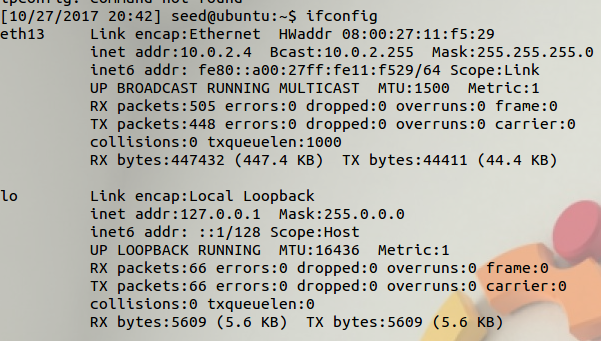
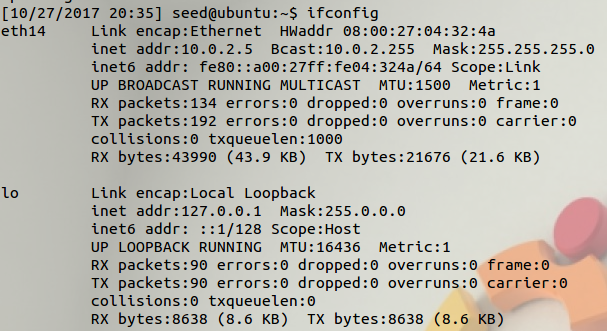
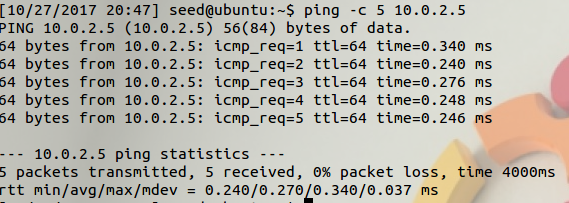
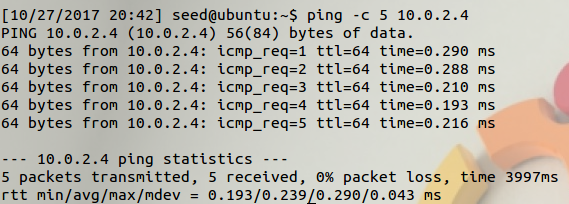
Alexander Kimea

Screenshots:

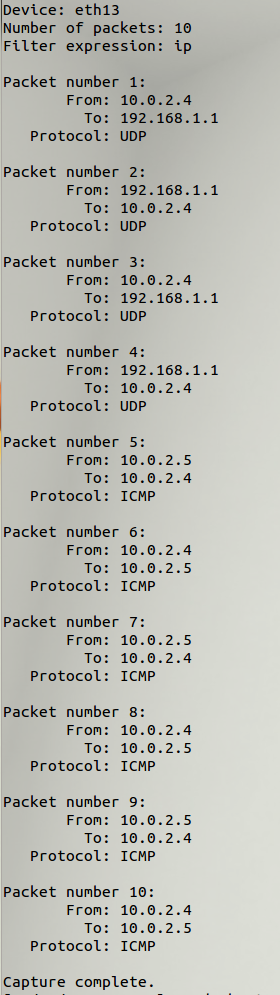
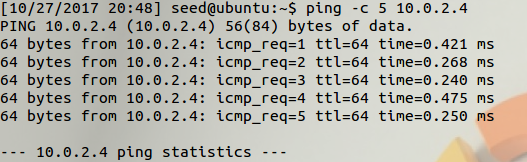
3.1

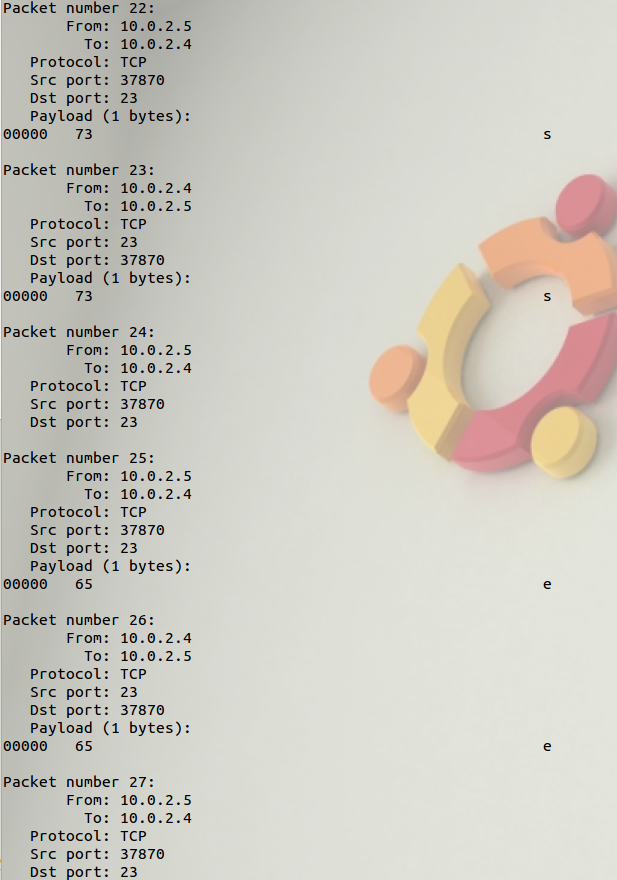
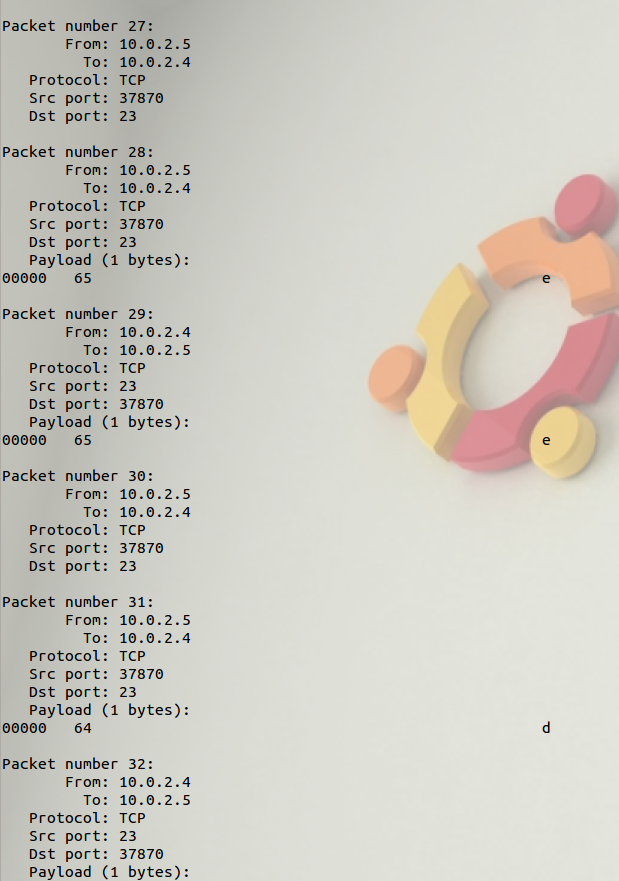
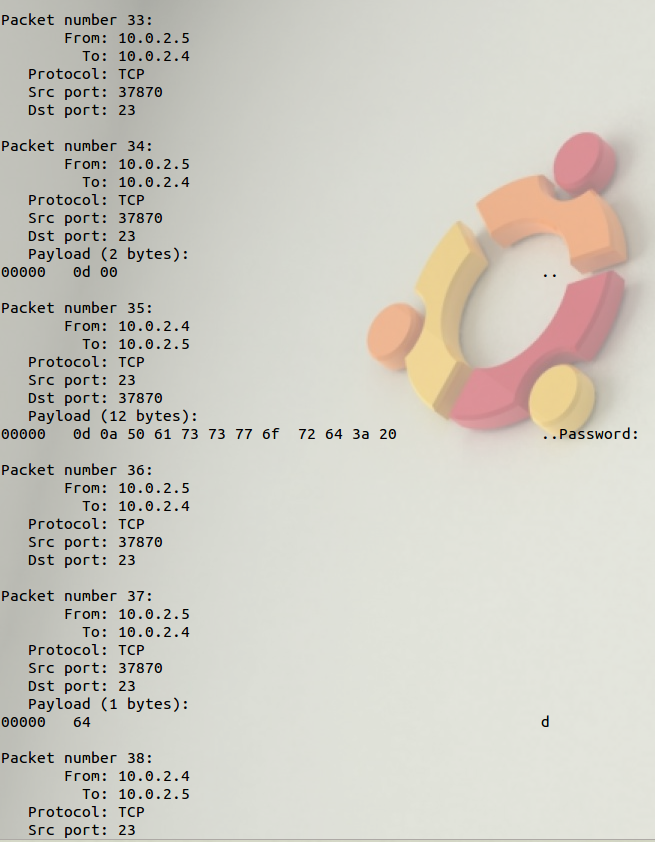
 

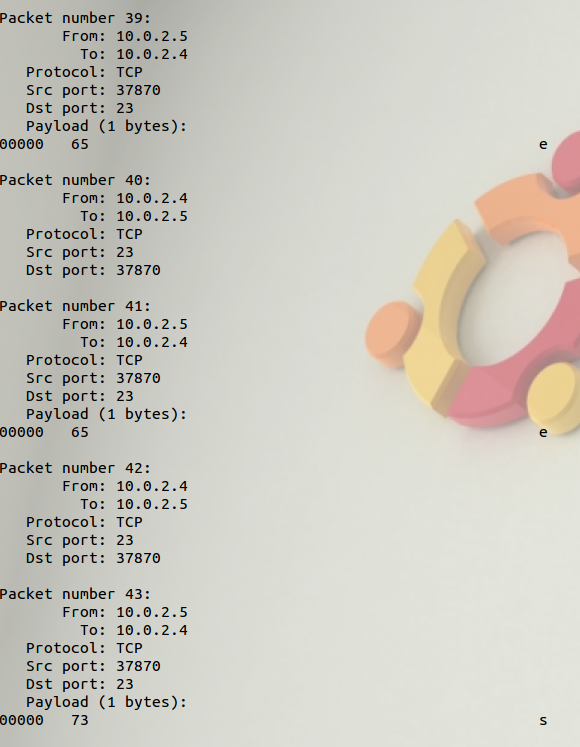
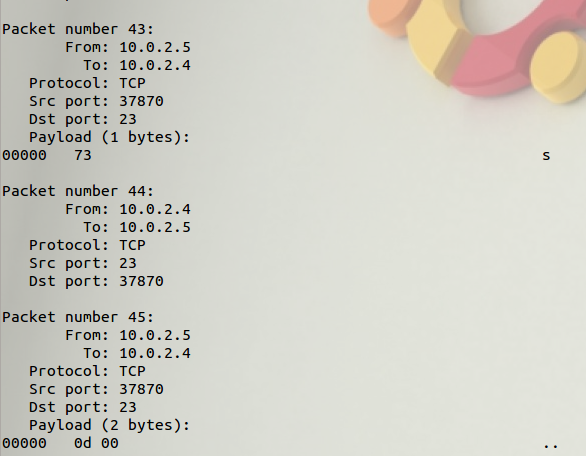
3.2

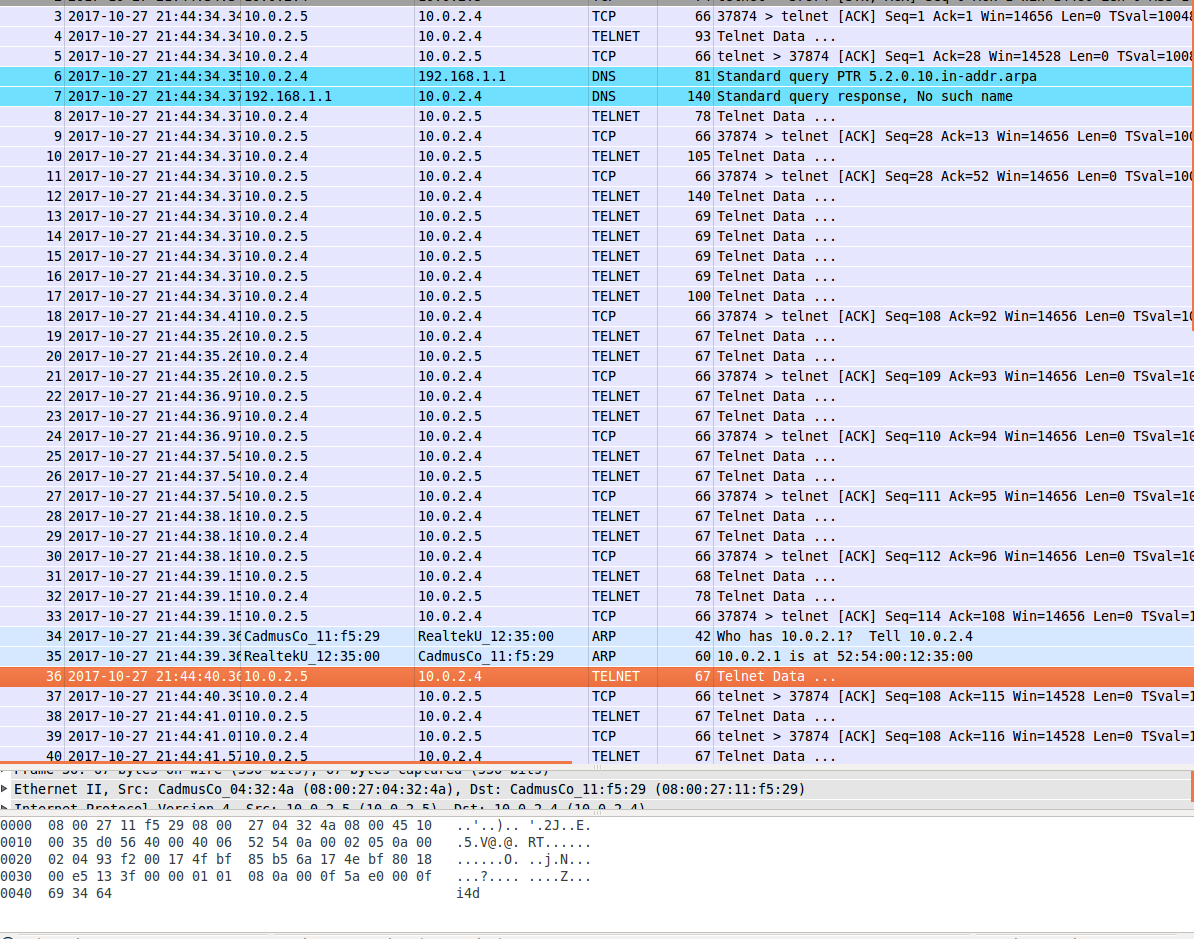
Determine an interface to packet sniff such as an ethernet interface. Initialize the library and tell what device pcap is sniffing on. Determine what kind of traffic to sniff such as TCP/IP packets. Enter pcap primary execution loop which pcap waits until it has received the user given number of packets.

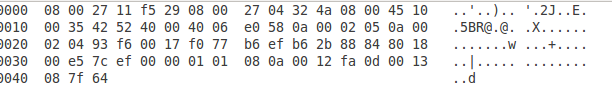
3.3

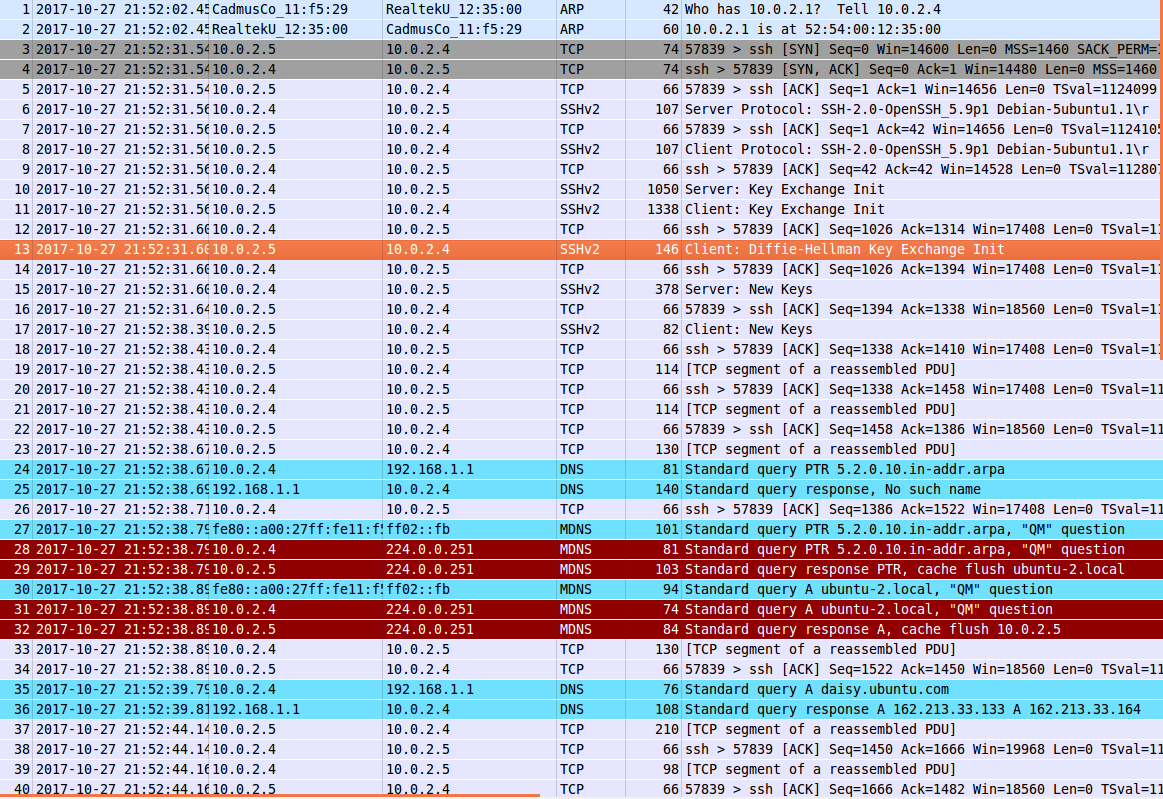


the below picture shows the first ‘d’ of ‘dees’ for the password at the bottom

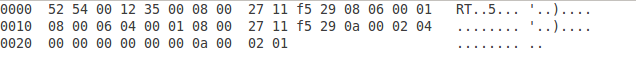


Once you recognize how it spits out the input then you can see the password. It seemed easy I suppose to sniff out what the other user was typing so I would assume that telnet is insecure and the packets are unencrypted or its encryption method is not very good. Reading the topic of the next problem, I would assume telnet is not secure because I know SSH uses encryption.

3.4



one of the packets



It’s jumbled mess. I don’t think I can find the password