CA169 Assignment 1 Lab Report

Submit these pages onwards.

Date:	06/03/2019
STUDENT NAME:	Andrew Finn
STUDENT NUMBER:	[redacted]
PROJECT NUMBER:	1
MODULE CODE:	CA169
DEGREE: [CA EC ECSA PSSD]	CA
LECTURER:	Brian Stone

Declaration

In submitting this project, I declare that the project material, which I now submit, is my own work. Any assistance received by way of borrowing from the work of others has been cited and acknowledged within the work. I make this declaration in the knowledge that a breach of the rules pertaining to project submission may carry serious consequences.

Answer Sheets

Ipconfig exercise.

IP address of the machine	136.206.18.168
MAC address	50-9A-4C-3D-94-7E

Ping exercise 1

```
Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP
                   Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
                   Per RFC 5095 the use of this routing header has been
                   deprecated. Some systems may drop echo requests if
                   this header is used.
    -S srcaddr     Source address to use.
    -c compartment Routing compartment identifier.
    -p             Ping a Hyper-V Network Virtualization provider address.
    -4             Force using IPv4.
    -6             Force using IPv6.
```

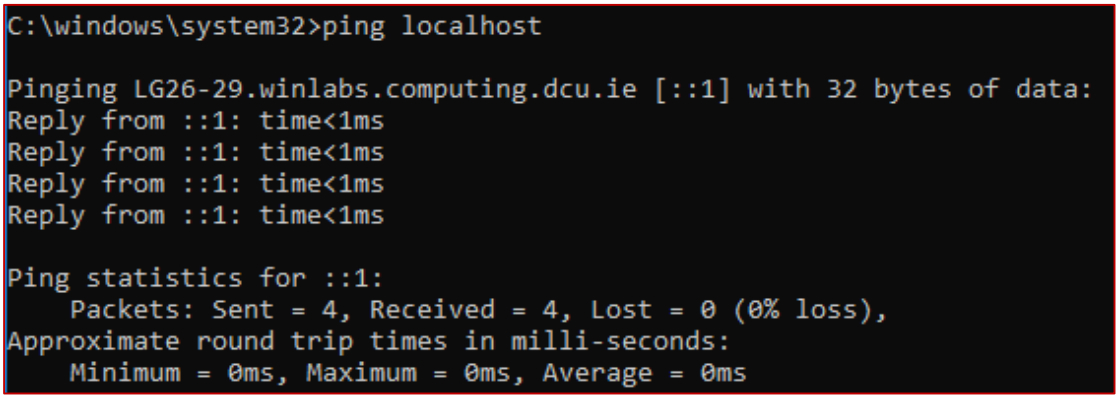
What is displayed?

The above is displayed. It shows the usage for the ping command and various arguments that can be used to alternate usage and settings

Ping exercise 2

Ping localhost

Paste window here.



1. *What information is returned?*
2. *What is the localhost?*

Answer 1

1. The command shows who it is pinging, the amount of data that is being pinged the replies from “localhost” and statistical data such as packet loss / send receive count and finally data concerning Ping time (Length of time between the message being sent and a reply received)

2. Localhost simply refers to the current machine. When you ping localhost or navigate to http://localhost the machine resolves that address to the current local ip address and operates the command as it would any other ip address as such pinging the machine it is executed on hence the near instant (<1ms) response time.

Second part exercise 2

For higher marks

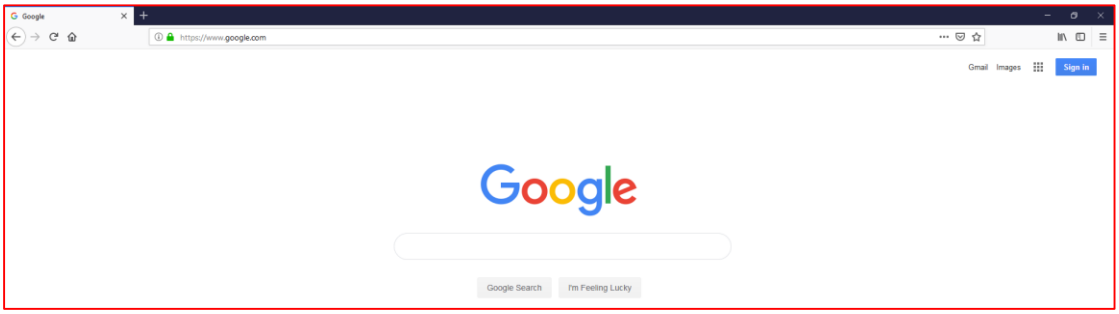
```
NetRange:       74.125.0.0 - 74.125.255.255
CIDR:           74.125.0.0/16
NetName:        GOOGLE
NetHandle:      NET-74-125-0-1
Parent:         NET74 (NET-74-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Google LLC (GOGL)
RegDate:        2007-03-13
Updated:        2012-02-24
Ref:            https://rdap.arin.net/registry/ip/74.125.0.0


OrgName:        Google LLC
OrgId:          GOGL
Address:        1600 Amphitheatre Parkway
City:           Mountain View
StateProv:      CA
PostalCode:     94043
Country:        US
RegDate:        2000-03-30
Updated:        2018-10-24
Comment:        Please note that the recommended way to file abuse comp
Comment:
Comment:        To report abuse and illegal activity: https://www.googl
Comment:
Comment:        For legal requests: http://support.google.com/legal
Comment:
Comment:        Regards,
Comment:        The Google Team
Ref:            https://rdap.arin.net/registry/entity/GOGL


OrgAbuseHandle: ABUSE5250-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-650-253-0000
OrgAbuseEmail:  network-abuse@google.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE5250-ARIN

OrgTechHandle: ZG39-ARIN
OrgTechName:   Google LLC
OrgTechPhone:  +1-650-253-0000
```

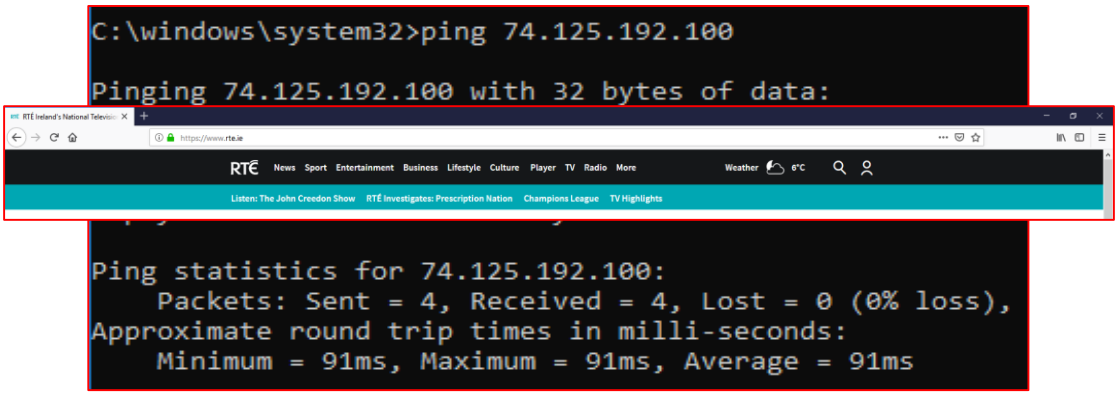
```
Domain:                   rte.ie
Domain Holder:            RTE Commercial Enterprises Limited
Admin-c:                  AWB910-IEDR
Admin-c:                  JM474-IEDR
Tech-c:                   JM474-IEDR
Account Name:             DIRECT REGISTRANT
Registrar Abuse Contact:  reg-abuse@iedr.ie
Registration Date:        11-February-2000
Renewal Date:             31-March-2024
Holder-type:              Billable
Locked status:            NO
Renewal status:           Active
In-zone:                  1
Nserver:                  ns1.rte.ie 162.159.0.73 2400:cb00:2049:1::a29f
Nserver:                  ns2.rte.ie 162.159.1.73 2400:cb00:2049:1::a29f
Nserver:                  ns3.rte.ie 162.159.2.27 2400:cb00:2049:1::a29f
Nserver:                  ns4.rte.ie 162.159.3.18 2400:cb00:2049:1::a29f
```

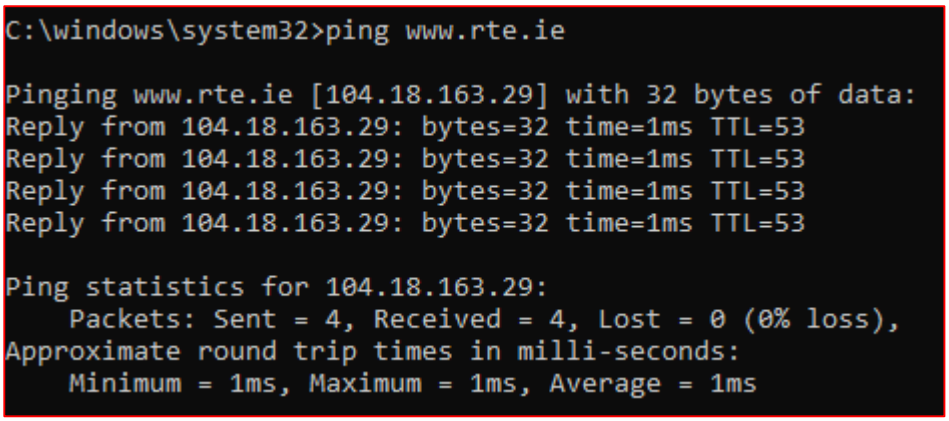
Using a WHOIS service to see the registered information on file from when the Organization registered their respective domain yields the above data.

	URL / IP	Owner	Phone	Postal
rte.ie	162.159.0.73 162.159.1.73 162.159.2.27 162.159.3.18	RTE Commercial Enterprises Limited	+353 1 208 3111	RTÉ Donnybrook, Dublin 4, IE
google.com	74.125.0.0 -> 74.125.255.255	Google LLC	+1-650-253-0000	1600 Amphitheatre Parkway, Mountain View, CA

Ping and/or enter into browser the three addresses.
Paste windows here







Picture 1.
When entering 74.125.193.100 or 74.125.193.100:80 into a browser the address it loads the google.com homepage. This is true with or without :80 as the browser automatically adjusts for this as port 80 is the default for http. www.google.com shows in the address bar as my DNS provider (CloudFlare, but in general it is ran by the users ISP) has resolved the IP address to google.

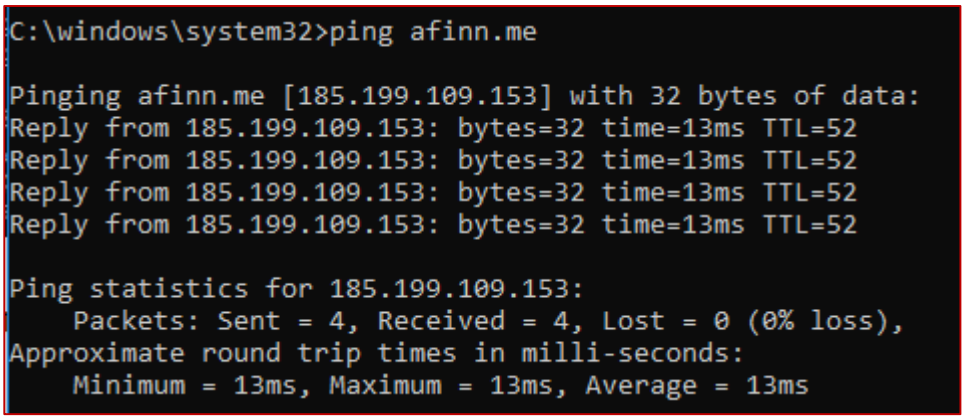
Picture 2.
Shows the response when pinging 74.125.193.100 and 74.125.193.100:80 respectively.
Pinging 74.125.193.100 works as expected (details about ping can be seen in the answer from pinging localhost). However, when pinging 74.125.193.100:80 the command fails as it can't find a host. This is because ping uses ICMP (Internet Control Message Protocol) and not UDP/TCP where ports are established.

Picture 3.
Shows the terminal when pinging www.rte.ie. The address is sent to my DNS provider and is resolved and returned the IP address which is then pinged in the same method as listed above for pinging localhost.

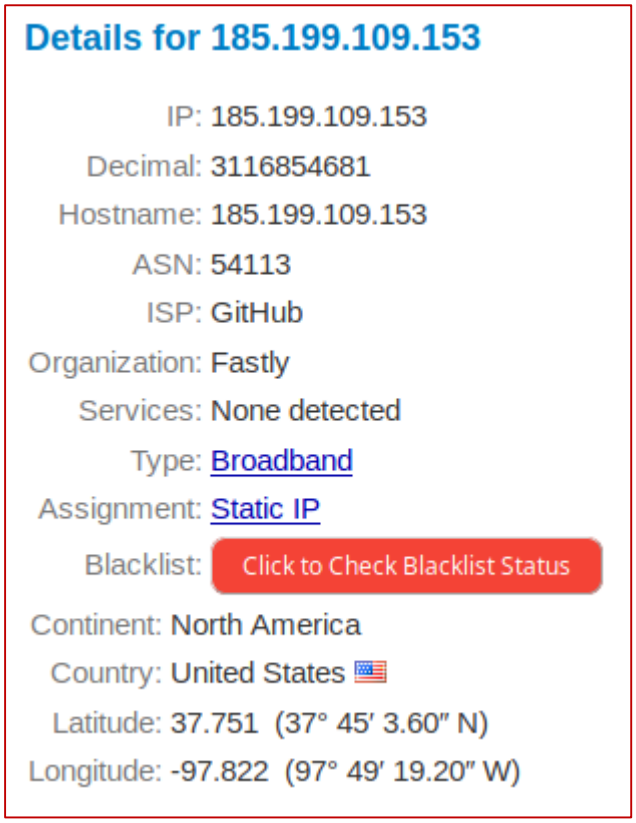
Picture 4.
Shows my browser loading www.rte.ie. This works as a DNS request is sent and an IP address is returned, my browser then connects to the IP address typically on port 80, downloads and then displays the homepage/ index.html

Exercise 3

Paste window 1



First I pinged my own website. This website is hosted by GitHub in the USA (Foreign website) as seen from the below screenshot.

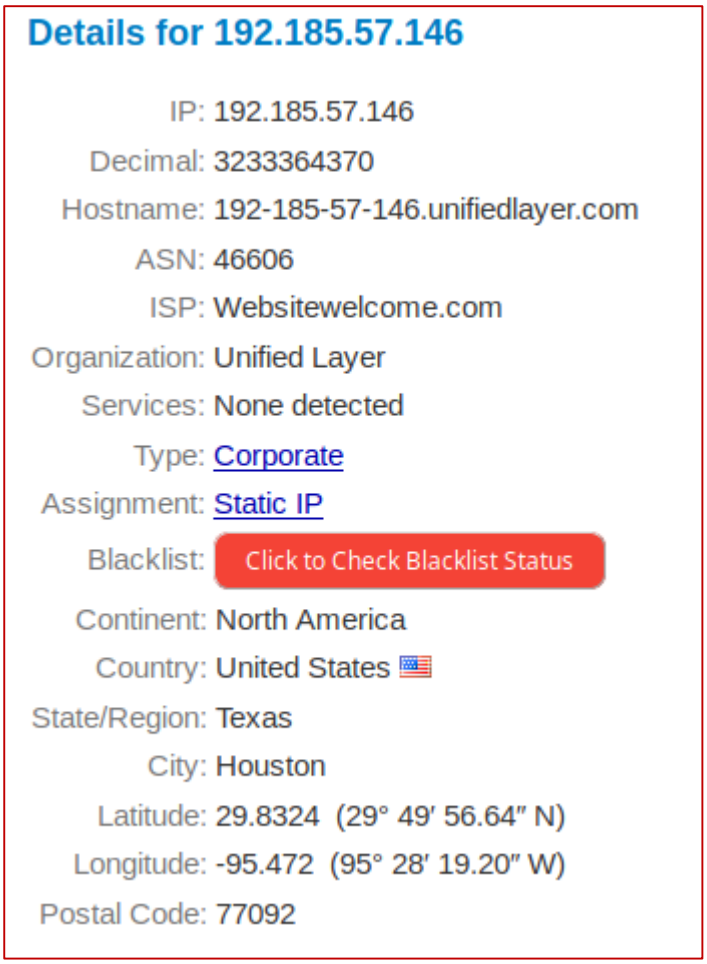


Paste window 2

The second website is a bit more interesting… After a bit of googling i found a database of sites indexed by ping. I sorted for the slowest average response, and the found one that was appropriate and who didn't use a privacy service for their WHOIS information.

```
Pinging mysorecarrental.com [192.185.57.146] with 32 bytes of data:
Reply from 192.185.57.146: bytes=32 time=318ms TTL=127
Reply from 192.185.57.146: bytes=32 time=268ms TTL=127
Reply from 192.185.57.146: bytes=32 time=150ms TTL=127
Reply from 192.185.57.146: bytes=32 time=320ms TTL=127

Ping statistics for 192.185.57.146:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 150ms, Maximum = 320ms, Average = 264ms
```

The website is hosted in the USA.



	Website 1	*Website 2*
Name of the website pinged	afinn.me	mysorecarrental.com
What is the IP address returned?	185.199.111.153	192.185.57.146
What is the TTL figure?	1780 Seconds	5928 Seconds
Average round trip time	34ms	264ms

Your comments on administrative information that you found by searching on the Internet about the websites from experiment 3. Things like, who owns it, phone numbers, email addresses, registered addresses etc, anything at all that tells us about the website and its administration.

afinn.me:

```
finna8@xps:~$ whois afinn.me
Domain Name: AFINN.ME
Registry Domain ID: D425500000081459820-AGRS
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: www.namecheap.com
Updated Date: 2019-02-19T21:15:14Z
Creation Date: 2018-12-20T22:54:46Z
Registry Expiry Date: 2019-12-20T22:54:46Z
Registrar Registration Expiration Date:
Registrar: NameCheap, Inc.
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registrant Organization:
Registrant State/Province: Panama
Registrant Country: PA
Name Server: DNS1.REGISTRAR-SERVERS.COM
Name Server: DNS2.REGISTRAR-SERVERS.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form  https://www.icann.org/wicf/)
>>> Last update of WHOIS database: 2019-03-06T21:33:35Z <<<
```

As I use a privacy setting for my WHOIS data no useful WHOIS data is displayed. However, when pinging afinn.me it redirects to andrew-finn.github.io. This is a standard format there for andrew-finn is my GitHub user name and details can then be found via my GitHub. The IP address is useless as it is for GitHub servers and has no connection to the domain. The response time is fairly quick considering the server is thousands kilometres away.

mysorecarrental.com:

```
Domain Name: MYSORECARRENTAL.COM
Registry Domain ID: 2022869511_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.syrahost.com
Registrar URL: http://www.crazydomains.com
Updated Date: 2019-02-11T20:17:09Z
Creation Date: 2016-04-20T00:00:00Z
Registrar Registration Expiration Date: 2021-04-20T00:00:00Z
Registrar: CRAZY DOMAINS FZ-LLC
Registrar IANA ID: 1291
Registrar Abuse Contact Email: domains@crazydomains.com
Registrar Abuse Contact Phone: +61.894220890
Reseller: DOMAIN REGISTRATION INDIA
Domain Status: ok https://icann.org/epp#ok
Registry Registrant ID: R-020879119-SN
Registrant Name: PRADEEP SHANKAR
Registrant Organization:
Registrant Street: 121, HEBBAL 1ST STAGE, METAGALLI
Registrant City: MYSORE
Registrant State/Province: KARNATAKA
Registrant Postal Code: 570016
Registrant Country: IN
Registrant Phone: +91.9480735315
Registrant Phone Ext:
Registrant Email: PRADIFOX@GMAIL.COM
Registry Admin ID: C-007839911-SN
Admin Name: PRADEEP SHANKAR
Admin Organization:
Admin Street: 121, HEBBAL 1ST STAGE, METAGALLI
Admin City: MYSORE
Admin State/Province: KARNATAKA
Admin Postal Code: 570016
Admin Country: IN
Admin Phone: +91.9480735315
Admin Phone Ext:
Admin Email: PRADIFOX@GMAIL.COM
Registry Tech ID: C-007839911-SN
Tech Name: PRADEEP SHANKAR
Tech Organization:
Tech Street: 121, HEBBAL 1ST STAGE, METAGALLI
Tech City: MYSORE
Tech State/Province: KARNATAKA
Tech Postal Code: 570016
Tech Country: IN
Tech Phone: +91.9480735315
Tech Phone Ext:
Tech Email: PRADIFOX@GMAIL.COM
Name Server: NS1.LINUXCONTROLPANEL.COM
Name Server: NS2.LINUXCONTROLPANEL.COM
```

The domain is owned and ran by Mr Shankar, his address, phone number, email etc. can be seen above. The response time is painfully slow and there is a noticeable delay in loading the website.

Exercise 4: Netstat exercise

Number of packets received by workstation:

Window here.

```
C:\windows\system32>netstat -sp IP

IPv4 Statistics

  Packets Received                   = 361551
  Received Header Errors             = 0
  Received Address Errors            = 494
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 29266
  Received Packets Delivered         = 365909
  Output Requests                    = 168883
  Routing Discards                   = 0
  Discarded Output Packets           = 6760
  Output Packet No Route             = 22
  Reassembly Required                = 0
  Reassembly Successful              = 0
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0

C:\windows\system32>ping www.google.ie

Pinging www.google.ie [74.125.193.94] with 32 bytes of data:
Reply from 74.125.193.94: bytes=32 time=1ms TTL=47
Reply from 74.125.193.94: bytes=32 time=2ms TTL=47
Reply from 74.125.193.94: bytes=32 time=2ms TTL=47
Reply from 74.125.193.94: bytes=32 time=2ms TTL=47

Ping statistics for 74.125.193.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\windows\system32>netstat -sp IP

IPv4 Statistics

  Packets Received                   = 361685
  Received Header Errors             = 0
  Received Address Errors            = 494
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 29266
  Received Packets Delivered         = 366048
  Output Requests                    = 169020
  Routing Discards                   = 0
  Discarded Output Packets           = 6765
  Output Packet No Route             = 22
  Reassembly Required                = 0
  Reassembly Successful              = 0
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0
```

361685 – 361551 = 134 Packets Revived

ICMP packets explained:

The Internet Control Message Protocol is the system in place to return feedback concerning network problems that are preventing the delivery of a packet(s). This is because the IP is unreliable and does not have a function to guarantee delivery.

```
C:\windows\system32>netstat -sp ICMP

ICMPv4 Statistics

                            Received    Sent
  Messages                  2821        2823
  Errors                    0           0
  Destination Unreachable   2643        2641
  Time Exceeded             0           0
  Parameter Problems        0           0
  Source Quenches           0           0
  Redirects                 0           0
  Echo Replies              178         0
  Echos                     0           182
  Timestamps                0           0
  Timestamp Replies         0           0
  Address Masks             0           0
  Address Mask Replies      0           0
  Router Solicitations      0           0
  Router Advertisements     0           0

C:\windows\system32>ping www.google.ie

Pinging www.google.ie [74.125.193.94] with 32 bytes of data:
Reply from 74.125.193.94: bytes=32 time=2ms TTL=47
Reply from 74.125.193.94: bytes=32 time=2ms TTL=47
Reply from 74.125.193.94: bytes=32 time=2ms TTL=47
Reply from 74.125.193.94: bytes=32 time=2ms TTL=47

Ping statistics for 74.125.193.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms

C:\windows\system32>netstat -sp ICMP

ICMPv4 Statistics

                            Received    Sent
  Messages                  2827        2829
  Errors                    0           0
  Destination Unreachable   2645        2643
  Time Exceeded             0           0
  Parameter Problems        0           0
  Source Quenches           0           0
  Redirects                 0           0
  Echo Replies              182         0
  Echos                     0           186
  Timestamps                0           0
  Timestamp Replies         0           0
  Address Masks             0           0
  Address Mask Replies      0           0
  Router Solicitations      0           0
  Router Advertisements     0           0
```

Pinging www.google.ie and loading www.dcu.ie resulting in the machine receiving 6 (2827 - 2821) IMCP Packets.

Discuss the connections opened by visiting the DCU website here.
Also, grab the window, showing connections opened as a result of visiting the DCU website.

```
C:\windows\system32>netstat -o

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    136.206.18.168:59356   40.67.253.249:https    ESTABLISHED     3928
  TCP    136.206.18.168:59379   136.206.217.61:microsoft-ds  ESTABLISHED     4
  TCP    136.206.18.168:59952   Caher:8000             CLOSE_WAIT      8448
  TCP    136.206.18.168:59953   Caher:8000             CLOSE_WAIT      8448
  TCP    136.206.18.168:59954   Caher:8000             CLOSE_WAIT      8448
  TCP    136.206.18.168:59955   Caher:8000             CLOSE_WAIT      8448
  TCP    136.206.18.168:59956   Caher:8000             CLOSE_WAIT      8448
  TCP    136.206.18.168:60039   Caher:8000             ESTABLISHED     4692

C:\windows\system32>netstat -o

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    136.206.18.168:59356   40.67.253.249:https    ESTABLISHED     3928
  TCP    136.206.18.168:59379   136.206.217.61:microsoft-ds  ESTABLISHED     4
  TCP    136.206.18.168:59952   Caher:8000             CLOSE_WAIT      8448
  TCP    136.206.18.168:59953   Caher:8000             CLOSE_WAIT      8448
  TCP    136.206.18.168:59954   Caher:8000             CLOSE_WAIT      8448
  TCP    136.206.18.168:59955   Caher:8000             CLOSE_WAIT      8448
  TCP    136.206.18.168:59956   Caher:8000             CLOSE_WAIT      8448
  TCP    136.206.18.168:60040   Caher:8000             ESTABLISHED     6364
  TCP    136.206.18.168:60041   Caher:8000             ESTABLISHED     6364
  TCP    136.206.18.168:60042   Caher:8000             ESTABLISHED     6364
  TCP    136.206.18.168:60043   Caher:8000             ESTABLISHED     4596
  TCP    136.206.18.168:60044   Caher:8000             ESTABLISHED     5836
  TCP    136.206.18.168:60045   Caher:8000             ESTABLISHED     6364
  TCP    136.206.18.168:60046   Caher:8000             ESTABLISHED     6364
  TCP    136.206.18.168:60047   Caher:8000             ESTABLISHED     6364
  TCP    136.206.18.168:60048   Caher:8000             ESTABLISHED     6364
  TCP    136.206.18.168:60049   Caher:8000             ESTABLISHED     6364
  TCP    136.206.18.168:60050   Caher:8000             ESTABLISHED     6364
  TCP    136.206.18.168:60051   Caher:8000             ESTABLISHED     6364
  TCP    136.206.18.168:60052   Caher:8000             ESTABLISHED     6364
  TCP    136.206.18.168:60053   Caher:8000             ESTABLISHED     6364
  TCP    136.206.18.168:60054   Caher:8000             TIME_WAIT       0
  TCP    136.206.18.168:60055   Caher:8000             TIME_WAIT       0
  TCP    136.206.18.168:60056   Caher:8000             TIME_WAIT       0
  TCP    136.206.18.168:60057   Caher:8000             TIME_WAIT       0
  TCP    136.206.18.168:60058   Caher:8000             ESTABLISHED     6364
  TCP    136.206.18.168:60059   Caher:8000             ESTABLISHED     6364
  TCP    136.206.18.168:60062   136.206.217.118:epmap  ESTABLISHED     2448
  TCP    136.206.18.168:60063   136.206.217.118:49155  ESTABLISHED     2448
  TCP    136.206.18.168:60067   Caher:8000             ESTABLISHED     4192
  TCP    136.206.18.168:60068   Caher:8000             ESTABLISHED     4192
  TCP    136.206.18.168:60069   Caher:8000             ESTABLISHED     4192
  TCP    136.206.18.168:60070   Caher:8000             ESTABLISHED     4192
  TCP    136.206.18.168:60071   Caher:8000             ESTABLISHED     4192
  TCP    136.206.18.168:60072   Caher:8000             ESTABLISHED     4192
  TCP    136.206.18.168:60073   Caher:8000             ESTABLISHED     4192
  TCP    136.206.18.168:60074   Caher:8000             ESTABLISHED     4192
```

The first commands shows the open connections prior to loading ww.dcu.ie the second shows the open connections after loading dcu.ie therefor the difference between the two are the connections opened as a result of loading dcu.ie.
Most listings are for 136.206.18.168 IP address which is a DCU owned IP Address.
Established – An active open connection

Close_wait – When the remote endpoint has closed the connection
Time_wait – indicated when the local endpoint has terminated the connection
These connections are being kept so that any delayed packets can be matched accordingly.

Netstat –r explained:
Netstat –r is a command used to generate the routing table for a system. It is used to determine routing information for both TCP and IP traffic. The below screenshot is the netstat –r command in use:

```
C:\windows\system32>netstat -r
===========================================================================
Interface List
  3...50 9a 4c 3d 94 7e ......Intel(R) Ethernet Connection (5) I219-V
  7...0a 00 27 00 00 07 ......VirtualBox Host-Only Ethernet Adapter
  6...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
  9...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0   136.206.18.254   136.206.18.168     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
     136.206.18.0    255.255.255.0         On-link    136.206.18.168    281
   136.206.18.168  255.255.255.255         On-link    136.206.18.168    281
   136.206.18.255  255.255.255.255         On-link    136.206.18.168    281
     192.168.17.0    255.255.255.0         On-link      192.168.17.1    291
     192.168.17.1  255.255.255.255         On-link      192.168.17.1    291
   192.168.17.255  255.255.255.255         On-link      192.168.17.1    291
     192.168.56.0    255.255.255.0         On-link      192.168.56.1    281
     192.168.56.1  255.255.255.255         On-link      192.168.56.1    281
   192.168.56.255  255.255.255.255         On-link      192.168.56.1    281
    192.168.179.0    255.255.255.0         On-link     192.168.179.1    291
    192.168.179.1  255.255.255.255         On-link     192.168.179.1    291
  192.168.179.255  255.255.255.255         On-link     192.168.179.1    291
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link    136.206.18.168    281
        224.0.0.0        240.0.0.0         On-link     192.168.179.1    291
        224.0.0.0        240.0.0.0         On-link      192.168.17.1    291
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      192.168.56.1    281
  255.255.255.255  255.255.255.255         On-link    136.206.18.168    281
  255.255.255.255  255.255.255.255         On-link     192.168.179.1    291
  255.255.255.255  255.255.255.255         On-link      192.168.17.1    291
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  1    331 ::1/128                  On-link
  7    281 fe80::/64                On-link
  3    281 fe80::/64                On-link
  6    291 fe80::/64                On-link
  9    291 fe80::/64                On-link
  3    281 fe80::45ec:747c:e05f:11ba/128
                                    On-link
  7    281 fe80::c10f:6383:741:170f/128
                                    On-link
  6    291 fe80::f8f6:2dcc:4970:dc24/128
                                    On-link
  9    291 fe80::fca3:5ddb:7209:deae/128
                                    On-link
```