Independent Study HW2

Lukas White

September 2025

1 Data Source and purpose

The source I will be using to start building an ai agent are

- A practical guide to building agents **PDF RESEARCH**
- OpenAI Agents SDK **BUILDING AGENT**
- https://www.youtube.com/watch?v=35nxORG1mtg **Research**
- Overleaf **DOCUMENTING**
- openAI and chatgbt. **RESEARCH, ai key**

2 Documentation of Process

Steps in setting up an AI agent

2.1 Download Materials

- Install Python 3.10 or higher
- Install openai-agents from internet

2.2 Create The Environment

Using the Terminal In Windows (CMD)

- `mkdir C:/Users/<YourName>/projects/my_agent`
- `cd C:/Users/<YourName>/projects/my_agent`
- **NOTE:** pip install will have (.venv) before it...

2.3 Get an OpenAI Key

- https://platform.openai.com/api-keys
- click on your profile picture → View API keys
- Create new secret key... You will only see once, SAVE IT!!!

2.4 Saving Key To Windows

This allows you to not need to enter it every time.

- `setx OPENAI_API_KEY "sk-your-real-key-here"`
- `echo %OPENAI_API_KEY%`
- **NOTE:** The echo is a test; only works in cmd, not PowerShell.

Now, everything is set up to go. Make sure you have a Python file in the folder where the project is that makes use of agents.

2.5 Running a Program

Must run in virtual environment; that is why we activate venv.

- `cd C:/Users/<YourName>/projects/my_agent`
- `.venv/Scripts/activate`
- `python "filename".py`

3 Usefulness of data

The data above is useful because it shows me and others how to set up and run an AI agent on a Windows device. It serves as a clear reference for future projects, helps avoid common setup errors, and provides a foundation for experimenting with and building more advanced AI agents. It also reinforces key skills like managing virtual environments, installing dependencies, and handling API keys.

4 Note from the PDF, Ignore

"Agents are systems that independently accomplish tasks on your behalf." Basically, typical LLM's do a single task, while agents make use of LLMs to manage workflow (sequence of steps needed to be executed).

- leverages an LLM to manage workflow execution and make decisions. Determines when workflow complete, can correct its actions if needed. Or even halt the execution.

- Accesses various tools to interact with external systems. Determines which is appropriate on the current task. Works within clearly defined guardrails.

When to use agents

- Complex decision-making
- Difficult-to-maintain rules
- Heavy reliance on unstructured data

Agent Design Foundation

- Model - The LLM powering the agent's reasoning.
- Tools - External Functions/APIs
- Instructions - Explicit guidelines defining agent behavior