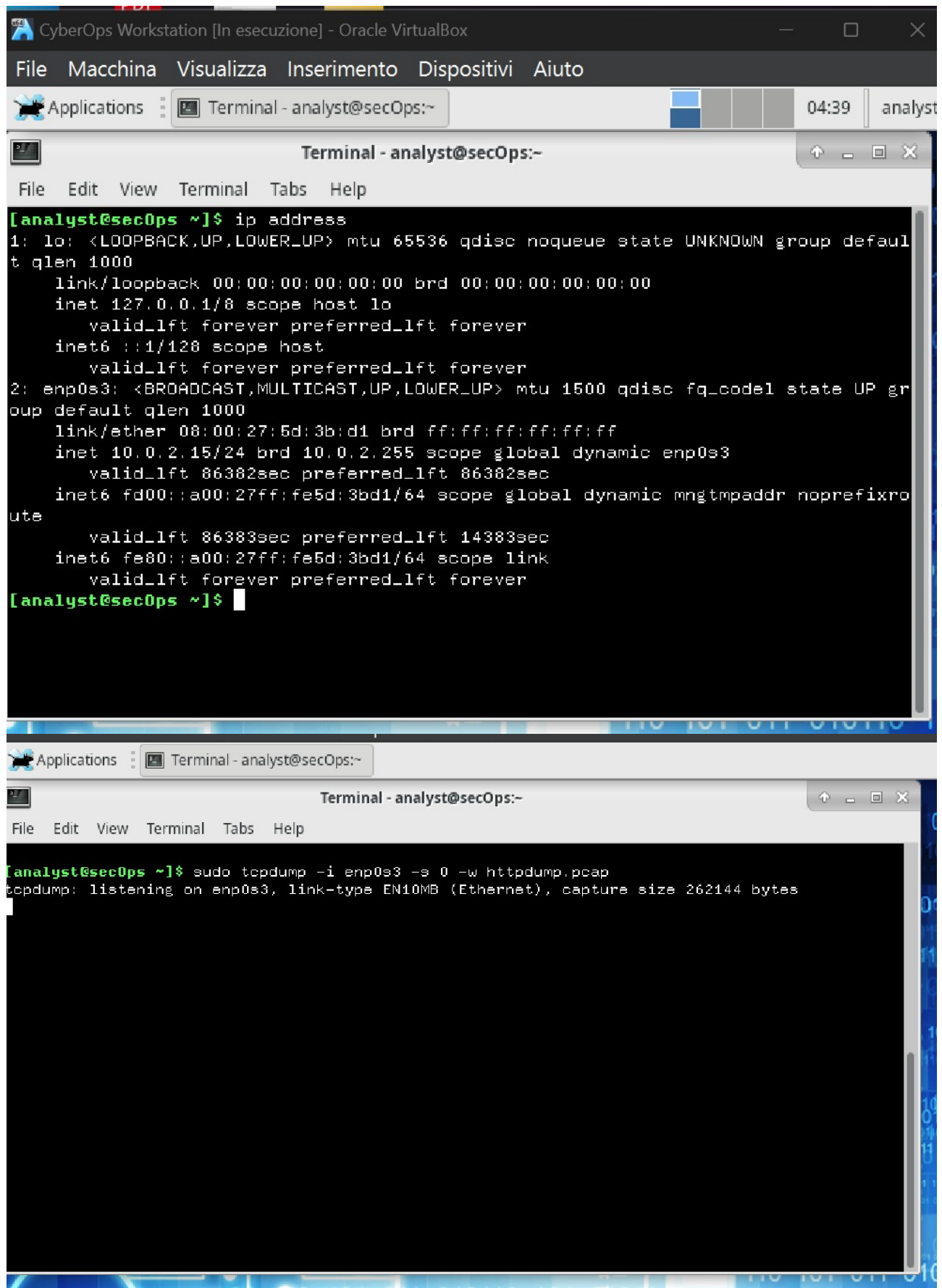
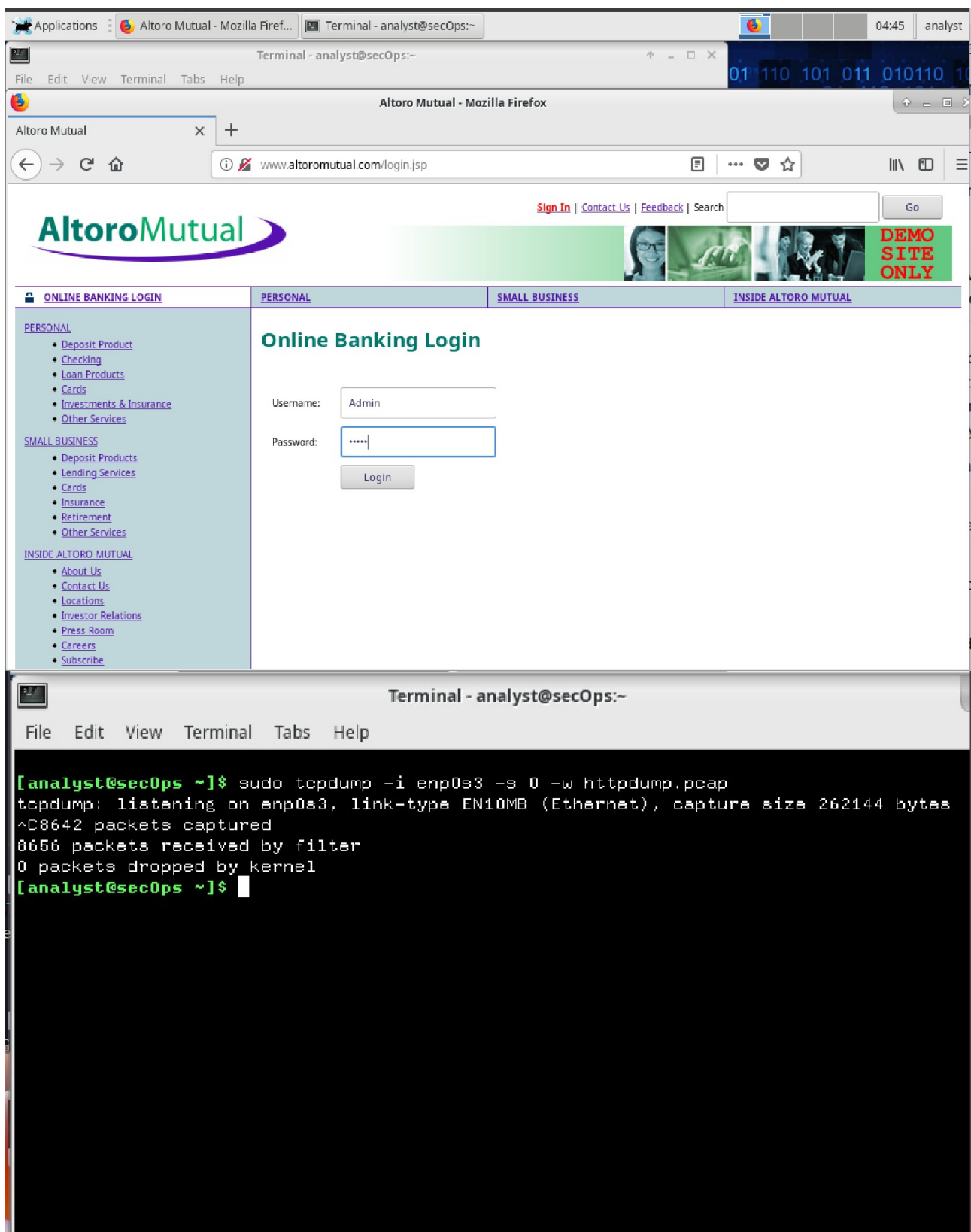


Utilizzo di Wireshark per Esaminare il Traffico HTTP e HTTPS





analyst - File Manager

/home/analyst/

Desktop

Downloads

capture.pcap

htpdump.pcap

htpdump.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
10	0.081730	10.0.2.15	34.107.221.82	HTTP	342	GET /success.txt HTTP/1.1
12	0.127841	34.107.221.82	10.0.2.15	HTTP	270	HTTP/1.1 200 OK (text/plain)
64	1.629160	10.0.2.15	173.222.245.33	OCSP	485	Request
68	1.632062	10.0.2.15	173.222.245.33	OCSP	485	Request
88	1.805743	173.222.245.33	10.0.2.15	OCSP	943	Response
90	1.808726	173.222.245.33	10.0.2.15	OCSP	943	Response
102	1.846016	10.0.2.15	173.222.245.9	OCSP	485	Request
108	1.893834	173.222.245.9	10.0.2.15	OCSP	943	Response
192	2.264743	10.0.2.15	173.222.245.33	OCSP	485	Request
194	2.294705	173.222.245.33	10.0.2.15	OCSP	943	Response
318	2.847244	10.0.2.15	216.58.204.227	OCSP	481	Request
323	2.991767	216.58.204.227	10.0.2.15	OCSP	755	Response
386	3.268870	10.0.2.15	216.58.204.227	OCSP	481	Request
393	3.290631	10.0.2.15	65.61.137.117	HTTP	383	GET /login.jsp HTTP/1.1
408	3.415092	216.58.204.227	10.0.2.15	OCSP	755	Response
426	3.455051	65.61.137.117	10.0.2.15	HTTP	143	HTTP/1.1 200 OK (text/html)

No.	Time	Source	Destination	Protocol	Length	Info
3396	4.859743	65.61.137.117	10.0.2.15	HTTP	131	HTTP/1.1 404 Not Found (text/html)
4898	53.501111	10.0.2.15	65.61.137.117	HTTP	589	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
5263	65.263268	10.0.2.15	65.61.137.117	HTTP	589	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)

▶ Frame 4898: 589 bytes on wire (4712 bits), 589 bytes captured (4712 bits)
▶ Ethernet II, Src: PcsCompu_5d:3b:d1 (08:00:27:5d:3b:d1), Dst: 52:55:0a:00:02:02 (52:55:0a:00:02:02)
▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 65.61.137.117
▶ Transmission Control Protocol, Src Port: 45244, Dst Port: 80, Seq: 1, Ack: 1, Len: 535
▶ Hypertext Transfer Protocol
▼ HTML Form URL Encoded: application/x-www-form-urlencoded
▶ Form item: "uid" = "Admin"
▶ Form item: "passw" = "Login"
▶ Form item: "btnSubmit" = "Login"

```

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

```

US
EN

Sign in

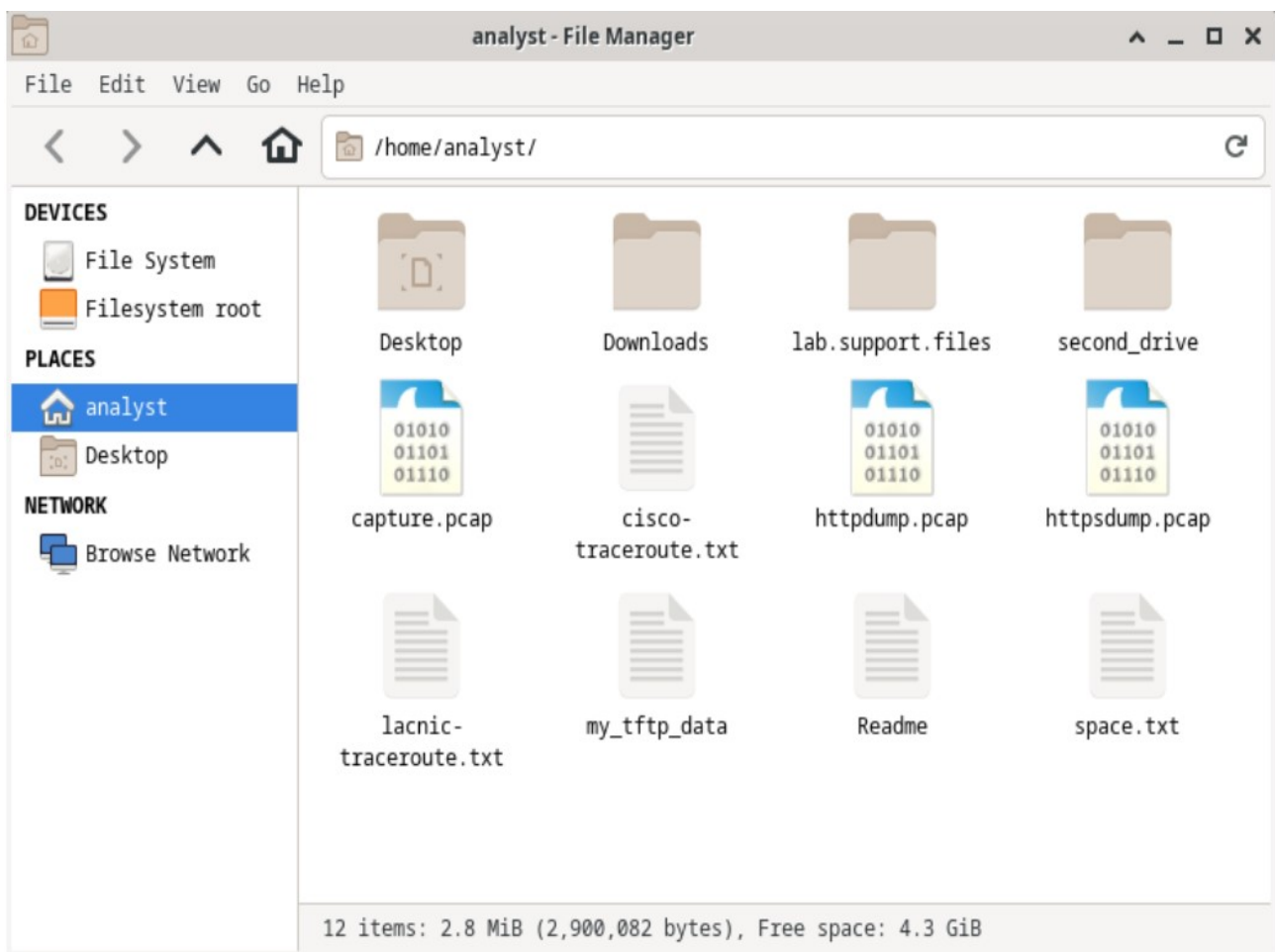
Username or Email

Next

?

powered by

[Terms & Conditions](#) |
 [Privacy](#) |
 [Feedback](#) |
 [Cookies](#) |
 [Trademarks](#)



httpsdump.pcap						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
tcp.port==443						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.15	104.16.248.249	TLSv1.2	110	Application Data
2	0.000044	10.0.2.15	104.16.248.249	TLSv1.2	133	Application Data
3	0.000383	104.16.248.249	10.0.2.15	TCP	60	443 → 52556 [ACK]
4	0.000383	104.16.248.249	10.0.2.15	TCP	60	443 → 52556 [ACK]
7	0.031225	104.16.248.249	10.0.2.15	TLSv1.2	286	Application Data
8	0.031256	10.0.2.15	104.16.248.249	TCP	54	52556 → 443 [ACK]
15	0.169127	10.0.2.15	104.16.248.249	TLSv1.2	114	Application Data
16	0.169169	10.0.2.15	104.16.248.249	TLSv1.2	136	Application Data

- ▶ 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...