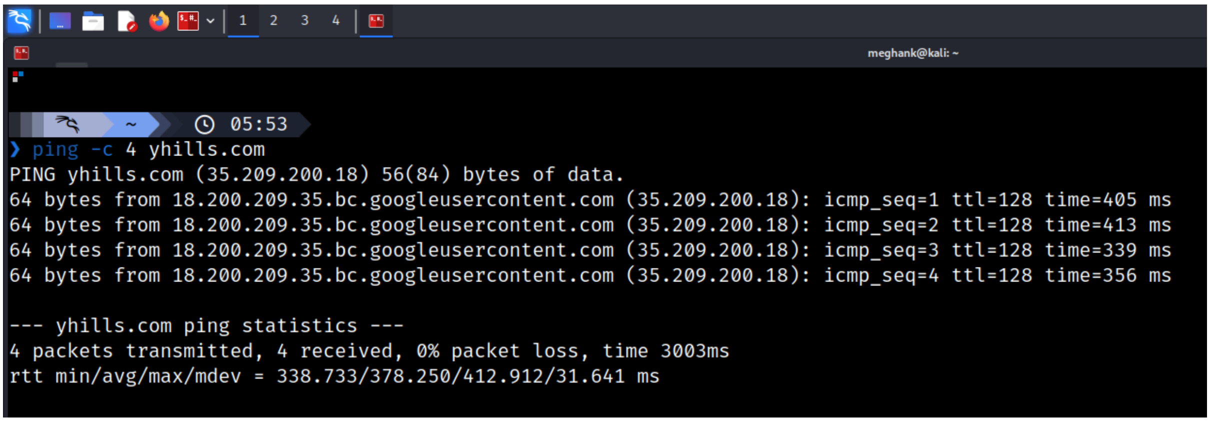
Day 7

Ping Command :

It is used to verify that whether we can able to establish connection between target or not.

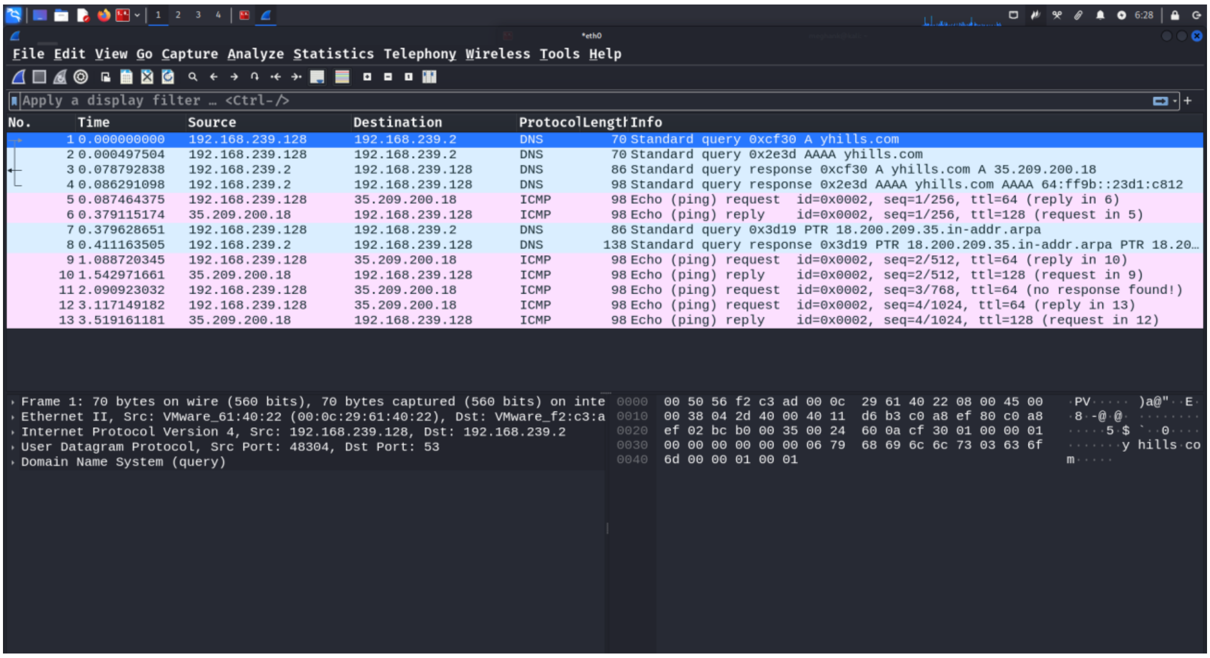


```
~  05:53
❯ ping -c 4 yhills.com
PING yhills.com (35.209.200.18) 56(84) bytes of data.
64 bytes from 18.200.209.35.bc.googleusercontent.com (35.209.200.18): icmp_seq=1 ttl=128 time=405 ms
64 bytes from 18.200.209.35.bc.googleusercontent.com (35.209.200.18): icmp_seq=2 ttl=128 time=413 ms
64 bytes from 18.200.209.35.bc.googleusercontent.com (35.209.200.18): icmp_seq=3 ttl=128 time=339 ms
64 bytes from 18.200.209.35.bc.googleusercontent.com (35.209.200.18): icmp_seq=4 ttl=128 time=356 ms

--- yhills.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 338.733/378.250/412.912/31.641 ms
```

Wireshark :

It is network monitoring tool that give brief information about each packet and also show all communication in network via packet.


1
2
3
4
*eth0
6:28
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

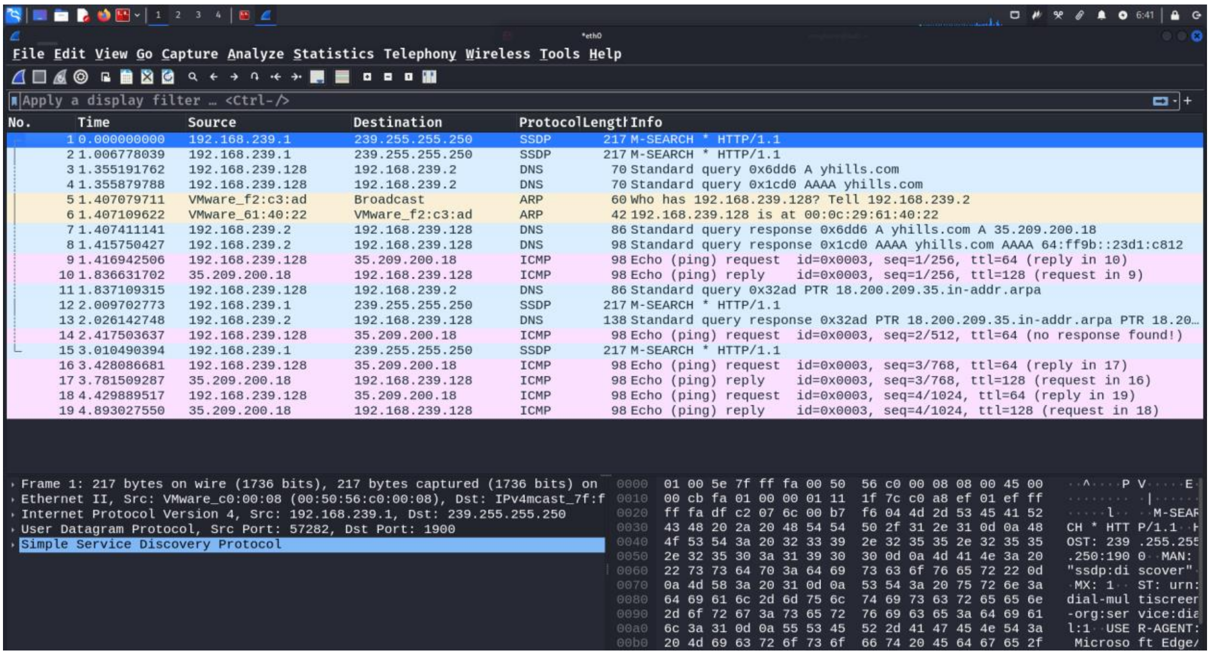
```
No.    Time         Source           Destination      ProtocolLengthInfo
    1 0.000000000  192.168.239.128  192.168.239.2    DNS        70 Standard query 0xcf30 A yhills.com
    2 0.000497504  192.168.239.128  192.168.239.2    DNS        70 Standard query 0x2e3d AAAA yhills.com
    3 0.078792838  192.168.239.2    192.168.239.128  DNS        86 Standard query response 0xcf30 A yhills.com A 35.209.200.18
    4 0.086291098  192.168.239.2    192.168.239.128  DNS        98 Standard query response 0x2e3d AAAA yhills.com AAAA 64:ff9b::23d1:c812
    5 0.087464375  192.168.239.128  35.209.200.18    ICMP       98 Echo (ping) request  id=0x0002, seq=1/256, ttl=64 (reply in 6)
    6 0.379115174  35.209.200.18    192.168.239.128  ICMP       98 Echo (ping) reply    id=0x0002, seq=1/256, ttl=128 (request in 5)
    7 0.379628651  192.168.239.128  192.168.239.2    DNS        86 Standard query 0x3d19 PTR 18.200.209.35.in-addr.arpa
    8 0.411163505  192.168.239.2    192.168.239.128  DNS       138 Standard query response 0x3d19 PTR 18.200.209.35.in-addr.arpa PTR 18.20…
    9 1.088720345  192.168.239.128  35.209.200.18    ICMP       98 Echo (ping) request  id=0x0002, seq=2/512, ttl=64 (reply in 10)
   10 1.542971661  35.209.200.18    192.168.239.128  ICMP       98 Echo (ping) reply    id=0x0002, seq=2/512, ttl=128 (request in 9)
   11 2.090923032  192.168.239.128  35.209.200.18    ICMP       98 Echo (ping) request  id=0x0002, seq=3/768, ttl=64 (no response found!)
   12 3.117149182  192.168.239.128  35.209.200.18    ICMP       98 Echo (ping) request  id=0x0002, seq=4/1024, ttl=64 (reply in 13)
   13 3.519161181  35.209.200.18    192.168.239.128  ICMP       98 Echo (ping) reply    id=0x0002, seq=4/1024, ttl=128 (request in 12)
```

```
› Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on inte   0000  00 50 56 f2 c3 ad 00 0c  29 61 40 22 08 00 45 00   ·PV·····)a@"··E·
› Ethernet II, Src: VMware_61:40:22 (00:0c:29:61:40:22), Dst: VMware_f2:c3:a   0010  00 38 04 2d 40 00 40 11  d6 b3 c0 a8 ef 80 c0 a8   ·8·-@·@·········
› Internet Protocol Version 4, Src: 192.168.239.128, Dst: 192.168.239.2        0020  ef 02 bc b0 00 35 00 24  60 0a cf 30 01 00 00 01   ·····5·$`··0····
› User Datagram Protocol, Src Port: 48304, Dst Port: 53                        0030  00 00 00 00 00 00 06 79  68 69 6c 6c 73 03 63 6f   ·······yhills·co
› Domain Name System (query)                                                   0040  6d 00 00 01 00 01                                  m·····
```

You can also use Wireshark filtration to get more precise output , It is kind of rule we can apply and at the result wireshark display packets we want.

Wireshark official manual is best for filteration : DisplayFilters - Wireshark Wiki

Example : packet communication of command “ping -c 4 yhills.com”



*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

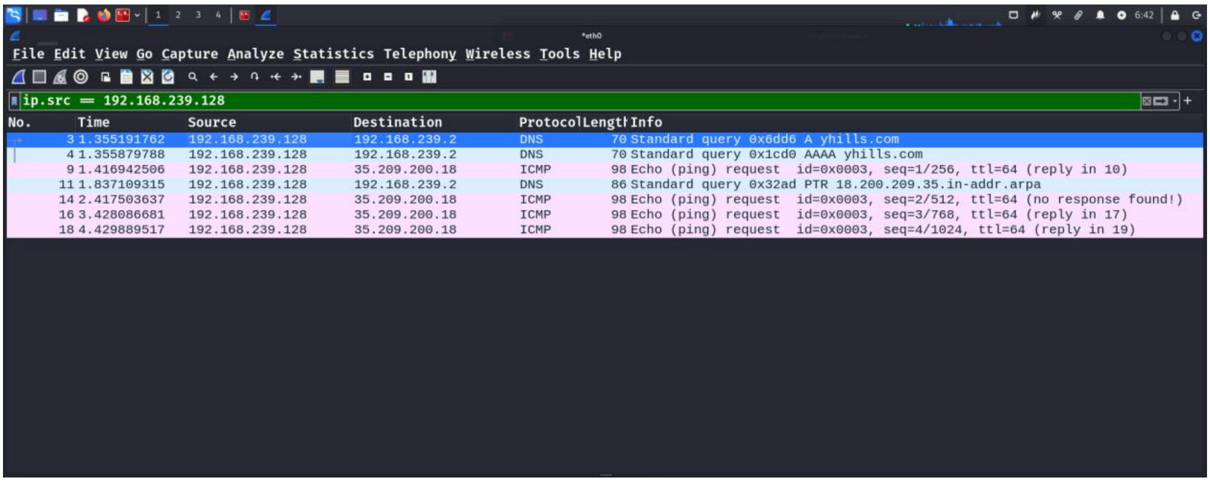
```
No.   Time          Source            Destination       Protocol Length Info
    1 0.000000000   192.168.239.1     239.255.255.250   SSDP      217 M-SEARCH * HTTP/1.1
    2 1.006778039   192.168.239.1     239.255.255.250   SSDP      217 M-SEARCH * HTTP/1.1
    3 1.355191762   192.168.239.128   192.168.239.2     DNS        70 Standard query 0x6dd6 A yhills.com
    4 1.355879788   192.168.239.128   192.168.239.2     DNS        70 Standard query 0x1cd0 AAAA yhills.com
    5 1.407079711   VMware_f2:c3:ad   Broadcast         ARP        60 Who has 192.168.239.128? Tell 192.168.239.2
    6 1.407109622   VMware_61:40:22   VMware_f2:c3:ad   ARP        42 192.168.239.128 is at 00:0c:29:61:40:22
    7 1.407411141   192.168.239.2     192.168.239.128   DNS        86 Standard query response 0x6dd6 A yhills.com A 35.209.200.18
    8 1.415750427   192.168.239.2     192.168.239.128   DNS        98 Standard query response 0x1cd0 AAAA yhills.com AAAA 64:ff9b::23d1:c812
    9 1.416942506   192.168.239.128   35.209.200.18     ICMP       98 Echo (ping) request  id=0x0003, seq=1/256, ttl=64 (reply in 10)
   10 1.836631702   35.209.200.18     192.168.239.128   ICMP       98 Echo (ping) reply    id=0x0003, seq=1/256, ttl=128 (request in 9)
   11 1.837109315   192.168.239.128   192.168.239.2     DNS        86 Standard query 0x32ad PTR 18.200.209.35.in-addr.arpa
   12 2.009702773   192.168.239.1     239.255.255.250   SSDP      217 M-SEARCH * HTTP/1.1
   13 2.026142748   192.168.239.2     192.168.239.128   DNS       138 Standard query response 0x32ad PTR 18.200.209.35.in-addr.arpa PTR 18.20…
   14 2.417503637   192.168.239.128   35.209.200.18     ICMP       98 Echo (ping) request  id=0x0003, seq=2/512, ttl=64 (no response found!)
   15 3.010490394   192.168.239.1     239.255.255.250   SSDP      217 M-SEARCH * HTTP/1.1
   16 3.428086681   192.168.239.128   35.209.200.18     ICMP       98 Echo (ping) request  id=0x0003, seq=3/768, ttl=64 (reply in 17)
   17 3.781509287   35.209.200.18     192.168.239.128   ICMP       98 Echo (ping) reply    id=0x0003, seq=3/768, ttl=128 (request in 16)
   18 4.429889517   192.168.239.128   35.209.200.18     ICMP       98 Echo (ping) request  id=0x0003, seq=4/1024, ttl=64 (reply in 19)
   19 4.893027550   35.209.200.18     192.168.239.128   ICMP       98 Echo (ping) reply    id=0x0003, seq=4/1024, ttl=128 (request in 18)
```

```
› Frame 1: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on
› Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: IPv4mcast_7f:f
› Internet Protocol Version 4, Src: 192.168.239.1, Dst: 239.255.255.250
› User Datagram Protocol, Src Port: 57282, Dst Port: 1900
› Simple Service Discovery Protocol
```

```
0000  01 00 5e 7f ff fa 00 50  56 c0 00 08 08 00 45 00   ··^····P V·····E·
0010  00 cb fa 01 00 00 01 11  1f 7c c0 a8 ef 01 ef ff   ········ ·|······
0020  ff fa df c2 07 6c 00 b7  f6 04 4d 2d 53 45 41 52   ·····l·· ··M-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1··H
0040  4f 53 54 3a 20 32 33 39  2e 32 35 35 2e 32 35 35   OST: 239 .255.255
0050  2e 32 35 30 3a 31 39 30  30 0d 0a 4d 41 4e 3a 20   .250:190 0··MAN: 
0060  22 73 73 64 70 3a 64 69  73 63 6f 76 65 72 22 0d   "ssdp:di scover"·
0070  0a 4d 58 3a 20 31 0d 0a  53 54 3a 20 75 72 6e 3a   ·MX: 1·· ST: urn:
0080  64 69 61 6c 2d 6d 75 6c  74 69 73 63 72 65 65 6e   dial-mul tiscreen
0090  2d 6f 72 67 3a 73 65 72  76 69 63 65 3a 64 69 61   -org:ser vice:dia
00a0  6c 3a 31 0d 0a 55 53 45  52 2d 41 47 45 4e 54 3a   l:1··USE R-AGENT:
00b0  20 4d 69 63 72 6f 73 6f  66 74 20 45 64 67 65 2f    Microso ft Edge/
```

We want to see only packets with source address of my kali linux.

Filter is : ip.src == 192.168.239.128



*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.src == 192.168.239.128
```

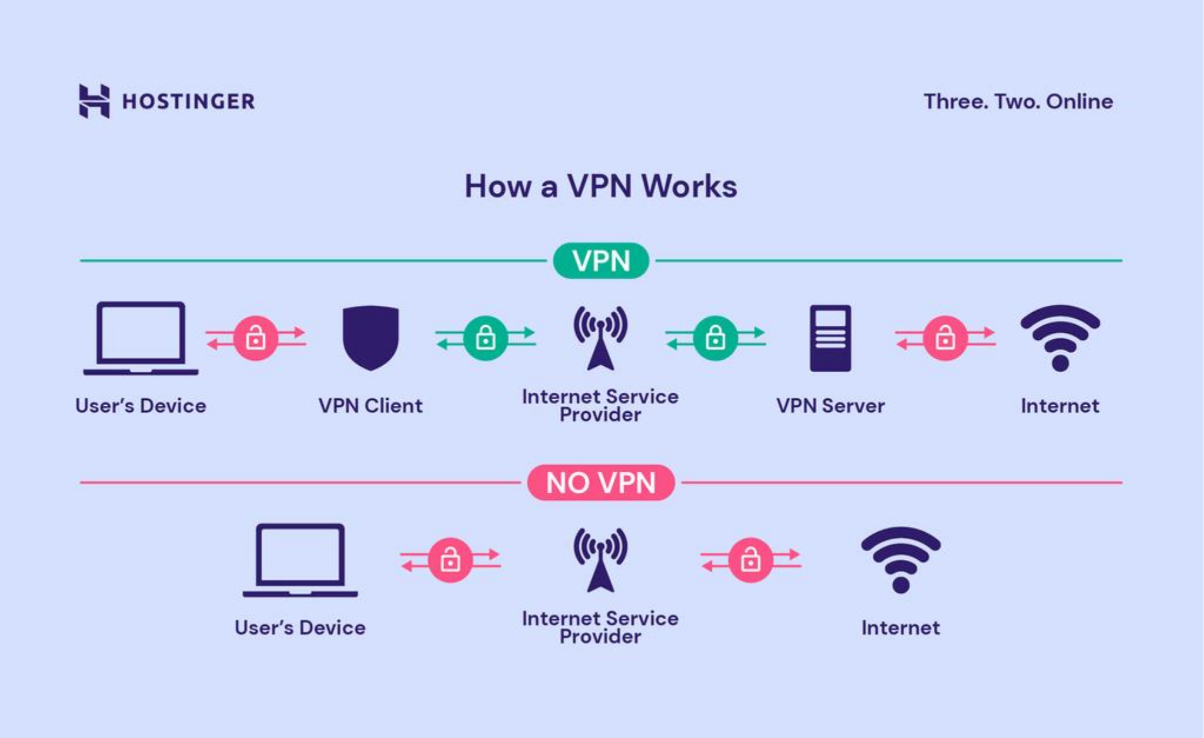
```
No.   Time          Source            Destination       Protocol Length Info
    3 1.355191762   192.168.239.128   192.168.239.2     DNS        70 Standard query 0x6dd6 A yhills.com
    4 1.355879788   192.168.239.128   192.168.239.2     DNS        70 Standard query 0x1cd0 AAAA yhills.com
    9 1.416942506   192.168.239.128   35.209.200.18     ICMP       98 Echo (ping) request  id=0x0003, seq=1/256, ttl=64 (reply in 10)
   11 1.837109315   192.168.239.128   192.168.239.2     DNS        86 Standard query 0x32ad PTR 18.200.209.35.in-addr.arpa
   14 2.417503637   192.168.239.128   35.209.200.18     ICMP       98 Echo (ping) request  id=0x0003, seq=2/512, ttl=64 (no response found!)
   16 3.428086681   192.168.239.128   35.209.200.18     ICMP       98 Echo (ping) request  id=0x0003, seq=3/768, ttl=64 (reply in 17)
   18 4.429889517   192.168.239.128   35.209.200.18     ICMP       98 Echo (ping) request  id=0x0003, seq=4/1024, ttl=64 (reply in 19)
```

Additional: You can check fraudulent score of any ip address at this website - https://scamalytics.com/

To get detail info about IP-Adress : https://ip-api.com/

What is VPN:

VPN stands for "Virtual Private Network" and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity. This makes it more difficult for third parties to track your activities online and steal data. The encryption takes place in real time.



“Highly recommended that Don’t Use Free VPN”

Because free VPN are not trusted as paid VPNs, free VPN server may use tool like Wireshark to capture packets so they can easily capture your data without your permission and you all internet activity is stored by free VPN providers .

Additionally they can decrypt your packet and can steal your password and other important credentials.