Step 2 (UDP)

a) Explain both the command you used in detail? What did you actually do?

NC - Netcat is a command-line utility that reads and writes data across network connections. We use nc -k -l to continue listening after disconnection and use the flag -u to specify UDP instead of TCP. We then used nc -u host port to execute a port scan. Then we passed the string.

b) How many frames were needed to capture those 2 lines?

2

c) How many packets were needed to capture those 2 lines?

2

d) How many packets were needed to capture the whole "process" (starting the communication, ending the communication)?

2

e) How many total bytes went over the wire? How much overhead was there (percent of bytes not in the above 2 lines)?

Total Bytes over wire:
78

Overhead: 0%

f) What is the difference in relative overhead between UDP and TCP and why? Specifically, what kind of information was exchanged in TCP that was not exchanged in UDP? Show the relative parts of the packet traces.

UDP has a lot less overhead than TCP. The reason is it is not connection oriented and does not provide sequencing, flow control and retransmission mechanisms where as TCP did exchange that.

TCP

```
63486 → 3333 [SYN] Seq=0 Win=65535 Len=0 MSS=16344 WS=64 TSva
3333 → 63486 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=16344
63486 → 3333 [ACK] Seq=1 Ack=1 Win=408256 Len=0 TSval=3356413
[TCP Window Update] 3333 → 63486 [ACK] Seq=1 Ack=1 Win=408256
63486 → 3333 [PSH, ACK] Seq=1 Ack=1 Win=408256 Len=7 TSval=335
```

UDP