

## Wireshark Evidence – ICMP to Google DNS using send()

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	172.16.161.129	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 2)
2	0.019549165	8.8.8.8	172.16.161.129	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=128 (request in 1)

```

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface
  Interface id: 0 (ens160)
  Encapsulation type: Ethernet (1)
  Arrival Time: Oct 23, 2025 14:35:52.881012079 UTC
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1761230152.881012079 seconds
  [Time delta from previous captured frame: 0.000000000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 0.000000000 seconds]
  Frame Number: 1
  Frame Length: 74 bytes (592 bits)
  Capture Length: 74 bytes (592 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:icmp:data]
  [Coloring Rule Name: ICMP]
  [Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: VMware_a4:0d:6d (00:0c:29:a4:0d:6d), Dst: VMware_ed:09:1a (00:50:56:ed:09:1a)
  Destination: VMware_ed:09:1a (00:50:56:ed:09:1a)
    Address: VMware_ed:09:1a (00:50:56:ed:09:1a)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
  Source: VMware_a4:0d:6d (00:0c:29:a4:0d:6d)
    0000 00 50 56 ed 09 1a 00 0c 29 a4 0d 6d 08 00 45 00 .PV.... )..m..E
    0010 00 3c 00 04 40 00 80 01 9d 1b ac 10 a1 81 08 08 .<..@. ....
    0020 08 08 08 00 f7 fd 00 01 00 01 00 00 00 00 00 00 .....
    0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
    0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

```

seed@niranjan: /mnt/hgfs/cosc60-lab3
seed@niranjan:/mnt/hgfs/cosc60-lab3$ sudo python3 test.py
Ping example
[*] Sent packet to 8.8.8.8
seed@niranjan:/mnt/hgfs/cosc60-lab3$ sudo python3 test.py
Ping example
[*] Sent packet to 8.8.8.8
seed@niranjan:/mnt/hgfs/cosc60-lab3$

```

## Wireshark Evidence – ICMP to Google DNS using sendp()

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	172.16.161.1	172.16.161.255	UDP	86	57621 → 57621 Len=44
2	3.461608220	172.16.161.129	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 5)
3	3.490407320	VMware_ed:09:1a	Broadcast	ARP	60	Who has 172.16.161.129? Tell 172.16.161.2
4	3.490463276	VMware_a4:0d:6d	VMware_ed:09:1a	ARP	42	172.16.161.129 is at 00:0c:29:a4:0d:6d
5	3.490613062	8.8.8.8	172.16.161.129	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=128 (request in 2)

  

▼ Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface id: 0 (ens160)

Interface id: 0 (ens160)

Encapsulation type: Ethernet (1)

Arrival Time: Oct 23, 2025 14:39:08.166746343 UTC

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1761230348.166746343 seconds

[Time delta from previous captured frame: 3.461608220 seconds]

[Time delta from previous displayed frame: 3.461608220 seconds]

[Time since reference or first frame: 3.461608220 seconds]

Frame Number: 2

Frame Length: 74 bytes (592 bits)

Capture Length: 74 bytes (592 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:icmp:data]

[Coloring Rule Name: ICMP]

[Coloring Rule String: icmp || icmpv6]

▼ Ethernet II, Src: VMware\_a4:0d:6d (00:0c:29:a4:0d:6d), Dst: VMware\_ed:09:1a (00:50:56:ed:09:1a)

Destination: VMware\_ed:09:1a (00:50:56:ed:09:1a)

Address: VMware\_ed:09:1a (00:50:56:ed:09:1a)

.... 0. .... = LG bit: Globally unique address (factory default)

.... 0 .... = IG bit: Individual address (unicast)

Source: VMware\_a4:0d:6d (00:0c:29:a4:0d:6d)

  

```

seed@niranjan: /mnt/hgfs/cosc60-lab3
seed@niranjan:/mnt/hgfs/cosc60-lab3$ sudo python3 test.py
Ping example
[*] Sent packet on interface ens160
seed@niranjan:/mnt/hgfs/cosc60-lab3$

```

  

```

0000 00 50 56 ed 09 1a 00 0c 29 a4 0d 6d 08 00 45 00  .PV.... )..m..E
0010 00 3c 00 04 40 00 80 01 9d 1b ac 10 a1 81 08 08  <...@... ..
0020 08 08 08 00 f7 fd 00 01 00 01 00 00 00 00 00 00  .....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....

```

## Wireshark Evidence – ICMP to Google DNS using sr()

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	172.16.161.129	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 2)
2	0.019897558	8.8.8.8	172.16.161.129	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=128 (request in 1)

  

▼ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0 (ens160)

- Interface id: 0 (ens160)
- Encapsulation type: Ethernet (1)
- Arrival Time: Oct 23, 2025 14:41:26.735731126 UTC
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1761230486.735731126 seconds
- [Time delta from previous captured frame: 0.000000000 seconds]
- [Time delta from previous displayed frame: 0.000000000 seconds]
- [Time since reference or first frame: 0.000000000 seconds]
- Frame Number: 1
- Frame Length: 74 bytes (592 bits)
- Capture Length: 74 bytes (592 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: eth:ethertype:ip:icmp:data]
- [Coloring Rule Name: ICMP]
- [Coloring Rule String: icmp || icmpv6]

▼ Ethernet II, Src: VMware\_a4:0d:6d (00:0c:29:a4:0d:6d), Dst: VMware\_ed:09:1a (00:50:56:ed:09:1a)

- Destination: VMware\_ed:09:1a (00:50:56:ed:09:1a)
- Address: VMware\_ed:09:1a (00:50:56:ed:09:1a)
- .... .. = LG bit: Globally unique address (factory default)
- .... .. = IG bit: Individual address (unicast)
- Source: VMware\_a4:0d:6d (00:0c:29:a4:0d:6d)

Offset	Hex	ASCII
0000	00 50 56 ed 09 1a 00 0c 29 a4 0d 6d 08 00 45 00	.PV.....).m..E
0010	00 3c 00 04 40 00 80 01 9d 1b ac 10 a1 81 08 08	<...@.....
0020	08 08 08 00 f7 fd 00 01 00 01 00 00 00 00 00 00	.....
0030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0040	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....

Epoch time when this frame was captured (frame.time\_epoch)

## DNS Request to resolve vibrantcloud.org:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	172.16.161.129	8.8.8.8	DNS	76	Standard query 0x3121 A vibrantcloud.org
2	0.020692054	8.8.8.8	172.16.161.129	DNS	92	Standard query response 0x3121 A vibrantcloud.org A 173.201.179.249
3	0.020746508	172.16.161.129	8.8.8.8	ICMP		

  

Flags: 0x8180 Standard query response, No error  
Questions: 1  
Answer RRs: 1  
Authority RRs: 0  
Additional RRs: 0

Queries

- vibrantcloud.org: type A, class IN  
Name: vibrantcloud.org  
[Name Length: 16]  
[Label Count: 2]  
Type: A (Host Address) (1)  
Class: IN (0x0001)

Answers

- vibrantcloud.org: type A, class IN, addr 173.201.179.249  
Name: vibrantcloud.org  
Type: A (Host Address) (1)  
Class: IN (0x0001)  
Time to live: 578 (9 minutes, 38 seconds)  
Data length: 4  
Address: 173.201.179.249  
[Unsolicited: True]

  

0000	00 50 56 ed 09 1a 00 0c 29 a4 0d 6d 08 00 45 c0	.PV..... )..
0010	00 6a 52 25 00 00 40 01 ca 0c ac 10 a1 81 08 08	.jR%..@. ...
0020	08 08 03 03 5a ea 00 00 00 00 45 00 00 4e 1e 6f	....Z....E
0030	00 00 80 11 be 8e 08 08 08 08 ac 10 a1 81 00 35	.....
0040	00 35 00 3a 66 aa 31 21 81 80 00 01 00 01 00 00	.5.:f.1! ...

  

Epoch time when this frame was captured (frame.time\_epoch)

seed@niranjan: /mnt/hgfs/cosc60-lab3

Packets: 3 - Displayed: 3 (100.0%) - Dropped: 0 (0.0%) Profile: Default

Evidence for Making TCP/HTTP request to vibrantcloud.org

### CODE:

*#Example 2: DNS Resolution*

```
print("\nDNS example")
domain_name = "vibrantcloud.org"
pkt = Ether(src_mac=my_mac, dst_mac=dst_mac)/IP(src_ip=my_ip, dst_ip="8.8.8.8", proto=17)/UDP(sport=12345,
dport=53)/DNS(qname=domain_name)
dns = sr(pkt)
dns.show()
dns_layer = dns.get_layer("DNS") #helper method to get a specified layer
#print(dns_layer.addr)
addr = dns_layer.addr
print("\n\n")

# #Example 3: TCP/HTTP
print("\nTCP example")
sport = random.getrandbits(16)
#turn off OS replying with RST after recieving SYN ACK reply from server
command = ['sudo', 'iptables', '-A', 'OUTPUT', '-p', 'tcp', '-m', 'tcp', '--tcp-flags', 'RST', 'RST', '-j', 'DROP']
# Execute the command
result = subprocess.run(command, check=True, capture_output=True, text=True)
print("STDOUT:", result.stdout)
print("STDERR:", result.stderr)

pkt = Ether(src_mac=my_mac, dst_mac=dst_mac)/IP(src_ip=my_ip, dst_ip=addr)/TCP(sport=sport, dport=80, flag='SYN')
reply = sr(pkt)
reply.show()
tcp = reply.get_layer('TCP')

my_seq = tcp.ack #GenAI helped refactor this section to more cleanly track seq and ack
my_ack = tcp.seq + 1
```

```

    pkt = Ether(src_mac=my_mac, dst_mac=dst_mac)/IP(src_ip=my_ip, dst_ip=addr)/TCP(sport=sport, dport=80, seq=my_seq,
ack=my_ack, flag='ACK')
    sendp(pkt, "ens160")

    http_request = f'GET / HTTP/1.1\r\nHost: vibrantcloud.org\r\n\r\n' # GenAI adjusted to correct formatting with this
    pkt = Ether(src_mac=my_mac, dst_mac=dst_mac)/IP(src_ip=my_ip, dst_ip=addr)/TCP(sport=sport, dport=80, seq=my_seq,
ack=my_ack, data=http_request, flag='PSH')
    rp = sr(pkt)
    rp.show()

    tcp_reply = rp.get_layer('TCP')
    rp = sniff("ens160")

    print("SNIFF")
    rp.show()
    tcp_reply = rp.get_layer('TCP')
    #print(tcp_reply.payload.decode())

    #reset firewall rules
    command = ['sudo', 'iptables', '-D', 'OUTPUT', '-p', 'tcp', '-m', 'tcp', '--tcp-flags', 'RST', 'RST', '-j', 'DROP']
    result = subprocess.run(command, check=True, capture_output=True, text=True)
    print("STDOUT:", result.stdout)
    print("STDERR:", result.stderr)

```

## RESPONSE:

[\*] Sent packet to 8.8.8.8, waiting for reply...

[\*] Received reply

... DNS resolution responds, and we get the IP.

TCP example

STDOUT:

STDERR:

[\*] Sent packet to 173.201.179.249, waiting for reply...

[\*] Received reply

##### Ether #####

dst\_mac : 00:0c:29:a4:0d:6d

src\_mac : 00:50:56:ed:09:1a

type : 2048

bytes:

000c29a40d6d005056ed091a08004500002c20e9000080066a8eadc9b3f9ac10a1810050527627b163c5000000026012faf00f920000020405b40000

##### IP #####

version\_ihl : 69

tos : 0

len : 44

id : 8425

flags\_frag : 0

ttl : 128

proto : 6

chksum : 27278

src\_ip : 173.201.179.249

dst\_ip : 172.16.161.129

bytes: 4500002c20e9000080066a8eadc9b3f9ac10a1810050527627b163c5000000026012faf00f920000020405b40000

##### TCP #####

sport : 80

dport : 21110

seq : 665936837

ack : 2

offset\_reserv\_flags : 24594

window : 64240

chksum : 3986

urgptr : 0

offset : 6

message :

[\*] Sent packet on interface ens160

[\*] Sent packet to 173.201.179.249, waiting for reply...

[\*] Received reply

##### Ether #####

dst\_mac : 00:0c:29:a4:0d:6d

src\_mac : 00:50:56:ed:09:1a

type : 2048

bytes:

000c29a40d6d005056ed091a08004500002820ea000080066a91adc9b3f9ac10a1810050527627b163c60000002c5010faf02725000000  
0000000000

##### IP #####

version\_ihl : 69

tos : 0

len : 40

id : 8426

flags\_frag : 0

ttl : 128

proto : 6

chksum : 27281

src\_ip : 173.201.179.249

dst\_ip : 172.16.161.129

bytes: 4500002820ea000080066a91adc9b3f9ac10a1810050527627b163c60000002c5010faf027250000000000000000

##### TCP #####

sport : 80

dport : 21110

seq : 665936838

ack : 44

offset\_reserv\_flags : 20496

window : 64240

chksum : 10021

urgptr : 0

offset : 5

message :

[\*] Captured packet



# SNIFF

##### Ether #####

dst\_mac : 00:0c:29:a4:0d:6d

src\_mac : 00:50:56:ed:09:1a

type : 2048

bytes:

000c29a40d6d005056ed091a08004500027920eb00008006683fadc9b3f9ac10a1810050527627b163c60000002c5018faf0d7a3000048  
5454502f312e3120323030204f4b0d0a446174653a205468752c203233204f637420323032352031343a35333a323020474d540d0a536  
5727665723a204170616368650d0a557067726164653a2068322c6832630d0a436f6e6e656374696f6e3a20557067726164650d0a4c61  
73742d4d6f6469666965643a204672692c2031362041707220323032312031353a31373a333020474d540d0a455461673a20223162323  
13061352d3133372d35633031383761373833363830220d0a4163636570742d52616e6765733a2062797465730d0a436f6e74656e742d  
4c656e6774683a203331310d0a566172793a204163636570742d456e636f64696e670d0a436f6e74656e742d547970653a20746578742f  
68746d6c0d0a0d0a3c21646f63747970652068746d6c3e0a0a3c68746d6c206c616e673d22656e223e0a3c686561643e0a20203c6d6574  
6120636861727365743d227574662d38223e0a0a20203c7469746c653e56696272616e74436c6f75643c2f7469746c653e0a20203c6d65  
7461206e616d653d226465736372697074696f6e2220636f6e74656e743d2256696272616e74436c6f7564223e0a20203c6d657461206e  
616d653d22617574686f722220636f6e74656e743d22416e6f6e223e0a0a3c2f686561643e0a0a3c626f64793e0a20203c68313e5669627  
2616e74436c6f75643c2f68313e0a20203c703e54686973206973207468652066616d6f75732056696272616e74436c6f756420796f752  
7766520686561726420736f206d7563682061626f75742e3c2f703e0a3c2f626f64793e0a3c2f68746d6c3e

##### IP #####

version\_ihl : 69

tos : 0

len : 633

id : 8427

flags\_frag : 0

ttl : 128

proto : 6

chksum : 26687

src\_ip : 173.201.179.249

dst\_ip : 172.16.161.129

bytes:

4500027920eb00008006683fadc9b3f9ac10a1810050527627b163c60000002c5018faf0d7a30000485454502f312e3120323030204f4b0  
d0a446174653a205468752c203233204f637420323032352031343a35333a323020474d540d0a5365727665723a204170616368650d0a  
557067726164653a2068322c6832630d0a436f6e6e656374696f6e3a20557067726164650d0a4c6173742d4d6f6469666965643a204672

692c2031362041707220323032312031353a31373a333020474d540d0a455461673a2022316232313061352d3133372d356330313837  
61373833363830220d0a4163636570742d52616e6765733a2062797465730d0a436f6e74656e742d4c656e6774683a203331310d0a566  
172793a204163636570742d456e636f64696e670d0a436f6e74656e742d547970653a20746578742f68746d6c0d0a0d0a3c21646f63747  
970652068746d6c3e0a0a3c68746d6c206c616e673d22656e223e0a3c686561643e0a20203c6d65746120636861727365743d22757466  
2d38223e0a0a20203c7469746c653e56696272616e74436c6f75643c2f7469746c653e0a20203c6d657461206e616d653d226465736372  
697074696f6e2220636f6e74656e743d2256696272616e74436c6f7564223e0a20203c6d657461206e616d653d22617574686f72222063  
6f6e74656e743d22416e6f6e223e0a0a3c2f686561643e0a0a3c626f64793e0a20203c68313e56696272616e74436c6f75643c2f68313e0a  
20203c703e54686973206973207468652066616d6f75732056696272616e74436c6f756420796f7527766520686561726420736f206d7  
563682061626f75742e3c2f703e0a3c2f626f64793e0a3c2f68746d6c3e

##### TCP #####

sport : 80

dport : 21110

seq : 665936838

ack : 44

offset\_reserv\_flags : 20504

window : 64240

chksum : 55203

urgptr : 0

offset : 5

message : HTTP/1.1 200 OK

Date: Thu, 23 Oct 2025 14:53:20 GMT

Server: Apache

Upgrade: h2,h2c

Connection: Upgrade

Last-Modified: Fri, 16 Apr 2021 15:17:30 GMT

ETag: "1b210a5-137-5c0187a783680"

Accept-Ranges: bytes

Content-Length: 311

Vary: Accept-Encoding

Content-Type: text/html

<!doctype html>

```
<html lang="en">
<head>
  <meta charset="utf-8">

  <title>VibrantCloud</title>
  <meta name="description" content="VibrantCloud">
  <meta name="author" content="Anon">

</head>

<body>
  <h1>VibrantCloud</h1>
  <p>This is the famous VibrantCloud you've heard so much about.</p>
</body>
</html>
```

STDOUT:

STDERR: