In this homework you should create a collection of apps that accomplishes the following:

1. One app will consist of a cloud function that can accept HTTP GET requests from web clients. The app should be able to respond to requests for the files in your bucket that you created in homework 2 and return the contents of the requested file along with a 200-OK status
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
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. A second app should 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. The first app should return a 400 (permission denied) error, and communicate such “forbidden” requests to the second app which should print an appropriate error message to its standard output.
8. Your second app must run on your local laptop

What to turn in:

- The python code for your first and second apps as a github link
- A pdf file describing all the necessary steps to configure and run your apps, including screenshots of your browser work from step #6, and the contents of cloud logging for the erroneous requests.