WireShark WorkSheet

|  |  |
| --- | --- |
| Wireshark location  cd C:\Program Files\Wireshark |  |
| pcap file location | C:\Users\savid\Desktop\malware\_analysis\ homies2.pcap |
| **tshark read**  basic read  tshark -r <filename.pcap>  tshark -r <filename.pcap>  **tshark -T fields -e frame.protocols -nr /path/to/file**  tshark -r <filename.pcap> -T fields -e frame.number -e frame.time -e eth.src -e eth.dst -e ip.src -e ip.dst -e ip.proto -E header=y -E separator=, -E quote=d -E occurrence=f > <filename.csv> | tshark -r C:\Users\savid\Desktop\malware\_analysis\homies2.pcap  Protocols (lists all)  tshark -r C:\Users\savid\Desktop\malware\_analysis\homies2.pcap **-T fields -e frame.protocols** |