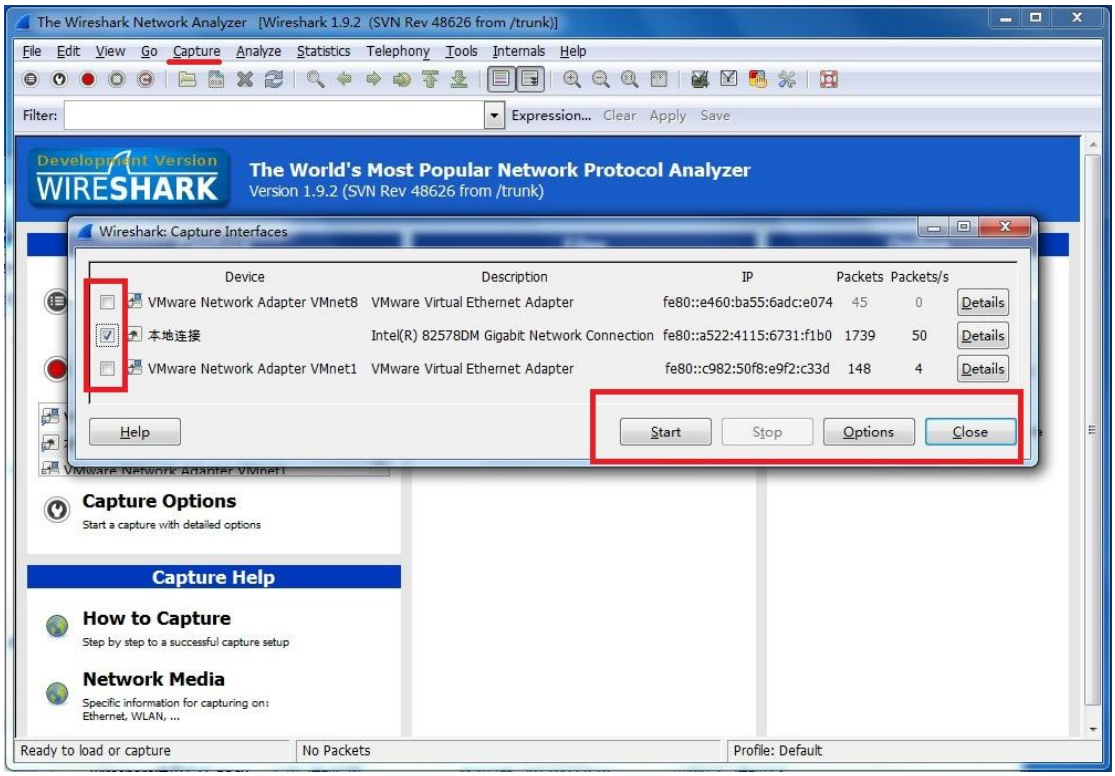
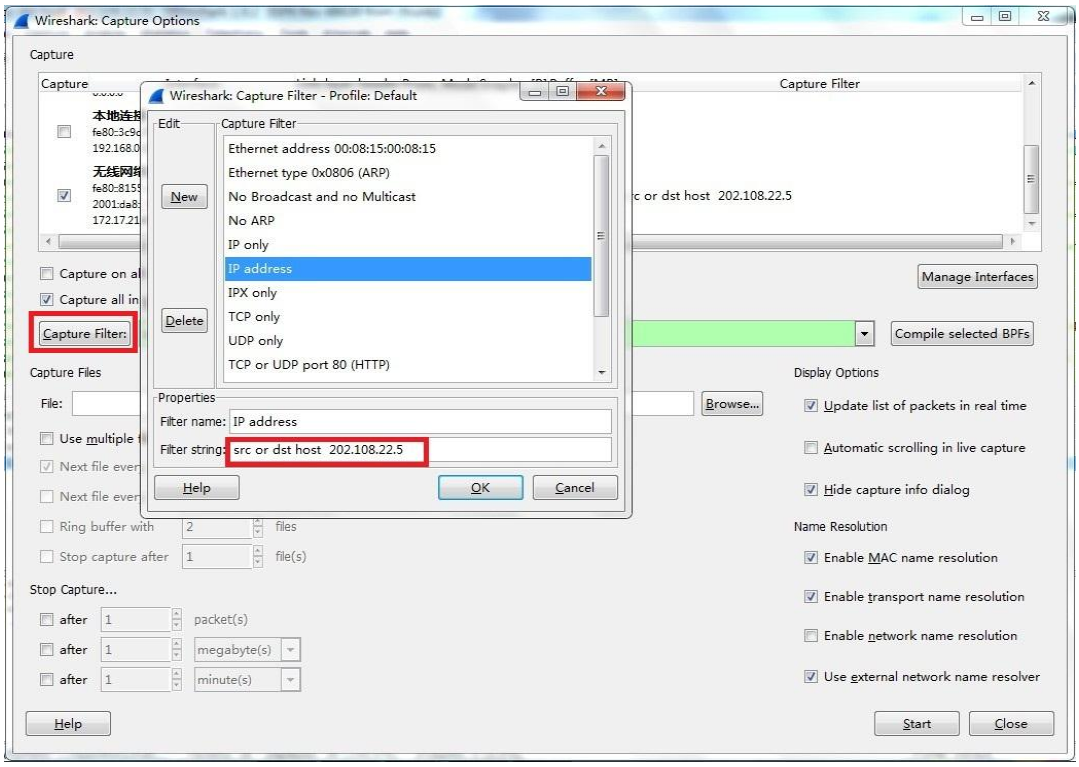
1. WireShark 开始捕获前需要进行必要的设置：

   1) Captrue->interface 中指定相应的网卡

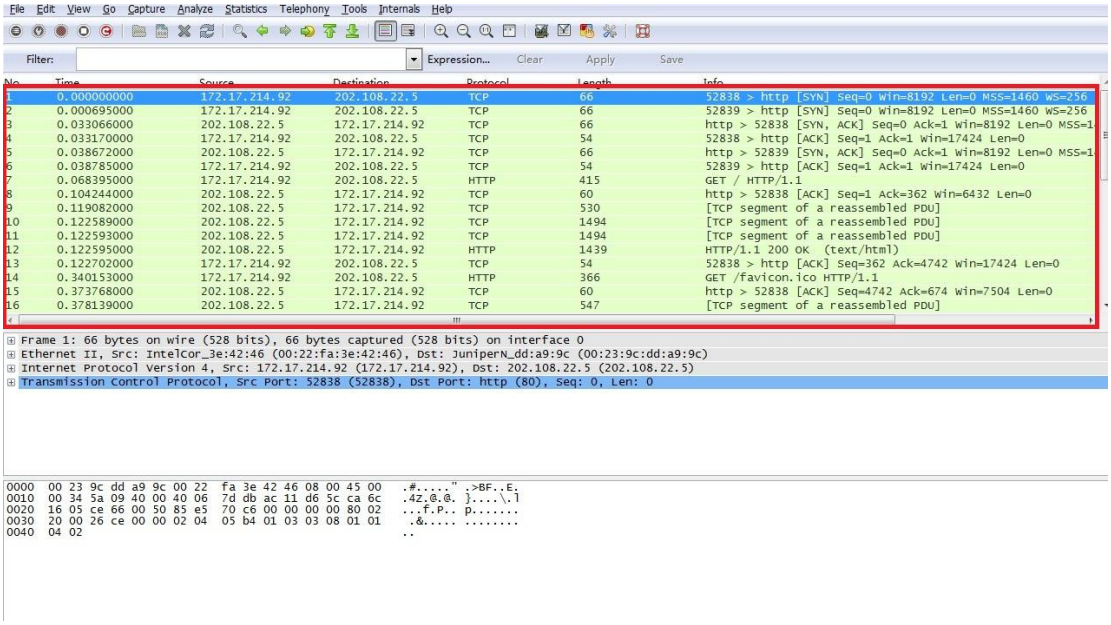


   2) 同时也可进入 options 选项中进行捕获前的过滤（有关过滤的详细介绍请看最后一节）设置。单击 Capture Filter 选项，进行捕获前 ip 过滤设置,例如百度的 ip 地址为 202.108.22.5 ,选择过滤器名为 IP address 的过滤器，设置过滤字符串设为：src or dst host 202.108.22.5 ，单击 OK。当然也可新建一个自定义的过滤器名进行保存或者直接填写 Capture Filter 不对该过滤器进行保存。



2. 捕获

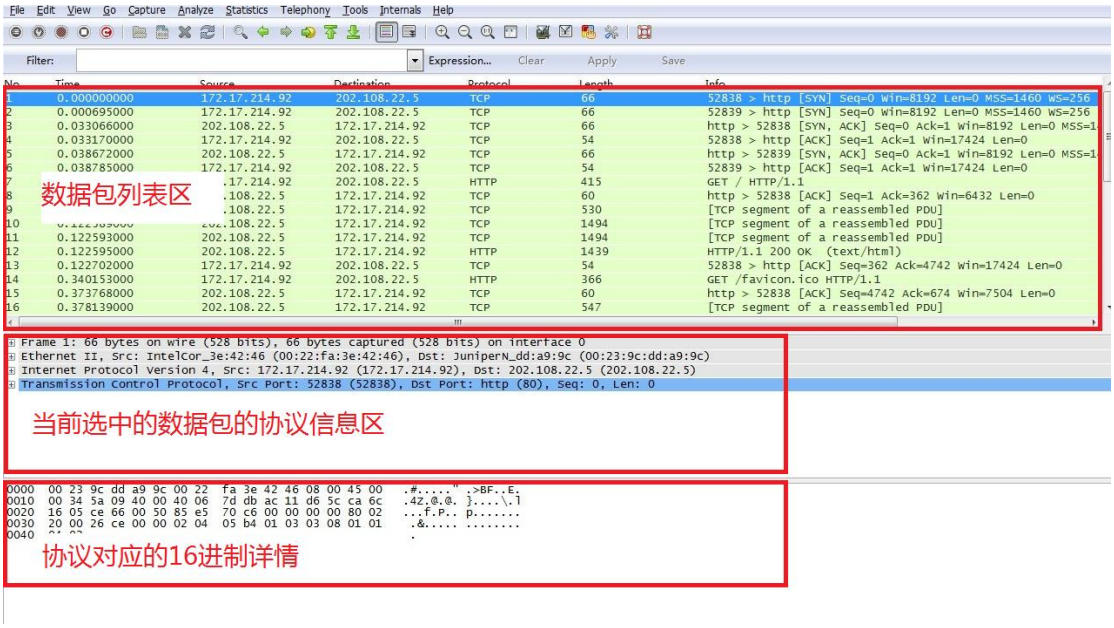
配置好后点击 start 按钮开始捕获，在浏览器上输入百度的 IP 202.108.22.5 ，运行的结果如下



3. 查看

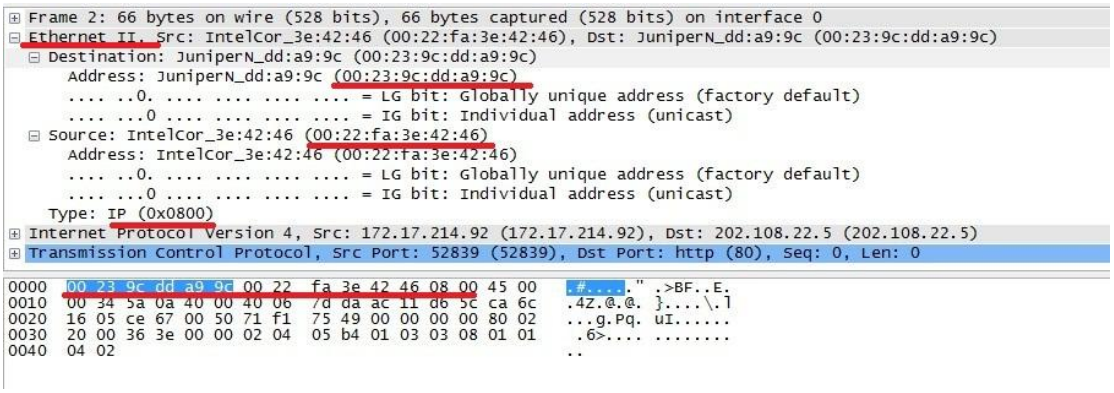
1) Wireshark 的查看与捕获是同一窗口分为三个区域：

数据包列表、当前包的协议信息、十六进制详情

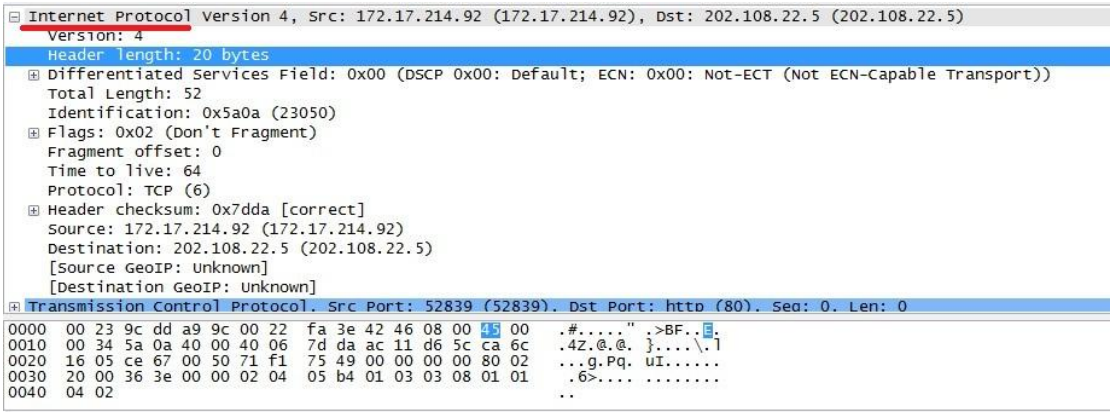


2) 查看一个数据包的协议信息

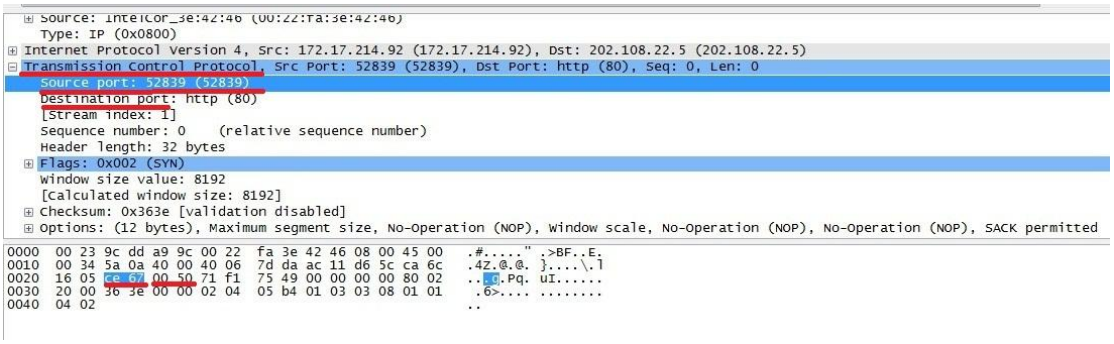
a) MAC 层：包含了目的 MAC 地址，源 MAC 地址，类型信息



b) 网络层：包含版本、头部长度、总长度等等一些信息



c) 传输层：包含了源端口、目的端口、序列号等等一些信息



4. 过滤器

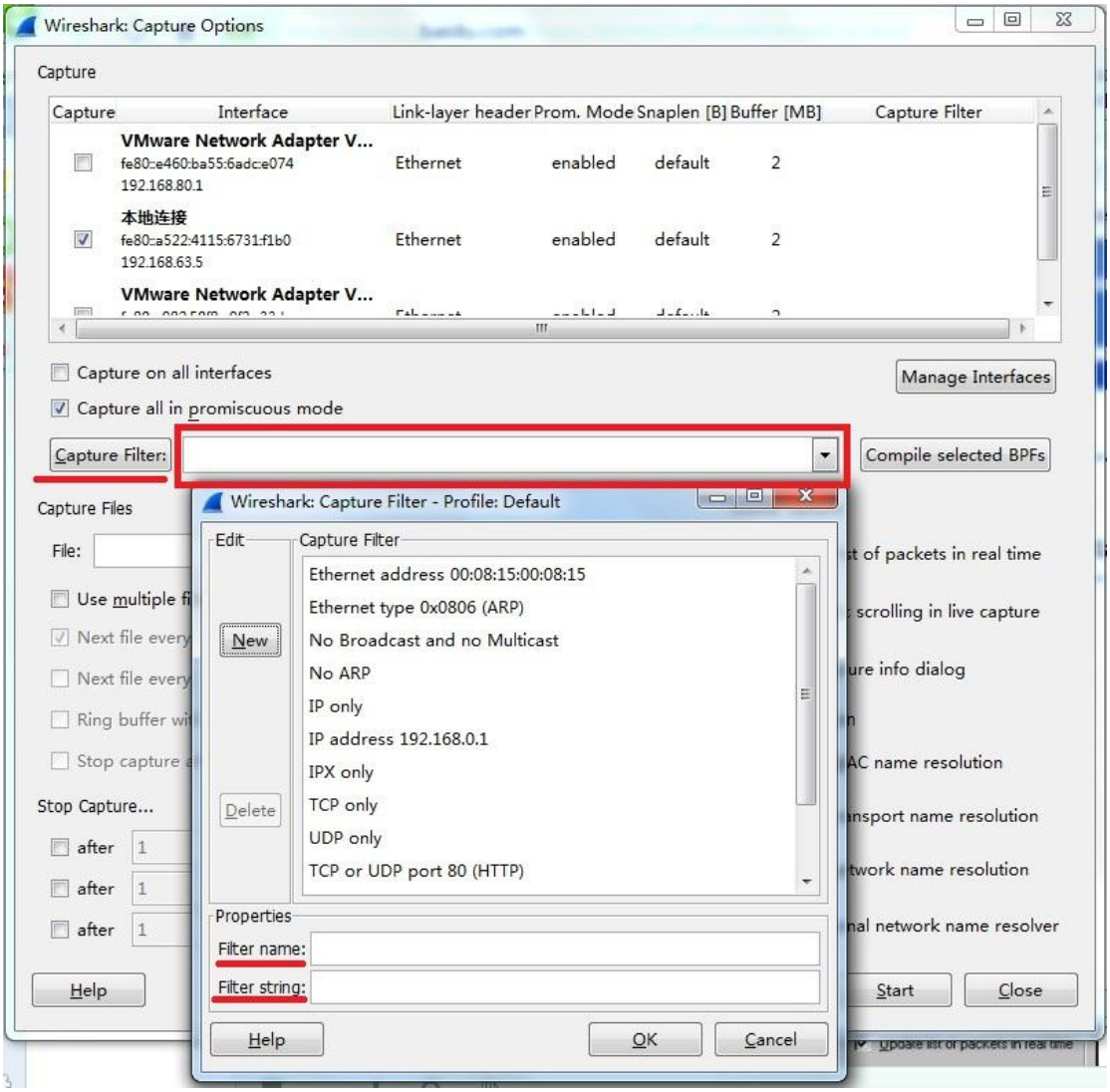
WireShark 的过滤器分为两种：捕获过滤器、显示过滤器。捕获过滤器用于决定将什么样的信息记录在捕获结果中，实在开始捕获前进行设置的。显示过滤器是在捕获的结果中进行查找，显示我们想要的信息，实在捕获之后的结果集中进行设置的。

1) 捕获过滤器

a) 设置捕获过滤器的步骤为：

（1） 选择 capture->options

（2） 填写”capture filter”或者点击”capture filter”按钮为您的过滤器起一个名字并保存，以便今后的捕获中继续使用这个过滤器



b) 捕获过滤器字符串的语法

语法：	Protocol	Direction	Host(s)	Value	Logical Operations	Other expression
例子：	tcp	dst	10.1.1.1	80	and	tcp dst 10.2.2.2 3128

（1） Protocol（协议）

可能的值：ether、fddi、ip、arp、rarp、decent、lat、sca、moprc、mopdl、tcp、udp

（2） Direction（方向）

可能的值：src、dst、src and dst、src or dst

（3） Host(s)

可能的值：net、port、host、portrange

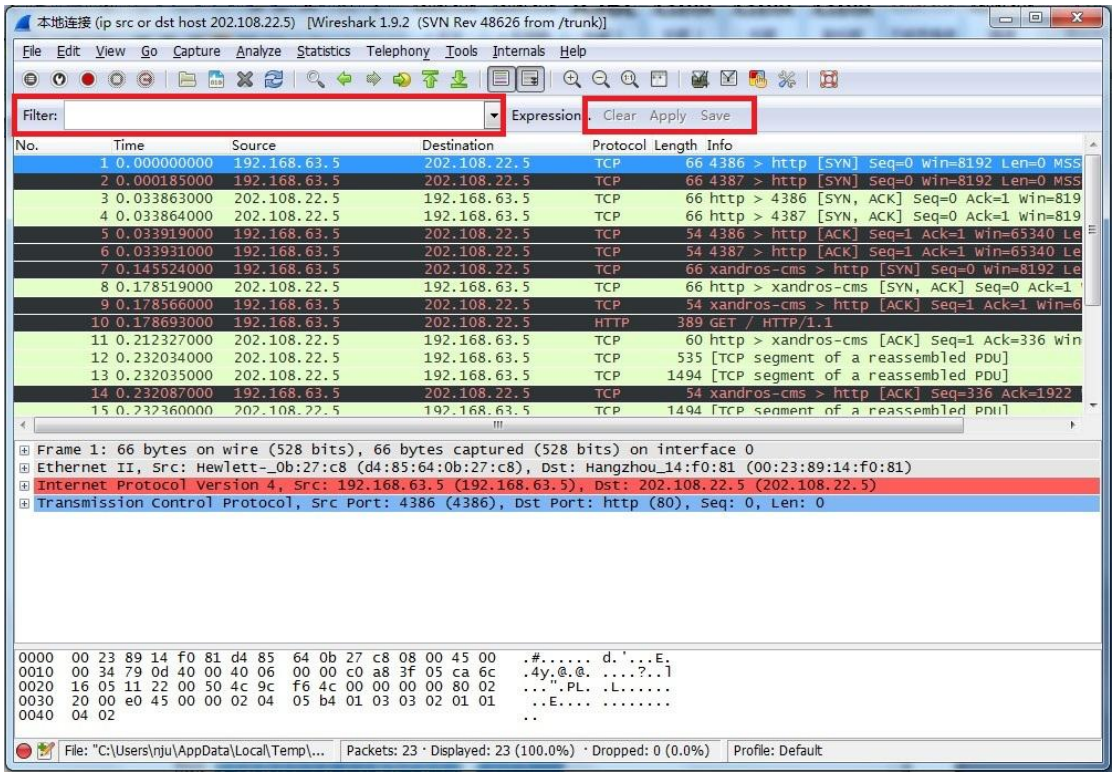
（4） Logical Operations（逻辑运算）

可能的值：and、or、not

2) 显示过滤器

a) 显示过滤器设置步骤

可直接在 Wireshark 主界面的 Filter 栏中直接填写。



b) 过滤规则

（1） 常见函数 1

eth：只显示以太网帧

eth.addr == AA:BB:CC:DD:EE:FF ：只显示源或目的 MAC 地址为 AA:BB:CC:DD:EE:FF 的以太网帧

eth.src/eth.dst == AA:BB:CC:DD:EE:FF :与 eth.addr 类是，可以具体指定源、目的的地址

（2） 常见函数 2

ip :只显示 IP 包

ip.addr == A.B.C.D :只显示源或目的地址为 A.B.C.D 的 IP 包

ip.src/ip.dst == A.B.C.D ：与 ip.addr 类似，可以指定源、目的地址

（3） 常见函数 3

tcp : 只显示 TCP 报文

tcp.port == Number ：只显示源或目的端口为 Number 的 TCP 报文

tcp.srcport/tcp.dstport == Number :与 tcp.port 类似，可以指定具体源。目的端口

（4） 常见函数 4

http : 只显示 http 的报文

telnet : 只显示 telnet 报文

dhcp：只显示 DHCP 的报文

arp：只显示 ARP 报文

c) 逻辑关系

有些时候，过滤需要多个函数联合定义，不同的函数之间可以使用如下的关系来定义，分别是与、否、或、括号：

and 、 not 、|| 、()

d) 举例

eth.addr == 11:22:33:44:55:66

ip.src == 1.2.3.4 and ip.dst == 4.3.2.1

not arp and !(udp.port == 53)

tcp.port == 69 || udp.port == 69