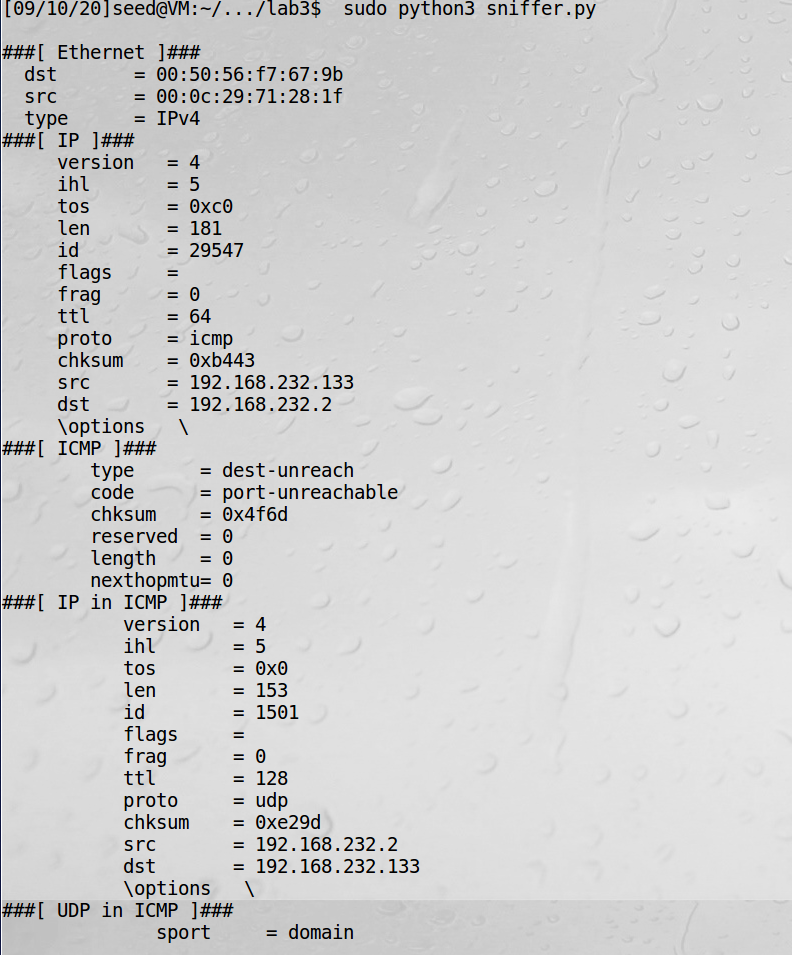
### Lab Task Set 1: Using Tools to Sniff and Spoof Packets

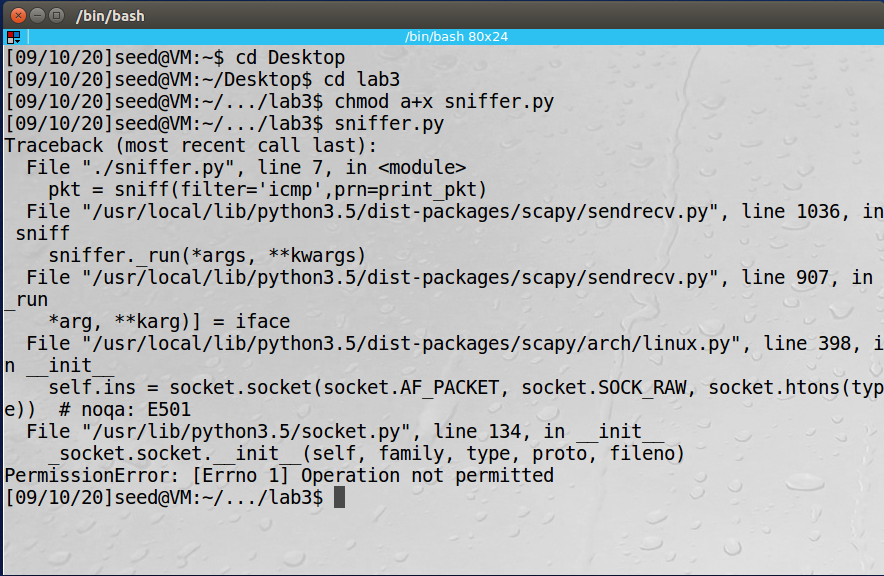
## Task 1.1: Sniffing Packets

#### Task 1.1A.

在root权限下：

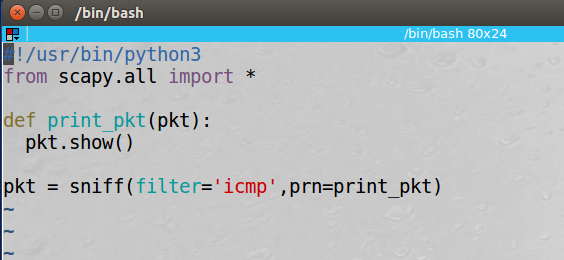


在普通用户权限下报错：



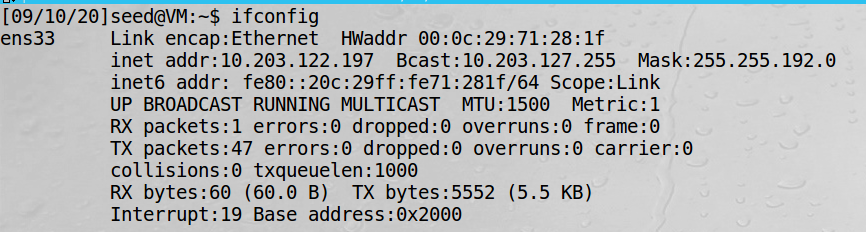
#### Task 1.1B

捕获ICMP报文：

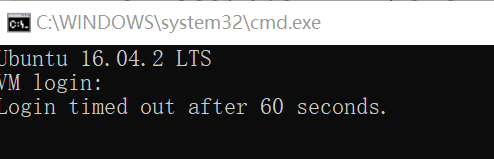


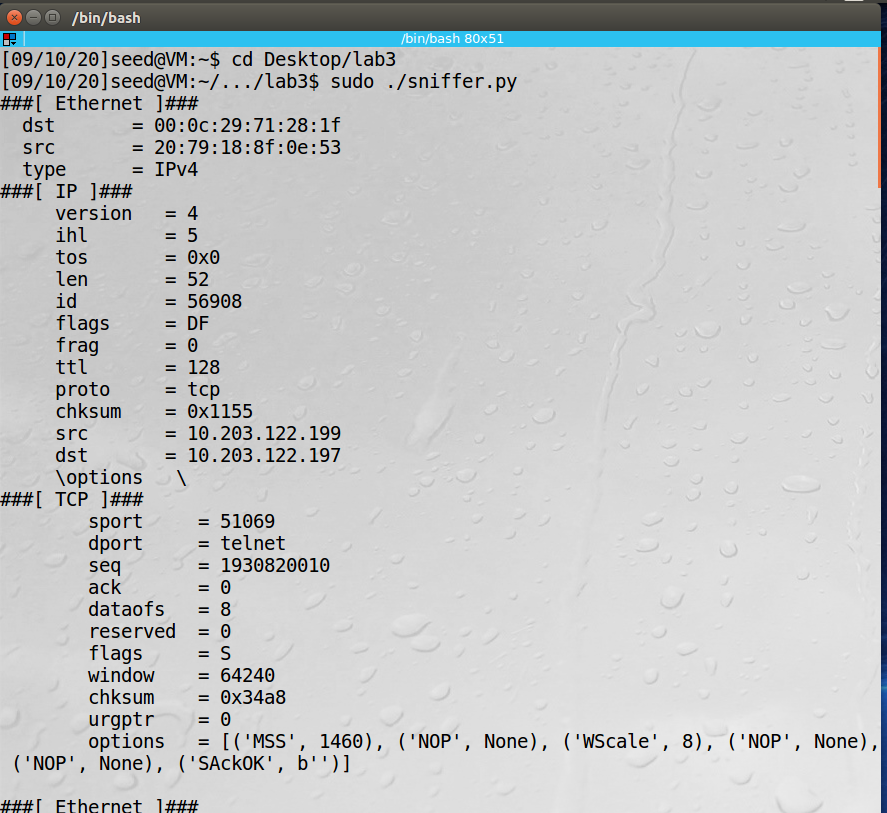
捕获结果如TASK1.1A所示

捕获特定IP发出的，目的端口为23的TCP包



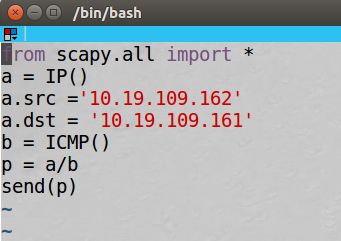
使用桥接模式，将ipv4、子网掩码、网关地址成功配置之后，使宿主机远程登录虚拟机。



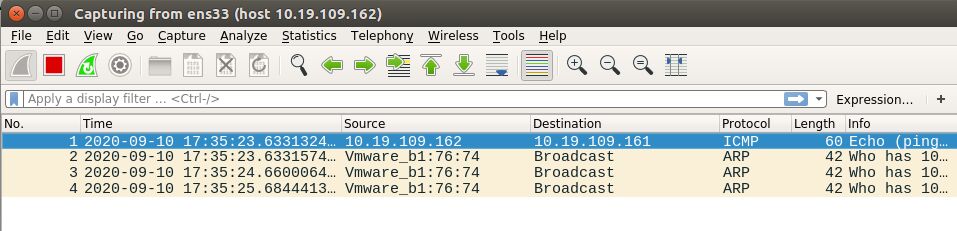


捕获成功

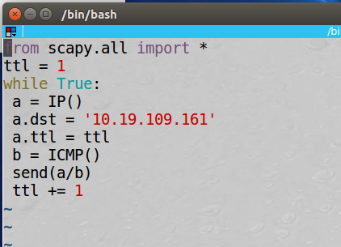
#### Task 1.2: Spoofing ICMP Packets

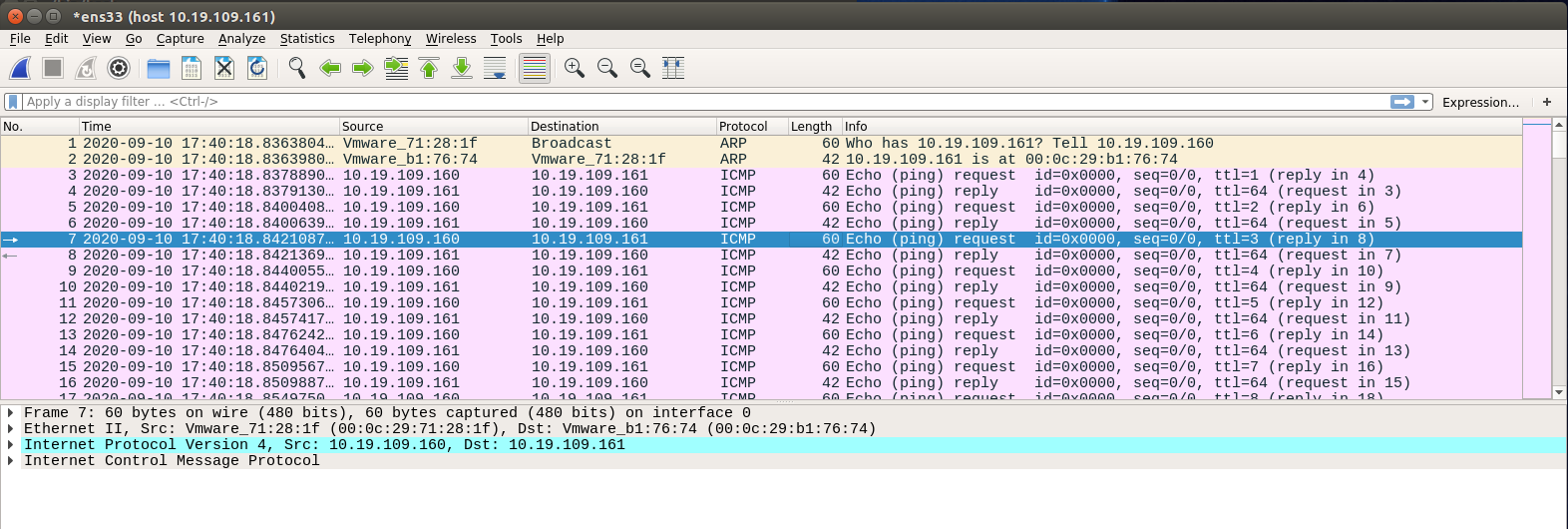


伪装成地址10.19.109.162，将报文发送给10.19.109.161，使用wireshark过滤，收到该报文，可见伪装成功。



#### Task 1.3: Traceroute

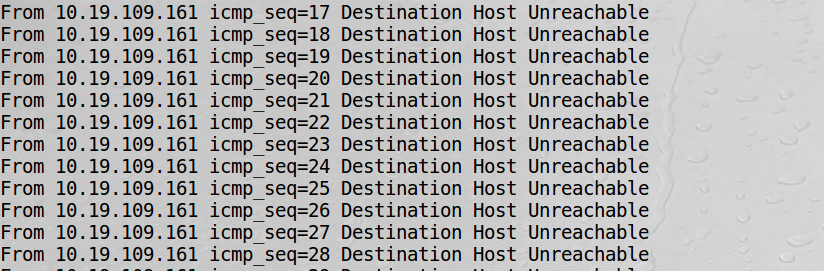


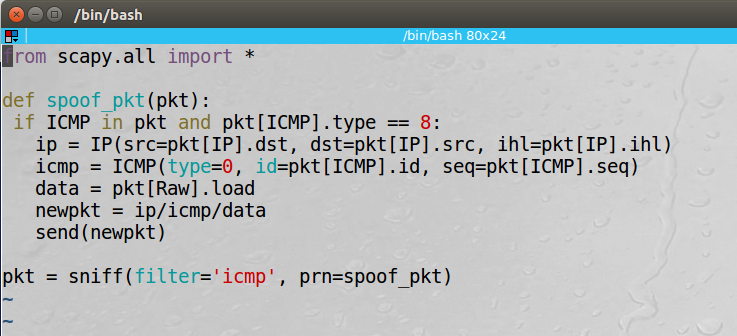


Ttl=1时即收到reply in 4

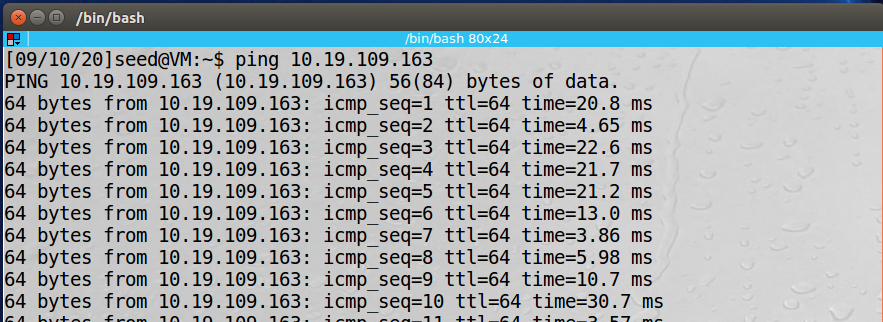
#### Task 1.4: Sniffing and-then Spoofing

虚拟机1（10.19.109.161）中ping 10.19.109.163无法ping通

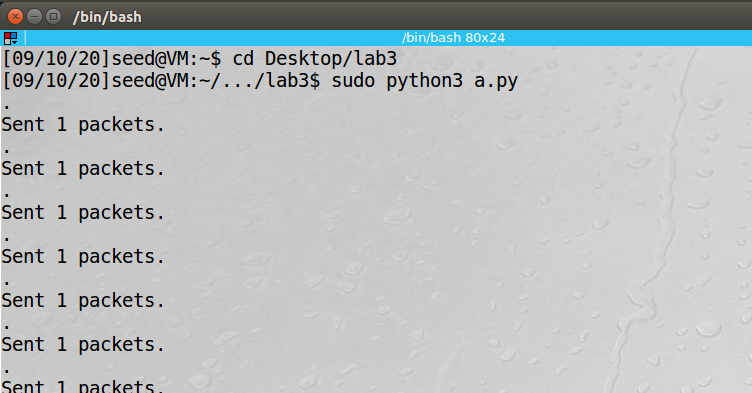




执行代码后成功ping通



另一台虚拟机中显示发送了报文

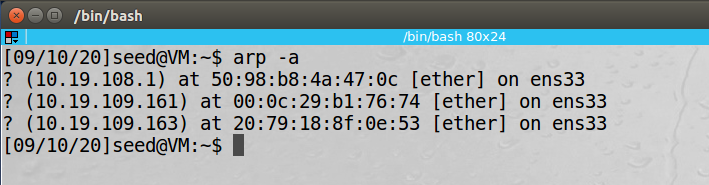


可见代码执行成功。

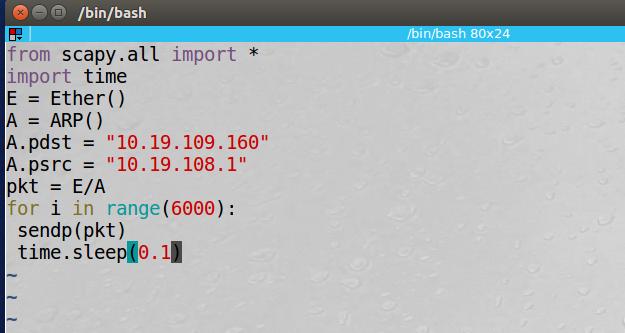
### ARP Cache Poisoning Attack Lab

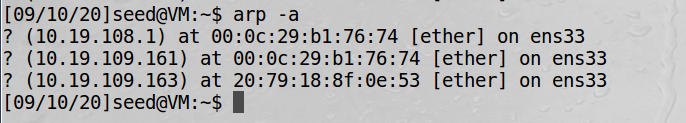
## Task 1: ARP Cache Poisoning

#### Task 1A (using ARP request)



使用arp -a命令查看，确定虚拟机1的地址为10.19.109.160，虚拟机2的地址为10.19.109.161。要污染的地址为10.19.108.1，要将其污染为虚拟机2的mac地址。

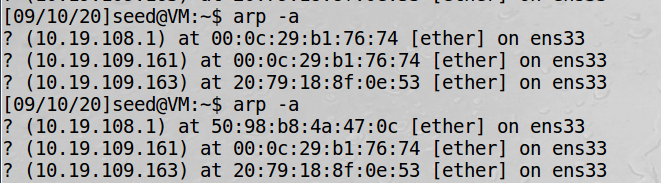




污染成功

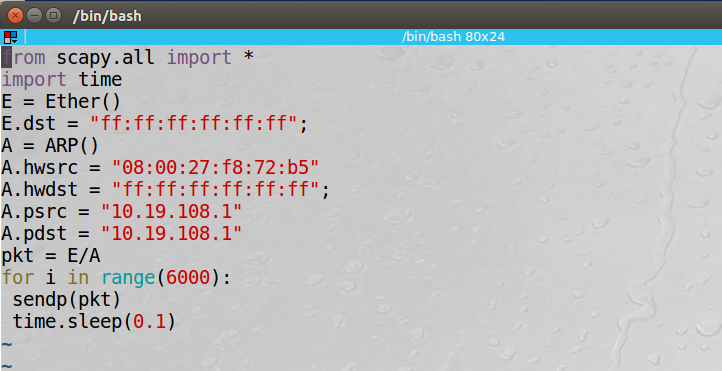
#### • Task 1B (using ARP reply)

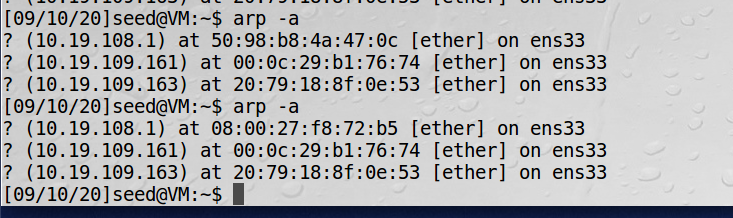




污染成功

#### Task 1C (using ARP gratuitous message)



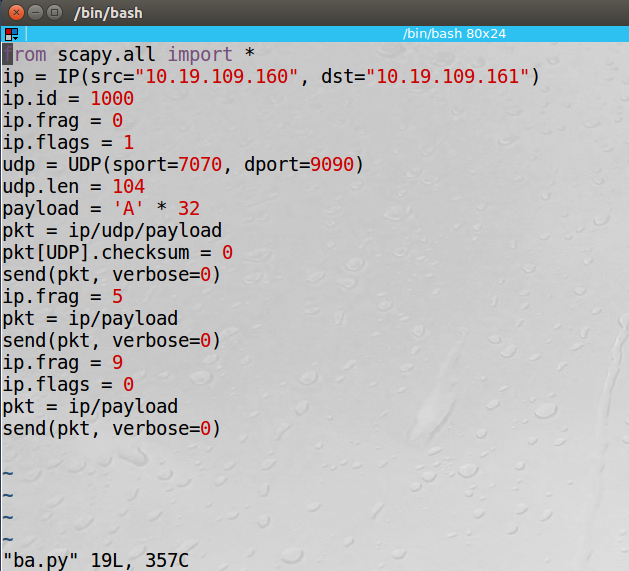


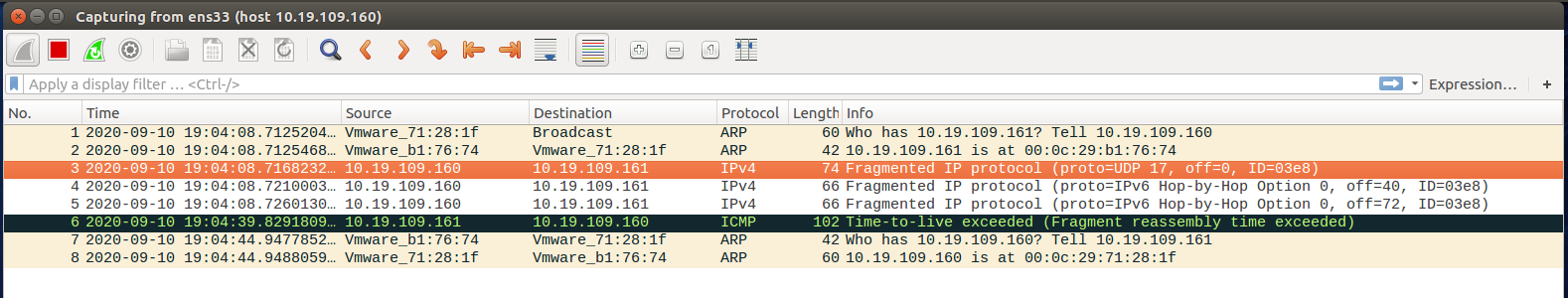
污染成功

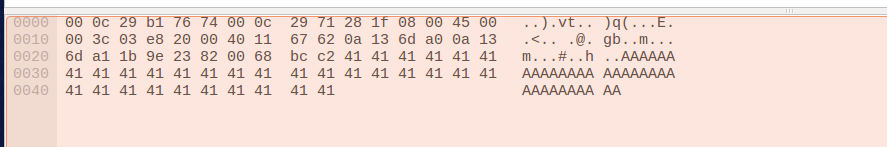
### IP/ICMP Attacks Lab

## Tasks 1: IP Fragmentation

#### Task 1.a: Conducting IP Fragmentation

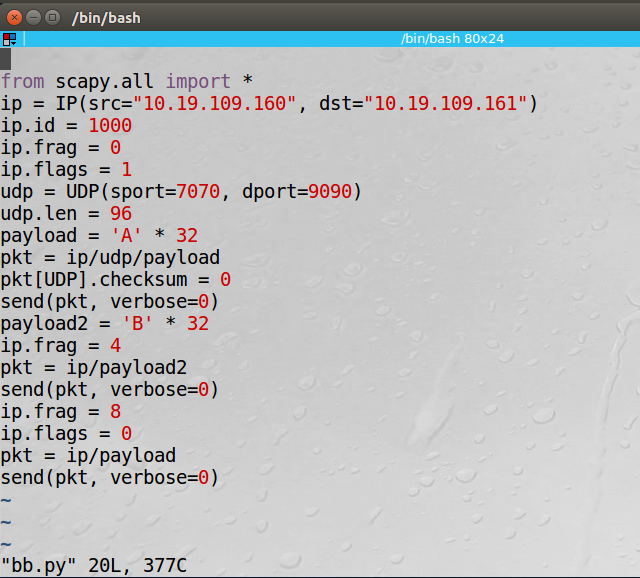


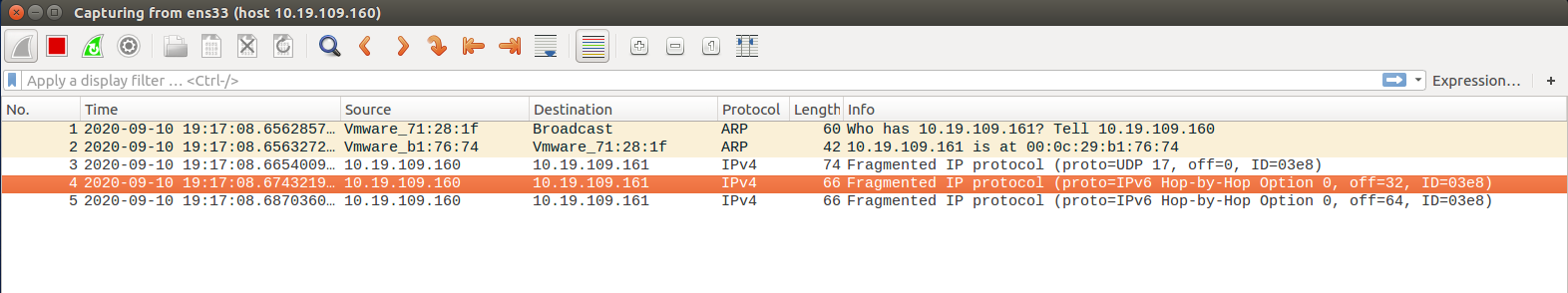


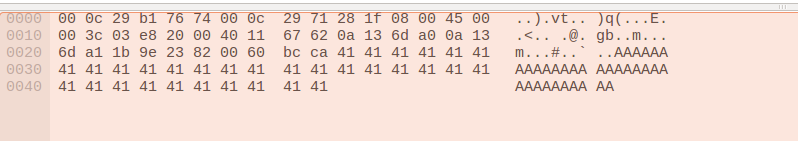


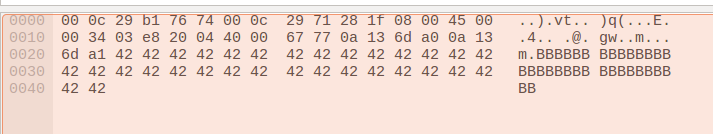
收到3次，每次带有32个A，共有96个A

#### 2.2 Task 1.b: IP Fragments with Overlapping Content











收到24个A， 32个B，32个A，后面的片会覆盖住前面的片

#### 2.3 Task 1.c: Sending a Super-Large Packet

UDP服务器崩溃

#### 2.4 Task 1.d: Sending Incomplete IP Packet

