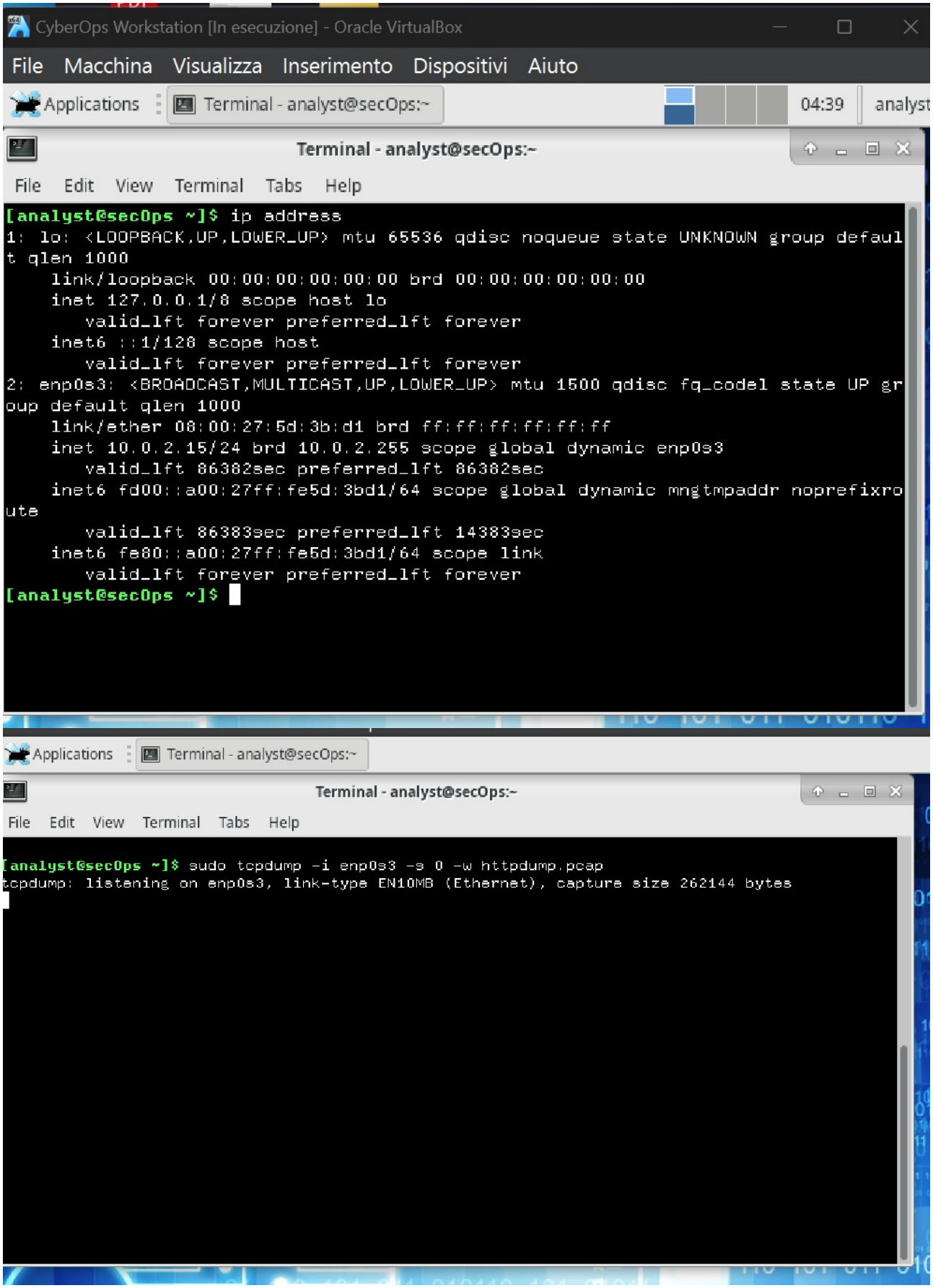
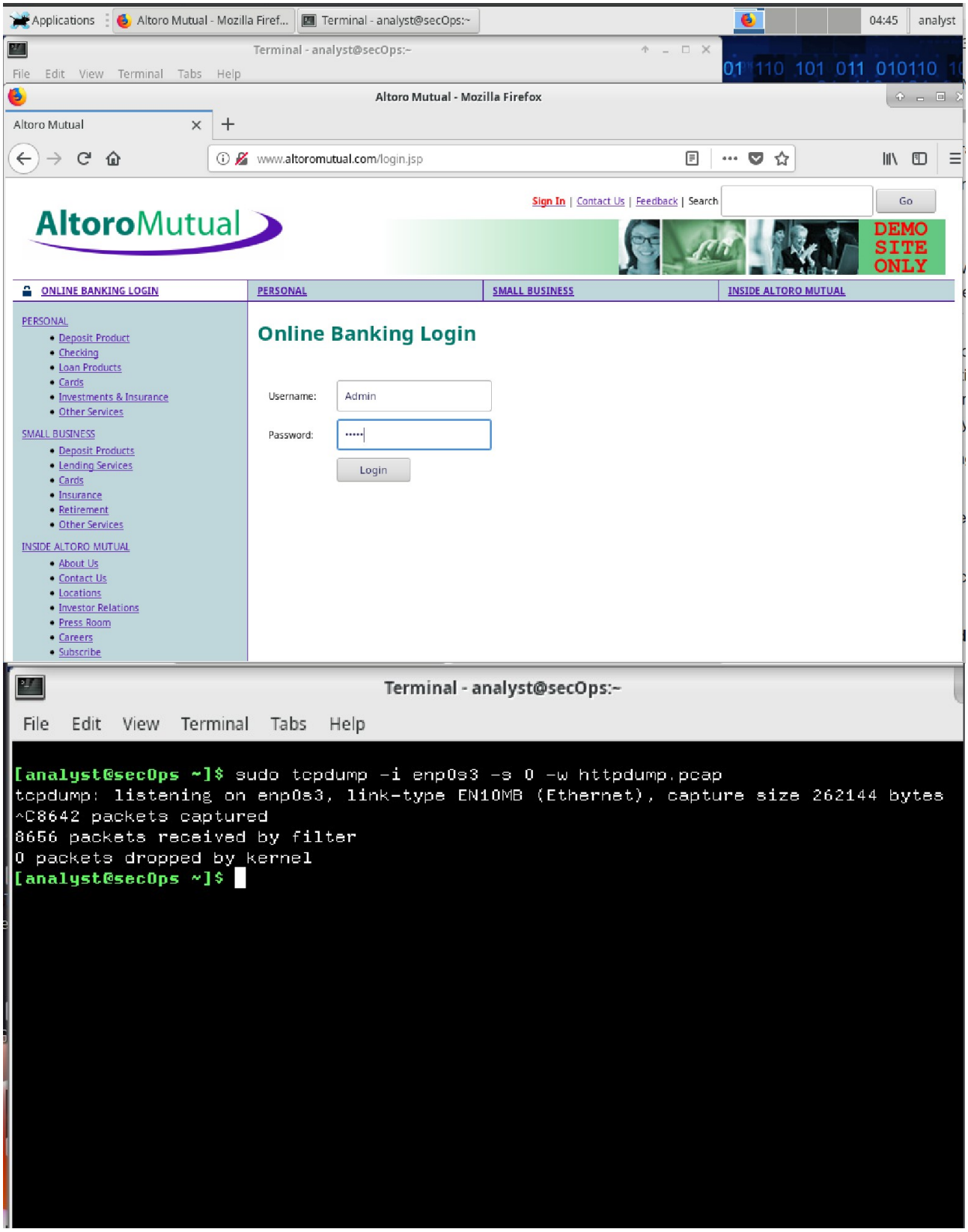
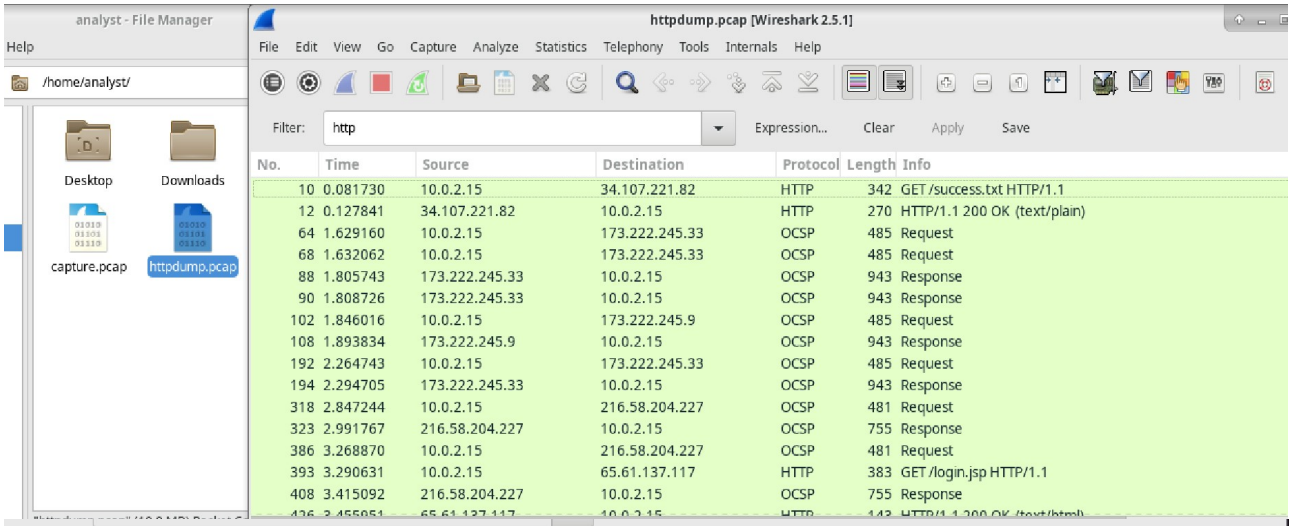
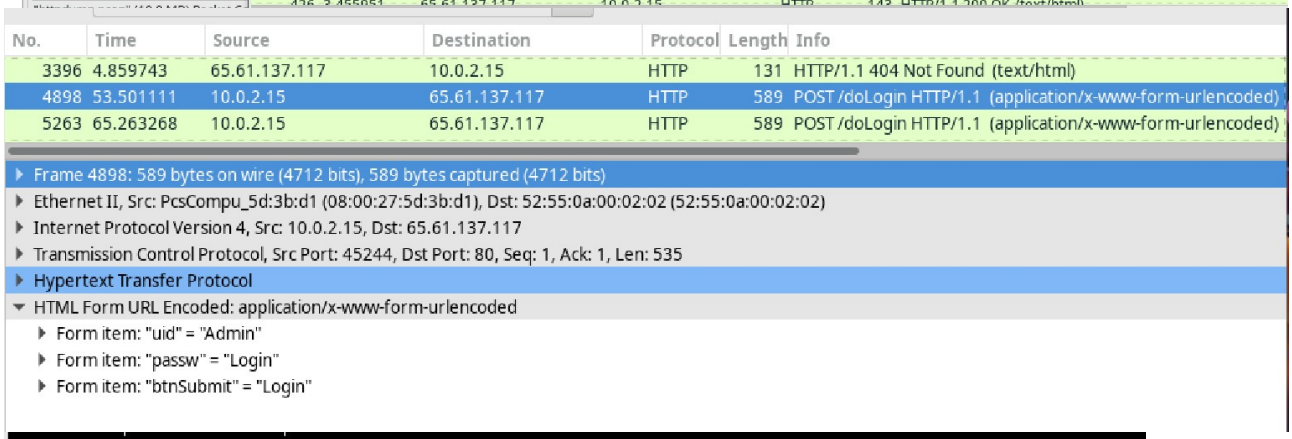
Utilizzo di Wireshark per Esaminare il Traffico HTTP e HTTPS

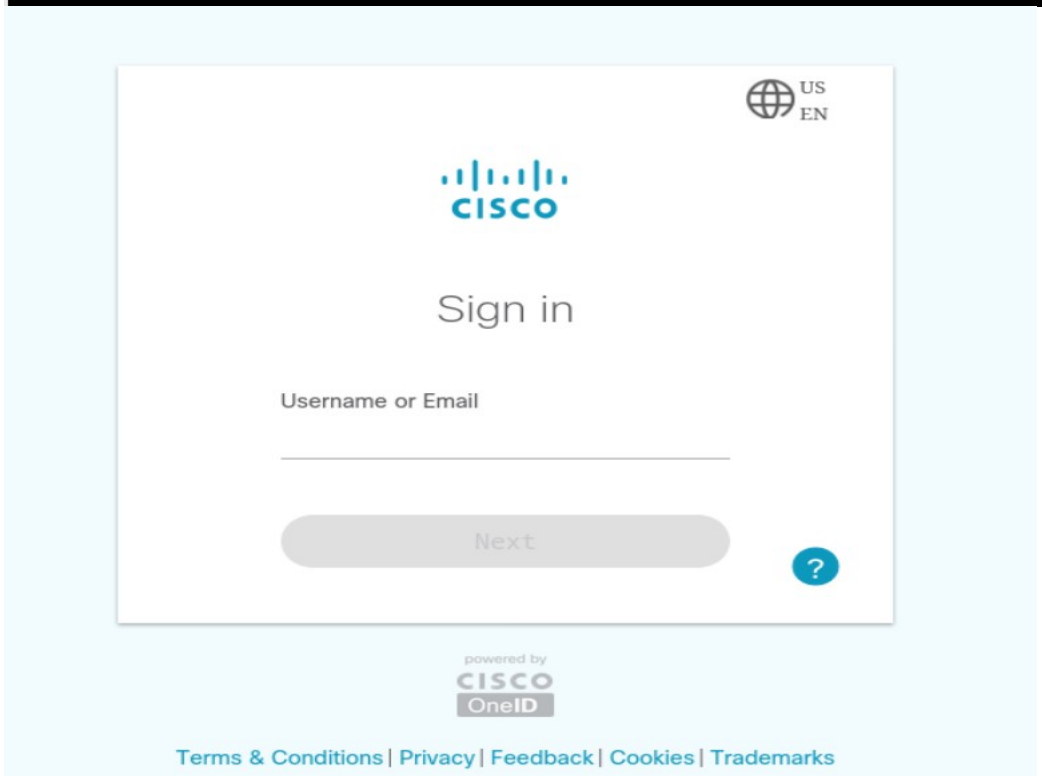


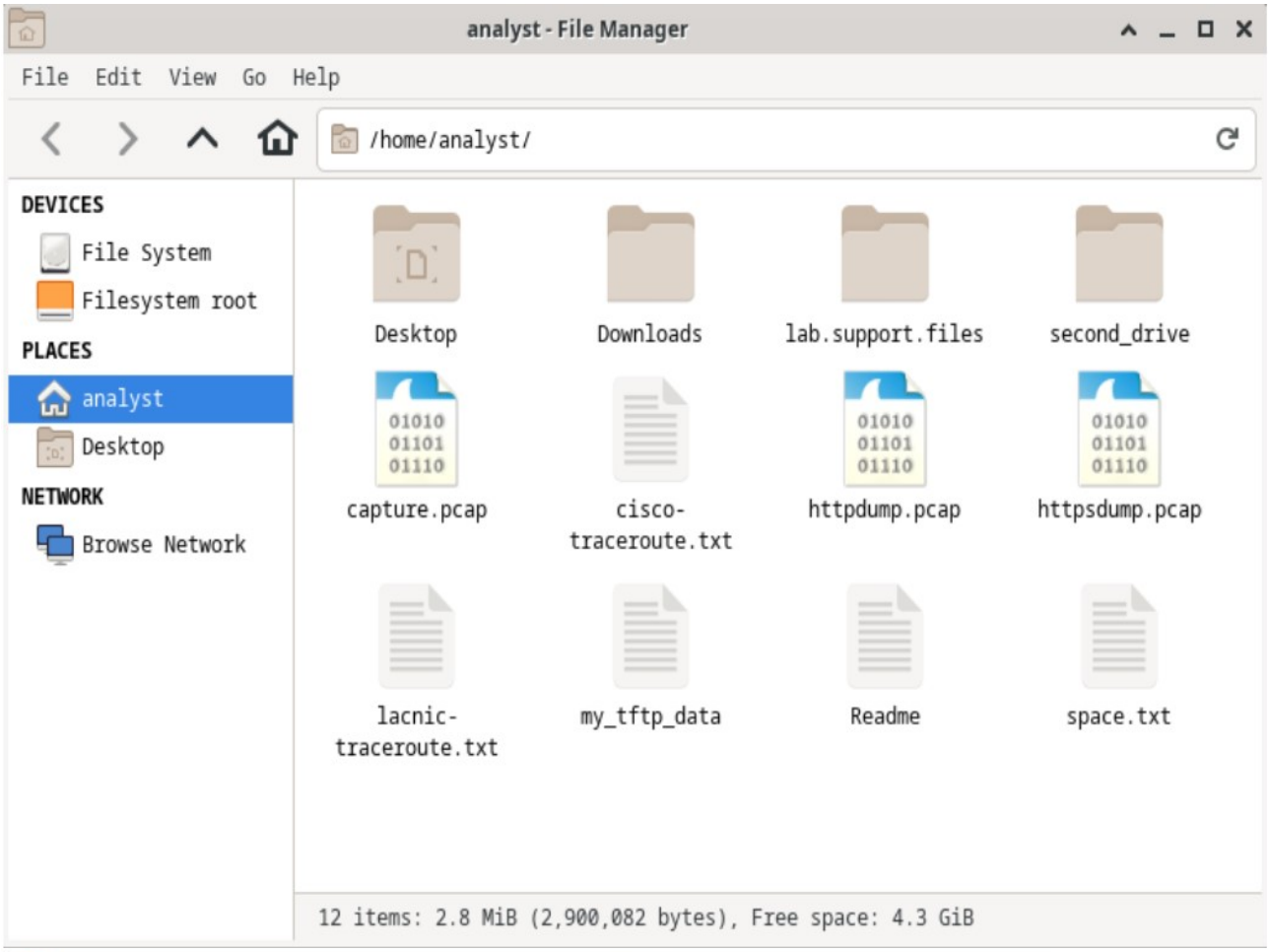

Applications
Altoro Mutual - Mozilla Firef...
Terminal - analyst@secOps:~
04:45
analyst
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
01 110 101 011 010110
Altoro Mutual - Mozilla Firefox
Altoro Mutual
www.altoromutual.com/login.jsp
AltoroMutual
Sign In | Contact Us | Feedback | Search
Go
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
PERSONAL
Deposit Product
Checking
Loan Products
Cards
Investments & Insurance
Other Services
SMALL BUSINESS
Deposit Products
Lending Services
Cards
Insurance
Retirement
Other Services
INSIDE ALTORO MUTUAL
About Us
Contact Us
Locations
Investor Relations
Press Room
Careers
Subscribe
Online Banking Login
Username:
Admin
Password:
Login
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
^C8642 packets captured
8656 packets received by filter
0 packets dropped by kernel
[analyst@secOps ~]$

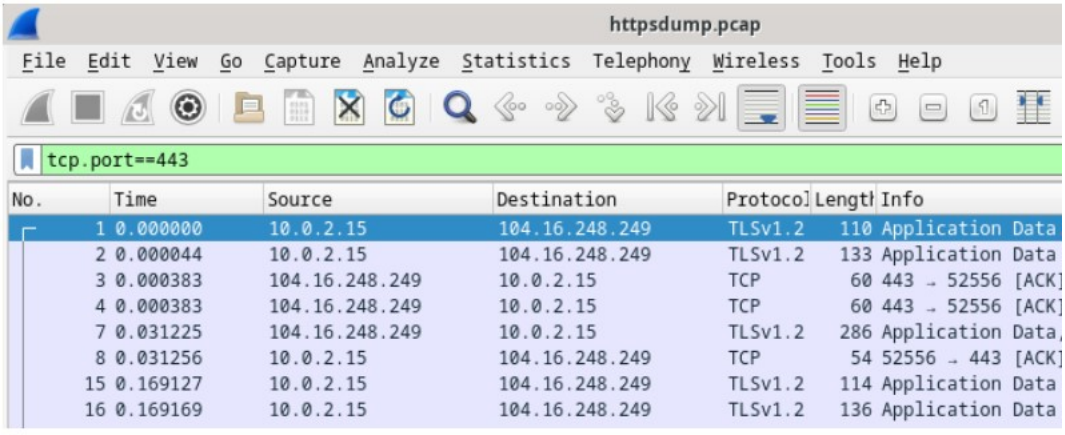





```
8656 packets received by filter
0 packets dropped by kernel
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap
[sudo] password for analyst:
tcpdump: illegal token: -
[analyst@secOps ~]$
```








```
▸ Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
▸ Ethernet II, Src: PcsCompu_82:75:df (08:00:27:82:75:df), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 104.16.248.249
▸ Transmission Control Protocol, Src Port: 52556, Dst Port: 443, Seq: 1, Ack: 1, Len: 56
▾ Transport Layer Security
  ▾ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 51
      Encrypted Application Data: 7fa9037731c6e38e6213aacc15a0a7281f94046fdb237be9…
```