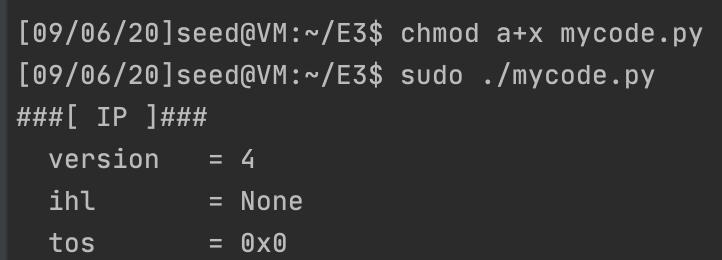
Lab3 Report

57111739吴星灿

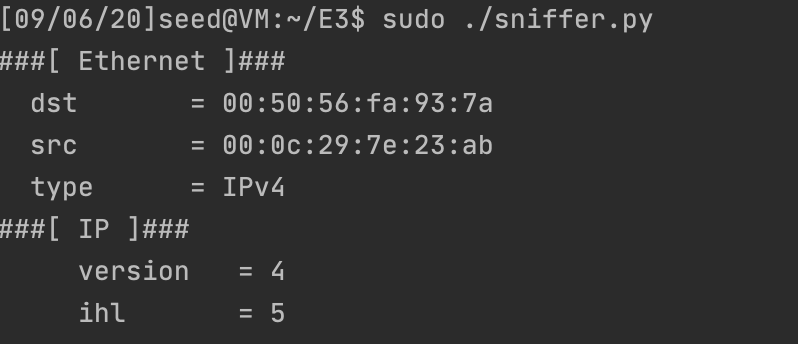
**Lab1**

**Task1**

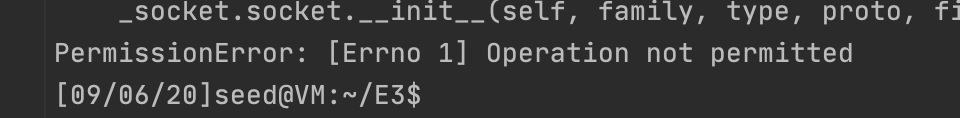




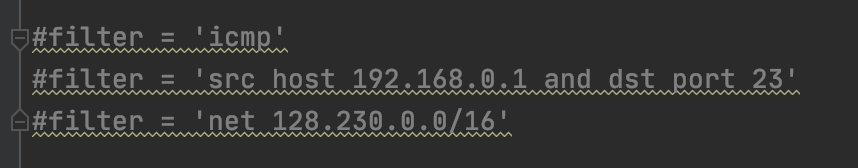
运行sniffer.py

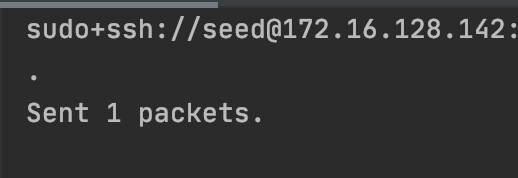


当没有root权限时，运行sniffer得到的权限错误。



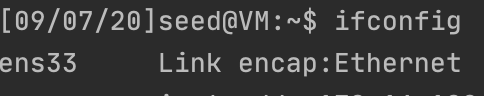
编写filter





**Task2.1**

ifconfig得到网卡



Q1 以混杂模式监听指定网卡，将设置filter与handle绑定，启动回调函数pcaploop当收到报文时调用gotpacket

Q2

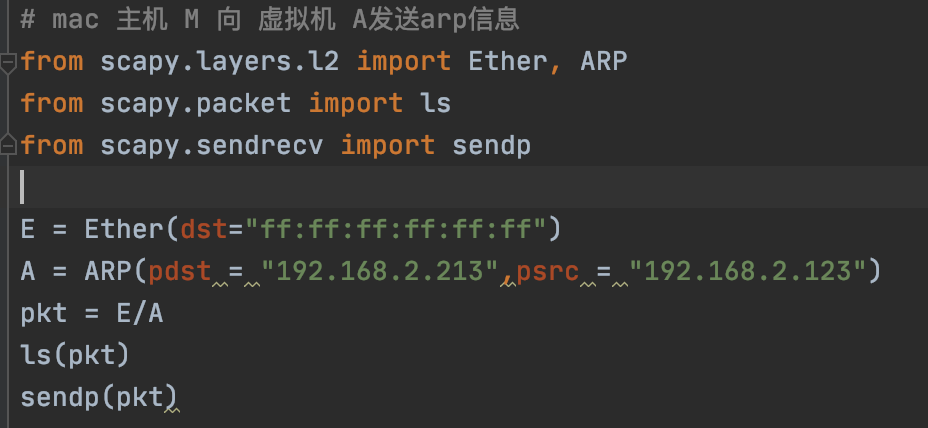


通过gdb调试发现，如果没有root权限，在执行pacp\_complie时发生分页错误。即无法拿到监听的句柄。

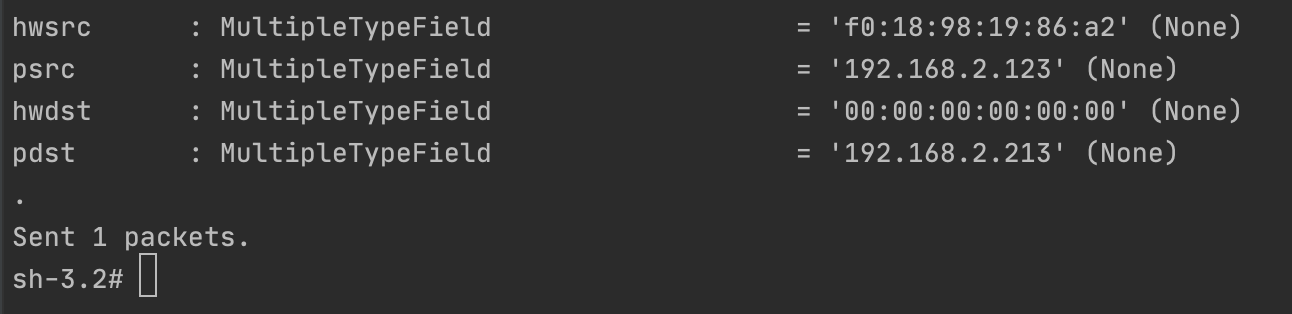
Q3 打开混杂模式，所有经过网卡的流量都会被监听，关闭只监听mac地址是自己的流量。

**Lab2**

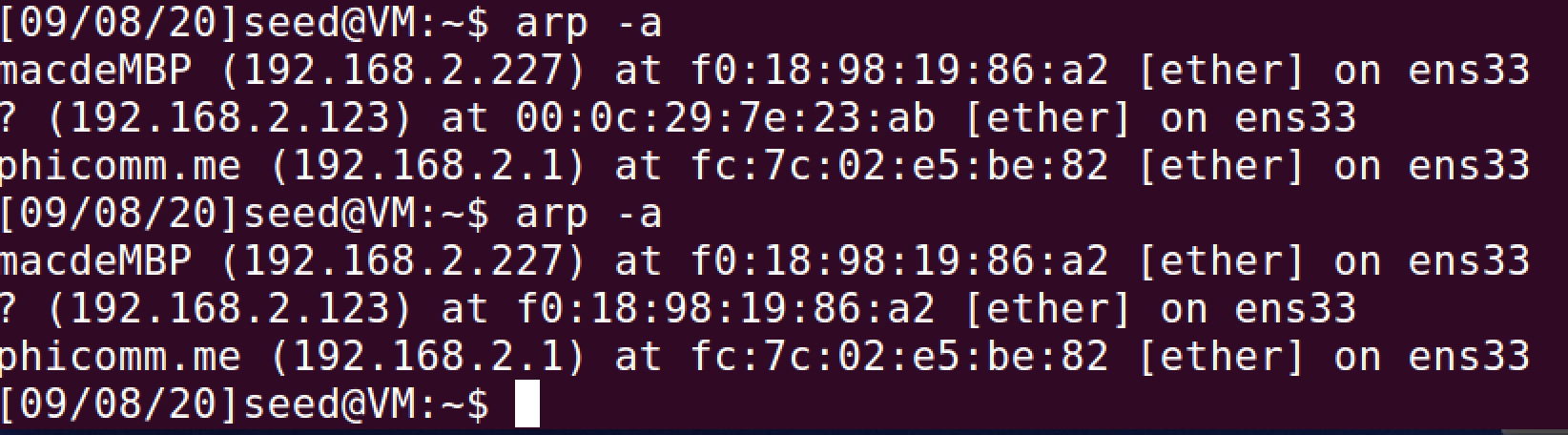
**Task1A**



用root权限发送



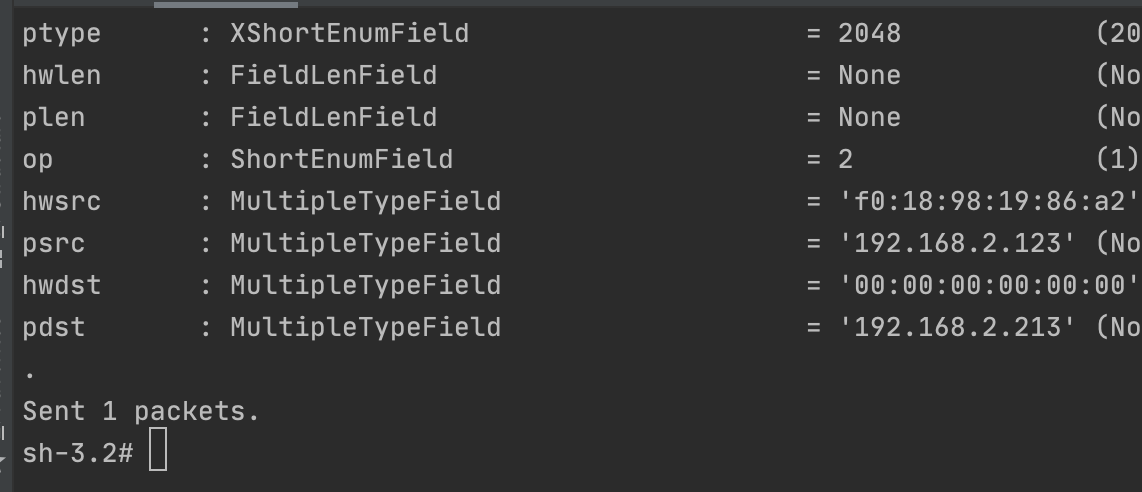
虚拟机A的arp表前后变化如下



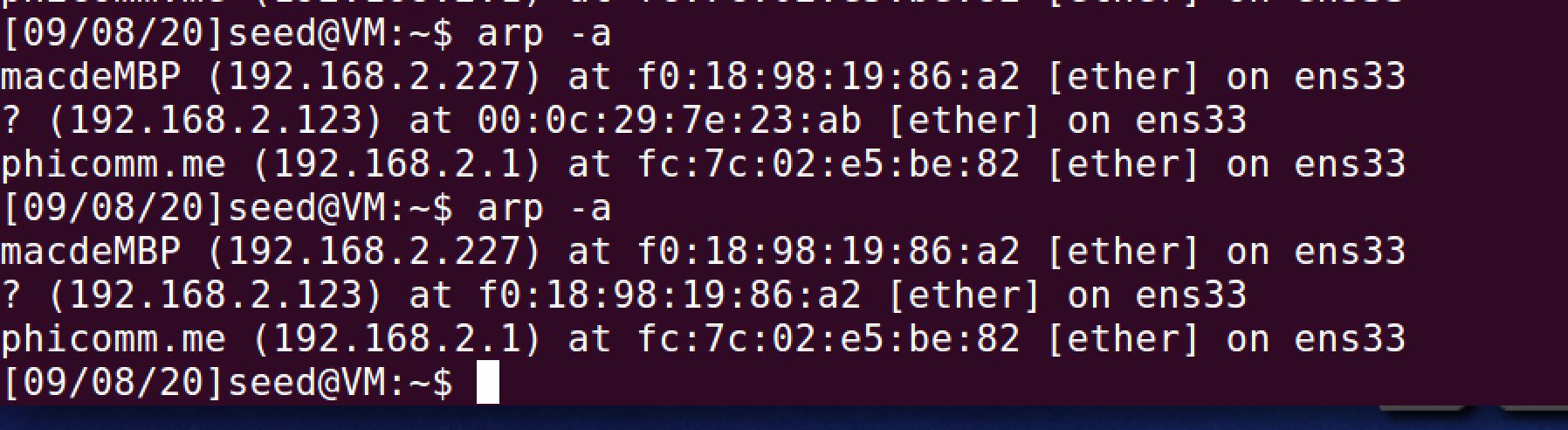
可以看出虚拟机B的mac地址已经被主机M的mac地址覆盖。

**Task1B**



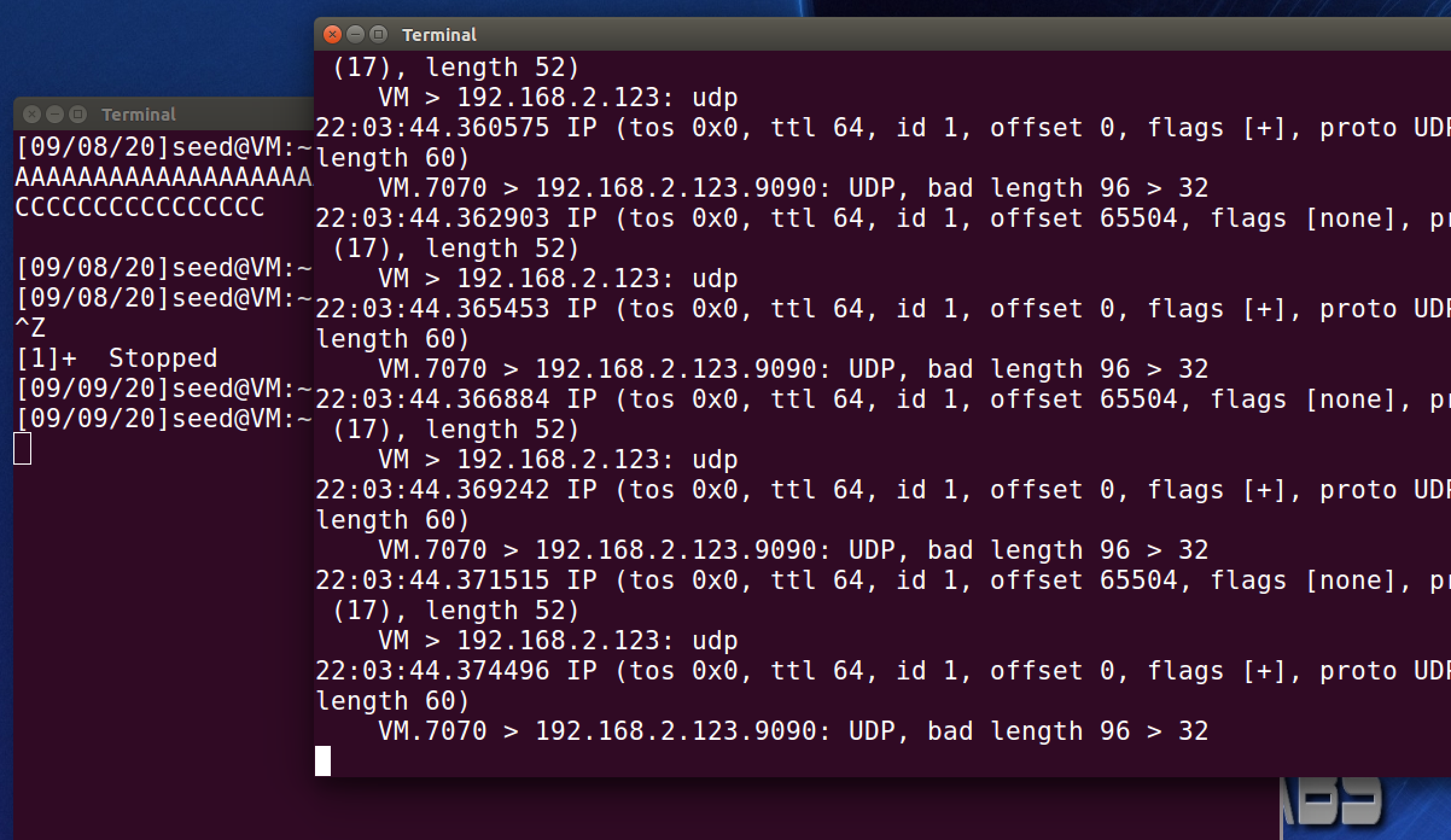
用root权限发送

虚拟机A的arp表前后对比



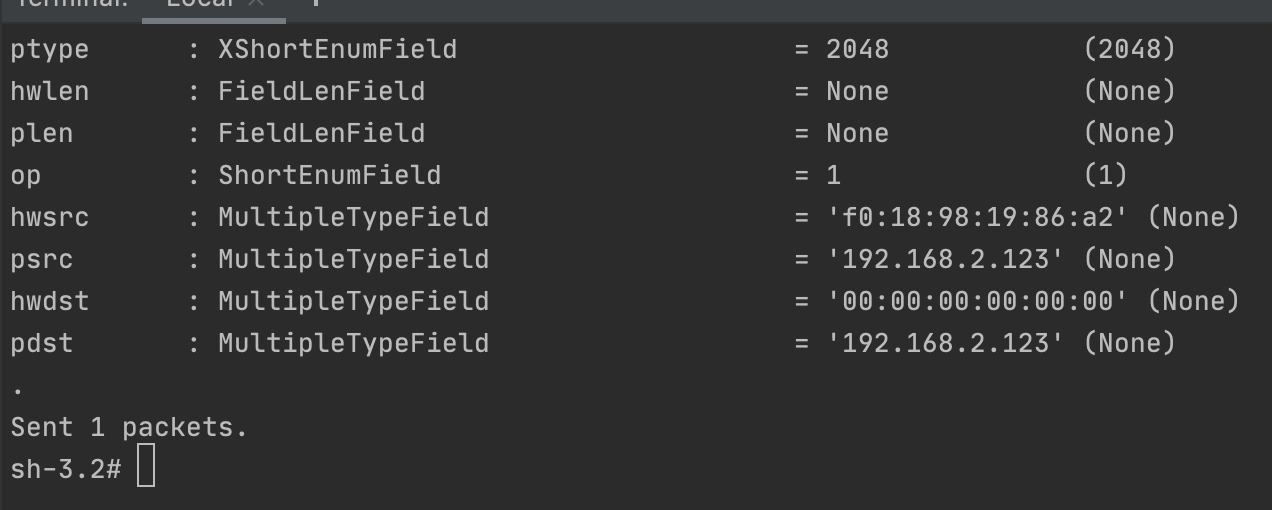
可以看出虚拟机B的mac地址已经被主机M的mac地址覆盖。

**Task1C**

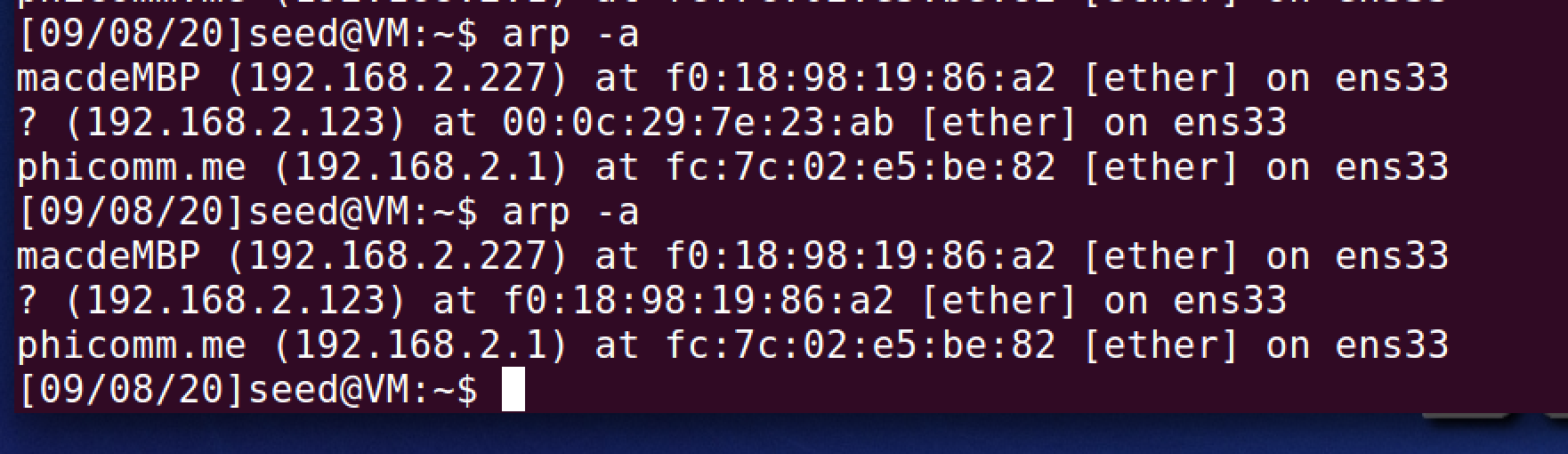




用root权限发送



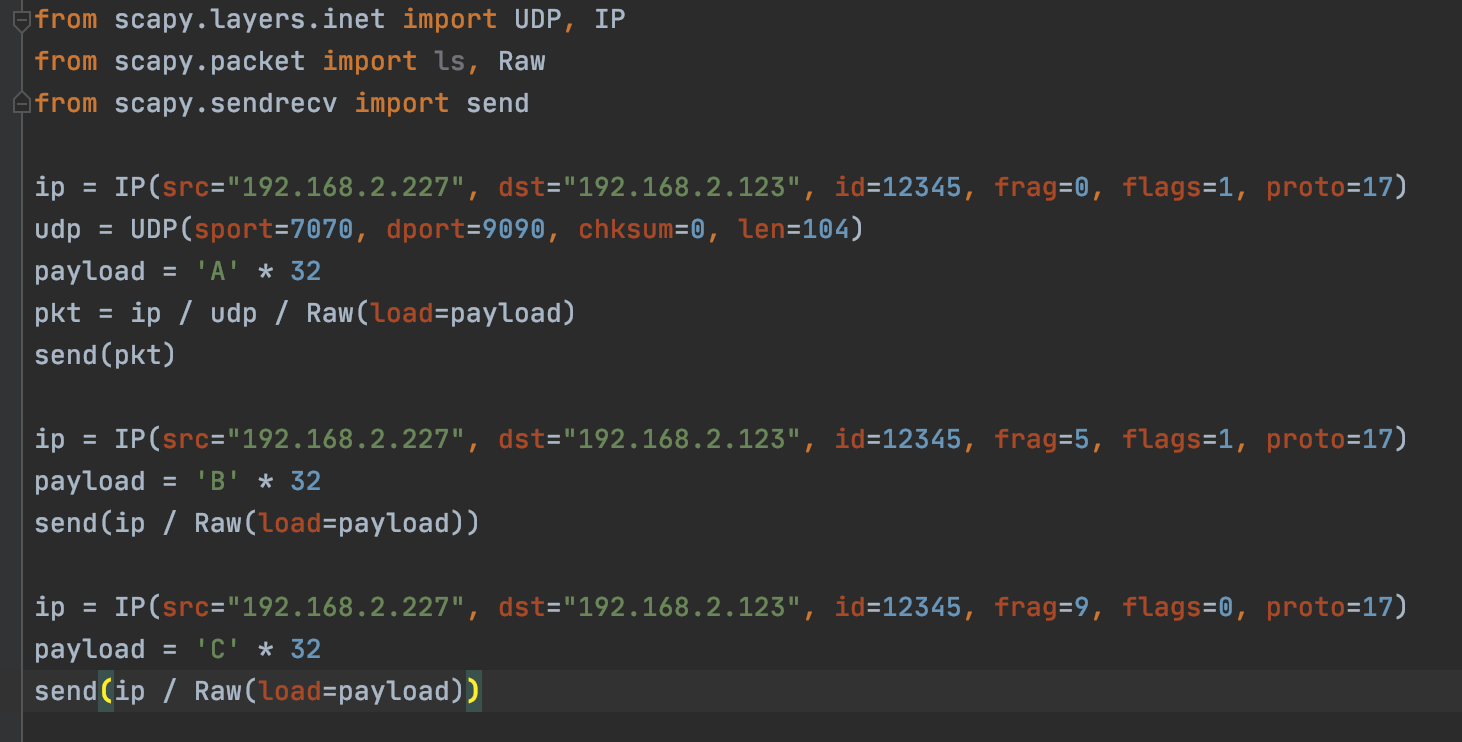
虚拟机前后arp表变化

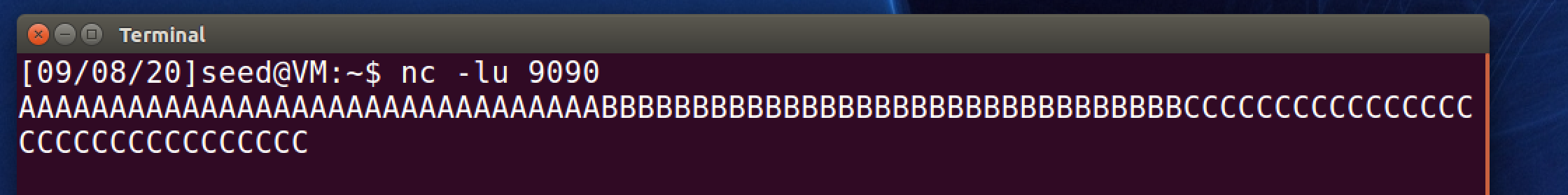


可以看出虚拟机B的mac地址已经被主机M的mac地址覆盖。

**Lab3**

**Task1.a**

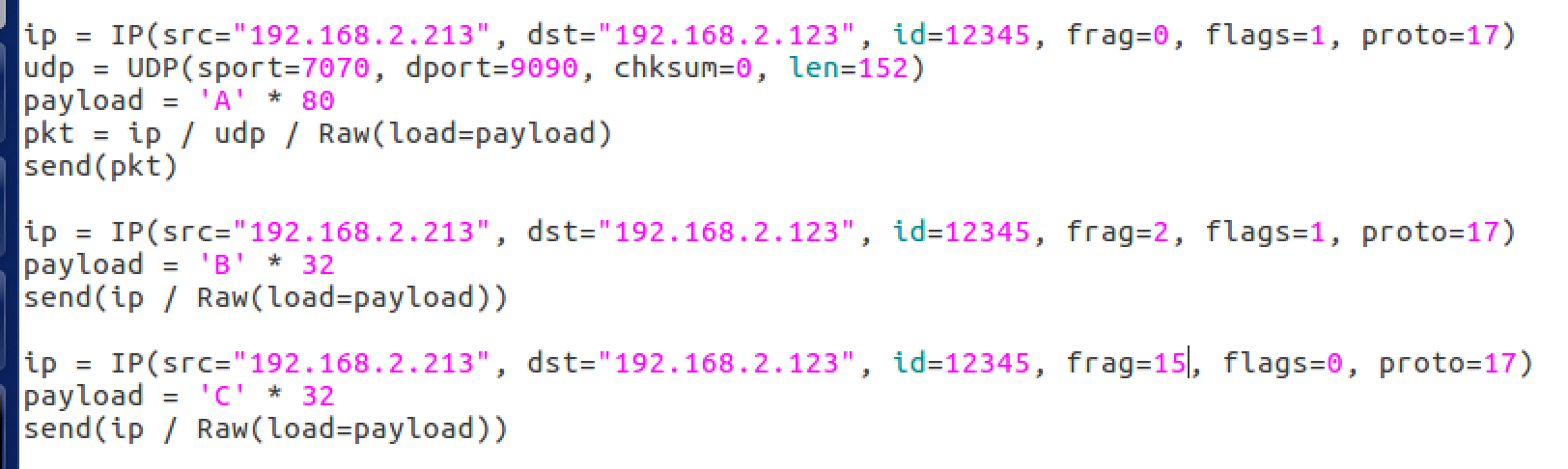




设置id为相同的任意数值,这里设置为12345，设置前两个分片的MF=1，最后一个分片的DF=0，设置三个分片的偏移量分别为0，(8+32/8=) = 5，(40+32)/8 = 9，设置udp的len为8+32\*3 = 104，将三个分片发送，发现另一台主机收到信息。

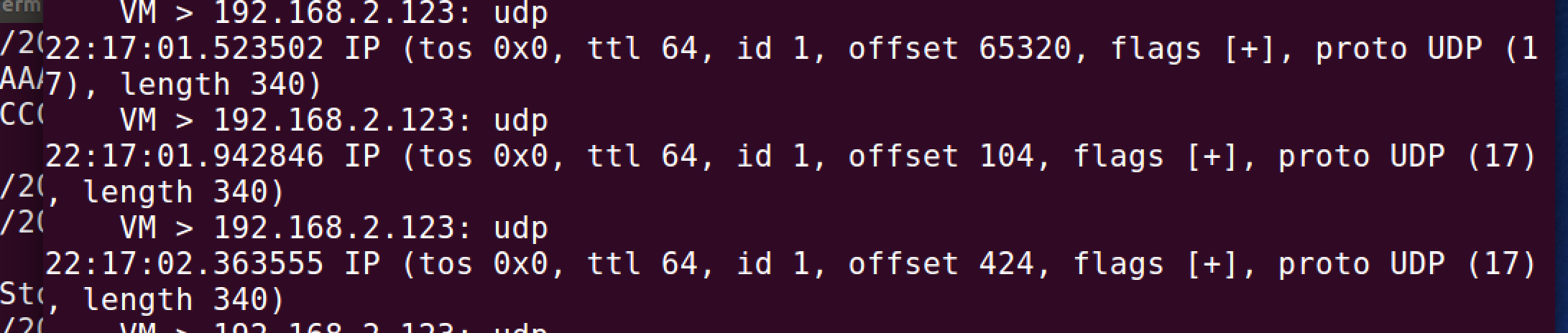
**Task1.b**

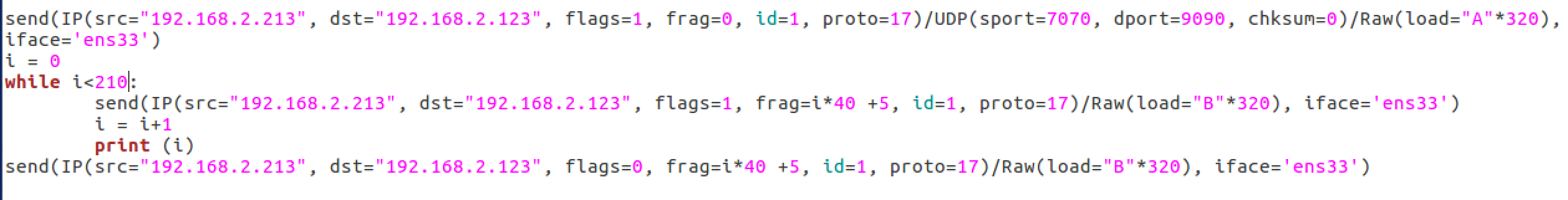
**确实没反应**



理论上应该接收方应该会用第二个分片的末尾偏移减去第一个分片的末尾偏移，得到一个负数（巨大的正整数），为他分配大量内存，导致宕机。但是我没能做出来实验效果。

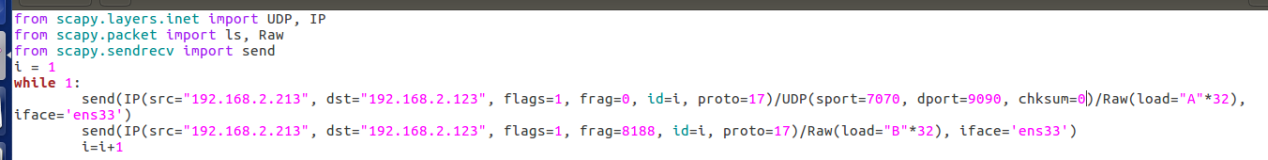
**Task1.c**

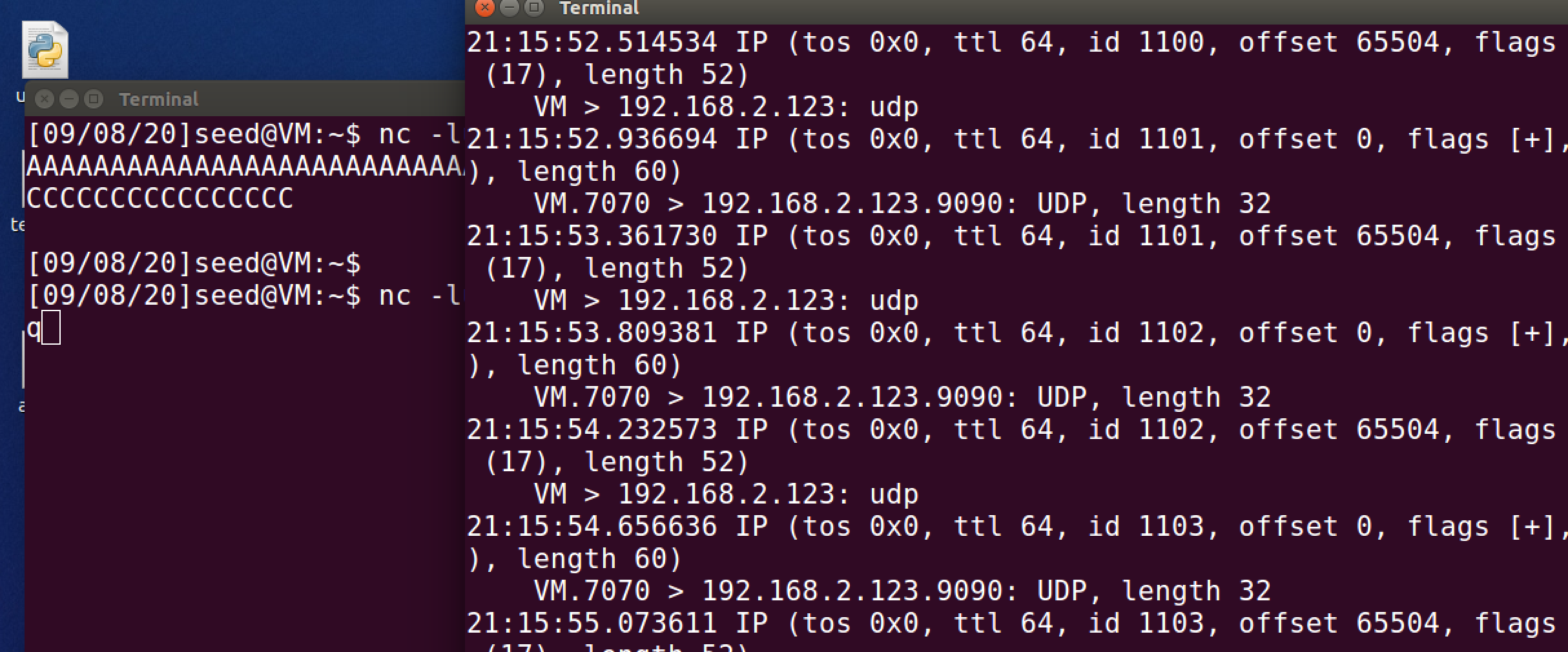




通过分片发送大于65320字节的报文，接收方在收到超过65320的报文后偏移量从0开始继续增加。

**Task1.d**





发送方不断发MF = 1的报文，试图占用接收方的buffer造成dos攻击，但是没有明显效果。