**Assignment 4:** Tensorflow and Data Privacy

By

Rachael Joan Dias

0651897

Addressed to,

Professor Brian Srivastava

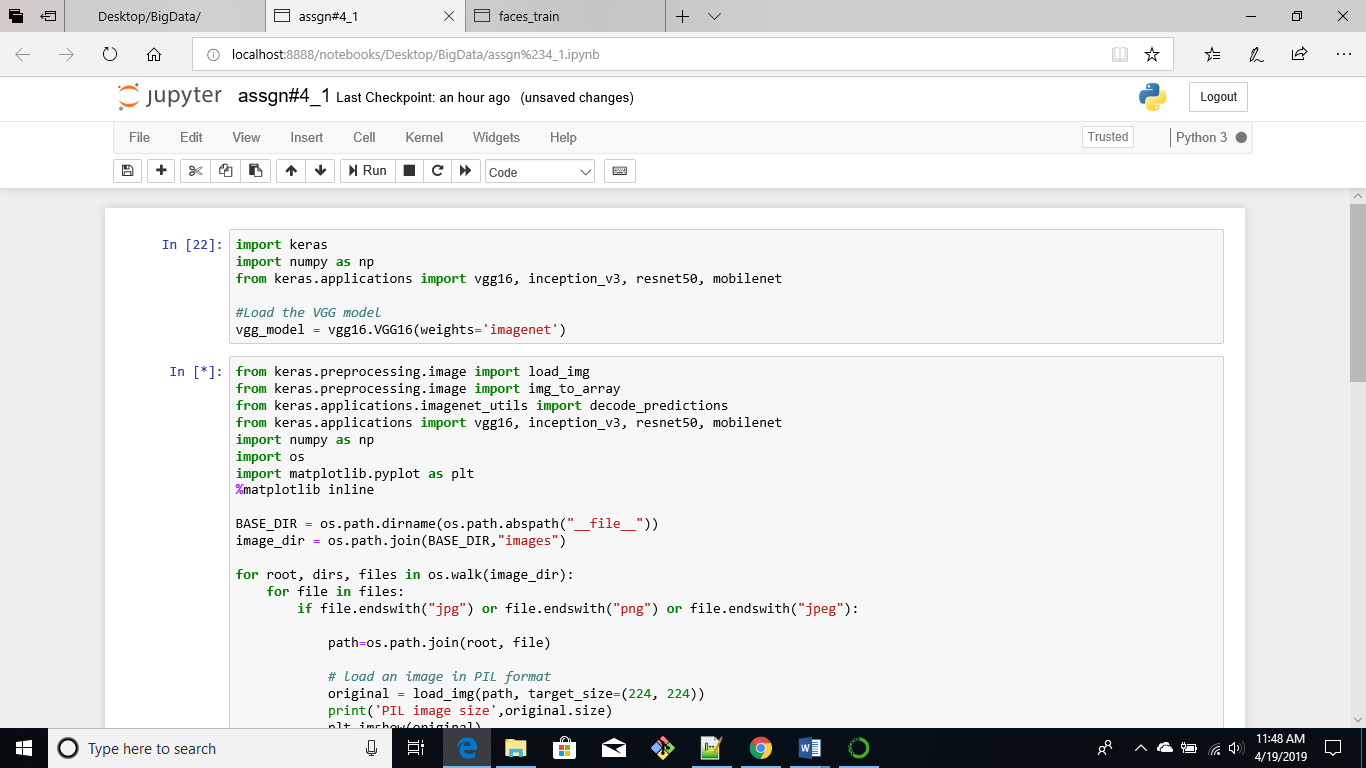
Trent University

AMOD-5410H-A-2019GW-PTBO Big Data

1. **Machine Learning Problems**

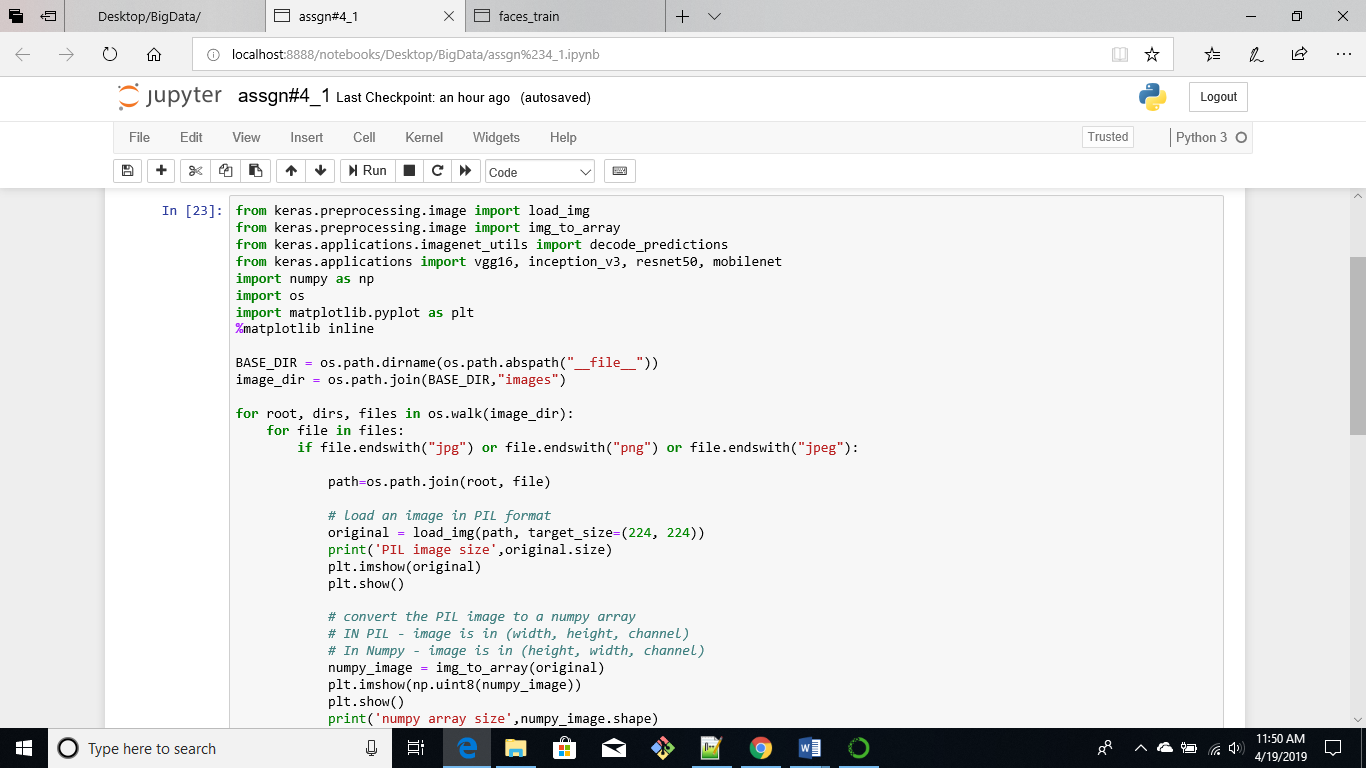
The Keras library contains several pretrained models, each model is broken into 2 parts, model architecture and pretrained weights, since the weights are very large the are not bundled with Keras. I used the VGG16 model and loaded ImageNet weights. ImageNet is a large database that contains 14 million images that belong to 20,000 classes [1].

We start by importing all the necessary libraries, from Keras we use the VGG model which we initialize by specifying imagenet weights.

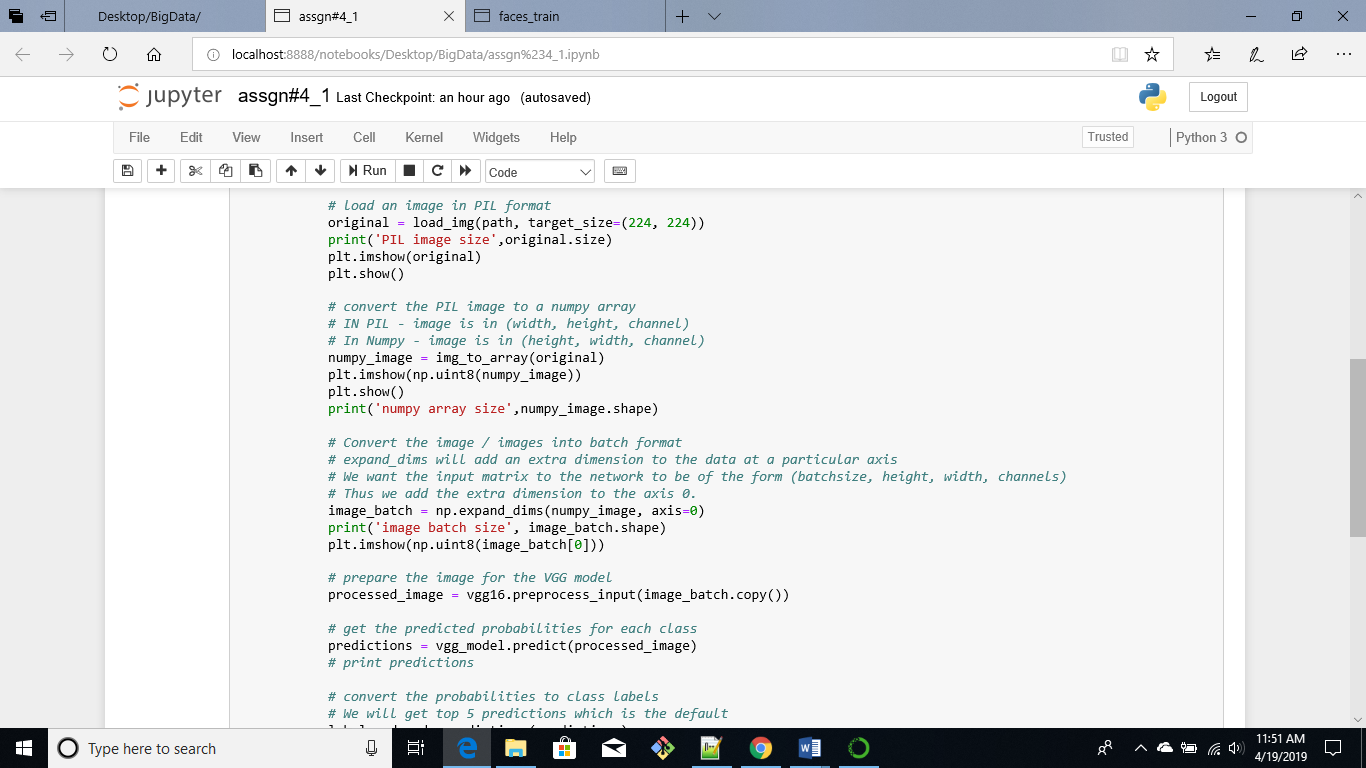


Next, we must load images and preprocess them so that we can apply them to the VGG model. We import all the preprocessing libraries from Keras, and other libraries such as numpy, os and matplotlib that are needed for converting the data to the right format and visualization

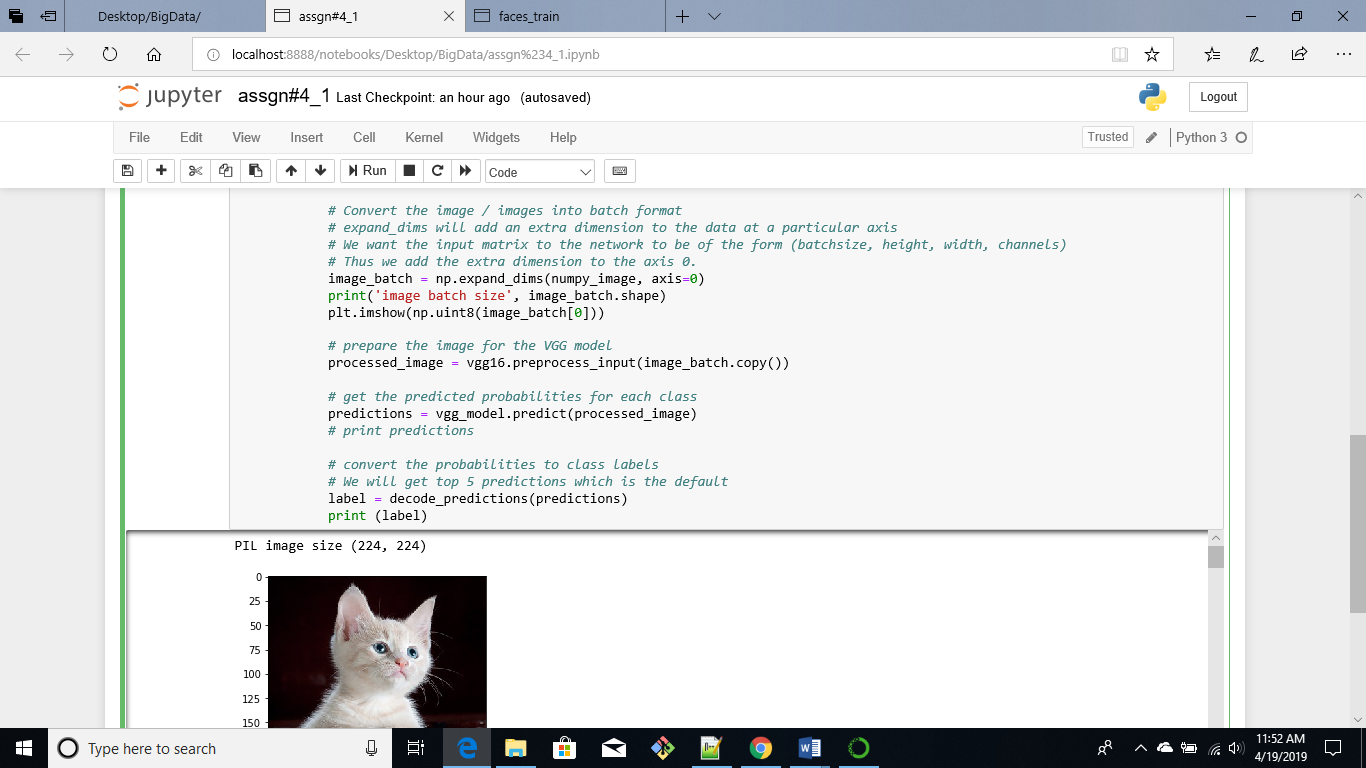
The os library helps us to read all the images that are saved in a folder. “BASE\_DIR” is the current working directory and within that directory we specify the directory “images” which contains all the images which we will use for our prediction. Using a for loop we iterate through all the .jpg, .png and .jpeg files that are present.



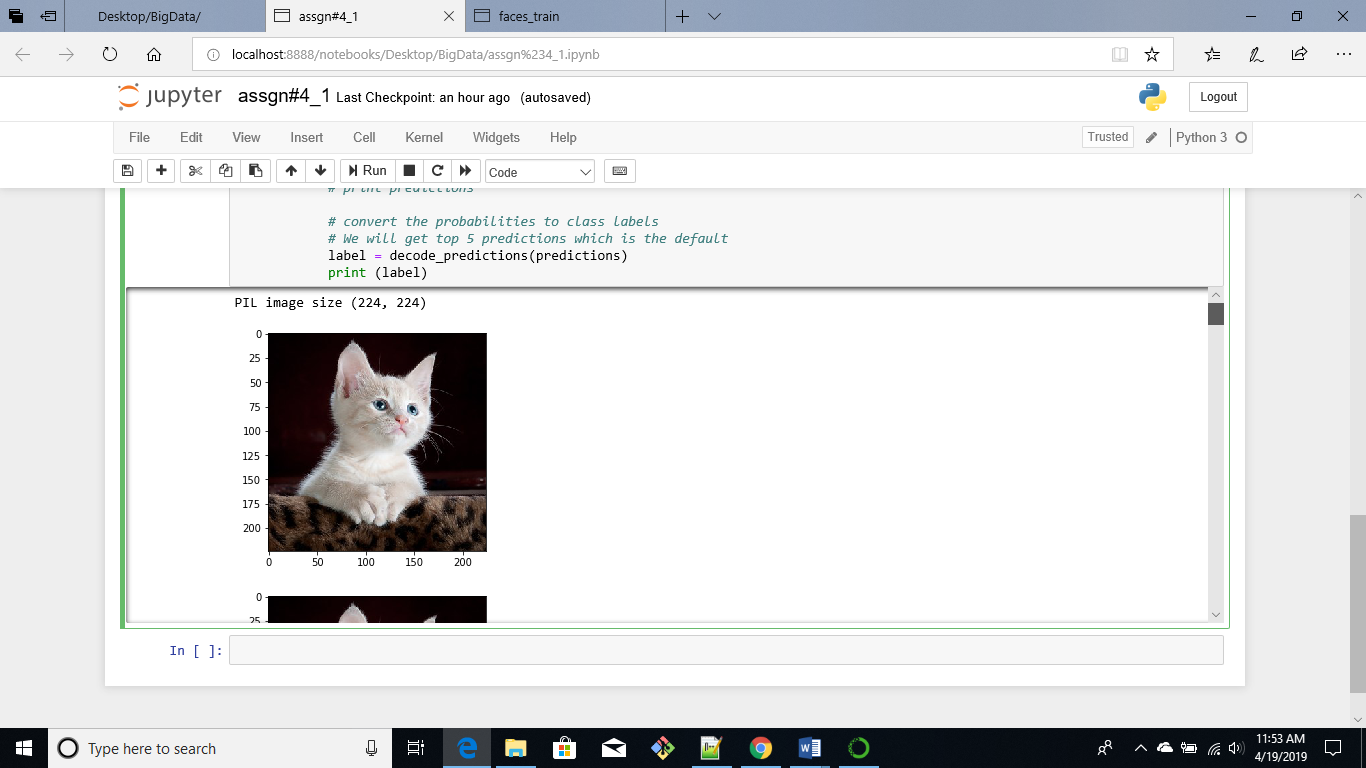
We use load\_img() to load the image, then we convert it into a size of 224x2244 and save it as the original image. In the next step we convert the image into a numpy array using the img\_to\_array() function. Since the network requries a 4-dimensional Tensor as input we convert the numpy array to batch format by adding an extra dimension to the image.

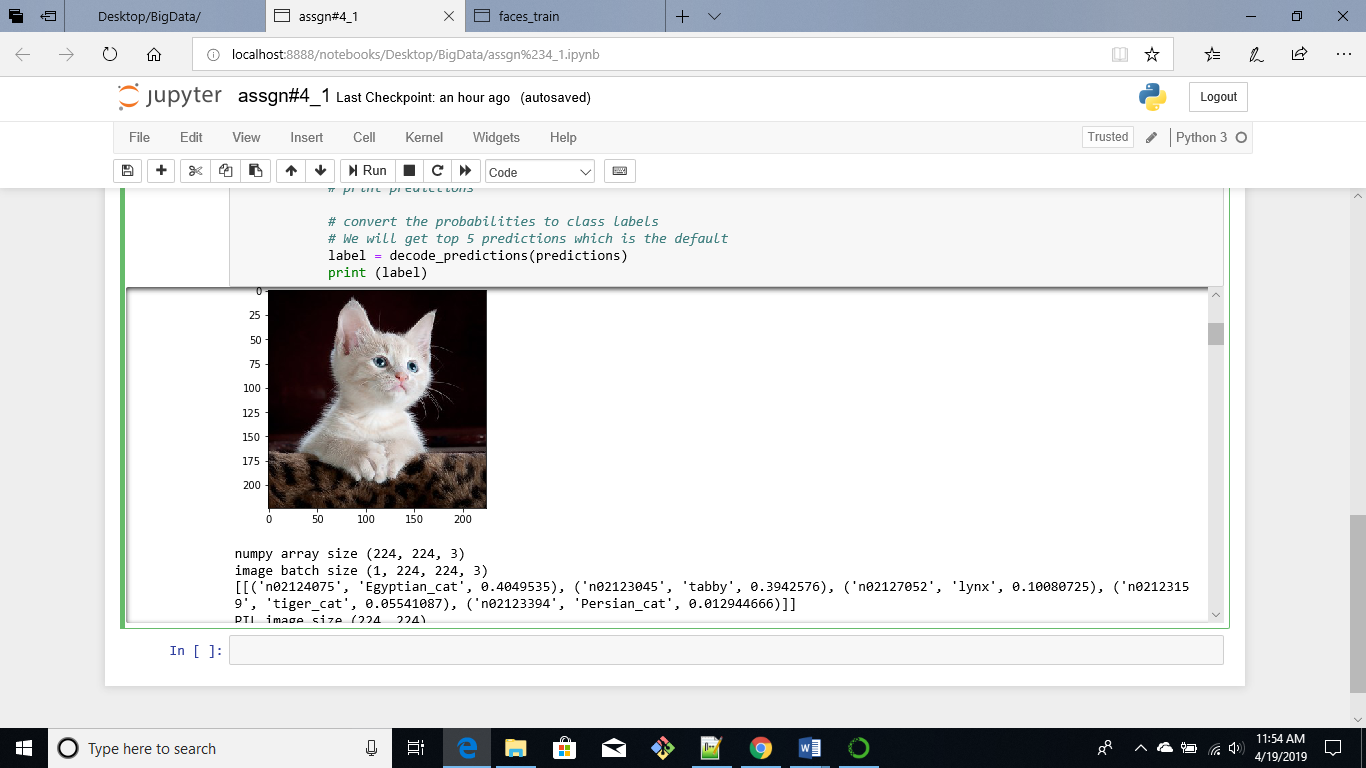


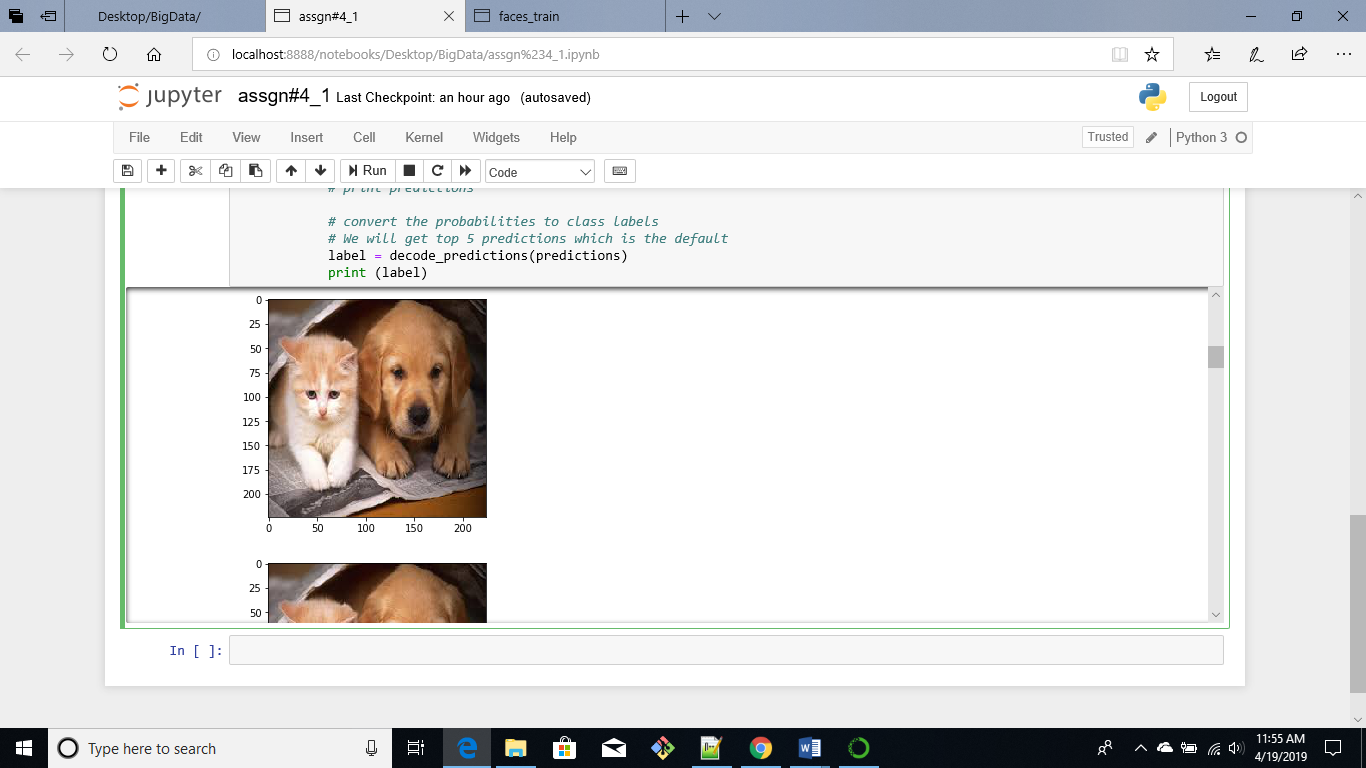
Once this is complete we pass the image to the vgg16 model by passing it to the preprocess\_input() function. Predictions can be made on the image, as the predictions returned are an array the decode\_predictions() function will give us the labels for each of the predictions



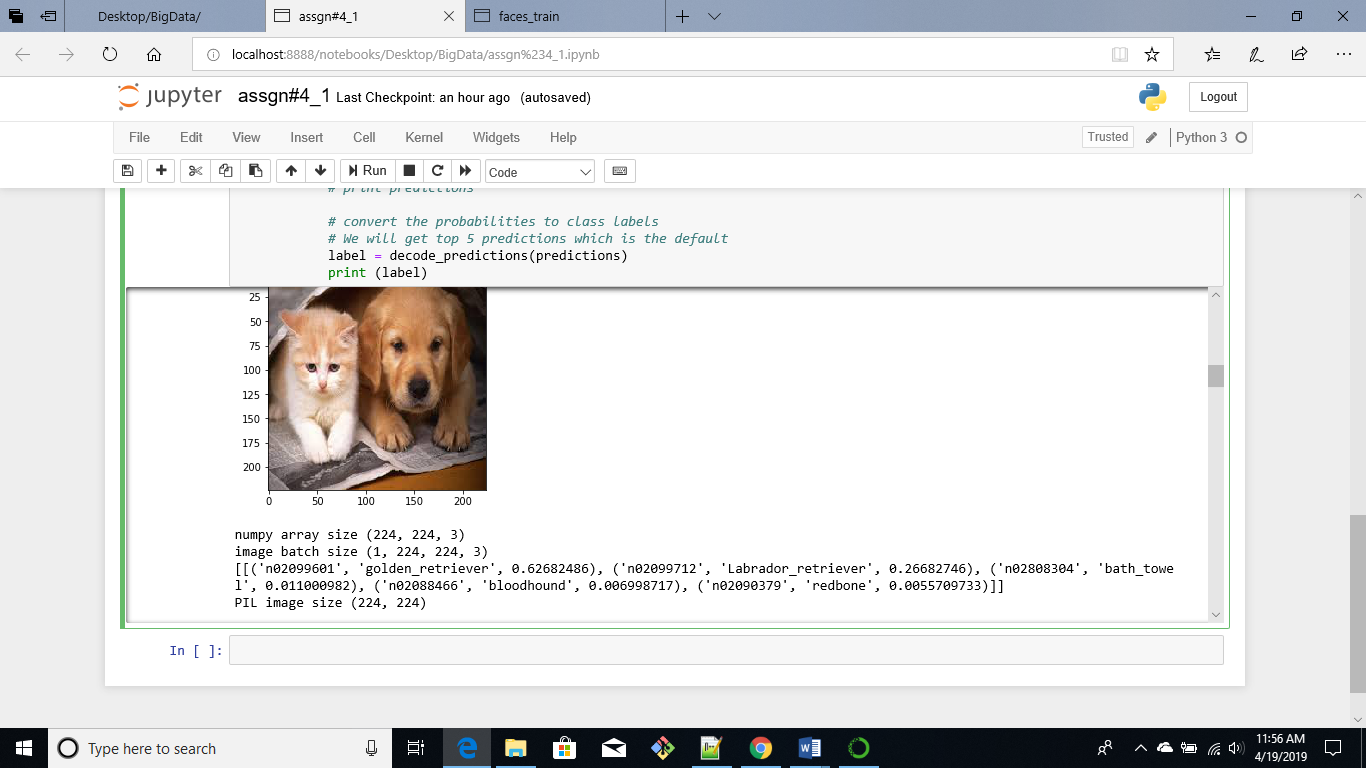
Below we can see the output image. The first image is in PIL format, the second image is the numpy array and finally we have the predictions for the image. The VGG16 model predicts that the cat looks like an Egyptian cat, tabby, lynx, tiger cart or Persian cat. Similarly, for all the other images the model makes a couple of predictions.



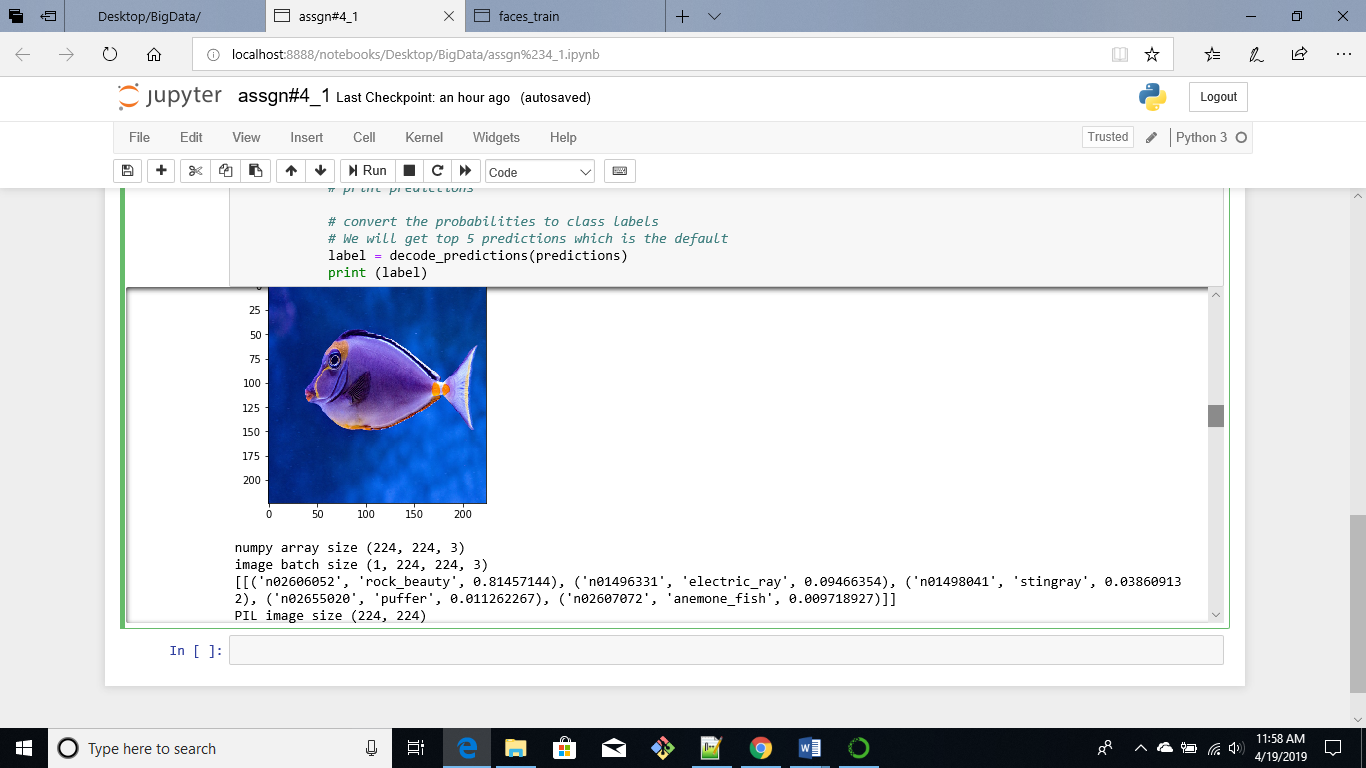




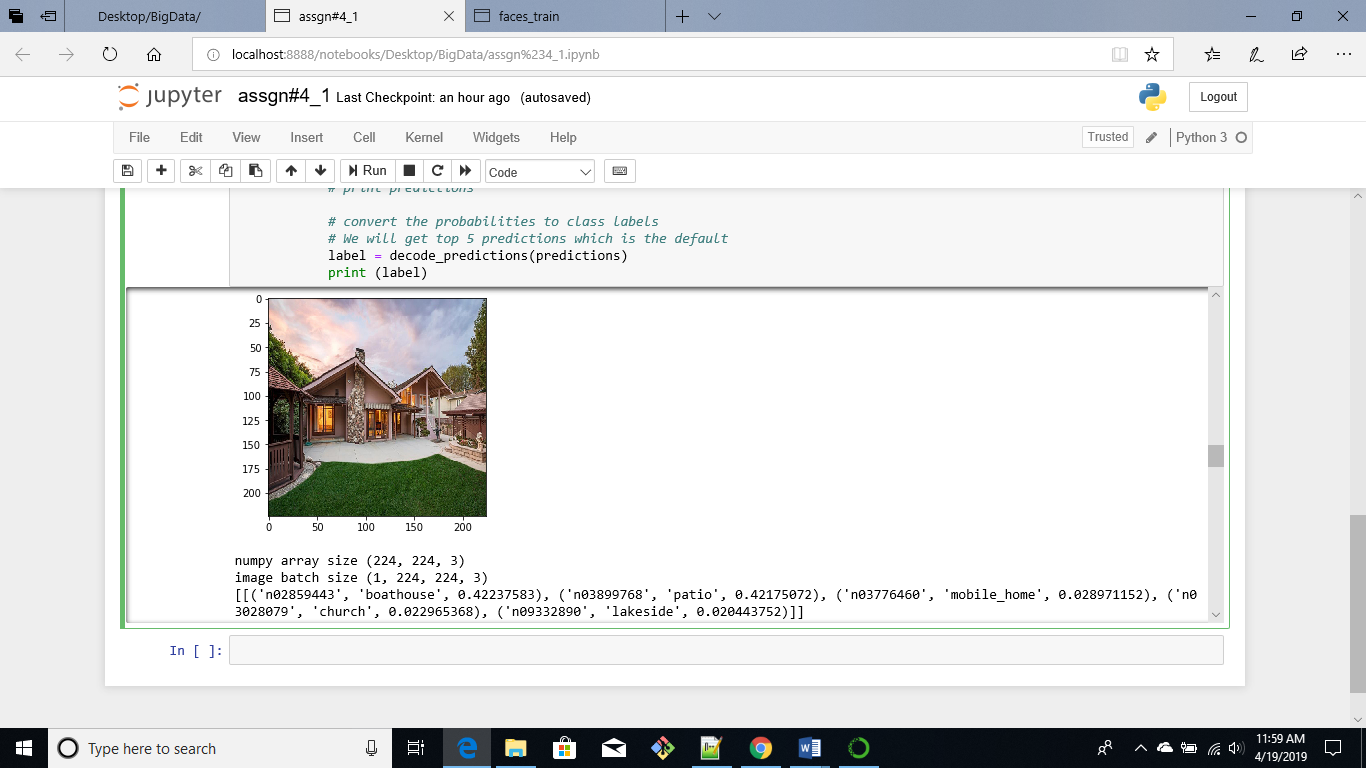
The model can detect the golden retriever from the image

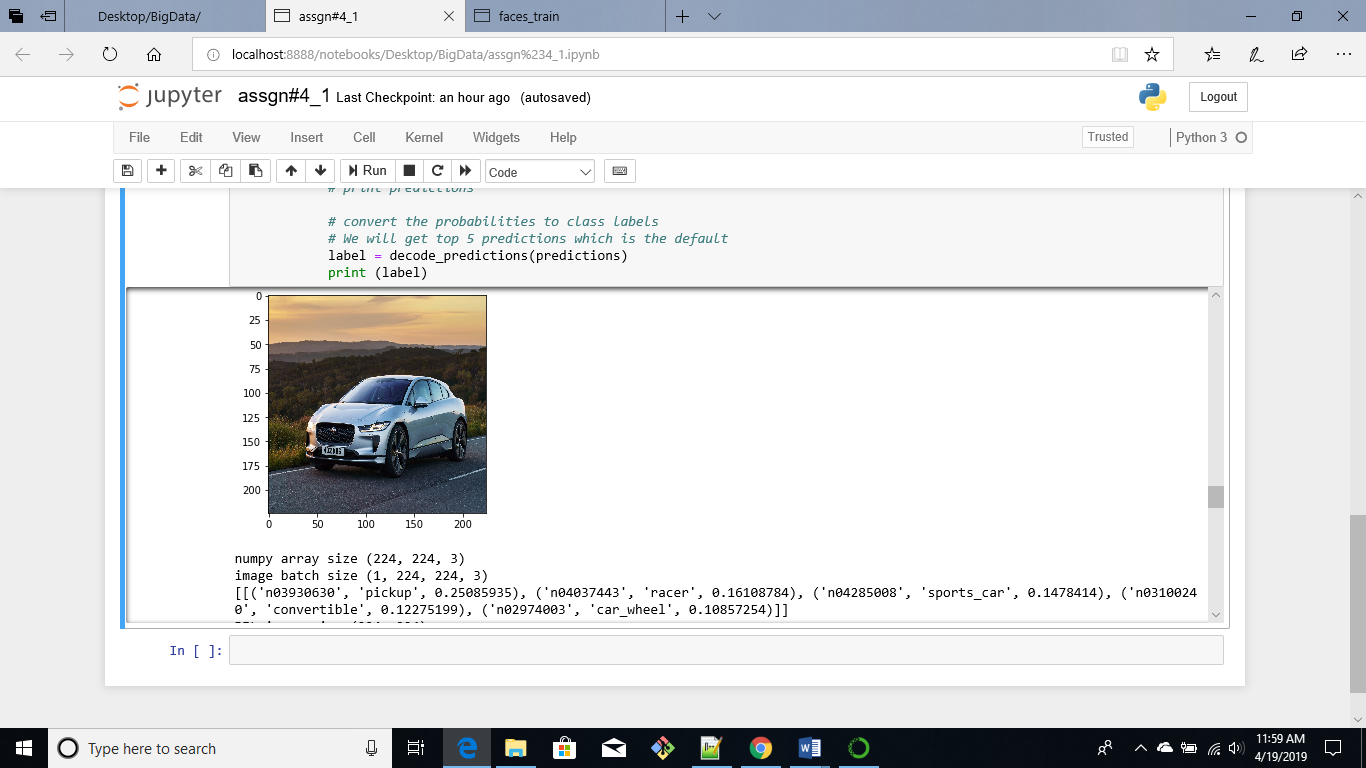


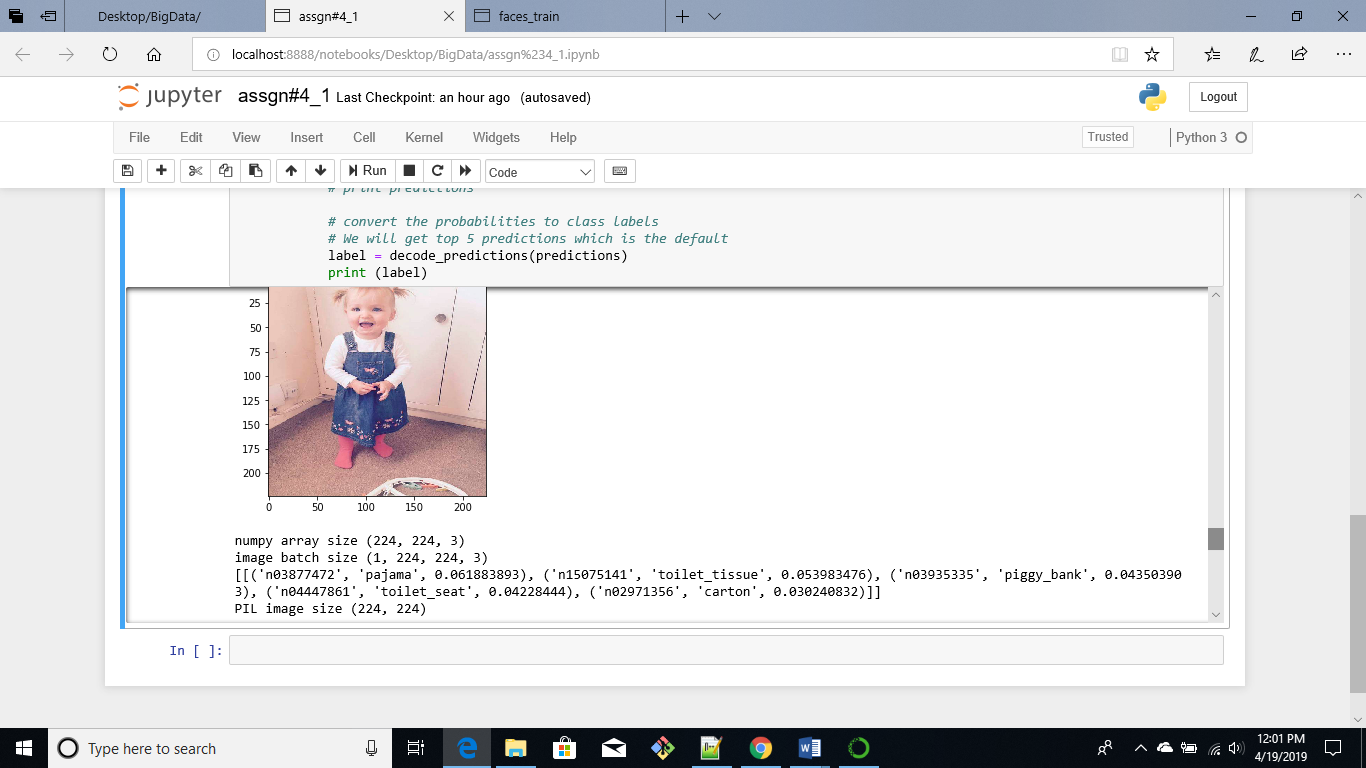
The model predicts that the fish looks like a puffer fish, anemone fish, stingray, electric ray and rock beauty fish



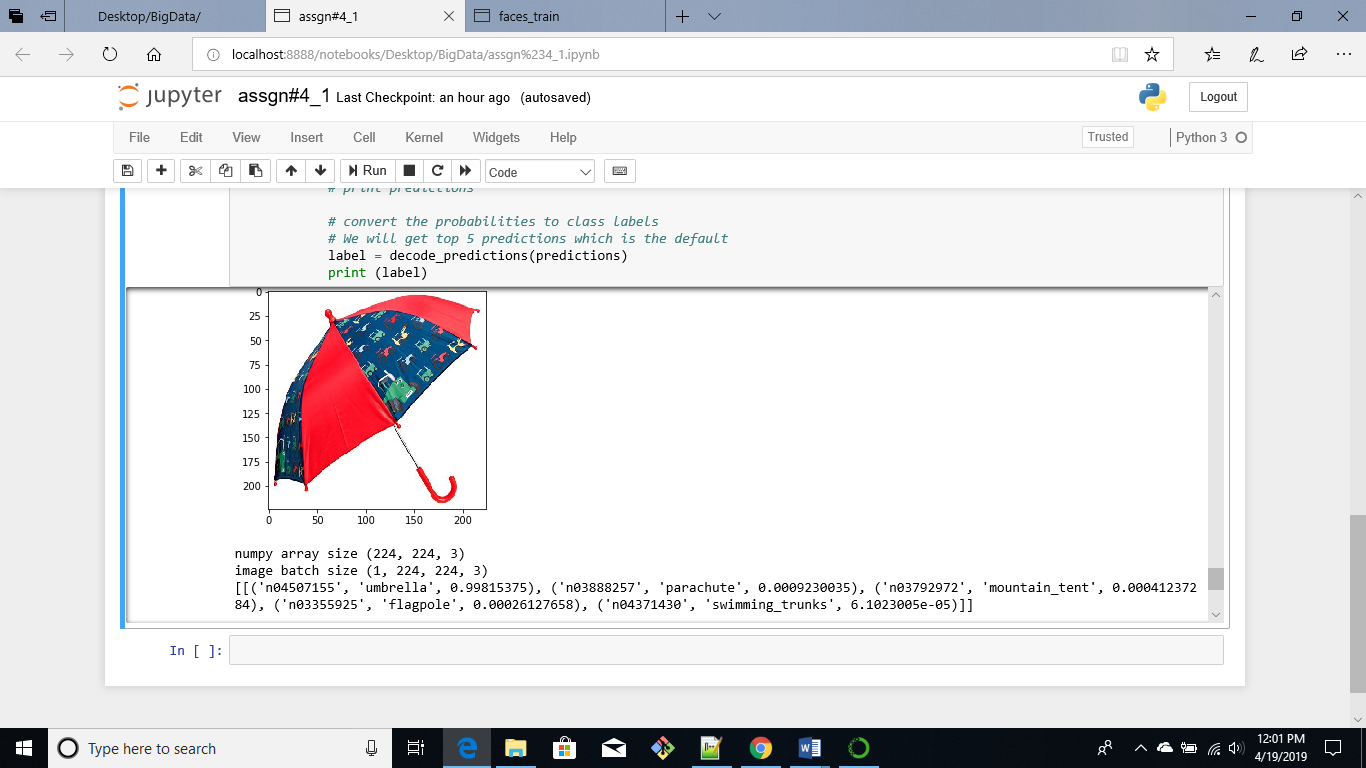
The model predicts that the image below looks like a boathouse







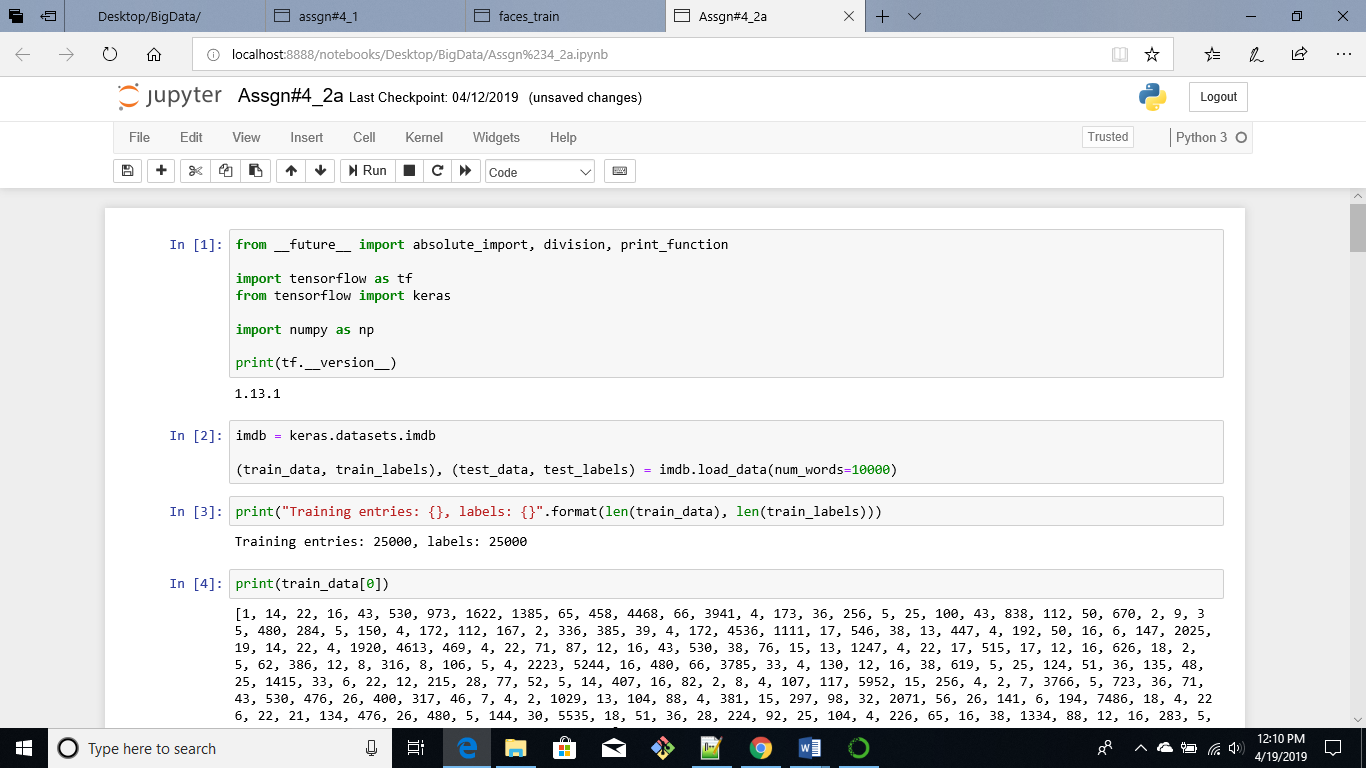
The first prediction for the image below is umbrella

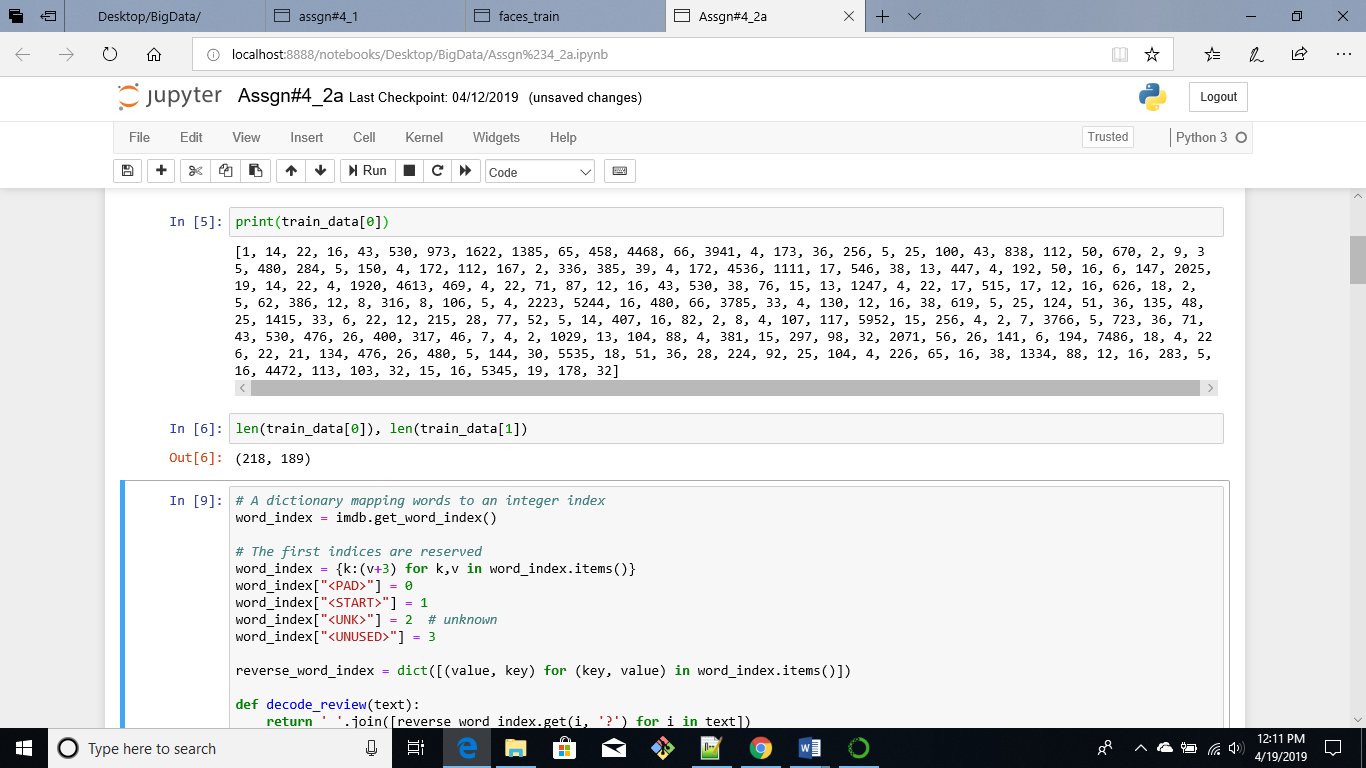


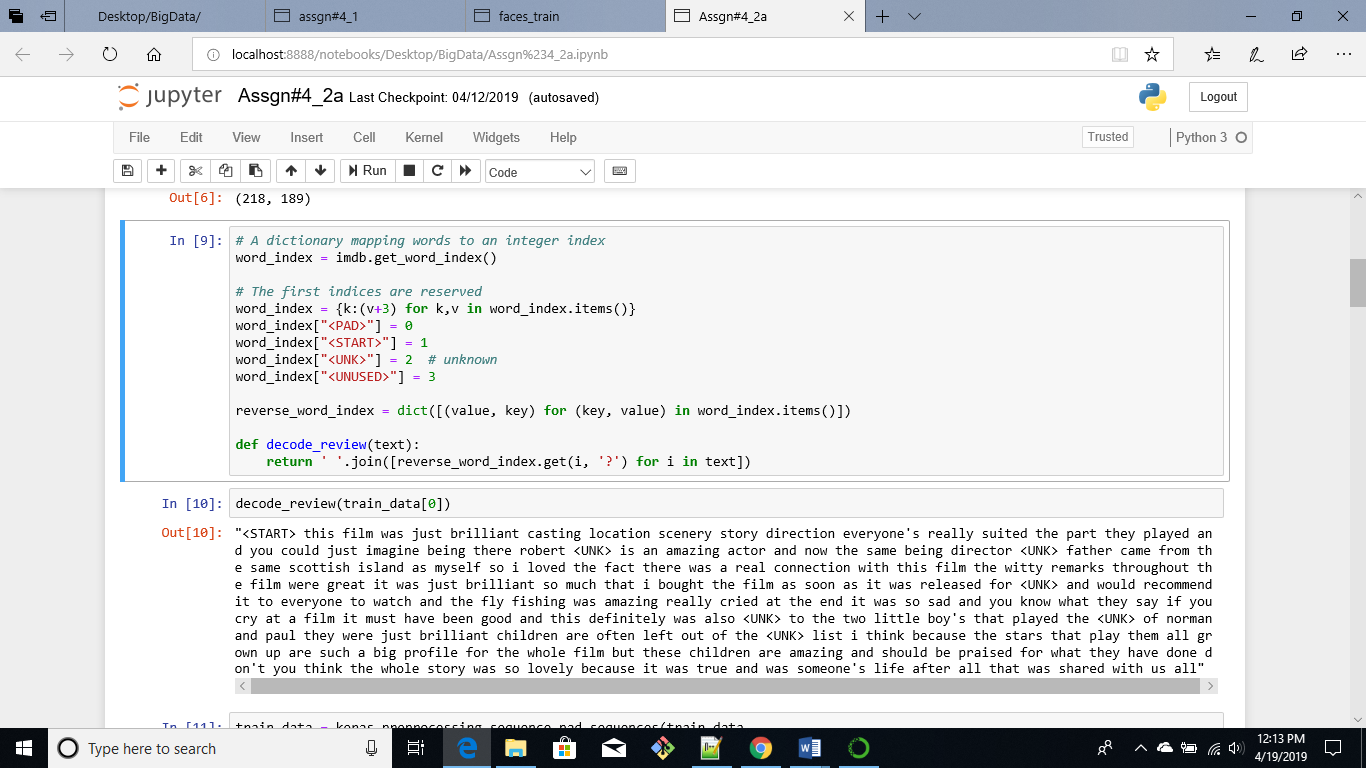
Script Name: assgn#4\_1.ipynb

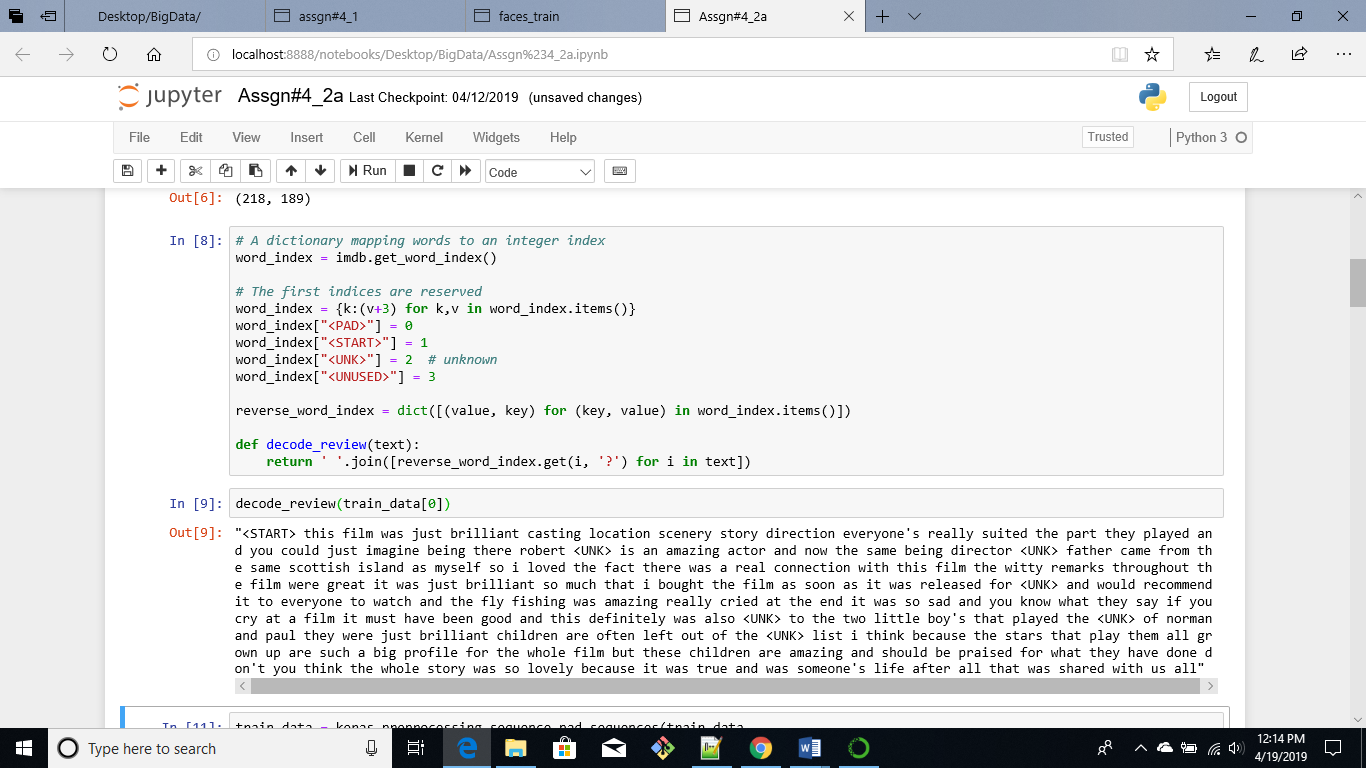
1. **TensorFlow Sample Problem**
2. Applying the Tensorflow model that was trained on the IMDB dataset I was able to classify positive and negative reviews of my dataset. I used the airline tweets dataset which consists of reviews of American airlines. The predictions gave values between 0 and 1, 0 represents negative sentiments and 1 indicates positive sentiments

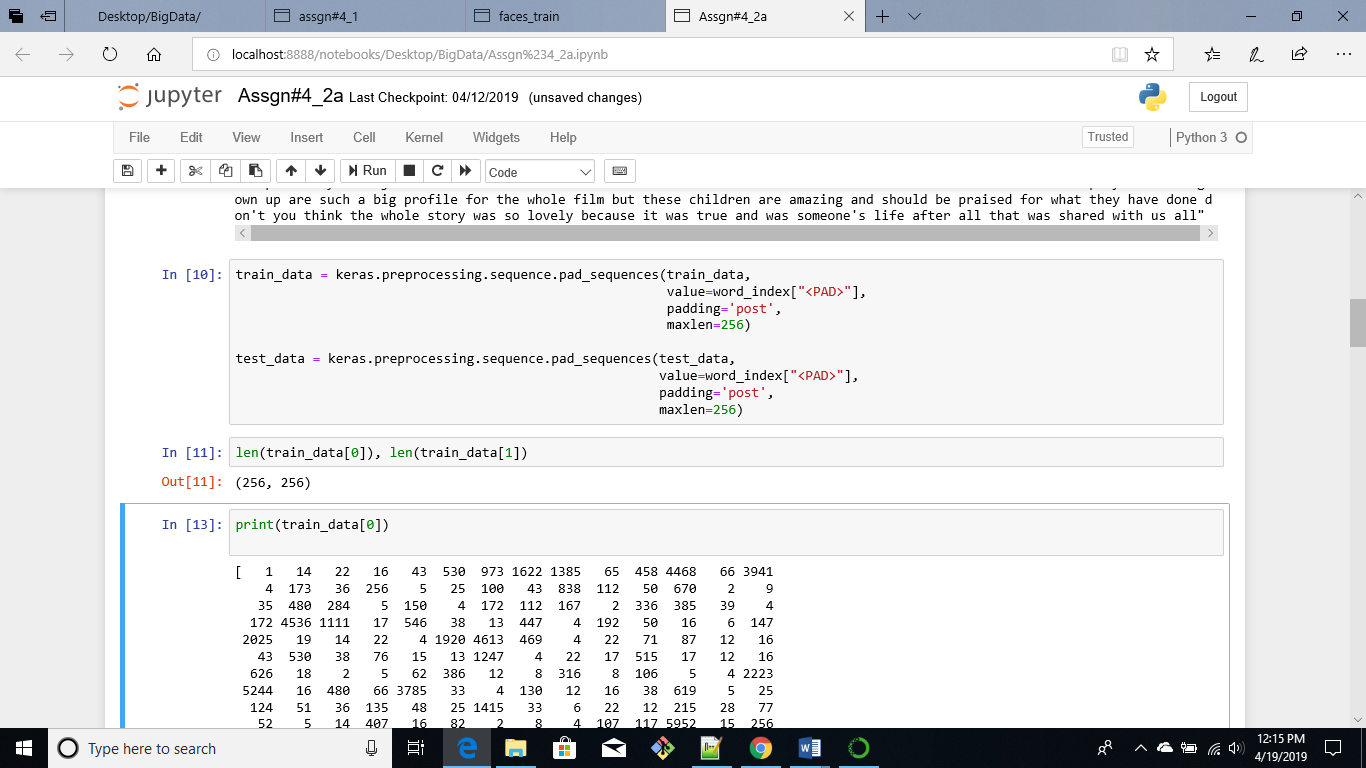
The screenshots below show how the model was trained on the IMDB dataset

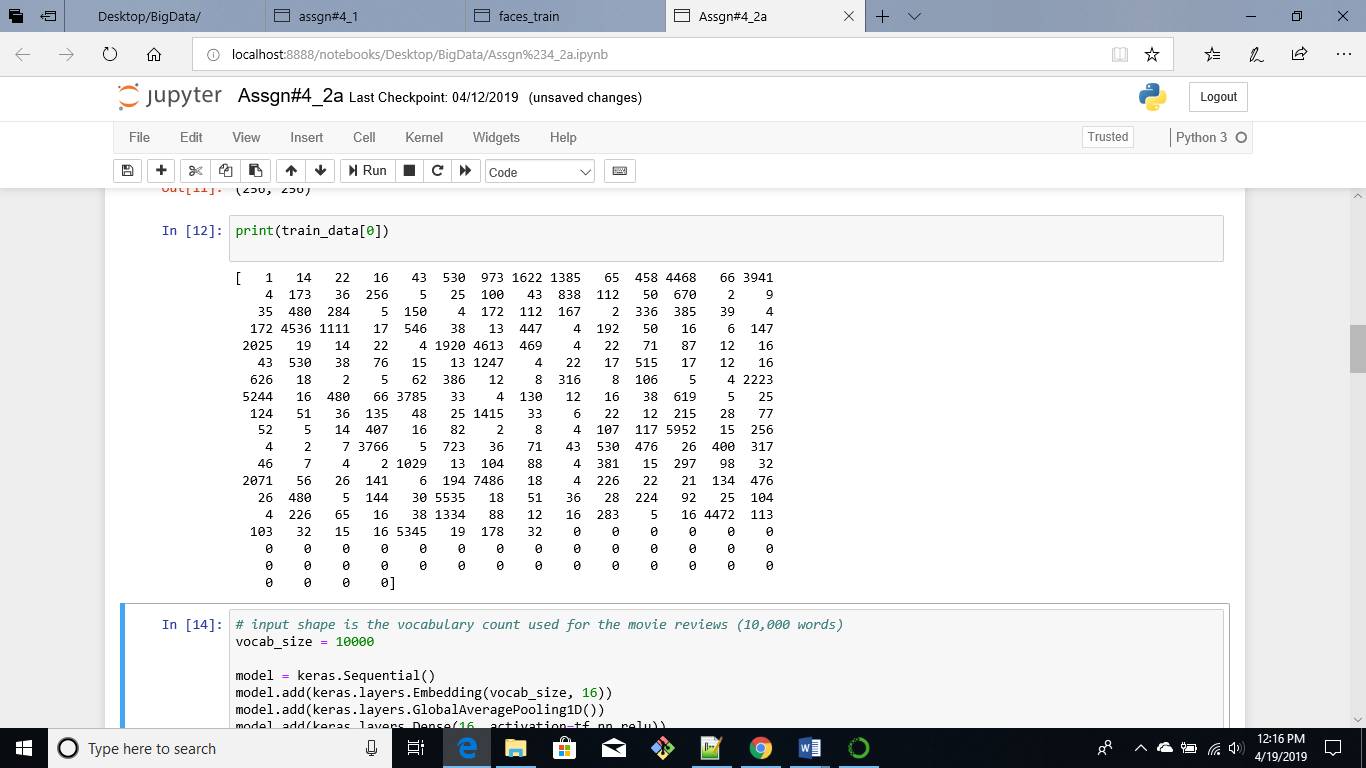


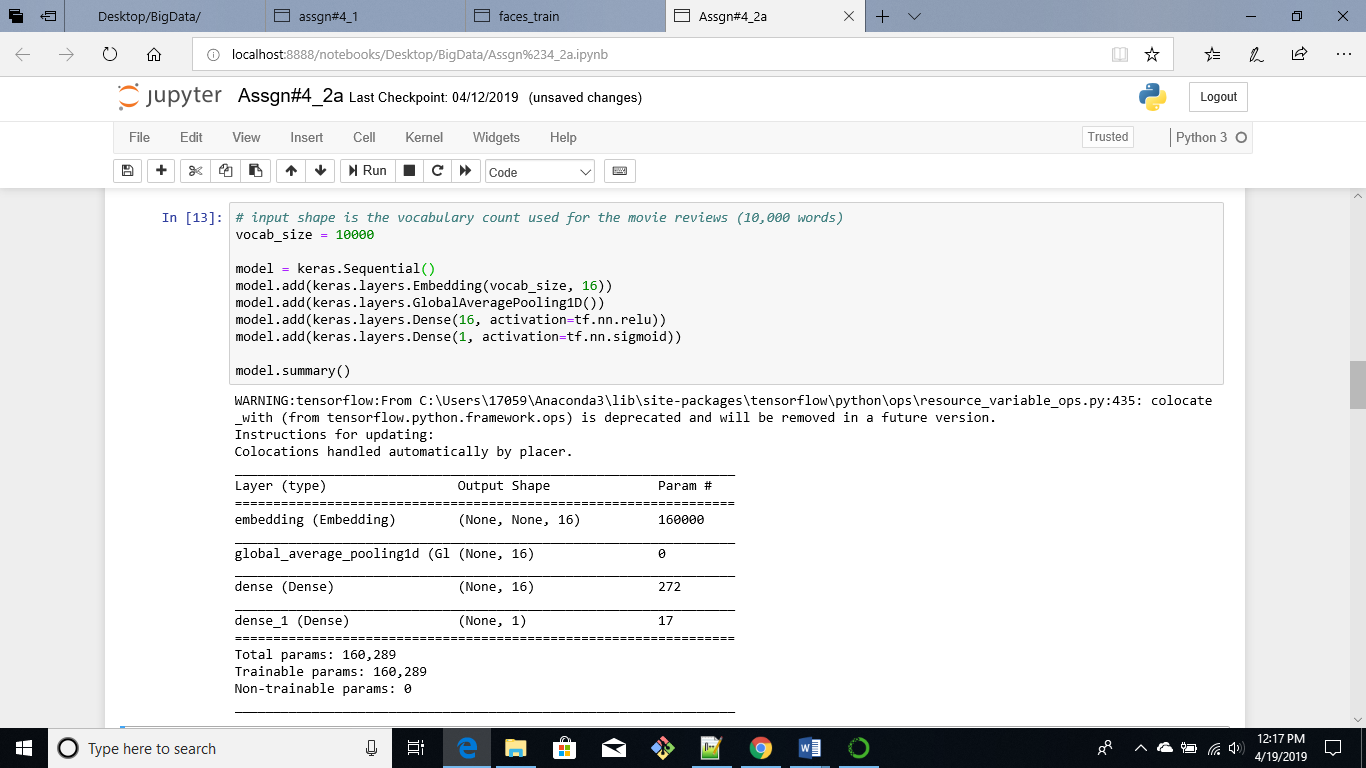


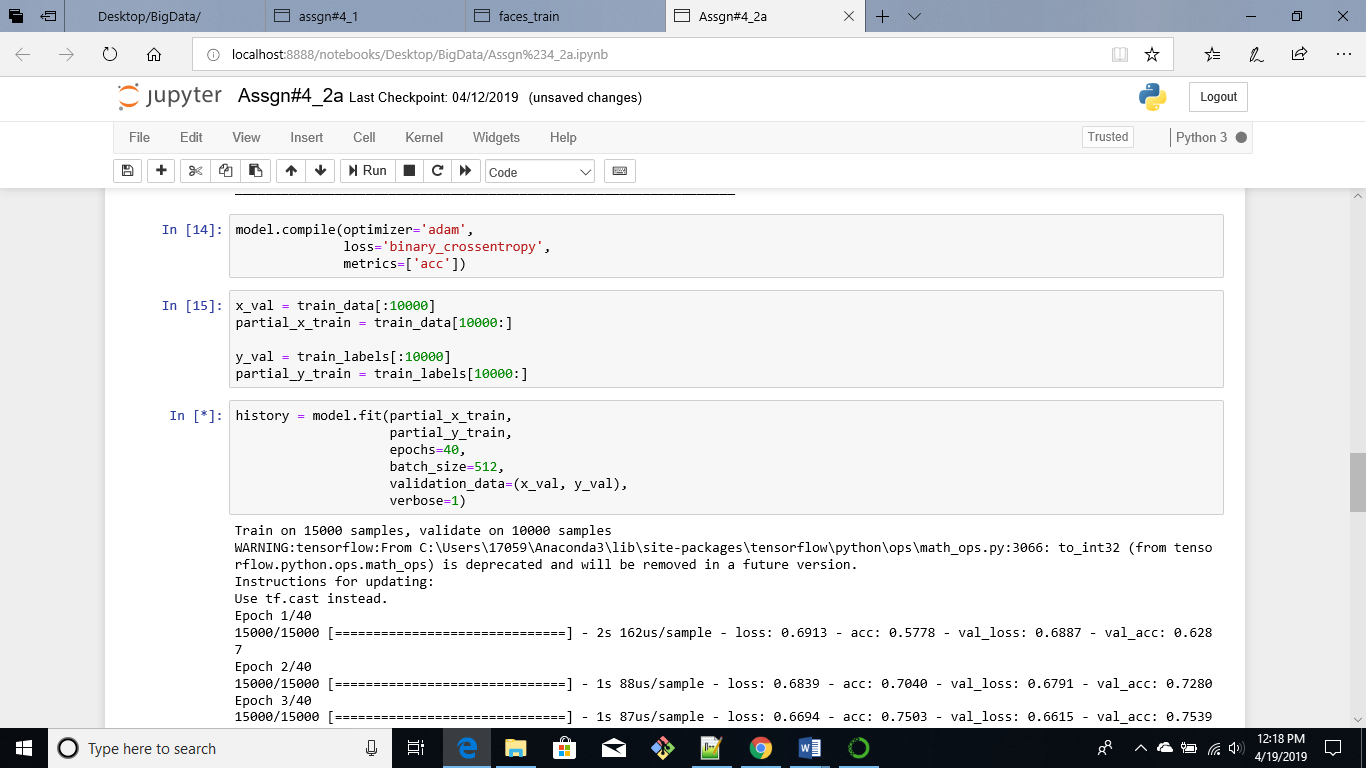


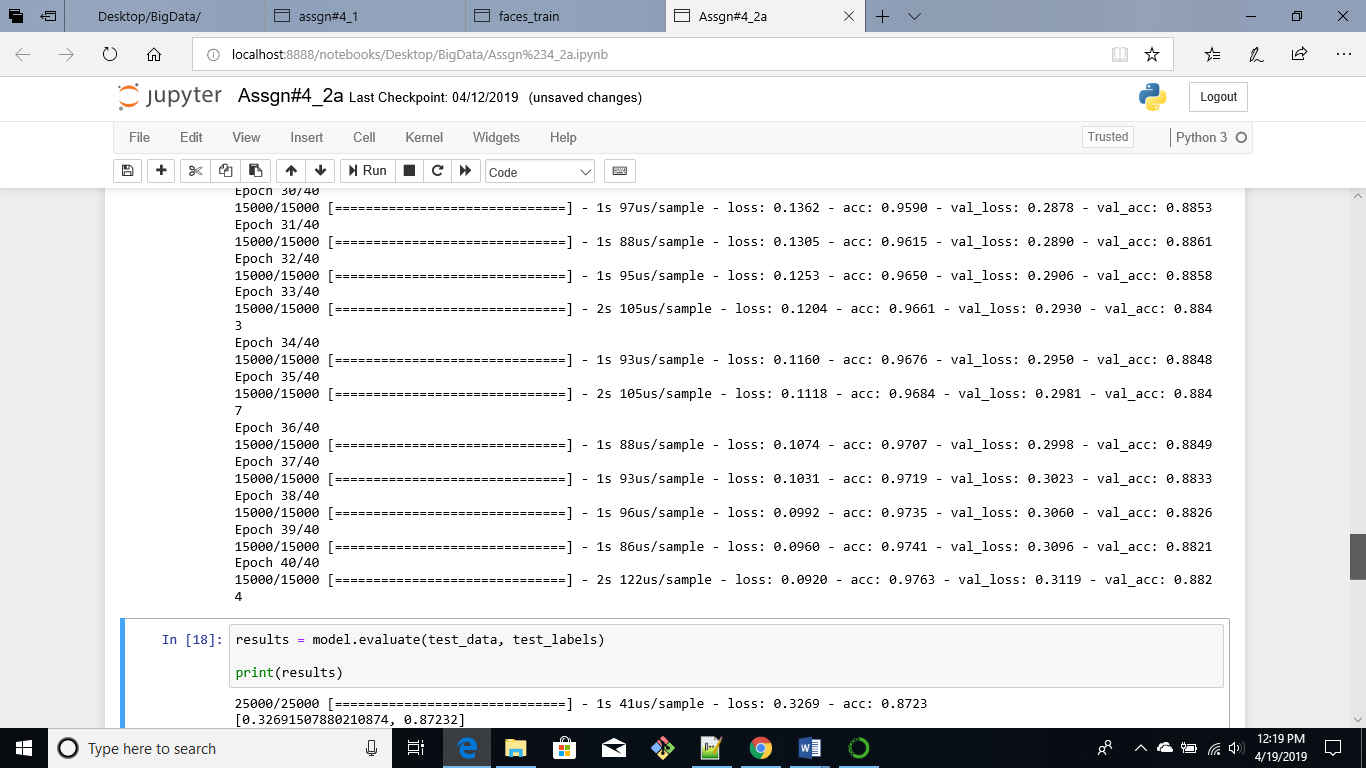


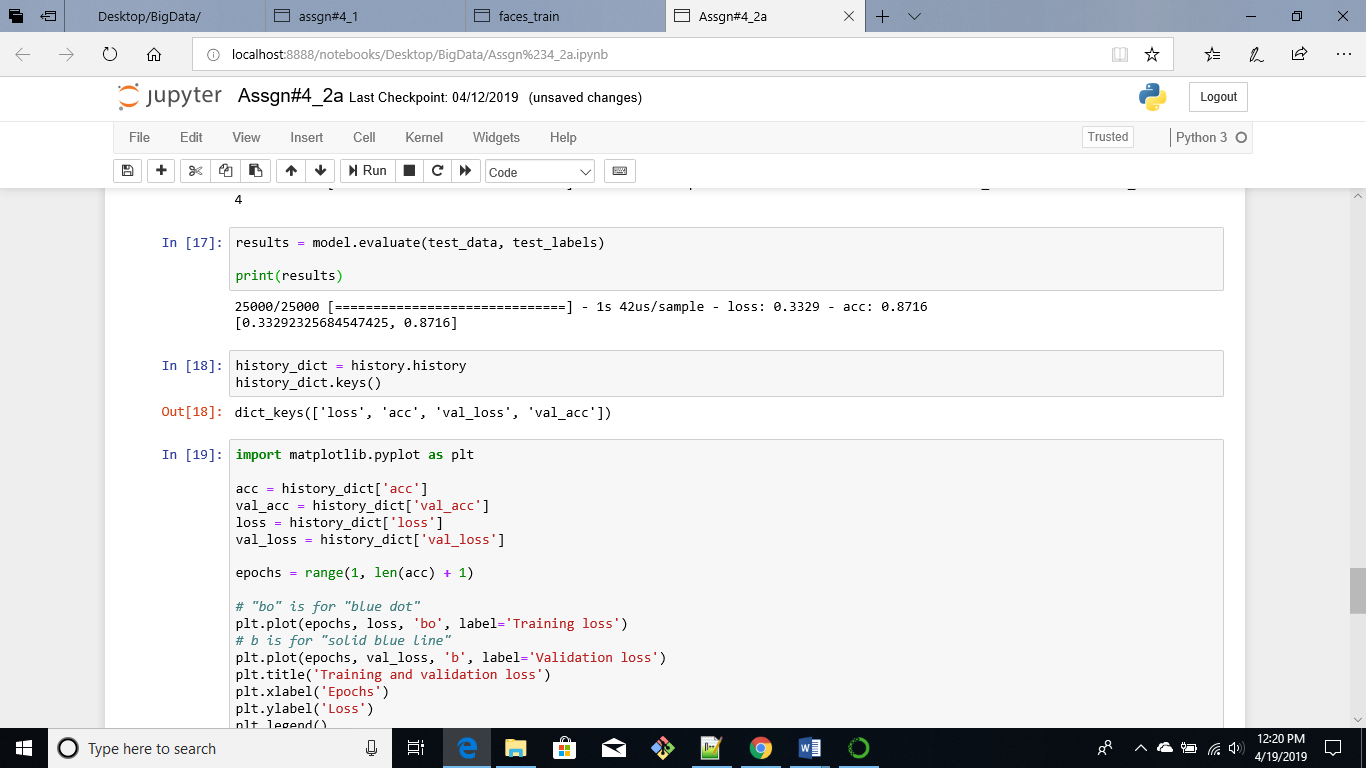


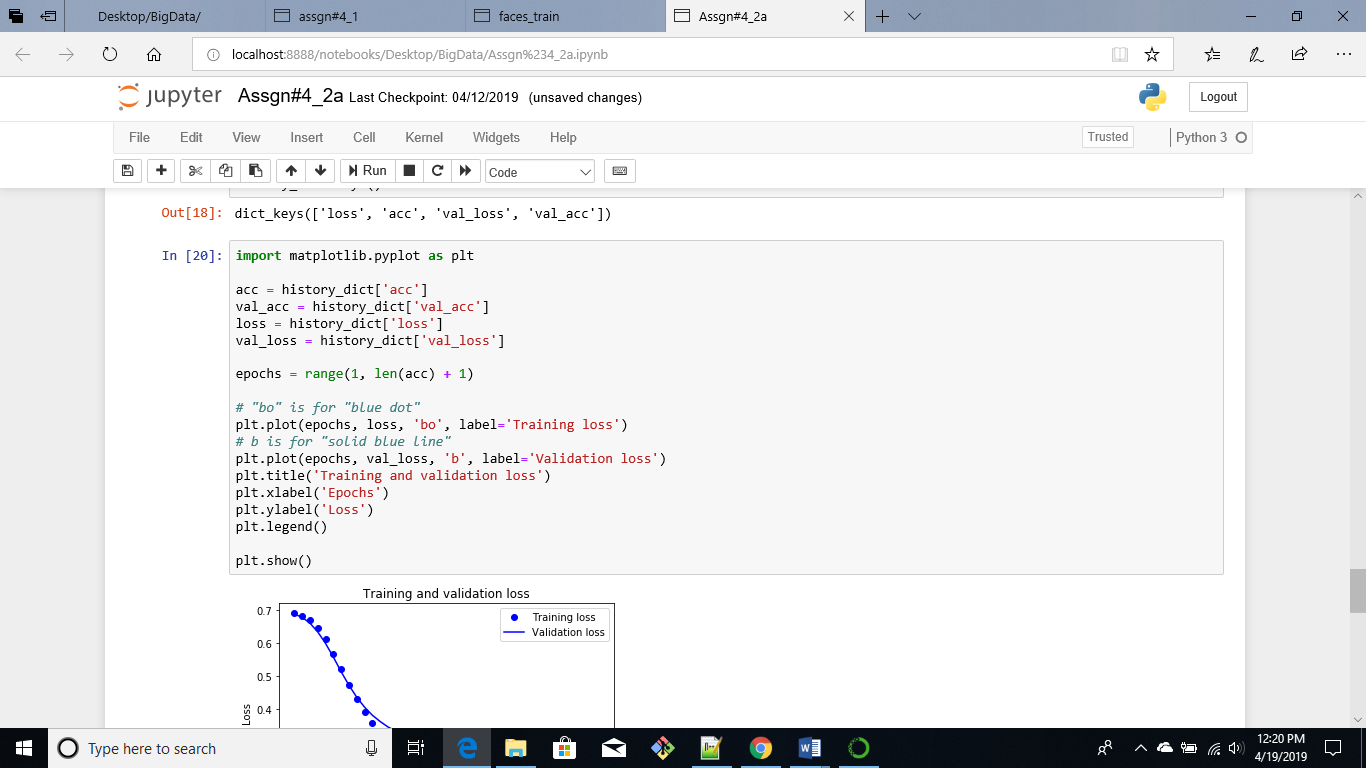


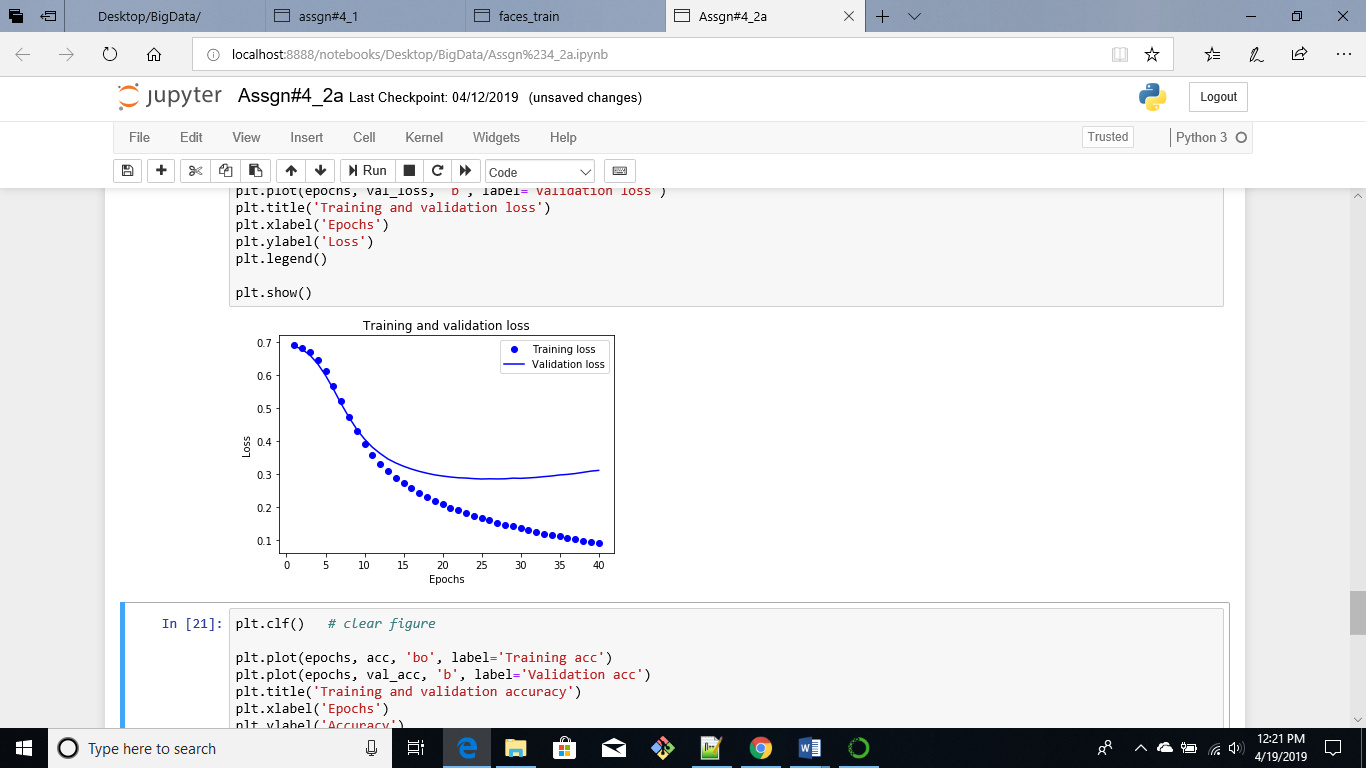


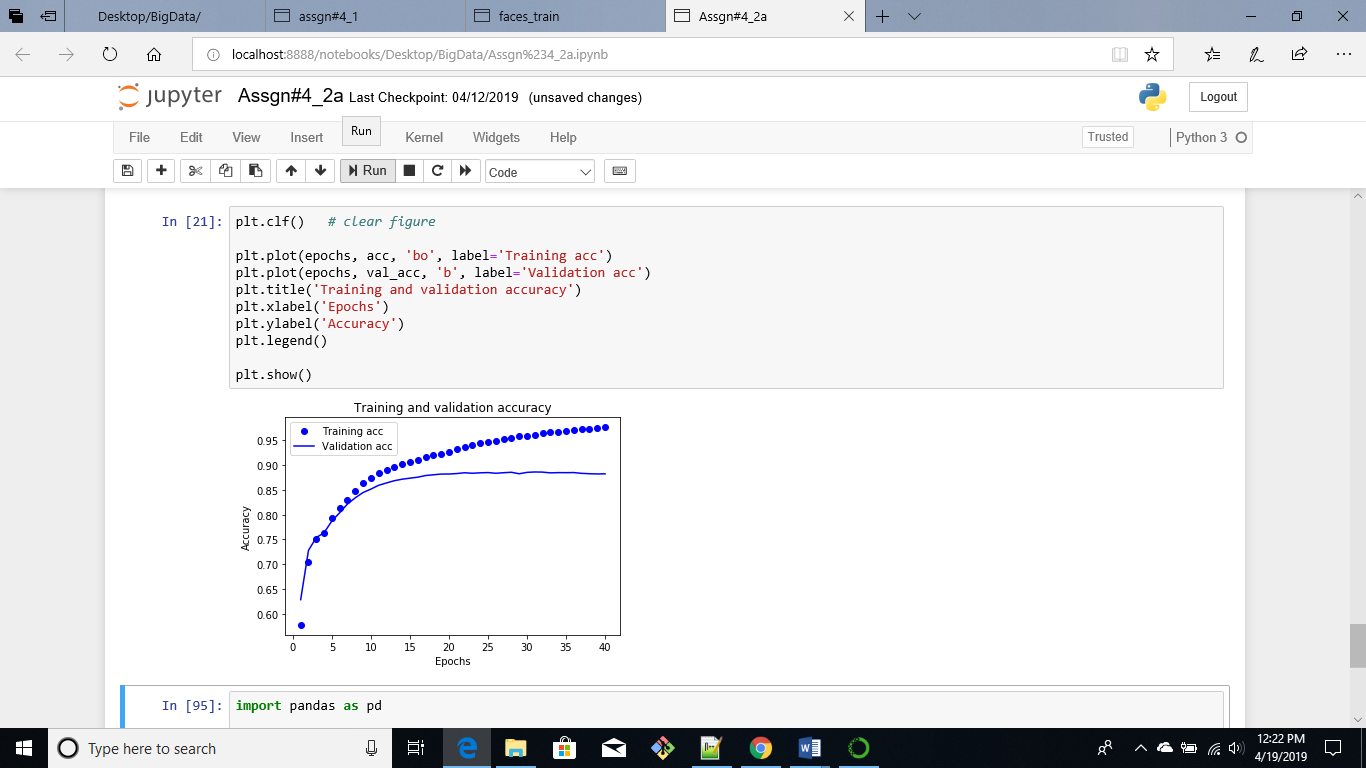


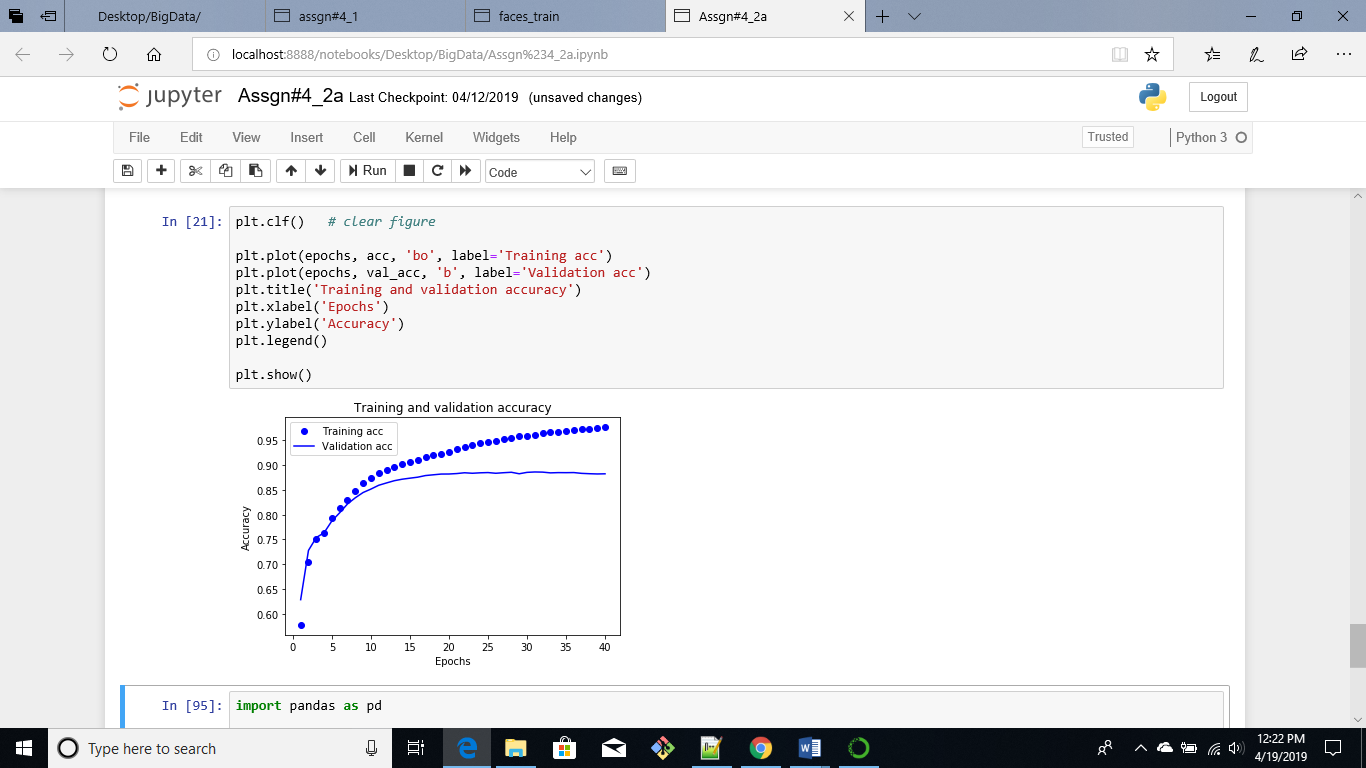




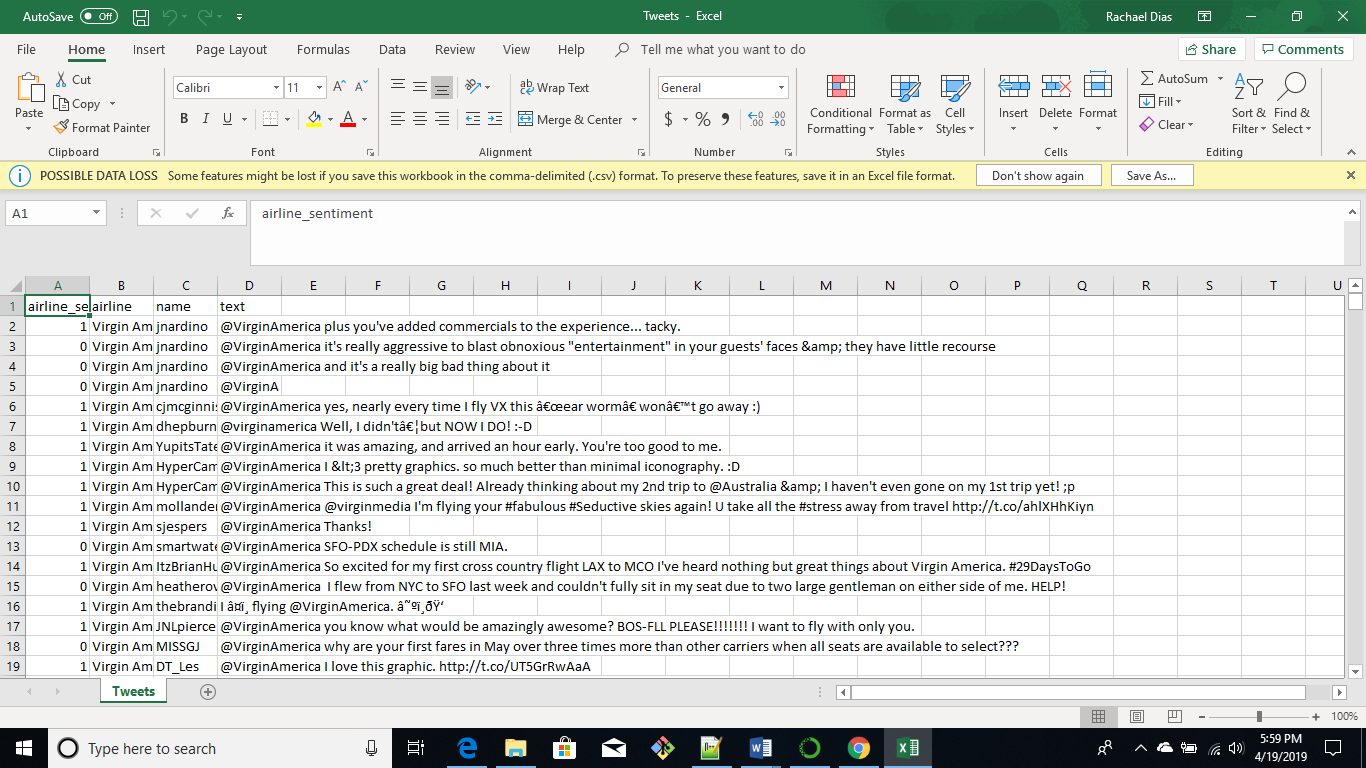






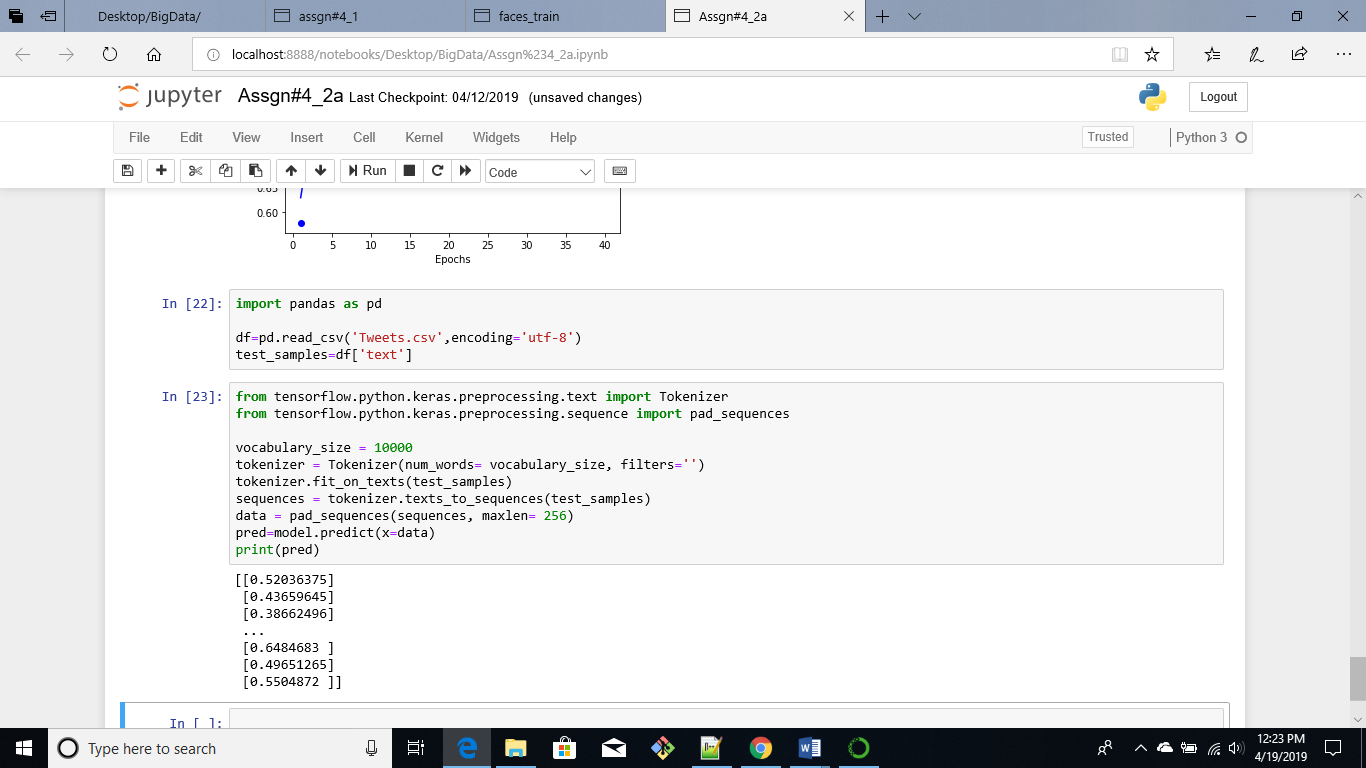


Below is a screenshot of the data the first column is airline sentiment which indicates if the reviews are positive or negative the text column contains passenger reviews.

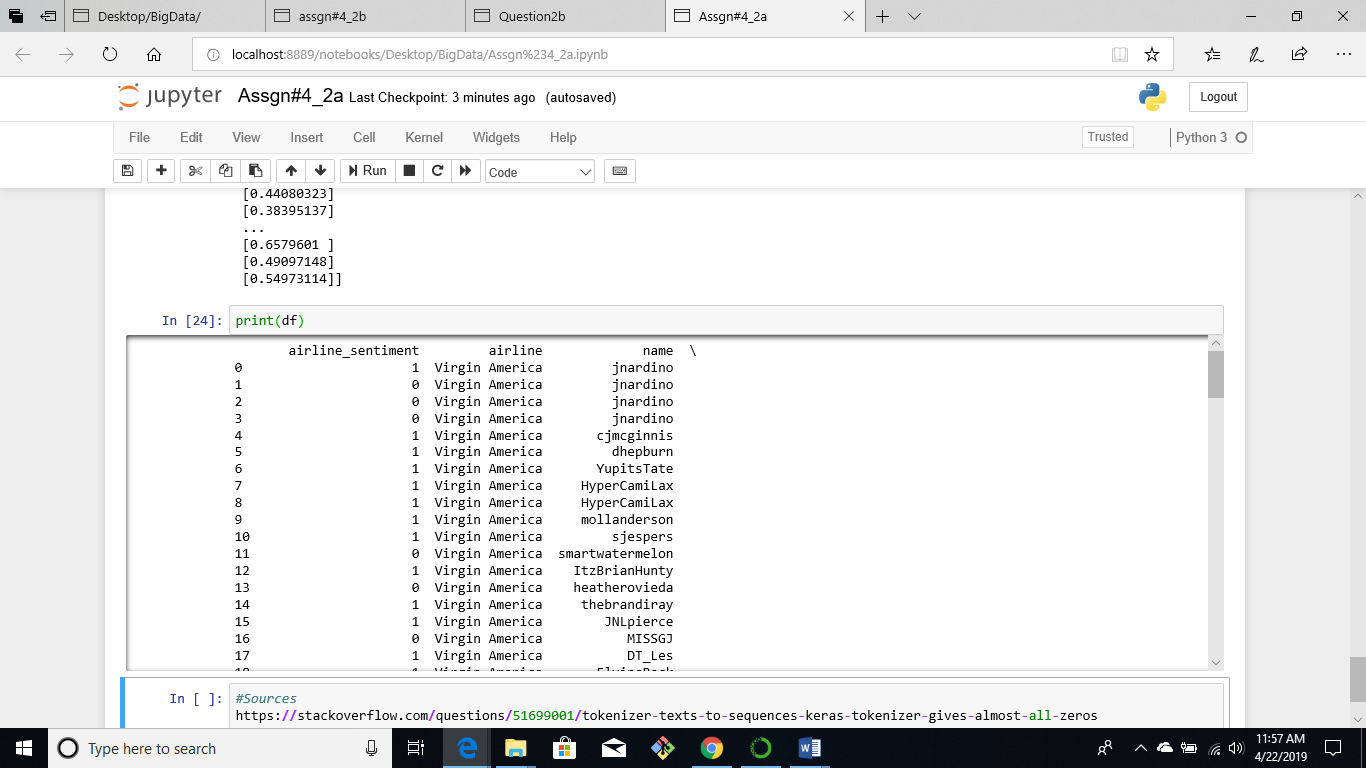


First, we import the pandas module to read the .csv file and specify the encoding as utf-8 the file is saved as a data frame “df” from which we select only the text column and save as another dataframe test\_samples.

From Tensorflow we import the preprocessing modules required Tokenizer and pad\_sequences. The text column data has to be converted into tokens using the tokenzier, and then into a series of sequences using the pad\_sequence function. This can be fed to the sentiment analysis model to make predictions. As, you can see we get an array of values between 0 and 1, those which are closer to 0 are classified as negative sentiments while those which are closer to 1 are positive sentiments [2].

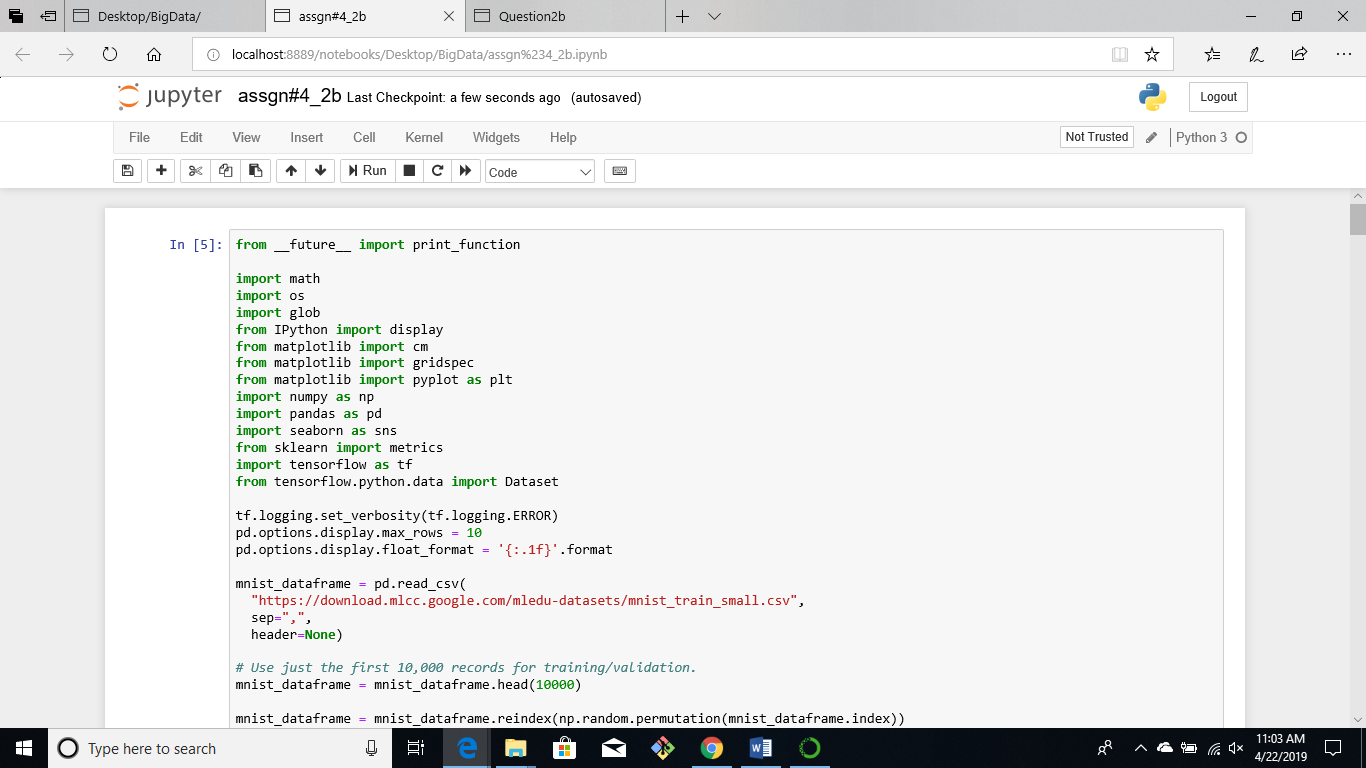


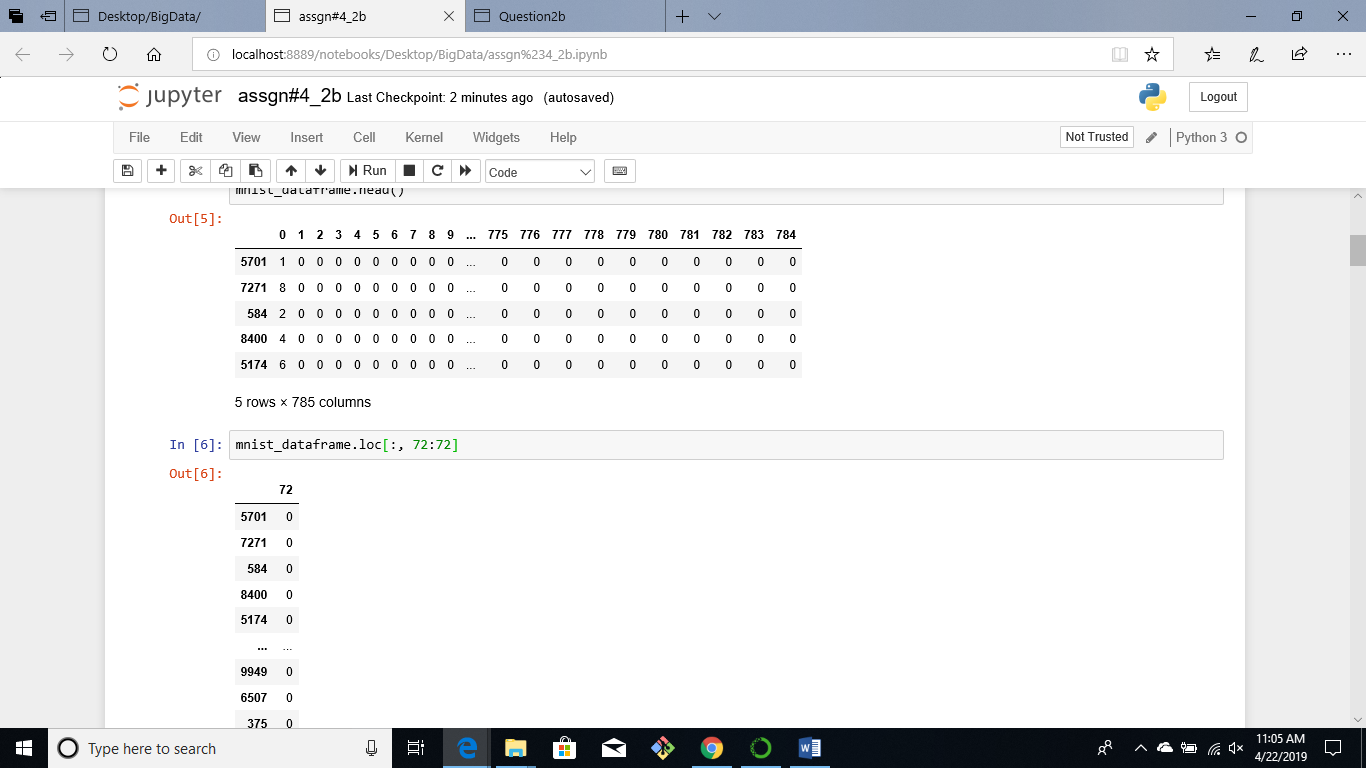
The first sentinment is positive while the second and third sentiments are negative. The model predicts .52, .436 and .386 for first, second and third respectively so we can assume that the first review is a positive review and the second and third reviews are negative.

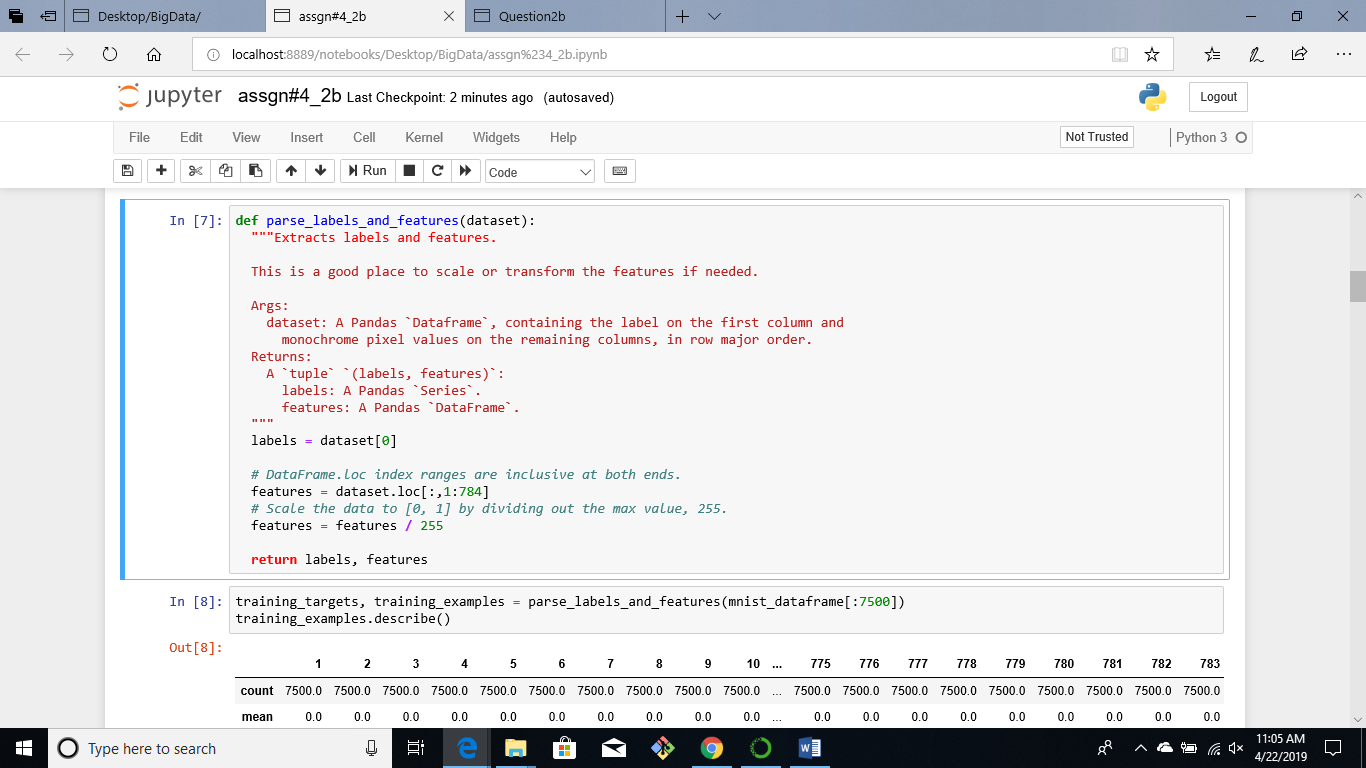


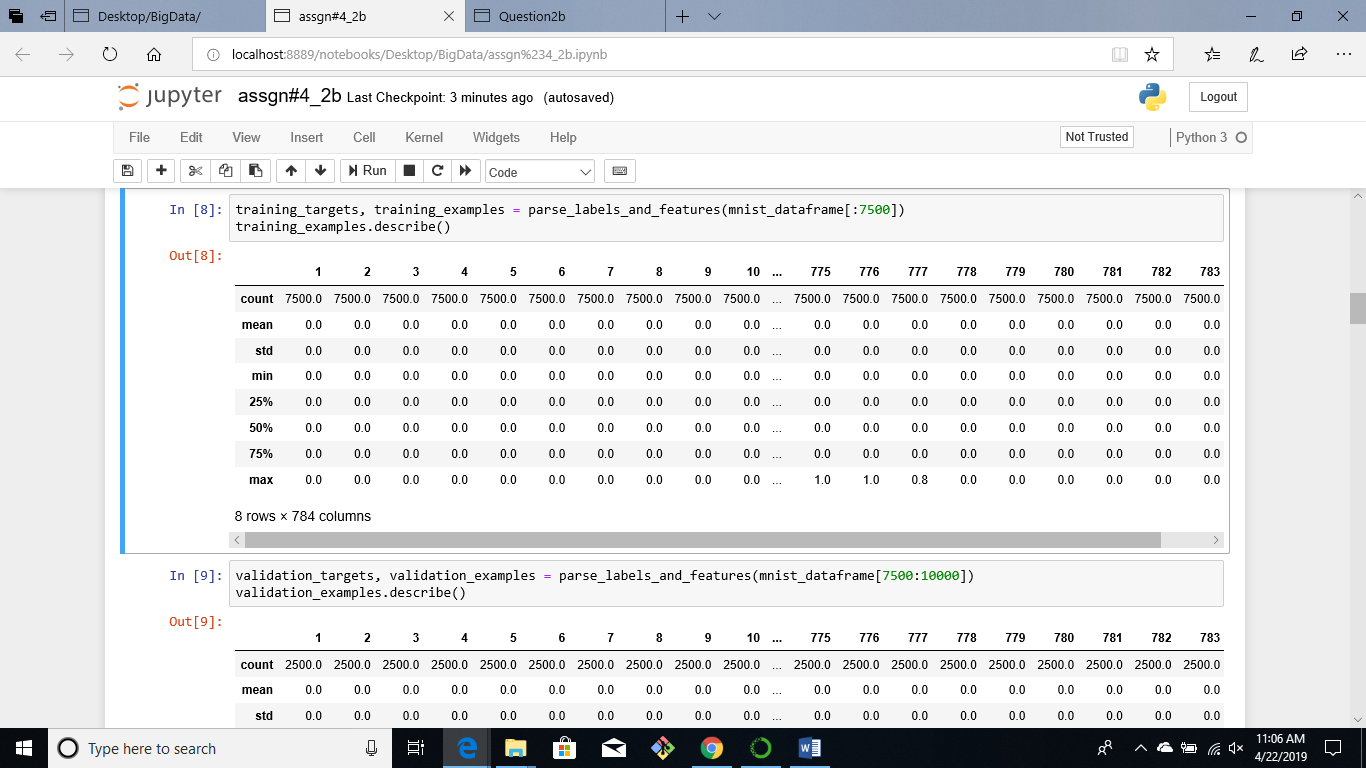
Script Name: Assgn#4\_2a

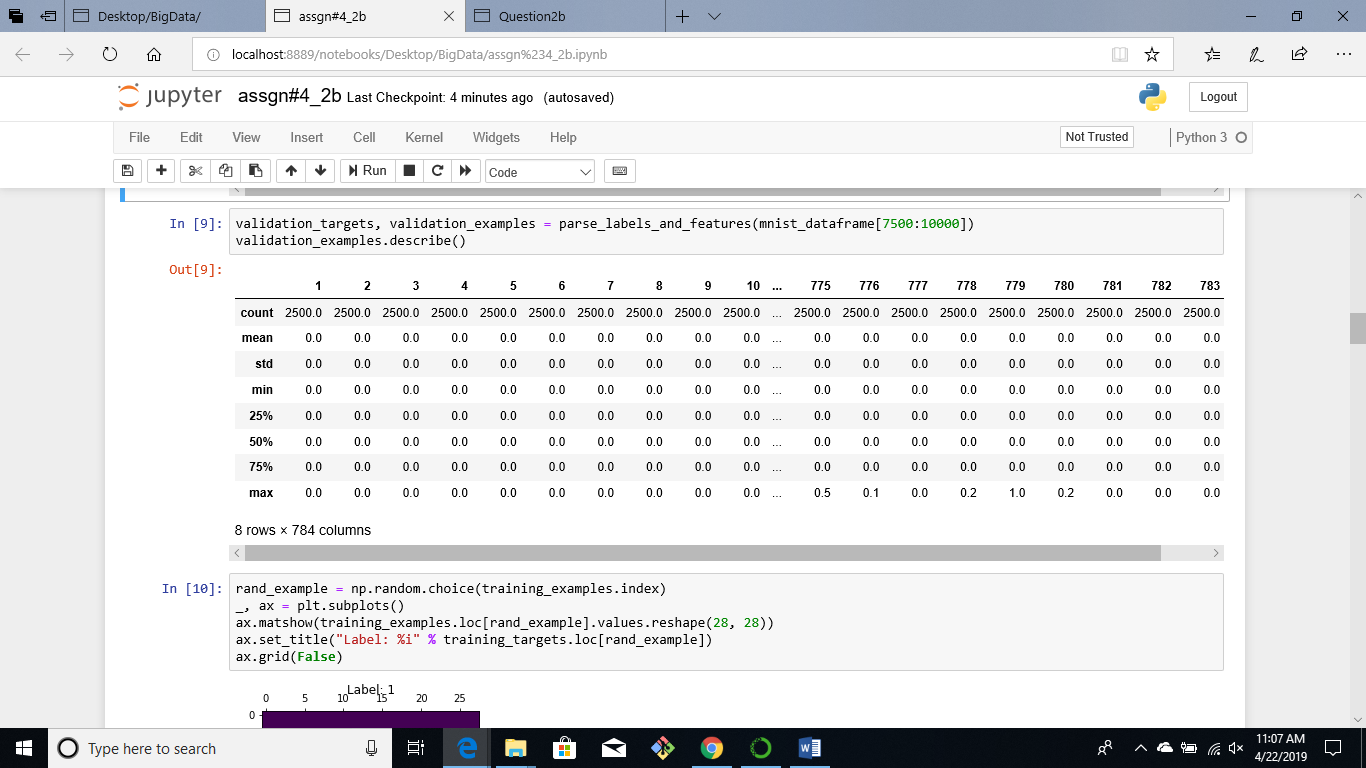
1. MNSIT model

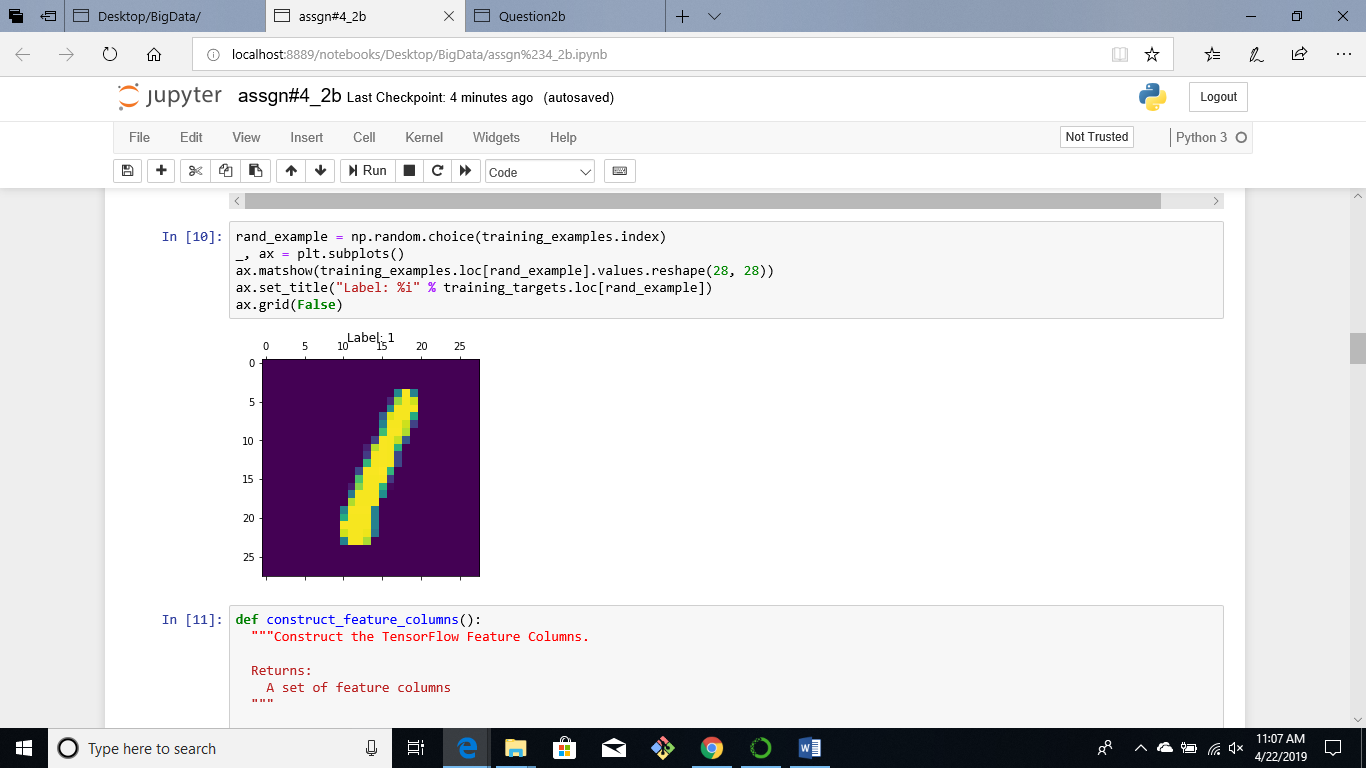


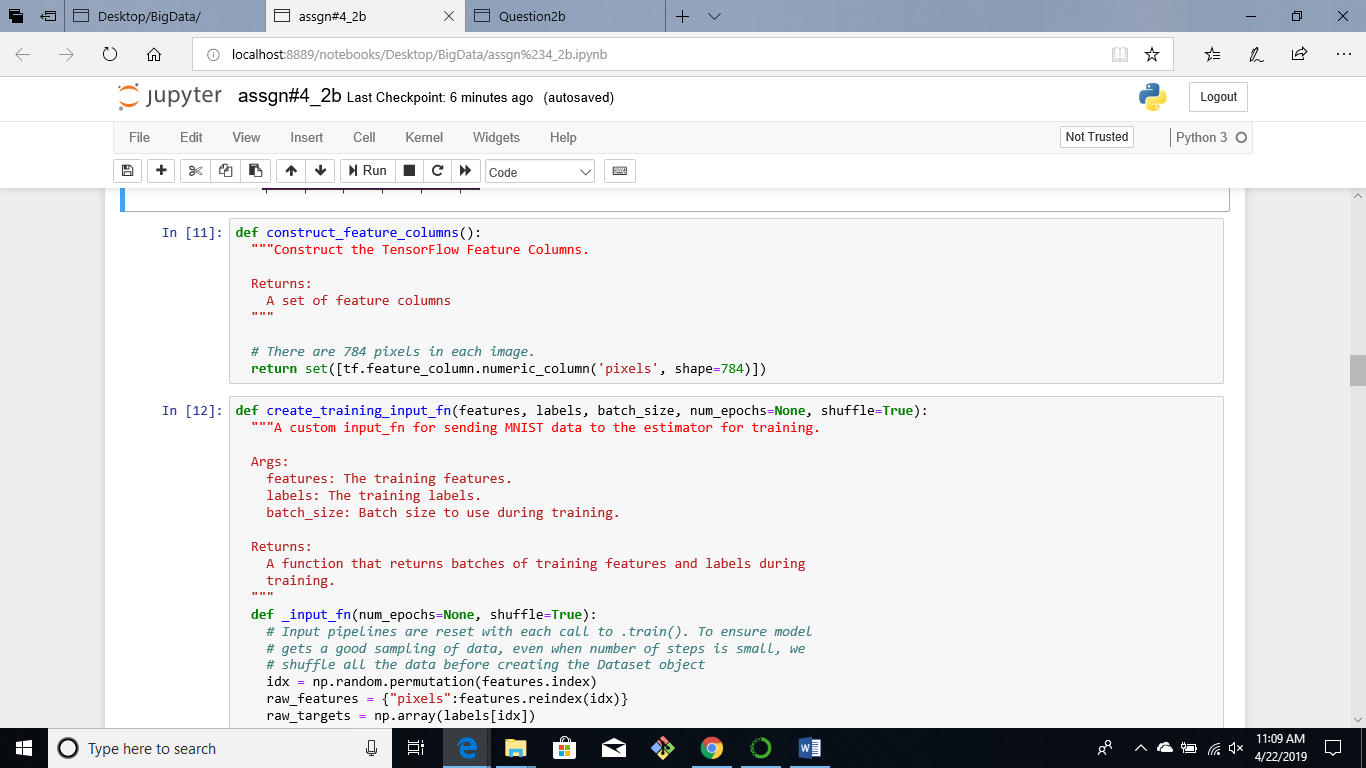


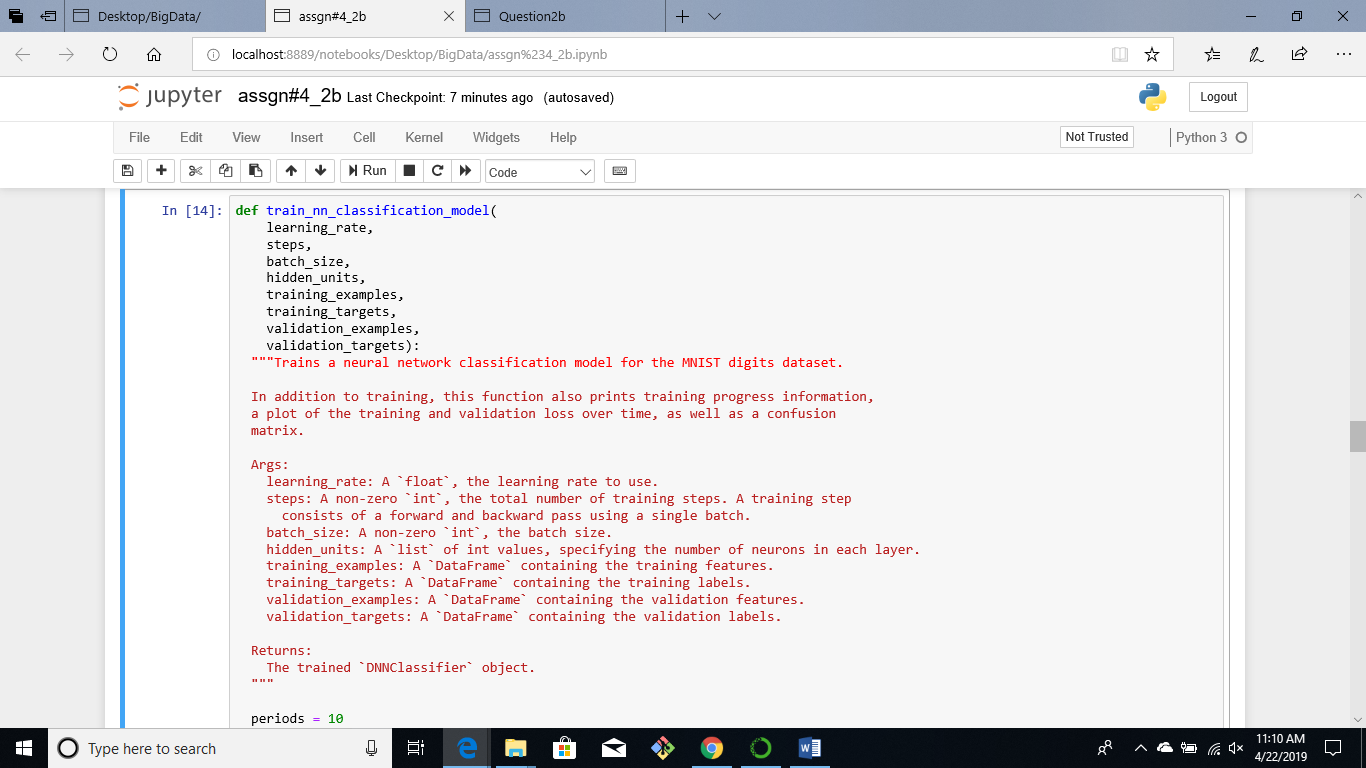




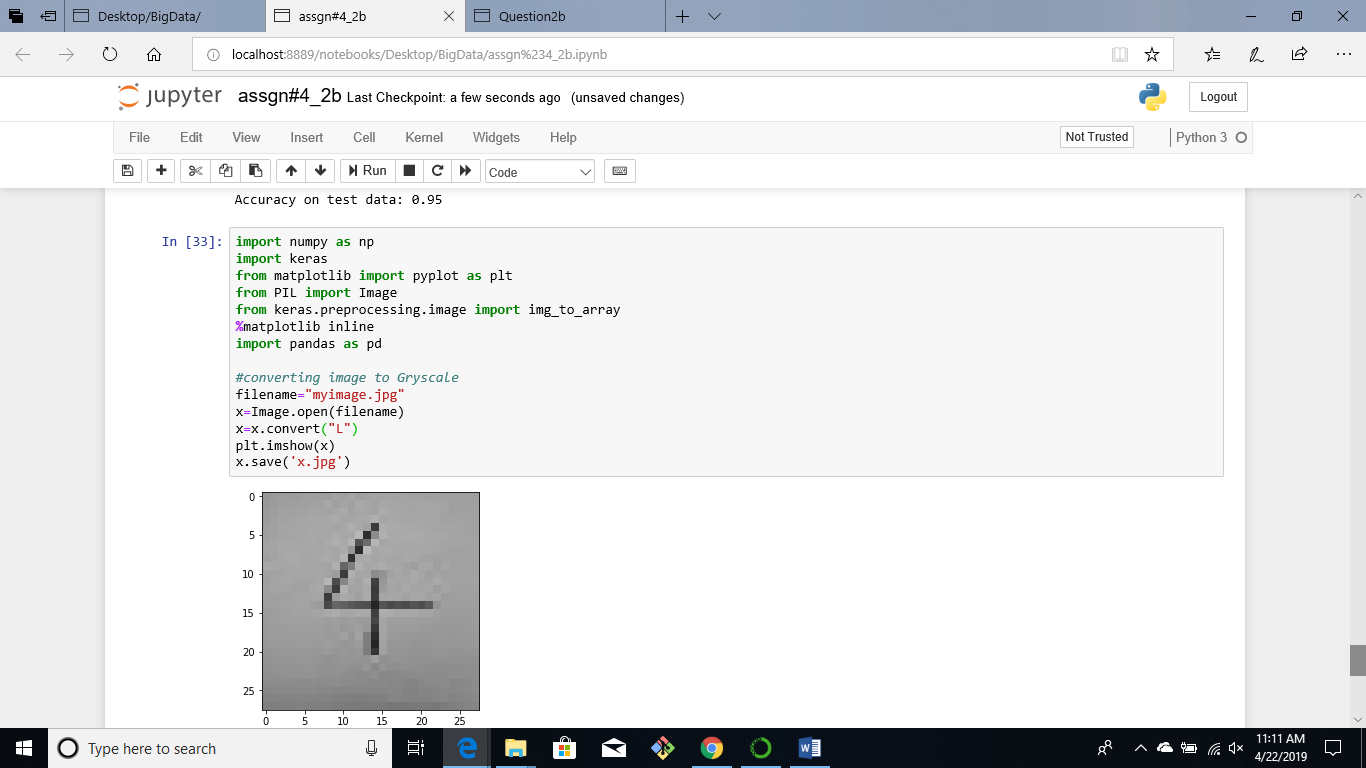




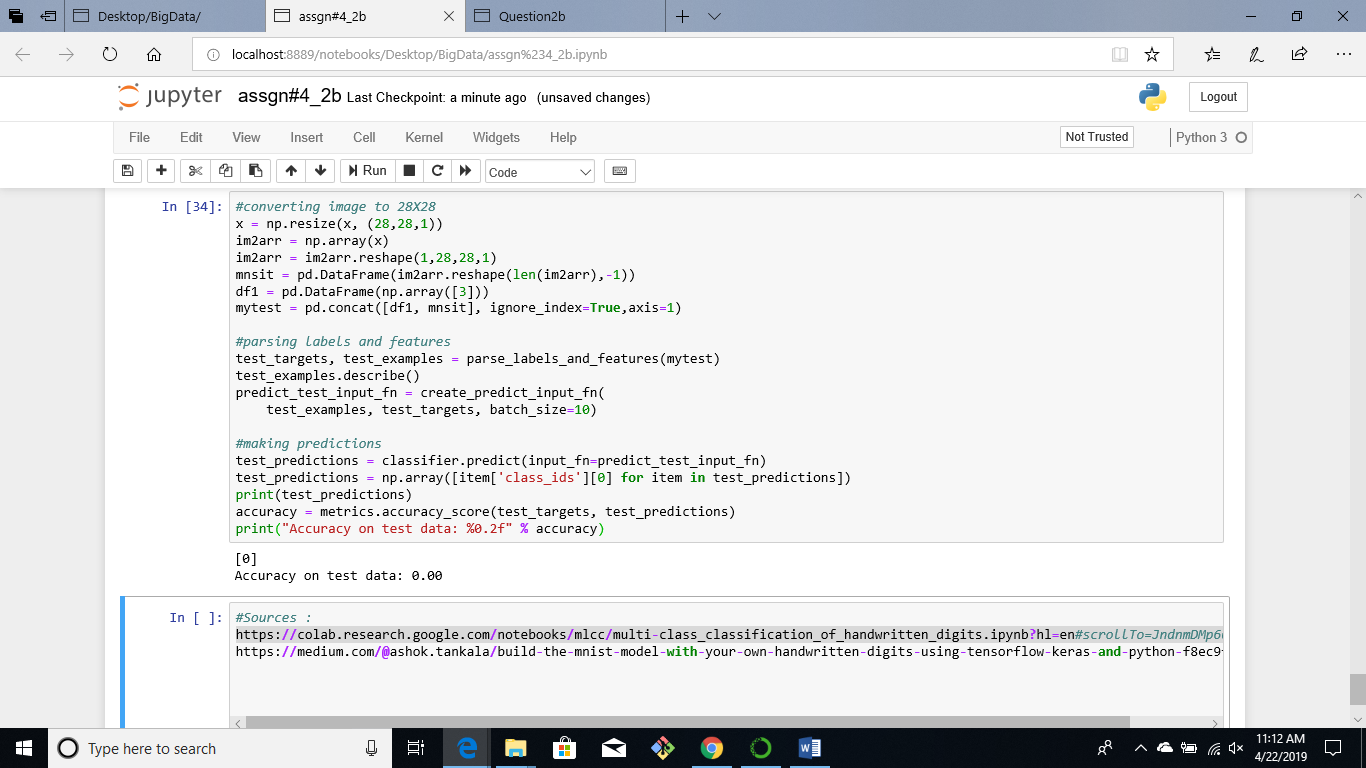




In order to apply the classifier to my handwritten image we need to convert the image to grayscale and resize it to 28x28. The code below converts the image to grayscale.



Next, the image has to be in the correct size and format after converting it to an array of 28x28 we then convert it to a dataframe and pass the image to the parse\_labels\_and\_features() function. Now, we can use the classifier to make predictions on the image, the classifier does not give very good results on the image



**Script Name:** assgn#4\_2b.ipynb

1. **Data Privacy**

In November of 2018, Marriott International hotels reported that cyber thieves had stolen data from 500 million customers. The breach began on systems supporting Starwood hotel brands in the year 2014. The cyber thieves continued to remain in the system after the Marriott group acquired Starwood in 2016 and remained undiscovered until September 2018 [3].

It is believed that for some of the victims only their name and contact information was compromised. However, the attackers also extracted passport information, Starwood Preferred Guest numbers, travel information and other personal information. There are claims that credit card information and expiration dates of as many as 100 million customers were stolen, although Marriott is not certain if the hackers were able to decrypt the credit card numbers [3].

The breach was attributed to a Chinese intelligence group which was trying to gather information on US citizens. A few individuals who were brief after an investigation also reported that the intelligence group hacked health insurers and security clearance files of millions of more Americans [3].

It is suspected that the hackers were working on behalf of the Ministry of State Security, the country’s Communist-controlled civilian spy agency. This discovery was made while the Trump was planning actions to target China’s trade, cyber and economics policies. The actions included criminal accusations against Chinese hackers working for intelligence services and the military, the Trump administration also plans on revealing intelligence reports that reveal Chinese efforts to set up a database containing the names of executives and American governments officials with security clearance [3].

Some of the other options included making it harder for Chinese companies to obtain critical components from telecommunications equipment, as stated by a senior American official [3].

Despite the 90-day truce negotiated by president Trump and President Xi Jinping in Buenos Aires, the administration believes this might do very little to change China’s behavior. Since China has coerced American companies to hand over valuable technology if they wish to enter the Chinese market, this also includes theft of industrial secrets on behalf of state-owned companies [3].

The Yahoo data breach was one of the largest data breaches in history, it impacted over 3 billion user accounts. While Yahoo was making negotiations to sell itself to Verizon it revealed that it had been a victim of the biggest data breach, that had been likely committed by a state-sponsored hacker in 2014, the announcement was made in September 2016, 2 years after the breach happened. The data breach compromised the real names, email addresses, date of birth and phone number of 500 million users. Yahoo reported that most of the passwords involved had been hashed by the bcrypt algorithm [3].

A few months later in the month of December 2018 it covered up the earlier record with the disclosure that a breach in 2013, by another group of cyber thieves had compromised 1 billion accounts. Aside from the names, dates of birth, email addresses and passwords that were protected not as well as the ones involved in the 2014 breach, it is estimated the even security questions and answers were compromised. By October of 2017, Yahoo reviewed that estimate, stating that all 3 billion user accounts had been compromised [3].

The data breaches severely affected Yahoo’s sales prices knocking of an estimated $350 million of the company’s sales price. Yahoo, founded in 1994, had been valued at $100 billion, ultimately Verizon paid $4.48 billion for Yahoo’s core internet business. The agreement meant that the two companies had to share regulatory and legal liabilities from the breaches. Yahoo failed to thoroughly investigate the data breaches and carried on carelessly which ultimately led to the downfall of the company [3].

In late 2016 personal information of 57 million Uber accounts and 600,00 drivers was exposed, Uber did not handle the breach well. By late 2016 the company learned that 2 hackers had extracted names, email addresses, and mobile numbers of 57 million users on the Uber app. They also hacked the drivers license numbers of 600,00 Uber drivers. Apart from this not other information such as credit card and Social Security numbers were stolen. The hackers accessed the information through Uber’s GitHub account, where thy were able to find username and password credentials to Uber’s AWS account. The username and password credentials should have never been on the GitHub account in the first place [3].

It wasn’t until about a year after the incident happened that Uber made the breach public. The worst part was that they paid the hackers $100,000 to destroy the data with no way of verifying that it was destroyed. Eventually Uber fired it’s CSO because of the breach, putting all the blame on him [3].

The breach cost Uber a lot of money and ruined it reputation. At the time when the breach was announced the company was negotiating to sell a stake of the company to Softbank. Uber’s was initially valued at $68 billion by the time the deal was sealed in December; its value dropped to $48 billion [3].

Data is growing at an exponential rate; it is estimated that nearly 1.7 megabytes of data are created every second. This makes it extremely hard for organizations to keep up and protect their customer’s personal information. Poor security practices such as the Uber data breach put organization at risk of a data breach [4].

A data breach can cost an organization millions of dollars and ruin its reputation. In the year 2017, the average cost of a breach was $3.62 million. If a data breach occurs the organization faces intense regulatory penalties from an array of institutions. Companies dealing with customer information in the European Union that face a huge breach because of lack of security control can face a penalty of up to 4% Adjusted Gross Revenue or 20 million euros. In order to avoid this companies must make investments in key security technologies such as data archiving, backup and redundant infrastructure to protect their data [4].

Human error is the biggest challenge that is faced in data privacy and security. Employees that are unaware may use weak passwords, mistakenly delete data, browse websites that are not acceptable. Data loss prevention tools can help prevent leaking sensitive data [4].

**References**

[1] <https://www.learnopencv.com/keras-tutorial-using-pre-trained-imagenet-models/>

[2] <https://stackoverflow.com/questions/51699001/tokenizer-texts-to-sequences-keras-tokenizer-gives-almost-all-zeros>

[3] <https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>

[4] <http://blog.cipher.com/the-5-biggest-challenges-in-global-data-privacy-and-data-protection>