In this homework we will build on top of the work from Homework 4

1. Port your web server so it runs inside a container image under GKE
2. Requests for non-existent files should return a 404-not found status. Such erroneous requests should be logged to cloud logging.
3. Requests for other HTTP methods (PUT, POST, DELETE, HEAD, CONNECT, OPTIONS, TRACE, PATCH) should return a 501-not implemented status. Such erroneous requests should be logged to cloud logging.
4. Demonstrate the functionality of your app by using the provided http client to request a few hundred of your cloud storage files. Run your http client on a VM.
5. Use the curl command line utility to demonstrate the functionality of your app with respect to the 404 and 501 use cases
6. Use a browser to demonstrate one request for each of the aforementioned response status cases.
7. Use your previously created second app to track requests from banned countries. The US defines a list of countries (North Korea, Iran, Cuba, Myanmar, Iraq, Libya, Sudan, Zimbabwe and Syria) to which export of sensitive cryptographic material is prohibited. We will pretend that files stored in your storage bucket contain such materials. Your web server should communicate such “forbidden” requests to the second app which should print an appropriate error message to its standard output.
8. Run your second app on a VM.

What to turn in:

- The python code for your web server and app for monitoring banned countries as a github link. This should be mostly the same as what you created for homework 4.
- A pdf file describing all the necessary steps to configure and run your apps, screenshots of your curl work from step #6, and console views of your Kubernetes deployment.