* Steps for installing ELK (Elasticsearch, Logstash, Kibana) in Ubuntu OS:

1. Open terminal and run the following command in the given order for installing Elasticsearch:
   1. wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add –
   2. sudo apt-get install apt-transport-https
   3. sudo apt-get update && sudo apt-get install elasticsearch
   4. sudo update-rc.d elasticsearch defaults 95 10
   5. sudo -i service elasticsearch start (for starting elasticsearch)
   6. sudo -i service elasticsearch stop (for stopping elasticsearch)
2. Open terminal and run the following command in the given order for installing Logstash:
   1. wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add –
   2. sudo apt-get install apt-transport-https
   3. sudo apt-get update && sudo apt-get install logstash
   4. sudo systemctl start logstash.service
3. Open terminal and run the following command in the given order for installing Kibana:
   1. wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add –
   2. sudo apt-get install apt-transport-https
   3. sudo apt-get update && sudo apt-get install kibana
   4. sudo update-rc.d kibana defaults 95 10
   5. sudo -i service kibana start (for starting Kibana)
   6. sudo -i service kibana stop (for stopping Kibana)

* Steps for running the ELK:

1. Go to the directory :- /etc/logstash/conf.d and paste the logstash config file there. User can change the location of input file from where to read the logs.
2. Restart logstash by running the command:- “sudo service logstash restart”.
3. Restart elasticsearch and kibana in the same way and open the browser and go to “localhost:9200”. It will start the kibana and logs can be seen there.

* Steps for running python code:

1. Copy the python code into an appropriate directory.
2. Install the pygeoip plugin following the instructions given in the code.
3. Change the location from where logs has to be read in the program and where output has to be updated.
4. Run the program using the following command:- “python3 ‘program-name’.py”