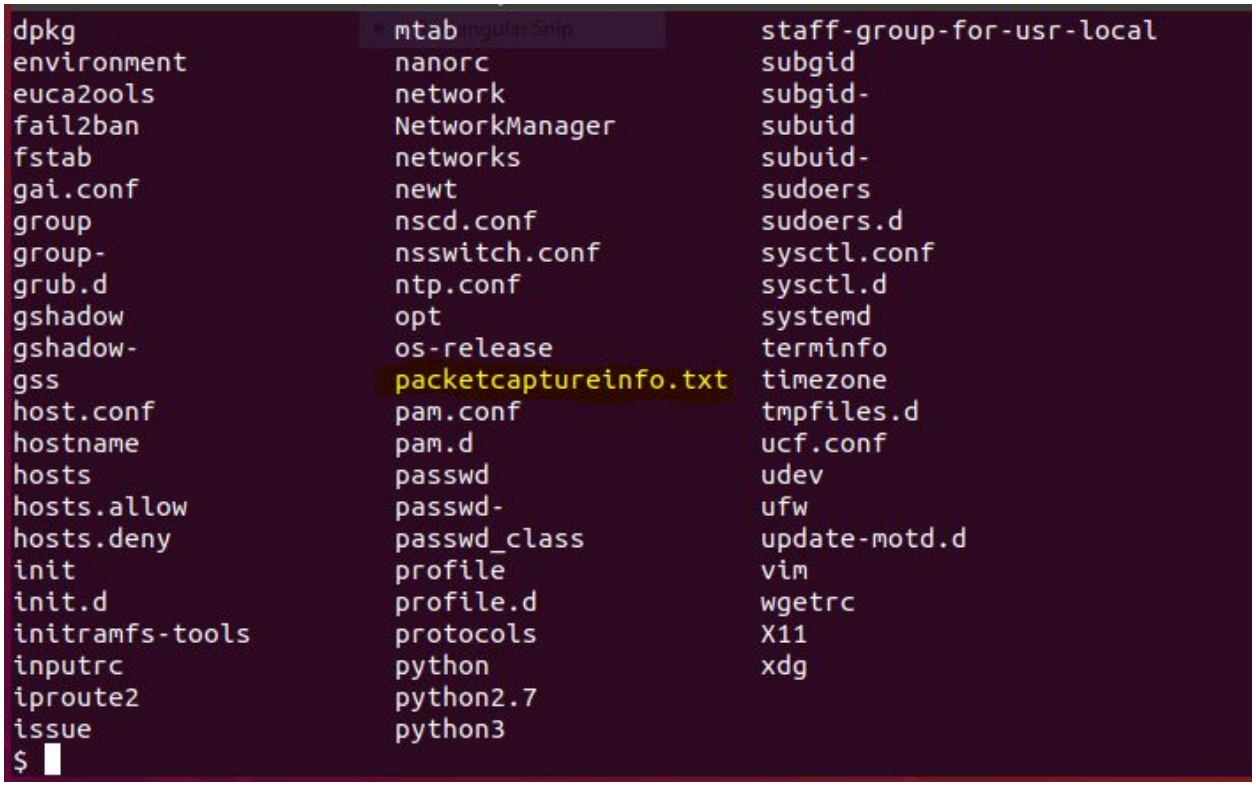
Phase 4: "ShARP Dressed Man"

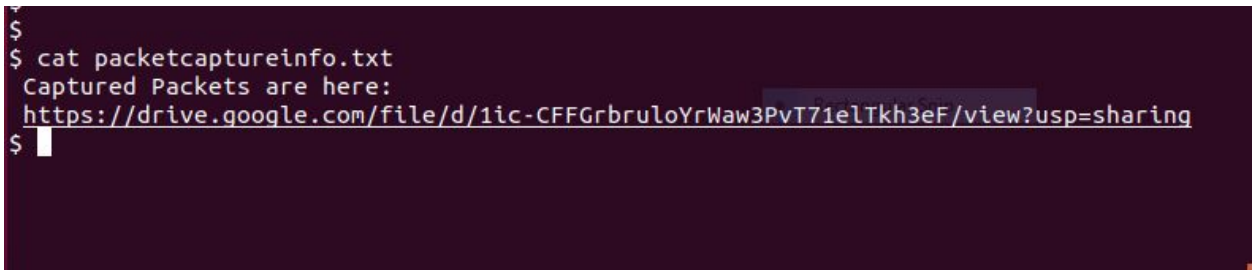
Solution:

View the file the hacker left to find where to recover the packet captures.

$ cd /etc
$ ls

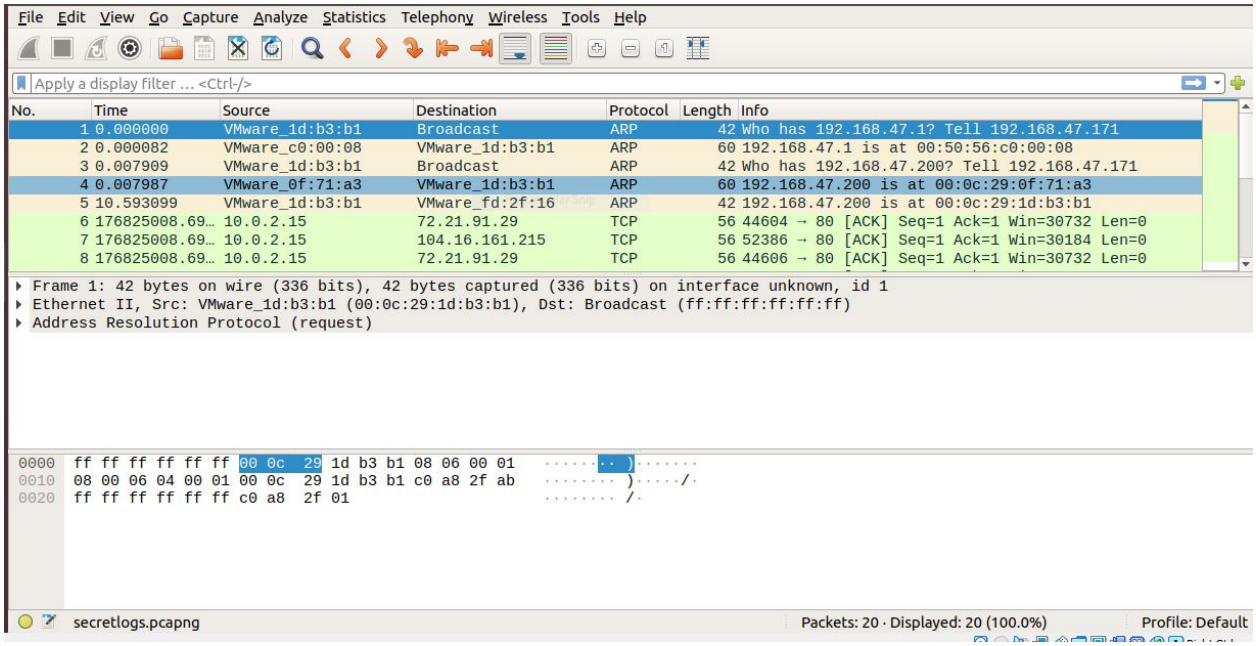


Open the file:



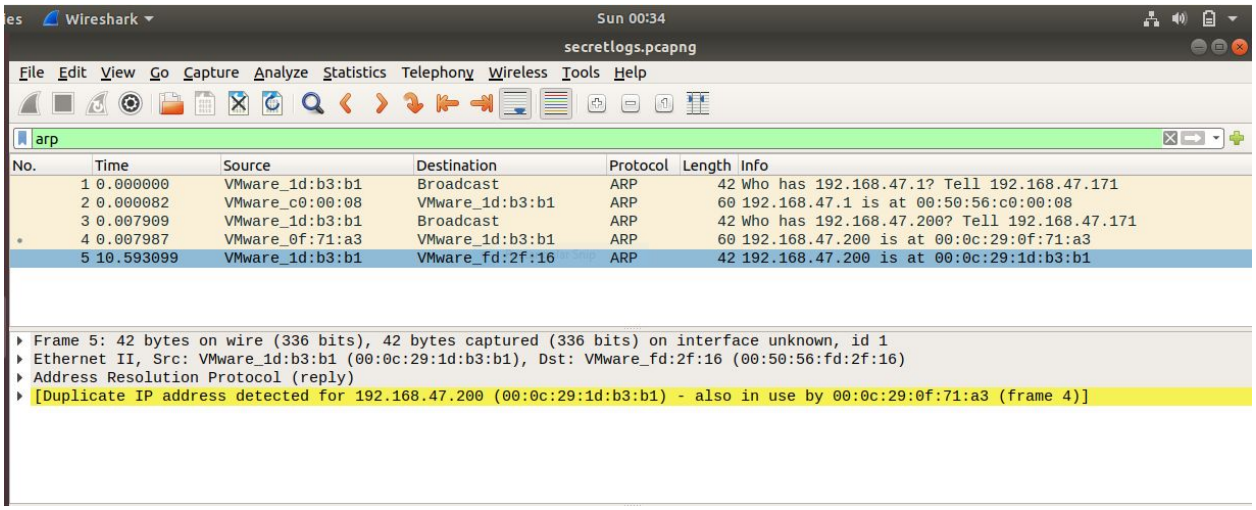
Browse the URL:

Open the secrelogs.pcapng with Wireshark:



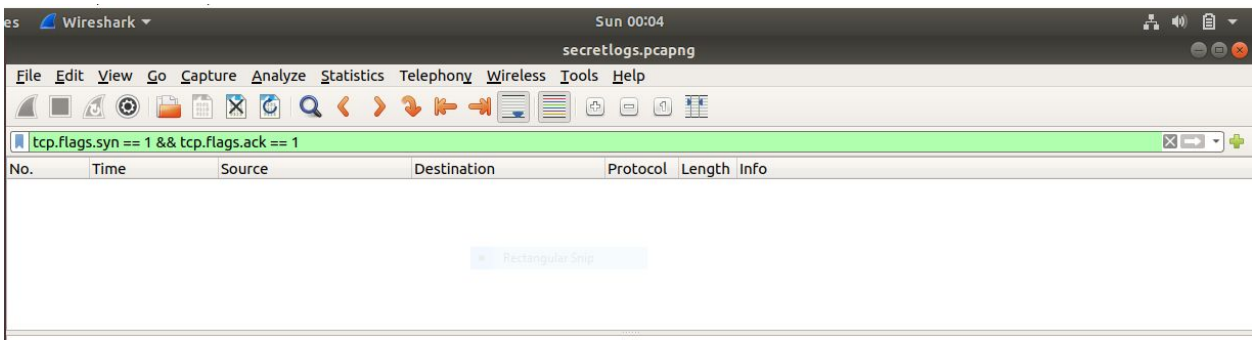
Checking for arp spoofing:

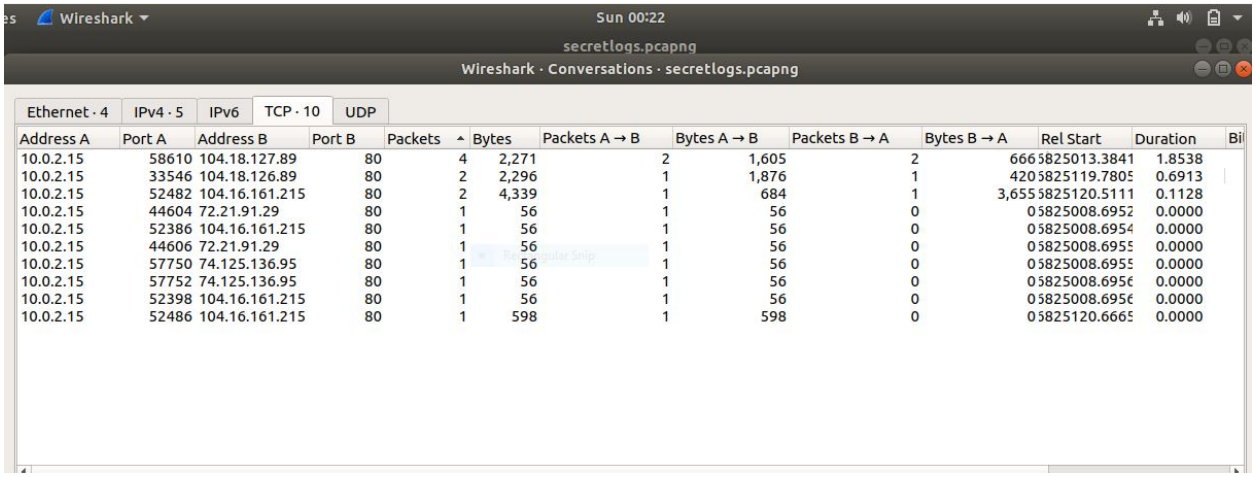
The hacker used spoof ARP message to the LAN, directing all traffic intended for host 192.168.47.200 (mac address - 00:0c:29:0f:71:a3) to it mac address - 00:0c:29:1d:b3:b1.
The OSI layer of the findings is DataLink layer (layer 2).



Checking for open ports.

Port 80 (HTTP)





The SYN scan shows that port 80 has 4 packets which indicated that the hacker closed it. We recommend it to be open immediately, since users need to communicate with the server.
The OSI layer these findings fall into is Transport layer (layer 4).