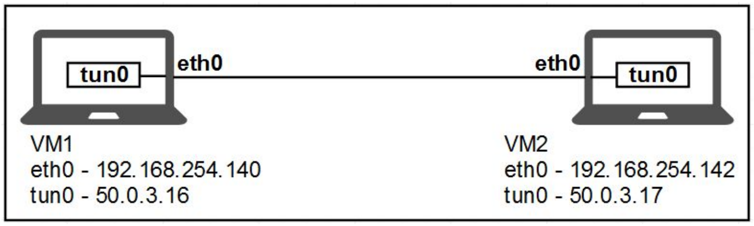
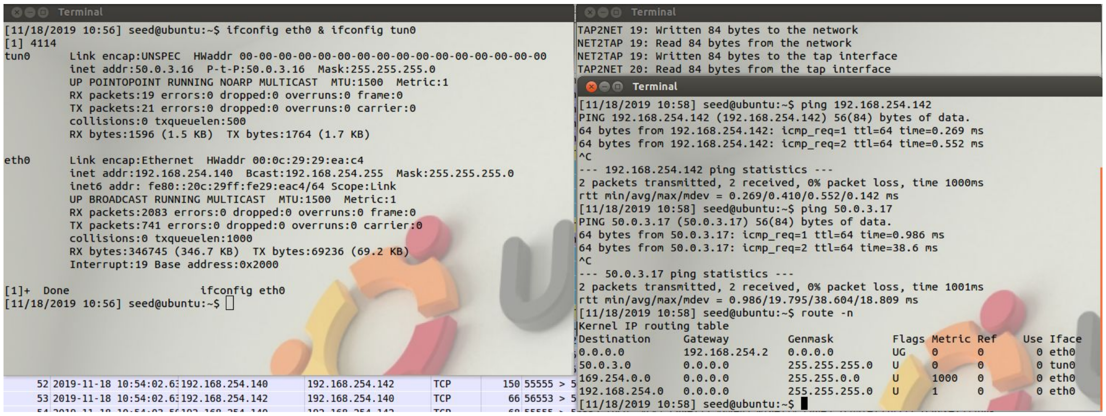
Parag Mhatre
ITIS 6167

1. The network environment contains two machines connected via a network in the 192.168.254.0/24 subnet. The address for the first machine (VM1) is 192.168.254.140 and the second machine (VM2) is 192.168.254.142. We have also established a VPN tunnel between the two machines with the address for tun0 in VM1 as 50.0.3.16 and the address for tun0 in VM2 as 50.0.3.17.



The packets sent from tun0 interface are first encapsulated and sent via the physical interfaces (eth0) to the destination where they are decapsulated and forwarded to their actual destination.

2. The following is a screenshot with ping and route outputs for VM1



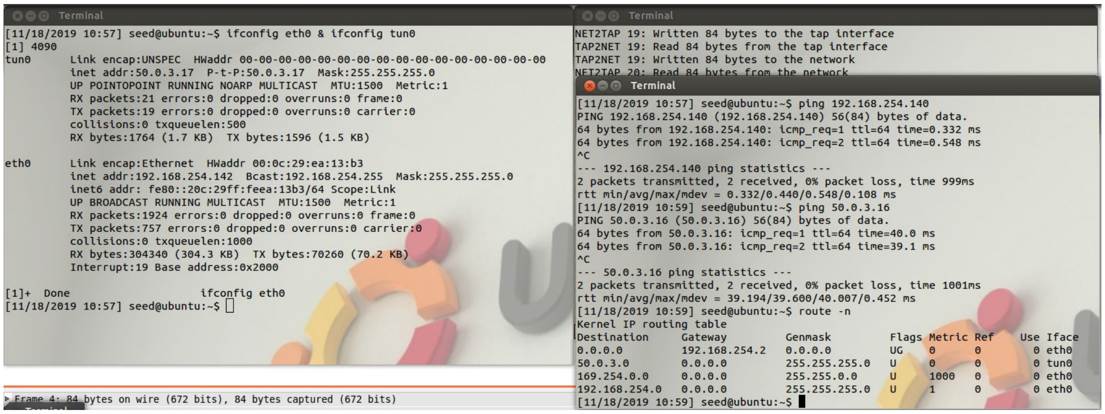
```
[11/18/2019 10:56] seed@ubuntu:~$ ifconfig eth0 & ifconfig tun0
[1] 4114
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:50.0.3.16  P-t-P:50.0.3.16  Mask:255.255.255.0
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:19 errors:0 dropped:0 overruns:0 frame:0
          TX packets:21 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:1596 (1.5 KB)  TX bytes:1764 (1.7 KB)

eth0      Link encap:Ethernet  HWaddr 00:0c:29:29:ea:c4
          inet addr:192.168.254.140  Bcast:192.168.254.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe29:eac4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2083 errors:0 dropped:0 overruns:0 frame:0
          TX packets:741 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:346745 (346.7 KB)  TX bytes:69236 (69.2 KB)
          Interrupt:19 Base address:0x2000

[1]+  Done                    ifconfig eth0
[11/18/2019 10:56] seed@ubuntu:~$ 
```

```
   52 2019-11-18 10:54:02.6 192.168.254.140   192.168.254.142   TCP    150 55555 > 5
   53 2019-11-18 10:54:02.6 192.168.254.142   192.168.254.140   TCP     66 56553 > 5
```

```
TAP2NET 19: Written 84 bytes to the network
NET2TAP 19: Read 84 bytes from the network
NET2TAP 19: Written 84 bytes to the tap interface
TAP2NET 20: Read 84 bytes from the tap interface
```

```
[11/18/2019 10:58] seed@ubuntu:~$ ping 192.168.254.142
PING 192.168.254.142 (192.168.254.142) 56(84) bytes of data.
64 bytes from 192.168.254.142: icmp_req=1 ttl=64 time=0.269 ms
64 bytes from 192.168.254.142: icmp_req=2 ttl=64 time=0.552 ms
^C
--- 192.168.254.142 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.269/0.410/0.552/0.142 ms
[11/18/2019 10:58] seed@ubuntu:~$ ping 50.0.3.17
PING 50.0.3.17 (50.0.3.17) 56(84) bytes of data.
64 bytes from 50.0.3.17: icmp_req=1 ttl=64 time=0.986 ms
64 bytes from 50.0.3.17: icmp_req=2 ttl=64 time=38.6 ms
^C
--- 50.0.3.17 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.986/19.795/38.604/18.809 ms
[11/18/2019 10:58] seed@ubuntu:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.254.2   0.0.0.0         UG    0      0        0 eth0
50.0.3.0        0.0.0.0         255.255.255.0   U     0      0        0 tun0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 eth0
192.168.254.0   0.0.0.0         255.255.255.0   U     1      0        0 eth0
[11/18/2019 10:58] seed@ubuntu:~$ 
```

The following is a screenshot with ping and route outputs for VM2



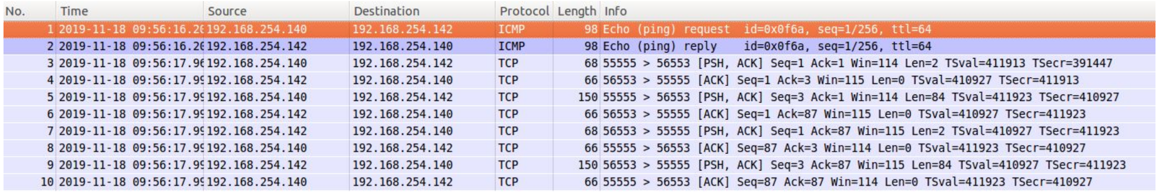
```
[11/18/2019 10:57] seed@ubuntu:~$ ifconfig eth0 & ifconfig tun0
[1] 4090
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:50.0.3.17  P-t-P:50.0.3.17  Mask:255.255.255.0
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:21 errors:0 dropped:0 overruns:0 frame:0
          TX packets:19 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:1764 (1.7 KB)  TX bytes:1596 (1.5 KB)

eth0      Link encap:Ethernet  HWaddr 00:0c:29:ea:13:b3
          inet addr:192.168.254.142  Bcast:192.168.254.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feea:13b3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1924 errors:0 dropped:0 overruns:0 frame:0
          TX packets:757 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:304340 (304.3 KB)  TX bytes:70260 (70.2 KB)
          Interrupt:19 Base address:0x2000

[1]+  Done                    ifconfig eth0
[11/18/2019 10:57] seed@ubuntu:~$ 
```

```
▸ Frame 4: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
```

```
NET2TAP 19: Written 84 bytes to the tap interface
TAP2NET 19: Read 84 bytes from the tap interface
TAP2NET 19: Written 84 bytes to the network
NET2TAP 20: Read 84 bytes from the network
```

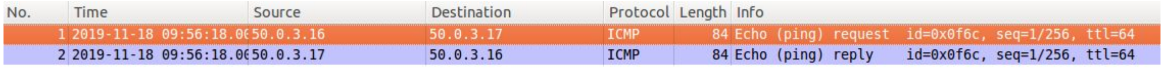
```
[11/18/2019 10:57] seed@ubuntu:~$ ping 192.168.254.140
PING 192.168.254.140 (192.168.254.140) 56(84) bytes of data.
64 bytes from 192.168.254.140: icmp_req=1 ttl=64 time=0.332 ms
64 bytes from 192.168.254.140: icmp_req=2 ttl=64 time=0.548 ms
^C
--- 192.168.254.140 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.332/0.440/0.548/0.108 ms
[11/18/2019 10:59] seed@ubuntu:~$ ping 50.0.3.16
PING 50.0.3.16 (50.0.3.16) 56(84) bytes of data.
64 bytes from 50.0.3.16: icmp_req=1 ttl=64 time=40.0 ms
64 bytes from 50.0.3.16: icmp_req=2 ttl=64 time=39.1 ms
^C
--- 50.0.3.16 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 39.194/39.600/40.007/0.452 ms
[11/18/2019 10:59] seed@ubuntu:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.254.2   0.0.0.0         UG    0      0        0 eth0
50.0.3.0        0.0.0.0         255.255.255.0   U     0      0        0 tun0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 eth0
192.168.254.0   0.0.0.0         255.255.255.0   U     1      0        0 eth0
[11/18/2019 10:59] seed@ubuntu:~$ 
```

3. Screenshot from Wireshark capture on eth0 interface



No.	Time	Source	Destination	Protocol	Length	Info
1	2019-11-18 09:56:16.2	192.168.254.140	192.168.254.142	ICMP	98	Echo (ping) request id=0x0f6a, seq=1/256, ttl=64
2	2019-11-18 09:56:16.2	192.168.254.142	192.168.254.140	ICMP	98	Echo (ping) reply id=0x0f6a, seq=1/256, ttl=64
3	2019-11-18 09:56:17.9	192.168.254.140	192.168.254.142	TCP	68	55555 > 56553 [PSH, ACK] Seq=1 Ack=1 Win=114 Len=2 TSval=411913 TSecr=391447
4	2019-11-18 09:56:17.9	192.168.254.142	192.168.254.140	TCP	66	56553 > 55555 [ACK] Seq=1 Ack=3 Win=115 Len=0 TSval=410927 TSecr=411913
5	2019-11-18 09:56:17.9	192.168.254.140	192.168.254.142	TCP	150	55555 > 56553 [PSH, ACK] Seq=3 Ack=1 Win=114 Len=84 TSval=411923 TSecr=410927
6	2019-11-18 09:56:17.9	192.168.254.142	192.168.254.140	TCP	66	56553 > 55555 [ACK] Seq=1 Ack=87 Win=115 Len=0 TSval=410927 TSecr=411923
7	2019-11-18 09:56:17.9	192.168.254.142	192.168.254.140	TCP	68	56553 > 55555 [PSH, ACK] Seq=1 Ack=87 Win=115 Len=2 TSval=410927 TSecr=411923
8	2019-11-18 09:56:17.9	192.168.254.140	192.168.254.142	TCP	66	55555 > 56553 [ACK] Seq=87 Ack=3 Win=114 Len=0 TSval=411923 TSecr=410927
9	2019-11-18 09:56:17.9	192.168.254.142	192.168.254.140	TCP	150	56553 > 55555 [PSH, ACK] Seq=3 Ack=87 Win=115 Len=84 TSval=410927 TSecr=411923
10	2019-11-18 09:56:17.9	192.168.254.140	192.168.254.142	TCP	66	55555 > 56553 [ACK] Seq=87 Ack=87 Win=114 Len=0 TSval=411923 TSecr=410927

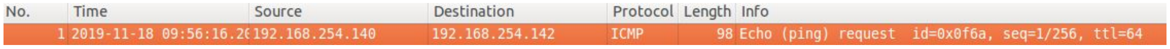
Screenshot from Wireshark capture on tun0 interface with the same traffic



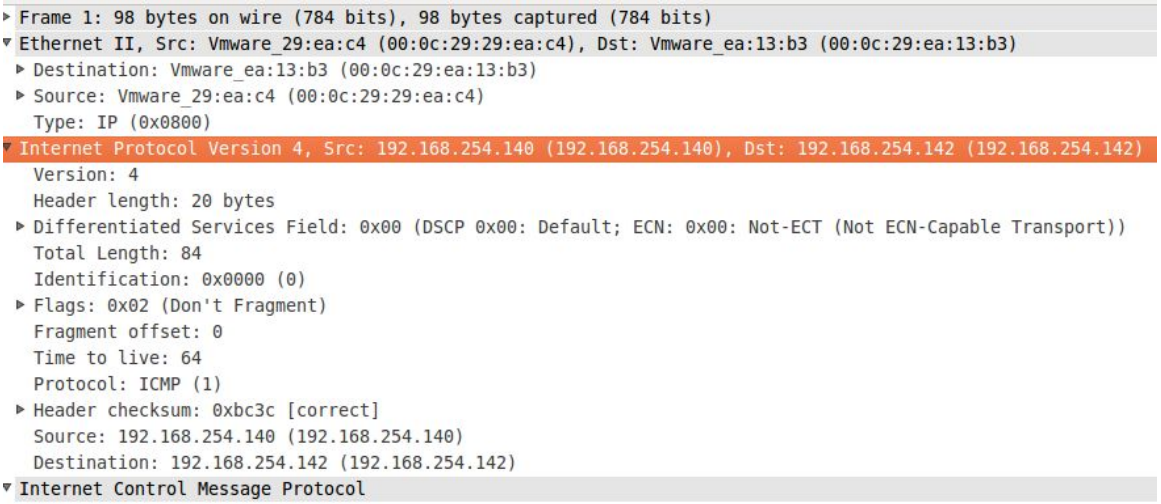
No.	Time	Source	Destination	Protocol	Length	Info
1	2019-11-18 09:56:18.0	50.0.3.16	50.0.3.17	ICMP	84	Echo (ping) request id=0x0f6c, seq=1/256, ttl=64
2	2019-11-18 09:56:18.0	50.0.3.17	50.0.3.16	ICMP	84	Echo (ping) reply id=0x0f6c, seq=1/256, ttl=64

4. A VPN (Virtual Private Network) uses tunneling to hide an IP packet into another IP packet. This is done using Encapsulation. Encapsulation can be described as wrapping of IP packet data into another IP packet such as all the contents of the original IP packet go into the data section of the new IP packet.

   Firstly, when we try to ping from VM1 to VM2 to the eth0 IP of VM2 (Ping from 192.168.254.140 to 192.168.254.142), the packets are sent in their original form and there is no part played by the VPN or VPN tunnel as shown in the screenshots below.



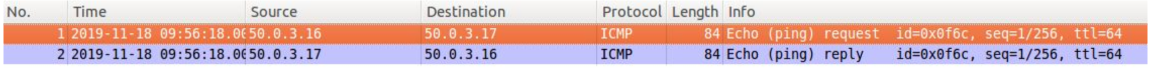
No.	Time	Source	Destination	Protocol	Length	Info
1	2019-11-18 09:56:16.2	192.168.254.140	192.168.254.142	ICMP	98	Echo (ping) request id=0x0f6a, seq=1/256, ttl=64



```
▸ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
▾ Ethernet II, Src: Vmware_29:ea:c4 (00:0c:29:29:ea:c4), Dst: Vmware_ea:13:b3 (00:0c:29:ea:13:b3)
  ▸ Destination: Vmware_ea:13:b3 (00:0c:29:ea:13:b3)
  ▸ Source: Vmware_29:ea:c4 (00:0c:29:29:ea:c4)
    Type: IP (0x0800)
▾ Internet Protocol Version 4, Src: 192.168.254.140 (192.168.254.140), Dst: 192.168.254.142 (192.168.254.142)
    Version: 4
    Header length: 20 bytes
  ▸ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 84
    Identification: 0x0000 (0)
  ▸ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
  ▸ Header checksum: 0xbc3c [correct]
    Source: 192.168.254.140 (192.168.254.140)
    Destination: 192.168.254.142 (192.168.254.142)
▾ Internet Control Message Protocol
```

   The above is also true if we try to ping from VM2 to VM1 to the eth0 IP.
   If we try to capture the data from the tun0 interface, we cannot see any traffic for the above communication and hence it can be confirmed again that no part is played by that interface.

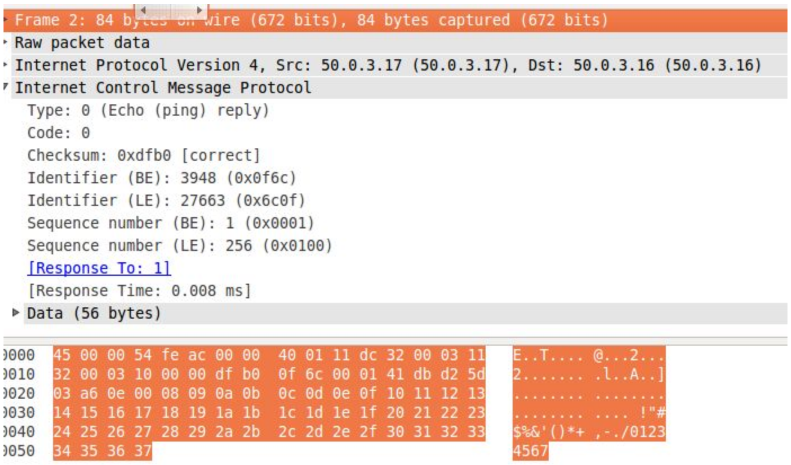
Secondly, when we try to ping from VM1 to VM2 on the tun0 interface, we can see the packets with their actual IPs (IPs of tun0 interface) if we are capturing data on the tun0 interface as shown in the below screenshot.



No.	Time	Source	Destination	Protocol	Length	Info
1	2019-11-18 09:56:18.0(	50.0.3.16	50.0.3.17	ICMP	84	Echo (ping) request id=0x0f6c, seq=1/256, ttl=64
2	2019-11-18 09:56:18.0(	50.0.3.17	50.0.3.16	ICMP	84	Echo (ping) reply id=0x0f6c, seq=1/256, ttl=64

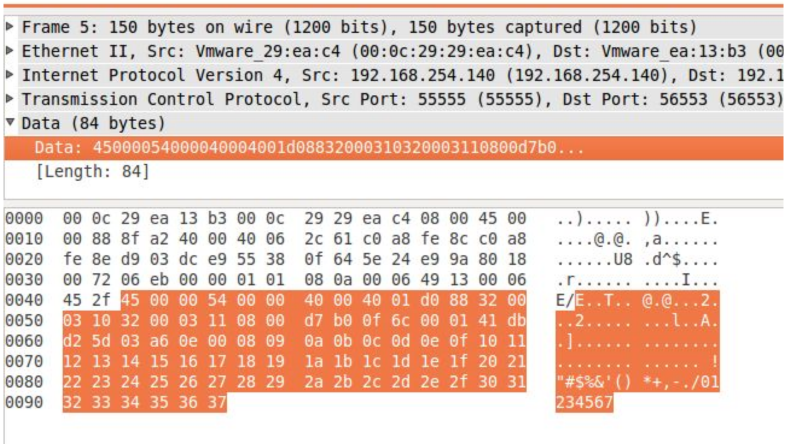
If we capture data for the same communication from the eth0 interface, we cannot see the actual IPs of the tun0 interface in the captured data. But we can see TCP communication instead of the ICMP communication that we expect to see. The source and destination IPs for this communication are the IPs of the eth0 interface. On closer inspection we can see that the ICMP packets from the tun0 interface are encapsulated inside TCP packets from eth0 interface and sent to the other node where they must be decapsulated and forwarded to the relevant destination. The screenshots showing this are shown below.

The ICMP frame as captured from tun0 interface



```
▸ Frame 2: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
▸ Raw packet data
▸ Internet Protocol Version 4, Src: 50.0.3.17 (50.0.3.17), Dst: 50.0.3.16 (50.0.3.16)
▾ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xdfb0 [correct]
    Identifier (BE): 3948 (0x0f6c)
    Identifier (LE): 27663 (0x6c0f)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Response To: 1]
    [Response Time: 0.008 ms]
  ▶ Data (56 bytes)

0000  45 00 00 54 fe ac 00 00  40 01 11 dc 32 00 03 11   E..T.... @...2...
0010  32 00 03 10 00 00 df b0  0f 6c 00 01 41 db d2 5d   2....... .l..A..]
0020  03 a6 0e 00 08 09 0a 0b  0c 0d 0e 0f 10 11 12 13   ........ ........
0030  14 15 16 17 18 19 1a 1b  1c 1d 1e 1f 20 21 22 23   ........ .... !"#
0040  24 25 26 27 28 29 2a 2b  2c 2d 2e 2f 30 31 32 33   $%&'()*+ ,-./0123
0050  34 35 36 37                                        4567
```

The TCP frame from eth0 interface. (Notice the highlighted parts are the same)



```
▶ Frame 5: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits)
▶ Ethernet II, Src: Vmware_29:ea:c4 (00:0c:29:29:ea:c4), Dst: Vmware_ea:13:b3 (00
▶ Internet Protocol Version 4, Src: 192.168.254.140 (192.168.254.140), Dst: 192.1
▶ Transmission Control Protocol, Src Port: 55555 (55555), Dst Port: 56553 (56553)
▼ Data (84 bytes)
    Data: 450000540000400040001d08832000310320003110800d7b0...
    [Length: 84]

0000  00 0c 29 ea 13 b3 00 0c  29 29 ea c4 08 00 45 00   ..)..... ))....E.
0010  00 88 8f a2 40 00 40 06  2c 61 c0 a8 fe 8c c0 a8   ....@.@. ,a......
0020  fe 8e d9 03 dc e9 55 38  0f 64 5e 24 e9 9a 80 18   ......U8 .d^$....
0030  00 72 06 eb 00 00 01 01  08 0a 00 06 49 13 00 06   .r...... ....I...
0040  45 2f 45 00 00 54 00 00  40 00 40 01 d0 88 32 00   E/E..T.. @.@...2.
0050  03 10 32 00 03 11 08 00  d7 b0 0f 6c 00 01 41 db   ..2..... ...l..A.
0060  d2 5d 03 a6 0e 00 08 09  0a 0b 0c 0d 0e 0f 10 11   .]...... ........
0070  12 13 14 15 16 17 18 19  1a 1b 1c 1d 1e 1f 20 21   ........ ...... !
0080  22 23 24 25 26 27 28 29  2a 2b 2c 2d 2e 2f 30 31   "#$%&'() *+,-./01
0090  32 33 34 35 36 37                                  234567
```

Thus, we can conclude from the above that VPN wraps the actual packets inside TCP packets which are sent to tunnel endpoint and then decapsulated and the actual packet is recovered from that.

Thus we can also say that the addresses 50.0.0.16 or 17 are hidden from the outside network and the outside network can never see these addresses. An additional layer of protection can be added if the VPN does encryption along with encapsulation.

You can also see that the total size of ICMP packet from tun0 interface is 84 bytes and the size of data in the TCP packet from eth0 interface is 84 bytes. The total size of the eth packet containing this ICMP packet data is 150 bytes.