**REPORT**

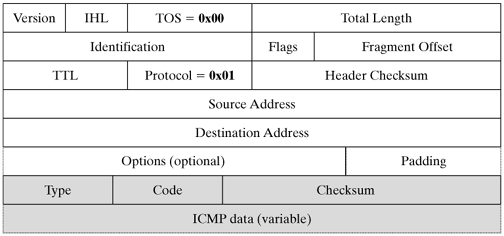
Ping Command- ICMP echo request/reply

# Introduction

ICMP stands for Internet Control Message Protocol. It is used to enhance the reliability which provides information about errors, loss of packets, unavailable destinations, etc. It is documented as **RFC 792**. It is mandatory that every device that implements IP (Internet Protocol), must also implement ICMP.

We have been using IP addresses for communication and IP is an unreliable datagram service. IP packets are incapable of sending error messages if anything goes wrong in the network, like sending a letter to a destination and the letter not getting received at the desired destination and you will never come to know about it. So, to handle this kind of issue an IP has an assistant called ICMP (Internet Control Message Protocol).

In ICMP any destination or router that detects any problem in handling a received IP packet, generated ICMP message addressed to the originating station of IP packet. ICMP message can be analysed by network management systems to generate network reports for the network administrators.



IP packet containing ICMP

ICMP messages are send as IP packets. The protocol field of IP header is set to **0x01 to indicate that this packet contains ICMP message.**

In this report, the use of ICMP for Request and Reply messages is illustrated.

# Concept of Request and Reply

In Request and Reply, Sender should send a request packet and get an ICMP reply packet either from the receiver or router along the way.

Request and Reply messages are used in different ways.

* Echo request and reply
* Router Solicitation and advertisement
* TimeStamp request and reply
* Network mask request and reply

Here, Echo request and reply are highlighted.

[ICMP](https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol) packets of echo request and reply are used to test the network layer of destination. In other words, the host at the destination is switched on or off. We can also check the network layer of all the devices on the way from sender to destination.

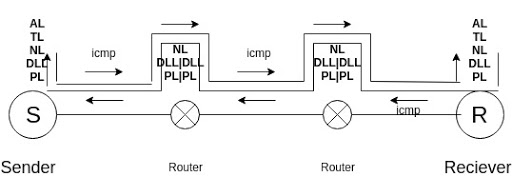


Figure:  Sender & Receiver sending and getting ICMP packets via network layer

In case, any network layer fails, the message will be discarded. ICMP packets are used at the network layer whenever we send an echo request. At the application layer, this echo request will never appear. So, no one will find out that there is actually a packet sent. Because of these, various attacks are possible. Generally, in our computer systems, the program called Ping (Packet Internet Groper) is implemented using echo request and reply.

# Observation

The different ICMP message types are:

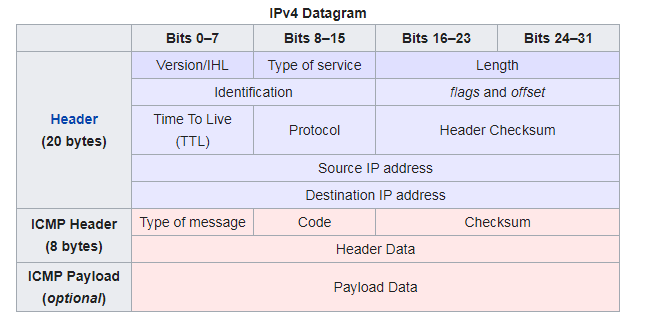
|  |  |  |
| --- | --- | --- |
| **ICMP Type** | **ICMP Code** | **Description** |
| 0 | 0 | Echo Reply (used by ping) |
| 3 | 0 | Destination Network Unreachable |
| 3 | 1 | Destination Host Unreachable |
| 3 | 3 | Destination Port Unreachable |
| 8 | 0 | Echo request (used by ping) |
| 11 | 0 | TTL Expired (used by traceroute) |

Basic ICMP message consists of three fields —**type, code and checksum (used for error detection).** Extension field is used with some of the messages.

**A) type field:**Specifies the message type (Ex: Destination unreachable)

**B) code field:** Describes the type (Ex: reason why the destination was unreachable)

When an IP packet containing ICMP echo request. (Type 8) is sent to a host, the host returns IP packet with ICMP echo reply (TYPE 0).



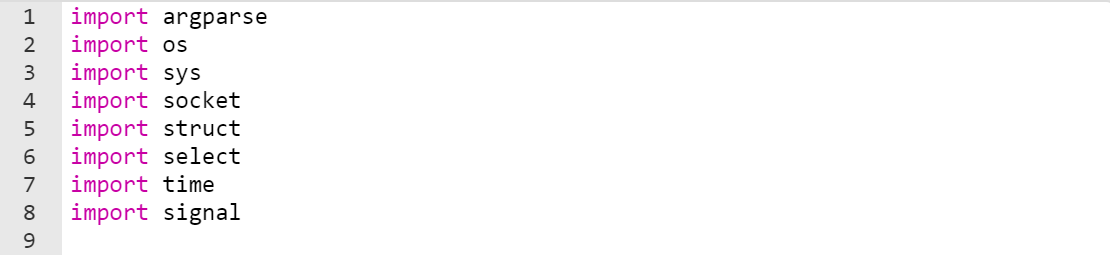
The payload of the packet is generally filled with[**ASCII**](https://en.wikipedia.org/wiki/ASCII) characters, as the output of the tcpdump command shows in the last 32 bytes of the following example (after the eight-byte ICMP header starting with 0x0800).

Ping **(**packet internet groper): It is **an application of ICMP echo**. It is used for estimation of round-trip delay, packet loss, and other parameters, Delay is measured by starting a timer at the time of sending the echo request and nothing the time when echo is received. Several PINGs are sent one after the other and round-trip time is expressed as minimum, maximum and average values.

Packet loss is estimated based on number of echo replies not on received. If out of 1000 echo requests, only 900 are replied to, the packet loss is 1%.

# Code & Explanation

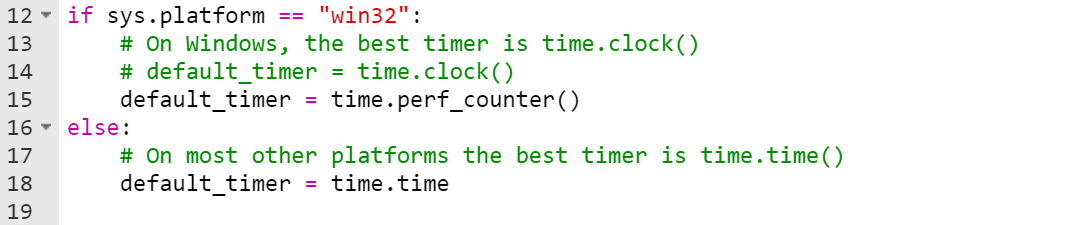
Importing the required libraries:



This Python program is for the implementation of ICMP echo request and reply using raw sockets.



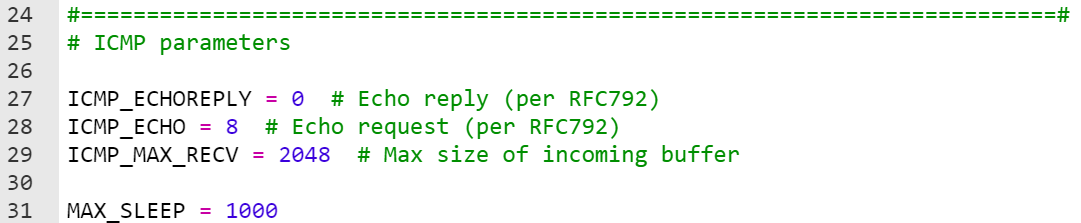
Defining the timer based on the architecture of the system:



Here, the sender is supposed to send out 2 ICMP requests constantly with the length of 256 bytes; given as:



Defining the ICMP parameters:



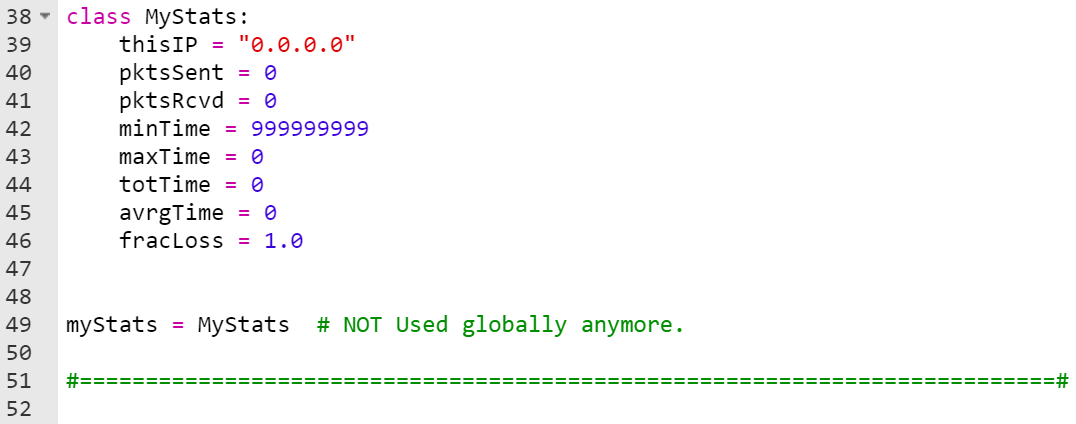
Defining the files to write the requests and replies to:



Opening the files in append mode for appending the messages on the respective text files:

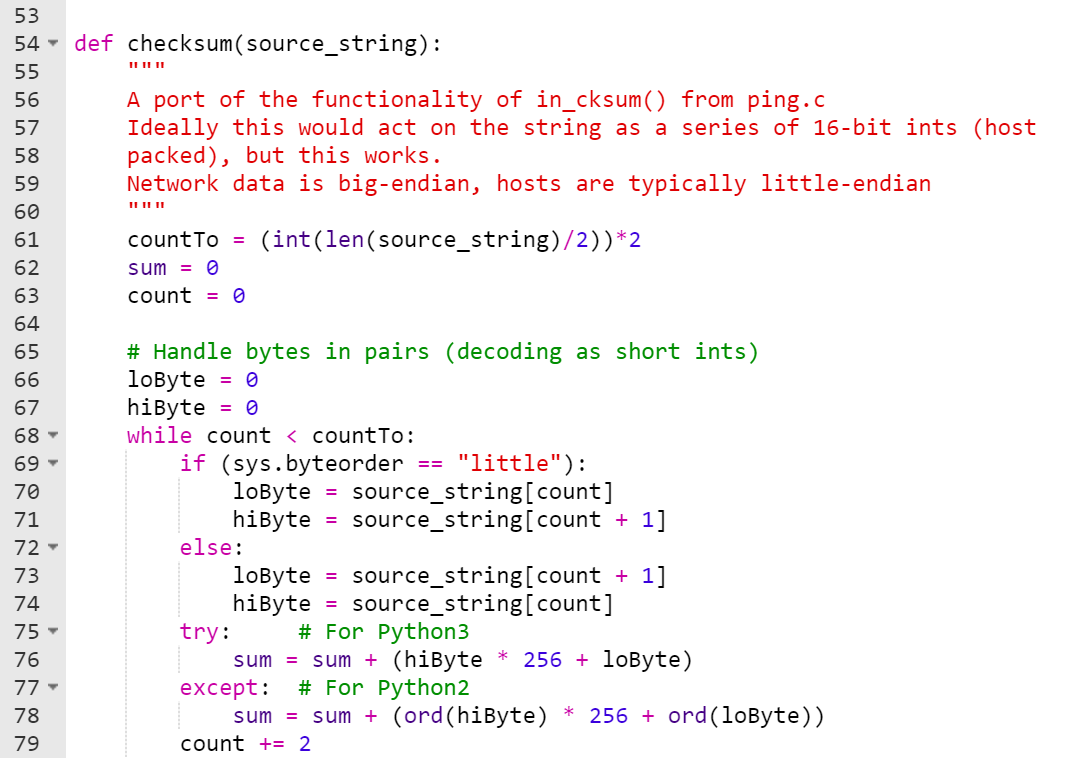


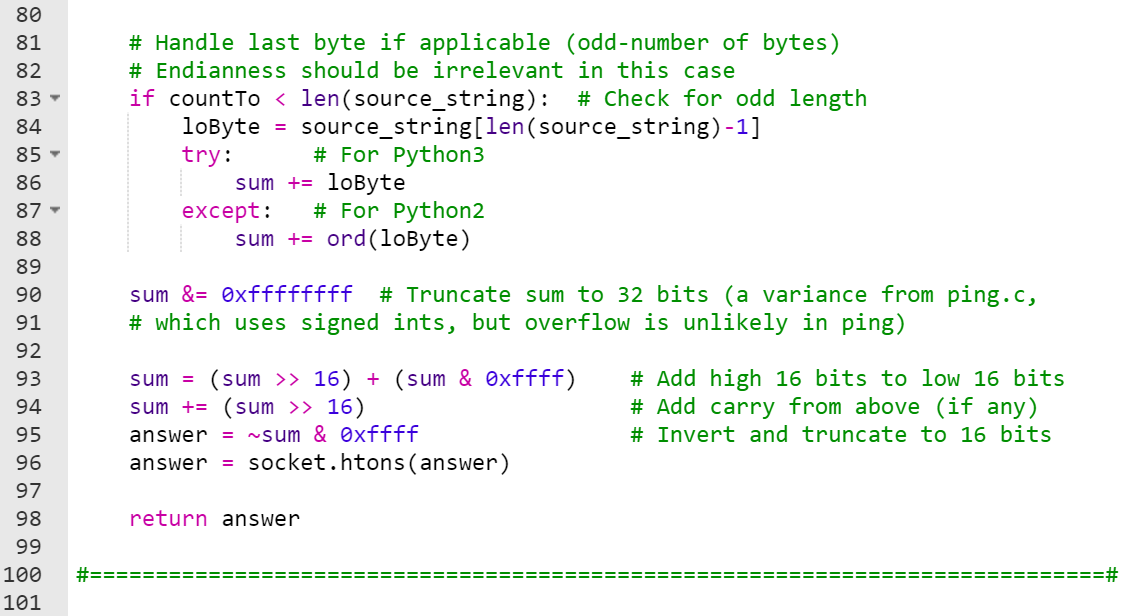
Defining the MyStats class for the statistics of the message exchange to be proceeded further in the program:



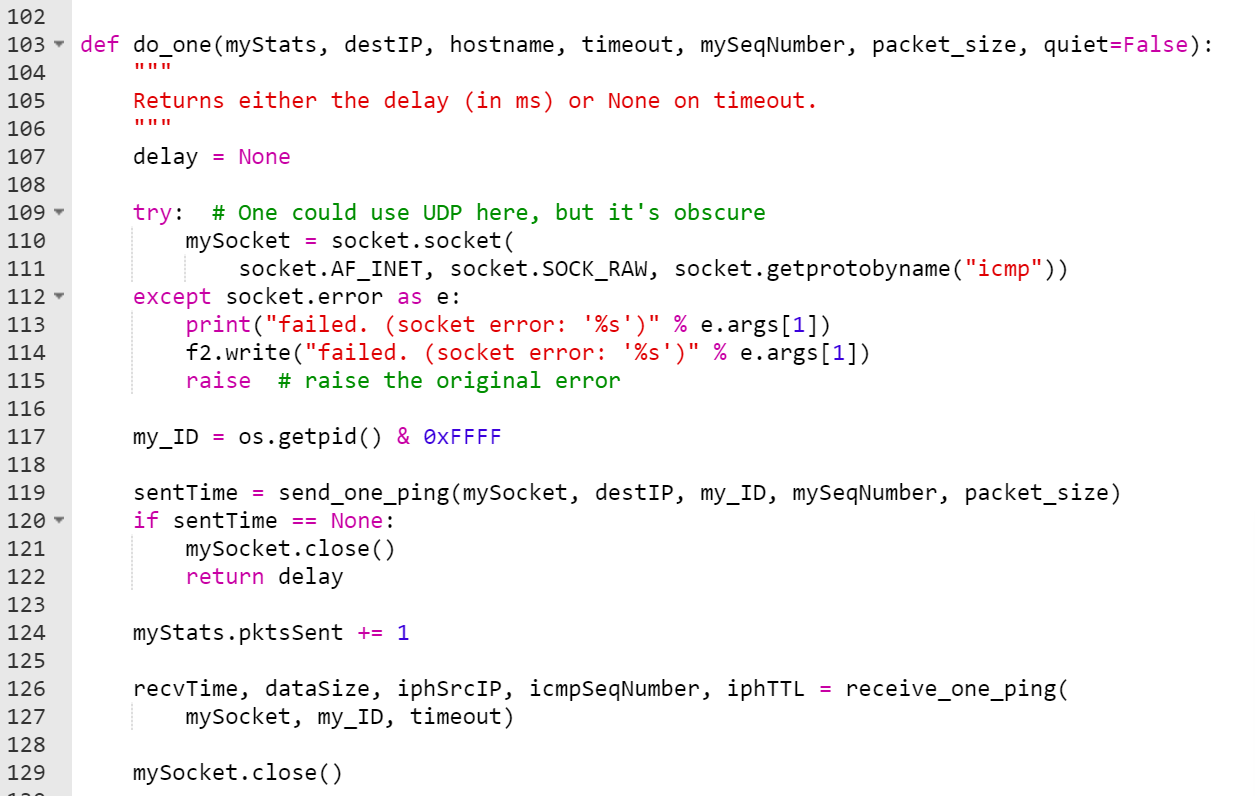
The checksum verifies the validity of the ICMP header. When the data packet is transmitted, the checksum is computed and inserted into this field. When the data packet is received, the checksum is again computed and verified against the checksum field. If the two checksums do not match then an error has occurred.

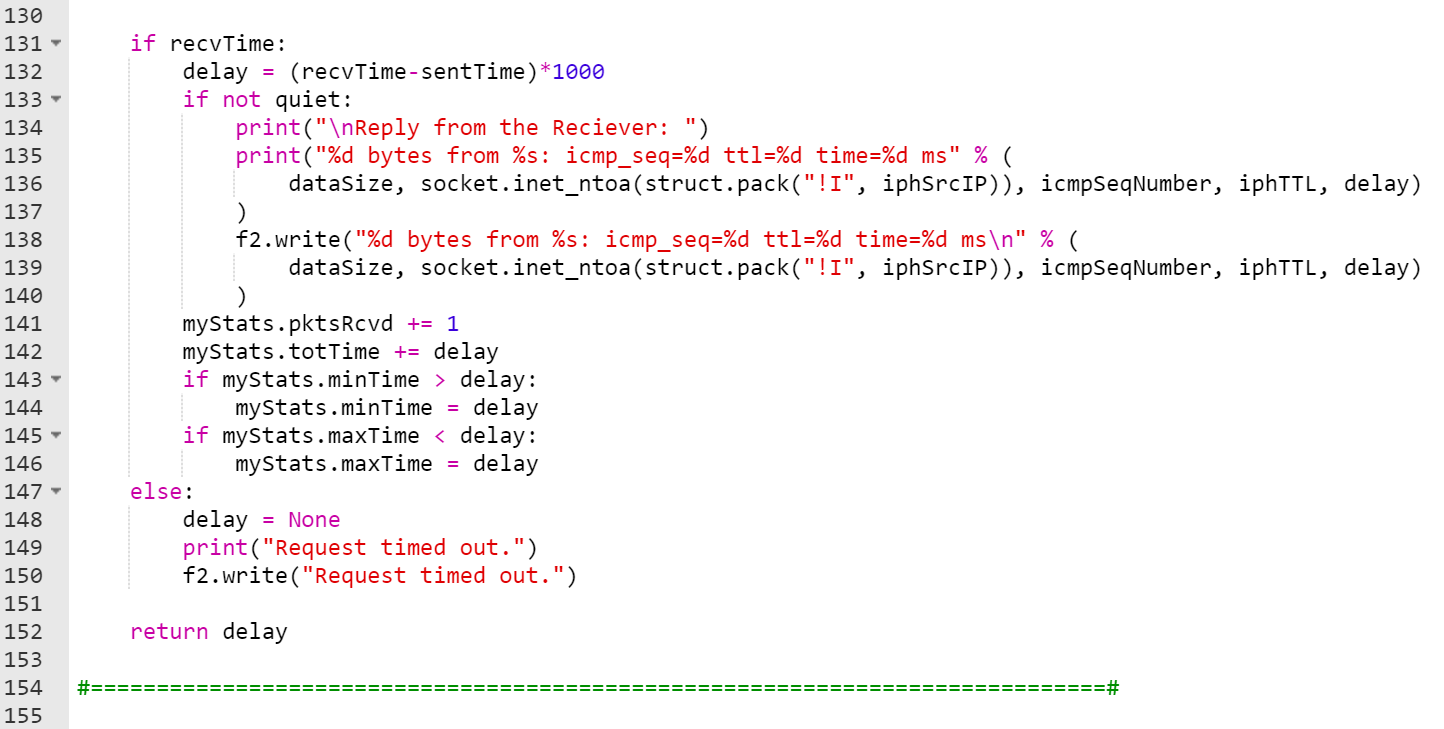
Defining the checksum function:



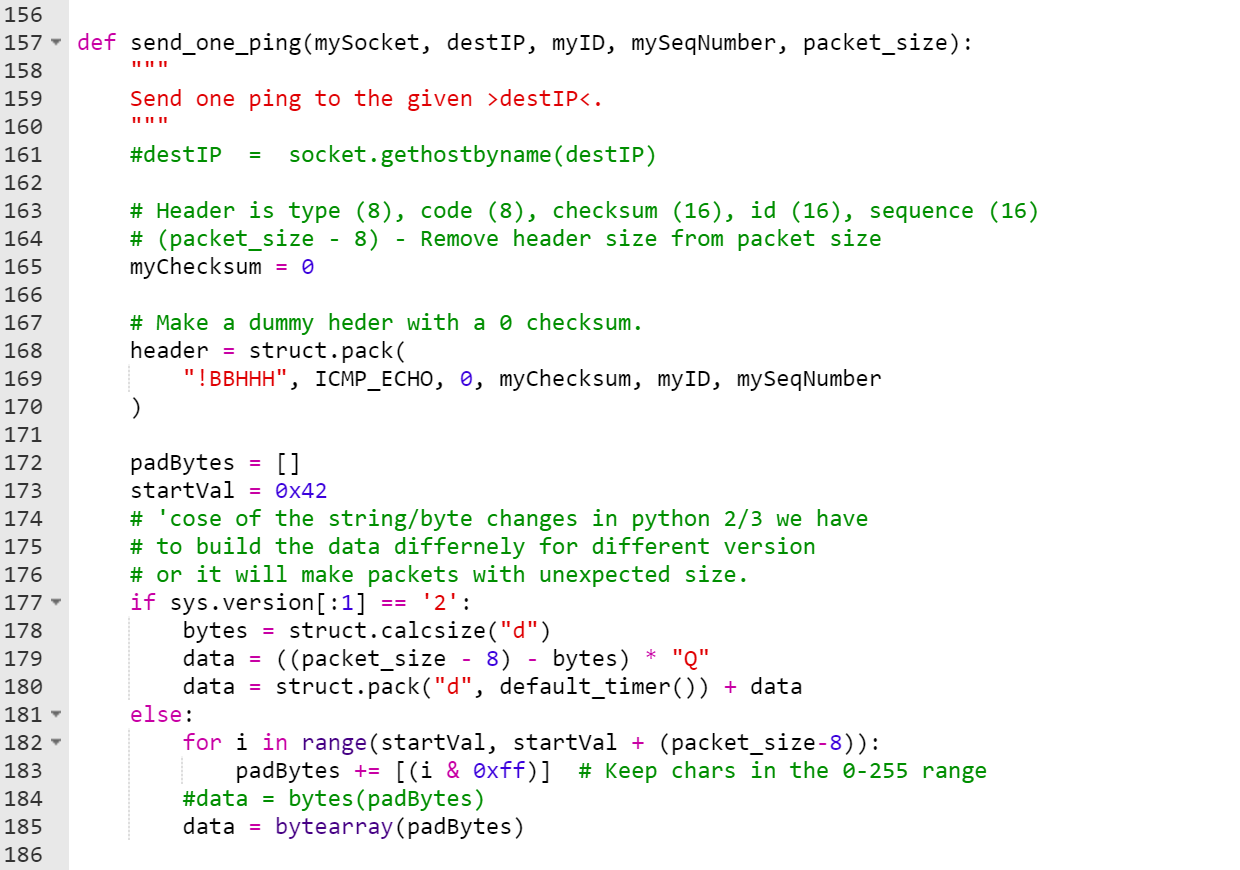


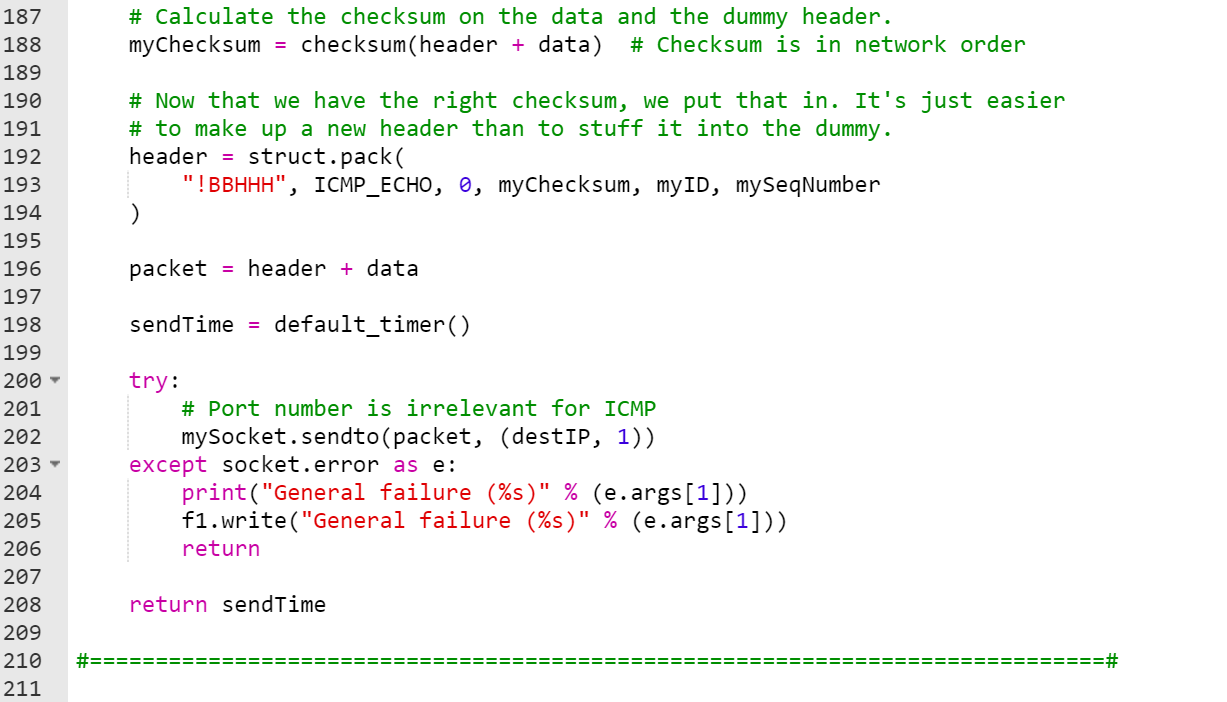
Checking for delay (in ms) or None on timeout:





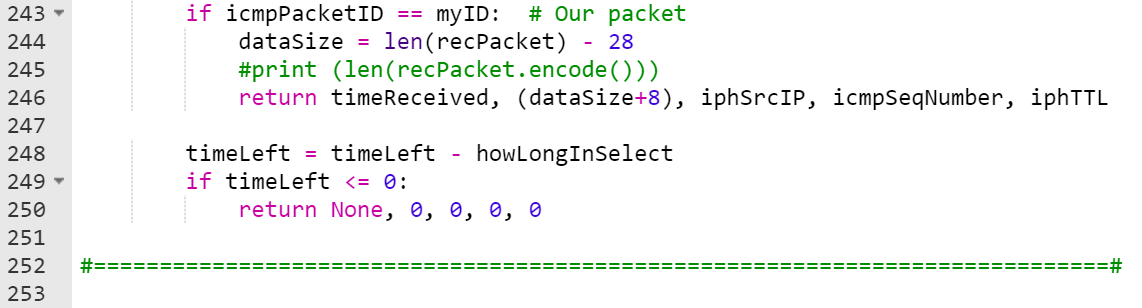
Now, lets ping the destination IP address:



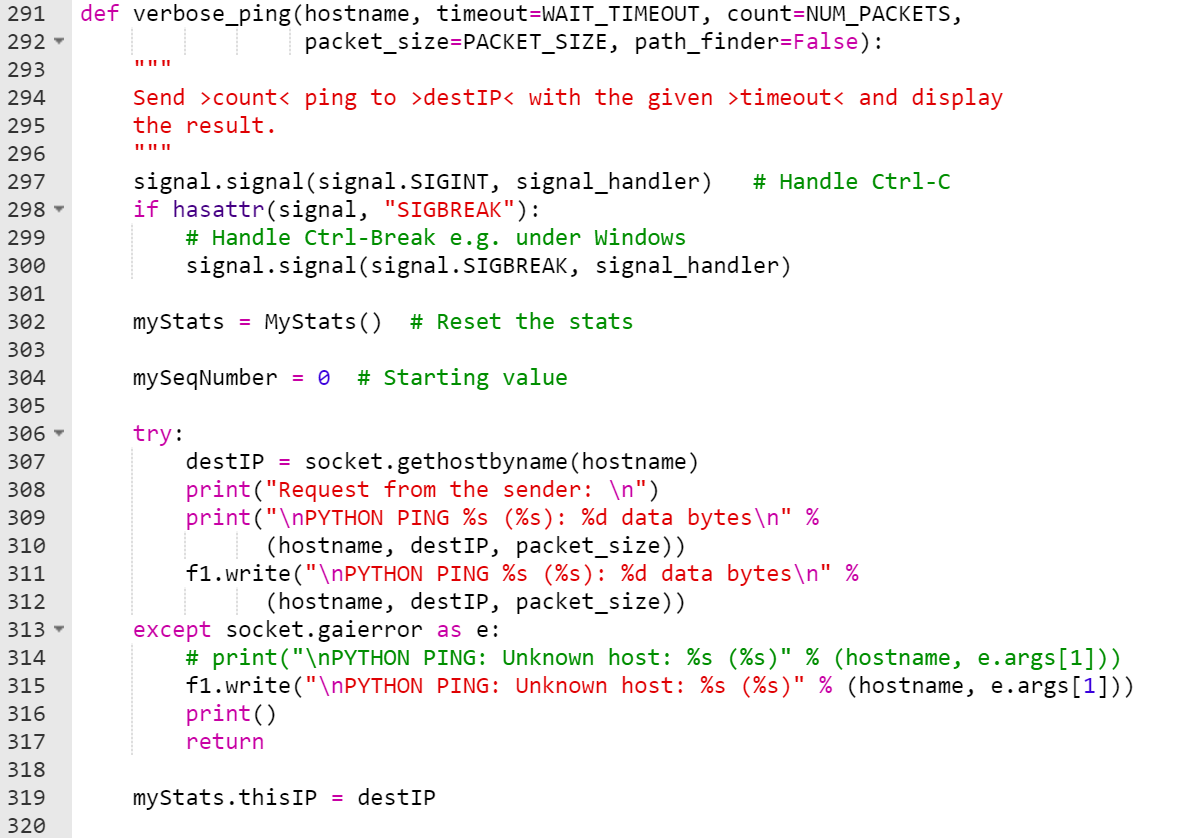


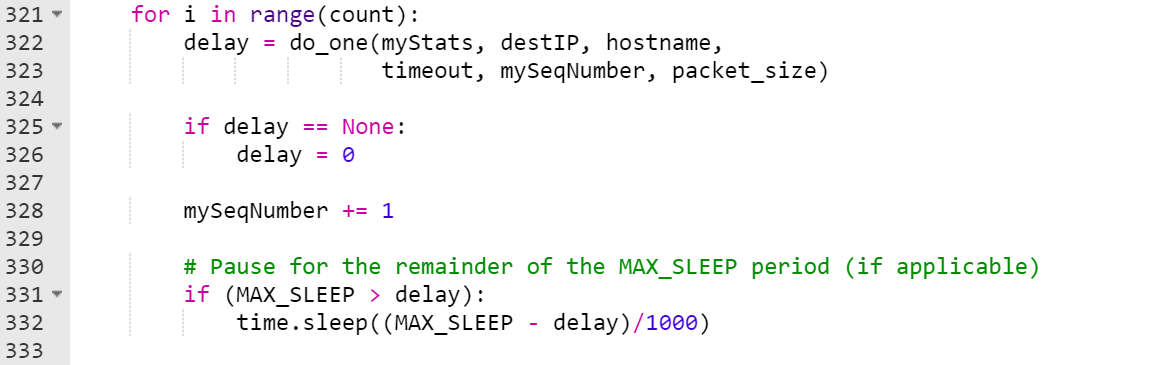
On the other end, receiving the ping from the socket:



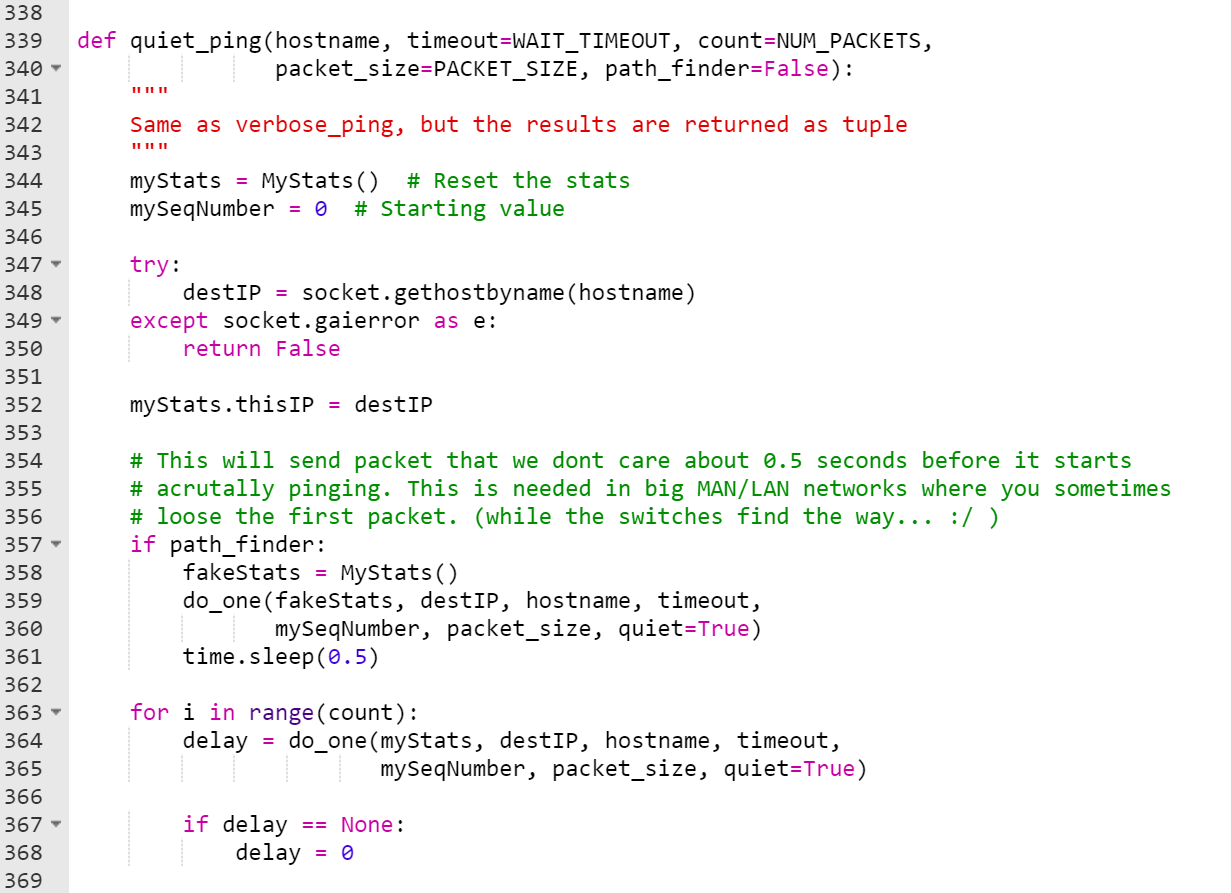


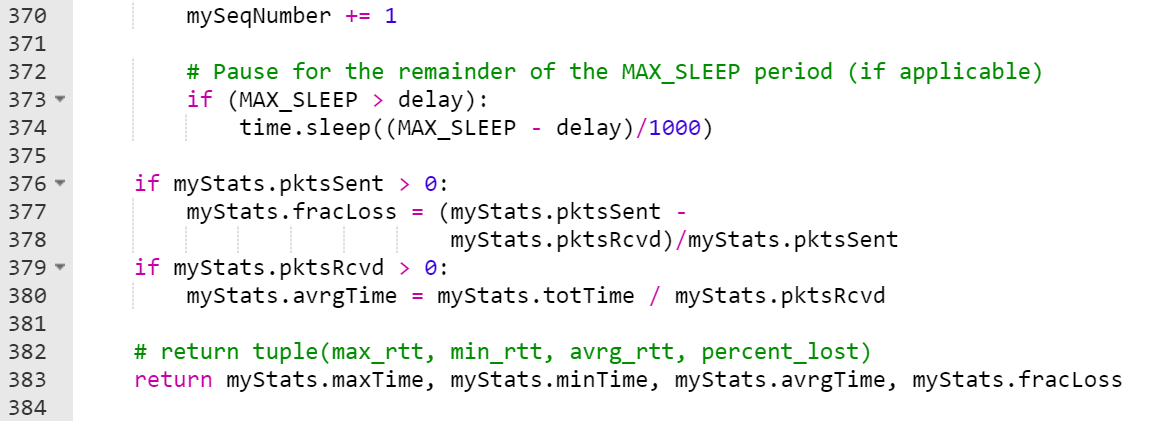
Now, the main function occurs here. Sending out 2 ICMP requests constantly with the length of 256 bytes to the destination IP address and the receiver sends back replies and print the requests (messages, not the statistics) it receives from the sender to a requests.txt file:



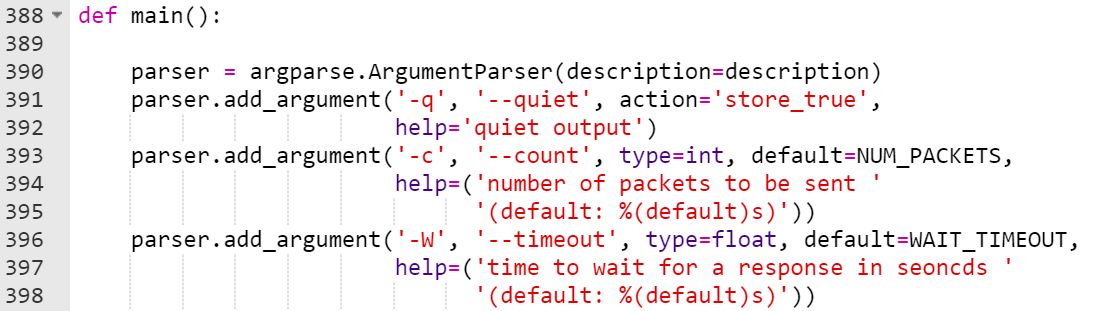


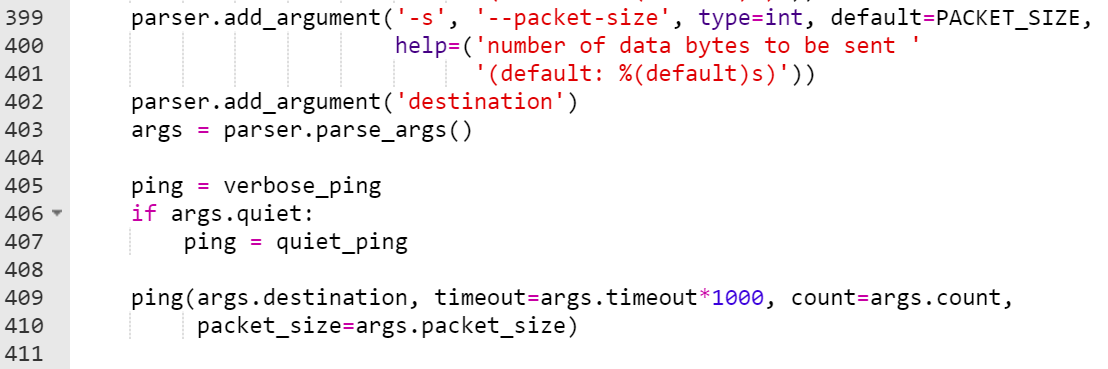
The sender receives replies, it prints the reply messages (not the statistics) on the screen and in a reply.txt file as well:



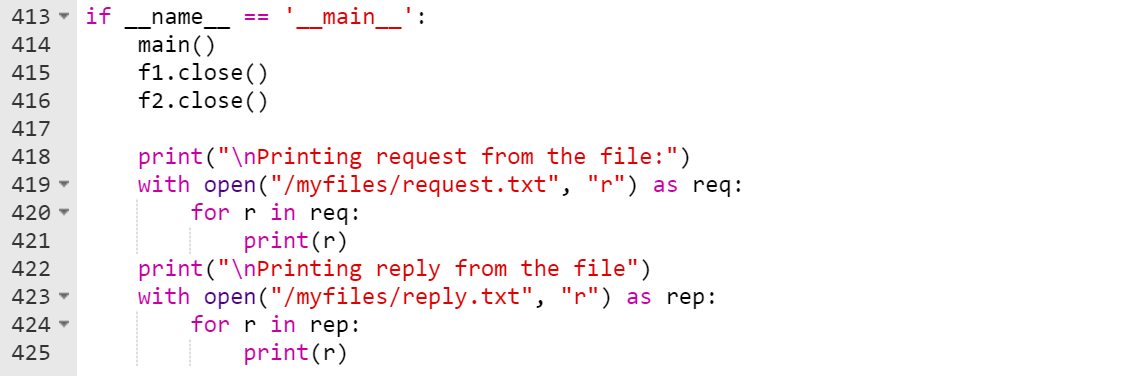


Finally, calling the functions in the main function for the implementation of ICMP echo request and reply:

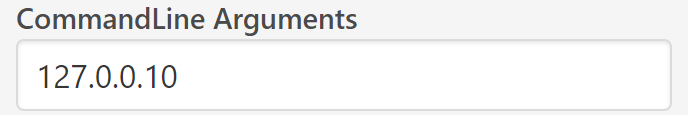




Finally:



Here, the destination IP address given as input is:



# Output screenshot:

