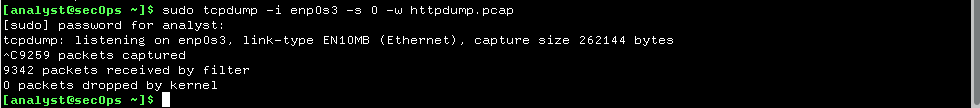
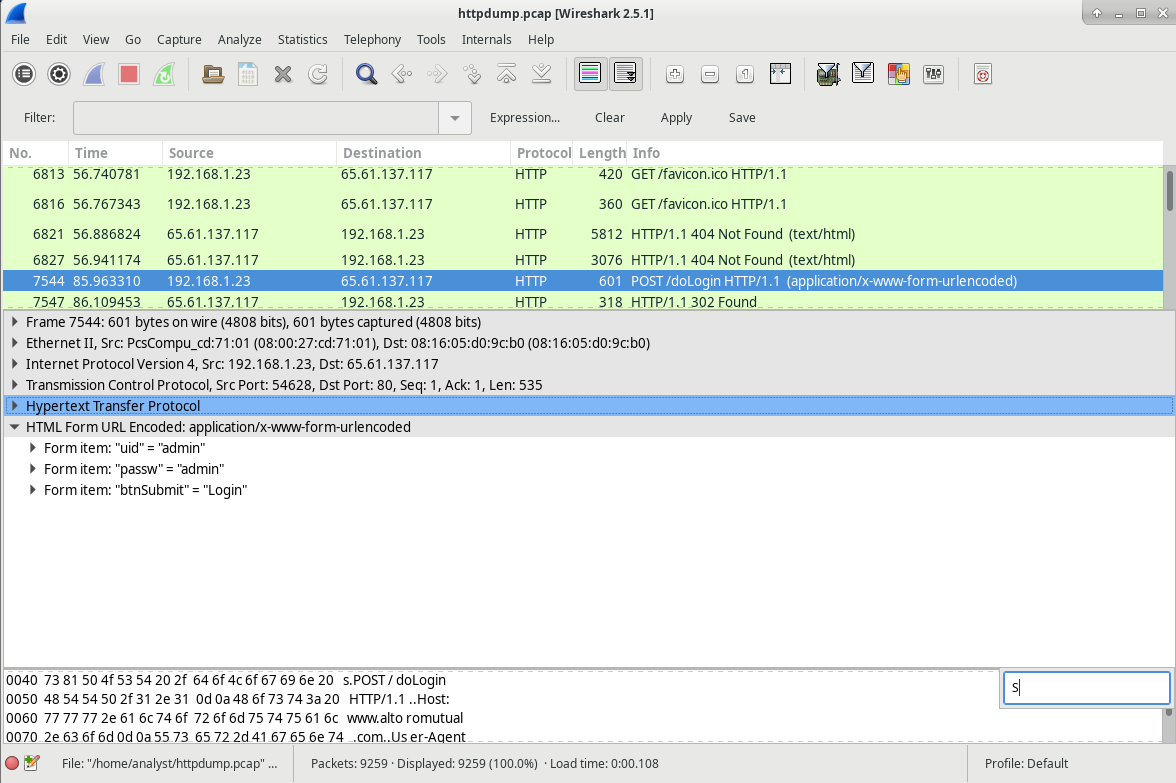
Usare Wireshark per esaminare traffico HTTP/HTTPS

Accediamo al Cyberops Workstation, accediamo al terminale e prepariamo un tcpdump del traffico internet:  
  


Il traffico HTTP ascoltato è della pagina login del sito web “altoromutual.com”, il quale non è cifrato.

Apriamo il file .pcap del traffico appena registrato su Wireshark e localizziamo la richiesta POST contenente le informazioni di login:



È stato poi provato con il traffico HTTPS, che usa un Secure Sockets Layer/Transport Layer Security per criptare le informazioni che prima potevano benissimo essere viste in chiaro.

