1. How you will match ICMP responses with the probes you are sending out (list all ways you could think of in your report and use the one that you found to work for you).
2. We could choose a port number for the header of the UDP datagram. Then when we receive the ICMP response we can extract the port number out of the header for the UDP datagram and compare it with the one we sent out. This is the one that I used.
3. We could look at the payload and check to see if the first x number of characters in the payload match with what we sent out similar to a checksum
4. We could look at the length field from the UDP header and compare that with the actual result.
5. List all possible reasons you can think of for not getting the answer when probing an arbitrary host:
   1. The website might not be up at the time. So the packet just gets lost
   2. The ICMP message gets lost or dropped due to server congestion.
6. I’m replacing a few sites from my list because they are not responding to the traces.
   1. [www.booking.com](http://www.booking.com) will become [www.google.com](http://www.google.com)
   2. [www.yelp.com](http://www.yelp.com) will become [www.amazon.com](http://www.amazon.com)
   3. [www.onet.pl](http://www.onet.pl) will become [www.facebook.com](http://www.facebook.com)
   4. [www.drom.ru](http://www.drom.ru) will become www.Wikipedia.org