

Milestone 2: Billionaire Secretary

Team Billionaires: Huandong Chang, Mingyuan Ma, Lance Lu, April Zhang

Virtual Environment Setup

Our virtual environment setup is included in the Dockerfile of each component. We used Pipenv with `Pipfile` and `Pipfile.lock` to manage dependencies.

Data Pipeline

```
(base) aprilzxd@DESKTOP-JKSGKNH:/mnt/c/Study@Harvard/AC215/AC215-project/src/datapipeline$ sh docker-shell.sh
[+] Building 0.5s (11/11) FINISHED                                docker:default
=> [internal] load build definition from Dockerfile              0.0s
=> => transferring dockerfile: 275B                               0.0s
=> [internal] load .dockerignore                                0.0s
=> => transferring context: 2B                                     0.0s
=> [internal] load metadata for docker.io/library/python:3.11-slim 0.3s
=> [1/6] FROM docker.io/library/python:3.11-slim@sha256:a9476aa83bc40fce9b019b8e5b6ff3f855ae5bdd2460f60173ae405c 0.0s
=> [internal] load build context                                0.0s
=> => transferring context: 306B                                   0.0s
=> CACHED [2/6] WORKDIR /app                                    0.0s
=> CACHED [3/6] COPY Pipfile Pipfile.lock /app/                 0.0s
=> CACHED [4/6] RUN pip install pipenv                          0.0s
=> CACHED [5/6] RUN pipenv lock && pipenv sync                   0.0s
=> CACHED [6/6] COPY . /app                                     0.0s
=> exporting to image                                           0.0s
=> => exporting layers                                           0.0s
=> => writing image sha256:d0005ed38ccad7333638a9443f072c1b74400d1b95f1c871ce8881249b344ebb 0.0s
=> => naming to docker.io/library/datapipeline                  0.0s

What's Next?
  View a summary of image vulnerabilities and recommendations → docker scout quickview
Launching subshell in virtual environment...
root@9a4dfed44173:/app# source /root/.local/share/virtualenvs/app-4PLAip0Q/bin/activate
(app) root@9a4dfed44173:/app# |
```

Gemini Finetuner

```
(base) aprilzxd@DESKTOP-JKSGKNH:/mnt/c/Study@Harvard/AC215/AC215-project/src/gemini-finetuner$ bash docker-shell.sh
[+] Building 1.0s (12/12) FINISHED                                docker:default
=> [internal] load .dockerignore                                0.0s
=> => transferring context: 2B                                     0.0s
=> [internal] load build definition from Dockerfile              0.0s
=> => transferring dockerfile: 1.56kB                             0.0s
=> [internal] load metadata for docker.io/library/python:3.9-slim-buster 0.8s
=> [auth] library/python:pull token for registry-1.docker.io    0.0s
=> [1/6] FROM docker.io/library/python:3.9-slim-buster@sha256:320a7a4250aba4249f458872adecf92eea88dc6abd2d76dc5c 0.0s
=> [internal] load build context                                0.0s
=> => transferring context: 220B                                   0.0s
=> CACHED [2/6] RUN set -ex; for i in $(seq 1 8); do mkdir -p "/usr/share/man/man${i}"; done && apt-get 0.0s
=> CACHED [3/6] WORKDIR /app                                    0.0s
=> CACHED [4/6] ADD --chown=app:app Pipfile Pipfile.lock /app/ 0.0s
=> CACHED [5/6] RUN pipenv sync                                  0.0s
=> CACHED [6/6] ADD --chown=app:app . /app                      0.0s
=> exporting to image                                           0.0s
=> => exporting layers                                           0.0s
=> => writing image sha256:f4c5b287295fe40ce4a576d8567ce984a5d197406a7e04e01b99aa6042d115c0 0.0s
=> => naming to docker.io/library/gemini-finetuner              0.0s

What's Next?
  View a summary of image vulnerabilities and recommendations → docker scout quickview
Container is running!!!

Launching subshell in virtual environment...
app@cee7e818a9a0:/app$ source /home/app/.local/share/virtualenvs/app-4PLAip0Q/bin/activate
(app) app@cee7e818a9a0:/app$ |
```

Agents

```
(base) aprilzxd@DESKTOP-JKSGKNH: /mnt/c/Study@Harvard/AC215/AC215-project/src/agents$ sh docker-shell.sh
[+] Building 1.0s (11/11) FINISHED                                docker:default
=> [internal] load build definition from Dockerfile              0.1s
=> => transferring dockerfile: 321B                             0.0s
=> [internal] load .dockerignore                                0.1s
=> => transferring context: 2B                                    0.0s
=> [internal] load metadata for docker.io/library/python:3.11-slim-buster 0.6s
=> [1/6] FROM docker.io/library/python:3.11-slim-buster@sha256:c46b0ae5728c2247b99903098ade3176a58e274d9c7d2efea 0.0s
=> [internal] load build context                                0.1s
=> => transferring context: 526B                                  0.1s
=> CACHED [2/6] RUN set -ex; pip install --no-cache-dir --upgrade pip && pip install pipenv 0.0s
=> CACHED [3/6] WORKDIR /app                                     0.0s
=> CACHED [4/6] COPY Pipfile Pipfile.lock /app/                 0.0s
=> CACHED [5/6] RUN pipenv install --deploy --ignore-pipfile    0.0s
=> CACHED [6/6] COPY . /app                                      0.0s
=> exporting to image                                           0.0s
=> => exporting layers                                           0.0s
=> => writing image sha256:3418854bb9fe35a1bc289fe4e326cb4c937cde4d4dd5dee94a430ac6677ba063 0.0s
=> => naming to docker.io/library/agents                        0.0s

What's Next?
View a summary of image vulnerabilities and recommendations → docker scout quickview
root@2537fc6e3c23:/app#
```

Containerized Components

As shown in the screenshots above, the data pipeline, Gemini fintuner, and agents components each run in their own container. The documentation and setup instructions for these containers are provided in the README file in our repository.

Versioned Data Strategy

Implement a data versioning strategy using tools like DVC or other suitable solutions. If feasible, this strategy should also be containerized to ensure portability and reproducibility of data processes. (Optional but recommended)

Please make sure to record your prompts as part of the data. For eg: If you are generating data using a LLM, please add the prompts and generated data as part of the dataset.

Deliverables:

- Documentation on the data versioning strategy chosen (e.g., DVC) and why
- A working containerized version of the data versioning pipeline (if applicable)
- Version control history showing tracked datasets, along with their respective versions, commits, and logs.

Teams Utilizing LLMs (Large Language Models)

Teams working with LLMs should implement a RAG setup. This setup should include data collection, chunking into appropriate sizes for processing, and the integration of a vector database. Teams should also fine-tune models and document the experimentation process.

Deliverables:

- A containerized RAG pipeline, including scripts for data chunking, vectorization, and integration with a vector database

Documentation of the fine-tuning process, including datasets used, hyperparameters, and models
Experiment logs showing model performance across different fine-tuning and RAG configurations.

Mock-up of the Application

A working prototype or mock-up of the final application that integrates all project components. Teams that have already submitted this in Milestone 1 should refine or extend their prototype based on feedback or new progress.

Deliverables:

An application mock-up or wireframe, including user interface elements and how the app will interact with back-end components

- **Use Branch 'milestone2':** Commit your work for Milestone 2 to the branch named 'milestone2'.
- **Mock Submission in README:** For each milestone, we include a mock submission section in your README file.
- **Canvas Group:** Finally, please choose your group for Milestone 2 on Canvas, where grades will be posted.
- **Canvas Submission:** You will be submitting your Github commit hash for grading. (See below on how to find commit hash)