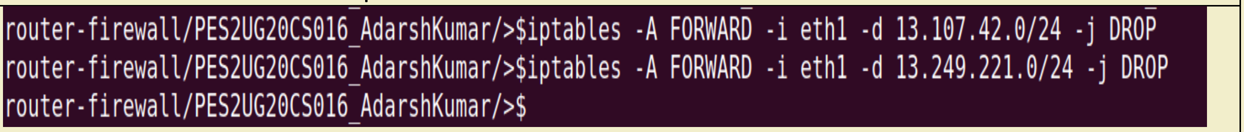
LAB: 08 Firewall Evasion Lab 2022

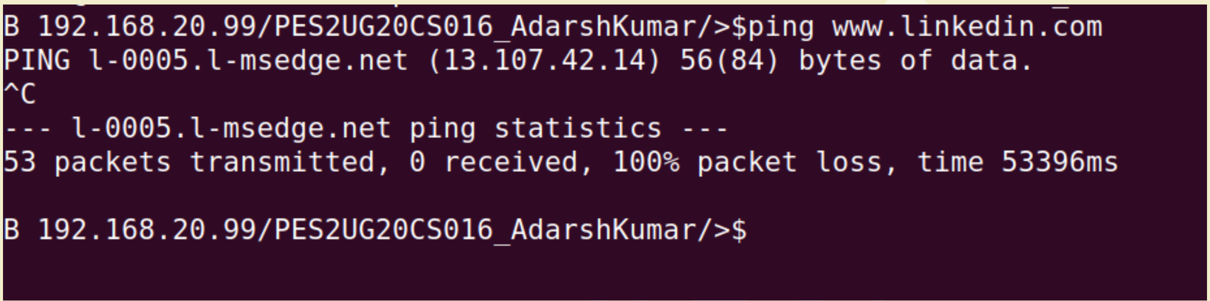
Name: Adarsh Kumar	SRN No: PES2UG20CS016	Assignment No: 08
	Section: B	Date: 5/11/2022

Task 0: Get Familiar with the Lab Setup

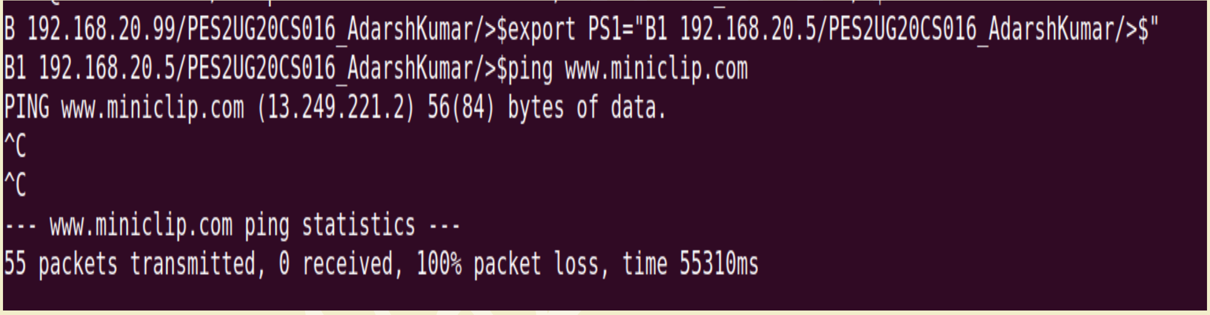


```
router-firewall/PES2UG20CS016_AdarshKumar/>$iptables -A FORWARD -i eth1 -d 13.107.42.0/24 -j DROP
router-firewall/PES2UG20CS016_AdarshKumar/>$iptables -A FORWARD -i eth1 -d 13.249.221.0/24 -j DROP
router-firewall/PES2UG20CS016_AdarshKumar/>$
```

Setting up the rule in Iptables for restricting 2 IP address. Eg: linkedin.com and miniclip.com



```
B 192.168.20.99/PES2UG20CS016_AdarshKumar/>$ping www.linkedin.com
PING l-0005.l-msedge.net (13.107.42.14) 56(84) bytes of data.
^C
--- l-0005.l-msedge.net ping statistics ---
53 packets transmitted, 0 received, 100% packet loss, time 53396ms

B 192.168.20.99/PES2UG20CS016_AdarshKumar/>$
```

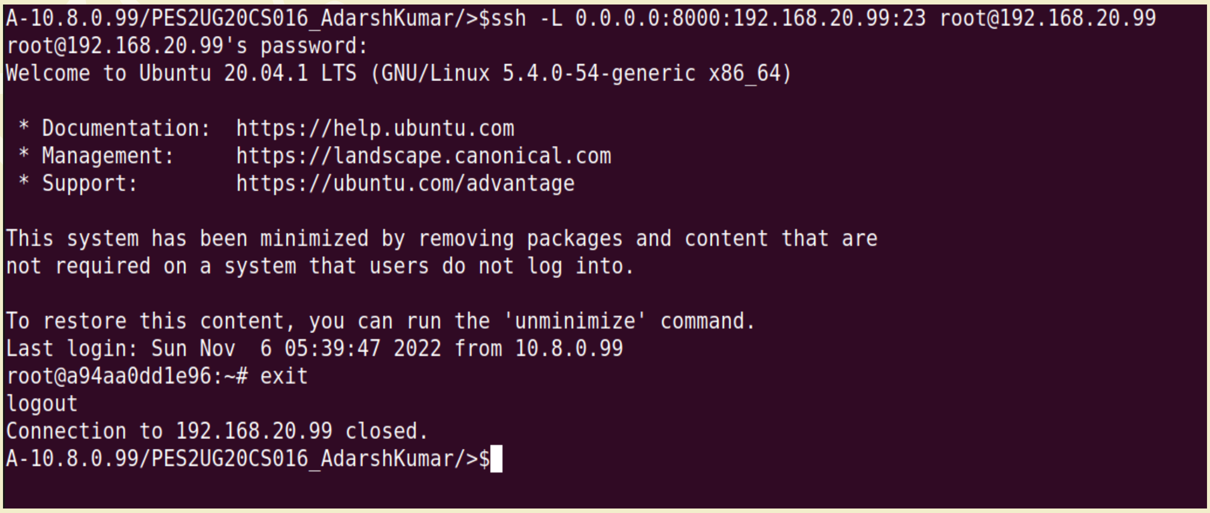


```
B 192.168.20.99/PES2UG20CS016_AdarshKumar/>$export PS1="B1 192.168.20.5/PES2UG20CS016_AdarshKumar/>$"
B1 192.168.20.5/PES2UG20CS016_AdarshKumar/>$ping www.miniclip.com
PING www.miniclip.com (13.249.221.2) 56(84) bytes of data.
^C
^C
--- www.miniclip.com ping statistics ---
55 packets transmitted, 0 received, 100% packet loss, time 55310ms
```

Observation: As we can see that now when we are trying to ping nothing appears on the terminal because they are blocked by the default firewall.

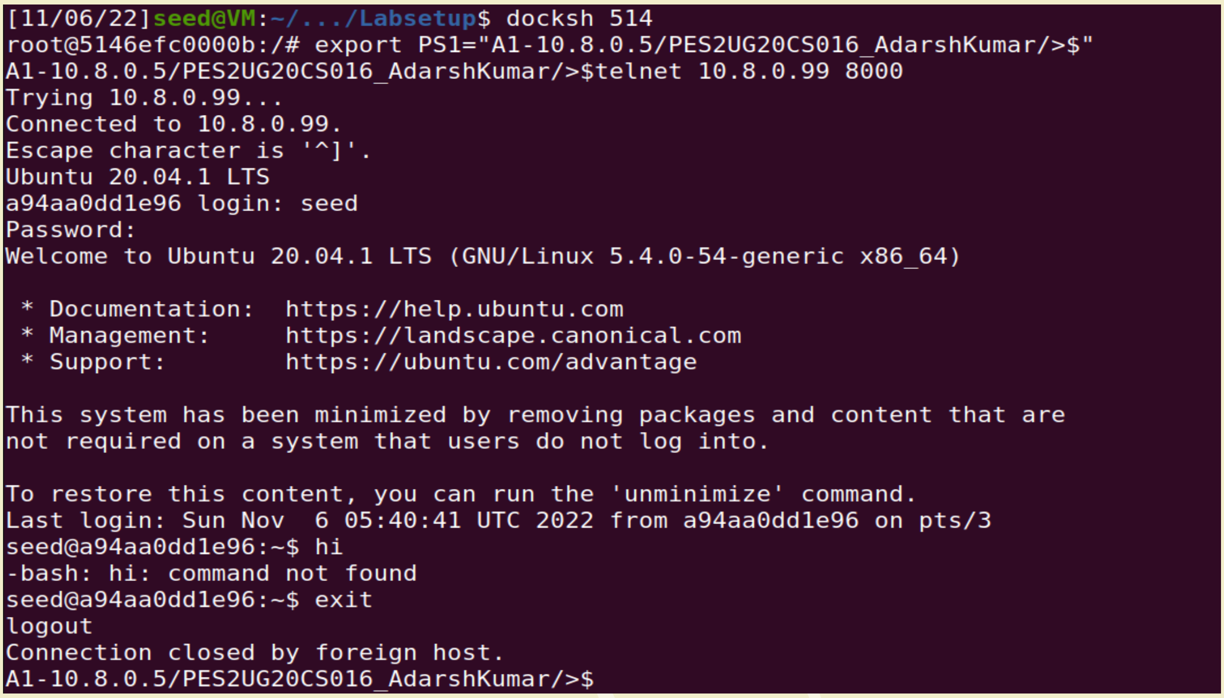
Task 1: Static Port Forwarding

On docker container A-10.8.0.99



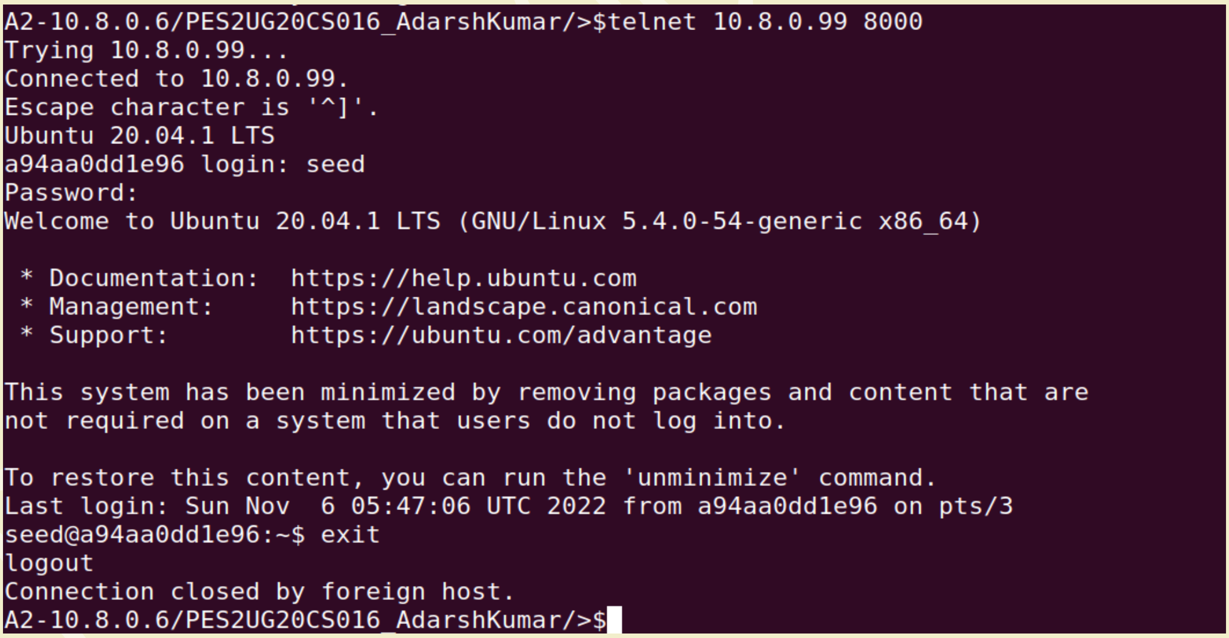
```
A-10.8.0.99/PES2UG20CS016_AdarshKumar/>$ssh -L 0.0.0.0:8000:192.168.20.99:23 root@192.168.20.99
root@192.168.20.99's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sun Nov  6 05:39:47 2022 from 10.8.0.99
root@a94aa0dd1e96:~# exit
logout
Connection to 192.168.20.99 closed.
A-10.8.0.99/PES2UG20CS016_AdarshKumar/>$
```

On docker container A1



```
[11/06/22]seed@VM:~/.../Labsetup$ docksh 514
root@5146efc0000b:/# export PS1="A1-10.8.0.5/PES2UG20CS016_AdarshKumar/>$"
A1-10.8.0.5/PES2UG20CS016_AdarshKumar/>$telnet 10.8.0.99 8000
Trying 10.8.0.99...
Connected to 10.8.0.99.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
a94aa0dd1e96 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sun Nov  6 05:40:41 UTC 2022 from a94aa0dd1e96 on pts/3
seed@a94aa0dd1e96:~$ hi
-bash: hi: command not found
seed@a94aa0dd1e96:~$ exit
logout
Connection closed by foreign host.
A1-10.8.0.5/PES2UG20CS016_AdarshKumar/>$
```

On docker container A2



```
A2-10.8.0.6/PES2UG20CS016_AdarshKumar/>$telnet 10.8.0.99 8000
Trying 10.8.0.99...
Connected to 10.8.0.99.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
a94aa0dd1e96 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sun Nov  6 05:47:06 UTC 2022 from a94aa0dd1e96 on pts/3
seed@a94aa0dd1e96:~$ exit
logout
Connection closed by foreign host.
A2-10.8.0.6/PES2UG20CS016_AdarshKumar/>$
```

We are trying to established a docker telnet connection form docker container A1 & A2

Question

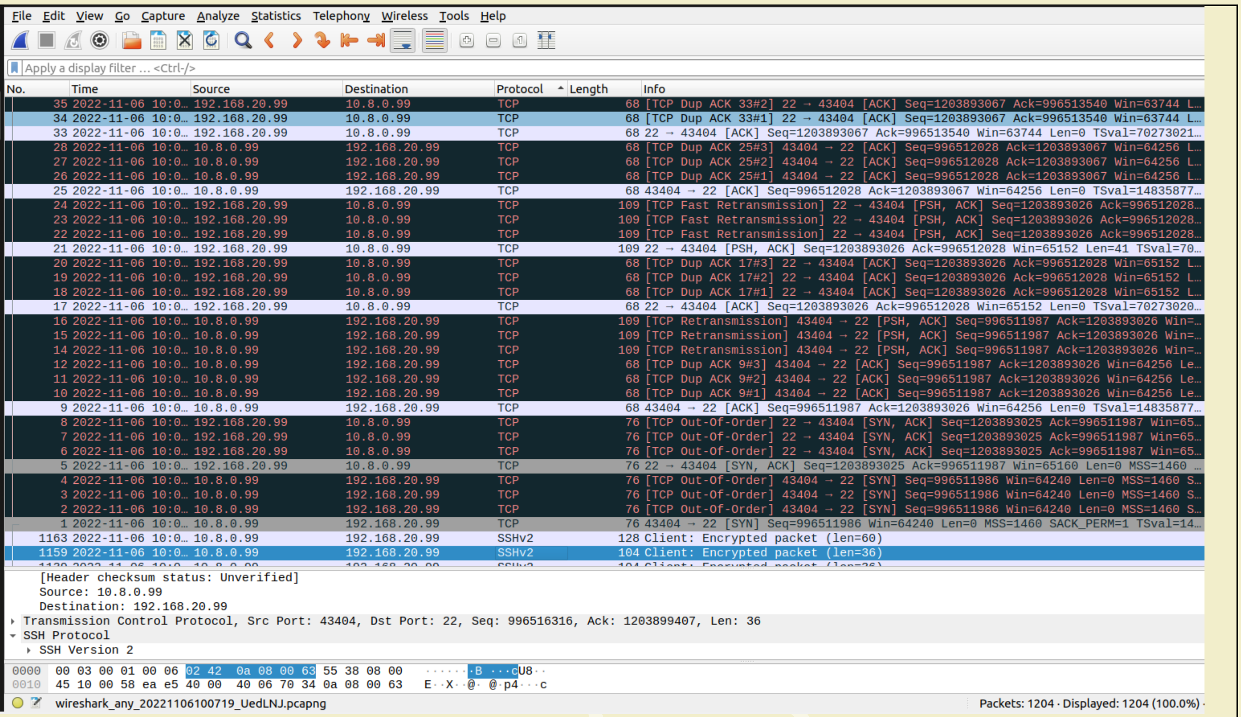
(1) How many TCP connections are involved in this entire process. You should run Wireshark or tcpdump to capture the network traffic, and then point out all the involved TCP connections from the captured traffic.

Ans: 3 TCP connection are involved in this process.

(2) Why can this tunnel successfully help users evade the firewall rule specified in the lab setup?

Ans: Yes, we can use this tunnel to evade the firewall rule. As port 23 is blocked but we can see that port no. 22 is still open, from that port we can establish a SSH connection which act as a tunnel between internal host and internal machine.

Wireshark


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

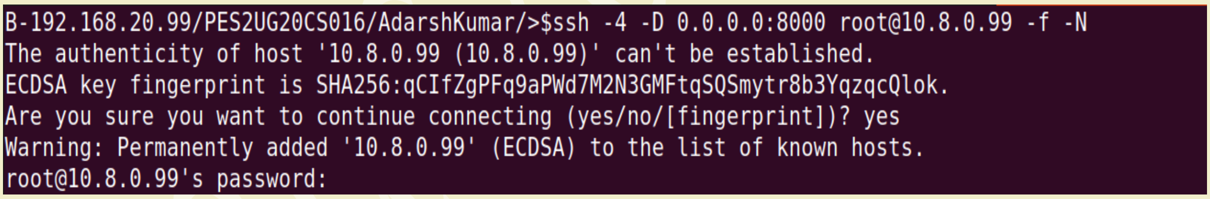
```
No.   Time               Source          Destination     Protocol  Length  Info
  35 2022-11-06 10:0… 192.168.20.99   10.8.0.99       TCP        68 [TCP Dup ACK 33#2] 22 → 43404 [ACK] Seq=1203893067 Ack=996513540 Win=63744 L…
  34 2022-11-06 10:0… 192.168.20.99   10.8.0.99       TCP        68 [TCP Dup ACK 33#1] 22 → 43404 [ACK] Seq=1203893067 Ack=996513540 Win=63744 L…
  33 2022-11-06 10:0… 192.168.20.99   10.8.0.99       TCP        68 22 → 43404 [ACK] Seq=1203893067 Ack=996513540 Win=63744 Len=0 TSval=70273021…
  28 2022-11-06 10:0… 10.8.0.99       192.168.20.99   TCP        68 [TCP Dup ACK 25#3] 43404 → 22 [ACK] Seq=996512028 Ack=1203893067 Win=64256 L…
  27 2022-11-06 10:0… 10.8.0.99       192.168.20.99   TCP        68 [TCP Dup ACK 25#2] 43404 → 22 [ACK] Seq=996512028 Ack=1203893067 Win=64256 L…
  26 2022-11-06 10:0… 10.8.0.99       192.168.20.99   TCP        68 [TCP Dup ACK 25#1] 43404 → 22 [ACK] Seq=996512028 Ack=1203893067 Win=64256 L…
  25 2022-11-06 10:0… 10.8.0.99       192.168.20.99   TCP        68 43404 → 22 [ACK] Seq=996512028 Ack=1203893067 Win=64256 Len=0 TSval=14835877…
  24 2022-11-06 10:0… 192.168.20.99   10.8.0.99       TCP       109 [TCP Fast Retransmission] 22 → 43404 [PSH, ACK] Seq=1203893026 Ack=996512028…
  23 2022-11-06 10:0… 192.168.20.99   10.8.0.99       TCP       109 [TCP Fast Retransmission] 22 → 43404 [PSH, ACK] Seq=1203893026 Ack=996512028…
  22 2022-11-06 10:0… 192.168.20.99   10.8.0.99       TCP       109 [TCP Fast Retransmission] 22 → 43404 [PSH, ACK] Seq=1203893026 Ack=996512028…
  21 2022-11-06 10:0… 192.168.20.99   10.8.0.99       TCP       109 22 → 43404 [PSH, ACK] Seq=1203893026 Ack=996512028 Win=65152 Len=41 TSval=70…
  20 2022-11-06 10:0… 192.168.20.99   10.8.0.99       TCP        68 [TCP Dup ACK 17#3] 22 → 43404 [ACK] Seq=1203893026 Ack=996512028 Win=65152 L…
  19 2022-11-06 10:0… 192.168.20.99   10.8.0.99       TCP        68 [TCP Dup ACK 17#2] 22 → 43404 [ACK] Seq=1203893026 Ack=996512028 Win=65152 L…
  18 2022-11-06 10:0… 192.168.20.99   10.8.0.99       TCP        68 [TCP Dup ACK 17#1] 22 → 43404 [ACK] Seq=1203893026 Ack=996512028 Win=65152 L…
  17 2022-11-06 10:0… 192.168.20.99   10.8.0.99       TCP        68 22 → 43404 [ACK] Seq=1203893026 Ack=996512028 Win=65152 Len=0 TSval=70273020…
  16 2022-11-06 10:0… 10.8.0.99       192.168.20.99   TCP       109 [TCP Retransmission] 43404 → 22 [PSH, ACK] Seq=996511987 Ack=1203893026 Win=…
  15 2022-11-06 10:0… 10.8.0.99       192.168.20.99   TCP       109 [TCP Retransmission] 43404 → 22 [PSH, ACK] Seq=996511987 Ack=1203893026 Win=…
  14 2022-11-06 10:0… 10.8.0.99       192.168.20.99   TCP       109 [TCP Retransmission] 43404 → 22 [PSH, ACK] Seq=996511987 Ack=1203893026 Win=…
  12 2022-11-06 10:0… 10.8.0.99       192.168.20.99   TCP        68 [TCP Dup ACK 9#3] 43404 → 22 [ACK] Seq=996511987 Ack=1203893026 Win=64256 Le…
  11 2022-11-06 10:0… 10.8.0.99       192.168.20.99   TCP        68 [TCP Dup ACK 9#2] 43404 → 22 [ACK] Seq=996511987 Ack=1203893026 Win=64256 Le…
  10 2022-11-06 10:0… 10.8.0.99       192.168.20.99   TCP        68 [TCP Dup ACK 9#1] 43404 → 22 [ACK] Seq=996511987 Ack=1203893026 Win=64256 Le…
   9 2022-11-06 10:0… 10.8.0.99       192.168.20.99   TCP        68 43404 → 22 [ACK] Seq=996511987 Ack=1203893026 Win=64256 Len=0 TSval=14835877…
   8 2022-11-06 10:0… 192.168.20.99   10.8.0.99       TCP        76 [TCP Out-Of-Order] 22 → 43404 [SYN, ACK] Seq=1203893025 Ack=996511987 Win=65…
   7 2022-11-06 10:0… 192.168.20.99   10.8.0.99       TCP        76 [TCP Out-Of-Order] 22 → 43404 [SYN, ACK] Seq=1203893025 Ack=996511987 Win=65…
   6 2022-11-06 10:0… 192.168.20.99   10.8.0.99       TCP        76 [TCP Out-Of-Order] 22 → 43404 [SYN, ACK] Seq=1203893025 Ack=996511987 Win=65…
   5 2022-11-06 10:0… 192.168.20.99   10.8.0.99       TCP        76 22 → 43404 [SYN, ACK] Seq=1203893025 Ack=996511987 Win=65160 Len=0 MSS=1460 …
   4 2022-11-06 10:0… 10.8.0.99       192.168.20.99   TCP        76 [TCP Out-Of-Order] 43404 → 22 [SYN] Seq=996511986 Win=64240 Len=0 MSS=1460 S…
   3 2022-11-06 10:0… 10.8.0.99       192.168.20.99   TCP        76 [TCP Out-Of-Order] 43404 → 22 [SYN] Seq=996511986 Win=64240 Len=0 MSS=1460 S…
   2 2022-11-06 10:0… 10.8.0.99       192.168.20.99   TCP        76 [TCP Out-Of-Order] 43404 → 22 [SYN] Seq=996511986 Win=64240 Len=0 MSS=1460 S…
   1 2022-11-06 10:0… 10.8.0.99       192.168.20.99   TCP        76 43404 → 22 [SYN] Seq=996511986 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=14…
1163 2022-11-06 10:0… 10.8.0.99       192.168.20.99   SSHv2     128 Client: Encrypted packet (len=60)
1159 2022-11-06 10:0… 10.8.0.99       192.168.20.99   SSHv2     104 Client: Encrypted packet (len=36)

    [Header checksum status: Unverified]
    Source: 10.8.0.99
    Destination: 192.168.20.99
▸ Transmission Control Protocol, Src Port: 43404, Dst Port: 22, Seq: 996516316, Ack: 1203899407, Len: 36
▾ SSH Protocol
  ▸ SSH Version 2

0000  00 03 00 01 00 06 02 42  0a 08 00 63 55 38 08 00   ······B ···cU8··
0010  45 10 00 58 ea e5 40 00  40 06 70 34 0a 08 00 63   E··X··@· @·p4···c

wireshark_any_20221106100719_UedLNJ.pcapng                                Packets: 1204 · Displayed: 1204 (100.0%)
```

Here we can see that that telnet connection is successfully established between internal host and external host via SSH tunnelling mechanism.

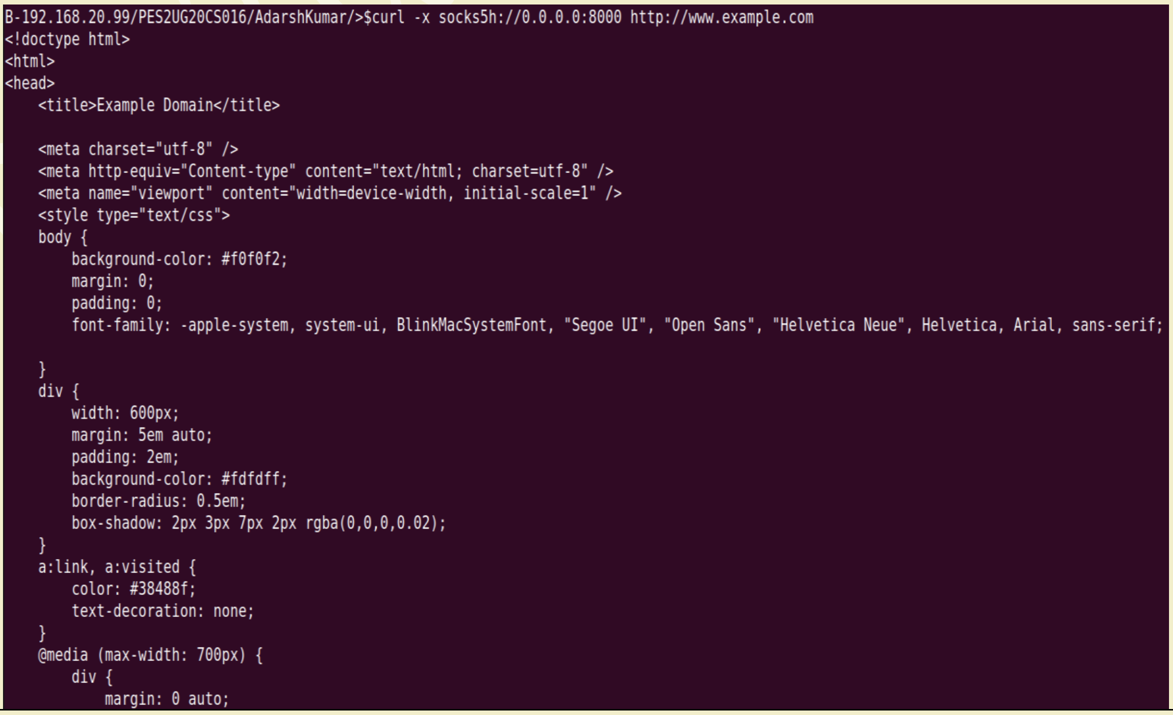
Task 2: **Dynamic Port Forwarding**

Task 2.1: Setting Up Dynamic Port Forwarding

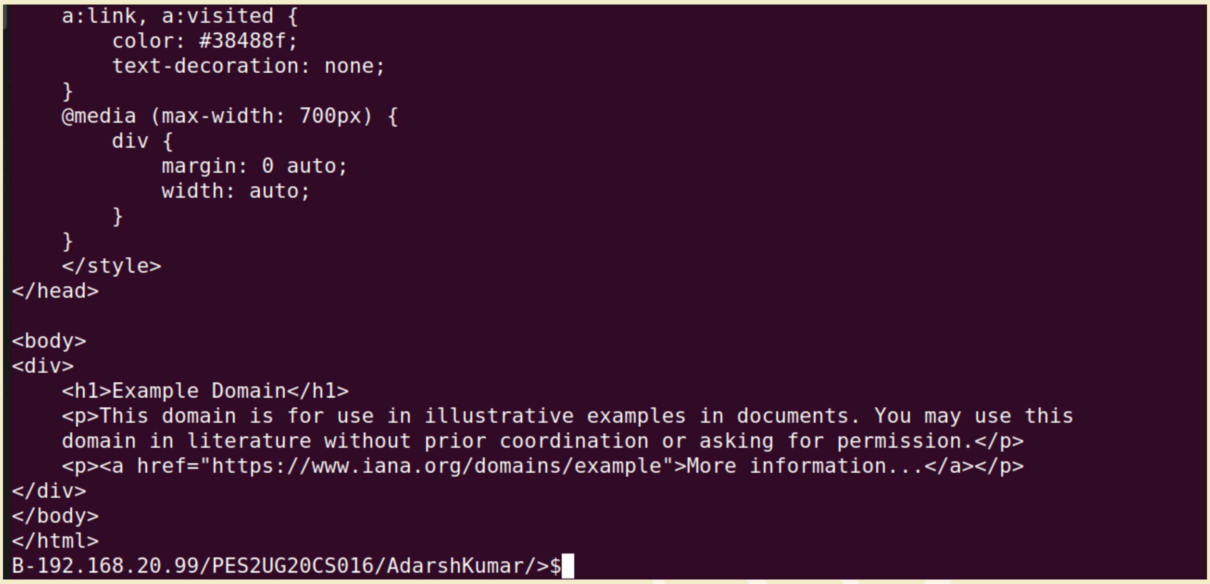
On container B



```
B-192.168.20.99/PES2UG20CS016/AdarshKumar/>$ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N
The authenticity of host '10.8.0.99 (10.8.0.99)' can't be established.
ECDSA key fingerprint is SHA256:qCIfZgPFq9aPWd7M2N3GMFtqSQSmytr8b3YqzqcQlok.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.8.0.99' (ECDSA) to the list of known hosts.
root@10.8.0.99's password:
```

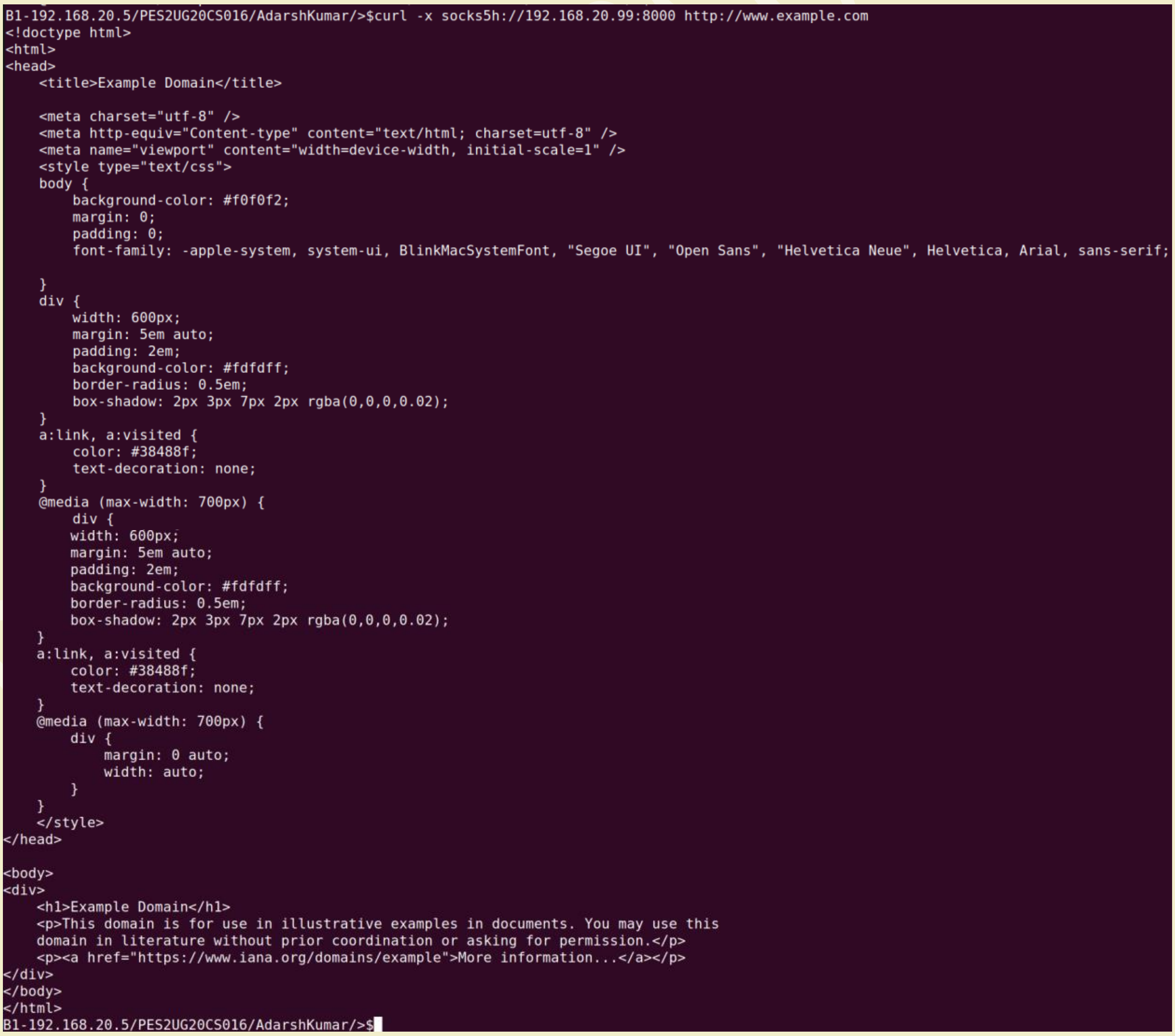


```
B-192.168.20.99/PES2UG20CS016/AdarshKumar/>$curl -x socks5h://0.0.0.0:8000 http://www.example.com
<!doctype html>
<html>
<head>
    <title>Example Domain</title>

    <meta charset="utf-8" />
    <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <style type="text/css">
    body {
        background-color: #f0f0f2;
        margin: 0;
        padding: 0;
        font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", "Helvetica Neue", Helvetica, Arial, sans-serif;

    }
    div {
        width: 600px;
        margin: 5em auto;
        padding: 2em;
        background-color: #fdfdff;
        border-radius: 0.5em;
        box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02);
    }
    a:link, a:visited {
        color: #38488f;
        text-decoration: none;
    }
    @media (max-width: 700px) {
        div {
            margin: 0 auto;
```



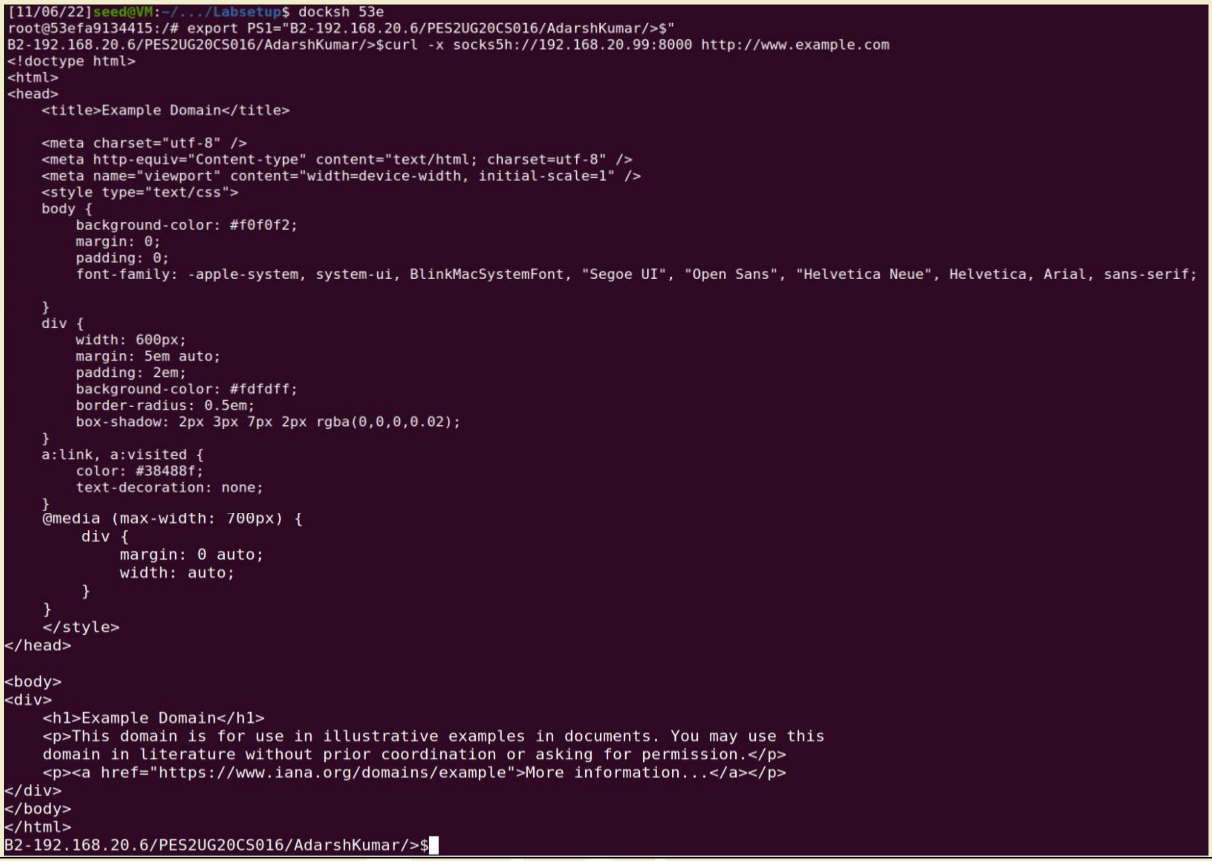
```
    a:link, a:visited {
        color: #38488f;
        text-decoration: none;
    }
    @media (max-width: 700px) {
        div {
            margin: 0 auto;
            width: auto;
        }
    }
    </style>
</head>

<body>
<div>
    <h1>Example Domain</h1>
    <p>This domain is for use in illustrative examples in documents. You may use this
    domain in literature without prior coordination or asking for permission.</p>
    <p><a href="https://www.iana.org/domains/example">More information...</a></p>
</div>
</body>
</html>
B-192.168.20.99/PES2UG20CS016/AdarshKumar/>$
```

On container B1



```
B1-192.168.20.5/PES2UG20CS016/AdarshKumar/>$curl -x socks5h://192.168.20.99:8000 http://www.example.com
<!doctype html>
<html>
<head>
    <title>Example Domain</title>

    <meta charset="utf-8" />
    <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <style type="text/css">
    body {
        background-color: #f0f0f2;
        margin: 0;
        padding: 0;
        font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", "Helvetica Neue", Helvetica, Arial, sans-serif;

    }
    div {
        width: 600px;
        margin: 5em auto;
        padding: 2em;
        background-color: #fdfdff;
        border-radius: 0.5em;
        box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02);
    }
    a:link, a:visited {
        color: #38488f;
        text-decoration: none;
    }
    @media (max-width: 700px) {
        div {
        width: 600px;
        margin: 5em auto;
        padding: 2em;
        background-color: #fdfdff;
        border-radius: 0.5em;
        box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02);
    }
    a:link, a:visited {
        color: #38488f;
        text-decoration: none;
    }
    @media (max-width: 700px) {
        div {
            margin: 0 auto;
            width: auto;
        }
    }
    </style>
</head>

<body>
<div>
    <h1>Example Domain</h1>
    <p>This domain is for use in illustrative examples in documents. You may use this
    domain in literature without prior coordination or asking for permission.</p>
    <p><a href="https://www.iana.org/domains/example">More information...</a></p>
</div>
</body>
</html>
B1-192.168.20.5/PES2UG20CS016/AdarshKumar/>$
```

On container B2



```
[11/06/22]seed@VM:~/.../Labsetup$ docksh 53e
root@53efa9134415:/# export PS1="B2-192.168.20.6/PES2UG20CS016/AdarshKumar/>$"
B2-192.168.20.6/PES2UG20CS016/AdarshKumar/>$curl -x socks5h://192.168.20.99:8000 http://www.example.com
<!doctype html>
<html>
<head>
    <title>Example Domain</title>

    <meta charset="utf-8" />
    <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <style type="text/css">
    body {
        background-color: #f0f0f2;
        margin: 0;
        padding: 0;
        font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", "Helvetica Neue", Helvetica, Arial, sans-serif;

    }
    div {
        width: 600px;
        margin: 5em auto;
        padding: 2em;
        background-color: #fdfdff;
        border-radius: 0.5em;
        box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02);
    }
    a:link, a:visited {
        color: #38488f;
        text-decoration: none;
    }
    @media (max-width: 700px) {
        div {
            margin: 0 auto;
            width: auto;
        }
    }
    </style>
</head>

<body>
<div>
    <h1>Example Domain</h1>
    <p>This domain is for use in illustrative examples in documents. You may use this
    domain in literature without prior coordination or asking for permission.</p>
    <p><a href="https://www.iana.org/domains/example">More information...</a></p>
</div>
</body>
</html>
B2-192.168.20.6/PES2UG20CS016/AdarshKumar/>$
```

Question

(1) How many TCP connections are involved in this entire process. You should run Wireshark or tcpdump to capture the network traffic, and then point out all the involved TCP connections from the captured traffic.

Ans: Here the actual connection is established by the external machine A. the internal host indirectly establish connection via SSH tunnelling.

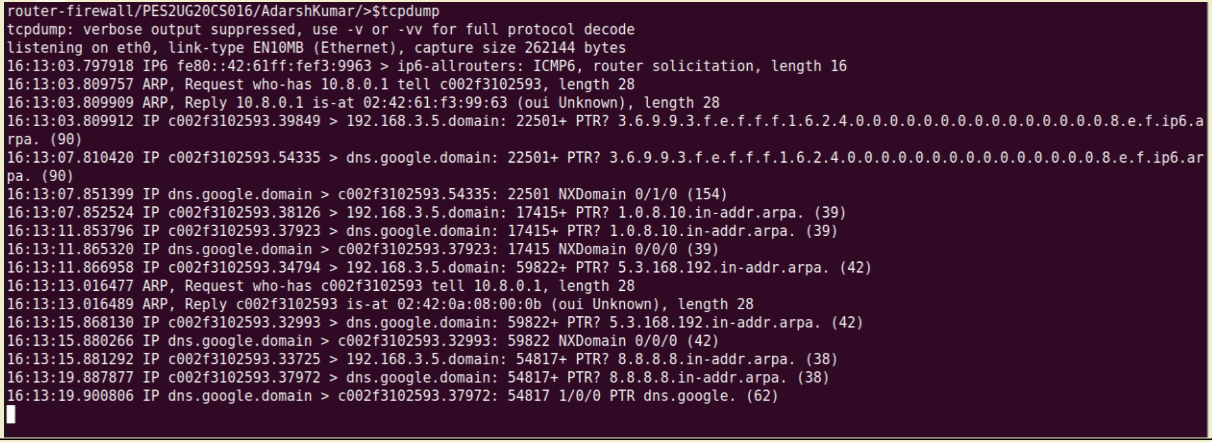
(2) Why can this tunnel successfully help users evade the firewall rule specified in the lab setup?

Ans: The curl commend will be forwarded to the external host to which we have established connection. That command will be used by the external host to fetch information required and it will send it to the internal host.

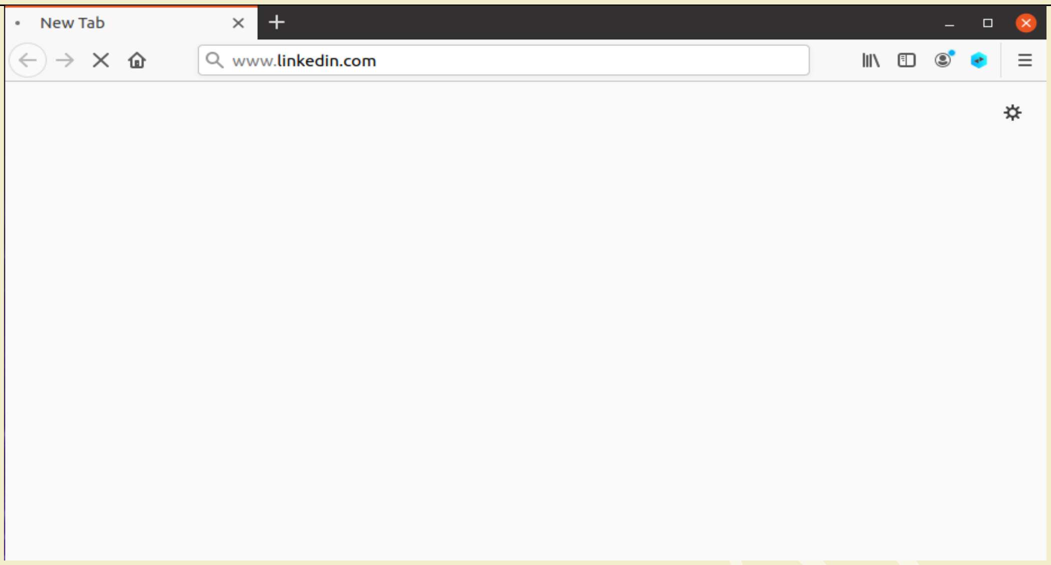
Task 2.2: Testing the Tunnel Using Browser

run tcpdump on the router-firewall, and point out the traffic involved in the entire port forwarding process.

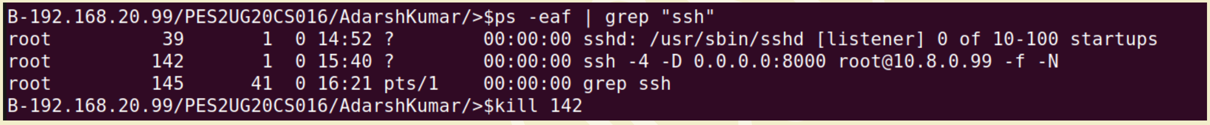
We can see that packets are being forwarded and the path is clearly visible on the router-firewall



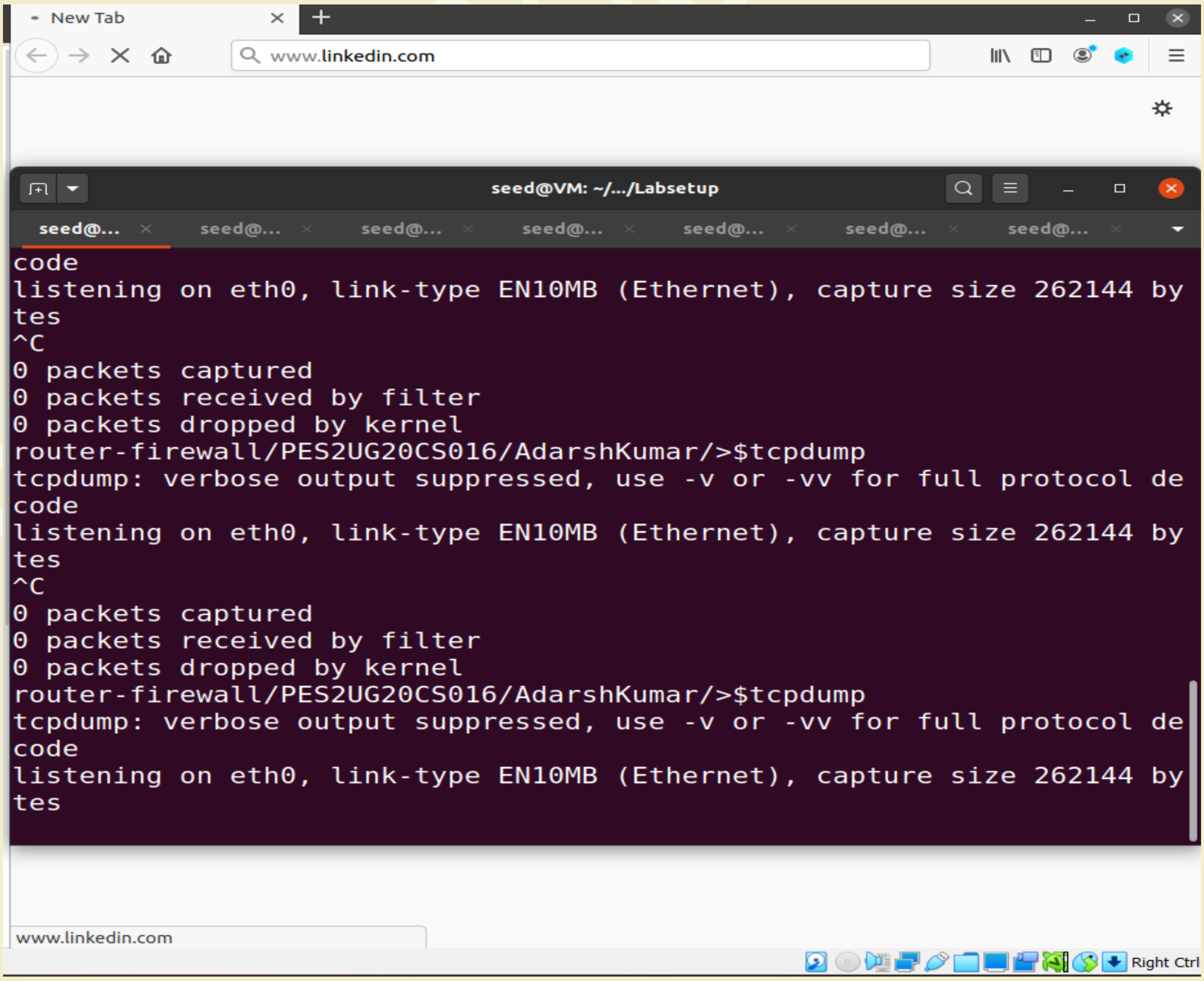
```
router-firewall/PES2UG20CS016/AdarshKumar/>$tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
16:13:03.797918 IP6 fe80::42:61ff:fef3:9963 > ip6-allrouters: ICMP6, router solicitation, length 16
16:13:03.809757 ARP, Request who-has 10.8.0.1 tell c002f3102593, length 28
16:13:03.809909 ARP, Reply 10.8.0.1 is-at 02:42:61:f3:99:63 (oui Unknown), length 28
16:13:03.809912 IP c002f3102593.39849 > 192.168.3.5.domain: 22501+ PTR? 3.6.9.9.3.f.e.f.f.f.1.6.2.4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.a
rpa. (90)
16:13:07.810420 IP c002f3102593.54335 > dns.google.domain: 22501+ PTR? 3.6.9.9.3.f.e.f.f.f.1.6.2.4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.ar
pa. (90)
16:13:07.851399 IP dns.google.domain > c002f3102593.54335: 22501 NXDomain 0/1/0 (154)
16:13:07.852524 IP c002f3102593.38126 > 192.168.3.5.domain: 17415+ PTR? 1.0.8.10.in-addr.arpa. (39)
16:13:11.853796 IP c002f3102593.37923 > dns.google.domain: 17415+ PTR? 1.0.8.10.in-addr.arpa. (39)
16:13:11.865320 IP dns.google.domain > c002f3102593.37923: 17415 NXDomain 0/0/0 (39)
16:13:11.866958 IP c002f3102593.34794 > 192.168.3.5.domain: 59822+ PTR? 5.3.168.192.in-addr.arpa. (42)
16:13:13.016477 ARP, Request who-has c002f3102593 tell 10.8.0.1, length 28
16:13:13.016489 ARP, Reply c002f3102593 is-at 02:42:0a:08:00:0b (oui Unknown), length 28
16:13:15.868130 IP c002f3102593.32993 > dns.google.domain: 59822+ PTR? 5.3.168.192.in-addr.arpa. (42)
16:13:15.880266 IP dns.google.domain > c002f3102593.32993: 59822 NXDomain 0/0/0 (42)
16:13:15.881292 IP c002f3102593.33725 > 192.168.3.5.domain: 54817+ PTR? 8.8.8.8.in-addr.arpa. (38)
16:13:19.887877 IP c002f3102593.37972 > dns.google.domain: 54817+ PTR? 8.8.8.8.in-addr.arpa. (38)
16:13:19.900806 IP dns.google.domain > c002f3102593.37972: 54817 1/0/0 PTR dns.google. (62)
```



(2) Break the SSH tunnel, and then try to browse a website. Describe your observation
After breaking the SSH tunnel, it shows that the connection is refused because of firewall rules

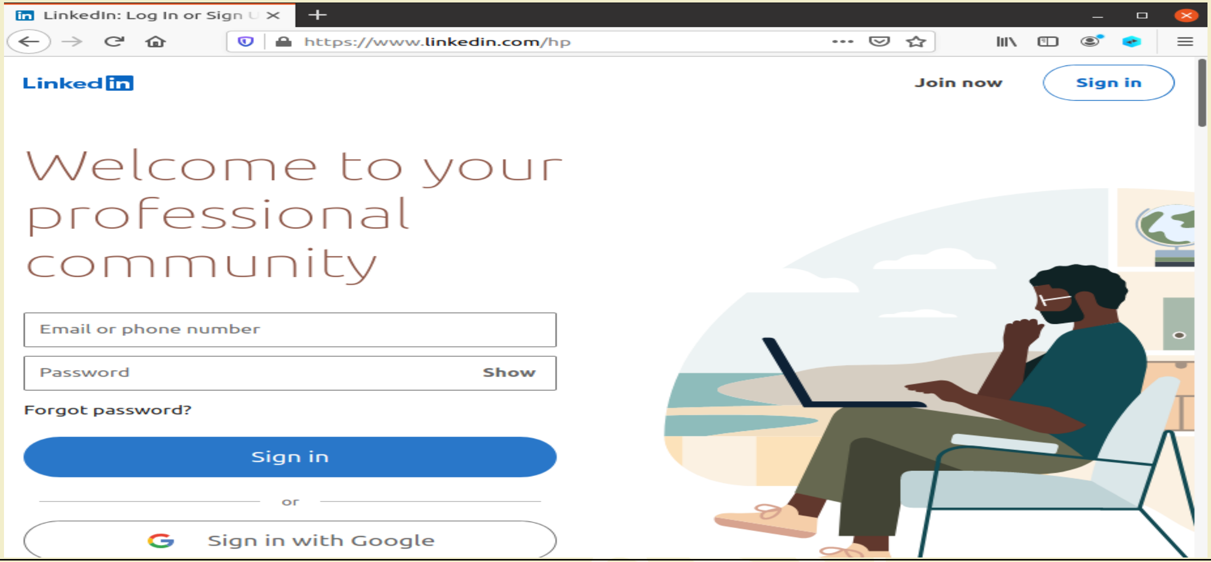


```
B-192.168.20.99/PES2UG20CS016/AdarshKumar/>$ps -eaf | grep "ssh"
root          39       1  0 14:52 ?        00:00:00 sshd: /usr/sbin/sshd [listener] 0 of 10-100 startups
root         142       1  0 15:40 ?        00:00:00 ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N
root         145      41  0 16:21 pts/1    00:00:00 grep ssh
B-192.168.20.99/PES2UG20CS016/AdarshKumar/>$kill 142
```



```
code
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 by
tes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
router-firewall/PES2UG20CS016/AdarshKumar/>$tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol de
code
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 by
tes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
router-firewall/PES2UG20CS016/AdarshKumar/>$tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol de
code
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 by
tes
```

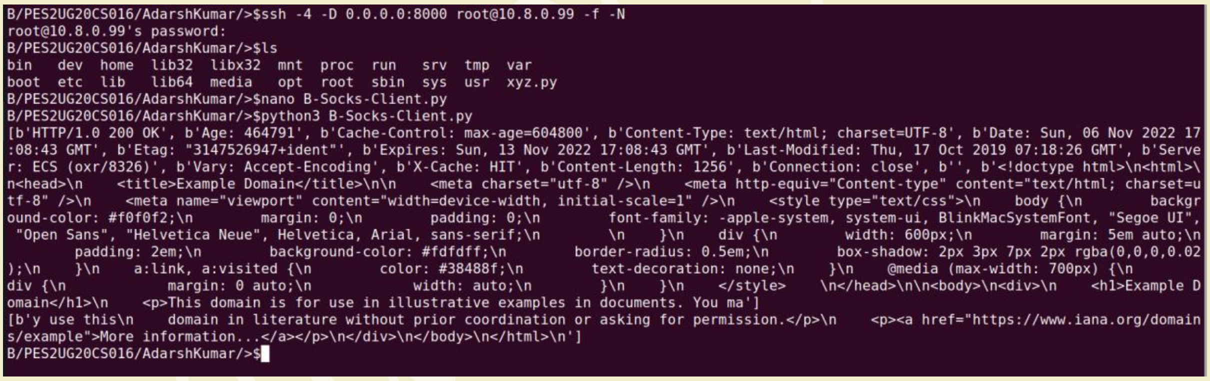
After cleaning up the proxy:
We can see that LinkedIn started working fine again



Welcome to your professional community

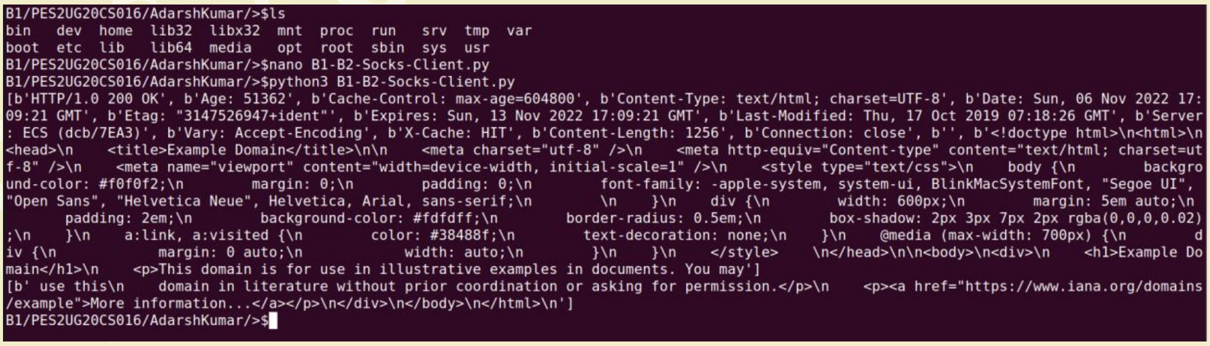
Task 2.3: Writing a SOCKS Client Using Python

Container B



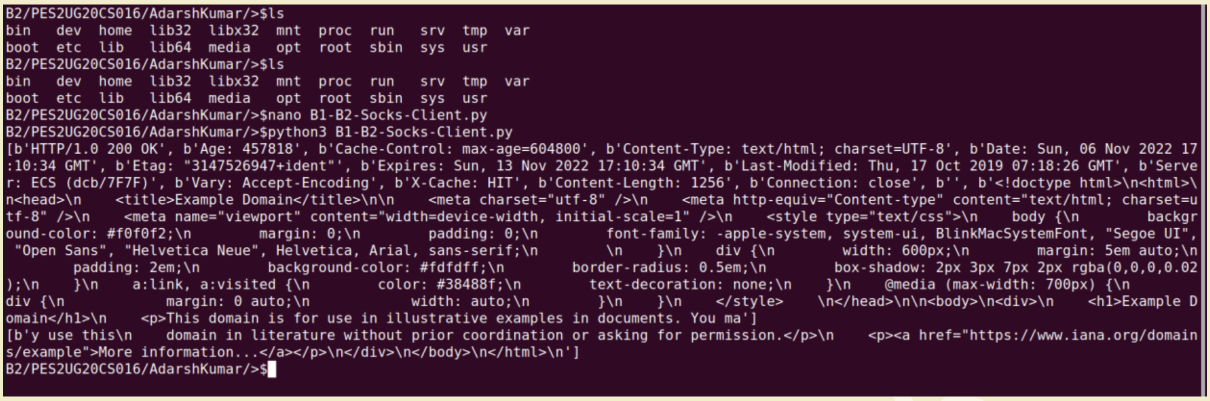
```
B/PES2UG20CS016/AdarshKumar/>$ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N
root@10.8.0.99's password:
B/PES2UG20CS016/AdarshKumar/>$ls
bin   dev  home  lib32  libx32  mnt  proc  run   srv  tmp  var
boot  etc  lib   lib64  media   opt  root  sbin  sys  usr  xyz.py
B/PES2UG20CS016/AdarshKumar/>$nano B-Socks-Client.py
B/PES2UG20CS016/AdarshKumar/>$python3 B-Socks-Client.py
[b'HTTP/1.0 200 OK', b'Age: 464791', b'Cache-Control: max-age=604800', b'Content-Type: text/html; charset=UTF-8', b'Date: Sun, 06 Nov 2022 17
:08:43 GMT', b'Etag: "3147526947+ident"', b'Expires: Sun, 13 Nov 2022 17:08:43 GMT', b'Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT', b'Serve
r: ECS (oxr/8326)', b'Vary: Accept-Encoding', b'X-Cache: HIT', b'Content-Length: 1256', b'Connection: close', b'', b'<!doctype html>\n<html>\
n<head>\n    <title>Example Domain</title>\n\n    <meta charset="utf-8" />\n    <meta http-equiv="Content-type" content="text/html; charset=u
tf-8" />\n    <meta name="viewport" content="width=device-width, initial-scale=1" />\n    <style type="text/css">\n    body {\n        backgr
ound-color: #f0f0f2;\n        margin: 0;\n        padding: 0;\n        font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI",
 "Open Sans", "Helvetica Neue", Helvetica, Arial, sans-serif;\n        \n    }\n    div {\n        width: 600px;\n        margin: 5em auto;\n
        padding: 2em;\n        background-color: #fdfdff;\n        border-radius: 0.5em;\n        box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02
);\n    }\n    a:link, a:visited {\n        color: #38488f;\n        text-decoration: none;\n    }\n    @media (max-width: 700px) {\n
div {\n            margin: 0 auto;\n            width: auto;\n        }\n    }\n    </style>    \n</head>\n\n<body>\n<div>\n    <h1>Example D
omain</h1>\n    <p>This domain is for use in illustrative examples in documents. You ma']
[b'y use this\n    domain in literature without prior coordination or asking for permission.</p>\n    <p><a href="https://www.iana.org/domain
s/example">More information...</a></p>\n</div>\n</body>\n</html>\n']
B/PES2UG20CS016/AdarshKumar/>$
```

Container B1



```
B1/PES2UG20CS016/AdarshKumar/>$ls
bin   dev  home  lib32  libx32  mnt  proc  run   srv  tmp  var
boot  etc  lib   lib64  media   opt  root  sbin  sys  usr
B1/PES2UG20CS016/AdarshKumar/>$nano B1-B2-Socks-Client.py
B1/PES2UG20CS016/AdarshKumar/>$python3 B1-B2-Socks-Client.py
[b'HTTP/1.0 200 OK', b'Age: 51362', b'Cache-Control: max-age=604800', b'Content-Type: text/html; charset=UTF-8', b'Date: Sun, 06 Nov 2022 17:
09:21 GMT', b'Etag: "3147526947+ident"', b'Expires: Sun, 13 Nov 2022 17:09:21 GMT', b'Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT', b'Server
: ECS (dcb/7EA3)', b'Vary: Accept-Encoding', b'X-Cache: HIT', b'Content-Length: 1256', b'Connection: close', b'', b'<!doctype html>\n<html>\n
<head>\n    <title>Example Domain</title>\n\n    <meta charset="utf-8" />\n    <meta http-equiv="Content-type" content="text/html; charset=ut
f-8" />\n    <meta name="viewport" content="width=device-width, initial-scale=1" />\n    <style type="text/css">\n    body {\n        backgro
und-color: #f0f0f2;\n        margin: 0;\n        padding: 0;\n        font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI",
"Open Sans", "Helvetica Neue", Helvetica, Arial, sans-serif;\n        \n    }\n    div {\n        width: 600px;\n        margin: 5em auto;\n
       padding: 2em;\n        background-color: #fdfdff;\n        border-radius: 0.5em;\n        box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02)
;\n    }\n    a:link, a:visited {\n        color: #38488f;\n        text-decoration: none;\n    }\n    @media (max-width: 700px) {\n        d
iv {\n            margin: 0 auto;\n            width: auto;\n        }\n    }\n    </style>    \n</head>\n\n<body>\n<div>\n    <h1>Example Do
main</h1>\n    <p>This domain is for use in illustrative examples in documents. You may']
[b' use this\n    domain in literature without prior coordination or asking for permission.</p>\n    <p><a href="https://www.iana.org/domains
/example">More information...</a></p>\n</div>\n</body>\n</html>\n']
B1/PES2UG20CS016/AdarshKumar/>$
```

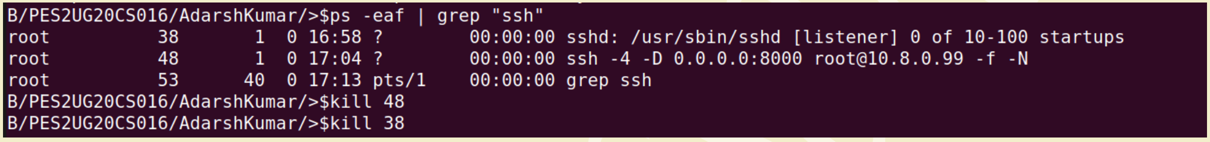
Container B2



```
B2/PES2UG20CS016/AdarshKumar/>$ls
bin   dev  home  lib32  libx32  mnt  proc  run   srv  tmp  var
boot  etc  lib   lib64  media   opt  root  sbin  sys  usr
B2/PES2UG20CS016/AdarshKumar/>$ls
bin   dev  home  lib32  libx32  mnt  proc  run   srv  tmp  var
boot  etc  lib   lib64  media   opt  root  sbin  sys  usr
B2/PES2UG20CS016/AdarshKumar/>$nano B1-B2-Socks-Client.py
B2/PES2UG20CS016/AdarshKumar/>$python3 B1-B2-Socks-Client.py
[b'HTTP/1.0 200 OK', b'Age: 457818', b'Cache-Control: max-age=604800', b'Content-Type: text/html; charset=UTF-8', b'Date: Sun, 06 Nov 2022 17
:10:34 GMT', b'Etag: "3147526947+ident"', b'Expires: Sun, 13 Nov 2022 17:10:34 GMT', b'Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT', b'Serve
r: ECS (dcb/7F7F)', b'Vary: Accept-Encoding', b'X-Cache: HIT', b'Content-Length: 1256', b'Connection: close', b'', b'<!doctype html>\n<html>\
n<head>\n    <title>Example Domain</title>\n\n    <meta charset="utf-8" />\n    <meta http-equiv="Content-type" content="text/html; charset=u
tf-8" />\n    <meta name="viewport" content="width=device-width, initial-scale=1" />\n    <style type="text/css">\n    body {\n        backgr
ound-color: #f0f0f2;\n        margin: 0;\n        padding: 0;\n        font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI",
 "Open Sans", "Helvetica Neue", Helvetica, Arial, sans-serif;\n        \n    }\n    div {\n        width: 600px;\n        margin: 5em auto;\n
        padding: 2em;\n        background-color: #fdfdff;\n        border-radius: 0.5em;\n        box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02
);\n    }\n    a:link, a:visited {\n        color: #38488f;\n        text-decoration: none;\n    }\n    @media (max-width: 700px) {\n
div {\n            margin: 0 auto;\n            width: auto;\n        }\n    }\n    </style>    \n</head>\n\n<body>\n<div>\n    <h1>Example D
omain</h1>\n    <p>This domain is for use in illustrative examples in documents. You ma']
[b'y use this\n    domain in literature without prior coordination or asking for permission.</p>\n    <p><a href="https://www.iana.org/domain
s/example">More information...</a></p>\n</div>\n</body>\n</html>\n']
B2/PES2UG20CS016/AdarshKumar/>$
```

Here can observe that traffic flow and we are able to fetch the content from the net as well.

SSH shell that is in the background



```
B/PES2UG20CS016/AdarshKumar/>$ps -eaf | grep "ssh"
root          38       1  0 16:58 ?        00:00:00 sshd: /usr/sbin/sshd [listener] 0 of 10-100 startups
root          48       1  0 17:04 ?        00:00:00 ssh -4 -D 0.0.0.0:8000 root@10.8.0.99 -f -N
root          53      40  0 17:13 pts/1    00:00:00 grep ssh
B/PES2UG20CS016/AdarshKumar/>$kill 48
B/PES2UG20CS016/AdarshKumar/>$kill 38
```

Task 3: Comparing SOCKS5 Proxy and VPN

- A SOCKS5 proxy is a more secure alternative to a traditional proxy that protects the traffic within a specific source, such as an application. When you use a SOCKS5 proxy, data packets from the configured source are routed through a remote server.
- This server changes the IP address associated with these data packets before they reach their final destination, offering greater anonymity online.
- SOCKS5 is the most recently optimized version of SOCKS, an internet protocol that funnels web traffic through a remote server.
- Using a SOCKS5 proxy for uTorrent or other P2P app will allow you to achieve better download/upload speeds when compared to VPN.
- While VPN encrypts your traffic, SOCK5 doesn't.
- In some instances, proxy servers might keep logs. That means if anyone is able to hack those servers, they will be able to obtain logs of your online activities

Difference between SOCKS5 Proxy vs VPN

	SOCKS5 Proxy	**VPN**
Encryption	SOCKS5 proxies don't encrypt your data.	VPNs encrypt all your network traffic, ensuring that no one can snoop on your activity.
IP Address	SOCKS5 proxies alter your IP address.	VPNs alter your IP address.
Speed	SOCKS5 proxies are faster than a VPN because they don't encrypt your traffic.	VPNs are acutely slower than your normal internet speed, as they encrypt your traffic.
Ease of Use	SOCKS5 proxies are manually configured, which is not difficult, but requires some technical knowledge.	VPNs are run from an app downloaded to your device, which makes it extremely easy to use by anyone.