Consegna 25 Ottobre

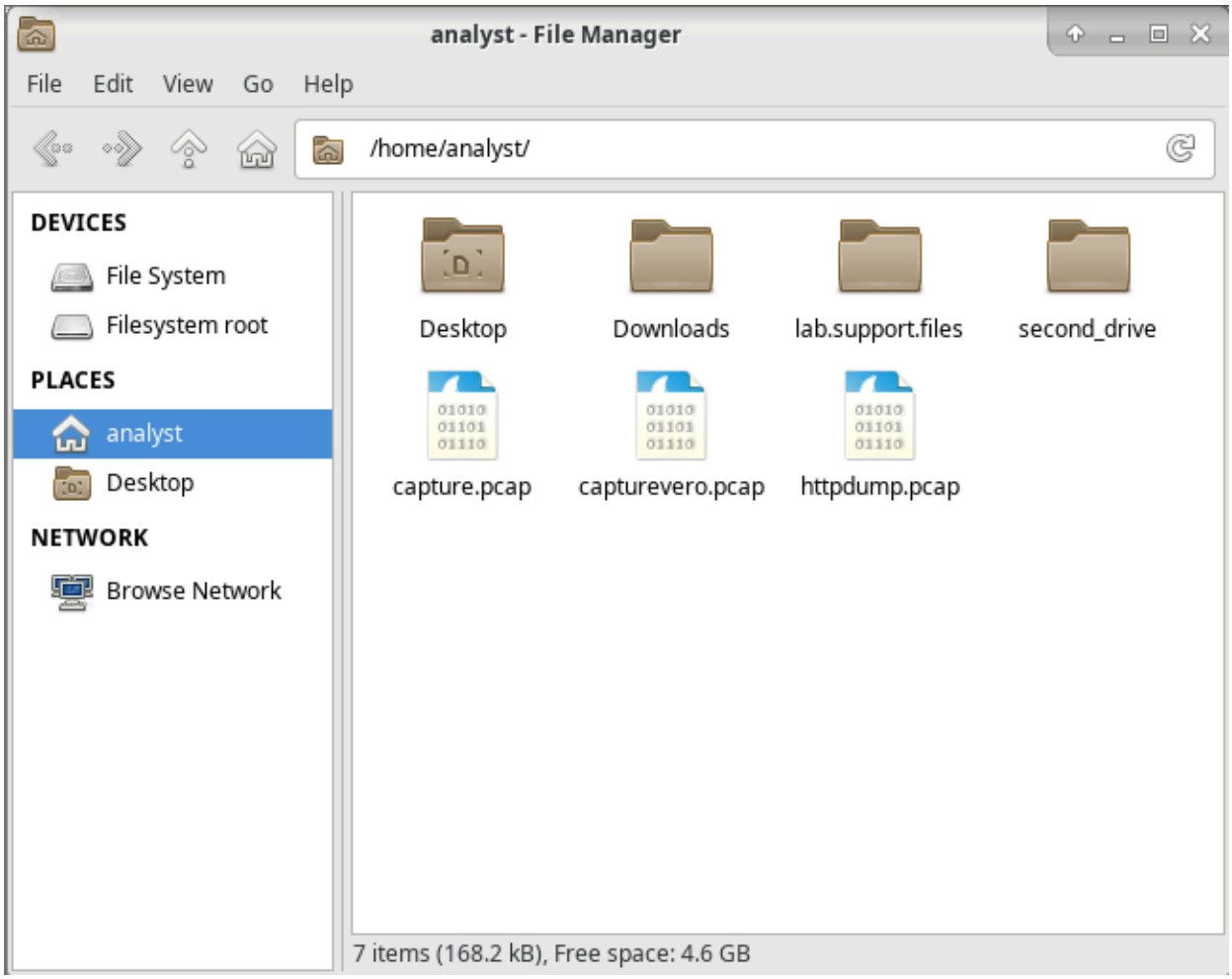
Laboratorio - Utilizzo di Wireshark per Esaminare il Traffico HTTP e HTTPS

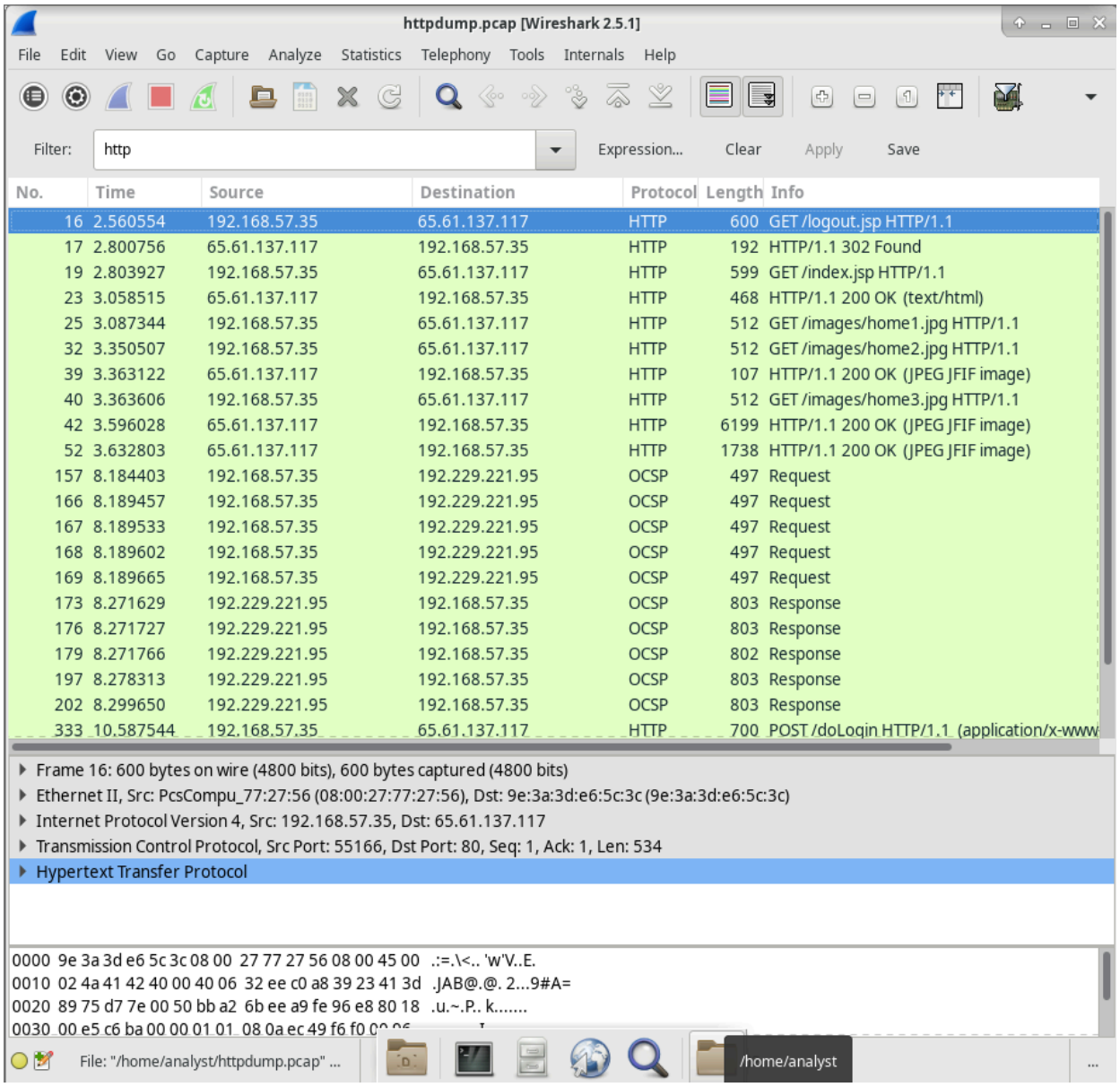
Obiettivo del Lab: Catturare e analizzare traffico HTTP e HTTPS utilizzando Wireshark, evidenziando le differenze tra traffico non crittografato e crittografato.
Configurazione Iniziale:

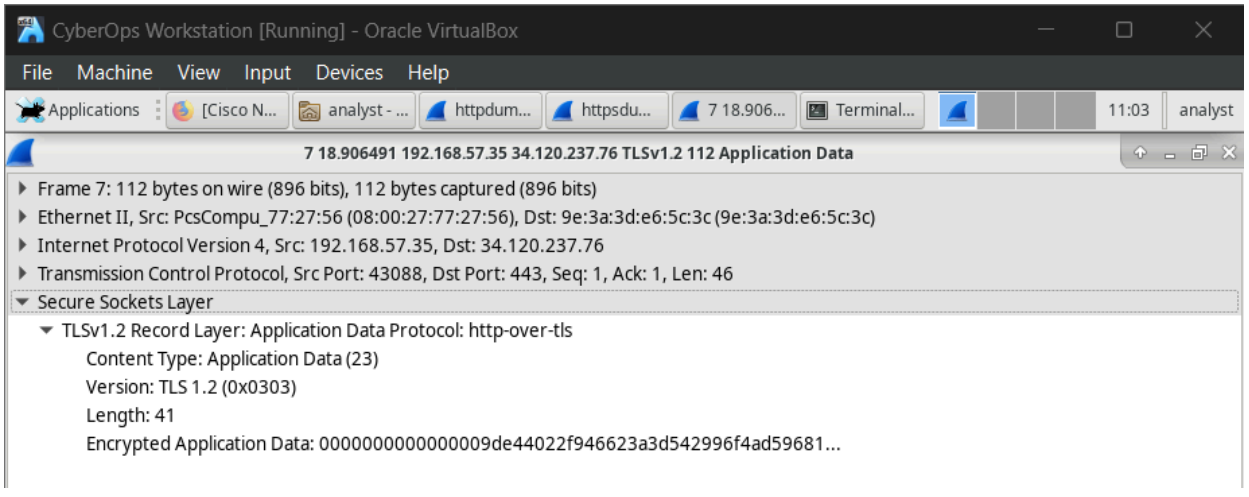
- Avviare la VM CyberOps e accedere come "analyst" (password: cyberops).
- Utilizzare `tcpdump` per catturare il traffico e salvare il file `.pcap` per l'analisi con Wireshark.

Parte 1 - Traffico HTTP:

- Avviare `tcpdump` per catturare il traffico HTTP non crittografato.
- Visitare un sito HTTP (http://www.altoromutual.com/login.jsp) e inserire credenziali di accesso.
- Analizzare il file `.pcap` in Wireshark: le credenziali inserite appaiono in chiaro.

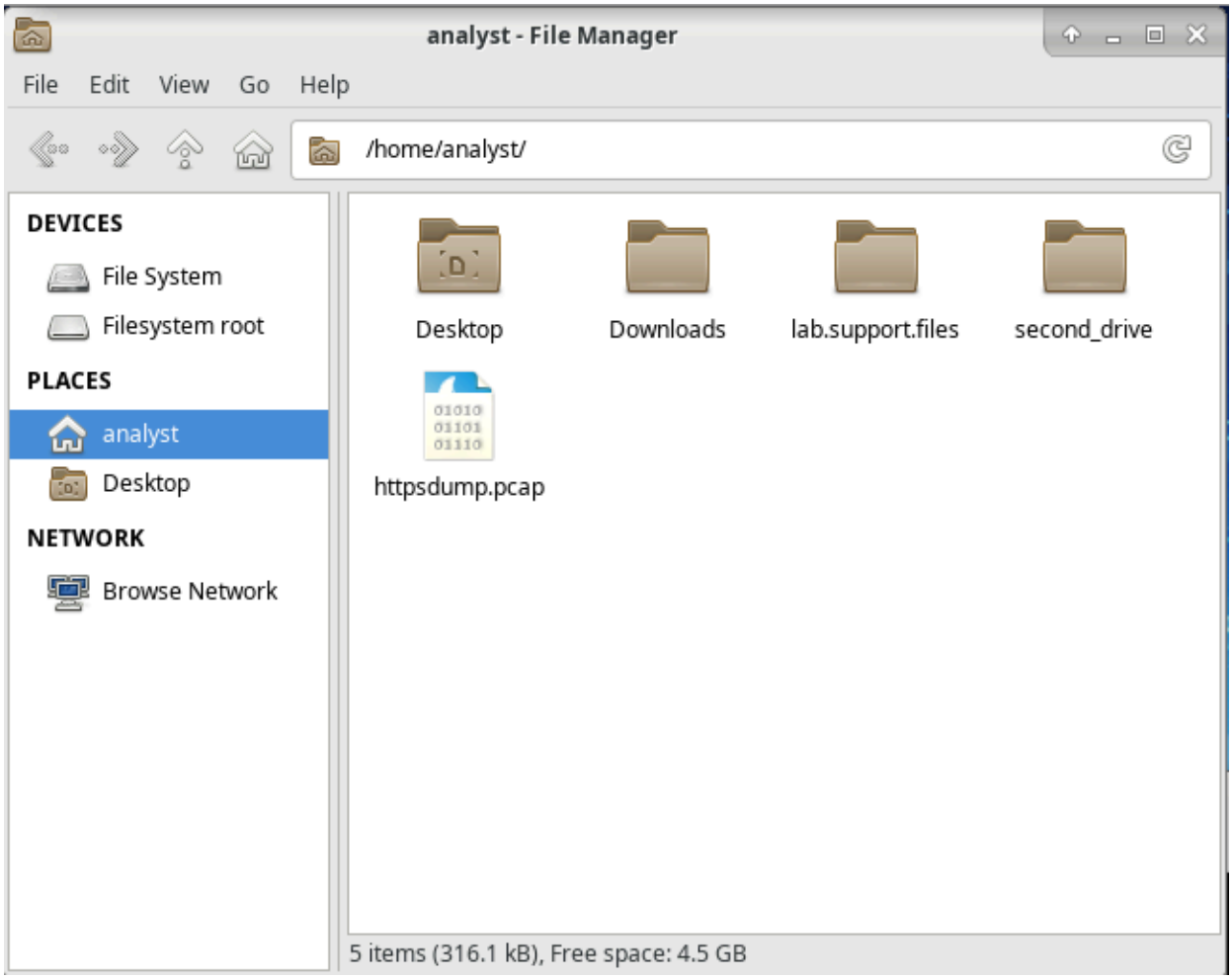

analyst - File Manager
File
Edit
View
Go
Help
/home/analyst/
DEVICES
File System
Filesystem root
PLACES
analyst
Desktop
NETWORK
Browse Network
Desktop
Downloads
lab.support.files
second_drive
capture.pcap
capturevero.pcap
httpdump.pcap
7 items (168.2 kB), Free space: 4.6 GB

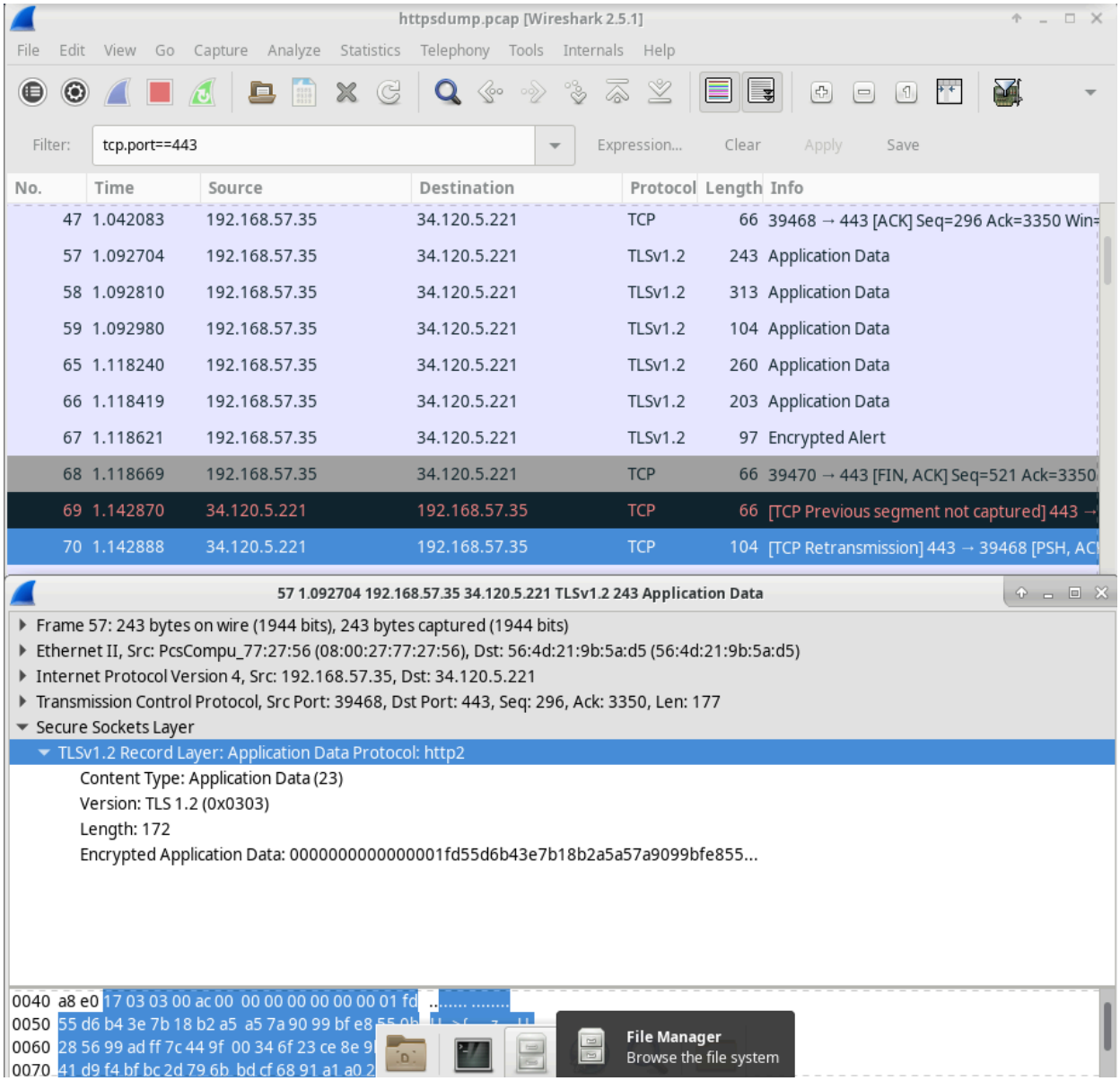

httpdump.pcap [Wireshark 2.5.1]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
16 2.560554 192.168.57.35 65.61.137.117 HTTP 600 GET /logout.jsp HTTP/1.1
17 2.800756 65.61.137.117 192.168.57.35 HTTP 192 HTTP/1.1 302 Found
19 2.803927 192.168.57.35 65.61.137.117 HTTP 599 GET /index.jsp HTTP/1.1
23 3.058515 65.61.137.117 192.168.57.35 HTTP 468 HTTP/1.1 200 OK (text/html)
25 3.087344 192.168.57.35 65.61.137.117 HTTP 512 GET /images/home1.jpg HTTP/1.1
32 3.350507 192.168.57.35 65.61.137.117 HTTP 512 GET /images/home2.jpg HTTP/1.1
39 3.363122 65.61.137.117 192.168.57.35 HTTP 107 HTTP/1.1 200 OK (JPEG JFIF image)
40 3.363606 192.168.57.35 65.61.137.117 HTTP 512 GET /images/home3.jpg HTTP/1.1
42 3.596028 65.61.137.117 192.168.57.35 HTTP 6199 HTTP/1.1 200 OK (JPEG JFIF image)
52 3.632803 65.61.137.117 192.168.57.35 HTTP 1738 HTTP/1.1 200 OK (JPEG JFIF image)
157 8.184403 192.168.57.35 192.229.221.95 OCSP 497 Request
166 8.189457 192.168.57.35 192.229.221.95 OCSP 497 Request
167 8.189533 192.168.57.35 192.229.221.95 OCSP 497 Request
168 8.189602 192.168.57.35 192.229.221.95 OCSP 497 Request
169 8.189665 192.168.57.35 192.229.221.95 OCSP 497 Request
173 8.271629 192.229.221.95 192.168.57.35 OCSP 803 Response
176 8.271727 192.229.221.95 192.168.57.35 OCSP 803 Response
179 8.271766 192.229.221.95 192.168.57.35 OCSP 802 Response
197 8.278313 192.229.221.95 192.168.57.35 OCSP 803 Response
202 8.299650 192.229.221.95 192.168.57.35 OCSP 803 Response
333 10.587544 192.168.57.35 65.61.137.117 HTTP 700 POST /doLogin HTTP/1.1 (application/x-www
Frame 16: 600 bytes on wire (4800 bits), 600 bytes captured (4800 bits)
Ethernet II, Src: PcsCompu_77:27:56 (08:00:27:77:27:56), Dst: 9e:3a:3d:e6:5c:3c (9e:3a:3d:e6:5c:3c)
Internet Protocol Version 4, Src: 192.168.57.35, Dst: 65.61.137.117
Transmission Control Protocol, Src Port: 55166, Dst Port: 80, Seq: 1, Ack: 1, Len: 534
Hypertext Transfer Protocol
0000 9e 3a 3d e6 5c 3c 08 00 27 77 27 56 08 00 45 00 .:=.\<.. 'w'V..E.
0010 02 4a 41 42 40 00 40 06 32 ee c0 a8 39 23 41 3d .JAB@.@. 2...9#A=
0020 89 75 d7 7e 00 50 bb a2 6b ee a9 fe 96 e8 80 18 .u.~.P.. k.....
File: "/home/analyst/httpdump.pcap" ...
/home/analyst


CyberOps Workstation [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications [Cisco N... analyst - ... httpdum... httpsdu... 7 18.906... Terminal... 11:03 analyst
7 18.906491 192.168.57.35 34.120.237.76 TLSv1.2 112 Application Data
Frame 7: 112 bytes on wire (896 bits), 112 bytes captured (896 bits)
Ethernet II, Src: PcsCompu_77:27:56 (08:00:27:77:27:56), Dst: 9e:3a:3d:e6:5c:3c (9e:3a:3d:e6:5c:3c)
Internet Protocol Version 4, Src: 192.168.57.35, Dst: 34.120.237.76
Transmission Control Protocol, Src Port: 43088, Dst Port: 443, Seq: 1, Ack: 1, Len: 46
Secure Sockets Layer
TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
Content Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 41
Encrypted Application Data: 0000000000000009de44022f946623a3d542996f4ad59681...

Parte 2 - Traffico HTTPS:

- Avviare `tcpdump` per catturare il traffico HTTPS.
- Visitare un sito HTTPS (www.netacad.com) e analizzare la cattura in Wireshark.
- In HTTPS, la sezione HTTP è sostituita dalla crittografia SSL/TLS, rendendo il contenuto dei dati non visibile.


analyst - File Manager
File
Edit
View
Go
Help
/home/analyst/
DEVICES
File System
Filesystem root
PLACES
analyst
Desktop
NETWORK
Browse Network
Desktop
Downloads
lab.support.files
second_drive
01010
01101
01110
httpsdump.pcap
5 items (316.1 kB), Free space: 4.5 GB



Riflessioni:

- **Vantaggi di HTTPS**: I dati sono crittografati, visibili solo ai dispositivi autorizzati.
- **Sicurezza del HTTPS**: Non tutti i siti HTTPS sono affidabili; alcuni siti malevoli usano HTTPS per sembrare sicuri.