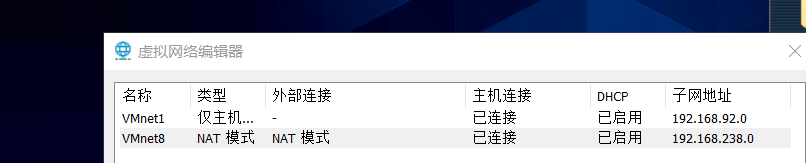
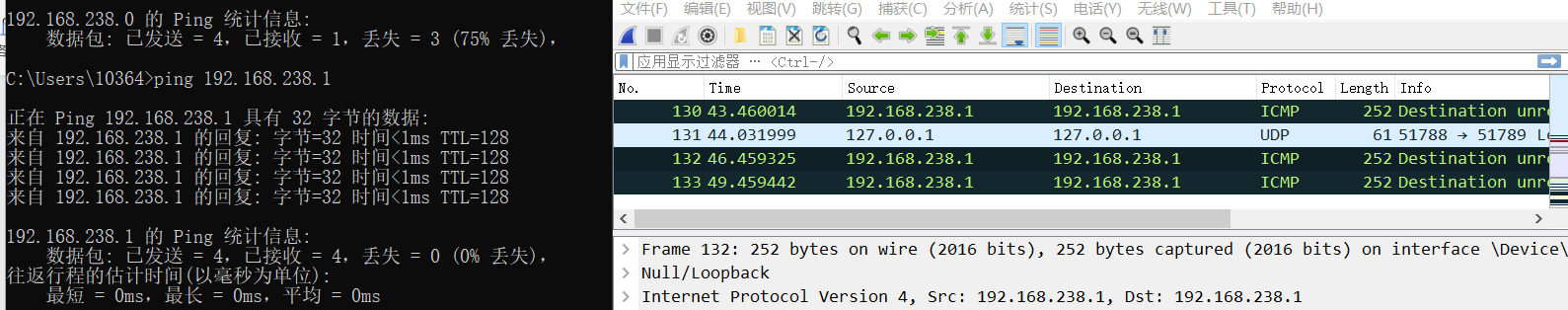
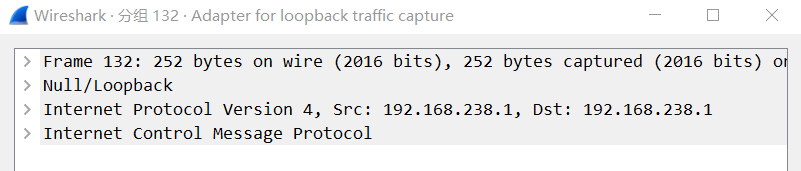
A:

1. **从图中可知我的虚拟机ip地址为“192.168.238.0”；**

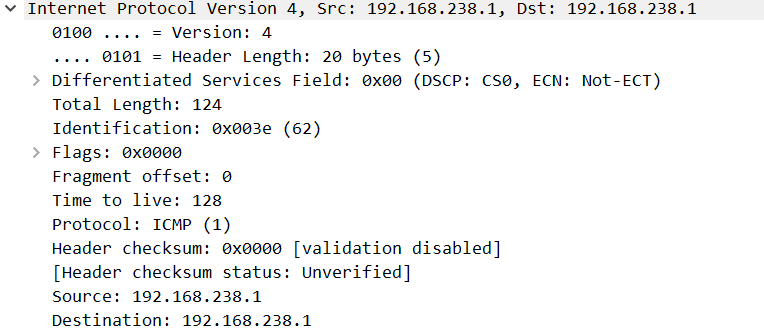


1. **命令框中ping虚拟机地址，并在wireshark中“protocol”为“ICMP”的一栏双击进入；**

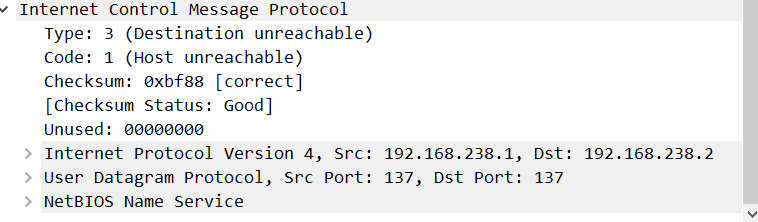


1. **得到上图并进行协议分析，以下是协议分析：**

**由于是本机通信，采用的是环回地址127.0.0.1，没有和其他主机进行交换，所以是空的。**



**以上就是ip报文的内容信息，包括版本，包头长度，源ip地址等信息；**



**以上是ICMP协议的具体信息，由图可知，checksum的值为“0xbf88”，checksum的计算步骤为：**

**1、 先将需要计算checksum数据中的checksum设为0；**

**2、 计算checksum的数据按2byte划分开来，每2byte组成一个16bit的值，如果最后有单个byte的数据，补一个byte的0组成2byte；**

**3、 将所有的16bit值累加到一个32bit的值中；**

**4、 将32bit值的高16bit与低16bit相加到一个新的32bit值中，若新的32bit值大于0Xffff,**

**再将新值的高16bit与低16bit相加；**

**5、 将上一步计算所得的16bit值按位取反，即得到checksum值0xbf88，存入数据的checksum字段即可。**

**B：**

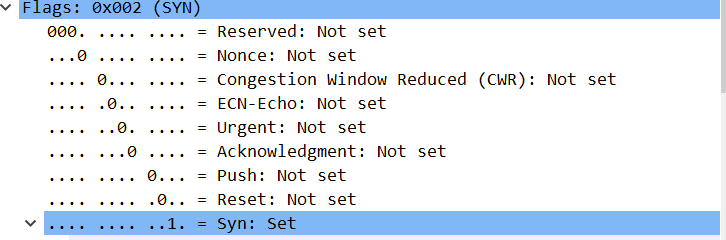
**虚拟机地址：192.168.238.0**

**本机地址：10.99.61.231**

**三次握手：**

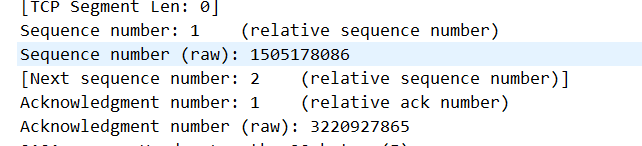
**在本机ping虚拟机并扔出了包后，虚拟机开始接收：**





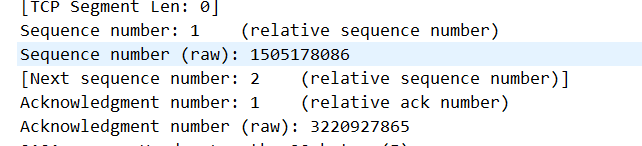
**第一次握手：主机A发送位码为syn＝1，随机产生seq number= X 的数据包到服务器，主机B由A发送的SYN=1知道，A要求建立联机 , A进入:SYN\_SENT状态；**





**第二次握手：主机B收到请求后要确认联机信息，向A发送ack number=(主机A的seq+1)，syn=1，ack=1，随机产生seq=Y的包,B进入SYN\_RCVD状态；**

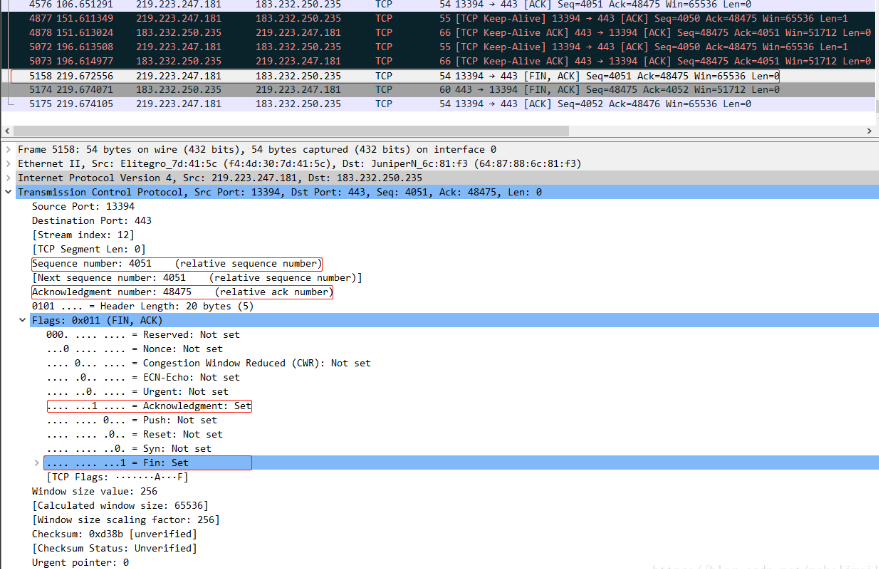




**第三次握手：主机A收到后检查ack number是否正确，即第一次发送的seq number+1，以及位码ack是否为1，若正确，主机A会再发送ack number=(主机B的seq+1)，ack=1，主机B收到后确认收到的seq值与发送给A的seq+1是否相等和ack是否为1来判断连接是否建立成功,A和B都进入ESTABLISED状态，FIN=1，表示此报文段的发送方已经发送完毕。并要求释放连接。**

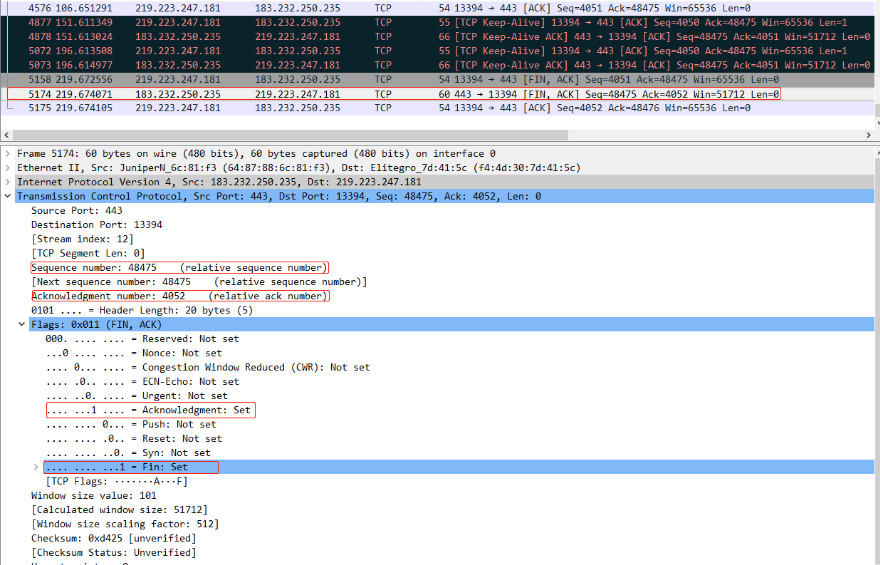
**四次挥手：**

**第一次挥手**



**主机发送一个FIN = 1，序号seq=u，主动发起并停止再发送数据 ，关闭主机到Server的数据传送，等待虚拟机端的确认；Client进入FIN\_WAIT\_1状态；主机发送Fin + Acknowledgement 给客户端，表示自己要断开连接，这个时候主机端已经没有数据要发送了。**

**第二次挥手**

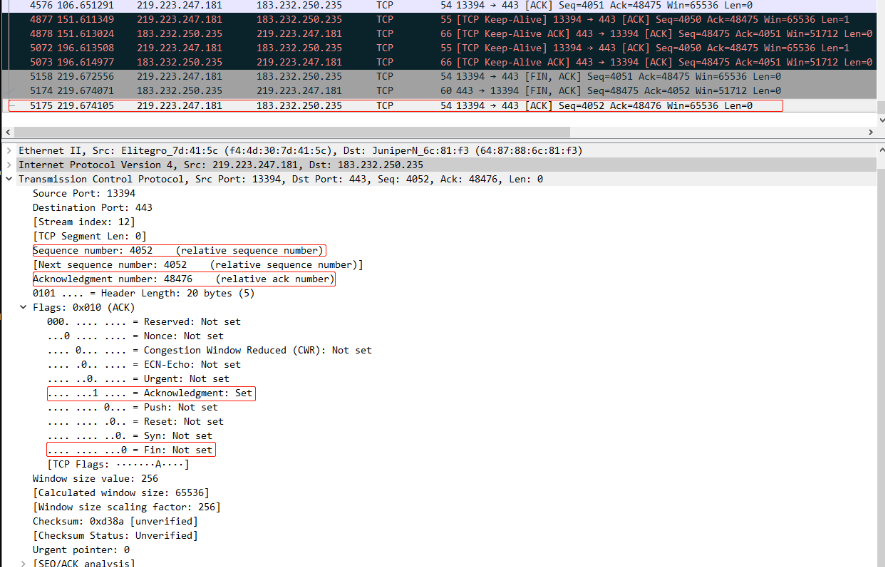


**虚拟机收到连接释放报文段后即发出确认报文段，（ACK=1，确认号ack=u+1，序号seq=v），虚拟机进入CLOSE-WAIT（关闭等待）状态，此时的TCP处于半关闭状态，主机到客户端的连接释放,但是客户端到主机还未释放。客户端接收到主机发送的断开请求连接，那么这个时候客户端需要发送一个Acknowledgement=1用于确定客户请求断开的信息成功接收了；**

**第三次挥手**

**主机收到虚拟机的确认后，进入FIN-WAIT-2（终止等待2）状态，等待虚拟机发出的连接释放报文段 FIN = 1，Seq=w, ACK=1，ack=u+1。客户端所有的数据已经接收完毕，会发送一个Fin=1，而Acknowledgement=0用于表示客户端已经没有数据要发送了，需要关闭连接。**

**第四次挥手**



**主机收到虚拟机的连接释放报文段后，对此发出确认报文段（ACK=1，seq=u+1，ack=w+1），主机进入TIME-WAIT（时间等待）状态。此时TCP未释放掉，需要经过时间等待计时器设置的时间2MSL后，主机才进入CLOSED状态。主机端需要发送一个Acknowledgement = 1表示这个主机端接收到了客户端的关闭请求信息，这样一来双方的就都关闭了。**

**C:**

TCP 第一次握手的 SYN 丢包了，会发生了什么？

**SYN是同步序列号，用来发起一个连接，SYN=1的报文不能携带数据，服务器通过SYN=1知道主机要求建立联机，所以丢包后建立连接失败。**

TCP 第二次握手的 SYN、ACK 丢包了，会发生什么？

**ACK是确认标识，当ACK=1时确认字段才有效。所以没有ACK时服务器发回客户端的是无效请求。**

TCP 第三次握手的 ACK 包丢了，会发生什么？

**主机A收到后检查ack number是否正确，即第一次发送的seq number+1,以及位码ack是否为1，若正确，主机A会再发送ack number(主机B的seq+1),ack=1，主机B收到后确认seq值与ack=1则连接建立成功。ACK包时确认标识，若丢了客户端无法确认，无法和主机连接成功。**

**参考文献**

1. CSDN博客：《TCP/IP协议三次握手和四次挥手之抓包详解》