Assignment 1 – IP and ICMP Attacks
Gunnar Yonker

1.

a. Sniffing is when someone uses an application like Wireshark to read the packets traveling through the network. This person can use an application like Wireshark to collect these packets and then gather information from them. One condition that needs to be met for one computer to sniff packets from another is that the network interface card needs to be set to promiscuous mode to ensure that the data packets are received and read by the network adapter. This allows a third-party to connect to the network and either choose to actively sniff by trying to redirect traffic to other ports such with IP spoofing attacks or they can passively sniff by just listening and reading the packets.

b. Blind-spoofing is when the attacker does not have any access to the reply from the host that the datagram is being sent to. For example, Host A could be sending a datagram to Host B and make it seem like the datagram was sent by Host C. Host B would receive the packet and if it was responded to, the response would go to Host C, not the attacker Host A. Non-Blind Spoofing is when the attacker is able to send the packet and is also able to be on the same subnet as the victim to sniff the reply packet. In the example above, it would be the same situation except Host A would be able to sniff the reply packet from Host B on its way to Host C.

2.

(1)

1500 datagram (20 bytes header + 1480 bytes payload)

MTU size in the WAN is 576

Fragmentation Enabled

Fragment	**ID**	**Flag**	**Offset**	**Payload Size**
1	111	1	0	552
2	111	1	69	552
3	111	0	138	376

- No ID given in prompt, so I used the ID example from the lecture slides of ID = 111, all packet fragments would have same ID so they could be correctly reassembled

(2)

ping www.google.com -l 1500 -f

All packets lost, needs to be fragmented

ping www.google.com -l 1400 -f

All packets sent and received

ping www.google.com -l 1470 -f

All packets sent and received

ping www.google.com -l 1476 -f

All packets lost, needs to be fragmented

ping www.google.com -l 1472 -f

All packets sent and received

ping www.google.com -l 1473 -f
All packets lost, needs to be fragmented

Starting with a payload size of 1500, the datagram needs to be fragmented but -f is set to not allow fragmentation so all the packets are lost. Adjusting the datagram size, 1400 was able to be sent and received. Through trial and error, the datagram size that can be sent and received is 1472. Anything larger than 1472 will need to be fragmented, anything equal to or smaller than 1472 can be sent without fragmentation. The datagram would need to have a 20 byte header and a payload size of 1480 to pass through the MTU size of 1500. Since we are using ping in this case, an additional 8 bytes are used for the ICMP header. Thus, the expected payload size for this ping on a path MTU size of 1500 would be 1500 – 20 – 8 = 1472 payload bytes. This is confirmed through my tested pings that fragmentation does not need to occur with a payload size of 1472, but any larger and fragmentation would need to occur. I think that the MTU is still 1500 bytes given this testing.

3.

(1)

Initial Ping

```
C:\Users\gunna>ping twitch.tv


Pinging twitch.tv [151.101.66.167] with 32 bytes of data:

Reply from 151.101.66.167: bytes=32 time=18ms TTL=57

Reply from 151.101.66.167: bytes=32 time=19ms TTL=57

Reply from 151.101.66.167: bytes=32 time=26ms TTL=57

Reply from 151.101.66.167: bytes=32 time=22ms TTL=57


Ping statistics for 151.101.66.167:

    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

    Minimum = 18ms, Maximum = 26ms, Average =
21ms
```

151.101.66.0-151.101.66.255 Range

1) 151.101.66.10

```
Ping statistics for 151.101.66.10:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
```

2) 151.101.66.37

```
Ping statistics for 151.101.66.37:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
```

3) 151.101.66.100

```
Ping statistics for 151.101.66.100:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
```

4) 151.101.66.116

```
Ping statistics for 151.101.66.116:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
```

5) 151.101.66.255

```
Ping statistics for 151.101.66.255:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

6) 151.101.66.0

```
Ping statistics for 151.101.66.0:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
```

7) 151.101.66.210

```
Ping statistics for 151.101.66.210:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
```

8) 151.101.66.200

```
Ping statistics for 151.101.66.200:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
```

9) 151.101.66.250

```
Ping statistics for 151.101.66.250:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
```

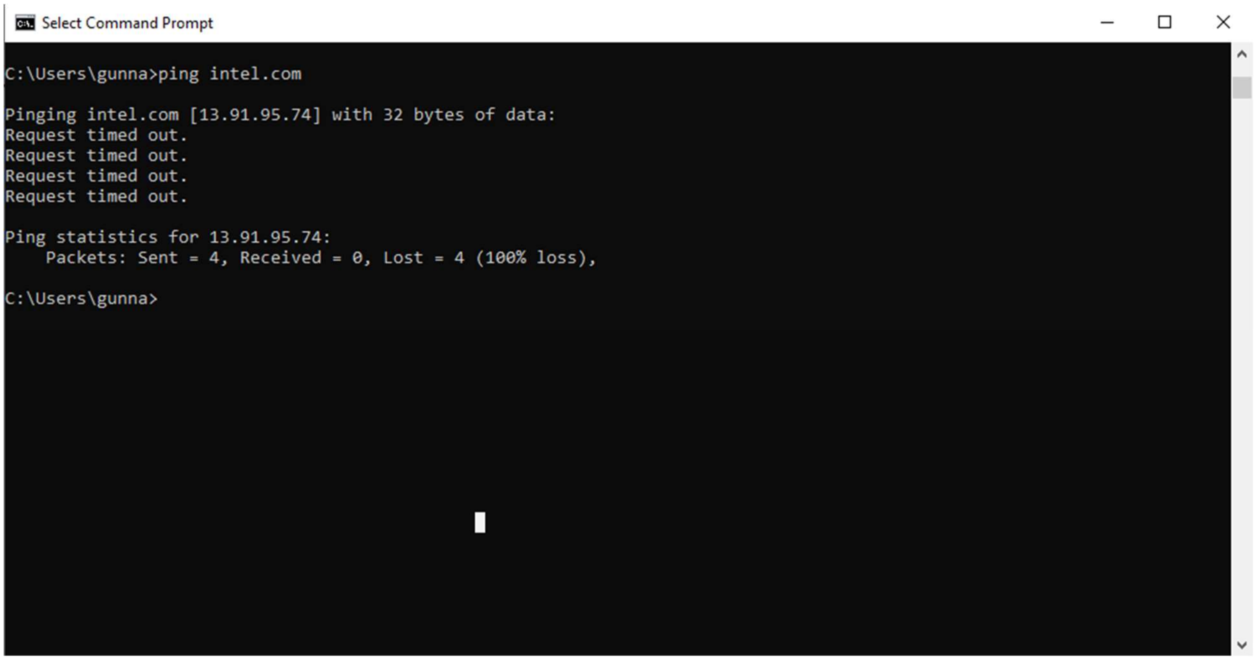
10) 151.101.66.254

Ping statistics for 151.101.66.254:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)

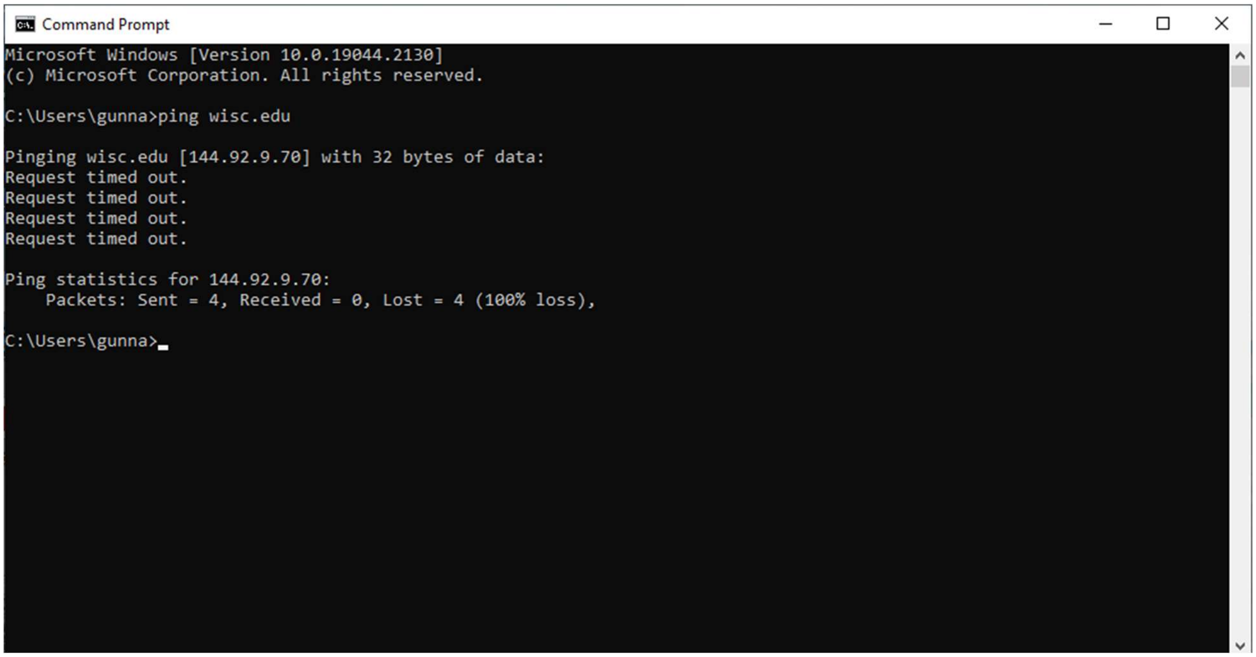
(2)

intel.com



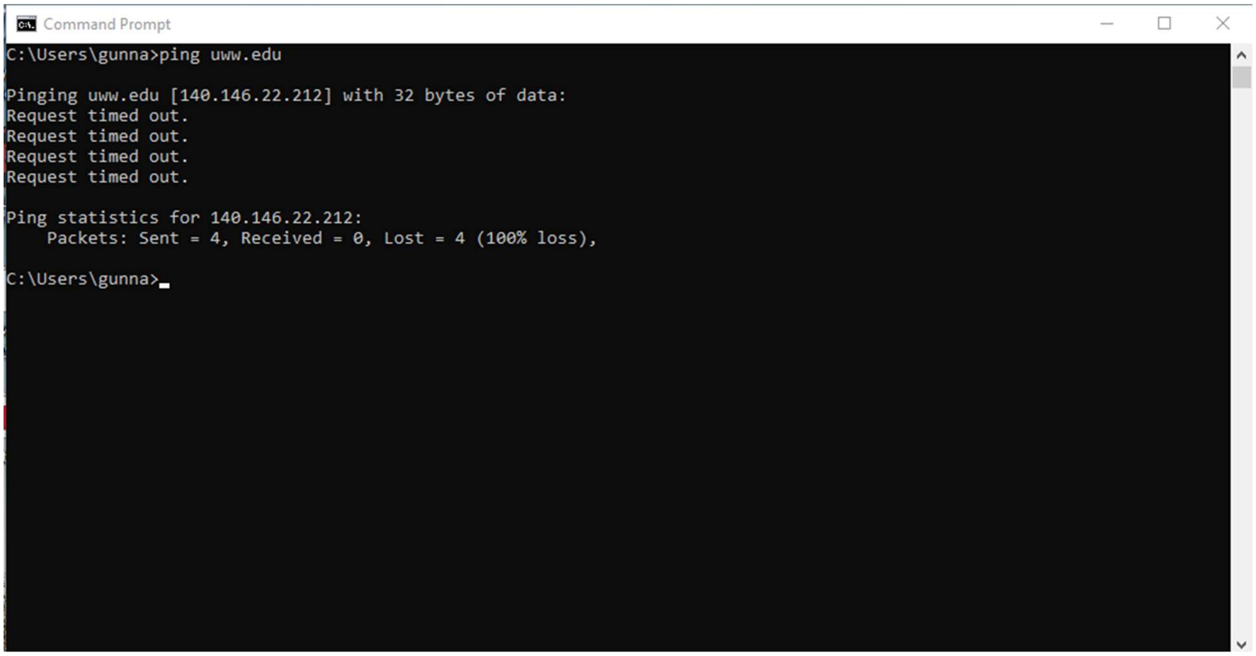
```
C:\Users\gunna>ping intel.com

Pinging intel.com [13.91.95.74] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 13.91.95.74:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\gunna>
```

wisc.edu



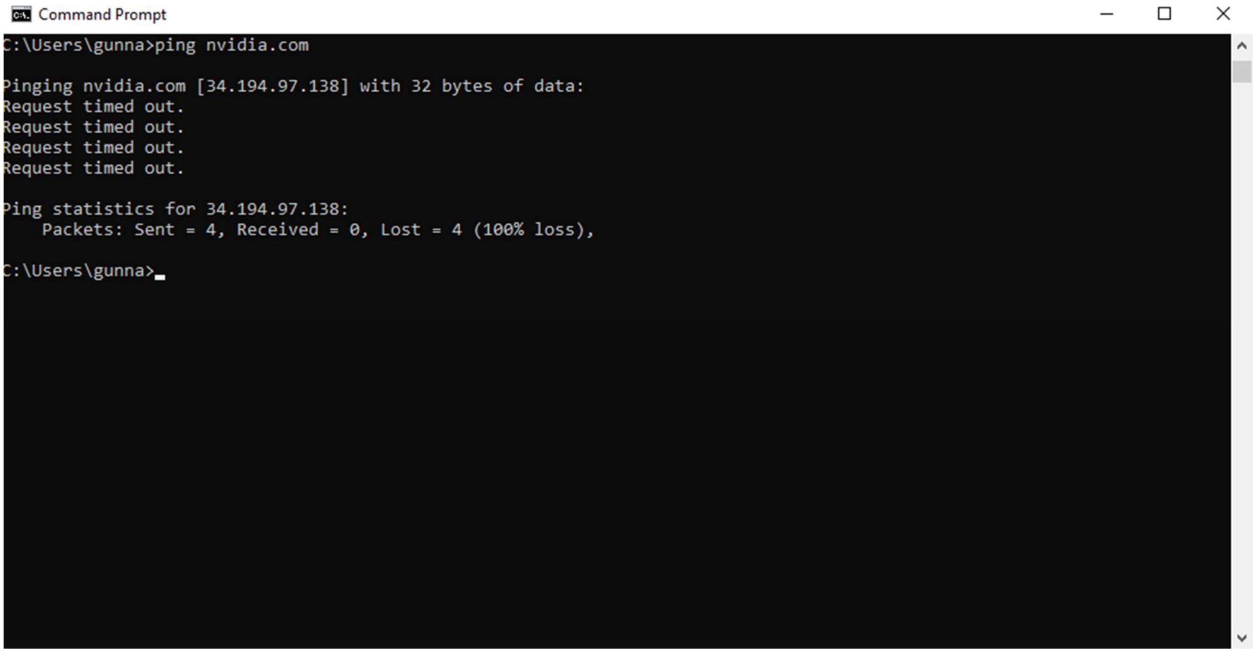
```
Microsoft Windows [Version 10.0.19044.2130]
(c) Microsoft Corporation. All rights reserved.

C:\Users\gunna>ping wisc.edu

Pinging wisc.edu [144.92.9.70] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 144.92.9.70:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\gunna>
```

uww.edu



```
C:\Users\gunna>ping uww.edu

Pinging uww.edu [140.146.22.212] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 140.146.22.212:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\gunna>
```

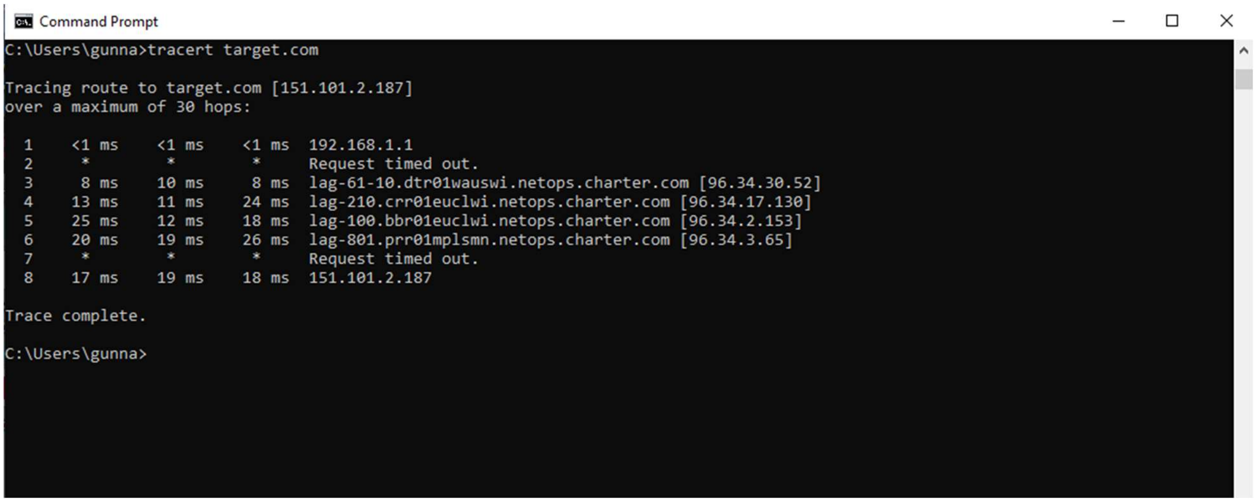
nvidia.com



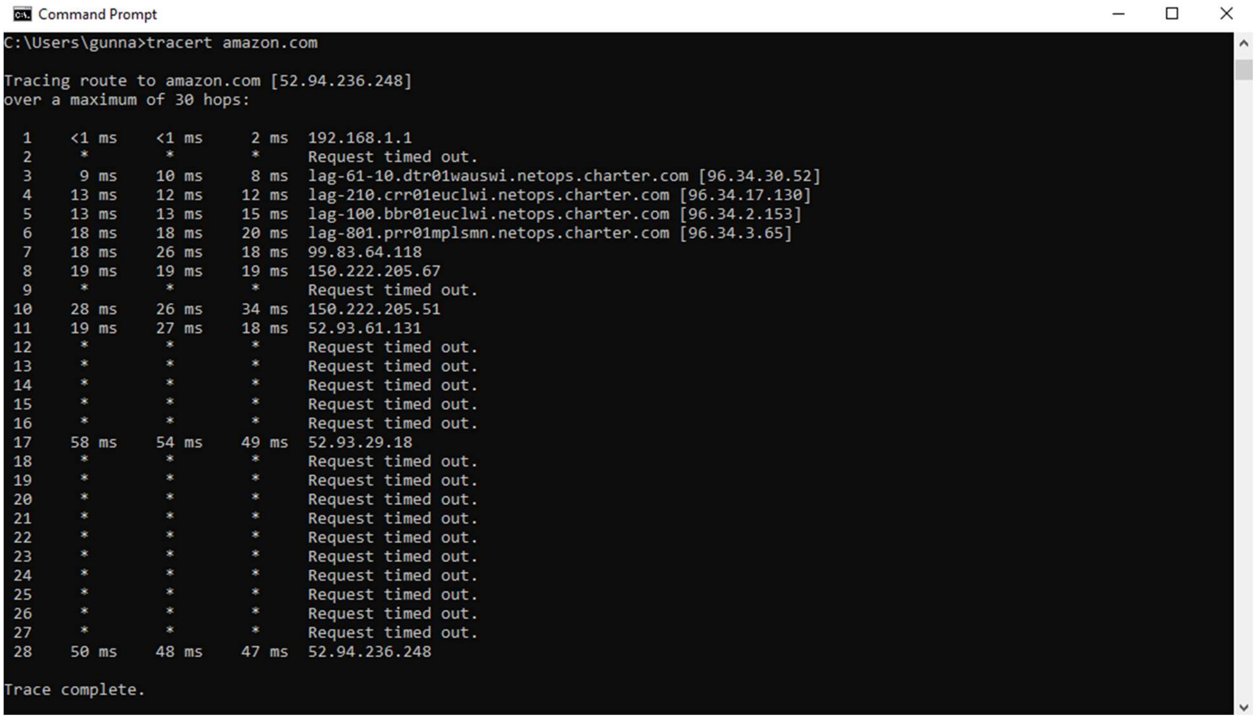
```
:\Users\gunna>ping nvidia.com

Pinging nvidia.com [34.194.97.138] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 34.194.97.138:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

:\Users\gunna>
```

It is possible that these websites have their ICMP commands blocked or have just the ping ICMP response blocked which would result in a request timed out result when pinged to that given website. This can be blocked on the firewall level for a website such as intel.com to protect against DoS attacks such as Ping flooding or the Ping of Death. Another reason could be is that in the network adapter settings that ping responses are blocked resulting in the request being timed out.

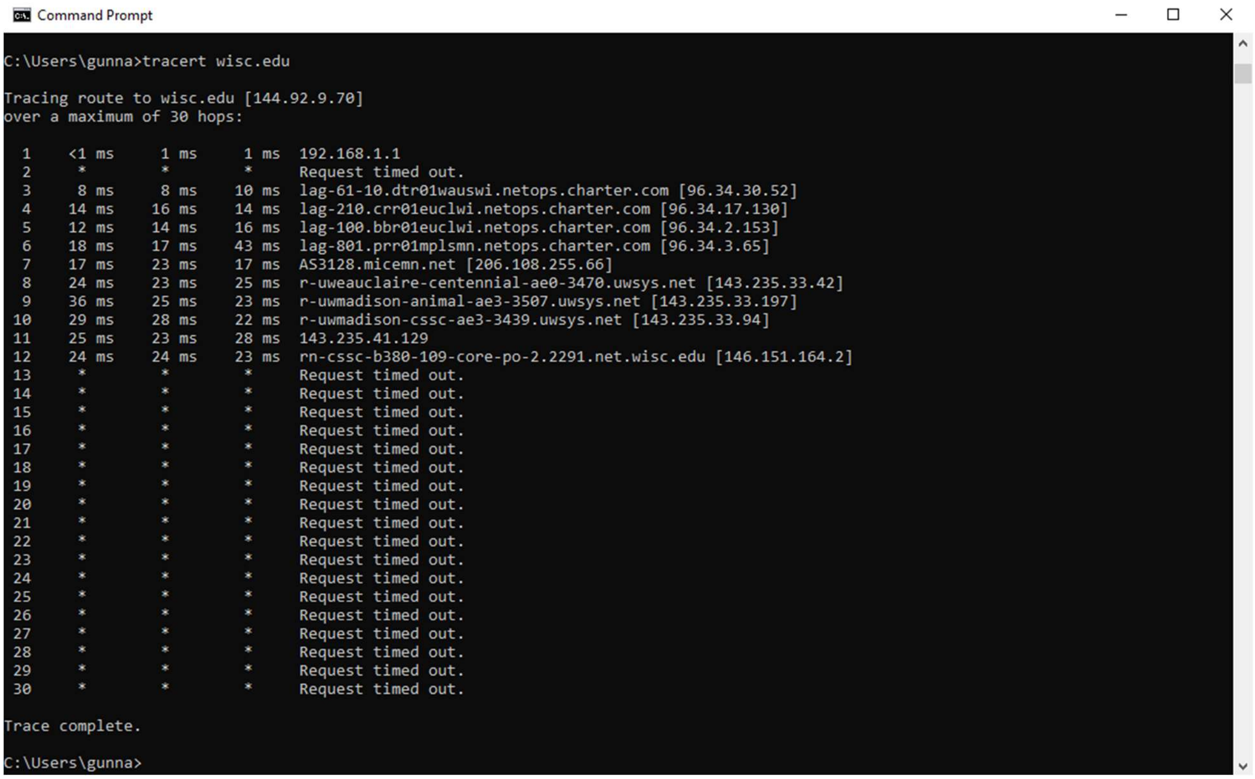
(3)



```
C:\Users\gunna>tracert target.com

Tracing route to target.com [151.101.2.187]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2     *        *        *     Request timed out.
  3     8 ms    10 ms     8 ms  lag-61-10.dtr01wauswi.netops.charter.com [96.34.30.52]
  4    13 ms    11 ms    24 ms  lag-210.crr01euclwi.netops.charter.com [96.34.17.130]
  5    25 ms    12 ms    18 ms  lag-100.bbr01euclwi.netops.charter.com [96.34.2.153]
  6    20 ms    19 ms    26 ms  lag-801.prr01mplsmn.netops.charter.com [96.34.3.65]
  7     *        *        *     Request timed out.
  8    17 ms    19 ms    18 ms  151.101.2.187

Trace complete.

C:\Users\gunna>
```



```
C:\Users\gunna>tracert amazon.com

Tracing route to amazon.com [52.94.236.248]
over a maximum of 30 hops:

  1    <1 ms    <1 ms     2 ms  192.168.1.1
  2     *        *        *     Request timed out.
  3     9 ms    10 ms     8 ms  lag-61-10.dtr01wauswi.netops.charter.com [96.34.30.52]
  4    13 ms    12 ms    12 ms  lag-210.crr01euclwi.netops.charter.com [96.34.17.130]
  5    13 ms    13 ms    15 ms  lag-100.bbr01euclwi.netops.charter.com [96.34.2.153]
  6    18 ms    18 ms    20 ms  lag-801.prr01mplsmn.netops.charter.com [96.34.3.65]
  7    18 ms    26 ms    18 ms  99.83.64.118
  8    19 ms    19 ms    19 ms  150.222.205.67
  9     *        *        *     Request timed out.
 10    28 ms    26 ms    34 ms  150.222.205.51
 11    19 ms    27 ms    18 ms  52.93.61.131
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17    58 ms    54 ms    49 ms  52.93.29.18
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28    50 ms    48 ms    47 ms  52.94.236.248

Trace complete.
```



```
C:\Users\gunna>tracert wisc.edu

Tracing route to wisc.edu [144.92.9.70]
over a maximum of 30 hops:

  1    <1 ms     1 ms     1 ms  192.168.1.1
  2     *        *        *     Request timed out.
  3     8 ms     8 ms    10 ms  lag-61-10.dtr01wauswi.netops.charter.com [96.34.30.52]
  4    14 ms    16 ms    14 ms  lag-210.crr01euclwi.netops.charter.com [96.34.17.130]
  5    12 ms    14 ms    16 ms  lag-100.bbr01euclwi.netops.charter.com [96.34.2.153]
  6    18 ms    17 ms    43 ms  lag-801.prr01mplsmn.netops.charter.com [96.34.3.65]
  7    17 ms    23 ms    17 ms  AS3128.micemn.net [206.108.255.66]
  8    24 ms    23 ms    25 ms  r-uweauclaire-centennial-ae0-3470.uwsys.net [143.235.33.42]
  9    36 ms    25 ms    23 ms  r-uwmadison-animal-ae3-3507.uwsys.net [143.235.33.197]
 10    29 ms    28 ms    22 ms  r-uwmadison-cssc-ae3-3439.uwsys.net [143.235.33.94]
 11    25 ms    23 ms    28 ms  143.235.41.129
 12    24 ms    24 ms    23 ms  rn-cssc-b380-109-core-po-2.2291.net.wisc.edu [146.151.164.2]
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.

C:\Users\gunna>
```

The request timed out message can be a result of the ICMP response being blocked by the firewall. It is also possible that the website is getting higher priority traffic which could result in the traceroute being packet being dropped simply because there is higher priority traffic taking place. Most likely, it is because the traceroute response on that hop has ICMP packet responses blocked so that they are dropped to prevent a DoS attack. After a bit of research, a Request Timed Out response on hop 2 is very common, as it most likely just means that it is a device that might not respond to traceroute requests. Even though the traceroute shows request timed out through this method, the website is still available to be actively browsed on the web.