# PF30-PF60 Didattica e Laboratorio di Reti di Elaboratori Lezione -3- TOOLS

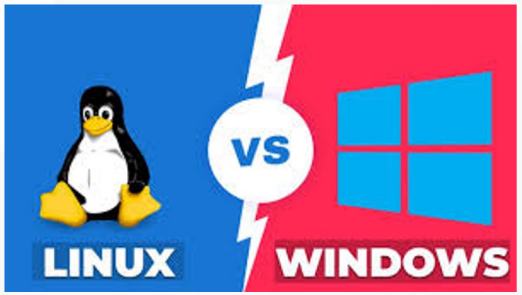
Fausto Marcantoni

fausto.marcantoni@unicam.it

# tools

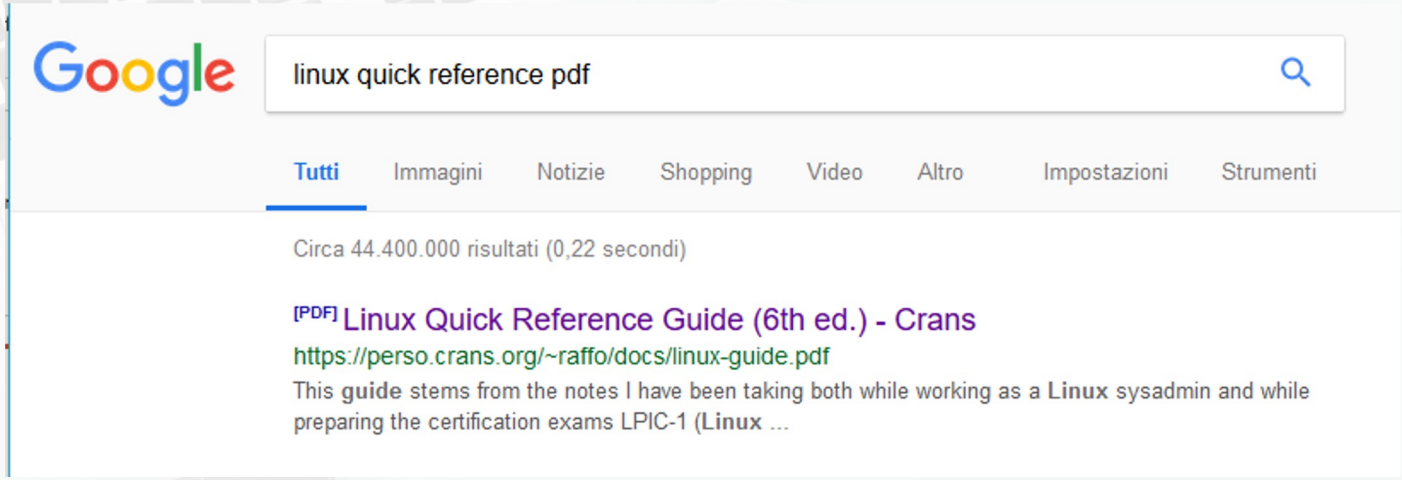
| TOOLS - Laboratorio - | | |
|---|---|---|
| Linux - Windows<br>shell<br>PowerShell | | |
| Wireshark | | |
| Nmap | | |
| Vmware - VirtualBox<br>Metasploitable2<br>Apache<br>Webmin<br><br>Nessus<br>Greenbone-openvas | Firewall | |
| | Pfsense | |
| | OPNsense | https://opnsense.org/ |
| | Ipcop | https://www.ipcop.org/ |
| | Ipfire | https://www.ipfire.org/ |
| GNS3 | | |
| Draw io<br>• https://www.drawio.com/<br>• https://github.com/jgraph/drawio-desktop/releases | | |
| | | |

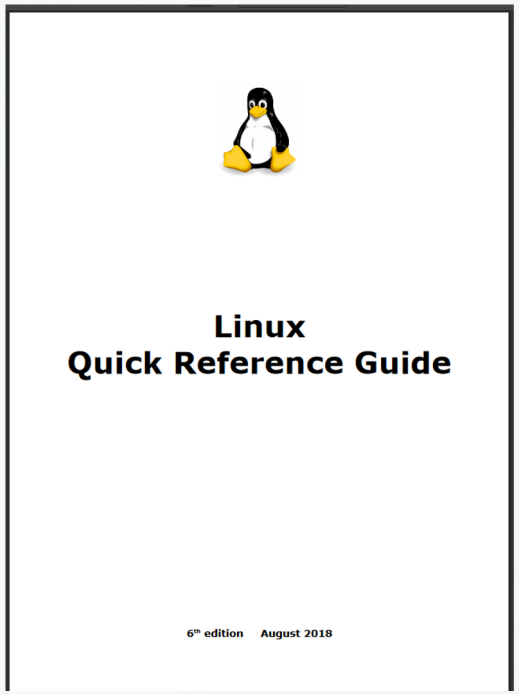
# Linux vs Windows



# Linux

un buon manuale per iniziare




https://dr0.ch/docs/linux-guide-8ed.pdf

# powershell

**Che cos'è PowerShell?**

https://learn.microsoft.com/it-it/powershell/scripting/overview?view=powershell-7.4

https://learn.microsoft.com/it-it/training/modules/introduction-to-powershell/

https://thesolving.com/it/sala-server/powershell-una-guida-completa-parte-1a/

C:\Users\studente\AppData\R

```
PS C:\Users\studente> $PSVersionTable

Name                           Value
----                           -----
PSVersion                      5.1.22621.1778
PSEdition                      Desktop
PSCompatibleVersions           {1.0, 2.0, 3.0, 4.0...}
BuildVersion                   10.0.22621.1778
CLRVersion                     4.0.30319.42000
WSManStackVersion              3.0
PSRemotingProtocolVersion      2.3
SerializationVersion           1.1.0.1


PS C:\Users\studente>
```

https://learn.microsoft.com/it-it/training/browse/

**Come installare Linux in Windows con WSL**

https://learn.microsoft.com/it-it/windows/wsl/install

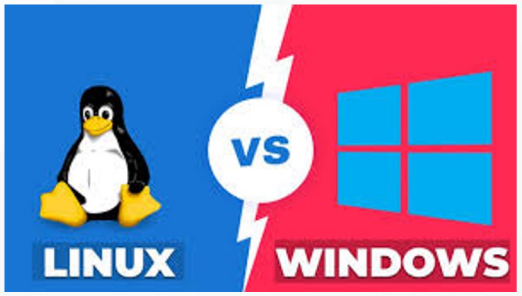
```
wsl --install

wsl --list --online o wsl -l -o

wsl.exe --install -d <Distribution Name>
```

**ma perché?!?!?!**

**Installare e iniziare a configurare Terminale Windows**

https://learn.microsoft.com/it-it/windows/terminal/install

# FINE



# Wireshark

https://www.wireshark.org/

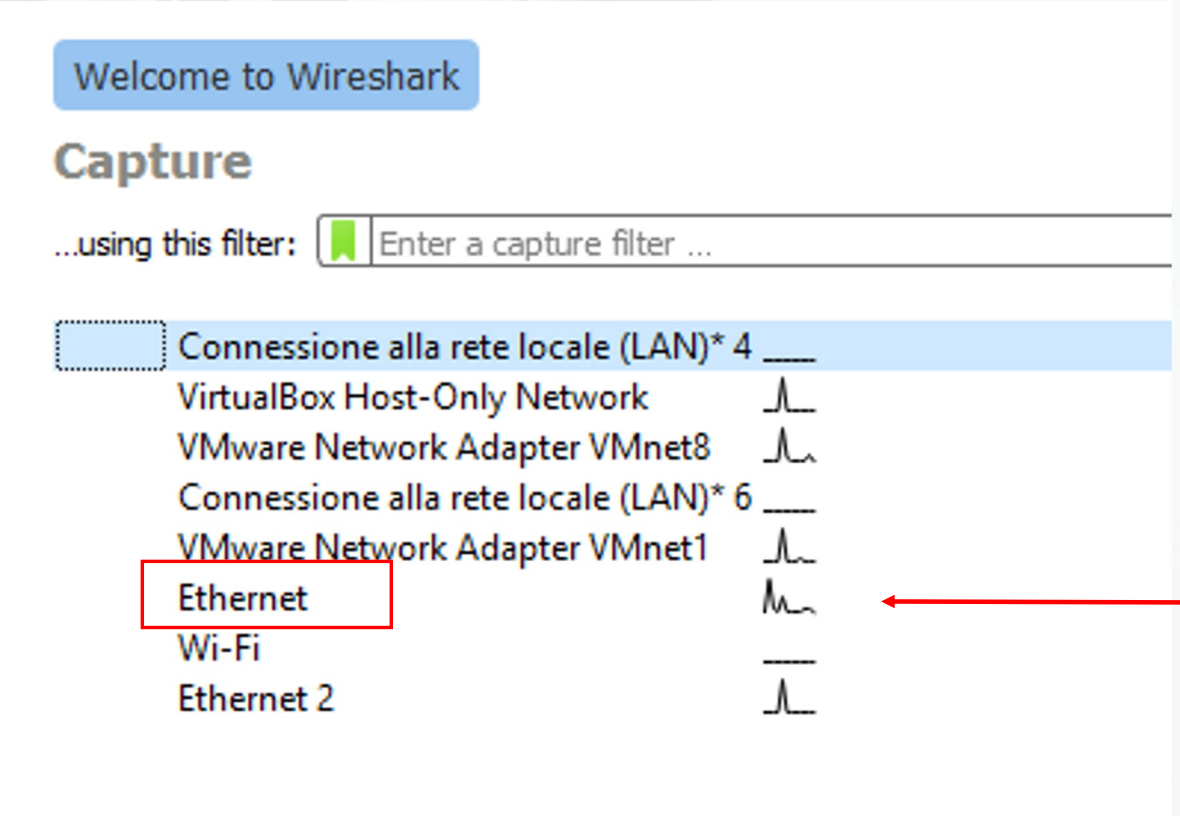
Tutorial e manuali

**https://www.wireshark.org/docs/wsug_html_chunked/**

https://imolug.org/sites/default/files/WireShark_Manual.pdf
http://security.polito.it/~lioy/01nbe/wireshark_intro.pdf
https://www.areanetworking.it/corso-wireshark-prima-lezione.html

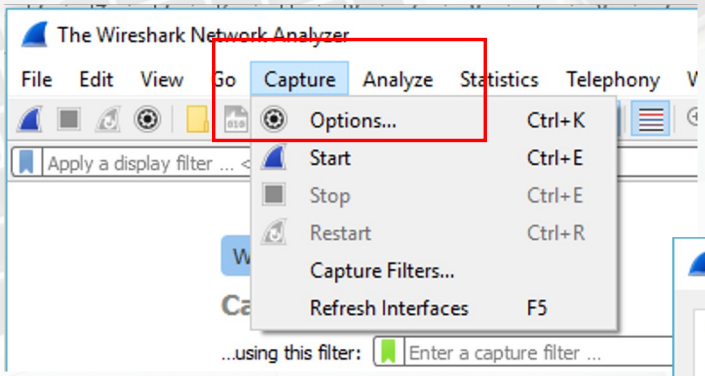
https://www.lifewire.com/wireshark-tutorial-4143298
https://www.guru99.com/wireshark-passwords-sniffer.html

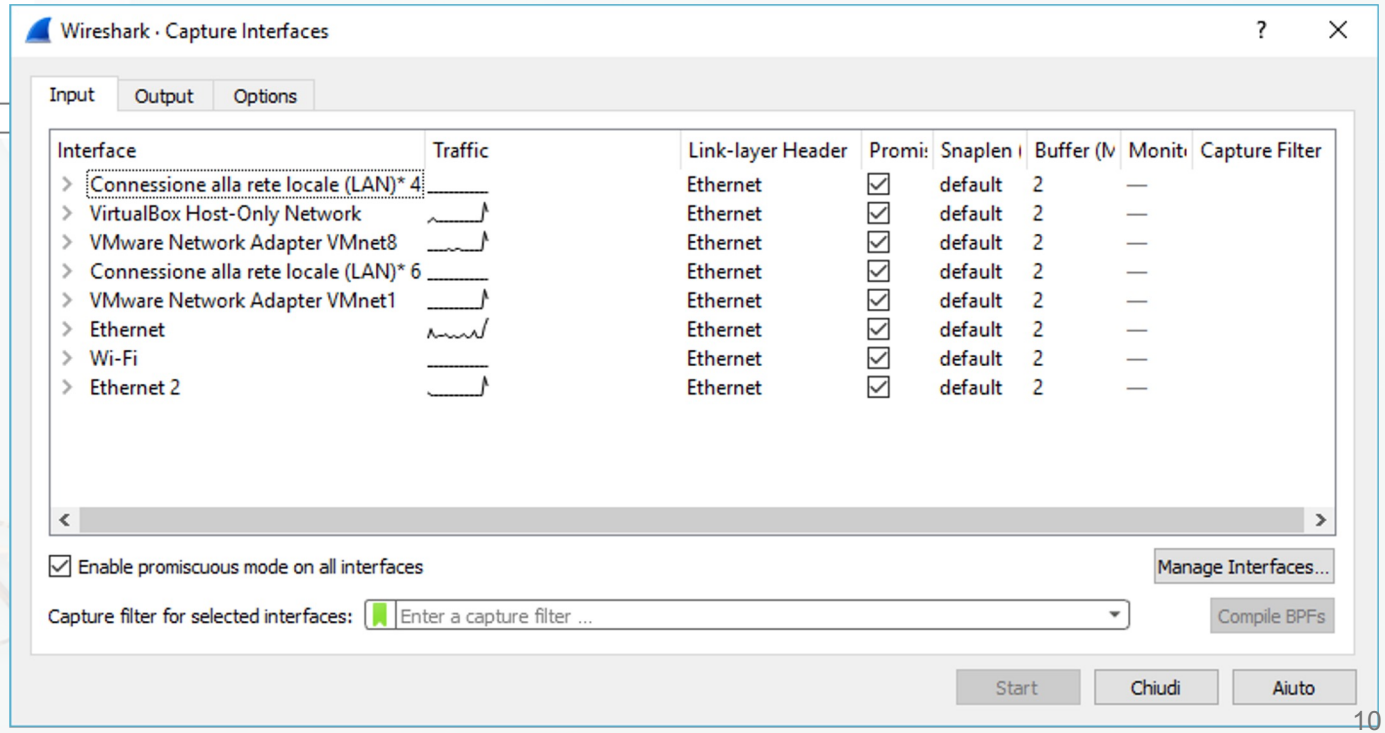
# Wireshark – scegliere l'interfaccia



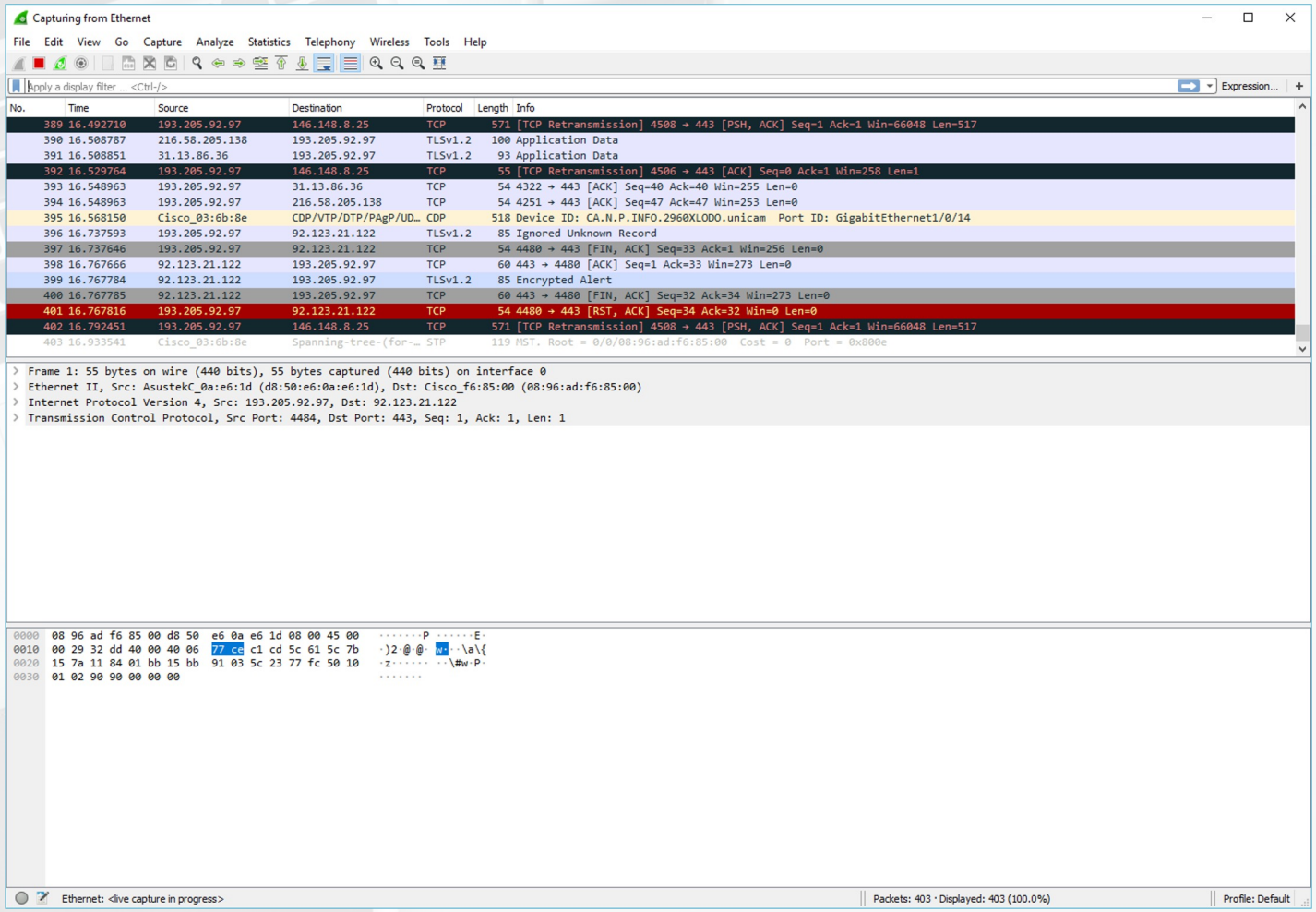

Vedere il traffico

# Wireshark – scegliere l'interfaccia



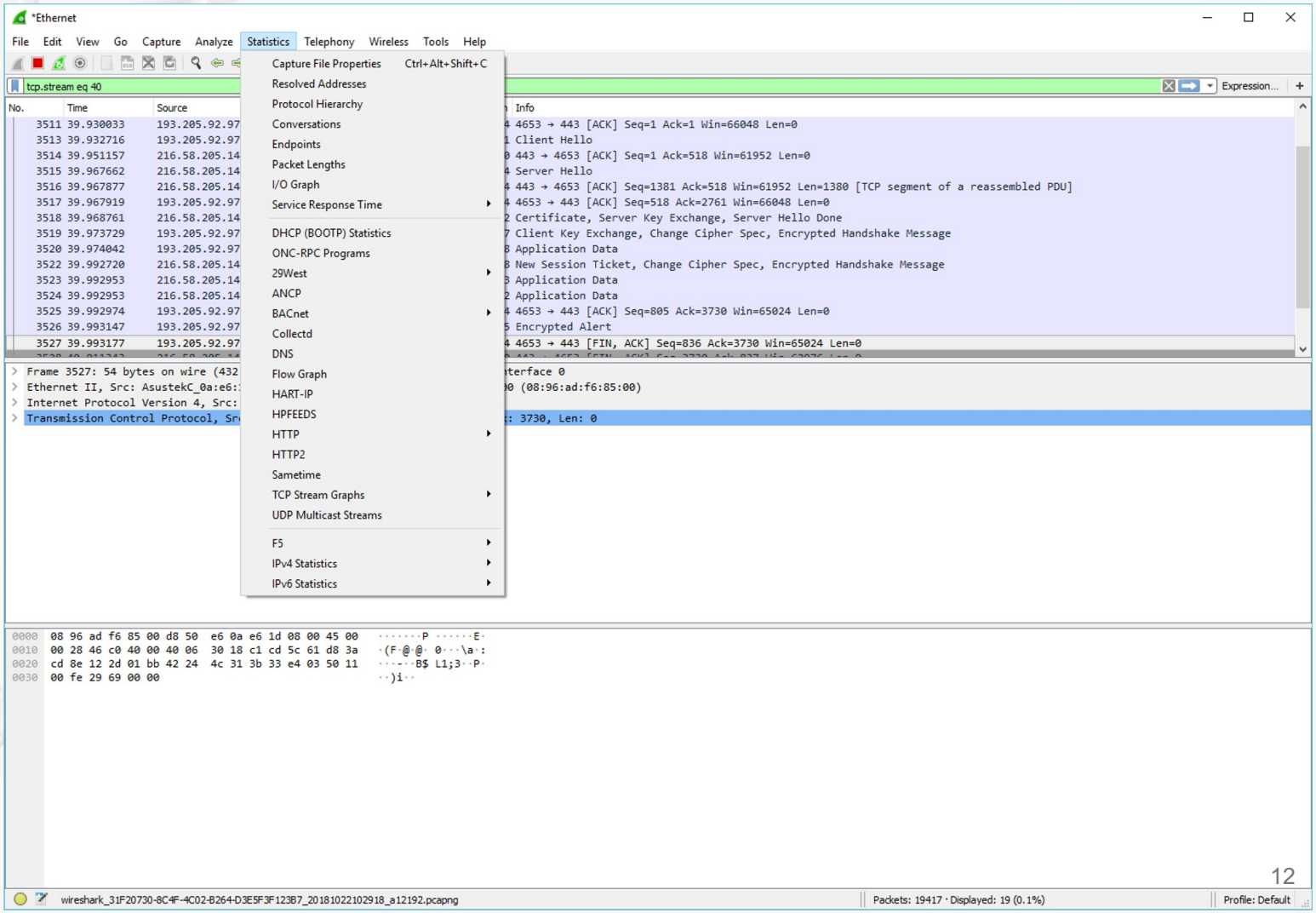
# Wireshark – pagina principale



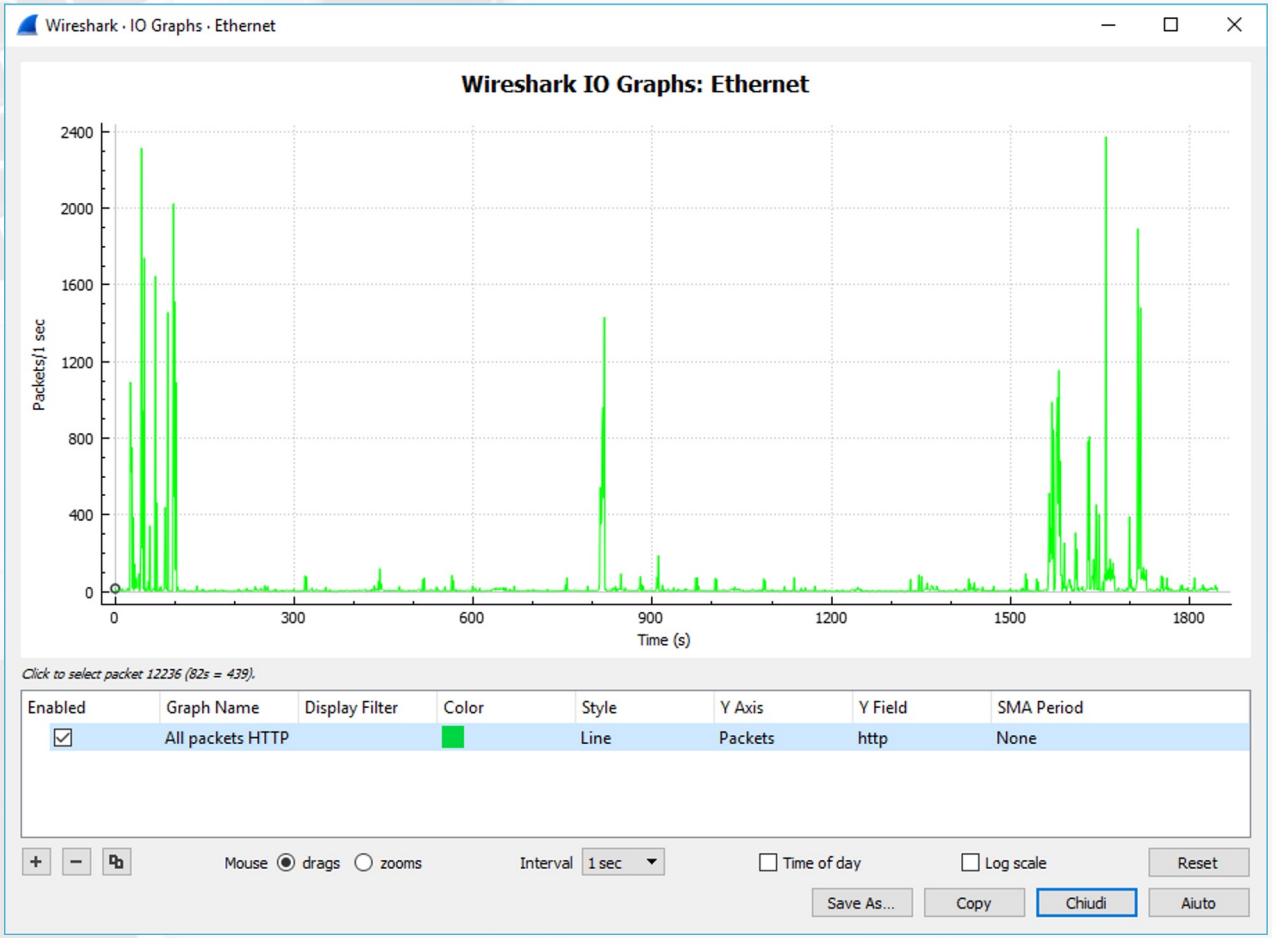
# Wireshark – Statistiche

Statistics | Telephony | Wireless | Tools | Help

- Capture File Properties — Ctrl+Alt+Shift+C
- Resolved Addresses
- Protocol Hierarchy
- Conversations
- Endpoints
- Packet Lengths
- I/O Graph
- Service Response Time ▸
- DHCP (BOOTP) Statistics
- ONC-RPC Programs
- 29West ▸
- ANCP
- BACnet ▸
- Collectd
- DNS
- Flow Graph
- HART-IP
- HPFEEDS
- HTTP ▸
- HTTP2
- Sametime
- TCP Stream Graphs ▸
- UDP Multicast Streams
- F5 ▸
- IPv4 Statistics ▸
- IPv6 Statistics ▸



# Wireshark – Statistiche - I/O Graph



# Wireshark – Statistiche - Conversation

Wireshark · Conversations · Ethernet

Ethernet · 170 | IPv4 · 198 | IPv6 · 29 | TCP · 199 | UDP · 541

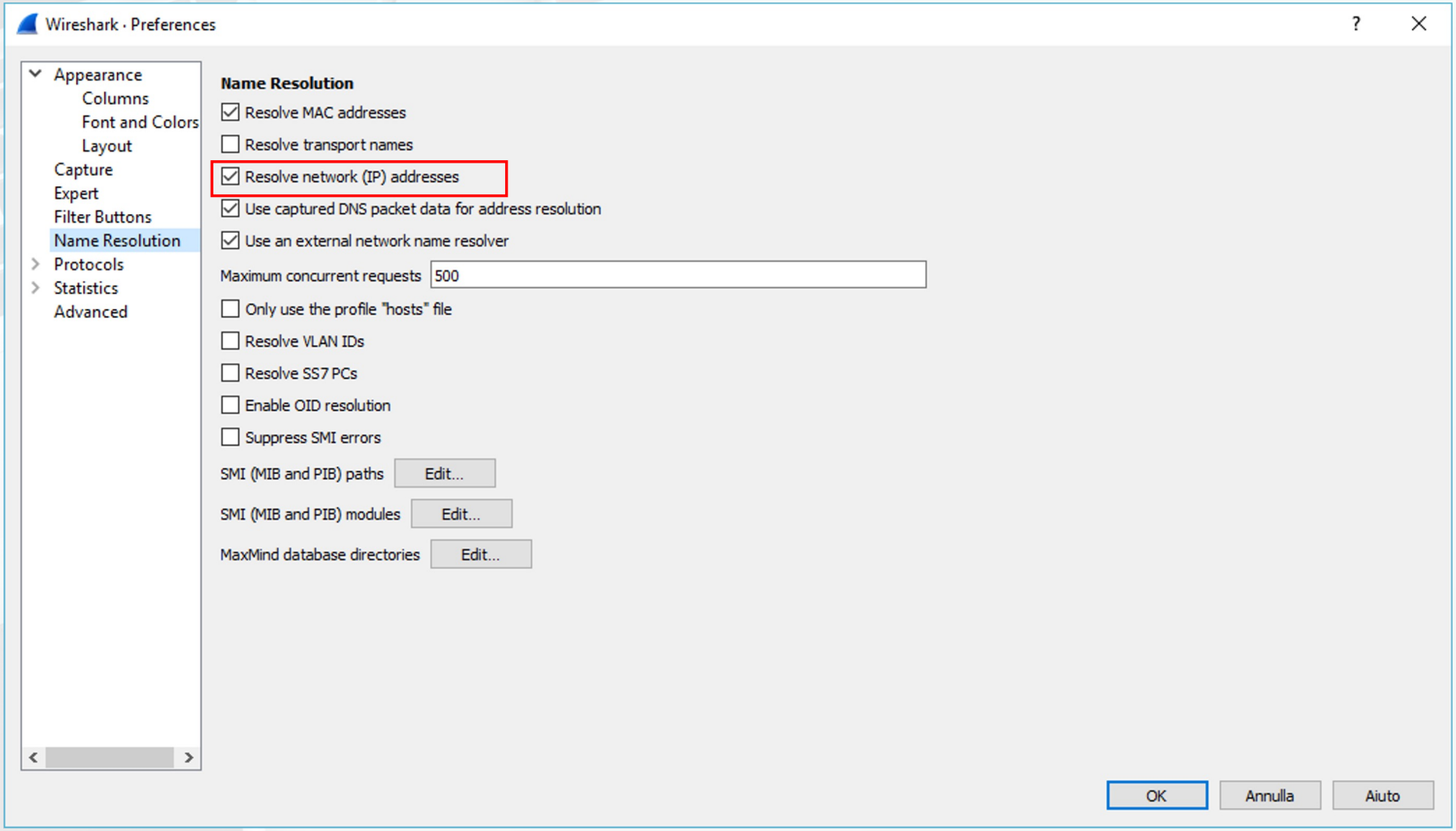
| Address A | Address B | Packets | Bytes | Packets A → B | Bytes A → B | Packets B → A | Bytes B → A | Rel Start | Duration | Bits/s A → B | Bits/s B → A |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0.0.0.0 | 255.255.255.255 | 3 | 1068 | 3 | 1068 | 0 | 0 | 1358.92528 | 0.0664 | 128 k | 0 |
| 2.237.133.169 | 193.205.92.124 | 1 | 66 | 1 | 66 | 0 | 0 | 1040.14386 | 0.0000 | — | — |
| 10.1.0.111 | 193.205.92.164 | 1 | 66 | 1 | 66 | 0 | 0 | 1643.93582 | 0.0000 | — | — |
| 13.107.5.88 | 193.205.92.97 | 28 | 9032 | 14 | 7438 | 14 | 1594 | 254.819504 | 67.5835 | 880 | 188 |
| 23.1.75.203 | 193.205.92.131 | 9 | 811 | 9 | 811 | 0 | 0 | 281.927049 | 13.3721 | 485 | 0 |
| 23.13.61.84 | 193.205.92.97 | 14 | 5645 | 8 | 5096 | 6 | 549 | 221.508485 | 3.6941 | 11 k | 1188 |
| 31.13.86.4 | 193.205.92.97 | 2.906 | 2634 k | 2.092 | 2557 k | 814 | 76 k | 1576.55572 | 208.7664 | 98 k | 2914 |
| 31.13.86.8 | 193.205.92.97 | 381 | 128 k | 165 | 30 k | 216 | 97 k | 1581.19598 | 246.0368 | 1002 | 3167 |
| 31.13.86.15 | 193.205.92.97 | 8.935 | 10 M | 7.438 | 10 M | 1.497 | 110 k | 1630.63330 | 164.1474 | 503 k | 5386 |
| 31.13.86.36 | 193.205.92.97 | 1.284 | 861 k | 751 | 652 k | 533 | 209 k | 1575.06985 | 270.1891 | 19 k | 6196 |
| 31.14.131.188 | 193.205.92.27 | 1 | 90 | 1 | 90 | 0 | 0 | 1054.58187 | 0.0000 | — | — |
| 35.163.53.118 | 193.205.92.97 | 6 | 452 | 2 | 170 | 4 | 282 | 102.209889 | 0.1946 | 6990 | 11 k |
| 37.77.114.151 | 193.205.92.67 | 1 | 66 | 1 | 66 | 0 | 0 | 1086.90181 | 0.0000 | — | — |
| 40.67.251.132 | 193.205.92.97 | 95 | 11 k | 32 | 5760 | 63 | 5705 | 41.479365 | 1800.0972 | 25 | 25 |
| 40.70.184.83 | 193.205.92.97 | 37 | 15 k | 15 | 12 k | 22 | 2962 | 539.240421 | 914.6945 | 109 | 25 |
| 40.77.226.249 | 193.205.92.97 | 24 | 8442 | 10 | 7070 | 14 | 1372 | 1471.44068 | 95.3014 | 593 | 115 |
| 52.11.162.210 | 193.205.92.97 | 26 | 11 k | 10 | 4180 | 16 | 7626 | 102.661996 | 0.8051 | 41 k | 75 k |
| 52.54.248.107 | 193.205.92.138 | 11 | 1078 | 11 | 1078 | 0 | 0 | 1576.56089 | 160.0151 | 53 | 0 |
| 52.114.158.91 | 193.205.92.97 | 17 | 7329 | 8 | 4655 | 9 | 2674 | 954.706102 | 0.9574 | 38 k | 22 k |
| 52.138.216.83 | 193.205.92.97 | 77 | 25 k | 34 | 21 k | 43 | 4170 | 249.746002 | 503.0874 | 341 | 66 |
| 54.38.180.81 | 193.205.92.112 | 2 | 140 | 2 | 140 | 0 | 0 | 475.550582 | 0.0246 | 45 k | 0 |
| 54.187.46.234 | 193.205.92.97 | 24 | 1474 | 12 | 818 | 12 | 656 | 0.332218 | 40.3812 | 162 | 129 |
| 54.201.6.28 | 193.205.92.97 | 10 | 598 | 5 | 325 | 5 | 273 | 6.592993 | 30.4884 | 85 | 71 |
| 54.210.203.205 | 193.205.92.138 | 11 | 1078 | 11 | 1078 | 0 | 0 | 1576.18391 | 160.2319 | 53 | 0 |
| 60.191.38.77 | 193.205.92.117 | 2 | 120 | 2 | 120 | 0 | 0 | 541.862935 | 1.3591 | 706 | 0 |
| 64.233.166.94 | 193.205.92.97 | 303 | 281 k | 202 | 275 k | 101 | 6185 | 27.595445 | 16.1797 | 136 k | 3058 |
| 64.233.166.154 | 193.205.92.97 | 49 | 8921 | 27 | 5950 | 22 | 2971 | 1576.14812 | 259.3192 | 183 | 91 |
| 64.233.166.189 | 193.205.92.131 | 10 | 1164 | 10 | 1164 | 0 | 0 | 8.126912 | 29.9172 | 311 | 0 |
| 64.233.166.189 | 193.205.92.79 | 1 | 105 | 1 | 105 | 0 | 0 | 1089.85023 | 0.0000 | — | — |
| 64.233.166.189 | 193.205.92.138 | 12 | 1512 | 12 | 1512 | 0 | 0 | 1565.74641 | 120.8466 | 100 | 0 |
| 64.233.166.189 | 193.205.92.97 | 362 | 65 k | 212 | 40 k | 150 | 24 k | 1581.20582 | 260.6950 | 1253 | 744 |

☐ Name resolution ☐ Limit to display filter ☐ Absolute start time

Conversation Types

Copy | Follow Stream... | Graph... | Chiudi | Aiuto

# Wireshark – Preferences



# Wireshark – Statistiche - Conversation

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 21 | 3.867041 | mfausto.amministraz… | a1089.d.akamai.net | HTTP | 55 | Continuation |
| 22 | 3.880216 | a1089.d.akamai.net | mfausto.amministraz… | TCP | 66 | 80 → 4608 [ACK] Seq=1 Ack=2 Win=237 Len=0 SLE=1 SRE=2 |
| 68 | 13.879620 | mfausto.amministraz… | a1089.d.akamai.net | TCP | 55 | [TCP Keep-Alive] 4608 → 80 [ACK] Seq=1 Ack=1 Win=257 |
| 69 | 13.892694 | a1089.d.akamai.net | mfausto.amministraz… | TCP | 66 | [TCP Keep-Alive ACK] 80 → 4608 [ACK] Seq=1 Ack=2 Win= |
| 129 | 23.892990 | mfausto.amministraz… | a1089.d.akamai.net | TCP | 55 | [TCP Keep-Alive] 4608 → 80 [ACK] Seq=1 Ack=1 Win=257 |
| 130 | 23.905880 | a1089.d.akamai.net | mfausto.amministraz… | TCP | 66 | [TCP Keep-Alive ACK] 80 → 4608 [ACK] Seq=1 Ack=2 Win= |
| 3276 | 33.808070 | mfausto.amministraz… | a1089.d.akamai.net | HTTP | 373 | GET /success.txt HTTP/1.1 |
| 3288 | 33.821166 | a1089.d.akamai.net | mfausto.amministraz… | TCP | 60 | 80 → 4608 [ACK] Seq=1 Ack=321 Win=245 Len=0 |
| 3289 | 33.821469 | a1089.d.akamai.net | mfausto.amministraz… | HTTP | 438 | HTTP/1.1 200 OK (text/plain) |
| 3291 | 33.862894 | mfausto.amministraz… | a1089.d.akamai.net | TCP | 54 | 4608 → 80 [ACK] Seq=321 Ack=385 Win=255 Len=0 |

```
> Frame 3289: 438 bytes on wire (3504 bits), 438 bytes captured (3504 bits) on interface 0
> Ethernet II, Src: Cisco_f6:85:00 (08:96:ad:f6:85:00), Dst: mfausto.amministrazione.unicam (d8:50:e6:0a:e6:1d)
> Internet Protocol Version 4, Src: a1089.d.akamai.net (193.206.135.170), Dst: mfausto.amministrazione.unicam (193.205.92.97)
> Transmission Control Protocol, Src Port: 80, Dst Port: 4608, Seq: 1, Ack: 321, Len: 384
> Hypertext Transfer Protocol
> Line-based text data: text/plain (1 lines)
```

```
0000  d8 50 e6 0a e6 1d 08 96  ad f6 85 00 08 00 45 00   ·P····· ·····E·
0010  01 a8 86 dc 40 00 3b 06  4f cc c1 ce 87 aa c1 cd   ····@·;· O·····
0020  5c 61 00 50 12 00 c0 1e  e7 fc c8 28 60 41 50 18   \a·P···· ···(`AP·
0030  00 f5 be a9 00 00 48 54  54 50 2f 31 2e 31 20 32   ·····HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 43  6f 6e 74 65 6e 74 2d 54   00 OK··C ontent-T
0050  79 70 65 3a 20 74 65 78  74 2f 70 6c 61 69 6e 0d   ype: tex t/plain·
0060  0a 43 6f 6e 74 65 6e 74  2d 4c 65 6e 67 74 68 3a   ·Content -Length:
0070  20 38 0d 0a 4c 61 73 74  2d 4d 6f 64 69 66 69 65    8··Last -Modifie
0080  64 3a 20 4d 6f 6e 2c 20  31 35 20 4d 61 79 20 32   d: Mon,  15 May 2
0090  30 31 37 20 31 38 3a 30  34 3a 34 30 20 47 4d 54   017 18:0 4:40 GMT
00a0  0d 0a 45 54 61 67 3a 20  22 61 65 37 38 30 35 38   ··ETag:  "ae78058
00b0  35 66 34 39 62 39 34 63  65 31 34 34 34 65 62 37   5f49b94c e1444eb7
00c0  64 32 38 39 30 36 31 32  33 22 0d 0a 41 63 63 65   d2890612 3"··Acce
00d0  70 74 2d 52 61 6e 67 65  73 3a 20 62 79 74 65 73   pt-Range s: bytes
```

wireshark_31F20730-8C4F-4C02-B264-D3E5F3F123B7_20181022102918_a12192.pcapng | Packets: 62145 · Displayed: 13 (0.0%) · Dropped: 0 (0.0%) | Profile: Default

| Source | Destination | Protocol |
|---|---|---|
| mfausto.amministraz… | a1089.d.akamai.net | HTTP |
| a1089.d.akamai.net | mfausto.amministraz… | TCP |
| mfausto.amministraz… | a1089.d.akamai.net | TCP |
| a1089.d.akamai.net | mfausto.amministraz… | TCP |
| mfausto.amministraz… | a1089.d.akamai.net | TCP |
| a1089.d.akamai.net | mfausto.amministraz… | TCP |
| mfausto.amministraz… | a1089.d.akamai.net | HTTP |
| a1089.d.akamai.net | mfausto.amministraz… | TCP |
| a1089.d.akamai.net | mfausto.amministraz… | HTTP |
| mfausto.amministraz… | a1089.d.akamai.net | TCP |

# Wireshark – Statistiche - Conversation

Wireshark · Conversations · Ethernet

Ethernet · 170 | IPv4 · 198 | IPv6 · 29 | TCP · 199 | UDP · 541

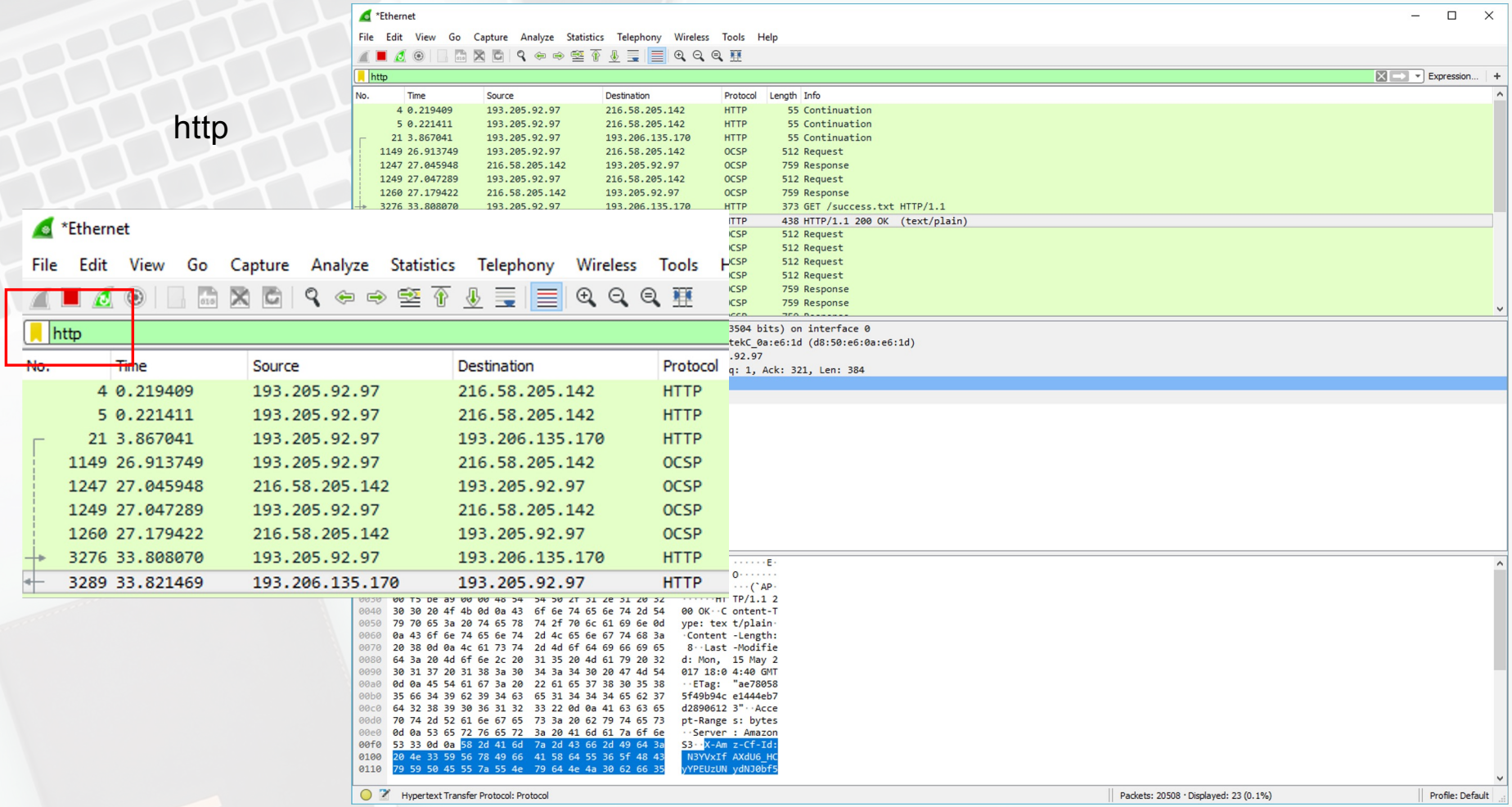
| Address A | Address B | Packets | Bytes | Packets A → B | Bytes A → B | Packets |
|---|---|---|---|---|---|---|
| 0.0.0.0 | 255.255.255.255 | 3 | 1068 | 3 | 1068 | |
| 2.237.133.169 | 4helix.amministrazione.unicam | 1 | 66 | 1 | 66 | |
| 10.1.0.111 | 193.205.92.164 | 1 | 66 | 1 | 66 | |
| e-0009.e-msedge.net | mfausto.amministrazione.unicam | 28 | 9032 | 14 | 7438 | |
| a23-1-75-203.deploy.static.akamaitechnologies.com | fabriziounicam.local | 9 | 811 | 9 | 811 | |
| e15275.g.akamaiedge.net | mfausto.amministrazione.unicam | 14 | 5645 | 8 | 5096 | |
| scontent-mxp1-1.xx.fbcdn.net | mfausto.amministrazione.unicam | 2.906 | 2634 k | 2.092 | 2557 k | |
| star.c10r.facebook.com | mfausto.amministrazione.unicam | 381 | 128 k | 165 | 30 k | |
| video-mxp1-1.xx.fbcdn.net | mfausto.amministrazione.unicam | 8.935 | 10 M | 7.438 | 10 M | |
| facebook.com | mfausto.amministrazione.unicam | 1.284 | 861 k | 751 | 652 k | |
| host188-131-14-31.serverdedicati.aruba.it | 193.205.92.27 | 1 | 90 | 1 | 90 | |
| ec2-35-163-53-118.us-west-2.compute.amazonaws.com | mfausto.amministrazione.unicam | 6 | 452 | 2 | 170 | |
| 37.77.114.151 | 193.205.92.67 | 1 | 66 | 1 | 66 | |
| 40.67.251.132 | mfausto.amministrazione.unicam | 95 | 11 k | 32 | 5760 | |
| ieonlinews.trafficmanager.net | mfausto.amministrazione.unicam | 37 | 15 k | 15 | 12 k | |
| db5-ap.settings.data.microsoft.com.akadns.net | mfausto.amministrazione.unicam | 24 | 8442 | 10 | 7070 | |
| pipeline-edge-prod-25-561439127.us-west-2.elb.amazonaws.com | mfausto.amministrazione.unicam | 26 | 11 k | 10 | 4180 | |
| ec2-52-54-248-107.compute-1.amazonaws.com | cippus-ThinkPad-13.local | 11 | 1078 | 11 | 1078 | |
| onecollector.cloudapp.aria.akadns.net | mfausto.amministrazione.unicam | 17 | 7329 | 8 | 4655 | |
| db5-eap.settings.data.microsoft.com.akadns.net | mfausto.amministrazione.unicam | 77 | 25 k | 34 | 21 k | |
| 81.ip-54-38-180.eu | farmy.amministrazione.unicam | 2 | 140 | 2 | 140 | |
| ec2-54-187-46-234.us-west-2.compute.amazonaws.com | mfausto.amministrazione.unicam | 24 | 1474 | 12 | 818 | |
| ec2-54-201-6-28.us-west-2.compute.amazonaws.com | mfausto.amministrazione.unicam | 10 | 598 | 5 | 325 | |
| ec2-54-210-203-205.compute-1.amazonaws.com | cippus-ThinkPad-13.local | 11 | 1078 | 11 | 1078 | |
| 60.191.38.77 | 193.205.92.117 | 2 | 120 | 2 | 120 | |
| wm-in-f94.1e100.net | mfausto.amministrazione.unicam | 303 | 281 k | 202 | 275 k | |
| stats.l.doubleclick.net | mfausto.amministrazione.unicam | 49 | 8921 | 27 | 5950 | |
| cello.client-channel.google.com | fabriziounicam.local | 10 | 1164 | 10 | 1164 | |
| cello.client-channel.google.com | pc-mancin-bea-2.amministrazione.unicam | 1 | 105 | 1 | 105 | |
| cello.client-channel.google.com | cippus-ThinkPad-13.local | 12 | 1512 | 12 | 1512 | |

☑ Name resolution ☐ Limit to display filter ☐ Absolute start time Conversation Types

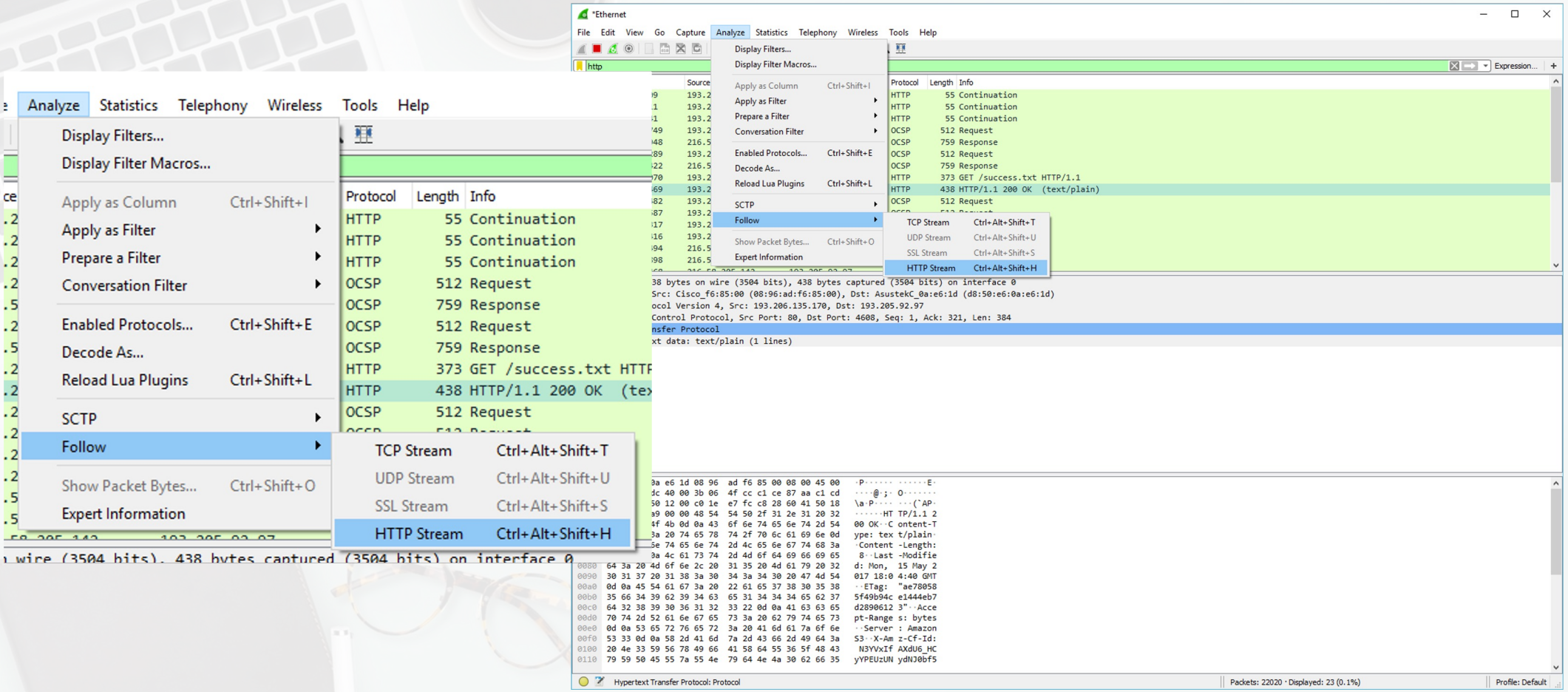
Copy | Follow Stream... | Graph... | Chiudi | Aiuto

# Wireshark – filtro http

http



# Wireshark – Analizza



# Wireshark – Follow HTTP Stream

Wireshark · Follow HTTP Stream (tcp.stream eq 7) · Ethernet

```
GET /success.txt HTTP/1.1
Host: detectportal.firefox.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Accept: */*
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
Pragma: no-cache
Connection: keep-alive

HTTP/1.1 200 OK
Content-Type: text/plain
Content-Length: 8
Last-Modified: Mon, 15 May 2017 18:04:40 GMT
ETag: "ae780585f49b94ce1444eb7d28906123"
Accept-Ranges: bytes
Server: AmazonS3
X-Amz-Cf-Id: N3YVxIfAXdU6_HCyYPEUzUNydNJ0bf5vyIt9MGI5rq3FnwDqh9CbOQ==
Cache-Control: no-cache, no-store, must-revalidate
Date: Mon, 22 Oct 2018 08:28:02 GMT
Connection: keep-alive

success
```

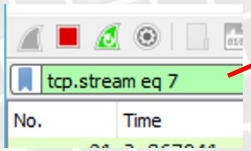
1 client pkt(s), 1 server pkt(s), 1 turn(s).

Entire conversation (703 bytes) | Show and save data as ASCII

Find: | Find Next

Filter Out This Stream | Print | Save as... | Back | Chiudi | Aiuto

# Wireshark – rimuovere filtri




*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

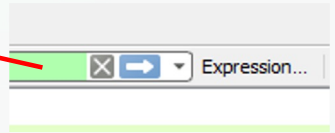
tcp.stream eq 7 | Expression... | +

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 21 | 3.867041 | 193.205.92.97 | 193.206.135.170 | HTTP | 55 | Continuation |
| 22 | 3.880216 | 193.206.135.170 | 193.205.92.97 | TCP | 66 | 80 → 4608 [ACK] Seq=1 Ack=2 Win=237 Len=0 SLE=1 SRE=2 |
| 68 | 13.879620 | 193.205.92.97 | 193.206.135.170 | TCP | 55 | [TCP Keep-Alive] 4608 → 80 [ACK] Seq=1 Ack=1 Win=257 Len=1 |
| 69 | 13.892694 | 193.206.135.170 | 193.205.92.97 | TCP | 66 | [TCP Keep-Alive ACK] 80 → 4608 [ACK] Seq=1 Ack=2 Win=237 L |
| 129 | 23.892990 | 193.205.92.97 | 193.206.135.170 | TCP | 55 | [TCP Keep-Alive] 4608 → 80 [ACK] Seq=1 Ack=1 Win=257 Len=1 |
| 130 | 23.905880 | 193.206.135.170 | 193.205.92.97 | TCP | 66 | [TCP Keep-Alive ACK] 80 → 4608 [ACK] Seq=1 Ack=2 Win=237 L |
| 3276 | 33.808070 | 193.205.92.97 | 193.206.135.170 | HTTP | 373 | GET /success.txt HTTP/1.1 |
| 3288 | 33.821166 | 193.206.135.170 | 193.205.92.97 | TCP | 60 | 80 → 4608 [ACK] Seq=1 Ack=321 Win=245 Len=0 |
| 3289 | 33.821469 | 193.206.135.170 | 193.205.92.97 | HTTP | 438 | HTTP/1.1 200 OK (text/plain) |
| 3291 | 33.862894 | 193.205.92.97 | 193.206.135.170 | TCP | 54 | 4608 → 80 [ACK] Seq=321 Ack=385 Win=255 Len=0 |

```
> Frame 3289: 438 bytes on wire (3504 bits), 438 bytes captured (3504 bits) on interface 0
> Ethernet II, Src: Cisco_f6:85:00 (08:96:ad:f6:85:00), Dst: AsustekC_0a:e6:1d (d8:50:e6:0a:e6:1d)
> Internet Protocol Version 4, Src: 193.206.135.170, Dst: 193.205.92.97
> Transmission Control Protocol, Src Port: 80, Dst Port: 4608, Seq: 1, Ack: 321, Len: 384
> Hypertext Transfer Protocol
> Line-based text data: text/plain (1 lines)
```

```
0000  d8 50 e6 0a e6 1d 08 96  ad f6 85 00 08 00 45 00   ·P····· ·····E·
0010  01 a8 86 dc 40 00 3b 06  4f cc c1 ce 87 aa c1 cd   ····@·;· O·····
0020  5c 61 00 50 12 00 c0 1e  e7 fc c8 28 60 41 50 18   \a·P···· ···(`AP·
0030  00 f5 be a9 00 00 48 54  54 50 2f 31 2e 31 20 32   ·····HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 43  6f 6e 74 65 6e 74 2d 54   00 OK··C ontent-T
0050  79 70 65 3a 20 74 65 78  74 2f 70 6c 61 69 6e 0d   ype: tex t/plain·
0060  0a 43 6f 6e 74 65 6e 74  2d 4c 65 6e 67 74 68 3a   ·Content -Length:
0070  20 38 0d 0a 4c 61 73 74  2d 4d 6f 64 69 66 69 65    8··Last -Modifie
0080  64 3a 20 4d 6f 6e 2c 20  31 35 20 4d 61 79 20 32   d: Mon,  15 May 2
0090  30 31 37 20 31 38 3a 30  34 3a 34 30 20 47 4d 54   017 18:0 4:40 GMT
00a0  0d 0a 45 54 61 67 3a 20  22 61 65 37 38 30 35 38   ··ETag:  "ae78058
00b0  35 66 34 39 62 39 34 63  65 31 34 34 34 65 62 37   5f49b94c e1444eb7
00c0  64 32 38 39 30 36 31 32  33 22 0d 0a 41 63 63 65   d2890612 3"··Acce
00d0  70 74 2d 52 61 6e 67 65  73 3a 20 62 79 74 65 73   pt-Range s: bytes
```

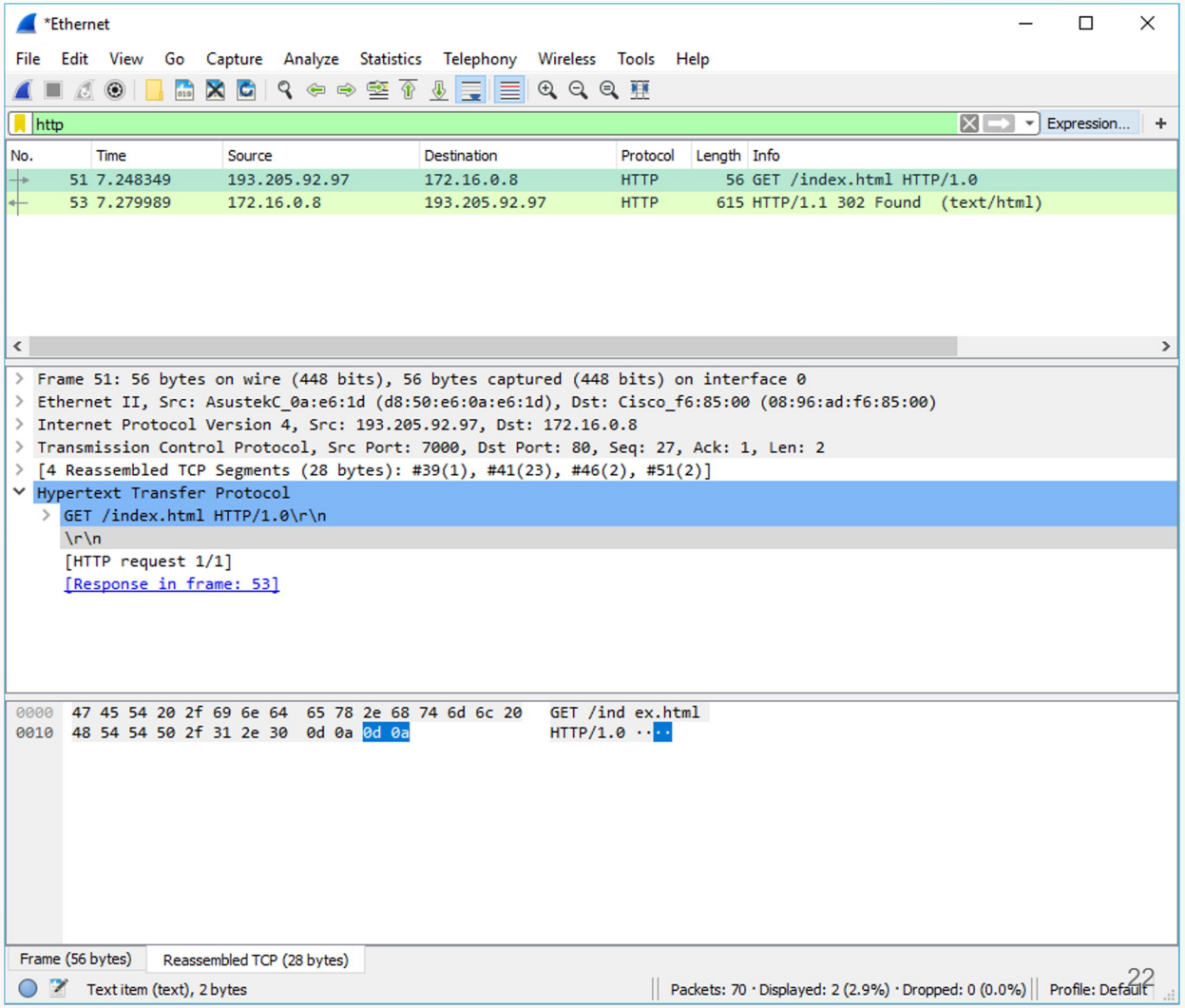
wireshark_31F20730-8C4F-4C02-B264-D3E5F3F123B7_20181022102918_a12192.pcapng | Packets: 33904 · Displayed: 13 (0.0%) | Profile: Default



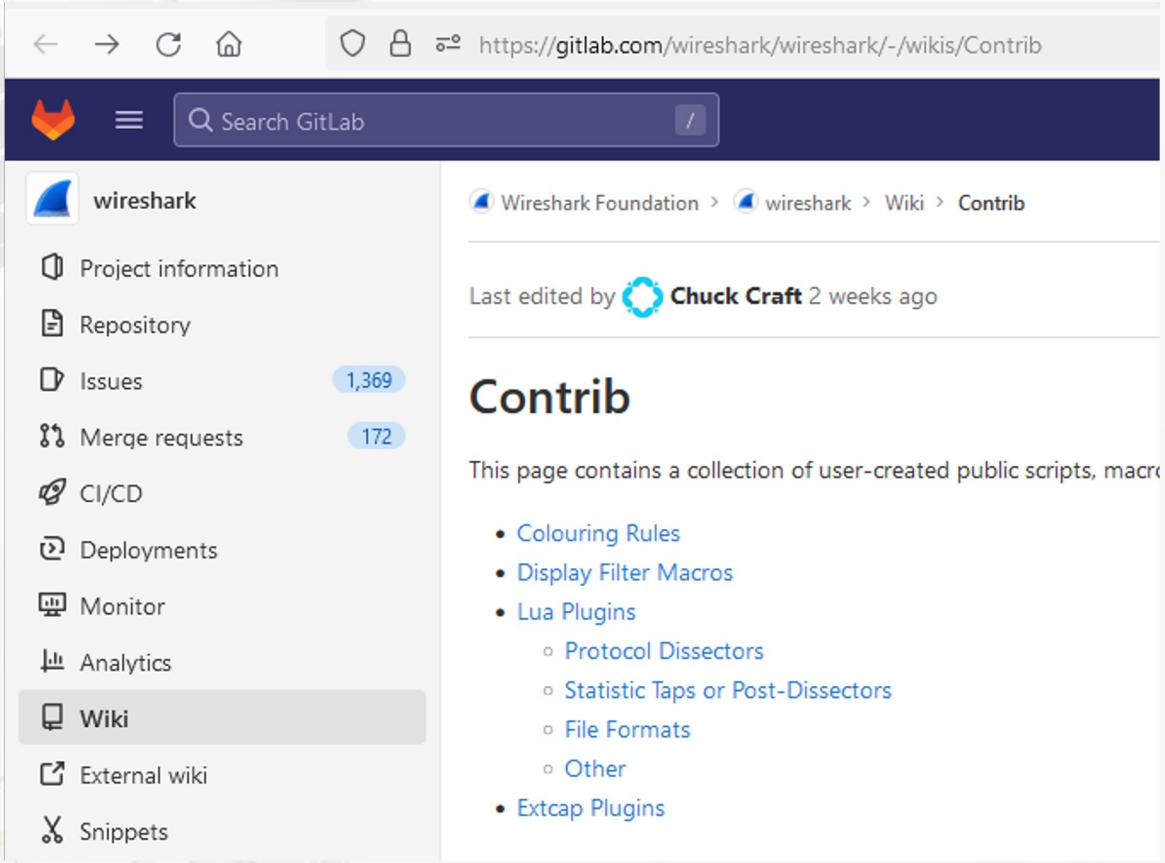
# Wireshark – esercitazione individuale

```
telnet 90.147.42.31 80
```

- digitare e commentare:
  - abcdef
  - GET /index.html HTTP/1.0
  - HEAD
  - HEAD /index.html HTTP/1.0
  - POST
  - GET /index.html HTTP/1.1



# Wireshark contrib




https://gitlab.com/wireshark/wireshark/-/wikis/Contrib

# FINE

# Virtual Machine

# Virtual Machine

**Che cos'è una macchina virtuale?**

Una macchina virtuale è **un file di computer**, chiamato in genere immagine, che si comporta come un vero computer. In altre parole, si tratta di **creare un computer all'interno di un computer**. Viene eseguito in una finestra, come qualsiasi altra applicazione, e offre all'utente finale la stessa esperienza fornita dal sistema operativo host stesso. La macchina virtuale è isolata dal resto del sistema in modo che il software al suo interno non possa fuoriuscire o interagire con il computer stesso. Si tratta quindi di un ambiente ideale per testare altri sistemi operativi e versioni beta, accedere a dati infettati da virus, creare backup di sistemi operativi ed eseguire software o applicazioni in sistemi operativi diversi da quelli originariamente supportati. È possibile **eseguire contemporaneamente più macchine virtuali nello stesso computer fisico**. Per i server, i vari sistemi operativi vengono eseguiti in modalità affiancata grazie a un software, chiamato **hypervisor**, che li gestisce, mentre in genere per i computer desktop viene usato un solo sistema operativo che esegue gli altri sistemi all'interno delle finestre del programma. Ogni macchina virtuale ha il suo **hardware virtuale**, che include CPU, memoria, unità disco rigido, interfacce di rete e altri dispositivi. L'hardware virtuale viene quindi mappato all'hardware reale nel computer fisico per ridurre i costi relativi ai sistemi hardware fisici necessari e i costi di gestione associati, oltre a ridurre la domanda di alimentazione e raffreddamento.

https://azure.microsoft.com/it-it/overview/what-is-a-virtual-machine/

# The Top Open-Source Hypervisor Technologies

https://slashdot.org/software/hypervisors/

https://wire19.com/comparison-top-server-virtualization-software/

https://opensourceforu.com/2016/03/the-top-open-source-hypervisor-technologies/

https://www.how2shout.com/tools/8-free-best-open-source-bare-metal-hypervisors-foss.html

# List of Best Open Source Hypervisors

1. **Xen:**
Xen is among the most popular open-source hypervisors in the present era, and it also comes with a commercial version of Citrix and Oracle VM. Moreover, since XEN gets cloud support, it is widely prevalent among all business enterprises.

2. **Linux KVM:**
If you are looking for hypervisors for Linux, kernel-based Linux is among the best. It has a kernel module KVM.ko which is a loadable kernel, and it can quickly turn the Linux kernel into a hypervisor. The Linux KVM belongs to the type 2 hypervisors because of the involvement of the kernel.

3. **Microsoft Hyper V:**
Microsoft Hyper V is a free hypervisor you can download easily from the net and use. It is an open-source application. The primary aim of the Microsoft Hyper V was to compete with the other open-source hypervisors. It is one of the best free hypervisors as it is a standalone software and includes all the features of Windows Server 2012.

4. **VMware Free ESXi:**
VMware ESXi is free software that you can download easily from the net. The benefit of using open-source software is that you can customize it according to your requirement. Hence, it is pretty popular among users.

5. **Guest:**
Guest is a lightweight hypervisor that is built into the Linux kernel. The software is apt to develop and test the kernel boot. Moreover, the functioning of the software is also interesting and exciting. During initialization, the Guest allocates memory and maps it to the kernel's address space, and it loads a small hypervisor in this allocated memory.

6. **Oracle VirtualBox:**
The Oracle VirtualBox is a type 2 hypervisor that you can run on any operating system, such as Solaris, Linux, Mac, and Windows. It is also compatible with both x86 and x64 operating systems. One of the benefits of using the Oracle VirtualBox is that it is pretty portable. It also allows virtual machines to be imported or exported using the Open Virtualization Format (OVF). It is one of the prominent features of this product.

7. **Xvisor:**
The Xvisor provides virtualization to various types of architectures. You can quickly transfer its code to most 32 and 64-bit architectures until they have PMMU.

8. **VMware Workstation Player:**
The VMware Workstation Player is a type 2 open-source hypervisor. It is one of the ideal software that can find a place in any enterprise, and it is because the software is simple and easy to use. The VMware Workstation Player is ideal for running and evaluating operating systems and applications on a virtual machine with either Linux or Windows.

9. **OpenVZ:**
OpenVZ is open-source container-based virtualization specially created for Linux. It also can create as many virtual machines as possible in a Linux container. Hence, it becomes easy for the admin to use each container as an individual server, and you can reboot without any hassles on the same physical server.

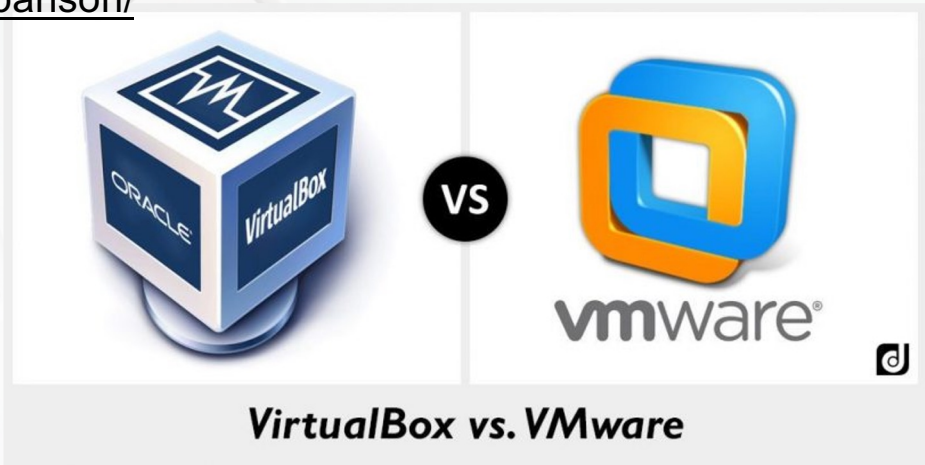
10. **SmartOS:**
The SmartOS is based on Linux's Kernel-based Virtual Machine Virtualization technology. You can easily download the VM hypervisor free from the net. One of the significant advantages of using the SmartOs is that anyone can use them according to their convenience.

# Top 10 Virtualization SoftwareVirtualization Systems

Comparison Table https://www.softwaretestinghelp.com/virtualization-software/

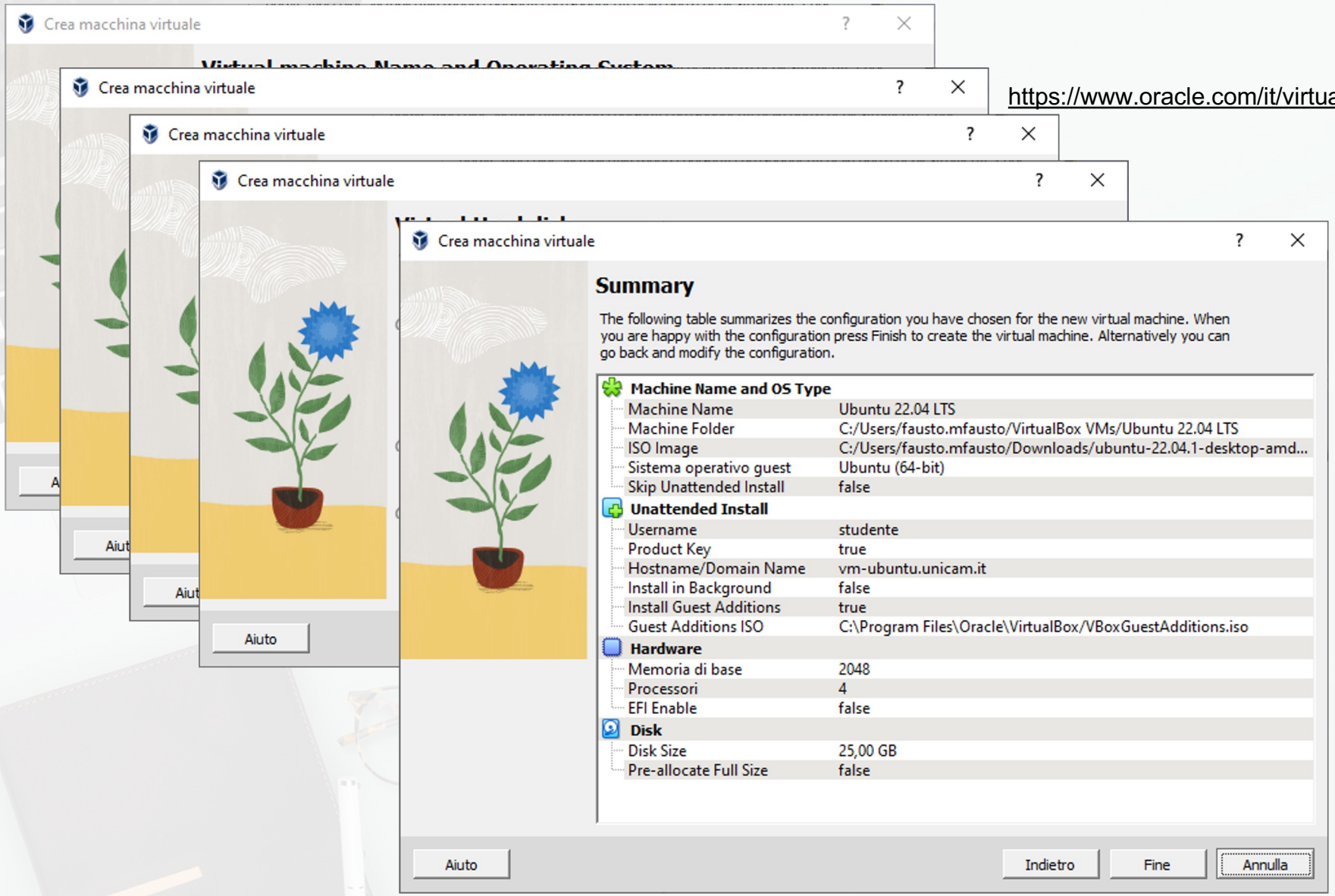
#1) SolarWinds Virtualization Manager
#2) Parallels Desktop
#3) V2 Cloud
#4) VMware Fusion
#5) Oracle VM Virtual Box
#6) VMware Workstation
#7) QEMU
#8) Windows Virtual PC
#9) Microsoft Hyper-V
#10) RedHat Virtualization
#11) Veertu for Mac
#12) Boot Camp

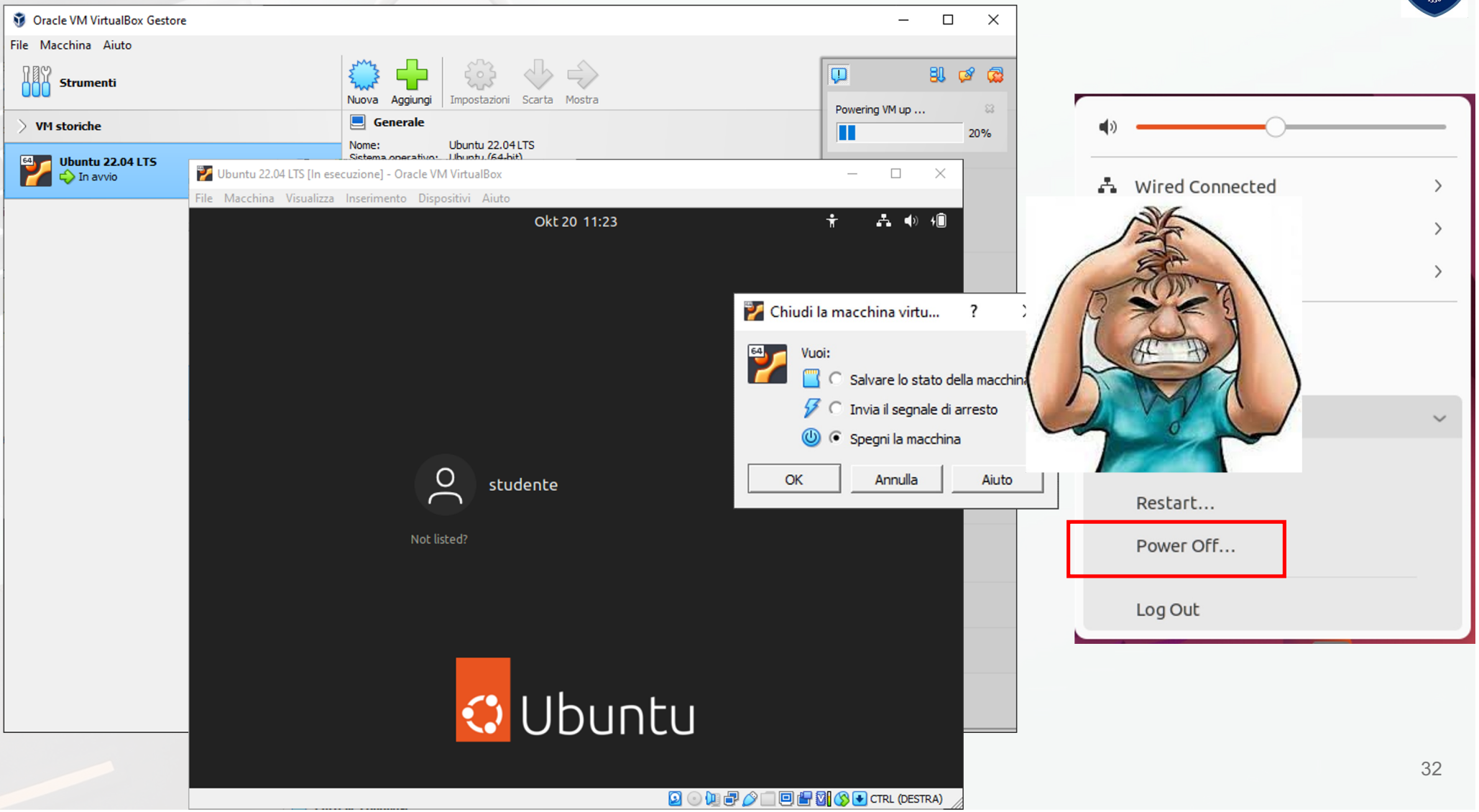
https://www.youlicense.com/virtualbox-vs-vmware-comparison/

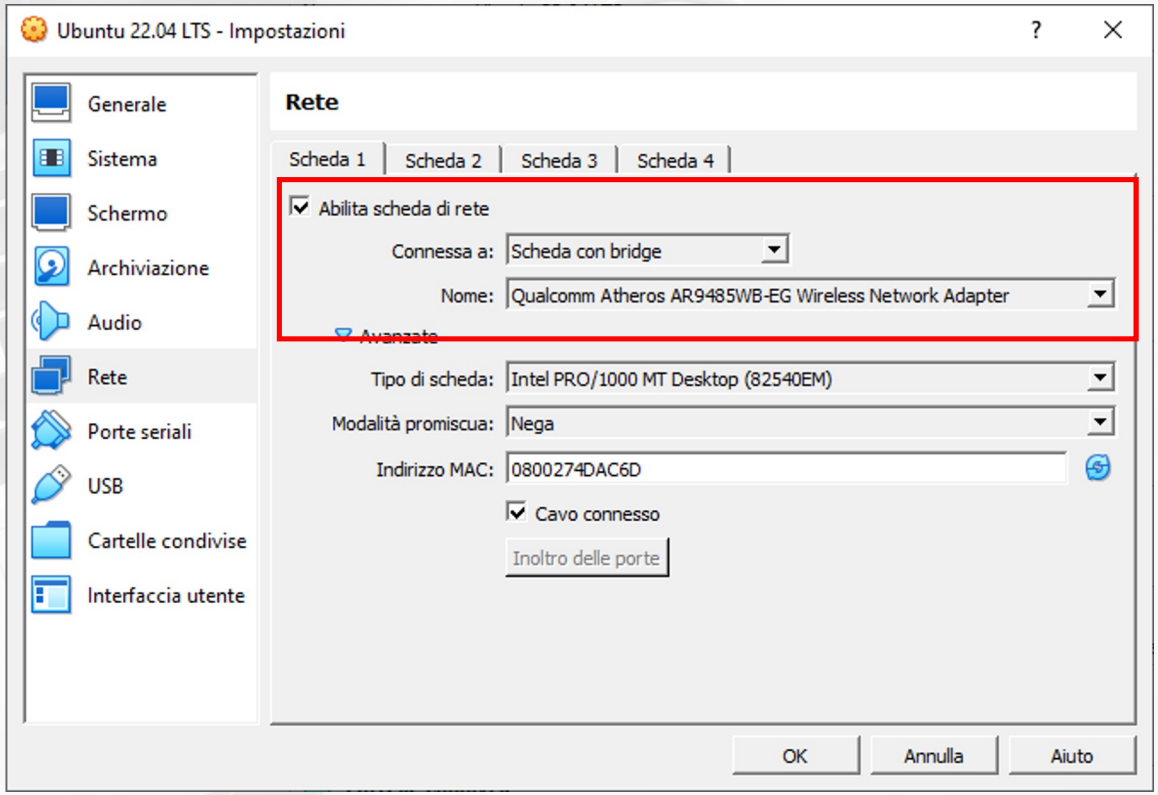




https://www.oracle.com/it/virtualization/virtualbox/




Oracle VM VirtualBox Gestore
File Macchina Aiuto
Strumenti
Nuova Aggiungi Impostazioni Scarta Mostra
VM storiche
Ubuntu 22.04 LTS
In avvio
Generale
Nome: Ubuntu 22.04 LTS
Powering VM up ...
20%
Ubuntu 22.04 LTS [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Okt 20 11:23
studente
Not listed?
Ubuntu
CTRL (DESTRA)
Chiudi la macchina virtu...
Vuoi:
Salvare lo stato della macchina
Invia il segnale di arresto
Spegni la macchina
OK
Annulla
Aiuto
Wired Connected
Restart...
Power Off...
Log Out


Ubuntu 22.04 LTS - Impostazioni
Generale
Sistema
Schermo
Archiviazione
Audio
Rete
Porte seriali
USB
Cartelle condivise
Interfaccia utente
Rete
Scheda 1
Scheda 2
Scheda 3
Scheda 4
Abilita scheda di rete
Connessa a:
Scheda con bridge
Nome:
Qualcomm Atheros AR9485WB-EG Wireless Network Adapter
Avanzate
Tipo di scheda:
Intel PRO/1000 MT Desktop (82540EM)
Modalità promiscua:
Nega
Indirizzo MAC:
0800274DAC6D
Cavo connesso
Inoltro delle porte
OK
Annulla
Aiuto

## Oracle VM VirtualBox Extension Pack

Free for personal, educational or evaluation use under the terms of the VirtualBox Personal Use and Evaluation License on Windows,

| Platform | File |
| --- | --- |
| For use with Version 7.0.10 only<br>All Platforms (Windows, Mac OS X, Solaris and Linux) | 7.0.10 ExtPack |

Depending on your browser, you may need to right click and "Save As..." this file.

You might want to compare the SHA256 checksum or the MD5 checksum to verify the integrity of downloaded packages.

vmware Docs | Home | Products | Resources | Search in this document

VMware Workstation Player for Windows

Expand All

- Installing and Upgrading VMware Tools
  - Installing VMware Tools
  - Upgrading VMware Tools
  - Configure Software Update Preferences
  - Configure VMware Tools Updates for a Specific Virtual Machine
  - Manually Installing and Upgrading

Docs / VMware Workstation Player for Windows / Using VMware Workstation Player for Windo

# Installing VMware Tools

Add to Library | RSS | Download PDF | Feedback

Updated on 09/09/2019

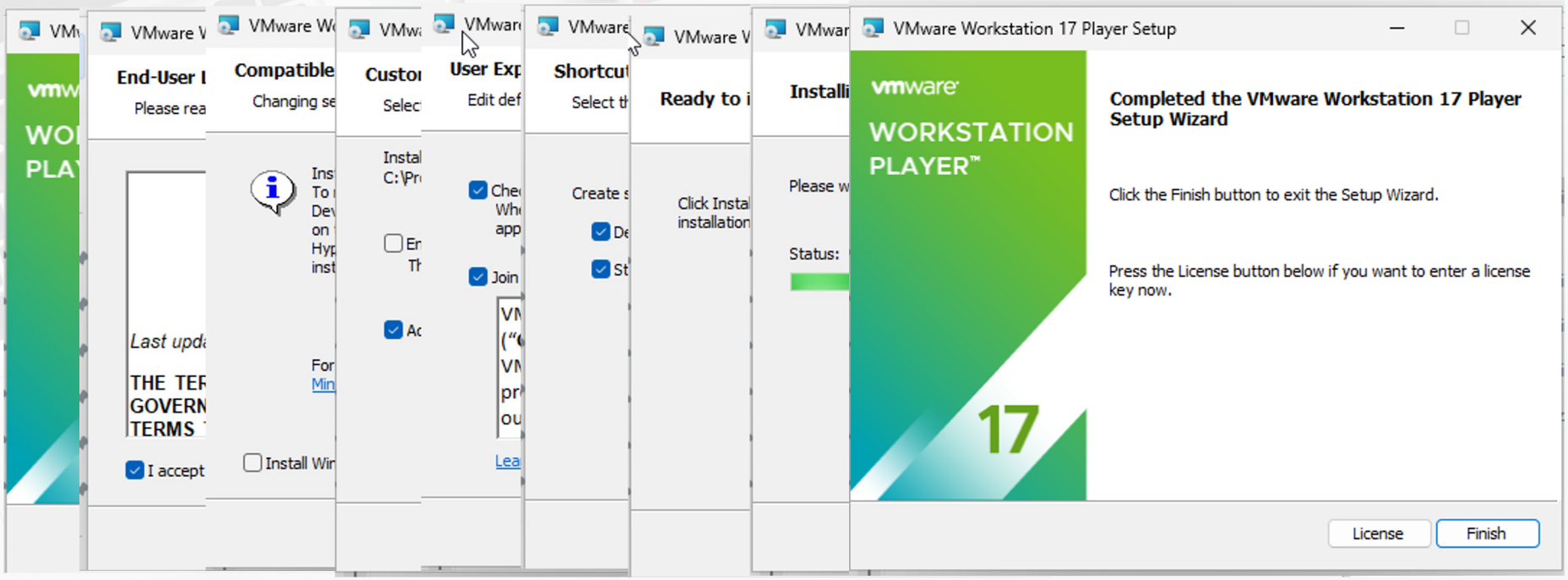
Selected product version: VMware Workstation Player for Windows 17.0

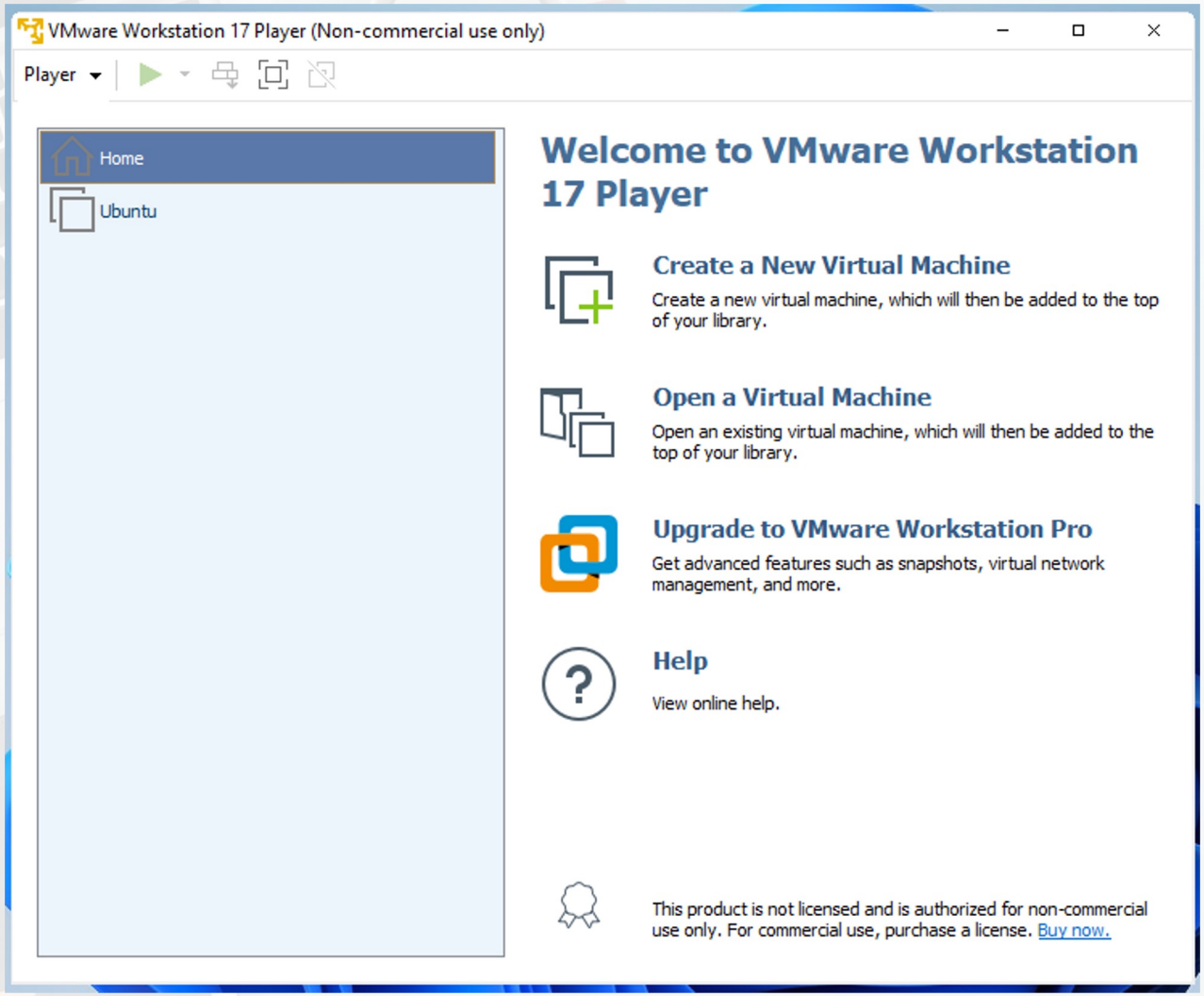
Installing VMware Tools is part of the process of creating a new virtual machine, an keeping your virtual machine up to current standards. Although your guest operati


Try Workstation 17 Player for Windows

DOWNLOAD NOW ›

https://support.broadcom.com/group/ecx/productdownloads?subfamily=VMware+Workstation+Pro


VMware Workstation 17 Player Setup
vmware
WORKSTATION
PLAYER™
17
Completed the VMware Workstation 17 Player Setup Wizard
Click the Finish button to exit the Setup Wizard.
Press the License button below if you want to enter a license key now.
License
Finish

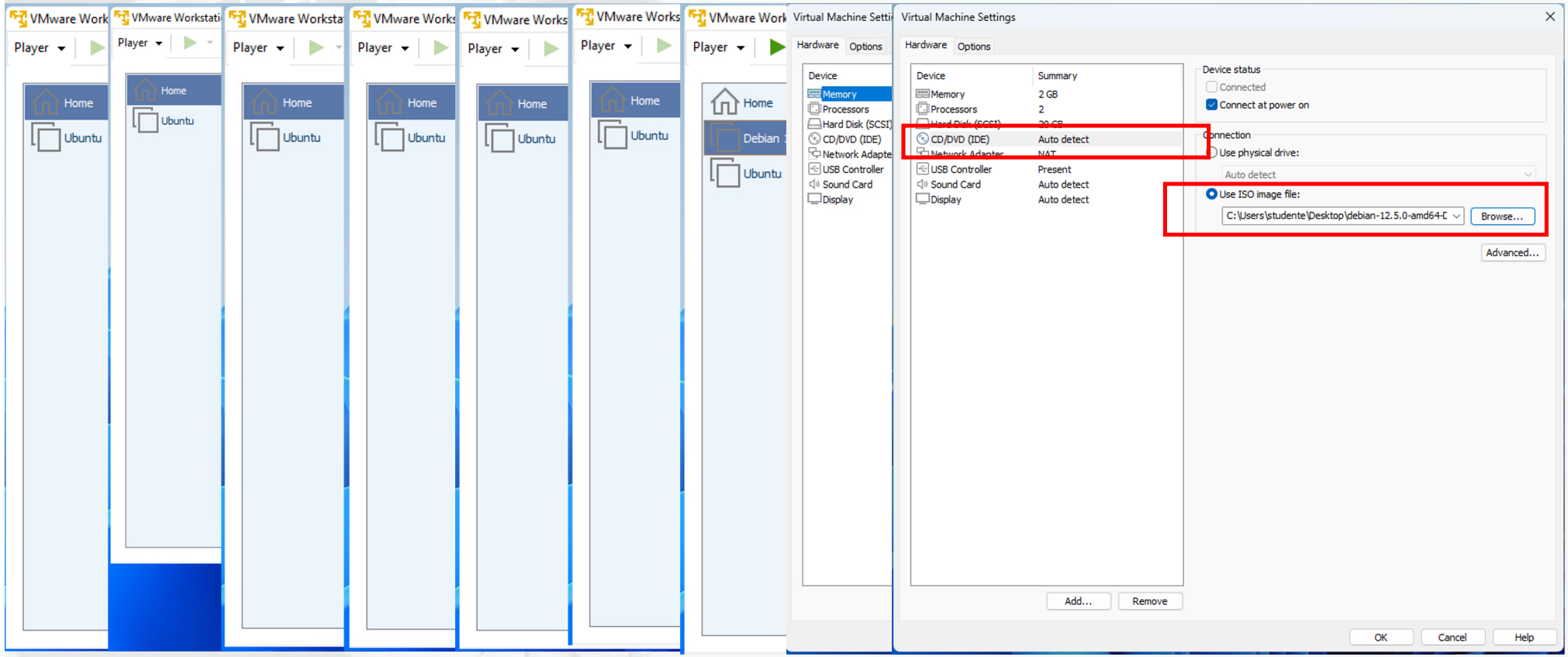

VMware Workstation 17 Player (Non-commercial use only)
Player
Home
Ubuntu
Welcome to VMware Workstation 17 Player
Create a New Virtual Machine
Create a new virtual machine, which will then be added to the top of your library.
Open a Virtual Machine
Open an existing virtual machine, which will then be added to the top of your library.
Upgrade to VMware Workstation Pro
Get advanced features such as snapshots, virtual network management, and more.
Help
View online help.
This product is not licensed and is authorized for non-commercial use only. For commercial use, purchase a license. Buy now.

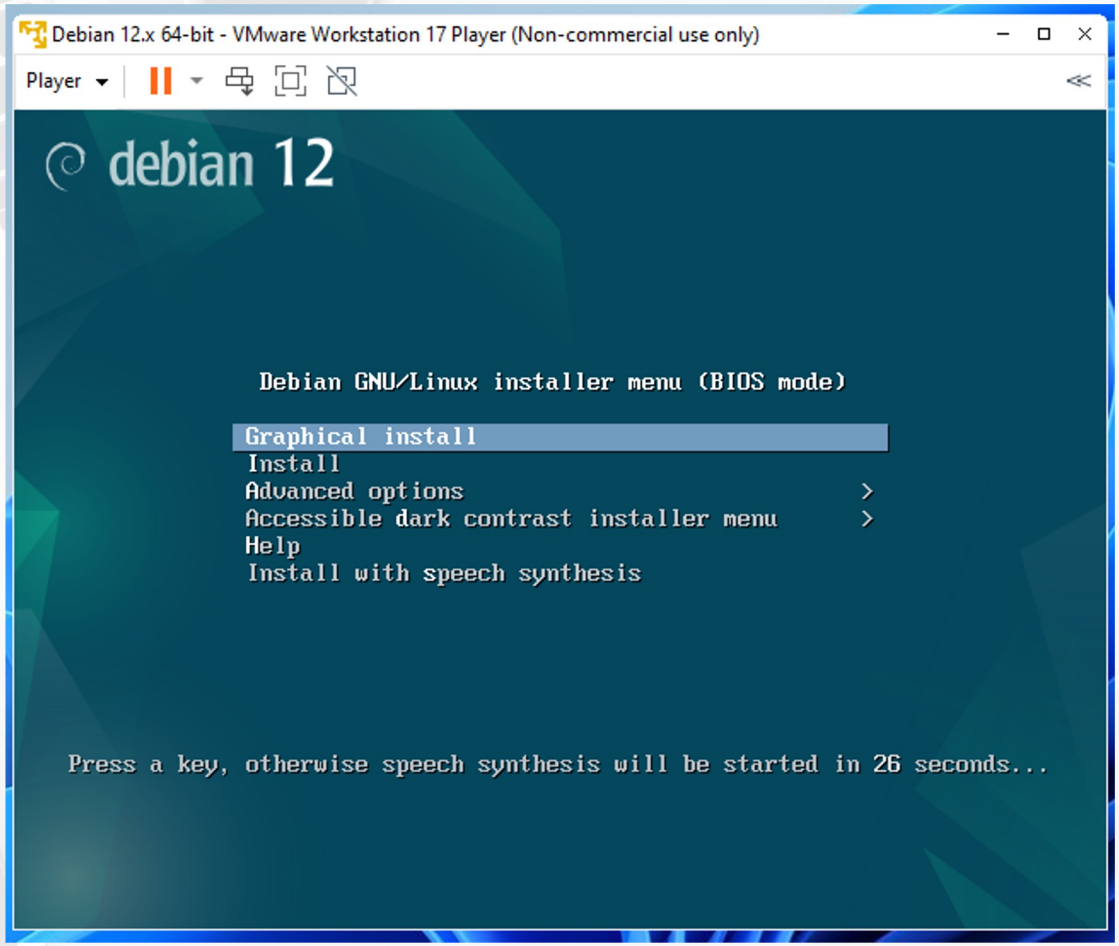
# Debian


| File Name ↓ | File Size ↓ |
|---|---|
| Parent directory/ | - |
| HEADER.html | 3.9 KiB |
| SHA256SUMS | 2.0 KiB |
| SHA256SUMS.sign | 833 B |
| SHA512SUMS | 3.3 KiB |
| SHA512SUMS.sign | 833 B |
| debian-12.5.0-amd64-DVD-1.iso | 3.7 GiB |

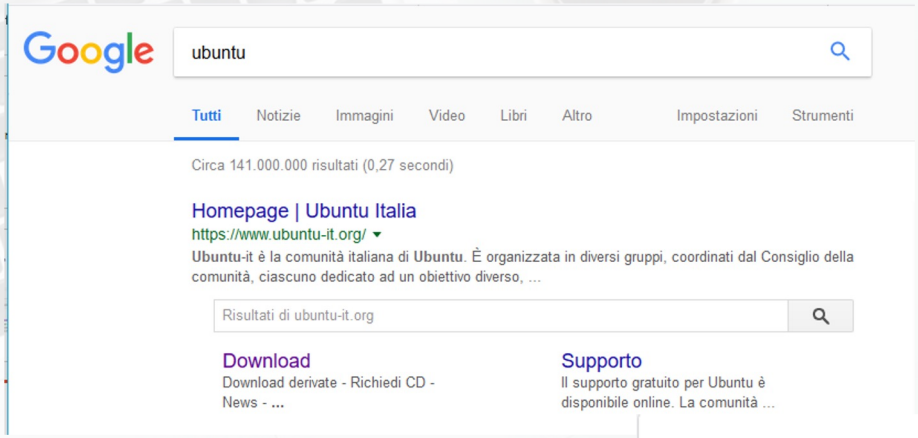
https://www.debian.org/distrib/index.en.html

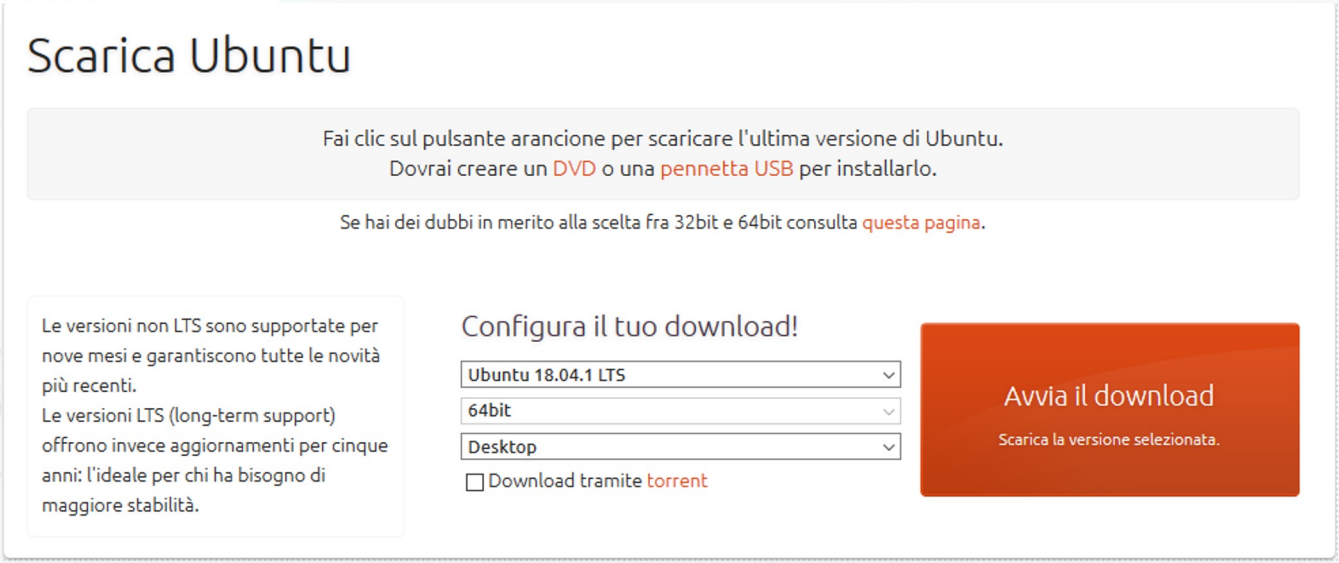
http://giano.com.dist.unige.it/debian-cd/12.5.0/amd64/iso-dvd/


VMware Work
Player
Home
Ubuntu
Debian
Virtual Machine Settings
Hardware
Options
Device
Memory
Processors
Hard Disk (SCSI)
CD/DVD (IDE)
Network Adapte
USB Controller
Sound Card
Display
Summary
2 GB
2
Auto detect
NAT
Present
Device status
Connected
Connect at power on
Connection
Use physical drive:
Use ISO image file:
C:\Users\studente\Desktop\debian-12.5.0-amd64-D
Browse...
Advanced...
Add...
Remove
OK
Cancel
Help


Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
debian 12
Debian GNU/Linux installer menu (BIOS mode)
Graphical install
Install
Advanced options
Accessible dark contrast installer menu
Help
Install with speech synthesis
Press a key, otherwise speech synthesis will be started in 26 seconds...

# Scaricare l'ultima versione della iso di Ubuntu



# Caratteristiche VM

Hardware | Options

| Device | Summary |
|---|---|
| Memory | 2 GB |
| Processors | 2 |
| Hard Disk (SCSI) | 20 GB |
| CD/DVD (SATA) | Using file D:\ISO\ubuntu-18.04... |
| Network Adapter | Bridged (Automatic) |
| USB Controller | Present |
| Sound Card | Auto detect |
| Printer | Present |
| Display | Auto detect |

**Generale**

Nome: ubuntu
Sistema operativo: Ubuntu (64-bit)

**Sistema**

Memoria di base: 2048 MB
Ordine di avvio: Floppy, Ottico, Disco fisso
Accelerazione: VT-x/AMD-V, Paginazione nidificata, Paravirtualizzazione KVM

**Anteprima**

ubuntu

**Schermo**

Memoria video: 16 MB
Server di desktop remoto: Disabilitato
Acquisizione video: Disabilitata

**Archiviazione**

Controller: IDE
IDE master secondario: [Lettori ottici] Vuoto
Controller: SATA
Porta SATA 0: ubuntu.vdi (Normale, 20,00 GB)

**Audio**

Driver host: Windows DirectSound
Controller: ICH AC97

**Rete**

Scheda 1: Intel PRO/1000 MT Desktop (Scheda con bridge, Realtek PCIe GbE Family Controller)

**USB**

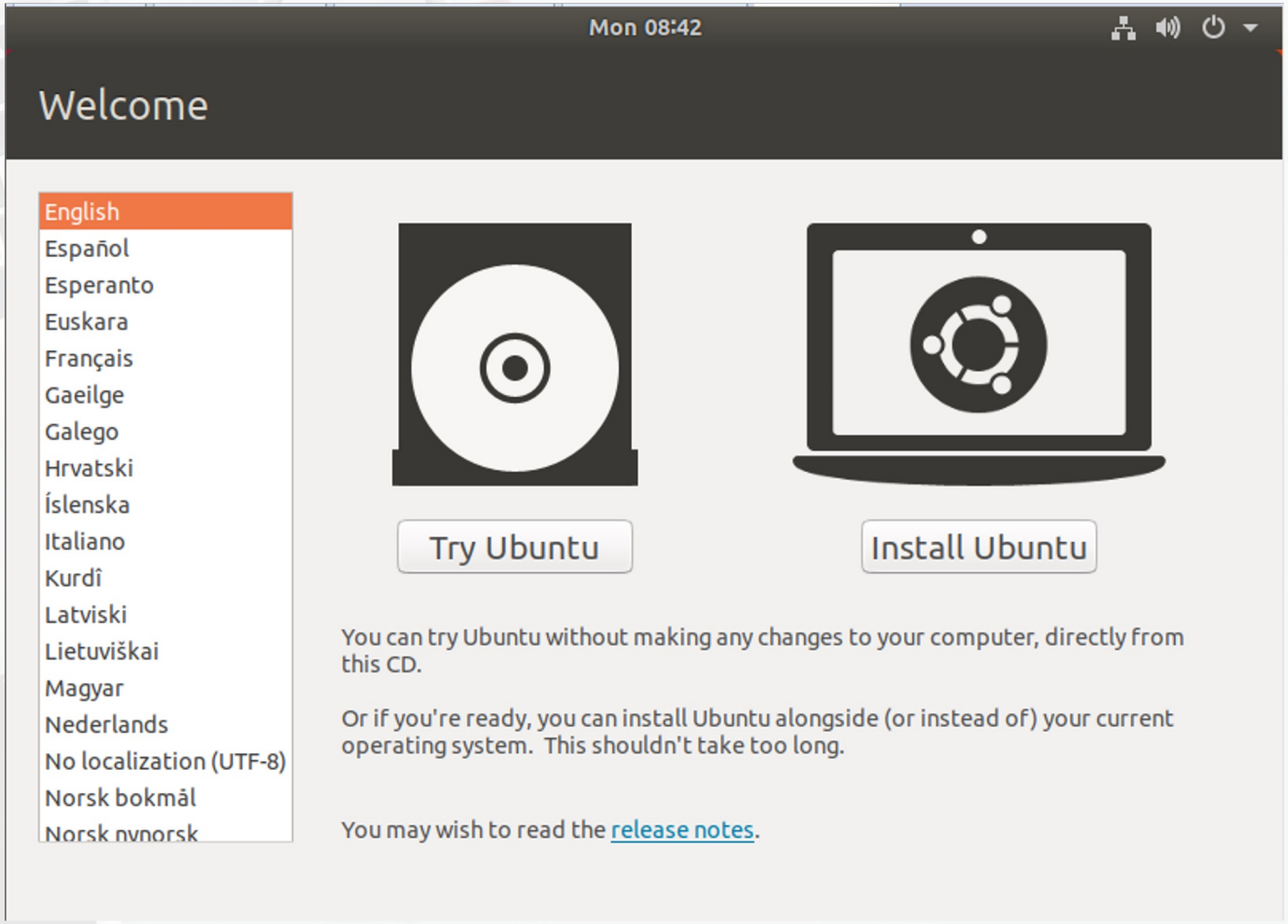
Controller USB: OHCI
Filtri dispositivi: 0 (0 attivo)

**Cartelle condivise**

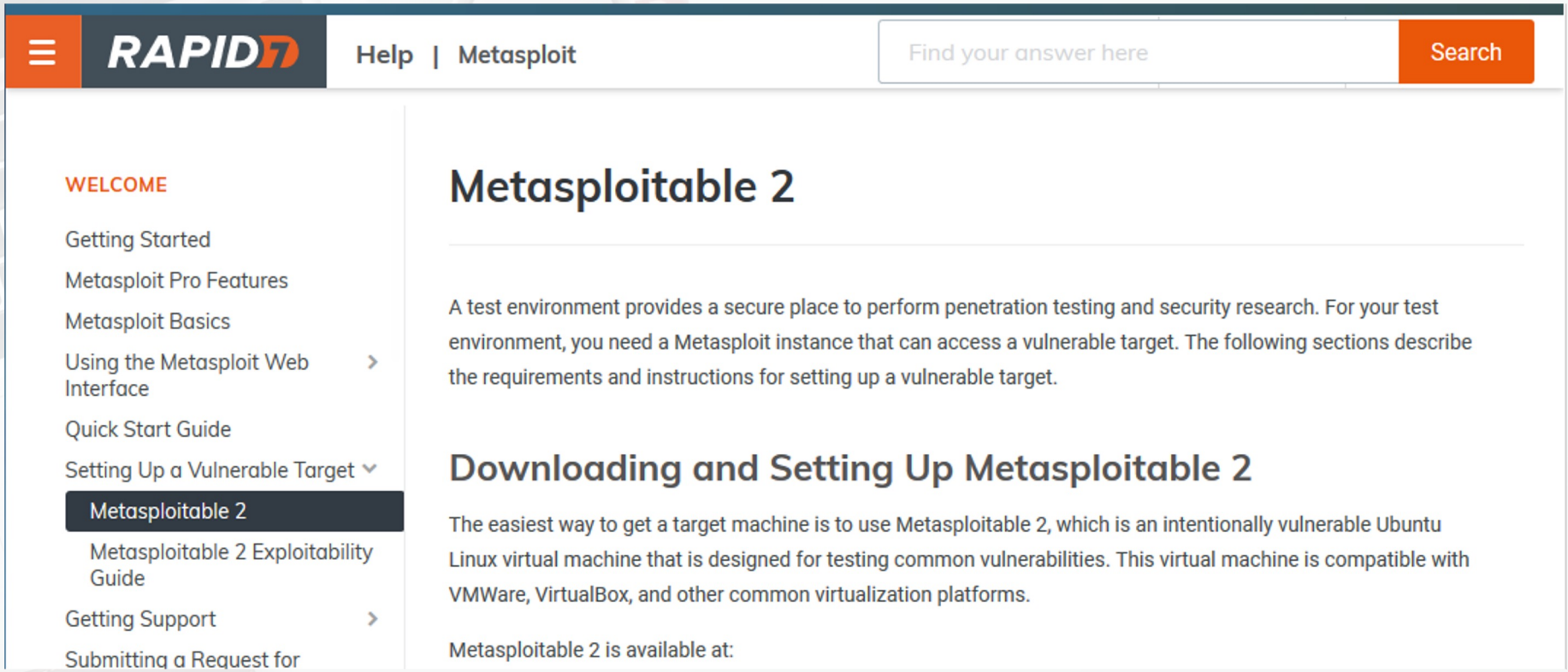
Nessuna

**Descrizione**

Nessuna


Mon 08:42
Welcome
English
Español
Esperanto
Euskara
Français
Gaeilge
Galego
Hrvatski
Íslenska
Italiano
Kurdî
Latviski
Lietuviškai
Magyar
Nederlands
No localization (UTF-8)
Norsk bokmål
Norsk nynorsk
Try Ubuntu
Install Ubuntu
You can try Ubuntu without making any changes to your computer, directly from this CD.
Or if you're ready, you can install Ubuntu alongside (or instead of) your current operating system. This shouldn't take too long.
You may wish to read the release notes.

# Metasploitable 2




https://metasploit.help.rapid7.com/docs/metasploitable-2

# Metasploitable2

https://docs.rapid7.com/metasploit/metasploitable-2/#metasploitable-2

The Metasploitable virtual machine is an intentionally vulnerable version of Ubuntu Linux designed for testing security tools and demonstrating common vulnerabilities.

Metasploitable 2 is available at:

- https://information.rapid7.com/metasploitable-download.html
- https://sourceforge.net/projects/metasploitable/

# Metasploitable 2 - VMWARE

## Metasploitable2-Linux

Power on this virtual machine
Edit virtual machine settings

### Devices

| | |
|---|---|
| Memory | 512 MB |
| Processors | 1 |
| Hard Disk (SCSI) | 8 GB |
| CD/DVD (IDE) | Auto detect |
| Network Adapter | Bridged (Autom... |
| Network Adapter 2 | Host-only |
| USB Controller | Present |
| Display | Auto detect |

### Description

This is Metasploitable2 (Linux)Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice common penetration testing techniques. The default login and password is msfadmin:msfadmin. Never expose this VM to an untrusted network (use NAT or Host-only mode if you have any questions what that means). To contact the developers, please send email to msfdev@metasploit.com

### Virtual Machine Details

**State:** Powered off
**Configuration file:** C:\Users\fausto.mfausto\Desktop\Virtual Machines\Metasploitable2-Linux\Metasploitable.vmx
**Hardware compatibility:** Workstation 15.x virtual machine
**Primary IP address:** Network information is not available

# Metasploitable 2 – VirtualBox

**Generale**

Nome: Metasploitable 2
Sistema operativo: Ubuntu (32-bit)
Posizione del file delle impostazioni: C:\Users\fausto.mfausto\VirtualBox VMs\Metasploitable 2

**Anteprima**


**Sistema**

Memoria di base: 512 MB
Ordine di avvio: Floppy, Ottico, Disco fisso
Accelerazione: VT-x/AMD-V, Paginazione nidificata, PAE/NX, Paravirtualizzazione KVM

**Schermo**

Memoria video: 16 MB
Scheda grafica: VBoxVGA
Server di desktop remoto: Disabilitato
Registrazione: Disabilitata

**Archiviazione**

Controller: IDE
Controller: SCSI
Porta SCSI 0: Metasploitable2-Linux-disk1.vdi (Normale, 8,00 GB)

**Audio**

Driver host: Windows DirectSound
Controller: ICH AC97

**Rete**

Scheda 1: PCnet-PCI II (Scheda con bridge, Realtek PCIe GbE Family Controller)
Scheda 2: PCnet-PCI II (Scheda solo host, 'VirtualBox Host-Only Ethernet Adapter')

**USB**

Controller USB: OHCI
Filtri dispositivi: 0 (0 attivo)

**Cartelle condivise**

Nessuna

**Descrizione**

This is Metasploitable2 (Linux)
Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice common penetration testing techniques.
The default login and password is msfadmin:msfadmin.
Never expose this VM to an untrusted network (use NAT or Host-only mode if you have any questions what that means).
To contact the developers, please send email to msfdev@metasploit.com

# Metasploitable2

## Getting Started

After the virtual machine boots, login to console with username `msfadmin` and password `msfadmin`. From the shell, run the `ifconfig` command to identify the IP address.

```
msfadmin@metasploitable:~$ ifconfig

eth0      Link encap:Ethernet  HWaddr 00:0c:29:9a:52:c1
          inet addr:192.168.99.131  Bcast:192.168.99.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe9a:52c1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

# Metasploitable2

| | |
|---|---|
| `ifconfig` | per vedere indirizzo IP |
| `sudo loadkeys it` | per settare la tastiera in italiano |
| `sudo shutdown -h now` | per spegnere il sistema |
| `sudo halt` | per spegnere il sistema |

# Install Apache on Debian

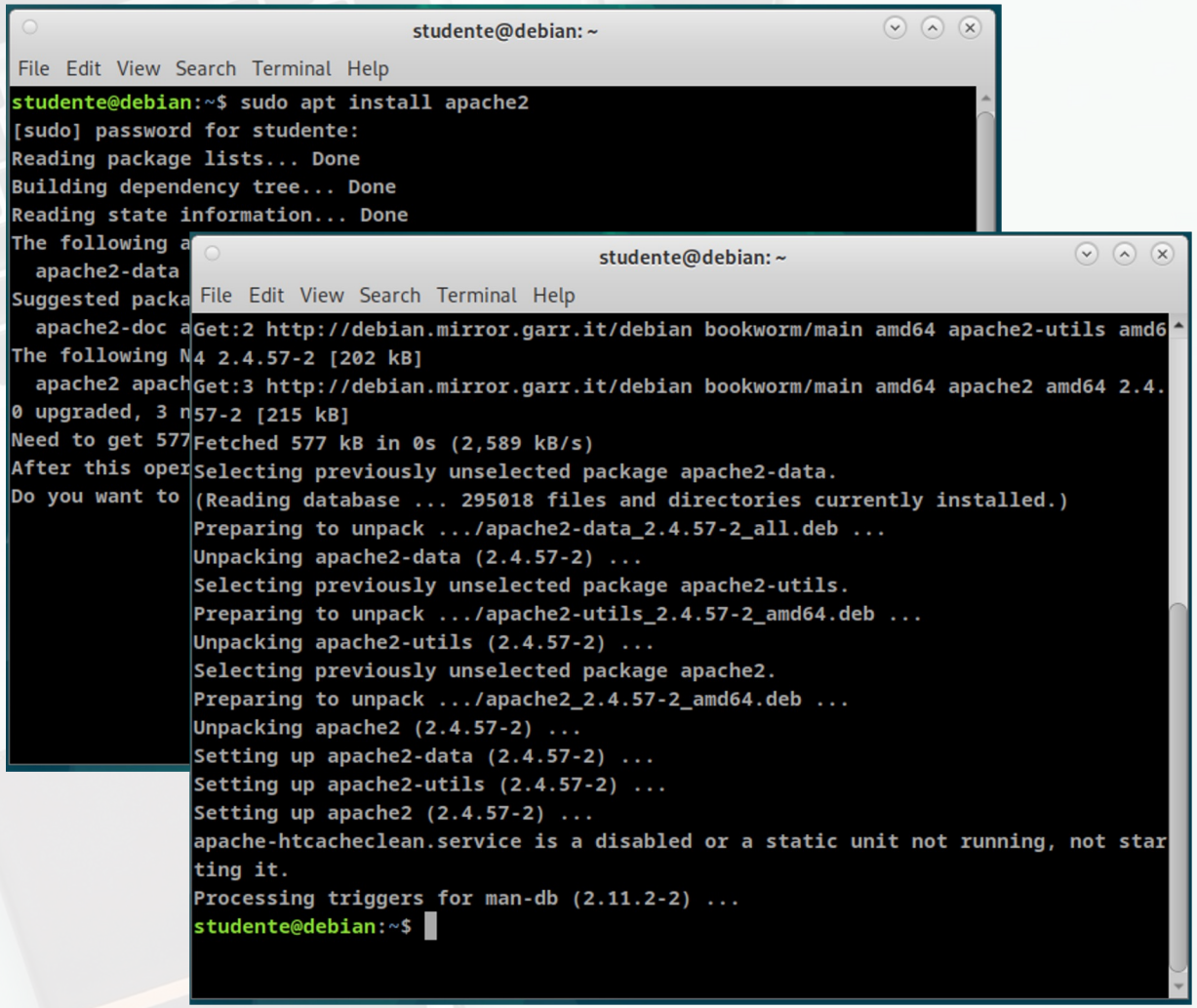
How to Enable and Disable Root User Account in Ubuntu

https://linuxize.com/post/how-to-enable-and-disable-root-user-account-in-ubuntu/

```
$ sudo apt update
$ sudo apt upgrade
$ sudo passwd root
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

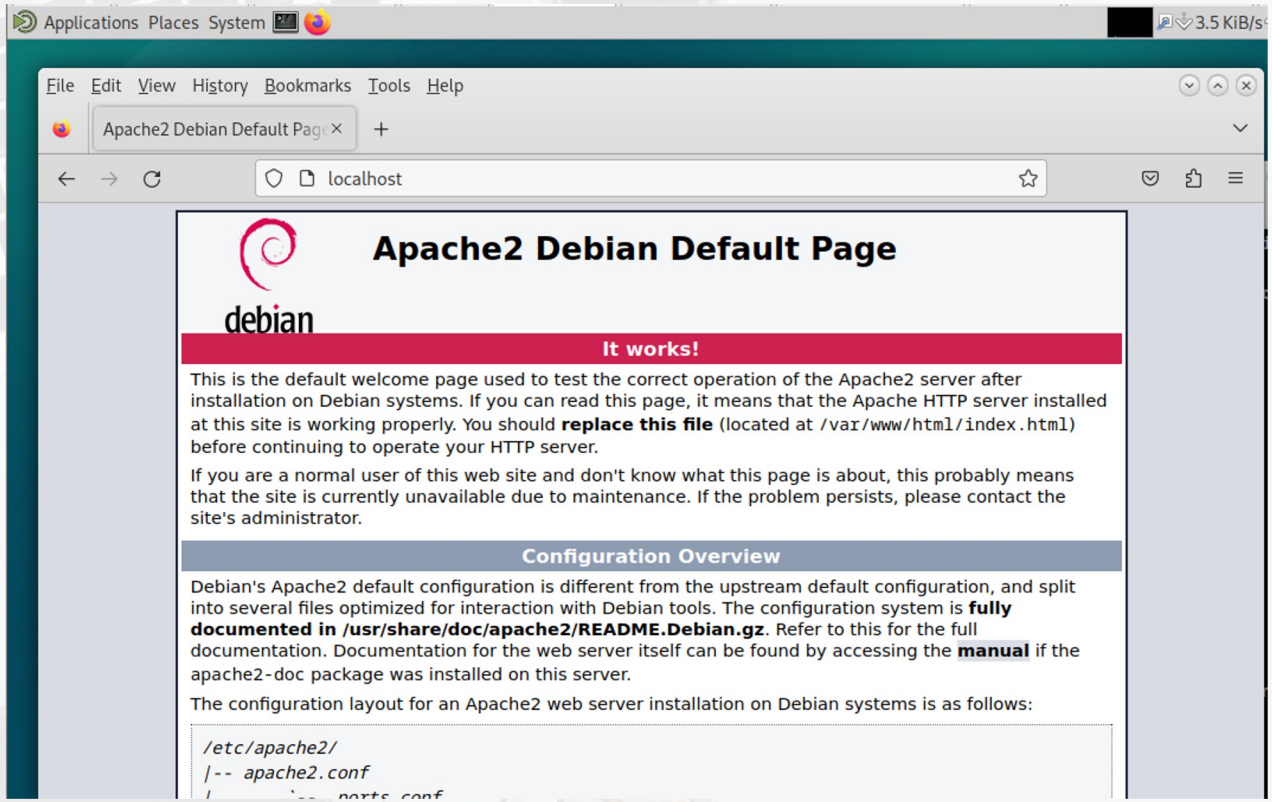
`$ ip a` *(per conoscere il proprio ip address)*

# Install Apache on Debian

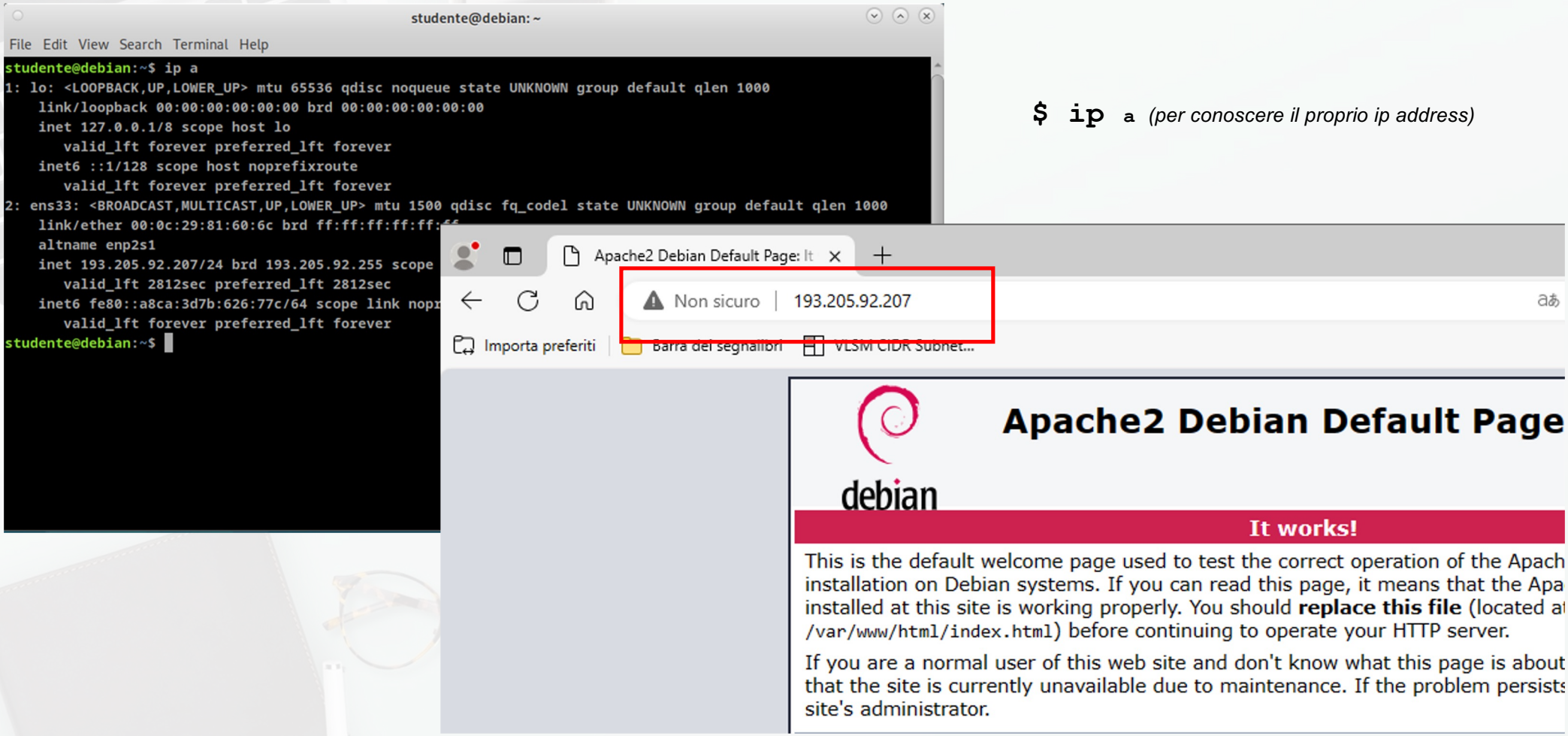



```
$ sudo apt install apache2

$ sudo systemctl status apache2

$ sudo systemctl stop apache2
$ sudo systemctl start apache2

$ sudo systemctl enable apache2
```

# Test apache - localhost

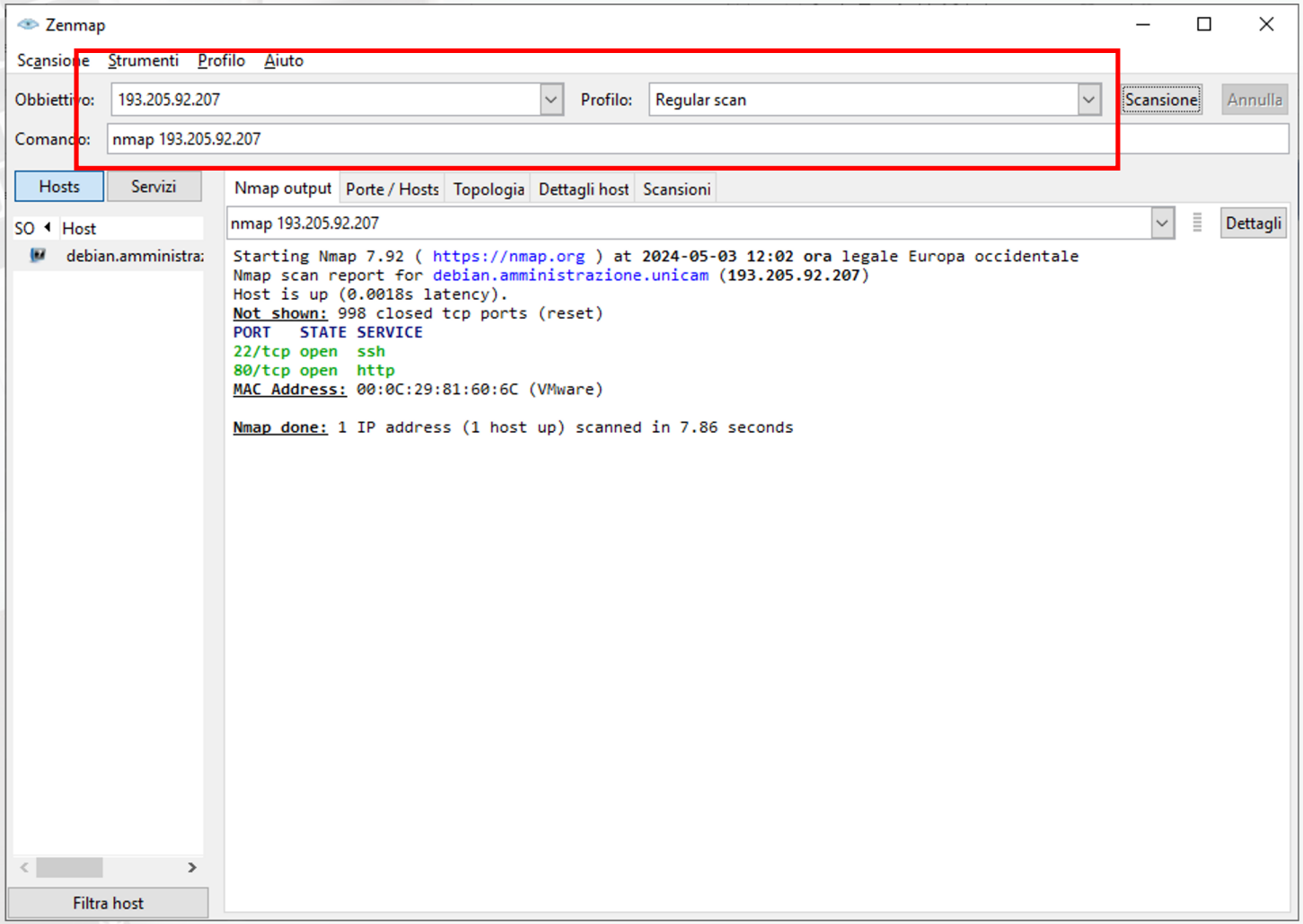


# Test apache - IP

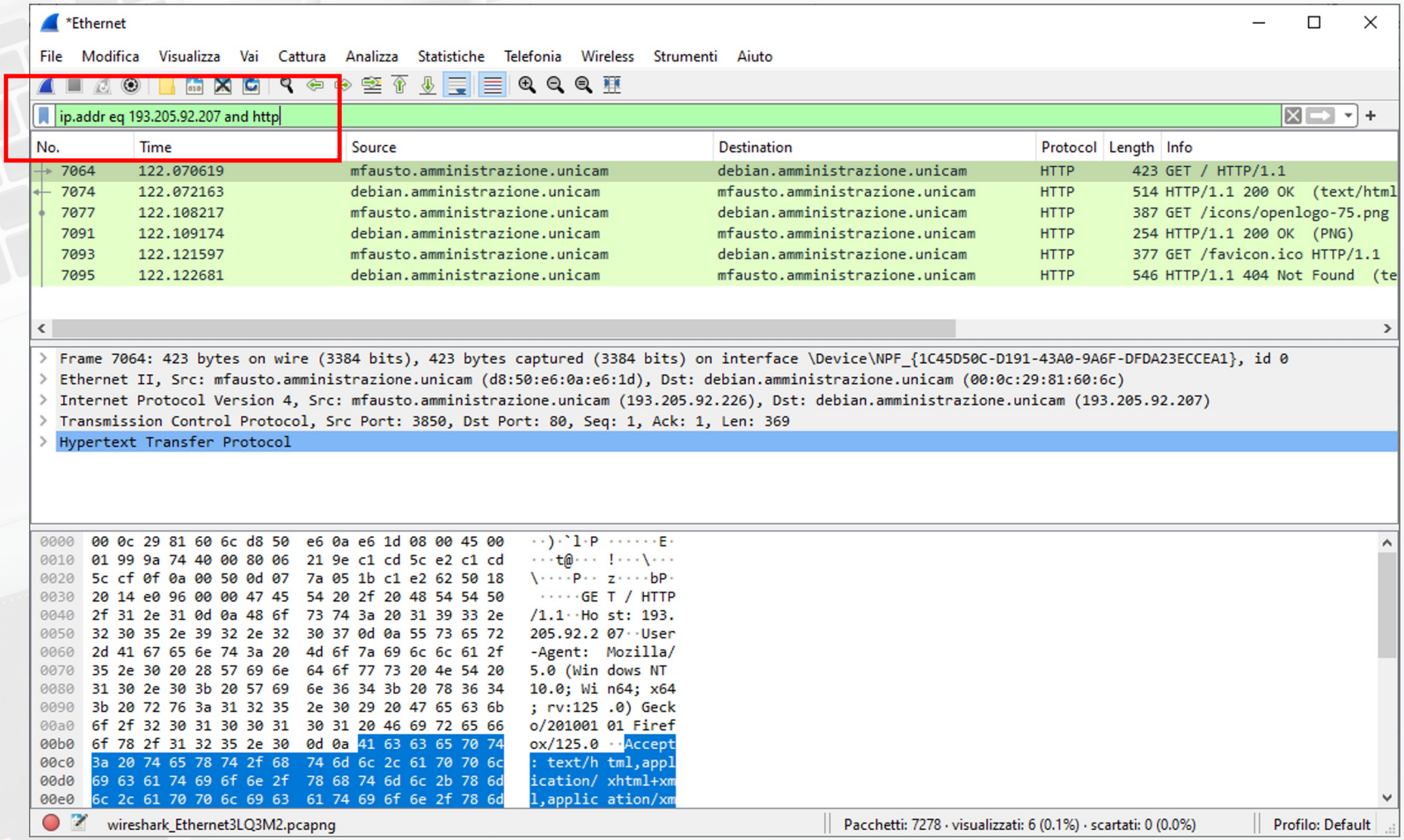



**$ ip a** *(per conoscere il proprio ip address)*

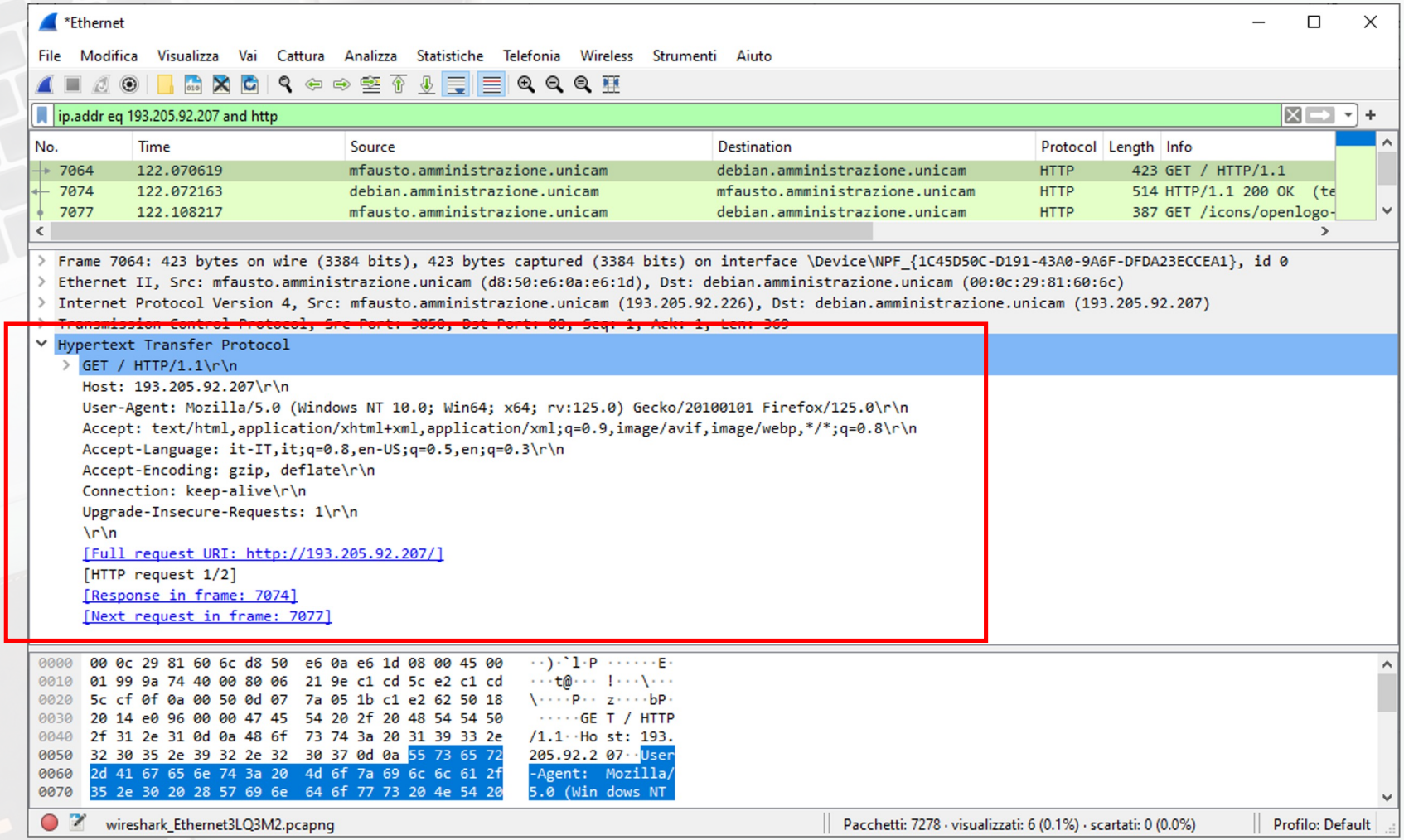
# Test apache - nmap



# Test apache - wireshark

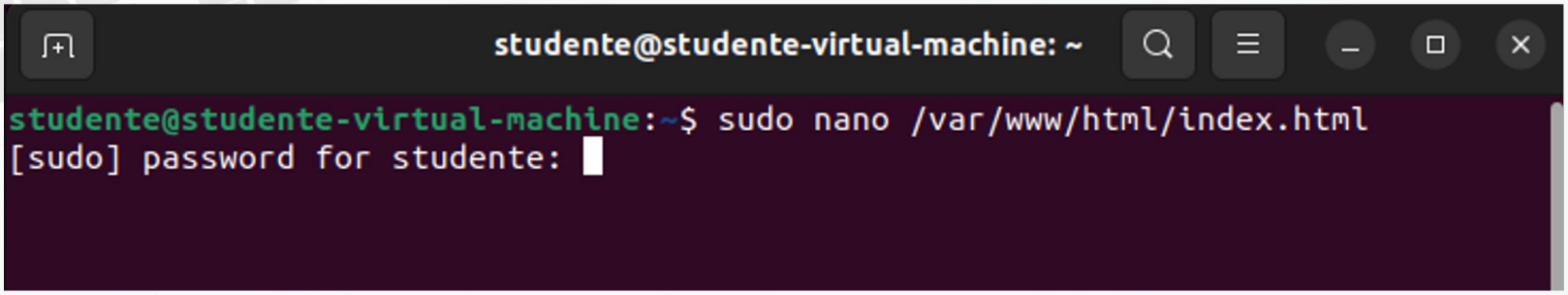


# Test apache - wireshark



# Test apache - home page

```
$ sudo nano /var/www/html/index.html
```




```
$ sudo vi /var/www/html/index.html

$ sudo gedit /var/www/html/index.html
```

# Codice javascript per visualizzare l'indirizzo ip del client browser

```
<!DOCTYPE html>
<html>
<head>
  <title>Visualizza IP Address</title>
</head>
<body>
  <h1>Il tuo indirizzo IP:</h1>
  <p id="ip-address">Sto cercando il tuo indirizzo IP...</p>
  <script type="text/javascript">
    // Funzione per ottenere l'indirizzo IP del client
    function getIpAddress() {
      fetch("https://api.ipify.org?format=json")
        .then(response => response.json())
        .then(data => {
          const ipAddress = data.ip;
          document.getElementById("ip-address").textContent = "Il tuo indirizzo IP è: " + ipAddress;
        })
        .catch(error => {
          document.getElementById("ip-address").textContent = "Impossibile ottenere l'indirizzo IP.";
        });
    }
    // Chiama la funzione per ottenere l'indirizzo IP quando la pagina si carica
    getIpAddress();
  </script>
</body>
</html>
```

# webmin

https://webmin.com/

http://doxfer.webmin.com/Webmin/Main_Page

```
sudo -s
apt install curl
curl -o setup-repos.sh https://raw.githubusercontent.com/webmin/webmin/master/setup-repos.sh
sh setup-repos.sh
apt-get install webmin --install-recommends
```

https://localhost:10000/

# Virtual Machine

FINE

# Firewall

https://opnsense.org/

https://docs.opnsense.org/

https://opnsense.org/download/

# Firewall

IPFire.org

https://www.ipfire.org/docs/installation

## Zones

A maximum of four(4) networks is possible: namely **Green**, **Blue**, **Orange** and **Red**.

| | | |
|---|---|---|
| **RED** | WAN | The external network - the connection to an Internet Service Provider (ISP) |
| **GREEN** | LAN | The local network (LAN) - an internal private network |
| **ORANGE** | DMZ | The DeMilitarized Zone - an unprotected network accessible from the internet |
| **BLUE** | WLAN | The wireless network - separate network for wireless clients |

**Note**: When using **BLUE**, it is recommended to assign it to a NIC and connect a separate access point to it. However, it is also possible to assign a **supported** wireless card **BLUE** status with the hostapd addon.
If a Blue network has been setup make sure to configure the MAC filtering on the Blue Access page.

# Firewall

https://www.ipcop.org/docs.html

https://192.168.1.1:8443.

# Firewall

FINE