Indirizzo IP Kali Linux

```
┌──(kali㉿kali)-[~]
└─$ ip a
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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:43:73:bc brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.100/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
       valid_lft 6338sec preferred_lft 6338sec
    inet6 fe80::a638:973e:856e:1b37/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Indirizzo IP Windows 7

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

   Suffisso DNS specifico per connessione: home.arpa
   Indirizzo IPv6 locale rispetto al collegamento . : fe80::d971:5b4b:8bc6:c8a3%
11
   Indirizzo IPv4. . . . . . . . . . . . : 192.168.50.101
   Subnet mask . . . . . . . . . . . . . : 255.255.255.0
   Gateway predefinito . . . . . . . . . : 192.168.50.1

Scheda Tunnel isatap.home.arpa:

   Stato supporto. . . . . . . . . . . . : Supporto disconnesso
   Suffisso DNS specifico per connessione: home.arpa
```

OS fingerprint con output reports in diversi formati:

La voce ‘Network Distance: 2 hops’ indica che le due macchine sono su reti diverse.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -oN fingerprint_scan -oX fingerprint_scan.xml -oS fingerprint_scriptk -O 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2024-07-20 04:57 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0016s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49159/tcp open  unknown
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS CPE: cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_7
OS details: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.44 seconds
```

~/fingerprint_scan [Read Only] - Mousepad

File Edit Search View Document Help

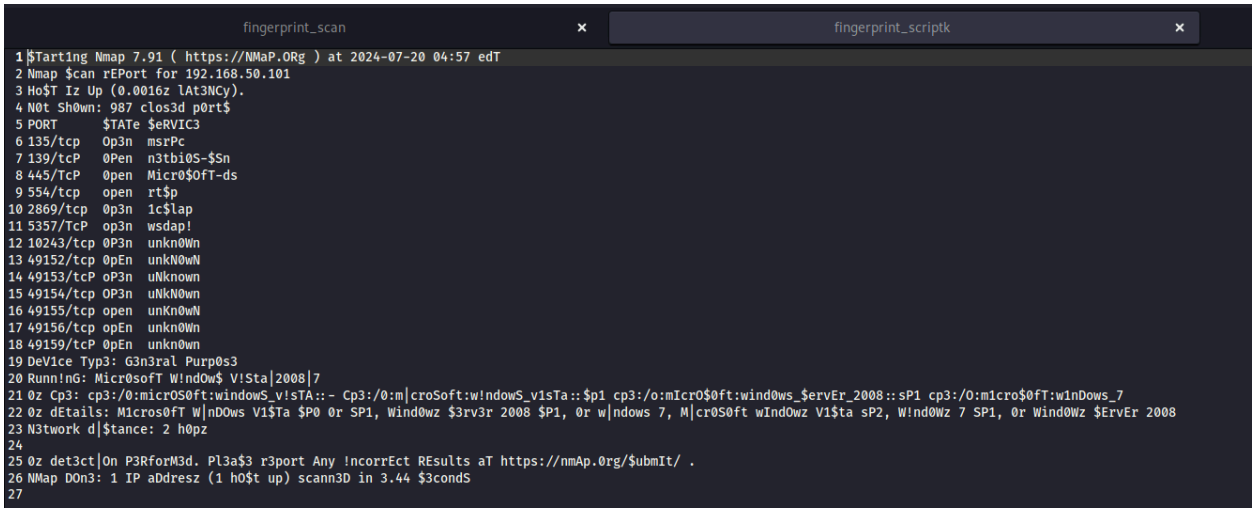
```
1 # Nmap 7.91 scan initiated Sat Jul 20 04:57:01 2024 as: nmap -oN fingerprint_scan -oX fingerprint_scan.xml -oS fingerprint_scriptk -O 192.168.50.101
2 Nmap scan report for 192.168.50.101
3 Host is up (0.0016s latency).
4 Not shown: 987 closed ports
5 PORT      STATE SERVICE
6 135/tcp   open  msrpc
7 139/tcp   open  netbios-ssn
8 445/tcp   open  microsoft-ds
9 554/tcp   open  rtsp
10 2869/tcp  open  icslap
11 5357/tcp  open  wsdapi
12 10243/tcp open  unknown
13 49152/tcp open  unknown
14 49153/tcp open  unknown
15 49154/tcp open  unknown
16 49155/tcp open  unknown
17 49156/tcp open  unknown
18 49159/tcp open  unknown
19 Device type: general purpose
20 Running: Microsoft Windows Vista|2008|7
21 OS CPE: cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_7
22 OS details: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
23 Network Distance: 2 hops
24
25 OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
26 # Nmap done at Sat Jul 20 04:57:04 2024 -- 1 IP address (1 host up) scanned in 3.44 seconds
27
```

/home/kali/fingerprint_scan

file:///home/kali/fingerprint_scan.xml

Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

cpe:/o:microsoft:windows_vista::-cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_vista::sp2 cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008



SYN scan con report:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -oN syn_scan -sS 192.168.50.101
Starting Nmap 7.91 ( https://nmap.org ) at 2024-07-20 04:59 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0016s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49159/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.45 seconds
```

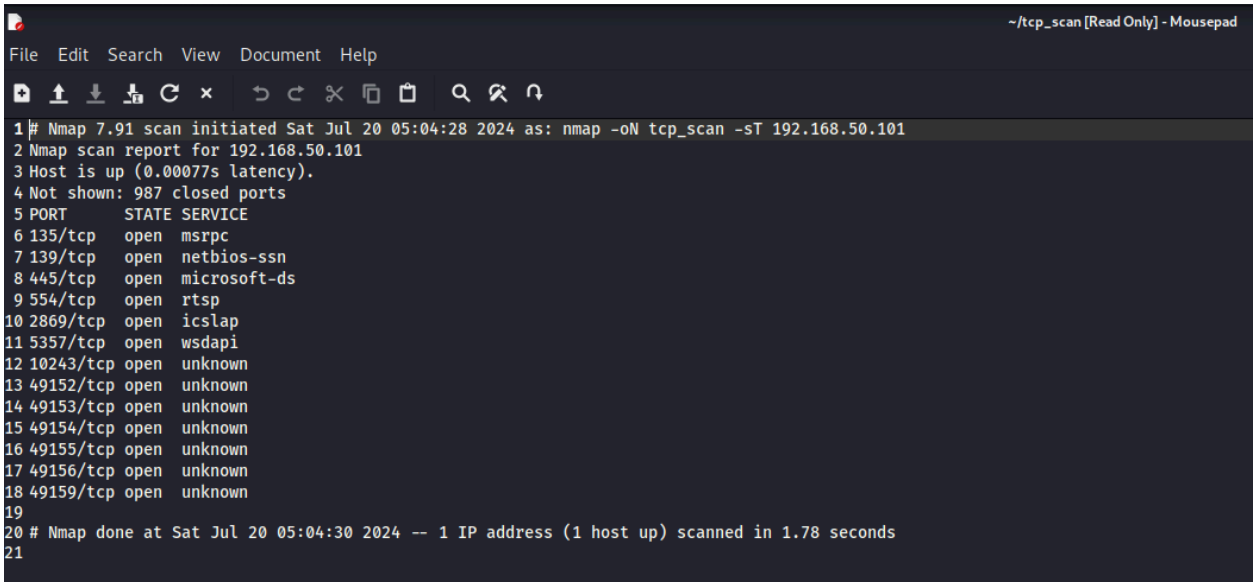
~/syn_scan [Read Only] - Mousepad

File Edit Search View Document Help

```
1 # Nmap 7.91 scan initiated Sat Jul 20 04:59:32 2024 as: nmap -oN syn_scan -sS 192.168.50.101
2 Nmap scan report for 192.168.50.101
3 Host is up (0.0016s latency).
4 Not shown: 987 closed ports
5 PORT      STATE SERVICE
6 135/tcp   open  msrpc
7 139/tcp   open  netbios-ssn
8 445/tcp   open  microsoft-ds
9 554/tcp   open  rtsp
10 2869/tcp  open  icslap
11 5357/tcp  open  wsdapi
12 10243/tcp open  unknown
13 49152/tcp open  unknown
14 49153/tcp open  unknown
15 49154/tcp open  unknown
16 49155/tcp open  unknown
17 49156/tcp open  unknown
18 49159/tcp open  unknown
19
20 # Nmap done at Sat Jul 20 04:59:34 2024 -- 1 IP address (1 host up) scanned in 1.45 seconds
21
```

TCP scan con report:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -oN tcp_scan -sT 192.168.50.101
Starting Nmap 7.91 ( https://nmap.org ) at 2024-07-20 05:04 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00077s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49159/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.78 seconds
```



Version detection:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.101
Starting Nmap 7.91 ( https://nmap.org ) at 2024-07-20 05:05 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0010s latency).
Not shown: 987 closed ports
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 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49159/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: UTENTE-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 127.31 seconds
```

Macchine sulla stessa rete:

```
C:\Users\utente>ipconfig

Configurazione IP di Windows


Scheda Ethernet Connessione alla rete locale (LAN):

   Suffisso DNS specifico per connessione: lan
   Indirizzo IPv6 locale rispetto al collegamento . : fe80::d971:5b4b:8bc6:c8a3%
11
   Indirizzo IPv4. . . . . . . . . . . . : 192.168.32.101
   Subnet mask . . . . . . . . . . . . . : 255.255.255.0
   Gateway predefinito . . . . . . . . . : fe80::a00:27ff:fe58:b2dd%11
                                           192.168.32.255

Scheda Tunnel isatap.{3471EE44-5A46-42A3-BB36-A869097FC1E8}:

   Stato supporto. . . . . . . . . . . . : Supporto disconnesso
   Suffisso DNS specifico per connessione: lan
```

```
┌──(kali㉿kali)-[~]
└─$ ip a
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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:43:73:bc brd ff:ff:ff:ff:ff:ff
    inet 192.168.32.100/24 brd 192.168.32.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::9f55:75c3:951a:6b53/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

OS fingerprint:

Dato che ora le macchine sono sulla stessa rete, la voce Network Distance indica un solo salto

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.32.101
Starting Nmap 7.91 ( https://nmap.org ) at 2024-07-20 05:16 EDT
Nmap scan report for 192.168.32.101
Host is up (0.00049s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49159/tcp open  unknown
MAC Address: 08:00:27:69:C4:C9 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.40 seconds
```

SYN scan:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.32.101
Starting Nmap 7.91 ( https://nmap.org ) at 2024-07-20 05:17 EDT
Nmap scan report for 192.168.32.101
Host is up (0.00077s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49159/tcp open  unknown
MAC Address: 08:00:27:69:C4:C9 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 15.67 seconds
```

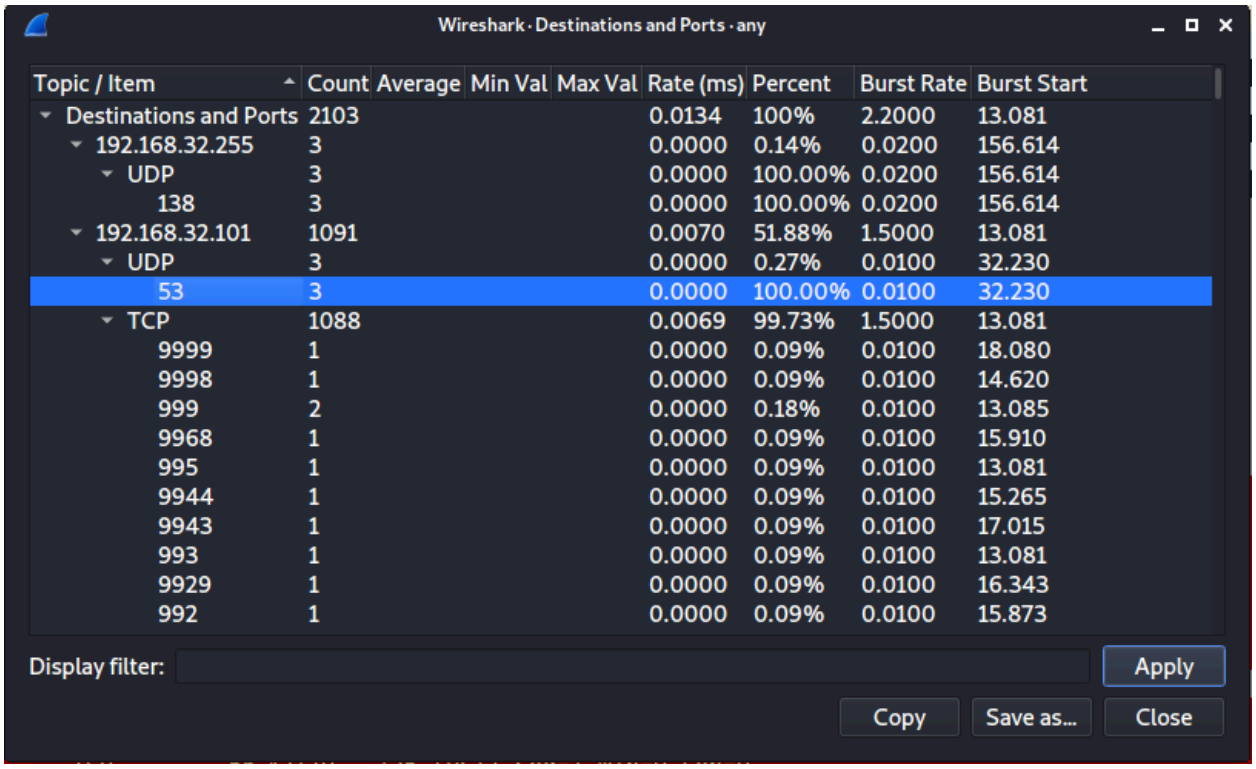
TCP scan:

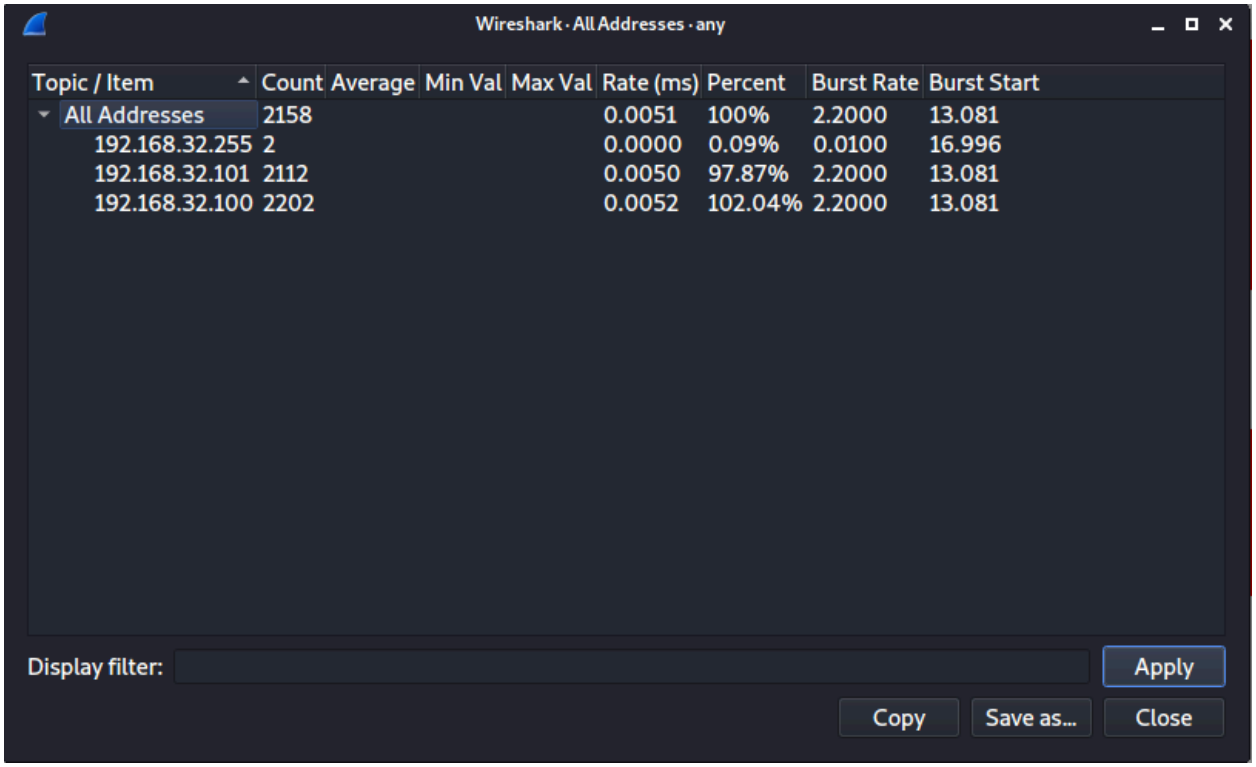
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.32.101
Starting Nmap 7.91 ( https://nmap.org ) at 2024-07-20 05:18 EDT
Nmap scan report for 192.168.32.101
Host is up (0.00083s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49159/tcp open  unknown
MAC Address: 08:00:27:69:C4:C9 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.90 seconds
```

Version detection:

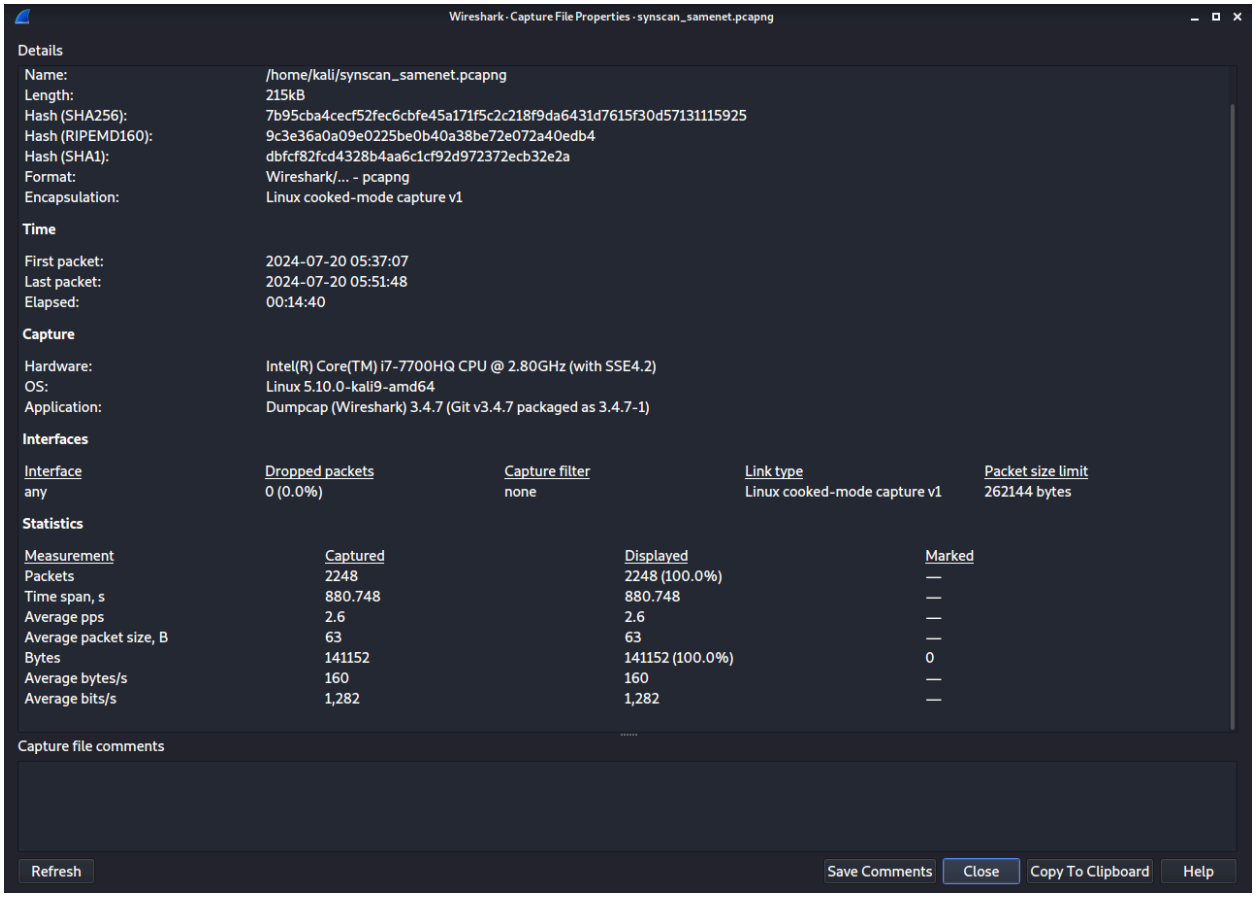
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.32.101
Starting Nmap 7.91 ( https://nmap.org ) at 2024-07-20 05:20 EDT
Nmap scan report for 192.168.32.101
Host is up (0.00087s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49159/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:69:C4:C9 (Oracle VirtualBox virtual NIC)
Service Info: Host: UTENTE-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 145.65 seconds
```

Stessa rete, cattura con WireShark durante SYN SCAN

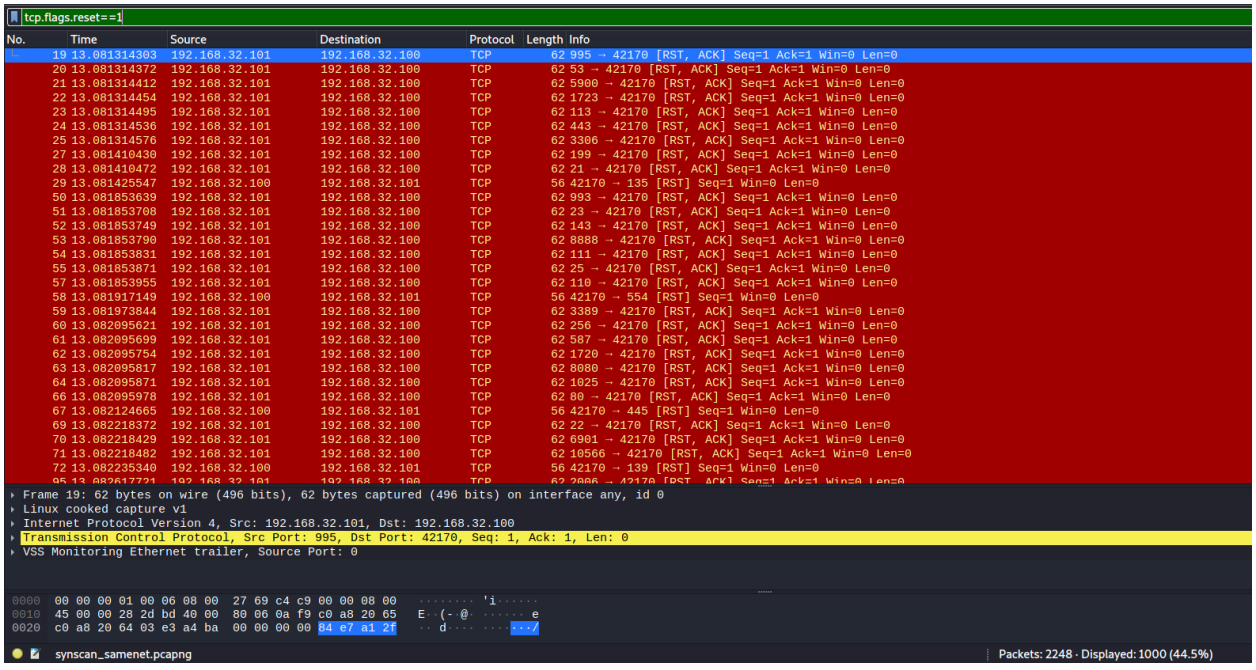




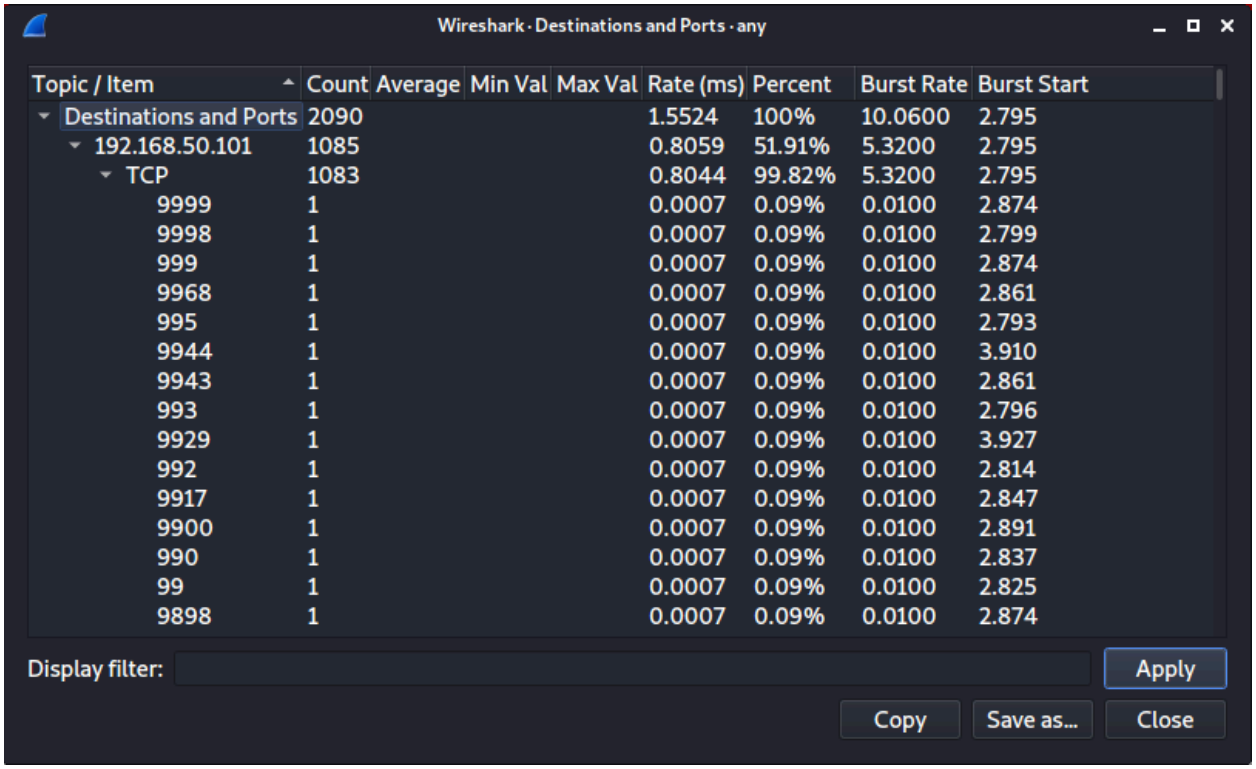
SYN SCAN - stessa rete - Statistiche Wireshark

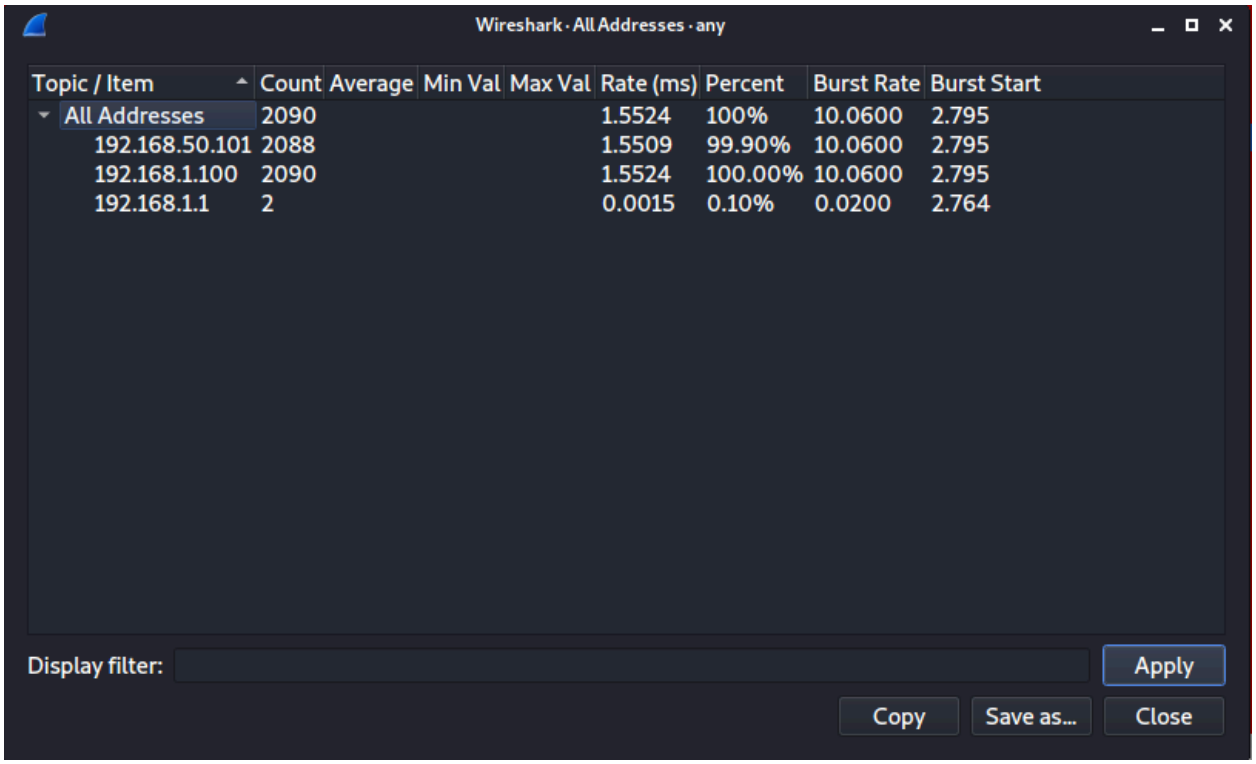


Stessa rete - SYN SCAN - Numero di RST

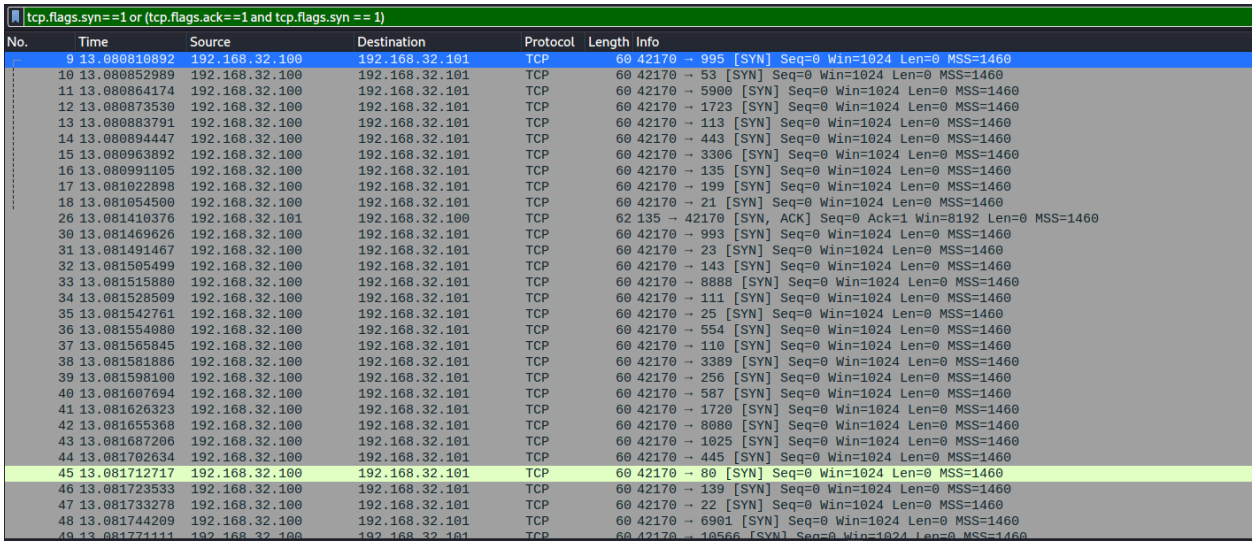


Reti diverse - SYN SCAN - Statistiche cattura Wireshark

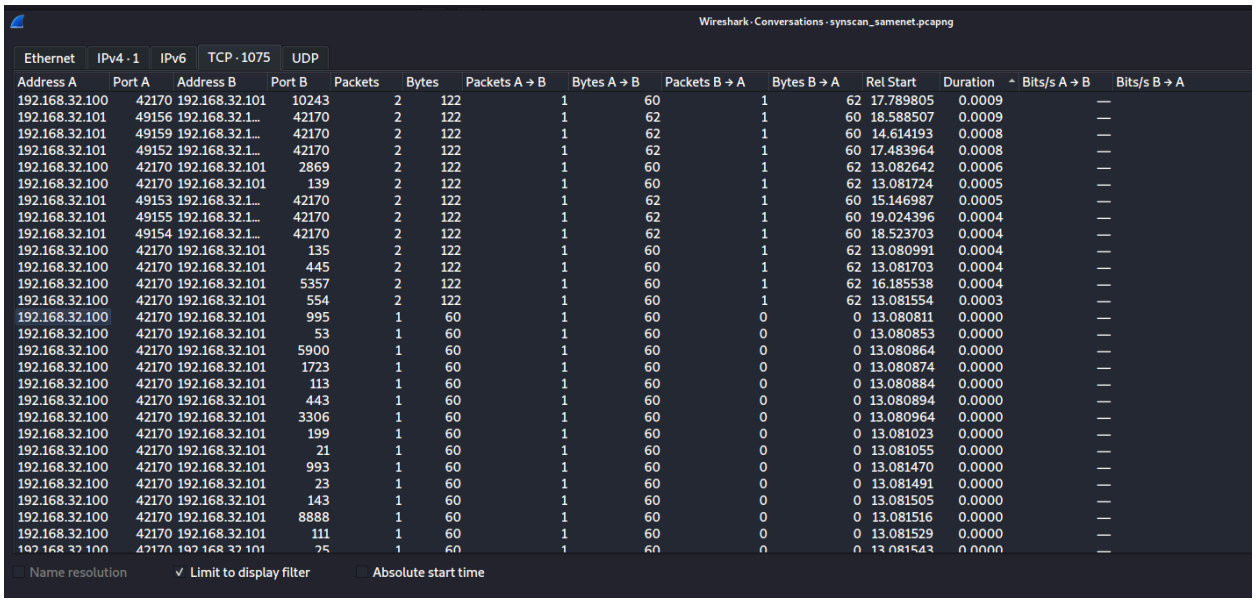




Stessa rete - Filtro per visualizzare solo statistiche per SYN e SYN/ACK



Stessa rete - Statistiche flag senza risposta e tempo di risposta



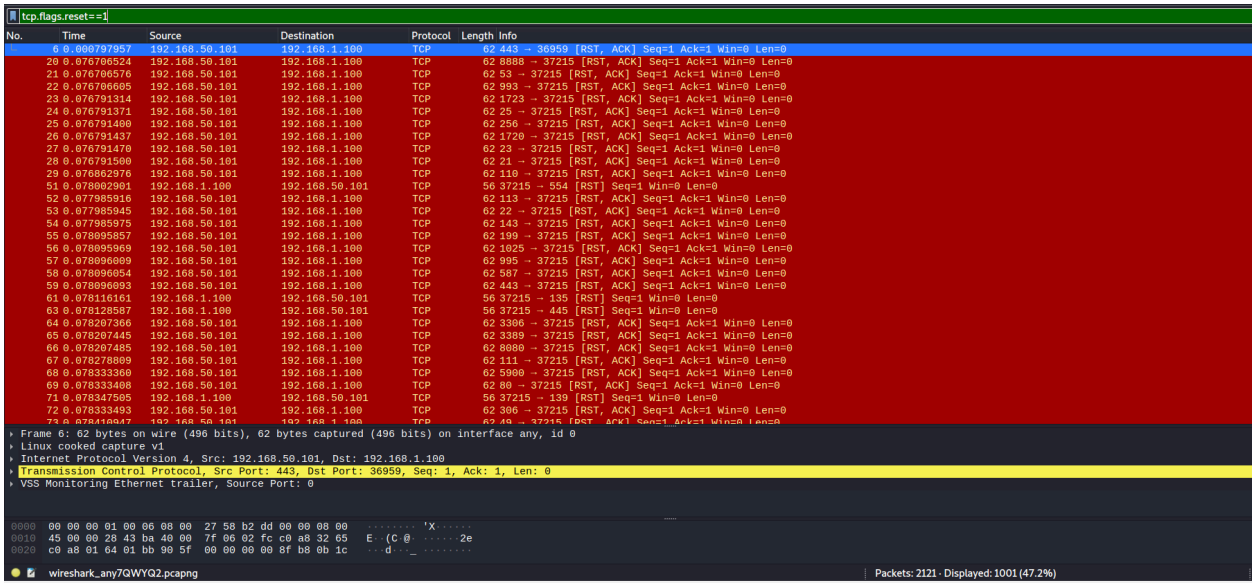
Wireshark · Conversations · synscan_samenet.pcapng

Ethernet | IPv4 · 1 | IPv6 | TCP · 1075 | UDP

Address A	Port A	Address B	Port 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
192.168.32.100	42170	192.168.32.101	10243	2	122	1	60	1	62	17.789805	0.0009		
192.168.32.101	49156	192.168.32.1…	42170	2	122	1	62	1	60	18.588507	0.0009		
192.168.32.101	49159	192.168.32.1…	42170	2	122	1	62	1	60	14.614193	0.0008		
192.168.32.101	49152	192.168.32.1…	42170	2	122	1	62	1	60	17.483964	0.0008		
192.168.32.100	42170	192.168.32.101	2869	2	122	1	60	1	62	13.082642	0.0006		
192.168.32.100	42170	192.168.32.101	139	2	122	1	60	1	62	13.081724	0.0005		
192.168.32.101	49153	192.168.32.1…	42170	2	122	1	62	1	60	15.146987	0.0005		
192.168.32.101	49155	192.168.32.1…	42170	2	122	1	62	1	60	19.024396	0.0004		
192.168.32.101	49154	192.168.32.1…	42170	2	122	1	62	1	60	18.523703	0.0004		
192.168.32.100	42170	192.168.32.101	135	2	122	1	60	1	62	13.080991	0.0004		
192.168.32.100	42170	192.168.32.101	445	2	122	1	60	1	62	13.081703	0.0004		
192.168.32.100	42170	192.168.32.101	5357	2	122	1	60	1	62	16.185538	0.0004		
192.168.32.100	42170	192.168.32.101	554	2	122	1	60	1	62	13.081554	0.0003		
192.168.32.100	42170	192.168.32.101	995	1	60	1	60	0	0	13.080811	0.0000		
192.168.32.100	42170	192.168.32.101	53	1	60	1	60	0	0	13.080853	0.0000		
192.168.32.100	42170	192.168.32.101	5900	1	60	1	60	0	0	13.080864	0.0000		
192.168.32.100	42170	192.168.32.101	1723	1	60	1	60	0	0	13.080874	0.0000		
192.168.32.100	42170	192.168.32.101	113	1	60	1	60	0	0	13.080884	0.0000		
192.168.32.100	42170	192.168.32.101	443	1	60	1	60	0	0	13.080894	0.0000		
192.168.32.100	42170	192.168.32.101	3306	1	60	1	60	0	0	13.080964	0.0000		
192.168.32.100	42170	192.168.32.101	199	1	60	1	60	0	0	13.081023	0.0000		
192.168.32.100	42170	192.168.32.101	21	1	60	1	60	0	0	13.081055	0.0000		
192.168.32.100	42170	192.168.32.101	993	1	60	1	60	0	0	13.081470	0.0000		
192.168.32.100	42170	192.168.32.101	23	1	60	1	60	0	0	13.081491	0.0000		
192.168.32.100	42170	192.168.32.101	143	1	60	1	60	0	0	13.081505	0.0000		
192.168.32.100	42170	192.168.32.101	8888	1	60	1	60	0	0	13.081516	0.0000		
192.168.32.100	42170	192.168.32.101	111	1	60	1	60	0	0	13.081529	0.0000		
192.168.32.100	42170	192.168.32.101	25	1	60	1	60	0	0	13.081543	0.0000		

Name resolution ✓ Limit to display filter Absolute start time

Reti diverse - SYN SCAN - Numero di RST



tcp.flags.reset==1

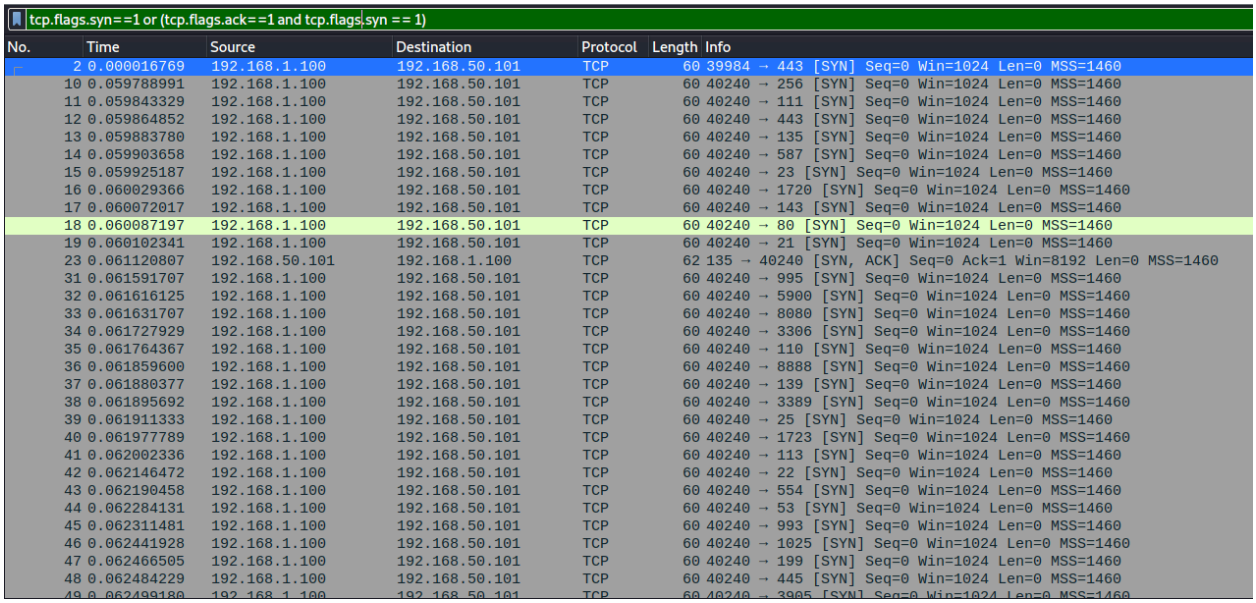
No.	Time	Source	Destination	Protocol	Length	Info
6	0.000797957	192.168.50.101	192.168.1.100	TCP	62	443 → 36959 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
20	0.076706524	192.168.50.101	192.168.1.100	TCP	62	8888 → 37215 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
21	0.076706576	192.168.50.101	192.168.1.100	TCP	62	53 → 37215 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	0.076706605	192.168.50.101	192.168.1.100	TCP	62	993 → 37215 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	0.076791314	192.168.50.101	192.168.1.100	TCP	62	1723 → 37215 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	0.076791371	192.168.50.101	192.168.1.100	TCP	62	25 → 37215 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	0.076791400	192.168.50.101	192.168.1.100	TCP	62	256 → 37215 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
26	0.076791437	192.168.50.101	192.168.1.100	TCP	62	1720 → 37215 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	0.076791470	192.168.50.101	192.168.1.100	TCP	62	23 → 37215 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
28	0.076791500	192.168.50.101	192.168.1.100	TCP	62	21 → 37215 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
29	0.076862976	192.168.50.101	192.168.1.100	TCP	62	110 → 37215 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
51	0.078002901	192.168.1.100	192.168.50.101	TCP	56	37215 → 554 [RST] Seq=1 Win=0 Len=0
52	0.077985916	192.168.50.101	192.168.1.100	TCP	62	113 → 37215 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
53	0.077985945	192.168.50.101	192.168.1.100	TCP	62	22 → 37215 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
54	0.077985975	192.168.50.101	192.168.1.100	TCP	62	143 → 37215 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
55	0.078095857	192.168.50.101	192.168.1.100	TCP	62	199 → 37215 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
56	0.078095969	192.168.50.101	192.168.1.100	TCP	62	1025 → 37215 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
57	0.078096009	192.168.50.101	192.168.1.100	TCP	62	995 → 37215 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
58	0.078096054	192.168.50.101	192.168.1.100	TCP	62	587 → 37215 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59	0.078096093	192.168.50.101	192.168.1.100	TCP	62	443 → 37215 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61	0.078116161	192.168.1.100	192.168.50.101	TCP	56	37215 → 135 [RST] Seq=1 Win=0 Len=0
63	0.078128587	192.168.1.100	192.168.50.101	TCP	56	37215 → 445 [RST] Seq=1 Win=0 Len=0
64	0.078207366	192.168.50.101	192.168.1.100	TCP	62	3306 → 37215 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
65	0.078207445	192.168.50.101	192.168.1.100	TCP	62	3389 → 37215 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
66	0.078207485	192.168.50.101	192.168.1.100	TCP	62	8080 → 37215 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
67	0.078278809	192.168.50.101	192.168.1.100	TCP	62	111 → 37215 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
68	0.078333360	192.168.50.101	192.168.1.100	TCP	62	5900 → 37215 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
69	0.078333408	192.168.50.101	192.168.1.100	TCP	62	80 → 37215 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
71	0.078347505	192.168.1.100	192.168.50.101	TCP	56	37215 → 139 [RST] Seq=1 Win=0 Len=0
72	0.078333493	192.168.50.101	192.168.1.100	TCP	62	306 → 37215 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

▸ Frame 6: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface any, id 0
▸ Linux cooked capture v1
▸ Internet Protocol Version 4, Src: 192.168.50.101, Dst: 192.168.1.100
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 36959, Seq: 1, Ack: 1, Len: 0
▸ VSS Monitoring Ethernet trailer, Source Port: 0

```
0000  00 00 00 01 00 06 08 00  27 58 b2 dd 00 00 08 00   ........ 'X......
0010  45 00 00 28 43 ba 40 00  7f 06 02 fc c0 a8 32 65   E..(C.@. ......2e
0020  c0 a8 01 64 01 bb 90 5f  00 00 00 00 8f b8 0b 1c   ...d..._ ........
```

wireshark_any7QWYQ2.pcapng Packets: 2121 · Displayed: 1001 (47.2%)

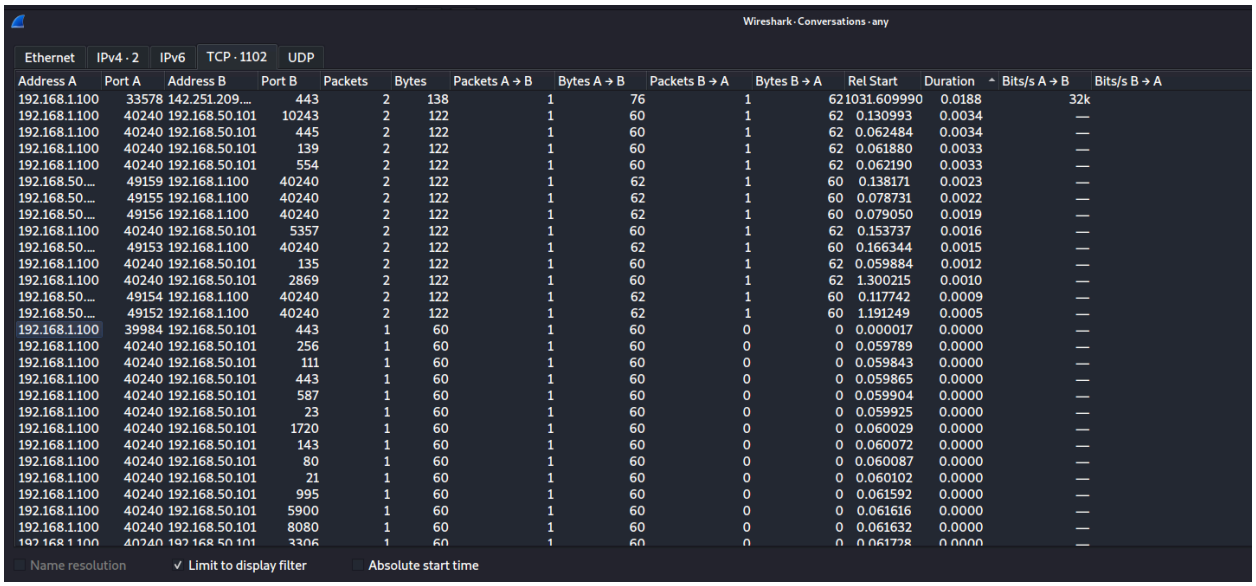
Filtro per visualizzare solo statistiche per SYN e SYN/ACK



tcp.flags.syn==1 or (tcp.flags.ack==1 and tcp.flags.syn == 1)

No.	Time	Source	Destination	Protocol	Length	Info
2	0.000016769	192.168.1.100	192.168.50.101	TCP	60	39984 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10	0.059788991	192.168.1.100	192.168.50.101	TCP	60	40240 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11	0.059843329	192.168.1.100	192.168.50.101	TCP	60	40240 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12	0.059864852	192.168.1.100	192.168.50.101	TCP	60	40240 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
13	0.059883780	192.168.1.100	192.168.50.101	TCP	60	40240 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14	0.059903658	192.168.1.100	192.168.50.101	TCP	60	40240 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15	0.059925187	192.168.1.100	192.168.50.101	TCP	60	40240 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	0.060029366	192.168.1.100	192.168.50.101	TCP	60	40240 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17	0.060072017	192.168.1.100	192.168.50.101	TCP	60	40240 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18	0.060087197	192.168.1.100	192.168.50.101	TCP	60	40240 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
19	0.060102341	192.168.1.100	192.168.50.101	TCP	60	40240 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
23	0.061120807	192.168.50.101	192.168.1.100	TCP	62	135 → 40240 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
31	0.061591707	192.168.1.100	192.168.50.101	TCP	60	40240 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
32	0.061616125	192.168.1.100	192.168.50.101	TCP	60	40240 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
33	0.061631707	192.168.1.100	192.168.50.101	TCP	60	40240 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
34	0.061727929	192.168.1.100	192.168.50.101	TCP	60	40240 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
35	0.061764367	192.168.1.100	192.168.50.101	TCP	60	40240 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
36	0.061859600	192.168.1.100	192.168.50.101	TCP	60	40240 → 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
37	0.061880377	192.168.1.100	192.168.50.101	TCP	60	40240 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
38	0.061895692	192.168.1.100	192.168.50.101	TCP	60	40240 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
39	0.061911333	192.168.1.100	192.168.50.101	TCP	60	40240 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
40	0.061977789	192.168.1.100	192.168.50.101	TCP	60	40240 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
41	0.062002336	192.168.1.100	192.168.50.101	TCP	60	40240 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
42	0.062146472	192.168.1.100	192.168.50.101	TCP	60	40240 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
43	0.062190458	192.168.1.100	192.168.50.101	TCP	60	40240 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
44	0.062284131	192.168.1.100	192.168.50.101	TCP	60	40240 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
45	0.062311481	192.168.1.100	192.168.50.101	TCP	60	40240 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
46	0.062441928	192.168.1.100	192.168.50.101	TCP	60	40240 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
47	0.062466505	192.168.1.100	192.168.50.101	TCP	60	40240 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
48	0.062484229	192.168.1.100	192.168.50.101	TCP	60	40240 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
49	0.062499180	192.168.1.100	192.168.50.101	TCP	60	40240 → 3905 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Reti diverse - Statistiche flag tempo di risposta



Wireshark · Conversations · any

Ethernet | IPv4 · 2 | IPv6 | TCP · 1102 | UDP

Address A	Port A	Address B	Port 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
192.168.1.100	33578	142.251.209....	443	2	138	1	76	1	62	1031.609990	0.0188	32k	
192.168.1.100	40240	192.168.50.101	10243	2	122	1	60	1	62	0.130993	0.0034	—	
192.168.1.100	40240	192.168.50.101	445	2	122	1	60	1	62	0.062484	0.0034	—	
192.168.1.100	40240	192.168.50.101	139	2	122	1	60	1	62	0.061880	0.0033	—	
192.168.1.100	40240	192.168.50.101	554	2	122	1	60	1	62	0.062190	0.0033	—	
192.168.50....	49159	192.168.1.100	40240	2	122	1	62	1	60	0.138171	0.0023	—	
192.168.50....	49155	192.168.1.100	40240	2	122	1	62	1	60	0.078731	0.0022	—	
192.168.50....	49156	192.168.1.100	40240	2	122	1	62	1	60	0.079050	0.0019	—	
192.168.1.100	40240	192.168.50.101	5357	2	122	1	60	1	62	0.153737	0.0016	—	
192.168.50....	49153	192.168.1.100	40240	2	122	1	62	1	60	0.166344	0.0015	—	
192.168.1.100	40240	192.168.50.101	135	2	122	1	60	1	62	0.059884	0.0012	—	
192.168.1.100	40240	192.168.50.101	2869	2	122	1	60	1	62	1.300215	0.0010	—	
192.168.50....	49154	192.168.1.100	40240	2	122	1	62	1	60	0.117742	0.0009	—	
192.168.50....	49152	192.168.1.100	40240	2	122	1	62	1	60	1.191249	0.0005	—	
192.168.1.100	39984	192.168.50.101	443	1	60	1	60	0	0	0.000017	0.0000	—	
192.168.1.100	40240	192.168.50.101	256	1	60	1	60	0	0	0.059789	0.0000	—	
192.168.1.100	40240	192.168.50.101	111	1	60	1	60	0	0	0.059843	0.0000	—	
192.168.1.100	40240	192.168.50.101	443	1	60	1	60	0	0	0.059865	0.0000	—	
192.168.1.100	40240	192.168.50.101	587	1	60	1	60	0	0	0.059904	0.0000	—	
192.168.1.100	40240	192.168.50.101	23	1	60	1	60	0	0	0.059925	0.0000	—	
192.168.1.100	40240	192.168.50.101	1720	1	60	1	60	0	0	0.060029	0.0000	—	
192.168.1.100	40240	192.168.50.101	143	1	60	1	60	0	0	0.060072	0.0000	—	
192.168.1.100	40240	192.168.50.101	80	1	60	1	60	0	0	0.060087	0.0000	—	
192.168.1.100	40240	192.168.50.101	21	1	60	1	60	0	0	0.060102	0.0000	—	
192.168.1.100	40240	192.168.50.101	995	1	60	1	60	0	0	0.061592	0.0000	—	
192.168.1.100	40240	192.168.50.101	5900	1	60	1	60	0	0	0.061616	0.0000	—	
192.168.1.100	40240	192.168.50.101	8080	1	60	1	60	0	0	0.061632	0.0000	—	
192.168.1.100	40240	192.168.50.101	3306	1	60	1	60	0	0	0.061728	0.0000	—	

Name resolution | ✓ Limit to display filter | Absolute start time

Con target e attaccante sulla stessa rete, il numero di risposte RST aumenta e diminuisce la latenza media e il rischio di perdita di pacchetti.