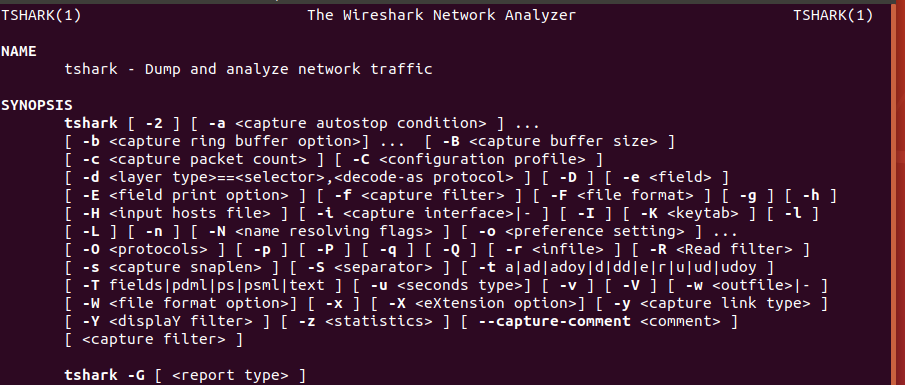
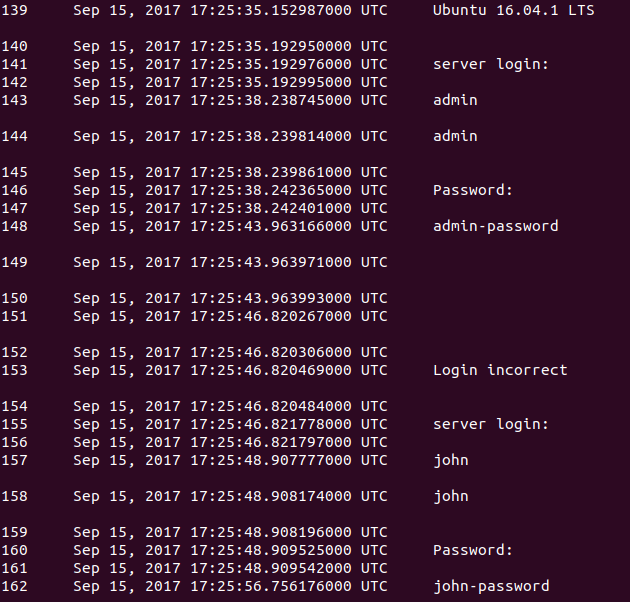
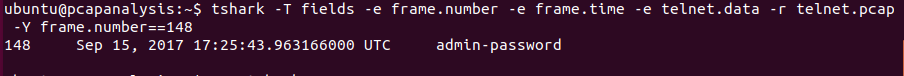
**PCAP ANALYSIS LAB**



Ran ‘man tshark’ to open the manual on how to use tshark.



Ran specified command ‘tshark -T fields -e frame.number -e frame.time -e telnet.data -r telnet.pcap’ to display specified fields.

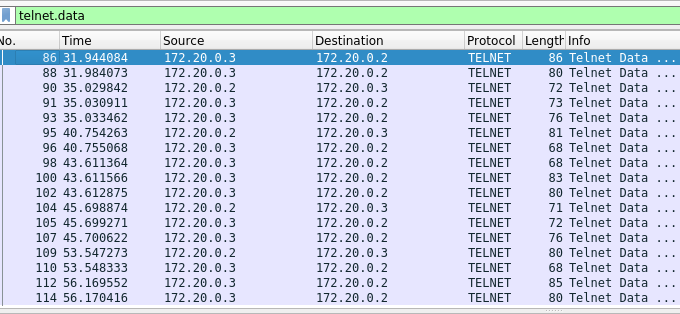


By adding filter to the end of specified command, we’ve isolated frame 148. This packet contains an invalid ‘admin’ password.

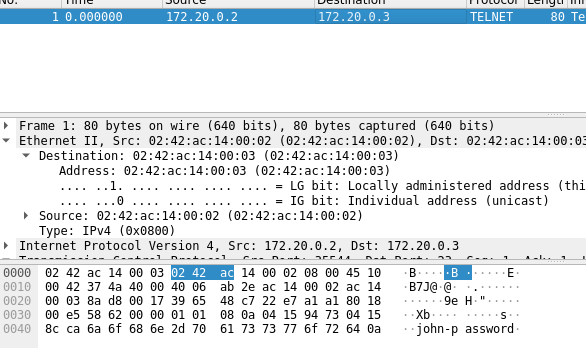
**Wireshark Introduction**



Ran ‘file telnet.pcap’ to view details regarding this file.



Opened telnet.data file on wireshark and searched for data within this file.



Isolated the packet containing John’s incorrect password. Saved the single packet to different file.



By selecting one of the telnet.data packets, I followed the TCP stream and was able to view the entire interaction between the systems.