How to do a packet capture (tcpdump)

Sample Command on how to use TCP Dump

Linux: tcpdump -w {filename}.pcap Â -c 200 {limit number of packets}

tcpdump -s 2000 -w dump.pcap

Then you can email the file to any one using command

mail -s "dump.pcap" email@gmail.com < dump.pcap

You can then open with file w/ Wireshark

Â

http://www.thegeekstuff.com/2010/08/tcpdump-command-examples/

Online URL: https://kb.naturalnetworks.com/article.php?id=27