La commande tcpdump est un puissant outil en ligne de commande pour l’analyse des paquets réseau . Tcpdump nous aide à résoudre les problèmes de réseau ainsi qu'à analyser le fonctionnement de certains outils de sécurité. Il permet à ses utilisateurs d'afficher les paquets TCP/IP et autres qui sont reçus et transmis sur le réseau .