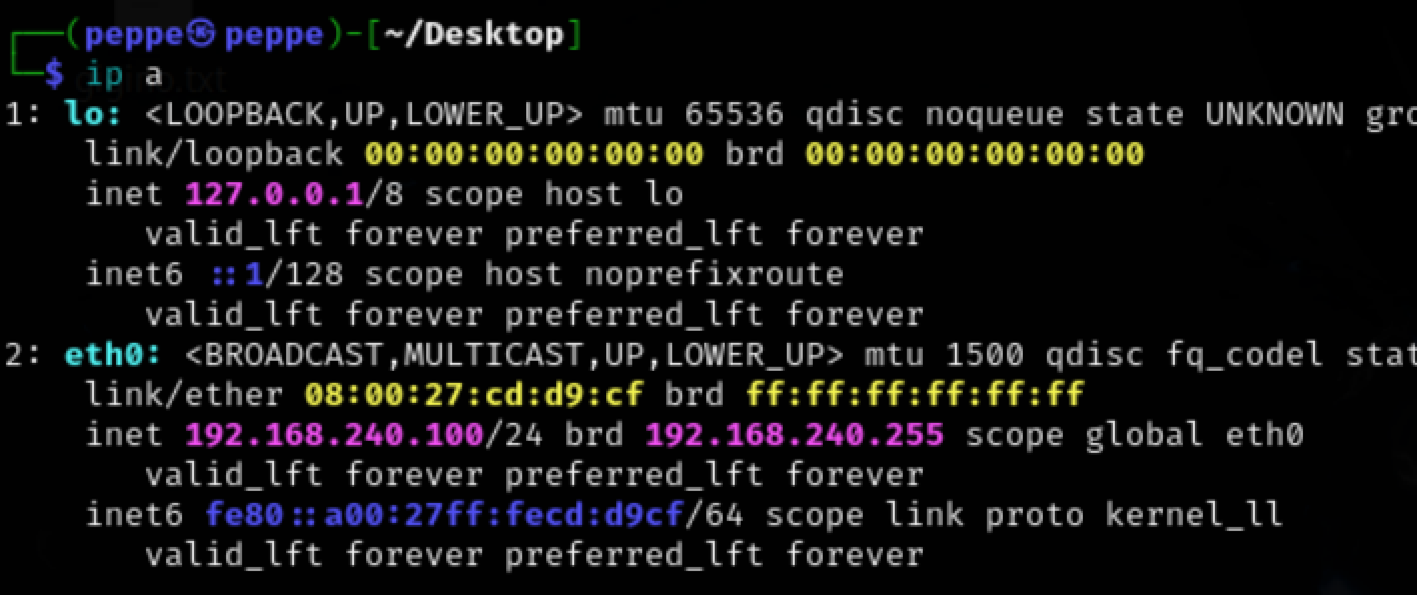
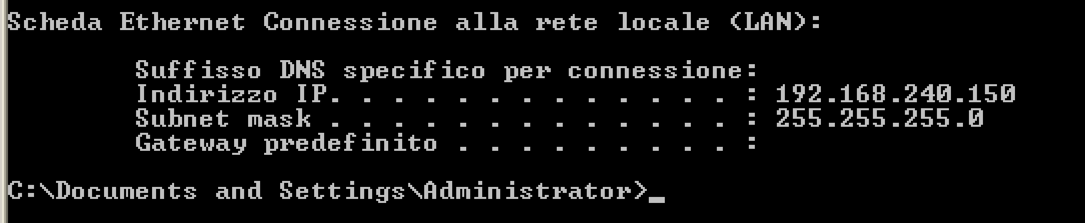
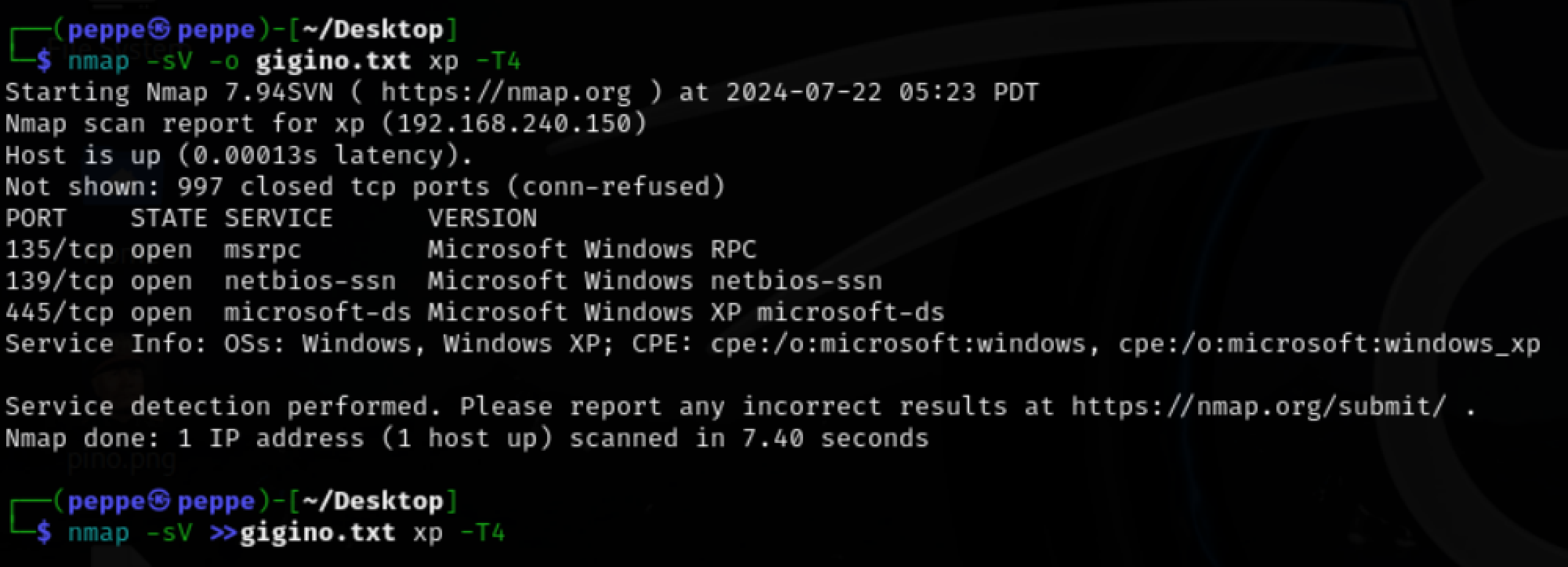


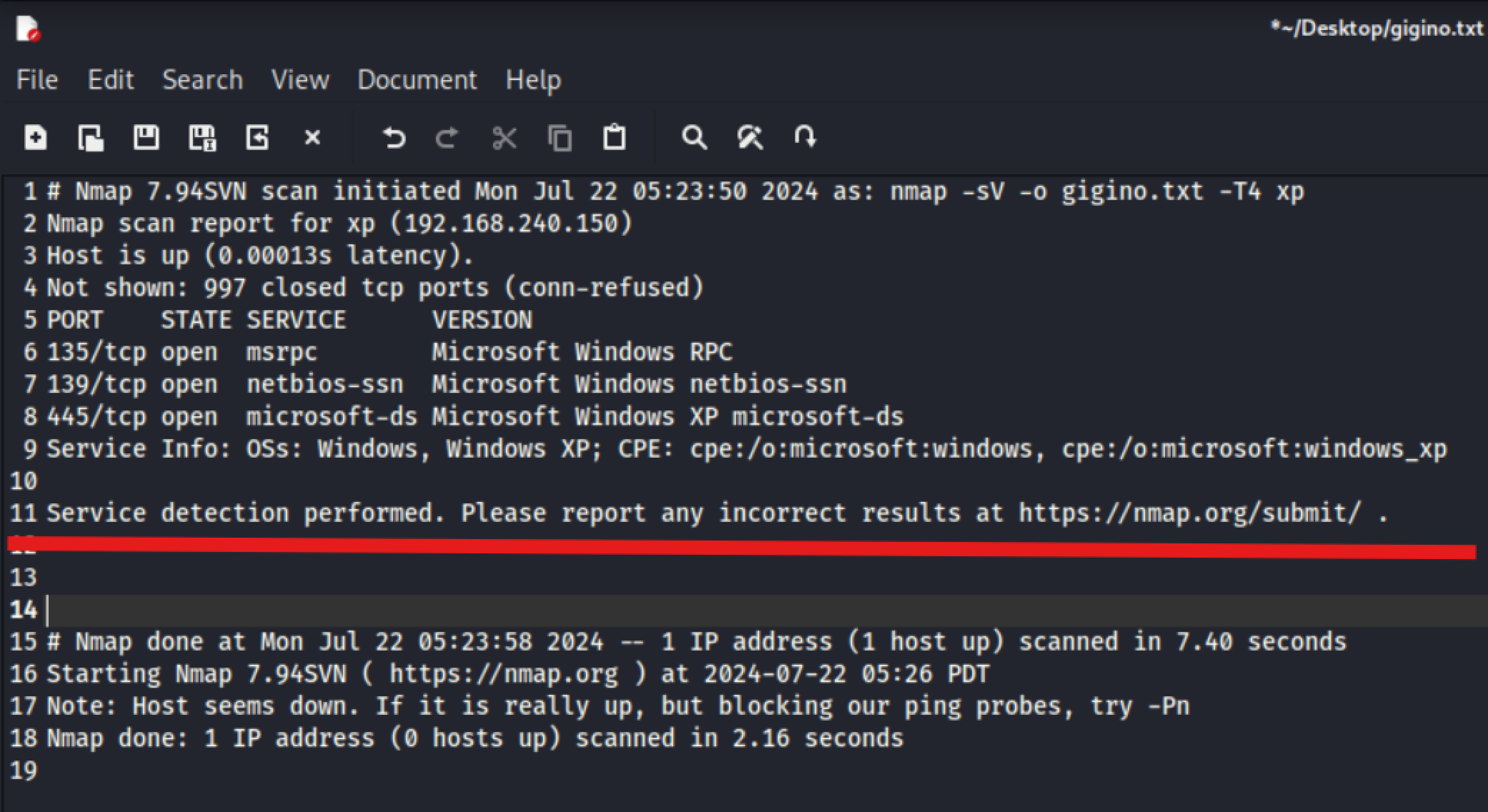
```
┌──(peppe㉿peppe)-[~/Desktop]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN gro
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel stat
    link/ether 08:00:27:cd:d9:cf brd ff:ff:ff:ff:ff:ff
    inet 192.168.240.100/24 brd 192.168.240.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fecd:d9cf/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
```



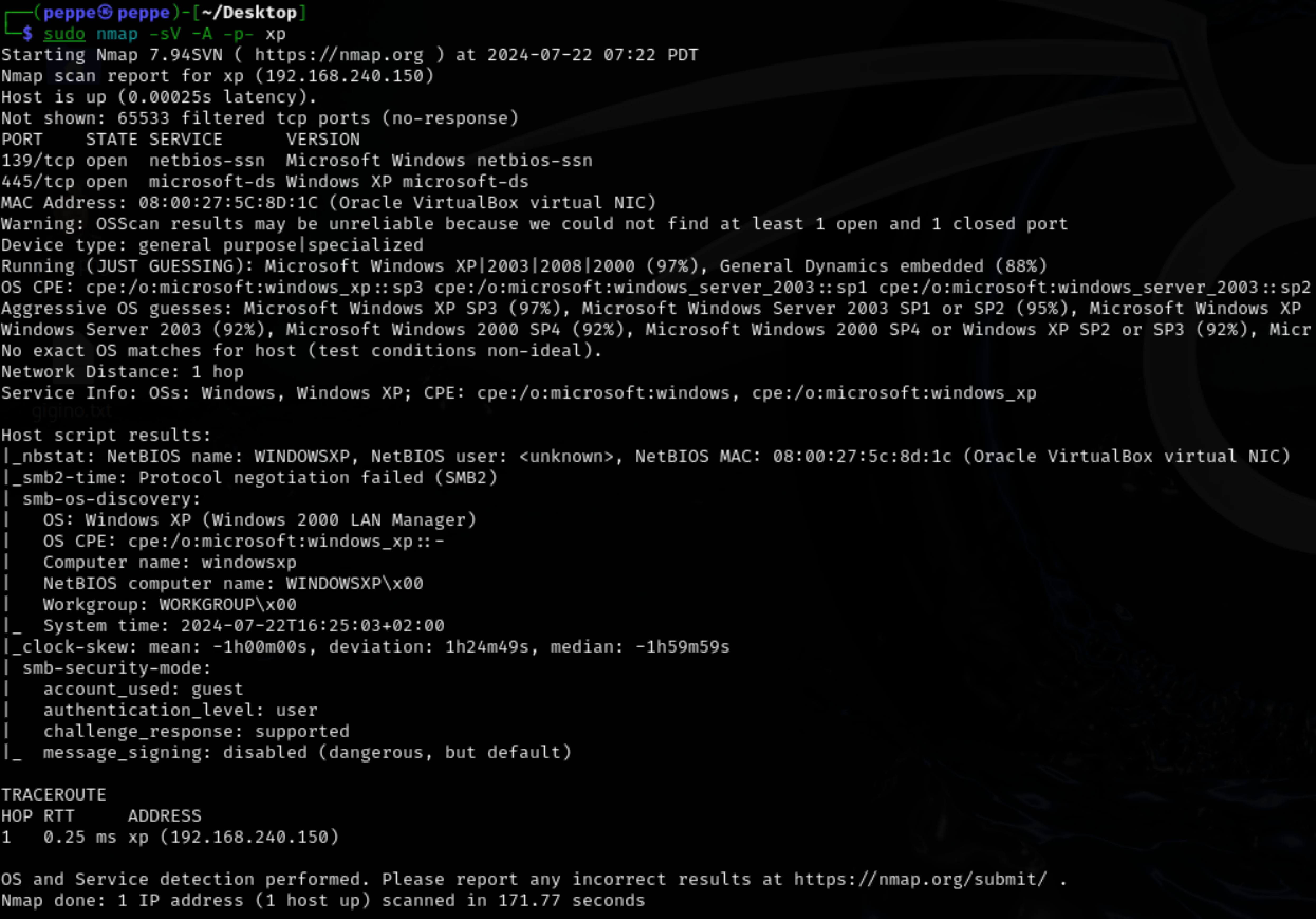
```
Scheda Ethernet Connessione alla rete locale (LAN):

        Suffisso DNS specifico per connessione:
        Indirizzo IP. . . . . . . . . . . . . : 192.168.240.150
        Subnet mask . . . . . . . . . . . . . : 255.255.255.0
        Gateway predefinito . . . . . . . . . :

C:\Documents and Settings\Administrator>_
```



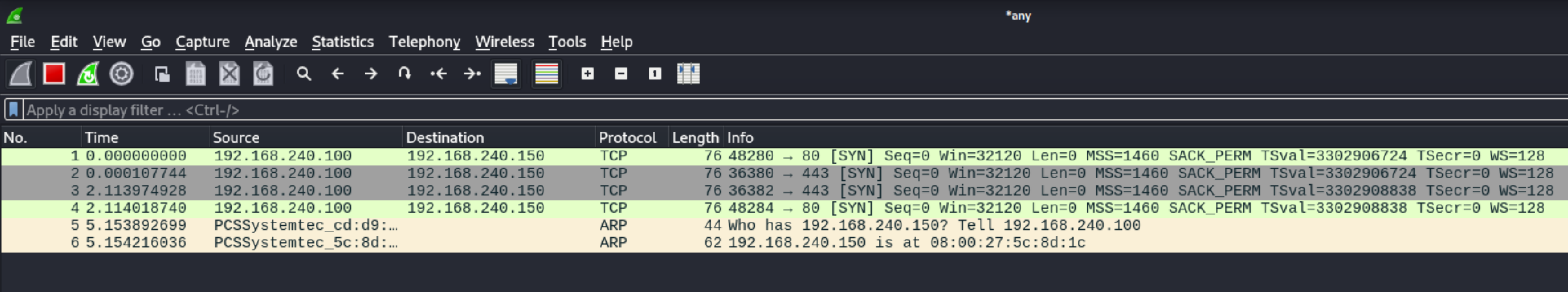
```
┌──(peppe㉿peppe)-[~/Desktop]
└─$ nmap -sV -o gigino.txt xp -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 05:23 PDT
Nmap scan report for xp (192.168.240.150)
Host is up (0.00013s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.40 seconds

┌──(peppe㉿peppe)-[~/Desktop]
└─$ nmap -sV >>gigino.txt xp -T4
```



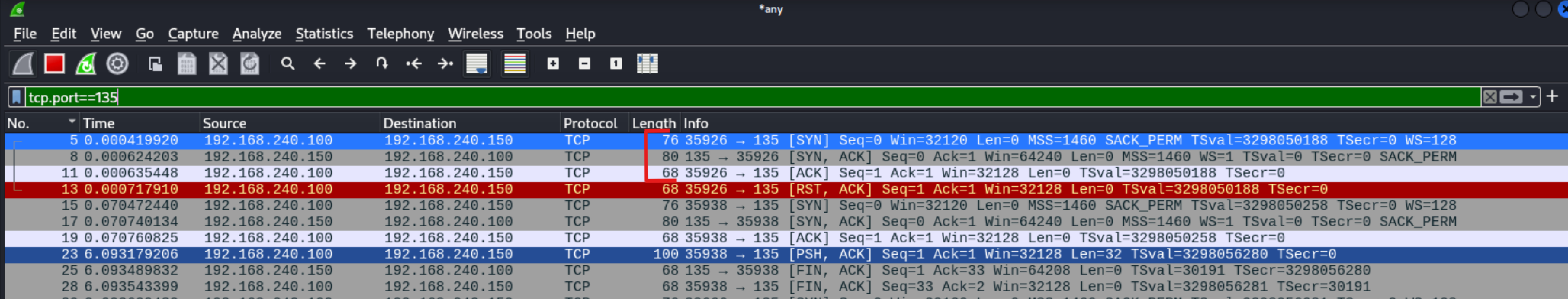
```
# Nmap 7.94SVN scan initiated Mon Jul 22 05:23:50 2024 as: nmap -sV -o gigino.txt -T4 xp
Nmap scan report for xp (192.168.240.150)
Host is up (0.00013s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .




# Nmap done at Mon Jul 22 05:23:58 2024 -- 1 IP address (1 host up) scanned in 7.40 seconds
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 05:26 PDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.16 seconds

```



```
┌──(peppe㉿peppe)-[~/Desktop]
└─$ sudo nmap -sV -A -p- xp
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 07:22 PDT
Nmap scan report for xp (192.168.240.150)
Host is up (0.00025s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT    STATE SERVICE      VERSION
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Windows XP microsoft-ds
MAC Address: 08:00:27:5C:8D:1C (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized
Running (JUST GUESSING): Microsoft Windows XP|2003|2008|2000 (97%), General Dynamics embedded (88%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2
Aggressive OS guesses: Microsoft Windows XP SP3 (97%), Microsoft Windows Server 2003 SP1 or SP2 (95%), Microsoft Windows XP
Windows Server 2003 (92%), Microsoft Windows 2000 SP4 (92%), Microsoft Windows 2000 SP4 or Windows XP SP2 or SP3 (92%), Micr
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_nbstat: NetBIOS name: WINDOWSXP, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:5c:8d:1c (Oracle VirtualBox virtual NIC)
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: windowsxp
|   NetBIOS computer name: WINDOWSXP\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-07-22T16:25:03+02:00
|_clock-skew: mean: -1h00m00s, deviation: 1h24m49s, median: -1h59m59s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT     ADDRESS
1   0.25 ms xp (192.168.240.150)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 171.77 seconds
```



```
No.  Time         Source                 Destination       Protocol Length Info
   1 0.000000000  192.168.240.100        192.168.240.150   TCP        76 48280 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3302906724 TSecr=0 WS=128
   2 0.000107744  192.168.240.100        192.168.240.150   TCP        76 36380 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3302906724 TSecr=0 WS=128
   3 2.113974928  192.168.240.100        192.168.240.150   TCP        76 36382 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3302908838 TSecr=0 WS=128
   4 2.114018740  192.168.240.100        192.168.240.150   TCP        76 48284 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3302908838 TSecr=0 WS=128
   5 5.153892699  PCSSystemtec_cd:d9:…                     ARP        44 Who has 192.168.240.150? Tell 192.168.240.100
   6 5.154216036  PCSSystemtec_5c:8d:…                     ARP        62 192.168.240.150 is at 08:00:27:5c:8d:1c
```


*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.port==135
```

```
No.   Time         Source           Destination      Protocol Length Info
    5 0.000419920  192.168.240.100  192.168.240.150  TCP       76 35926 → 135 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3298050188 TSecr=0 WS=128
    8 0.000624203  192.168.240.150  192.168.240.100  TCP       80 135 → 35926 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=1 TSval=0 TSecr=0 SACK_PERM
   11 0.000635448  192.168.240.100  192.168.240.150  TCP       68 35926 → 135 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3298050188 TSecr=0
   13 0.000717910  192.168.240.100  192.168.240.150  TCP       68 35926 → 135 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3298050188 TSecr=0
   15 0.070472440  192.168.240.100  192.168.240.150  TCP       76 35938 → 135 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=3298050258 TSecr=0 WS=128
   17 0.070740134  192.168.240.150  192.168.240.100  TCP       80 135 → 35938 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=1 TSval=0 TSecr=0 SACK_PERM
   19 0.070760825  192.168.240.100  192.168.240.150  TCP       68 35938 → 135 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3298050258 TSecr=0
   23 6.093179206  192.168.240.100  192.168.240.150  TCP      100 35938 → 135 [PSH, ACK] Seq=1 Ack=1 Win=32128 Len=32 TSval=3298056280 TSecr=0
   25 6.093489832  192.168.240.150  192.168.240.100  TCP       68 135 → 35938 [FIN, ACK] Seq=1 Ack=33 Win=64208 Len=0 TSval=30191 TSecr=3298056280
   28 6.093543399  192.168.240.100  192.168.240.150  TCP       68 35938 → 135 [FIN, ACK] Seq=33 Ack=2 Win=32128 Len=0 TSval=3298056281 TSecr=30191
```