

Laboratorio - Utilizzo di Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tutti i diritti riservati.

Installa la versione più recente di PowerShell per nuove funzionalità e miglioramenti. https://aka.ms/PSWindows

PS C:\Users\salvo> dir

Directory: C:\Users\salvo

Mode                LastWriteTime       Length Name
----                -----        ---- 
d----
```

Mode	LastWriteTime	Length	Name
d----	13/03/2025	14:38	.lmstudio
d----	31/03/2025	10:27	.splunk
d----	18/04/2025	18:03	.VirtualBox
d----	13/02/2025	15:01	.vscode
d----	21/02/2025	09:58	Cisco Packet Tracer 8.2.2
d-r----	13/02/2025	10:59	Contacts
d-r----	18/04/2025	12:37	Desktop
d-r----	31/03/2025	10:02	Documents
d-r----	18/04/2025	18:00	Downloads
d-r----	13/03/2025	11:25	Favorites
d-r----	13/02/2025	10:59	Links
d-r----	13/02/2025	10:59	Music
d----	13/03/2025	11:25	NCH Software Suite
dar----	13/02/2025	14:24	OneDrive
d-r----	04/04/2025	15:47	Pictures
d-r----	13/02/2025	10:59	Saved Games
d-r----	13/02/2025	11:16	Searches
d-r----	26/02/2025	12:25	Videos
d----	10/04/2025	17:06	VirtualBox VMs
-a----	13/02/2025	11:26	.gitconfig
-a----	27/02/2025	11:03	24 .lmstudio-home-pointer
-a----	21/02/2025	09:58	176 .packettracer

```
PS C:\Users\salvo> ipconfig

Configurazione IP di Windows
```

```
Prompt dei comandi
Microsoft Windows [Versione 10.0_26100.3775]
(C) Microsoft Corporation. Tutti i diritti riservati.

C:\Users\salvo>dir
Il volume nell'unità C è OS
Numero di serie del volume: 16F6-11A9

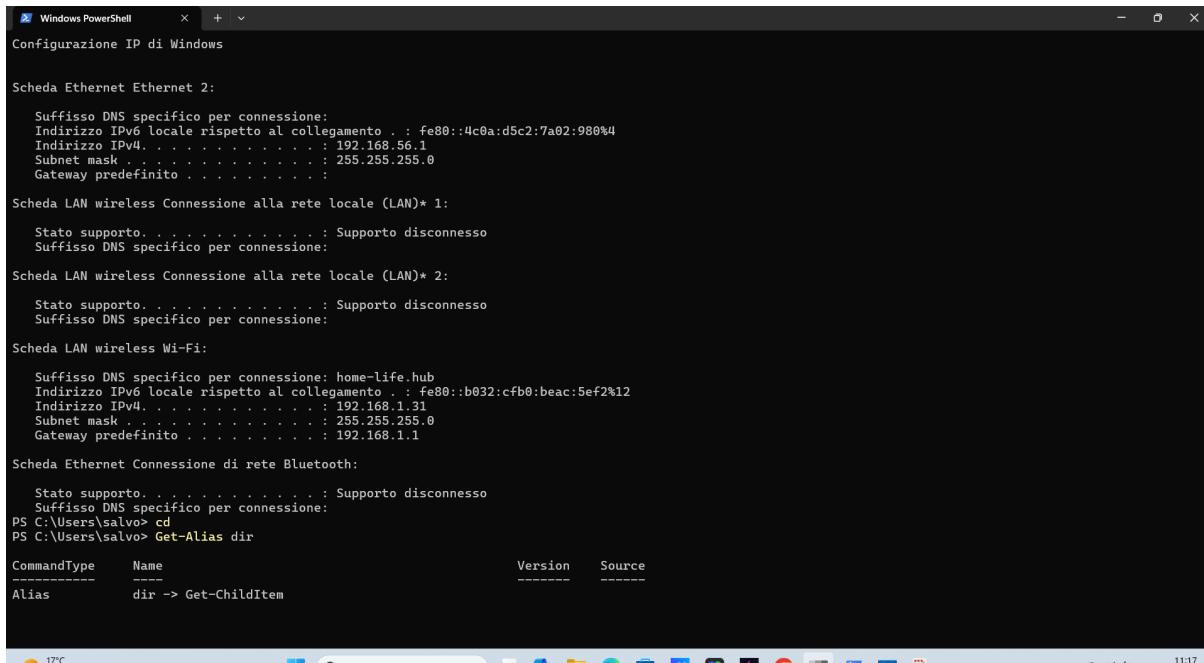
Directory di C:\Users\salvo

13/03/2025 16:27    <DIR>      .
13/02/2025 12:16    <DIR>      ..
13/02/2025 12:26    190 .gitconfig
13/03/2025 15:38    <DIR>      .lmstudio
27/02/2025 12:03    24 .lmstudio-home-pointer
21/02/2025 10:58    176 .packettracer
31/03/2025 10:27    <DIR>      .splunk
10/04/2025 18:03    <DIR>      .VirtualBox
13/02/2025 10:01    <DIR>      .vscode
21/02/2025 10:58    <DIR>      Cisco Packet Tracer 8.2.2
13/02/2025 11:59    <DIR>      Contacts
10/04/2025 12:37    <DIR>      Desktop
31/03/2025 10:02    <DIR>      Documents
10/04/2025 18:00    <DIR>      Downloads
13/03/2025 12:25    <DIR>      Favorites
13/02/2025 11:59    <DIR>      Links
13/02/2025 11:59    <DIR>      Music
13/03/2025 12:25    <DIR>      NCH Software Suite
13/02/2025 15:24    <DIR>      OneDrive
04/04/2025 15:47    <DIR>      Pictures
13/02/2025 11:59    <DIR>      Saved Games
13/03/2025 12:16    <DIR>      Searches
26/02/2025 13:25    <DIR>      Videos
10/04/2025 17:06    <DIR>      VirtualBox VMs
            3 File          390 byte
            21 Directory  57.269.899.264 byte disponibili

C:\Users\salvo>ipconfig

Configurazione IP di Windows
```

Nel primo passaggio ho eseguito il comando **dir** su PowerShell e sul Prompt dei Comandi in modo che entrambe le finestre fornissero un elenco di sottodirectory e file, con informazioni associate come tipo, dimensione del file, data e ora dell'ultima scrittura. In PowerShell vengono visualizzati anche gli attributi/modalità.



```

Windows PowerShell
Configurazione IP di Windows

Scheda Ethernet Ethernet 2:
Suffisso DNS specifico per connessione:
Indirizzo IPv6 locale rispetto al collegamento . : fe80::4c0a:d5c2:7a02:980%4
Indirizzo IPv4 . . . . . : 192.168.56.1
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . :

Scheda LAN wireless Connessione alla rete locale (LAN)* 1:
Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:

Scheda LAN wireless Connessione alla rete locale (LAN)* 2:
Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:

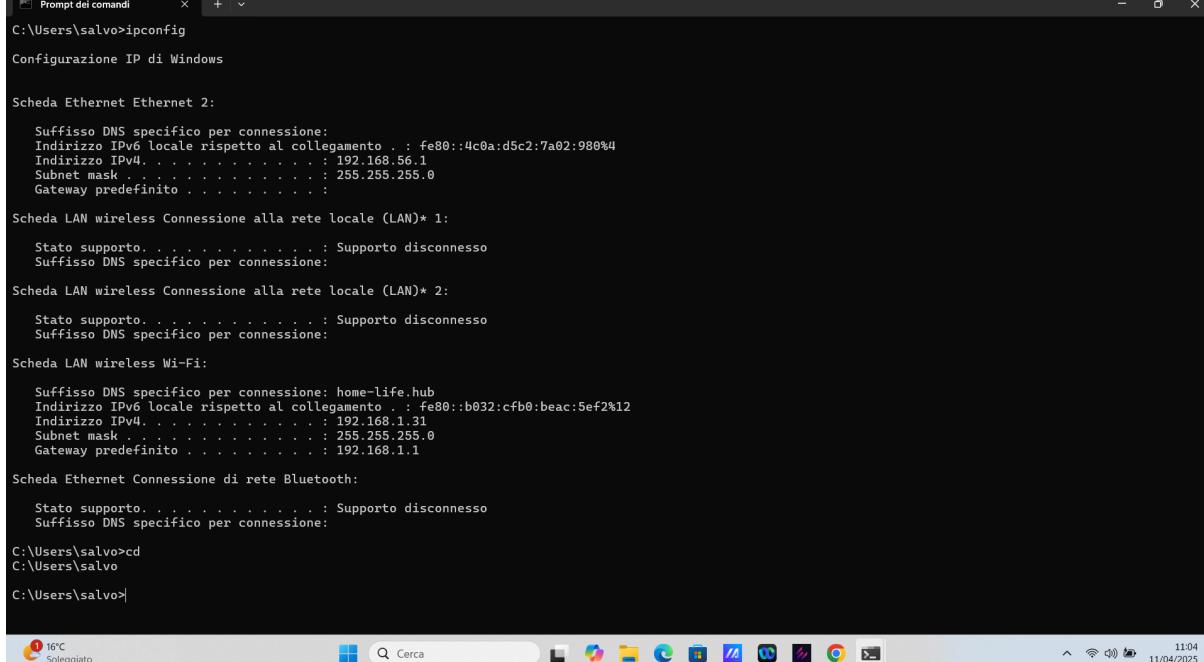
Scheda LAN wireless Wi-Fi:
Suffisso DNS specifico per connessione: home-life.hub
Indirizzo IPv6 locale rispetto al collegamento . : fe80::b032:cfb0:beac:5ef2%12
Indirizzo IPv4. . . . . : 192.168.1.31
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.1.1

Scheda Ethernet Connessione di rete Bluetooth:
Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:
PS C:\Users\salvo> cd
PS C:\Users\salvo> Get-Alias dir

 CommandType      Name          Version      Source
-----      ----          -----      -----
 Alias          dir -> Get-ChildItem

```





```

Prompt dei comandi
C:\Users\salvo>ipconfig
Configurazione IP di Windows

Scheda Ethernet Ethernet 2:
Suffisso DNS specifico per connessione:
Indirizzo IPv6 locale rispetto al collegamento . : fe80::4c0a:d5c2:7a02:980%4
Indirizzo IPv4. . . . . : 192.168.56.1
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . :

Scheda LAN wireless Connessione alla rete locale (LAN)* 1:
Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:

Scheda LAN wireless Connessione alla rete locale (LAN)* 2:
Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:

Scheda LAN wireless Wi-Fi:
Suffisso DNS specifico per connessione: home-life.hub
Indirizzo IPv6 locale rispetto al collegamento . : fe80::b032:cfb0:beac:5ef2%12
Indirizzo IPv4. . . . . : 192.168.1.31
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.1.1

Scheda Ethernet Connessione di rete Bluetooth:
Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:
C:\Users\salvo>cd
C:\Users\salvo>
C:\Users\salvo>
```

Successivamente, vado ad eseguire il comando **ipconfig** (Mostra le info della rete (IP, gateway, ecc.), notando che i risultati di entrambe le interfacce sono molto simili. Con il comando **Get-Alias dir** vado ad identificare il comando che elenca la sottodirectory e i file in una directory. Infine chiudo il Prompt dei Comandi e continuo a lavorare con PowerShell.

```
Windows PowerShell
PS C:\Users\salvo> cd
PS C:\Users\salvo> Get-Alias dir
 CommandType      Name          Version      Source
-----      ----          -----      -----
 Alias        dir -> Get-ChildItem

PS C:\Users\salvo> Get-ChildItem

Directory: C:\Users\salvo

Mode                LastWriteTime     Length Name
----                -----           -----    Name
d----       13/03/2025 14:38 .lstudio
d----       31/03/2025 10:27 .splunk
d----       18/04/2025 18:03 .VirtualBox
d----       13/02/2025 15:01 .vscode
d----       21/02/2025 09:58 Cisco Packet Tracer 8.2.2
d-r----      13/02/2025 10:59 Contacts
d-r----      18/04/2025 12:37 Desktop
d-r----      31/03/2025 10:02 Documents
d-r----      18/04/2025 18:00 Downloads
d-r----      13/03/2025 11:25 Favorites
d-r----      13/02/2025 10:59 Links
d-r----      13/02/2025 10:59 Music
d----       13/03/2025 11:25 NCH Software Suite
d-a----      13/02/2025 14:24 OneDrive
d-r----      04/04/2025 15:47 Pictures
d-r----      13/02/2025 10:59 Saved Games
d-r----      13/02/2025 11:16 Searches
d-r----      26/02/2025 12:25 Videos
d----       18/04/2025 17:06 VirtualBox VMs
-a----       13/02/2025 11:26 .gitconfig
-a----       27/02/2025 11:03 24 .lstudio-home-pointer
-a----       21/02/2025 09:58 176 .packettracer

PS C:\Users\salvo> netstat -h
```

Polline molto alto Oggi 11:18 11/04/2025

Selezionando il comando **Get-ChildItem** ottengo l'elenco di file e cartelle in una directory. Poco dopo scrivo il comando **netstat -h** per visualizzare le opzioni disponibili di **netstat**.

```
PS C:\Users\salvo> netstat -h
Socket Handle Count

  PID      Count  Closing Count
  2952        8       0
  6688        5       0
  1564       11       0
  3612       23       0
  5412        4       0
  3112        1       0
  14376       2       0
  6652        6       0
  8920       2       0
  4168        4       0
  1629       2       0
  4184        7       0
  12888       2       0
  15794       1       0
  1116        4       0
  14688      13       0
  1892        2       0
  10864      12       0
  8324        2       0
  2456        4       0
  12444       4       0
  5024       12       0
  7076        3       0
  1200        4       0
  3252        4       0
  5304        6       0
  11960       2       0
  4540        1       0
  4036        4       0
  4804        1       0
  15832      19       6
  15592       4       0
  2032        1       0
  1268        4       0
  8948        8       0
```

Polline molto alto Oggi □ Cerca 11:18 11/04/2025

```
PS C:\Windows\system32> netstat -r
IPv4 Tabella route
=====
Route attive:
=====  
Indirizzo rete      Mask     Gateway   Interfaccia Metrica
  0.0.0.0      0.0.0.0  192.168.1.1  192.168.1.31    55
  127.0.0.0    255.0.0.0  On-link   127.0.0.1     331
  127.0.0.1    255.255.255  On-link   127.0.0.1     331
127.255.255.255 255.255.255.255  On-link   127.0.0.1     331
  192.168.1.0   255.255.255.0  On-link   192.168.1.31    311
  192.168.1.31 255.255.255.255  On-link   192.168.1.31    311
  192.168.1.255 255.255.255.255  On-link   192.168.1.31    311
  192.168.56.0   255.255.255.0  On-link   192.168.56.1    281
  192.168.56.1   255.255.255.255  On-link   192.168.56.1    281
  192.168.56.255 255.255.255.255  On-link   192.168.56.1    281
  224.0.0.0     240.0.0.0  On-link   127.0.0.1     331
  224.0.0.0     240.0.0.0  On-link   192.168.56.1    281
  224.0.0.0     240.0.0.0  On-link   192.168.1.31    311
  255.255.255.255 255.255.255.255  On-link   127.0.0.1     331
  255.255.255.255 255.255.255.255  On-link   192.168.56.1    281
  255.255.255.255 255.255.255.255  On-link   192.168.1.31    311
=====  
Route permanenti:  
Nessuna  
  
IPv6 Tabella route
=====
Route attive:
=====  
Interf Metr Rete Destinazione     Gateway
  1    331 :1/128  On-link
  0    281 fe80::/64  On-link
  12   311 fe80::/64  On-link
  4    281 fe80::d5c2:7a02:980/128
  12   311 fe80::b032:cfa0:beac:5ef2/128
  1    331 ff00::/8   On-link
  4    281 ff00::/8   On-link
  12   311 ff00::/8   On-link
=====  
Route permanenti:  
Nessuna
```

Polline molto alto Oggi □ Cerca 11:19 11/04/2025

Scelgo il comando **netstat -r** per visualizzare la tabella di routing con i percorsi attivi

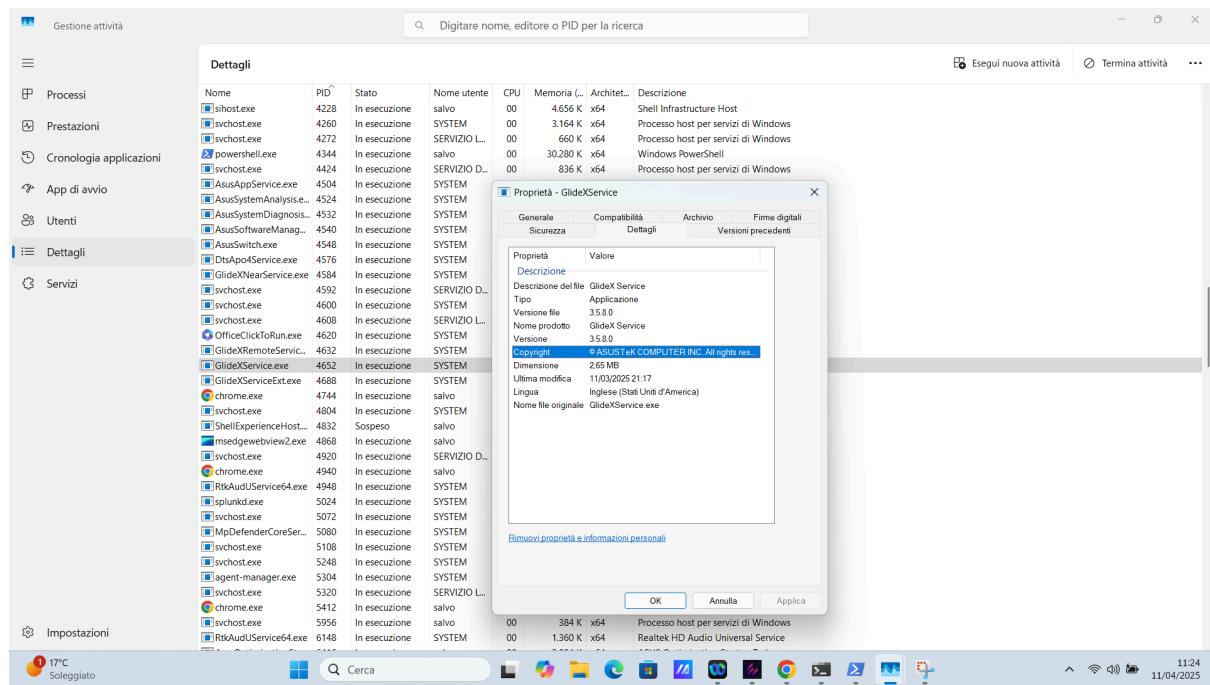
```

[glideXService.exe] 0.0.0.0:49671 0.0.0.0:0 LISTENING 4652
[glideXService.exe] 0.0.0.0:49672 0.0.0.0:0 LISTENING 4652
[glideXService.exe] 0.0.0.0:49673 0.0.0.0:0 LISTENING 4652
[glideXService.exe] 0.0.0.0:49674 0.0.0.0:0 LISTENING 4652
[glideXService.exe] 0.0.0.0:49675 0.0.0.0:0 LISTENING 4652
[TCP 127.0.0.1:8065 [Python3.9.exe]] 0.0.0.0:0 LISTENING 8324
[TCP 127.0.0.1:8089 [splunkd.exe]] 127.0.0.1:49708 ESTABLISHED 5024
[TCP 127.0.0.1:8089 [splunkd.exe]] 127.0.0.1:51658 ESTABLISHED 5024
[TCP 127.0.0.1:8191 [mongod.exe]] 127.0.0.1:49713 ESTABLISHED 3612
[TCP 127.0.0.1:8191 [mongod.exe]] 127.0.0.1:49727 ESTABLISHED 3612
[TCP 127.0.0.1:8191 [mongod.exe]] 127.0.0.1:49729 ESTABLISHED 3612
[TCP 127.0.0.1:8191 [mongod.exe]] 127.0.0.1:49730 ESTABLISHED 3612
[TCP 127.0.0.1:8191 [mongod.exe]] 127.0.0.1:49745 ESTABLISHED 3612
[TCP 127.0.0.1:8191 [mongod.exe]] 127.0.0.1:49748 ESTABLISHED 3612
[TCP 127.0.0.1:8191 [mongod.exe]] 127.0.0.1:51011 ESTABLISHED 3612
[TCP 127.0.0.1:8191 [mongod.exe]] 127.0.0.1:51510 ESTABLISHED 3612
[TCP 127.0.0.1:8191 [mongod.exe]] 127.0.0.1:51604 ESTABLISHED 3612
[TCP 127.0.0.1:8191 [mongod.exe]] 127.0.0.1:51606 ESTABLISHED 3612
[TCP 127.0.0.1:8191 [mongod.exe]] 127.0.0.1:51656 ESTABLISHED 3612
[TCP 127.0.0.1:8191 [mongod.exe]] 127.0.0.1:51739 ESTABLISHED 3612
[TCP 127.0.0.1:8191 [mongod.exe]] 127.0.0.1:51740 ESTABLISHED 3612
[TCP 127.0.0.1:8191 [mongod.exe]] 127.0.0.1:51741 ESTABLISHED 3612
[TCP 127.0.0.1:8191 [mongod.exe]] 127.0.0.1:51754 ESTABLISHED 3612
[TCP 127.0.0.1:8191 [mongod.exe]] 127.0.0.1:51817 ESTABLISHED 3612

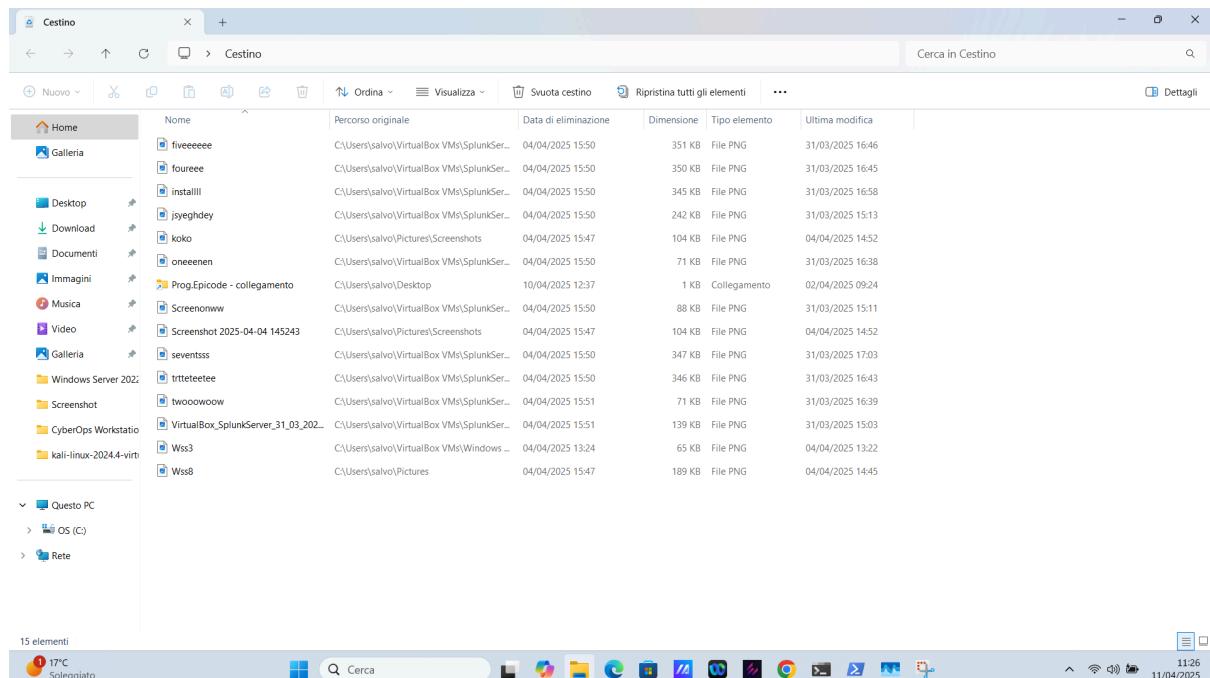
```

Ho avviato PowerShell come amministratore ed eseguito il comando **netstat -abno**, che mostra tutte le connessioni di rete attive, le porte in ascolto, i nomi dei processi associati, i PID (Process ID) e gli indirizzi IP locali/remoti. Dallo screenshot, si nota ad esempio che processi come **GlideXService.exe**, **Python3.exe**, **splunkd.exe** e **mongod.exe** stanno comunicando su diverse porte, alcune in **LISTENING**, altre in **ESTABLISHED** (connessioni attive).

Dettagli								
	Nome	PID	Stato	Nome utente	CPU	Memoria (L...)	Architet...	Descrizione
Processes	spoolsv.exe	4168	In esecuzione	SYSTEM	00	1.076 K	x64	Applicazione sottosistema spooler
Prestazioni	svchost.exe	4184	In esecuzione	SERVIZIO L...	00	3.148 K	x64	Processo host per servizi di Windows
Cronologia applicazioni	svchost.exe	4228	In esecuzione	salvo	00	4.640 K	x64	Shell Infrastructure Host
App di avvio	svchost.exe	4260	In esecuzione	SYSTEM	00	3.232 K	x64	Processo host per servizi di Windows
Utenti	svchost.exe	4272	In esecuzione	SERVIZIO L...	00	664 K	x64	Processo host per servizi di Windows
Dettagli	powershell.exe	4344	In esecuzione	salvo	00	30.280 K	x64	Windows PowerShell
App di avvio	svchost.exe	4424	In esecuzione	SERVIZIO D...	00	848 K	x64	Processo host per servizi di Windows
Utenti	AsusAppService.exe	4504	In esecuzione	SYSTEM	00	1.128 K	x64	ASUS App Service
Impostazioni	AsusSystemAnalysis...	4524	In esecuzione	SYSTEM	00	2.032 K	x64	ASUS System Analysis
Services	AsusSystemDiagnos...	4532	In esecuzione	SYSTEM	00	632 K	x64	ASUS System Diagnosis
	AsusSoftwareManag...	4540	In esecuzione	SYSTEM	00	2.400 K	x64	ASUS Software Manager
	AsusSwitch.exe	4548	In esecuzione	SYSTEM	00	1.008 K	x64	ASUS Switch
	OtsApol4Service.exe	4576	In esecuzione	SYSTEM	00	1.252 K	x64	Controls the DTS audio processing object.
	GlideXNearService.exe	4584	In esecuzione	SYSTEM	00	812 K	x64	GlideX Near Service
	svchost.exe	4592	In esecuzione	SERVIZIO D...	00	2.524 K	x64	Processo host per servizi di Windows
	svchost.exe	4600	In esecuzione	SYSTEM	00	23.048 K	x64	Processo host per servizi di Windows
	svchost.exe	4608	In esecuzione	SERVIZIO L...	00	18.194 K	x64	Processo host per servizi di Windows
	OfficeClickToRun.exe	4620	In esecuzione	SYSTEM	00	13.628 K	x64	Microsoft Office Click-to-Run (SxS)
	GlideXRemoteServic...	4632	In esecuzione	SYSTEM	00	1.196 K	x64	GlideX Remote Service
	GlideXService.exe	4652	In esecuzione	SYSTEM	00	1.496 K	x64	GlideX Service
	GlideXServiceExt.exe	4688	In esecuzione	SYSTEM	00	1.384 K	x64	GlideX Service Extension
	chrome.exe	4744	In esecuzione	salvo	00	21.380 K	x64	Google Chrome
	svchost.exe	4804	In esecuzione	SYSTEM	00	1.344 K	x64	Processo host per servizi di Windows
	ReatekHDUserService64.exe	4948	In esecuzione	SYSTEM	00	1.692 K	x64	Reatek HD Audio Universal Service
	splunkd.exe	5024	In esecuzione	SYSTEM	00	135.164 K	x64	splunkd service
	svchost.exe	5072	In esecuzione	SYSTEM	00	1.040 K	x64	Processo host per servizi di Windows
	MpDefenderCoreSer...	5080	In esecuzione	SYSTEM	00	4.040 K		Antimalware Core Service
	svchost.exe	5108	In esecuzione	SYSTEM	00	412 K	x64	Processo host per servizi di Windows
	svchost.exe	5248	In esecuzione	SYSTEM	00	856 K	x64	Processo host per servizi di Windows
	agent-manager.exe	5304	In esecuzione	SYSTEM	00	4.492 K	x64	agent-manager
	svchost.exe	5320	In esecuzione	SERVIZIO L...	00	904 K	x64	Processo host per servizi di Windows
	chrome.exe	5412	In esecuzione	salvo	00	132.980 K	x64	Google Chrome



Successivamente, ho aperto **Gestione Attività**, sono andato nella scheda **Dettagli** e ho cercato il **PID 4652**. Dopo averlo individuato (associato a **GlideXService.exe**), ho fatto clic destro e selezionato **Proprietà**. Dalla finestra aperta ho ottenuto ulteriori informazioni: il file è firmato da **ASUSTeK COMPUTER INC.**, appartiene al software **GlideX Service**, versione **3.5.8.0**, ed è localizzato in **inglese (Stati Uniti d'America)**.



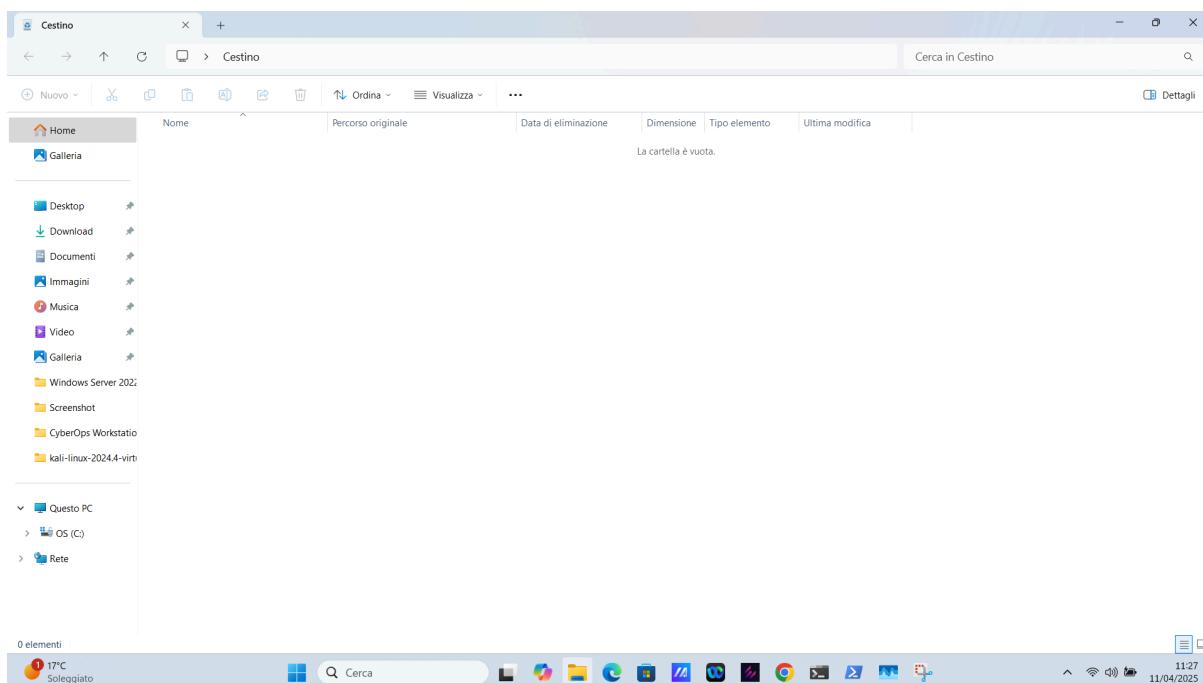
```

Windows PowerShell x + -
192.168.56.1 255.255.255.255      On-link       192.168.56.1    281
192.168.56.255 255.255.255.255      On-link       192.168.56.1    281
224.0.0.0     240.0.0.0      On-link        127.0.0.1     331
224.0.0.0     240.0.0.0      On-link       192.168.56.1    281
224.0.0.0     240.0.0.0      On-link       192.168.1.31    311
255.255.255.255 255.255.255.255      On-link        127.0.0.1     331
255.255.255.255 255.255.255.255      On-link       192.168.56.1    281
255.255.255.255 255.255.255.255      On-link       192.168.1.31    311
=====
Route permanenti:
Nessuna

IPv6 Tabella route
=====
Route attive:
Interf Metrica Rete Destinazione      Gateway
 1   331 ::1/128          On-Link
 4   281 fe80::/64         On-Link
12   311 fe80::/64         On-Link
 4   281 fe80::4c0a:d5c2:7a02:980/128
                                         On-Link
12   311 fe80::b032:cfb0:beac:5ef2/128
                                         On-Link
 1   331 ff00::/8          On-Link
 4   281 ff00::/8          On-Link
12   311 ff00::/8          On-Link
=====
Route permanenti:
Nessuna
PS C:\Users\salvo> clear-recyclebin

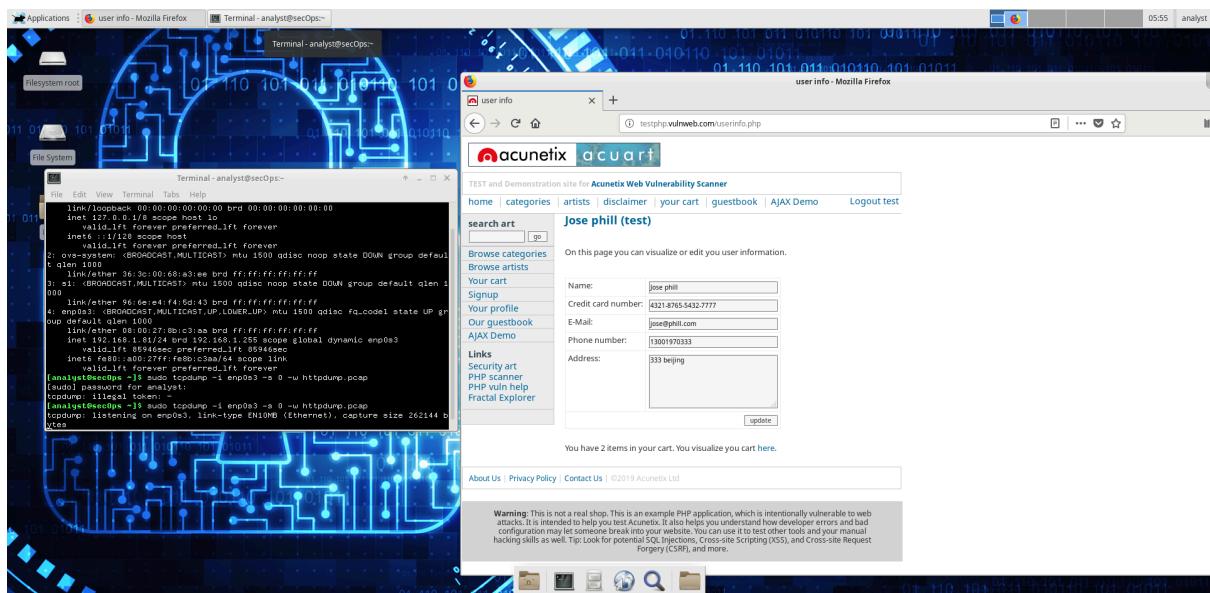
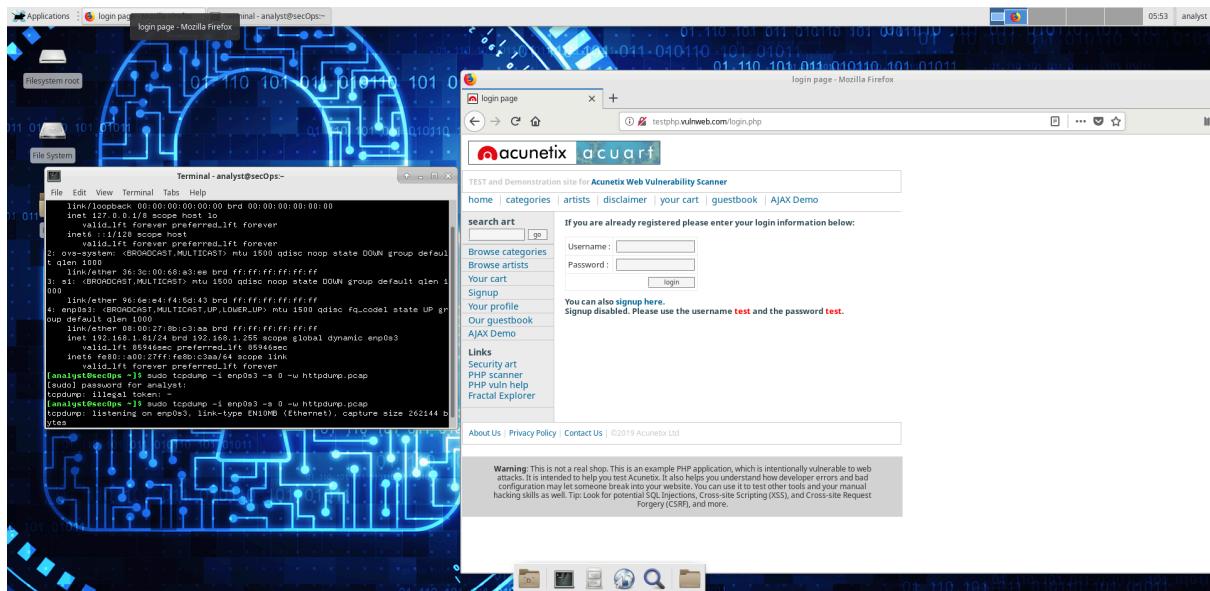
Conferma
Eseguire l'operazione?
Esecuzione dell'operazione "Clear-RecycleBin" sulla destinazione "Tutto il contenuto del Cestino".
[S] Si [T] Si a tutti [N] No [U] No a tutti [O] Sospendi [?] Guida (il valore predefinito è "S"): S
PS C:\Users\salvo> |

```

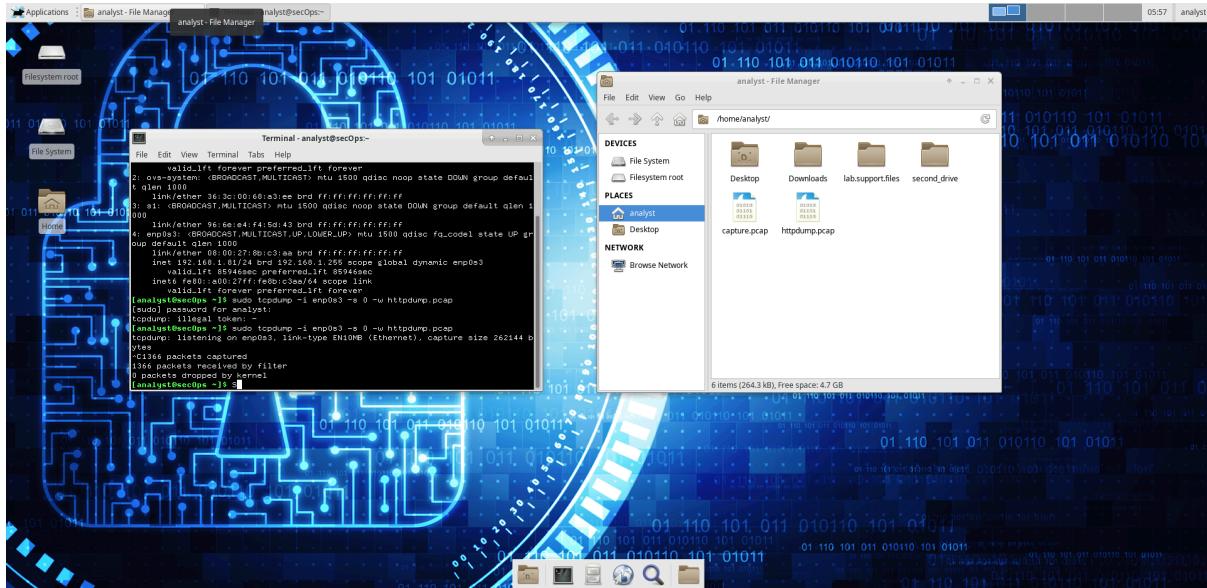


Infine mi reco nel **Cestino** per verificare se sono presenti file da eliminare, vedendo che ce ne sono, apro **PowerShell** e scrivo il comando **clear-recyclebin**, confermo con "S", e controllo nuovamente il Cestino per verificare che sia stato **svuotato correttamente**.

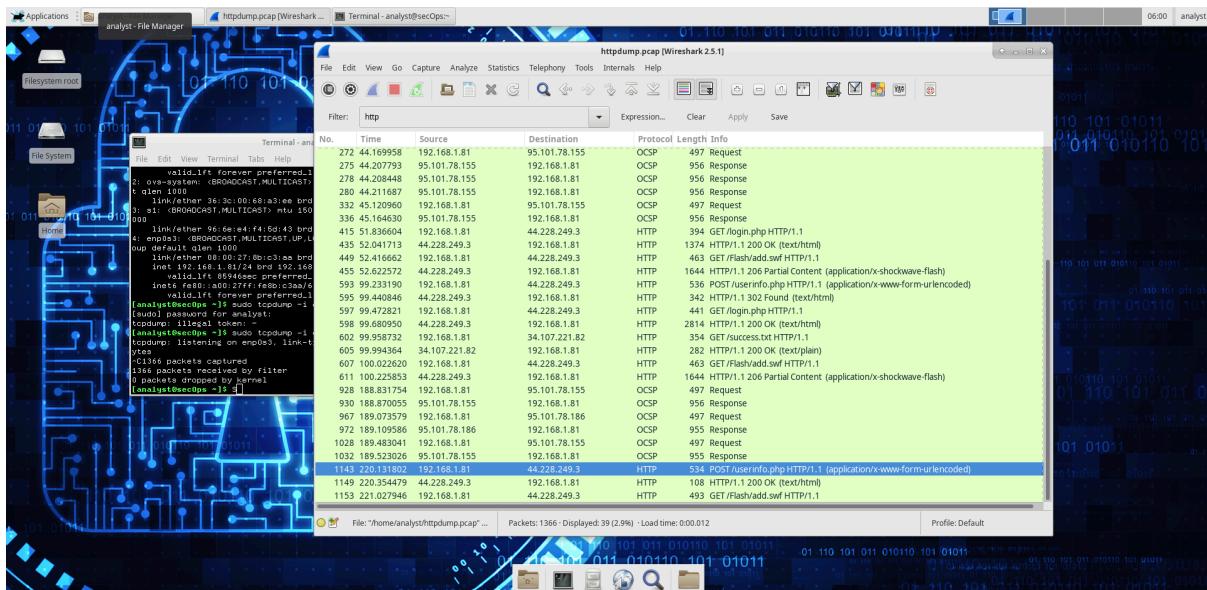
Laboratorio - Utilizzo di Wireshark per Esaminare il Traffico HTTP e HTTPS



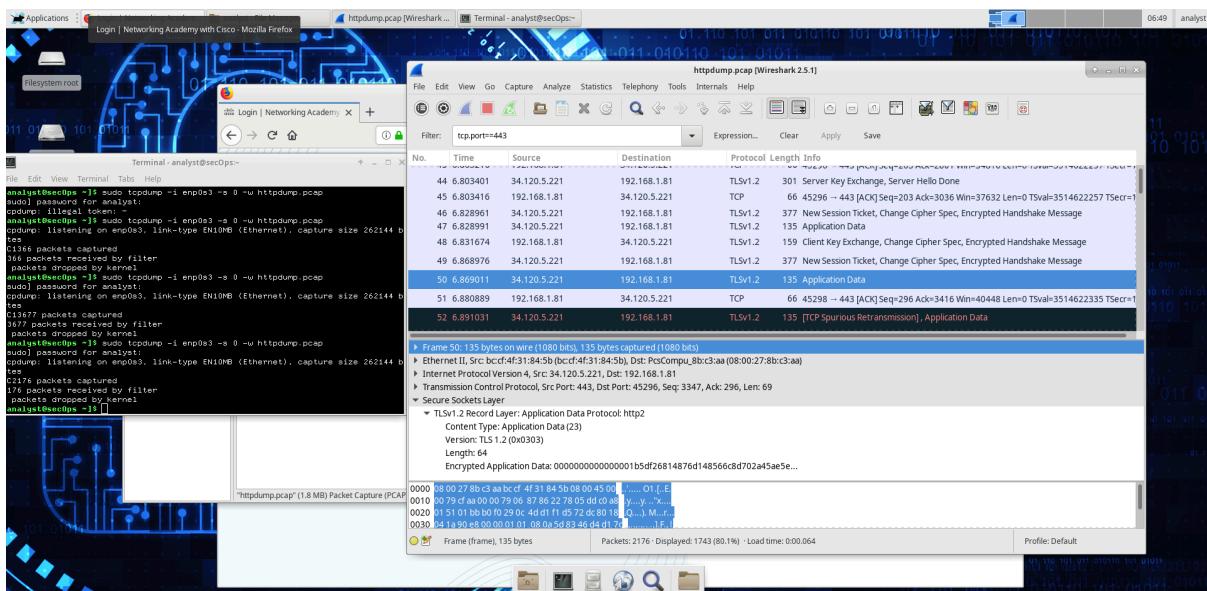
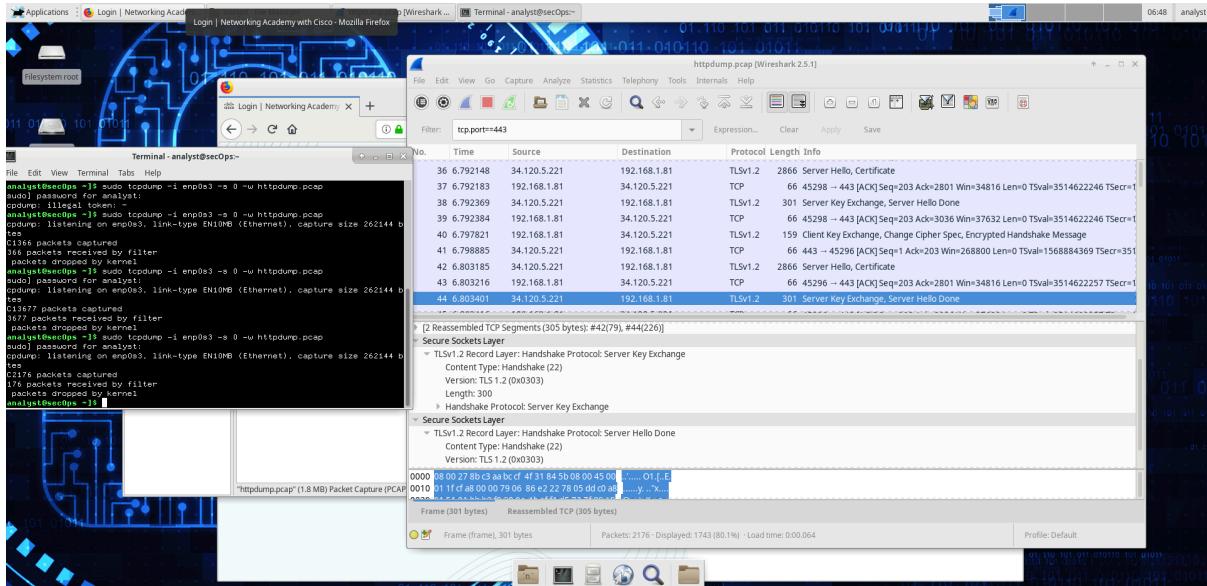
Eseguo **ipconfig** a per trovare l'interfaccia (enp0s3), poi lancio **sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap** per catturare il traffico. Apro testphp.vulnweb.com, faccio login con test/test e genero pacchetti da analizzare.



Il comando `tcpdump` ha salvato l'output nel file `httpdump.pcap`, visibile nella home dell'utente `analyst`. Apro il File Manager dal desktop, entro nella cartella `/home/analyst/`, faccio doppio clic su `httpdump.pcap`, seleziono Wireshark nella finestra "Apri con" e clicco su Apri per analizzare i pacchetti.

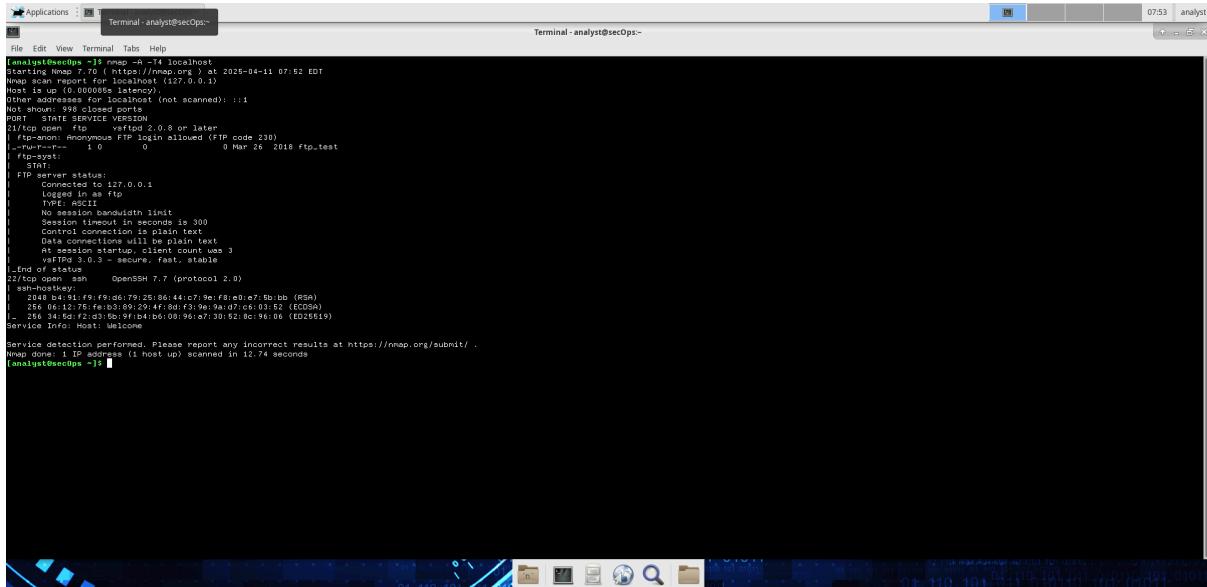


In Wireshark applico il filtro **http** e clicco su **Applica**. Scorro i pacchetti HTTP finché trovo una **richiesta POST**, la seleziono e nella finestra inferiore espando la sezione **HTML Form URL Encoded**. Qui visualizzo i dati inviati: **uname=test** e **pass=test**



Ripeto la stessa procedura, ma questa volta accedo al sito www.netacad.com. Dopo aver avviato la cattura del traffico con tcpdump, apro Wireshark e applico il filtro `tcp.port==443`, che serve per isolare il traffico cifrato HTTPS, comunemente utilizzato dai siti sicuri. Scorro i pacchetti TLS registrati e noto che, a differenza del traffico HTTP visto in precedenza (dove username e password erano in chiaro), qui il contenuto trasmesso è completamente cifrato. I dati sono visibili solo come Application Data o Handshake TLS, senza alcuna informazione leggibile come credenziali o contenuti in testo semplice. Questo dimostra l'efficacia della cifratura TLS nel proteggere le informazioni sensibili durante la trasmissione.

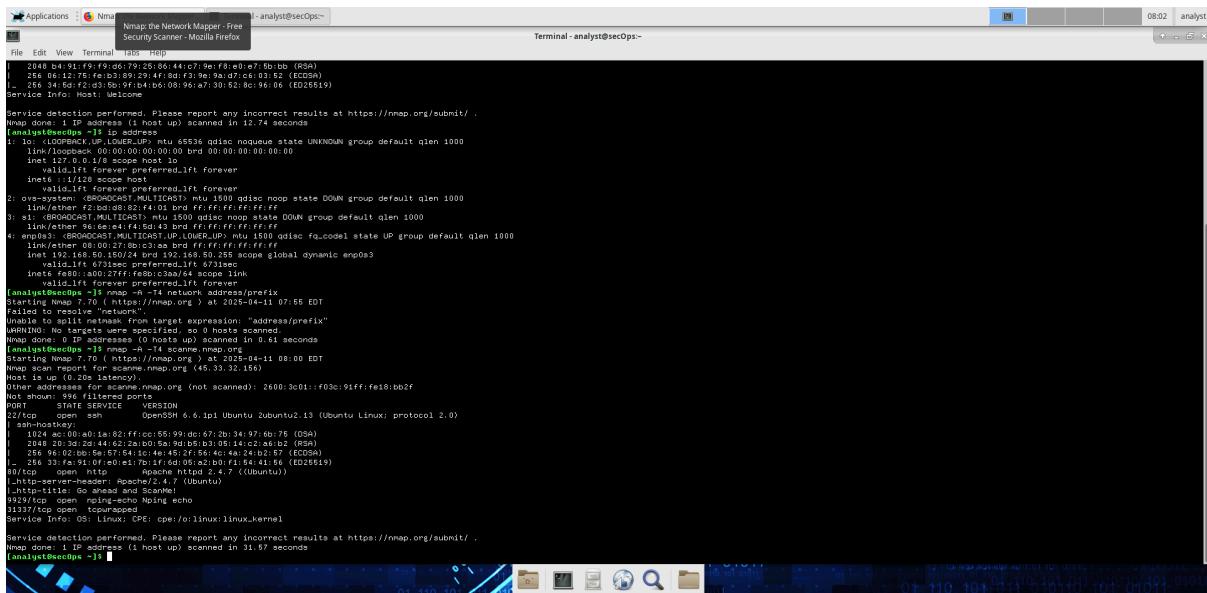
Bonus 1



```
[root@secOps ~]# nmap -A -T4 localhost
Starting Nmap 7.00 ( https://nmap.org ) at 2025-04-11 07:52 EDT
Nmap done: 1 IP address (1 host up) scanned in 0.000085s
Host is up (0.000085s latency)
Other addresses for 127.0.0.1 (not scanned): ::1
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  vsftpd  3.0.2 or later
|_vsftpd  3.0.2 Apache2.2.47 (Ubuntu)
22/tcp    open  ssh     OpenSSH 7.7 (protocol 2.0)
|_ssh-hostkey:
|   2340 b4:91:f2:00:79:25:66:44:c7:9e:f8:e0:ef:fb:bb (RSA)
|   286 06:12:76:fe:b3:89:29:4f:8d:f3:9c:ba:d7:c5:03:52 (ECDSA)
|_ 286 34:5d:f2:d3:5b:9f:bd:b6:08:96:a7:30:52:8c:96:06 (ED25519)
Service Info: Host: Welcome

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.74 seconds
[elasticsearch@secOps ~]
```

Eseguo una scansione **Nmap** con il comando `nmap -T4 localhost` per identificare le porte aperte sulla macchina locale. Il risultato mostra che sono attivi due servizi: FTP sulla porta 21 (con vsftpd 3.0.2) e SSH sulla porta 22 (con OpenSSH 7.7). Nmap fornisce anche informazioni sullo stato della connessione FTP e sulle chiavi host SSH disponibili.



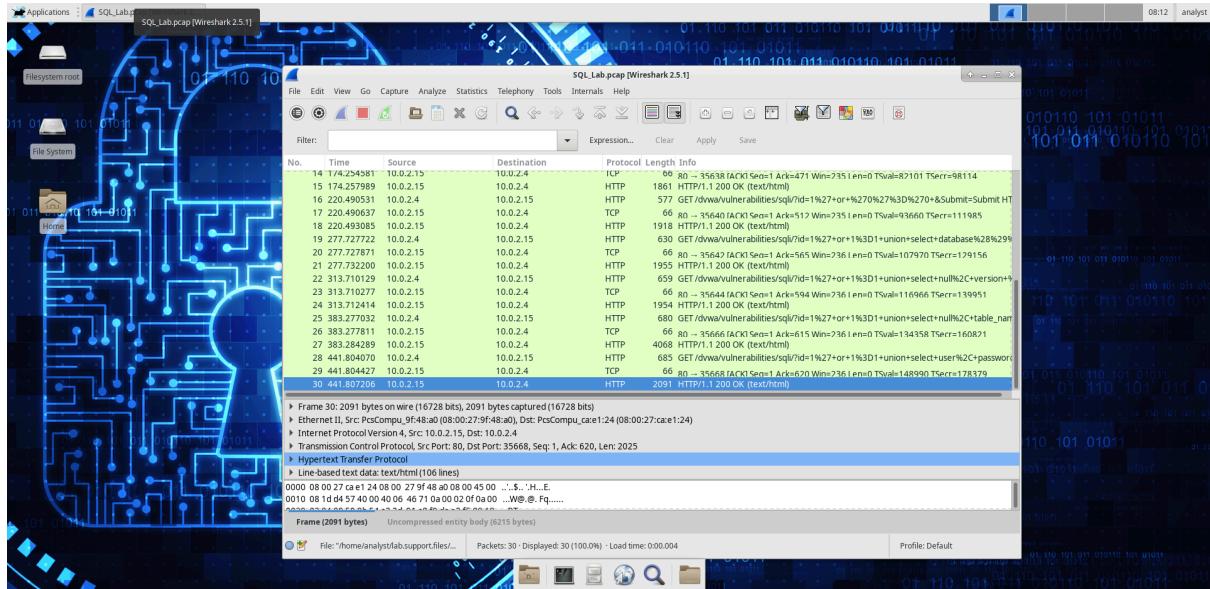
```
[root@secOps ~]# nmap -A -T4 nmap.org
Starting Nmap 7.00 ( https://nmap.org ) at 2025-04-11 08:02 EDT
Nmap done: 1 IP address (1 host up) scanned in 31.57 seconds
[elasticsearch@secOps ~]#
```

```
[root@secOps ~]# nmap -A -T4 nmap.org
Starting Nmap 7.00 ( https://nmap.org ) at 2025-04-11 08:02 EDT
Failed to resolve "nmap.org".
Nmap scan report for nmap.org (45.33.32.156)
nmap.org:0 IP addresses (0 hosts up) scanned in 0.61 seconds
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.61 seconds
Starting Nmap 7.00 ( https://nmap.org ) at 2025-04-11 08:08 EDT
Nmap scan report for scanne.nmap.org (45.33.32.156)
Host: 45.33.32.156 (Ubuntu 20.04 LTS)
Other addresses for scanne.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 8.9.1p1 Ubuntu-1ubuntu1.1 (Ubuntu; protocol 2.0)
|_ssh-hostkey:
|   1340 0a:74:52:15:4c:55:99:dc:07:20:34:97:60:75 (RSA)
|   24af 26:30:20:44:62:2a:0b:51:9d:b5:b3:05:14:c2:1xb12 (DSA)
|_ 286 96:02:bb:5e:67:54:1c:4e:45:f7:65:4c:4a:24:b2:57 (ECDSA)
|_ 286 33:00:91:0e:01:7b:01:f6:00:99:32:91:f1:94:41:96 (ED25519)
|_tcp 443/tcp https OpenSSH 8.9.1p1 Ubuntu-1ubuntu1.1 (Ubuntu)
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
|_http-x-powered-by: PHP/8.0.28
|_http-keep-alive: timeout=5, max=100
|_http-echo: 
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

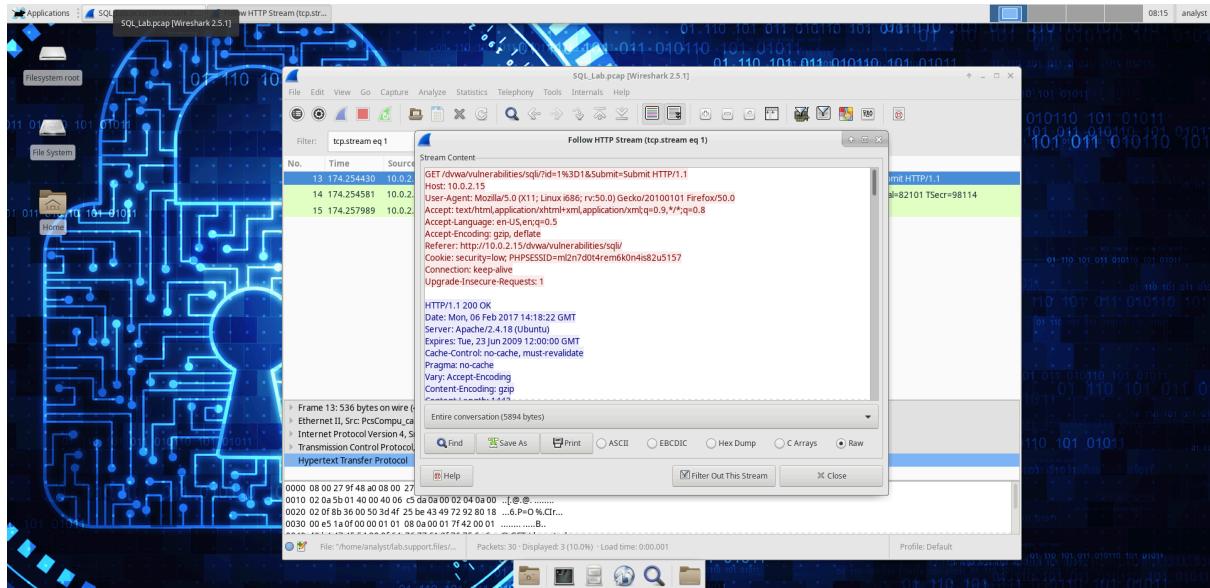
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.57 seconds
[elasticsearch@secOps ~]
```

Eseguo una scansione con **nmap -A -T4 nmap.org** per analizzare il dominio ufficiale. Nmap rileva che le porte aperte sono la 22 per SSH, la 80 per HTTP e la 443 per HTTPS. Vengono identificati i servizi attivi come OpenSSH e Apache, con le rispettive versioni. La scansione fornisce anche informazioni sul sistema operativo e sulle chiavi pubbliche del server SSH.

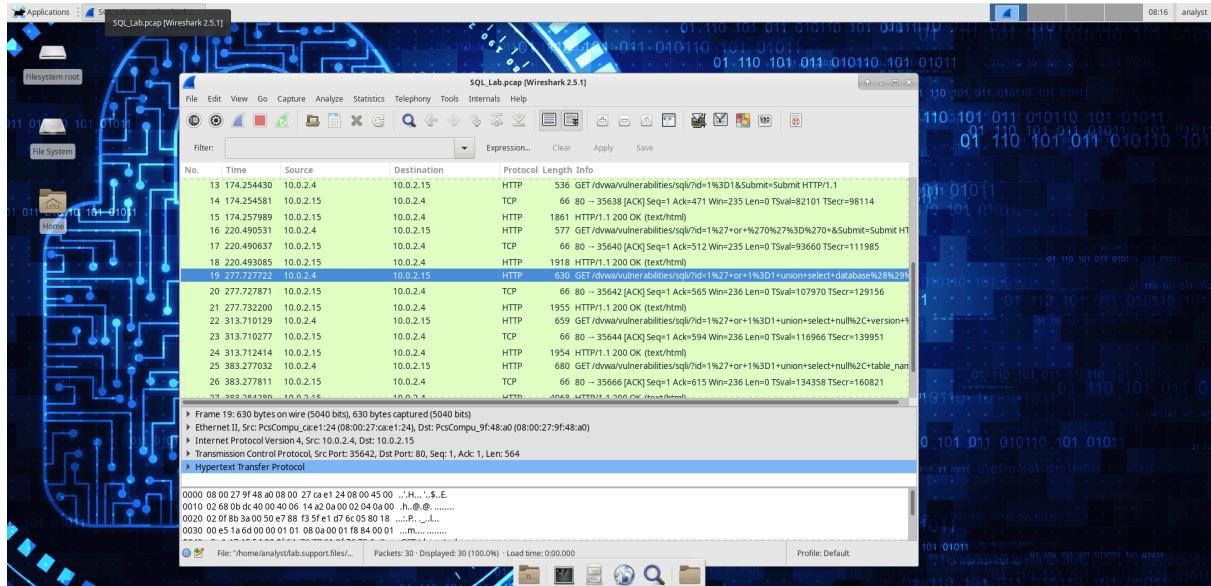
Bonus 2



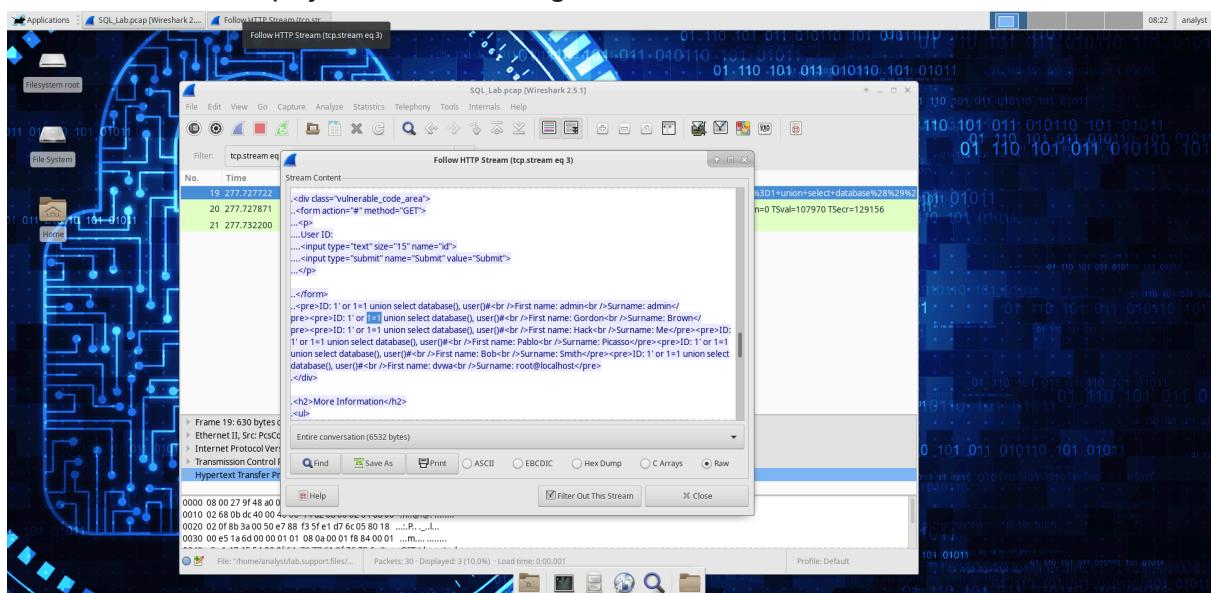
Apro Wireshark e carico il file **SQL_Lab.pcap**. Questo file contiene il traffico registrato durante una sessione in cui è stato eseguito un attacco **SQL Injection** su un'applicazione vulnerabile.



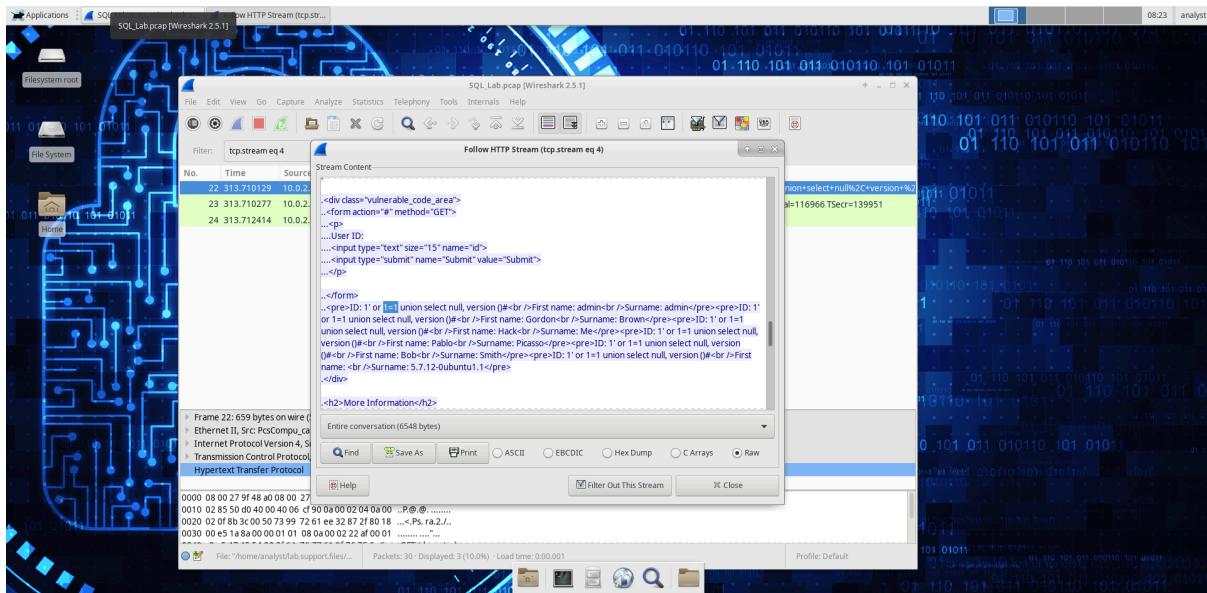
Applico il filtro HTTP e visualizzo le richieste inviate dal client al server. In particolare, osservo una richiesta GET verso la pagina **dvwa/vulnerabilities/sql?id=1%3D1&Submit=Submit**, che rappresenta un tentativo iniziale di SQL Injection.



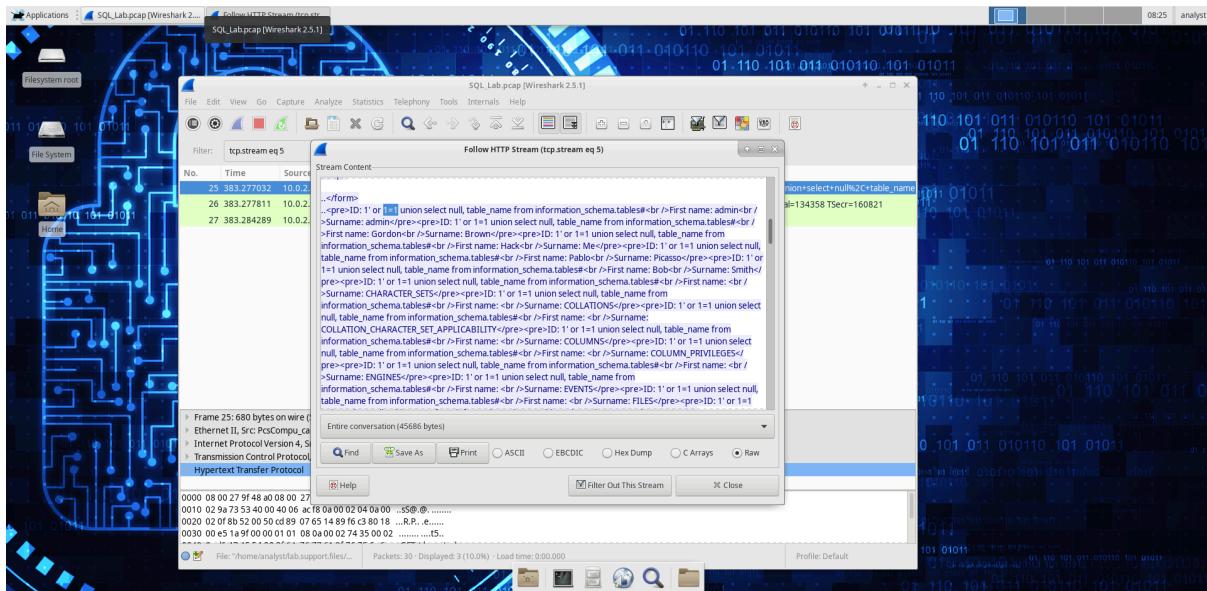
Il flusso continua con query più complesse, come **union select+database()**, che cerca di esfiltrare il nome del database attivo. La risposta HTML mostra chiaramente che il payload è stato eseguito con successo.



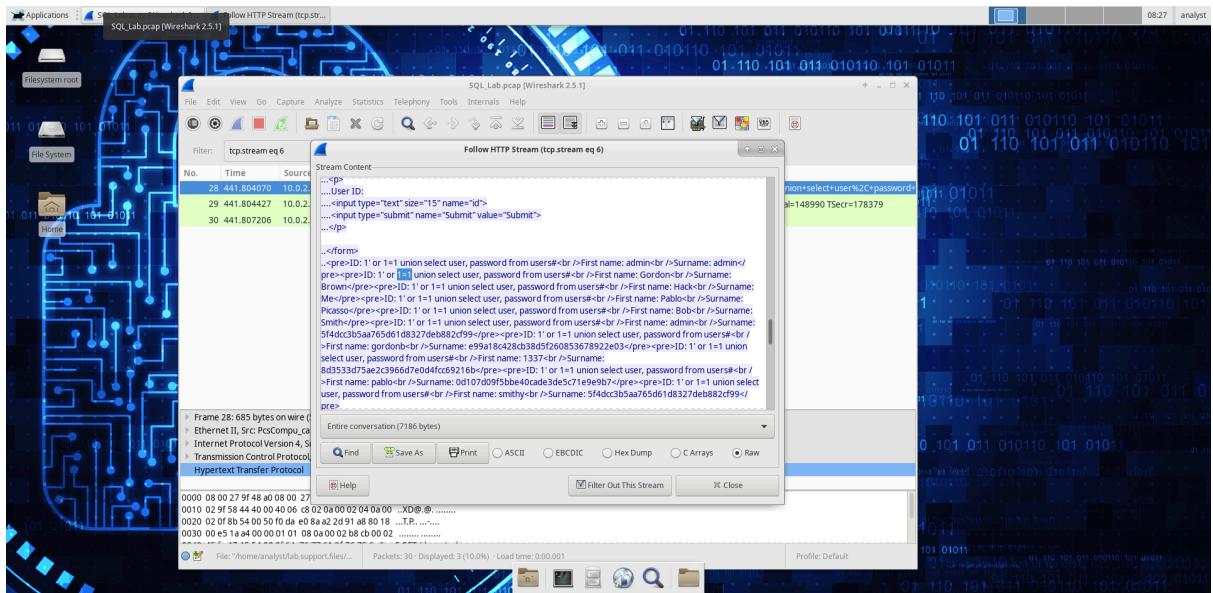
In questa fase viene usato il comando **union select null, version()** per ottenere la **versione del DBMS**. L'output della risposta rivela che si tratta di **MySQL 5.7.12 su Ubuntu**.



La SQL Injection continua, ora l'obiettivo è accedere alla struttura interna del database. Il payload `union select null, table_name from information_schema.tables` permette di elencare i nomi delle tabelle presenti nel database, dimostrando un'escalation del livello di attacco.



Infine, l'attacco si conclude con l'estrazione di **dati sensibili** dalla tabella **users**. Viene utilizzato **union select user, password from users** e tra i risultati compaiono nomi utenti e **password hashate**, segno evidente di un attacco riuscito.



Tutti i dati vengono visualizzati all'interno della funzione **Follow TCP Stream**, che consente di ricostruire l'intera conversazione HTTP. In questo modo ho potuto osservare l'attacco SQL Injection in tutte le sue fasi: dall'iniezione iniziale fino all'estrazione di dati sensibili.