

```
sudo tshark -i any -a duration:5 -T fields -e ip.src -e ip.dst -e ip.proto -e frame.len -e udp > /Users/farhadsafi/Desktop/WireSharkPackets/example1.txt
```

Run Shell File
Through the terminal

The Shell file runs t-shark
and captures data
packets for 5 seconds

Navigate to the
WireSharkPackets
directory
cd WireSharkPackets

#It prints a header
echo "Src IP Dst
IP Proto Len
UDP port"

The time and the fields are
editable. You can capture
whichever ones you want

sudo: Execute the command with superuser privileges.
tshark: Command-line packet capture tool.
-i any: Capture packets on any available interface.
-a duration:5: Capture packets for a duration of 5 seconds.
-T fields: Output the captured data in fields format.
-e ip.src: Display source IP address.
-e ip.dst: Display destination IP address.
-e ip.proto: Display IP protocol.
-e frame.len: Display frame length.
-e udp: Display UDP-related information.
> /Users/farhadsafi/Desktop/WireSharkPackets/example1.txt:
Redirect the output to the specified text file.