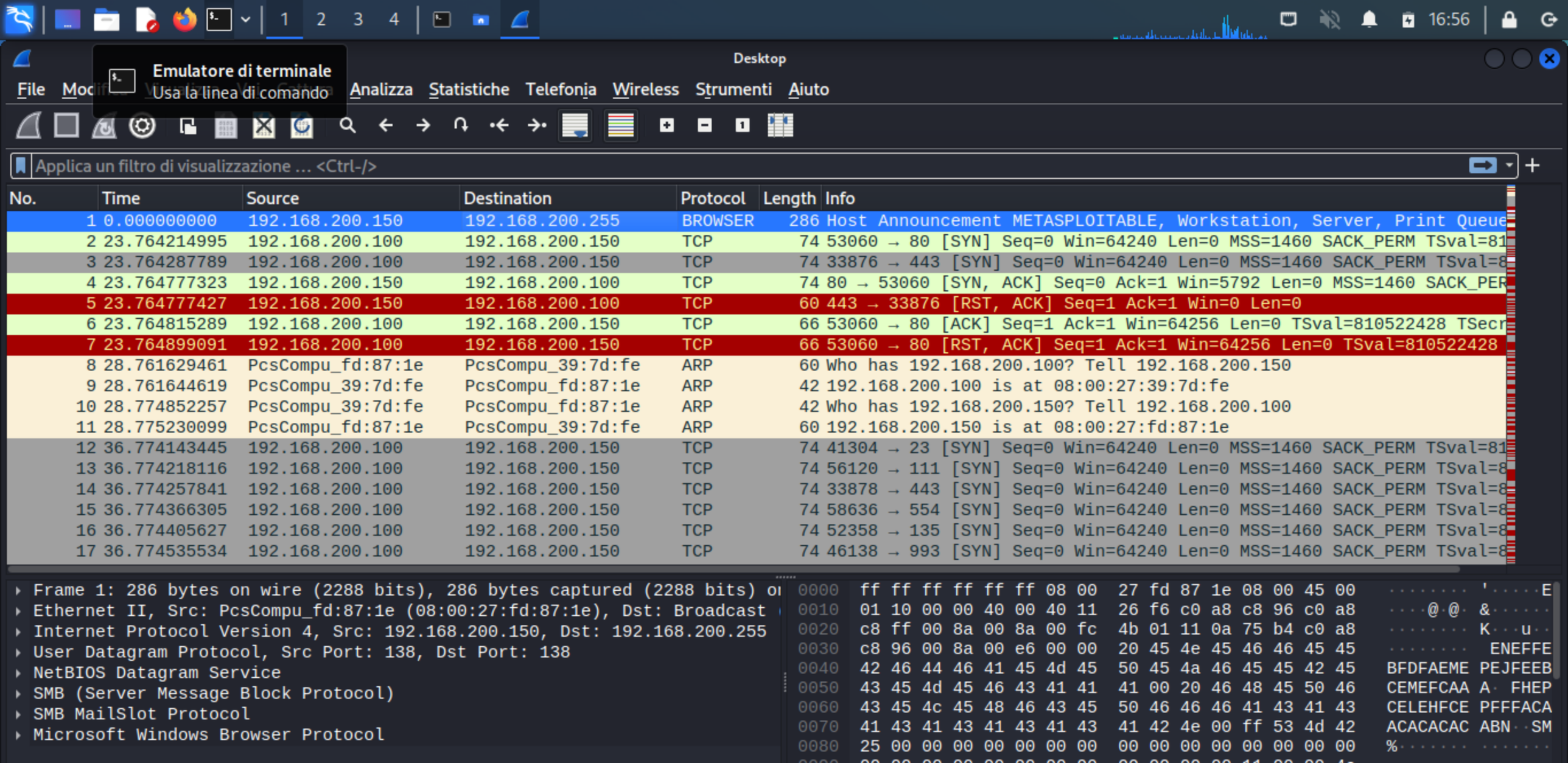
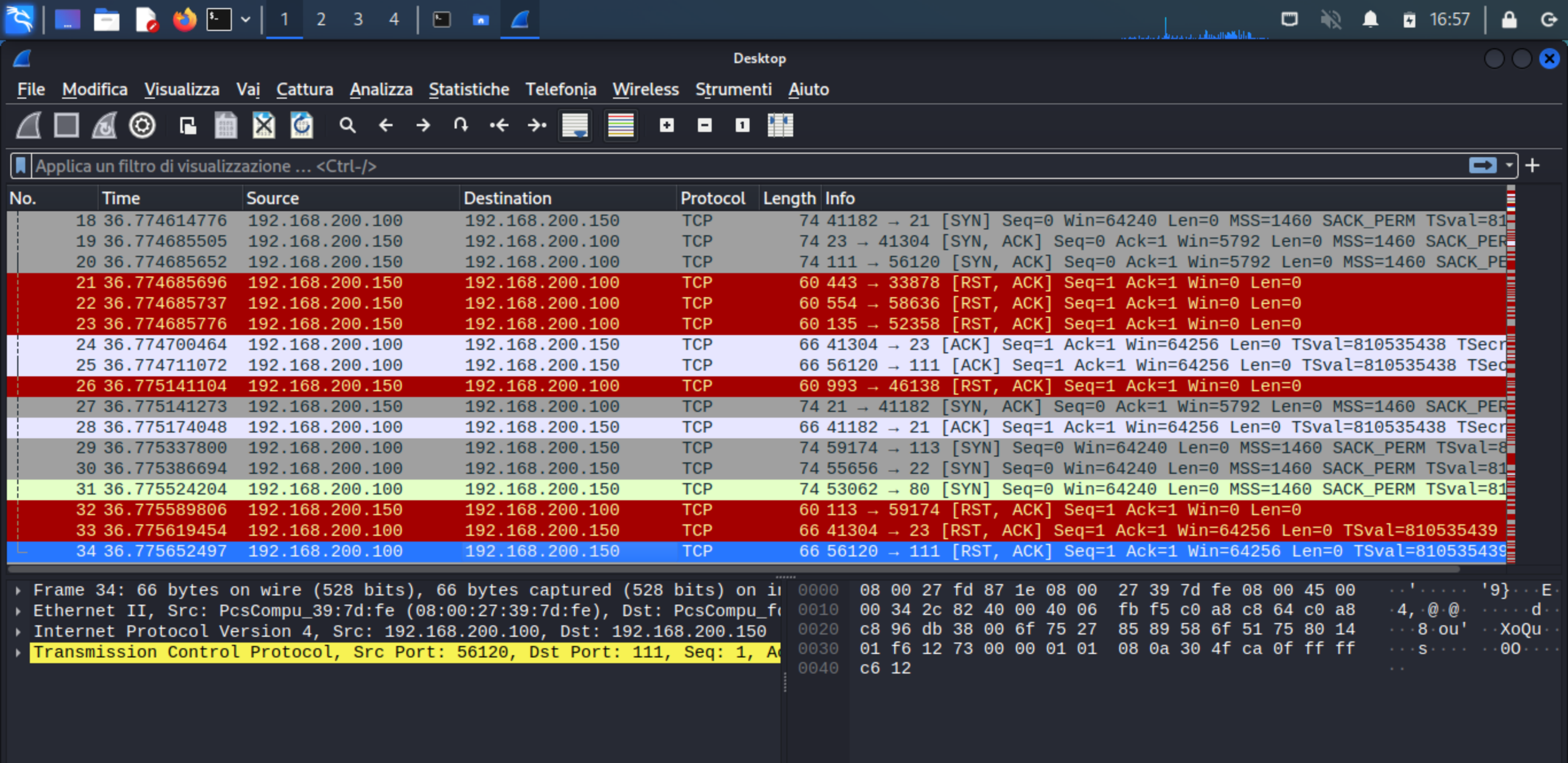
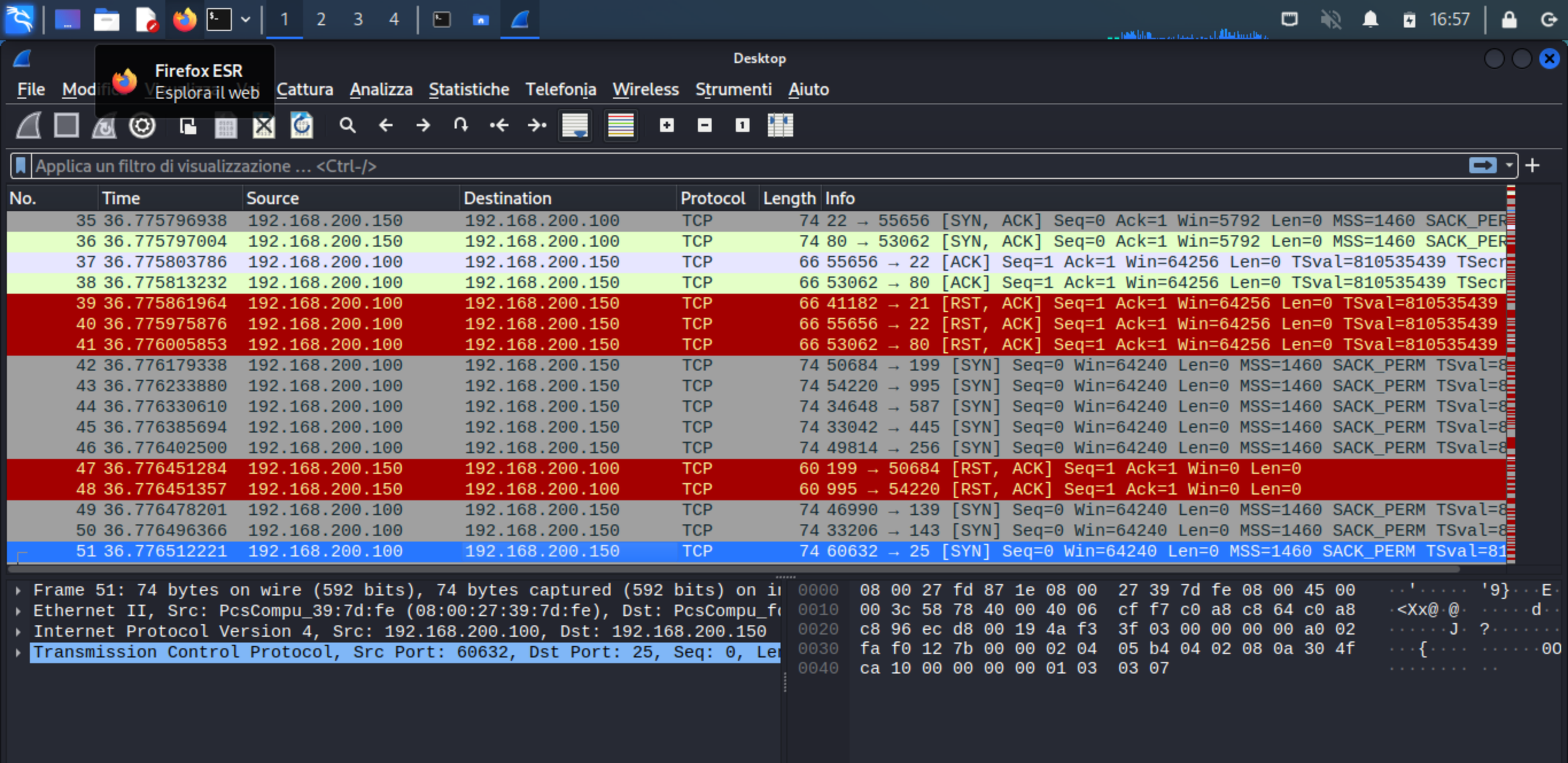
File Azioni Modifica Visualizza Aiuto

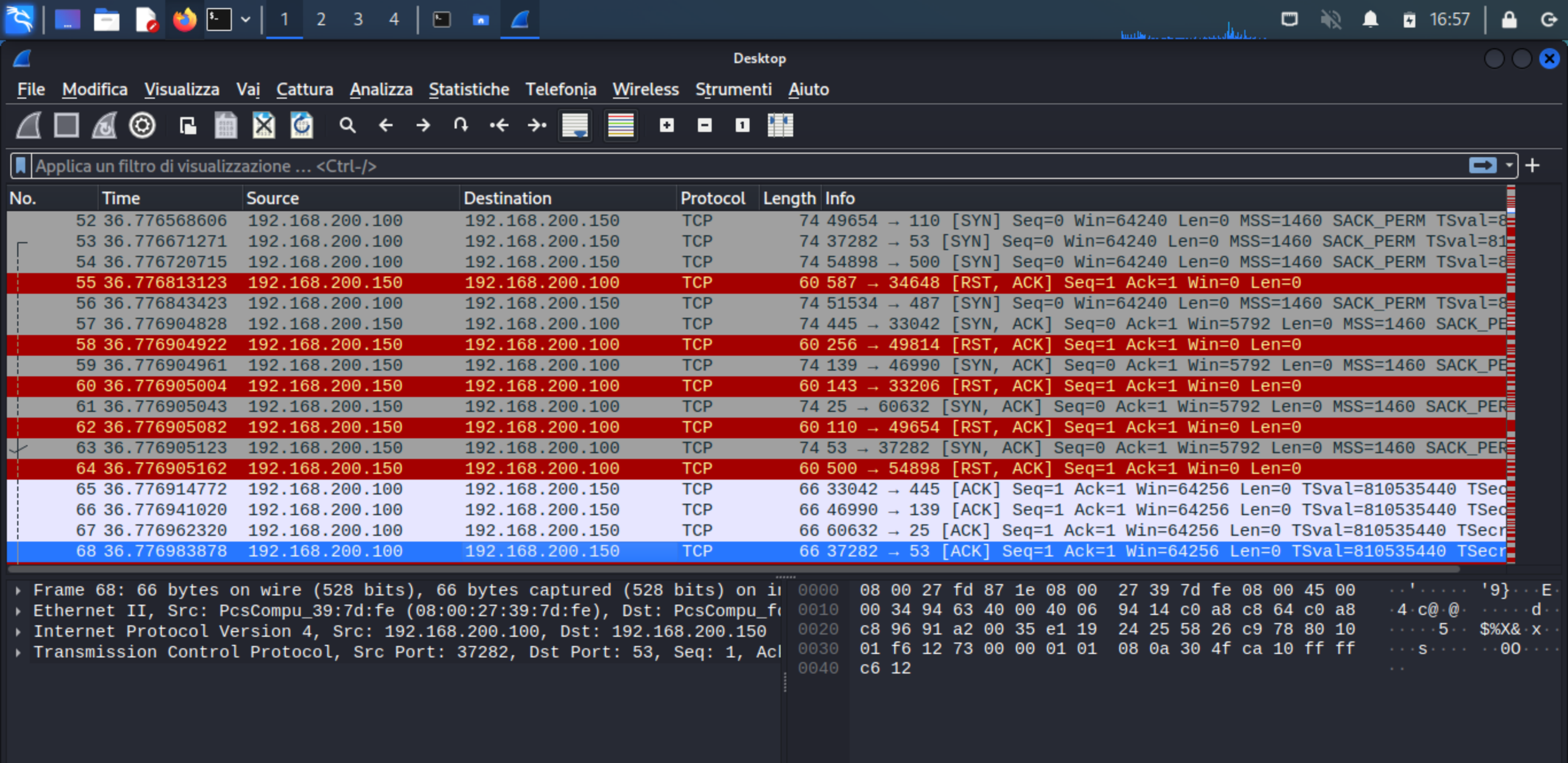
```
┌──(mattiadesimei㉿kali)-[~]
└─$ sudo su
[sudo] password di mattiadesimei:
┌──(root㉿kali)-[/home/mattiadesimei]
└─# cd /media

┌──(root㉿kali)-[/media]
└─# ls
cdrom  cdrom0  sf_Cattura_U3_W1_L3

┌──(root㉿kali)-[/media]
└─# cd sf_Cattura_U3_W1_L3

┌──(root㉿kali)-[/media/sf_Cattura_U3_W1_L3]
└─# ls
Cattura_U3_W1_L3.pcapng

┌──(root㉿kali)-[/media/sf_Cattura_U3_W1_L3]
└─# ls -la
totale 212
drwxrwx--- 1 root vboxsf      0  2 lug 16.40 .
drwxr-xr-x 4 root root     4096  2 lug 16.41 ..
-rwxrwx--- 1 root vboxsf 209024  2 lug 16.40 Cattura_U3_W1_L3.pcapng

┌──(root㉿kali)-[/media/sf_Cattura_U3_W1_L3]
└─# mv Cattura_U3_W1_L3.pcapng /home/mattiadesimei/Desktop
```

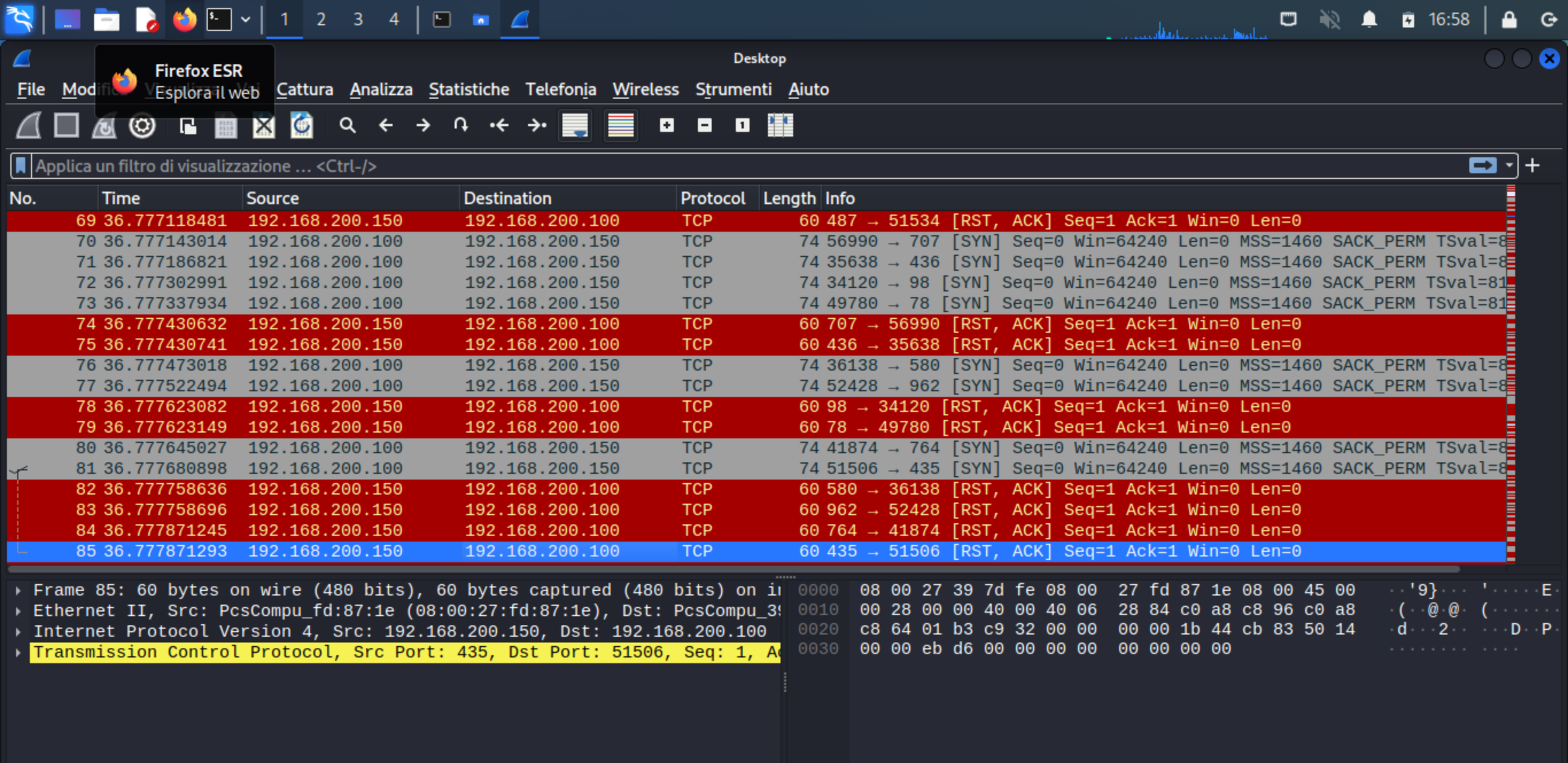
```
┌──(root㉿kali)-[/media/sf_Cattura_U3_W1_L3]
└─# cd /home/mattiadesimei

┌──(root㉿kali)-[/home/mattiadesimei]
└─# ls
BURPSUITE  Cattura_U3_W1_L3.zip  Documenti      gioco    Home           Immagini     Modelli  Pubblici     Scaricati  Video
C          Desktop               Esercitazioni  gioco.c  hydra.restore  Informatica  Musica   README.save  Scrivania

┌──(root㉿kali)-[/home/mattiadesimei]
└─# cd Desktop
cd: non è una directory: Desktop

┌──(root㉿kali)-[/home/mattiadesimei]
└─# ls
BURPSUITE  Cattura_U3_W1_L3.zip  Documenti      gioco    Home           Immagini     Modelli  Pubblici     Scaricati  Video
C          Desktop               Esercitazioni  gioco.c  hydra.restore  Informatica  Musica   README.save  Scrivania

┌──(root㉿kali)-[/home/mattiadesimei]
└─# chmod ugo+rw Desktop

┌──(root㉿kali)-[/home/mattiadesimei]
└─# chown kali Desktop
chown: utente non valido: "kali"

┌──(root㉿kali)-[/home/mattiadesimei]
└─# chown mattiadesimei Desktop

┌──(root㉿kali)-[/home/mattiadesimei]
└─#
```

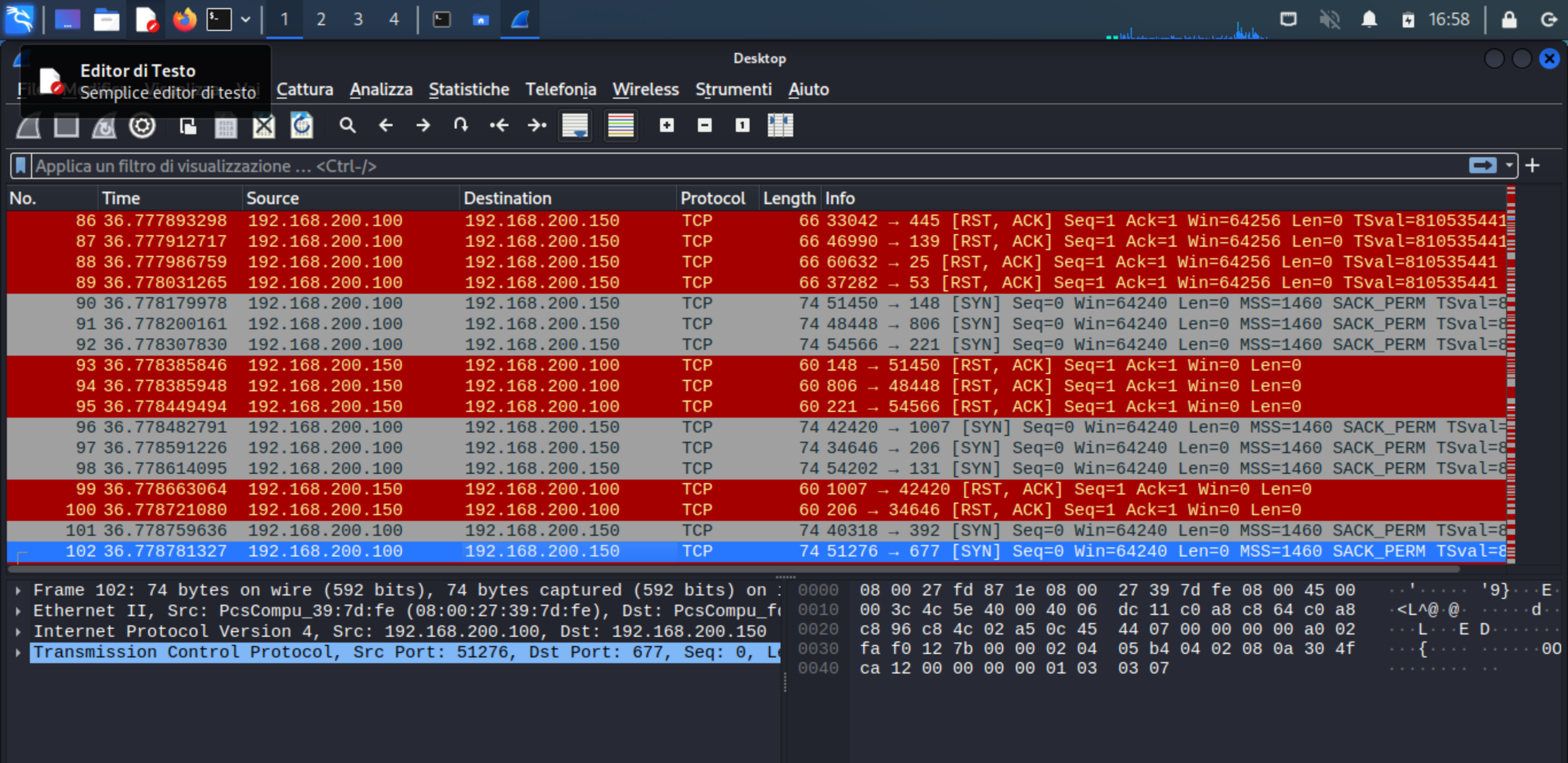

1 2 3 4
16:56
Emulatore di terminale
Usa la linea di comando
Desktop
File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonia Wireless Strumenti Aiuto
Applica un filtro di visualizzazione ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.200.150 192.168.200.255 BROWSER 286 Host Announcement METASPLOITABLE, Workstation, Server, Print Queue
2 23.764214995 192.168.200.100 192.168.200.150 TCP 74 53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=81
3 23.764287789 192.168.200.100 192.168.200.150 TCP 74 33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
4 23.764777323 192.168.200.150 192.168.200.100 TCP 74 80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PER
5 23.764777427 192.168.200.150 192.168.200.100 TCP 60 443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6 23.764815289 192.168.200.100 192.168.200.150 TCP 66 53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr
7 23.764899091 192.168.200.100 192.168.200.150 TCP 66 53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428
8 28.761629461 PcsCompu_fd:87:1e PcsCompu_39:7d:fe ARP 60 Who has 192.168.200.100? Tell 192.168.200.150
9 28.761644619 PcsCompu_39:7d:fe PcsCompu_fd:87:1e ARP 42 192.168.200.100 is at 08:00:27:39:7d:fe
10 28.774852257 PcsCompu_39:7d:fe PcsCompu_fd:87:1e ARP 42 Who has 192.168.200.150? Tell 192.168.200.100
11 28.775230099 PcsCompu_fd:87:1e PcsCompu_39:7d:fe ARP 60 192.168.200.150 is at 08:00:27:fd:87:1e
12 36.774143445 192.168.200.100 192.168.200.150 TCP 74 41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=81
13 36.774218116 192.168.200.100 192.168.200.150 TCP 74 56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
14 36.774257841 192.168.200.100 192.168.200.150 TCP 74 33878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
15 36.774366305 192.168.200.100 192.168.200.150 TCP 74 58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
16 36.774405627 192.168.200.100 192.168.200.150 TCP 74 52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
17 36.774535534 192.168.200.100 192.168.200.150 TCP 74 46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
Frame 1: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) o
Ethernet II, Src: PcsCompu_fd:87:1e (08:00:27:fd:87:1e), Dst: Broadcast
Internet Protocol Version 4, Src: 192.168.200.150, Dst: 192.168.200.255
User Datagram Protocol, Src Port: 138, Dst Port: 138
NetBIOS Datagram Service
SMB (Server Message Block Protocol)
SMB MailSlot Protocol
Microsoft Windows Browser Protocol
0000 ff ff ff ff ff ff 08 00 27 fd 87 1e 08 00 45 00
0010 01 10 00 00 40 00 40 11 26 f6 c0 a8 c8 96 c0 a8
0020 c8 ff 00 8a 00 8a 00 fc 4b 01 11 0a 75 b4 c0 a8
0030 c8 96 00 8a 00 e6 00 00 20 45 4e 45 46 46 45 45
0040 42 46 44 46 41 45 4d 45 50 45 4a 46 45 45 42 45
0050 43 45 4d 45 46 43 41 41 41 00 20 46 48 45 50 46
0060 43 45 4c 45 48 46 43 45 50 46 46 46 41 43 41 43
0070 41 43 41 43 41 43 41 43 41 42 4e 00 ff 53 4d 42
0080 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

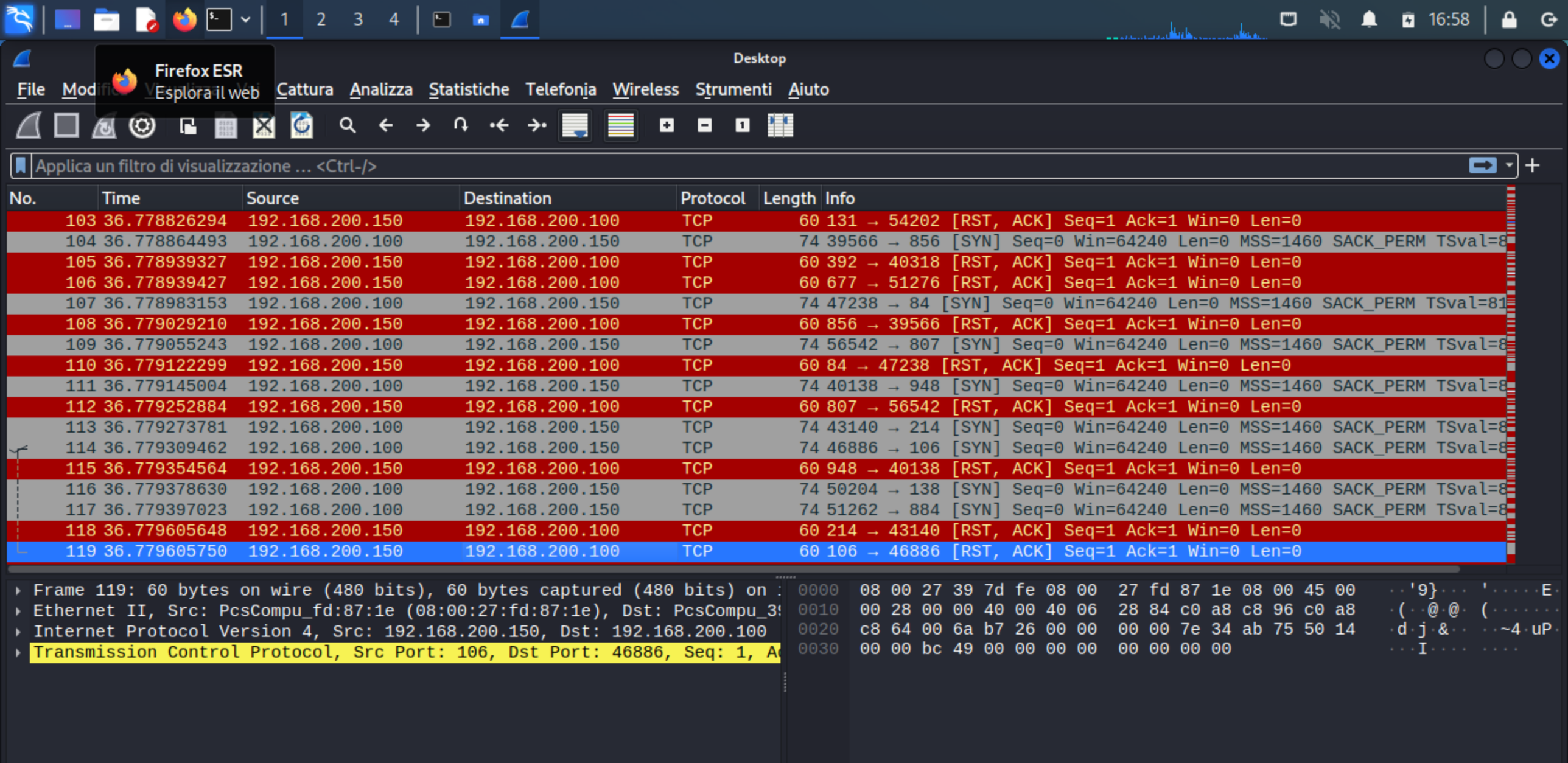

Desktop
File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonia Wireless Strumenti Aiuto
Applica un filtro di visualizzazione ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
18 36.774614776 192.168.200.100 192.168.200.150 TCP 74 41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=81
19 36.774685505 192.168.200.150 192.168.200.100 TCP 74 23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PER
20 36.774685652 192.168.200.150 192.168.200.100 TCP 74 111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PE
21 36.774685696 192.168.200.150 192.168.200.100 TCP 60 443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22 36.774685737 192.168.200.150 192.168.200.100 TCP 60 554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23 36.774685776 192.168.200.150 192.168.200.100 TCP 60 135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24 36.774700464 192.168.200.100 192.168.200.150 TCP 66 41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr
25 36.774711072 192.168.200.100 192.168.200.150 TCP 66 56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSec
26 36.775141104 192.168.200.150 192.168.200.100 TCP 60 993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27 36.775141273 192.168.200.150 192.168.200.100 TCP 74 21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PER
28 36.775174048 192.168.200.100 192.168.200.150 TCP 66 41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr
29 36.775337800 192.168.200.100 192.168.200.150 TCP 74 59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
30 36.775386694 192.168.200.100 192.168.200.150 TCP 74 55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=81
31 36.775524204 192.168.200.100 192.168.200.150 TCP 74 53062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=81
32 36.775589806 192.168.200.150 192.168.200.100 TCP 60 113 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33 36.775619454 192.168.200.100 192.168.200.150 TCP 66 41304 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439
34 36.775652497 192.168.200.100 192.168.200.150 TCP 66 56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439
Frame 34: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on i
Ethernet II, Src: PcsCompu_39:7d:fe (08:00:27:39:7d:fe), Dst: PcsCompu_f
Internet Protocol Version 4, Src: 192.168.200.100, Dst: 192.168.200.150
Transmission Control Protocol, Src Port: 56120, Dst Port: 111, Seq: 1, A
0000 08 00 27 fd 87 1e 08 00 27 39 7d fe 08 00 45 00
0010 00 34 2c 82 40 00 40 06 fb f5 c0 a8 c8 64 c0 a8
0020 c8 96 db 38 00 6f 75 27 85 89 58 6f 51 75 80 14
0030 01 f6 12 73 00 00 01 01 08 0a 30 4f ca 0f ff ff
0040 c6 12

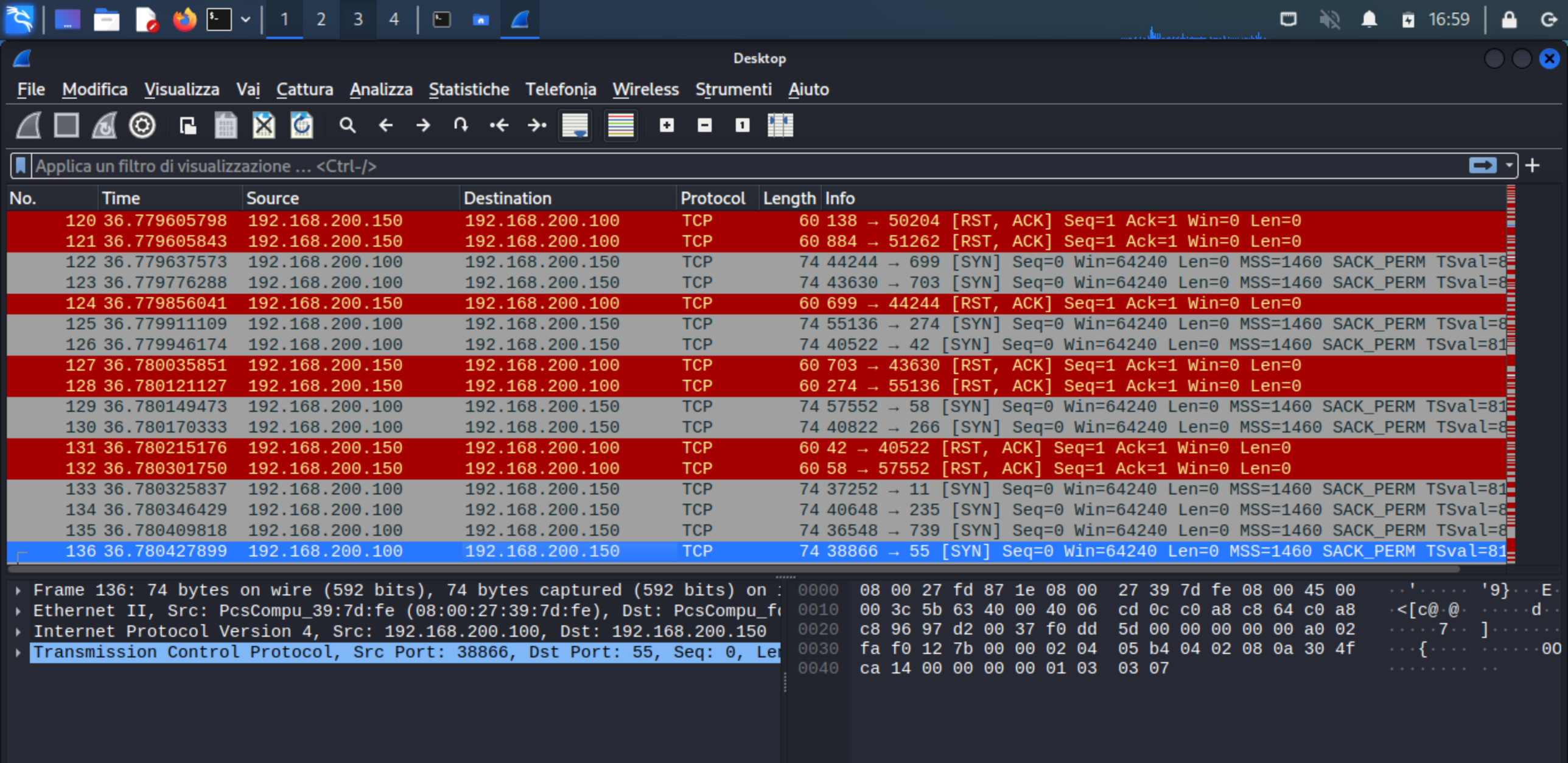

Firefox ESR
Esplora il web
Desktop
File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonia Wireless Strumenti Aiuto
Applica un filtro di visualizzazione ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
35 36.775796938 192.168.200.150 192.168.200.100 TCP 74 22 → 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PER
36 36.775797004 192.168.200.150 192.168.200.100 TCP 74 80 → 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PER
37 36.775803786 192.168.200.100 192.168.200.150 TCP 66 55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr
38 36.775813232 192.168.200.100 192.168.200.150 TCP 66 53062 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr
39 36.775861964 192.168.200.100 192.168.200.150 TCP 66 41182 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439
40 36.775975876 192.168.200.100 192.168.200.150 TCP 66 55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439
41 36.776005853 192.168.200.100 192.168.200.150 TCP 66 53062 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439
42 36.776179338 192.168.200.100 192.168.200.150 TCP 74 50684 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
43 36.776233880 192.168.200.100 192.168.200.150 TCP 74 54220 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
44 36.776330610 192.168.200.100 192.168.200.150 TCP 74 34648 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
45 36.776385694 192.168.200.100 192.168.200.150 TCP 74 33042 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
46 36.776402500 192.168.200.100 192.168.200.150 TCP 74 49814 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
47 36.776451284 192.168.200.150 192.168.200.100 TCP 60 199 → 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48 36.776451357 192.168.200.150 192.168.200.100 TCP 60 995 → 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49 36.776478201 192.168.200.100 192.168.200.150 TCP 74 46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
50 36.776496366 192.168.200.100 192.168.200.150 TCP 74 33206 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
51 36.776512221 192.168.200.100 192.168.200.150 TCP 74 60632 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=81
Frame 51: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on i
Ethernet II, Src: PcsCompu_39:7d:fe (08:00:27:39:7d:fe), Dst: PcsCompu_f
Internet Protocol Version 4, Src: 192.168.200.100, Dst: 192.168.200.150
Transmission Control Protocol, Src Port: 60632, Dst Port: 25, Seq: 0, Le
0000 08 00 27 fd 87 1e 08 00 27 39 7d fe 08 00 45 00
0010 00 3c 58 78 40 00 40 06 cf f7 c0 a8 c8 64 c0 a8
0020 c8 96 ec d8 00 19 4a f3 3f 03 00 00 00 00 a0 02
0030 fa f0 12 7b 00 00 02 04 05 b4 04 02 08 0a 30 4f
0040 ca 10 00 00 00 00 01 03 03 07

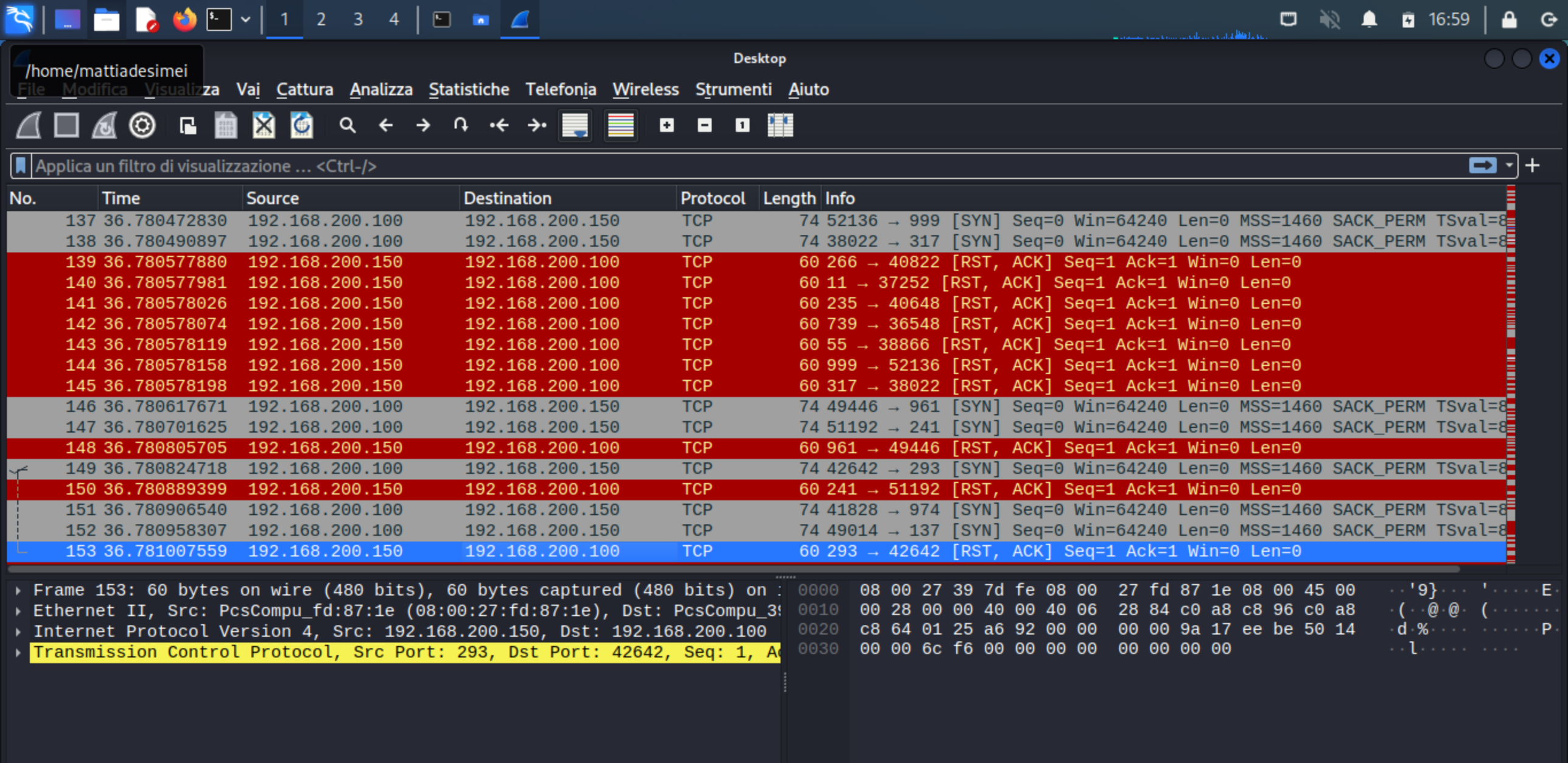

Desktop
File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonia Wireless Strumenti Aiuto
Applica un filtro di visualizzazione ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
52 36.776568606 192.168.200.100 192.168.200.150 TCP 74 49654 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
53 36.776671271 192.168.200.100 192.168.200.150 TCP 74 37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=81
54 36.776720715 192.168.200.100 192.168.200.150 TCP 74 54898 → 500 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
55 36.776813123 192.168.200.150 192.168.200.100 TCP 60 587 → 34648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
56 36.776843423 192.168.200.100 192.168.200.150 TCP 74 51534 → 487 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
57 36.776904828 192.168.200.150 192.168.200.100 TCP 74 445 → 33042 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PE
58 36.776904922 192.168.200.150 192.168.200.100 TCP 60 256 → 49814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59 36.776904961 192.168.200.150 192.168.200.100 TCP 74 139 → 46990 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PE
60 36.776905004 192.168.200.150 192.168.200.100 TCP 60 143 → 33206 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61 36.776905043 192.168.200.150 192.168.200.100 TCP 74 25 → 60632 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PER
62 36.776905082 192.168.200.150 192.168.200.100 TCP 60 110 → 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
63 36.776905123 192.168.200.150 192.168.200.100 TCP 74 53 → 37282 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PER
64 36.776905162 192.168.200.150 192.168.200.100 TCP 60 500 → 54898 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
65 36.776914772 192.168.200.100 192.168.200.150 TCP 66 33042 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSec
66 36.776941020 192.168.200.100 192.168.200.150 TCP 66 46990 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSec
67 36.776962320 192.168.200.100 192.168.200.150 TCP 66 60632 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr
68 36.776983878 192.168.200.100 192.168.200.150 TCP 66 37282 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr
Frame 68: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on i
Ethernet II, Src: PcsCompu_39:7d:fe (08:00:27:39:7d:fe), Dst: PcsCompu_f
Internet Protocol Version 4, Src: 192.168.200.100, Dst: 192.168.200.150
Transmission Control Protocol, Src Port: 37282, Dst Port: 53, Seq: 1, Ac
0000 08 00 27 fd 87 1e 08 00 27 39 7d fe 08 00 45 00
0010 00 34 94 63 40 00 40 06 94 14 c0 a8 c8 64 c0 a8
0020 c8 96 91 a2 00 35 e1 19 24 25 58 26 c9 78 80 10
0030 01 f6 12 73 00 00 01 01 08 0a 30 4f ca 10 ff ff
0040 c6 12

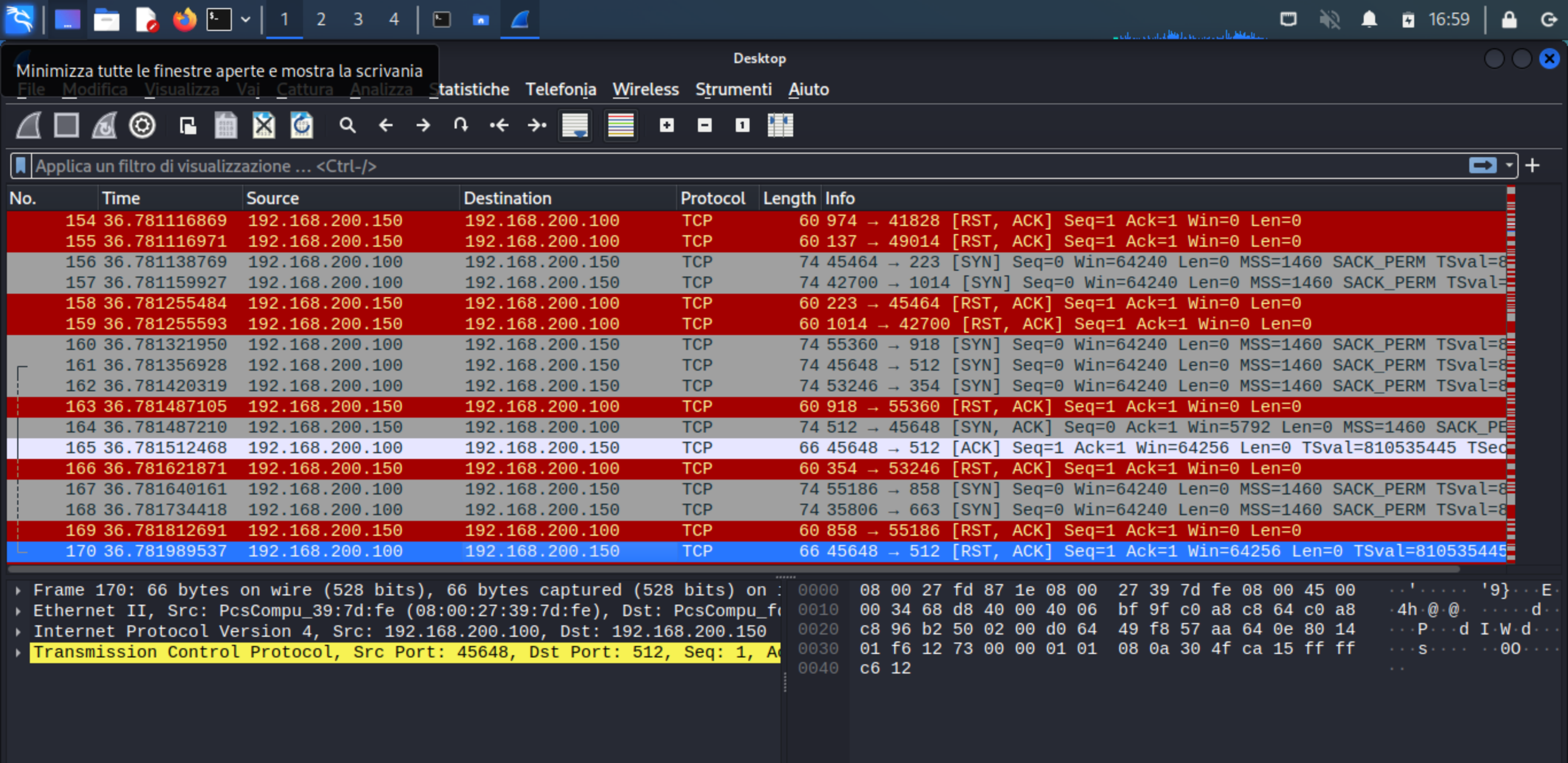

1 2 3 4
16:58
Firefox ESR
Esplora il web
Desktop
File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonia Wireless Strumenti Aiuto
Applica un filtro di visualizzazione ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
69 36.777118481 192.168.200.150 192.168.200.100 TCP 60 487 → 51534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
70 36.777143014 192.168.200.100 192.168.200.150 TCP 74 56990 → 707 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
71 36.777186821 192.168.200.100 192.168.200.150 TCP 74 35638 → 436 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
72 36.777302991 192.168.200.100 192.168.200.150 TCP 74 34120 → 98 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=81
73 36.777337934 192.168.200.100 192.168.200.150 TCP 74 49780 → 78 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=81
74 36.777430632 192.168.200.150 192.168.200.100 TCP 60 707 → 56990 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
75 36.777430741 192.168.200.150 192.168.200.100 TCP 60 436 → 35638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
76 36.777473018 192.168.200.100 192.168.200.150 TCP 74 36138 → 580 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
77 36.777522494 192.168.200.100 192.168.200.150 TCP 74 52428 → 962 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
78 36.777623082 192.168.200.150 192.168.200.100 TCP 60 98 → 34120 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79 36.777623149 192.168.200.150 192.168.200.100 TCP 60 78 → 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
80 36.777645027 192.168.200.100 192.168.200.150 TCP 74 41874 → 764 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
81 36.777680898 192.168.200.100 192.168.200.150 TCP 74 51506 → 435 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
82 36.777758636 192.168.200.150 192.168.200.100 TCP 60 580 → 36138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
83 36.777758696 192.168.200.150 192.168.200.100 TCP 60 962 → 52428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
84 36.777871245 192.168.200.150 192.168.200.100 TCP 60 764 → 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
85 36.777871293 192.168.200.150 192.168.200.100 TCP 60 435 → 51506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
Frame 85: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on i
Ethernet II, Src: PcsCompu_fd:87:1e (08:00:27:fd:87:1e), Dst: PcsCompu_3
Internet Protocol Version 4, Src: 192.168.200.150, Dst: 192.168.200.100
Transmission Control Protocol, Src Port: 435, Dst Port: 51506, Seq: 1, A
0000 08 00 27 39 7d fe 08 00 27 fd 87 1e 08 00 45 00
0010 00 28 00 00 40 00 40 06 28 84 c0 a8 c8 96 c0 a8
0020 c8 64 01 b3 c9 32 00 00 00 00 1b 44 cb 83 50 14
0030 00 00 eb d6 00 00 00 00 00 00 00 00

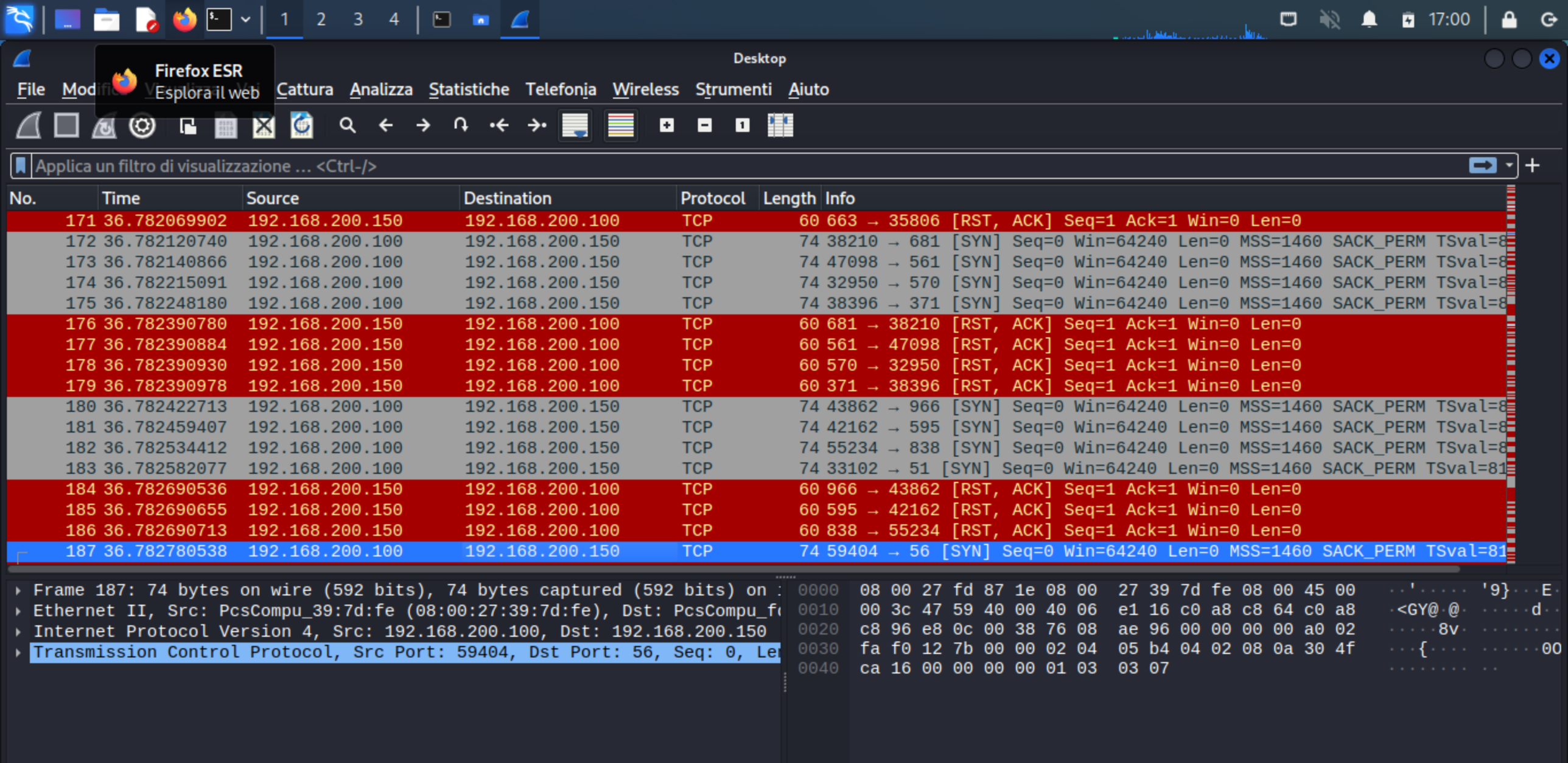

Editor di Testo
Semplice editor di testo
Desktop
Cattura Analizza Statistiche Telefonia Wireless Strumenti Aiuto
Applica un filtro di visualizzazione ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
86 36.777893298 192.168.200.100 192.168.200.150 TCP 66 33042 → 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441
87 36.777912717 192.168.200.100 192.168.200.150 TCP 66 46990 → 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441
88 36.777986759 192.168.200.100 192.168.200.150 TCP 66 60632 → 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441
89 36.778031265 192.168.200.100 192.168.200.150 TCP 66 37282 → 53 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441
90 36.778179978 192.168.200.100 192.168.200.150 TCP 74 51450 → 148 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
91 36.778200161 192.168.200.100 192.168.200.150 TCP 74 48448 → 806 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
92 36.778307830 192.168.200.100 192.168.200.150 TCP 74 54566 → 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
93 36.778385846 192.168.200.150 192.168.200.100 TCP 60 148 → 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
94 36.778385948 192.168.200.150 192.168.200.100 TCP 60 806 → 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
95 36.778449494 192.168.200.150 192.168.200.100 TCP 60 221 → 54566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
96 36.778482791 192.168.200.100 192.168.200.150 TCP 74 42420 → 1007 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=
97 36.778591226 192.168.200.100 192.168.200.150 TCP 74 34646 → 206 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
98 36.778614095 192.168.200.100 192.168.200.150 TCP 74 54202 → 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
99 36.778663064 192.168.200.150 192.168.200.100 TCP 60 1007 → 42420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
100 36.778721080 192.168.200.150 192.168.200.100 TCP 60 206 → 34646 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
101 36.778759636 192.168.200.100 192.168.200.150 TCP 74 40318 → 392 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
102 36.778781327 192.168.200.100 192.168.200.150 TCP 74 51276 → 677 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
Frame 102: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on
Ethernet II, Src: PcsCompu_39:7d:fe (08:00:27:39:7d:fe), Dst: PcsCompu_f
Internet Protocol Version 4, Src: 192.168.200.100, Dst: 192.168.200.150
Transmission Control Protocol, Src Port: 51276, Dst Port: 677, Seq: 0, L
0000 08 00 27 fd 87 1e 08 00 27 39 7d fe 08 00 45 00
0010 00 3c 4c 5e 40 00 40 06 dc 11 c0 a8 c8 64 c0 a8
0020 c8 96 c8 4c 02 a5 0c 45 44 07 00 00 00 00 a0 02
0030 fa f0 12 7b 00 00 02 04 05 b4 04 02 08 0a 30 4f
0040 ca 12 00 00 00 00 01 03 03 07


1 2 3 4
16:58
Firefox ESR
Esplora il web
Desktop
File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonia Wireless Strumenti Aiuto
Applica un filtro di visualizzazione ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
103 36.778826294 192.168.200.150 192.168.200.100 TCP 60 131 → 54202 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
104 36.778864493 192.168.200.100 192.168.200.150 TCP 74 39566 → 856 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
105 36.778939327 192.168.200.150 192.168.200.100 TCP 60 392 → 40318 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
106 36.778939427 192.168.200.150 192.168.200.100 TCP 60 677 → 51276 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
107 36.778983153 192.168.200.100 192.168.200.150 TCP 74 47238 → 84 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=81
108 36.779029210 192.168.200.150 192.168.200.100 TCP 60 856 → 39566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
109 36.779055243 192.168.200.100 192.168.200.150 TCP 74 56542 → 807 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
110 36.779122299 192.168.200.150 192.168.200.100 TCP 60 84 → 47238 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
111 36.779145004 192.168.200.100 192.168.200.150 TCP 74 40138 → 948 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
112 36.779252884 192.168.200.150 192.168.200.100 TCP 60 807 → 56542 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
113 36.779273781 192.168.200.100 192.168.200.150 TCP 74 43140 → 214 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
114 36.779309462 192.168.200.100 192.168.200.150 TCP 74 46886 → 106 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
115 36.779354564 192.168.200.150 192.168.200.100 TCP 60 948 → 40138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
116 36.779378630 192.168.200.100 192.168.200.150 TCP 74 50204 → 138 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
117 36.779397023 192.168.200.100 192.168.200.150 TCP 74 51262 → 884 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
118 36.779605648 192.168.200.150 192.168.200.100 TCP 60 214 → 43140 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
119 36.779605750 192.168.200.150 192.168.200.100 TCP 60 106 → 46886 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
Frame 119: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on
Ethernet II, Src: PcsCompu_fd:87:1e (08:00:27:fd:87:1e), Dst: PcsCompu_3
Internet Protocol Version 4, Src: 192.168.200.150, Dst: 192.168.200.100
Transmission Control Protocol, Src Port: 106, Dst Port: 46886, Seq: 1, A
0000 08 00 27 39 7d fe 08 00 27 fd 87 1e 08 00 45 00
0010 00 28 00 00 40 00 40 06 28 84 c0 a8 c8 96 c0 a8
0020 c8 64 00 6a b7 26 00 00 00 00 7e 34 ab 75 50 14
0030 00 00 bc 49 00 00 00 00 00 00 00 00


Desktop
File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonia Wireless Strumenti Aiuto
Applica un filtro di visualizzazione ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
120 36.779605798 192.168.200.150 192.168.200.100 TCP 60 138 → 50204 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
121 36.779605843 192.168.200.150 192.168.200.100 TCP 60 884 → 51262 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
122 36.77637573 192.168.200.100 192.168.200.150 TCP 74 44244 → 699 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
123 36.779776288 192.168.200.100 192.168.200.150 TCP 74 43630 → 703 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
124 36.779856041 192.168.200.150 192.168.200.100 TCP 60 699 → 44244 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
125 36.779911109 192.168.200.100 192.168.200.150 TCP 74 55136 → 274 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
126 36.779946174 192.168.200.100 192.168.200.150 TCP 74 40522 → 42 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=81
127 36.780035851 192.168.200.150 192.168.200.100 TCP 60 703 → 43630 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
128 36.780121127 192.168.200.150 192.168.200.100 TCP 60 274 → 55136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
129 36.780149473 192.168.200.100 192.168.200.150 TCP 74 57552 → 58 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=81
130 36.780170333 192.168.200.100 192.168.200.150 TCP 74 40822 → 266 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
131 36.780215176 192.168.200.150 192.168.200.100 TCP 60 42 → 40522 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
132 36.780301750 192.168.200.150 192.168.200.100 TCP 60 58 → 57552 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
133 36.780325837 192.168.200.100 192.168.200.150 TCP 74 37252 → 11 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=81
134 36.780346429 192.168.200.100 192.168.200.150 TCP 74 40648 → 235 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
135 36.780409818 192.168.200.100 192.168.200.150 TCP 74 36548 → 739 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
136 36.780427899 192.168.200.100 192.168.200.150 TCP 74 38866 → 55 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=81
Frame 136: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on
Ethernet II, Src: PcsCompu_39:7d:fe (08:00:27:39:7d:fe), Dst: PcsCompu_f
Internet Protocol Version 4, Src: 192.168.200.100, Dst: 192.168.200.150
Transmission Control Protocol, Src Port: 38866, Dst Port: 55, Seq: 0, Le
0000 08 00 27 fd 87 1e 08 00 27 39 7d fe 08 00 45 00
0010 00 3c 5b 63 40 00 40 06 cd 0c c0 a8 c8 64 c0 a8
0020 c8 96 97 d2 00 37 f0 dd 5d 00 00 00 00 00 a0 02
0030 fa f0 12 7b 00 00 02 04 05 b4 04 02 08 0a 30 4f
0040 ca 14 00 00 00 00 01 03 03 07


/home/mattiadesimei
Desktop
File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonia Wireless Strumenti Aiuto
Applica un filtro di visualizzazione ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
137 36.780472830 192.168.200.100 192.168.200.150 TCP 74 52136 → 999 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
138 36.780490897 192.168.200.100 192.168.200.150 TCP 74 38022 → 317 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
139 36.780577880 192.168.200.150 192.168.200.100 TCP 60 266 → 40822 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
140 36.780577981 192.168.200.150 192.168.200.100 TCP 60 11 → 37252 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
141 36.780578026 192.168.200.150 192.168.200.100 TCP 60 235 → 40648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
142 36.780578074 192.168.200.150 192.168.200.100 TCP 60 739 → 36548 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
143 36.780578119 192.168.200.150 192.168.200.100 TCP 60 55 → 38866 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
144 36.780578158 192.168.200.150 192.168.200.100 TCP 60 999 → 52136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
145 36.780578198 192.168.200.150 192.168.200.100 TCP 60 317 → 38022 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
146 36.780617671 192.168.200.100 192.168.200.150 TCP 74 49446 → 961 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
147 36.780701625 192.168.200.100 192.168.200.150 TCP 74 51192 → 241 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
148 36.780805705 192.168.200.150 192.168.200.100 TCP 60 961 → 49446 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
149 36.780824718 192.168.200.100 192.168.200.150 TCP 74 42642 → 293 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
150 36.780889399 192.168.200.150 192.168.200.100 TCP 60 241 → 51192 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
151 36.780906540 192.168.200.100 192.168.200.150 TCP 74 41828 → 974 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
152 36.780958307 192.168.200.100 192.168.200.150 TCP 74 49014 → 137 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
153 36.781007559 192.168.200.150 192.168.200.100 TCP 60 293 → 42642 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
Frame 153: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on
Ethernet II, Src: PcsCompu_fd:87:1e (08:00:27:fd:87:1e), Dst: PcsCompu_3
Internet Protocol Version 4, Src: 192.168.200.150, Dst: 192.168.200.100
Transmission Control Protocol, Src Port: 293, Dst Port: 42642, Seq: 1, A
0000 08 00 27 39 7d fe 08 00 27 fd 87 1e 08 00 45 00
0010 00 28 00 00 40 00 40 06 28 84 c0 a8 c8 96 c0 a8
0020 c8 64 01 25 a6 92 00 00 00 00 9a 17 ee be 50 14
0030 00 00 6c f6 00 00 00 00 00 00 00 00


Minimizza tutte le finestre aperte e mostra la scrivania
16:59
Desktop
File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonia Wireless Strumenti Aiuto
Applica un filtro di visualizzazione ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
154 36.781116869 192.168.200.150 192.168.200.100 TCP 60 974 → 41828 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
155 36.781116971 192.168.200.150 192.168.200.100 TCP 60 137 → 49014 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
156 36.781138769 192.168.200.100 192.168.200.150 TCP 74 45464 → 223 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
157 36.781159927 192.168.200.100 192.168.200.150 TCP 74 42700 → 1014 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=
158 36.781255484 192.168.200.150 192.168.200.100 TCP 60 223 → 45464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
159 36.781255593 192.168.200.150 192.168.200.100 TCP 60 1014 → 42700 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
160 36.781321950 192.168.200.100 192.168.200.150 TCP 74 55360 → 918 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
161 36.781356928 192.168.200.100 192.168.200.150 TCP 74 45648 → 512 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
162 36.781420319 192.168.200.100 192.168.200.150 TCP 74 53246 → 354 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
163 36.781487105 192.168.200.150 192.168.200.100 TCP 60 918 → 55360 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
164 36.781487210 192.168.200.150 192.168.200.100 TCP 74 512 → 45648 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PE
165 36.781512468 192.168.200.100 192.168.200.150 TCP 66 45648 → 512 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535445 TSec
166 36.781621871 192.168.200.150 192.168.200.100 TCP 60 354 → 53246 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
167 36.781640161 192.168.200.100 192.168.200.150 TCP 74 55186 → 858 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
168 36.781734418 192.168.200.100 192.168.200.150 TCP 74 35806 → 663 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
169 36.781812691 192.168.200.150 192.168.200.100 TCP 60 858 → 55186 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
170 36.781989537 192.168.200.100 192.168.200.150 TCP 66 45648 → 512 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535445
Frame 170: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on
Ethernet II, Src: PcsCompu_39:7d:fe (08:00:27:39:7d:fe), Dst: PcsCompu_f
Internet Protocol Version 4, Src: 192.168.200.100, Dst: 192.168.200.150
Transmission Control Protocol, Src Port: 45648, Dst Port: 512, Seq: 1, A
0000 08 00 27 fd 87 1e 08 00 27 39 7d fe 08 00 45 00
0010 00 34 68 d8 40 00 40 06 bf 9f c0 a8 c8 64 c0 a8
0020 c8 96 b2 50 02 00 d0 64 49 f8 57 aa 64 0e 80 14
0030 01 f6 12 73 00 00 01 01 08 0a 30 4f ca 15 ff ff
0040 c6 12


1 2 3 4
17:00
Firefox ESR
Esplora il web
Desktop
File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonia Wireless Strumenti Aiuto
Applica un filtro di visualizzazione ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
171 36.782069902 192.168.200.150 192.168.200.100 TCP 60 663 → 35806 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
172 36.782120740 192.168.200.100 192.168.200.150 TCP 74 38210 → 681 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
173 36.782140866 192.168.200.100 192.168.200.150 TCP 74 47098 → 561 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
174 36.782215091 192.168.200.100 192.168.200.150 TCP 74 32950 → 570 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
175 36.782248180 192.168.200.100 192.168.200.150 TCP 74 38396 → 371 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
176 36.782390780 192.168.200.150 192.168.200.100 TCP 60 681 → 38210 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
177 36.782390884 192.168.200.150 192.168.200.100 TCP 60 561 → 47098 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
178 36.782390930 192.168.200.150 192.168.200.100 TCP 60 570 → 32950 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
179 36.782390978 192.168.200.150 192.168.200.100 TCP 60 371 → 38396 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
180 36.782422713 192.168.200.100 192.168.200.150 TCP 74 43862 → 966 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
181 36.782459407 192.168.200.100 192.168.200.150 TCP 74 42162 → 595 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
182 36.782534412 192.168.200.100 192.168.200.150 TCP 74 55234 → 838 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=8
183 36.782582077 192.168.200.100 192.168.200.150 TCP 74 33102 → 51 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=81
184 36.782690536 192.168.200.150 192.168.200.100 TCP 60 966 → 43862 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
185 36.782690655 192.168.200.150 192.168.200.100 TCP 60 595 → 42162 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
186 36.782690713 192.168.200.150 192.168.200.100 TCP 60 838 → 55234 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
187 36.782780538 192.168.200.100 192.168.200.150 TCP 74 59404 → 56 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=81
Frame 187: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on
Ethernet II, Src: PcsCompu_39:7d:fe (08:00:27:39:7d:fe), Dst: PcsCompu_f
Internet Protocol Version 4, Src: 192.168.200.100, Dst: 192.168.200.150
Transmission Control Protocol, Src Port: 59404, Dst Port: 56, Seq: 0, Le
0000 08 00 27 fd 87 1e 08 00 27 39 7d fe 08 00 45 00
0010 00 3c 47 59 40 00 40 06 e1 16 c0 a8 c8 64 c0 a8
0020 c8 96 e8 0c 00 38 76 08 ae 96 00 00 00 00 a0 02
0030 fa f0 12 7b 00 00 02 04 05 b4 04 02 08 0a 30 4f
0040 ca 16 00 00 00 00 01 03 03 07

Possibili vettori di attacco:

1) Malware: Gli attaccanti potrebbero aver utilizzato malware per compromettere i sistemi. Potrebbe essere utile esaminare i flussi di rete per rilevare comunicazioni sospette o attività anomale.

2) Phishing: Gli attaccanti potrebbero aver utilizzato attacchi di phishing per ottenere credenziali o informazioni sensibili. Potrebbe essere utile analizzare il traffico di posta elettronica o i collegamenti sospetti per identificare eventuali tentativi di phishing.

3) Vulnerabilità del sistema: Gli attaccanti potrebbero aver sfruttato vulnerabilità conosciute o zero-day per compromettere i sistemi. Potrebbe essere necessario esaminare le comunicazioni di rete per individuare tentativi di sfruttare vulnerabilità note o analizzare il traffico per identificare eventuali comportamenti anomali.

Per quanto riguarda le azioni per ridurre gli impatti di un attacco:

Aggiornare e patchare i sistemi regolarmente: Assicurarsi di applicare gli aggiornamenti di sicurezza e le patch più recenti per proteggere il sistema dalle vulnerabilità note.

Utilizzare soluzioni antivirus/antimalware aggiornate: Mantenere il software antivirus/antimalware aggiornato e attivato per rilevare e bloccare eventuali minacce.

Impiegare firewall e monitoraggio del traffico di rete: Configurare e utilizzare un firewall per limitare l'accesso non autorizzato ai sistemi e monitorare attentamente il traffico di rete per individuare attività anomale.

Educazione degli utenti: Fornire formazione sulla sicurezza informatica agli utenti per insegnare loro a riconoscere le minacce comuni come phishing, attacchi di social engineering, e adottare pratiche sicure durante l'utilizzo dei sistemi.

Implementare autenticazione multi-fattore (MFA): Utilizzare l'autenticazione multi-fattore per rendere più difficile per gli attaccanti ottenere accesso non autorizzato.

Effettuare backup regolari dei dati: Eseguire backup regolari dei dati importanti e assicurarsi che siano conservati in un luogo sicuro per poter ripristinare i sistemi in caso di attacco.

Notando i vari pacchetti degli screen precedenti, si nota dove viene fatto l' handshake e dove si resetta. Molteplici sono stati i pacchetti inviati senza un motivo valido, tale da poter dedurre che si possa trattare di possibili e probabili scansioni Nmap.