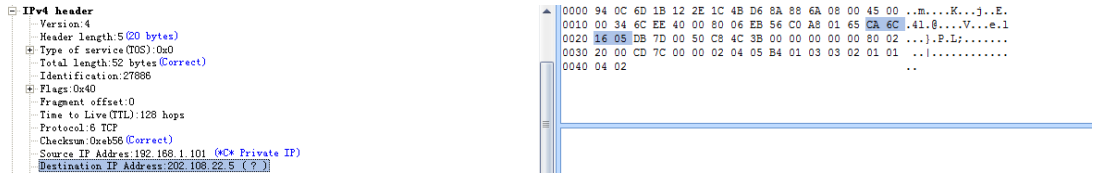
IP header 部分

这里只描述源跟目的地的 IP 地址，其余内容可以参照 IP 报文对应的图：

4) 源 IP 地址 32bit



5) 目的地 IP 地址 32bit



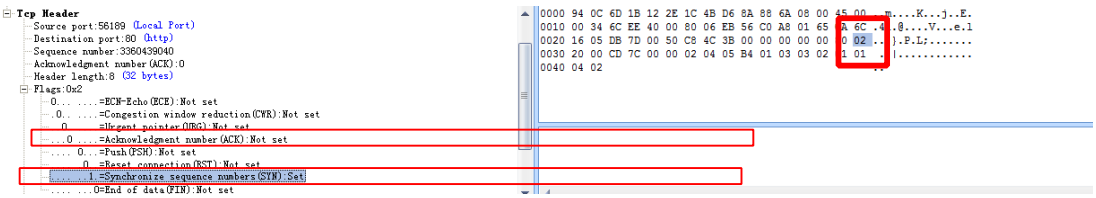
TCP header 部分

前面已经展示三次握手协议，但是并没有明显的显示，可以在 header 里面显示

第一次握手：

ACK not set ack=0

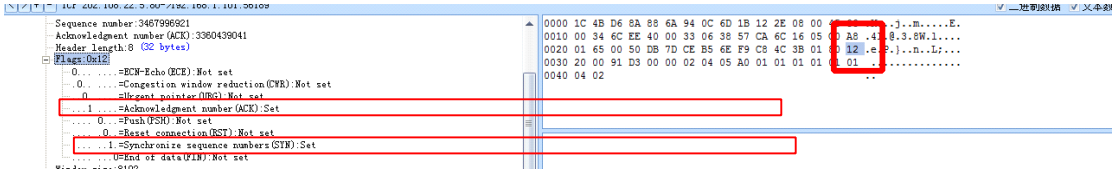
SYN set syn=1



第二次握手协议：

ACK set ack=1

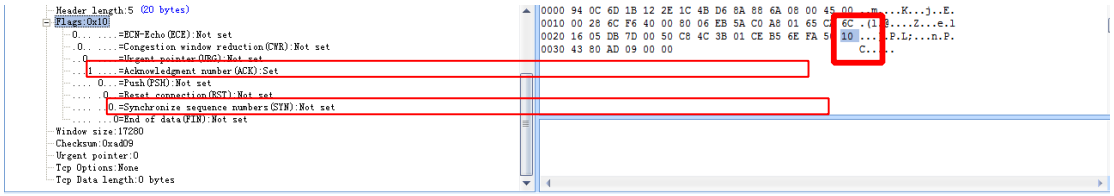
SYN set syn=1



第三次握手协议

ACK set ack=1

SYN not set　syn =0



6)　TCP 其他内容显示