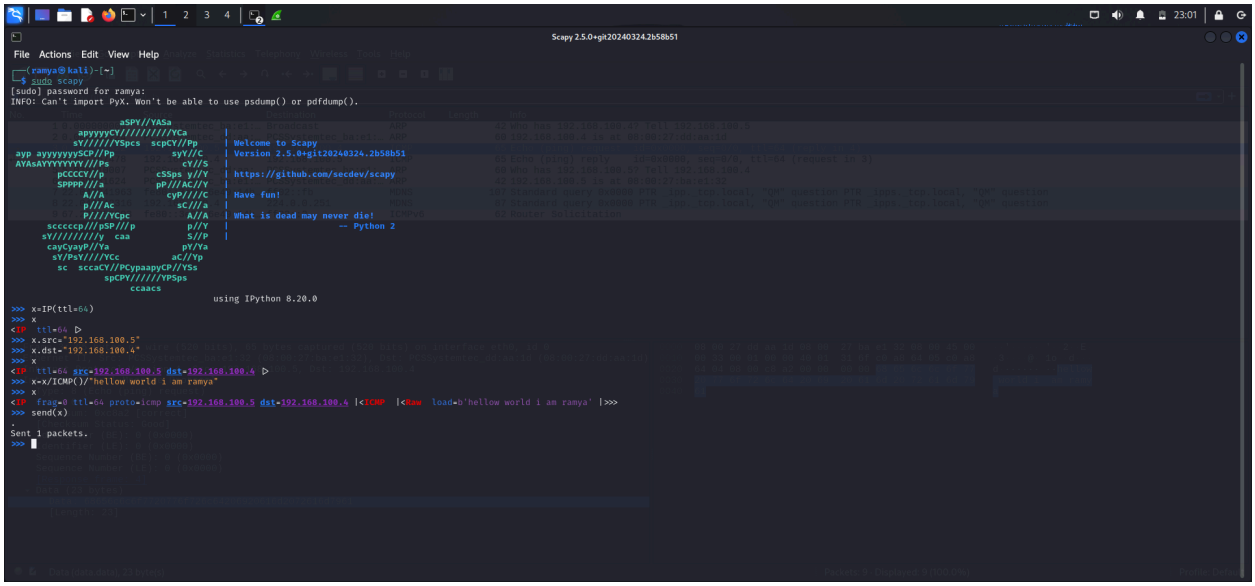
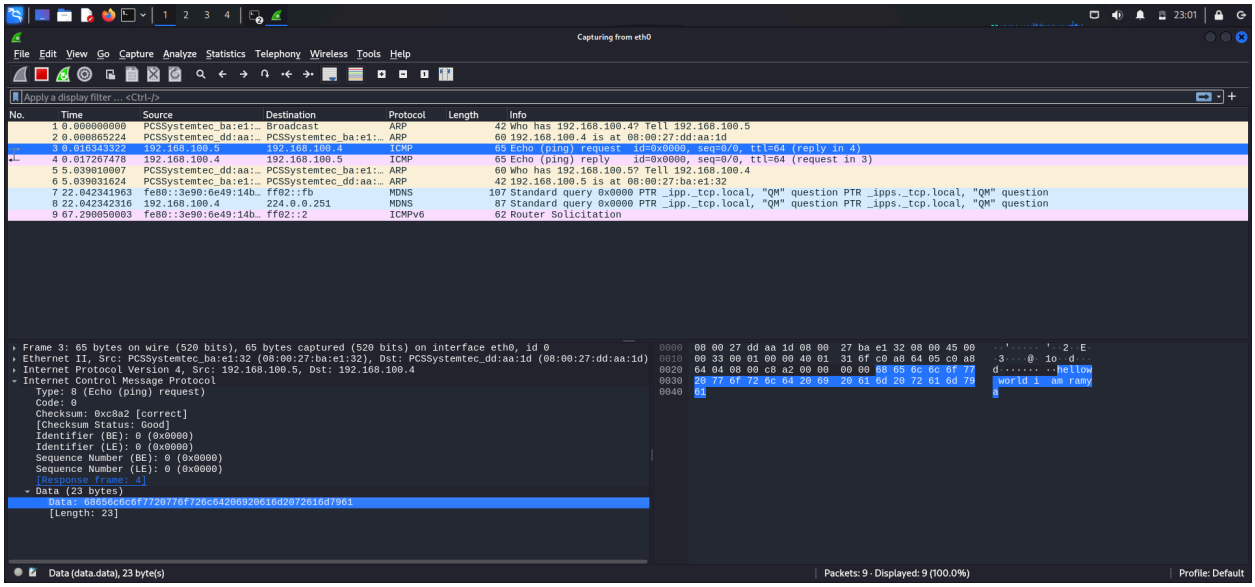
BakkaRamyasree

Create Traceroute using ICMP

SteP1:trying with one packet

- Start scapy
- Given a code which traceroute using ICMP with src addr 192.168.100.5
- And dst addr : 192.168.100.4 including a raw msg “hello world i am ramya”
- After running that i can see the packets are sent from wireshark

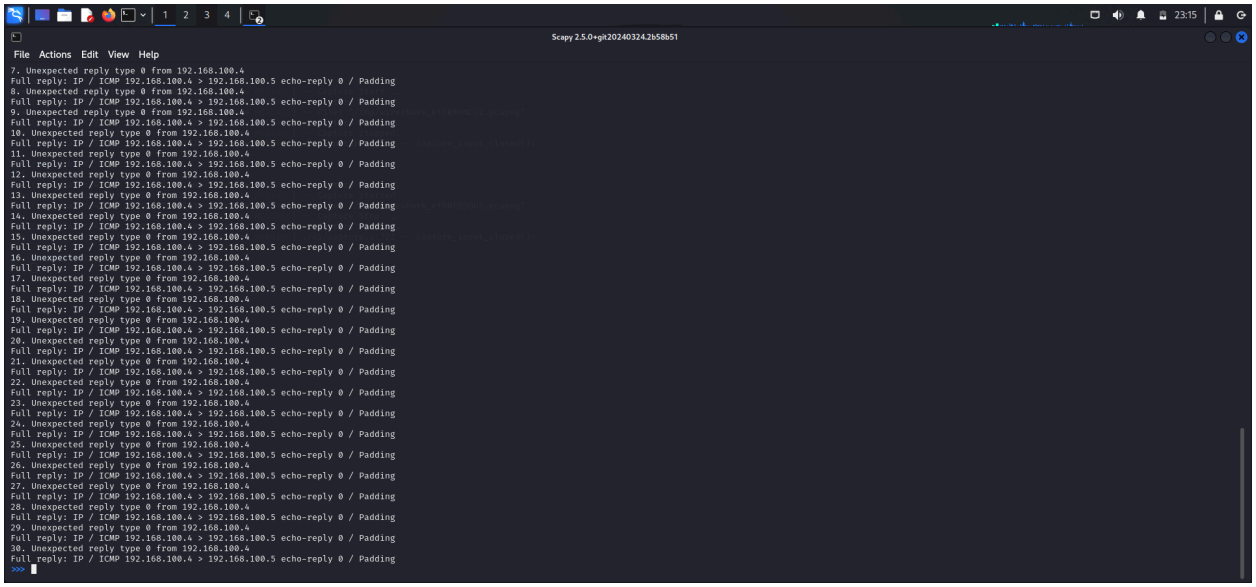


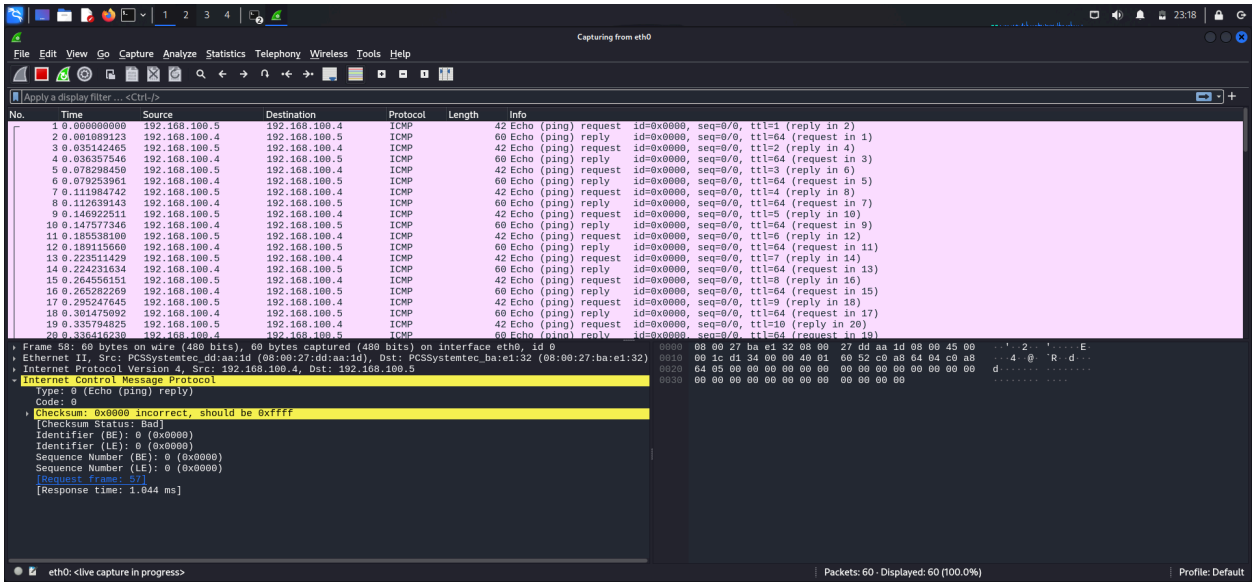


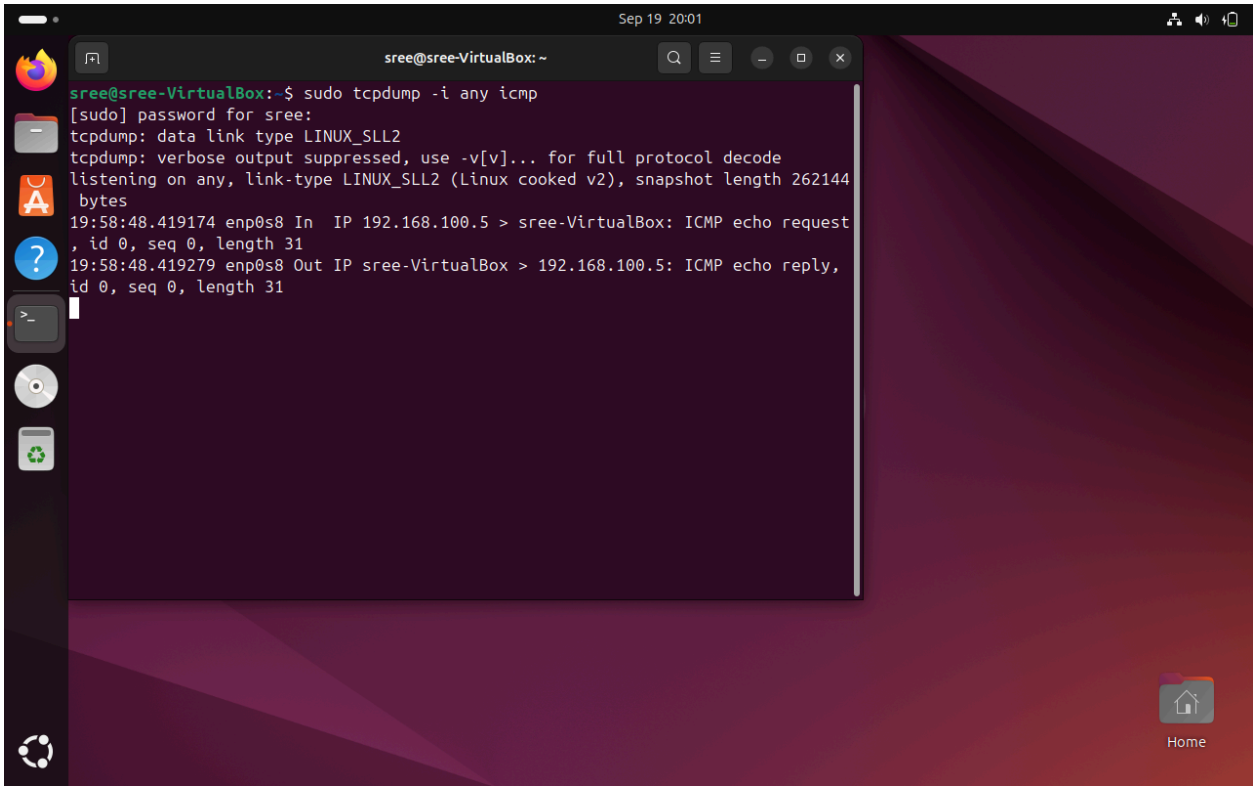
- step2:entered the code given
- Before running the code we need to check the firewall setting in ubuntu to me disable
- After executing the code i got an output saying that
-
- **25. Unexpected reply type 0 from 192.168.100.4**
- **Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding**

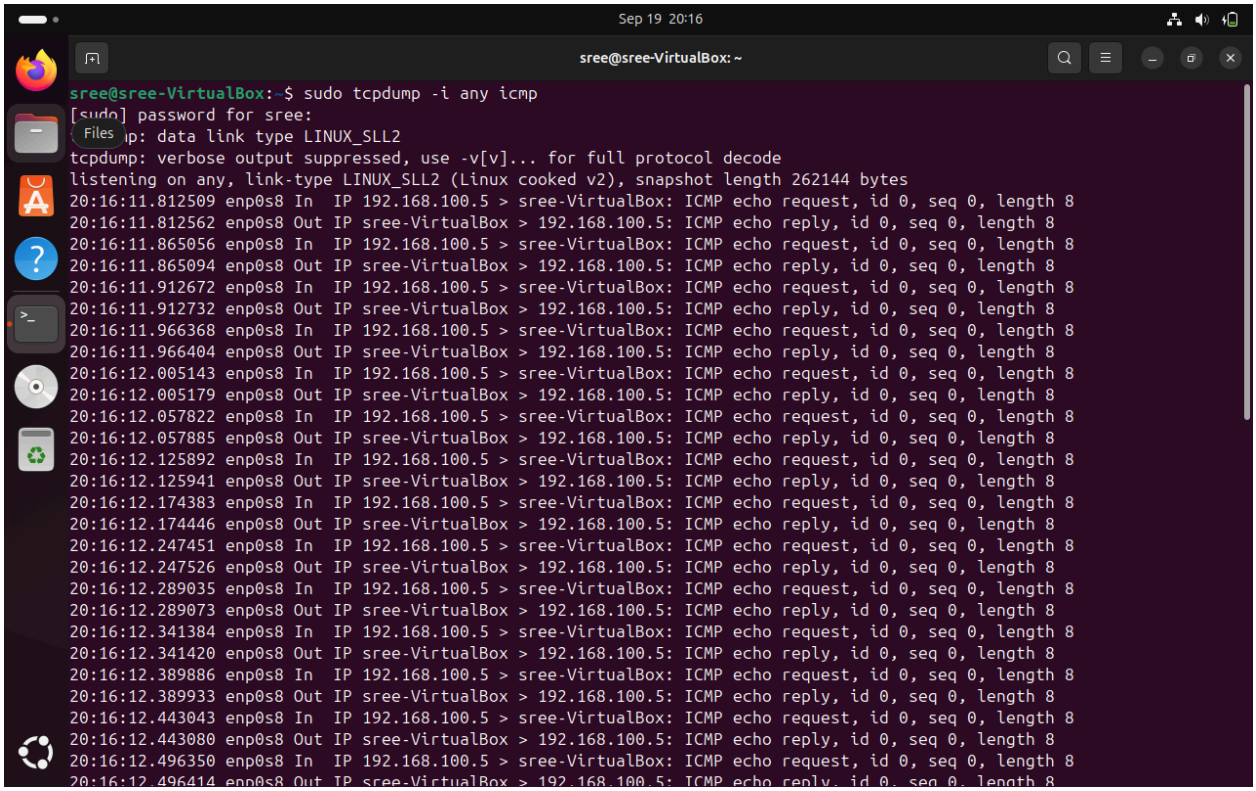
- **Output is telling reply type 0 that means Type 0 (Echo Reply): This is the reply to an ICMP Echo Request (ping). It means that the target is reachable.**
- Some common ICMP types
- Type 3 (Destination Unreachable): Indicates that the destination is unreachable. This can have various codes indicating the reason (e.g., network unreachable, host unreachable).
- Type 11 (Time Exceeded): This type is used when a packet's TTL (Time To Live) has expired, which usually happens in the context of traceroute. It indicates that a router has dropped the packet because it couldn't be delivered in time.
- Type 8 (Echo Request): This is the request type used in ping operations.


Scapy 2.5.0+git20240324.2b58b51
File Actions Edit View Help
>>> from scapy.all import IP, ICMP, sr1
... :
... : def traceroute(target_ip, max_hops=30, timeout=2):
... :   print(f"Traceroute to {target_ip}, {max_hops} hops max")
... :   for ttl in range(1, max_hops + 1):
... :   packet = IP(dst=target_ip, ttl=ttl) / ICMP()
... :   reply = sr1(packet, timeout=timeout, verbose=0)
... :
... :   if reply is None:
... :   print(f"{ttl}. No reply")
... :   continue
... :   elif reply.type == 3: # Destination Unreachable
... :   print(f"{ttl}. Reached destination {reply.src}")
... :   break
... :   elif reply.type == 11: # Time Exceeded
... :   print(f"{ttl}. Hop {reply.src}")
... :   else:
... :   print(f"{ttl}. Unexpected reply type {reply.type} from {reply.src}")
... :   print(f"Full reply: {reply.summary()}") # Detailed output
... :
... : if __name__ == "__main__":
... :   target = "192.168.100.4" # Replace with your Ubuntu IP
... :   traceroute(target)
... :
Traceroute to 192.168.100.4, 30 hops max
1. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
2. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
3. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
4. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
5. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
6. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
7. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
8. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
9. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
10. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
11. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
12. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding


Scapy 2.5.0+git20240324.2b58b51
File Actions Edit View Help
7. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
8. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
9. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
10. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
11. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
12. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
13. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
14. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
15. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
16. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
17. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
18. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
19. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
20. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
21. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
22. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
23. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
24. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
25. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
26. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
27. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
28. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
29. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
30. Unexpected reply type 0 from 192.168.100.4
Full reply: IP / ICMP 192.168.100.4 > 192.168.100.5 echo-reply 0 / Padding
>>>


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.100.5 192.168.100.4 ICMP 42 Echo (ping) request id=0x0000, seq=0/0, ttl=1 (reply in 2)
2 0.001089123 192.168.100.4 192.168.100.5 ICMP 60 Echo (ping) reply id=0x0000, seq=0/0, ttl=64 (request in 1)
3 0.035142465 192.168.100.5 192.168.100.4 ICMP 42 Echo (ping) request id=0x0000, seq=0/0, ttl=2 (reply in 4)
4 0.036357546 192.168.100.4 192.168.100.5 ICMP 60 Echo (ping) reply id=0x0000, seq=0/0, ttl=64 (request in 3)
5 0.078298450 192.168.100.5 192.168.100.4 ICMP 42 Echo (ping) request id=0x0000, seq=0/0, ttl=3 (reply in 6)
6 0.079253961 192.168.100.4 192.168.100.5 ICMP 60 Echo (ping) reply id=0x0000, seq=0/0, ttl=64 (request in 5)
7 0.111984742 192.168.100.5 192.168.100.4 ICMP 42 Echo (ping) request id=0x0000, seq=0/0, ttl=4 (reply in 8)
8 0.112639143 192.168.100.4 192.168.100.5 ICMP 60 Echo (ping) reply id=0x0000, seq=0/0, ttl=64 (request in 7)
9 0.146922511 192.168.100.5 192.168.100.4 ICMP 42 Echo (ping) request id=0x0000, seq=0/0, ttl=5 (reply in 10)
10 0.147577346 192.168.100.4 192.168.100.5 ICMP 60 Echo (ping) reply id=0x0000, seq=0/0, ttl=64 (request in 9)
11 0.185538100 192.168.100.5 192.168.100.4 ICMP 42 Echo (ping) request id=0x0000, seq=0/0, ttl=6 (reply in 12)
12 0.189115660 192.168.100.4 192.168.100.5 ICMP 60 Echo (ping) reply id=0x0000, seq=0/0, ttl=64 (request in 11)
13 0.223511429 192.168.100.5 192.168.100.4 ICMP 42 Echo (ping) request id=0x0000, seq=0/0, ttl=7 (reply in 14)
14 0.224231634 192.168.100.4 192.168.100.5 ICMP 60 Echo (ping) reply id=0x0000, seq=0/0, ttl=64 (request in 13)
15 0.264556151 192.168.100.5 192.168.100.4 ICMP 42 Echo (ping) request id=0x0000, seq=0/0, ttl=8 (reply in 16)
16 0.265282269 192.168.100.4 192.168.100.5 ICMP 60 Echo (ping) reply id=0x0000, seq=0/0, ttl=64 (request in 15)
17 0.295247645 192.168.100.5 192.168.100.4 ICMP 42 Echo (ping) request id=0x0000, seq=0/0, ttl=9 (reply in 18)
18 0.301475092 192.168.100.4 192.168.100.5 ICMP 60 Echo (ping) reply id=0x0000, seq=0/0, ttl=64 (request in 17)
19 0.335794825 192.168.100.5 192.168.100.4 ICMP 42 Echo (ping) request id=0x0000, seq=0/0, ttl=10 (reply in 20)
20 0.336416230 192.168.100.4 192.168.100.5 ICMP 60 Echo (ping) reply id=0x0000, seq=0/0, ttl=64 (request in 19)
Frame 58: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_dd:aa:1d (08:00:27:dd:aa:1d), Dst: PCSSystemtec_ba:e1:32 (08:00:27:ba:e1:32)
Internet Protocol Version 4, Src: 192.168.100.4, Dst: 192.168.100.5
Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0x0000 incorrect, should be 0xffff
[Checksum Status: Bad]
Identifier (BE): 0 (0x0000)
Identifier (LE): 0 (0x0000)
Sequence Number (BE): 0 (0x0000)
Sequence Number (LE): 0 (0x0000)
[Request frame: 57]
[Response time: 1.044 ms]
0000 08 00 27 ba e1 32 08 00 27 dd aa 1d 08 00 45 00
0010 00 1c d1 34 00 00 40 01 60 52 c0 a8 64 04 c0 a8
0020 64 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00
eth0: <live capture in progress>
Packets: 60 · Displayed: 60 (100.0%)
Profile: Default


Sep 19 20:01
sree@sree-VirtualBox: ~
sree@sree-VirtualBox:~$ sudo tcpdump -i any icmp
[sudo] password for sree:
tcpdump: data link type LINUX_SLL2
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
19:58:48.419174 enp0s8 In IP 192.168.100.5 > sree-VirtualBox: ICMP echo request, id 0, seq 0, length 31
19:58:48.419279 enp0s8 Out IP sree-VirtualBox > 192.168.100.5: ICMP echo reply, id 0, seq 0, length 31
Home


Sep 19 20:16
sree@sree-VirtualBox: ~
Files
sree@sree-VirtualBox:~$ sudo tcpdump -i any icmp
[sudo] password for sree:
tcpdump: data link type LINUX_SLL2
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
20:16:11.812509 enp0s8 In IP 192.168.100.5 > sree-VirtualBox: ICMP echo request, id 0, seq 0, length 8
20:16:11.812562 enp0s8 Out IP sree-VirtualBox > 192.168.100.5: ICMP echo reply, id 0, seq 0, length 8
20:16:11.865056 enp0s8 In IP 192.168.100.5 > sree-VirtualBox: ICMP echo request, id 0, seq 0, length 8
20:16:11.865094 enp0s8 Out IP sree-VirtualBox > 192.168.100.5: ICMP echo reply, id 0, seq 0, length 8
20:16:11.912672 enp0s8 In IP 192.168.100.5 > sree-VirtualBox: ICMP echo request, id 0, seq 0, length 8
20:16:11.912732 enp0s8 Out IP sree-VirtualBox > 192.168.100.5: ICMP echo reply, id 0, seq 0, length 8
20:16:11.966368 enp0s8 In IP 192.168.100.5 > sree-VirtualBox: ICMP echo request, id 0, seq 0, length 8
20:16:11.966404 enp0s8 Out IP sree-VirtualBox > 192.168.100.5: ICMP echo reply, id 0, seq 0, length 8
20:16:12.005143 enp0s8 In IP 192.168.100.5 > sree-VirtualBox: ICMP echo request, id 0, seq 0, length 8
20:16:12.005179 enp0s8 Out IP sree-VirtualBox > 192.168.100.5: ICMP echo reply, id 0, seq 0, length 8
20:16:12.057822 enp0s8 In IP 192.168.100.5 > sree-VirtualBox: ICMP echo request, id 0, seq 0, length 8
20:16:12.057885 enp0s8 Out IP sree-VirtualBox > 192.168.100.5: ICMP echo reply, id 0, seq 0, length 8
20:16:12.125892 enp0s8 In IP 192.168.100.5 > sree-VirtualBox: ICMP echo request, id 0, seq 0, length 8
20:16:12.125941 enp0s8 Out IP sree-VirtualBox > 192.168.100.5: ICMP echo reply, id 0, seq 0, length 8
20:16:12.174383 enp0s8 In IP 192.168.100.5 > sree-VirtualBox: ICMP echo request, id 0, seq 0, length 8
20:16:12.174446 enp0s8 Out IP sree-VirtualBox > 192.168.100.5: ICMP echo reply, id 0, seq 0, length 8
20:16:12.247451 enp0s8 In IP 192.168.100.5 > sree-VirtualBox: ICMP echo request, id 0, seq 0, length 8
20:16:12.247526 enp0s8 Out IP sree-VirtualBox > 192.168.100.5: ICMP echo reply, id 0, seq 0, length 8
20:16:12.289035 enp0s8 In IP 192.168.100.5 > sree-VirtualBox: ICMP echo request, id 0, seq 0, length 8
20:16:12.289073 enp0s8 Out IP sree-VirtualBox > 192.168.100.5: ICMP echo reply, id 0, seq 0, length 8
20:16:12.341384 enp0s8 In IP 192.168.100.5 > sree-VirtualBox: ICMP echo request, id 0, seq 0, length 8
20:16:12.341420 enp0s8 Out IP sree-VirtualBox > 192.168.100.5: ICMP echo reply, id 0, seq 0, length 8
20:16:12.389886 enp0s8 In IP 192.168.100.5 > sree-VirtualBox: ICMP echo request, id 0, seq 0, length 8
20:16:12.389933 enp0s8 Out IP sree-VirtualBox > 192.168.100.5: ICMP echo reply, id 0, seq 0, length 8
20:16:12.443043 enp0s8 In IP 192.168.100.5 > sree-VirtualBox: ICMP echo request, id 0, seq 0, length 8
20:16:12.443080 enp0s8 Out IP sree-VirtualBox > 192.168.100.5: ICMP echo reply, id 0, seq 0, length 8
20:16:12.496350 enp0s8 In IP 192.168.100.5 > sree-VirtualBox: ICMP echo request, id 0, seq 0, length 8